UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

PEDRO PAULO ALEXANDRINO

PERÍCIA FORENSE APLICADA EM CELULARES COM SISTEMA OPERACIONAL SYMBIAN: FERRAMENTAS, ANÁLISES E ESTUDO DE CASO

CRICIÚMA, JUNHO DE 2011

PEDRO PAULO ALEXANDRINO

PERÍCIA FORENSE APLICADA EM CELULARES COM SISTEMA OPERACIONAL SYMBIAN: FERRAMENTAS, ANÁLISES E ESTUDO DE CASO

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

CRICIÚMA, JUNHO DE 2011

PEDRO PAULO ALEXANDRINO

PERÍCIA FORENSE APLICADA EM CELULARES COM SISTEMA OPERACIONAL SYMBIAN: FERRAMENTAS, ANÁLISES E ESTUDO DE CASO

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. Fabrício Giordani (UNESC)

Prof. Esp. Sérgio Coral (UNESC)

A minha família, em especial minha mãe Beatriz e meu pai Taylor, pelo incentivo, exemplo e apoio concedido.

AGRADECIMENTOS

Agradeço primeiramente aos meus pais, pelo exemplo de vida, por me incentivar nos momentos mais difíceis e nunca me deixando desistir dos meus objetivos e sonhos.

Agradeço também aos meus professores, em especial ao professor Paulo, orientador deste trabalho, por me colocar sempre no caminho certo e disposição para ajudar em qualquer momento.

Aos meus amigos e colegas de graduação, pela amizade e experiência compartilhada durante todos esses anos de estudo.

Meus sinceros agradecimentos a todas as pessoas que de alguma maneira contribuíram para a realização deste trabalho.

"Não sabendo que era impossível, foi lá e fez"

(Jean Cocteau)

RESUMO

Objetivo: Aplicar técnicas computacionais forenses para a busca e análise de informações contidas em celulares**,** bem como, contribuir socialmente aumentando o leque de pesquisas sobre o tema. **Métodos:** pesquisa bibliográfica; elaboração de um estudo de caso fictício simulando a condução de uma pericia forense computacional em um telefone móvel; utilização da junção das metodologias DFRWS, Reith, Carr e Gunsch, SOP e NIST, porém utilizando a NIST como principal, aplicando onze etapas: autorização, identificação, preparação, estratégia de abordagem, coleta e preservação, aquisição, exame e análise, apresentação ou documentação, decisão, devolução das provas e reconstrução da cena do crime. **Resultados:** conseguiu-se estudar e aplicar os conceitos de pericia forense computacional, analisando os arquivos da memória interna e externa do celular, utilizando as ferramentas MobilEdit, Forensic Toolkit e PhotoRec. Ocasionalmente ocorreram falhas ao trabalhar com determinadas ferramentas, como por exemplo, a ferramenta MobilEdit utilizada para aquisição dos dados, que falhou ao recuperar todas as informações da memória interna. Outras ferramentas foram testadas, porém não obtiveram sucesso como essas citadas. Provas periciais foram encontradas no celular investigado podendo chegar a uma conclusão para o caso.

Palavras-chave: Segurança; Crimes Digitais; Perícia Forense; Celular.

ABSTRACT

Objective: To apply forensic computational techniques in order to the acquisition and analysis of information stored in cellphones, as well as to contribute socially, increasing the range of research on the subject. **Methods:** literature research; preparation of a fictional case study simulating the driving of a computer forensic in a mobile phone; use of the combination of the technologies DFRWS, Reith, Carr and Günsche, SOP, and NIST, but using NIST as the main methodology, applying eleven steps: identification, preparation, approach strategy, collecting and preservation, acquisition, examination and analysis, presentation and documentation, decision, returning the evidence and crime scene reconstruction. **Results:** We managed to study and apply the concepts of computer forensics, analyzing the files of internal and external memory of the phone, using the tools Mobiledit, Forensic Toolkit and PhotoRec. Occasionally failures occur when working with certain tools, such as the MOBILedit, a tool used for data acquisition, which failed to retrieve all the information from internal memory. Other tools have been tested, but did not succeed as those cited. Forensic evidence were found in the investigated cell may reach a conclusion to the case.

Keywords: Security, Computer Crime, Forensics, Mobile.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

ARM	*Advanced RISC Machine*
ASCII	*American Standard Code for Information Interchange*
CDMA	*Code Division Multiple Access*
DFRWS	*Digital Forensics Research Workshop*
D-AMPS	*Digital Advanced Mobile Phone System*
EUA	Estados Unidos da América
FCC	*Federal Communication Comission*
FCR	*Forense Card Reader*
FST	*Forensic Toolkit SIM*
GSM	*Global System for Mobile Communications*
HTML	*HyperText Markup Language*
ICCID	*Integrated Circuit Card ID*
IHCFC	*International Hi-Tech Crime and Forensics Conference*
IMSI	*International Mobile Subscriber Identity*
IMTS	*Improved Mobile Telephone System*
IOCE	*International Organization on Computer Evidence*
JTAG	*Test Action Group*
LCD	*Liquid Crystal Display*
MD5	*Message-Digest algorithm 5*
MIAT	*Mobile Internal Acquisition Tool*
MP3	*MPEG 1 Layer-3*
NIST	*National Institute of Standards and Technology*
NTFS	*New Technologies File System*

OPM	*Oxygen Phone Manager*
OS	*Operation System*
PDA	*Personal Digital Assistants*
PDC	*Personal Digital Cellular*
PIN	*Personal Identification Number*
RAM	*Random Access Memory*
ROM	*Read Only Memory*
RTF	*Rich Text Format*
SIM	*Subscriber Identity Module*
SO	Sistemas Operacionais
SMS	*Short Message Service*
SWGDE	*Scientific Working Group on Digital Evidence*
TDMA	*Time Division Multiple Access*
URL	*Uniform Resource Locator*
USB	*Universal Serial Bus*
USIM	*Universal Subscriber Identity Module*
WAP	*Wireless Application Protocol*
XLS	*eXtensible Stylesheet Language*
XML	*eXtensible Markup Language*

SUMÁRIO

1 INTRODUÇÃO

Os telefones celulares estão rapidamente se tornando uma necessidade para muitas pessoas ao redor do mundo, inclusive criminosos. Muitos oficiais de justiça consideram telefones celulares, como parte integrante do tráfico de drogas. Esta ligação tem motivado algumas famílias e escolas a proibir estes dispositivos. Além disso, os conselhos de liberdade condicional estão incluindo esses e outros dispositivos eletrônicos na lista de itens que não se pode possuir (CASEY, 2004, tradução nossa).

Apesar de compacto, estes dispositivos podem conter elementos de prova digital significativas, incluindo horários, memorandos, livros de endereços, e-mails, senhas, números de cartões de crédito e outras informações pessoais (VACCA, 2002, tradução nossa). Alguns dispositivos, tais como modelos Kyocera Qualcomm, combinam um Palm OS PDA com telefone celular para fornecer uma ampla gama de características e tipos de provas correspondentemente. Outros dispositivos portáteis são otimizados para aquisição de dados, tais como códigos de barras e medições científicas, por exemplo, tensão, temperatura aceleração. Além disso, alguns telefones celulares usam *Bluetooth* e outros protocolos sem fio para se comunicar com outros computadores próximos para formar redes de proximidade (CASEY, 2004, tradução nossa).

Muitos dispositivos portáteis já podem ser usados para troca de fotografias e acesso a Internet. Como a tecnologia se desenvolve, maiores taxas de transmissão de dados permitem que as pessoas possam transferir arquivos grandes e o uso de dispositivos portáteis na mesma forma como usamos atualmente sistemas de laptop. Este rápido desenvolvimento da computação móvel e tecnologia de comunicação criaram oportunidades para os criminosos e pesquisadores do assunto (KRAUSE; HEISER, 2002, tradução nossa).

As provas digitais estão se tornando importante, pois 80% dos processos judiciais em curso estão usando alguns tipos de prova digital que lhes são associados. Nos últimos anos, dezenas de assassinos foram condenados, em parte como um resultado de provas sobre os seus telefones celulares ou de suas vítimas. No domínio da ciência forense digital, ferramentas de software têm dominado o mercado na aquisição de provas digitais a partir de telefones móveis (BAGGILI; MISLAN; ROGERS, 2007, tradução nossa).

O celular pode ser de extrema importância na busca de evidências de um crime, pois o meliante pode fazer algumas ligações, ou troca de mensagens, gerando evidências para resolução do caso. Porém, as informações como, últimas ligações, mensagens, fotos, podem ser apagadas, dificultando a busca de pistas que auxiliam a resolução de um caso.

Perícia forense computacional pode ser entendida como busca, armazenamento preservado, análise relacional, e apresentação de evidências. Métodos científicos e ferramentas são utilizados para investigação, resultando as evidências (REITH; CARR; GUNSCH, 2002, tradução nossa).

De acordo com Wilkinson (2007, tradução nossa) existem algumas boas práticas para a utilização da perícia forense em celulares, que podem ser divididas em quatro princípios. O primeiro princípio proíbe que os dados contidos em um celular ou qualquer mídia de armazenamento possam ser alterados. O segundo princípio, afirma que o responsável pela perícia deve ser competente e capaz de prestar depoimento, explicando a importância e aplicações de suas ações. O terceiro princípio diz que o resultado de uma perícia feita por um especialista deve ser o mesmo, caso seja feito por outro especialista. O último princípio aborda que o gestor do caso tem responsabilidade global de garantir que os resultados levantados sejam respeitados.

Dessa forma, essa pesquisa realizou uma análise e explanação sobre métodos de busca de informações ou evidências resultando em um auxílio na busca de informações restritas em celulares.

1.1 OBJETIVO GERAL

Aplicar técnicas computacionais forenses para a busca e análise de informações contidas em celulares.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos desta pesquisa são:

a) entender e aplicar os princípios básicos de perícia forense computacional em aparelhos celulares;
b) documentar os aspectos que envolvem a análise de evidências em dispositivos móveis;
c) descrever e utilizar as ferramentas de perícia forense para obter evidências em aparelhos celulares;
d) definir um cenário para realizar os experimentos na busca por evidências.

1.3 JUSTIFICATIVA

Existem muitos benefícios gerados pelo avanço da tecnologia. Alguns como, computadores para diversas tarefas auxiliando e automatizando processos, comunicação globalizada, especialmente da Internet e muitos outros. Tudo isso, alimenta a paixão da

população pelo conhecimento e cultura. Contudo, esses benefícios são utilizados por algumas pessoas de maneira ilegal. Esse ato é chamado de crime digital, onde o indivíduo pode executar seu plano de várias maneiras, sem necessitar sair de casa. Contudo, a perícia forense computacional, estuda esse tipo de delito, trazendo métodos e soluções para se alcançar a resolução de um determinado caso.

Alguns agentes da lei reconhecem que evidências obtidas por meio de dispositivos digitais, podem contribuir muito na solução de certos crimes. Muitas vezes, são mais precisas, do que outros itens como, documentos, impressão digital e pegadas (SCHWEITZER, 2003, tradução nossa).

Segundo Casey (2004, tradução nossa) e Reyes (2007, tradução nossa) as informações referentes a um incidente, devem ser coletadas, as evidências devem ser identificadas, extraídas, documentadas e preservadas. Desta forma, as evidências podem ser correlacionadas para a reconstrução dos acontecimentos relacionados ao incidente em questão.

A evidência digital em sua síntese pode ser definida como qualquer dado armazenado ou transmitido em um dispositivo eletrônico, que pode provar ou negar a teoria de como ocorreu um crime. Os campos magnéticos e pulsos eletrônicos podem ser coletados e analisados utilizando ferramentas adequadas. Contudo, a evidência remete a confiabilidade ao trabalho do perito (REITH; CARR; GUNSCH, 2002, tradução nossa).

Pela extrema facilidade de um indivíduo possuir um celular, esse acesso pode e traz problemas relacionados muitas vezes a crimes, como ameaças, falsos sequestros extorquindo dinheiro dos familiares, mensagens e ligações no narcotráfico, muitas vezes dentro de ambientes, como presídios onde a utilização de celular é proibida.

Perícia forense para celulares é extremamente importante na busca de informações que podem ajudar na rastreabilidade de um crime ou até mesmo obter informações que

possam impedir um crime. Ela se torna ainda mais importante quando não existem evidências concretas na coleta de informações investigativas.

Essa pesquisa tem como ponto positivo, facilitar o entendimento dos processos envolvidos a analise forense, mostrando detalhadamente os passos para obtenção de informações que podem ser recuperadas nos celulares, como ligações e mensagens apagadas pelo usuário do dispositivo.

Alguns sistemas operacionais para celulares como Windows Mobile, Android, Symbian serão avaliados para que os mesmos sejam focados no objeto de estudo. Da mesma forma, alguns programas serão utilizados para realização e simulação de cenários para que a perícia forense busque as evidências e transforme em informação.

Existem poucas fontes de pesquisas relacionadas à perícia forense em aparelhos celulares. Perante essa e outras informações que mostram a extrema importância na obtenção de evidências digitais, esse estudo tem a finalidade de realizar um estudo de caso com a aplicação de ferramentas e metodologias da perícia forense em celulares, tendo como resultado a extração da informação para avaliação e por fim gerar um laudo da perícia.

1.4 ESTRUTURA DO TRABALHO

Esse trabalho está dividido em seis capítulos. Sendo que no Capítulo 1, é apresentada a introdução ao trabalho proposto, os objetivos gerais e específicos, e a justificativa para realização desse projeto.

Os crimes digitais, classificação de crimes digitais, evidências digitais e importância da segurança da informação podem ser encontrados no Capítulo 2.

No Capítulo 3 a perícia forense computacional, celulares, sistemas operacionais para celulares, perícia forense em celulares, os aspectos a serem analisados em um celular,

metodologias forenses, uso de celulares em crimes digitais e a importância de periciar um celular, são apresentados.

Os trabalhos correlatos são apresentados no Capítulo 4. O primeiro comenta sobre as técnicas computacionais no auxílio à perícia forense na análise de evidências. O segundo trabalho foca na perícia forense em softwares livres. O terceiro demonstra uma proposta de uma metodologia de coleta de indícios para em ambiente Windows. O quarto trabalho relata procedimentos computacionais no auxílio à perícia forense aplicada em *Web Browsers*. Já o último retrata a perícia forense computacional aplicada em ambientes NTFS.

O trabalho desenvolvido, juntamente com o estudo de caso são apresentados no Capítulo 5.

2 CRIMES DIGITAIS

Nos últimos anos, uma nova classe de cenas de crimes tem se tornado mais prevalente nos domínios eletrônicos ou digitais, principalmente em ciberespaço. Serviços de justiça criminal em todo o mundo estão sendo confrontados com uma necessidade crescente de investigar crimes cometidos, total ou parcialmente, na Internet ou outros meios digitais.

Segundo Casey (2004, tradução nossa), Vacca (2005, tradução nossa) e Reyes (2007, tradução nossa) recursos e procedimentos são necessários para efetivamente procurar e preservar todos os tipos de provas digitais. Estas provas variam desde dados comuns, como fotos e documentos ilegais, até dados criptografados, usados para uma variedade de atividades criminosas. Mesmo nas investigações que não utilizam primariamente evidências eletrônicas, em algum momento dispositivos podem ser investigados, permitindo novas descobertas que devem ser analisadas.

Os computadores e dispositivos móveis têm inspirado novos tipos de conduta, tais como *hackers* agindo de várias formas ilegais. Uma vez que esses atos exigem alguma especialização a partir de um computador e anos de experiência, os *hackers* obtendo essa informação sentem-se glamorosos, pois consideram como heroico e não criminal. Na era eletrônica, algumas pessoas comportam-se de forma ilegal, mas cada vez com mais imaginação (MOHAY et al, 2003, tradução nossa).

Alguns crimes digitais são difíceis de serem resolvidos. Como por exemplo, no caso de pornografia infantil, quando o suspeito pode alegar que não teve a intenção de baixar um arquivo contendo fotos, no momento que estava sendo rastreado remotamente, ou até mesmo, no levantamento de evidências relacionadas a um crime (REYES, 2007, tradução nossa).

Cada vez mais, os criminosos estão usando a tecnologia para facilitar seus crimes e evitar a apreensão. Criam novos desafios para os advogados, juízes, agentes da lei, os examinadores forenses e os profissionais de segurança corporativa. Criminosos organizados ao redor do mundo estão usando tecnologia para manter os registros, comunicação, obtendo informações de computadores sobre um policial e sua família para intimidar e desencorajar evitando confrontamento. Alguns criminosos mais experientes na área digital têm invadido sistemas restritos para alterar seus registros legais, e até mesmo monitoram a comunicação interna das autoridades. Como resultado dessas infrações, grande quantidade de drogas, pornografia infantil e outros materiais ilegais trafegam com o auxilio da *Internet*. (MCQUADE, 2009, tradução nossa).

Segundo Galvão (2009) qualquer ação realizada utilizando um dispositivo digital como instrumento ou objeto do delito, é chamado de crime digital.

2.1 CLASSIFICAÇÃO DOS CRIMES DIGITAIS

Segundo Castro (2003) os crimes digitais devem ser classificados quanto ao objetivo material, e não ao fato do uso de dispositivo ser considerado indiferente ao direito penal. Podendo ser classificados em três modalidades:

a) crime de informática puro: é a ocorrência de violação do sistema de computador, físico ou técnico ao equipamento e componentes. Como por exemplo, ações provocadas por vândalos, contra a integridade física do sistema;
b) crime de informática misto: é a realização do uso de um sistema computacional para operar transferências bancárias ilícitas pela Internet. São todas as ações em que o agente visa um bem diverso da informática

juridicamente protegido, contudo, o sistema de informática é a ferramenta imprescindível a sua consumação;

c) crime de informática comum: o dispositivo digital é somente para uso do sistema para cometer um delito tipificado na lei penal. Como crime com envolvimento de pornografia infantil com fotos via e-mail, sites, entre outros.

2.2 EVIDÊNCIAS DIGITAIS

A complexidade dos casos forenses realizado em computadores na obtenção de provas tem aumentado significativamente ao logo dos anos com o aumento da sofisticação dos sistemas de computador autônomo, e a uma maior utilização da Internet. A Internet fornece um quadro com crescimento em aplicações sofisticadas, que são vulneráveis ao computador, como por exemplo, o comércio eletrônico, um canal de comunicação permitindo a ocorrência crime podendo ser planejados, geridos ou facilitados (PROSISE; MANDIA, 2003, tradução nossa).

No passado a perícia forense tinha uma tendência de confiar em provas que consistiam essencialmente em discos independentes ou arquivos do disco, porém os casos mais recentes têm contado cada vez mais com provas eletrônicas colhidas a partir de uma variedade de fontes. Como por exemplo, em caso de pirataria, além de informações providas do disco rígido, podemos encontrar evidências em registros telefônicos, redes sociais, rastreando outros endereços permitindo a averiguação de outros discos ou dispositivos correlacionados. Contudo, provas obtidas a partir dos discos magnéticos de cada um dos computadores individuais, continuam a ser importantes e muitas vezes cruciais, pois os

procedimentos evoluíram permitindo mais compreensão, gerenciamento e uma análise mais completa (WILKINSON, 2010, tradução nossa).

Como resultado da continuação da utilização de meios magnéticos pela grande maioria de computadores pessoais, algumas vezes os mesmos podem estar danificados, requerendo auxilio de um setor de serviços que vem crescendo ultimamente, que trabalham na recuperação de informações dos meios de armazenamento, para fins de investigação forense ou até mesmo apenas para recuperação de dados pessoais. Esse tipo de serviço se estende a outras mídias de armazenamento, como fitas magnéticas e tecnologias ópticas (MOHAY et al, 2003, tradução nossa).

Segundo Casey (2004, tradução nossa), Philipp, Cowen e Davis (2010, tradução nossa), Reyes e Wiles (2007, tradução nossa) as evidências digitais podem desempenhar um papel importante em uma ampla gama de crimes, incluindo homicídio, estupro, rapto, abuso infantil, fraude, roubo, invasão de computadores, terrorismo, entre outros. Embora um número crescente de criminosos esteja utilizando computadores e rede de computadores, poucos são os investigadores bem versados nas questões de provas relacionadas com provas digitais. Como resultado, essas provas muitas vezes são esquecidas, pelo fato de serem obtidas de forma incorreta, e analisadas de forma ineficaz.

Dispositivos móveis como celulares e PDAs se tornaram essenciais nas áreas de negócio e pessoal, sendo que são extremamente suscetíveis de conter informação pessoal considerável, como evidências eletrônicas e informações sobre atividades de uma pessoa, que pode ter um valor significativo em investigação criminal. Existem algumas diferenças entre o tratamento destes dispositivos e manipulação de computadores e discos, causados pela diferença de tecnologias. Em particular, há pouca padronização entre os dispositivos deste tipo porque são mais recentes, portanto menos experiência de como lidar com eles. No entanto, como resultado de sua penetração no mercado em rápido crescimento, os dispositivos

móveis como uma questão de rotina, difundida em casa, no trabalho, automóvel, armazenando informações do cotidiano, apresentam grande potencial para investigação forense computacional (SCHWEITZER, 2003, tradução nossa).

Casey (2004, tradução nossa) afirma que crimes digitais podem ser úteis em uma ampla grade de investigações criminais, incluindo crimes sexuais, a pedofilia, tráfico de drogas entre outros. Além disso, os processos civis podem depender de provas e descobertas digitais, tornando parte da rotina de litígios em matéria civil. Informações podem ajudar a determinar quando os eventos ocorreram, onde as vítimas e os suspeitos foram, e quem comunicou com quem, e pode até mostrar a sua intenção de cometer um crime. Como por exemplo, de um crime cometido por Robert Durall, que manteve no histórico de seu navegador da Internet uma busca de: matar esposa + acidente mortes + sufocar + assassinato, antes de matar a esposa. Em outro caso, as mensagens de correio eletrônico foram à única ligação entre a investigação e o assassino e sua vítima. Muitas vezes a informação armazenada em um computador, é a única pista para uma investigação.

2.3 IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO

Vive-se em um mundo onde a informação é muito importante, e independentemente do seu formato é uma grande riqueza para a organização moderna, sendo vital para qualquer tipo de classe ou instituição.

A tecnologia da informação e comunicação tem evoluído de forma muito rápida, permitindo que as organizações possam tomar decisões precisas, utilizando um sistema de informação. Contudo se torna inviável uma organização progredir sem um sistema de informação, porém é preciso um mecanismo de segurança para que o acesso à informação seja controlado (MOREIRA, 2008, tradução nossa).

De acordo com Galvão (2009) a legislação Brasileira vem sendo motivo de discussões em crimes digitais, pois grande parte da população transportou suas vidas para as redes virtuais, resultando no crescimento de fatos e ocorrências jurídicas, da mesma forma que ocorre no mundo real. Essas ocorrências estão na aplicação de normas comerciais, transações on-line, mensagens por e-mail, validação jurídica de um documento eletrônico, privacidade e a integridade do usuário.

Segundo Laureno e Moraes (2005) o domínio da informação sempre teve grande importância para as corporações do ponto de vista estratégico e empresarial. Pois dispor da informação correta, no momento adequado, resulta em uma decisão de forma ágil e eficiente. Portanto, com a evolução dos sistemas de informação, ganhou-se mobilidade, inteligência e real capacidade de gestão.

No passando a segurança da informação era mais simples, pois as informações contidas em inúmeros papéis podiam ficar guardadas fisicamente em locais seguros. Hoje, com a chegada da tecnologia da informação e comunicação, a segurança ficou mais complexa, pois a maiorias dos computadores conectam-se a Internet e visse versa. Além disso, os dados digitais são portáteis, tornando esse delito um atrativo para os ladrões de informações (MONTEIRO, 2003).

Outros fatores que devem ser levados em consideração em relação à segurança da informação são as inúmeras situações de insegurança que podem afetar os sistemas de informação como incêndio, alagamentos, problemas elétricos, poeira, fraudes, uso inadequado dos sistemas, guerras, sequestros e muitos outros. Dessa forma, podemos dizer que não existe segurança absoluta. É preciso agir no sentido de descobrir quais são os pontos vulneráveis e a partir daí, avaliar os riscos e as consequências, para conseguir ao máximo manter a informação segura e inalterável (MARCIANO, 2006).

Moreira (2008) afirma que muitas empresas continuam sem dar valor à questão da segurança da informação, pelo fato de que o preço é muito alto, portanto o melhor caminho é reduzir ao máximo quaisquer riscos às informações, seguindo um caminho único de manter a integridade e a disponibilidade dos sistemas de informação.

Marcella e Greenfield (2002, tradução nossa) explicam que para se implantar uma forma segura de assegurar a informação dentro de uma organização, devemos ficar atentos para algumas questões, como, uma boa análise de riscos, a definição da política de segurança, finalizando com um plano de contingências.

A análise de riscos visa identificar os pontos de riscos onde a informação está exposta, identificando quais pontos necessitam de maior empenho e proteção. A política de segurança é a formalização explícita de quais ações serão realizadas em sentido único de garantir a segurança e disponibilidade dos mesmos, sendo muito importante, pois é nela que estão as regras necessárias para o uso seguro dos sistemas de informação. Os planos de contingência também possuem um papel muito importante, pois descrevem o que deve ser feito em caso de problemas com as informações.

Normalmente as pessoas são a parte mais frágil quando o assunto é segurança da informação. As soluções técnicas não completam totalmente sua segurança. Desta forma, torna-se necessário que os conceitos pertinentes à segurança sejam compreendidos e seguidos por todos dentro da organização, até mesmo sem distinção de níveis hierárquicos. Pois quando são identificados os riscos que as informações estão expostas, deve-se iniciar um processo de segurança física e lógica, com a finalidade de alcançar um nível tolerável de segurança (LAURENO; MORAES, 2005).

A segurança da informação lida com a proteção das informações de empresas ou pessoas. Podendo ser afetada por fatores comportamentais de ambiente ou infraestrutura, pessoas mal intencionadas com objetivo de furtar, destruir ou modificar tal informação.

A falta de segurança pode causar prejuízos significativos, e muitas vezes irreversíveis. A principal ameaça à segurança são as pessoas. Hoje, existem inúmeros problemas relacionados à interferência humana, não de forma direta, ligados a ações fraudulentas, ou demais situações em que o funcionário tem o objetivo de prejudicar a sua empresa, pelo contrário, a grande maioria dos incidentes de segurança ocorre por falta de informação, de processos de orientação aos recursos humanos (MOREIRA, 2008).

Outro fator que está relacionado à falta de segurança, está vinculado à evolução rápida das tecnologias, pois em pouco tempo, até mesmo os computadores domésticos ganham recursos em potencial e em capacidade de armazenamento. Ao mesmo tempo em que essa evolução proporciona inúmeros benefícios, traz como bagagem novos riscos e ameaças virtuais.

Laureno e Moraes (2005) defendem que para uma informação seja considerada segura, o sistema que o administra deve respeitar os seguintes critérios:

a) autenticidade: garante que a informação ou o usuário da mesma é autêntico;
b) não repúdio: não é possível negar, no sentido de dizer que não foi feito, uma operação ou serviço que alterou ou criou uma informação, e não é possível recusar o envio ou recepção de uma informação ou dado;
c) legalidade: garante a legalidade jurídica da informação, a aderência de um sistema à legislação, e as características das informações que possuem valor legal dentro de um processo de comunicação, onde todos os envolvidos estão de acordo com as cláusulas do contrato ou a legislação nacional ou internacional vigente;
d) privacidade: foge do aspecto de confidencialidade, pois uma informação pode ser considerada sigilosa, mas não privada. Uma informação privada precisa poder ser visualizada e alterada exclusivamente pelo seu dono. Garante ainda,

que uma informação não deverá ser disponibilizada para outras pessoas. Para este caso é posto o caráter de confiável à informação. É a capacidade de realizar ações em um sistema sem que seja identificado o usuário;

e) auditoria: rastreabilidade dos diversos passos de um negócio ou processo, identificando os participantes, os locais e horários de cada etapa. A auditoria adiciona a confiabilidade da empresa e é responsável pela ajuste da empresa às políticas legais e internas.

Na visão de Albuquerque e Ribeiro (2002), Krause e Tipton (1999) e Galvão (2009) há três princípios básicos para garantir a segurança da informação, já que os negócios estão cada vez mais dependentes das tecnologias:

a) confidencialidade: a informação somente pode ser acessada por pessoas explicitamente autorizadas. É a proteção de sistemas de informação para prevenir que pessoas não autorizadas obtenham acesso;

b) disponibilidade: a informação deve estar disponível no momento em que a mesma for necessária;

c) integridade: a informação deve ser recuperada em sua forma original, no momento em que foi armazenada. É a proteção dos dados.

Uma boa prática de prevenir problemas relacionados ao segurança da informação é a utilização de softwares de segurança e prover soluções no espaço de tempo mais curtos possível. Devendo estar atrelada a um amplo programa de segurança, com ferramentas, configurações, instalação de soluções, criações de projetos específicos e recomendações de uso, como Antivírus, Firewall, sistemas Antspam entre outros. Para tanto, não basta comprar as soluções, os produtos de segurança direcionados à prevenção são bons, mas são apenas uma parte do conceito geral. Não é o bastante ter os melhores produtos de segurança, é preciso mantê-los atualizados, instalando novas versões, aplicando pacotes de correção entre

outros, para então interpretar suas informações e responder efetivamente aos alertas registrados por eles (MOREIRA, 2008).

Pinheiro (2007) afirma que os principais focos jurídicos da segurança da informação são:

a) estar em conformidade com as leis vigentes;
b) proteger as empresas de riscos e contingências legais relacionados ao mau uso da informação, vazamento de informações confidenciais, uso não autorizado, fraudes e invasão de privacidade;
c) atender aos preceitos da Constituição Federal do Código Civil, Código Penal, Lei de Direitos Autorais, Lei de Softwares, Consolidação de Leis do Trabalho entre outros dispositivos nacionais e internacionais;
d) na hipótese de investigação, deve garantir que a empresa possa usar as provas coletadas de forma preventiva, possa praticar monitoramento, sem que isso gere riscos legais;
e) garantir que os contratos estejam adequados relacionados às responsabilidades nos níveis de serviços acordados e aos termos de confidencialidade exigidos;
f) fazer com que respostas a incidentes atuem com segurança jurídica, de forma legítima.

Dentro de uma corporação, todos os colaboradores devem ser responsabilizados por cumprir a Política de Segurança da Informação da empresa. Para tanto é necessário que exista ciência formal do documento, seja com assinatura física ou eletrônica. A etapa de divulgação e conscientização dessa Política é fundamental tanto para proteção da empresa no sentido de que capacitou seus profissionais no correto uso da tecnologia, quanto para prevenção de incidentes. Dessa forma, os mesmos serão responsáveis por seus atos (PINHEIRO, 2007).

No novo capítulo são apresentados os conceitos da perícia forense computacional, celulares, os sistemas operacionais para celulares, algumas ferramentas e metodologias forenses.

3 PERÍCIA FORENSE COMPUTACIONAL

Perícia forense computacional refere-se aos métodos utilizados por profissionais para, obtenção, preservação, análise e documentação de provas com o objetivo de reuni-las, para reconstruir o cenário no momento da fraude, utilizando em um processo judicial as evidências encontradas. As provas podem ser as mais diversas possíveis, como e-mails, arquivos de registros, conhecidos como logs, arquivos temporários com informações pessoais, conexões abertas, processos em execução, entre outras evidências que possam existir na máquina, mas para serem aceitas num processo jurídico, devem ter sido obtidas de forma lícita (MARCELLA; GREENFIELD, 2002; JOHNSON, 2005, tradução nossa).

Segundo Vacca (2002, tradução nossa), Volonino e Anzaldua (2008, tradução nossa) de forma resumida, perícia forense computacional, pode ser entendida como coleta, preservação, análise e apresentação de evidências. Consiste no uso de métodos científicos e ferramentas para desenvolver a pesquisa de forma correta. Resultando conclusões sobre o incidente investigado, apresentando os fatos e as evidências.

De acordo com Krause e Heiser (2002, tradução nossa) a análise pericial é o processo usado pelo investigador para encontrar informações valiosas, e localização e extração de dados proeminentes em uma investigação. A análise pericial pode ser dividida em duas partes: análise física e análise lógica.

Durante a análise física, todos os dados da mídia de armazenamento são investigados, mesmo os que estão apagados. É preciso começar a investigação por essa parte, quando se está investigando o conteúdo de um disco rígido danificado ou que não se tenha conhecimento da origem. Depois que o software criador da imagens extrair a mesma, os dados podem ser verificados por três processos principais: uma pesquisa sequencial, processo

de localização e extração e uma amostra de espaço livre de arquivos. Todas as operações são realizadas na imagem criada do dispositivo ou na cópia das provas restaurada.

Na análise lógica, o conteúdo de cada partição é pesquisado com um sistema operacional que consiga entender o sistema de arquivos. É neste momento que ocorre a maioria dos problemas de manipulação das provas. O investigador deve estar ciente de todas as medidas que serão realizadas na imagem restaurada, tendo com objetivo básico, proteger as provas contra qualquer tipo de alteração.

Na visão de Marcella e Menendez (2008, tradução nossa) a perícia forense computacional pode ser dividida em quatro partes: identificação, preservação, análise e preservação.

A identificação avalia dentre os vários fatores abrangidos no caso. É necessário formar com clareza quais são as conexões ressaltantes, como datas, nomes de pessoas, empresas, órgãos públicos, entre outros. Discos rígidos e memórias de dispositivos podem trazer a sua origem, com grandes quantidades de informações, após a recuperação de dados.

Em relação à preservação, todas as provas precisam ser legítimas, para terem sua validade jurídica. Dessa forma, todo o processo relacionado à coleta das mesmas, podendo ser no elemento lógico ou físico, deve seguir normas internacionais. É preciso partir do principio de que existe outra parte envolvida no caso que deverá pedir a contraprova sobre os mesmos elementos.

