UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

ANICETO JÚLIO JOÃO DE CARVALHO

ANÁLISE FORENSE EM *PERSONAL DIGITAL ASSISTANT* (PDA) COM WINDOWS MOBILE: TÉCNICAS, PROCEDIMENTOS E FERRAMENTAS

CRICIUMA, JULHO DE 2011

ANICETO JÚLIO JOÃO DE CARVALHO

ANÁLISE FORENSE EM *PERSONAL DIGITAL ASSISTANT* (PDA) COM WINDOWS MOBILE: TÉCNICAS, PROCEDIMENTOS E FERRAMENTAS

Trabalho de Conclusão de Curso apresentado para obtenção do Grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense.

Orientador: Prof. MSc. Paulo João Martins
Co-orientador: Prof. Esp. Sergio Coral

CRICIUMA, JULHO DE 2011

ANICETO JÚLIO JOÃO DE CARVALHO

ANÁLISE FORENSE EM *PERSONAL DIGITAL ASSISTANT* (PDA) COM WINDOWS MOBILE: TÉCNICAS, PROCEDIMENTOS E FERRAMENTAS

Submetido ao corpo docente do Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense como um dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

Profa. MSc. Ana Claudia Garcia Barbosa
Coordenadora do Curso de Ciência da Computação

Banca Examinadora:

Prof. MSc. Paulo João Martins (UNESC)
Orientador

Prof. Esp. Sérgio Coral (UNESC)
Co-Orientador

Prof. MSc. Gustavo Bisogni (UNESC)

Prof. Esp. Fabrício Giordani (UNESC)

Aos meus Pais e Irmãs, por ser a razão do esforço que tenho dedicado ao longo destes anos. Aos meus familiares e amigos que sempre me têm apoiado.

AGRADECIMENTOS

Antes de tudo agradeço a Deus por me ter iluminado durante toda a minha vida. Aos meus pais por me colocarem neste mundo e por tudo que têm feito para o meu bem estar. À Sonangol (Sociedade Nacional de Petróleos de Angola), por me dar a oportunidade de realizar um sonho e pelo grande projeto que se criou para o desenvolvimento de Angola. A todo coletivo da Unesc – Universidade do Extremo Sul Catarinense (direção, professores e funcionários), pelo apoio e atenção que tem dado aos estudantes Angolanos nesta grande Universidade.

Deixar um agradecimento especial aos meus pais Matias João de Carvalho e Maria Júlia Adão João, pelo carinho e por tudo que têm feito por mim, às minhas irmãs Herédia da Purificação João de Carvalho, Edna da Purificação João de Carvalho e Liudmila da Purificação João de Carvalho, pelo amor, atenção e paciência que têm dito com o irmão delas caçula. Ao Benja Satula, que tem sido como o Irmão mais velho que não tive a oportunidade de ter, pelo apoio, força, motivação e toda experiência que me transmitido, ao João Nime, pelo apoio de amigo, irmão que tenho recebido de ti, ao André Gonçalves por ser o meu irmão, amigo, e por toda paciência que acredito tiveste comigo durante os últimos quatro anos e meio. Ao coletivo da MSTUDIO, Sidney Webba, Ferraz Manuel, Heyde Ramos e Aguinaldo Cristiano, pela força, companheirismo e experiência que me têm transmitido. À Alexandra Dala, Winnie Machado, que me têm aturado durante a temporada no Brasil, a todos os Estudantes Angolanos em criciúma que direta ou indiretamente me têm apoiado em particular Emanuel Garcia, Erilson Barros (Wowo). A todos meus amigos e familiares que de certa forma sempre estiveram comigo.

“Procura deixar o mundo, hoje melhor do que ontem e amanha melhor do que hoje.” *Baden Powell*.

RESUMO

Atualmente o PDA, é um dispositivo equipado com funcionalidades de telefone, proporcionando maior poder computacional ao usuário. Ainda que tenham surgido diversas tecnologias para aquisição e análise forense em PDA, poucas são capazes de realizar a coleta em dispositivos com Windows Mobile, visto que eles dependem de protocolos e sistema operacional proprietário. Este documento fornece uma visão geral da perícia forense em Windows Mobile, descrevendo alguns métodos de aquisição e análise de dados. Os locais e formatos de dados, que são informações úteis sobre estes sistemas são descritos, incluindo mensagens de texto, multimídia, e-mail, artefatos de navegação na Web e entradas de registro. Este trabalho teve como objetivo a análise forense em PDA com Windows Mobile de forma a que possa coletar evidências existentes nestes dispositivos para reconstituição fatos criminalísticos. Foi usado o método da pesquisa bibliográfica; elaboração de um estudo de caso fictício que simulou a pericia forense computacional; com utilização da metodologia forense para dispositivos com Windows Mobile e suas 12 fases: preparação, segurança do cenário, levantamento e reconhecimento, documentação do cenário, comunicação, coleta das evidências voláteis, coleta das evidências não voláteis, preservação, exame, análise, apresentação e revisão. Conseguiu-se estudar e aplicar os conceitos de pericia forense computacional, analisando com sucesso muitos dos arquivos gerados pela aquisição da memória ROM do dispositivo, fazendo-se o uso das ferramentas MIAT, RAPI, MOBILedit e FTK. Provas periciais foram encontradas em alguns arquivos examinados, o que fez com que o caso tivesse um veredicto, embora, durante a análise de outros arquivos, não se tenha obtido sucesso.

Palavras-chave: Segurança; Crimes Digitais; Perícia Forense; PDA, Windows Mobile.

ABSTRACT

Nowadays the PDA is a device equipped with phone features, providing greater computer operability power to the user. Although several technologies have emerged for acquisition and forensic analysis on PDA, few of them are able to perform the collection in Windows Mobile devices, since they depend on protocols and proprietary operating system. This document provides an overview of forensic expertise on Windows Mobile, describing some methods of acquisition and data analysis. The locations and data formats that are useful information about these systems are described, including text messaging, multimedia, e-mail, Web browsing devices and registry entries. This study aimed the forensic analysis on Windows Mobile PDA in order to collect evidence that may exist in these devices for forensic reconstruction facts. It was carried out the method of literature search with the preparation of a fictional case study that simulated computer forensic expertise, with the use of forensic methodology for devices running Windows Mobile and its 12 stages: preparation, scenario security, survey and reconnaissance, documentation of the scene, communication, collection of volatile evidence, collection of non-volatile evidence, preservation, examination, analysis, presentation and review. It was possible to study and apply the concepts of computer forensic expertise, successfully analyzing many of the files generated by the acquisition of ROM memory device, making the use of tools MIAT, RAPI, MOBILedit and FTK. Forensic evidences were found in some files analyzed, which meant that the case had a verdict, although the analysis of other files has not been successful.

Keywords: Security, Computer Crime, Forensic expertise, PDA, Windows Mobile.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS

ACPO	*Association of Chief Police Officers*
API	*Application Programming Interface*
ARM	*Acorn RISC Machine*
ASCII	*American Standard Code for Information Interchange*
ATA	*Advanced Technology Attachment*
AVI	*Audio Video Interleave*
BMP	*Bitmap*
CPU	*Central Processing Unit*
CF	*Compact Flash*
CSI	*Crime Scene Investigation*
CRC	*Cyclic Redundancy Check*
DLL	*Dynamic Link Library*
DNA	*DeoxyriboNucleic Acid*
ENFSI	*European Network of Forensic Science Institutes*
FAT	*File Allocation Table*
FM	Frequência Modular
FTK	*Forensic Toolkit*
FTL	*Flash Translation Layer*
GB	*Giga Byte*
GIF	*Graphics Interchange Format*
GPRS	*General Packet Radio Service*
GPS	*Global Positioning System*
GSM	*Global System for Mobile Communications*

GWES	*Graphics, Windowing and Events*
HPCS	*High Performance Computing Systems*
HTML	*HyperText Markup Language*
ICCID	*Integrated Circuit Card Identifier*
IDC	*International Data Corporation*
IMEI	*International Mobile Equipment Identity*
IMSI	*International Mobile Subscriber Identity*
IOCE	*International Organization of Computer Evidence*
IrDA	*Infrared Data Association*
ISO	*International Organization for Standardization*
JFFS2	*Journaling Flash File System Version 2*
JPEG	*Joint Photographic Experts Group*
JTAG	*Joint Test Action Group*
MB	*Mega Byte*
MD5	*Message-Digest algorithm 5*
MIAT	*Mobile Internal Acquisition Tool*
MIDI	*Musical Instrument Digital Interface*
MIPS	*Microprocessor without Interlocked Pipeline Stages*
MMC	*Multi-Media Card Memory*
MMS	*Multimedia Messaging Service*
NIJ	*National Institute of Justice*
NTFS	*New Technology File System*
OEM	*Original Equipment Manufacturer*
OID	*Object Identifier*
PC	*Personal Computer*

PCMCIA	*Personal Computer Memory Card International Association*
PDA	*Personal Digital Assistant*
PDF	*Portable Document Format*
PIN	*Personal Identification Number*
PNG	*Portable Network Graphics*
PPC	*Pocket PC*
RAM	*Random Access Memory*
RAPI	*Remote Application Programming Interface*
ROM	*Read Only Memory*
RPC	*Remote Procedure Call*
RT	*Ray Tracing*
RTF	*Rich Text Format*
SD	*Secure Digital*
SH	*Super H*
SIM	*Subscriber Identity Module*
SO	Sistema Operacional
SoC	*System on Chip*
SWGDE	*Scientific Working Group on Digital Evidence*
TI	Tecnologia de Informação
TIFF	*Tagged Image File Format*
URL	*Uniform Resource Locator*
USB	*Universal Serial Bus*
WAV	*Waveform Audio File Format*
WLAN	*Wireless Local Area Network*
WWW	*World Wide Web*

XACT *Cross-platform Audio Creation Toolkit*

SUMÁRIO

1 INTRODUÇÃO

A evolução da sociedade foi acompanhada pelo avanço tecnológico que cada vez mais atinge as diferentes camadas da sociedade de forma benéfica. Mas também há um lado sinistro a tecnologia quando é usada para práticas ilegais de tipo pessoal, privado ou incorporado. Há muito que com a evolução, a sociedade tem convivido com os crimes e a violência que igualmente têm evoluído. Para tentar manter a ordem foram estabelecidas leis pelas autoridades.

A preservação, identificação, aquisição, documentação, interpretação e relatório do computador ou dados digitais, estão definidos como Forense digital. Este procedimento tem enfatizado a coleta e recuperação de evidências de um computador pessoal. Mas hoje em dia, o criminoso está correndo em paralelo com a tecnologia e está usando os mais recentes dispositivos atualizados consequentemente para alcançar as suas necessidades em atividades ilegais. Com esta evolução, a vida de peritos forenses se tornou mais complicada (KRUSE II; HEISER, 2002, tradução nossa).

Uma definição simples para crimes digitais segundo Stephenson (2000) são delitos cometidos com o uso de um computador ou um sistema computacional. Porém, a natureza de um crime digital é mais complexa.

A segurança da informação é uma área computacional que, ao longo dos anos, vêm adquirindo novos meios de tratamento. A necessidade de redes e computadores seguros existe há muitas décadas, e as organizações têm a responsabilidade de manter um controle completo sobre os dados e informações relevantes que ficam armazenados em seus equipamentos. Esse comprometimento com o controle dos ativos deu origem às investigações forenses (FIGG; ZHOU, 2007, tradução nossa).

Para Beal (2005) Segurança da informação é o processo de proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade.

A investigação forense em dispositivos eletrônicos portáteis é um campo relativamente novo e emergente, de grande interesse dentro do mundo da perícia forense digital. Na era moderna, o *Personal Digital Assistant* (PDA) é extremamente popular e é propenso a estar envolvido em crimes eletrônicos, principalmente devido ao seu tamanho compacto e características integradas. A família do PDA inclui principalmente dispositivos *Palm OS, BlackBerry, OS X, Symbian*, aparelhos com *Windows Mobile* (*Pocket PCs*) e *Android*. Entre estes, de acordo com IDC[1] o Windows Mobile, da Microsoft será a tecnologia que mais vai crescer nos próximos anos, saltando de uma participação de 5,5% para 20,9%, em 2015, quando ocupará o segundo lugar no ranking dos sistemas operacionais para *smartphone*, que é baseado no popular sistema operacional Windows da Microsoft e oferece uma aparência familiar. Além de fazer e receber chamadas telefônicas permite navegar na Internet, enviar e receber mensagens de texto / multimídia, bem como visualizar e editar documentos do Word, Excel e PowerPoint (NELSON; PHILIPS; ENFINGER; STEUART, 2005, tradução nossa).

Discrepâncias entre computação forense e perícia em dispositivo eletrônico portátil existem devido a vários fatores, incluindo:

a) vasta gama de modelos de hardware e acessórios;
b) diferente variedade de sistema operacional embarcado;
c) ciclo do produto pequeno, com novos modelos surgindo com grande frequência;
d) extrema orientação para mobilidade;

[1] Empresa líder em inteligência de mercado, consultoria e conferências nos segmentos de Tecnologia da Informação e Telecomunicações. Consultar (IDC, 2011).

e) sistema de arquivos residente em memória volátil em determinados dispositivos, enquanto não volátil em outros;
f) dispositivos híbridos, com recursos avançados de rede e comunicação;
g) suspensão de processos, quando desligado ou inativo, enquanto o dispositivo está ativo em segundo plano.

Dispositivos móveis, como Celulares, PDA e *Smartphone* podem conter algumas das mais importantes provas em investigações criminais. Os responsáveis pela aplicação da lei em todo o mundo precisam cada vez mais de possíveis vantagens para ajudar a solucionar crimes. Em muitos casos, os dispositivos móveis podem conter provas incriminatórias importantes que requerem peritos investigadores legais para resolverem um caso (KLAVER, 2010, tradução nossa).

O Windows CE (atualmente chamado de Windows Mobile) está no mercado há mais de 10 anos, No terceiro trimestre de 2009 a Microsoft atingiu uma quota de mercado de 8.8% dos mais de 41 milhões de celulares vendidos mundialmente neste trimestre. Isto faz com que seja um tema relevante na comunidade forense (KLAVER, 2010, tradução nossa).

Embora possam ser aplicados conhecimentos forenses em vários sistemas operacionais, há diferenças que requerem conhecimento especializado e ferramentas para localizar e interpretar dados digitais sobre esses sistemas. Esse é o papel da Perícia Forense, que tem por objetivo demonstrar, por meio de métodos científicos, a verdade, auxiliando na tomada de decisão final nos casos judiciais (CASEY, 2004, tradução nossa). De realçar a necessidade cada vez maior do uso de técnicas e ferramentas que venham a dificultar a prática delituosa e seu autor, facilitando os investigadores na busca e preservação de potenciais evidências digitais.

Este trabalho demonstrou como é realizada a análise forense, a utilização dos seus recursos, técnicas e ferramentas para a obtenção, recuperação e preservação de evidências

digitais em PDA como Windows Mobile, evidências que posteriormente possam ser utilizadas em questões judiciais. Usou-se um cenário genérico criado para espelhar situações de como resgatar as evidências, onde as mesmas foram inseridas, de formas a exemplificar o seu uso. Também se mostrou uma visão geral de algumas ferramentas, descrevendo a diversidade funcional e facilidades para a aquisição e análise das informações contidas no PDA. O cenário utilizado para revelar como determinadas ferramentas reagem em diversas situações. Embora um cenário genérico fosse utilizado na análise de ferramentas forense, os procedimentos não estão destinados a servir como um teste formal do produto ou como uma avaliação global. Além disso, não se pretendeu analisar as vantagens comparativas de uma ferramenta em relação a outras. O trabalho, ao contrário, oferece uma perspectiva e sondagem sobre o estado da perícia forense e das técnicas e ferramentas para dispositivos PDA atualmente.

1.1 OBJETIVO GERAL

Análise Forense em PDA com Windows Mobile de forma a que possa coletar evidências existentes nestes dispositivos para reconstituição fatos criminalísticos.

1.2 OBJETIVOS ESPECÍFICOS

Para concretizar esta pesquisa foram traçados os seguintes objetivos específicos:

a) enunciar e aplicar os conceitos e princípios de perícia forense computacional;
b) descrever o funcionamento e arquitetura do Sistema Operacional Windows Mobile;
c) elencar as diferentes técnicas e ferramentas utilizadas na obtenção, recuperação e preservação de evidências em PDA;

d) documentar e coletar evidências em dispositivos PDA;

e) utilizar um cenário para demonstrar como coletar as evidências.

1.3 JUSTIFICATIVA

A tecnologia avança e emerge de forma muito rápida em comparação há 10 anos, e em meio a milhões de telefones celulares e mais de 50 milhões de internautas, onde todos estão conectados de alguma, já está no inconsciente coletivo que ninguém pode, ou deve, ficar de fora desta viagem.

Dispositivos digitais portáteis, tais como PDA, tornaram-se mais acessíveis e comuns no ambiente de trabalho. Eles fornecem alta capacidade de armazenamento de dados, além de recursos computacionais e de rede, para gerenciar compromissos e informações de contato, revisão de documentos, comunicação via correio eletrônico e executar outras tarefas (AYERS; JANSEN, 2004, tradução nossa).

Dispositivos digitais portáteis são computadores simples com uma CPU, memória, baterias, interfaces de entrada, como um teclado e interfaces de saída, como uma tela ou fone de ouvido. Os dados contidos na memória são geralmente o foco de uma análise forense, mas é necessário ter-se compreensão de como é a entrada/saída dos dados, e os componentes necessários para acessar esses dados. Em alguns casos, pode ser suficiente operar manualmente um dispositivo lendo as informações do visor. No entanto, para recuperar dados apagados ou realizar exames mais avançados, especialmente projetados são necessárias ferramentas para interface com o dispositivo. O conhecimento de como os dados são manipulados e armazenados em dispositivos portáteis é por vezes necessário para adquirir todas as evidências digitais disponíveis a partir de dispositivos portáteis sem alterá-las e traduzi-las em uma forma legível (CASEY, 2004, tradução nossa).

Quando um PDA é encontrado durante uma investigação, algumas questões que no decorrer deste documento serão respondidas têm de ser consideradas: O que deve ser feito? Como o PDA deve ser tratado? Quão valiosos ou potencialmente relevantes podem ser os dados contidos no dispositivo a ser analisado? A chave para responder a essas perguntas está na compreensão do hardware e características de software do dispositivo (JANSEN; AYERS, 2004, tradução nossa).

Computação forense, também conhecida como análise forense computacional, realiza a descoberta de provas eletrônicas, descoberta digital, recuperação de dados, descoberta de dados, análise computacional. É o processo de análise de dispositivos digitais metodicamente computador (discos rígidos, disquetes, fitas, entre outros) para provas. Uma análise completa feita por um examinador qualificado pode resultar na reconstrução das atividades de um usuário de computador (VACCA, 2005, tradução nossa).

A Computação forense envolve a preservação, identificação, extração e documentação de dados ou informações codificadas de um computador ou qualquer outro dispositivo eletrônico, que servem como prova. A parte interessante da ciência é que as evidências são geralmente transparentes, criadas pelo sistema operacional do computador ou dispositivo sem o conhecimento do operador do computador. Para encontrá-las, ferramentas especiais de software e técnicas forenses são obrigatórias (ECKERT, 2002, tradução nossa).

Segundo Brill e Pollitt (2006) entender como forense computacional a coleta e a preservação de informações de mídias eletrônicas, hardware, software ou redes, deixa o gerenciamento dessa atividade uma questão crucial no processo investigativo.

Existem ferramentas especializadas para preservar e examinar certos tipos de evidências em dispositivos PDA. Para lidar com alguma dessas ferramentas, torna-se necessário entender o seu funcionamento completo, de forma a aproveitar-se a qualidade e funcionalidade das mesmas. Entender os métodos de execução da análise forense em PDA e

as definições da forense computacional mostra-se importante no sentido de explorar o seu conteúdo de forma detalhada e explicativa. A escolha e a análise das ferramentas para a coleta de evidências e o estudo de sua aplicação e preservação também representaram uma motivação adicional para a realização deste trabalho.

1.4 ESTRUTURA DA PESQUISA

Como já foi dito anteriormente, esta pesquisa tem como objetivo, a presente pesquisa tem como finalidade o estudo do processo forense em PDA com Windows Mobile, focando as técnicas e softwares usados atualmente para coletar e analisar evidências oriundas destes dispositivos. Contudo, o trabalho foi divido em duas partes: a primeira parte desta pesquisa foi constituída de um meticuloso levantamento bibliográfico a fim de obter referencial teórico para esta pesquisa, seguida pela parte prática que simulou um caso fictício para das técnicas e ferramentas forenses para coleta, exame e análise de evidências, em ambiente controlado.

No primeiro capítulo é apresentada uma introdução ao tema proposto, os objetivos gerais e específicos e a justificativa para realização deste projeto. De seguida é descrito o conceito geral de segurança da informação, crimes e evidências digitais, bem como é descrito o conceito de perícia forense computacional e questões jurídicas no que concernem crimes digitais, isto no capítulo dois. Ainda no segundo capítulo são apresentadas a metodologias para perícia forense computacional. Depois, no terceiro capítulo é apresentado o conceito de PDA, conceito e informações sobre o sistema operacional Windows Mobile, a arquitetura e características dos dispositivos PDA com Windows Mobile, estados genéricos, bem como um modelo de processo forense em PDA com Windows Mobile. Modelo este que foi usado como base nesta pesquisa. Neste capítulo (terceiro) são apresentadas ferramentas forense para

análise, coleta e preservação de evidências nestes dispositivos e a importância da perícia forense em dispositivos PDA.

O quarto capítulo são apresentados alguns os trabalhos correlatos, na área de forense computacional. No quinto capítulo tem-se o trabalho proposto, a metodologia utilizada bem como a descrição de um caso de estudo fictício, que simula uma perícia digital real.

Por fim, é possível encontrar a conclusão, descrevendo os resultados obtidos e recomendações para trabalhos futuros.

2 SEGURANÇA DA INFORMAÇÃO

A grande utilização de recursos de processamento e armazenamento de informações em um elevado número de computadores, nas mais diversas áreas de atividade humana tornou perspicaz a dependência em relação ao tipo de recurso utilizado. Porém, mais importante do que o aspecto de indisponibilidade dos equipamentos é a perda ou violação das informações que guardam (REZENDE; ABREU, 2000).

Nenhuma corrente é mais forte que seu elo mais fraco; da mesma forma, nenhuma parede é mais forte que sua porta ou janela mais fraca, do modo que se precisam colocar trancas resistentes. De forma similar, quando se implementa segurança em um ambiente de informações, o que na realidade procura-se fazer é eliminar os pontos fracos ou garantir a máxima segurança (CARUSO; STEFFEN, 1999).

Segundo Rezende e Abreu (2000) a informação é o dado com uma interpretação dada por seu usuário. Ela contém um valor bastante significativo, visto que está integrada com processos, pessoas, tecnologias e pode conceber grande poder para quem a possui.

Segurança da informação é a proteção física e lógica dos sistemas de informação contra acessos não autorizados e sua preservação contra destruição, tendo que se contemplar o aspecto da recuperação, da capacidade operacional em casos de destruição parcial ou total da capacidade de processamento (KRAUSE; TIPTON, 1999, tradução nossa).

Conforme Campos (2007) um sistema de segurança da informação baseia-se em três princípios básicos:

a) **confidencialidade**: significa proteger informações contra pessoas que não são explicitamente autorizadas. A informação deve ser protegida onde quer que esteja guardada, como por exemplo, mídia impressa ou mídia digital. Deve-se cuidar não apenas da proteção da informação como um todo, mas também de

partes da informação que podem ser utilizadas para interferir sobre o todo (CAMPOS, 2007).

b) **integridade**: é garantido quando a informação acessada está completa, sem alterações e, portanto, confiável. A alteração inclui ações como escrita, alteração no conteúdo, alteração no status, remoção e criação de informações. Deve-se considerar a proteção da informação nas suas mais variadas formas, como por exemplo, armazenada em discos (CAMPOS, 2007).

c) **disponibilidade**: é quando a informação está acessível, por pessoas autorizadas, sempre que necessário. O que consiste na proteção dos serviços prestados pelo sistema para que eles não sejam degradados ou se tornem indisponíveis sem autorização, assegurando ao usuário o acesso aos dados sempre que deles precisar (CAMPOS, 2007).

Segurança, mais do que uma estrutura hierárquica que envolve homens e equipamentos, está relacionada a uma postura gerencial. Dado o dinamismo que as atividades relacionadas com o processamento de informações adquiriram ao longo do tempo, exige-se que as políticas de segurança de informações sejam mais abrangentes e simples (CARUSO; STEFFEN, 1999).

Entende-se que política de segurança, é a política elaborada e implantada para formalização dos anseios da organização quanto à proteção das informações (CARUSO; STEFFEN, 1999).

Para Dias (2000) política de segurança é uma estrutura preventiva de proteção dos dados e processos importantes de uma organização que determina um padrão de segurança a ser adotado.

A política de segurança de informações estabelece princípios de como a organização deve proteger, controlar e monitorar os recursos computacionais e,

consequentemente, informações manipuladas dentro da organização, estabelecendo responsabilidades das funções relacionadas com a segurança, descriminando as principais ameaças, riscos e impactos envolvidos, indo além dos aspectos relacionados com sistemas de informação ou recursos computacionais (DIAS, 2000).

2.1 CRIMES DIGITAIS

Hoje se vive e trabalha-se em um mundo de conectividade. Pode-se conversar ou fazer transações monetárias de milhões de dólares com pessoas do outro lado do planeta de forma rápida e barata. A proliferação de computadores pessoais, acesso fácil à Internet, e um mercado em expansão relacionado com novos dispositivos de comunicação, mudaram a forma como se gasta o tempo e como se faz negócio.

A forma com que os criminosos cometem crimes também tem mudado. A acessibilidade universal ao digital abre novas oportunidades para os inescrupulosos. Milhões de dólares são perdidos para os criminosos que usam dispositivos computacionais (MIDDLETON, 2002, tradução nossa).

Em muitos casos, as autoridades policiais têm ficado para trás destes criminosos, por falta de tecnologia e pessoal treinado para resolver esta nova e crescente ameaça que tem sido apropriadamente chamada de Crime Digital.

Recentemente, em tecnologias de informação (TI) não se tinha consciência nem interesse no fenômeno de crimes digitais. Em muitos casos, a aplicação da lei e a falta de ferramentas necessárias para resolver o problema (CASEY, 2004, tradução nossa).

O “Crime digital” é um termo amplo que abrange todas as formas em que os computadores e outros tipos de dispositivos eletrônicos, capazes de se conectar a Internet são usados para quebrar as leis e causar danos. Uma definição um pouco mais técnica seria, uso

de computadores ou outros dispositivos eletrônicos por meio de sistemas de informação, tais como redes organizacionais ou na Internet para facilitar os comportamentos ilegais (MCQUADE, 2009, tradução nossa).

Conforme Vacca (2005) o crime digital ocorre quando a tecnologia de informação (dispositivos eletrônicos, rede) é usada para cometer ou encobrir um crime, onde estes dispositivos eletrônicos podem ou não podem ter desempenhado um papel fundamental na prática de um crime.

Crimes digitais incluem:

a) Fraude financeira;
b) Sabotagem de dados ou redes;
c) Roubo de propriedade de informação;
d) Penetração em sistemas de informação a partir do exterior e negação de acesso ao serviço;
e) Vírus de Internet, que são a principal causa para que usuários não autorizados tenham acesso a sistemas e redes por meio da Internet.

Crimes digitais podem ser categorizados como eventos internos ou externos. Normalmente, a maior ameaça para as organizações tem sido os empregados, razão pela qual o crime informático é muitas vezes referido como um crime de informação privilegiada (VACCA, 2005, tradução nossa).

Além do roubo de componentes, alguns dos primeiros crimes digitais registrados ocorreram em 1969 e 1970, quando certos indivíduos descobriram métodos para ganhar acesso não autorizado aos computadores compartilhados, um ato que foi ilegal na época. Foram julgados de acordo com as leis existentes. No entanto, houve contradição legal porque a propriedade digital era vista como intangível, portanto, fora das leis de proteção da propriedade física. Desde então, a distinção entre a propriedade digital e física tornou-se

menos pronunciada e as leis são muitas vezes as mesmas utilizadas para proteger os dois casos (CASEY, 2004, tradução nossa).

Invasão de computadores e fraudes cometidas com a ajuda de computadores foram os primeiros crimes a ser amplamente reconhecidos como um novo tipo de crime. A lei da Florida de crimes digitais definiu o acesso não autorizado a um computador como um crime, mesmo que não houve maldade no ato. Foi durante este tempo que os governos ao redor do mundo começaram a promulgar leis similares. (VACCA, 2005, tradução nossa).

Na década de 1990, a comercialização da Internet e o desenvolvimento da *World Wide Web* (WWW) popularizou a Internet, tornando o crime global e diversificado. Como o leque de crimes que são cometidos com o auxílio do computador aumentou, novas leis para lidar com direitos de autor, pornografia infantil e privacidade foram decretadas (CASEY, 2004, tradução nossa).

A rápida evolução da tecnologia e da criminalidade digital criou uma necessidade de especialização: técnicos de crime digital, cenário para recolher evidências digitais, examinadores para o processo de evidências obtidas, investigadores digitais que analisem todos os elementos disponíveis para construir um caso. Além de recuperar evidências de um incidente de segurança, muitas vezes é necessário recolher a evidência digital para determinar o que ocorreu e ajudar os tomadores de decisão avaliar o problema (SHINDER; TITTEL, 2002, tradução nossa).

Mesmo quando um indivíduo é responsável pela coleta, processamento e análise de evidências digitais, é útil considerar essas tarefas separadamente. Cada área de especialização exige procedimentos e habilidades diferentes - lidar com eles separadamente facilita a formação e definição de padrões em cada área. Percebendo a necessidade de padronização no treinamento e melhores práticas, em 2002, o *Scientific Working Group on Digital Evidence* (SWGDE) publicou orientações para a formação e boas práticas. Existem

esforços semelhantes para desenvolver o exame de evidências digitais em uma disciplina acreditada sob as normas internacionais[2] ISSO/IEC 17025 e ENFSI 2003 (JOHNSON, 2005, tradução nossa).

O desenvolvimento de algumas normas criou uma necessidade de normas de conduta para os indivíduos no campo. Para responder a esta necessidade, certificação e programas de treinamento foram desenvolvidos para garantir que os examinadores de provas digitais tenham as habilidades necessárias para executar o seu trabalho com competência e seguir os procedimentos aprovados (PROSISE; MANDIA, 2003, tradução nossa).

Há um aspecto positivo para o uso crescente da tecnologia por criminosos - a participação dos computadores no crime resultou em uma abundância de evidências digitais que podem ser usadas para deter e processar infratores (CASEY, 2004, tradução nossa).

Provas digitais podem ser úteis em uma ampla gama de investigações criminais incluindo homicídios, crimes sexuais, pessoas desaparecidas, abuso infantil, tráfico de drogas e assédio. Além disso, os processos civis podem depender de prova digital, e a descoberta digital está se tornando uma rotina de litígios em matéria civil (SHINDER; TITTEL, 2002, tradução nossa).

2.2 EVIDÊNCIAS DIGITAIS

A evidência digital é definida como todos os dados armazenados ou transmitidos por meio de um computador que apoiar ou refutar uma teoria de como um delito ocorreu ou que abordem elementos críticos do delito, tais como intenção ou álibi (VACCA, 2005, tradução nossa).

[2]Norma que estabelece os critérios para laboratórios que desejam demonstrar sua competência técnica, que possuem um sistema da qualidade efetivo e que são capazes de produzir resultados tecnicamente válidos Consultar (IPAC, 2010).

Segundo Casey (2004) evidências digitais são quaisquer dados que provam que um crime foi cometido, ou que podem proporcionar uma ligação entre um crime e sua vítima ou um crime e o seu autor.

A definição proposta pelo *Scientific Working Group on Digital Evidence*, diz que evidência digital é toda a informação de valor probatório que seja armazenada ou transmitida de forma digital (SCHWEITZER, 2003, tradução nossa). Outra definição proposta pela *Internation Organization of Computer Evidence* (IOCE), é a informação armazenada ou transmitida na forma binária que pode ser invocada em juízo. No entanto, estas definições concentram-se na evidência e os dados de negligência que formam uma investigação. Além disso, o binário na definição do termo posterior é inexato, descrevendo apenas uma das muitas representações comuns de dados informatizados (STEPHENSON, 2000, tradução nossa).

Os dados referidos nestas definições são essencialmente uma combinação de números que representam informações de vários tipos, incluindo textos, imagens, áudio e vídeo. Os termos Evidências digitais e provas eletrônicas são por vezes utilizados de forma intercambiável (HENSELER, 2000, tradução nossa).

Dada à onipresença de evidências digitais, é raro que o crime não tenha dados relacionados armazenados e transmitidos por meio de sistemas informáticos. Uma pessoa treinada pode usar estes dados para compilar muita coisa sobre um indivíduo, fornecendo a introspecção tal que é como olhar por meio de um vitral para a vida pessoal do indivíduo e pensamentos (STEPHENSON, 2000, tradução nossa).

O computador pessoal de um indivíduo e a utilização dos serviços de rede são arquivos de comportamento eficazes, podendo reter mais informações sobre atividades do indivíduo, e até mesmo de seus familiares e amigos mais próximos (CASEY 2003, tradução nossa).

2.2.1 Aspectos Desafiadores da Evidência Digital

A evidência digital como uma forma de evidência física cria vários desafios para os examinadores forenses. Por exemplo, um prato de disco rígido contém uma mistura de elementos de dados diversos – pedaços misturados de informação em camadas, que ficam em cima uns dos outros ao longo do tempo. Apenas uma pequena parte destes elementos pode ser relevante para um processo, tornando-se necessário extrair partes úteis, encaixá-los juntos, e traduzi-los em um formulário que pode ser interpretado (HORSEWELL 2004, tradução nossa).

Da mesma forma, as ondas de rádio e micro-ondas viajam por meio do ar e contêm um emaranhado de dados, tornando-se necessário encontrar o sinal desejado entre o ruído e traduzi-lo para dados que podem ser entendidos (Figura 1). Esta é conceitualmente semelhante à análise de DNA - as informações pertinentes devem ser extraídas do fluido humano / tecido, processadas e convertidas de uma forma que se compreenda (CASEY 2003, tradução nossa).

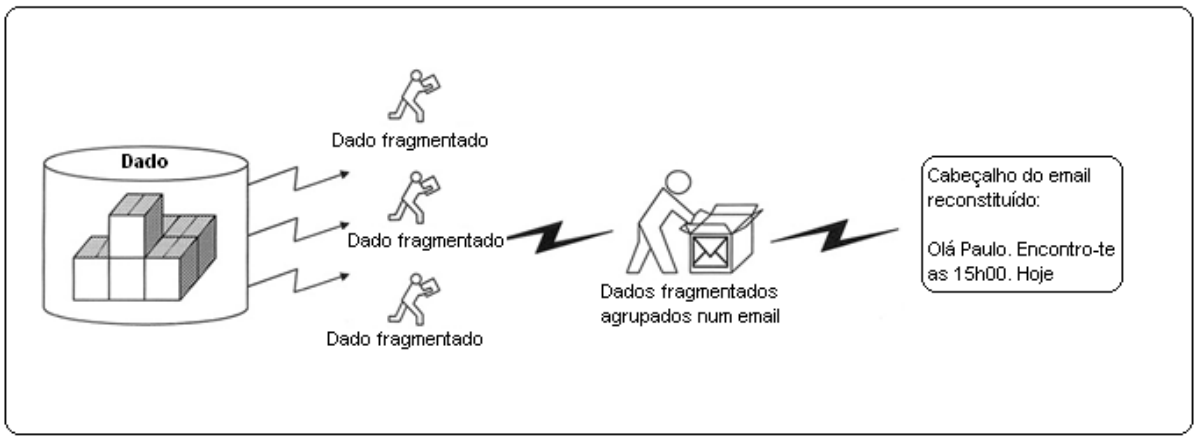


Figura 1. Representação conceitual de fragmentos de dados sendo extraídos de um prato de disco rígido, combinados e traduzidos em uma mensagem de email.
Fonte: CASEY, E. (2003)

A evidência digital é geralmente uma abstração de algum evento ou objeto digital. Quando uma pessoa instrui um computador a executar uma tarefa, como enviar um e-mail, as atividades geram resíduos resultantes dos dados que dão apenas uma visão parcial do que ocorreu (CASEY, 2004, tradução nossa).

Quando essas minúcias são registradas, os impulsos elétricos dos nossos cliques do mouse e pressão nas teclas devem ser traduzidos em dados antes que tenham algum significado. Da mesma forma, uma mensagem de e-mail e servidor de log armazenados em um disco são o resultado de várias camadas de abstração de campos magnéticos sobre o disco para as letras e números que vemos na tela. Portanto, nunca vemos os dados reais, apenas uma representação, e cada camada de abstração pode introduzir erros (CASEY, 2004, tradução nossa).

O fato de que a evidência digital pode ser manipulada tão facilmente traz novos desafios para os pesquisadores digitais. Estas evidências podem ser alteradas maliciosamente por criminosos ou acidentalmente durante a coleta, sem deixar sinais evidentes de distorção (CASEY, 2003, tradução nossa). A prova digital tem as seguintes características para atenuar esse problema:

- pode ser copiada com precisão, e esta cópia pode ser examinada como se fosse a original. É prática comum quando se trata de prova digital para examinar uma cópia, evitando assim o risco de danificar o original.
- com as ferramentas certas, é fácil determinar se a evidência digital tenha sido modificada ou alterada comparando-a com uma cópia do original.
- evidência digital é difícil de destruir, mesmo quando um arquivo é “excluído” ou um disco rígido é formatado, a evidência pode ser recuperada.

Apesar de sua predominância, poucas pessoas estão bem versadas nas questões de evidências técnicas e jurídicas relacionadas com as evidências digitais e, como resultado é

muitas das vezes esquecida, recolhida de forma incorreta, ou analisada de forma ineficaz (LEE; PALMBACH; MILLER, 2001, tradução nossa).

A complexidade dos casos forenses e as evidências que se baseiam em computador têm aumentado significativamente ao longo dos anos com o aumento na sofisticação dos sistemas de computador e uma maior utilização da Internet.

Para Lee, Palmbach e Miller (2001), por conseguinte, no passado, tenderam a confiar em provas de computador que consistiam essencialmente de discos independentes ou arquivos do disco. Os casos mais recentes têm contado cada vez mais com provas digitais recolhidas a partir de uma variedade de fontes.

Como resultado da utilização de meios magnéticos pela grande maioria de computadores pessoais, há um setor de serviços que cresce nas áreas de recuperação de dados eletrônicos e descoberta de evidências em mídias magnética (MARCELLA; GREENFIELD, 2008, tradução nossa).

Imagem e procedimentos de investigação para dispositivos móveis, tais como telefones e PDA, não são tão bem estabelecidas como para laptops, computadores desktop e dispositivos de armazenamento do computador. No entanto, dispositivos móveis tornaram-se um item padrão de negócios, na vida doméstica, e são susceptíveis de conter informações importantes sobre as atividades de uma pessoa, que podem ter um valor significativo na investigação de um crime. Existem algumas diferenças entre a manipulação destes dispositivos e a dos computadores e discos devido à diferença de tecnologia (CASEY, 2004, tradução nossa). Em particular, não há padronização e muito menos entre os dispositivos deste tipo porque eles são mais recentes. No entanto, como resultado de sua colocação no mercado em rápido crescimento, já se tem lidado com os dispositivos móveis como uma questão de rotina e, em certa medida, também com PDA (GEORGE ET AL, 2003, tradução nossa).

2.2.2 Questões de Jurisdição

Outro fator que torna difícil uma definição rápida de crime digital é o dilema de jurisdição. As leis em diferentes jurisdições definem os termos de maneira diferente, e é importante para peritos que investigam a criminalidade digital, bem como administradores de rede que querem envolver-se em julgar crimes digitais que são cometidos contra suas redes, familiarizar-se com as leis aplicáveis (ECKERT, 2002, tradução nossa).

Como crimes digitais ocorrem frequentemente em um lugar "virtual" que se chama de espaço digital, torna-se mais difícil saber que leis se aplicam. Em muitos casos, o autor e a vítima estão a centenas ou milhares de quilômetros de distância e talvez nunca estiveram no mesmo estado ou até mesmo país. Como as leis podem variar drasticamente em diferentes jurisdições geográficas, um ato que é ilegal em um local pode ser legal em outro (SHINDER; TITTEL, 2002, tradução nossa).

A noção de crimes digitais ou crimes cometidos com o uso de dispositivos computacionais é relativamente recente, por isso ainda não existem no Brasil, leis específicas para tais atos. Tem-se nos dias de hoje, os seguintes artigos do código civil: Art. 186, o Art. 186, e o Art. 927, que são usados para condenar os praticantes de tais delitos (AGUIAR, 2009). Para visualizá-los na íntegra, consultar o anexo A.

Ainda para Aguiar (2009) a penalidade para esse tipo de crime, é atualmente assentada por meio de uma adaptação do mesmo para leis vigorantes, não específicas para crimes digitais, levando-se em consideração a consequência deles sobre as vitimas. Em algumas ocorrências, tais adaptações geram falhas nas tipificações de crimes cometidos usando-se dispositivos computacionais.

Por exemplo, segundo Pinheiro (2008) usar a tipificação de crime de latrocínio em ambiente computacional, pode em certas ocorrências, invalidar o crime, visto que um agente

criminoso que invade um servidor e copia informações a partir dele, não poderá ser condenado por latrocínio, já que a tipificação do mesmo significa subtrair coisa alheia. Neste caso é importante ressalvar que, o fato de copiar a informação não a subtraiu, fazendo com que este tipo de crime seja desqualificado para tal tipificação. Devido a este motivo, projetos de lei estão de fase de votação de formas a suprimir tais carências, visando punir e diminuir ocorrências de crimes de natureza digitais.

De acordo com Aguiar (2009) o Projeto de Lei (PL) nº 84/99 é um dos projetos mais importantes na câmara dos Deputados, que estão em tramite no Congresso Nacional e cujo objetivo é a regulamentação dos casos de crimes digitais.

O PL nº 84/99, prevê sete modalidades de crimes digitais, chegando até seis anos de reclusão e multa. O objetivo fundamental do projeto é o suprimento das lacunas na legislação brasileira, retratando atos que não existem na legislação penal em vigor. No anexo B poderá ser visualizado na íntegra.

2.3 PERÍCIA FORENSE COMPUTACIONAL

Conforme Vacca (2005) computação forense é a ciência de adquirir, recuperar, preservar e apresentar dados que foram processados eletronicamente e armazenados em suportes informáticos.

A computação forense é uma disciplina relativamente nova que tem o potencial de afetar significativamente a tipos específicos de investigações e processos. Com o número maior de pessoas a fazem o uso de computadores, mais e mais informações de diferentes tipos têm sido armazenadas neles. Isso inclui informações que são de importância significativa, tais como indícios de fraude financeira, latrocínio, rescisão de emprego ilícita, assédio sexual,

pornografia infantil, roubo de segredos comerciais, ou a infidelidade conjugal, só para citar alguns (CASEY, 2003, tradução nossa).

Esta ciência é diferente das tradicionais ciências forense. Para começar, as ferramentas e técnicas necessárias estão facilmente disponíveis a qualquer pessoa que pretenda realizar uma investigação forense. Em contraste com a tradicional análise forense, não há geralmente a exigência de que os exames sejam realizados apenas em um ambiente controlado. Ao invés de produzir conclusões que exigem interpretação técnica, a ciência da computação forense produz informação direta e, dados que podem desempenhar um papel significativo na apreensão ou condenação de criminosos cibernéticos (ECKERT, 2002, tradução nossa).

A aquisição de dados digitais começa quando as informações e / ou bens físicos são coletados ou armazenados em antecipação a serem examinados. O termo “evidência” implica que o coletor de dados é reconhecido pelos tribunais e que o processo de coleta é entendido como um processo legal apropriado. Um objeto de dados ou item físico só se prova quando assim consideradas por um oficial da lei ou representante (FARMER; VENEMA, 2007).

A seguir, são várias definições importantes usadas para delinear certos aspectos da ciência da computação forense:

a) **objetos de dados**: informações de valor potencial probatório que estão associados a elementos físicos. Os objetos de dados podem ocorrer em diferentes formatos de arquivo (por exemplo, o NTFS ou FAT32), sem alteração da informação original (ECKERT, 2002, tradução nossa).
b) **evidências digitais**: são as informações de valor probatório que são armazenados ou transmitidos de forma digital CASEY, 2004, tradução nossa).

c) **itens físicos**: os itens em que os objetos de dados ou informações podem ser armazenados e / ou por meio do qual os objetos de dados são transferidos.

d) **evidência digital original**: elementos físicos e objetos de dados associados com esses itens no momento da aquisição ou da apreensão (ECKERT, 2002, tradução nossa).

e) **evidências digitais duplicadas**: é uma reprodução digital exata de todos os objetos de dados contidos em um item físico original (ECKERT, 2002, tradução nossa).

Nenhuma investigação envolvendo a revisão dos documentos, seja em um ambiente criminal ou empresarial, é completa sem a inclusão de provas devidamente tratadas. A Computação forense garante a preservação e autenticação de dados digitais, que são frágeis por natureza e podem ser facilmente alterados, apagados, se não forem devidamente tratados (JOHNSON, 2005, tradução nossa).

Além disso, a computação forense facilita a recuperação e análise de arquivos apagados e outras formas de informações convincentes de que normalmente são invisíveis para o usuário.

Segundo Reyes (2007) a computação forense está preocupada principalmente com os procedimentos forenses, as regras da evidência, e processos judiciais. É só secundariamente envolvida com computadores e outros dispositivos eletrônicos. Portanto, em contraste com todas as outras áreas da computação, onde a velocidade é a principal preocupação, em computação forense é de absoluta precisão. Fala-se de concluir os trabalhos tão eficientemente quanto possível, isto é, o mais rápido possível sem sacrificar a precisão.

Neste mundo onde aparentemente o recurso de tempo é geralmente um prêmio, a pressão é empilhada em cima de todos para trabalhar mais rápido possível. Trabalhando sob

essa pressão para conseguir prazos pode induzir as pessoas a tomar atalhos, a fim de poupar tempo.

Em computação forense, como em qualquer ramo da ciência forense, a ênfase deve ser a integridade e a segurança da evidência. Ao observar esta prioridade, cada profissional forense deve obedecer rigorosamente. Essas orientações não abrangem a obtenção de atalhos, e o profissional forense admite que o recurso de tempo deva ser gasto para manter os mais altos padrões de trabalho (MARCELLA; GREEFIELD, 2008, tradução nossa).

De acordo com Vacca (2005) um especialista forense é a pessoa responsável por fazer uma investigação forense digital. Este profissional terá várias etapas cuidadosas para identificar, na tentativa de obter evidências possíveis que podem existir em um sistema computacional:

a) proteger o dispositivo durante o exame forense contra qualquer alteração possível, danos, corrupção de dados ou introdução de vírus;
b) descobrir todos os arquivos no sistema. Isso inclui arquivos normais existentes, arquivos excluídos, arquivos ocultos, arquivos protegidos por senha e arquivos criptografados;
c) recuperar todos (ou tanto quanto possível) arquivos apagados;
d) revelar (na medida do possível) o conteúdo dos arquivos ocultos, bem como temporário ou trocar arquivos usados por ambos os programas de aplicação do sistema operacional;
e) acessar (se possível e se legalmente apropriado) o conteúdo das áreas protegidas ou arquivos criptografados;
f) analisar todos os dados possivelmente relevantes encontrados em especial (e normalmente inacessíveis) nas áreas de um disco;

g) imprimir uma análise global do sistema de computador, bem como uma listagem de todos os arquivos possivelmente relevantes e descobrir o arquivo de dados;

h) fornecer consulta a um especialista e / ou testemunhas.

2.3.1 Princípios e Procedimentos

As investigações e os incidentes são tratados de maneira diferente, dependendo das circunstâncias do incidente, a gravidade do incidente, bem como a preparação e experiência da equipa de investigação. Investigações digitais são comparáveis às cenas do crime, onde técnicas de investigação utilizadas pela aplicação da lei têm sido aplicadas como fundamento para a criação de procedimentos utilizados quando se trata de evidências digitais (JOHNSON, 2005, tradução nossa). Este capítulo fornecerá uma visão geral de vários modelos de procedimentos e princípios que têm sido propostos.

O'Connor (2004) propõe um conjunto de normas que servem como um guia para lidar com provas em um tribunal de justiça. Vários fatores de confiabilidade, que devem ser mantidos em mente a quando da aplicação e elaboração de relatórios sobre uma técnica científica que se está a usar em um exame forense:

a) **testabilidade**: A teoria científica ou técnica foi testada empiricamente? De acordo com Popper (1974) sobre o crescimento do conhecimento científico, o critério sobre o status científico de uma teoria é sua falseabilidade, refutabilidade, e testabilidade;

b) **aceitação**: Será que a teoria científica ou técnica foi submetida à revisão e publicada? Isso garante que as falhas na metodologia sejam detectadas para que a técnica encontre seu caminho para o uso por meio da literatura;

c) **taxa de erro**: Qual é a potencial taxa de erro detectada? Medidas científicas estão geralmente, associadas taxas de erro, que pode ser estimada com razoável precisão. Conhecido existem ameaças contra a validade e confiabilidade em cada evidência de uma teoria;

d) **credibilidade**: O que é qualificação do perito e estatura na comunidade científica? A técnica deve contar com as habilidades especiais e equipamentos de um especialista, ou pode ser replicado por outros peritos em outro lugar?

e) **clareza**: Pode a técnica e os seus resultados serem explicados com suficiente clareza e simplicidade para que o juiz e os jurados podem entender o seu significado simples? Este critério é assumido a ser incorporados implicitamente.

Em geral, mesmo fora das investigações policiais, as evidências devem ser coletadas de maneira que sejam admissíveis em tribunal. Pode não ser óbvio quando uma investigação é iniciada.

