UNIVERSIDADE DO EXTREMO SUL CATARINENSE - UNESC

CURSO CIÊNCIA DA COMPUTAÇÃO

ANDERSON DO ROSÁRIO FRANCISCO DA SILVA

METODOLOGIAS E FERRAMENTAS DE PERÍCIA FORENSE UTILIZADAS EM SISTEMAS DE ARQUIVOS NEW TECHNOLOGIES FILE SYSTEM (NTFS): ARQUIVOS EXCLUÍDOS, OCULTOS E SEGMENTADOS.

CRICIÚMA

2013

ANDERSON DO ROSÁRIO FRANCISCO DA SILVA

METODOLOGIAS E FERRAMENTAS DE PERÍCIA FORENSE UTILIZADAS EM SISTEMAS DE ARQUIVOS NEW TECHNOLOGIES FILE SYSTEM (NTFS): ARQUIVOS EXCLUÍDOS, OCULTOS E SEGMENTADOS.

Trabalho de Conclusão de Curso, apresentado para obtenção do grau de Bacharel no curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC.

Orientador: Prof. MSc. Paulo João Martins

CRICIÚMA

2013

ANDERSON DO ROSÁRIO FRANCISCO DA SILVA

METODOLOGIAS E FERRAMENTAS DE PERÍCIA FORENSE UTILIZADAS EM SISTEMAS DE ARQUIVOS NEW TECHNOLOGIES FILE SYSTEM (NTFS): ARQUIVOS EXCLUÍDOS, OCULTOS E SEGMENTADOS

Trabalho de Conclusão de Curso aprovado pela Banca Examinadora para obtenção do Grau de Bacharel, no Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC, com Linha de Pesquisa em Perícia Forense Computacional.

Criciúma, 24 de Junho de 2013.

BANCA EXAMINADORA

Prof. MSc. Paulo João Martins - (Unesc) - Orientador

Prof. MSc. Rogério Antonio Casagrande - (Unesc)

Prof. Esp. Sérgio Coral - (Unesc)

Dedico este trabalho aos meus pais, por terem sido o combustível do meu motor e que sempre me incentivaram a estudar e realizar os meus sonhos.

AGRADECIMENTOS

À SONANGOL (Sociadade Nacional de Petróleos de Angola) pela oportunidade concedida. À UNESC (Universidade do Extremo Sul Catarinense) pelo suporte indispensável, a todos os funcionários e professores pelo carinho, apoio, em especial a professora Ana Claudia, Merisandra, Priscila, Margareth, ao meu orientador e professor Paulo João Martins pelo apoio e ideias durante a pesquisa.

À Sianorego pelo apoio prestado ao tratar de assuntos acadêmicos, agradecimentos especiais às senhoras Paula Donda, Marcela Alves e ao senhor Fabrício Rego.

Aos meus pais, João Carlos da Silva e Maria do Rosário Bernardo Franciso, um especial agradecimento pelo carinho, amor, conselhos, atenção e suporte mostrados no decorrer desta jornada, são eles os responsáveis pela pessoa que sou hoje. As minhas queridissimas colegas (amigas) Silvia Campos e Maria Isabel pela companhia e otimos momentos proporcionados durante a formação, aos meus irmãos de outra mãe Juary e Janilson o meu muito obrigado por esses quatro anos e meio, me suportando e aturando (risos). Aos meus amigos: Vunda Xavier, Aguinaldo Crispin, Diamantino Domingos, Cucho Caracol, Keven Rodolfo pela força e companheirismo. Agradecer também a todos os Angolanos criciumenses pelo carinho fraternal.

Por fim, e nao menos importatnte quero agradecer a Deus por me ter dado muitas bençãos.

“O fracasso é a oportunidade de começar de novo, com mais inteligência e redobrada vontade.”

Henry Ford

RESUMO

Os usuários vivem apagando arquivos importantes de forma acidental e, é extremamente importante que se tenha um backup (cópia de segurança) dos dados como recurso de restauração dos mesmo. Com os crimes digitais aumentando para um nível bastante alarmante, surge a necessidade de cada vez mais criar-se e inovar-se as técnicas para combate à esses crimes. É de extrema importância à aplicação correta da perícia, para que os resultados coletados durante a pesquisa sejam aceitos e utilizados em segurança como prova em um tribunal de justiça. O objetivo deste trabalho compreendeu em aplicar técnicas de computação forense de duplicação pericial, recuperação de dados apagados, ocultos para busca e análise de evidências em sistemas de arquivos New Technologies File System (NTFS), realizando um estudo de caso com as ferramentas de recuperação em um dispositivo com sistema de arquivos NTFS, buscando resgatar arquivos deletados de forma acidental ou proposital, arquivos ocultos e segmentados. Para realização do mesmo efetuou-se uma pesquisa bibliográfica, bem como um estudo de caso fictício em ambiente controlado simulando a condução de uma perícia forense computacional, utilizando-se da metodologia SOP aplicando apenas as 4 primeiras etapas: coleta de prova, preparação dos equipamentos, imagem forense e exame (análise). Como resultado, conseguiu-se estudar e aplicar os conceitos de perícia forense computacional, analisando o conteúdo de alguns arquivos que se encontravam alocados na partição após a sua formatação, mantendo-se a integridade e confidencialidade das informações neles contidos. Ocasionalmente observou-se algumas falhas ao trabalhar com determinadas ferramentas, como por exemplo, a ferramenta iCare Data Recovery Free que não conseguiu recuperar arquivos superior a 2 GB permitido por fábrica, bem como foi informado que é necessário um registro ou cópia de ativação para prosseguir com a operação desejada. Foram apresentados metodologias e técnicas forense para busca e análise de evidências em dispositivos de armazenamento em NTFS, justificando com clareza e objetividade para que o mesmo possa ser aceito como objeto de estudo.

Palavras-chave: Peícia forense, Forense computacional, Crimes digitais, Sistema de arquivo NTFS.

ABSTRACT

Users living deleting important files by accident and it is extremely important to have a backup (backup) data as a resource for restoring it. With cybercrime increasing to a level quite alarming, the need arises to increasingly create and innovate the techniques to combat these crimes. It is extremely important to the proper application of expertise, so that the results collected during the survey are accepted and used safely as evidence in a court of law. This work consisted in applying techniques of computer forensics expert duplication, deleted data recovery, search for hidden evidence and analysis on filesystems New Technologies File System (NTFS), conducting a case study with the tools of recovery a device with NTFS file system, seeking to recover deleted files from accidentally or purposefully hidden files and segmented. To achieve the same we performed a literature search, as well as a fictional case study in a controlled environment simulating conducting a forensic computing, using the methodology SOP applying only the first 4 etapadas: gathering evidence, preparing equipment , forensic imaging and examination (analysis). As a result, we were able to study and apply the concepts of computer forensics, analyzing the contents of some files that were allocated to the partition after formatting, maintaining the integrity and confidentiality of the information contained therein. Occasionally there was some glitches when working with certain tools, such as tool iCare Data Recovery Free that could not recover files exceed 2 GB allowed by factory, and was informed that it is necessary to record or copy activation to proceed with the desired operation. Were presented methodologies and techniques for searching and analyzing forensic evidence storage devices in NTFS, explaining clearly and objectively so that it can be accepted as an object of study.

Keywords: Forensics Analysis, Computer Forensics, Computer Crime, NTFS File System.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AFF	Advanced Forensic Format
API	Application Programming Interface
CERT	Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança
DEFT	Digital Evidence & Forensics Toolkit
DFF	Digital Forensics Framework
DFRWS	Digital Evidence Research WorkShop
FDTK	Forensic Digital Tool Kit
FAT	File Allocation Table
FTK	Forense Toolkit
GPL	General Public License
HD	Hard Disk
IHCFC	International Hi-Tech Crime and Forensics Conference
IOCE	International Organization on Computer Evidence
MTF	Master File Table
NTFS	New Technologies File System
SO	Sistema Operacional
SOP	Standard Operating Procedures
SWGDE	Scientific Working Group on Digital Evidence
SGDE	Standard Group on Digital Evidence
TCC	Trabalho de Conclusão de Curso
UNESC	Universidade do Extremo Sul Catarinense

SUMÁRIO

1 INTRODUÇÃO

Cada vez mais é difícil de conceber que em tempos remotos não existia tantos meios tecnológicos (Computadores, *Smartphone*, *Ipad*, entre outros) que estão disponíveis hoje. Estes recursos se tornaram parte integrante na vida das pessoas, e o grande relevo desses meios tecnológicos é o computador.

Atualmente as pessoas usam computadores para se comunicar**,** guardar informações pessoais, fazer pesquisas na Internet e/ou até mesmo para execução de trabalhos profissionais. Com o aparecimento dessas tecnologias, surgiram também algumas técnicas de cometer crimes. Com isso os computadores e sistemas digitais são ferramentas e também alvos dos criminosos.

Em uma pesquisa divulgada pela consultoria Mi2g Intelligence Unit, em dezembro de 2004, foi constatado que o Brasil é o sétimo de dez países que mais possuem *hackers* responsáveis pelas invasões de sites no mês de outubro de 2004. Além disso, o Brasil é considerado um dos países que tem mais *hackers* ativos no mundo, com 75% dos ataques às redes mundiais partindo do Brasil.

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

Diariamente há diversos tipos de casos de fraudes e crimes onde o meio eletrônico foi em algum momento utilizado para este fim, sendo este tipo de caso chamado, de acordo com Ebrich e Valle (2005), de CyberCrime.

Segundo Adams (2000), atualmente já existem padrões metodológicos bem definidos e desenvolvidos pelo Scientific Working Group on Digital Evidence (SWGDE), que é o representante norte-americano na International Organization on Computer Evidence (IOCE). Esses padrões foram apresentados durante a International Hi-Tech Crime and Forensics Conference (IHCFC), realizada em Londres, de 4 a 7 de Outubro de 1999.

Esses padrões metodológicos seguem um único princípio: de que todas as organizações que lidam com a investigação forense devem manter um alto nível

de qualidade a fim de assegurar a confiabilidade e a precisão das evidências. Esse nível de qualidade pode ser atingido por meio de elaboração de *Standard Operating Procedures* (SOP), que devem conter os procedimentos para todo tipo de análise conhecida e prever a utilização de técnicas aceitas na comunidade científica internacional.

Segundo o CERT.br (2012), Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil, de 1999 a Setembro de 2012 foram reportados a está organização cerca de 356946 incidentes em relação à crimes cibernéticos.

Existem no mercado várias ferramentas que permitem realizar uma análise forense em ambientes com o sistemas de arquivo NTFS, auxiliando o perito, dentre elas o *Digital Forensics Framework* (DFF), onde a mesma possui particularidades de suma importância que ajudam a melhorar o processo de uma perícia.

O DFF é um software de forense livre e de código aberto construída em cima de uma interface de aplicação e programação dedicada Application Programming Interface (API). Ele pode ser usado tanto por profissionais e não especializados, com fácil e rápida finalidade de recolher, preservar e revelar evidências digitais, sem comprometer os sistemas de dados.

Feitas as considerações até o momento, o presente trabalho tem como objetivo propor um estudo, com o auxilio de algumas técnicas forenses computacionais e metodológicas, para busca de uma análise digital para arquivos excluídos, ocultos e segmentados visando o uso apropriado das ferramentas e as respectivas metodologias ao usuário empregando as mesmas.

1.1 OBJETIVO GERAL

Aplicar técnicas de computação forense de duplicação pericial, recuperação de dados apagados, ocultos para busca e análise de evidências em sistemas de arquivos New Technologies File System (NTFS), realizando um estudo de caso com as ferramentas.

1.2 OBJETIVOS ESPECIFICOS

Os Objetivos específicos desta pesquisa são:

a) compreender e aplicar os princípios básicos de perícia forense computacional em cima de arquivos NTFS (arquivos excluídos, ocultos e segmentados);
b) examinar e documentar os aspectos que envolvem a análise de evidências em ambiente Windows;
c) descrever e aplicar os conceitos das metodologias existentes para realizar perícia forense para obter evidências em ambientes Windows;
d) definir um cenário para realizar os experimentos na busca por evidências.

1.3 JUSTIFICATIVA

A tecnologia vem avançando e tomando proporções enormes em comparação há alguns anos, e o uso da Internet está em paralelo à esse avanço, proporcionando assim, um crescimento bastante expressivo no leque de fraudes por esse meio. As ameaças digitais causam inúmeros problemas, uma vez que muitos usuários abdicam do uso da Internet para executar tarefas que envolvam uso de dados pessoais e principalmente financeiros. Estes problemas ainda são maiores quando uma fraude é concretizada.

Com este grande avanço os peritos forenses computacionais necessitam de uma metodologia de padronização, desde a obtenção de evidências, passando pela padronização de laudos até a apresentação das mesmas perante a justiça (VARGAS, 2006).

Segundo Stephenson (2000, tradução nossa) crimes digitais, são delitos cometidos com o uso de um computador ou um sistema computacional. Porém, a natureza de um crime digital é mais complexa.

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

Tendo como base, o sistema de arquivos NTFS, que é amplamente

utilizado (CHOFFNES; DEITEL; DEITEL, 2005), porém, carente de estudos que abordam as técnicas forenses corretas, este trabalho vem a contribuir e suprir essa carência, por meio de pesquisa e aplicação das técnicas de busca, preservação e análise das evidências no ambiente NTFS.

Pretende-se com este trabalho contribuir também para o engrandecer em termos de referências bibliográficas para a comunidade científica, onde poderão ser enumeradas várias contribuições importantes como, metodologias e ferramentas utilizadas em sistemas de arquivos New Technologies File System (NTFS).

1.4 ESTRUTURA DO TRABALHO

Como dito anteriormente, o presente trabalho tem como proposito aplicar técnicas de computação forense para análise de evidências em ambientes NTFS. O mesmo está compreendido em duas partes: a primeira aborda a fundamentação teórica com assuntos relacionados como aprentado no título do trabalho e a segunda etapa, a parte desenvolvida, o estudo de caso realizado visando demonstradar os princípios básicos de perícia forense com auxílio das ferramentas.

O primeiro capítulo apresenta aspectos sobre perícia forense computacional, a finalidade do trabalho, a justificativa e os objetivos a serem alcançados. O segundo aborda o sistema de segurança empregues em sistemas de arquivos NTFS, extruturas, entre outros.

O terceiro capítulo apresenta questões sobre pericia forense computacional, metodologias forenses e investigarivas aplicadas no presente trabalho, bem como algumas distribuições para pericia forense encontradas no mercado.

O capitulo seguinte esboça alguns trabalhos relacionados ao tema da pesquisa, onde são apresentados como trabahos correlatos.

Foi feita a análise de um caso de estudo para auxíliar na compreenção das metodologias empreagadas para fazer a perícia, foram apresentadas também as ferramentas usadas.

E no final encontra-se a parte prática e a conclusão, aonde podem ser encontradas informações resumidas sobre os resultados obtidos.

2 SEGURANÇA DA INFORMAÇÃO

Com a dependência do negócio aos sistemas de informação e com o aparecimento de novas tecnologias e outras formas de trabalho, como a venda de produtos eletrônicos, as redes virtuais privadas e os funcionários móveis, as empresas começaram a despertar para a necessidade de segurança, uma vez que se tornaram vulneráveis a um número maior de ameaças.

As redes de computadores, e consequentemente Internet mudaram as formas como se usam sistemas de informação. As possibilidades e oportunidades de utilização são muito mais amplas que em sistemas fechados, assim como riscos à privacidade e integridade da informação. Portanto, é muito importante que mecanismos de segurança de sistemas de informação sejam projetados de maneira a prevenir acessos não autorizados aos recursos e dados destes sistemas (LAURENÇO, 2004).

Segurança de informação é a proteção de informações, sem se preocupar onde esteja armazenada (no papel, na memória do computador ou em um dispositivo de armazenamento). Um computador é considerado seguro caso haja qualquer autenticação de que é capaz de exercer exatamente as mesmas funções. Todo usuário de computador almeja, no que diz respeito à segurança de dados, que as informações armazenadas, nem que por algumas semanas, permaneça, sem que outros usuários não autorizados acessem o mesmo conteúdo. O usuário espera que suas informações esteja disponíveis no momento e local que ele determinar que seja correta e mantida fora do alcance e das vistas de pessoas não autorizadas (DIAS, 2000).

> Na época em que as informações eram armazenadas apenas em papel, a segurança era relativamente simples. Bastava trancar os documentos em algum lugar e restringir o acesso físico àquele local. Com as mudanças tecnológicas e o uso de computadores de grande porte, a estrutura de segurança já ficou um pouco mais sofisticada, englobando controles lógicos, porém ainda centralizados. Com a chegada dos computadores pessoais e das redes de computadores que conectam o mundo inteiro, os aspectos de segurança atingiram tamanha complexidade que há a necessidade de desenvolvimento de equipes cada vez mais especializadas para sua implementação e gerência. Paralelamente, os sistemas de informação também adquiriram uma importância vital para a sobrevivência da maioria das organizações modernas, já que, sem computadores e redes de comunicação, a prestação de serviços de informação pode se tornar inviável (DIAS, 2000, p.39).

Com o passar dos anos é possível verificar que a urgência de obter e de registrar as informações não era a única preocupação. Não era preciso somente guardá-las, era necessário também mantê-las a salvo. Casos como incêndio da lendária Biblioteca de Alexandria trouxeram à tona a questão da segurança da informação (SOUZA, 2005).

Foram desenvolvidas inúmeras técnicas para este fim, técnicas como: vigias controlando o espaço onde se armazenavam os registros; e/ou as coisas mais atuais como cofres, com o único propósito de proteger as informações, que nos dias de hoje são consideradas patrimônio.

Segurança da informação é aplicada em todos os aspectos de proteção e armazenamento de informações e dados, de qualquer forma. Caracteriza-se pelo estudo de técnicas que tendem a fornecer um estado de proteção ao patrimônio computacional e intelectual de uma organização (OLIVEIRA, 2007).

No ambiente computacional, a segurança é vista também como sendo, proteção ao patrimônio da organização e aos investimentos feitos em equipamentos, software e pessoal. Os meios da computação e as informações sobre a organização, por terem alto valor de mercado, podem ser interesse para ladrões ou espiões (DIAS, 2000).

Conforma Dias (2000) segurança é a proteção de informações, sistemas, meios e serviços contra desastres, erros e manipulação não autorizada, de forma a reduzir a probabilidade e o impacto de incidentes de segurança.

2.1 OBJETIVOS DA SEGURANÇA

Tecnologia da Informação (TI) ou segurança da informação, a segurança baseia-se em três objetivos principais: a preservação da confidencialidade da informação, a integridade e disponibilidade (OLSON; ABRAMS, 1995, tradução nossa).

Como existem várias formas de implementação de segurança em informática, os objetivos de segurança variam de acordo com o tipo de ambiente computacional e a natureza do sistema (administrativo, financeiro, entre outros). Para identificar os objetivos é essencial fazer uma análise da natureza da aplicação, dos riscos e impactos prováveis. Tanto usuários comuns como profissionais do departamento de informática deve se preocupar, em maior ou menor grau, com os

seguintes objetivos de segurança (DIAS, 2000):

a) **confidencialidade ou privacidade** – é a garantia do resguardo das informações dadas pessoalmente em confiança e a proteção contra a sua revelação não autorizada;
b) **integridade de dados** – é a garantia de que a informação não sofreu alterações durante a sua transmissão. Tipos de integridade:
   - **receptor -** assinatura digital,
   - **dados -** algoritmos de hash;
c) **disponibilidade –** a informação ou sistema de computador deve estar disponível no momento em que a mesma for necessária.

2.1.1 Problemas de segurança no Windows

No mundo existem as vulnerabilidades, existem também os ataques e eles vêm crescendo a cada dia que passa, tanto em qualidade como em quantidade. A necessidade de se ter uma Infraestrutura de segurança é de caráter obrigatório, existindo, um planejamento específico, uma gerência e uma metodologia bem definida (COPPE/UFRJ, 2006).

2.1.2 Análise dos dados ocultos no Windows

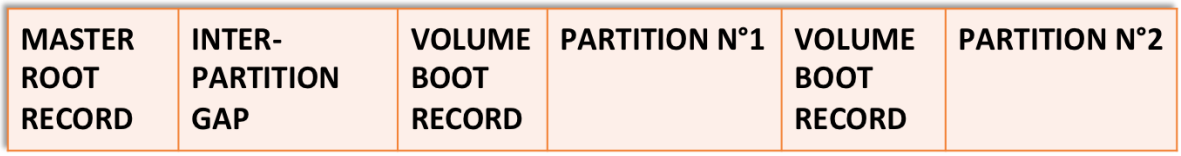
Comumente, os criminosos ocultam dados no disco rígido. Existem duas técnicas conhecidas para esconder dados na unidade de disco rígido (BANSOD, 2009, tradução nossa):

a) por formatação de baixo nível: os hackers preferem setores redundantes e setores ruins;
b) por particionamento: os dados podem ser ocultos na partição inter-lacunas, espaços não alocados, partições ocultas, registros de inicialização de partição, tabelas e partições apagadas.

Para a plena compreensão desse assunto, devemos conhecer os detalhes do sistema de arquivos do Windows ou outros sistemas de arquivos conhecidos atualmente (BANSOD, 2009, tradução nossa).

Formatação de baixo nível é realizado na fábrica, o que cria setores. Cada sector tem 512 bytes e alguns aéreos, que fornece correções de erros. As unidades de disco rígido do controlador remapeia sectores maliciosos por sectores redundantes. Os criminosos podem abusar desses sectores redundantes. A figura 1 mostra detalhes do particionamento do disco rígido. O Master Boot Record (MBR), que começa em um setor, consiste no código de inicialização mestre - *Master begin Code* (MBC) e a tabela de partição mestre – *Master Partition Table* (MPT). O volume de registro de arranque - *Volume Root Record* (VBR) consiste no código de inicialização do volume e do bloco de parâmetros de disco (BANSOD, 2009, tradução nossa):

Figura 1 – Particionamento do disco rígido



Fonte: Adaptado de Bansod (2009).

2.2 CRIMES DIGITAIS

Acusação, advém do significado da palavra crime, que em latim pronuncia-se *crimen*. Segundo Aguiar (2009), para que um crime seja executado faz-se necessário uma conduta humana positiva (ação) ou negativa (omissão), que seja típica e descrita na lei de infração penal ,e que, por conseguinte haverá crime se o fato for antijurídico.

Apesar de Brasil e Angola seguirem caminhos diferentes para atingir seu desenvolvimento, ambos compartilham muito mais do que um passado semelhante. O Brasil é um país enorme na América Latina, seus recursos naturais, sua economia, as suas políticas internas e externas, e sua sociedade da informação são muito semelhantes aos de Angola. Como resultado, a cooperação e as parcerias entre os dois países têm vindo a crescer nos últimos anos (CUMMIS, 2009, tradução nossa).

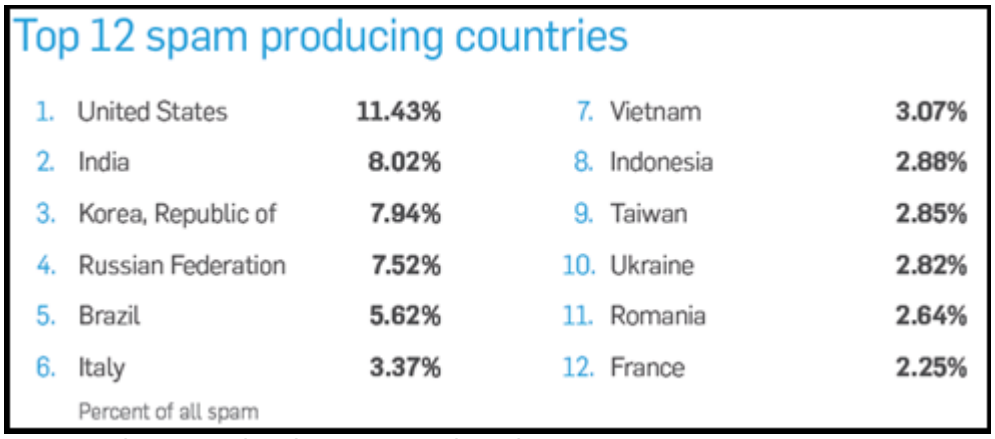
O autor, em particular, está interessado no Brasil por causa de dois fatores: as altas taxas de criminalidade em ambiente que se utiliza de elementos computacionais e também na falta de leis de tecnologia da informação.

De acordo com a Sophos Secutity Threat (2012), o Brasil encontra-se

entre os cinco países do mundo com a maioria em disseminação de spam, contabilizado por 4,3% do restante total. O crime informático é uma grande preocupação para o governo brasileiro e, apesar de as taxas diminuírem, o país tem sido vítima e ofensor. As principais razões para isso são que: o número de pessoas alfabetizadas no uso do computador é elevado, os recursos para monitorar e controlar a criminalidade informática são ainda muito escassos por causa da falta parcial de leis de tecnologia da informação (CUMMIS, 2009, tradução nossa).

A figura 2 ilustra o ranking dos países com a maior disseminação de spam, onde se pode observar que o país que lidera o top é o Estados Unidos e por final encontra-se a França.

Figura 2 – Top dos 12 países disseminadores de Spam



Fonte: Sophos Security Threat Report (2012).

Crime digital refere-se a fraudes ou roubos cometidos por meio de um computador e *Internet*. O fraudador invade um computador, obtém senhas ou outros dados confidenciais e realiza um desvio financeiro. Há outros crimes realizados como pedofilia, difamação, roubo de identidade, racismo, tráfico de drogas, que se enquadram no termo crime digital, e que não serão citados na pesquisa.

O crescimento das redes de computadores e as exposições cada vez maior da nossa privacidade nas redes sociais, o aumento do furto de dados financeiros e bancários, à informações pessoais, fazem de nós alvos fáceis conectando-se à essa grande rede que é a Internet, e qualquer que seja a pessoa conectada a ela corre algum tipo de risco, seja em casa, no trabalho, na rua usando um dispositivo móvel, na escola. Se o acesso à Internet aumenta, os riscos também.

2.2.1 Etapas da forense digital

A computação Forense faz parte de um processo de investigação, que tem por objetivo provar os fatos ocorridos com a maior clareza possível. Para que isso ocorra, o perito que for nomeado para realizar a perícia deve trabalhar de uma forma sistemática e cuidadosa com as evidências com o intuito de sempre preservar a integridade dos dados e detalhar toda a atividade executada no laudo final. Todo esse processo pericial na forense computacional é dividido em quatro etapas conforme a seguir (KENT et al, 2006, tradução nossa; PEREIRA et al, 2007):

a) **coleta de dados:** esta etapa é considerada a mais vital de todo o processo, ou seja, a que mais precisa de cuidados. Ela tem tal importância, pois é nela que toda a massa crítica de dados será coletada, sendo necessário cuidado especial para manter a integridade das informações (SWGDE, 2006, tradução nossa). Outras atividades que são realizadas nesta etapa são relacionadas ao equipamento questionado, que deve ser identificado, devidamente embalado de uma forma segura, etiquetada as suas partes e suas identificações registradas no documento de cadeia de custódia (PEREIRA et al, 2007);

b) **exame de dados:** nesta segunda etapa o objetivo principal é separar as informações relevantes ao caso de outras sem importância, como os arquivos do próprio sistema. Antes de iniciar o processo é preciso definir quais as ferramentas que serão utilizadas para o exame dos dados. Esta escolha está relacionada a cada tipo de investigação e informações que estão sendo procurados. Diante disso, pode se definir ferramentas que captem um número maior de dados úteis (KENT et al, 2006, tradução nossa). Peritos geralmente utilizam filtros de arquivos, busca por palavras-chaves, entre outros procedimentos para agilizar a busca por evidências;

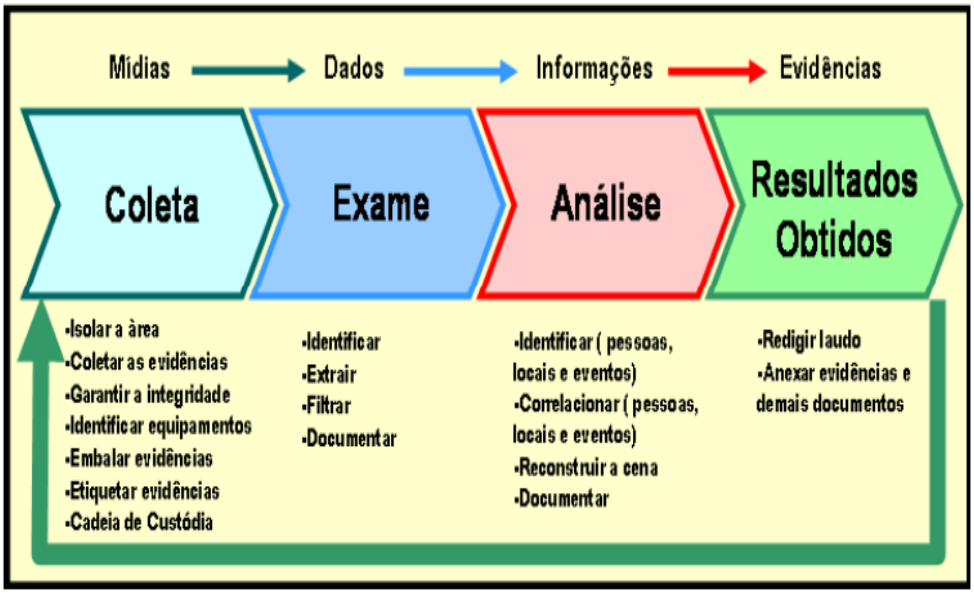
c) **análise das informações:** na terceira fase, as informações anteriormente separadas serão analisadas com o intuito de encontrar dados úteis e relevantes que auxiliem na investigação do caso. Todos os dados encontrados considerados relevantes referentes à

investigação, para que assim seja possível realizar a conclusão (PEREIRA et al, 2007);

d) **interpretação dos resultados:** nesta última etapa, o objetivo é apresentar um laudo (relatório técnico) que deve informar com toda a veracidade possível o que foi encontrado nos dados analisados. Todo o processo pericial desde o início, ferramentas e informações que comprovem a integridade das informações devem ser relatadas no laudo (SWGDE, 2006, tradução nossa).

Conforme a descrição nas etapas apresentadas anteriormente, a figura 3 demostra de forma clara de todo o processo de investigação em computação forense.

Figura 3 – Fases do processo de investigação.



Fonte: Adaptado de Pereira et al (2007).

