UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

MODELAGEM DE AMEAÇAS ANTIFORENSES APLICADA AO PROCESSO FORENSE DIGITAL

MARCELO BRITO MAUÉS

ORIENTADOR: BRUNO WERNECK PINTO HOELZ

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

PUBLICAÇÃO: PPGENE.DM – 631/16

BRASÍLIA / DF: Dezembro/2016

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

MODELAGEM DE AMEAÇAS ANTIFORENSES APLICADA AO PROCESSO FORENSE DIGITAL

MARCELO BRITO MAUÉS

DISSERTAÇÃO DE MESTRADO 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:

BRUNO WERNECK PINTO HOELZ, Dr., UNB
(ORIENTADOR)

ROBSON DE OLIVEIRA ALBUQUERQUE Dr., UNB
(EXAMINADOR INTERNO)

HÉLVIO PEREIRA PEIXOTO Dr., POLÍCIA FEDERAL
(EXAMINADOR EXTERNO)

Brasília, 13 de Dezembro de 2016.

FICHA CATALOGRÁFICA

MAUÉS, MARCELO BRITO
Modelagem de ameaças antiforenses aplicada ao processo forense digital [Distrito Federal] 2016.
xxiv, 113p., 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2016).

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

1. Antiforense 2. Forense digital
3. Modelagem de ameaças

I. ENE/FT/UnB. II. Título (Série)

REFERÊNCIA BIBLIOGRÁFICA

MAUÉS, MARCELO BRITO (2016). Modelagem de Ameaças Antiforenses Aplicada ao Processo Forense Digital. Dissertação de Mestrado, Publicação PPGENE.DM – 631/16, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 113p.

CESSÃO DE DIREITOS

NOME DO AUTOR: Marcelo Brito Maués
TÍTULO DA DISSERTAÇÃO: Modelagem de Ameaças Antiforenses Aplicada ao Processo Forense Digital.
GRAU/ANO: Mestre/2016.

Marcelo Brito Maués
Av. Conselheiro Furtado, 1508
CEP 66.035-435 – Belém – PA - Brasil

Dedico esta dissertação aos meus pais,
à minha esposa e
ao meu filho.

AGRADECIMENTOS

Ao meu orientador Prof. Dr. Bruno Werneck Pinto Hoelz, pelo constante apoio, incentivo, dedicação e amizade essenciais para o desenvolvimento deste trabalho e para o meu desenvolvimento como pesquisador.

A Perita Samira Maria Carmo Luz Bricio, pelo apoio durante todo o curso de Mestrado.

Aos colegas do curso de Mestrado, pela amizade e incentivo.

A todos, os meus sinceros agradecimentos.

O presente trabalho foi realizado com o apoio do Instituto de Criminalística do Estado do Pará, com recursos do Programa Nacional de Segurança Pública com Cidadania – PRONASCI, do Ministério da Justiça.

RESUMO

MODELAGEM DE AMEAÇAS ANTIFORENSES APLICADA AO PROCESSO FORENSE DIGITAL

Autor: Marcelo Brito Maués

Orientador: Bruno Werneck Pinto Hoelz

Programa de Pós-graduação em Engenharia Elétrica

Brasília, dezembro de 2016

Na perícia forense digital, o papel do perito é coletar e analisar as evidências digitais. No entanto, ações antiforenses ameaçam o processo do exame pericial, podendo comprometer suas conclusões. Este trabalho propõe um processo de modelagem de ameaças com o objetivo de reduzir os riscos de ameaças antiforenses. O processo proposto introduz atividades de gestão de risco como um complemento aos processos de perícia digital encontrados na literatura, permitindo uma abordagem sistêmica para a avaliação de risco e o emprego de contramedidas e estratégias de mitigação de risco. Estudos de caso foram feitos com o intuito de validar o modelo proposto. Os estudos de caso demonstraram que a incorporação do modelo nas atividades do perito permite identificar e avaliar riscos de ameaças antiforenses ainda no início do processo forense digital e oferecer medidas de detecção e mitigação que podem ser aplicadas nas fases de coleta e análise de dados, evitando que ameaças antiforenses deixem de ser tratadas e que medidas de tratamento sejam adotadas desnecessariamente.

ABSTRACT

ANTI-FORENSICS THREAT MODELING APPLIED TO THE DIGITAL FORENSIC PROCESS

Author: Marcelo Brito Maués

Supervisor: Bruno Werneck Pinto Hoelz

Programa de Pós-graduação em Engenharia Elétrica

Brasília, December of 2016

In digital forensics, the role of the expert is to collect and analyze digital evidence. However, anti-forensics actions threaten the forensic examination process and may compromise its conclusions. This work proposes a threat modeling process in order to reduce the risks associated with anti-forensics threats. The proposed process introduces risk management activities as a complement to digital forensic processes found in the literature, allowing a systemic approach for measuring risk and employing countermeasures and risk mitigation strategies. Case studies were done with the purpose of validating the proposed model. Case studies demonstrated that the use of the model in the expert's activities allows for the identification and evaluation of risks of anti-forensics threats still in the beginning of the digital forensic process. It also offers detection and mitigation measures that can be applied in the phases of data collection and analysis, avoiding anti-forensic threats are not treated and treatment measures adopted unnecessarily.

SUMÁRIO

1. INTRODUÇÃO 1

1.1 OBJETIVO 1

1.2 JUSTIFICATIVA 2

1.3 ORGANIZAÇÃO 3

2. FUNDAMENTAÇÃO TEÓRICA 4

2.1 CRIMES CIBERNÉTICOS E A PERÍCIA FORENSE DIGITAL 4

2.1.1 Panorama atual 5

2.1.2 Perícia forense digital 8

2.1.2.1 A atividade pericial no Brasil 8

2.1.3 Exames periciais 9

2.1.4 Evidências digitais 10

2.1.5 Processo forense digital 11

2.1.6 Prontidão forense 15

2.2 ANTIFORENSE DIGITAL 16

2.2.1 Métodos antiforenses 19

***2.2.1.1 Slack Space* 20**

2.2.1.2 *Alternate Data Streams* (ADS) 23

2.2.1.3 Atributo $DATA de diretórios 24

2.2.1.4 *Clusters* adicionais 25

2.2.1.5 Arquivo $BadClus 26

2.2.1.6 Esteganografia 27

2.2.1.7 Criptografia 29

2.3 MODELAGEM DE AMEAÇAS 32

2.3.1 Ameaças ao sistema 34

2.3.1.1 Agente de ameaças maliciosas 35

2.3.2 Identificação de ameaças 40

2.3.3 Avaliação de riscos 41

2.3.4 Determinação de riscos 42

2.3.4.1 Probabilidade e Impacto 42

2.3.4.2 DREAD 44

2.3.4.3 Bug Bar 46

2.3.5 identificação de contramedidas 49

2.3.6 Mitigação de Riscos 50

3. PROPOSTA DE MODELAGEM DE AMEAÇAS ANTIFORENSES APLICADA AO PROCESSO FORENSE DIGITAL 52

3.1 COMPREENSÃO DO CASO INVESTIGADO 52

3.2 IDENTIFICAÇÃO DE FONTES DE EVIDÊNCIAS DIGITAIS 53

3.3 IDENTIFICAÇÃO DE AMEAÇAS ANTIFORENSES 54

3.4 GESTÃO DE RISCOS 54

3.4.1 Determinação do risco 55

3.4.2 Identificação de contramedidas 61

3.4.3 Mitigação de Riscos 61

3.5 REGISTRO DOS RESULTADOS E ATUALIZAÇÃO DO MODELO 63

3.6 APLICAÇÃO DA MODELAGEM DE AMEAÇAS NO PROCESSO FORENSE DIGITAL 63

4. ESTUDO DE CASO 67

4.1 PRIMEIRO CASO: PEDOFILIA 67

4.1.1 Determinação do risco 71

4.2 SEGUNDO CASO: JOGO DO BICHO 76

4.2.1 Determinação do risco 80

5. CONCLUSÃO 84

5.1 TRABALHOS PUBLICADOS 85

5.2 TRABALAHOS FUTUROS 85

REFERÊNCIAS BIBLIOGRÁFICAS 86

A – VISÃO GERAL DO SISTEMA DE ARQUIVOS NTFS 93

B – QUESTIONÁRIO PARA COLETA DE INFORMAÇÕES 94

C - CATÁLOGO DE AMEAÇAS ANTIFORENSES 95

D - CATÁLOGO DE OCORRÊNCIAS DE AÇÕES ANTIFORENSES 96

E - CATÁLOGO DE CONTRAMEDIDAS 97

F - MODELO DE RELATÓRIO DE MODELAGEM DE AMEAÇAS 99

G - ESTUDO DE CASO 01: RELATÓRIO DE MODELAGEM DE AMEAÇAS 101

H - ESTUDO DE CASO 02: RELATÓRIO DE MODELAGEM DE AMEAÇAS..... 105

I – RESULTADO DA PESQUISA SOBRE A GESTÃO DE RISCOS NO PROCESSO PERICIAL EM INFORMÁTICA 109

LISTA DE TABELAS

Tabela 2.1: Crimes praticados por computador, adaptada de Wendt e Jorge (2013) 5

Tabela 2.2: Exemplos de evidências digitais 10

Tabela 2.3: Modelos de Processo Forense Digital, adaptada de Sachowski (2016) 11

Tabela 2.4: Definições de níveis de probabilidade (NIST, 2002) 43

Tabela 2.5: Definições dos níveis de impacto (NIST, 2002) 43

Tabela 2.6: Matriz de risco, adaptada de NIST (2002) 44

Tabela 2.7 - Níveis de risco e ações necessárias (NIST, 2002) 44

Tabela 2.8: Tabela de estimativa de ameaças, adaptada de Meier et al. (2003) 45

Tabela 2.9: Estimativa DREAD, adaptada de Meier et al. (2003) 46

Tabela 2.10: Exemplo de *Bug Bar* de segurança (SULLIVAN, 2010) 47

Tabela 2.11: Ameaças STRIDE e contramedidas (MEIER, et al., 2003) 49

Tabela 3.1: Pontuação associada à avaliação da capacidade 57

Tabela 3.2: Pontuação associada à avaliação da motivação 57

Tabela 3.3: Pontuação associada à avaliação da oportunidade 57

Tabela 3.4: Pontuação associada ao histórico de ocorrências 58

Tabela 3.5: Pontuação associada à facilidade de exploração 58

Tabela 3.6: Níveis de probabilidade da ameaça por pontuação 59

Tabela 3.7: Exemplo de pontuação dos fatores relacionados ao agente 59

Tabela 3.8: Exemplo de pontuação dos fatores amplificadores 59

Tabela 3.9: Níveis de impacto da ameaça 60

Tabela 3.10: Matriz de cálculo do risco da ameaça antiforense, adaptada de NIST (2002) 60

Tabela 3.11: Proposta de contramedidas 61

Tabela 3.12: Níveis de custo de aplicação 62

Tabela 3.13: Matriz de mitigação 63

Tabela 4.1 - Estudo de caso 01: ameaças antiforenses identificadas 68

Tabela 4.2: Estudo de caso 01: níveis de probabilidade, impacto e risco 68

Tabela 4.3: Estudo de caso 01: contramedidas identificadas e custo de aplicação 69

Tabela 4.4: Estudo de caso 01: estratégia de mitigação 71

Tabela 4.5: Estudo de caso 01: pontuação capacidade 72

Tabela 4.6: Estudo de caso 01: pontuação motivação 72

Tabela 4.7: Estudo de caso 01: pontuação oportunidade 73

Tabela 4.8: Estudo de caso 01: pontuação histórico de ocorrências 74

Tabela 4.9: Estudo de caso 01: pontuação facilidade de exploração 74

Tabela 4.10: Estudo de caso 01: cálculo da probabilidade 75

Tabela 4.11: Estudo de caso 01: impacto 75

Tabela 4.12: Estudo de caso 02: ameaças antiforenses identificadas 76

Tabela 4.13: Estudo de caso 02: níveis de probabilidade, impacto e risco 77

Tabela 4.14: Estudo de caso 02: contramedidas identificadas e custo de aplicação 78

Tabela 4.15: Estudo de caso 02: estratégia de mitigação 79

Tabela 4.16: Estudo de caso 02: pontuação capacidade 80

Tabela 4.17: Estudo de caso 02: pontuação motivação 81

Tabela 4.18: Estudo de caso 02: pontuação oportunidade 81

Tabela 4.19: Estudo de caso 02: pontuação facilidade de exploração 82

Tabela 4.20: Estudo de caso 02: cálculo da probabilidade 82

Tabela 4.21: Estudo de caso 02: impacto 83

LISTA DE FIGURAS

Figura 2.1: Total de incidentes reportados ao CERT.br por ano (Fonte: CERT.br [A], 2016).. 5

Figura 2.2: Tipos de ataques de janeiro a dezembro de 2014 (Fonte: CERT.br [C], 2016) 6

Figura 2.3: Origem dos ataques por país (Fonte: CERT.br [D], 2016)..... 7

Figura 2.4: Tríade do principio de troca de Locard, adaptada de Sachowski (2016)..... 10

Figura 2.5: Acesso ao *file system slack* pelo FTK..... 21

Figura 2.6: *Slack Space* de um arquivo de 1280 *Bytes* com *clusters* de 4096 *Bytes*..... 21

Figura 2.7: Acesso ao *file slack space* pelo FTK 23

Figura 2.8: Detecção de ADS pelo comando DIR 24

Figura 2.9: Identificação de ADS no FTK 24

Figura 2.10: Ocultando dados em arquivo "JPG" 28

Figura 2.11: Visualização da imagem após a inserção dos dados..... 28

Figura 2.12: Visualização dos dados inseridos no arquivo 28

Figura 2.13 - *Bitlocker* ativado..... 31

Figura 2.14: Engenharia de segurança do sistema (MYAGMAR, 2005) 34

Figura 2.15: Componentes do agente de ameaça malicioso, adaptada de Jones (2002)..... 36

Figura 2.16: Elementos de ameaça e seus relacionamentos, adaptada de Jones (2002) 37

Figura 2.17: Componentes de capacidade, adaptada de Jones (2002) 38

Figura 2.18: Componentes de motivação, adaptada de Jones (2002) 38

Figura 2.19: Componentes inibidores, adaptada de Jones (2002)..... 39

Figura 2.20: Componentes amplificadores, adaptada de Jones (2002)..... 39

Figura 2.21 - Componentes catalisadores, adaptada de Jones (2002)..... 40

Figura 2.22: Pontos de ação para a mitigação de riscos, adaptada de NIST (2002) 51

Figura 3.1: Processo de modelagem de ameaças antiforenses..... 52

Figura 3.2: Elementos envolvidos na gestão de riscos..... 55

Figura 3.3: Fases do processo forense digital 64

Figura 3.4: Aplicação da modelagem ao processo forense digital 64

LISTA DE SÍMBOLOS, NOMENCLATURA E ABREVIAÇÕES

ABNT - Associação Brasileira de Normas Técnicas

ADS - *Altenate Data Streams*

ADSL - *Asymmetric Digital Subscriber Line*

CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CM - Contramedida

CNSEG - Confederação Nacional das Empresas de Seguros Gerais, Previdência Privada e Vida, Saúde Suplementar e Capitalização

CPP - Código de Processo Penal

DCO - *Device Configuration Overlay*

DFD - *Diagrama de Fluxo de Dados*

DFRWS - *Digital Foreniscs Research Workshop*

DKOM - *Kernel, Direct Kernel Manipulation*

DLL - *Dynamic Link Library*

e-discovery – Processo de descoberta de evidências

FTK – *Forensic Tool Kit*

HPA - *Host Protected Area*

IBGE - Instituto Brasileiro de Geografia e Estatística

IP – *Internet Protocol*

ISO - *International Organization for Standardization*

JPEG - *Joint Photographic Experts Group*

NIST - *National Institute of Standards and Technology*

NTFS - *New Technology File System*

OWASP - *Open Web Application Security Project*

RAM - *Random Access Memory*

TELNET - *Telecommunication Network*

TI - Tecnologia da Informação

TIC - Tecnologia da Informação e Comunicação

1. INTRODUÇÃO

Um volume cada vez maior de solicitações de perícias forenses digitais se apresenta à medida que a tecnologia se populariza e se difunde na sociedade. São ameaças, espionagem industrial, calúnia e difamação (pessoal e corporativa) por meio de *e-mails*, *blogs* etc., violação de privacidade, uso indevido da imagem, desfiguração de *sites*, destruição de informações, interrupção de comunicações, interrupção de serviços, provocando danos à imagem e ao patrimônio das pessoas e empresas, entre outras consequências (COSTA, 2011).

A perícia forense digital tem como objetivo esclarecer um incidente a partir da busca de evidências digitais em diferentes tecnologias como, por exemplo, computadores, telefones móveis e redes de computadores (SACHOWSKI, 2016). Vários modelos para a condução do processo forense digital foram desenvolvidos ao longo dos anos, alguns para lidar com uma necessidade específica e outros com escopo generalizado para serem adotados universalmente.

No âmbito da perícia oficial, o perito criminal é o responsável por coletar e analisar evidências digitais a serem apresentadas como provas em um tribunal ou em um processo legal (BEER, STANDER e BELLE, 2014). Contudo, ações antiforenses comprometem a capacidade do profissional de processar corretamente tais evidências (HARRIS, 2006).

As ações antiforenses estão relacionadas a qualquer tentativa de comprometer a disponibilidade ou utilidade de evidências digitais. Logo, representam uma ameaça permanente ao processo pericial. O resultado antiforense pode ser obtido com o uso de ferramentas ou métodos maliciosos, muitos de conhecimento público, ou simplesmente pelo uso de proteções legítimas, como senhas e criptografia. Segundo Conlan, Baggili, e Breitinger (2016), ações antiforenses têm se tornado um grande obstáculo para a comunidade forense, exigindo novas iniciativas e estratégias de investigação para resolver esse problema crescente.

1.1 OBJETIVO

O objetivo deste trabalho é propor um método para tratar ameaças antiforenses que podem comprometer a recuperação e apresentação de evidências digitais utilizáveis em um processo judicial. Para alcançar esse objetivo, propõe-se um processo de modelagem de ameaças para tratar riscos antiforenses de forma estruturada e possa complementar os processos forenses digitais encontrados na literatura que não consideram a gestão dos riscos

associados a ameaças antiforenses. Por meio do modelo será possível identificar ameaças antiforenses, estimar seus riscos e propor medidas de mitigação, dando oportunidade ao perito de tratá-las durante os procedimentos periciais.

Esta dissertação tem por objetivos específicos:

- identificar e descrever métodos antiforenses;
- abordar o processo de modelagem de ameaças adotado no desenvolvimento de *software;*
- analisar os processos forenses digitais;
- desenvolver um processo de modelagem de ameaças antiforenses para ser aplicado ao processo forense digital;
- realizar estudos de caso para testar e avaliar o modelo proposto.

O trabalho tem como desafio demonstrar que preceitos de modelagem de ameaças utilizados no desenvolvimento de *software* podem ser aplicados ao processo forense digital para o tratamento de riscos de ameaças antiforenses.

1.2 JUSTIFICATIVA

O trabalho do perito é realizado, predominantemente, em ambientes fora de seu controle, sobre os quais informações preliminares podem ser escassas ou inexistentes. Por isso, a realização do exame pericial requer preparação prévia das ferramentas, técnicas e procedimentos a serem aplicados em cada cenário de atuação. Contudo, um dos aspectos comumente ignorados nessa preparação é a avaliação de riscos associados a ameaças antiforenses, apesar dos peritos estarem conscientes dos riscos de ameaças antiforenses antes de iniciar os procedimentos periciais, conforme mostra pesquisa realizada (apêndice I).

Apesar da constatação de que ações antiforenses representam uma ameaça ao processo forense digital, tal preocupação não se reflete nos modelos encontrados na literatura, que não consideram a gerência de riscos de ameaças antiforenses nos processos periciais.

Embora diversos estudos estejam sendo realizados sobre detecção de ações antiforenses, como o uso de esteganografia, por exemplo, a ausência de um processo bem definido de identificação e avaliação de riscos contribui para que técnicas de detecção não sejam incorporadas ao processo pericial ou que sejam aplicadas desnecessariamente. No primeiro caso, evidências digitais cruciais ao exame podem deixar de ser recuperadas por falta

de tratamento adequado, enquanto no segundo há desperdício de recursos, especialmente de tempo.

A modelagem de ameaças é uma técnica amplamente utilizada no desenvolvimento de *software* com o objetivo de analisar a segurança do aplicativo, identificando, quantificando e tratando riscos associados ao sistema de forma estruturada (OWASP, 2015). Na literatura, é possível encontrar diversas formas de conduzir um processo de modelagem de ameaças, conforme pode ser visto em Sindre e Opdahl (2005), Shostack (2014) e OWASP (2015). Entretanto, no âmbito da perícia digital, não foi encontrado um processo de modelagem de ameaças bem definido para tratamento de ações antiforenses no processo pericial.

O processo proposto permite que uma organização avalie continuamente seu nível de preparação, seja em termos de treinamento ou das ferramentas disponíveis, identificando lacunas que apresentem risco à realização adequada do exame pericial. Por fim, o processo proposto também auxilia na adoção do preceito de prontidão forense (ou *forensic readiness*), segundo o qual se deve maximizar o uso de evidências digitais e ao mesmo tempo minimizar o custo de uma investigação forense digital (SULE, 2014).

1.3 ORGANIZAÇÃO

A dissertação está dividida em cinco capítulos. No capítulo 2 são apresentados conceitos necessários ao entendimento do trabalho, como crimes informáticos, forense digital, antiforense digital e modelagem de ameaças. O capítulo 3 apresenta o processo de modelagem de ameaças proposto, detalhando cada etapa do modelo e sua aplicação no processo forense digital. No capítulo 4 são apresentados estudos de caso, demonstrando os resultados da aplicação do modelo em dois casos reais, um relacionado à pedofilia e outro ao jogo do bicho. Finalmente, no capítulo 5 conclui-se o trabalho apresentando-se uma síntese do modelo proposto e sua relevância para o processo forense digital a partir dos resultados obtidos com os estudos de caso. Também recomenda-se, para o futuro, o desdobramento e a continuidade deste trabalho.

2. FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são apresentados conceitos necessários ao entendimento do trabalho, como crimes informáticos, forense digital, antiforense digital e modelagem de ameaças. O capítulo dá um panorama dos crimes cibernéticos e apresenta dados estatísticos que demonstram o aumento desses tipos de crime no Brasil. Ainda aborda a perícia forense digital, dando uma visão da atividade pericial no país e apresentando conceitos e modelos relacionados ao tema, e apresenta o termo Antiforense Digital, como demonstra a aplicação de métodos antiforenses voltados à ocultação de dados e formas de detecção. Por fim, trata o processo de modelagem de ameaças no desenvolvimento de *software*, com a descrição de técnicas e métodos adotados.

2.1 CRIMES CIBERNÉTICOS E A PERÍCIA FORENSE DIGITAL

A popularização dos computadores e do acesso à Internet trouxe benefícios às pessoas e à comunidade. Pesquisa do Instituto Brasileiro de Geografia e Estatística (IBGE), realizada em setembro de 2014 mostra que em 2001 12,6% das unidades residenciais tinham computadores, e em 2013 esse percentual evoluiu para quase metade dos domicílios (49,5%). No mesmo período, as moradias com computadores conectados à Internet aumentaram de 8,5% para 43,7% (IBGE, 2015). Todavia, com a disseminação tecnológica, surgiu também a possibilidade de realização de novas práticas ilegais e criminosas (ELEUTÉRIO e MACHADO, 2011), como os crimes cibernéticos.

Segundo Moore (2005), crimes cibernéticos referem-se a qualquer prática criminal que envolva um computador ou uma rede de computadores. Para Wendt e Jorge (2013), os crimes cibernéticos dividem-se em “crimes cibernéticos abertos” ou “crimes exclusivamente cibernéticos”. Os crimes cibernéticos abertos são aqueles em que o computador não é imprescindível, sendo apenas um meio, ou seja, os crimes poderiam ser praticados da forma “tradicional”, sem o auxílio de recursos computacionais. No segundo tipo, exclusivamente cibernéticos, os crimes só podem ser praticados com a utilização de computadores ou recursos tecnológicos. A Tabela 2.1 classifica cada um desses crimes conforme sejam eles cibernéticos abertos ou exclusivamente cibernéticos.

Tabela 2.1: Crimes praticados por computador, adaptada de Wendt e Jorge (2013)

CRIMES CIBERNÉTICOS "ABERTOS"	CRIMES EXCLUSIVAMENTE CIBERNÉTICOS
• Crimes contra a honra • Ameaça • Pornografia infantil • Estelionato • Furto mediante fraude • Racismo • Apologia ao crime • Falsa identidade • Concorrência desleal • Tráfico de drogas	• Invasão de computador mediante violação de mecanismo de segurança com o fim de obter, adulterar ou excluir dados e informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. • Interpretação telemática ilegal • Pornografia infantil por meio de sistema de informática • Corrupção de menores em salas de bate papo • Crimes contra a urna eletrônica

2.1.1 Panorama atual

Os dados estatísticos produzidos pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira, permitem observar o aumento no números de incidentes no Brasil, e o quanto a atividade criminosa tem se expandido. A Figura 2.1 mostra o aumento siginificativo do número de notificações desde 1999.

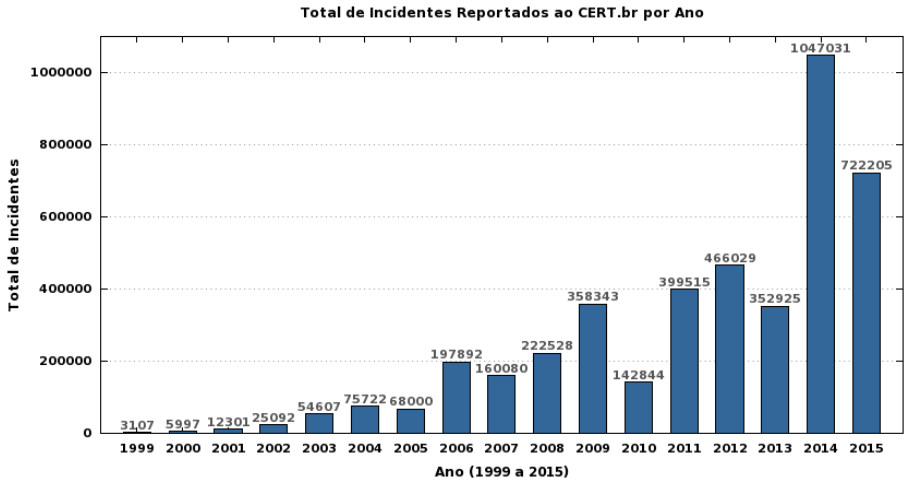


Figura 2.1: Total de incidentes reportados ao CERT.br por ano (Fonte: CERT.br [A], 2016)

Segundo o CERT.br (CERT.br [B], 2016), no período de janeiro a dezembro de 2015 alguns fatos de interesse foram observados em relação a 2014, conforme se verifica a seguir:

- aumento de 128% nas notificações de ataques a servidores *Web*;
- manutenção da grande quantidade de notificações de ataques de força bruta contra sistemas de gerenciamento de conteúdos (ou *Content Management System* – CMS);
- redução do número de notificações sobre computadores que participaram de ataques de negação de serviço (DoS);
- queda do número de notificações de fraudes, com destaque para a redução do número de casos de páginas falsas de bancos e *sites* de comércio eletrônico. Contudo, houve aumento no número de notificações de casos de páginas falsas que não envolvem bancos e *sites* de comércio eletrônico, como por exemplo nos serviços de *webmail* e nas redes sociais;
- aumento no número de notificações referentes a varreduras[1], com destaque para varreduras em serviços de TELNET (*Telecommunication Network*), cujo foco principal são equipamentos de rede alocados às residências de usuários finais, tais como *modems* ADSL(*Asymmetric Digital Subscriber Line*), roteadores *Wi-Fi* etc.;
- redução no número de computadores comprometidos. A maioria refere-se a servidores *Web* que tiveram suas páginas desfiguradas.

Nos dados levantados pelo CERT.br, verifica-se que os ataques do tipo "varredura" (ou *Scan*) apresentaram maior número de notificações em 2015 (54,17%). A Figura 2.2 mostra um gráfico comparativo entre as modalidades mais frequentes de ataques no período de janeiro a dezembro de 2015.

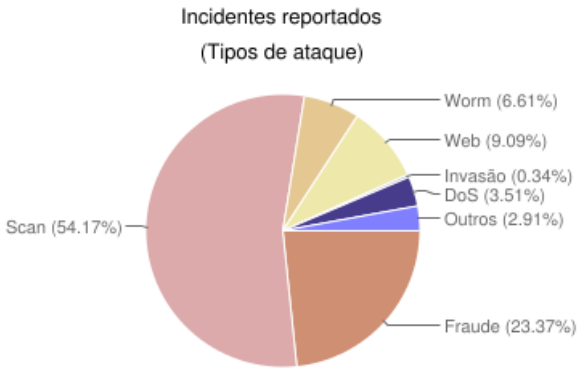


Figura 2.2: Tipos de ataques de janeiro a dezembro de 2014 (Fonte: CERT.br [C], 2016)

[1] Entende-se como "varredura" o processo de identificação dos computadores ativos e dos serviços disponibilizados por eles.

