UNIVERSIDADE DO EXTREMO SUL CATARINENSE - UNESC

CURSO CIÊNCIA DA COMPUTAÇÃO

AGUINALDO GREGÓRIO CRISTIANO

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

CRICIÚMA, DEZEMBRO 2011

AGUINALDO GREGÓRIO CRISTIANO

FORENSE COMPUTACIONAL: FERRAMENTAS E METODOLOGIAS PARA RESPOSTA A INCIDENTES, ESTUDO DO CASO "HELIX 3"

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

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

CRICIÚMA, DEZEMBRO 2011

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

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

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

Banca Examinadora:

Prof. MSc. Paulo João Martins (UNESC)
Orientador

Prof. Esp. Sergio Coral

Prof. Esp. Fabrício Giordani

A Deus, pelas bênçãos e dádivas que tem me concedido e aos meus pais, pela maneira sábia, dedicada e carinhosa como têm me conduzido.

AGRADECIMENTO

A Deus pelas bênçãos que me tem concedido até agora, pois ele é meu guia nesta empreitada: a vida.

Agradeço especialmente aos meus pais, Joaquim José Cristiano e Maria Paula Cristiano, pelos conselhos sábios, pela maneira inteligente e sábia como me têm conduzido, o carinho e toda atenção dispensada, eles são responsáveis pelo que sou hoje. A senhora Conceição Webba, que tem sido como uma segunda mãe para mim, nem sequer tenho palavras para agradecer: muito obrigado.

À Sociedade Nacional de Petróleos de Angola (Sonangol), deixo aqui patente o meu muito obrigado pela oportunidade concedida para que eu possa contribuir de maneira sábia para o desenvolvimento de Angola. A Sianorego, agradeço pela prontidão que sempre teve em tratar dos meus assuntos quer sejam acadêmicos, de saúde, e tantos outros, especialmente para as senhoras Marcela Alves, Paula Donda, e os senhores Fabrício e Luciano Rego. A UNESC - Universidade do Extremo Sul Catarinense (direção, professores e funcionários), especialmente a professora Ana Claudia, Margareth, professores Sérgio Coral e Paulo Martins, agradeço com a mais alta estima. Agradeço ao meu irmão Aurio Cristiano pelas provações a que me submete, pois têm sido de muito aprendizado, as minhas irmãs Rita Cristiano e Wilma Cristiano pela companhia e bons momentos que me proporcionaram no decorrer da formação, a Laureth Spinola por me aturar e ser sempre compreensível comigo, e ao meu mano Celio Filipe: obrigado. Aos meus amigos, Antônio Gaspar (Miro), Sidney Webba, Ferraz Manuel, Heidy Rhamos e Aniceto de Carvalho agradeço pela força e companheirismo. A todas as pessoas que, direta ou indiretamente, contribuíram para minha formação como pessoa, deixo aqui um agradecimento extensivo.

Minha vida é como um software na versão beta, de vez em quando pego o código fonte para corrigir alguns *bugs*.

Aguinaldo Cristiano.

RESUMO

Computadores, apesar de facilitarem a maneira como o ser humano resolve alguns problemas do dia-a-dia, por outro lado abriram portas perigosas de acesso ao mundo do crime, comumente chamado de Cyber Crime quando estes têm sistemas computacionais como principais alvos. Com isso, a necessidade de profissionais para responderem a estes incidentes de segurança tornou-se urgente, eis que surge um grupo denominado de Grupo de Resposta a Incidentes de Segurança. De maneira geral concentrou-se em estudar algumas técnicas e metodologias para resposta a incidentes presentes no Helix, objetivando dar facilidade ao uso direcionado por usuários na aplicação das mesmas. Foram realizadas pesquisas bibliográficas sobre perícia forense, resposta a incidentes e sobre ferramentas presentes no Helix; para demonstrar o funcionamento das ferramentas e a aplicação dos metodos foi objeto de análise um caso de estudo; a metodologia usada para realização da análise no caso de estudo foi a SOP que compreende sete passos: coleta da prova, preparação do equipamento, imagem forense, exame/análise, documentação, relatórios, revisão. De maneira prática, foram atingidos os objetivos propostos, aplicando na análise os conhecimentos obtidos no decorrer do trabalho. Foram encontradas evidências bastante sólidas, que incriminam o suspeito, nomeadamente arquivos de texto, imagens e páginas de Internet salvas. As ferramentas para recuperação dos dados revelaram-se de um modo geral eficientes, bem como o principal software de análise, o Autopsy, encontrado no Helix

Palavras-Chave: Resposta a Incidentes ; Perícia Forense, Crimes Digitais.

ABSTRACT

Computers, while facilitating the way humans solve problems of day-to-day, on the other side doors have opened access to the dangerous world of crime, commonly called Cyber Crime when they have computer systems as main targets. Thus, the need for professionals to respond to these security incidents has become urgent, here comes a group called Group Security Incident Response. To study some techniques and methodologies for incident response present in the Helix 3 aiming to ease the use of tools and methodologies directed users to the application of the same. We performed literature searches on forensics, incident response, and on some tools, to demonstrate the operation of tools and application of the methodology have been considered something to study, the methodology used for analysis on a case tostudy was the SOP which consists of seven steps: collection of evidence, preparation of equipment, forensic imaging, examination/analysis, documentation, reports, review. From a practical way, the proposed objectives were achieved by applying the knowledge obtained in the analysis in this work. We have found solid evidence that incriminates the suspect, including text files, images and web pages saved. Tools for data recovery have proved generally effective, as well as the main software analysis, Autopsy, found in Helix

Keywords: Incident Response, Forensics, Computer Crime.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS E ABREVIATURAS

CAINE	*Computer Aided Investigative Environment*
CEO	*Chief Executive Officer*
CERT	*Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança*
CIRC	*Computer Incident Response Capability*
CIRT	*Computer Incident Response Team*
CSIRT	*Computer Security Incident Response Team*
DEFT	*Digital Evidence & Forensic Toolkit*
DFRW	*Digital Forensics Research Workshop*
DLL	*Dynamic Link Library*
EDRM	*Electronic Discovery Reference Model*
FDTK	*Forensic Digital Tool Kit*
FRED	*First Responder's Evidence Disk*
FRU	*First Responder Utility*
ICS	*Cyber Institute Security*
IOCE	*International Organization on Computer Evidence*
IRC	*Incident Response Center ou Incident Response Capability*
IRCR2	*Incident Response Collection Report*
IWIR	*International Workshop on Incident Response*
SERT	*Security Emergency Response Team*

SGDE	*Standard Group on Digital Evidence*
SIRT	*Security Incident Response Team*
SOP	*Standard Operating Procedures*
SWGDE	*Scientific Working Group on Digital Evidence*
WTF	*Windows Forensic Tool chest*

SUMÁRIO

1 INTRODUÇÃO

É quase que impossível imaginar que no passado não havia os recursos tecnológicos (Celulares, Computadores, GPS, entre outros) que estão disponíveis hoje. Eles tornaram-se de vital importância na sociedade, e dentre estes itens tecnológicos, em destaque está o computador.

O computador faz parte do cotidiano, desempenhando um papel fundamental na organização de informações, compartilhamento de dados, pesquisas por meio da Internet e no entretenimento. Junto com esses benefícios, surgiu também um problema que é a falta de segurança dos sistemas.

Pessoas passaram a estudar vulnerabilidades e técnicas de invasão em computadores e adotaram-nas como um meio para facilitar a execução de atividades criminosas, tendo início a era de crimes digitais, que segundo Guimarães, Furlaneto Neto (2003) diz respeito a toda e qualquer conduta ilegal, não ética, ou não autorizada, que envolva o processamento e ou transmissão de dados.

Em resposta ao surgimento dos crimes digitais surgiu a necessidade da criação de uma área, a Forense Computacional, cujos profissionais recebem a denominação de Peritos Forenses. Um perito forense no campo computacional tem as atribuições de usar o conhecimento das Técnicas e Metodologias criadas na Computação Forense, aplicadas com o apoio ferramental apropriado para obter dados e artefatos, tendo por objetivo qualificá-los como vestígios, evidências, ou provas no âmbito judicial (MELO, 2009).

Nos Estados Unidos, a Forense Computacional existe há anos, entretanto, aqui no Brasil, não obstante o mercado estar carente desse tipo de profissionais, o tema é relativamente ainda muito novo. Nesse universo existe certa dificuldade em encontrar um

profissional especializado na área, e a demanda por este tipo de serviço cresce a cada dia que passa.

Embora seja recente no Brasil, esta área teve um crescimento significativo no que concerne a área de Segurança da Informação nos últimos tempos, e tem como objetivos a investigação de supostos ataques a sistemas de informação, com o propósito de se responder perguntas como: Quem perpetuou o ataque em causa? Qual é seu endereço de Internet? Como se deu o ataque? Quais ferramentas foram utilizadas? Que falhas ou vulnerabilidade de segurança foram utilizadas pelo atacante? Qual a razão do ataque? Qual o nível de destruição do ataque? (MELO, 2009) mediante softwares e metodologias específicas para resposta a incidente de segurança que pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores.

Segundo o CERT (2010), Grupo de Resposta a Incidentes de Segurança para a Internet brasileira, de 1999 a junho de 2010 foram reportados a esta organização cerca de 358343 incidentes relacionados com crimes cibernéticos.

No mercado existem vários softwares para resposta a incidentes, dentre eles o Helix 3, e cada um possui as suas particularidades bem como ferramentas que os desenvolvedores acham de vital importância para o melhor andamento de uma perícia. Mediante dificuldades com documentação, a não padronização, o não direcionamento das ferramentas para casos específicos, e a escassez de documentação das mesmas têm contribuído para aumentar as dificuldades para os peritos, e justamente é uma das preocupações que se levará em consideração durante a elaboração do projeto.

O Helix é uma customização da distribuição Linux Knoppix básica. Foi criado nos Estados Unidos da América e contém um conjunto de ferramentas para resposta a

incidentes, tornando-se um produto integrado, capaz de analisar, realizar coletas e responder a incidentes forenses em ambiente Linux e Windows.

A metodologia de resposta a incidentes presente no trabalho compreende: a preparação pré-incidente, a detecção do incidente, a resposta inicial, a estratégia de formação da resposta, duplicação, investigação, implementação de medidas de segurança, monitorização da rede, recuperação, geração de relatórios e a finalização.

O Helix contém um conjunto de ferramentas para resposta a incidentes capazes de analisar, fazer coletas e responder a incidentes forenses em ambiente Windows, e dentre elas serão usadas as ferramentas *Windows Forensics Toolchest* (WFT*), Incident Response Colet Report* (IRCR2), *First Responder as Evidence Disk* (FRED) e *o First Responder Utility* (FRU) objetivando mostrar o funcionamento das mesma com casos fictícios.

Os estudos serão feitos em ambiente Windows principalmente no HD, serão feitas simulações usando no mínimo 2 computadores presentes nos laboratórios de Ciências da Computação da UNESC.

Partindo das considerações feitas, este projeto propõe o estudo de algumas técnicas e metodologias para resposta a incidentes presentes no Helix 3 objetivando dar facilidade ao uso direcionado das ferramentas e metodologias ao usuários para aplicação das mesmas.

1.1 OBJETIVO GERAL

Analisar ferramentas e metodologias para resposta a incidentes computacionais usando como objeto de estudo o Helix 3.

1.2 OBJETIVOS ESPECIFICOS

Os Objetivos desta pesquisa foram os seguintes:

a) demonstrar mediante casos fictícios o funcionamento de algumas ferramentas presentes no Helix 3;

b) citar e aplicar os quesitos básicos para a elaboração de uma perícia forense;

c) documentar e demonstrar a cópia e o tratamento de evidências;

d) utilizar um caso fictício para demonstrar como realizar o processo forense.

1.3 JUSTIFICATIVA

Segundo pesquisa da Symantec divulgada no mês de Abril de 2010, o Brasil ocupava a terceira posição no ranking de crimes pela Internet. A nível mundial, no Brasil ocorrem 6% de todos os delitos digitais, que vão desde a divulgação de spams até roubo de senhas e desvio de dinheiro.

Atos de vandalismo estão ocorrendo dentro do contexto computacional, em redes de computadores e na própria Internet em índices relativamente altos segundo ainda o CERT, gerando demanda de profissionais e, consequentemente, informações e metodologias forenses detalhadas para esta ramificação da Ciência da Computação criada para apoiar na investigação e no combate ao crime, seja ele organizado ou não.

O Helix é importante para o projeto porque é uma distribuição com características bastante notáveis que fazem a diferença no processo de análise forense que dentre as quais podemos destacar; segundo a E-Fense, nunca monta nenhuma Swap[1] ainda que forçada, impossibilitando então que o sistema seja alterado, característica essa muito importante em

[1] Segundo Henriques (2011) Swap é uma expansão da memória RAM por a mesma ser limitada pelo computador. Seu uso é indicado para computadores que possuem pouca memória.
[2]Segundo Gomes (2008) Malware são softwares cuja finalidade é infiltrar, causar danos a computadores

comparação com os outros softwares, monta as partições automaticamente, dá a possibilidade de fazer forense ao vivo tanto no Windows, Linux e no Mac. Implementa como uma das principais características para coleta de informações a possibilidade do sistema realizar gravações em mídia de CD e DVD para uso da perícia e suporta os sistemas de arquivos mais comuns. Outro grande ponto forte do Helix é a sua interface amigável, e em comparação com os outros, é considerado o mais fácil de ser usado (E-FENSE, 2009).

Partindo da problemática existente que é a carência de bibliografia e documentação em geral sobre perícia forense computacional e objetivando contribuir para o combate da incidência de crimes digitais na sociedade, bem como contribuir para o enriquecimento em termos de referências para comunidade científica, com a elaboração deste trabalho poderão ser relacionadas contribuições bastante relevante como, informações sobre procedimentos e metodologias para resposta a incidentes computacionais, bem como será dedicada especial atenção no modus operandi de um perito forense.

1.4 ESTRUTURA DO TRABALHO

Como dito anteriormente, o trabalho objetiva descrever as principais metodologias e ferramentas para resposta a incidentes, tendo como objeto de estudo o Helix 3. O projeto está repartido em duas etapas, cujo a primeira compreende a fundamentação teórica de assuntos relacionados ao estudo e a segunda e a segunda fase contém o estudo de caso, feito para demonstrar o funcionamento das ferramentas.

Primeiramente é apresentado qual a finalidade do trabalho, justificativas e são apresentados de maneira específica os objetivos a serem atingidos.

O segundo capítulo apresenta conceitos sobre resposta a incidentes, as metodologias propostas por algumas organizações a nível mundial, explicam que objetivos se

pretende atingir com a resposta a incidentes, os tipos de incidentes mais comuns, como se preparar face a um problema em que se tenha que dar resposta a ações criminosas, nos explica ainda qual o perfil de ameaças deste gênero, os passos para lidar com este problema, e termina falando um pouco sobre os profissionais que atuam neste segmento, no caso o Grupo de Resposta a Incidentes Computacionais.

Sendo Coleta e tratamento de evidências parte integrante importante no trabalho, conceitos sobre eles são descritos no terceiro capítulo, falando sobre procedimentos para coleta de evidências volatéis e não voláteis, bem como alguns desafios que esse procedimento apresenta no ato da sua efetivação.

Conceitos básicos sobre perícia forense são falados no capítulo quatro, que é seguido pela descrição de algumas metodologias existentes para prática de perícia forense, algumas considerações são feitas a respeito de crimes digitais e tratamento de evidências, e finaliza com a listagem de algumas das principais distribuições disponíveis no mercado, dando ênfase ao Helix 3.

O quinto capítulo apresenta breves descrições das ferramentas encontradas na ferramenta estudada, Helix. Encontram-se também alguns conceitos e ferramentas relacionadas com sistema de detecção de intrusão.

Alguns trabalhos cujo o tema relaciona-se com o presente projeto são apresentados no capítulo quatro, sendo estes os trabalhos correlatos

A análise de um caso de estudo, feita para auxiliar no entendimento das metodologias aplicadas para fazer uma perícia bem como as ferramentas necessárias, são apresentaos no capítulo sete.

Já, no final encontra-se a conclusão, aonde pode-se encontrar resumidantes informações sobre os resutados obtidos, dificuldade encontradas durante a análise, e uma recomendação para um possível trabalho futuro.

2 RESPOSTA A INCIDENTES DE SEGURANÇA

Resposta a Incidente é o processo que tem por objetivo identificar, conter, erradicar e recuperar um sistema, logo após o mesmo ser comprometido, é realizado por um pessoal de segurança responsável (CHUVAKIN; PEIKARI, 2004, tradução nossa). Qualquer atividade anormal confirmada que tenha como objetivo subverter o funcionamento e que comprometa a estabilidade de um sistema de computação ou de uma rede de computadores explicita ou implicitamente, é um incidente (CERT, 2004).

A resposta a incidente inclui ações para proteger e restaurar para condições normais o funcionamento de computadores e as informações armazenadas neles quando um evento adverso como uma invasão ou um ataque de negação de serviço ocorreu. O objetivo é o fechamento de cada incidência, restauração dos sistemas afetados, aplicações e bases de dados dentro de um prazo aceitável e com impacto a nível baixo para posteriormente dar sequência normal as atividades (SHULTZ, 2008, tradução nossa).

2.1 TIPOS DE INCIDENTES DE SEGURANÇA

De acordo com SCHEITZER (2003, tradução nossa) o incidente de segurança, abrange as seguintes categorias gerais de eventos adversos:

a) **ataques com códigos maliciosos** - incluem ataques por programas como Vírus, Cavalos de Tróia, Worms e scripts usados por Crackers ou Hackers para ganhar privilégios, obter senhas ou modificar logs de auditoria para eliminar dados de atividades ilegais.

b) **acesso não autorizado** - inclui uma série de incidentes, uso abusivo em uma conta de usuário e diretórios armazenados em um sistema ou meios de armazenamento por meio da obtenção de privilégios de super usuário.

c) **uso não autorizado de serviços** - obtendo acesso à informação ou desenvolver programas prejudiciais utilizando indevidamente os serviços disponíveis.

d) **interrupção do serviço** - os usuários contam com os serviços prestados pela rede de computação e serviços. Esses serviços podem ser interrompidos de varias maneiras, apagando programas críticos, o spamming (inundação de uma conta de utilizador com correio eletrônico) e alterando a funcionalidade de sistemas.

e) **desvios** - ocorrem quando alguém usa um sistema de computação para fins diferentes dos oficiais, tais como quando um usuário do governo usa um computador para armazenar registros pessoais.

f) **espionagem** - acontece quando são roubadas informações para subverter os interesses de uma corporação ou governo.

g) **boatos**- ocorrem quando informações falsas sobre incidentes ou vulnerabilidades se espalham.

2.2 OBJETIVOS DA RESPOSTA A INCIDENTES DE SEGURANÇA

Com o uso da metodologia para resposta a incidentes, têm-se como meta, alcançar objetivos para poderem ser formuladas respostas que depois serão apresentadas a alguma entidade, os objetivos a serem atingidos com uma resposta a incidentes segundo Mandia e Prosise (2001, tradução nossa) são os seguintes:

a) obter a confirmação ou, se for o caso, descartar a ocorrência de um incidente;

b) fazer com que as informações acumuladas sejam precisas;
c) encontrar meios para que a recuperação, tratamento e uso das provas sejam adequados;
d) garantir a proteção da privacidade que é estabelecida pela lei e pelas políticas empresariais;
e) garantir que as interrupções dos serviços e das operações em rede sejam as mínimas possíveis;
f) permitir que os autores dos delitos sejam responsabilizados legal e criminalmente pelos seus atos;
g) fornecer relatórios e recomendações que sirvam de referência para prevenção no futuro.

2.3 METODOLOGIA PARA RESPOSTA A INCIDENTES DE SEGURANÇA

Existem várias metodologias para resposta a um incidente de segurança. Será apresentada aqui a metodologia mais antiga e mais consagrada na área de resposta a incidentes segundo o especialista em segurança Eugene Shultz. É constituída de seis fases: preparação, detecção, contenção, erradicação, recuperação e acompanhamento, por isso, é chamada de metodologia das 6 etapas (SHULTZ et al, 2001, tradução nossa).

A metodologia das seis etapas foi criada no *International Workshop on Incident Response* (IWIR) no *Software Engineering Institute*, em Pittsburgh, Pensilvânia, em julho de 1989 (figura 1):

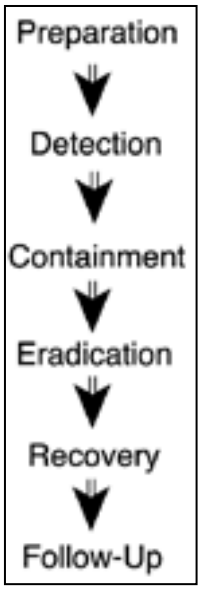


Figura 1. Metodologia para resposta a incidentes
Fonte: Schultz, E. (2008)

a) **preparação** - definir agentes para cada entidade que estarão envolvidas na célula de crise. Esses agentes devem ser documentados em uma lista de contatos mantidos permanentemente atualizados. Certificar-se que as ferramentas de análise estão nos conforme e funcionais, (antivírus, analisadores de logs), não comprometidas e atualizada, ter a arquitetura de suas redes. Efetua segurança permanente, assistir e informar as pessoas encarregadas da segurança sobre as tendências de ameaças (LACOME, 2011, tradução nossa);
b) **detecção** - desta fase irá se determinar se o código malicioso está presente, arquivos ou diretórios que tenham sido alterados, ou se outros sintomas de um incidente estão em causa, se forem, qual é o problema, bem como qual é a magnitude. Significa que será confirmado ou não, se o acesso não autorizado a um sistema tem acontecido (SHULTZ et al, 2001, tradução nossa);
c) **contenção** - o objetivo agora é limitar a extensão do ataque e, assim, minimizar os prejuízos. Atividades relacionadas com a contenção devem naturalmente ocorrer somente se as indicações observadas durante a segunda fase mostrarem conclusivamente que o incidente está a ocorrer. Medidas de

confinamento relacionadas podem em alguns casos ser relativamente simples e rápidas (SHULTZ et al, 2001, tradução nossa). As seguintes ações devem ser executadas e monitoradas pelo time que gere a crise segundo (LACOME, 2011, tradução nossa):

- desconectar a área infectada da Internet;
- isolar a zona infectada desligando o sistema de qualquer rede;
- caso o tráfego não possa ser interrompido, certificar-se que este não venha a ser um vetor de infeção ou encontre técnicas validas de invasão;
- neutralizar os vetores de propagação, o vetor de propagação pode ser o tráfego de rede, a falha de software, entre outros;
- repetir os passos 2-4 em cada subárea da zona infectada até a ameaça for neutralizada. Se possível, controlar a infecção usando as ferramentas de análise (console antivírus, servidor de logs, chamadas de suporte).

d) **erradicação -** a quarta etapa da metodologia da 6 etapas objetiva a erradicação da causa do incidente (SHULTZ et al, 2001, tradução nossa). Após um incidente ser contido, a erradicação é necessária para eliminar os componentes do incidente, como a exclusão de códigos maliciosos e desabilitar contas de usuários violados. Para alguns incidentes, a erradicação não é necessária ou é realizada durante a recuperação (SCARFONE et al, 2008, tradução nossa)**;**

e) **recuperação -** visa devolver o sistema comprometido completamente de volta ao seu estado normal de funcionamento (SHULTZ et al, 2001, tradução nossa);

f) **acompanhamento -** objetiva analisar e integrar informações relacionadas com o incidente que ocorreu. Esta fase, é talvez a mais negligenciada, porque pela escassez de recursos, os técnicos tendem a gastar muito tempo na recuperação prejudicando esta etapa. A realização da etapa de acompanhamento é

> importante por várias razões. Ela ajuda os elementos envolvidos na manipulação de um incidente, desenvolvendo um conjunto de lições aprendidas, para melhorar as habilidades em situações futuras, fornece informações, incluindo métricas, que podem ajudar a justificar o esforço de uma organização, fornece bases para construção da equipe e ainda informações que podem ser úteis em processos judiciais e sua tramitação de maneira a encontrar a verdade (SHULTZ et al, 2001, tradução nossa).

2.4 PREPARAÇÃO PARA RESPOSTA A INCIDENTES

Estare preparado para lidar com um incidente de segurança tornou-se uma prioridade para a maioria dos administradores de sistema. A presença das empresas online hoje é uma realidade, e, com isso vão ficando cada vez mais dependentes dos sistemas de informação, e, consequentemente o nível de incidentes também aumenta. As organizações, agora reconhecem a necessidade de adaptarem-se quanto a sua posição em relação à segurança (SCHEITZER, 2003, tradução nossa).

A filosofia por trás da preparação de uma resposta a incidentes é a criação de uma infraestrutura que venha prover respostas para perguntas urgentes que surgirão logo após um incidente (MANDIA et al 2003, tradução nossa):

a) O que aconteceu exatamente?
b) O sistema foi afetado pelo incidente?
c) Quem se deve avisar?
d) Que passos se deve seguir para garantir a recuperação e dar continuidade ao sistema normal?

2.5 PERFIL DE UM INCIDENTE DE SEGURANÇA

Sendo o local da prática de crimes a Internet, as ações estão se tornando mais remediadas, no entanto um profissional de segurança da informação, deve estar capacitado para enfrentar este tipo de variações em termos criminais, poder responder a um incidente de segurança e identificar o seguinte (MELO, 2009):

a) **origem -** se o acidente ocorreu interna ou externamente;
b) **motivação -** o que o ataque perspectiva? Trocar uma página, ou então se estão a estruturar para um dano maior, como uma eventual sabotagem total de dados;
c) **classificação -** visa responder se o ataque é um crime que ainda esta ocorrendo;
d) **tecnologia -** responder se o ataque é automatizado, se esta por alguma razão sendo executado por um malware[2];
e) **meta -** se são feitas violações de confiança, disponibilidade e ou se pecam na garantia da integridade da informação;
f) **danos -** se os sistemas foram usados de forma a que foram feridas diretrizes;
g) **robustez da infraestrutura -** se por acaso violações e acessos foram detectados;
h) **foco da Exploração -** determinar se o mau funcionamento partiu do hardware ou do software;
i) **grau de Resistência -** se a segurança física eventualmente foi violada,
j) **extensão** - determinar o que prejudicou o funcionamento dos serviços, e quais foram afetados temporariamente.

[2]Segundo Gomes (2008) Malware são softwares cuja finalidade é infiltrar, causar danos a computadores individuais ou servidores de rede e englobam Cavalos de Tróia, Worms e Adwares.

2.6 PASSOS PARA RESPOSTA A UM INCIDENTE DE SEGURANÇA

Quando o assunto é respostas a incidentes, cada organização tem uma maneira diferente de abordagem do problema, muitas são as companhias que preferem terceirizar a uma empresa especializada, no entanto não é fácil encontrar uma boa equipe de resposta a incidentes. Empresas terceirizadas entram em desvantagem pelo simples fato de não conhecerem o sistema com que irão lidar. Possuem pouca informação sobre a arquitetura de TI da organização. Independentemente de quem responderá o ocorrido, se for uma equipe externa ou interna, os passos sugeridos na imagem abaixo e descritos posteriormente provavelmente serão usados (KLEIMAN, 2007, tradução nossa).

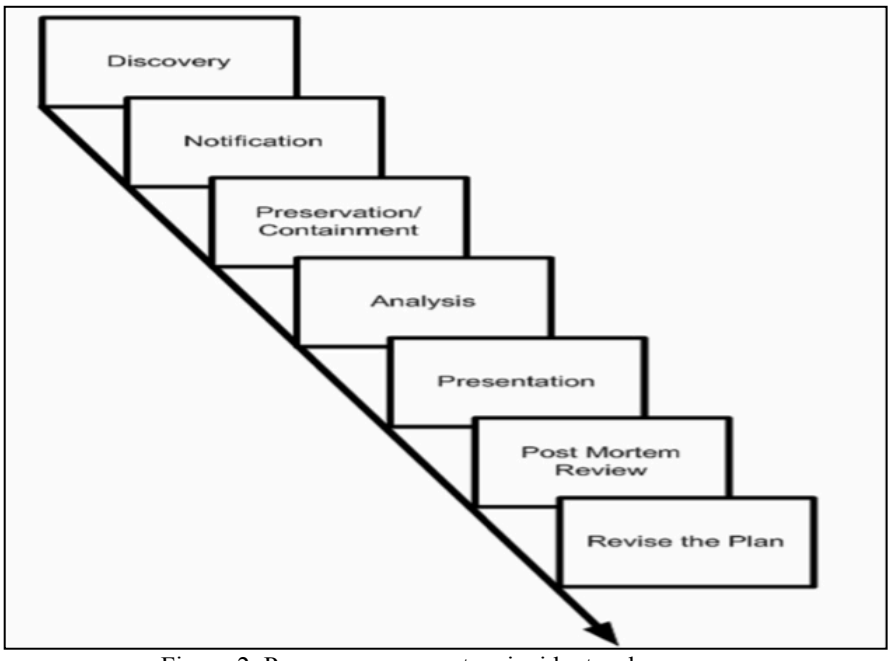


Figura 2. Passos para resposta a incidentes de segurança
Fonte: (KLEIMAN, 2007).

a) **preparação** - precisa-se criar uma estrutura local para que se possa responder a um incidente de segurança, a preparação vai desde a criação da equipe, a criação de políticas e procedimentos;

b) **identificação** - um incidente normalmente é descoberto acidentalmente por alguém que possui algum treinamento adequado e conhecimentos necessários que o ajudem a identificar quando algo vai mal, alguns ainda são identificados no decurso de revisões em logs de firewalls, sistemas de detecção de intrusão, ips, roteadores e servidores. Na fase da identificação é feita uma investigação preliminar para confirmação que o incidente ocorreu e envolve as seguintes etapas segundo ainda os autores:

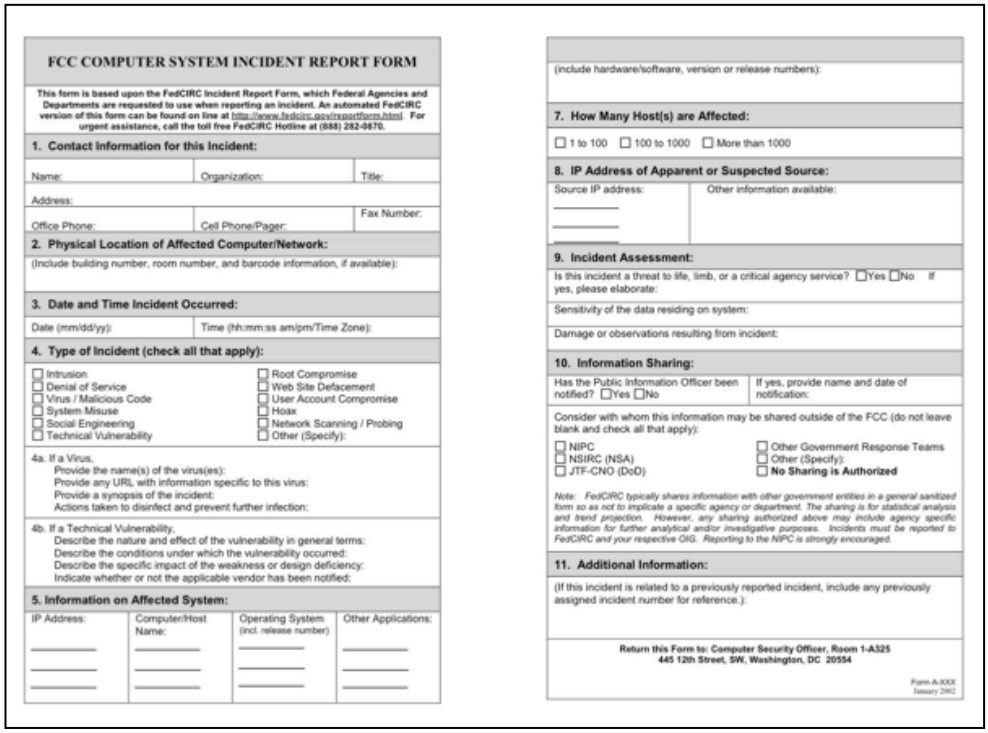
- **determinar se o crime ocorreu** - objetivo inicial da investigação;
- **avaliação da denúncia** - confirmação ou não de que o acidente ocorreu;
- **inspeção dos danos** - acontece quando os danos foram feitos com código malicioso ou acesso não autorizado;
- **entrevista das testemunhas** - visa obter confirmação por parte de outras pessoas que viram o incidente;
- **análise de logs** - os logs são potênciais fontes de informação, aqui eles serão analisados, pressupondo que eles estejam habilitados;
- **identificar os requisitos da investigação** - nesta última etapa, o investigador determina as metas para o inquérito.

c) **notificação -** deve-se alertar a gerência sênior e deixar claro que existem possibilidades de que o evento se transforme em um incidente. Normalmente a equipe da hierarquia mais alta em conformidade com o pessoal jurídico irá reunir condições pra determinar se a notificação deve ser feita a mídia, as autoridades, aos parceiros de negócios ou clientes;

d) **preservação e contenção** - muitas vezes quando os incidentes ocorrem, estes lidam com dados transientes (informações que eventualmente serão perdidas caso o sistema seja desligado como conexões abertas, trabalhos na rede, e

programas residentes na memória) e frágeis (dados no disco rígido, mas que podem facilmente ser alterados). Deve-se ter cuidado com a preservação das provas durante a reposta ao incidente. Depois vem a contenção, o confinamento visa evitar que o sistema seja mais afetado por meio da conexão de rede, isto pode ser interpretado como retirar a infecção ou a parte que compromete a rede;

e) **análise** - nesta fase tudo deve ser documentado, números de serie gravados, pois, as máquinas deverão ser movidas para a etapa de processamento forense. A figura abaixo mostra a forma como é usada a análise, trata-se de um formulário de notificação do CERT (figura 3);



FCC COMPUTER SYSTEM INCIDENT REPORT FORM

This form is based upon the FedCIRC Incident Report Form, which Federal Agencies and Departments are requested to use when reporting an incident. An automated FedCIRC version of this form can be found on line at http://www.fedcirc.gov/reportform.html. For urgent assistance, call the toll free FedCIRC Hotline at (888) 282-0870.