2.2.2 Investigação de forense digital

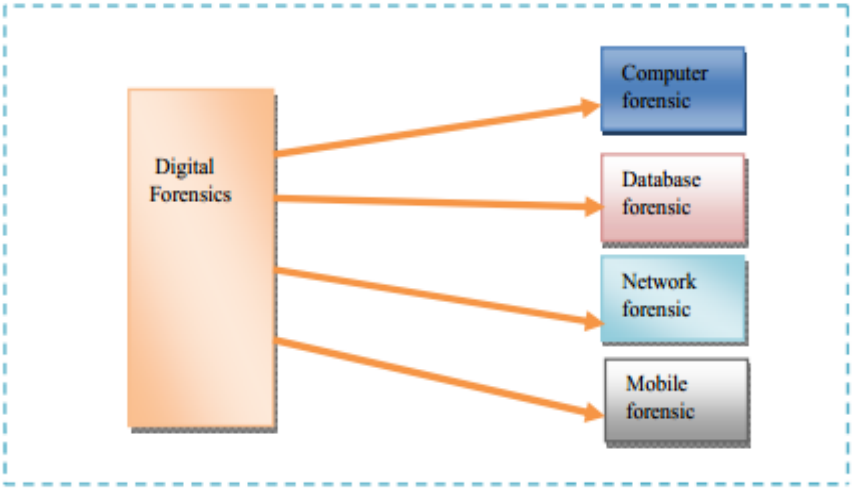
A investigação forense de um crime é um método muito complexo, primeiramente toma seu início na cena do crime, passado para os laboratórios de perícia, posteriormente encaminhado para investigação e tem como final, o tribunal, onde será feito o julgamento preciso.

A Forense Digital é um ramo da ciência forense, usado para recuperação, envolvendo investigação de dados em dispositivos digitais, quase sempre em relação ao crime computacional. Forense digital é a parte mais importante da

investigação computacional para recuperação de dados (YADAV; AHMAD; SHEKHAR, 2011, tradução nossa).

Crime computacional é definido como um ato de sabotagem, a exploração de um sistema de computador individual, grupo de sistema interligado e dispositivos tecnológicos, como telefones celulares, assistentes digitais pessoais para cometer crime doloso e digitais podem aparecer romance, muitas de suas características é a mesma como os de crimes convencionais. A Forense digital está dividida em quatro tipos de áreas forenses, conforme detalhes destas forense, figura 4 (YADAV; AHMAD; SHEKHAR, 2011, tradução nossa):

Figura 4 – Classificação de forense digital



Fonte: YADAV et al (2011)

a) **forense computacional:** explica o estado atual de um artefato digital, como meio de armazenamento ou documento eletrônico do computador, ele pode lidar com ampla gama de informações digitais de registros do sistema, tais como históricos do navegador com a ajuda de arquivos reais armazenados no disco;
b) **banco de dados forense:** é o estudo de bancos de dados e seus metadados. Banco de dados forense usa conteúdo de banco de dados, arquivos de log a fim de recuperar a informação relevante;
c) **Redes forense:** controlam e analisam o tráfego das redes de computadores (tanto a LAN como a internet MAN) para coleta de informações com a finalidade de prova legal. Forense de rede nos

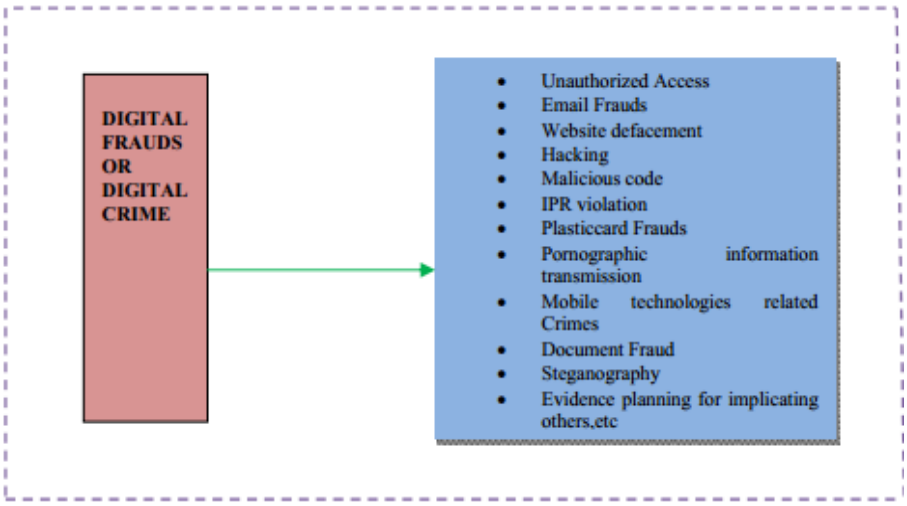
permite fazer determinações forenses com base no tráfego observado da rede;

d) **Celular forense:** recuperação de dados a partir de dispositivos móveis. Nesta investigação forense geralmente se concentra em dados simples como detalhes de chamadas e de SMS ou e-mails ao invés de recuperação de dados apagados. Os dispositivos móveis oferecem também informações sobre a localização.

2.2.3 Tipos de fraudes ou crimes digitais

O sistema de redes e de computadores não pode ser utilizado na execução de crimes de computador, mas fazem parte dos crimes computacionais. Análise forense digital deste tipo de sistema e redes pode fornecer evidências digitais, por exemplo, o planejamento de um assassinato, assédio e pornografia, roubo de informações armazenadas eletronicamente e os dados do sistema de computador, gerar documentos fraudulentos com a ajuda de scanners e impressoras. Internet é a aplicação mais importante para as pessoas da sociedade moderna. Internet tem muita comodidade para comunicação entre humanos em todo o mundo. Os rápidos desenvolvimentos e a carência de normas adequadas e regulamentos de Internet se converte em um centro de crimes. Existem muitos tipos de crimes digitais, alguns deles estão indicados na figura 5 (YADAV; AHMAD; SHEKHAR, 2011, tradução nossa):

Figura 5 – Tipos de fraudes ou crimes digitais

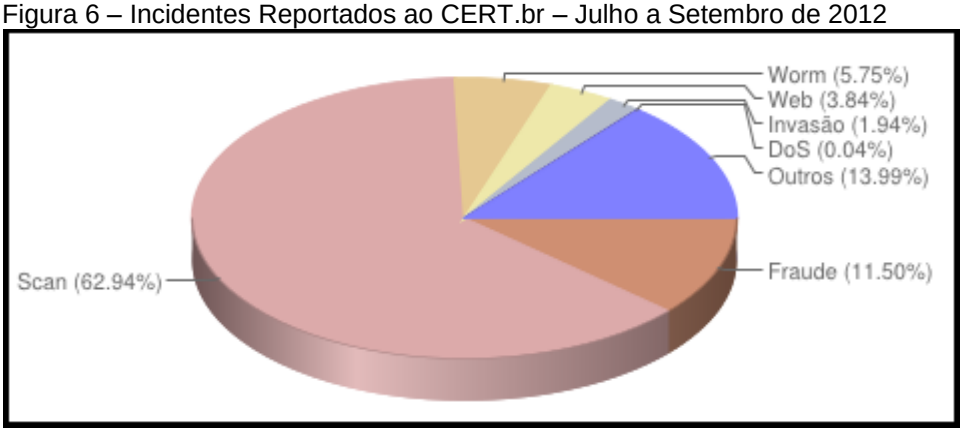


Fonte: YADAV et al (2011)

2.2.4 Tipos mais comuns de crimes digitais

A figura 6 permite-nos observar as percentagens de vários incidentes que ocorreram entre Julho a Setembro durante o ano corrente e foram reportados ao (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança) CERT.br, separados por tipos de ataques.

Figura 6 – Incidentes Reportados ao CERT.br – Julho a Setembro de 2012



Fonte: Adaptado de CERT.br (2012)

De acordo com o CERT.br (2012) e como se pode observar na figura anterior, os tipos mais comuns de crimes digitais são:

a) **fraude:** conceituada como sendo qualquer ação astuta, dolosa e de má-fé, com o objetivo de lesar ou ludibriar outrem, ou de não cumprir determinado dever (Houaiss, 2009). Nesta categoria encontram-se notificações de tentativas de fraudes, onde o invasor tentou obter uma vantagem;

b) **Denial of Service (DOS):** ataques DoS são feitos enviando um grande volume de solicitações a páginas *web* com o objetivo de tornar o sistema indisponível, podendo ser lançado contra outro host conectado à Internet. O atacante, utilizando-se de uma computador, tem como objetivo remover de serviço um computador ou rede (MORIMOTO, 2008);

c) **worm:** atividades maliciosas e automatizado, que se propagam automaticamente na rede de computadores.

d) **scan:** serviços de varreduras realizadas em redes de computadores, com o intuito de identificar quais computadores estão funcionando e quais serviços estão sendo utilizados por eles. Atacantes utilizam para

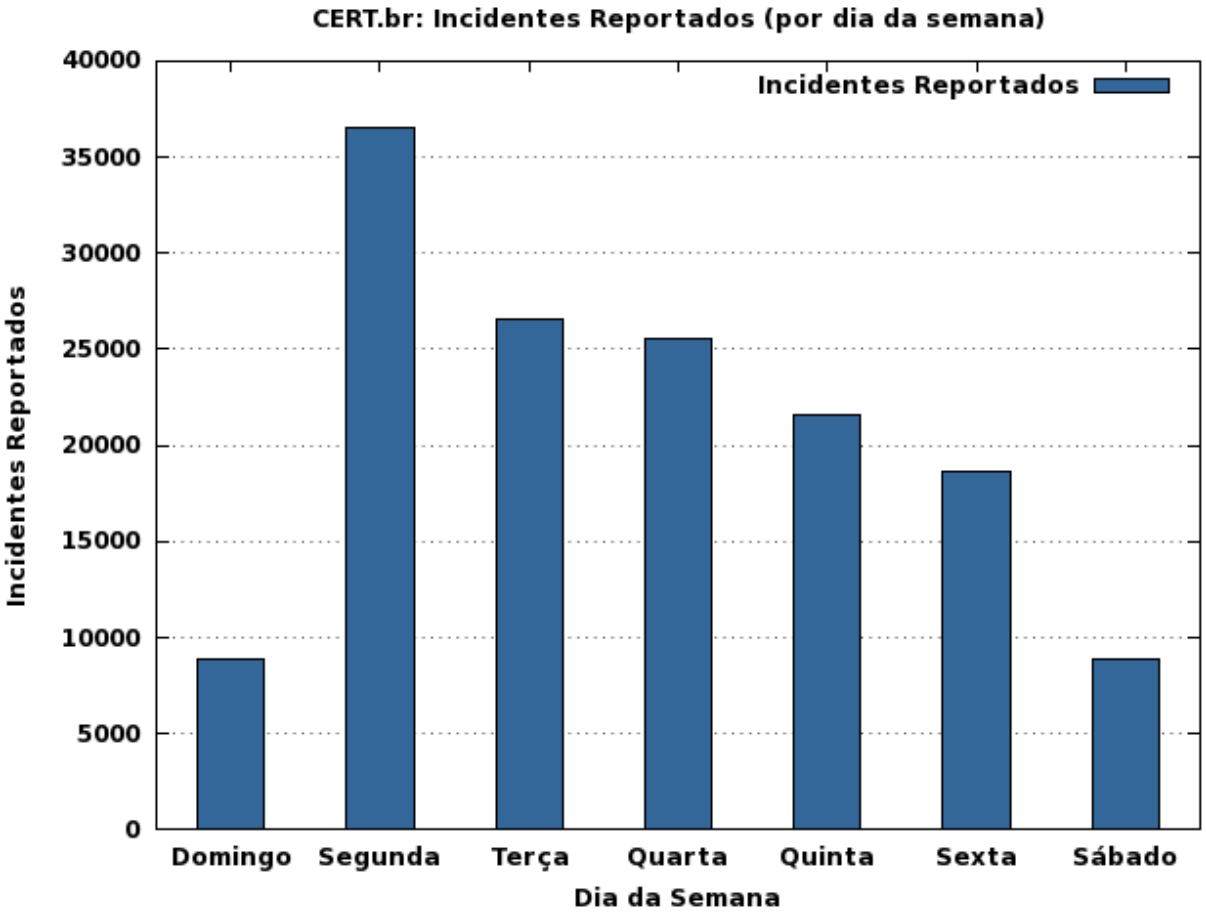
identificar potenciais alvos, sendo que a mesma, permite associar possíveis vulnerabilidades aos serviços habilitados em um computador;

e) web: particularidade de ataques cujo o alvo é o comprometimento de servidores Web ou desfigurações de páginas na Internet;

f) outros: notificações de incidentes recebidas pelo CERT.br que não se enquadram nas categorias anteriores.

Ainda de acordo com o CERT.br (2012), a maioria dos crimes reportados no mesmo foi o de *Scan* (62,94%) e que as tentativas ocorrem maioritariamente na segunda-feira, indicando uma forte tendência dos criminosos na busca por informações de usuários e também à outras notificações de incidentes recebidas pelo CERT.br que não se enquadram nas categorias apresentadas anteriormente, conforme observa-se na figura 7.

Figura 7 – Incidentes Reportados ao CERT.br – Por dias da semana



Fonte: Adaptado de CERT.br (2012)[1]

[1] CERT.br. **Incidentes Reportados ao CERT.br—Julho a Setembro de 2012.** 2012. Disponível em: < http://www.cert.br/stats/incidentes/2012-jul-sep/weekdays-incidentes.html> Acesso em: 10 nov. 2012, 20:10:15.

2.2.5 Análise de forense digital

O objetivo de qualquer tipo de análise forense é desvendar as evidências digitais para uma possível investigação. Uma investigação forense emprega evidência física ou digital com processos ou procedimentos científicos para a descoberta de conclusões (YADAV; AHMAD; SHEKHAR, 2011, tradução nossa). A investigação forense digital consiste em três etapas:

a) **apreensão** – esta é a transferência de preservação ou de propriedade de mídia digital antes que seja examinado pelo perito (ISSUE, 2010, tradução nossa);

b) **aquisição e coleção de imagem -** fase onde são armazenados os estados dos dispositivos digitais onde serão analisados posteriormente. Este método é quase igual a tirar uma foto, tirar amostras de sangue e impressões digitais de uma cena de crime, ou seja, áreas alocadas e não alocadas de um disco rígido são duplicados, referenciando à imagem de uma investigação (YADAV et al, 2011, tradução nossa);

c) **análise de mídia digital –** nesta fase, as informações contidas nos arquivos de imagem são analisados pelos examinadores forenses com ferramentas especializadas, como EnCase Guidance e Sleuth Kit (TSK), para identificação de evidências (ISSUE, 2010, tradução nossa);

d) **relatório -** esta é a fase final, quando a prova é recuperada os dados são analisados para reconstruir as ações e chegar a conclusões, quando uma está completa o investigador apresenta as suas informações, geralmente sob forma de uma escrita a relatar. Um “relatório digital forense” deve incluir as seguintes informações (YADAV et al, 2011, tradução nossa). Adaptado de (ISSUE, 2010, tradução nossa):

- qualquer informação relevante, a respeito do que leva você como perito e quando você se envolveu com a evidência digital,
- as etapas detalhadas tomadas e as pessoas entrevistadas para preservar e adquirir prova forense, incluindo quaisquer medidas adicionais que você tomar (como por exemplo, exame de mídia),
- todos os fatos que você encontrar durante a sua análise relacionados com o caso,

conclusão da prova forense.

2.3 LEGISLAÇÃO INTERNACIONAL (BRASIL)

O Brasil não possui uma legislação específica para crimes de informática, sendo assim, são aplicadas as leis existentes que podem ser interpretadas para o meio digital e, consequentemente, os responsáveis podem ser indicados por crimes de extorsão, difamação e furto de dados, privados ou secretos.

As legislações utilizadas em discussões sobre Internet atualmente são embasadas em conceitos de Direito Constitucional, Direito Civil, Direito Penal, Direito Internacional Público e Privado e também às legislações especiais como o Estatuto da Criança e do adolescente (Lei 9.610/98), Lei do Direito Autoral (Lei 9.610/98), Lei do Software (Lei 9.609/96), Lei da Escuta Telefônica (Lei 9.296/96), entre outras. Ainda pode-se dividir o Direito de Informática em Direito Civil da Informática e Direito Penal da Informática. O Direito Civil da Informática passaria a concentrar seus estudos no conjunto de normas para regulamentação de relações privadas que envolvam a aplicação da informática, como computadores, sistemas, direitos autorais, documentos eletrônicos, assinaturas digitais. Já o Direito Penal de informática seria o conjunto de normas destinadas a regulamentar a prevenção, repressão e punição aos fatos que atentem contra o acesso, uso, exploração, segurança, transmissão e sigilo de dados armazenados e de sistemas manipulados por computador (ROSA, 2007, p. 46)

Assim como Angola, o Brasil não tem uma legislação independente para alvejar crimes feitos por meio de um computador ou a questões relacionadas com computadores. A forma como as autoridades brasileiras têm encontrado para enfrentar esses casos, nos tribunais, é adaptar sua legislação existente, dando diferentes interpretações possíveis de leis específicas. Como exemplo: Lei nº 2848/40 artigo 163 “Destruir, inutilizar ou deteriorar a coisa alheia”, provavelmente um criminoso poderia ser condenado nos termos desta lei, caso ele seja o autor de um vírus ou de qualquer outro software, que cause algum dano ao computador, ou corromper os dados que não era de sua parte (CUMMIS, 2009, tradução nossa).

Abaixo estão relacionadas algumas leis utilizadas para punir os criminosos digitais (BRASIL, 2012):

a) **Lei nº 9296:** é crime uma pessoa interceptar ou apenas monitorar tráfego de comunicação de outra pessoa sem possuir uma autorização judicial;
b) **art. 10.:** “Constitui crime realizar interceptação de comunicações telefônicas, de com informática ou telemática, ou quebrar segredo da justiça, sem autorização judicial ou com objetivos não autorizados em lei” (L9296/96). Baseando-se no artigo 10, muitos fraudadores poderiam ser devidamente enquadrados, pois para ter acesso a senhas e/ou outros dados importantes da vítima, ele (o fraudador) necessitará interceptar ou monitorar o tráfego de Internet para roubar os dados assim que a vítima efetuar alguma transação;
c) **Lei nº 2848 no artigo 153:** “Divulgar alguém, sem justa causa, conteúdo de documento particular, ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem” (L2848/40). O acesso às informações pessoais da vítima quer seja descobrindo a senha e com isso ter acesso aos e-mails, por invasão de servidores buscando informações pessoais de um grupo, ou com a finalidade de analisar o tráfego em uma rede privada, pode ser considerado como sendo infração do artigo em questão, pois um tráfego de rede provavelmente terão muitas informações privadas ou até secretos, como senhas;
d) **Lei nº 2848 no artigo 155:** “Subtrair, para si ou para outrem, coisa alheia móvel” (l2848/40).

Existem vários vírus quem têm como característica enviar *e-mails* para usuários do catálogo de endereços da vítima, com partes de *e-mails* enviados e/ou recebidos por outros usuários ou colocar no corpo da mensagem fragmentos de textos que são de caráter secreto.

Com base neste artigo, o criminoso responsável pelo envio do *e-mail* poderia ser punido, pois estaria propagando informações secretas e sigilosas.

Ainda de acordo com Cummins (2009, tradução nossa), Angola não pode de modo simples, copiar e colar leis em sua legislação e esperar que a Comunidade Lei entenda essas novas leis, dizendo que o autor acredita que a melhor estratégia para a criação de leis de TI, é seguir uma abordagem que tenha em conta as leis já existentes, porque ao fazê-lo, seria muito mais fácil para a Comunidade Lei de

entender pelo menos o básico das Tecnologias de Informação e Comunicação e os crimes que podem derivar deles.

2.3.1 Legislação internacional (Portugal)

Segundo Cummins (2009, tradução nossa), ao longo dos anos, levantou-se um caso que não foi incluído na legislação atual. As entidades portuguesas atualizaram algumas de suas leis mais importantes de Tecnologia de Informação (TI) e eles são os seguintes:

a) **a Lei de Crime Cibernético:** esta lei consiste em definir terminologias tais como: redes de computadores, sistemas de computador, software, topografia e interceptação. Em seguida propõe os seguintes assuntos: falsidade, danos em dados de computador, sabotagem de computadores, acesso ilegal, intercepção ilegal e reprodução ilegal de software (DIÁRIO DA REPÚBLICA PORTUGUESA, a Lei nº 109/91);

b) **a lei de Transmissão e Recepção:** esta lei regula a transmissão e recepção de documentos eletrônicos certificados por qualquer entidade governamental (DIÁRIO DA REPÚBLICA PORTUGUESA, a Lei nº 66/2005).

A caracterização dos crimes informáticos deu-se com a chegada da Lei nº 109/91, época onde foram criadas figuras penais na área da computação. Para certificar, segue abaixo as condutas punidas (CRESPO, 2011):

a) falsidade informática: art. 4º - penalização da introdução, modificação ou supressão de informações ou programas de informática, visando falsificar a obtenção de dados eletrônicos;

b) dano a dados ou programas informáticos: art. 5º - fase onde a conduta é a devastação de dados eletrônicos ou de programas informáticos, visando de alguma vantagem ilícita;

c) sabotagem informática: art. 6º - penalização da conduta de apagar, alterar, introduzir ou abolir informações, visando-se dificultar ou impedir o funcionamento da comunicação de dados à distância;

d) acesso ilegítimo: art. 7º - sendo penalizada a conduta de ocupar sistemas alheios.

e) **Interceptação legítima:** art. 8º - penalização por interceptações irregulares em ambiente computacional;
f) **Reprodução legítima de programa protegido:** art. 9º - penalização da reprodução, divulgação ou a comunicação de *software*, sem, autorização.

2.3.2 Legislação internacional (França)

A tradição da França nunca foi expor modelos penais designados a reprimir os crimes digitais. Na década de 1988, 5 de Janeiro, o Código Penal francês sofreu uma alteração, pela Lei n.88-19, incorporando-se um capítulo especial (atrs. 462-2 a 462-9) impedindo que continue os atentados contra sistemas computacionais. Em designação a Lei nº 88-19, foram feitas as seguintes incriminações (CRESPO, 2011):

a) **acesso fraudulento a sistema de elaboração de dados:** (462-2) – é considerado crime ter-se acesso ilegal em sistema, havendo alteração dos dados ou do sistema, a pena é aumentada;
b) **sabotagem informática:** (462-3) – penalização da conduta de quem apaga ou falsifica bom funcionamento do sistema computacional;
c) **destruição dos dados:** (462-4) – é apontado como culpado o cidadão que, com o intuito de lesar, introduz, modificar os dados do sistema;
d) **falsificação de documentos informatizados:** (462-5) – é penalizado quem falsifica documentos informatizados com o intuito de causar prejuízo a outrem;
e) **uso de documentos informatizados falsos:** (462-6) – penaliza aquele que faz o uso de documentos falsos.

2.3.3 Legislação internacional (Japão)

Bem antes da reforma penal de 1987, Japão, apresentava algumas irregularidades na maneira como tratava os ilícitos penais informáticos. A adaptação da lei era feita de forma “aplicável”, de acordo com as regras de diplomacia. Existia uma concepção de crime informático denotado pela Agência Nacional de Polícia, abarcando as seguintes condutas (CRESPO, 2011):

a) forjar dados informáticos;
b) adquirir de forma ilegal ou por acesso não autorizado os dados;
c) uso desautorizado da máquina com o intuito de saquear tempo;
d) sabotagem informática.

2.4 ANÁLISE DO SISTEMA DE ARQUIVOS NTFS

A preocupação com a análise do sistema de arquivos fundamenta-se pela complexidade de se atacar um computador sem que este personagem seja alterado, transformando-o em uma importante fonte de evidências. O objetivo é fornecer ao leitor uma visão geral acerca da estrutura do sistema de arquivos nativo no Windows 2000, além de discutir técnicas e ferramentas que poderiam ser utilizadas durante sua análise. Através do exame minucioso do NTFS em baixo nível é possível visualizar dados e estruturas que são geralmente ocultados pela interface entre o SO e o usuário, o que pode, consequentemente, levantar indícios que criem, comprovem ou descartem teorias sobre o incidente (OLIVEIRA, 2002).

2.4.1 Conhecendo Arquivos NTFS

Em NTFS, tudo é arquivo. Isto inclui metadados do sistema de arquivos sobre a estrutura do sistema de arquivos. Master File Table (MFT) é o coração dos NTFS. Cada arquivo ou diretório tem pelo menos uma entrada MFT e, cada entrada a MFT é chamada como registro de arquivo, seu tamanho padrão é 1024 bytes. Os primeiros 42 bytes são fixados para MFT, cabeçalho de entrada e no resto é armazenado os atributos de entrada, que é a pequena estrutura de dados com um propósito específico. Os dados são armazenados no aglomerado, o que é um espaço pequeno. Exemplo de alguns atributos: $STANDARD_INFORMATION; $FILE_NAME; $DATA (MIKHAILOV, 2000, tradução nossa).

O conteúdo de um atributo pode ser (CARRIER, 2006, tradução nossa):

a) **residente**: armazena o seu conteúdo na entrada MFT com o cabeçalho atributo;
b) **não residente**: armazena o conteúdo em um cluster externo no sistema de arquivos.

A lista de *clusters* utilizada é armazenada como executado na lista de execução de um atributo. Unidade de dados em NTFS é chamado de cluster, que é a menor unidade de alocação de espaço em disco. Cada cluster em NTFS tem um *Logical Cluster Number – Número de Cluster Lógico (LCN)*. O número de cluster começa com 0 no primeiro cluster do sistema de arquivos. Cluster pertencem a um arquivo também associado a *Virtual Cluster Number – Número Virtual Cluster (VCN)*, como exemplo, um arquivo com 6 conjuntos terão 1 arquivo com VCN 0 e o último cluster com VCN 5 (BANSOD, 2009, tradução nossa).

O próximo capítulo visa abordar sobre aspetos bastante relevantes voltados para a perícia forense computacional.

3 PERÍCIA FORENSE COMPUTACIONAL

A perícia forense aplicada à informática, que também é conhecida como computação forense, forense computacional, criminalística computacional, forense digital, investigação eletrônica e perícia eletrônica, é a aplicação de conhecimentos em informática e técnicas de investigação com a finalidade de obtenção de provas (FREITAS, 2006).

Segundo Melo (2009), a Computação Forense também é definida como uma área da Ciência da Computação que se desenvolve gradualmente para acolher à demanda oriunda da área da Criminalística, e também como uma parte da Criminalística que se apropria de fundamentos da Ciência da Computação.

A perícia forense é uma área relativamente nova e tornou-se uma prática investigada importante tanto para as empresas quanto para a polícia. Utiliza de métodos científicos para identificar, preservar, analisar e documentar evidências localizadas em computadores e outros dispositivos eletrônicos (FREITAS, 2006).

> A computação forense é uma ciência voltada para o estudo e avaliação de situações que envolvam a computação como meio para cometer crimes. Muitas pessoas acreditam que a atividade pericial na computação é recente, devido ao pouco tempo em que a informática vem fazendo parte de nossas vidas, mas essa ciência é um pouco mais antiga do que nós imaginamos (COSTA, 2003, p. 28).

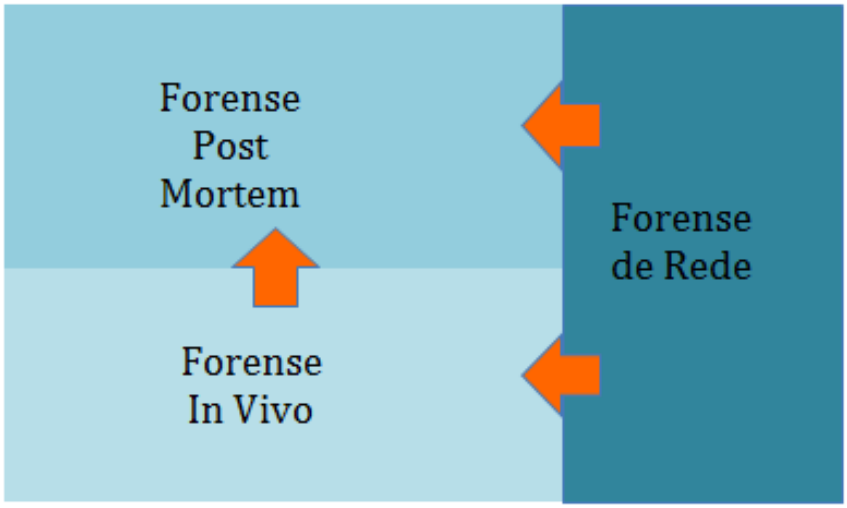
Conforme Costa (2003), a computação é empregada em grandes empresas e desde a década de 60 os crimes já aconteciam. Na década de 80, surgia o primeiro vírus de computador na história de computação, e daí para frente os vírus tornaram-se cada vez mais sofisticados e perigosos. Uma vasta nomenclatura foi criada para diferenciar os tipos de vírus. Diversos programas de computadores foram criados para “impedir” que dados fossem causados.

Devido ao surgimento de casos que envolvem o meio computacional, tornou-se necessário o desenvolvimento de uma nova disciplina forense, cujo objetivo é criar metodologias e acumular conhecimentos para a aquisição, manipulação e análise de evidências digitais. A Forense Computacional é o ramo da criminalística que compreende a aquisição, prevenção, restauração e análise de evidências computacionais, que podem ser os componentes físicos ou dados que foram processados eletronicamente e armazenados em mídias computacionais (VARGAS; QUINTÃO; GRIZENDI, 2007).

Primeiramente deve-se planejar de que forma será realizada a investigação, antes de iniciar a coleta dos dados, para que não se percam as evidências sensíveis e voláteis.

A ciência forense tem produzido, ao longo dos anos, resultados que são considerados válidos e confiáveis consequentes de fato da prova pericial ser produzida a partir de fundamentação cientifica. As atividades desenvolvidas pelos especialistas na área da perícia forense podem ser compreendidas em três fases conforme ilustra a figura 7, do ponto de vista macro (MELO, 2009).

