

**UNIVERSIDADE DE BRASÍLIA  
FACULDADE DE TECNOLOGIA  
DEPARTAMENTO DE ENGENHARIA ELÉTRICA**

**METODOLOGIA E FERRAMENTA DE COLETA DE DADOS  
VOLÁTEIS EM SISTEMAS WINDOWS**

**PEDRO AULER**

**ORIENTADOR: FLÁVIO ELIAS GOMES DE DEUS**

**DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA  
ÁREA DE CONCENTRAÇÃO INFORMÁTICA FORENSE E  
SEGURANÇA DA INFORMAÇÃO**

**PUBLICAÇÃO: PPGENE.DM – 86 A/11**

**BRASÍLIA / DF: DEZEMBRO/2011**

**UNIVERSIDADE DE BRASÍLIA  
FACULDADE DE TECNOLOGIA  
DEPARTAMENTO DE ENGENHARIA ELÉTRICA**

**METODOLOGIA E FERRAMENTA DE COLETA DE  
DADOS VOLÁTEIS EM SISTEMAS WINDOWS**

**PEDRO AULER**

**DISSERTAÇÃO DE MESTRADO PROFISSIONALIZANTE  
SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA  
DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE  
BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA  
A OBTENÇÃO DO GRAU DE MESTRE.**

**APROVADA POR:**

---

**FLÁVIO ELIAS GOMES DE DEUS, Dr., ENE/UNB  
(ORIENTADOR)**

---

**WILLIAM FERREIRA GIOZZA, Dr., ENE/UNB  
(EXAMINADOR INTERNO)**

---

**HÉLVIO PEREIRA PEIXOTO, Dr., DITEC/DPF  
(EXAMINADOR EXTERNO)**

**Brasília, 16 de dezembro de 2011.**

## FICHA CATALOGRÁFICA

AULER, PEDRO

Metodologia e Ferramenta de coleta de Dados Voláteis em Sistemas Windows [Distrito Federal] 2011. xii, 95p., 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2011).

Dissertação de Mestrado – Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica.

1. Informática forense 2. Coleta 3. Dados  
4. Voláteis 5. Windows

I. ENE/FT/UnB. II. Título (Série)

## REFERÊNCIA BIBLIOGRÁFICA

AULER, P. (2011). Metodologia e Ferramenta de coleta de Dados Voláteis em Sistemas Windows. Dissertação de Mestrado, Publicação PPGENE.DM – 86 A/11, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 95p.

## CESSÃO DE DIREITOS

NOME DO AUTOR: PEDRO AULER

TÍTULO DA DISSERTAÇÃO: Metodologia e Ferramenta de coleta de Dados Voláteis em Sistemas Windows.

GRAU/ANO: Mestre/2011.

É concedida à Universidade de Brasília permissão para reproduzir cópias desta Dissertação de Mestrado e para emprestar ou vender tais cópias somente para propósitos acadêmicos e científicos. Do mesmo modo, a Universidade de Brasília tem permissão para divulgar este documento em biblioteca virtual, em formato que permita o acesso via redes de comunicação e a reprodução de cópias, desde que protegida a integridade do conteúdo dessas cópias e proibido o acesso a partes isoladas desse conteúdo. O autor reserva outros direitos de publicação e nenhuma parte deste documento pode ser reproduzida sem a autorização por escrito do autor.

---

Pedro Auler  
SQSW 304, Bloco G, Ap. 204  
CEP 70673-407 - Brasília – DF - Brasil

Dedico esta dissertação à minha esposa,  
aos meus filhos,  
e aos meus pais.

## **AGRADECIMENTOS**

Ao meu orientador Prof. Dr. Flávio Elias Gomes de Deus, pelo apoio e incentivo, essenciais para o desenvolvimento deste trabalho e para o meu amadurecimento como pesquisador.

Ao Prof. Laerte Peotta de Melo, pelo imprescindível apoio, incentivo e amizade prestados durante a fase de elaboração da Dissertação de Mestrado.

Ao Perito Criminal Federal, Marcelo Caldeira Ruback, colega de trabalho e de mestrado, pelo apoio durante a fase presencial do Curso de Mestrado.

Ao Perito Criminal Federal Hέλvio Pereira Peixoto e aos peritos criminais federais lotados no Serviço de Perícias em Informática da Polícia Federal, pelo incentivo.

Aos colegas do Curso de Mestrado, pela amizade.

A todos, os meus sinceros agradecimentos.

O presente trabalho foi realizado com o apoio do Departamento Polícia Federal, com recursos do Programa Nacional de Segurança Pública com Cidadania – PRONASCI, do Ministério da Justiça.

## **RESUMO**

### **METODOLOGIA E FERRAMENTA DE COLETA DE DADOS VOLÁTEIS EM SISTEMAS WINDOWS**

**Autor: Pedro Auler**

**Orientador: Flávio Elias Gomes de Deus**

**Programa de Pós-graduação em Engenharia Elétrica**

**Brasília, dezembro de 2011**

Este trabalho tem o objetivo de apresentar uma metodologia de coleta de dados voláteis em sistemas operacionais baseados em Windows. Para tal, elaborou-se uma ferramenta (CADAV – Coleta Automatizada de Dados Voláteis) e uma proposta de modelo de atuação do perito criminal durante o procedimento de busca e apreensão de equipamentos de informática. O CADAV é executado a partir de um *flash drive* inserido no computador a ser apreendido, sendo o resultado da coleta copiado para uma pasta criada durante o processo. Devido ao crescente uso de métodos criptográficos e de máquinas virtuais, a ferramenta propõe alguns testes para diagnosticar esta situação. Para evitar o risco de perda de informações, sistemas que utilizam criptografia ou virtualização de sistema devem ter seu conteúdo copiado para uma mídia externa, antes do desligamento do computador. Além disso, é apresentada uma metodologia para o procedimento de busca e apreensão, levando em conta a garantia da integridade dos dados coletados através do procedimento chamado Cadeia de Custódia. Basicamente, a Cadeia de Custódia trata dos cuidados que devem ser tomados para garantir a integridade e a idoneidade das evidências coletadas. Todos os passos realizados, desde a chegada ao local de busca e apreensão, passando pela análise da máquina suspeita, até o encaminhamento de todo o material apreendido, deve ser cuidadosamente documentado. A metodologia proposta é necessária porque, caso não sejam utilizadas técnicas adequadas de coleta e documentação, há grande risco de perda de evidências ou de falta de credibilidade das provas coletadas, em um futuro processo judicial.

## **ABSTRACT**

### **METHODOLOGY AND TOOL FOR VOLATILE DATA ACQUISITION ON WINDOWS-BASED SYSTEMS**

**Author: Pedro Auler**

**Supervisor: Flávio Elias Gomes de Deus**

**Programa de Pós-graduação em Engenharia Elétrica**

**Brasília, December of 2011**

This paper presents a methodology for volatile data acquisition on Windows-based operating systems. For that, a tool (CADAV - Automated Volatile Data Acquisition) has been developed. Furthermore, this work presents a model on how the forensic expert should behave during a digital search and seizure. CADAV runs from a flash drive inserted in the suspect's computer and the result is copied to a folder created during the process. Due to the increasing use of cryptography and virtual machines, the tool offers some tests to detect these situations. To avoid the risk of information loss, systems that are running encryption or virtualization programs must have their contents copied to an external drive before the computer is shut down. In addition, considering the collected data integrity during the procedure called Chain of Custody, a search and seizure procedure methodology is presented. Basically, Chain of Custody deals with the issues that must be taken to ensure collected evidence integrity and reliability. All the steps taken since the arrival at the search and seizure location should be carefully documented, including the suspect's computer analysis and the seized material hand over. If inappropriate acquisition and documentation techniques are used, there is a great risk of evidence loss and lack of credibility in a future lawsuit. That's why the proposed methodology is necessary.

# SUMÁRIO

<b>1. INTRODUÇÃO .....</b>	<b>1</b>
<b>1.1. OBJETIVOS .....</b>	<b>4</b>
<b>1.1.1. Objetivos específicos:.....</b>	<b>5</b>
<b>1.2. JUSTIFICATIVA .....</b>	<b>5</b>
<b>1.3. ORGANIZAÇÃO .....</b>	<b>7</b>
<b>2. REVISÃO BIBLIOGRÁFICA .....</b>	<b>8</b>
<b>2.1. PERÍCIA COMPUTACIONAL E EVIDÊNCIA DIGITAL .....</b>	<b>8</b>
<b>2.2. PRINCIPAIS COMPONENTES DE UM COMPUTADOR.....</b>	<b>8</b>
<b>2.2.1. Processadores.....</b>	<b>9</b>
<b>2.2.2. Registradores .....</b>	<b>9</b>
<b>2.2.3. Memória Cache.....</b>	<b>10</b>
<b>2.2.4. Memória Principal (RAM).....</b>	<b>10</b>
<b>2.2.5. Memória Secundária .....</b>	<b>11</b>
<b>2.2.6. Dispositivos de Entrada e Saída.....</b>	<b>11</b>
<b>2.3. PRINCÍPIOS BÁSICOS DE SEGURANÇA.....</b>	<b>11</b>
<b>2.4. FUNÇÕES DE HASH .....</b>	<b>12</b>
<b>2.5. MALWARE .....</b>	<b>13</b>
<b>2.6. ROOTKIT .....</b>	<b>13</b>
<b>2.7. CADEIA DE CUSTÓDIA.....</b>	<b>13</b>
<b>2.8. PRINCÍPIOS FUNDAMENTAIS DA COLETA DE DADOS VOLÁTEIS .....</b>	<b>16</b>
<b>2.9. COLETA DE DADOS VOLÁTEIS EM SISTEMAS INFORMATIZADOS.....</b>	<b>19</b>
<b>3. COLETA DE DADOS.....</b>	<b>24</b>
<b>3.1. FERRAMENTAS X COMANDOS DE SISTEMA .....</b>	<b>24</b>
<b>3.2. FTK IMAGER (ACCESS DATA).....</b>	<b>25</b>
<b>3.3. FERRAMENTAS INTEGRADAS.....</b>	<b>26</b>
<b>3.3.1. Incident Response Collection Report (IRCR).....</b>	<b>26</b>
<b>3.3.2. First Responders Evidence Disk (FRED).....</b>	<b>27</b>
<b>3.3.3. Nigilant32.....</b>	<b>27</b>
<b>3.3.4. Windows Forensics Toolchest (WFT).....</b>	<b>27</b>
<b>3.3.5. Computer Online Forensic Evidence Extractor (COFEE).....</b>	<b>29</b>
<b>3.4. COMPARAÇÃO DAS FERRAMENTAS INTEGRADAS.....</b>	<b>30</b>



3.5.	LIMITAÇÕES DAS FERRAMENTAS INTEGRADAS EXISTENTES .....	31
4.	METODOLOGIA PROPOSTA .....	32
4.1.	PROCEDIMENTOS DA BUSCA E APREENSÃO .....	32
4.1.1.	<i>Fase 1</i> .....	34
4.1.2.	<i>Fase 2</i> .....	36
4.1.3.	<i>Fase 3</i> .....	36
4.1.4.	<i>Fase 4</i> .....	37
4.1.5.	<i>Procedimentos pós-coleta</i> .....	37
4.2.	PROTÓTIPO DA FERRAMENTA .....	38
4.2.1.	<i>Detalhamento do arquivo batch “ColetaDados.bat”</i> .....	41
4.3.	ESTUDO DE CASO .....	46
4.3.1.	<i>Cenário 1</i> .....	48
4.3.2.	<i>Cenário 2</i> .....	51
4.3.3.	<i>Cenário 3</i> .....	55
4.3.1.	<i>Cenário 4</i> .....	56
4.3.2.	<i>Cenário 5</i> .....	59
4.3.3.	<i>Cenário 6</i> .....	61
4.4.	ANÁLISE DOS TESTES .....	64
5.	CONCLUSÃO .....	66
	REFERÊNCIAS BIBLIOGRÁFICAS .....	68
	ANEXO A – FERRAMENTAS E COMANDOS DE SISTEMA .....	74
	ANEXO B – CHECKLIST – BUSCA E APREENSÃO .....	83
	ANEXO C – BUSCA E APREENSÃO DE MATERIAL DE INFORMÁTICA .....	85
	ANEXO D - CONTEÚDO DO ARQUIVO “COLETADADOS.BAT” .....	87
	ANEXO E – CONTEÚDO DO ARQUIVO “RECALCULA HASHES.BAT” .....	92
	ANEXO F – CONTEÚDO DO ARQUIVO “LEIAME.TXT” .....	93

## LISTA DE SÍMBOLOS E ABREVIACÕES

<i>Boot</i>	Processo de inicialização do computador
<i>Buffer</i>	Região de memória temporária para escrita e leitura de dados
COFEE	<i>Computer Online Forensic Evidence Extractor</i>
CPU	<i>Central Processing Unit</i>
DLL	<i>Dynamic-link library</i>
GB	<i>Gigabyte = 1024 MB</i>
EULA	<i>End-user licence agreement</i>
FRED	<i>First Responders Evidence Disk</i>
GPL	<i>General Public Licence</i>
IRCR	<i>Incident Response Collection Report</i>
JPEG	<i>Joint Photographic Experts Group</i>
KB	<i>Kilobyte = 1024 bytes (1 byte = 8 bits)</i>
MB	<i>Megabyte = 1024 KB</i>
MD5	<i>Message Digest 5</i>
NW3C	<i>National White Collar Crime Center</i>
<i>Popup</i>	Pequena janela que se abre automaticamente na tela
RAM	<i>Random Access Memory</i>
RFC	<i>Request For Comments</i>
SHA	<i>Secure Hash Algorithm</i>
UC	Unidade de Controle
ULA	Unidade Lógica e Aritmética
WFT	<i>Windows Forensics Toolchest</i>

## LISTA DE TABELAS

Tabela 1.1: Evolução dos sistemas operacionais mais utilizados.....	3
Tabela 3.1: Exemplos de ferramentas da Nirsoft. ....	24
Tabela 3.2: Exemplos de ferramentas da Sysinternals. ....	25
Tabela 3.3: Recursos do Windows Forensic Toolchest.....	28
Tabela 3.4: Comparação das ferramentas COFEE e WFT (AULER, 2009). ....	30
Tabela 4.1: Comparação entre soluções de captura em sistemas Windows XP.....	43
Tabela 4.2: Cenários de coleta utilizados. ....	46
Tabela 4.3: Descrição da máquina utilizada no Cenário 1. ....	48
Tabela 4.4: Descrição da máquina utilizada no Cenário 2. ....	51
Tabela 4.5: Descrição da máquina utilizada no Cenário 3. ....	55
Tabela 4.6: Descrição da máquina utilizada no Cenário 4. ....	56
Tabela 4.7: Descrição da máquina utilizada no Cenário 5. ....	59
Tabela 4.8: Descrição da máquina utilizada no Cenário 6. ....	62

## LISTA DE FIGURAS

Figura 1.1: Sistemas operacionais mais utilizados. ....	3
Figura 1.2: Comparação de uso de Windows XP, 7, e outros. ....	3
Figura 1.3: Projeção do uso dos sistemas Windows XP e 7. ....	4
Figura 2.1: Interação entre os subsistemas básicos do computador. ....	9
Figura 2.2: Fases da perícia digital. ....	19
Figura 4.1: Etapas do procedimento de busca e apreensão. ....	33
Figura 4.2: Metodologia da apreensão de computadores. ....	35
Figura 4.3: Conteúdo do diretório raiz do Protótipo. ....	39
Figura 4.4: Conteúdo da pasta "Ferramentas". ....	40
Figura 4.5: Conteúdo do diretório raiz do <i>flash drive</i> , após a coleta. ....	40
Figura 4.6: Aviso de possível presença de criptografia no sistema. ....	48
Figura 4.7: Conteúdo do arquivo "Processos.txt" ....	49
Figura 4.8: Arquivos coletados - Cenário 1. ....	50
Figura 4.9: Conteúdo do arquivo "DetectaCripto.txt" ....	50
Figura 4.10: Arquivos coletados - cenário 2. ....	51
Figura 4.11: Conteúdo parcial do arquivo Resultados.txt - parte 1. ....	52
Figura 4.12: Conteúdo parcial do arquivo Resultados.txt - parte 2. ....	53
Figura 4.13: Conteúdo parcial do arquivo Resultados.txt - parte 3. ....	53
Figura 4.14: Ferramentas identificadas como ameaças pelo antivírus. ....	54
Figura 4.15: Arquivos coletados - Cenário 3. ....	55
Figura 4.16: Mensagem de alerta para máquina virtual - Cenário 3. ....	56
Figura 4.17: Conteúdo do arquivo "Processos.txt" – Cenário 3. ....	57
Figura 4.18: Arquivos coletados - Cenário 4. ....	58
Figura 4.19: Ferramentas identificadas como ameaças pelo antivírus. ....	58
Figura 4.20: Arquivos coletados - Cenário 5. ....	60
Figura 4.21: Conteúdo do arquivo "DetectaWMware.txt" ....	60
Figura 4.22: Conteúdo do arquivo "Processos.txt" – Cenário 5. ....	61
Figura 4.23: Arquivos coletados – Cenário 6. ....	62
Figura 4.24: Conteúdo parcial do arquivo "DispUSB.txt". ....	63
Figura 4.25: Valor do <i>hash</i> a ser anotado. ....	64
Figura 4.26: Conteúdo do arquivo "Hash_do_Hashes.txt" ....	64

# 1. INTRODUÇÃO

Os procedimentos de busca e apreensão de materiais de informática vêm sofrendo drásticas mudanças nos últimos tempos. A abordagem tradicional, que consiste em retirar o cabo de energia da máquina suspeita, com a apreensão de todo o material para análise posterior, em laboratório, pode trazer grave comprometimento da investigação, levando à perda irreversível de dados. Com o uso cada vez mais frequente de criptografia de sistema ou de volumes e de armazenamento remoto de dados, o desligamento precoce da máquina examinada pode causar a perda imediata e irreversível das informações nela contidas (SUTHERLAND, *et al.*, 2010). As técnicas utilizadas em procedimentos de busca e apreensão estão cada vez mais elaboradas e é necessário que o perito da área de informática acompanhe esta mudança de paradigmas para não comprometer a coleta de dados. A captura e a análise de dados voláteis vêm se tornando uma das áreas mais importantes e desafiadoras da investigação forense digital.

As ferramentas de captura de dados voláteis devem ser capazes de extrair e preservar de forma sistemática e automática, os dados de um sistema de informática ligado, produzindo o mínimo de alterações possíveis no sistema. Devem ainda ser capazes de auxiliar na interpretação e organização das informações coletadas, de forma a levar a conclusões lógicas e de fácil demonstração, para o caso de serem apresentadas em Juízo.

Na abordagem tradicional, onde o material é apreendido para exame posterior, a análise é realizada sobre uma cópia forense (*bit a bit*) do material original, utilizando técnicas de proteção contra gravação. São empreendidos os máximos esforços para não danificar o material original, para o caso de serem necessários novos exames no futuro. Além disso, não deve haver nenhuma interferência do perito no material apreendido, para não haver futuros questionamentos quanto a eventuais evidências terem sido acrescentadas por ele. Deve haver a preocupação de não contaminar o material apreendido com alterações produzidas pelas ferramentas periciais. Entretanto, há casos em que o custo/benefício autoriza a manipulação do sistema ligado, sabendo-se de antemão que serão produzidas pequenas alterações no mesmo. Na disputa entre a não introdução de pequenas alterações no sistema examinado pelo perito, e a eventual perda de informações relevantes que poderiam ter sido coletadas, este último aspecto tem se mostrado mais importante.

Para a perda de informações voláteis que se encontram em sistemas ligados, dados

contidos em sistemas ou volumes criptografados, ou dados armazenados remotamente através da rede, não há solução fácil. Uma vez perdidos estes dados, sua recuperação pode se tornar impossível. A maior parte das informações contidas na memória volátil, caso não estejam salvas em disco, estarão definitivamente perdidas. Para a recuperação de dados contidos em sistemas ou volumes criptografados, depender-se-á da recuperação de senhas ou chaves de criptografia. Por outro lado, para as pequenas alterações introduzidas no sistema pelo perito com suas ferramentas de coleta, existem maneiras de documentação capazes de preservar a prova, através da Cadeia de Custódia.

Quando há necessidade de intervir em sistemas ligados, todos os passos devem ser bem documentados, de preferência incluindo fotografias e filmagens dos procedimentos e do estado do material periciado e apreendido. A integridade dos arquivos resultantes da coleta deve ser garantida, normalmente através de funções unidirecionais de resumo (*hash*). Os valores obtidos devem ser incluídos no Auto de Busca e Apreensão para fins de documentação, para o caso de futuros questionamentos.

Por ser uma área relativamente nova, os peritos normalmente não estão preparados para intervir nos sistemas de informática ligados. Falta-lhes familiaridade com o grande número de ferramentas possíveis de uso. Além disso, caso as ferramentas sejam utilizadas de forma aleatória, não sistemática, tendem a causar maiores alterações no sistema e aumentar o risco de esquecimento de coleta de determinados dados.

O sistema operacional Microsoft Windows é o mais utilizado no mundo (NETMARKETSHARE, 2011a), estando instalado em mais de 90% de todos os computadores, conforme Figura 1.1.

Dentre os sistemas operacionais Microsoft Windows, o sistema ainda predominante, instalado em mais de 50% dos computadores, segundo NETMARKETSHARE (2011b), é o Windows XP, conforme Figura 1.2. A Tabela 1.1, por sua vez, mostra a evolução da utilização dos sistemas operacionais no período de outubro de 2010 a agosto de 2011 (NETMARKETSHARE, 2011c).

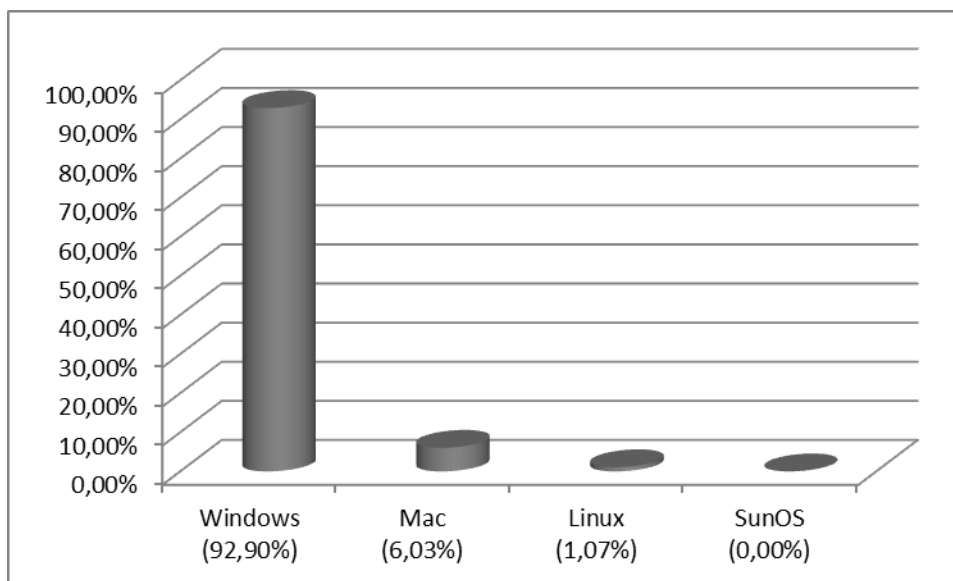


Figura 1.1: Sistemas operacionais mais utilizados.

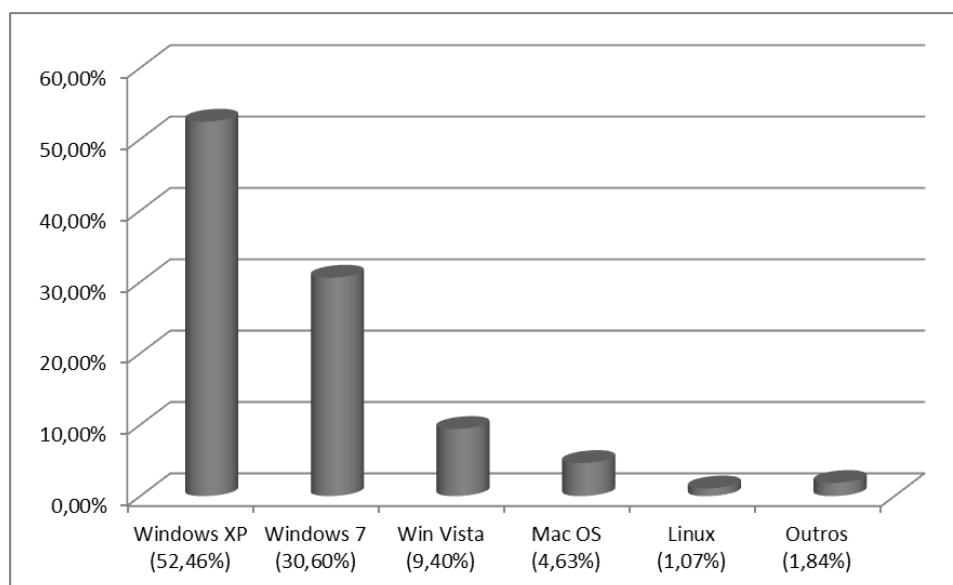


Figura 1.2: Comparação de uso de Windows XP, 7, e outros.

Tabela 1.1: Evolução dos sistemas operacionais mais utilizados.

Mês Ano	Win XP	Win 7	Win Vista	Mac OS	Outros
<b>Out. 2010</b>	60,76%	18,90%	13,33%	4,55%	2,46%
<b>Nov. 2010</b>	59,80%	20,34%	13,04%	4,63%	2,19%
<b>Dez. 2010</b>	58,92%	21,67%	12,58%	4,67%	2,15%
<b>Jan. 2011</b>	57,62%	23,26%	12,15%	4,97%	1,99%
<b>Fev. 2011</b>	57,51%	24,09%	11,49%	4,95%	1,96%
<b>Mar. 2011</b>	56,78%	25,23%	11,02%	5,02%	1,95%
<b>Abr. 2011</b>	55,84%	26,36%	10,73%	5,2%	1,87%
<b>Mai. 2011</b>	55,22%	27,27%	10,46%	5,18%	1,87%
<b>Jun. 2011</b>	54,04%	28,68%	10,06%	5,25%	1,96%
<b>Jul. 2011</b>	52,80%	29,66%	9,84%	5,24%	2,45%
<b>Ago. 2011</b>	52,46%	30,60%	9,40%	4,63%	2,91%

A Figura 1.3 apresenta uma projeção logarítmica para os próximos meses, comparando a utilização dos sistemas Windows XP e Windows 7, a partir dos dados da Tabela 1.1. Seguindo a tendência atual, é provável que o número de computadores com sistema operacional Windows 7 alcance o número de computadores com Windows XP instalado, em julho ou agosto de 2012, tornando-se predominante a partir de então.

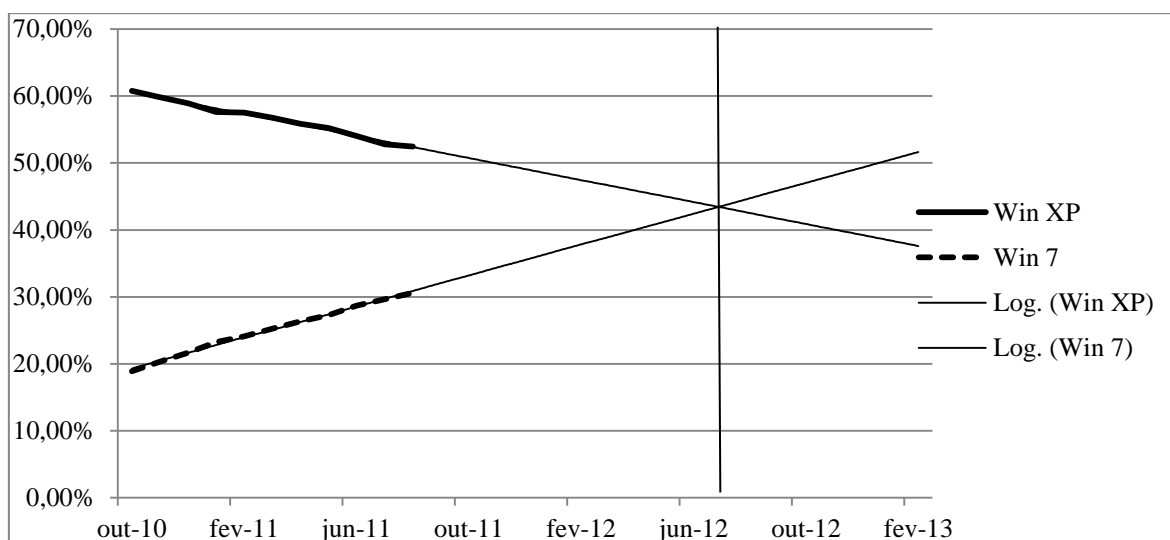


Figura 1.3: Projeção do uso dos sistemas Windows XP e 7.

Para efeito de testes e análise de adequação das ferramentas de captura de dados voláteis selecionadas, o presente trabalho foi desenvolvido em sistemas operacionais Microsoft Windows XP, de 32 bits. Este sistema foi escolhido para fins de padronização dos testes, por ser ainda o mais utilizado e por possuir grande estabilidade. Esta escolha não traz prejuízo para a continuidade do desenvolvimento deste trabalho, já que todas as ferramentas testadas e listadas no Anexo A, são também compatíveis com o sistema operacional Windows 7. O problema da utilização de eventuais ferramentas específicas para determinado sistema operacional poderá ser tratado em trabalhos futuros, através do reconhecimento automático do sistema operacional e utilização da ferramenta correspondente.

## 1.1. OBJETIVOS

Como objetivo desta dissertação propõe-se o desenvolvimento de um método a ser utilizado durante o procedimento de busca e apreensão de material de informática, levando em consideração o estado em que o computador é encontrado: ligado ou desligado.