1. Contact Information for this Incident:

Name: | Organization: | Title:

Address:

Office Phone: | Cell Phone/Pager: | Fax Number:

2. Physical Location of Affected Computer/Network:

(Include building number, room number, and barcode information, if available):

3. Date and Time Incident Occurred:

Date (mm/dd/yy): | Time (hh:mm:ss am/pm/Time Zone):

4. Type of Incident (check all that apply):

☐ Intrusion
☐ Denial of Service
☐ Virus / Malicious Code
☐ System Misuse
☐ Social Engineering
☐ Technical Vulnerability
☐ Root Compromise
☐ Web Site Defacement
☐ User Account Compromise
☐ Hoax
☐ Network Scanning / Probing
☐ Other (Specify):

4a. If a Virus,
Provide the name(s) of the virus(es):
Provide any URL with information specific to this virus:
Provide a synopsis of the incident:
Actions taken to disinfect and prevent further infection:

4b. If a Technical Vulnerability,
Describe the nature and effect of the vulnerability in general terms:
Describe the conditions under which the vulnerability occurred:
Describe the specific impact of the weakness or design deficiency:
Indicate whether or not the applicable vendor has been notified:

5. Information on Affected System:

IP Address:	Computer/Host Name:	Operating System (incl. release number)	Other Applications:

(include hardware/software, version or release numbers):

7. How Many Host(s) are Affected:

☐ 1 to 100 ☐ 100 to 1000 ☐ More than 1000

8. IP Address of Apparent or Suspected Source:

Source IP address: | Other information available:

9. Incident Assessment:

Is this incident a threat to life, limb, or a critical agency service? ☐Yes ☐No If yes, please elaborate:

Sensitivity of the data residing on system:

Damage or observations resulting from incident:

10. Information Sharing:

Has the Public Information Officer been notified? ☐Yes ☐No | If yes, provide name and date of notification:

Consider with whom this information may be shared outside of the FCC (do not leave blank and check all that apply):

☐ NIPC
☐ NSIRC (NSA)
☐ JTF-CNO (DoD)
☐ Other Government Response Teams
☐ Other (Specify):
☐ **No Sharing is Authorized**

Note: FedCIRC typically shares information with other government entities in a general sanitized form so as not to implicate a specific agency or department. The sharing is for statistical analysis and trend projection. However, any sharing authorized above may include agency specific information for further analytical and/or investigative purposes. Incidents must be reported to FedCIRC and your respective OIG. Reporting to the NIPC is strongly encouraged.

11. Additional Information:

(If this incident is related to a previously reported incident, include any previously assigned incident number for reference.):

Return this Form to: Computer Security Officer, Room 1-A325
445 12th Street, SW, Washington, DC 20554

Form A-XXX
January 2002

Figura 3. Formulário de participação de incidente
Fonte: KLEIMAN, D. (2007).

f) **erradicação e recuperação** - sendo que o incidente esta contido, faz-se necessário que o CSIRT (Computer Security Incident Response Team) corrija problemas subjacentes que possam ser a causa. Estas medidas devem ser

tomadas em consonância com a prevenção para que não ocorra novamente. Quando um sistema é comprometido, além do reparo que pode ser preciso, deve-se subir os backups para que se mantenha o funcionamento normal;

g) **apresentação -** durante a apresentação é exibido o inquérito para a equipe forense, este, é a folha de resposta a incidentes (Figura 11)**.** Qualquer descoberta deve ser apresentada a equipe de resposta a incidentes, e dai em diante tudo é tratado pelo grupo. Quando a empresa possui um CSIRT, apenas é necessário que seja reportado a gerência sênior;

h) **revisão *post mortem*** - logo após a equipe de resposta a incidentes, entregar as provas para o time forense, deve-se começar a encontrar maneiras de aperfeiçoar o processo de resposta a incidentes para o próximo nível;

- adequar o plano de resposta para que da próxima vez seja mais fácil de lidar;
- definir a política de divulgação da informação, se porventura a informação do incidente vazou, ou se foram repassadas informações sensíveis, deve-se elaborar uma política de difusão da informação;
- deve-se criar uma política de comunicação de incidentes, definir o que o usuário que encontrar o incidente deve fazer, quem chamar;
- precisa-se criar a declaração de monitoramento eletrônico, todo o acesso deve ser registrado, lembrando que qualquer usuário que mexer com o sistema estará concordando com o monitoramento, sendo que o mesmo é apenas para pessoas autorizadas;
- criar política de trilha de auditoria se não existe. Estabelecer que todo o usuário deve ser registrado;

- manter um controle adicional de pessoal para segurança, caso o acesso ao edifício não seja controlado pois é muito mais difícil controlar ameaças internas. Um dispositivo que lê cartões, pode ser bom para segurança, e ajuda eliminar o publico geral da esfera de suspeitos.

i) **revisar o plano ou dar seguimento** - tem de haver sempre espaço para que se produza uma revisão nos procedimentos aplicados. Um plano *post mortem* irá de antemão prover mudanças na maneira como se respondem os incidentes, posteriormente deve-se deixar o sistema livre de risco para que se possa dar sequência as atividades normais.

2.7 GRUPO DE RESPOSTA A INCIDENTES

Um grupo de resposta a incidente, ou *Computer Security Incident Response Team* (CSIRT) é um grupo organizado que tem como responsabilidade receber, analisar e posteriormente responder a alertas que sejam relacionados com segurança em computadores. Estes grupos comumente são vinculados a organizações bem definidas que vão desde uma empresa, um organismo estatal, ou mesmo uma comunidade acadêmica, podendo também emprestar os seus conhecimentos a um país ou a pessoas que irão pagar pelos seus serviços (CERT, 2004).

Existem vários acrônimos para um grupo de resposta a incidentes que serão mostrados logo no quadro abaixo (figura 4), segundo o CERT (2004):

CSIRT	Computer Security Incident Response Team
CIRC	Computer Incident Response Capability
CIRT	Computer Incident Response Team
IRC	Incident Response Center or Incident Response Capability
IRT	Incident Response Team
SERT	Security Emergency Response Team
SIRT	Security Incident Response Team

Figura 4. Outros acrônimos para grupos de resposta a incidentes
Fonte: CERT (2004)

Resposta a incidentes é frequentemente relacionado a grupo de resposta a incidentes, superficialmente pode até ter lógica, mas na realidade não passam de conceitos, pois as coisas não funcionam bem assim. Pessoas que desconhecem a metodologia de resposta a incidentes podem sempre estar de uma maneira ou outra envolvidas em lidar com casos relacionados a incidentes de segurança (CERT, 2004).

3 COLETA E TRATAMENTO DE EVIDÊNCIAS

Os dados para serem analisados, precisam ser adquiridos primeiro. Isto quer dizer que os mesmo necessitam ser duplicados para que o perito que for realizar a análise forense possa trabalhar a partir da imagem gerada, para que não se comprometa a fonte original. Qualquer ferramenta que se proponha a coletar os dados pode ser usada, desde que a mesma produza uma copia bit a bit, ou seja que possibilite uma cópia exatamente igual a original. Isto irá permitir que o analista tenha acesso a dados fragmentados, escondidos e até mesmo delegados, é importante que não sejam alterados nem corrompidos os dados durante o processo de duplicação (REYES; WILES, 2008, tradução nossa).

É essencial que se lembre os princípios aplicáveis pela lei vigente quando se vai realizar uma investigação. Sem evidência, não existe crime. Decisões tomadas no principio da investigação desde a cena do crime, desempenham um papel importante para resolução de um caso, é crucial que se faça uma investigação criteriosa para que se assegure que as provas físicas em potencial não sejam destruídas, contaminadas ou negligenciadas em nenhuma hipótese. Deve-se ter o máximo de cuidados no ato da coleta e preservação das evidências recolhidas no local do incidente (SCHWEITZER, 2003, tradução nossa).

Segundo ainda o mesmo autor, quando as evidências são coletadas seguindo um uma ordem, torna-se mais fácil detectar o atacante ou, em outro caso encontrar o que se procura, e, a probabilidade da prova ser aceita em juízo, é maior. A coleta deve seguir a seguinte ordem (SCHWEITZER, 2003, tradução nossa):

a) **encontrar as provas** - detectar em que parte do sistema está armazenada a informação que se procura. Elaborar uma lista do tipo de dados e palavras chaves, ajuda no processo de coleta;

b) **determinar a relevância dos dados** - para se descobrir evidências, é necessário que se decida que partes são relevantes para o caso em referência. Mas com cuidado, pois deve-se coletar mais do que excluir possíveis evidências, não se deve ignorar informação, pois em algum momento do caso ela pode ser importante;

c) **ordem de volatilidade** - depois de escolher quais itens serão colhidos, deve-se decidir em que ordem serão capturados. Deve-se tomar como principal fator aqueles dispositivos susceptíveis de serem mais voláteis, estes devem ser coletados primeiro;

d) **eliminar a interferência de fora** - é importante evitar a alteração dos dados originais. É melhor evitar a adulteração do que corrigir as consequências. Se por ventura isto acontecer, esses cuidados são essências, porque apenas é considerada evidência dados inalterados;

e) **coleta de evidências** - agora é chegado o momento de efetuar a aquisição, deve-se utilizar as melhores ferramentas nesta etapa.

3.1 COLETA DE DADOS VOLÁTEIS

Um sistema operacional armazena dados temporários em memórias RAM. Enquanto o mesmo encontra-se em execução, o conteúdo da RAM muda de segundo a segundo. Em certos momentos uma memória pode conter dados ou informações que podem ser de algum interesse na investigação. Muitas vezes, contêm nelas dados acessados recentemente, *hash* de senhas, comandos recentes, também podem existir dados residuais na folga ou em espaços livres. Os tipos de dados voláteis (MARCELA; MENENDEZ, 2008, tradução nossa):

a) **conteúdo da memória** - várias ferramentas para copiar os dados existentes na RAM e viabilizar uma posterior análise dos dados estão disponíveis. Em uma grande parte dos sistemas é quase impossível não fazer alterações na memória quando se executa um utilitário que possibilita fazer uma copia, em UNIX podemos usar o comando memdump (figura 5);

b) **configuração da rede** - grande parte dos sistemas operacionais possuem utilitários em que nele aparecem as configurações de rede, por exemplo ifconfig em UNIX e Ipconfig em Windows. Nas informações contém o nome do host, informações sobre interfaces lógicas e físicas, configurações de cada uma como por exemplo endereços IP, MAC e o atual estado;

c) **conexões de rede** - são fornecidos pelos sistemas, métodos para que se exibam a lista de conexões de rede atuais. Para Windows e baseados em UNIX existe o programa Netstat, este que faz uma lista com as conexões de rede com os endereços de IP e Portas de origem e destino, e lista as portas que no momento encontram-se abertas em cada interface de rede;

d) **processos em execução** - os sistemas baseados em UNIX possuem o comando ps, este, exibe os processos em execução. O Windows oferece um programa com interface gráfica para visualizar os processos, o Gerenciador de Tarefas, mas, ainda assim, é preferível usar aqueles que geram uma lista de texto;

e) **arquivos abertos** - existe o comando lsof para UNIX, este exibe uma lista com todos arquivos abertos. Para Windows pode-se usar utilitários vindo de terceiros;

f) **login de sessão** - sistemas operacionais há, que possuem comandos embutidos, estes, listam usuários conectados em tempo real, exemplo é o comando w para

UNIX, possibilita listar também o endereço de origem de cada usuário e quando esse iníciou no sistema;

g) **tempo de operação do sistema** - para recuperar informações de tempo no Windows como data e hora, pode-se usar o comando nlsinfo, já em UNIX tem o comando date que também captura informações de fusos horários e as configurações de horário de verão.

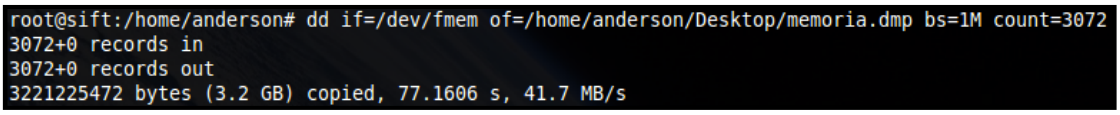


Figura 5. Dump da memória principal usando o comando dd no LINUX
Fonte: PERÍCIADIGITAL DF (2010)

Devido a prospecção de mudança que os dados voláteis possuem, devem ser observadas a pontualidade e a ordem em que os dados serão colhidos. Em uma grande parte dos casos, os peritos devem numa primeira fase, colher informações sobre conexões de rede e sessões de login, porque as conexões estão susceptíveis a expirar ou desligar a qualquer momento, para além de que os usuários logados no sistema podem variar. Dados que não oferecem muito perigo de mudança podem ser coletados posteriormente. A ordem que se recomenda coletar os dados em geral, é a seguinte (MARCELA, MENENDEZ, 2008, tradução nossa):

a) conexões de rede;

b) sessões de login;

c) conteúdo da memória;

d) processos em execução;

e) arquivos abertos;

f) configuração de rede

g) tempo de operação do sistema.

3.2 DADOS NÃO VOLÁTEIS

Dados para análise podem ser obtidos a partir de backups, pen drives, CDs ou do disco rígido. Estes dados, depois de coletados serão analisados em um processo chamado de análise *post mortem*, para peritos que estão interessados apenas em obter dados armazenados ou indícios de que um incidente aconteceu é a mais indicada (4LINUX, 2010).

Toda informação que permanece sem alteração quando o sistema é privado de energia ou não esta conectado é um dado não volátil. Documentos de processamento de texto, e-mails, planilhas, entre outros podem ser tomados como exemplo. Grande parte de toda informação coletada para análise forense será proveniente de dados não voláteis, por isso, os peritos precisam prestar a máxima atenção na coleta dos mesmos, esses dados podem ser os seguintes, segundo (CONYERS, 2010, tradução nossa):

a) **arquivos temporários** - arquivos temporários geralmente são criados por programas, quando estes não conseguem alocar suficiente memória para executar as suas funções ou então está executando um grande número de instruções. Comumente estes arquivos são deletados quando o programa é terminado, mas, em alguns casos, eles são deixados para trás;

b) **registros do sistemas** - não deixa de ser uma base de dados em que na qual são encontradas informações e configurações da parte física do sistema, operações, preferências de usuários e atividades em geral de computação;

c) **logs de eventos** - em conformidade com configurações definidas pelo administrador do sistema, logs registram alguns eventos. Eles podem fornecem um caminho de auditoria normalmente usados para detectar problemas ou para checar atividades consideradas suspeitas;

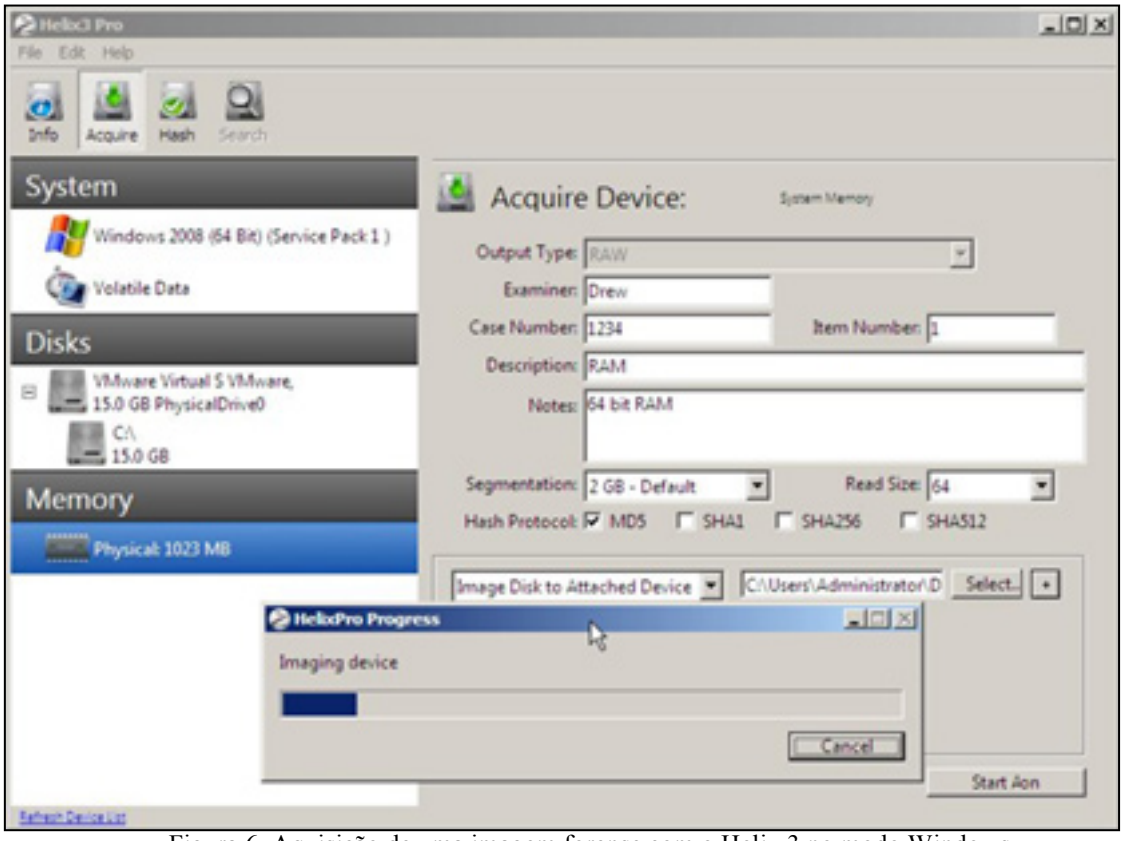


Figura 6. Aquisição de uma imagem forense com o Helix 3 no modo Windows
Fonte: PERÍCIADIGITAL DF (2010)

d) **unidades de inicialização** - sistemas usados como ambiente de produção, muitas das vezes são organizados em várias partições e, cada uma delas pode possuir um sistema operacional diferente, unidades de inicialização contém as instruções precisas para arranque do sistema operativo.

e) **web browser** - armazena conteúdo das páginas web em cache para que sites frequentemente visitados abram com mais facilidade. Este conteúdo fica no disco rígido até que seja excluído, mas, mesmo sendo eliminado, ele ainda pode estar presente no espaço não alocado.

4 PERÍCIA FORENSE COMPUTACIONAL

Perícia Forense Computacional é a preservação, identificação, extração, interpretação, análise e documentação de evidências computacionais colhidas em equipamentos eletrônicos (KLEIMAN, 2007, tradução nossa).

Steve *Haileys*, CEO e professor do *Institute Cyber security* (ICS), define forense computacional como sendo preservação, identificação, coleta, interpretação e documentação de evidências computacionais, incluindo as regras de evidência, processo legal, integridade da evidência, relatório factual da evidência e provisão de opinião de especialista em uma corte judicial, ou outro tipo de processo administrativo e/ou legal com relação ao que foi encontrado (HAILEYS, 2002, tradução nossa).

O processo Forense tem produzido ao longo dos anos resultados válidos e confiáveis decorrentes de procedimentos e protocolos detalhados com documentações e revisões aceitas pela comunidade científica. O uso de metodologia e de protocolos deve ser considerado na prática de investigação como garantia de aceitação em uma corte judicial. As atividades desenvolvidas pelos especialistas em perícia forense podem ser entendidas do ponto de vista macro em três fases ilustradas na figura 7 (MELO, 2009).

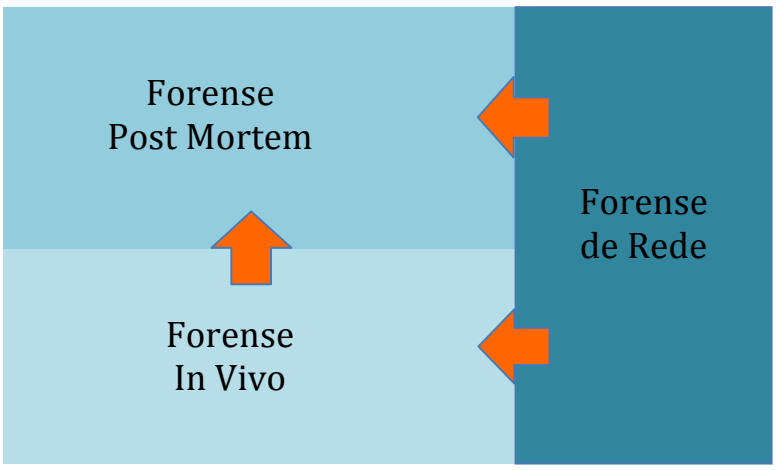


Figura 7. Atividades operacionais da Computação Forense
Fonte: MELO, S. (2009)

Forense *post mortem* consiste em coletar ou analisar dados logo após o desligamento do sistema como pode ser visto na figura 8, serão coletados dados apenas não voláteis que incluem discos digitais, disquetes, discos rígido, entre outros. É considerada a etapa mais difícil devido ao grande volume de dados encontrados nas memórias. É preferencial que se faça a análise em outra máquina para não comprometer as provas da perícia (MELO, 2009).

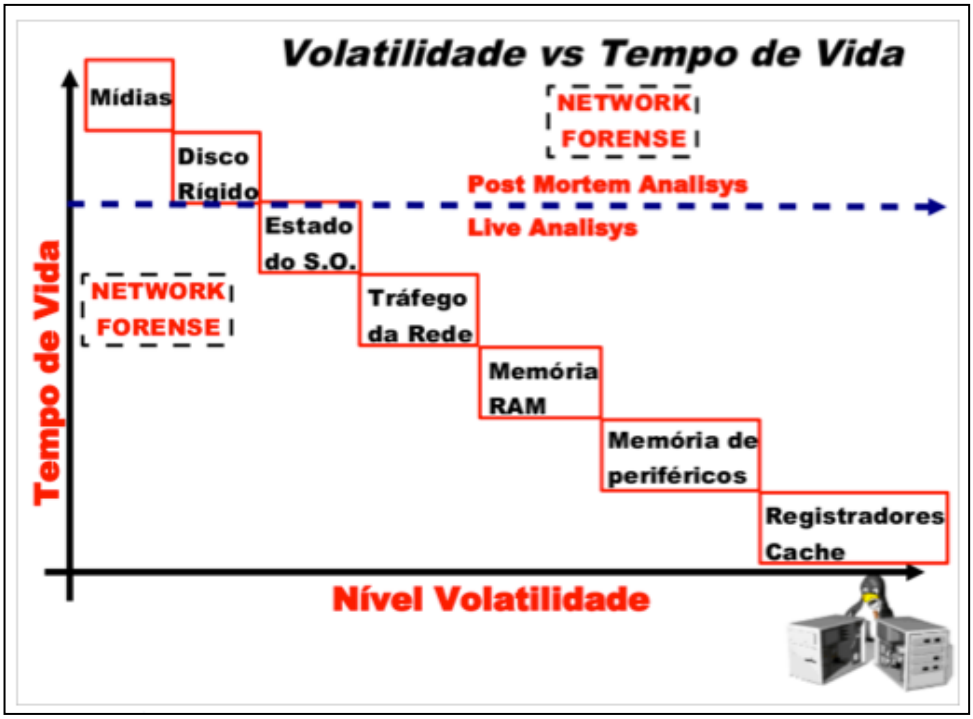


Figura 8. Grau de volatilidade versus tempo de vida
Fonte: MELO, S. (2009)

Forense *In vivo* são procedimentos utilizados para coletar dados sem ter que desligar o sistema. Os dados nesse caso são coletados mediante níveis de prioridade como visto na figura anterior, dos mais voláteis para os menos voláteis, porque na maioria das vezes depois que o sistema é desligado os dados mais voláteis são perdidos. Forense em rede, visa analisar dados capturados da comunicação entre a máquina atacada e a do atacante, dados

esses capturados por meio de *sniffers*[3] e que durante a perícia servirão para correlacionar e ou cruzar informações de dados colhidos durante a *post mortem* e na forense *in vivo* (MELO, 2009).

4.1 METODOLOGIAS DE INVESTIGAÇÃO FORENSE

Metodologias na área da forense computacional, são práticas e técnicas usadas para coleta, armazenamento, análise e apresentação da informação e evidências obtidas em um computador alvo de uma perícia computacional. Enquanto que os passos individuais para executar essas tarefas podem variar de caso para caso e dependendo do tipo de software e equipamentos utilizados, as práticas mais usadas serão sempre melhor aceitas e mais consistentes (KLEIMAN, 2000, tradução nossa).

4.1.1 Metodologia de Reith, Carr e Gunsh

Reith, Carr e Gunsch (2002, tradução nossa) criaram o *Abstract Digital Forensics Model* tendo como base o modelo da *Digital Forensics Research Workshop* (DFRW) possuindo algumas particularidades, pois este modelo não é dependente de uma determinada tecnologia ou crime eletrônico, e compreende as seguintes etapas determinadas pelos pesquisadores:

a) **identificação** - é o primeiro contacto com a cena do crime, visa reconhecer um incidente de indicadores e determinar o seu tipo;

[3]Um *sniffer* é um programa que o objetiva monitorar e registrar as atividades de rede em um arquivo *sniffing* de tráfego e sem modificar os pacotes de rede (SCHWEITZER, 1991, tradução nossa).

b) **preparação** - é a etapa na qual são criadas condições em termos de ferramentas, revisão da capacidade técnica, obtenção de mandados de busca e autorizações de acompanhamento e apoio à gestão;

c) **abordagem da estratégia** - objetiva, de forma dinâmica, a elaboração de uma abordagem baseada no potencial impacto sobre as especificidades tecnológicas em questão, e também maximizar o recolhimento das provas, procurando minimizar o impacto à vítima;

d) **preservação** - Compreende isolar, proteger e preservar o estado de provas físicas e digitais;

e) **coleção** - gravação e duplicação de provas digitais utilizando procedimentos padronizados e aceitos internacionalmente;

f) **exame** - etapa focada em buscar o máximo de dados relacionados com a suspeita do crime, identificar e localizar possíveis evidências dentro de locais não convencionais;

g) **análise** - compreende a interpretação, reconstrução de fragmentos de dados e emissão de conclusões baseadas nas provas encontradas. Refere-se que podem ser levadas a cabo varias iterações de exame e análise para apoiar a teoria do crime;

h) **apresentação** - visa resumir e apresentar uma explicação das conclusões;

i) **devolvendo as provas** - garante que as propriedades físicas e digitais serão devolvidas ao verdadeiro proprietário.

4.1.2 Metodologia Eletronic Discovery Reference Model

Eletronic Discovery Reference Model (EDRM) foi definido por um grupo de trabalho visando padronizar o processo de análise e produção de dados eletrônicos, conforme mostra a figura 9. Os Padrões definidos pela EDRM usados como metodologia para perícia forense são os seguintes (EDRM, 2011, tradução nossa):

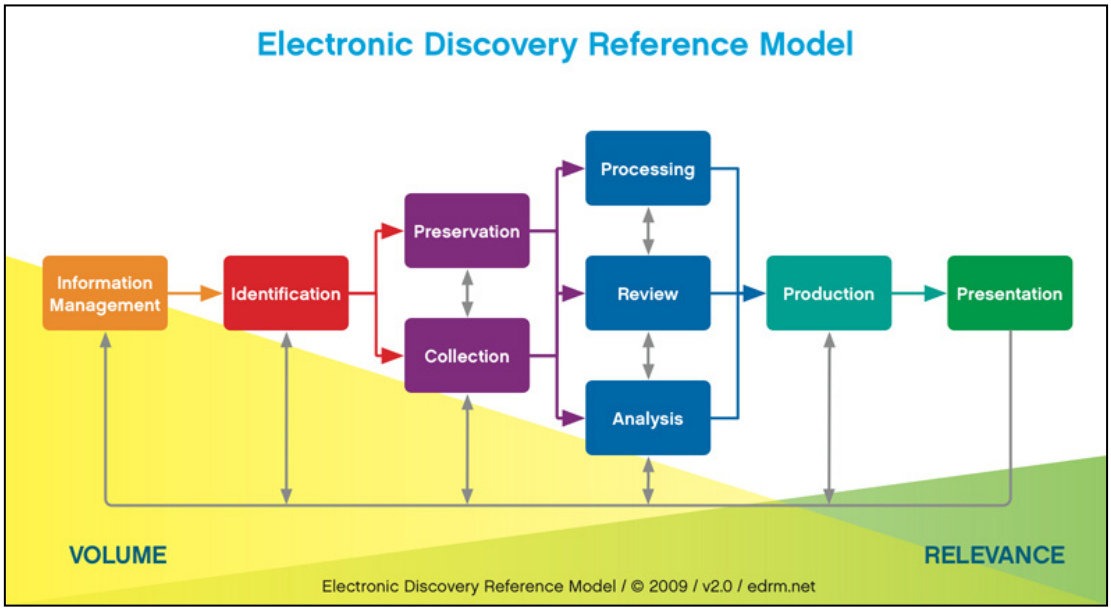


Figura 9. Modelo de Referência de descoberta de provas eletrônicas
Fonte: EDRM (2011)

a) **identificação -** localização de fontes potenciais em informação armazenadas eletronicamente e determinar a sua amplitude, o escopo e a profundidade;

b) **preservação** - assegurar as fontes potenciais de informação armazenadas eletronicamente, determinar a sua amplitude e protegê-las contra qualquer alteração inadequada ou destruição;

c) **coleta** - recuperar as provas para posterior utilização no processo de descoberta eletrônica (análise, processamento, entre outros);

d) **processamento** - reduzir o volume de dados e convertê-los, se necessário, para as formas mais adequadas para a revisão e análise;

e) **revisão** - avaliar os dados, sua relevância, e os que são privilegiados;

f) **análise** - avaliar o conteúdo e contexto, incluindo os principais padrões, temas, pessoas e discussão;

g) **produção** - produzir provas electrônicas cumprindo os padrões;

h) **apresentação** - exibir as informações em depoimentos, audiências, julgamentos, entre outros, sobretudo nas formas nativa e próximo-nativa para extrair mais informações, validar fatos, posições, ou persuadir uma audiência.

4.1.3 Metodologia SOP

A metodologia *Standard Operating Procedures* (SOP) foi criada pela *Scientific Working Group on Digital Evidence* (SWGDE), representante norte-americano na *Organization Computer Evidence* (IOCE) e é feita em 7 etapas que serão descritas segundo a (SWGDE, 2006, 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) **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;

c) **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;

d) **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;

e) **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;

f) **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.

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

4.2 CRIMES DIGITAIS E EVIDÊNCIAS

Cada dia que passa vão aumentando cada vez mais os números de fatos ocorridos em nível de incidentes de segurança, e justificam o desenvolvimento das técnicas de perícia forense computacional e a formação de profissionais de segurança (MELO, 2009).

Computação forense envolve a investigação de evidências baseadas em computador, e isto, exige necessariamente que os investigadores compreendam o papel desempenhado pela tecnologia informática. Isso não pode ser feito sem alguma compreensão da tecnologia informática (MOHAY et al, 2003, tradução nossa).

4.2.1 Crimes Digitais

A definição de atividades criminosa digitais é que são crimes dirígidos a um computador ou um sistema de computadores. A natureza do delito cibernético, no entanto, é deveras mais complicada do que se pensa. O vandalismo cibernético pode assumir a forma de simples *snooping*[4] em um sistema de computador para o qual não se tem autorização. Pode também ser por vandalismo por causa de insatisfação de algum cliente ou funcionário, ou ainda, por roubo de dados, dinheiro, ou informação sensível por meio de um sistema de computador (STEPHENSON, 1999, tradução nossa).

O crime cibernético pode vir de várias fontes, o hacker que explora um sistema de computador sem autorização pela maioria das definições atuais realizando um ato criminoso, pode-se estar perante o roubo de dados sensíveis de marketing, um vírus pode derrubar um sistema ou um dos seus componentes, não há um perfil único e fácil de crimes cibernéticos ou para criminoso cibernético (STEPHENSON, 1999, tradução nossa).

[4]Snooping ocorre quando dados de pessoas ou empresas são acessados sem autorização, observação casual de e-mails ou espiando o que o outro digita em seu computador (SEARCH Security, 2005).

Como se observa, muitas investigações não precisam terminar em um processo penal (por exemplo, aqueles relacionados com a ação civil ou de processos disciplinares internos), mas eles precisam ser realizados se a responsabilidade ou culpabilidade é ser justamente atribuída. O âmbito de um inquérito, inclui a detecção de atos planejados e em andamento, bem como os atos no passado, assim os pesquisadores (sejam humanos ou de seus prepostos do sistema, tais como sistemas de detecção de intrusão) também podem desempenhar um papel em cenários de crime (MOHAY et al, 2003, tradução nossa).

Os computadores têm inspirado novos tipos de má conduta, tais como hackers e negação de serviço. Uma vez que esses atos exigem alguns conhecimentos de computador de um criminoso, eles mantêm certo glamour em alguns círculos que os consideram como heróis e não criminosos. Talvez o mais desalentador para a aplicação da lei é a taxa com que as pessoas comuns e inexperientes têm para encontrar novas oportunidades para os crimes mais antigos, como fraude de cartão de crédito, apropriação indébita, e até chantagens. Na era eletrônica as pessoas se comportam tão ilegais como sempre, mas cada vez mais imaginativas (MOHAY et al, 2003, tradução nossa).

4.2.1.1 Classificação dos Crimes Digitais

Os crimes digitais podem ser classificados em três tipos segundo a 4LINUX, empresa de soluções e serviços de Tecnologias de Informação baseados em softwares livres e padrões abertos para ambientes de missão crítica (4LINUX, 2010):

a) **crimes de informática puros** - toda e qualquer conduta que tem por objetivo violar um sistema de computadores, atentando física ou tecnicamente ao equipamento e respectivos componentes;

b) **crimes de informática mistos** - são ações em que o computador é condicional para efetivação de um crime;

c) **crimes de informática comuns** - são atos criminosos em que o computador é apenas usado como ferramenta para cometer crimes já tipificados na lei penal.

4.2.2 Evidências

Em perícia forense computacional, evidência é definida como sendo todos os dados armazenados ou transmitidos por meio de um computador que apoiam ou refutam uma teoria de como um delito ocorreu ou quais os elementos críticos, endereço do delito, tais como intenção ou álibi (CHISUM, 1999, tradução nossa).

Evidência tem sido previamente definida como sendo qualquer dado que visa estabelecer que o delito tenha sido cometido ou fornecer uma ligação entre um crime e a sua vítima ou um crime e seu autor (CASEY, 2000, tradução nossa). O grupo *Standard Group on Digital Evidence* (SGDE) define evidência digital como sendo toda informação de valor probatório, que é armazenada ou transmitida de forma digital. Outra definição proposta pela *International Organization on Computer Evidence* (IOCE), é a informação armazenada ou transmitida de forma binária, que pode ser invocada em juízo.

Os dados referidos nestas definições são essencialmente uma combinação de números que representam informações de vários tipos, incluindo texto, imagens, áudio e vídeo. Devem-se considerar todos os tipos digitais que existem e como eles podem ser úteis para uma investigação. Os computadores são onipresentes e dados digitais são transmitidos pelo ar em torno de nós e também de fios no chão sob os nossos pés muitas vezes não garantindo segurança (CASEY, 2004, tradução nossa).

As provas digitais e as eletrônicas são por vezes intercambiáveis. No entanto, um esforço deve ser feito para distinguir entre dispositivos eletrônicos como telefones celulares e dados digitais que contêm (HENSELER, 2000, tradução nossa).

Dada ubiquidade das provas digitais, é raro que o crime não tenha alguns dados associados, armazenados e transmitidos por meio de sistemas informáticos. Um olho treinado pode usar estes dados para compilar muitas coisas sobre um indivíduo, fornecendo a introspecção tal como olhar sob um vitral para a vida pessoal do mesmo em pensamentos. O computador pessoal e a sua utilização em serviços de rede são efetivamente arquivos comportamentais, podendo reter mais informação sobre as atividades de uma pessoa e os desejos que até mesmo seus familiares e amigos mais próximos desconheciam. Sites de e-commerce usam algumas destas informações para o marketing direto, e, um investigador especializado pode aprofundar estes arquivos comportamentais e ganhar introspecção profunda na vida de uma vítima ou um transgressor (CASEY, 2002, tradução nossa).

