FACULDADE UNIBRATEC
BRUNO VINELLI NUNES DE OLIVEIRA ARAÚJO

PROCEDIMENTOS FORENSE PARA ENCONTRAR EVIDÊNCIAS DE CRIME DE PORNOGRAFIA INFANTIL EM COMPUTADORES

João Pessoa
2009

BRUNO VINELLI NUNES DE OLIVEIRA ARAÚJO

PROCEDIMENTOS FORENSE PARA ENCONTRAR EVIDÊNCIAS DE CRIME DE PORNOGRAFIA INFANTIL EM COMPUTADORES

Monografia apresentada no Curso de Segurança da Informação, para conclusão da Pós-Graduação. Ou Como parte dos requisitos necessários para obtenção do título de Especialista em Segurança da Informação.

Orientador: M.S.c. Márcio Luiz Machado Nogueira

João Pessoa

2009

Bruno Vinelli Nunes de Oliveira Araújo

PROCEDIMENTOS FORENSE PARA ENCONTRAR EVIDÊNCIAS DE CRIME DE PORNOGRAFIA INFANTIL EM COMPUTADORES

Data da Defesa:

Msc. Márcio Luiz Machado Nogueira, iDez
Prof. Orientador

Gerson Castro, iDez
Componente da Banca

Msc. Marileuza Fernandes, iDez
Componente da Banca

João Pessoa, 2009.

Dedicatória

Dedico este trabalho primeiramente a Deus, pois Ele me deu à sabedoria para concluir este trabalho...

Como também minha família que estava por perto dando apoio e cuidando do jeito dela, principalmente Minha Avó que me ajudou nos custos dos livros e Minha Mãe que me mostrou com suas atitudes e que sigo como exemplo que estudar é a melhor saída para ser alguém no mundo.

Minha Grande Namorada, Daniele, que me acompanhou todo o processo de início e fim desta especialização e abdicou nossos dias de Sábado para que eu terminasse bem.

E meus Amigos que tanto me apoiaram e acreditaram que eu possa ser um bom profissional nesta área, como Andrey, Ivandro, Paula, Érica e Walter.

A Professora Marileuza pelas aulas motivadoras de como fazer um trabalho de conclusão de curso.
E a todos da Faculdade iDez que sempre nos atenderam com educação e eficiência.

Por último, meu grande orientador Márcio Nogueira, pela enorme paciência, dedicação e orientação, pois se não fosse ele, eu mesmo estaria desorientado e não finalizaria este trabalho.

Agradecimentos

Totalmente Grato a Deus, por tudo: Vida, Saúde e Inteligência.

Agradeço a cada pessoa em que posso confiar, ou apenas tentou me ajudar a concluir este trabalho, que são: Todos da minha turma de Pós-Graduação, principalmente, Ivandro, Márcio Bencid, Moisés, Flávio, Sílvio e Michele, pela ajuda, apoio e brincadeiras

Agradeço mais uma vez a Andrey, Érica e Danielle, por ter feito a correção do trabalho, com muita responsabilidade e dedicação.

Minha namorada Daniele que ouviu falar nessa monografia todos os dias durante quase 1 ano.

A Professora Marileuza, Professor Gerson pelo apoio que nos deram nesta última etapa do curso...

E ao meu Professor e Orientador Marcio Nogueira que sem ele este trabalho não sairia bem polido.

RESUMO

A internet sendo cada vez mais popularizada abre margem para que alguns criminosos virtuais atuem de forma que pensem e ajam como se não houvesse lei e, por isso, acabam escancarando seus atos inescrupulosos como quiserem. Certos comportamentos que antes eram apenas encontros em locais secretos, como os clubes de pedofilia para trocas de material com conteúdo de pornografia infantil, hoje acontece pelo computador, bastando apenas estar conectado à Internet. Este trabalho propõe estudar um padrão de procedimentos para investigar uma estação de trabalho em ambiente com plataforma proprietária, usando ferramentas de software livre como o Linux FDTK-UbuntuBR e o Helix, a fim de investigar as evidências de crime de pornografia infantil pela Internet, baseado nas leis vigentes no Brasil. A metodologia usada foi baseada nos procedimentos demonstrados por Venema e Wietse, Andrey Rodrigues de Freitas e estudos de algumas monografias na área de Perícia Forense Computacional e as ferramentas específicas para que possa fazer uma investigação segura no computador analisado. Sendo finalizada com um experimento fictício de laboratório feito em casa, resultando que se o suspeito não tiver nenhum malware instalado em seu computador e for encontrada arquivos com pornografia infantil, então ele poderá ser condenado de acordo com a lei vigente no Brasil.

Palavras-chaves: pedofilia, forense computacional, cibercrimes.

ABSTRACT

The Internet is increasingly popular open space for some criminal act in a virtual think and act as if there is no law and so eventually gaping as their unscrupulous acts like. Some behaviors that were previously found only in secret places, such as pedophilia clubs in exchange for material with content of child pornography, today is the computer, just be connected to the Internet. This research study proposes a standard of procedures to investigate in a workstation environment with proprietary platform, using free software tools such as Linux and Helix FDTK-UbuntuBR in order to investigate the evidence of a crime of child pornography over the Internet, based on laws in Brazil. The methodology used was based on procedures established by and Wietse Venema, Andrey Rodrigues de Freitas and studies of some papers in the area of Computer Forensic Expertise and the specific tools that can make a secure research in computer analysis. Being finalized with a fictitious laboratory experiment at home, resulting that the suspect does not have any malware installed on your computer and is found files with child pornography, then he may be convicted under the law in force in Brazil.

Keywords: pedophilia evidence, computer forensics, cybercrime

Lista de Tabelas

Lista de Figuras

Glossário

ABIN – Agência Brasileira de Inteligência

BMP(BitMap) – Mapa de Pontos

CD-ROM (Compact Disc - Read-Only Memory) – Disco Compacto de Memória de Somente de Leitura

DOS (Disk Operating System) – Sistema Operacional de Disco

DSM (Diagnostic and Statistical Manual of Mental Disorders) - Manual Diagnóstico e Estatístico de Doenças Mentais

Ext (extended file system) – Sistema de Arquivos Extendido

FAT (File Allocation Table) - Tabela de Alocação de Arquivos

FDTK (Forense Digital ToolKit) – Kit de Ferramentas para a Forense Digital

FTK (Forensics Toolkit) – Kit de Ferramentas Forense

JPEG ou JPG - Joint Picture Expert Group

GPL (*Global Public License*) – Licença Pública Geral

HFS (HTTP File Server download) – HTML Servidor de Download

HTML (HyperText Markup Language) - Linguagem de Marcação de Hipertexto

HW (Hardware) – Parte Física do Computador

MS - Microsoft

NIST (Institute for Standards and Technology) - Instituto Nacional de Padrões e Tecnologia

NTFS (New Tecnology File System) – Nova Tecnologia de Sistema de Arquivos

OCDE - Organização para a Cooperação e Desenvolvimento Econômico

PLC – Projeto de Lei na Câmara

RAM (Randon Access Memory) – Memória de Acesso Aleatório

TCT (The Coroner's ToolKit) – Kit de Ferramentas do Coroner.

TCP (*Transmission Control Protocol) – Protocolo de Controle de Transmissão*

UDP (User Datagrama Protocol) – Protocolo de Datagrama de Usuário

USB (Universal Serial Bus) – Barramento de Serie Universal

WWW (Wide World Web) – A Grande Teia Mundial

Sumário

INTRODUÇÃO

A pedofilia já existe há pelo menos uns 6000 anos, e hoje é considerado um transtorno mental ou um desvio sexual de acordo com a Organização Mundial de Saúde. “A Pedofilia é o desvio sexual caracterizado pela atração por crianças ou adolescentes sexualmente imaturos, com os quais os portadores dão vazão ao erotismo pela prática de obscenidades ou de atos libidinosos” [CROCE, 2004]. E “A pornografia infantil na Internet é um dos crimes mais evidentes no ciberespaço. Tanto localmente quanto internacionalmente” afirma Fábio A. S. Reis (2004. p.1).

E conforme Fábio A. S. Reis, “No Brasil, a Polícia Federal afirma que, dentre os crimes de computador, a pornografia envolvendo crianças responde pelo maior número de denúncias recebidas pela instituição”.

Com o crescimento da Internet este evento, a pedofilia e pornografia infantil pela Internet, ao qual este último se diferencia da pedofilia visto que é uma violação ou crime contra os Direitos Humanos envolvendo uma criança em atividades sexuais explícitas reais ou simuladas ou qualquer representação dos órgãos sexuais de uma criança para fins primordialmente sexuais, tem mais incidência e cresce a cada dia (SaferNet, 2009) e também por causa do anonimato e a dificuldade em que a polícia se encontra e para obter provas lícitas para que se conduza a um ato litigioso de reclusão ou detenção.

Portanto, este trabalho visa propor um procedimento de auditoria para conseguir identificar prova lícitas em uma estação de trabalho, adotando s*oftwares* específicos para investigação do computador suspeito para que assim se possa entrar com um processo judicial.

Ele foi dividido em três partes: os conceitos sobre pedofilia e sua legislação vigente no Brasil, foi mostrado o conjunto de ferramentas usadas em uma investigação em um computador suspeito e finalizando, uma investigação de um procedimento para combater a pedofilia pela Internet através de um ambiente feito em casa em uma máquina virtual para estudar os conceitos aqui mostrados durante o trabalho.

1.1 Motivação

A motivação é estudar o processo forense em si para encontrar vestígios de pornografia infantil em um computador investigando, para que desta forma se inicie um processo judicial com a finalidade de responder perguntas chave, como por exemplo elucidar quem foi o responsável pela colocação de arquivos no computador e quando aconteceu.

Na prática em uma empresa ou um computador pessoal, quando alguém é acusado de algum delito, é necessário o ônus da prova, ou seja, as evidências para garantir se houve um crime. Portanto, este trabalho tem a motivação de ajudar a equipe técnica a avaliar a situação e encontrar esses vestígios ou possa estar com algum tipo de malware.

1.2 Objetivos

1.2.1 Objetivos Gerais

Construir um modelo para um procedimento de análise forense, para estações de trabalhos ou computadores pessoais que usam o sistema operacional da Microsoft (pois este sistema é o mais popular na faixa de idade em que os suspeitos se encontram, entre 30 e 45 anos(RODRIGUES, 2006)) a fim de identificar evidências que conduzam a um processo judiciário de pornografia infantil.

1.2.2 Objetivos Específicos

- ✓ Relacionar critérios previstos em leis contra pedofilia com os procedimentos forense.
- ✓ Relacionar as ferramentas necessárias para atender os procedimentos forenses.
- ✓ Realizar um estudo de caso para verificar a adoção das ferramentas selecionadas.

1.3 Relevância

De acordo com a página eletrônica de denúncias de crimes pela Internet, (Safernet, 2009), afirma que um dos grandes tráfegos da Internet é a pornografia e junto com ela, está inclusa a pornografia infantil e a pedofilia que continua crescendo. Para tentar diminuir, há acordos internacionais, como o da Google que se compromete a cumprir de forma integral a legislação brasileira a cerca dos cibercrimes praticados por brasileiros ou por conexões feitas no Brasil, dando jurisprudência no mundo inteiro. Um desses grandes males é a pornografia infantil, que são apenas trocas de fotos e vídeos, mas nem sempre há o ato sexual, por outro lado a pedofilia sim é um desvio no desenvolvimento da sexualidade, ou seja, uma psicopatologia, segundo a Organização Mundial de Saúde.

Mesmo com todo este cerco contra este tipo de pornografia, há grupos de pessoas que formam um grande mercado consumidor e lucrativo desse tipo de material, de difícil acesso e para serem encontrados, afirma (RODRIGUES, 1999).

Para o perito, ele só poderá agir se ele tiver um mandado de busca e apreensão (Art 5, Inc XI da Constituição Federal de 1988) do computador do suspeito para assim iniciar a coleta, exame, análise para no final obter o laudo técnico e assim sustentar um processo legal contra o acusado.

No final do ano de 2008 o Brasil sancionou o projeto de lei, Nº 11.829, que aumenta a punição contra a pornografia infantil e crimes de abuso sexual envolvendo crianças e adolescentes na Internet que entrou em vigor dia 26 de novembro de 2008. Agora, quem "produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente", deverá enfrentar pena de reclusão, de quatro a oito anos, e multa. E também será punido "quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia", a participação de criança ou adolescente nessas cenas.

1.4 Metodologia da Pesquisa

O trabalho sobre Perícia Forense Computacional foi baseado em procedimentos para encontrar evidências, demonstrados por [VENEMA, WIETSE 2007] em seu livro, Perícia Forense Computacional, teoria e prática aplicada, ao qual eles conceituam sobre a ordem de volatilidade e o MAC times e no livro do [FREITAS, 2006]. Perícia Forense Aplicada à Informática, que ele mostra esta perícia feita em uma estação que tenha o sistema operacional da Microsoft.

Algumas monografias foram estudadas em relação apenas a auditoria de computadores suspeitos de crimes em geral, não apenas com pedofilia.

Foram analisados alguns programas que possam ser utilizados para compor um conjunto de ferramentas para que se tenha uma boa auditoria no computador investigado.

A pesquisa sobre Perícia Forense Computacional foi também feita através de pesquisas na Internet como as páginas eletrônicas da Technet, jurídicas e de organizações não governamentais específicas sobre pornografia infantil e pedofilia.

Citações das leis vigentes no Brasil sobre o assunto de crimes cibernéticos e suas aplicações.

Esse estudo foi baseado nos livros do [VENEMA, WIETSE 2007] e também no de [FREITAS, 2006] iniciando um estudo sobre os procedimentos de como são coletadas, examinadas e analisadas as evidências.

Concluindo, um experimento de laboratório feito em uma máquina virtual privada, inserindo-lhe propositadamente algumas imagens impróprias e, em seguida acessando uma página eletrônica de pesquisa fazendo uma busca com palavras-chave, mostrou que é possível o programa final veja o que foi procurado e baixado na máquina auditada

CAPÍTULO 2 - FUNDAMENTAÇÃO TEÓRICA

Este capítulo trata dos conceitos e procedimentos da perícia forense aplicada na informática e as leis vigentes sobre pedofilia e pornografia infantil no Brasil.

2.1 Crimes de Informática

Conhecidos como cibercrimes, são crimes que atacam as redes de computadores, causando roubo de informações, danificando elementos físicos, como os próprios computadores que estão nestas redes ou fora delas. Ou seja, toda conduta ilegal realizada mediante o uso do computador, desde um simples programa pirata, roubo de senhas de bancos e até troca de fotos de pornografia pela Internet, tudo isso é considerado crime cibernético. E de acordo com a página eletrônica SaferNet Brasil, cibercrimes são práticas criminosas utilizando meios eletrônicos como a Internet. Uso das novas tecnologias para ações ilícitas como roubo, chantagem, difamação, calúnia e violações aos direitos humanos fundamentais.

Este fenômeno de cibercrimes nasceu e cresceu muito rápido, desde quando a Internet começou a se difundir nos anos 90 e até o final desta década. Este problema todo vem mostrar que os criadores dessas ferramentas, que facilitam o uso da Internet, são vulneráveis no nosso dia-a-dia e estão sempre precisando de uma nova camada de proteção e de novas condutas, que possam incriminar atos lesivos às redes e aos computadores que nelas estão inseridos.

> O cibercrime se aplicava a novos tipos de criminalidade, tais como a pornografia na Internet ou a distribuição de fotos com imagens pornográficas que violam a legislação de determinados países (porém não de todos), no que diz respeito ao material que explora a pornografia ou que a apresenta de forma inaceitável. Como a Internet não tem fronteiras, foi ficando cada vez mais fácil para os indivíduos distribuírem materiais para

> além da fronteira de seus países, às vezes sem mesmo deixar rastros de origem. (PERRIN, Stephanie, 2005)

(PERRIN, 2005) também afirma que há 5 tipos de cibercrimes:

1. Crimes contra a confidencialidade, integridade e disponibilidade de dados de computador e sistemas.
2. Crimes relacionados a computadores como falsificação e fraude.
3. Crimes relacionados ao conteúdo: pornografia infantil.
4. Crimes relacionados à infração da propriedade intelectual e direitos conexos.
5. Responsabilidade subsidiária e sanções: esforço e auxílio ou responsabilização corporativa.

De acordo com a OECD, o crime de computador é “qualquer comportamento ilegal, aético ou não autorizado envolvendo processamento automático de dados e, ou transmissão de dados”.

Na doutrina brasileira, há dois tipos de crimes de informática: puros (próprios) e impuros (impróprios). Nos puros os crimes têm a participação direta com o computador ou um meio eletrônico. Já nos impuros o agente se vale do computador para cometer atos ilícitos no mundo físico ou “real”, ameaçando ou lesando outros bens, como a pornografia infantil na Internet.

Alguns crimes que acontecem não têm lei específica, então há uma adaptação direta com o Direito Penal. Por exemplo, ter páginas de Internet de agenciamento de garotas de programa pode ser enquadrado no artigo 228 do Código Penal, que prevê crime no fato de “Induzir ou atrair alguém à prostituição, facilitá-la ou impedir que alguém a abandone”. O assunto principal deste trabalho, o crime de pornografia infantil, se enquadra no artigo 241 do Estatuto da Criança e do Adolescente, consistindo em “Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente”. Também como um texto base, temos a Constituição Federal, servindo de proteção dos bens jurídicos atingidos por meios eletrônicos, podendo também aplicar-se o Código Civil, a Lei dos Direitos Autorais e até o *Habeas Data*.

Contudo, é bom observar que, de acordo com o artigo 72 do Código de Processo Penal, fica estabelecida a competência de foro de domicílio do réu, quando não for conhecido o lugar da infração. Desta forma, por causa da internacionalização da Internet, alguns crimes cometidos no Brasil têm origem em outro país, no qual o acusado deveria teoricamente sofrer as sanções locais. O problema é que muitos dos fatos considerados crimes por aqui, não o são em outros países, e isso dificulta o combate. Desta forma, defende-se que esses crimes sejam padronizados em qualquer lugar do globo, facilitando o seu julgamento.

O artigo 6º do Código Penal brasileiro estabelece: “Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado”.

De acordo com o escritor americano, Richard Spinello, a internet é uma tecnologia global, sem fronteiras e sem donos, sendo quase impossível para qualquer nação garantir a execução de leis ou restrições que se busque impor no ciberespaço.

Se os Estados Unidos, o México ou o Brasil decidirem proibir a pornografia *online*, esses países podem fiscalizar o cumprimento de tal proibição apenas entre os provedores e usuários em seus territórios. Infratores localizados na Europa ou na Ásia não estarão proibidos de disponibilizar material pornográfico na rede, acessível a qualquer pessoa, em qualquer parte, afirma o escritor do livro *Readings in Cyberethics*.

Outro problema é o anonimato, bastante marcante na cultura da Internet, que permite ao usuário assumir a identidade que bem lhe aprouver, inclusive com a utilização de diferentes e-mails, tornando sua identificação ainda mais difícil.

2.2. Legislação Aplicada na Informática

Com esse aumento da criminalidade pelo computador e sem uma legislação adequada em relação a esse cibercrimes, houve uma necessidade de criar leis específicas para este tipo de delito. Em relação do Brasil, o Código Penal é de 1940, ou seja, ainda não existia computador em grande escala e muito menos uma grande rede de computadores, portanto o poder legislativo está tentando criar uma lei que

garanta direitos e deveres de uma pessoa que usa meios eletrônicos, porém seus passos são lentos, enquanto que a tecnologia se evolui cada dia mais rápido. A Internet neste século XXI, praticamente criou um novo tipo de sociedade de pessoas que estão sempre conectadas a ela.

E para que uma sociedade seja bem organizada e harmônica necessita de normas, mesmo que seja ligada aos costumes ou a regras feitas pelo parlamento. Este é um produto da nossa cultura que nasceu há muito tempo, para obter uma segurança das relações interpessoais e internacionais.

Com o passar dos anos, o Direito foi se transformando para se adaptar aos novos costumes da sociedade. Quando chegou à terceira revolução industrial, cuja principal característica é a informação, o atraso, que normalmente existia por conta da mudança mais rápida da sociedade em relação ao direito, aumentou com a velocidade maior das mudanças e continua até hoje a tentativa de acompanhar esta evolução.

Com o advento da Internet, novas questões surgiram para o profissional do Direito, que tem que procurar novas respostas de como resolver estes problemas, uma vez que as leis existentes até então só serviam para o mundo real e não para o mundo virtual. Como encaixá-las para a nova realidade se tornou a questão a ser resolvida. Então, tentando interpretar algumas leis da Carta Magna e assim relacioná-las na doutrina de crimes à distância, como por exemplo:

- O art. 5º, inciso X da Constituição Federal, que diz: "invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação";

Para que infrinja este artigo, há a necessidade que o agente viole a intimidade da vítima, ou seja, algum momento íntimo entre os dois gravam e por vingança o agente coloca este vídeo na Internet e todos vejam e denegrindo a imagem e a honra da pessoa que foi destruída. E se esta pessoa for menor de idade, então além da violação de acordo com o artigo 5º, o executor estará praticando o ato de pornografia infantil, que assim terá um agravante, se for pego e for provado que foi ele.

Porém, um dos grandes mitos da Internet é que ela não podia ser regulamentada pelo Estado e que haveria liberdade absoluta nesse ambiente. Ou seja, uma sociedade anárquica, onde todos podem fazer o que quiserem porque não seriam presos. Ledo engano. Contudo, a Internet, infelizmente, permite a prática de delitos a distância e no anonimato, o que muitas vezes vai contra o afirmado na Carta Magna.