É proposta ainda uma ferramenta de integração de aplicativos de coleta de dados voláteis em sistemas de informática baseados em Windows. Preconiza-se a captura automática com o objetivo de acelerar o processo, diminuindo o tempo necessário e a possibilidade de erros na coleta.

#### **1.1.1. Objetivos específicos:**

- Propor um método para orientar os peritos criminais durante os procedimentos de busca e apreensão de equipamentos de informática, de forma a garantir a integridade e a credibilidade dos dados coletados;
- Desenvolver um protótipo que verifique a exequibilidade e a possibilidade de desenvolver uma futura solução de integração de ferramentas para coleta de dados voláteis em sistemas informatizados, que possa ser efetivamente utilizada por peritos criminais ou, eventualmente, outros profissionais capacitados, na coleta de dados voláteis;
- Desenvolver um estudo de caso em que a proposta será testada e avaliada.

#### **1.2. JUSTIFICATIVA**

O presente trabalho pretende desenvolver uma ferramenta visando integrar uma solução de coleta de dados voláteis, utilizando de forma sistemática e organizada, algumas das diversas ferramentas existentes no mercado. Os utilitários utilizados são, de forma geral, programas grátis, encontrados na Internet. Quando não totalmente gratuitos, são permitidos sem ônus para uso particular ou sem fins lucrativos, e alguns ainda são disponibilizados apenas para as forças policiais.

Com a utilização de uma solução integrada de ferramentas, diminui-se o risco de erro por esquecimento de alguma ferramenta específica para coletar determinado dado, ou pelo uso das ferramentas na ordem incorreta, permitindo a coleta mais rápida e correta de todos os dados, na sequência ideal.

A coleta de dados voláteis deve ser feita em uma sequência que parta dos dados mais voláteis para os menos voláteis. Os dados mais voláteis tendem a desaparecer mais rapidamente, tendo a preferência na ordem de coleta.

A RFC 3227 (BREZINSKI e KILLALEA, 2002) traz um exemplo de ordem de coleta, em

um sistema de informática típico, partindo dos dados mais voláteis para os menos voláteis:

- Registros e memória *cache*;
- Tabela de roteamento, tabela de processos e memória física;
- Sistemas de arquivos temporários;
- Conexões remotas;
- Topologia de rede.

As ferramentas preferencialmente utilizadas para a coleta são as de linha de comando, que são mais leves e comprometem menos recursos da máquina alvo. A ferramenta utilizada ocupa parte da memória RAM, reforçando a ideia que os dados mais voláteis, que tendem a desaparecer mais rapidamente, devem ser coletados primeiro.

Existem diversas ferramentas voltadas para resposta a incidentes e segurança na Tecnologia da Informação (TI) (IEONG, 2011). Um dos problemas de se utilizar estas ferramentas está no fato de que o usuário tem que lembrar todos os comandos e parâmetros para executar as ferramentas corretamente em linha de comando. Após, o perito terá que consolidar os resultados de forma a realizar seu relatório. Assim, para utilizar estas ferramentas em todo o seu potencial, é necessário agregá-las em um aplicativo que as execute de forma automática e na ordem correta, atendendo aos princípios forenses relacionados, e salvando os resultados de forma integrada e lógica em um arquivo, para análise posterior.

Algumas das ferramentas encontradas podem ser utilizadas tanto para segurança da informação, protegendo os computadores contra ataques em tempo real, quanto para perícia forense, mais preocupada na preservação das evidências.

Existem algumas soluções integradas para o problema da coleta de dados voláteis no mercado. Entretanto, a maioria delas tem fins comerciais e não permite fácil atualização e adequação necessária ao caso específico da Polícia Federal. Além do aspecto financeiro, existe a necessidade de se aguardar o lançamento de novas versões, além de não possibilitar acesso ao código fonte.

Para isso, será necessário realizar uma ampla revisão das ferramentas voltadas à captura de dados voláteis, das soluções de integração existentes, da maneira de integrar as ferramentas escolhidas, e da maneira de formatar o relatório de saída dos dados coletados.

Devido à rápida evolução da computação forense, dos sistemas de informática, e dos crimes relacionados, as ferramentas de análise forense não conseguem acompanhar no mesmo passo. Para cada novo sistema operacional, nova versão ou novo programa de roubo de dados desenvolvido, há necessidade de adequação, atualização e adaptação das ferramentas de detecção e análise.

### **1.3. ORGANIZAÇÃO**

Este trabalho está dividido em cinco capítulos e seis anexos. O primeiro capítulo trata da introdução, versando sobre os objetivos, a justificativa e a organização da dissertação. O segundo capítulo traz uma revisão bibliográfica, tratando de alguns conceitos fundamentais para a compreensão do problema e buscando o estado da arte na área de coleta de dados voláteis em sistemas informatizados. No terceiro capítulo é feita uma revisão das principais ferramentas passíveis de utilização na extração de dados voláteis, seguindo o princípio da utilização de ferramentas de acesso gratuito, de pouca interferência no sistema analisado, de linha de comando, e que colham as informações julgadas mais importantes para a análise necessária. Além disso, aborda algumas soluções de integração de ferramentas de coleta de dados voláteis, com a finalidade de embasar a solução aqui proposta. O quarto capítulo trata da metodologia proposta, detalhando o método proposto para o procedimento de busca e apreensão e a ferramenta de coleta de dados proposta. Este capítulo termina com a apresentação de um estudo de caso, contendo algumas coletas realizadas, que comprovam a exequibilidade do método. No quinto capítulo são apresentadas as conclusões e a proposta de trabalhos futuros. No final, são incluídos seis anexos: o primeiro apresenta um resumo das funcionalidades de algumas ferramentas de captura de dados voláteis; o segundo propõe um *checklist* com um roteiro de tarefas que o perito deve realizar no local de busca e apreensão; o terceiro traz um roteiro básico de procedimentos a serem seguidos durante o procedimento da busca e apreensão; o quarto mostra o conteúdo do arquivo “coletadados.bat”, efetivamente utilizado na coleta de dados voláteis; o quinto, mostra o conteúdo do arquivo “Recalcula Hashes.bat”, utilizado para refazer o cálculo de *hashes*, em caso de inclusão de novos arquivos na pasta “Resultados”; e, por fim, o sexto anexo apresenta o conteúdo do arquivo “LeiaMe.txt”, incluído no *flash drive* de aquisição de dados voláteis, com um manual básico de operação da coleta.

## **2. REVISÃO BIBLIOGRÁFICA**

Este capítulo apresenta alguns conceitos básicos, necessários ao entendimento do tema em estudo, e faz um levantamento do estado da arte em matéria de coleta de dados voláteis em sistemas informatizados.

### **2.1. PERÍCIA COMPUTACIONAL E EVIDÊNCIA DIGITAL**

Perícia Computacional ou Informática Forense é o processo de coletar, analisar e preservar dados relacionados a computadores, de modo a preservar seu valor probatório junto à Justiça (STACY JR. e LUNSFORD, 2011).

Evidência digital é a informação ou dado de valor para a investigação, armazenado ou transmitido através de um dispositivo eletrônico. Evidências armazenadas em computadores são, muitas vezes, latentes, frágeis e podem ser facilmente alteradas, danificadas ou destruídas. Arquivos criados pelo usuário do computador podem conter importantes evidências de atividades criminosas, como agendas de endereços, bancos de dados, fotografias (incluindo pedofilia), arquivos de áudio ou vídeo, planilhas eletrônicas, senhas, comunicação entre os criminosos através de e-mails ou outros mecanismos de comunicação instantânea, etc. (STACY JR. e LUNSFORD, 2011).

Evidência pode ser definida como qualquer informação de valor probatório, significando que ela ou prova ou ajuda a provar algo relevante para o caso. É mais prudente tratar qualquer informação de valor probatório obtido durante a investigação como evidência (MANDIA, PROSISE e PEPE, 2003).

Para facilitar o entendimento da importância de se coletar dados voláteis em computadores, é realizada, na Seção 2.2, uma breve revisão a respeito dos principais componentes de um computador. Este conhecimento é necessário para uma melhor compreensão de como e onde os dados são armazenados e porque correm o risco de serem perdidos durante o desligamento do sistema.

### **2.2. PRINCIPAIS COMPONENTES DE UM COMPUTADOR**

Os componentes de um computador são agrupados em três subsistemas básicos: a unidade central de processamento (CPU), a memória principal (RAM) e os dispositivos de entrada

e saída. Na Figura 2.1 é ilustrada a interação destes componentes (MACHADO e MAIA, 1992).

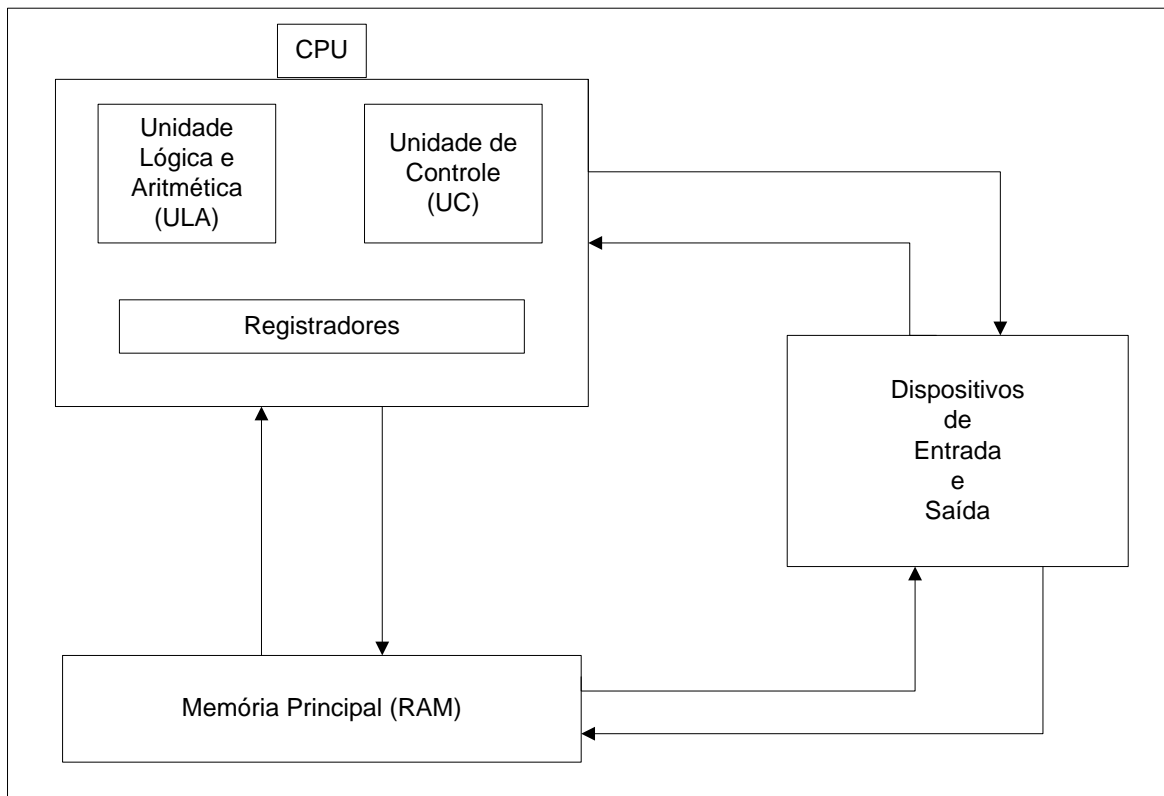


Figura 2.1: Interação entre os subsistemas básicos do computador.  
Fonte: (MACHADO e MAIA, 1992)

### 2.2.1. Processadores

O Processador, ou Unidade Central de Processamento (CPU), tem como função principal unificar todo o sistema, controlando as funções realizadas pelos outros componentes. A CPU é composta por dois componentes básicos, a unidade de controle (UC) e a unidade lógica e aritmética (ULA) (MACHADO e MAIA, 1992).

A função da CPU é buscar instruções na memória e executá-las, em seguida. Seu ciclo básico de execução consiste em buscar a instrução da memória, decodificá-la para determinar seus operandos e funções a executar, executá-la, e em seguida, tratar a instrução seguinte, até que o programa pare (TANEMBAUM, 2009).

### 2.2.2. Registradores

“São dispositivos de alta velocidade, localizados fisicamente na CPU, para armazenamento temporário de dados” (MACHADO e MAIA, 1992).

O registrador é o elemento superior da pirâmide da memória, por possuir a maior velocidade de transferência dentro do sistema, menor capacidade de armazenamento e maior custo (MONTEIRO, 1995).

Existem registradores para propósitos gerais, como conter variáveis e resultados temporários, e registradores especiais, para propósitos específicos, como o contador de programa, o ponteiro de pilha e o PSW (*program status word*). O sistema operacional deve estar sempre atento ao estado e ao conteúdo dos registradores. Quando o sistema operacional compartilha a CPU com mais de um programa, necessita, às vezes, interromper um programa e iniciar outro. Nestes casos, é necessário que os dados contidos nos registradores sejam salvos, para que possam ser recuperados posteriormente, quando seu programa de origem voltar a ser executado (TANEMBAUM, 2009).

### **2.2.3. Memória Cache**

Esta memória, hierarquicamente, está abaixo da camada de registradores, sendo controlada principalmente por hardware (TANEMBAUM, 2009). É uma memória de alta velocidade, mais lenta que os registradores, porém mais rápida que a memória principal.

Os modernos computadores costumam ter dois ou até três níveis de *cache*, sendo o seu tamanho limitado pelo alto custo. A cada nível subsequente, diminui a velocidade e aumenta a capacidade de armazenamento.

Todas as requisições da CPU que não podem ser atendidas pela memória *cache* são direcionadas para a memória principal.

### **2.2.4. Memória Principal (RAM)**

Também conhecida como memória primária, real ou RAM (*random access memory*).

A memória principal é dividida em linha de cache (*cache lines*). As linhas de cache mais frequentemente utilizadas são mantidas em um *cache* de velocidade maior. Quando o programa precisa ler uma palavra de memória, o *hardware* verifica se a linha necessária está na *cache* (*cache hit*). Neste caso, nenhuma requisição adicional é necessária. Entretanto, caso a linha requisitada esteja ausente da *cache* (*cache miss*), há necessidade de uma requisição adicional, enviada à memória principal, com perda substancial de tempo (TANEMBAUM, 2009).

Palavra é a unidade de informação do sistema CPU/memória principal, que deve representar o valor de um número (um dado) ou uma instrução de máquina (MONTEIRO, 1995).

Durante a operação normal de um sistema informatizado, é necessária certa quantidade de memória, chamada de memória de acesso aleatório (RAM) ou memória principal, onde todas as requisições da CPU que não podem ser atendidas imediatamente pela memória *cache* são temporariamente armazenadas (TANEMBAUM, 2009).

#### **2.2.5. Memória Secundária**

É um meio permanente de armazenamento. Enquanto os dados contidos em registradores, memória *cache* e memória principal são voláteis, sendo perdidos no momento de desligamento do computador, a memória secundária permanece armazenada mesmo depois do desligamento da máquina (MACHADO e MAIA, 1992).

Trata-se de uma memória de acesso bem mais lento, quando comparado às memórias voláteis. Sua vantagem, porém, está no menor custo e na alta capacidade de armazenamento.

Exemplos deste tipo de memória são os discos rígidos e os *flash drives*.

#### **2.2.6. Dispositivos de Entrada e Saída**

São os dispositivos que permitem a comunicação entre o computador e o mundo externo. Podem ser divididos em duas categorias: na primeira estão os dispositivos utilizados como memória secundária e na segunda, os dispositivos que permitem a interação do ser humano com o computador, como teclado, monitor, *mouse*, impressora e *scanners*, etc.

Na Seção 2.3 são apresentados os princípios básicos relacionados à segurança e à preservação dos dados coletados, com vistas a garantir sua validade em um futuro processo judicial.

### **2.3. PRINCÍPIOS BÁSICOS DE SEGURANÇA**

Os mecanismos de segurança da informação buscam reduzir os riscos de vazamentos, fraudes, erros, uso indevido, sabotagens, paralisações ou qualquer outro mecanismo de desvio ou alteração de informações (MEDEIROS, 2011).

Os princípios básicos de segurança da informação são a autenticidade, a confidencialidade, a integridade e a disponibilidade das informações (SOUSA e PUTTINI, 2011):

- Autenticidade. Visa garantir a correta identificação de um usuário ou de um computador, assegurando ao receptor que a mensagem é realmente procedente da origem informada em seu conteúdo;
- Confidencialidade. Protege as informações contra acessos indevidos por pessoas não autorizadas;
- Integridade. Consiste em proteger a informação contra modificações não autorizadas explicitamente pelo seu proprietário, assegurando que os dados originais não sofreram qualquer tipo de alteração. Uma das formas de alcançar este objetivo é através das funções de *hash*;
- Disponibilidade. Significa que as informações tem que estar sempre acessíveis e prontas pra uso.

Na Seção 2.4 são apresentas as funções de *hash*, utilizadas como meio de garantia de integridade dos dados coletados.

## **2.4. FUNÇÕES DE *HASH***

São funções que relacionam um arquivo de entrada de tamanho variável a um valor de saída de tamanho fixo, que serve como autenticador (STALLINGS, 2008).

As funções de *hash* podem ser usadas para criptografia, autenticação e até mesmo para assinatura digital. Alguns exemplos de algoritmos utilizados são MD5, SHA-1, SHA-256, SHA-384 E SHA-512 (FERGUSON e SCHNEIER, 2003).

Sua característica marcante é que é muito difícil encontrar dois arquivos de entrada que produzam o mesmo resultado na saída, e, a partir da saída, é computacionalmente inviável encontrar a entrada. Dessa forma, estas funções são utilizadas para garantir a integridade de arquivos digitais.

Nas Seções 2.5 e 2.6, são apresentados, respectivamente, os conceitos de *Malware* e *Rootkit*, importantes devido ao risco de alterações que podem provocar nos dados coletados.



## 2.5. MALWARE

Este termo vem do inglês (*malicious software*), significando *software* malicioso. Refere-se a programas desenvolvidos para alterar ou danificar o sistema, roubar informações, ou provocar outras ações não pretendidas pelo usuário atual. Exemplos comuns de *malware* incluem vírus, *worms*, *trojans* e *spyware* (TECHTERMS.COM, 2011).

## 2.6. ROOTKIT

*Rootkit* é um *software* que permite acesso privilegiado e contínuo a um computador, ao mesmo tempo em que fica invisível aos administradores do sistema, subvertendo as respostas normais e esperadas de comandos do sistema operacional ou de outros aplicativos. O termo *rootkit* é uma concatenação dos termos *root* e *kit*. *Root* é nome tradicional da conta com privilégios de administrador do sistema, nos sistemas operacionais *Unix*, enquanto o termo *kit* refere-se aos componentes de *software* que integram a ferramenta. Tipicamente, o *rootkit* é instalado na máquina pelo atacante após ter obtido poderes de administrador do sistema, explorando alguma vulnerabilidade conhecida ou tendo acesso à senha de administrador. Os *rootkits* são de difícil detecção, uma vez que podem subverter o próprio *software* que supostamente deveria detectá-lo (LINFO, 2011).

A Seção 2.7 apresenta o conceito de Cadeia de Custódia, importantíssimo para a correta manipulação e documentação das evidências, de modo a preservar seu valor probatório.

## 2.7. CADEIA DE CUSTÓDIA

“A Cadeia de Custódia é um processo usado para manter e documentar a história cronológica da evidência, para garantir a idoneidade e o rastreamento das evidências utilizadas em processos judiciais” (LOPES, GABRIEL e BARETA, 2006).

A Cadeia de Custódia trata dos procedimentos que buscam garantir a idoneidade das evidências através da descrição e da documentação detalhada de como a evidência foi encontrada e de como foi tratada dali por diante. Todo o procedimento deve ser documentado de tal maneira que fique registrado onde, quando, e por quem a evidência foi descoberta, manipulada, coletada e armazenada. Quando a evidência passa para a responsabilidade de outra pessoa, este fato, com todos os detalhes envolvidos, incluindo número de lacres e outros procedimentos de segurança, deve ser também cuidadosamente

documentado (BREZINSKI e KILLALEA, 2002).

O procedimento de busca e apreensão deve ser acompanhado de duas testemunhas presenciais, que de preferência não tenham parentesco com o suspeito ou com a vítima e não sejam policiais.

O Código de Processo Penal (BRASIL, 1941) dispõe sobre as testemunhas no procedimento de busca e apreensão da seguinte forma:

- “Finda a diligência, os executores lavrarão auto circunstanciado, assinando-o com duas testemunhas presenciais...” (art. 245, §7º);
- “Toda pessoa poderá ser testemunha” (art. 202);
- “A testemunha não poderá eximir-se da obrigação de depor. Poderão, entretanto, recusar-se a fazê-lo o ascendente ou descendente, o afim em linha reta, o cônjuge, ainda que desquitado, o irmão e o pai, a mãe, ou o filho adotivo do acusado, salvo quando não for possível, por outro modo, obter-se ou integrar-se a prova do fato e de suas circunstâncias (art. 206);
- “A testemunha fará, sob palavra de honra, a promessa de dizer a verdade do que souber e lhe for perguntado, devendo declarar seu nome, sua idade, seu estado e sua residência, sua profissão, lugar onde exerce sua atividade, se é parente, e em que grau, de alguma das partes, ou quais suas relações com qualquer delas, e relatar o que souber, explicando sempre as razões de sua ciência ou as circunstâncias pelas quais possa avaliar-se de sua credibilidade” (art. 203);
- “Não se deferirá o compromisso a que alude o art. 203 aos doentes e deficientes mentais e aos menores de 14 (quatorze) anos, nem às pessoas a que se refere o art. 206” (art. 208).

(Grifos nossos)

O Código Penal (BRASIL, 1940) define o crime de falso testemunho:

- “Fazer afirmação falsa, ou negar ou calar a verdade como testemunha, perito, contador, tradutor ou intérprete em processo judicial, ou administrativo, inquérito policial, ou em juízo arbitral:

Pena - reclusão, de um a três anos, e multa” (art. 342).

Por fim, a Instrução Normativa nº 11-01/DG-DPF-MJ (BRASIL, 2001) da Direção-Geral

do Departamento de Polícia Federal, publicada no Boletim de Serviço nº 129, de 09/07/2001, e no DOU nº 126, Seção 1, de 02/07/2001 recomenda que as testemunhas não sejam policiais:

- “A busca domiciliar será feita mediante mandado judicial, precedida de investigação sobre o morador do local onde será realizada, visando colher elementos sobre sua pessoa (atividades, periculosidade e contatos), sempre que possível com a presença da autoridade policial e de testemunhas não policiais...” (art. 65);
- “No caso de consentimento do morador a busca será presenciada por duas testemunhas não policiais, que assinarão o respectivo auto, além do termo de consentimento de busca” (art. 66.1);
- “Os executores da busca providenciarão para que o morador e as testemunhas acompanhem a diligência em todas as dependências do domicílio” (art. 68.1);
- “Ocorrendo entrada forçada em virtude da ausência dos moradores, os executores adotarão medidas para que o imóvel seja fechado e lacrado após a realização da busca, que será assistida por duas testemunhas não policiais” (art. 69);
- “Após a realização da busca, mesmo quando resultar negativa, será lavrado auto circunstanciado, assinado por duas testemunhas presenciais” (art. 70).

(Grifos nossos)

Assim, apesar de a Lei não proibir expressamente a utilização de testemunhas que sejam parentes do suspeito ou da vítima, esta conduta não é aconselhável. Em primeiro lugar, os parentes podem se recusar a prestar este papel. Além disso, não são obrigados a falar a verdade. Da mesma forma, os policiais não estão proibidos de testemunhar, mas a recomendação da Instrução Normativa citada e o bom senso dizem que esta situação deve ser evitada.

A seguir, são apresentados os principais princípios que regem a adequada coleta de dados voláteis, na Seção 2.8.

## 2.8. PRINCÍPIOS FUNDAMENTAIS DA COLETA DE DADOS VOLÁTEIS

A aquisição de dados voláteis baseada em software necessita, necessariamente, de relaxar o critério da fidelidade, devido à natureza de constantes mutações no conteúdo da memória. Esta condição é inevitável em um sistema de informática em funcionamento, ainda mais quando são executadas ferramentas de captura neste mesmo sistema (SCHATZ, 2011).

Os princípios fundamentais que norteiam a extração de dados em sistemas ligados orientam as seguintes condutas (IEONG, 2011):

- Devem-se coletar todos os dados que serão perdidos ao desligar o sistema;
- Devem-se coletar primeiramente os dados mais voláteis, deixando os menos voláteis para o final;
- Os dados devem ser coletados no menor tempo possível e levando em conta a sua importância;
- Os dados coletados devem permanecer disponíveis para futuras análises, se necessárias, e os exames realizados devem ser tão repetíveis quanto possível;
- Deve-se manter a integridade dos dados coletados;
- As ferramentas de coleta devem capturar os dados de forma fidedigna;
- As ações realizadas em cada caso em particular devem ser relevantes e específicas o caso.

Os dados voláteis incluem qualquer dado armazenado na memória, ou em trânsito, que serão perdidos durante uma queda de energia ou quando o sistema é desligado. Dados voláteis são encontrados em registradores, na *cache*, e na memória *RAM* (Memória de acesso aleatório). Dados voláteis passíveis de coleta podem incluir (SUTHERLAND, *et al.*, 2010) (SHIPLEY e REEVE, 2011):

1. Data e hora do sistema;
2. Usuários ativos e suas credenciais de autenticação;
3. Informação sobre processos em execução;
4. Informações dos registros do Windows;
5. Dispositivos conectados ao sistema;
6. Informações do sistema;

7. Conexões de rede;
8. Estado da rede;
9. Conteúdo da área de transferência;
10. Histórico de comandos;
11. Arquivos abertos.

Perícia em sistemas ligados exige uma abordagem mais criteriosa do que o exame tradicional, com o sistema desligado. Deve haver extremo cuidado para minimizar o impacto das ferramentas utilizadas (SUTHERLAND, *et al.*, 2010).

A partir da memória principal, pode ser possível encontrar senhas ou dados de usuários, não gravados em disco. É aconselhável que o perito capture todos os dados voláteis possíveis. A ordem de coleta pode ser crucial para a investigação. O perito deve avaliar o caso cuidadosamente, para decidir a ordem de coleta, partindo dos dados mais voláteis para os menos voláteis. Uma sequência possível poderia ser (SUTHERLAND, *et al.*, 2010):

1. Registradores e memória *cache*;
2. Memória física;
3. Estado da rede;
4. Processos em execução;
5. Volumes criptografados montados, etc.

Na avaliação de ferramentas para coleta de dados voláteis, devem ser considerados, entre outros aspectos (SUTHERLAND, *et al.*, 2010):

1. Total de memória alocada pela ferramenta;
2. O impacto da ferramenta nos Registros do Windows;
3. O impacto da ferramenta no sistema de arquivos;
4. Uso de DLLs presentes no sistema.

A memória RAM é chamada volátil porque os dados são perdidos quando a máquina é desligada. A grande importância em se coletar a memória RAM antes de desligar o computador suspeito é que nela podem ser encontradas informações de grande interesse para a condução da análise posterior, ou mesmo no processo investigatório, como por exemplo (SHIPLEY e REEVE, 2011):

1. Processos em execução;
2. Lista de comando executados;
3. Senhas em texto claro;
4. Versões decifradas de dados criptografados;
5. Mensagens instantâneas;
6. Endereços IP;
7. *Malwares*.

É importante ressaltar que um computador ligado encontra-se em constante alteração de dados, tanto de memória, quanto de disco e processos. Assim, uma coleta de memória levará a resultados diferentes, a cada vez que for executada. Consequentemente, não há como executar uma função de *hash* de memória, pois os resultados serão sempre diferentes. O que se recomenda, e deve ser feito, é um *hash* do arquivo resultante da coleta de memória (WAITS, et. al., 2010). O resultado do *hash* deste arquivo deve ser incluído no Auto de Busca e Apreensão, buscando garantir a Cadeia de Custódia e evitar que haja questionamentos futuros. Agindo desta forma, teremos um arquivo contendo a cópia da memória física com garantia de integridade, possibilitando a repetição dos exames, caso necessário.

A análise dos dados voláteis coletados, realizada em momento posterior, em laboratório, é bastante complexa. Um único endereço físico de memória pode conter instruções de máquina, dados inicializados e não inicializados, e estruturas de dados específicas para um diferente número de programas. Além disso, muitos processadores suportam virtualização de memória, onde cada programa ou sistema operacional pode enxergar o mesmo endereço físico de diferentes maneiras. Partes deste endereço virtual podem estar na memória, no disco, ou pode mesmo não existir. Diferenças entre linguagens de programação, compiladores, interfaces de programação de aplicações (API) e bibliotecas de sistemas, podem tornar cada sistema levemente diferente. Devido a esses desafios, ainda não existe uma ferramenta que faça uma análise completa e abrangente dos dados de baixo nível coletados em um sistema ligado (PETRONI JR., WALTERS, et al., 2011).

A computação forense é uma área que evolui rapidamente. Como consequência, os crimes de informática também evoluem na mesma proporção. Mais ainda, os sistemas de informática evoluem em velocidade superior à das ferramentas de análise desenvolvidas (STACY JR. e LUNSFORD, 2011).

Apesar da intensa pesquisa realizada nos últimos anos, a captura e a análise da memória física em sistemas operacionais em execução ainda está em um estágio inicial de compreensão e desenvolvimento e ainda não existe uma técnica totalmente eficaz. Apesar disso, a análise da memória volátil (RAM) é capaz de recuperar informações relevantes, que de outra maneira seriam perdidas, caso fosse utilizada a técnica de retirar o cabo de energia. É altamente recomendável que a análise tradicional, baseada em disco rígido, seja complementada através da análise de memória física, que está se tornando cada vez mais importante, e em alguns casos determinante, na medida em que as ferramentas de captura e análise se tornam mais sofisticadas e eficazes (RUFF, 2008).