Observando-se o histórico da origem dos ataques no CERT.br, apresentado na Figura 2.3, percebe-se que a maioria (54,02%) é proveniente do Brasil, vindo bem distante, em segundo lugar, os Estados Unidos (11,16%). Segundo estudo do ano de 2013 da empresa Trend Micro[2] (TREND MICRO, 2013), são motivo para o aumento de crimes cibernéticos no Brasil:

- tamanho da população brasileira, aspecto que contribui para determinar o número de usuários conectados à Internet. O Brasil é o sexto país mais populoso e o sétimo em uso de Internet (INTERNET WORLD STATS, 2016);
- melhoria no serviço de acesso à Internet, com o crescimento da velocidade média de conexão;
- aumento do número de usuários que fazem uso dos serviços de banco *online*;
- desenvolvimento do mercado de Tecnologia da Informação e Comunicação (TIC), no qual, segundo o estudo, o Brasil consta como terceiro maior no mercado de computadores, quarto em celulares e segundo em caixas automáticos.

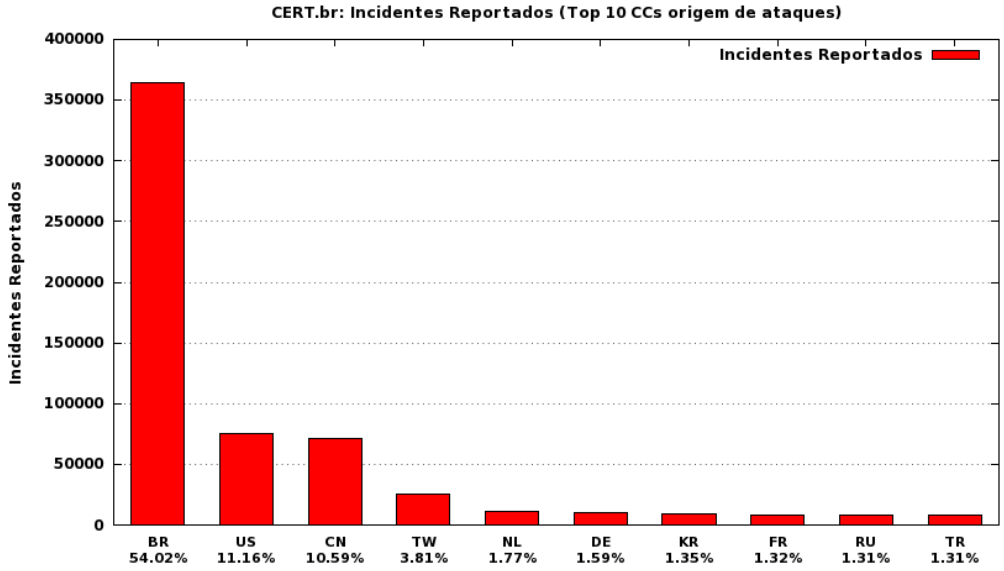


Figura 2.3: Origem dos ataques por país (Fonte: CERT.br [D], 2016)

O especialista Peter Armstrong, da área de *Cyber Risks* do *Willis Group*, em Londres, afirma que o Brasil precisa adotar medidas para reduzir os riscos gerados pelos crimes cibernéticos e que o cenário é perfeito para a atração de *hackers* locais e internacionais (CNSEG, 2015). Consequentemente, o aumento dos crimes cibernéticos ocasiona uma

[2] Empresa de soluções de segurança para conteúdo e gerenciamento de ameaças na Internet.

demanda maior por exames periciais em meios digitais para a investigação e solução desses crimes.

2.1.2 Perícia forense digital

De acordo com Sachowski (2016), antes da década de 1980 crimes cibernéticos eram tratados usando leis gerais, já existentes. No entanto, ainda segundo o autor, com o aumento dos crimes cibernéticos, diversos países criaram leis específicas para tratá-los, como a *Computers Crimes Act* criada em 1978 nos Estados Unidos, e permitiram que termos como análise de informática forense ou computação forense fossem evidenciados. Contudo, com o passar do tempo, evidências digitais começaram a ser encontradas em outras tecnologias, como redes de computadores, impressoras, telefones celulares etc. Diante dessa nova realidade, em 2001 o primeiro *Digital Forensics Research Workshop* (DFRWS) propôs a utilização do termo *Digital Forensics*, aqui traduzido como "Perícia Forense Digital", para descrever o campo como um todo, incluindo subáreas, como a computação forense, a perícia forense de redes de computadores e de dispositivos móveis (SACHOWSKI, 2016).

A perícia forense digital pode ser definida como a aplicação da ciência à lei, em que princípios científicos, metodologias e técnicas são utilizados durante uma investigação digital. Sua formalização levou à primeira publicação, entre 1999 e 2000, dos princípios forenses digitais concebidos a partir do trabalho conjunto da *Internacional Organization On Computer Evidence* (ou Organização Internacional sobre Evidência de Computador), a *G-8 High Tech Crime subcommittee* (ou subcomitê G-8 de Tecnologia de Ponta) e o *Scientific Working Group on Digital Evidence* (ou Grupo de Trabalho Científico da Evidência Digital). Da mesma forma, ferramentas forenses evoluíram, resultando em maior diversidade de *hardware* especializado, aplicativos comerciais e de *software* livre, bem como programas de certificação de profissionais e de ambientes de laboratório que preenchem os requisitos da ciência forense (SACHOWSKI, 2016).

2.1.2.1 A atividade pericial no Brasil

De acordo com o artigo 158 do Código de Processo Penal (CPP), "quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado". Dessa forma, impõe-se o acompanhamento de um Perito, profissional qualificado, que examinará os vestígios e produzirá laudos de interesse da Justiça no esclarecimento de um delito, conforme previsto no CPP: "o exame de corpo de

delito e outras perícias serão realizados por Perito Oficial, portador de diploma de curso superior" (artigo 159) e "os peritos elaborarão o laudo pericial, no qual descreverão minuciosamente o que examinarem e responderão aos quesitos formulados" (artigo 160).

No caso de crimes cibernéticos, as atividades serão oficialmente realizadas por um Perito Criminal da área de computação. No entanto, dependendo da necessidade, outros profissionais podem também realizar os trabalhos como: peritos particulares, auditores de sistemas, profissionais de Tecnologia da Informação (TI) e outros. Além disso, é necessário que juízes, advogados, delegados, promotores e demais profissionais da área de direito também saibam apurar corretamente e apresentar as evidências e provas digitais (ELEUTÉRIO e MACHADO, 2011).

2.1.3 Exames periciais

De acordo com Eleutério e Machado (2011), novos exames devem surgir nos próximos anos. Entretanto, os autores consideram os seguintes como principais:

- exames e procedimentos em locais de crime de informática: "consistem no mapeamento, identificação e correta preservação dos equipamentos computacionais, a fim de permitir melhor seleção do material a ser apreendido, para ser examinado em laboratório posteriormente";
- exames em dispositivos de armazenamento computacional: "consistem basicamente em analisar arquivos, sistemas e programas instalados em discos rígidos, CDs, DVDs, *Blu-Rays*, *pen drives* e outros dispositivos de armazenamento digital de dados";
- exames em aparelhos de telefone celular: consiste na extração de dados disponíveis na memória do telefone para posterior análise e formalização;
- exames em *sites* da Internet: consiste na análise de informações contidas em *sites* da Internet, incluindo a verificação do responsável pelo domínio e/ou endereço IP (*Internet Protocol*);
- exames em mensagens eletrônicas (*e-mails*): consiste basicamente em analisar o cabeçalho das mensagens, do qual constam informações como hora, data e endereço IP.

2.1.4 Evidências digitais

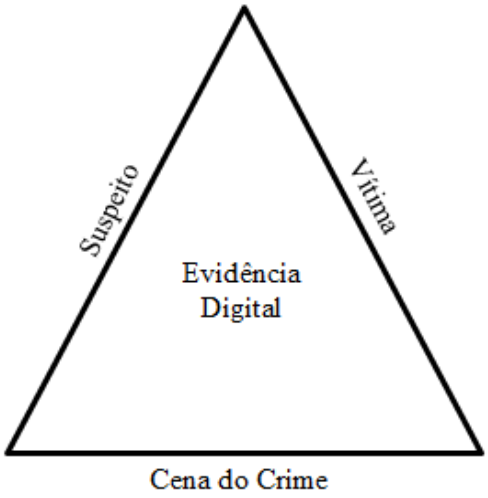


Figura 2.4: Tríade do principio de troca de Locard, adaptada de Sachowski (2016).

De acordo com o princípio de troca de Locard, ilustrado na Figura 2.4, todo o autor de crime deixa alguma coisa dentro de uma cena de crime e leva alguma coisa da cena do crime com ele (TILSTONE, et. al., 2006). No mundo digital, ambas as ocorrências podem ser usadas como evidência digital numa investigação forense (SACHOWSKI, 2016).

Segundo Sachowski (2016), o campo da perícia forense digital abrange uma variedade de tecnologias que servem como fontes de evidências, desde o tradicional computador até dispositivos mais modernos, como telefones móveis, consoles de jogos e ambientes virtualizados, e elas podem ser voláteis e não voláteis. A Tabela 2.2 exemplifica os dois tipos de evidências digitais.

Tabela 2.2: Exemplos de evidências digitais

Evidencias digitais voláteis	**Evidências digitais não voláteis**
Configurações de rede	Informações de contas
Conexões de rede	Arquivos de configuração e *logs*
Processos em execução	Arquivos de dados
Arquivos abertos	Arquivos de páginas e *swap*
Sessões de *login*	Arquivos temporários ou *cache*
Informações de data e hora	Registro do sistema operacional

O maior desafio de evidências digitais voláteis é saber como coletá-las, pois elas só estão disponíveis enquanto o sistema estiver ativo, desde que não tenha sido reiniciado ou

desligado após a ocorrência do incidente. Além disso, qualquer ação executada no sistema, por uma pessoa ou pelo sistema, certamente vai modificar o estado atual dos dados voláteis disponíveis para o perito (SACHOWSKI, 2016). Portanto, o perito deve planejar com antecedência as ações que devem ser tomadas, a fim de evitar que dados voláteis utilizáveis para a investigação sejam modificados ou perdidos.

2.1.5 Processo forense digital

Vários modelos de processo forense digital foram desenvolvidos ao longo dos anos. Não há um critério para determinar qual dos modelos de processos identificados é a melhor opção, já que cada um tem vantagens e desvantagens para cada tipo de cenário. A Tabela 2.3 apresenta uma lista cronológica de modelos, apresentando o número de fases em cada um.

Tabela 2.3: Modelos de Processo Forense Digital, adaptada de Sachowski (2016)

Nome	Autor(es)	Ano	Fases
Computer Forensic Investigate Process	Pollitt	1995	4
Computer Forensic Process Model	U.S. Department of Justice	2001	4
Digital Forensic Reaseach Workshop Investigate Model (Generic Investigation Process)	Palmer	2001	6
Scientific Crime Scene Investigation Model	Lee et al.	2001	4
Abstract Model of the Digital Forensic Procedures	Reith et al.	2002	9
Integrated Digital Investigation Process	Carrier and Spalford	2003	5
End to End Digital Investigation	Stephenson	2003	9
Enhanced Integrated Digital Investigation Process	Baryamureeba and Tushabe	2004	5
Extended Model of Cyber Crime Investigation	Ciardhuáin	2004	6
A hierarchical Objective-Based Framework for the Digital Investigations Process	Beebe and Clark	2004	6
Event-Based Digital Forensic Investigation Framework	Carrier and Spalford	2004	5
Four Step Forensic Process	Kent et al.	2006	4
Framework for a Digital Forensic Investigation	Kohn et al.	2006	3
Computer Forensic Field Triage Process Model	Rogers et al.	2006	12
FORZA-Digital forensics investigation framework	Leong	2006	6
Common Process Model for incident and Computer Forensics	Freiling and Schwittay	2007	3
Dual Data Analysis Process	Bem and Huebner	2007	4
Digital Forensic Model based on Malaysian Process	Perumal	2009	7

Generic Framework for Network Forensics	Pilli et al.	2010	9
Generic Computer Forensic Investigation Model	Yusoff	2011	5
Systematic Digital Forensic Investigation Model	Agarwal et al.	2011	11
Metodologia e arquitetura para sistematização do processo investigatório de análise da informação digital	*Costa*	2012	4

A Tabela 2.3 apresenta um número significativo de modelos, com diferentes números de fases. Alguns focam somente na coleta e análise de evidências digitais e outros incluem ações de planejamento. As ações de planejamento estão relacionadas a atividades sugeridas nos modelos para serem executadas antes dos exames periciais. No entanto, entre as ações de planejamento previstas nos modelos não se observa a preocupação com a gestão de riscos associados a ações antiforenses, apesar de representarem uma ameaça aos procedimentos periciais, conforme descrito na seção 2.2.

Para exemplificar o processo forense digital, serão descritas a seguir as fases do modelo sugerido por Beebe e Clark (2004), que incorpora a maioria das ações dos outros modelos. Os autores propõem uma estrutura de processo forense digital dividido em seis etapas: Preparação, Resposta ao Incidente, Coleta de Dados, Análise de Dados, Apresentação dos Resultados e Encerramento do Incidente.

Fase 01: Preparação

Essa fase visa maximizar a disponibilidade e a qualidade das evidências digitais, e inclui medidas que precisam ser tomadas pelas empresas para maximizar a disponibilidade de evidências digitais. A preparação inclui atividades como:

- avaliação de riscos de vulnerabilidades, ameaças, perda/exposição etc.;
- desenvolvimento do plano de retenção de informações (pré e pós incidente);
- elaboração de um plano de resposta a incidentes, incluindo definição de políticas, procedimentos, atribuições pessoais e requisitos técnicos;
- desenvolvimento de capacidades técnicas (por exemplo, *kit* de ferramentas de respostas);
- treinamento pessoal;
- preparação de *hosts* e dispositivos de redes;
- desenvolvimento de procedimentos de manuseio e preservação de evidências;

- documentação do resultado das atividades;
- elaboração de um plano de coordenação de atividades legais (pós e pré incidentes).

Fase 02: Resposta ao Incidente

O objetivo dessa fase é detectar, validar, avaliar e determinar uma estratégia de resposta ao incidente. São atividades previstas nessa fase:

- detecção ou suspeição de atividade não autorizada;
- relato da detecção ou suspeição de atividade à autoridade competente;
- validação do incidente;
- avaliação do dano/impacto através de entrevistas com o pessoal técnico/negócio, revisão de registros de *logs*, revisão da topologia da rede etc.;
- desenvolvimento de uma estratégia para contenção, erradicação, recuperação e investigação, considerando fatores/metas de negócios, técnicos, políticos e legais;
- coordenação da aplicação de recursos jurídicos e humanos;
- formulação de um plano de investigação inicial para a coleta e análise de dados.

Fase 03: Coleta de Dados

Apesar de ser necessária a coleta de alguns dados na fase de resposta aos incidentes, é nessa fase que ocorre a coleta formal dos dados. O objetivo dessa etapa é coletar evidências digitais em apoio a uma estratégia de resposta e a um plano de investigação. São atividades para a coleta de dados:

- complementação da coleta de dados, iniciada provavelmente durante a fase de resposta de incidentes;
- obtenção de evidências de redes a partir de fontes como sistemas de detecção de intrusão, roteadores, *firewalls*, servidores de *log* etc.;
- obtenção de evidências de *hosts* a partir de fontes como dados voláteis, informações de data/hora do sistema, discos rígidos ou cópias forenses deles etc.;
- obtenção de evidências de mídias removíveis como fitas de *backup*, disquetes, *CD-ROMs*, dispositivos de memória *flash* etc.;

- implementação de atividades de monitoramento com a aplicação de monitores de rede, monitores de sistema, câmeras de vigilância etc.;
- preservação da integridade e autenticidade das evidências digitais, protegendo-as contra gravação, utilizando códigos *hash*[3] etc.;
- embalagem, transporte e armazenamento da evidência digital.

Fase 04: Análise de Dados

O objetivo dessa fase é confirmar ou refutar as alegações da atividade suspeita e/ou a reconstrução do evento. Essa fase prevê as seguintes atividades:

- redução do volume e da quantidade de dados coletados na fase anterior em um tamanho mais manejável para a análise dos dados;
- realização de um levantamento inicial de dados para identificar partes óbvias de evidências digitais e avaliar o nível de habilidade do(s) suspeito(s);
- emprego de técnicas de extração de dados, como pesquisa por palavra-chave, extração de espaço não alocado e *slack space*, mapeamento de linha do tempo de arquivos, extração e coleta de dados ocultos etc.;
- exame, análise e reconstrução de eventos para responder a questões críticas da investigação.

Fase 05: Apresentação dos Resultados

A apresentação dos resultados pode ser escrita, oral ou exibida em ambos os formatos. A apresentação é destinada a fornecer informações de forma sucinta ou detalhada da confirmação e reconstrução de eventos relacionados aos dados analisados na fase de análise de dados.

Fase 06: Encerramento do Incidente

O propósito da fase de encerramento do incidente inclui as seguintes etapas:

- realização de revisão crítica de todo o processo de investigação para identificar e aplicar as lições aprendidas em outros processos;
- ação compatível com os resultados da fase de apresentação dos resultados;

[3] Sequência de *bits* representada na base hexadecimal e gerada por um algoritmo, que busca identificar uma informação unicamente.

- descarte de evidências, como “retorne ao proprietário”, “destrua” ou “limpe”, se aplicável ou legalmente permitido;
- coleta e preservação de todas as informações relacionadas ao incidente.

2.1.6 Prontidão forense

O conceito de prontidão forense (ou *forensic readiness*) está relacionado à capacidade de uma organização de maximizar de forma proativa o uso de evidências digitais, minimizando os custos da investigação forense (SACHOWSKI, 2016; SULE, 2014). O conceito foi publicado pela primeira vez em 2001 por John Tan (SACHOWSKI, 2016).

Rowlingson (2004) cita como objetivos de um programa de prontidão forense:

- reunir evidências admissíveis em um processo legal, sem interferir nos negócios;
- reunir evidências visando crimes potenciais e disputas que possam afetar negativamente uma organização;
- permitir que uma investigação aconteça com um custo proporcional ao incidente;
- minimizar a interrupção dos negócios de uma organização durante uma investigação;
- assegurar que uma evidência tenha um impacto positivo sobre o resultado de qualquer ação legal.

Grobber e Louwarens (2007) ainda incluem como objetivo do programa a prevenção do uso de estratégias antiforenses. Nesse caso, o autor sugere como atividade para o alcance do objetivo o uso de controles de segurança para impedir quaisquer ações antiforenses.

Conforme pode ser observado na literatura, o cerne da prontidão forense é fazer com que uma empresa esteja preparada para passar por um processo de descoberta de evidências (ou *e-discovery*). No âmbito da perícia oficial, o processo forense digital pode ganhar aspectos de prontidão forense com a adoção de um processo de modelagem de ameaças antiforenses. Com o processo de modelagem proposto, estratégias para a mitigação de riscos antiforenses podem ser definidas preventivamente, fato que contribui para a maximização proativa do uso de evidências digitais, preceito da prontidão forense.

2.2 ANTIFORENSE DIGITAL

Desde que o crime começou, criminosos tentam cobrir seus rastros. Para cada avanço na ciência forense, tem havido uma contramedida. Quando surgiu o processo de identificação por impressão digital, ladrões começaram a usar luvas. Quando *hackers* começaram a ter êxito no acesso privilegiado a sistemas remotos, passaram a ter cuidado de excluir arquivos de *log* para mascarar o que fizeram. E quando métodos forenses melhoraram, apareceram técnicas antiforenses projetadas para derrotá-los (MANSFIELD-DEVINE, 2010).

Não há uma única definição para "antiforense", o que não é surpresa, pois o campo ainda é pouco explorado. Alguns autores definem "antiforense" como ferramentas de destruição ou que evitam a detecção de informações. A melhor forma de definir é interpretar separadamente as palavras "anti" e "forense", para, posteriormente, combinando o significado das duas, chegar-se à definição de "antiforense" como "o método usado para evitar (ou agir contra) a aplicação da ciência às leis civis e criminais em um sistema de justiça criminal" (HARRIS, 2006).

Diversos autores sugerem a divisão das técnicas antiforenses em categorias, pois, dessa forma, é possível separá-las de acordo com as ações que propõem. Rogers (2006) sugere, por exemplo, que as técnicas antiforenses sejam divididas quanto à ocultação de dados, eliminação de artefatos, ofuscação de evidências e ataques contra ferramentas ou computador. Já Peron e Legacy (2005) recomendam que sejam classificadas quanto à destruição, ocultação, manipulação ou prevenção de criação de evidências. Por fim, Harris (2006) propõe uma nova divisão baseada na semelhança entre as categorias anteriores, em que as técnicas antiforenses devem ser classificadas quanto à destruição, ocultação, falsificação e eliminação de fontes de evidências.

Destruição de Evidências

Tem como objetivo destruir dados ou deixá-los inutilizáveis para o processo investigatório (HARRIS, 2006; CHANDRAN e YAN, 2013). Não é uma técnica simples, pois as próprias ações tomadas podem deixar rastros. Por exemplo, a sobrescrita de um arquivo pode destruir parcialmente ou totalmente seu conteúdo, entretanto o *software* utilizado para destruí-lo pode criar novas evidências (HARRIS, 2006).

A destruição pode ser de dois tipos: lógica ou física. A primeira é realizada apenas sobrescrevendo os dados repetidamente (CHANDRAN e YAN, 2013). A segunda pela desmagnetização, quando as mídias são magnéticas (disco rígido), ou, caso contrário, pela

destruição total das mídias, no caso de *CDs* e *DVDs* (CALOYANNIDES, 2009). A destruição dos dados é usada para remover fragmentos de arquivos apagados, informações do sistema ativo e de qualquer informação que possa contribuir para a identificação de um crime (CHANDRAN e YAN, 2013). A seguir são descritos alguns métodos voltados à destruição de evidências:

- "Limpeza" de arquivos (ou *wipe*): permite apagar arquivos substituindo os *clusters* ocupados pelo arquivo por dados aleatórios (BEER, STANDER e BELLE, 2014);
- Alteração de atributos de arquivos: destruição de atributos do sistema de arquivos ou substituição por dados aleatórios (HARRIS, 2006);
- Destruição de artefatos de atividades de usuários: eliminação de forma segura de artefatos de atividades dos usuários, como histórico de internet, acesso a arquivos, *downloads* de arquivos e bate-papos (BEER, STANDER e BELLE, 2014);
- Desmagnetização de mídias: varrer a mídia com um imã poderoso, deixando os dados instáveis (BEER, STANDER e BELLE, 2014).

Ocultação de Evidências

É a ação de deixar as evidências menos visíveis para o perito, de modo que não sejam descobertas para uso em processo investigatório. Nesse caso, as evidências não são destruídas e nem modificadas (HARRIS, 2006), mas a presença de ferramentas de ocultação de dados no sistema pode tornar-se um indício do uso dessa técnica (MCCULLAGH, 2005).

Não há garantia de sucesso, mas a técnica pode ser bastante eficaz caso seja bem executada. A escolha de locais normalmente não examinados por peritos e de locais não explorados por ferramentas forenses são altamente indicados. Pode-se também renomear arquivos como forma de ludibriar as atividades periciais (HARRIS, 2006). Essa técnica depende amplamente da ineficácia da ferramenta forense e da falta de habilidade do perito (CHANDRAN e YAN, 2013). A seguir são descritos alguns métodos voltados à ocultação de evidências:

- Exploração de áreas reservadas do disco: esconder dados em áreas reservadas do disco chamadas *Host Protected Area* (HPA) e *Device Configuration Overlay* (DCO) (BERGHEL, HOELZER e STHULTZ, 2008);

- Exploração de áreas do sistema de arquivos: esconder dados em estruturas de sistemas de arquivos. Por exemplo, *Slack Space* e *Altenate Data Streams* (ADS) no sistema de arquivos NTFS (BERGHEL, HOELZER e STHULTZ, 2008);
- Criptografia: permite tornar arquivos ilegíveis (CRAIGER, POLLITT e SWAUGER, 2005);
- Remoção de arquivos: deleção de arquivos e substituição do ponteiro no sistema de arquivos (HARRIS, 2006);
- Esteganografia: permite esconder dados digitais dentro de outro arquivo (CHANAALII e JADHAV, 2009).

Eliminação de fontes de evidências

Consiste em evitar a geração de evidências, ou seja, diferentemente das outras técnicas já comentadas, não há necessidade de destruir ou ocultar evidências, pois elas não serão criadas. Entretanto, o processo pode deixar rastros. Por exemplo, saindo do mundo dos crimes digitais, caso sejam utilizadas luvas de borracha para segurar uma arma, não haverá registros de impressões digitais. Entretanto, um bom perito deve perceber que, em função da ausência de impressões, o assassinato deve ter sido planejado. O mesmo acontece nos crimes digitais (HARRIS, 2006). A seguir são descritos alguns métodos voltados à eliminação de evidências:

- Desativação de *Logs*: informações sobre atividades não vão ser registradas (HARRIS, 2006);
- Uso de aplicações portáteis: uso de aplicativos que não requerem instalação evitam deixar rastros (BEER, STANDER e BELLE, 2014);
- Uso de *Live Distros*: uso de sistemas operacionais que funcionam a partir de dispositivos como *CDs* e *pen drives* (BEER, STANDER e BELLE, 2014);
- Uso de *Syscall proxing*: a chamada de sistema local ou função é um *proxy* para outro sistema concluir (BEER, STANDER e BELLE, 2014);
- Injeção de biblioteca remota: bibliotecas, como *Dynamic Link Library* (DLL), são inseridas diretamente na memória RAM, sem deixar rastros no disco rígido (BEER, STANDER e BELLE, 2014);

- Manipulação direta de *Kernel* (ou *Direct Kernel Manipulation* - DKOM): a operação que permite a invasão do espaço de memória utilizado por objetos do *kernel*[4] por outros processos (BEER, STANDER e BELLE, 2014);
- Utilização de navegadores "*in-private*": permite que navegadores, como por exemplo *Mozilla Firefox*, mantenham todo o *cache*[5] e histórico em memória de acesso aleatório (ou *Random Access Memory* - RAM), evitando escrever qualquer informação em disco para posterior análise (BEER, STANDER e BELLE, 2014).

Falsificação de evidências

É a ação de criar evidências falsas ou modificar evidências para comprometer a validade de uma evidência real. Nessa técnica, não há a preocupação de destruir a evidência ou ocultá-la, pois, ainda assim, será inválida. A falsificação tem como objetivo imputar a alguém a responsabilidade de um crime (HARRIS, 2006). A seguir são descritos alguns métodos voltados à falsificação:

- Alteração dos atributos do sistema de arquivos: modificação dos valores de atributos de arquivos, como por exemplo, data e hora, de forma que possam enganar as ações forenses (HARRIS, 2006);
- *Spoofing*: falsificação de endereço IP (BEER, STANDER e BELLE, 2014);
- Sequestro de contas: criar evidências para atribuir a responsabilidade por ações danosas a outra pessoa (HARRIS, 2006).

2.2.1 Métodos antiforenses

Nessa seção, são apresentados alguns métodos antiforenses voltados à ocultação de dados, bem como formas de detecção com o auxílio de utilitários do sistema operacional *Windows* e *Linux*, ferramentas do *Sleuth Kit* (CARRIER [B]), *Winhex* (WINHEX) e a ferramenta comercial *Forensic Tool Kit* (ACCESS DATA).

Tendo em vista que para o entendimento de alguns métodos há necessidade de conhecimento da estrutura do sistema de arquivos NTFS (*New Technology File System*), no apêndice A o sistema é abordado sucintamente.

[4] Componente central ou núcleo do sistema operacional.
[5] Área de armazenamento onde dados acessados frequentemente são guardados para um acesso futuro mais rápido.

2.2.1.1 Slack Space

O *Slack Space* corresponde a sobras de espaços no disco rígido que não podem ser utilizadas pelo sistema de arquivos. O *Slack Space* existe em todos os sistemas de arquivos (HUEBNER, BEM e WEE, 2006). A seguir serão apresentados alguns tipos de *Slack Space* que podem ser explorados para a ocultação de dados no sistema de arquivos NTFS.

File System Slack Space

É um espaço não alocado para *clusters* localizado no final do sistema de arquivos NTFS. Esse espaço surge quando o tamanho da partição não é múltiplo do tamanho do *cluster* (CARRIER [A], 2006). Segundo exemplo de Huebner, Bem e Wee (2006), se existirem 10.001 setores na partição e o NTFS trabalhar com clusters de quatro setores, serão alocados somente os primeiros 10.000 setores, totalizando 2.500 *clusters*. Portanto, o último setor será o *file system slack*, que pode ser utilizado para a ocultação de dados. O espaço pode ser explorado utilizando-se um editor de texto em hexadecimal para inserir os dados a serem ocultados nos setores do *File System Slack Space*.

Detecção

Para a detecção dos dados ocultados é necessário identificar a existência de *file system slack space* na partição. Para isso, é necessário verificar se o número de setores por partição é múltiplo do número de setores por *cluster*. Se não for, haverá *file system slack space* na partição. Portanto, os setores desse espaço deverão ser extraídos e analisados (HUEBNER; BEM e WEE, 2006). O número de setores por partição e o número de setores por *cluster* podem ser obtidos utilizando-se o utilitário *fsstat* do *Sleuth Kit*, conforme abaixo:

```
fsstat /prova/imagem01.dd –f ntfs
```

Confirmada a existência de *file system slack space*, ele poderá ser extraído com o uso do comando dd do *Linux* e posteriormente analisado com uma ferramenta de recuperação de dados por *datacarving*[6], como por exemplo, o *foremost* (FOREMOST), conforme abaixo:

```
dd if=/prova/imagem01.dd bs=512 skip=10000 count=1 \
          of=/prova/setor10001.dd

foremost /prova/setor10001.dd –o /recuperados
```

[6] Técnica que faz a busca de arquivos em um conjunto de dados com base em sua assinatura (cabeçalho ou rodapé).