2.3.2 Princípios Evidenciais

Segundo a *Association of Chief Police Officers* **(**ACPO, 2007, tradução nossa), para qualquer investigação princípios básicos são propostos na hora de lidar com evidências digitais (em ambos os aspectos, físicos e lógicos). O lado físico envolve componentes de hardware, periféricos e meios de comunicação, que podem conter dados ou os meios para acessá-los, enquanto o lado lógico lida com os dados brutos extraídos de uma fonte de informação relevante (WILKINSON, 2007, tradução nossa). O Guia de boas práticas para o computador baseado em provas digitais apresentado pela ACPO (ACPO, 2007, tradução nossa) sugere quatro princípios básicos. A citar:

a) nenhuma ação realizada por investigadores deve resultar na alteração dos dados contidos em dispositivos digitais ou meios de armazenamento;
b) os indivíduos que têm acesso aos dados originais devem ser competentes para fazer isso e ter a capacidade de explicar suas ações;
c) uma trilha de auditoria ou outro registro de processos aplicados devem ser adequados para revisão de terceiros. Precisa-se documentar cada passo do processo investigativo;
d) o indivíduo encarregado da investigação tem a responsabilidade de garantir que os procedimentos acima mencionados sejam seguidos em conformidade com as leis que regem tais práticas.

Os princípios anteriormente citados visam garantir a integridade e a responsabilidade das evidências digitais por meio de seu ciclo de vida. O manuseio correto de uma evidência é sempre vital para que seja admissível em processos judiciais. No entanto, padrões diferentes podem ser aplicados a diferentes tipos de investigações. O grau de formação e competências necessárias para executar uma tarefa judicial depende muito do nível de evidência necessária no caso (ACPO, 2007, tradução nossa).

2.4 METODOLOGIAS INVESTIGATIVAS

A metodologia a ser utilizada pelo perito forense pode ser diferenciada, no que concerne o sistema e dispositivo tecnológico envolvido. Visto que não havia métodos específicos que não alterassem de acordo com a tecnologia usada, fazia com que houvesse pouca credibilidade nas provas periciais apresentadas em casos judiciais.

Na tentativa aumentar a credibilidade e solidificar a perícia forense computacional em casos judiciais, criaram-se metodologias que são usadas como guias no

processo investigativo, que definem etapas a serem cumpridas pelos peritos, independentemente do dispositivo ou sistema computacional em causa, bem como as ferramentas a serem utilizadas (BERNARDO, 2006).

2.4.1 Modelo DFRWS

Criado por Gary Palmer no primeiro Digital Forensics Research WorkShop (DFRWS), recomenda sete etapas (BERTOGLIO, 2008):

a) **identificação**: compreende o método por meio do qual o perito é notificado sobre o incidente;
b) **preservação**: fase em que a integridade e estado das evidências devem ser asseguradas;
c) **coleta**: é realizada a extração ou coleta de itens individuais ou em grupo, usando-se de métodos específicos e ferramentas para aquisição de evidências;
d) **exame**: faz-se a análise cuidadosa dos itens e suas características e atributos. Nesta fase o foco está na extração de informações das evidências encontradas, sem o intuito de tirar conclusões sobre o caso;
e) **análise**: nesta fase analisam-se todas as evidências encontradas desde o início da investigação, com a finalidade de desenvolver um conjunto de conclusões em relação às evidências apresentadas;
f) **apresentação**: o perito deve relatar os fatos de maneira organizada, clara, concisa e objetiva;
g) **decisão**: contempla-se a etapa anterior, a apresentação de laudos periciais para o tribunal, onde o perito determina as suas conclusões sobre o caso.

2.4.2 Modelo de Reith, Carr e Gunsch

Modelo proposto por Reith, Carr e Gunsch (2002), também conhecido como *Abstract Digital Forensics Model*, possui certas analogias com o modelo DFRWS. Ambos apresentam as etapas de preservação, coleta, exame e apresentação, sendo a particularidade presente neste modelo, o fato de ele proporcionar suporte à preparação de ferramentas e uma dinâmica formulação de abordagens investigativas.

A estrutura do modelo é fundamentada em nove etapas, citadas a seguir (BARYAMUREEBA; TUSHABE, 2004, tradução nossa):

- **identificação**: reconhecimento do incidente;
- **preparação**: preparação das ferramentas, técnicas, monitoração de autorização, mandatos de busca e suporte;
- **estratégia** e abordagem: desenvolvimento de uma estratégia de coleta de evidências que maximize a coleta de evidências não infectadas, e minimize o impacto para a vítima;
- **preservação**: proteção e conservação do estado físico e digital das evidências;
- **coleta**: gravação da cena do crime e reprodução das evidências digitais usando procedimentos aceitos e padronizados;
- **exame**: busca aprofundada e sistemática das provas relativas à suspeita do crime;
- **análise**: reconstrução dos fragmentos de dados e elaboração de conclusões baseadas nas provas encontradas;
- **apresentação**: explicação das conclusões;

- **devolução das evidências**: garante que a propriedade física e digital seja devolvida ao proprietário.

2.4.3 Modelo de aplicação da Lei do NIJ (National Institute of Justice)

O guia de investigação de cenas de crimes digitais, também conhecido como *NIJ Law Enforcement Model* é um documento para primeiros socorros, produzido pelo Departamento de justiça dos EUA (NIJ, 2004), que oferece as seguintes sugestões quando se trata de uma cena de crime digital:

a) **preservar e avaliar a cena:** são tomadas medidas para garantir a segurança das pessoas e identificar e proteger a integridade das provas;

b) **documentar a cena:** cria-se um registro permanente da cena, onde serão registradas com precisão todas as provas convencionais relacionadas;

c) **coleta de provas:** provas tradicionais e digitais devem ser coletadas de forma que se preserve o valor probatório;

d) **acondicionamento, transporte e armazenamento**: deve-se tomar precauções adequadas quanto à embalagem, transporte e armazenamento das provas, mantendo a cadeia de custódia.

2.4.4 Modelo IDIP (Integrated Digital Investigation Model)

Brian Carrier e Eugene Spafford propuseram outro modelo que organiza o processo em cinco grupos constituídos no geral por 17 fases (Figura 2).

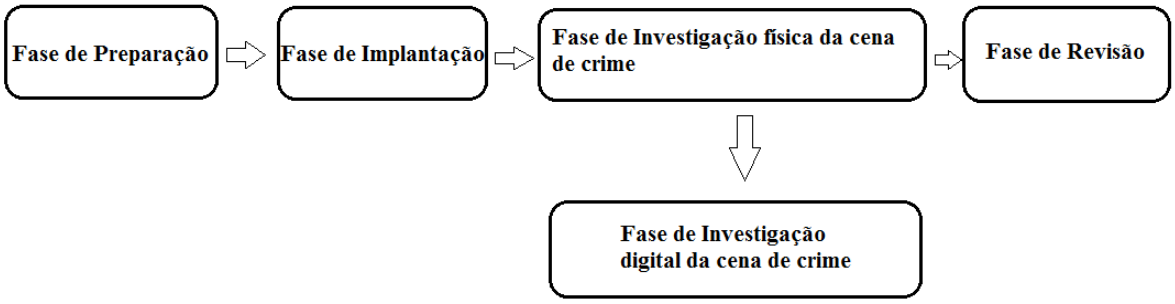


Figura 2. Fase do Modelo IDIP
Fonte: CARRIER, B; SPAFFORD, E. H. (2003)

2.4.4.1 Fases de Preparação

O objetivo desta fase é garantir que as operações e infra**e**struturas sejam capazes de apoiar completamente uma investigação. Ela inclui duas fases:

a) fase de preparação da operação: garante que a capacidade humana esteja totalmente preparada e equipada para lidar com um incidente;
b) fase de preparação da infraestrutura: que garante que a infraestrutura básica seja suficiente para lidar com incidentes. Por exemplo, equipamentos como as câmeras vídeo, leitores de cartão de memória e boas condições de trabalho.

2.4.4.2 Fase de Implantação

O objetivo desta fase é fornecer um mecanismo para que um incidente seja detectado e confirmado. Compreende duas fases:

a) Fase de detecção e notificação: onde o incidente é detectado e, em seguida, garantir que as pessoas adequadas sejam notificadas;
b) Fase de confirmação e autorização: confirmar o incidente e obter autorização e aprovação legal para a realização de um mandado de busca.

2.4.4.3 Fase de Investigação Física da Cena do Crime

O objetivo dessa fase é coletar e analisar as evidências físicas e reconstruir as ações que aconteceram durante o incidente. Inclui seis fases:

a) Fase de preservação: visa preservar a cena do crime, para que as evidências possam ser posteriormente identificadas e coletadas por pessoal treinado na identificação de evidências digitais;
b) Fase de inquérito: que requer um investigador para percorrer a cena física do crime e identificar as evidências físicas;
c) Fase de documentação: visa tirar fotografias, desenhar e fazer vídeos da cena do crime e das evidências físicas. O objetivo é capturar o máximo de informações possíveis para que os detalhes importantes da cena do crime sejam preservados e registrados;
d) Fase de busca e coleta: envolve fazer uma pesquisa em profundidade da cena de modo que alguma evidência física adicional seja identificada e, portanto, abrindo caminho para que a investigação de crimes digitais possa começar;
e) Fase de reconstrução: envolve a organização dos resultados e das análises feitas, de formas a usá-los para desenvolver uma teoria para o incidente;
f) Fase de apresentação: visa apresentar a evidência física e digital para um órgão de Justiça.

2.4.4.4 Fase de Investigação Digital da Cena do Crime

O objetivo é coletar e analisar as evidências digitais que obtidas a partir da fase de investigação física. Ela inclui fases semelhantes à fase de investigação física, embora o foco principal seja sobre as evidências digitais. Inclui as seguintes fases:

- fase de preservação: preservar a cena do crime digital, de modo que as evidências passam ser posteriormente sincronizadas e analisadas;
- fase de inquérito: fase pela qual o pesquisador transfere os dados relevantes a partir de um local fora do controle físico ou administrativo do investigador para um local controlado;
- fase de documentação: envolve documentar adequadamente as evidências digitais quando são encontradas. Esta informação é útil na fase de apresentação;
- fase de busca e coleta: uma análise aprofundada dos elementos de evidência digital é realizada. Ferramentas são usadas para revelar os arquivos escondidos, suprimidos, corrompidos e trocados que foram utilizados, incluindo as datas, duração, timelining[3], arquivo de log, que são realizados para rastrear as atividades e identidade de um usuário;
- fase de reconstrução: inclui colocar as peças de um quebra-cabeça digital juntas, e desenvolver hipóteses de investigação;
- fase de apresentação: envolve a apresentação da evidência digital que foi encontrada pela equipe de investigação física.

[3] Linha do tempo é uma demonstração gráfica de acontecimentos.

2.4.4.5 Fase de Revisão

Isto implica uma revisão de toda a investigação e identificar as áreas de melhoria. O modelo IDIP ilustra bem um processo judicial, e também está de acordo para responder com a capacidade do terrorismo cibernético (NIJ, 2001, tradução nossa), que exigem uma investigação digital para abordar as questões de proteção de dados, aquisição de dados, imagens, extração, interrogatório, análise e relatórios.

Uma vez que um computador pode ser usado como uma ferramenta e como uma vítima (KIZZA, 2003, tradução nossa). Henry Lee, Timothy Palmbach e Marilyn Miller (2001) definem a cena do crime como o principal lugar onde o ato criminoso ocorreu.

2.4.5 Modelo Forense para Dispositivos com Windows Mobile

Há muitos modelos de forense digital propostos em diferentes partes do mundo. No entanto nenhuma conclusão foi alcançada em relação ao mais adequado. Cada framework pode trabalhar bem com um determinado tipo de investigação (RAMABHADRAN, 2007, tradução nossa).

O modelo de processo forense em PDA com Windows Mobile foi desenvolvido e apresentado por Anup Ramabhadran para ajudar os profissionais forenses e autoridades policiais na investigação de crimes que envolvam tais dispositivos. As práticas e técnicas padrões do mundo físico e digital de investigação são incorporadas, sempre que adequado. Esse modelo tenta superar as grandes deficiências dos atuais modelos de forense digital, e enfatiza uma abordagem sistemática e metódica para investigação forense digital (JANSEN; AYERS, 2004). O modelo proposto é composto de doze etapas, que serão explicadas posteriormente (Figura 3).

Figura 3. Fases do modelo Forense em Dispositivos com Windows Mobile.
Fonte: RAMABHADRAN, A (2007).

2.4.5.1 Preparação

A fase de preparação ocorre antes da investigação real. Trata-se de conseguir uma compreensão inicial da natureza do crime e as atividades, bem como preparar as ferramentas necessárias para o padrão de investigações em dispositivos portáteis, organizar uma equipa adequada, atribuindo funções a cada um. É muito importante obter a melhor avaliação possível sobre as circunstâncias relativas ao crime, antes de prosseguir para a cena do crime (NELSON; PHILIPS; ENFINGER, 2005, tradução nossa).

Uma questão crucial nas investigações envolvendo dispositivos com Windows Mobile é que a bateria se esgote antes da coleta de provas. Por isso, é essencial preparar um

kit de ferramentas composto de fontes de alimentação padrão, cabos e bases (RAMABHADRAN, 2007, tradução nossa).

A investigação deve seguir nos trâmites legais e jurisdicionais. Esta fase também envolve a obtenção de mandados de busca, autorizações necessárias, antes de prosseguir para a cena do crime. Os direitos de privacidade dos suspeitos devem ser levados em conta. Advertência jurídica deve ser fornecida para todas as partes envolvidas na investigação forense (BARYAMUREEBA; TUSHABE, 2004, tradução nossa).

Nota-se que uma estratégia adequada para a investigação deve ser desenvolvida, tendo em conta a natureza do incidente, fatores técnicos, jurídicos e comerciais. Formação, educação e a experiência dos investigadores contribuirão nesta fase.

Após uma fase de preparação minuciosa, aumenta a qualidade das provas e minimiza os riscos e ameaças associadas a uma investigação.

2.4.5.2 Segurança do Cenário

Lida principalmente com a segurança da cena do crime contra o acesso não autorizado e preservar as provas da contaminação. Deve haver um protocolo formal para preservar uma cena de crime, a fim de assegurar que a cadeia de custódia é seguida corretamente. Será difícil avaliar o quanto a cena do crime é realmente a prova (RAMABHADRAN, 2007, tradução nossa).

Os pesquisadores devem identificar o âmbito do crime e estabelecer um perímetro. Garantir a segurança de todas as pessoas na cena do crime e proteger a integridade de todas as provas. No entanto, uma tentativa que não deve ser feita é determinar o que está presente no dispositivo nesta fase. Os dispositivos devem ser deixados no seu estado atual até que uma avaliação adequada seja feita (RAMABHADRAN, 2007, tradução nossa).

A máxima prioridade deve ser dada, nesta fase, em minimizar a corrupção de evidências. Esta fase tem um papel importante no processo global de investigação, porque determina a qualidade das provas.

2.4.5.3 Levantamento e Reconhecimento

Esta etapa envolve um levantamento inicial realizado pelos pesquisadores para avaliar o cenário, identificando possíveis fontes de evidência e formular um plano de pesquisa apropriado. Em um ambiente complexo, isso pode não ser simples (RAMABHADRAN, 2007, tradução nossa). Avaliar os equipamentos eletrônicos no local para determinar se alguma assistência especializada é necessária no processamento da cena. Identificação de pessoas na cena e realização preliminar de entrevistas é extremamente importante (BRILL; POLLITT, 2006, tradução nossa).

Os proprietários ou utilizadores dos dispositivos eletrônicos ou os administradores do sistema podem fornecer informações valiosas, como a finalidade do sistema, sistemas de segurança, vários aplicativos presentes nos dispositivos, nomes de usuário, senhas, detalhes de criptografia sem violar as leis de competência e políticas corporativas.

Quando se torna necessária a busca por itens que não estão incluídos no mandado de busca, as devidas alterações devem ser feitas para o mandado já existente ou um novo mandado deve ser obtido, que inclui os itens adicionais. Um plano inicial para coleta e análise de evidências deve ser desenvolvido no final do inquérito e na fase de reconhecimento (RAMABHADRAN, 2007, tradução nossa).

2.4.5.4 Documentação da Cena

Esta etapa envolve a devida documentação da cena do crime, juntamente com a fotografia, desenho e mapeamento da cena do crime. Todos os dispositivos eletrônicos no local devem ser fotografados junto com os adaptadores de energia, cabos, suportes e outros acessórios (RAMABHADRAN, 2007, tradução nossa).

Se o dispositivo está no estado ligado, o que está aparece na tela também deve ser documentado. Um registro de todos os dados visíveis deve ser criado, o que ajuda na recriação da cena. Isto é particularmente importante quando o especialista forense tem que fazer um depoimento em um tribunal, o que poderia ser vários meses após a investigação (RAMABHADRAN, 2007, tradução nossa).

É necessário manter um registro de quem estava presente na cena, quem chegou ou quem deixou a cena, juntamente com o resumo de suas atividades, enquanto estiveram na cena do crime. É necessário classificar as pessoas em grupos separados, como vítimas, suspeitos, espectadores, testemunhas, pessoal auxiliar, e gravar a sua localização no momento da entrada. A documentação é uma atividade contínua, exigida em todas as etapas e é bastante crítica (HORSEWELL, 2004, tradução nossa).

2.4.5.5 Comunicação

Esta etapa ocorre antes da coleta de provas. Todas as outras opções possíveis de comunicação dos dispositivos devem ser bloqueadas. Mesmo se o dispositivo pareça desligado, alguns recursos de comunicação como Bluetooth ou rede sem fio podem ser ativado. Isso pode resultar em substituição da informação existente e, portanto, essas possibilidades devem ser evitadas (RAMABHADRAN, 2007, tradução nossa). A melhor

opção após apreender um dispositivo é isolá-lo, desativando todas as suas capacidades de comunicação. Se o dispositivo estiver conectado, remove-se qualquer cabo USB ou serial, que se conecta a um computador.

2.4.5.6 Coleção de evidências voláteis

A maioria das evidências envolvendo dispositivos PDA é de natureza volátil, estando presente na memória ROM. Coleta de evidências voláteis apresenta um problema como o estado do dispositivo e o conteúdo da memória podem ser alterados (RAMABHADRAN, 2007, tradução nossa).

A decisão de recolher evidências na cena do crime ou mais tarde, em um laboratório forense seguro depende da natureza particular da situação, incluindo o estado atual da bateria. Se o dispositivo ficar sem bateria, toda a informação será perdida em breve (HORSEWELL, 2004, tradução nossa). Se o tempo de duração da energia da bateria for duvidoso, o conteúdo da memória deve ser trabalhado com ferramentas adequadas o mais rapidamente possível.

Uma combinação de ferramentas deve ser utilizada para obter melhores resultados (RAMABHADRAN, 2007, tradução nossa). A presença de qualquer software malicioso instalado pelo usuário também deve ser verificado nesta fase.

2.4.5.7 Coleta de evidências não voláteis

Esta fase envolve a coleta de evidências dos meios de armazenamento externo suportado por estes dispositivos, como os cartões de memória *MultiMedia Card* (MMC), cartões *Compact Flash* (CF), cartões Secure Digital (SD), cartões de memória USB.

Evidências a partir de computadores, que são sincronizados com estes dispositivos, devem ser recolhidas. Se o aparelho tem integrado as funções de telefone, a aquisição de informações de cartão SIM tem lugar nesta fase. A integridade e a autenticidade dos elementos de evidências recolhidos devem ser asseguradas por meio de mecanismos como hashing, e proteção escrita (RAMABHADRAN, 2007, tradução nossa). Todos os cabos de alimentação, adaptadores e outros acessórios também devem ser coletados. Cuidados devem ser tomados para procurar evidências de natureza não eletrônica, como senhas escritas, manuais de hardware e software, documentos relacionados e impressões de computador (CIARDHUÁIN, 2004, tradução nossa).

2.4.5.8 Preservação

Esta fase inclui o transporte, embalagem e armazenamento. Procedimentos apropriados devem ser seguidos e documentados para assegurar que as provas eletrônicas recolhidas não serão alteradas ou destruídas. Todas as potenciais fontes de evidências devem ser identificadas e devidamente rotuladas antes de embalar (RAMABHADRAN, 2007, tradução nossa). Uso de sacolas de plástico comum pode gerar eletricidade estática. Assim a embalagem anti-estática de provas é essencial. O aparelho e os acessórios devem ser colocados em um envelope e lacrados antes de colocá-lo no saco de evidências. O saco plástico deve ser mantido em um recipiente de isolamento de rádio frequência para evitar novas comunicações com qualquer outro dispositivo. Todos os recipientes também devem ser adequadamente rotulados. Posteriormente, o dispositivo pode ser movido para um local seguro, onde a análise e processamento de dados podem ser iniciados.

As evidências devem ser armazenadas em uma área segura e devem ser protegidas das radiações eletromagnéticas, calor, poeira e umidade. Pessoas não autorizadas não podem ter acesso à área de armazenamento (RAMABHADRAN, 2007, tradução nossa).

2.4.5.9 Exame

Esta fase envolve a análise do conteúdo das evidências coletadas pelo especialista forense e extração de informações, que é fundamental para comprovar o caso. Adequado número de backups das evidências devem ser criados antes de proceder ao exame. Nesta etapa visa-se tornar visível a evidência, ao explicar sua originalidade e importância (RAMABHADRAN, 2007, tradução nossa).

A filtragem de dados, validação de correspondência de padrões e busca de palavras-chave específicas no que respeita à natureza do crime ou do suspeito, recuperando códigos ASCII relevantes, bem como dados que não ASCII, são alguns dos principais passos realizados durante esta fase. Dados do organizador de informações pessoais como endereços, compromissos, agenda, mensagens de texto, mensagens de voz, documentos e e-mails são algumas das fontes mais comuns de provas, que devem ser analisadas em detalhe (RAMABHADRAN, 2007, tradução nossa).

Encontrar evidências de violação do sistema, dados ocultos ou excluídos, modificações não autorizadas do sistema também deve realizar-se. Detecção e recuperação de informação escondida é uma importante tarefa. Os dados devem ser pesquisados a fundo para recuperação de senhas, encontrar arquivos incomuns, ocultos, diretórios ou extensão de arquivo e assinatura incompatíveis (HORSEWELL, 2004, tradução nossa).

A capacidade do kit de ferramentas forense utilizado pelo profissional, desempenham um papel importante na fase de exame. É necessário provar que a evidência

não foi alterada depois de ser examinada pelo especialista forense e, portanto, técnicas de hashing como MD5 devem ser usadas para autenticação de dados matemáticos (RAMABHADRAN, 2007, tradução nossa).

2.4.5.10 Análise

Nesta etapa é mais uma análise técnica realizada pela equipe de investigação com base nos resultados do exame das evidências. Identificar as relações entre os fragmentos de dados, análise de dados ocultos, determinar o significado das informações obtidas a partir da fase de exame, reconstruindo os dados do evento, com base nos dados extraídos e chegar a conclusões adequadas, são algumas das atividades a serem realizada nesta fase (RAMABHADRAN, 2007, tradução nossa).

Recomenda-se a análise temporal, análise de dados ocultos, a análise da aplicação e análise de arquivo dos dados extraídos. Resultados da fase de análise podem indicar a necessidade de medidas adicionais nos processos de extração e análise. Deve-se verificar se a cadeia de evidências e o cronograma dos eventos são consistentes. Usando uma combinação de ferramentas para a análise produzirá melhores resultados. Os resultados da análise devem ser corretamente documentados (HORSEWELL, 2004, tradução nossa).

2.4.5.11 Apresentação

Depois de extrair e analisar as evidências recolhidas, os resultados podem ser apresentados. Como resultado desta fase, deve ser possível confirmar ou descartar as acusações relativas a determinado incidente, crime ou suspeito (RAMABHADRAN, 2007, tradução nossa).

Os resultados individuais de cada uma das fases anteriores podem não ser suficientes para chegar a uma conclusão correta sobre o crime. Os resultados do exame e análise devem ser analisados na sua totalidade para obter uma imagem completa. Um relatório contendo um resumo detalhado das várias etapas do processo de investigação e as conclusões deve ser fornecido. Em muitos casos, o especialista forense poderá testemunhar em tribunal como especialista do caso (JOHNSON, 2005, tradução nossa).

Os termos complexos envolvidos em vários estágios do processo de investigação terão de ser explicados, em terminologia para leigo. A experiência e conhecimento do examinador forense, a metodologia adotada, ferramentas e técnicas utilizadas, são susceptíveis de serem contestados perante um júri. Junto com o relatório, materiais de apoio, como cópias de evidências digitais do documento de custódia, as impressões de vários itens de provas, também devem ser apresentados (PROSISE; MANDIA, 2003, tradução nossa).

2.4.5.12 Revisão

A fase final do modelo é a fase de revisão. Isso implica uma revisão de todas as etapas da investigação e identificação de áreas para melhoria. Como parte da fase de revisão, os resultados e sua interpretação posterior podem ser usados para refinação, coleta de exames e análise de evidências em investigações futuras. Em muitos casos, muita iteração das fases de exame e análise é necessária para obter a imagem total de um incidente ou crime. Esta informação também ajuda a estabelecer melhores políticas e procedimentos em vigor no futuro (RAMABHADRAN, 2007, tradução nossa).

2.4.5.13 Vantagens do Modelo Forense para Dispositivos com Windows Mobile

Para Ramabhadran (2007) há inúmeras vantagens para o modelo proposto. Este modelo pode ser usado como um padrão para a investigação forense de qualquer dispositivo com Windows Mobile. Ele separa a investigação preliminar de crimes envolvendo dispositivos com Windows Mobile e os computadores. Além de padronizar a investigação forense de dispositivos com Windows Mobile, permite a criação de políticas e procedimentos adequados quando os crimes que envolvam tais dispositivos ocorrer.

O modelo é aplicável em investigações executivas, resposta a incidentes e atividades afins. As práticas comprovadas no domínio da investigação física são incorporadas. É feita uma tentativa para capturar todo o escopo de uma investigação, em vez de processamento único de provas. As principais tarefas associadas com a investigação, incluindo a preservação, identificação, coleta e análise de evidências estão descritas e adequado fluxo de informações entre as diversas fases é garantida (RAMABHADRAN, 2007, tradução nossa).

Muitos dos métodos utilizados para o processamento judicial de outros sistemas operacionais Windows da Microsoft podem ser aplicados ao Windows Mobile, incluindo a compreensão dos sistemas de arquivos *File Allocation Table* (FAT) e arquivos de *index.dat*. Tal como acontece com um computador desktop ou laptop, aparelhos com Windows Mobile retêm informações importantes sobre as atividades do usuário que podem ser relevantes para a investigação digital, como navegação na Web, arquivos criados pelo usuário e as entradas do registro (CASEY; BANN; DOYLE, 2010, tradução nossa).

Para terminar, ainda que o perito siga rigidamente metodologias internacionais de perícia como as mostradas acima, ele deve sempre levar em consideração as leis e regras que regem o ambiente onde a perícia será executada. Por exemplo, se a perícia for executada

numa empresa, ela deve estar de acordo com as regras internas da empresa, leis municipais, estaduais e federais para que a mesma não seja invalidada (BERNARDO, 2006).

Cada um dos modelos processuais acima apresentados contém pontos chave que devem ser considerados quando se trata de evidências digitais. Porque toda investigação de um incidente é diferente, partindo do pressuposto que cada uma tem seu próprio conjunto de circunstâncias, no entanto uma abordagem processual única e definitiva é difícil de prever. Contudo, a maioria dos modelos toca em iguais áreas-chave, embora salientando aspectos diferentes.

2.4.6 Comparação entre os modelos abordados

A Tabela 1 apresenta uma comparação entre as atividades dos modelos abordados neste documento. Cada modelo, apesar de suas diferenças, tem muito em comum com outros modelos. No entanto, existem muitas atividades como comunicação e coleta de evidências voláteis, que são exclusivas para o modelo forense em dispositivos com Windows Mobile. Cada modelo, apesar de suas diferenças, tem muito em comum com outros modelos.

Tabela 1. Tabela comparativa das metodologias investigativas.

Modelo para dispositivos com Windows Mobile	Modelo de aplicação da Lei do NIJ	Modelo DFRWS	Modelo de Reith, Carr e Gunsch	Modelo IDIP
Preparação			✓	✓
Segurança do cenário		✓		✓
Levantamento e Reconhecimento		✓	✓	✓
Documentação da cena				✓
Comunicação				
Coleta de evidências voláteis				
Coleta de evidências não voláteis	✓	✓	✓	✓
Preservação		✓	✓	✓
Exame	✓	✓	✓	✓

Análise	✓	✓	✓	
Apresentação	✓	✓	✓	✓
Revisão				✓

3 PERSONAL DIGITAL ASSISTANT (PDA)

Por estar extremamente popular, o PDA é propenso a estar envolvido em crimes eletrônicos, devido ao seu tamanho compacto e características integradas.

Estando a pôr em causa esta evolução, é necessário para a análise desses dispositivos a combinação de procedimentos forenses e metodologias já existentes para acompanhar a tecnologia. No entanto, a maioria dos PDA que está no mercado segue um projeto básico similar, mas obviamente é diferente no seu sistema operacional (SO), e os seus componentes de hardware, que por sua vez, infelizmente, não facilitam a aquisição de dados forenses sobre estes dispositivos de mão sem modificar o seu estado real ou atual (AYERS; JANSEN, 2004, tradução nossa).

A família de PDA inclui principalmente dispositivos *Palm*, Symbian, aparelhos com Windows Mobile (*Pocket PC*), Androide e iOS. Entre estes, os dispositivos com Windows Mobile tem ganhando popularidade nos últimos tempos, que são baseados no popular sistema operacional Microsoft Windows e oferece uma aparência familiar. Além de fazer e receber chamadas telefônicas, que permite navegar na Internet, bate-papo, enviar e receber mensagens de texto / multimídia, bem como visualizar e editar arquivos do Word, Excel e PowerPoint (JANSEN; AYERS, 2004, tradução nossa).

Desenvolver a compreensão dos componentes e funcionamento interno desses dispositivos (por exemplo, organização de memória e uso) é um pré-requisito para a análise forense envolvendo esses dispositivos. Por exemplo, a memória do PDA usado para armazenar dados do usuário geralmente é volátil (isto é, a memória RAM) e requer energia contínua para manter o conteúdo, ao contrário dos dados que residem no disco rígido de um

computador pessoal (AYERS; JANSEN, 2004, tradução nossa). A tecnologia dos dispositivos portáteis tem mudado rapidamente, com novos produtos e recursos que estão a ser introduzidos com regularidade. Devido ao ritmo acelerado com que as tecnologias dos dispositivos portáteis têm evoluindo, esta discussão representa um instantâneo da área no momento presente (VOLONINO; ANZALDUA, 2008, tradução nossa).

3.1. PERÍCIA FORENSE EM PDA

A maior parte dos dispositivos PDA segue um modelo básico que oferece recursos semelhantes aos modelos apresentados anteriormente. Embora semelhante em princípio, os diversos tipos de PDA existentes atualmente diferem em áreas como o estilo de interação, o sistema operacional (OS) e os componentes de hardware (AYERS; JANSEN, 2004, tradução nossa).

Este documento teve o foco em dispositivos com Windows Mobile, visto que é um dos modelos mais populares de dispositivo PDA. O restante deste documento fornece uma visão geral de PDA, cartões de memória e ferramentas forense; descreve o cenário usado para analisar o kits de ferramentas, dá o resultado da aplicação do cenário, e resume as conclusões.

3.1.1 Preservação

É o processo de apropriação de propriedade suspeita, sem alterar ou modificar o conteúdo dos dados que residem em dispositivos e mídias removíveis (JANSEN; AYERS, 2004, tradução nossa). É o primeiro passo na recuperação de evidências digitais. Este capítulo começa com uma introdução genérica para a preservação, em seguida, fornece um olhar mais detalhado em dispositivos PDA.

Preservação envolve a busca, reconhecimento, documentação e recolha de provas por via eletrônica. A fim de utilizar as provas com sucesso, seja em um tribunal ou um processo menos formal, no entanto devem ser preservadas. A falta de preservação da prova em seu estado original poderia comprometer toda a investigação, perdendo valiosas informações sobre um incidente de forma permanente (JANSEN; AYERS, 2004, tradução nossa).

Segundo o relatório do departamento de justiça dos EUA, sobre investigação de cena de crime eletrônico (NIJ, 2001, tradução nossa), a questão de preservação das provas de abordada de forma detalhada, oferecendo princípios, políticas e procedimentos a seguir quando se deparam com uma cena de evidências digitais. A seguir, os principais pontos a observar.

a) proteção e avaliação da cena;
b) documentar a cena;
c) coleta de evidências;
d) embalagem, transporte e armazenamento de evidências.

Os capítulos a seguir fornecem informações complementares relacionadas com PDA, seguindo o paradigma de busca, identificação, documentação e coleta.

3.1.2 Busca

Quando a equipe de investigação chega à cena com a devida autorização para examinar o dispositivo de um suspeito, deve-se proceder com cautela e seguindo os passos necessários para assegurar que o aparelho chegue ao laboratório forense, sem depleção dos dados (JANSEN; AYERS, 2004). Procedimentos incorretos durante a apreensão pode causar perda crítica na informação contida no dispositivo.

Por acidente ou ação deliberada, o equipamento eletrônico pode ser encontrado em um estado danificado. Dispositivos ou meios de comunicação com danos externos visíveis não necessariamente impedem que dados sejam extraídos deles (JANSEN; AYERS, 2004).

O equipamento danificado deve ser levado ao laboratório para posterior investigação. Reparação dos componentes danificados em um dispositivo e restaurá-lo para exame e análise pode ser possível. Os componentes de memória também podem ser reparados/examinados no local, ou removidos e examinados por um examinador especialmente treinado.

Assessores jurídicos devem ser contatados para obter assistência, necessária, com as seguintes duas considerações críticas legais (NIJ, 2001):

a) determinar a extensão da autoridade de busca e qual o processo legal adicional podem ser necessários para continuar a busca, se a evidência está localizada que não foi autorizada para a entidade de pesquisa original;
b) identificar possíveis preocupações relacionadas com as políticas locais aplicáveis e as leis e estatutos internacionais, federais ou do Estado.

3.1.3 Identificação

Para continuar eficazmente, o tipo exato do dispositivo deve ser identificado. Alteração do dispositivo pode variar como remover a etiqueta do fabricante. Além disso, o sistema operacional pode ser modificado ou completamente substituído, fazendo com que o dispositivo pareça diferente, bem como se comportar igualmente de forma diferente.

Se o dispositivo digital, tal como PDA estiver no estado “ligado” o tipo de dispositivo pode ser identificado pelo sistema operacional, que é mais consistente na identidade do dispositivo, em vez de um logotipo (JANSEN; AYERS, 2004, tradução nossa).

Embora os sistemas operacionais dominantes sejam *Symbian OS, Windows Mobile*, *Blackberry*, *iOS* e *Android*. O PDA é fabricado para rodar um sistema operacional, podendo executar frequentemente um sistema operacional alternativo. Outros indícios que permitem a identificação de um dispositivo são os seguintes: a interface, fabricante, número de série, do tipo, alimentação.

3.1.4 Documentação

Evidências devem ser rigorosamente contabilizadas e identificadas. O processo de etiquetagem deve documentar o número do processo, uma breve descrição de sua assinatura, a data e hora em que as evidências foram recolhidas (JANSEN; AYERS, 2004, tradução nossa). Além disso, a cena do crime deve ser fotografada, anexando-se um relatório documentando o estado de cada dispositivo digital ou computador pessoal. Isso é útil se questionou sobre o meio ambiente depois (KRUSE II; HEISER, 2002, tradução nossa).

Um registro de todos os dados visíveis deve ser criado. Todos os dispositivos digitais (PDA), que podem eventualmente ter armazenamento de dados devem ser fotografados com todos os cabos, suportes, conectores de alimentação, mídia removível e conexões. Ter uma pessoa responsável para prestar serviço de custódia na cena do crime, juntamente com um responsável pela documentação da evidência, é importante durante a fase de coleta (JANSEN; AYERS, 2004, tradução nossa).

A cadeia de custódia é um processo simples, mas eficaz de documentar todo o percurso da evidência por meio do ciclo de vida do caso. Com cuidado, a manutenção da cadeia de custódia não só protege a integridade das evidências, mas também torna difícil para alguém argumentar que as evidências foram adulteradas (KRUSE II; HEISER, 2002, tradução nossa). A documentação deve responder às seguintes perguntas:

a) quem coletou?

b) como e onde?

c) quem tomou posse?

d) como foi guardada e protegida a evidência?

e) quem tirou de armazenamento e por quê?

A documentação para todas as perguntas acima deve ser mantida e arquivada em um local seguro para referências atuais e futuras.

3.1.5 Coleta

Quando o PDA está em causa, o processo de coleta normalmente envolve informações dinâmicas e voláteis que podem ser perdidas a menos que sejam tomadas precauções na cena do incidente ou crime (ACPO, 2007).

Mantêm os dados do usuário em um estado volátil alimentado por uma bateria. O projeto do dispositivo determina o tipo de fonte de bateria fornecida; baterias podem ser recarregáveis ou substituíveis. Se os dispositivos perderem a bateria por um tempo demasiado longo, a chance de recuperar todos os dados do dispositivo que foi apreendido é improvável. Antes que um técnico possa ensacar e etiquetar um PDA, o estado de energia atual deve ser considerado (ACPO, 2007, tradução nossa).

3.1.6 Aquisição

Processo de obtenção de imagens ou informações de um dispositivo digital, seus equipamentos periféricos e meios de comunicação. A aquisição deve ocorrer em um laboratório forense, uma vez que o dispositivo foi apreendido com

segurança. A desvantagem de realizar a aquisição no local é que pode haver perda de informações devido ao esgotamento da bateria e outros danos que se tem de evitar (JANSEN; AYERS, 2004, tradução nossa).

No entanto, encontrar um ambiente controlado para efetuar este tipo de trabalho, ter o equipamento adequado, e satisfazer outros pré-requisitos, e a melhor maneira no que se refere a boas práticas de aquisição forense. Tudo isso se encontra disponível dentro de um ambiente de laboratório, equipado para tal (JANSEN; AYERS, 2004, tradução nossa).

O examinador forense é aconselhado a fazer experiências com vários *toolkits*[4] em dispositivos de teste para descobrir quais ferramentas para aquisição trabalharam com maior eficiência com um tipo específico de dispositivo, e para determinar o grau de interoperabilidade entre diferentes ferramentas de aquisição e de exame para determinados tipos de dispositivos (JANSEN; AYERS, 2004, tradução nossa).

Não importa o modelo do dispositivo, para aquisição de dados a partir dele, uma conexão deve ser estabelecida a partir da estação de trabalho do especialista forense para o dispositivo. Antes de efetuar uma aquisição, a versão da ferramenta a ser utilizada deve ser documentada, juntamente com as correções aplicáveis ou errata do fabricante aplicada à ferramenta. Quando a ligação tiver sido estabelecida, o conjunto de software forense poderá adquirir os dados do dispositivo corretamente (JANSEN; AYERS, 2004, tradução nossa).

Ao contrário das máquinas desktop ou servidores de rede, o PDA nos dias de hoje não tem disco rígido e refugia-se em memória de semicondutor. Existem softwares especializados para produzir uma imagem do dispositivo, bem como executar uma lógica de aquisição de dados do *Personal Information Management*[5] (PIM). No entanto, o conteúdo de um PDA é dinâmico e em constante mudança, mesmo quando desligado (ou seja, no estado de repouso) (ACPO, 2007, tradução nossa).

---

[4] Kits de Ferramentas
[5] Gerenciamento de informações pessoais

Duas aquisições de um dispositivo usando a mesma ferramenta produzem resultados diferentes em geral, embora a maioria das informações, como dados de PIM, permanecem inalteradas. Para se fazer imagem da memória de um dispositivo PDA, o dispositivo tem de estar ligado, que é uma grande diferença quando comparado com aquisições em computadores pessoais. Isso efetivamente significa que o princípio referido anteriormente – de que medidas tomadas não devem modificar os dados contidos no dispositivo - não pode ser cumprido, estritamente falando (JANSEN; AYERS, 2004, tradução nossa).

Portanto, o objetivo com a aquisição do PDA é afetar o conteúdo da memória o menos possível e apenas no conhecimento do que está acontecendo internamente, dando mais importância em garantir a adesão aos princípios que enfatizam a competência do especialista e a geração de uma trilha de auditoria detalhada (ACPO, 2007, tradução nossa).

Após a conclusão da aquisição, o especialista forense deve sempre confirmar que o conteúdo inteiro do dispositivo foi capturado corretamente (ou seja, verificar RAM / ROM assegurar a coerência com o tamanho do dispositivo). Na ocasião, uma ferramenta pode falhar a sua missão sem nenhuma notificação de erro e exigir ao especialista para que refaça a aquisição com a mesma ferramenta ou usando outra. Da mesma forma, algumas ferramentas não funcionam bem com determinados dispositivos como em outros, e podem falhar com uma notificação de erro. Assim, sempre que possível, é aconselhável ter várias ferramentas disponíveis.

3.1.6.1 Dispositivos Desobstruídos

Um dispositivo sem obstrução é um dispositivo que não requer uma senha ou outra técnica de autenticação a ser satisfeita para ter acesso ao dispositivo. A partir de

informações pontuais, a maioria dos aparelhos apreendidos nas investigações parece cair nesta categoria. Como mencionado anteriormente, ao apreender um "dispositivo desobstruído" deve-se ter cuidado para evitar, por exemplo, alteração no estado do dispositivo pressionando as principais sequencias de teclas chaves, que têm a potencial função de danificar ou apagar dados valiosos (JANSEN; AYERS, 2004, tradução nossa).

Em geral, um PDA tem quatro categorias principais de armazenamento a considerar: o código do sistema operacional, incluindo o *kernel*[6], *drivers*[7] de dispositivos e bibliotecas do sistema; memória alocada dinamicamente para a execução de aplicativos do sistema operacional e armazenar e executar aplicações adicionais do usuário carregados para o dispositivo, armazenamento do usuário para vários tipos de arquivos de dados, incluindo texto, imagens e sons, e backup de dados críticos e informações do *PIM* importantes de aplicativo e arquivos de dados (JANSEN; AYERS, 2004, tradução nossa).

As características destas quatro categorias variam de estabilidades altas a temperaturas extremamente voláteis. Estas diferenças combinadas com as características de um sistema operacional específico determinam como a *ROM* e *RAM* são usadas para apoiar cada uma das categorias de armazenamento (JANSEN; AYERS, 2004, tradução nossa).

A Figura 4 ilustra o arranjo mais típico. A *Flash ROM* é usada principalmente para armazenar o código do sistema operacional e, opcionalmente, algum dado do *PIM*, ou backup de arquivos do usuário no espaço restante. A memória flash tem uma vida útil de aproximadamente 100.000 ciclos do processo de escrita, antes de ficar inutilizada. A memória *RAM* é usada para armazenamento dinâmico e armazenamento de arquivos do usuário (JANSEN; AYERS, 2004, tradução nossa).

[6] Componente central do sistema operativo
[7] Driver de dispositivo é aceitar requerimentos abstratos do software independente do dispositivo acima dele e cuidar para que a solicitação seja executada, permitindo que o software interaja com o dispositivo.

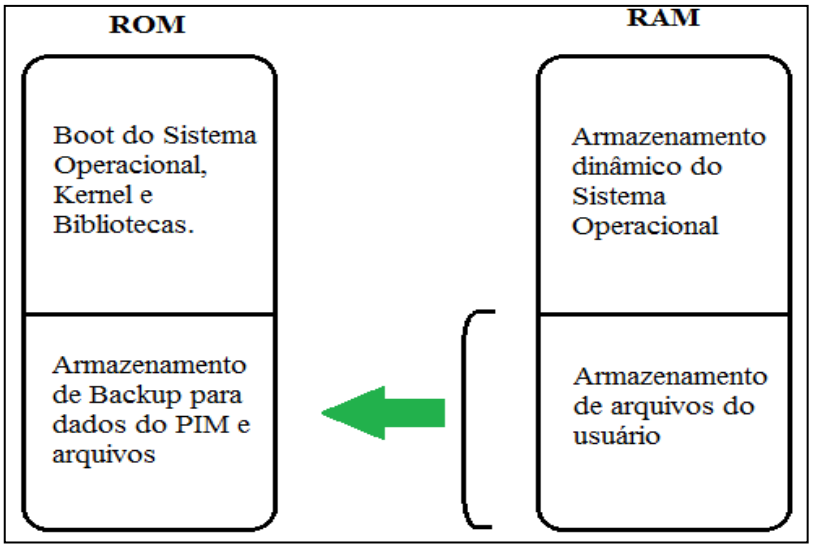


Figura 4. RAM/ROM - Atribuições de armazenamento
Fonte: JANSEN, W.; AYERS, R. (2004)

Um comum arranjo de memória alternativo é mostrado na Figura 5. Onde o armazenamento de arquivos do usuário reside na Flash ROM com o código do sistema operacional, o que evita a necessidade de utilitários de backup, uma vez que o armazenamento é persistente e não é afetado pela redefinição do sistema ou a drenagem da carga da bateria. Os tamanhos da ROM e RAM são normalmente diferentes (mais ROM, e menos RAM) quando comparado com o arranjo anterior para fornecer capacidade proporcional. Para manter o armazenamento de arquivos do usuário na ROM versus RAM, um sistema de arquivos especializado é necessário para evitar atingir de forma rápida a vida útil da mídia (JANSEN; AYERS, 2004).

Os sistemas de arquivos, tais como *Journaling Flash File System* (JFFS2), versão 2 são projetados especificamente para gerenciar o uso de memória flash com cuidado (WOODHOUSE, 2001). Por exemplo, os arquivos JFFS2 previnem a reescrita de todo um sector para apagar um único byte e garantem que as áreas diferentes de memória sejam usadas em rotação de formas a gerir o desgaste.

Porque um número limitado de ferramentas forenses existentes para aquisição de conteúdo da ROM e RAM a partir de um PDA, a escolha geralmente é simples. Uma consideração principal é manter a compatibilidade com o kit de ferramentas usado

eventualmente no exame e análise, uma vez que a interoperabilidade entre diferentes ferramentas de PDA, formatos de arquivo, especialmente em casos comerciais, não é garantida.

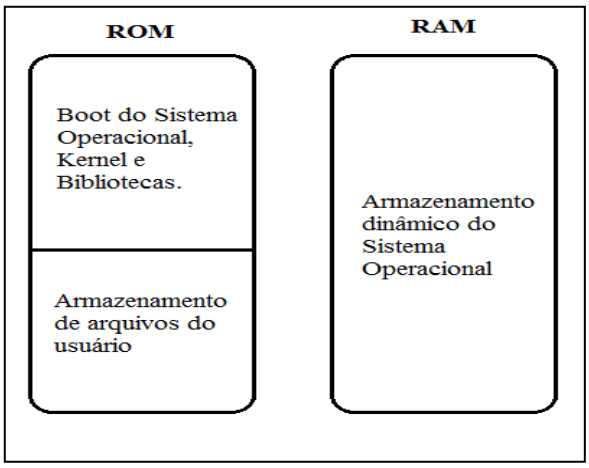


Figura 5. Atribuições RAM/ROM alternativas
Fonte: JANSEN, W.; AYERS, R. (2004)

A fim de preservar a integridade dos dados, os examinadores devem lidar com as provas originais o mínimo possível. Geralmente, recomenda-se criar uma "cópia máster" cópia legal do dispositivo, que é mantida completamente pura. A cópia máster é então utilizada para criar imagens adicionais em espelho, necessários para a análise e o exame das provas (GAST, 2003, tradução nossa). Uma forte maneira seria usar um código *hash* criptografado (por exemplo, *SHA1*[8]) para garantir que as imagens adicionais criadas a partir da cópia máster sejam idênticas.

3.1.6.2 Dispositivos Obstruídos

Dispositivos obstruídos geralmente referem-se a dispositivos que estão desligados (ou seja, no estado de repouso) e exigem a autenticação com sucesso usando uma senha ou qualquer outro meio para obter acesso. Dispositivos protegidos por senha normalmente exigem a perícia de um especialista forense, especialmente treinado para ter acesso ao

[8] Secure Hash Algorithm

conteúdo do dispositivo, mantendo a integridade das informações e evitar danos ao dispositivo (JANSEN; AYERS, 2004, tradução nossa). Uma série de maneiras existe para extrair dados de dispositivos obstruídos. Dividindo-se em três categorias: método investigativo, os métodos baseados em software e hardware.

Métodos baseados em *software* e *hardware* muitas vezes são desenvolvidos especificamente para um determinado dispositivo ou uma classe restrita de dispositivos. No desenvolvimento de um método, as seguintes ações devem ser consideradas para determinar possíveis abordagens (JANSEN; AYERS, 2004, tradução nossa):

a) Contatar o fabricante do dispositivo para obter informações sobre *backdoors* (é uma falha de segurança que pode existir em um programa de computador ou sistema operacional, que pode permitir a invasão do sistema, para que se possa obter um total controle da máquina) e vulnerabilidades conhecidas que podem ser exploradas;
b) Revisar as especificações do fabricante e outros documentos ao se formular uma exploração plausível;
c) Contatar profissionais comerciais de recuperação de evidências que se especializaram em dispositivos portáteis;
d) Pesquisar sites da internet para desenvolvedores, hackers e segurança da informação;
e) Contatar empresas de manutenção e reparação do dispositivo, bem como as organizações comerciais, que fornecem informações sobre a arquitetura de dispositivo portátil[9].

[9] Para mais informações sobre a arquitetura de dispositivos portáteis consulte: http://www.portelligent.com.

3.1.6.3 Equipamentos Tangenciais

Equipamentos tangenciais incluem os dispositivos que contêm memória e estão associados com um PDA. As duas categorias principais são cartões de memória e computadores onde um PDA tenha sincronizado seu conteúdo. Surpreendentemente, os drives de memória USB, que são comuns de periféricos para computadores, geralmente não são um fator para PDA, devido a problemas de interface (JANSEN; AYERS, 2004, tradução nossa).

PDA, especialmente modelos de gama mais elevada, tipicamente suportam Compact Flash (CF), Secure Digital (SD), Multi-Media Card (MMC), e outros tipos de mídias removíveis projetadas especificamente para dispositivos portáteis, que podem conter uma quantidade significativa de dados. Como a memória RAM e ROM, cartões de memória são normalmente memórias de semicondutor.

Os dados contidos em um PDA estão frequentemente presentes em um computador pessoal, devido à capacidade de um PDA para sincronizar ou compartilhar informações entre um ou mais computadores. Tais computadores pessoais ou estações de trabalho são referidos como dispositivos sincronizados. Por causa da sincronização, uma quantidade significativa de evidências valiosas em um PDA, se não todas, podem também estar presentes no *Laptop* do suspeito ou computador pessoal, e podem ser recuperadas usando uma ferramenta convencional forense para a aquisição e exame de disco rígido (JANSEN; AYERS, 2004, tradução nossa).