Para finalizar este capítulo de Revisão Bibliográfica, são apresentados, na Seção 2.9, os principais conceitos relacionados à coleta de dados voláteis.

## 2.9. COLETA DE DADOS VOLÁTEIS EM SISTEMAS INFORMATIZADOS

A extração de dados voláteis de sistemas informatizados ligados vem sendo alvo de crescente interesse pelos pesquisadores. Dados voláteis podem ser definidos como qualquer dado que deixe de existir quando o computador é desligado, não sendo possível recuperá-lo posteriormente (SUTHERLAND, *et al.*, 2010).

No nível mais básico, a perícia digital é composta de três grandes fases, descritas como: Aquisição, Análise e Apresentação (CARRIER, 2011), conforme Figura 2.2.

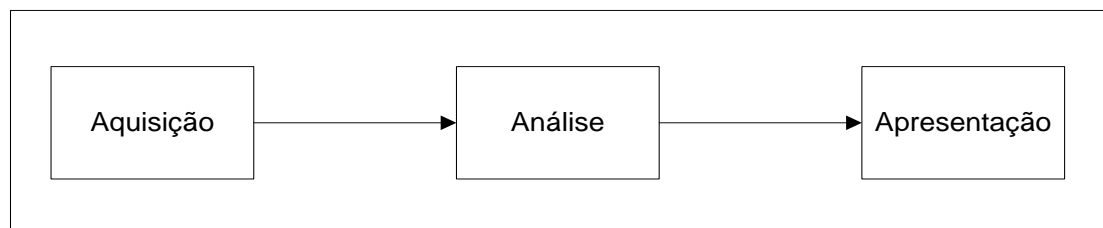


Figura 2.2: Fases da perícia digital.

1. **AQUISIÇÃO:** Na fase de aquisição, ocorre a coleta de todos os dados encontrados em um sistema digital, para análise posterior. Como nessa fase ainda não é sabido exatamente qual informação será útil, tudo deve ser coletado, incluindo espaços alocados e não alocados. As ferramentas utilizadas devem interferir o mínimo possível no sistema investigado;
2. **ANÁLISE:** Na fase de análise, o material obtido na fase de aquisição é

examinado para que sejam identificadas as evidências presentes. O exame de arquivos e o conteúdo de pastas, além da recuperação de conteúdo apagado, faz parte dos objetivos desta fase. O exame é feito sobre uma cópia fiel do original, que deve ser verificada através de funções de *hash*;

3. APRESENTAÇÃO: Na fase de apresentação, são apresentadas as evidências encontradas e as conclusões alcançadas através da fase de análise.

A abordagem pericial tradicional consiste em retirar o cabo de energia da máquina suspeita, para analisar os dados presentes na mídia de armazenamento, posteriormente, em laboratório. Esta técnica pode levar à perda de importantes evidências presentes nos dados voláteis, devido ao crescente uso de criptografia de disco e de sistema (SUTHERLAND, *et al.*, 2010). Há uma forte tendência a se utilizar armazenamento remoto de dados, em servidores remotos, através de conexões de rede ou Internet. Neste caso, dependendo da solução utilizada, também poderá haver perda irreversível das informações em caso de desligamento precoce do sistema.

Desligar o computador através de seu cabo de energia produz menos alterações nas evidências armazenadas no disco rígido, mas, por outro lado, tende a destruir uma quantidade significativa de evidências voláteis. Quando é utilizada criptografia, principalmente de disco, a senha é fornecida pelo usuário durante o boot, e pode ser armazenada na memória RAM. Assim, se for realizada uma coleta da memória RAM para análise posterior, é possível que a senha seja recuperada. Outra abordagem interessante é realizar uma cópia lógica do conteúdo do disco, enquanto o sistema ainda está ligado e os dados estão acessíveis (RICHARD III e ROUSSEV, 2010).

Coletar dados digitais em um sistema já desligado traz a vantagem de tornar a sobrescrita acidental ou modificação de dados praticamente impossível. Por outro lado, não permite a aquisição de dados voláteis, que são perdidos durante o processo de desligamento do sistema. Além disso, há outras situações em que a recuperação de dados permanentes também é praticamente inviabilizada. É o caso, por exemplo, do uso de criptografia, quando só é possível recuperar as informações com o uso da senha de acesso correta. Mais uma vez, este problema seria contornado caso a aquisição lógica dos dados criptografados tivesse se dado com o sistema ainda ligado. Outro exemplo é a aquisição de informações referentes ao estado da rede e suas portas relacionadas, que também são perdidas ao se



desligar o sistema (LESSING e VON SOLMONS, 2011).

Devido às limitações da coleta de dados tradicional, em sistemas desligados, a aquisição com o computador ainda ligado pode ser de extrema importância. Esta técnica permite a recuperação de relevantes informações que de outra maneira poderiam ser perdidas. Infelizmente, esta abordagem também tem suas limitações. A mais importante é que cada computador analisado possui um sistema operacional diferente instalado. Assim, o perito precisa ter conhecimento de uma grande variedade de *hardware*, *software* e sistemas operacionais. O perito deve verificar o sistema em análise e aplicar os princípios periciais corretamente, de maneira a não inviabilizar a futura aceitação das evidências no devido processo legal. Parte do processo de aquisição de dados voláteis consiste em executar aplicativos na CPU do sistema suspeito, podendo levar a potenciais alterações de dados de registradores, memória RAM ou do próprio disco rígido. Dependendo de como se dá a abordagem no local de aquisição dos dados voláteis, a alteração do sistema pode ser tão expressiva que pode inviabilizar o uso futuro das informações coletadas (LESSING e VON SOLMONS, 2011).

A popularização do uso de programas de criptografia, cada vez mais fáceis de utilizar e muitas vezes incorporados aos sistemas operacionais, está tornando mais comum o fato de se encontrar sistemas ligados utilizando esta tecnologia. Normalmente não é muito fácil detectar a criptografia em uso no sistema, uma vez que o *software* utilizado pode ser muito discreto, deixando poucos rastros da sua presença. Assim, a abordagem na coleta de dados voláteis em sistemas ligados tem que se ser bastante criteriosa, a fim de detectar a presença de criptografia e, se for o caso, realizar uma cópia lógica do sistema antes de desligá-lo. A análise com o volume ainda montado possibilita ainda a aquisição lógica dos dados nele contidos. De outra forma, apareceria apenas um arquivo criptografado, difícil de ser detectado e praticamente impossível de se acessado, No caso de criptografia de sistema, todos os dados devem ser copiados antes do seu desligamento (LOWMAN, 2010).

A grande capacidade de armazenamento da memória RAM, geralmente com mais de 4 GB, na maioria dos computadores vendidos à pessoas físicas atualmente, é capaz de guardar grande quantidade de dados, podendo incluir, entre outras informações, senhas usadas para criptografia (SUTHERLAND, *et al.*, 2010).

Podem ser encontradas várias evidências extremamente úteis na memória RAM, como por

exemplo, o conteúdo inteiro ou parcial de arquivos apagados, senhas em texto claro, *buffers* com conteúdo da área de transferência, informações sobre processos em execução ou já encerrados, etc. O conteúdo da memória física é o dado mais volátil e mais vulnerável encontrado em um sistema informatizado, podendo desaparecer rapidamente, caso não seja coletado rapidamente antes dos demais procedimentos (AKKAN, 2006).

Análise de memória é parte importante de qualquer investigação digital, permitindo o acesso aos dados voláteis não encontrados em uma imagem de disco rígido. Apesar dos recentes progressos da análise de memória, as dificuldades ainda são grandes, devido à falta de flexibilidade das ferramentas existentes, que geralmente só podem ser utilizadas em sistemas operacionais específicos e respectivas versões para os quais foram codificadas. A razão para isso é que já que as estruturas de dados utilizados pelos sistemas operacionais mudam a cada nova versão, as ferramentas forenses também precisam ser atualizadas (OKOLICA e PETERSON, 2010).

Memórias RAM de grande capacidade também facilitam a utilização de *malwares* residentes em memória. Assim, não é mais possível ignorar a memória volátil dos computadores (WAITS, et. al., 2010).

Apesar da inegável importância da captura da memória volátil, a necessária execução de ferramentas no computador investigado provoca mudanças no estado do sistema e no conteúdo da memória capturada. Além disso, a ferramenta de captura não possui controle sobre os processos executados na máquina alvo, de forma que programas maliciosos podem detectar as ferramentas de captura de memória e provocar alterações defensivas no sistema, causando inconsistências na imagem de memória capturada (LIBSTER e KORNBLUM, 2011).

Um dos princípios mais importantes ligados à informática forense é o Princípio da Troca, de Locard (*Locard's Exchange Principle*), segundo o qual ocorrem mudanças em um sistema de informática ativo, simplesmente pela passagem do tempo. Isto ocorre devido aos processos que estão em execução, aos dados que estão sendo gravados ou apagados na memória, a conexões de rede sendo criadas ou finalizadas, e assim por diante. Se as mudanças ocorrem simplesmente pela passagem do tempo, são agravadas quando o perito executa seus programas de coleta de dados. A execução de ferramentas no sistema provoca o seu carregamento na memória física, sobrescrevendo outros dados ali presentes

(CARVEY, 2007).

A coleta de dados em computadores ligados deve ser realizada com impacto mínimo sobre a integridade do sistema. Até há pouco tempo os resultados obtidos desta forma não eram bem aceitos na Justiça, devido à interferência do perito no sistema original. Entretanto, não há mais como fugir destas técnicas, para que não haja perda definitiva de informações. Pequenas interferências no sistema podem e devem ser aceitas, desde que bem documentadas, com o objetivo maior de preservar informações vitais para a investigação e para o processo judicial (GROBLER e VON SOLMONS, 2010).

É importante salientar que a inserção de qualquer dispositivo em um computador ligado produz pequenas alterações no sistema. O uso apropriado das ferramentas de captura de dados voláteis e a inserção destes dispositivos não adiciona nenhuma evidência ao sistema. A execução de uma ferramenta capaz de realizar a coleta de memória RAM, por exemplo, necessita de uma pequena porção da própria memória a ser capturada. Assim, a inserção de um dispositivo USB também adiciona uma entrada no Registro do sistema operacional. Todas essas pequenas alterações não produzem grandes consequências no sistema como um todo e podem ser explicadas posteriormente, através do exame minucioso e detalhado do material coletado. Essas pequenas alterações são produzidas pela interação das ferramentas com o sistema operacional, interferindo apenas com os arquivos do sistema operacional, não acarretando nenhuma mudança importante no conteúdo dos dados salvos no sistema (SHIPLEY e REEVE, 2011).

### 3. COLETA DE DADOS

As ferramentas utilizadas neste trabalho enviam as informações coletadas para arquivos texto. Optou-se por este tipo de saída pela possibilidade de fácil verificação de seu conteúdo, ainda durante o período da coleta, com pequeno esforço computacional. Os dados contidos nestes arquivos podem subsidiar a conduta do perito no restante da análise, enquanto o computador continua ligado. Dependendo das informações encontradas, pode ser necessário realizar uma cópia lógica de dados, por exemplo.

Posteriormente, as informações coletadas, serão examinadas exaustivamente pelo perito criminal. Essa análise será realizada no laboratório forense, juntamente com o restante do material apreendido.

#### 3.1. FERRAMENTAS X COMANDOS DE SISTEMA

A Tabela 3.1 apresenta algumas das ferramentas gratuitas para coleta de dados voláteis utilizadas, com resumos de suas funcionalidades, desenvolvidas pela Nirsoft (NIRSOFT, 2011a).

Tabela 3.1: Exemplos de ferramentas da Nirsoft.

<b>Ferramenta</b>	<b>Funcionalidade</b>
USBDeview	Lista os dispositivos USB conectados
IEHistoryView	Recupera páginas acessadas pelo Internet Explorer
MozillaHistoryView	Recupera páginas acessadas pelo Mozilla Firefox
ChromeHistoryView	Recupera páginas acessadas pelo Google Chrome
MyLastSearch	Recupera últimos termos pesquisados

A Tabela 3.2 apresenta algumas das ferramentas gratuitas para coleta de dados voláteis do pacote Sysinternals, com resumos de suas funcionalidades, disponibilizadas pela Microsoft (MICROSOFT, 2011a).

Tabela 3.2: Exemplos de ferramentas da Sysinternals.

<b>Ferramenta</b>	<b>Funcionalidade</b>
Handle	Recupera relação de processos com arquivos e pastas abertos
ListDLLs	Recupera DLLs carregadas no sistema
PsFile	Exibe os arquivos abertos remotamente
PsInfo	Recupera informações sobre o sistema
PsList	Exibe os processos em execução
PsLoggedOn	Verifica quais usuários estão ativos

Outras ferramentas e comandos do próprio sistema operacional Windows podem ser encontrados no Anexo A. A seleção baseou-se no fato de estarem disponíveis gratuitamente, possibilitarem execução através de linha de comando, e por coletarem os dados e as informações consideradas mais relevantes por este estudo.

### **3.2. FTK IMAGER (ACCESS DATA)**

Este programa é extremamente útil para a coleta de dados em local de busca e apreensão, sendo disponibilizado gratuitamente pela empresa AccessData (ACCESSDATA, 2011). São disponibilizadas duas versões, uma que requer instalação e está atualmente na versão 3.0 e outra que não requer instalação e está atualmente na versão 2.9.0 (FTK Imager Lite).

Apesar de não ser um programa de linha de comando, possibilitando coleta automatizada de dados, como é o foco deste trabalho, trata-se de uma ferramenta de grande valia e com boas soluções para alguns dos problemas que podem ser encontrados durante a coleta de dados.

No caso de ser detectada a presença de criptografia ou de armazenamento remoto de dados no sistema investigado. O FTK Imager pode ser utilizado para a coleta lógica de dados. Além disso, ele também pode ser usado para realizar a captura da memória física e dos registros do sistema operacional. A vantagem dos aplicativos de linha de comando está na sua facilitada automação. Entretanto, nos casos em que houver necessidade de intervenção adicional do perito, o “FTK Imager” traz uma interface intuitiva e de fácil utilização.

Algumas vantagens adicionais do FTK Imager, além de ser grátis, é que ele pode realizar imagens em diferentes formatos. Além de permitir uma cópia forense (*bit a bit*) de disco inteiro, possibilita a aquisição de arquivos ou pastas, utilizando o formato AD1 (cópia lógica). Seguindo a filosofia da captura de dados voláteis, de intervenção mínima no sistema analisado, o “FTK Imager” pode ser executado a partir de um drive USB (como um *flash drive*) ou a partir de uma mídia ótica, sem necessidade de instalação.

O “FTK Imager” possui suporte para linha de comando para apenas três funcionalidades, que não incluem nenhuma daquelas de interesse para o presente trabalho. As linhas de comando suportadas são (ACCESSDATA, 2011):

1. `/CreateDirListing` – Cria um arquivo de lista de diretório na pasta onde o “FTK Imager” é executado;
2. `/VerifyImage` – verifica uma imagem quando especificado o nome do arquivo e seu caminho;
3. `/EnableDebuLog` – permite acesso ao arquivo `FTKImageDebug.log` criado na pasta em que o “FTK Imager” é executado.

### **3.3. FERRAMENTAS INTEGRADAS**

Apesar da disponibilidade de diversas ferramentas e comandos de sistema para coleta de dados voláteis, o usuário se defronta com a dificuldade de ter que se lembrar de diversos comandos e parâmetros correspondentes. Além disso, após a coleta adequada dos dados, o perito teria que consolidar todos os resultados em seu relatório. Assim, para utilizar estas ferramentas em todo o seu potencial, seria necessário agregá-las em um aplicativo que as executasse de forma automática e na ordem correta, atendendo aos princípios forenses relacionados, e salvando os resultados de forma integrada e lógica em um arquivo, para análise posterior (ACCESSDATA, 2011).

#### **3.3.1. Incident Response Collection Report (IRCR)**

O IRCR (*Incident Response Collection Report*) é conhecido como o primeiro conjunto de ferramentas, desenvolvido no ano de 2000, para coletar informações forenses em um computador ligado. A ferramenta é desenvolvida através de um arquivo de lote. Escrita em linguagem DOS e Windows, depende de uma série de programas selecionados que podem ser modificados pelo perito, de acordo com suas necessidades. Antes de sua utilização, é

necessário que o perito forneça as pastas e links para todas as ferramentas utilizadas. De acordo com as ferramentas selecionadas, é possível coletar o histórico de comandos, conexões de rede, portas abertas, processos em execução, informação de registros e log de eventos do sistema investigado (IEONG, 2011).

### **3.3.2. First Responders Evidence Disk (FRED)**

Logo após o lançamento do IRCR, surgiu o FRED (*First Responders Evidence Disk*), codificado de forma similar ao IRCR, em arquivos de lote e utilizando uma série de ferramentas pré-selecionadas com a finalidade de coletar informações voláteis em sistemas ligados. O FRED inicia executando uma série de programas e salva os resultados em um arquivo, calculando seu *hash*. Baseado em treze comandos, o aplicativo consegue coletar informações sobre portas abertas, processos correntes, usuários ativos, configurações de rede, e outras informações (IEONG, 2011).

### **3.3.3. Nigilant32**

Trata-se de uma ferramenta de interface gráfica do tipo *freeware*, desenvolvida pela empresa Agile Risk Management, com base no código da ferramenta *Sleuthkit* (SLEUTHKIT.ORG, 2011). O utilitário foi desenvolvido para operar em sistemas Windows 2000, XP, e 2003 (SHANNON, 2011). A ferramenta está disponibilizada para download isolado (AGILE RISK MANAGEMENT LLC, 2011) e também está disponível nas distribuições do Helix (E-FENSE, 2011). Versões anteriores do Helix eram disponibilizadas gratuitamente e incluíam o Nigilant32. Atualmente, o Helix está disponível apenas mediante pagamento, em uma versão comercial (Helix Enterprise) e em uma versão apenas para membros do fórum da E-FENSE (Helix Pro) mediante pagamento de taxas anuais.

### **3.3.4. Windows Forensics Toolchest (WFT)**

No ano de 2003, Monty McDougal apresentou um sistema de coleta de dados em sistemas de informática ligados mais abrangente e sofisticado, chamado *Windows Forensics Toolchest* (WFT). Para seu desenvolvimento, foram observados os princípios gerais da análise forense baseados em: manutenção da integridade do material examinado; mínima interação do usuário; e coleta de toda informação pertinente para análise posterior. O WFT foi projetado, codificado e compilado como um programa executável. O usuário não pode

modificar o código ou alterar a ordem de execução das ferramentas incorporadas. Assim como ocorre com as ferramentas IRCR e FRED, o WFT também faz uso de ferramentas pré-existentes para a aquisição de dados. Os dados de memória coletados pelo WFT consistem na memória física, informações sobre o sistema, processos correntes, informações de usuário e configurações de rede, além de todos os dados também coletados pelo IRCR e pelo FRED. O WFT inova trazendo um gerador instantâneo de relatório no formato HTML, que é gerado durante o processo de aquisição, possibilitando verificação mais amigável dos resultados (IEONG, 2011).

A última versão do WFT é a v3.0.06, lançada em setembro de 2011. Segundo informação que consta na página de Internet do desenvolvedor (FOOL MOON SOFTWARE & SECURITY, 2011) o WFT é projetado para prover coleta de dados em sistemas ligados, resposta a incidentes ou auditoria em sistemas Windows de forma automatizada, estruturada e repetível. Essencialmente, trata-se de um processamento em lote (*batch*) capaz de executar outras ferramentas de segurança e produzir um relatório em formato HTML seguindo os princípios forenses. O *software* propõe-se a atuar em sistemas Windows NT/2K/XP/2K3/VISTA (MCDUGAL, 2007).

A Tabela 3.3 apresenta alguns dos recursos da ferramenta, segundo a página na Internet da desenvolvedora (FOOL MOON SOFTWARE & SECURITY, 2011).

Tabela 3.3: Recursos do Windows Forensic Toolchest.

<b>Recursos do Windows Forensic Toolchest</b>	<b>2.x</b>	<b>3.x</b>
Geração de relatório em formato texto ou html	Sim	Sim
Capacidade de ser executado localmente, por CD/DVD ou <i>pendrive</i>	Sim	Sim
Verificação da saída através de funções de <i>Hash</i>	Sim	Sim
Suporte a <i>Hash</i> MD5	Sim	Sim
Suporte a <i>Hash</i> SHA1	Não	Sim
Geração de relatório em momento posterior à coleta	Não	Sim
Habilidade de executar ferramentas do SysInternals sem “-accepteula”	Não	Sim
Deteção automática de Sistema Operacional e Drives	Não	Sim
Capacidade de executar comandos “run-time” do Sistema Operacional	Não	Sim
Capacidade de incorporar ferramentas de terceiros	Não	Sim



### 3.3.5. Computer Online Forensic Evidence Extractor (COFEE)

No ano de 2006, inspirado pela ferramenta WFT, Ricci Jeong (2011) iniciou o desenvolvimento do *Computer Online Forensic Evidence Extractor* (COFEE), que utiliza um processamento em lote (*batch*) para executar uma série de ferramentas de resposta a incidentes, de segurança e de coleta de dados voláteis, de maneira similar ao WFT e ao Nigilant32. O COFEE incorporou mais algumas ferramentas ao processo de aquisição, como captura da tela e ferramentas de captura de senhas. A diferença principal entre o COFFE e as soluções apresentadas nas seções 3.3.1, 3.3.2, 3.3.3 e 3.3.4, está no fato de que todas as ferramentas são armazenadas em um dispositivo USB, antes da aquisição dos dados. Ao contrário de interagir com o usuário no momento da coleta, solicitando o destino dos dados coletados, o programa direciona a saída das ferramentas automaticamente para o dispositivo USB já inserido na máquina em análise. O programa consegue detectar automaticamente a versão do sistema operacional da máquina alvo. Assim, com detecção automática do sistema operacional e direcionamento automático da saída para o dispositivo USB, tudo que o perito necessita fazer para iniciar o processo de aquisição de dados é inserir o dispositivo USB na máquina a ser analisada e clicar em um ou dois botões. Outra inovação do COFFE, é que ele separa os procedimentos de aquisição de dados e os procedimentos de análise dos dados. No WFT, por exemplo, os processos de geração do relatório são executados imediatamente após a extração de dados, na própria máquina alvo da investigação, podendo alterar o conteúdo da memória. No COFEE, a seleção de ferramentas a serem utilizadas, a análise, e o processamento dos dados coletados, são realizados na máquina do perito (IEONG, 2011).

A versão 1.0 do COFFE consiste em três componentes principais: uma interface gráfica (GUI) voltada para o perito, um terminal de linha de comandos a serem executados na máquina investigada e os programas nativos do Sistema Operacional, em geral, gratuitos, gerenciados pelo COFEE no terminal de linha de comandos (MICROSOFT, 2007).

A versão 1.1.2, lançada em 2009, não trouxe mudanças importantes no *software*, corrigindo apenas algumas falhas apresentadas nas versões anteriores. Conforme consta no manual, o sistema operacional Windows XP é o único suportado na máquina alvo, onde será realizada a coleta. Ainda segundo o manual, o software poderia, eventualmente, funcionar em algum outro sistema. Entretanto, não foram realizados testes em outros sistemas e não há suporte para eles (MICROSOFT, 2009).

A solução foi projetada para necessitar do mínimo de interação do usuário no momento da coleta de dados. A configuração do dispositivo USB que será levado para o local de busca e apreensão é realizada pelo perito na sua própria máquina, antes de se dirigir ao local de aquisição dos dados. Assim, chegando ao local, basta inserir o dispositivo USB e, após mínima interação, a captura é concluída. Depois, os dados coletados são analisados novamente na máquina do perito, minimizando o tempo de contato e o grau de interação do mesmo com a máquina suspeita (MICROSOFT, 2007).

Trata-se de um bom conjunto de ferramentas, com bom projeto, de fácil instalação e escolha das ferramentas a serem utilizadas em cada caso. Trata-se de um software disponibilizado sem custo, apenas para as forças policiais (AULER, 2009). Nos Estados Unidos e no Canadá, está disponível para membros do *National White Collar Crime Center* (NW3C) (NATIONAL WHITE COLLAR CRIME CENTER, 2011).

### 3.4. COMPARAÇÃO DAS FERRAMENTAS INTEGRADAS

No trabalho de AULER (2009) foi realizada uma comparação entre as ferramentas WFT e COFFE, nas suas versões 1.0 e 3.0.03, apresentada na Tabela 3.4.

Tabela 3.4: Comparação das ferramentas COFEE e WFT (AULER, 2009).

	<b>COFEE v. 1.0</b>	<b>WFT v. 3.0.03</b>
Windows XP	Sim	Sim
Windows 2000	Sim	Sim
Windows 2003	Sim	Sim
Windows Vista	Não	Não
Memória física (RAM)	Segundo manual: Sim Nos testes: Não	Segundo desenvolvedor: Sim Nos testes: Não
Dump de Senhas	Segundo manual: Sim Nos testes: Não	Não
Data e hora do sistema	Sim	Sim
Arquivos abertos	Sim	Sim
Processos em execução	Sim	Sim
Usuários do sistema	Sim	Sim
Portas abertas	Sim	Sim
Configuração de ferramentas	Sim	Não
Configuração de ordem de execução	Sim	Não

Possibilidade de executar a partir de Pen Drive	Sim	Sim
Possibilidade de coletar os dados em Pen Drive	Sim	Sim
Formato do relatório	HTML	HTML
Apresentação do Relatório	Boa	Muito boa
Checagem dos dados coletados ( <i>Hash</i> )	Sim	Sim

### 3.5. LIMITAÇÕES DAS FERRAMENTAS INTEGRADAS EXISTENTES

Durante a avaliação das soluções de captura de dados voláteis na Seção 3.3, verificou-se as seguintes limitações:

- Custo de aquisição, quando pagas;
- Dificuldade de obtenção, quando gratuitas;
- Dificuldade de atualização e adaptação. No caso de surgirem novas necessidades de coleta, há a necessidade de se aguardar o lançamento de novas versões. Além disso, não permitem a adaptação das ferramentas para necessidades específicas, por não disponibilizarem o código fonte;
- Falta de mecanismos de verificação de criptografia, máquinas virtuais ou armazenamento remoto de dados durante a coleta. Consequente perda dos dados relacionados a estas técnicas, que poderiam ser resguardados através de cópia lógica dos mesmos antes do desligamento do sistema.

## **4. METODOLOGIA PROPOSTA**

Neste capítulo é apresentada a ferramenta de coleta de dados proposta e sugerido um método a ser seguido pelos peritos criminais durante a o procedimento de busca e apreensão. O objetivo é minimizar as alterações provocadas no sistema, ao mesmo tempo em que seja coletado o maior número possível de informações voláteis, preservando seu valor probatório através da Cadeia de Custódia.

### **4.1. PROCEDIMENTOS DA BUSCA E APREENSÃO**

Os procedimentos de coleta devem ser tão detalhados quanto possível, facilitando a tomada de decisões durante o procedimento da apreensão. Além disso, os procedimentos da Cadeia de Custódia devem ser claramente documentados (BREZINSKI e KILLALEA, 2002).

Evidências de crimes de informática, assim como todas as outras evidências, devem ser manuseadas com cuidado, de maneira a preservar seu valor probatório. Alguns tipos de evidência computacional requerem cuidados especiais no processo de embalagem e transporte, tomando cuidados especiais com equipamentos suscetíveis a danos ou alterações devido à proximidade de campos eletromagnéticos, como aqueles gerados por eletricidade estática, magnetismo, radiotransmissores ou outros. Deve-se evitar o armazenamento das evidências forenses em veículos, por tempo prolongado, evitando ainda o contato com calor excessivo, frio ou umidade (STACY JR. e LUNSFORD, 2011).

Para uma busca e apreensão realizada de forma ideal, deve o perito participar também das fases de planejamento e coordenação, orientando a equipe quanto ao melhor momento para a abordagem e quanto aos procedimentos de coleta e transporte dos materiais arrecadados.

Não é comum encontrar computadores ligados no momento da execução do mandado de busca e apreensão. Assim, se for sabido de antemão que o alvo da busca utiliza criptografia, por exemplo, é importante que sejam escolhidos um dia e um horário mais propício a encontrar a máquina ligada, de forma a tornar possível a captura dos dados da mesma, antes do seu desligamento para apreensão.

Os procedimentos de busca e apreensão que tratam de crimes de informática podem ser divididos, basicamente, em quatro etapas, ilustradas na Figura 4.1 (HOELZ, RUBACK e

SILVA, 2009).

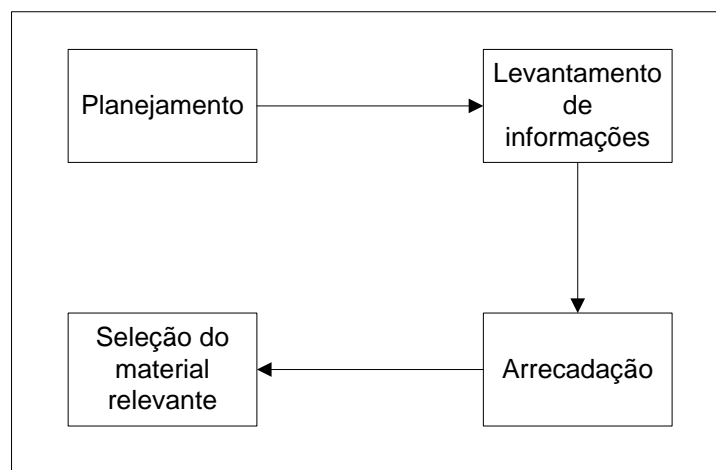


Figura 4.1: Etapas do procedimento de busca e apreensão.