- Art 5º, inciso IV da Constituição Federal, considera que “é livre a manifestação do pensamento, sendo vedado o anonimato”

> Porque, se há lesão ou ameaça a liberdades individuais ou ao interesse público, deve o Estado atuar para coibir práticas violadoras desse regime de proteção, ainda que realizadas por meio de computadores. Isto porque, tanto a máquina quanto a rede, são criações humanas e, como tais, têm natureza ambivalente, dependente do uso que se faça delas ou da destinação que se lhes dê. Do mesmo modo que aproxima as pessoas e auxilia a disseminação da informação, a Internet permite a prática de delitos à distância no anonimato, com um poder de lesividade muito mais expressivo que a criminalidade dita "convencional", nalguns casos. (ARAS, 2001)

2.2.1 Omissão dos Provedores de Internet

Outro problema com a Internet no Brasil é a atuação limitada do Estado e provedores de acesso. Com relação a estes últimos existe um grande problema, pois eles são atuam frequentemente de forma omissa nos casos de crimes, fazendo “vista grossa” e dificultando o trabalho do perito de investigar os fatos.

> “O provedor que não quer ser cúmplice de um crime tem que tomar precauções, perguntando ao usuário o que pretende fazer com seu espaço na Internet, catalogando seus dados a fim de que a investigação chegue à autoria do delito. Ressalte-se, porém, que a cooperação dos provedores de acesso à Internet é de vital importância para identificar os elementos necessários à comprovação da materialidade delitiva e bons indícios de

> autoria, pois é através dos equipamentos pertencentes a esses prestadores de serviços que o usuário divulga sua comunicação ilícita junto à comunidade virtual" (Barros *apud* Nogueira, 2007, p.)

O problema maior é o tempo para a investigação, pois quanto mais tempo se passa, mais difícil fica de encontrar evidências, já que estes rastros podem ser apagados.

O Delegado Mauro Marcelo, ex-diretor Geral da Abin, fala da dificuldade de obter informações desses provedores, relata que precisa de um mandado judicial e que todo esse processo acaba levando geralmente em torno de uma semana, tornando a investigação inviável. Ele acrescenta que no *site* de registros dos domínios FAPESP, há o cancelamento de domínios pela falta de pagamento, mas, quando os domínios são utilizados de forma criminosa, o referido *site* "lava as mãos".

Então, além de uma legislação antiga, como a do Código Penal Brasileiro, não há uma lei da informática, pois os legisladores não entram em acordo para a criação de uma legislação específica para meios eletrônicos, dificultando o trabalho de quem quer uma Internet séria e honesta. E pelo lado dos provedores de Internet e, querem tirar a culpa deles próprios e dificultando a investigação para saber onde foi pego arquivos com conteúdo de pornografia infantil.

Para este trabalho seria que teria um procedimento padrão para garantir que essas provas sejam lícitas e de aquisição das evidências mais rápidas, neste caso, se essas informações estiverem nos banco de dados dos provedores.

2.3 O que é Pedofilia ?

De acordo com o Novo Dicionário Eletrônico Aurélio, a palavra pedofilia vem do grego, e se constitui a partir da união de duas partículas: *Pedo,* que significa infância, criança, juventude, e *Filia,* que é a atração, filiação, amizade, desejo forte e repetido de práticas e de fantasias sexuais com crianças pré-púberes.

A Pedofilia é uma atração sexual compulsiva por crianças e adolescentes e é classificada no DSM IV (*Diagnostic and Statistical Manual of Mental Disorders - Fourth Edition* – Manual de Diagnósticos e Estatísticos de Doenças Mentais – Quarta Edição) (que é a classificação dos transtornos mentais da Associação Americana de Psiquiatria) no item F65.4 – 302.2 no livro de diagnóstico que define estes critérios.

No Brasil não é crime a Pedofilia e sim as conseqüências do ato que são consideradas um crime, como:

- Atentado Violento ao Pudor
- Estupro
- Pornografia Infantil

Porem, só existe pedofilia quando esses crimes forem praticados com criança menores de 12 anos e adolescentes de 13 a 18 anos (Art. 2 da Lei Nº 8069/90). Neste caso, a pedofilia traduz-se juridicamente em crime de estupro (art. 213 do Código Penal Brasileiro) ou atentado violento ao pudor (Art. 214 do Código Penal Brasileiro). Mas no Brasil a pornografia infantil é crime, pela Lei Nº 11.829/08

> A pornografia infantil é uma Violação / Crime contra os Direitos Humanos que significa qualquer representação, por qualquer meio, de uma criança envolvida em atividades sexuais explícitas reais ou simuladas, ou qualquer representação dos órgãos sexuais de uma criança para fins primordialmente sexuais '(DECRETO N o 5.007, DE 8 DE MARÇO DE 2004). A Legislação Brasileira em vigor tipifica como crime a(s) conduta(s) de "Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente" (Art. 241 do Estatuto da Criança e do Adolescente). (SAFERNET, 2009)

2.4 A Pedofilia e a Internet

Afirma uma pesquisa realizada pela Revista *Isto é*, no dia 8 de março de 2006, com a matéria intitulada “Pedofilia: O Brasil lidera o *ranking* mundial de pornografia infantil pela Internet. Seu filho está seguro?” - os pedófilos são jovens de classe média, entre 17 e 24 anos, que produzem e disponibilizam o material na Internet, e suas vítimas são menores de idade que muitas vezes pertencem à própria família do criminoso. Os compradores geralmente são solteiros, com emprego e têm aproximadamente 40 anos de idade.

No Brasil, a primeira notícia sobre pedofilia na Internet data de 1999, publicada pelo Jornal do Comércio de Recife com o título “Infração cibernética ganha polícia especial”, em que se noticiou que a Policia Civil de São Paulo estava com uma equipe preparada para combater o uso de softwares piratas e sites com pedofilia.

Aos poucos, por causa do crescimento da Internet, estes crimes aumentaram exponencialmente, principalmente o de pedofilia, enquanto o investimento para combater tais condutas foi aquém do esperado.

Porém, há páginas eletrônicas capazes de oferecer efetiva ajuda a polícia, através de denúncias diretas, como a SaferNet, que também disponibiliza no site uma ferramenta interativa de estatísticas da Central Nacional de Denúncias de Crimes Cibernéticos. Por meio desta página, é possível consultar o número de denúncias já oferecidas, com a possibilidade de realizar pesquisas pelo tipo de crime e pelo seu período. Conquanto a contagem só seja disponibilizada a partir de 2006, é possível perceber o aumento assustador relativo à pornografia infantil durante esse período até os dias de hoje.

As representações gráficas (figuras 1 e 2 abaixo) mostram as denúncias, sem incluir o site de relacionamento Orkut e a outra figura com a inclusão do site.

Denúncias de **1 de Janeiro de 2006** a **1 de Julho de 2006** e de **1 de Janeiro de 2008** a **1 de Julho de 2008**

Tipo de Conteúdo	Período de 2006-1-1 a 2006-7-1		Período de 2008-1-1 a 2008-7-1		Variação
	Domínio: Não-Orkut	Únicas	Domínio: Não-Orkut	Únicas	Domínio
Apologia e Incitação a crimes contra a Vida	377	3632	305	9068	-19.1%
Homofobia	79	643	51	618	-35.4%
Intolerância Religiosa	109	860	85	1371	-22.0%
Maus Tratos Contra Animais	176	1026	116	1122	-34.1%
Neo Nazismo	119	1319	90	1891	-24.4%
Pornografia Infantil	1244	5254	3024	27876	143.1%
Racismo	149	1308	137	1380	-8.1%
Xenofobia	38	314	31	737	-18.4%
Todos	**2291**	**14356**	**3839**	**44063**	**67.6%**

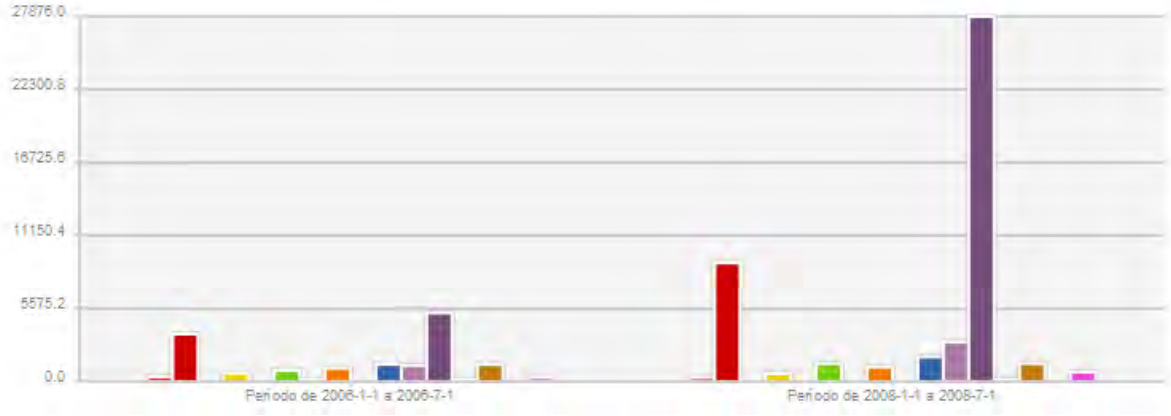
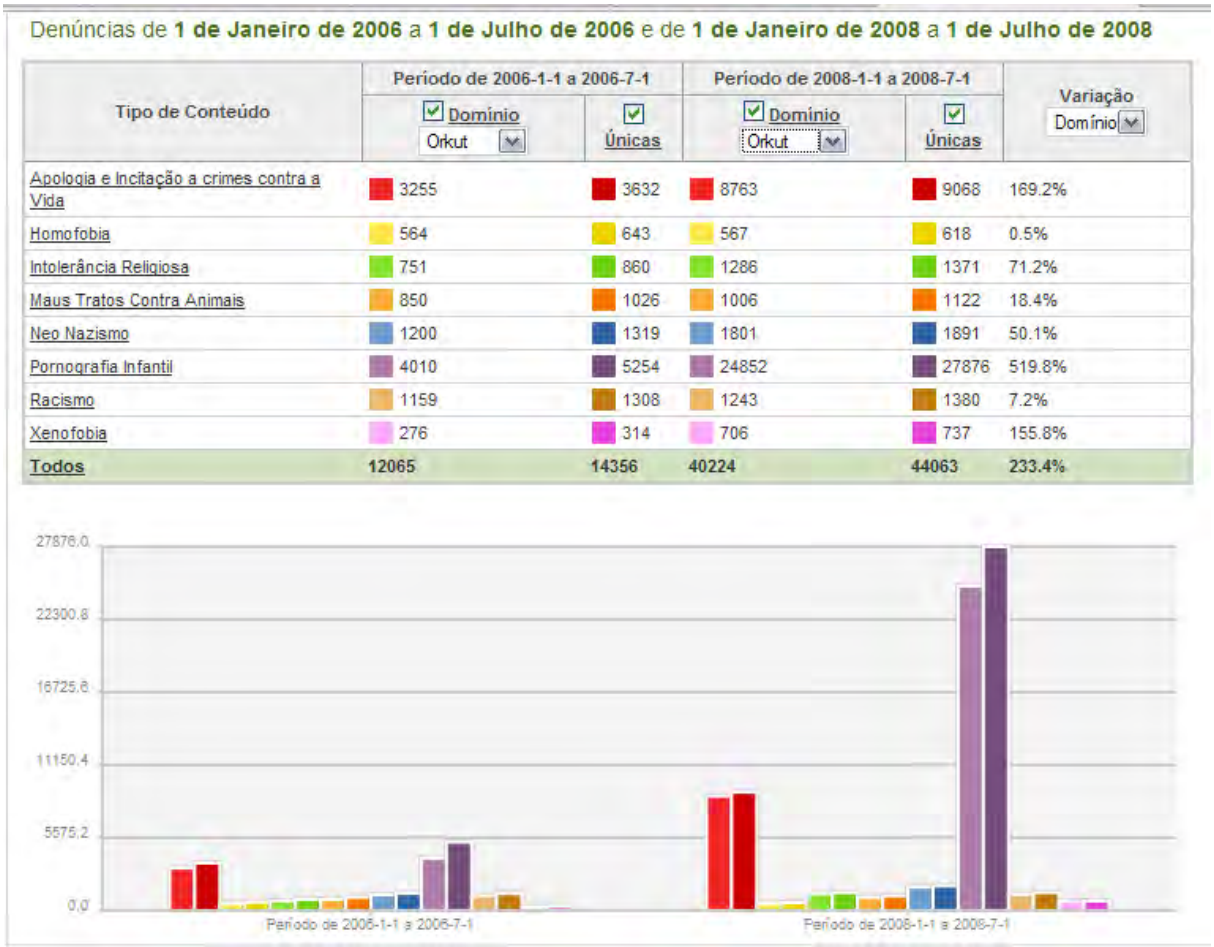


Figura 1 – Denuncias sobre Crimes na Internet de 2006 a 2008. Disponível em: http://www.safernet.org.br/site/indicadores. Acesso no dia 20/01/2009



Denúncias de **1 de Janeiro de 2006** a **1 de Julho de 2006** e de **1 de Janeiro de 2008** a **1 de Julho de 2008**

Tipo de Conteúdo	Período de 2006-1-1 a 2006-7-1		Período de 2008-1-1 a 2008-7-1		Variação
	Domínio: Orkut	Únicas	Domínio: Orkut	Únicas	Domínio
Apologia e Incitação a crimes contra a Vida	3255	3632	8763	9068	169.2%
Homofobia	564	643	567	618	0.5%
Intolerância Religiosa	751	860	1286	1371	71.2%
Maus Tratos Contra Animais	850	1026	1006	1122	18.4%
Neo Nazismo	1200	1319	1801	1891	50.1%
Pornografia Infantil	4010	5254	24852	27876	519.8%
Racismo	1159	1308	1243	1380	7.2%
Xenofobia	276	314	706	737	155.8%
Todos	**12065**	**14356**	**40224**	**44063**	**233.4%**

Figura 2 - Denuncias sobre Crimes na Internet de 2006 a 2008 incluindo o Orkut. Disponível em: http://www.safernet.org.br/site/indicadores. Acesso no dia 20/01/2009

Excluindo o orkut, apenas a pornografia infantil sofreu um aumento, com 143,1% das denúncias, enquanto os outros tipos de cibercrimes tiveram quedas. Porém, com a inclusão do site de relacionamento, todos tiveram um aumento de suas denúncias, ficando novamente em destaque a pedofilia, com 519,8% das denúncias. Isso revela apenas a “ponta do iceberg”, pois são os dados colhidos apenas por meio das pessoas que têm a preocupação de procurar o site e fazer o registro, que representam a minoria.

O crescimento pode ser ainda maior do que esperado, pois este universo é muito obscuro, e só com o apoio das polícias e da população se poderá combater e diminuir drasticamente essas estatísticas.

Como foi mostrado anteriormente, o artigo 241 do Estatuto da Criança e do Adolescente afirma que é crime “fotografar ou publicar cena de sexo explícito ou

pornográfica envolvendo criança ou adolescente", prevendo a reclusão de 1 a 4 anos.

2.5 Lei 11.829/2008 - Combate à pornografia infantil e à pedofilia na Internet

Em uma terça-feira, dia 25 de novembro de 2008, o Presidente Luis Inácio Lula da Silva sancionou a lei nº 11.829/2008, que altera a Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet.

Antes desta lei se aprovada, ela dependia do Estatuto da Criança e do Adolescente, prevendo pena de no máximo 4 anos de reclusão. Agora esta pena será de 4 a 8 anos, aumentando o tempo da pena de 1/3, se o crime for em casa, hospitalidade e que tenha qualquer parentesco até o terceiro grau ou de autoridade sobre a criança ou até mesmo com seu consentimento. E a posse e a venda de material contendo pedofilia tem a pena de 4 a 8 anos de prisão.

Outra novidade é a tipificação para o aliciamento de crianças e adolescentes por meio de salas de bate-papo. Segundo as autoridades, a prática é bastante comum e considerada a mais perigosa, pois por meio dela o pedófilo tem condições de marcar encontros com as crianças.

Essa prática não era considerada crime porque o Estatuto da Criança e do Adolescente foi criado em 1990. Somente depois disso a Internet ganhou espaço, e as salas de bate-papo se tornaram cada vez mais comuns.

Esta lei estabelece que, quando acontecer um caso desses, o provedor terá que bloquear o acesso à internet do usuário suspeito e armazenar os seus dados e seus *logs*, quando as autoridades entrarem em contato.

2.6 Perícia Forense Aplicada à Informática

A palavra perícia (do latim, *peritia*), quer dizer de acordo com o Novo Dicionário eletrônico Aurélio versão 5.0:

Substantivo feminino.

1. Qualidade de perito.
2. Habilidade, destreza.
3. Vistoria ou exame de caráter técnico e especializado (v. *peritagem*).
4. Conjunto de peritos (ou um só) que faz essa vistoria:
5. Conhecimento, ciência.

Então alguns conceitos de Pericia Forense Digital são: :

> Um conjunto de técnicas, cientificamente comprovadas, utilizadas para coletar, reunir, identificar, examinar, correlacionar e analisar e documentar evidências digitais processadas, armazenadas ou transmitidas por computadores. (Pires, 2003, p. 2)

Outro conceito adotado por GUIMARÃES et al apud NOBLETT (p.2), afirma que:

> A Forense Computacional é a ciência que estuda a aquisição, preservação, recuperação e análise de dados que estão em formato eletrônico e armazenados em algum tipo de mídia computacional.

Portanto, a Forense Computacional é a ciência que estuda provas eletrônicas para que o perito possa coletar, preservar, recuperar e relacionar estas evidências para saber o que aconteceu no local, sendo este um lugar virtual, que não se pode tocar, que é o ambiente cibernético, onde encontramos evidências digitais.

> O termo evidência digital refere-se a toda e qualquer informação digital que pode ser capaz de determinar que uma intrusão ocorreu ou que provê alguma ligação entre a intrusão e as vítimas ou entre a intrusão e o atacante. (REIS, 2003. p. 70)

No estudo forense que produz resultados interpretativos, a forense computacional pode produzir respostas diretas que podem decidir em um caso. Em GUIMARÃES et al, exemplifica:

> No caso de assassinato, o legista verifica que há traços de pele em baixo das unhas da vítima, isso é interpretado como um indício de que houve luta antes da consumação do crime, contudo não passa de uma interpretação. Já no caso de uma perícia em uma máquina suspeita podem ser conseguidos arquivos incriminadores como diários e agendas.

A perícia forense possui quatro procedimentos básicos: todas as evidências devem ser identificadas, preservadas, analisadas e apresentadas (FREITAS, 2006, p.2). Ou seja, por este trabalho é necessário que sejam coletados, examinados, sendo este que difere do conceito de Freitas, porém ele está contido na coleta dos dados, analisados e apresentados com um laudo técnico.

Para que se tenha uma investigação legal, é necessário um padrão, que hoje no Brasil não há para esses crimes eletrônicos e sim para perícias em geral, ou seja, normas gerais que abrangem todo tipo de perícia (citadas no Código de Processo Penal), no entanto, este pode ser usado e aplicado à informática. Para que este tipo de perícia seja validado é necessária a presença de um perito criminal, o Perito Oficial (dois por exame) e esse profissional precisa ter nível universitário e prestar concurso público específico.

De acordo com o exame do Corpo de Delito do Código do Processo Penal Brasileiro, que em seu capítulo II, afirma:

- **Art. 158.** Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado.

- **Art. 160.** Os peritos elaborarão o laudo pericial, onde descreverão minuciosamente o que examinarem, e responderão aos quesitos formulados.

- **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.

- **Art. 170.** Nas perícias de laboratório, os peritos guardarão material suficiente para a eventualidade de nova perícia. Sempre que conveniente, os laudos serão ilustrados com provas fotográficas, ou microfotográficas, desenhos ou esquemas.

Quando acontece um crime ou uma suspeita de crime, pelo Código Processual Penal brasileiro, há a necessidade de seguir alguns procedimentos legais, mesmo em caso de um crime cibernético, como por exemplo, fazer o corpo de delito e ninguém mexer nas provas exceto os peritos. Neste caso é de extrema importância que nenhum curioso toque nas evidências, apenas o perito da área da informática. E como será visto qualquer cópia ou até mesmo um clicar descuidado do mouse, pode colocar tudo a perder. Se o computador estiver ligado, deixar ligado até que o perito o faça ou então, o perito o leva e deixa como cadeia de custódia. De qualquer maneira, o perito tirará uma cópia do sistema, pois “é sempre possível fazer cópias assinadas digitalmente das mídias que estão sendo investigadas para que possam ser feitas análises futuras se necessário. Na verdade o interessante é sempre atuar em cima de cópias”(GUIMARÃES et al, p.4).

Além de fazer as cópias é necessário documentar e guardar essas prova, que será chamada de cadeia de custódia.

2.6.1 Cadeia de Custódia

A Cadeia de Custódia é um processo usado para manter e documentar a história cronológica da evidência coletada. Para garantir a idoneidade e a documentação das provas utilizadas em processos judiciais.

> Se houver alguma chance de um caso ir para o tribunal, é de extrema importância que a evidência digital seja manipulada corretamente por todos que tenham acesso a ela. O processo de manipulação da evidência de uma pessoa para outra é conhecido como "cadeia de custódia". (MICROSOFT, 2007)

Ou seja, o perito realiza a aquisição da imagem das evidências, envelopa e lacra o disco rígido, inicia a lista da cadeia de custódia indicando a data e hora em que o ele foi lacrado, e o *hash* para garantir a integridade da mídia e dos dados.

O *hash* é como se fosse uma assinatura digital onde cada arquivo possui um valor exclusivo. Se mudar um pequeno detalhe, esta assinatura é mudada totalmente.

2.7 Ordem de Volatilidade

Em uma investigação os dados são coletados e analisados a todo o momento. “Quanto mais precisos e completos os dados, melhor e mais abrangente a avaliação pode ser” (FARMER, VENEMA, 2006. p.5). Por causa das fragilidades desses dados, a modificação de dados em uma perícia forense poderá por em dúvida todo o processo de investigação e portando anulando-o.

Como será vista, a primeira regra em uma perícia é realizar o processo através de uma cópia idêntica a original, pois existe a possibilidade de erros (humanos ou não) que podem resultar na destruição dos dados.

No entanto, há situações em que a clonagem dos dados não seja aconselhada, quando o computador que foi apreendido está ligado, portanto nessa situação, que é chamado de “análise ao vivo (*on line*)”, é importante saber esta ordem de volatilidade das informações que estão armazenadas no sistema.