Apesar de sua predominância, poucas pessoas estão versadas nas questões de provas técnicas e jurídicas relacionadas com as provas digitais e, como resultado, a evidência digital é muitas vezes esquecida, recolhidas de forma incorreta, ou analisadas de forma ineficaz. (CASEY, 2004, tradução nossa).

2.2.3 Aspectos desafiadores da Evidência Digital

A evidência digital como forma de evidência física, cria vários desafios para os examinadores forenses. São uma confusão, forma escorregadia de provas que podem ser muitos difíceis de lidar. Por exemplo, um disco rígido contém uma confusão de dados, pedaços de informações misturados e em camadas, armazenados em cima uns dos outros ao longo do tempo. Apenas uma pequena parte desses dados pode ser relevante para um

processo, tornando-se necessário extrair partes úteis, encaixá-los juntos, e traduzi-los em um formulário que pode ser interpretado (CASEY, 2004, tradução nossa).

As ondas de rádio e micro-ondas que viajam pelo ar podem conter um emaranhado de dados, tornando-se necessário encontrar a informação desejada entre o ruído e a traduzi-la para dados que podem ser compreendidos. Isso é conceitualmente semelhante à análise de DNA, as informações relevantes devem ser extraídas do fluido humano/tecido, processadas e traduzidas para uma forma que seja possível de ser analisada e posteriormente interpretada em juízo (CASEY, 2004, tradução nossa).

Provas digitais são uma abstração de algum evento ou objeto digital. Quando uma pessoa instrui um computador a executar uma tarefa, como enviar um e-mail, as atividades geram resíduos resultantes dos dados que dão uma visão parcial do que ocorreu (VENEMA; FARMER, 2000, tradução nossa).

Sendo que ninguém instalou equipamentos de vigilância, os cliques de mouse, teclas, comandos do sistema interno, e outras minúcias não são mantidos arquivados. Apenas alguns resultados de atividades tais como a mensagem de e-mail e logs do servidor permanecem a dar uma visão parcial do que aconteceu. Mesmo quando tais minúcias estiverem registradas, os impulsos elétricos dos nossos cliques do mouse e do teclado devem ser traduzidos em dados antes que eles tenham algum significado. Da mesma forma, uma mensagem de e-mail e de logs do servidor armazenados em um disco são o resultado de várias camadas de abstração de campos magnéticos sobre o disco para as letras e números que vemos na tela. Portanto, nunca vemos os dados reais, mas apenas uma representação, e cada camada de abstração pode eventualmente introduzir erros (CARRIER, 2003, tradução nossa).

4.3 ALGUNS LIVE CDS PARA PERÍCIA FORENSE

Um live CD roda um sistema operacional sobre um ramdisk, ou seja, 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 de CD e não exigindo muita memória (MORIMOTO, 2005). Nos capítulos seguintes serão apresentados alguns destes sistemas operacionais que funcionam com live CD.

4.3.1 FDTK

É uma distribuição que tem como objetivo realizar perícia forense, coleta e análise de dados. É baseada em Ubuntu e nele podemos encontrar mais de 100 ferramentas que guiaram o perito forense a realizar todas etapas de uma investigação forense. Na figura quatro pode-se observar a tela da distribuição. Pode-se usá-lo como live CD e, ou ainda instalar em um computador, acabando por transformá-lo em uma estação forense. Possui uma interface amigável, estruturada conforme as etapas para a perícia. Atualmente encontra-se na sua versão 3.0 e disponível em português (figura10) (NEUKAMP, 2011, tradução nossa).

Figura 10. Distribuição para perícia forense - FDTK
Fonte: FDTK (2011)

4.3.2 CAINE

Computer Aided Investigative Environment (CAINE), é uma ferramenta para perícia forense computacional de origem italiana, é baseada em Linux e tem licença livre, pode-se observar na figura 11 a sua área de trabalho. Caracteriza-se por ser uma ferramenta com softwares organizados em categorias e integrados. Segundo os desenvolvedores da distribuição, os objetivos principais da ferramenta são os seguintes (LEHR, 2009?, tradução nossa):

a) manter o ambiente inter operável que garanta que o investigar cumpra as fases da perícia;

b) manter a interface amigável;

c) a criação semiautomática e compilação do relatório final.

Figura 11. CAINE, distro para perícia forense
Fonte: CAINE (2009)

Alguns pontos não passam despercebidos neste software, as atualizações constantes, a quantidade de ferramentas, a política de montagem de mídia que é formalizada, é facilmente instalável, podendo ser usado a partir de uma pendrive (RODRIGUES, 2009).

4.3.3 DEFT

É uma distribuição para perícia (GNU/Linux) baseado no Xubuntu e no XFCE4 Desktop, possui cerca de 40 ferramentas e foi desenvolvido na Universidade de Bolonha na Itália em 2005 no curso de Computação Forense, a figura 12 representa o ambiente de trabalho do mesmo (FRATIPIETRO; ROSSETI, 2009, tradução nossa).

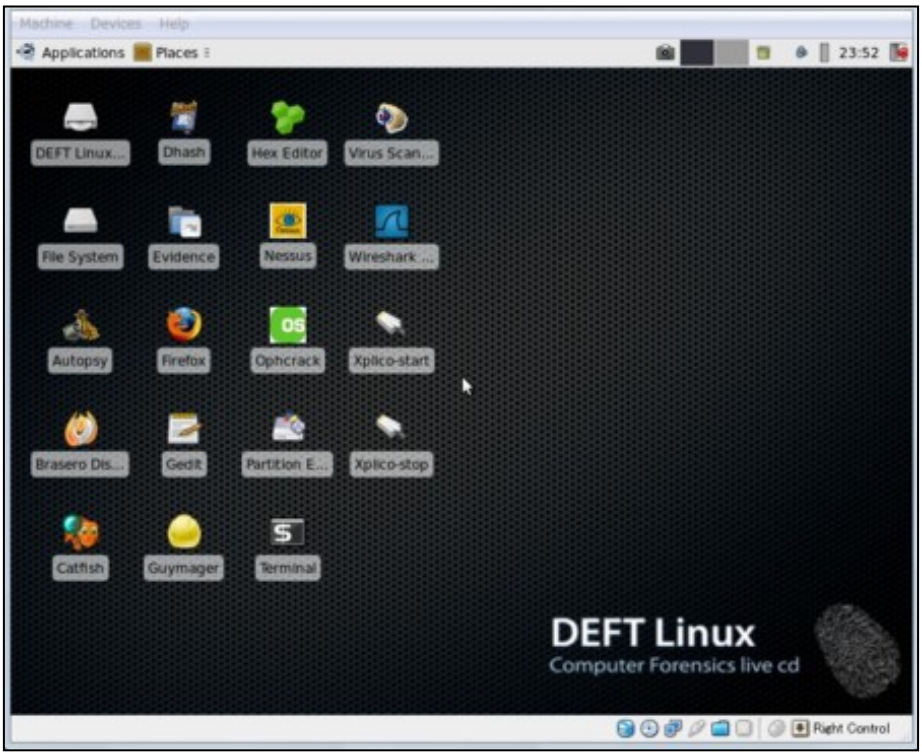


Figura 12. DEFT distribuição para perícia forense
Fonte: DEFT (2009)

É destinado para perícia forense digital, ele garante a durabilidade da estrutura dos arquivos que estão sendo analisados, minimiza o risco de alteração da cena do crime e

segundo o manual possui como mais notáveis as seguintes características ainda (FRATIPIETRO, ROSSETI, 2009, tradução nossa):

a) não usa partições Swap na inicialização do sistema;

b) não monta nenhuma partição automaticamente;

c) não automatiza nenhum processo durante um processo de análise;

d) no ato da aquisição sobre IP nenhum dado é alterado.

4.3.4 HELIX

Foi personalizado a partir de uma distribuição Knoppix padronizada, é baseado no Ubuntu. Ele foi majoritariamente desenvolvido por Klaus Knopper e contém varias contribuições de programadores pelo mundo. O Helix é mantido pela empresa E-fense, e Segundo manual distribuído pela empresa, a ferramenta possui detalhes que a diferenciam do resto que se encontra no mercado (GLEASON; FAHEY, 2006, tradução nossa).

Podemos encontrar nesta distribuição ferramentas para detecção, identificação, análise, preservação e emissão de relatório que são necessárias para que se realize uma resposta a incidente e ou perícia forense sem nenhum problema. O Helix é multiplataforma, atende os principais três sistemas operacionais do mercado, Mac OS Windows e Linux, a figura 13 mostra a ferramenta (E-FENSE, 2009, tradução nossa).

Figura 13. Helix ,distro para resposta a incidentes e perícia forense
Fonte: E-FENSE (2006)

Atualmente o Helix já não é grátis, possui 3 versões descritas abaixo (E-FENSE, 2009, tradução nossa):

a) o Live Response software tem o objetivo de fazer a aquisição de dados voláteis (memória, registro, entre outros), bem como o histórico da Internet. É adquirido e usado por meio de pendrive;

b) a versão Enterprise, tem como base o Helix 3, contém uma das ferramentas que é entendida por muitos como sendo uma grande evolução, que é direcionada para corporações que sentem necessidade de monitorar e ou visualizar toda rede a proteger do mau uso, softwares maliciosos, ou ainda contra violação de privacidade e hacking;

c) o Helix 3 Pro tem a função de funcionar de maneira proativa, dando resposta a incidentes e suporte para realização de perícia forense.

4.3.4.1 Modo de operação Windows

O modo de operação do Helix no Windows foi desenvolvido porque a maioria dos incidentes ocorre nesta plataforma, no entanto, se fez necessário criar uma ferramenta que interaja com este SO de maneira a facilitar a coleta de dados e posterior envio para análise em uma estação forense. Neste modo é executada uma aplicação padrão que possibilitará fazer a coleta da informação *in vivo* (GLEASON; FAHEY, 2006, tradução nossa).

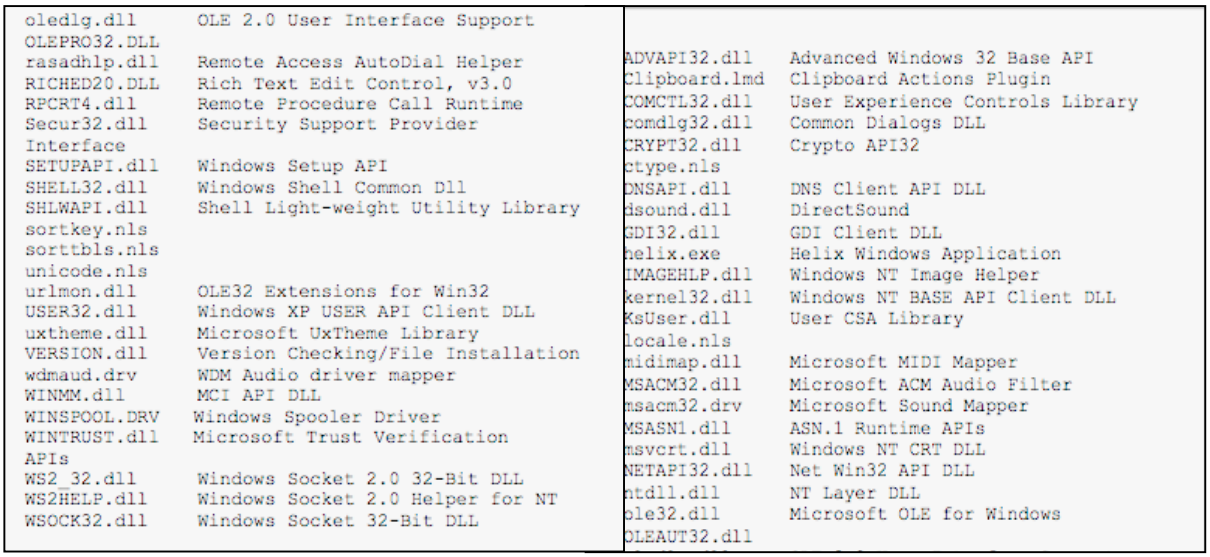


Figura 14. DLL usadas no Windows com o Helix em execução
Fonte: GLEASON, B.; FAHEY, D. (2006).

O sistema estando ligado, um dos fatores mais importantes é o fato da máquina estar a ser alvo de mudanças constantemente, não importando que ferramenta use, pois até quando ninguém está em contato com o sistema, este ainda assim é alterado. Algo que não pode ser ignorado, é que ao executar o Helix no Windows, DLL do sistema serão automaticamente carregadas, é importante que o perito tenha conhecimento quais são (GLEASON, FAHEY, 2006, tradução nossa).

4.3.4.2 Modo de operação Linux

O Helix no modo Linux é inicializado pelo CD com sistema operacional autocontido que é usado para fazer a análise detalhada de sistemas off-line ou conhecidos também como *Post mortem.* Ao ser inicializado, executa completamente pelo Live CD, montando todos os discos apenas em modo leitura para que estes não sejam modificados, fator importante para que não se contamine uma evidência digital. Uma grande vantagem deste modo é sem dúvida a portabilidade, pois permite ser inicializado na maioria dos computadores utilizando arquitetura x86 (GLEASON; FAHEY, 2006, tradução nossa).

4.3.5 Quadro comparativo entre os LIVE CDS descritos

Ramos, Saturnino, e Ferreira, no trabalho de conclusão de curso apresentam uma comparação entre diversos Live Cds para perícia forense. Esta comparação é disposta em um quadro aonde encontram-se informações como vantagens, desvantagens, características que mais se destacam, e a quantidade de ferramentas, pode-se conferir o resultado da comparação mais abaixo com algumas atualizações (Quadro 1) (RAMOS; SATURNINO, et al, 2009):

LIVECD	Vantagens	Desvantagens	Características em destaque	Quantidade de ferramentas
FDTK	- Quase Todas as ferramentas são acessíveis pelo menu, manutenção contínua;	- Carência na parte de forense em rede, teclado brasileiro como padrão	- Língua Portuguesa	Cerca de 100
CAINE	- Está em desenvolvimento, e recebe muitas atualizações, não usa Swap nem monta drive automaticamente	- Teclado padrão italiano, não oferece confiança para trabalhos mais complexos	Provê resposta a incidentes para Windows, gera relatórios automaticamente, ferramentas exclusivas	Cerca de 80
DEFT	- Não monta drive automaticamente, não usa swap e não automatiza nenhum processo durante a análise	- Algumas ferramentas necessárias estão em falta para análise de memória, browser, registro	Ferramentas exclusivas	Cerca de 40
HELIX	- multiplataforma, não monta drive automaticamente e não usa swap	- Ausência de ferramentas atualizadas, é pago	- Vários artifícios para evitar a modificação do sistema	Cerca de 150

Quadro 1: Comparação entre os live CDs apresentados

5 FERRAMENTAS FORENSES

Existem várias ferramentas que têm como objetivo, coletar, duplicar, recuperar, e analisar dados. O uso de ferramentas já amplamente aceitas no meio judicial ajudam a não afetar a força probatória das provas recolhidas. Um conjunto de ferramentas, deve ser composto por softwares de backup, descriptografia, coleta, monitoramento de protocolos de Internet, recuperação de arquivos, e para análise (PLADNA, 2009, tradução nossa).

5.1 ALGUMAS FERRAMENTAS PARA RESPOSTA A INCIDENTES PRESENTES NO HELIX, MODO WINDOWS

No Helix encontramos várias ferramentas para resposta a incidentes, elas estão distribuídas em painéis, e são, *Windows Forensics Toolchest* (WFT), *Incident Response Collection Report* (IRCR2), *First Responder's Evidence* Disk (FRED), *First Responder Utility* (FRU), *Security Reports*, *Md5 Generator*, *File Recovery*, *Rootkit Revealer*, *VNC Server*, *Putty SSH, Screen Capture, Messenger Password, Mail Password Viewer, Protected Storage Viewer, Network Password Viewer, Registry Viewer, Asterisk Logger, IE History Viewer, IE Cookie Viewer, Mozilla Cookie Viewer* (E-FENSE, 2005, tradução nossa). Dentre estas ferramentas, com breve detalhes algumas:

a) ***Windows Forencics Toolchest (WFT)*** - tem como função dar resposta a incidentes ao vivo (figura15), auditoria em sistemas Windows de forma estruturada e automatizada de forma interativa, ao mesmo tempo que coleta dados relevantes para a segurança do sistema. Basicamente ele funciona agrupado a outras ferramentas com mesmo objetivo e produz relatórios forenses em HTML com os resultados obtidos. Os peritos também podem usar

esta ferramenta para localizar vestígios deixados por uma possível invasão, ou apenas para que se confirme uma má utilização do computador. O WFT emite no seu formulário, respostas úteis para os administradores do sistema, e que também possivelmente, possam ser usadas em juízo, autenticadas pelos algoritmos MD5/SHA1 (FOOLMOON, 2011, tradução nossa);

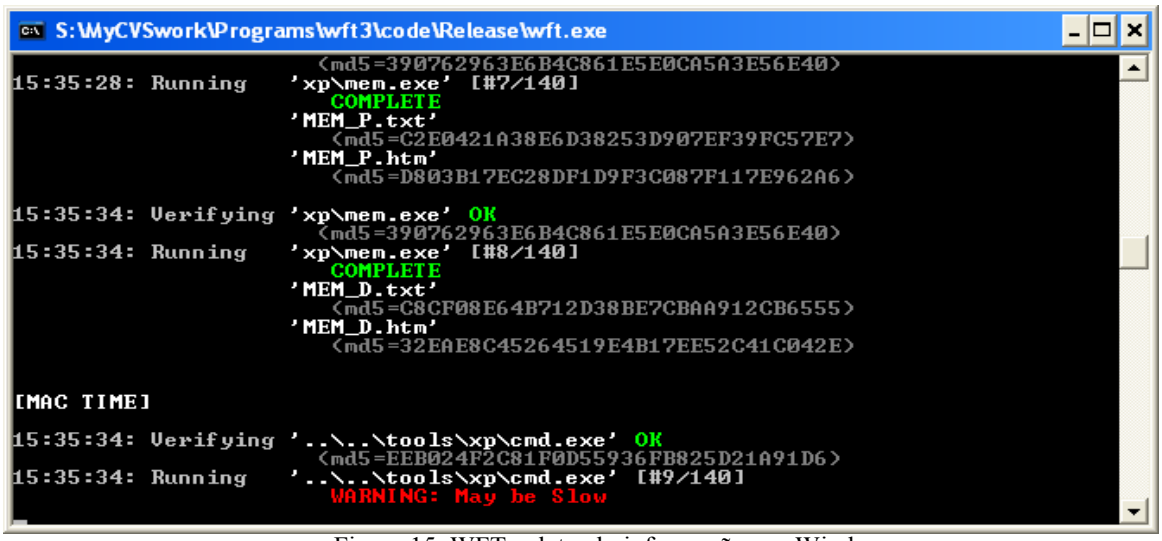


Figura 15. WFT coletando informações no Windows
Fonte: FOOLMOON (2011)

b) ***Incident Response Collection Report (IRCR)*** - é composto com um conjunto de ferramentas baseadas em Windows (figura 16). É semelhante a ferramenta criada por Dan Farmer e Witese Venema, o *The Coroners Toolkit* (TCT). Tem como principal objetivo facilitar a coleta de dados por qualquer pessoa, e envia-lo para alguém especializado na matéria para que se efetue a análise forense computacional (E-FENSE, 2002, tradução nossa);

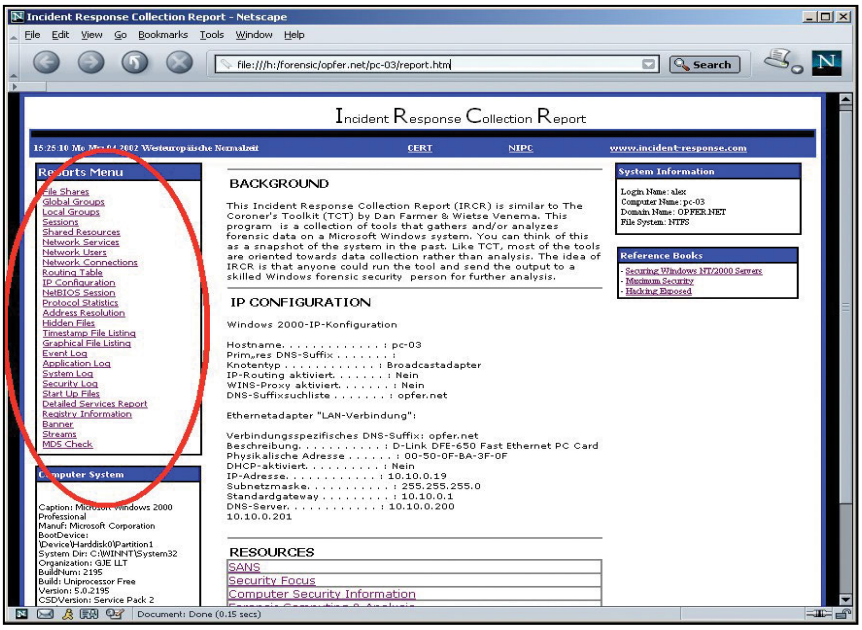


Figura 16. Relatório gerado pelo IRCR
Fonte: GESCHOONNEK (2002)

c) ***First Responder Utility (FRU)*** - as equipes de resposta a incidentes de segurança usam-no para a coleta de dados voláteis provenientes de sistemas que provavelmente estejam comprometidos. Atualmente possui um outro nome, (Frutose). A ferramenta funciona com uma interface de linha de comandos que carrega dados combinados de um arquivo INI (figura 17);

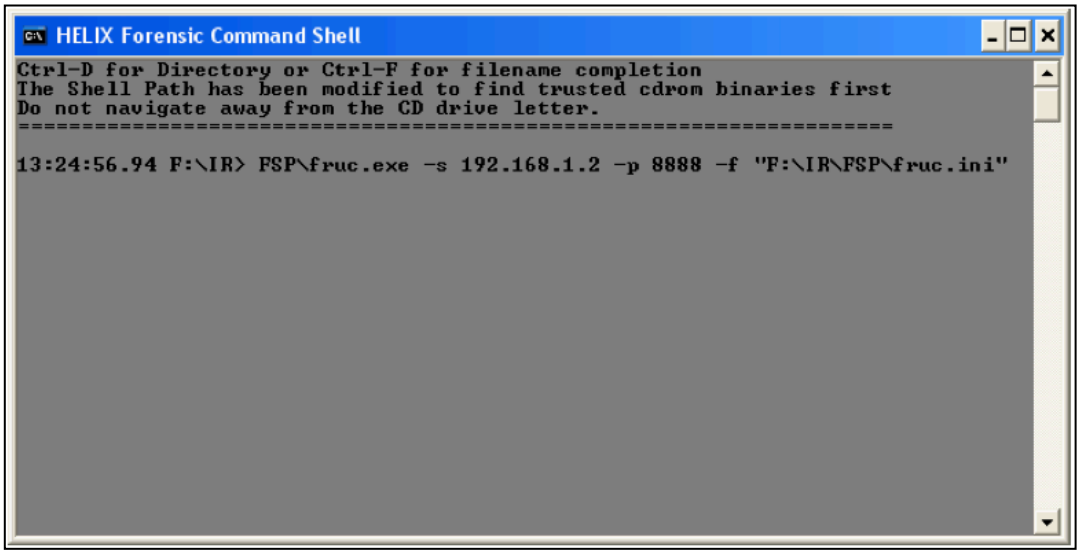


Figura 17. Captura de dados e posterior envio via Netcat
Fonte: E-FENSE (2005)

d) ***First Responder's Evidence Disk (FRED)*** - é uma ferramenta para resposta a incidentes projetada para obter dados voláteis de um computador para que posteriormente sejam analisados sem que se modifique nada no sistema alvo da possível ocorrência.

5.2 ALGUMAS FERRAMENTAS DE RESPOSTA A INCIDENTES PRESENTES NO HELIX, MODO LINUX

A investigação forense possui metodologias para sua realização, algumas delas já mencionadas mais acima neste trabalho. Tais metodologias para serem seguidas efetivamente necessitam de apoio ferramental para poder por exemplo: manter a cena do crime e as evidências intactas, fazer a aquisição, a reconstrução do auto, e a sua posterior análise (CARRIER, 2003). Algumas destas ferramentas são descritas abaixo, sobretudo aquelas que se encontram no ambiente a ser estudado.

5.2.1 The Sleuth Kit (TSK*)*

Compreende um conjunto de ferramentas de perícia forense computacional baseadas em UNIX, usadas em linha de comandos. Estas ferramentas possibilitam que o perito realize um exame não evasivo do sistema de arquivos de uma máquina suspeita, com elas é possível ter acesso a dados apagados e escondidos. As ferramentas contidas neste conjunto são majoritariamente suportadas por uma interface gráfica, é chamado de *Autopsy Forensic Browser* (DOWLING, 2006, tradução nossa).

Figura 18. Tela do Autopsy depois da imagem ser adicionada
Fonte: SLEUTH KIT (2011)

5.2.2 The Coroner's Toolkit (TCT)

É uma coleção de ferramentas compiladas por Wietese Venema e Dan Farmer, renomados peritos forenses, que têm como objetivo ajudar o perito forense a fazer análises de copias provenientes de sistemas provavelmente comprometidos. Elas foram escritas misturando duas linguagens de programação, C e Perl. A ferramentas fazem uma análise com profundidade de modo a fazer uma reconstrução do que aconteceu no passado. No *The Coroner's Toolkit* existem as segundas ferramentas segundo (VENEMA; FARMER, 2000, tradução nossa):

a) **Grave Robber** - coleta dados executando vários comandos, objetivando colher informações relevantes e guardá-las para posterior análise;

b) **Mactime** - como o nome sugere, esta ferramenta cria uma linha de tempo contendo as últimas atividades executadas no sistema suspeito em ASCII;

c) **Icat(inode-cat*)*** - pelo inode, permite que o conteúdo de um arquivo ou diretório seja visualizado;

d) **Ils** - lista rastros de arquivos apagados ou removidos;

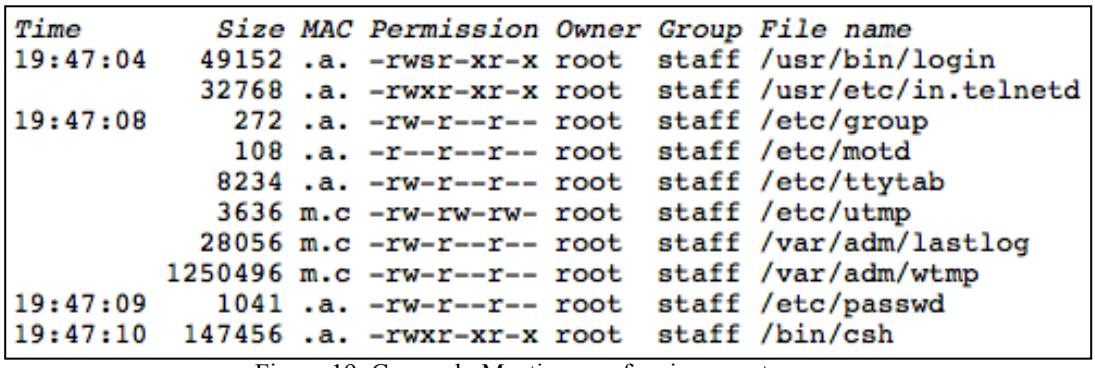
e) **Pcat** - captura processos na memória;

f) **Md5** - verifica a integridade de um arquivo gerando um *hash* MD5;

g) **Timeout** - executa comandos com restrição de tempo;

h) **Unrm** -faz o dump de espaços não alocados de um disco;

i) **Lazarus** - Pega os dados produzidos pela ferramenta unrm e tenta criar alguma estrutura a partir de dados não estruturados.



```
Time          Size MAC Permission Owner Group File name
19:47:04     49152 .a. -rwsr-xr-x root  staff /usr/bin/login
             32768 .a. -rwxr-xr-x root  staff /usr/etc/in.telnetd
19:47:08       272 .a. -rw-r--r-- root  staff /etc/group
               108 .a. -r--r--r-- root  staff /etc/motd
              8234 .a. -rw-r--r-- root  staff /etc/ttytab
              3636 m.c -rw-rw-rw- root  staff /etc/utmp
             28056 m.c -rw-r--r-- root  staff /var/adm/lastlog
           1250496 m.c -rw-r--r-- root  staff /var/adm/wtmp
19:47:09      1041 .a. -rw-r--r-- root  staff /etc/passwd
19:47:10    147456 .a. -rwxr-xr-x root  staff /bin/csh
```

Figura 19. Comando Mactime em funcionamento
Fonte: SLEUTH KIT (2011)

5.2.3 Ferramentas para Coleta de Dados em Dispositivos de Memória

Peritos forenses, sempre são auxiliados por ferramentas que fazem a coleta de evidências em computadores suspeitos, sendo assim, estes softwares precisam ser adquiridos e levados para o local da ocorrência. Sempre podem acontecer problemas relacionados com incompatibilidade com sistemas operacionais, ou outros prováveis inconvenientes que mais tarde resultam em uma perda de tempo para o processo investigativo. Para a coleta de dados, uma boa opção contra esses riscos é otimização, usando ferramentas de LiveCD Linux, que podem ser usadas sem a necessidade de instalá-las (IEONG, 2006). Algumas destas ferramentas (RAMOS; SATURNINO, et al, 2009):

a) **Guymager** - é uma ferramenta usada em modo gráfico para aquisição de imagens forenses. Nela é possível destacar os seguintes pontos:
   - possui uma interface amigável, com acessibilidade para vários idiomas;
   - funciona em Linux;
   - novas unidades podem ser adicionadas a qualquer momento;
   - consegue usar mais de um núcleo de processamento em máquinas com esta característica.

b) **Memdump** - efetua Dump de memória em sistemas UNIX;

c) **Aimage** - utiliza o padrão aff para a geração de imagens forenses;

d) **Air (Automated Image & Restore)** - captura imagens com dd e dcfldd, determina o algoritmo hash e envia a imagem capturada via netcat ou cryptcat;

e) **Dc3ddgui** - versão com interface gráfica do dc3dd, usado para criação de imagem;

f) **Dcfldd** - é uma versão do dd aprimorada pelo departamento de defesa dos Estados Unidos;

g) **Dd** - gera imagem de dados;

h) **Dc3dd** - cria imagens bit-a-bit de uma mídia.

5.2.4 Análise de Tráfego de Rede

Como já visto anteriormente neste projeto, a forense em rede é uma parte importante da Resposta a Incidentes. Eis aqui algumas ferramentas para coleta e análise de dados:

a) **Nmap** - é uma ferramenta com código livre para exploração e auditoria de segurança em rede. Muitos administradores de rede têm de realizar um

inventário da rede, gestão de serviço, monitoramento ou disponibilidade de serviço. É possível com a ferramenta escanear redes de grande porte e também pequenas, é executado pela maioria dos sistemas operacionais como Linux, Mac OS X e Windows (NMAP, 2009);

b) **Xplico** - tem como objetivo extrair dados que estão contidos em pacotes capturados na rede como por exemplo arquivos no formato PCAP. Propõe extrair informações de e-mails, conteúdos HTTP, informação provenientes de VOIP, FTP, TFTP, entre outros. É distribuído sob a licença GNU (General Public License) (XPLICO, 2011);

c) **Xtraceroute** -versão do traceroute em modo gráfico, serve para traçar rotas;

d) **NTOP** - ferramenta que mostra o uso atual da rede (NTOP, 2011).

5.2.5 Identificação e Análise de Arquivos

Metodologias para identificação e análise de arquivos foram descritas mais acima no trabalho com exceção das ferramentas. Elas são muitas, mas segundo um trabalho de conclusão de curso usado para enriquecimento em termos de conhecimento neste projeto, são (RAMOS; SATURNINO, et al, 2009):

a) **Chkrootkit, Rkhunter** - detectam a presença de rootkits no computador;

b) **Cabextract, Orange** - acessam conteúdos de arquivos com extensão .cab;

c) **Pyflag** - conjunto de ferramentas para análise forense;

d) **Grisson Analizer** - a partir dela executa-se comandos como Mml, fsstat e imgstat, que fazem parte do Sleuth Kit para análise forense;

e) **Stegdetect** - ferramenta automatizada que tem como objetivo de detectar imagens que portam conteúdo esteganográfico;

f) **Eindeutig** - analisa arquivos com a extensão .dbx;

g) **Fccu-Evtreader, Grocevt** - visualizam arquivos de eventos provenientes de sistema Windows;

h) **Regripper** - extrai e analisa dados do registro;

j) **Rifiuti** - tem como objetivo analisar arquivos INF2.

5.2.6 Recuperação de dados em disco

Algumas ferramentas para recuperação de dados em discos rígidos presentes no Helix, modo Linux (RAMOS; SATURNINO, et al, 2009):

a) **Magicrescue** - recupera imagens raw;

b) **Ntfsundelete**, **Scrounge-Ntfs**, **Fatback**, **E2undel** - têm como objetivo recuperar arquivos deletados em partições ext3, Ntfs;

c) **Recover** - sua principal função é recuperar informações apagadas de inodes;

d) **Recoverjpg**, **Jpgforemost** - como o nome sugere, recupera, imagens no formato jpg;

i) **Photorec** - recupera arquivos de vários tipos, mas seu principal foco é recuperar arquivos de imagem e vídeo;

j) **Testdisk** - objetiva a recuperação de partições, geralmente quando ocorreu algum tipo de erro específico ou problemas com vírus;

k) **Mondorestore** - ferramenta usada pare restaurar informações de fitas, CD's ou HD's;

l) **Ddrescu** - ferramenta que recupera dados de uma partição para outra, efetuando uma cópia.

5.2.7 Análise de arquivos temporários de navegadores

Algumas ferramentas para análise de arquivos provenientes de navegadores (RAMOS; SATURNINO, et al, 2009):

a) **Mork** -visualiza arquivos history.dat do Firefox;

b) **Galleta** - tem como objetivo analisar cookies do Windows;

c) **Pasco** - analisa a cache do Internet Explorer;

d) **Coockie_cruncher** - analisa cookies de vários navegadores

5.3 SISTEMA DE DETECÇÃO DE INTRUSÃO (IDS)

São sistemas com objetivo de monitorar e analisar eventos que acontecem em um computador ou rede quando existe riscos de ocorrência de um provável incidente, que correspondem a violações ou ameaças iminentes de políticas de segurança de informação de uso aceitável ou praticas de segurança comuns. Um sistema de detecção de intrusão automatiza processos que visam detectar intrusões (SCARFONE; MELL, 2007, tradução nossa).

Uma organização quando não tem a capacidade de detectar uma falha de segurança rapidamente, dificilmente proverá uma resposta ao incidente de forma eficaz. A etapa de detecção é uma das mais importantes, é a fase, em que, curiosamente, os profissionais experientes têm menor controle (MANDIA, PROSISE, 2003, tradução nossa).