Um dos aspectos mais importantes do campo da computação forense é a documentação. Além de documentar seus próprios atos durante a apreensão, o perito deve também documentar o ambiente da busca antes de começar efetivamente a intervir nos sistemas. Para que a documentação seja feita da melhor forma possível, é recomendado que haja uma pessoa responsável exclusivamente por esta tarefa. Itens que requerem atenção especial durante a documentação, devendo ser fotografados, são (STEEL, 2006):

- Telas do computador, com resolução suficiente para leitura de textos ali presentes, se necessário;
- Conexões de rede, mostrando quaisquer cabos de rede conectados ao computador. As duas pontas do cabo devem ser fotografadas, para o caso em que o perito tenha que provar que o computador estava conectado a algum equipamento específico;
- Conexões de periféricos, para provar que estavam conectados ao computador.

Ao chegar ao local de busca e apreensão, o perito deve cumprir uma série de procedimentos ordenados, de modo a preservar os vestígios e garantir a sua validade no processo judicial. Como ferramenta de auxílio, foi elaborado um *checklist* com as providências a serem tomadas (Anexo B).

Primeiramente deve ser exibido o mandado judicial ao destinatário do mesmo, autorizando a apreensão e análise do material. Imediatamente após ter o local sob controle, deve-se

isolar os equipamentos de informática presentes no recinto. Deve-se impedir que um equipamento ligado seja desligado por intervenção humana, ou que fique indisponível através de hibernação automática ou de execução de protetor de tela com senha, por exemplo, já que será alvo de captura de dados voláteis. Deve-se impedir também que outras evidências sejam ocultadas, adulteradas ou destruídas.

As fotografias devem ser, de preferência, digitais, com no mínimo cinco megapixels de resolução (O'BRIEN, 2011), devendo ser incluídas no procedimento de Cadeia de Custódia. Uma solução possível é armazená-las em uma mídia ótica, que será incluída no Auto de Apreensão e identificada de modo a relacioná-la ao computador correspondente, através de marca, modelo, número de série, etc.

A Figura 4.2 representa a metodologia a ser seguida durante o procedimento de busca e apreensão, no que tange aos equipamentos de informática, e é composta de quatro fases principais.

#### **4.1.1. Fase 1**

Se o computador estiver desligado, deve assim permanecer e deve ser apreendido para exames posteriores, em laboratório. O Anexo C apresenta os detalhes do procedimento de apreensão de equipamentos de informática.

Se o computador estiver ligado, sua tela deve ser fotografada e deve ser providenciado algum mecanismo que o impeça de hibernar ou entrar em descanso de tela. O computador pode estar protegido por senha e não ser possível voltar a ter acesso ao sistema.

A integridade das fotografias deve ser garantida através de uma função unidirecional de resumo (*hash*), cujo resultado será incluído no Auto de Busca e Apreensão ou na Informação Técnica, conforme o caso, podendo ser verificado posteriormente.

Todas as informações relevantes para a investigação ou para futuros exames, tais como senhas, nomes de usuários ou peculiaridades de configuração de sistemas, devem ser solicitadas ao responsável que se encontra no local, e devidamente documentadas, de forma que estejam disponíveis quando necessárias.

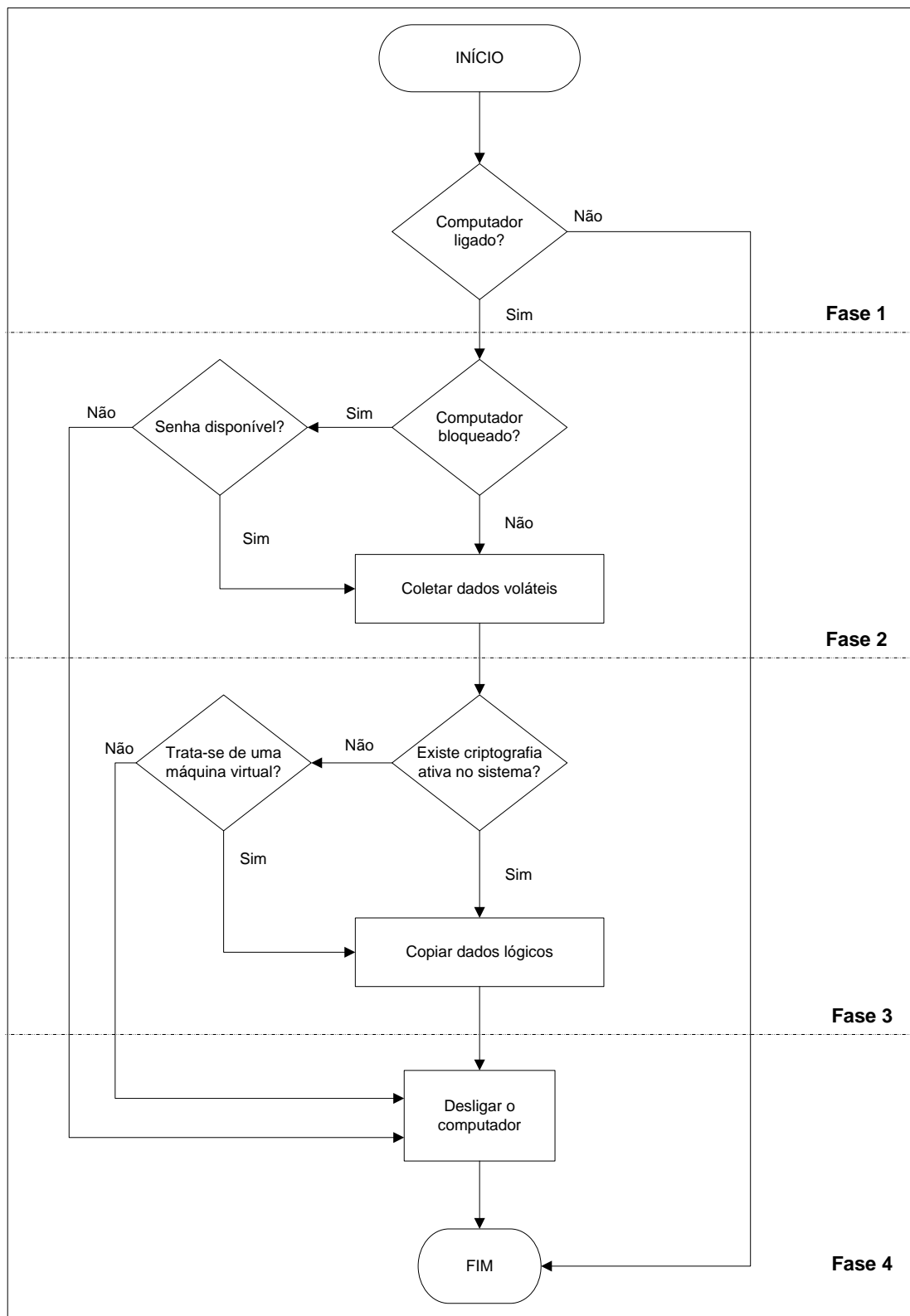


Figura 4.2: Metodologia da apreensão de computadores.

Quando houver intervenção do perito em um sistema informatizado ligado, todos os procedimentos devem ser minuciosamente documentados. Neste caso, para não

sobrecarregar o Auto de Busca e Apreensão, normalmente elaborado pelo escrivão, com detalhes atinentes aos procedimentos periciais, recomenda-se que o perito elabore uma Informação Técnica. Neste documento devem ser detalhados todos os passos realizados, incluindo os *hashes* dos arquivos coletados e/ou das fotografias tiradas.

#### **4.1.2. Fase 2**

O perito deve certificar-se de que as ferramentas de coleta contidas no *flash drive* estejam com suas características originais. Para garantir sua integridade, o perito deve comparar os valores de *hash* dos arquivos contidos no *flash drive*, com os originais, armazenados em sua estação pericial. Antes de reutilizá-lo em um outro computador suspeito, deve conferir novamente a integridade dos arquivos e garantir que não há contaminação por *software* malicioso.

Se o computador não estiver bloqueado, deve-se inserir o *flash drive* contendo os aplicativos automatizados de coleta de dados voláteis (CADAV).

Caso o sistema esteja habilitado para executar automaticamente a partir de *flash drives*, a ferramenta de coleta iniciará automaticamente. Provavelmente isto não ocorrerá, porque o Windows XP, a partir do *Service pack 3*, desabilitou completamente o *autorun* a partir de dispositivos USB. Neste caso, deve-se executar um duplo clique sobre o ícone do arquivo "ColetaDados.bat", contido no diretório raiz do *flash drive* e aguardar a mensagem de término do procedimento.

Caso o computador esteja bloqueado, deve-se verificar se a senha está disponível. Deve-se verificar se há algum documento cotendo a senha nos locais próximos ao computador. Pode também ser perguntado ao usuário, que eventualmente informará a senha, no intuito de colaborar com as investigações. Caso não seja possível desbloquear o computador, o mesmo deve ser desligado e apreendido, conforme instruções do Anexo C.

#### **4.1.3. Fase 3**

Durante a coleta, podem aparecer mensagens na tela, apresentando informações sobre a possível presença de criptografia de volumes, criptografia de sistema, ou virtualização do sistema operacional através do programa "VMWare". Em qualquer um destes casos, o sistema deve ser examinado para confirmar as suspeitas. Devem-se verificar os arquivos "DetectaCripto.txt" e "DetectaVMware.txt" na pasta Resultados, criada no *flash drive* de



coleta durante o procedimento, para maiores detalhes. Em caso de confirmação, deve-se realizar uma cópia lógica dos arquivos encontrados no volume criptografado ou de todo o sistema, dependendo do tipo de criptografia utilizada. Se o sistema estiver sendo executado em máquina virtual, também deve ser realizada uma cópia lógica de todo o sistema.

A cópia lógica pode ser realizada através do programa “FTK Imager” (AccessData), disponibilizado no *flash drive* de coleta, e o resultado deve ser direcionado a um disco rígido externo conectado a outra porta USB.

#### **4.1.4. Fase 4**

Ao final, deve ser verificado se há mais algum dado a copiar, como arquivos lógicos ou memória física. Caso contrário, o *flash drive* de coleta deve ser retirado e o computador desligado. O computador deve ser desligado através da retirada do cabo da fonte de alimentação. No caso de computadores portáteis, além de retirar o cabo da fonte de alimentação, deve-se retirar a bateria ou pressionar o botão de liga/desliga. O material deve ser apreendido conforme instruções do Anexo C.

#### **4.1.5. Procedimentos pós-coleta**

Terminado o procedimento de coleta, o *flash drive* de coleta é inserido no *notebook* do perito para os procedimentos finais. Caso tenham sido tiradas fotografias durante o procedimento de busca e apreensão, elas devem ser copiadas para a pasta “Resultados” do *flash drive* de coleta. Assim, se tiverem sido adicionadas fotografias à pasta “Resultados” e/ou tiver havido coleta adicional de memória física através do programa “FTK Imager” deve ser realizado novo cálculo de *hashes* da pasta “Resultados”, clicando no ícone "Recalcula Hashes.bat". Será criado um novo arquivo chamado "Hashes.txt" na raiz do *flash drive*, contendo o *hash* SHA256 de todos os arquivos contidos na pasta Resultados. Também será criado um arquivo chamado "Hash\_do\_Hashes.txt" na raiz do *flash drive*, contendo o *hash* MD5 do arquivo de *hashes* "Hashes.txt". Este *hash* deve substituir o valor anotado anteriormente, já que houve modificações na pasta “Resultados”. O valor do *hash* deve ser incluído na Informação Técnica elaborada pelo perito criminal, de forma a garantir a integridade dos arquivos coletados durante o procedimento.

Para fins de logística, sugere-se que a pasta “Resultados” seja transferida para mídias óticas, do tipo DVD. Considerando os tamanhos comuns de memória física encontrados na

maioria dos casos, bastará um DVD, ou dois, em casos excepcionais. Desta forma, o perito permanece com seu *flash drive* de coleta e o DVD pode acompanhar o trâmite do Processo, sem qualquer prejuízo. Nos casos em que houver necessidade de cópia lógica de arquivos para discos rígidos externos, devido ao maior volume de dados, o próprio disco rígido utilizado para a coleta deve acompanhar o restante do material de informática apreendido. Neste caso também não há necessidade de realizar novo cálculo de *hashes*, já que o próprio “FTK Imager” cria um arquivo de *log* com estes cálculos. Entretanto, o perito criminal deve verificar o valor do *hash* criado e incluí-lo também em sua Informação Técnica.

#### **4.2. PROTÓTIPO DA FERRAMENTA**

O protótipo da ferramenta de integração proposto no presente trabalho utiliza arquivos *batch* do sistema operacional Windows para automatizar a execução de algumas das ferramentas de coleta apresentadas no Anexo A, direcionando os resultados para uma pasta chamada “Resultados”.

A escolha das ferramentas e a ordem de execução das mesmas tiveram por fundamento os seguintes aspectos:

- Preferência por ferramentas de linha de comando, que acarretam menor consumo de memória, resultando em menor impacto sobre o sistema examinado, quando comparadas a aplicativos que utilizam interfaces gráficas;
- Início da coleta pelos dados mais importantes e mais voláteis;
- Coleta automatizada.

O protótipo de coleta de dados voláteis proposto sugere que as ferramentas sejam executadas a partir de um *flash drive*, que contém todas as ferramentas necessárias, e também receberá o resultado da coleta realizada.

A Figura 4.3 apresenta o conteúdo do diretório raiz do *flash drive* utilizado para captura de dados voláteis.

```
E:\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\>dir
Volume in drive E is Forense
Volume Serial Number is E8D3-1B7B

Directory of E:\

15/05/2011  10:07                43 autorun.inf
31/03/2011  14:43            389.120 cmd.exe
16/07/2011  09:25             8.444 ColetaDados.bat
16/07/2011  09:25          <DIR>      Ferramentas
14/05/2011  18:33             55 FTK Imager.bat
15/05/2011  12:39             32 LeiaMe.bat
15/05/2011  12:36            472 Recalcula Hashes.bat
                6 File(s)          398.166 bytes
                1 Dir(s)    7.901.966.336 bytes free

E:\>_
```

Figura 4.3: Conteúdo do diretório raiz do Protótipo.

Os arquivos presentes no diretório raiz do *flash drive* são os seguintes:

- “autorun.inf” - responsável pela autoexecução da ferramenta, quando permitido pelo sistema operacional da máquina analisada;
- “cmd.exe” - cópia segura do terminal de comandos, independente do sistema analisado;
- “ColetaDados.bat” – seu conteúdo é apresentado no Anexo D;
- “FTK Imager.bat” – faz chamada ao programa “FTK Imager”, presente na pasta “Ferramentas” e descrito na Seção 3.2;
- “LeiaMe.bat” – faz chamada ao arquivo de texto “LeiaMe.txt”, localizado na pasta Ferramentas, contendo breve manual de utilização da ferramenta;
- “Recalcula Hashes.bat” – arquivo *batch* que realiza novo cálculo de *Hashes*, caso haja modificações na pasta “Resultados” posteriormente à coleta primária. Seu conteúdo é apresentado no Anexo E.

Juntamente com as ferramentas disponibilizadas no *flash drive* de coleta de dados voláteis, há também um arquivo de ajuda, chamado “LeiaMe.txt”, com um atalho “LeiaMe.bat” na raiz do *flash drive*, contendo um manual básico sobre a utilização das ferramentas de coleta. O conteúdo do arquivo “LeiaMe.txt” é apresentado no Anexo F.

A Figura 4.4 apresenta o conteúdo da pasta “Ferramentas”, detalhada no Anexo A.

```

c:\ E:\cmd.exe
E:\Ferramentas>dir
Volume in drive E is Foreense
Volume Serial Number is E8D3-1B7B

Directory of E:\Ferramentas

16/07/2011  09:25  <DIR>          .
16/07/2011  09:25  <DIR>          ..
14/07/2011  15:27  <DIR>          chromehistoryview
14/07/2011  15:27  <DIR>          chromePASS
31/03/2011  14:43          717.616 cygwini.dll
16/07/2011  09:09          40.960 Edd120.exe
31/03/2011  14:43          114.688 Fport.exe
14/07/2011  15:27  <DIR>          fsun
23/10/2003  13:35          135.680 grep.exe
31/03/2011  13:25          423.264 handle.exe
14/07/2011  15:27  <DIR>          iehv
31/03/2011  14:43          37.376 iehv.exe
14/07/2011  15:27  <DIR>          iepv
14/07/2011  15:27  <DIR>          Imager_Lite_ 2.9.0
16/06/2011  10:55          5.829 LeiaMe.txt
31/03/2011  14:43          53.248 listdlls.exe
14/07/2011  15:27  <DIR>          mailpv
31/03/2011  14:43          95.104 mdd_1.3.exe
14/07/2011  15:27  <DIR>          mozillahistoryview
14/07/2011  15:27  <DIR>          mspass
14/07/2011  15:27  <DIR>          mylastsearch
31/03/2011  14:43          36.864 netstat.exe
14/07/2011  15:27  <DIR>          passwordfox
31/03/2011  14:43          8.192 pclip.exe
31/03/2011  14:43          10.240 ps.exe
31/03/2011  14:43          232.240 Psinfo.exe
31/03/2011  14:43          86.016 pslist.exe
31/03/2011  14:43          105.264 psloggedon.exe
31/03/2011  14:43          146.432 regedit.exe
14/07/2011  15:27  <DIR>          ScoopyNG
14/07/2011  15:27  <DIR>          skypeLogview
27/02/2009  16:22          136.592 strings.exe
31/03/2011  14:43          72.192 tasklist.exe
14/07/2011  15:27  <DIR>          usbdevview
14/07/2011  15:27  <DIR>          wirelesskeyview
          18 File(s)          2.457.797 bytes
          17 Dir(s)          7.901.966.336 bytes free

E:\Ferramentas>

```

Figura 4.4: Conteúdo da pasta "Ferramentas".

Na Figura 4.5 é apresentado o conteúdo do *flash drive* após a coleta. Pode-se notar que é incluída uma pasta, chamada “Resultados”, contendo os arquivos coletados, e dois arquivos, “Hashes.txt” e “Hash\_do\_Hashes.txt”, contendo o resultado da função de garantia de integridade dos arquivos (*hash*).

```

c:\ E:\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\>dir
Volume in drive E is Foreense
Volume Serial Number is E8D3-1B7B

Directory of E:\

15/05/2011  10:07          43 autorun.inf
31/03/2011  14:43          389.120 cmd.exe
16/07/2011  09:25          8.444 ColetaDados.bat
16/07/2011  09:25  <DIR>          Ferramentas
14/05/2011  18:33          55 FTK Imager.bat
16/07/2011  10:22          1.553 Hashes.txt
16/07/2011  10:22          169 Hash_do_Hashes.txt
15/05/2011  12:39          32 LeiaMe.bat
15/05/2011  12:36          472 Recalcula Hashes.bat
16/07/2011  10:21  <DIR>          Resultados
          8 File(s)          399.888 bytes
          2 Dir(s)          5.691.056.128 bytes free

E:\>

```

Figura 4.5: Conteúdo do diretório raiz do *flash drive*, após a coleta.

#### 4.2.1. Detalhamento do arquivo *batch* “ColetaDados.bat”

O arquivo *batch* “ColetaDados.bat” está localizado no diretório raiz do *flash drive* utilizado na coleta de dados voláteis e contém a chamada às ferramentas de coleta contidas na pasta “Ferramentas”. Durante a execução, será criada uma pasta chamada “Resultados”, no diretório raiz do *flash drive*, para onde serão direcionados os arquivos contendo as informações coletadas.

A sequência de coleta de dados, contida no arquivo “ColetaDados.bat”, através das respectivas ferramentas utilizadas para cada tipo de captura, é a seguinte:

1. Coleta da data e da hora do sistema, para documentação do início do procedimento de coleta, através dos comandos de sistema do Windows <date /t> e <time /t>;
2. Coleta dos dados contidos no registro do Windows, através do comando de sistema do Windows <regedit /e>;
3. Coleta da memória física (RAM) através da ferramenta “mdd”;
4. Coleta do conteúdo da área de transferência, através da ferramenta “pclip”;
5. Coleta das informações relacionadas às conexões TCP ativas, através do comando de sistema do Windows <netstat -ano>;
6. Coleta das informações relacionadas às portas abertas e aplicações associadas, através do comando de sistema do Windows < fport>;
7. Coleta das informações relacionadas às configurações das interfaces de rede, através do comando de sistema do Windows < ipconfig /all>;
8. Coleta de informações sobre processos em execução, através das ferramentas “pslist”, “ps” e “handle”;
9. Coleta da listagem de arquivos recentemente abertos, através do comando de sistema do Windows < tasklist>;
10. Coleta de informações sobre usuários ativos no sistema, através da ferramenta “psloggedon” e do comando de sistema do Windows < dir "%UserProfile%\Recent">;
11. Coleta de informações genéricas sobre o sistema, através da ferramenta “psinfo”;
12. Coleta de senhas, históricos e logs de navegadores, programas de mensagens instantâneas, correio eletrônico, Skype, Internet sem fio, etc.,

através dos programas “iepv”, “passwordfox”, “ChromePass”, “mypass”, “mailpv”, “wirelesskeyview”, “iehv”, “mozillahistoryview”, “chromehistoryview”, “mylastsearch” e “skypelogview”;

13. Coleta de informações sobre os dispositivos USB conectados ao sistema, no momento da análise ou mesmo anterior, através da ferramenta “usbdevice”;
14. Por fim, é feita nova coleta da data e da hora do sistema, para documentação do término do procedimento de coleta, através dos comandos de sistema do Windows <date /t> e <time /t>.

O arquivo “ColetaDados.bat”, além de conter os comandos necessários à execução da coleta de dados referida anteriormente, executa alguns testes para otimizar a coleta, descritos a seguir:

1. Verifica a presença de criptografia pelos programas Truecrypt, PGP, Safeboot ou BitLocker, através do programa “edd”;
2. Verifica se o sistema está sendo executado em máquina virtual do tipo VMWare, através do programa “ScoopyNG”;
3. Verifica o arquivo “Processos.txt”, que contém as informações coletadas sobre processos em execução, pela presença de termos como “vmware”, “pgp”, “truecrypt”, “virtualbox”, “bitlocker”, “VBoxService” e “VBoxTray”, com vistas a aumentar a abrangência da detecção de criptografia e de máquinas virtuais.

O resultado destas verificações é direcionado a um arquivo de texto. Através do programa “strings” é verificada a presença de palavras que confirmem a suspeita do uso de algum dos programas ou termos questionados. Em caso positivo, o perito recebe um alerta na tela, informando-o sobre a suspeita. Neste caso, devem-se examinar os arquivos “DetectaCripto.txt”, “DetectaVMware.txt” e “Processos.txt”, contidos na pasta “Resultados” do *flash drive*. Confirmada a presença de criptografia ou virtualização de sistema, o perito deve executar uma cópia lógica dos arquivos que correm risco de serem perdidos durante o desligamento do computador.

Para finalizar a coleta, são ainda executados os seguintes testes:

1. A coleta de memória física (RAM) é realizada através do programa mdd.exe (Mantech). Devido à extrema importância deste item da coleta, a ferramenta de coleta automatizada de dados voláteis executa um teste para verificar a presença do arquivo correspondente “Memorydump.dd” na pasta Resultados do *flash drive* de coleta. Se este arquivo não estiver presente, o usuário recebe uma mensagem de texto na tela, orientando-o a realizar a coleta de memória física através do programa “FTK Imager”, também disponibilizado no *flash drive*.
2. Por fim, através do programa “fsum”, é realizada uma função unidirecional de resumo (cálculo de *hash*) dos arquivos coletados, utilizando o algoritmo SHA256, e o resultado é salvo no arquivo “Hashes.txt”. Este arquivo, por sua vez, tem também seu *hash* calculado, utilizando o algoritmo MD5 e o resultado é salvo no arquivo “Hash\_do\_Hashes.txt”. A escolha deste último algoritmo (32 caracteres) se deu em razão de ser menor que o SHA256 (64 caracteres) e facilitar a anotação no Auto de Busca e Apreensão.

O conteúdo completo do arquivo “ColetaDados.txt” é apresentado no Anexo D.

A partir da comparação das ferramentas WFT E COFEE apresentada na Tabela 3.4, foram acrescentados testes realizados com a ferramenta Nigilant32 e com a ferramenta proposta neste trabalho (CADAV). Os resultados são apresentados na Tabela 4.1. A eficácia das ferramentas na coleta dos dados propostos foi avaliada com a seguinte escala:

- (-) Não realiza a coleta proposta;
- (+) Realiza a coleta proposta de forma básica;
- (++) Realiza a coleta proposta e traz funcionalidades adicionais.

Tabela 4.1: Comparação entre soluções de captura em sistemas Windows XP.

<b>Dados coletados</b>	<b>Nigilant 32</b>	<b>WFT 3.0.05</b>	<b>COFEE 1.1.2</b>	<b>CADAV 1.0</b>
Data do sistema	+	+	+	+
Hora do sistema	+	+	+	+
Informações do Sistema	+	+	+	+
Cópia de memória física	+	+	+	+
Recuperação de Senhas	-	+	+	+
Arquivos abertos	-	+	+	+
Processos em execução	+	+	+	+

Usuários ativos	+	+	+	+
Conexões de rede	+	+	+	+
Estado da rede	+	+	+	+
Inclusão ou exclusão de ferramentas	-	+	++	+
Configuração da ordem de execução	-	+	++	+
Detecção de Criptografia	-	+	+	++
Detecção de Máquinas Virtuais	-	+	+	++
Cópia dos logs do Skype	-	+	+	+
Cópia dos últimos termos de busca	-	+	+	+
Cópia dos históricos de Internet	-	+	+	+
Cópia do conteúdo da área de transferência	-	+	+	+
Coleta de registros do Windows	-	+	+	+
Coleta de comandos recentemente utilizados	-	+	+	+
Coleta de informações sobre DLLs	-	+	+	+
Calculo do <i>hash</i> dos dados coletados	-	+	+	+

A comparação levou em conta testes realizados em outros trabalhos e funcionalidades anunciadas pelos desenvolvedores das ferramentas. Todas as soluções de integração de ferramentas de captura de dados voláteis recentes utilizam, em geral, ferramentas de acesso gratuito, de fácil obtenção, que podem ser adicionadas e configuradas.

Como diferenciais importantes, destaca-se a facilidade de inclusão, exclusão e da ordem de execução das ferramentas no COFEE. Por outro lado, o CADAV apresenta os testes de detecção de criptografia e máquinas virtuais, não oferecidos pelas outras soluções.

A quantidade e a qualidade de dados capturados não dependem muito da solução de integração propriamente dita. O fator mais importante é a correta seleção e configuração das ferramentas mais apropriadas para cada caso concreto investigado. O WFT e o COFEE oferecem esta funcionalidade através de arquivos de configuração. O protótipo aqui apresentado permite a inclusão e configuração de ferramentas e de sua ordem de execução, de forma estática, através da manipulação do arquivo *batch*, que serializa a extração de dados.

O objetivo principal a ser atingido é coletar, no local de apreensão, com o computador ligado, todas as informações importantes que poderiam ser perdidas em caso de desligamento do sistema. É primordial que as informações estejam à disposição dos peritos para as análises a serem realizadas posteriormente. Por isso, optou-se por destinar a saída de dados a arquivos texto, mais leves e de fácil manipulação e recuperação de informações.

As ferramentas selecionadas foram aquelas consideradas mais úteis do ponto de vista da



perícia criminal. A meta é coletar todos os dados relevantes, seguindo a ordem de importância e a volatilidade.

Durante a captura de dados realizada de forma semiautomática através do protótipo da ferramenta sugerida neste trabalho, pode ser detectada a presença de criptografia ou de utilização de máquinas virtuais. O perito deve estar atento a este fato, estando preparado para tomar outras providências necessárias para evitar a perda de dados de forma irreversível em caso de desligamento do sistema. Caso alguma destas situações seja detectada durante a coleta, o perito deve realizar uma análise mais cuidadosa do sistema, de modo a minimizar a chance de perda de importantes informações durante o desligamento do sistema, mas, ao mesmo tempo, ser extremamente cuidadoso, causando o mínimo possível de alterações no sistema examinado.

Caso as suspeitas de criptografia ou máquina virtual sejam confirmadas, o perito deve executar uma cópia lógica dos arquivos em risco de perda irreversível. Esta pode e provavelmente será a única oportunidade de acesso às informações, que podem ser relevantes e cruciais ao esclarecimento do caso.

Se a cópia automatizada, que inclui cópia da memória física, for bem sucedida, podem-se encontrar senhas, permitindo o acesso a dados criptografados ou a um sistema protegido. Assim, ainda seria possível ter acesso a estas informações, montando o volume novamente no momento da análise em laboratório, ou ligando o sistema com auxílio de alguma das senhas encontradas. Entretanto, esta solução deve ficar reservada para casos excepcionais em que, por algum motivo não foi possível executar a cópia lógica no momento da apreensão.

Pode ocorrer que as senhas encontradas não sejam úteis à primeira vista, ou mesmo não sejam encontradas senhas, aparentemente. As senhas encontradas em navegadores de Internet ou serviços de e-mail, por exemplo, ou mesmo as informações aparentemente sem utilidade, extraídas da coleta de memória física, são importantíssimas. Elas podem ser utilizadas na elaboração de um dicionário de palavras específico para aquele caso, sendo de grande valia em uma quebra de senha por dicionário, realizada em momento posterior.

De qualquer forma, além da captura dos dados voláteis e da cópia lógica, quando necessária, devem ser coletados todos os elementos normalmente apreendidos, para análise

posterior em laboratório. Desta forma ter-se-á o máximo de dados possível e um menor risco de perda de informações essenciais ao esclarecimento do caso.