Figura 8 – Atividades operacionais da Computação Forense

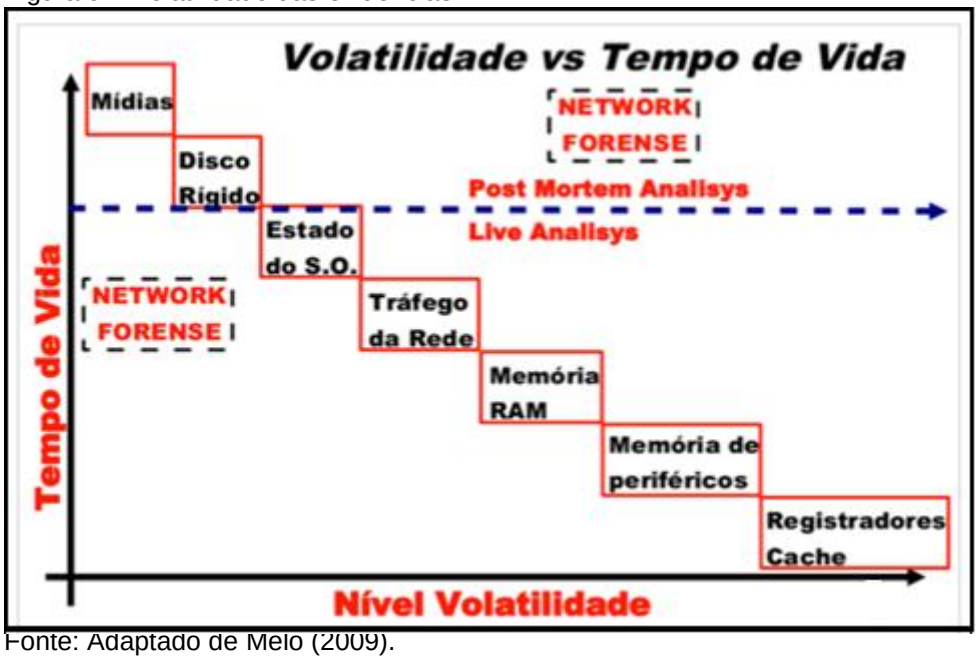


Fonte: Adaptado de Melo (2009).

Forense *post mortem* (*Post Mortem Forensics*) caracteriza-se em coletar e analisar o máximo de evidências digitais após o desligamento do computador (caso esses dados não forem necessários ou já terem sido coletados) conforme mostra a figura 8, serão coletadas informações não voláteis (fazendo uma cópia fiel) que incluem pen drive, discos rígido, entre outros. Esta metodologia não requer muitos cuidados durante a aquisição das evidências digitais (comparando com a *Live Forensics*), pois não há coleta de dados voláteis, é necessário validar a garantia de integridade dos dados por meio de funções *hash*[2]*(*MELO, 2009*)*.

[2] Uma função *hash* é qualquer algoritmo ou sub-rotina que mapeia grandes conjuntos de dados de comprimento variável, denominadas chaves, para conjuntos de dados menos de um comprimento fixo (WIKIPEDIA, 2010, tradução nossa). Disponível em: < http://en.wikipedia.org/wiki/Hash_function>.

Figura 9 – Volatilidade das evidências



Fonte: Adaptado de Melo (2009).

Forense *In Vivo* (*Live Forensics*) caracteriza-se em coletar e investigar os dados obtidos com o sistema ainda ligado e em rede, como pode ser observado na figura 6. Este método de trabalho é o único que autoriza a obtenção de dados voláteis, tendo em conta os processos que são executados no sistema, como por exemplo, arquivos temporários, dados da memória principal, entre outros. Forense em rede (Network *Forensics*) consiste na coleta e análise de dados de atividade de rede, capturados do servidor que registrem informações correlacionadas ao Incidente de Segurança em curso, objetivando identificar ações efetuadas e recuperar arquivos transferidos que são devidamente analisados na Forense *Post Mortem* e posteriormente se tornar dados periciais relevantes (MELO, 2009).

A seguir, serão apresentadas algumas metodologias de investigação forense onde, uma delas, foi usado para o desenvolvimento deste trabalho.

3.1 METODOLOGIAS FORENSES E INVESTIGATIVAS

Ao iniciar o procedimento de perícia em um equipamento questionado, o perito deve fazer a escolha de qual metodologia será empregada em seu trabalho: tem a *Live Forensics* ou a *Post Mortem Forensics,* que foram abordados anteriormente, ou ainda, em alguns casos, usam-se ambas (CARRIER, 2006).

3.1.1 Metodologia Digital Forensics Research WorkShop (DFRWS)

A Metodologia foi elaborada por Gary Palmer no primeiro Digital Forensics Research WorkShop (DFRWS), está compreendida em sete etapas (BERTOGLIO, 2008):

a) **identificação**: esta fase infere sobre o método do qual o perito é informado sobre possíveis incidentes;
b) **preservação**: fase onde são asseguradas a integridade e o estado das evidências.
c) **coleta**: fase onde são feitas a extração e a coleta de itens individuais ou em grupos, adotando métodos específicos e ferramentas usadas pelo perito para aquisição de evidências.
d) **exame**: realizam-se exames cuidadosos dos itens e suas características e atributos. Esta fase tem como propósito o uso de ferramentas e a respetiva extração das evidências para exames detalhados, sem o intuito de formar conclusões sobre o caso;
e) **análise**: são feitas analises de todas as evidências que foram identificadas desde o início da investigação, a fim de expandir uma série de conclusões em relação às provas apresentadas;
f) **apresentação**: nesta etapa o perito de apresentar os fatos de forma organizada, clara e concisa e objetiva.
g) **decisão**: fase contemplada pela etapa anterior, de apresentação de laudos periciais para o tribunal e onde o perito delimita as suas considerações sobre o caso.

3.1.2 Metodologia de Reith, Carr and Gunsch

A metodologia proposta por Reith, Carr e Gunsch (2002), também conhecida como *Abstract Digital Forensics Model,* possui algumas características semelhantes a da DFRWS. Ambas apresentam etapas similares presentes nas metodologias, que são a de preservação, coleta, exame e apresentação, sendo que fornece suporte à preparação de ferramentas e uma dinâmica formulação de abordagens investigativas. A estrutura da metodologia é baseada em nove etapas, que são citadas abaixo (BARYAMUREEBA; TUSHABE, 2004):

a) **identificação**: reconhece e avalia o incidente;
b) **preparação**: fase da preparação das ferramentas, técnicas, monitoração de autorizações, mandados de busca e suporte;
c) **estratégia de abordagem**: são desenvolvidas procedimentos estratégicos a fim de maximizar a coleta de evidências não infectadas, ao ponto de minimizar o impacto para a vítima;
d) **preservação**: envolve o afastamento e proteção do estado físico e digital das evidências;
e) **coleta**: fase detalhada da gravação da cena do crime e duplicação das evidências, fazendo uso de procedimentos aceitos e padronizados;
f) **exame**: busca aprofundada e sistemática das provas relativas à suspeita do crime;
g) **análise**: envolve a reconstrução dos fragmentos de dados e elaboração de conclusões baseadas nas evidências encontradas;
h) **apresentação**: envolve o resumo das considerações finais;
i) **devolução** das evidências: garantia de que a propriedade física seja devolvida ao proprietário.

3.1.3 Metodologia SOP

Metodologia *Standard Operating Procedures* (SOP), criada pelo *Scientific Working group on Digital Evidence* (SWDGE) que é o representante norte-americano na *Organization on Computer Evidence* (IOCE). Objetivando a criação de um documento de amostra de trabalho que as organizações podem utilizar como um modelo para reproduzir sua própria documentação de Procedimentos Operacionais Padrão, e é constituída por seis etapas de acordo com (SWGDE, 2012, tradução nossa):

a) **coleta da prova:** a partir do responsável pela investigação, consultar que ferramentas deve-se levar para o local da ocorrência. Sempre que for impossível remover as evidências do local, promover uma cópia ou imagem dos dados seguindo os procedimentos locais. Os suspeitos devem ser afastados do local do crime depois de certificado que os mesmos não estão em posse de provas em potencial;

b) **identificação:** Nesta etapa deve-se fazer o levantamento das informações relevantes ao crime e a identificação de todo o hardware e software do computador a ser examinado;
c) **preparação do equipamento** - equipamento aqui é referenciado como sendo o hardware e software utilizados pelo examinador para que se efetue a imagem forense e posteriormente a análise. Preferencialmente, devem ser usados equipamentos padronizados;
d) **imagem forense** - documentar o estado atual da prova, devem-se tomar medidas para que os itens não sejam expostos. Hardware ou Software devem ser utilizados para garantir que a prova não seja alterada, e as mídias devem ser devidamente preparadas para receber a cópia forense para assegurar o não entrelaçamento dos dados;
e) **exame/análise** - para análise devem-se considerar a urgência com que o requisitante necessita da informação, que exames forenses podem ser executados na evidência, quais os itens que oferecem melhor escolha em termos probatórios. Realizar a análise diretamente na evidência coletada não é seguro, os exames devem ser conduzidos em cópias forenses;
f) **documentação** - a documentação de manipulação de provas deve incluir cópia da autorização judicial, cadeia de custódia, contagem das provas a serem periciadas, dados sobre a condição da evidência após ser recebida pelo examinador, uma descrição das evidências, e comunicações com o caso. A documentação do exame deve em casos específicos, conter detalhes que permitam outro perito forense competente na mesma área de especialização ser capaz de identificar o que foi feito e chegar aos resultados de forma independente;

g) **relatórios** - os relatórios deverão satisfazer aos requisitos do examinador, estes deverão abordar as necessidades do solicitante, com o objetivo de fornecer ao leitor todas as informações relevantes de forma clara e concisa;

h) **revisão** - deve-se ter uma política escrita contendo os protocolos para revisão técnica e administrativa.

3.2 ALGUNS LIVES CDS PARA PERÍCIA FORENSE

Um live CD roda um sistema operacional sobre um ramdisk, isto é, um disco virtual é criado usando parte da memória RAM. O live CD possibilita fazer o uso de um sistema operacional sem ter a necessidade de este estar instalado, dependendo apenas de requisitos básicos como um drive CD e não exigindo muita memória (MORIMOTO, 2005).

Nos próximos capítulos são apresentados alguns dos sistemas operacionais que funcionam com live CD.

3.2.1 Deft 7.2

É uma distribuição para perícia composta de um GNU/Linux e DART (Digital Advanced Response Toolkit) suíte dedicada às atividades digital forensics3 e intelligence4. A primeira versão do Linux DEFT foi introduzido em 2005, graças ao Curso de Computação Forense da Faculdade de Direito da Universidade de Bolonha na Itália, a figura 9 ilustra o ambiente de trabalho da mesma (FRATIPIETRO; ROSSETI, 2012, tradução nossa).

Figura 10 – DEFT distribuição para perícia forense

Fonte: DEFT (2012).

Possuí um número considerável de aplicações Linux e scripts, também apresenta a suíte DART contendo aplicativos do Windows (tanto open source e de código fechado). É capaz de certificar a integridade das estruturas de arquivos e metadados sobre o sistema a ser investigado, a fim de proporcionar uma análise exata. Também analisa de forma confiável o sistema que está sendo investigado, sem alterar, excluir, substituir ou alterar os dados de outra forma. Existem certas características inerentes ao DEFT que minimizem o risco de alterar os dados submetidos a análise. Algumas características (FRATIPIETRO; ROSSETI, 2012, tradução nossa):

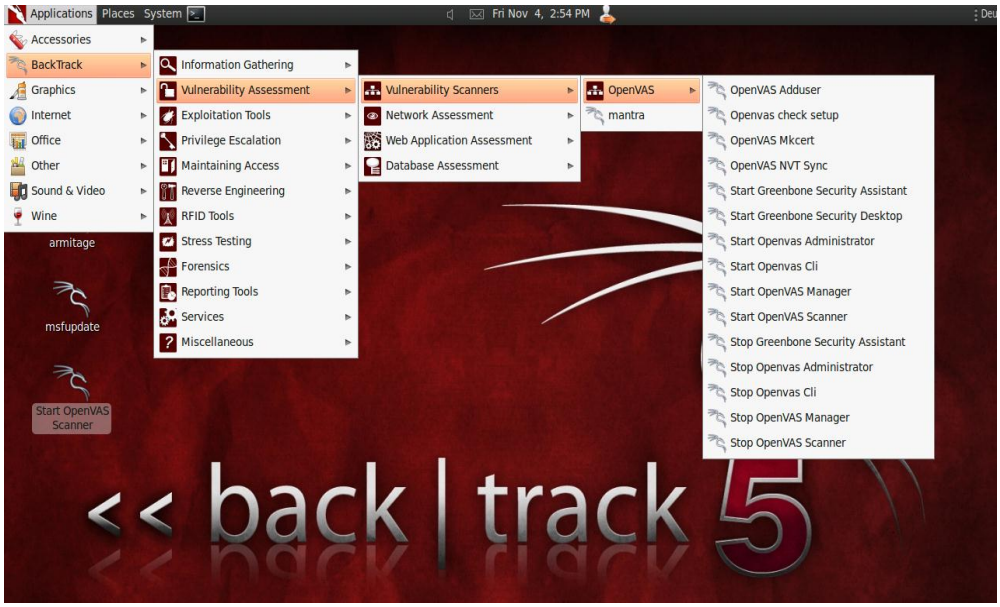
a) o sistema não usa partições swap na sua inicialização;
b) na inicialização do sistema, não monta partições automaticamente;
c) não automatiza qualquer processo durante a análise de provas;
d) não sofre alteração de dados na obtenção sobre IP.

3.2.2 Backtrack 5

É uma distribuição de segurança Linux que contém um ótimo conjunto de ferramentas necessárias para executar uma avaliação completa de segurança de sistemas, redes e aplicações. É importante realçar que pode ser configurado de

diferentes formas, como a criação de um Live CD ou montar um drive USB de inicialização e executá-lo em um ambiente vivo, também é possível instalar em uma máquina virtual (VM) ou ser instalado diretamente em um disco rígido e inicializar a ele como o sistema operacional principal. Portanto, cada método tem as suas vantagens e desvantagens, mas, em casos de realizações constantes de avaliações e testes é recomendável que se crie um BACKTRACK 5 por meio de uma máquina virtual, como pode ser observado na figura 11(HACKING9-TEAM, 2012, tradução nossa).

Figura 11 – BACKTRACK 5



Fonte: HACKING9-TEAM (2012).

3.3 KIT DE FERRAMENTAS PARA EXAME FORENSE COMPUTACIONAL

Os investigadores precisam de ferramentas de software para visualização de arquivo, imagens de disco, arquivos de descompactação, identificação de arquivos conhecidos, realizando pesquisas de cadeia e acessar os metadados do arquivo (BANSOD, 2009, tradução nossa).

Existem várias ferramentas que permitem realizar uma análise forense em sistemas de arquivos NTFS – arquivos excluídos, ocultos e segmentados auxiliando o perito, como: analyzeMFT, Digital Forensics Framework, Autopsy, Forense Tool Kit, Encase, recoveryMyFiles, FDTK, entre outras ferramentas que não são voltadas para perícia forense como: iCare Data Recovery Free, DiskDigger, Lazesoft Data

Recovery, Power Data Recovery, Recuva, Easeus Deleted File Recovery, Wise Data Recovery, Glary Undelete, Data Recovery Wizard Free, NTFS Undelete.

Para o presente trabalho foram escolhidas ferramentas *open source*, isto é, softwares disponibilizados sob licença de código aberto, e softwares livres, se bem que não tenham disponibilizado o seu código fonte, estas se encontram gratuitamente distribuídas. É vantajoso trabalhar com software livre, por uma única razão, o baixo custo de aquisição. Porém, segundo Argolo (2005) os benefícios de se trabalhar com softwares de código aberto são:

a) **baixo custo:** softwares sob uma licença de código aberto são usualmente são grátis, ou o custo de aquisição é muito sumaria;
b) **segurança:** a fluente disponibilidade do seu código fonte para os usuários, denota um melhoramento regular;
c) **continuidade:** mesmo que os responsáveis do software original deixem de o atualizar, esta pode ser feita pela comunidade, sendo que, o código fonte poderá ainda ser usado em outros projetos;
d) **flexibilidade:** o código fonte do software pode ser alterado, de acordo com a satisfação do seu usuário, e características específicas.

As ferramentas escolhidas e que na qual serão melhor apresentadas, são: iCare Data Recovery Free, DiskDigger, RecoveryMyFiles, Lazesoft Data Recovery, Power Data Recovery, Recuva, Easeus Deleted File Recovery, Wise Data Recovery, Glary Undelete, Data Recovery Wizard Free, Digital Forensics Framework , Autopsy. Todas elas são gratuitas, algumas possui o seu código fonte disponível e são usadas por peritos durante as suas pesquisas.

Alguns softwares também considerados importantes, poderão, se surgir alguma chance, ser usadas no presente trabalho, são elas:

a) **FDTK:** a distribuição visa realizar perícia forense, coletar e analisar os dados. Baseada em Ubuntu e podemos encontrar mais de 100 ferramentas que guiaram o perito forense a realizar todas etapas de uma investigação forense (NEUKAMP, 2011, tradução nossa).

3.3.1 iCare Data Recovery Free

A primeira ferramenta a ser usada foi a iCare [3]Data Recovery Free, programa simples e gratuito de recuperação de informações (dados), apresenta uma forma fácil e prática de recuperação de arquivos apagados do HD (disco rígido), *pendrive*, entre outros. Permite recuperar arquivos excluídos acidentalmente, excluídos da lixeira, excluídos por vírus, partição apagada, acidente de software, entre outros. Recupera qualquer arquivo como fotos, documentos, mp3, funciona com qualquer tipo de mídia de armazenamento, cartão SD, camera digital, entre outros, figura 11 ilustra a ferramenta (ICARERECOVERY, 2003, tradução nossa).

Figura 12 – Tela inicial da ferramenta iCareRecovery

Fonte: iCareRecovery (2013).

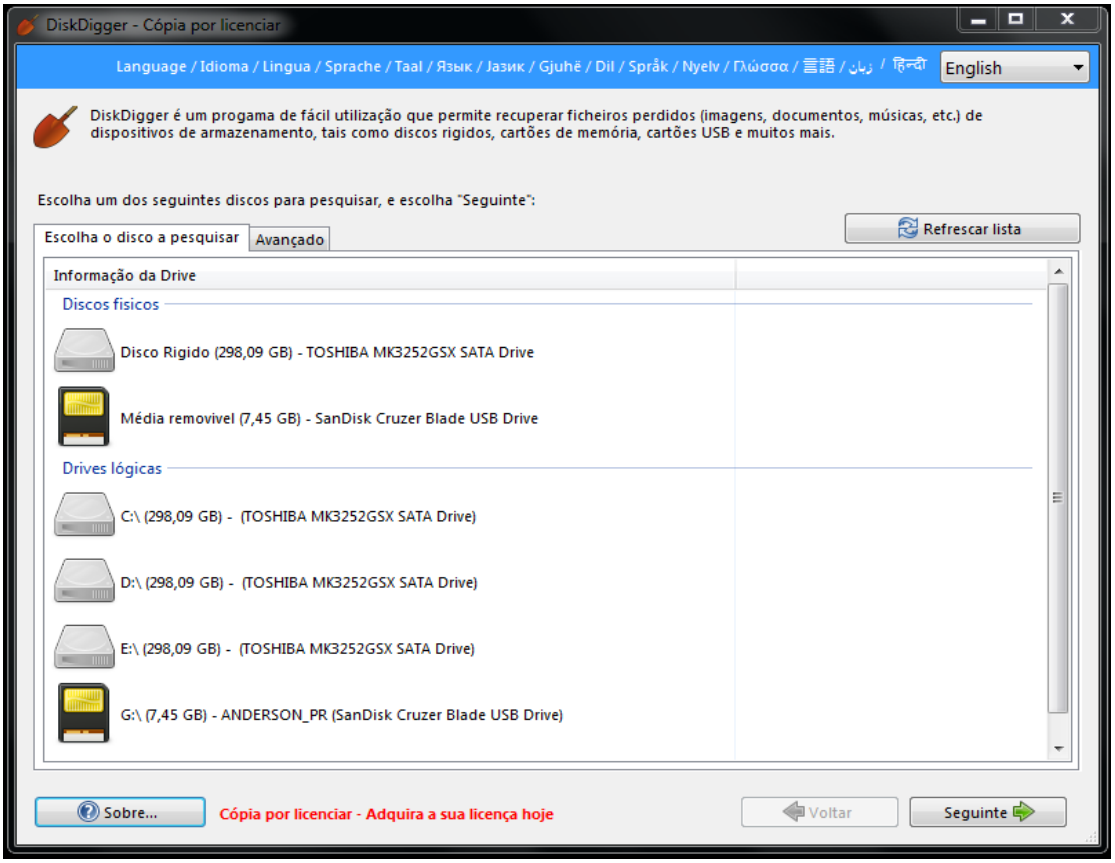
3.3.2 DiskDigger

DiskDigger[4] é um programa capaz de recuperar arquivos perdidos a partir do disco rígido, cartões de memória, *drives flash* USB e *pendrives*. Ele pode recuperar documentos (DOC, DOCX, XLS, PPT, PDF, entre outros), fotos (JPG,

[3] http://www.icare-recovery.com/about-us.html
[4] http://diskdigger.org/

PNG, GIF, BMP, entre outros), musicas (MP3, WMA, M4A, WAV, entre outros), vídeos (WMV, MOV, 3GP, RMVB, MKV, MPEG, entre outros) e muitos outros formatos de arquivos. O software tem dois (2) modos de operação “Pesquisa funda” e “Pesquisa Profunda”. O primeiro faz uma verificação simples e rápida, envolvendo filtragem pelo nome e tamanho dos arquivos recuperados, porem a segunda opção faz a verificação e digitalização do HD inteiro, vestígios de determinados, o que aumenta as chances de recuperação de informações excluídas há mais tempo, por outro lado, é bem mais demorado, como observa-se na figura 12 (DISKDIGGER, 2013, tradução nossa).

Figura 13 – Tela inicial da ferramenta DiskDigger



Fonte: DiskDigger (2013).

3.3.4 RecoveryMyFiles

RecoveryMyFiles ou recuperação de dados em português, é um software de recuperação de arquivos apagados a partir da lixeira do Windows, perdidos ao ser formatado ou em uma reinstalação de um sistema operacional, disco rígido, ou removidos por infecção de vírus, infecção por *trojan* que é o mais conhecido, ou por encerramento indevido do sistema ou mesmo por falha de um software, que pode ser visualizado na figura 13. É compatível com Windows (2003, XP, Vista, Windows 7, Windows 8) e trabalha com FAT 12, FAT16, FAT 32 + sistemas de ficheiros do Mac. (RECOVERMYFILES, 2013, tradução nossa).

Inclui um apoio específico para mais de 200 tipos de arquivos. Listagem das características fortes que a ferramenta apresenta para os arquivos (RECOVERMYFILES, 2013, tradução nossa):

a) Recupera arquivos mesmo tendo esvaziado a lixeira;
b) Recupera arquivos após uma formatação de forma acidental;
c) Recupera discos com falhas;
d) Resgata arquivos após falha de particionamento;
e) Recupera documentos, fotos, música e e-mail;
f) Recupera *FAT*, *exFAT*, *NTFS*, *HFS*, *HFS +.*

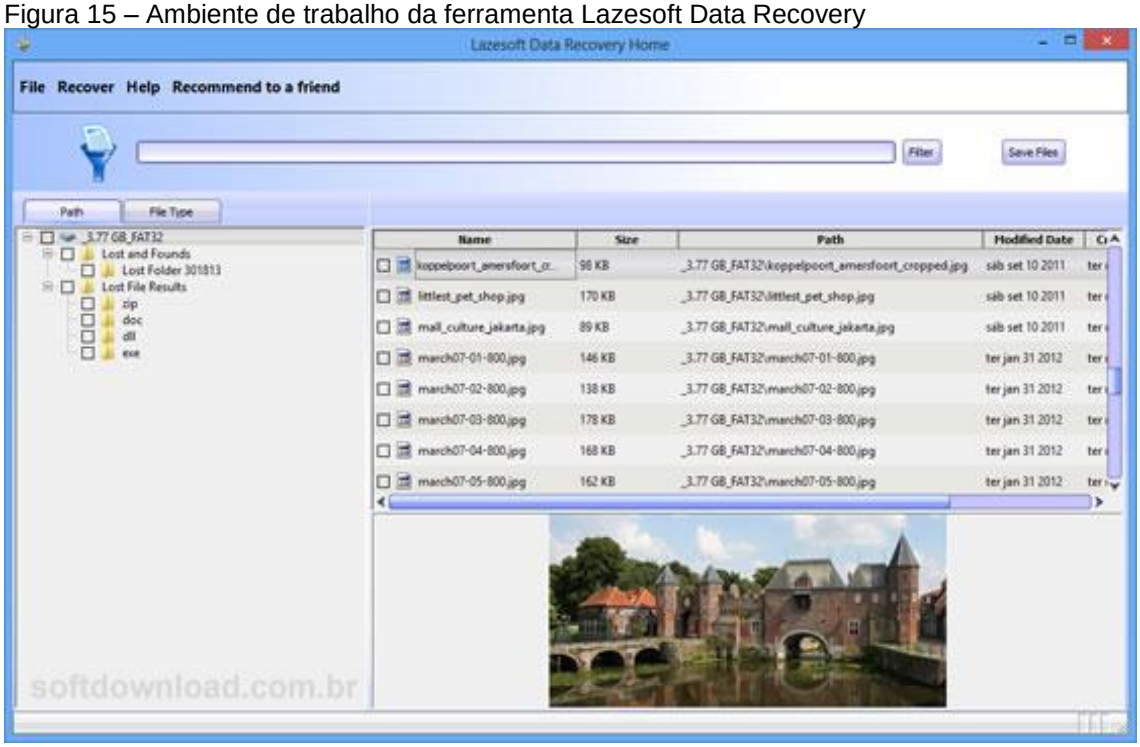
Figura 14 – Ambiente de trabalho da ferramenta RecoveryMyFiles

Fonte: RecoveryMyFiles (2013).

3.3.4 Lazesoft data recovery

A ferramenta de recuperação Lazesoft concede aos usuários domésticos e à empresas, soluções completas para recuperar arquivos apagados ou perdidos devido à uma reformatação ou corrupção de um disco rígido, vírus ou infecção de Trojan, por encerramento inesperado do sistema ou por falha de um software. Com uma forma fácil de usar a interface e o mais potente software de recuperação e dados, pode-se usar a ferramenta para recuperar seus dados, pode pre-visualizar os arquivos apagados enquanto a varredura estiver sendo operada (LAZESOFT, tradução nossa, 2012).

Figura 15 – Ambiente de trabalho da ferramenta Lazesoft Data Recovery



Fonte: Lazesoft (2012).

No próximo capítulo são apresentados alguns trabalhos compreendidos em propósitos semelhantes à presente pesquisa.

4 TRABALHOS CORRELATOS

Ao longo dos estudos objetivando esta pesquisa, seja na proposta ou no seu desenvolvimento, foram investigados alguns trabalhos com propósitos semelhantes, porém com o foco diferente. Abaixo, pode-se observar a descrição de alguns trabalhos escolhidos, envolvendo a perícia forense computacional.

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

O primeiro trabalho analisado para a pesquisa foi apresentado na Universidade do Extremo Sul Catarinense – Unesc como trabalho de conclusão de curso, foi elaborado por Ramiro Dimer com o objetivo de aplicar técnicas computacionais forenses de duplicação pericial, recuperação de dados para a busca e análise de evidências em sistemas de arquivos NTFS.

Ele pode ser visualizado no seguinte endereço: http://www.kiron.unesc.net/tcc/arquivos/trabalhos/151.pdf

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

O segundo trabalho estudado para a pesquisa foi apresentado no Centro Universitário Feevale como trabalho de conclusão de curso, foi elaborado por Daniel Bertoglio, tem como objetivo estudar definições e características da análise forense computacional, propondo uma metodologia para coleta de indícios para um ambiente Windows.

Ele pode ser visualizado no seguinte endereço: http://tconline.feevale.br/tc/files/0001_1690.pdf

4.3 ANÁLISE DE FERRAMENTAS FORENSES DE RECUPERAÇÃO DE DADOS

O terceiro trabalho estudado para a pesquisa foi apresentado na Faculdade de Tecnologia de Jão Pessoa como trabalho para obtenção de título de Especialista em Segurança da Informação, elaborado por Josilene Nascimento, teve como proposito a análise de ferramentas de recuperação de dados forenses com o objetico de estabelecer como e em que cenários elas podem ser usadas, foi usado o tipo de análise forense *Post Mortem*.

Ele pode ser visualizado no seguinte endereço: http://www.fatecjp.com.br/revista/tcc/seginf01.pdf

4.4 FORENSE COMPUTACIONAL: FERRAMENTAS E METODOLOGIAS PARA RESPOSTA A INCIDENTES, ESTUDO DE CASO “HELIX 3”

O quarto trabalho analisado para a pesquisa foi apresentado na Universidade do Extremo Sul Catarinense – Unesc como trabalho de conclusão de curso, foi elaborado por Aguinaldo Cristiano, tem como objetivo analisar ferramentas e metodologias para respostas a incidentes computacionais usando como objeto de estudo a ferramenta Helix 3, a metodologia usada para realização da análise no caso de estudo foi a SOP. Onde de segundo Cristiano (2011) foram encontradas evidências bastante sólidas, que incriminam o suspeito, nomeadamente arquivos de texto, imagens e páginas de Internet salvas.

5 ESTUDO DE CASO DE PERÍCIA FORENSE EM ARQUIVOS EXCLUÍDOS, OCULTOS E SEGMENTADOS EM UMA PARTIÇÃO NTFS

No presente capítulo será apresentado o estudo de caso na obtenção de avaliação de documentação da perícia forense computacional em arquivos na partição NTFS, bem como a parte prática do projeto de pesquisa, objetivando buscar uma análise digital, fazendo a demonstração e a utilização das ferramentas forenses e não só, o conhecimento adquirido na teoria, enfocando a busca, coleta e análise de evidências em ambientes NTFS.

Sendo assim, o presente estudo de caso foi executado em um ambiente controlado em um laboratório de uma instituição de ensino na região de criciúma. Atualmente a instituição comporta uma estrutura com mais de 25 laboratórios de informática de grande porte com no máximo 24 máquinas por sala e, seis (6) laboratórios de pequeno porte com no máximo 12 computadores.

Para ter acesso às máquinas disponíveis, com Internet, que na qual são reservados para os acadêmicos da comunidade interna (não só do curso de Perícia), os mesmo devem ter em mãos o código de matrícula que é acompanhado da senha no momento em que for efetuar o login[5].

O controle de acesso às máquinas disponíveis em cada laboratório da instituição, visando a sua segurança, é feita pela coordenação dos laboratórios de Informática que é responsável por utilizar uma política de segurança apropriada ao ambiente pedagógico, o mesmo é aplicada para o uso de Internet. Os sites estão organizados por categoria, portanto nem todos os sites estão habilitados a serem acessados, de acordo com o padrão dos responsáveis, se por acaso algum aluno ou professor quiser acessar um site que não esteja dentro dessa categoria, o bloqueio do mesmo é efetuado. Entretanto, existem algumas restrições regidas pelas Normas de Utilização dos Laboratórios no Departamento de Tecnologia que encontram-se fixadas em cada laboratório de informática.