3.1.6.3.1 Cartões de Memória

Uma grande variedade de cartões de memória existente no mercado hoje, que vão desde o tamanho de um selo a uma caixa de fósforos. Mídia de armazenamento removível

com capacidade varia de 8MB para mais de 32GB. Com os avanços tecnológicos, esses meios de comunicação tornaram-se menor e oferecem maior densidade de armazenamento. A mídia removível estende a capacidade de armazenamento do PDA, permitindo que os indivíduos possam armazenar arquivos adicionais para além da capacidade do dispositivo. Os cartões de memória permitem o compartilhamento de dados entre vários usuários que possuem hardware compatível (JANSEN; AYERS, 2004, tradução nossa).

Ao contrário da Memória RAM dentro de um dispositivo, a mídia removível é um armazenamento não volátil e não requer nenhuma bateria para manter os dados. Felizmente, esses meios de comunicação podem ser tratados de forma semelhante a uma unidade de disco removível, fotografados e analisados usando ferramentas forense convencionais, com a utilização de um leitor de mídia externa (JANSEN; AYERS, 2004, tradução nossa).

Adaptadores de cartão de memória existentes suportam um ambiente integrado de desenvolvimento (IDE). Esses adaptadores permitem uma mídia removível para serem tratados como um disco rígido e utilizados com software de bloqueio de escrita, o que garante que a mídia removível permaneça inalterada. Os dados contidos na mídia podem ser trabalhados, pesquisados, e os arquivos apagados podem ser recuperados oferecendo possibilidades de descobrir evidências (JANSEN; AYERS, 2004, tradução nossa). A seguir está um breve resumo dos vários meios de armazenamento comum em uso hoje, que podem conter informações importantes relacionadas com uma investigação segundo Jansen e Ayers (2004).

a) **cartões *compact flash* (CF):** é um cartão de disco de estado sólido com um conector de 50 pinos, que consiste em duas fileiras paralelas de 25 pinos em uma extremidade do cartão. Normalmente são projetados para funcionalidade e compatibilidade PCMCIA - ATA, tem um barramento de 16 bits de dados e é usado mais como um disco rígido do que uma RAM. Eles usam a tecnologia de

memória flash, uma solução de armazenamento não volátil que retém as informações quando a energia é removida do cartão (JANSEN; AYERS, 2004, tradução nossa).

b) **microdrives**: A mídia Microdrive digital é de alta capacidade, do tipo Compact Flash II, com um barramento de dados de 16 bits. Semelhante em função do estado sólido aos cartões de memória Flash, o cartão de memória de 4GB Microdrive é pré-formatado com um sistema de arquivos FAT32. Ao passar para FAT32, mais espaço de armazenamento pode ser acessado, mas as câmeras e outros dispositivos devem suportar o novo sistema de arquivos. Muitas câmeras digitais e a maioria dos PDA suportam FAT32 (JANSEN; AYERS, 2004, tradução nossa).

c) ***multimedia card* (MMC)**: é um cartão de disco de estado sólido com um conector de 7 pinos. Cartões MMC têm um bit de barramento de dados. Tal como acontece com os cartões CF, eles são fabricados com tecnologia flash, uma solução de armazenamento não-volátil que retém as informações quando a energia é removida do cartão. As placas não contêm partes móveis e uma maior proteção de dados do que discos rígidos magnéticos convencionais (JANSEN; AYERS, 2004, tradução nossa).

d) **secure digital (SD):** *cartões Secure Digital* (SD) (comprimento 32 mm, largura 24 mm, e a espessura de 2,1 milímetros) são comparáveis à concepção de estado sólido e tamanho dos cartões MMC. Na verdade, slots para cartões SD podem frequentemente acomodar também cartões MMC (JANSEN; AYERS, 2004, tradução nossa). No entanto, os cartões SD têm um conector de 9 pinos e 4 bits de barramento de dados, que proporcionam uma maior taxa de transferência. Possuem um dispositivo de prevenção de apagamento. Mantendo

a chave na posição fechada protege os dados contra exclusão acidental. (JANSEN; AYERS, 2004, tradução nossa).

e) **memory Sticks**: estes cartões de memória fornecem memória de estado sólido com um tamanho similar (comprimento 50 mm, largura de 21,45 milímetros, 2,8 milímetros de espessura). Eles têm um conector de 10 pinos e de 1-bit de barramento de dados. Tal como acontece com os cartões SD, Memory Sticks também têm incorporados um dispositivo de prevenção de apagamento, para proteger o conteúdo do cartão (JANSEN; AYERS, 2004, tradução nossa).

3.1.6.4 Exame e Análise

O processo de exame dá luz aos dados probatórios. Os resultados, adquiridos por meio da aplicação de métodos estabelecidos com base científica, devem descrever o conteúdo e estado dos dados completamente. Esta documentação permite descobrir o que está contido, incluindo informações que possam ter sido escondidas ou obscuras. Uma vez que todas as informações estão expostas, a redução de dados pode começar, separando informação relevante de informação irrelevante (JANSEN; AYERS, 2004, tradução nossa).

O processo de análise difere da análise na medida em que se olha para o produto da análise, seu significado e valor probatório do caso (ACPO, 2007, tradução nossa). Exame é um processo técnico que é a parte do especialista forense. Entretanto, a análise pode ser feita por outros, tais como o analista forense, o investigador ou o examinador forense. Um único indivíduo pode executar todas as funções envolvidas.

O processo de análise começa depois que uma estação de trabalho forense foi criada com as ferramentas adequadas e uma cópia das evidências adquiridas a partir do dispositivo (JANSEN; AYERS, 2004, tradução nossa). Se tudo estiver disponível, o

examinador deve estudar o caso e se familiarizar com os parâmetros do crime, as partes envolvidas, e as possíveis evidências que foram encontradas. Na realização do exame, o analista forense ou investigador orienta a construção do caso que será aconselhável para o examinador. O investigador ou analista fornece introspecção sobre o que procurar, enquanto o examinador forense fornece os meios para encontrar informações relevantes que possam estar no sistema (WOLFE, 2003, tradução nossa).

Dependendo do tipo de caso, a estratégia varia. Um caso sobre pornografia infantil pode começar com a navegação de todas as imagens gráficas no sistema, enquanto um caso sobre uma infração relacionado com a Internet pode começar a visitar os arquivos de histórico da Internet (WOLFE, 2003, tradução nossa).

O exame revela frequentemente não apenas potencialmente dados incriminadores, mas também informações úteis, tais como senhas, nomes de usuário de rede e atividade de Internet. Além de evidências diretamente relacionadas a um incidente, podem ser descobertas informação sobre a vida de um suspeito, os seus associados, e os tipos de atividades nas quais eles estão envolvidos.

3.1.6.4.1 Localizando a Evidência

O PDA normalmente oferece informações similares que tratam de recursos e capacidades, incluindo *Personal Information Management* (PIM), suporte para e-mail e navegação na web. Dispositivos híbridos que incorporam funcionalidades de PDA para telefone celular também existem. Potencias evidências sobre esses dispositivos inclui (NIJ, 2001, tradução nossa): catálogo de endereços, calendário de apontamentos, documentos, e-mail, senha, agenda, as mensagens de texto e mensagens de voz.

Geralmente, existem dois tipos de investigação forense computacional. A primeira é quando algum incidente ocorreu, mas a identidade do autor do crime é desconhecida (por exemplo, ataques de códigos maliciosos, incidente com hackers). A segunda é quando o autor do crime e o incidente são conhecidos (por exemplo, investigação de pornografia infantil) (JANSEN; AYERS, 2004, tradução nossa).

Com o conhecimento das circunstâncias do incidente, o examinador forense e o analista podem prosseguir em direção a realização dos seguintes objetivos:

a) reunir informações sobre o(s) indivíduo envolvido (quem);

b) determinar a natureza exata dos eventos que ocorreram (o que);

c) construir um cronograma de eventos (quando);

d) descobrir as ferramentas que foram utilizadas ou feitos (como);

e) descobrir informações que explicam a motivação para o crime (por que).

A Tabela 2 mostra uma referência cruzada de fontes genérica de evidências encontrado em PDA e provavelmente a sua contribuição para a satisfação dos objetivos acima referidos. A maioria das informações é proveniente da fonte de dados do PIM, Internet e informações relacionadas. Arquivos do usuário colocados no dispositivo para renderização, visualização ou edição também são outra fonte importante de evidência. Além de arquivos gráficos, o conteúdo de arquivos pertinentes inclui planilhas, slides, apresentação e artigos similares. Para dispositivos híbridos, tais como PDA ou GPS, fontes de evidências adicionais existem, por exemplo, o último número discado ou coordena de algum destino.

Tabela 2. Referência cruzada das origens e objetivos

	Quem	O que	Onde	Quando	Por que	Como
Info. do proprietário	**x**					
Contactos	**x**				**x**	**x**
Calendário	**x**	**x**	**x**	**x**	**x**	**x**
Lista de afazeres	**x**	**x**	**x**	**x**		**x**
Email de Contato	**x**	**x**	**x**	**x**	**x**	**x**
URLs e conteúdo Web		**x**	**x**	**x**		**x**
Arquivos gráficos	**x**	**x**				
Outro conteúdo arquivado		**x**	**x**	**x**	**x**	**x**

Fonte: JANSEN, W.; AYERS, R. (2004)

3.1.6.4.2 Aplicação de Ferramentas

Depois que a imagem adquirida for copiada, o próximo passo é começar a pesquisar os dados, a criação de bookmarks, e desenvolver o conteúdo de um relatório final. Ferramentas de análise forense são elementos fundamentais nesse processo, que traduzem os dados a partir de imagens de bits brutos para um formato e estrutura que é compreensível pelo examinador e pode ser efetivamente usado para identificar e recuperar evidências (JANSEN; AYERS, 2004, tradução nossa).

É importante notar que as ferramentas têm a possibilidade de conter algum grau de erro. Por exemplo, a implementação da ferramenta pode ter um erro de programação, a especificação de uma estrutura de arquivo utilizada pela ferramenta para traduzir bits em dados compreensíveis pelo examinador pode estar imprecisa ou fora da data, ou a estrutura do arquivo gerado por outro programa pode ter entradas incorretas, fazendo com que a ferramenta funcione inadequadamente (CARRIER, 2002, tradução nossa).

O exame forense de evidência digital, um guia para a aplicação da legislação, produzido pelo Departamento de Justiça dos EUA, oferece as seguintes sugestões para a análise dos dados extraídos (NIJ, 2001, tradução nossa):

a) **período de análise**: determinar quando os eventos ocorreram no sistema para uso associado a um indivíduo, analisando os logs selos presentes e a data / hora no sistema de arquivos, como o tempo da última modificação;

b) **análise dos dados de cobertura**: detecção e recuperação de dados ocultos que possam indicar o conhecimento, a propriedade, ou a intenção, correlacionando os cabeçalhos de arquivo de extensões de arquivo para mostrar ofuscação intencional. Acesso a arquivos protegidos por senha, criptografados e compactados, acesso à informação esteganografada detectada em imagens, e ter acesso a áreas reservadas do armazenamento de dados fora do sistema de arquivos normal.

c) **aplicação e análise de arquivos**: identificar informações relevantes para a investigação por meio da análise de conteúdo do arquivo, correlacionando os arquivos para aplicações instaladas, identificar as relações entre os arquivos, determinar o significado dos tipos de arquivo desconhecido, analisar o sistema, definições de configuração e analisar os metadados do arquivo.

d) **propriedade e posse**: identificar os usuários criados, modificados ou quem acessou um arquivo, a propriedade e posse dos dados questionados, colocando o assunto com o dispositivo em uma determinada hora e data, localizar de arquivos de interesse em locais que não são padrão, recuperar senhas que indicam a posse ou propriedade, e identificar o conteúdo de arquivos que são específicos para um usuário.

A capacidade das ferramentas, a riqueza de recursos, o sistema e o tipo de dispositivo em exame determina quais informações podem ser encontradas, recuperadas, relatadas e o esforço necessário. Áreas de variabilidade incluem a busca e recuperação de informação apagada, informações sobre os dispositivos que sofreram um reset, ou

informações dentro de arquivos compactados ou arquivos com extensões desconhecidas (AYERS; JANSEN, 2004).

O motor de busca tem um papel significativo na descoberta de informações utilizadas para a criação de fichas e relatórios finais. Dados de busca de resultados positivos em evidências incriminatórias exigem paciência e pode ser demorado (JANSEN; AYERS, 2004).

Algumas ferramentas têm um motor de busca simples, que corresponde a uma sequência de texto de entrada exata, permitindo apenas para pesquisas fundamentais a serem realizadas. Outras ferramentas mais inteligentes em recursos de motores de busca, permitindo *Grep* (padrões generalizados de expressões de busca), tipo de procura, filtragem de arquivos por diretório, extensão e scripts em lotes que procuram por tipos específicos de conteúdo (ou seja, endereços de email, url). Quanto maior a capacidade da ferramenta, mais experiente e com maior conhecimento da ferramenta se torna o examinador forense (JANSEN; AYERS, 2004, tradução nossa).

Os seguintes critérios têm sido sugeridos como um conjunto de requisitos fundamentais para ferramentas forenses, e devem ser considerados a quando da escolha de ferramentas disponíveis (CARRIER, 2002, tradução nossa):

a) **usabilidade**: capacidade de apresentar dados de forma que sejam úteis a um pesquisador.
b) **integridade**: a aptidão de apresentar todos os dados a um investigador para que ambos os elementos de acusação e defesa possam ser identificados.
c) **precisão**: a qualidade gerada pela saída de dados da ferramenta e a margem de erro verificada.
d) **determinação**: a habilidade da ferramenta de produzir o mesmo resultado quando recebe o mesmo conjunto de instruções e dados de entrada.

e) **verificabilidade**: a garantia de precisão dos resultados por ter acesso a tradução intermediária e apresentação dos resultados.

3.1.6.5 Relatório

É o processo de elaboração de um resumo detalhado de todos os passos dados e as conclusões alcançadas na investigação de um caso. No relatório, todos os participantes devem de forma cuidadosa manter um registro de suas ações e observações, relatando os resultados dos testes e explicar as inferências extraídas da evidência. A base de um bom relatório é a sólida documentação, notas, desenhos, fotografias e relatórios gerados pelas ferramentas utilizadas (JOHNSON, 2005, tradução nossa).

O relato dos resultados de um exame forense tende a seguir modelos pré-definidos, personalizados conforme exigido pelas circunstâncias específicas de cada investigação. Devem incluir todas as informações necessárias para identificar o caso e sua fonte, o contorno do ensaio, os resultados e descobertas, e conter a assinatura da pessoa responsável pelo seu conteúdo. De forma geral, o relatório pode incluir as seguintes informações (NIJ, 2004, tradução nossa):

a) identificação da agência que reportou;
b) identificador do caso ou número de apresentação;
c) investigador do caso;
d) identidade do remetente;
e) data de recepção;
f) data do relatório;
g) lista descritiva de itens apresentados para exame, incluindo o número de série, marca e modelo;

h) identidade e assinatura do examinador;

i) os equipamentos e as condições utilizadas na análise;

j) breve descrição das medidas tomadas durante o exame;

k) materiais de apoio tais como impressões de itens de evidências, cópias digitais das evidências e a cadeia de custódia da documentação;

l) detalhes dos resultados;

m) conclusões do relatório.

Algumas ferramentas forenses têm instalações de software de relatórios embutidas. Os examinadores devem incluir apenas os resultados relevantes no relatório para minimizar o tamanho e evitar confusão para quem vai revisá-lo. Relatórios automatizados normalmente contêm os seguintes componentes principais: número do processo, data, nome do examinador, nome do suspeito e arquivos adquiridos (mostra código *hash*, dados ASCII, representação gráfica de dados).

3.2 WINDOWS MOBILE

O Windows CE (atualmente, chamado de Windows Mobile) está no mercado há mais de 10 anos. No terceiro trimestre de 2009, a Microsoft atingiu uma quota de mercado de 8,8% dos mais de 41 milhões PDA vendidos no mundo. Isto torna a perícia forense em PDA um tema relevante para a comunidade forense. A maioria das ferramentas forenses disponíveis comercialmente com suporte para Windows Mobile proporciona a aquisição lógica, gerando dados ativo. As possibilidades de aquisição física têm aumentado, como alguns fabricantes de ferramentas começaram a implementar formas de aquisição física (KLAVER, 2010, tradução nossa).

O PDA com Windows Mobile tornou-se mais amplamente usado e pode ser uma valiosa fonte de evidências em uma grande variedade de investigações. Embora o analista forense possa aplicar seu conhecimento em outros sistemas operacionais, para PDA com Windows Mobile da Microsoft, há diferenças suficientes que exigem conhecimento especializado e ferramentas, para localizar e interpretar evidências digitais nestes sistemas. (CASEY; BANN; DOYLE, 2010, tradução nossa).

Estes dispositivos representam uma oportunidade e um desafio importante para os profissionais forenses, porque são essencialmente "computadores" que as pessoas carregam, que contêm quantidades substanciais de informação que podem ser úteis do ponto de vista forense, incluindo as comunicações, multimídia e informações de localização.

Conforme Klaver (2010) a natureza pessoal da informação sobre estes dispositivos pode fornecer aos investigadores informações valiosas sobre o *modus operandi* do suspeito e das atividades da vítima. Além disso, os pesquisadores em contextos penal, empresariais e militares devem ser capazes de detectar a presença de programas que permitem o monitoramento remoto de dispositivos com Windows Mobile.

Novos métodos de aquisição tornaram-se disponíveis, dando aos investigadores acesso a mais informações sobre estes dispositivos, incluindo os dados apagados. Ao mesmo tempo, os formatos de dados em PDA com Windows Mobile é desconhecido para a maioria dos profissionais forense, como arquivos de bancos de dados de volume incorporado (JANSEN; AYERS, 2004, tradução nossa).

Ferramentas para a interpretação e análise de dados em PDA com Windows Mobile têm lutado para manter o ritmo com os avanços na tecnologia. Analistas forense precisam entender as tecnologias e formatos que existem, antes de usar uma variedade de ferramentas para extrair informações úteis (CASEY; BANN; DOYLE, 2010, tradução nossa).

3.2.1 Arquitetura de PDA com Windows Mobile

A plataforma Windows de dispositivos móveis baseados na arquitetura Windows CE é composta por quatro camadas principais (Figura 6), descritas a seguir (CASEY; BANN; DOYLE, 2010, tradução nossa):

a) **camada de hardware:** está composta por microprocessadores, memória RAM, ROM, processadores de sinal digital, várias entradas / saídas;

b) **camada do fabricante original do equipamento (*Original Equipment Manufacturer* OEM):** inclui o carregador de inicialização, arquivos de configuração, drivers e a camada de adaptação (OAL). A OAL permite à OEM adaptar-se a uma plataforma específica e consiste em funções relacionadas com o sistema startup, gerenciamento de interrupção, perfis, gerenciamento de energia, temporizador e relógio;

c) **camada do sistema operacional:** esta camada inclui o *kernel*, o núcleo DLL, o dispositivo de armazenamento, tecnologias multimídia, gerenciador de dispositivos, serviços de comunicação, redes, janela gráfica e subsistema de eventos (GWES). O GWES fornece uma interface entre o aplicativo, o usuário e o sistema operacional. O dispositivo de armazenamento inclui três tipos de armazenamentos persistentes, que são os arquivos do sistema, registros e as propriedades do banco de dados. O registro armazena informações sobre a configuração do sistema, aplicações e configurações de preferências do usuário. Propriedade do banco de dados é um armazenamento de dados que pode ser pesquisado e recuperado por aplicações associadas;

d) **camada de aplicação:** consiste em aplicações como o *office mobile*, *outlook mobile*, o *windows media player*, *internet explorer pocket*, *MSN Pocket*,

visualizador de imagem e vídeo, a interface do usuário e vários aplicativos personalizados.

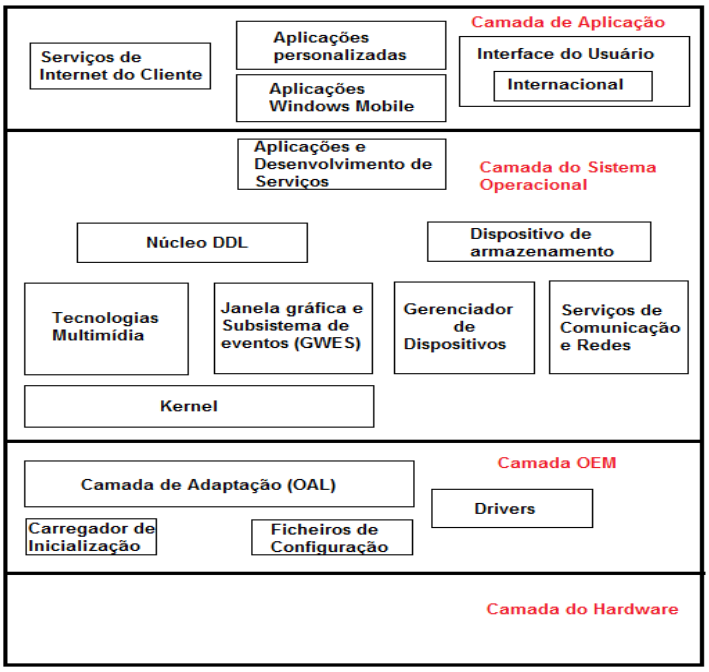


Figura 6. Arquitetura simplificada de um dispositivo com Windows Mobile.
Fonte: JANSEN, W.; AYERS, R. (2004)

Os diferentes tipos de memória suportados pelo sistema operacional são:

a) **memória RAM:** é constituída por duas áreas, dispositivo de armazenamento no qual os dados são armazenados e memória de programa onde os programas são executados. O dispositivo de armazenamento é semelhante a um disco virtual de RAM e os dados contidos serão mantidos mesmo quando o sistema estiver desligado (CASEY; BANN; DOYLE, 2010, tradução nossa).

b) **RAM de expansão:** é suportada para proporcionar armazenamento adicional para os usuários (CASEY; BANN; DOYLE, 2010, tradução nossa).

c) **ROM:** consiste no sistema operacional, aplicativos, arquivos de dados, suporte para arquivos executáveis comprimidos e arquivos DLL. Programas não comprimido são executados nesta memória. Quando um programa é executado diretamente na ROM, o tempo necessário para iniciar um aplicativo é menor,

pois não tem necessidade de ser carregado na memória RAM (CASEY; BANN; DOYLE, 2010, tradução nossa).

d) **armazenamento persistente:** as opções de armazenamento persistente estão principalmente na forma de cartões de memória removíveis como Compact Flash (CF), Secure Digital (SD) e Multimídia Card (MMC). Os dados armazenados em cartões de armazenamento removíveis são mapeados para a memória RAM quando necessário (CASEY; BANN; DOYLE, 2010, tradução nossa).

3.2.2 Características do Hardware

Sendo concebido para locomoção, PDA com Windows Mobile é de tamanho muito compacto, alimentado por bateria e peso leve. Existem muitos fabricantes de hardware fabricando dispositivos utilizando a plataforma do Windows Mobile. Todos eles têm um conjunto básico de características comparáveis e capacidades. Características físicas como tamanho, forma, peso e especificações técnicas, como velocidade do processador, capacidade de memória e capacidade de expansão, podendo variar para cada modelo (CASEY; BANN; DOYLE, 2010, tradução nossa).

A plataforma do Windows Mobile permite a flexibilidade do fabricante de hardware, integradores de sistemas ou desenvolvedor de incorporar a sua escolha de serviços em sua versão do dispositivo. Um dispositivo com Windows Mobile em geral é constituído por RAM, ROM, microprocessador, toque em tela de cristal líquido, módulos de comunicação GSM / GPRS, WLAN, Bluetooth e IrDA, slots para cartões de memória e periféricos externos, módulos opcionais como rádio FM, GPS, processador de sinal digital, câmera, alto-falante, microfone e um pouco de chaves de hardware e interfaces (CASEY; BANN; DOYLE,

2010, tradução nossa). A Figura 7 mostra um diagrama de hardware genérico de um dispositivo com Windows Mobile moderno.

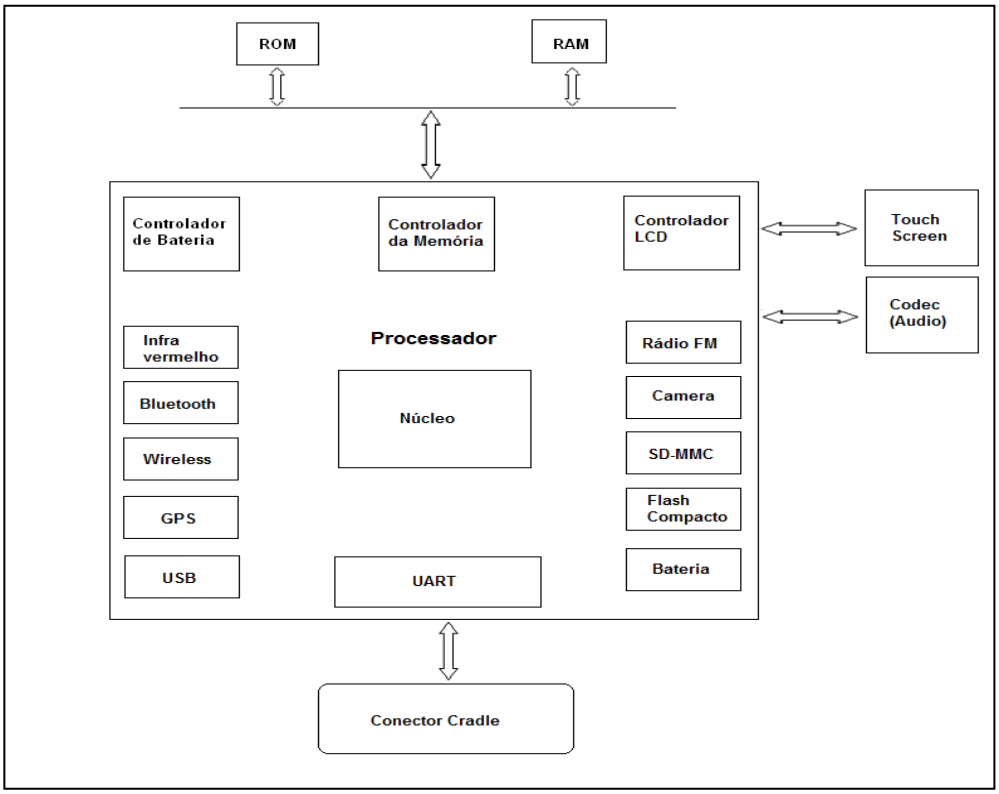


Figura 7. Diagrama de Hardware genérico em dispositivos com Windows Mobile.
Fonte: CASEY, E.; BANN, M.; DOYLE, J. (2010)

3.2.2.1 Processador

Com o Windows Mobile, a Microsoft pretende oferecer um sistema operacional que pode ser executado em uma variedade de plataformas de hardware. Atualmente, quatro famílias de núcleos de processadores são suportadas: ARM, MIPS SH4 e x86 (MICROSOFT, 2011). Destes, ARM é atualmente o mais comum em eletrônicos, como smartphone, PDA e dispositivos de navegação (GPS). Este documento teve o seu foco em dispositivos baseados na arquitetura ARM (KLAVER, 2010, tradução nossa).

3.2.2.2 Memória Flash

A memória flash é amplamente utilizada para o armazenamento dado não volátil. Existem dois tipos principais de memória Flash, NOR e NAND. Ela tem propriedades específicas que têm relevância jurídica. Por exemplo, como os dados não podem ser atualizados no local na memória flash, primeiro os dados do têm que ser copiado da memória flash para a RAM, modificados e, em seguida, copiados para um local diferente e vazio na flash. Os dados antes da mudança podem estar disponíveis após a mudança por meio de aquisições físicas (KNIJFF, 2010, tradução nossa).

3.2.2.2.1 Memória Flash NOR

Este tipo de memória flash tem uma interface semelhante a RAM, mas possui um barramento de dados, um barramento de endereços e linhas de controle. A flash NOR é mapeada no mapa do processador da memória e o processador de código pode ser executado diretamente a partir dela. Também podendo ser usada como local de armazenamento de dados do usuário. Muitos dispositivos Windows Mobile mais antigos têm uma única pasta no diretório raiz que é mapeada para uma seção na flash NOR (KNIJFF, 2010, tradução nossa).

Com um driver especial, como o *Intel Persistent Storage Manager* (INTEL, 2005), a parte da memória flash NOR que não é usada para o código pode ser usada para dados do usuário. Em uma investigação forense, essa pasta não deve ser negligenciada. Esta pasta é, por exemplo, muito apropriada para o armazenamento de backups do sistema e como ela reside na flash, os dados apagados podem persistir (KNIJFF, 2010, tradução nossa). Quando um dispositivo com uma bateria completamente descarregada faz uma redefinição

completa do sistema, esta pasta pode conter ainda uma cópia de segurança de todos os dados recente do usuário.

3.2.2.2.2 Memória Flash NAND

Pode ser considerada como o equivalente de estado sólido de um disco rígido. Ela tem uma interface com um barramento de E/S e as linhas de controle que ligam o chip de memória ao processador. Durante este barramento de E/S, comandos, endereços e dados são enviados. Como a memória flash NAND não é mapeada no espaço de memória do processador, o código armazenado em um chip de memória flash NAND não pode ser executado diretamente, mas tem que ser carregado em primeiro lugar na memória RAM, muito parecida com um disco rígido (CASEY; BANN; DOYLE, 2010, tradução nossa).

O comportamento típico do dispositivo Windows Mobile inteligente é que, após o sistema operacional ser carregado, ele detecta quando se trata de um arranque a frio. Nesse caso, ele instalará a personalização "*.cab*" a partir da personalização da partição flash, muitas vezes TFAT. Depois que esses arquivos são instalados, o aparelho é reiniciado e ele está pronto para ser usado (CASEY; BANN; DOYLE, 2010, tradução nossa).

3.2.3 Componentes de Software Típicos em Windows Mobile

Este capítulo descreve os componentes de software em um dispositivo Windows Mobile que estão envolvidos no armazenamento de dados do usuário ou podem ser usados em um contexto forense.

3.2.3.1 Bootloader

Em alguns dispositivos Windows Mobile, o *bootloader* pode ser usado como uma ferramenta para obter uma imagem física de memória. Alguns gestores de arranque já têm recursos para isso, embora às vezes barrados por algum mecanismo de segurança, como uma senha ou a inserção de um cartão de memória especial. Outros dispositivos precisam de um gerenciador adaptado para fornecer a funcionalidade necessária para criar uma imagem física (CASEY; BANN; DOYLE, 2010, tradução nossa).

Bootloaders às vezes têm a funcionalidade de cópiar vários tipos de memória do dispositivo para mídia externa, mas a funcionalidade nem sempre é acessível. Porque poderia facilitar o desbloqueo do cartão SIM ou outras formas de pirataria informática. Fabricantes de aparelhos tornam difícil o acesso a essa funcionalidade (CASEY; BANN; DOYLE, 2010, tradução nossa).

3.2.3.2 Heap

É uma parte da memória reservada para um aplicativo a ser usado para alocar e liberar memória (MICROSOFT, 2008b). A pilha contém variáveis que são criadas com as funções do sistema operacional como "*malloc()*". Funções como esta retornam um ponteiro para o bloco de memória oferecida pelo sistema operacional, se a quantidade requisitada de memória está disponível (CASEY; BANN; DOYLE, 2010, tradução nossa).

Quando se investiga o heap de um processo podem-se produzir dados muito interessantes. Muitas vezes buffers para várias finalidades estão localizados no heap.

3.2.3.2 Sistema de Arquivos

Os mais modernos dispositivos Windows Mobile são equipados com memória flash de hospedagem (T)FAT, partições para dados do usuário ou extensões de firmware, e partições de binário com firmware e código do bootloader (ROGERS; GLAUM; TONKELOWITZ, 2005, tradução nossa). Os sistemas de arquivos não são normalmente armazenados na memória flash NAND diretamente. É a interface do sistema operacional chamada Flash Translation Layer (FTL), que se encarrega de armazenar arquivos do sistema em blocos de memória flash NAND (KNIJFF, 2010, tradução nossa).

Ao analisar os dispositivos de armazenamento a nível do sistema de arquivos em um dispositivo Windows Mobile, ambas as partições binárias, assim como as partições do sistema de arquivos podem ser encontradas. Em uso normal, a única partição interessante para análise forense é a partição que contém o sistema de arquivos do usuário. Esta partição contém normalmente uma FAT ou um sistema de arquivos TFAT (CASEY; BANN; DOYLE, 2010, tradução nossa).

TFAT é uma transação segura da variante do FAT. Como a TFAT é uma transação segura, a perda repentina de energia, ou outras interrupções de mudanças no sistema de arquivos, não corrompe o sistema (MICROSOFT, 2010a).

Nas versões recentes do Windows Mobile, o sistema de arquivos hospeda os bancos de dados e os arquivos de registro. Em dispositivos onde este sistema de arquivos é baseado em memória flash, os dados do usuário são menos dependentes da vida útil da bateria.

3.2.3.3 Banco de Dados

Sistemas de arquivos baseados em memória Flash também facilitam a imagem do sistema de arquivos, em comparação com os sistemas baseados em memória RAM base. Depois que a imagem de um sistema de arquivos baseado em memória é criada a partir do dispositivo com Windows Mobile, os bancos de dados contendo os dados do usuário podem ser extraídos da imagem. Isso pode ser feito com ferramentas forenses que suportam TFAT; como TFAT é compatível com FAT, a maioria das ferramentas irá carregar imagens TFAT sem problemas. Uma vez carregado, os dois bancos de dados mais interessantes são *cemail.vol* e *pim.vol*, ambos localizados no diretório raiz do sistema de arquivos (CASEY; BANN; DOYLE, 2010, tradução nossa).

3.2.4 Estados Genéricos

A simples visão de um dispositivo de computação, tais como um computador desktop, é que ele está em estado "ligado (*on*)" ou estado "desligado (*off*)". No entanto, a amplificação adicional é necessária, particularmente para PDA, cujo comportamento é mais complexo. A Figura 8 apresenta um diagrama de alto nível, que ilustra os vários estados em que um PDA pode estar a qualquer momento, junto com as transições que podem ocorrer para causar uma mudança de estado (JANSEN; AYERS, 2004, tradução nossa). Enquanto um diagrama de estado é mais detalhado possível, os seguintes quatro estados fornecem um modelo simples, mas abrangente, genérico que se aplica ao PDA:

a) **estado nascente**: o dispositivo está no estado nascente, quando sai da fábrica - não contém dados de usuário e observa as configurações de fábrica. O PDA deve ser cobrado a um nível mínimo de tensão para ser utilizado e para ganhar

a entrada inicial para o estado nascente, que é atingido quando o dispositivo é ligado pela primeira vez, premindo o botão de energia. Este estado pode ser atingido novamente quando se faz uma reinicialização (Hard Reset), que limpa os arquivos e a memória de trabalho dinâmica e restaura as configurações de fábrica (CASEY; BANN; DOYLE, 2010, tradução nossa);

b) **estado ativo**: dispositivo que está no estado ativo, está ligado, executando tarefas, e pode ser personalizado pelo usuário e ter seus arquivos preenchidos com dados. Se uma reinicialização flexível (*soft reset*) é executada, o dispositivo retorna para o estado ativo depois de limpar a memória de trabalho. Se os mecanismos de autenticação do usuário estiverem habilitados, eles são afirmados em uma transição suave que redefinirá dispositivo a este estado (CASEY; BANN; DOYLE, 2010, tradução nossa);

c) **estado de repouso**: o estado de repouso é um modo inativo, que conserva a vida da bateria, mantendo os dados do usuário e desempenhando outras funções. Neste contexto, as informações para o dispositivo estão preservadas na memória para permitir uma rápida retomada do processamento ao retornar para o estado ativo. Pressionando o botão de energia quando no estado ativo ou semi-ativo (isto é, para desligar o dispositivo), ou ter um timer de inatividade, quando expira no estado semi-ativo, faz uma transição para o estado inativo (CASEY; BANN; DOYLE, 2010, tradução nossa);

d) **estado semi-ativo**: é um estado parcial entre ativo e inativo. Atingido por um timer, que é acionado depois de um período de inatividade permitindo que a vida da bateria seja preservada, escurecendo a tela e tomando outras medidas adequadas. O estado semi-ativo retorna para o estado ativo quando se dá um

> toque na tela, pressiona-se um botão, ou um *Soft Reset*[10] ocorre. Os dispositivos que não suportam um estado semi-ativo só precisam de um timer de inatividade única para a transição direta do ativo para estado de repouso (CASEY; BANN; DOYLE, 2010, tradução nossa).

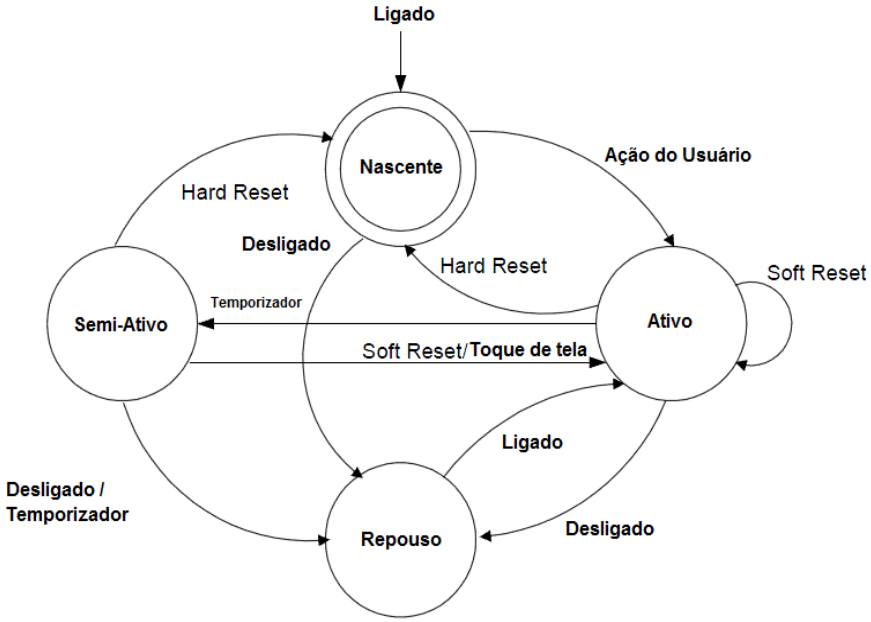


Figura 8. Diagrama de estados genéricos
Fonte: CASEY, E.; BANN, M.; DOYLE, J. (2010)

Simplesmente declarado - *um PDA com bateria suficiente nunca é realmente desligado, já que os processos estão ativos mesmo quando não há sinais visíveis presentes.*

Para simplificar, um dispositivo é dito está "*off*" ou "*desligado*" se está no estado de repouso, e "*on*" ou '*ligado*" se estiver em qualquer um dos demais estados. Da mesma forma, um dispositivo é dito ser "*limpo*" e desprovido de dados quando está no estado nascente (JANSEN; AYERS, 2004, tradução nossa).

Segundo Casey, Bann e Doyle (2010), no entanto, existem diferenças suficientes entre os sistemas Windows Mobile e outros sistemas operacionais Windows, de tal forma que

[10] Um *soft reset* faz com que o PDA deixe de fazer qualquer operação em execução e reinicie, não perdendo a informação que nele se conserva.

se exige conhecimentos especializados e ferramentas para localizar e interpretar evidências digitais.

O Windows Mobile usa uma variação do sistema de arquivos FAT chamado de transação segura do sistema de arquivos FAT (TFAT), que tem algumas características de recuperação no caso de um dispositivo der parada súbita (CASEY; BANN; DOYLE, 2010, tradução nossa).

Como mostrado na Figura 9, a hierarquia do sistema de arquivos destes dispositivos tem semelhanças com outros sistemas operacionais da Microsoft, que deve ser familiar a qualquer pessoa que tenha realizado um exame forense de sistemas de computador com Windows.

A maioria dos arquivos criados pelo usuário, incluindo fotografias e vídeos digitais tiradas com a câmera do dispositivo, é armazenada na pasta "*Meus Documentos*". Por outro lado, os PDA com Windows Mobile retêm os restos das atividades do usuário em uma variedade de locais. Estes artefatos incluem o uso de arquivos *index.dat* associados com o uso do Internet Explorer e arquivos de banco de dados integrados, que termina com a extensão "*.vol*" mostrado na painel do lado direito da Figura 9. Além disso, os registros em dispositivo Windows Mobile podem armazenar informações sobre usuários e suas atividades, conforme será demonstrado no "exame de registro" deste documento.

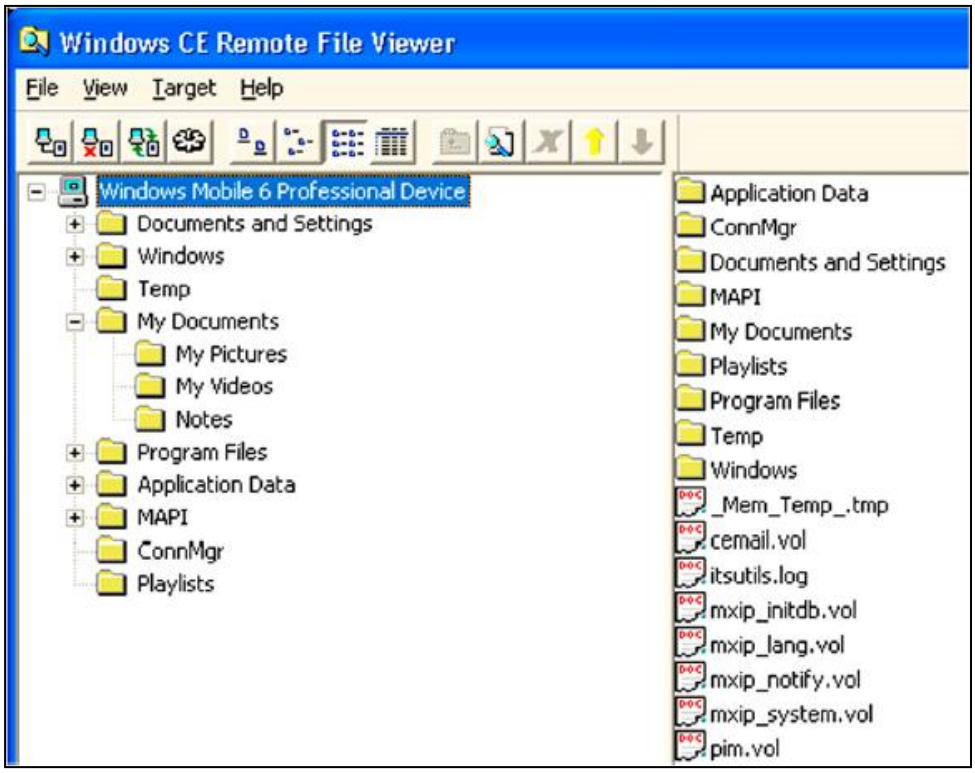


Figura 9. Arquivo hierarquia do sistema em um Samsung i607 (Blackjack).
Fonte: CASEY, E.; BANN, M.; DOYLE, J. (2010)

3.2.5 Locais de Artefatos de Uso em PDA com Windows Mobile

Apesar de alguns arquivos como *cemail.vol* podem ser encontrados em todos os dispositivos com Windows Mobile, a localização dos artefatos de uso nos diferentes modelos de dispositivos móveis pode variar. A Figura 9 fornece uma visão geral das fontes potencialmente úteis de evidências sobre o Samsung i607 (Blackjack), S62 HTC (Dash), e dispositivos Motorola Q. Muitos dessas locais também serão encontrados em outros tipos de dispositivos com Windows Mobile. Arquivos adicionais podem ser encontrados em outros locais, como a pasta "\ *Temp*". Mais detalhes sobre as áreas listadas na Figura 10 são fornecidos mais adiante neste documento com exemplos de como a informação pode ser útil do ponto de vista legal.

File	Description
\cemail.vol	An embedded database that stores information relating to communications, including text messages and portions of e-mails, not including file attachments.
\pim.vol	An embedded database that includes call logs (clog.db), address book information, calendar items, speed dial details (speed.db), and to do tasks.
\ReplStorVol	A file replication database used to synchronize items on the device with data in another location (Microsoft, 2008a).
\My Documents\My Pictures	A repository of photographs taken or downloaded by the user. This is the default download location for pictures.
\My Documents\UAContents	A folder with artifacts of user activities, including portions of MMS in ".dat" files and an MMS log file.
\Documents and Settings\default\user.hv	The User Registry hive.
\Documents and Settings\default.hv OR system.hv[a]	The System Registry hive.
\Windows\Messaging	A repository of viewed SMS and e-mail messages, stored in ".mpb" files.
\Windows\Messaging\Attachments	A repository of downloaded e-mail attachments in ".att" files.
\Windows\Profiles\guest	Contains Internet Explorer history, as well as cache and cookie files, including `index.dat` files.
\Windows\Favorites	Internet Explorer bookmarks.
Windows\eT9Cdb.Cdb and eT9Rudb.Rdb	Custom user T9 dictionary files.

a The location of the system Registry hive may vary. The Registry value under HKEY_LOCAL_MACHINE\init\BootVars\SystemHive contains the full path of the system hive.

Figura 10. Fonte de dados Potencialmente úteis de em PDA com Windows Mobile.
Fonte: CASEY, E.; BANN, M.; DOYLE, J. (2010)

Do ponto de vista legal, pode ser difícil adquirir e analisar as informações sobre dispositivos com Windows Mobile. Alguns dos arquivos são bloqueados pelo sistema operacional, tornando mais difícil a obtenção de uma segunda via forenses de seus conteúdos (CASEY; BANN; DOYLE, 2010, tradução nossa).

Por exemplo, certas ferramentas de aquisição forense que dependem de APIs do Windows Mobile não conseguem copiar o conteúdo dos arquivos que estão bloqueados pelo sistema operacional como *cemail.vol, pim.vol* e alguns registros. Como resultado desta e de outras restrições em dispositivos com Windows Mobile, métodos de aquisição mais amplamente disponíveis não obtêm todos os dados armazenados nesses dispositivos; algumas ferramentas obtêm muito mais dados do que outros.

Além disso, muitas ferramentas forenses têm dificuldade em interpretar os dados adquiridos a partir de dispositivos com Windows Mobile. Estas dificuldades de interpretação podem resultar em deturpação do sistema de arquivos TFAT ou exclusão de informações úteis a partir de arquivos importantes, exigindo que profissionais forenses decifrem os formatos de arquivo proprietários. Discrepâncias também podem existir na interpretação de dados de atributos entre as ferramentas, que é assunto também abordado neste documento (CASEY; BANN; DOYLE, 2010, tradução nossa).

3.2.6 Aquisição Forense em Windows Mobile

Alguns dispositivos PDA com Windows Mobile não permitem que programas não autenticado funcionem. Devem ser reconfigurados para permitir que ferramentas forenses de aquisição funcionem corretamente (CASEY; BANN; DOYLE, 2010, tradução nossa).

Muitos dispositivos suportam mídias de armazenamento removíveis, como cartões micro SD que podem armazenar arquivos maiores, como fotografias digitais, vídeos e música. Apesar de ferramentas forenses poderem ser capazes de adquirir dados lógicos destas mídias removíveis por meio do próprio dispositivo, este processo pode alterar dados na mídia e não dar ao analista acesso aos dados que foram excluídos. Portanto, a menos que o cartão seja protegido por senha ou criptografado, é geralmente aconselhável remover a mídia de armazenamento, e criar uma duplicação forense usando métodos padrão de computação forense (CASEY; BANN; DOYLE, 2010, tradução nossa).

3.2.7 Recuperar Dados Apagados

Embora ferramentas forense possam recuperar nome de arquivos apagados a partir do volume TFAT do dispositivo Windows Mobile, o analista forense pode encontrar obstáculos para a recuperação de arquivos. Por exemplo, a falha na reconstrução correta do sistema de arquivos TFAT em um dispositivo Windows Mobile pode resultar em falta de arquivos e pastas (CASEY; BANN; DOYLE, 2010, tradução nossa). A Figura 11 mostra o sistema de arquivos adquiridos a partir de um HTC S620 (Dash), faltando subpastas da pasta "*Documents and Settings*".

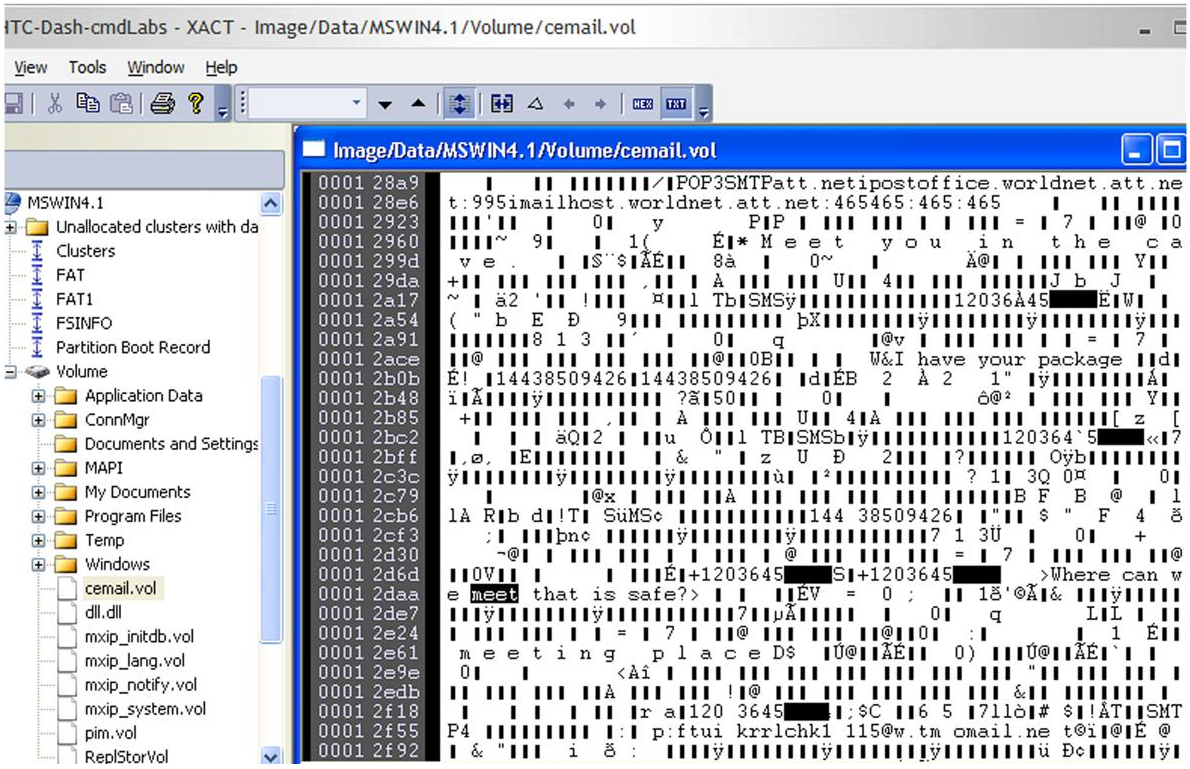


Figura 11. Sistema de arquivos no Windows Mobile visualizado utilizando a ferramenta XACT, com a falta de pastas.
Fonte: CASEY, E.; BANN, M.; DOYLE, J. (2010)

Em alguns casos, os arquivos importantes, como *pim.vol* não aparecem na visualização do sistema de arquivos. A reconstrução incompleta dos sistemas de arquivos não está limitada aos dispositivos móveis, e ocorreu em ferramentas do sistema de arquivos forenses (CASEY, 2005, tradução nossa). A dificuldade de reconstruir os sistemas de arquivos em dispositivos móveis é agravada pela presença repetida de "DONT DEL" nos diretórios de entrada, e da natureza em rápida mudança de dispositivos móveis. Esses tipos de discrepâncias enfatizam a importância de validar as ferramentas forenses presente, apresentado em um dos capítulos deste documento.