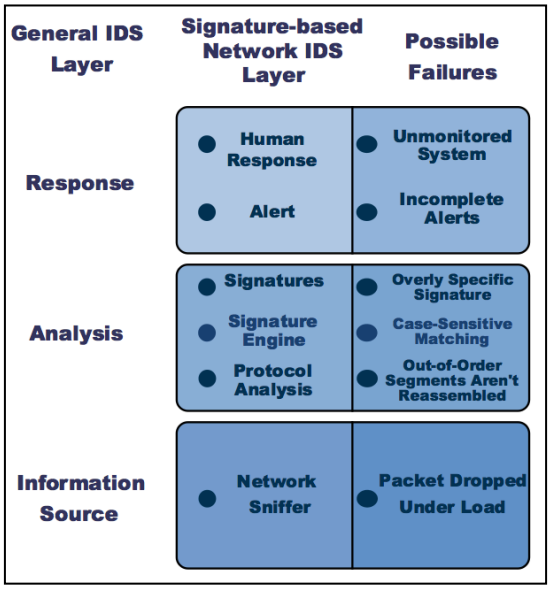


Figura 20. Modelo de Sistema de Detecção de Intrusão e casos de falha
Fonte: SKAION (2009)

Incidentes, normalmente são detectados quando alguém do time de segurança suspeita que um evento não autorizado, inaceitável ou ilegal, está ocorrendo ou ocorreu envolvendo a rede da organização, computadores, ou algum outro equipamento de processamento (MANDIA, PROSISE, 2003, tradução nossa).

5.3.1 Tipos de Sistemas de Detecção de Intrusão

Segundo a RED HAT (2005, tradução nossa) muitos IDS baseiam-se em conhecimentos, que preventivamente alertam os administradores de segurança, fazendo uso de um banco de dados contendo informações sobre os ataques mais comuns. IDS são baseados em comportamentos, a partir destes são feitos rastreios a procura de anomalias que comumente são sinais que atestam a ocorrência de algum tipo de atividade maliciosa. As IDS atuam de maneira autônoma, quase sempre em segundo plano e ficam monitorando todas as atividades de modo passivo, fazendo um registro de todos os pacotes suspeitos do lado de fora do sistema.

Na área da segurança da informação, os tipos mais conhecidos de IDS são os baseados em hosts e em redes. Em *host* são considerados por muitos como sendo mais completo. Compreende a implementação de um sistema detector de intrusão para cada host, desse modo o host mantem-se protegido não importando a que ambiente de rede o mesmo pertence. Os baseados em rede são tidos como menos abrangentes, isto porque em um ambiente com mobilidade ele pode tornar-se indisponível para que se efetue uma triagem de confiança nos pacotes. Abaixo encontram-se com mais detalhes informações sobre os 2 tipos de IDS (RED HAT, 2005, tradução nossa):

a) **IDS baseado em host** - possibilita fazer análise de vários segmentos o que ajuda a determinar mau uso (atividades maliciosas ou uso indevido da rede), ou intrusão (alguma ameaça vinda de fora). Sendo baseado em *host* possui a possibilidade de consultar vários tipos de logs (kernel do sistema, servidor, rede, firewall, entre outros). Verificam a veracidade dos dados de arquivos executáveis importantes em um banco de dados confidencial e cria um checksum para cada ficheiro md5sum (algoritmo de 128 bits) ou também sha1sum (algoritmo de 160 bits), em seguida são armazenados valores em um arquivo de texto que é comparado periodicamente. Caso algum checksum não seja igual, será emitido um alerta por e-mail para o administrador;

b) **IDS baseado em rede** - escaneiam pacotes da rede a nível do roteador ou host, dados de pacote, auditoria e registra todos os pacotes suspeitos em arquivos especiais com dados extras. Capturando pacotes suspeitos, os mesmo são comparados com dados presentes em um banco de dados contendo assinatura com os ataques mais comuns. Com isso, atribui um nível de severidade para cada um dos pacotes. Caso estes níveis atinjam níveis incomuns é enviado um e-mail ao administrador para que seja feita um

investigação sobre a natureza da anomalia. Grande parte deste IDS têm como exigência a definição do dispositivo de rede para modo promiscuo.

5.3.2 Algumas Ferramentas para Detecção de Intrusão

São ferramentas de IDS aquelas que são usadas para detecção de alguma atividade não autorizada pelo administrador do sistema, analisam todos os pacotes que trafegam pela rede, sobretudo aqueles suspeitos, que são prontamente comparados com assinatura existentes (NETO .R, 2006?):

5.3.2.1 RealSecure

É um filtro contra intrusão que age protegendo a rede e sistemas que se encontram em missões críticas ou conectados. Quando o trâfego circula pelo mesmo é analisado ao mesmo tempo, e são procurados dados que evidênciam a iminência de um ataque ou algum uso indevido. Caso seja detectado alguma anomalia, os dados ficam encapsulados em um bloco que o mantém de quarentena para que não passe para outra interface. Protege a capacidade de processamento de pacotes, garantindo a alta velocidade dos links de rede (B2NET, 2011, tradução nossa).

5.3.2.2 Asgaard

É um sistema com métodos próprios para IDS, a sua arquitetura baseia-se em formas modulares que são repartidos em vários computadores da rede e possuem diferentes

conceitos, que vão desde funções básicas como colher e analisar informações tidas como atividades finais, até autenticação. Este sistema e dotado de uma infraestrutura que possibilita primitivas de iteração, confiança, e autenticidade (CAMPELLO; WEBER, 2001).

5.3.2.3 Intruder Alert

É um Sistema de Detecção de Intrusão baseado em host, monitora e detecta violações de segurança em tempo real, respondendo automaticamente. Quando é detectada uma ameaça, é ativado um alarme levando em conta as politicas de segurança estabelecidas. São tomadas outras medidas preventivas. No painel central podem-se implantar diretrizes seguras para coletar e arquivar logs, que, posteriormente serão analisados por um auditor, mantendo sempre o sistema ativo, garantindo a integridade dos dados contidos no mesmo (SUPERWAREHOUSE, 2011).

5.3.2.4 Snort

É um software de segurança moderno que pode atuar como um Sniffer de pacotes, Packet Logger, ou como um sistema de detecção de intrusão (IDS). Junto com o programa foram desenvolvidos módulos adicionais que proporcionam modos diferentes para manutenção de um conjunto de regras, formas de gravação e gerenciamento dos logs arquivados, alertando, permitindo assim que seus administradores saibam sobre a presença no trafego de algum dado malicioso (BAKER; CASWELL, 2004, tradução nossa).

Como Sniffer, o Snort atua fazendo a leitura de todos pacotes que trafegam na rede, como Packet Logger ele funciona registrando todos os pacotes no disco, e como

detector de intrusão que é a parte aonde ele é mais completo e consequentemente possui uma configuração mais complexa, ele efetua análises do tráfego de rede procurando por eventuais tentativas de invasão, a partir de algumas regras que são definidas pelo administrador da rede (SILVA, 2003).

6 TRABALHOS CORRELATOS

A área da perícia forense computacional, sendo relativamente nova em relação a outras ciências, ainda possui muito pouco material de consulta, e, principalmente em língua portuguesa. Essa carência tende a diminuir, levando em conta que o número de peritos e pessoas interessadas neste assunto cresce. Alguns trabalhos notáveis serão descritos nos capítulos a seguir.

6.1 SISTEMA PARA GRUPOS DE RESPOSTAS A INCIDENTES DE SEGURANÇA EM COMPUTADORES

Projeto de Conclusão de Curso desenvolvido por Cristiano da Costa na Universidade Luterana do Brasil, constituiu parte do objeto de estudo do presente projeto. O autor teve como principal objetivo, fazer a integração de um sistema de acompanhamento de requisições para resposta a incidentes.

O autor falou sobre as ferramentas de segurança para Linux atualmente existentes no mercado, mas focando para varreduras de vulnerabilidades, detecção de intrusão, trabalho com filtros de pacotes, bem como monitoramento de serviços de rede e servidores.

A resposta a incidentes foi tratada de maneira a relacionar-se com políticas e procedimentos em perícia forense

6.2 CRIMES CIBERNÉTICOS, COMO ENFRENTÁ-LOS DE MANEIRA CORRETA ATRAVÉS DA LEGISLAÇÃO BRASILEIRA UTILIZANDO-SE DA COMPUTAÇÃO FORENSE, BOAS PRÁTICAS, METODOLOGIAS E FLUXO DE PROCESSOS, SOLUCIONANDO OS QUESITOS TÉCNICOS COM O SOFTWARE LIVRE HELIX

Projeto de conclusão de curso feito por Marcelo Ingarano, Paulo Francisco e Silvio Pereira no Instituto Tecnológico de Aeronáutica cuja orientação foi do escritor e perito forense Sandro Melo. O objetivo foi efetuar uma relação entre a computação e a parte jurídica criminal por meio das leis existentes. O autor falou das metodologias usadas para efetivação de uma perícia forense, práticas jurídicas diárias entre outros, sempre frisando a parte de crimes de informática.

Com os casos fictícios o autor deixou claro o uso das ferramentas livres presentes nos softwares proposto para estudo de caso, o Helix 3. Elas foram explicadas detalhadamente, funcionamento e regras de manipulação das mesmas, para que não se invalide as provas digitais.

6.3 ANÁLISE FORENSE EM SISTEMAS GNU/LINUX

Trabalho de conclusão de curso escrito por Frederico Argolo, na Universidade Federal do Rio de Janeiro, teve como principal objetivo descrever os passos guiados por lei para efetivação de uma perícia forense.

O autor deu preferência à abordagem de tópicos relacionado ao tratamento de evidências digitais, desde a coleta até o processo de análise. Por ser um trabalho focado em ferramentas livres, foram descritas e exemplificadas algumas das ferramentas mais usadas

presentes no Linux. Este é um trabalho que também serviu como meio de estudo em vários pontos para efetivação do presente projeto.

6.4 PERÍCIA FORENSE COMPUTACIONAL - ATAQUES, IDENTIFICAÇÃO DA AUTORIA, LEIS E MEDIDAS PREVENTIVAS

Ana Trevenzoli, é a autora deste projeto de conclusão de curso, feito em 2006 na Faculdade SENAC de Sorocaba.

O projeto teve o objetivo de descrever as técnicas usadas por peritos forenses na identificação da origem de um ataque, autoria e as medidas preventivas a posterior.

O trabalho focou os procedimentos usados para realização de uma fraude objetivando o desvio de dinheiro. Tratou de explicar também algumas técnicas chamadas de métodos anti-forenses, que servem para inibir o trabalho feito por um perito.

6.5 PERÍCIA FORENSE APLICADA À INFORMÁTICA

Realizado por Andrey Freitas, o trabalho apresenta conceitos sobre perícia forense computacional, nomeadamente falando sobre as etapas discorridas neste processo, desde a coleta, até a análise dos resultados.

Parte importante neste trabalho, é a quantidade de comandos forenses que o autor apresenta, demonstrando como devem ser usados, por meio de imagens. Apresenta ainda uma descrição das mesmas ferramentas com o objetivo de clarear, para quê? E quando elas devem ser usadas.

7 FERRAMENTAS E METODOLOGIAS PARA RESPOSTA A INCIDENTES

Tratar Incidentes de Segurança em tempos globalizados como hoje é essencial para as organizações, sobretudo para as que têm altos lucros e as que precisam manter um nível de segurança elevado para que os seus dados não sejam comprometidos.

Muitos profissionais da área da segurança da informação, mais especificamente da área de perícia forense computacional, debatem-se muito com algumas lacunas que existem quando se fala em forense na computação. Isso porque a área carece de normas devidamente padronizadas por especialistas e estudiosos da área, existem ainda outras dificuldades como a falta de ferramentas acessíveis e de fácil uso, bem como a falta de documentação das poucas que existem.

Com o presente trabalho, objetiva-se demonstrar mediante a um estudo de caso, fazendo análises e seguindo passo a passo, como e quando se deve prover uma resposta a incidentes, quais as ferramentas, metodologias e outras técnicas utilizadas para efetivação de uma perícia forense computacional. No decorrer do estudo, será mostrado o funcionamento de cada ferramenta estudada, como e quando usa-la.

Com isso, pretende-se que o trabalho venha também dar uma contribuição na área, e que sirva de um guia para estudantes e pessoas que pretendam ampliar os seus conhecimentos.

7.1 METODOLOGIA

A primeira etapa deste projeto, compreendeu a coleta de material bibliográfico, recolheu-se bibliografia relacionada a crimes digitais, algumas metodologias existentes para perícia forense computacional e resposta a incidentes, algumas particularidades do Helix 3

dentre outros assuntos não menos importantes incluídos no tema. A bibliografia usada foi grande parte traduzida da língua inglesa devido à carência de material em português. Foi usado material proveniente de bases de dados que contêm publicações de congressos e trabalhos de conclusão de curso relacionados com perícia forense.

Na segunda etapa será realizado um estudo de caso com o objetivo de demonstrar mediante a um caso fictício o uso de algumas ferramentas forenses e metodologias para resposta a incidentes.

7.2 ESTUDO DE CASO

Nesta etapa será apresentado um caso de estudo, que como dito anteriormente, facilita por meios práticos na compreensão de como e quando as ferramentas devem ser usadas, e qual a confiabilidade da ferramenta tendo em conta os objetivos que estas se propõem alcançar.

7.2.1 Metodologia da perícia forense

O presente caso de estudo é um desafio proposto pelo especialista forense Eriberto Mota. Foi montado pelo mesmo e simula um ambiente real propício para análise forense.

Um executivo há muito tempo vinha sendo investigado internamente por usar os computadores da empresa para fins proibidos, bem como criminosos perante à lei. Em conjunto com a polícia, foi descoberto que o mesmo facilitava e ou proporcionava encontros com menores de idade. Depois de quase 2 anos de investigação, a empresa foi tomada de assalto por policiais que efetuaram a sua prisão. Após se procurar por elementos que incriminassem o suspeito ou que de alguma forma o ligassem a estas atividades ilícitas, nada

foi encontrado. Foi então apreendido o computador do suspeito para que posteriormente fosse mandado para um perito forense computacional.

Mediante acesso ao relatório de interrogação do suspeito, conseguiu-se saber que o mesmo vinha aperfeiçoando técnicas que facilitassem o mesmo a atrair as crianças, bem como provavelmente poderia manter um banco de dados contendo fotos que ele posteriormente disponibilizava na Internet com o objetivo de atrair interessados por esta prática.

Para este caso em especifico, será utilizada a metodologia de perícia forense denominada SOP já descrita neste trabalho, que é feita em 7 etapas conforme a figura 21. A escolha desta metodologia deve-se pelo fato de a mesma ser amplamente aceita em território brasileiro, de referir que a escolha da metodologia pode condicionar a aceitação da prova em ambiente judicial.

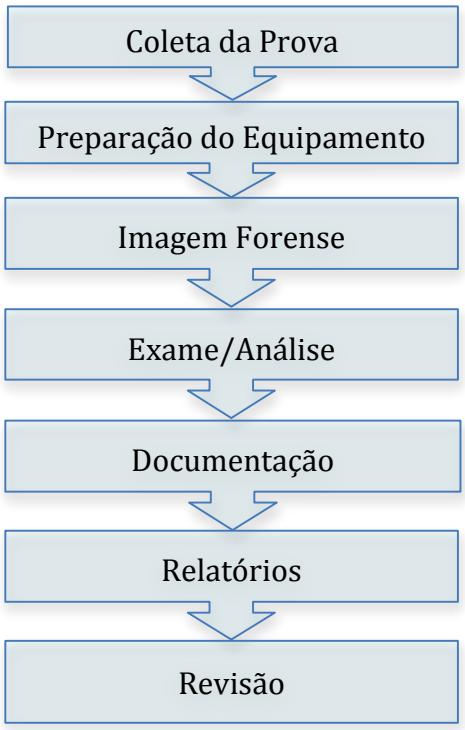


Figura 21. Fluxograma da metodologia SOP
Fonte: SWGDE (2006)

7.2.2 Coleta da Prova

Sabendo-se que o caso é proveniente de um ambiente de estudo, o mesmo já se encontra devidamente armazenado, ou seja, já foi coletado. A coleta da prova foi efetuada com software livre, sendo este baseado no comando DD.

A fase da coleta constitui uma parte importante no processo forense como já foi dito em vários capítulos. As evidências devem ser coletadas tomando todo cuidado possível para que não sejam alteradas ou danificada, tendo atenção nos softwares que ira utilizar, para que estes não alterem o estado como foi encontrada a máquina.

7.2.3 Preparação do equipamento

Naturalmente para que faça uma pesquisa forense é necessário que se criem condições para que a mesma ocorra sem sobressaltos, condições essas que vão de software a hardware.

Para análise das evidências depois de coletada foi criado um laboratório improvisado com condições minimamente aceitáveis em termos de software e hardware:

Figura 22. Computador usado para análise forense

a) um computador com 500 Gb de disco rígido, 4 Gb de memória ram, com os sistemas operacional Windows 7 e Ubuntu;
b) um disco rígido Samsung com 320 Gb;
c) um disco rígido externo com dois Terabytes;
d) softwares para perícia forense - Helix 3 pro, Helix 2008, FDTK, CAINE dentre outros de origem livre.

7.2.4 Imagem Forense

A imagem foi recolhida com êxito, e armazenada em um disco rígido externo com a capacidade de 320 Gb que antes foi devidamente formatado.

Como toda e qualquer perícia forense, a imagem a ser analisada, depois de coletada, deve ser submetida a um algoritmo com a finalidade de gerar um código *Hash,* nesse caso foi utilizadoo algoritmo MD5, conforme a figura 23.

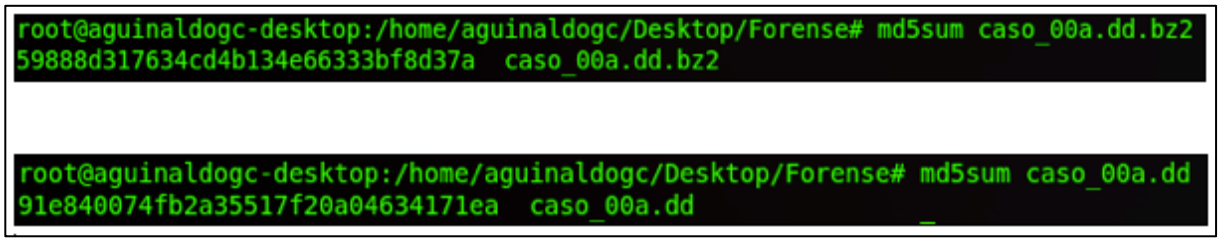


Figura 23. Geração do Hash na imagem comprimida e descomprimida

7.2.5 Exame/Análise

Para realizar a análise efetuou-se primeiro uma duplicação da cópia da imagem como determina os procedimentos estabelecidos pela metodologia SOP, pois, em caso de algo

inesperado acontecer, pode-se recorrer a imagem inicialmente coletada, e dar sequência à pesquisa.

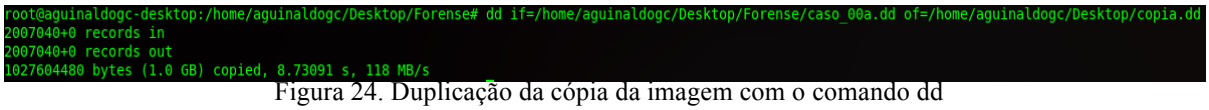


Figura 24. Duplicação da cópia da imagem com o comando dd

Figura 25. Geração do Hash da cópia da imagem com o dd

A cópia da imagem foi feita utilizando o comando dd, que é encontrada no CD do Helix conforme mostra a figura 24, e foi gerado um código Hash para confirmar, que a imagem não sofreu alteração nenhuma. Durante a duplicação da mesma, pode ser verificado na figura 25 que o código Hash é igual ao código Hash inicial da imagem, conforme ilustrado igualmente na figura 23.

Naturalmente para se fazer a análise é necessário que a imagem forense seja montada no sistema, e para tanto é necessário que a mesma receba somente a permissão de leitura. Por se tratar de uma imagem em formato RAW e possuindo 2 partições cada uma com um tipo de sistema de arquivo, torna-se um pouco mais trabalhoso fazer a montagem, devendo-se utilizar opções adicionais para que isto seja realizado.

Primeiramente foi usado o comando sfdisk com o argumento -luS, que serve para listar as informações de todas as partições presentes na imagem como o setor em que iniciam e terminam, a letra de identificação, e o tipo de sistema.

No caso da imagem a ser analisada, possui 2 partições com sistemas de arquivos diferentes, a primeira é formatada em FAT32, começa no sector 62 e termina no 1051519, e a segunda está formatada em ext3 (Linux), começa no sector 1051520 e termina no 2005823, conforme mostra a figura 26.

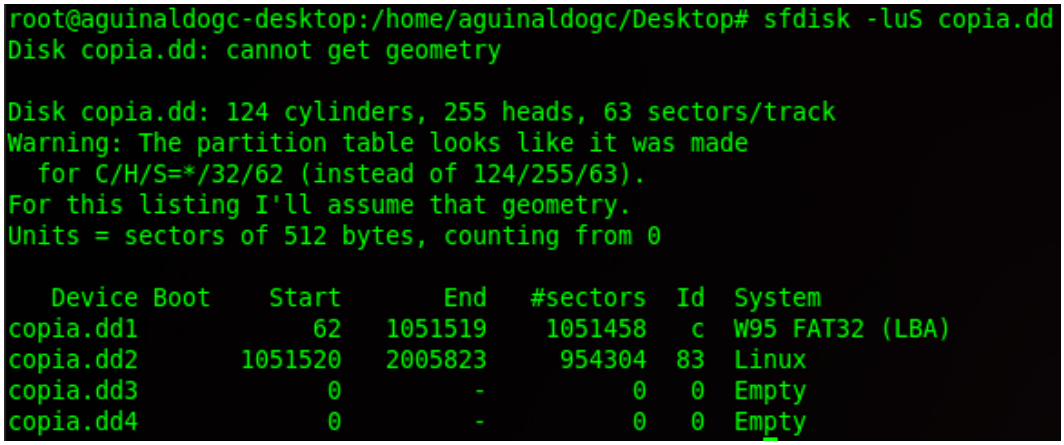


Figura 26. Uso do comando sfdisk

Depois da obtenção das informações das partições, passou-se a etapa da montagem das mesmas. Foram montadas em modo de leitura via terminal com o comando *mount* e alguns parâmetros adicionais (figura 27):

a) **mount** - monta um sistema de arquivos;

b) **o** - indica que a partição será montada com opções adicionais;

c) **loop** - identifica as partições

d) **ro** - monta a imagem apenas em modo de leitura;

e) **noexec** - desabilita a execução que qualquer arquivo binário na imagem;

f) **offset** - usado quando é feita a montagem de uma imagem com mais de uma partição.

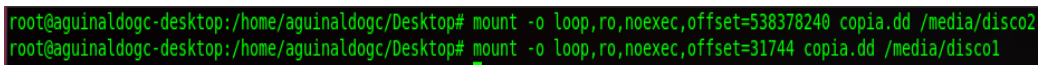


Figura 27. Montagem da imagem

Foi feita uma análise preliminar para que se visualizasse a estrutura interna de cada partição detalhadamente. A ferramenta usada para tal foi a *tree*, que pode ser encontrada

nos repositórios do Ubuntu. Acessandodo a partição (disco 1) e executando o comando, obteve-se as seguintes informações (figura 28):

a) possui apenas um diretório, chamado “fotos”;

b) dentro do diretório fotos encontram-se vários arquivos no formato .jpg;

c) a partição possui um total de 18 arquivos.

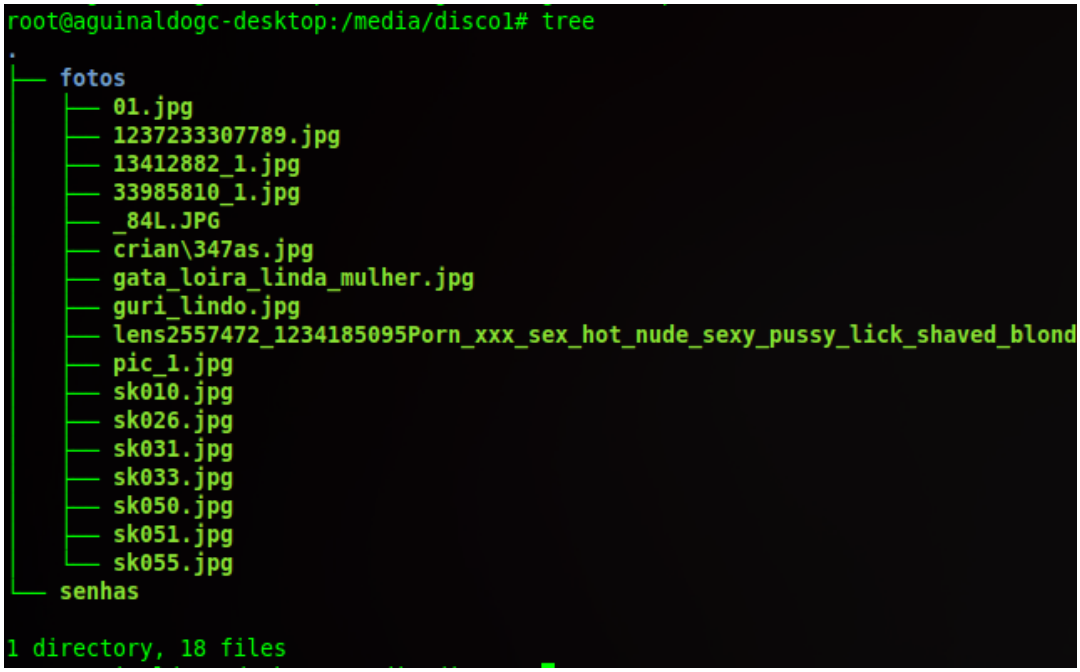


Figura 28. Uso do comando tree no disco 1

Pode-se observar nesta árvore de arquivos que alguns dos arquivos possuem nomes que vão de encontro com o que se procura, que são informações relativamente a respeito de atividades criminosas relacionadas com pornografia infantil:

a) crian\347as.jpg;

b) gata_loira_linda_mulher.jpg;

c) guri_lindo.jpg;

d) arquivos com nome com várias expressões pornográficas em língua inglesa.

Usou-se o mesmo comando, *tree*, na segunda partição, com o sistema de arquivos Ext3 (Linux), que retornou a informação de que a partição (disco2) possui um total de 162

arquivos, distribuídos em 9 diretórios, e, nesse espaço, foram encontradas as seguintes informações suspeitas:

a) arquivos html com expressões como pedófilos e criança (figura 29);

b) arquivos com extensão jpg., alguns com nomes que se relacionam as buscas (figura 30);

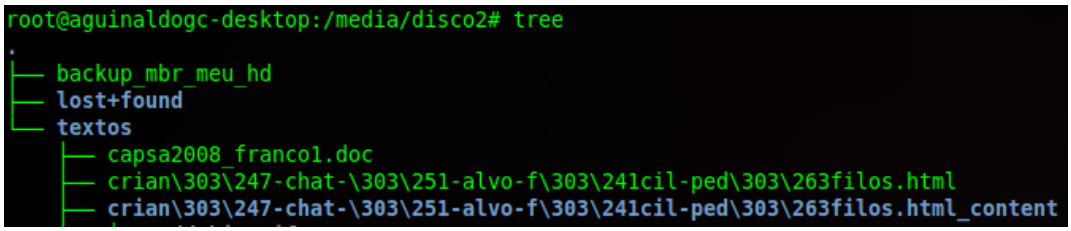


Figura 29. Uso do comando tree no disco 2

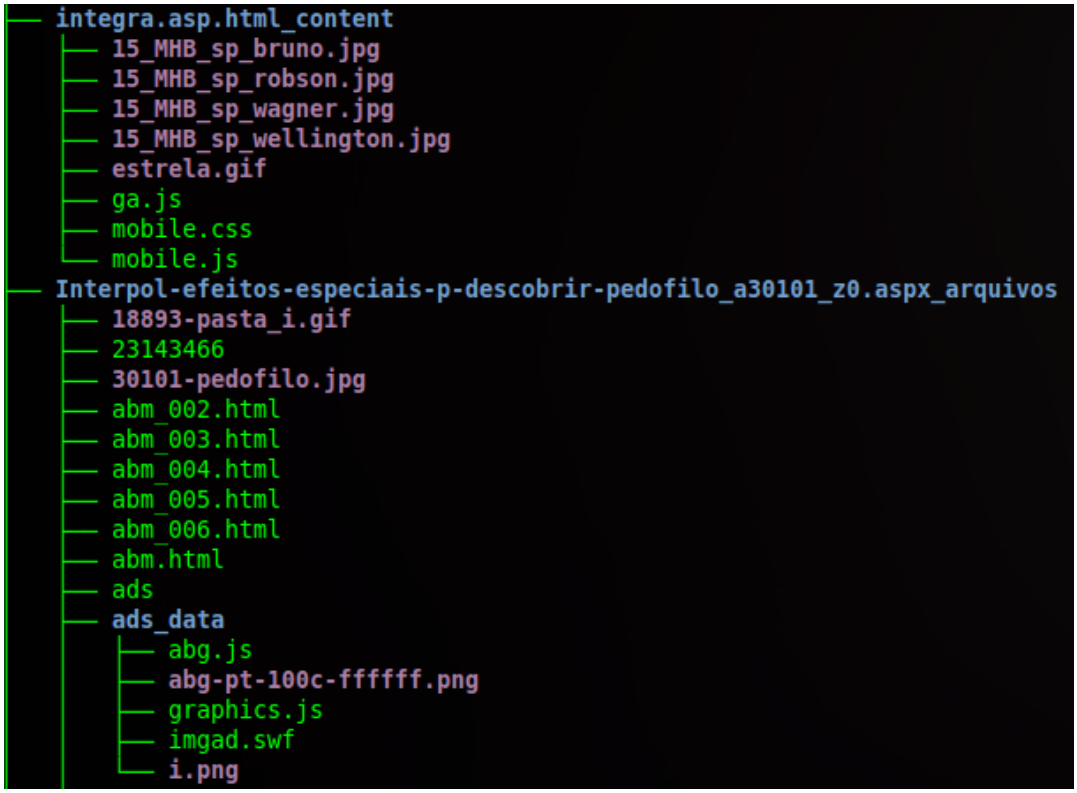


Figura 30. Uso do comando tree no disco 2

Por se tratar de uma análise preliminar, não se tirou nenhuma conclusão a respeito dos arquivos considerados suspeitos encontrados nas duas partições, sendo que até ao

momento, as evidências encontradas ainda não foram visualizadas, para comprovação de que se tratam realmente de imagens de pornografia infantil.

Passou-se para o uso de um software presente no Helix, já falado nos capítulos anteriores, o *Autopsy*, é um software que funciona por meio de um browser, e serve para fazer análise da imagem forense em diversos formatos, fornecendo diversos tipos de informações, bem como ajuda na visualização de arquivos apagados e sua posterior recuperação.

Para ser iniciado, precisa-se apenas digitar "*Autopsy*" no terminal, é apresentado então informações com procedimentos de como abri-lo no navegador (figura 31). Deve-se digitar no navegador, o endereço http://localhost:9999/autopsy. É importante que o script no terminal mantenha-se rodando.

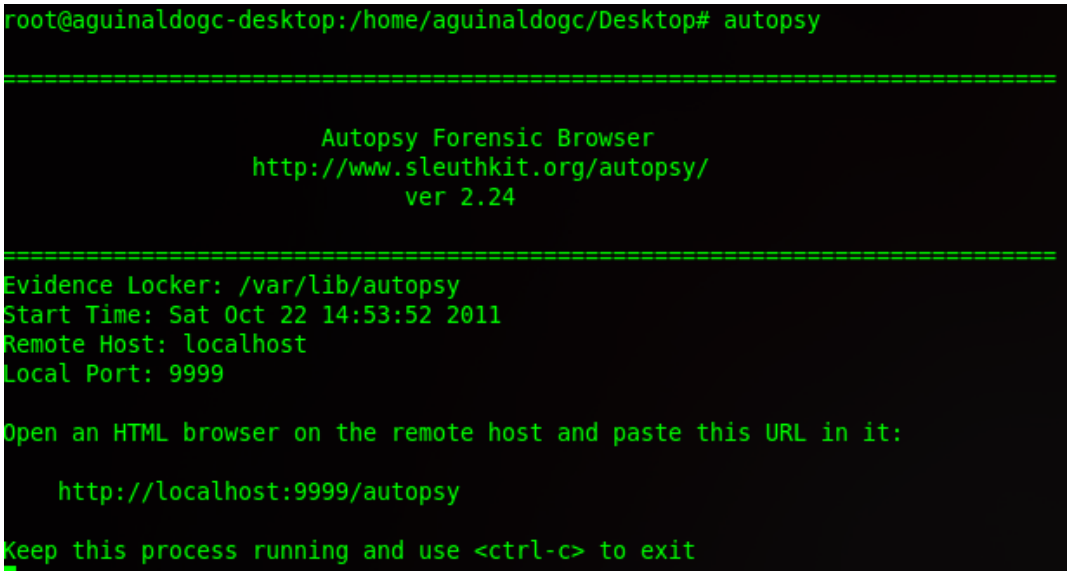


Figura 31. Início do Autopsy Forensic Browser

Na primeira tela, pode-se abrir um caso que estava sendo estudado em um momento anterior, criar um novo caso ou ainda acessar a ajuda, aonde contém instruções de como utilizar a ferramenta (figura 32).

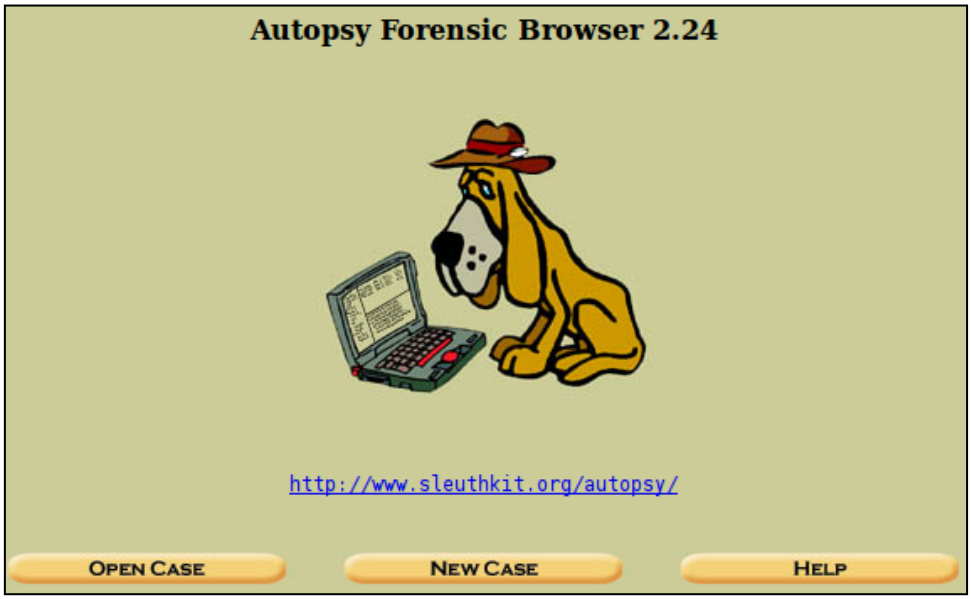


Figura 32. Tela inicial do Autopsy

O passo a seguir é a criação de um caso, com informações que deverão ser inseridas em campos pré-definidos na ferramenta, como, o nome do caso, uma breve descrição do caso, e o nome dos investigadores. No caso a ser analisado foi definido com o nome “Pedofilia”, descrição “Análise de HD suspeito”, e como investigador “Aguinaldo Cristiano“ conforme a figura 33.