Escolheu-se de forma aleatória dois laboratórios: os laboratórios 1 e 2 do Bloco A. Além disso, reservou-se 5 computadores em cada sala para serem devidamente analisados. Neste contexto, é importante ressaltar que a forma correta de se fazer uma perícia forense neste tipo de caso, é analisar um-a-um os

[5] Login é o ato de logar-se na rede informando seu nome de usuário e senha (MORIMOTO, 2003).

computadores da instituição. Por esta razão, e, por se tratar de uma demonstração de casos, optou-se por escolher um modelo de todos os computadores.

Dessa forma, foi realizada uma simulação com este trabalho objetivando fazer menção em quais benefícios poderão ser obtidos aplicando este estudo à perícia forense computacional nos seguintes casos:

a) arquivos excluídos;
b) arquivos ocultos;
c) arquivos segmentados.

Para facilitar a compreensão das fases realizadas, simula-se a seguinte ocorrência:

a) Supõe-se que o fulano de tal (usuário qualquer), usando uma das máquinas dos laboratórios da UNIP (nome fictício) tenha excluído, ocultado ou corrompido um arquivo importante de forma acidental ou propositada, sendo que o mesmo não havia feito um Backup, isto é, uma cópia de segurança desse arquivo. Qual o procedimento a ser seguido para a sua recuperação? Será que é possível recuperar este mesmo arquivo perdido (por engano ou não)? Será que é possível recuperar informações de um disco rígido formatado? E ainda, como recuperar uma partição apagada indevidamente?.

Em seguida, foi descrito os conceitos importantes a todo sistema de metodologia empregados neste trabalho.

5.1 METODOLOGIA

Para realizar este estudo, foi feito um levantamento bibliográfico em livros, relacionados a crimes digitais em ambientes NTFS, por meio de Internet em banco de dados, como trabalhos científicos, trabalhos de monográfia, dissertações, artigos de forma a obter informações suficientes sobre tema e, quais procedimentos ou metodologias serão aplicados e/ou investigadas no momento em que for feita a perícia. Parte da bibliografia usada neste trabalho foi traduzida da língua inglesa.

Estudo das ferramentas forenses Autopsy, Digital Forense Framework (DFF), Forense Tool Kit (FTK), estudo de outras ferramentas de recuperação de arquivos excluídos e segmentados utilizadas no trabalho, 5.2, a fim de serem aplicados em dispositos de armazenamento com sistemas de arquivos NTFS.

Em seguida, a aplicação de tecnicas forenses em uma partição formatada com capacidade de *29.5 GB*. Escolheu-se a capacidade de armazenamento reduzida das partições, sob o critério de redução de tempo na recuperação das imagens durante o decorrer do trabalho.

Primeiramente chegou-se a fazer a análise na partição formatada de *29.5 GB* visando a busca por informações perdidas, o que torna a pesquisa um pouco mais demorada devido a sua capacidade de armazenamento. Porém, por se tratar de um estudo de caso em ambiente controlado, optou-se por trabalhar com um dispositivo de armazenamento menor, um *pendrive*, com capacidade de oito Gigabyte. Formatou-se a mesma para o sistema de arquivos NTFS, sendo o objetivo deste trabalho, trabalhar apenas com esse sistema de arquivos.

É importante salientar que o *Dos* lê (reconhece) apenas FAT32 do *MS-Dos 7* ou superior, não lê NTFS. Algumas versões mais antigas do Windows não lê essa partição. Existem muitas vantagens em se utilizar NTFS sob o FAT32, sendo que o NTFS oferece suporte a segurança de dados, suporte a compreenção de dados, isto é, compactação de dados e suporte para arquivos superior a quatro Gigabyte, entre outros.

Por final realizou-se uma simulação pericial com o objetivo de demonstrar mediante a um acontecimento o uso de alguns softwares de perícia e de recuperação informações, e metodologias na busca evidências.

5.2 ESTUDO DE CASO

Nesta fase será apresentado um estudo de caso, auxiliando, sob meios práticos na percepção de quando e como deve-se usar as ferramentas forense e, alem disso, qual a confiabilidade que as mesmas propõem alcançar tendo em conta o seu escopo.

5.1.1 Metodologia forense

O presente estudo de caso foi proposto pelo especialista forense Brian Carrier. Montado pelo mesmo e simula um ambiente real favorável para análise.

Trata-se da criação de um caso e uma imagem forense para teste, apresentado em 29 de fevereiro de 2004. Esta imagem, Raw (dd), é um sistema de arquivos NTFS com tamanho de 6 MB com oito arquivos apagados, dois diretórios apagados e um fluxo de dados alternativo também apagado. Os arquivos variam de arquivos residentes, arquivos de *cluster* único e vários fragmentos. Com suas Estruturas de dados modificadas para impedir o processo de recuperação dos mesmos. Eles foram craidos no Windows XP e posteriormente excluídos no XP. A imagem foi liberada sob a General Public License (GPL)

O autor aponta como proposito do caso de estudo 11 etapas e também uma tabela onde encontram-se os arquivos que devem ser recuperados, seus tamanhos e seus respetivos MD5:

a) Consegue observar qualquer um dos nomes de arquivos excluídos? Quais?
b) Consegue recuperar o arquivo res1.dat? Ele tem o mesmo MD5?
c) Consegue recuperar o arquivo sing1.dat? Ele tem o mesmo MD5?
d) Consegue recuperar a pasta3 / arquivo sing2.dat? Ele tem o mesmo MD5?
e) Consegue recuperar o arquivo mult1.dat? Ele tem o mesmo MD5?
f) Consegue recupear o mult1.dat: file ADS? Ele tem o mesmo MD5?
g) Consegue recuperar o dir1 / arquivo mult2.dat? Ele tem o mesmo MD5?
h) Consegue recuperar o arquivo frag1.dat? Ele tem o mesmo MD5?
i) Consegue recuperar o arquivo frag2.dat? Ele tem o mesmo MD5?
j) Consegue recuperar o dir1 / dir2 / frag3.dat? Ele tem o mesmo MD5?
k) As datas mostradas correspondem a de 29 de fevereiro de 2004?

O conteúdo do relátorio aprensentado por Brian pode ser observado a partir da figura 16.

Figura 16 – Tabela correspondente aos arquivos que serão recupedos

Num	MFT Entry	Name	Size	MD5	Note
1	37	\res1.dat	101	9036637712b491904cd0bfbdbe648453	Resident file (data is stored in MFT entry and not in a cluster)
2	31	\sing1.dat	780	59b20779f69ff9f0ac5fcd2c38835a79	single cluster file
3	32-128-3	\mult1.dat	3801	ffd27bd782bdce67750b6b9ee069d2ef	multiple cluster, non-fragmented file
4	32-128-6	\mult1.dat:ADS	1234	ba1b9eedb1c091ddca253d35dde8f616	multiple cluster, second data attribute (Alternate Data Stream)
5	29	\frag1.dat	1584	7a3bc5b763bef201202108f4ba128149	fragmented file
6	30	\frag2.dat	3873	0e80ab84ef0087e60dfc67b88a1cf13e	fragmented file with frag1.dat mixed in
7	33	\dir1\	1024	N/A	directory
8	36	\dir1\mult2.dat	1715	59cf0e9cd107bc1e75afb7374f6e05bb	multiple cluster, non-fragmented in deleted directory
9	34	\dir1\dir2\	1024	N/A	directory in deleted directory
10	35	\dir1\dir2\frag3.dat	2027	21121699487f3fbbdb9a4b3391b6d3e0	fragmented file in deleted directories
11	38	\dir3\sing2.dat	1005	c229626f6a71b167ad7e50c4f2fccdb1	single cluster file in a directory whose MFT entry has been reallocated (to res1.dat)

Fonte: Carrier (2004).

De acordo com o que foi o apresentado e, conforme se pode observar, pretende-se com esse estudo mostrar resultados semelhantes proposto pelo especialista, bem como recuperá-los, aplicando uma perícia com as ferramentas forenses e seguindo as normas da metodologia forense.

Existem várias metodologias forense, sendo assim surge a necessidade de se utilizar apenas uma para a realização da pericia forense computacional. Porem, na presente pesquisa tratou-se de três metodologias com algumas particularidades diferentes, tendo em conta o quesito eficiência e que são amplamente utilizadas por peritos no mundo da perícia computacional.

Várias referências existentes de utilização de metodologias, mas dentre as várias utilizadas no Brasil e que é mais aceita pela comunidade científica é a metodologia forense Standard Operating Procedures (SOP), já descrita neste trabalho e, será utilizada para o cumprimento da realização do estudo de caso, sendo que a mesma insere várias práticas metodológicas, princípios e técnicas forenses que são recomendadas pela comunidade.

Definida assim a metodologia a ser utilizada para a realização da pesquisa, a SOP, onde a mesma está compreendida em 7 etapas conforme pode-se observar na figura 12. Vale realçar que a escolha deste método se deu pelo fato de ser mais aceite em comunidades brasileiras e que, também pode, se for o caso, dar

condições de ser aceite como prova em um ambiente judicial fazendo-se acompanhar de relatórios periciais oficiais.

Figura 17 – Fluxograma da metodologia SOP

Fonte: SWGDE (2006).

Sabendo do objetivo deste trabalho, que é a de recuperação de arquivos excluidos, ocultos e segmentados em uma partição com sistema de arquivos NTFS, somente foram aplicadas as fases de coleta de prova, preparação do equipamento, imagem forense e exame/análise como rege metodologia SOP.

5.1.1.1 Análise e resultados do dispositivo para pericia forense

Na primeira fase do desenvolvimento, inseriu-se arquivos no dispositivo de armazenamento USB que antes foi devidamente formatada com sistema de arquivo NTFS. Alguns destes arquivos foram selecionados e excluídos e ocultados propositalmente, como foi suposto no estudo de caso da pesquisa. Utilizou-se algumas ferramentas forense neste momento para ser feita a análise do mesmo.

Como já foi mencionado anteriormente no trabalho, existem várias ferramentas de investigação forense e de recuperação de informações, dos quais optou-se por utilizar o kit de ferramentas forense para fazer a descrição dos casos.

Os softwares mencionados na metodologia (5.1) foram selecionados por fazerem parte do kit de ferramentas forenses das mais utilizadas no pela comunidade cientifica, como é o caso do Autopsy, e por possuírem particularidades de extrema confiança em relação a outras, sendo que também são utilizadas por peritos profissionais.

5.1.2 Coleta da Prova

Tendo conhecimento de que o caso provem de um ambiente estudo, o computador para exame já se encontrada em perfeitas condições de armazenamento, isolou-se área de trabalho, foram coletadas todas as evidências de formas a garantir a integridade das informações contidas no no dispositivo, ou seja, para que não corra nenhum tipo de risco de perda dos dados. A coleta da prova foi realizada com a ferramente forense FTK Imager.

Para que não exista nenhuma deterioração e substituição das evidências, as mesmas devem ser coletadas com a maior precaução possível, havendo atenção com os softwares a serem usados para que estes não alterem o estado nem as informações encontradas no computador.

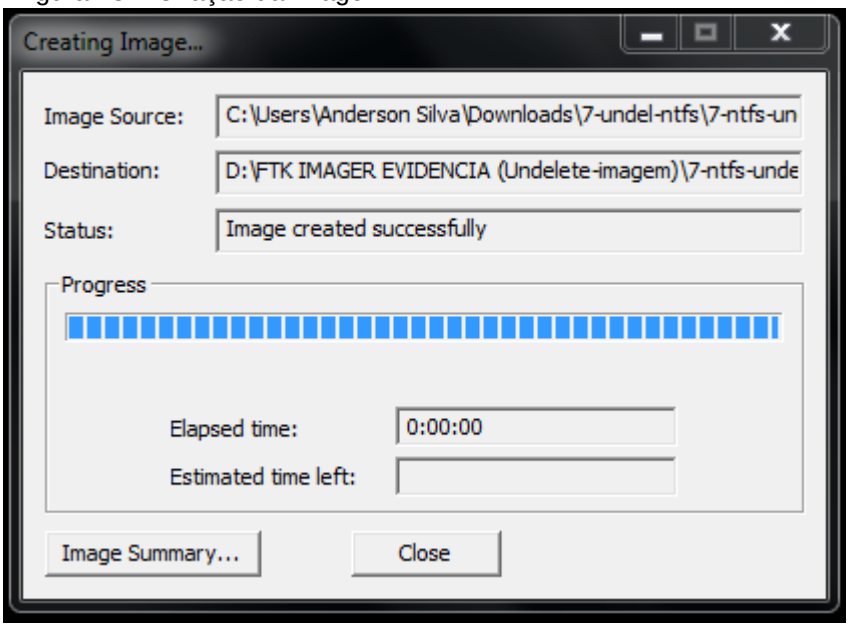
5.1.3 Preparação do equipamento

Para que fosse possível prosseguir com a pesquisa forense, foi necessário a criação de condições seguras sem o risco de perda dos dados. Assegurando-se de que o ambiente esteja seguro, as condições recaem em torno de software e harware.

5.1.4 Criação da Imagem forense

A ferramenta FTKImager foi utilizada para fazer a recolha da imagem do dispositivo em questão, e posteriormente armazenada em um disco rígido externo com a capacidade de 500 GB anteriormente formatada. Ela nos oferece quatro opções: a imagem não processada – *Raw (dd)* , *Smart Expert Witness (E01)* e a *Advanced Forensic Format (AFF).*

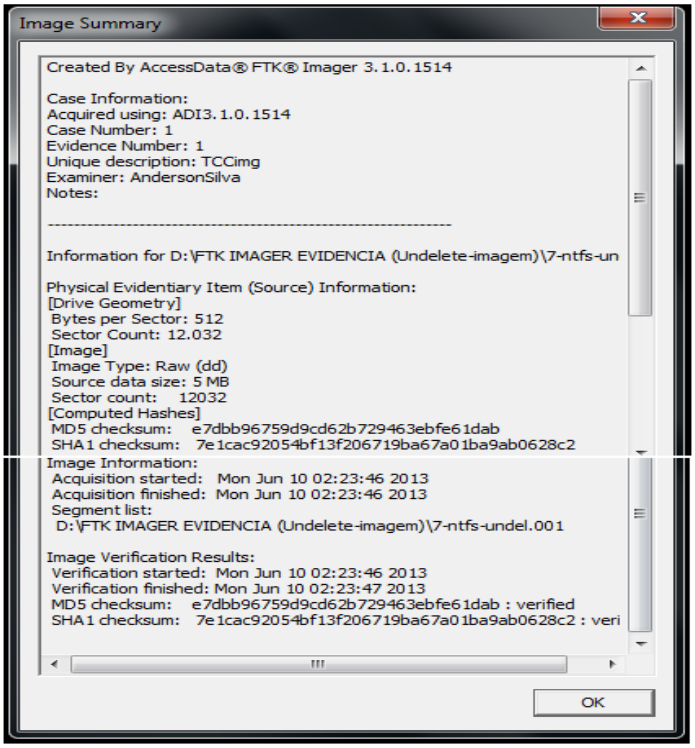
Figura 18 – Criação da imagem



Fonte: Do autor.

Optou-se por escolher a extensão padrão da ferramenta, a *Expert Witness (E01)* por ser proprietário do Encase, sendo que a mesma utiliza compatação, tratamento de erros e sem perdas. O resumo da criação dessa imagem está disponível na figura 14.

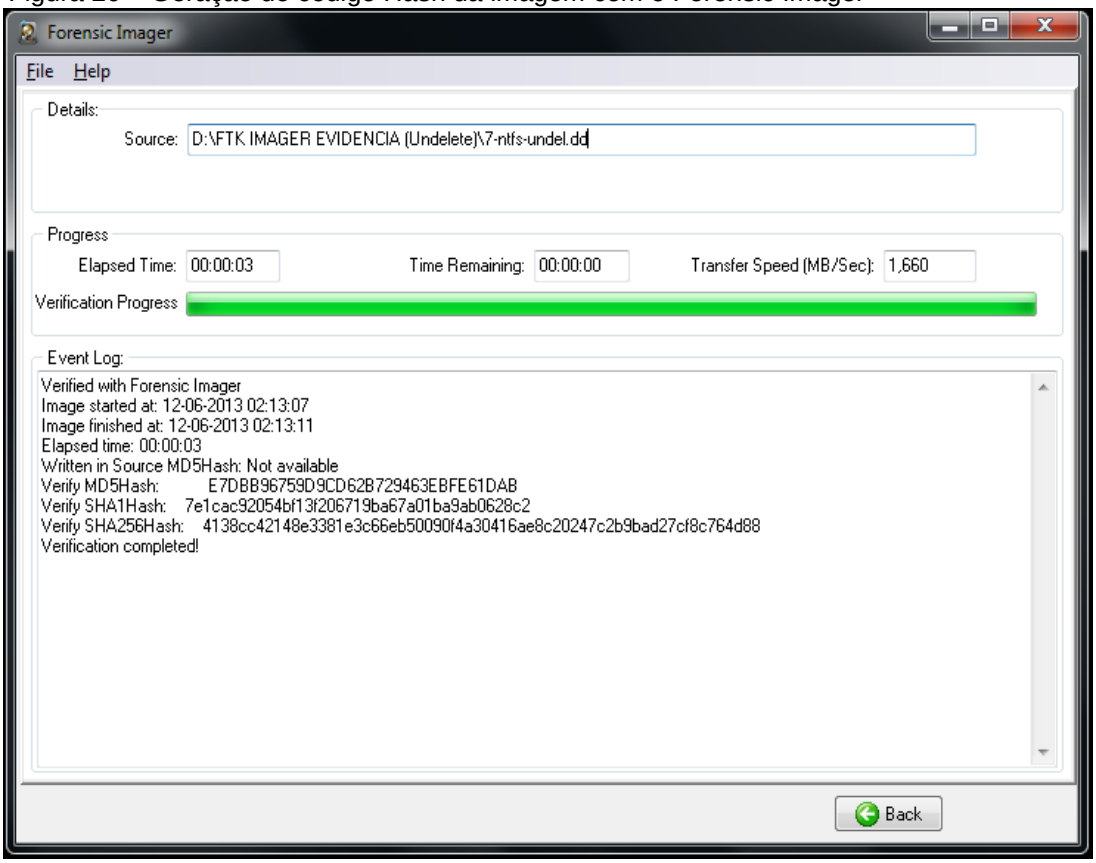
Figura 19 – Resumo da imagem criada



Fonte: Do autor.

Conforme determina a pesquisa de perícia forense, a imagem em análise, após a sua coleta, o mesmo deve passar pelo processo de geração de um código *Hash*, para este caso foi utilizado a ferramenta RecoveryMyfile, onde a mesma possui uma ferramenta interna para geração de código *hash* de um drive físico, lógico ou diretório da imagem. A figura 15 pode ilustrar melhor o mesmo.

Figura 20 – Geração do código Hash da imagem com o Forensic Imager



Fonte: Do autor.

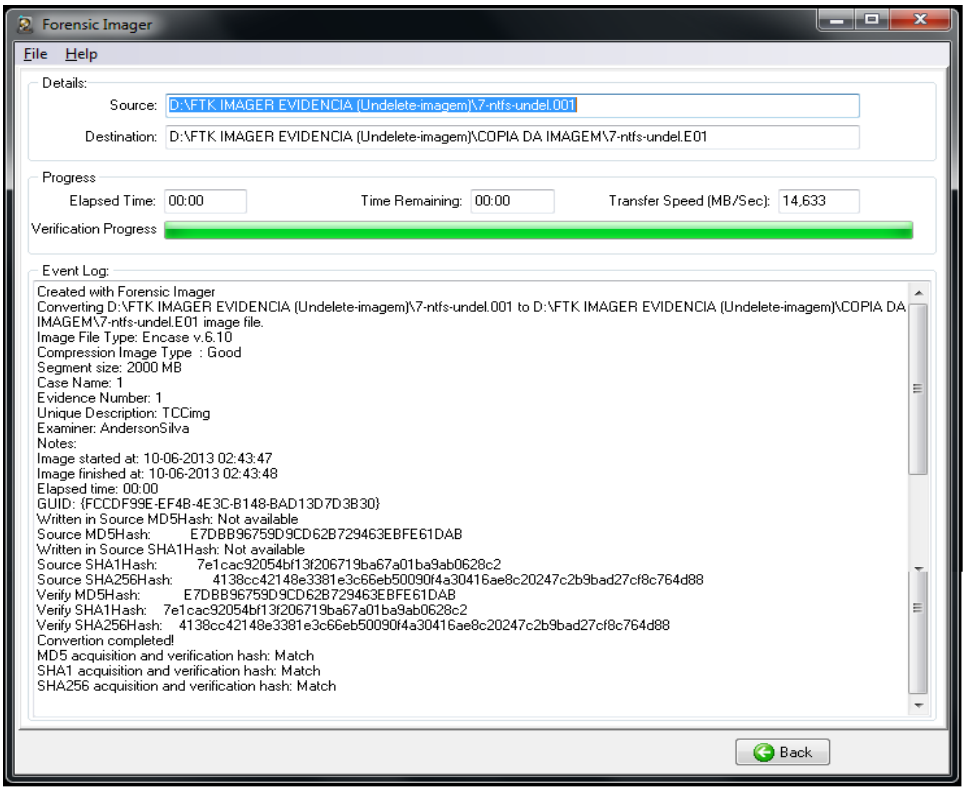
É possível verificar a partir do resumo da imagem, conforme a figura figura 14, e que na qual foi gerado um código Hash dessa imagem, figura 15 como confirmação, que a imagem não sofreu nenhum tipo de alteração e, verifica-se também que o código Hash é o mesmo da imagem inicial.

5.1.5 Exame e Análise dos dados

Para que se cumprisse a análise da imagem e, como estabelece os procedimentos propostos pela metodologia SOP, realizou-se uma duplicação da imagem, figura 21, pois, se por ventura algum imprevisto aconteça se consiga

recorrer à imagem coletada anteriormente e por conseguinte prosseguir com a pesquisa forense.

Figura 21 – Duplicação da imagem com o Forensic Imager

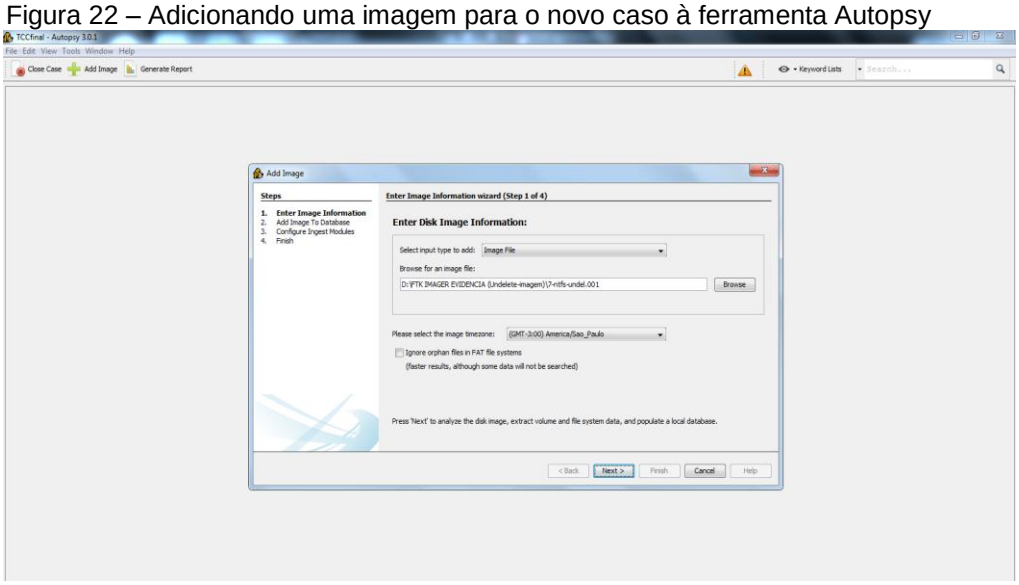


Fonte: Do autor.

5.1.5.1 Análise dos dados realizada com a ferramenta Autopsy

A ferramenta forense Autopsy é uma plataforma de análise forense digital, pode ser usada para recuperar determinados tipos de arquivos. Em algumas versões a mesma não requer instalação, porem, para esse caso específico instala-se a mesma. Com a sua versão 3.0.1, a mais recente, cria-se um novo caso e adiciona-se a imagem criada à mesma (figura 22).

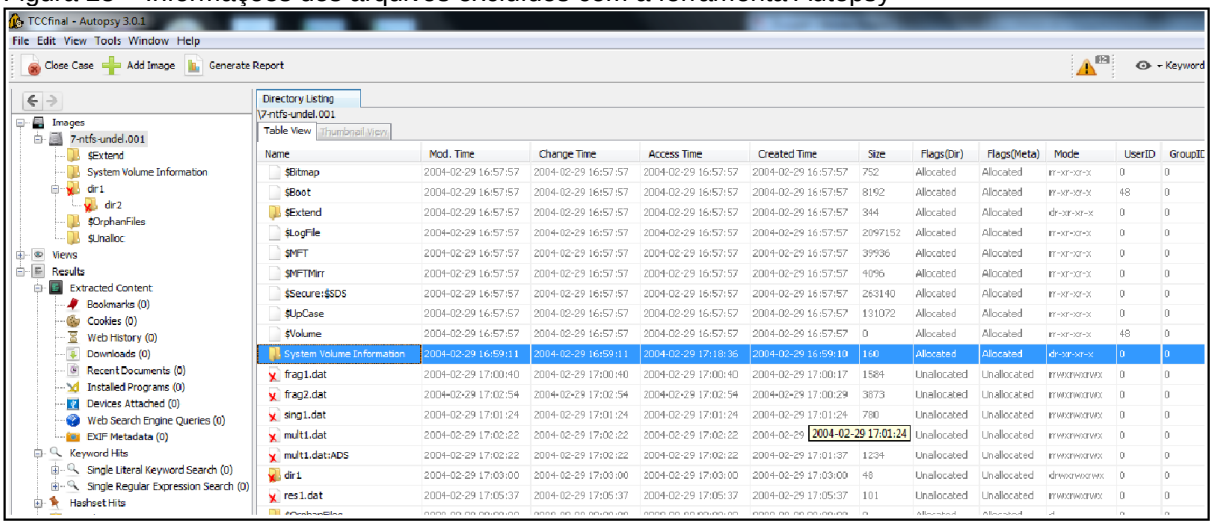
Figura 22 – Adicionando uma imagem para o novo caso à ferramenta Autopsy



Fonte: Do autor.

Com o caso já criado, conforme mostra a figura 22 e, analisando a imagem forense com a ferramenta em questão, nota-se que é possível verificar as informações correspondentemente às que são aprensentadas no estudo de caso descrita anteriormente (5.1.1). A análise trouxe as mesmas informações já inseridas, excluídas e testadas no decorrer do estudo. Conseguiu-se verificar todos os arquivos com o auxílio da mesma, arquivos que possuem os mesmos nomes que vão de encontro com o que se procura. A figura 23 oferece uma melhor compreensão no caso.

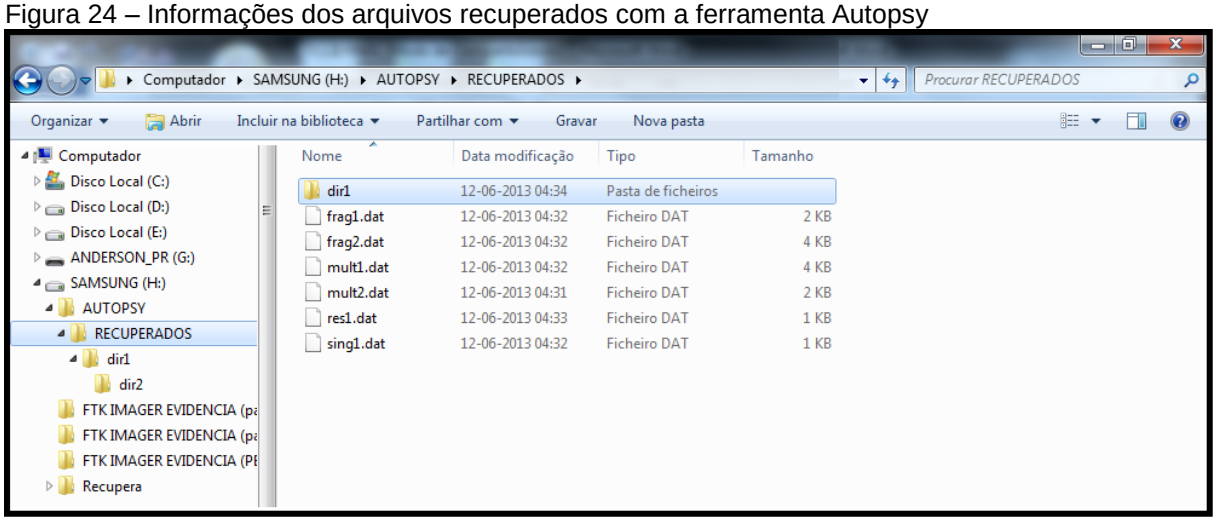
Figura 23 – Informações dos arquivos excluídos com a ferramenta Autopsy



Fonte: Do autor.

Ao final foi possível recupera-los e posteriormente salvá-los em um disco rígido externo formatado, figura 24.