Todos os arquivos coletados contêm informações relevantes para a análise completa do caso, que será realizada em etapa posterior, em laboratório. Entretanto, alguns dos arquivos coletados merecem atenção especial, ainda no local de apreensão, por conterem informações relevantes para tomadas de decisão relacionadas à própria coleta de dados. Entre eles, estão os arquivos:

- DetectaCrypto.txt – contém informações relevantes sobre a presença ou não de volumes criptografados no sistema;
- DetectaVMware.txt – contém informações relevantes sobre a presença ou não de virtualização de sistema através do programa VMware;
- Processos.txt – contém a lista de processos em execução no sistema, podendo evidenciar a presença de criptografia ativa ou virtualização de sistema, casos em que a providência a ser tomada é imediata: cópia lógica dos arquivos envolvidos, que correm sério risco de ficarem completamente inacessíveis após o desligamento do computador.

O arquivo coletado, “DispUSB.txt” pode conter importantes informações sobre dispositivos USB conectados ao sistema no momento da apreensão ou mesmo em períodos anteriores. A análise deste arquivo pode trazer pistas a respeito de dispositivos USB que podem estar presentes no ambiente e devem ser localizados e apreendidos.

### 4.3. ESTUDO DE CASO

Para o teste do protótipo proposto neste trabalho, foram escolhidos seis cenários, todos executados em Sistema Operacional Windows XP, Service Pack 3, 32 bits (Tabela 4.2). Os cenários foram selecionados na tentativa de reproduzir uma coleta real que possa surgir durante um procedimento de busca e apreensão.

Tabela 4.2: Cenários de coleta utilizados.

Cenário	Máquina	Truecrypt Ativo	Antivírus Ativo
1	Real	X	

2	Real		X
3	VMware	X	
4	VMware		X
5	VirtualBox	X	
6	VirtualBox		X

Os testes foram realizados em máquina real, e em máquinas virtuais *VMware* (VMWARE, 2011) e (VIRTUALBOX, 2011), por estarem entre os cinco melhores aplicativos do segmento (LIFEHACKER, 2011) e estarem disponíveis para testes. Quanto ao programa de criptografia, foi utilizado o *Truecrypt* (TRUECRYPT, 2011) por ser um dos mais populares e estar disponível para download e instalação, sem custo para o usuário. Outros programas de criptografia, como o PGP (SYMANTECH, 2011) e o *DriveCrypt* (SECURE STAR, 2011), são pagos. O *BitLocker* não foi testado por ser específico para algumas versões do sistema operacional Windows Vista e 7 (MICROSOFT, 2011c), não utilizado nestes testes. Também foram realizados testes com programa antivírus ativo e inativo, para verificar as possíveis interferências causadas na coleta. Os programas utilizados foram o AVG (AVG, 2011) e o *Microsoft Security Essentials* (MICROSOFT, 2011d), disponíveis gratuitamente na Internet.

Todas as coletas de dados foram realizadas no dia 18/06/2011, após realizar todas as atualizações possíveis do sistema operacional e do programa antivírus, quando utilizado.

Optou-se por limitar os testes ao Windows XP de 32 bits para simplificar os testes do modelo proposto. Em trabalhos futuros, é possível estender o modelo para outros sistemas operacionais de 32 ou de 64 bits. Para isso, será necessário fazer testes para determinar o sistema operacional e a versão instalada no sistema alvo, logo no início da captura, utilizando ferramentas compatíveis para cada caso.

A título de exemplificação, será apresentado o conteúdo de alguns dos arquivos coletados e algumas fotografias tiradas da tela do computador analisado, durante a coleta. Optou-se por fotografias da tela ao invés de capturá-la através do comando “Print Screen”, para diminuir a intervenção no sistema, como recomendado neste trabalho.

### 4.3.1. Cenário 1

A máquina utilizada está descrita na Tabela 4.3.

Tabela 4.3: Descrição da máquina utilizada no Cenário 1.

Tipo de máquina	Real
Processador	Intel(R) Pentium(R) 4, 2.3 GHz
Sistema operacional	Microsoft Windows XP Professional, Service Pack 3
Memória Física	2048 MB
Programa de criptografia	Truecrypt versão 7.0a – modo volume
Programa antivírus	Inativo
Tempo de coleta	5min54s

#### 4.3.1.1. Resultados obtidos:

A ferramenta de captura faz alguns testes durante a coleta. Sendo verificado que existe a probabilidade de presença de criptografia no sistema, através da verificação do arquivo “DetectaCripto.txt”, é lançado um a aviso na tela informando esta situação, conforme Figura 4.6.

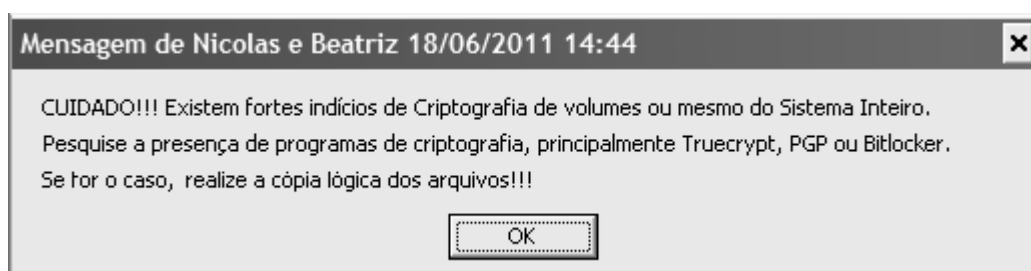
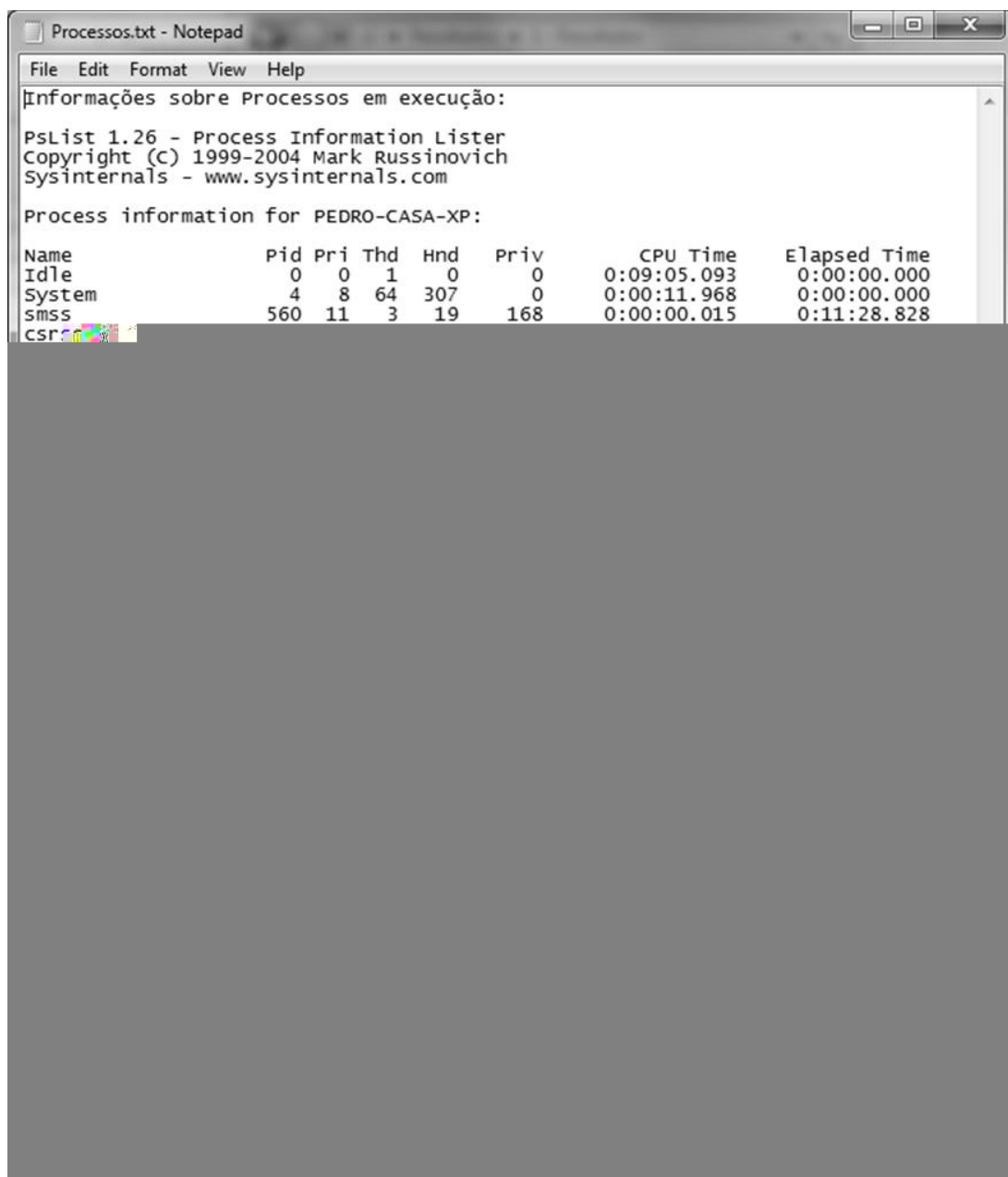


Figura 4.6: Aviso de possível presença de criptografia no sistema.

Em virtude de ter aparecido este aviso na tela, o perito deve fazer uma análise mais cuidadosa da máquina suspeita, verificando se realmente existe o volume criptografado detectado. Sendo confirmada a presença de um volume criptografado, é necessário fazer uma cópia lógica dos dados contidos neste volume, já que os mesmos ficarão inacessíveis no caso de desligamento do sistema.

A presença de criptografia também pode ser evidenciada pela análise do arquivo “Processos.txt”, cujo conteúdo é apresentado na Figura 4.7, resultante da execução da execução da ferramenta “pslist”, onde é possível verificar a presença do processo “TrueCrypt”.



```
Processos.txt - Notepad
File Edit Format View Help
|Informações sobre Processos em execução:
PsList 1.26 - Process Information Lister
Copyright (C) 1999-2004 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for PEDRO-CASA-XP:

Name                Pid Pri Thd  Hnd  Priv      CPU Time  Elapsed Time
Idle                 0  0  1    0    0      0:09:05.093  0:00:00.000
System              4  8  64   307  0      0:00:11.968  0:00:00.000
smss                 560 11  3    19   168    0:00:00.015  0:11:28.828
csrss
```

Figura 4.7: Conteúdo do arquivo "Processos.txt".

A Figura 4.8 apresenta os arquivos coletados, enquanto a Figura 4.9 apresenta o conteúdo do arquivo “DetectaCripto.txt”, resultante da execução da ferramenta “Encrypted Disk Detector (EDD)”, onde pode ser verificada a presença de possível volume criptografado no drive “m”.

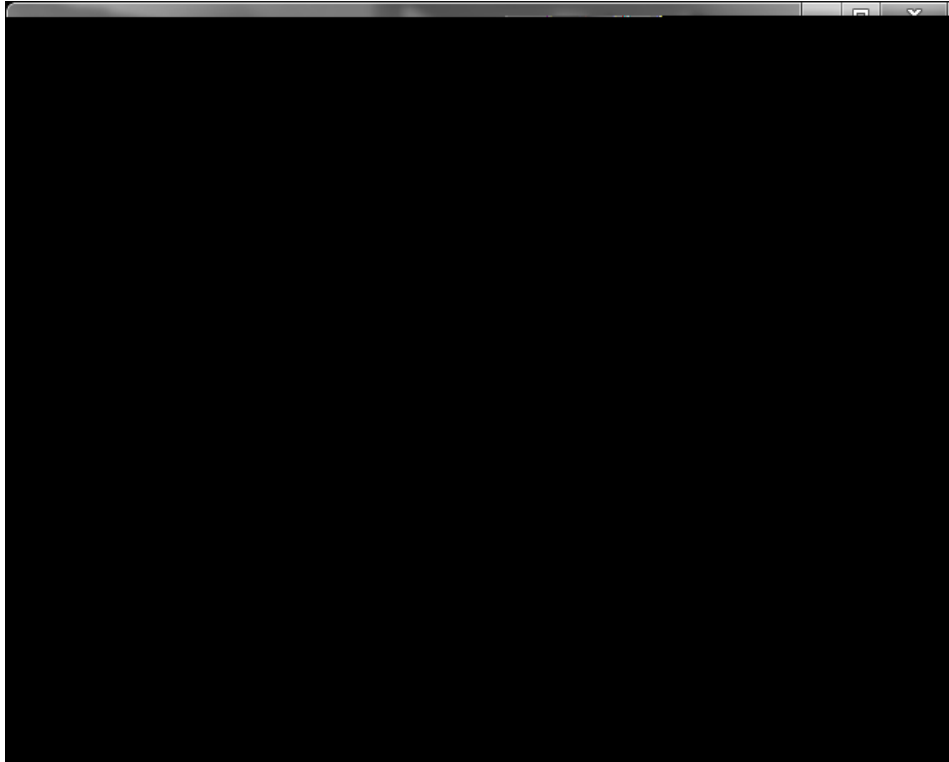


Figura 4.8: Arquivos coletados - Cenário 1

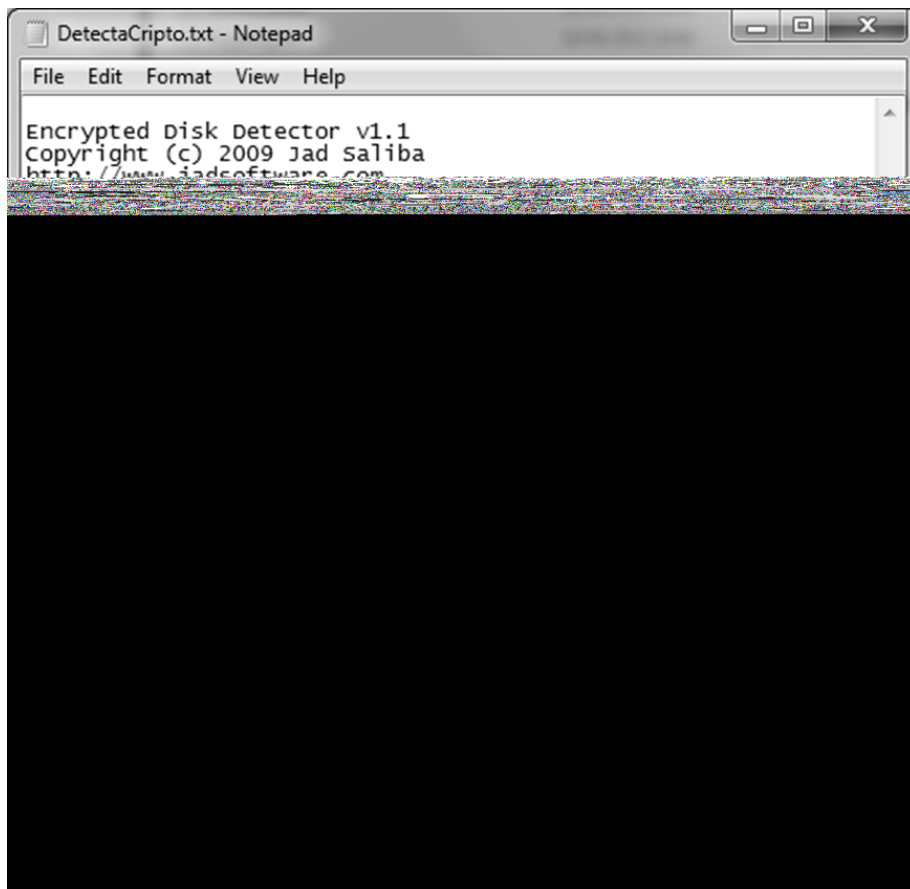


Figura 4.9: Conteúdo do arquivo "DetectaCripto.txt".

### 4.3.2. Cenário 2

A máquina utilizada está descrita na Tabela 4.4.

Tabela 4.4: Descrição da máquina utilizada no Cenário 2.

Tipo de máquina	Real
Processador	Intel(R) Pentium(R) 4, 2.3 GHz
Sistema operacional	Microsoft Windows XP Professional, Service Pack 3
Memória Física	2048 MB
Programa de criptografia	Inativo
Programa antivírus	<i>Microsoft Security Essentials</i>
Tempo de coleta	6min05s

#### 4.3.2.1. Resultados obtidos:

A Figura 4.10 apresenta os arquivos coletados.

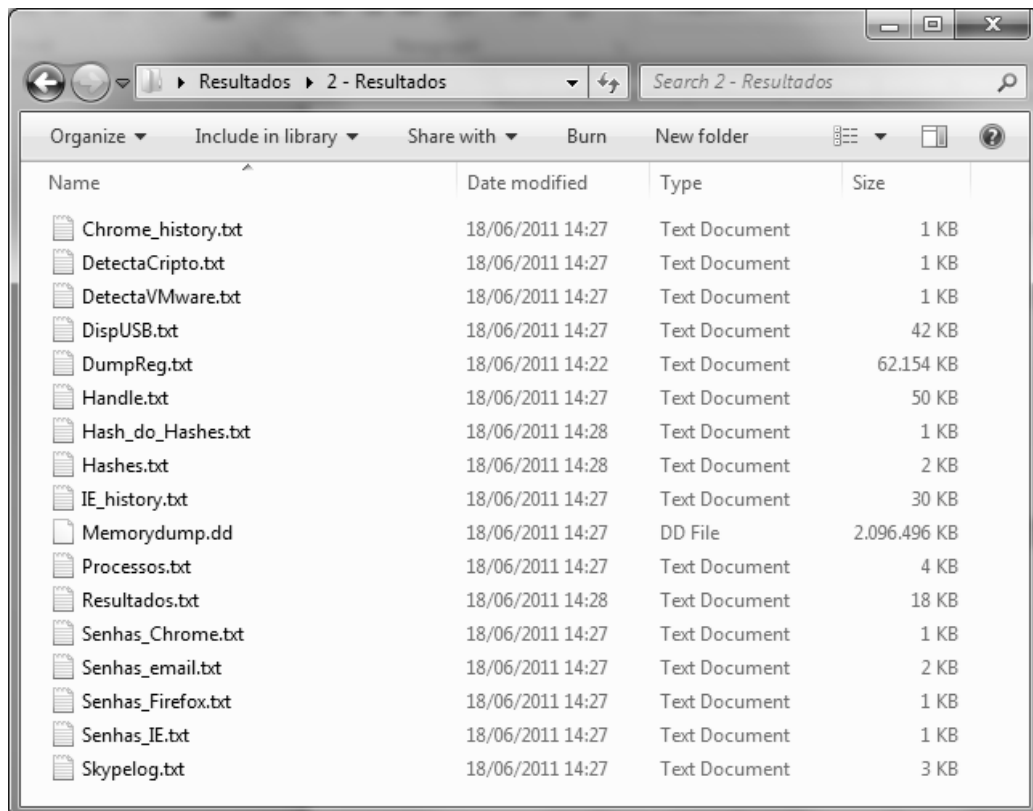


Figura 4.10: Arquivos coletados - cenário 2.

O arquivo “Resultados.txt” é um dos principais resultados da coleta. Devido ao seu grande conteúdo, serão apresentadas apenas algumas partes mais relevantes deste arquivo. A Figura 4.11 mostra data e hora de início da coleta, conteúdo da área de transferência e conexões TCP ativas. A Figura 4.12 apresenta informações sobre as interfaces de rede. A Figura 4.13 apresenta informações sobre o sistema e data e hora do término da coleta.

```

File Edit Format View Help
Data do Sistema:
s b 18/06/2011

-----

Hora do Sistema:
14:22

-----

Conteúdo da área de transferência:

-----

Conexões TCP ativas:
Active Connections

Proto Local Address          Foreign Address         State                   PID
TCP   0.0.0.0:135             0.0.0.0:0               LISTENING               1020
TCP   0.0.0.0:445             0.0.0.0:0               LISTENING                4
TCP   127.0.0.1:1029          0.0.0.0:0               LISTENING               2676
TCP   192.168.1.102:139      0.0.0.0:0               LISTENING                4
TCP   192.168.1.102:1082    201.82.108.9:80         TIME_WAIT               0
TCP   192.168.1.102:1083    201.82.108.9:80         TIME_WAIT               0
TCP   192.168.1.102:1084    201.82.108.9:80         TIME_WAIT               0
TCP   192.168.1.102:1085    201.82.108.9:80         TIME_WAIT               0
TCP   192.168.1.102:1098    74.125.234.96:80        ESTABLISHED             2084
UDP   0.0.0.0:427            *:*                      *:*                      1004
UDP   0.0.0.0:445            *:*                      *:*                      4
UDP   0.0.0.0:500            *:*                      *:*                      696
UDP   0.0.0.0:4500           *:*                      *:*                      696
UDP   127.0.0.1:123          *:*                      *:*                      1152
UDP   127.0.0.1:1900         *:*                      *:*                      1392
UDP   192.168.1.102:123     *:*                      *:*                      1152
UDP   192.168.1.102:137     *:*                      *:*                      4
UDP   192.168.1.102:138     *:*                      *:*                      4
UDP   192.168.1.102:427     *:*                      *:*                      1004
UDP   192.168.1.102:1900    *:*                      *:*                      1392

```

Figura 4.11: Conteúdo parcial do arquivo Resultados.txt - parte 1.

Esta coleta ocorreu de forma praticamente idêntica à coleta do cenário 1, com a diferença de que aqui não há criptografia e o antivírus está ativo. O programa antivírus identificou as ferramentas “mailpassview” e “passwordfox” como ameaças, conforme pode ser visto na Figura 4.14.



```
Resultados.txt - Notepad
File Edit Format View Help
-----
Configuração de interfaces de rede:
Configuração de IP do windows
Nome do host . . . . . : pedro-casa-xp
Sufixo DNS primário. . . . . :
Tipo de nó . . . . . : desconhecido
Roteamento de IP ativado . . . . . : não
Proxy WINS ativado . . . . . : não

Adaptador Ethernet Conexão local:
sufixo DNS específico de conexão . . :
Descrição . . . . . : VIA Rhine II Fast Ethernet
Adapter
Endereço físico . . . . . : 00-13-D4-F1-1A-A9
DHCP ativado. . . . . : Sim
Configuração automática ativada . . : Sim
Endereço IP . . . . . : 192.168.1.102
Máscara de sub-rede . . . . . : 255.255.255.0
Gateway padrão. . . . . : 192.168.1.1
Servidor DHCP . . . . . : 192.168.1.1
Servidores DNS. . . . . : 189.6.0.133
                             189.6.0.138
Concessão obtida. . . . . : sábado, 18 de junho de 2011
14:16:28
Concessão expira. . . . . : domingo, 19 de junho de 2011
14:16:28
-----
```

Figura 4.12: Conteúdo parcial do arquivo Resultados.txt - parte 2.

```
Resultados.txt - Notepad
File Edit Format View Help
-----
Informações do sistema:
System information for \\PEDRO-CASA-XP:
Uptime: Error reading uptime
Kernel version: Microsoft windows XP, Uniprocessor Free
Product type: Professional
Product version: 5.1
Service pack: 3
Kernel build number: 2600
Registered organization:
Registered owner: Pedro Auler
Install date: 14/11/2010, 22:14:23
Activation status: Error reading status
IE version: 8.0000
System root: C:\WINDOWS
Processors: 1
Processor speed: 2.3 GHZ
Processor type: Intel(R) Pentium(R) 4 CPU
Physical memory: 2048 MB
Video driver: NVIDIA GeForce 8500 GT

-----

Data do sistema:
s b 18/06/2011

-----

Hora do sistema:
14:28

-----
```

Figura 4.13: Conteúdo parcial do arquivo Resultados.txt - parte 3.

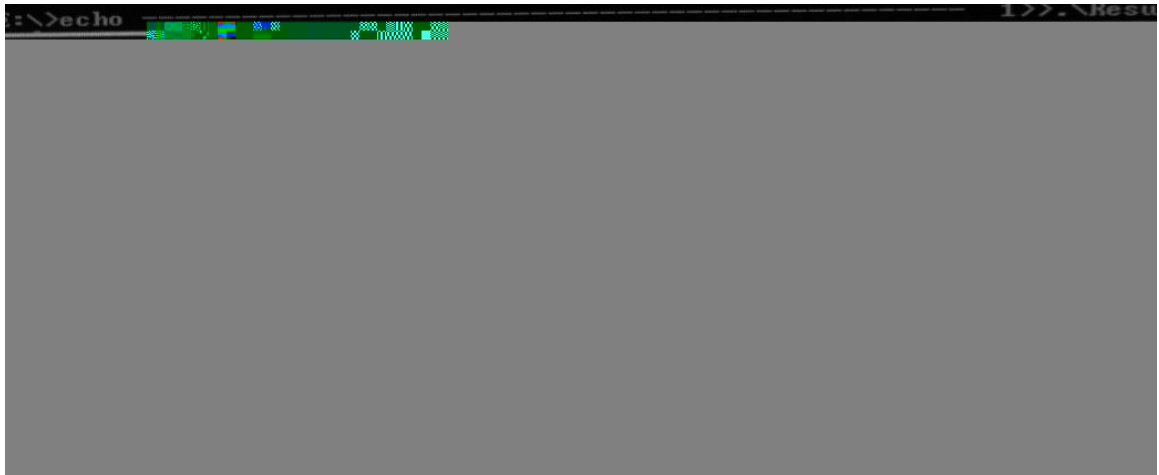


Figura 4.14: Ferramentas identificadas como ameaças pelo antivírus.

Não obstante esta identificação positiva como vírus, não há nenhum prejuízo para a coleta como um todo, que continua normalmente. São perdidas apenas as informações que seriam coletadas pelas ferramentas bloqueadas.

Algumas das ferramentas utilizadas, principalmente as de recuperação de senhas, são classificadas como ameaças pelos antivírus eventualmente instalados na máquina alvo da busca e apreensão. Devido ao fato de recuperarem informações sensíveis como senhas, chaves de instalação e registros do Windows, entre outras, estas ferramentas são consideradas nocivas pelos programas antivírus. As empresas desenvolvedoras de programas antivírus partem do pressuposto de que essa recuperação de dados sensíveis ocorre sempre em favor dos mal intencionados. Não é bem assim, já que um programa de recuperação de senhas, por exemplo, pode perfeitamente ser utilizado para recuperar as senhas perdidas ou esquecidas pelo usuário legítimo. De qualquer forma, é recomendável que se desabilite qualquer antivírus instalado antes de iniciar a coleta dos dados, quando possível.

Em trabalhos futuros, pode ser adicionado algum mecanismo de detecção e desligamento automático dos antivírus executados na máquina investigada. A detecção, com determinação dos processos envolvidos pode ser realizada, por exemplo, pela ferramenta “pslist” (MICROSOFT, 2011a) e o desligamento pode ser realizado, por exemplo, através das ferramentas “pskill” (MICROSOFT, 2011a) ou “nircmd” (NIRSOFT, 2011b).

### 4.3.3. Cenário 3

A máquina utilizada está descrita na Tabela 4.5.

Tabela 4.5: Descrição da máquina utilizada no Cenário 3.

Tipo de máquina	Virtual - VirtualBox versão 4.08 r71778
Processador da máquina hospedeira	Intel(R) Core(TM)2 Duo CPU T7500
Sistema operacional da máquina hospedeira	Ubuntu 10.04, 32 bit, Kernel Linux 2.6.32-32-generic
Memória Física da máquina hospedeira	3048 MB
Sistema operacional da máquina virtual	Microsoft Windows XP Professional, Service Pack 3
Memória Física da máquina virtual	1024 MB
Programa de criptografia	Truecrypt versão 7.0a – modo volume
Programa antivírus	Inativo
Tempo de coleta	13min41s

#### 4.3.3.1. Resultados obtidos:

A Figura 4.15 apresenta os arquivos coletados.

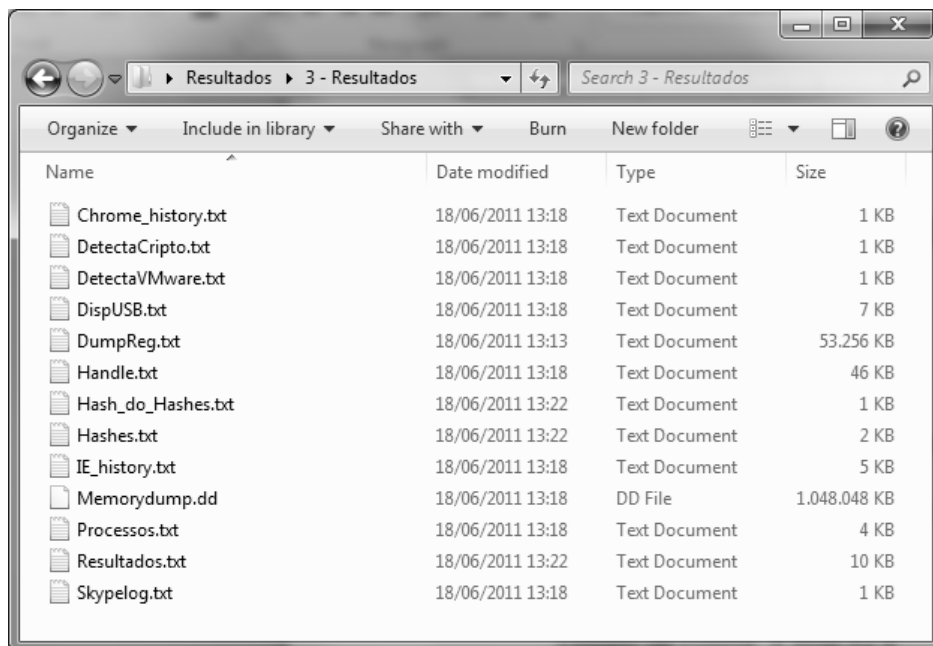


Figura 4.15: Arquivos coletados - Cenário 3.

O volume criptografado pelo programa “Truecrypt” foi identificado, da mesma forma já discutida e ilustrada no Cenário 1, através dos arquivos “DetectaCripto.txt” e “Processos.txt”. O volume criptografado encontrado deve ter seu conteúdo copiado durante o procedimento de coleta de dados, para não ser perdido durante o desligamento do sistema.