As informações inseridas em todos os passos durante a criação do caso forense para posterior análise devem ser as mais completas possíveis, pois elas deverão fazer parte do relatório final que o perito irá emitir quando o caso for finalizado.

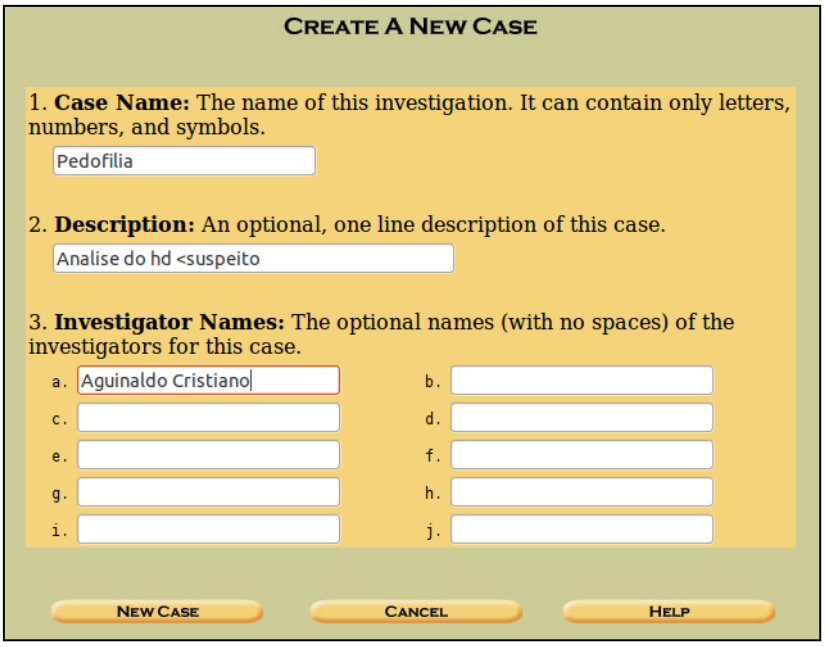


Figura 33. Criação de um novo caso

Todas as informações relativas à investigação, todos os hash gerados, anotações feitas durante a análise, relatórios, e outros dados que sejam relacionados ao caso, serão armazenados sempre no diretório criado com o nome do mesmo. A localização do diretório é apresentada logo que o caso é criado, onde as informações ficaram armazenadas no diretório /var/lib/autopsy/Pedofilias (figura 34).

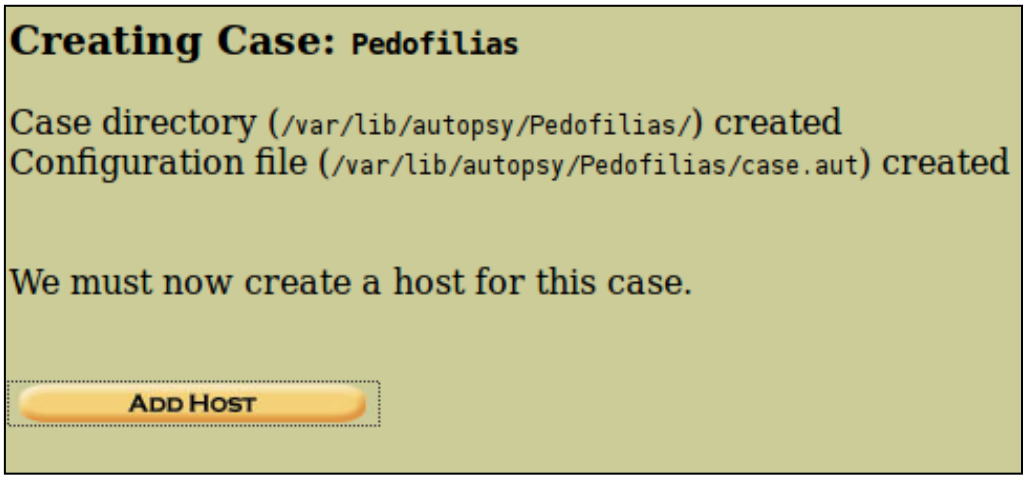


Figura 33. Diretório aonde foi criado o caso

Com o caso criado, é necessário que se identifique um *host* (figura 34), ou seja, o computador a ser investigado, deve-se inserir uma breve descrição que relacione o computador com a investigação no campo “Description”. O campo *time zone* refere-se as horas que se deverão ter como base na hora de traçar um *timeline,* ou quando os relatórios forem gerados.

No campo *timeskew adjustment* é para ser inserido quantos *clocks* o computador encontra-se atrasado, caso estiver, deve-se compensar a diferença digitando um valor no campo com sinal negativo.

Path of alert hash database, nesse campo a ferramenta oferece a possibilidade de se criar um banco de dados aonde serão armazenados todos os códigos hash gerados durante a análise forense.

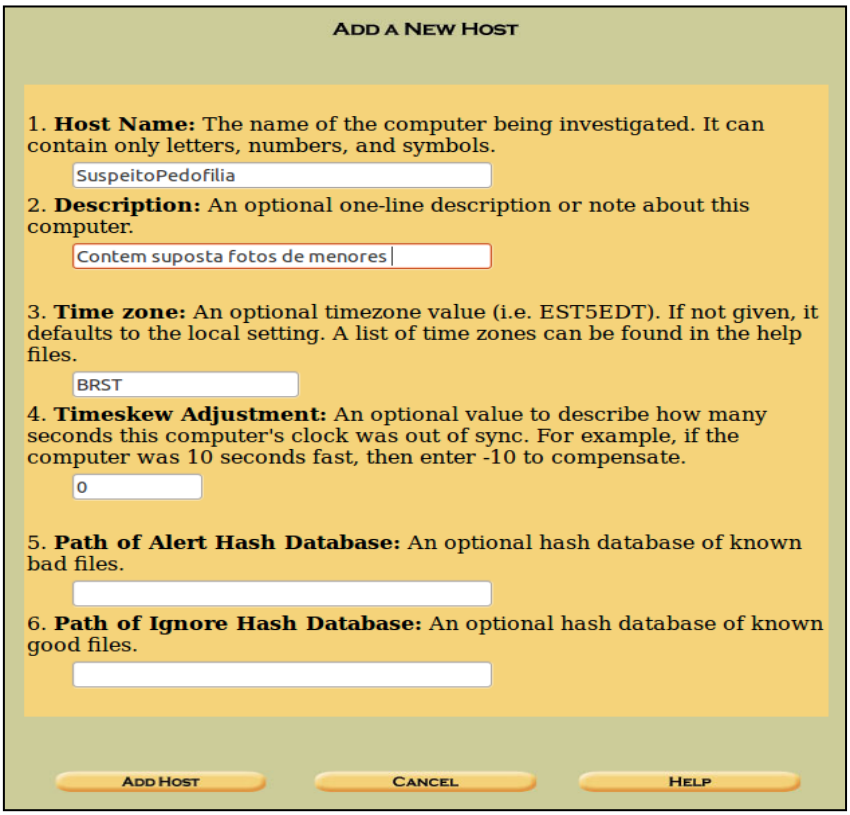


Figura 34. Criação do identificador do host

É chegado então o momento em que a cópia da imagem forense criada tem de ser adicionada, aqui tem de ser observados aspectos importantes, como por exemplo o fato de não se poder ter espaço no nome dos diretórios, e, no caso da imagem for gerada por partes no formato .RAW ou Encase, deve-se utilizar como extensão um asterisco "*". A imagem é .RAW, mas como foi gerada a partir do comando dd, possui o formato .dd.

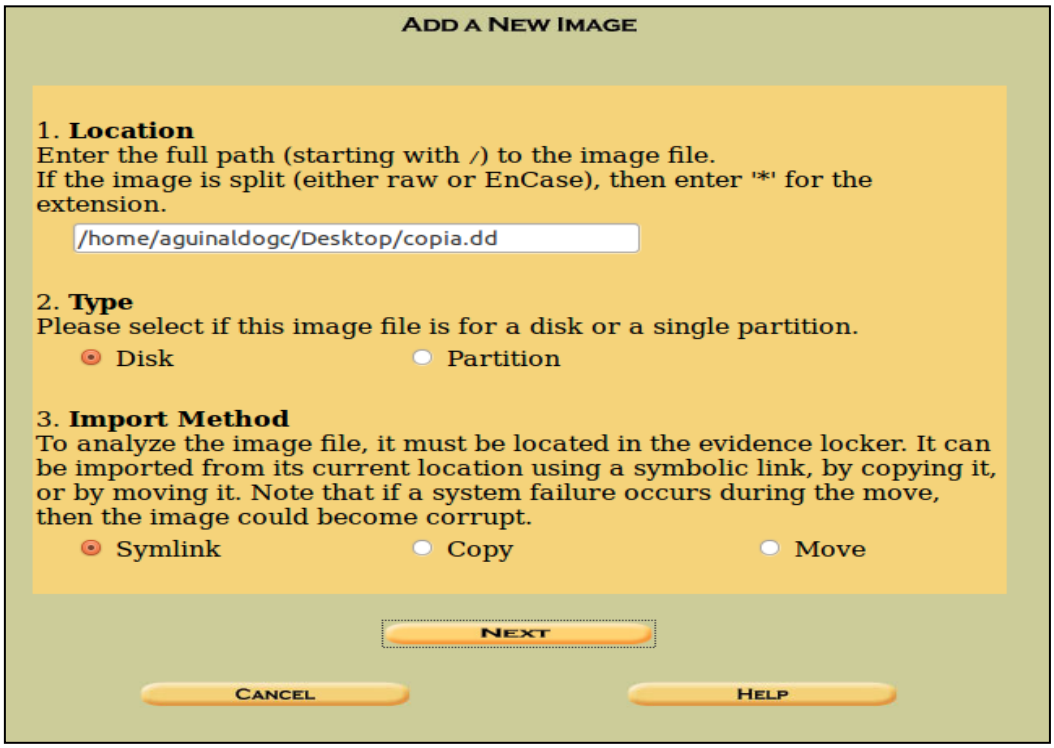


Figura 35. Adição da imagem

Um disco rígido pode ser coletado na sua totalidade ou então apenas as partições que se pressupõe serem de utilidade para o caso, para o presente caso foi copiado o disco rígido inteiro. O disco rígido possui um total de duas partições como já foi explicado.

Feita a etapa de cópia foi então importado com o método Symlink, onde o mesmo cria um link para o diretório aonde se encontra a imagem que é passado por parâmetro para o autopsy. A imagem pode ainda ser copiada ou movida para o diretório aonde o caso foi criado.

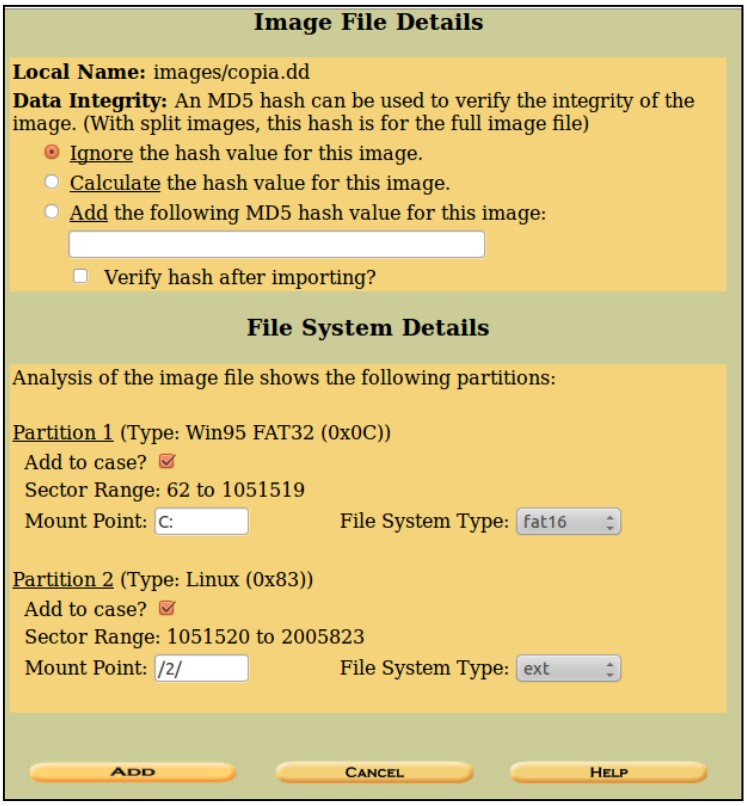


Figura 36. Geração do hash e detalhes do sistema de arquivos

A figura 36, é a tela seguinte, logo que a imagem é adicionada para análise, e nela é de forma opcional gerado um código hash. Aqui ele foi gerado de forma a garantir a autenticidade da cópia conforme pode-se observar na figura 37. De reparar que o código gerado agora e o representado na figura 25 são iguais, provando assim que a mesma continua intacta, ou seja no seu estado inicial, esta prática ajuda no processo de validação da prova digital em tribunal.

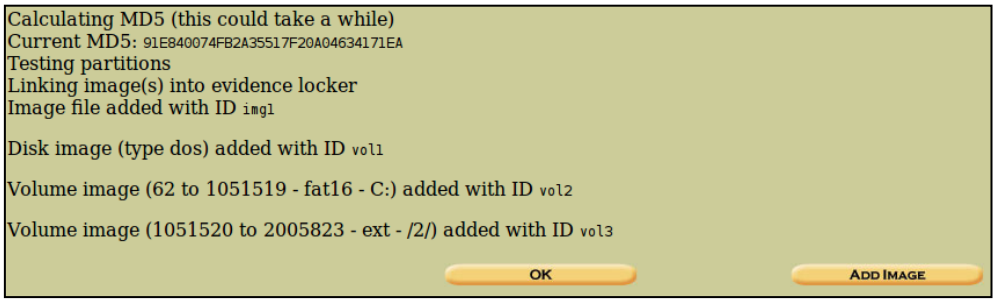


Figura 37. Código hash gerado e detalhes dos sectores dos disco duro.

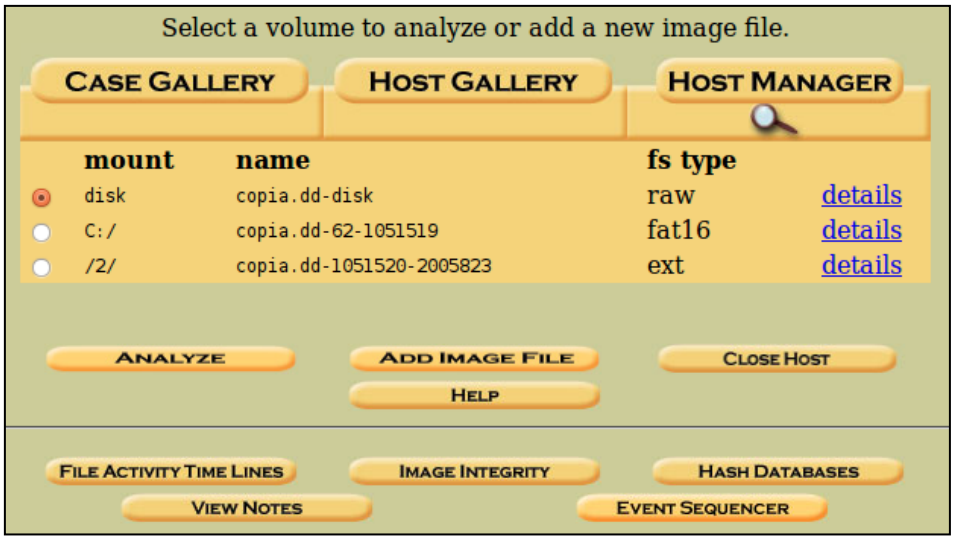


Figura 37. Código hash gerado e detalhes dos sectores dos disco duro.

Na figura 37, são apresentadas algumas informações como o tipo de arquivos do sistema, e o ponto de montagem de cada partição. As opções presentes na figura referem-se a:

a) ***analyze*** - ponto de partida para o princípio da análise propriamente dita, mostra a estrutura dos diretório e os respectivos arquivos contidos;

b) ***add image file*** - serve para adicionar outras imagens forenses ao caso;

c) ***close host*** - fecha o host, encerrando a análise;

d) ***help*** - apresenta algumas informações que podem ajudar no uso da ferramenta;

e) ***file activity time lines*** - cria uma *timeline* dos eventos ocorridos;

f) ***image integrity*** - verifica o estado atual no que concerne a integridade da imagem, comparando os hash armazenados na base de dados com os atuais;

g) ***hash databases*** - apresenta os códigos hash armazenados no banco de dados;

h) ***view notes*** - contém as notas feitas no decorrer da análise;

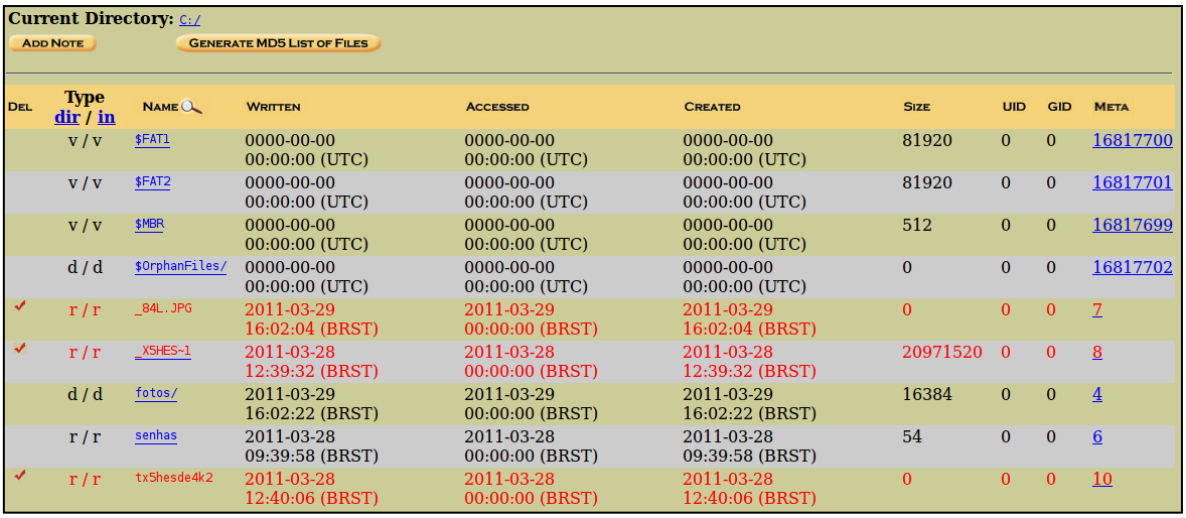
i) ***event sequencer*** - estabelece uma sequência de eventos.

Com a opção *analyze* começa-se então fazer-se a análise do caso proposto efetivamente, de modo gráfico, com a ferramenta. Começou-se primeiro por analisar a

partição que se encontra no formato FAT, e foi encontrada a seguinte estrutura de arquivos, conforme mostra a figura 38.

A figura mostra a raiz da partição “C:/” que ao contrário da ferramenta *tree* apresenta dois diretórios, fica aqui evidênciado a importância de se fazer a análise utilizando mais de uma ferramenta, pois algumas podem conter atributos mais eficientes que a outra, conforme o resultado que nos é apresentado aqui. Os diretórios que não apareceram com o uso do comando *tree* são o “$OrphanFiles, $FAT1, $FAT2, $MBR”.

Arquivos ou diretórios “$FAT1, $FAT2 e $MBR, contêm informações nativas do sistema de arquivos da partição, e o “OrphanFiles “ contém arquivos deletados.



Current Directory: C:/

ADD NOTE | GENERATE MD5 LIST OF FILES

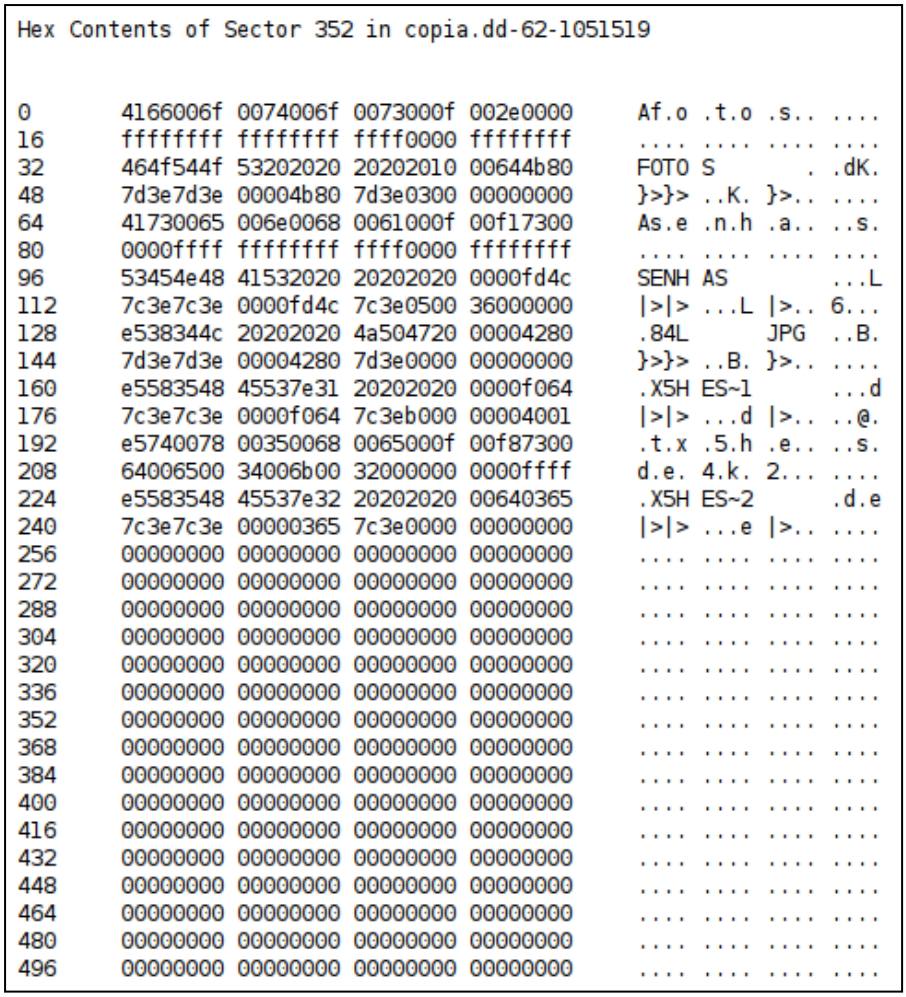
DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
	v / v	$FAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	81920	0	0	16817700
	v / v	$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	81920	0	0	16817701
	v / v	$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	16817699
	d / d	$OrphanFiles/	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	16817702
✓	r / r	_84L.JPG	2011-03-29 16:02:04 (BRST)	2011-03-29 00:00:00 (BRST)	2011-03-29 16:02:04 (BRST)	0	0	0	7
✓	r / r	_X5HES~1	2011-03-28 12:39:32 (BRST)	2011-03-28 00:00:00 (BRST)	2011-03-28 12:39:32 (BRST)	20971520	0	0	8
	d / d	fotos/	2011-03-29 16:02:22 (BRST)	2011-03-29 00:00:00 (BRST)	2011-03-29 16:02:22 (BRST)	16384	0	0	4
	r / r	senhas	2011-03-28 09:39:58 (BRST)	2011-03-28 00:00:00 (BRST)	2011-03-28 09:39:58 (BRST)	54	0	0	6
✓	r / r	tx5hesde4k2	2011-03-28 12:40:06 (BRST)	2011-03-28 00:00:00 (BRST)	2011-03-28 12:40:06 (BRST)	0	0	0	10

Figura 38. Diretório raiz da primeira partição

Pode-se verificar ainda na figura 38 arquivos apagados, estes, são marcados com a cor vermelha, trata-se de um arquivo com extensão .JPG e dois sem extensão visível, de realçar que um dos arquivos sem extensão, o “_X5HES-1” possui um tamanho de aproximadamente 21Mb, que pode ser observado no campo “Size”. Foram feitas algumas análises que serão mostradas em passos seguintes, e chegou-se a conclusão de que não se trata de um arquivo, mas, provavelmente trata-se de um diretório, dificultando assim a sua

recuperação, pois, como se sabe os diretórios possuem vários arquivos, e estes arquivos ocupam espaço em vários setores do disco rígido, tornando assim quase impossível a sua recuperação.

Um dos que mais chamou a atenção foi o arquivo ”senhas”, o mesmo foi acessado via relatório Hexadecimal para ter-se acesso ao seu conteúdo, como mostra a figura 39, e foram encontradas algumas informações que se pressupõe ser de contas de e-mail do suspeito. O Arquivo encontra-se no sector 480 e foi acessado pela última vez na Segunda feira de Março, no dia 28 às 09h39min58seg de 2011.



Hex Contents of Sector 352 in copia.dd-62-1051519

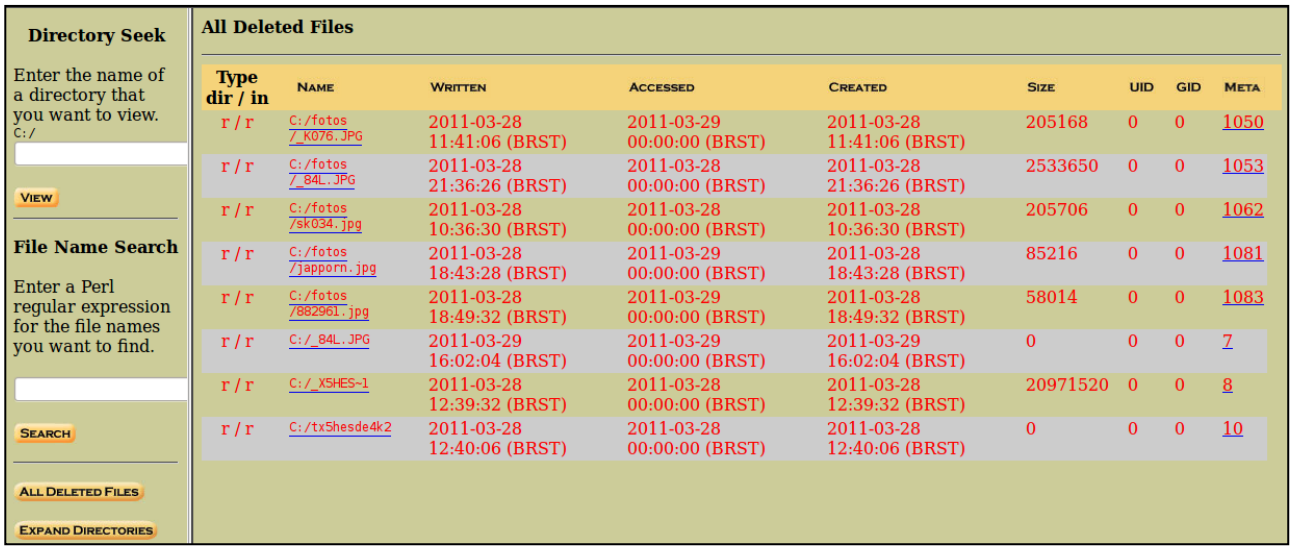
0	4166006f	0074006f	0073000f	002e0000	Af.o .t.o .s.. ....
16	ffffffff	ffffffff	ffff0000	ffffffff	....
32	464f544f	53202020	20202010	00644b80	FOTO S . .dK.
48	7d3e7d3e	00004b80	7d3e0300	00000000	}>}> ..K. }>.. ....
64	41730065	006e0068	0061000f	00f17300	As.e .n.h .a.. ..s.
80	0000ffff	ffffffff	ffff0000	ffffffff	....
96	53454e48	41532020	20202020	0000fd4c	SENH AS ...L
112	7c3e7c3e	0000fd4c	7c3e0500	36000000	|>|> ...L |>.. 6...
128	e538344c	20202020	4a504720	00004280	.84L JPG ..B.
144	7d3e7d3e	00004280	7d3e0000	00000000	}>}> ..B. }>.. ....
160	e5583548	45537e31	20202020	0000f064	.X5H ES~1 ...d
176	7c3e7c3e	0000f064	7c3eb000	00004001	|>|> ...d |>.. ..@.
192	e5740078	00350068	0065000f	00f87300	.t.x .5.h .e.. ..s.
208	64006500	34006b00	32000000	0000ffff	d.e. 4.k. 2... ....
224	e5583548	45537e32	20202020	00640365	.X5H ES~2 .d.e
240	7c3e7c3e	00000365	7c3e0000	00000000	|>|> ...e |>.. ....
256	00000000	00000000	00000000	00000000	....
272	00000000	00000000	00000000	00000000	....
288	00000000	00000000	00000000	00000000	....
304	00000000	00000000	00000000	00000000	....
320	00000000	00000000	00000000	00000000	....
336	00000000	00000000	00000000	00000000	....
352	00000000	00000000	00000000	00000000	....
368	00000000	00000000	00000000	00000000	....
384	00000000	00000000	00000000	00000000	....
400	00000000	00000000	00000000	00000000	....
416	00000000	00000000	00000000	00000000	....
432	00000000	00000000	00000000	00000000	....
448	00000000	00000000	00000000	00000000	....
464	00000000	00000000	00000000	00000000	....
480	00000000	00000000	00000000	00000000	....
496	00000000	00000000	00000000	00000000	....

Figura 39. Arquivo contendo possíveis senhas

Fez-se em toda a partição a busca de arquivos deletados pelo suspeito, utilizando uma opção presente na altura em que se faz a análise. O botão é o “All Deleted Files”. Ao

executar esta ação obteve-se uma lista de todos os arquivos deletados da partição (figura 40). Pode-se observar que vários arquivos apagados são provavelmente imagens. Pode-se observar na figura 41 algumas opções para exibição dos dados presentes na imagem.

A primeira opção “ASCII (display - report)” exibe o arquivos em ASCII e gera um relatório com “report“ contendo todas as informações como data de criação, de acesso e o setor em que se encontra o arquivo, o mesmo acontece com a opção “HEX“ apenas alterando para Hexadecimal a forma de exibição, e de igual modo também acontece com a opção “ASCII Strings“.



Directory Seek

Enter the name of a directory that you want to view.
C:/

VIEW

File Name Search

Enter a Perl regular expression for the file names you want to find.

SEARCH

ALL DELETED FILES

EXPAND DIRECTORIES

All Deleted Files

Type dir / in	Name	Written	Accessed	Created	Size	UID	GID	Meta
r / r	C:/fotos /_K076.JPG	2011-03-28 11:41:06 (BRST)	2011-03-29 00:00:00 (BRST)	2011-03-28 11:41:06 (BRST)	205168	0	0	1050
r / r	C:/fotos /_84L.JPG	2011-03-28 21:36:26 (BRST)	2011-03-28 00:00:00 (BRST)	2011-03-28 21:36:26 (BRST)	2533650	0	0	1053
r / r	C:/fotos /sk034.jpg	2011-03-28 10:36:30 (BRST)	2011-03-28 00:00:00 (BRST)	2011-03-28 10:36:30 (BRST)	205706	0	0	1062
r / r	C:/fotos /japporn.jpg	2011-03-28 18:43:28 (BRST)	2011-03-29 00:00:00 (BRST)	2011-03-28 18:43:28 (BRST)	85216	0	0	1081
r / r	C:/fotos /882961.jpg	2011-03-28 18:49:32 (BRST)	2011-03-29 00:00:00 (BRST)	2011-03-28 18:49:32 (BRST)	58014	0	0	1083
r / r	C:/_84L.JPG	2011-03-29 16:02:04 (BRST)	2011-03-29 00:00:00 (BRST)	2011-03-29 16:02:04 (BRST)	0	0	0	7
r / r	C:/_X5HES~1	2011-03-28 12:39:32 (BRST)	2011-03-28 00:00:00 (BRST)	2011-03-28 12:39:32 (BRST)	20971520	0	0	8
r / r	C:/tx5hesde4k2	2011-03-28 12:40:06 (BRST)	2011-03-28 00:00:00 (BRST)	2011-03-28 12:40:06 (BRST)	0	0	0	10

Figura 40. Arquivos deletados

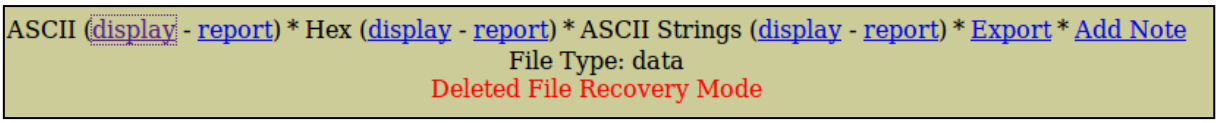


Figura 41. Opções de visualização dos arquivos na tela

Figura 42. Recuperação de um arquivo deletado

A figura acima, mostra a visualização do arquivo ”882961.jpg“, a imagem por ter sido deletada não se apresenta muito visível, no entanto se utilizara outras técnicas para recuperação das demais.

Como dito anteriormente, o uso de apenas uma ferramenta pode dificultar o processo de análise, sendo assim como ficou evidênciado uma grande quantidade de arquivos

deletados, achou-se por bem utilizar outras ferramentas que prometem recuperar arquivos deletados de uma partição.

Com isso recorreu-se a duas ferramentas de referência no cenário forense com software livre, o Foremost e o Scalpel:

a) **Scalpel** - bisturi em português, é uma ferramenta que contém um banco de dados interno com informações com as principais extensões de arquivos. Ele usa essa informações para percorrer a fundo imagens de disco ou discos físicos a procura dos dados para serem posteriormente recuperados, e esta disponível para plataforma Windows, Linux e Mac Os, nesse projeto se utilizará a versão para Linux disponível também na distribuição forense estudada, "Helix" (DIGITAL FORENSCICS SOLUTION, 2011, tradução nossa);

b) **Foremost** - é um programa baseado em linha de comandos que possibilita recuperar arquivos analisando seu cabeçalho, rodapé e estruturas internas. Ele trabalha tanto em discos físicos como em arquivos de imagens, está disponível no "Helix", (FOREMOST, 2006, tradução nossa).

Apresenta-se na figura 43 a execução da ferramenta Foremost, a mesma é executada de maneira relativamente simples como o observado na figura abaixo. É chamada pelo terminal seguido pela caminho da imagem, e a pasta aonde serão armazenados os resultados.

