Centro Universitário de Brasília – UNICEUB
FATECS – Faculdade de Tecnologia e Ciências
Curso de Engenharia da Computação
Disciplina: Projeto Final
Prof. Francisco Javier

LUIS GUSTAVO SANTOS FERNANDEZ

ANÁLISE FORENSE DE INTRUSÕES EM SISTEMAS COMPUTACIONAIS

Brasília / DF

1º Semestre de 2009

LUIS GUSTAVO SANTOS FERNANDEZ

ANALISE FORENSE DE INTRUSÕES EM SISTEMAS COMPUTACIONAIS

Monografia apresentada ao Curso de Engenharia da Computação, como requisito parcial para obtenção do grau de Engenheiro de Computação.

Orientador: Marco Antonio Araújo

.

Brasília / DF

1º Semestre de 2009

Resumo

Este trabalho tem como objetivo desenvolver uma metodologia forense para coleta e análise de dados de intrusões digitais, que consiste no uso de um protótipo que por meio do levantamento de evidências criminais seja capaz de indiciar um indivíduo judicialmente. A análise forense em sistemas computacionais tem como objetivo buscar provas de evidências após uma intrusão ao sistema. Essas provas podem ser usadas como evidências judiciais e assim indiciar uma pessoa judicialmente. A construção de uma arquitetura computacional específica permite levantar essas evidências e minimizar as intrusões digitais.

Palavras-chave: Intrusão, intruso, forense, segurança, prevenção, detecção, metodologia, captura, armazenamento, análise.

Abstract

The present work main objective is develop a forensic methodology for collection and analysis of data of digital intrusions, what consists in the use of a prototype that through the lifting of you show up you criminate that it is able to charge an individual judicially. The forensic analysis in computational systems has as objective looks for proofs of you show up after an intrusion to the system. These proofs can be used as you show up that you judge, and show up that you criminate to charge a person judicially. The construction of a specific computer architecture allows us to raise these criminal evidence and minimize intrusion digital.

Keywords: Intrusion, intruder, forensic, security, prevention, detection, methodology, capture, storage, analysis.

Eu dedico esse trabalho especialmente a minha mãe, Miriam dos Anjos Santos, que sempre esteve do meu lado, sempre insistindo e apoiando minha caminhada.

Agradecimentos

Agradeço preferencialmente aos meus familiares que sempre me apoiaram incondicionalmente e sempre pacientes.

Agradeço aos meus amigos que sempre estão ao meu lado nos momentos bons e ruins, sempre me apoiando e me dando forças para seguir meu caminho em frente.

Além de agradecer aos meus amigos não posso esquecer-me de citar grandes pessoas, amigos e irmãos que sempre estarão ao meu lado na luta do dia a dia são eles Adriel Kendrick de Melo, Eduardo Moreira Braga Neto, Felipe Kladi Gonçalves, Rômulo Cavalcante Pessoa e Thiago Edecio Galitezi.

Agradeço ao meu pai, José Luiz Rozatto Fernandez, por me ajudar especialmente nessa monografia com o seu empenho de ver seu filho se formando.

Agradecimento em especial para duas pessoas que estiveram sempre ao meu lado. Quero que seu caminho seja iluminado com brilho forte feito pelo sol do amanhecer, vamos tocar a vida com cuidado não quero ver nada de ruim acontecer.

E finalmente agradeço a todos que estavam me acompanhando nessa jornada nesses últimos meses e que sentiram a minha falta nas atividades de companheirismo e brincadeiras.

Sumário

1 INTRODUÇÃO 14
1.1 Estrutura do Trabalho 15
2 O INTRUSO E A INTRUSÃO 16
2.1 O intruso 16
2.1.1 Tipos de intruso 17
2.2 A intrusão 18
2.2.1 Método de operação do atacante 20
2.2.1.1 Negação de serviço (DoS) 20
2.2.1.2 Sniffing 23
2.2.1.3 Engenharia Social 24
2.2.1.4 Spoofing 25
2.2.1.5 Cavalo de Tróia 27
2.3 Crescimento dos Ataques 28
3 A ANÁLISE FORENSE 31
3.1 Análise Forense Computacional 31
3.2 Análise Física 32
3.3 Análise Lógica 33
4 METODOLOGIAS ESTUDADAS 34
4.1 Metodologia da Polícia Civil do Distrito Federal 34
4.1.1 Preservação do Sistema 35
4.1.1.1 Preservação de Sistemas Computacionais Ligados 36
4.1.1.2 Preservação de Sistemas Computacionais Desligados 37
4.1.2 Coleta de Evidências 38
4.1.3 Análise de evidências 39
4.1.3.1 Análise ao Vivo 39

4.1.3.2 Análise *Post Mortem* 40

4.1.4 Reconstrução dos Eventos 42

4.2 Metodologia do Departamento de Justiça norte americano (*U.S Departament of Justice)* 43

4.2.1 Segurança e Avaliação do Local do Crime 44

4.2.1.1 Documentação do Local do Crime 45

4.2.2 Preservação do Sistema 45

4.2.2.1 Preservação em Ambiente de Complexidade Baixa 45

4.2.2.2 Preservação em Ambiente de Complexidade Alta 46

4.2.3 Análise das Evidências 47

4.2.3.1 Análise dos Dados Extraídos 48

4.2.3.2 Análise *Timeframe* 48

4.2.3.3 Análise em Dados Ocultos 48

4.2.3.4 Análise em Arquivos e Aplicação 49

4.2.3.5 Análise Propriedade e Posse 49

4.2.4 Armazenamento 50

4.3 Análise das metodologias 52

5 METODOLOGIA PROPOSTA 55

5.1 Preservação do sistema 56

5.2 Coleta das informações 57

5.2.1 Imagem do Disco 59

5.2.2 Gerando a imagem 61

5.3 Análise das evidências 63

5.3.1 Memória Principal do Sistema 64

5.3.2 Tráfego de rede 66

5.3.3 Processos em execução 68

5.3.4 Interface e conexões de rede 70

5.3.5 Módulos de *Kernel* 71
5.3.6 Dispositivos de armazenagem secundária 72
5.3.6.1 Analisando sistema de arquivos 72
5.3.6.2 Arquivos de configuração 73
5.3.6.3 Diretórios temporários 73
5.3.6.4 Diretório de arquivos de dispositivos 74
5.3.6.5 Arquivos e diretórios escondidos ou não usuais 74
5.3.6.6 Executáveis e bibliotecas 75
5.3.6.7 Arquivos de *log* 76
5.4 Documentação 78
6 ESTUDO DE CASO 81
6.1 Ferramenta utilizada 81
6.2 Objeto investigado 82
6.3 Utilização da metodologia proposta 83
6.4 Resultados obtidos 87
7 CONCLUSÃO 89
7.1 Trabalhos futuros 90
REFERÊNCIAS 91

Índice de Tabelas

Tabela 1 – Relacionamento das metodologias estudadas 54
Tabela 2 – Comando PsList.exe, relacionamento dos parâmetros 68
Tabela 3 – Informações contidas em sistema de arquivos 73
Tabela 4 – Principais arquivos de log, sistemas GNU/Linux. 76

Índice de Figuras

Figura 1 – Ataque DoS 21
Figura 2 - Ataque DDoS 21
Figura 3 – Ataque Smurf..... 23
Figura 4 – Ataque Sniffing, captura de dados..... 24
Figura 5 – Troca de mensagens SYN ACK 26
Figura 6 – Ataque Spoofing 26
Figura 7 - Esquema trojan 27
Figura 8 – Dump de memória 65
Figura 9 – Captura do trafego de rede pelo Wireshark..... 67
Figura 10 – Ferramenta PsList, utilizando argumento -M 69
Figura 11 – Comando NETSTAT, utilizando o argumento -AN 71
Figura 12 – Comando cat, utilizando o argumento -A..... 75
Figura 13 – Diretivas de segurança, sistema Windows 77
Figura 14 – Partições do objeto investigado..... 82
Figura 15 – Resumo da geração da imagem..... 84
Figura 16 – Analisando o sistema de arquivos 85
Figura 17 – Setor de Boot do NTFS. 87

Índice de Fluxogramas

Fluxograma 1 – Metodologia PCDF 35
Fluxograma 2 – Estado inicial do sistema, ligado 36
Fluxograma 3 – Estado inicial do sistema, desligado 37
Fluxograma 4 – Metodologia proposta 56

Índice de Gráficos

Gráfico 1 – Total de incidentes reportados ao CERT 28
Gráfico 2 – Gráfico de Ataque Acumulado, reportados ao CERT..... 29
Gráfico 3 – Tipos de Ataque Acumulado, reportados ao CERT 29
Gráfico 4 – Origem de Ataques, reportados ao CERT 30
Gráfico 5 – Softwares instalados no Objeto investigado..... 83

1 INTRODUÇÃO

A Tecnologia da Informação (T.I) avançou rapidamente em pouco tempo. As instituições estão utilizando esses recursos tecnológicos para melhorar as operações empresarias e indiretamente o mercado. Por meio dessas tecnologias é possível realizar, por exemplo, pagamentos bancários e a venda e compra de objetos e mantimentos, de forma digital. Por outro lado, uma vasta quantidade de dados sensíveis e confidenciais pode cair em mãos maliciosas aumentando o número de criminosos que utilizam computadores ou servidores de rede em suas atividades ilícitas.

A importância do uso dos computadores na vida cotidiana é inegável, mas, por outro lado, pode prover meios para a consumação de um crime virtual, como obtenção de informação sigilosa e confidencial de sistema empresarial ou pessoal.

O combate aos crimes relacionados à tecnologia da informação requer o desenvolvimento de novas táticas e técnicas que visem obter evidências digitais armazenadas em um computador.

Toda investigação, mesmo que não seja para iniciar um processo criminal, deve considerar como prática comum o uso de metodologias e protocolos que garantam sua possível aceitação em uma corte judicial [WARREN; KRUSE, 2002]. Além disso, conduzir o caso com a formalidade de um processo criminal ajuda a desenvolver bons hábitos de investigação.

Sob essa perspectiva foi desenvolvida, neste trabalho, uma metodologia para a investigação forense de intrusões digitais em sistemas computacionais, visando fornecer procedimentos válidos e confiáveis que possibilitam adquirir evidências digitais em atividades ilícitas. A metodologia proposta tem por base aquelas utilizadas pela Polícia Civil do Distrito Federal e pelo Departamento de Justiça norte americano (*U.S Departament of Justice*), sendo estruturada por procedimentos de preservação do sistema, coleta de dados, análise forense e documentação.

1.1 Estrutura do Trabalho

Além do capítulo introdutório e conclusão, o trabalho está estruturado em mais cinco capítulos, assim descritos:

- Capítulo 2 – O intruso e a Intrusão: apresenta os conceitos teóricos, os diversos tipos de intruso e alguns tipos de intrusão realizada pelo intruso;
- Capítulo 3 – A Análise Forense: conceitua a análise forense computacional (análise física e lógica);
- Capítulo 4 – Metodologias Estudadas: apresenta as duas metodologias que serviram de base para a metodologia proposta neste estudo ([SHIMABUKO, 2009]; [CASEY, 2000]);
- Capítulo 5 – Metodologia Proposta: apresenta a metodologia forense desenvolvida neste trabalho, a qual integra os pontos fortes das duas metodologias pesquisadas e adéquam os pontos fracos das mesmas;
- Capítulo 6 – Estudo de Caso: apresenta os resultados da análise realizada em um disco rígido de um computador de uso pessoal aplicando-se a metodologia proposta;

2 O INTRUSO E A INTRUSÃO

> Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. Se você se conhece, mas não conhece o inimigo, para cada vitória ganha sofrerá também uma derrota. Se você não conhece nem a si mesmo perderá todas as batalhas (Sun Tzu – A Arte da Guerra, 1983).

2.1 O intruso

Manipular dados sem permissão, obter acesso indevido ao meio eletrônico ou sistema informatizado, introduzir vírus em computadores, clonar celular e falsificar cartão de crédito, entre outros atos, são ações de um intruso.

Com a popularização dos microcomputadores o termo *hacker* tem sido designado, atualmente, como o intruso virtual que tenta obter informações confidenciais através da espionagem quebrando a segurança de redes.

Neste estudo, o uso do termo intruso será considerado por suas ações.

Para os administradores de sistema, uma intrusão ou tentativa de intrusão só é considerada quando existe uma quantificação mínima aceitável de um dado comportamento. Que personaliza um limite aceitável de erros que não pode ser considerado como ataques, distinguindo-se assim o intruso de uma falha de sistema.

Segundo Oliveira (1999) existe dois tipos de intruso: interno e externo. Para contextualizar o que seja um ataque interno ou externo devemos esclarecer o que seja um ambiente interno e externo. O primeiro se refere ao local aonde o administrador do parque tecnológico tem acesso físico e lógico, enquanto o segundo é o local aonde esse não tem acesso ao parque tecnológico tanto na parte física quanto na lógica.

Assim, as intrusões externas consistem em ataques originados do ambiente externos, por exemplo, um ataque oriundo da maior rede mundial, a internet. E as intrusões internas são ataques originados do ambiente interno, como ataques internos a corporação por um funcionário tentando obter um dado confidencial da empresa.

À medida que a complexidade dos programas vai evoluindo, novas vulnerabilidades vão aparecendo assim como novas formas de invadir são desenvolvidas. Com o mínimo de conhecimento em redes de computadores e

consultas na internet qualquer pessoa pode obter gratuitamente uma ferramenta que permite invadir um sistema computacional.

2.1.1 Tipos de intruso

Existe uma hierarquia imposta a quem decide entrar na jornada do mundo de intrusões. Os intrusos podem agir sozinhos ou formarem grupos, comumente chamados de “clãs”.

A classificação desses intrusos é um folclore no meio dos *hackers* e dependendo do “clã” que o intruso pertença essa classificação pode ser uma regra ou apenas um tratamento informal. Segundo [ULBRICH; VALLE, 2004] podem ser classificados, como:

- Newbie: Intruso iniciante, geralmente estudando e colhendo informações para realizar sua primeira intrusão;
- Luser: Intruso que objetiva ter o conhecimento mínimo e necessário para operar o computador e realizar sua intrusão o mais rápido possível. Ao contrário do Newbie, não se interessa por aprender nada. A própria formação da palavra, de origem inglesa, reflete isso: *user* (usuário) e *loser (perdedor)*. Geralmente os hackers utilizam esses intrusos como vítimas intermediárias para chegarem a um objetivo maior;
- Lamer: Intrusos comuns que aprendem a utilizar *softwares* básicos para realizarem suas intrusões. Geralmente os Lamers utilizam basicamente três tipos de ferramentas: *scan*, *exploit* e *trojan*;
- Wannabe: Intruso que almeja ser *hacker*, podendo ser uma pessoa que já se aprimorou bastante ou que pretenda entrar no mundo do “*hackerismo*”, não tendo idéia do que se trata esse novo mundo. Essa palavra foi utilizada primeiramente nos anos 80 tendo como referência os fãs da Madonna que se vestiam e agiam segundo os costumes da cantora.
- Larval *Stage*: Indivíduo que se encontra no estágio larval ou Spawn (etapa anterior para se tornar um hacker), que pode durar de seis meses a dois anos. Para se atingir essa etapa o indivíduo deve possuir um alto nível de conhecimento em programação;
- Hacker: Indivíduo que se dedica a explorar detalhe de sistemas programáveis, sendo um profundo conhecedor de computadores, geralmente utiliza sistemas

operacionais como *Unix* e *Windows* e programas em linguagens como *Assembly*, *C* entre outras. Os hackers possuem um rígido código de ética no qual nunca usam os seus conhecimentos para o "mal", mesmo que a noção da palavra "bem" seja contra a lei. O termo *hacker*, de origem inglesa, derivada do verbo *hack* (cortar, cavar) que originalmente significava alguém que fabricava móveis utilizando um machado.

- Cracker: Indivíduo que utiliza dos seus conhecimentos técnicos para "quebrar" todo e qualquer tipo de barreira em sistemas de segurança de programas ou para acessar de forma ilícita informações armazenadas em computadores, que na maioria das vezes são conteúdos confidenciais. De modo simplista, o *cracker* é o "*hacker do mal"*.
- Phreaker: é o *cracker* dos sistemas telefônicos com alto nível de conhecimento nas áreas de eletrônica e telefonia, podendo fazer chamadas telefônicas de qualquer lugar sem pagar por elas.
- *Card*er: Intruso especialista em cartões de créditos, com que conhecimento para adquiri-los através de uma em *sites* que os utilizam, de modo a clonar os cartões e gerar números falsos que passam pelas validações dos sites;
- *War Driver*: Intruso comparado aos *crackers* e *war driver*, que aproveitam as inúmeras vulnerabilidades das redes sem fios, *wireless,* e se conectam a elas. Esta classificação de intruso é recente.

Para a obtenção de dados relevantes aos intrusos, é preciso que haja uma intrusão no sistema visado por eles. De certo modo, os intrusos se utilizam de técnicas para conseguir burlar as seguranças de rede.

2.2 A intrusão

A intrusão pode ser entendida como qualquer ação ou conjunto de ações que tenham como objetivo denegrir a integridade, confiabilidade e disponibilidade de um sistema, ou seja, qualquer violação de segurança de um sistema computacional.

Novas formas de denegrir e invadir um sistema computacional são desenvolvidos diariamente.

Com o mínimo de conhecimento, na área de Tecnologia de Informação, indivíduos adquirem ferramentas gratuitas da Internet que podem ser utilizadas para invadir e provocar algum dano em sistemas computacionais.

Esse procedimento tem sido classificado, por muitos países, como um risco à segurança nacional, e por isso estimulando a realização de estudos que propiciem a compreensão deste e os métodos utilizados.

A intrusão a sistemas computacionais são motivadas por diversas finalidades, destacando [ULBRICH; VALLE, 2004]:

- Utilização do sistema para apropriação tendo por objetivo distinto disseminar ataques distribuídos;
- Obtenção de informações confidenciais dos sistemas, por exemplo, de números de cartões de crédito;
- Denegrir o sistema para promover algum tipo de estrago como, por exemplo, a pichação a sites;

A primeira linha de raciocínio de um *hacker* ou *cracker* é escolher seu alvo em potencialidade. Com seu alvo pré-estabelecido, o intruso começa a coletar dados sobre o sistema alvo com o intuito de identificar possíveis vulnerabilidades ou processos de rede disponíveis. Ao descobrir um ponto de entrada utiliza-se de métodos para a obtenção de senhas; caso contrário, usa a engenharia social para obter o ponto de entrada no sistema alvo. Após isso, realiza o comprometimento inicial do sistema. Nessa primeira intrusão, o sistema cria alardes caso esteja devidamente protegido, que costuma acontecer nos horários que não tenha um administrador presente. Esses alardes são criados na tentativa de adivinhar usuários e senhas para o sistema, essas tentativas geram registros de *logon* falhos.

Com todos os seus objetivos primordiais obtidos, ou seja, sucesso na intrusão e usuário com *logon* no sistema, a busca do intruso é por privilégios irrestritos do sistema (perfil de administrador ou *root*). Quando na intrusão o usuário não tem o privilégio irrestrito do sistema, o invasor estabelece a transferência de programas maliciosos, conhecidos como *exploits*, na tentativa de explorar as vulnerabilidades que possam ajudá-lo na obtenção do acesso com privilégios irrestritos, quando então começa a remover traços que comprovem sua intrusão utilizando programas como *rootkits* e *trojan hourses*, tornando-se “invisível”.

Com a “invisibilidade” perante o sistema alvo, o intruso instala outros programas, chamados *backdoors*, que facilitam o seu retorno e apaga os traços de sua intrusão. Na utilização desses programas o intruso retorna ao sistema alvo mais

discreto, que na fase inicial, e pode ser feito um inventário acerca dos dados da máquina invadida e possíveis alvos ao redor.

Para se apropriar do sistema alvo, o intruso pode utilizar alguns métodos ou tipos de ataque ao sistema para estabelecer o primeiro contato com o sistema alvo.

2.2.1 Método de operação do atacante

Com a popularização da Internet, a segurança da informação se tornou um assunto constante nas empresas. Cada empresa se conecta na Internet deixando seus dados expostos, gerando uma quantidade de dados que ao trafegarem na rede aumentam o interesse dos intrusos. Isso faz com que empresas e pessoas aumentem o interesse pela segurança da rede, propiciando o aparecimento de várias formas de ataques e conseqüentemente à defesa a essas invasões.

Para a aquisição de dados vitais do sistema alvo escolhido existem algumas técnicas, como:

2.2.1.1 Negação de serviço (DoS)

Esse ataque também é conhecido simplesmente como DoS (*Denial of Service*), e consiste em tentativas de impedir que usuários da máquina alvo utilizem um determinado serviço do sistema.

O DoS pode ser executado localmente ou remotamente, sendo necessário para o primeiro estar dentro da rede ou logado ao sistema. O ataque remoto não precisa que o invasor esteja logado no sistema alvo, visto que esse ataque funciona independente dos sistemas operacionais.

Esses ataques DoS consistem em aproveitar das vulnerabilidades e/ou falhas presentes no sistema alvo ou enviar um grande número de pacotes que esgotem algum recurso do sistema alvo, conforme ilustrado na Figura 1.

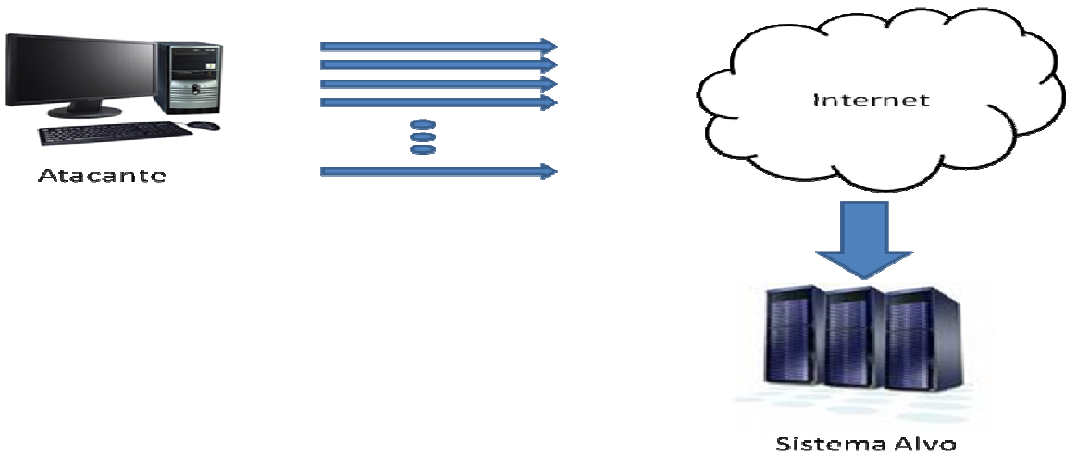


Figura 1 – Ataque DoS

Para se executar esse ataque é necessário uma máquina com capacidade de processamento e banda “poderosas”, capazes de gerar inúmeros pacotes que possam causar a interrupção do sistema alvo.