A análise será propriamente a pesquisa. Onde os filtros de informações já foram transpostos e podem-se deter especificamente nos elementos relevantes ao caso em questão. É preciso ser muito profissional nos termos da prova legítima. Onde consiste numa demonstração e inquestionável dos rastros e subsídios da comunicação entre partes envolvidas e seu teor, além de trilhas, datas, e histórico de disco utilizado.

A apresentação aborda no ajuste das evidências dentro do formato jurídico, como o caso poderá ou será tratado. Os advogados ou juiz do caso poderão enquadrá-lo na esfera civil ou criminal, ou mesmo em ambas. Desta forma, quando se tem a certeza material em relação às evidências, deve-se atuar em conjunto com uma das partes acima descritas para a apresentação das mesmas.

3.1 CELULARES

Os celulares são dispositivos digitais, onde a comunicação é feita por ondas eletromagnéticas, que permite transmissão bidirecional de dados e voz (CERQUEIRA FILHO; PINTO, 2004).

O conceito de celular pode ser definido como um transmissor de baixa potência, onde a frequência pode ser reutilizada dentro de uma área geográfica determinada. Um telefone celular é um dispositivo sem fio que conecta a uma rede telefônica pública comutada e é oferecido ao público em geral, por um comum transportador ou utilidade pública.

Após a Segunda Guerra Mundial, muitas cidades estavam em ruínas. Suas infraestruturas precisavam de reconstrução, necessitando de comunicação entre pessoas e regiões. Como os americanos não foram fisicamente afetados puderam liderar o movimento de expansão da comunicação. Possuindo laboratórios como Bell Telephone, que tinha um grande grupo de engenheiros e cientistas, a Motorola com crescimento significativo durante a guerra, outros centro de pesquisas e a demanda dos consumidores. Em outras palavras, os Estados Unidos possuíam a capacidade de fabricação (FARLEY, 2005, tradução nossa).

Os primeiros dispositivos móveis foram criados nos Estados Unidos da América (EUA) pela empresa AT&T, e regulamentado por todo o país pela Federal Communication Comission (FCC). Sendo que era o único sistema móvel de telefonia dos EUA. Já na Europa,

cada País criou o seu próprio sistema de celular, causando problemas, pois não era possível, por exemplo, que países pudessem se comunicar (FARLEY, 2005, tradução nossa).

Os dispositivos celulares passaram por três gerações com diferentes tecnologias. A primeira geração foi a voz analógica, a segunda foi a voz digital e a terceira voz digital e transferência de dados (FARLEY, 2005, tradução nossa).

Na primeira geração, na década de 1950, o sistema era realizado por radiotelefones móveis, que eram fornecidos aos militares que utilizavam esporadicamente. Possuíam um canal único para transmissão e recepção de voz, muito bem empregados em carros de polícia, taxi entre outros.

Na década de 1960, a tecnologia foi melhorada com a criação do Improved Mobile Telephone System (IMTS), que utilizava um transmissor de alta potência, localizado no topo das montanhas, possuindo dois canais, um para transmissão e outro para recepção. Não foi muito eficaz pelo fato de que havia poucos canais para atender a demanda de usuários, e os canais não suportavam muitas comunicações simultâneas.

Da mesma forma que não houve padronizações na primeira geração, na segunda e na terceira geração dos dispositivos móveis, que são de telefonia digital e no caso da terceira, transferência de dados, também não existiu padrão. A consequência é que atualmente existem vários sistemas de telefonia móvel com tecnologia digital, como tecnologia GSM, TDMA ou D-AMPS, CDMA, PDC e PSC 1900.

O serviço celular funciona a partir da divisão de uma região geográfica em pequenas áreas denominadas de células. Sendo que cada uma utiliza um conjunto de sinais de rádio frequência e um conjunto de rádio transmissões e receptores de baixa potência (CERQUEIRA FILHO; PINTO, 2004).

Os celulares de uma determinada área geográfica possuem uma estação base, que é responsável pela realização das chamadas recebidas ou enviadas aos móveis localizados em

cada uma das células, sendo elo entre conexões de móveis com o restante do sistema. Quando um usuário se locomove, de uma cidade para outra, por exemplo, o sinal do dispositivo passa automaticamente de uma célula para outra, sem sofrer falhas ou interrupções no sinal (CERQUEIRA FILHO; PINTO, 2004).

3.2 SISTEMAS OPERACIONAIS PARA CELULARES

Segundo Wang, Yao, Yang, e ZHU (2001, tradução nossa) os sistemas operacionais de celulares, são sistemas microprocessados no qual o computador é completamente dedicado ao dispositivo ou sistema que o mesmo controla. Diferente de um computador normal, utilizados para diversos fins, um sistema operacional para celular, desempenha um conjuntos de serviços predefinidos, normalmente com requisitos particulares. Desta forma, já que o sistema é dedicado a serviços específicos, com a engenharia pode-se aprimorar o projeto reduzindo tamanho, recursos computacionais e custo do produto.

No mercado para dispositivos, existe uma grande pressão para que os mesmos tenham um crescente aumento de novas funcionalidades devido à convergência digital. Eles necessitam cada vez mais ter diferentes funcionalidades, fazendo com que exista um aumento na complexidade dos sistemas embarcados, pois os celulares permanecem com a premissa de que têm uma funcionalidade peculiar, por exemplo, em um *smartphone* jogar vídeo game ou executar músicas em formato MP3, é possível, mesmo assim o fator da sua existência é permitir comunicação e essa funcionalidade nunca deve fracassar (WANG; YAO; YANG; ZHU 2001, tradução nossa).

Com a crescente expansão da Internet, algumas empresas migraram suas aplicações de uma arquitetura convencional cliente/servidor para aplicações *web*, permitindo o acesso de todos via um navegador como o *Internet Explorer* ou *Firefox*. Com a finalidade

de dar mobilidade a estas aplicações, que se buscou desenvolver a Internet móvel ou Internet wireless. No caso do celular, a navegação é feita por meio de um *microbrowser*, de maneira que ele se adapte às limitadas condições do aparelho celular. Assim como o navegador normal, o micronavegador utiliza um endereço Uniform Resource Locator (URL) para contatar um servidor específico. O retorno é processado no servidor do aplicativo é traduzido pelo browser que apresenta ao usuário.

Existem microbrowsers, com o WAP, OpenWave, Microsoft, Avantgo, Go, Palm eOpera, porém o WAP é o protocolo mais aproveitado em celulares. A vantagem desse tipo de arquitetura é fato de que aplicações podem ser construídas em cima de aplicações existentes na Internet sem precisarem ser implementadas nos aparelhos dos clientes e, quando necessário, sua atualização pode ser realizada a qualquer momento, afetando somente o servidor. O maior problema dessa arquitetura está na qualidade da Internet móvel, pois ela requer uma rede eficaz durante todo o tempo, e se a taxa de transmissão for baixa, a aplicação será prejudicada. De qualquer forma, pode ser utilizada em e-commerce, entretenimento, bem como outros aplicativos que contam com a conectividade oferecida pela rede existente.

Os softwares escritos para sistemas de celulares são muitas vezes chamados firmware, e armazenado em uma memória Read Only Memory (ROM) ou memória flash, ao invés de um disco rígido.

Existem muitos Sistemas Operacionais (SO) para dispositivos móveis no mercado, como o SymbianOS, Windows Mobile da Microsoft, Android, entre outros.

A seguir serão demonstradas as características principais do Symbian OS.

3.2.1 SymbianOS

De acordo com Harrison (2007, tradução nossa) SymbianOS é um sistema cooperativo criado para ser utilizado por dispositivos móveis com suporte a câmeras fotográficas, wireless, *Bluetooth*, entre outras funções. Possui um ambiente gráfico bastante simples, e atualmente é utilizado na maioria dos recentes modelos de celulares dos grandes fabricantes.

Uma das grandes preocupações do SymbianOS é de evitar ao máximo o desperdício dos recursos do celular, como por exemplo, bateria e memória. Portanto ele conta com diversos mecanismos que são eficientes ao tratar com esses problemas.

Existem algumas vantagens em utilizar o SymbianOS, como por exemplo: é um sistema operativo mais estável e seguro, em relação aos seus concorrentes; utiliza muito bem todas as áreas do aparelho, como memória, processador, entre outras; permite instalação de softwares de terceiros; possui recursos para gerenciar e utilizar pouca bateria e memória; é baseado em padrões de comunicação de dados; é um sistema de baixo custo.

O que torna o SymbianOS um sistema operacional tão versátil, é o fato de que permite o desenvolvimento de aplicativos em diversas linguagens como Symbian C/C++, JavaME, FlashLite, Perl, Python, Ruby, Lua, Acelerômeter e QT.

Segundo Martinelli (2009) Symbian é uma sistema operacional que tem como alvo o mercado de *smartphones*. Para tanto, contém muitos recursos relacionados a gerenciamento de memória e execução de multitarefas, permitindo operações eficientes e seguras dos recursos limitados que caracterizam os dispositivos móveis.

De acordo com Luiz e Maas (2010) o Symbian é um software de 32 bits e multitarefas destinado à dispositivos móveis e smartphones. Seus padrões são abertos e visa uma robustez inigualável, trazendo uma forte garantia em relação a integridade, segurança dos

dados do usuário, fazendo o OS funcionar sem falhar, além de ter uma interface totalmente dirigida ao usuário.

Luiz e Maas (2010) afirmam que o SymbianOS foi baseado em cinco pontos principais: pequenos dispositivos móveis, estar disponível para uma grande parte do mercado, conexão *wireless*, variedade de plataformas abertas para implementações de terceiros e produtos.

A família Symbian é dividida em duas plataformas que de certa forma são incompatíveis:

a) S60: desenvolvido pela Nokia, também encontrado em alguns aparelhos da LG e Samsung.
b) UIQ: encontrado em aparelhos da Sony-Ericsson e da Motorola.

S60 é o mais utilizado entre essas duas famílias, pelo simples fato de que a Nokia vende muito mais (LUIZ; MAAS, 2010).

O Symbian é o sistema operacional que possui *drivers* e bibliotecas, enquanto o S60 e o UIQ são somente interfaces que rodam sob ele, incluindo aplicativos e bibliotecas de desenvolvimento. Caso fosse feito uma comparação com o Linux, o Symbian seria composto pelas bibliotecas básicas do sistema e o Kernel, enquanto o S60 e o UIQ seria K Desktop Environment (KDE) e o GNU Network Object Model Environment (GNOME), interfaces que rodam sob ele.

3.2.1.1 Kernel

Segundo Luiz e Maas (2010) o Kernel é responsável pelo controle do sistema operacional. Gerencia desde a funcionalidade de comunicação entre os processos até as estruturas de sincronismo e threads.

As bibliotecas chamadas de Dynamic Link Libraries (DLL) também estão na composição do Kernel. Elas estão carregadas na memória do sistema, possuindo funções básicas para as aplicações. Essas DLLs são muito utilizadas no Symbian OS. Tendo um total de quase cem bibliotecas em cada telefone móvel comum.

Existem dois tipos de DLL:

a) estáticas: são coleções de classes e de funções básicas do sistema, ou seja, a base de bibliotecas do sistema operacional;
b) polimórficas: funcionam como *plug-ins* para as aplicações.

3.2.1.1.1 Processos e Threads

O SymbianOS é um sistema operacional multitarefas. Sendo que um aplicativo pode ter várias theads, porém não é recomendado pelo fato do custo que é originado para gerência destes recursos. Com a finalidade de evitar esse tipo de situação, possui um *framework* com finalidade de comunicação assíncrona denominado *Active Objects*. Os *Objects* tem a intuito de simular a existência de várias threads.

Os processos realizados possuem espaço de memória reservado. Tornando impossível que outro processo acesse a área diretamente por questões de segurança. Todos os processos possuem pelo menos uma thread para cada, e se existir mais de uma, todas acessam o espaço de memória referente ao processo que as contém.

3.2.1.1.2 Estados dos processos

De acordo com Luiz e Maas (2010) o estado de um processo pode ser definido pelo processo momentâneo. Na figura 1 podemos visualizar os estados:

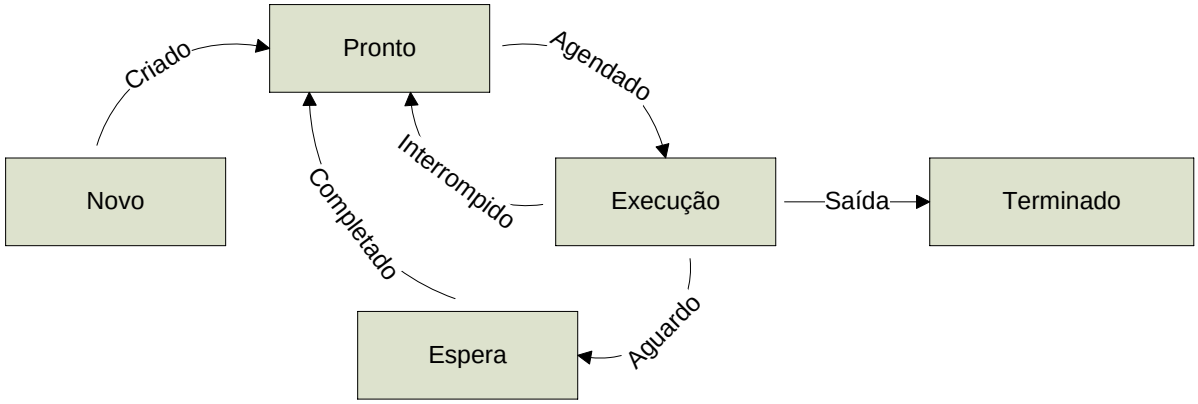

Figura 1. Processos e Threads
Fonte: LUIZ; MAAS. (2010)

O estado Novo é o processo que está sendo criado e tem sua seção de texto edificado a partir do código em um programa. Essa sessão é alocada na memória em forma de pilhas inicializando componentes de hardware.

O estado “Pronto” é o processo que está pronto para execução em um processador à espera de execução.

O estado “Execução” é o processo que está sofrendo execução no processador, gerenciando o hardware e executando as instruções promovidas.

O estado “Espera” é o processo que está aguardando um evento para seguir. Esse evento pode ser como uma interrupção para finalização de um pedido de saída ou entrada.

O estado Terminado é o processo acabado. Foi finalizada a execução no processador deixando de ser um processo armazenando com um dado.

É importante salientar que um processo não pode se transferir do estado Novo para Execução prontamente. Um processo também não pode estar esperando um evento e se transferir para o estado encerrado diretamente. Finalizando, é importante entender que enquanto um processo poder ser executado em apenas um processador, muitos processos podem estar nos estados de Espera ou Pronto.

3.2.1.2 Gerência de Memória

Luiz e Maas (2010) afirma que uma plataforma operada pelo Symbian OS permite vários tipos de memórias que seguem: RAM, ROM, Flash Disk interno e cartões de memória.

A memória RAM é utilizada durante a execução das aplicações. É nela que os programas e o sistema operacional alocam memória durante e execução dos processos e fluxos de execução. Normalmente os celulares possuem uma quantidade bem pequena de memória RAM.

Apenas uma parte do sistema operacional SymbianOS fica armazenada na memória ROM, tanto quanto o código de boot (processo de inicialização), drivers (pequenos programas de comunicação entre SO e Hardware) e código específico do hardware. Pode-se dizer que a memória ROM é exclusiva do sistema, pois o usuário não pode manipular nem escrever dados nesta memória.

Em relação ao Flash Disk, ele representa memórias adicionais que funcionam como um disco rígido para escrita e leitura de dados, que pode ser feita pelo usuário ou sistema de arquivos do sistema operacional.

Já os cartões de memória funcionam como discos de armazenamento, só que removíveis, desta maneira é possível alterar a capacidade de armazenamento de um dispositivo.

3.2.1.3 Processador

Segundo Luiz e Maas (2010) os celulares têm sua arquitetura de hardware baseado em microprocessadores assíncronos Advanced RISC Machine (ARM) de 32 bits. O

tamanho reduzido e o baixo consumo de energia fazer parte de suas características principais, sendo requisitos do Symbian OS, com desempenho entre 100 e 200 MHz.

3.3 PERÍCIA FORENSE EM CELULARES

Perícia forense e análise forense computacional estão se tornando atividades com grande importância na sociedade, devido a onipresença de dispositivos digitais e das redes de computadores e comunicações, onde os mesmo são utilizados em operações pessoais ou de trabalho.

Por meio dos dispositivos móveis e microcomputadores, temos acessos a servidores web, servidores de e-mail, entre outros servidores, que quer saibamos ou não, temos acesso a um conjuntos de computadores que estão escondidos no coração dos sistemas integrados que usamos em casa, no trabalho e no lazer.

Enquanto muitas das novas formas de comportamento ilegal ou antissocial crescem de forma contínua, a análise forense pode proporcionar oportunidades muito maiores de localização de provas eletrônicas, pois quanto maior a quantidade de evidências for encontrada, melhor será a precisão na resolução de um caso (MOHAY et al, 2003, tradução nossa).

Segundo Mohay et al (2003, tradução nossa) relatórios sobre as operações forenses da Price Waterhouse Coopers, que é uma das maiores prestadoras de serviços profissionais do mundo, que presta os serviços de auditoria, consultoria e outros serviços para todo tipo de empresas e no mundo, destaca que o existe um grande aumento de incidência de casos em que telefones celulares e PDAs, desempenham um papel e que exigem uma investigação forense. O relatório menciona que uma ferramenta chamada Zert, desenvolvida

pelo Instituto Forense, dos Países Baixos, é uma das poucas ferramentas desenvolvidas especificamente para investigar PDAs e celulares.

O Instituto Forense dos Países Baixos, também desenvolveu programas relacionados, tais como Cards4Labs Tulp, que são usados para leitura de cartões inteligentes e telefones celulares, respectivamente.

Os pré-requisitos para uma investigação de tais dispositivos móveis, como qualquer análise forense, é um levantamento de circunstâncias que permitam a apreensão e pesquisa do dispositivo, e que tenha uma autorização judicial. É fundamental ao investigador que exista uma restrição de acesso a outras pessoas para preservação, ou seja, para garantir a manutenção de todas as provas em potencial, assim garantindo que a alimentação do aparelho não seja interrompida, evitando perda de qualquer informação no armazenamento volátil.

Na primeira fase, é importante identificar a natureza dos requisitos de energia do dispositivo, e evitar a remoção de baterias, pelo menos até que todas as informações residentes na memória volátil sejam extraídas. Caso seja possível ter acesso a carregadores de bateria, o mesmo também deve ser aproveitado.

No caso dos celulares, uma vez que a memória volátil seja preservada, o Subscriber Identity Module (SIM), do cartão inteligente, do coração do dispositivo, pode ser analisado utilizando ferramentas de análise de cartões inteligentes, tais como o Card4Tools.

No entanto, alguns dispositivos celulares não utilizam cartões SIM, neste caso o fabricante pode ser contatado para permitir a extração dos dados.

Mohay et al (2003, tradução nossa) apresenta um relato da análise de telefones celulares, em especial, os cartões inteligentes que sem a qual a maioria dos celulares são inúteis. Seguem abaixo quatro fontes de evidências forenses disponível em investigações envolvendo esse tipo de análise:

a) fonte 1: equipamentos se houver, conectado ao dispositivo móvel;

b) fonte 2: dispositivo de comunicações móveis;

c) fonte 3: a rede sem fio em que estão as funções do dispositivo móvel;

d) fonte 4: a rede subsequentes se houver, que acessa o chamador.

A segunda e a terceira fonte são as mais importantes. As duas fontes podem fornecer acesso às seguintes informações:

a) números chamados, números que chamaram, marcação de tempos para cada chamada, duração da chamada do chamador, e receptor de localização;

b) endereço da lista telefônica;

c) mensagens de voz;

d) mensagens Short Message Service (SMS);

e) possivelmente, um diário ou agenda.

3.4 ASPECTOS A SEREM ANALISADOS EM CELULARES

A comunidade digital forense enfrenta um desafio constante para ficar a par das mais recentes mudanças tecnológicas que podem ser utilizadas para expor pistas relevantes em uma investigação (JANSEN; AYERS, 2007, tradução nossa).

Segundo Mohay (2003, tradução nossa) o estudo forense em um celular pode ser entendido como uma ciência de recuperar provas digitais a partir de um telefone celular, em condições predefinidas usando métodos aceitos.

Quando um celular é encontrado durante uma investigação, surgem novas questões: O que deve ser feito sobre a manutenção do celular em posse? Como deve ser tratado o dispositivo? A chave para responder a essas perguntas é a compreensão das características de hardware e software de um telefone celular.

Os celulares são projetados para a mobilidade, possuem tamanho compacto, alimentados por bateria e são leves. A maioria dos celulares tem um conjunto básico de características comparáveis à capacidade. Possui um microprocessador, memória apenas para leitura (ROM), memória de acesso aleatório (RAM), um módulo de rádio, um processador de sinal digital, um microfone e alto-falante, uma variedade de chaves de hardwares e interfaces, e um display de cristal líquido (LCD). O Sistema Operacional (SO) do dispositivo é realizado na ROM, que, com as ferramentas apropriadas, normalmente pode ser apagado e reprogramado eletronicamente. A RAM, para alguns modelos pode ser usada para armazenar dados do usuário, que é mantida ativa por baterias, cuja falência ou esgotamento causa perda de informação (JANSEN; AYERS, 2007, tradução nossa).

Já os celulares mais modernos, estão equipados com microprocessadores que reduzem o número de arquivos de apoio necessários e incluem a capacidade de memória considerável, suportando cartões de memória removíveis ou periféricos especializados. As comunicações sem fios, tais como infravermelho e ou *Bluetooth* também podem ser incorporados no dispositivo (JANSEN; AYERS, 2007, tradução nossa).

Dispositivos diferentes têm diferentes características técnicas e físicas, como por exemplo, tamanho, peso, velocidade do processador e capacidade de memória. Os dispositivos também podem utilizar diferentes tipos de capacidades de expansão para fornecer funcionalidade adicional. Além disso, as capacidades do telefone celular, por vezes, incluem as de outros dispositivos como PDAs, como sistemas de posicionamento global, e as câmeras. Em geral, eles podem ser classificados como telefones básicos que são principalmente de voz simples e dispositivos de comunicação de mensagens. Telefones avançados que oferecem recursos e serviços adicionais para multimídia como *smartphones* ou telefones *high-end* que mesclam as capacidades de um telefone avançado com as de um PDA. Dispositivos mais avançados também fornecem a capacidade de executar as mensagens multimídia, navegar na

Web, troca de correio eletrônico, bate-papo ou uso de mensagens instantâneas. Eles também podem fornecer aplicações avançadas que trabalham com *hardware* embutido, como uma câmera.

3.4.1 Ferramentas Forenses

A situação com ferramentas de software forense para telefones celulares é consideravelmente diferente dos computadores pessoais. Embora os computadores pessoais sejam concebidos como sistemas de propósito gerais, os celulares são concebidos mais como aparelhos que executam um conjunto de tarefas predefinidas.

Os fabricantes de telefone celular também tendem a confiar em diversos sistemas operacionais proprietários em vez da abordagem mais normalizada encontrados em computadores pessoais. Devido a isso, a variedade de kits de ferramentas para aparelhos móveis é muito variada e vasta gama de dispositivos sobre os quais eles operam normalmente é reduzido para plataformas distintas, para uma linha de produto do fabricante, uma família de sistema operacional, ou um tipo de arquitetura de hardware. Os ciclos de lançamento do produto curto são a norma para telefones celulares, obrigando os fabricantes de ferramentas atualizarem suas ferramentas continuamente para manter a cobertura atual.

De acordo com Jansen e Ayers (2007, tradução nossa), ferramentas forenses podem adquirir dados de um dispositivo de duas formas: Aquisição física ou aquisição lógica. Aquisição física implica um *bit-by-bit*, que é a cópia de toda parte física, por exemplo, um chip de memória, enquanto a aquisição lógica implica um *bit-by-bit* cópia de objetos de armazenamento lógico, como por exemplo, diretórios e arquivos, que residem em uma unidade lógica, por exemplo, uma partição de sistema de arquivos. A diferença reside na distinção entre a memória de como pode ser visto através de um processo com as facilidades

do sistema operacional, ou seja, uma visão lógica, já a visão física, a memória pode ser vista na sua forma bruta pelo processador e outros componentes de hardware relacionados.

A aquisição de Física tem vantagens sob a aquisição lógica, pois permite que arquivos apagados e todo o resto possam ser encontrados, como por exemplo, na memória ou espaço não alocado do sistema de arquivos, a ser examinado, que caso contrário iria desaparecer. A imagem dos dispositivos deve ser extraída, interpretadas, decodificadas e traduzidas para descobrir os dados presentes. O trabalho é tedioso e demorado para executar manualmente. As Imagens do dispositivo físico podem ser importadas em uma ferramenta para automatizar a análise e elaboração de relatórios, no entanto, apenas alguns instrumentos adequados para a obtenção de imagens de celular estão disponíveis no momento. A aquisição lógica, embora mais limitado do que uma aquisição física, tem a vantagem de que as estruturas de dados do sistema são normalmente mais fácil para uma ferramenta extrair e fornecer uma organização mais natural de entender e usar durante a análise. Se possível, fazer os dois tipos de aquisição é preferível, a aquisição física antes de uma aquisição lógica.

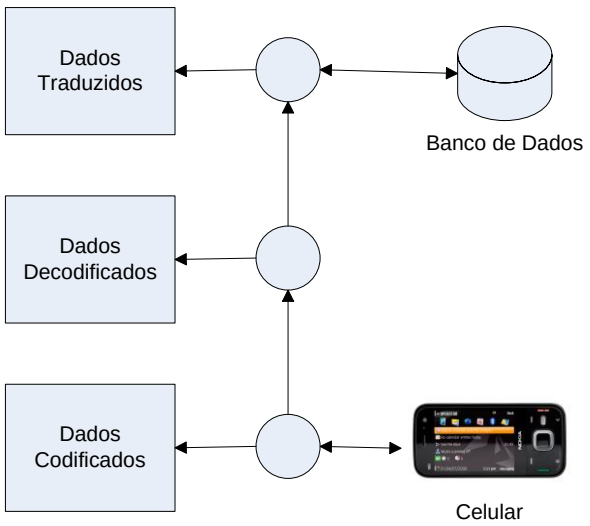

Figura 2. Aquisição de Dados, Decodificação e Tradução.
Fonte: JANSEN; AYERS. (2007)

A maioria das ferramentas forenses para telefones celulares utilizam aquisição de dados logicamente, usando protocolos comuns de dispositivo para sincronização, comunicações e depuração, conforme Figura 2. Algumas ferramentas podem também serem capazes de adquirir dados fisicamente para determinadas classes de telefones. Comandos AT, Sync ML, e os outros protocolos listados são comumente utilizados na aquisição lógica de telefones celulares. Pelo fato de que aparelhos podem suportar múltiplos protocolos, uma ferramenta pode empregar vários deles em sucessão para adquirir a maior gama de dados disponíveis. Mesmo se uma ferramenta usa vários protocolos para um aparelho especial, todos os dados disponíveis não poderão ser recuperados (JANSEN; AYERS, 2007, tradução nossa).

Enquanto a maioria das ferramentas forenses apoia uma ampla gama de exames, aquisição e funções de relatórios, algumas ferramentas focam em um subconjunto. Diferentes ferramentas podem também suportar interfaces diferentes. Por exemplo, cabo IrDA, *Bluetooth* ou serial, para adquirir os conteúdos do dispositivo. A aquisição por meio de um cabo de interface geralmente produz resultados superiores aos de outras interfaces. No entanto, em certas condições, uma interface sem fio, como *Bluetooth* ou infravermelhos, pode servir como uma alternativa razoável, por exemplo, quando o cabo correto não está prontamente disponível e as questões forenses de usar outras interfaces são entendidas.

Independentemente da interface utilizada, a vigilância dos potenciais problemáticos associados a fundamentação forense, relacionado, por exemplo, ao *Bluetooth*, tipicamente envolve uma troca de informações como a estação de trabalho forense para configurar a conexão, que é retida no dispositivo. Ativando a conexão e emparelhar o dispositivo para a estação de trabalho também requer entradas de tecla no telefone.

A maioria das ferramentas de software forense aborda uma ampla gama de dispositivos aplicáveis, lidam com as situações mais comuns de investigação, e exigem um nível modesto de habilidade para operar. A Tabela 1 dá uma visão geral das ferramentas

disponíveis utilizados nas investigações de telefone celular, e identifica as instalações que prestam: aquisição, análise, ou de informação. Para cobrir a mais ampla gama de telefones móveis e SIM, um conjunto de várias ferramentas é necessário. As capacidades das ferramentas listadas estão melhorando constantemente e podem ser ligeiramente diferentes da descrição dada (JANSEN; AYERS, 2007, tradução nossa).

Em seguida seguem algumas ferramentas utilizadas na perícia forense em aparelhos celulares:

Ferramentas	Funções	Dispositivo Alvo
Forensic Card Reader	Aquisição e Relatórios	SIMs
ForensicSIM	Aquisição, Análise e Relatórios.	SIMs e USIMs
SIMCon8	Aquisição, Análise e Relatórios.	SIMs e USIMs
SIMIS	Aquisição, Análise e Relatórios.	SIMs e USIMs
USIMdetective	Aquisição, Análise e Relatórios.	SIMs e USIMs
BitPIM	Aquisição e Análise	Dispositivos CDMA usando chip sets Qualcomm
Oxygen PM (forensic version)	Aquisição, Análise e Relatórios.	Dispositivos Nokia
Oxygen PM for Symbian (forensic version)	Aquisição, Análise e Relatórios.	Dispositivos com Symbian
PDA Seizure9	Aquisição, Análise e Relatórios.	Palm OS, Windows Mobile/Pocket PC, e Black Berry devices
Pilot-Link	Aquisição	Dispositivos Palm OS
Function Target Devices Cell Seizure10	Aquisição, Análise e Relatórios.	TDMA, CDMA, e dispositivos GSM. SIMs e USIMs
CellDEK	Aquisição, Análise e Relatórios.	GSM e CDMA. SIMs e USIMs
GSM .XRY	Aquisição, Análise Relatórios.	GSM e CDMA. SIMs e USIMs
MobilEdit!	Aquisição, Análise e Relatórios.	GSM. SIMs
PhoneBase	Aquisição, Análise e Relatórios.	GSM. SIMs e USIMs
Secure View	Aquisição, Análise e Relatórios.	TDMA, CDMA, e GSM SIMs

TULP 2G	Aquisição e Relatórios	GSM
Forensic Toolkit	Análise	Imagem
PC Inspector File Recovery	Aquisição e Análise	Unidade de disco ou flash.
Symbian Tool	Aquisição e Análise	Dispositivos com Symbian
MIAT	Aquisição	Dispositivos com Symbian
Photorec	Aquisição e Análise	Unidade de disco ou flash.
BackupToGo	Aquisição	Dispositivos com Symbian
GSimReader	Aquisição e Análise	SIMs
USB Image Tool	Aquisição	Cartão de Memória

Figura 3. Ferramentas Forenses

3.4.1.1 Ferramentas SIM

Algumas ferramentas forenses lidam exclusivamente com cartão SIM. Essas ferramentas executam uma leitura direta do conteúdo de um módulo através de um leitor de SIM, ou oposição a uma leitura indireta através do aparelho de telefone. A riqueza e abrangência dos dados adquiridos variam de acordo com as capacidades e funcionalidades da ferramenta. A maioria dos instrumentos SIM adquirem exclusivamente os seguintes dados: International Mobile Subscriber Identity (IMSI), Integrated Circuit Card ID (ICCID), últimos números discados, mensagens SMS e Localização da Informação (JANSEN; AYERS, 2007, tradução nossa).

3.4.1.1.1 Forense Card Reader (FCR)

Forense Card Reader (FCR) é uma ferramenta que fornece os meios para extrair dados de SIMs. FCR não gera um arquivo, mas a saída dos dados adquiridos em um formato eXtensible Markup Language (XML) que pode ser visualizado com o editor apropriado. FCR

consiste no software proprietário e um leitor de *smart card* USB necessários para a aquisição. Não são fornecidos relatórios personalizáveis (JANSEN; AYERS, 2007, tradução nossa).

3.4.1.1.2 Forensic Toolkit SIM (FST)

O Forensic Toolkit SIM (FST) é uma ferramenta forense que fornece os meios para extrair dados de SIMs. O dossiê é armazenado em um formato proprietário e pode ser extraído em HTML ou arquivo RTF em formato Word. É necessário um cabo USB para operar o software em um computador desktop. O terminal de aquisição FST, uma unidade autônoma, duplica o conteúdo do alvo SIM para um conjunto de arquivos de armazenamento de dados, ou seja, o mestre de armazenamento de dados do cartão de armazenamento. A análise dos dados pode ser realizada através do cartão de armazenamento de dados com o leitor de cartão ForensicSIM PC, ou seja, leitor de cartões compatível, conectado a um PC rodando o aplicativo de análise ForensicSIM. Um MD5 fornece a proteção da integridade dos dados gerados. O FST permite a importação de arquivos de casos arquivados e pesquisas básicas do arquivo de dados adquiridos (JANSEN; AYERS, 2007, tradução nossa).

3.4.1.1.3 SIMCon

SIMCon é uma ferramenta forense que fornece os meios para extrair dados do SIM e USIMs. O dossiê tem um formato proprietário, mas podem ser exportados para um formato de texto padrão ASCII. Hardware adicional, por exemplo, dongle USB, leitores de cartão proprietário, não são necessárias para a aquisição. SIMCon adquire dados de um SIM através de um PC e leitor de cartões compatível e usa um *hash* Secure Hash Algorithm (SHA1) para proteger a integridade dos dados gerados caso. SIMCon fornece a capacidade de

importar arquivos de casos arquivados e exportação de dados específicos para fora em um relatório final (JANSEN; AYERS, 2007, tradução nossa).