> No método de investigação *online* ou análise ao vivo, a perícia é realizada com o computador ligado. Esta análise ocorre quando o sistema está com energia, têm tráfego de rede, processos ativos, conteúdo na tela e disco sendo acessado. (FREITAS, 2006, p.3).

Caso essa ordem não seja respeitada, o risco de perda e alteração dos dados será maior e trará prejuízos à investigação.

Para uma boa perícia, de acordo com REIS, GEUS(2001. p.5), há a necessidade de seguir alguns passos:

Passo 0: Determinar a melhor abordagem para o exame, identificando todas as atividades que precisarão ser executadas.

Passo 1: Preparar o sistema de análise, provisionando a melhor configuração de *hardware e software*, devidamente testado testados e “esterilizados”, para a realização dos exames

Passo 2: Estabilizar o sistema auditado de modo a preservar o máximo de vestígios possíveis e proteger dados e sistemas não comprometidos.

Passo 3: Obter à cópia das informações armazenadas eletronicamente no sistema computacional. A cópia deve conter toda a informação, em seu estado original e deve ser autenticada.

Passo 4: Coletar o máximo de informações importantes na ordem de volatilidade das mesmas.

Neste passo, como mostrado a importância da ordem de volatilidade em uma investigação.

A seguir, na Tabela 1 (FARMER, VENEMA, 2006, p.6) é mostrado o tempo de vida de cada dados importante no computador.

Tabela 1 - O Ciclo de vida esperado dos dados (FARMER, VENEMA, 2006, p.6)

Tipo de Dados	Tempo de Vida
Registradores, memória periférica, caches e etc.	Nanosegundos
Memória Principal	Dez nanosegundos
Estado da Rede	Milissegundos
Processos em Execução	Segundos
Disco	Minutos
Disquetes, mídia de backup e etc	Anos
CD-ROMs, impressões e etc.	Dezenas de Anos

Este ciclo de vida é o tempo médio que o arquivo esteja no computador ativo, ou seja, ele ainda pode ser copiado e não foi apagado do sistema. Cada tipo de dados tem seu tempo médio de vida útil distinto um do outro, como foi mostrado na Tabela 1. Por este motivo, há a necessidade de planejar quais os dados mais importantes e seu tempo de vida e assim poder capturar todos os dados possíveis antes de sua “morte”.

Então, Farmer e Venema (2006, p.5), criaram o conceito de Ordem de Volatilidade. Seguindo esta ordem, há uma grande probabilidade de se preservar os detalhes mais importantes sem que haja perdas.

Portanto, não tem como capturar todos os dados de uma vez só se que não tenha perda de alguma informação, pois em cada análise ou captura dos dados em uma parte do computador, o perito estará alterando dados em outro local da máquina. E também não é possível registrar todas as alterações nos processos e arquivos precisamente em tempo real.

Nesta sessão foi visto que para os dados serem coletados e logo após investigados tem que seguir uma ordem de volatilidade, senão muitos dados que

tem esta ordem de poucos nanossegundos se perderam e podendo assim perder evidências, então sempre deverá ser feito seguindo rigorosamente sua ordem de volatilidade e assim seguir com os procedimentos de uma perícia forense.

2.8 Procedimentos de uma Perícia Forense

> "A maneira como as mídias são armazenadas e manipuladas, é o fato determinante para a realização de uma perícia com sucesso ou perda de informações valiosas, resultando na destruição das provas digitais" (TREVENZOLI, 2006, p.34).

Os procedimentos padrões que os peritos trabalham, é inicialmente tirar fotos do local a ser investigado para depois iniciar a coleta. "E é necessário fazer o registro dos dados voláteis, como exemplo conexões estabelecidas processos em execução, informações na memória RAM" (TREVENZOLI, 2006, p.35). Se um perito, que não tenha experiência, desligar o computador sem tirar uma cópia e nem salvar estes conteúdos, quando desligado, será apagado.

Outro caso é que o usuário pode ter trocado algum comando para visualizar arquivos como o *dir* do DOS (que exibe uma lista de todos os arquivos, pastas e subpastas em um determinado local do disco rígido), com o *format*,(que serve para formatar um disco, ou seja, preparar para receber dados, apagando todos os dados do disco formatado) e na hora de executado o falso comando, o perito inexperiente, perderá todos os dados e assim invalidando o caso.

Cada suspeito tem seu nível de experiência de acordo com suas habilidades e quais os tipos de evidências eles deixam no local auditado como mostrado na Tabela 2.

Tabela 2: Relação entre a habilidade do invasor e a quantidade de evidências deixadas.

Nível de Habilidade	Habilidades	Evidências
Clueless	Nenhuma habilidade	Todas as atividades são bastante aparentes
Script Kiddie	Capaz de encontrar programas prontos na Internet e executá−los seguindo instruções detalhadas. Não escrevem programas	Pode tentar cobrir rastros com o uso de *rootkits* prontos, mas com sucesso limitado. Pode ser detectado com esforço mínimo
Guru	Equivalente a um administrador experiente. Hábil em programação. Checa a existência de programas de segurança e esquemas de seguros, evitando alvos protegidos	Cuidadosamente apaga evidências em *back doors* para um acesso futuro de sua presença. Capaz de encontrar *log* de arquivos. Não deixa traços óbvios
Wizard	Possui um grande conhecimento do funcionamento interno de um sistema. Capaz de manipular *hardware* e *software*	Praticamente não deixa evidências úteis. Pode comprometer totalmente o sistema

Portando, quanto maior o nível de experiência mais difícil fica para coletar as evidências.

Caso a máquina esteja ainda ligada, o perito terá que fazer um registro fotográfico do local e da tela do computador e depois “não usar programas que

possam alterar as datas de último acesso dos arquivos existentes.”(TREVENZOLI, 2006, p.36). Então iniciar a duplicação pericial.

> A duplicação pericial, que consiste em criar uma imagem (cópia perfeita) de um sistema. Através da imagem o perito poderá realizar suas análises, preservando assim as provas originais. (FREITAS, Andrey Rodrigues. 2006. P. 4)

Há dois tipos de métodos de investigação em meio eletrônico, quando ele está ligado, ou seja, será feito uma investigação *online* e outro quando se encontra desligado, que é o método *offline.*

No método *offline*, a investigação é executada em uma cópia da imagem do computador original, chamado também cópia baseada em bits que é “Uma cópia baseada em bits é uma cópia completa de todos os dados provenientes da fonte à qual a investigação se destina, incluindo informações como o setor de inicialização, partições, e espaço de disco não-alocado.”(Microsoft TechNet, 2007). Este tipo de investigação minimiza os riscos de danos possíveis na evidência digital, pois o computador estará desligado.

Para que um procedimento seja realizado sem que não tenha nenhum problema processual, nem obtenção ilícita das provas, há uma necessidade de seguir um modelo de investigação, adaptado da página eletrônica da Microsoft, visto na Figura 3 e suas etapas:

Figura 3 – Modelo de Investigação Computacional, adaptado da fonte http://www.microsoft.com/brasil/technet/prodtechnol/security/guidance/disasterrecovery/computer_investigation/9545b739-1ef9-415f-a1c4-3ca29f0ce5af.mspx. Acesso no dia 25/01/2009.

- Identificação das Evidências
- Coleta das Evidências
- Analise das Evidências
- Apresentação das Evidências

Sem um padrão bem definido em com código de leis, alguém poderá contestar a veracidade dessas provas e inocentando o suspeito, pois se não tiver uma garantia essas evidências perderá a validade legal.

Para isso é necessário uma padronização, de acordo com REIS, GEUS (2001, p.3), que “padrões para exames periciais em sistemas computacionais deve ser regido por aspectos de ordem legal e técnica”.

Sendo cada aspecto com suas divisões, como visto na Figura 4.

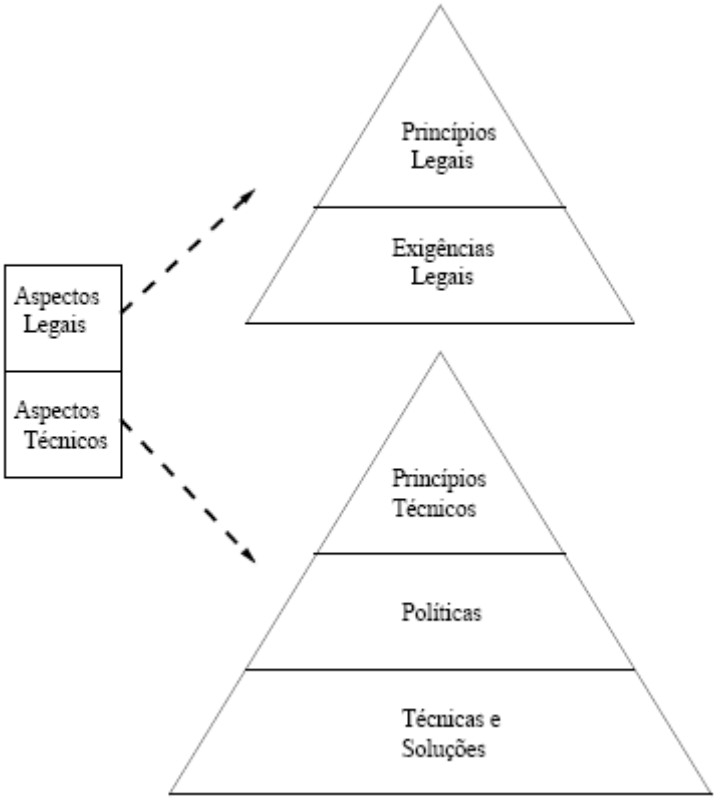


Figura 4 – Modelo de padronização Fonte:(REIS, GEUS. 2001. p.4)

Este modelo é uma estrutura hierárquica de duas classes de níveis diferentes e relacionadas entre si:

Na parte de Aspectos Legais são as “formalidades e enquadramentos judiciais a que estão sujeitos os peritos e a função pericial. Tais exigências legais estão dispostas no Código de Processo Penal Brasileiro”(REIS, GEUS. 2001. p.5).

Alguns exemplos dos Aspectos Legais.

- O perito deve ser judicialmente responsável pelos resultados da perícia e pelas evidências.
- O estado original dos vestígios deve ser mantido até a chegada dos peritos. Qualquer alteração deve ser relatada.
- O resultado do exame pericial deve ser o mais transparente possível, sendo permitida a utilização de fotografias, desenhos e esquemas.

Enquanto que nos Aspectos Técnicos “referem-se aos requisitos práticos e condutas para a execução do exame propriamente dito”(REIS, GEUS. 2001. p.5). Então, estes aspectos são divididos em 3:

- **Princípios Técnicos:** Devem garantir a confiabilidade e integridade. Exemplificando mais alguns:
- **Políticas**: como serão planejados, executados, monitorados para assegurar a qualidade e integridade dos resultados obtidos.
- **Técnicas e Soluções**: Soluções de *hardware* e *software* para obter melhor investigação.

E quanto maior competência dos peritos nos procedimentos básicos, maior a capacidade de identificar, coletar e analisar os dados. Além do mais, o perito que irá fazer este trabalho, deve assegurar que as informações coletadas existem e são verdadeiras e que estão no computador auditado e não foram alteradas nem inseridas durante todo o processo.

Na próxima sessão, serão detalhados os procedimentos básicos para fixar os conceitos de cada etapa.

2.8.1 Identificação das Evidências

A identificação das evidências se inicia com o perito que tem a responsabilidade de chegar primeiro onde aconteceu do incidente para que ninguém “suje” a local auditado ou, se o computador estiver ligado, ele começar a salvar os arquivos que tem ordem de volatilidade baixa.

> Diferentes crimes resultam em diferentes tipos de evidências. Por exemplo, em um caso de acesso não autorizado, o perito deverá procurar por arquivos de log, conexões e compartilhamentos suspeitos, já em casos de pornografia, buscará por imagens armazenadas no computador, histórico dos sites visitados recentemente, arquivos temporários do browser etc. (FREITAS, 2006. p.2)

Afirma Freitas (2006, p.2) que “A habilidade do perito em identificar as evidências vai depender da sua familiaridade com o tipo de crime que foi cometido e dos programas e Sistemas Operacionais envolvidos”

Por outro lado, o computador que está sendo auditado, pode está infectado com algum tipo de *Malware* que esteja colocando estes arquivos em sua máquina. Por isso que o perito tem que ter essa familiaridade com Sistema Operacional e seus programas de auditoria.

Algumas evidências são encontradas geralmente em:

- Dispositivos de armazenamento como: *laptops*, discos rígidos, disquetes, CDs, DVDs, *pendrives*, câmeras fotográficas analógicas e digitais, MP3 players e celulares.

2.8.2 Preservação

Sua principal regra é: “Não destruir ou alterar as provas. Portanto, as as evidências precisam ser preservadas de tal forma que não haja dúvida alguma de sua veracidade.”(FREITAS, 2006. p.3).

Nesta fase, que é bem delicada, alguns dados eletrônicos são frágeis, altamente voláteis e que podem ser danificados, perdidos e alterados com facilidade, portanto, é necessário garantir que os dados sejam preservados a cada bit.

Inicialmente, precisa-se criar um bom conjunto de ferramentas para manipular os dados e fazer uma boa cópia deles para serem manipulados corretamente, sem a necessidade de alterar os dados originais.

No entanto, há regras a serem seguidas com muito cuidado, como mostrado na Figura 5:

Figura 5 – Fluxograma de Preservação dos Dados

- Tirar fotos do local
- Criar somas de verificação e assinaturas, ou seja, o *hash* de cada arquivo.
- Criar uma imagem do sistema investigado
- Todas as evidências serão lacradas em sacos de preferência antiestáticos, para não danificar as partes eletrônicas e não perder os dados, e etiquetá-las.
- Ter o cadastro de cada evidência coletada
- Evidências serão trancadas e armazenadas para não danificar o material coletado
- Tudo o que foi feito, ser documentado detalhadamente e justificado.

2.8.3 Análise

O profissional nesta fase deve ser altamente cuidadoso ao manipular a evidência e saber onde procurar, como na Figura 6. A chamada prova deve ser inquestionável. Todas as evidências digitais encontradas precisam estar em conformidade com a lei, além de serem autênticas, exatas e completas. (FREITAS, 2006)

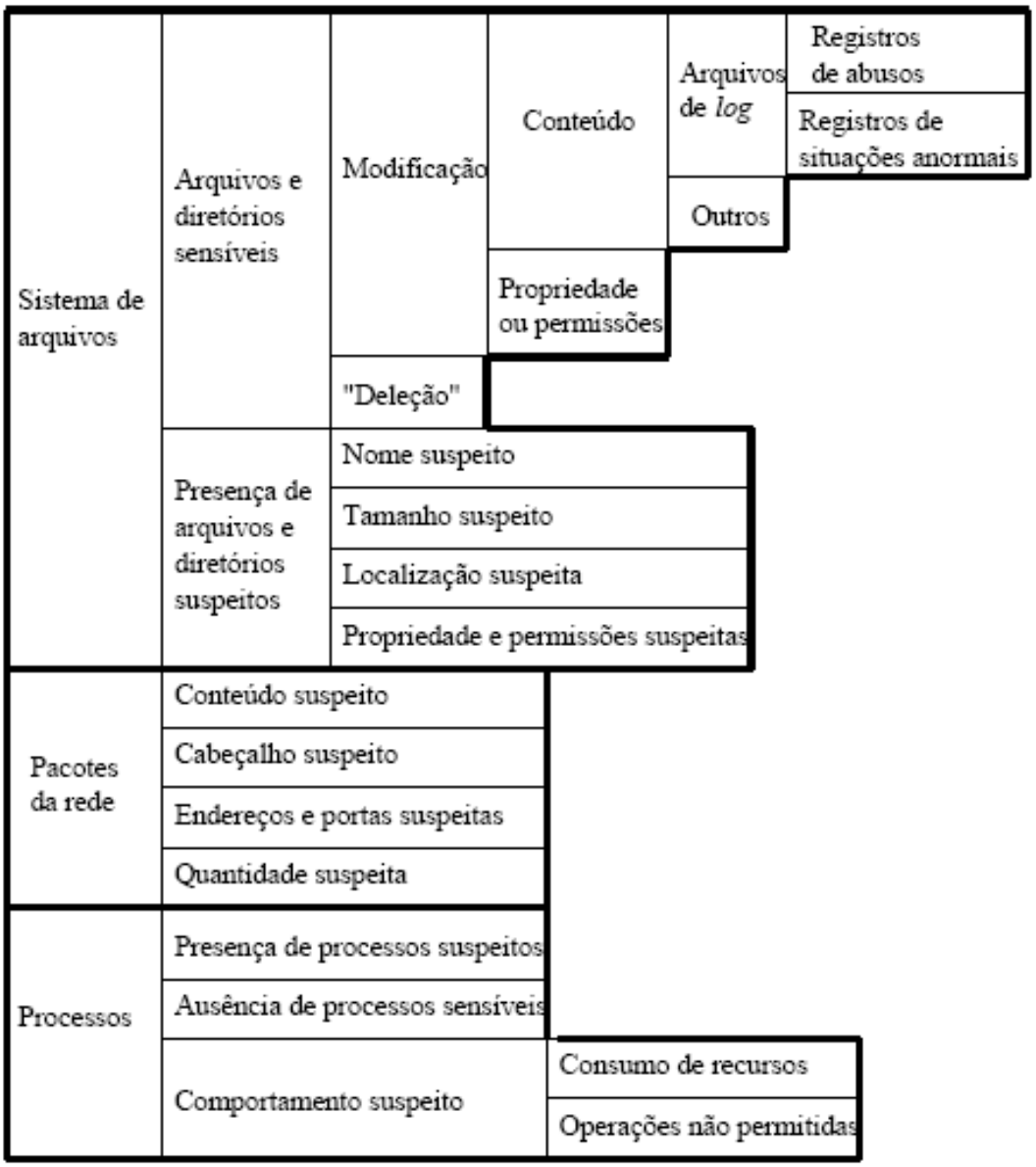


Figura 6 - Exemplos gerais de possíveis evidências a serem procuradas, retirado de REIS, página 111.

Neste trabalho será estudado, pela Figura 6, o sistema de arquivos, porque se houver alguma evidência de arquivos que tenha algum conteúdo com pedofilia, será aberto o inquérito policial para ser enviado ao Juiz para que ele encaminhe ao Ministério Público para levar a júri popular.

Nos outros pontos, como Pacotes de Redes e Processos, serve para saber se o computador auditado está infectado com algum *Malware.*

Com este estudo, o perito tentará identificar quem fez, quando fez, que dano causou e como foi realizado.

- E como procurar?
    - Será que vai ser feita a análise *online* ou apenas a *offline*?
- O que procurar?
    - Dependendo da acusação, será procurado logs, fotos e arquivos de Internet temporários.
- Onde procurar?
    - Lixeira, arquivos temporários e cookies.
- Como procurar?
    - Só usando as técnicas simples de procura.

Se a evidência for bem analisada, então algumas questões abaixo, por exemplo, serão respondidas:

- Qual o sistema operacional e sua versão?
- Quem estava conectado no momento do crime?
- Quais os arquivos que foram usados na hora do crime?
- Quais as portas que estavam abertas no sistema operacional?
- Quem eram os usuários que “logaram” na máquina e de qual grupo eles pertenciam?
- Quais os arquivos foram criados e excluídos?

Estas evidências precisam ser: autênticas, exatas, completas, convencer o júri, e ser uma prova lícita e ter toda a sua documentação do trabalho que foi feito. Para que isto seja verdade, então segundo (NOGUEIRA, 2007. p.9):

> Para que um documento eletrônico tenha validade jurídica e possa servir, por si só, de meio probatório em juízo, faz-se necessário a ocorrência de dois requisitos: impossibilidade de alteração do seu conteúdo e perfeita identificação das partes.

Outro cuidado é ter a certeza de que estas provas são realmente usadas e criadas pelo suspeito, ou sua estação pode estar com um *Malware* infectado.

Terminado este momento, o perito irá fazer a apresentação do trabalho.

2.8.4 Apresentação

Nesta etapa, o perito entrega o laudo (do latim, *med laudu*), que é um documento em que ele, o perito ou árbitro emite seu parecer e responde todas as questões propostas pelo juiz e pelas partes interessadas.

> O laudo deve ser claro, conciso estruturado e sem ambiguidade de tal forma que não deixe dúvida alguma de sua veracidade. E deverão ser informados os métodos empregados na perícia, incluindo os procedimentos de identificação, preservação e análise, e os softwares e hardwares utilizados. O laudo pericial deve conter apenas afirmações e conclusões que possam ser provadas e demonstradas técnica e cientificamente.(FREITAS, 2006. p.5)

Contudo, nesta fase é a finalização do procedimento que se inicia quando o perito é chamado e assim finaliza seu trabalho.

É nesta etapa que toda a documentação é organizada, toda a lista das evidências que foram coletadas, a evolução de todo o processo, quais são as partes relevantes para colocar no relatório final e que sustente as teses e acusações que foram colocadas no início do inquérito, para que ele seja claro, conciso.

Neste relatório que irá para o Juiz, deverá ter um resumo escrito de forma que uma pessoa sem muitos conhecimentos técnicos possa entender o que ocorreu e como ocorreu.

Portanto, para que uma investigação seja bem feita, é necessário seguir estes quatro passos detalhadamente: Inicialmente, identificar quais são as evidências, preservá-las, analisá-las e assim finalizar com a apresentação, ou seja, o laudo técnico. Um bom perito deve saber com qual evidência ele deve iniciar, pois alguns dados são voláteis e podem se perder rápido, que é chamado de ordem de volatilidade.

CAPÍTULO 3 – CONJUNTO DE FERRAMENTAS

> Além de experiência e sólidos conhecimentos, o investigador depende totalmente do conjunto de ferramentas que ele utiliza para coletar, documentar, preservar e processar as informações provenientes do sistema investigado. No mundo real da investigação forense, o investigador deve estar preparado para lidar com as mais diversas arquiteturas e sistemas operacionais, logo, seu conjunto de ferramentas deve ser o mais amplo possível. (REIS e GEUS, 2002, p.64)

Portanto, o investigador também tem que conhecer muito sobre o Sistema Operacional envolvido e os softwares necessários para validar a prova ou refutá-la.