Outra forma de se executar esse ataque é através da negação de serviço distribuído ou DDoS (*Distributed Denial of Service*) que consiste de um grupo de máquinas, que juntas, enviam pacotes ao sistema alvo, causando a interrupção do alvo, conforme a Figura 2.

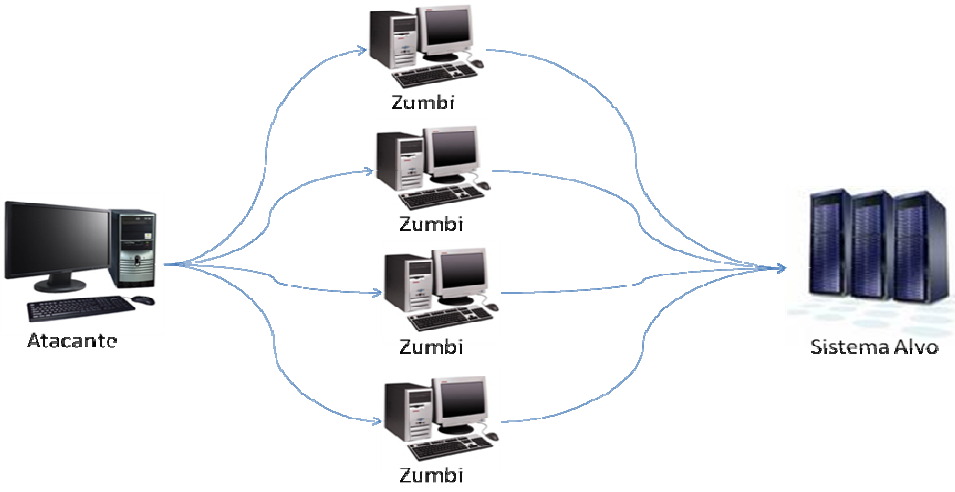


Figura 2 - Ataque DDoS

Embora qualquer forma de ataque DoS seja perigoso para o sistema alvo, a forma distribuída se torna um risco maior, justamente por se tratar de um ataque em

máquinas distintas que podem estar separadas geograficamente e não possuir uma relação entre si, somente que estão sob controle do invasor.

Os ataques de DoS pode ser classificados em:

- Ataque por inundação: é a inundação do tráfego da rede ocasionado por aberturas de conexões, sendo utilizado em serviços que necessitam de entrega confiável de dados;
- Ataque reflexivo: é uma variação do ataque de inundação, que exige a presença de um agente entre o atacante e a vítima. Esse agente espelha o tráfego de ataque em direção a vítima objetivando exaurir os recursos dessa com os recursos do agente;
- Ataque à infra-estrutura da rede: exigem grandes recursos de processamento e memória. Os recursos de DDoS de pequena escala não conseguem exaurir rapidamente os recursos para que os usuários tenham serviços negados. Outra forma desse ataque seria concentrar recursos em algum elemento vital de fornecimento de serviços, como consumir toda a banda passante [1] da vítima com o tráfego de ataque, ocasionando perdas de requisição na infra-estrutura da rede;
- Ataque de vulnerabilidade: tem por objetivo principal deixar a vítima inoperante. O intuito desse ataque é explorar por vulnerabilidades na implementação da pilha de protocolos ou da aplicação do sistema alvo;

Alguns subtipos de ataque por negação de serviço são: Smurf muito utilizado em servidores de divulgação, *broadcast*; *Sniffing*; Engenharia Social; *Spoofing* e Cavalo de Tróia;

2.2.1.1.1 Smurf

O ataque Smurf consiste na utilização dos servidores de divulgação, *broadcast* [2], para paralisar a rede. Um servidor de divulgação, ou servidor de *broadcast*, tem a capacidade de difundir uma mensagem a todas as máquinas presentes na rede.

O cenário do ataque consiste em se ter uma máquina fonte (máquina do atacante) que faz uma requisição a um ou vários servidores de *broadcast*

[1] É usada para especificar a quantidade de dados que podem ser enviados em um canal de comunicação.
[2] O processo que transmite informações à um conjunto de máquinas da mesma rede, com a característica que esses dados contenham a mesma informação.

falsificando o endereço para o qual o servidor deve responder, ou fornecendo um endereço de outra máquina orientada. O servidor de *broadcast* reflete o conjunto de dados a ser enviado à rede. Todas as máquinas que receberam o pedido do servidor enviam uma resposta. Por final o servidor de divulgação reflete as mensagens de respostas das máquinas para a máquina orientada, conforme ilustrado na Figura 3.

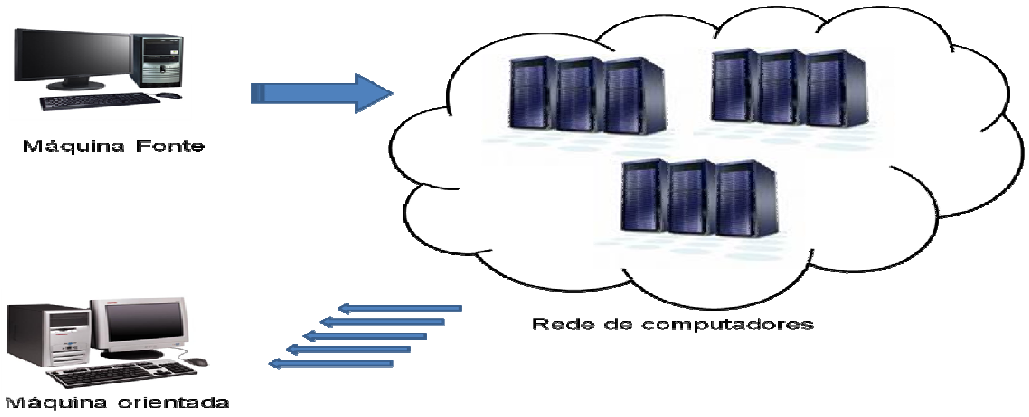


Figura 3 – Ataque Smurf

Com isso o trabalho do atacante é descobrir na rede servidores de divulgação e falsificar o endereço de resposta com o intuito de dirigir o conjunto de pacotes à máquina orientada.

2.2.1.2 Sniffing

É o processo no qual os intrusos capturam e analisam todo o conteúdo no tráfego da rede (Figura 4). As ferramentas utilizadas são chamadas de *Sniffer*, sendo usadas para monitorar, identificar e obter informações da rede. Esse processo é utilizado pelos *hackers* para obterem acesso às informações sigilosas que trafegam na rede.

Os *Sniffers* podem analisar somente um protocolo ou um conjunto, dependendo da funcionalidade e projeto do software. Os protocolos mais comuns para essa análise são:

- Ethernet padrão;
- TCP/IP;
- IPX;

- DECnet;

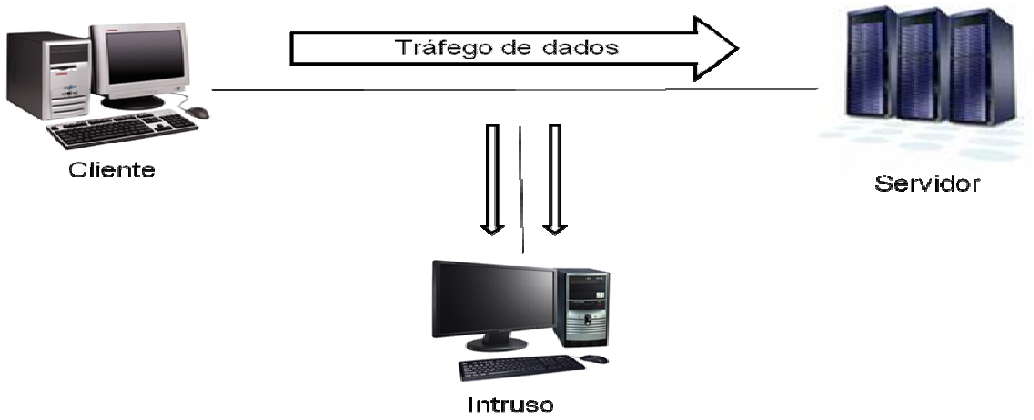


Figura 4 – Ataque Sniffing, captura de dados.

2.2.1.3 Engenharia Social

O termo engenharia social, à primeira vista, parece algo distante ao mundo *hacker*. Este tipo de ação busca informações vitais sobre uma determinada pessoa, empresa ou organização, utilizando-se de informações obtidas de pessoas próximas ao alvo ou do próprio quadro de funcionários de uma empresa ou organização. Em outras palavras, pode ser tida como “espionagem”, por utilizar táticas que vão de cartas e telefonemas, passando por pesquisa nos depósitos de lixo até uma abordagem pessoal.

As técnicas dessa metodologia necessitam de uma preparação psicológica profunda e contínua, pois o candidato a invasor deve estudar o comportamento diário do seu alvo.

Mesmo com grandes investimentos na área de segurança a maioria das empresas não está preparada para lidar com esse tipo de situação, cuja abordagem de ataque pode ser indireto ou direto. O primeiro consiste na utilização de ferramentas, como cavalos de tróia e imposturas como cartas para a obtenção das informações pessoais. O usuário, de quem o *hacker* extrai os dados, são apenas intermediários para a coleta de informações. O objetivo maior desse ataque não é atacar os usuários e sim a entidade a que eles pertencem. O segundo método é caracterizado pelo contato pessoal, geralmente feito por telefone ou pessoalmente, exigindo um planejamento detalhado. O invasor deve ser bem articulado e ter um

raciocínio rápido para encontrar saídas caso ocorra algum imprevisto no seu planejamento.

Em resumo, o invasor utiliza dois métodos na elaboração do ataque por engenharia social: a pesquisa e aquisição de material, por exemplo, lista de pagamento, aonde o *hacker* descobre o indivíduo que detém a informação necessária para executar a invasão e a impostura, no qual o *hacker* obtém as informações de outras pessoas como funcionários da mesma empresa, cliente ou fornecedor. De posse das informações inicia sua invasão.

Comportamentos como descuidos dos usuários e administradores de rede das empresas ou organizações facilitam a execução desse tipo de ataque. Mesmo empresas com sofisticado mecanismo de segurança pode deixar escapar alguma informação, basta uma informação óbvia apenas, para que o *hacker* prontamente se apodere desta e diminua o tempo utilizado na engenharia social.

2.2.1.4 Spoofing

É uma técnica, usada por *hackers*, de se fazer passar por um computador da rede para conseguir o acesso ao sistema alvo, ocasionando falsificação do endereço de origem.

Para entender o mecanismo dessa técnica é necessário conhecer o processo de autenticação dos protocolos TCP (*Transmission Control Protocol*) e IP (*Internet Protocol*), criados com o intuito de estabelecer a intercomunicação entre os computadores de uma rede.

O TCP tem como principal objetivo de intercomunicar aplicações de diferentes máquinas, sendo um protocolo da camada de transporte para trabalhar com mensagens de reconhecimento, especificação dos pacotes e mecanismos de segurança. O IP tem como principal atribuição transportar os datagramas de uma rede a outra.

Todo processo de autenticação da máquina pela rede começa na troca de mensagens entre o computador de origem e o destino, no qual o primeiro utiliza mensagens *SYN* para iniciar a conexão no destino. A máquina de destino confirma a mensagem *SYN* retornando uma mensagem *SYN-ACK* para a máquina de origem que recebe as mensagens completando a conexão e retorna a mensagem *ACK*.

Assim a conexão entre as duas máquinas é estabelecida e os dados entre essas podem ser trocados (Figura 5).

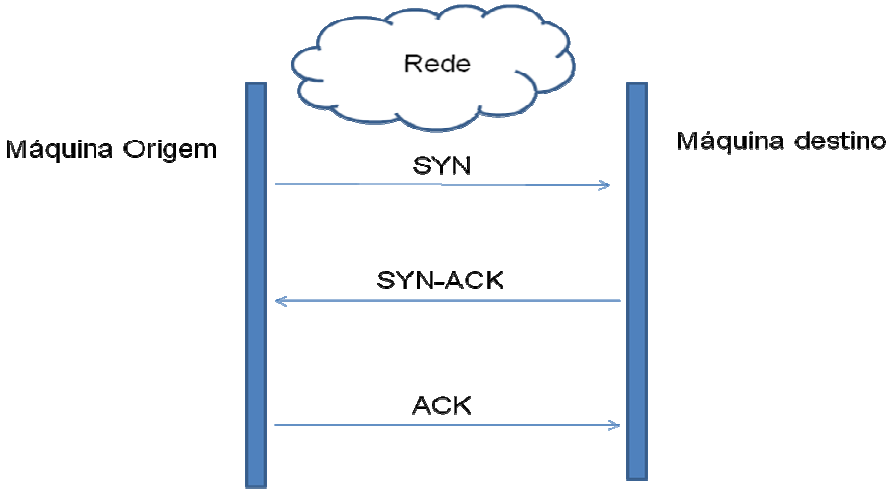


Figura 5 – Troca de mensagens SYN ACK

Para realizar o ataque o intruso pode optar por duas formas, falsificando o endereço de origem ou mantendo o número seqüencial com o destino. Essa última é a mais complicada de se aplicar, pois o destino configura o número seqüencial inicial e o intruso deve responder de forma correta a esse número, exigindo um ajuste correto do número seqüencial para que o intruso possa efetuar a sincronização com o destino e estabelecer uma conexão confiável (Figura 6).

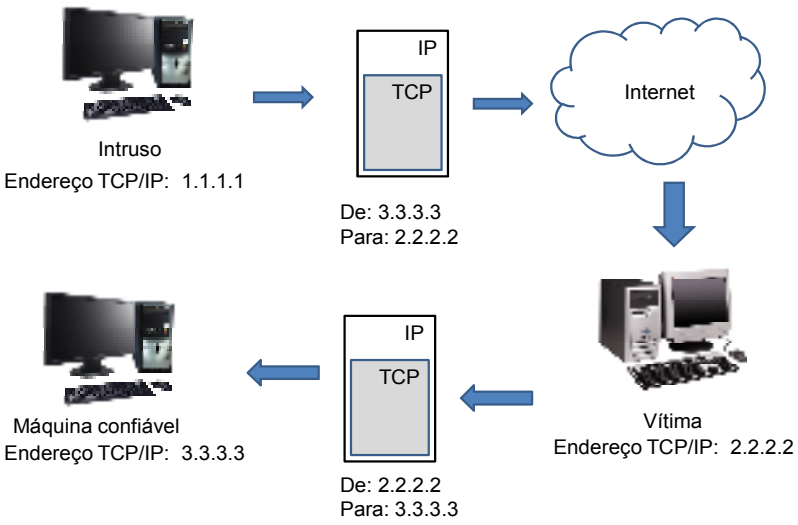


Figura 6 – Ataque Spoofing

2.2.1.5 Cavalo de Tróia

Cavalo de tróia, do inglês "*Trojan horse*", também conhecido como *trojans,* é outra forma do intruso estabelecer uma comunicação com o alvo em potencial, e consiste na utilização de programas maliciosos, com aparência inofensiva e atrativa, como pequenos aplicativos de jogos, fotos entre outros, que uma vez executados instalam na máquina alvo programas maliciosos (vírus, *worm*, *malware*[3]), normalmente são utilizados *backdoor* (utilitário que permite ao intruso acessar o computador infectado a qualquer hora) (Figura 7).

Diferentes dos vírus, os *trojans* não possuem instruções de auto-replicação, pois são autônomos (não precisando infectar outras máquinas) e não objetivam a própria disseminação, mas costumam permanecer indefinidamente na máquina hospedeira.

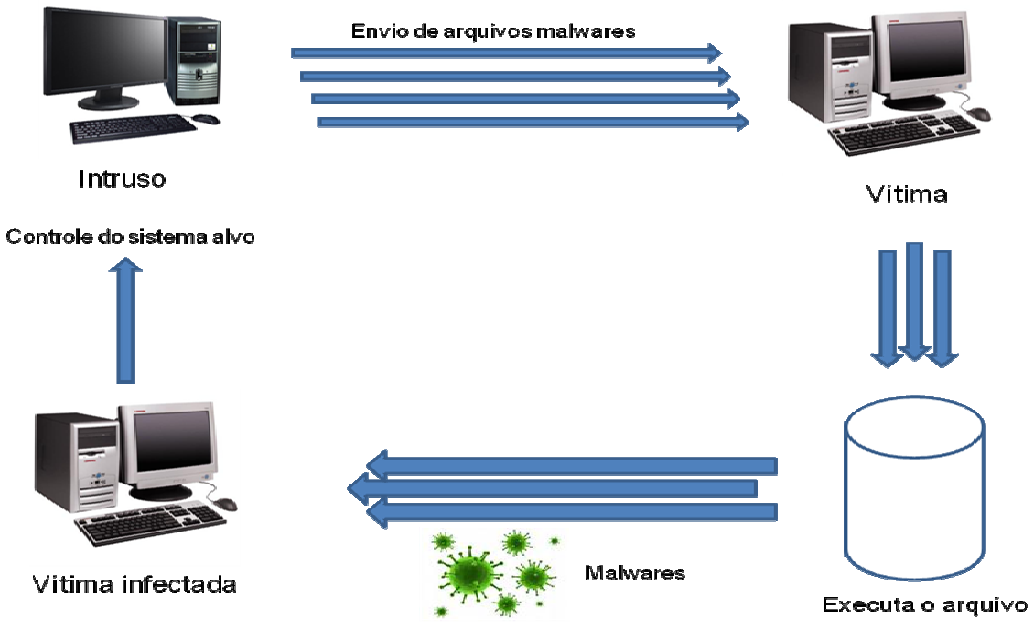


Figura 7 - Esquema trojan

Os *trojans* são aplicativos que aparentemente estão realizando uma tarefa inofensiva, mas na verdade estão infectando a máquina hospedeira. São ferramentas usadas por *crackers* para monitorar e controlar os alvos.

As funções do cavalo de tróia são [ULBRICH; VALLE, 2004]:

- Fornecer um *Shell* para o cliente com acesso irrestrito;

[3] Qualquer software desenvolvido para causar danos em outros computadores.

- Controlar todos os dispositivos de hardware da máquina;
- Gravar uma imagem da tela do computador invadido;
- Fazer exames da rede, podendo obter senhas e outras informações;
- Gravar um arquivo contendo informações sobre tudo o que foi teclado no micro;
- Possibilitar a abertura de janelas DOS remotamente;

Um problema comum com os cavalos de tróia tradicionais, como aplicativos externos ao sistema, é que são facilmente detectados por ferramentas de auditoria, mesmo quando camuflados no sistema com nomes insuspeitos entre os arquivos do sistema alvo.

2.3 Crescimento dos Ataques

No Brasil, os incidentes sobre ataques virtuais como fraude, invasão para obtenção de informações sigilosas entre outros são registrados pelo grupo de resposta a incidente de segurança na internet mantido pelo NIC (Núcleo de Informação e Coordenação do Ponto BR) do Centro de Estudos e Tratamento de Incidentes de Segurança no Brasil - CERT. De acordo com o Gráfico 1, observa-se que os incidentes tiveram um acréscimo de cerca de 72 vezes entre os anos de 1999 e 2008.

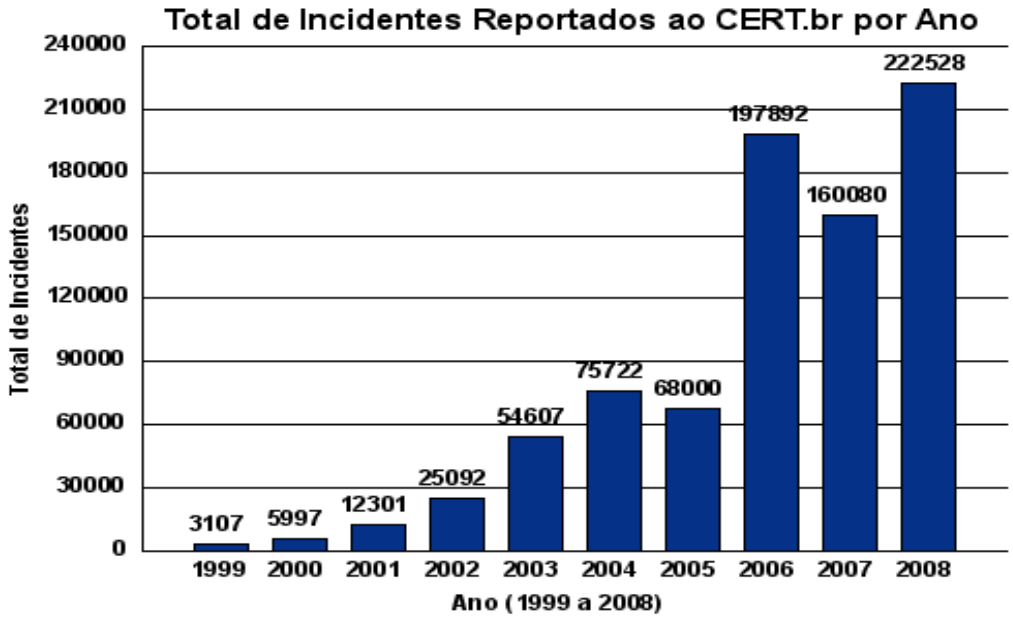


Gráfico 1 – Total de incidentes reportados ao CERT

(Fonte: www.cert.br)

Analisando os dados divulgados pelo CERT, observa-se que no período de janeiro a dezembro de 2008, os principais ataques registrados no Brasil foram à fraude (62,94%) e o *Scan* (19,69%), segundo os Gráficos 2 e 3.