3.4.1.1.4 SIMIS

SIMIS é uma ferramenta forense que fornece meios para extrair dados do SIM e USIMs. O dossiê é gerado em um formato de arquivo HTML. Possui um adicional que fornece um arquivo de caso mais detalhado em um formato padrão de texto ASCII. Um dongle USB é necessário para operar o software em um computador desktop. SIMIS adquire informações a partir de um SIM através de um PC com leitor de cartões compatível e gera hashes MD5 e SHA2 dos dados adquiridos. SIMIS fornece a capacidade de criar notas do relatório, a importação de casos arquivados, pesquisa de dados adquiridos e administrar PINs. A função de busca pode ser realizada em qualquer SIMs arquivado na pasta do programa (JANSEN; AYERS, 2007, tradução nossa).

3.4.1.1.5 USIMdetective

USIMdetective é uma ferramenta de aquisição SIM que tem a capacidade de adquirir, analisar e produzir relatórios a partir de qualquer cartão SIM ou USIM usando um PC com leitor compatível. Elementos adquiridos podem ser exibidos em um formato textual ou hexadecimal. USIMdetective utiliza um mecanismo interno de hashing para garantir a integridade do processo. Imagens de verificação de integridade dos arquivos são criadas a cada aquisição para se proteger contra a adulteração de dados. Hashes MD5 e SHA1 garantem que o arquivo original adquirido seja compatível com o arquivo, caso fosse reaberto.

USIMdetective fornece vários tipos de relatórios de saída (JANSEN; AYERS, 2007, tradução nossa).

3.4.1.2 Ferramentas Handset

Algumas ferramentas forenses lidam exclusivamente com aparelhos para a aquisição de sua memória interna. Essas ferramentas, por vezes, resultam de ferramentas destinadas aos PDA e, portanto, são úteis com telefones inteligentes que incorporam sistemas operacionais com uma herança à PDA, tais como dispositivos Palm OS e Windows Mobile. Essas ferramentas geralmente excluem a capacidade de adquirir dados de SIMs e usar uma leitura direta. Abaixo está uma breve descrição de algumas ferramentas criadas para a aquisição de memória a partir de dispositivos móveis com recursos de celular (JANSEN; AYERS, 2007, tradução nossa).

3.4.1.2.1 PDA Seizure

PDA Seizure é uma ferramenta de software forense que fornece os meios para extrair dados de dispositivos móveis rodando Palm OS, Windows CE, e RIM OS. O dossiê tem um formato proprietário e pode ter saída em um formato de arquivo HTML. A aquisição ocorre por meio de um cabo, IrDA ou interface *Bluetooth*. Nenhum hardware adicional é necessário. Embora a ferramenta possa ser usada com telefones inteligentes, o kit de ferramentas é voltado para dispositivos diferentes de celulares. PDA Seizure tem características que incluem a capacidade de realizar uma aquisição lógica e, para determinados dispositivos, uma aquisição física, proporcionando visualização de memória interna, bem como arquivos e bancos de dados. Além disso, utiliza criptografia para evitar

adulterações e modificação de dados. Também fornece examinadores com a capacidade de criar relatórios personalizados, importar arquivos caso arquivado, marcador de resultados significativos, e pesquisar os dados adquiridos (JANSEN; AYERS, 2007, tradução nossa).

3.4.1.2.2 Pilot-link

Pilot-link é uma organização não forense de software de código aberto originalmente desenvolvido para a comunidade Linux como um meio de transferência de dados entre máquinas Linux e Palm OS. Pilot-link fornece a capacidade de extrair RAM, ROM e arquivos individuais presentes em dispositivos Palm OS. Dois programas de interesse para examinadores forenses são Getram e Getrom, que, respectivamente, recuperam o conteúdo físico de memória RAM e ROM de um dispositivo. Outro programa útil é o Pilot-xfer, que fornece um meio para adquirir o conteúdo de um dispositivo lógico. Nem um arquivo do caso geral, cálculo de hash, integridade, nem instalação de relatório personalizáveis são fornecidos (JANSEN; AYERS, 2007, tradução nossa).

3.4.1.2.3 Oxygen Phone Manager (OPM)

A versão forense de Oxygen Phone Manager (OPM) é uma variante do produto de gestão de telefones com o mesmo nome, que trabalha principalmente em telefones Nokia. A versão forense difere da versão não judicial, proibindo a modificação do dispositivo de destino. OPM fornece examinadores com a capacidade de extrair dados de aparelhos celulares operando sobre a rede GSM. OPM não permitem aos examinadores exportar um arquivo do caso geral, no entanto, os dados adquiridos são armazenados em vários arquivos (por exemplo, Agenda, SMS, e Galeria) que se correlacionam com a função relacionada. OPM não

protege os dados adquiridos através de funções hash. Os dados adquiridos podem ser exportados em vários tipos de formato compatível.

Existe uma versão para Symbian OS, com alvo em celulares e *smartphones* que utilizam o sistema operacional Symbian. As características acima mencionadas de OPM são igualmente aplicáveis à OPM para dispositivos com Symbian OS (JANSEN; AYERS, 2007, tradução nossa).

3.4.1.2.4 BitPim

BitPim é um software de código aberto disponível sob a licença GNU General Public License. É um programa de gerenciamento de telefone que permite a visualização e manipulação de dados principalmente de telefones celulares CDMA por vários fabricantes. BitPim não permitem aos examinadores exportar ou salvar um arquivo do caso geral, no entanto, os dados adquiridos são armazenados em vários arquivos, por exemplo, Agenda, SMS, e do Sistema de Arquivos, e podem ser exportados em formatos comuns para fins de notificação. BitPim não protege os dados adquiridos através de funções hash (JANSEN; AYERS, 2007, tradução nossa).

3.4.1.2.5 BackupToGo

Backup2Go é uma aplicação para realizar backup em arquivos de dispositivo móvel com sistema operacional Symbian. O aplicativo foi construído usando linguagem de programação C++ para o mecanismo de aplicação e Qt Quick para a interface do usuário. Para seu funcionamento é preciso copiar um arquivo com extensão .sys para dentro da memória

externa do dispositivo e executar. Após a execução, os dados da memória interna são copiados para a externa, podendo ser analisados fora do dispositivo.

3.4.1.2.6 Photorec

PhotoRec é software de recuperação de dados concebido para recuperar arquivos perdidos, incluindo vídeo, documentos e arquivos de discos rígidos, CD-ROMs e imagens perdidas da memória da câmera digital. PhotoRec ignora o sistema de arquivos e vai atrás dos dados subjacentes, assim ele continuará funcionando mesmo se o seu sistema de arquivos de mídia tenha sido severamente danificado ou reformatado.

PhotoRec é um software livre multiplataforma e é distribuído sob a GNU General Public License. PhotoRec é um programa que acompanha o TestDisk, um aplicativo para recuperar partições perdidas em uma ampla variedade de sistemas de arquivo.

Para obter mais segurança, PhotoRec utiliza o acesso somente leitura para lidar com o disco ou cartão de memória prestes a recuperar dados perdidos.

3.4.1.2.7 MIAT

Mobile Internal Acquisition Tool (MIAT) é software forense de código aberto projetado para adquirir dados de memória interna, sem usar nenhum tipo de hardware externo.

MIAT é uma aplicação que penetra nas APIs do sistema operacional do celular a fim de obter um acesso somente leitura à memória interna do sistema de arquivos.

Durante sua execução, MIAT adquire mensagens, contatos, arquivos, entre outros, para o cartão de memória removível. No final da execução, uma imagem lógica dos dados será armazenada no volume de armazenamento removível escolhido.

3.4.1.2.8 Symbian Tool

Symbian Tool é um software que permite realizar várias tarefas em um dispositivo com sistema operacional Symbian. Realiza tarefas como backup, restauração e limpeza.

3.4.1.2.9 PC Inspector File Recovery

PC Inspector File Recovery é um programa de recuperação de dados com suporte para FAT 12/16/32 e NTFS. Ele recupera arquivos com a hora e data original, mesmo quando uma entrada de cabeçalho não está mais disponível. Em sistemas FAT, o programa encontra partições automaticamente, mesmo se o setor de boot ou FAT foram apagados ou danificados. PC Inspector File Recovery oferece uma interface fácil de usar que irá analisar o dispositivo e automaticamente criar arquivos que podem ser recuperados disponíveis a partir de uma pasta excluídos" em uma árvore de navegação estilo Explorer.

3.4.1.2.10 Forensic Toolkit

Forensic Toolkit (FTK) é reconhecido como alto padrão em software de computação forense. Esta é uma ferramenta válida em casos judiciais, pois proporciona investigações de ponta em forense digital, tais como: análise, descriptografia e software de quebra de senha, tudo dentro de uma interface intuitiva e personalizável. O FTK foi construído para ser prático, analítico e de escala empresarial. As suas principais características de funcionamento variam desde criação de imagens, análise de registros, decodificação de arquivos até recuperação de senhas.

3.4.1.2.11 EnCase Forensic

EnCase é uma ferramenta destinada aos profissionais forenses que necessitam de coleta de dados eficiente e investigações em um processo defensável. Permite adquirir dados de uma ampla variedade de dispositivos, resultando em relatórios detalhados de suas descobertas, tudo isso mantendo a integridade das evidências. Com ele se pode criar uma imagem exata do disco ou mídia original, gerando valores de hash MD5 para arquivos de imagens relacionadas. Com isso, mantem todas as evidências intactas para uso em processos judiciais.

3.4.1.2.12 USB Image Tool

USB Image Tool é um software que possui função de criar cópias de segurança gerando arquivos de imagem de dispositivos USB e cartão de memória. É preciso apenas selecionar o dispositivo e começa a realizar um backup.

O software reconhece automaticamente os dispositivos conectados em seu microcomputador e ainda possui um botão muito chamado “Rescan” que serve para quando você conecta um novo dispositivo com o USB Imagem Tool já aberto.

3.4.1.3 Ferramentas Integradas

Vários kits incorporam os recursos de ambas as ferramentas SIM e o telefone com uma estrutura unificada. A vantagem é que os resultados dos exames podem aparecer dentro do mesmo relatório gerado. Essa vantagem desaparece se outra ferramenta é usada para

qualquer dispositivo, como no caso de um aparelho especial, não poderia ser suportada pela ferramenta (JANSEN; AYERS, 2007, tradução nossa).

3.4.1.3.1 Cell Seizure

Cell Seizure é um conjunto de ferramentas de software forense que fornece os meios para extrair dados de GSM, CDMA, TDMA e aparelhos celulares com SIM. O expediente é em um formato proprietário e dados do caso podem ter uma saída em qualquer formato ASCII ou HTML. A aquisição ocorre por meio de um cabo, IrDA ou interface *Bluetooth*. Cell Seizure também permite a aquisição direta de cartões SIM com o leitor de cartão incluído RS-232 SIM. O pacote vem completo com cabos e drivers para telefones compatíveis, bem como a aplicação de software. Características Cell Seizure incluem a capacidade de realizar uma aquisição lógica e física, proporcionando visualização da memória interna, bem como processos individuais e bases de dados. O dossiê também é criptografado, evitando manipulação e modificação de dados. Esse kit fornece examinadores com a capacidade de criar relatórios personalizados e observa o relatório, importar arquivos caso arquivados, marcar resultados significativos, e pesquisar os dados adquiridos (JANSEN; AYERS, 2007, tradução nossa).

3.4.1.3.2 CellDEK

CellDEK é projetado para adquirir dados de telefones celulares operando em redes GSM e não GSM, PDAs, cartões SIM e de mídia baseados em memória flash. O terminal CellDEK contém incorporado um PC *touchscreen*, cabos de dados para vários dispositivos, PC com SC leitor de cartão SIM e um leitor de cartão de memória protegido contra gravação.

É muito bem embalado em uma caixa resistente para transporte. A unidade fornece a capacidade de se conectar a telefones celulares e PDAs, através de um cabo, IrDA ou *Bluetooth*. As aquisições são armazenadas no disco rígido do CellDEK e podem ser movidos ou copiados para um *pendrive* USB. Todos os dados são individualmente criptografados usando o algoritmo MD5 para garantir que a integridade dos dados pode ser verificado. CellDEK gera arquivos de relatório em formato HTML, contendo todos os dados recuperados. Relatórios podem ser personalizados com logotipos da empresa e detalhes do caso (JANSEN; AYERS, 2007, tradução nossa).

3.4.1.3.3 GSM. XRY

GSM. XRY é uma ferramenta de software forense que fornece os meios para extrair dados de GSM e não GSM, aparelhos celulares e cartões SIM / USIM. Um cabo USB é necessário para operar o software. O GSM XRY fornece uma interface para os cabos dongle e dispositivo, e interfaces para *Bluetooth* e IrDA. O pacote vem completo com cabos e drivers para telefones compatíveis, bem como a aplicação de software. Dados obtidos a partir de dispositivos de telefonia celular são armazenados na propriedade, formato XRY e não pode ser alterado, mas pode ser exportado em formatos externos e visto com aplicativos de terceiros. GSM. XRY criptografa os dados do caso e compara as assinaturas digitais de consistência quando previamente armazenado os dados do caso é reaberto para exame. Além disso, os arquivos caso pode ser bloqueado e protegido por senha, proporcionando uma camada extra de segurança contra a alteração. GSM. XRY fornece a capacidade de criar relatórios personalizados, importar arquivos de casos arquivados e realizar pesquisas sobre os dados adquiridos (JANSEN; AYERS, 2007, tradução nossa).

3.4.1.3.4 MOBILedit! Forense

MOBILedit! Forense da Compelson Labs é uma aplicação que fornece os meios para adquirir dados logicamente de dispositivos GSM ou não GSM, e cartões SIM. A ferramenta é baseada no software não forense do telefone de gestão do mesmo nome. Os dados do telefone pode ser adquirido via cabo, *Bluetooth* ou IrDA, e através de um leitor de cartões compatível para SIMs. Os dados adquiridos são armazenados em um formato proprietário mad e podem ser exportados para XML. MOBILedit! fornece a capacidade de criar relatórios personalizados, importar caso arquivados e realizar pesquisas em pastas específicas. MOBILedit! não protege os dados adquiridos através de cálculos de valor de hash (JANSEN; AYERS, 2007, tradução nossa).

3.4.1.3.5 PhoneBase 2

PhoneBase 2 da Prever Systems Ltd. fornece os meios para adquirir dados de GSM e aparelhos celulares não GSM e dados contidos em cartões SIM. PhoneBase 2 usa o mecanismo do MOBILedit! de aquisição para o apoio de celulares, mas complementa com suas próprias instalações de aquisição em cartões SIM. Um dongle USB é necessário para operar o software. Os dados podem ser adquiridos via cabo, *Bluetooth*, IrDA ou um leitor de cartões compatível para SIMs. Os dados adquiridos são armazenados em um formato de banco de dados comum e protegidas contra violação através de um segurança PhoneBase (PBS) de arquivos. PhoneBase 2 fornece examinadores com a capacidade de criar relatórios personalizados, importar arquivos de casos arquivados e realizar pesquisas sobre vários casos (JANSEN; AYERS, 2007, tradução nossa).

3.4.1.3.6 Secure View

Secure View é uma ferramenta comercial, derivada de um software de gestão da empresa DataPilot, que fornece examinadores com a capacidade de extrair dados de aparelhos celulares operando em GSM e não GSM. As versões recentes do Secure View também podem adquirir os dados do cartão SIM usando um leitor compatível. Secure View não permitem aos examinadores exportar um arquivo do caso geral, no entanto, dados obtidos são armazenados em vários arquivos, por exemplo, a lista de endereços, SMS, gráficos e áudio, que se correlacionam com a função relacionada. O pacote vem completo com cabos e drivers para telefones compatíveis, e software do aplicativo. Secure View não protege os dados através de funções hash. No entanto, os dados podem ser protegidos por senha, permitindo apenas acesso autorizado. Secure View fornece um motor de busca que permite que um subconjunto dos dados adquiridos para serem analisados e à capacidade de importar dados de caso pré-existente (JANSEN; AYERS, 2007, tradução nossa).

3.4.1.3.7 TULP2G

TULP2G, segunda geração é uma ferramenta forense de código aberto do Instituto Forense Holanda, que fornece os meios para adquirir dados de celulares GSM e não GSM e dispositivos SIMs. Os dados podem ser adquiridos através de um cabo, *Bluetooth* ou IrDA interface. Leitura SIMs requer leitor de cartões compatível com o smart. TULP2G gera um conjunto de dados brutos em formato XML, que pode ser convertido para um formato legível usando folhas de estilo XSL incorporado. *Hashes* SHA1 e MD5 são criados durante o expediente inteiro, garantindo a integridade dos dados adquiridos. TULP2G fornece a

capacidade de criar um relatório sobre elementos de dados selecionados ou o arquivo caso inteiro e importar arquivos de casos arquivados (JANSEN; AYERS, 2007, tradução nossa).

A seguir podemos comparar algumas metodologias forenses.

3.5 METODOLOGIAS FORENSES

Com o intuito de dar credibilidade à perícia forense computacional em frente à jurados, algumas metodologias foram criadas para serem usadas como guias do processo investigativo, definindo passos a serem seguidos pelos peritos, independentemente do sistema computacional ou de ferramentas e softwares utilizados (BERNARDO, 2006).

Contudo, os procedimentos a serem realizado pelo perito forense podem ser diferentes de acordo com os sistemas e aparatos tecnológicos envolvidos. A falta de métodos específicos de acordo com a tecnologia usada enfraquecia a credibilidade das provas mediantes os casos judiciais.

Basicamente, as metodologias além de permitir o compartilhamento de ações e experiências sobre investigações comuns, elas podem ser usadas para o desenvolvimento de aplicações de novas metodologias adequadas a determinados inquéritos, através de questões sobre técnicas e procedimento a serem utilizados e fornecimento de suporte a prática da perícia.

3.5.1 Metodologias DFRWS

Proposta em 2001, utilizando passos para análise forense digital como processo linear. Foi elaborada por Gary Palmer no primeiro Digital Forensics Research Workshop (DFRWS).

Esse modelo é formando por sete etapas que seguem abaixo:

a) identificação: consiste na determinação de itens, componentes e possíveis dados associados com o incidente. Representa o método por meio do qual o perito é notificado desse possível incidente. Elementos como a detecção do crime e de anomalias, análise de auditoria, reclamações, queixas e monitoração do sistema caracterizam essa etapa;

b) preservação: trata de assegurar a integridade e o estado das evidências. A manutenção das propriedades dos indícios é uma questão básica do processo investigativo e é relatada para as ações legais da perícia. Utilização de controles de processo e de qualidade está totalmente inclusa na manutenção do caso e identifica essa etapa, assim como a cadeia de custódia e a sincronização do tempo;

c) coleta: retrata a extração e a coleta de itens individuais ou em grupos. É a utilização de métodos específicos e ferramentas usadas pelo investigador para aquisição de evidências no ambiente do incidente. Alguns elementos representativos dessa etapa são: uso de métodos e ferramentas aprovadas, autoridade legal para a execução da coleta, compressão sem perdas, amostras, redução de dados e técnicas de recuperação;

d) exame: trabalha com o exame cuidadoso dos itens e suas características e atributos. Essa parte detalha o uso das ferramentas para o exame das evidências, voltada para a descoberta e extração das mesmas, e não com o intuito de formar conclusões sobre o caso. A principal diferença para a etapa anterior, é que a coleta envolve os procedimentos para a aquisição de dados brutos que podem conter as evidências, e o exame extrai e identifica os possíveis indícios a partir das informações coletadas. A rastreabilidade é a

principal característica dessa etapa, pois ela possibilita uma continuidade e forma uma cadeia de provas, dando credibilidade e auxiliando na futura elaboração das conclusões. Outras características são: uso de técnicas de validação e filtragem, comparação de padrões, descoberta e extração de dados ocultos;

e) análise: é definida como a fusão, correlação e assimilação do material para conclusões fundamentadas. É a análise de todas as evidências que foram coletadas, identificadas e extraídas desde o início. Os elementos dessa etapa referem-se ao meio pelo qual o perito pode desenvolver uma série de conclusões em relação às provas apresentadas.

f) apresentação: é a etapa que relata os fatos de maneira organizada, clara, concisa e objetiva;

g) decisão: apenas contempla a etapa posterior a da apresentação de documentos e laudos periciais para o tribunal, de forma a determinar as conclusões acerca do caso.

O propósito do modelo, mesmo elaborado de forma linear, permite que as etapas tenham um retorno de informações, caso isso seja necessário. As classes definidas categorizam as atividades executadas na investigação em forma de grupos. Suas especificidades são redefinidas para cada perícia em particular, atendendo assim, as necessidades requeridas para cada ação a ser tomada (RAY; BRADFORD, 2007).

3.5.2 Metodologia de Reith, Carr e Gunsch

A metodologia proposta por Reith, Carr e Gunsch (2002) também conhecida como Abstract Digital Forensics Model, possui alguns tópicos presentes também na

metodologia da DFRWS, o que o torna semelhante em seus princípios. As etapas que mostram essa semelhança são a de preservação, coleta, exame e apresentação. Como particularidade, o modelo apresenta a capacidade de fornecer suporte à preparação de ferramentas e uma dinâmica formulação de abordagens investigativas.

É explicitamente entendida a definição de um modelo abstrato devido a sua aplicabilidade em qualquer tecnologia ou tipo de crime computacional. A estrutura da metodologia é baseada em nove etapas, citadas abaixo (BARYAMUREEBA; TUSHABE, 2004):

a) identificação: reconhece o incidente e determina o seu tipo.
b) preparação: trata da elaboração e preparação das ferramentas, técnicas, monitoração de autorizações, mandados de busca e suporte.
c) estratégia de abordagem: desenvolve o procedimento para maximizar a coleta de evidências não infectadas ao mesmo tempo em que minimiza o impacto para a vítima.
d) preservação: envolve o isolamento, proteção e preservação do estado físico e digital das evidências.
e) coleta: detalha a gravação da cena física do crime e duplica as evidências digitais utilizando procedimentos aceitos e padronizados.
f) exame: trata da busca aprofundada e sistemática das provas relativas à suspeita do crime.
g) análise: envolve a determinação dos conceitos e significados, reconstrução dos fragmentos de dados e elaboração de conclusões baseadas nas evidências encontradas.
h) apresentação: envolve o resumo e a explicação das conclusões.

i) devolução das provas: garante que a propriedade física e digital seja devolvida ao proprietário.

Uma característica relevante desse modelo é o fato do mesmo representar uma padronização sem a necessidade da especificação da tecnologia envolvida. Dessa forma, existe uma consistência notória da metodologia que pode ser aplicada a dispositivos passados, presentes e futuros, de maneira aceitável e de fácil entendimento. O desenvolvimento dessa estrutura aborda um ponto de vista com o objetivo de aumentar as práticas de forense computacional através de tecnologias em comum, possibilitando uma aplicabilidade de ações em conjunto (REITH; CARR; GUNSCH, 2002).

Reith, Carr e Gunsch (2002), tratando sobre a abordagem da sua metodologia, citam algumas vantagens e desvantagens sobre a sua proposta. Dentre as vantagens estão: criação de um modelo padronizado e consistente para o desenvolvimento da forense digital; metodologia generalizada que membros judiciais podem utilizar para relatar tecnologia a pessoas que não são técnicas; identificação da necessidade de ferramentas específicas e dependentes da tecnologia. Como desvantagens podem ser citadas: etapas que podem ser definidas como muito generalizadas para a prática e que não existe nenhum método óbvio e fácil para o teste da metodologia.

3.5.3 Metodologia SOP

Originada pelo Scientific Working Group on Digital Evidence (SWGDE), que é o representante norte-americano na International Organization on Computer Evidence (IOCE).

A metodologia Standard Operating Procedures (SOP), foi apresentada durante uma conferência na International Hi-Tech Crime and Forensics Conference (IHCFC), que foi realizada em Londres, no período de 4 à 7 de outubro de 1999 (BERTOGLIO, 2008). Essa

metodologia incorpora os procedimentos e conceitos da ciência forense, incluindo a comparação, classificação, individualização e avaliação da fonte de evidências, sendo separada por seis etapas explicitadas a seguir (BERNARDO, 2006):

a) autorização e preparação: nessa etapa o perito forense deve se certificar de que com sua investigação, não está infringindo nenhuma lei. Caso contrário sua perícia será invalidada. Dessa forma é preciso que o perito receba a autorização de um juiz, para efetuar a mesma, ficando o exame restrito somente ao que for determinado pelo órgão judicial;

b) identificação: nesta etapa inicia-se o levantamento das informações relevantes ao crime e a identificação de todo o hardware e software do computador a ser examinado;

c) coleta e preservação: após a identificação das fontes de evidências, estas devem ser coletadas e mais tarde autenticadas. É de extrema importância que as evidências não sejam alteradas durante todo o processo investigativo. Aconselha-se que o perito calcule o valor hash dos arquivos originais, antes de copiar as evidências. Segundo Place (2008) um hash é uma sequencia de letras ou números gerados por um algoritmo de dispersão, buscando identificar um arquivo ou informação unicamente. É um método para transformar dados de tal forma que o resultado seja o mais exclusivo possível. Assim sendo, uma função hash recebe determinado valor e retorna um código que funciona como um identificador único. Ao fazer-se a cópia de um arquivo, se a mesma for fiel ao arquivo original, ambas apresentarão o mesmo valor hash. O perito garante assim a integridade dos dados e a credibilidade da sua perícia;

d) exame e análise: nesta fase, a coleta das evidências serão analisadas pelo perito na busca de provas;

e) documentação: é essencial em todas as etapas da perícia forense. Primeiramente, caso seja necessário outro perito dar sequência ao processo, o seu trabalho estará facilitado, e também visto que, a perícia terá maior credibilidade se a documentação estiver completa, com dados referentes a quem coletou e tratou as evidências com data e hora, e os valores hash de todas as evidências copiadas para demonstrar que as cópias estão livres de alteração e são autênticas;

f) reconstrução da cena do crime: esta etapa busca responder perguntas como: o que aconteceu? Quem executou? Quando aconteceu? Onde aconteceu? Como aconteceu? E Por quê?

Segundo o SWGDE (2008) SOPs são documentos únicos, específicos para determinado propósito, que descrevem os métodos e procedimentos a serem seguidos na realização de operações de rotina. Elas devem ser revistas anualmente, sendo as versões previamente aprovadas, guardadas para referência.

Um perito deve sempre levar em considerações as leis e regras que regem o ambiente onde a perícia será executada, mesmo que siga rigidamente as metodologias internacionais. Como por exemplo, leis municipais, estaduais e federais (BERNARDO, 2006).

3.5.4 Metodologia National Institute of Standards and Technology (NIST)

Essa metodologia criada por Wayne Jansen e Rick Ayers, também conhecida como orientações de como realizar perícia forense em celulares, realizado pela National Institute of Standards and Technology (NIST), tem como princípios recuperar provas digitais a partir de um telefone celular em condições forenses, utilizando métodos aceitos. Todo o

conteúdo dessa parte do trabalho foi baseado na referencia desses dois autores, Wayne Jansen e Rick Ayers, pelo fato de existir poucas referências relacionadas à perícia forense em celulares, e esta estar bastante detalhada.

Os telefones móveis, especialmente os que possuem recursos avançados, são um fenômeno relativamente recente, sendo assim, não costumam utilizar perícia forense computacional clássica. Essa metodologia pretende fechar essa lacuna, oferecendo uma visão aprofundada sobre as relações e procedimentos forenses (JANSEN; AYERS, 2007, tradução nossa).

3.5.4.1 Princípios

As investigações e os incidentes são tratados de maneiras diferentes, dependendo das circunstâncias do incidente, a gravidade, bem como a preparação e experiência da equipe de investigação. Investigações digitais são comparáveis às cenas do crime, onde técnica de investigação utilizada pela lei tem sido aplicada como fundamento para a criação de procedimentos utilizados quando se trata de evidências digitais.

Como plano de fundo de qualquer investigação, os princípios básicos têm sido propostos para lidar com provas digitais. A prova digital por sua própria natureza é extremamente frágil, especialmente quando encontrados em telefones celulares. O conteúdo de um celular e as provas que ele contém podem ser afetadas ou até mesmo perdidas a qualquer momento enquanto está ligado. Provas digitais são encontradas nos componentes físicos, periféricos e meios de comunicação. Cada uma tem associado uma cadeia de questões guardadas. A Association of Chief Police Officers (ACPO) sugere quatro princípios ao lidar com evidências digitais:

a) nenhuma ação realizada por investigadores devem alterar dados contidos em dispositivos digitais ou mídia de armazenamento que possa posteriormente ser invocado em juízo;
b) os indivíduos que têm acesso aos dados originais devem ser competentes para fazer isso e ter a capacidade de explicar suas ações;
c) os registro de processos aplicados, adequados para a replicação dos resultados por uma terceira parte independente, deve ser criado e preservado, precisando documentar cada passo investigativo;
d) a pessoa encarregada da investigação tem a responsabilidade de garantir que os procedimentos acima mencionados são seguidas e em conformidade com as leis que regem.

Os princípios visam garantir a integridade das provas digitais através de seu ciclo de vida. Manuseamento correto de prova 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. Por exemplo, usando uma ferramenta de software forense requer níveis de habilidade modestos para adquirir dados ativos, comparados com aqueles necessários para remover um chip de memória e recuperar o conteúdo dos dados, que inclui os dados ativos e excluídos.

Jansen e Ayers (2007, tradução nossa) afirmam que procedimentos utilizados para adquirir provas afetam sua admissibilidade. Isso se aplica também a provas obtidas a partir de telefones móveis que utilizam ferramentas de software forense. Mesmo fora das investigações policiais, as provas devem ser coletadas de forma que sejam adequadas para admissibilidade no tribunal. Pode não ser óbvio quando uma investigação é iniciada, por exemplo, quando um incidente de segurança é detectado pela primeira vez, que a ação judicial pode seguir.

Evidências importantes podem ser negligenciadas, mal tratadas, ou acidentalmente destruídas antes que a seriedade do incidente seja compreendida.

3.5.4.2 Preservação

De acordo com Jansen e Ayers (2007, tradução nossa) preservação de provas é o processo de apropriação de propriedade do suspeito, sem alterar ou modificar o conteúdo dos dados que residem em dispositivos e mídias removíveis. É o primeiro passo na recuperação de evidências digitais.

Preservação envolve a busca, reconhecimento, documentação e recolha de provas por via eletrônica, a fim de utiliza-las com sucesso, seja em um tribunal ou um processo menos formal. A falta de preservação da prova em seu estado original pode comprometer toda a investigação, perdendo as informações relacionadas com processos valiosos.

3.5.4.2.1 Segurança e Avaliação da Cena

Segundo Jansen e Ayers (2007, tradução nossa) para iniciar o processo de investigação é preciso garantir que as autorizações necessárias, por exemplo, um mandado de busca ou o consentimento do proprietário sejam concebidos. Procedimentos incorretos ou manuseio inadequado de um telefone celular durante o processo pode causar perda de evidências digitais. Além disso, as medidas tradicionais forenses, como impressões digitais ou testes de DNA, podem precisar ser aplicadas para estabelecer uma ligação entre um telefone celular e seu dono ou usuário, ou por outras razões. Se o dispositivo não for tratado adequadamente, provas físicas podem ser facilmente contaminadas tornando-se inúteis.

É preciso estar sob alerta para as características do dispositivo e questões, por exemplo, a volatilidade da memória e familiaridade com os acessórios associados, por exemplo, meios de comunicação, cabos, suportes e adaptadores de energia são essenciais. Para evitar a interação com dispositivos indesejados encontrados na cena, deve desligar as interfaces sem fio, tais como *Bluetooth* e *Wi-Fi*, em equipamento trazido para dentro da área de pesquisa.

Equipamento associado com o telefone celular tais como mídia removível, SIM, ou até mesmo computadores pessoais eventualmente sincronizados com ele, podem ser mais valioso do que o próprio telefone. A mídia removível varia do tamanho de uma unha ao de um selo postal, e pode ser facilmente escondido e difícil de encontrar. Na maioria das vezes, cartões de memória removíveis são identificáveis por sua forma característica e a presença de pinos, receptáculos de pinos ou contatos localizados em seu corpo, usada para estabelecer uma interface elétrica com o dispositivo.

Ao entrevistar o proprietário ou usuário de um dispositivo móvel, deve-se solicitar quaisquer códigos de segurança ou senhas necessárias para ter acesso ao seu conteúdo. Os suspeitos não devem ser autorizados a lidar com telemóveis ou outros dispositivos móveis. Muitos celulares têm códigos máster reset que limpa o conteúdo do telefone com as condições originais de fábrica. A remoção da bateria também pode causar perda do conteúdo de alguns dispositivos, tal como certos telefones inteligentes.

Em alguns casos o celular pode ser encontrado em um estado comprometido que pode complicar apreensão, tais como imerso em um líquido. No caso dos líquidos, a bateria deve ser removida para evitar curto-circuito elétrico. O restante do telefone deve ser selado em um recipiente apropriado preenchido com o mesmo líquido para o transporte até o laboratório, desde que o líquido não seja cáustico. Alguns estados comprometidos, como a contaminação de sangue ou uso de explosivos, por exemplo, como um componente de bomba,

pode representar um perigo para as provas coletadas. Em tais situações, um especialista deve ser consultado para obter instruções específicas, se houver dúvida sobre a forma de proceder.

Os telefones celulares e mídias associadas podem ser encontrados em um estado danificado, causada por acidente ou por ação deliberada. Dispositivos ou meios de comunicação com danos externos visíveis não necessariamente impedem a extração de dados a partir deles. O equipamento danificado deve ser levado de volta ao laboratório, para uma inspeção mais minuciosa. Componentes de memória intactos também podem ser removidos de um dispositivo com danos e recuperar seu conteúdo de forma independente.