Mesmo que este sistema for comprometido, o investigador precisará de utilitários confiáveis, já que o suspeito pode alterar os dados e comprometer as evidências. Por exemplo o criminoso trocar o comando de reiniciar pelo apagar todos os dados e danificar o disco rígido, dificultando ainda mais a investigação, como foi falado no capítulo anterior.

Os programas usados neste trabalho são:

- TCT(*The Coroner's Tookit)* [VENEMA, FARMER. 2009]
- Windows Sysinternals
- FDTK-UbuntuBR [FDTK-UbuntuBR, 2009] que é uma distribuição brasileira do FTK (*Forensics Tool Kit*).
- Helix [FAHEY, GLEASON. 2006]

3.1 The Coroner's ToolKit - TCT

O The Coroner's ToolKit é uma coleção de utilitários para a perícia forense computacional de Sistemas Operacionais baseado em Unix, desenvolvido por Wietse Venema e Dan Farmer criado em 1999 e distribuído gratuitamente em 2000 no site dos autores.

Uma das características é respeitar a ordem de volatilidade dos dados, como mostrado no Capítulo 2, ou seja, salvar logo os dados que podem se perder rapidamente.

Há também o conceito de MACtimes, que são os atributos de tempo dos arquivos, por exemplo:

- mtime: Muda quando o conteúdo de um arquivo é modificado.
- atime: Última data/hora em que o arquivo ou diretório(ou pasta) foi acessado.
- ctime: monitora quando o conteúdo sobre o arquivo mudaram, como o seu dono e suas permissões e mostra também quando o arquivo foi excluído.

O comando mactime gera um relatório cronológico de todos os acessos aos arquivos a partir das informações dos atributos dos arquivos.

Este software serve como referência para toda a auditoria por causa dos conceitos de ordem de volatilidade e MACtimes e usado em todos os programas deste trabalho.

3.2 Utilitário Windows Sysinternals

São um conjunto de utilitários feito por Mark Russinovich e Bryce Cogswell em 1996 e comprado pela Microsoft em junho de 2006. Estas ferramentas servem para ajudar a gerenciar, solucionar problemas e diagnosticar os aplicativos do sistema operacional da Microsoft.

Estas ferramentas serão utilizadas para saber se a máquina auditada tem algum *Malware* instalado no sistema. Pois, se o suspeito for leigo no assunto e tiver apenas conhecimentos básicos, ele pode ter um cavalo de tróia e que descarregue fotos com conteúdo de pornografia infantil em sua máquina. Provando que o suspeito é inocente, pelo motivo que ele não tinha intenção e nem sabia que tinha esses tipos de arquivos ilegais.

Na proposta deste trabalho se inicia sempre com a frase, “todos são inocentes até que se prove ao contrário”, conforme a garantia da Constituição Federal do Brasil. Então, estes programas são apenas para identificar se há programas mal-intencionados e não analisá-los.

3.2.1 Autoruns

Com este aplicativo, é possível ver quais programas estão configurados para serem iniciados automaticamente quando o seu sistema inicializa e quando faz logon. O Autoruns também mostra a lista completa de locais no Registro e em arquivos onde os aplicativos podem definir configurações de inicialização automática. Ver Figura 7

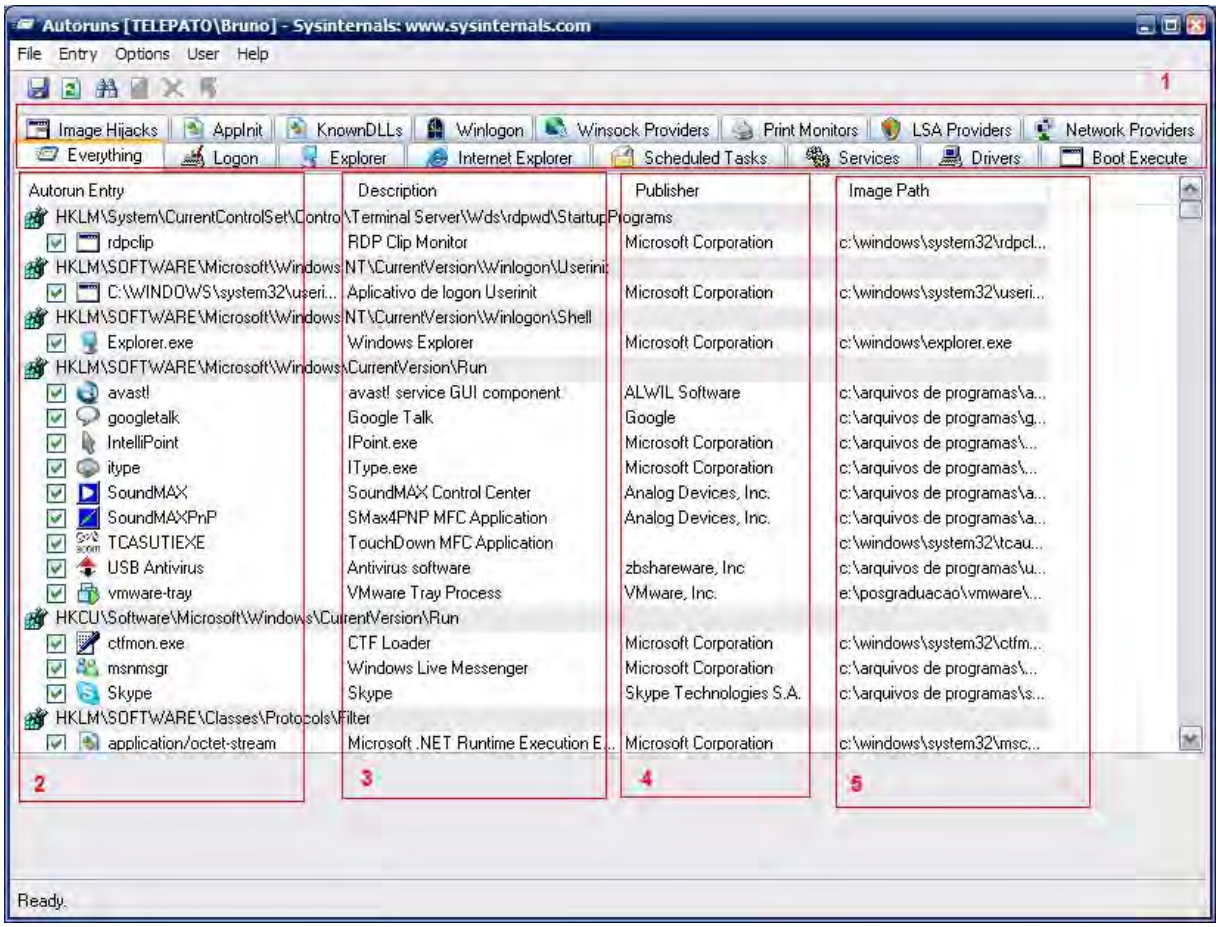


Figura 7 – Autoruns – Versão 9.39
1 – Aba de Ferramentas
2 – Arquivos em Execução
3 – Descrição de cada aplicativo
4 – A Empresa que fez o aplicativo
5 – Local onde está o aplicativo

Detalhando cada aba, para obter mais conhecimento do programa, então será visto a seguir:

- **Everything** → Mostra todos os resultados que o programa monitora no computador.
- **Logon** → Mostra todos os resultados dos programas que inicializa quando o Windows é inicializado e suas Chaves de Registro.
- **Explorer** → Mostra as extensões shell do Windows e Barra de Ferramentas**.**
- **Internet Explorer** → Mostra as extensões do Internet Explorer.
- **Scheduled Task** → Poderá ver as Tarefas Agendadas.
- **Services** → Mostra os Serviços do Sistema.
- **Drivers** → Todos os Drivers que estão sendo executado pelo Sistema.
- **Boot Execute** → Qual arquivo está sendo executado na inicialização do Windows.
- **Image Hijacks** → Mostra arquivos que se auto-iniciam no prompt de comando
- **AppInit** → Mostra DLLs registradas como DLL de aplicativos da inicialização.
- **KnownDLL** → Mostra DLLs conhecidas, que estão geralmente, na pasta System32.
- **WinLogon** → Mostra os DLLs ligadas diretamente com a inicialização.
- **Winsock Providers** → Mostra os protocolos Winsock registrados, incluindo provedores de serviço Winsock. Nesta Aba pode-se encontrar se há Malwares instalados e esta ferramenta poderá desistalá-los.
- **Print Monitors** → Mostra DLLs que carregam em serviço spooling de impressão. Malware tem utilizado este apoio automático para si.
- **LSA Providers** → Mostra registros Autoridade de Segurança local (LSA) autenticação, notificação e pacotes de segurança.

3.2.2 AcessEnum

Essa ferramenta de segurança muito eficiente, mostra quem tem acesso e com que tipo de diretórios, arquivos e chaves do Registro no sistema. Usado apenas para localizar falhas nas permissões(Figura 8).

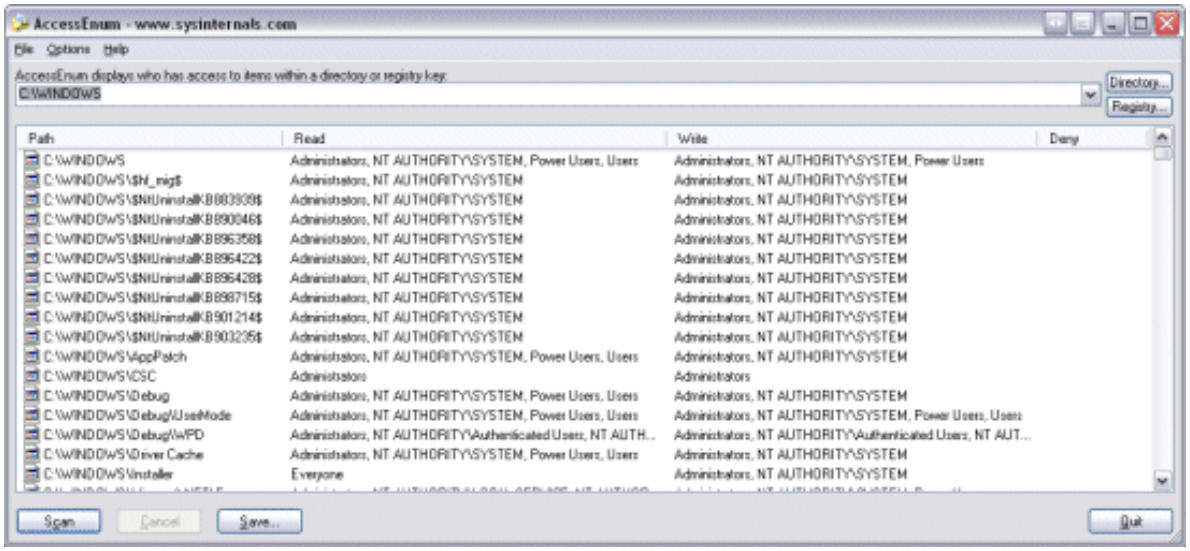


Figura 8 – AcessEnum

3.2.3 Process Explorer

Este software é muito parecido com do Windows XP, Gerenciador de Tarefas. Ele é uma ferramenta de auditoria da memória RAM e monitora em tempo real o que esta acontecendo no computador. Sua tela é mostrada na Figura 9.

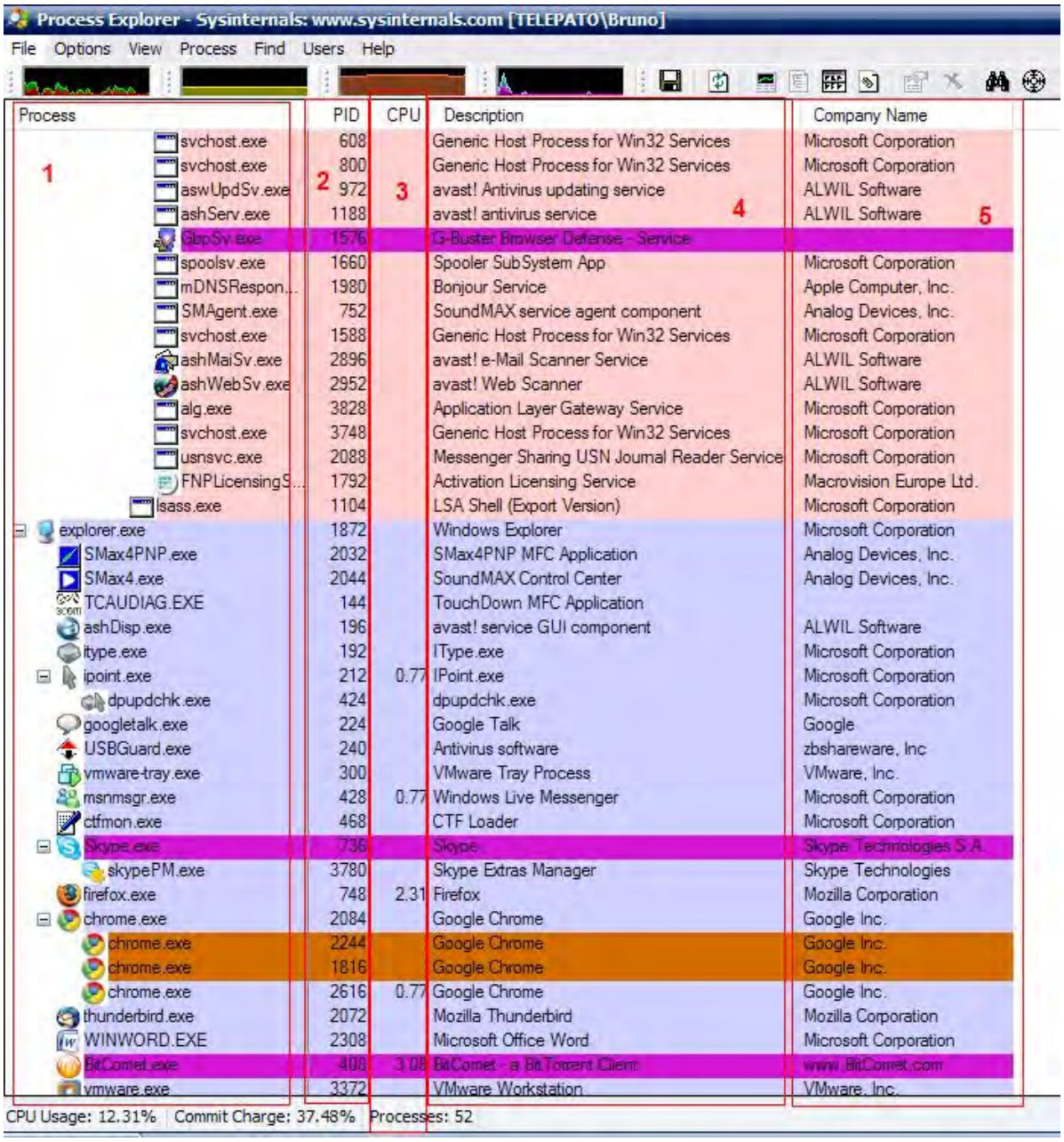


Figura 9 – Process Explorer – versão 11.33

1 – Processos e Subprocessos
2 – Número do Processo
3 – Parcela que está usando o CPU
4 – Descrição do processo
5 – Nome da Empresa

Como visto, este utilitário é bem mais completo que o Gerenciador de Tarefas.

Se tiver um Malware instalado, aparecerá o processo, porém com nome da companhia diferente do original, então para removê-lo, só clicar com o botão direito do mouse e clicar na opção "*Kill Process Tree*".

3.2.4 Process Monitor

É uma ferramenta de monitoramento que mostra o sistema de arquivos, o Registro e a atividade de processo em tempo real. Ele é a combinação de duas ferramentas do Sysinternals, o FileMon que monitora a execução dos arquivos em tempo real e RegMon que monitora o registro do Windows, também em tempo real. Na Figura 10 é mostrado a tela e seus elementos.

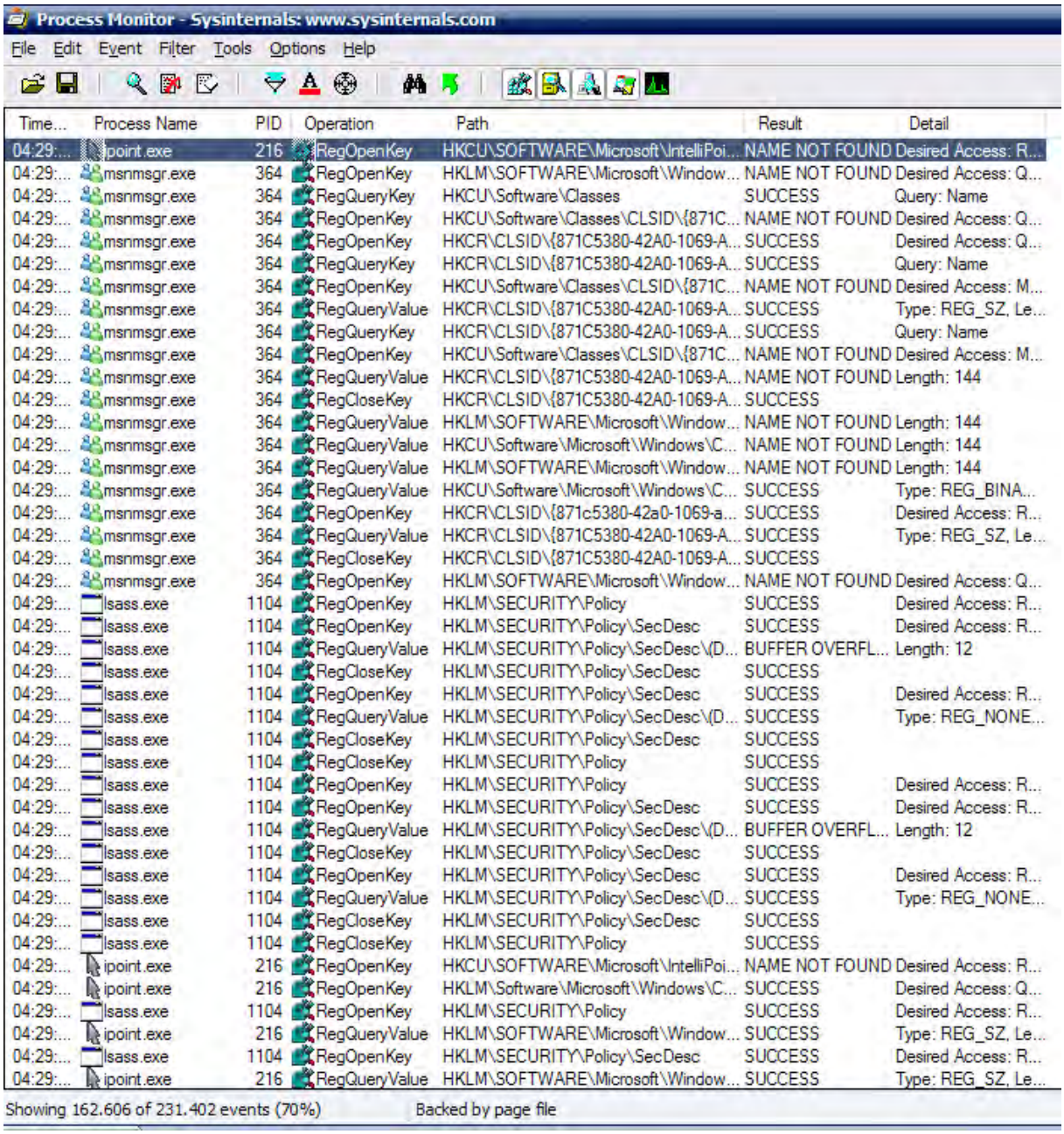


Figura 10– Process Monitor versão 2.04

3.4.5 TCPView

Esta ferramenta apresenta em tempo real quais os endereços IP dos computadores aos quais estão sendo auditados e ligados, o seu tipo de ligação e se ela está enviando e recebendo dados.

Logo quando iniciado no Windows, o TCPView exibe o nome do processo que possui e suas conexões TCP e UDP ativas e atualizando a cada segundo. Veja a sua tela na Figura 11.

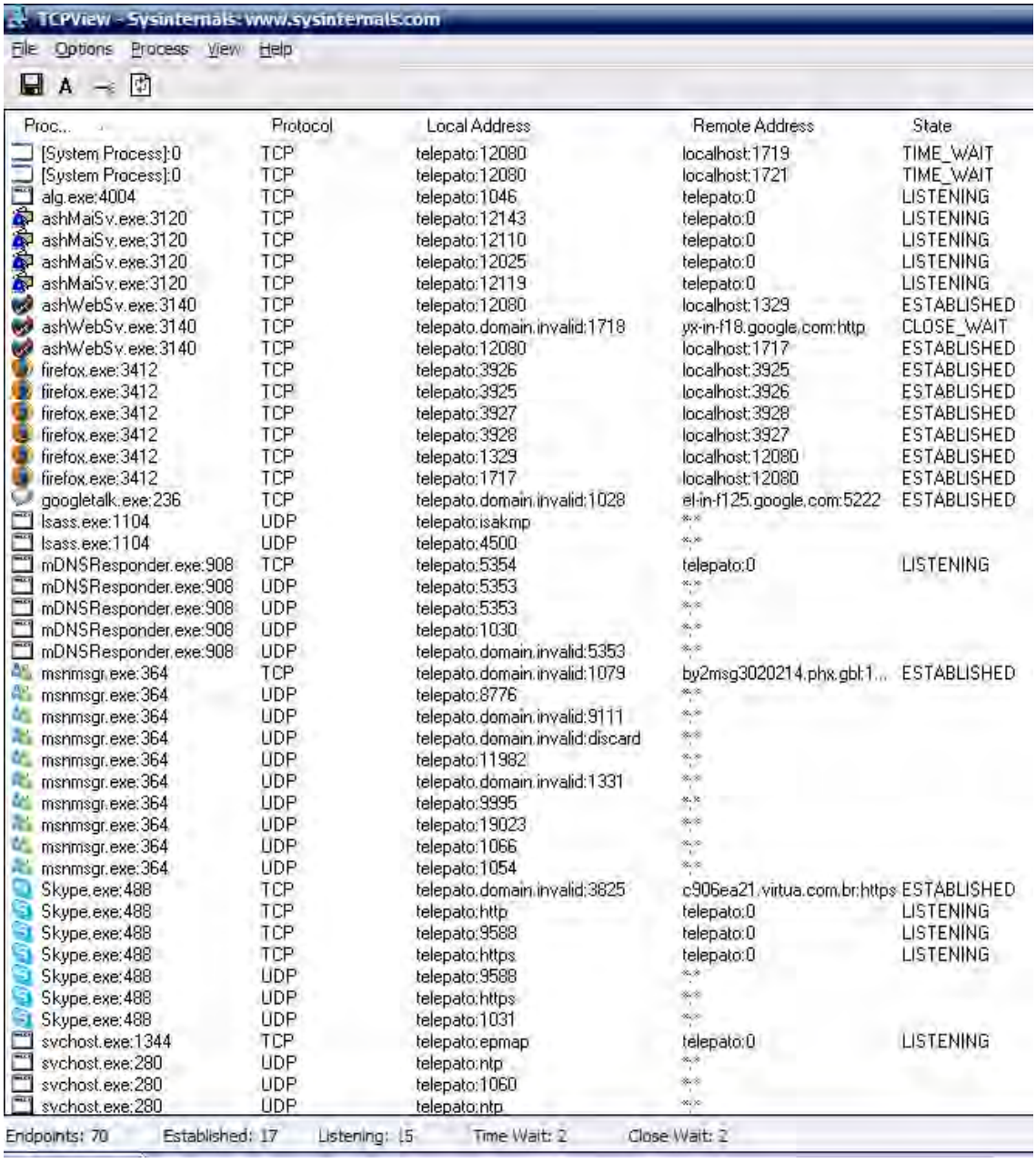


Figura 11 – TCPView versão 2.54.