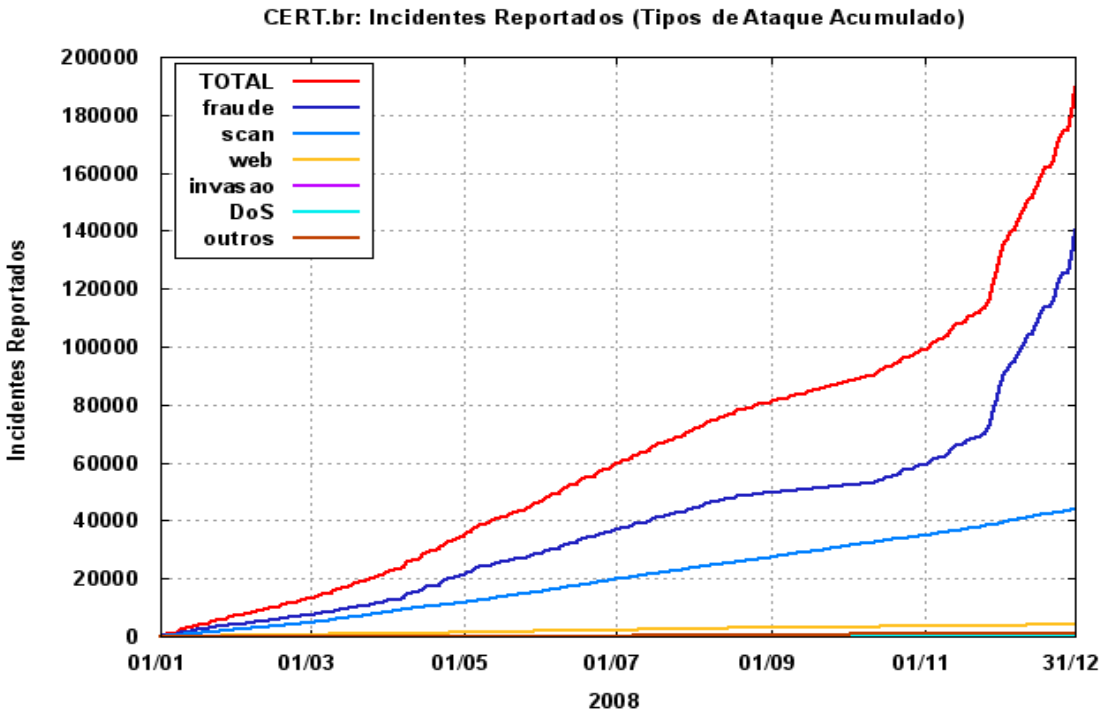


Gráfico 2 – Gráfico de Ataque Acumulado, reportados ao CERT

(Fonte: www.cert.br)

Gráfico 3 – Tipos de Ataque Acumulado, reportados ao CERT

(Fonte: www.cert.br)

Quanto à origem dos ataques, observa-se que o Brasil é o país mais prevalente (68,43%) (Gráfico 4).

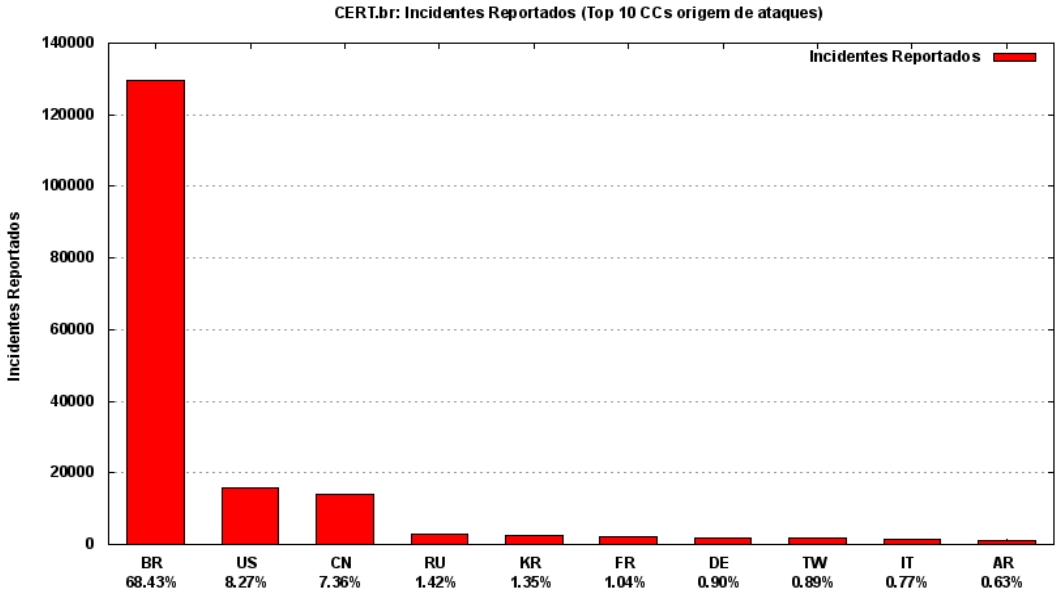


Gráfico 4 – Origem de Ataques, reportados ao CERT

(Fonte: www.cert.br)

A melhor ferramenta de combate aos incidentes é a análise forense que possibilita aos administradores dos sistemas identificar e coletar informações, reconhecer as evidências e documentar o incidente.

3 A ANÁLISE FORENSE

3.1 Análise Forense Computacional

De acordo com J. Thorton [THORTON, 1997], a ciência forense é exercida em favor da lei para uma justa resolução de um conflito. Em outras palavras, seria aquela que se baseia em procedimentos científicos para obtenção de informações que possam ser úteis durante uma disputa judicial. Este termo é muito comum no meio policial e até poucos anos atrás não se tinha qualquer relação com o meio computacional.

De acordo com o Manual de Patologia Forense do Colégio de Patologistas Americanos (1990), a ciência forense é "*a aplicação de princípios das ciências físicas ao direito na busca da verdade em questões cíveis, criminais e de comportamento social para que não se cometam injustiças contra qualquer membro da sociedade*".

A forense computacional foi criada em função dessa nova vertente de crime para apoiar as instituições legais[4], na aplicação da justiça. Sendo a ciência que compreende a aquisição, preservação, identificação, restauração, análise e documentação de evidências computacionais [NOBLETT, 2000], através da:

- Coletas de informações: na coleta evidências para análise existem dois perigos: perda e alteração [Atílio, 2003]. Se cuidados necessários não forem tomados, dados relevantes a análise podem ser sobrescritos e/ou apagados;
- Reconhecimento das evidências: caracterização da ameaça e seus efeitos nos sistemas alvos;
- Coleta, restauração, documentação e preservação das evidências encontradas;
- Correlação das evidências: retomada das atividades em andamento antes do incidente ocorrer. E restauração de dados se necessário
- Reconstrução dos eventos: correlacionamento de logs, recuperação de arquivos apagados, analise de artefatos encontrados no sistema;

O processo de análise, como em outras disciplinas forenses, deve ser metódico e seguir procedimentos previamente testados e validados cientificamente,

[4] Polícia, Departamento de Segurança Civil e Militar.

de forma que todos os resultados obtidos na fase de análise sejam passíveis de reprodução.

A análise forense pode ser dividida em duas partes: a análise física e a lógica [Freitas, 2003].

3.2 Análise Física

A análise física é a pesquisa de seqüências e a extração dos dados, onde são investigados os dados brutos do equipamento de armazenamento. Em alguns casos, a análise forense inicia-se a partir dessa investigação, quando o objeto de análise é o conteúdo de um disco rígido desconhecido. Para tal, deve-se manter o objeto de estudo intacto, utilizando-se para isso *softwares* de criação de imagens que criam uma cópia idêntica ao do objeto de estudo, fixando as provas do sistema. Os dados podem ser investigados e analisados através dos seguintes processos:

- Pesquisa de seqüência: é feito uma pesquisa de seqüências de byte em todo sistema, retornando o conteúdo da pesquisa de seqüências e o deslocamento de byte do inicio do arquivo;
- Busca e Extração: é a pesquisa mais especializada de seqüências, onde se analisa uma evidência em busca de cabeçalhos dos tipos de arquivos, de acordo com o tipo que estiver sendo analisado;
- Extração de Espaços Subaproveitados e Livre de Arquivos: é a extração do espaço dos resíduos dos sistemas que são classificados de resíduos livre[5] e resíduos subaproveitados[6], através de uma ferramenta que distingue a estrutura particular desses sistemas de arquivos.

Todos esses processos são realizados nas evidências ou copias restauradas.

As pesquisas de seqüências produzem listas de dados, que serão úteis em fases posteriores, algumas dessas informações são:

- As URL's encontradas nas evidências;
- Endereços de e-mail encontrado no dispositivo de armazenamento;
- Entre outros;

[5] Qualquer dado encontrado no disco rígido que não esteja alocado em um arquivo.
[6] São dados escritos nos discos rígidos em blocos, no qual o tamanho da escrita seja menor que o pré-estabelecido pelo sistema operacional.

3.3 Análise Lógica

Análise lógica consiste na investigação dos arquivos das partições. O sistema de arquivos é analisado percorrendo-se a árvore de diretórios do objeto de estudo, de forma que no decorrer da análise o conteúdo de cada arquivo lógico é pesquisado.

Neste estágio o perito responsável pela investigação lógica dos dados precisa estar ciente de todos os procedimentos tomados na cópia restaurada, evitando erros de manipulação das provas, bastante comuns nesta fase. Seguindo assim o objetivo primordial de preservação e proteção das evidências encontradas contra alterações oriundas de um meio externo.

A restauração da imagem, normalmente, não é documentada, nem disponível ao público e não pode ser verificada. Essa imagem deve ser preservada e protegida geralmente montada em um sistema de arquivos somente leitura.

4 METODOLOGIAS ESTUDADAS

Este capítulo aborda as metodologias forenses utilizadas pela Polícia Civil do Distrito Federal (PCDF) e pelo Departamento de Justiça norte americano (*U.S Departament of Justice)*.

Segundo Aidil Barros e Neide Lehfeld (2000), no livro Fundamentos de Metodologia Cientifica, metodologia é “estudar e avaliar os vários métodos disponíveis, identificando suas limitações ou não em nível das implicações de suas utilizações”.

A metodologia avalia e examina as técnicas de pesquisa, alem da geração de novos métodos que conduzem à captação e processamento de informações com vistas à resolução de problemas de investigação [BARROS; LEHFELD, 2000].

Portanto, para se obter evidências digitais de uso forense é necessário adotar um conjunto de procedimentos e métodos (metodologia) que garantam sua legitimidade. A metodologia não procura soluções, mas escolhe as maneiras de encontrá-las, integrando os conhecimentos a respeitos dos métodos e vigor nas diferentes disciplinas cientificas ou filosóficas [BARROS; LEHFELD, 2000], tendo o interesse pelo estudo, descrição e análise dos métodos e esclarecimentos do objetivo.

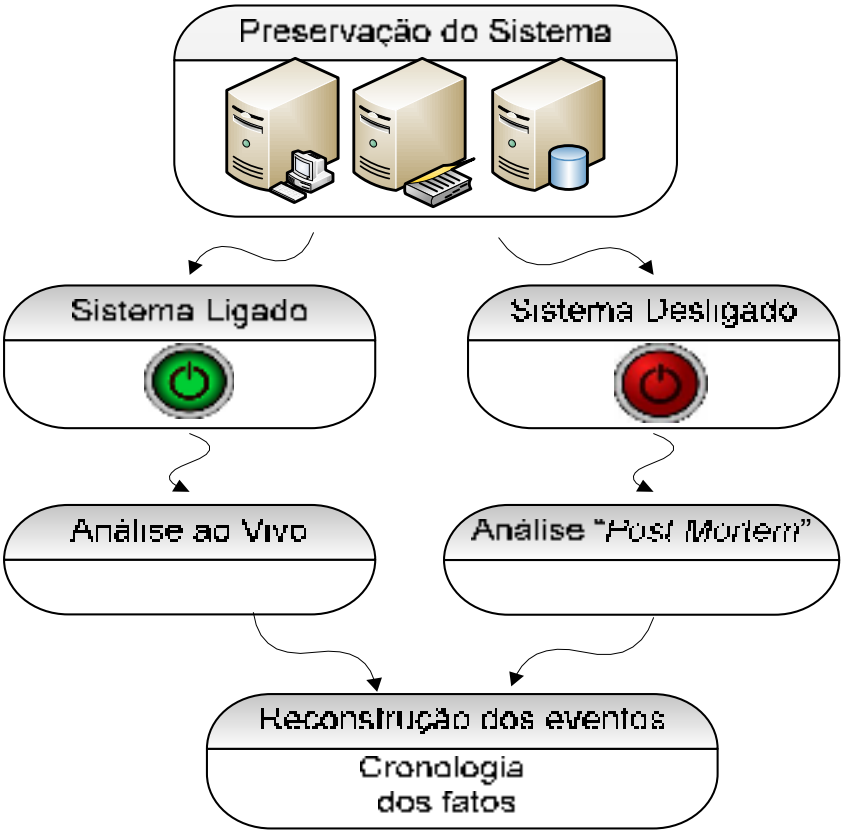
As informações relativas à metodologia utilizada pela PCDF foram obtidas nas diversas reuniões realizadas com os peritos criminais e pelo questionário enviado a esses. Os arquivos do *U.S Departament of Justice* foram obtidos nas reuniões acima referidas.

4.1 Metodologia da Polícia Civil do Distrito Federal

Com o crescimento de crimes cibernéticos, as autoridades responsáveis se adéquam com novas formas de criminalidade. Visando uma forma prática e metódica, a Polícia Civil do Distrito Federal (PCDF), concretizou uma metodologia para a investigação digital que consiste nos seguintes pontos seqüenciados (Fluxograma 1):

- Preservação do sistema: cuidado com o estado inicial do sistema, cuja preservação do sistema é essencial;
- Coleta de evidências: extração das evidências digitais, após o procedimento acima;

- Análise de evidências: análise das evidências digitais, possibilitando o investigador incriminar judicialmente o intruso;



Fluxograma 1 – Metodologia PCDF

4.1.1 Preservação do Sistema

> O artigo 169 Código de Processo Penal, [BRASIL, 1941]: *"Art 169. Para o efeito de exame do local onde houver sido praticada a infração, a autoridade providenciará imediatamente para que não se altere o estado das coisas até a chegada dos peritos, que poderão instruir seus laudos com fotografias, desenhos ou esquemas elucidativos.*
> *Parágrafo único. "Os peritos registrarão, no laudo, as alterações do estado das coisas e discutirão, no relatório, as conseqüências dessas alterações na dinâmica dos fatos."*

O responsável pela cena da infração, contendo sistemas ligados, deve fazer uma análise ao vivo ou desligar os equipamentos. Numa análise ao vivo, realizada com o sistema ligado, deve-se ter o cuidado de preservar a memória principal (RAM), que por sua vez pode ser a única evidência digital útil. O desligamento de

um sistema pode ser executado pelo sistema operacional, de modo ordenado; alternativamente, pode ser de súbito, cortando o fornecimento da energia como botão desligar ou desconectando o cabo de alimentação elétrica [SHIMABUKO, 2009].

Segundo Shimabuko (2009), é importante em qualquer dos procedimentos adotados que todos os passos realizados sejam devidamente documentados, pois se alguma decisão incorreta for adotada, a documentação permitirá a avaliação dos prejuízos para a investigação. Além disso, equipamentos eletrônicos podem conter vestígios físicos, tais como digitais ou resíduos orgânicos (sangue, cabelo e outros).

4.1.1.1 Preservação de Sistemas Computacionais Ligados

Segundo Shimabuko (2009), a maneira correta de lidar com sistemas computacionais ligados pode ser expresso, conforme o fluxograma 2.

Fluxograma 2 – Estado inicial do sistema, ligado

A primeira ação a ser tomada diante de um sistema ligado, se possível, fotografar a imagem que aparece no monitor. O Departamento de Justiça norte

americano acrescenta que todas as ações e quaisquer mudanças, identificadas pelo perito, no monitor, impressora e/ou outros periféricos devem ser anotadas.

O responsável pela análise deve realizar o desligamento súbito do sistema, quando houver indícios de atividades em que os dados estão sendo alterados, apagados e/ou algum processo destrutivo do sistema for detectado.

Apesar do Departamento de Justiça norte americano recomendar a retirada do cabo de energia, independente do estado de energia que o sistema se encontre, assim como também a bateria em computadores móveis, o desligamento súbito do sistema não é recomendado quando estiver visível no monitor dados de potencial valor à investigação, tais como, conversação em sala de chats, documentos de texto aberto e armazenamento remoto de dados entre outras evidências. Essas informações devem ser capturadas.

4.1.1.2 Preservação de Sistemas Computacionais Desligados

Segundo Shimabuko (2009), a maneira correta de lidar com sistemas computacionais desligados, ocorre conforme o Fluxograma 3.

Fluxograma 3 – Estado inicial do sistema, desligado

A primeira ação a ser tomada é manter o estado inicial do sistema, sendo que em hipótese alguma deve ser ligado o sistema. Tal procedimento evita que dados preciosos à investigação não se danifiquem. Segundo o Departamento de Justiça

norte americano deve ser anotado o estado inicial do sistema com o status de “off”, desligado.

O próximo passo do Fluxograma 3 é documentar e fotografar o equipamento com os periféricos (cabos, unidades removíveis e outros), assim como verificar e documentar possíveis unidades removíveis junto ao equipamento e lacrar as unidades removíveis. Deve-se também verificar se existe alguma conectividade com a linha telefônica, em caso positivo, tentar identificar o número do telefone, segundo o Departamento de Justiça norte americano deve ser verificado.

Os dispositivos eletro-eletrônicos devem ser manuseados com cuidado, pois dados armazenados nesses dispositivos podem ser alterados ou apagados por meios externos quando expostos a campos eletromagnéticos, transmissores de ondas magnéticas e outros dispositivos.

4.1.2 Coleta de Evidências

A preservação do sistema e a busca de evidências são, às vezes, potencialmente excludentes. Assim como ocorre com amostras físicas cuja análise pode provocar sua destruição, algumas evidências digitais somente podem ser obtidas com o sistema ligado (análise ao vivo ou *live analysis*), o que eventualmente as altera ou destrói [SHIMABUKO, 2009].

Em um sistema ligado, qualquer coleta de evidências poderá acarretar alterações na estrutura do gerenciamento de memória e tabela de processos.

Para Shimabuko (2009) uma análise ao vivo pode ser imprescindível para a coleta dessas informações. O simples ato de desligar o computador pode ocasionar a perda de informações como conexão de rede, processos em execução e a identificação de usuários que estejam acessando a máquina entre outras informações.

Para uma análise ao vivo é importante identificar qual conjunto de ferramentas a utilizar [SHIMABUKO, 2009]. Por exemplo, num sistema suspeito no qual suas bibliotecas e ferramentas nativas estejam comprometidas, as informações coletadas poderão estar incorretas, sendo aconselhável que as ferramentas utilizadas sejam compiladas estaticamente, executando-as a partir de uma mídia confiável.

Outra forma para a obtenção de evidências é a análise *post mortem*, que possibilita a análise de dados com um mínimo de alteração, sendo os procedimentos efetuados sobre meios de armazenamento permanente, por exemplo, um disco rígido.

4.1.3 Análise de evidências

É realizada pela Polícia Civil do Distrito Federal tanto a análise ao vivo quanto a análise *post mortem*.

4.1.3.1 Análise ao Vivo

Segundo Keith Jones e Curtis Rose (colocar ano da referência), os dados coletados durante uma análise ao vivo consistem em dois subconjuntos principais: dados voláteis e não voláteis. Os primeiros são aqueles que estão apenas em memória RAM e serão perdidos com o desligamento do sistema, e os segundos são dados que podem permanecer no sistema durante longos períodos de tempo, sendo recuperados mesmo que o sistema seja desligado, a exemplo de conteúdo de arquivos e *logs* do sistema.

O acesso aos dados não voláteis é difícil devido [SHIMABUKO, 2009]:

- Formatos difíceis de analisar, como registro de ocorrências (logs) do Windows;
- Dados criptografados;
- Dados armazenados em dispositivos remotos via rede, cujo acesso é perdido com o desligamento do sistema ou a desconexão da rede;

Alguns dados voláteis de importância na investigação foram obtidos através de comandos executados nos *Shell* dos sistemas operacionais, no sistema Windows na versão Windows XP *Service Pack* 3 e o software PsTools [SYSTERNALS,___] [JONES; ROSE, 2006]. Por exemplo:

- Data e Hora - utilizando os comandos date /t (obtenção da data) e time /t (obtenção do horário);
- Conexões de rede aberta - utilizando o comando *netstat –n*, esse comando informa às conexões que estão em ativas;

- Portas e respectivos serviços TCP e UDP abertos- utilizando o comando *netstat –abn;*
- Tabela de nome *NetBIOS*;
- Usuários com sessões abertas;
- Tabela de roteamento IP. O comando *netstat –r* mostra a tabela de roteamento IP;
- Processos e serviços em execução;
- Tarefas agendadas;
- Arquivos abertos;
- *Dumps* de memória;

Segundo Keith Jones e Curtis Rose (2006) alguns dados não voláteis são mais facilmente obtidos com o sistema ligado, por exemplo:

- Versão e correção do sistema operacional;
- Aplicativos instalados e dados de registro;
- Registro de ocorrência em formato legível;
- Data e hora do sistema;
- Contas de usuários;
- Arquivos suspeitos;

4.1.3.2 Análise *Post Mortem*

É realizada, basicamente, em procedimentos efetuados sobre meios de armazenamento permanente, como disco rígidos, em duas etapas. A primeira etapa consiste na geração de imagem de mídia para a preservação da evidência digital e a segunda na pesquisa e recuperação de dados em sistemas de arquivos [SHIMABUKO, 2009].

Devem ser feitas pelo menos duas cópias da mídia original em análise [VACCA, 2005], sendo uma das cópias lacrada na presença do responsável pelo material (dono) e guardada em local seguro, podendo ser aberto somente sob determinação judicial e a segunda seria utilizada para a pesquisa e recuperação de dados. Para Shimabuko (2009), *por falta de recursos (tanto para efetuar diversas cópias como para armazenar objetos), no Brasil basta apenas uma cópia, armazenado-se a mídia original para eventual contraprova*.

No procedimento de geração de cópias das mídias dois requisitos fundamentais devem ser observados [SHIMABUKO, 2009]:

- Assegurar a geração da imagem fiel ao original, algumas vezes essa geração de imagens é chamada de *cópia bit a bit*, e
- Garantir que o original não foi alterado.

Um método para assegurar que esses requisitos foram corretamente adotados é a utilização de algoritmos de integridade, como uma função *hash*[7]. Alguns algoritmos utilizados para essa verificação é o MD-5 ou a SHA-1 para gerar a assinatura original da mídia, antes e depois da operação de cópia.

Segundo Shimabuko (2009), deve-se evitar conectar mídias passíveis de escrita, como disco rígidos e *pendrives*, em sistemas Windows ou Unix que não tenham sido corretamente configurados, pois o conteúdo pode ser indevidamente alterado. A cópia de unidades de armazenamento que contenham sistemas de arquivo com *journaling*, como o NTFS, é delicada, pois mesmo montando-se um sistema em modo somente leitura, pode ocorrer modificação deste ou a montagem pode nem ser executada. Essas alterações podem ser evitadas através do uso de bloqueadores de escrita (por *hardware* e por *software*).

Os bloqueadores de escrita por *softwares* podem operar de dois modos:

- Usando um dos serviços da BIOS denominado *INT13h*. O uso da interrupção *INT13h* é feito por sistemas limitados, como o *DOS* [SHIMABUKO, 2009];
- Acessando diretamente a controladora dos discos rígidos;

Sistemas operacionais mais atuais, Windows XP ou Linux, em modo protegido, acessam diretamente a controladora utilizando *drivers* de dispositivos, componentes de *software* que conheçam os comandos e registradores definidos pelos fabricantes.