Nos comandos acima, o comando dd armazena os dados do setor 10001 no arquivo "setor10001.dd", e o comando *foremost* analisa os dados extraídos.

Utilizando o programa FTK, o processo é facilitado, pois ele identifica e mostra o *file system slack space*, conforme Figura 2.5.

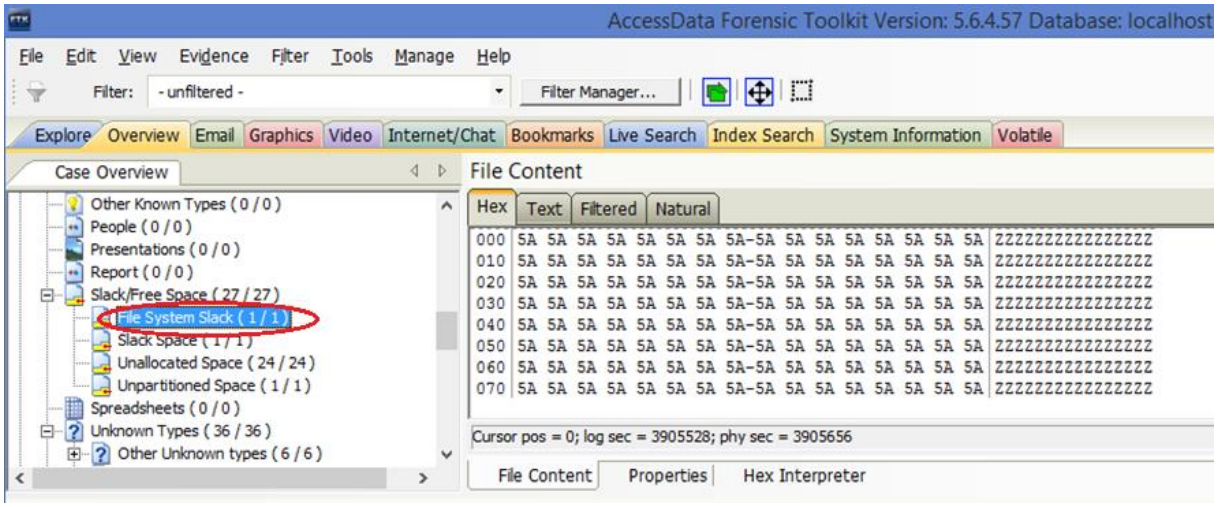


Figura 2.5: Acesso ao *file system slack* pelo FTK

File Slack Space

Como estratégia para acelerar o gerenciamento de arquivos, os sistemas operacionais modernos escrevem dados de um arquivo em *clusters*. Se o tamanho do arquivo não for múltiplo do tamanho do setor, o sistema operacional deve preencher o espaço remanescente no último setor. Quando o sistema operacional é *Windows 9x*, esse espaço é preenchido por dados provenientes da memória, por isso historicamente ele é chamado de "*RAM SLACK*". Já em sistemas operacionais modernos, o espaço é preenchido por zeros (BERGHEL, HOELZER e STHULTZ, 2008). Se o total de dados do arquivo não preencher um *cluster* completo, o restante do *cluster* após o "*RAM SLACK*" é chamado de "*DRIVE SLACK*" (HUEBNER; BEM e WEE, 2006). Portanto, esse espaço composto pelo "*RAM SLACK*" e "*DRIVE SLACK*" é chamado de *file slack* e pode ser utilizado para ocultar dados.

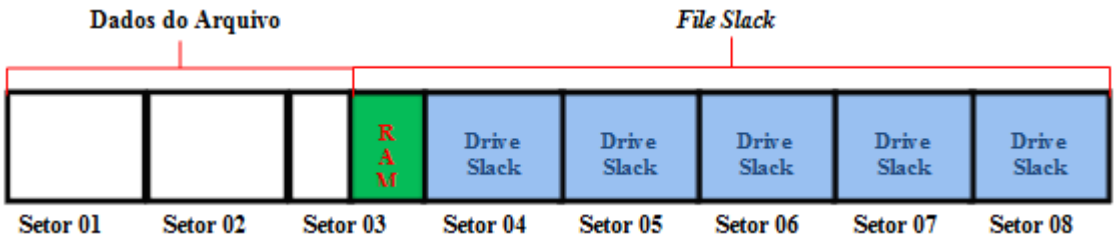


Figura 2.6: *Slack Space* de um arquivo de 1280 *Bytes* com *clusters* de 4096 *Bytes*

O *file slack space* pode ser facilmente explorado com o uso do programa Slacker.exe (Slacker). Abaixo é mostrado um exemplo de sua utilização.

```
slacker –s artigo.txt c:\imagens c:\meta.jpg \
        password –d –n
```

No exemplo acima, o arquivo "artigo.txt" foi ocultado nos *slacks spaces* dos arquivos contidos no diretório "imagens". O arquivo "meta.jpg" foi usado para armazenar informações sobre a ocultação e o parâmetro *password* refere-se a uma senha para a recuperação dos dados. Abaixo, o comando para recuperação dos dados ocultados.

```
slacker –r c:\meta.jpg password –o artigo.txt
```

Detecção

A forma de detecção compreende a análise do espaço de "*RAM SLACK*" de cada arquivo. Se os dados não estiverem zerados, o *file slack* deverá ser analisado (HUEBNER, BEM e WEE, 2006). O *file slack* de cada arquivo pode ser extraído com utilitários como *istat* e *icat* do *Sleuth kit* e o comando dd do *Linux*, conforme abaixo:

```
istat –f ntfs /prova/imagem01.dd 30

icat –sf ntfs /prova/imagem01.dd  30   >                \
/prova/arquivo30.dd

dd  if=/prova/arquivo30.dd  of=/prova/ram_arquivo30.dd  \
        bs=1 skip=1851910 count=506

dd  if=/prova/arquivo30.dd  of=/prova/drive_arquivo30.dd  \
        bs=512 skip=3618 count=6
```

No exemplo acima, suponha-se que o *istat* mostre que o arquivo localizado na entrada 30 da MFT possui tamanho real de 1851910 *bytes* e o espaço alocado para ele é de 1855488 *bytes*. Portanto, considerando-se que um *cluster* tem tamanho de 4096 *bytes*, é possível descobrir que o *file slack* do arquivo tem tamanho de 3578 *bytes* (1855488 – 1851910) e o "*DRIVE SLACK*" e "*RAM SLACK*" são respectivamente 3072 *bytes* e 506 *bytes*.

Com o comando *icat*, os dados dos setores alocados para o arquivo são copiados para o arquivo "arquivo30.dd" e, em seguida, utilizando-se o comando dd, consegue-se copiar os dados do "*DRIVE SLACK*" e "*RAM SLACK*" para o arquivo "drive_arquivo30.dd" e "ram_arquivo30.dd", respectivamente, para serem analisados posteriormente.

A análise pode ser feita utilizando-se um editor de hexadecimal ou uma ferramenta de recuperação por *data carving*. Vale ressaltar que esse procedimento deverá ser realizado para cada arquivo suspeito. Já o FTK identifica o *file slack space*, facilitando o processo de análise, conforme a Figura 2.7 .

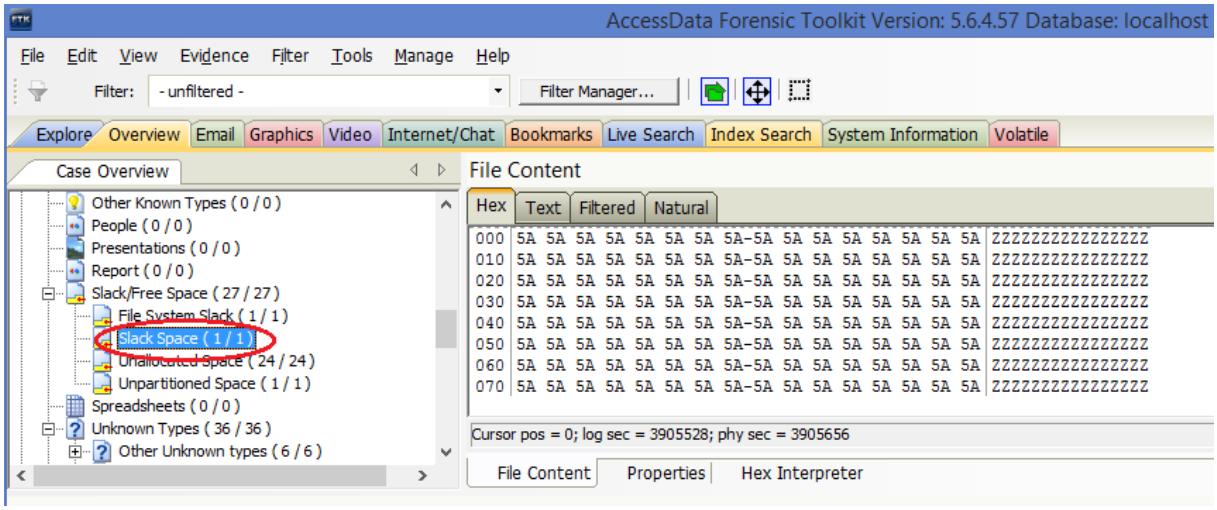


Figura 2.7: Acesso ao *file slack space* pelo FTK

2.2.1.2 *Alternate Data Streams* (ADS)

Em sistemas de arquivos NTFS um registro de arquivo na MFT pode ter mais de um atributo $DATA. Esses atributos $DATA adicionais são chamados de fluxos alternativos de dados ou *Alternate Data Streams* (ADS) e tornaram-se interessantes para a ocultação de dados, pois a maioria dos utilitários de sistema mostra apenas o conteúdo do atributo $DATA primário (HUEBNER; BEM e WEE, 2006). Os ADS podem ser facilmente criados e acessados por comandos DOS, sem a ajuda de programas específicos, conforme abaixo:

```
type dados.txt > c:\artigo.txt:ocultos.txt

notepad c:\artigo.txt:ocultos.txt
```

No primeiro comando acima, o conteúdo do arquivo “dados.txt” é inserido em um atributo $DATA criado e nomeado como “ocultos.txt”. O segundo comando mostra uma forma de acessar os dados ocultados. Durante os testes, e seguindo os mesmos procedimentos acima, foi observada a possibilidade de criação de ADS também em diretórios.

Detecção

Hoje existem diversos *software*, comerciais ou não, que auxiliam na procura de ADS no NTFS. O próprio comando dir do DOS, utilizando a opção /r, permite visualizar ADS,

conforme Figura 2.8. Já o FTK consegue identificar ADS durante o processo de análise, conforme Figura 2.9.

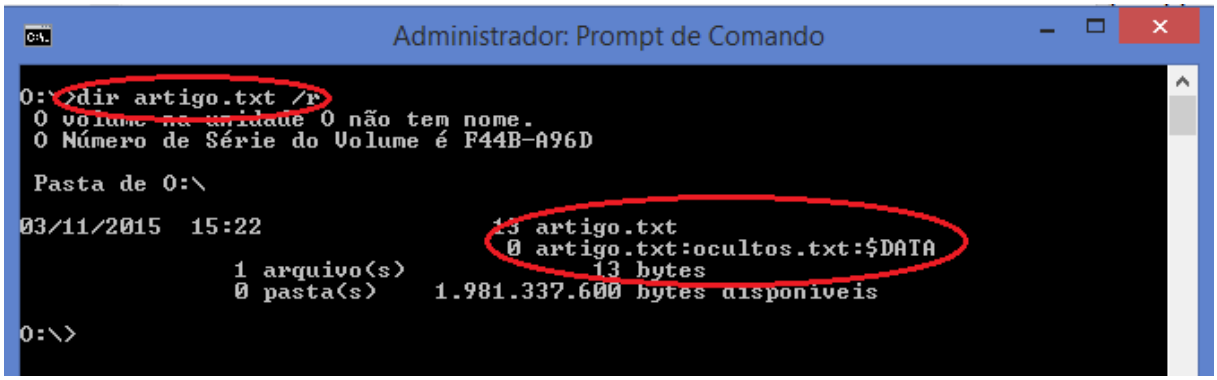


Figura 2.8: Detecção de ADS pelo comando DIR

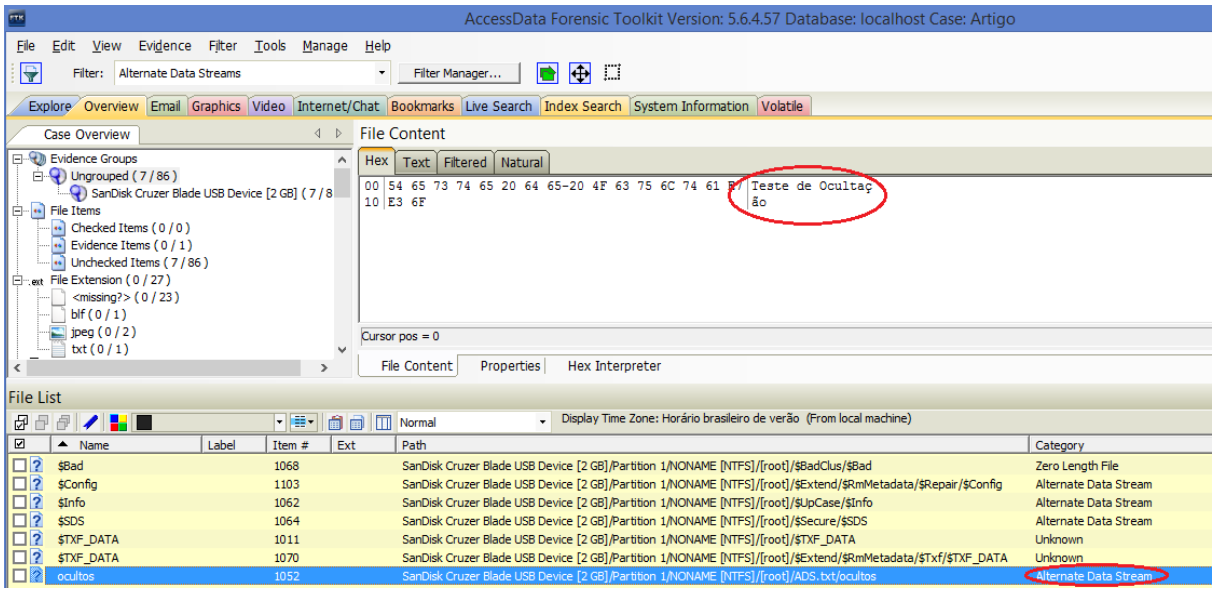


Figura 2.9: Identificação de ADS no FTK

Vale ressaltar que os ADS nem sempre são utilizados para práticas antiforenses. Algumas aplicações legítimas fazem uso deles. Portanto, nem sempre a sua presença caracteriza a intenção de ocultar dados.

2.2.1.3 Atributo $DATA de diretórios

O atributo $DATA do sistema de arquivos NTFS é usado geralmente para armazenar o conteúdo de um arquivo, mas não é comum encontrar diretórios com esse atributo. Contudo, observa-se que a criação dele em diretórios não interfere no funcionamento do sistema NTFS. Em função desse fato, a criação do atributo $DATA em diretório para ocultação de dados torna-se interessante (CARRIER [A], 2005).

Segundo (HUEBNER; BEM e WEE, 2006), os seguintes procedimentos são necessários para ocultar dados no atributo $DATA de um diretório do NTFS:

- criar um diretório;
- inserir um atributo $DATA no diretório antes dos atributos $INDEX_ROOT, $INDEX_ALLOCATION e $BITMAP;
- alterar o identificador de atributos dos demais atributos em função da inserção do atributo $DATA;
- modificar o tamanho da entrada do diretório na MFT;
- modificar para "1" (alocado) o *status* de alocação dos *clusters* para o atributo $DATA;
- inserir os dados a serem ocultados nos *clusters* alocados para o atributo $DATA.

Detecção

A única forma encontrada de detecção é analisando-se todas as entradas de diretório e verificando-se se possuem o atributo $DATA. Se algum atributo $DATA for encontrado, o conteúdo deve ser analisado.

Na ferramenta FTK não foi observado nenhum mecanismo que identifique automaticamente atributos $DATA em diretórios. Ou seja, todas as entradas de diretório também deverão ser verificadas individualmente.

2.2.1.4 *Clusters* adicionais

Esse método é baseado na possibilidade de alocação manual de *clusters* a um arquivo já existente. Nesses *clusters* adicionais pode-se ocultar dados. Com esse método, o espaço disponível para ocultação dependerá da quantidade de *clusters* adicionais alocados, tendo como limite apenas a capacidade do sistema de arquivos (BERGHEL, HOELZER e STHULTZ, 2008). Segundo Huebner, Bem e Wee (2006), os seguintes procedimentos são necessários para a implementação do método:

- a lista de *clusters runs* deverá ser modificada para alocar mais clusters;
- o último número de *cluster virtual* (ou *Virtual Cluster Number* - VCN), do arquivo deverá ser modificado;
- o tamanho de alocação do arquivo deverá ser modificado;

- o *status* dos *clusters* adicionados deverão ser modificados para “1” (alocado) no $Bitmap.

Detecção

Segundo Huebner, Bem e Wee (2006), é necessário buscar todos os arquivos, um de cada vez, e comparar o tamanho alocado e o tamanho real de cada arquivo. Esses valores podem ser encontrados no cabeçalho do atributo $DATA dos arquivos.

Ferramentas do *Sleuth Kit*, como *fls* e *istat*, podem ser utilizadas para o processo de detecção, conforme abaixo:

```
fls –rFf ntfs /prova/imagem01.dd

istat /prova/imagem01.dd 30
```

Utilizando-se o *fls* é possível listar as entradas da MFT e com o *istat* pode-se obter o número de *clusters* alocados e o tamanho real de um determinado arquivo. Caso o tamanho alocado para um arquivo seja maior do que o seu tamanho real, é possível que dados estejam sendo ocultados nele. Portanto, o arquivo deve ser analisado. No FTK, nenhum mecanismo foi observado para agilizar o processo de identificação.

2.2.1.5 Arquivo $BadClus

No sistema de arquivos NTFS, *clusters* marcados como inutilizáveis (ou “ruins”) são registrados em um atributo $DATA chamado $Bad do arquivo $BadClus. É possível manipular o arquivo $BadClus para marcar *clusters* utilizáveis como “ruins”, não podendo ser acessados posteriormente pelo sistema operacional. Esses *clusters* poderão ser utilizados para a ocultação de dados (BERGHEL, HOELZER e STHULTZ, 2008).

Para a realização do procedimento, é necessário modificar a lista de *Cluster Run* do atributo $DATA, nomeado como $Bad, bem como o tamanho do atributo e o tamanho da entrada do arquivo na MFT. O *status* de alocação dos *clusters* a serem utilizados para ocultação deverão ser modificados para “1” (alocado).

Detecção

A simples existência de registros de *clusters* “ruins” no arquivo $BadClus já pode indicar uma atividade incomum, pois hoje é raro sistemas operacionais lidarem com setores defeituosos. Tal função é desempenhada pelos controladores do disco rígido (HUEBNER; BEM e WEE, 2006). Portanto, caso seja detectada a existência de *clusters* rotulados como

“ruins” no arquivo $BadClus, é recomendável fazer a extração e análise desses *clusters*. Para identificar *clusters* no atributo $DATA $Bad, o seguinte comando do *Sleuth Kit* pode ser utilizado:

```
istat /prova/imagem01.dd –f ntfs 8
```

No FTK, a análise também deverá ser realizada checando-se a existência de *clusters* marcados como “ruins” no $BadClus.

2.2.1.6 Esteganografia

O principal objetivo da esteganografia é esconder informações para que outra pessoa não perceba sua presença. A maioria dos empregos da esteganografia foi realizada em arquivos de imagens, vídeos, textos, música e sons. Esse tipo de técnica é muito utilizado na troca secreta de informações (CHANAALII e JADHAV, 2009).

Existem várias técnicas e protocolos para esconder informações dentro de um objeto. Todavia, eles devem obedecer às seguintes condições para que a esteganografia possa ser aplicada corretamente (CUMMINS et al., 2004):

- a integridade da informação deve ser preservada após ser incorporada ao objeto;
- o objeto usado para ocultar as informações não deve sofrer alterações que possam ser percebidas a olho nu;
- em marca d´água, mudanças nos objetos não devem afetá-las;
- deve haver sempre a preocupação de que pessoas saibam que informações estão sendo escondidas no objeto.

Uma demonstração simples de esteganografia pode ser feita através do comando *echo* e de um arquivo no formato JPG ou JPEG (*Joint Photographic Experts Group*). A Figura 2.10 mostra a inserção da mensagem “senha de acesso 123456” no final do arquivo de imagem “bandeira.jpg”, utilizando um sistema operacional *Linux*.

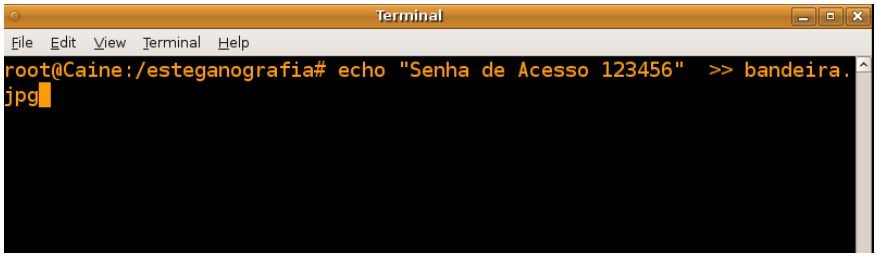


Figura 2.10: Ocultando dados em arquivo "JPG"

Na Figura 2.11, percebe-se que, após o procedimento, o arquivo “bandeira.jpg” não sofre alterações em sua visualização.

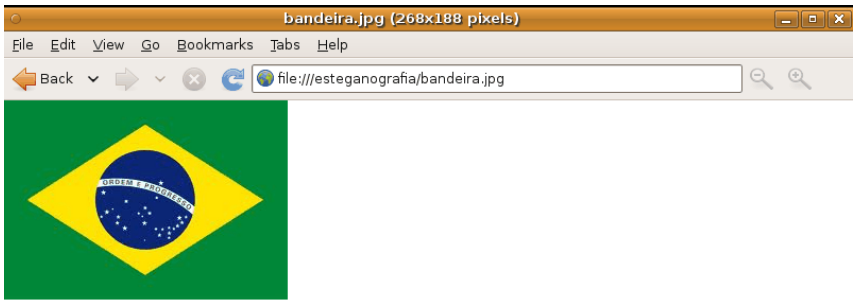


Figura 2.11: Visualização da imagem após a inserção dos dados

Entretanto, na Figura 2.12, através do comando *strings*, nativo do *Linux*, observa-se que o arquivo oculta as informações inseridas pelo comando *echo*.

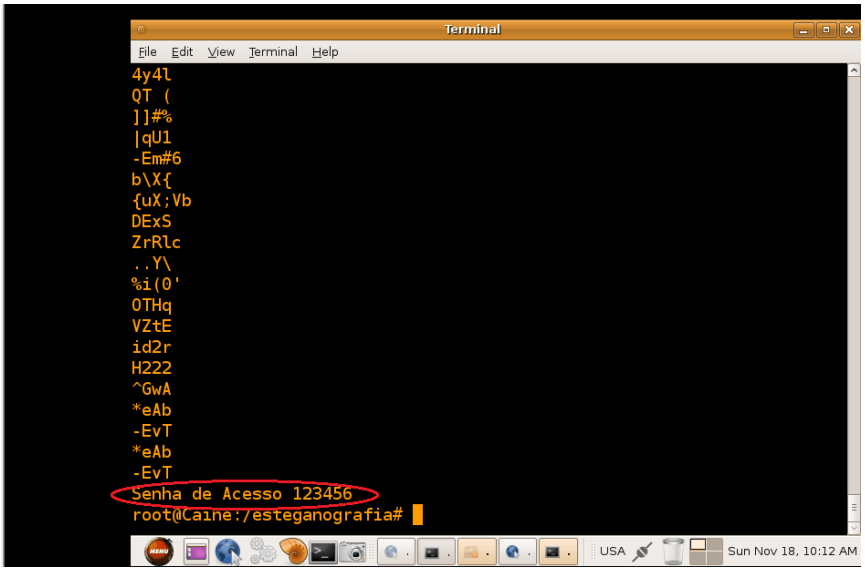


Figura 2.12: Visualização dos dados inseridos no arquivo

Detecção

O grande problema da esteganografia é a dificuldade de perceber que está sendo utilizada. Um documento pode ser incorporado a um arquivo de imagem e o perito pode não

perceber, mesmo visualizando-o. É impossível determinar através de um exame visual se um arquivo gráfico contém provas vitais incorporadas como dados ocultados (CRAIGER, POLLITT e SWAUGER, 2005).

O tratamento da esteganografia em exames periciais pode ser iniciado pela busca de ferramentas ou aplicações de esteganografia no computador do suspeito. A existência delas pode ser um forte indício do uso da técnica (CRAIGER, POLLITT e SWAUGER, 2005). Caso sejam encontradas, a tarefa seguinte é descobrir quais arquivos contêm informações escondidas. Uma forma de descobrir é indagar o suspeito. Caso ele se negue a dizer, ferramentas de detecção automatizada podem ser utilizadas, mesmo que não sejam tão eficazes (CRAIGER, POLLITT e SWAUGER, 2005). Uma das ferramentas que pode ser utilizada é o *Stegdetect*, que é gratuita e tenta descobrir se uma imagem contém dados escondidos.

2.2.1.7 Criptografia

A criptografia é considerada como a ciência e a arte de escrever mensagens de forma cifrada ou em código (CERT.br [E], 2012). A criptografia pode fazer com que artefatos digitais (texto, imagem vídeo, áudio etc.) fiquem ilegíveis (CRAIGER, POLLITT e SWAUGER, 2005). O processo é baseado em um algoritmo de criptografia e uma chave (senha). Com o algoritmo e a chaves são realizados cálculos para tornar arquivos ilegíveis (CRAIGER, POLLITT e SWAUGER, 2005). Para reverter o processo, é necessário conhecer o algoritmo utilizado e, principalmente e mais importante, a chave (CRAIGER, POLLITT e SWAUGER, 2005).

Na criptografia, a segurança do processo não está relacionada aos algoritmos, mas às chaves que os algoritmos recebem como parâmetro para cifrar e decifrar dados. A criptografia pode ser simétrica ou assimétr ica, onde a primeira utiliza a mesma chave para cifrar e decifrar, enquanto a segunda utiliza duas chaves diferentes (VECCHIA; WEBER e ZORZO, 2013). Em caso de perda da chave pelo proprietário do arquivo, provavelmente ninguém mais terá acesso ao seu conteúdo. O *Blowfish*, DES, 3DES, AES, *Serpent* e *Twofish* são exemplos de algoritmos de criptografia de chave simétrica e o RSA, TLS, ElGammal, PGP e Bitcoin são exemplos de criptografia assimétrica (VECCHIA, WEBER e ZORZO, 2013).

Hoje a criptografia está integrada ou pode ser adicionada à maioria dos sistemas operacionais e aplicativos (CERT.br [D], 2012). Por meio dela é possível:

- proteger arquivos sigilosos armazenados em computadores: um exemplo é o sistema de arquivos com criptografia (ou *Encrypting File System* - EFS), recurso da Microsoft, nativo em algumas versões do sistema operacional Windows. O EFS é um componente do sistema de arquivos NTFS que permite cifrar e decifrar arquivos usando um algoritmo de criptografia avançado (BRAGG, 2016);
- restringir o acesso a volumes do disco rígido: o *Bitlocker* é um exemplo. O *Bitlocker* é um recurso da Microsoft que permite que dados sejam protegidos mediante a criptografia de volumes (BITLOCKER, 2016). Com o *Bitlocker*, os dados ficam protegidos enquanto o sistema estiver *offline* (BITLOCKER, 2016);
- Prover sigilo na troca de dados em redes de computadores: o tráfego de rede pode ser cifrado utilizando protocolos padrões como SSL (*Secure Sockets Layer*), SSH (*Secure Shell*) ou TLS (*Transport Layer Security*) (BEER, STANDER e BELLE, 2014).

A criptografia é usada legalmente e legitimamente em negócios, indústria, governos, instituições militares e indivíduos para garantir a privacidade das informações. Infelizmente, ela também pode ser usada por criminosos para esconder o fruto de seus crimes (CRAIGER, POLLITT e SWAUGER, 2005). Nesse contexto, a criptografia é uma ferramenta extremamente poderosa para frustrar ações periciais (BEER, STANDER e BELLE, 2014), sendo considerada por peritos como o método antiforense mais preocupante, conforme pesquisa realizada (apêndice I).

Detecção

A criptografia pode ser detectada visivelmente em algumas situações e em outras com o uso de ferramentas forenses. Por exemplo, um volume criptografado com *BitLocker* pode ser percebido por um cadeado no volume, conforme Figura 2.13. Já em casos de criptografia em arquivos, há indicação de uso de aplicações forenses para automatizar o processo. Geralmente a detecção é feita pela análise de informações contidas nos cabeçalhos de todos os arquivos do disco para saber se estão cifrados (CRAIGER, POLLITT e SWAUGER, 2005). A ferramenta comercial FTK pode ser utilizada para auxiliar a identificação de arquivos criptografados. Quando se trata de criptografia, o desafio para as atividades periciais não é a detecção, que pode ser identificada muitas vezes visualmente, mas sim saber lidar com ela quando detectada.