Além disso, o sistema estava sendo executado em uma máquina virtual “VirtualBox”. A ferramenta de coleta faz procura por termos específicos para a presença da máquina virtual no arquivo coletado “Processos.txt” e quando os encontra, gera uma mensagem de alerta (Figura 4.16), para que o perito verifique o sistema mais detalhadamente, e, confirmando a suspeita, execute a cópia lógica de todo o sistema.

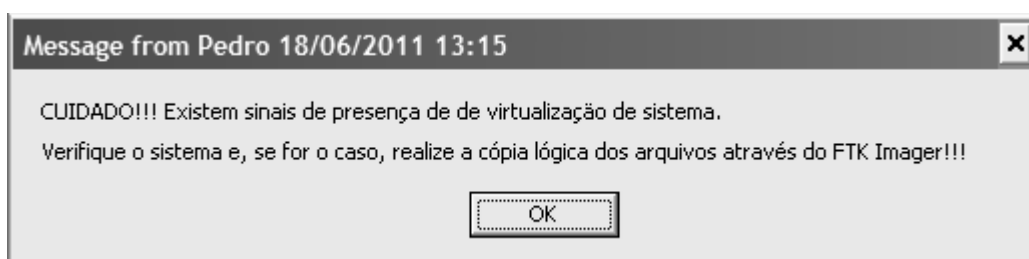


Figura 4.16: Mensagem de alerta para máquina virtual - Cenário 3.

A presença de virtualização do sistema através do programa VirtualBox pode ser evidenciada pela análise do arquivo “Processo.txt”, resultante da execução da ferramenta “pslist”, cujo conteúdo é apresentado na Figura 4.17. Alí é possível verificar os processos “VBoxService” e “VBoxTray”. Neste mesmo arquivo também é possível verificar a presença do processo “TrueCrypt”, comprovando a presença de criptografia.

#### 4.3.1. Cenário 4

A máquina utilizada está descrita na Tabela 4.6.

Tabela 4.6: Descrição da máquina utilizada no Cenário 4.

Tipo de máquina	Virtual - VirtualBox versão 4.08 r71778
Processador da máquina hospedeira	Intel(R) Core(TM)2 Duo CPU T7500
Sistema operacional da máquina hospedeira	Ubuntu 10.04, 32 bit, Kernel Linux 2.6.32-32-generic
Memória Física da máquina hospedeira	3048 MB

Sistema operacional da máquina virtual	Microsoft Windows XP Professional, Service Pack 3
Memória Física da máquina virtual	1024 MB
Programa de criptografia	Ausente
Programa antivírus	AVG <i>Free</i>
Tempo de coleta	14min08s

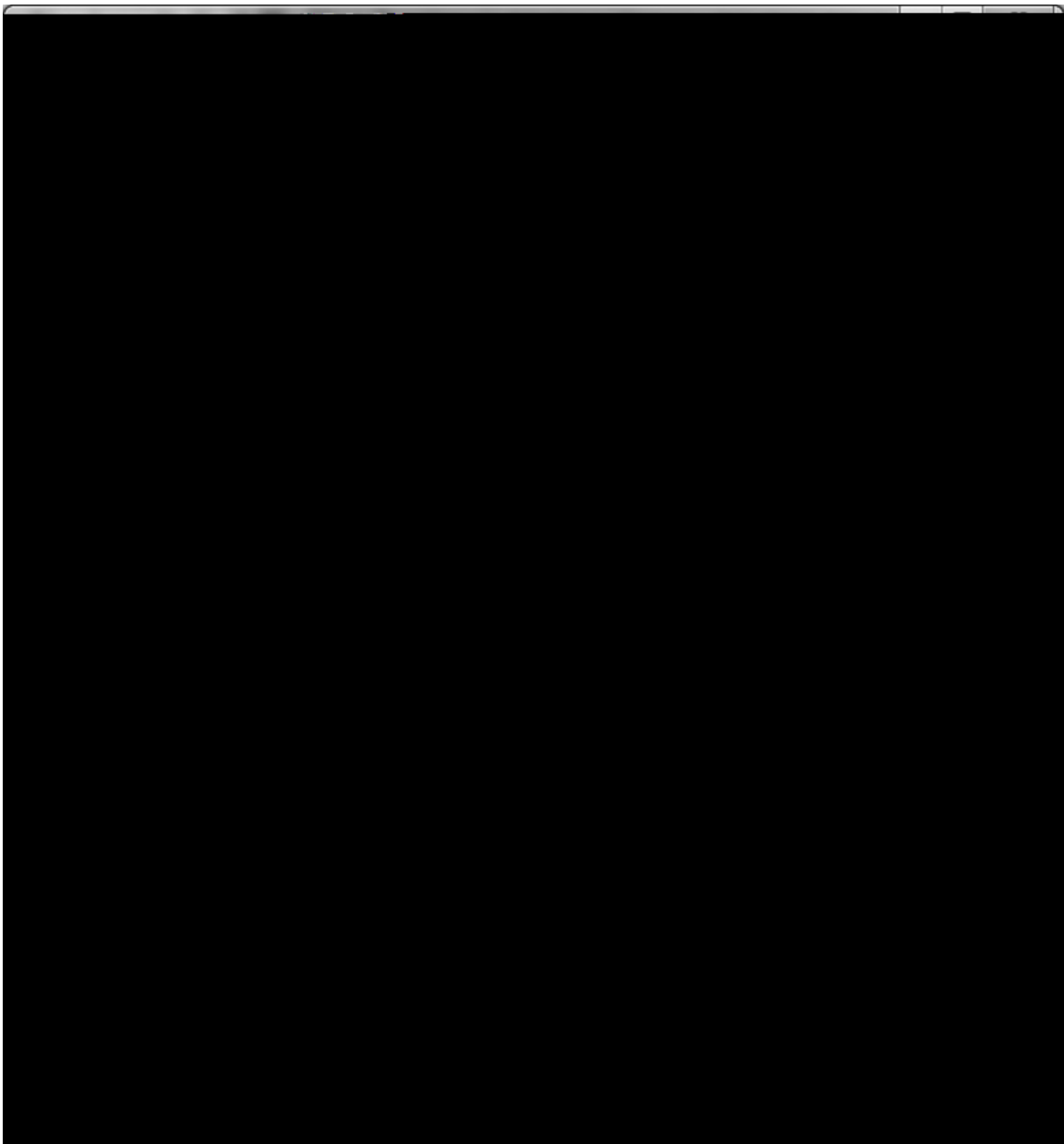


Figura 4.17: Conteúdo do arquivo "Processos.txt" – Cenário 3.

#### 4.3.1.1. Resultados obtidos:

Esta coleta ocorreu de forma semelhante àquela do Cenário 2, onde o programa antivírus identificou algumas ferramentas como ameaças. A Figura 4.18 apresenta os arquivos coletados. Neste caso, o programa antivírus é o AVG Free, que identificou como nocivas as ferramentas “passwordfox”, “iepv”, “chromepass”, “mypass” e “mailpv”, conforme Figura 4.19. Da mesma forma, a coleta continuou até o final, com prejuízo apenas das informações que seriam coletadas pelas ferramentas bloqueadas.

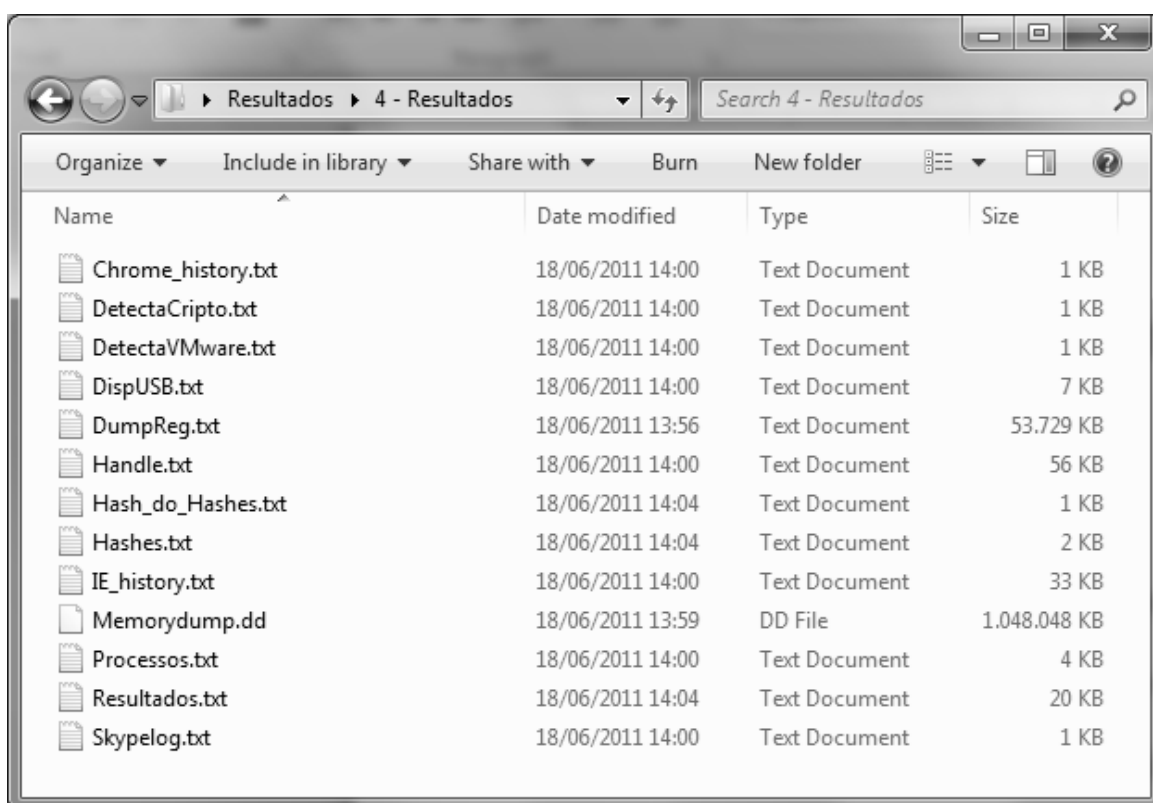


Figura 4.18: Arquivos coletados - Cenário 4.

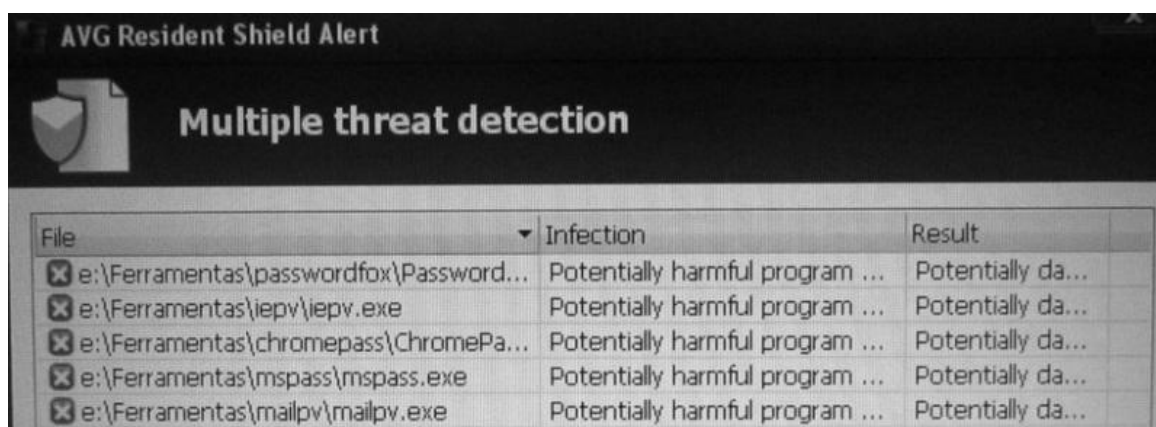


Figura 4.19: Ferramentas identificadas como ameaças pelo antivírus.

A presença de virtualização de sistema pelo programa VirtualBox foi identificado, da mesma forma já discutida e ilustrada no Cenário 3, através do alerta gerado na tela do computador analisado e do exame do conteúdo do arquivo “Processos.txt”. Após a confirmação da suspeita de virtualização, deve ser executada cópia lógica de todo o conteúdo do sistema.

#### 4.3.2. Cenário 5

A máquina utilizada está descrita na Tabela 4.7.

Tabela 4.7: Descrição da máquina utilizada no Cenário 5.

Tipo de máquina	Virtual - VMware versão 7.1.4
Processador da máquina hospedeira	Intel(R) Core(TM)2 Duo CPU T7500
Sistema operacional da máquina hospedeira	Windows 7 Professional, 64 bit, Service Pack 1
Memória Física da máquina hospedeira	3048 MB
Sistema operacional da máquina virtual	Microsoft Windows XP Professional, Service Pack 3
Memória Física da máquina virtual	1280 MB
Programa de criptografia	Truecrypt versão 7.0a – modo volume
Programa antivírus	Inativo
Tempo de coleta	11min59s

##### 4.3.2.1. Resultados obtidos:

A Figura 4.20 apresenta os arquivos coletados.

O volume criptografado pelo programa “Truecrypt” foi identificado, de forma semelhante àquela já discutida e ilustrada nos Cenário 1 e 3, através dos arquivos “DetectaCripto.txt” e “Processos.txt”. Ao ser encontrado o volume criptografado, deve ser executada a cópia lógica dos arquivos ali presentes.

O detalhe diferente neste caso se refere à presença de virtualização pelo programa VMware, que, ao ser detectado pela ferramenta “ScoopyNG”, o protótipo proposto envia um alerta para a tela do computador em análise. Além disso, pode ser verificado o arquivo

“DetectaVMware.txt”, gerado pela ferramenta citada, presente na pasta “Resultados”, que confirmará a suspeita, conforme Figura 4.21.

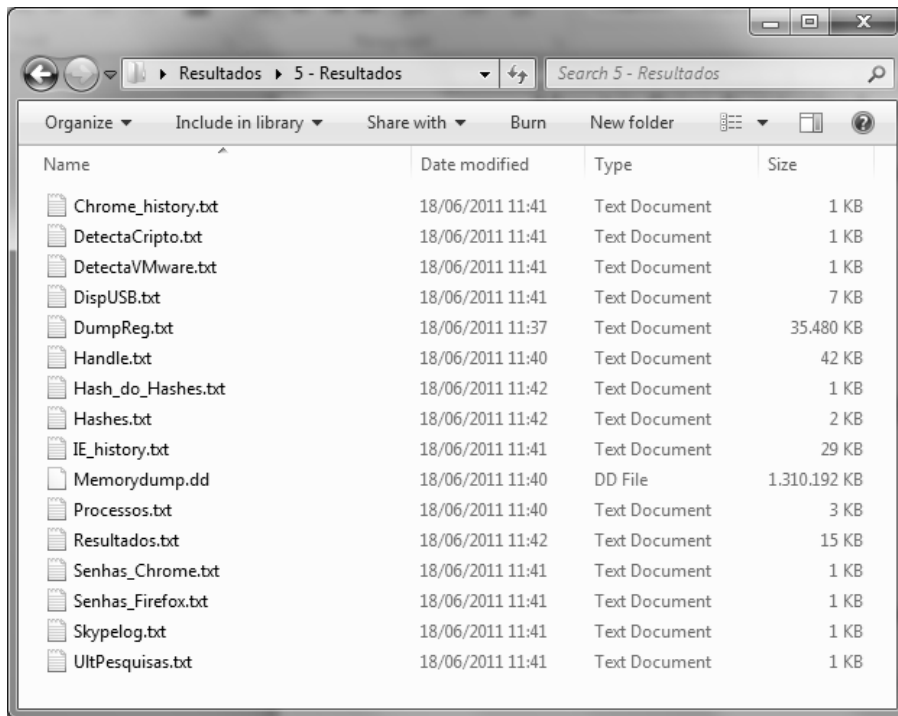


Figura 4.20: Arquivos coletados - Cenário 5.

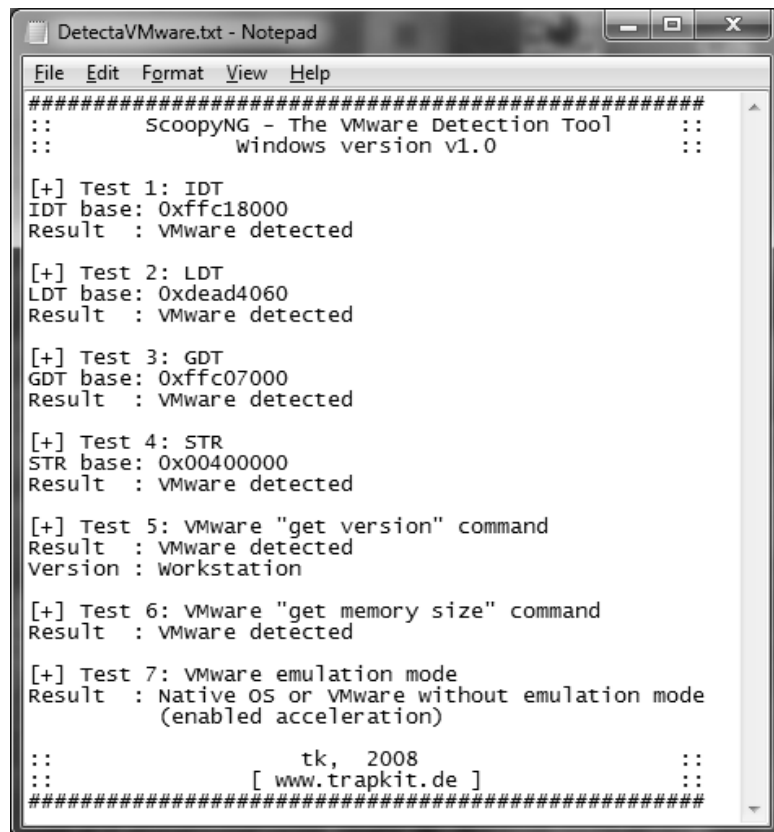


Figura 4.21: Conteúdo do arquivo “DetectaVMware.txt”.



A virtualização pode ainda ser detectada, mais uma vez, pelo exame do arquivo “Processos.txt”, conforme Figura 4.22, onde é possível encontrar os processos “VMwareTray” e “VMwareUser”. Ali também se encontra o processo “TrueCrypt”, confirmando a presença de criptografia.

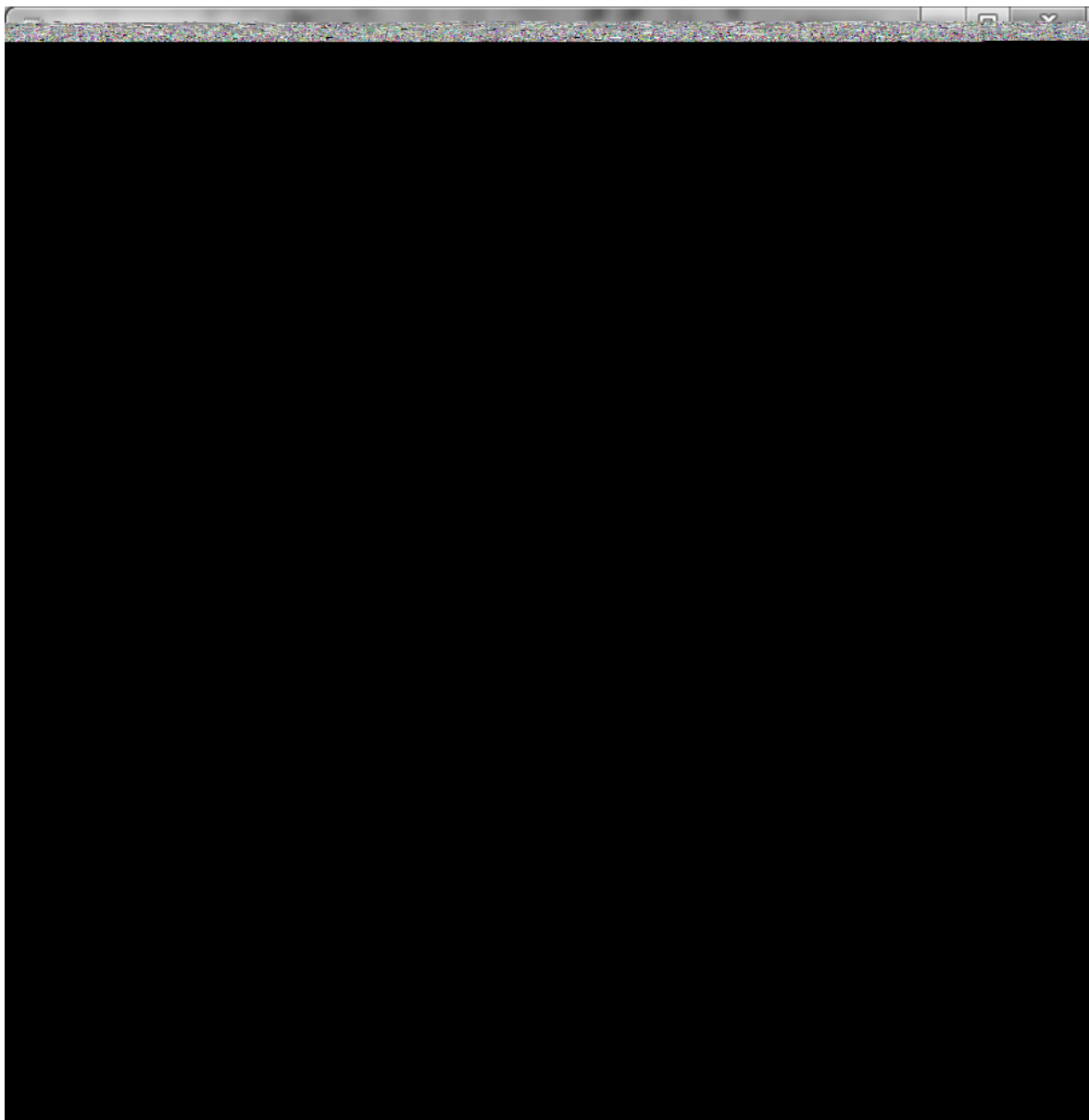


Figura 4.22: Conteúdo do arquivo "Processos.txt" – Cenário 5.

### 4.3.3. Cenário 6

A máquina utilizada está descrita na Tabela 4.8.

Tabela 4.8: Descrição da máquina utilizada no Cenário 6.

Tipo de máquina	Virtual - VMware versão 7.1.4
Processador da máquina hospedeira	Intel(R) Core(TM)2 Duo CPU T7500
Sistema operacional da máquina hospedeira	Windows 7 Professional, 64 bit, Service Pack 1
Memória Física da máquina hospedeira	3048 MB
Sistema operacional da máquina virtual	Microsoft Windows XP Professional, Service Pack 3
Memória Física da máquina virtual	1280 MB
Programa de criptografia	Inativo
Programa antivírus	AVG Free
Tempo de coleta	12min02s

#### 4.3.3.1. Resultados obtidos:

A Figura 4.23 apresenta os arquivos coletados.

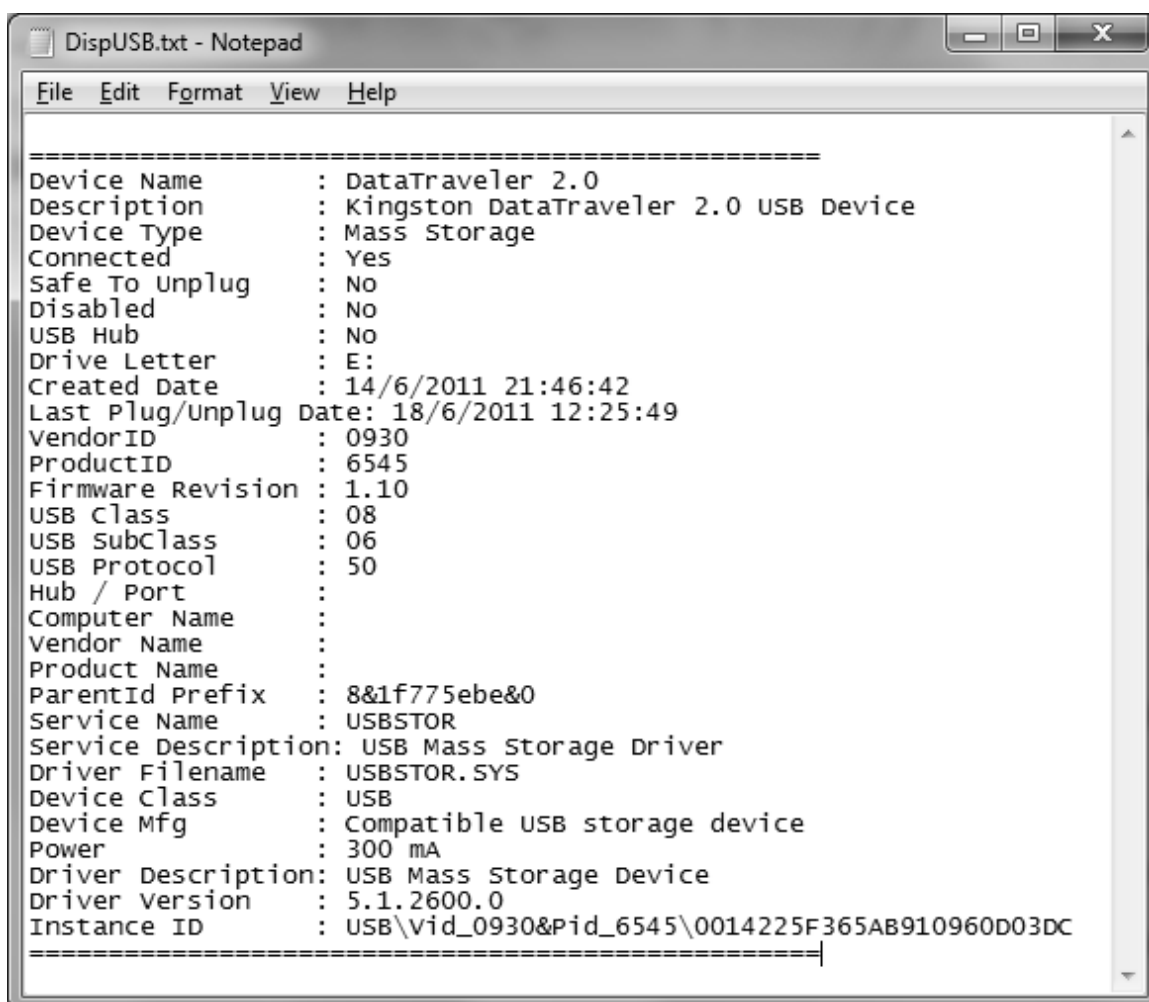


Figura 4.23: Arquivos coletados – Cenário 6.

Trata-se de uma máquina virtual “VMware”, corretamente detectada pela ferramenta “ScoopNG”, conforme discutido e ilustrado no Cenário 5. Da mesma forma é gerado um alerta na tela e a detecção pode ser confirmada pela análise dos arquivos “DetectaWMware.txt” e “Processos.txt”. Deve ser executada a cópia lógica de todo o sistema.

Em relação ao antivírus, a coleta se comporta da mesma forma ao já discutido no Cenário 4, já que em ambos os casos estava sendo executado o mesmo programa antivírus (AVG Free).

A figura 4.24 apresenta, a título de exemplo, conteúdo parcial do arquivo “DispUSB.txt”, apresentando informações relacionadas a dispositivos USB conectados ao sistema.



```
-----
Device Name       : DataTraveler 2.0
Description       : Kingston DataTraveler 2.0 USB Device
Device Type       : Mass Storage
Connected         : Yes
Safe To Unplug   : No
Disabled          : No
USB Hub           : No
Drive Letter      : E:
Created Date      : 14/6/2011 21:46:42
Last Plug/unplug Date: 18/6/2011 12:25:49
VendorID          : 0930
ProductID         : 6545
Firmware Revision : 1.10
USB Class         : 08
USB SubClass      : 06
USB Protocol      : 50
Hub / Port        :
Computer Name     :
Vendor Name       :
Product Name      :
ParentId Prefix   : 8&1f775ebe&0
Service Name      : USBSTOR
Service Description: USB Mass Storage Driver
Driver Filename   : USBSTOR.SYS
Device Class      : USB
Device Mfg        : Compatible USB storage device
Power             : 300 mA
Driver Description: USB Mass Storage Device
Driver Version    : 5.1.2600.0
Instance ID       : USB\vid_0930&pid_6545\0014225F365AB910960D03DC
-----
```

Figura 4.24: Conteúdo parcial do arquivo "DispUSB.txt".

Ao terminar de coletar todos os dados, a ferramenta de coleta emite um aviso na tela informando que o perito deve anotar o *hash* resultante, para garantir a integridade dos

dados coletados. São gerados dois arquivos relacionados, o “Hashes.txt”, que contém a relação de todos os arquivos coletados na pasta “Resultados”, com seus respectivos *hashes* SHA256, e o arquivo “Hash\_do\_Hashes.txt”, que contém o *hash* MD5 do arquivo “Hashes.txt”. Este último valor é lançado na tela (Figura 4.25) e pode também ser verificado abrindo o próprio arquivo “Hash\_do\_Hashes.txt” (Figura 4.26), encontrado na pasta “Resultados”.



Figura 4.25: Valor do *hash* a ser anotado.