3.5.4.2.2 Documentação da Cena

De acordo com Jansen e Ayers (2007, tradução nossa) um registro de todos os dados visíveis deve ser criado. Todos os dispositivos digitais, incluindo telefones móveis, que podem armazenar dados, devem ser fotografados junto com todos os cabos de periféricos, suportes, conectores de alimentação, mídia removível e conexões. É preciso evitar tocar ou contaminar o telefone quando fotografa-lo no ambiente que foi encontrado. Se o visor do aparelho está em estado visível, o conteúdo da tela deve ser fotografado e se necessário registrado manualmente, capturando o tempo, a situação do serviço, nível de bateria, e outros ícones exibidos. Outras características como a luz de atividade, por exemplo, piscando, a condição física, a conectividade física, ou identificadores visíveis também deve ser anotado. Ter uma pessoa responsável para prestar serviço de custódia das provas na cena do crime, juntamente com um sócio responsável pela documentação da prova, é desejável durante a fase de coleta.

Medidas tomadas no sistema para ver e gravar outros dados não voláteis sob exposição no tempo pode afetar o estado do dispositivo. Por exemplo, o lançamento de uma

aplicação em um telefone inteligente pode substituir partes da memória. Além disso, corre o risco de ativar um código indesejado escondido dentro da aplicação, acidentalmente acertando uma sequencia incorreta da chave e causando efeitos indesejáveis.

Por mais que a cadeia de custódia seja um processo simples, deve ser feita de forma eficaz. Documentar todo o percurso da prova através do ciclo de vida do caso. Com cuidado, a manutenção da cadeia de custódia não só protege a integridade das provas, mas também tornar difícil para alguém argumentar que as provas foram adulteradas. A documentação deve responder às seguintes perguntas:

a) quem recolheu? (dispositivos de mídia e periféricos associados);

b) como e onde? (como foi a prova recolhida e onde foi localizado);

c) quem tomou posse? (pessoa encarregada da apreensão de provas);

d) como foi guardado e protegido? (procedimento de custódia de provas);

A documentação para todas as perguntas devem ser mantidas e arquivadas em um local seguro para referências atuais e futuras.

3.5.4.2.3 Coletando Provas

Em relação a coleta de evidências, Jansen e Ayers (2007, tradução nossa) afirmam que isolar o telemóvel de outros dispositivos utilizados para a sincronização de dados é importante para manter os novos dados não contaminados com os existentes. O telefone deve ser apreendido, juntamente com os cabos encontrados. Cartões de mídia, SIMs, e outros hardwares que residem no telefone não devem ser removidos. Além disso, a apreensão do computador que estiver conectado ao telefone, caso esteja, permite a possibilidade de adquirir dados sincronizados a partir do disco rígido que não pode ser obtida a partir do telefone. Os cartões de mídia, SIM, adaptadores de energia, dispositivos ou periféricos, devem ser

apreendidos, juntamente com os materiais relacionados, tais como manuais de produtos, embalagens e software.

Isolar o telefone da rede de rádio é importante para manter os registros, como mensagens SMS apagadas, pois novas informações podem substituir dados existentes. Além do risco de sobrescrever a evidências em potencial, a questão pode surgir se os dados recebidos no telefone após a apreensão estão dentro do escopo da autoridade concedida originalmente.

Antes de coletar tal telefone móvel, o estado de energia da bateria deve ser considerado. Por exemplo, o dispositivo pode estar completamente carregado, recebendo energia de um carregador ou uma base conectada a uma tomada, ou muito pouca energia da bateria. Devem ser tomadas medidas para manter o nível da bateria a um nível adequado até que a aquisição seja bem sucedida. Isso pode ser especialmente difícil se o dispositivo precisa que seu sinal seja isolado, exigindo que ele seja colocado junto a uma fonte portátil de energia suplementar. Se a bateria estiver fraca e não poder ser fornecida, deverá ser desligado o telefone para preservar a vida da bateria, documentando o estado atual do dispositivo com hora e data do desligamento. É preciso evitar o desligamento do aparelho, pois caso aconteça, os dados localizados na memória volátil serão perdidos.

Mesmo quando o telefone está isolado, alterações de conteúdo podem ocorrer em um dispositivo ativo que pode ser indesejável, como a execução de um script (códigos fontes executados no interior de programas) agendado que limpa os dados antigos.

Para conservar a energia, alguns telefones inteligentes são normalmente configurados para entrar no modo de poupança de energia e desligar o monitor após um curto período de inatividade. Alguns celulares também entram em modo de poupança de energia caso o nível da bateria fique abaixo de certo limite, para proteger os dados armazenados na memória volátil. Se a energia adicional não pode ser fornecida a um dispositivo e ele está

desligado para economizar energia e preservar o conteúdo da memória, o risco de encontrar um mecanismo de proteção quando for ligado novamente deve ser baixa. Além disso, mecanismos de autenticação, como senhas, geralmente não podem ser desativados sem primeiro satisfazer o mecanismo, por exemplo, fornecendo a senha correta. Por estas razões, os procedimentos de algumas organizações pode recomendar desligar certas classes de telefones, se encontrou ligado.

Alguns telefones inteligentes usam baterias recarregáveis que são substituíveis, permitindo uma troca. Estes mesmos telefones mantêm uma pequena taxa para o dispositivo manter os dados voláteis por um curto período de tempo durante até a substituição da bateria. Para evitar perda de dados voláteis, as baterias devem ser substituídas rapidamente.

Se a tela está com baixa luminosidade, devido ao gerenciamento de energia, pode ser necessário pressionar uma tecla tão insignificante como a tecla de volume para iluminar o a tela do dispositivo, chamada de ecrã. Ao preparar os rótulos da embalagem, não deve se esquecer de registrar o fabricante e modelo do equipamento apreendido, e também a sua condição. A marca e o modelo podem ser marcados no corpo do aparelho e também aparecem no interior do aparelho embaixo da bateria. No entanto, não deve ser removida a bateria para ler esta informação, se o telefone estiver ligado.

Devem ser tomadas precauções ao manusear um telefone suspeito de ser modificado, especialmente se as alterações se presumem serem feitas por um indivíduo de mentalidade de segurança ou organização. Certos tipos de modificações para as aplicações de software e sistema operacional do dispositivo pode afetar a maneira como ela é tratada. A seguir está uma lista de exemplos de algumas classes de modificações a serem considerados:

a) melhorias na segurança: organizações e indivíduos podem aumentar os recursos de mecanismos de segurança. Uma variedade de login visual, biométricos, e mecanismos de autenticação baseada em *tokens* (seguimentos de

texto ou símbolos) estão disponíveis para telefones inteligentes utilizando como substitutos ou complementos aos mecanismos de senha padrões;

b) programas mal-intencionados: um telefone pode conter um vírus ou outros softwares maliciosos. Tais *malware16* podem tentar se espalhar para outros dispositivos através de interfaces com ou sem fio, incluindo multiplataforma, completamente diferentes da plataforma do dispositivo, como computadores com Windows. Utilitários ou funções comuns também podem ser intencionalmente substituídos por versões que contêm software projetado para alterar ou danificar os dados presentes em um telefone. Tais programas podem ser ativados ou condicionalmente baseados em parâmetros como de entrada ou interrupções da chave do hardware. Algumas aplicações também podem executar eventos específicos, por exemplo, realizar ações como a limpeza do dispositivo.

c) chave remapeamento: as chaves de hardware podem ser remapeadas para desempenhar uma função diferente da padrão. Uma tecla ou combinação de teclas destinadas para uma finalidade pode lançar um programa arbitrário.

3.5.4.2.4 Embalagem, Transporte e Armazenamento da Prova

Segundo Jansen e Ayers (2007, tradução nossa) uma vez que o dispositivo está pronto para ser apreendido, o especialista forense deve selar o aparelho em um saco de prova anti estática e marcá-lo. O indivíduo que se apodera do dispositivo deve assinar e datar a *tag* (linguagem de marcação) para iniciar uma cadeia de custódia. O dispositivo deve ser protegido adequadamente para evitar que as teclas sejam pressionadas acidentalmente. Recipientes rígidos são fabricados especificamente para este fim e são recomendados para uso

em isolamento de frequência e também estão disponíveis para atenuar o sinal de um dispositivo de rádio. Um carregador de energia externa independente podem ser conectado e colocado no saco com o dispositivo para manter o nível de potência máxima durante o transporte. Telefones com memória de dados volátil podem ser empacotados para permitir que um adaptador de energia fique conectado ao equipamento através de um buraco no saco para manter o nível de alta potência.

Os aparelhos digitais são frágeis e facilmente danificados. Quando um dispositivo é transportado, deve ser manuseado com cuidado e devidamente protegidos contra choques, quebras e temperaturas extremas. Devido à natureza volátil de alguns telefones inteligentes, eles devem ser imediatamente verificados em um laboratório forense, pois se deve estar ciente da situação das necessidades de energia.

O armazenamento das provas deve fornecer um ambiente fresco e seco, adequado para equipamentos eletrônicos valiosos. Todas as provas devem estar em recipientes fechados, em uma área segura, com acesso controlado.

3.5.4.3 Aquisição

Segundo Jansen e Ayers (2007, tradução nossa) a aquisição é o processo de obtenção de imagens ou informações de um dispositivo digital e seus equipamentos periféricos e meios de comunicação. Realizar aquisição no local tem a vantagem de que a perda de informações devido ao esgotamento da bateria, danos, entre outros, durante o transporte e armazenagem é evitado. No entanto, encontrar um ambiente controlado no qual trabalhar, ter o equipamento adequado, e satisfazer os pré-requisitos, não pode ser possível na cena, mas facilmente realizável dentro de um ambiente de laboratório. Os dispositivos devem

ser manuseados com cuidado com frequência de rádio blindada na área de trabalho ou ter suas comunicações wireless desativado por outros meios.

3.5.4.3.1 Dispositivo de Identificação

Jansen e Ayers (2007, tradução nossa) afirmam que para avançar de forma eficaz uma aquisição, os dispositivos precisam ser identificados pela marca, modelo e prestador de serviços. Esta informação permite que os examinadores selecionem as ferramentas apropriadas para a aquisição. É preciso estar atento para o sistema operacional e os aplicativos que podem ser modificados ou em raras situações completamente substituído, e aparecem de maneira diferente, assim podendo se comportar diferente do esperado. Por exemplo, remover ou substituir as telas de apresentação é uma modificação amplamente discutida em fóruns telefone.

Se o telefone estiver ligado, as informações que aparecem no visor pode às vezes ajudar a identificar o tipo de telefone. Por exemplo, o fabricante ou o nome do prestador de serviços pode aparecer no visor, ou o layout da tela pode indicar a família de sistema operacional utilizado. Informações como o rótulo do fabricante podem ser encontradas na cavidade da bateria, por exemplo, marca, modelo, IMEI ou ESN. Retirar a bateria da cavidade de um telefone, mesmo quando desligado, pode afetar seu estado, em especial o conteúdo da memória volátil. A maioria dos telefones mantém os dados do usuário na memória não volátil. Se o telefone estiver ligado, a remoção da bateria irá desligá-lo, possivelmente causando um mecanismo de autenticação para acionar quando novamente ligado.

Outros indícios que permitem a identificação de um dispositivo incluem coisas como o logotipo do fabricante, número de série e adaptador de energia. De modo geral, saber a marca e o modelo ajudam a limitar prestadores de serviços, através da diferenciação do tipo

de rede que o dispositivo opera mais, isto é, GSM, não GSM, e vice-versa. O software de sincronização descoberto em um computador associado também ajuda a diferenciar entre as famílias do sistema operacional.

3.5.4.3.2 Seleção de Ferramentas

Segundo Jansen e Ayers (2007, tradução nossa) uma vez que a marca e o modelo do celular são conhecidos, os manuais disponíveis podem ser estudados. O site do fabricante é um bom lugar para começar. Digitando o número do modelo no Google ou outro motor de busca também pode revelar uma quantidade significativa de informações sobre o dispositivo. Como mencionado anteriormente, o dispositivo que está sendo adquirido em grande parte determina a escolha de ferramentas forenses. Os seguintes critérios têm sido sugeridos como um conjunto de requisitos fundamentais para ferramentas forenses e devem ser considerados quando da escolha de ferramentas está disponível:

a) usabilidade: é a capacidade de apresentar dados de uma forma que seja útil a um pesquisador;
b) integral: é a capacidade de apresentar todos os dados a um investigador para que ambos os elementos de acusação e defesa possam ser identificados;
c) precisão: é a qualidade das saídas utilizando a ferramenta em relação a uma margem de erro verificada;
d) deterministas: é a capacidade da ferramenta para produzir o mesmo resultado quando recebe o mesmo conjunto de instruções e dados de entrada;
e) verificável: é a capacidade de garantir a precisão dos resultados por ter acesso a tradução intermediária e apresentação dos resultados.

Outros fatores na escolha da ferramentas de software incluem as considerações seguintes:

a) qualidade: apoio técnico e confiabilidade nas atualizações de versão;
b) capacidade: conjunto de funcionalidades suportadas, desempenho e riqueza de recursos em matéria de flexibilidade e customização;
c) acessibilidade: relação entre os custos e benefícios de produtividade.

É altamente recomendado obter experiências com diversas ferramentas em dispositivos testes para descobrir quais utilizar para aquisição e trabalhar de forma eficiente com os tipos de dispositivo específico. Além de ganhar familiaridade com as funcionalidades das ferramentas, a experimentação permite que os filtros de pesquisas e configurações personalizadas para se criar antes de usar em um caso real.

Alguns procedimentos estabelecidos devem orientar o processo do técnico de aquisição, bem como o exame das evidências. Novas circunstâncias podem surgir de forma esporádica exigindo adaptação dos procedimentos existentes, e em algumas situações requerem novos procedimentos e métodos de ser concebido. Os procedimentos devem ser testados para garantir que os resultados obtidos sejam válidos e reproduzíveis independentemente. O desenvolvimento e validação dos procedimentos devem ser documentados e incluem as seguintes etapas:

a) identificar o problema ou tarefa;
b) propor soluções possíveis;
c) testar cada solução em um dispositivo de teste e em condições de controle conhecidos;
d) avaliar os resultados do teste;
e) finalizar o procedimento.

3.5.4.3.3 Considerações sobre a Memória

De acordo com Jansen e Ayers (2007, tradução nossa) um telefone celular contém vários tipos de memória volátil e não volátil em várias categorias gerais de dados, como armazenamento do código do sistema operacional, incluindo o *kernel* (núcleo do SO), *drivers* de dispositivos e bibliotecas do sistema, além de memória para a execução de aplicativos do sistema operacional e de aplicativos do usuário, como tipos texto, imagem, vídeo, áudio e outros arquivos. A estrutura da memória do telefone pode ser particionada em áreas fixas para certos dados, tais como entradas da agenda, entradas de calendário, registros de chamadas e mensagens SMS, ou atribuído dinamicamente a partir de uma base comum compartilhada da memória. A mesma também pode ser estruturada de forma mais rigorosa como um sistema de arquivos formatado.

O tipo de memória em que cada categoria de dados são armazenados e estruturados variam entre os fabricantes e frequentemente são baseadas nas características do sistema operacional utilizado. Mesmo para um determinado modelo de telefone, dados de atribuições de armazenamento local podem variar entre telefones subsidiados fornecidos por operadoras de rede diferentes, dependendo das adaptações feitas pelo fabricante.

3.5.4.3.4 Aquisição em um Telefone Celular

Jansen e Ayers (2007, tradução nossa) relatam que muitas vezes, os telefones são enviados para processamento laboratorial apenas com itens específicos solicitados para a recuperação, como históricos de telefonemas ou imagens. Se qualquer dúvida ou preocupação existir sobre os dados solicitados, é recomendado contatar a pessoa que iniciou o exame para esclarecimento. Embora não seja sempre necessário recuperar todos os dados disponíveis,

uma aquisição completa evita ter que refazer o processo mais tarde, se outros dados são necessários, evitando a possibilidade de ocorrer problemas técnicos em uma nova tentativa.

Para adquirir os dados de um telefone, uma conexão deve ser estabelecida com o dispositivo da estação de trabalho forense. 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. Como mencionado anteriormente, o cuidado deve ser tomado para evitar a alteração do estado de um telefone móvel ao manuseá-lo, por exemplo, pressionando as teclas que poderiam danificar ou apagar os vestígios. Quando a conexão estiver estabelecida, a suíte de software forense pode proceder para adquirir os dados do dispositivo. É preciso informar uma conexão, que identifica o dispositivo a ser adquirido, identificando os dados a serem recuperados, e exibir os dados recuperados. Portanto, o objetivo durante a aquisição é afetar o conteúdo da memória o mínimo possível e somente com o conhecimento do que está ocorrendo internamente, contando com a adesão aos princípios que e a alta competência do especialista em relação a captura de uma trilha de auditoria detalhada das ações tomadas.

A data e horário mantidos no telefone móvel é uma importante peça de informação. A data e a hora podem ser obtidas a partir da rede ou configurar manualmente pelo usuário. Os suspeitos podem configurar manualmente o dia ou a hora para um valor completamente diferente da atual para deixar valores enganosos nos registros de chamadas e mensagens encontradas no celular. Se o telefone estava ligado quando apreendidos, a data e a hora mantidas e diferenças de um relógio de referência já deveria ter sido gravado, como mencionado anteriormente. No entanto, a confirmação de aquisição pode ser útil. Se o telefone estava desligado quando apreendidos, a data e a hora mantidas e diferenças de um relógio de referência deve ser registrada imediatamente quando ligado pela primeira vez em

laboratório. Note que as ações tomadas durante a aquisição, tais como a remoção da bateria para ler o rótulo do dispositivo, pode afetar o valor do tempo.

Ao contrário das máquinas desktop ou servidores de rede, apenas alguns aparelhos têm um disco rígido e refugiam-se completamente em memória semicondutora. Existe software especializado para executar uma lógica de aquisição de dados de Personal Identification Number (PIN) e, para alguns telefones, produzindo uma imagem física. No entanto, os conteúdos de um telefone são tipicamente dinâmicos e em constante mutação. Duas aquisições de um dispositivo usando a mesma ferramenta podem produzir resultados diferentes em geral. Por exemplo, se a compactação de memória ocorre, embora a maioria das informações, como dados de PIN, permanece inalterada.

Cada vez mais, os telefones celulares vêm com um slot (conector) integrado para alguma família de cartões de memória. Ferramentas forenses que adquirem o conteúdo de um cartão de memória residente normalmente realizam uma aquisição de lógica. Para recuperar dados apagados que podem residir no cartão de memória, uma aquisição direta pode ser realizada sobre ele depois que o conteúdo do telefone celular ter sido adquirido com sucesso. Com qualquer tipo de aquisição, pode ou não ter a capacidade de decodificar os dados recuperados do telefone guardados no cartão, por exemplo, mensagens de texto SMS, requerendo etapas manuais adicionais a serem tomadas.

Após a aquisição concluída, o especialista forense deve sempre confirmar que o conteúdo de um dispositivo foi capturado corretamente. Na ocasião, uma aquisição pode falhar a sua missão sem nenhuma notificação de erro e exigir que o especialista faça novamente a aquisição com a mesma ferramenta ou outra. Da mesma forma, alguns softwares não funcionam tão bem com certos dispositivos podendo falhar com uma notificação de erro. Assim, sempre que possível, é aconselhável ter várias disponíveis e estar preparados para mudar para outra se ocorrer dificuldades com a inicial.

Invariavelmente, nem todos os dados relevantes sobre um telefone podem ser visualizados e capturados através de uma aquisição lógica. Por exemplo, mensagens de rascunho e arquivados por vezes não são recuperados. Manualmente analisando o conteúdo através dos menus da interface do telefone enquanto a gravação do vídeo, o processo não apenas permite que tais itens sejam capturados e relatados, mas também confirma que os conteúdos relatados pela ferramenta são consistentes com os dados observáveis. Aquisição manual deve sempre ser feita com cuidado, preservando a integridade do dispositivo.

O conteúdo da memória do telefone, muitas vezes contêm informações, como dados excluídos, que não é recuperável, quer através de aquisição lógica ou um exame manual. Na falta de uma ferramenta de software capaz de realizar uma aquisição física, pode ser necessário recorrer a uma técnica baseada em hardware. Duas técnicas comumente utilizadas para a memória não volátil, a aquisição através de uma interface chamada Joint Test Action Group (JTAG), se suportada pelo dispositivo, e aquisição lendo diretamente memória que foi removido do dispositivo.

3.5.4.3.5 Aquisição em Cartão SIM

De acordo com Jansen e Ayers (2007, tradução nossa) a aquisição em um cartão SIM é similar a um telefone celular. Uma conexão deve ser estabelecida a partir da estação de trabalho forense para o dispositivo, usando um leitor. Como mencionado anteriormente, a versão a ser utilizada deve ser documentada, juntamente com as correções aplicáveis ou errata do fabricante. Quando a conexão estiver estabelecida, o software forense pode proceder para adquirir os dados do dispositivo.

Capturar uma imagem direta dos dados do SIM não é possível porque os mecanismos de proteção construído dentro do módulo impedem esse processo. Em vez disso,

os softwares enviam diretrizes de comandos chamados Application Protocol Data Units (APDUs) para o SIM na busca da extração dos dados de forma lógica, sem modificação, a partir de cada arquivo de dados elementares do sistema de arquivos. O protocolo APDU é uma troca de comando resposta simples. Cada elemento do sistema de arquivos, definidos nas normas GSM tem um identificador numérico único atribuído, que pode ser usado para percorrer o sistema de arquivo e recuperação de dados, referenciando um elemento e realizar algumas operações, tais como a leitura de seu conteúdo.

Os SIMs são dispositivos altamente padronizados, alguns problemas existem com relação a uma aquisição lógica. A principal consideração é a seleção de uma ferramenta que informa o status de qualquer PINs e recupera os dados de interesse. Existem grandes diferenças nos dados recuperados por ferramentas SIM, com algumas recuperando apenas os dados que tem uma maior relevância em uma investigação típica, e outros fazendo a recuperação completa de todos os dados, mesmo que não tenha um valor investigativo.

3.5.4.3.6 Aquisição em Cartão de Memória

Segundo Jansen e Ayers (2007, tradução nossa) os telefones móveis usam uma grande variedade de cartões de memória, que vão desde o tamanho de uma lente de contato até uma caixa de fósforos. Ao contrário da RAM em um dispositivo, tal mídia de armazenamento é removível, não volátil e não requer nenhuma bateria para manter os dados. A capacidade de memória de armazenamento do cartão varia de 8 MB à 8 GB podendo ir além dependendo do suporte do celular. Com os avanços tecnológicos, esses meios de comunicação tornam-se menores e oferecem maior densidade de armazenamento. A mídia removível estende a capacidade de armazenamento de celulares, permitindo que os indivíduos

possam armazenar arquivos adicionais além da memória interna embutida no dispositivo e capacidade para compartilhar dados entre dispositivos compatíveis.

Algumas ferramentas forenses são capazes de adquirir o conteúdo de cartões de memória. Se a aquisição for lógica, os dados apagados do cartão presentes não são recuperados. Felizmente, esses meios de comunicação podem ser tratados de forma semelhante a uma unidade de disco removível, e analisados usando as ferramentas convencionais forense, com a utilização de um leitor de mídia externa, como adaptadores de cartão de memória que suportem uma interface Integrated Drive Electronics (IDE). Esses adaptadores permitem que uma mídia removível seja tratada como um disco rígido usado um bloqueador de gravação, que garante que a mídia removível permaneça inalterada.

Os dados contidos nos meios de comunicação podem ser analisados e pesquisados, e arquivos apagados podem ser recuperados, oferecendo possibilidades de descobrir provas. Uma desvantagem é que os dados do telefone, como mensagens de texto SMS, armazenado na mídia pode exigir decodificação manual ou uma ferramenta de decodificação separada para interpretar. Uma questão mais grave é que recursos de proteção de conteúdo incorporado no cartão que pode bloquear a recuperação de dados.

3.5.4.4 Levantamento e Análise

Jansen e Ayers (2007, tradução nossa) afirmam que o processo de exame descobre evidências digitais, incluindo o que pode estar oculto ou obscuro. Os resultados são obtidos através da aplicação de métodos estabelecidos com base científica, e deve descrever o conteúdo e estado dos dados na íntegra, incluindo a origem e o significado em potencial. Redução dos dados, separando informações relevantes e irrelevantes, ocorre uma vez que os dados são expostos. O processo de análise difere da análise em que se olha para os resultados

do exame e seu significado direto e valor probatório do caso. Exame é um processo técnico que é proveniente de um especialista forense. Entretanto, a análise pode ser feita por outros personagens forenses, como o investigador ou o examinador forense.

O processo de análise começa com uma cópia das provas adquiridas a partir do dispositivo. Felizmente, comparado com o exame clássico de estações de trabalho individuais ou servidores de rede, a quantidade de dados adquiridos para examinar é muito menor com os telemóveis. Por causa da prevalência de formatos de arquivo proprietários, o Forensic Toolkit usado para a aquisição será normalmente o utilizado para exame e análise.

O examinador deve estudar o caso, se possível, e se familiarizar com os parâmetros do delito, as partes envolvidas, e as provas possíveis que possam ser encontradas. A realização do exame, em parceria com o analista forense ou o investigador pode orientar a construção de caso e é aconselhável para o examinador. O investigador ou analista pode localizar coisas que seja o foco, enquanto o examinador forense fornece os meios para encontrar informações relevantes que possam estar no sistema.

Se o examinador forense executa a análise de forma independente, sem conferir diretamente com o analista ou investigador forense, a compreensão adquirida pelo estudo do caso deve fornecer ideias sobre os tipos de dados para direcionar palavras-chaves específicas ou frases para usar quando a consulta dos dados é adquirida. Dependendo do tipo de caso, a estratégia varia. Por exemplo, um caso de pornografia infantil pode começar a visitar todas as imagens gráficas no sistema, enquanto um caso sobre uma infração relacionada com a Internet pode começar a visitar os arquivos de histórico da Internet.

O exame revela frequentemente que não apenas dados incriminadores, mas também informações úteis, tais como senhas, nomes de logon de rede e atividade de Internet são encontrados. Determinados dados podem também fornecer a ligação a outras fontes potenciais de provas mantidas em outros lugares, principalmente pelos prestadores de serviços

de rede. Além de evidências diretamente relacionadas a um incidente, a informação pode ser descoberta sobre a vida dos suspeitos, os seus associados, e os tipos de atividades nas quais eles estão envolvidos.

3.5.4.4.1 Provas Possíveis

Os fabricantes de celulares em geral oferecem um conjunto semelhante de características e capacidades de manipulação de informações, incluindo Personal Information Management (PIM), mensagens, e-mail e navegação na web. O conjunto de características e capacidades podem variar, claro, com a época em que o telefone foi fabricado, a versão do *firmware* em execução, as modificações feitas por um determinado fornecedor de serviços, e quaisquer modificações ou aplicativos instalados pelo usuário. As evidências possíveis destes dispositivos incluem os seguintes itens:

a) assinante e identificadores de equipamentos;
b) data, hora, idioma e outras configurações;
c) informações da agenda;
d) informações de calendário de compromisso;
e) mensagens de texto;
f) números discado, recebidos e chamadas não atendidas;
g) correio eletrônico;
h) fotos;
i) gravações de áudio e vídeo;
j) mensagens multimídia;
k) mensagens instantâneas e as atividades de navegação na Web;
l) documentos eletrônicos;

m) informações de localização.

Outros dados encontrados em um telefone celular também podem ser úteis para uma investigação. Por exemplo, algo aparentemente irrelevante, como tons de toque pode ter relevância, muitas vezes tons de toque diferenciado em um telefone para distingui-los dos outros. Uma testemunha de um incidente pode lembrar-se de ter ouvido uma música em particular no telefone de um suspeito, que pode contribuir para a identificação de um indivíduo.

3.5.4.5 Reportagem

Segundo Jansen e Ayers (2007, tradução nossa) a reportagem é o processo de elaboração de um resumo detalhado de todos os passos dados e as conclusões alcançadas na investigação de um caso. Reportagem depende da manutenção de um registro cuidadoso de todas as ações e observações, descrevendo os resultados dos testes e exames, e explicar as inferências extraídas da prova. Um bom relatório se baseia em uma sólida documentação, notas, fotos e conteúdo gerados pelo instrumento.

Reportagem ocorre uma vez que os dados foram exaustivamente pesquisados e itens relevantes marcados. Muitas ferramentas forenses vêm com uma base de comunicação facilitada que normalmente segue modelos pré-definidos e pode permitir a personalização da estrutura do relatório, fornecendo personalizações, permitindo incluir logotipos, descrição da organização, cabeçalhos de relatório e seleção de estilos e estrutura para proporcionar um olhar mais profissional adaptado às necessidades da organização. Os relatórios gerados por uma ferramenta forense geralmente incluem itens como, o nome do especialista, o número do processo, data e título, as categorias de provas, e os elementos de prova pertinentes encontrados. A geração de relatórios em geral, requer as saídas de todos os dados obtidos ou

permite que os examinadores selecionem os dados relevantes. Ou seja, os itens marcados para o relatório final. Incluindo apenas resultados relevantes no relatório minimiza seu tamanho e diminui a confusão para o leitor.

Os conteúdos gerados por software são apenas uma parte do relatório global. O relatório final contém o conteúdo gerado por software, juntamente com os dados acumulados ao longo da investigação, que resume as ações desenvolvidas, a análise feita, e a relevância das evidências descobertas.

A geração de relatórios em geral pode tornar um relatório completo em um dos vários formatos comuns, por exemplo, .txt, .rtf, .csv, .doc, .HTML, ou, pelo menos, fornecer um meio para exportar os itens individuais de dados para compor um relatório manualmente. Algumas ferramentas incluem a falta de meios de geração de relatório ou exportar dados e, exigem examinadores para capturar *screenshots* (captura de imagem) individuais da interface, montando posteriormente o relatório. Independentemente de como os relatórios são gerados, verificar que o relatório finalizado é consistente com os dados apresentados na representação de interface do usuário, é fundamental para identificar e eliminar possíveis incoerências que possam surgir.

A capacidade de modificar um relatório pré-existentes e incorporar os dados, por exemplo, imagens e vídeo capturados por meios alternativos é vantajoso. Técnicas de aquisição auxiliares são várias vezes obrigadas a recuperar os tipos de dados específicos, como mencionado anteriormente.

O tipo de dado determina se ele é apresentável em um formato impresso. Hoje, muitos dispositivos celulares populares são capazes de capturar vídeo e áudio. Esses dados probatórios, por exemplo, áudio, vídeo, não podem ser apresentadas em formato impresso e em vez disso deve ser incluído no relatório finalizado em uma mídia removível, por exemplo, CD-ROM, DVD-ROM ou *pendrive*, juntamente com o aplicativo adequado para boa exibição.

Em geral, o relatório pode incluir as seguintes informações:

a) identificação da agência de comunicação;
b) processo identificador ou número de apresentação;
c) investigador do caso;
d) identificação do remetente;
e) data de recepção;
f) data do relatório;
g) lista descritiva dos itens apresentados para exame, incluindo o número de série, marca e modelo;
h) identificação e assinatura do examinador;
i) os equipamentos e as condições utilizadas na análise;
j) breve descrição das medidas tomadas durante o exame, tais como pesquisas de cadeia, buscas de gráficos, imagens e recuperação de arquivos apagados;
k) materiais de apoio, tais como impressões de itens de provas, cópias digitais das provas, e a cadeia de custódia de documentação;
l) conclusões do relatório.

Provas digitais, bem como as ferramentas, técnicas e metodologias utilizadas no exame estão sujeitas a ser contestada em um tribunal ou outro processo formal. Uma documentação apropriada é essencial para garantir aos indivíduos a capacidade de recriar o processo do começo ao fim. Como parte do processo de comunicação, fazendo uma cópia do software utilizado, inclusive, com a saída produzida é aconselhável. Isto é especialmente pertinente para ferramentas personalizadas, caso se torne necessário para reproduzir os resultados forenses de processamento em um momento posterior. A mesma prática se aplica a ferramentas de software comercial, o que pode ser atualizada após um exame é concluído.

A seguir uma comparação e correlação entre as metodologias forenses abordadas nesse trabalho.

3.5.5 Tabela Comparativa de Metodologias Forenses

Passos das Metodologias	DFRWS	Reith, Carr e Gunsch.	SOP	NIST
Autorização	-	-	X	X
Identificação	X	X	X	X
Preparação	-	X	-	X
Estratégia de abordagem	-	X	X	X
Coleta e Preservação	X	X	X	X
Aquisição	X	X	X	X
Exame e Análise	X	X	X	X
Apresentação ou Documentação	X	X	X	X
Decisão	X	-	-	-
Devolução das evidências	-	X	-	-
Reconstrução da cena do crime	-	-	X	-

Figura 4. Comparação de Metodologias Forenses

Podemos visualizar na Figura 4 que as quatro metodologias mencionadas nesse projeto possuem alguns passos em comuns, na investigação de casos forenses. Sendo eles a identificação das evidências, coleta e preservação, aquisição, exame e análise e apresentação ou documentação.

Dessa forma, é possível concluir que ambas seguem a mesma linha de processos. Algumas com peculiaridades e características próprias para incrementar a investigação e ter uma maior aceitação perante um tribunal.

Para um melhor entendimento dos crimes digitais realizados em celulares, a seguir uma breve explicação.