Figura 2.13 - *Bitlocker* ativado

A seguir, são apresentadas algumas abordagens para tratar a criptografia quando detectada:

- persuadir o suspeito a fornecer a chave para decifrar os dados é o método mais fácil de superar a criptografia (CRAIGER, POLLITT e SWAUGER, 2005). O investigador deve pedir todas as senhas e chaves de criptografia usadas no computador (WOLFE, 2003). O grande problema é se o suspeito decidir não revelar as senhas/chaves ou alegar que esqueceu (HARGREAVES e CHIVERS, 2008);
- localizar cópias de dados não cifradas pode ser possível se durante o processo de criptografia os dados originais forem eliminados e não sobrescritos. Por exemplo, durante a criptografia, cópias dos dados originais podem ser deixadas em arquivos de paginação (*swap*), pastas temporárias, lixeira e espaços não alocados. Essa abordagem pode ser gravemente prejudicada caso o volume todo do disco seja cifrado, pois, neste caso, as cópias também seriam cifradas (HARGREAVES e CHIVERS, 2008).
- localizar chaves ou *passphrases* pode ser possível, pois muitas vezes estão armazenadas no próprio disco rígido ou em outras mídias de armazenamento de dados, localizadas na mesma área física da perícia. Por exemplo, o *software* de criptografia pode gravar a chave na memória RAM (*Random Access Memory*) e, posteriormente, durante uma operação de *swap*, ela pode ser gravada no disco rígido (CRAIGER, POLLITT e SWAUGER, 2005). Ou o suspeito pode gravar intencionalmente a senha em algum lugar do disco para evitar esquecê-la (HARGREAVES e CHIVERS, 2008). O software FTK pode automatizar o procedimento, gerando uma lista completa com palavras chave extraídas disco rígido do suspeito para depois serem testadas como possíveis senhas (HARGREAVES e CHIVERS, 2008).

- ataque de senha inteligente visa testar a força do mecanismo. A maioria das pessoas não cria chaves que sejam difíceis de adivinhar. A maior preocupação é que sejam capazes de sempre lembrar suas chaves (WOLFE, 2002). É provável que usuários usem senhas que tenham algum significado pessoal, pois assim serão lembradas facilmente, por exemplo, aniversários, nomes de crianças, animais etc. (CRAIGER, POLLITT e SWAUGER, 2005). Ferramentas podem ser utilizadas para testar frases e palavras derivadas de detalhes pessoais sobre o suspeito obtidas durante o inquérito (HARGREAVES e CHIVERS, 2008);
- uso de busca exaustiva (força bruta) para localizar a chave. O uso de uma chave muito grande pode inviabilizar o método, pois é improvável que as chaves sejam identificadas num tempo útil (HARGREAVES e CHIVERS, 2008);
- obtenção de imagens dos volumes criptografados quando ainda estão montados (HARGREAVES e CHIVERS, 2008). Essa prática pode se tornar complicada caso o volume seja muito grande;
- despejo da memória RAM do computador quando o volume ainda estiver montado (HARGREAVES e CHIVERS, 2008) para posterior tentativa de localização da chave.

Os métodos antiforenses apresentados, bem como as formas de detecção e tratamento, ilustram a necessidade de um processo que possa modelá-los e incluí-los no processo pericial. Pesquisa realizada (apêndice I) mostra que 18,8% dos peritos fazem uso de ferramentas ou métodos de tratamento de ameaças antiforenses sem critérios e 75% somente quando há suspeita ou identificação prévia de ameaças antiforense. Esses dados demostram que métodos antiforenses não estão sendo tratados ou técnicas de detecção estão sendo aplicadas desnecessariamente, contribuindo para a ideia de adoção de um processo bem definido para tratamento de ameaças antiforenses. Na seção 2.3 é apresentado um processo adotado no desenvolvimento de software para o tratamento de ameaças, que serve de referência para o modelo proposto.

2.3 MODELAGEM DE AMEAÇAS

A Modelagem de Ameaças é um assunto amplamente tratado no âmbito da segurança no desenvolvimento de *software* e tem como objetivo analisar a segurança de um aplicativo, identificando, quantificando e tratando riscos associados ao sistema de forma estruturada

(OWASP, 2015). Este capítulo abordará o assunto no âmbito do desenvolvimento de *software.*

A aplicação do processo de modelagem de ameaças atende à necessidade do mercado, que tem pressionado os fornecedores a adotarem um processo de desenvolvimento de *software* cada vez mais rigoroso no quesito segurança, com o objetivo de minimizar o número de vulnerabilidades, além de eliminá-las o mais cedo possível durante o ciclo de vida de desenvolvimento (LIPNER e HOWARD, 2005).

A Microsoft tem sido uma das defensoras dessa prática nos últimos anos, incluindo o procedimento dentro da etapa de projeto de seu ciclo de vida de desenvolvimento (ou *System Development Life-Cycle*), o que, segundo a empresa, foi um dos motivos para o aumento da segurança de seus produtos (OWASP, 2015). A empresa entende que, por meio do processo, é possível identificar e estimar, de maneira sistemática, as ameaças que mais atacam sistemas que necessitam resistir a ataques mal-intencionados (LIPNER e HOWARD, 2005). A documentação produzida durante o processo de Modelagem de Ameaças ajuda a compreender melhor o sistema e identificar as ameaças associadas a cada ponto de entrada da aplicação (OWASP, 2015).

Na literatura é possível encontrar diversas formas de conduzir um processo de Modelagem de Ameaças, conforme pode ser visto em SANS (2005), OWASP (2015), Meier et. al. (2003), Shostack (2014), Sindre e Opdahl (2005), entre outros. Cada modelo é criado segundo as necessidades e estrutura de cada organização, o que impede uma comparação direta de sua eficácia e qualidade.

Por exemplo, segundo Myagmar (2005), o processo de Modelagem de Ameaças consiste em três grandes etapas: caracterização do sistema, identificação de ativos e pontos de acesso e identificação de ameaças.

A caracterização do sistema visa entender completamente o seu funcionamento, definindo cenários de uso, de forma a revelar suas características essenciais. O entendimento do sistema é fundamental para compreender o que o invasor quer. No caso de desenvolvimento de *software*, o uso de Diagrama de Fluxo de Dados (DFD) é indicado para auxiliar o processo (MYAGMAR, 2005).

Para a identificação de ativos, é necessário ter em mente que eles são essencialmente alvos de uma ameaça, portanto o sistema precisa protegê-los, e que pontos de acesso podem

ser usados para acessá-los. Como exemplo, pode-se considerar os dados de uma aplicação um "ativo" e o sistema de arquivos um "ponto de acesso" (MYAGMAR, 2005).

A etapa de "identificação de ameaças" tem como principal objetivo identificar as ameaças ao sistema utilizando as informações recolhidas nas etapas anteriores (MYAGMAR, 2005). Normalmente, algumas ameaças são facilmente identificadas desde o início do processo de "Modelagem de Ameaças", em decorrência da semelhança com outros sistemas. Para entendimento dessa etapa, é fundamental compreender o que são ameaças ao sistema, como se manifestam e como podem ser identificadas, assuntos que serão tratados nas seções 2.3.1 e 2.3.2.

O processo de modelagem de ameaças não deve se concentrar somente na identificação das ameaças, mas também na definição da criticidade delas (MYAGMAR, 2005), que é obtida por meio de uma avaliação de risco, necessária para mapear cada ameaça a uma medida de mitigação ou simplesmente subsidiar a decisão de aceitar o risco da ameaça (MYAGMAR, 2005). Esse assunto será abordado na seção 2.3.3.

A partir do processo de modelagem de ameaças, requisitos de segurança do *software* poderão ser definidos. Uma vez definidos, os mecanismos de segurança são desenvolvidos seguindo ao ciclo geral do projeto de engenharia de *software*: implementar, testar e manter. A Figura 2.14 apresenta uma visão do processo de engenharia de segurança com a aplicação do processo de modelagem de ameaças.

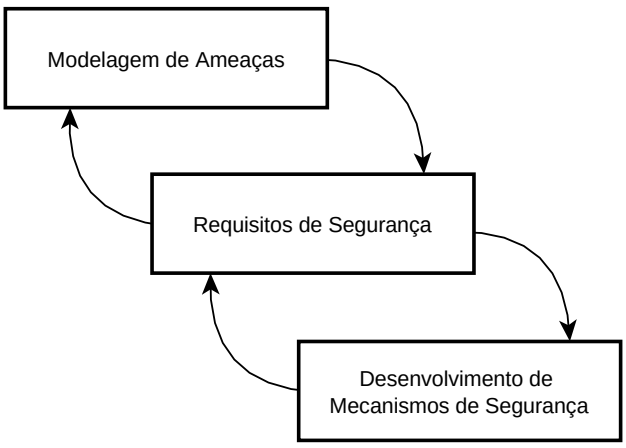


Figura 2.14: Engenharia de segurança do sistema (MYAGMAR, 2005)

2.3.1 Ameaças ao sistema

A ameaça é uma causa potencial de um incidente indesejado, que caso se concretize pode resultar em dano (NIST, 2002).

Com o desenvolvimento das tecnologias de informação e comunicação e com o aumento do acesso à Internet, os sistemas são frequentemente expostos a vários tipos de ameaças que podem causar diferentes tipos de danos e levar a perdas financeiras significativas. Algumas ameaças podem afetar a confidencialidade ou a integridade dos dados, enquanto outras afetam a disponibilidade de um sistema (JOUINI et al., 2014).

Os sistemas podem apresentar dois pontos capazes de contribuir para a manifestação de uma ameaça. O primeiro ponto está relacionado à existência de pelo menos uma vulnerabilidade a ser explorada no sistema. A vulnerabilidade pode estar relacionada ao *hardware*, ao sistema operacional ou à aplicação. O segundo ponto é que o sistema deve ter uma importância significativa para a organização, a ponto de a perda ou a degradação de sua disponibilidade, confidencialidade ou integridade causarem impacto considerável sobre o negócio da organização, ou pelo fato ser o único alvo à disposição de atacantes (JONES, 2002).

As ameaças podem manifestar-se através de um agente de ameaça usando uma técnica maliciosa (ALHABEEB et. al., 2010). Segundo Jones (2002), esses agentes são chamados de agentes de ameaças maliciosas e serão tratados na seção 2.3.1.1.

Segundo Jouini et. al. (2014), as ameaças podem ser definidas de duas formas: técnicas que os atacantes usam para explorar uma vulnerabilidade no sistema ou o impacto das ameaças aos ativos do sistema. Portanto, segundo os autores, as ameaças podem ser categorizadas baseadas em dois tipos de abordagem de classificação:

- métodos de classificação baseados em técnicas de ataque;
- métodos de classificação baseados nos impactos das ameaças.

Na seção 2.3.2 será apresentado um método de classificação das ameaças baseado em seus impactos, o STRIDE. O método foi desenvolvido pela empresa Microsoft e é muito utilizado para a identificação de ameaças no processo de desenvolvimento de *software.*

2.3.1.1 Agente de ameaças maliciosas

Um agente de ameaça malicioso pode ser um grupo ou combinações de grupos de indivíduos que tenham a intenção de causar impactos negativos a um sistema (JONES, 2002; VIDALIS e JONES, 2005). A Figura 2.15 mostra alguns deles.

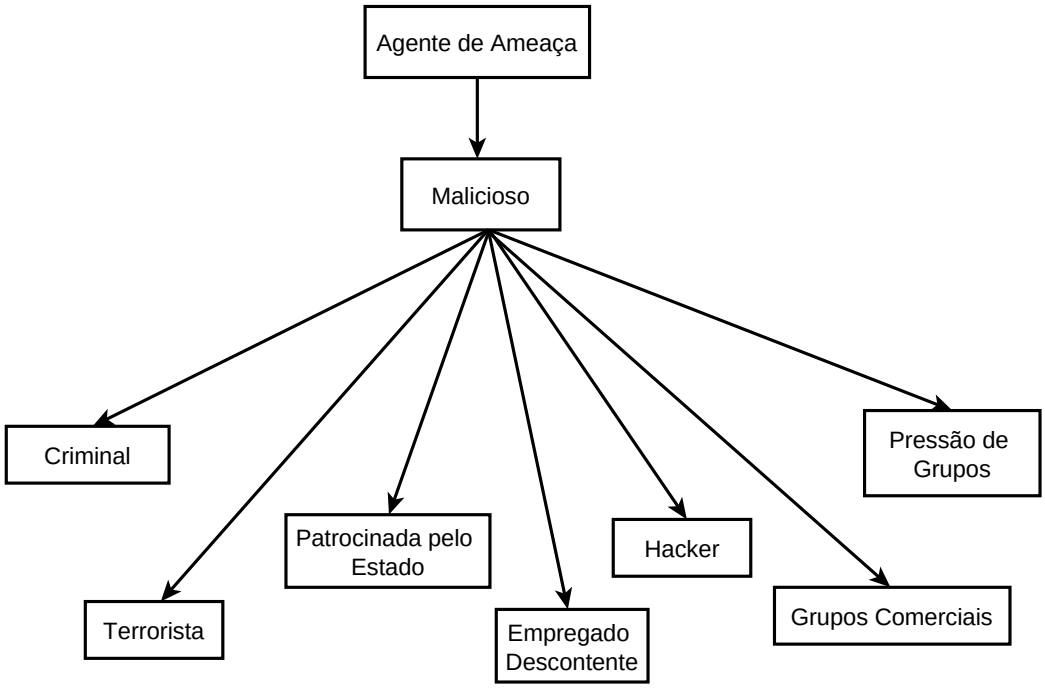


Figura 2.15: Componentes do agente de ameaça malicioso, adaptada de Jones (2002)

Cada um desses grupos está relacionado a atividades que podem tornar-se uma ameaça ao sistema. Por exemplo, grupos criminosos são ameaças nas seguintes situações (JONES, 2002):

- tentando acessar o sistema para fraudar recursos (dinheiro ou bens) de alguém;
- impedindo a detecção e investigação de outras atividades criminosas;
- obtendo informações que lhes permitam cometer outros crimes;
- tendo acesso a informações pessoais que lhes permitam cometer outros crimes (roubo de identidade, chantagem, perseguição, assédio etc.).

Para torna-se uma ameaça efetiva a um sistema, um agente de ameaça maliciosa é influenciado por alguns elementos (JONES, 2002). A Figura 2.16 apresenta cada um deles e suas relações.

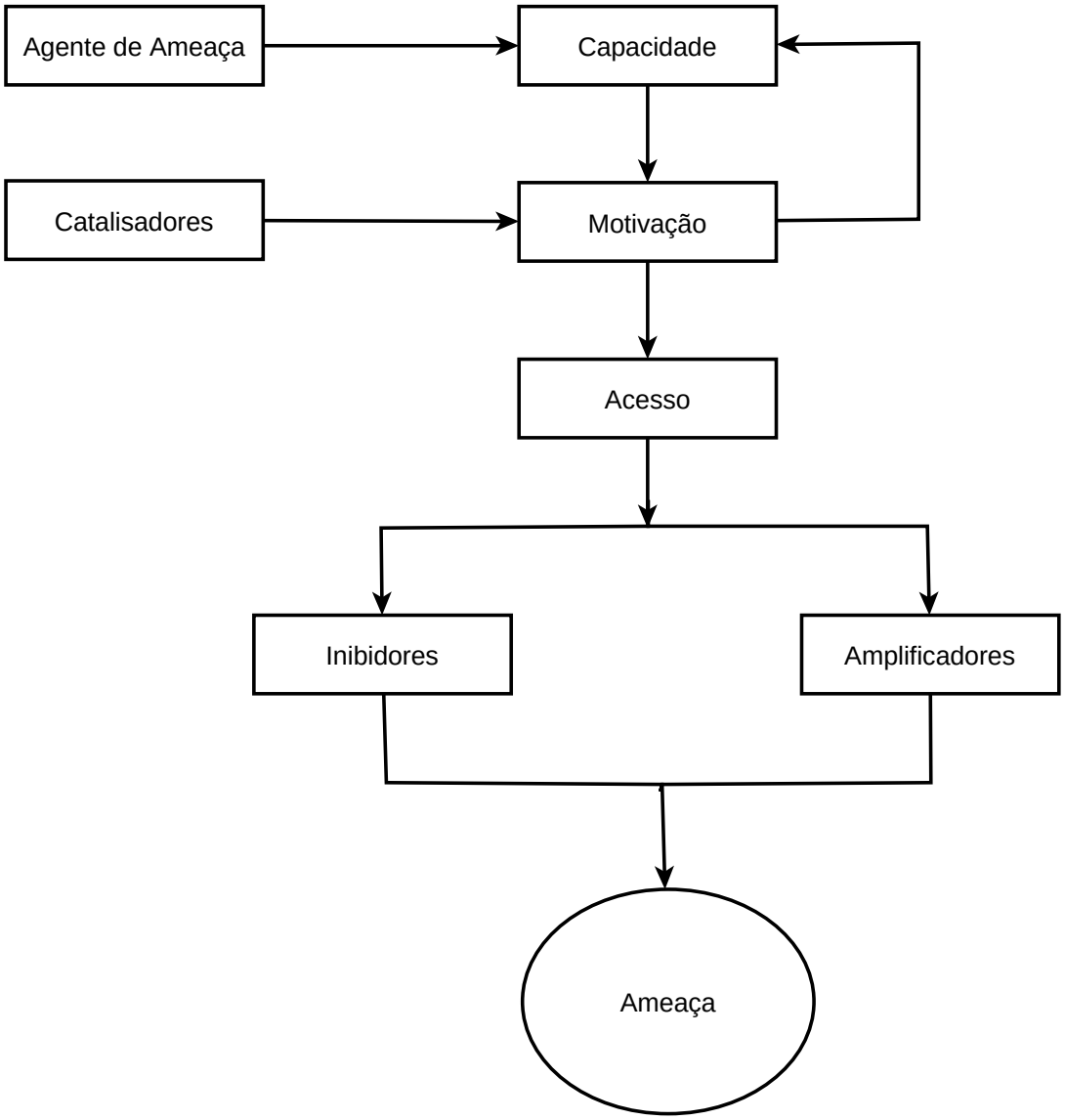


Figura 2.16: Elementos de ameaça e seus relacionamentos, adaptada de Jones (2002)

A Figura 2.16 mostra que para representar uma ameaça, um agente de ameaça deve estar capacitado e motivado e precisa ter acesso suficiente ao sistema. Entretanto, o agente pode ser enfraquecido por fatores que inibem sua capacidade (inibidores) e fortalecido por outros (amplificadores). Além disso, elementos catalisadores podem influenciar a sua ação, dependendo da motivação. A seguir são apresentados cada um desses elementos segundo Jones (2002).

Capacidade

Para que um agente de ameaça maliciosa seja eficaz, deve possuir a capacidade de conduzir e sustentar um ataque ou de destruir totalmente um sistema. Para isso, e para que seja bem-sucedido, ele deve ter os meios, as habilidades e os métodos necessários. A Figura 2.17 mostra alguns elementos que influenciam a capacidade.

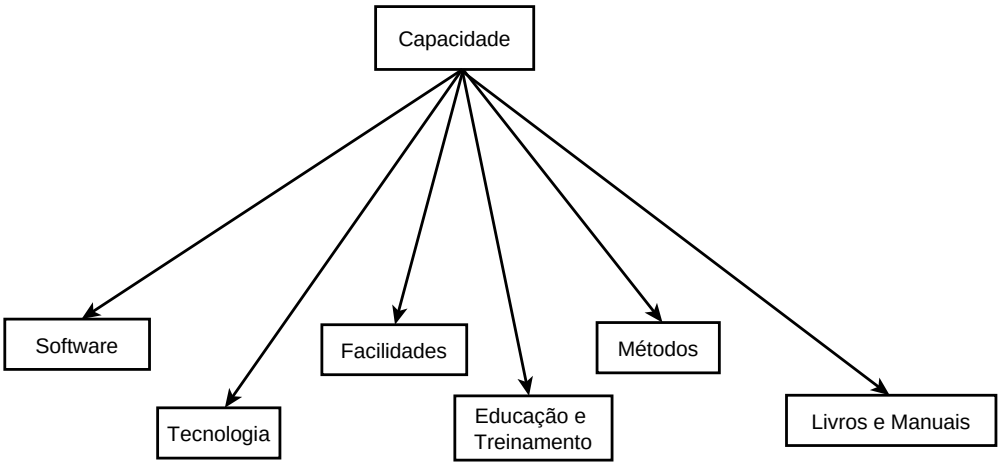


Figura 2.17: Componentes de capacidade, adaptada de Jones (2002)

Motivação

A motivação de um agente é subjetiva e pode ser influenciada por uma série de fatores relacionados ao perfil dos agentes de ameaças ou pela combinação deles. A Figura 2.18 indica alguns elementos que podem afetar a motivação.

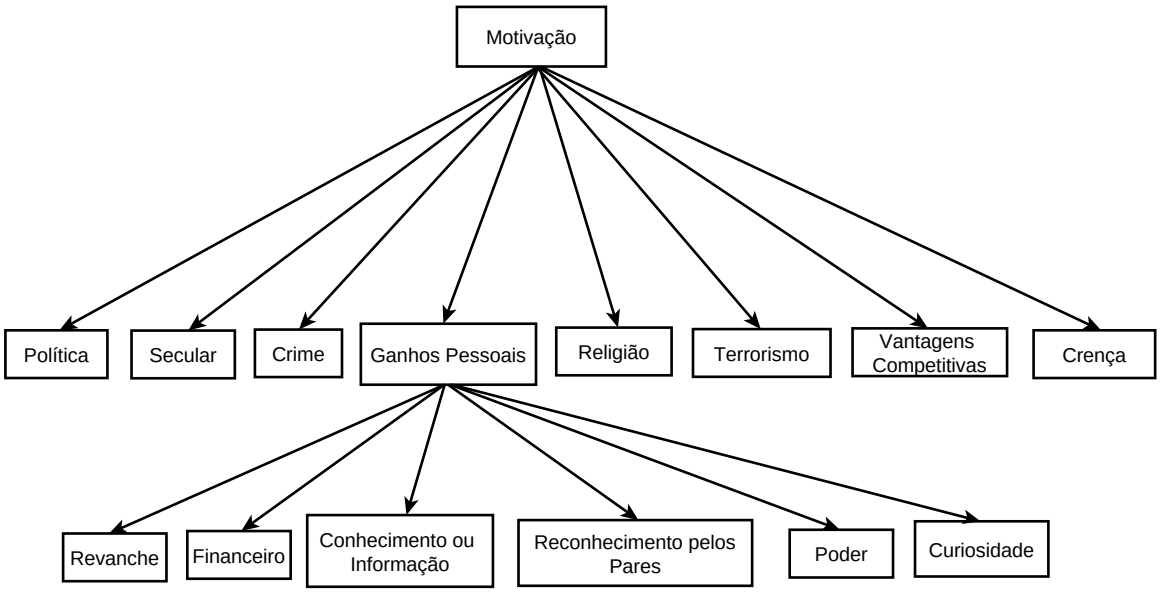


Figura 2.18: Componentes de motivação, adaptada de Jones (2002)

Acesso

Um agente de ameaça não pode iniciar um ataque sem ter acesso ao sistema. Esse acesso pode ser realizado diretamente no sistema ou via rede.

Inibidores e Amplificadores

Alguns fatores podem inibir ou potencializar um agente de ameaça de realizar um ataque bem-sucedido, sendo denominados de fatores inibidores ou amplificadores

respectivamente. Entretanto, alguns deles podem agir em ambas as situações. Por exemplo, medidas de segurança em um sistema, se fracas, incentivarão um atacante a montar um ataque e, se fortes, impedirão a ação de um atacante.

Fatores inibidores podem impedir um agente de ameaça de iniciar ou realizar um ataque, ou podem minimizar o impacto de um ataque bem-sucedido ou ainda influenciar na intenção de um agente de ameaça de iniciar um ataque. A Figura 2.19 mostra alguns fatores inibidores.

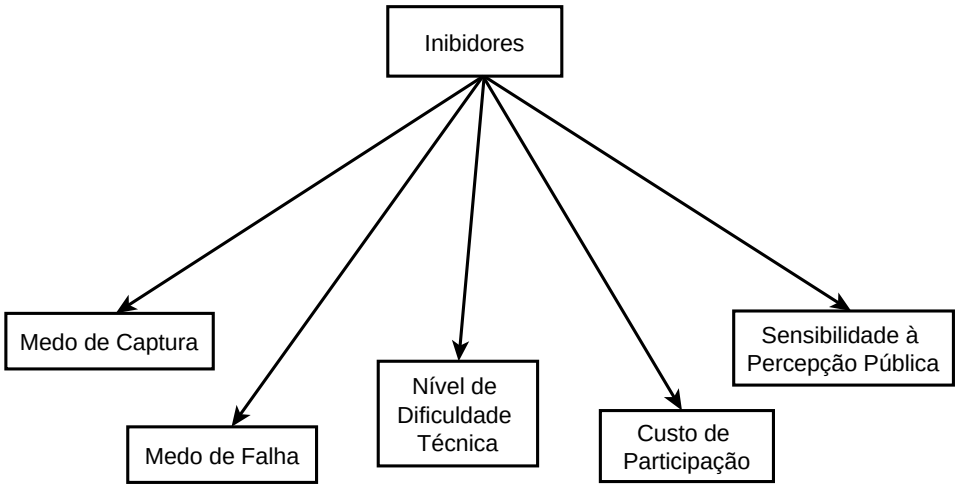


Figura 2.19: Componentes inibidores, adaptada de Jones (2002)

Já fatores amplificadores são influências que podem contribuir para a ocorrência de um ataque. A Figura 2.20 mostra alguns fatores inibidores.

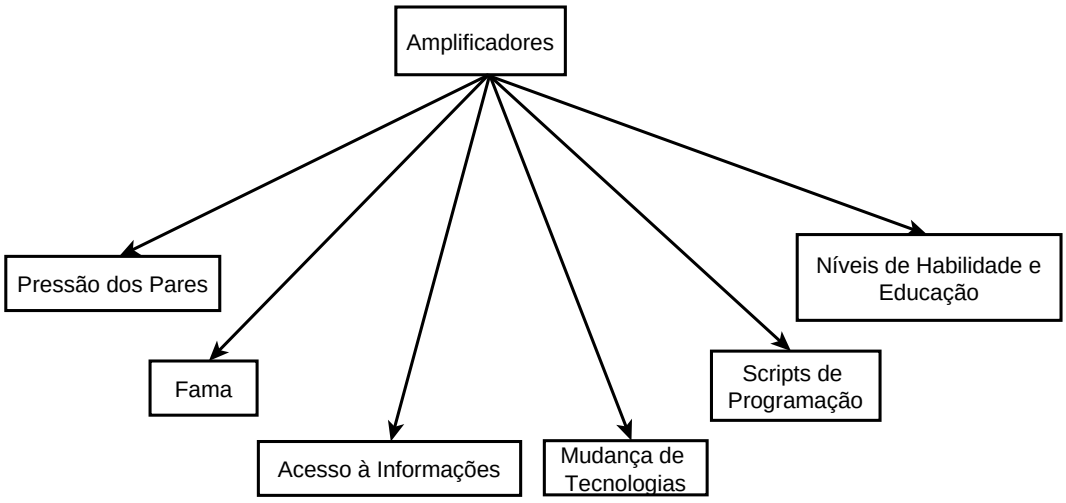


Figura 2.20: Componentes amplificadores, adaptada de Jones (2002)

O desejo de ser reconhecido e respeitado por seus colegas ou amigos por meio da demonstração de suas habilidades são tipos de influências que podem reforçar a vontade de realizar o ataque. O nível de instrução e de habilidade que um agente de ameaça possui ou ao qual pode ter acesso pode melhorar sua confiança e aumentar a probabilidade de sucesso. O acesso a informações sobre o alvo, organizações ou a *scripts* de programação voltados à execução de ataque permitem a montagem de um ataque com boas possibilidades de sucesso.

Catalisadores

Os catalisadores estão relacionados a fatores ou a ações que influenciam o momento de realizar um ataque. A Figura 2.21 mostra alguns fatores que podem agir como catalisadores.

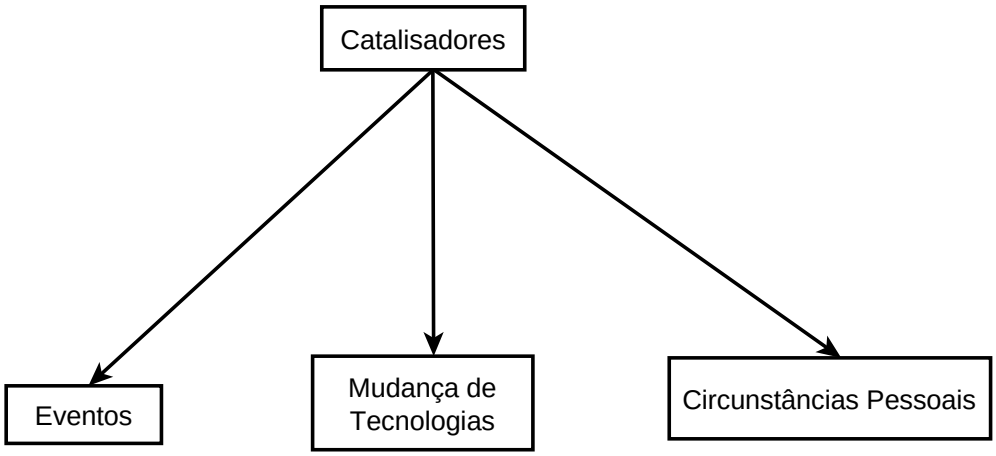


Figura 2.21 - Componentes catalisadores, adaptada de Jones (2002)

O resultado de um evento, como a publicidade para uma organização com a qual o agente está em desacordo ou questões pessoais podem afetar sua capacidade ou vontade de realizar um ataque. O aparecimento de novas tecnologias pode criar possibilidades de afetar alvos que antes pareciam impossíveis.