Figura 43. Uso do Foremost

Ao final da recuperação dos arquivos, é gerado um relatório em .txt que retornou as seguintes informação quanto ao número de arquivos e suas extensões:

a) .**gif** - vinte e três (23) imagens;

b) .**jpg** - quarenta e três (43) fotos;

c) .**ole** - um (1) arquivo;

d) .**html** - vinte (20) arquivos;

e) .**png** - treze (13).

Estes arquivos recuperados perfazem um total de 100 arquivos.

Optou-se em caráter de segurança por usar também a ferramenta Scalpel que já foi descrita em momento anterior. Para funcionar, é necessário executar o comando como administrador, chamar a ferramenta e definir o local de destino dos arquivos recuperados (figura 43).

Figura 44. Scalpel copiando os arquivos

A figura 44 mostra os arquivos sendo copiados para pasta "recuperadoScalpel" situada no ambiente de trabalho, observa-se também algumas informações como a versão do software e o progresso do processo.

A recuperação após ser concluída, retorna dados com o objetivo de situar o investigador a respeito da quantidade de arquivos recuperados, separando-os por extensões. Pode-se ter uma visão do relatório na figura 44. Foram recuperados um total de 131 arquivos com varias extensões:

a) .**gif** - vinte e três (23) imagens;

b) .**jpg** - setenta (70) fotos;

c) .**bmp** - um (1) arquivos;

d) .**mov** - sete (7) vídeos;

e) .**doc** - dois (2) documentos;

f) .**html** - dezoito (18) arquivos.

```
root@aguinaldogc-desktop:/home/aguinaldogc/Desktop# sudo scalpel copia.dd -o /home/aguinaldogc/Desktop/recuperadoSca
lpel
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/home/aguinaldogc/Desktop/copia.dd"

Image file pass 1/2.
copia.dd: 100.0% |*****************************************************************************|  980.0 MB    00:00 ETA
Allocating work queues...
Work queues allocation complete. Building carve lists...
Carve lists built.  Workload:
gif with header "\x47\x49\x46\x38\x37\x61" and footer "\x00\x3b" --> 0 files
gif with header "\x47\x49\x46\x38\x39\x61" and footer "\x00\x3b" --> 23 files
jpg with header "\xff\xd8\xff\xe0\x00\x10" and footer "\xff\xd9" --> 70 files
png with header "\x50\x4e\x47\x3f" and footer "\xff\xfc\xfd\xfe" --> 0 files
bmp with header "\x42\x4d\x3f\x3f\x00\x00\x00" and footer "" --> 1 files
avi with header "\x52\x49\x46\x46\x3f\x3f\x3f\x3f\x41\x56\x49" and footer "" --> 0 files
mov with header "\x3f\x3f\x3f\x3f\x6d\x6f\x6f\x76" and footer "" --> 0 files
mov with header "\x3f\x3f\x3f\x3f\x6d\x64\x61\x74" and footer "" --> 0 files
mov with header "\x3f\x3f\x3f\x3f\x77\x69\x64\x65\x76" and footer "" --> 0 files
mov with header "\x3f\x3f\x3f\x3f\x73\x6b\x69\x70" and footer "" --> 7 files
mov with header "\x3f\x3f\x3f\x3f\x66\x72\x65\x65" and footer "" --> 10 files
mov with header "\x3f\x3f\x3f\x3f\x69\x64\x73\x63" and footer "" --> 0 files
mov with header "\x3f\x3f\x3f\x3f\x70\x63\x6b\x67" and footer "" --> 0 files
mpg with header "\x00\x00\x01\xba" and footer "\x00\x00\x01\xb9" --> 0 files
mpg with header "\x00\x00\x01\xb3" and footer "\x00\x00\x01\xb7" --> 0 files
doc with header "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00" and footer "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00" -->
 2 files
wpc with header "\x3f\x57\x50\x43" and footer "" --> 0 files
htm with header "\x3c\x68\x74\x6d\x6c" and footer "\x3c\x2f\x68\x74\x6d\x6c\x3e" --> 18 files
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0d" --> 0 files
mail with header "\x41\x4f\x4c\x56\x4d" and footer "" --> 0 files
Carving files from image.
Image file pass 2/2.
copia.dd: 100.0% |*****************************************************************************|  980.0 MB    00:00 ETA
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 131, elapsed = 56 seconds.
```

Figura 45. Recuperação com Scalpel concluida

Comparando a eficiência das ferramentas, claramente fica aqui mais uma vez a importância da variação no uso delas. Nos relatórios podem-se observar que a ferramenta que recuperou mais arquivos foi a Scalpel, arquivos esses que podem, com certeza, fazer diferença no processo de análise forense, pois, nunca se sabe que tipo de evidências se tratam.

Passado o processo de recuperação, é chegado o momento de analisar os arquivos que foram recuperados. Foram então abertos e analisados todos os arquivos, primeiramente os adquiridos com o Scalpel.

Um total de 94 arquivos com extensões .JPG, .BMP. e .GIF, foram catalogados como sendo de pornografia infantil, fazendo apologia, ou ainda relacionando-se de alguma forma negativa. Dentre eles foram destacados alguns apresentados na figura 46:

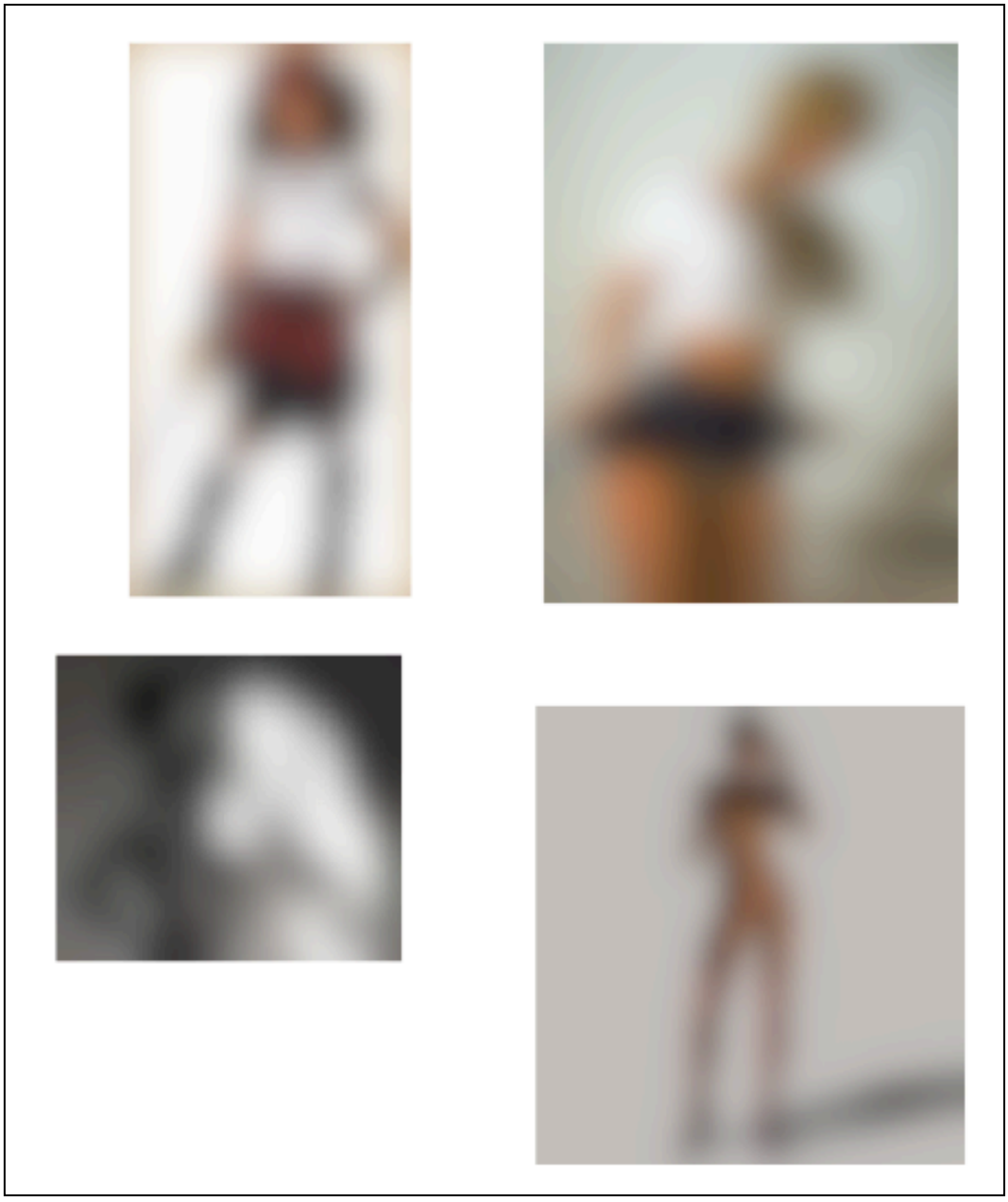


Figura 46. Fotos de pornografia infantil extraídas do disco rígido suspeito

De forma preliminar, pelo conteúdo apresentado já se pode afirmar que o suspeito mantinha contato de alguma forma com conteúdo pornográfico infantil tendo em conta que as

provas estão bastante visíveis e por serem mais de uma, indicam que não houve nenhum incidente para as fotos terem ido parar no computados do mesmo.

Foi recuperado também um arquivo de imagem que provavelmente o suspeito usava de forma maliciosa para aperfeiçoar as suas técnicas de atração de menores, na imagem estão descritos vários métodos usados por pedófilos para esta prática, estas informações provavelmente foram criadas por uma equipe de combate a este crime (figura 47).

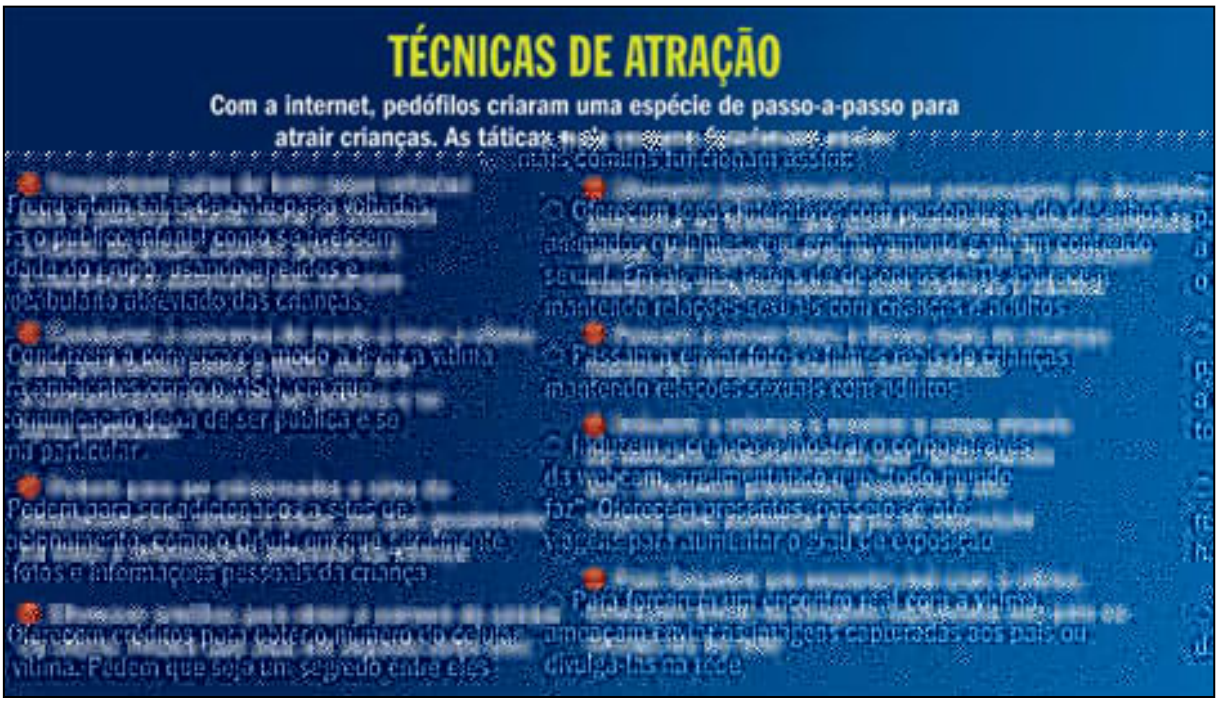


Figura 47. Arquivo contendo técnicas para atração de menores

Os arquivos recuperados com o Foremost já não foram analisados, pois foi verificado que todos os arquivos recuperados com o mesmo também estavam presentes no conjunto de arquivos extraídos com o Scalpel.

Até o presente momento foram analisados apenas arquivos de imagens, mas, também existem outros arquivos nos formato .MOV e .HTML.

Os arquivos .MOV recuperados não puderam ser abertos pois encontram-se danificados. Estes danos podem ter sido causados pelo fato do arquivo ter um tamanho relativamente grande, e não ter sido recuperado de forma integral.

Os arquivos com extensão HTML (figura 48) contêm dados relacionado com o objeto da pesquisa (pornografia infantil), mas, porém não constituem a prática efetiva do crime, embora, com os indícios já recuperados, pode-se afirmar que o suspeito mantinha essas informações para poder ter noção do *modus operandi* das autoridades que investigam esse tipo de crime.

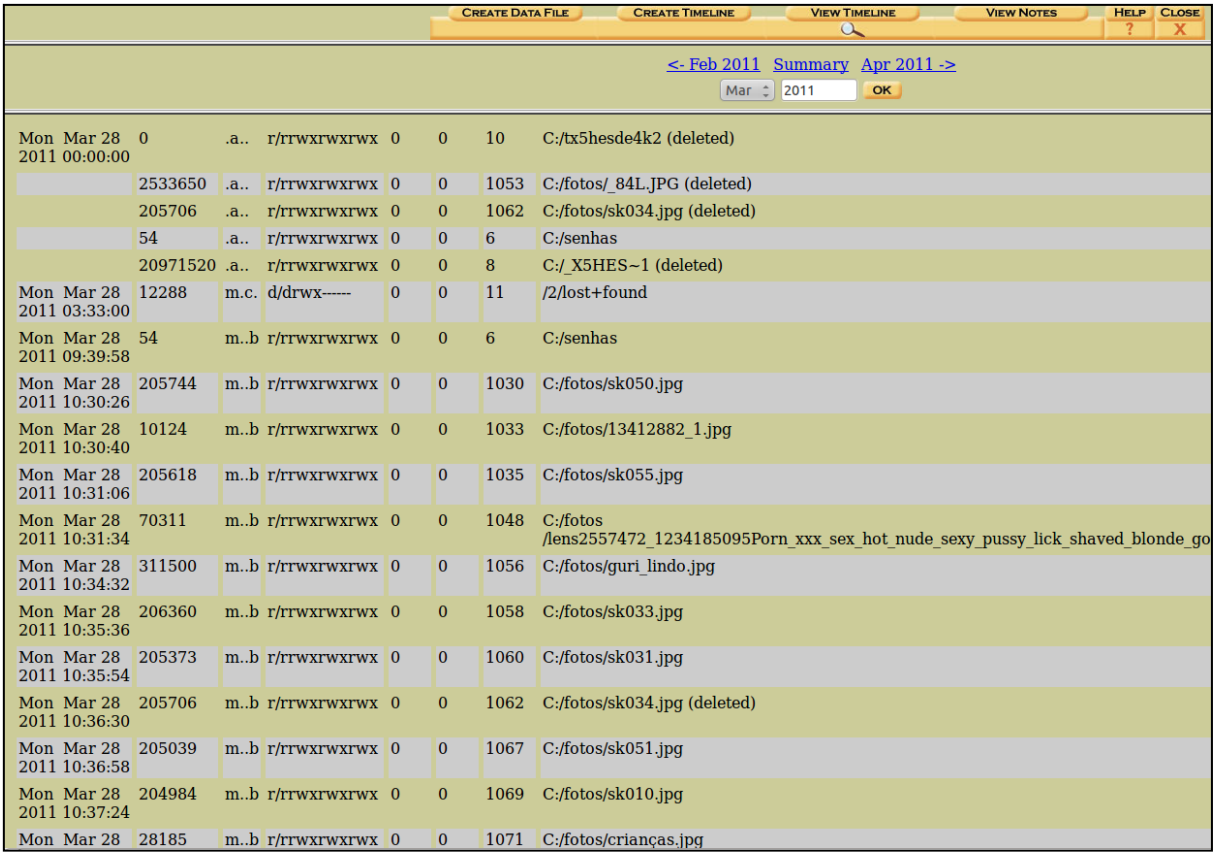
Figura 48. Algumas informações contidas nos arquivos html

É importante que se estabeleça uma linha de tempo entre os fatos ocorridos no exercício de atividade na máquina suspeita, no caso analisado o mais importante é descobrir artefatos que impliquem o suspeito, e não, necessariamente, traçar uma linha de

acontecimentos, mas, isso pode fazer um diferencial, e pode ajudar a descobrir algumas respostas que possam surgir no futuro.

A linha do tempo, também conhecida como *"File Activity Times Lines"*, segundo o manual do Autopsy, poderá fornecer informações sobre a data de quando o arquivo foi acessado, modificado e ou alterado.

Primeiramente, criou-se um ficheiro de dados "Data File" e selecionou-se a opção para gerar o *timeline* no disco rígido inteiro (partição 1 e partição 2) que, consequentemente, produziu o resultado apresentados na figura abaixo.



Mon Mar 28 2011 00:00:00	0	.a..	r/rrwxrwxrwx	0	0	10	C:/tx5hesde4k2 (deleted)
	2533650	.a..	r/rrwxrwxrwx	0	0	1053	C:/fotos/_84L.JPG (deleted)
	205706	.a..	r/rrwxrwxrwx	0	0	1062	C:/fotos/sk034.jpg (deleted)
	54	.a..	r/rrwxrwxrwx	0	0	6	C:/senhas
	20971520	.a..	r/rrwxrwxrwx	0	0	8	C:/_X5HES~1 (deleted)
Mon Mar 28 2011 03:33:00	12288	m.c.	d/drwx------	0	0	11	/2/lost+found
Mon Mar 28 2011 09:39:58	54	m..b	r/rrwxrwxrwx	0	0	6	C:/senhas
Mon Mar 28 2011 10:30:26	205744	m..b	r/rrwxrwxrwx	0	0	1030	C:/fotos/sk050.jpg
Mon Mar 28 2011 10:30:40	10124	m..b	r/rrwxrwxrwx	0	0	1033	C:/fotos/13412882_1.jpg
Mon Mar 28 2011 10:31:06	205618	m..b	r/rrwxrwxrwx	0	0	1035	C:/fotos/sk055.jpg
Mon Mar 28 2011 10:31:34	70311	m..b	r/rrwxrwxrwx	0	0	1048	C:/fotos /lens2557472_1234185095Porn_xxx_sex_hot_nude_sexy_pussy_lick_shaved_blonde_go
Mon Mar 28 2011 10:34:32	311500	m..b	r/rrwxrwxrwx	0	0	1056	C:/fotos/guri_lindo.jpg
Mon Mar 28 2011 10:35:36	206360	m..b	r/rrwxrwxrwx	0	0	1058	C:/fotos/sk033.jpg
Mon Mar 28 2011 10:35:54	205373	m..b	r/rrwxrwxrwx	0	0	1060	C:/fotos/sk031.jpg
Mon Mar 28 2011 10:36:30	205706	m..b	r/rrwxrwxrwx	0	0	1062	C:/fotos/sk034.jpg (deleted)
Mon Mar 28 2011 10:36:58	205039	m..b	r/rrwxrwxrwx	0	0	1067	C:/fotos/sk051.jpg
Mon Mar 28 2011 10:37:24	204984	m..b	r/rrwxrwxrwx	0	0	1069	C:/fotos/sk010.jpg
Mon Mar 28	28185	m..b	r/rrwxrwxrwx	0	0	1071	C:/fotos/crianças.jpg

Figura 49. Geração do *timeline*

Os eventos gerados pelo *timeline* começam no dia 28 de Março de 2011 pelas zero hora (00:00), conforme mostra a primeira linha da figura 49, pode-se observar que houve uma

sucessão de deleção de arquivos de imagens que já foram recuperadas nos passos anteriores, e as mesma estavam relacionadas diretamente com pornografia infantil.

Dado o horário zero hora (00:00) remete ao pensamento de algum tipo de acesso não autorizado feito pelo suspeito, pois, tratando-se de um computador presente no interior das instalações da empresa, era suposto que o mesmo não estivesse sendo acessado a esta hora.

Mon Mar 28 2011 11:41:06	205168	m..b	r/rrwxrwxrwx	0	0	1050	C:/fotos/_K076.JPG (deleted)
Mon Mar 28 2011 11:47:10	79339	m..b	r/rrwxrwxrwx	0	0	1052	C:/fotos/01.jpg
Mon Mar 28 2011 11:47:42	39827	m..b	r/rrwxrwxrwx	0	0	1065	C:/fotos/33985810_1.jpg
Mon Mar 28 2011 11:48:00	157221	m..b	r/rrwxrwxrwx	0	0	1073	C:/fotos/pic_1.jpg
Mon Mar 28 2011 11:48:16	122147	m..b	r/rrwxrwxrwx	0	0	1077	C:/fotos/gata_loira_linda_mulher.jpg
Mon Mar 28 2011 12:25:34	205778	m..b	r/rrwxrwxrwx	0	0	1079	C:/fotos/sk026.jpg
Mon Mar 28 2011 12:39:32	20971520	m..b	r/rrwxrwxrwx	0	0	8	C:/_X5HES~1 (deleted)
Mon Mar 28 2011 12:40:06	0	m..b	r/rrwxrwxrwx	0	0	10	C:/tx5hesde4k2 (deleted)
Mon Mar 28 2011 12:58:47	512	m.c.	r/rrw-r--r--	0	0	12	/2/backup_mbr_meu_hd
Mon Mar 28 2011 12:58:56	512	.a..	r/rrw-r--r--	0	0	12	/2/backup_mbr_meu_hd
Mon Mar 28 2011 14:52:12	48381	m...	r/rrw-r--r--	1000	1000	91082	/2/textos/pedofilos1.jpg
Mon Mar 28 2011 14:53:59	1	m...	r/rrw-r--r--	1000	1000	91086	/2/textos/perfil-do-pedofilo.html_conte
	162	m...	r/rrw-r--r--	1000	1000	91095	/2/textos/perfil-do-pedofilo.html_conte
	20135	m...	r/rrw-r--r--	1000	1000	91096	/2/textos/perfil-do-pedofilo.html_conte
	98375	m...	r/rrw-r--r--	1000	1000	91097	/2/textos/perfil-do-pedofilo.html_conte
	3404	m...	r/rrw-r--r--	1000	1000	91098	/2/textos/perfil-do-pedofilo.html_conte
Mon Mar 28 2011 14:54:00	1024	m...	d/drwxr-xr-x	1000	1000	91083	/2/textos/perfil-do-pedofilo.html_conte
	5487	m...	r/rrw-r--r--	1000	1000	91084	/2/textos/perfil-do-pedofilo.html_conte

Figura 50. *Timeline* do disco rígido

No mesmo dia, as 11:h41min 6seg até as 14h54min (figura 50), foram criados, acessados e deletados vários arquivos com conteúdo proibido, que compreende desde

arquivos de imagem, documentos e sites com informações sobre pedofilia salvos no computador que de maneira direta podiam não ser para implicação do suspeito, mas dado o histórico da investigação, acredita-se que foram informações usadas de maneiras a gerarem benefícios que facilitassem a execução do crime.

Mon Mar 28 2011 15:00:33	32768	m...	r/rrw-r--r--	1000	1000	91137	/2/textos/doc1.doc
Mon Mar 28 2011 15:02:14	32768	.a..	r/rrw-r--r--	1000	1000	91137	/2/textos/doc1.doc
Mon Mar 28 2011 15:04:05	99328	m...	r/rrw-r--r--	1000	1000	91101	/2/textos/capsa2008_franco1.doc
Mon Mar 28 2011 15:04:18	99328	.a..	r/rrw-r--r--	1000	1000	91101	/2/textos/capsa2008_franco1.doc
Mon Mar 28 2011 15:05:21	48381	..c.	r/rrw-r--r--	1000	1000	91082	/2/textos/pedofilos1.jpg

Figura 51. *Timeline* do disco rígido (2)

Foram criados documentos no período das 15h às 15h4min, provavelmente transferidos da Internet ou de algum tipo de dispositivo removível dado o tempo curto (4 minutos) entre a criação de um e de outro (figura 51).

2011 18:43:28							
Mon Mar 28 2011 18:49:32	58014	m..b	r/rrwxrwxrwx	0	0	1083	C:/fotos/882961.jpg (deleted)
Mon Mar 28 2011 21:36:26	2533650	m..b	r/rrwxrwxrwx	0	0	1053	C:/fotos/_84L.JPG (deleted)
Mon Mar 28 2011 21:36:36	580150	m..b	r/rrwxrwxrwx	0	0	1086	C:/fotos/1237233307789.jpg
Tue Mar 29 2011 00:00:00	205744	.a..	r/rrwxrwxrwx	0	0	1030	C:/fotos/sk050.jpg
	10124	.a..	r/rrwxrwxrwx	0	0	1033	C:/fotos/13412882_1.jpg
	205618	.a..	r/rrwxrwxrwx	0	0	1035	C:/fotos/sk055.jpg
	70311	.a..	r/rrwxrwxrwx	0	0	1048	C:/fotos /lens2557472_1234185095Porn_xxx_se
	2533650	.a..	r/rrwxrwxrwx	0	0	1049	C:/fotos/_84L.JPG
	205168	.a..	r/rrwxrwxrwx	0	0	1050	C:/fotos/_K076.JPG (deleted)
	79339	.a..	r/rrwxrwxrwx	0	0	1052	C:/fotos/01.jpg
	311500	.a..	r/rrwxrwxrwx	0	0	1056	C:/fotos/guri_lindo.jpg
	206360	.a..	r/rrwxrwxrwx	0	0	1058	C:/fotos/sk033.jpg
	205373	.a..	r/rrwxrwxrwx	0	0	1060	C:/fotos/sk031.jpg
	39827	.a..	r/rrwxrwxrwx	0	0	1065	C:/fotos/33985810_1.jpg
	205039	.a..	r/rrwxrwxrwx	0	0	1067	C:/fotos/sk051.jpg
	204984	.a..	r/rrwxrwxrwx	0	0	1069	C:/fotos/sk010.jpg
	28185	.a..	r/rrwxrwxrwx	0	0	1071	C:/fotos/crianças.jpg
	157221	.a..	r/rrwxrwxrwx	0	0	1073	C:/fotos/pic_1.jpg
	122147	.a..	r/rrwxrwxrwx	0	0	1077	C:/fotos/gata_loira_linda_mulher.jpg
	205778	.a..	r/rrwxrwxrwx	0	0	1079	C:/fotos/sk026.jpg
	85216	.a..	r/rrwxrwxrwx	0	0	1081	C:/fotos/japporn.jpg (deleted)
	58014	.a..	r/rrwxrwxrwx	0	0	1083	C:/fotos/882961.jpg (deleted)
	580150	.a..	r/rrwxrwxrwx	0	0	1086	C:/fotos/1237233307789.jpg

Figura 51. *Timeline* do disco rígido (3)

Tue Mar 29 2011 17:57:41	12288	.a..	d/drwx------	0	0	11	/2/lost+found
Tue Mar 29 2011 17:57:42	1024	.a..	d/drwxr-xr-x	1000	1000	91081	/2/textos
	48381	.a..	r/rrw-r--r--	1000	1000	91082	/2/textos/pedofilos1.jpg
Tue Mar 29 2011 17:57:47	2048	.a..	d/drwxr-xr-x	1000	1000	91175	/2/textos/Interpol-efeitos-especiais-p-descobrir-pedofilo_a30101_z(
Tue Mar 29 2011 17:57:48	1024	.a..	d/drwxr-xr-x	1000	1000	91181	/2/textos/Interpol-efeitos-especiais-p-descobrir-pedofilo_a30101_z(
	1002	.a..	r/rrw-r--r--	1000	1000	91184	/2/textos/Interpol-efeitos-especiais-p-descobrir-pedofilo_a30101_z(
	291	.a..	r/rrw-r--r--	1000	1000	91185	/2/textos/Interpol-efeitos-especiais-p-descobrir-pedofilo_a30101_z(
Tue Mar 29 2011 17:57:51	1024	.a..	d/drwxr-xr-x	1000	1000	91083	/2/textos/perfil-do-pedofilo.html_content
Tue Mar 29 2011 17:57:52	1024	.a..	d/drwxr-xr-x	1000	1000	91088	/2/textos/perfil-do-pedofilo.html_content/comment-iframe_data
Tue Mar 29 2011 17:57:57	1024	.a..	d/drwxr-xr-x	1000	1000	91139	/2/textos/integra.asp.html_content
	6405	.a..	r/rrw-r--r--	1000	1000	91145	/2/textos/integra.asp.html_content/15_MHB_sp_bruno.jpg
Tue Mar 29 2011 17:57:58	4960	.a..	r/rrw-r--r--	1000	1000	91141	/2/textos/integra.asp.html_content/15_MHB_sp_wagner.jpg
	7638	.a..	r/rrw-r--r--	1000	1000	91146	/2/textos/integra.asp.html_content/15_MHB_sp_wellington.jpg
	7307	.a..	r/rrw-r--r--	1000	1000	91147	/2/textos/integra.asp.html_content/15_MHB_sp_robson.jpg
Tue Mar 29 2011 17:57:59	1024	.a..	d/drwxr-xr-x	1000	1000	91103	/2/textos/crianç-chat-é-alvo-fácil-pedófilos.html_content
	6228	.a..	r/rrw-r--r--	1000	1000	91124	/2/textos/crianç-chat-é-alvo-fácil-pedófilos.html_content/logo.png
Tue Mar 29 2011 17:58:01	2377	.a..	r/rrw-r--r--	1000	1000	91176	/2/textos/Interpol-efeitos-especiais-p-descobrir-pedofilo_a30101_z(
	22753	.a..	r/rrw-r--r--	1000	1000	91177	/2/textos/Interpol-efeitos-especiais-p-descobrir-pedofilo_a30101_z(

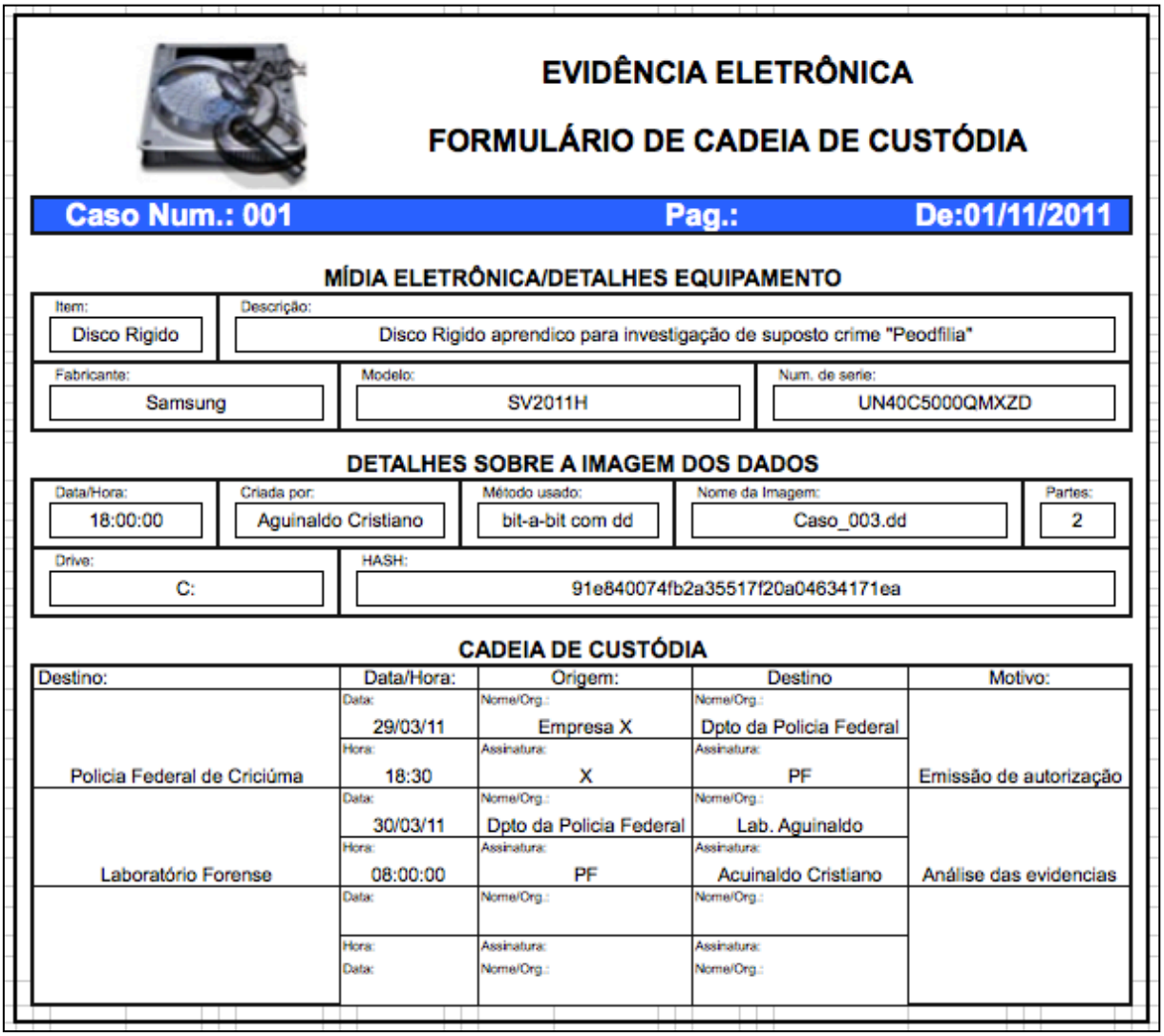
Figura 52. *Timeline* do disco rígido (4)

A figura 52 mostra o final das atividades no computador as 17h58min 1seg do dia 29 de Março, véspera em que o material foi apreendido. Pode-se observar que momentos antes o suspeito grava dados relacionados com pedofilia, dados esses que já foram apresentados anteriormente.

7.2.6 Documentação

No ato da documentação da cena do crime, era suposto que fosse incluída uma cópia da autorização judicial emitida pelos órgãos competentes para que a coleta e o manuseio das provas periciais fossem feitas dentro da lei, mas, tratando-se de um caso fictício, não houve esta necessidade, pois o mesmo destina-se apenas para uso acadêmico e não para ser apresentado em um tribunal.

A cadeia de custódia foi gerada baseando-se em informações fictícias como o tipo de evidência, a descrição do mesmo, o fabricante, modelo, número de série (figura 53). Também são inclusos detalhes sobre a imagem dos dados como a hora da sua criação, o nome do perito responsável, os métodos usados para obtenção da mesma e os locais para onde o material apreendido foi levado até chegar ao laboratório para a análise efetiva.