3.6 USO DE CELULARES EM CRIMES DIGITAIS

Segundo Casey (2004, tradução nossa) uma nova classe de crimes tem se tornado mais prevalente dentro dos domínios digitais, em particular em aparelhos celulares. Órgãos da justiça criminal estão sendo confrontados com a necessidade de investigar os crimes cometidos total ou parcialmente por esse meio eletrônico. Dessa forma, a perícia forense precisa analisar vários crimes digitais, como por exemplo, imagens e vídeos de pornografia infantil, mensagens enviadas e recebidas, com o intuito de procurar, localizar e preservar todos os tipos de provas eletrônicas.

Campi (2010) relata que de acordo com um estudo realizado pela empresa de segurança digital Symantec, os dispositivos móveis, serão os principais alvos de ataques virtuais no próximo ano. Pois com o aumento do número de smartphones e do uso de redes sociais nesses dispositivos, será um grande desafio manter segurança digital em 2011. A previsão é que o número de smartphones conectados a Internet seja maior que o número de PCs online, fazendo com que golpes virtuais sejam focados nesses tipos de dispositivos, afirmou Enrique Salem, da Symantec.

Atualmente existem 1,4 bilhão de *smarphones* conectados a Internet. A Symantec ainda prevê que em 2014, a quantidade deve atingir 10 bilhões, podendo representar novas ameaças de segurança (CAMPI, 2010).

Utilizando o celular, é possível realizar muitos tipos de crimes digitais, como extorsão ou estelionato. Pode-se considerar como um ato de certa forma cruel, pois mexe com a efetividade de uma pessoa. Com informações privilegiadas sobre familiares, mentem que estão com os filhos, esposas, irmãos sequestrados, e exigem resgate para que não façam mal a estes entes queridos. Para tornar o golpe ainda mais real, ligam para o suposto sequestrado e inventam outra história para que o mesmo desligue o celular, dificultado o contato com a

pessoa que está sendo extorquida. Outro crime praticado com o telefone é o roubo de veículo, e posterior pedido de resgate com o uso celular e dados do proprietário do veículo roubado.

3.7 IMPORTÂNCIA EM PERICIAR UM CELULAR

A grande importância de se periciar um celulares é o fato que o mesmo pode conter as provas mais importantes em investigações criminais, encontradas na forma de mensagens, histórico de ligações, agenda de contatos e até mesmo em dispositivos mais avançados, histórico de acesso a páginas da Internet (CERQUEIRA FILHO, 2004).

Agências criminalistas ao redor do mundo precisam de todas as evidências possíveis para ajudar a solucionar crimes, que muitas vezes podem ser escassos de evidências tornando complicado o prosseguimento das investigações, que correm o risco de nunca serem finalizadas. Muitas vezes, celulares contêm informações importantes e incriminatórias que investigadores precisam para solucionar um caso, pois sua facilidade e mobilidade na comunicação facilita a prática de delitos, seja na comunicação ou até mesmo no relacionamento que o meliante tem com seus contados cadastrados na agenda do dispositivo (CERQUEIRA FILHO, 2004).

Marcella e Menendez (2008, tradução nossa) explica que um examinador qualificado que realiza perícia forense em celular pode recuperar arquivos apagados de um celular, pode ver quais sites foram visitados a partir de um dispositivo específico, mesmo após a exclusão do histórico do navegador, é capaz de rever as comunicações enviadas e recebidas anteriormente através de um chat e mensagens instantâneas, tais como Yahoo e (MSN). Também é capaz de restaurar imagens e mensagens excluídas de e-mail. Além disso, o legista é treinado para analisar e recriar mensagens de texto suprimidas e registros de chamadas de telefones celulares, PDAs e aparelhos Black Berry.

Em seguida seguem alguns casos de delitos praticados que possibilitam estudo à perícia forense em celulares segundo Marcella e Menendez (2008, tradução nossa):

a) Casos de adultério: Nesses casos, a pessoa suspeita entra em contato com seu ou sua amante utilizando celulares para enviar mensagens, realizar ligações e após excluir o histórico da ligação realizada, bate-papo on-line ou envio/recebimento de e-mail. Um perito forense com as ferramentas certas pode restaurar essas informações;

b) Busca de um suspeito qualquer: Quando localiza um suspeito, com o celular do mesmo é possível buscar informações de possíveis contatos, podendo localiza-los, e assim possuir uma rede de informações. Pois os fatos podem se entrelaçar, ajudando na resolução de um caso;

c) Casos de Assédio: Há muitos tipos diferentes de assédio. Frequentemente acontece o caso que o seu cliente pode não só estar recebendo o assédio em pessoa, mas também através de telefone e ou e-mail. Um legista pode preservar registros de chamadas telefônicas recebidas de telefones celulares e apresentá-los como elementos de prova a manutenção de uma cadeia de custódia. Todos os e-mails enviados a partir de uma determinada fonte para um destino específico incorporadas no e-mail. O examinador forense pode analisar o cabeçalho do e-mail e relacioná-las com as origens do endereço IP que lhe foi enviado.

No próximo capítulo são apresentados alguns trabalhos estudados com propósitos semelhantes a presente pesquisa.

4 TRABALHOS CORRELATOS

Durante os estudos com o intuito de realizar o desenvolvimento da pesquisa, foram estudados alguns trabalhos semelhantes, mas com outro enfoque. Abaixo, está a descrição de alguns trabalhos envolvendo a perícia forense computacional.

4.1 TÉCNICAS COMPUTACIONAIS NO AUXÍLIO À PERÍCIA FORENSE NA ANÁLISE DE EVIDÊNCIAS COLETADAS EM SERVIDORES GNU/LINUX

Trabalho de autoria de Adauto de Souza Bernardo, realizado na Universidade do Extremo Sul Catarinense, com o objetivo de graduação em ciência da computação em 2006.

Esse trabalho tem como objetivo aplicar técnicas computacionais forenses na análise dos resultados gerados pela etapa de busca de evidências na memória principal, memória secundária, processos e módulos do kernel em servidores GNU/Linux.

Nesse trabalho, são apresentadas algumas formas publicamente conhecidas na análise das evidências em ambientes GNU/Linux. Analisando basicamente a memória, módulos do kernel e sistema de arquivos de maneira prática, fazendo uso do embasamento teórico presente na literatura e a utilização de ferramentas livres (BERNARDO, 2006).

4.2 PERÍCIA FORENSE EM SOFTWARE LIVRE

Trabalho de Conclusão de Curso em Ciência da Computação de autoria de Thiago Figueireto Marques Leite realizado na UNIDES, em 2006, com o objetivo de apresentar um estudo sobre perícia forense utilizando Software Livre, bem como criar um documento de base para servir como uma primeira recorrência por peritos, em casos em que uma perícia

forense computacional deve ser utilizada. É demonstrada a análise de evidências em logs de acesso do sistema operacional, logs de servidores web, mensagens eletrônicas e como ocultar rastros utilizando técnicas antiforenses (LEITE, 2006).

4.3 PERÍCIA FORENSE: PROPOSTA DE UMA METODOLOGIA DE COLETA DE INDÍCIOS PARA AMBIENTE WINDOWS

Trabalho de conclusão de curso apresentado no Centro Universitário Feevale, elaborado por Daniel Bertoglio. Tem como meta abordar e explicar o tema de perícia forense computacional, propondo uma metodologia de coleta de indícios para um ambiente Windows. (BERTOGLIO, 2008).

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

Trabalho de autoria de Sidney Roberto da Silva Webba, realizado na Universidade do Extremo Sul Catarinense, com o objetivo de graduação em ciência da computação em 2010.

Esse trabalho tem 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.

Como resultado desse trabalho conseguiu-se 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. Ocasionalmente ocorreram falhas ao trabalhar com determinadas ferramentas, como por exemplo, a ferramenta Firefox3Extractor que falhou ao converter arquivos de cache do Firefox, bem como ao mostrar as senhas e nomes de usuário salvos pelo mesmo browser.

Provas periciais foram encontradas em alguns dos computadores investigados, mas a análise de muitos outros, mostrou-se inconclusiva (Webba, 2010).

4.5 PERÍCIA FORENSE COMPUTACIONAL APLICADA A AMBIENTES NEW TECHNOLOGIES FILE SYSTEM (NTFS)

Trabalho realizado por Ramiro Webber Dimer, realizado na Universidade do Extremo Sul Catarinense, com o objetivo de graduação em ciência da computação em 2007.

Esse trabalho tem como objetivo aplicar técnicas computacionais forenses de duplicação pericial, recuperação de dados para a busca e análise de evidências em ambientes baseados em sistemas de arquivo New Technologies File System (NTFS) (Dimer, 2007).

No próximo capítulo são apresentados o estudo desenvolvido e a metodologia usada para desenvolver o mesmo, visando ratificar a pesquisa.

5 TRABALHO DESENVOLVIDO

O presente estudo de caso foi realizado na Universidade do Extremo Sul Catarinense (UNESC), localizada em Criciúma/SC. A instituição possui uma estrutura com 27 laboratórios de informática de grande porte com até 24 computadores, e 6 laboratórios de pequeno porte com até 12 computadores, sendo os laboratórios 13 e 14 do Bloco XXI-C reservados para uso livre da comunidade interna da mesma. A comunidade externa da universidade tem disponível, Internet gratuita nos computadores da biblioteca.

Para a realização da perícia forense e aplicação da junção das metodologias DFRWS, Reith, Carr e Gunsch, SOP e NIST em celulares com SO Symbian foi escolhido o aparelho Nokia N85 que possui versão do OS 9.3 da série S60 3ª edição.

O processo será baseado em todas essas metodologias. Porém, a NIST será a base do processo. Algumas peculiaridades das outras serão introduzidas para uma perícia mais completa e robusta.

Agora, para melhor contextualizar o estudo de caso fictício, e permitir uma compreensão facilitada das etapas realizadas, foi suposto que o seguinte crime digital foi cometido:

- Um homem com nome fictício José Alfredo é suspeito de estar traficando drogas, usando um celular Nokia N85 para manter contato com seus clientes, podendo ter enviado e recebido mensagens (SMS), fotos, ligações entre outras informações. Para tanto, deverá ser feito uma busca nas informações contidas no dispositivo a fim de encontrar provas que possam ajudar na resolução do caso. Para criação desse caso, foi contado com a colaboração de uma terceira pessoa, que realizou tarefas desconhecidas no celular, a fim de gerar provas relacionadas a um fictício comércio de drogas. O Celular Nokia N85, ficou em

posse do colaborador no período de 22 de maio de 2011 à 02 de junho de 2011. A simulação da apreensão do mesmo foi datada para 02 de junho de 2011, momento em que recuperei o dispositivo.

A seguir, são expostos os conceitos relevantes a todos os processos das metodologias científica aplicadas neste trabalho.

5.1 METODOLOGIA

A pesquisa tem como embasamento um estudo de caso fictício, que simula a ocorrência de uma perícia forense em um dispositivo celular, objetivando buscar conhecimento detalhado sobre os procedimentos de interesse para este estudo, considerando a ocorrência de um crime digital.

De acordo com Martins e Theóphilo (2009) um estudo de caso trata-se de uma investigação empírica que tem como objetivo pesquisar fenômenos dentro de seu contexto real. De uma forma onde o pesquisador não tem controle sobre eventos e variáveis, mas buscando aprender a totalidade de uma situação e criativamente descrever, compreender e interpretar a complexidade de um caso concreto.

O fato de que cada caso tem suas características próprias, faz com que não exista um modelo traçado de forma específica para elaboração de um estudo de caso, mas existe uma sequência de práticas metodológicas para orientação, que são: coleta de evidências, composição e validação dos resultados, conclusões, verificação de possíveis interferências e relatório final (MARTINS; THEÓPHILO, 2009).

Portanto, para que se cumpram os objetivos desta pesquisa, definiu-se que as metodologias DFRWS, Reith, Carr e Gunsch, SOP e NIST serão utilizadas durante a

realização do estudo, pois a junção das mesmas incorpora algumas das práticas metodológicas recomendadas acima, tanto quanto os princípios e técnicas da ciência forense.

A seguir a figura 5 ilustra cada uma das etapas com algumas ações a serem tomadas no decorrer da perícia. Essas ações atuam como processos em um projeto, pois respeitam uma ordem, mesmo que a investigação retorne a uma etapa anterior.

Etapas do Processo Forense

Autorização
- Autorização judicial ou consentimento do proprietário do celular.

Identificação
- Adquirir todas as informações subjetivas possíveis em relação à investigação.

Preparação
- Definir o que se deve provar.

Estratégia de abordagem
- Não infectar o dispositivo.

Coleta e Preservação
- Identificar fontes de provas.
- Coleta de provas.
- Documentação da cena e provas encontradas.
- Armazenamento das provas.

Aquisição na Memória Interna do Celular
- Identificação do dispositivo.
- Seleção de ferramentas.
- Aquisição na memória do celular.

Exame e Análise na Memória Interna do Celular
- Analisar provas coletadas.
  - Contatos.
  - Mensagens de texto e multimídias.
  - Agendamentos e Tarefas.

Aquisição na Memória Externa do Celular
- Seleção de ferramentas.
- Aquisição em cartão de memória.

Exame e Análise na Memória Externa do Celular
- Analisar provas coletadas.
  - Fotos.
  - Arquivos de texto entre outros encontrados.

Apresentação ou Documentação
- Identificar perito.
- Registrar hora e data do início e fim da investigação.

Decisão
- Determinar conclusões do caso.

Devolução das provas

• Devolução do dispositivo e outros materiais encontrados durante a preservação e coleta.
Reconstrução da Cena do Crime
• Deve responder perguntas como: o que aconteceu? Quem executou? Quando aconteceu? Onde aconteceu? Como aconteceu? E Por quê?

Figura 5. Tabela de Etapas do Processo Forense

A explicação detalhada de como cada etapa foi aplicada, é apresentada a seguir.

5.2 ETAPA 1 - AUTORIZAÇÃO

Pelo fato de o presente estudo de caso ser fictício, não se fez necessária a busca por uma autorização judicial ou consentimento do suspeito, para que a perícia forense fosse realizada.

Foi definido o escopo da pesquisa, determinando o que se deseja provar. Para tal, estabeleceu-se que se pretende descobrir ao final da mesma se o portador do celular utilizou o mesmo para realizar algum tipo de crime digital, buscando a forma que realizou o contato, a data e hora e com quem manteve esse contato. Esta etapa é baseada na metodologia NIST.

5.3 ETAPA 2 - IDENTIFICAÇÃO

Novamente por se tratar de um estudo de caso hipotético, não foi necessário o levantamento junto às pessoas envolvidas no crime (pessoas que identificaram a ocorrência do crime) que permitiriam ao perito contextualizar melhor os fatos que surgissem durante o decorrer da investigação. Esta etapa, também é baseada na metodologia NIST.

Passou-se então para a preparação, a fim de definir o que se deve provar.

5.4 ETAPA 3 – PREPARAÇÃO

No momento da preparação é preciso definir o que se deve provar. Esse passo é importante, pois ajuda a focar na busca de provas e conciliações das informações encontradas.

Tratando-se de um caso hipotético onde uma pessoa é suspeita de estar realizando tráfico de drogas, foi decidido que informações relacionadas a drogas, pagamentos, cobranças e entregas, deverão ser localizadas com maior enfoque, com o intuito de chegar a uma conclusão sem precisar analisar todos os dados encontrados no dispositivo. É uma etapa da metodologia NIST.

5.5 ETAPA 4 – ESTRATÉGIA DE ABORDAGEM

Nessa etapa, referente à metodologia NIST, é preciso garantir que nenhuma informação do dispositivo será alterada. Para isso, toda forma de acesso utilizando hardwares ou softwares deverá garantir que nenhum dado será inserido, alterado ou excluído do dispositivo.

Todas as ferramentas utilizadas nesse processo forense garantem que essa etapa será validada garantindo a integridade e confiabilidade das provas. Pois acessam o dispositivo com a restrição de somente leitura.

5.6 ETAPA 5 – COLETA E PRESERVAÇÃO

Para simular o caso, utilizando a metodologia NIST, o celular foi deixado sob a cama do suspeito portador do dispositivo, junto a um cabo de alimentação de energia e outro cabo USB para transferência de dados, conforme podemos visualizar na figura 6.

Figura 6. Coleta do Dispositivo e Periféricos

Na coleta é preciso resgatar todos os periféricos que podem ajudar na aquisição de dados e análise posteriormente. Para isso, foram coletados além do celular, o cabo de alimentação e o cabo USB para transferência de dados.

Pelo fato do dispositivo ter sido encontrado ligado, o mesmo foi mantido ligado para não perder os dados voláteis caso existam. Outros hardwares do celular como cartão de memória e SIM, não foram removidos até o momento.

Foram procurados nos locais próximos ao dispositivo, o manual e CDs de software, porém nada foi encontrado. Provavelmente, não estejam mais acessíveis.

Durante a coleta foi preciso isolar o celular da rede de rádio para manter os registros que foram apagados. Pois novas informações podem substituir os dados existentes e novos dados recebidos após a apreensão podem estar fora do escopo da autoridade concedida originalmente. Para isolar foi preciso entrar no menu do celular e escolher uma opção de conexão *off-line*.

Com o celular em mãos, pôde-se visualizar o nível da bateria, que por sinal estava quase completamente carregada. Caso contrário, seria preciso utilizar o cabo de energia para recarregar a bateria evitando um desligamento do dispositivo não esperado.

Uma parte muito importante na preservação é garantir a segurança do dispositivo e suas informações. Para isso o mesmo foi colocado em um saco especial e marcado com a assinatura e data do acontecimento, para poder iniciar uma cadeia de custódia. Nesse processo foi preciso uma atenção especial para evitar que as teclas sejam pressionadas acidentalmente.

Após o transporte do dispositivo o mesmo foi armazenado em um ambiente fresco e seco em um local seguro com acesso controlado.

Durante a coleta foi preciso documentar todo o percurso da coleta de provas através do ciclo de vida do caso que seguem na figura 7. Essa parte do processo é extremamente importante, pois não só protege a integridade das provas, mas também torna difícil para alguém argumentar que as provas foram adulteradas.

Responsável pela coleta	Pedro Paulo Alexandrino.
Localização do dispositivo	Sob a cama do suspeito.
Forma da coleta	O dispositivo e os periféricos foram coletados com uma luva para evitar que novas impressões digitais contaminem o mesmo.
Responsável pela posse	Pedro Paulo Alexandrino.
Procedimento de custódia	O dispositivo e os periféricos foram guardados em um local seguro, hipoteticamente em um cofre, a fim de manter a segurança.

Figura 7. Tabela de Documentação

Nas próximas etapas, aquisição e análise, ambas foram baseadas na metodologia NIST.

5.7 ETAPA 6 – AQUISIÇÃO NA MEMÓRIA INTERNA DO CELULAR

Para iniciar a aquisição é preciso identificar o dispositivo. Para tanto, foi possível visualizar na parte frontal do celular, que a marca é Nokia e o modelo, N85. Após obter essas

informações, foi realizada uma pesquisa no site do fabricante, com o intuito de descobrir o sistema operacional para poder selecionar algumas ferramentas que deverão ser utilizadas na aquisição.

Durante a pesquisa sobre o dispositivo, foi verificado que o mesmo possui um Sistema operacional SymbianOS versão 9.3 S60 3ª edição. E em relação à memória de armazenamento, possui um cartão externo de 128 MB, e interna *flash* de 78 MB.

A aquisição em um celular pode ser entendida como uma extração de todos os dados acessíveis gravados no dispositivo, resultando em um arquivo de imagem com formato especificado pela ferramenta utilizada. Em um celular existem três locais onde podem existir informações: memória interna, externa e SIM. Para esse trabalho, apenas as memórias interna e externa serão analisadas.

Para o celular N85, objeto desse trabalho, foram testadas diversas ferramentas. Porém quase todas as ferramentas de aquisição, funcionam apenas para versões mais antigas do SymbianOS. Por exemplo, a ferramenta Oxygen PM, que foi criada exatamente para esse sistema operacional, a mesma não reconhece o dispositivo, mostrando uma mensagem informando que nenhum dispositivo está conectado.

Outra ferramenta bastante utilizada para aquisição é o Symbian Tool, porém também não funciona para a 3ª edição do SymbianOS, conforme discutido em alguns fórum na internet.

Durante todo esse processo de busca de uma ferramenta de aquisição que funcione corretamente e que seja sem custo, foi percebido que essas ferramentas *free* não são compatíveis com essa versão do sistema operacional do celular. Muitas outras ferramentas para Windows foram testadas sem obter algum tipo de sucesso. Foi testada exaustivamente uma ferramenta para Linux, chamada Wammo, porém a mesma apenas mostrava informações técnicas do dispositivo, não dando a possibilidade de realizar a aquisição, mesmo que essa

fosse uma das suas características principais, pois no momento de dar o comando de backup, surgia uma mensagem informando que nenhum dispositivo está conectado.

A única ferramenta que conseguiu realizar a aquisição no N85 foi a MobilEdit!. Porém a mesma na versão free apenas mostrou informações como SMS, contatos, fotos entre outros, mas não permitiu realizar o backup de toda a memória interna, para permitir uma aquisição física. Então foi realizada na memória interna do celular apenas a aquisição lógica. Ou seja, os dados apagados não foram recuperados.

Após a ferramenta MobilEdit! instalada foi executada a aplicação e feito o reconhecimento do dispositivo via cabo USB. Então foi possível realizar o backup conforme na figura 8, da agenda, SMS, sistema de arquivos, alarmes e MMS.

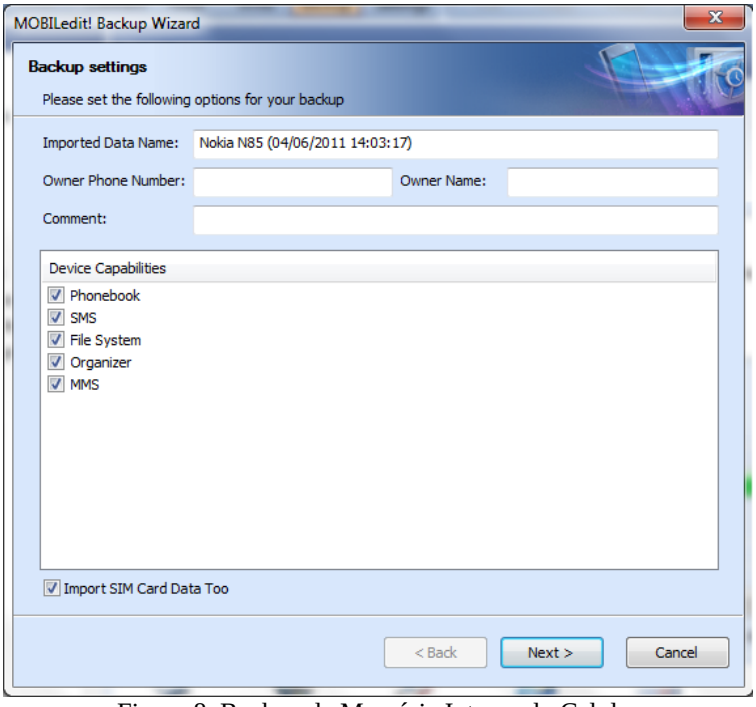

Figura 8. Backup da Memória Interna do Celular

Com o backup realizado, o próprio programa exibe conforme na imagem 9 o local onde se localiza o arquivo de backup, a fim de permitir ao usuário realizar a análise. O arquivo gerado foi nomeado “00000005.dat” com tamanho de 15.350 KB. Nesse momento, foi possível perceber, que essa ferramenta apenas teve acesso às informações lógicas da memória, pois o tamanho total da memória física é 78 MB e apenas 15 MB foram adquiridos.

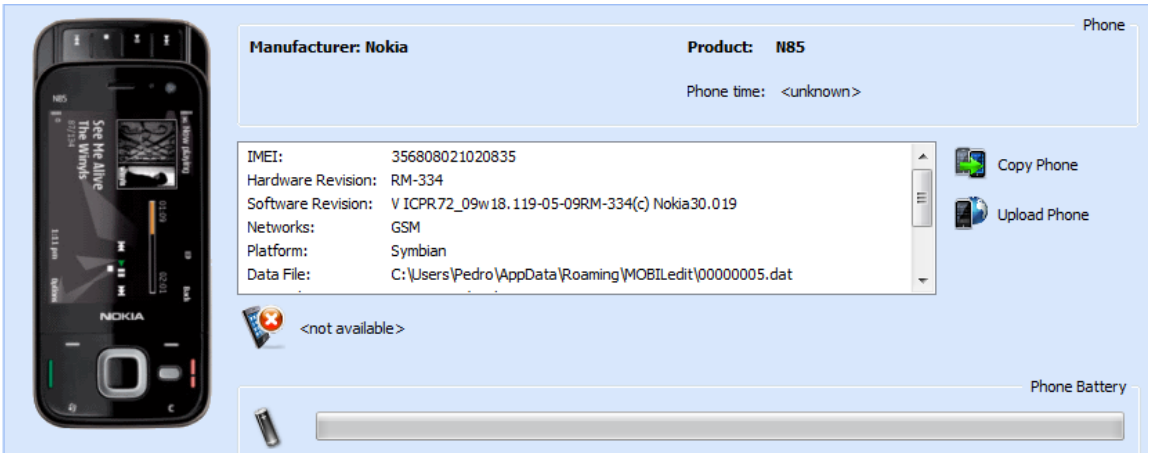

Figura 9. Informações do Celular e Local do Backup

Outras ferramentas documentadas nesse trabalho, como, BackupToGo, SymbianOPM, SymbianTool, Device Seizure, entre outras, não conseguiram realizar a aquisição dos dados na versão free. Possivelmente poderiam conseguir caso a licença fosse adquirida. É preciso salientar que muitas existentes no mercado necessitam hardware além de software, aumentando consideravelmente o custo da ferramenta.

A ferramenta MIAT, que tem como finalidade fazer uma cópia dos dados da memória interna para externa foi utilizada, porém não conseguiu realizar esse processo. Pesquisando em alguns fóruns foi descoberto que não é possível realizar essa aquisição para celulares com SymbianOS da terceira geração. Nada oficial sobre o assunto foi encontrado.

A seguir serão mostrados os passos para realizar o exame e análise na imagem de backup criada.

5.8 ETAPA 7 – EXAME E ANÁLISE NA MEMÓRIA INTERNA DO CELULAR

Existem muitas ferramentas que realizam a análise em um arquivo de backup com informações em hexadecimal. Algumas ferramentas mostram as informações contidas de forma visual separando conforme a estrutura lógica do celular, como a própria ferramenta MobilEdit!. Outra ferramenta utilizada nesse trabalho para exame e análise, é a Forensic

Toolkit. Essa ferramenta é muito utilizada pelas comunidades forenses, pois possibilita uma análise muito detalhada em um arquivo imagem de backup.

A seguir veremos como foi feito o exame e análise na ferramenta MobilEdit!.

5.8.1 MobilEdit! 5

Com a ferramenta em execução foi possível importar o backup gerado pela própria ferramenta. De forma visual, a mesma mostra todas as informações lógicas do celular. Como na imagem 10, podemos ver os alguns contatos cadastrados. Informações como data e hora do cadastro, não são fornecidos pela ferramenta. Na posição onde está escrito "número" na cor em vermelho, estava o número do celular referente ao nome cadastrado.

Figura 10. Contatos Cadastrados na Agenda do Celular

Nas próximas figuras 11 e 12 pode-se visualizar as mensagens de texto recebidas e enviadas separadamente ordenadas por data e hora da mais atual para mais antiga. Da mesma forma que na agenda de contatos não são mostrados os números, das mensagens também foram retirados.

Figura 11. Mensagens de Texto Recebidas

Figura 12. Mensagens de Texto Enviadas

Em relação às mensagens multimídias, apenas foram encontradas nas mensagens enviadas do celular. Na opção de mensagens multimídias recebidas, conta que nada foi recebido.

Pode-se ver nas imagens 12 e 13, que é possível visualizar as fotos e o número do destinatário.

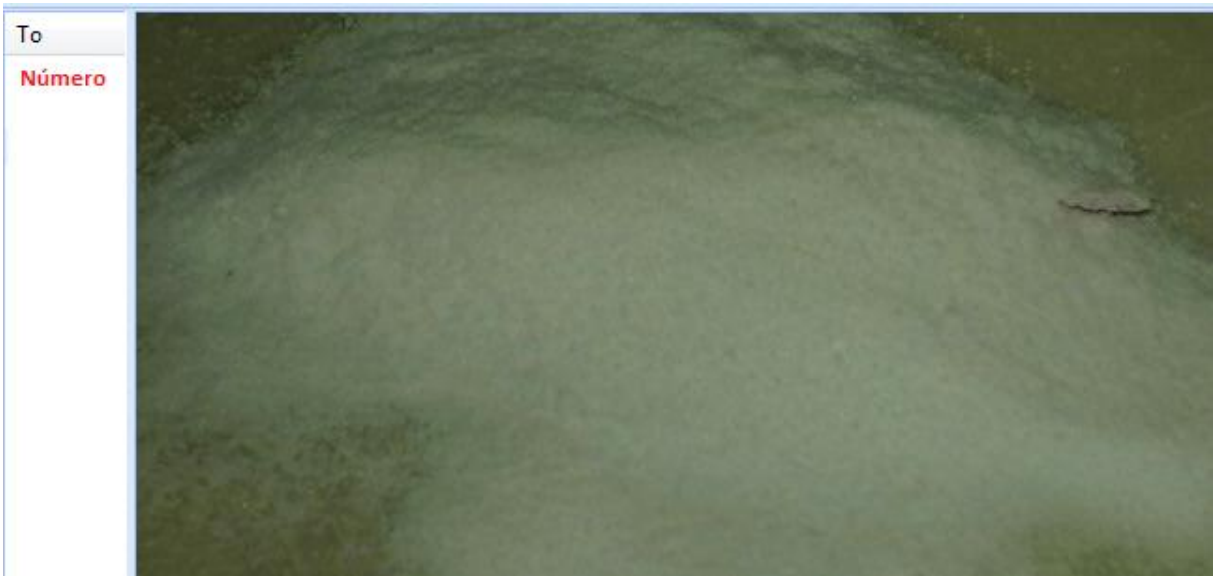

Figura 13. Primeira Mensagem Multimídias Enviada

Em uma análise superficial apenas visualizando as fotos, não é possível concluir que materiais são esses. Pois a figura 12, apenas mostra um pó branco sem características peculiares. E na foto 13 apenas mostra cápsulas que podem ser de remédios. Porém, essas mensagens multimídias contêm mensagem de texto inclusa, que referente a figura 12 a mensagem é “poh. e é puro”. Já na figura 13, a mensagem é “bomba”. Nesse momento, juntando essas informações com as mensagens de texto, algumas provas já podem se transformar em evidências.

Figura 14. Segunda Mensagem Multimídias Enviada

Outra busca foi feita nos agendamentos e tarefas da imagem extraída do celular. Porém nenhuma informação foi registrada.

A seguir poderemos ver como conseguir algumas dessas informações obtidas pelo MobilEdit na ferramenta Forensic Toolkit.

5.8.2 Forensic Toolkit v1.5

Essa ferramenta tem a capacidade de ler a imagem gerada pelo MobilEdit e fazer busca em todo o backup com palavras chaves. Logo veremos que, por exemplo, as mesmas mensagens encontradas com a análise do MobilEdit podem ser encontradas também no Forensic Toolkit. Porém de uma forma mais desordenada sem padrões. Da mesma forma os contatos entre outras informações também podem ser encontradas.

Inicialmente a ferramenta pede para criar um caso ou escolher um já existente. Como está sendo trabalhado na imagem do celular, foi criado um novo caso conforme imagem 15.

Avançando na criação do caso, outras informações como agência, nome do examinador, telefone e-mail, são solicitados pelo software.

Todas essas informações solicitadas pelo software são importantes para que se crie um padrão de documentação. Torna-se complicado gerenciar vários casos abertos se suas peculiaridades não são informadas. Mesmo assim, essa ferramenta permite que essas informações não sejam cadastradas.

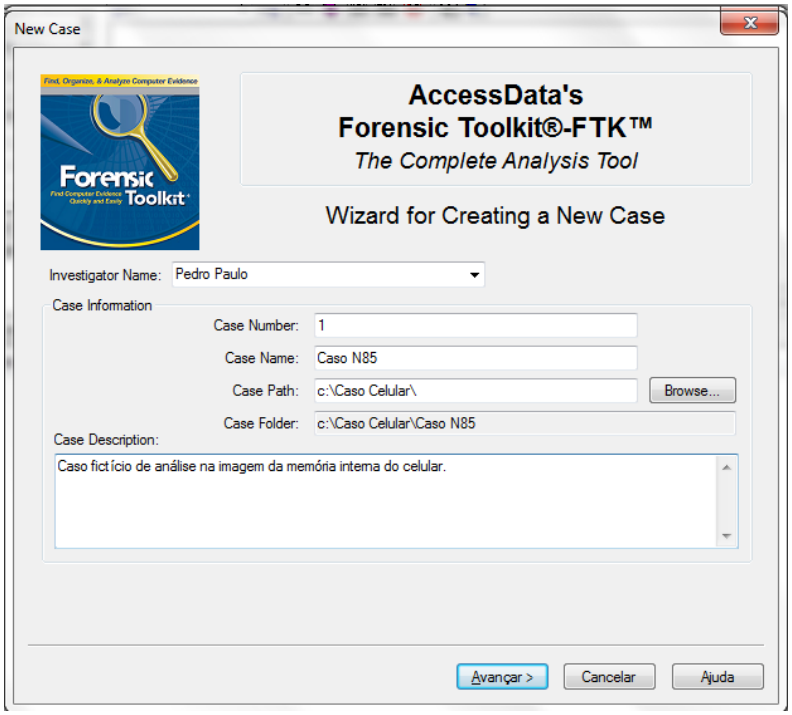

Figura 15. FTK - Novo Caso

Seguindo com o próximo passo, é preciso adicionar o arquivo de imagem gerado pelo MobilEdit conforme imagem 16.