Outra barreira para recuperação de arquivos apagados, é que em alguns dispositivos Windows Mobile aparece padrão repetido *0xFF* para substituir o conteúdo de arquivos apagados. Há que se ter em mente que o conteúdo original destes arquivos excluídos

podem ser recuperados usando avançadas técnicas forenses que dão acesso ao conteúdo completo da memória Flash física (CASEY; BANN; DOYLE, 2010, tradução nossa).

Embora os arquivos apagados possam ser difíceis de recuperar, as cópias podem existir em outros lugares no dispositivo como anexos de mensagens MMS ou e-mails conforme será apresentado mais adiante neste documento. A pesquisa de palavras-chave pode ser a abordagem mais eficaz para encontrar fragmentos de dados de interesse em alguns casos.

3.2.8 Exame de Banco de Dados Incorporados

O dispositivo Windows Mobile armazena algumas informações importantes em arquivos de volume que encapsulam múltiplos bancos de dados integrados que incluem detalhes sobre as comunicações, contatos e chamadas. Por exemplo, o arquivo *pim.vol* contém incorporado informações do banco de dados como o histórico de chamadas e informações de contato por meio do banco de dados *clog.db* ((MICROSOFT, 2005, 2010, tradução nossa).

Embora o formato não seja formalmente documentado, muitos aspectos dos arquivos *pim.vol* e *cemail.vol* têm sido exploradas por desenvolvedores de aplicativos. A relação entre os bancos de dados dentro *cemail.vol* está representado na Figura 12. Cada banco de dados contém vários registros, cada um com sua própria *Object Identifier* (OID) que fornece o mecanismo mais rápido para encontrar um registro específico no arquivo *cemail.vol*. Cada registro contém campos (propriedades) que armazenam os dados reais (CASEY; BANN; DOYLE, 2010, tradução nossa).

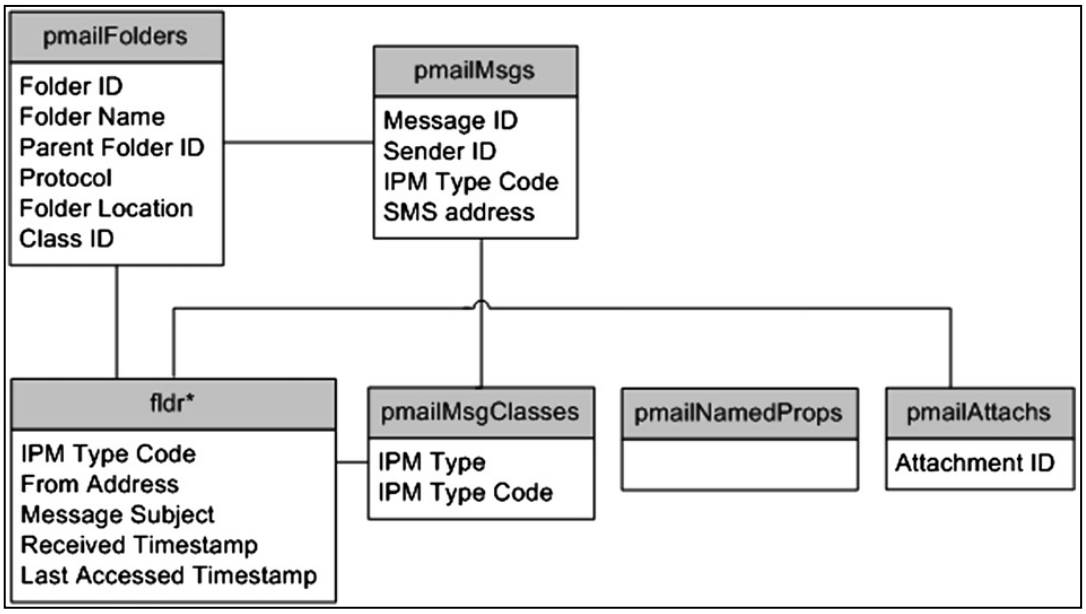


Figura 12. Visão geral do arquivo *cemail.vol*.
Fonte: CASEY, E.; BANN, M.; DOYLE, J. (2010)

O arquivo *cemail.vol* armazena detalhes sobre cada mensagem e contém referências a conteúdo associado em outros arquivos no dispositivo, como um volume do conteúdo de mensagens e anexos (CASEY; BANN; DOYLE, 2010, tradução nossa).

Geralmente, os componentes de mensagens são armazenados em vários locais: "*pMail*" e "fldr" bancos de dados em *cemail.vol*, ".mpb" e ".att" arquivos no dispositivo. Os banco de dados incorporados mais úteis dentro *cemail.vol* são descritos a seguir:

a) **pmailFolders**: esse banco de dados define a hierarquia da pasta de mensagens (por exemplo, entrada, saída, rascunhos, itens excluídos) para cada endereço com que o dispositivo Windows Mobile é configurado (CASEY; BANN; DOYLE, 2010, tradução nossa).Para cada pasta de mensagens, há um registro em "*pmailFolder*" que mostra o banco de dados "*fldr*" associado com detalhes da mensagem;

b) **pmailMsgs**: contém informações sintéticas sobre as mensagens no dispositivo, incluindo a identificação da mensagem, tipo de mensagem e informação de endereço da mensagem (CASEY; BANN; DOYLE, 2010, tradução nossa). Os

valores do banco de dados que indicam o banco de dados "*fldr*" de cada mensagem são associados com base na identificação da pasta, geralmente no formato de "*fldr*" + "folder ID" (por exemplo, *fldr31000026*). A Tabela 3 mostra a tabela que descreve alguns identificadores de propriedade útil dentro de cada registro;

Tabela 3. Tabela de identificadores de propriedade de itens úteis na base de dados "*pmailMsgs*".

ID da Propriedade	Descrição
0x800C	Contém informações de identificação do remetente, tal como um número de telefone no caso de uma mensagem SMS.
0x8001	Contém o código do tipo de mensagem interpessoais (IPM), que indica o tipo de mensagem enviada (por exemplo, SMS, MMS, e-mail). A tabela de pesquisa para o IPM, tipo de código que reside no banco de dados "*pmailMsgClasses*".
0x0E09	Contém a ID de pasta na forma decimal. Que deve ser convertida em hexadecimal equivalente para determinar o que contém na base de dados "*fldr*"

Fonte: CASEY, E.; BANN, M.; DOYLE, J. (2010)

c) **pmailMsgClasses**: oferece uma tabela de tipos de IPM utilizado no banco de dados "*pmailMsgs*" e "fldr" bancos de dados. Por exemplo, as associações de IPM "*pmailMsgClasses*" em um HTC S620 (*Dash*) estão listadas na figura 13, com o tipo de conteúdo do lado esquerdo e o identificador associado à direita (CASEY; BANN; DOYLE, 2010, tradução nossa);

IPM.MMS	822083597
IPM.Note	822083598
IPM.SI	822083600
IPM.SL	822083601
IPM.SMStext	822083599
IPM.SMStext.SIM	855638066
REPORT.IPM.Note.DR	822083603
REPORT.IPM.Note.IPNNRN	822083606
REPORT.IPM.Note.IPNRN	822083605
REPORT.IPM.Note.NDR	822083604
REPORT.IPM.Note.Status	822083602

Figura 13. Associações de IPM no banco de dados "*pmailMsgClasses*" em um HTC S620 (Dash).
Fonte: CASEY, E.; BANN, M.; DOYLE, J. (2010)

d) **pmailNamedProps**: contém uma tabela de pesquisa de nomes de propriedade do objeto que reside no interior do dispositivo (por exemplo, SMS: SMSCAddress, Reunião: Lembrete). Sua estrutura é similar ao banco de dados "*pmailMsgClasses*", mas usa dois pontos para a demarcação dentro dos valores em vez de um período (CASEY; BANN; DOYLE, 2010, tradução nossa);

e) **fldr**: este banco de dados contém uma riqueza de informações sobre as mensagens que estão no dispositivo, incluindo o tipo de IPM, o assunto, o endereço do remetente, e quando a mensagem foi recebida e modificada pela última vez . Quando o corpo da mensagem é pequeno o suficiente, o conteúdo completo é armazenado no banco de dados incorporado. Propriedades específicas que podem ser armazenadas em registros de um banco de dados "fldr" estão listadas na Tabela 4, com seus identificadores de propriedade associados. Qualquer propriedade pode ou não estar presente, dependendo do tipo de registro.

Tabela 4. Identificadores de propriedade de itens úteis no banco de dados "*fldr*".

ID da Propriedade	Descrição
0x8005	OID usado como um valor de pesquisa.
0x0C1F	A partir do endereço (nome do contato não resolvido)
0x0C1A	A partir do endereço (nome do contato resolvido)
0x003D	Indica o prefixo da mensagem, quer "'Re:" ou "Fw:", denotando responder, encaminhar e nulo respectivamente.
0x0037	Assunto da mensagem ou, quando aplicável, o corpo da mensagem se for pequeno o suficiente.
0x0E06	Timestamp da mensagem recebida.
0x3008	Timestamp da última mogificação feita na mensagem.
0x001A	Campo de pesquisa, que liga o banco de dados ao banco de dados "pmailMsgClasses".

Fonte: CASEY, E.; BANN, M.; DOYLE, J. (2010)

O banco de dados "*fldr*" adota uma abordagem estática para armazenar dados, de tal forma que quando o nome de um contato é excluído dos contactos do dispositivo, as mensagens anteriores mantêm o nome do contato. Mensagens subsequentes não conterão o nome do contato, e ambos os endereços listados na Tabela 4 manterão o mesmo valor.

Isso pode ser de especial interesse para pesquisadores, se um usuário exclui um contato da sua agenda de endereços, na tentativa de esconder um relacionamento pessoal.

3.3 FERRAMENTAS PARA ANÁLISE FORENSE EM PDA COM WINDOWS MOBILE

O crescimento das indústrias de recuperação de dados e descoberta eletrônica tem sido acompanhado por forte crescimento do número de ferramentas de informática forense disponível e em uso. Mais importante, tem havido uma tendência de ferramentas sofisticadas ou pacotes integrados que executam uma maior gama de funções forense. O desenvolvimento mais notável dos últimos tempos na funcionalidade de algumas das ferramentas usadas, ou

seja, a integração dos vários aspectos de uma investigação forense em um portfólio baseado em casos (KLAVER, 2010, tradução nossa).

Pode-se, em geral, identificar três categorias de funcionalidade forense: de imagem, análise e visualização. Essas categorias podem ser naturalmente discriminadas, um número crescente de ferramentas integra essas funcionalidades (GEORGE et al, 2003, tradução nossa).

Imagem:

a) Imagem da memória volátil (incluindo PDA e celulares telefones);
b) Imagem de disco e arquivo;
c) Bloqueadores;
d) Geradores de código de integridade.

Análise:

a) Ambiente de recuperação de dados e busca de dados em disco para sequências de texto, por sector (incluindo áreas normalmente não utilizadas);
b) De dados e recuperação de arquivos;
c) Disco e arquivo ferramentas de verificação de integridade do sistema;
d) Conversão de arquivo (ou seja, a conversão de arquivos de texto em arquivos proprietários ou vice-versa, ou entre formatos proprietários, a fim de facilitar processamento adicional);
e) A filtragem de dados por data modificada e outras propriedades do arquivo como tipo de aplicação, tais como e-mail, gráficos, palavras processamento de arquivos, planilhas e apresentação;
f) Ferramentas de busca, motores de busca com a sofisticada lógica fuzzy;
g) Ferramentas de mineração de dados.

Visualização:

Esta é uma visão geral de algumas das funcionalidades e características de ferramentas forense e, como tal, não se destina a ser uma análise abrangente e detalhada. Não é agora, nem existe a possibilidade haver uma ferramenta que faça tudo o que um investigador pode exigir.

Três áreas representam um desafio permanente, que devem ser abordadas para ferramentas do futuro:

a) O volume crescente de dados com os quais o analista tem de lidar é encarado como um resultado da maior largura de banda das ligações Internet;

b) A necessidade de fornecer um software que apóia e incentiva trabalho colaborativo por vários examinadores, que podem estar geograficamente separados e, possivelmente, de diferentes jurisdições;

c) A necessidade de ser capaz de acomodar novas ferramentas forenses para inter-operar com as ferramentas e sistemas existentes, a fim de poder correlacionar os dados forenses de uma variedade de registros (ou seja, a necessidade de extensibilidade, a fim de apoiar, pelo menos em algum grau a noção de uma capacidade genérica forense em face da mudança tecnologia).

A maioria dos softwares exige constante desenvolvimento e apoio, a fim de se adaptarem aos novos ambientes de hardware. O desenvolvimento de software forense é especialmente afetado por esse ambiente em mudança.

O problema é agravado pela rápida mudança no tipo de computador ou crime a ser investigado e a complexidade das investigações (por exemplo, múltiplos atores distribuídos em vários computadores, em diferentes localizações geográficas). O software forense precisa acompanhar essas mudanças, a fim de ser utilizados em um amplo espectro de investigações (GEORGE; et al, 2003, tradução nossa).

Ao contrário da situação com os computadores pessoais, o número e a variedade de kits de ferramentas para PDA e outros dispositivos portáteis são consideravelmente reduzidos. Não só há poucas ferramentas especializadas, mas também a gama de dispositivos sobre os quais eles operam normalmente é reduzido para apenas a família mais popular dos dispositivos de PDA. Estas ferramentas permitem que o examinador tenha acesso livre para adquirir o conteúdo (isto é, nenhuma técnica de autenticação precisa ser satisfeita para ter acesso) (JANSEN; AYERS, 2004, tradução nossa).

Conforme Jansen e Ayers (2004) as ferramentas forense adquirem dados de um dispositivo de duas formas: aquisição física ou aquisição lógica. Aquisição física implica uma cópia bit a bit de toda a informação física (por exemplo, uma unidade de disco ou chip de memória RAM), enquanto a lógica de aquisição implica uma cópia bit a bit de objetos de armazenamento lógico (por exemplo, diretórios e arquivos) que residem em um armazenamento lógico (por exemplo, uma partição de sistema de arquivos) (JANSEN; AYERS, 2004, tradução nossa).

A diferença reside na distinção de como a memória pode ser vista por meio de um processo e das facilidades do sistema operacional (ou seja, uma visão lógica), memória versus como pode ser vista na sua forma bruta pelo processador e outros componentes de hardware relacionados (isto é, uma visão física) (JANSEN; AYERS, 2004, tradução nossa).

A aquisição de física tem vantagens sobre a aquisição lógica, uma vez que permite ver arquivos apagados e todos os restos de dados (RAM ou espaço não alocado de arquivos não utilizados) para serem examinados, que caso contrário desapareceria. Dispositivos físicos para imagens são geralmente mais facilmente importados para outra ferramenta para análise e relatórios. No entanto, uma estrutura lógica tem a vantagem de que é uma organização mais natural de entender e usar durante o exame. Assim, se possível, fazer os dois tipos de aquisição, em PDA é preferível (JANSEN; AYERS, 2004, tradução nossa).

Ferramentas que não foram concebidas especificamente para fins forenses são questionáveis e devem ser cuidadosamente avaliadas antes do uso. Em algumas situações, elas podem ser o único meio para obter informações que possam ser relevantes como prova (CASEY; BANN; DOYLE, 2010, tradução nossa). A seguir está a Tabela 5 e a descrição de algumas ferramentas úteis para investigação, aquisição e análise forense em dispositivos PDA.

Tabela 5. Ferramentas forense para dispositivos PDA e sua função.

Ferramentas	Symbian OS	Windows Mobile	Android OS	iPhone OS	Blackberry	Palm OS
EnCase Forensic	AQ / EX / RL	AQ / EX / RL	AQ / EX / RL	AQ / EX / RL	AQ / EX / RL	AQ / EX / RL
PDA Device Seizure	AQ / EX / RL	AQ / EX / RL	N/D	AQ / EX / RL	N/D	AQ / EX / RL
Pocket PC Forensic	N/D	AQ / EX / RL	N/D	N/D	AQ / EX / RL	AQ / EX / RL
UFED Physical Analyzer	AQ / EX / RL	AQ / EX / RL	AQ / EX / RL	AQ / EX / RL	AQ / EX / RL	AQ / EX / RL
RAPI	ND	AQ / EX	AQ / EX	ND	ND	ND
Oxygen Forensic Suite	AQ / EX / RL	AQ / EX / RL	AQ / EX / RL	AQ / EX / RL	AQ / EX / RL	AQ / EX / RL
XACT / XRY	AQ / EX / RL	AQ / EX / RL	AQ / EX / RL	AQ / EX / RL	AQ / EX / RL	ND
MOBILedit! Forensic	AQ / EX / RL	AQ / EX / RL	AQ / EX / RL	AQ / EX / RL	AQ / EX / RL	N/D
FTK	EX / RL	EX / RL	EX / RL	EX / RL	EX / RL	EX / RL
Autopsy	EX / RL	EX / RL	EX / RL	EX / RL	EX / RL	EX / RL
MIAT	AQ	AQ	ND	ND	ND	ND

Legenda			
AQ – Aquisição	**EX – Exame / Análise**	**RL – Relatório**	**ND – Não Disponível**

3.3.1 Paraben’s Device Seizure

Paraben’s Device Seizure é uma ferramenta forense disponível comercialmente, que permite adquirir e analisar informações em celulares, PDA e GPS. Dentre as suas características incluem a capacidade de adquirir a imagem do dispositivo, realizar pesquisas transformando em dados os arquivos adquiridos, bem como gerar valores de hashing de

arquivos individuais e gerar um relatório dos resultados. Também oferece um arquivo de marcação com a capacidade de organizar as informações, juntamente com uma biblioteca de gráficos que monta automaticamente as imagens encontradas em um único local, com base na extensão do arquivo adquirido.

Dependendo do modelo do dispositivo, o Device Seizure pode adquirir os seguintes dados:

a) histórico de SMS (mensagens de texto);
b) sms excluídas;
c) agenda telefônica (tanto armazenada na memória do telefone como do cartão SIM);
d) histórico de chamadas
e) agenda;
f) calendário;
g) RAM / ROM;
h) bancos de dados;
i) e-mail;
j) registro (dispositivo com Windows Mobile).

3.3.2 MOBILedit! Forensic

É um das ferramentas de investigação forense para dispositivos móveis (telefones, PDA) mais confiáveis e usadas do mundo. Avaliado pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos da América, MOBILedit Forensic é uma das principais ferramentas de investigação de dispositivos móveis, utilizada em mais de 70 países. Basta

conectar um telefone e o MOBILedit Forensic extrai todo o conteúdo e gera um relatório forense pronto para a apresentação nos tribunais. E contém as seguintes características:

a) análise do dispositivo via Bluetooth, IrDA ou conexão a cabo;
b) análise da agenda, últimos números marcados, chamadas perdidas, chamadas recebidas, mensagens SMS, mensagens multimídia, fotografias, arquivos, detalhes do telefone, notas, tarefas;
c) análise do cartão SIM;
d) leitor de mensagens suprimidas e as mensagens do cartão SIM
e) gerador de Relatórios baseados no modelo do dispositivo;
f) possibilidade de imprimir os relatórios prontos para uso (gerados em qualquer idioma);
g) é um software que mantém a evidência segura e à prova de falsificação usando hash MD5;

3.3.3 Pocket PC Forensics Tool

Esta ferramenta forense está a torna-se um dos instrumentos de investigação muito poderoso para extrair informações detalhadas dos dispositivos móveis baseados em Windows para o uso como evidência. É usada para coletar dados, análise forense e investigação científica, sendo plenamente capaz de capturar informações detalhadas, tais como registros de banco de dados, arquitetura de processador e outras informações relacionadas com o dispositivo em causa. Não obstante a isso, é uma ferramenta útil para examinar outras informações relevantes do dispositivo, incluindo SMS (mensagens enviadas ou recebidas), histórico de chamadas (duração da chamada e registro de chamadas), Registro de contatos,

pastas de arquivos (de fotos, imagens, histórico de documentos de texto). E contém as seguintes características:

a) extrair as informações gerais, como números de telefone do livro de contato, SMS, arquivos salvos e pastas do dispositivo;
b) analisar os detalhes do nome do fabricante, modelo, número de IMEI, número de identificação do sim e outras informações relacionadas ao dispositivo;
c) da mesma forma fornece as informações sobre o hardware, uso de memória, arquitetura de software e a versão do sistema operacional instalado no dispositivo;
d) gerar o relatório de informações detalhadas em formato txt para uso posterior;
e) suporta vários dispositivos;
f) permite salvar as informações do adquiridas na unidade de disco do PC.

3.3.4 UFED Physical Analyzer

É uma ferramenta que fornece uma análise em profundidade da memória física dos dados extraídos de um dispositivo (conteúdo da agenda, mensagens SMS, os registros de chamadas, arquivos de imagem, arquivos de vídeo, arquivos de áudio e muito mais). Também gerar relatórios de dados abrangentes e verificar dados relevantes extraídos e analisados a partir do dispositivo. É das mais recentes ferramentas usadas para análise, decodificação de scripts e relatórios, em um ambiente acessível e fácil de navegar.

A função de extração de memória física proporciona um acesso mais abrangente aos dados dos dispositivos, incluindo informações suprimidas e escondidas, bem como o acesso às senhas. Diferentemente do processo de extração lógica, a extração física ignora o

sistema operacional do dispositivo, sendo a aquisição dos dados feita diretamente como uma imagem, a partir da memória flash interna.

3.3.4.1 Análise dos dados

O UFED Physical Analyzer permite ao investigador realizar a análise em profundidade dos dados extraídos e gerar relatórios, oferecendo os seguintes recursos principais:

a) análise do hexadecimal com uma visão em camadas de conteúdo da memória;
b) visualização e navegação simples e amigável de informações;
c) poderosas ferramentas de busca.

3.3.5 Oxygen Forensic Suite

É um software forense para dispositivos móveis, que vai além da análise lógica padrão de celulares, smartphones e PDA. O uso de protocolos avançados e APIs proprietárias de celulares permitem extrair dados muito mais do que podem ser extraídos por meio de ferramentas forenses utilizando protocolos de lógica padrão, especialmente para smartphones. Ajuda os peritos a extrair o máximo das informações a partir de uma grande maioria dos dispositivos móveis para fins de investigação.

3.3.6 EnCase Forensic

É uma ferramenta destinada aos profissionais forenses que necessitam de condução eficiente, coleta de dados e investigações em um processo repetitivo e defensável.

EnCase Forensic permite adquirir dados de uma ampla variedade de dispositivos, de formas a encontrar potenciais evidências, resultando em relatórios detalhados de suas descobertas, tudo isso mantendo a integridade das evidências. Produz uma cópia binária exata do disco ou mídia original, gerando valores de hash MD5 para arquivos de imagens relacionadas e atribui valores de CRC[11] para os dados. Essas verificações e balanços revelam caso a evidência tenha sido adulterada ou alterada, ajudando a manter todas as evidências intactas para uso em processos judiciais.

3.3.7 FTK

Forensic Toolkit[12] é reconhecido mundialmente como o padrão em software de computação forense. Esta é uma ferramenta válida em casos judiciais (tribunal), proporciona investigações de ponta em forense digital, tais como: análise, descriptografia e software de quebra de senha software, tudo dentro de uma interface intuitiva e personalizável. FTK foi construída para ser rápida, analítica e de escala empresarial. E contém as seguintes características:

- cria imagens, analisa o registro, conduz uma investigação, decodifica os arquivos, as senhas, identifica esteganografia, e constrói um relatório com uma solução única;
- recupera senhas de mais de 100 aplicações. Quando a CPU está ociosa, aproveita toda a rede para descriptografar os arquivos e executar ataque robusto de dicionário;
- KFF biblioteca *hash*;

[11] Verificação de redundância cíclica é um código detector de erros. Um tipo de função hash que gera um valor expresso em poucos bits em função de um bloco maior de dados, como um pacote de dados, ou um ficheiro, por forma a detectar erros de transmissão ou armazenamento.
[12] Para mais informações, acessar: http://accessdata.com/products/forensic-investigation/ftk.

- suporte para grandes e complexos conjuntos de dados;
- componentes compartimentados;
- capacidade de fazer backup e arquivamento dos casos;

3.3.8 XACT / XRY

É uma ferramenta projetada para rodar no sistema operacional Windows que permite que você execute uma extração segura forense de dados de uma ampla variedade de dispositivos móveis, como smartphones, GPS de navegação, modems 3G, tocadores portáteis de música e os tablets. Existem diversas variantes XRY diferentes disponíveis, dependendo da necessidade.

XRY lógica é uma solução para qualquer PC baseado em Windows, com o hardware necessário para a investigação forense de dispositivos móveis. XRY é a norma em análise forense de dispositivos móveis.

XRY Física é mais avançada, permite realizar uma extração de “físico” de um dispositivo.

XACT é um aplicativo analisador hexadecimal que complementa a ferramenta XRY, permitindo que os examinadores possam visualizar os dados hexadecimais extraídos durante o despejo físico de um dispositivo.

3.3.9 *Remote Application Programmers Interface* (RAPI)

É um conjunto de ferramentas que podem ser usadas para obter imagens de um dispositivo Windows Mobile, desenvolvido pela Hengeveld (2009). Este conjunto de ferramentas é uma coleção de cerca de 30 programas de linha de comando que podem ser

executados em um PC e que operam no dispositivo Windows Mobile por meio de uma conexão ActiveSync.

Todos os comandos se comunicam com o servidor RAPI que é executado no dispositivo. Algumas ferramentas apenas usam a API nativa que o servidor RAPI fornece, outras ferramentas precisam ter acesso mais avançado e estas usam uma biblioteca auxiliar chamada "*itsutils.dll*". Esta biblioteca é copiada para o dispositivo e carregada na memória pelo processo do servidor RAPI. A ferramenta pode acessar funções especializadas na biblioteca auxiliar (KLAVER, 2010, tradução nossa) .

A Figura 14 mostra como o processo é feito. O servidor RAPI interage com o dispositivo diretamente por meio das funções da API (seta pontilhada), e por meio da DLL auxiliar (seta tracejada).

Em versões anteriores das ferramentas RAPI, a *DLL* sempre foi copiado para o diretório \Windows. A partir da versão 080731 da ferramenta RAPI, o local no dispositivo onde a biblioteca é copiada para auxiliar pode ser mudado pela adição de uma chave no registro do PC:

HKEY_CURRENT_USER\Software\itsutils\devicedllpath = "\Storage Card\itsutils.dll"

Além disso, *itsutils.dll* pode escrever mensagens para um arquivo de log. Adicionando outra chave definirá o destino do arquivo de log e mudará para log on ou off:

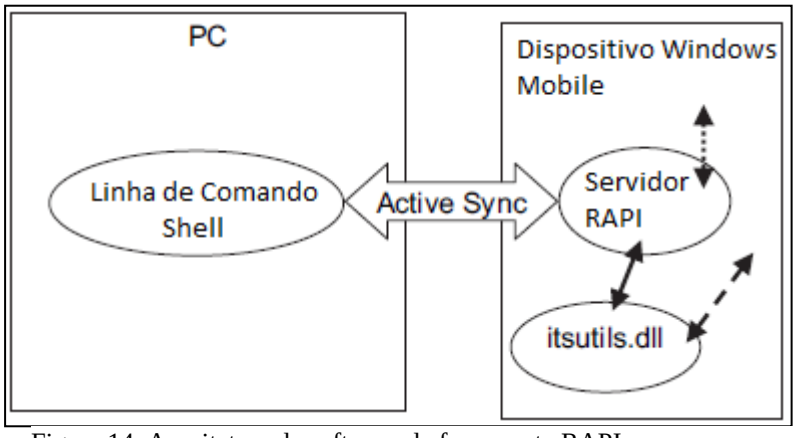


Figura 14. Arquitetura de software da ferramenta RAPI
Fonte: KLAVER, C. (2010).

A seguir estão listadas as aplicações deste eficiente conjunto e suas funções.

a) pps - analisar processos ativos
b) pdblist - analisar banco de dados
c) pdel - excluir arquivo
d) pdir - lista de diretórios
e) pmkdir - criar um diretório
f) pget - copiar um arquivo
g) preboot - reiniciar o dispositivo
h) pmemdump - cópia do bloco de memória
i) pput – copiar arquivo
j) pregutl - manipular o registro
k) prun – programas em execução
l) dump - hexdump de arquivo local.
m) pdocread – cópia bit a bit da flash ROM
n) psdread - cópia bit a bit do cartão SD no dispositivo
o) psdwrite - escrever para o cartão SD no seu dispositivo
p) psynctime - tempo de sincronização com o PC.

3.3.10 *Mobile Internal Acquisition Tool* (MIAT)

Esta ferramenta foi proposta por Fabio Dellutri, Vittorio Ottaviani e Gianluigi Me, nos anais do Seminário sobre Segurança e sistemas computacionais de alto desempenho, parte da Conferência Internacional sobre computação de alto desempenho e Simulação (HPCS) em 2008. É uma ferramenta *open source* que se centra na aquisição de dados da memória de dispositivos móveis de armazenamento interno. Os dados são copiados para uma memória

externa removível (como SD, mini SD). Tal tarefa é realizada sem a necessidade de conectar o aparelho ao PC (Figura 16). Graças a isso, evita-se o uso de qualquer hardware específico (DELLUTRI; OTTAVIANI; ME, 2008, tradução nossa).

MIAT é uma aplicação de software, que mergulha nas APIs do sistema operacional a fim de obter um acesso somente de leitura para a memória interna do sistema de arquivos. Durante sua execução, o MIAT adquire o sistema de arquivos (sms, contatos, arquivos) para um cartão de memória removível, no final da execução, uma imagem lógica do sistema de arquivos é armazenada no volume de armazenamento removível escolhido (DELLUTRI; OTTAVIANI; ME, 2008, tradução nossa).

Segundo Distefano e Me (2008), o MIAT é uma ferramenta representada pelo paralelismo, podendo ser usada para apreender n smartphones, simultaneamente, utilizando *n* cartões de memória. De fato, a partir da estação de trabalho forense pode-se remotamente adquirir os dados de dispositivo por vez. Por sua vez também pode ser espelhado em um número de cartões de memória para adquirir a imagem de vários aparelhos em paralelo. Isso reduz drasticamente o tempo de aquisição total, quando o número do dispositivo apreendidos é consideravelmente maior.

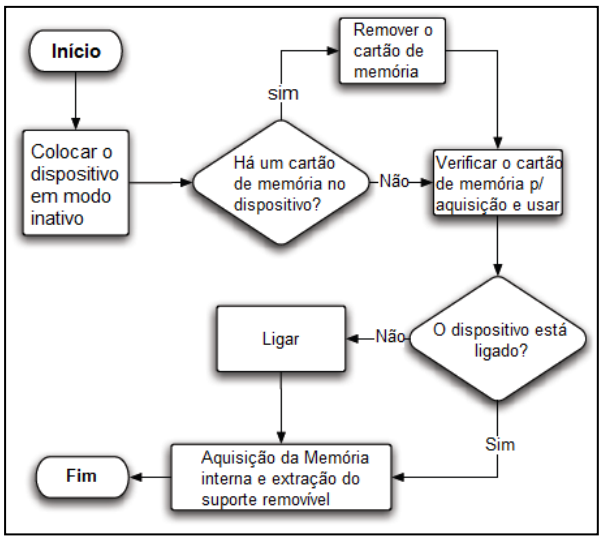


Figura 15. Dados do fluxo de trabalho.
Fonte: DELLUTRI, F.; OTTAVIANI, V.; ME, G. (2008).

MIAT pode ser definida como auto executável, para evitar iniciar aplicativos como *fexplore.exe*, navegar no sistema de arquivos e iniciar o aplicativo de aquisição, na verdade, é importante para que seja executado como poucas aplicações, para evitar problemas de bloqueio e alterações no sistema de arquivos desencadeado por outros processos. Esta ferramenta executa um *hash* de cada arquivo antes e depois da cópia, para garantir a integridade da imagem adquirida. O relatório contendo os *hashes* do arquivo é salvo em um arquivo de log (DELLUTRI; OTTAVIANI; ME, 2008, tradução nossa).

Os dados armazenados no cartão de memória original podem ser adquiridos por meio de um leitor de cartões MMC ou SD (USB ou integrado) e uma ferramenta de fluxo de bytes de imagens: dados binários são lidos a partir da fonte, em seguida, armazenado como um arquivo de imagem, que representa todos os únicos bytes, incluindo os metadados do sistema de arquivo (DISTEFANO; ME, 2008, tradução nossa).

Depois disso, é possível analisar a tabela de alocação de arquivo para recuperar dados apagados. Depois da aquisição dos dados da memória interna, o cartão SIM pode ser removido e analisado com ferramentas específicas.

3.3.10.1 Detalhes da Implementação

O aplicativo foi desenvolvido usando o C++ nativo, cumprindo a exigência de ser uma ferramenta executada a partir de um cartão de memória externo, sem a necessidade de um ambiente de execução pré-instalado (como máquina virtual Java), nem a necessidade de instalar a ferramenta no dispositivo (DISTEFANO; ME, 2008, tradução nossa). O aplicativo é executado em modo autônomo e não requer qualquer *DLL* de terceiros.

Uma vez que a ferramenta usa a APIs padrão do Windows Mobile para acessar o sistema de arquivos (como abrir, ler e escrever, e copiar os ficheiros), pensando na

possibilidade de que essas APIs não mudarão com futuras versões do sistema operacional, sendo assim a compatibilidade com o futuro pode ser assegurada. No algoritmo apresentado na Figura 16, está representado o pseudocódigo do processo de aquisição, que começa após a aplicação principal matar todos os outros processos não vitais em execução (DELLUTRI; OTTAVIANI; ME, 2008, tradução nossa).

```
Input: A path p.
Output: none.

for all objects obj (files and directories) in p do
  if obj is a directory then
    Create a directory named p in the SD Card
    Recursively call Seizure(p/obj)
  else if obj is a file then
    Compute MD5 hash of obj
    Copy obj in path p on the SD Card
    if obj has not been copied then
      Access to obj with CEDB APIs
      if obj could be accessed then
        recreate a similar database in path p on the
        SD Card
      end if
    end if
    Compute MD5 hash of the copied obj on the SD
    Card
  end if
end for
```

Figura 16. Algoritmo de aquisição
Fonte: DELLUTRI, F.; OTTAVIANI, V.; ME, G. (2008).

Tal algoritmo executa duas tarefas principais:

a) a tarefa de cópia, que copia todos os arquivos da memória interna do dispositivo no cartão de memória;

b) a tarefa de *hash*, o que garante a integridade dos arquivos copiados e permite descobrir quais arquivos foram modificados durante o processo de aquisição.

3.3.11 Interpretação dos Arquivos e Dados

As ferramentas forense para Windows Mobile têm sido desenvolvidas para interpretar algumas informações no arquivo *cemail.vol*. Por exemplo, a Figura 17 a seguir mostra os dados do arquivo *cemail.vol* em um dispositivo Samsung i607 (Blackjack), interpretados pela ferramenta XACT. A lista de catálogo no canto inferior esquerdo mostra itens recuperáveis, incluindo mensagens SMS. Detalhes do texto selecionado, mensagens são exibidas no painel nó no canto inferior direito. No canto superior direito, a mesma informação no arquivo *cemail.vol* é mostrada em ambos os formatos hexadecimal e ASCII.

DGande parte do texto em *cemail.vol* é ASCII, incluindo texto SMS. Desde que os registros excluídos não sejam removidos do arquivo *cemail.vol* imediatamente, é aconselhável examinar o arquivos cemail.vol em um *hexviewer*.

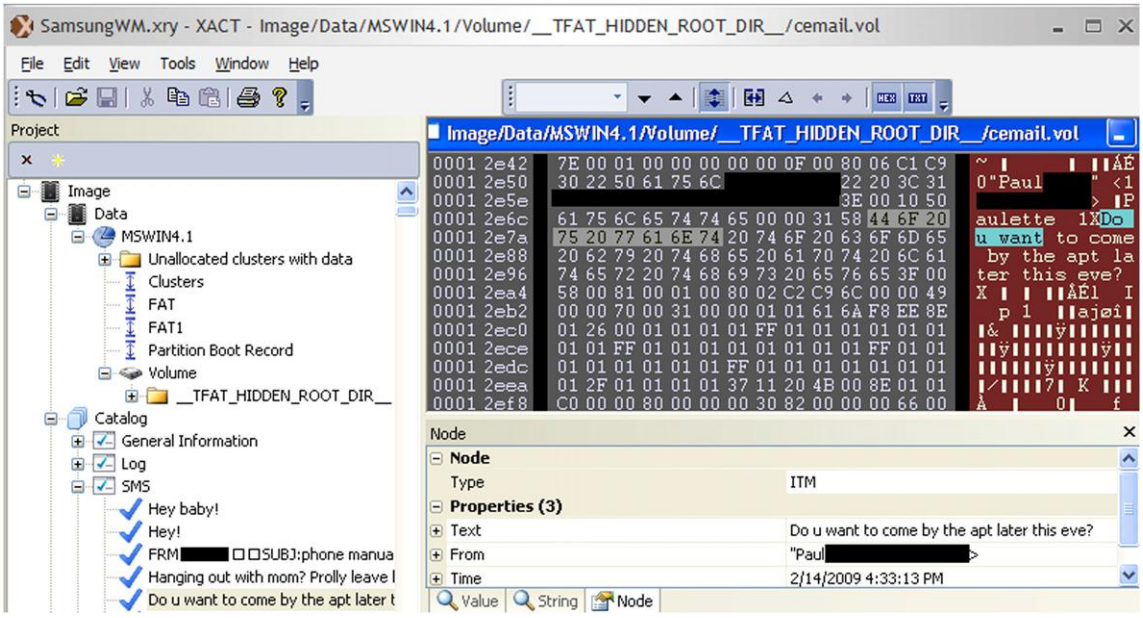


Figura 17. XACT mostrando os dados do arquivo *cemail.vol*.
Fonte: CASEY, E.; BANN, M.; DOYLE, J. (2010).

O registro no Windows Mobile contém vários detalhes sobre a configuração e uso de um dispositivo. Possui uma estrutura hierárquica semelhante à de outros sistemas

operacionais da Microsoft, como mostra a Figura 18, usando o *Microsoft Remote Registry Editor*. O Sistema de Registro contém informações tais como das ligações à rede. Por exemplo, informações sobre recentes ligações a pontos de acesso Wi-Fi, está registrado sob a chave "HKLM\Comm\ConnMgr\Providers". O registro do usuário contém informações associadas a um perfil de usuário em particular no dispositivo, tais como dados de contactos inseridos pelo proprietário do aparelho, como mostra a Figura 19.

Exemplos de outras chaves úteis do registro do usuário estão listados na Tabela 6.

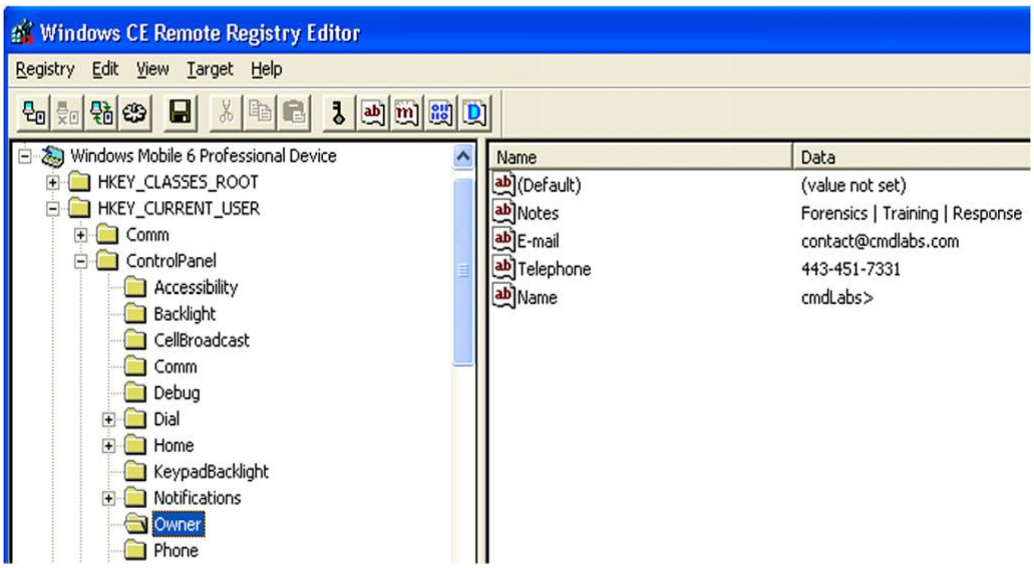


Figura 18. Valores de registro em um dispositivo.
Fonte: CASEY, E.; BANN, M.; DOYLE, J. (2010).

Tabela 6. Tabela de registro de usuários em dispositivo Windows Mobile

Chaves de Registro	**Descrição**
HKCU\ControlPanel\Owner	Detalhes de contatos inseridos pelo usuário
HKCU\System\State\Shell	Itens recentemente usados
HKCU\Software\Microsoft\pMSN\SavedUsers	Identificação do Windows Live
HKCU\ControlPanel\Home\CurBgImageName	Imagem de fundo da tela
HKCU\Comm\EAPOL\Config	Informações de ponto de acesso Wi-Fi

Fonte: CASEY, E.; BANN, M.; DOYLE, J. (2010).

Quando mensagens MMS e de correio eletrônico são recebidas e abertas, ou são criadas e enviadas, em um dispositivo Windows Mobile, artefatos de algumas dessas tarefas são criados. Esses artefatos podem ser úteis para os analistas forenses, porque indicam quando

as mensagens específicas foram criadas ou vistas no dispositivo, até mesmo depois que a mensagem original foi apagada. Além disso, quando se trata de mensagens apagadas, artefatos associados podem permanecer no aparelho por tempo indeterminado e podem conter dados associados com a mensagem original.

Os detalhes de cabeçalho de mensagens de E-mail, incluindo de quem enviou, para quem enviou, o assunto e o nome do anexo (se tiver), são armazenados no arquivo *cemail.vol*. Quando essas mensagens são abertas em um dispositivo Windows Mobile, arquivos ".mpb" são criados na pasta "\Windows\Messaging" com o conteúdo da mensagem. Além disso, quando os anexos de e-mail são abertos em um dispositivo, arquivos ".att" são criados na pasta "\Windows\Messaging\Attachments".

Dados de mensagens SMS/MMS vistas são armazenados em "\Windows\Messaging" nos arquivos ".mpb", podem incluir restos de itens que foram excluídos do arquivo *cemail.vol*. A Figura 19 mostra um arquivo ".mpb" associado a uma mensagem MMS em um dispositivo Samsung i607 (Blackjack), com a criação de um arquivo que com contém a data e hora, indicando que a mensagem foi aberta no dia 5 de dezembro de 2009. Este arquivo inclui uma fotografia digital com informações de cabeçalho embutidas, mostrando que ela foi tirada com um Blackberry no dia 30 de novembro de 2009. O mensagem original recebida está associada ao arquivo ".mpb" excluído.

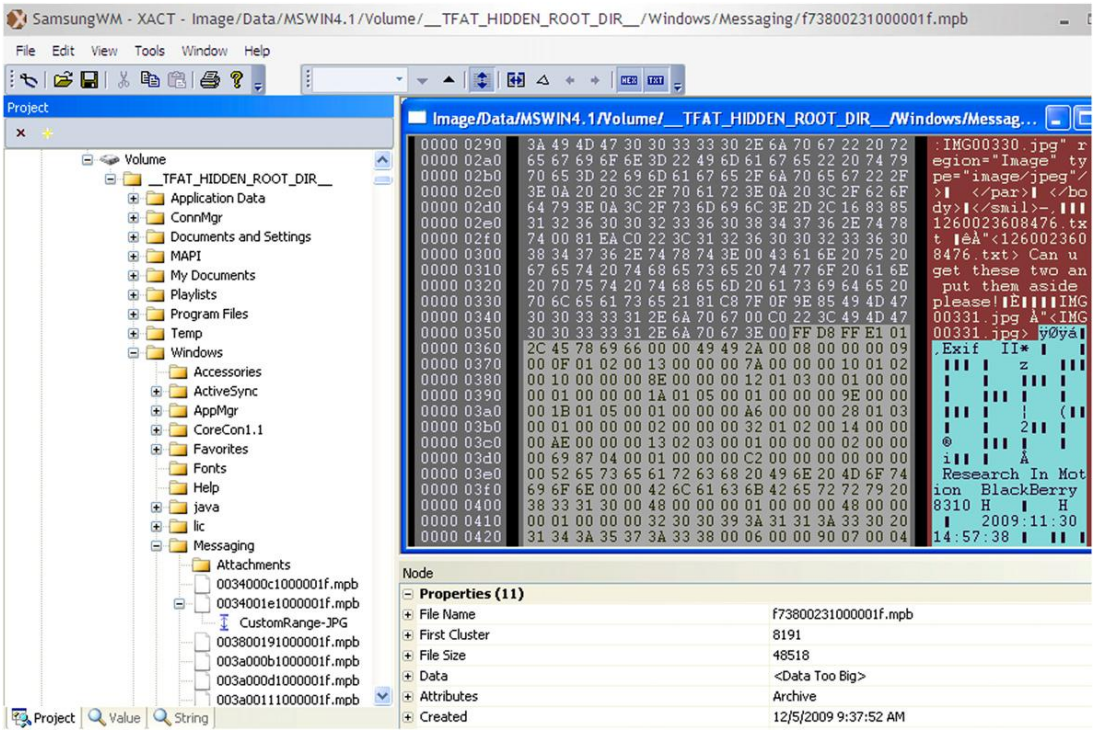


Figura 19. Conteúdo da mensagem em um dispositivo Windows Mobile que contém uma fotografia digital embutida com detalhes de cabeçalho de um Blackberry.
Fonte: CASEY, E.; BANN, M.; DOYLE, J. (2010).

O identificador de objeto (OID - *Object Identifier*) de uma determinada mensagem pode ser usado para associar as entradas no "*cemail.vol*" com o arquivo ".mpb" correspondente na pasta "\Windows\Messaging". Por exemplo, o conteúdo associado com a mensagem de exemplo listadas no parágrafo anterior é armazenado em "\Windows\Messaging\ EA3C00071000001f.mpb", onde o nome do arquivo começa com a mensagem OID (0xEA3C0007). Os últimos 8 caracteres de um arquivo ".mpb " definem o valor de marca de propriedade da Microsoft para o arquivo, que neste caso é o texto completo da mensagem original (MICROSOFT, 2008).

Alguns dispositivos também têm uma pasta "\My Documents\UAContents", que contém os restos de mensagens enviadas. Esta pasta contém arquivos ".dat" com cópias de imagens enviadas via MMS, mesmo depois que a mensagem original foi apagada. A Figura 20 mostra o conteúdo de um arquivo "\My Documents\UAContents\ 45215.dat" que inclui uma fotografia digital que foi tirada usando um HTC S620 (Dash) e enviada em uma

mensagem MMS. A criação do selo de data e hora presente neste arquivo "*.dat*" mostra quando a mensagem MMS foi criada. Detalhes adicionais sobre mensagens MMS enviadas e recebidas são gravados em arquivos de texto na pasta "MyDocuments\UAContents\MMS Log".

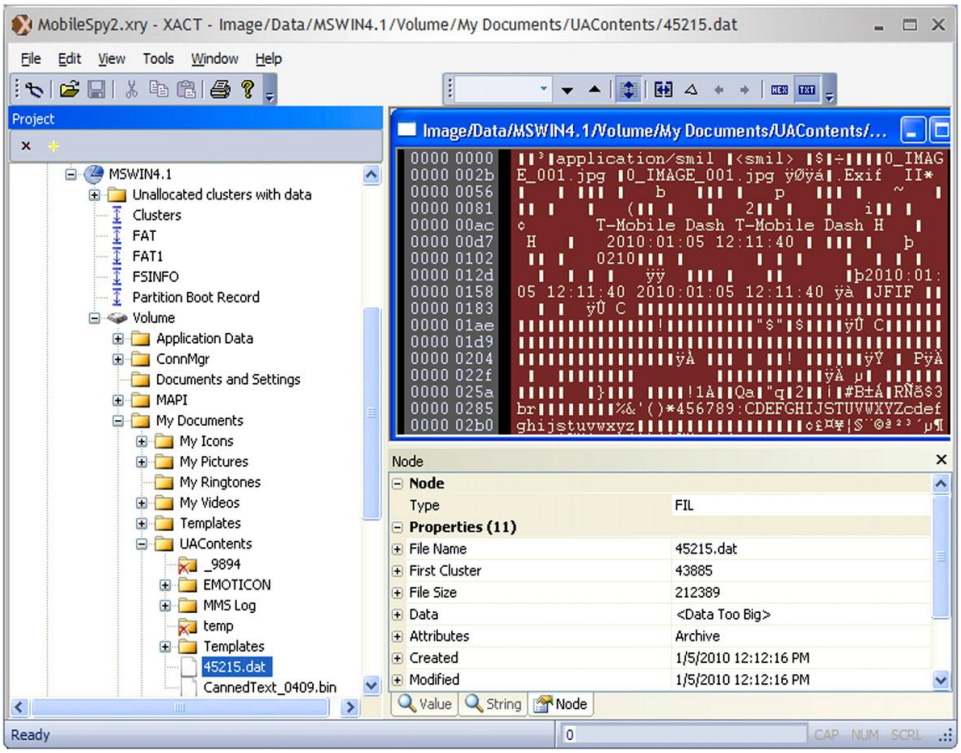


Figura 20. Exemplo de um arquivo "*.dat*" contendo dados associados a uma mensagem MMS enviada.
Fonte: CASEY, E.; BANN, M.; DOYLE, J. (2010).