Existem aplicativos, principalmente para Windows, que efetuam bloqueio de escrita em determinados dispositivos. Alguns foram testados pelo CFTT (*Computer Forensic Tool Testing*) do NIST (*National Institute of Standards and Technology*), que estabeleceu uma metodologia de teste para esse tipo de aplicativo [NIST, 2003].

A grande desvantagem da utilização dos bloqueadores de escrita através de dispositivos de *softwares* é a dependência, dos mesmos, com a plataforma utilizada pelos sistemas operacionais.

---

[7] Sequência de bits gerados por algoritmos de integridade.

Os bloqueadores de escrita por *hardware* suprem a deficiência do bloqueio por *software*, desvantagem citada anteriormente. Um dispositivo físico é conectado entre o disco rígido e um sistema de cópia impedindo a execução de operações de escrita.

Utilizando esses dois métodos de bloqueio de escrita no disco de evidência é realizada a preservação da mídia original, para futuras análises.

4.1.4 Reconstrução dos Eventos

A elaboração do laudo pericial, com descrição minuciosa do que foi examinado [BRASIL, 1941], pressupõe o entendimento da sequência dos eventos que produziram as evidências encontradas [SHIMABUKO, 2009].

Nos sistemas computacionais, a cronologia dos fatos é registrada com a utilização de rótulos de tempo cuja precisão dos registros depende do método utilizado para a determinação desses rótulos [SHIMABUKO, 2009].

O Comitê Gestor da Internet no Brasil, por meio de resolução (2003) considera que a sincronização com fontes de tempo confiáveis dos computadores e outros equipamentos interligados à Internet é essencial para a documentação e preservação de evidências que possam vir a ser utilizadas em investigações de crimes de informática e recomenda, [*CGI.br*, 2008]:

1. Sincronizar, com à Hora Legal Brasileira, todos os dispositivos de rede e servidores conectados à Internet no Brasil, de forma continuada, utilizando-se de programas de computador apropriados e fontes de tempo confiáveis;
2. Sempre que possível e apropriado, sincronizar, com a Hora legal Brasileira, estações de trabalho conectadas à Internet no Brasil, de forma continuada, utilizando-se de programas de computador apropriados e fontes de tempo confiáveis;
3. Estabelecer procedimentos de ajuste do tempo ao fuso horário local e ao horário de verão, quando necessários;
4. Gerar registro de eventos (logs) pertinentes, de forma a manter informações inequívocas sobre o fuso horário em que se deu um evento.

5. Utilizar, preferencialmente, o protocolo *NTP*[8] (Network Time Protocol), conforme padrões de referência e instruções presentes na página Web do Projeto *NTP* do *NIC.br*;
6. Utilizar, preferencialmente, os servidores de tempo implantados pelo *NIC.br*, através do projeto *NTP.br*, como referências de tempo;

O sistema operacional conta o tempo usando tiques de um relógio, cuja calibração é executada na inicialização. A sincronização do tempo é geralmente executada optando-se por um dos seguintes métodos: (i) lendo o relógio interno do computador, que é mantido por uma bateria quando o equipamento está desligado; (ii) usando uma fonte externa, via rede pode ser um servidor de tempo na rede local ou um disponível na Internet normalmente usando o protocolo *NTP*, conforme recomendação do Comitê Gestor da Internet no Brasil [*CGI.br*, 2008] [SHIMABUKO, 2009].

Registro de ocorrências (logs) consiste em uma fonte importante para se determinar a sequência de eventos. Sistemas operacionais utilizados como servidores possuem, por padrão, registros de ocorrências de segurança, de sistema e de aplicação.

Os registros de segurança (*security log*) registram eventos *logons* válidos ou inválidos. Registros de ocorrência de sistema (*system log*) registram eventos pré-definidos, como a inicialização de determinados serviços e sincronização com o relógio. Registros de ocorrências de aplicação (*application log*) registram eventos definidos pela aplicação.

4.2 Metodologia do Departamento de Justiça norte americano (*U.S Departament of Justice)*

O êxito da investigação e repressão de crimes eletrônicos, segundo o FBI[9], requer na maioria dos casos, coleta, preservação e análise forense das evidências, crucial para determinação de culpa ou inocência.

Os princípios gerais e processuais forense adotados são:

- Medidas de proteção e coleta de evidências digitais que não afetem a integridade das evidências;

[8] NTP é um protocolo de sincronização dos relógios, contidos em uma rede de computadores, baseado em UDP.
[9] Federal Bureal of Investigation

- Treinamento específico dos responsáveis pelo exame das provas digitais; e
- Documentação, preservação e disponibilidade para revisão das atividades relacionadas com a apreensão, análise, armazenamento ou transferência de dados digitais.

4.2.1 Segurança e Avaliação do Local do Crime

Para *U.S Departamento of Justice*, a primeira resposta a um incidente é garantir a segurança de todas as pessoas que se encontram no local e proteger a integridade das evidências eletrônicas ou convencionais. Posteriormente, identifica-se visualmente as potencias evidências eletrônicas ou convencionais físicas.

O procedimento a ser tomado é a reavaliação da natureza de *software* e *hardware*, potenciais evidências procuradas e as circunstancias que rodeiam na aquisição das evidências a ser examinada.

O investigador responsável deve sempre garantir que o local esteja devidamente assegurado antes e depois da coleta das evidências, adotando os seguintes procedimentos no local do crime:

- Identificar a quantidade e o tipo de computadores;
- Determinar se existe uma rede;
- Entrevistar o administrador e usuários do sistema;
- Identificar e documentar os tipos e volumes de mídia e a documentação da localização da mídia ao ser retirada;
- Identificar software proprietário;
- Determinar o sistema operacional ativo;

A evidência digital, devido a sua natureza, é frágil e pode ser alterada, danificada ou destruída pelo manuseio incorreto, não somente a integridade física dos componentes como também a transferência eletrônica de dados. Por essa razão são necessárias precauções especiais na preservação das evidências, pois atitudes incorretas podem inutilizá-las ou conduzir a uma conclusão imprecisa.

4.2.1.1 Documentação do Local do Crime

A documentação do local do crime cria um registro histórico da cena permanentemente. É importante registrar a localização e condição inicial dos computadores, suporte de armazenamento e outros dispositivos periféricos.

Os procedimentos na cena do crime devem ser documentados em detalhes, tais como:

- Observar e documentar o local do crime, tais como a posição do mouse e a localização dos componentes em relação a outros componentes. Por exemplo, a localização do mouse a esquerda do computador pode indicar que o usuário é canhoto;
- Documentar as condições e local do computador, o status do computador se o mesmo está ligado, desligado ou em modo de hibernação;
- Fotografar todo o local do crime, criando um registro visual do mesmo. A documentação completa da cena deve ser registrada em 360 graus de cobertura, quando possível;
- Fotografar de frente o computador, assim como o monitor e outros componentes. Tomar notas por escrito sobre o que está aparecendo na tela do computador;

4.2.2 Preservação do Sistema

As evidências digitais são recolhidas de acordo com as orientações departamentais da justiça norte americana. Na ausência dessas orientações são adotados os seguintes procedimentos de coleta de dados.

4.2.2.1 Preservação em Ambiente de Complexidade Baixa

Computadores portáteis se diferem dos outros na medida em que podem ser alimentado por uma fonte ou bateria elétrica, por isso, exige a remoção da bateria, além dos procedimentos de desligar o computador.

Anotar todas as ações executadas pelo investigador e qualquer mudança que venha acontecer no monitor, computador, impressora ou outros periféricos. Identificar certamente se o computador está ligado, desligado ou em modo de

espera, e em seguida, decidir quais ações serão aplicadas para a situação descoberta.

Para a situação aonde o computador encontra-se ligado e o ambiente de trabalho é visível, o investigador deve fotografar a tela do computador e gravar as informações exibidas. Quando o computador encontra-se em modo de espera, deve-se mover o mouse lentamente (sem pressionar botões), a tela deve apresentar o ambiente de trabalho ou solicitar a senha do computador. Se o movimento do mouse, não resultou no aparecimento do ambiente de trabalho na tela, o investigador deve acionar qualquer tecla ou ação do mouse. Com o aparecimento de informações na tela, deve ser fotografado e gravado qualquer informação que se apresente na tela.

E quando o monitor encontra-se desligado deve-se anotar esse fato como condição inicial do monitor.

Após a verificação desses três estados que um *stand-alone* pode ser encontrado, o seguinte procedimento é adotado:

- Independente do estado de energia do computador, retirar o cabo de alimentação do computador. Se for um computador portátil retirar também a bateria;

O investigador deve verificar qualquer conectividade do computador, como por exemplo, ADSL e modem. Se for identificada uma conectividade, tentar identificar a origem.

Para evitar danos a potencias evidências, remover qualquer disquete, que estejam presentes, empacotar e rotular separadamente os disquetes. Se houver presença de CD-ROM, não retirar da unidade.

4.2.2.2 Preservação em Ambiente de Complexidade Alta

Em ambientes empresarias que possuem múltiplos computadores interligados por uma rede, por um servidor central ao investigar um ambiente de complexidade alta, deve-se planejar com antecedência ações a serem tomadas e se possível assistência de pessoal especializado.

A possibilidade de encontrar diferentes sistemas operacionais e hardwares complexos exige procedimentos especializados para o desligamento, o importante é

identificar e reconhecer as diferentes topologias da rede, a assistência especializada poderá auxiliar nesse tratamento.

Os itens a seguir podem indicar que um computador está conectado a uma rede:

- A presença de múltiplos sistemas computacionais;
- A presença de cabos e conectores, correndo entre os computadores ou dispositivos centrais como hubs; e
- As informações fornecidas pelo pessoal especializado.

4.2.3 Análise das Evidências

Para o *U.S. Department of Justice* existem dois tipos diferentes de extração de dados: extração física e lógica. O primeiro recupera os dados de toda a unidade física, não levando a respeito o sistema de arquivos, e o segundo recupera os dados e arquivos baseados no sistema operacional instalado e/ou sistema de arquivo.

Durante a fase de extração física dos dados, a movimentação dos dados ocorre no nível físico, independente dos sistemas de arquivos presentes nos discos rígidos. Nessa fase pode ser incluso métodos de pesquisa por palavra chave, extração de arquivos da tabela de partição e espaço não utilizado em unidade física.

Os arquivos *carving* (*file carving*), que é o processo aonde se utilizam uma entrada para a pesquisa de arquivos ou outros tipos de dados com base no conteúdo. Esse processo é utilizado para extrair arquivos e dados que não podem ser contabilizados pelo sistema operacional ou sistema de arquivos.

Na fase de extração lógica, a coleta de dados é baseada no sistema de arquivo presentes no disco rígido. Podendo incluir dados provenientes de áreas distintas do sistema de arquivos, tais como arquivos ativos, arquivos excluídos, arquivo de somente leitura e arquivos bloqueados.

A extração de dados do sistema de arquivos pode revelar características de estrutura de diretórios, atributos de arquivo, os nomes de ficheiro, data e hora, tamanho do arquivo e localização do ficheiro.

Para o investigador identificar e eliminar ficheiros conhecidos pode ser feito pela comparação de valores *hash*. O *U.S. Department of Justice* utiliza os seguintes métodos de analise de evidências.

4.2.3.1 Análise dos Dados Extraídos

De acordo com *U.S. Department of Justice*, “a análise é o processo de interpretação dos dados extraídos para determinar o seu significado para o caso”. Alguns exemplos dessa análise a ser realizada incluem calendário, os dados do sistema, a aplicação e os tipos de arquivos.

4.2.3.2 Análise *Timeframe*

Essa análise pode ser útil para determinar os eventos ocorridos em um sistema, podendo ser usado como parte da associação do uso do sistema com um determinado indivíduo no momento em que os eventos ocorrem. Dois métodos podem ser utilizados [*CASEY, 2000*] :

- Rever à hora e data contida no sistema de arquivos e nos metadados, para vincular arquivos de interesses para os prazos relevantes para o inquérito. Um exemplo dessa análise seria a utilização da data e hora para definir quando o conteúdo de um arquivo foi modificado;
- Rever o sistema e os logs da aplicação que possa estar presente. Esses arquivos podem incluir erro de registros, logs de instalação, logs de segurança entre outros. O exame dos logs de segurança quando a combinação de usuário e senha foi utilizada para o acesso ao sistema;

4.2.3.3 Análise em Dados Ocultos

Os dados de um sistema podem ser ocultados, essa análise em dados ocultos pode ser útil na detecção e recuperação desses dados e poderá indicar o conhecimento, a propriedade, ou intenções contidas nesses dados. Métodos que podem ser utilizados nessa análise:

- Correlacionamento do cabeçalho dos arquivos com a correspondente extensão para identificar possíveis desajustes. A presença inadequação dos arquivos pode identificar que o usuário intencionalmente ocultou os dados;
- O acesso a dados protegidos por senha, criptografados e arquivos compactados podem identificar uma tentativa de ocultação dos dados a usuários não autorizados;

- Acesso a um espaço *host-protected área* [10] (HPA). A presença de um HPA pode indicar a tentativa de ocultação de dados;

4.2.3.4 Análise em Arquivos e Aplicação

Muitos arquivos e programas identificados podem conter informações relevantes para a investigação e dar uma idéia da capacidade do sistema, assim como o conhecimento do usuário. Os resultados dessas análise pode indicar os passos adicionais que devem ser tomados na extração e análise dos processos. Como por exemplo:

- Revisão da nomenclatura dos arquivos para a relevância e padrão utilizado;
- Examinando o conteúdo dos arquivos;
- Identificar o tipo do sistema operacional;
- Correlacionar os arquivos para as aplicações instaladas;
- Considerar as relações dos arquivos. Podemos citar a Internet com o histórico e arquivos de e-mail;
- Identificar os tipos de arquivos desconhecidos determinando o seu valor para o inquérito;
- Analisar os usuários padrões de armazenamento local para as aplicações e as estrutura dos fichários, para identificar se os fichários estão armazenados no diretório padrão ou em uma localização alternativa;
- Analisar a configuração do sistema operacional;

4.2.3.5 Análise Propriedade e Posse

Identificar os usuários que criaram, modificaram ou acessaram um determinado arquivo pode ser essencial para a investigação, sendo necessário e de grande importância obter a informação dos usuários cujos arquivos questionados pertencem. Elementos de propriedade e posse dos usuários podem incluir os seguintes fatores:

- Colocar o assunto no computador em uma determinada data e hora (Análise Temporal) pode auxiliar na determinação da propriedade e posse;

[10] É definido como uma área reservada em um disco rígido.

- Arquivos de interesse podem ser localizados em locais definidos, como por exemplo, um diretório criado pelo usuário chamado “Pornografia Infantil”;
- O nome do arquivo questionado pode ser de valor probatório e também pode identificar o conteúdo do arquivo;
- Dados ocultos podem identificar a tentativa deliberada de evitar a detecção dos dados;
- O acesso a arquivos codificados e protegidos por senha pode identificar a propriedade e posse dos arquivos ao usuário;
- O conteúdo do arquivo pode identificar propriedade ou posse por conter informações especificas para o proprietário;

4.2.4 Armazenamento

Responsabilidade e muito cuidado deve ser tomando com as evidências digitais e registros devem ser feitos com relação à posse das mesmas. As evidências devem ser armazenadas adequadamente em local seguro, com acesso restrito somente à equipe de investigação. Deve ser utilizado embalagens adequadas e seguras, mantendo a integridade das mesmas, sendo utilizadas para o armazenamento das evidências coletadas para uma futura análise.

Ao se realizar cópias eletrônicas de registros, a informação original nunca deve ser alterada. Sendo necessário analisar os dados do mesmo, obter e trabalhar com a cópia. Em caso de evidências coletadas sejam papeis, armazenar os originais e trabalhar sobre as cópias.

As medidas adotadas não devem adicionar, modificar ou destruir dados armazenados em um computador ou outros meios de comunicação. Computadores são frágeis, sensíveis à temperatura, umidade, choque físico, eletricidade estática, e fontes magnéticas. Portanto, precauções especiais devem ser tomadas no transporte e armazenamento de dados eletrônicos [*CASEY, 2000*].

De acordo com o Departamento de Justiça norte americano, os procedimentos para embalagem, transporte e armazenamento das evidências devem ser tomados com precaução.

Procedimentos para embalagem das evidências:

- Assegurar que todas as evidências recolhidas está devidamente documentado, etiquetado e inventariados antes da embalagem;

- Atenção especial nas evidências latentes ou vestígios de provas e tomar medidas para preservá-la;
- Pacote de suportes magnéticos em embalagem anti-estática (em papel ou sacos de plástico anti-estático). Evite o uso de materiais que podem produzir eletricidade estática;
- Evite dobrar ou encurvar multimídias, como disquetes, CD-ROM e fitas;
- Assegurar que todos os recipientes utilizados para armazenar dados são devidamente etiquetados;

  Procedimentos para o transporte das evidências:
- Manter afastado das evidências digitais fontes magnéticas. Rádios transmissores e assentos aquecidos são exemplos de itens que podem danificar as evidências digitais;
- Evitar guardar evidências digitais em veículos por períodos prolongados. Condições de calor excessivo, frio ou umidade, pode danificar as evidências digitais;
- Assegurar que os computadores e outros componentes que não são armazenados em embalagens, estejam em recipientes que evite choque e excesso de vibração. Por exemplo, os computadores podem ser colocados no chão do veículo;

  Procedimentos para armazenagem das evidências:
- Assegurar que as provas sejam inventariadas;
- Armazenar dados em área segura, distantes de temperatura e umidade extremos e proteger de fontes magnéticas;

O investigador responsável pelo manuseio das evidências digitais deve elaborar uma documentação das mesmas. Assim todas as evidências estarão armazenadas em recipientes adequados e documentos.

4.3 Análise das metodologias

Analisando primeiramente a metodologia da Polícia Civil do Distrito Federal e em seguida *U.S Departament of Justice*. Cada procedimento tem seus pontos fortes e pontos a serem melhorados.

Para o início da investigação forense em sistemas computacionais, a PCDF começa destacando a preservação do sistema aonde destaca os pontos fortes em preservação do sistema independente do estado inicial do mesmo, seja ligado ou desligado. Compreendendo o desligamento súbito do sistema em casos extremos, por exemplo, arquivos sendo modificados ou excluídos.

Em contra partida poderia ser observado à complexidade do ambiente em que o sistema investigado se encontra, averiguando o conjunto completo do sistema. Com esse procedimento de verificação da complexidade do ambiente o investigador tem um maior domínio da situação ao seu alcance, sendo possível determinar a topologia de rede encontrada no local.

O item de complexidade é abordado pela metodologia da *U.S Departament of Justice*. No qual determina a abordagem do investigador quanto à complexidade do ambiente, no procedimento de preservação do sistema. Para *U.S Departament of Justice* os sistemas computacionais devem ser mantidos da mesma forma que foram encontrados, se eles estiverem ligados, deixe-os, se eles estiverem desligados, deixe-os. "*If it is off, leave it off. If it is on, leave it on.*" fazendo a distinção somente entre a complexidade do local do crime.

Essa afirmativa de manter o sistema da forma em que foram encontrados é uma falha nesse procedimento, já que em um sistema encontrado ligado e esteja sobre controle de um intruso e o mesmo perceber a presença de investigadores, ele pode começar uma serie de ações para eliminar as evidências deixadas no ato da intrusão. Deixando assim esse procedimento sem ações para acontecimentos extremos de alteração e exclusão de dados.

Um ponto forte na metodologia de preservação do sistema destacado pela *U.S Departament of Justice* é a segurança e avaliação do local do crime. Avaliando as medidas de segurança das pessoas presentes na cena do crime e a identificação do local. Determinando um amplo campo de ação para a preservação do ambiente em que o sistema se encontra, garantindo sempre que o local está devidamente assegurado antes e depois da coleta das evidências.

Juntando os pontos de preservação do sistema adotados pelas metodologias estudas, juntamente com o procedimento de segurança e avaliação do local do crime, construiria uma metodologia mais consistente e integra para a preservação total do sistema a ser investigado.

Analisando o procedimento de coleta de dados verifica-se na metodologia *U.S Departament of Justice* que esse método é incluso com a análise das evidências. Evidenciando somente a extração dos dados de duas formas distintas. A extração de dados física, coleta de dados em nível físico e a extração de dados lógica, coleta de dados em sistemas de arquivos presentes no disco rígido. Esse método deixa muito vaga à idéia de coleta de evidências.

Para a PCDF o procedimento de coleta de dados é baseado no estado inicial do sistema, ligado ou desligado. Para a coleta em sistemas ligados, Angelo Shimabuko, esclarece que esse procedimento poderá acarretar em alteração na estrutura do sistema operacional, colocando também que a coleta de informações presente nesse estado é de grande importância, podemos destacar para os processos em execução e conexões de rede.

Para os sistemas com estado inicial desligado a coleta de dados é feita por meios de armazenagem de dados, como disco rígido. Colocando as duas análises para esses tipos de coleta, análise ao vivo e *post mortem*.

Ambas as metodologias trabalham com a coleta de dados dependente do estado inicial do sistema, colocando os dois pontos fortes desses procedimentos. A falha encontrada nesse procedimento é a falta da geração de cópia da mídia do sistema suspeito, deixando o original intacto, integro e confiável.

Esse procedimento de cópia da mídia pode ser feita independente do estado inicial do sistema, com o sistema ligado essa cópia poderia ser feita através de conexões de rede, com sistemas desligados a cópia seria feita para uma mídia externa, destaco um *HD* externo.

As análises das evidências da metodologia da PCDF são coesas e completas, o investigador tem duas formas de realizar a análise dependendo do estado inicial do sistema. Com o sistema ligado o investigador pode realizar a análise ao vivo, enquanto na outra opção é possível realizar a análise *post mortem*.

Esse procedimento na metodologia *U.S Departament of Justice* aborda uma serie de análises, podendo ser utilizada de acordo com o estado inicial do sistema, a

não conformidade desse procedimento é a falta de clareza de quais métodos de análise pode ser usado dependendo do estado inicial do sistema investigado.

No procedimento de reconstrução dos eventos relatados pela PCDF é de grande valia para a documentação final, que seria um laudo técnico-pericial. Esse procedimento junto com duas análises feitas pela *U.S Departament of Justice*, análise *timeframe* e análise de propriedade e posse, reforçaria a reconstrução dos eventos com dados precisos, íntegros e confiáveis para serem inclusos no laudo final.

De acordo com o estudo de cada metodologia e com a análise feitas entre ambas é possível distinguir os procedimentos adotados pelos órgãos responsáveis por cada metodologia. Com a junção de processos realizados por cada metodologia estudada fornece um processo mais robusto e concreto de acordo com a tabela 1.