3.3 FDTK-UbuntuBr – Forense Digital ToolKit

O FDTK é um projeto livre que objetiva a produção de uma distribuição *live* cd para coleta e análise de dados, bastante poderosa, em perícias computacionais e com a finalidade principal de ajudar os peritos.

Ideal para uso no meio acadêmico e por ter a licença GPL (*Global Public License* – Licença Pública Geral) facilitando o seu estudo, principalmente os códigos fontes dos programas de auditoria, porque o perito sabe exatamente o que cada utilitário faz.

Portanto, foi criado aqui no Brasil um Linux com essas características, chamado de FDTK-UbuntuBR, que tem dentro dela, mais de 100 ferramentas capazes de atender a todas as etapas de uma investigação forense. Com a interface bem amigável, como visto na Figura 12 e com o idioma em português.

Figura 12 – FDTK-UbuntuBR

3.3.1 Coleta de Dados

O FDTK é bem intuitivo e segue a sequência padrão para iniciar a perícia forense, portanto o primeiro passo é a coleta dos dados, mostrado na Figura 13.

Figura 13 – Coleta de Dados

3.3.1.1 Cadeia de Custódia e Capturar Imagem

Logo no início há um programa que gera um formulário para construir a Cadeia de Custódia e logo após, Capturar a Imagem da tela da estação a ser auditada.

3.3.1.2 Criar Imagem dos Dados

Nesta aba há um conjunto de utilitários para gerar uma imagem das evidências, como: dd, aimage, dd_rescue e outras mais. A mais usada é o utilitário dd, então ele gerará o arquivo da imagem com a extensão dd. Este programa também faz o *dump* de memória, como veremos a seguir.

3.3.1.3 Dump de Memória

Dump de Memória é o nome do processo de capturar informações da memória. A memória quanto mais rápida for capturada, mais informações serão armazenadas, pois ela se perde muito rápido.

3.3.1.4 Geração de HASH

E como faço para provar que esses arquivos coletados são verdadeiros e não foi mudado durante as investigações ou até no deslocamento deles. Portanto, na aba Geração de HASH, que é um grupo de utilitários que calculam este *hash*, ou seja, é uma transformação de uma grande quantidade de informações em uma sequência hexadecimal. O md5sum é um software que gera uma assinatura digital de qualquer arquivo. Ele é um código de 32 bits que é a soma de todos os bits contidos no arquivo.

O md5sum funciona do seguinte modo:

Ele gera um código a partir de um arquivo, por exemplo, um arquivo texto chamado “bibliografia.txt”, ele gerará este código:

- 22a6c8f1eae563c2118fff86f4ba8eea.

Se mudar e colocar dentro deste texto, uma letra “a”, o código será:

- 8014ea940d476838580529ed28384fb0.

Houve uma grande mudança no código, mostrando que é um programa confiável. Sabendo disto, para que se tenha uma boa perícia e que se prove ao final do processo que nada foi modificado na estação de trabalho e garantindo a integridade dos dados.

Os softwares mais usado são o md5sum, como falado, e sha512sum, com comando em linha de texto simples, por exemplo:

- md5sum [opção] arquivo
- sha512sum [opção] arquivo

3.3.1.5 Identificação do Hardware

Para saber qual a estação de trabalho o perito vai trabalhar precisa conhecer com detalhes os periféricos e qual versão do sistema operacional, portanto na

Identificação do HW, mostra todas as informações que o perito precisará para iniciar sua investigação.

3.3.1.6 Limpa Mídias

E por último, Limpa Mídias, que é para salvar a imagem em uma mídia como USB, limpa e que não mude o *hash*, garantindo a integridade dos dados.

3.3.2 Exame dos Dados

Após a coleta, o calculo do *hash*, gravação das imagens e guardar as evidências originais em local seguro, os dados serão examinados detalhadamente e tentará encontrar provas em que o suspeito é um pedófilo ou que ele tenha um *Malware* instalado na sua máquina sem que ele saiba e inocentando o suspeito. Nesta distribuição mostra estes detalhes conforme visto na Figura 14.

Figura 14 Exame dos Dados

3.3.2.1 Antivirus & Malware

Utilitário que vai procurar se há vírus ou *Malwares* no sistema investigado, pois se tiver, o suspeito poderá ser inocentado, porque os arquivos sobre pedofilia foi colocado em seu computador sem o consentimento do dono. A Ferramenta usada é a chamada nepenthes, de código livre, que coleta o *malware* emulando vulnerabilidades disseminadas atraindo-o e assim estudando o que ele poderá fazer no sistema.

3.3.2.2 Arquivos Compactados

Alguns arquivos ficam compactados para que na busca por outros dados como fotos, ficam escondidos nestes arquivos e assim demorando mais a investigação no sistema, então este conjunto de ferramentas facilita esta procura, descompatando-os seguramente.

- **cabextract:** Acessa conteúdo de arquivos .cab
- **orange:** Ferramenta que manipula arquivos .cab
- **p7zip:** Acessa o conteúdo de arquivo ZIP
- **unace:** Ferramenta de descompactação .ace
- **unrar-free:** Ferramenta de descompactação de arquivos RAR
- **unshield:** Ferramenta para descompactar arquivo da Microsoft .cab
- **Xarchive:** Cria, modifica e acessa arquivos compactados.
- **zoo:** Acessa arquivos compactador em .zoo

3.3.2.3 Arquivos de Imagem

Para este trabalho, o mais importante, pois nestas ferramentas, eles procuram e analisam cada arquivo de imagens, pelo o motivo que um bom hacker esconderia alguma informação dentro da imagem.

3.3.2.4 Arquivos MS

Um bom perito conhece o sistema de arquivos de um sistema operacional. Neste local, mostra as ferramentas em que pudemos usar para investigar o Microsoft Windows®, como:

- Dumpster: Ver o conteúdo da lixeira
- Readpst: Ferramenta que ler arquivos do MS-Outlook
- RegLookup: Utilitário ler e resgata os dados do registro do Windows
- Regp: Acessa os conteúdos de arquivos .dat
- Tnef: Acessa anexos de emails do MS-Outlook

3.3.2.5 Crypto-Stegano

Se alguém gostaria de esconder alguma informação e que tenha uma segurança perto dos 100% confiável, então ela criptografará seus dados ou apenas esteganografá-las, ou seja, esconder um conteúdo dentro de um arquivo como uma imagem. Para descobrir, há ferramentas específicas que procura dados ocultos imagens com extensão jpg, programas que encripta e decripta arquivos.

3.3.2.6 Localizar Dados

Programa básico para localizar arquivos. Ele procura dentro de imagens mesmo com extensões dd, se for o caso.

3.3.2.7 Mactime dos Dados

Como foi visto, os mactimes são atributos aos arquivos de tempo, modificação e acesso. Nesta sessão há duas ferramentas, a Mac-robber que serve para coletar os dados em um sistema de arquivos montada e o mactime que gera uma linha do tempo das atividades dos arquivos.

3.3.2.8 Partições NTFS

Usado em sistemas operacionais Microsoft Windows, portanto neste local, se encontra todas as ferramentas que pode ser usada sem nenhum problema, como encontrar arquivos, clonar os arquivos e obter informações sobre o sistema e seus arquivos.

3.3.2.9 Quebra de Senhas

Se um arquivo ou sistema estiver protegido com senha, serão usados estes utilitários e neste trabalho se utilizará a ferramenta John the Ripper que localiza as senhas dos usuários, se for necessário.

3.3.2.10 Restaurar Dados

Lista de ferramentas em recuperar dados apagados, corrompidos de qualquer sistema de arquivos.

3.3.2.11 RootKits

Os Rootkits são um tipo de Malware que a sua principal intenção é se camuflar, impedindo que seu código seja encontrado por qualquer antivírus e depois tentar acesso irrestrito ao sistema. Portanto, na ferramenta rkhunter, ou seja, ele é um caçador de RootKits, pode detectar Trojans e problemas de segurança.

3.3.3 Análise das Evidências

Após coletar e examinar os dados, o perito irá analisar as evidências que ele viu que era mais importante e foi para a terceira etapa que são essas análises, como visto na Figura 15.

Figura 15 – Análise das Evidências

- **Cookie_cruncher:** Analise os *Cookies* do Sistema
    - Exemplo: # /usr/share/fdtk-sh/cookie_cruncher.pl <arquivo de cookie>

- **Eindeutig**: Analisa os arquivos mbx, ou seja, os arquivos de correio eletrônico como caixa de entrada, saída e lixeira.

- **Galleta**: Analisa os *cookies* do Microsoft Windows.
    - Exemplo: #galleta [opções] <arquivo de cookie>

- **Mork**: Utilitário de análise dos arquivos dat (que são arquivo de dados e podem pertencer a qualquer tipo de programa) do Mozilla FireFox.

- **Pasco**: Analisa o cache do Internet Explorer
    - Exemplo: #pasco [opções] Pasta do Cache

- **Traceroute**: É uma ferramenta que permite descobrir o caminho feito pelos pacotes desde a sua origem até o seu destino.
    - Exemplo: #traceroute <IP de destino**>**

- **Xtraceroute:** Versão gráfica do traceroute

3.3.4 ToolKit

O autopsyg é uma ferramenta gráfica de código aberto para a Perícia Forense. Criado por Brian Carrier. Ele pode investigar o sistema enquanto estiver desligado ou ligado, ou seja, morto ou vivo. Ver Figura 16.

Figura 16 – A Ferramenta Autopsy

Maiores informações sobre o AFB podem ser encontradas em suas páginas manuais ou na página http://www.sleuthkit.org/autopsy/

3.4 Helix

O Helix é uma distribuição baseada na distribuição Linux Ubuntu, criada em 2005 utilizando a distribuição knoppix, trata-se de uma distribuição dedicada à investigação forense digital e usada como ferramenta de estudo.

Ele foi modificado de forma a que não danifique de qualquer forma no sistema a ser investigado. A Figura 17 mostra a tela inicial do Helix.

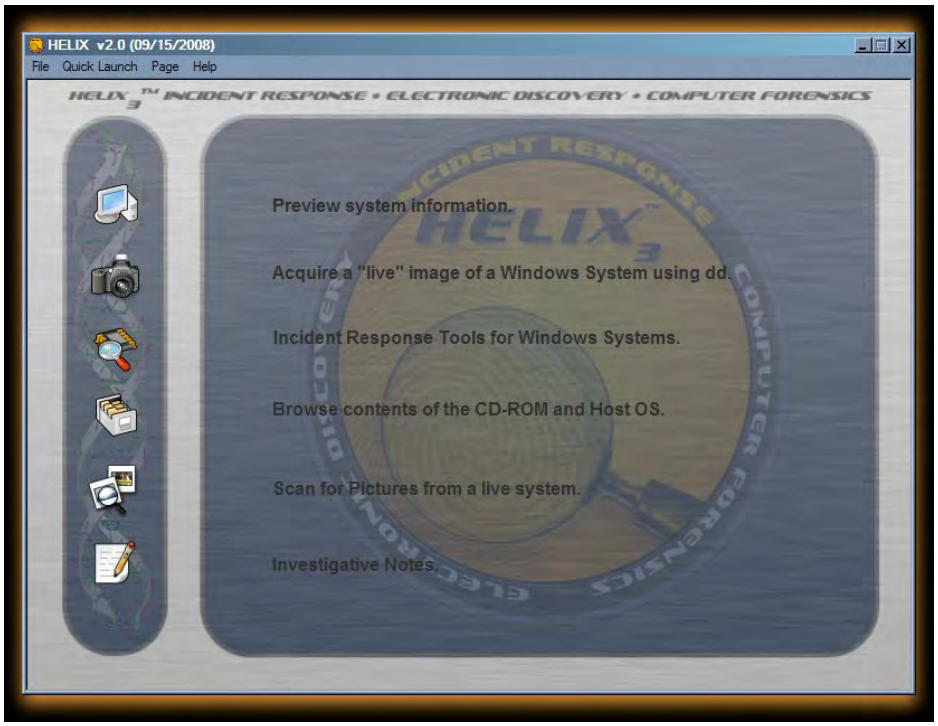


Figura 17 – Tela Inicial do Helix

Iniciando a auditoria, então serão usados programas de acordo com a sequência do estudo padrão de investigação, como será visto a seguir.

3.4.1 Coleta

Coletando os dados, então o investigador saberá sobre as informações do Sistema, o qual ele pode coletar as imagens dos discos rígidos e memórias voláteis como as RAMs, usando os próprios utilitários do Helix ou a ferramenta da empresa AccessData, FTK Imager, como visto nas Figura 18 e Figura 19, respectivamente.

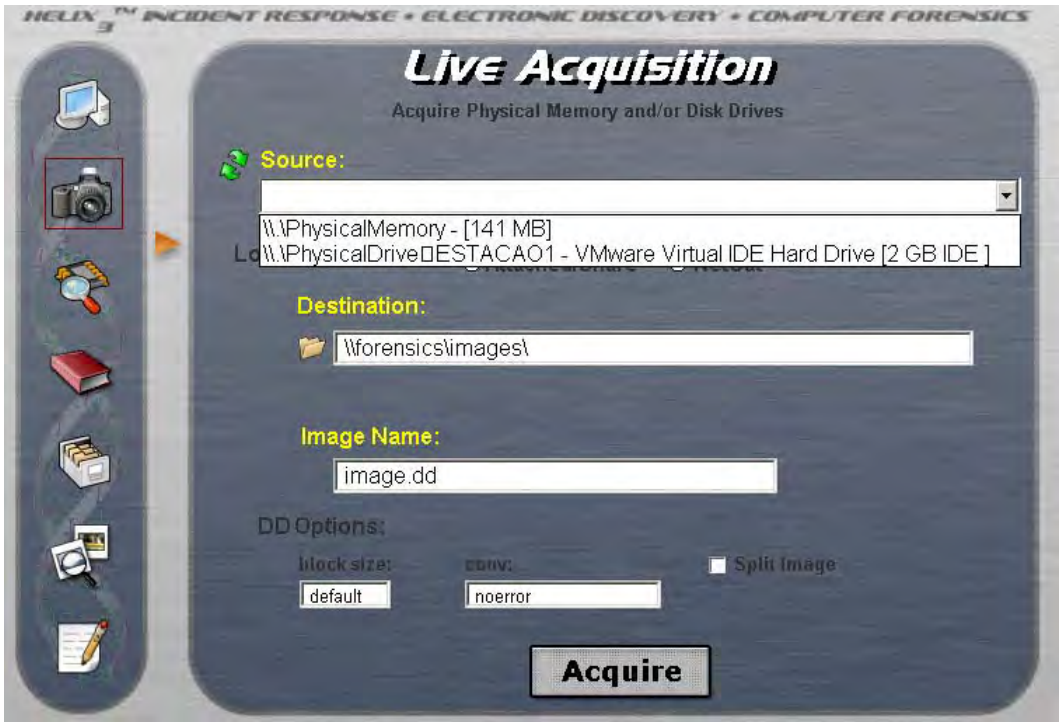


Figura 18 – Utilitários do Helix para fazer uma imagem

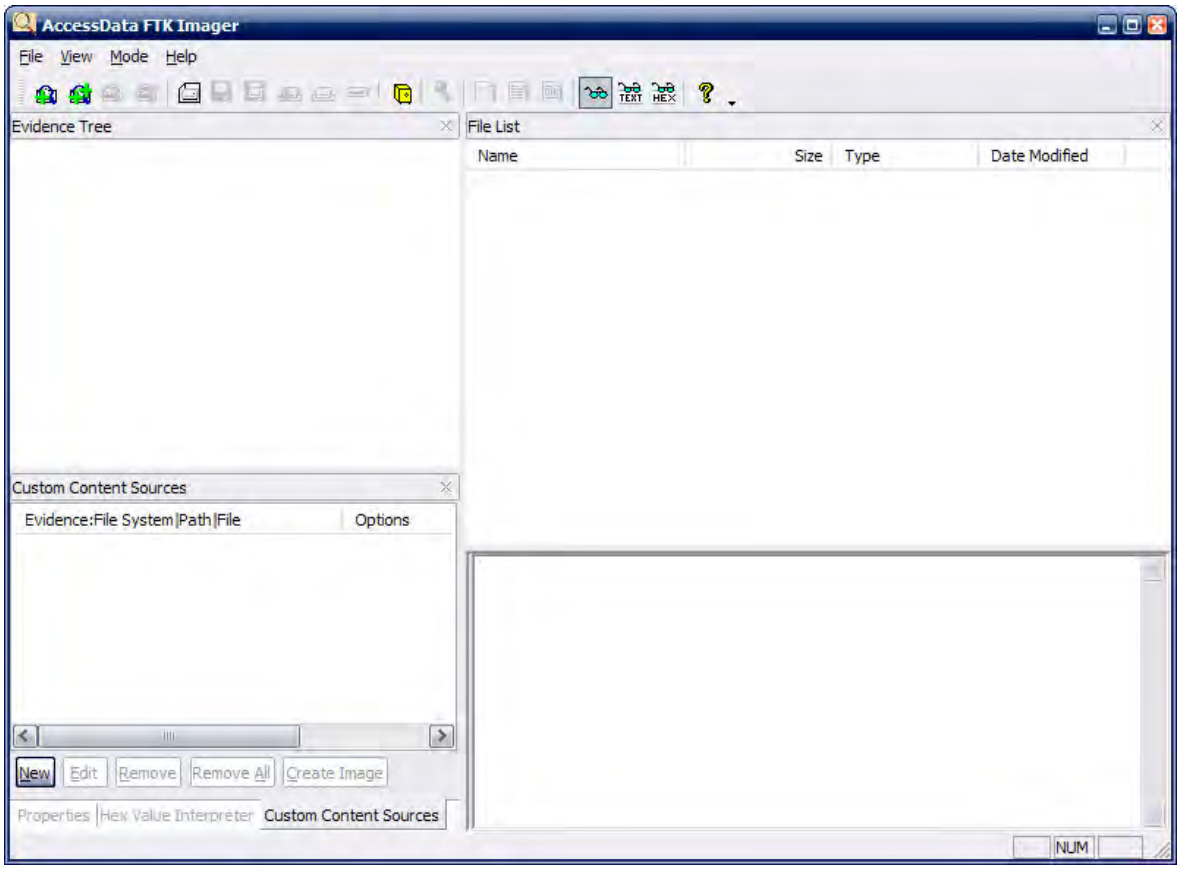


Figura 19 – FTK Imager

3.4.2 Exame

Com a coleta, é necessário tirar o *hash* e garantindo a integridade dos dados que serão analisados com a própria ferramenta, conforme visto na Figura 20

Figura 20 – Exame dos Dados, calculando o Hash pelo Helix

Pode-se procurar se há algum Rootkit no sistema, usando a ferramenta Rootkit Revealer, “tirar fotos” do sistema com o Screen Capture e até tentar recuperar arquivos possivelmente danificados.

Na terceira página (ver Figura 21) tem programas para encontrar senhas de arquivos PST, que é um arquivos do Microsoft Outlook e o Mail Password Viewer que é para quebrar as senhas dos programas de correio eletrônico instalado no sistema.

Figura 21 – Coleta dos Dados do Helix, página 3.

O *Messenger Password serve para obterr* as senhas salvas nos programas de mensagens instantâneas, mostrado na Figura 22 em um computador privado. Enquanto que no ícone de *Protected Storage Viewer*, descobre as senhas que são armazenadas em *sites* como também a ferramenta IE Password Viewer.

Figura 22 – Messenger Password na Prática

Para ver o históricos dos *sites* visitados pelo Internet Explorer e arquivos explorados no Windows, então é usado pelo aplicativo *IE History Viewer* (ver o exemplo na Figura 23) e para ver os cookies tanto do navegador da Microsoft e do Mozilla, o Firefox, há 2 programas: IE Cookie Viewer e o Mozilla Cookie Viewer.