O surgimento de programas que podem monitorar as atividades remotamente em dispositivo Windows Mobile tem levantado preocupações de privacidade e segurança em governos e empresas. O *MobileSpy* e *Flexispy*, são dois programas, que podem ser instalados em um dispositivo Windows Mobile para permitir que um indivíduo remotamente possa monitorar as atividades dos usuários, como SMS e as conversas de áudio. Esses programas enviam informações a partir do dispositivo móvel para um servidor Web onde o indivíduo remotamente pode revisar as informações coletadas, como mostrado na Figura 21.

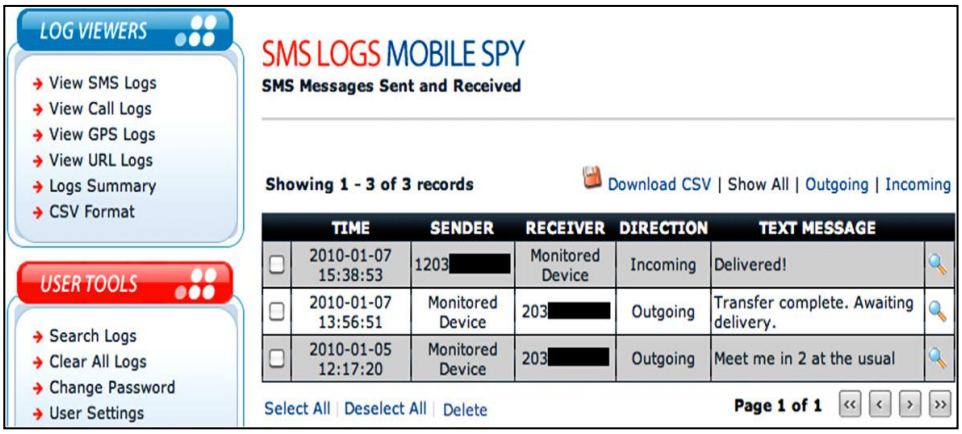


Figura 21. Web site do MobileSpy mostrando o tráfego de SMS em um dispositivo monitorado.
Fonte: CASEY, E.; BANN, M.; DOYLE, J. (2010).

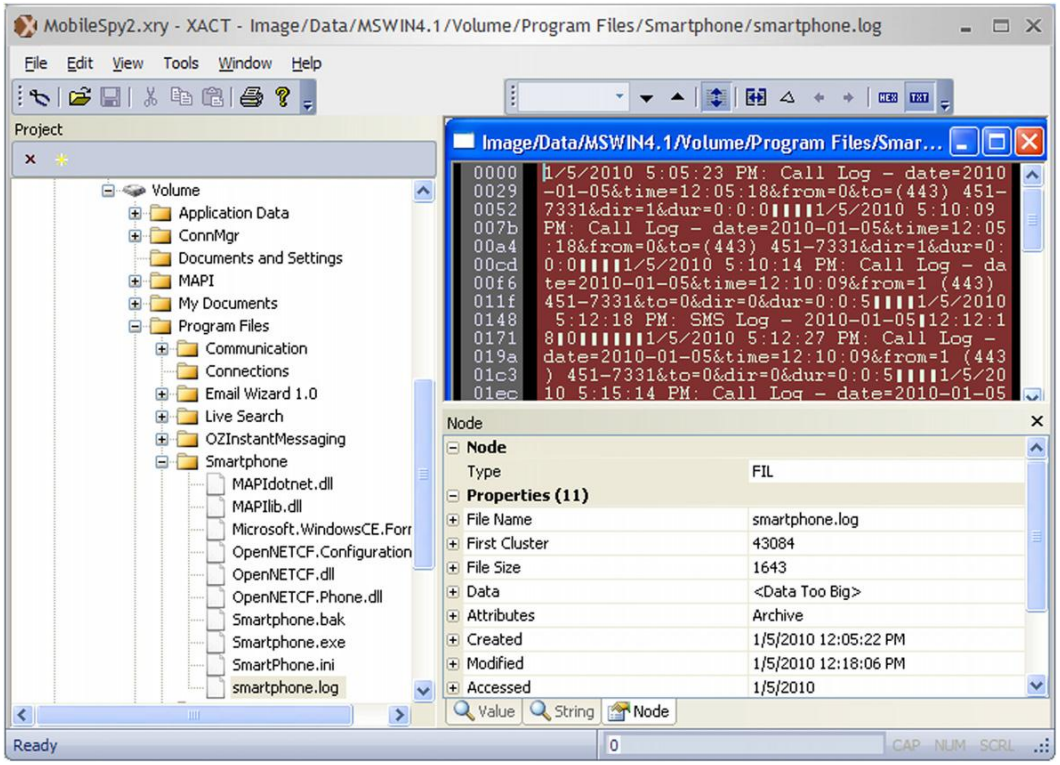


Figura 22. ProgamaMobileSpy instalado em “ProgramFiles\Applications\Smartphone” com arquivo “*smartphone.log*” que grava as atividades no dispositivo**.**
Fonte: CASEY, E.; BANN, M.; DOYLE, J. (2010).

A maioria dos usuários não nota que tal programa está sendo executado em seu dispositivo. Embora o processo *MobileSpy* (Smartphone.exe) pode ser visto rodando na memória do dispositivo usando o *Remote Process Viewer*, ele não aparece no Gerenciador de Tarefas. No entanto, esses programas deixam vestígios suficientes que podem ser detectados

por analistas forenses. A análise forense em dispositivo Windows Mobile com o Mobile Spy instalado revela traços do sistema de arquivo e registro. Por exemplo, o programa MobileSpy é colocado na pasta “Program Files\Applications\Smartphone”. Como mostrado na Figura 22, esta pasta contém um arquivo “*smartphone.log*” que mantém um registro das atividades que foram monitorados pelo programa MobileSpy.

Em versões anteriores do MobileSpy, o nome de usuário e senha para autenticação entre o dispositivo e o servidor Web estavam armazenados no registro em texto simples (FOGIE, 2007, tradução nossa). Versões posteriores protegem o usuário e senha, mas ainda podem ser obtidas pelo dumping da memória do processo “Smartphone.exe”.

3.3.12 Hardware Específico

O campo da forense digital tem se tornado cada vez mais amplo. Os peritos em computação forense precisam lidar com diversos tipos de dispositivos para análise (CASEY; BANN; DOYLE, 2010, tradução nossa). Visto que o foco deste trabalho é voltado para dispositivos PDA, neste capítulo apresentar-se-á alguns equipamentos específicos para análise forense em dispositivos móveis, desenvolvidos por empresas como a *Micro Systemation*, *Paraben Corporation*, *Cellebrite*. Pelo alto custo dos mesmos, não foram usados no desenvolvimento deste trabalho, apenas serão apresentados como alternativa para resposta a incidentes, no caso do perito forense precisar fazer a análise no local do crime.

3.3.12.1 XRY Complete

É um sistema móvel forense “tudo em um” da Micro Systemation; combinação das soluções lógicas e físicas em um pacote, que permite aos investigadores o acesso completo a todos os métodos possíveis para recuperar dados de um dispositivo móvel.

Este equipamento tem a solução baseada em software, com todo o hardware necessário para recuperar dados de dispositivos móveis de forma segura. Com ela consegue-se ir mais fundo em um dispositivo móvel para recuperar dados vitais. Com uma combinação de ferramentas de análise lógica e física disponível com suporte completo (Figura 23).

Figura 23. XRY, kit completo
Fonte: http://www.msab.com/xry/xry-complete

3.3.12.2 Mobile Field Kit

Mobile Field Kit é uma solução forense totalmente portátil, desenvolvido pela empresa *Paraben Corporation*. O kit inclui tudo que se precisa para realizar uma análise forense digital em mais de 4.000 telefones celulares, PDA e aparelhos de GPS em qualquer lugar, a qualquer momento.

3.3.12.3 Cellebrite UFED

É um equipamento forense autônomo, pronto para uso no campo ou no laboratório. O sistema UFED extrai informações vitais de 95% de todos os telefones celulares no mercado hoje, incluindo smartphone e PDA (Palm OS, Microsoft, Blackberry, Symbian, iPhone e Google Android). Simples de usar, mesmo no campo, sem necessidade de PC, o UFED pode facilmente armazenar centenas de listas telefônicas e itens de conteúdo em um cartão SD ou flash drive USB, suportando várias interfaces de dispositivo, incluindo serial, USB, infravermelho e Bluetooth. O sistema UFED Cellebrite vem completo com um aplicativo de análise e relatório para o PC. Podem ser gerados registros concisos e fáceis de analisar nos formatos HTML, XLS, CSV e XML, fornecendo resultados organizados para uso como referência e no tribunal (Figura 24).

Figura 24. Cellebrite UFED
Fonte: http://www.cellebrite.com/

3.4 IMPORTÂNCIA DA PERÍCIA DIGITAL EM PDA

Apesar de seu pequeno tamanho, os dispositivos PDA com Windows Mobile podem conter quantidades substanciais de informações sobre seus usuários, inclusive com

quem eles se comunicam e o que eles fazem em determinados momentos. Embora haja aspectos destes dispositivos que são familiares para os analistas forenses, há variações suficientes para tornar a investigação forense em dispositivos PDA com Windows Mobile uma disciplina distinta, com seus próprios instrumentos e técnicas originais (CASEY; BANN; DOYLE, 2010, tradução nossa).

Como os dispositivos PDA com Windows Mobile tornaram-se mais prevalentes, existe uma necessidade crescente de analistas forense que poderão adquirir evidência destes dispositivos, e examinar seu conteúdo. Há também uma necessidade de mais investigação e desenvolvimento para melhorar a capacidade de extrair informações a partir destes, incluindo mais dados apagados (JANSEN; AYERS, 2004, tradução nossa).

Um novo modelo de processo judicial foi proposto, focando exclusivamente as questões relacionadas com investigação forense em dispositivos PDA com Windows Mobile. Este modelo pode ser um passo para superar a lacuna entre os modelos de aplicação da lei e modelos de investigação digital (JANSEN; AYERS, 2004, tradução nossa). O conjunto de atividades proposto no modelo não está completo e há uma margem considerável de trabalho no futuro. Embora o modelo funcione como um padrão para a família Windows Mobile, procedimentos adicionais são necessários para sistematizá-lo para toda a família de PDA, que inclui dispositivos Palm OS, Android OS, iOS, Blackberry e Symbian OS.

Mas para tal, em um modelo genérico quando se chega à fase de coleta de evidências voláteis, os procedimentos de aquisição de memória serão diferentes dependendo do sistema operacional (CASEY; BANN; DOYLE, 2010, tradução nossa).

Um trabalho adicional deve ser feito para se certificar de que o modelo pode ser aplicado à outra família de dispositivos eletrônicos digitais, incluindo leitores de música portáteis, câmeras digitais, telefones celulares, dispositivos removíveis de armazenamento de

dados e assim por diante. No entanto, a adição de novos procedimentos pode tornar este modelo desajeitado.

O modelo precisa ser testado para sua praticidade. Não há um método simples para testar o modelo. A aplicação do modelo em diferentes contextos deve ser estudada para verificar se este é um quadro de referência geral. O modelo precisa ser amplamente avaliado por especialistas forense e autoridades policiais em diversas partes do mundo para o aperfeiçoamento dos processos. A tecnologia associada com dispositivos portáteis está mudando drasticamente a cada dia. Este modelo é restrito à atual gama de produtos. Como mais e mais recursos são incorporados nestes dispositivos, no futuro os desafios para o investigador forense também aumentará. Assim, o modelo precisa ser constantemente revisto e procedimentos adicionais precisam ser adicionados quando necessário.

4 TRABALHOS CORRELATOS

Ao longo dos estudos com o objetivo de concluir esta pesquisa, seja na proposta ou no procedimento do desenvolvimento, foram analisados alguns trabalhos com propósitos semelhantes, porém com seu foco virado para outras áreas de perícia forense aplicada à informática. Abaixo é feita a descrição de alguns trabalhos escolhidos, envolvendo a perícia forense computacional.

4.1 PERÍCIA FORENSE APLICADA À INFORMÁTICA

Este trabalho é uma monografia de Pós – Graduação “Latu Sensu” que foi apresentado por: Andrey Rodrigues de Freitas, curso de ciência da computação, pela Universidade da IBPI, no ano de 2003, afim de obtenção do titulo de Pós-Graduando, sob orientação do Prof. Msc. Duval Costa.

O assunto tratado neste trabalho possibilitou um vasto campo para estudo e pesquisas, desta forma com sua modesta abrangência, este trabalho pretendeu servir como motivação ao leitor para busca de novos conhecimentos no campo da perícia forense aplicada à informática. Não houve a pretensão de esgotar o assunto, mas sim fornecer ao leitor um texto condensado reunindo conceitos fundamentais ao entendimento dos termos relacionados.

Contou com detalhes sobre o processo de perícia forense aplicada à informática e a importância de seguir procedimentos específicos imediatamente depois de um crime por computador.

4.2 ANÁLISE FORENSE: ESTUDO TEÓRICO E PRÁTICO

Este trabalho foi apresentado por Daniel Dalalana Bertoglio, curso de ciência da computação, pela Universidade Feevale no ano de 2008, como Trabalho de Conclusão do Curso, sob orientação do Prof. Msc. Eduardo Leivas Bastos.

Este trabalho teve como objetivo o estudo de definições e características da análise forense computacional, apresentando suas formas e métodos. Além disso, um experimento prático foi realizado envolvendo duas ferramentas de análise para ratificar a pesquisa e avaliar as formas de exame ressaltadas.

As etapas de todo o processo da forense, citadas neste trabalho, representam importantes ações a serem tomadas durante a execução da investigação. Elas seguem um padrão de metodologia que é utilizado no contexto geral de um inquérito, e os demais critérios são adaptados por cada perito, a fim de qualificar os procedimentos.

4.3 ANÁLISE PERICIAL EM SISTEMA OPERACIONAL MS-WINDOWS 2000

Esta monografia foi julgada adequada para obtenção do título de Especialista, e aprovada em sua forma final pela Coordenação do Curso de Especialização em Redes de Computadores e Comunicação de Dados, do Departamento de Computação da Universidade Estadual de Londrina. Foi apresentado por: Wagner de Paula Rodrigues, curso de ciência da computação, pela Universidade da Londrina, no ano de 2004, afim de obtenção do titulo de Especialista, sob orientação do Prof. Dr. Alan Salvany Felinto.

Devido aos inúmeros tipos de ataques sofridos em equipamentos ligados à Internet, sejam eles vindos de rede interna ou externa, faz-se necessário preparar o ambiente

para que possa ser realizada a perícia em caso de ataques bem sucedidos, para que seja possível em uma segunda fase, realizar uma auditoria em um sistema-alvo.

Este trabalho teve como objetivo apresentar algumas informações para serem utilizadas na criação deste ambiente formal, e também algumas ferramentas que possibilitem a realização de auditoria. Não forma alguma não se esgotou a abordagem para este item, mas sim reuniu-se alguns dos conceitos disponíveis e permite o entendimento dos mesmos.

Com este trabalho foi possível avaliar a gama de possibilidades de busca de informações para resposta a incidentes, bem como para auditoria em sistemas computacionais.

4.4 BOAS PRÁTICAS PARA PERÍCIA FORENSE

Este trabalho é uma monografia apresentada à disciplina de Trabalho de Graduação da Faculdade de Jaguariúna que foi apresentado por: Daniel Moraes da Costa, curso de ciência da computação, pela Universidade de Faguariúna, no ano de 2008, como exigência parcial para conclusão do curso de graduação, sob orientação do Prof. Msc. Sílvio Petroli Neto.

Com a evolução das tecnologias e o uso cada vez maior da informática na sociedade, os crimes também atualmente fazem uso desta tecnologia. A cada dia torna-se mais primordial a análise de computadores pela perícia forense computacional, já que muitos criminosos utilizam recursos de criptografia como métodos anti-forenses visando assim retardar e até mesmo impedir a investigação de um equipamento. Este trabalho objetivou demonstrar a possibilidade ou não de se obter o conteúdo da memória do equipamento no momento da apreensão baseado em metodologias de pericia convencional como a balística forense e a papiloscopia forense onde as provas são manuseadas para se obter a veracidade

dos fatos, ou seja, tal fato só é permitido devido à metodologia poder ser comprovada e aceita perante um tribunal.

Foi igualmente mostrado neste trabalho que existem ferramentas que tornam possível a coleta dos dados contidos na memória de um dispositivo, porém para que a evidência seja aceita em um tribunal como prova válida de um crime é necessário que o procedimento desde sua coleta até sua perícia não tenha falhas. Para isso o profissional que realizar a perícia deve estar certo de que o procedimento realizado é o mais adequado para cada caso. Ainda para contribuir muito para que esta evidência seja aceita existe a Ata Notarial, um recurso que muitas vezes é esquecido pelos profissionais, por exemplo, em um caso que envolva um risco grande de ser invalidado durante o processo de coleta das evidências.

4.5 PROCEDIMENTOS COMPUTACIONAIS NO AUXÍLIO À PERÍCIA FORENSE APLICADA EM WEB BROWSERS

Este trabalho foi apresentado por Sidney Roberto da Silva Webba, curso de ciência da computação, pela Universidade do Extremo Sul Catarinense, no ano de 2010, como Trabalho de Conclusão do Curso, para obtenção do grau de Bacharel, sob orientação do Prof. Msc. Paulo João Martins.

Este trabalho teve como objetivo analisar e aplicar os procedimentos de perícia forense computacional, com foco na coleta e análise de evidências em web browsers, bem como, contribuir socialmente aumentando o leque de pesquisas sobre o tema. A elaboração de um estudo de caso fictício simulando a condução de uma pericia forense computacional na presente universidade, utilizando a metodologia SOP aplicando as suas 6 etapas: autorização e preparação, identificação, coleta e preservação, exame e análise, documentação e reconstrução da cena do crime. Conclui-se que se conseguiu estudar e aplicar os conceitos de

pericia forense computacional, analisando com sucesso muitos dos arquivos de cache, cookies, histórico de navegação e outros, dos browsers Internet Explorer e Firefox, utilizando-se das ferramentas Pasco, Galleta, Web Historian, Firefox3Extractor, Mozilla Cache View e PasswordFox.

Contou com detalhes sobre o processo de perícia forense aplicada à informática e a importância de seguir procedimentos específicos imediatamente depois de um crime por computador.

5 ANÁLISE FORENSE EM PDA COM WINDOWS MOBILE

A tecnologia muitas vezes provou ser uma faca de dois gumes, que gera o crime e soluciona. Naturalmente dispositivo com Windows Mobile não é exceção e desempenham um papel importante em crimes eletrônicos no futuro. A metodologia e a abordagem são extremamente importantes na investigação forense de tais crimes. O modelo de processo forense para dispositivos com Windows mobile foi desenvolvido com o objetivo de auxiliar os profissionais forenses e de organizações para a criação de políticas e procedimentos adequados.

O objetivo deste documento é informar sobre os recursos, a metodologia e as ferramentas forenses que têm a capacidade de adquirir, analisar e examinar informações em PDA com Windows Mobile. Uma visão geral de cada ferramenta descreve a diversidade funcional e facilidades para a aquisição e análise de evidências contidas nos dispositivos.

Um cenário genérico foi elaborado para espelhar uma situação que geralmente surge durante um caso forense em PDA com Windows Mobile e mídias associadas. O cenário será utilizado para revelar como a metodologia pode ser aplicada, como algumas ferramentas reagem e qual deve ser a postura e atitude do perito forense em determinadas situações. Embora o cenário genérico foi utilizado na análise de ferramentas forense, os procedimentos não são destinados a servir como um teste formal do produto ou como uma avaliação global. Além disso, nenhuma reivindicação foi feita sobre as vantagens comparativas de uma ferramenta contra outra. O documento, ao contrário, oferece uma perspectiva ampla e sondagem sobre o estado da arte de hoje em dia, usando ferramentas forenses para dispositivo PDA com Windows Mobile.

Este documento visa ser usado como um guia para a execução de uma investigação forense ao lidar com novas tecnologias como PDA, ou interpretadas como

consultoria jurídica. Sua finalidade é informar sobre as várias tecnologias e potenciais formas de abordá-las de um ponto de vista legal.

5.1 CASO DE ESTUDO

Neste ponto será apresentado um caso fictício, para demonstrar os passos necessários durante o processo de investigação forense, como segue: no dia 06 de junho de 2011 foi pego no bairro Monte Alegre o Fulano de Tal, suspeito de envolvimento com tráfico de drogas. Segundo o chefe do Setor de Investigação, inspetor senhor Fulano, a prisão foi resultado do mapeamento do tráfico na cidade da Região dos Lagos. Com o suspeito, foi apreendido um dispositivo PDA, que poderá conter evidências de que Fulano de Tal esteja ou não envolvido com o suposto crime mencionado.

A missão do perito neste caso ao tomar posse do dispositivo, é efetuar uma análise pericial do mesmo e usar os procedimentos necessários de formas a extrair o máximo de informação possível, para que possa servir de provas neste suposto caso.

5.2 METODOLOGIA

Esta pesquisa tem como fundamento um estudo de caso fictício, que simula a ocorrência de um caso de suspeita de tráfico de drogas, de formas a se aplicar os conhecimentos e procedimentos necessários quando se trata da ocorrência de um crime, em que se usa um dispositivo digital.

De acordo com Becker (1994), o estudo de caso tem origem com a análise qualitativa de modo detalhado de um determinado contexto ou acontecimento específico e que explica a dinâmica do mesmo. Com este procedimento se conjetura a possibilidade de se

adquirir conhecimento do estudo apresentado, a partir da exploração intensa de caso.

Martins e Theóphilo (2009) afirmam que um estudo de caso:

> "trata-se de uma investigação empírica que pesquisa fenômenos dentro de seu contexto real [...] onde o pesquisador não tem controle sobre eventos e variáveis, buscando apreender a totalidade de uma situação e criativamente descrever, compreender e interpretar a complexidade de um caso concreto. [...] possibilita a penetração na realidade social, não conseguida pela avaliação quantitativa".

Quando se utilizar o Estudo de Caso pode-se envolver situações de estudo de um único ou de vários casos (YIN, 2001, tradução nossa). Ao se analisar que os casos têm características próprias, descarta-se a possibilidade de existência de um modelo específico para estruturação do estudo. Um prosseguimento de práticas metodológicas pode ser usado para orientação, tal como a coleta das evidências, composição, análise, exame e validação dos resultados, conclusões, verificação e relatório (MARTINS; THEÓPHILO, 2009).

Após o cumprimento dos objetivos desta pesquisa, definiu-se que a metodologia de processo forense em PDA com Windows Mobile foi usada durante a realização do caso de estudo, pois ela congrega as práticas metodológicas recomendadas, bem como os princípios e técnicas da ciência forense.

As etapas do modelo proposto estão presentes na Figura 25, apresentada a seguir. A Figura ilustra cada uma das etapas com algumas das ações a serem tomadas no decorrer da perícia.

Figura 25. Etapas do modelo de processo forense em PDA com Windows Mobile

A seguir temos uma explicação detalhada de como cada etapa da modelo foi aplicada neste estudo.

5.2.1 Preparação

Por se tratar de um caso de estudo fictício, não foi necessária a obtenção de autorização ou mandato de busca judicial, para que se realizasse a perícia forense, visto que é um aspecto importante, no respeito aos direitos de privacidade do suspeito. Posteriormente, definiu-se a finalidade da pesquisa, que pretendia provar o caso de estudo criado, compreendendo-se inicialmente a natureza do crime, prepararam-se as ferramentas

necessárias para o padrão de investigações em dispositivos portáteis Windows Mobile e obteve-se uma melhor avaliação sobre as circunstâncias relativas ao crime e fatores técnicos.

Nas investigações envolvendo dispositivos com Windows Mobile há que se levar em conta o fato de que a bateria pode se esgotar antes da coleta de provas. Por isso, preparou-se uma fonte de alimentação padrão para o dispositivo.

Após a preparação minuciosa, o que contribuiu para o aumento da qualidade das provas e minimizou os riscos e ameaças associadas à investigação.

5.2.2 Segurança do Cenário

Outro aspecto que não se precisou levar em conta neste estudo de caso foi a segurança da cena do crime, visto que o dispositivo foi encontrado em posse do suspeito a quando da sua apreensão, descartando a necessidade de haver o protocolo formal para preservar o cenário. Contudo, teve-se o cuidado necessário de formas a preservar a integridade de todas as evidências, deixando-se o dispositivo no estado em que foi encontrado até que a avaliação adequada seja realizada. Esta fase teve um papel importante no processo global de investigação, porque determinou a qualidade das evidências.

5.2.3 Levantamento e Reconhecimento

Esta etapa envolveu um levantamento inicial para avaliar o cenário, identificaram-se as possíveis fontes de evidência e formulou-se o plano de pesquisa apropriado. Avaliou-se o dispositivo, sendo que foi necessária a identificação e realização preliminar de uma entrevista com o suspeito de formas a se ter informações valiosas como: sistema de segurança,

vários aplicativos presentes nos dispositivos, nomes de usuário, senhas e detalhes de criptografia sem violar as leis de competência.

Caso existisse um mandado de busca e fosse necessária a busca por itens que não estão incluídos no respectivo mandado, as devidas alterações deveriam ser feitas para o mandado existente ou um novo deveria ser obtido, incluindo os itens adicionais.

Foi feito um plano inicial para coleta e análise de evidências no final do inquérito com o suspeito.

5.2.4 Documentação do Cenário

Esta etapa envolveu a devida documentação da cena do crime. O dispositivo apreendido foi fotografado (Figura 26), também se verificou que o mesmo foi encontrado desligado, sem a presença do cartão SIM e cartão de memória, suspeitando-se de que o suspeito tenha-se desfeito dos mesmos quando se apercebeu de que já não tinha chances de fuga.

Figura 26. Imagem do dispositivo apreendido.

Foram registradas as seguintes especificações referentes ao dispositivo:

Tabela 7. Especificações técnicas do dispositivo

Marca /Fabricante /Nome Proj. / Modelo	**Software / Kernel**	**Processador**	**Memória**	**Conectividade**	**Redes / Ligações de dados / Interfaces de expansão**
SoftBank	Microsoft Windows Mobile 5.0 para Pocket PC /AKU 2.6.0	*Clock* da CPU: 400 MHz	RAM: SDRAM	Bluetooth 2.0, antena interna	GSM850, GSM900, GSM1800, GSM1900, UMTS800, UMTS850, UMTS1900, UMTS2100
HTC	Windows CE 5.1.195 Build 14989.2.6.0	CPU: Samsung SC32442, 32 bits	64 MB, 48.8MB accessíveis	Wireless: IEEE 802.11b, IEEE 802.11g, 54 Mbit/s	Ligações de Dados: CSD, GPRS, EDGE, UMTS, HSDPA
		Cache L1: 16 Kbits	ROM: Flash EEPROM	IrDA 1.2, 115200bit/s (SIR/CIR)	USB 1.1 (12Mbit/s)
HTC Hermes 200		Núcleo da CPU: ARM920T	ROM: 128 MB, incluindo 57.08MB acessíveis.		microSD, TransFlash, SDIO
HERM200		Conjuntos de Instruções: ARMv4T			

Após o detalhamento de hardware e software foi possível identificar as fontes de evidências digitais, e selecionar as ferramentas que foram usadas, o que constituiu o kit de investigação.

5.2.5 Comunicação

Esta etapa ocorre antes da coleta de evidências. De acordo ao estudo de caso criado, esta foi a fase em que foram bloqueadas todas as outras opções possíveis de

comunicação dos dispositivos. Como o dispositivo estava desligado, alguns recursos de comunicação como Bluetooth ou rede sem fio não poderiam ser visualizados. Contudo, a melhor opção após apreender um dispositivo é isolá-lo, desativando todas as suas capacidades de comunicação.

5.2.6 Coleta das Evidências Voláteis

Como a maioria das evidências envolvendo dispositivos PDA é de natureza volátil, estando presente na memória ROM, tendo em conta que o dispositivo foi encontrando desligado, foram selecionadas ferramentas que permitem a coleta de evidências voláteis, visando manter a integridade das informações. O dispositivo foi levado ao laboratório forense para que a análise do mesmo pudesse ser feita em um ambiente controlado.

A combinação de ferramentas utilizadas para obter os melhores resultados foi a seguinte:

a) MIAT

b) RAPI

c) MOBILedit

d) FTK

Para além destas ferramentas, outros utilitários foram utilizados, tais como: os nativos do sistema operacional como a linha de comandos do Windows, e outros programas como: *Windows Mobile Device Center* (serve para sincronização dos dados entre o computador e o dispositivos com Windows Mobile), *CeRegEditor* (editor de registros para dispositivos com Windows Mobile) também compõem o kit.

Como o dispositivo achado com o suspeito estava desligado não se obtiveram informações referentes aos dados não voláteis, visto que são informações que ficam

armazenadas na memória RAM do dispositivo e têm um ciclo de vida curto, se comparadas com informações armazenadas na memória ROM. Estão informações foram perdidas quando o sistema foi religado, pois o processo de boot fez uma espécie de limpeza na memória principal, para que pudesse carregar uma nova sessão, com novos aplicativos e processos executados.

Surge a necessidade e importância de saber-se o estado atual do dispositivo a quando da apreensão, de formas a evitarem-se maiores comprometimentos. Porque essas informações voláteis podem ser importantes para a investigação. Tais informações armazenadas unicamente na memória RAM normalmente são constituídas de: processos executados, conexões estabelecidas e informações carregadas na memória no momento de sua utilização.

5.2.7 Coleta das Evidências não Voláteis

Depois da análise real do caso, seleção das ferramentas a serem utilizadas, criaram-se as condições para a coleta das evidências voláteis, quer dizer, os dados armazenados na memória flash ROM do dispositivo. Como o dispositivo estava desligado, nesta fase ligou-se o mesmo, porque as ferramentas de aquisição das evidências funcionam apenas com o dispositivo em funcionamento. Antes da coleta propriamente dita, é necessária desbloquear o dispositivo em causa, porque no sistema operacional Windows Mobile, a sua configuração padrão não permite que software não assinado possa ser executado. Contudo, o desbloqueio permitiu que as ferramentas de aquisição, pudessem ser executadas no dispositivo, de formas a coletar informações importantes. Para o desbloqueio do dispositivo, usou o software *CeRegEditor*. Como se trata de um editor de registros para Windows, apenas foi necessário alterar o registro de segurança do dispositivo (Figura 27).

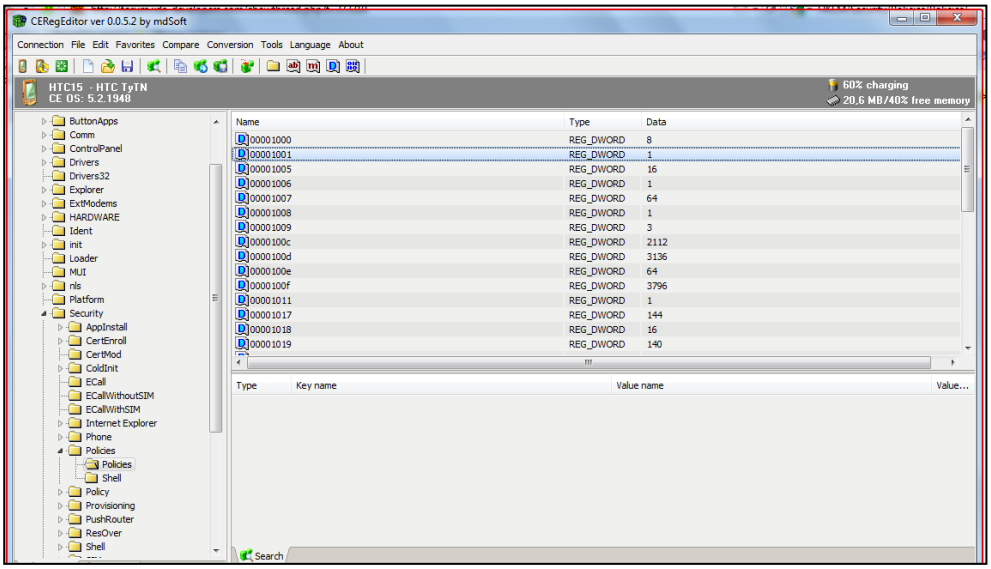


Figura 27. Editor de registros *CeRegEditor*.

Na configuração padrão o registro aparece: HKLM\Security\Policies\Policies "00001001" = DWORD: 2. Alterou o 2 que é padrão por 1, permitindo desse jeito a execução de software não assinado no dispositivo. Após o desbloqueio, fez-se um soft reset para que a alteração fosse efetivada.

Para coleta das evidências não voláteis usaram-se as ferramentas MIAT, MOBILedit e RAPI, que foram explicadas anteriormente.

5.2.7.1 Aquisição das Evidências Usando o MOBILedit

Usou-se o MOBILedit para aquisição lógica, no qual observou-se que o resultado não foi o esperado, acredita-se que o motivo seja o fato de ter-se usado a versão "demo" da ferramenta, o que fez com que muito pouca informação fosse extraída do dispositivo. De realçar que há a necessidade do uso do software de sincronização do dispositivo com o computador (*Windows Mobile Device Center*) para que ela funcione (Figura 28).

Figura 28. Dispositivo sincronizado com o Computador.

Após a conexão do dispositivo com o *MOBILedit versão 5.0*, criou-se um backup do dispositivo para que se preservasse a integridade do mesmo, desta forma a análise das evidências foi feita no backup do dispositivo (Figura 29). Durante o backup notou-se que algumas informações não foram resgatadas com sucesso, impedindo que a aquisição lógica dos dados fosse feita com sucesso (Figura 30).

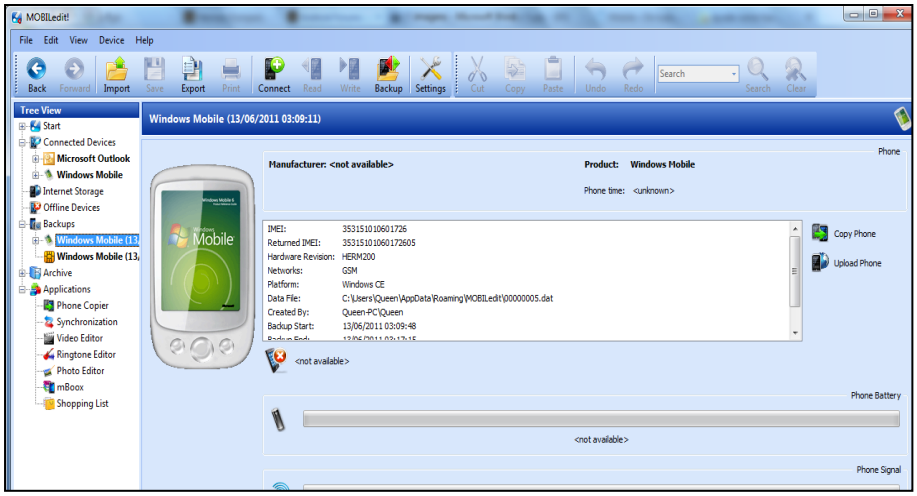


Figura 29. Backup do dispositivo

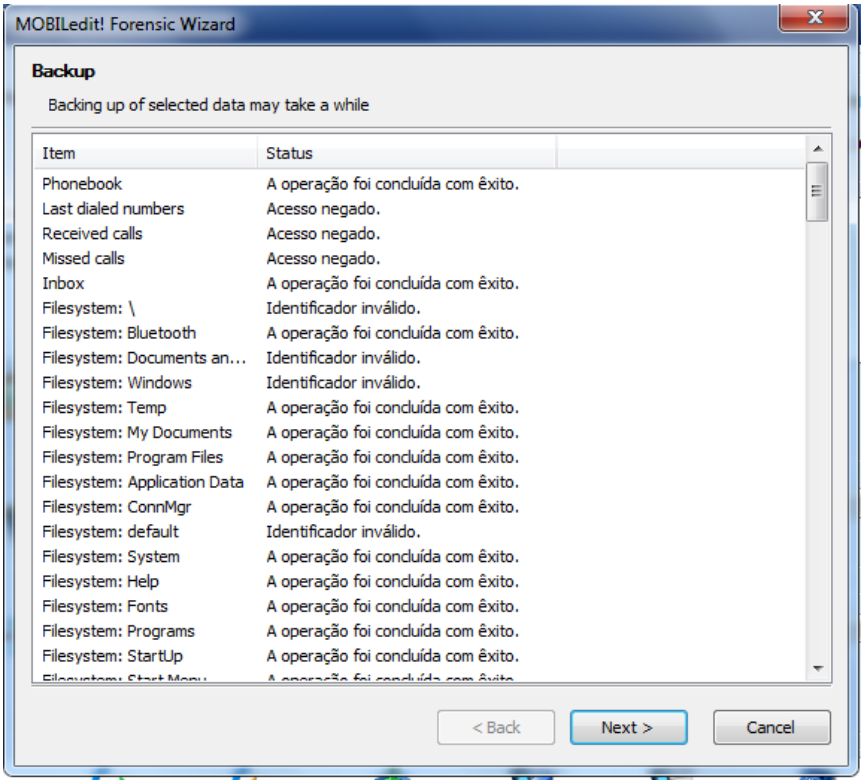


Figura 30. Momento em que se gerava o backup.

5.2.7.2 Aquisição das Evidências Usando o pacote RAPI

Para a coleta usando o pacote de código aberto RAPI, do qual foi usada a ferramenta Itsutils para extrair a memória ROM do dispositivo. Esta ferramenta funciona a base de comandos (prompt), para tal o dispositivo tinha de estar sincronizado com o computador tal como na ferramenta MOBILedit. O componente *pdocread* deste pacote adquiriu mais dados a partir do dispositivo comparando com a ferramenta MOBILedit, visto que ele permitiu fazer uma cópia bit a bit de toda memória ROM. Para o funcionamento desta ferramenta copiou-se todos os arquivos da mesma para o *C:\itsutils*, para ao acessar esta path, os comandos possam ser usados na linha de comandos e os arquivos gerados sejam salvos na pasta *C:\itsutils* (Figura 31).

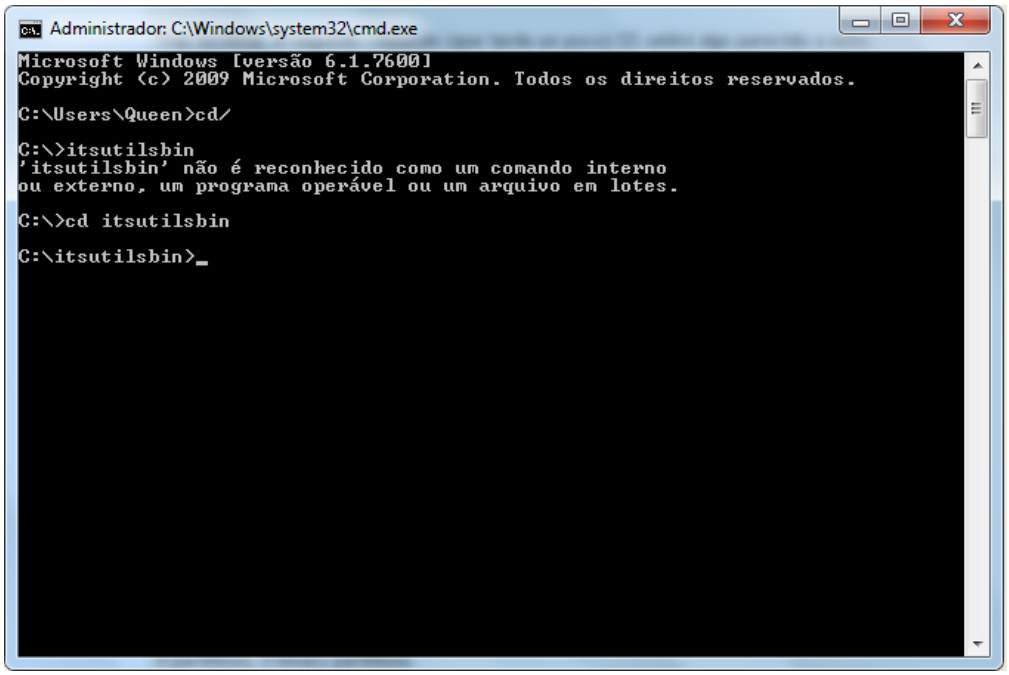


Figura 31. Acessando a pasta *C:\itsutils* por meio do prompt.

Antes da aquisição da memória com do dispositivo, usou-se o comando *pdocread –l*, que permitiu listar a memória ROM completa e cada uma das partições, tal como qual está subdividida no dispositivo e os respectivos tamanhos de cada uma delas (Figura 32).

Podem-se analisar na lista da Figura 32, entradas da referência da memória flash ROM do sistema de aquisição. As entradas subsequentes referem-se aos discos remotos no dispositivo, que são as áreas de armazenamento do sistema e dados, respectivamente.

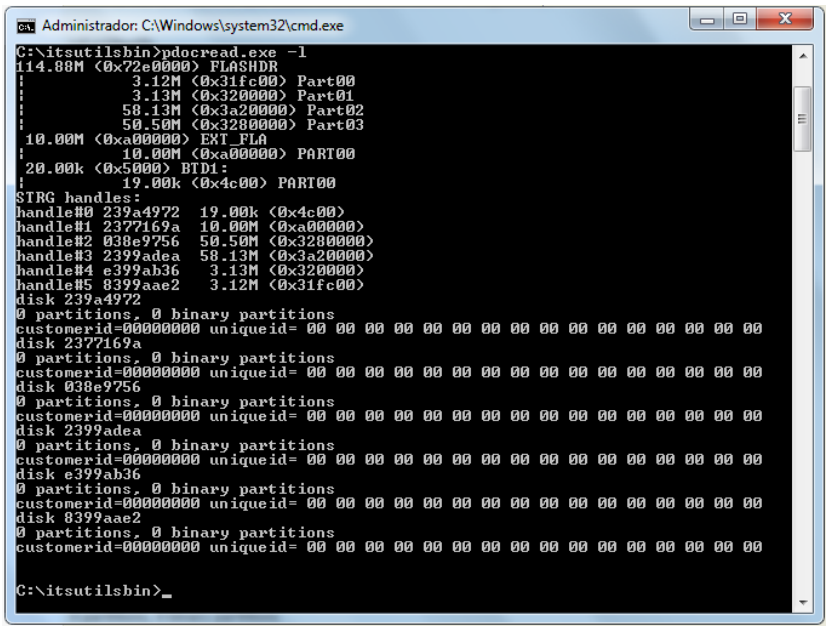


Figura 32. Saída do comando *pdocread* listando todas as partições do dispositivo.

Depois de analisada a memória ROM, fez-se a coleta (imagem bit a bit) de cada uma das partições da memória, no qual se usou o comando *pdocread -w -d FLASHDR -b 0x200 -p Part00 0 0x11f000 Part00.raw*, que permitiu criar uma imagem (.raw) de cada partição da flash ROM do dispositivo (Figura 33). Onde:

a) *-w* – leitura via API do Windows;

b) *-d* – especifica o nome do sistema de armazenamento do dispositivo;

c) FLASHDIR– Nome do sistema de armazenamento;

d) *-b* – especifica o tamanho do setor;

e) *0x200* – tamanho do setor;

f) *-p* – especifica o nome da partição;

g) *0x11f000* – nome da partição;

h) *Part00.raw* – nome da imagem da partição.

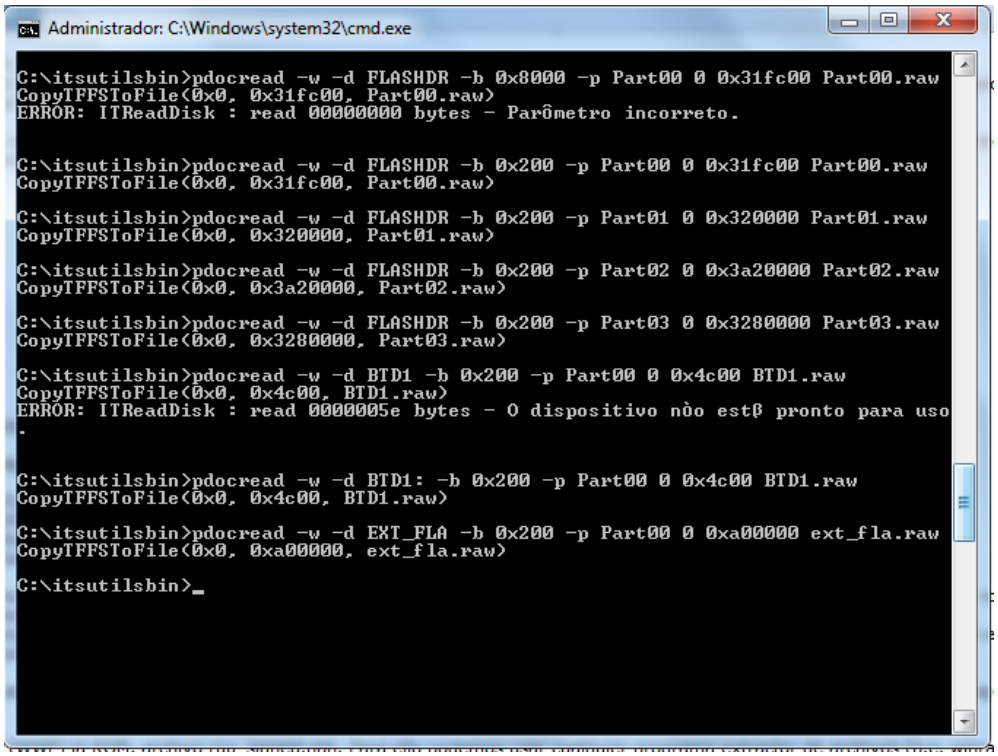


Figura 33. Copiando cada partição da flash ROM.

No uso dos componentes da ferramenta RAPI para aquisição há que ter em conta

determinados aspectos. Ela cria arquivos no dispositivo, que não necessariamente substituem dados, mas tais informações têm de ser reportadas. Especificamente, um arquivo executável chamado "*itsutils.dll*" é copiado para o dispositivo e um log de erro "*itsutils.log*" é criado no dispositivo.

Depois de gerada as imagens da flash ROM do dispositivo usando a ferramenta RAPI, as arquivos gerados estão prontos para serem examinados.

5.2.7.1 Aquisição das Evidências Usando o MIAT

O MIAT é uma ferramenta de código aberto, que tem um algoritmo de aquisição que funciona usando APIs que copiam recursivamente cada entrada do sistema interno de arquivo no cartão de memória, invocando a função *hash* antes e depois da cópia de cada arquivo, permitindo perceber se aconteceram mudanças durante a cópia dos arquivos internos para cartão de memória (Figura 34). Esta tarefa preserva a estrutura de diretórios, copiar arquivos de acordo com sua posição original. A função *hash* calcula o MD5 de cada arquivo encontrado na memória inserido no dispositivo. Os *hashes* são escritos em um arquivo de log e salvos em um ficheiro criado pelo MIAT (*Statistics*), que contém informações sobre cada arquivo copiado da memória, bem como a data em que foram criados e acessados pela última vez (Figura 35).

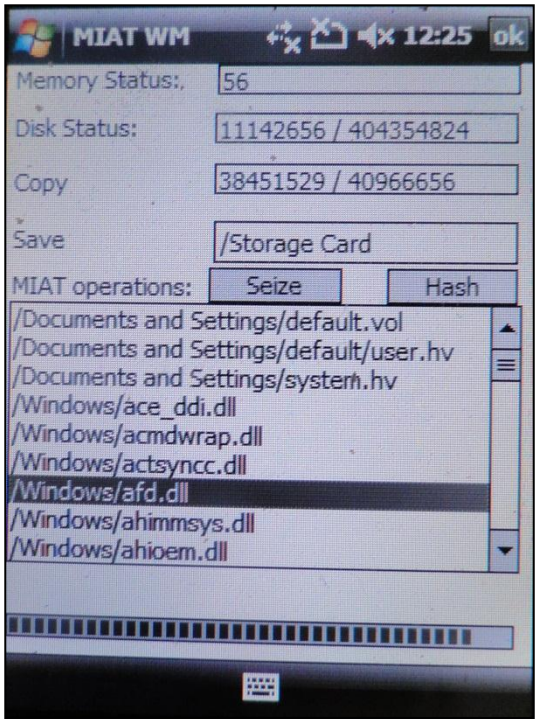


Figura 34. Tela do dispositivo enquanto o MIAT vai fazendo a cópia bit a bit da memória flash ROM.

```
FileSize="13312"  MD5="c338c69749d354312677af1ce55a52a4"
USecDuration="149323" />
<File name="stwater_320_240.jpg"  normal="no" readonly="no"
systemfile="yes" archivefile="no" created="14/06/2010
00:45:56"  accessed="13/06/2010  03:00:00"
modified="14/06/2010  00:45:56"  attribute="6"
FileSize="10623"  MD5="fc9f453c8d3c7b6428ada4b9c8e51961"
USecDuration="111402" />
<File name="ha_skin_cache_p.dat"  normal="no" readonly="no"
systemfile="no" archivefile="yes" created="15/03/2009
20:34:46"  accessed="15/03/2009  03:00:00"
modified="15/03/2009  20:34:46"  attribute="32"
FileSize="21768"  MD5="c7ba16745797cc29d5190394482c1312"
USecDuration="102962" />
<File name="ha_skin_cache_l.dat"  normal="no" readonly="no"
systemfile="no" archivefile="yes" created="16/03/2009
09:08:16"  accessed="16/03/2009  03:00:00"
modified="16/03/2009  09:08:16"  attribute="32"
FileSize="21768"  MD5="63e7a76e1b7343be6a9dba838410b70a"
USecDuration="96084" />
<File name="Customize_CSP.xml"  normal="no" readonly="no"
systemfile="no" archivefile="yes" created="15/03/2009
16:55:58"  accessed="15/03/2009  03:00:00"
modified="15/03/2009  16:55:58"  attribute="32"
FileSize="7490"  MD5="1b792bc78874f474d4e1639f5bd851a6"
USecDuration="95163" />
<File name="stwater_240_320.jpg"  normal="no" readonly="no"
systemfile="yes" archivefile="no" created="14/06/2010
00:45:56"  accessed="13/06/2010  03:00:00"
modified="14/06/2010  00:45:56"  attribute="6"
FileSize="14871"  MD5="5c6a9e6945456ee6ce161a6fc3715a63"
USecDuration="101753" />
```

Figura 35. Arquivo *Hash* criado pela MIAT

Após a com cópia da memória flash ROM do dispositivo, foram encontrados arquivos relevantes, como mostra a tabela a seguir.

Tabela 8. Tabela de arquivos relevantes.