EVIDÊNCIA ELETRÔNICA

FORMULÁRIO DE CADEIA DE CUSTÓDIA

Caso Num.: 001	Pag.:	De:01/11/2011

MÍDIA ELETRÔNICA/DETALHES EQUIPAMENTO

Item:	Descrição:		
Disco Rigido	Disco Rigido aprendico para investigação de suposto crime "Peodfilia"		
Fabricante:	Modelo:	Num. de serie:	
Samsung	SV2011H	UN40C5000QMXZD	

DETALHES SOBRE A IMAGEM DOS DADOS

Data/Hora:	Criada por:	Método usado:	Nome da Imagem:	Partes:
18:00:00	Aguinaldo Cristiano	bit-a-bit com dd	Caso_003.dd	2
Drive:	HASH:			
C:	91e840074fb2a35517f20a04634171ea			

CADEIA DE CUSTÓDIA

Destino:	Data/Hora:	Origem:	Destino	Motivo:
	Data: 29/03/11	Nome/Org.: Empresa X	Nome/Org.: Dpto da Policia Federal	
Policia Federal de Criciúma	Hora: 18:30	Assinatura: X	Assinatura: PF	Emissão de autorização
	Data: 30/03/11	Nome/Org.: Dpto da Policia Federal	Nome/Org.: Lab. Aguinaldo	
Laboratório Forense	Hora: 08:00:00	Assinatura: PF	Assinatura: Acuinaldo Cristiano	Análise das evidencias
	Data:	Nome/Org.:	Nome/Org.:	
	Hora: Data:	Assinatura: Nome/Org.:	Assinatura: Nome/Org.:	

Figura 53. Formulário de Cadeia de Custódia

A perícia foi baseada em apenas uma evidência, disco rígido, que foi encontrado em uso no momento da apreensão feita pela policia. Após ser recebida pelo examinador

forense, a prova foi submetida a uma validação com o algoritmo de hash md5, usando o software md5sum, validação esta que foi de encontro com o código hash inicial.

Conforme manda a metodologia SOP, todos os dados da investigação devem estar presentes na documentação, sendo assim foram recolhidos todos os logs que compreendem um período que vai desde a criação do caso até a geração do *timeline* que praticamente foi a última etapa em que se teve contato efetivo com a imagem forense (apêndice B).

7.2.7 Relatório/Revisão

Devem conter informações no relatório e na revisão que abordam as necessidades do solicitante, que objetivam dar informações de forma relevante ao leitor.

Por se tratar de um trabalho para fins de aprendizado e contribuição bibliográfica de modo geral, todas as etapas foram escritas de modos a que os iniciante na área e curiosos pudessem compreender todo o processo envolvido no ato de uma perícia, sendo assim fica desnecessário reapresentar tais informações neste passo.

O estudo do caso serviu dentre outros objetivos para medir o nível de eficiência das ferramentas, isso foi feito de maneira prática, como por exemplo na recuperação dos dados apagados (capítulo 7.2.5), quando foram usadas as ferramentas Scalpel e Foremost, a primeira demontrou ser mais eficiente, recuperando um numero maior de informações. No caso do Software de análise, o Autopsy, não foi feita comparação com nenhuma outra, mas a mesma mostrou ser eficiente, dada a quantidade de informação que encontrou, sem a necessidade de usar comandos complexos, sendo feita a análise a partir de uma interface gráfica, informações estas, sobre o sistema de arquivos das partições, arquivos apagados, e sobre os setores alocados ou não.

Com o uso do Autopsy conseguiu-se fazer uma procura em toda cópia do disco rígido por meio do sistema de busca por palavras chave, e, como resultado obteve-se a localização exata dos arquivos que continham conteúdo que faziam menção a algumas palavras como (criança, senha, porn, pornô, sex, fotos, pics, pictures, entre outros). Sendo o mecanismo de recuperação de arquivos do Autopsy um pouco limitado, recorreu-se a softwares secundários, já falados anteriormente.

Com o Scalpel e o Foremost, fez-se uma varredura um todos os disco, que resultou na recuperação de uma grande quantidade de arquivos, que vão desde imagens, documentos, vídeos, entre outros.

Diante das evidências recuperadas, por estas terem relação direta com o suspeito, e por serem de conteúdo ilegal, podem ser usadas futuramente para provar o envolvimento do mesmo neste tipo de atividades (pornografia infantil) em futuras análises feita pela justiça

CONCLUSÃO

Cada dia que passa, crimes praticados envolvendo computadores aumentam e a capacidade de resposta dos profissionais na área forense ainda tem sido limitadas por conta de vários aspectos de ordem organizacional da categoria. No Brasil, as muitas metodologias criadas e usadas internacionalmente ainda não são aceitas, ficando sempre restringidos a uma apenas, que muitas das vezes dependendo da especificidade da ocorrência não proporciona uma resposta efetiva ao problema.

Não obstante há alguns problemas na categoria. Ainda assim, o número de interessados pela área forense tem crescido, sobretudo mais voltados a ferramentas com licença livre. Nas pesquisas foi possível ter contato com algumas informações referentes a processos que tiveram como base um perito forense para o seu desfecho.

A pesquisa feita revelou-se de certa forma importante para evidênciar o papel de um time de resposta a incidentes na formulação de estratégias com o objetivo de dar solução a problemas referentes à segurança da informação, quer no caráter preventivo como de contenção e erradicação de ameaças ocorridas com auxílio de algumas ferramentas para detecção de intrusão e para perícia forense em geral.

Os objetivos específicos propostos foram alcançados, sendo que o primeiro compreendia a demonstração do funcionamento de algumas ferramentas presentes no Helix por meio de um caso fictício. Foi realizado com sucesso, e produziu resultados confiáveis que certamente poderiam ser usados para representação de um caso real, dado os mínimos detalhes que se teve com o manuseio da evidência digital e a aplicação efetiva da metodologia usada.

Citar e aplicar quesitos básicos para elaboração de uma perícia forense foi definido como o segundo objetivo específico, que foi alcançado no ato da aplicação da

metodologia forense para a resolução do estudo de caso. Haja visto que em todas as etapas foram explicados nos mínimos detalhes possíveis e por intermédio de figuras contendo os dados reais, detalhes sobre como realizar uma perícia forense, e que efetivamente venha a ser aceita em uma corte judicial.

O terceiro objetivo foi atingido também, embora a imagem utilizada não tenha sido coletada, mas sim obtida de outra fonte, isto porque quando se pensou no caso aonde seria aplicada a análise, ficou patente a questão de o caso fictício ser montado pelo próprio perito forense (acadêmico), sendo assim com o objetivo de não comprometer, e fidelizar ainda mais os resultados, foi usado um caso criado por um terceiro, um profissional da área forense.

A utilização de vários cenários foi definida como o quarto objetivo a ser alcançado, não foi possível a utilização de mais de um cenário, dada a demora e a complexidade do processo de análise em si, percebido apenas no momento, que durou aproximadamente 10 dias, mas ainda assim não comprometeram em nada os resultados, pois o uso e demonstração das ferramentas no caso foi deveras satisfatório, dado a quantidade de informação que foi subtraída e o sucesso na implicação do suspeito.

Com os objetivos específicos praticamente alcançados, com o objetivo geral não podia ser diferente, visto que o mesmo visava a análise de ferramentas e metodologias para resposta a incidentes presentes no Helix. As metodologias foram descritas e usadas para resolução do caso, por meio das ferramentas presentes no software proposto.

No decorrer do estudo foram encontrados vários obstáculos, nomeadamente a falta de bibliografia na área em Língua Portuguesa, a falta de padrões nas metodologias, e, principalmente o fato de a ferramenta principal a ser estudada ter passado de livre para paga, tornando assim alguns softwares específicos contidos na distribuição e definidos para estudo anteriormente, obsoleto, mas, este problema foi ultrapassado com a compra da versão paga. Desta forma foram usados consequentemente outros softwares substituindo os obsoletos.

Finalizando, acredita-se que irá contribuir para minimizar a carência bibliográfica na área, problema este apresentado como parte da justificativa. O estudo acabou por dar origem também a ideia de compilar uma nova distribuição para perícia forense composta por ferramentas livres baseada em Ubuntu.

REFERÊNCIAS

ARUSO, Carlos A. A.; STEFFEN, Flávio Denys.**Segurança em informática e de informações**. 2.ed. São Paulo: SENAC/SP, 1999.

BAKER; CASWELL. **Snort Intrusion Detection and Prevention Toolkit**. Boston: Addison Wesley, 2004.

B2NET. **ISS RealSecure SiteProtector** Disponível em: <http://www.b2net.co.uk/iss /iss_realsecure_siteprotector.htm> Acesso em: 9 Setembro. 2011, 10:30

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

BUENO, M. L. P**. Forense computacional:** técnicas e ferramentas. Catalão, 2007.

CAMPOS, André L. N. **Sistema de Segurança da Informação**. Florianópolis: Visual Books. 2006.

CARVALHO, Menezes, REVOREDO, Marcelo. **A Trajetória da Internet no Brasil l:** do surgimento das redes de computadores à instituição dos mecanismos de governança. Dissertação, Universidade Federal do Rio de Janeiro, 2006.

CARVEY, H. **Windows Forensics and Incident Recovery**. Boston: Addison Wesley, 2004.

CAMPELLO, *WEBER*. **O Sistema de Detecção de Intrusão *Asgaard*** Disponível em: <*labcom.inf.ufrgs.br/ceseg/anais/2001/05.pdf*> Acesso em: 9 Setembro. 2011, 10:35

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

CASEY, E. **Digital Evidence and Computer Crime:** forensic science, computers and the Internet. 2. ed. London: Academic Press, 2004.

CASEY, E. **Digital Evidence and Computer Crime**. London: Academic Press, 2000.

CERT.br. **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.** Cartilha de Segurança para Internet Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 9 de Setembro de 2010.

COMER, Douglas E. **Redes de computadores e Internet:**abrange transmissão de dados, ligação inter-redes e web. 2.Ed Porto Alegre: Bookman, 2001.

COUTINHO, Luciano; CASSIOLATO, José Eduardo; SILVA, Ana Lucia Gonçalves da (Coord.).**Telecomunicações, globalização e competitividade**. Campinas: Papirus, 1995.

CYBERCON. **Computer Incident Response Guidebook**.Disponível em: <http://www.cybercon.org/Security/Docs/Intrusion/Computer%20Incident%20Response%20Guidebook.pdf>Acessoem: 18 maio. 2011, 20:49

DANTAS, Mario. **Computação distribuída de alto desempenho:**redes, clusters e grids computacionais. Rio de Janeiro: Axcel Books do Brasil, 2005.

Department of Justice. **Electronic Crime Scene Investigation:** A Guide for First Responders, Second Edition. Washington: Cover photographs, 2001.

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

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

DOS REIS, M. A. **Forense Computacional e sua aplicação em segurança imunológica**.Tese de Mestrado, Universidade Estadual de Campinas, 2003.

E-FENSE. **HELIX 3 Pro**: Meeting your computer forensics needs! Disponível em: <http://accessdata.com/downloads/media/Helix3Pro.pdf>Acesso em: 6 Junho. 2011, 15:10

EDRM. **EDRM Stages Explanation** Disponível em: <http://www.edrm.net/resources/edrm-stages-explanation>Acesso em: 18 maio. 2011, 10:30

FARMER, Dan; VENEMA, Wietse. **Perícia Forense Computacional:** Teoria e Prática Aplicada. São Paulo: Pearson Prentice-Hall, 2007.

FIGG, William; ZHOU, Zehai. **A computer forensics minor curriculum proposal.** Texas: 2007.

FRATEPIETRO, Stefan, ROSSETI, Sandro. **DEFT**: Manual de uso. Disponivelem<http://www.deftlinux.net/doc/%5Bit%5Ddeft_manuale_full.pdf>Acessoem: 6 d ejunho. 2011, 15:57

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

GLEASON, BJ; FAHEY, Drew. **Helix 1.7 for Beginners**. EUA: E-fense, 2006.

GLEASON; Fahey, Drew. **Helix 1.7 for Beginners**. New York: E-fense. 2006.

GOMES, Olavo, ANSHIESHI José. **Segurança Total:** Protegendo-se contra os Hackers. São Paulo: Makron Books, 2000.

GOMES, Pedro. **Definição: Spywares e Malwares** Disponível em: <http://www.computadorseguro.com /definicao-malware-spyware/>Acesso em: 6 Junho. 2011, 16:30

HAILEYS, Steve. **What is Computer Forensics**: CyberSecurity Institute, 2002. Disponível em: <http://www.cybersecurityinstitute.biz/forensics.htm>Acesso em: 13 abr. 2011, 14:30

HENRIQUE, Lucas. **O que é uma partição Swap? Disponivel** em: <http://www.acheiobyte.com.br/o-que-e-uma-particao-swap/>Acessoem: 6 junho. 2011, 13:58

IOCE. **G8 Proposed Principles for the Procedures Relating To Digital Evidence** Disponível em: <http://www.ioce.org/fileadmin/user_upload/2002/G8%20Proposed%20principles%20for%20forensic%20evidence.pdf>Acessoem: 18 Maio. 2011, 22:30

ISKANDAR, Jamil. **Normas da ABNT:** Comentadas para Trabalhos Científicos. Curitiba: Juruá Editora, 2009

LACOME, Vincent. **Worm Infection Response:** Guidelines to handle information system Worm infections. Disponível em: <http://cert.societegenerale.com/resources/files/IRM-1-Worm-Infection.pdf>Acessoem: 19 maio. 2011, 00:30

MANDIA, Kevin, PROSISE, Chris. **Hackers:** Resposta e Contra-Ataque. Rio de Janeiro: Campus, 2001.

MARCELO, Antonio; PEREIRA, Marcos. **A arte de Hackear Pessoas**. Rio de Janeiro: Brasport, 2005.

MELO, Sandro. **Computação forense com software livre**: conceitos, ferramentas e estudos de casos. Rio de Janeiro: Alta Books, 2009.

MOHAY, G.; ANDERSON, A.; COLLIE, B.; VEL, O.; MCKEMMISH, R. **Computer and Intrusion Forensics**, London: Artech House, 2003.

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

NMAP. Nmap Security Disponível em: <http://nmap.org/> Acesso em: 18 outubro. 2011, 13:20

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

RAIMUNDO, Neto. **Implementacão de Ferramenta para Deteccao de Intrusao** Disponível em: <*www.faete.edu.br/revista/artigo-rneto.pdf*> Acesso em: 19 maio. 2011, 21:30

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

RODRIGUES, Tony. **Imagens forenses**. Disponível em: <http://forcomp.blogspot.com/2008/01/imagens-forenses.html>. Acesso em: 10 out. 2010.

RUSS, John C. **Forensic uses of digital imaging**. Boca Raton: CRC Press, 2001.

SALOMON, Michael G.; BARRETT, Diane; BROOM, Neil. **Computer forensics jumpstart**. San Francisco: Sybex, 2005.

SCARFONE, Karen, GRANCE, Tim, MASONE, Kelly. **Computer Security Incident Handling Guide.** Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf>Acessoem: 19 maio. 2011, 14:30

SCHWEITZER, Douglas. **Incident Response:** computer forensics toolkit. Indiana: Wiley Publishing, 2003.
Schweitzer, Douglas. Incident Response: Computer Forensics Toolkit. Indianapolis: Wiley, 2003.

SEARCH SECURITY. **Definition:** snooping Disponível em: <http://searchsecurity.techtarget.com/definition/snooping>Acesso em: 6 de Junho, 2001, 14:30 2011, 14:20

SÊMOLA, Marcos. **Gestão da segurança da informação:** uma visão executiva. Rio de Janeiro: Campus, 2003.

SHULTZ, Eugene. **Seventeen Mistakes in Incident Response**. Disponível em: <http://www.pliroforiki.org/joomla/index.php?option=com_docman&task=doc_download&gid=11&Itemid=64>Acessoem: 18 maio. 2011, 23:30

SYMANTEC. **Symantec 2010 SMB Information Protection Survey**. Dispónivel em: <http://www.symantec.com/content/pt/br/enterprise/images/theme/smbsurvey/SMB_ProtectionSurvey_2010.pdf>. Acesso em: 10 out. 2010.

SYMANTEC. **Symantec Intruder Alert 3.6** Disponível em: <http://www.superwarehouse.com/Symantec_Intruder_Alert_3.6/16-00-00035/p/66787> Acesso em: 18 maio. 2011, 20:30

ULBRICH, Henrique César; VALLE, James Della**. Universidade H4CK3R**. São Paulo: Digerati Books, 2009.

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

APÊNDICE - A LOG COM INFORMAÇÕES SOBRE O HORARIO E TIPO DE ATIVIDADE REALIZADA

```
Sat Oct 22 15:25:18 2011: Host SuspeitoPedofilia added to case Pedofilias
Sat Oct 22 15:25:43 2011: Host SuspeitoPedofilia opened by unknown
Sat Oct 22 15:31:07 2011: Sym Linking image /home/aguinaldogc/Desktop/copia.dd into
Pedofilias:SuspeitoPedofilia
Sat Oct 22 15:31:07 2011: Image added: image img1 raw  images/copia.dd
Sat Oct 22 15:31:07 2011: Volume added: disk  vol1 img1    dos
Sat Oct 22 15:31:07 2011: Volume added: part  vol2 img1   62  1051519    fat16  C:
Sat Oct 22 15:31:07 2011: Volume added: part  vol3 img1   1051520  2005823    ext  /2/
Sat Oct 22 15:32:46 2011: Image vol1 opened by unknown
Sat Oct 22 15:33:17 2011: Volume added: strings  vol4 vol2   output/copia.dd-62-1051519-fat16.asc
Sat Oct 22 15:33:27 2011: Volume added: unistrings  vol5 vol2    output/copia.dd-62-1051519-fat16.uni
Sat Oct 22 15:34:15 2011: Image vol2 opened by unknown
Sat Oct 22 15:45:43 2011: Host SuspeitoPedofilia opened by unknown
Sat Oct 22 15:45:46 2011: Image vol2 opened by unknown
Sat Oct 22 19:19:27 2011: Volume added: body  vol6 output/body
Sat Oct 22 19:19:40 2011: Volume added: timeline  vol7 output/timeline.txt
Wed Oct 26 23:37:58 2011: Host SuspeitoPedofilia opened by unknown
Wed Oct 26 23:38:01 2011: Image vol2 opened by unknown
Sun Oct 30 21:50:16 2011: Image vol2 opened by unknown
Sun Oct 30 22:05:23 2011: Volume added: body  vol8 output/body
Sun Oct 30 22:05:55 2011: Volume added: timeline  vol9 output/timeline.txt
Mon Oct 31 19:14:45 2011: Image vol3 opened by unknown
Mon Oct 31 19:17:44 2011: Volume added: timeline  vol10 output/HDinteiro
Mon Oct 31 19:18:43 2011: Volume added: body  vol11 output/body
Mon Oct 31 19:18:59 2011: Volume added: timeline  vol12 output/timeline.txt
```

APÊNDICE B - PASSO A PASSO RELIZADO NO AUTOPSY ATÉ A CONCLUSÃO DA ANÁLISE

Sat Oct 22 15:27:49 2011: '/usr/bin/img_stat' -t "/home/aguinaldogc/Desktop/copia.dd"
Sat Oct 22 15:27:49 2011: '/usr/bin/mmstat' -i raw "/home/aguinaldogc/Desktop/copia.dd"
Sat Oct 22 15:27:49 2011: '/usr/bin/mmls' -a -i raw -aM -t dos -r "/home/aguinaldogc/Desktop/copia.dd"
Sat Oct 22 15:27:49 2011: '/usr/bin/fsstat' -o 62 -i raw -t "/home/aguinaldogc/Desktop/copia.dd"
Sat Oct 22 15:27:49 2011: '/usr/bin/fsstat' -o 1051520 -i raw -t "/home/aguinaldogc/Desktop/copia.dd"
Sat Oct 22 15:31:04 2011: '/usr/bin/img_stat' -t "/home/aguinaldogc/Desktop/copia.dd"
Sat Oct 22 15:31:04 2011: '/usr/bin/blkls' -f raw -e "/home/aguinaldogc/Desktop/copia.dd" | '/usr/bin/md5sum'
Sat Oct 22 15:31:07 2011: '/usr/bin/fsstat' -o 62 -i raw -f fat16 "/home/aguinaldogc/Desktop/copia.dd"
Sat Oct 22 15:31:07 2011: '/usr/bin/fsstat' -o 1051520 -i raw -f ext "/home/aguinaldogc/Desktop/copia.dd"
Sat Oct 22 15:31:07 2011: /bin/ln -s '/home/aguinaldogc/Desktop/copia.dd' '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd'
Sat Oct 22 15:32:59 2011: '/usr/bin/blkcat' -f fat16 -s -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd'
Sat Oct 22 15:33:03 2011: '/usr/bin/blkls' -e -f fat16 -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' | '/usr/bin/srch_strings' -a -t d > '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/output/copia.dd-62-1051519-fat16.asc'
Sat Oct 22 15:33:17 2011: '/usr/bin/md5sum' /var/lib/autopsy/Pedofilias/SuspeitoPedofilia/output/copia.dd-62-1051519-fat16.asc
Sat Oct 22 15:33:17 2011: '/usr/bin/blkls' -e -f fat16 -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' | '/usr/bin/srch_strings' -a -t d -e l > '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/output/copia.dd-62-1051519-fat16.uni'
Sat Oct 22 15:33:27 2011: '/usr/bin/md5sum' /var/lib/autopsy/Pedofilias/SuspeitoPedofilia/output/copia.dd-62-1051519-fat16.uni

Sat Oct 22 15:33:55 2011: '/usr/bin/blkcat' -f fat16 -s -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd'
Sat Oct 22 15:34:19 2011: '/usr/bin/fls' -f fat16 -la -z "BRST" -s '0' -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 2
Sat Oct 22 15:35:53 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/file' -z -b -
Sat Oct 22 15:35:53 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8
Sat Oct 22 15:35:53 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/file' -z -b -
Sat Oct 22 15:36:06 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/md5sum'
Sat Oct 22 15:36:06 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/sha1sum'
Sat Oct 22 15:36:07 2011: '/usr/bin/istat' -f fat16 -z "BRST" -s '0' -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8
Sat Oct 22 15:36:07 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/file' -z -b -
Sat Oct 22 15:36:07 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8
Sat Oct 22 15:36:12 2011: '/usr/bin/fls' -V
Sat Oct 22 15:38:12 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/file' -z -b -
Sat Oct 22 15:38:12 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/file' -z -b -
Sat Oct 22 15:38:12 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8
Sat Oct 22 15:39:32 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/md5sum'
Sat Oct 22 15:39:32 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/sha1sum'
Sat Oct 22 15:39:32 2011: '/usr/bin/istat' -f fat16 -z "BRST" -s '0' -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8

Sat Oct 22 15:39:32 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/file' -z -b -

Sat Oct 22 15:39:32 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8

Sat Oct 22 15:40:00 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/srch_strings' -a

Sat Oct 22 15:40:15 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/md5sum'

Sat Oct 22 15:40:15 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/sha1sum'

Sat Oct 22 15:40:15 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/srch_strings' -a | '/usr/bin/md5sum'

Sat Oct 22 15:40:16 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/srch_strings' -a | '/usr/bin/sha1sum'

Sat Oct 22 15:40:16 2011: '/usr/bin/istat' -f fat16 -z "BRST" -s '0' -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8

Sat Oct 22 15:40:17 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/file' -z -b -

Sat Oct 22 15:40:17 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/srch_strings' -a

Sat Oct 22 15:40:19 2011: '/usr/bin/fls' -V

Sat Oct 22 15:42:38 2011: '/usr/bin/ils-sleuthkit' -f fat16 -e -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700

Sat Oct 22 15:42:38 2011: '/usr/bin/icat-sleuthkit' -f fat16 -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -

Sat Oct 22 15:42:38 2011: '/usr/bin/icat-sleuthkit' -f fat16 -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/md5sum'

Sat Oct 22 15:42:39 2011: '/usr/bin/icat-sleuthkit' -f fat16 -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/sha1sum'

Sat Oct 22 15:42:39 2011: '/usr/bin/istat' -f fat16 -z "BRST" -s '0' -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700

Sat Oct 22 15:42:44 2011: '/usr/bin/fls' -V

Sat Oct 22 15:43:51 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/md5sum'

Sat Oct 22 15:43:51 2011: '/usr/bin/ils-sleuthkit' -f fat16 -e -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700

Sat Oct 22 15:43:51 2011: '/usr/bin/icat-sleuthkit' -f fat16 -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -

Sat Oct 22 15:43:51 2011: '/usr/bin/icat-sleuthkit' -f fat16 -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/md5sum'

Sat Oct 22 15:43:51 2011: '/usr/bin/icat-sleuthkit' -f fat16 -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/sha1sum'

Sat Oct 22 15:43:51 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/sha1sum'

Sat Oct 22 15:43:51 2011: '/usr/bin/istat' -f fat16 -z "BRST" -s '0' -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700

Sat Oct 22 15:43:51 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/md5sum'

Sat Oct 22 15:43:51 2011: '/usr/bin/istat' -f fat16 -z "BRST" -s '0' -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8

Sat Oct 22 15:43:51 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/sha1sum'

Sat Oct 22 15:43:51 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/file' -z -b -

Sat Oct 22 15:43:51 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8

Sat Oct 22 15:43:51 2011: '/usr/bin/istat' -f fat16 -z "BRST" -s '0' -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8

Sat Oct 22 15:43:51 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/file' -z -b -

Sat Oct 22 15:43:51 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8

Sat Oct 22 15:43:54 2011: '/usr/bin/fls' -V

Sat Oct 22 15:45:47 2011: '/usr/bin/fls' -f fat16 -la -z "BRST" -s '0' -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 2

Sat Oct 22 15:46:59 2011: '/usr/bin/fls' -f fat16 -ldr -z "BRST" -s '0' -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 2

Sat Oct 22 16:15:39 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/sha1sum'

Sat Oct 22 16:15:39 2011: '/usr/bin/istat' -f fat16 -z "BRST" -s '0' -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8

Sat Oct 22 16:16:37 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 7 | '/usr/bin/file' -z -b -

Sat Oct 22 16:16:37 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 7 | '/usr/bin/file' -z -b -

Sat Oct 22 16:16:37 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 7

Sat Oct 22 16:16:41 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 7

Sat Oct 22 16:16:47 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1081 | '/usr/bin/file' -z -b -

Sat Oct 22 16:16:47 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1081

Sat Oct 22 16:16:47 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1081 | '/usr/bin/file' -z -b -

Sat Oct 22 16:16:50 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1081

Sat Oct 22 16:17:07 2011: '/usr/bin/ils-sleuthkit' -f fat16 -e -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8

Sat Oct 22 16:17:07 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/file' -z -b -

Sat Oct 22 16:17:07 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/md5sum'

Sat Oct 22 16:17:07 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/sha1sum'

Sat Oct 22 16:17:07 2011: '/usr/bin/istat' -f fat16 -z "BRST" -s '0' -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8

Sat Oct 22 16:17:12 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/file' -z -b -

Sat Oct 22 16:17:12 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8

Sat Oct 22 16:17:12 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/file' -z -b -

Sat Oct 22 16:17:36 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8

Sat Oct 22 16:19:20 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1081 | '/usr/bin/file' -z -b -

Sat Oct 22 16:19:20 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1081

Sat Oct 22 16:19:20 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1081 | '/usr/bin/file' -z -b -

Sat Oct 22 16:19:23 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1081

Sat Oct 22 16:19:35 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1053 | '/usr/bin/file' -z -b -

Sat Oct 22 16:19:35 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1053 | '/usr/bin/file' -z -b -

Sat Oct 22 16:19:35 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r   -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1053 | '/usr/bin/file' -z -b -

Sat Oct 22 16:19:35 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r   -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1053

Sat Oct 22 16:19:39 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r   -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1053 | '/usr/bin/file' -z -b -

Sat Oct 22 16:19:39 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r   -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1053

Sat Oct 22 16:19:47 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1053

Sat Oct 22 16:20:03 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1050 | '/usr/bin/file' -z -b -

Sat Oct 22 16:20:03 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1050 | '/usr/bin/file' -z -b -
Sat Oct 22 16:20:03 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1050
Sat Oct 22 16:20:08 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1050
Sat Oct 22 16:20:28 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1053 | '/usr/bin/file' -z -b -
Sat Oct 22 16:20:28 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1053 | '/usr/bin/file' -z -b -
Sat Oct 22 16:20:28 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r   -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1053 | '/usr/bin/file' -z -b -
Sat Oct 22 16:20:28 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r   -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1053
Sat Oct 22 16:20:29 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1053 | '/usr/bin/file' -z -b -
Sat Oct 22 16:20:29 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1053 | '/usr/bin/file' -z -b -
Sat Oct 22 16:20:29 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r   -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1053 | '/usr/bin/file' -z -b -
Sat Oct 22 16:20:29 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r   -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1053
Sat Oct 22 16:20:30 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r   -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1053 | '/usr/bin/file' -z -b -
Sat Oct 22 16:20:30 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r   -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1053
Sat Oct 22 16:20:31 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1050 | '/usr/bin/file' -z -b -
Sat Oct 22 16:20:31 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1050
Sat Oct 22 16:20:31 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1050 | '/usr/bin/file' -z -b -
Sat Oct 22 16:20:33 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1050

Sat Oct 22 16:29:17 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/file' -z -b -

Sat Oct 22 16:29:17 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8

Sat Oct 22 16:29:17 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8 | '/usr/bin/file' -z -b -

Sat Oct 22 16:29:22 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 8

Sat Oct 22 18:27:11 2011: '/usr/bin/fls' -f fat16 -la -z "BRST" -s '0' -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 2

Sat Oct 22 18:27:25 2011: '/usr/bin/icat-sleuthkit' -f fat16 -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -

Sat Oct 22 18:27:25 2011: '/usr/bin/icat-sleuthkit' -f fat16 -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700

Sat Oct 22 18:27:25 2011: '/usr/bin/icat-sleuthkit' -f fat16 -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -

Sat Oct 22 18:27:34 2011: '/usr/bin/icat-sleuthkit' -f fat16 -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700

Sat Oct 22 18:27:37 2011: '/usr/bin/icat-sleuthkit' -f fat16 -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817701 | '/usr/bin/file' -z -b -

Sat Oct 22 18:27:37 2011: '/usr/bin/icat-sleuthkit' -f fat16 -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817701 | '/usr/bin/file' -z -b -

Sat Oct 22 18:27:37 2011: '/usr/bin/icat-sleuthkit' -f fat16 -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817701

Sat Oct 22 18:27:39 2011: '/usr/bin/icat-sleuthkit' -f fat16 -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -

Sat Oct 22 18:27:39 2011: '/usr/bin/icat-sleuthkit' -f fat16 -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -

Sat Oct 22 18:27:39 2011: '/usr/bin/icat-sleuthkit' -f fat16 -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700

Sat Oct 22 18:27:40 2011: '/usr/bin/icat-sleuthkit' -f fat16 -o 62 -i raw '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -

Sat Oct 22 18:27:40 2011: '/usr/bin/icat-sleuthkit' -f fat16 -o 62 -i raw

```
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -
Sat Oct 22 18:27:40 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700
Sat Oct 22 18:27:41 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -
Sat Oct 22 18:27:41 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700
Sat Oct 22 18:27:41 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -
Sat Oct 22 18:27:41 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -
Sat Oct 22 18:27:41 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -
Sat Oct 22 18:27:41 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700
Sat Oct 22 18:27:42 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -
Sat Oct 22 18:27:42 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700
Sat Oct 22 18:27:42 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -
Sat Oct 22 18:27:42 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -
Sat Oct 22 18:27:42 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -
Sat Oct 22 18:27:42 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700
Sat Oct 22 18:27:42 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -
Sat Oct 22 18:27:42 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700
Sat Oct 22 18:27:42 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -
```

```
Sat Oct 22 18:27:43 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -
Sat Oct 22 18:27:43 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -
Sat Oct 22 18:27:43 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700
Sat Oct 22 18:27:43 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -
Sat Oct 22 18:27:43 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -
Sat Oct 22 18:27:43 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700
Sat Oct 22 18:27:43 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -
Sat Oct 22 18:27:43 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700 | '/usr/bin/file' -z -b -
Sat Oct 22 18:27:43 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700
Sat Oct 22 18:27:46 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817700
Sat Oct 22 18:27:52 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817699 | '/usr/bin/file' -z -b -
Sat Oct 22 18:27:52 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817699 | '/usr/bin/file' -z -b -
Sat Oct 22 18:27:52 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817699
Sat Oct 22 18:28:08 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817699 |
'/usr/bin/srch_strings' -a
Sat Oct 22 18:28:13 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817699 | '/usr/bin/md5sum'
Sat Oct 22 18:28:13 2011: '/usr/bin/icat-sleuthkit' -f fat16  -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817699 | '/usr/bin/sha1sum'
```

Sat Oct 22 18:28:13 2011: '/usr/bin/istat' -f fat16 -z "BRST" -s '0' -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817699
Sat Oct 22 18:28:13 2011: '/usr/bin/icat-sleuthkit' -f fat16 -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817699 | '/usr/bin/file' -z -b -
Sat Oct 22 18:28:13 2011: '/usr/bin/icat-sleuthkit' -f fat16 -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 16817699
Sat Oct 22 18:28:13 2011: '/usr/bin/fls' -V
Sat Oct 22 18:28:33 2011: '/usr/bin/fls' -f fat16 -la -z "BRST" -s '0' -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 4
Sat Oct 22 18:28:35 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1083 | '/usr/bin/file' -z -b -
Sat Oct 22 18:28:35 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1083 | '/usr/bin/file' -z -b -
Sat Oct 22 18:28:35 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r   -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1083 | '/usr/bin/file' -z -b -
Sat Oct 22 18:28:35 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r   -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1083
Sat Oct 22 18:28:45 2011: '/usr/bin/fls' -f fat16 -ldr -z "BRST" -s '0' -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 2
Sat Oct 22 18:28:57 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
Sat Oct 22 18:29:21 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r   -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1053 | '/usr/bin/file' -z -b -
Sat Oct 22 18:29:21 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r   -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1053
Sat Oct 22 18:29:24 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1083 | '/usr/bin/file' -z -b -
Sat Oct 22 18:29:24 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1083 | '/usr/bin/file' -z -b -
Sat Oct 22 18:29:24 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r   -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1083 | '/usr/bin/file' -z -b -
Sat Oct 22 18:29:24 2011: '/usr/bin/icat-sleuthkit' -f fat16 -r   -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 1083
Sat Oct 22 18:34:12 2011: '/usr/bin/fls' -f fat16 -la -z "BRST" -s '0' -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 2

Sat Oct 22 18:34:23 2011: '/usr/bin/blkcat' -f fat16 -s -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd'

Sat Oct 22 18:34:23 2011: '/bin/grep' -i -E 'porn'

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/output/copia.dd-62-1051519-fat16.asc'

Sat Oct 22 18:34:24 2011: '/bin/grep' -i -E 'porn'

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/output/copia.dd-62-1051519-fat16.uni'

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 352 | '/usr/bin/file' -z -b -

Sat Oct 22 18:41:41 2011: '/usr/bin/blkstat' -f fat16 -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 352

Sat Oct 22 18:44:00 2011: '/usr/bin/blkcat' -f fat16 -s -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd'

Sat Oct 22 18:44:00 2011: '/bin/grep' -i -E 'hack'

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/output/copia.dd-62-1051519-fat16.asc'

Sat Oct 22 18:44:01 2011: '/bin/grep' -i -E 'hack'

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/output/copia.dd-62-1051519-fat16.uni'

Sat Oct 22 18:45:52 2011: '/usr/bin/fsstat' -f fat16 -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd'

Sat Oct 22 18:46:10 2011: '/usr/bin/blkcat' -f fat16 -s -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd'

Sat Oct 22 18:46:10 2011: '/usr/bin/blkcat' -f fat16 -s -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd'

Sat Oct 22 18:46:10 2011: '/usr/bin/blkcat' -f fat16 -s -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd'

Sat Oct 22 18:46:37 2011: '/usr/bin/blkcat' -f fat16 -s -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd'

Sat Oct 22 18:46:37 2011: '/usr/bin/blkcat' -f fat16 -a -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 7840 1

Sat Oct 22 18:46:37 2011: '/usr/bin/blkcat' -f fat16 -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 7840 | '/usr/bin/file' -z -b -

Sat Oct 22 18:46:37 2011: '/usr/bin/blkstat' -f fat16 -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 7840

Sat Oct 22 18:46:40 2011: '/usr/bin/blkls' -el -f fat16 -o 62 -i raw

'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 0-499
Sat Oct 22 18:46:47 2011: '/usr/bin/blkcat' -f fat16 -s -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd'
Sat Oct 22 18:46:47 2011: '/usr/bin/blkcat' -f fat16 -s -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd'
Sat Oct 22 18:46:47 2011: '/usr/bin/blkcat' -f fat16 -a -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 448 1
Sat Oct 22 18:46:47 2011: '/usr/bin/blkcat' -f fat16 -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 448 | '/usr/bin/file' -z -b -
Sat Oct 22 18:46:47 2011: '/usr/bin/blkstat' -f fat16 -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' 448
/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/output/HDinteiro
Mon Oct 31 19:18:42 2011: '/usr/bin/fls' -z "BRST" -s '0' -m 'C:/' -f fat16 -r -o 62 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' >>
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/output/body'
Mon Oct 31 19:18:42 2011: '/usr/bin/fls' -z "BRST" -s '0' -m '/2/' -f ext -r -o 1051520 -i raw
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/images/copia.dd' >>
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/output/body'
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/output/body'
Mon Oct 31 19:18:43 2011: '/usr/bin/md5sum'
/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/output/body
Mon Oct 31 19:18:59 2011: LANG=C LC_ALL=C '/usr/bin/mactime-sleuthkit' -b
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/output/body' -z "BRST" -i day
'/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/output/timeline.txt.sum' 2011-01-01..2011-10-01
> '/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/output/timeline.txt'
Mon Oct 31 19:18:59 2011: '/usr/bin/md5sum'
/var/lib/autopsy/Pedofilias/SuspeitoPedofilia/output/timeline.txt

APÊNDICE C - ARTIGO: PERICIA FORENSE COMPUTACIONAL: FERRAMENTAS E METODOLOGIAS PARA RESPOSTA A INCIDENTES

Aguinaldo Gregório Cristiano[1], Paulo João Martins[2], Sergio Coral[2]

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

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

aguinaldogc@hotmail.com, pjm@unesc.net, sc@unesc.net

Abstract. *This study aimed to demonstrate by a fictitious case, the operation of some tools on Helix 3, cite and apply the basic requirements for the development of a forensic, document and demonstrate the copy and the treatment of evidence and use a fictional case study to demonstrate how to perform the forensic process, using the method SOP. In terms of results, it was possible to find evidence that can be used in a court of law to judge the suspect.*

Resumo. *Este trabalho teve como objetivos demonstrar mediante um caso fictício o funcionamento de algumas ferramentas presentes no Helix 3, citar e aplicar os quesitos básicos para a elaboração de uma perícia forense, documentar e demonstrar a cópia e o tratamento de evidências e utilizar um caso fictício para demonstrar como realizar o processo forenses, utilizando a metodologia SOP. Em termos de resultados, foi possível encontrar provas que podem ser utilizadas em um corte judicial para condenar o suspeito.*

1. Introdução

É quase que impossível imaginar que no passado não havia os recursos tecnológicos (Celulares, Computadores, GPS, entre outros) que estão disponíveis hoje. Eles tornaram-se de vital importância na sociedade, e dentre estes itens tecnológicos, em destaque está o computador.