Figura 24 – Informações dos arquivos recuperados com a ferramenta Autopsy



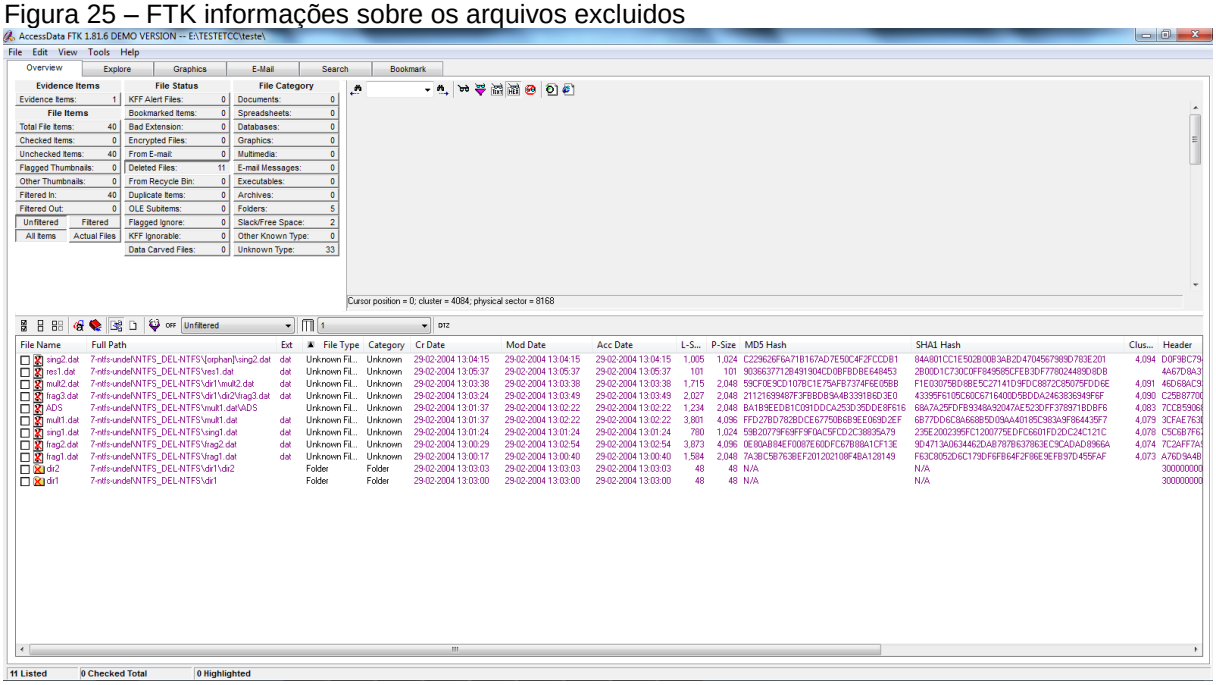
Fonte: Do autor.

5.1.5.2 Análise dos dados realizada com a ferramenta Forense Tool Kit (FTK)

Utilizando a ferramenta com a versão mais recente 1.81.6, o passo a seguir foi a criação de um novo caso e em seguida adicionou-se a imagem criada na fase anterior à mesma. No final da análise obteve-se como resultado a ilustração completa de todos os arquivos que se encontravam no dispositivo, com maior exclusividade aos excluídos.

As informações em relação aos arquivos podem ser visualizadas na figura 25, informações como a data e hora que os mesmos foram criados, acessados, modificados e alterados.

Figura 25 – FTK informações sobre os arquivos excluidos



Fonte: Do autor.

Todos os dados correspondem aos mesmos da tabela criada e aprensentada pelo autor Carrier (figura 26). Os oito arquivos apagados, os dois diretórios e os demais dados, como arquivos residentes e também os fragmentos foram recuperados e salvos com sucesso em um dispositivo formatado em NTFS.

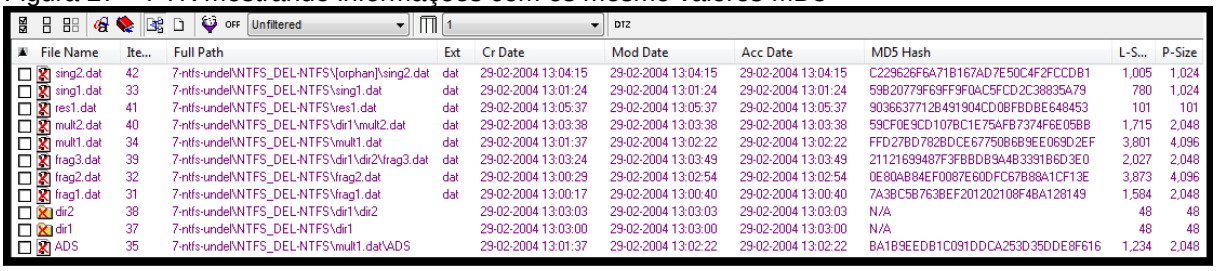
Figura 26 – Formulário dos resultados comparando MD5

These are the files that should be recovered, their sizes, and their MD5 values. (Fill in the blank results form)

Num	MFT Entry	Name	Size	MD5	Note
1	37	\res1.dat	101	9036637712b491904cd0bfbdbe648453	Resident file (data is stored in MFT entry and not in a cluster)
2	31	\sing1.dat	780	59b20779f69ff9f0ac5fcd2c38835a79	single cluster file
3	32-128-3	\mult1.dat	3801	ffd27bd782bdce67750b6b9ee069d2ef	multiple cluster, non-fragmented file
4	32-128-6	\mult1.dat:ADS	1234	ba1b9eedb1c091ddca253d35dde8f616	multiple cluster, second data attribute (Alternate Data Stream)
5	29	\frag1.dat	1584	7a3bc5b763bef201202108f4ba128149	fragmented file
6	30	\frag2.dat	3873	0e80ab84ef0087e60dfc67b88a1cf13e	fragmented file with frag1.dat mixed in
7	33	\dir1\	1024	N/A	directory
8	36	\dir1\mult2.dat	1715	59cf0e9cd107bc1e75afb7374f6e05bb	multiple cluster, non-fragmented in deleted directory
9	34	\dir1\dir2\	1024	N/A	directory in deleted directory
10	35	\dir1\dir2\frag3.dat	2027	21121699487f3fbbdb9a4b3391b6d3e0	fragmented file in deleted directories
11	38	\dir3\sing2.dat	1005	c229626f6a71b167ad7e50c4f2fccdb1	single cluster file in a directory whose MFT entry has been reallocated (to res1.dat)

Fonte: Do autor.

Figura 27 – FTK mostrando informações com os mesmo valores MD5



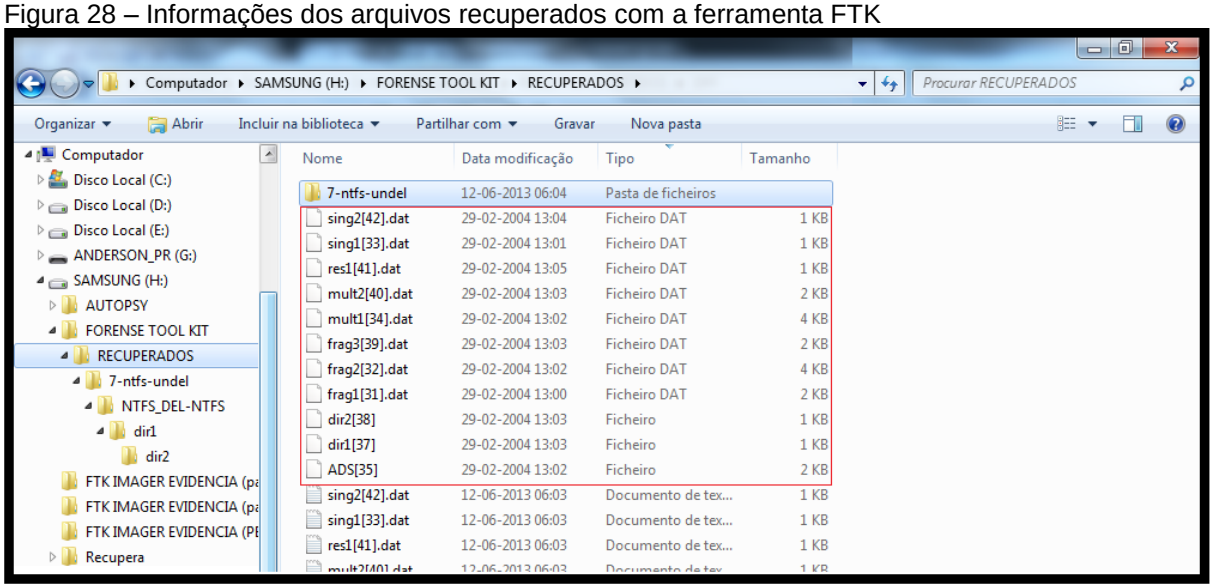
Fonte: Do autor.

É possível observar a partir do formulário dos resultados propostos pelo autor, que os respectivos valores MD5, figura 26, e que na qual foi gerado o mesmo valor correspondente dessa imagem, figura 27 como confirmação, além disso, a imagem não sofreu nenhum tipo de alteração são iguais. Verifica-se também que os números relacionados à Tabela de arquivos mestres (MFT) são iguais, a data em que eles foram criados, modificas e acessados também são as mesmas, 29 de Fevereiro de 2004.

É importante salientar que a ferramenta mostrou-se bastante eficiente tendo em conta a recuperação dos arquivos excluídos, fragmentados, bem com os seus diretórios apagados.

Foi possível verificar todo o conteúdo interno da imagem. Por conseguinte, conseguiu-se recuperar os 11 arquivos deletados e de fato salvá-los em um disco de armazenamento externo formatado, figura 28.

Figura 28 – Informações dos arquivos recuperados com a ferramenta FTK

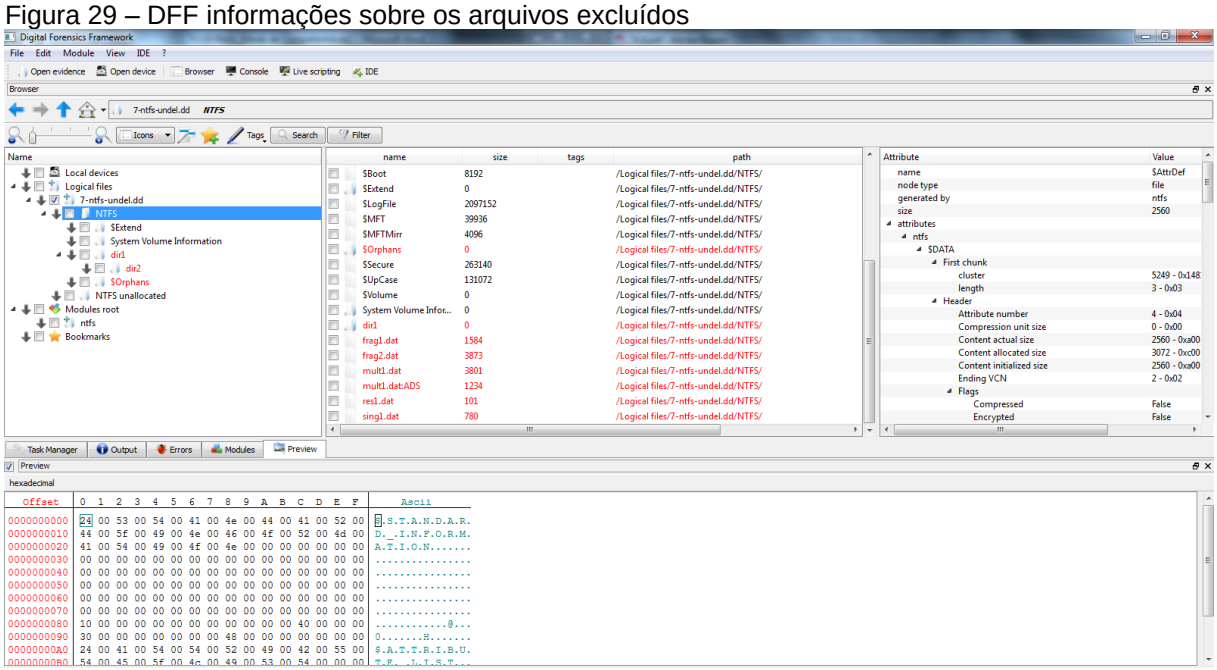


Fonte: Do autor.

5.1.5.3 Análise dos dados realizada com a ferramenta Digital Forense Framework (DFF)

Executando-se a ferramenta em sua versão mais recente 1.3.0, usado para recolher, preservar e revelar evidências digitais, sem comprometer dados e sistemas. Não é necessário criar-se um caso para adição da imagem forense do dispositivo como nas ferramentas anteriores, figura 29.

Figura 29 – DFF informações sobre os arquivos excluídos



Fonte: Do autor.

O estudo trouxe os mesmos resultados encontrados com as ferramentas Autopsy e FTK. Conseguiu-se achar todos os arquivos contidos na imagem forense gerada do sistema de arquivos NTFS proposto, arquivos deletados. Com as três ferramentas é possível recuperar todos os arquivos e salvá-los em um disco.

5.2 APRESENTAÇÃO, ANÁLISE DOS DADOS E DISCUSSÕES.

Como trata-se de um estudo de caso de simulação de ambiente academico, abdicou-se em fazer o levantamento perante as pessoas que podem estar envolvidas no ato (onde as mesmas identificaram o acontecimento e com isso culminou com as consequências do crime digital) por meio de um interrogatório, informações valiosas, objetivando ao perito uma melhor análise dos fatos que aparecessem durante a investigação.

À aquisição das especificações sobre Hardware e Software dos computadores a serem feitas as análises, para este tipo de casos de perícia, é importante conhecer. Sendo assim, acessou-se o programa – Ferramenta do Sistema – que pode ser encontrado no menu Iniciar *(Todos os programas/Acessórios/Ferramentas do Sistema)*, disponível no Windows 7. Apresentação da configuração de hardware de todos os computadores, abaixo:

a) Memória RAM instalada: 4 GB;

b) Disco Rígido: 320 GB – possuí três partições (C:\, D:\, E;\);

c) Processador: Intel Core 2 Duo;

d) Velocidade do Processador: 2,26 GHz;

e) Número de Processadores: 2;

f) Número de Núcleos: 2;

g) Placas de áudio, vídeo e rede on-board

As seguintes especificações de software, abaixo:

a) Windows 7, Service Pack 1.

Com as especificações já feitas, pode-se observar que a capacidade do HD é de 320 GB, particionadas em: C:\ *com 78.1 GB*, D:\ *com 29.5 BG* e o E:\ *com 190 GB*. Todas as partições possuem o sistema de arquivos NTFS.

A escolha do kit de ferramentas *open source* que se utilizou recai devido ao fato de apresentarem maior confiabilidade, conforme apresentado por seus fabricantes, dando uma maior credibilidade ao trabalho do perito para recuperar arquivos na partição NTFS, são eles:

a) iCare Data Recovery Free;
b) Lazesoft Data Recovery;
c) RecoveryMyFiles;
d) MiniTool Power Data Recovery;
e) Easeus Data Recovery Wizard Free;
f) DiskDigger;
g) Easeus Deleted File Recovery;
h) Wise Data Recovery;
i) Glary Undelete;
j) Recuva;
k) NTFS Undelete.

Para além desses, foram usados utilitários nativos do sistema operacional Windows como a linha de comandos, que também fazem parte do kit de ferramentas.

Primeiramente utilizou-se estas ferramentas, para recuperar arquivos excluídos da lixeira ou de forma permanente na busca por evidências. Tanto os softwares de perícia quanto os softwares *open source* possuem módulos de recuperação, para tal foi realizado um teste com cada uma das ferramentas tendo como propósito a recuperação desses arquivos, resgatando assim os valores a serem apresentados como prova da ocorrência de um crime digital a ser analisado, porem diferenciados.

Os testes foram realizados em função ate da escolha dos softwares usados durante o processo de perícia forense, como sua credibilidade e eficiência no quesito funcional. No momento em que fez-se as comparações, a ideia foi verificar quais dos softwares consegue resgatar uma quantidade maior de arquivos.

Dentre os onze (11) softwares de código fonte aberto mencionados, optou-se por escolher 5 deles a serem utilizados. A escolha dos mesmos deu-se por ser gratuito e software livre, embora alguns deles necessitam de licença para recuperação dos arquivos. Esses são alguns dos motivos que chamaram a atenção na escolha dos softwares.

5.2.1 Análise e resultados da partição em NTFS

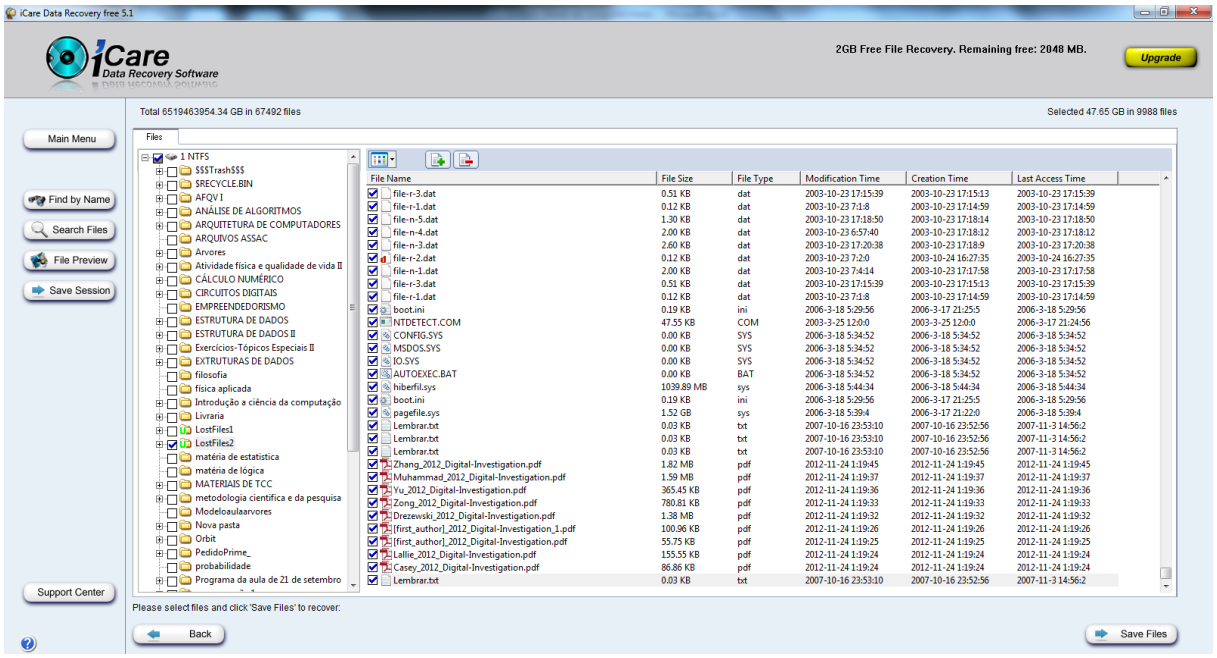
Na segunda fase do desenvolvimento, inseriu-se vários arquivos na partição E:\ *com 190 GB* que antes foi devidamente formatada. Neste caso escolheu-se a maior das partições de capacidade de armazenamento. Selecionou-se alguns destes arquivos e posteriormente excluí-se propositalmente (como suposto no estudo de caso da pesquisa). Utilizou-se algumas ferramentas para recuperação neste momento afim de poder resgata-las.

5.2.1.1 Análise utilizando a ferramenta iCare Data Recovery Free

Com a sua versão mais recente 5.1, executou-se a ferramenta afim de recuperar os arquivos perdidos. Ao término da varredura com a mesma, é possível observar-se de maneira clara o resultado completo de todos os arquivos, os excluídos, que se encontravam na partição de maior capacidade com o sistema de arquivos NTFS, sendo que parte dos arquivos resgatados, muitos deles, excluiu-se propositalmente.

As informações em relação aos dados podem ser visualizadas na figura 30, informações como a data e hora que os mesmos foram criados, acessados, modificados e alterados. A ferramenta apresentou um total de 18448 arquivos, o que corresponde a 60.66 GB de uma partição de 190 GB.

Figura 30 – Icare Data Recovery mostrando informações dos arquivos excluídos.

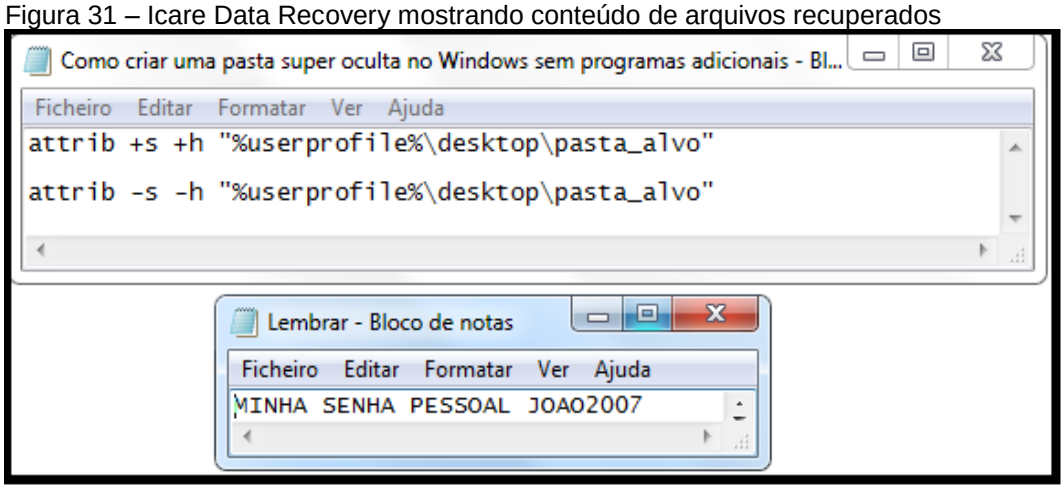


Fonte: Do autor.

Durante o decorrer da análise com a ferramenta em questão, constatou-se um pormenor bastante pertinente para o presente trabalho. A mesma recuperou arquivos que haviam sido selecionados aleatoriamente e excluídos posteriormente, porem, obteve-se acesso ao conteúdo de um dos arquivos recuperados pós formatação do HD.

Ao final da recuperação, um dos arquivos chamou a atenção apenas pelo seu nome *"Como criar uma pasta super oculta no Windows sem programas adicionais.txt"*, arquivos perdidos depois de ter sido formatado a máquina. Observou-se também um arquivo do tipo *.txt* criado no ano de 2007 com o nome *"Lembrar.txt"* (figura 31). A ferramenta possui a capacidade de resgatar arquivos perdidos, ocultos que estejam a bastante tempo alocados no HD sem que eles sofressem alterações ou tenha sido sobreescritos.

Figura 31 – Icare Data Recovery mostrando conteúdo de arquivos recuperados

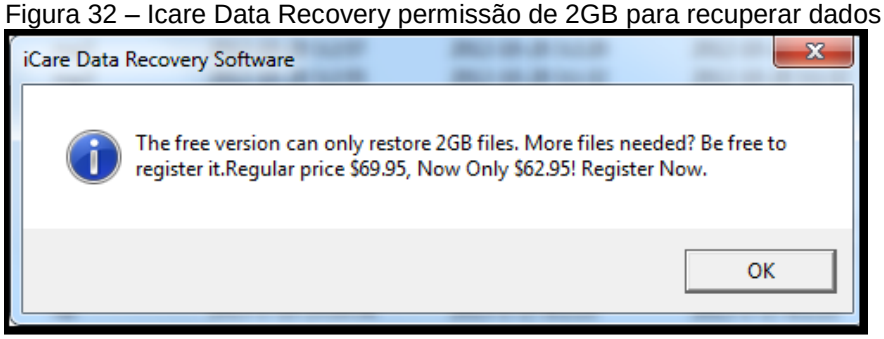


Fonte: Do autor.

Entretanto, o que se pode observar na figura 31, o usuário pretendia com o uso de alguns comandos nativos do Windows, criar pastas super ocultas sem precisar de programas adicionais, o que pode-se suspeitar que o mesmo tinha conhecimentos suficientes para prejudicar outrem, uma empresa ou ate mesmo uma instituição de ensino. Pos se tratar de uma prévia análise, não se tirou nenhuma conclusão a respeito do arquivo considerado suspeito encontrado na partição, mesmo tendo sido visualizado para comprovação de que se trata realmente re tentava de ocultar dados no Windows.

Assim sendo, por tratar-se de uma ferramenta com a sua versão gratuita e sem licença, ela só permite recuperar 2GB de informações, que chega a ser satisfatório para resgatar os arquivos que foram excluídos acidental e/ou propositalmente. Ao tentar-se recuperar arquivos superior a 2Gb, que é permite por fábrica, uma tela informando que deve ser feito um registro e comprar a ferramenta para obter uma cópia de ativação do mesmo, é apresentada mostrando que não é possível prosseguir com a operação desejesada, figura 32.

Figura 32 – Icare Data Recovery permissão de 2GB para recuperar dados

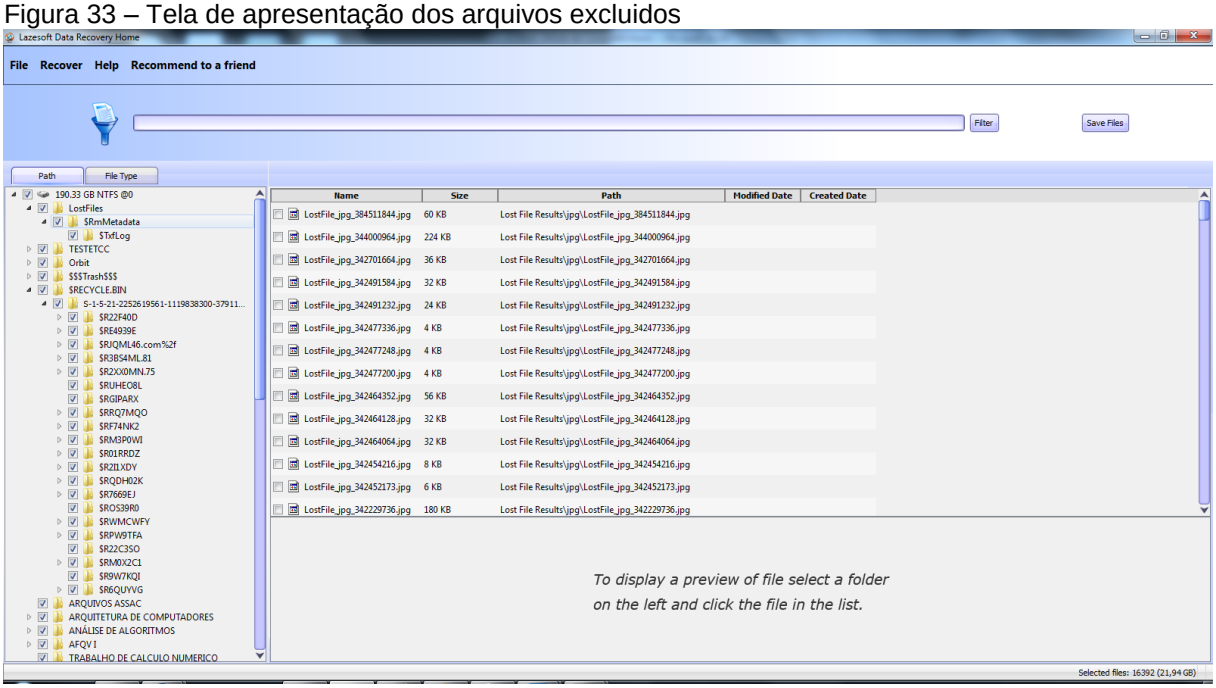


Fonte: Do autor.

5.2.1.2 Análise utilizando a ferramenta Lazesoft Data Recovery

E executou-se a ferramenta a fim de recuperar os arquivos perdidos. Ao término da varredura com a mesma, é possível observar-se o resultado completo de todos os arquivos, os excluídos, que se encontravam na partição de maior capacidade com o sistema de arquivos NTFS, sendo que parte dos arquivos recuperados, excluiu-se propositalmente, figura 33.

Figura 33 – Tela de apresentação dos arquivos excluidos



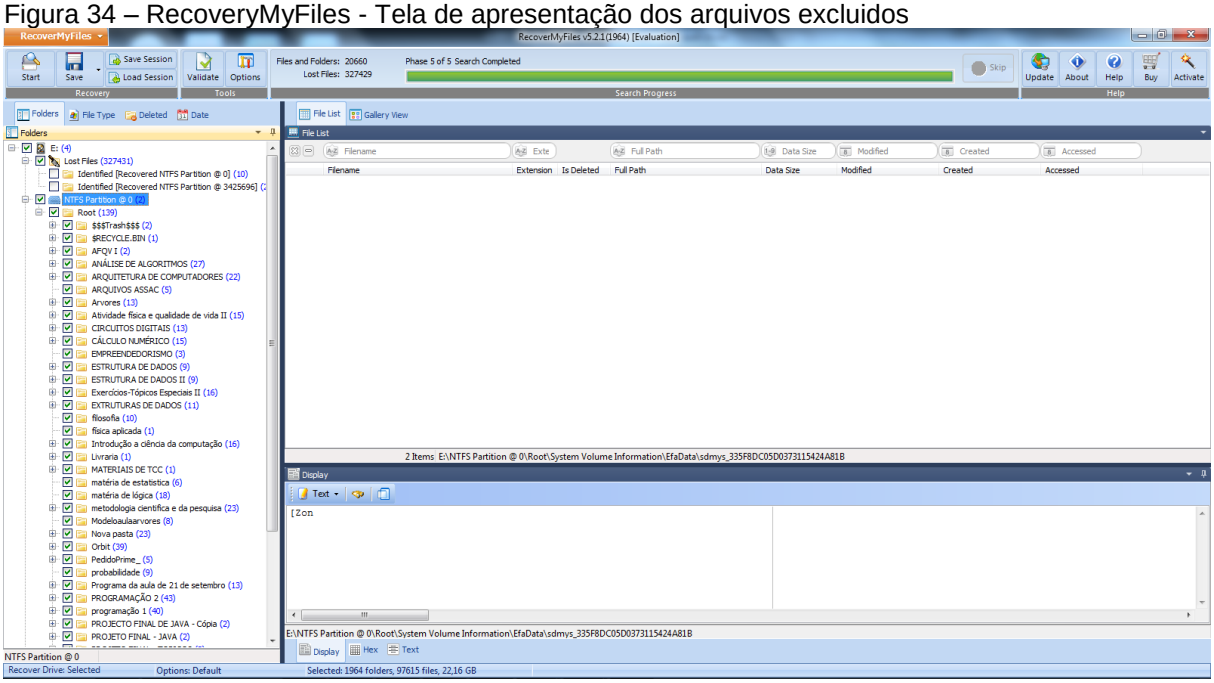
Fonte: Do autor.

A ferramenta trouxe os mesmo resultados apresentados pelas ferramentas anteriores.

5.2.1.3 Análise utilizando a ferramenta RecoveryMyFiles

Com uma capacidade poderosa de recuperação, a ferramenta também precisa de uma chave de ativação para permitir que o usuário salve os resultados da recuperação de arquivos. Com a sua versão mais recente no mercado a 5.2.1, foi possível recuperar arquivos excluídos independente do seu formato sem compromentendo a integridade do mesmo, figura 34.