Arquivos		Descrição
Mxip lang.vol, Mxip notify.vol	/	Dados específicos do idioma e armazenamento para as notificações.
Cemail.vol	/	Armazenamento de mensagens de SMS e E-mail.
Pim.vol	/	Gerenciamento de informações pessoais, como agenda de endereços, registro de chamadas, e contatos do cartão SIM.
\Windows\Messaging		Repositório de SMS e mensagens de correio eletrônico, armazenadas nos arquivos "*.mpb*".
\Windows\Profiles		Repositório do histórico do Internet Explorer, bem como arquivos de cache e cookies, incluindo arquivos index.dat.
\Windows\Favorites		Bookmarks do Internet Explorer

5.2.8 Preservação

Após a coleta das evidências, fez uma cópia do cartão de memória que continha os dados coletados do dispositivo. Colocou-se o dispositivo e o cartão de memória em um envelope e posteriormente foram colocados em um saco de evidências, com a devida etiqueta de identificação, de formas a manter-se a integridade, visto que se trata de potenciais fontes de evidências. Posteriormente, a análise e processamento de dados tiveram início.

5.2.9 Exame

Nesta fase fez-se a análise do conteúdo das evidências coletadas e extraíram-se informações, que foram fundamentais para comprovar o caso.

Criou-se uma imagem do cartão de memória usando a ferramenta *Access Data FTK Imager* (anexo C), que continha a cópia dos dados coletados do dispositivo, para que pudesse ser examinado com uma ferramenta apropriada. Depois de gerar a imagem a ferramenta gerou a arquivo em *.xls*, que contém a lista de todos (2514) os arquivos extraídos

da memória do dispositivo, bem como o caminho, a data em foi criado e a última data de modificação (Figura 36). No arquivo também contém o espaço não alocado na memória (Figura 37).

	A	B	C	D	E	F	G
1	Filename	Full Path	Size	Created	Modified	Accessed	Is Deleted
2	[root]	NONAME [FAT16]\[root]\	16384				no
3	VBR	NONAME [FAT16]\VBR	512				no
4	reserved sectors	NONAME [FAT16]\reserved sectors	512				no
5	[unallocated space]	NONAME [FAT16]\[unallocated space]\	0				no
6	file system slack	NONAME [FAT16]\file system slack	32256				no
7	FAT1	NONAME [FAT16]\FAT1	122368				no
8	FAT2	NONAME [FAT16]\FAT2	122368				no
9	MIAT.EXE	NONAME [FAT16]\[root]\MIAT.EXE	1504768	2011-Jun-04 14:20:41.6	2009-Jun-22 14:40:46		no
10	Statistics	NONAME [FAT16]\[root]\Statistics\	32768	2011-Jun-04 14:23:04	2011-Jun-04 14:23:04		no
11	Bluetooth	NONAME [FAT16]\[root]\Bluetooth\	32768	2011-Jun-04 14:23:04	2011-Jun-04 14:23:04		no
12	Documents and Settings	NONAME [FAT16]\[root]\Documents and Settings\	32768	2011-Jun-04 14:23:06	2011-Jun-04 14:23:06		no
13	Windows	NONAME [FAT16]\[root]\Windows\	229376	2011-Jun-04 14:23:06	2011-Jun-04 14:23:06		no
14	Temp	NONAME [FAT16]\[root]\Temp\	32768	2011-Jun-04 17:12:36	2011-Jun-04 17:12:36		no
15	My Documents	NONAME [FAT16]\[root]\My Documents\	32768	2011-Jun-04 17:12:44	2011-Jun-04 17:12:44		no
16	Program Files	NONAME [FAT16]\[root]\Program Files\	32768	2011-Jun-04 17:13:44	2011-Jun-04 17:13:44		no
17	mxip_initdb.vol	NONAME [FAT16]\[root]\mxip_initdb.vol	28672	2008-Jan-15 04:26:00.5	2009-Mar-20 01:27:48		no
18	mxip_notify.vol	NONAME [FAT16]\[root]\mxip_notify.vol	344064	2011-Jun-04 17:13:48	2011-Jun-04 17:13:50		no
19	mxip_system.vol	NONAME [FAT16]\[root]\mxip_system.vol	151552	2008-Jan-15 04:26:00.5	2011-Jun-04 09:46:42		no
20	mxip_lang.vol	NONAME [FAT16]\[root]\mxip_lang.vol	28672	2007-Sep-18 00:14:10	2011-Jun-04 09:46:42		no
21	ati_dbg.txt	NONAME [FAT16]\[root]\ati_dbg.txt	0	2009-Mar-15 13:50:04	2011-Jun-04 14:21:44		no
22	Application Data	NONAME [FAT16]\[root]\Application Data\	32768	2011-Jun-04 17:13:52	2011-Jun-04 17:13:52		no
23	ConnMgr	NONAME [FAT16]\[root]\ConnMgr\	32768	2011-Jun-04 17:14:16	2011-Jun-04 17:14:16		no
24	cemail.vol	NONAME [FAT16]\[root]\cemail.vol	442544	2011-Jun-04 17:14:16	2011-Jun-04 17:14:22		no
25	pim.vol	NONAME [FAT16]\[root]\pim.vol	2138112	2009-Mar-15 13:50:34	2011-Jun-04 08:51:08		no
26	Microsoft .NET CF 2.0.LOG.TXT	NONAME [FAT16]\[root]\Microsoft .NET CF 2.0.LOG.TX	7072	2011-May-19 19:52:54	2011-May-19 19:53:24		no
27	kill.log	NONAME [FAT16]\[root]\Statistics\kill.log	128	2011-Jun-04 14:23:04	2011-Jun-04 14:23:04		no
28	memstat.log	NONAME [FAT16]\[root]\Statistics\memstat.log	2	2011-Jun-04 14:23:04	2011-Jun-04 14:23:04		no
29	storagestat.log	NONAME [FAT16]\[root]\Statistics\storagestat.log	20	2011-Jun-04 14:23:04	2011-Jun-04 14:23:04		no
30	checksum.xml	NONAME [FAT16]\[root]\Statistics\checksum.xml	44	2011-Jun-04 14:23:04	2011-Jun-04 14:23:04		no
31	errors.xml	NONAME [FAT16]\[root]\Statistics\errors.xml	43	2011-Jun-04 14:23:04	2011-Jun-04 14:23:04		no
32	info.xml	NONAME [FAT16]\[root]\Statistics\info.xml	1048	2011-Jun-04 14:23:04	2011-Jun-04 17:14:26		no
33	default	NONAME [FAT16]\[root]\Documents and Settings\defa	32768	2011-Jun-04 14:23:06	2011-Jun-04 14:23:06		no

Figura 36. Lista dos arquivos extraídos da memória, após a criação da imagem.

2515	52	NONAME [FAT16]\[unallocated space]\00052	32768				no
2516	5105	NONAME [FAT16]\[unallocated space]\05105	104857600				no
2517	8305	NONAME [FAT16]\[unallocated space]\08305	104857600				no
2518	11505	NONAME [FAT16]\[unallocated space]\11505	104857600				no
2519	14705	NONAME [FAT16]\[unallocated space]\14705	104857600				no
2520	17905	NONAME [FAT16]\[unallocated space]\17905	104857600				no
2521	21105	NONAME [FAT16]\[unallocated space]\21105	104857600				no
2522	24305	NONAME [FAT16]\[unallocated space]\24305	104857600				no
2523	27505	NONAME [FAT16]\[unallocated space]\27505	104857600				no
2524	30705	NONAME [FAT16]\[unallocated space]\30705	104857600				no
2525	33905	NONAME [FAT16]\[unallocated space]\33905	104857600				no
2526	37105	NONAME [FAT16]\[unallocated space]\37105	104857600				no
2527	40305	NONAME [FAT16]\[unallocated space]\40305	104857600				no
2528	43505	NONAME [FAT16]\[unallocated space]\43505	104857600				no
2529	46705	NONAME [FAT16]\[unallocated space]\46705	104857600				no
2530	49905	NONAME [FAT16]\[unallocated space]\49905	104857600				no
2531	53105	NONAME [FAT16]\[unallocated space]\53105	104857600				no
2532	56305	NONAME [FAT16]\[unallocated space]\56305	104857600				no
2533	59505	NONAME [FAT16]\[unallocated space]\59505	52625408				no

Figura 37. Lista do espaço não alocado na memória.

Foram feitos alguns backups desta evidência antes ser examinada. Esta fase visou tornar visível a evidência, ao explicar sua originalidade e importância. Para o exame das evidências foram utilizadas as ferramentas *Acess Data FTK* versão 1.5, *Acess Data FTK Imager versão 2.9* e *Autopsy*.

Analisando os arquivos da cópia da memória ROM do dispositivo, que contém as evidências usando o *Acess Data FTK Imager*, constatou-se a presença de arquivos de potencial valor para investigação (Figura 38). Para tal análise, criou-se um caso onde foi colocada a evidência para análise. Como resultado do exame, foram coletados diversos arquivos, com várias informações referentes aos mesmos, como: nome, path (endereço na memória), a extensão, tipo de arquivo, categoria, data em que foi criado, data em que foi modificado, data em que foi acessado pela última vez, tamanho cabeçalho e outras informações não menos relevantes e os respectivos códigos Hash MD5, de formas a garantir a integridade dos mesmos (Figuras 39). Foram colhidos os seguintes dados:

a) Foi encontrado um total de 2569 ficheiros;

b) 1130 em imagens (GIF, JPG, PNG, BMP);

c) 160 arquivos com extensões diversas (.docx, .mui, .xml);

d) 291 documentos;

e) 380 arquivos executáveis;

f) 62 arquivos de outros tipos conhecidos;

g) 684 arquivos de tipo desconhecido;

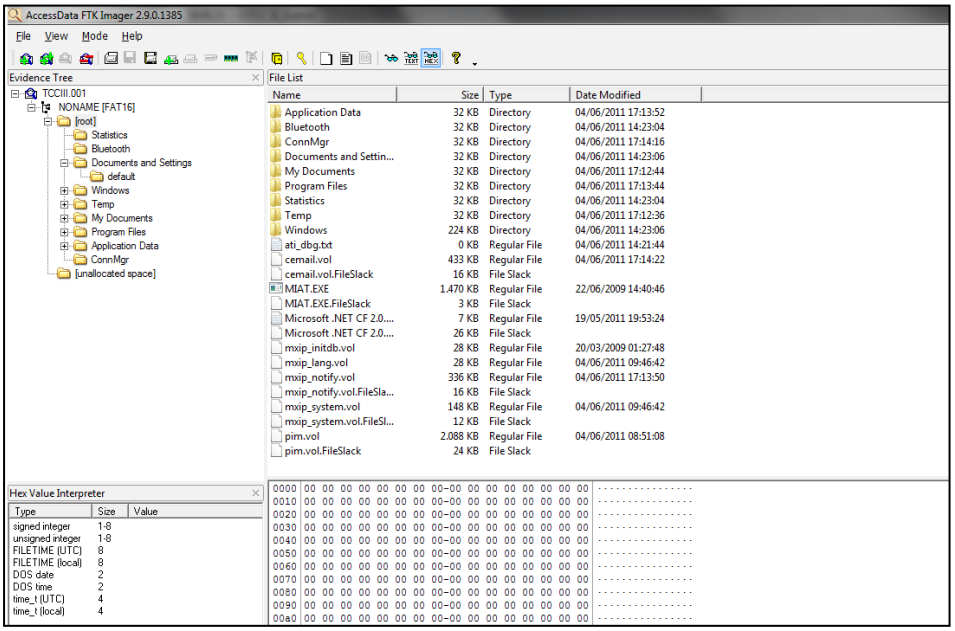


Figura 38. Sistema de arquivos do dump da memória do dispositivo visto usando a ferramenta *Acess Dara FTK Imager*.

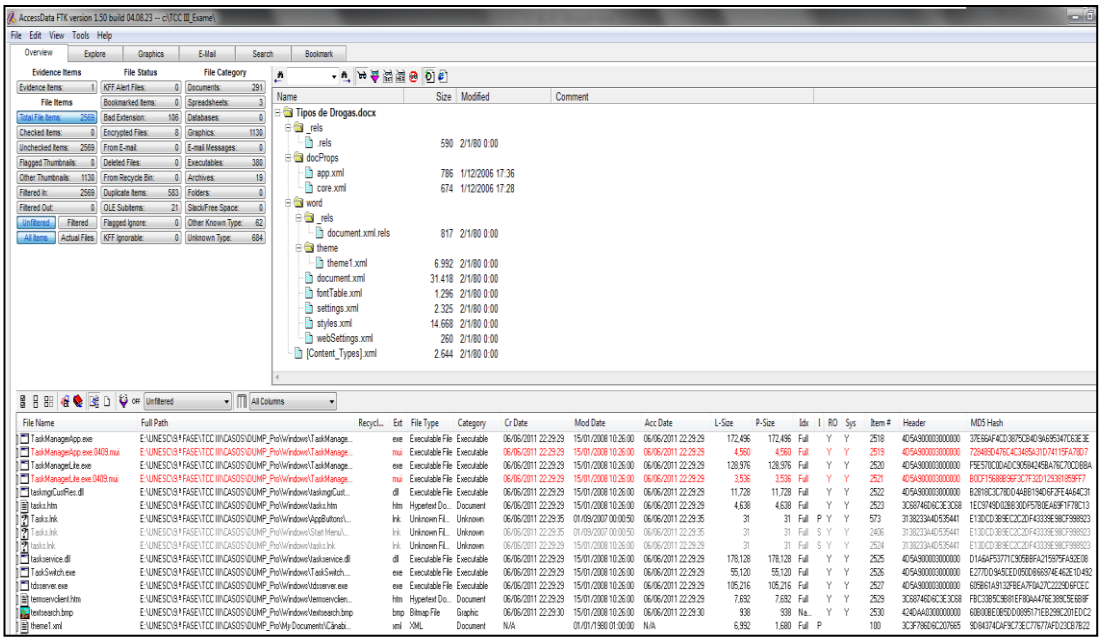


Figura 39. Sistema de arquivos com o código Hash MD5 gerado.

5.2.9.1 Exame do Conteúdo das Evidências Coletadas

Depois de feita a coletas das evidências, eis o momento de examinar os arquivos coletados. Começou-se por examinar os bancos de dados incorporados, porque os dispositivos *Windows Mobile* armazenam algumas informações importantes em arquivos que encapsulam múltiplos bancos de dados integrados, que incluem detalhes sobre as comunicações, contatos e chamadas.

Destes arquivos pode-se citar o *cemail.vol*[13] e *pim.vol*[14], como já foi dito em capítulos anteriores, contém incorporado informações de banco de dados como o histórico de chamadas e informações de contato através de *clog.db* e bases de contatos. Embora o formato não seja formalmente documentado, muitos aspectos dos arquivos *pim.vol* e *cemail.vol* foram explorados neste exame. Para examinar estes arquivos foram usadas as ferramentas *Acess Data FTK* versão 1.5, *Acess Data FTK Imager versão 2.9* e *Autopsy*.

[13] Armazenamento de mensagens de SMS e E-mail.
[14] Gerenciamento de informações pessoais, como agenda de endereços, registro de chamadas, e contatos do cartão SIM.

Ao fazer-se o exame das evidências geradas pelo log de aquisição criado pelo MOBILedit, foi possível achar informações relevante e significativas (lista de contatos, lembrete da agenda e lista de clientes), que serviram para ajudar a esclarecer o caso (Figura 40 e 41). Para além destas informações, encontrou-se o registro de um arquivo com o nome "clientes", onde estavam relacionados alguns nomes (Figura 42).

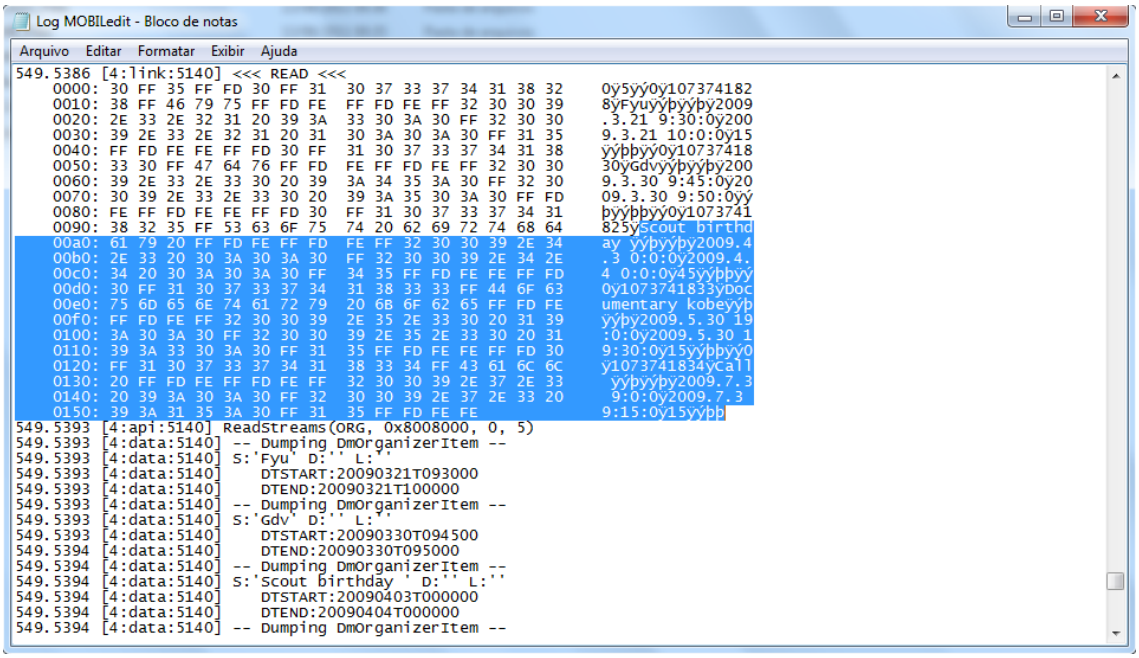


Figura 40. Parte do timeline criado pelo MOBILedit.

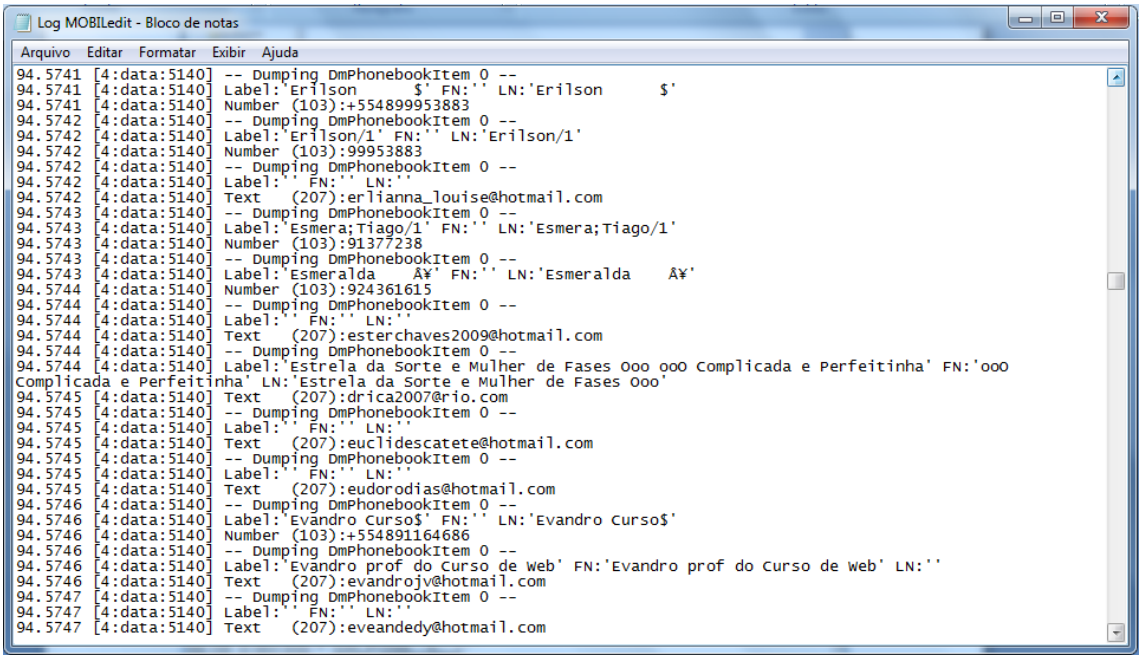


Figura 41. Parte da lista de contatos do log criado pelo MOBILedit.

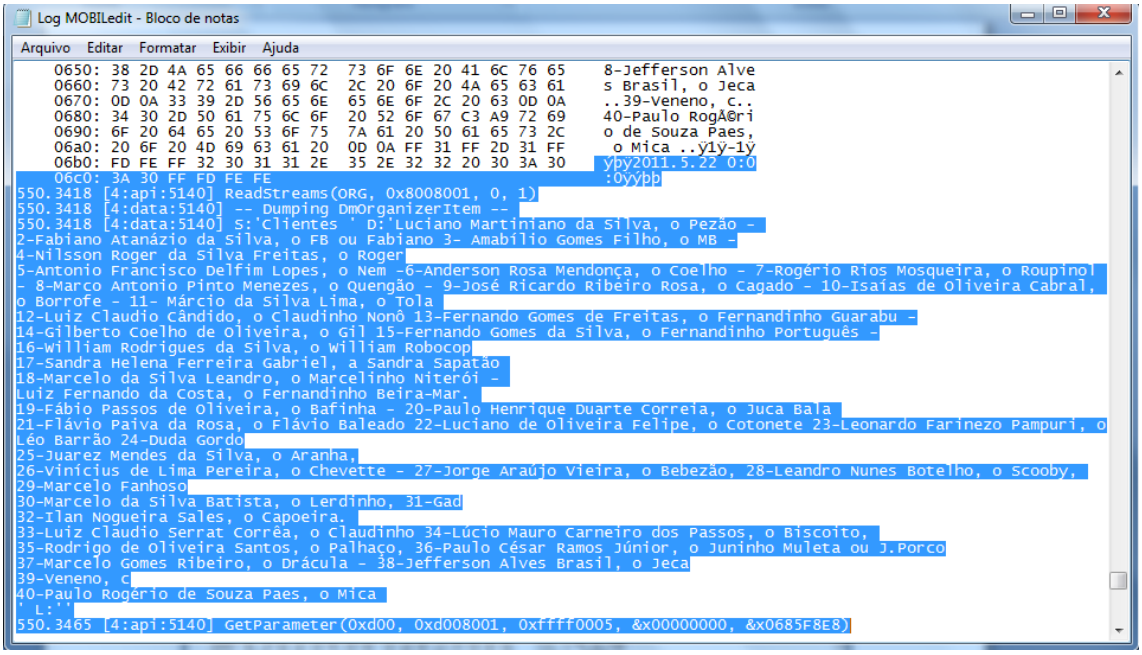


Figura 42. Lista de clientes do log criado pelo MOBILedit

Ao analisar-se o arquivo pim.vol da imagem gerada dos dispositivo, verificou-se também a presença da lista de contatos existentes no dispositivo (Figura 43).

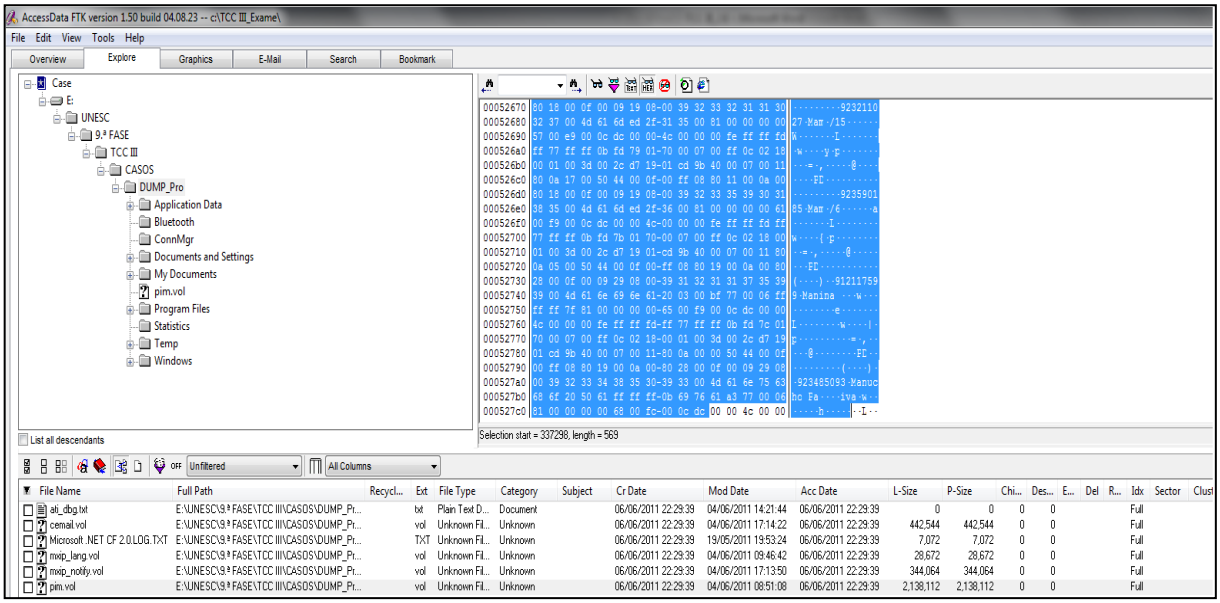


Figura 43. Acess Data FTK mostrando os dados do arquivo *pim.vom*.

Continuando a análise dos arquivos gerados pela dump a memória flash ROM do dispositivo usando a ferramenta *Acess Data FTK*, constatou-se a presença de informações importante no histórico de arquivos temporários da Internet. De realçar a presença de no histórico da hashish, bubba kush e honey oil, que são tipos conhecidos de drogas (Figura 44).

Ainda nos arquivos temporários nota-se a presença de um arquivo apagado, visto que a ferramenta destaca com a cor vermelha estes arquivos (Figura 45). Ainda nesta análise, nota-se a presença de mais evidências, com a presença de imagens que correspondem busca de informações na internet sobre flor da cânabis e os efeitos corporais provocados por ela (Figura 46), bem como uma mensagem de texto que com informação de elevada importância nesta investigação, tais como as lista das drogas mais perigosas do mundo e os traficantes mais procurados do Rio (Figura 47, 48 e 49).

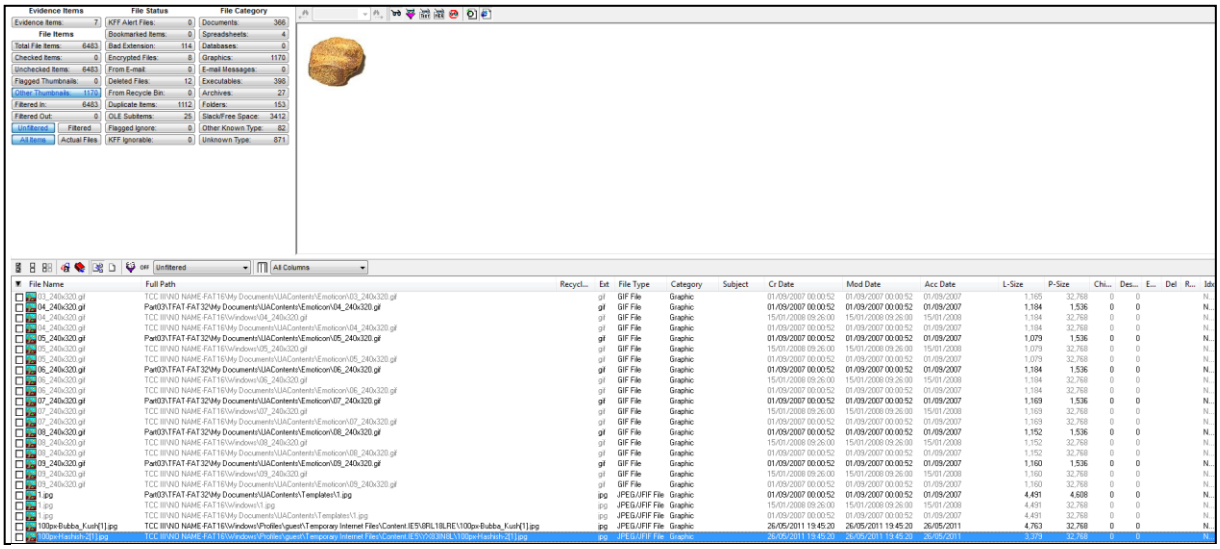


Figura 44. Acess Data FTK mostrando arquivos temporários do histórico da Internet.

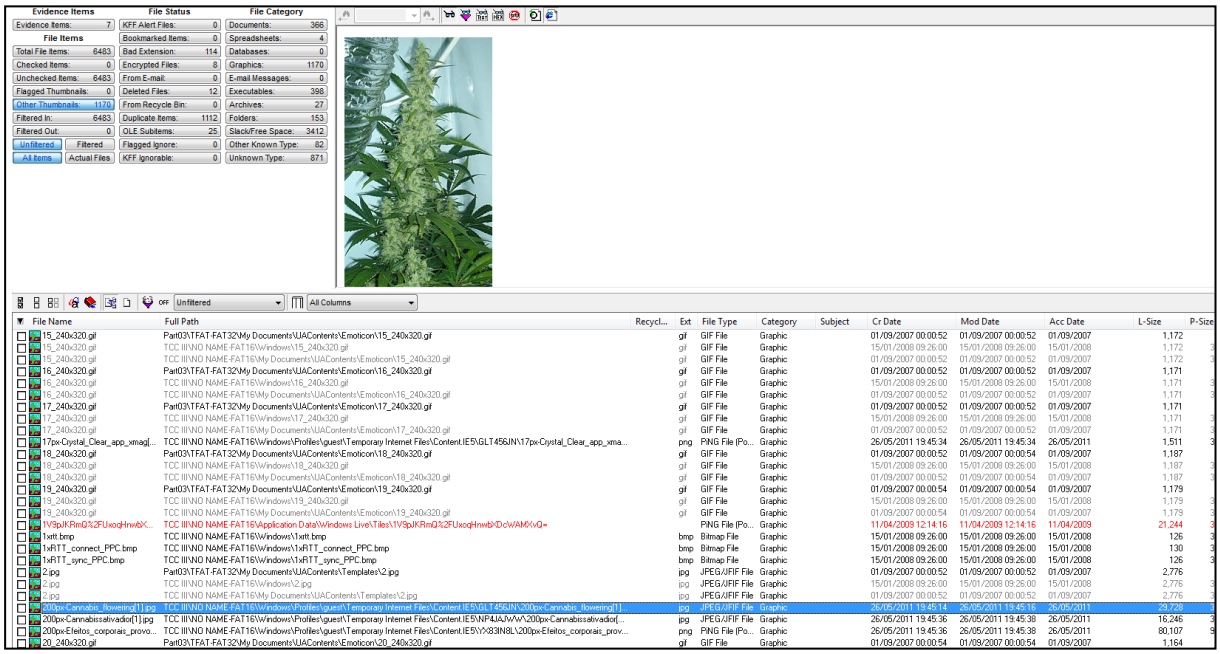


Figura 45. Acess Data FTK mostrando arquivos temporários do histórico da Internet.

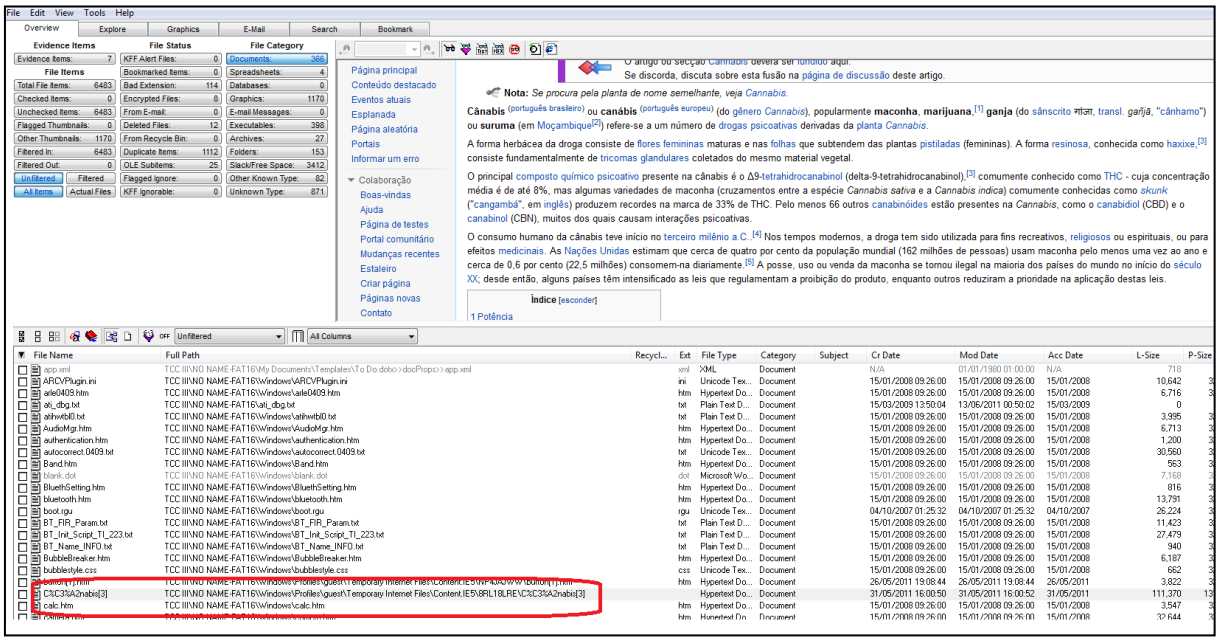


Figura 46. Acess Data FTK mostrando arquivos temporários do histórico da Internet.

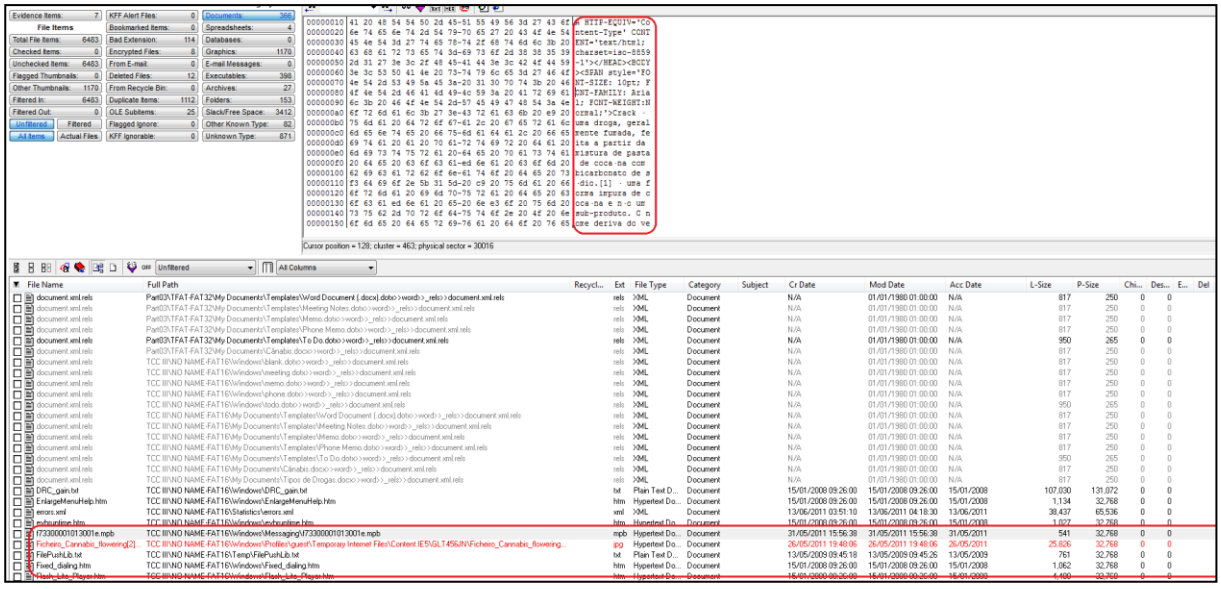


Figura 47. Acess Data FTK mostrando arquivos do histórico de mensagens de e-mail.

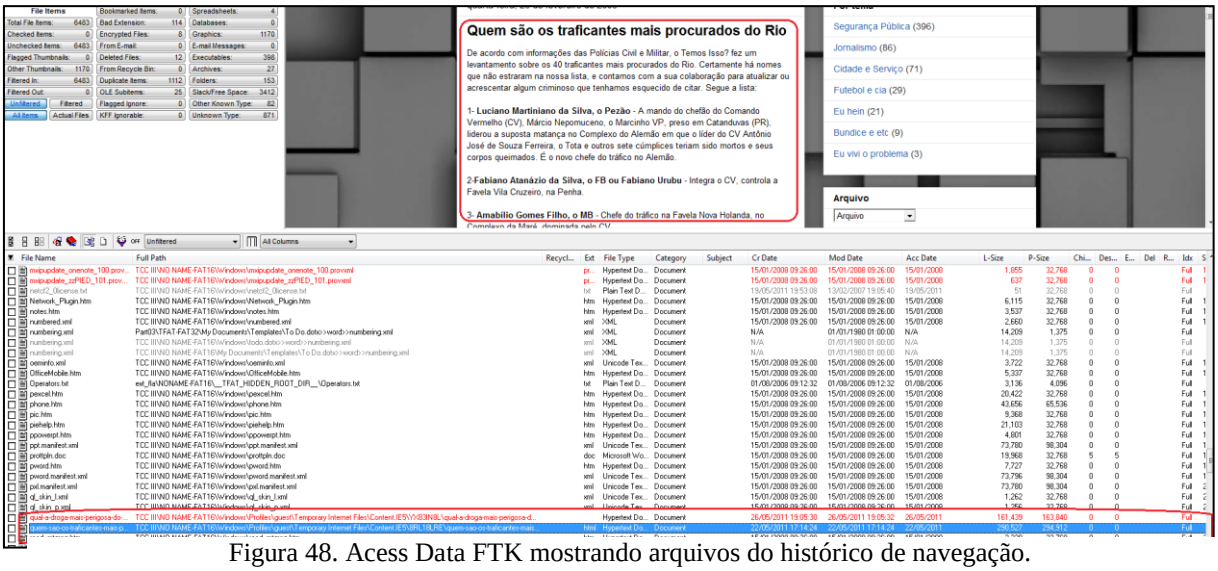


Figura 48. Acess Data FTK mostrando arquivos do histórico de navegação.

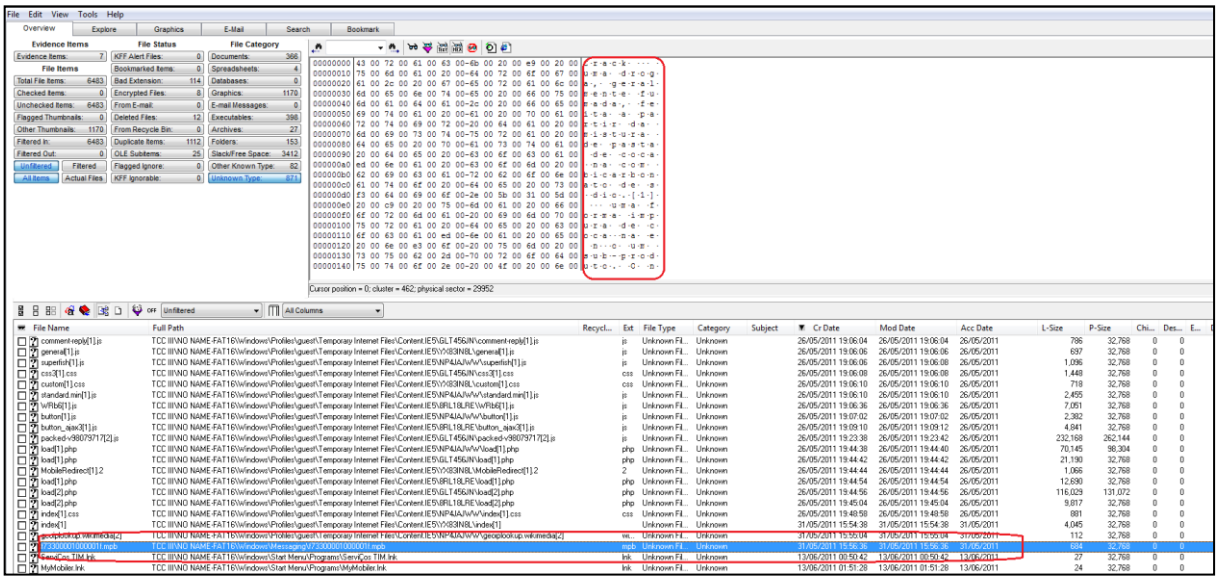


Figura 49. Acess Data FTK mostrando arquivos de mensagem de texto.

5.2.10 Análise

Nesta fase mais técnica do caso foi realizada uma investigação com base nos resultados do exame das evidências. Onde foram identificadas analogias entre os fragmentos de dados, análise de dados ocultos, que mostraram ser bastante significativas, ajudando na reconstrução dos eventos.

Durante a análise das evidências notou-se a presença de dois arquivos com as mesmas características (iguais), um foi resgatado da imagem feita pela ferramenta Itsutils outro pela ferramenta MIAT. Nota-se que o arquivo na versão gerada pelo Itsutils é relativamente menor em relação ao outro, bem como não se notou a presença se informações nele. Já a versão do arquivo tirada da imagem gerada pela MIAT contém informações importantes. De realçar que as duas imagens foram analisadas em simultâneo usando o Acess Data FTK, que separou cada imagem com o seu respectivo nome (Figura 50). Neste momento constata-se a maior eficiência na coleta das evidências, de uma ferramenta em relação à outra.

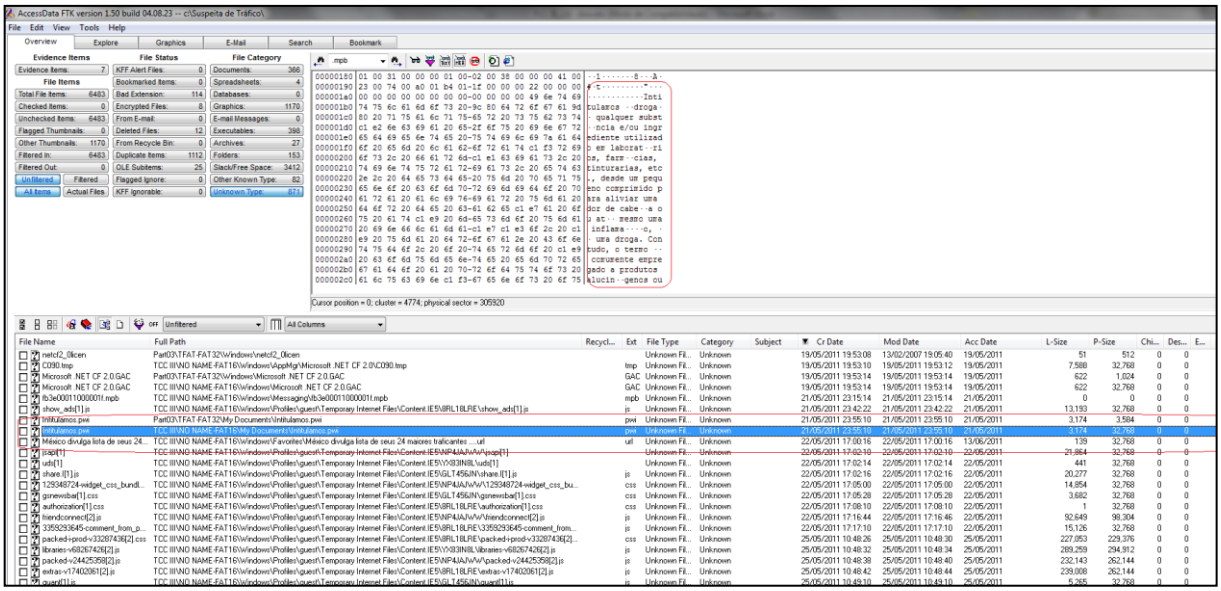


Figura 50. Acess Data FTK mostrando arquivos de mensagem de texto.

Por se tratar de um caso fictício não se fez necessária a análise de todos os arquivos coletados. Mas com o exame feito chegou-se a uma conclusão que será apresentada posteriormente a quando na análise dos resultados.

Como base nas evidências coletadas, fez-se uma busca por palavras chaves, que corresponde a natureza do caso (suspeita de tráfico de drogas), permitindo que mais evidências fossem encontradas. Procurou-se pela palavra “droga”, foi achado um total de 771 correspondências da palavra em 49 arquivos (Figura 51).

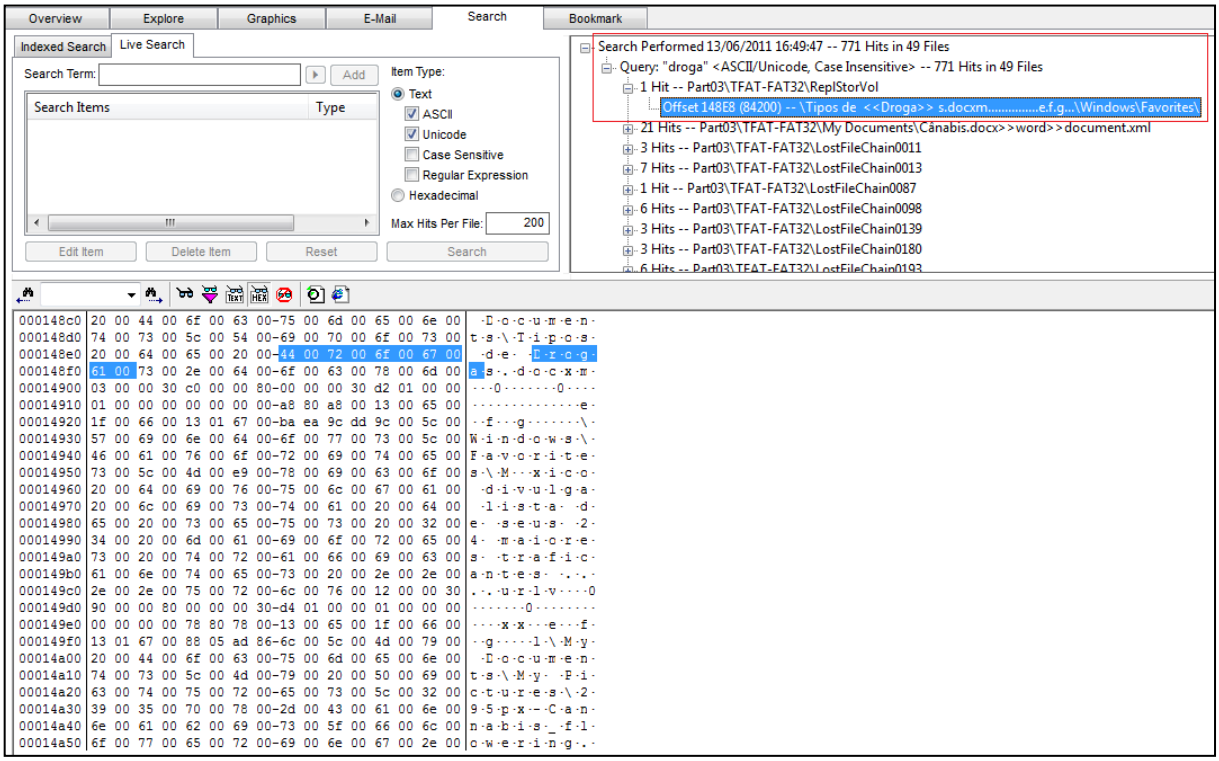


Figura 51. Acess Data FTK mostrando arquivos da busca pela palavra “droga”.

5.2.11 Apresentação

Na fase, fez-se a reconstrução dos eventos, juntando-se todas as evidências examinadas para se determinar o que ocorrido.

Como foi referido, o presente caso simula a investigação de um possível envolvimento em tráfico de drogas, no apreendeu-se o dispositivo que estava sob posse do suspeito no momento em que foi detido. Realizou-se a perícia forense computacional, de forma, a saber-se se o suspeito tem envolvimento direto com o tráfico de substâncias ilícitas.

Para que se cumprissem os propósitos da pesquisa, supôs-se que o suspeito foi detido no dia 06/06/2011 e com ele foi apreendido o dispositivo analisado no caso.

Ao fazer-se a reconstrução dos fatos, examinados e analisados no cenário pode-se dizer que:

a) ocorreu um busca na Internet, no dia 22/05/2011 as 17:14:24 uma pesquisa da

lista dos traficantes mais procurados do Rio. O que tem ligação com a lista encontra com o título clientes, visto que o nome dos clientes da lista corresponde aos nomes encontrados na lista dos traficantes mais procurados do Rio.

b) no dia 26/05/2011 por volta das 19:05:30, de acordo com o histórico de navegação na Internet, o suspeito pesquisou na internet informações referentes a lista das drogas mais perigosas que existem, e por volta das 19:48:06 fez uma busca no Wikipédia sobre a flor da cânabis.

c) ainda analisando o histórico de navegação, o suspeito no dia 31/05/2011 por volta das 15:54:00 fez uma pesquisa no Wikipédia, sobre o crack, minutos depois enviou uma mensagem de email com o seguinte conteúdo: *<HTML><HEAD><META HTTP-EQUIV='Content-Type' CONTENT='text/html; charset=iso-8859-1'></HEAD><BODY><SPAN style='FONT-SIZE: 10pt; FONT-FAMILY: Arial; FONT-WEIGHT:Normal;'>Crack é uma droga, geralmente fumada, feita a partir da mistura de pasta de cocaína com bicarbonato de sódio.[1] É uma forma impura de cocaína e não um sub-produto. O nome deriva do verbo "to crack", que, em inglês, significa quebrar, devido aos pequenos estalidos produzidos pelos cristais (as pedras) ao serem queimados, como se quebrassem.</SPAN></BODY></HTML>*. No mesmo dia, por volta das 16:00:52 o suspeito fez outra pesquisa no Wikipédia de informações sobre a cânabis.

d) foi encontrado extrato de um documento .docx com o nome cânabis, com o seguinte conteúdo: *A forma herb..cea da droga consiste de flores femininas maturas e nas folhas que subtendem das plantas pistiladas (femininas). A forma resinosa, conhecida como haxixe, [3] consiste fundamentalmente de tricomas glandulares coletados do mesmo material vegetal*. Por ter sido um documento apagado pelo suspeito, poucas informações referente ao mesmo foram encontradas.

e) foram feitas buscas em alguns sites pela pela palavra “droga”, tal como se

pode ser na análise feita pela busca de palavras chave nos arquivos coletados: *Visited:http://www.google.com.br/m?q=drogas+...HTTP/1.0 200 OK Title: d / http://api.tweetmeme.com/button.js?url=http%3A//www.mundogump.com.br/qual-a-droga-mais-perigosa-do-mundo/&style=normal&source=philipe3d&service=bit.ly&b=1. button[1].js...HTTP/1.1 200 OK Content-Type: text/html Transfer-Encoding: chunked P3P: CP="CAO PSA" X-Url-Lookup: OrAdd (549) X-Served-By: h01 Content-Encoding: gzip ~U:guest*.