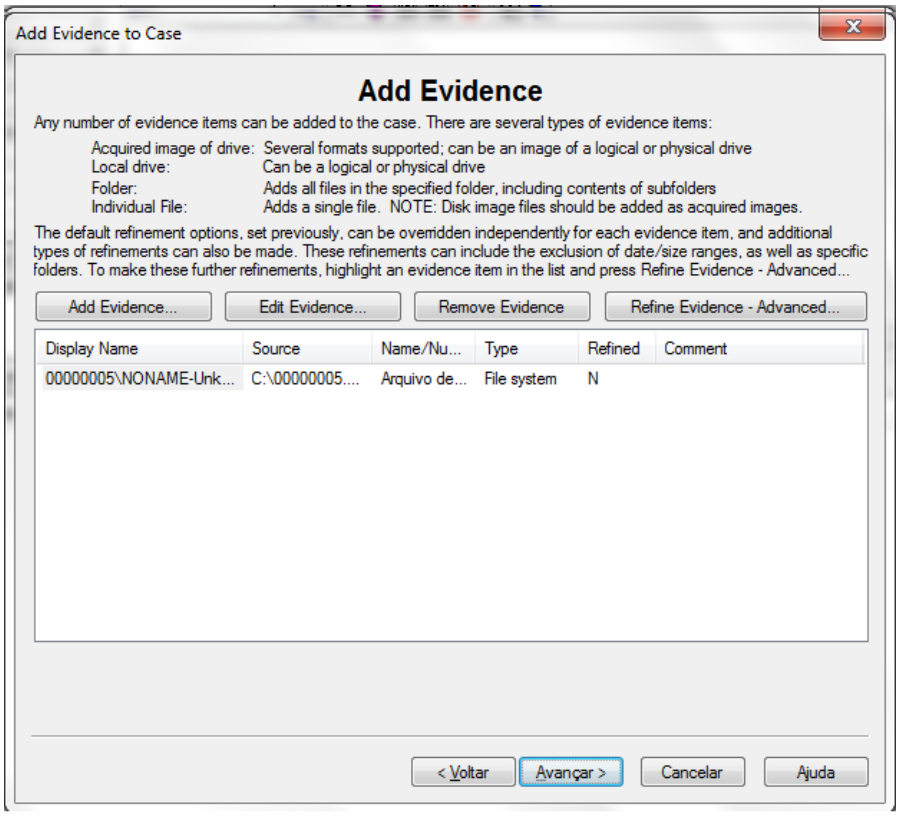

Figura 16. Adicionar Arquivo de Imagem

Nessa ferramenta, é possível analisar várias imagens ao mesmo tempo. Mas nesse caso, apenas uma imagem foi preciso analisar.

Na imagem 16 podemos ver a área de trabalho da ferramenta. Logo é possível visualizar que onde está circulado, estão as informações da imagem em hexadecimal. Já no quadro ao lado, as informações em ASC respectivamente à mesma linha.

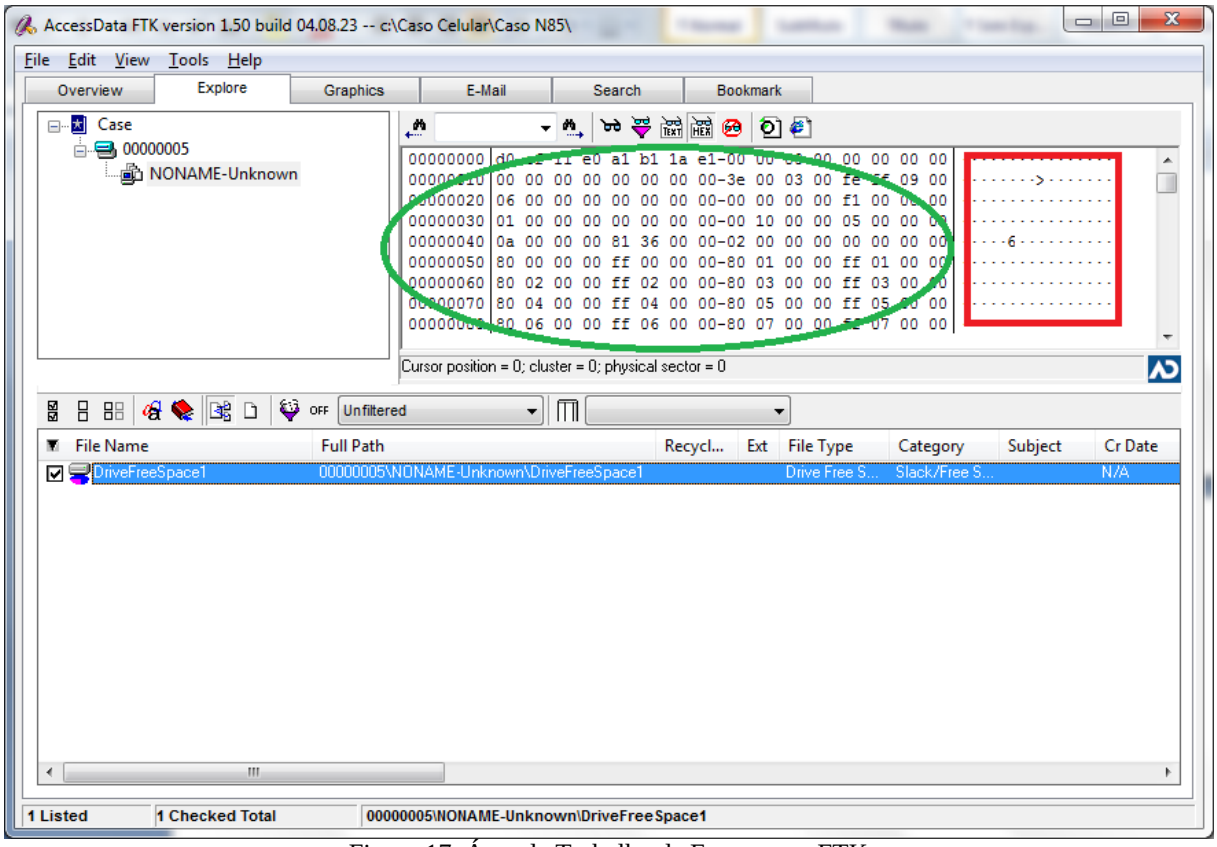

Figura 17. Área de Trabalho da Ferramenta FTK

Nesse momento é possível fazer uma varredura completa em todas as informações deslizando a barra de colagem ou simplesmente filtrar utilizando uma palavra chave.

Como já sabemos que na agenda de contatos existe hipoteticamente um número cadastrado com nome de Andrei, fiz um busca para mostrar como a informação aparece na tela, conforme imagem 18.

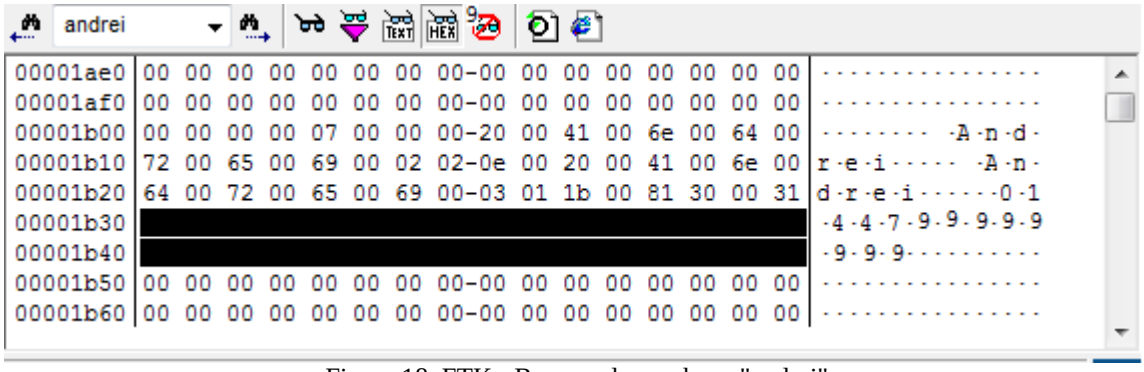

Figura 18. FTK - Busca palavra chave "andrei"

Note que nessa imagem 18 aparece do lado direito da imagem o nome Andrei e na sequência o número correspondente. Por motivos de sigilo o número foi alterado e os valores correspondentes em hexadecimal receberam uma tarja preta.

Conforme podemos ver na imagem 19, fiz uma busca da palavra “maconha”, resultando na mensagem de texto que foi enviada. Veja na figura 18 que nessa ferramenta ao selecionar a mensagem ASC, automaticamente também é selecionado a parte hexadecimal correspondente.

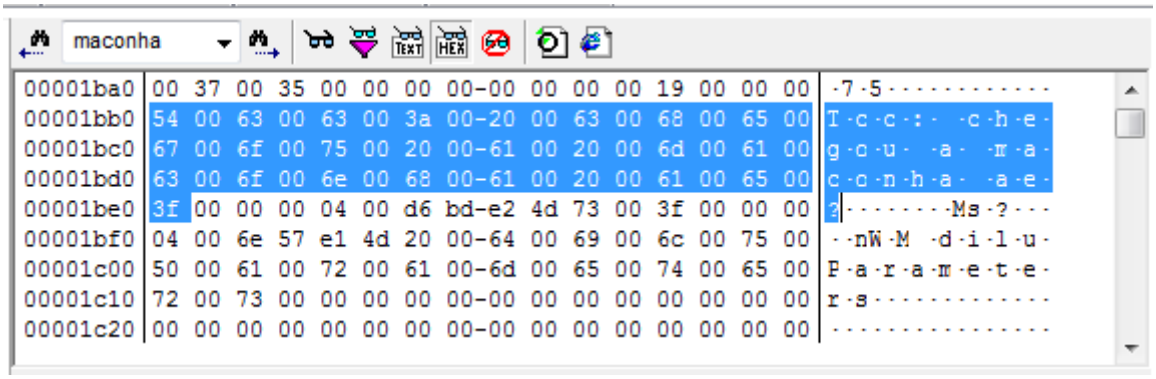

Figura 19. FTK - Busca palavra chave "maconha"

5.9 ETAPA 6 – AQUISIÇÃO NA MEMÓRIA EXTERNA DO CELULAR

Em relação à memória externa do celular, para esse caso, um cartão micro SD, existe muitas ferramentas *free* e pagas que conseguem recuperar informações de cartão de memória, tanto para Windows quanto Linux Porém, para utiliza-las dentro da metodologia

forense, é preciso inicialmente fazer uma cópia das informações originais, criando um arquivo imagem.

Para realizar uma aquisição na memória externa é preciso retirar o cartão de memória do dispositivo. No caso do Celular N85, foi preciso retirar o cartão e conecta-lo em um leitor.

Após conecta-lo no leitor foi aberto o terminal dentro do Linux. Na sequência executado o comando “fdisk -l” para saber o endereço do cartão de memória, conforme imagem 20.

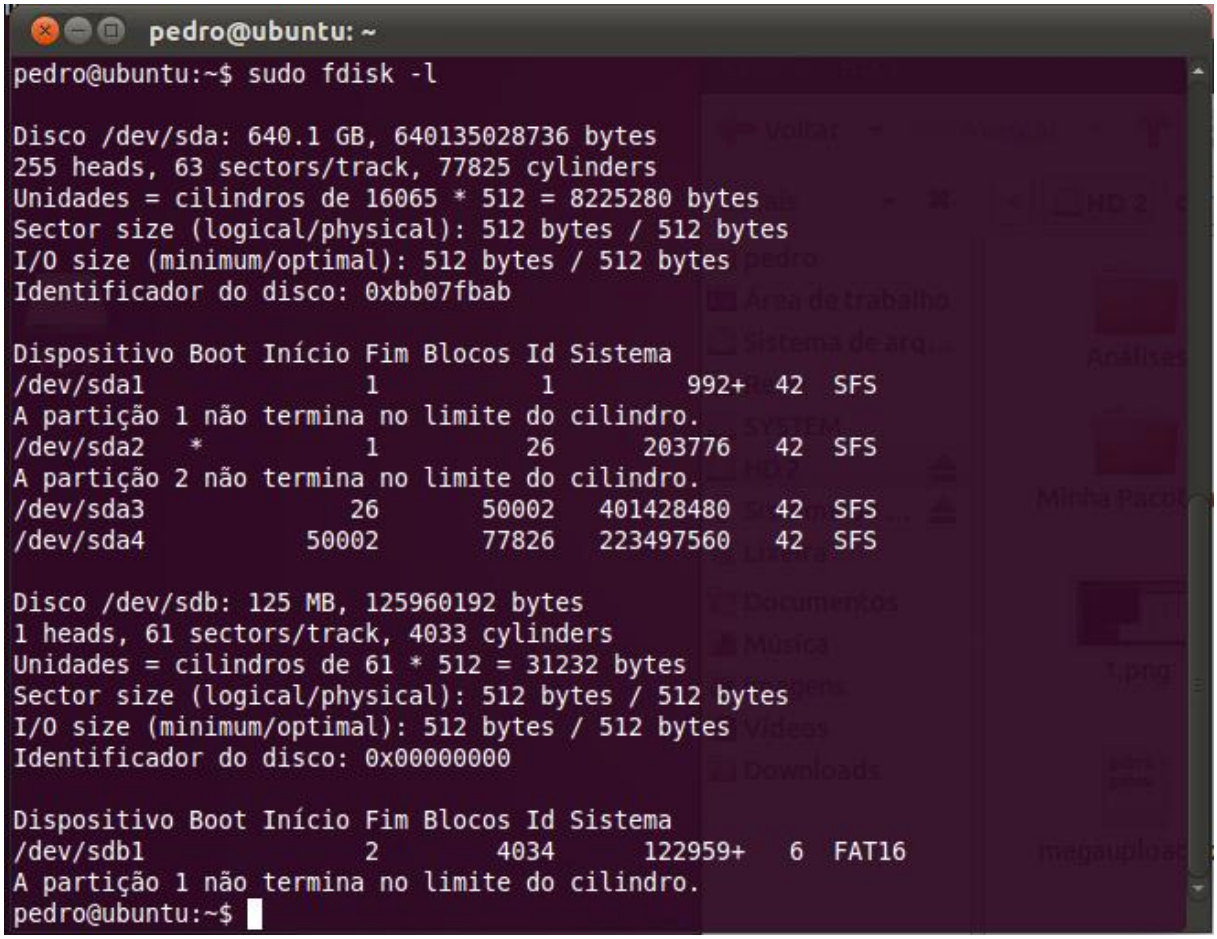

Figura 20. Comando: fdisk -l

Pode-se visualizar na parte de cima da imagem 20 que foi encontrado um disco de 640.1 GB, que é o principal do computador e um outro disco na parte de baixo, no caso,

cartão de memória de 125 MB que é o dispositivo que sofrerá uma cópia. O local de acesso ao cartão de memória foi “⁄dev⁄sdb”.

O próximo passo foi criar um diretório para gravar a imagem do cartão do celular. Para criar o diretório “recuperados” foi utilizado o comando “mkdir recuperados” conforme segue na imagem 21.

Figura 21. Comando: mkdir recuperados

Para criar a imagem do cartão foi preciso executar o comando “dd if=/dev/sdb1 of=cartao.img”, onde o “if” é o dispositivo a ser recuperado e o “of” é o local onde deseja salvar a imagem.

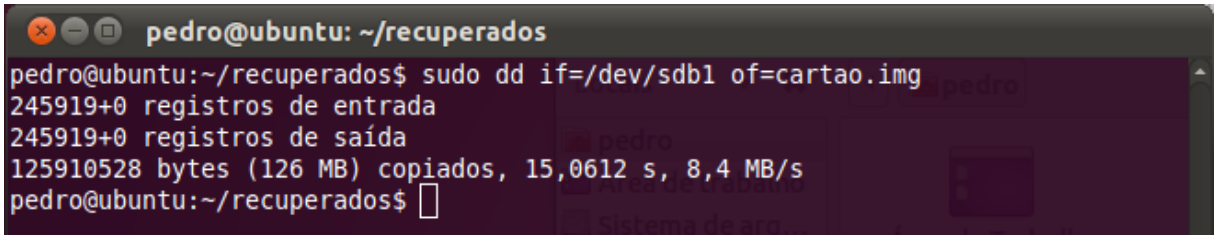

Figura 22. Comando: dd if=/dev/sdb1 of=cartao.img

Nesse momento foi criado o arquivo “cartao.img” com tamanho de 126 MB no diretório “recuperados”. O tempo de processo foi 15,06 segundos.

A seguir serão mostrados os passos para realizar a análise na imagem criada do cartão de memória.

5.10 ETAPA 7 – EXAME E ANÁLISE NA MEMÓRIA EXTERNA DO CELULAR

5.10.1 PhotoRec

Com a ferramenta PhotoRec foi possível realizar a análise da imagem criada. Essa ferramenta tem a função de extrair todas as informações da imagem, até mesmo os arquivos que foram excluídos.

A figura 23 mostra a ferramenta PhotoRec iniciada. Para tanto, foi preciso executar o comando “PhotoRec cartao.img”.

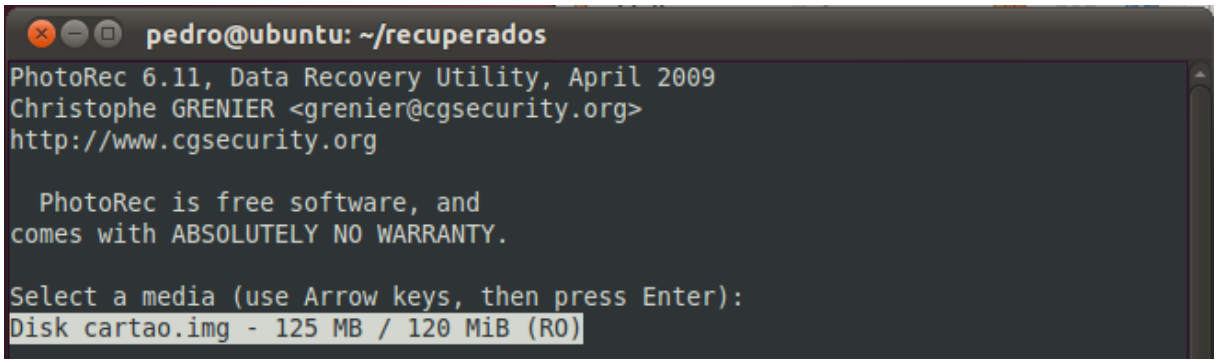

Figura 23. Comando: PhotoRec cartao.img

Na figura 24 foi preciso selecionar a opção “No partition”.

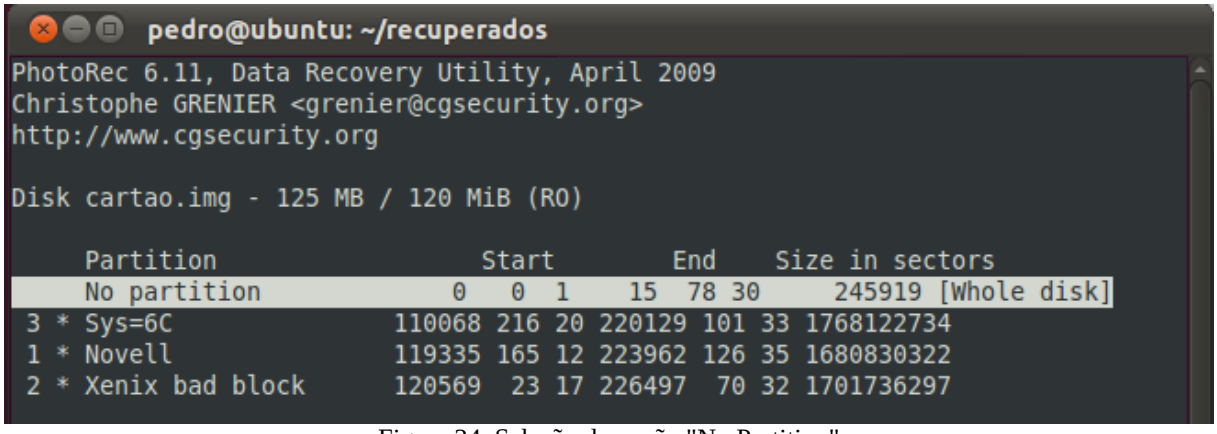

Figura 24. Seleção da opção "No Partition"

A seguir foi selecionado o sistema de arquivos “Other” ilustrado na figura 25.

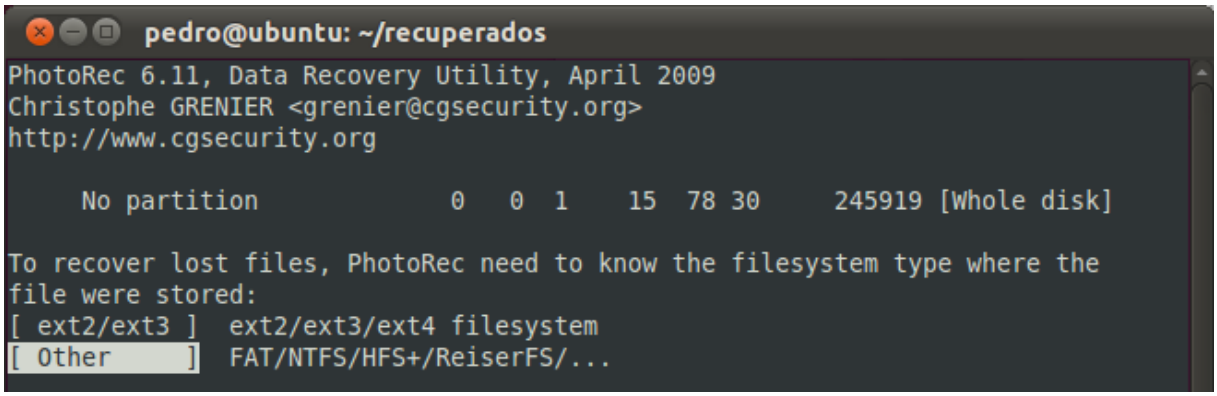

Figura 25. Seleção da opção "Other"

Conforme figura 26 foi selecionado a opção “-rw-r--r--” e pressionado a tecla “Y” para confirmar.

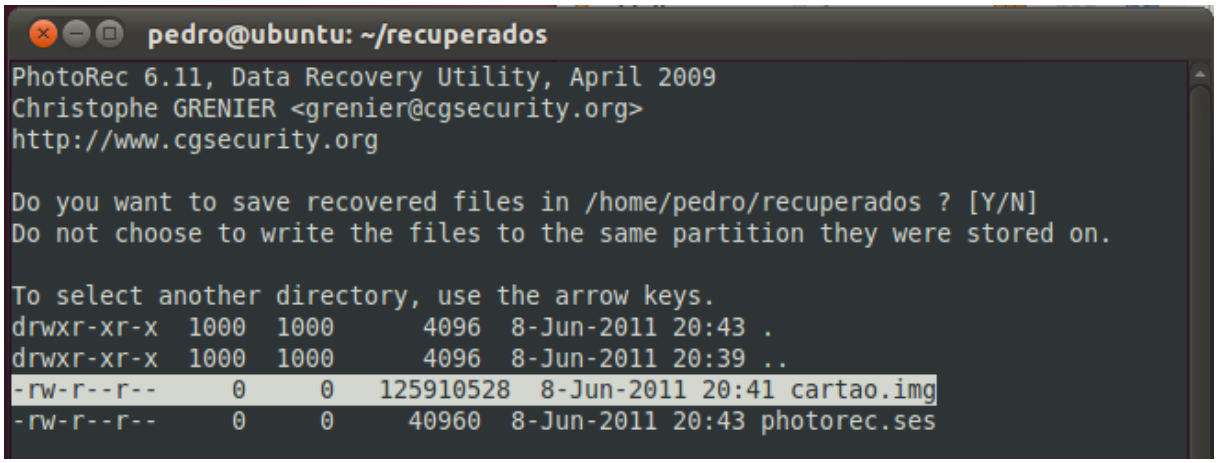

Figura 26. Seleção da opção "-rw-r--r--"

Por fim, foram recuperados 98 arquivos. Sendo que 75 possuiem extensão TXT/VCF, 21 JPG, 1 MP3 e 1 ZIP, conforme imagem 27.

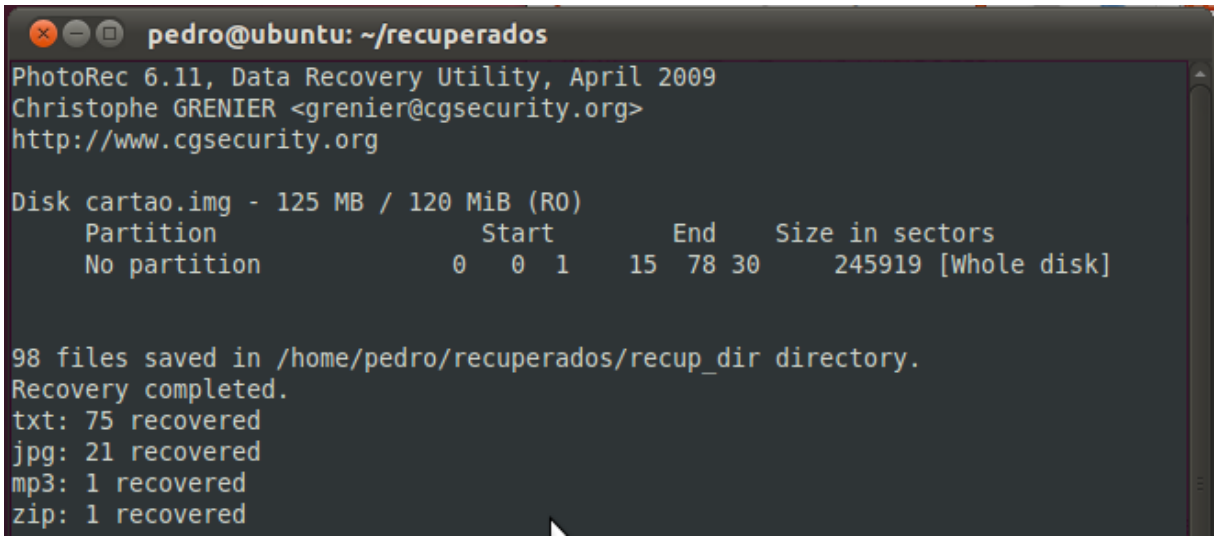

Figura 27. Fim do Processo de Recuperação

Na Figura 28 podemos ver os arquivos recuperados com a ferramenta PhotoRec, localizados no diretório "/home/pedro/recuperados/recup_dir".

Figura 28. Arquivos Recuperados

Analizando esses arquivos, foi percebido que existem alguns com extenção .vcf, que são os contatos cadastrados. Todos esses arquivos não estavam disponíveis no cartão de memória, porém o PhotoRec conseguiu recuperar conforme imagem 29.

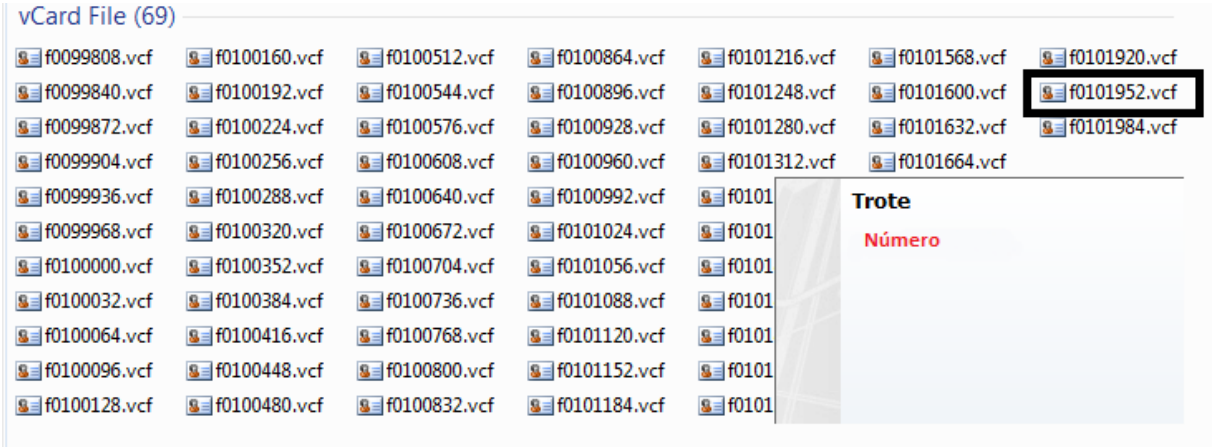

Figura 29. Contatos Excluídos

Note na Figura 29, que o arquivo circulado, é corresponndente ao contato “Trote”, que é um contato excluido.

Dentre os arquivos com extenção .jpg, estão muitas fotos pessoais como a Figura 30, porém outras fotos suspeitas podem serem visualizadas nas Figuras 31 e 32.

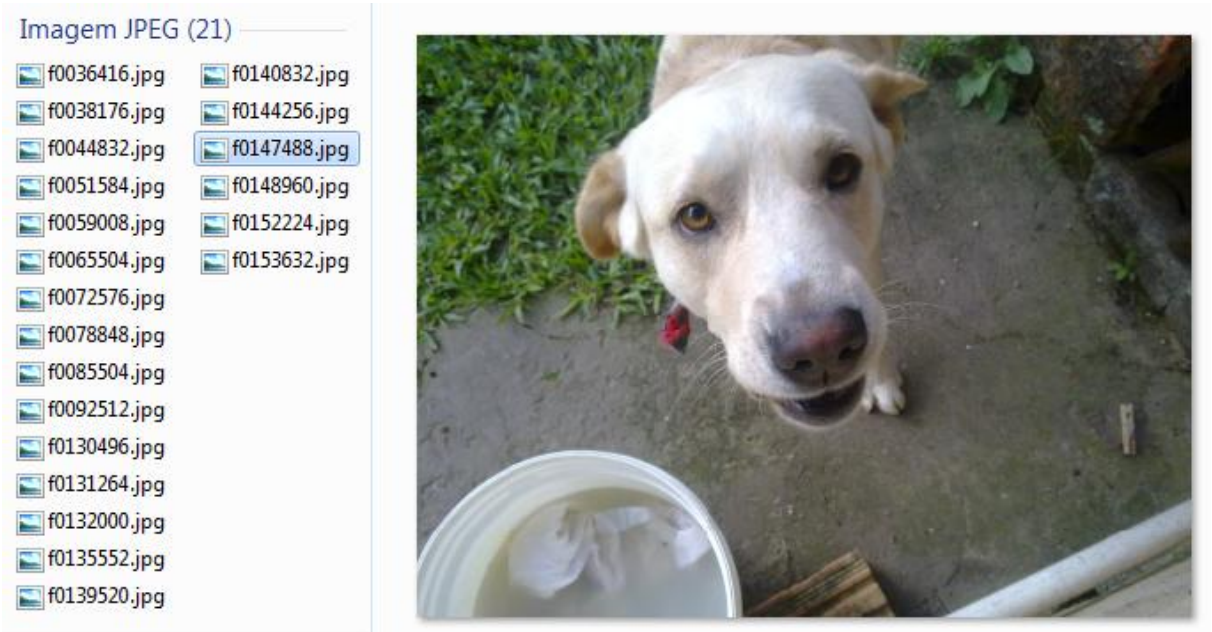

Figura 30. Foto Pessoal Recuperada

Figura 31. Primeira Foto Suspeita Recuperada

Figura 32. Segunda Foto Suspeira Recuperada

Outros arquivos encontrados na memória, como, música e arquivos de texto, foram encontrados a avaliados, porém nenhuma informação importante foi encontrada, portando não têm relevância para o caso.

Em relação a memória externa, outras ferramentas principamente para Windows foram avaliadas. Porém como é preciso inicialmente criar uma imagem antes de extrar os

dados do cartão de memórias, foi utilizado a ferramenta USB Image Tool, que permite fazer essa cópia fiel das informações.

As ferramentas de recuperação de informações, normalmente extraem apenas as informações de unidades de armazenamentos do SO, dificultando realizar a análise em imagem. Portanto, foi utilizado a ferramenta chamada Gizmo para que seja possível montar a imagem tornando-a uma unidade virtual. Para realizar essa montagem, poderia também ser utilizado o programa UltraIso ou até mesmo o Daemon Tools.

5.10.2 Recuva v1.38

Após imagem emulda foi utilizada a ferramenta Recuva v1.38, porém a mesma apenas recuperou um arquivos com formato JPG, conforme Figura 33, com cor em verde. Essa ferramenta mostra os registros que foram excluídos, possibilitantdo recuperar caso a cor seja verde. Caso contrário, não consegue recuperar.