2.3.2 Identificação de ameaças

Um dos métodos mais observados para a identificação de ameaças é o STRIDE, conforme pode ser visto em Ingalsbe; Shoemaker e Mead (2011), Khajeh-Hosseini et.al. (2012), Shostack (2014), Sans (2005), Myagmar (2005), entre outros. O método consiste em pensar nas ameaças com foco no atacante, tendo como base as seis categorias a seguir (MEIER, et al., 2003):

- ***S****POOFING* (Falsificação): é uma forma de se ter acesso ao sistema usando uma identifidade falsa, como por exemplo, utilizando um endereço de IP falso;
- ***T****AMPERING* (Manipulação): é a modificação de dados sem a devida autorização, por exemplo, durante a troca de dados entre dois computadores em rede;
- ***R****EPUDIATION* (Repúdio): é a negação de ações ou transações específicas por parte de usuários, independentemente de serem ou não os verdadeiros autores;
- ***I****NFORMATION DISCLOSURE* (Revelação de Informações): é a divulgação de informações privadas, como exemplo de vulnerabilidade, como deixar que detalhes internos do sistema sejam revelados ao cliente, o que pode ser muito útil para um ataque;
- ***D****ENIAL OF SERVICE* (Negação de Serviço): é uma tentativa de deixar uma aplicação ou sistema indisponível através de uma sobrecarga. Por exemplo, um ataque pode ser feito através da obstrução de um meio de comunicação;
- ***E****LEVATION OF PRIVILEGE* (Elevação de Privilégio): tem como objetivo transformar um usuário com privilégios limitados em um usuário privilegiado para ganhar acesso a uma aplicação, com o intuito de comprometer o sistema.

Com o método, as ameaças são identificadas fazendo-se perguntas a cada aspecto da arquitetura e *design* da aplicação. Por exemplo, um invasor pode modificar uma credencial para acessar a aplicação (MEIER, et al., 2003)?

2.3.3 Avaliação de riscos

O processo de avaliação de riscos possibilita um entendimento dos riscos, suas causas, consequências e probabilidades (ISO, 2012). Essa avaliação é fundamental, pois nem sempre é viável tratar todas as ameaças tendo em vista os recursos disponíveis, incluindo o tempo.

Segundo a NBR ISO/IEC 31010:2012, o processo de avaliação de riscos inclui os seguintes benefícios:

- entender o risco e seu potencial sobre os objetivos;
- contribuir para o entendimento dos riscos a fim de auxiliar na seleção das opções de tratamento;

- identificar os principais fatores que contribuem para os riscos e os elos fracos em sistemas e organizações;
- auxiliar no estabelecimento de prioridades;
- selecionar diferentes formas de tratamento de riscos;
- fornecer informações que ajudarão a avaliar a conveniência da aceitação de riscos quando comparados com critérios predefinidos.

A saída desse processo ajuda a identificar os controles apropriados para reduzir ou eliminar o risco durante o processo de mitigação de risco (NIST, 2002). A avaliação de riscos é composta por três etapas importantes: determinação de risco, identificação de contramedidas e mitigação de risco. Esses processos serão tratados nas seções 2.3.4, 2.3.5 e 2.3.6.

2.3.4 Determinação de riscos

A determinação do potencial de risco é uma das principais etapas de um processo de avaliação de risco e a partir dele é possível estabelecer prioridades e propor formas de tratamento. Na literatura são encontradas diversas formas de determiná-lo. Nas seções 2.3.4.1, 2.3.4.2 e 2.3.4.3 são apresentadas algumas abordagens.

2.3.4.1 Probabilidade e Impacto

Nessa abordagem, o risco é determinado com a combinação de valores de probabilidade e impacto numa matriz de risco. Para exemplificar o processo, é utilizada como referência a publicação SP 800-30 do NIST (NIST, 2002).

NIST 800-30

A documentação estabelece um padrão de gerenciamento de risco para sistemas de tecnologia da informação baseado em elementos relacionados à probabilidade e impacto para determinação do risco. A probabilidade está relacionada à possibilidade de um agente de ameaça[7] explorar uma determinada vulnerabilidade e o impacto às consequências que essa ação pode causar sobre um ponto de vista organizacional.

O processo inicia com a determinação da probabilidade, que poderá ser alta, média ou baixa, conforme Tabela 2.4. Para determinação do nível devem ser levados em consideração

[7] Qualquer circunstância ou evento com potencial para prejudicar um sistema de tecnologia da informação (NIST, 2002).

os seguintes fatores:

- motivação e capacidade da fonte da ameaça;
- natureza ou origem da vulnerabilidade;
- existência e eficácia de controles.

Tabela 2.4: Definições de níveis de probabilidade (NIST, 2002)

	Definição de Probabilidade
Alta	A motivação da fonte da ameaça é altíssima e suficientemente capaz e os controles são ineficientes.
Média	A fonte da ameaça está motivada e é capaz, mas controles impedem que a vulnerabilidade seja explorada.
Baixa	A fonte da ameaça não está motivada ou não é capaz, ou existem controles de prevenção, ou aptos a impedir, pelo menos, significativamente, que a vulnerabilidade seja explorada.

Em seguida, estima-se o impacto que também pode ser alto, médio ou baixo, conforme Tabela 2.5. Para a análise do impacto, as seguintes informações precisam ser obtidas:

- missão do sistema (processos realizados pelo sistema);
- criticidade dos dados e do sistema (importância para a organização);
- sensibilidade dos dados e do sistema.

Tabela 2.5: Definições dos níveis de impacto (NIST, 2002)

	Definição de Impacto
Alta	A exploração da vulnerabilidade pode gerar grandes perdas financeiras de ativos e recursos; pode violar, prejudicar ou impedir significativamente a missão da organização, a reputação ou resultar em perda de interesse ou em morte ou ferimentos graves de pessoas.
Média	A exploração da vulnerabilidade pode gerar perdas financeiras de ativos e recursos; pode violar, prejudicar ou impedir significativamente a missão da organização, a reputação ou resultar em perda de interesse ou, em morte ou ferimentos graves de pessoas.
Baixa	A exploração da vulnerabilidade pode resultar na perda de alguns ativos tangíveis ou recursos ou pode afetar significativamente uma organização, missão, reputação, ou interesse.

Por fim, o risco é obtido com a multiplicação da probabilidade pelo impacto, conforme apresentado na Tabela 2.6. O risco resultante poderá ser alto (entre 50 e 100), médio (de 10 a 50) ou baixo (1 a 10). Estabelecido o nível de risco, a Tabela 2.7 apresenta ações necessárias para cada um.

Tabela 2.6: Matriz de risco, adaptada de NIST (2002)

Probabilidade x Impacto				
Probabilidade	ALTO (1.0)	**Baixo** (1.0 x 10 = 10)	**Médio** (1.0 x 50 = 50)	**Alto** (1.0 x 100 = 100)
	MÉDIO (0.5)	**Baixo** (0.5 x 10 = 5)	**Médio** (0.5 x 50 = 25)	**Médio** (0.5 x 100 = 50)
	BAIXO (0.1)	**Baixo** (0.1 x 10 = 1)	**Baixo** (0.1 x 50 = 5)	**Baixo** (0.1 x 100 = 10)
		BAIXA (10)	MÉDIA (50)	ALTA(100)
	Impacto			

Tabela 2.7 - Níveis de risco e ações necessárias (NIST, 2002)

Nível de Risco	Ações
Alto	Existe forte necessidade de medidas corretivas. Um sistema existente pode continuar a operar, mas um plano de ação corretiva deve ser posto em prática o mais rápido possível.
Médio	Necessidade de ações corretivas e de desenvolvimento de um plano para incorporá-las dentro de um período razoável de tempo.
Baixo	O gerente do sistema deve decidir se as ações corretivas ainda são necessárias ou se deve-se aceitar o risco.

2.3.4.2 DREAD

O modelo DREAD é composto por cinco categorias, cujas iniciais dão origem à sigla (MEIER, et al., 2003). O risco é estimado fazendo-se perguntas em cada uma das categorias, conforme abaixo:

- ***D****amage potential* (Potencial de Danos): Qual o tamanho do dano se a vulnerabilidade for explorada?
- ***R****eproducibility* (Capacidade de Reprodução): Com que facilidade um ataque é reproduzido?
- ***E****xploitability* (Capacidade de Exploração): Com que facilidade um ataque é lançado?
- ***A****ffected* users (Usuários afetados): Quantos usuários são afetados?

- ***D****iscoverability* (Descoberta): Com que facilidade é encontrada a vulnerabilidade?

Quando determinada ameaça é avaliada através de DREAD, cada categoria recebe uma estimativa. A Tabela 2.8 mostra um exemplo de tabela de estimativa na qual cada categoria pode ser classificada como alta (3), média (2) ou baixa (1). A escolha da classificação dependerá do resultado das respostas às perguntas (MEIER, et al., 2003).

Tabela 2.8: Tabela de estimativa de ameaças, adaptada de Meier et al. (2003)

	Estimativa	**Alta (3)**	**Média (2)**	**Baixa (1)**
D	Potencial de Danos (*Damage potential*)	O invasor pode subverter o sistema de segurança; obter autorização completa; executar como administrador; *upload* de conteúdo.	Vazamento de informações confidenciais.	Vazamento de informações triviais.
R	Capacidade de Reprodução (*Reproducibility*)	O ataque pode ser reproduzido a toda hora e não requer uma janela de tempo.	O ataque pode ser reproduzido, mas somente com janela de tempo e situação particular.	O ataque é muito difícil de ser reproduzido, mesmo com vasto conhecimento de segurança.
E	Capacidade de Exploração (*Exploitability*)	Um programador novato pode fazer o ataque em curto espaço de tempo.	Um programador habilidoso pode atacar e depois repetir os passos.	O ataque requer uma pessoa muito capacitada para explorar.
A	Usuários Afetados (*Affected users*)	Todos os usuários, configuração padrão e principais clientes.	Alguns usuários, configuração não padrão.	Porcentagem muito pequena de usuários, recursos obscuros, afeta usuários anônimos
D	Descoberta (*Discoverability)*	Informações publicadas explicam os ataques. A vulnerabilidade é encontrada no recurso mais comumente usado e é muito divulgado.	A vulnerabilidade está numa parte raramente usada do produto. Apenas alguns usuários vão se deparar com ela. É preciso analisar muito para ver o uso malicioso.	O *bug* é obscuro e é improvável que usuários descubram a vulnerabilidade.

A soma da pontuação obtida em cada categoria de DREAD poderá variar de 5 a 15. A pontuação total servirá para estimar o risco da ameaça. Se a pontuação estiver entre 12 e 15, considera-se alto risco, entre 8 e 11 médio risco e entre 5 e 7 baixo risco (MEIER, et al., 2003). A tabela 2.9 mostra um exemplo da aplicação da tabela de estimativa.

Tabela 2.9: Estimativa DREAD, adaptada de Meier et al. (2003)

	D	**R**	**E**	**A**	**D**	**Total**	**Estimativa**
Ameaça 01	3	3	1	1	3	11	Médio

É importante notar no exemplo acima que, se se pensar no DREAD em termos de Probabilidade e Impacto para estimativa de risco, os dois fatores teriam pesos distintos, visto que a probabilidade está relacionada a três categorias (“Capacidade de Reprodução”, “Capacidade de Exploração” e “Descoberta”) e o Impacto a apenas duas (Potencial de Danos e Usuários Afetados) (OWASP, 2015).

Em 2010, o DREAD parou de ser recomendado pela equipe do SDL (*Security Development Lifecycle* - Ciclo de Vida do Desenvolvimento da Segurança) da Microsoft, pois era muito subjetivo e gerava resultados pouco confiáveis em muitas situações (SHOSTACK, 2014).

2.3.4.3 Bug Bar

Como parte da modelagem de ameaças, em seu processo de desenvolvimento de *software*, atualmente a Microsoft tem adotado a abordagem de *Bug B*ar para definir o nível de risco de uma ameaça. O processo tem como objetivo classificar as ameaças com base em seus efeitos.

O processo utiliza o modelo STRIDE acrescido de informações extras em cada categoria para determinação do nível de gravidade. Por exemplo, no caso de um ataque de negação de serviço, é importante saber quem o executou e também quanto tempo vai durar. Dependendo das respostas, a gravidade pode variar. A partir da combinação das categorias com essas informações, níveis de gravidade são atribuídos à *Bug Bar*. Os níveis não devem ser modificados durante o projeto. A gravidade será determinada tendo como base as informações da *Bug Bar* (SULLIVAN, 2010). A Tabela 2.10 mostra um exemplo de uma *Bug Bar*.

Tabela 2.10: Exemplo de *Bug Bar* de segurança (SULLIVAN, 2010)

Categorias STRIDE	Cliente / Servidor	Escopo	Severidade
Falsificação (*Spoofing*)	Cliente	Capacidade de um invasor de apresentar uma *interface* de usuário falsa, mas visualmente idêntica à interface na qual os usuários devem basear-se para tomar decisões de confiança válidas em um cenário padrão. Uma decisão de confiança é definida por uma ação tomada por um usuário por acreditar que algumas informações estão sendo apresentadas por uma entidade específica (sistema ou alguma fonte de local específico ou remoto).	Importante
		Capacidade de um invasor de apresentar uma *interface* de usuário falsa, mas visualmente idêntica à *interface* à qual os usuários estão acostumados a confiar em um cenário específico. Entende-se como "acostumado a confiar", a qualquer coisa na qual um usuário está normalmente familiarizado com base na interação normal com o sistema operacional ou aplicativo, mas não pensa como uma "decisão de confiança".	Moderado
		Capacidade de um invasor de apresentar uma interface de usuário falsa, mas visualmente idêntica à interface do usuário, que é uma única parte de um cenário de ataque maior.	Baixa
	Servidor	Computador conectado a um servidor é capaz de mascarar-se como um usuário diferente ou computador utilizando um protocolo projetado e comercializado para prover autenticação forte.	Importante
		Usuário ou computador cliente é capaz de mascarar-se como um usuário ou computador aleatório através de um protocolo que é projetado e comercializado para fornecer autenticação forte.	Moderada
Manipulação\ Repúdio (*Tampering / Repudiation*)	Cliente	Modificação permanente de dados do usuário ou dados usados para tomar decisões de confiança em um cenário comum ou padrão que persiste após a reinicialização de aplicativos/Sistema Operacional.	Importante
		Modificações temporárias de qualquer dado que não persiste depois de reiniciado o sistema operacional/aplicativo.	Baixa
	Servidor	Modificação permanente de dados do usuário ou dados usados para tomada de decisões de confiança em um cenário comum ou padrão que persiste depois de reiniciado o sistema operacional/aplicativo.	Importante
		Modificação permanente de dados do usuário ou dados usados para tomada de decisões de confiança em um cenário específico que persiste depois de reiniciado o sistema operacional/aplicativo.	Moderado
		Modificações temporárias de dados em um cenário comum ou padrão que não persiste depois de reiniciado o sistema operacional/aplicativo.	Moderado
		Modificações temporárias de dados em um cenário específico que não persiste depois de reiniciado o	Baixo

		sistema operacional/aplicativo.	
Revelação de informações (*Information Disclosure*)	Cliente	Casos em que o invasor pode localizar e ler as informações no sistema, incluindo informações que não estavam previstas ou projetadas para serem expostas.	Importante
		Casos em que o invasor pode ler informações do sistema em locais conhecidos, incluindo informações que não estavam previstas ou projetadas para serem expostas.	Moderado
		Qualquer divulgação de informações não visadas (isto é, divulgação de dados aleatórios).	Baixa
	Servidor	Casos em que o invasor pode localizar e ler informações de qualquer lugar no sistema, incluindo as informações que não estavam previstas ou projetadas para serem expostas.	Importante
		Casos em que invasor pode facilmente ler as informações no sistema em locais conhecidos, incluindo informações que não estavam previstas ou projetadas para serem expostas.	Moderado
		Qualquer divulgação de informações não visadas (por exemplo, divulgação de dados aleatórios) incluindo dados de tempo de execução.	Baixa
Negação de Serviço (*Denial of Service*)	Cliente	"Negação de serviço de sistema corrompido": requer a reinstalação do sistema e/ou componentes.	Importante
		"Negação de serviço permanente": requer o reinicialização ou provoca tela azul/*Bug Check*.	Moderada
		"Negação de serviço temporária": requer a reinicialização do aplicativo.	Baixa
	Servidor	Anônimo, deve ser "fácil de explorar" através do envio uma pequena quantidade de dados ou caso contrário, ser induzido rapidamente.	Importante
		Anônimo, negação de serviço temporária sem amplificação de uma instalação padrão/comum.	Moderado
		Autenticado, negação de serviço permanente.	Moderado
		Autenticado, negação de serviço temporária com amplificação de uma instalação padrão/comum.	Moderado
Elevação de Privilégio (*Elevation of Privilege*)	Cliente	Usuário remoto, a capacidade de executar código arbitrário ou de obter mais privilégios que o previsto.	Fundamental
		Usuário remoto, a execução de código arbitrário com ampla ação do usuário.	Importante
		Usuário local, de baixo privilégio pode elevar-se para outro usuário, administrador ou sistema local.	Importante
	Servidor	Usuário remoto anônimo, a capacidade de executar código arbitrário *ou* de obter mais privilégios que o previsto.	Crítico
		Usuário remoto autenticado, a capacidade de executar código arbitrário *ou* de obter mais privilégios que o previsto.	Importante
		Usuário local autenticado, a capacidade de executar código arbitrário *ou* de obter mais	Importante

		privilégios que o previsto.	

No exemplo acima, em cada categoria da STRIDE, através da coluna Escopo, são mencionadas possibilidades em que o ataque pode ocorrer, bem como suas consequências. Além disso, na coluna Servidor/Cliente, é informado se o efeito do *bug* afetará o lado cliente ou servidor da aplicação. Essas informações extras servem de base para estimar a gravidade em cada uma das situações.

2.3.5 identificação de contramedidas

Esse processo visa identificar se existe algum controle de segurança que pode ser adotado para minimizar ou eliminar a ação de ameaças identificadas durante o processo de modelagem.

Para esse processo, o método STRIDE também pode ser utilizado como referência. Cada categoria descrita no STRIDE tem um conjunto de técnicas de contramedidas que podem ser usadas para reduzir o risco (MEIER, et al., 2003). A Tabela 2.11 mostra algumas delas.

Tabela 2.11: Ameaças STRIDE e contramedidas (MEIER, et al., 2003)

Categorias	Contramedidas
Falsificação de identidade de usuário (*Spoofing*)	Usar autenticação forte Não armazenar senha em texto simples (*plaintext)* Não enviar senha em texto simples pela rede cabeada Proteger *cookies* de autenticação com SSL (*Secure Sockets Layer*)
Manipulação com dados (*Tampering)*	Usar *hashing* de dados e assinatura Usar assinaturas digitais Usar autorização forte Usar protocolos resistentes à adulteração em *links* de comunicação *Links* de comunicação seguros com o uso de protocolos que fornecem integridade à mensagem
Repúdio (*Repudiation*)	Criar "trilhas" de auditoria segura Usar assinaturas digitais
Revelação de informações (*Information Disclosure*)	Usar autorização forte Usar algoritmos de encriptação fortes Utilizar *links* de comunicação seguros que proveem confidencialidade das mensagens Não armazenar senha em texto simples
Negação de Serviço (*Denial of Service*)	Usar técnicas de "estrangulamento" de largura de banda Validar e filtrar as entradas
Elevação de Privilégio (*Elevation of Privilege*)	Seguir o princípio do menor privilégio. Utilizar contas de serviço com menos privilégio para executar processos e acessar recursos.

2.3.6 Mitigação de Riscos

O processo de mitigar riscos está relacionado à priorização, avaliação e implementação dos controles de segurança (contramedidas) recomendados. O processo de mitigação pode ser tratado das seguintes formas (NIST, 2002; OWASP, 2015):

- Assunção do risco: aceitar o risco potencial e continuar operando o sistema ou implementar controles para reduzir o risco a um nível aceitável;
- Prevenção de risco: evitar o risco eliminando sua causa e/ou consequência (por exemplo, eliminar certas funções do sistema ou desligá-lo quando os riscos são identificados);
- Limitação do risco: implementar controles que minimizem o impacto negativo de uma ameaça (por exemplo, controles de detecção);
- Planejamento de risco: gerenciar o risco através do desenvolvimento de um plano de mitigação de risco que prioriza, implementa e mantém controles de segurança;
- Pesquisa e reconhecimento: diminuir o risco de perda em função de reconhecer a vulnerabilidade ou falha, pesquisando controles para corrigi-las;
- Transferência de risco: transferir o risco usando outras opções para compensar a perda, como por exemplo, a compra de seguro.

A escolha da melhor opção para mitigar riscos deve levar em consideração a missão e os objetivos da organização (NIST, 2002). Além disso, é importante saber o melhor momento para agir.

A Figura 2.22 mostra quatro situações, indica pela palavra SIM, que demandam tomadas de ações. As duas primeiras situações ocorrem após a confirmação da existência da vulnerabilidade e da possibilidade de exploração. Nessas situações, sugere-se a aplicação de técnicas para reduzir a probabilidade de a vulnerabilidade ser explorada e de controles para minimizar o risco ou prevenir sua ocorrência. Na terceira situação, após perceber que os ganhos do atacante serão maiores do que seu custo, sugere-se a adoção de medidas que possam aumentar o grau de dificuldade do atacante, desmotivando-o. Na última situação, ciente da possibilidade de grandes perdas, propõe-se o uso de ações para limitar a extensão do ataque, desta forma reduzindo perdas (NIST, 2002).

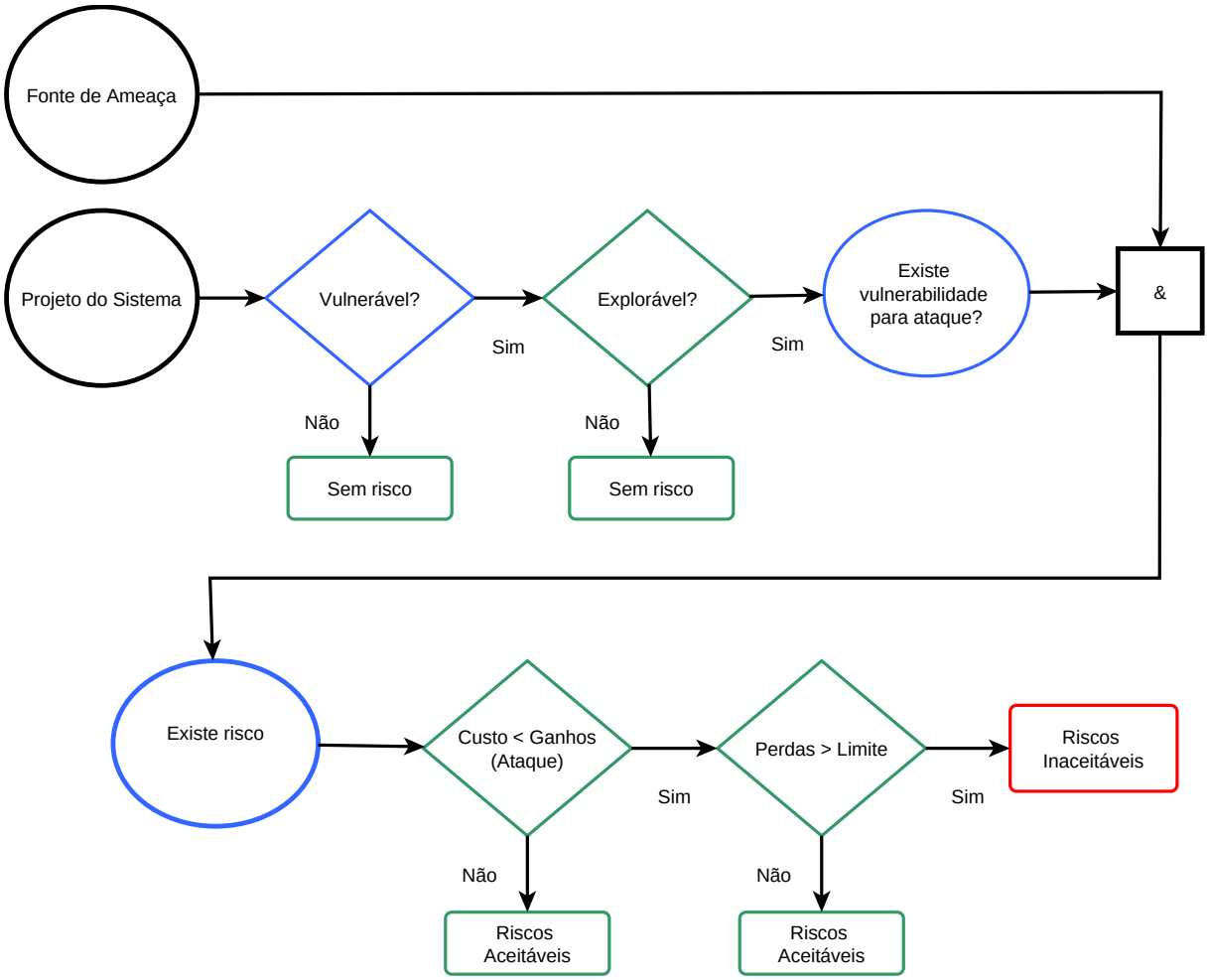


Figura 2.22: Pontos de ação para a mitigação de riscos, adaptada de NIST (2002)

3. PROPOSTA DE MODELAGEM DE AMEAÇAS ANTIFORENSES APLICADA AO PROCESSO FORENSE DIGITAL

Conforme comentado na seção 2.3, a modelagem de ameaças é um assunto amplamente abordado para o desenvolvimento de *software* com o objetivo de tratar riscos de ameaças a sistemas de forma estruturada. Contudo, no âmbito pericial, os modelos para condução de perícias forenses digitais encontrados na literatura não tratam riscos de ameaças antiforenses, apesar da constatação dos riscos que essas ameaças podem representar aos resultados periciais, conforme demonstrado na seção 2.2. Logo, este capítulo é dedicado integralmente a apresentar um processo de modelagem de ameaças antiforenses que complemente os processos forenses digitais propostos na literatura que não consideram tais riscos.

O modelo foi desenvolvido tendo como referência os processos de modelagem utilizados no desenvolvimento de *software*. Assim, o modelo de ameaças resultante permite identificar e tratar riscos de ameaças antiforenses que podem afetar a coleta de evidências digitais nos processos forenses digitais. O modelo proposto é dividido em cinco etapas, detalhadas a seguir, conforme a Figura 3.1.

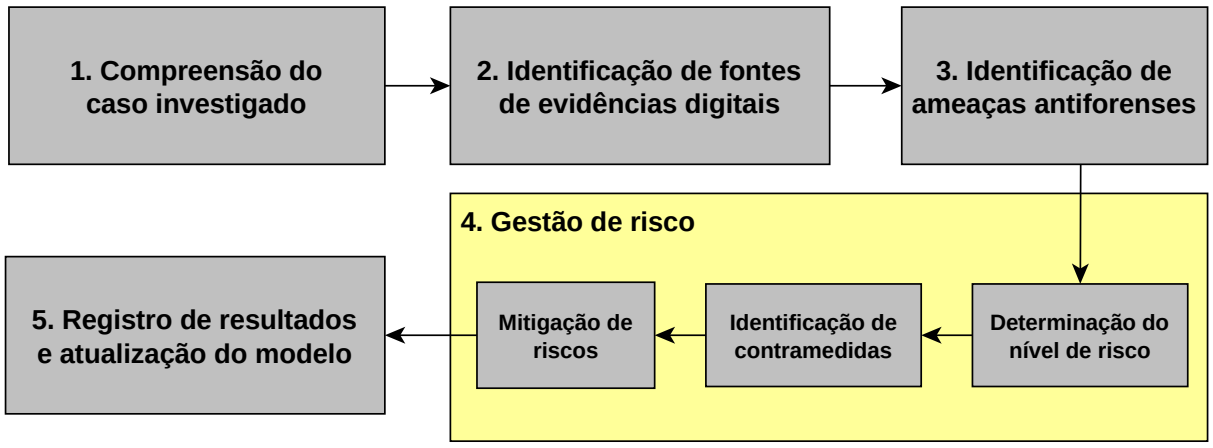


Figura 3.1: Processo de modelagem de ameaças antiforenses

3.1 COMPREENSÃO DO CASO INVESTIGADO

O objetivo desta etapa é levantar informações sobre o caso investigado para tomada de decisões em etapas futuras do processo de modelagem.

O levantamento de informações enfoca três elementos que envolvem o caso investigado: o suspeito, o ambiente a ser periciado e a ação criminal. A coleta de informações sobre esses elementos é fundamental para a condução do processo de modelagem, principalmente no que tange à determinação de riscos, conforme será visto na seção 3.4.1.