Com as evidências examinadas e analisadas, pode-se provar que o suspeito não passa de um curioso. De acordo com as análises feitas, chegou-se a conclusão que o mesmo apenas tem investigado sobre o assunto (drogas), procurando adquirir mais conhecimento, ou no intuito futuramente envolver-se neste mundo, o que faz com que seja alvo de investigação por parte da polícia.

Para documentação dos procedimentos e registro das informações sobre o caso, foi criado um laudo pericial com tais informações. O mesmo pode ser visualizado no apêndice A.

5.2.12 Revisão

Esta é a fase final da investigação. Onde foi feita uma revisão de todas as etapas da investigação e identificação de áreas para melhoria. Depois da revisão, os resultados e sua interpretação posterior sofreram certa refinação, para uso em investigações futuras. Em muitos casos, é necessário haver certa iteração entre a fase de exame e análise, para se conseguir uma imagem total do incidente.

CONCLUSÃO

Apesar de seu pequeno tamanho, os dispositivos Windows Mobile podem conter quantidades substanciais de informação sobre seus usuários, inclusive com quem eles se comunicam e o que fazem em determinados momentos. Embora haja aspectos do dispositivo com Windows Mobile que são familiares aos analistas, há variações suficientes que tornam a perícia forense me Windows Mobile algo distinto, com seus próprios instrumentos e técnicas originais. Como os dispositivos Windows Mobile tendem a tornar-se cada vez mais usados, existe uma necessidade crescente de analistas que possam adquirir a prova a partir destes dispositivos, e examinar seu conteúdo. Há também uma necessidade de mais investigação e desenvolvimento para melhorar a nossa capacidade de extrair informações a partir de dispositivo com Windows Mobile, incluindo mais dados apagados.

Para a conclusão desta pesquisa, foi necessário pesquisar e documentar as técnicas convenientes para análise, coleta e preservação de evidências forense em dispositivos PDA com Windows Mobile, realizar testes com variadas ferramentas estudadas, analisar e documentar os resultados obtidos.

O modelo apresentado precisa ser testado para sua praticidade. Não há um método simples para testar o modelo. A aplicação do modelo em diferentes contextos deve ser estudada para verificar se este é um quadro de referência geral. O modelo precisa ser amplamente avaliado por especialistas forenses e autoridades policiais em diversas partes do mundo para o aperfeiçoamento dos processos. A tecnologia associada com dispositivos portáteis está mudando drasticamente a cada dia. Este modelo é restrito à atual gama de produtos. Como mais e mais recursos são incorporados nestes dispositivos, no futuro os desafios para o investigador forense também aumentará. Assim, o modelo precisa ser constantemente revisto e procedimentos adicionais precisam ser adicionados quando necessário.

É importante mencionar que qualquer erro do perito durante a realização de uma investigação, pode invalidar a mesma, ou pior ainda, inocentar culpados ou culpar inocentes. Torna-se primordial que o perito conduza a pericia usando metodologias aprovadas e padronizadas, que certificarão aos órgãos judiciais a credibilidade da mesma.

Por existirem poucos estudos no País sobre pericia forense computacional, sobretudo com foco na coleta e análise de evidências em *web browsers*, o presente trabalho objetivou analisar e aplicar os procedimentos de perícia forense computacional na busca por evidências em tal ambiente. Para tal foram estabelecidos cinco objetivos específicos que foram alcançados no decorrer do estudo.

O primeiro objetivo específico foi abordado no Capítulo 2, onde se delineou quais os aspectos relevantes de segurança da informação, crimes digitais, evidências digitais bem como conceitos e metodologias da Perícia forense digital. Ainda neste capítulo foram abordados os principais conceitos de pericia forense computacional, e no Capítulo 5 onde foram aplicadas as técnicas e metodologias da mesma, na execução de um estudo de caso.

O segundo objetivo específico foi alcançado no Capítulo 3, ao se descrever o funcionamento do dispositivo PDA com Windows Mobile, arquitetura e características do hardware, bem como os locais de artefato em uso na análise forense com estes dispositivos. O terceiro objetivo específico foi atingido ainda no Capítulo 3, onde foram apresentadas as técnicas e ferramentas forenses open source e/ou livres que seriam usadas no estudo, bem como outras disponíveis no mercado.

Por fim, o quarto e quinto objetivo específico foi alcançado no Capítulo 5, ao se criar um caso de estudo fictício de formas a se aplicar as técnicas de análise forense em PDA com Windows Mobile, a utilização de um cenário para demonstrar como é feita a coleta e documentação das evidências nestes dispositivos. Foram analisados os tipos de evidências

coletadas no decorrer do estudo, de formas a se chegar a um resultado plausível simulando uma situação real de crime envolvendo dispositivos eletrônicos.

Dessa forma, ao se alcançar os objetivos específicos, acredita-se que o objetivo geral tenha sido atingido, pois foi possível analisar os procedimentos necessários a execução de uma perícia forense computacional e aplicá-los com sucesso em um estudo de caso fictício.

Contudo, é importante referir que a aplicação prática comprovou que as ferramentas estudadas não são infalíveis, ocorrendo ocasionalmente erros na conversão das evidências coletadas, e que existem outras ferramentas, técnicas e procedimentos, que dependendo do ambiente podem ser utilizadas.

Por fim, este documento surge como um ponto de partida para uma investigação mais aprofundada em dispositivo com Windows Mobile. Muitas perguntas surgiram durante o estudo de caso conduzido nesta pesquisa, mas no decorrer da mesma, soluções foram encontradas.

REFERÊNCIAS

AGUIAR, Daniel Pedrosa. **Estudo sobre crimes praticados na Internet com o uso do computador**. São Paulo: Faculdade de Tecnologia da Zona Leste, 2009. Disponível: <http://www.fateczl.edu.br/TCC/2009-2/tcc-16.pdf> Acesso em: 10 fev. 2011.

ASSOCIATION OF CHIEF POLICE OFFICERS (ACPO) , Sue. **Good Practice Guide for Computer - Based Electronic Evidence**. London, UK: 7safe, 2007. 72p. Disponível em: <http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf> Acesso em: 16 jun. 2010.

AYERS, R.; JANSEN, W. **PDA Forensic Tools:** an overview and analysis. Gaithersburg: National Institute of Standards and Technology, 2004. Disponível em: <http://csrc.nist.gov/publications/nistir/nistir-7100-PDAForensics.pdf> Acesso em: 03 jun. 2010.

BARYAMUREEBA, V.; TUSHABE, F. **The Enhanced Digital Investigation Process Model**, 2004. In: Digital Forensic Research Workshop. Disponível em: < https://www.dfrws.org/2004/day1/Tushabe_EIDIP.pdf > Acesso em: 23 mai. 2010.

BEAL, A. **Segurança da Informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

BERNARDO, Adauto de Souza. **Técnicas Computacionais no Auxílio à Perícia Forense na análise de evidências coletadas em servidores GNU/LINUX**. 2006. 106 f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) - Universidade do Extremo Sul Catarinense, Criciúma.

BERTOGLIO, Daniel Dalalana. **Perícia Forense:** proposta de uma metodologia de coleta de indícios para ambiente windows. Trabalho de Conclusão de Curso - Curso de Ciência da Computação, Departamento de Instituto de Ciências Exatas e Tecnológicas, Centro Universitário Feevale, Novo Hamburgo, 2008.

BRILL, A. E.; POLLITT, M. **The Evolution of Computer Forensic Best Practices**. In: Journal of Digital Forensic Practice, 2006. Disponível em: < http://www.informaworld.com/smpp/content~db=all?content=10.1080/15567280500541488 > Acesso em: Acesso em: 10 fev. 2011.

BYARD, R.; COREY T.; HENDERSON, C. **The encyclopedia of forensic and legal medicine**. Elsevier: 2005.

CAMPOS, André. **Sistema de Segurança de Informação:** controlando riscos. 2. ed. Florianópolis: Visual Books, 2007.

CARRIER, Brian. **Defining Digital Forensic Examination and Analysis Tools**, Digital Forensics Research Workshop II, 2002. Disponível em: <http://www.dfrws.org/dfrws2002/papers/Papers/Brian_carrier.pdf> Acesso em: 08 mar. 2010.

CARRIER, Brian; SPAFFORD, Eugene H. **Getting Physical with the Investigative Process** International Journal of Digital Evidence, 2003. Volume 2, 3 ed. Disponível em: <http://www.utica.edu/academic/institutes/ecii/publications/articles/A0AC5A7A-FB6C-325D-BF515A44FDEE7459.pdf > Acesso em: 03 mar. 2010.

CARUSO, Carlos Alberto Antônio; STEFFEN, Flavio Deny. **Segurança em informática e de informações**. 2. ed. São Paulo: SENAC, 1999.

CASEY, E. **Crime Investigation:** forensic tools and technology. 2. ed. London: Academic Press, 2003.

_____. **Digital Evidence and Computer Crime:** forensic science, computers and the internet. 2. ed. London: Academic Press, 2004.

_____. **Digital Evidence and Computer Crime**. In: BYARD R, COREY T, HENDERSON C, editors. **The encyclopedia of forensic and legal medicine**. Elsevier: 2005.

CASEY, E.; BANN, M.; DOYLE, J. **Introduction to Windows Mobile Forensics**. Digital Investigation, Missouri, v. VI, p. 136-146, 2010. ISSN 1742-2876. Disponível em: <http://forensic.sc.su.ac.th/seminar/seminari53/ref/52312338.pdf> Acesso em: 03 jun. 2010.

CIARDHUÁIN, S. **An Extended Model of Cybercrime Investigations**, 2004. International Journal of Digital Evidenc. Disponível em: <https://utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf> Acesso em: 23 mai. 2010.

DELLUTRI, F.; OTTAVIANI, V.; ME, G**. MIAT-WM5:** forensic acquisition for windows mobile pocketpc. Proc. of the Workshop on Security and High Performance Computing Systems, 2008. In: **International Conference on High performance Computing & Simulation (HPCS 2008)**. Disponível em: <http://miatforensics.org/contents/pdf/MIAT-WM5_ForensicAcquisitionForWindowsMobilePocketPC.pdf>. Acesso em: 03 mai. 2011.

DIAS, Cláudia. **Segurança e auditoria da tecnologia da informação**. Rio de Janeiro: Axcel Books, 2000.

DISTEFANO, Alessandro; ME, Gianluigi. **An overall assessment of Mobile Internal Acquisition Tool.** Digital Investigation, Missouri, 2008. Disponível em: <http://www.miatforensics.org/contents/pdf/AnOverallAssessmentOfMobileInternalAcquisitionTool.pdf> Acesso em: 06 fev. 2011.

ECKERT, W. G. **Introduction to forensic sciences**. 2. ed. Florida: CRC Press, 2002.

FARMER, Dan; VENEMA, Wietse. **Perícia Forense Computacional:** teoria e prática aplicada. São Paulo: Pearson Prentice-Hall, 2007.

FIGG, William; ZHOU, Zehai. **A computer forensics minor curriculum proposal**. Journal of Computing Sciences in Colleges, Texas, USA, v. 22, n. 4, p. 32 – 38, 2007. Disponível em: < http://www.sciencedirect.com/science/journal/17422876 > Acesso em: 03 jun. 2010.

FREITAS, Andrey Rodrigues de. **Perícia Forense Aplicada à Informática**. Rio de Janeiro: Brasport, 2006.

GAST, Ty. **Forensic Data Handling, Security Assurance Group**, 2003. Disponível em: <http://www.securityassurancegroup.com/PDF/SAG-forensics-data-handling.PDF>. Acesso em: 04 set. 2010.

GEORGE, Mohay A. A. et al. **Computer and Intrusion Forensics**. Boston: Artech House, 2003.

HENGEVELD, W. **XDA tools**, 2009. Disponível em: <www.xs4all.nl/witsme/projects/xda/tools.html>. Acesso em: 03 mar. 2011.

HENSELER, J. **Computer Crime and Computer Forensics**. In: *The Encyclopedia of Forensic Science*, London: Academic Press, 2000.

HORSEWELL, F. **The Practice of Crime Scene Investigation**, New York: CRC, 2004.

IDC. **IDC Forecasts Worldwide Smartphone Market to Grow by Nearly 50% in 2011**, 2011. Disponível em: < http://www.idc.com/getdoc.jsp?containerId=prUS22762811>. Acesso em: 07 mai. 2011.

INTEL. **Persistent storage manager user's guide**, 2005. Disponível em: <www.developers.net/filestore2/download/2613> Acesso em: 13 mar. 2011.

INSTITUTO PORTUGUÊS DE ACREDITAÇÃO (IPAC). **Guia para a Aplicação da NP EN ISO/IEC 17025**, 2010. Disponível em: <http://www.ipac.pt/docs/publicdocs/regras/OGC001.pdf>. Acesso em: 30 mai. 2011.

JANSEN, W.; AYERS, R. **Guidelines on PDA Forensics**. Gaithersburg: National Institute of Standards and Technology (NIST), 2004. Disponível em: < http://csrc.nist.gov/publications/nistpubs/800-72/sp800-72.pdf> Acesso em: 03 jun. 2010.

JOHNSON, T. A. **Forensic Computer Crime Investigation**. Florida: Taylor & Francis Group, 2005.

JTAG testing with XJTAG, Version 0.1, XJTAG, 2003. Disponível em: <http://www.xjtag.com/images/TestingWithXJTAG.pdf> Acesso em: 19 fev. 2010.

KIZZA, Joseph Migga. **Ethical and Social Issues in the Information Age**. 2. ed.US: Springer , 2003.

KLAVER, C. Windows Mobile advanced forensics. **Digital Investigation**, Missouri, v. VI p. 147-167, 2010. ISSN 1742/2876. Disponível em: <http://www.sciencedirect.com/science/journal/17422876 > Acesso em: 03 jun. 2010.

KNIJFF, Ronald Van Der. **Handbook of Computer Crime Investigation:** embedded systems analysis. London: Academic Press, 2010.

KRAUSE, Micki; TIPTON, Harold F. **Handbook of Information Security Management**. New York: Auerbach Publications, 1999.

KRUSE II, W. G.; HEISER, J. G. **Computer Forensics:** incident response essentials. Boston: Addison, 2002.

LEE, Henry; PALMBACH, Timothy; MILLER, Marilyn. **Henry Lee's Crime Scene Handbook**, Academic Press, 2001.

MARCELLA, A. J.; GREENFIELD, R. S. **Cyber forensics:** a field manual for collecting, examining, and preserving evidence of computer crimes. 2. ed. New York: Auerbach Publications, 2008.

MARTINS, G. A; THEÓPHILO, C. R. **Metodologia da investigação científica para ciências aplicadas.** São Paulo: Atlas, 2009.

MCQUADE, S. C. **Encyclopedia of Cybercrime**. London: GREENWOOD PRESS, 2009.

MICROSOFT. **Supported Processors**, 2011. Disponível em: <http://msdn.microsoft.com/en-us/windowsembedded/ce/aa714536.aspx#ARM>. Acesso em: 15 mar. 2011.

_____. **Windows embedded CE 6.0 evaluation edition**, 2007. Disponível em: <http://www.microsoft.com/downloads/details.aspx?familyid=7E286847-6E06-4A0C-8CACCA7D4C09CB56&displaylang=en>. Acesso em: 08 mar. 2011.

_____. **EDB data types and size limits**, 2010. Disponível em: <http://msdn.microsoft.com/en-us/library/ms885368.aspx>. Acesso em: 02 mai. 2010.

_____. **TFAT overview**, 2010a. Disponível em: <http://msdn.microsoft.com/en-us/library/aa915463.aspx>. Acesso em: 18 mar. 2011.

_____. **Embedded database system technologies**, 2005. Disponível em: <http://msdn.microsoft.com/en-us/library/ms838188.aspx>. Acesso em: 02 mai. 2010.

_____. **Message content properties**, 2008. <http://msdn.microsoft.com/en-us/library/bb446140.aspx>. Acesso em: 02. fev. 2011.

_____. **TFAT File naming limitations**, 2008a. Disponível em: <http://msdn.microsoft.com/en-us/library/ms892402. aspx> Acesso em: 21 fev. 2011.

_____. **Heaps**, 2008b. Disponível em: <http://msdn.microsoft.com/en-us/library/aa450550.aspx>. Acesso em: 08 mar. 2011.

_____. **Virtual memory layout:** windows ce 5.0 vs. windows embedded ce 6.0, 2008c. Disponível em: <http://msdn.microsoft.com/en-us/library/aa914933.aspx>. Acesso em: 08 mar. 2011.

_____. **Databases**, 2008d. Disponível em: <http://msdn.microsoft.com/en-us/library/ms885343.aspx>. Acesso em: 13 mar. 2011.

_____. **Driving connectivity**, 2008e. Disponível em: <http://download.microsoft.com/download/6/5/0/6505FA0E-1F39-4A34-BDC9-A655A5D3D2DB/MicrosoftAutoOverview.pdf> Acesso em: 16 mar. 2011.
MIDDLETON, B. **Cyber Crime Investigator's field guide**. London: Auerbach, 2002.

NATIONAL INSTITUTE OF JUSTICE (NIJ), **Crime Scene Investigation –** a guide for first responders, 2001. Disponível em: < http://www.ncjrs.gov/pdffiles1/nij/219941.pdf > Acesso em: 11 out. 2010.

_____. **Forensic Examination of Digital Evidence**: a guide for law enforcement, 2004. Disponível em: <http://www.ncjrs.gov/pdffiles1/nij/199408.pdf> Acesso em: 12 nov. 2010.

_____. **Guidelines on PDA Forensics**. (Special Publication), 2004a. Disponível em: <http://www.csrc.nist.gov/publications/nistpubs/800-72/sp800-72.pdf> Acesso em: 18 out. 2010.

NELSON, B.; PHILIPS, A.; ENFINGER, F.; STEUART, C. **Guide to Computer Forensics and Investigations**. 2. ed. Canada, Thomson Learning Inc. Course Technology, 2005.

O'CONNOR, Thomas R. **Admissibility of Scientific Evidence Under Daubert**. North Carolina Wesleyan College, 2004. Disponível em: <http://faculty.ncwc.edu/toconnor/daubert.htm> Acesso em: 03 jul. 2010.

PINHEIRO, Patrícia Peck. **Direito Digital.** 2. ed, São Paulo: Saraiva, 2008.

POPPER, K. R. **A Lógica da Pesquisa Científica**. 2. ed, São Paulo: Cultrix, 1974.

PROSISE, C.; MANDIA, K. **Incident Response & Computer Forensics**. 2. ed. Berkeley: McGraw-Hill, 2003.

RAMABHADRAN, Anup. **Forensic Investigation Process Model for Windows Mobile Devices**, 2007. Disponível em: <http://www.forensicfocus.com/downloads/windows-mobile-forensic-process-model.pdf> Acesso em: 23 mai. 2010.

REITH, Mark; CARR, Clint; GUNSCH, Gregg. **An Examination of Digital Forensic Models**. International Journal of Digital Evidence, 2002. Volume 1, 2 ed. Disponível em: <http://www.ijde.org/docs/02_fall_art2.pdf> Acesso em: 03 mar. 2010.

REYES, A. **Cyber Crime Investigations:** bridging the gaps between, security professionals, law enforcement, and prosecutors. New York: Syngress, 2007.

REZENDE, Denis Alcides; ABREU, Aline França. **Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais**. São Paulo: Editora Atlas, 2000.

ROGERS. A.; GLAUM, J.; TONKELOWITZ, M. **Creating file systems within an image file in a storage technology - abstracted manner**, 2005. Disponível em: <http://www.freepatentsonline.com/EP1544732.pdf>. Acesso em: 16 mar. 2011.
SCHWEITZER, Douglas. **Incident Response:** computer forensics toolkit. Indiana: Wiley Publishing, 2003.

SHINDER, D. L.; TITTEL, E. **Scene of the Cybercrime:** computer forensics handbook. Boston: Syngress, 2002.

STEPHENSON, P. **Investigating computer-related crime:** handbook for corporate investigators. Florida: CRC PRESS, 2000.

SWGDE, SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE. Digital Evidence: standards and principles, 2008. Disponível em: <http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm> Acesso em: 12 nov. 2010.

VACCA, J. **Computer Forensics** - computer crime scene investigation. 2. ed. Hingham: Charles River Media Inc., 2005.

VOLONINO, Linda; ANZALDUA, Reynaldo. **Computer Forensics for Dummies**. Indianapolis: Wiley Publishing, 2008.

WOLFE, Henry B. **Evidence Analysis, Computers and Security**, 2003. Disponível em: <http://www.sparksdata.co.uk/elseforms/order/COSE%202201.pdf> Acesso em: 15 fev. 2011.

WOODHOUSE, David. **JFFS:** the journalling flash file system. Ottawa Linux Symposium, 2001. Disponível em: <http://sources.redhat.com/jffs2/jffs2.pdf>. Acesso em: 07 set. 2010.
BECKER, H. S. **Métodos de pesquisa em ciências sociais**. 2. ed. São Paulo: HUCITEC, 1994.

YIN, Robert K. **Estudo de caso** – planejamento e métodos. 2. ed. Porto Alegre: Bookman, 2001.

APÊNDICE A – LAUDO PERICIAL

Perito/Examinador: Aniceto Júlio João de Carvalho

Data: 13 de junho de 2011 **Horário:** 20:05

Descrição da Perícia: *Análise de um PDA com Windows Mobile*

Observações: Esta pericia foi realizada como um estudo de caso para o Trabalho de Conclusão de Curso requisitado pela Universidade do Extremo Sul Catarinense, para obtenção do grau de Bacharel em Ciência da Computação.

Identificação do Dispositivo Analisado

Marca /Fabricante /Nome Proj. / Modelo	**Software / Kernel**	**Processador**	**Memória**	**Conectividade**	**Redes / Ligações de dados / Interfaces de expansão**
SoftBank	Microsoft Windows Mobile 5.0 para Pocket PC /AKU 2.6.0	*Clock* da CPU: 400 MHz	RAM: SDRAM	Bluetooth 2.0, antena interna	GSM850, GSM900, GSM1800, GSM1900, UMTS800, UMTS850, UMTS1900, UMTS2100
HTC	Windows CE 5.1.195 Build 14989.2.6.0	CPU: Samsung SC32442, 32 bits	64 MB, 48.8MB accessíveis	Wireless: IEEE 802.11b, IEEE 802.11g, 54 Mbit/s	Ligações de Dados: CSD, GPRS, EDGE, UMTS, HSDPA
		Cache L1: 16 Kbits	ROM: Flash EEPROM	IrDA 1.2, 115200bit/s (SIR/CIR)	USB 1.1 (12Mbit/s)
HTC Hermes 200		Núcleo da CPU: ARM920T	ROM: 128 MB, incluindo 57.08MB acessíveis.		microSD, TransFlash, SDIO
HERM200		Conjuntos de			

Instruções:
ARMv4T

Ferramentas Utilizadas para Coleta e Análise das Evidências:

a) **coleta**: MIAT, RAPI, MOBILedit.

b) **análise**: FTK.

Análise de Arquivos Gerados após a coleta dos dados:

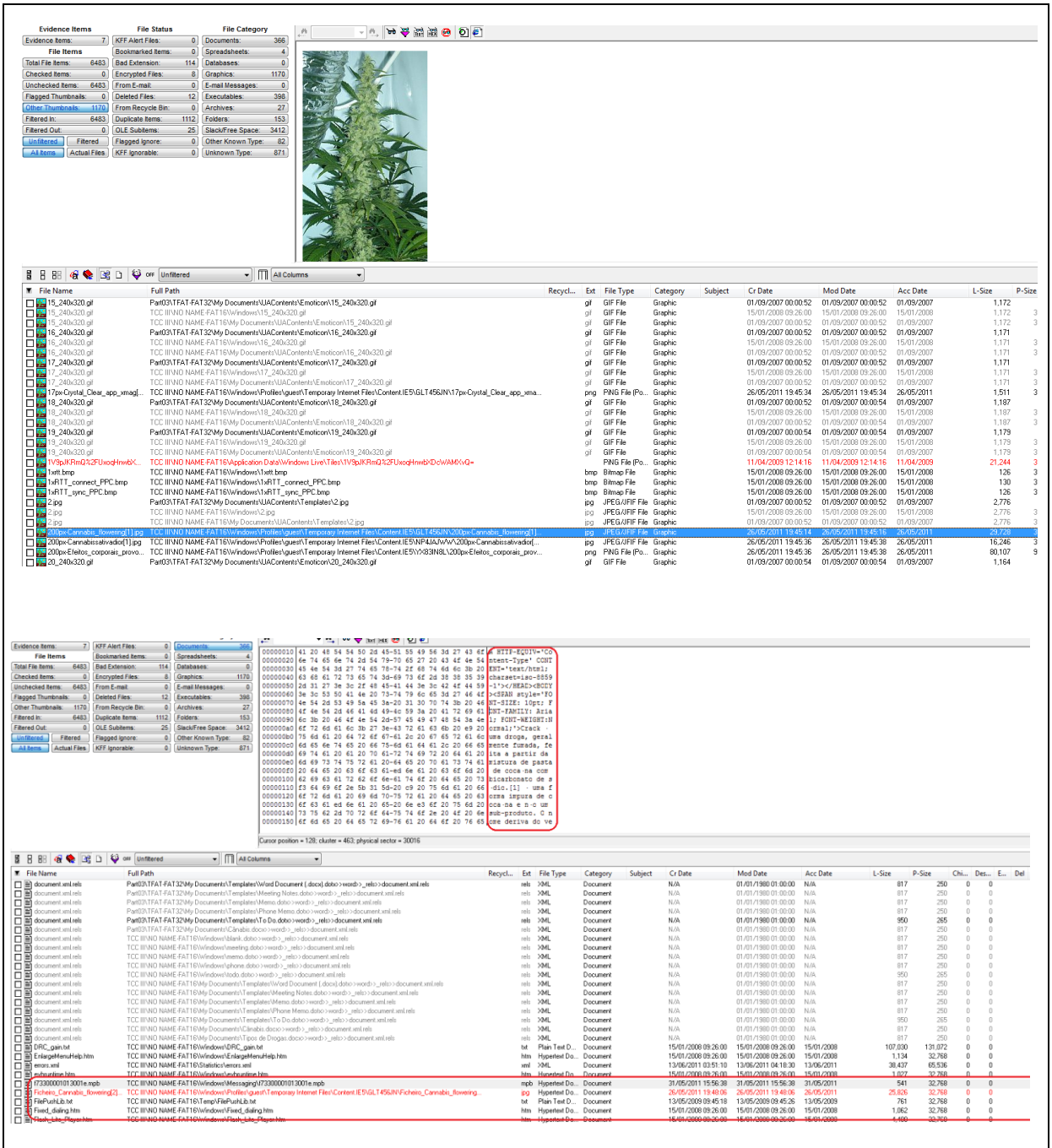
Usando-se a ferramenta *Acess Data FTK*, gerou-se o sistema de arquivos com a imagem da flash ROM do dispositivo, puderam ser examinadas e analisadas as evidências.

	A	B	C	D	E	F	G
1	Filename	Full Path	Size	Created	Modified	Accessed	Is Deleted
2	[root]	NONAME [FAT16]\[root]\	16384				no
3	VBR	NONAME [FAT16]\VBR	512				no
4	reserved sectors	NONAME [FAT16]\reserved sectors	512				no
5	[unallocated space]	NONAME [FAT16]\[unallocated space]\	0				no
6	file system slack	NONAME [FAT16]\file system slack	32256				no
7	FAT1	NONAME [FAT16]\FAT1	122368				no
8	FAT2	NONAME [FAT16]\FAT2	122368				no
9	MIAT.EXE	NONAME [FAT16]\[root]\MIAT.EXE	1504768	2011-Jun-04 14:20:41.6	2009-Jun-22 14:40:46		no
10	Statistics	NONAME [FAT16]\[root]\Statistics\	32768	2011-Jun-04 14:23:04	2011-Jun-04 14:23:04		no
11	Bluetooth	NONAME [FAT16]\[root]\Bluetooth\	32768	2011-Jun-04 14:23:04	2011-Jun-04 14:23:04		no
12	Documents and Settings	NONAME [FAT16]\[root]\Documents and Settings\	32768	2011-Jun-04 14:23:06	2011-Jun-04 14:23:06		no
13	Windows	NONAME [FAT16]\[root]\Windows\	229376	2011-Jun-04 14:23:06	2011-Jun-04 14:23:06		no
14	Temp	NONAME [FAT16]\[root]\Temp\	32768	2011-Jun-04 17:12:36	2011-Jun-04 17:12:36		no
15	My Documents	NONAME [FAT16]\[root]\My Documents\	32768	2011-Jun-04 17:12:44	2011-Jun-04 17:12:44		no
16	Program Files	NONAME [FAT16]\[root]\Program Files\	32768	2011-Jun-04 17:13:44	2011-Jun-04 17:13:44		no
17	mxip_initdb.vol	NONAME [FAT16]\[root]\mxip_initdb.vol	28672	2008-Jan-15 04:26:00.5	2009-Mar-20 01:27:48		no
18	mxip_notify.vol	NONAME [FAT16]\[root]\mxip_notify.vol	344064	2011-Jun-04 17:13:48	2011-Jun-04 17:13:50		no
19	mxip_system.vol	NONAME [FAT16]\[root]\mxip_system.vol	151552	2008-Jan-15 04:26:00.5	2011-Jun-04 09:46:42		no
20	mxip_lang.vol	NONAME [FAT16]\[root]\mxip_lang.vol	28672	2007-Sep-18 00:14:10	2011-Jun-04 09:46:42		no
21	ati_dbg.txt	NONAME [FAT16]\[root]\ati_dbg.txt	0	2009-Mar-15 13:50:04	2011-Jun-04 14:21:44		no
22	Application Data	NONAME [FAT16]\[root]\Application Data\	32768	2011-Jun-04 17:13:52	2011-Jun-04 17:13:52		no
23	ConnMgr	NONAME [FAT16]\[root]\ConnMgr\	32768	2011-Jun-04 17:14:16	2011-Jun-04 17:14:16		no
24	cemail.vol	NONAME [FAT16]\[root]\cemail.vol	442544	2011-Jun-04 17:14:16	2011-Jun-04 17:14:22		no
25	pim.vol	NONAME [FAT16]\[root]\pim.vol	2138112	2009-Mar-15 13:50:34	2011-Jun-04 08:51:08		no
26	Microsoft .NET CF 2.0.LOG.TXT	NONAME [FAT16]\[root]\Microsoft .NET CF 2.0.LOG.TX	7072	2011-May-19 19:52:54	2011-May-19 19:53:24		no
27	kill.log	NONAME [FAT16]\[root]\Statistics\kill.log	128	2011-Jun-04 14:23:04	2011-Jun-04 14:23:04		no
28	memstat.log	NONAME [FAT16]\[root]\Statistics\memstat.log	2	2011-Jun-04 14:23:04	2011-Jun-04 14:23:04		no
29	storagestat.log	NONAME [FAT16]\[root]\Statistics\storagestat.log	20	2011-Jun-04 14:23:04	2011-Jun-04 14:23:04		no
30	checksum.xml	NONAME [FAT16]\[root]\Statistics\checksum.xml	44	2011-Jun-04 14:23:04	2011-Jun-04 14:23:04		no
31	errors.xml	NONAME [FAT16]\[root]\Statistics\errors.xml	43	2011-Jun-04 14:23:04	2011-Jun-04 14:23:04		no
32	info.xml	NONAME [FAT16]\[root]\Statistics\info.xml	1048	2011-Jun-04 14:23:04	2011-Jun-04 17:14:26		no
33	default	NONAME [FAT16]\[root]\Documents and Settings\defa	32768	2011-Jun-04 14:23:06	2011-Jun-04 14:23:06		no

Análise de Arquivos Contendo Evidências:

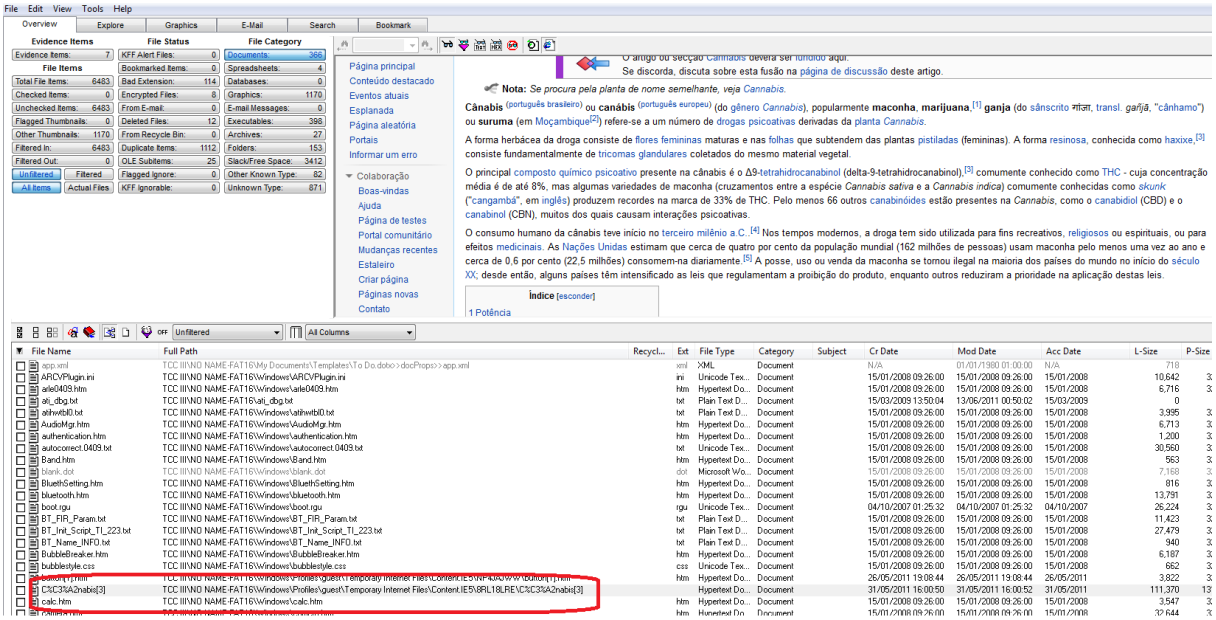
Com a ferramenta *Acess Data FTK* foram arquivos que continham evidências, que serviram para se concluir o caso.

Foram examinadas as várias imagens geradas do dispositivo, de formas a se analisarem arquivos que estavam presentes nas duas imagens, de forma a analisar-se o potencial das ferramentas de aquisição.



Análise de Arquivos de Arquivos Temporários:

Com a ferramenta *Acess Data FTK* foi possível analisar os arquivos temporários gerados pelo histórico de navegação, documentos criados e mensagens enviadas. Provas periciais que indicaram que o suspeito buscou informações referentes ao crime no qual foi suspeito.



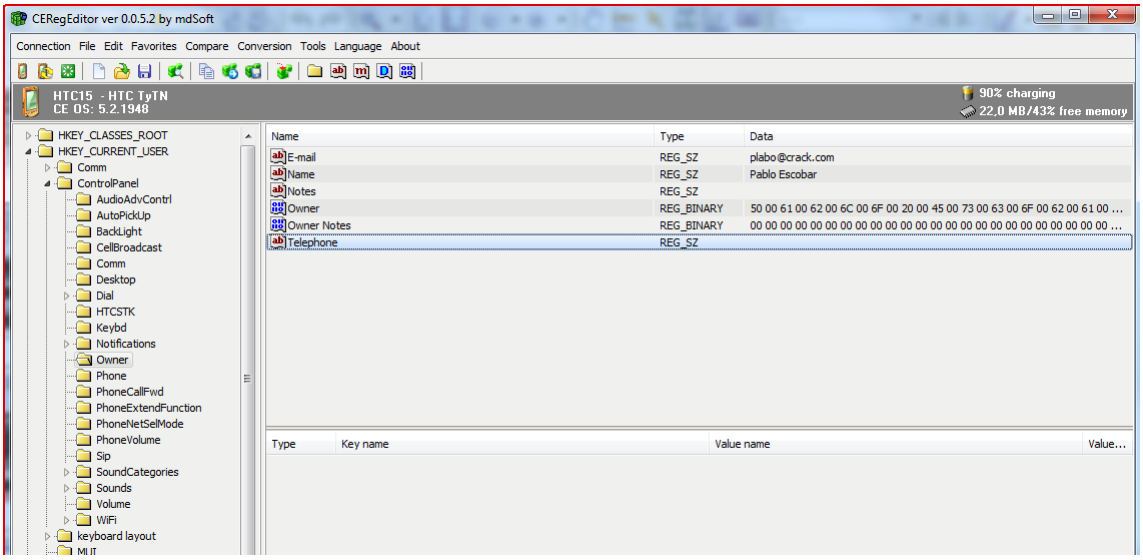
Análise de Arquivos de Hash Gerado de Cada Arquivo:

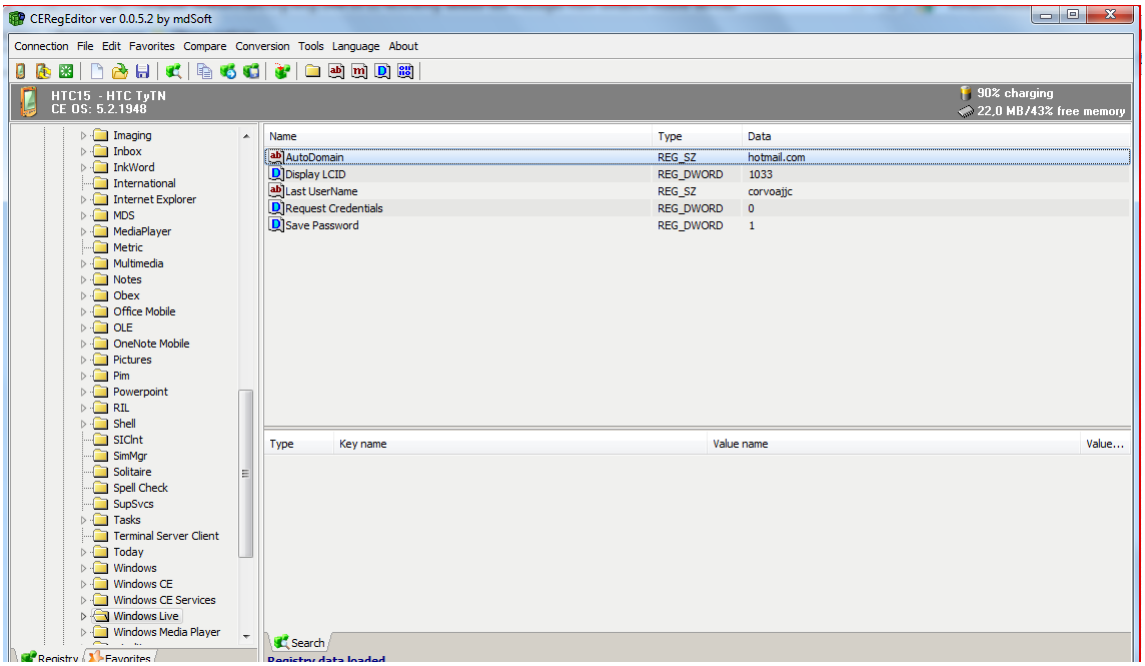
De forma a manter a integridade as evidências, ao fazer a coleta dos dados a ferramenta MIAT gera um arquivo com a lista de todos os arquivos copiados bom como o seu código MD5.

```
<FILE name="ati_dbg.txt" size="0" modified="12/06/2011
21:01:50" md5="D41D8CD98F00B204E9800998ECF8427E">File5.txt
</FILE>
<FILE name="cemail.vol" size="258048" modified="09/06/2011
20:08:02" md5="D41D8CD98F00B204E9800998ECF8427E">File6.vol
</FILE>
<FILE name="pim.vol" size="2138112" modified="12/06/2011
21:12:28" md5="D41D8CD98F00B204E9800998ECF8427E">File7.vol
</FILE>
<FILE name="Microsoft .NET CF 2.0.LOG.TXT" size="7072"
modified="19/05/2011 16:53:24" md5
="4715E0C37BA4D395BE0FD37F06E205E8">File8.txt</FILE>
<FOLDER path="\">
<FILE name="default.vol" size="28672" modified="09/06/2011
20:08:02" md5="D41D8CD98F00B204E9800998ECF8427E">File9.vol
</FILE>
<FILE name="system.hv" size="540672" modified="12/06/2011
21:03:50"/>
<FOLDER path="\Documents and Settings\">
<FILE name="user.hv" size="344064" modified="12/06/2011
21:03:38"/>
<MD5>D41D8CD98F00B204E9800998ECF8427E</MD5></FOLDER>
<FILE name="default.mky" size="52" modified="31/08/2007
21:00:12" md5="A743D7BD1FC3AAD8085F51275D2EE722">File10.mky
</FILE>
<FILE name="compimeh.0409.dat" size="151552"
modified="12/06/2011 21:01:46" md5
="D41D8CD98F00B204E9800998ECF8427E">File11.dat</FILE>
<FILE name="System.mky" size="52" modified="15/03/2009
10:50:14" md5="E8B437A1F556861D7BEA969705428B1F">File12.mky
</FILE>
<FILE name="devcert.dat" size="4582" modified="15/03/2009
```

Análise das Informações do Proprietário do Dispositivo

Usando a ferramenta CERegEditor, navegou-se nos arquivos de registro do dispositivo de formas a extrair-se informações do proprietário do mesmo.





Resultado:

Analisando-se todas as evidências encontradas, combinando a análise dos arquivos temporários, histórico de navegação, extratos de mensagens e documentos, baseando-se nas provas encontradas foi possível concluir que suspeito Fulano de Tal, não poderá ser acusado de envolvimento com tráfico de drogas. De salientar que ao se fazer a aquisição com a ferramenta RAPI, ela deixa alguns registros (*ddl*) no dispositivo, o que não altera em nada o resultado ou as evidências coletadas.

APÊNDICE A – ARTIGO: ANÁLISE FORENSE EM PERSONAL DIGITAL ASSISTANT (PDA) COM WINDOWS MOBILE: TÉCNICAS, PROCEDIMENTOS E FERRAMENTAS

Análise Forense em Personal Digital Assistant (PDA) com Windows Mobile: Técnicas, Procedimentos e Ferramentas

Aniceto Júlio João de Carvalho[1], Paulo João Martins[2], Sérgio Coral[2]

[1]Acadêmico do Curso de Ciência da Computação - Departamento de Ciência da Computação - Universidade do Extremo Sul Catarinense (UNESC) – Criciúma / SC – Brazil

[2]Professor do Curso de Ciência da Computação - Departamento de Ciência da Computação - Universidade do Extremo Sul Catarinense (UNESC) – Criciúma / SC – Brazil

anicetojjc@gmail.com, pjm@unesc.net, sc@unesc.net

Abstract. *This paper describes the conclusion work submitted for obtaining the Degree of Bachelor of Computer Science at the UNESC University, whose goal was to analyze and apply the procedures of forensic computing, focusing on collecting and analyzing evidence in PDA with Windows Mobile, contributing to increasing the range of research on the subject. To achieve it we performed a literature search and a fictional case study simulating the execution of a computer forensics analysis at the university in question, using the process model for Windows Mobile Device PDA.*

Keywords*: Security, Computer Crime, Forensic expertise, PDA, Windows Mobile.*

Resumo. *O presente artigo descreve o trabalho de conclusão de curso apresentado para obtenção do Grau de Bacharel em Ciência da Computação da Universidade do extremo Sul Catarinense, cujo objetivo foi analisar e aplicar os procedimentos de perícia forense computacional, com foco na coleta e análise de evidências em web browsers, contribuindo para o aumentando do leque de pesquisas sobre o tema. Para a realização do mesmo efetuou-se uma pesquisa bibliográfica, bem como um estudo de caso fictício simulando a condução de uma pericia forense computacional na universidade em questão, utilizando-se do processo modelo para dispositivos PDA com Windows Mobile.*

Palavras-chave*: Segurança; Crimes Digitais; Perícia Forense; PDA, Windows Mobile.*

1. Introdução

A evolução da sociedade foi acompanhada pelo avanço tecnológico que cada vez mais atinge as diferentes camadas da sociedade de forma benéfica. Mas também há um lado sinistro a tecnologia quando é usada para práticas ilegais de tipo pessoal, privado ou incorporado. Há

muito que com a evolução, a sociedade tem convivido com os crimes e a violência que igualmente têm evoluído. Para tentar manter a ordem foram estabelecidas leis pelas autoridades.

Dispositivos digitais portáteis, tais como PDA, tornaram-se mais acessíveis e comuns no ambiente de trabalho. Eles fornecem alta capacidade de armazenamento de dados, além de recursos computacionais e de rede, para gerenciar compromissos e informações de contato, revisão de documentos, comunicação via correio eletrônico e executar outras tarefas (AYERS; JANSEN, 2004, tradução nossa).

Uma definição simples para crimes digitais segundo Stephenson (2000) são delitos cometidos com o uso de um computador ou um sistema computacional. Porém, a natureza de um crime digital é mais complexa.

Para Beal (2005) Segurança da informação é o processo de proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade.

A investigação forense em dispositivos eletrônicos portáteis é um campo relativamente novo e emergente, de grande interesse dentro do mundo da perícia forense digital. Na era moderna, o *Personal Digital Assistant* (PDA) é extremamente popular e é propenso a estar envolvido em crimes eletrônicos, principalmente devido ao seu tamanho compacto e características integradas (NELSON; PHILIPS; ENFINGER; STEUART, 2005, tradução nossa).

A escolha e a análise das ferramentas para a coleta de evidências e o estudo de sua aplicação e preservação também representaram uma motivação adicional para a realização desta pesquisa, que teve como objetivo a análise forense em PDA com Windows Mobile de forma a que possa coletar evidências existentes nestes dispositivos para reconstituição fatos criminalísticos.

2. Segurança da Informação

Segurança da informação é a proteção física e lógica dos sistemas de informação contra acessos não autorizados e sua preservação contra destruição, tendo que se contemplar o aspecto da recuperação, da capacidade operacional em casos de destruição parcial ou total da capacidade de processamento (KRAUSE; TIPTON, 1999, tradução nossa).

Conforme Campos (2007) um sistema de segurança da informação baseia-se em três princípios básicos: confidencialidade, integridade, e disponibilidade.

Segurança, mais do que uma estrutura hierárquica que envolve homens e equipamentos, está relacionada a uma postura gerencial. Dado o dinamismo que as atividades relacionadas com o processamento de informações adquiriram ao longo do tempo, exige-se que as políticas de segurança de informações sejam mais abrangentes e simples (CARUSO; STEFFEN, 1999).

Entende-se que política de segurança, é a política elaborada e implantada para formalização dos anseios da organização quanto à proteção das informações (CARUSO; STEFFEN, 1999).

A política de segurança de informações estabelece princípios de como a organização deve proteger, controlar e monitorar os recursos computacionais e, consequentemente, informações manipuladas dentro da organização (DIAS, 2000).

3. Crimes Digitais

A forma com que os criminosos cometem crimes também tem mudado. A acessibilidade universal ao digital abre novas oportunidades para os inescrupulosos. Milhões de dólares são

perdidos para os criminosos que usam dispositivos computacionais (MIDDLETON, 2002, tradução nossa).

O “Crime digital” é um termo amplo que abrange todas as formas em que os computadores e outros tipos de dispositivos eletrônicos, capazes de se conectar a Internet são usados para quebrar as leis e causar danos. Uma definição um pouco mais técnica seria, uso de computadores ou outros dispositivos eletrônicos por meio de sistemas de informação, tais como redes organizacionais ou na Internet para facilitar os comportamentos ilegais (MCQUADE, 2009, tradução nossa).

3.1 Evidências Digitais

Segundo Casey (2004) evidências digitais são quaisquer dados que provam que um crime foi cometido, ou que podem proporcionar uma ligação entre um crime e sua vítima ou um crime e o seu autor.

Dada à onipresença de evidências digitais, é raro que o crime não tenha dados relacionados armazenados e transmitidos por meio de sistemas informáticos. Uma pessoa treinada pode usar estes dados para compilar muita coisa sobre um indivíduo, fornecendo a introspecção tal que é como olhar por meio de um vitral para a vida pessoal do indivíduo e pensamentos (STEPHENSON, 2000, tradução nossa).

3.2 Questões de Jurisdição

Outro fator que torna difícil uma definição rápida de crime digital é o dilema de jurisdição. As leis em diferentes jurisdições definem os termos de maneira diferente, e é importante para peritos que investigam a criminalidade digital, bem como familiarizar-se com as leis aplicáveis (ECKERT, 2002, tradução nossa).

A noção de crimes digitais ou crimes cometidos com o uso de dispositivos computacionais é relativamente recente, por isso ainda não existem no Brasil, leis específicas para tais atos. Tem-se nos dias de hoje, os seguintes artigos do código civil: Art. 186, o Art. 186, e o Art. 927, que são usados para condenar os praticantes de tais delitos (AGUIAR, 2009).

Ainda para Aguiar (2009) a penalidade para esse tipo de crime, é atualmente assentada por meio de uma adaptação do mesmo para leis vigorantes, não específicas para crimes digitais, levando-se em consideração a consequência deles sobre as vitimas. Em algumas ocorrências, tais adaptações geram falhas nas tipificações de crimes cometidos usando-se dispositivos computacionais.

4. Perícia Forense Computacional

Conforme Vacca (2005) computação forense é a ciência de adquirir, recuperar, preservar e apresentar dados que foram processados eletronicamente e armazenados em suportes informáticos.

Esta ciência é diferente das tradicionais ciências forense. Para começar, as ferramentas e técnicas necessárias estão facilmente disponíveis a qualquer pessoa que pretenda realizar uma investigação forense. Em contraste com a tradicional análise forense, não há geralmente a exigência de que os exames sejam realizados apenas em um ambiente controlado. Ao invés de produzir conclusões que exigem interpretação técnica, a ciência da computação forense produz informação direta e, dados que podem desempenhar um papel significativo na apreensão ou condenação de criminosos cibernéticos (ECKERT, 2002, tradução nossa).

Segundo Reyes (2007) a computação forense está preocupada principalmente com os procedimentos forenses, as regras da evidência, e processos judiciais. É só secundariamente envolvida com computadores e outros dispositivos eletrônicos. Portanto, em contraste com todas as outras áreas da computação, onde a velocidade é a principal preocupação, em computação forense é de absoluta precisão.