O computador faz parte do cotidiano, desempenhando um papel fundamental na organização de informações, compartilhamento de dados, pesquisas por meio da Internet e no entretenimento. Junto com esses benefícios, surgiu também um problema que é a falta de segurança dos sistemas.

Em resposta ao surgimento dos crimes digitais surgiu a necessidade da criação de uma área, a Forense Computacional, cujos profissionais recebem a denominação de Peritos Forenses. Um perito forense no campo computacional tem as atribuições de usar o conhecimento das Técnicas e Metodologias criadas na Computação Forense, aplicadas com o apoio ferramental apropriado para obter dados e artefatos, tendo por objetivo qualificá-los como vestígios, evidências, ou provas no âmbito judicial (MELO, 2009).

Partindo das considerações feitas, este projeto propõe o estudo de algumas técnicas e metodologias para resposta a incidentes presentes no Helix 3 objetivando dar facilidade ao uso direcionado das ferramentas e metodologias ao usuários para aplicação das mesmas.

2 Resposta A Incidentes De Segurança

Resposta a Incidente é o processo que tem por objetivo identificar, conter, erradicar e recuperar um sistema, logo após o mesmo ser comprometido, é realizado por um pessoal de segurança responsável (CHUVAKIN; PEIKARI, 2004, tradução nossa). Qualquer atividade

anormal confirmada que tenha como objetivo subverter o funcionamento e que comprometa a estabilidade de um sistema de computação ou de uma rede de computadores explicita ou implicitamente, é um incidente (CERT, 2004).

2.1 Tipos De Incidentes De Segurança

De acordo com SCHEITZER (2003, tradução nossa) o incidente de segurança, abrange as seguintes categorias gerais de eventos adversos, ataques com códigos maliciosos, acesso não autorizado, uso não autorizado de serviços, interrupção do serviço, desvios, espionagem e boatos.

2.2 Objetivos Da Resposta A Incidentes De Segurança

Com o uso da metodologia para resposta a incidentes, têm-se como meta, alcançar objetivos para poderem ser formuladas respostas que depois serão apresentadas a alguma entidade, os objetivos a serem atingidos com uma resposta a incidentes segundo Mandia e Prosise (2001, tradução nossa), passam por obter a confirmação ou, se for o caso, descartar a ocorrência de um incidente; fazer com que as informações acumuladas sejam precisas; encontrar meios para que a recuperação, tratamento e uso das provas sejam adequados, entre outros.

3 Perícia Forense Computacional

Perícia Forense Computacional é a preservação, identificação, extração, interpretação, análise e documentação de evidências computacionais colhidas em equipamentos eletrônicos (KLEIMAN, 2007, tradução nossa).

Steve *Haileys*, CEO e professor do *Institute Cyber security* (ICS), define forense computacional como sendo preservação, identificação, coleta, interpretação e documentação de evidências computacionais, incluindo as regras de evidência, processo legal, integridade da evidência, relatório factual da evidência e provisão de opinião de especialista em uma corte judicial, ou outro tipo de processo administrativo e/ou legal com relação ao que foi encontrado (HAILEYS, 2002, tradução nossa).

4 Metodologia SOP

A metodologia *Standard Operating Procedures* (SOP) foi criada pela *Scientific Working Group on Digital Evidence* (SWGDE), representante norte-americano na *Organization Computer Evidence* (IOCE) e é feita em 7 etapas que serão descritas segundo a (SWGDE, 2006, 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) **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;

c) **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;

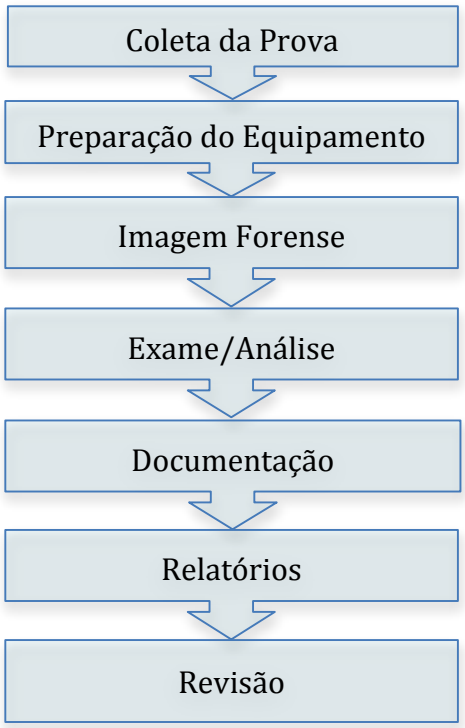


Figura 1. Fluxograma da metodologia SOP
Fonte: SWGDE (2006)

d) **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;

e) **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;

f) **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;

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

5 HELIX

Foi personalizado a partir de uma distribuição Knoppix padronizada, é baseado no Ubuntu. Ele foi majoritariamente desenvolvido por Klaus Knopper e contém varias contribuições de programadores pelo mundo. O Helix é mantido pela empresa E-fense, e Segundo manual distribuído pela empresa, a ferramenta possui detalhes que a diferenciam do resto que se encontra no mercado (GLEASON; FAHEY, 2006, tradução nossa).

Pode-se encontrar nesta distribuição ferramentas para detecção, identificação, análise, preservação e emissão de relatório que são necessárias para que se realize uma

resposta a incidente e ou perícia forense sem nenhum problema. O Helix é multiplataforma, atende os principais três sistemas operacionais do mercado, Mac OS Windows e Linux (E-FENSE, 2009, tradução nossa).

O modo de operação do Helix no Windows foi desenvolvido porque a maioria dos incidentes ocorre nesta plataforma, no entanto, se fez necessário criar uma ferramenta que interaja com este SO de maneira a facilitar a coleta de dados e posterior envio para análise em uma estação forense. Neste modo é executada uma aplicação padrão que possibilitará fazer a coleta da informação *in vivo* (GLEASON; FAHEY, 2006, tradução nossa).

O Helix no modo Linux é inicializado pelo CD com sistema operacional autocontido que é usado para fazer a análise detalhada de sistemas off-line ou conhecidos também como *Post mortem.* Ao ser inicializado, executa completamente pelo Live CD, montando todos os discos apenas em modo leitura para que estes não sejam modificados, fator importante para que não se contamine uma evidência digital. Uma grande vantagem deste modo é sem dúvida a portabilidade, pois permite ser inicializado na maioria dos computadores utilizando arquitetura x86 (GLEASON; FAHEY, 2006, tradução nossa).

6 Estudo de Caso

Nesta etapa será apresentado um caso de estudo, que como dito anteriormente, facilita por meios práticos na compreensão de como e quando as ferramentas devem ser usadas, e qual a confiabilidade da ferramenta tendo em conta os objetivos que estas se propõem alcançar.

6.1 Metodologia da perícia forense

O presente caso de estudo é um desafio proposto pelo especialista forense Eriberto Mota. Simula um ambiente real propício para análise forense. Objetiva-se encontrar provas que liguem um suspeito de praticar pedofilia.

6.2 Coleta da Prova

Sabendo-se que o caso é proveniente de um ambiente de estudo, o mesmo já se encontra devidamente armazenado, ou seja, já foi coletado. A coleta da prova foi efetuada com software livre, sendo este baseado no comando DD.

6.3 Preparação do equipamento

Para análise das evidências depois de coletada foi criado um laboratório improvisado com condições minimamente aceitáveis em termos de software e hardware.

6.4 Imagem Forense

A imagem foi recolhida com êxito, e armazenada em um disco rígido externo com a capacidade de 320 Gb que antes foi devidamente formatado.

Como toda e qualquer perícia forense, a imagem a ser analisada, depois de coletada, deve ser submetida a um algoritmo com a finalidade de gerar um código *Hash,* nesse caso foi utilizadoo algoritmo MD5.

6.5 Exame/Análise

Naturalmente para se fazer a análise é necessário que a imagem forense seja montada no sistema, e para tanto é necessário que a mesma receba somente a permissão de leitura. Por se tratar de uma imagem em formato RAW e possuindo 2 partições cada uma com um tipo de sistema de arquivo, torna-se um pouco mais trabalhoso fazer a montagem, devendo-se utilizar opções adicionais para que isto seja realizado.

Foi feita uma análise preliminar para que se visualizasse a estrutura interna de cada partição detalhadamente. A ferramenta usada para tal foi a *tree*, que pode ser encontrada nos repositórios do Ubuntu. Acessandodo a partição (disco1) e executando o comando, obteve-se as seguintes informações: possui apenas um diretório, chamado "fotos"; dentro do diretório fotos encontram-se vários arquivos no formato .jpg; partição possui um total de 18 arquivos.

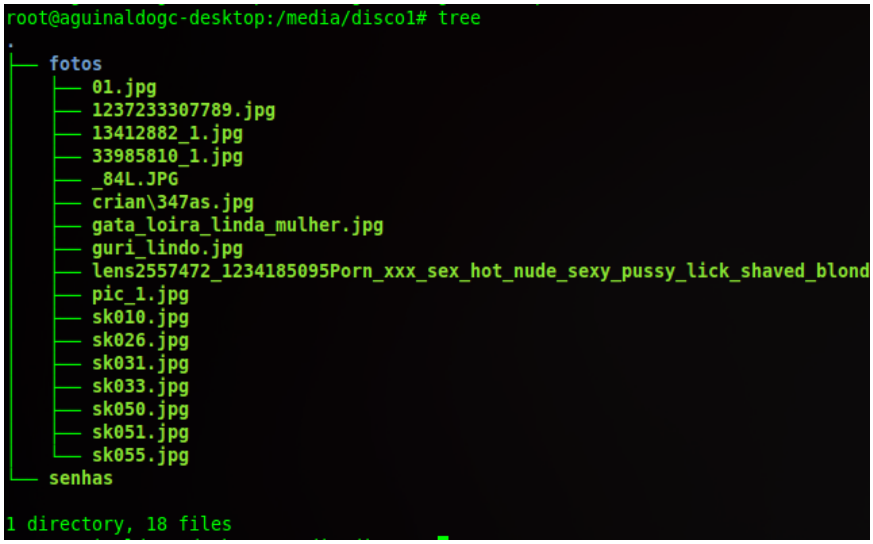


Figura 2. Uso do comando tree no disco 1

Pode-se observar nesta árvore de arquivos que alguns dos arquivos possuem nomes que vão de encontro com o que se procura, que são informações relativamente a respeito de atividades criminosas relacionadas com pornografia infantil:crian\347as.jpg, gata_loira_linda_mulher.jpg, guri_lindo.jpg, arquivos com nome com várias expressões pornográficas em língua inglesa.

Usou-se o mesmo comando, *tree*, na segunda partição, com o sistema de arquivos Ext3 (Linux), que retornou a informação de que a partição (disco2) possui um total de 162 arquivos, distribuídos em 9 diretórios, e, nesse espaço, foram encontradas as seguintes informações suspeitas: arquivos html com expressões como pedófilos e criança; arquivos com extensão jpg., alguns com nomes que se relacionam as buscas.

Por se tratar de uma análise preliminar, não se tirou nenhuma conclusão a respeito dos arquivos considerados suspeitos encontrados nas duas partições, sendo que até ao momento, as evidências encontradas ainda não foram visualizadas, para comprovação de que se tratam realmente de imagens de pornografia infantil.

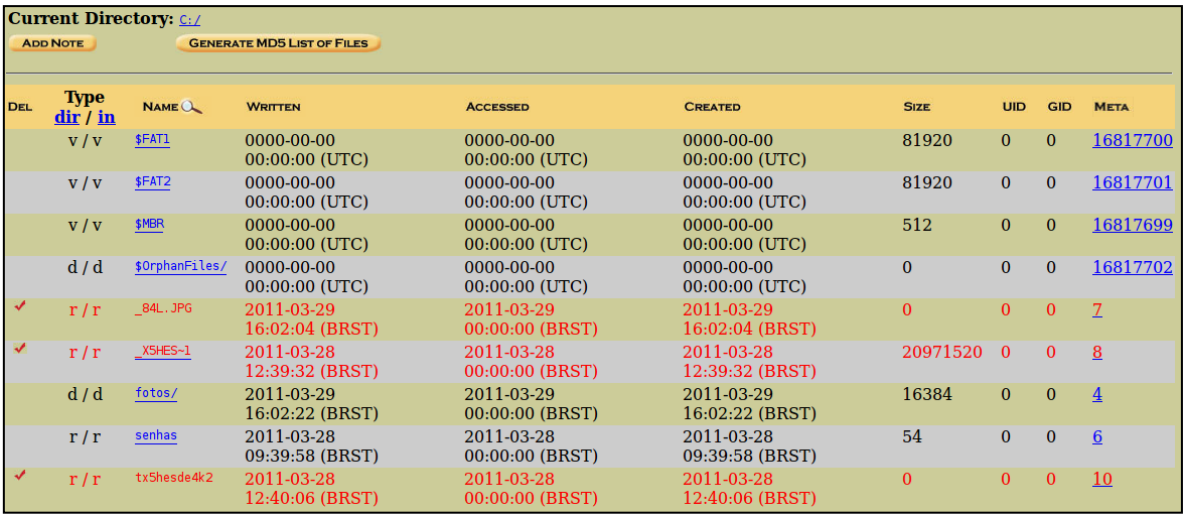
Passou-se para o uso de um software presente no Helix, o *Autopsy*, é um software que funciona por meio de um browser, e serve para fazer análise da imagem forense em diversos formatos, fornecendo diversos tipos de informações, bem como ajuda na visualização de arquivos apagados e sua posterior recuperação.

Com a opção *analyze* começa-se então fazer-se a análise do caso proposto efetivamente, de modo gráfico, com a ferramenta. Começou-se primeiro por analisar a partição que se encontra no formato FAT, e foi encontrada a seguinte estrutura de arquivos, conforme mostra a figura 38.

A figura mostra a raiz da partição "C:/" que ao contrário da ferramenta *tree* apresenta dois diretórios, fica aqui evidênciado a importância de se fazer a análise utilizando mais de uma ferramenta, pois algumas podem conter atributos mais eficientes que a outra,

conforme o resultado que nos é apresentado aqui. Os diretórios que não apareceram com o uso do comando *tree* são o "$OrphanFiles, $FAT1, $FAT2, $MBR".

Arquivos ou diretórios "$FAT1, $FAT2 e $MBR, contêm informações nativas do sistema de arquivos da partição, e o "OrphanFiles " contém arquivos deletados.



Current Directory: C:/

ADD NOTE | GENERATE MD5 LIST OF FILES

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
	v / v	$FAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	81920	0	0	16817700
	v / v	$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	81920	0	0	16817701
	v / v	$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	16817699
	d / d	$OrphanFiles/	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	16817702
✓	r / r	_84L.JPG	2011-03-29 16:02:04 (BRST)	2011-03-29 00:00:00 (BRST)	2011-03-29 16:02:04 (BRST)	0	0	0	7
✓	r / r	_X5HES~1	2011-03-28 12:39:32 (BRST)	2011-03-28 00:00:00 (BRST)	2011-03-28 12:39:32 (BRST)	20971520	0	0	8
	d / d	fotos/	2011-03-29 16:02:22 (BRST)	2011-03-29 00:00:00 (BRST)	2011-03-29 16:02:22 (BRST)	16384	0	0	4
	r / r	senhas	2011-03-28 09:39:58 (BRST)	2011-03-28 00:00:00 (BRST)	2011-03-28 09:39:58 (BRST)	54	0	0	6
✓	r / r	tx5hesde4k2	2011-03-28 12:40:06 (BRST)	2011-03-28 00:00:00 (BRST)	2011-03-28 12:40:06 (BRST)	0	0	0	10

Figura 3. Diretório raiz da primeira partição

Pode-se verificar ainda na figura 3 arquivos apagados, estes, são marcados com a cor vermelha, trata-se de um arquivo com extensão .JPG e dois sem extensão visível, de realçar que um dos arquivos sem extensão, o "_X5HES-1" possui um tamanho de aproximadamente 21Mb, que pode ser observado no campo "Size". Foram feitas algumas análises que serão mostradas em passos seguintes, e chegou-se a conclusão de que não se trata de um arquivo, mas, provavelmente trata-se de um diretório, dificultando assim a sua recuperação, pois, como se sabe os diretórios possuem vários arquivos, e estes arquivos ocupam espaço em vários setores do disco rígido, tornando assim quase impossível a sua recuperação.

Um dos que mais chamou a atenção foi o arquivo "senhas", o mesmo foi acessado via relatório Hexadecimal para ter-se acesso ao seu conteúdo, e foram encontradas algumas informações que se pressupõe ser de contas de e-mail do suspeito. O Arquivo encontra-se no sector 480 e foi acessado pela última vez na Segunda feira de Março, no dia 28 às 09h39min58seg de 2011.

Fez-se em toda a partição a busca de arquivos deletados pelo suspeito, utilizando uma opção presente na altura em que se faz a análise. O botão é o "All Deleted Files". Ao executar esta ação obteve-se uma lista de todos os arquivos deletados da partição. Pode-se observar que vários arquivos apagados são provavelmente imagens. Pode-se observar na figura 41 algumas opções para exibição dos dados presentes na imagem.

A primeira opção "ASCII (display - report)" exibe o arquivos em ASCII e gera um relatório com "report" contendo todas as informações como data de criação, de acesso e o setor em que se encontra o arquivo, o mesmo acontece com a opção "HEX" apenas alterando para Hexadecimal a forma de exibição, e de igual modo também acontece com a opção "ASCII Strings".

Directory Seek

Enter the name of a directory that you want to view.
C:/

VIEW

File Name Search

Enter a Perl regular expression for the file names you want to find.

SEARCH

ALL DELETED FILES

EXPAND DIRECTORIES

All Deleted Files

Type dir / in	Name	Written	Accessed	Created	Size	UID	GID	Meta
r / r	C:/fotos /_K076.JPG	2011-03-28 11:41:06 (BRST)	2011-03-29 00:00:00 (BRST)	2011-03-28 11:41:06 (BRST)	205168	0	0	1050
r / r	C:/fotos /_84L.JPG	2011-03-28 21:36:26 (BRST)	2011-03-28 00:00:00 (BRST)	2011-03-28 21:36:26 (BRST)	2533650	0	0	1053
r / r	C:/fotos /sk034.jpg	2011-03-28 10:36:30 (BRST)	2011-03-28 00:00:00 (BRST)	2011-03-28 10:36:30 (BRST)	205706	0	0	1062
r / r	C:/fotos /japporn.jpg	2011-03-28 18:43:28 (BRST)	2011-03-29 00:00:00 (BRST)	2011-03-28 18:43:28 (BRST)	85216	0	0	1081
r / r	C:/fotos /882961.jpg	2011-03-28 18:49:32 (BRST)	2011-03-29 00:00:00 (BRST)	2011-03-28 18:49:32 (BRST)	58014	0	0	1083
r / r	C:/_84L.JPG	2011-03-29 16:02:04 (BRST)	2011-03-29 00:00:00 (BRST)	2011-03-29 16:02:04 (BRST)	0	0	0	7
r / r	C:/_X5HES~1	2011-03-28 12:39:32 (BRST)	2011-03-28 00:00:00 (BRST)	2011-03-28 12:39:32 (BRST)	20971520	0	0	8
r / r	C:/tx5hesde4k2	2011-03-28 12:40:06 (BRST)	2011-03-28 00:00:00 (BRST)	2011-03-28 12:40:06 (BRST)	0	0	0	10

Figura 4. Arquivos deletados

Com isso recorreu-se a duas ferramentas de referência no cenário forense com software livre, o Foremost e o Scalpel.

O Foremost recuperou um total de 100 arquivos, entre imagens e aruqivos de texto e paginas web salvas. O Scalpel recuperou ao total 131 arquivos, incluido videos.

Um total de 94 arquivos com extensões .JPG, .BMP. e .GIF, foram catalogados como sendo de pornografia infantil, fazendo apologia, ou ainda relacionando-se de alguma forma negativa. Dentre eles foram destacados alguns apresentados na figura 5:

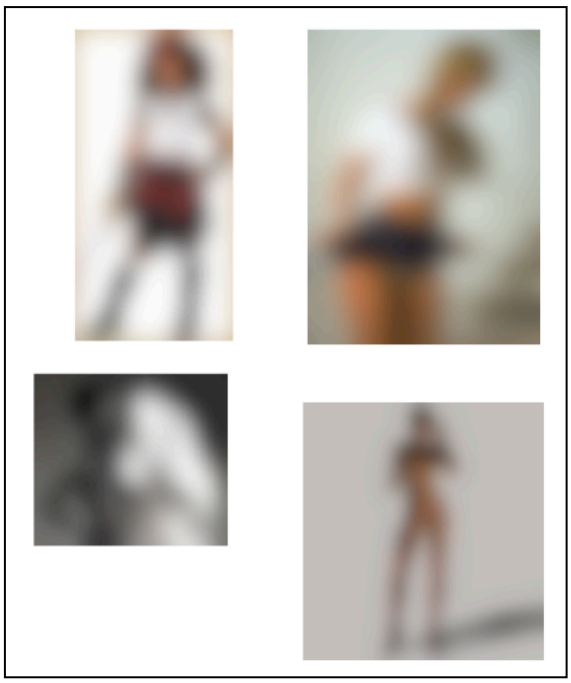


Figura 5. Arquivo contendo técnicas para atração de menores

De forma preliminar, pelo conteúdo apresentado já se pode afirmar que o suspeito mantinha contato de alguma forma com conteúdo pornográfico infantil tendo em conta que as

provas estão bastante visíveis e por serem mais de uma, indicam que não houve nenhum incidente para as fotos terem ido parar no computados do mesmo.

6.6 Documentação

No ato da documentação da cena do crime, era suposto que fosse incluída uma cópia da autorização judicial emitida pelos órgãos competentes para que a coleta e o manuseio das provas periciais fossem feitas dentro da lei, mas, tratando-se de um caso fictício, não houve esta necessidade, pois o mesmo destina-se apenas para uso acadêmico e não para ser apresentado em um tribunal.

A cadeia de custódia foi gerada baseando-se em informações fictícias como o tipo de evidência, a descrição do mesmo, o fabricante, modelo, e o número de série. Também são inclusos detalhes sobre a imagem dos dados como a hora da sua criação, o nome do perito responsável, os métodos usados para obtenção da mesma e os locais para onde o material apreendido foi levado até chegar ao laboratório para a análise efetiva.

6.7 Relatório/Revisão

Devem conter informações no relatório e na revisão que abordam as necessidades do solicitante, que objetivam dar informações de forma relevante ao leitor.

Por se tratar de um trabalho para fins de aprendizado e contribuição bibliográfica de modo geral, todas as etapas foram escritas de modos a que os iniciante na área e curiosos pudessem compreender todo o processo envolvido no ato de uma perícia, sendo assim fica desnecessário reapresentar tais informações neste passo.

O estudo do caso serviu dentre outros objetivos para medir o nível de eficiência das ferramentas, isso foi feito de maneira prática, como por exemplo na recuperação dos dados apagados, (quando foram usadas as ferramentas Scalpel e Foremost, a primeira demontrou ser mais eficiente, recuperando um numero maior de informações. No caso do Software de análise, o Autopsy, não foi feita comparação com nenhuma outra, mas a mesma mostrou ser eficiente, dada a quantidade de informação que encontrou, sem a necessidade de usar comandos complexos, sendo feita a análise a partir de uma interface gráfica, informações estas, sobre o sistema de arquivos das partições, arquivos apagados, e sobre os setores alocados ou não.

Com o uso do Autopsy conseguiu-se fazer uma procura em toda cópia do disco rígido por meio do sistema de busca por palavras chave, e, como resultado obteve-se a localização exata dos arquivos que continham conteúdo que faziam menção a algumas palavras como (criança, senha, porn, pornô, sex, fotos, pics, pictures, entre outros). Sendo o mecanismo de recuperação de arquivos do Autopsy um pouco limitado, recorreu-se a softwares secundários, já falados anteriormente.

Com o Scalpel e o Foremost, fez-se uma varredura um todos os disco, que resultou na recuperação de uma grande quantidade de arquivos, que vão desde imagens, documentos, vídeos, entre outros.

Diante das evidências recuperadas, por estas terem relação direta com o suspeito, e por serem de conteúdo ilegal, podem ser usadas futuramente para provar o envolvimento do mesmo neste tipo de atividades (pornografia infantil) em futuras análises feita pela justiça

7. CONCLUSÃO

O número de interessados pela área forense tem crescido, sobretudo mais voltados a ferramentas com licença livre. Nas pesquisas foi possível ter contato com algumas informações referentes a processos que tiveram como base um perito forense para o seu desfecho.

A pesquisa feita revelou-se de certa forma importante para evidênciar o papel de um time de resposta a incidentes na formulação de estratégias com o objetivo de dar solução a problemas referentes à segurança da informação, quer no caráter preventivo como de contenção e erradicação de ameaças ocorridas com auxílio de algumas ferramentas para detecção de intrusão e para perícia forense em geral.

Os objetivos específicos propostos foram alcançados, sendo que o primeiro compreendia a demonstração do funcionamento de algumas ferramentas presentes no Helix por meio de um caso fictício. Foi realizado com sucesso, e produziu resultados confiáveis que certamente poderiam ser usados para representação de um caso real, dado os mínimos detalhes que se teve com o manuseio da evidência digital e a aplicação efetiva da metodologia usada.

Citar e aplicar quesitos básicos para elaboração de uma perícia forense foi definido como o segundo objetivo específico, que foi alcançado no ato da aplicação da metodologia forense para a resolução do estudo de caso. Haja visto que em todas as etapas foram explicados nos mínimos detalhes possíveis e por intermédio de figuras contendo os dados reais, detalhes sobre como realizar uma perícia forense, e que efetivamente venha a ser aceita em uma corte judicial.

O terceiro objetivo foi atingido também, embora a imagem utilizada não tenha sido coletada, mas sim obtida de outra fonte, isto porque quando se pensou no caso aonde seria aplicada a análise, ficou patente a questão de o caso fictício ser montado pelo próprio perito forense (acadêmico), sendo assim com o objetivo de não comprometer, e fidelizar ainda mais os resultados, foi usado um caso criado por um terceiro, um profissional da área forense.

Com os objetivos específicos praticamente alcançados, com o objetivo geral não podia ser diferente, visto que o mesmo visava a análise de ferramentas e metodologias para resposta a incidentes presentes no Helix. As metodologias foram descritas e usadas para resolução do caso, por meio das ferramentas presentes no software proposto.

No decorrer do estudo foram encontrados vários obstáculos, nomeadamente a falta de bibliografia na área em Língua Portuguesa, a falta de padrões nas metodologias, e, principalmente o fato de a ferramenta principal a ser estudada ter passado de livre para paga, tornando assim alguns softwares específicos contidos na distribuição e definidos para estudo anteriormente, obsoleto, mas, este problema foi ultrapassado com a compra da versão paga. Desta forma foram usados consequentemente outros softwares substituindo os obsoletos.

Finalizando, acredita-se que irá contribuir para minimizar a carência bibliográfica na área, problema este apresentado como parte da justificativa.

REFERÊNCIAS

ARUSO, Carlos A. A.; STEFFEN, Flávio Denys.**Segurança em informática e de informações**. 2.ed. São Paulo: SENAC/SP, 1999.

BAKER; CASWELL. **Snort Intrusion Detection and Prevention Toolkit**. Boston: Addison Wesley, 2004.

B2NET. **ISS RealSecure SiteProtector** Disponível em: <http://www.b2net.co.uk/iss /iss_realsecure_siteprotector.htm> Acesso em: 9 Setembro. 2011, 10:30

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

BUENO, M. L. P**. Forense computacional:** técnicas e ferramentas. Catalão, 2007.

CAMPOS, André L. N. **Sistema de Segurança da Informação**. Florianópolis: Visual Books. 2006.

CARVALHO, Menezes, REVOREDO, Marcelo. **A Trajetória da Internet no Brasil l:** do surgimento das redes de computadores à instituição dos mecanismos de governança. Dissertação, Universidade Federal do Rio de Janeiro, 2006.

CARVEY, H. **Windows Forensics and Incident Recovery**. Boston: Addison Wesley, 2004.
CAMPELLO, *WEBER*. **O Sistema de Detecção de Intrusão *Asgaard*** Disponível em: <*labcom.inf.ufrgs.br/ceseg/anais/2001/05.pdf*> Acesso em: 9 Setembro. 2011, 10:35

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

CERT.br. **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.** Cartilha de Segurança para Internet Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 9 de Setembro de 2010.

COUTINHO, Luciano; CASSIOLATO, José Eduardo; SILVA, Ana Lucia Gonçalves da (Coord.).**Telecomunicações, globalização e competitividade**. Campinas: Papirus, 1995.

DANTAS, Mario. **Computação distribuída de alto desempenho:**redes, clusters e grids computacionais. Rio de Janeiro: Axcel Books do Brasil, 2005.

DOS REIS, M. A. **Forense Computacional e sua aplicação em segurança imunológica**.Tese de Mestrado, Universidade Estadual de Campinas, 2003.

E-FENSE. **HELIX 3 Pro**: Meeting your computer forensics needs! Disponível em: <http://accessdata.com/downloads/media/Helix3Pro.pdf>Acesso em: 6 Junho. 2011, 15:10

FARMER, Dan; VENEMA, Wietse. **Perícia Forense Computacional:** Teoria e Prática Aplicada. São Paulo: Pearson Prentice-Hall, 2007.

FIGG, William; ZHOU, Zehai. **A computer forensics minor curriculum proposal.** Texas: 2007.

FRATEPIETRO, Stefan, ROSSETI, Sandro. **DEFT**: Manual de uso. Disponivelem<http://www.deftlinux.net/doc/%5Bit%5Ddeft_manuale_full.pdf>Acessoem: 6 d ejunho. 2011, 15:57

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

GLEASON, BJ; FAHEY, Drew. **Helix 1.7 for Beginners**. EUA: E-fense, 2006.

GLEASON; Fahey, Drew. **Helix 1.7 for Beginners**. New York: E-fense. 2006.

GOMES, Olavo, ANSHIESHI José. **Segurança Total:** Protegendo-se contra os Hackers. São Paulo: Makron Books, 2000.

GOMES, Pedro. **Definição: Spywares e Malwares** Disponível em: <http://www.computadorseguro.com /definicao-malware-spyware/>Acesso em: 6 Junho. 2011, 16:30

HAILEYS, Steve. **What is Computer Forensics**: CyberSecurity Institute, 2002. Disponível em: <http://www.cybersecurityinstitute.biz/forensics.htm>Acesso em: 13 abr. 2011, 14:30

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.