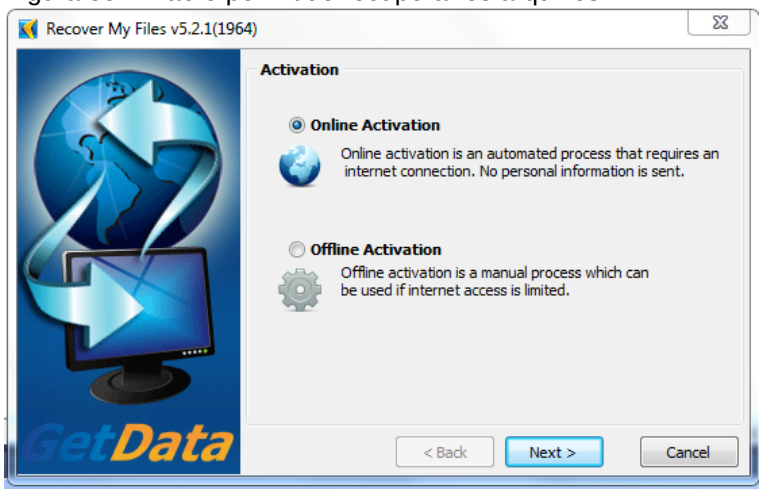
Figura 34 – RecoveryMyFiles - Tela de apresentação dos arquivos excluidos



Fonte: Do autor.

Como trata-se de uma ferramenta com a versão gratuita, com as características similiares a da ferramenta iCare, só permite recuperar 1GB de informações, que não tão satisfatório para resgatar arquivos que tenha sido excluídos acidental. Sem fugir muito o modo de ação das outras, tentar-se recuperar arquivos superior a 1Gb, uma tela informando que deve comprar a ferramenta para obter uma licença de ativação do mesmo, é apresentada mostrando que não é possível prosseguir com a operação desejesada, figura 35.

Figura 35 – Não é permitido recuperar os arquivos



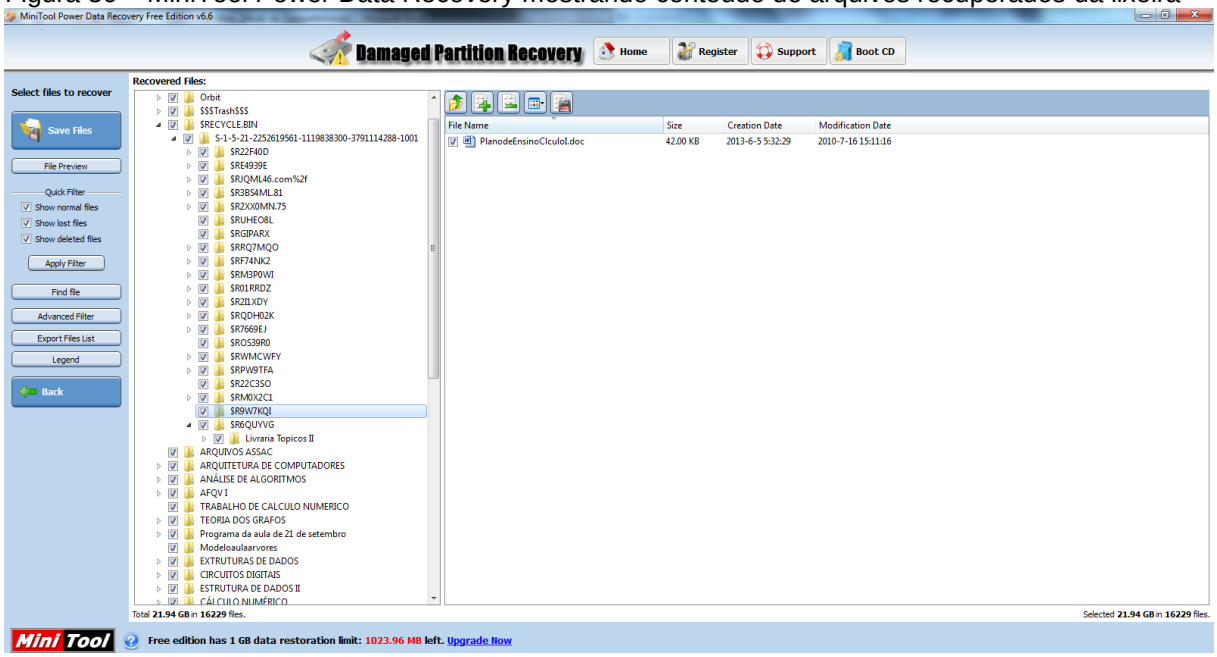
Fonte: Do autor.

5.2.1.4 Análise utilizando a ferramenta MiniTool Power Data Recovery

Com a versão 6.6, executou-se a ferramenta com o mesmo proposito das anteriores. Ao final da análise, é possível observar-se de forma clara o resultado completo de todos os arquivos, os excluídos, sendo que parte dos arquivos recuperados, apagou-se propositalmente e muitos deles ainda encontram-se na lixeira.

As informações em relação aos dados podem ser visualizadas na figura 36, informações como a data e hora que os mesmos foram criados, acessados, modificados e alterados. A ferramenta apresentou um total de 16229 arquivos o que corresponde a 21.94 GB.

Figura 36 – MiniTool Power Data Recovery mostrando conteúdo de arquivos recuperados da lixeira

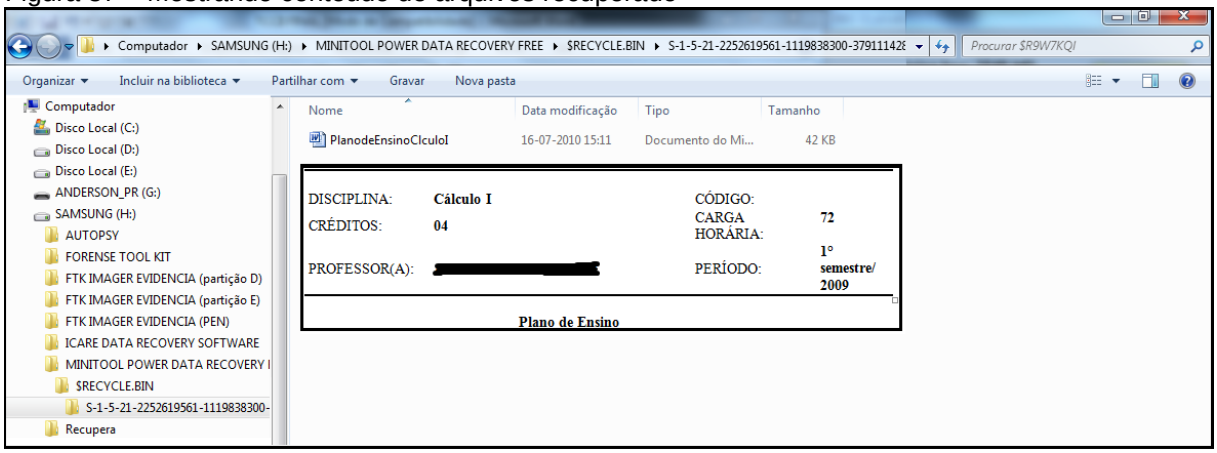


Fonte: Do autor.

No final da análise, observou-se com atenção ao conteúdo de um arquivo recuperado da lixeira com o nome *“PalnodeEnsinoCIculoI.doc”*. este arquivo foi criado no ano de 2010, onde a mesma fez parte da grade de ensino da referida

instituição (figura 37). A ferramenta também possui a capacidade de resgatar arquivos perdidos, ocultos que se encontram a bastante tempo inseridos no HD.

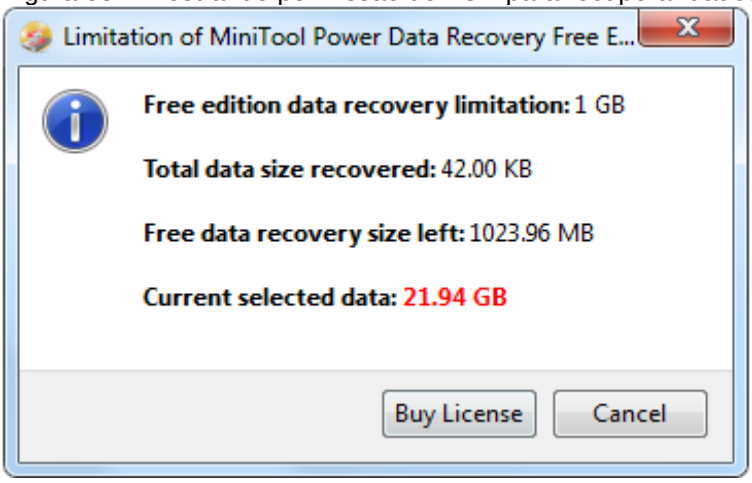
Figura 37 – Mostrando conteúdo de arquivos recuperado



Fonte: Do autor.

Por tratar-se de uma ferramenta com a versão gratuita, com as características similares a da ferramenta iCare, só permite recuperar 1GB de informações, que não tão satisfatório para resgatar arquivos que tenha sido excluídos acidental. Sem fugir muito a redia das outras, tentar-se recuperar arquivos superior a 1Gb, uma tela informando que deve comprar a ferramenta para obter uma licença de ativação do mesmo, é apresentada mostrando que não é possível prosseguir com a operação desejada, figura 38.

Figura 38 – Mostrando permissão de 1GB para recuperar dados



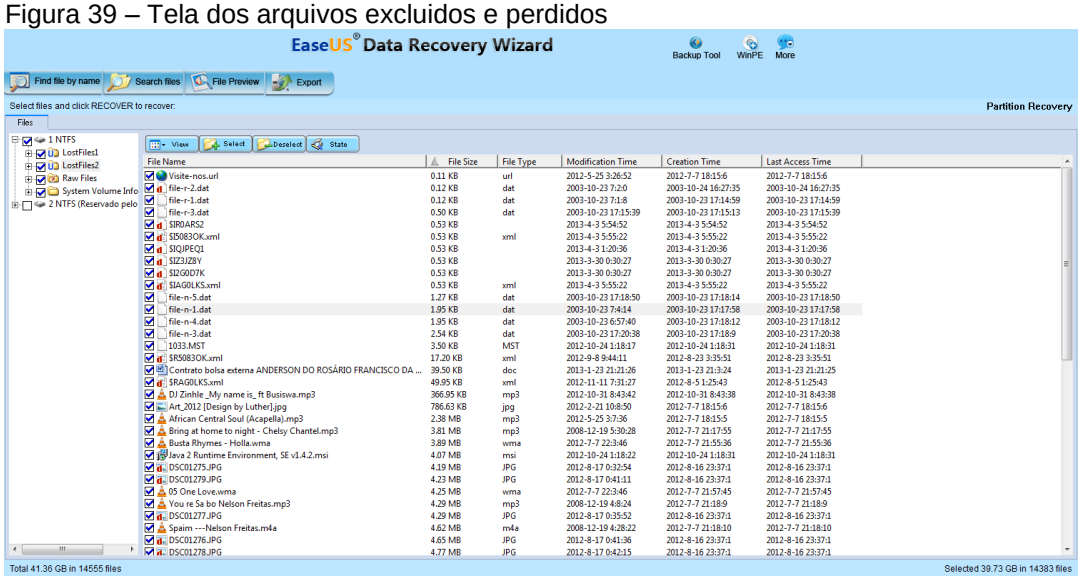
Fonte: Do autor.

5.2.1.5 Análise utilizando a ferramenta Easeus Data Recovery Wizard Free

A ultima ferramenta selecionada para o teste de recuperação dos arquivos, com a versão gratuita 5.8.0, oferece 3 formas fáceis de recuperação: *Data File Recovery*, *Complete Recovery* e *Partition Recovery*. Possui um aspecto bastante interessante em relação à algumas ferramentas anteriores, ele é capaz de recuperar arquivos em partições formatadas, com o mesmo nome, mesmo caminho origial, após a reinstalação do Windows na partição referida.

Optou-se por escolhar a opção *Partion* Recovery para recuperação de uma partição deletada. Mostrou-se bastante eficiente também, porém, em contrapartida não trouxe o mesmo número de arquivos recuperados como as ferramentas anteriores. Obteve um elevado número de arquivos recuperados, um total de 14338 arquivos, figura 39.

Figura 39 – Tela dos arquivos excluidos e perdidos



Fonte: Do autor.

No final da varredura conseguiu-se obter o conteúdo de um arquivo perdido, do tipo *.wav* com o nome *“Windows Information Bar”*. este arquivo teve seu ultimo acesso no ano de 2009, (figura 40). A ferramenta também possui a capacidade de resgatar arquivos perdidos, ocultos que se encontram a bastante tempo inseridos no HD.

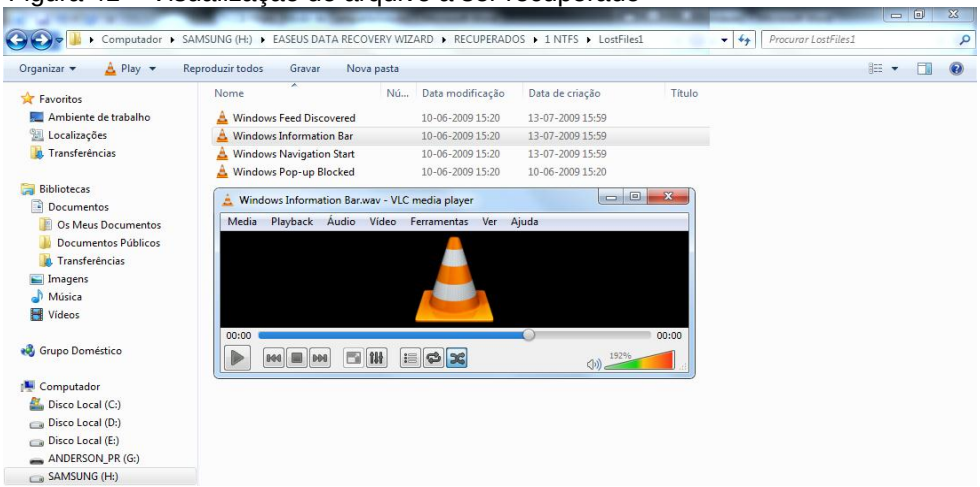
Figura 40 – Visualização do arquivo a ser recuperado

File Name	File Size	File Type	Modification Time	Creation Time	Last Access Time
Windows Navigation Start.wav	11.07 KB	wav	2009-6-10 21:20:33	2009-7-13 21:59:50	2009-7-13 21:59:50
Windows Pop-up Blocked.wav	83.54 KB	wav	2009-6-10 21:20:33	2009-6-10 21:20:33	2009-6-10 21:20:33
Windows Information Bar.wav	22.76 KB	wav	2009-6-10 21:20:33	2009-7-13 21:59:50	2009-7-13 21:59:50
Windows Feed Discovered.wav	19.42 KB	wav	2009-6-10 21:20:33	2009-7-13 21:59:50	2009-7-13 21:59:50
MediaPlayer-DLMigPlugin.dll	540.50 KB	dll	2009-7-14 1:16:13	2009-7-14 0:9:17	2009-7-14 0:9:17

Fonte: Do autor.

Conseguiu-se então, com sucesso, verificar o conteúdo do mesmo. O mesmo pode ser observado a partir da figura 41.

Figura 41 – Visualização do arquivo a ser recuperado



Fonte: Do autor.

Estudou-se todos os casos com a ferramenta, fez-se toda a análise e não foi possivel recuperar todos os dados como se almejava. Porém, conseguiu-se um material na Internet onde o pesquisador Professor Ramos, fazendo uso da mesma ferramenta conseguiu recuperar com uma versão profissional, recuperar todo conteúdo de uma partição formatada indevidamente.

6 RESULTADOS OBTIDOS.

De acordo com as etapas de coleta e análise das evidênias coletadas, o perito tem a capacidade de desenvolver um relatório contendo informações sobre o sistema periciado, abordando as evidências encontradas, que visam dar informações relevantes ao perito e atingir o objetivo da perícia em questão.

Por se tratar de um trabalho com fins de aprendizado e que pretende dar um contribuição bibliográfica num modo geral, as etapas, em geral, foram produzidas de formas a que os mais leigos ná área da computação pudessem perceber todo o processo que envolve uma pericia computacional, e torna-se inprescindivel aprensetar as informações necessárias.

O estudo de caso apresentou objetivos visando aferir o estado da eficiência das ferramentas forenses usadas. Na recuperação dos dados apagados, foi feito de maneira bastante prática, a demonstração e recuperação de um número maior de informações.

Conseguiu-se recuperar um total de arquivos controlados, ou seja, que foram selecionados e excluidos para teste com todas as ferramentas. O que demostra que as ferramentas são tão eficientes.

Mesmo a comunidade cientifica de desenvolvedores, ainda não conseguiram colocar disponível no mercado uma que conseguisse recuperar arquivos apagados permantentemente.

6.1 COMPARAÇÃO DOS RESULTADOS.

Após realizar a análise das ferramentas iCare Data Recovery Free, Lazesoft Data Recovery, RecoveryMyFiles, MiniTool Power Data Recovery, Easeus Data Recovery Wizard Free, foram obtidos resultados diferentes, respectivamente. Porém, a ferramenta MiniTool Power Data Recovery resgatou um total de 16229 arquivos correspondentes a 21.94 GB e a Easeus Data Recovery Wizard Free recuperou um total aproximado de 14338 arquivos. Com estes resultados é possível observar que a ferramenta MiniTool Power Data Recovery possui uma maior capacidade de recuperação de arquivos deletados. Sendo assim, ela é a que mais se aproxima do serviço esperado em recuperação de arquivos.

O objetivo deste estudo comparativo foi analisar qual das ferramentas estudadas possui uma maior capacidadede em resgatar dados deletados e analisar a qualidade dos mesmo. Portanto, baseando-se nos resultados obtidos, o MiniTool Power Data Recovery seria a melhor opção na escolha de um *software* de recuperação de arquivos.

7 CONCLUSÃO

A medida que os crimes praticados por meio de computadores vão aumentando, também cresce a necessidade de resposta da utilização da perícia

forense no combate a esse tipo de crimes digitais. No Brasil, muitas das evidências digitais documentas e as metodologias criadas internacionalmente são aceites pela comunidade científica e vêm sendo usadas com uma maior brevidade em processos criminais, objetivando buscar um julgamento correto do acusado. Tornando-as assim importantes e cada vez mais eficientes em relação às provas que são encontradas proporcionadas pelo trabalho do perito.

Baseados nestes fatos, os mesmos procedimentos empregados durante o decorrer da perícia, precisam ser claras e objetivas procurando sempre relatar a verdade, sem comprometer ou ocultar informações pertinetes ao relatório final. O uso de ferramentas livres e técnicas avançadas por parte dos criminosos, sendo que o mesmo foi demonstrado através deste trabalho, torna-se necessário que os peritos estejam capacitados para conseguir combater e disseminar o avanço de crimes digitais que vêm acontecendo com bastante frência nos diversos ambientes computacionais.

Diante da pesquisa feita, em perícia forense em ambientes New Technologies File System para arquivos excluídos, ocultos e segmentados, foi possível constatar resultados suficientemente positivos durante a investigação à segurança da informação. As evidências encontradas na imagem proposta pelo especialista Carreir puderam ser comprovadas e, utilizou-se a metodologia escolhida, a SOP, sob forma de demonstrar por meios seguros buscar os mesmo resultados anteriormente apresentados na pesquisa.

Os objetivos especifícos propostos inicialmente foram atingidos com sucesso durante a execução do trabalho, sendo ele compreendido em aplicar os príncipios básicos de perícia forense computacional para recuperação de arquivos excluídos em cima de sistema de arquivos NTFS, demonstrando a utilização de ferramentas forenses e de recuperação. Conseguiu-se resultados pertinentes que poderiam ser usados para representação de um caso real.

Examinar e documentar os aspectos que envolvem a análise foi definido como o segundo ponto do objetivo especifico, onde a mesma foi atingida no ato do emprego da metodologia forense para a execução do estudo de caso.

Um dos pontos negativos que encontrou-se durante o trabalho é a falta de bibliográfia baseado na área da perícia em Língua Portuguesa, bem como a carência de padrões metodológicos e principalmente a falta de versões mais recentes das princípais ferramentas forenses e de recuperação sem a obtenção das

respectivas licenças para que fosse possível resgatar o maior número de arquivos excluídos no ato pesquisa. Não se obteve a versão profissional (paga) das ferramentas específicas por se tratar de um estudo de caso baseado em ambiente acadêmico.

Para concluir, estima-se que o presente trabalho irá contribuir para diminuir a carência de referências bibliográficos na área, sendo que o memso problema foi aprensentado na justificativa. Por ser tão constante as formas como os crimes digitais se proliferam nos dias de hoje, surge a ideia, como trabalhos futuros, de se aplicar a perícia forense computacional em um ambiente baseado em Mac OX empregando as metodologias aplicadas no trabalho.

REFERÊNCIAS

ARGOLO, Frederico Henrique Böhm. **Análise Forense em sistemas GNU/Linux.** Universidade Federal do Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799**: Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

BANSOD, Tularam. **Basics Of Digital Forensics: How Hackers Hide Data in Computares**. 2009. Disponível em: <http://www.miel.in/pdfs/Digital%20Forensics.pdf> Acesso em: 08 de out. 2012.

BARYAMUREEBA, Venansius; TUSHABE, Florence. The Enhanced Digital Investigation Process Model. DIGITAL FORENSIC RESEARCH WORKSHOP, 2004, Maryland, USA. **Proceedings of the 2004 Digital Forensic Research Workshop.** Maryland, EUA: DFRWS, 2004. p. 1 - 9.

BERTOGLIO, Daniel Dalalana. **Perícia Forense: Proposta de Uma Metodologia de Coleta de Indícios Para Ambiente Windows.** 2008. Trabalho de Conclusão de Curso (Graduação) - Curso de Ciência da Computação, Departamento de Instituto de Ciências Exatas e Tecnológicas, Centro Universitário Feevale, Novo Hamburgo, 2008.

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

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

CARRIER, B. **File System Forensic Analysis**. 2006.

CARRIER, B. **Risks of live digital forensic analysis:** Commun. ACM, 49 No.2: 56–61. 2006.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em Informática e de Informações.** 2a ed. São Paulo: Editora SENAC, 1999.

CERT.br. CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Incidentes Reportados ao CERT.br—Julho a Setembro de 2012.** 2012. Disponível em: < http://www.cert.br/stats/incidentes/2012-jul-sep/weekdays-incidentes.html> Acesso em: 10 nov. 2012, 20:10:15.

CERT.br. CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Incidentes Reportados ao CERT.br—Julho a Setembro de 2012.** 2012. Disponível em: < http://www.cert.br/stats/incidentes/2012-jul-sep/tipos-ataque.html> Acesso em: 10 nov. 2012, 20:20:45.

CHOFFNES, David; DEITEL, Harvery; DEITEL, Paul. **Sistemas Operacionais.** 3. ed. São Paulo: Pearson Pretice Hall, 2005

COPPE/UFRJ - RAVEL. **Laboratório de Redes de Alta Velocidade.** 2006

COSTA, Marcelo Antonio Sampaio Lemos. **Computação Forense.** Campinas: Millennium, 2003. 150 p.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais.** São Paulo: Saraiva, 2011. 242 p.

CRESPO, Marcelo Xavier de Freitas; SYDOW, Spencer Toth. **Novas tendências da criminalidade telemática**. Revista de Direito Administrativo, Rio de Janeiro, n. 246, set./dez. 2007.

CORREA, Gustavo Testa. **Aspectos Jurídicos da Internet.** 2.ed.rev. São Paulo: Saraiva, 2002.

CUMMINS, Chris. **Lack of Information Technology Laws in Angola**. Disponível em <http://www.datasecurity.com.br/index.php/biblioteca/file/13-lack> Acesso em: 15 Setembro, 2012, 16h26.

ELEUTERIO, P. M. S; MACHAD, M. P. **Desvendando Computação Forense**. São Paulo: Novatec, 2011.

FARMER, Dan; VENEMA, Wietse. **Perícia Forense Computacional.** São Paulo: Pearson Prentice Hall, 2007. 190 p.

FARMER, Dan; VENEMA, Wietse. **Perícia Forense Computacional – Teoria e Prática Aplicada** – Como investigar e esclarecer ocorrências no mundo cibernético. São Paulo: Perarson Prentice, 2007.

FRATEPIETRO, Stefan, ROSSETI, Sandro. **DEFT**: Manual de uso. Disponivelem < http://www.deftlinux.net/doc/EN-deft7.pdf> Acesso em: 6 de Janeiro. 2012, 14:05

FREITAS, Andrey Rodrigues de. **Perícia Forense Aplicada à Informática**. Trabalho para o curso de Pós – Graduação "*Lato Sensu*" em Internet Securit IBPI/ Janeiro 2003.

FREITAS, Andrey Rodrigues de. **Perícia forense aplicada à informática**. Rio de Janeiro: Brasport, 2006. 216 p.

GOUVÊA, Sandra. **O direito na era digital: crimes praticados por meio da informática.** Rio de Janeiro: Mauad, 1997.

HACKING9-TEAM. **Hacking On Demand**. The Guide to Backtrack. Disponível em: <http://www.backtracklinux.org/documents/Hakin9_On_Deman_03_2012_Teasers.pdf>. Acesso em: 02 Abr. 2013.

HOUAISS, António. **Dicionário Houaiss da Língua Portruguesa: Com a nova Ortografia da Língua Portuguesa.** Editora: Objetiva, 2009.

KENT, Karen; CHEVALIER, Suzanne; GRANCE, Tim; DANG, Hung. **Guide to Integrating Forensic Techniques into Incident Response**. Gaithersburg. NIST.

2006. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>. Acesso em: 03 Outubro. 2012, 01:00 PM.

LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional**. Campinas – SP: Millennium Editora, 2006.

LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional.** 2. ed. São Paulo: Atlas, 2011. 166 p.

L9296. **LEI Nº 9.296, DE 24 DE JULHO DE 1996.** Presidência da República. Disponível em: < https://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm> Acessado em: 03 Outubro. 2012, 01:37PM.

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

MARCHIORI, Rafael Bernardes. **Estudo de Ferramentas para Análise Forense Computacional**. Curso de Analise de Sistemas. Universidade São Francisco. Itatiba – São Paulo – Brasil. Junho de 2006.Disponível em <http://www.hardware.com.br/livros/redes/denial-service-dos.html> Acesso em: 17 Nov de 2012, 00h40:30.

MELO, Sandro. **Computação Forense com Software Livre.** Rio de Janeiro: Altas Books, 2009. 152 p.

MIKHAILOV, D. **NTFS File System**. 2000. Disponível em: <http://www.digit-life.com/articles/ntfs/> Acesso em:

MORIMOTO, Carlos E. **Guia do Hardware:** Redes, Guia Prático 2ª Ed. 2008.

MONTEIRO, Marcos. **Perito em Computação**. Disponível em <http://www.marcosmonteiro.com.br> Acesso em: Junho, 2012.

NG, Reynaldo. **Forense computacional corporativa.** Rio de Janeiro: Brasport 2007. 158 p.

BRASIL. **Novo Código Civil.** Disponível em: <http://www.presidencia.gov.br/ccivil_03/LEIS/2002/L10406.htm> Acesso em: 08 de out. 2012.

OLIVEIRA, Sabrina Vitório. **Perícia Forense Em Sistemas Gnu/Linux.** 2007. 79 f. Monografia - Faculdade Salesiana de Vitória - Pós-Graduação em Segurança de Redes de Computadores, Vitória, 2007.

PEREIRA, E.; FAGUNDES, L.; NEUKAMP, P.; LUDWIG, G.; KONRATH, M. **Forense Computacional**: fundamentos, tecnologias e desafios atuais. In: VII SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, Rio de Janeiro. Minicursos ... Rio de Janeiro: VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2007.

QUEIROZ, Claudemir; VARGAS, Raffael. **Investigação e Perícia Forense Computacional:** certificações, Leis Processuais, Estudo de casos. Rio de Janeiro: Brasport, 2010.

ROSA, Fabrízio. **Crimes de Informática.** Bookseller, 2007.

SOPHOS. **Secutity Threat Report 2012**. Disponível em: <http://www.sophos.com/en-us/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf> Acesso em 10 set. 2012

SOUZA, Clarice Muhlethaler de. **Biblioteca – uma Trajetória**. In: III Congresso Internacional de Biblioteconomia, 2005, Rio de Janeiro. Disponível em: <http://geocities.yahoo.com.br/csouza952/IIICIB.pdf.>. Acesso em: 08 out. 2012.

STEPHENSON, P. **Investigating Computer-related Crime**. CRC Press. Boca Raton, 2000.

SWGDE, SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE. Best Practices for Computer Forensics. Disponível em: <http://www.oas.org/juridico/spanish/cyb_best_pract.pdf>. Acesso em: 03 Outubro. 2012, 01:37:15.

SWGDE. SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE. Digital Evidence: **Model Standard Operation Procedures for Computer**. 2012. Disponível em:<https://www.swgde.org/documents/Current%20Documents/SWGDE%20QAM%20and%20SOP%20Manuals/2012-09-13%20SWGDE%20Model%20SOP%20for%20Computer%20Forensics%20v3> Acesso em: 03 out. 2012, 02:40:10.