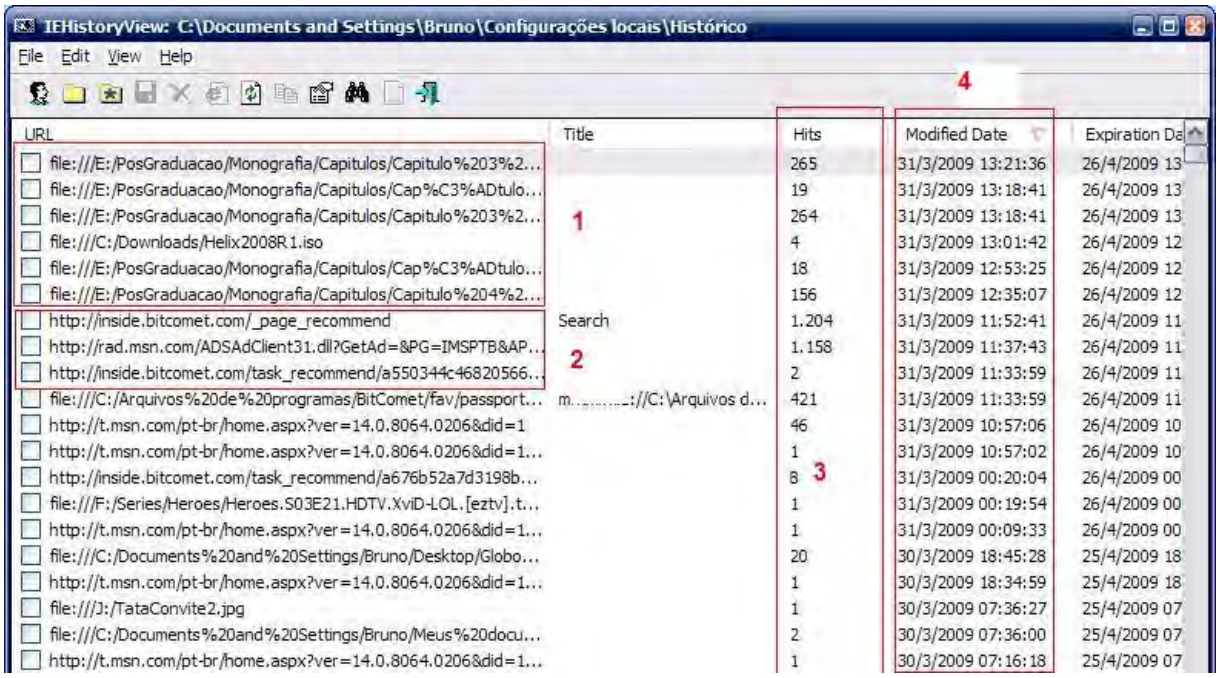


Figura 23 – IEHistoryView

1 – Arquivos Acessados

2 – Sites Visitados

3 – Quantidade de acessos

4 – Data de Modificação

No aplicativo, Mail Password View, é outro modo de conseguir os usuários e senhas de quem usa programas de correio eletrônico e salva suas senhas no próprio Windows. A seguir, vemos na Figura 24, um exemplo usando um computador privado.

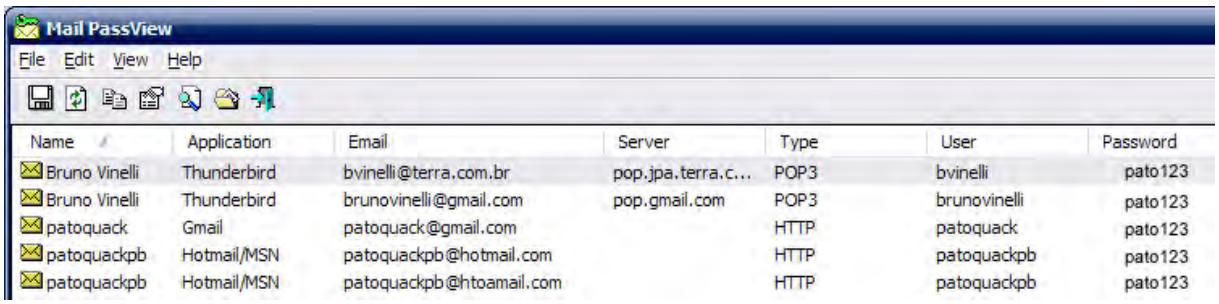


Figura 24 – Mail Password View na prática

Já no Registry Viewer, verifica o registro do sistema e o Asterisk Logger, revela as senhas que quando é digitado aparece apenas o asterisco.

Finalizando, o aplicativo USB Deview, mostra toda vez que uma porta de USB foi usada e qual foi o periférico que trocou informações com o sistema, com detalhes, ver exemplo da Figura 25.

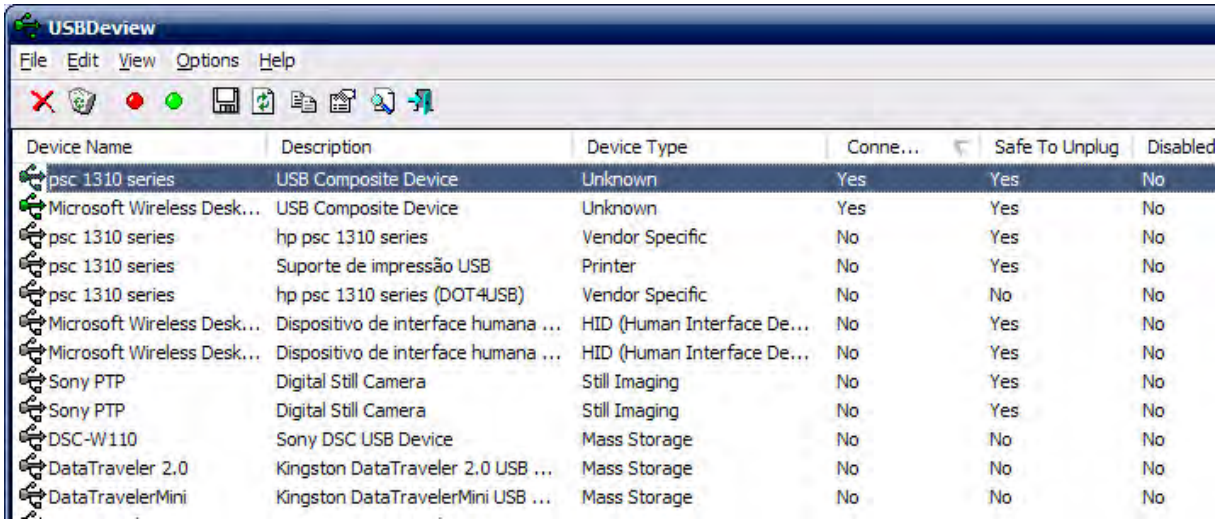


Figura 25 - USBDeview

Terminando esta fase de exames dos dados coletados, o perito vai fazer a análise detalhada de cada arquivo examinado.

.

3.4.3 Análise

Nesta etapa, o perito fará a análise bem detalhada para procurar qualquer vestígio que prova que o suspeito é um pedófilo ou não. Portanto, cada aplicativo que foi utilizado, agora será filtrado e procurar com detalhes cada arquivo coletado e examinado e sempre calculando o seu hash para garantir que nada foi modificado durante a investigação.

CAPÍTULO 4 - INVESTIGAÇÃO NO SISTEMA OPERACIONAL DA MICROSOFT

O Sistema Operacional proprietário da Microsoft é o mais usado na atualidade, principalmente nas faixas etárias dos perfis dos pedófilos.

> Na maioria dos casos apurados pela polícia, o perfil é de um homem entre 30 e 45 anos, solteiro, que mora sozinho, é reservado, inseguro, tem dificuldade de manter relações afetivas por muito tempo e, em alguns casos, cansou de consumir pornografia adulta, migrando para a pedofilia. (NUBLAT, Johanna IGLESIAS, Simone. 2008)

Portanto, em sua totalidade são usuários deste sistema operacional e muito pouco conhecimento do Sistema Operacional Linux. Daí, a investigação deste trabalho ser totalmente no ambiente da Microsoft.

> De acordo com a preferência sexual pode-se verificar a existência de outros grupos que estão envolvidos com a sedução de menores, classificados dentro de categorias como: Hebefilia (preferência por adolescentes) e Ninfofilia (preferência por meninas).[...] Os *Boys Lovers,* não obstante afirmarem que são apenas admiradores da figura angelical das criancas, dando conotação artísticas para a imagens. (RODRIGUES, Jorison da Silva, 1999. p.16)

Então, este trabalho, é uma proposta para o procedimento para encontrar arquivos de pedofilia em uma estação Windows XP, de início há uma necessidade de mandado judicial de busca e apreensão do computador do suspeito. Após a chegada no local, inicia-se o processo que veremos a seguir.

Para fins didáticos, será usada, uma máquina virtual, usando um programa específico, com o Sistema Operacional da Microsoft. Conforme a Tabela 2 é mostrada um modelo para investigar um caso de pornografia infantil.

Tabela 3 – Modelo para Investigar um computador suspeito

Objetivo	Distribuição	Software
Coletar Imagens	FDTK HELIX	dd
Avaliar se há algum Malware	Windows Sysinternals	autoruns
Avaliar se há algum Malware	Windows Sysinternals	ProcessExplorer
Avaliar se há algum Malware	Windows Sysinternals	TCPView
Tirar o Hash do arquivo	FDTK	md5sum
Encontrar Fotos	Windows XP	Pesquisar Arquivos ou Pastas e Lixeira
Encontrar Fotos	Windows XP	Arquivos Temporário da Internet
Encontrar Fotos	Windows XP	Cookies
Quebrar Senha	Windows XP	John The Ripper
Visualizar Senhas do Windows	Helix	PST Password Viewer
Vizualizar os histórico do Internet Explorer	Helix	IEHistory Viewer
Timeline	Helix	FTK Imager

4.1 Coleta

O primeiro passo de um bom perito, que é chamado pelo termo em inglês, *First Reponser,* é avaliar a situação, se o computador está ligado ou não. Estando ligado, então este perito tirará fotos do local, do programa que esta sendo executado naquela hora, para que se possa fazer a reconstituição perfeita, após o registro fotográfico. Com um Pendrive limpo de vírus e próprio para fazer este tipo de auditoria, ele vai capturar os processos e arquivos armazenados da memória, obedecendo a sua ordem de volatilidade. O perito fará o *dump* da memória, isto é, gravar o que tem dentro dela naquele exato momento, pois qualquer descuido como desligar o computador, ela se apagará e os dados que estavam dentro dela se

perderão. Para fazer este *dump* e a cópia será feita em uma mídia de apenas de leitura como um cd-rom ou DVD-rom, impedindo escritas acidentais. Utilizando a ferramenta dd, que permite também copiar os fluxos dos dados com os seguintes comandos:

```
# dd if=/dev/mem of=mem.dump bs=1024
# dd if=/dev/kmem of=kmem.dump bs=1024
```

Esta execução deste procedimento causa alteração de uma parte da memória, impossibilitando verificar futuramente se estas informações são iguais as das originais.

E após esta etapa, usando as ferramentas do Sysinternals poderá avaliar se o computador tem algum Malware, e que este esteja baixando essas fotos de pornografia e assim obter a inocência do suspeito.

Um dos exemplos é o utilitário Autoruns, falado no Capítulo 2 e aqui veremos algumas aplicações práticas, mostrado na Figura 26 e assim, comprovando, neste caso. que não há nenhum Malware, pois cada aplicativo está correspondido com o seu fabricante.

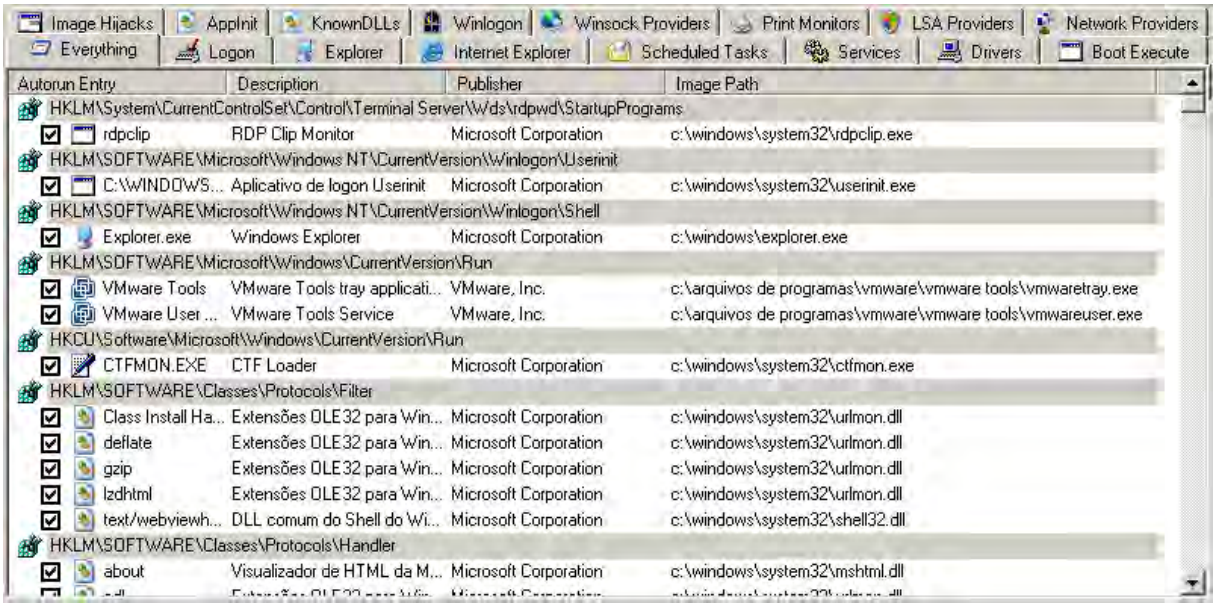


Figura 26 – Autoruns Executado na Máquina Virtual

Com esta análise pósinicial, o próximo passo é verificar os processos que estão em execução naquele instante, portanto será usado o aplicativo do Sysinternals, Process Explorer, mostrando na Figura 27. Por esta figura é verificado que não há nenhum vírus ou cavalo de tróia em seus processos, portanto se houver alguma foto nesta máquina virtual, até neste momento, poderá ter sido o dono do computador auditado.

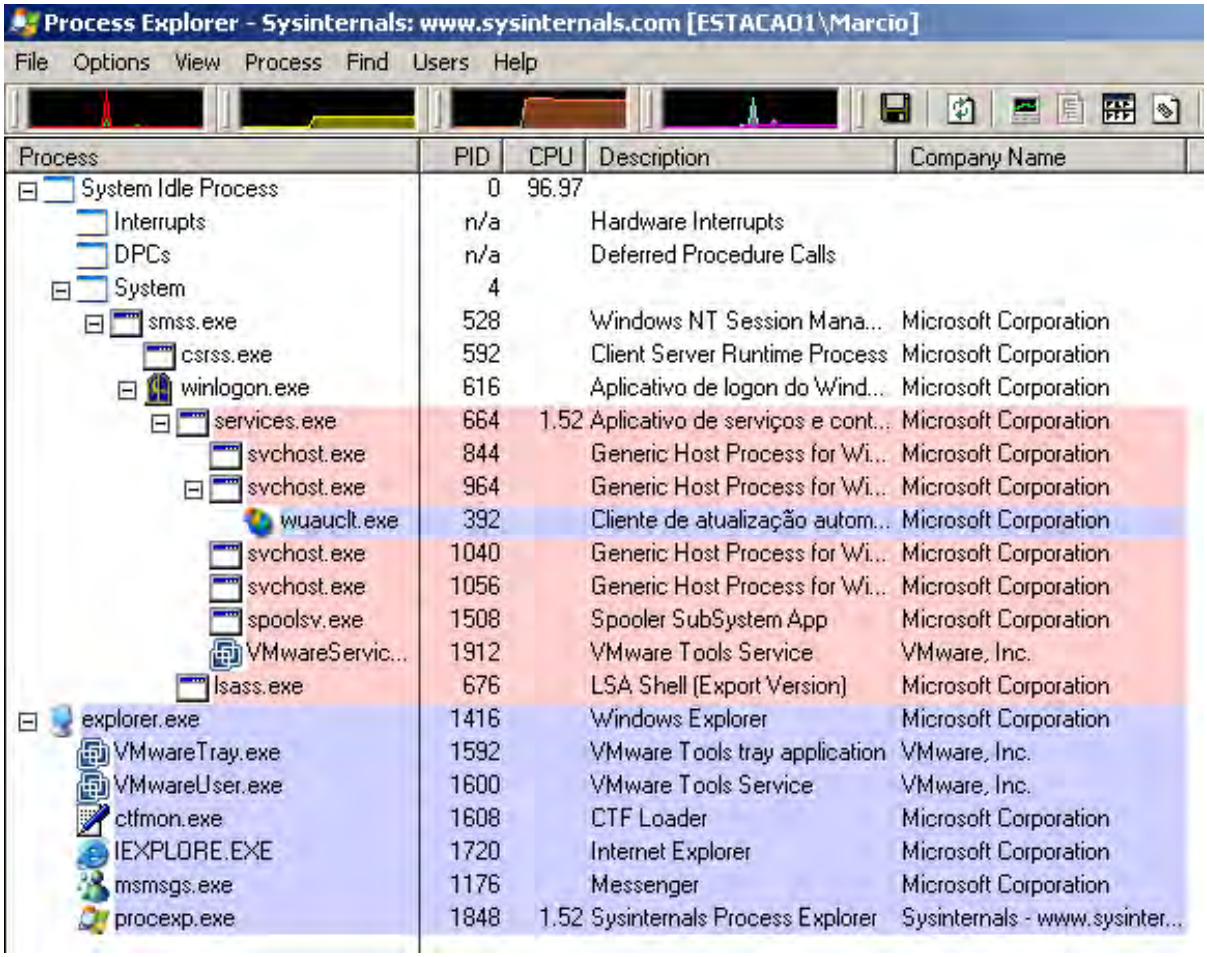


Figura 27 – Process Explorer da Máquina Virtual

Outra captura importante é o tráfego da rede através de programas como *sniffers* (farejadores). Além de capturar os pacotes, estes programas podem decodificar e exibir os arquivos em um formato legível e ter uma ideia de quais os programas está trocando informações com esta estação. Um bom utilitário é a ferramenta do Sysinternals, o TCPView, que mostra as conexões no momento em que o programa foi executado. Na Figura 28, é mostrado a tela sendo executada na máquina auditada. Conforme visto, não há nenhuma conexão “estranha”.

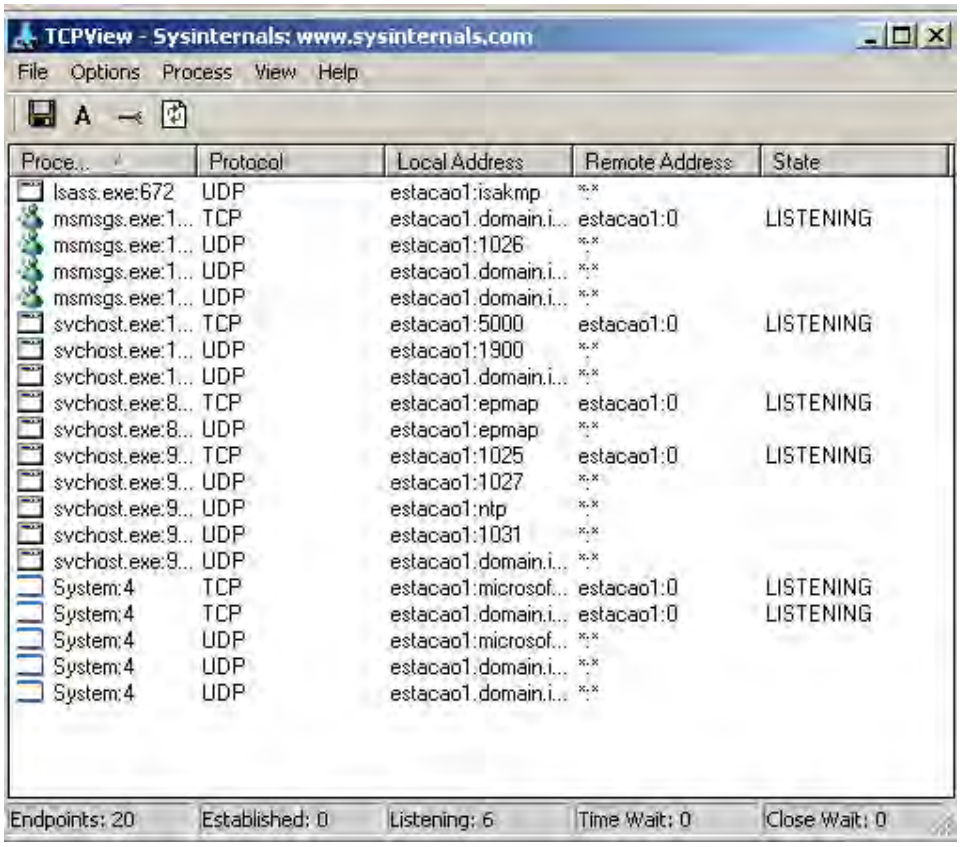


Figura 28 – TCPView da Máquina Virtual

Com a memória salva e verificada se tinha algum Malware na máquina auditada, então será tirada a imagem dos discos, este princípio é obter toda a informação contida no computador, seja ela pertencente a um sistema de arquivos ou não, de tal forma que a imagem possa ser examinada como se fosse o disco original. Neste trabalho será usada a ferramenta dd, que faz este tipo de cópia exatamente igual do início ao fim e nunca utilizar programas de cópia de backup, pois ele copia apenas os dados reconhecidos pelo o sistema de arquivo.

E logo após tirar o *hash* de cada disco e seus arquivos, mostrando que são iguais. O programa utilizado é o md5sum e para garantir esta integridade:

- md5sum arquivo

E garantindo mais a integridade dos dados será usado também o sha512sum, para que não tenham dúvidas de sua veracidade:

- sha512sum arquivo

Sempre, fazer isso com pelo menos uma testemunha de conduta ilibada. Estas réplicas serão usadas para fazer testes para inocentar ou culpar o suspeito, enquanto que o disco original ficará guardado com toda segurança de queda ou de campos magnéticos que possam danificar as evidências, que é chamado de cadeia de custódia e finalizando o processo de auditoria com o computador ligado.

Para desligar o computador investigado é aconselhável que desligue da tomada e não finalizar indo em iniciar e desligar o computador, pois fazendo isto poderá executar algum utilitário e apague as provas. Outro detalhe é que alguns arquivos seriam modificados pelo próprio Microsoft Windows® após desligado, não reiniciá-lo, apenas usar suas imagens e se precisar refazer, tirar uma cópia com o computador desligado.