Fazendo-se uma analogia com o processo de modelagem de ameaças para sistemas proposto por Myagmar (2005), esta etapa é similar àquela de "Caracterização do sistema", na qual informações são coletadas para melhor compreensão do sistema. No caso de modelagem para sistemas, a coleta de informações pode ser realizada por meio de diversas técnicas, tais como questionários e entrevistas no local (ou *on-site*) (EKELHART, FENZ e NEUBAUER, 2009), ou com o auxílio do Diagrama de Fluxo de Dados (DFD) (MYAGMAR, 2005). Para o modelo proposto, adotou-se o questionário por sua simplicidade e objetividade, características essenciais dentro da realidade pericial, na qual o fator tempo é determinante.

Portanto, com base no conhecimento de especialistas, um questionário foi elaborado para nortear a coleta de informações, evitando que dados desnecessários sejam levantados. O questionário, disponível no apêndice B, está voltado a aspectos relacionados aos três elementos citados: o suspeito, o ambiente a ser periciado e a ação criminal. Por exemplo: Há suspeitos com conhecimento de informática? Quais tecnologias podem ser encontradas no ambiente a ser periciado?

3.2 IDENTIFICAÇÃO DE FONTES DE EVIDÊNCIAS DIGITAIS

Visa identificar meios de armazenamento de dados nos quais podem ser encontradas evidências digitais relacionadas ao delito investigado. A identificação desses meios é fundamental para que posteriormente possam ser identificadas as ameaças antiforenses.

As evidências digitais podem ser obtidas de diversas fontes, tais como arquivos produzidos por usuários, *logs* do sistema operacional, históricos de navegadores da Internet, arquivos de banco de dados, registro do sistema operacional ou atributos de arquivos (COSTA, 2011). Também são consideradas fontes de evidências digitais, dispositivos como câmeras digitais, consoles de jogos ou GPS. Contudo, não é viável analisar todas as fontes durante os exames periciais.

O tipo de crime e a experiência do perito é que vão indicar quais locais deverão efetivamente ser analisados. Por exemplo, em uma investigação relacionada à produção de material pornográfico envolvendo criança ou adolescente, é fundamental que arquivos

produzidos por usuários, principalmente imagens e vídeos, sejam coletados e analisados. Portanto, esses arquivos serão considerados fontes potenciais de evidências digitais.

3.3 IDENTIFICAÇÃO DE AMEAÇAS ANTIFORENSES

O principal objetivo desta etapa é identificar ameaças antiforenses que podem afetar a coleta e análise de dados de qualquer uma das fontes de evidências identificadas na fase anterior.

Essa etapa consiste em analisar cada uma das fontes de evidências e verificar quais ações antiforenses podem ser aplicadas para comprometê-las. Para auxiliar essa etapa, é proposto um catálogo, apêndice C, com registros de ameaças antiforenses identificadas durante o desenvolvimento deste trabalho, como criptografia de disco, esteganografia, ocultação de dados em *slack space*, entre outros.

Seguindo a ideia de busca de ameaças por categorias adotada no modelo STRIDE, abordado na seção 2.3.2, o catálogo é organizado em categorias definidas com base na classificação de ações antiforenses sugerida por Harris (2006). Segundo o autor, ações antiforenses podem ser classificadas quanto à destruição, ocultação, falsificação e eliminação de fontes de evidências digitais, discutidas na seção 2.2. Cabe ressaltar que o catálogo precisa ser alimentado sempre que se tenha conhecimento de novas práticas antiforenses. Para exemplificar o processo, suponha que para a apuração de um determinado delito, é fundamental analisar *logs* de um sistema operacional (fonte de evidências). Nesse caso, o foco devem ser as ações que permitam a falsificação, desativação ou destruição de registros de *logs*.

3.4 GESTÃO DE RISCOS

Esta é a principal etapa do processo de modelagem e tem como objetivo estimar os riscos que as ameaças antiforenses identificadas representam ao exame forense digital, bem como identificar e avaliar estratégias de mitigação. A etapa está dividida em três partes:

- determinação do nível do risco;
- identificação de contramedidas;
- mitigação de riscos.

Na primeira parte, o nível de risco é determinado pela combinação de fatores relacionados à probabilidade e ao impacto da ameaça antiforense. A segunda parte, identificação de contramedidas, busca medidas que possam minimizar os impactos das ameaças antiforenses e a última parte, mitigação de riscos, visa avaliar a aplicação ou não das medidas identificadas.

A Figura 3.2 apresenta os elementos envolvidos na gestão do risco. Os três elementos principais são o suspeito, a ameaça e o risco. A capacidade, a motivação e a oportunidade do suspeito são elementos determinantes na probabilidade da ameaça, enquanto o tipo da ameaça determina seu impacto. A probabilidade e o impacto são então utilizados para determinar o risco, que pode ser mitigado com a aplicação de contramedidas.

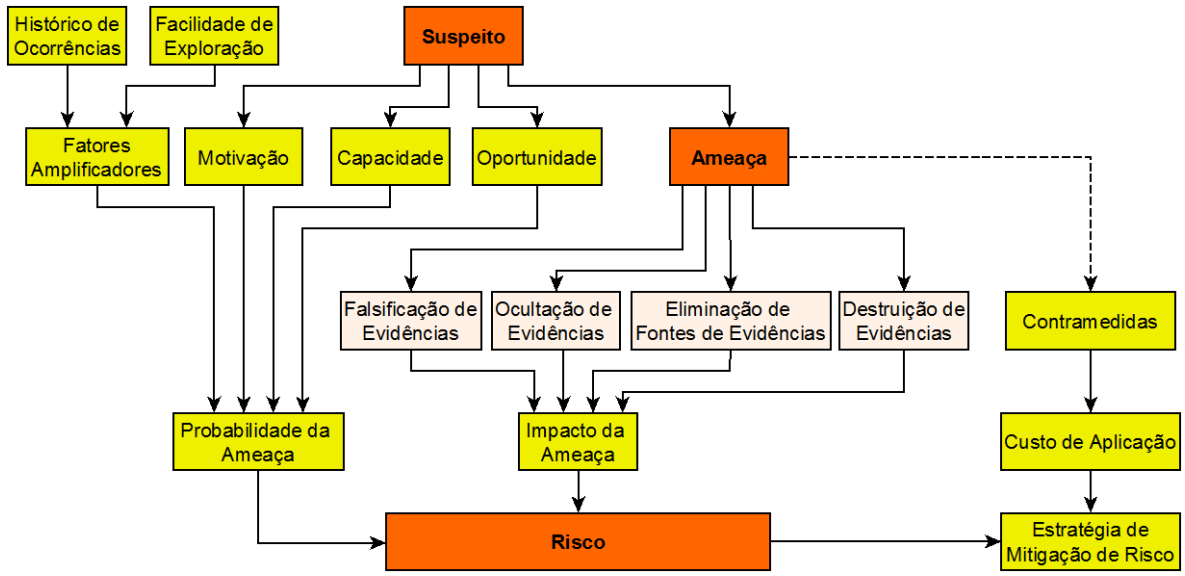


Figura 3.2: Elementos envolvidos na gestão de riscos

3.4.1 Determinação do risco

Conforme demonstrado na seção 2.3.4, na literatura é possível encontrar diversas abordagens para a determinação de risco, entretanto não é foco deste trabalho avaliar ou eleger a melhor. Portanto, para este modelo, optou-se por adotar uma abordagem baseada em elementos como probabilidade e impacto, tendo como referência a publicação especial 800-30 do NIST (*National Institute of Standards and Technology*), que estabelece um padrão de gerenciamento de risco para sistemas de tecnologia da informação, conforme discutido na seção 2.3.4.1. Na documentação do NIST, o risco é determinado pela combinação dos elementos (probabilidade e impacto) em uma matriz de risco, técnica de determinação de risco prevista na NBR ISO/IEC 31010:2012 (ISO, 2012).

Neste trabalho, a probabilidade está relacionada à possibilidade de ocorrência da ameaça antiforense e é estimada levando-se em consideração fatores relacionados ao agente da ameaça (suspeito) e a fatores relacionados à ação antiforense, estes chamados de fatores amplificadores. A probabilidade poderá ser alta, média ou baixa, de acordo com a soma da pontuação atribuída a cada fator.

Já o impacto está relacionado às consequências que a ameaça antiforense pode causar ao processo forense digital e seus resultados, e é estimado pelo potencial de danos que a ameaça antiforense pode causar na recuperação e apresentação de evidências digitais utilizáveis. O impacto poderá ser também alto, médio ou baixo.

O risco da ameaça é determinado por uma matriz de risco gerada pela combinação de valores de probabilidade e impacto. A seguir, são demonstrados detalhadamente os procedimentos para determinação do risco.

Determinação da Probabilidade

Para estimar a probabilidade, serão levados em consideração fatores relacionados ao agente da ameaça (suspeito), como motivação, capacidade e oportunidade, fatores considerados determinantes por Vidalis e Jones (2005) e por peritos em pesquisa realizada (apêndice I).

A capacidade está relacionada às condições que o suspeito possui para a aplicação da ação antiforense. A seguir, são citados alguns elementos que devem ser considerados:

- *software* e *hardware*: disponibilidade financeira para adquirir *software* e/ou *hardware*, caso seja necessário;
- nível de conhecimento: habilidades que o suspeito possui para a aplicação da ação antiforense;
- mão de obra: disponibilidade financeira para contratar profissionais especializados.

A motivação está relacionada aos ganhos obtidos com a atividade criminal com o uso da ação antiforense pelo suspeito. O uso da ação antiforense é fundamental para o sucesso da atividade criminal? Ou pouco contribui? Por exemplo, em casos de pedofilia, o uso da criptografia em disco é bem eficaz para a ocultação de arquivos de imagens e vídeo. Em contrapartida, a ocultação dos arquivos em *slack space* pode não ser tão interessante, pois não permite o armazenamento de um grande volume de dados.

Já a oportunidade refere-se às circunstâncias que favorecem a aplicação da ação antiforense pelo suspeito. Está relacionada à percepção do suspeito quanto à área pericial. Por exemplo: técnica antiforense pouco documentada e divulgada, inexistência de *software* adequado para tratamento, dificuldade de detecção etc.

Para determinar os fatores de capacidade, motivação e oportunidade relacionados ao suspeito no cálculo da probabilidade da ameaça, são propostas as pontuações apresentadas nas Tabelas 3.1, 3.2 e 3.3.

Tabela 3.1: Pontuação associada à avaliação da capacidade

Pontos	Capacidade
20	O suspeito possui amplas condições de fazer uso da ação antiforense.
10	O suspeito possui condições moderadas de fazer uso da ação antiforense.
5	O suspeito possui poucas condições de fazer uso da ação antiforense.
0	O suspeito não apresenta condições de fazer uso da ação antiforense.

Tabela 3.2: Pontuação associada à avaliação da motivação

Pontos	Motivação
20	O uso da ação antiforense pelo suspeito é fundamental à prática do delito investigado.
10	O uso da ação antiforense pelo suspeito contribui para a prática do delito investigado.
5	O uso da ação antiforense pelo suspeito pouco contribui para a prática do delito investigado.
0	O uso da ação antiforense pelo suspeito não contribui para a prática do delito investigado.

Tabela 3.3: Pontuação associada à avaliação da oportunidade

Pontos	Oportunidade
20	As circunstâncias são altamente favoráveis à aplicação da técnica antiforense.
10	As circunstâncias são moderadamente favoráveis à aplicação da técnica antiforense.
5	As circunstâncias são pouco favoráveis à aplicação da técnica antiforense.
0	As circunstâncias não são favoráveis à aplicação da técnica antiforense.

Além da capacidade, motivação e oportunidade, percebeu-se que alguns fatores podem aumentar a probabilidade de ocorrência de uma ação antiforense. Esses fatores são chamados

de fatores amplificadores. Segundo Jones (2002), fatores amplificadores são influências que podem contribuir para a ocorrência de um ataque. Para o modelo proposto, são fatores amplificadores:

- histórico de ocorrências: está relacionado ao emprego da ação antiforense em situações anteriores. Observou-se em pesquisa realizada (apêndice I) que a maioria dos peritos já teve conhecimento de ocorrências de ameaças antiforenses em procedimento anteriores.
- facilidade de exploração: nível de recursos necessários para a exploração da ação antiforense. A existência de ferramentas para a execução da ação e de documentação do método são exemplos de facilitadores.

As Tabelas 3.4 e 3.5 devem ser usadas para determinar a pontuação dos fatores amplificadores.

Tabela 3.4: Pontuação associada ao histórico de ocorrências

Pontos	Histórico de ocorrências
20	A ação antiforense foi amplamente utilizada em situações anteriores.
15	A ação antiforense foi moderadamente utilizada em situações anteriores.
10	A ação antiforense foi pouco utilizada em situações anteriores.
0	Não há relatos da aplicação da ação antiforense em situações anteriores.

Tabela 3.5: Pontuação associada à facilidade de exploração

Pontos	Facilidade de exploração
20	Há diversos facilitadores para a aplicação da técnica antiforense.
10	Há alguns facilitadores para a aplicação da técnica antiforense.
5	Há poucos facilitadores para a aplicação da técnica antiforense
0	Não há facilitadores para a aplicação da técnica antiforense.

Em relação ao "histórico de ocorrências", um modelo de catálogo, apêndice D, é proposto para registrar ações antiforenses identificadas em exames anteriores ou conhecidas a partir de outras fontes de informação, como outros órgãos periciais ou trabalhos científicos. É denominado de catálogo de "Ocorrências de Ações Antiforenses", e para que tenha eficácia precisa ser atualizado constantemente.

A pontuação para cada um dos fatores foi estabelecida de forma que fatores relacionados ao suspeito (capacidade, motivação e oportunidade) fossem suficientes para indicar uma alta probabilidade de ocorrência de uma ação antiforense. Para os fatores amplificadores, a pontuação utilizada visa potencializar a probabilidade de ocorrência, sendo incapaz de, isoladamente, estabelecer uma probabilidade alta de ameaça. No entanto, em ações que são fácil e frequentemente empregadas, a pontuação dos fatores amplificadores aumentaria a probabilidade de ameaça de baixa para média, de baixa para alta ou de média para alta.

Por fim, a probabilidade é estimada pela somatória da pontuação atribuída a cada um dos fatores e poderá ser baixa, média ou alta, conforme Tabela 3.6.

Tabela 3.6: Níveis de probabilidade da ameaça por pontuação

Probabilidade por pontuação	
< 45	Baixa
45 a 70	Média
> 70	Alta

Para exemplificar, suponha-se que, para ameaça "Ocultação de dados no *Slack Space*", sejam obtidas as pontuações contidas nas Tabelas 3.7 e 3.8.

Tabela 3.7: Exemplo de pontuação dos fatores relacionados ao agente da ameaça "ocultação de dados no *slack space"*

Agente da Ameaça	**Pontos**
Capacidade	20
Motivação	10
Oportunidade	05

Tabela 3.8: Exemplo de pontuação dos fatores amplificadores da ameaça de ocultação de dados no *slack space*

Amplificadores	**Pontos**
Histórico de ocorrências	15
Facilidade de exploração	10

Então, realizando-se a soma da pontuação apresentada, obtém-se uma probabilidade de ameaça média, conforme demonstrado a seguir:

```
Probabilidade = Capacidade + Motivação + Oportunidade + Histórico + Exploração = 20 + 10 + 05 + 15 + 10 = 60 (média)
```

Determinação do Impacto

Segundo Jones (2002), o impacto que a ameaça causará é um dos elementos que devem ser tratados na condução de uma avaliação de risco. Para o autor, a realização de um ataque está condicionada ao impacto negativo que ele pode causar.

Beer, Stander e Belle (2014) entendem que as ações antiforenses podem impactar na recuperação de evidências (a capacidade do profissional forense de recuperar evidências úteis), apresentação de evidências (a capacidade do profissional de apresentar provas de valor probatório) e na absolvição (quando a ação leva à absolvição de um suspeito). Com base nessa afirmativa, são propostos três níveis de impacto: alto, médio ou baixo, conforme Tabela 3.9.

Tabela 3.9: Níveis de impacto da ameaça

Impacto	
Alto	Pode comprometer totalmente a recuperação e apresentação de evidências digitais utilizáveis.
Médio	Pode comprometer parcialmente a recuperação e apresentação de evidências digitais utilizáveis.
Baixo	Pouco pode comprometer a recuperação e apresentação de evidências digitais utilizáveis.

Determinação do risco da ameaça

Calculados a probabilidade e o impacto, o risco da ameaça antiforense é obtido com a multiplicação da probabilidade pelo impacto, conforme apresentado na Tabela 3.10. O risco resultante poderá ser alto (entre 50 e 100), médio (de 10 a 50) ou baixo (de 1 a 10).

Tabela 3.10: Matriz de cálculo do risco da ameaça antiforense, adaptada de NIST (2002)

Risco = Probabilidade x Impacto			
Probabilidade	**Impacto**		
	BAIXO (10)	MÉDIO (50)	ALTO (100)
ALTA (1,0)	Baixo (1,0 x 10 = 10)	Médio (1,0 x 50 = 50)	Alto (1,0 x 100 = 100)
MÉDIA (0,5)	Baixo (0,5 x 10 = 5)	Médio (0,5 x 50 = 25)	Médio (0,5 x 100 = 50)
BAIXA (0,1)	Baixo (0,1 x 10 = 1)	Baixo (0,1 x 50 = 5)	Baixo (0,1 x 100 = 10)

Por exemplo, suponha-se que o impacto para a ameaça “ocultando dados no *slack space*” seja alto, então combinado com sua probabilidade média na matriz, obtém-se um risco médio.

O nível de tolerância ao risco resultante da combinação dos valores de probabilidade e impacto da ameaça é subjetivo e deve ser avaliado no contexto das demais ameaças identificadas. Algumas ameaças de baixo risco podem ser toleradas em face a uma ameaça simultânea de médio risco, caso os recursos para tratá-las sejam limitados. Portanto, o nível de risco não determina, isoladamente, a obrigatoriedade de qualquer ação por parte do perito. É necessário também identificar as contramedidas disponíveis e avaliar o custo de mitigação desses riscos.

3.4.2 Identificação de contramedidas

Após a determinação do nível de risco das ameaças, verifica-se a existência de medidas que podem minimizar os impactos nos exames periciais. Por exemplo, a Tabela 3.11 propõe uma medida para tratar o uso de *slack space* para ocultação de dados. Através da medida, tenta-se evitar a perda de possíveis evidências digitais.

Tabela 3.11: Proposta de contramedidas

Ameaça	Ocultação de dados no *slack space*
Risco	Médio
Contramedidas	Analise de dados contidos no *Slack Space* (*File System Slack Space e File Slack Space*)

Para esta etapa, é proposta a utilização de um catálogo de “Contramedidas” para manter os procedimentos e ferramentas a serem utilizados para cada situação, bem como observações sobre o custo associado à sua aplicação. O catálogo deve ser atualizado com a descoberta de novas contramedidas. O apêndice E apresenta um modelo de catálogo com o registro de contramedidas identificadas durante o desenvolvimento deste trabalho.

3.4.3 Mitigação de Riscos

Feito o levantamento de contramedidas que podem ser adotadas para minimizar riscos, esta etapa visa avaliar a conveniência da aplicação ou não delas. A decisão mais adequada está relacionada ao risco da ameaça e ao custo de aplicação da contramedida. Algumas

medidas podem ser muito custosas e, dependendo do risco da ameaça, podem ser julgadas desnecessárias.

Custo de aplicação da medida

O custo de aplicação pode ser alto, médio ou baixo, e é estimado tendo como referência o esforço necessário para sua implantação, conforme Tabela 3.12. A determinação do custo depende dos recursos, inclusive tempo, disponíveis para o perito ou órgão pericial.

Tabela 3.12: Níveis de custo de aplicação

Custo de aplicação da contramedida	
Alto	Requer muito esforço para aplicar.
Médio	Requer esforço moderado para aplicar.
Baixo	Requer pouco esforço para aplicar.

Por exemplo, na Tabela 3.11 é proposta uma medida para minimizar o risco da ameaça "Ocultação de dados no *Slack Space*". Nessa situação, a medida não requer maiores esforços e nem muito tempo de trabalho, pois ferramentas forenses já fazem análise de *slack space*, conforme demonstrado na seção 2.2.1.1. Portanto, nesse caso, entende-se que o custo de aplicação é baixo.

No catálogo de contramedidas, comentado anteriormente, foi criado um campo para o registro do custo de aplicação das contramedidas. Desta forma, evita-se a repetição de trabalho em procedimentos de modelagem futuros. Para todas as contramedidas identificadas durante o trabalho, os custos de aplicação foram estimados seguindo a visão do autor e registrados no catálogo.

Definição da estratégia de mitigação de riscos

Para auxiliar na decisão de aceitar ou não o risco da ameaça, foi elaborada uma matriz composta por valores do risco da ameaça e custo de aplicação da contramedida. A combinação do risco e custo na matriz resulta em dois valores: mitigar ou aceitar. O primeiro valor, mitigar, significa que o custo de aplicação da contramedida compensa diante do risco da ameaça, ou seja, a contramedida deve ser aplicada para tentar evitar perdas de evidências digitais. Já o segundo valor, aceitar, significa que o risco da ameaça deve ser aceito, pois o custo de aplicação da contramedida não compensa. A Tabela 3.13 mostra a matriz.

Tabela 3.13: Matriz de mitigação

Estratégia de Mitigação				
Risco	ALTO	Mitigar	Mitigar	Mitigar
	MÉDIO	Mitigar	Mitigar	Aceitar
	BAIXO	Mitigar	Aceitar	Aceitar
		BAIXA	MÉDIA	ALTO
	Custo de aplicação			

Aplicando-se a matriz à ameaça "Ocultando dados no *Slack Space*", é possível observar que a melhor opção é tratar o risco (mitigar) aplicando a contramedida proposta, visto que:

```
Risco = Médio (conforme Tabela 3.11)

Custo de Aplicação da contramedida = Baixo
```

Vale ressaltar que a determinação dos valores da matriz foi totalmente subjetiva e pode ser redefinida de acordo com a visão de cada perito ou órgão pericial.

3.5 REGISTRO DOS RESULTADOS E ATUALIZAÇÃO DO MODELO

Uma vez concluídas as etapas anteriores, é gerado um relatório com o resultado do processo de modelagem. O modelo de relatório contido no apêndice F pode ser usado. Assim, é possível recorrer posteriormente a essa documentação para revisar a avaliação realizada pelo perito ou verificar ameaças que porventura não tenham sido consideradas, mas que foram detectadas durante o exame. Essa etapa também é utilizada para a atualização dos catálogos propostos anteriormente: ocorrências de ações antiforenses, ameaças e contramedidas.

3.6 APLICAÇÃO DA MODELAGEM DE AMEAÇAS NO PROCESSO FORENSE DIGITAL

Esta seção tem como finalidade mostrar como o processo de modelagem proposto pode ser incorporado ao processo forense digital. Para isso, utilizou-se como base o modelo sugerido por Beebe e Clark (2004), que sintetiza a maioria dos demais modelos preconizados na literatura. Os autores propõem uma estrutura dividida em seis fases ilustradas na Figura 3.3.

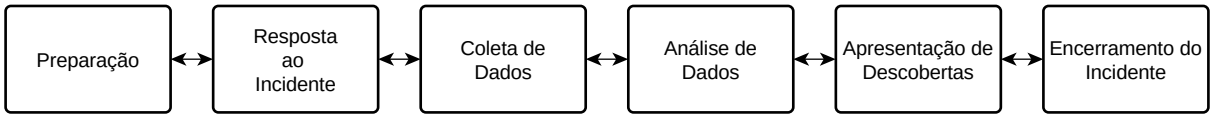


Figura 3.3: Fases do processo forense digital

Sucintamente, a fase de “Preparação” envolve a tomada de ações técnicas e administrativas pré-incidente, visando maximizar a coleta de evidências. Na fase de “Resposta ao Incidente” ocorre a definição da estratégia que será adotada para a realização do exame. As fases de “Coleta de Dados” e “Análise de Dados” têm como objetivo principal, respectivamente, a coleta de evidências e a análise das evidências. A fase de “Apresentação de Descobertas” refere-se à apresentação dos resultados por meio de relatório ou laudo pericial. Por último, a fase de “Encerramento do Incidente” sugere a avaliação de todo o processo visando melhorias em investigações futuras.

Com base na definição dessas fases, é possível determinar quais ações devem ser aplicadas ao longo do processo forense digital para a condução da modelagem de ameaças proposta. A Figura 3.4 ilustra essa sobreposição. Pode-se observar que as ações permeiam as várias fases do processo, desde a preparação até o encerramento do exame.

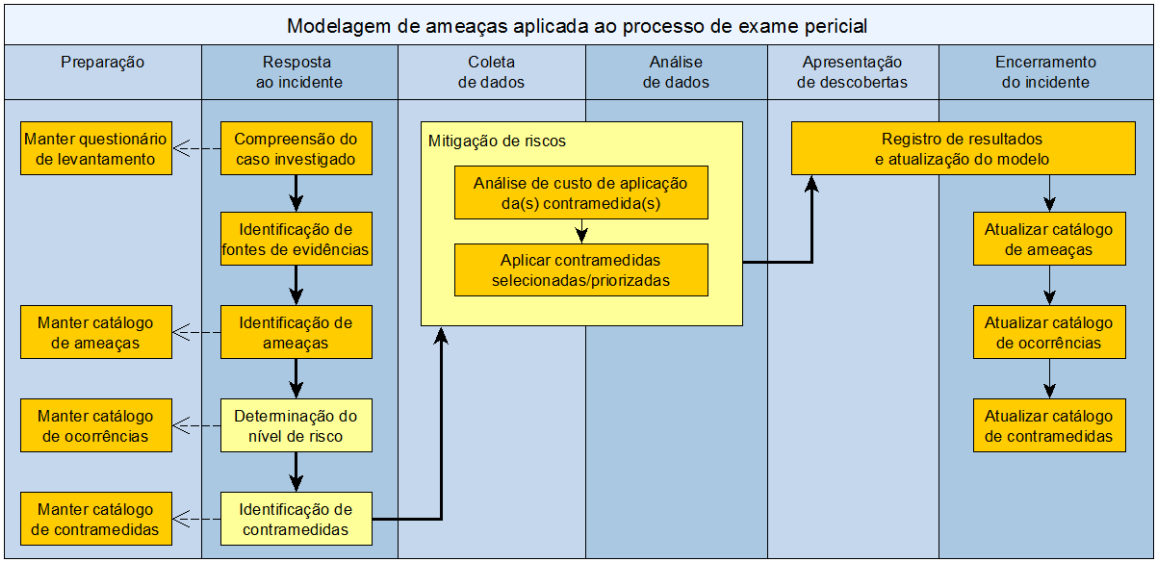


Figura 3.4: Aplicação da modelagem ao processo forense digital

A Figura 3.4 mostra que o processo de modelagem proposto é iniciado efetivamente no momento da ocorrência de um incidente, na etapa de “Resposta ao Incidente”. Antes disso, na etapa de “Preparação”, são mantidos atualizados os catálogos e o questionário de levantamento de informações que serão utilizados na fase de resposta. A aplicação da modelagem de ameaças resultará em uma lista de contramedidas para tratamento de ameaças

antiforenses que apresentam risco ao processo forense digital. Dependendo do perfil de risco das ameaças antiforenses, contramedidas poderão ser aplicadas na fase de coleta e/ou análise de dados, após a avaliação de custos. Na etapa de apresentação de descobertas, são registradas as ameaças antiforenses efetivamente encontradas, as contramedidas aplicadas e seus resultados. No encerramento do incidente, é realizada a atualização dos catálogos com os dados do incidente em curso.

A manutenção e atualização dos catálogos, bem como a manutenção do questionário, são atividades complementares ao processo de modelagem proposto, contudo extremamente necessárias para o sucesso do modelo. Conforme já visto neste capítulo, os catálogos e o questionário auxiliam quase todas as etapas do modelo. A seguir são comentadas cada uma dessas ações que ocorrem nas fases de "Preparação" e "Encerramento do Incidente" respectivamente:

Manter questionário de levantamento

A ação está relacionada à alteração ou à adição de novas perguntas ao questionário. Com o uso do modelo, a modificação do questionário pode ocorrer, por exemplo, pela percepção da necessidade de levantamento de novos dados para uma melhor gestão de risco. O questionário é a ferramenta utilizada na etapa de "Compreensão do caso investigado".

Manter e atualizar catálogo de ocorrências

A atualização e a manutenção estão relacionadas ao incremento do catálogo por meio do registro de novas ocorrências de ameaças antiforenses em processos periciais forenses digitais. A manutenção tem como objetivo manter o catálogo permanentemente atualizado através do levantamento de casos já finalizados, com incidência de ações antiforenses. O levantamento pode ser feito junto a outros órgãos periciais ou/e por meio de notícias veiculadas pela mídia. Já na atualização, o foco é registrar o caso em curso, caso seja detectada alguma ação antiforense durante o processo forense digital. A contabilização do incidente corrente contribuirá na condução do processo de modelagem em processos futuros. O enriquecimento do catálogo de ocorrências auxilia o processo de determinação do risco da ameaça.