Tabela 1 – Relacionamento das metodologias estudadas

	Polícia Civil do Distrito Federal (PCDF)	***U.S Departament of Justice***
Segurança e Avaliação do local do crime	Não relatado.	Medidas de segurança a pessoas no local e identificação do local do crime.
Preservação do sistema	Preservação em sistemas ligados/desligados.	Preservação de sistema de acordo com a complexidade do ambiente.
Coleta das evidências	De acordo com a preservação do sistema, distingue a forma de análise.	Acopla a extração das informações (evidências) e a análise.
Análise das evidências	Utiliza duas análise: • análise ao vivo; • análise *post mortem*;	Descreve uma serie de métodos para análise, sem aprofundamento do tema.
Reconstrução do evento	Referência a cronologia dos fatos.	Encontrado na análise timeframe e análise de propriedade e posse
Armazenamento	Não relatado.	Proteção, transporte e embalagem das evidências

5 METODOLOGIA PROPOSTA

Os crimes cibernéticos realizado por intruso passam por despercebido pelos administradores de rede. Por exemplo, um intruso invade um sistema alvo, ele pode acessar os dado e copiá-los. Ou seja, o intruso está roubando dados do sistema alvo, mas ninguém vai sentir falta do arquivo, já que o original permanece na máquina.

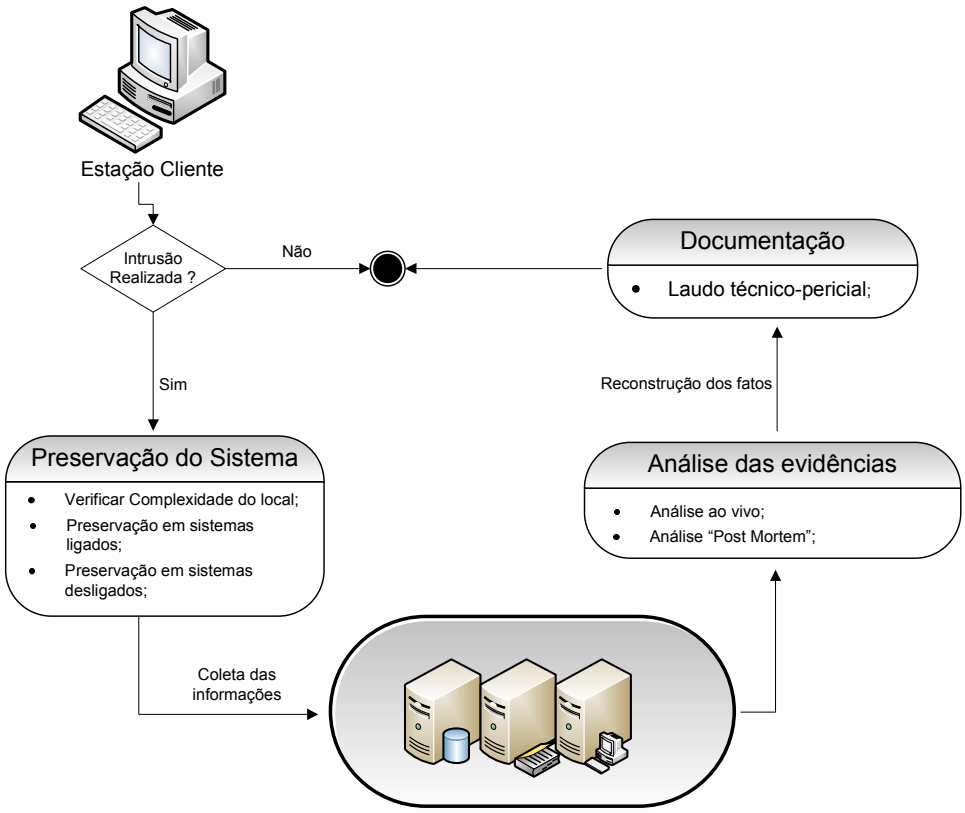
Outro caso seria que a vítima detecta a intrusão porém não reporta a ninguém sobre o ocorrido. Isso acontece, geralmente, com empresas que ao reportar que foram invadidas podem ter sua imagem prejudicada no cenário comercial.

Contendo os pontos fortes das metodologias estudadas e a melhoria dos pontos fracos. Essa metodologia visa o melhoramento continuo do estudo de análise forense de acordo com o fluxograma 4.

Como analisado no capítulo quatro (4), os pontos fortes da metodologia da Polícia Civil do Distrito Federal. Esses itens contemplam de forma substancial a metodologia proposta e complementa a metodologia do *U.S Departament of Justice*.

- Preservação do sistema;
- Análise das evidências;
    - Análise ao vivo;
    - *Post Mortem*;
- Documentação;
- Reconstrução dos eventos, de acordo com a cronologia dos fatos;

  Os pontos fortes da metodologia do *U.S Departament of Justice*:
- Verificação da complexidade do ambiente;
- Medidas de segurança e avaliação do local da análise;
- Armazenamento: Proteção das evidências, transporte e embalagem das mesmas;
- Documentação;
- Análise *timeframe* e análise de propriedade e posse;



Fluxograma 4 – Metodologia proposta

5.1 Preservação do sistema

Para a preservação do sistema, o investigador deve inicialmente verificar o estado inicial do sistema, observando se o mesmo está ligado ou desligado.

Se deparando com o sistema ligado, o mesmo, deve se possível fotografar a tela do monitor com os dados aparentes. Permanecendo o sistema ligado, o responsável deve analisar os processos em execução. Encontrado alguma atividade maliciosa que possa danificar ou comprometer os dados, o mesmo deve desligar o sistema abruptamente (desligar a força de energia).

O investigador deve classificar o ambiente de acordo com sua complexidade. A complexidade do ambiente e caracterizada pela quantidade de sistemas operacionais distintos e a interligação dos sistemas de acordo com a topologia de rede. Um computador autônomo, interligado somente pela *Internet* e conectado a periféricos, esse ambiente é classificado com complexidade baixa. Um sistema empresarial que possua vários sistemas operacionais distintos, computadores

interligados a uma rede interna e outra externa, esse ambiente é classificado com a complexidade alta.

O investigador pode executar as ações tomadas na metodologia exposta pela Polícia Civil do Distrito Federal, para sistema ligado e sistemas desligados. Abordando assim os procedimentos necessários para a preservação do ambiente no seu estado inicial.

Independente das ações tomadas pelo responsável, o passo a passo dos procedimentos realizados deve ser documentado. Se alguma decisão for incorreta, a documentação permitirá a avaliação dos prejuízos para a investigação.

O procedimento de preservação do sistema utilizado pela metodologia da Polícia Civil do Distrito Federal foi utilizada nessa metodologia por corresponder a um conjunto de procedimentos a serem utilizados na preservação do sistema, alem de abordar, de forma eficiente e eficaz, os problemas no estado atual do sistema.

5.2 Coleta das informações

Evidência digital, pela sua própria natureza, é frágil e pode ser alterada ou danificada pelo manuseio inadequado das mesmas. Por essas razões é necessário precauções para o manuseio e preservação dessas provas. Se não o fizer, as evidências se tornam inutilizáveis ou pode conduzir a uma análise imprecisa.

Realizar análise sobre os dados adquiridos, sempre que possível, não deve ser realizado nas evidências originais. O responsável pela coleta de dados deve fazer uma imagem precisa da original, mantendo a original intacta.

Analisar a estrutura das partições pode identificar o sistema de arquivos presente e determinar se o tamanho físico do disco rígido é contabilizado.

A extração dos dados do sistema de arquivos pode revelar características como estrutura de diretórios, atributos, nomes de fichário, data e hora, tamanho do arquivo e a localização do fichário.

Os procedimentos de coleta de evidências devem ser coerentes com um conjunto de princípios legais e técnicos, conforme argumenta Argolo (2005):

- As ações do investigador não devem alterar as evidências;
- A evidência original deve ser preservada no estado mais próximo possível em que foi encontrada;

- Todas as evidências digitais coletadas e as cópias produzidas devem ser autenticadas por meio de *hash* criptografado, para verificar sua integridade;
- O investigador não deve confiar nos programas e nem nas bibliotecas dinâmicas;
- Fazer uma cópia exata da evidência original sempre que possível, para preservar a integridade;
- A cópia dos dados que serão examinados devem ser feitas para uma mídia "esterilizada" e sem defeitos;
- Toda evidência deve ser apropriadamente etiquetada, contendo por exemplo, o nome do caso investigado, data e hora da coleta, entre outros;
- Todas as informações relativas à investigação devem ser documentadas;
- As ferramentas utilizadas na investigação devem ser aceitas pelos especialistas forenses e testadas para garantir sua operação correta e confiável;

Na coleta das informações a autenticidade e a integridade são de suma importância para a análise dos itens, podendo ser estabelecida através de assinaturas criptográficas, como *MD5* e *SHA*. Utilizando essas assinaturas é possível determinar que os itens coletados sejam autênticos, através da comparação do *hash* com a assinatura criptográfica original.

Dan Farmer e Wietse Venema introduziram um conceito denominado “ordem de volatilidade”. A definição desse conceito é que o tempo de vida de uma evidência digital é determinado de acordo com o local aonde é armazenado. As principais fontes de evidências são apresentadas de forma descendente de volatilidade [CANSIAN, 2000] [FARMER; VENEMA, 1999]:

- Dispositivos de armazenagem da CPU (registradores e *caches*);
- Memória de periféricos (memória de vídeo, por exemplo);
- Memória principal do sistema;
- Tráfego de rede (pacotes em trânsito na rede);
- Estado do sistema operacional (como, por exemplo, estado das conexões de rede e dos processos em execução, usuários logados e configurações do sistema);

- Dispositivos de armazenagem secundária;

Quanto maior a volatilidade das evidências digitais, maior será a dificuldade de coleta e menos tempo para o investigador coletar. Entretanto informações voláteis como o estado do sistema operacional, o tráfego de rede e a memória principal do sistema podem ser capturadas mais facilmente, em comparação a itens com volatilidade superior, e podem conter informações preciosas a respeito de intrusões em andamento.

É de suma importância que os investigadores sigam o procedimento, de forma correta garantindo, assim, que as evidências foi coletada, preservada e analisada de forma, minuciosa, correta e livre de contaminações. Uma coleta conduzida impropriamente pode comprometer totalmente a investigação [ARGOLO, 2005].

O procedimento de coleta de evidências utilizada nessa metodologia é a junção de ambas as metodologias estudadas, foi observado que a junção dessas metodologias construiu um procedimento mais robusto e eficaz para a análise forense.

O procedimento de geração de imagem através da mídia original coletada foi descrita de forma sucinta nas metodologias estudadas. A partir dessa descrição sucinta e de materiais coletados na fase de pesquisa foi possível reunir informações suficientes para a especificação da geração de imagem.

5.2.1 Imagem do Disco

A imagem do disco é um processo de se fazer cópias exatas dos dados contidos no disco original, preservando sua estrutura. No processo de cópia dos dados do disco original para outro disco rígido, os dados armazenados no outro disco serão de forma seqüencial. Independente da forma em que foi gerada a imagem o conteúdo dos dados serão o mesmo, mas a forma como está distribuído será diferente.

Na geração da imagem dados que estejam em lugares não acessíveis pelo sistema não serão replicados para a imagem. Nesses lugares o intruso pode esconder evidências de sua intrusão. Alguns lugares não acessíveis são [ARGOLO, 2005]:

- O sistema de arquivo pode não ocupar totalmente a partição devido ao tamanho do bloco (*cluster*) utilizado. Os últimos setores desperdiçados devem ser verificados;
- Espaços alocados a arquivos que não são totalmente utilizados (*file slacks*) podem ser utilizados para esconder informações. Por exemplo, um arquivo com tamanho de 2460 bytes, em um sistema de arquivos com tamanho de bloco de 1024 bytes, ocupa três blocos de alocação (3 * 1024 = 3072), desperdiçando os últimos 612 (3072 - 2460 = 612) bytes alocados;
- A BIOS pode não suportar a geometria do disco de modo que, não é permitido o acesso a toda porção física do disco;
- As partições acessíveis podem não ocupar todo o disco, podendo surgir assim, espaço entre partições ou no final do disco;
- Podem existir partições que não contêm um sistema de arquivos e mesmo assim esconder informações;
- Vestígio de arquivos apagados. Quando um arquivo é apagado, sua referência é removida das estruturas do sistema de arquivos, entretendo os dados contidos no arquivo não são apagados do disco [CASEY, 200]. Estes dados ficam no disco até que sejam sobrescritos por outros arquivos;
- Arquivos de swap podem conter dados importantes que ainda não foram gravadas no disco;

Programas normais de cópia ou de backup não devem ser utilizados para efetuar uma análise forense por só conterem os dados reconhecidos pelo sistema de arquivos, não capturando todos os dados residuais (arquivos apagados, *slack space*, arquivos *swap*). Já uma cópia bit a bit possui todas as informações do disco [ARGOLO, 2005].

A etapa de criação de imagem do disco original é de suma importância para a investigação, despreocupando o investigador de danificar evidências e é nessa etapa em que o investigador gasta o seu maior tempo de análise.

As imagens dos dados podem ser feito por alguns procedimentos:

- Uma máquina pode ser posto na mesma rede em que o sistema alvo, através da conexão de rede, transfere os dados do sistema suspeito para a segunda máquina;

- Pode-se extrair o disco da máquina suspeita, colocando-o em outra máquina e transferir os dados do disco da máquina suspeita para o disco da segunda máquina;
- Na máquina suspeita pode ser incluso um novo disco para realizar a transferência dos dados do disco suspeito ao novo disco incluso na máquina;

A escolha de ferramentas para a criação de imagens do disco deve atender recomendações de acordo *National Institute of Standards and Technology* (NIST) [NIST, 2003].

- Capaz de fazer uma imagem do disco original, uma partição do disco ou uma mídia removível;
- Sua execução não pode alterar o original;
- Capaz de acessar tanto disco IDE quanto SCSI;
- Registrar (log) erros de entrada e saída (input/output);
- A documentação deve estar correta;
- Deve ser capaz de verificar a integridade do arquivo de imagem do disco;

Para a geração de imagem foi escolhido o programa **dd**, um programa que atende aos requisitos do *NIST*. Esse programa foi desenvolvido para sistemas *GNU/Linux*, sendo um programa *freeware* (não tem custo adicional), e faz a cópia de imagem e de cada setor de um dispositivo *IDE* e *SCSI*.

5.2.2 Gerando a imagem

De acordo com o programa escolhido para a geração da imagem, que no caso foi o **dd**, o investigador deve configurar seu laboratório de acordo com os programas por ele escolhido durante a fase do planejamento.

Supondo que o investigador esteja com o laboratório configurado, e está na etapa de geração da imagem, o disco rígido suspeito deve ser instalado como *master* da *IDE* secundaria, por exemplo, para que a geração da imagem seja, hdb_img.dd. O comando utilizado para a geração dessa imagem:

#dd if=/dev/hdb of=hdb_img.dd

Outra forma de gerar a imagem, importando-a para outro disco rígido (hdc) é a utilização do comando:

#dd if=/deve/hdb of=/dev/hdc

Na geração de imagem com o comando acima, a imagem foi gerada da *IDE master* para a *IDE slave*. Ressaltando que o disco rígido que receber a imagem do disco suspeito deve estar totalmente "esterilizado", completamente limpo, zerado, para que as informações anteriores não confundam na investigação. Outra funcionalidade da ferramenta **dd** é realizar a "limpeza" do disco rígido:

#dd if=/dev/zero of=/dev/hdb

É de grande importância que o investigador, ao gerar a imagem do disco suspeita, faça também um *hash* criptográfico dessa imagem. Comparando a imagem com o *hash* e essas informações forem exatas o investigador está garantindo a integridade da imagem coletada.

O investigador pode se deparar com a seguinte situação, ao chegar no local do sistema suspeito o mesmo se encontra ligado, e para realizar a análise deve ser feito uma imagem. Como o investigador não pode inserir um disco rígido na *IDE* da máquina suspeita, os dados da imagem deve ser transferida pela rede.

A ferramenta **netcat** auxilia o investigador na geração de imagem pela rede, pois permite escreve e ler informações através de uma conexão de rede, sendo possível assim criar um ambiente *cliente-servidor* para realizar a imagem do disco suspeito.

O servidor em caráter especial deve ser uma estação forense, no qual deve está preparado para receber a imagem do disco suspeito. No comando a seguir utilizaremos o servidor escutará na porta 2222:

#nc –l –p 2222 | tee img_hd.dd | md5sum –b > img_md5.dd

Note que o comando **nc**, da ferramenta **netcat**, foi utilizada passando os parâmetros **–l** e **–p**, indicando que a máquina ficará em modo de escuta (*listen*), a espera de pacotes na porta 2222. O comando **tee** recebe o fluxo de dados da entrada padrão, armazena em um arquivo e o replica de forma idêntica para a saída padrão. Com isso os dados recebidos pela porta 2222, serão armazenados no arquivo img_hd.dd e recebidos pelo *md5sum*, gerando seu *hash* criptográfico, e por fim esse arquivo sendo armazenado no *img_md5.dd*.

Finalizado a configuração do servidor, uma estação forense, aonde receberá os dados através de uma porta especificada pelo investigador. Agora é necessário configurar a máquina suspeita para transmitir os dados pela rede ao servidor. Ressaltando que o sistema suspeito pode ter sido modificado ou comprometido

tornando qualquer arquivo desconfiável. Por isso o investigador deve usar os binários a partir de um CD-ROM.

Para a transferência dos dados da maquina suspeita ao servidor, consideramos que o acesso do CD-ROM seja feito através do diretório **/mnt/cdrom**, o cliente pode enviar os dados a partir do comando:

 # /mnt/cdrom/dd if=/dev/hda | tee img_hd.dd | md5sum -b > img_hd.md5

 # cat img_hd.dd | /mnt/cdrom/nc 10.0.0.1 2222

O primeiro comando gera a imagem *img_hd.dd*, recebido pelo *md5sum* que gera o *hash* criptográfico da imagem e armazenado no arquivo *img_hd.md5*. O segundo comando faz a transferência da imagem pela rede, do cliente ao servidor, considerando que o *IP* do servidor seja 10.0.0.1, escutando pela porta 2222.

Após a etapa de geração da imagem pela rede, o investigador deve comparar a imagem gerada com o conteúdo do arquivo *img_hd.md5*. Se a comparação entre os arquivos forem iguais está garantido à integridade da imagem enviada.

5.3 Análise das evidências

A análise das evidências representa o objetivo principal de investigação forense. É o momento em que todo o material coletado é minuciosamente examinado em buscas de evidências, proporcionando ao investigador formular conclusões acerca do incidente que originou a investigação.

Nessa etapa é de suma importância investigar cuidadosamente todas as fontes de informação do sistema analisado, visando à busca de características anormais e indevidas, provavelmente alteradas pelo intruso.

É de grande valia o conhecimento do investigador sobre os modos de operação de um intruso, sendo um requisito essencial para o sucesso e eficácia do processo de análise, esse conhecimento pode aumentar a capacidade do investigador em reconhecer possíveis evidências.

Feito a análise crítica das metodologias estudadas foi constatado a melhor maneira para analisar as evidências digitais, os procedimentos levados pela Polícia Civil do Distrito Federal, a análise ao vivo realizada em sistemas que permanecem com o estado inicial e nada foi feita para o seu desligamento e a análise *Post Mortem*, tal análise pode ser descrita como aquela conduzida a partir de cópias das evidências originais em uma máquina preparada para a tarefa.

A análise ao vivo é de extrema importância para a investigação, uma vez que a única oportunidade de coleta de dados voláteis não estará mais disponível quando o sistema for desligado. O grande problema dessa análise é a falta de domínio total sobre o sistema investigado, dado que esse sistema ainda pode estar sobre ação do intruso, contendo bibliotecas ou processos em execução desenvolvidos para ocultar informações e ludibriar o investigador.

A solução mais apropriada para se evitar o acesso a bibliotecas dinâmicas inseguras é eliminar todo e qualquer acesso dinâmico através da compilação estática de todas as ferramentas necessárias para a análise. No entanto, em virtude da cultura comercial da plataforma Windows, poucas ferramentas desenvolvidas para este sistema possuem código aberto, inviabilizando a recompilação da maioria dos programas e conseqüentemente, o uso de programas estáticos [OLIVEIRA, 2002].

Diferente da análise ao vivo, onde as informações são coletadas em um nível mais alto de abstração, aonde os dados são organizados em estruturas bem definidas como conexões de rede e processos em execução. Na análise *Post Mortem* é necessário lidar com o fato de que tal tipo de organização é obtido através da atuação de várias camadas de software (*drivers*, *kernel* e aplicações) [OLIVEIRA, 2002].

Os itens a seguir exemplificam a análise realizada na investigação, utilizando a análise ao vivo ou análise *Post Mortem*, relembrando que a análise *Post Mortem* é geralmente utilizada em sistemas com estado inicial desligada.

5.3.1 Memória Principal do Sistema

A memória principal do sistema possui informações importantíssimas para a investigação, alguns itens voláteis como os processos em execução, dados que estão sendo manipulador momentaneamente ou dados que ainda não foram salvos na memória secundaria. Tais informações são facilmente recuperadas através de *dumps*[11] de memória ou pela geração de *core files* [WARREN; KRUSE, 2002].

O *Dump* de memória é o processo de recuperação de informações oriundas da memória, para isso foi utilizado o *software "Memorize"* para recuperar essas

[11] Captura de informações da memória.

informações, esse programa é encontrado no site http://www.mandiant.com/software/memoryze.htm.

O "*Memorize*" é uma ferramenta de análise de memória, podendo adquirir a memória física de um sistema *Windows* e pode realizar análises avançadas de elementos em processo na memória enquanto o computador está em execução. Todas as análises podem ser feitas através de uma imagem ou com o sistema ativado.

A figura a seguir ilustra um dumping de memória recuperado pelo "*Memorize*", no qual algumas informações foram retiradas, por motivos da imagem estar muito extensa.