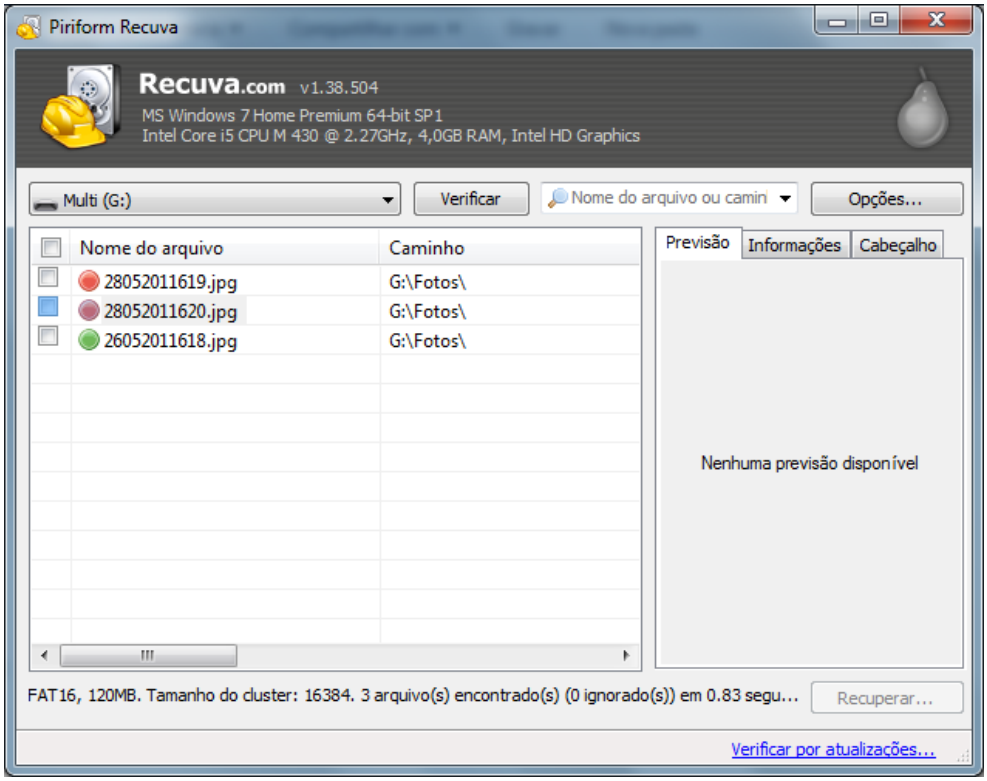

Figura 33. Análise na ferramenta Recuva v1.38

5.10.3 PC Inspector File Recovery

Outra ferramenta testada foi a PC Inspector File Recovery. Ela conseguiu um resultado um pouco melhor, pois permitiu recuperar três aquivos com extenção JPG, conforme imagem 34.

Figura 34. Análise na Ferramenta PC Inspector File Recovery

Fazendo uma comparação, entre as três ferramentas, podemos concluir que a PhotoRec é muito superior às outras. Pois ela extraiu todas as informações da imagem. Tanto arquivos apagados quanto os disponíveis. É importante salientar, que antes de iniciar o estudo de caso, o cartão de memória possuia informações, e o mesmo foi formatado para iniciar o trabalho. Mas a ferramenta PhotoRec conseguiu até mesmo recuprar os dados formatados. Por

esse fato, a mesma foi utilizada como ferramenta principal na análise dos dados do cartão de memória externa do celular.

5.11 ETAPA 8 – APRESENTAÇÃO OU DOCUMENTAÇÃO

Esta etapa da metodologia NIST foi trabalhada durante todo o processo pericial. É crucial para que se possa redigir um laudo pericial fiel aos fatos. A documentação completa pode ser visualizada no apêndice A do presente trabalho.

5.12 ETAPA 9 – DECISÃO

Nessa etapa é preciso chegar a uma conclusão para o caso analisado. Devido às evidências fictícia encontradas nas mensagens de texto e multimídia, enviadas e recebidas, contendo informações ligadas a um tráfico de drogas, foi concluído que o portador do celular, José Alfredo realmente realizou um crime digital.

5.13 ETAPA 10 – DEVOLUÇÃO DAS PROVAS

Por ser um caso fictício, não se faz necessário realizar a devolução das provas encontradas. Caso contrário, o celular juntos com os demais periféricos, deveriam ser devolvidos ao proprietário. Essa etapa é baseada na metodologia de Reithm Carr e Gunsch.

5.14 ETAPA 11 – RECONSTRUÇÃO DA CENA DO CRIME

Nessa etapa, baseada na metodologia SOP, é preciso fazer a reconstrução dos eventos corridos relacionados ao crime digital. Juntando todas as evidências para determinar o que realmente aconteceu.

Portanto, devido às evidências encontradas, hipoteticamente o portador do celular utilizou o mesmo para envio de mensagem, realizando uma suposta venda de drogas e recebeu algumas mensagens correspondendo às mensagens enviadas. Também utilizou o celular para capiturar fotos do seu produto. Algumas dessas fotos foram enviadas para supostos usuários do mesmo. Tudo isso aconteceu no período de 22 de maio de 2011 à 02 de junho de 2011.

A seguir pode-se visualizar a documentação dos registros e procedimentos realizados sobre a perícia. Para tanto, foi criado um laudo pericial que seque abaixo.

LAUDO PERICIAL

Perito/Examinador: Pedro Paulo Alexandrino
Data: 03 de Junho de 2011 Horário: 20:15

Descrição da Perícia: Perícia realizada em um Celular N85.

Observações: A presente 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.

1 PRIMEIRA PARTE - Análise na Memória Interna do Celular:

1.1 Contatos Cadastrados

Com a ferramenta MobilEdit foi possível realizar a extração de todos os contatos cadastrados no celular, logicamente, conforme imagem a seguir.

Nome	Numeri	Nome	Número	Nome	Número	Nome	Número
Francine	96347959	Alemao	99999999	Bernardo	99999999	Danilo	99999999
Franco	99999999	Amor	99999999	Bom Jovi	99999999	Dany	99999999
Unita	99999999	Amor Casa	99999999	Botini	99999999	Dany Casa	99999999
Diego	99999999	Anderson Henri	99999999	Bruno	99999999	Darlan	99999999
Anderson	99999999	Anderson Wz ¡	99999999	Carlos Henriqu	99999999	Departam	99999999
Lanche	99999999	Andrei	99999999	Carlota	99999999	Dessa	99999999
Adreana	99999999	Angelo	99999999	Colonetti	99999999	Dimi	99999999
Zecar	99999999	Aniceto	99999999	Comp. Angel	99999999	Edi	99999999
Airtu	99999999	Aniceto 2	99999999	Contato	99999999	Elaine	99999999
Alan	99999999	Bereta	99999999	Dacio	99999999	Fabiano	99999999

1.2 Mensagens de Texto Enviadas:

Em relação às mensagens de texto enviadas foram encontradas com o MobilEdit apenas as mensagens listadas a seguir.

Número	Data e Hora	Mensagens
99999999	28/05/2011 17:13	Tcc: vai querer quantos gramas?
99999999	29/05/2011 18:42	Tcc: chegou a maconha ae?
99999999	31/05/2011 20:19	Chegou um bagulho novo e puro. Ta afim?
99999999	31/05/2011 20:29	Ta na mao tua encomenda. 200 reais
99999999	31/05/2011 20:42	300 mangos na buxa. Feito?
99999999	01/06/2011 13:36	Tem. Queis quanto?

1.3 Menagens de Texto Recebidas:

Em relação às mensagens de texto recebidas foram encontradas com o MobilEdit apenas as mensagens demonstradas na imagem a seguir.

Número	Data e Hora	Mensagens
99999999	22/05/2011 13:41	alcool, barbituricos, maconha, diluentes,...
99999999	23/05/2011 09:03	Tcc: Eh uma lista e tanto. Erva pura
99999999	28/05/2011 17:23	Quando chega o pacote?
99999999	24/05/2011 19:01	Ligue Agora! Ja estou disponivel para receber chamadas ...
99999999	30/05/2011 20:49	vou pra cademia agora, se quiser passar por lah...
99999999	31/05/2011 20:37	ok. vou buscar. segura o po ae
99999999	31/05/2011 20:37	To afim sim. Quanto faz pra mim um pacote fechado?
99999999	31/05/2011 20:44	To afim sim . Quanto faz pra mim um pacote fechado?
99999999	31/05/2011 20:44	Feito.
99999999	01/06/2011 13:35	tem produto?
99999999	01/06/2011 13:39	me ve um 50 pila

1.4 Mensagens Multimídia Enviadas:

Nas mensagens multimídias não existem registros de data e hora de envio. A seguir segue as 3 mensgens enviadas:

Número	Mensagem	Imagem
99999999	bomba	

Número	Mensagem	Imagem
99999999	poh	

Número	Mensagem	Imagem
99999999	eh pura	

1.5 Mensagens Multimídia Recebidas:

Nenhuma mensagem multimídias recebida foi encontrada.

1.6 Agendamentos:

Nenhum agendamento foi encontrado.

1.7 Tarefas:

Nenhuma tarefa foi encontrada.

1.8 Ligações:

Com a ferramenta MobilEdit não foi possível encontrar as ligações realizadas e recebidas.

Observações: Informações excluídas da memória interna do celular, não puderam ser recuperadas. Mesmo assim, informações importantes foram extraídas. Outras informações como e-mails, páginas da Web, entre outras, não foram localizadas, pois nenhuma ferramenta estudada, conseguiu encontrar essas informações.

2 SEGUNDA PARTE - Análise na Memória Externa do Celular:

2.1 Fotos:

Com a ferramenta PhotoRec foram encontradas 21 fotos. Dentre elas duas são suspeitas que seguem abaixo:

2.2 Arquivos de Texto:

Com a mesma ferramenta foram localizados 3 arquivos de texto, porém nada que possa ser utilizado como prova.

2.3 Contatos Cadastrados:

Em relação aos contatos cadastrados na memória externa do celular, foram encontrados 69 arquivos. Todos foram recuperados fisicamente. Não existia nenhum vinculo desses contatos com as mensagens encontradas na memória interna do celular. Apenas para um melhor entendimento, os contatos de um celular, podem ficar armazenados na memória interna, externa ou no SIM do celular.

2.4 Outros Arquivos:

Foram localizado outros arquivos com a ferramenta PhotoRec, porém nada com significância para o caso.

Resultado:

Analisando-se todas as provas encontradas, combinando a análise da memória interna com a externa, foi possível concluir que o proprietário do celular N85, José Alfredo, realisou um crime digital enviando mensagens como “chegou a maconha ae?”, no dia 29/05/2011 às 18:42:46, algumas mensagens suspeitas como “Chegou um bagulho novo e puro. Ta afim?” no dia 31/05/2011 às 20:19:45, “Ta na mao tua encomenda. 200 reais” no dia 31/05/2011 às 20:29:35, entre outras.

Parar reforçar o resultado, José Alfredo enviou mensagens multimídias para três contatos, com fotos aparentemente de anabolisante e cocaína. A data e a hora de envio não foi possível recuperar. Essas mesmas fotos enviadas, foram encontradas na memórias externa do celular. As mesmas precisaram ser recuperadas, pois foram excluídas. O que demonstra, que José encaminhou as mensagens e logo excluiu as fotos.

CONCLUSÃO

Devido ao aumento crescente de usuários utilizando celulares inteligentes, os crimes digitais estão se tornando um problema cada vez maior. A perícia forense computacional surge, como uma grande aliada na batalha contra a impunidade existente atualmente, contribuindo para que a sociedade seja mais justa e segura.

A perícia forense, utiliza meios científicos na identificação e ação contra crimes digitais. Com o passar do tempo, os resultados periciais estão tomando gradativamente um espaço nos processos judiciais, fazendo com que aumente a necessidade de otimizar o proceso de coleta, preservação, aquisição e análise de provas.

É extremamente importante que a metodologia utilizada em uma investigação seja aceita pelos órgãos judiciais, e que os procedimentos sejam feitos da maneira correta. Pois um erro durante a realização pode culpar um inocente, vice versa, ou até mesmo invalidar a investigação.

Perícia forense em celular é um assunto muito recente no País. É conhecido como complexo, pois diferentemente dos microcomputadores pessoais, os celulares possuem arquiteturas e softwares diferentes. Fazendo com que os procedimentos realizados com sucesso em um dispositivo, não ter o mesmo resultado em outro. Por esse fato, esse trabalho tem como objetivo aplicar técnicas computacionais forenses para a busca e análise de informações contidas em celulares com SymbianOS. Para cumprir esse objetivo foram traçados quatro objetivos específicos alcançados no decorrer desse estudo.

O primeiro objetivo específico foi iniciado no Capítulo 3, a fim de entender os princípios básicos da perícia forense computacional, e foi aplicado no Capítulo 5, demonstrando os passos para se realizar o processo pericial.

O segundo objetivo específico foi abortado durante o Capítulo 3, mostrando os aspectos que envolvem a análise de evidências em um dispositivo móvel. Desde aspectos a serem analisados, ferramentas disponíveis, até metodologias forenses.

A utilização das ferramentas forenses na busca de evidências em aparelhos celulares faz parte do terceiro objetivo específico. Essas informações são demonstradas durante todo o Capítulo 5.

Também no capítulo 5 é definido o cenário para realizar os experimentos na buscar por evidências.

Pelo fato de que os objetivos específicos foram alcançados, acredita-se que o objetivo geral também foi atingido. Pois com auxilio do caso fictício, foram demonstrados todos os passos da junção das metodologias forenses abordadas.

Contudo foi percebido que existem poucas ferramentas disponíveis sem custo para realizar aquisições das informações. Muitas delas na versão free são restritas, porém prometem absoluto sucesso caso seja adquirida a licença.

Entre outras, existem os Kits, agregando Hardware ao Software, abrangendo quase todos os modelos de celulares, com conectores para diferentes fabricantes, tornando o processo menos complexo, adquirindo os dados com maior facilidade. Esses Kits possuem um custo bastante elevado, mas é altamente recomendado para peritos que desejam trabalhar com a ciência forense em dispositivos celulares.

O presente estudo abre caminhos para futuros trabalhos, como perícia forense em celulares com sistema operacional Android, processo anti forense em dispositivos móveis e perícia forense no cartão SIM do celular.

REFERÊNCIAS

ALBUQUERQUE, Ricardo; RIBEIRO, Bruno. **Segurança no Desenvolvimento de Software:** Como desenvolver sistemas seguros e avaliar a segurança de aplicações desenvolvidas com base na ISO 15.408. Editora Campus. Rio de Janeiro. 2002

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 6023**: informação e documentação: referências: elaboração. Rio de Janeiro, 2002.

BARYAMUREEBA, Venansius; TUSHABE, Florence. **The Enhanced Digital Investigation Process Model**. DIGITAL FORENSIC RESEARCH WORKSHOP, 2004, Maryland, USA, 2004.

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.

BAGGILI, I. M.; MISLAN, R.; ROGERS, M. Mobile Phone Forensics Tool Testing: A Database Driven Approach. **International Journal of Digital Evidence**, New York, v. VI, p. 1-11, 2007. ISSN 1938/0917.

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.

BRASIL. ABNT. **Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão de segurança da informação.** 2009. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=1532>. Acesso em: 15 set. 2010.

CASEY, Eoghan. **Crime Investigation:** Forensic Tools and Technology. 2ª. ed. Londres, UK: Academic Press, 2003.

CASEY, Eoghan. **Digital Evidence and Computer Crime:** Forensic Science, Computers, and the Internet. 2d. Londres, UK: Academic Press, 2004.

CASTRO, C. R. A. **Crimes de Informática e Seus Aspectos Processuais**. 2.ed., Rio de Janeiro: Lúmen Júris, 2003.

CERQUEIRA FILHO, A. L. P; PINTO, M. B. C. **A Telefonia Celular**, Salvador: CienteFico, BR-BA, 2004. 9 f. Disponível em: <http://www.frb.br/ciente/Impressa /Info/I.6.Filho, ALPC.TELEFONIACELULAR.pdf> . Acesso em: 10 de Novembro de 2010.

DIMER, Ramiro Webber. **Perícia Forense Computacional Aplicada a Ambientes New Technologies File System (NTFS)**. 2007. 94 f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) - Universidade do Extremo Sul Catarinense, Criciúma.

FARLEY, Tom. **Mobile Telephone History**, Califórnia, 2005. 34 f. Disponível em: <http://www.cems.uwe.ac.uk/~rwilliam/ CSA_course/mobile_phone_history.pdf> . Acesso em: 10 de Novembro de 2010.

GALVÃO, M. L. **Tratamento de Evidências Digitais na Segurança de Informações**. 2009. 49 f. Trabalho de Conclusão de Curso (Graduação Tecnologia em Análise e Desenvolvimento de Sistemas) – Faculdade de Ciências Sociais, Cascavel.

HARRISON, R. SHACKMAN. **Symbian OC C**++for mobile phones. England: WILEY, 2007.

JANSEN, Wayne; AYERS, Rick. **Guidelines on Cell Phone Forensics:** Recommendations of the National Institute of Standards and Technology. USA, 2007.

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

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

KRAUSE, W. G.; HEISER, J. G. **Computer Forensics:** Incident Response Essentials. Boston: Addison, 2002.

LAURENO, Marcos A. P; MORAES, Paulo E. S. **Segurança Como Estratégia de Gestão da Informação**. Brasília, BR, 2005.

LEITE, Thiago F. M. **Perícia Forense em Software Livre**. 2006. 155 f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – UNIDESC.

LUIZ, Daniel Junior Oliboni; MAAS, Juliano Henrique. **Sistema Operacional Symbian OS**. BR, 2010. 4p. Disponível em: <

http://www.oficinadanet.com.br/artigo/outros_sistemas/sistema_operacional_symbian_os/1 > Acesso em: 01 abril 2011.

MARCELLA, A. J.; GREENFIELD, R. S. **Cyber Forensics:** A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes. New York: Auerbach, 2002.

MARCELLA, A. J.; MENENDEZ, J. D. **Cyber forensics:** A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes. 2ª ed. New York: Auerbach Publications, 2008.

MARCIANO, João L. P. **Segurança da Informação:** Uma Abordagem Social. Brasília, BR, 2006.

MARTINELLI, Juliana. **Transmissão de Dados para Aplicação de Segurança em Symbian OS**, 2009. 59 f. Monografia - Engenharia em Computação com Ênfase em Sistemas Embarcados, Escola de Engenharia de São Carlos, São Carlos, BR – SP. Disponível em: <http://www.tcc.sc.usp.br/tce/disponiveis/97/970010/tce-12042010-091246/publico/Martinelli_Juliana.pdf>. Acesso em: 10 Novembro 2010

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.
MIDDLETON, B. **Cyber crime investigator's field guide**. London: Auerbach, 2002.

MOHAY, George M. et al. **Computer and Intrusion Forensics**. Massachusetts, USA: Artech House, 2003.

MONTEIRO, Emiliano Soares. **Segurança em Ambientes Corporativos**. Florianópolis: Visual books ltda, 2003.

MOREIRA, Ademilson. **A Importância da Segurança da Informação**. 2008. Disponível em: <http://www.oficinadanet.com.br/artigo/1124/a_importancia_da_seguranca_da_informacao> Acesso em: 18 Setembro 2010.

PHILIPP, A.; COWEN, D.; DAVIS, C. **Hacking Exposed:** Computer Forensics. 2ª. ed. New York: McGraw-Hill , 2010.

PINHEIRO, P. P. **A Evolução dos Aspectos Legais do Risco Corporativo**. BR, 2007.

PLACE, Ricardo Leocádio. **Criptografia, assinatura digital e alguns outros conceitos**. Disponível em: <http://eltiger.wordpress.com/2008/10/12/ciptografia-assinatura-digital-ealguns-
outros-conceitos/> Acesso em: 11 abril. 2011.

PROSISE, Chris; MANDIA, Kevin. **Incident Response & Computer Forensics**. 2.d. Columbus, USA: McGraw-Hill/Osborne, 2003.

RAY, Daniel A.; BRADFORD, Phillip G. **Models of Models**: Digital Forensics and Domain-Specific Languages. Tennessee, USA,2007.

REITH, Marc; CARR, Clint; GUNSCH, Gregg. **An Examination of Digital Forensic Model**. International Journal of Digital Evidence, New York, USA, 2002.

REYES, A. **Cyber Crime Investigations:** Bridging the Gaps Between, Security Professionals, Law Enforcement, and Prosecutors. New York: Syngress, 2007.

REYES, A.; WILES, J. **The Best Damm Cybercrime and Digital Forensics Book Period**. Burlington: Syngress, 2007.

SCHWEITZER, D. **Incident Response:** Computer Forensics Toolkit. Indiana: Wiley Publishing, 2003.

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: 11 abril. 2011.

VACCA, J. R. **Computer Forensics**: Computer Crime Scene Investigation. Massachusetts, USA: Charles River Media, 2002.

VACCA, J. R. **Computer Forensics:** Computer Crime Scene Investigation. 2ª. ed. Boston, Massachusetts: CHARLES RIVER MEDIA, INC, 2005.

VOLONINO, L.; ANZALDUA, R. **Computer Forensics For Dummies**. Indianapolis: Wiley Publishing, 2008.

WEBBA, Sidney Roberto da Silva. **Procedimentos Computacionais no Auxílio à Perícia Forense Aplicada em Web Browsers**. 2010. 150 f. Trabalho de Conclusão de Curso

(Graduação em Ciência da Computação) - Universidade do Extremo Sul Catarinense, Criciúma.

WANG, C. L.; YAO, B.; YANG, Y.; ZHU, Z.; A **Survey of Embedded Operating System**. California: 2001.

WILKINSON, 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: 26 maio 2010.

APÊNDICE A - DOCUMENTAÇÃO DA PERICIA FORENSE REALIZADA EM 3 DE JUNHO DE 2011

Identificação do Perito

Nome: Pedro Paulo Alexandrino

Qualificações: Finalista do Curso de Ciência da Computação da UNESC

Endereço: Rua Sete de Setembro, 170 - Bairro Centro C.P. 3167 | CEP: 88801-170

Criciúma / Santa Catarina

Telefone para contato: +55 48 9914-6630

Data e Horário de Início da Pericia Forense: 02 de Junho de 2011. 18h25m

Data e Horário de Fim da Pericia Forense: 03 de Junho de 2011. 23h15m

Local da Pericia Forense: Apartamento no Edifício Solar das Esmeraldas. : Rua Sete de Setembro, 170 - Bairro Centro C.P. 3167 | CEP: 88801-170

Criciúma / Santa Catarina

Alguns dados acima não correspondem a realidade para manter a confidencialidade de informações consideradas pessoais.

A seguir segue as especificações de Hardware do aparelho celular N85:

Especificações de Hardware:

Dimensões	**Tela e Interface do Usuário**	**Memória**
Formato: slide bidirecional	Tamanho: 2,6"	Slot para cartão de memória microSD com hot-swapping, máx. 8 GB
Volume: 76 cc	Resolução: 320 x 240 pixels (QVGA)	74 MB de memória dinâmica interna
Peso: 128 g	Até 16,7 milhões de cores	
Dimensões: 103 x 50 x 16 mm	Tecnologia OLED de matriz ativa	

Especificações de Software:

Sistema Operacional do Celular	**Sistema Operacional de Trabalho**
Windows Seven	Symbian OS versão 9.3 S60 3ª edição,

Procedimentos Computacionais:

Memória Interna:

a) Com a ferramenta MobilEdit foi feito o reconhecimento do dispositivo celular via cabo USB;
b) Seleção das informações a serem recuperadas: Agenda, SMS, sistema de arquivos, alarmes e MMS. O arquivo gerado como imagem “00000005.dat” foi gravado no diretório “C\Users\Pedro\AppData\Roaming\MOBILedit\”;
c) Usando a mesma ferramenta foi importado o arquivo “00000005.dat”.
d) Dentro da aplicação foram visualizados 88 contatos cadastrados, 10 mensagens de texto recebidas, 6 mensagens de texto enviadas e 2 mensagens multimídias enviadas. Nenhuma tarefa ou agendamentos foram encontrados.

Memória Externa:

a) Foi retirnado o cartão de memória do celular;
b) Usando um adaptador, o mesmo foi conectado ao computador;
c) Dentro do terminal do Linux foi executado o comando “fdisk -l” para saber o local do dispositivo a fim de localiza-lo para realizar o backup. Foi descuberto que o local é “⁄dev⁄sdb”;
d) Foi criado um diretório para armazernar a imagem do dispositivo utilizando o comando “mkdir recuperados”;
e) A seguir foi executado o comando “dd if=/dev/sdb1 of=cartao.img” para copiar os dados fisicamente do dispositivo para o arquivo de imagem, originando um arquivo de 126 MB;
f) Usando a ferramenta PhotoRec foi possível selecionar a imagem criada para extração das informações;
g) Na opção “Partition” foi escolhido “No Partition”;

h) Na opção “FileSystem” foi escolhido “Other”;

i) No momento de salvar, foi precionado a telha “Y” do teclado, para realizar a recuperação dos dados;

j) Por fim, foram recuperados 98 arquivos. Sendo que 75 possuem extensão TXT⁄VCF, 21 JPG, 1 MP3 e 1 ZIP.

Resultados:

Foram encontradas provas periciais na memória interna do celular, entre elas estão as mensagens de texto enviadas e recebidas e mensagens multimídias enviadas.

Na memórias externa foram encontradas duas fotos que também serão utilizadas como provas.

APÊNDICE B – ARTIGO: PERÍCIA FORENSE APLICADA EM CELULARES COM SISTEMA OPERACIONAL SYMBIAN: FERRAMENTAS, ANÁLISE E ESTUDO DE CASO

Perícia Forense Aplicada em Celulares com Sistema Operacional Symbian: Ferramentas, Análises e Estudo de Caso

Pedro Paulo Alexandrino[1], Paulo João Martins[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

qlale@hotmail.com, pjm@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 apply forensic computational techniques to the search and analysis of information stored in cellphones, 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, using the combination of the technologies DFRWS, Reith, Carr and Gunsche, SOP and NIST, but using NIST as the main methodology.*

Keywords: *Security, Computer Crime, Forensics, 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 aplicar técnicas computacionais forenses para a busca e análise de informações contidas em celulares, contribuindo socialmente aumentando o 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 em um telefone móvel, utilizando a junção das metodologias DFRWS, Reith, Carr e Gunsch, SOP e NIST, porém utilizando a NIST como principal.*

Palavras-chave*: Segurança; Crimes Digitais; Perícia Forense; Celular.*

1. Introdução

Os telefones celulares estão rapidamente se tornando uma necessidade para muitas pessoas ao redor do mundo, inclusive criminosos. Muitos oficiais de justiça consideram telefones

celulares, como parte integrante do tráfico de drogas. Esta ligação tem motivado algumas famílias e escolas a proibir estes dispositivos.

Apesar de compacto, estes dispositivos podem conter elementos de prova digital significativas, incluindo horários, memorandos, livros de endereços, e-mails, senhas, números de cartões de crédito e outras informações pessoais (VACCA, 2002, tradução nossa).

O celular pode ser de extrema importância na busca de evidências de um crime, pois o meliante pode fazer algumas ligações, ou troca de mensagens, gerando evidências para resolução do caso. Porém, as informações como, últimas ligações, mensagens, fotos, podem ser apagadas, dificultando a busca de pistas que auxiliam a resolução de um caso.

De acordo com Wilkinson (2007, tradução nossa) existem algumas boas práticas para a utilização da perícia forense em celulares, que podem ser divididas em quatro princípios. O primeiro princípio proíbe que os dados contidos em um celular ou qualquer mídia de armazenamento possam ser alterados. O segundo princípio, afirma que o responsável pela perícia deve ser competente e capaz de prestar depoimento, explicando a importância e aplicações de suas ações. O terceiro princípio diz que o resultado de uma perícia feita por um especialista deve ser o mesmo, caso seja feito por outro especialista. O último princípio aborda que o gestor do caso tem responsabilidade global de garantir que os resultados levantados sejam respeitados.

Dessa forma, essa pesquisa realizou uma análise e explanação sobre métodos de busca de informações ou evidências resultando em um auxílio na localização de informações restritas em celulares.

2. Crimes Digitais

Nos últimos anos, uma nova classe de cenas de crimes tem se tornado mais prevalente nos domínios eletrônicos ou digitais, principalmente em ciberespaço. Serviços de justiça criminal em todo o mundo estão sendo confrontados com uma necessidade crescente de investigar crimes cometidos, total ou parcialmente, na Internet ou outros meios digitais.

Segundo Casey (2004, tradução nossa), Vacca (2005, tradução nossa) e Reyes (2007, tradução nossa) recursos e procedimentos são necessários para efetivamente procurar e preservar todos os tipos de provas digitais. Estas provas variam desde dados comuns, como fotos e documentos ilegais, até dados criptografados, usados para uma variedade de atividades criminosas. Mesmo nas investigações que não utilizam primariamente evidências eletrônicas, em algum momento dispositivos podem ser investigados, permitindo novas descobertas que devem ser analisadas.

Os computadores e dispositivos móveis têm inspirado novos tipos de conduta, tais como *hackers* agindo de várias formas ilegais. Uma vez que esses atos exigem alguma especialização a partir de um computador e anos de experiência, os *hackers* obtendo essa informação sentem-se glamorosos, pois consideram como heroico e não criminal. Na era eletrônica, algumas pessoas comportam-se de forma ilegal, mas cada vez com mais imaginação (MOHAY et al, 2003, tradução nossa).

Alguns crimes digitais são difíceis de serem resolvidos. Como por exemplo, no caso de pornografia infantil, quando o suspeito pode alegar que não teve a intenção de baixar um arquivo contendo fotos, no momento que estava sendo rastreado remotamente, ou até mesmo, no levantamento de evidências relacionadas a um crime (REYES, 2007, tradução nossa).

Segundo Galvão (2009) qualquer ação realizada utilizando um dispositivo digital como instrumento ou objeto do delito, é chamado de crime digital.

2.1. Evidências Digitais

A complexidade dos casos forenses realizado em computadores na obtenção de provas tem aumentado significativamente ao logo dos anos com o aumento da sofisticação dos sistemas de computador autônomo, e a uma maior utilização da Internet. A Internet fornece um quadro com crescimento em aplicações sofisticadas, que são vulneráveis ao computador, como por exemplo, o comércio eletrônico, um canal de comunicação permitindo a ocorrência crime podendo ser planejados, geridos ou facilitados (PROSISE; MANDIA, 2003, tradução nossa).

No passado a perícia forense tinha uma tendência de confiar em provas que consistiam essencialmente em discos independentes ou arquivos do disco, porém os casos mais recentes têm contado cada vez mais com provas eletrônicas colhidas a partir de uma variedade de fontes. Como por exemplo, em caso de pirataria, além de informações providas do disco rígido, podemos encontrar evidências em registros telefônicos, redes sociais, rastreando outros endereços permitindo a averiguação de outros discos ou dispositivos correlacionados. (WILKINSON, 2010, tradução nossa).

Dispositivos móveis como celulares e PDAs se tornaram essenciais nas áreas de negócio e pessoal, sendo que são extremamente suscetíveis de conter informação pessoal considerável, como evidências eletrônicas e informações sobre atividades de uma pessoa, que pode ter um valor significativo em investigação criminal. Existem algumas diferenças entre o tratamento destes dispositivos e manipulação de computadores e discos, causados pela diferença de tecnologias. Em particular, há pouca padronização entre os dispositivos deste tipo porque são mais recentes, portanto menos experiência de como lidar com eles. No entanto, como resultado de sua penetração no mercado em rápido crescimento, os dispositivos móveis como uma questão de rotina, difundida em casa, no trabalho, automóvel, armazenando informações do cotidiano, apresentam grande potencial para investigação forense computacional (SCHWEITZER, 2003, tradução nossa).

2.2. Importância da Segurança da Informação

Vive-se em um mundo onde a informação é muito importante, e independentemente do seu formato é uma grande riqueza para a organização moderna, sendo vital para qualquer tipo de classe ou instituição.

A tecnologia da informação e comunicação tem evoluído de forma muito rápida, permitindo que as organizações possam tomar decisões precisas, utilizando um sistema de informação. Contudo se torna inviável uma organização progredir sem um sistema de informação, porém é preciso um mecanismo de segurança para que o acesso à informação seja controlado (MOREIRA, 2008, tradução nossa).

De acordo com Galvão (2009) a legislação Brasileira vem sendo motivo de discussões em crimes digitais, pois grande parte da população transportou suas vidas para as redes virtuais, resultando no crescimento de fatos e ocorrências jurídicas, da mesma forma que ocorre no mundo real. Essas ocorrências estão na aplicação de normas comerciais, transações on-line, mensagens por e-mail, validação jurídica de um documento eletrônico, privacidade e a integridade do usuário.

No passando a segurança da informação era mais simples, pois as informações contidas em inúmeros papéis podiam ficar guardadas fisicamente em locais seguros. Hoje, com a chegada da tecnologia da informação e comunicação, a segurança ficou mais complexa, pois a maiorias dos computadores conectam-se a Internet e visse versa. Além disso, os dados digitais são portáteis, tornando esse delito um atrativo para os ladrões de informações (MONTEIRO, 2003).

Outros fatores que devem ser levados em consideração em relação à segurança da informação são as inúmeras situações de insegurança que podem afetar os sistemas de informação como incêndio, alagamentos, problemas elétricos, poeira, fraudes, uso inadequado

dos sistemas, guerras, sequestros e muitos outros. Dessa forma, podemos dizer que não existe segurança absoluta. É preciso agir no sentido de descobrir quais são os pontos vulneráveis e a partir daí, avaliar os riscos e as consequências, para conseguir ao máximo manter a informação segura e inalterável (MARCIANO, 2006).

Uma boa prática de prevenir problemas relacionados ao segurança da informação é a utilização de softwares de segurança e prover soluções no espaço de tempo mais curtos possível. Devendo estar atrelada a um amplo programa de segurança, com ferramentas, configurações, instalação de soluções, criações de projetos específicos e recomendações de uso, como Antivírus, Firewall, sistemas Antspam entre outros. Para tanto, não basta comprar as soluções, os produtos de segurança direcionados à prevenção são bons, mas são apenas uma parte do conceito geral. Não é o bastante ter os melhores produtos de segurança, é preciso mantê-los atualizados, instalando novas versões, aplicando pacotes de correção entre outros, para então interpretar suas informações e responder efetivamente aos alertas registrados por eles (MOREIRA, 2008).

3. Perícia Forense Computacional

Perícia forense computacional refere-se aos métodos utilizados por profissionais para, obtenção, preservação, análise e documentação de provas com o objetivo de reuni-las, para reconstruir o cenário no momento da fraude, utilizando em um processo judicial as evidências encontradas. As provas podem ser as mais diversas possíveis, como e-mails, arquivos de registros, conhecidos como logs, arquivos temporários com informações pessoais, conexões abertas, processos em execução, entre outras evidências que possam existir na máquina, mas para serem aceitas num processo jurídico, devem ter sido obtidas de forma lícita (MARCELLA; GREENFIELD, 2002; JOHNSON, 2005, tradução nossa).