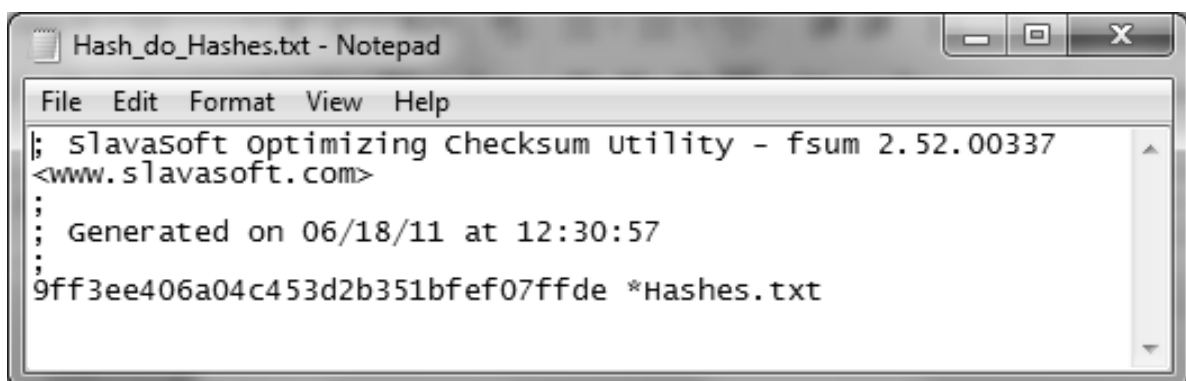


Figura 4.26: Conteúdo do arquivo "Hash\_do\_Hashes.txt".

#### 4.4. ANÁLISE DOS TESTES

A coleta de dados voláteis em sistemas operacionais baseados em Windows XP de 32 bits mostrou-se adequada, detectando corretamente a presença de criptografia e virtualização de sistema.

Apesar de o programa antivírus ter bloqueado algumas ferramentas relacionadas à captura de senhas, não houve prejuízo para a coleta como um todo, que não foi interrompida em momento algum, seguindo até o final.

O tempo de coleta variou de um tempo mínimo de 5min54s no Cenário 1 e um tempo máximo de 14min08s no Cenário 4. Por se tratar de coletas em condições diferenciadas de processador, quantidade de memória física, máquina real ou virtual, e outros fatores, a inclusão dos tempos de coleta tem apenas o intuito de fornecer uma idéia do tempo que uma coleta real pode levar.

## 5. CONCLUSÃO

Devido às limitações da coleta tradicional de dados em sistemas desligados, a aquisição com o computador ainda ligado parece ser uma alternativa de vital importância. Esta técnica permite a recuperação de relevantes informações que de outra maneira poderiam ser perdidas.

Para a captura de dados voláteis podem ser utilizadas soluções desenvolvidas por terceiros, trazendo as limitações de custo de aquisição e dificuldades de atualização e adaptação às necessidades da perícia. As soluções disponíveis capturam uma grande quantidade de informações, nem sempre necessárias ao caso concreto, trazendo assim uma invasão adicional desnecessária ao sistema analisado.

O perito pode criar seu próprio conjunto de ferramentas de captura de dados voláteis, todas disponíveis gratuitamente na Internet, integrando e automatizando-as através de um arquivo *batch*. As vantagens desta solução são a ausência de custo de aquisição, a facilidade na atualização das ferramentas, a rápida adaptação às novas necessidades e a oportunidade de coletar somente as informações julgadas essenciais para o caso concreto em análise. Além disso, pode incluir alguns testes para detecção de criptografia ou máquina virtual, coadjuvantes na tomada de decisão durante a apreensão, que deve ser rápida e precisa, com o mínimo possível de alteração do sistema alvo.

Conclui-se assim que o procedimento de busca e apreensão de itens relacionados a sistemas informatizados deve incluir as abordagens:

- Coleta dos dados voláteis quando possível (computador ligado, desbloqueado, senha conhecida, etc.);
- Cópia lógica de dados quando for detectada a presença de criptografia ou máquina virtual;
- Apreensão física dos equipamentos para análise tradicional em laboratório:
  - Após desligamento do sistema, posteriormente à coleta de dados voláteis;
  - Quando o computador for encontrado desligado.

O desenvolvimento deste trabalho proporcionou a oportunidade de colaboração com o estado da arte no assunto, através da submissão de artigos científicos em Simpósios

especializados em computação forense. Assim, foram aceitos para publicação o artigo “Uma Nova Abordagem em Apreensão de Computadores” na 6ª ICoFCS (2011) – *International Conference on Forensic Computer Science* (AULER, *et al.*, 2011) e o capítulo de livro “*Live Forensics* em ambiente Microsoft Windows” no minicurso do 11º SBSeg (2011) – Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (HOELZ, MESQUITA e AULER, 2011).

Em trabalho futuros é possível e recomendável adicionar outras funcionalidades ao CADAV, tornando sua aplicação mais completa e abrangente. Dentre elas, podem se destacar as seguintes:

- Reconhecimento automático do sistema operacional e da versão correspondente;
- Conjunto de comandos e ferramentas apropriados e específicos para cada versão de sistema operacional reconhecido;
- Mecanismo de escolha das ferramentas a serem utilizadas em cada caso, pelo perito, em momento anterior ao da apreensão;
- Mecanismo facilitador de atualização das ferramentas;
- Aprimoramento dos testes de auxílio à decisão durante o procedimento de captura de dados;
- Incorporação de solução para tratamento de computação em nuvem;
- Detecção automática do antivírus executado, com desligamento do mesmo, antes do início da coleta de dados.

## REFERÊNCIAS BIBLIOGRÁFICAS

- ACCESSDATA. FTK Imager User Guide, 2011. Disponível em:  
<[http://accessdata.com/downloads/current\\_releases/imager/FTKImager\\_UserGuide.pdf](http://accessdata.com/downloads/current_releases/imager/FTKImager_UserGuide.pdf)>.  
Acesso em: 02 abr. 2011.
- AGILE RISK MANAGEMENT LLC. Nigilant32, 2011. Disponível em:  
<<http://www.agileriskmanagement.com/download.html>>. Acesso em: 11 jun. 2011.
- AKKAN, H. Digital Forensics - Tools for Live Data Collection, 2006. Disponível em:  
<<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.114.5329&rep=rep1&type=pdf>>.  
>. Acesso em: 30 abr. 2011.
- AULER, P. Captura de Dados em Sistemas Windows em Execução: Ferramentas e Técnicas. Brasília: Universidade Católica de Brasília (Monografia - Pós-graduação em Perícia Digital), 2009.
- AULER, P. et al. Uma Nova Abordagem em Apreensão de Computadores. 6ª ICoFCS (2011) – International Conference on Forensic Computer Science. Florianópolis: [s.n.]. 2011.
- AVG. AVG Anti-virus Free, 2011. Disponível em:  
<<http://www.avgbrasil.com.br/landings/download-free/>>. Acesso em: 02 jun. 2011.
- BRASIL. Decreto-Lei n. 2848, de 7 de dezembro de 1940, 1940. Acesso em: 12 out. 2011.
- BRASIL. Decreto-Lei n. 3.689, de 3 de outubro de 1941, 1941. Disponível em:  
<[http://www.planalto.gov.br/ccivil\\_03/Decreto-Lei/Del3689.htm](http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689.htm)>. Acesso em: 12 out. 2011.
- BRASIL. Instrução Normativa n. 11, de 27 de junho de 2001, da Direção-Geral do Departamento de Polícia Federal, 2001. Disponível em:  
<<http://www.in.gov.br/imprensa/visualiza/index.jsp?jornal=1&pagina=232&data=02/07/2001>>. Acesso em: 12 out. 2011.
- BREZINSKI, D.; KILLALEA, T. Guidelines for Evidence Collection and Archiving, 2002. Disponível em: <<http://www.faqs.org/rfcs/rfc3227.html>>. Acesso em: 16 jun. 2011.
- CARRIER, B. Open Source Digital Forensics Tools - The Legal Argument, 2011. Disponível em: <[http://www.digital-evidence.org/papers/opensrc\\_legal.pdf](http://www.digital-evidence.org/papers/opensrc_legal.pdf)>. Acesso em: 28 mai. 2011.
- CARVEY, H. Windows Forensics Analysis. Burlington: Syngress Publishing, Inc., 2007.
- E-FENSE. Helix, 2011. Disponível em: <<http://www.e-fense.com/index.php>>. Acesso em: 11 jun. 2011.
- FERGUSON, N.; SCHNEIER, B. Practical Cryptography. Indianapolis: Willey Publishing, Inc., 2003.



FOOL MOON SOFTWARE & SECURITY. Windows Forensic Toolchest (WFT), 2011. Disponível em: <<http://www.foolmoon.net/security/wft/>>. Acesso em: 06 nov. 2011.

FREE SOFTWARE FOUNDATION, INC. GNU GENERAL PUBLIC LICENSE, 2007. Disponível em: <<http://www.gnu.org/licenses/gpl.html>>. Acesso em: 17 jun. 2011.

GROBLER, M. M.; VON SOLMONS, S. H. A Best Practice Approach To Live Forensic Acquisition, 2010. Disponível em: <<http://hdl.handle.net/10204/3509>>. Acesso em: 09 ago. 2010.

HOELZ, B. W.; MESQUITA, F. I.; AULER, P. Live Forensics em Ambiente Microsoft Windows. 11º SBSeg – Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. Brasília: [s.n.]. 2011.

HOELZ, B. W.; RUBACK, M. C.; SILVA, J. H. Informática Forense. Brasília: Academia Nacional de Polícia (Caderno Didático), 2009.

IEONG, R. Freeware Live Forensics tools evaluation and operation tips, 2011. Disponível em: <<http://scissec.scis.ecu.edu.au/proceedings/2006/forensics/Ieong%20-%20Freeware%20Live%20Forensics%20tools%20evaluation%20and%20operation%20tips.pdf>>. Acesso em: 09 abr. 2011.

JADSOFTWARE. Encrypted Disk Detector, 2011. Disponível em: <[http://www.jadsoftware.com/go/?page\\_id=167](http://www.jadsoftware.com/go/?page_id=167)>. Acesso em: 16 jul. 2011.

LESSING, M.; VON SOLMONS, B. Live Forensic Acquisition as Alternative to Traditional Forensic Processes, 2011. Disponível em: <<http://www.pdfio.com/k-52494.html#>>. Acesso em: 09 mai. 2011.

LIBSTER, E.; KORNBLUM, J. D. A Proposal for an Integrated Memory Acquisition Mechanism, 2011. Disponível em: <[http://delivery.acm.org/10.1145/1370000/1368510/p14-libster.pdf?ip=164.41.100.240&CFID=25987712&CFTOKEN=66491704&\\_\\_acm\\_\\_=1306592372\\_aa92bf3fa0d9054711773546196fa317](http://delivery.acm.org/10.1145/1370000/1368510/p14-libster.pdf?ip=164.41.100.240&CFID=25987712&CFTOKEN=66491704&__acm__=1306592372_aa92bf3fa0d9054711773546196fa317)>. Acesso em: 28 mai 2011.

LIFEHACKER, 2011. Disponível em: <<http://translate.google.com.br/translate?hl=pt-BR&langpair=en%7Cpt&u=http://lifehacker.com/5714966/five-best-virtual-machine-applications>>. Acesso em: 11 nov. 2011.

LINFO. Rootkit Definition, 2011. Disponível em: <<http://www.linfo.org/rootkit.html>>. Acesso em: 17 jun. 2011.

LOPES, M.; GABRIEL, M. M.; BARETA, G. M. Cadeia de Custódia: Uma Abordagem Preliminar, 2006. Disponível em: <<http://ojs.c3sl.ufpr.br/ojs2/index.php/academica/article/download/9022/6315>>. Acesso em: 16 jun. 2011.

LOWMAN, S. The Effect of File and Disk Encryption on Computer Forensics, 2010. Disponível em: <<http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf>>. Acesso em: 30 abr. 2011.

MACHADO, F. B.; MAIA, L. P. Introdução à arquitetura de sistemas operacionais. Rio de Janeiro: Editores, LTC - Livros Técnicos e Científicos, 1992.

MANDIA, K.; PROSISE, C.; PEPE, M. Incident Response & Computer Forensics. 2nd. ed. Emeryville: McGraw-Hill/Osborne, 2003.

MANTECH. ManTech Memory DD, 2011. Disponível em:  
<<http://www.mantech.com/capabilities/mdd.asp>>. Acesso em: 31 mar. 2011.

MCDOUGAL, M. What Is New With Windows Forensic Toolchest™ (WFT) v3.0, 2007. Disponível em:  
<[http://www.foolmoon.net/downloads/SANSfire\\_2007\\_WFT\\_3.0\\_BOF.pdf](http://www.foolmoon.net/downloads/SANSfire_2007_WFT_3.0_BOF.pdf)>. Acesso em: 06 nov. 2011.

MEDEIROS, C. Segurança da Informação, 2011. Disponível em:  
<[http://www.ivanfm.com/files/docs/TCE\\_Seguranca\\_da\\_Informacao.pdf](http://www.ivanfm.com/files/docs/TCE_Seguranca_da_Informacao.pdf)>. Acesso em: 10 set. 2011.

MICROSOFT. User Guide for COFEE v1.0, 2007.

MICROSOFT. User Guide for COFEE v1.1.2, 2009.

MICROSOFT. Windows Sysinternals Suite, 2011a. Disponível em:  
<<http://technet.microsoft.com/en-us/sysinternals/bb842062>>. Acesso em: 30 mar. 2011.

MICROSOFT. Command-line reference A-Z, 2011b. Disponível em:  
<<http://technet.microsoft.com/en-us/library/bb490890.aspx>>. Acesso em: 04 abr. 2011.

MICROSOFT. BitLocker, 2011c. Disponível em: <<http://windows.microsoft.com/pt-BR/windows7/products/features/bitlocker>>. Acesso em: 18 jul. 2011.

MICROSOFT. Microsoft Security Essentials, 2011d. Disponível em:  
<<http://windows.microsoft.com/pt-BR/windows/products/security-essentials>>. Acesso em: 02 jun. 2011.

MOCKRIDGE, T. Unix Commands ported to Windows, 2011. Disponível em:  
<<http://mysite.mweb.co.za/residents/thomas/unix-cmds/default.htm>>. Acesso em: 07 mai. 2011.

MONTEIRO, M. A. Introdução à Organização de Computadores. 2ª. ed. Rio de Janeiro: S.A., LTC- Livros Técnicos e Científicos Editora, 1995. ISBN 2ª.

NATIONAL WHITE COLLAR CRIME CENTER, 2011. Disponível em:  
<<http://www.nw3c.org/>>. Acesso em: 09 abr. 2011.

NETMARKETSHARE, 2011a. Disponível em:  
<<http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=0>>. Acesso em: 09 set. 2011.

NETMARKETSHARE, 2011b. Disponível em:  
<<http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0>>. Acesso em: 09 set. 2011.

- NETMARKETSHARE, 2011c. Disponivel em:  
<<http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=11&qpcustomb=0>>. Acesso em: 09 set. 2011.
- NIRSOFT, 2011a. Disponivel em: <<http://www.nirsoft.net/>>. Acesso em: 09 set. 2011.
- NIRSOFT. Other Utilities, 2011b. Disponivel em:  
<[http://www.nirsoft.net/utills/index.html#other\\_utills](http://www.nirsoft.net/utills/index.html#other_utills)>. Acesso em: 30 mar. 2011.
- NIRSOFT. Password Recovery Utilities, 2011c. Disponivel em:  
<[http://www.nirsoft.net/utills/index.html#password\\_utills](http://www.nirsoft.net/utills/index.html#password_utills)>. Acesso em: 28 mai. 2011.
- NIRSOFT. System Utilities, 2011d. Disponivel em:  
<[http://www.nirsoft.net/utills/index.html#system\\_utills](http://www.nirsoft.net/utills/index.html#system_utills)>. Acesso em: 28 mai. 2011.
- NIRSOFT. Web Browser Tools, 2011e. Disponivel em:  
<[http://www.nirsoft.net/utills/index.html#browser\\_tools](http://www.nirsoft.net/utills/index.html#browser_tools)>. Acesso em: 28 mai. 2011.
- O'BRIEN, S. Digital Forensic Photography Update - Appropriate Techniques for Law Enforcement, 2011. Disponivel em:  
<[http://www.iowaiai.org/digital\\_forensic\\_phototgraphy\\_update.html](http://www.iowaiai.org/digital_forensic_phototgraphy_update.html)>. Acesso em: 21 mai. 2011.
- OKOLICA, J.; PETERSON, G. L. Windows operating systems agnostic memory analysis, 2010. Disponivel em: <<http://www.dfrws.org/2010/proceedings/2010-306.pdf>>. Acesso em: 30 abr. 2011.
- PETRONI JR., N. L. et al. A Framework for the Extraction and Analysis of Digital Forensic Data from Volatile System Memory, 2011. Disponivel em:  
<[http://www.google.com.br/url?sa=t&source=web&cd=4&ved=0CDYQFjAD&url=http%3A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownload%3Fdoi%3D10.1.1.102.2189%26rep%3Drep1%26type%3Dpdf&ei=jmG8TdxmpbrRAaqHwMAF&usg=AFQjCNHeB9Pl-dZ\\_9Q21e4WpahCeOTTkgA](http://www.google.com.br/url?sa=t&source=web&cd=4&ved=0CDYQFjAD&url=http%3A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownload%3Fdoi%3D10.1.1.102.2189%26rep%3Drep1%26type%3Dpdf&ei=jmG8TdxmpbrRAaqHwMAF&usg=AFQjCNHeB9Pl-dZ_9Q21e4WpahCeOTTkgA)>. Acesso em: 30 abr. 2011.
- RICHARD III, G. G.; ROUSSEV, V. Next-Generation Digital Forensics, 2010. Disponivel em: <<http://delivery.acm.org/10.1145/1120000/1113074/p76-richard.pdf?key1=1113074&key2=9086641821&coll=GUIDE&dl=GUIDE&CFID=10011939&CFTOKEN=81363570>>. Acesso em: 10 ago. 2010.
- RUFF, N. Windows memory forensics, 2008. Disponivel em:  
<<http://www.springerlink.com/content/h336r32ju3032v61/fulltext.pdf>>. Acesso em: 16 abr. 2011.
- SCHATZ, B. BodySnatcher: Towards reliable volatile memory acquisition by software, 2011. Disponivel em: <<http://www.dfrws.org/2007/proceedings/p126-schatz.pdf>>. Acesso em: 30 abr. 2011.
- SECURE STAR. DriveCrypt, 2011. Disponivel em:  
<[http://www.securstar.com/products\\_drivecrypt.php](http://www.securstar.com/products_drivecrypt.php)>. Acesso em: 18 jul. 2011.

SHANNON, M. M. Nigilant32 for Active Memory Management, 2011. Disponível em: <<http://www.agileriskmanagement.com/pdfs/Nigilant32forFirstResponders-ActiveMemoryImaging.pdf>>. Acesso em: 11 jun. 2011.

SHIPLEY, T. G.; REEVE, H. R. Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community, 2011. Disponível em: <<http://www.search.org/files/pdf/CollectEvidenceRunComputer.pdf>>. Acesso em: 11 abr. 2011.

SHIPLEY, T. G.; REEVE, H. R. Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community, 2011. Disponível em: <<http://www.search.org/files/pdf/CollectEvidenceRunComputer.pdf>>. Acesso em: 11 abr. 2011.

SLAVASOFT. Fast File Integrity Checker, 2011. Disponível em: <<http://www.slavasoft.com/fsum/>>. Acesso em: 12 mai. 2011.

SLEUTHKIT.ORG. The Sleuth Kit (TSK), 2011. Disponível em: <<http://www.sleuthkit.org/sleuthkit/>>. Acesso em: 12 set 2011.

SOUSA, R.; PUTTINI, R. Princípios Básicos, 2011. Disponível em: <<http://webserver.redes.unb.br/security/introducao/aspectos.html>>. Acesso em: 10 set. 2011.

STACY JR., H.; LUNSFORD, P. Computer Forensics For Law Enforcement, 2011. Disponível em: <[http://www.infosecwriters.com/text\\_resources/pdf/Forensics\\_HStacy.pdf](http://www.infosecwriters.com/text_resources/pdf/Forensics_HStacy.pdf)>. Acesso em: 28 mai. 2011.

STALLINGS, W. Criptografia e Segurança de Redes - Princípios e Práticas. 4ª. ed. São Paulo: Hall, Pearson Prentice, 2008.

STEEL, C. Windows Forensics: The Field Guide for Conducting Corporate Computer Investigations. Indianapolis: Wiley Publishing, Inc., 2006.

SUTHERLAND, I. et al. Acquiring Volatile Operating System Data Tools and Techniques, 2010. Disponível em: <<http://doi.acm.org/10.1145/1368506.1368516>>. Acesso em: 09 ago. 2010.

SYMANTECH. PGP, 2011. Disponível em: <<http://www.symantec.com/business/theme.jsp?themeid=pgp>>. Acesso em: 18 jul. 2011.

TANEMBAUM, A. S. Sistemas Operacionais Modernos. 3ª. ed. São Paulo: Hall, Pearson Prentice, 2009.

TECHTERMS.COM. Malware, 2011. Disponível em: <<http://www.techterms.com/definition/malware>>. Acesso em: 17 jun. 2011.

TRAPKIT. ScoopyNG - The VMware detection tool, 2011. Disponível em: <<http://www.trapkit.de/research/vmm/scoopyng/index.html>>. Acesso em: 05 mai. 2011.

TRUECRYPT, 2011. Disponível em: <<http://www.truecrypt.org/>>. Acesso em: 17 jul. 2011.

UNIXUTILS. GNU Utilities for WIN32. Disponível em: <<http://unxutils.sourceforge.net/>>. Acesso em: 30 mar. 2011.

VIRTUALBOX, 2011. Disponível em: <<http://www.virtualbox.org/wiki/VirtualBox>>. Acesso em: 17 jul. 2011.

VMWARE. Desktop & End-User Computing Solutions, 2011. Disponível em: <<http://www.vmware.com/solutions/desktop/>>. Acesso em: 17 jul. 2011.

WAITS, C. et al. Computer Forensics: Results of Live Response Inquiry vs. Memory Image Analysis., 2010. Disponível em: <<http://www.cert.org/archive/pdf/08tn017.pdf>>. Acesso em: 08 nov. 2010.

## ANEXO A – FERRAMENTAS E COMANDOS DE SISTEMA

1. Mdd\_1.3 (MANTECH, 2011). Ferramenta para coleta da memória física (RAM), disponibilizado gratuitamente para órgãos governamentais e uso privado, sob licença GPL (FREE SOFTWARE FOUNDATION, INC, 2007).

```
mdd_1.3 -o arquivo_de_saída.img
```

Figura A.1: Execução da ferramenta mdd.

2. Regedit. Editor de registros do Windows que possibilita a realização de cópia de registros.

```
regedit /e arquivo_de_saída.txt
```

Figura A.2: Execução do comando regedit.

3. Outros comandos de sistema do Windows:

```
date /t > arquivo_de_saída.txt
```

Figura A.3.1: Data do sistema.

```
time /t > arquivo_de_saída.txt
```

Figura A.3.2: Hora do sistema.

```
tasklist > arquivo_de_saída.txt
```

Figura A.3.3: Lista de arquivos recentemente abertos.

```
dir "%UserProfile%\Recent" > arquivo_de_saída.txt
```

Figura A.3.4: Usuário que já logaram na máquina.

```
netstat -ano > arquivo_de_saída.txt
```

Figura A.3.5: Informações sobre conexões de rede.

```
ipconfig /all > arquivo_de_saída.txt
```

Figura A.3.6: Informações sobre as interfaces de rede.

```
doskey /history > arquivo_de_saída.txt
```

Figura A.3.7: Comandos recentemente utilizados.

4. Handle v3.45 (MICROSOFT, 2011a). Utilitário que apresenta a relação de processos com arquivos e pastas abertos. Pode ser executado em sistemas Windows XP ou mais recentes. Necessita ser executado por usuário com poderes de administrador do sistema.

```
handle -accepteula > arquivo_de_saída.txt
```

Figura A.4: Execução da ferramenta handle.

5. ListDLLs v3.0 (MICROSOFT, 2011a). Este utilitário relaciona as DLLs carregadas no sistema. Pode ser executado em sistemas Windows XP ou mais recentes, retornando o nome completo dos módulos carregados. Além disso, ele as sinaliza as DLLs que apresentam número de versão diferente dos seus arquivos correspondentes gravados em disco (isto ocorre quando um arquivo é atualizado depois do programa carregar suas DLLs), podendo ainda informar quais DLLs foram realocadas.

```
listdlls > arquivo_de_saída.txt
```

Figura A.5: Execução da ferramenta listdlls.

6. PsFile v1.02 (MICROSOFT, 2011a). Este utilitário de linha de comando mostra os arquivos que foram abertos remotamente. Pode ser executado em sistemas Windows XP ou mais recentes.

```
psfile -accepteula > arquivo_de_saída.txt
```

Figura A.6: Execução da ferramenta psfile.

7. PsInfo v1.77 (MICROSOFT, 2011a). Ferramenta de linha de comando que retorna informações importantes sobre o sistema, incluindo tipo de instalação, usuário registrado, organização, número e tipo de processador, quantidade de

memória física, data de instalação do sistema, entre outras. Pode ser executado em sistemas Windows XP ou mais recentes.

```
psinfo -accepteula > arquivo_de_saída.txt
```

Figura A.7: Execução da ferramenta psinfo.

8. PsList v1.29 (MICROSOFT, 2011a). Ferramenta de linha de comando que lista os processos em execução. Pode ser executado em sistemas Windows XP ou mais recentes.

```
pslist -accepteula > arquivo_de_saída.txt
```

Figura A.8: Execução da ferramenta pslist.

9. PsLoggedOn v1.34 (MICROSOFT, 2011a). Este utilitário permite determinar quem está utilizando ativamente o sistema, seja localmente ou remotamente. Pode ser executado em sistemas Windows XP ou mais recentes.

```
Psloggedon -accepteula > arquivo_de_saída.txt
```

Figura A.9: Execução da ferramenta psloggedon.

10. Strings v2.41 (MICROSOFT, 2011a). Utilitário que permite pesquisa de caracteres UNICODE (ou ASCII) em arquivos.

```
strings -accepteula arquivo_de_entrada > arquivo_de_saída.txt
```

Figura A.10: Execução da ferramenta strings.

11. Grep (UNIXUTILS). Este é um aplicativo de linha de comando proveniente de sistemas Unix/Linux, capaz de fazer buscas no conteúdo de arquivos ou saídas de outros comandos executados, estando também disponível para ambiente Windows. Exemplos de utilização: `<pslist | grep -i truecrypt>` - procura a palavra “truecrypt” nos processos listados pelo comando `<pslist>`. A opção `<-i>` faz com que opções de letras maiúsculas ou minúsculas sejam ignoradas; `<grep -`



i truecrypt teste.txt> - procura a palavra “truecrypt” no arquivo teste.txt.

```
pslist | grep -i truecrypt
```

Figura A.11.1: Exemplo de execução da ferramenta grep.

(Procura a palavra “truecrypt” nos processos listados pelo comando <pslist>).

```
grep -i truecrypt teste.txt
```

Figura A.11.2: Outro exemplo de execução da ferramenta grep.

(Procura a palavra “truecrypt” no arquivo teste.txt).

12. IEHistoryView v1.61 (NIRSOFT, 2011e). Utilitário que permite visualizar as páginas acessadas através do navegador Internet Explorer.

```
iehv /stext arquivo_de_saída.txt
```

Figura A.12: Execução da ferramenta IEHistoryView.

13. MozillaHistoryView v1.35 (NIRSOFT, 2011e). Programa Utilitário que permite visualizar as páginas acessadas através de navegadores Mozilla/Firefox.

```
mozillahistoryview /stext arquivo_de_saída.txt
```

Figura A.13: Execução da ferramenta MozillaHistoryView.

14. ChromeHistoryView v1.00 (NIRSOFT, 2011e). Utilitário que permite visualizar as páginas acessadas através do navegador Google Chrome.

Quadro 0-2: Execução da ferramenta 14. ChromeHistoryView.

```
chromehistoryview /stext arquivo_de_saída.txt
```

Figura A.14: Execução da ferramenta ChromeHistoryView.

15. MyLastSearch v1.50 (NIRSOFT, 2011e). Utilitário que permite para visualizar os últimos termos pesquisados em diversos programas de busca (Google, Yahoo e MSN) e em sites de redes sociais (Twitter, Facebook, MySpace).

```
mylastsearch /stext arquivo_de_saída.txt
```

Figura A.15: Execução da ferramenta MyLastSearch.

16. SkypeLogView v1.21 (NIRSOFT, 2011b). Este utilitário acessa os arquivos de log criados pelo Skype e mostra detalhes com chamadas realizadas ou recebidas, mensagens de chat transferências de arquivos.

```
skypelogview /stext arquivo_de_saída.txt
```

Figura A.16: Execução da ferramenta SkypeLogView.

17. MessenPass v1.42 (NIRSOFT, 2011c). Utilitário que permite a recuperação de senhas do usuário atualmente ativo no sistema e somente funciona se o usuário configurar o programa para salvar as senhas utilizadas. Os programas de mensagem instantânea suportados são os seguintes: MSN Messenger, Windows Messenger (em Windows XP), Windows Live Messenger (em Windows XP/Vista/7), Yahoo Messenger (versões 5.x e 6.x), Google Talk, ICQ Lite (versões 4.x/5.x/2003), AOL Instant Messenger (versão 4.6 ou abaixo, AIM 6.x e AIM Pro), Trillian, Trillian Astra, Miranda, GAIM/Pidgin, MySpace IM, PaltalkScene e Digsby.

```
mypass /stext arquivo_de_saída.txt
```

Figura A.17: Execução da ferramenta MessenPass.

18. Mail PassView v1.73 (NIRSOFT, 2011c). Este utilitário pode ser executado em qualquer versão do Windows, desde a versão 98 até o Windows 7, e permite recuperar senhas de programas de e-mail, tais como: Outlook Express, Microsoft Outlook 2000 (POP3 e SMTP), Microsoft Outlook 2002/2003/2007/2010 (POP3, IMAP, HTTP e SMTP), Windows Mail,

Windows Live Mail, IncrediMail, Eudora, Netscape 6.x/7.x (se a senha não estiver criptografada com senha mestre), Mozilla Thunderbird (se a senha não estiver criptografada com senha mestre), Group Mail Free, Yahoo! Mail (se a senha estiver salva em alguma aplicação do Yahoo! Messenger) e Gmail (se a senha estiver salva na aplicação Gmail Notifier, Google Desktop ou Google Talk).

```
mailpv /stext arquivo_de_saída.txt
```

Figura A.18: Execução da ferramenta Mail PassView.