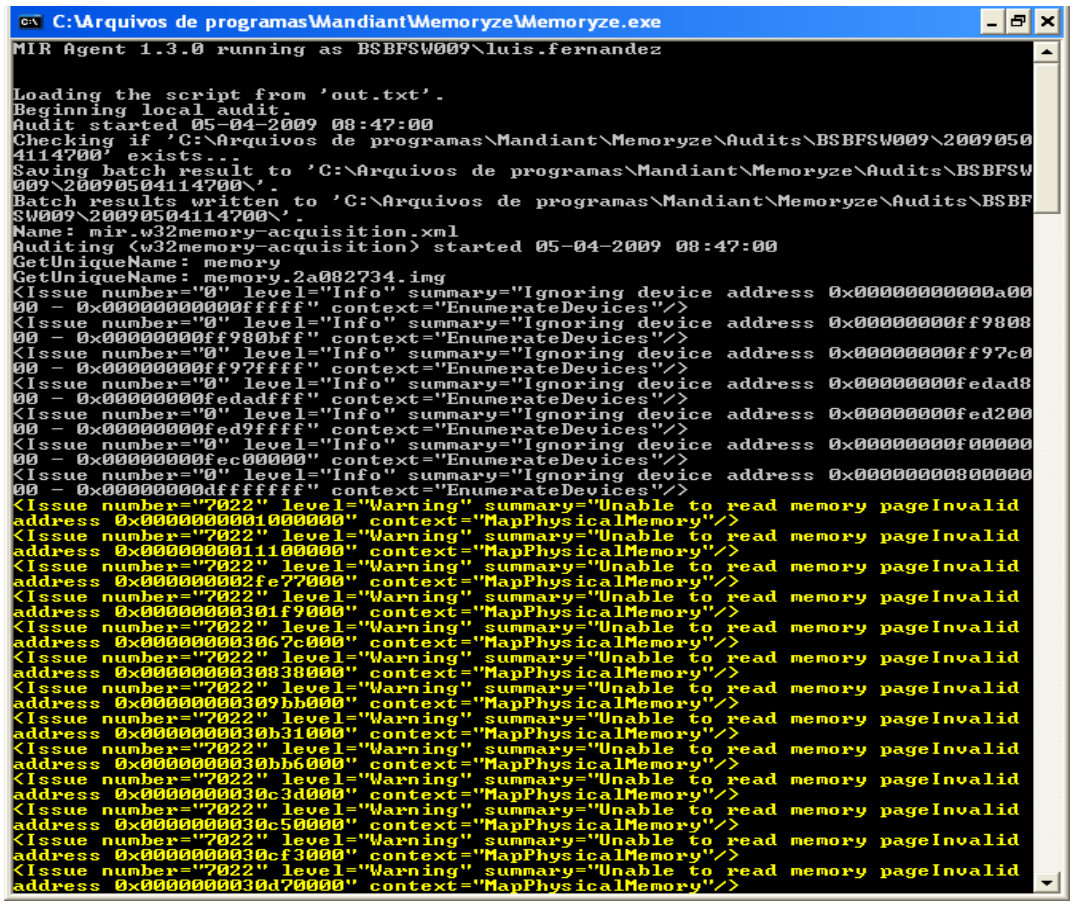


Figura 8 – Dump de memória

Core files são arquivos que contêm a cópia exata da memória ocupada pelo processo quando este é terminado pelo sistema [ARGOLO, 2005]. Por questões de segurança esse recurso é desabilitado, nos arquivos são guardadas informações sensíveis que podem ser usadas por intrusos.

O *core file* deve ser habilitado somente em um servidor que esteja apresentando problemas, por *default* os sistemas operacionais Unix vem com a opção de *core filem* desabilitados e sistema Windows vem habilitado.

Os arquivos de *core file* podem revelar informações preciosas para a investigação, dentre essa informações destacamos as rotinas que estão sendo executadas, os valores dos registradores, o conteúdo do espaço de endereçamento virtual do processo e a estrutura de usuário. O interessante ao investigador é identificar qual programa que originou o *core file*, já que nesses arquivos podem conter comportamentos anormais, geralmente, ocasionados por intrusos. Esses programas são considerados suspeitos e podem ser uma evidência, assim como os arquivos pelo qual o programa faz referencia [ARGOLO, 2005].

5.3.2 Tráfego de rede

A partir do tráfego de rede é possível analisar toda a comunicação entre atacante e máquina invadida, estabelecendo uma seqüência de eventos e comparando com as outras evidências encontradas [ARGOLO, 2005].

Os programas utilizados para capturar o tráfego de rede, são conhecidos como *sniffers*. O programa utilizado para fazer essa captura de dados é o *Wireshark*, [ETHERAL,___].

Em primeiro plano o *sniffer* deve ser colocado em um ponto da rede que tenha acesso ao tráfego de rede relacionado com o sistema suspeito. Quanto maior a quantidade de dados adquiridos e maior o número de operações realizadas sobre os datagramas gerados pelo programa, como decodificação, ou exibição, maior será a carga sobre o sistema de coleta, aumentando a chance de que alguns datagramas sejam descartados [CASEY , 2001].

Algumas ferramentas que analisam os datagramas capturados auxiliam na reconstrução e exibição das informações em formato mais adequado para o investigador. Ferramentas como o *ethereal*, permitem a reprodução da sessão capturada, além da visualização de eventos de forma mais simplificada. Outra ferramenta que auxilia na investigação para a reconstrução de arquivos que foram transferidos durante a sessão de captura, permitindo a recuperação de todo tipo de informação transferida pelo intruso, como a ferramenta *review*.

Utilizando a ferramenta *Wireshark*, que pode capturar todo tipo de tráfego de rede, decodificar e exibir os datagramas a medida que eles forem coletados ou armazenando os datagramas em arquivos binários para uma posterior investigação. Na figura 5 temos um exemplo do programa, utilizado como um *snifer*, capturando todo o tipo de tráfego de rede entre um ponto de rede com acesso ao tráfego de rede do sistema suspeito.

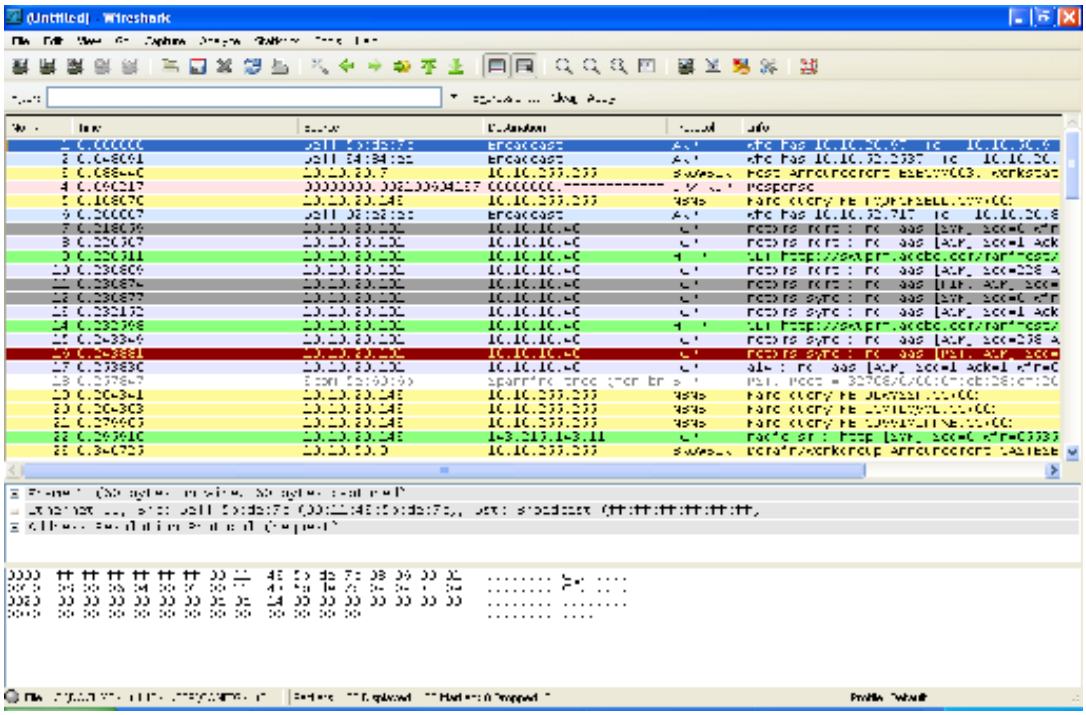


Figura 9 – Captura do trafego de rede pelo Wireshark

O *Wireshark* possui um conjunto de filtros que permite selecionar os datagramas que devem ser capturados, como no exemplo a seguir que foi utilizado um filtro para buscar somente requisições TCP ou UDP na porta 80 do sistema suspeito. Mais informações sobre o filtro do programa pode ser encontrado em sua documentação, [ETHERAL,___a].

Analisando os datagramas capturados pelos *sniffers*, podemos obter evidências como [ARGOLO, 2005]:

- Endereço de IP inválido ou suspeito;
- Tráfego em portas desconhecidas;
- Tráfego em portas ou serviços que não deveriam estar acontecendo;
- Datagramas com opções, *flags* ou tamanhos que não respeitam os padrões dos protocolos (*Request for Comment - RFC*);

- *Flood* de datagramas na rede;
- Tráfego de TCP em portas incomuns;

5.3.3 Processos em execução

A análise dos processos em execução para a investigação é de suma importância, pois indicam o estado atual do comportamento naquele dado momento. Os processos em execução podem ser modificados pelo intruso, no intuito de aumentar o nível de acesso ao sistema.

Os processos em execução relacionam diversas formas de descobrir informações para a investigação, como o comando executado, arquivos abertos, consumo de recursos, entre outros, podendo revelar atividade não autorizadas.

Para a visualização dos processos em execução em sistemas *Windows* pode ser visualizados através do gerenciador de tarefas do *Windows*, essa forma de visualização geralmente é inexata, já que o gerenciador de tarefas lista os processos de execução do *SYSTEM* e conseqüentemente não podemos visualizar todos os processos reais em execução. Para suprir essa falha, o software *PsTools*, utilizado para listar os processos em execução do *Windows*.

Dentro do framework PsTool, existe a ferramenta PsList que mostra os processos em execução. Para executar essa ferramenta é necessário executar o arquivo *PsList.exe*. Nesse comando podemos passar parâmetros que possibilita a visualização de mais recursos.

Tabela 2 – Comando PsList.exe, relacionamento dos parâmetros

Argumento	Detalhamento
-m	Detalhamento da memória.
-d	Detalhamento dos *threads*.
-x	Mostra processos em execução, informação de memória e *threads*.
-t	Mostra a árvore de processos.
-u	Possibilita matar um processo em execução remotamente. Se o usuário utilizado não for administrador do sistema, o investigador deve logar no sistema como qual.
-p	Permite que você especifique o login senha na linha de comando de modo que você pode usar PsList de arquivos em lote.

A saída gerada pela ferramenta *PsList* será uma lista contendo todos os processos correntes no sistema indicado pelo seu número de identificação PID[12].

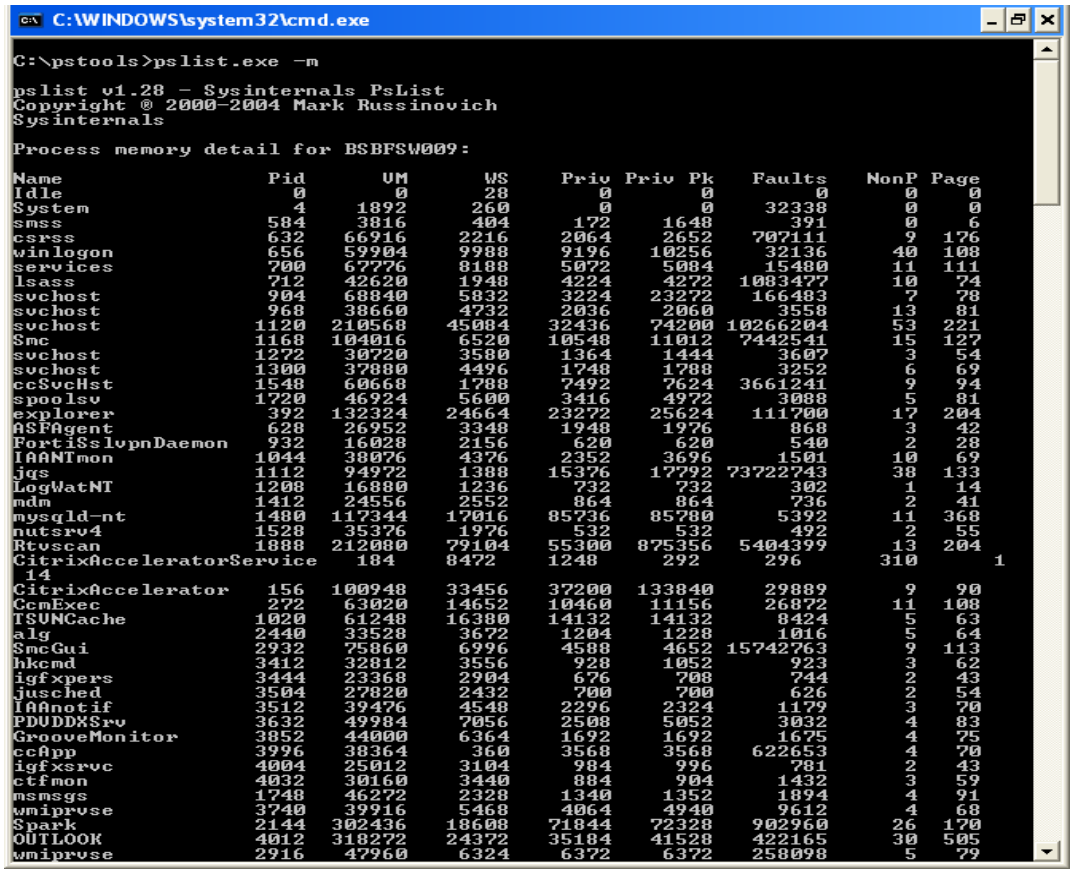


Figura 10 – Ferramenta PsList, utilizando argumento -M

A saída gerada pela execução do comando *pslist.exe –m*, no qual utilizamos o argumento *–m*, contém todos os processos em execução identificados pelo *PID* e o detalhamento da memória. Na coluna *VM* (*Virtual Machine*) demonstra o consumo da memória virtual, na coluna *PRIV* (*Private Virtual Memory*) e *PRIV PK* (*Private Virtual Memory Peak*).

Com todas as informações geradas acerca dos processos em execução citados anteriormente, possibilita a identificação de situações que podem ser evidências de uma intrusão [ARGOLO, 2005]:

- Existência de processos com nomes suspeitos;
- Acesso a arquivos suspeitos ou não permitidos;
- Ausência de processos que deveriam estar sendo executados;

[12] Process Identifier

- Informações inconsistentes entre o comando *pslist* e o *core file*;
- Processo em execução em portas suspeitas;
- Processo com usuário alterado;
- Consumo de recurso incomum ao processo relacionado;

5.3.4 Interface e conexões de rede

Intrusos para coletarem dados dos sistemas alvos podem instalar programas *sniffers*, com o intuito de capturar algum datagrama que contenha senha ou um dado essencial para seu ataque, por isso é importante analisar as interfaces de rede.

Analisando as interfaces de rede o investigador pode se deparar com interfaces sendo executada no modo promíscuo. Dizer que uma interface opera no modo promíscuo significa que todos os datagramas serão recebidos pela interface, mesmo que não sejam endereçadas a esta interface. Caracterizando assim a existência de um *sniffer*.

O estado de rede provê informações valiosas para a investigação a cerca de conexões de rede em andamento e dos processos aguardando uma conexão [WARREN; KRUSE, 2002] A partir dessas informações é possível do investigador determinar se o intruso utilizou de recursos como *back doors*, ou se existe alguma conexão suspeita ou em andamento. Ao executar o comando **netstat**, no *prompt* de comando do *Windows*, é possível capturar informações sobre o estado da rede e portas abertas do sistema.

Assim como vário comandos executados no *prompt* de comando, o **netstat** pode receber parâmetros. A opção ***–a*** permite a visualização de todas as conexões de rede e o número de identificação do processo (*PID*), ***–p*** permite a visualização do nome do programa associado a cada conexão de rede, ***-t*** e ***–u*** informa que somente serão exibidas conexões *TCP* e *UDP*, respectivamente, ***-n*** desabilita a conversão de nomes para endereços *IP*.

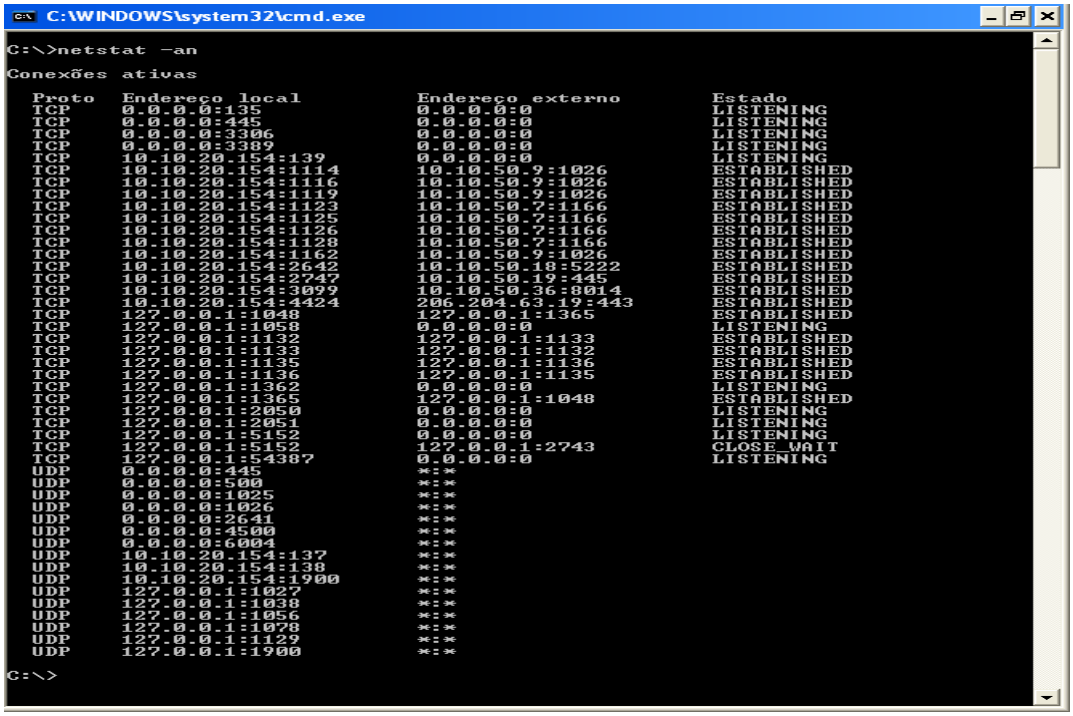


Figura 11 – Comando NETSTAT, utilizando o argumento -AN

Através do resultado gerado pelo comando **netstat** o investigador pode obter informações que podem ajudar na investigação como [ATÍLIO, 2003]:

- Ausência de serviços que deveriam estar habilitados;
- Presença de serviços que deveriam estar desabilitados;
- Serviços estabelecendo conexões suspeitas;
- Endereço de IP suspeitos;

5.3.5 Módulos de *Kernel*

O investigador deve analisar os módulos *kernel*, pois intrusos podem inserir dentro do *LKM* (l*oadable kernel modules*) módulos maliciosos comprometendo o funcionamento do sistema. O intuito do intruso em adicionar um módulo *kernel* malicioso no sistema é o de esconder suas atividades de possíveis ferramentas de auditoria.

Módulos maliciosos podem comprometer o funcionamento do sistema operacional, interceptando comandos e gerando resultados falsos. Comandos como o **netstat** pode ser interceptado, pelo módulo malicioso, e produzir resultados falsos para enganar a investigação.

Como as aplicações trabalham no chamado espaço de usuário (*user space*), chamando funções do espaço de *kernel* (*kernel space*), qualquer informação adulterada no núcleo do sistema passará despercebida pela aplicação. Entretanto, a identificação desses módulos maliciosos representa uma evidência de intrusão [ATÍLIO, 2003].

5.3.6 Dispositivos de armazenagem secundária

Esse procedimento se destina a análise do sistema suspeito desligado, possuindo somente memória não volátil, CD-ROM, disco rígido como exemplo. O disco representa a maior fonte de informação para o exame forense [SAMMES; JENKINSON, 2000], representando assim a etapa mais lenta da análise.

O primeiro procedimento a ser realizado é a construção de imagens do disco original, preservando-o. É aconselhado que seja feito ao menos duas imagens do disco original, uma das imagens para realizar a análise e a outra para garantir que se algo acontecer à primeira imagem, o disco original não será utilizado.

5.3.6.1 Analisando sistema de arquivos

O sistema de arquivos é a porção do sistema operacional responsável por organizar as informações do disco na forma de arquivos [SILBERSCHATZ, 1998].

Após o investigador ter realizado a imagem do disco original, e ter armazenado o original em local de acesso restrito, a próxima etapa é começar a analisar o sistema de arquivo. Todo processo de análise do sistema de arquivo deve ser feito na imagem, relembrando que a imagem é uma cópia exata do original.

No processo de análise dos sistemas de arquivos, a imagem do disco deve ser montada de forma a ter acesso aos diretórios e arquivos, somente com permissão de leitura, evitando que alterações indesejáveis sejam feitos e o processo de análise invalidado.

A tabela 3 mostra as principais fontes de informações contidas no sistema de arquivos [DOS REIS, 2003]:

Tabela 3 – Informações contidas em sistema de arquivos

Fonte de informação	Descrição
Arquivos de configuração	O sistema Linux possui certos arquivos de configuração comumente acessados e/ou alterados pelos atacantes em seu benefício.
Diretórios temporários	Os diretórios temporários /tmp e /usr/tmp servem como diretórios de "rascunho" para todo o sistema. Eles costumam ter seus conteúdos apagados freqüentemente pelo próprio sistema. Outra característica desses diretórios, por padrão, é a permissão de escrita para todos os usuários.
Diretório de arquivos de dispositivos	Com exceção do arquivo *MAKEDEV*, o diretório */dev* deve conter apenas os arquivos de dispositivos (*device files*)
Arquivos e diretórios escondidos ou não usuais	Arquivos e diretórios ocultos ou com nomes incomuns são freqüentemente criados pelos atacantes com intuito de esconder sua presença.
Executáveis e bibliotecas	Arquivos executáveis e bibliotecas são alterados pelos atacantes para esconder sua presença.
Arquivos de log	Arquivos de log registram, por exemplo, atividades dos usuários, processos, conexões, entre outros, representando assim, um papel crucial na análise do sistema de arquivos, pois permite a reconstituição de fatos que ocorreram no sistema.

5.3.6.2 Arquivos de configuração

Os sistemas operacionais possuem arquivos de configuração que são comumente alterados pelo intruso. Essas alterações têm como objetivo do intruso esconder seus rastros, criação de meios que permita o seu retorno, entre outros.

De acordo com César Eduardo Atílio, os arquivos desse gênero que merecem destaque são relacionados ao controle de acesso a máquina, como configuração de *firewall*, sistemas de *log*, configuração de usuários/grupos e scripts de inicialização.

O investigador ao realizar uma análise do sistema suspeito, nos arquivos de configuração, exige uma atenção especial para entender qual foi a verdadeira intenção do intruso ao comprometer o sistema.

5.3.6.3 Diretórios temporários

Os sistemas operacionais como *Windows* e *GNU/Linux*, criam arquivos temporários para o seu uso. Por padrão, os sistemas *GNU/Linux* possuem dois diretórios temporários: /var/temp e /temp. Os sistemas Windows armazenam seus arquivos temporários na pasta: X:\Documents and settings\<NomeDoUsuário>\Configurações locais\Temp.