Segundo Vacca (2002, tradução nossa), Volonino e Anzaldua (2008, tradução nossa) de forma resumida, perícia forense computacional, pode ser entendida como coleta, preservação, análise e apresentação de evidências. Consiste no uso de métodos científicos e ferramentas para desenvolver a pesquisa de forma correta. Resultando conclusões sobre o incidente investigado, apresentando os fatos e as evidências.

De acordo com Krause e Heiser (2002, tradução nossa) a análise pericial é o processo usado pelo investigador para encontrar informações valiosas, e localização e extração de dados proeminentes em uma investigação. A análise pericial pode ser dividida em duas partes: análise física e análise lógica.

Durante a análise física, todos os dados da mídia de armazenamento são investigados, mesmo os que estão apagados. É preciso começar a investigação por essa parte, quando se está investigando o conteúdo de um disco rígido danificado ou que não se tenha conhecimento da origem. Depois que o software criador da imagem extrair a mesma, os dados podem ser verificados por três processos principais: uma pesquisa sequencial, processo de localização e extração e uma amostra de espaço livre de arquivos. Todas as operações são realizadas na imagem criada do dispositivo ou na cópia das provas restaurada.

Na análise lógica, o conteúdo de cada partição é pesquisado com um sistema operacional que consiga entender o sistema de arquivos. É neste momento que ocorre a maioria dos problemas de manipulação das provas. O investigador deve estar ciente de todas as medidas que serão realizadas na imagem restaurada, tendo com objetivo básico, proteger as provas contra qualquer tipo de alteração.

Na visão de Marcella e Menendez (2008, tradução nossa) a perícia forense computacional pode ser dividida em quatro partes: identificação, preservação, análise e preservação.

3.1. Celulares

Os celulares são dispositivos digitais, onde a comunicação é feita por ondas eletromagnéticas, que permite transmissão bidirecional de dados e voz (CERQUEIRA FILHO; PINTO, 2004).

O conceito de celular pode ser definido como um transmissor de baixa potência, onde a frequência pode ser reutilizada dentro de uma área geográfica determinada. Um telefone celular é um dispositivo sem fio que conecta a uma rede telefônica pública comutada e é oferecido ao público em geral, por um comum transportador ou utilidade pública.

O serviço celular funciona a partir da divisão de uma região geográfica em pequenas áreas denominadas de células. Sendo que cada uma utiliza um conjunto de sinais de rádio frequência e um conjunto de rádio transmissões e receptores de baixa potência (CERQUEIRA FILHO; PINTO, 2004).

3.2. Sistemas Operacionais para Celulares

Segundo Wang, Yao, Yang, e ZHU (2001, tradução nossa) os sistemas operacionais de celulares, são sistemas microprocessados no qual o computador é completamente dedicado ao dispositivo ou sistema que o mesmo controla. Diferente de um computador normal, utilizados para diversos fins, um sistema operacional para celular, desempenha um conjuntos de serviços predefinidos, normalmente com requisitos particulares. Desta forma, já que o sistema é dedicado a serviços específicos, com a engenharia pode-se aprimorar o projeto reduzindo tamanho, recursos computacionais e custo do produto.

No mercado para dispositivos, existe uma grande pressão para que os mesmos tenham um crescente aumento de novas funcionalidades devido à convergência digital. Eles necessitam cada vez mais ter diferentes funcionalidades, fazendo com que exista um aumento na complexidade dos sistemas embarcados, pois os celulares permanecem com a premissa de que têm uma funcionalidade peculiar, por exemplo, em um *smartphone* jogar vídeo game ou executar músicas em formato MP3, é possível, mesmo assim o fator da sua existência é permitir comunicação e essa funcionalidade nunca deve fracassar (WANG; YAO; YANG; ZHU 2001, tradução nossa).

Existem muitos Sistemas Operacionais (SO) para dispositivos móveis no mercado, como o SymbianOS, Windows Mobile da Microsoft, Android, entre outros.

A seguir serão demonstradas as características principais do Symbian OS.

3.3. SymbianOS

De acordo com Harrison (2007, tradução nossa) SymbianOS é um sistema cooperativo criado para ser utilizado por dispositivos móveis com suporte a câmeras fotográficas, wireless, *Bluetooth*, entre outras funções. Possui um ambiente gráfico bastante simples, e atualmente é utilizado na maioria dos recentes modelos de celulares dos grandes fabricantes.

Uma das grandes preocupações do SymbianOS é de evitar ao máximo o desperdício dos recursos do celular, como por exemplo, bateria e memória. Portanto ele conta com diversos mecanismos que são eficientes ao tratar com esses problemas.

Existem algumas vantagens em utilizar o SymbianOS, como por exemplo: é um sistema operativo mais estável e seguro, em relação aos seus concorrentes; utiliza muito bem todas as áreas do aparelho, como memória, processador, entre outras; permite instalação de softwares de terceiros; possui recursos para gerenciar e utilizar pouca bateria e memória; é baseado em padrões de comunicação de dados; é um sistema de baixo custo.

O que torna o SymbianOS um sistema operacional tão versátil, é o fato de que permite o desenvolvimento de aplicativos em diversas linguagens como Symbian C/C++, JavaME, FlashLite, Perl, Python, Ruby, Lua, Acelerômeter e QT.

Segundo Martinelli (2009) Symbian é uma sistema operacional que tem como alvo o mercado de *smartphones*. Para tanto, contém muitos recursos relacionados a

gerenciamento de memória e execução de multitarefas, permitindo operações eficientes e seguras dos recursos limitados que caracterizam os dispositivos móveis.

3.4. Perícia Forense em Celulares

Perícia forense e análise forense computacional estão se tornando atividades com grande importância na sociedade, devido a onipresença de dispositivos digitais e das redes de computadores e comunicações, onde os mesmo são utilizados em operações pessoais ou de trabalho.

Por meio dos dispositivos móveis e microcomputadores, temos acessos a servidores web, servidores de e-mail, entre outros servidores, que quer saibamos ou não, temos acesso a um conjuntos de computadores que estão escondidos no coração dos sistemas integrados que usamos em casa, no trabalho e no lazer.

Enquanto muitas das novas formas de comportamento ilegal ou antissocial crescem de forma contínua, a análise forense pode proporcionar oportunidades muito maiores de localização de provas eletrônicas, pois quanto maior a quantidade de evidências for encontrada, melhor será a precisão na resolução de um caso (MOHAY et al, 2003, tradução nossa).

Os pré-requisitos para uma investigação de tais dispositivos móveis, como qualquer análise forense, é um levantamento de circunstâncias que permitam a apreensão e pesquisa do dispositivo, e que tenha uma autorização judicial. É fundamental ao investigador que exista uma restrição de acesso a outras pessoas para preservação, ou seja, para garantir a manutenção de todas as provas em potencial, assim garantindo que a alimentação do aparelho não seja interrompida, evitando perda de qualquer informação no armazenamento volátil.

3.5. Aspectos a Serem Analisados em Celulares

A comunidade digital forense enfrenta um desafio constante para ficar a par das mais recentes mudanças tecnológicas que podem ser utilizadas para expor pistas relevantes em uma investigação (JANSEN; AYERS, 2007, tradução nossa).

Segundo Mohay (2003, tradução nossa) o estudo forense em um celular pode ser entendido como uma ciência de recuperar provas digitais a partir de um telefone celular, em condições predefinidas usando métodos aceitos.

Quando um celular é encontrado durante uma investigação, surgem novas questões: O que deve ser feito sobre a manutenção do celular em posse? Como deve ser tratado o dispositivo? A chave para responder a essas perguntas é a compreensão das características de hardware e software de um telefone celular.

3.6. Ferramentas Forenses

A situação com ferramentas de software forense para telefones celulares é consideravelmente diferente dos computadores pessoais. Embora os computadores pessoais sejam concebidos como sistemas de propósito gerais, os celulares são concebidos mais como aparelhos que executam um conjunto de tarefas predefinidas.

Os fabricantes de telefone celular também tendem a confiar em diversos sistemas operacionais proprietários em vez da abordagem mais normalizada encontrados em computadores pessoais. Devido a isso, a variedade de kits de ferramentas para aparelhos móveis é muito variada e vasta gama de dispositivos sobre os quais eles operam normalmente é reduzido para plataformas distintas, para uma linha de produto do fabricante, uma família de sistema operacional, ou um tipo de arquitetura de hardware. Os ciclos de lançamento do produto curto são a norma para telefones celulares, obrigando os fabricantes de ferramentas atualizarem suas ferramentas continuamente para manter a cobertura atual.

De acordo com Jansen e Ayers (2007, tradução nossa), ferramentas forenses podem adquirir dados de um dispositivo de duas formas: Aquisição física ou aquisição lógica. Aquisição física implica um *bit-by-bit*, que é a cópia de toda parte física, por exemplo, um chip de memória, enquanto a aquisição lógica implica um *bit-by-bit* cópia de objetos de armazenamento lógico, como por exemplo, diretórios e arquivos, que residem em uma unidade lógica, por exemplo, uma partição de sistema de arquivos. A diferença reside na distinção entre a memória de como pode ser visto através de um processo com as facilidades do sistema operacional, ou seja, uma visão lógica, já a visão física, a memória pode ser vista na sua forma bruta pelo processador e outros componentes de hardware relacionados.

A aquisição de Física tem vantagens sob a aquisição lógica, pois permite que arquivos apagados e todo o resto possam ser encontrados, como por exemplo, na memória ou espaço não alocado do sistema de arquivos, a ser examinado, que caso contrário iria desaparecer. A imagem dos dispositivos deve ser extraída, interpretadas, decodificadas e traduzidas para descobrir os dados presentes. O trabalho é tedioso e demorado para executar manualmente. As Imagens do dispositivo físico podem ser importadas em uma ferramenta para automatizar a análise e elaboração de relatórios, no entanto, apenas alguns instrumentos adequados para a obtenção de imagens de celular estão disponíveis no momento. A aquisição lógica, embora mais limitado do que uma aquisição física, tem a vantagem de que as estruturas de dados do sistema são normalmente mais fácil para uma ferramenta extrair e fornecer uma organização mais natural de entender e usar durante a análise. Se possível, fazer os dois tipos de aquisição é preferível, a aquisição física antes de uma aquisição lógica.

3.7. Metodologias Forenses

Com o intuito de dar credibilidade à perícia forense computacional em frente à jurados, algumas metodologias foram criadas para serem usadas como guias do processo investigativo, definindo passos a serem seguidos pelos peritos, independentemente do sistema computacional ou de ferramentas e softwares utilizados (BERNARDO, 2006).

Contudo, os procedimentos a serem realizado pelo perito forense podem ser diferentes de acordo com os sistemas e aparatos tecnológicos envolvidos. A falta de métodos específicos de acordo com a tecnologia usada enfraquecia a credibilidade das provas mediantes os casos judiciais.

Basicamente, as metodologias além de permitir o compartilhamento de ações e experiências sobre investigações comuns, elas podem ser usadas para o desenvolvimento de aplicações de novas metodologias adequadas a determinados inquéritos, através de questões sobre técnicas e procedimento a serem utilizados e fornecimento de suporte a prática da perícia.

3.7.1. Metodologia DFRWS

Proposta em 2001, utilizando passos para análise forense digital como processo linear. Foi elaborada por Gary Palmer no primeiro Digital Forensics Research Workshop (DFRWS).

3.7.2. Metodologia de Reith, Carr e Gunsh

A metodologia proposta por Reith, Carr e Gunsch (2002) também conhecida como Abstract Digital Forensics Model, possui alguns tópicos presentes também na metodologia da DFRWS, o que o torna semelhante em seus princípios. As etapas que mostram essa semelhança são a de preservação, coleta, exame e apresentação. Como particularidade, o modelo apresenta a capacidade de fornecer suporte à preparação de ferramentas e uma dinâmica formulação de abordagens investigativas.

3.7.3. Metodologia SOP

Originada pelo Scientific Working Group on Digital Evidence (SWGDE), que é o representante norte-americano na International Organization on Computer Evidence (IOCE).

A metodologia Standard Operating Procedures (SOP), foi apresentada durante uma conferência na International Hi-Tech Crime and Forensics Conference (IHCFC), que foi realizada em Londres, no período de 4 à 7 de outubro de 1999 (BERTOGLIO, 2008). Essa metodologia incorpora os procedimentos e conceitos da ciência forense, incluindo a comparação, classificação, individualização e avaliação da fonte de evidências.

3.7.4. Metodologia National Institute of Standards and Technology (NIST)

Essa metodologia criada por Wayne Jansen e Rick Ayers, também conhecida como orientações de como realizar perícia forense em celulares, realizado pela National Institute of Standards and Technology (NIST), tem como princípios recuperar provas digitais a partir de um telefone celular em condições forenses, utilizando métodos aceitos.

3.7.5. Comparação de Metodologias Forenses

Podemos visualizar na Figura 1 que as quatro metodologias mencionadas nesse projeto possuem alguns passos em comuns, na investigação de casos forenses. Sendo eles a identificação das evidências, coleta e preservação, aquisição, exame e análise e apresentação ou documentação.

Passos das Metodologias	DFRWS	Reith, Carr e Gunsch.	SOP	NIST
Autorização	-	-	X	X
Identificação	X	X	X	X
Preparação	-	X	-	X
Estratégia de abordagem	-	X	X	X
Coleta e Preservação	X	X	X	X
Aquisição	X	X	X	X
Exame e Análise	X	X	X	X
Apresentação ou Documentação	X	X	X	X
Decisão	X	-	-	-
Devolução das evidências	-	X	-	-
Reconstrução da cena do crime	-	-	X	-

Figura 1. Comparação de Metodologias Forenses

Dessa forma, é possível concluir que ambas seguem a mesma linha de processos. Algumas com peculiaridades e características próprias para incrementar a investigação e ter uma maior aceitação perante um tribunal.

4. Estudo de Caso

Para a realização da perícia forense e aplicação da junção das metodologias DFRWS, Reith, Carr e Gunsch, SOP e NIST em celulares com SO Symbian foi escolhido o aparelho Nokia N85 que possui versão do OS 9.3 da série S60 3ª edição.

Agora, para melhor contextualizar o estudo de caso fictício, e permitir uma compreensão facilitada das etapas realizadas, foi suposto que o seguinte crime digital foi cometido:

- Um homem com nome fictício José Alfredo é suspeito de estar traficando drogas, usando um celular Nokia N85 para manter contato com seus clientes, podendo ter enviado e recebido mensagens (SMS), fotos, ligações entre outras informações. Para tanto, deverá ser feito uma busca nas informações contidas no dispositivo a fim de encontrar provas que possam ajudar na resolução do caso. Para criação desse caso, foi contado com a colaboração de uma terceira pessoa, que realizou tarefas desconhecidas no celular, a fim de gerar provas relacionadas a um fictício comércio de drogas. O Celular Nokia N85, ficou em posse do colaborador no período de 22 de maio de 2011 à 02 de junho de 2011. A simulação da apreensão do mesmo foi datada para 02 de junho de 2011, momento em que recuperei o dispositivo.

A seguir, são expostos os conceitos relevantes a todos os processos das metodologias científica aplicadas neste trabalho.

4.1. Metodologia

A pesquisa tem como embasamento um estudo de caso fictício, que simula a ocorrência de uma perícia forense em um dispositivo celular, objetivando buscar conhecimento detalhado sobre os procedimentos de interesse para este estudo, considerando a ocorrência de um crime digital.

De acordo com Martins e Theóphilo (2009) um estudo de caso trata-se de uma investigação empírica que tem como objetivo pesquisar fenômenos dentro de seu contexto real. De uma forma onde o pesquisador não tem controle sobre eventos e variáveis, mas buscando aprender a totalidade de uma situação e criativamente descrever, compreender e interpretar a complexidade de um caso concreto.

O fato de que cada caso tem suas características próprias, faz com que não exista um modelo traçado de forma específica para elaboração de um estudo de caso, mas existe uma sequência de práticas metodológicas para orientação, que são: coleta de evidências, composição e validação dos resultados, conclusões, verificação de possíveis interferências e relatório final (MARTINS; THEÓPHILO, 2009).

Portanto, para que se cumpram os objetivos desta pesquisa, definiu-se que as metodologias DFRWS, Reith, Carr e Gunsch, SOP e NIST serão utilizadas durante a realização do estudo, pois a junção das mesmas incorpora algumas das práticas metodológicas recomendadas acima, tanto quanto os princípios e técnicas da ciência forense.

A seguir a figura 3 ilustra cada uma das etapas com algumas ações a serem tomadas no decorrer da perícia. Essas ações atuam como processos em um projeto, pois respeitam uma ordem, mesmo que a investigação retorne a uma etapa anterior.

Autorização
- Autorização judicial ou consentimento do proprietário do celular.

Identificação
- Adquirir todas as informações subjetivas possíveis em relação à investigação.

Preparação
- Definir o que se deve provar.

Estratégia de abordagem
- Não infectar o dispositivo.

Coleta e Preservação
- Identificar fontes de provas.
- Coleta de provas.
- Documentação da cena e provas encontradas.
- Armazenamento das provas.

Aquisição na Memória Interna do Celular
• Identificação do dispositivo. • Seleção de ferramentas. • Aquisição na memória do celular.
Exame e Análise na Memória Interna do Celular
• Analisar provas coletadas. - Contatos. - Mensagens de texto e multimídias. - Agendamentos e Tarefas.
Aquisição na Memória Externa do Celular
• Seleção de ferramentas. • Aquisição em cartão de memória.
Exame e Análise na Memória Externa do Celular
• Analisar provas coletadas. - Fotos. - Arquivos de texto entre outros encontrados.
Apresentação ou Documentação
• Identificar perito. • Registrar hora e data do início e fim da investigação.
Decisão
• Determinar conclusões do caso.
Devolução das provas
• Devolução do dispositivo e outros materiais encontrados durante a preservação e coleta.
Reconstrução da Cena do Crime
• Deve responder perguntas como: o que aconteceu? Quem executou? Quando aconteceu? Onde aconteceu? Como aconteceu? E Por quê?

Figura 3. Tabela de Etapas do Processo Forense

A explicação detalhada de como cada etapa foi aplicada, é apresentada a seguir.

4.2. Etapa 1 - Autorização

Pelo fato de o presente estudo de caso ser fictício, não se fez necessária a busca por uma autorização judicial ou consentimento do suspeito, para que a perícia forense fosse realizada.

Foi definido o escopo da pesquisa, determinando o que se deseja provar. Para tal, estabeleceu-se que se pretende descobrir ao final da mesma se o portador do celular utilizou o mesmo para realizar algum tipo de crime digital, buscando a forma que realizou o contato, a data e hora e com quem manteve esse contato. Esta etapa é baseada na metodologia NIST.

4.3. Etapa 2 - Identificação

Novamente por se tratar de um estudo de caso hipotético, não foi necessário o levantamento junto às pessoas envolvidas no crime (pessoas que identificaram a ocorrência do crime) que permitiriam ao perito contextualizar melhor os fatos que surgissem durante o decorrer da investigação. Esta etapa, também é baseada na metodologia NIST.

4.4. Etapa 3 - Preparação

No momento da preparação é preciso definir o que se deve provar. Esse passo é importante, pois ajuda a focar na busca de provas e conciliações das informações encontradas.

Tratando-se de um caso hipotético onde uma pessoa é suspeita de estar realizando tráfico de drogas, foi decidido que informações relacionadas a drogas, pagamentos, cobranças

e entregas, deverão ser localizadas com maior enfoque, com o intuito de chegar a uma conclusão sem precisar analisar todos os dados encontrados no dispositivo. É uma etapa da metodologia NIST.

4.5. Etapa 4 - Estratégia de Abordagem

Nessa etapa, referente à metodologia NIST, é preciso garantir que nenhuma informação do dispositivo será alterada. Para isso, toda forma de acesso utilizando hardwares ou softwares deverá garantir que nenhum dado será inserido, alterado ou excluído do dispositivo.

Todas as ferramentas utilizadas nesse processo forense garantem que essa etapa será validada garantindo a integridade e confiabilidade das provas. Pois acessam o dispositivo com a restrição de somente leitura.

4.6. Etapa 5 - Coleta e Preservação

Para simular o caso, utilizando a metodologia NIST, o celular foi deixado sob a cama do suspeito portador do dispositivo, junto a um cabo de alimentação de energia e outro cabo USB para transferência de dados, conforme podemos visualizar na figura 6.

Durante a coleta foi preciso isolar o celular da rede de rádio para manter os registros que foram apagados. Pois novas informações podem substituir os dados existentes e novos dados recebidos após a apreensão podem estar fora do escopo da autoridade concedida originalmente. Para isolar foi preciso entrar no menu do celular e escolher uma opção de conexão *off-line*.

Uma parte muito importante na preservação é garantir a segurança do dispositivo e suas informações. Para isso o mesmo foi colocado em um saco especial e marcado com a assinatura e data do acontecimento, para poder iniciar uma cadeia de custódia. Nesse processo foi preciso uma atenção especial para evitar que as teclas sejam pressionadas acidentalmente.

Após o transporte do dispositivo o mesmo foi armazenado em um ambiente fresco e seco em um local seguro com acesso controlado.

4.7. Etapa 6 - Aquisição na Memória Interna do Celular

Para iniciar a aquisição é preciso identificar o dispositivo. Para tanto, foi possível visualizar na parte frontal do celular, que a marca é Nokia e o modelo, N85. Após obter essas informações, foi realizada uma pesquisa no site do fabricante, com o intuito de descobrir o sistema operacional para poder selecionar algumas ferramentas que deverão ser utilizadas na aquisição.

Durante a pesquisa sobre o dispositivo, foi verificado que o mesmo possui um Sistema operacional SymbianOS versão 9.3 S60 3ª edição. E em relação à memória de armazenamento, possui um cartão externo de 128 MB, e interna *flash* de 78 MB.

A aquisição em um celular pode ser entendida como uma extração de todos os dados acessíveis gravados no dispositivo, resultando em um arquivo de imagem com formato especificado pela ferramenta utilizada. Em um celular existem três locais onde podem existir informações: memória interna, externa e SIM. Para esse trabalho, apenas as memórias interna e externa serão analisadas.

Após a ferramenta MobilEdit! instalada foi executada a aplicação e feito o reconhecimento do dispositivo via cabo USB. Então foi possível realizar o backup da agenda, SMS, sistema de arquivos, alarmes e MMS.

Com o backup realizado, o próprio programa exibe o local onde se localiza o arquivo de backup, a fim de permitir ao usuário realizar a análise. O arquivo gerado foi nomeado “00000005.dat” com tamanho de 15.350 KB. Nesse momento, foi possível perceber, que essa ferramenta apenas teve acesso às informações lógicas da memória, pois o tamanho total da memória física é 78 MB e apenas 15 MB foram adquiridos.

4.8. – Etapa 7 - Exame e Análise na Memória Interna do Celular

Existem muitas ferramentas que realizam a análise em um arquivo de backup com informações em hexadecimal. Algumas ferramentas mostram as informações contidas de forma visual separando conforme a estrutura lógica do celular, como a própria ferramenta MobilEdit!. Outra ferramenta utilizada nesse trabalho para exame e análise, é a Forensic Toolkit. Essa ferramenta é muito utilizada pelas comunidades forenses, pois possibilita uma análise muito detalhada em um arquivo imagem de backup.

Com a ferramenta MobilEdit em execução foi possível importar o backup gerado pela própria ferramenta. De forma visual, a mesma mostra todas as informações lógicas do celular. Informações como data e hora do cadastro, não são fornecidos pela ferramenta. Foi possível visualizar os contatos cadastrados, mensagens de texto recebidas e enviadas separadamente ordenadas por data e hora da mais atual para mais antiga, e mensagens multimídias enviadas.

Com a ferramenta Forensic Toolkit foi possível ler imagem gerada pelo MobilEdit e fazer busca em todo o backup com palavras chaves. A duas ferramentas citadas obtiveram o mesmo resultado, porém a MobilEdit para esse caso é de mais fácil utilização.

4.9. Etapa 6 - Aquisição na Memória Externa do Celular

Em relação à memória externa do celular, para esse caso, um cartão micro SD, existe muitas ferramentas *free* e pagas que conseguem recuperar informações de cartão de memória, tanto para Windows quanto Linux Porém, para utiliza-las dentro da metodologia forense, é preciso inicialmente fazer uma cópia das informações originais, criando um arquivo imagem.

Para realizar uma aquisição na memória externa é preciso retirar o cartão de memória do dispositivo. No caso do Celular N85, foi preciso retirar o cartão e conecta-lo em um leitor.

Após conecta-lo no leitor foi aberto o terminal dentro do Linux. Na sequência executado o comando “fdisk -l” para saber o endereço do cartão de memória.

No terminal do OS, foi possível visualizar um disco de 640.1 GB, que é o principal do computador e um outro disco, no caso, cartão de memória de 125 MB que é o dispositivo que sofrerá uma cópia. O local de acesso ao cartão de memória foi “⁄dev⁄sdb”.

O próximo passo foi criar um diretório para gravar a imagem do cartão do celular. Para criar o diretório “recuperados” foi utilizado o comando “mkdir recuperados”.

Para criar a imagem do cartão foi preciso executar o comando “dd if=/dev/sdb1 of=cartao.img”, onde o “if” é o dispositivo a ser recuperado e o “of” é o local onde deseja salvar a imagem.

Nesse momento foi criado o arquivo “cartao.img” com tamanho de 126 MB no diretório “recuperados”. O tempo de processo foi 15,06 segundos.

A seguir serão mostrados os passos para realizar a análise na imagem criada do cartão de memória.

4.10 Etapa 7 - Exame e Análise na Memória Externa do Celular

Com a ferramenta PhotoRec foi possível realizar a análise da imagem criada. Essa ferramenta tem a função de extrair todas as informações da imagem, até mesmo os arquivos que foram excluídos.

Para iniciar a análise, foi preciso executar o comando “PhotoRec cartao.img”, selecionar a opção “No partition”, o sistema de arquivos “Other”, a opção “-rw-r--r--” e pressionado a tecla “Y” para confirmar.

Por fim, foram recuperados 98 arquivos. Sendo que 75 possuiem extensão TXT⁄VCF, 21 JPG, 1 MP3 e 1 ZIP.

Analizando esses arquivos, foi percebido que existem alguns com extenção .vcf, que são os contatos cadastrados. Todos esses arquivos não estavam disponíveis no cartão de memória, porém o PhotoRec conseguiu recuperar conforme imagem 29.

Dentre os arquivos com extenção .jpg, estão muitas fotos pessoais, porém outras fotos suspeitas foram localizadas.

Outros arquivos encontrados na memória, como, música e arquivos de texto, foram encontrados a avaliados, porém nenhuma informação importante foi encontrada, portando não têm relevância para o caso.

4.11. Etapa 8 - Apresentação ou Documentação

Esta etapa da metodologia NIST foi trabalhada durante todo o processo pericial. É crucial para que se possa redigir um laudo pericial fiel aos fatos. A documentação completa pode ser visualizada no apêndice A do presente trabalho.

4.12. Etapa 9 - Decisão

Nessa etapa é preciso chegar a uma conclusão para o caso analisado. Devido às evidências fictícia encontradas nas mensagens de texto e multimídia, enviadas e recebidas, contendo informações ligadas a um tráfico de drogas, foi concluído que o portador do celular, José Alfredo realmente realizou um crime digital.

4.13. Etapa 10 - Devolução das Provas

Por ser um caso fictício, não se faz necessário realizar a devolução das provas encontradas. Caso contrário, o celular juntos com os demais periféricos, deveriam ser devolvidos ao proprietário. Essa etapa é baseada na metodologia de Reithm Carr e Gunsch.

4.14. Etapa 11 - Reconstrução da Cena do Crime

Nessa etapa, baseada na metodologia SOP, é preciso fazer a reconstrução dos eventos corridos relacionados ao crime digital. Juntando todas as evidências para determinar o que realmente aconteceu.

Portanto, devido às evidências encontradas, hipoteticamente o portador do celular utilizou o mesmo para envio de mensagem, realizando uma suposta venda de drogas e recebeu algumas mensagens correspondendo às mensagens enviadas. Também utilizou o celular para capiturar fotos do seu produto. Algumas dessas fotos foram enviadas para supostos usuários do mesmo. Tudo isso aconteceu no período de 22 de maio de 2011 à 02 de junho de 2011.

Conclusão

Devido ao aumento crescente de usuários utilizando celulares inteligentes, os crimes digitais estão se tornando um problema cada vez maior. A perícia forense computacional surge, como uma grande aliada na batalha contra a impunidade existente atualmente, contribuindo para que a sociedade seja mais justa e segura.

A perícia forense, utiliza meios científicos na identificação e ação contra crimes digitais. Com o passar do tempo, os resultados periciais estão tomando gradativamente um espaço nos processos judiciais, fazendo com que aumente a necessidade de otimizar o proceso de coleta, preservação, aquisição e análise de provas.

É extremamente importante que a metodologia utilizada em uma investigação seja aceita pelos órgãos judiciais, e que os procedimentos sejam feitos da maneira correta. Pois um erro durante a realização pode culpar um inocente, vice versa, ou até mesmo invalidar a investigação.

Perícia forense em celular é um assunto muito recente no País. É conhecido como complexo, pois diferentemente dos microcomputadores pessoais, os celulares possuem

arquiteturas e softwares diferentes. Fazendo com que os procedimentos realizados com sucesso em um dispositivo, não ter o mesmo resultado em outro. Por esse fato, esse trabalho tem como objetivo aplicar técnicas computacionais forenses para a busca e análise de informações contidas em celulares com SymbianOS.

Contudo foi percebido que existem poucas ferramentas disponíveis sem custo para realizar aquisições das informações. Muitas delas na versão free são restritas, porém prometem absoluto sucesso caso seja adquirida a licença.

Entre outras, existem os Kits, agregando Hardware ao Software, abrangendo quase todos os modelos de celulares, com conectores para diferentes fabricantes, tornando o processo menos complexo, adquirindo os dados com maior facilidade. Esses Kits possuem um custo bastante elevado, mas é altamente recomendado para peritos que desejam trabalhar com a ciência forense em dispositivos celulares.

Referências

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.

CASEY, Eoghan. **Crime Investigation:** Forensic Tools and Technology. 2ª. ed. Londres, UK: Academic Press, 2003.

CASEY, Eoghan. **Digital Evidence and Computer Crime:** Forensic Science, Computers, and the Internet. 2d. Londres, UK: Academic Press, 2004.

CERQUEIRA FILHO, A. L. P; PINTO, M. B. C. **A Telefonia Celular**, Salvador: CienteFico, BR-BA, 2004. 9 f. Disponível em: <http://www.frb.br/ciente/Impressa /Info/I.6.Filho, ALPC.TELEFONIACELULAR.pdf> . Acesso em: 10 de Novembro de 2010.

GALVÃO, M. L. **Tratamento de Evidências Digitais na Segurança de Informações**. 2009. 49 f. Trabalho de Conclusão de Curso (Graduação Tecnologia em Análise e Desenvolvimento de Sistemas) – Faculdade de Ciências Sociais, Cascavel.

HARRISON, R. SHACKMAN. **Symbian OC C++**for mobile phones. England: WILEY, 2007.

JANSEN, Wayne; AYERS, Rick. **Guidelines on Cell Phone Forensics:** Recommendations of the National Institute of Standards and Technology. USA, 2007.

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

KRAUSE, W. G.; HEISER, J. G. **Computer Forensics:** Incident Response Essentials. Boston: Addison, 2002.

MARCELLA, A. J.; GREENFIELD, R. S. **Cyber Forensics:** A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes. New York: Auerbach, 2002.

MARCELLA, A. J.; MENENDEZ, J. D. **Cyber forensics:** A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes. 2ª ed. New York: Auerbach Publications, 2008.

MARCIANO, João L. P. **Segurança da Informação:** Uma Abordagem Social. Brasília, BR, 2006.

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

MOHAY, George M. et al. **Computer and Intrusion Forensics**. Massachusetts, USA: Artech House, 2003.

MONTEIRO, Emiliano Soares. **Segurança em Ambientes Corporativos**. Florianópolis: Visual books ltda, 2003.

MOREIRA, Ademilson. **A Importância da Segurança da Informação**. 2008. Disponível em: <http://www.oficinadanet.com.br/artigo/1124/a_importancia_da_seguranca_da_ informacao> Acesso em: 18 Setembro 2010.

ALEXANDRINO, Pedro Paulo. **Perícia Forense Aplicada em Celulares com Sistemas Operacional Symbian: Ferramentas, Análises e Estudo de Caso**. 2011. 170 f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) - Universidade do Extremo Sul Catarinense, Criciúma.

PROSISE, Chris; MANDIA, Kevin. **Incident Response & Computer Forensics**. 2.d. Columbus, USA: McGraw-Hill/Osborne, 2003.
REITH, Marc; CARR, Clint; GUNSCH, Gregg. **An Examination of Digital Forensic Model**. International Journal of Digital Evidence, New York, USA, 2002.

SCHWEITZER, D. **Incident Response:** Computer Forensics Toolkit. Indiana: Wiley Publishing, 2003.
VACCA, J. R. **Computer Forensics**: Computer Crime Scene Investigation. Massachusetts, USA: Charles River Media, 2002.

VACCA, J. R. **Computer Forensics:** Computer Crime Scene Investigation. 2ª. ed. Boston, Massachusetts: CHARLES RIVER MEDIA, INC, 2005.

VOLONINO, L.; ANZALDUA, R. **Computer Forensics For Dummies**. Indianapolis: Wiley Publishing, 2008.

WANG, C. L.; YAO, B.; YANG, Y.; ZHU, Z.; A **Survey of Embedded Operating System**. California: 2001.

WILKINSON, 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: 26 maio 2010.

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.