Se o computador estiver já desligado, então ele não será ligado, apenas tirar fotos, lacrado e levado para o laboratório. Com testemunhas, será aberto e retirado os discos, colocado em um computador que tenha a distribuição Linux FDTK-UbuntuBR e usado o programa dd e criado a imagem, tirar os *hashes* e guardar para se puder ser usado em um futuro próximo.

4.2 Exames dos Dados

Com as imagens dos discos feitas, haverá um exame de todos os dados e assim filtrá-los para analisá-los mais a frente, se for necessário.

Nesta etapa, é a fase que poderá inocentar o suspeito, pois nela faremos um estudo detalhado do sistema e será procurado que existe mais vírus e outros *malwares* que não foram encontrados na coleta e que ainda possam colocar fotos sem que o usuário suspeito saiba, pois sua estação está sendo usada como uma Botnet (ver no glossário). Os programas usados são: o nephentes para encontrar um *malware* e rkhunter para a procura de algum rootkit.

Não encontrando nenhum *malware*, então o perito irá procurar em locais dos arquivos mais comuns como:

4.2.1 Arquivos de imagens

Algumas ferramentas simples do Windows como, Pesquisar, Arquivos ou Pastas e ir na opção “Imagens e Fotos” e colocar para pesquisar, podendo ser muito útil.

Na máquina virtual foi usado um exemplo simples com arquivos salvos da Internet, porém sem conteúdo pornográfico, apenas com nomes suspeitos, visto na Figura 29.

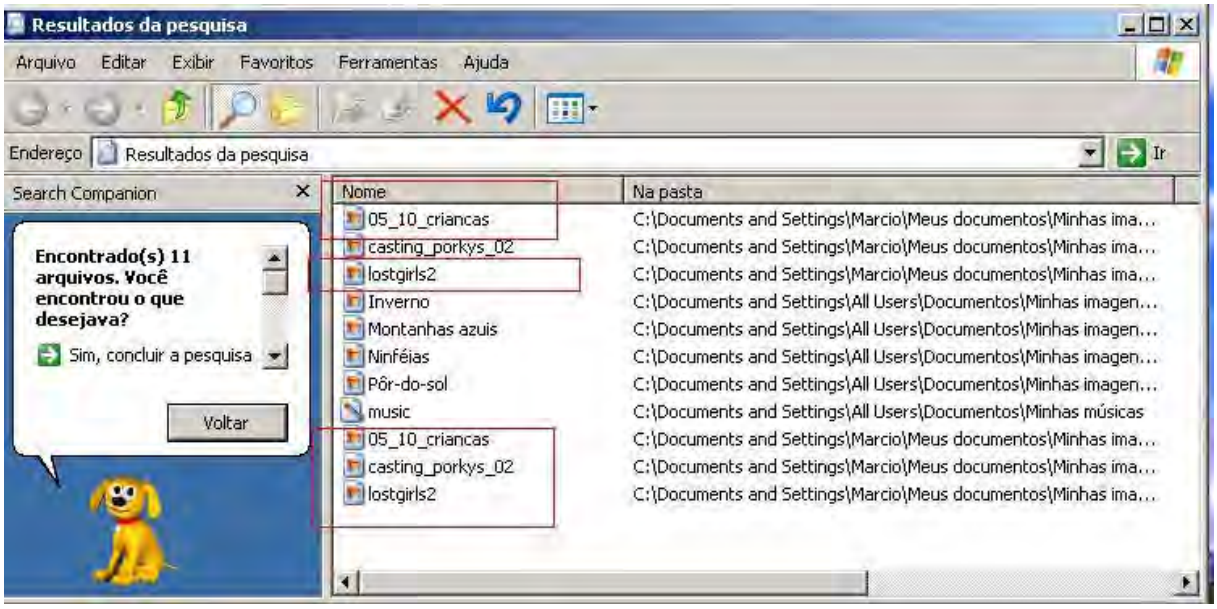


Figura 29 –Resultado da Pesquisa de Imagens e Fotos do Windows XP

Portanto, há nomes suspeitos onde tem quadrados vermelhos na Figura 25, assim ver o conteúdo, pois este detalhe pode ser apenas o início de uma investigação mais detalhada.

4.2.2 Arquivos compactados

Arquivos compactados em si não têm nenhum problema, só é apenas trabalhoso ver um por um para saber se há fotos ou indícios de pornografia infantil. Porém, se ele estiver com uma senha de segurança, pode se tornar bem difícil, no entanto há programas especialistas em quebrar essas senhas.

Outro exemplo de um arquivo compactado são os com extensões “.cab”. No Sistema Operacional FTDK-UbuntuBR, contém uma ferramenta para acessar o conteúdo desta extensão que é *cabextract* ou *unshield* e outra ferramenta para manipular este tipo de arquivo, o *orange*.

4.2.3 Lixeira

Quando um arquivo do Windows é apagado, ele fica armazenado na Lixeira e permanece neste local até que esvazie ou restaure este arquivo. Mesmo assim, se o usuário apagou da Lixeira, ainda é possível recuperá-lo. Quando o arquivo é esvaziado, ele vai para o local chamado *Recycled* ou *Recycled*.

4.2.4 Arquivos temporários de navegadores de Internet

Uma pessoa experiente em esconder suas pistas, por onde passou, ela vai tentar apagar estes registros, se houver tempo.

Usando a máquina virtual, neste endereço do sistema.

- **C:\Documents and Settings\Marcio\Configurações locais**

É onde ficam as configurações locais e os arquivos temporários.

Na pasta a seguir:

- **C:\Documents and Settings\Marcio\Configurações locais\Histórico**

Dentro desta pasta, é o histórico da Internet, quais os sites que foram acessados, como visto na Figura 30, Figura 31 e Figura 32, mostrado com detalhes.

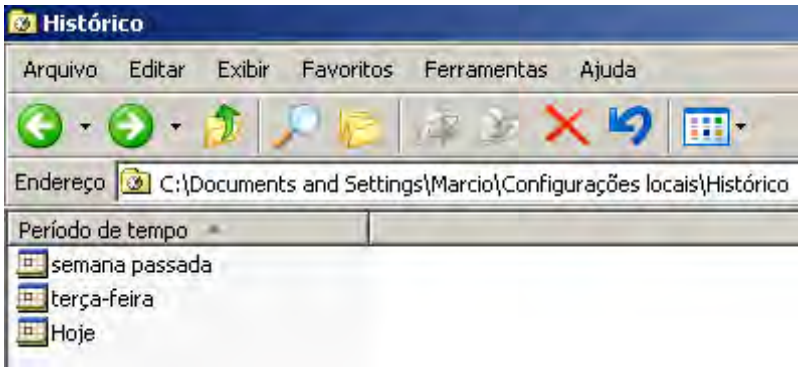


Figura 30 – Dentro da Pasta C:\Documents and Settings\Marcio\Configurações locais\Histórico

Figura 31 – Registro dos Sites Acessado Semana Passada

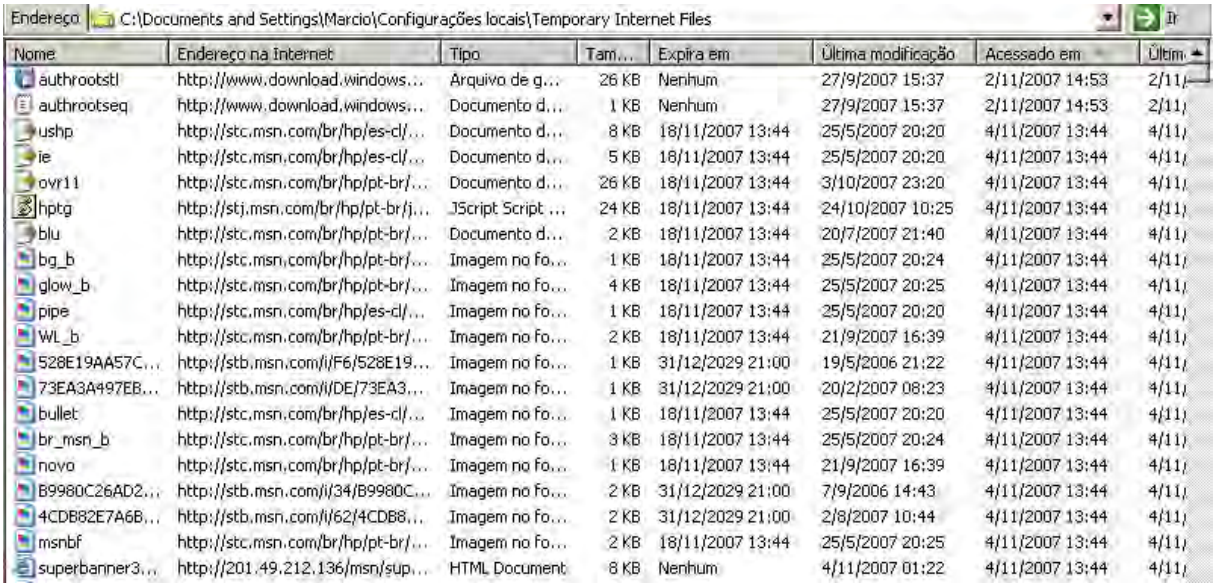
Figura 32 – O que foi pesquisado no Google

Ou seja, o suspeito acessou o *site* do Google e fez uma pesquisa sobre *boylovers* e fotos.

Outro local importante é:

- **C:\Documents and Settings\Marcio\Configurações locais\Temporary Internet Files**

O Temporary Internet Files, ver Figura 33, é um diretório ou pasta da Microsoft Windows. Esta pasta é usada pelo Internet Explorer para cache de páginas e seus conteúdos como vídeo e áudio dos sites visitados anteriormente, permitindo que a página seja carregada mais rapidamente.



Nome	Endereço na Internet	Tipo	Tam...	Expira em	Última modificação	Acessado em	Últim
authrootstl	http://www.download.windows...	Arquivo de g...	26 KB	Nenhum	27/9/2007 15:37	2/11/2007 14:53	2/11/
authrootseq	http://www.download.windows...	Documento d...	1 KB	Nenhum	27/9/2007 15:37	2/11/2007 14:53	2/11/
ushp	http://stc.msn.com/br/hp/es-cl/...	Documento d...	8 KB	18/11/2007 13:44	25/5/2007 20:20	4/11/2007 13:44	4/11/
ie	http://stc.msn.com/br/hp/es-cl/...	Documento d...	5 KB	18/11/2007 13:44	25/5/2007 20:20	4/11/2007 13:44	4/11/
ovr11	http://stc.msn.com/br/hp/pt-br/...	Documento d...	26 KB	18/11/2007 13:44	3/10/2007 23:20	4/11/2007 13:44	4/11/
hptg	http://stj.msn.com/br/hp/pt-br/j...	JScript Script ...	24 KB	18/11/2007 13:44	24/10/2007 10:25	4/11/2007 13:44	4/11/
blu	http://stc.msn.com/br/hp/pt-br/...	Documento d...	2 KB	18/11/2007 13:44	20/7/2007 21:40	4/11/2007 13:44	4/11/
bg_b	http://stc.msn.com/br/hp/pt-br/...	Imagem no fo...	1 KB	18/11/2007 13:44	25/5/2007 20:24	4/11/2007 13:44	4/11/
glow_b	http://stc.msn.com/br/hp/pt-br/...	Imagem no fo...	4 KB	18/11/2007 13:44	25/5/2007 20:25	4/11/2007 13:44	4/11/
pipe	http://stc.msn.com/br/hp/es-cl/...	Imagem no fo...	1 KB	18/11/2007 13:44	25/5/2007 20:20	4/11/2007 13:44	4/11/
WL_b	http://stc.msn.com/br/hp/pt-br/...	Imagem no fo...	2 KB	18/11/2007 13:44	21/9/2007 16:39	4/11/2007 13:44	4/11/
528E19AA57C...	http://stb.msn.com/i/F6/528E19...	Imagem no fo...	1 KB	31/12/2029 21:00	19/5/2006 21:22	4/11/2007 13:44	4/11/
73EA3A497EB...	http://stb.msn.com/i/DE/73EA3...	Imagem no fo...	1 KB	31/12/2029 21:00	20/2/2007 08:23	4/11/2007 13:44	4/11/
bullet	http://stc.msn.com/br/hp/es-cl/...	Imagem no fo...	1 KB	18/11/2007 13:44	25/5/2007 20:20	4/11/2007 13:44	4/11/
br_msn_b	http://stc.msn.com/br/hp/pt-br/...	Imagem no fo...	3 KB	18/11/2007 13:44	25/5/2007 20:24	4/11/2007 13:44	4/11/
novo	http://stc.msn.com/br/hp/pt-br/...	Imagem no fo...	1 KB	18/11/2007 13:44	21/9/2007 16:39	4/11/2007 13:44	4/11/
B9980C26AD2...	http://stb.msn.com/i/34/B9980C...	Imagem no fo...	2 KB	31/12/2029 21:00	7/9/2006 14:43	4/11/2007 13:44	4/11/
4CDB82E7A6B...	http://stb.msn.com/i/62/4CDB8...	Imagem no fo...	2 KB	31/12/2029 21:00	2/8/2007 10:44	4/11/2007 13:44	4/11/
msnbf	http://stc.msn.com/br/hp/pt-br/...	Imagem no fo...	2 KB	18/11/2007 13:44	25/5/2007 20:25	4/11/2007 13:44	4/11/
superbanner3...	http://201.49.212.136/msn/sup...	HTML Document	8 KB	Nenhum	4/11/2007 01:22	4/11/2007 13:44	4/11/

Figura 33 – Pasta do Temporary Internet Files

Outros arquivos para se investigar rastros, são os *Cookies*, ou seja, um *cookie* é um grupo de dados trocados entre o navegador e o servidor de páginas, colocado num arquivo de texto criado no computador do utilizador, mostrado na Figura 34.

Nome	Tamanho	Tipo	Data de modificac
index	32 KB	Arquivo DAT	13/3/2009 02:22
marcio@ad.yieldmanager[1]	1 KB	Documento de texto	7/3/2009 23:45
marcio@atdmt[1]	1 KB	Documento de texto	5/3/2009 00:03
marcio@br.msn[1]	1 KB	Documento de texto	7/3/2009 23:51
marcio@c.msn[2]	1 KB	Documento de texto	5/3/2009 00:03
marcio@cert[1]	1 KB	Documento de texto	5/3/2009 20:36
marcio@doubleclick[1]	1 KB	Documento de texto	5/3/2009 20:35
marcio@google.com[1]	1 KB	Documento de texto	7/3/2009 23:43
marcio@hometerra.terra.atmo.pre...	1 KB	Documento de texto	5/3/2009 20:35
marcio@ig.atmo.predicta.com[1]	1 KB	Documento de texto	7/3/2009 23:53
marcio@ig.com[1]	1 KB	Documento de texto	7/3/2009 23:53
marcio@live[1]	1 KB	Documento de texto	4/11/2007 13:44
marcio@msn[2]	1 KB	Documento de texto	5/3/2009 00:03
marcio@msnportal.112.2o7[1]	1 KB	Documento de texto	4/11/2007 13:44
marcio@nytimes[1]	1 KB	Documento de texto	7/3/2009 23:45
marcio@predicta.com[1]	1 KB	Documento de texto	5/3/2009 20:35
marcio@rad.msn[2]	1 KB	Documento de texto	4/11/2007 13:44
marcio@statcounter[1]	1 KB	Documento de texto	7/3/2009 23:46
marcio@terra.atmo.predicta.com[1]	1 KB	Documento de texto	5/3/2009 20:35
marcio@terra.com[1]	1 KB	Documento de texto	5/3/2009 20:35
marcio@www.terra.com[1]	1 KB	Documento de texto	5/3/2009 20:35
marcio@yourminis[1]	1 KB	Documento de texto	7/3/2009 23:55

Figura 34 – Diretório dos Cookies

Dentro dos *Cookies* há um texto, como no exemplo a seguir, onde foi clicado em marcio@google.com, então aparecerá o seguinte texto:

PREF

ID=bf4e47389559c905:TM=1194194728:LM=1236480163:S=fMWjG4-kjaGSumz-

google.com.br/

1536

2141967232

30137658

2455912128

29990807

*

NID

20=F1ROLQZzP6O-SvJ4comH8Wl0VIXZ_nM7iWkGg7s_DGhMpqlc5qy98yL7GemTyO28OHDJUE2rOpXqLtJ9UwXBFa51uS7v7rbH-f26Qoa6Jo1AtgtOG-KtOK56b7KEy-o8

google.com.br/

9728
18317184
30027621
3013252128
29990807
*

Que estes detalhes não serão estudados neste trabalho.

4.2.5 Registro do Windows

O Registro é onde o Windows guarda seus “segredos”: praticamente tudo que você faz no Sistema Operacional tem um valor no registro. Por exemplo, suas configurações de pasta, do Internet Explorer e do Outlook Express. O registro é tipo um “banco de dados” onde o Windows guarda várias informações sobre o sistema e seus aplicativos.

4.2.6 Correio Eletrônico do MS-Outlook

Uma das formas de obter provas é pelas trocas de mensagens eletrônicas como MSN e correio eletrônicos, então uma dessas formas é encontrar os arquivos que guarda a Caixa de Entrada, Itens Enviados e Rascunhos.

Se tiver algum problema com um arquivo de senha, usar o utilitário John The Ripper, que descobrirá a senha.

4.3 Análise

É a etapa em que o perito irá analisar e filtrar as informações usando os seguintes passos

1. Interpretação dos vestígios encontrados

2. Estabelecer uma relação entre os vestígios encontrados com o que procura
3. Tentar responder se houve invasão ao sistema ou foi utilizado processos dentro da máquina auditada
4. Decisão para o próximo passo da investigação se haverá necessidade de uma investigação mais profunda ou não.

É onde separaremos o que é importante ou não das evidências coletadas. Serão analisados minuciosamente:

4.3.1 Cookies

Os *Cookies* são as grandes pistas por onde o usuário passou. É simples de apagar no Windows, pois é só ir na pasta onde ficam estes arquivos e excluí-la. Porém, para o perfil de um pedófilo, ele pode não conhecer este tipo de arquivo e assim facilitar o trabalho do perito. Geralmente esta pasta fica em "*Documents and Settings*", a pasta do usuário e dentro desta pasta, está o diretório "*Cookies"*, porém este está oculto.

4.3.2 Arquivos de email

Os usuários de Windows, geralmente tem seu email cadastrado no aplicativo MS-Outlook. Este programa tem alguns arquivos padrões, como "Caixa de Entrada", "Lixeira", "Caixa de Saída", todos estes com extensões DBX. Então, será usado o aplicativo do FDTK, o Eindeutig. Porque se abrir usando o próprio Windows, poderá modificar o arquivo e assim inutilizando a prova.

4.3.3 Histórico do MSN

Um dos programas mais populares de conversa na Internet, é onde também os pedófilos mais atacam, pois o MSN hoje é como se fosse o telefone fixo de antigamente, ficou algo íntimo. Aí, o perito tem que encontrar qual pasta ele salvou seu histórico. Algo não impossível. Para uma grande empresa, seria necessário

colocar um *sniffer* de Mensagens instantâneas, se o servidor for Linux, uma boa recomendação é o IMSniffer.

4.4 Apresentação

Finalizando a apresentação com um laudo pericial, porém não faz parte deste trabalho e portanto não será detalhado.

4.5 Distribuição LiveCD do Helix

No primeiro momento vamos coletar as informações do computador auditado, neste caso, uma máquina virtual do Microsoft Windows XP® SP1, como mostrado na Figura 35. Nesta figura, identifica qual o Sistema Operacional, a quem pertence, a sua organização, o usuário que está neste momento de acesso, seu IP e quais são os dispositivos de armazenamento que a máquina possui.

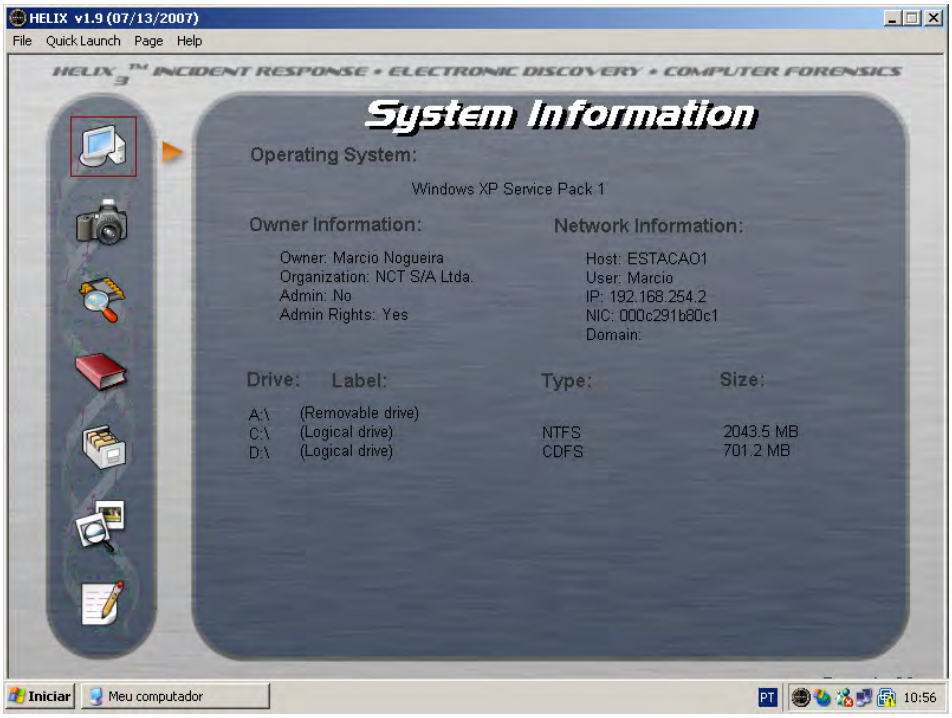


Figura 35 – Informação do Sistema no Helix

4.5.1 Coleta

Após armazenar as informações do sistema, então será coletado os dados da memória física, por exemplo a RAM e os dados dos discos rígidos, para garantir a integridades dos dados posteriormente, pois com estas informações copiadas, ou seja, criada sua imagem, haverá uma melhor análise das provas obtidas. Após a coleta das memórias, será salva em lugar seguro, por exemplo, um pendrive, e os arquivos com extensões DD, visto na Figura 36.