YADAV, Seema.VSRD International Journal of Computer Science e Information Technology: **Analysis of Digital Forensic and Investigation.** 2011

APÊNDICE A - LOG COM INFORMAÇÕES REALIZADAS NO FTK ATE A CONCLUSÃO DA ANÁLISE

```
10-06-2013 01:34:05 -- FTK Version 1.81.6 build 10.04.02
        FTK Exe Path:  C:\Program Files\AccessData\AccessData Forensic Toolkit
1.81.6\Program\ftk.exe
        Examiner's Machine:
        Phys Mem:  Total: 3,052,437,504  Available: 247,812,096  Used: 2,804,625,408
        Virt Mem:  Total: 2,147,352,576  Available: 1,105,469,440  Used: 1,041,883,136
        Page File Available: 1,535,266,816
        ----------------------------------------------------
10-06-2013 01:34:05 -- KFF database being used:  none
10-06-2013 01:34:05 -- Examiner's Local Machine Setting is time zone used for file times (create,
modify, accessed) in file display and reports.
10-06-2013 01:34:05 -- New case started by examiner AndersonSilva using FTK version 1.81.6 build
10.04.02
        Investigator: AndersonSilva
        Case Name: teste
        Case Number: 1
        Case Folder: E:\TESTETCC\teste
        Description:
        Case Log Options (NOT Case Reviewer Logging Options):
          Log case and evidence events: Yes
          Log error messages: Yes
          Log bookmarking events: Yes
          Log searching events: Yes
          Log special searching events: Yes
          Log other events: Yes
          Log extended information: Yes
        Processes to be performed:
          File Extraction: Yes
          File Identification: Yes
          MD5 Hash: Yes
          SHA1 Hash: Yes
          KFF (Known File Filter): Yes
          Entropy Test: Yes
          Full Text Index: Yes
          Prerender Thumbnails: Yes
          File Listing Database: Yes
            DB Include OLE-embedded items: No
            DB Include Slack Files: No
            DB Include image name in filename: Yes
          HTML File Listing: No
          Data Carving: No
          Preprocess Registry Files: No
          Decrypt EFS Files: Yes
        Default Case Refinement Settings:
          Add files only if they satisfy BOTH the file status and the file type criteria as follows:
            File Status Criteria:
              Deletion status: any
              Encryption status: any
              From email status: any
              Duplicate status: any
              OLE stream status: any
            File Type Criteria:
              documents: yes
```

```
            spreadsheets: yes
            databases: yes
            graphics: yes
            email messages: yes
            executables: yes
            archives: yes
            folders: yes
            other recognized: yes
            unknown: yes
        Default Index Refinement Settings:
          Don't index KFF ignorable files
          Index files only if they satisfy BOTH the file status and the file type criteria as follows:
            File Status Criteria:
              Deletion status: any
              Encryption status: any
              From email status: any
              Duplicate status: any
              OLE stream status: any
            File Type Criteria:
              documents: yes
              spreadsheets: yes
              databases: yes
              graphics: yes
              email messages: yes
              executables: yes
              archives: yes
              folders: yes
              other recognized: yes
              unknown: yes
        -- Evidence 1 --
        Name/Number:
        Location: C:\Users\Anderson Silva\Downloads\7-undel-ntfs\7-ntfs-undel.dd
        Display name: 7-ntfs-undel\NTFS_DEL-NTFS
        Type: Raw Drive Image, NTFS
        Comment:
        Evidence-specific Case Refinement Settings:
          Add all files
        Evidence-specific Index Refinement Settings:
          Index all files
10-06-2013 01:34:05 -- Starting to add evidence items...
10-06-2013 01:34:05 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\$MFT
10-06-2013 01:34:05 --   Identifying...
10-06-2013 01:34:05 --   Hashing and Entropy Test...
10-06-2013 01:34:05 -- MD5: 985CAD322621CD6D22F17E118477F1CA
        Type: Unknown File Type
10-06-2013 01:34:05 --   Adding to database...
10-06-2013 01:34:05 --   Filtering...
10-06-2013 01:34:05 --   Indexing 626 characters... (Index size: 19 KB)
10-06-2013 01:34:05 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\$MFTMirr
10-06-2013 01:34:05 --   Identifying...
10-06-2013 01:34:05 --   Hashing and Entropy Test...
10-06-2013 01:34:05 -- MD5: B69C1C7D24817B2A38DC59F1447B29D3
        Type: Unknown File Type
10-06-2013 01:34:05 --   Adding to database...
10-06-2013 01:34:05 --   Filtering...
10-06-2013 01:34:05 --   Indexing 61 characters... (Index size: 20 KB)
10-06-2013 01:34:05 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\$LogFile
10-06-2013 01:34:05 --   Identifying...
10-06-2013 01:34:05 --   Hashing and Entropy Test...
10-06-2013 01:34:05 -- MD5: 11D7A99DD20A2329ACBC07649EBCD7D6
```

```
        Type: Unknown File Type
10-06-2013 01:34:05 --   Adding to database...
10-06-2013 01:34:05 --   Filtering...
10-06-2013 01:34:06 --   Indexing 2552 characters... (Index size: 20 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\$Volume
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
        Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Indexing info only... (Index size: 21 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\$AttrDef
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
10-06-2013 01:34:06 -- MD5: AD617AC3906958DE35EACC3D90D31043
        Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing 212 characters... (Index size: 21 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\[unnamed]
        Type: Folder
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing info only... (Index size: 21 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\$I30
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
10-06-2013 01:34:06 -- MD5: BE8FBF716D5BB381C27312AD228BA219
        Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing 178 characters... (Index size: 21 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\$Bitmap
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
10-06-2013 01:34:06 -- MD5: B4F39623F5DD17CD68F5D501C67E6711
        Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing info only... (Index size: 21 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\$Boot
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
10-06-2013 01:34:06 -- MD5: 7C2E97A4BC3B3C9E300094DD7D41C281
        Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing 351 characters... (Index size: 21 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\$BadClus
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
        Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Indexing info only... (Index size: 22 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\$BadClus\$Bad
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
        Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Indexing info only... (Index size: 22 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\$Secure\$SDS
```

```
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
10-06-2013 01:34:06 -- MD5: AB306261AE99A0FFB18A89EA682AB722
         Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing info only... (Index size: 22 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\$Secure
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
10-06-2013 01:34:06 -- MD5: 00646F2B99F9D0E90C4F56792672314B
         Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing info only... (Index size: 22 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\$Secure
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
10-06-2013 01:34:06 -- MD5: 2A47E6522B836D2ED94140640D2E30FB
         Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing info only... (Index size: 22 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\$Secure\$SDH
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
10-06-2013 01:34:06 -- MD5: 32310474A98ACDE1A59BD4CD29BAE0B4
         Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing 6 characters... (Index size: 22 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\$UpCase
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
10-06-2013 01:34:06 -- MD5: 6FA3DB2468275286210751E869D36373
         Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing 9397 characters... (Index size: 22 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\$Extend
         Type: Folder
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing 24 characters... (Index size: 23 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\[unnamed]
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
         Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Indexing info only... (Index size: 23 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\[unnamed]
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
         Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Indexing info only... (Index size: 23 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\[unnamed]
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
         Type: Unknown File Type
```

```
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Indexing info only... (Index size: 23 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\[unnamed]
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
         Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Indexing info only... (Index size: 23 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\$Extend\$Quota
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
10-06-2013 01:34:06 -- MD5: 170EE56864CD803BC34E48549F70E178
         Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing info only... (Index size: 23 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\$Extend\$Quota
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
10-06-2013 01:34:06 -- MD5: 081A72DA1E34BA9C4C80B8393EC8DC3E
         Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing info only... (Index size: 24 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\$Extend\$ObjId
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
10-06-2013 01:34:06 -- MD5: 0A4DDCB6FB4143CC73C6F7B948B0D356
         Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing info only... (Index size: 24 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\$Extend\$Reparse
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
10-06-2013 01:34:06 -- MD5: D9866AE700562A59CE3F30577717ACD4
         Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing info only... (Index size: 24 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\System Volume Information
         Type: Folder
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing 14 characters... (Index size: 24 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\System Volume
Information\tracking.log
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
10-06-2013 01:34:06 -- MD5: 822A0FC574EF4AAD6CF407C24A718674
         Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing 11 characters... (Index size: 24 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\frag1.dat
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
10-06-2013 01:34:06 -- MD5: 7A3BC5B763BEF201202108F4BA128149
         Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
```

```
10-06-2013 01:34:06 --   Indexing info only... (Index size: 24 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\frag2.dat
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
10-06-2013 01:34:06 -- MD5: 0E80AB84EF0087E60DFC67B88A1CF13E
         Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Indexing info only... (Index size: 25 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\sing1.dat
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
10-06-2013 01:34:06 -- MD5: 59B20779F69FF9F0AC5FCD2C38835A79
         Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Indexing info only... (Index size: 25 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\mult1.dat
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
10-06-2013 01:34:06 -- MD5: FFD27BD782BDCE67750B6B9EE069D2EF
         Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing 68 characters... (Index size: 25 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\mult1.dat\ADS
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
10-06-2013 01:34:06 -- MD5: BA1B9EEDB1C091DDCA253D35DDE8F616
         Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing 21 characters... (Index size: 25 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\mult1.dat\ADS>>FileSlack
         Type: File Slack
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing info only... (Index size: 25 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\dir1
         Type: Folder
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing info only... (Index size: 25 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\dir1\dir2
         Type: Folder
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing info only... (Index size: 25 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\dir1\dir2\frag3.dat
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
10-06-2013 01:34:06 -- MD5: 21121699487F3FBBDB9A4B3391B6D3E0
         Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing 55 characters... (Index size: 26 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\dir1\mult2.dat
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
10-06-2013 01:34:06 -- MD5: 59CF0E9CD107BC1E75AFB7374F6E05BB
         Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
```

```
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing 28 characters... (Index size: 26 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\res1.dat
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
10-06-2013 01:34:06 -- MD5: 9036637712B491904CD0BFBDBE648453
         Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing 6 characters... (Index size: 26 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\[orphan]\sing2.dat
10-06-2013 01:34:06 --   Identifying...
10-06-2013 01:34:06 --   Hashing and Entropy Test...
10-06-2013 01:34:06 -- MD5: C229626F6A71B167AD7E50C4F2FCCDB1
         Type: Unknown File Type
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing 25 characters... (Index size: 26 KB)
10-06-2013 01:34:06 -- File name: 7-ntfs-undel\NTFS_DEL-NTFS\DriveFreeSpace1
         Type: Drive Free Space
10-06-2013 01:34:06 --   Adding to database...
10-06-2013 01:34:06 --   Filtering...
10-06-2013 01:34:06 --   Indexing 302 characters... (Index size: 26 KB)
10-06-2013 01:34:07 -- Completed adding 7-ntfs-undel\NTFS_DEL-NTFS
10-06-2013 01:34:07 --   Merging Index...
10-06-2013 01:34:07 -- Updating Overview Cache
10-06-2013 01:34:07 -- Updating counts
10-06-2013 01:34:07 -- Flushing case data to disk
10-06-2013 01:34:10 -- Loading case
10-06-2013 01:34:10 -- Building explore path tree
10-06-2013 01:34:10 -- Building explore, graphic and email path tree
10-06-2013 01:34:10 -- Updating Overview Cache
10-06-2013 01:34:10 -- Filtering file list
10-06-2013 01:34:10 -- Initializing thumbnail view
10-06-2013 01:34:10 -- Resetting search terms list
10-06-2013 01:34:10 -- Building the indexed search results tree...
10-06-2013 01:34:11 -- Building the live search results tree...
10-06-2013 01:34:11 -- Building the bookmark tree
10-06-2013 01:34:12 -- Final Status Update:
         Total Elapsed Time:       0.00:00:07
         Total Items Examined:     40
         Total Items Added:        40
         Total Indexing Completed:
            Items Indexed:         28
            Index Time:            0.00:00:00
            Data Indexed:          6,156,389
            Data Indexed (filt):   27,874
            Index granularity set at:  4
         Indexing completed since last update:
            Items Indexed:         41
            Index Time:            0.00:00:00
            Data Indexed:          6,156,389
            Data Indexed (filt):   27,874
         Total Bytes Processed:    6,162,626
         Drive E: Available (case): 176,565,920KB of 199,572,476KB
         Drive C: Available (temp): 21,927,396KB of 81,919,996KB
         Physical Memory Available: 309,932KB of 2,980,896KB
         Virtual Memory Available:  1,069,080KB of 2,097,024KB
         Page File Available:      1,492,036KB of 4,194,303KB
10-06-2013 01:34:35 -- Successfully created default MS Access database during case pre-
```

processing.
10-06-2013 01:34:35 -- Loading case
10-06-2013 01:34:35 -- Updating Overview Cache
10-06-2013 01:34:35 -- Filtering file list
10-06-2013 01:34:35 -- Initializing thumbnail view
10-06-2013 01:34:35 -- Resetting search terms list
10-06-2013 01:34:35 -- Building the indexed search results tree...
10-06-2013 01:34:35 -- Building the live search results tree...
10-06-2013 01:34:35 -- Building the bookmark tree
10-06-2013 02:02:13 -- Column settings changed to: Default File List Column Setting
10-06-2013 02:02:14 -- Column settings changed to: All Columns
10-06-2013 02:02:19 -- Column settings changed to: Preprocessing File Listing Database Column Setting
10-06-2013 02:02:22 -- Column settings changed to: All Columns
10-06-2013 02:03:44 -- Column settings saved: 1
10-06-2013 02:03:47 -- Column settings saved: 1
10-06-2013 02:03:49 -- Column settings saved: 1
10-06-2013 02:03:50 -- Column settings saved: 1
10-06-2013 02:03:51 -- Column settings changed to: 1
10-06-2013 02:05:18 -- Column settings saved: 1
10-06-2013 02:05:22 -- Column settings changed to: 1
10-06-2013 02:06:06 -- Column settings saved: 1
10-06-2013 02:06:08 -- Column settings changed to: 1
10-06-2013 03:01:38 -- Column settings saved: 1
10-06-2013 03:01:39 -- Column settings changed to: 1
10-06-2013 03:04:33 -- Opening View File Sectors... for: 7-ntfs-undel\NTFS_DEL-NTFS\[orphan]\sing2.dat
10-06-2013 03:04:43 -- View File Sectors... search for: [not found]
10-06-2013 03:04:44 -- Closing View File Sectors... for: 7-ntfs-undel\NTFS_DEL-NTFS\[orphan]\sing2.dat
10-06-2013 03:04:50 -- Launched independent view of file7-ntfs-undel\NTFS_DEL-NTFS\[orphan]\sing2.dat
10-06-2013 03:04:54 -- Closed independent view of file 7-ntfs-undel\NTFS_DEL-NTFS\[orphan]\sing2.dat
10-06-2013 03:05:51 -- Analysis Tools -- MD5: yes, SHA1: yes, KFF: no, Recheck all: no, Index: no, Reindex all: no, Entropy test: no
Target files: currently highlighted files
10-06-2013 03:05:51 -- Analyzing item: 7-ntfs-undel\NTFS_DEL-NTFS\res1.dat
10-06-2013 03:05:51 -- Analysis Tools: analysis complete
10-06-2013 03:05:51 -- Final Status Update:
Total Elapsed Time: 0.00:00:00
Total Items Examined: 1
Total Items Added: 0
Total Indexing Completed:
Items Indexed: 0
Index Time: 0.00:00:00
Data Indexed: 6,156,389
Data Indexed (filt): 27,874
Index granularity set at: 4
Indexing completed since last update:
Items Indexed: 0
Index Time: 0.00:00:00
Data Indexed: 0
Data Indexed (filt): 0
Total Bytes Processed: 101
Drive E: Available (case): 176,565,828KB of 199,572,476KB
Drive C: Available (temp): 21,930,528KB of 81,919,996KB
Physical Memory Available: 909,040KB of 2,980,896KB
Virtual Memory Available: 1,337,676KB of 2,097,024KB
Page File Available: 1,335,076KB of 4,194,303KB

```
10-06-2013 03:06:10 -- Analysis Tools --  MD5: yes,  SHA1: no,  KFF: no,  Recheck all: no,  Index:
no,  Reindex all: no,  Entropy test: no
        Target files: currently highlighted files
10-06-2013 03:06:10 -- Analyzing item: 7-ntfs-undel\NTFS_DEL-NTFS\res1.dat
10-06-2013 03:06:10 -- Analysis Tools: analysis complete
10-06-2013 03:06:10 -- Final Status Update:
        Total Elapsed Time:       0.00:00:00
        Total Items Examined:     1
        Total Items Added:        0
        Total Indexing Completed:
          Items Indexed:        0
          Index Time:           0.00:00:00
          Data Indexed:         6,156,389
          Data Indexed (filt):  27,874
          Index granularity set at:  4
        Indexing completed since last update:
          Items Indexed:        0
          Index Time:           0.00:00:00
          Data Indexed:         0
          Data Indexed (filt):  0
        Total Bytes Processed:    101
        Drive E: Available (case): 176,565,828KB of 199,572,476KB
        Drive C: Available (temp): 21,930,528KB of 81,919,996KB
        Physical Memory Available: 907,488KB of 2,980,896KB
        Virtual Memory Available:  1,337,676KB of 2,097,024KB
        Page File Available:      1,334,612KB of 4,194,303KB
10-06-2013 03:52:28 -- Loading case
10-06-2013 03:52:28 -- Updating Overview Cache
10-06-2013 03:52:28 -- Filtering file list
10-06-2013 03:52:28 -- Initializing thumbnail view
10-06-2013 03:52:28 -- Resetting search terms list
10-06-2013 03:52:28 -- Building the indexed search results tree...
10-06-2013 03:52:28 -- Building the live search results tree...
10-06-2013 03:52:28 -- Building the bookmark tree
12-06-2013 02:56:45 -- Opening case
12-06-2013 02:56:48 -- KFF database being used:  none
12-06-2013 02:56:48 -- Examiner's Local Machine Setting is time zone used for file times (create,
modify, accessed) in file display and reports.
12-06-2013 02:56:48 --
12-06-2013 02:56:48 -- Loading case
12-06-2013 02:56:48 -- Building explore path tree
12-06-2013 02:56:48 -- Building explore, graphic and email path tree
12-06-2013 02:56:48 -- Updating Overview Cache
12-06-2013 02:56:48 -- Filtering file list
12-06-2013 02:56:48 -- Initializing thumbnail view
12-06-2013 02:56:48 -- Resetting search terms list
12-06-2013 02:56:48 -- Building the indexed search results tree...
12-06-2013 02:56:48 -- Building the live search results tree...
12-06-2013 02:56:48 -- Building the bookmark tree
12-06-2013 02:56:49 -- Opened case: E:\TESTETCC\teste\ using FTK version 1.81.6 build 10.04.02
12-06-2013 02:56:49 -- Examiner's Local Machine Setting is time zone used for file times (create,
modify, accessed) in file display and reports.
12-06-2013 03:07:02 -- Column settings saved:  1
12-06-2013 03:07:05 -- Column settings saved:  1
12-06-2013 03:07:05 -- Column settings changed to:  1
12-06-2013 05:12:12 -- Column settings saved:  1
12-06-2013 05:12:31 -- Column settings saved:  1
12-06-2013 05:12:37 -- Column settings saved:  1
12-06-2013 05:12:43 -- Column settings saved:  1
12-06-2013 05:12:49 -- Column settings saved:  1
```

12-06-2013 05:12:57 -- Column settings saved: 1
12-06-2013 05:13:03 -- Column settings changed to: 1
12-06-2013 06:03:05 -- Export File Options: Prepend archive name: yes; Append item number: yes; Append appropriate extension: no; Include email attachments: no; Export FTK's HTML view: yes; Export Filtered Text View: yes; Don't export Raw with filtered or HTML view: no.
12-06-2013 06:03:05 -- Export Files -- the following files were exported to H:\FORENSE TOOL KIT\RECUPERADOS\
ADS[35].txt from case path 7-ntfs-undel\NTFS_DEL-NTFS\mult1.dat
ADS[35] from case path 7-ntfs-undel\NTFS_DEL-NTFS\mult1.dat
dir1[37].txt from case path 7-ntfs-undel\NTFS_DEL-NTFS
dir1[37] from case path 7-ntfs-undel\NTFS_DEL-NTFS
dir2[38].txt from case path 7-ntfs-undel\NTFS_DEL-NTFS\dir1
dir2[38] from case path 7-ntfs-undel\NTFS_DEL-NTFS\dir1
frag1[31].dat.txt from case path 7-ntfs-undel\NTFS_DEL-NTFS
frag1[31].dat from case path 7-ntfs-undel\NTFS_DEL-NTFS
frag2[32].dat.txt from case path 7-ntfs-undel\NTFS_DEL-NTFS
frag2[32].dat from case path 7-ntfs-undel\NTFS_DEL-NTFS
frag3[39].dat.txt from case path 7-ntfs-undel\NTFS_DEL-NTFS\dir1\dir2
frag3[39].dat from case path 7-ntfs-undel\NTFS_DEL-NTFS\dir1\dir2
mult1[34].dat.txt from case path 7-ntfs-undel\NTFS_DEL-NTFS
mult1[34].dat from case path 7-ntfs-undel\NTFS_DEL-NTFS
mult2[40].dat.txt from case path 7-ntfs-undel\NTFS_DEL-NTFS\dir1
mult2[40].dat from case path 7-ntfs-undel\NTFS_DEL-NTFS\dir1
res1[41].dat.txt from case path 7-ntfs-undel\NTFS_DEL-NTFS
res1[41].dat from case path 7-ntfs-undel\NTFS_DEL-NTFS
sing1[33].dat.txt from case path 7-ntfs-undel\NTFS_DEL-NTFS
sing1[33].dat from case path 7-ntfs-undel\NTFS_DEL-NTFS
sing2[42].dat.txt from case path 7-ntfs-undel\NTFS_DEL-NTFS\[orphan]
sing2[42].dat from case path 7-ntfs-undel\NTFS_DEL-NTFS\[orphan]
12-06-2013 06:04:20 -- Started exporting files to H:\FORENSE TOOL KIT\RECUPERADOS
7-ntfs-undel\NTFS_DEL-NTFS\dir1\dir2\frag3.dat
12-06-2013 06:04:20 -- Failed to create destination directory H:\FORENSE TOOL KIT\RECUPERADOS\7-ntfs-undel\NTFS_DEL-NTFS\dir1: Impossível criar um ficheiro quando esse ficheiro já existe.

METODOLOGIAS E FERRAMENTAS DE PERÍCIA FORENSE UTILIZADAS EM SISTEMAS DE ARQUIVOS NEW TECHNOLOGIES FILE SYSTEM (NTFS): ARQUIVOS EXCLUÍDOS, OCULTOS E SEGMENTADOS.

Anderson do Rosário Francisco da Silva[1], Paulo João Martins[2]

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

andelerolxio@hotmail.com, pjm@unesc.net

Abstract: *This paper decribes the conclusion work submetted for obtaining the Degree of Bachelor of Computer Science at the UNESC University, whose goal was to apply techniques of computer forensics expert duplication, deleted data recovery, search for hidden evidence and analysis on filesystem New Technnologies File System (NTFS), conducting a case study with the tools. To achieve the same we performed a literature search, as well a fictional case study in a controleed environment simulating conducting a forensic computing, using the method SOP.*

Keywords: *Forensics Analysis, Computer Forensics, Computer Crime, NTFS File System.*

Resumo: *O presente artigo descreve o trabalho de conclusão de curso apresentado para obtenção de Grau de Bacharel em Ciência da Computação da Universidade do extremo Sul Catarinense, cujo objetivo foi aplicar técnicas de computação forense de duplicação pericial, recuperação de dados apagados, ocultos para busca e análise de evidências em sistemas de arquivos New Technologies File System (NTFS), realizando um estudo de caso com as ferramentas. Para realização do mesmo efetuou-se uma pesquisa bibliográfica, bem como um estudo de caso fictício em ambiente controlado simulando a condução de uma perícia forense computacional, utilizando-se da metodologia SOP.*

Palavras-chave: Peícia forense, Forense computacional, Crimes digitais, Sistema de arquivo NTFS.

1. Introdução

Cada vez mais é difícil de conceber que em tempos remotos não existia tantos meios tecnológicos (Computadores, *Smartphone*, *Ipad*, entre outros) que estão disponíveis hoje. Estes recursos se tornaram parte integrante na vida das pessoas, e o grande relevo desses meios tecnológicos é o computador.

Atualmente as pessoas usam computadores para se comunicar**,** guardar informações pessoais, fazer pesquisas na Internet e/ou até mesmo para execução de trabalhos profissionais. Com o aparecimento dessas tecnologias, surgiram também algumas técnicas de cometer crimes. Com isso os computadores e sistemas digitais são ferramentas e também alvos dos criminosos.

Em uma pesquisa divulgada pela consultoria Mi2g Intelligence Unit, em dezembro de 2004, foi constatado que o Brasil é o sétimo de dez países que mais possuem

hackers responsáveis pelas invasões de sites no mês de outubro de 2004. Além disso, o Brasil é considerado um dos países que tem mais *hackers* ativos no mundo, com 75% dos ataques às redes mundiais partindo do Brasil.

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

2. Segurança da Informação

Com a dependência do negócio aos sistemas de informação e com o aparecimento de novas tecnologias e outras formas de trabalho, como a venda de produtos eletrônicos, as redes virtuais privadas e os funcionários móveis, as empresas começaram a despertar para a necessidade de segurança, uma vez que se tornaram vulneráveis a um número maior de ameaças.

As redes de computadores, e consequentemente Internet mudaram as formas como se usam sistemas de informação. As possibilidades e oportunidades de utilização são muito mais amplas que em sistemas fechados, assim como riscos à privacidade e integridade da informação. Portanto, é muito importante que mecanismos de segurança de sistemas de informação sejam projetados de maneira a prevenir acessos não autorizados aos recursos e dados destes sistemas (LAURENÇO, 2004).

Segurança de informação é a proteção de informações, sem se preocupar onde esteja armazenada (no papel, na memória do computador ou em um dispositivo de armazenamento). Um computador é considerado seguro caso haja qualquer autenticação de que é capaz de exercer exatamente as mesmas funções. Todo usuário de computador almeja, no que diz respeito à segurança de dados, que as informações armazenadas, nem que por algumas semanas, permaneça, sem que outros usuários não autorizados acessem o mesmo conteúdo. O usuário espera que suas informações esteja disponíveis no momento e local que ele determinar que seja correta e mantida fora do alcance e das vistas de pessoas não autorizadas (DIAS, 2000).

3. Perícia Forense Computacional

A perícia forense aplicada à informática, que também é conhecida como computação forense, forense computacional, criminalística computacional, forense digital, investigação eletrônica e perícia eletrônica, é a aplicação de conhecimentos em informática e técnicas de investigação com a finalidade de obtenção de provas (FREITAS, 2006).

Segundo Melo (2009), a Computação Forense também é definida como uma área da Ciência da Computação que se desenvolve gradualmente para acolher à demanda oriunda da área da Criminalística, e também como uma parte da Criminalística que se apropria de fundamentos da Ciência da Computação.

A perícia forense é uma área relativamente nova e tornou-se uma prática investigada importante tanto para as empresas quanto para a polícia. Utiliza de métodos científicos para identificar, preservar, analisar e documentar evidências localizadas em computadores e outros dispositivos eletrônicos (FREITAS, 2006).

3.1 Metodologias Forenses e Investigativas

Ao iniciar o procedimento de perícia em um equipamento questionado, o perito deve fazer a escolha de qual metodologia será empregada em seu trabalho: tem a *Live Forensics* ou a *Post Mortem Forensics,* que foram abordados anteriormente, ou ainda, em alguns casos, usam-se ambas (CARRIER, 2006).

3.1 Metodologia SOP

Metodologia *Standard Operating Procedures* (SOP), criada pelo *Scientific Working group on Digital Evidence* (SWDGE) que é o representante norte-americano na *Organization on Computer Evidence* (IOCE). Objetivando a criação de um documento de amostra de trabalho que as organizações podem utilizar como um modelo para reproduzir sua própria documentação de Procedimentos Operacionais Padrão, e é constituída por seis etapas de acordo com (SWGDE, 2012, tradução nossa):

a) **coleta da prova:** a partir do responsável pela investigação, consultar que ferramentas deve-se levar para o local da ocorrência. Sempre que for impossível remover as evidências do local, promover uma cópia ou imagem dos dados seguindo os procedimentos locais. Os suspeitos devem ser afastados do local do crime depois de certificado que os mesmos não estão em posse de provas em potencial;

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

c) **preparação do equipamento** - equipamento aqui é referenciado como sendo o hardware e software utilizados pelo examinador para que se efetue a imagem forense e posteriormente a análise. Preferencialmente, devem ser usados equipamentos padronizados;

d) **imagem forense** - documentar o estado atual da prova, devem-se tomar medidas para que os itens não sejam expostos. Hardware ou Software devem ser utilizados para garantir que a prova não seja alterada, e as mídias devem ser devidamente preparadas para receber a cópia forense para assegurar o não entrelaçamento dos dados;

e) **exame/análise** - para análise devem-se considerar a urgência com que o requisitante necessita da informação, que exames forenses podem ser executados na evidência, quais os itens que oferecem melhor escolha em termos probatórios. Realizar a análise diretamente na evidência coletada não é seguro, os exames devem ser conduzidos em cópias forenses;

f) **documentação** - a documentação de manipulação de provas deve incluir cópia da autorização judicial, cadeia de custódia, contagem das provas a serem periciadas, dados sobre a condição da evidência após ser recebida pelo examinador, uma descrição das evidências, e comunicações com o caso.

A documentação do exame deve em casos específicos, conter detalhes que permitam outro perito forense competente na mesma área de especialização ser capaz de identificar o que foi feito e chegar aos resultados de forma independente;

g) **relatórios** - os relatórios deverão satisfazer aos requisitos do examinador, estes deverão abordar as necessidades do solicitante, com o objetivo de fornecer ao leitor todas as informações relevantes de forma clara e concisa;
h) **revisão** - deve-se ter uma política escrita contendo os protocolos para revisão técnica e administrativa.

3.2 Alguns Lives CDs Para Perícia Forense

Um live CD roda um sistema operacional sobre um ramdisk, isto é, um disco virtual é criado usando parte da memória RAM. O live CD possibilita fazer o uso de um sistema operacional sem ter a necessidade de este estar instalado, dependendo apenas de requisitos básicos como um drive CD e não exigindo muita memória (MORIMOTO, 2005).

3.2.1 Deft 7.2

É uma distribuição para perícia composta de um GNU/Linux e DART (Digital Advanced Response Toolkit) suíte dedicada às atividades digital forensics3 e intelligence4. A primeira versão do Linux DEFT foi introduzido em 2005, graças ao Curso de Computação Forense da Faculdade de Direito da Universidade de Bolonha na Itália, a figura 9 ilustra o ambiente de trabalho da mesma (FRATIPIETRO; ROSSETI, 2012, tradução nossa).

3.2.2 Backtrack 5

É uma distribuição de segurança Linux que contém um ótimo conjunto de ferramentas necessárias para executar uma avaliação completa de segurança de sistemas, redes e aplicações. É importante realçar que pode ser configurado de diferentes formas, como a criação de um Live CD ou montar um drive USB de inicialização e executá-lo em um ambiente vivo, também é possível instalar em uma máquina virtual (VM) ou ser instalado diretamente em um disco rígido e inicializar a ele como o sistema operacional principal. Portanto, cada método tem as suas vantagens e desvantagens, mas, em casos de realizações constantes de avaliações e testes é recomendável que se crie um BACKTRACK 5 por meio de uma máquina virtual, como pode ser observado na figura 11(HACKING9-TEAM, 2012, tradução nossa).

3.3 Kit de Ferramentas para Exame Forense Computacional

Os investigadores precisam de ferramentas de software para visualização de arquivo, imagens de disco, arquivos de descompactação, identificação de arquivos conhecidos, realizando pesquisas de cadeia e acessar os metadados do arquivo (BANSOD, 2009, tradução nossa).

Existem várias ferramentas que permitem realizar uma análise forense em sistemas de arquivos NTFS – arquivos excluídos, ocultos e segmentados auxiliando o perito, como: analyzeMFT, Digital Forensics Framework, Autopsy, Forense Tool Kit, Encase, recoveryMyFiles, FDTK, entre outras ferramentas que não são voltadas para perícia forense como: iCare Data Recovery Free, DiskDigger, Lazesoft Data

Recovery, Power Data Recovery, Recuva, Easeus Deleted File Recovery, Wise Data Recovery, Glary Undelete, Data Recovery Wizard Free, NTFS Undelete.