Manter e atualizar catálogo de ameaças

A manutenção e a atualização estão relacionadas ao incremento do catálogo por meio do registro de novos métodos antiforenses que podem ameaçar o processo forense digital. A

manutenção foca na identificação de novos métodos antiforenses antes da ocorrência de um incidente. Publicações na Internet devem ser usadas como fonte de pesquisas. Já a atualização foca no registro de métodos antiforenses que não foram previstos durante o processo de modelagem finalizado, mas que foram identificados durante a coleta e análise de dados. A contabilização da ameaça contribuirá na condução do processo de modelagem em investigações futuras. O enriquecimento do catálogo de ameaças é fundamental para a etapa de identificação de ameaças antiforenses no processo de modelagem proposto.

Manter e atualizar catálogo de contramedidas

A manutenção e atualização estão relacionadas ao incremento do catálogo em função da descoberta de novas formas de tratamento de ameaças antiforenses. A manutenção refere-se ao registro de medidas de tratamento descobertas antes do incidente, o que pode ocorrer por meio de literaturas disponíveis ou trabalhos desenvolvidos pela equipe pericial local. Já a atualização visa documentar medidas de tratamento adotadas durante o processo forense digital, mas que não foram previstas no processo de modelagem finalizado.

4. ESTUDO DE CASO

Com o intuito de validar o modelo de modelagem proposto, este capítulo é dedicado a demonstrar a aplicação do modelo através de dois estudos de caso - um ligado à prática de pedofilia e outro ligado à exploração do jogo do bicho.

Conforme demonstrado na Figura 3.4, algumas ações precedem e sucedem a aplicação efetiva do processo de modelagem, como a manutenção e atualização de catálogos, e manutenção do questionário. Contudo, por serem apenas ações complementares ao processo proposto e que não impedem a validação do modelo, serão apenas citadas nos estudos de casos.

4.1 PRIMEIRO CASO: PEDOFILIA

Refere-se a um caso real de busca e apreensão realizado em uma empresa privada no Estado do Pará, com o objetivo de apurar crime de exploração e abuso sexual de criança ou adolescente. Nos próximos parágrafos, são apresentados os resultados obtidos em cada etapa do processo de modelagem de ameaças antiforenses conduzidos pelo Perito designado para participar da operação.

Na primeira etapa - compreensão do caso investigado -, com o suporte do questionário proposto no apêndice B, apurou-se que o caso envolvia um funcionário lotado na Gerência de Informática, com conhecimentos avançados na área, sem antecedentes criminais e com idade aproximada de 30 anos. Em termos de equipamentos computacionais, a operação previa apenas a apreensão do computador de uso diário do funcionário.

Na segunda etapa - identificação de fontes de evidências digitais -, foram consideradas como fontes potenciais de evidências digitais apenas arquivos de imagem e vídeo produzidos pelo usuário e armazenados no disco rígido do computador.

Na terceira etapa - identificação de ameaças antiforenses -, com suporte do catálogo de ameaças antiforenses proposto no apêndice C, foram identificadas ameaças antiforenses que poderiam afetar a coleta de arquivos de imagem e vídeo. O foco foi centrado em métodos antiforenses voltados à ocultação de dados, visto que, a princípio, as demais categorias de métodos antiforenses não representavam uma ameaça efetiva às fontes de evidências. A Tabela 4.1 apresenta as ameaças identificadas e algumas observações sobre seus riscos à coleta de evidências.

Tabela 4.1 - Estudo de caso 01: ameaças antiforenses identificadas

Ameaças antiforenses	Observações
Slack Space	Uso de sobras de espaços no disco rígido que não podem ser utilizadas pelo sistema de arquivos para esconder dados de arquivos.
Alternate Data Streams (ADS)	Criação de atributos $DATA adicionais são chamados de fluxos alternativos de dados ou *Alternate Data Streams* (ADS) para esconder dados de arquivos.
Clusters Adicionais	Alocação manual de *clusters* a um arquivo já existente para esconder dados de arquivos neles.
Arquivo $BadClus	Manipulação do arquivo $BadClus para marcar clusters utilizáveis como "ruins" para posterior utilização desses *clusters* para esconder dados de arquivos.
Atributo $DATA de diretórios	Criação de atributo $DATA em diretório para esconder dados de arquivos.
Criptografia de arquivos	O uso de algoritmo de criptografia com o objetivo de deixar o conteúdo do arquivo ilegível.
Criptografia do disco	O uso de algoritmo de criptografia com o objetivo de deixar o conteúdo do disco ilegível.
Esteganografia	Técnica para ocultação de dados de arquivos dentro de outros arquivos.

Na quarta etapa - gestão de riscos -, primeiramente foram estimados a probabilidade e o impacto e, em seguida, foi estimado o risco efetivo da ameaça antiforense com a combinação dos valores em uma matriz de risco. A Tabela 4.2 apresenta os resultados obtidos. O detalhamento do processo é apresentado na seção 4.1.1.

Tabela 4.2: Estudo de caso 01: níveis de probabilidade, impacto e risco

Ameaça antiforense	Probabilidade	Impacto	Risco (Probabilidade x Impacto)
Slack Space	Baixa	Alto	Baixo
Alternate Data Streams (ADS)	Baixa	Alto	Baixo
Clusters Adicionais	Baixa	Alto	Baixo
Arquivo $BadClus	Baixa	Alto	Baixo
Atributo $DATA de diretórios	Baixa	Alto	Baixo
Criptografia em arquivos	Alta	Alto	Alto
Criptografia em disco	Alta	Alto	Alto
Esteganografia	Média	Alto	Médio

Estimado o risco, contramedidas foram sugeridas para cada ameaça antiforense, com apoio do catálogo de contramedidas. Cabe ressaltar que na inexistência de soluções no catálogo, outras fontes devem ser pesquisadas. Em seguida, foi feita uma análise do custo de aplicação das contramedidas para cada ameaça antiforense, obedecendo aos níveis propostos na Tabela 3.12. A Tabela 4.3 apresenta as contramedidas propostas, seu custo e algumas observações sobre sua aplicação.

Tabela 4.3: Estudo de caso 01: contramedidas identificadas e custo de aplicação

Ameaça antiforense	**Contramedidas**	**Custo**	**Observações**
Slack Space (OE01)	Verificar *File System Slack Space* e *File Slack Space*, utilizando o *software* forense *Forensic Tool Kit* (FTK) para automatizar a verificação (CM1).	Médio	É facilmente implementada, mas requer um pouco de tempo para a recuperação e análise dos dados.
Alternate Data Streams (OE02)	Verificar ADS utilizando o *software* forense *Forensic Tool Kit* (FTK) para automatizar a verificação (CM2).	Médio	É facilmente implementada, mas requer um pouco de tempo para a recuperação e análise dos dados.
Clusters Adicionais (OE03)	Verificar se *clusters* foram adicionados manualmente a um arquivo já existente para ocultar dados. Comparar o tamanho alocado e o tamanho real de cada arquivo. Caso o tamanho alocado para um arquivo seja maior do que o seu tamanho real, é possível que dados estejam sendo ocultados nele (CM3).	Alto	A verificação é custosa, portanto o procedimento pode ser proibitivo, dependendo do volume de dados.
Arquivo $BadClus (OE04)	Verificar a existência de *clusters* rotulados como "ruins" no arquivo $BadClus. Se existir, fazer a sua extração e análise. Utilizar o *software* forense *Forensic Tool Kit* (FTK) como facilitador (CM4).	Médio	A verificação é custosa e requer um pouco de tempo para a recuperação e análise dos dados.
Atributo $DATA de diretórios (OE05)	Analisar todas as entradas de diretório e verificar se possuem o atributo $DATA. Se algum atributo $DATA for encontrado, o conteúdo dele deve ser analisado (CM5).	Alto	A verificação é custosa, portanto o procedimento pode ser proibitivo dependendo do volume de dados.
Criptografia em arquivos (OE06)	Utilizar ferramentas que analisam o cabeçalho dos arquivos para identificar arquivos encriptados. Se forem encontrados, persuadir o	Médio	Não há garantia de sucesso e requer um pouco de tempo

	suspeito a fornecer a chave para decifrar os dados (CM6).		
	Utilizar ferramentas que analisam o cabeçalho dos arquivos para identificar arquivos encriptados. Se forem encontrados, tentar localizar chaves (ou *passphrases)* no próprio disco periciado (CM7).	Alto	Não há garantia de sucesso, mesmo com grande custo de tempo.
	Utilizar ferramentas que analisam o cabeçalho dos arquivos para identificar arquivos encriptados. Se forem encontrados, usar ferramentas para testar frases e palavras derivadas de detalhes pessoais do suspeito obtidas durante o inquérito (CM8).	Alto	Não há garantia de sucesso, mesmo com grande custo de tempo.
	Localizar cópias de dados não cifradas deixadas em arquivos de paginação (*swap*), pastas temporárias, lixeira e espaços não alocados (CM9).	Médio	Não há garantia de sucesso e requer um pouco de tempo
Criptografia em disco (OE07)	Obtenção dos volumes criptografados quando ainda estão montados (CM10).	Médio	Requer oportunidade adequada para a realização da cópia dos dados (cujo tempo depende do volume de dados encontrado).
	Obtenção da chave criptográfica do volume (CM11).	Alto	Não há garantia de sucesso, mesmo com grande custo de tempo.
Esteganografia (OE08)	Busca por ferramentas ou aplicações de esteganografia no computador do suspeito. Se forem encontradas, indagar o suspeito sobre sua utilização (CM12).	Baixo	A verificação de ferramentas conhecidas pode ser feita facilmente (caso não haja outro obstáculo), mas não é exaustiva.
	Analisar o conteúdo de arquivos com ferramentas de detecção automatizada, como s*tegdetect* (CM13).	Alto	O tempo de execução das ferramentas pode ser proibitivo dependendo do volume de dados.

Com a combinação do custo de aplicação e risco da ameaça antiforense na matriz de estratégia de mitigação sugerida no modelo (Tabela 3.13), é definido se o risco da ameaça deve ser aceito ou se as contramedidas devem ser aplicadas (mitigar). A Tabela 4.4 apresenta esses resultados.

Tabela 4.4: Estudo de caso 01: estratégia de mitigação

Ameaça antiforense	Risco	Custo de aplicação da contramedida	Estratégia de mitigação
Slack Space	Baixo	CM1: Médio	Aceitar
Alternate Data Streams (ADS)	Baixo	CM2: Médio	Aceitar
Clusters Adicionais	Baixo	CM3: Alto	Aceitar
Arquivo $BadClus	Baixo	CM4: Médio	Aceitar
Atributo $DATA de diretórios	Baixo	CM5: Alto	Aceitar
Criptografia em arquivos	Médio	CM6: Médio	Mitigar
		CM7: Alto	Aceitar
		CM8: Alto	Aceitar
		CM9: Médio	Mitigar
Criptografia em disco	Alto	CM10: Médio	Mitigar
		CM11: Alto	Mitigar
Esteganografia	Médio	CM12: Baixo	Mitigar
		CM13: Alto	Aceitar

Na última etapa, um relatório - apêndice G - foi gerado com todos os resultados da aplicação do processo de modelagem de ameaças antiforenses, bem como da constatação de fato dessas ameaças e do emprego das contramedidas. No caso em questão, a ameaça criptografia em arquivos não foi confirmada, portanto as contramedidas CM6 e CM9 foram aplicadas parcialmente. Não foram identificadas ameaças de esteganografia com o uso da busca por ferramentas ou aplicações conhecidas para esse fim. A ameaça de criptografia de disco também não foi confirmada, embora a contramedida CM10 tenha sido aplicada preventivamente, considerando que a confirmação da ameaça só seria possível após o acesso ao computador. Cabe ressaltar que apenas a contramedida CM10 foi aplicada no local de apreensão do equipamento, as demais foram aplicadas em laboratório pericial.

4.1.1 Determinação do risco

Conforme abordado na seção 3.4.1, o risco é calculado pela combinação de valores de probabilidade e impacto na matriz de risco. O valor de probabilidade é estimado através da atribuição de pontos a fatores como capacitação, motivação e oportunidade relacionados ao

agente da ameaça (suspeito), bem como a fatores relacionados à ação antiforense, estes chamados de fatores amplificadores: histórico de ocorrência e facilidade de exploração. A pontuação deve obedecer às condições apresentadas nas Tabelas 3.1, 3.2, 3.3, 3.4 e 3.5. A soma dos pontos determina o nível de probabilidade de ocorrência da ameaça. As Tabelas 4.5, 4.6, 4.7, 4.8 e 4.9 apresentam a pontuação atribuída a cada fator e na Tabela 4.10 o cálculo da probabilidade.

Tabela 4.5: Estudo de caso 01: pontuação capacidade

Ameaça antiforense	**Capacidade**	**Observações**
Slack Space	20	O suspeito possui conhecimentos avançados de informática
Alternate Data Streams (ADS)	20	O suspeito possui conhecimentos avançados de informática.
Clusters Adicionais	20	O suspeito possui conhecimentos avançados de informática
Arquivo $BadClus	20	O suspeito possui conhecimentos avançados de informática.
Atributo $DATA de diretórios	20	O suspeito possui conhecimentos avançados de informática.
Criptografia em arquivos	20	O suspeito possui conhecimentos avançados de informática.
Criptografia em disco	20	O suspeito possui conhecimentos avançados de informática.
Esteganografia	20	O suspeito possui conhecimentos avançados de informática.

Tabela 4.6: Estudo de caso 01: pontuação motivação

Ameaça antiforense	**Motivação**	**Observações**
Slack Space	05	O método precursor da ameaça não é fundamental à prática do delito investigado. Entretanto, pode contribuir para a ocultação de informações referentes à prática de pedofilia. O método não permite a ocultação de um grande volume de dados, fato que pode limitar seu uso.
Alternate Data Streams (ADS)	10	O método precursor da ameaça não é fundamental à prática do delito investigado. Entretanto, pode contribuir para a ocultação de informações referentes à prática de pedofilia.
Clusters Adicionais	10	O método precursor da ameaça não é fundamental à prática do delito investigado. Entretanto, pode contribuir para a ocultação de informações referentes à prática de pedofilia.
Arquivo $BadClus	10	O método precursor da ameaça não é fundamental à prática do delito investigado. Entretanto, pode contribuir para a ocultação de informações

		referentes à prática de pedofilia.
Atributo $DATA de diretórios	10	O método precursor da ameaça não é fundamental à prática do delito investigado. Entretanto, pode contribuir para a ocultação de informações referentes à prática de pedofilia.
Criptografia em arquivos	10	O método precursor da ameaça não é fundamental à prática do delito investigado. Entretanto, pode contribuir para a ocultação de informações referentes à prática de pedofilia.
Criptografia em disco	10	O método precursor da ameaça não é fundamental à prática do delito investigado. Entretanto, pode contribuir para a ocultação de informações referentes à prática de pedofilia.
Esteganografia	10	O método precursor da ameaça não é fundamental à prática do delito investigado. Entretanto, pode contribuir para a ocultação de informações referentes à prática de pedofilia.

Tabela 4.7: Estudo de caso 01: pontuação oportunidade

Ameaça antiforense	**Oportunidade**	**Observações**
Slack Space	0	Ferramentas forenses, como o FTK (*Forense Tool, Kit*) e *Encase*, amplamente utilizadas em órgãos periciais no Brasil, já tratam a ameaça antiforense.
Alternate Data Streams (ADS)	0	Ferramentas forenses, como o FTK (*Forense Tool, Kit*) e *Encase*, amplamente utilizadas em órgãos periciais no Brasil, já tratam a ameaça antiforense.
Clusters Adicionais	05	Com o uso de ferramentas de recuperação de dados por *datacarving*, comumente utilizadas em procedimentos pericias no Brasil, é provável que os dados ocultados sejam recuperados.
Arquivo $BadClus	05	Com o uso de ferramentas de recuperação de dados por *datacarving*, comumente utilizadas em procedimentos pericias no Brasil, é provável que os dados ocultados sejam recuperados.
Atributo $DATA de diretórios	05	Com o uso de ferramentas de recuperação de dados por *datacarving*, comumente utilizadas em procedimentos pericias no Brasil, é provável que os dados ocultados sejam recuperados.
Criptografia em arquivos	20	O tratamento da ameaça antiforense é bastante custoso. Dependendo do algoritmo e do tamanho da chave, não há garantia de sucesso.
Criptografia em disco	20	O tratamento da ameaça antiforense é bastante custoso. Dependendo do algoritmo e do tamanho da chave, não há garantia de sucesso.
Esteganografia	20	A ameaça antiforense é bem difícil de ser detectada e o tratamento é bastante custoso.

Tabela 4.8: Estudo de caso 01: pontuação histórico de ocorrências

Ameaça antiforense	Histórico de Ocorrências	Observações
Slack Space	0	Não há relatos da aplicação da ação antiforense em situações anteriores.
Alternate Data Streams (ADS)	0	Não há relatos da ameaça antiforense em situações anteriores.
Clusters Adicionais	0	Não há relatos da ameaça antiforense em situações anteriores.
Arquivo $BadClus	0	Não há relatos da ameaça antiforense em situações anteriores.
Atributo $DATA de diretórios	0	Não há relatos da ameaça antiforense em situações anteriores.
Criptografia em arquivos	15	A ação antiforense foi moderadamente utilizada em situações anteriores.
Criptografia em disco	15	A ação antiforense foi moderadamente utilizada em situações anteriores.
Esteganografia	0	Não há relatos da ameaça antiforense em situações anteriores.

Tabela 4.9: Estudo de caso 01: pontuação facilidade de exploração

Ameaça antiforense	Facilidade de exploração	Observações
Slack Space	10	Há alguns facilitadores para a aplicação da técnica antiforense.
Alternate Data Streams (ADS)	10	Há alguns facilitadores para a aplicação da técnica antiforense.
Clusters Adicionais	0	Não há facilitadores para a aplicação da técnica antiforense.
Arquivo $BadClus	0	Não há facilitadores para a aplicação da técnica antiforense.
Atributo $DATA de diretórios	0	Não há facilitadores para a aplicação da técnica antiforense.
Criptografia em arquivos	20	Há diversos facilitadores para a aplicação da técnica antiforense.
Criptografia em disco	20	Há diversos facilitadores para a aplicação da técnica antiforense.
Esteganografia	10	Há alguns facilitadores para a aplicação da técnica antiforense.

Tabela 4.10: Estudo de caso 01: cálculo da probabilidade

Ameaça antiforense	Probabilidade
Slack Space	Capacidade + Motivação + Oportunidade + Histórico de Ocorrências + Facilidade de Exploração = 20 + 05 + 0 + 0 + 10 = 35 (Baixa)
Alternate Data Streams (ADS)	Capacidade + Motivação + Oportunidade + Histórico de Ocorrências + Facilidade de Exploração = 20 + 10 + 0 + 0 + 10 = 40 (Baixa)
Clusters Adicionais	Capacidade + Motivação + Oportunidade + Histórico de Ocorrências + Facilidade de Exploração = 20 + 10 + 05 + 0 + 0 = 35 (Baixa)
Arquivo $BadClus	Capacidade + Motivação + Oportunidade + Histórico de Ocorrências + Facilidade de Exploração = 20 + 10 + 05 + 0 + 0 = 35 (Baixa)
Atributo $DATA de diretórios	Capacidade + Motivação + Oportunidade + Histórico de Ocorrências + Facilidade de Exploração = 20 + 10 + 05 + 0 + 0 = 35 (Baixa)
Criptografia em arquivos	Capacidade + Motivação + Oportunidade + Histórico de Ocorrências + Facilidade de Exploração = 20 + 10 + 20 + 15 + 20 = 85 (Alta)
Criptografia em disco	Capacidade + Motivação + Oportunidade + Histórico de Ocorrências + Facilidade de Exploração = 20 + 10 + 20 + 15 + 20 = 85 (Alta)
Esteganografia	Capacidade + Motivação + Oportunidade + Histórico de Ocorrências + Facilidade de Exploração = 20 + 10 + 20 + 0 + 10 = 60 (Média)

O impacto é estimado com base no potencial de dano que as ameaças antiforenses apresentam aos procedimentos periciais, e pode ser alto, médio ou baixo, conforme Tabela 3.9. A Tabela 4.11 apresenta o nível de impacto de cada ameaça no estudo de caso.

Tabela 4.11: Estudo de caso 01: impacto

Ameaça antiforense	Impacto	Observações
Slack Space	Alto	Arquivos cruciais para comprovação da prática de pedofilia podem deixar de ser recuperados e apresentados.
Alternate Data Streams (ADS)	Alto	Arquivos cruciais para comprovação da prática de pedofilia podem deixar de ser recuperados e apresentados.
Clusters Adicionais	Alto	Arquivos cruciais para comprovação da prática de pedofilia podem deixar de ser recuperados e apresentados.
Arquivo $BadClus	Alto	Arquivos cruciais para comprovação da prática de pedofilia podem deixar de ser recuperados e apresentados.
Atributo $DATA de diretórios	Alto	Arquivos cruciais para comprovação da prática de pedofilia podem deixar de ser recuperados e apresentados.
Criptografia de arquivos	Alto	Arquivos cruciais para comprovação da prática de pedofilia podem deixar de ser recuperados e apresentados.
Criptografia do disco	Alto	Arquivos cruciais para comprovação da prática de pedofilia podem deixar de ser recuperados e apresentados.
Esteganografia	Alto	Arquivos cruciais para comprovação da prática de pedofilia podem deixar de ser recuperados e apresentados.

Por fim, os valores de probabilidade e impacto de cada ameaça são combinados utilizando a matriz de risco proposta no modelo (Tabela 3.10).

4.2 SEGUNDO CASO: JOGO DO BICHO

Refere-se a um caso real de busca e apreensão realizado em residência particular. A investigação apurava a exploração de jogo de azar (jogo do bicho). Para esse caso, nenhum perito foi designado para participar da operação de busca e apreensão. O material apreendido durante a operação, um *notebook*, foi encaminhado diretamente pela autoridade policial para exame pericial em laboratório. Nos próximos parágrafos, serão apresentados os resultados obtidos em cada etapa do processo de modelagem de ameaças antiforenses conduzido pelo perito que realizou o exame.

Na primeira etapa - compreensão do caso investigado -, com o suporte do questionário proposto no apêndice B, apurou-se que o caso envolvia um indivíduo aposentado, com idade aproximada de 60 anos, nível de escolaridade fundamental e sem antecedentes criminais. O indivíduo era acusado de ser apontador de jogo do bicho ("cambista"). O exame pericial concentrou-se na busca de informações relacionadas à operação do jogo do bicho em *notebook* apreendido em posse do suspeito.

Na segunda etapa - identificação de fontes de evidências digitais -, foram considerados como fontes potenciais de evidências digitais quaisquer tipos de arquivo produzidos pelo usuário e armazenados no disco rígido do *notebo*k, como documentos, imagens, vídeos etc.

Na terceira etapa - identificação de ameaças antiforenses -, com suporte do catálogo de ameaças antiforenses proposto no apêndice C, foram identificadas ameaças antiforenses que poderiam afetar a coleta de arquivos de imagem e vídeo. O foco foi centrado em métodos antiforenses voltados à ocultação de dados, visto que, a princípio, as demais categorias de métodos antiforenses não representavam uma ameaça efetiva às fontes de evidências. A Tabela 4.12 apresenta as ameaças identificadas e algumas observações sobre seus riscos à coleta de evidências.

Tabela 4.12: Estudo de caso 02: ameaças antiforenses identificadas

Ameaças antiforenses	**Observações**
Slack Space	Uso de sobras de espaços no disco rígido que não podem ser utilizadas pelo sistema de arquivos para esconder dados de arquivos.
Alternate Data Streams (ADS)	Criação de atributos $DATA adicionais são chamados de fluxos alternativos de dados ou *Alternate Data Streams* (ADS) para esconder dados de arquivos.
Clusters Adicionais	Alocação manual de *clusters* a um arquivo já existente para esconder dados de arquivos neles.

Arquivo $BadClus	Manipulação do arquivo $BadClus para marcar *clusters* utilizáveis como "ruins" para posterior utilização desses *clusters* para esconder dados de arquivos.
Atributo $DATA de diretórios	Criação de atributo $DATA em diretório para esconder dados de arquivos.
Criptografia de arquivos	O uso de algoritmo de criptografia com o objetivo de deixar o conteúdo do arquivo ilegível.
Criptografia do disco	O uso de algoritmo de criptografia com o objetivo de deixar o conteúdo do disco ilegível.
Esteganografia	Técnica para ocultação de dados de arquivos dentro de outros arquivos.

Na quarta etapa - gestão de riscos -, primeiramente foram estimados a probabilidade e o impacto e, em seguida, foi estimado o risco efetivo da ameaça antiforense com a combinação dos valores em uma matriz de risco. A Tabela 4.13 apresenta os resultados obtidos. O detalhamento do processo é apresentado na seção 4.2.1.

Tabela 4.13: Estudo de caso 02: níveis de probabilidade, impacto e risco

Ameaça antiforense	**Probabilidade**	**Impacto**	**Risco (Probabilidade x Impacto)**
Slack Space	Baixa	Alto	Baixo
Alternate Data Streams (ADS)	Baixa	Alto	Baixo
Clusters Adicionais	Baixa	Alto	Baixo
Arquivo $BadClus	Baixa	Alto	Baixo
Atributo $DATA de diretórios	Baixa	Alto	Baixo
Criptografia em arquivos	Média	Alto	Médio
Criptografia em disco	Média	Alto	Médio
Esteganografia	Baixa	Alto	Baixo

Estimado o risco, contramedidas foram sugeridas para cada ameaça antiforense, com apoio do catálogo de contramedidas. Cabe ressaltar que na inexistência de soluções no catálogo, outras fontes devem ser pesquisadas. Em seguida, foi feita uma análise do custo de aplicação das contramedidas para cada ameaça antiforense, obedecendo aos níveis propostos na Tabela 3.12. A Tabela 4.14 apresenta as contramedidas propostas, seu custo e algumas observações sobre sua aplicação.

Tabela 4.14: Estudo de caso 02: contramedidas identificadas e custo de aplicação

Ameaça antiforense	Contramedidas	Custo	Observações
Slack Space (OE01)	Verificar *File System Slack Space* e *File Slack Space*, utilizando o *software* forense *Forensic Tool Kit* (FTK) para automatizar a verificação (CM1).	Médio	É facilmente implementada, mas requer um pouco de tempo para a recuperação e análise dos dados.
Alternate Data Streams (OE02)	Verificar ADS utilizando o *software* forense *Forensic Tool Kit* (FTK) para automatizar a verificação (CM2).	Médio	É facilmente implementada, mas requer um pouco de tempo para a recuperação e análise dos dados.
Clusters Adicionais (OE03)	Verificar se *clusters* foram adicionados manualmente a um arquivo já existente para ocultar dados. Comparar o tamanho alocado e o tamanho real de cada arquivo. Caso o tamanho alocado para um arquivo seja maior do que o seu tamanho real, é possível que dados estejam sendo ocultados nele (CM3).	Alto	A verificação é custosa, portanto o procedimento pode ser proibitivo dependendo do volume de dados.
Arquivo $BadClus (OE04)	Verificar a existência de *clusters* rotulados como "ruins" no arquivo $BadClus. Se existirem, fazer a extração e análise deles. Utilizar o *software* forense *Forensic Tool Kit* (FTK) como facilitador (CM4).	Médio	A verificação é custosa e requer um pouco de tempo para a recuperação e análise dos dados.
Atributo $DATA de diretórios (OE05)	Analisar todas as entradas de diretório e verificar se possuem o atributo $DATA. Se algum atributo $DATA for encontrado, o conteúdo dele deve ser analisado (CM5).	Alto	A verificação é custosa, portanto o procedimento pode ser proibitivo dependendo do volume de dados.
Criptografia em arquivos (OE06)	Utilizar ferramentas que analisam o cabeçalho dos arquivos para identificar arquivos encriptados. Se forem encontrados, persuadir o suspeito a fornecer a chave para decifrar os dados. (CM6).	Médio	Não há garantia de sucesso e requer um pouco de tempo
	Utilizar ferramentas que analisam o cabeçalho dos arquivos para identificar arquivos encriptados. Se forem encontrados, tentar localizar chaves (ou *passphrases)* no próprio disco periciado (CM7).	Alto	Não há garantia de sucesso, mesmo com grande custo de tempo.
	Utilizar ferramentas que analisam	Alto	Não há garantia de sucesso,

	o cabeçalho dos arquivos para identificar arquivos encriptados. Se forem encontrados, usar ferramentas para testar frases e palavras derivadas de detalhes pessoais do suspeito obtidas durante o inquérito (CM8).		mesmo com grande custo de tempo.
	Localizar cópias de dados não cifradas deixadas em arquivos de paginação (*swap*), pastas temporárias, lixeira e espaços não alocados (CM9).	Médio	Não há garantia de sucesso e requer um pouco de tempo
Criptografia em disco (OE07)	Obtenção dos volumes criptografados quando ainda estão montados (CM10).	Médio	Requer oportunidade adequada para realização da cópia dos dados (cujo tempo depende do volume de dados encontrado).
	Obtenção da chave criptográfica do volume (CM11).	Alto	Não há garantia de sucesso, mesmo com grande custo de tempo.
Esteganografia (OE08)	Busca por ferramentas ou aplicações de esteganografia no computador do suspeito. Se forem encontradas, indagar o suspeito sobre sua utilização (CM12).	Baixo	A verificação de ferramentas conhecidas pode ser feita facilmente (caso não haja outro obstáculo), mas não é exaustiva.
	Analisar o conteúdo de arquivos com ferramentas de detecção automatizada, como s*tegdetect* (CM13).	Alto	O tempo de execução das ferramentas pode ser proibitivo dependendo do volume de dados.