Os arquivos temporários são excluídos temporariamente do sistema operacional, tem arquivos temporários que não são excluídos, acabam se tornando locais de armazenamento de dados que não serão utilizados posteriormente. Por esse motivo, muitos intrusos acabam utilizando esse espaço em disco como diretórios de trabalho, não se importando em excluir seus rastros.

A investigação dos arquivos temporários e de suma importância, pois nesses diretórios podem conter evidências de intrusões, como código fonte, *malwares*, entre outros.

5.3.6.4 Diretório de arquivos de dispositivos

Os sistemas operacionais possuem diretórios vários arquivos de configuração, sendo pouco acessado pelos administradores, já que esses diretórios são utilizados pelo sistema operacional, podemos destacar para o sistema *GNU/Linux* o diretório ***/*dev**.

Esse diretório por ser pouco acessado pelo administrador do sistema torna-se interessante para o intruso. O intruso pode guardar arquivos maliciosos nesses diretórios, sem que tenha uma atenção particular do administrador.

O investigador deve analisar cuidadosamente esses diretórios, arquivos exclusivos desse local podem ter sido alterados durante uma intrusão, modificando o arquivo. Com isso o investigador deve analisar a legibilidade de cada arquivo encontrado nesses diretórios.

5.3.6.5 Arquivos e diretórios escondidos ou não usuais

Normalmente os intrusos criam arquivos ocultos ou com nomes poucos usuais, para armazenaram arquivos maliciosos ou suas informações.

No sistema *Windows* a opção de visualizar arquivos ou diretórios ocultos ficam desabilitados, por padrão. Para visualizar esses arquivos/diretórios é preciso modificar a configuração do modo de exibição das pastas.

No sistema *GNU/Linux*, podemos utilizar o comando **cat** com o parâmetro –A, que marca o final de linha com o caractere “$” e permite a visualização de caracteres especiais.

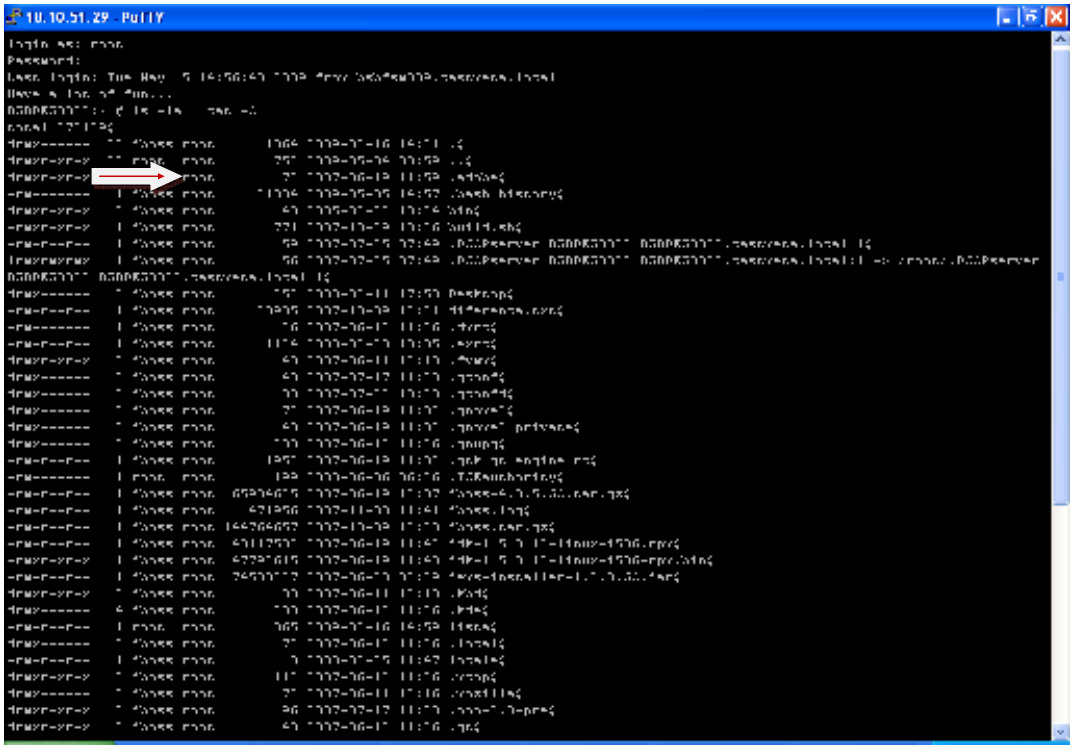


Figura 12 – Comando cat, utilizando o argumento -A

É crucial na investigação a procura de arquivos ou diretórios ocultos, podendo utilizar esses dois métodos demonstrados anteriormente, assim esses arquivos não passam por despercebido pela análise.

5.3.6.6 Executáveis e bibliotecas

O intruso ao realizar o ataque pode instalar *back doors*, *malwares* ou qualquer outro tipo de arquivos maliciosos, para um futuro ataque ou esconder seu rastro no sistema alvo.

Esses arquivos instalados pelo intruso geralmente modificam arquivos de bibliotecas ou executáveis que são carregados dinamicamente. Muitos intrusos podem deixar os arquivos maliciosos no sistema suspeito, esses arquivos podem ser utilizados na investigação para análise em busca de informações sobre a intrusão.

O investigador deve localizar todos os executáveis e bibliotecas do sistema, isolar aqueles que julgarem suspeitos e examinar cada um para verificar se são legítimos [ATÍLIO, 2003].

5.3.6.7 Arquivos de *log*

Os arquivos de log representam um papel crucial na análise do sistema de arquivos, pois permitem a reconstituição de fatos que ocorreram no sistema.
Tais arquivos podem registrar, entre outras informações, as atividades dos usuários, dos processos e do sistema, as conexões e atividades da rede, e informações específicas dos aplicativos e serviços [ARGOLO, 2005].

No caso do GNU/Linux, o programa responsável por registrar as atividades do sistema é o *syslogd* e a maioria dos arquivos de *log* fica dentro do diretório /var/log [ATÍLIO, 2003]. A tabela a seguir demonstra os principais arquivos de *log* de um sistema *GNU/Linux*.

Tabela 4 – Principais arquivos de log, sistemas GNU/Linux. (Fonte: Argolo, 2005)

Arquivos de log	Descrição
utmp	Registra os usuários que estão conectados naquele momento no sistema. É o arquivo acessado pelos comandos **w**, **who**, **finger**, por exemplo.
wtmp	Registra as conexões (login) e desconexões (logout) do sistema. É acessado através do comando **lastlog**, por exemplo.
btmp	Registra as falhas de conexão. Pode ser acessado pelo comando **lastb**.
messages/syslog	Registra eventos e informações do sistema e aplicativos.
boot.log/dmesg	Registra as mensagens relativas ao processo de inicialização do sistema.
secure	Mensagens privadas de programas e autorização de usuários são registrados nesse arquivo.
sulog	Registra o uso do comando **su**
Arquivos de históricos	Arquivos como **.history**, **.bash_history**, entre outros, registram o histórico dos comandos que foram executados por cada usuário. Esses arquivos podem ser encontram no diretório pessoal do usuário.

Os arquivos de *logs* apresentado na Tabela acima podem possuir nomes e funcionalidades diferente do apresentado e localização em outros diretórios. Isso depende da configuração do arquivo *syslogd*, por padrão encontra-se no diretório **/etc/syslog.conf**. Com essa informação o investigador pode entender como foi construído a estrutura de *log* do sistema suspeito.

Em um sistema *Windows* encontramos os arquivos de *log* na pasta que o sistema operacional foi instalado. Nos sistema *Windows* deve informar quais eventos queremos auditar. Para isso é preciso habilitar a configuração de *logs*, acessando

Ferramentas Administrativa, no painel de controle, acessa o ícone *Diretiva de Segurança Local*. Na janela de configurações locais de segurança disciplinamos os eventos que queremos auditar, e ainda em qual modalidade utilizar, sucesso ou falha.

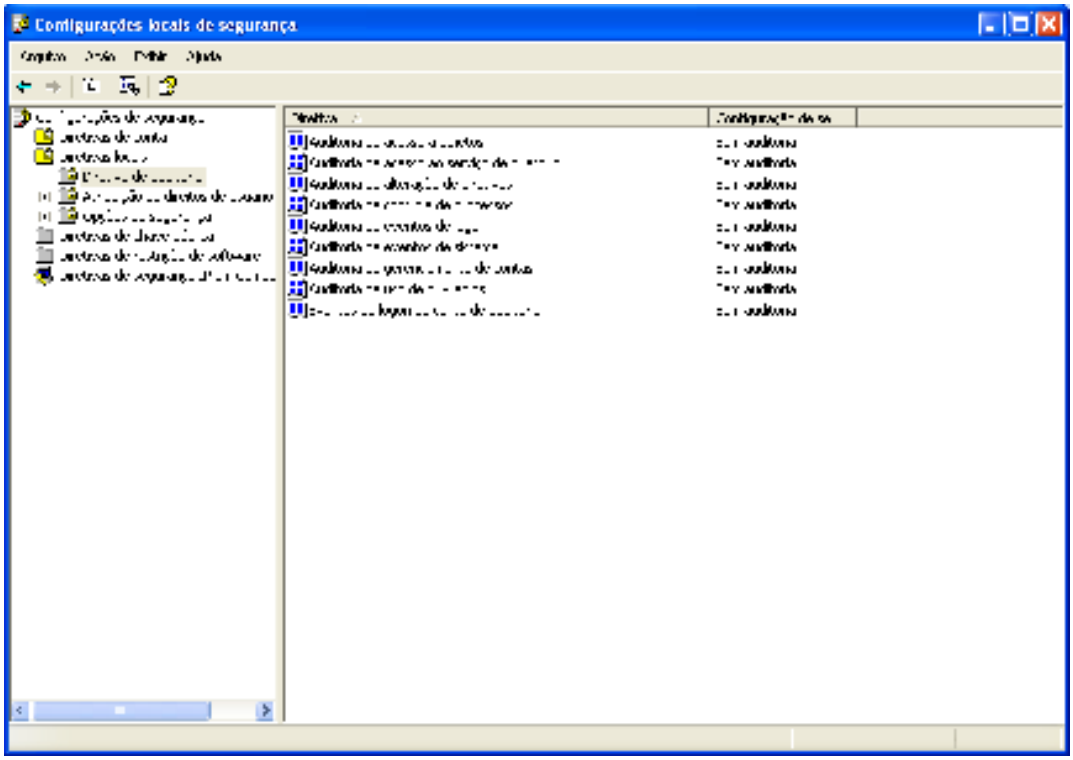


Figura 13 – Diretivas de segurança, sistema Windows

As informações da auditoria podem ser determinantes para a investigação, quando o escopo é quem criou ou apagou arquivos em um disco rígido, quem obteve acesso, ou até mesmo que utilizou um determinado periférico de armazenamento e impressora.

O investigador ao analisar cada arquivo de *log* pode se perder na análise, os arquivos de *logs* contem várias informações. Uma forma de solucionar esse problema é a utilização de programas que percorrem os arquivos de *logs* automaticamente, em busca de padrões específicos de acordo com o especificado pelo investigador. Uma ferramenta que executa esse tipo de varredura é o **swatch**, [SWATCH,___]**.**

5.4 Documentação

A retirada de material do local para posterior análise ou arquivamento deve seguir alguns cuidados básicos, particularmente a contabilização e o registro da cadeia de custódia[13]. [SHIMABUKO, 2009].

O investigador deve se preocupar em registrar quem teve acesso as evidências. O método mais simples é manter uma lista detalhada dos indivíduos que tiveram acesso as evidências, desde a apreensão até a devolução. As informações necessárias como data e a hora da ação, a quem pertencia o material, quem forneceu o material, local da apreensão, descrição completa do material, de quem foram recebidas (necessariamente deve possuir data e hora), a quem foram entregues (necessariamente deve possuir data e hora) e outra informações peculiares ao caso devem ser anotadas e documentadas.

Cada equipamento deve ser detalhado e descrito corretamente. Para um sistema computacional, como o computador, devem ser anotadas suas características externas, como os periféricos externos se houver. As unidades removíveis devem ser documentadas e contabilizadas, em separado. Todo o material deve ser etiquetado e enumerado.

O responsável pelo local deve confeccionar um formulário para registro da cadeia de custódia, [SHIMABUKO, 2009]. Nesse formulário devem constar os seguintes registros:

- Identificação do responsável e local de origem do objeto;
- Identificação do responsável e local de destino do objeto;
- Data e hora da transferência;

Para o Departamento de Justiça norte americano, a documentação é um processo longo de todo o curso de um inquérito. É de extrema importância registrar, com precisão, a localização e a condição dos computadores, suporte de armazenamento e outros dispositivos eletrônicos.

É de forma essencial documentar e observar a cena do crime com detalhes. Detalhar o máximo possível da cena física do local, como a posição do *mouse*, se o mouse estiver à esquerda do computador pode indicar que o usuário é canhoto. Documentar a posição dos elementos um com relação ao outro.

[13] Processo usado para documentar a história cronológica das evidências, garantindo a idoneidade e o rastreamento das evidências utilizadas em processos judiciais

Outros detalhes que devem ser considerados na documentação é o estado inicial dos equipamentos eletrônicos, geralmente computadores têm luzes que indicam se alguma atividade está ativa, ou observar a temperatura do equipamento. Anexar ao documento às fotos retiradas do local, essas fotos devem ser retiradas em 360º de cobertura.

A recuperação das evidências em sistemas computacionais pode ser crucial para a investigação do sistema. Cuidados devem ser tomados para que as evidências sejam recuperadas e essencialmente preservadas. Os itens de uma investigação eletrônica podem estar em elementos de formas distintas, como senhas, escritas em notas manuscrito, fotografias e outros.

Cada tipo de análise pericial deverá ter orientado os tópicos mínimos indispensáveis que deverão conter no laudo pericial. Isso forçará determinadas ações a que os investigadores se dediquem ao próprio exame com mais intensidade, a fim de obter informações precisas e minuciosas que ele terá que abordar e discutir no laudo.

Uma estrutura proposta de laudo pericial pode ser observada abaixo:

I. Histórico: Nesse item deve ser descrito todo o histórico da apreensão do material, a coleta das evidências, os exames realizados e todos os fatos decorridos do inicio ao fim da investigação, nesse item todos os descritivos deve conter data e hora;
II. Do material coletado: Deve ser descrito todo material coletado no local da ocorrência até a entrega do material ao responsável pela análise pericial. Deve conter o dado cadastral do responsável pela coleta e o responsável pela análise;
III. Objetivo dos exames: Deve ser relatado o objetivo do exame a ser realizado, o motivo da escolha do exame e possíveis softwares a ser utilizado;
IV. Considerações técnico-pericial: Deve ser descrito as considerações técnicas e periciais da investigação;
V. Análise executadas: Deve ser descrito o passo a passo da análise realizada, juntamente com data e hora de cada etapa realizada;
VI. Respostas aos quesitos: Devem ser relatadas as respostas aos quesitos da investigação;

VII. Conclusão pericial: Conclusão lógica e técnica do perito, com a indicação se a investigação foi realizada corretamente e as evidências incriminam o intruso;

VIII. Assinatura do perito responsável pelo laudo pericial, contendo data e hora;

6 ESTUDO DE CASO

O estudo de caso foi baseado através de uma reunião com os peritos criminais do Instituto de Criminalística do Distrito Federal, no qual foi perguntado quais exames (análises) mais realizados pelos peritos, após alguns momentos de levantamentos de requisições de análise foi constatado que praticamente 80% (oitenta por cento) dos exames realizados é a recuperação de dados excluídos ou apagados de um disco externo.

6.1 Ferramenta utilizada

No estudo de caso foi utilizada uma ferramenta denominada **HELIX 2009 PRO**. Essa ferramenta é um kit de ferramentas que auxiliam na análise forense computacional.

Essa ferramenta foi escolhida dentre outra ferramenta semelhante, como F.I.R.E (*Forensic Incident Response Environment*), que semelhante ao Helix, é um conjunto de ferramentas formando um kit para a análise forense. Sendo que o Helix é mais completa para a análise forense por conter os mesmos programas utilizado pelo F.I.R.E contém também outras opções de programas.

O Helix 2009 pro é um *live CD*, é um CD que contem um sistema operacional que não precisa ser instalado no disco rígido do usuário que o sistema operacional é executado diretamente do CD [E-FORENSE,___].

Essa ferramenta é multi-plataforma, podendo ser executado em três ambientes distintos, Mac OS X, Linux e Windows. Com uma interface simples e amigável para o investigador e possui as seguintes finalidades:

- Ferramentas básicas para os sistemas operacionais;
- Recuperação de dados;
- Resposta a incidentes;
- Provas de invasão;
- Associação binária estática
- Detecção de vírus;

As finalidades acima citadas são amplamente justificada com a coleção de ferramentas que estão no live CD Helix 2009 Pro, como as ferramentas abaixo:

- Sleuthkit + Autopsy: é um conjunto de ferramentas que permite o investigar o conteúdo de sistemas de arquivos;
- LinEn: é utilizado para a geração das imagens dos discos (CD-ROMs, disco rígidos, disquetes, dentre outros);
- Cryptsetup: ferramenta para encriptografar as imagens dos discos, utilzando o hash;
- WinAudit: ferramenta que análise a configuração de hardware e software do sistema analisado;

6.2 Objeto investigado

Um disco de *nootebook* com capacidade de 160 GiB. Com duas partições distintas, uma com 100 GiB com 37,4% de espaço livre e outra partição com 40 GiB com 37% de espaço livre. A figura 14 exemplifica as partições encontradas no objeto investigado, essa imagem foi retirada utilizando a ferramenta Helix 2009 pro, utilizando o software Driver Manager, utilizado para obtenção de informações de discos rígidos contidos no sistema a ser investigado.

Drive	Label	Type	Size	Used	Available	Bytes Free	Format	Volume Serial	% Free	Visibility
C:		Local Disk	100,47 GB	62,94 GB	37,54 GB	40.307.249.152	NTFS	189C - CEFB	37,4%	Visible
D:	Not mounted	Removable Disk	0,00 MB	0,00 MB	0,00 MB	0		004B - 660C	0,0%	Visible
E:	Not mounted	Removable Disk	0,00 MB	0,00 MB	0,00 MB	0		01AE - A2FC	0,0%	Visible
F:	Helix2008R1	CD / DVD Drive	697,03 MB	697,03 MB	0,00 MB	0	CDFS	50DC - 624B	0,0%	Visible
G:	arquivos	Local Disk	40,91 GB	25,78 GB	15,12 GB	16.239.267.840	NTFS	4AB0 - 5304	37,0%	Visible
H:	Not mounted	CD / DVD Drive	0,00 MB	0,00 MB	0,00 MB	0		01AE - A2FC	0,0%	Visible
I:	Not mounted	CD / DVD Drive	0,00 MB	0,00 MB	0,00 MB	0		01AE - B014	0,0%	Visible
J:	Not mounted	CD / DVD Drive	0,00 MB	0,00 MB	0,00 MB	0		01AE - 4F88	0,0%	Visible

Figura 14 – Partições do objeto investigado

Para o estudo de caso será utilizado à partição de disco G. Essa partição foi criada para a realização do estudo de caso. Assim não afetará o conteúdo do sistema operacional instalado no sistema utilizado como computador forense.

No objeto investigado possui o sistema operacional Windows Vista, com softwares auxiliares demonstrados no gráfico 5, esse gráfico foi retirado utilizando uma ferramenta do live CD *Helix 2009 Pro*, a ferramenta utilizada foi o WinAudit que informa toda a configuração existente no sistema investigado:

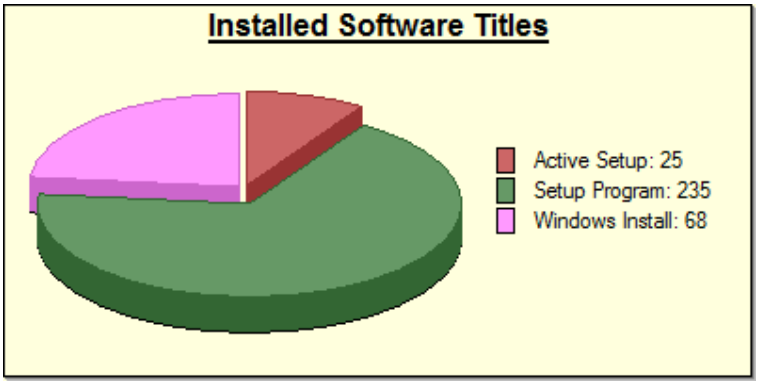


Gráfico 5 – Softwares instalados no Objeto investigado

6.3 Utilização da metodologia proposta

Para o estudo de caso o procedimento de preservação do sistema é suprimido, uma vez que esse estudo de caso é experimental e acadêmico, e na preservação de sistema com estado inicial desligado o investigador deveria fotografar o ambiente em que o sistema se encontra e armazenar todos os equipamentos.

O primeiro procedimento, uma vez que o objeto investigado encontra-se desligado, foi realizar a criação da imagem do disco rígido investigado. Para isso foi utilizado a ferramenta Helix 2009 Pro.

Ao inicializar o computador forense, com o live CD Helix 2009 pro, foi possível utilizar o programa *FTK Imager*, ferramenta que constitui o live CD . A ferramenta *FTK Imager* é utilizada para recuperação, obtenção e geração de imagens dos discos rígidos. Com essa ferramenta foi possível realizar a imagem da partição G, *sda3_img.dd*.

Foi utilizada a opção de criar a imagem em arquivo, devido a sua facilidade de transporte e manuseio, quando comparado com a imagem em um disco rígido.

Assim como a geração da imagem foi gerado um *hash* em *MD5* da imagem. Na estação forense, foi verificado o *hash* da imagem e constatado que o *hash* da imagem idêntico ao do disco original está provado que ambos contém o mesmo conteúdo, conseqüentemente, o que for encontrado na cópia também será encontrado no original.

Após a obtenção e verificação da imagem do original, prossegue o procedimento de montagem da imagem, no servidor forense, para inicializar a análise forense. A imagem do disco deve ser montada de forma a ter acesso aos

diretórios e arquivos, somente com permissão de leitura, evitando que alterações indesejáveis sejam feitos e o processo de análise invalidado.

 # mount -o ro,noexec,nodev,loop /sda3_img.dd /mnt/analise

Os parâmetros acima indicam que a montagem foi feita como somente leitura, impedindo a execução de binários e não interpretando os arquivos de dispositivos. A opção loop é necessária para utilizar os recursos de loop do kernel. Esse procedimento de criação da imagem está descrita na metodologia proposta, no procedimento de coleta de dados especificamente na geração de imagem dos discos rígidos.