19. IE PassView v1.26 (NIRSOFT, 2011c). Utilitário que revela as senhas armazenadas pelo navegador Internet Explorer, suportando desde a versão 4.0 até a 9.0.

```
iepv /stext arquivo_de_saída.txt
```

Figura A.19: Execução da ferramenta IE PassView.

20. ChromePass v1.20 (NIRSOFT, 2011c). Utilitário que revela as senhas armazenadas pelo navegador Google Chrome.

```
ChromePass /stext arquivo_de_saída.txt
```

Figura A.20: Execução da ferramenta ChromePass.

21. PasswordFox v1.30 (NIRSOFT, 2011c). Utilitário que revela as senhas armazenadas pelo navegador Firefox, suportando qualquer versão do Windows 2000, XP, Server 2003, Vista, até o Windows 7.

```
passwordfox /stext arquivo_de_saída.txt
```

Figura A.21: Execução da ferramenta PasswordFox.

22. WirelessKeyView v1.35 (NIRSOFT, 2011c). Utilitário que recupera as senhas de Internet sem fio (WEP/WPA) armazenadas no computador, em sistemas

Windows XP e Vista.

```
wirelesskeyview /stext arquivo_de_saída.txt
```

Figura A.22: Execução da ferramenta WirelessKeyView.

23. USBDeview v1.89 (NIRSOFT, 2011d). Utilitário que lista os dispositivos USB conectados ao computador, bem como aqueles que estiveram conectados recentemente.

```
usbdeview /stext arquivo_de_saída.txt
```

Figura A.23: Execução da ferramenta USBDeview.

24. Encrypted Disk Detector (EDD) 1.2.0 (JADSOFTWARE, 2011). Ferramenta de linha de comando que verifica a presença de volumes criptografados pelos programas TrueCrypt, PGP, Safeboot (*McAfee® Endpoint Encryption*) e Bitlocker. O programa foi testado pelo desenvolvedor em sistemas Windows XP, Vista e 7 (32 e 64 bits), necessitando de apenas 40 KB de espaço em disco e aproximadamente 3 MB de memória. Atualmente, o programa é disponibilizado gratuitamente na Internet.

```
edd120.exe /batch arquivo_de_saída.txt
```

Figura A.24: Execução da ferramenta Encrypted Disk Detector (EDD).

25. ScoopyNG v1.0 (TRAPKIT, 2011). Este utilitário combina as técnicas de outras duas ferramentas mais antigas - *ScoobyDoo* e *Jerry*, e incorpora algumas novas técnicas para determinar se o sistema operacional corrente está sendo executado dentro de uma máquina virtual *VMware* ou em um sistema nativo. O aplicativo funciona em qualquer CPU moderna, independente do número de processadores utilizados. Além disso, é capaz de detectar a presença do *VMware* mesmo quando utilizados mecanismos anti-deteção.

```
scoopyng > arquivo_de_saída.txt
```

Figura A.25: Execução da ferramenta ScoopyNG.

26. PCLIP (MOCKRIDGE, 2011). Copia o conteúdo da área de transferência.

```
pclip > arquivo_de_saída.txt
```

Figura A.26: Execução da ferramenta PCLIP.

27. FSUM v2.52 (SLAVASOFT, 2011). Utilitário de linha de comando para verificar a integridade de arquivos. Permite a escolha entre várias funções de *hash*.

```
fsum -d".\Resultados" -r -sha256 * > Hashes.txt
```

Figura A.27.1: Exemplo de execução da ferramenta FSUM.

(Onde a ferramenta é executada sobre a pasta “Resultados”, de forma recursiva (-r) e o arquivo de saída é o “Hashes.txt”).

```
fsum -d"." Hashes.txt > Hash_do_Hashes.txt
```

Figura A.27.2: Outro exemplo de execução da ferramenta FSUM.

(Onde a ferramenta calcula o *hash* do arquivo “Hashes.txt”, salvando o resultado no arquivo “Hash\_do\_Hashes.txt”).

O Windows disponibiliza algumas ferramentas de linha de comando no próprio sistema, e podem ser executadas a partir de um *prompt* de comandos cmd (MICROSOFT, 2011b). Estas ferramentas podem ser utilizadas para diagnosticar e resolver problemas do computador, além de servirem para coletar alguns dados de interesse para a investigação. Alguns comandos úteis aos procedimentos de coleta de dados são, por exemplo: *cmd*, *time*, *date*, *echo*, *ipconfig*, *set* e *tasklist*. Parte destas ferramentas exige privilégios de administrador do sistema para ser executada. Os comandos precisam ser executados em um *prompt* de comando do interpretador de comandos Cmd.exe. Para iniciar o *Prompt* de

Comando basta clicar em Iniciar, depois em Executar, digitar cmd e após clicar em OK. Para a coleta de dados, não é aconselhável que se utilize o Cmd.exe do sistema investigado, que pode responder de forma imprevisível por estar comprometido por algum Rootkit instalado na máquina. O kit de coleta de dados utilizado pelo perito deve conter uma cópia do cmd.exe sabidamente limpa, para que os comandos ali executados tenham a resposta correta e esperada.

Algumas ferramentas de linha de comando Windows Sysinternals (MICROSOFT, 2011a) costumam retornar um *popup* (pequena janela mostrada sobre a tela atual) perguntando se o usuário aceita as condições da licença de uso (*eula*). O inconveniente do *popup* é que a coleta automatizada fica interrompida, até que o usuário aceite ou não a licença do *software*. Para evitar este inconveniente em uma ferramenta automatizada de linha de comando, em que os resultados são dirigidos a um arquivo para análise posterior, deve ser utilizada a opção `<-accepteula>` logo após o comando, aceitando assim as condições da licença e evitando o aparecimento da janela.

As ferramentas distribuídas pela empresa Nirsoft (NIRSOFT, 2011a) podem ser executadas em linha de comando sem necessidade de interface gráfica, podendo direcionar o resultado da pesquisa para um arquivo de texto ( comando `/stext <nome_do_arquivo.txt>`), para um arquivo HTML (comando `/shtml <nome_do_arquivo.html>`), para um arquivo XML (comando `/sxml <nome_do_arquivo.xml>`) ou outros formatos, que podem ser consultados no site da Nirsoft. Os utilitários são distribuídos gratuitamente, podendo ser utilizados livremente para uso particular ou empresarial, desde que não haja fins lucrativos ou cobranças de qualquer natureza para recuperar senhas de eventuais clientes, a não ser com autorização expressa dos autores do software. Todos os arquivos do pacote devem ser incluídos na distribuição, sem qualquer modificação.

Os aplicativos podem ser livremente distribuídos, desde que todos os arquivos do pacote sejam incluídos sem qualquer modificação e que não haja nenhum tipo de cobrança financeira.

## **ANEXO B – CHECKLIST – BUSCA E APREENSÃO**

1. Providenciar duas testemunhas para acompanhar todo o procedimento (não parentes e não policiais).
2. Exibir o mandado de busca e apreensão.
3. Controlar o local (isolar computadores e cuidar da segurança).
4. Providenciar para que computadores ligados não sejam desligados ou entrem em modo de hibernação ou proteção de tela (podem estar com senha).
5. Fotografar e/ou filmar o ambiente (incluindo telas e conexões).
6. Verificar se o *flash drive* (CADAV) está íntegro (ferramentas de coleta com suas características originais e ausência de software malicioso).
7. Computador desligado?
  - a. Sim. - Apreender o material;  
- Ir para o item 13;
  - b. Não. - Continuar no passo seguinte.
8. Computador bloqueado?
  - a. Não. - Realizar a coleta de dados;  
- Ir para o item 10.
  - b. Sim. - Continuar no passo seguinte.
9. Pode ser desbloqueado?
  - a. Não. - Desligar o computador;  
- Apreender o material;  
- Ir para o item 13.
  - b. Sim. - Realizar a coleta de dados;  
- Continuar no passo seguinte.

10. Presença de criptografia ou máquina virtual?

- a. Não.
  - Desligar o computador;
  - Apreender o material;
  - Ir para o item 12.
  
- b. Sim.
  - Continuar no passo seguinte.

11. Dados acessíveis?

- a. Não.
  - Desligar o computador;
  - Apreender o material;
  - Continuar no passo seguinte.
  
- b. Sim.
  - Realizar a cópia lógica dos dados acessíveis;
  - Desligar o computador;
  - Apreender o material;
  - Continuar no passo seguinte.

12. Procedimentos a realizar no *notebook* do perito.

- Inserir *flash drive* de coleta (CADAV) no *notebook*;
- Copiar fotografias e/ou filmagem digital para a pasta “Resultados”;
- Executar ferramenta “Recalcula Hashes.bat” contido no diretório raiz;
- Gravar o conteúdo da pasta “Resultados” em mídia ótica;
- Gravar arquivos “Hashes.txt” no diretório raiz da mídia ótica;
- Juntar mídia ótica gravada ao material apreendido;
- Anotar o conteúdo do arquivo “Hash\_do\_Hashes.txt” no documento da Busca e Apreensão.

13. Encerrar documento da Busca e Apreensão – lembrar da assinatura das testemunhas.

14. Verificar se todo o material apreendido consta do Documento de Busca e Apreensão, com a descrição de suas características principais: tipo de material, marca, modelo, número de série, cor, ou outras características individualizadoras.

15. Conferir se o material apreendido está devidamente lacrado e acondicionado.



## ANEXO C – BUSCA E APREENSÃO DE MATERIAL DE INFORMÁTICA

### 1. Procedimentos Genéricos (HOELZ, RUBACK e SILVA, 2009)

1. Ao chegar ao local, assim que a segurança do ambiente estiver estabelecida, assegurar a integridade dos equipamentos e dados a serem apreendidos;
2. Apreensão de computadores de mesa (*desktops*):
  - 2.1. Quando ligados: Procedimentos específicos a cargo do perito criminal;
  - 2.2. Quando desligados: Não devem ser ligados. Desconectar todos os cabos externos. Documentar o estado das conexões relevantes. Se possível, retirar o(s) disco(s) rígido(s), caso contrário, apreender o gabinete inteiro;
3. Apreensão de computadores portáteis (*notebooks*):
  - 3.1. Quando ligados: Procedimentos específicos a cargo do perito criminal;
  - 3.2. Quando desligados: Não devem ser ligados. Retirar a bateria, encaminhando em conjunto com o respectivo *notebook*. Desconectar todos os cabos externos. Documentar o estado das conexões relevantes. Apreender o equipamento, acompanhado de sua fonte de alimentação;
4. Apreensão de periféricos:
  - 4.1. Devem normalmente ser apreendidos: discos rígidos externos, chaves de *hardware* e mídias removíveis (*flash drives*);
  - 4.2. Não devem normalmente ser apreendidos: dispositivos de entrada e saída de dados – impressoras, teclados, monitores;
5. Apreensão de mídias avulsas: *flash drives*, CDs, DVDs, cartões de memória, chips de celular, disquetes, iPods, máquinas fotográficas, filmadoras digitais, celulares, smartphones, etc., também podem conter dados relevantes e deve ser apreendidos. Para mídias pouco usuais, é aconselhável apreender também os dispositivos de leitura correspondentes e para dispositivos eletrônicos é recomendado que sejam apreendidos os carregadores e cabos de dados correspondentes;
6. Os equipamentos arrecadados devem ser adequadamente etiquetados, acondicionados e lacrados. Sempre que possível, devem ser separados em embalagens diferentes, dando preferência ao uso de plásticos transparentes como elementos de embalagem. As etiquetas identificadoras devem,

preferencialmente, ser afixadas sobre o equipamento em si, não sobre as embalagens. Os cabos de dados e conexão, carregadores, acessórios e manuais devem ser embalados juntamente com o equipamento correspondente;

7. Os discos rígidos removidos de um mesmo gabinete ou servidor, as mídias e dispositivos removíveis relacionados, e, se for o caso de ter havido coleta de dados no local pelo perito criminal, o disco rígido e/ou DVDs originados, deverão ser embalados e lacrados em um único volume;
8. Outras mídias removíveis encontradas não relacionadas diretamente a determinado computador, devem ser agrupadas por tipo e cada conjunto deve ser embalado e lacrado separadamente.

## **2. Cuidados Com o Material Apreendido**

1. Não deixar o material apreendido próximo a fontes de calor ou em locais fechados submetidos a altas temperaturas;
2. Manter o material distante de campos magnéticos gerados por motores elétricos, alto-falantes, imã, etc.;
3. Coletar os equipamentos com componentes eletrônicos expostos, como discos rígidos ou placas mãe, através de embalagens anti-estáticas;
4. Utilizar proteção contra choques mecânicos, embalando o equipamento em embalagens com proteção, como plástico-bolha, por exemplo.

## **3. Acondicionamento e lacre**

1. Separar os equipamentos através de embalagens e lacres diferentes;
2. Dar preferência a sacos plásticos transparentes;
3. Proteger a integridade física do equipamento, contra choques mecânicos ou descargas eletrostáticas;
4. Discos rígidos e mídias removíveis provenientes de um mesmo computador devem ser embalados e lacrados em um único volume;
5. Mídias de armazenamento avulsas devem ser agrupadas por tipo e cada conjunto deve ser embalado e lacrado individualmente.

## ANEXO D - CONTEÚDO DO ARQUIVO “COLETADADOS.BAT”

```
mkdir Resultados
echo Data do Sistema: > .\Resultados\Resultados.txt
date /t >> .\Resultados\Resultados.txt
echo.>> .\Resultados\Resultados.txt
echo ----- >>
.\Resultados\Resultados.txt
echo. >> .\Resultados\Resultados.txt

echo Hora do Sistema: >> .\Resultados\Resultados.txt
time /t >> .\Resultados\Resultados.txt
echo.>> .\Resultados\Resultados.txt
echo ----- >>
.\Resultados\Resultados.txt
echo. >> .\Resultados\Resultados.txt

echo Coleta de Registros do Windows
regedit /e .\Resultados\DumpReg.txt

echo Coleta de memória física (RAM)
.\Ferramentas\mdd_1.3.exe -o .\Resultados\Memorydump.dd

echo Conteúdo da área de transferência: >>
.\Resultados\Resultados.txt
.\Ferramentas\pclip >> .\Resultados\Resultados.txt
echo.>> .\Resultados\Resultados.txt
echo ----- >>
.\Resultados\Resultados.txt
echo. >> .\Resultados\Resultados.txt

echo Conexões TCP ativas: >> .\Resultados\Resultados.txt
.\Ferramentas\netstat -ano >> .\Resultados\Resultados.txt
echo.>> .\Resultados\Resultados.txt
echo ----- >>
.\Resultados\Resultados.txt
echo. >> .\Resultados\Resultados.txt

echo Portas abertas e aplicações associadas: >>
.\Resultados\Resultados.txt
.\Ferramentas\fport >> .\Resultados\Resultados.txt
echo.>> .\Resultados\Resultados.txt
echo ----- >>
.\Resultados\Resultados.txt
echo. >> .\Resultados\Resultados.txt

echo Configuração de interfaces de rede: >>
.\Resultados\Resultados.txt
ipconfig /all >> .\Resultados\Resultados.txt
echo.>> .\Resultados\Resultados.txt
echo ----- >>
.\Resultados\Resultados.txt
```

```

echo. >> .\Resultados\Resultados.txt

echo Informações sobre Processos em execução: >
.\Resultados\Processos.txt
.\Ferramentas\pslist >> .\Resultados\Processos.txt
echo.>> .\Resultados\Processos.txt
echo ----- >>
.\Resultados\Processos.txt
echo. >> .\Resultados\Processos.txt

echo Status dos Processos em execução: >>
.\Resultados\Processos.txt
.\Ferramentas\ps -accepteula >> .\Resultados\Processos.txt
echo.>> .\Resultados\Processos.txt
echo ----- >>
.\Resultados\Processos.txt
echo. >> .\Resultados\Processos.txt

echo Relação de processos com arquivos e pastas abertos: >
.\Resultados\Handle.txt
.\Ferramentas\handle -accepteula >> .\Resultados\Handle.txt

echo Lista de arquivos recentemente abertos: >>
.\Resultados\Resultados.txt
.\Ferramentas\tasklist >> .\Resultados\Resultados.txt
echo.>> .\Resultados\Resultados.txt
echo ----- >>
.\Resultados\Resultados.txt
echo. >> .\Resultados\Resultados.txt

echo Usuários logados ao sistema: >> .\Resultados\Resultados.txt
.\Ferramentas\psloggedon -accepteula >>
.\Resultados\Resultados.txt
echo.>> .\Resultados\Resultados.txt
echo ----- >>
.\Resultados\Resultados.txt
echo. >> .\Resultados\Resultados.txt

echo Usuários logados ao sistema: >> .\Resultados\Resultados.txt
dir "%UserProfile%\Recent" >> .\Resultados\Resultados.txt
echo.>> .\Resultados\Resultados.txt
echo ----- >>
.\Resultados\Resultados.txt
echo. >> .\Resultados\Resultados.txt

echo Informações do sistema: >> .\Resultados\Resultados.txt
.\Ferramentas\psinfo -accepteula >> .\Resultados\Resultados.txt
echo.>> .\Resultados\Resultados.txt
echo ----- >>
.\Resultados\Resultados.txt
echo. >> .\Resultados\Resultados.txt

echo off
.\Ferramentas\iepv\iepv /stext .\Resultados\Senhas_IE.txt

```

```

.\Ferramentas\passwordfox\passwordfox /stext
.\Resultados\Senhas_Firefox.txt

.\Ferramentas\ChromePass\ChromePass /stext
.\Resultados\Senhas_Chrome.txt

.\Ferramentas\mspass\mspass /stext .\Resultados\Senhas_msn.txt

.\Ferramentas\mailpv\mailpv /stext .\Resultados\Senhas_email.txt

.\Ferramentas\wirelesskeyview\wirelesskeyview /stext
.\Resultados\Senhas_wireless.txt

.\Ferramentas\iehv\iehv /stext .\Resultados\IE_history.txt

.\Ferramentas\mozillahistoryview\mozillahistoryview /stext
.\Resultados\Firefox_history.txt

.\Ferramentas\chromehistoryview\chromehistoryview /stext
.\Resultados\Chrome_history.txt

.\Ferramentas\mylastsearch\mylastsearch /stext
.\Resultados\UltPesquisas.txt

.\Ferramentas\skypelogview\skypelogview /stext
.\Resultados\Skypelog.txt

.\Ferramentas\edd120.exe /batch > .\Resultados\DetectaCripto.txt

.\Ferramentas"strings -accepteula .\Resultados\DetectaCripto.txt |
.\Ferramentas\grep -i "appears to be a virtual disk" >
.\Resultados\CriptoYesNo.txt

set "filemask=.\Resultados\CriptoYesNo.txt"
for %%A in (%filemask%) do if not %%~zA==0 Msg * "CUIDADO!!!
Existem fortes indícios de Criptografia de volumes ou mesmo do
Sistema Inteiro. Pesquise a presença de programas de criptografia,
principalmente Truecrypt, PGP ou Bitlocker. Se for o caso, realize
a cópia lógica dos arquivos!!!"

.\Ferramentas"strings -accepteula .\Resultados\Processos.txt |
.\Ferramentas\grep -ie "pgp" -ie "truecrypt" -ie "bitlocker" >
.\Resultados\TestesAdCYesNo.txt

set "filemask=.\Resultados\TestesAdCYesNo.txt"
for %%A in (%filemask%) do if not %%~zA==0 Msg * "CUIDADO!!!
Existem sinais de presença de programas de criptografia. Verifique
o sistema e, se for o caso, realize a cópia lógica dos arquivos
através do FTK Imager!!!"

.\Ferramentas\ScoopyNG\ScoopyNG.exe >
.\Resultados\DetectaVMware.txt

.\Ferramentas"strings -accepteula .\Resultados\DetectaVMware.txt |
.\Ferramentas\grep -i "VMware detected" >
.\Resultados\VMWareYesNo.txt

```

```

set "filemask=.\Resultados\VMWareYesNo.txt"
for %%A in (%filemask%) do if not %%~zA==0 Msg * "CUIDADO!!!
Existem fortes indícios de que o sistema esteja sendo executado em
maquina virtual WMWare. Verifique o sistema e, se for o caso,
realize a cópia logica dos arquivos através do FTK Imager!!!"

.\Ferramentas\strings -accepteula .\Resultados\Processos.txt |
.\Ferramentas\grep -ie "vmware" -ie "virtualbox" -
ie"VBoxService" -ie "VBoxTray" > .\Resultados\TestesAdYesNo.txt

set "filemask=.\Resultados\TestesAdYesNo.txt"
for %%A in (%filemask%) do if not %%~zA==0 Msg * "CUIDADO!!!
Existem sinais de presença de virtualização de sistema. Verifique
e, se for o caso, realize a cópia logica dos arquivos através do
FTK Imager!!!"

.\Ferramentas\usbdeview\usbdeview /stext .\Resultados\DispUSB.txt

set "filemask=.\Resultados\*.txt"
for %%A in (%filemask%) do if %%~zA==0 del /F /Q "%%A"

echo off
if EXIST .\Resultados\VMWareYesNo.txt del
.\Resultados\VMWareYesNo.txt
if EXIST .\Resultados\CriptoYesNo.txt del
.\Resultados\CriptoYesNo.txt
if EXIST .\Resultados\TestesAdYesNo.txt del
.\Resultados\TestesAdYesNo.txt
if EXIST .\Resultados\TestesAdCYesNo.txt del
.\Resultados\TestesAdCYesNo.txt
echo on

echo Data do Sistema: >> .\Resultados\Resultados.txt
date /t >> .\Resultados\Resultados.txt
echo.>> .\Resultados\Resultados.txt
echo ----- >>
.\Resultados\Resultados.txt
echo. >> .\Resultados\Resultados.txt

echo Hora do Sistema: >> .\Resultados\Resultados.txt
time /t >> .\Resultados\Resultados.txt
echo.>> .\Resultados\Resultados.txt
echo ----- >>
.\Resultados\Resultados.txt
echo. >> .\Resultados\Resultados.txt

echo off
if not EXIST .\Resultados\Memorydump.dd Msg * "CUIDADO!!! Houve
algum problema na captura da memória física (RAM) com a ferramenta
MDD. Faça a captura através do FTK Imager!!!"

.\Ferramentas\fsum\fsum -d".\Resultados" -r -sha256 * > Hashes.txt
.\Ferramentas\fsum\fsum -d"." Hashes.txt > Hash_do_Hashes.txt

echo on

```

Msg \* "A coleta de dados terminou. Verifique se existe necessidade de realizar alguma cópia lógica de dados ou de memória adicionais!!! Depois, retire o *flash drive* da maquina analisada e desligue o computador."

Msg \* "Anote o resultado do hash MD5 do arquivo "Hash\_do\_hashes.txt", que contém a lista de arquivos coletados com seus respectivos hashes SHA256. Veja o valor no prompt de comandos".

@echo Anote o HASH MD5 correspondente ao arquivos de Hashes.txt com a lista de arquivos e hashes HSA256 coletados na pasta

Resultados:

```
cmd /K"type Hash_do_Hashes.txt"
```

## **ANEXO E – CONTEÚDO DO ARQUIVO “RECALCULA HASHES.BAT”**

```
@echo off
```

```
.\Ferramentas\fsุม\fsุม -d".\Resultados" -r -sha256 * > Hashes.txt
```

```
.\Ferramentas\fsุม\fsุม -d"." Hashes.txt > Hash_do_Hashes.txt
```

```
@echo Despreze o HASH anotado anteriormente. Se você executou este comando é porque teve uma falha na coleta da memória física.
```

```
@echo Anote o novo HASH MD5 correspondente ao arquivo de Hashes.txt, que contém a lista de arquivos coletados na pasta Resultados e seus hashes SHA256 correspondentes:
```

```
cmd /K"type Hash_do_Hashes.txt"
```



## ANEXO F – CONTEÚDO DO ARQUIVO “LEIAME.TXT”

Ao inserir o *flash drive* no computador, aguarde alguns instantes para verificar se a coleta de dados irá iniciar automaticamente. Provavelmente isto não ocorrerá, porque o Windows XP, a partir do Service pack 3, desabilitou completamente o *autorun* a partir de dispositivos USB.

Caso a coleta automática não inicie, dê um duplo clique sobre o ícone "ColetaDados.bat" e aguarde a mensagem de término. Durante a coleta podem aparecer mensagens de texto na tela, informando a possível presença de criptografia de volumes, criptografia de sistema, ou virtualização do sistema operacional através do programa VMWare (VMWARE, 2011). Em qualquer destes casos, examine o sistema para confirmar as suspeitas. Em caso positivo, execute uma cópia lógica dos arquivos encontrados no volume criptografado ou cópia lógica de todo o sistema, no caso de criptografia de sistema ou virtualização do sistema. Se houver necessidade de realizar cópia lógica do sistema ou de volume, será necessário conectar um disco rígido externo em alguma outra porta USB do computador analisado.

A cópia dos arquivos pode ser feita a partir do programa FTK Imager (ACCESSDATA, 2011), cujo atalho encontra-se no diretório raiz do *flash drive*, com o nome: "FTK Imager.bat". Uma vez que o FTK Imager esteja sendo executado, para fazer cópia lógica de todo o sistema, clique em "File", depois "Add Evidence Item". Após, selecione "Physical Drive", encontre o drive correspondente ao Disco Rígido do sistema onde estiver realizando a coleta de dados, clique em "Finish" e expanda as opções até encontrar a pasta chamada "[root]". Clique nesta pasta com o botão direito do mouse e a seguir clique com o botão esquerdo em "Export logical Image (AD1)". Será aberta uma caixa de opções onde deve ser clicado em "Add...", depois clique em "Next", a seguir em "Browse", e encontre o drive correspondente ao disco rígido externo (USB) que irá receber os dados. Em "Image Filename" pode ser dado um nome genérico, como "Sistema", já que o disco rígido de destino e o *flash drive* (ou uma mídia ótica gravada a partir dele) utilizado na coleta acompanharão o restante do material de informática apreendido e serão cadastrados conjuntamente no Auto de Apreensão. Na pasta de destino, será criado um arquivo de texto pelo FTK Imager, contendo alguns dados da coleta, como o "Checksum" MD5 E SHA1, data e hora da coleta. Por fim, clique em "Finish" e a seguir, em "Start". Agora basta

esperar o término da cópia. Quando estiver pronto, verifique se há mais alguma coisa a copiar, como arquivos lógicos ou memória física. Caso contrário, desligue o computador e prossiga na arrecadação dos materiais de informática, inclusive do disco rígido da máquina examinada, se for possível retirá-lo, ou, em caso contrário, da máquina inteira.

Para fazer cópia dos arquivos de algum volume criptografado encontrado, clique em "File", depois "Add Evidence Item". Após, selecione "Logical Volume", encontre o drive correspondente ao volume criptografado e clique em "Finish". Expanda as opções até encontrar a pasta chamada "[root]". Clique nesta pasta com o botão direito do mouse e a seguir clique com o botão esquerdo do mouse em "Export logical Image (AD1)". Será aberta uma caixa de opções onde deve ser clicado em "Add...", depois em "Avançar". A seguir clique em "Browse" e encontre o drive correspondente ao Disco Rígido externo (USB) que irá receber os dados. Em "Image Filename" pode ser dado um nome genérico, como "Volume", já que o Disco Rígido de destino e o *flash drive* utilizado na coleta vão acompanhar o restante do material de informática apreendido e relacionado no Auto. Na pasta de destino, será criado um arquivo de texto pelo FTK Imager, contendo alguns dados da coleta, como o "Checksum" MD5 E SHA1, data e hora da coleta. Por fim, clique em "Finish" e a seguir, em "Start". Agora basta esperar o término da cópia. Quando estiver pronto, verifique se há mais alguma coisa a copiar, como arquivos ou memória física. Caso contrário, desligue o computador e prossiga na arrecadação dos materiais de informática, inclusive do disco rígido da máquina examinada, se for possível retirá-lo, ou, em caso contrário, da máquina inteira.

A coleta de memória física (RAM) é efetuada pelo programa "mdd" (MANTECH, 2011). Nos casos de virtualização de sistema pelo programa "VMWare" (VMWARE, 2011), o programa "mdd" pode não funcionar adequadamente. Neste caso, o protótipo de coleta de dados gerará um alerta (*popup*) durante a coleta, informando esta situação. Nesta situação, execute a coleta de memória a partir do programa "FTK Imager" (ACCESSDATA, 2011), cujo atalho encontra-se no diretório raiz deste *flash drive*, com o nome: "FTK Imager.bat". Uma vez que o FTK Imager esteja sendo executado, clique em "File" e depois na opção "Capture memory". Será aberta uma caixa de texto onde deve ser escolhido o destino do arquivo "memdump.mem", através de um clique na opção "Browse" e selecionando como destino a pasta "Resultados" do *flash drive* inserido durante a coleta.

Caso seja realizada nova coleta de memória, deve ser realizado novo cálculo de hashes da pasta Resultados, clicando no ícone "Recalcula Hashes.bat". Será criado um novo arquivo chamado "Hashes.txt" na raiz do flash drive, com o hash SHA256 de todos os arquivos contidos na pasta Resultados. Também será criado um arquivo chamado "Hash\_do\_Hashes.txt" na raiz do flash drive, contendo o hash MD5 do arquivo de hashes "Hashes.txt". Este hash deve substituir o valor anotado anteriormente, já que o valor anterior não incluía a coleta de memória. O valor do hash deve ser incluído no Auto de Busca e Apreensão ou na Informação Técnica elaborada pelo perito criminal, conforme for o caso, de forma a garantir a integridade dos arquivos coletados durante o procedimento na pasta Resultados.