Para o presente trabalho foram escolhidas ferramentas *open source*, isto é, softwares disponibilizados sob licença de código aberto, e softwares livres, se bem que não tenham disponibilizado o seu código fonte, estas se encontram gratuitamente distribuídas. É vantajoso trabalhar com software livre, por uma única razão, o baixo custo de aquisição. Porém, segundo Argolo (2005) os benefícios de se trabalhar com softwares de código aberto são:

a) **baixo custo:** softwares sob uma licença de código aberto são usualmente são grátis, ou o custo de aquisição é muito sumaria;

b) **segurança:** a fluente disponibilidade do seu código fonte para os usuários, denota um melhoramento regular;

c) **continuidade:** mesmo que os responsáveis do software original deixem de o atualizar, esta pode ser feita pela comunidade, sendo que, o código fonte poderá ainda ser usado em outros projetos;

d) **flexibilidade:** o código fonte do software pode ser alterado, de acordo com a satisfação do seu usuário, e características específicas.

As ferramentas escolhidas e que na qual serão melhor apresentadas, são: iCare Data Recovery Free, DiskDigger, RecoveryMyFiles, Lazesoft Data Recovery, Power Data Recovery, Recuva, Easeus Deleted File Recovery, Wise Data Recovery, Glary Undelete, Data Recovery Wizard Free, Digital Forensics Framework , Autopsy. Todas elas são gratuitas, algumas possui o seu código fonte disponível e são usadas por peritos durante as suas pesquisas.

3.3.1 iCare Data Recovery Free

A primeira ferramenta a ser usada foi a iCare [6]Data Recovery Free, programa simples e gratuito de recuperação de informações (dados), apresenta uma forma fácil e prática de recuperação de arquivos apagados do HD (disco rígido), *pendrive*, entre outros. Permite recuperar arquivos excluídos acidentalmente, excluídos da lixeira, excluídos por vírus, partição apagada, acidente de software, entre outros. Recupera qualquer arquivo como fotos, documentos, mp3, funciona com qualquer tipo de mídia de armazenamento, cartão SD, camera digital, entre outros, figura 11 ilustra a ferramenta (ICARERECOVERY, 2003, tradução nossa).

3.3.2 DiskDigger

DiskDigger[7] é um programa capaz de recuperar arquivos perdidos a partir do disco rígido, cartões de memória, *drives flash* USB e *pendrives*. Ele pode recuperar documentos (DOC, DOCX, XLS, PPT, PDF, entre outros), fotos (JPG, PNG, GIF, BMP, entre outros), musicas (MP3, WMA, M4A, WAV, entre outros), vídeos (WMV, MOV, 3GP, RMVB, MKV, MPEG, entre outros) e muitos outros formatos de arquivos. O software tem dois (2) modos de operação “Pesquisa funda” e “Pesquisa Profunda”. O primeiro faz uma verificação simples e rápida, envolvendo filtragem pelo nome e tamanho dos arquivos recuperados, porem a segunda opção faz a verificação e digitalização do HD inteiro, vestígios de determinados, o que aumenta

[6] http://www.icare-recovery.com/about-us.html
[7] http://diskdigger.org/

as chances de recuperação de informações excluídas há mais tempo, por outro lado, é bem mais demorado, como observa-se na figura 12 (DISKDIGGER, 2013, tradução nossa).

3.3.3 RecoveryMyFiles

RecoveryMyFiles ou recuperação de dados em português, é um software de recuperação de arquivos apagados a partir da lixeira do Windows, perdidos ao ser formatado ou em uma reinstalação de um sistema operacional, disco rígido, ou removidos por infecção de vírus, infecção por *trojan* que é o mais conhecido, ou por encerramento indevido do sistema ou mesmo por falha de um software, que pode ser visualizado na figura 13. É compatível com Windows (2003, XP, Vista, Windows 7, Windows 8) e trabalha com FAT 12, FAT16, FAT 32 + sistemas de ficheiros do Mac. (RECOVERMYFILES, 2013, tradução nossa).

Inclui um apoio específico para mais de 200 tipos de arquivos. Listagem das características fortes que a ferramenta apresenta para os arquivos (RECOVERMYFILES, 2013, tradução nossa):

g) Recupera arquivos mesmo tendo esvaziado a lixeira;

h) Recupera arquivos após uma formatação de forma acidental;

i) Recupera discos com falhas;

j) Resgata arquivos após falha de particionamento;

k) Recupera documentos, fotos, música e e-mail;

Recupera *FAT*, *exFAT*, *NTFS*, *HFS*, *HFS +.*

3.3.4 Lazesoft data recovery

A ferramenta de recuperação Lazesoft concede aos usuários domésticos e à empresas, soluções completas para recuperar arquivos apagados ou perdidos devido à uma reformatação ou corrupção de um disco rígido, vírus ou infecção de Trojan, por encerramento inesperado do sistema ou por falha de um software. Com uma forma fácil de usar a interface e o mais potente software de recuperação e dados, pode-se usar a ferramenta para recuperar seus dados, pode pre-visualizar os arquivos apagados enquanto a varredura estiver sendo operada (LAZESOFT, tradução nossa, 2012).

4. Estudo de Caso de Perícia Forense em Arquivos Excluídos, Ocultos e Segmentados em uma Partição NTFS.

No presente capítulo são apresentados os estudos de casos na obtenção de avaliação de documentação da perícia forense computacional em arquivos na partição NTFS, bem como a parte prática do projeto de pesquisa, objetivando buscar uma análise digital, fazendo a demonstração e a utilização das ferramentas forenses e não só, o conhecimento adquirido na teoria, enfocando a busca, coleta e análise de evidências em ambientes NTFS.

Para ter acesso às máquinas disponíveis, com Internet, que na qual são reservados para os acadêmicos da comunidade interna (não só do curso de Perícia), os mesmo devem ter em mãos o código de matrícula que é acompanhado da senha no momento em que for efetuar o login[8]

[8] Login é o ato de logar-se na rede informando seu nome de usuário e senha (MORIMOTO, 2003).

Escolheu-se de forma aleatória dois laboratórios: os laboratórios 1 e 2 do Bloco A. Além disso, reservou-se 5 computadores em cada sala para serem devidamente analisados. Neste contexto, é importante ressaltar que a forma correta de se fazer uma perícia forense neste tipo de caso, é analisar um-a-um os computadores da instituição. Por esta razão, e, por se tratar de uma demonstração de casos, optou-se por escolher um modelo de todos os computadores.

Dessa forma, foi realizada uma simulação com este trabalho objetivando fazer menção em quais benefícios poderão ser obtidos aplicando este estudo à perícia forense computacional nos seguintes casos:

a) arquivos excluídos;

b) arquivos ocultos;

c) arquivos segmentados.

Para facilitar a compreensão das fases realizadas, simula-se a seguinte ocorrência:

a) Supõe-se que o fulano de tal (usuário qualquer), usando uma das máquinas dos laboratórios da UNIP tenha excluído, ocultado ou corrompido um arquivo importante de forma acidental ou propositada, sendo que o mesmo não havia feito um Backup, isto é, uma cópia de segurança desse arquivo. Qual o procedimento a ser seguido para a sua recuperação? Será que é possível recuperar este mesmo arquivo perdido (por engano ou não)? Será que é possível recuperar informações de um disco rígido formato? E ainda, como recuperar uma partição apagada indevidamente?

4.1 Metodologia

Para realizar este estudo, foi feito um levantamento bibliográfico em livros, relacionados a crimes digitais em ambientes NTFS, por meio de Internet em banco de dados, como trabalhos científicos, trabalhos de monográfica, dissertações, artigos de forma a obter informações suficientes sobre tema e, quais procedimentos ou metodologias serão aplicados e/ou investigadas no momento em que for feita a perícia. A maior parte da bibliografia usada neste trabalho foi traduzida da língua inglesa tendo em conta a insuficiência de material em português.

Estudo das ferramentas forenses Autopsy, Digital Forense Framework (DFF), Forense Tool Kit (FTK), estudo de outras ferramentas de recuperação de arquivos excluídos e segmentados utilizadas no trabalho, 5.2, a fim de serem aplicados em dispositos de armazenamento com sistemas de arquivos NTFS.

É importante salientar que o *Dos* lê (reconhece) apenas FAT32 do *MS-Dos 7* ou superior, não lê NTFS. Algumas versões mais antigas do Windows não lê essa partição. Existem muitas vantagens em se utilizar NTFS sob o FAT32, sendo que o NTFS oferece suporte a segurança de dados, susporte a compreenção de dados, isto é, compactação de dados e suporte para arquivos superior a quatro Gigabyte, entre outros.

Por final realizou-se uma simulação pericial com o objetivo de demonstrar mediante a um acontecimento o uso de alguns softwares de perícia e de recuperação informações, e metodologias na busca evidências.

4.2 Estudo de Caso

Nesta fase será apresentado um estudo de caso, auxiliando, sob meios práticos na percepção de quando e como deve-se usar as ferramentas forense e, alem disso, qual a confiabilidade que as mesmas propõem alcançar tendo em conta o seu escopo.

4.1.1 Metodologia Forense

O presente estudo de caso foi proposto pelo especialista forense Brian Carrier. Montado pelo mesmo e simula um ambiente real favorável para análise.

Trata-se da criação de um caso e uma imagem forense para teste, apresentado em 29 de fevereiro de 2004. Esta imagem, Raw (dd), é um sistema de arquivos NTFS com tamanho de 6 MB com oito arquivos apagados, dois diretórios apagados e um fluxo de dados alternativo também apagado. Os arquivos variam de arquivos residentes, arquivos de *cluster* único e vários fragmentos. Com suas Estruturas de dados modificadas para impedir o processo de recuperação dos mesmos. Eles foram craidos no Windows XP e posteriormente excluídos no XP. A imagem foi liberada sob a General Public License (GPL)

O autor aponta como proposito do caso de estudo 11 etapas e também uma tabela onde encontram-se os arquivos que devem ser recuperados, seus tamanhos e seus respetivos MD5:

l) Consegue observar qualquer um dos nomes de arquivos excluídos? Quais?

m) Consegue recuperar o arquivo res1.dat? Ele tem o mesmo MD5?

n) Consegue recuperar o arquivo sing1.dat? Ele tem o mesmo MD5?

o) Consegue recuperar a pasta3 / arquivo sing2.dat? Ele tem o mesmo MD5?

p) Consegue recuperar o arquivo mult1.dat? Ele tem o mesmo MD5?

q) Consegue recupear o mult1.dat: file ADS? Ele tem o mesmo MD5?

r) Consegue recuperar o dir1 / arquivo mult2.dat? Ele tem o mesmo MD5?

s) Consegue recuperar o arquivo frag1.dat? Ele tem o mesmo MD5?

t) Consegue recuperar o arquivo frag2.dat? Ele tem o mesmo MD5?

u) Consegue recuperar o dir1 / dir2 / frag3.dat? Ele tem o mesmo MD5?

v) As datas mostradas correspondem a de 29 de fevereiro de 2004?

O conteúdo do relátorio aprensentado por Brian pode ser observado a partir da figura 1.

Definida assim a metodologia a ser utilizada para a realização da pesquisa, a SOP, onde a mesma está compreendida em 7 etapas conforme pode-se observar na figura 12. Vale realçar que a escolha deste método se deu pelo fato de ser mais aceite em comunidades brasileiras e que, também pode, se for o caso, dar condições de ser aceite como prova em um ambiente judicial fazendo-se acompanhar de relatórios periciais oficiais.

Figura 1 – Fluxograma da metodologia SOP

Fonte: SWGDE (2006).

4.1.1.1 Análise e resultados do dispositivo para pericia forense

Na primeira fase do desenvolvimento, inseriu-se arquivos no dispositivo de armazenamento USB que antes foi devidamente formatada com sistema de arquivo NTFS. Alguns destes arquivos foram selecionados e excluídos e ocultados propositalmente, como foi suposto no estudo de caso da pesquisa. Utilizou-se algumas ferramentas forense neste momento para ser feita a análise do mesmo.

Como já foi mencionado anteriormente no trabalho, existem várias ferramentas de investigação forense e de recuperação de informações, dos quais optou-se por utilizar o kit de ferramentas forense para fazer a descrição dos casos.

Os softwares mencionados na metodologia (5.1) foram selecionados por fazerem parte do kit de ferramentas forenses das mais utilizadas no pela comunidade cientifica, como é o caso do Autopsy, e por possuírem particularidades de extrema confiança em relação a outras, sendo que também são utilizadas por peritos profissionais ou mesmo por acadêmicos da Unesc.

4.1.2 Coleta de Prova

Tendo conhecimento de que o caso provem de um ambiente estudo, o computador para exame já se encontrada em perfeitas condições de armazenamento, isolou-se área de trabalho, foram coletadas todas as evidências de formas a garantir a integridade das informações contidas no no dispositivo, ou seja, para que não corra nenhum tipo de risco de perda dos dados. A coleta da prova foi realizada com a ferramente forense FTKImager.

Para que não exista nenhuma deterioração e substituição das evidências, as mesmas devem ser coletadas com a maior precaução possível, havendo atenção com os softwares a serem usados para que estes não alterem o estado nem as informações encontradas no computador.

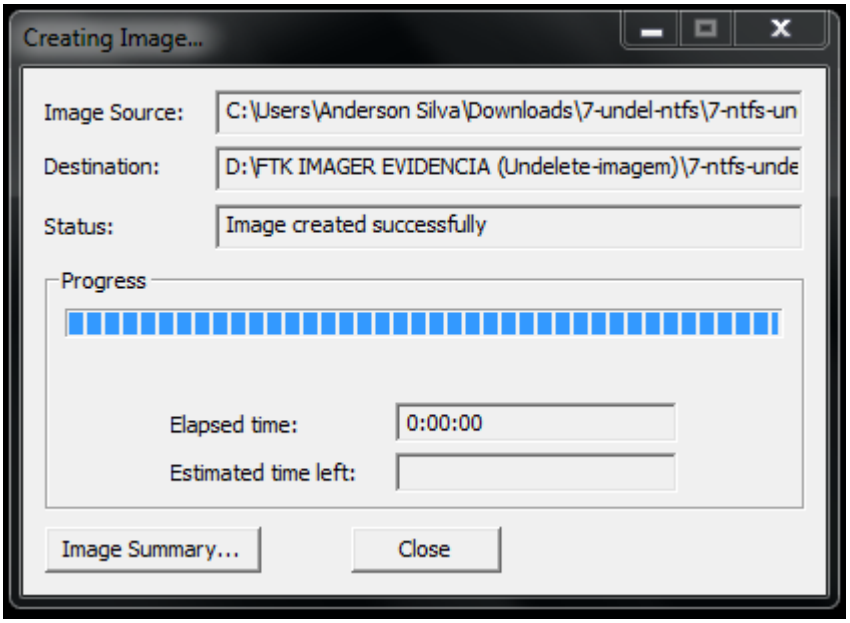
4.1.3 Preparação do equipamento

Para que fosse possível prosseguir com a pesquisa forense, foi necessário a criação de condições seguras sem o risco de perda dos dados. Assegurando-se de que o ambiente esteja seguro, as condições recaem em torno de software e harware.

4.1.4 Criação da Imagem forense

A ferramenta FTKImager foi utilizada para fazer a recolha da imagem do dispositivo em questão, e posteriormente armazenada em um disco rígido externo com a capacidade de 500 GB anteriormente formatada. Ela nos oferece quatro opções: a imagem não processada – *Raw (dd)* , *Smart Expert Witness (E01)* e a *Advanced Forensic Format (AFF).*

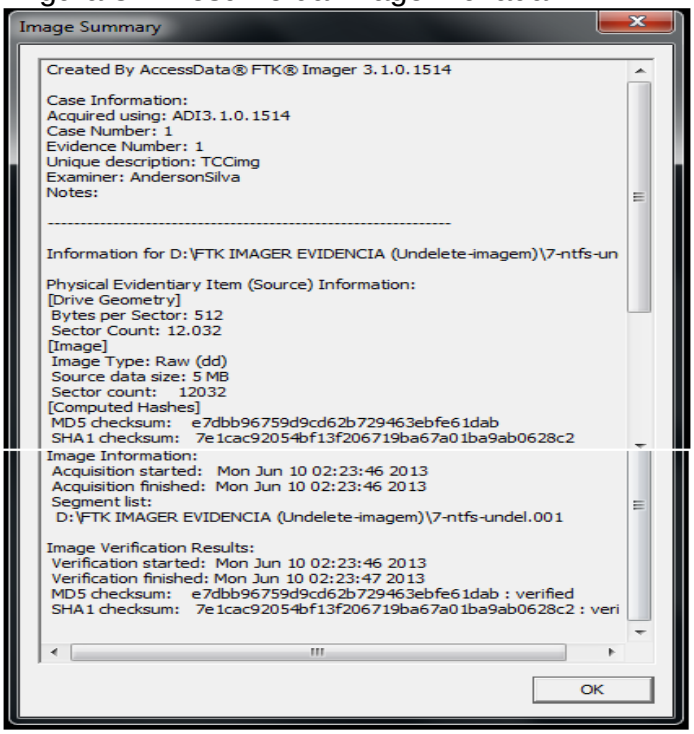
Figura 2 – Criação da imagem



Fonte: Do autor.

Optou-se por escolher a extensão padrão da ferramenta, a *Expert Witness (E01)* por ser proprietário do Encase, sendo que a mesma utiliza compatação, tratamento de erros e sem perdas. O resumo da criação dessa imagem está disponível na figura 3.

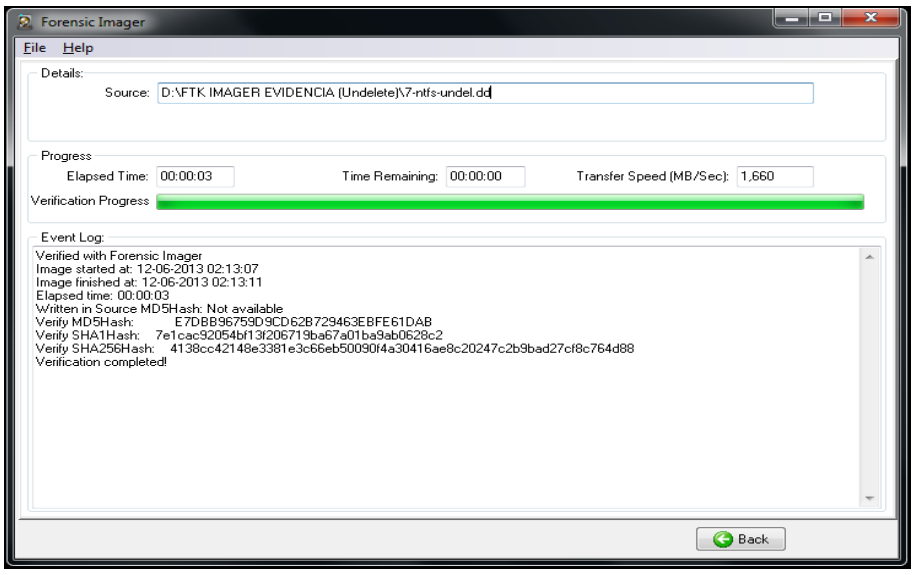
Figura 3 – Resumo da imagem criada



Fonte: Do autor.

Conforme determina a pesquisa de perícia forense, a imagem em análise, após a sua coleta, o mesmo deve passar pelo processo de geração de um código *Hash*, para este caso foi utilizado a ferramenta RecoveryMyfile, onde a mesma possui uma ferramenta interna para geração de código *hash* de um drive físico, lógico ou diretório da imagem. A figura 4 pode ilustrar melhor o mesmo.

Figura 4 – Geração do código Hash da imagem com o Forensic Imager



Fonte: Do autor.

É possível verificar a partir do resumo da imagem, conforme a figura figura 14, e que na qual foi gerado um código Hash dessa imagem, figura 15 como confirmação, que a imagem não sofreu nenhum tipo de alteração e, verifica-se também que o código Hash é o mesmo da imagem inicial.

4.1.5 Exame e Análise dos dados

Para que se cumprisse a análise da imagem e, como estabelece os procedimentos propostos pela metodologia SOP, realizou-se uma duplicação da imagem, pois, se por ventura algum imprevisto aconteça se consiga recorrer à imagem coletada anteriormente e por conseguinte prosseguir com a pesquisa forense.

4.2 Apresentação, Análise dos Dados e Discuções

Como trata-se de um estudo de caso de simulação de ambiente academico, abdicou-se em fazer o levantamento perante as pessoas que podem estar envolvidas no ato (onde as mesmas identificaram o acontecimento e com isso culminou com as consequências do crime digital) por meio de um interrogatório, informações valiosas, objetivando ao perito uma melhor análise dos fatos que aparecessem durante a investigação.

À aquisição das especificações sobre Hardware e Software dos computadores a serem feitas as análises, para este tipo de casos de perícia, é importante conhecer. Sendo assim, acessou-se o programa – Ferramenta do Sistema – que pode ser encontrado no menu Iniciar *(Todos os programas/Acessórios/Ferramentas do Sistema)*, disponível no Windows 7. Apresentação da configuração de hardware de todos os computadores, abaixo:

a) Memória RAM instalada: 4 GB;

b) Disco Rígido: 320 GB – possuí três partições (C:\, D:\, E;\);

c) Processador: Intel Core 2 Duo;

d) Velocidade do Processador: 2,26 GHz;

e) Número de Processadores: 2;

f) Número de Núcleos: 2;

g) Placas de áudio, vídeo e rede on-board

As seguintes especificações de software, abaixo:

a) Windows 7, Service Pack 1.

Com as especificações já feitas, pode-se observar que a capacidade do HD é de 320 GB, particionadas em: C:\ *com 78.1 GB*, D:\ *com 29.5 BG* e o E:\ *com 190 GB*. Todas as partições possuem o sistema de arquivos NTFS.

A escolha do kit de ferramentas *open source* que se utilizou recai devido ao fato de apresentarem maior confiabilidade, conforme apresentado por seus fabricantes, dando uma maior credibilidade ao trabalho do perito para recuperar arquivos na partição NTFS, são eles:

a) iCare Data Recovery Free;

b) Lazesoft Data Recovery;

c) RecoveryMyFiles;

d) MiniTool Power Data Recovery;

e) Easeus Data Recovery Wizard Free;

f) DiskDigger;

g) Easeus Deleted File Recovery;

h) Wise Data Recovery;

i) Glary Undelete;

j) Recuva;

k) NTFS Undelete.

Para além desses, foram usados utilitários nativos do sistema operacional Windows como a linha de comandos, que também fazem parte do kit de ferramentas.

Primeiramente utilizou-se estas ferramentas, para recuperar arquivos excluídos da lixeira ou de forma permanente na busca por evidências. Tanto os softwares de perícia quanto os softwares *open source* possuem módulos de recuperação, para tal foi realizado um teste com cada uma das ferramentas tendo como propósito a recuperação desses arquivos, resgatando assim os valores a serem apresentados como prova da ocorrência de um crime digital a ser analisado, porem diferenciados.

Os testes foram realizados em função ate da escolha dos softwares usados durante o processo de perícia forense, como sua credibilidade e eficiência no quesito funcional. No momento em que fez-se as comparações, a ideia foi verificar quais dos softwares consegue resgatar uma quantidade maior de arquivos.

Dentre os onze (11) softwares de código fonte aberto mencionados, optou-se por escolher 5 deles a serem utilizados. A escolha dos mesmos deu-se por ser gratuito e software livre, embora alguns deles necessitam de licença para recuperação dos arquivos. Esses são alguns dos motivos que chamaram a atenção na escolha dos softwares.

5. Resultados Obtidos

De acordo com as etapas de coleta e análise das evidênias coletadas, o perito tem a capacidade de desenvolver um relatório contendo informações sobre o sistema periciado, abordando as evidências encontradas, que visam dar informações relevantes ao perito e atingir o objetivo da perícia em questão.

Por se tratar de um trabalho com fins de aprendizado e que pretende dar um contribuição bibliográfica num modo geral, as etapas, em geral, foram produzidas de formas a que os mais leigos ná área da computação pudessem perceber todo o processo que envolve uma pericia computacional, e torna-se inprescindivel aprensetar as informações aqui.

O estudo de caso apresentou objetivos visando aferir o estado da eficiência das ferramentas forenses usadas. Na recuperação dos dados apagados, foi feito de maneira bastante prática, a demonstração e recuperação de um número maior de informações.

Conseguiu-se recuperar um total de arquivos controlados, ou seja, que foram selecionados e excluidos para teste com todas as ferramentas. O que demostra que as ferramentas são tão eficientes.

Mesmo a comunidade cientifica de desenvolvedores, ainda não conseguiram colocar disponível no mercado uma que conseguisse recuperar arquivos apagados permantentemente.

6. Conclusão

A medida que os crimes praticados por meio de computadores vão aumentando, também cresce a necessidade de resposta da utilização da perícia forense no combate a esse tipo de crimes digitais. No Brasil, muitas das evidências digitais documentas e as metodologias criadas internacionalmente são aceites pela comunidade científica e vêm sendo usadas com uma maior brevidade em processos criminais, objetivando buscar um julgamento correto do acusado. Tornando-as assim importantes e cada vez mais eficientes em relação às provas que são encontradas proporcionadas pelo trabalho do perito.

Baseados nestes fatos, os mesmos procedimentos empregados durante o decorrer da perícia, precisam ser claras e objetivas procurando sempre relatar a verdade, sem comprometer ou ocultar informações pertinetes ao relatório final. O uso de ferramentas livres e técnicas avançadas por parte dos criminosos, sendo que o mesmo foi demonstrado através deste trabalho, torna-se necessário que os peritos estejam capacitados para conseguir combater e disseminar o avanço de crimes digitais que vêm acontecendo com bastante frência nos diversos ambientes computacionais.

Um dos pontos negativos que encontrou-se durante o trabalho é a falta de bibliográfia baseado na área da perícia em Língua Portuguesa, bem como a carência de padrões metodologicos e principalmente a falta de versões mais recentes das princípais ferramentas forenses e de recuperação sem a obtenção das respectivas licenças para que fosse possível resgatar o maior número de arquivos excluídos no ato pesquisa. Não se obteve a versão profissional (paga) das ferramentas específicas por se tratar de um estudo de caso baseado em ambiente acadêmico.

Para concluir, estima-se que o presente trabalho irá contribuir para diminuir a carência de referências bibliográficos na área, sendo que o memso problema foi aprensentado na justificativa. Por ser tão constante as formas como os crimes digitais se proliferam nos dias de hoje, surge a ideia, como trabalhos futuros, de se aplicar a perícia forense computacional em um ambiente baseado em Mac OX empregando as metodologias aplicadas no trabalho.

Referências

ARGOLO, Frederico Henrique Böhm. **Análise Forense em sistemas GNU/Linux.** Universidade Federal do Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799**: Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

BANSOD, Tularam. **Basics Of Digital Forensics: How Hackers Hide Data in Computares**. 2009. Disponível em:

<http://www.miel.in/pdfs/Digital%20Forensics.pdf> Acesso em: 08 de out. 2012.

BERTOGLIO, Daniel Dalalana. **Perícia Forense: Proposta de Uma Metodologia**

de Coleta de Indícios Para Ambiente Windows. 2008. Trabalho de Conclusão de Curso (Graduação) - Curso de Ciência da Computação, Departamento de Instituto de Ciências Exatas e Tecnológicas, Centro Universitário Feevale, Novo Hamburgo, 2008.

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

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

CARRIER, B. **File System Forensic Analysis**. 2006.

CARRIER, B. **Risks of live digital forensic analysis:** Commun. ACM, 49 No.2: 56–61. 2006.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em Informática e de Informações.** 2a ed. São Paulo: Editora SENAC, 1999.

CERT.br. CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Incidentes Reportados ao CERT.br—Julho a Setembro de 2012.** 2012. Disponível em: < http://www.cert.br/stats/incidentes/2012-jul-sep/weekdays-incidentes.html> Acesso em: 10 nov. 2012, 20:10:15.

ELEUTERIO, P. M. S; MACHAD, M. P. **Desvendando Computação Forense**. São Paulo: Novatec, 2011.

FARMER, Dan; VENEMA, Wietse. **Perícia Forense Computacional.** São Paulo: Pearson Prentice Hall, 2007. 190 p.

FARMER, Dan; VENEMA, Wietse. **Perícia Forense Computacional – Teoria e Prática Aplicada** – Como investigar e esclarecer ocorrências no mundo cibernético. São Paulo: Perarson Prentice, 2007.

FRATEPIETRO, Stefan, ROSSETI, Sandro. **DEFT**: Manual de uso. Disponivelem < http://www.deftlinux.net/doc/EN-deft7.pdf> Acesso em: 6 de Janeiro. 2012, 14:05

FREITAS, Andrey Rodrigues de. **Perícia Forense Aplicada à Informática**. Trabalho para o curso de Pós – Graduação “*Lato Sensu*” em Internet Securit IBPI/ Janeiro 2003.

GOUVÊA, Sandra. **O direito na era digital: crimes praticados por meio da informática.** Rio de Janeiro: Mauad, 1997.

HACKING9-TEAM. **Hacking On Demand**. The Guide to Backtrack. Disponível em: <http://www.backtracklinux.org/documents/Hakin9_On_Deman_03_2012_Teasers.pdf>. Acesso em: 02 Abr. 2013.

KENT, Karen; CHEVALIER, Suzanne; GRANCE, Tim; DANG, Hung. **Guide to Integrating Forensic Techniques into Incident Response**. Gaithersburg. NIST. 2006. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>. Acesso em: 03 Outubro. 2012, 01:00 PM.

LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional**. Campinas – SP: Millennium Editora, 2006.

LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional.** 2. ed. São Paulo: Atlas, 2011. 166 p.

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

MARCHIORI, Rafael Bernardes. **Estudo de Ferramentas para Análise Forense Computacional**. Curso de Analise de Sistemas. Universidade São Francisco. Itatiba – São Paulo – Brasil. Junho de 2006.Disponível em <http://www.hardware.com.br/livros/redes/denial-service-dos.html> Acesso em: 17 Nov de 2012, 00h40:30.

MELO, Sandro. **Computação Forense com Software Livre.** Rio de Janeiro: Altas Books, 2009. 152 p.

MORIMOTO, Carlos E. **Guia do Hardware:** Redes, Guia Prático 2ª Ed. 2008.

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.

CAPÍTULO 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.