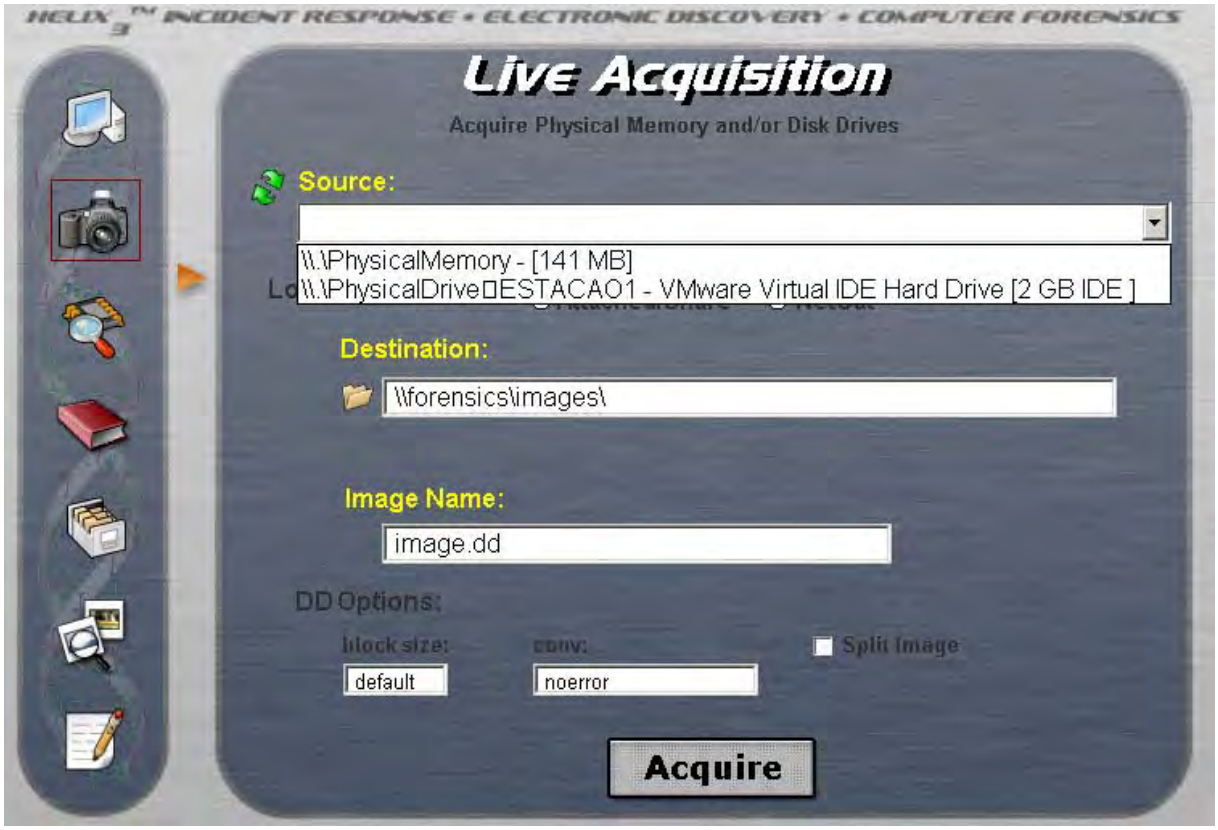


Figura 36 – Criando Imagem da Memória RAM e Disco Rígido

Porém, para tirar uma boa imagem do disco, aconselha-se usar o FTK Imager.

4.5.2 Exame

No exame dos dados, é a etapa que tudo que foi coletado será estudado minuciosamente para que estas informações sejam filtradas e assim obter uma

análise mais detalhada. Portanto, todas as ferramentas que serão usadas, terão uma grande importância para um bom estudo.

Estes utilitários estão contidos conforme a Figura 37, e que foi mostrado no Capitulo 3. Porem, aqui será a prática e provando que a teoria está correta.

Figura 37 – Exame dos Dados

Iniciando este exame, será procurado no primeiro ícone do PST Password Viewer, se há senhas gravadas no sistema ou não, neste caso, mostrado na Figura 38, não há senha gravadas no Windows.

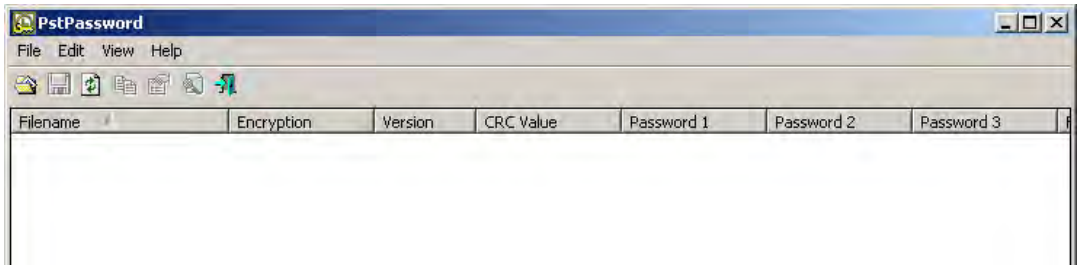


Figura 38 – Programa PSTPassword sem encontrar senha

E acontecendo o mesmo caso para o aplicativo Messenger Password, porém para o programa IEHistory Viewer, há muita coisa para se examinar, como será visto na Figura 39 a seguir:

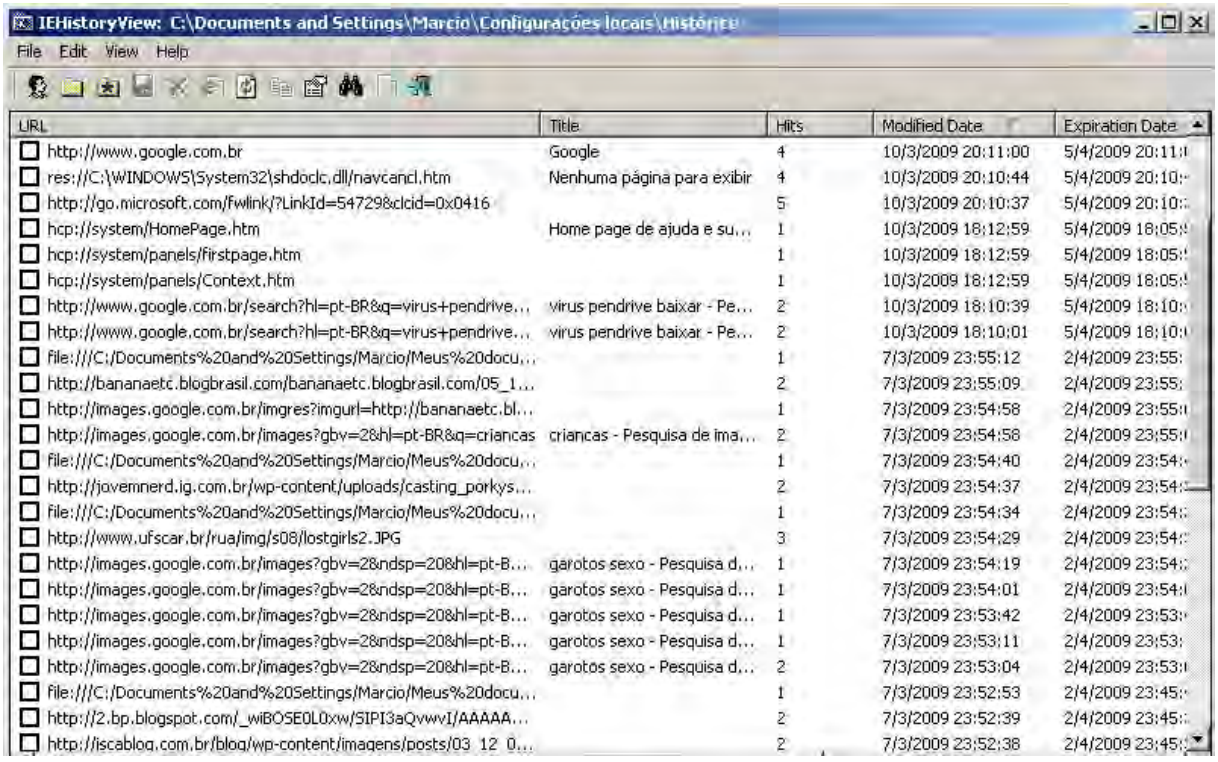


Figura 39 – IEHistory View da Máquina Virutal

Como mostrado na Figura 35 anterior, há arquivos a serem analisados, como:

- ✓ Vírus de Pendrive
- ✓ Imagens do Google
- ✓ Crianças
- ✓ Garotos sexo

Estes são alguns detalhes da parte do exame em que o perito irá ter mais cuidado com esses tópicos, que serão detalhados na etapa da análise.

Outro aplicativo é o USBDeview que mostra todos os dispositivos de USB e quais e como foram utilizados, visto na Figura 40.

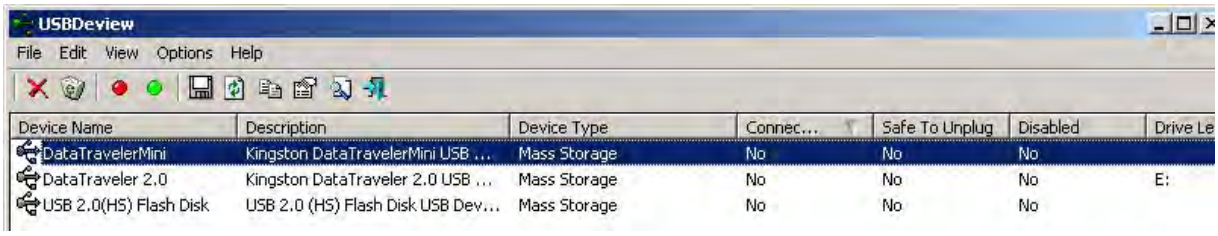


Figura 40 – USBDeview

Com todos os arquivos do sistema examinados, então o perito irá agora para a parte da análise.

4.5.3 Análise

A etapa final deste trabalho e do perito, o qual ele analisará mais detalhes do tópico anterior para encontrar pistas que levem o suspeito a ser inocente ou culpado.

A princípio e de acordo com o conjunto de aplicativos do Helix, é sabido que o usuário Márcio estava conectado nesta máquina, visto com mais detalhes na Figura 41.

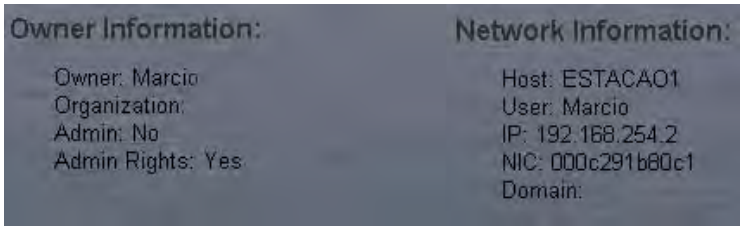


Figura 41 – Informação do Sistema

Porém, em alguns aplicativos não foi retornado nada, então não há como analisar, como os programas PST Password Viewer e Messenger Password, pois nesta máquina virtual não foi gravado nenhuma senha.

No entanto, pelo programa IEHistoryView, há muito para se analisar, por exemplo na Figura 42:

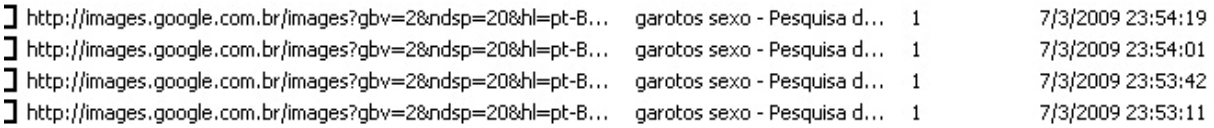


Figura 42 – Exemplo Retirado do IEHistoryView

Neste exemplo, é mostrado que o suspeito procurou fotos de “garotos” e “sexo” no Google Imagens no dia 7 de Março de 2009 às 23 horas e 53 minutos. Isto já é uma grande prova, pois se ele tiver pelo menos arquivos com conteúdo de

pedofilia, pela nova lei, sancionada pelo Presidente do Brasil, Lula, no final de novembro de 2008, já é considerado crime.

Neste caso, o perito terá que procurar imagens com conteúdo pornográfico, mais exatamente com indícios de pedofilia.

Para procurar fotos, então usa-se o aplicativo Scan for Pictures, mostrado na Figura 43.

Figura 43 – Scan for Pictures

Encontrando, apenas incluir no laudo técnico e levar ao júri.

CONCLUSÃO

Este trabalho teve a proposta de padronizar um procedimento de auditoria em um computador com o Sistema Operacional Microsoft Windows XP que está sob suspeita de ter arquivos com conteúdo de pornografia infantil, que aqui no Brasil é crime de acordo com a Lei 11.829 de 25 de Novembro de 2008.

Não é um trabalho fácil, pois sem um padrão toda a investigação poderá ser perdida e aqui no Brasil principalmente, pois este hábitos de se lidar com provas eletrônicas é novidade para todos, como suas leis.

Os programas usados foram todos de código livre e aberto, pois os pagos só poderão ter se comprar a “caixa completa” e não vende pela Internet para pessoas físicas. Portanto, foi usado a distribuição Linux chamada, FDTK-UbuntuBR, o Helix e os utilitários da Sysinternals, este último para provar que o computador apreendido não tinha nenhum *Malware* que pudesse inocentar o suspeito.

Para a padronização teve um preparo cuidadoso em cada etapa da investigação.

1. Coleta
2. Exame
3. Análise

Sendo omitida a 4ª etapa que é o Laudo Pericial e apenas citado durante o trabalho.

Então, para cada perito, mesmo usando o FTDK ou o Helix, há uma necessidade de se iniciar fazendo uma copia da imagem de cada disco rígido e calculando o seu *hash*, se possível com dois aplicativos diferentes e com uma testemunha ao lado do perito para comprovar a veracidade das provas, assim como os *hashes* dos arquivos, depois disso trabalhar apenas nas imagens e nunca nas provas originais.

Finalizando, foi mostrada as leis aplicadas no Brasil em relação a pornografia infantil.

Sugestões de Trabalhos Futuros

1. Provar que o computador auditado e suspeito por pornografia infantil, não foi o dono da máquina quem colocou e sim um *Malware* que injetou o conteúdo ilícito
2. Procedimento de como encontrar um pedófilo pela Internet
3. Padrões para escrever um laudo técnico

REFERÊNCIAS

ACCESSDATA Corp. **Access Data Forensics Tool Kit 2.0**. Jan. 2009. Disponível em: <http://www.accessdata.com/downloads/media/ftkug.pdf>. Acesso em: 12/03/2009

ARAS, W. **Crimes de informática: Uma nova criminalidade**. Jus Navigand, Jun. 2001. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=2250>. Acesso em: 01/02/2009

ARGOLO, Frederico Henrique Böhm. **Análise Forense em Sistemas GNU/Linux**. UFRJ, Rio de Janeiro, 2005.

BRASIL. **Novo Código Civil**. **Lei Nº 10.406 de 10 de Janeiro de 2002** Presidência da República. Disponível em: <http://www.planalto.gov.br/CCIVIL/leis/2002/L10406.htm>. Acesso em 27/04/2009

_____. **Código de Processo Penal**. **DECRETO-LEI Nº 3.689, DE 3 DE OUTUBRO DE 1941.** Presidência da República. Disponível em: <http://www.planalto.gov.br/CCIVIL/Decreto-Lei/Del3689.htm>. Acesso em 20/01/2009

_____. **Constituição Da República Federativa do Brasil de 1988.** Presidência da República. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituiçao.htm >. Acesso em 27/05/2009

_____. LEI Nº 11.829, DE 25 DE NOVEMBRO DE 2008. **Altera a Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet.** Presidência da República. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm>. Acesso em 14/03/2009

_____. **Estatuto da Criança e do Adolescente e dá outras providências. Lei Nº 8.069, de 13 de Julho de 1990.** Presidente da República. Disponível em: <http://www.planalto.gov.br/ccivil/LEIS/L8069.htm>. Acesso em 20/01/2009

_____. **Altera a Lei nº 8.069, de 13 de julho de 1990** Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11829.htm>. Acesso em 20/01/2009

CASTRO, Carla Rodrigues Araújo de. Impunidade na Internet . **Jus Navigandi**, Teresina, ano 6, n. 52, nov. 2001. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=2327>. Acesso em: 28 fev. 2009.

CONSULTOR JURÍDICO. **Crimes Virtuais.** Disponível em: <http://www.conjur.com.br/2002-mar-27/policia_dificuldades_chegar_aos_pedofilos>. Acesso em 27 de Abril de 2009.

CROCE, Delton**. Manual de Medicina Legal.** 4ª Ediçao, Brasil. Ed. Saraiva 2004.

FAHEY, Gleason. FAHEY, Drew. **Helix 1.7 for begginners.** Seul – Corea, Março de 2006.

FDTK-UbuntuBr. ***Forense Digital Toolkit*.** Disponível em: < http://www.fdtk.com.br>. Acesso em 27 de Abril de 2009.

FREITAS, Andrey Rodrigues de. **Perícia Forense Aplicada à Informática:** 1ª Edição, Brasil. Ed Brasport, 2006

GUIMARÃES et al. **Forense Computacional: Aspectos Legais e Padronização.** Campinas – SP, 2002.

HELIX.**Distribuição Live CD**. Disponível em: < http://www.e-fense.com>. Acesso em 13 de Marco de 2009.

John The Ripper. ***Password Cracker.*** Disponível em: <http://www.openwall.com/john>. Acesso em 27 de Abril de 2009.

LIMA, Erica Rocha. **Levantamento do histórico na cena do crime, fator relevante na análise de evidências em crimes eletrônicos.** In: I Conferência Internacional de Perícias em Crimes Cibernéticos, 2004. Brasília – DF. Anais da 1ª Conferência Internacional de Perícias em Crimes Cibernéticos, Brasília – DF, Editora Departamento de Polícia Federal, 2004. p.217 até p.221

Microsoft TechNet. **Guia básico de investigação computacional para Windows: Visão geral.** Jan. 2007. Disponível em: <http://www.microsoft.com/brasil/technet/prodtechnol/security/guidance/disasterrecovery/computer_investigation/9545b739-1ef9-415f-a1c4-3ca29f0ce5af.mspx>. Acesso em 10/01/2009

NOGUEIRA, Márcio Luiz Machado. **MREFCON Modelo de Rastreamento de Evidências Forenses Conta Crimes Online – Proposta Acadêmica para integração e agilização de investigações entre a Polícia, Justiça e Provedores de Internet.** Recife, 2007

NUBLAT, Johanna IGLESIAS, Simone. **PF traça perfil de pedófilo na Internet.** Folha de São Paulo, Brasília. Maio de 2008. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u398251.shtml>. Acesso em 28/04/2009.

PERRIN, Stephanie. **Desafios de Palavras***: Enfoques Multiculturais sobre as Sociedades da Informação*. Editora C & F Éditions. França, 2005.

PIRES, Paulo S. da Motta. **FORENSE COMPUTACIONAL: UMA PROPOSTA DE ENSINO.** Disponível em: <http://www.dca.ufrn.br/~pmotta/trabalhos.html>. Acesso em 29/04/2009.

PONTES, Gabriela. **Segurança na Internet deve ser garantida.** Disponível em: <http://www.comunicacao.pro.br/setepontos/13/provedores.htm>. Acesso em 20/01/2009

REIS, Fábio André Silva. **O enfrentamento da pornografia infantil na Internet: O papel dos canis de denúncia.** In: I Conferência Internacional de Perícias em Crimes Cibernéticos, 2004. Brasília – DF. Anais da 1ª Conferência Internacional de Perícias em Crimes Cibernéticos, Brasília – DF, Editora Departamento de Polícia Federal, 2004. p.23 até p.27

REIS, Marcelo Abdalla dos. **Forense Computacional e sua aplicação em segurança imunológica.** Campinas - SP, 2003.

REIS, Marcelo Abdalla dos; GEUS, Paulo Lício de. **Análise Forense de Intrusões em Sistemas Computacionais: Técnicas, Procedimentos e Ferramentas.** Campinas – SP, 2002.

REIS, Marcelo Abdalla dos; GEUS, Paulo Lício de. **Forense Computacional: Procedimentos e Padrões.** Campinas – SP, 2001

RODRIGUES, Alan. **Pedofilia. Pesquisa inédita alerta:** o Brasil lidera o ranking mundial de pornografia infantil pela internet. Seu filho está seguro? Revista Isto é. Disponível em <http://www.terra.com.br/istoe/1898/comportamento/1898_pedofilia.htm> . Acesso em 10/04/2009.

RODRIGUES, Jorison da Silva. **Pedofilia: Pornografia envolvendo a criança.** Revista Perícia Federal: Publicação da Associação dos Peritos Criminais Federais, Ano I, Nº3. Brasília, DF, 1999.

RODRIGUES, T. **Resposta a Incidentes e Forense Computacional.** Jun. 2007. Disponível em: <http://forcomp.blogspot.com/2008/02/processo-litrgico-preservao-de.html>. Acesso em 20/01/2009

SaferNet Brasil. Disponível em: <http://www.safernet.org.br>. Acesso em 28/02/2009

TREVENZOLI, Ana Cristina. **Perícia forense computacional:** ataques, identificação da autoria, leis e medidas preventivas. Sorocaba, 2006.

VENEMA, Wietse; FARMER, Dan. **Perícia Forense Computacional - Como Investigar e Esclarecer Ocorrências no Mundo Cibernético:** Prentice Hall (pearson), 2007.

_____. **TCT – The Coroner's Toolkit.** Disponível em:<http://www.porcupine.org/forensics/tct.html>. Acesso em 29 de Março de 2009.

VIOTTI, Alberto Luiz Alves. **Possibilidades de uso de software livre como ferramentas de análise em investigações digitais.** Lavras – MG, 2005.