4.1 Princípios e Procedimentos

As investigações e os incidentes são tratados de maneira diferente, dependendo das circunstâncias do incidente, a gravidade do incidente, bem como a preparação e experiência da equipa de investigação. Investigações digitais são comparáveis às cenas do crime, onde técnicas de investigação utilizadas pela aplicação da lei têm sido aplicadas como fundamento para a criação de procedimentos utilizados quando se trata de evidências digitais (JOHNSON, 2005, tradução nossa).

Em geral, mesmo fora das investigações policiais, as evidências devem ser coletadas de maneira que sejam admissíveis em tribunal. Pode não ser óbvio quando uma investigação é iniciada.

4.2 Metodologias Investigativas

A metodologia a ser utilizada pelo perito forense pode ser diferenciada, no que concerne o sistema e dispositivo tecnológico envolvido. Visto que não havia métodos específicos que não alterassem de acordo com a tecnologia usada, fazia com que houvesse pouca credibilidade nas provas periciais apresentadas em casos judiciais.

Na tentativa aumentar a credibilidade e solidificar a perícia forense computacional em casos judiciais, criaram-se metodologias que são usadas como guias no processo investigativo, que definem etapas a serem cumpridas pelos peritos, independentemente do dispositivo ou sistema computacional em causa, bem como as ferramentas a serem utilizadas (BERNARDO, 2006).

4.3 Modelo Forense para dispositivos com Windows Mobile

Há muitos modelos de forense digital propostos em diferentes partes do mundo. No entanto nenhuma conclusão foi alcançada em relação ao mais adequado. Cada framework pode trabalhar bem com um determinado tipo de investigação (RAMABHADRAN, 2007, tradução nossa).

O modelo de processo forense em PDA com Windows Mobile foi desenvolvido e apresentado por Anup Ramabhadran para ajudar os profissionais forenses e autoridades policiais na investigação de crimes que envolvam tais dispositivos. Esse modelo tenta superar as grandes deficiências dos atuais modelos de forense digital, e enfatiza uma abordagem sistemática e metódica para investigação forense digital (JANSEN; AYERS, 2004). O modelo proposto é composto de doze (12) etapas, que serão explicadas posteriormente no estudo de caso.

5. Análise Forense em PDA com Windows Mobile

O PDA com Windows Mobile tornou-se mais amplamente usado e pode ser uma valiosa fonte de evidências em uma grande variedade de investigações. Embora o analista forense possa aplicar seu conhecimento em outros sistemas operacionais, para PDA com Windows Mobile da Microsoft, há diferenças suficientes que exigem conhecimento especializado e ferramentas,

para localizar e interpretar evidências digitais nestes sistemas. (CASEY; BANN; DOYLE, 2010, tradução nossa).

A plataforma Windows de dispositivos móveis baseados na arquitetura Windows CE é composta por quatro camadas principais que são: camada de aplicação, do sistema operacional, camada Original Equipment Manufacturer (OEM) e do hardware.

5.1 Locais de artefatos de uso em PDA com Windows Mobile

Apesar de alguns arquivos como cemail.vol e pim.vol podem ser encontrados em todos os dispositivos com Windows Mobile, a localização dos artefatos de uso nos diferentes modelos de dispositivos móveis pode variar. Arquivos adicionais podem ser encontrados em outros locais, como a pasta "\ Temp".

Por exemplo, certas ferramentas de aquisição forense que dependem de APIs do Windows Mobile não conseguem copiar o conteúdo dos arquivos que estão bloqueados pelo sistema operacional como cemail.vol, pim.vol e alguns registros. Como resultado desta e de outras restrições em dispositivos com Windows Mobile, métodos de aquisição mais amplamente disponíveis não obtêm todos os dados armazenados nesses dispositivos; algumas ferramentas obtêm muito mais dados do que outros.

Embora ferramentas forense possam recuperar nome de arquivos apagados a partir do volume TFAT do dispositivo Windows Mobile, o analista forense pode encontrar obstáculos para a recuperação de arquivos. Por exemplo, a falha na reconstrução correta do sistema de arquivos TFAT em um dispositivo Windows Mobile pode resultar em falta de arquivos e pastas (CASEY; BANN; DOYLE, 2010, tradução nossa).

5.2 Ferramentas para análise forense em PDA com Windows Mobile

O desenvolvimento mais notável dos últimos tempos na funcionalidade de algumas das ferramentas usadas, ou seja, a integração dos vários aspectos de uma investigação forense em um portfólio baseado em casos (KLAVER, 2010, tradução nossa).

Conforme Jansen e Ayers (2004) as ferramentas forense adquirem dados de um dispositivo de duas formas: aquisição física ou aquisição lógica. Aquisição física implica uma cópia bit a bit de toda a informação física (por exemplo, uma unidade de disco ou chip de memória RAM), enquanto a lógica de aquisição implica uma cópia bit a bit de objetos de armazenamento lógico (por exemplo, diretórios e arquivos) que residem em um armazenamento lógico (por exemplo, uma partição de sistema de arquivos) (JANSEN; AYERS, 2004, tradução nossa).

A seguir estão descritas as ferramentas utilizadas nesta pesquisa.

a) MOBILedit! Forensic: É um das ferramentas de investigação forense para dispositivos móveis (telefones, PDA) mais confiáveis e usadas do mundo. Basta conectar um telefone e o MOBILedit Forensic extrai todo o conteúdo e gera um relatório forense pronto para a apresentação nos tribunais.

b) FTK: Forensic Toolkit[15] é reconhecido mundialmente como o padrão em software de computação forense. Esta é uma ferramenta válida em casos judiciais (tribunal), proporciona investigações de ponta em forense digital, tais como: análise, descriptografia e software de quebra de senha software, tudo dentro de uma interface intuitiva e personalizável. FTK foi construída para ser rápida, analítica e de escala empresarial.

[15] Para mais informações, acessar: http://accessdata.com/products/forensic-investigation/ftk.

c) Remote Application Programmers Interface (RAPI): É um conjunto de ferramentas que podem ser usadas para obter imagens de um dispositivo Windows Mobile, desenvolvido pela Hengeveld (2009). Este conjunto de ferramentas é uma coleção de cerca de 30 programas de linha de comando que podem ser executados em um PC e que operam no dispositivo Windows Mobile por meio de uma conexão ActiveSync.

d) Mobile Internal Acquisition Tool (MIAT): É uma ferramenta open source que se centra na aquisição de dados da memória de dispositivos móveis de armazenamento interno. Os dados são copiados para uma memória externa removível (como SD, mini SD). Tal tarefa é realizada sem a necessidade de conectar o aparelho ao PC. Graças a isso, evita-se o uso de qualquer hardware específico (DELLUTRI; OTTAVIANI; ME, 2008, tradução nossa).

6. Estudo de Caso

Um cenário genérico foi elaborado para espelhar uma situação que geralmente surge durante um caso forense em PDA com Windows Mobile e mídias associadas. O cenário foi utilizado para revelar como a metodologia pode ser aplicada, como algumas ferramentas reagem e qual deve ser a postura e atitude do perito forense em determinadas situações (Figura 1).

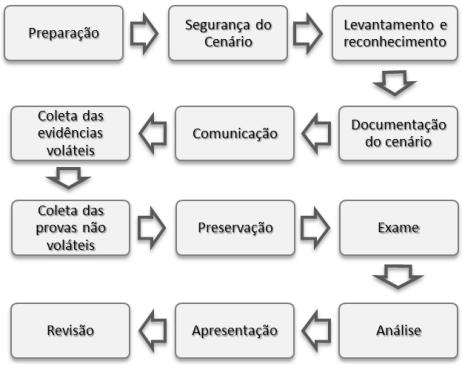


Figura 1. Fases do modelo Forense em Dispositivos com Windows Mobile.
Fonte: RAMABHADRAN, A (2007).

A seguir temos uma explicação detalhada de como cada etapa da modelo foi aplicada neste estudo.

6.1 Preparação

Por se tratar de um caso de estudo fictício, não foi necessária a obtenção de autorização ou mandato de busca judicial, para que se realizasse a perícia forense, visto que é um aspecto importante, no respeito aos direitos de privacidade do suspeito. Posteriormente, definiu-se a finalidade da pesquisa, que pretendia provar o caso de estudo criado, compreendendo-se inicialmente a natureza do crime, prepararam-se as ferramentas necessárias para o padrão de investigações em dispositivos portáteis Windows Mobile e obteve-se uma melhor avaliação sobre as circunstâncias relativas ao crime e fatores técnicos.

Nas investigações envolvendo dispositivos com Windows Mobile há que se levar em conta o fato de que a bateria pode se esgotar antes da coleta de provas. Por isso, preparou-se uma fonte de alimentação padrão para o dispositivo.

Após a preparação minuciosa, o que contribuiu para o aumento da qualidade das provas e minimizou os riscos e ameaças associadas à investigação.

6.2 Segurança do Cenário

Outro aspecto que não se precisou levar em conta neste estudo de caso foi a segurança da cena do crime, visto que o dispositivo foi encontrado em posse do suspeito a quando da sua apreensão, descartando a necessidade de haver o protocolo formal para preservar o cenário. Contudo, teve-se o cuidado necessário de formas a preservar a integridade de todas as evidências, deixando-se o dispositivo no estado em que foi encontrado até que a avaliação adequada seja realizada. Esta fase teve um papel importante no processo global de investigação, porque determinou a qualidade das evidências.

6.3 Levantamento e Reconhecimento

Esta etapa envolveu um levantamento inicial para avaliar o cenário, identificaram-se as possíveis fontes de evidência e formulou-se o plano de pesquisa apropriado. Avaliou-se o dispositivo, sendo que foi necessária a identificação e realização preliminar de uma entrevista com o suspeito de formas a se ter informações valiosas como: sistema de segurança, vários aplicativos presentes nos dispositivos, nomes de usuário, senhas e detalhes de criptografia sem violar as leis de competência.

Caso existisse um mandado de busca e fosse necessária a busca por itens que não estão incluídos no respectivo mandado, as devidas alterações deveriam ser feitas para o mandado existente ou um novo deveria ser obtido, incluindo os itens adicionais.

Foi feito um plano inicial para coleta e análise de evidências no final do inquérito com o suspeito.

6.4 Documentação do Cenário

Esta etapa envolveu a devida documentação da cena do crime. O dispositivo apreendido foi fotografado, também se verificou que o mesmo foi encontrado desligado, sem a presença do cartão SIM e cartão de memória, suspeitando-se de que o suspeito tenha-se desfeito dos mesmos quando se apercebeu de que já não tinha chances de fuga.

Foram registradas as seguintes especificações referentes ao dispositivo:

Tabela 1. Especificações técnicas do dispositivo

Marca /Fabricante /Nome Proj. / Modelo	**Software / Kernel**	**Processador**	**Memória**	**Conectividade**
SoftBank	Microsoft Windows Mobile 5.0 para Pocket PC /AKU 2.6.0	*Clock* da CPU: 400 MHz	RAM: SDRAM	Bluetooth 2.0, antena interna
HTC	Windows CE 5.1.195 Build 14989.2.6.0	CPU: Samsung SC32442, 32 bits	64 MB, 48.8MB accessíveis	Wireless: IEEE 802.11b, IEEE 802.11g, 54 Mbit/s
		Cache L1: 16 Kbits	ROM: Flash EEPROM	IrDA 1.2, 115200bit/s (SIR/CIR)
HTC Hermes 200		Núcleo da CPU: ARM920T	ROM: 128 MB, incluindo 57.08MB acessíveis.	

HERM200	Conjuntos de Instruções: ARMv4T

Após o detalhamento de hardware e software foi possível identificar as fontes de evidências digitais, e selecionar as ferramentas que foram usadas, o que constituiu o kit de investigação.

6.5 Comunicação

Esta etapa ocorre antes da coleta de evidências. De acordo ao estudo de caso criado, esta foi a fase em que foram bloqueadas todas as outras opções possíveis de comunicação dos dispositivos. Como o dispositivo estava desligado, alguns recursos de comunicação como Bluetooth ou rede sem fio não poderiam ser visualizados. Contudo, a melhor opção após apreender um dispositivo é isolá-lo, desativando todas as suas capacidades de comunicação.

6.6 Coleta das Evidências Voláteis

Como a maioria das evidências envolvendo dispositivos PDA é de natureza volátil, estando presente na memória ROM, tendo em conta que o dispositivo foi encontrando desligado, foram selecionadas ferramentas que permitem a coleta de evidências voláteis, visando manter a integridade das informações. O dispositivo foi levado ao laboratório forense para que a análise do mesmo pudesse ser feita em um ambiente controlado.

A combinação de ferramentas utilizadas para obter os melhores resultados foi a seguinte: MIAT, RAPI, MOBILedit, FTK.

Para além destas ferramentas, outros utilitários foram utilizados, tais como: os nativos do sistema operacional como a linha de comandos do Windows, e outros programas como: Windows Mobile Device Center (serve para sincronização dos dados entre o computador e o dispositivos com Windows Mobile), CeRegEditor (editor de registros para dispositivos com Windows Mobile) também compõem o kit.

6.7 Coleta das Evidências não Voláteis

Depois da análise real do caso, seleção das ferramentas a serem utilizadas, criaram-se as condições para a coleta das evidências voláteis, quer dizer, os dados armazenados na memória flash ROM do dispositivo. Como o dispositivo estava desligado, nesta fase ligou-se o mesmo, porque as ferramentas de aquisição das evidências funcionam apenas com o dispositivo em funcionamento. Antes da coleta propriamente dita, é necessária desbloquear o dispositivo em causa, porque no sistema operacional Windows Mobile, a sua configuração padrão não permite que software não assinado possa ser executado.

Contudo, o desbloqueio permitiu que as ferramentas de aquisição, pudessem ser executadas no dispositivo, de formas a coletar informações importantes. Para o desbloqueio do dispositivo, usou o software CeRegEditor. Como se trata de um editor de registros para Windows, apenas foi necessário alterar o registro de segurança do dispositivo. Na configuração padrão o registro aparece: HKLM\Security\Policies\Policies “00001001” = DWORD: 2. Alterou o 2 que é padrão por 1, permitindo desse jeito a execução de software não assinado no dispositivo. Após o desbloqueio, fez-se um soft reset para que a alteração fosse efetivada.

Para coleta das evidências não voláteis usaram-se as ferramentas MIAT, MOBILedit e RAPI, que foram explicadas anteriormente.

6.7.1 Aquisição das Evidências Usando o MOBILedit

Usou-se o MOBILedit para aquisição lógica, no qual observou-se que o resultado não foi o esperado, acredita-se que o motivo seja o fato de ter-se usado a versão "demo" da ferramenta, o que fez com que muito pouca informação fosse extraída do dispositivo. De realçar que há a necessidade do uso do software de sincronização do dispositivo com o computador (Windows Mobile Device Center) para que ela funcione.

Após a conexão do dispositivo com o MOBILedit versão 5.0, criou-se um backup do dispositivo para que se preservasse a integridade do mesmo, desta forma a análise das evidências foi feita no backup do dispositivo. Durante o backup notou-se que algumas informações não foram resgatadas com sucesso, impedindo que a aquisição lógica dos dados fosse feita com sucesso.

6.7.2 Aquisição das Evidências Usando o pacote RAPI

Para a coleta usando o pacote de código aberto RAPI, do qual foi usada a ferramenta Itsutils para extrair a memória ROM do dispositivo. Esta ferramenta funciona a base de comandos (prompt), para tal o dispositivo tinha de estar sincronizado com o computador. O componente pdocread deste pacote adquiriu mais dados a partir do dispositivo comparando com a ferramenta MOBILedit, visto que ele permitiu fazer uma cópia bit a bit de toda memória ROM. Para o funcionamento desta ferramenta copiou-se todos os arquivos da mesma para o C:\itsutils, para ao acessar esta path, os comandos possam ser usados na linha de comandos e os arquivos gerados sejam salvos na pasta C:\itsutils.

Antes da aquisição da memória com do dispositivo, usou-se o comando pdocread –l, que permitiu listar a memória ROM completa e cada uma das partições, tal como qual está subdividida no dispositivo e os respectivos tamanhos de cada uma delas (Figura 2).

Podem-se analisar na lista da Figura 2, entradas da referência da memória flash ROM do sistema de aquisição. As entradas subsequentes referem-se aos discos remotos no dispositivo, que são as áreas de armazenamento do sistema e dados, respectivamente.

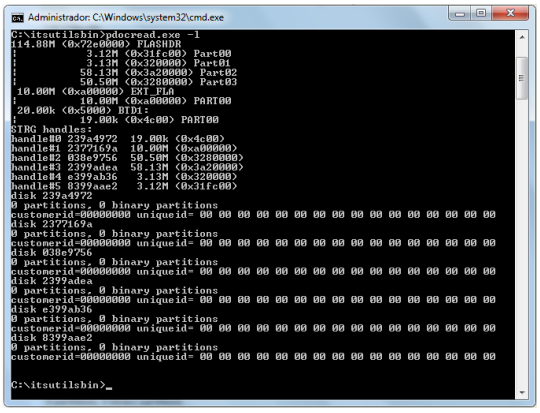


Figura 2. Saída do comando *pdocread* listando todas as partições do dispositivo.

Depois de analisada a memória ROM, fez-se a coleta (imagem bit a bit) de cada uma das partições da memória, no qual se usou o comando pdocread -w -d FLASHDR -b 0x200 -p Part00 0 0x11f000 Part00.raw, que permitiu criar uma imagem (.raw) de cada partição da flash ROM do dispositivo.

No uso dos componentes da ferramenta RAPI para aquisição há que ter em conta determinados aspectos. Ela cria arquivos no dispositivo, que não necessariamente substituem

dados, mas tais informações têm de ser reportadas. Especificamente, um arquivo executável chamado “itsutils.dll” é copiado para o dispositivo e um log de erro “itsutils.log” é criado no dispositivo.

Depois de gerada as imagens da flash ROM do dispositivo usando a ferramenta RAPI, as arquivos gerados estão prontos para serem examinados.

6.7.3 Aquisição das evidências usando o MIAT

O MIAT é uma ferramenta de código aberto, que tem um algoritmo de aquisição que funciona usando APIs que copiam recursivamente cada entrada do sistema interno de arquivo no cartão de memória, invocando a função hash antes e depois da cópia de cada arquivo, permitindo perceber se aconteceram mudanças durante a cópia dos arquivos internos para cartão de memória (Figura 3). Esta tarefa preserva a estrutura de diretórios, porque copia arquivos de acordo com sua posição original. A função hash calcula o MD5 de cada arquivo encontrado na memória inserido no dispositivo. Os hashes são escritos em um arquivo de log e salvos em um ficheiro criado pelo MIAT (Statistics), que contém informações sobre cada arquivo copiado da memória, bem como a data em que foram criados e acessados pela última vez.

Figura 3. Tela do dispositivo enquanto o MIAT vai fazendo a cópia bit a bit da memória flash ROM.

Após a com cópia da memória flash ROM do dispositivo, foram encontrados arquivos e diretórios relevantes como: Mxip lang.vol, Mxip notify.vol, Cemail.vol, Pim.vol, \Windows\Messaging, \Windows\Profiles\, \Windows\Profiles\, \Windows\Favorites, que armazenam dados específicos do usuário, agenda, repositório de SMS e Email, histórico de navegação e outras.

6.8 Preservação

Após a coleta das evidências, fez uma cópia do cartão de memória que continha os dados coletados do dispositivo. Colocou-se o dispositivo e o cartão de memória em um envelope e posteriormente foram colocados em um saco de evidências, com a devida etiqueta de identificação, de formas a manter-se a integridade, visto que se trata de potenciais fontes de evidências. Posteriormente, a análise e processamento de dados tiveram início.

6.9 Exame e Resultados

Nesta fase fez-se a análise do conteúdo das evidências coletadas e extraíram-se informações, que foram fundamentais para comprovar o caso.

Criou-se uma imagem do cartão de memória usando a ferramenta Access Data FTK Imager (anexo C), que continha a cópia dos dados coletados do dispositivo, para que pudesse ser examinado com uma ferramenta apropriada. Depois de gerar a imagem a ferramenta gerou a arquivo em .xls, que contém a lista de todos (2514) os arquivos extraídos da memória do dispositivo, bem como o caminho, a data em foi criado e a última data de modificação. No arquivo também contém o espaço não alocado na memória.

Foram feitos alguns backups desta evidência antes ser examinada. Esta fase visou tornar visível a evidência, ao explicar sua originalidade e importância. Para o exame das evidências foram utilizadas as ferramentas Acess Data FTK versão 1.5, Acess Data FTK Imager versão 2.9 e Autopsy.

Analisando os arquivos da cópia da memória ROM do dispositivo, que contém as evidências usando o Acess Data FTK Imager, constatou-se a presença de arquivos de potencial valor para investigação. Para tal análise, criou-se um caso onde foi colocada a evidência para análise. Como resultado do exame, foram coletados diversos arquivos, com várias informações referentes aos mesmos, como: nome, path (endereço na memória), a extensão, tipo de arquivo, categoria, data em que foi criado, data em que foi modificado, data em que foi acessado pela última vez, tamanho cabeçalho e outras informações não menos relevantes e os respectivos códigos Hash MD5, de formas a garantir a integridade dos mesmos. Foram colhidos os seguintes dados:

- Foi encontrado um total de 2569 ficheiros;
- 1130 em imagens (GIF, JPG, PNG, BMP);
- 160 arquivos com extensões diversas (.docx, .mui, .xml);
- 291 documentos;
- 380 arquivos executáveis;
- 62 arquivos de outros tipos conhecidos;
- 684 arquivos de tipo desconhecido;

6.9.1 Exame do Conteúdo das Evidências Coletadas

Depois de feita a coletas das evidências, eis o momento de examinar os arquivos coletados. Começou-se por examinar os bancos de dados incorporados, porque os dispositivos Windows Mobile armazenam algumas informações importantes em arquivos que encapsulam múltiplos bancos de dados integrados, que incluem detalhes sobre as comunicações, contatos e chamadas.

Destes arquivos pode-se citar o cemail.vol[16] e pim.vol[17], como já foi dito em capítulos anteriores, contém incorporado informações de banco de dados como o histórico de chamadas e informações de contato através de clog.db e bases de contatos. Embora o formato não seja formalmente documentado, muitos aspectos dos arquivos pim.vol e cemail.vol foram explorados neste exame. Para examinar estes arquivos foram usadas as ferramentas Acess Data FTK versão 1.5, Acess Data FTK Imager versão 2.9 e Autopsy.

Ao fazer-se o exame das evidências geradas pelo log de aquisição criado pelo MOBILedit, foi possível achar informações relevante e significativas (lista de contatos, lembrete da agenda e lista de clientes), que serviram para ajudar a esclarecer o caso (Figura 4 e 5).

[16] Armazenamento de mensagens de SMS e E-mail.

[17] Gerenciamento de informações pessoais, como agenda de endereços, registro de chamadas, e contatos do cartão SIM.

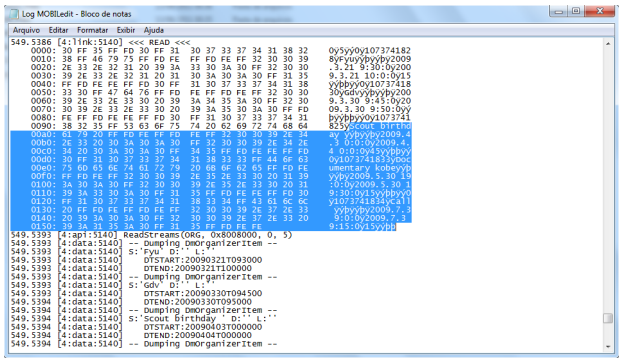


Figura 4. Parte do timeline criado pelo MOBILedit.

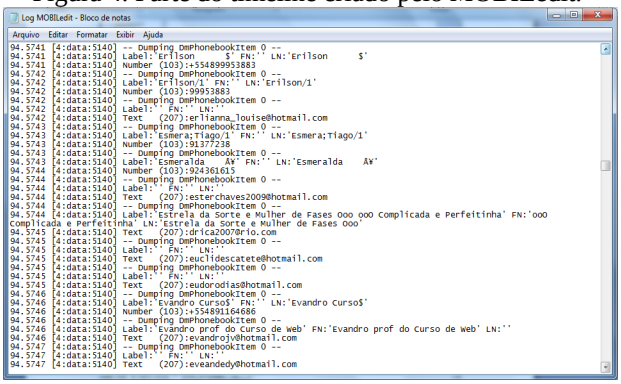


Figura 5. Parte da lista de contatos do log criado pelo MOBILedit.

Ao analisar-se o arquivo pim.vol da imagem gerada dos dispositivo, verificou-se também a presença da lista de contatos existentes no dispositivo (Figura 6).

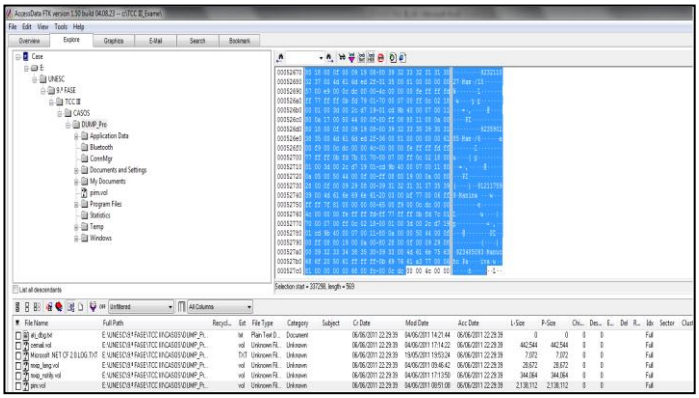


Figura 6. Acess Data FTK mostrando os dados do arquivo pim.vom.

Continuando a análise dos arquivos gerados pela dump a memória flash ROM do dispositivo usando a ferramenta Acess Data FTK, constatou-se a presença de informações importante no histórico de arquivos temporários da Internet. De realçar a presença de no histórico da hashish, bubba kush e honey oil, que são tipos conhecidos de drogas. Ainda nos arquivos temporários nota-se a presença de um arquivo apagado, visto que a ferramenta destaca com a cor vermelha estes arquivos (Figura 7). Ainda nesta análise, nota-se a presença de mais evidências, com a presença de imagens que correspondem busca de informações na internet sobre flor da cânabis e os efeitos corporais provocados por ela (Figura 8), bem como uma mensagem de texto (Figura 9).

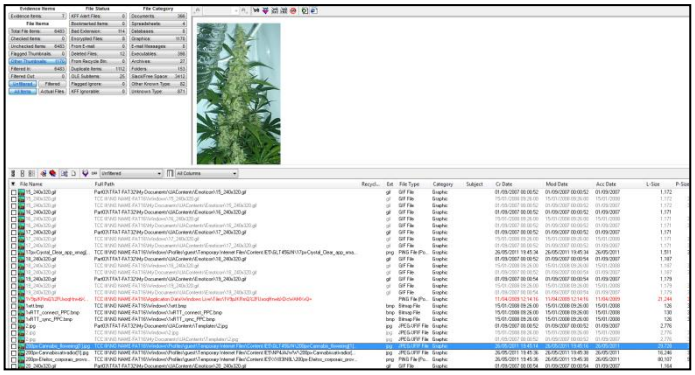


Figura 7. Acess Data FTK mostrando arquivos temporários do histórico da Internet.

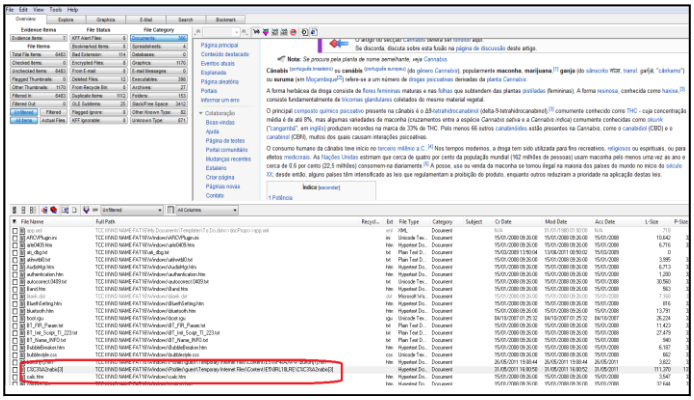


Figura 8. Acess Data FTK mostrando arquivos temporários do histórico da Internet.

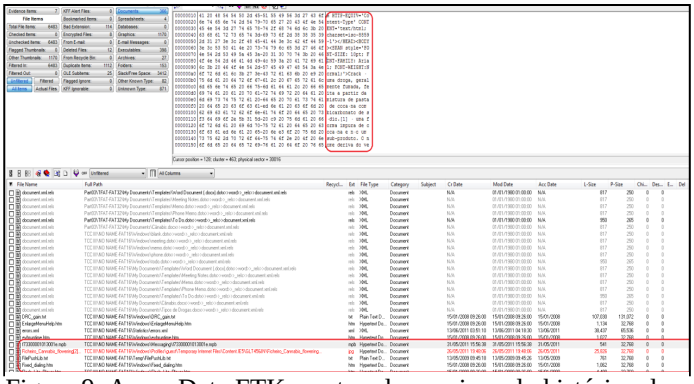


Figura 9. Acess Data FTK mostrando arquivos do histórico de mensagens de e-mail.

6.10 Análise e Resultados

Nesta fase mais técnica do caso foi realizada uma investigação com base nos resultados do exame das evidências. Onde foram identificadas analogias entre os fragmentos de dados, análise de dados ocultos, que mostraram ser bastante significativas, ajudando na reconstrução dos eventos.

Durante a análise das evidências notou-se a presença de dois arquivos com as mesmas características (iguais), um foi resgatado da imagem feita pela ferramenta Itsutils outro pela ferramenta MIAT. Nota-se que o arquivo na versão gerada pelo Itsutils é relativamente menor em relação ao outro, bem como não se notou a presença se informações nele. Já a versão do arquivo tirada da imagem gerada pela MIAT contém informações importantes. De realçar que as duas imagens foram analisadas em simultâneo usando o Acess Data FTK, que separou cada imagem com o seu respectivo nome (Figura 10). Neste momento constata-se a maior eficiência na coleta das evidências, de uma ferramenta em relação à outra.

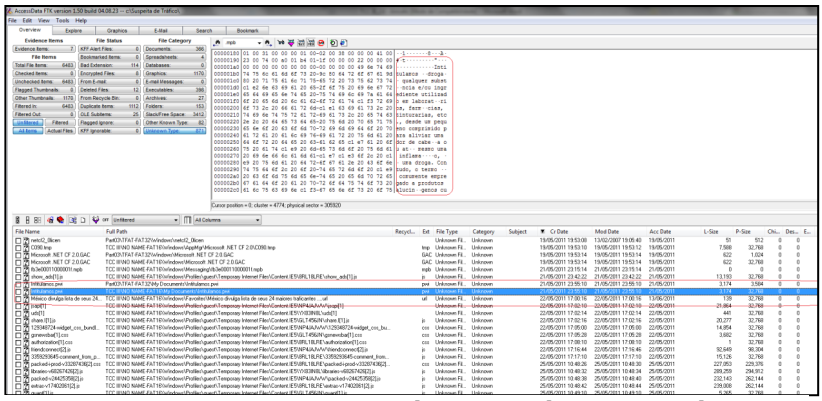


Figura 10. Acess Data FTK mostrando arquivos de mensagem de texto.

Por se tratar de um caso fictício não se fez necessária a análise de todos os arquivos coletados. Mas com o exame feito chegou-se a uma conclusão que será apresentada posteriormente a quando na análise dos resultados.

Como base nas evidências coletadas, fez-se uma busca por palavras chaves, que corresponde a natureza do caso (suspeita de tráfico de drogas), permitindo que mais evidências fossem encontradas. Procurou-se pela palavra “droga”, foi achado um total de 771 correspondências da palavra em 49 arquivos.

6.11 Apresentação

Na fase, fez-se a reconstrução dos eventos, juntando-se todas as evidências examinadas para se determinar o que ocorrido.

Como foi referido, o presente caso simula a investigação de um possível envolvimento em tráfico de drogas, no apreendeu-se o dispositivo que estava sob posse do suspeito no momento em que foi detido. Realizou-se a perícia forense computacional, de forma, a saber-se se o suspeito tem envolvimento direto com o tráfico de substâncias ilícitas.

Para que se cumprissem os propósitos da pesquisa, supôs-se que o suspeito foi detido no dia 06/06/2011 e com ele foi apreendido o dispositivo analisado no caso.

Ao fazer-se a reconstrução dos fatos, examinados e analisados no cenário pode-se dizer que:

a) ocorreu um busca na Internet, no dia 22/05/2011 as 17:14:24 uma pesquisa da lista dos traficantes mais procurados do Rio.
b) no dia 26/05/2011 por volta das 19:05:30, de acordo com o histórico de navegação na Internet, o suspeito pesquisou na internet informações referentes a lista das drogas mais perigosas que existem, e por volta das 19:48:06 fez uma busca no Wikipédia sobre a flor da cânabis.
c) ainda analisando o histórico de navegação, o suspeito no dia 31/05/2011 por volta das 15:54:00 fez uma pesquisa no Wikipédia, sobre o crack, minutos depois enviou uma mensagem de email com o seguinte conteúdo.
d) foi encontrado extrato de um documento .docx com o nome cânabis, com o seguinte conteúdo.

Com as evidências examinadas e analisadas, pode-se provar que o suspeito não passa de um curioso. De acordo com as análises feitas, chegou-se a conclusão que o mesmo apenas tem investigado sobre o assunto (drogas), procurando adquirir mais conhecimento, ou no intuito futuramente envolver-se neste mundo, o que faz com que seja alvo de investigação por parte da polícia.

Para documentação dos procedimentos e registro das informações sobre o caso, foi criado um laudo pericial com tais informações.

6.12 Revisão

Esta é a fase final da investigação. Onde foi feita uma revisão de todas as etapas da investigação e identificação de áreas para melhoria. Depois da revisão, os resultados e sua interpretação posterior sofreram certa refinação, para uso em investigações futuras. Em muitos casos, é necessário haver certa iteração entre a fase de exame e análise, para se conseguir uma imagem total do incidente.

7. Considerações Finais

Para a conclusão desta pesquisa, foi necessário pesquisar e documentar as técnicas convenientes para análise, coleta e preservação de evidências forense em dispositivos PDA com Windows Mobile, realizar testes com variadas ferramentas estudadas, analisar e documentar os resultados obtidos.

O modelo apresentado precisa ser testado para sua praticidade. Não há um método simples para testar o modelo. A aplicação do modelo em diferentes contextos deve ser estudada para verificar se este é um quadro de referência geral. O modelo precisa ser amplamente avaliado por especialistas forenses e autoridades policiais em diversas partes do mundo para o aperfeiçoamento dos processos. A tecnologia associada com dispositivos portáteis está mudando drasticamente a cada dia. Este modelo é restrito à atual gama de produtos. Como mais e mais recursos são incorporados nestes dispositivos, no futuro os desafios para o investigador forense também aumentará. Assim, o modelo precisa ser constantemente revisto e procedimentos adicionais precisam ser adicionados quando necessário.

De salientar que os objetivos traçados para realização de pesquisa foram alcançados, embora dificuldades tenham surgido no decorrer da mesma. Dessa forma, ao se alcançar os objetivos específicos, acredita-se que o objetivo geral tenha sido atingido, pois foi possível analisar os procedimentos necessários a execução de uma perícia forense computacional e aplicá-los com sucesso em um estudo de caso fictício.

Por fim, este documento surge como um ponto de partida para uma investigação mais aprofundada em dispositivo com Windows Mobile. Muitas perguntas surgiram durante o estudo de caso conduzido nesta pesquisa, mas no decorrer da mesma, soluções foram encontradas.

8. Referências

AGUIAR, Daniel Pedrosa. **Estudo sobre crimes praticados na Internet com o uso do computador**. São Paulo: Faculdade de Tecnologia da Zona Leste, 2009. Disponível: <http://www.fateczl.edu.br/TCC/2009-2/tcc-16.pdf> Acesso em: 10 fev. 2011.

AYERS, R.; JANSEN, W. **PDA Forensic Tools:** an overview and analysis. Gaithersburg: National Institute of Standards and Technology, 2004. Disponível em: <http://csrc.nist.gov/publications/nistir/nistir-7100-PDAForensics.pdf> Acesso em: 03 jun. 2010.

BARYAMUREEBA, V.; TUSHABE, F. **The Enhanced Digital Investigation Process Model**, 2004. In: Digital Forensic Research Workshop. Disponível em: < https://www.dfrws.org/2004/day1/Tushabe_EIDIP.pdf > Acesso em: 23 mai. 2010.

BEAL, A. **Segurança da Informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

BERNARDO, Adauto de Souza. **Técnicas Computacionais no Auxílio à Perícia Forense na análise de evidências coletadas em servidores GNU/LINUX**. 2006. 106 f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) - Universidade do Extremo Sul Catarinense, Criciúma.

CARUSO, Carlos Alberto Antônio; STEFFEN, Flavio Deny. **Segurança em informática e de informações**. 2. ed. São Paulo: SENAC, 1999.

CASEY, E. **Crime Investigation:** forensic tools and technology. 2. ed. London: Academic Press, 2003.

_____. **Digital Evidence and Computer Crime:** forensic science, computers and the internet. 2. ed. London: Academic Press, 2004.

_____. **Digital Evidence and Computer Crime**. In: BYARD R, COREY T, HENDERSON C, editors. **The encyclopedia of forensic and legal medicine**. Elsevier: 2005.

CASEY, E.; BANN, M.; DOYLE, J. **Introduction to Windows Mobile Forensics**. Digital Investigation, Missouri, v. VI, p. 136-146, 2010. ISSN 1742-2876. Disponível em: <http://forensic.sc.su.ac.th/seminar/seminari53/ref/52312338.pdf> Acesso em: 03 jun. 2010.

DELLUTRI, F.; OTTAVIANI, V.; ME, G**. MIAT-WM5:** forensic acquisition for windows mobile pocketpc. Proc. of the Workshop on Security and High Performance Computing Systems, 2008. In: **International Conference on High performance Computing & Simulation (HPCS 2008)**. Disponível em: <http://miatforensics.org/contents/pdf/MIAT-WM5_ForensicAcquisitionForWindowsMobilePocketPC.pdf>. Acesso em: 03 mai. 2011.

DIAS, Cláudia. **Segurança e auditoria da tecnologia da informação**. Rio de Janeiro: Axcel Books, 2000.

HENGEVELD, W. **XDA tools**, 2009. Disponível em: <www.xs4all.nl/witsme/projects/xda/tools.html>. Acesso em: 03 mar. 2011.

IDC. **IDC Forecasts Worldwide Smartphone Market to Grow by Nearly 50% in 2011**, 2011. Disponível em: < http://www.idc.com/getdoc.jsp?containerId=prUS22762811>. Acesso em: 07 mai. 2011.

JANSEN, W.; AYERS, R. **Guidelines on PDA Forensics**. Gaithersburg: National Institute of Standards and Technology (NIST), 2004. Disponível em: < http://csrc.nist.gov/publications/nistpubs/800-72/sp800-72.pdf> Acesso em: 03 jun. 2010.

JOHNSON, T. A. **Forensic Computer Crime Investigation**. Florida: Taylor & Francis Group, 2005.

JTAG testing with XJTAG, Version 0.1, XJTAG, 2003. Disponível em: <http://www.xjtag.com/images/TestingWithXJTAG.pdf> Acesso em: 19 fev. 2010.

KLAVER, C. Windows Mobile advanced forensics. **Digital Investigation**, Missouri, v. VI p. 147-167, 2010. ISSN 1742/2876. Disponível em: <http://www.sciencedirect.com/science/journal/17422876 > Acesso em: 03 jun. 2010.

KRAUSE, Micki; TIPTON, Harold F. **Handbook of Information Security Management**. New York: Auerbach Publications, 1999.

MCQUADE, S. C. **Encyclopedia of Cybercrime**. London: GREENWOOD PRESS, 2009.

NELSON, B.; PHILIPS, A.; ENFINGER, F.; STEUART, C. **Guide to Computer Forensics and Investigations**. 2. ed. Canada, Thomson Learning Inc. Course Technology, 2005.

PINHEIRO, Patrícia Peck. **Direito Digital.** 2. ed, São Paulo: Saraiva, 2008.

RAMABHADRAN, Anup. **Forensic Investigation Process Model for Windows Mobile Devices**, 2007. Disponível em: <http://www.forensicfocus.com/downloads/windows-mobile-forensic-process-model.pdf> Acesso em: 23 mai. 2010.

REYES, A. **Cyber Crime Investigations:** bridging the gaps between, security professionals, law enforcement, and prosecutors. New York: Syngress, 2007.

REZENDE, Denis Alcides; ABREU, Aline França. **Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais**. São Paulo: Editora Atlas, 2000.

SHINDER, D. L.; TITTEL, E. **Scene of the Cybercrime:** computer forensics handbook. Boston: Syngress, 2002.

STEPHENSON, P. **Investigating computer-related crime:** handbook for corporate investigators. Florida: CRC PRESS, 2000.

VACCA, J. **Computer Forensics** - computer crime scene investigation. 2. ed. Hingham: Charles River Media Inc., 2005.

ANEXO A - ART. 186, ART. 187 E ART. 927 DO CÓDIGO CIVIL BRASILEIRO.

Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.

Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.

Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.

Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

ANEXO B – PROJETO DE LEI 84/99 DO CONGRESSO NACIONAL

Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências.

De autoria do Deputado Luiz Piauhylino.

O Congresso Nacional decreta:

CAPÍTULO I
DOS PRINCÍPIOS QUE REGULAM A PRESTAÇAO DE SERVIÇO POR REDES DE COMPUTADORES

Art. 1º - O acesso, o processamento e a disseminação de informações por meio das redes de computadores devem estar a serviço do cidadão e da sociedade, respeitados os critérios de garantia dos direitos individuais e coletivos e de privacidade e segurança de pessoas físicas e jurídicas e da garantia de acesso às informações disseminadas pelos serviços da rede.

Art. 2º - É livre a estruturação e o funcionamento das redes de computadores e seus serviços, ressalvadas as disposições específicas reguladas em lei.

CAPÍTULO II
DO USO DE INFORMAÇÕES DISPONÍVEIS EM COMPUTADORES OU REDES DE COMPUTADORES.

Art. 3º - Para fins desta lei, entende-se por informações privadas aquelas relativas a pessoa física ou jurídica identificada ou identificável.

Parágrafo único. É identificável a pessoa cuja individuação não envolva custos ou prazos desproporcionados.

Art. 4º - Ninguém será obrigado a fornecer informações sobre sua pessoa ou de terceiros, salvo nos casos previstos em lei.

Art. 5º - A coleta, o processamento e a distribuição, com finalidades comerciais, de informações privadas ficam sujeitas à prévia aquiescência da pessoa a que se referem, que poderá ser tomada sem efeito a qualquer momento, ressalvando-se o pagamento de indenizações a terceiros, quando couberem.

§ 1º. A toda pessoa cadastrada dar-se-á conhecimento das informações privadas armazenadas e das respectivas fontes.

§ 2º. Fica assegurado o direito à retificação de qualquer informação privada incorreta.

§ 3º. Salvo por disposição legal ou determinação judicial em contrário, nenhuma informação privada será mantida à revelia da pessoa a que se refere ou além do tempo previsto para a sua validade.

§ 4º. Qualquer pessoa, física ou jurídica, tem o direito de interpelar o proprietário de rede de computadores ou provedor de serviço para saber se mantém informações a seu respeito, e o respectivo teor.

Art. 6º - Os serviços de informações ou de acesso a bancos de dados não distribuirão informações privadas referentes, direta ou indiretamente, a origem racial, opinião política, filosófica, religiosa ou de orientação sexual, e de filiação a qualquer entidade, pública ou privada, salvo autorização expressa do interessado.

Art. 7º - O acesso de terceiros, não autorizados pelos respectivos interessados, a informações privadas mantidas em redes de computadores dependerá de prévia autorização judicial.

CAPÍTULO III
DOS CRIMES DE INFORMÁTICA

Seção I
Dano a dado ou programa de computador

Art. 8º - Apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, dado ou programa de computador, de forma indevida ou não autorizada.

Pena: detenção, de um a três anos e multa.

Parágrafo único. Se o crime é cometido:

I - contra o interesse da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
II- com considerável prejuízo para a vítima;
III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
IV - com abuso de confiança;
V - por motivo fútil;
VI - com o uso indevido de senha ou processo de identificação de terceiro, ou
VII - com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de dois a quatro anos e multa.

Seção II
Acesso indevido ou não autorizado

Art. 9º Obter acesso, indevido ou não autorizado, a computador ou rede de computadores.

Pena: detenção, de seis meses a um ano e multa.

Parágrafo primeiro. Na mesma pena incorre quem. sem autorização ou indevidamente, obtém, mantém ou fornece a terceiro qualquer meio de identificação ou acesso a computador ou rede de computadores.

Parágrafo segundo. Se o crime é cometido:

I - com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
II - com considerável prejuízo para a vítima;

III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
IV - com abuso de confiança;
V - por motivo fútil;
VI - com o uso indevido de senha ou processo de identificação de terceiro; ou
VII - com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de um a dois anos e multa.

Seção III
Alteração de senha ou mecanismo de acesso a programa de computador ou dados

Art. 10. Apagar, destruir, alterar, ou de qualquer fama inutilizar, senha ou qualquer outro mecanismo de acesso a computador, programa de computador ou dados, de forma indevida ou não autorizada.

Pena: detenção, de um a dois anos e multa.

Seção IV
Obtenção indevida ou não autorizada de dado ou instrução de computador

Art. 11. Obter, manter ou fornecer, sem autorização ou indevidamente, dado ou instrução de computador.
Pena: detenção, de três meses a um ano e multa.

Parágrafo Único. Se o crime é cometido:

I - com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
II - com considerável prejuízo para a vítima;
Parágrafo Único. Se o crime é cometido:
I - com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
II - com considerável prejuízo para a vítima;
III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
IV - com abuso de confiança;
V - por motivo fútil;
VI - com o uso indevido de senha ou processo de identificação de terceiro; ou
VII - com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de um a dois anos e multa.

Seção V
Violação de segredo armazenado em computador, meio magnético, de natureza magnética, óptica ou similar.

Art. 12. Obter segredos, de indústria ou comércio, ou informações pessoais armazenadas em

computador, rede de computadores, meio eletrônico de natureza magnética, óptica ou similar, de forma indevida ou não autorizada.

Pena: detenção, de um a três anos e multa.

Seção VI
Criação, desenvolvimento ou inserção em computador de dados ou programa de computador nocivo.

Art. 13. Criar, desenvolver ou inserir, dado ou programa em computador ou rede de computadores, de forma indevida ou não autorizada com a finalidade de apagar, destruir, inutilizar ou modificar dado ou programa de computador ou de qualquer forma dificultar ou impossibilitar, total ou parcialmente, a utilização de computador ou rede de computadores.

Pena: reclusão, de um a quatro anos e multa.
Parágrafo único. Se o crime é cometido:

I - contra o interesse da União, Estado, Distrito Federal. Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
II - com considerável prejuízo para a vítima;
III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
IV - com abuso de confiança;
V - por motivo fútil;
VI - com o uso indevid6 de senha ou processo de Identificação de terceiro; ou
VII - com a utilização de qualquer outro meto fraudulento.

Pena: reclusão, de dois a seis anos e multa.

Seção VII
Veiculação de pornografia por meio de rede de computadores

Art. 14. Oferecer serviço ou informação de caráter pornográfico, em rede de computadores, sem exibir, previamente, de forma facilmente visível e destacada, aviso sobre sua natureza, indicando o seu conteúdo e a inadequação para criança ou adolescentes.

Pena: detenção, de um a três anos e multa.

CAPITULO IV
DAS DISPOSIÇÕES FINAIS

Art. 15. Se qualquer dos crimes previstos nesta lei é praticado no exercício de atividade profissional ou funcional, a pena é aumentada de um sexto até a metade.

Art. 16. Nos crimes definidos nesta lei somente se procede mediante representação do ofendido, salvo se cometidos contra o interesse da União, Estado, Distrito Federal Município, órgão ou entidade da administração direta ou indireta, empresa concessionária de serviços públicos, fundações instituídas ou mantidas pelo poder público, serviços sociais autônomos, instituições financeiras ou empresas que explorem ramo de atividade controlada pelo poder público, casos em que a ação é pública incondicionada.

Art. 17. Esta lei regula os crimes relativos à informática sem prejuízo das demais comunicações previstas em outros diplomas legais.

Art. 18. Esta lei entra em vigor 30 (trinta) dias a contar da data de sua publicação.

ANEXO C – RESULTADO DA IMAGEM DO CARTÃO DE MEMÓRIA QUE CONTÉM AS EVIDÊNCIAS

Created By AccessData® FTK® Imager 2.9.0.1385 100406

Case Information:
Case Number: 0001
Evidence Number: 0001
Unique description: Dump1
Examiner: Aniceto de Carvalho
Notes:

Information for E:\UNESC\9.ª FASE\TCC III\CASOS\Imagem\TCCIII:

Operating System Information:

Microsoft Windows Mobile version 5
OS Build: 5.2.1948

Processor Information:

Processor Architecture: ARM
Processor Type: Strong ARM
Number of Processor: 1
Processor Level: 4
Processor Revision: 0
Device OEM ID: 5

Free memory space on Device: 8.4 Mb

Used memory space on Device: 49.7 Mb

Total memory space of Program: 50.8 Mb

Free memory space of Program: 18.5 Mb

Physical Evidentiary Item (Source) Information:
[Drive Geometry]
Bytes per Sector: 512
Sector Count: 3.911.551
Source data size: 1909 MB
Sector count: 3911551
[Computed Hashes]
MD5 checksum: 0d66a04d36d7325f7ff75718f12f4e7c
SHA1 checksum: 4fd50c14e1e17006d59494102d5b99773cdd75e5

Image Information:
Acquisition started: Mon Jun 06 23:09:18 2011
Acquisition finished: Mon Jun 06 23:15:03 2011
Segment list:
E:\UNESC\9.ª FASE\TCC III\CASOS\Imagem\TCCIII.001
E:\UNESC\9.ª FASE\TCC III\CASOS\Imagem\TCCIII.002

Image Verification Results:
Verification started: Mon Jun 06 23:15:03 2011
Verification finished: Mon Jun 06 23:15:15 2011
MD5 checksum: 0d66a04d36d7325f7ff75718f12f4e7c : verified
SHA1 checksum: 4fd50c14e1e17006d59494102d5b99773cdd75e5 : verified