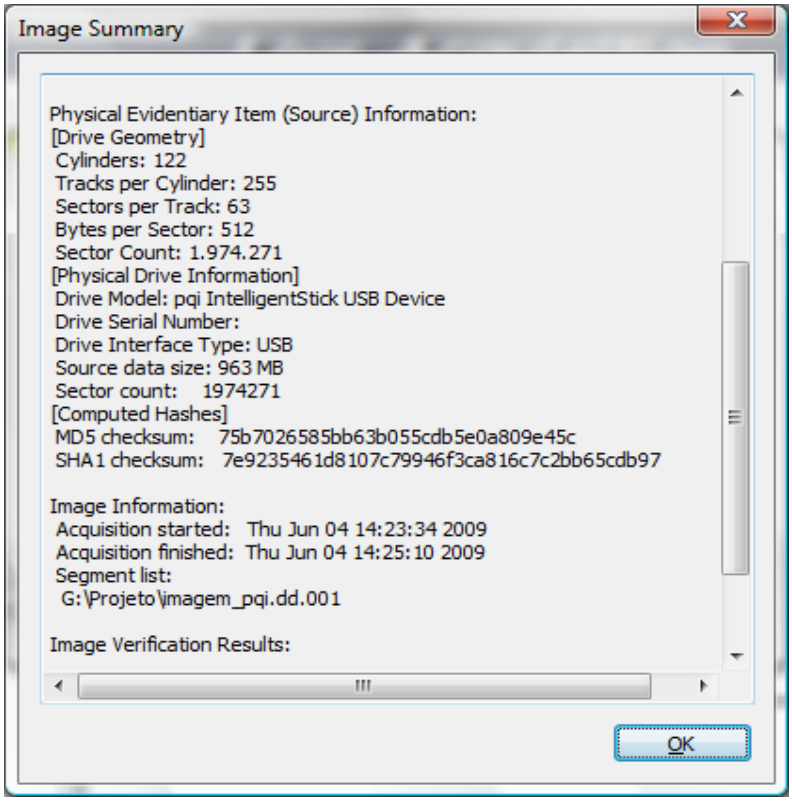


Figura 15 – Resumo da geração da imagem

Esse procedimento de criação da imagem está descrita na metodologia proposta, no procedimento de coleta de dados especificamente na geração de imagem dos discos rígidos originais.

O próximo passo a ser seguido é realizar a análise *post mortem*, procedimento basicamente realizado sobre meios de armazenamento permanente, exemplo discos rígidos ou *pen drive*. Essa análise pode ser dividida em duas etapas, a geração da imagem que é realizada na coleta e preservação do ambiente, já

descrita acima e na segunda etapa a pesquisa e recuperação de dados em sistemas de arquivos.

Para essa pesquisa e recuperação de dados em sistemas de arquivos será utilizada a mesma ferramenta utilizada para a geração da imagem do original, o *FTK Imager*. Essa ferramenta proporciona uma interface amigável e de fácil utilização, a primeira etapa é adicionar uma nova evidência ao *software*, será utilizado à imagem criada anteriormente e verificada com o *hash*.

Adicionado a imagem ao analisador de arquivos é apresentada uma árvore de diretórios, contendo todas as partições contidas na imagem. Ao selecionar a raiz do diretório da imagem gerada é possível analisar os dados excluídos ou presentes no objeto investigado. Outro ponto importante na análise do sistema de arquivos utilizando essa ferramenta é observar o campo que contem dados em hexadecimal, assim como a máquina investigada interpreta os dados, quando apresentado os dados em hexadecimal nos informa que esse arquivo está presente no objeto investigado, do contrário nos indica que o arquivo foi excluído do objeto investigado.

No campo a direita, onde demonstra os arquivos identificados no objeto investigado aparecem os arquivos e diretórios ainda presentes, seja ele ativo ou excluído, os dados excluídos são apresentados com um ícone “X” de exclusão. Como observado na figura abaixo:

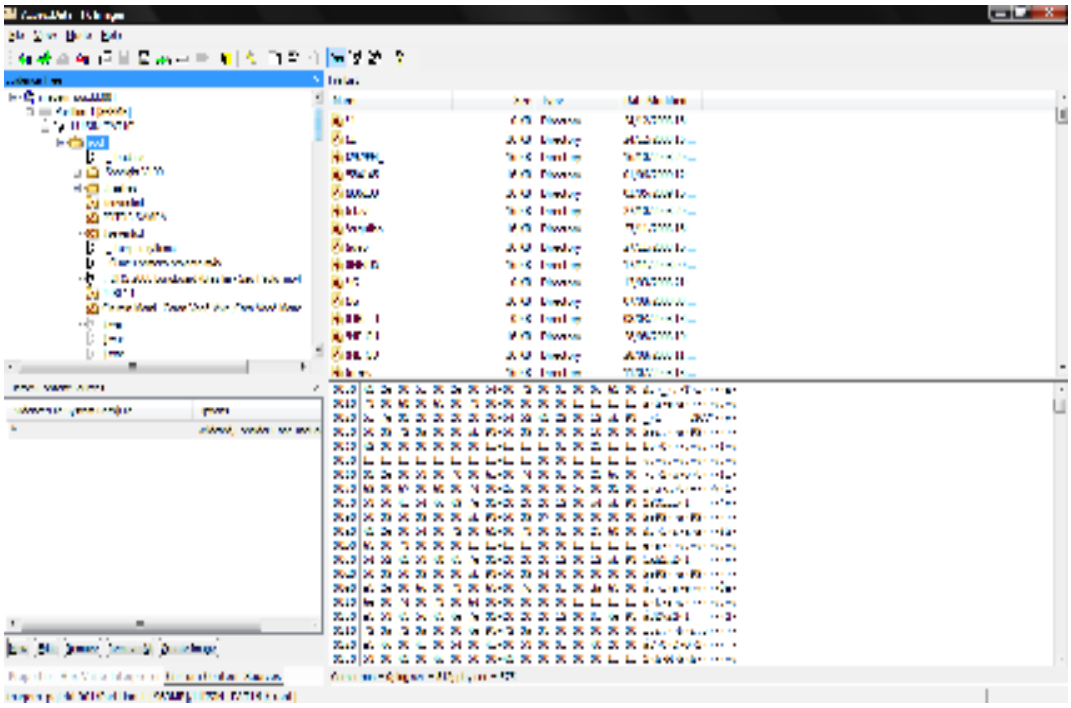


Figura 16 – Analisando o sistema de arquivos

Os arquivos são excluídos temporariamente do sistema operacional, tem arquivos temporários que não são excluídos, acabam se tornando locais de armazenamento de dados que não serão utilizados posteriormente. Por esse motivo muitos intrusos acabam utilizando esse espaço em disco como diretórios de trabalho, não se importando em excluir seus rastros.

A investigação dos sistemas de arquivos e de suma importância, pois nesses diretórios pode conter evidências de intrusões, como código fonte, *malwares*, entre outros.

Outra ferramenta de análise do sistema de arquivos, utilizando a análise *post mortem* e de acordo com a metodologia proposta é a utilização do software *ZeroView*, encontrado no pacote de ferramentas do live CD *Helix 2009 Pro*. Essa ferramenta nos informa de forma hexadecimal o conteúdo da imagem gerada.

Ao processar o programa *ZeroView*, é possível verificar que o objeto investigado está no formato *NTFS* e possui somente uma partições de disco, de acordo com o estudo de caso que é realizado em cima somente de uma partição do disco rígido, como demonstrado na figura abaixo.

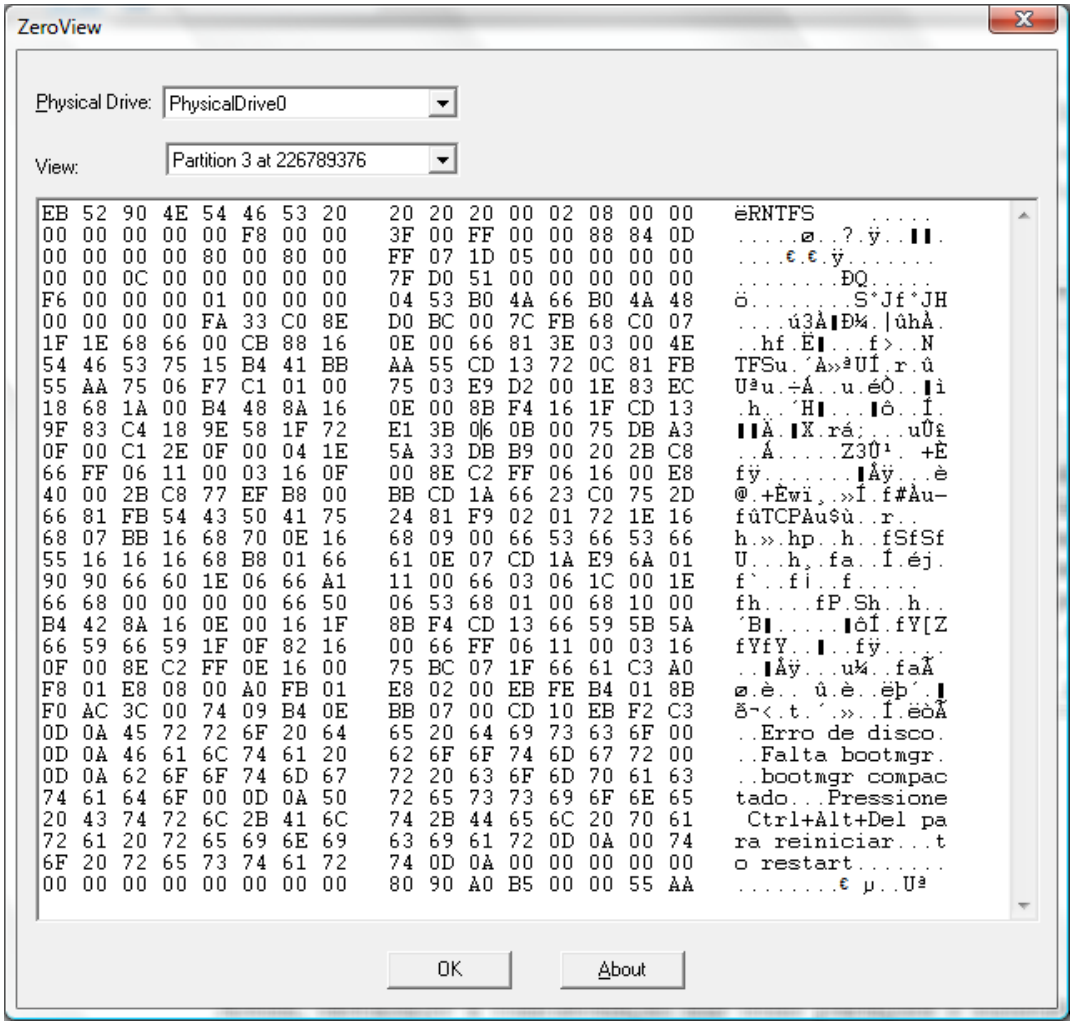


Figura 17 – Setor de Boot do NTFS.

6.4 Resultados obtidos

Foi possível realizar de forma coesa e eficaz, a implementação da metodologia proposta com o estudo de caso apresentado. O estudo de caso compreende e manipula os dados, e compreende a realidade do Distrito Federal em análises de sistemas computacionais, uma vez que o estudo de caso foi idealizado de acordo com os exames realizados na Polícia Civil do Distrito Federal (PCDF).

A metodologia proposta compreende a aquisição, preservação, identificação, extração, restauração, análise e documentação de evidências computacionais. Assim o propósito da metodologia é a procura e extração de evidências relacionada com o caso investigado, permitindo conclusões acerca da infração.

Passando pelo processo de preservação do sistema e coleta de dados, independente do estado inicial do sistema. A análise realizada no estudo de caso foi à análise *post mortem*, também utilizada pela PCDF, realizada basicamente em sistemas de arquivos.

Nessa análise foi possível demonstrar o grande auxílio que o live CD Helix 2009 pro proporciona em uma investigação. Por possuir uma interface amigável e de fácil utilização é possível ao investigador realizar a análise.

Para finalizar, conclui-se que a metodologia proposta é usual e compreende a realidade do Distrito Federal, para investigações computacionais e incrementa a metodologia existente. Com o auxílio da ferramenta foi possível realizar a investigação, não precisando instalar nenhuma ferramenta no computador forense, uma vez que se utilizou um live CD completo para a investigação.

7 CONCLUSÃO

Com os avanços tecnológicos na troca de informações entre pessoas, corporações e empresas, os crimes relacionados à informática se espalharam. Os distintos tipos de se realizar a intrusão continuarão a aumentar nos próximos anos, muitas empresas oferecerão treinamentos na aquisição, examinação e na utilização correta das evidências eletrônicas.

O campo de Análise Forense aplicada a sistemas computacionais continuará a crescer e se desenvolver compreendendo as empresas com profissionais treinados para realizar todos os procedimentos da perícia forense, com o afinco de combater ameaças internas e externas a suas corporações, além de analisar e preparar procedimentos protetores para as empresas.

A busca por materiais para essa monografia mostra a dificuldade que é o tratamento de questões de segurança e a aquisição de fontes, principalmente quando falamos de crimes na internet.

A metodologia proposta buscou pontos fortes das duas metodologias estudadas, a respeito dos procedimentos apresentados por ambas, como preservação do sistema, coleta de dados, análise das evidências e reconstrução dos eventos. Com o estudo de duas outras metodologias apresentadas nesse estudo, foi possível apresentar peculiaridades entre ambas e aproveitar os pontos positivos e o inter-relacionamento de ambas.

A utilização da ferramenta demonstrada no estudo de caso pode auxiliar na investigação disponibilizando um conjunto de ferramentas úteis para os investigadores, seja na análise ao vivo ou *post mortem*.

Portanto, pode ser constatado que a metodologia proposta é eficiente, prática e de fácil utilização aos peritos criminais, que possibilita uma série de procedimentos com o melhoramento e praticidade de duas outras metodologias.

7.1 Trabalhos futuros

Finalmente registra-se a pretensão futura:

i. Ajustar a metodologia à padronização forense;
ii. Realizar um estudo da legislação brasileira e comparar com as análises da metodologia proposta;
iii. Utilizar a metodologia em um estudo de caso mais complexo; e
iv. Realizar estudo de caso com componentes de armazenamento com principio de memória *flash;*

REFERÊNCIAS

[ANDERSON, 1972] ANDERSON, James P. "**Computer Security Tecnology Planning Sudy***"*. Volume 2. Divisão de Sistemas Eletrônicos. Out, 1972. Disponível em: http://seclab.cs.ucdavis.edu/projects/history/papers/ande72.pdf - Visitado em: Mar, 2009.

[ARGOLO, 2005] ARGOLO, Frederico Henrique Böhm. "**Análise Forense em sistemas GNU/Linux**". Rio de Janeiro: RJ, 2005, 111f. Projeto Final em Tecnologia da Informação, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2005.

[ATÍLIO, 2003] ATÍLIO, César Eduardo. "**Padrão "ACME" para análise forense de intrusões em sistemas computacionais**". São José do Rio Preto: SP, 2003, 64f. Projeto Final em Tecnologia da Informação, Departamento de Ciência de Computação e Estatística do Instituto de Biociências, Universidade Estadual Paulista Júlio de Mesquita Filho, São Paulo, 2003.

[BARROS; LEHFELD, 2000] BARROS, Aidil Jesus Paes; LEHFELD, Neide Aparecida de Souza. "**FUNDAMENTOS DE METODOLOGIA: UM GUIA PARA A INICIACAO CIENTIFICA**". 2 º Edição. São Paulo: MCGRAW-HILL, 1986.

[BRASIL, 1941] BRASIL. Decreto-Lei no 3.689, de 03 de outubro de 1941. Código de Processo Penal. 1941. Disponível em: <http://www.planalto.gov.br/ccivil_03/Codigos/quadro_cod.htm>. Visitado em: Mar, 2009.

[CANSIAN, 2000] Cansian, A. M. "**Crime na Internet: Panorama atual**". SSI 2000: Simpósio Segurança em Informática. São José dos Campos. SP. Outubro 2000.

[CASEY, 2000] CASEY, E. "**Handbook of Computer Crime**". Academic Press. San Diego. California. 2000.

[CASEY, 2001] CASEY, Eoghan; "**Handbook of Computer Crime Investigation - Forensic Tools an Technology**". Academic Press; 1ª Edição; 2001;

[*CGI.br*, 2008] "**Comitê Gestor da Internet no Brasil***"*. Disponível em: <*http://www.cgi.br*>. Acessado em: MAr, 2009.

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

[E-FORENSE,___] "***E-Forense****"*. Disponível em: <http://www.e-fense.com/helix3pro.php>. Acessado em: Abr, 2009.

[ETHERAL,___] "***Wireshark****"*. Disponível em: <*http://www.ethereal.com/download.html*>. Acessado em: Mai, 2009.

[ETHERAL,___a] "**Interactively dump and analyze network traffic**". Disponível em: <http://www.ethereal.com/docs/man-pages/ethereal.1.html>. Acessado em: Mai, 2009.

[FARMER; VENEMA, 1999] FARMER, D., VENEMA W. "**Computer forensics analysis class handouts***"*. Disponível em: <http://www.fish2.com/forensics/class.html>. Acessado em: Mai, 2009.

[FBI, 2009] FEDERAL Bureau of Investigation Home Page; Disponível em: <http://www.fbi.gov>. Acesso em: Abril/2009;

[FREITAS, 2003] FREITAS, Andrey Rodrigues de. "**Perícia Forense Aplicada à Informática**". IBPI, Janeiro de 2003. Trabalho de curso de pós-graduação em Tecnologia da Informação.

[GEUS, 2002] GEUS, P. L., Reis, M. A. "**Análise forense de intrusões em sistemas computacionais: técnicas, procedimentos e ferramentas**". Anais do I Seminário Nacional de Perícia em Crimes de Informática. Maceió. AL. 2002.

[JONES; ROSE, 2006] JONES, Keith J., BEJTLICH, Richard., ROSE, Curtis W. "**Real digital forensics: computer security and incident response**". Upper Saddle River: Addison-Wesley, 2006.

[LAUF, 2003] LAUFER, Rafael P. "**Introdução a Sistemas de Detecção de Intrusão**". Disponível em: <http://www.gta.ufrj.br/grad/03_1/sdi/sdi-1.htm>. Acessado em: Mar, 2009.

[MAIA; REHEN, 2005] MAIA, Igor da Silva Neiva., REHEN, Sandro Herman Pereira. "**Sistema de Prevenção de Intrusão baseado em software livre: Derbian e Snort.**", Disponível em: <http://www.scribd.com/doc/13224983/Sistemas-de-Prevencao-de-Intrusao-baseado-em-Software-Livre-Igor-Neiva-e-Sandro-Herman-UCB>. Acessado em: Mar, 2009.

[MITNICK; SIMON, 2003] MITNICK, Kevin D., SIMON, William L. "**A Arte de Enganar: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação**". 1º Edição. São Paulo: Pearson, 2003.

[MITNICK; SIMON, 2005] MITNICK, Kevin D., SIMON, William L. "**A Arte de Invadir: As verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos**". 1º Edição. São Paulo: Pearson, 2005.

[NIST, 2003] *National Institute of Standards and Technology*. FIPS 180-3 secure hash standard (SHA). U.S. Department of Commerce. 2008. Disponível em: <http://csrc.nist.gov/publications/PubsFIPS.html>. Acessado em: Abr, 2009.

[NOBLETT, 2000] NOBLETT, Michel G., POLLITT, Mark M., PRESLEY, Lawrence A. "**Recovering and Examining Computer Forensic Evidence**". Forense Science Communications, Federal Bureau of Investigation; Outubro 2000, Vol. 2 N.4.

[OLIVEIRA, 2001] OLIVEIRA, Flávio de Souza., REIS, Marcelo Abdalla dos., CARDOSO, Célio Guimarães., GEUS, Paulo Lício; "**Forense Computacional: Aspectos Legais e de Padronização**". 9º Simpósio de Computação Tolerante a Falhas - I Workshop em Segurança de Sistemas Computacionais (WSeg'2001); p. 80-85; Florianópolis, Santa Catarina, Brasil; março 2001;

[OLIVEIRA, 2002] OLIVEIRA, Flávio de Souza. "**Resposta a Incidentes e Análise Forense para Redes Baseadas em Windows 2000**"**.** Campinas: SP, 2002, 144f. Dissertação de Mestrado, Instituto de Computação, Universidade Estadual de Campinas, São Paulo, 2002.

[SAMMES; JENKINSON, 2000] SAMMES, T., JENKINSON, B. "**Forensic Computing: A Practitioner's Guide**". Springer. London. UK. 2000.

[SHIMABUKO, 2009] SHIMABUKO, Angelo. "**Introdução à perícia em informática**". Março, 2009.

[SILBERSCHATZ, 1998] SILBERSCHATZ, A., GALVIN, P. "**Operating System Concepts**". John Wiley & Sons. New york. 5 Edição. 1998.

[STEPHENSON, 2000] STEPHENSON, P. "**Investigating Computer-related Crime**"**.** CRC Press. Boca Raton. Florida. 2000.

[SWATCH,___] "***Swatch****"*. Disponível em: <http://swatch.sourceforge.net/>. Acessado em: Mai, 2009.

[SYSTERNALS,___] "***Windows Sysinternals****"*. Disponível em: <http://technet.microsoft.com/en-us/sysinternals/default.aspx>. Acessado em: Mai, 2009.

[TANENBAUM, 1997], TANENBAUM, Andrew S. "**Redes de Computadores***"*. 5º edição. Rio de Janeiro: Campus, 1997.

[THORTON, 1997] THORTON, J. “**The general assumptions and rationale of forensic identification**”. Modem Scientific evidence, The Law and Science of Expert Testimony, West Publishing Co. Volume 2, 1997.

[ULBRICH; VALLE, 2004] ULBRICH, Henrique Cesar., VALLE, James Della. “**Universidade H4ck3r: Desvende todos os segredos do submundo dos hackers**”. 4º Edição. São Paulo: Digerati Books, 2004.

[ULBRICH, 2008] ULBRICH, Henrique Cesar. “**Hackademia: Treinamento 100% prático para desvendar o Submundo Hacker**”. 1º Edição. São Paulo: Digerati, 2008.

[ULBRICH, 2008a] ULBRICH, Henrique Cesar. “**Hackademia: Conheça as táticas do Universo H4ck3r**”. 1º Edição. São Paulo: Digerati, 2008.

[VACCA, 2005] VACCA, John R. “**Computer forensics: computer crime cene investigation**”. 2. ed. Boston: Charles River Media, 2005.

[WARREN; KRUSE, 2002] WARREN G., KRUSE II, Jay G. “**Computer Forensics: Incident Response Essentials**”. Addison-Wesley, Massachusetts, 2002.