Com a combinação do custo de aplicação e risco da ameaça antiforense na matriz de estratégia de mitigação sugerida no modelo (Tabela 3.13), é definido se o risco da ameaça deve ser aceito ou se as contramedidas devem ser aplicadas (mitigar). A Tabela 4.15 apresenta esses resultados.

Tabela 4.15: Estudo de caso 02: estratégia de mitigação

Ameaça antiforense	**Risco**	**Custo de aplicação da contramedida**	**Estratégia de mitigação**
Slack Space	Baixo	CM1: Médio	Aceitar
Alternate Data Streams (ADS)	Baixo	CM2: Médio	Aceitar
Clusters Adicionais	Baixo	CM3: Alto	Aceitar
Arquivo $BadClus	Baixo	CM4: Médio	Aceitar
Atributo $DATA de diretórios	Baixo	CM5: Alto	Aceitar
Criptografia em arquivos	Médio	CM6: Médio	Mitigar

		CM7: Alto	Aceitar
		CM8: Alto	Aceitar
		CM9: Médio	Mitigar
Criptografia em disco	Médio	CM10: Médio	Mitigar
		CM11: Alto	Aceitar
Esteganografia	Baixo	CM12: Baixo	Aceitar
		CM13: Alto	Aceitar

Na última etapa, um relatório - apêndice H - foi gerado com todos os resultados da aplicação do processo de modelagem de ameaças antiforenses, bem como da constatação de fato dessas ameaças e do emprego das contramedidas. No caso em questão, a ameaça criptografia em arquivos não foi confirmada, portanto as contramedidas CM6 e CM9 foram aplicadas parcialmente. Não foi possível aplicar a contramedida CM10, pois o equipamento foi encaminhado para exame pericial desligado. No entanto, não houve prejuízo ao processo pericial, visto que, a ameaça criptografia de disco não foi confirmada.

4.2.1 Determinação do risco

Conforme abordado na seção 3.4.1, o risco é calculado pela combinação de valores de probabilidade e impacto na matriz de risco. O valor de probabilidade é estimado através da atribuição de pontos a fatores como capacitação, motivação e oportunidade relacionados ao agente da ameaça (suspeito), bem como a fatores relacionados à ação antiforense, estes chamados de fatores amplificadores: histórico de ocorrência e facilidade de exploração. A pontuação deve obedecer às condições apresentadas nas Tabelas 3.1 a 3.5. A soma dos pontos determina o nível de probabilidade de ocorrência da ameaça. As Tabelas 4.16 a 4.20 apresentam a pontuação atribuída a cada fator e a Tabela 6.21, o cálculo da probabilidade.

Tabela 4.16: Estudo de caso 02: pontuação capacidade

Ameaça antiforense	Capacidade	Observações
Slack Space	0	O suspeito não possui condições técnicas.
ADS	0	O suspeito não possui condições técnicas.
Clusters Adicionais	0	O suspeito não possui condições técnicas.
Arquivo $BadClus	0	O suspeito não possui condições técnicas.
Atributo $DATA de diretórios	0	O suspeito não possui condições técnicas.
Criptografia em arquivos	0	O suspeito não possui condições técnicas.

Criptografia em disco	0	O suspeito não possui condições técnicas.
Esteganografia	0	O suspeito não possui condições técnicas.

Tabela 4.17: Estudo de caso 02: pontuação motivação

Ameaça antiforense	Motivação	Observações
Slack Space	05	O método precursor da ameaça não é fundamental à prática do delito investigado. Entretanto, pode contribuir para a ocultação de informações referentes à operação do jogo do bicho. O método não permite a ocultação de um grande volume de dados, fato que pode limitar seu uso.
Alternate Data Streams (ADS)	10	O método precursor da ameaça não é fundamental à prática do delito investigado. Entretanto, pode contribuir para a ocultação de informações referentes à operação do jogo do bicho.
Clusters Adicionais	10	O método precursor da ameaça não fundamental à prática do delito investigado. Entretanto, pode contribuir para a ocultação de informações referentes à operação do jogo do bicho.
Arquivo $BadClus	10	O método precursor da ameaça não é fundamental à prática do delito investigado. Entretanto, pode contribuir para a ocultação de informações referentes à operação do jogo do bicho.
Atributo $DATA de diretórios	10	O método precursor da ameaça não é fundamental à prática do delito investigado. Entretanto, pode contribuir para a ocultação de informações referentes à operação do jogo do bicho.
Criptografia em arquivos	10	O método precursor da ameaça não é fundamental à prática do delito investigado. Entretanto, pode contribuir para a ocultação de informações referentes à operação do jogo do bicho.
Criptografia em disco	10	O método precursor da ameaça não é fundamental à prática do delito investigado. Entretanto, pode contribuir para a ocultação de informações referentes à operação do jogo do bicho.
Esteganografia	10	O método precursor da ameaça não é fundamental à prática do delito investigado. Entretanto, pode contribuir para a ocultação de informações referentes à operação do jogo do bicho.

Tabela 4.18: Estudo de caso 02: pontuação oportunidade

Ameaça antiforense	Oportunidade	Observações
Slack Space	0	Ferramentas forenses, como o FTK (*Forense Tool, Kit*) e *Encase*, amplamente utilizadas em órgãos periciais no Brasil, já tratam a ameaça antiforense.
Alternate Data Streams (ADS)	0	Ferramentas forenses, como o FTK (*Forense Tool, Kit*) e *Encase*, amplamente utilizadas em órgãos periciais no Brasil, já tratam a ameaça antiforense.

Clusters Adicionais	05	Com o uso de ferramentas de recuperação de dados por *datacarving*, comumente utilizadas em procedimentos pericias no Brasil, é provável que os dados ocultados sejam recuperados.
Arquivo $BadClus	05	Com o uso de ferramentas de recuperação de dados por *data carving*, comumente utilizadas em procedimentos pericias no Brasil, é provável que os dados ocultados sejam recuperados.
Atributo $DATA de diretórios	05	Com o uso de ferramentas de recuperação de dados por *data carving*, comumente utilizadas em procedimentos pericias no Brasil, é provável que os dados ocultados sejam recuperados.
Criptografia em arquivos	20	O tratamento da ameaça antiforense é bastante custoso. Dependendo do algoritmo e do tamanho da chave, não há garantia de sucesso.
Criptografia em disco	20	O tratamento da ameaça antiforense é bastante custoso. Dependendo do algoritmo e do tamanho da chave, não há garantia de sucesso.
Esteganografia	20	A ameaça antiforense é bem difícil de ser detectada e o tratamento é bastante custoso.

Tabela 4.19: Estudo de caso 02: pontuação facilidade de exploração

Ameaça antiforense	Facilidade de exploração	Observações
Slack Space	10	Há alguns facilitadores para a aplicação da técnica antiforense.
Alternate Data Streams (ADS)	10	Há alguns facilitadores para a aplicação da técnica antiforense.
Clusters Adicionais	0	Não há facilitadores para a aplicação da técnica antiforense.
Arquivo $BadClus	0	Não há facilitadores para a aplicação da técnica antiforense.
Atributo $DATA de diretórios	0	Não há facilitadores para a aplicação da técnica antiforense.
Criptografia em arquivos	20	Há diversos facilitadores para a aplicação da técnica antiforense.
Criptografia em disco	20	Há diversos facilitadores para a aplicação da técnica antiforense.
Esteganografia	10	Há alguns facilitadores para a aplicação da técnica antiforense.

Tabela 4.20: Estudo de caso 02: cálculo da probabilidade

Ameaça antiforense	Probabilidade
Slack Space	Capacidade + Motivação + Oportunidade + Histórico de Ocorrências + Facilidade de Exploração = 0 + 05 + 0 + 0 + 10 = 15 (Baixa)
Alternate Data Streams (ADS)	Capacidade + Motivação + Oportunidade + Histórico de Ocorrências + Facilidade de Exploração = 0 + 10 + 0 + 0 + 10 = 20 (Baixa)

Clusters Adicionais	Capacidade + Motivação + Oportunidade + Histórico de Ocorrências + Facilidade de Exploração = 0 + 10 + 05 + 0 + 0 = 15 (Baixa)
Arquivo $BadClus	Capacidade + Motivação + Oportunidade + Histórico de Ocorrências + Facilidade de Exploração = 0 + 10 + 05 + 0 + 0 = 15 (Baixa)
Atributo $DATA de diretórios	Capacidade + Motivação + Oportunidade + Histórico de Ocorrências + Facilidade de Exploração = 0 + 10 + 05 + 0 + 0 = 15 (Baixa)
Criptografia em arquivos	Capacidade + Motivação + Oportunidade + Histórico de Ocorrências + Facilidade de Exploração = 0 + 10 + 20 + 15 + 20 = 65 (Média)
Criptografia em disco	Capacidade + Motivação + Oportunidade + Histórico de Ocorrências + Facilidade de Exploração = 0 + 10 + 20 + 15 + 20 = 65 (Média)
Esteganografia	Capacidade + Motivação + Oportunidade + Histórico de Ocorrências + Facilidade de Exploração = 0 + 10 + 20 + 0 + 10 = 40 (Baixa)

Já o impacto é estimado com base no potencial de dano que as ameaças antiforenses apresentam aos procedimentos pericias. O impacto pode ser alto, médio ou baixo, conforme Tabela 3.9. A Tabela 4.21 apresenta o nível de impacto de cada ameaça no estudo de caso.

Tabela 4.21: Estudo de caso 02: impacto

Ameaça antiforense	Impacto	Observações
Slack Space	Alto	Arquivos cruciais para comprovação da prática de jogo do bicho podem deixar ser recuperados e apresentados.
Alternate Data Streams (ADS)	Alto	Arquivos cruciais para comprovação da prática de jogo do bicho podem deixar ser recuperados e apresentados.
Clusters Adicionais	Alto	Arquivos cruciais para comprovação da prática de jogo do bicho podem deixar ser recuperados e apresentados.
Arquivo $BadClus	Alto	Arquivos cruciais para comprovação da prática de jogo do bicho podem deixar ser recuperados e apresentados.
Atributo $DATA de diretórios	Alto	Arquivos cruciais para comprovação da prática de jogo do bicho podem deixar ser recuperados e apresentados.
Criptografia de arquivos	Alto	Arquivos cruciais para comprovação da prática de jogo do bicho podem deixar ser recuperados e apresentados.
Criptografia do disco	Alto	Arquivos cruciais para comprovação da prática de jogo do bicho podem deixar ser recuperados e apresentados.
Esteganografia	Alto	Arquivos cruciais para comprovação da prática de jogo do bicho podem deixar ser recuperados e apresentados.

Por fim, os valores de probabilidade e impacto de cada ameaça são combinados utilizando a matriz de risco proposta no modelo (Tabela 3.10).

5. CONCLUSÃO

Este trabalho propôs a aplicação do processo de modelagem de ameaças no tratamento de riscos de ações antiforenses em processos forenses digitais. O modelo, dividido em cinco etapas (compreensão do caso investigado, identificação de fontes de evidências, identificação de ameaças, gestão de riscos e registro dos resultados), complementa as fases comumente utilizadas no processo forense digital, introduzindo a gestão de risco de ações antiforenses que possam prejudicar o resultado da atividade pericial.

A proposta também contribui para complementar o processo pericial ao sugerir a adoção de um questionário para auxiliar o levantamento de informações sobre o caso investigado e de catálogos que servem de fontes de informações para auxiliar na tomada de decisões durante a aplicação do modelo de ameaça.

Os estudos de caso demonstram que a incorporação do modelo proposto nas atividades do perito permite identificar e avaliar riscos de ameaças antiforenses ainda no início do processo e oferecer medidas de detecção e mitigação que podem ser aplicadas nas fases de coleta e análise de dados. Com isso, o processo pericial torna-se mais robusto, e evita-se que ameaças antiforenses deixem de ser tratadas e que medidas de tratamento sejam adotadas desnecessariamente.

Em nível organizacional, a utilização do processo proposto, incluindo a atualização constante dos catálogos apresentados, permite avaliar o nível de preparação para atender determinadas ameaças. Pode-se, por exemplo, identificar a indisponibilidade de ferramentas para detecção de esteganografia ou a necessidade de abordar um suspeito enquanto um volume criptografado está disponível no computador. Alguns riscos que podem parecer improváveis para determinadas organizações podem apresentar-se críticos em outros (uso de esteganografia em casos associados a terrorismo). Portanto, a forma de aplicação da proposição depende da realidade objetiva encontrada pelos peritos. Além disso, o modelo contribui para padronização do processo de tratamento de ameaças antiforenses na organização, evitando a adoção de estratégias distintas em exames pericias semelhantes.

Cabe destacar que a gestão de risco no processo forense também é preventiva, em preparação às ameaças antiforenses, e não somente reativa. Portanto, algumas contramedidas implicam ações de planejamento anteriores à realização da coleta de dados e exame pericial, como foi possível observar nos estudos de caso.

5.1 TRABALHOS PUBLICADOS

O trabalho resultou em artigo (MAUES e HOELZ, 2016) apresentado no Workshop de Forense Computacional (WFC) do XVI Simpósio Brasileiro de Segurança da Informação (SBSeg 2016).

5.2 TRABALAHOS FUTUROS

Trabalhos devem ser realizados na expansão dos catálogos de ameaças contramedidas e de ocorrências de ameaças, bem como em formas de compartilhamento desse conhecimento entre organizações. Naturalmente, a aplicação do processo proposto torna-se mais eficiente com uma base de conhecimento mais abrangente e com um histórico de ocorrências que permite ao perito avaliar com maior precisão os riscos envolvidos em determinado cenário.

O desenvolvimento de uma ferramenta para automatizar todo processo, incluindo o formulário e catálogos, também é interessante para agilizar o procedimento.

REFERÊNCIAS BIBLIOGRÁFICAS

ACCESS DATA. Forensic ToolKit (FTK). Disponível em http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk?/solutions/digital-forensics/ftk. Acessado em 28/10/2015.

ALHABEEB, M.; ALMUHAIDEB A.; LE, P. D. e SRINIVASAN, B. (2010). Information Security Threats Classification Pyramid. 24th IEEE International Conference on Advanced Information Networking and Applications Workshops: 2010. p. 208-213.

BARYAMUREEBA, V. e FLORENCE, T. (2004). The Enhanced Digital Investigation Process Model. *Asian Journal of Information Technology*, *5*, 790–794.

BEEBE, N. L. e CLARK, J. G. (2004). A Hierarchical, Objectives-Based Framework for the Digital Investigations Process. *Proceedings of the Digital Forensic Research Workshop (DFRWS)*, (August), 146–166.

BEER, R.; STANDER, A. e BELLE, J. V. (2014). Anti-Forensic Tool Use and Their Impact on Digital Forensic Investigations : A South African Perspective. Departament of Information Systems. University of Cape Tpwn Private. Conference Paper.

BERGHEL, H.; HOELZER, D. e STHULTZ, M. (2008). Data Hiding Tactics for Windows and Unix File Systems. *Advances in Computers*.

BITLOCKER (2016). Bitlocker Drive Encryption Overview. Microsoft Corporation. Disponível em https://technet.microsoft.com/en-us/library/cc732774(v=ws.11).aspx. Acessado em 19/05/2016.

BRAGG, R. (2016). Security Guidance, Data Protection and Privacy, The Encrypting File System. Microsoft Corporation. Disponível em https://technet.microsoft.com/en-us/library/cc700811.aspx. Acessado em 13/05/2016.

CALOYANNIDES, M. A. (2009). Forensics is so "yesterday." IEEE Security and Privacy, 7(2), 18–25.

CARRIER, B. [A] (2005). File System Forensic Analysis. Upper Saddle River, Nj: Addison Wesley.

CARRIER, B [B]. The Sleuth Kit (TSK) & Autopsy: Open Source Digital Forensics Tools. Disponível em http://www.sleuthkit.org/. Acessado em 28/10/2015.

CERT.br [A] (2016). Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em http://www.cert.br/stats/incidentes/. Acessado em 19 /10/2016.

CERT.br [B] (2016). Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em http://www.cert.br/stats/incidentes/2015-jan-dec/analise.html. Acessado em 19 /10/2016.

CERT.br [C] (2015). Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em http://www.cert.br/stats/incidentes/2015-jan-dec/tipos-ataque.html. Acessado em 19/10/2016.

CERT.br [D] (2015). Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em http://www.cert.br/stats/incidentes/2015-jan-dec/top-atacantescc.html. Acessado em 19/10/2016.

CERT.br [E] (2012). Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha de Segurança para Internet. Disponível em http://cartilha.cert.br/criptografia/. Acessado em 13/05/2016.

CHANAALII, S. e JADHAV, A. (2009). Steganography An Art of Hiding Data, Vol.1(3), 137–141.

CHANDRAN, R. e YAN, W. Q. (2013). A Comprehensive Survey of Antiforensics for Network Security. Managing Trust in Cyberspace, 419.

CNSEG (2015). Confederação Nacional das Empresas de Seguros Gerais, Previdência Privada e Vida, Saúde Suplementar e Capitalização. Disponível em http://www.cnseg.org.br/fenseg/servicos-apoio/noticias/brasil-na-rota-de-crimes-ciberneticos.html. Acessado em 06/02/2016.

CONLAN, K.; BAGGILI, I. e BREITINGER, F. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. Digital Investigation, 18(December 2015), S66–S75

COSTA, L. R. (2012). Metodologia e arquitetura para sistematização do processo investigatório de análise da informação digital. Universidade de Brasília (UnB). Disponível em http://repositorio.unb.br/handle/10482/12117.

COSTA, M. A. S. L. (2011). Computação Forense: A análise forense no contexto da resposta a incidentes computacionais. 3ª Edição. Campinas/SP: Millennium Editora, 2011.

CRAIGER, J. P.; POLLITT, M. e SWAUGER, J. (2005). Law Enforcement and Digital Evidence. *ReVision*, 1–42.

CUMMINS, J.; DISKIN, P.; LAU, S. e PARLETT, R. (2004). "Steganography and digital watermarking" School of Computer Science, The University of Birmingham. Disponível em https://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS5/Steganography.pdf. Acessado em 17/02/2016.

EKELHART, A.; FENZ, S. e NEUBAUER, T. (2009). AURUM: A Framework for Information Security Risk Management. 42nd Hawaii International Conference on System Sciences, HICSS '09.

ELEUTÉRIO, P. M. S. e MACHADO, M. P. (2011). Desvendando a Computação Forense. São Paulo: Novatec.

FOLHA (2008). Traficante enviaria e-mails com ordens escondidas em imagens da Hello Kitty. Disponível em http://www1.folha.uol.com.br/fsp/cotidian/ff1003200801.htm. Acessado em 02/05/2016.

FOREMOST. Disponível em http://foremost.sourceforge.net/. Acessado em 28/10/2015.

GLOBO (2010). Nem FBI consegue decifrar arquivos de Daniel Dantas. Disponível em http://g1.globo.com/politica/noticia/2010/06/nem-fbi-consegue-decifrar-arquivos-de-daniel-dantas-diz-jornal.html. Acessado em 10/10/2016.

GROBBER, T. e LOUWARENS, B. (2007).“Digital Forensic Readiness as a Componentof Information Security Best Practice”, Proceedings of New Approaches for Security, Privacy and Trust in Complex Environments, 22nd International Information Security Conference, Vol 232, pp 13-24.

HARGREAVES, C. e CHIVERS, H. (2008). Recovery of encryption keys from memory using a linear scan. ARES 2008 - 3rd International Conference on Availability, Security, and Reliability, Proceedings, 1369–1376.

HARRIS, R. (2006). Arriving at an Anti-Forensics Consensus: Examining How to Define and Control the AntiForensics Problem. Digital Investigation, 3(S), S44-S49. Disponível em http://dfrws.org/2006/proceedings/6-Harris.pdf. Acessado em 15/02/2016.

HUEBNER, E.; BEM, D. e WEE, C.K. (2006). Data hiding in the NTFS file system. Digital Investigation 3, Austrália, 211-226.

IBGE. (2015). Pesquisa Nacional por Amostra de Domicílios. Síntese de Indicadores. 2ª Edição. Instituto Brasileiro de Geografia e Estatística.

INGALSBE, J. A,; SHOEMAKER, D. e MEAD, N. R. (2011). Threat Modeling the Cloud Computing, Mobile Device Toting, Consumerized Enterprise – an overview of considerations. *AMCIS 2011 Proceedings*, 1–6.

INTERNET WORLD STATS (2016). Brasil - Internet Stats and Telecom Market Reports. Disponível em http://www.internetworldstats.com/sa/br.htm. Acessado em 06/02/2016.

ISO (2012). ABNT NBR ISO/IEC 31010:2012. Gestão de riscos — Técnicas para o processo de avaliação de riscos. ABNT - Associação Brasileira de Normas Técnicas.

JONES, A. (2002). Identification of a Method for the Calculation of Threat in na Information Environment, *44*(abril).

JOUINI, M.; BEN, L.; RABAI, A. e BEN, A. (2014). Classification of Security Threats in Information Systems. *Procedia - Procedia Computer Science*, *32*, 489–496.

KHAJEH-HOSSEINI, A.; GREENWOOD, D.; SMITH, J. e SOMMERVILLE, I. (2012). The Cloud Adoption Toolkit: supporting cloud adoption decisions in the enterprise. *Software - Practice and Experience*, *43*(4), 447–465.

LIPNER, S. e HOWARD, M. (2005). The Trustworthy Computing Security Development Lifecycle. Security Engineering and Communications. Security Business and Technology Unit. Microsoft Corporation. Disponível em https://msdn.microsoft.com/en-us/library/ms995349.aspx. Acessado em 04/03/2016.

MANSFIELD-DEVINE, S. (2010). Going to court : Fighting forensics. Computer Fraud & Security Bulletin, 2010(1), 17–20.

MAUÉS, M. B. e HOELZ, B. W. P. (2016). Modelagem de Ameaças Antiforenses Aplicada ao Processo Forense Digital. XVI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais – SBSEG 2016. V Workshop de Forense Computacional. Universidade Federal Fluminense, Niterói, RJ.

MCCULLAGH, D. (2005). Minnesota court takes dim view of encryption. Cnet.com. Disponível em http://www.cnet.com/news/minnesota-court-takes-dim-view-of-encryption/. Acessado em 15/02/2016.

MEIER, J. D.; MACKMAN, A.; DUNNER, M.; VASIREDDY, S.; ESCAMILLA, R. e MURUKAN, A. (2003). Improving Web Application Security: Threats and Countermeasures. Microsoft Corporation. Disponível em https://msdn.microsoft.com/es-us/library/ff648641.aspx. Acessado em 26/03/2016.

MOORE, R. (2005). Cyber crime: Investigating High-Technology Computer Crime. Cleveland, Mississippi: Anderson Publishing

MYAGMAR, S. (2005). Threat Modeling as a Basis for Security Requirements. In StorageSS '05: Proceedings of the 2005 ACM Workshop on Storage Security and Survivability, 94–102.

NIST. (2002). Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology (NIST). Special Publication 800-53. Department of Commerce.

OWASP (2015). Application Threat Modeling. Open Web Application Security Project. Disponível em https://www.owasp.org/index.php/Application_Threat_Modeling. Acessado em 20/02/2016.

PERON, C. S. J. e LEGACY, M. (2005). Digital anti-forensics: emerging trends in data transformation techniques. Seccuris Labs. Disponível em http://pt.slideshare.net/mlegary/digital-antiforensics-emerging-trends-in-data-transformation-techniques. Acessado em 15/02/2016.

PERUMAL, S. (2009). Digital Forensic Model Based On Malaysian Investigation Process. *IJCSNS International Journal of Computer Science and Network Security*, *9*(8), 38–44.

ROGERS, M. (2006). Panel session at CERIAS 2006 Information Security Symposium. Disponível Em http://www.cerias.purdue.edu/symposium/2006/materials/pdfs/antiforensics.pdf. Acessado em 15/02/2016.

ROWLINGSON, A. (2004). Ten Step Process for Forensic Readiness, International Journal of Digital Evidence, Volume 2 Issue 3 Winter 2004. Elsevier.

SACHOWSKI, J. (2016). Implementing Digital Forensic Readiness: From Reactive to Proactive Process. Syngress.

SANS. (2005). Threat Modeling : A Process To Ensure Application Security. InfoSec Reading Room. SANS Institute. Disponível em https://www.sans.org/reading-room/whitepapers/securecode/threat-modeling-process-ensure-application-security-1646. Acessado em 11/03/2016.

SINDRE, G. e OPDAHL, A. L. (2005). Requirements Eng. Eliciting security requirements with misuse cases. Disponível em https://link.springer.com/article/10.1007/s00766-004-0194-4.

SHOSTACK, A. (2014). *Threat Modeling: Designing for Security*. John Wiley & Sons, Inc., Indianapolis, Indiana.

SLACKER. Disponível em http://www.jbbrowning.com/sandbox/security.html. Acessado em 10/10/2015.

SULE, D. (2014). Importance of Forensic Readiness. ISACA Journal. Disponível em http://www.isaca.org/Journal/archives/2014/Volume-1/Pages/JOnline-Importance-of-Forensic-Readiness.aspx.

SULLIVAN, B. (2010). Security Briefs - Add a Security Bug Bar to Microsoft Team Foundation Server 2010. Microsoft Magazine. Disponível em https://msdn.microsoft.com/en-us/magazine/ee336031.aspx. Acessado em 26/03/2016.

TILSTONE, W. J.; SAVAGE, K. A. e CLARK, L. A. (2006). *Forensic science: An encyclopedia of history, methods, and techniques*. ABC-CLIO.

TREND MICRO (2013). Estudo da Trend Micro: Brasil – Desafios de Segurança Cibernética Enfrentados por uma Economia em Rápido Crescimento. Disponível em http://www.trendmicro.com.br/cloud-content/br/pdfs/home/wp-brasil-final.pdf. Acessado em 06/02/2016.

VECCHIA, E. D.; WEBER, D. e ZORZO, A. (2013). Antiforense Digital: conceitos, técnicas, ferramentas e estudo de caso. Mini Cursos SBseg 2013. Disponível em http://wiki.inf.ufpr.br/maziero/lib/exe/fetch.php?media=ceseg:2013-sbseg-mc1.pdf. Acessado em 17/02/2016.

VIDALIS, S. e JONES, A. (2005). Analyzing Threat Agents and Their Attributes. Disponível em https://www.researchgate.net/publication/220947230_Analyzing_Threat_Agents_and_Their_Attributes. Acessado em 01/05/2016.

WENDT, E. e JORGE, H. V. N. (2013). Crimes Cibernéticos – Ameaças e Procedimentos de Investigação. 3ª Edição. São Paulo/SP: Brasport.

WINHEX. Disponível em http://www.x-ways.net/winhex/. Acessado em 15/10/2015.

WOLFE, H. (2003). Encountering encryption. *Computers and Security*, vol. 22, no. 5, 2003.

WOLFE, H. B. (2002). Encountering Encrypted Evidence (potential). University of Otago. Dunedin, New Zealand.

YUSOFF, Y.; ISMAIL, R.; e HASSAN, Z. (2011). Common Phases of Computer Forensics Investigation Models. International Journal of Computer Science and Information Technology, 3(3), 17–31.

APÊNDICES

A – VISÃO GERAL DO SISTEMA DE ARQUIVOS NTFS

No sistema de arquivos NTFS tudo é um arquivo, inclusive a própria estrutura do sistema de arquivos (CARRIER [A], 2005). A menor unidade de alocação é o cluster que consiste de um ou mais setores consecutivos. Dados da estrutura do sistema são armazenados em arquivos chamados de arquivos especiais. Um dos mais importantes arquivos especiais é o $MFT porque nele está contido a Master File Table (MFT) que é considerada o coração do sistema. A MFT contém informações de todos os arquivos e diretórios. Todo objeto no sistema possui pelo menos uma entrada na MFT, inclusive o próprio arquivo $MFT (CARRIER [A], 2005).

Cada entrada da MFT é chamada de registro de arquivo e possui o tamanho de 1024 bytes, sendo que 42 bytes são reservados para cabeçalho e o restante para atributos (HUENNER, BEM e WEE, 2006).

Um atributo é uma pequena estrutura de dado que armazena um tipo específico de dado, como por exemplo, $STANDARD_INFORMATION, $FILE_NAME e $DATA (CARRIER [A], 2005).

O conteúdo de um atributo pode ser residente ou não residente. Um atributo residente armazena seu conteúdo na entrada da MFT. Um atributo não residente armazena o conteúdo em clusters externos a MFT. Na entrada da MFT é armazenada uma lista dos intervalos de clusters consecutivos, chamados cluster runs, usados na alocação dos dados (CARRIER [A], 2005).

B – QUESTIONÁRIO PARA COLETA DE INFORMAÇÕES

Há suspeitos com conhecimento de informática? Se sim, qual o nível de conhecimento?

_____
_____

O suspeito dispõe de recursos financeiros para investimentos em *hardware* e *software* ou contratação de mão de obra especializada na área de informática? Se sim, qual o potencial financeiro?

_____
_____

O suspeito pertence ou relaciona-se com algum grupo de indivíduos com histórico de ações antiforenses? Por exemplo: terroristas, *hackers* e traficantes. Se sim, quais?

_____
_____

Há relatos do uso de métodos antiforenses pelo suspeito? Se sim, quais?

_____
_____

Quais tecnologias podem ser encontradas no ambiente a ser periciado? Por exemplo, aparelhos de telefonia móvel, rede de computadores, notebook, *tablets*, etc.

_____
_____

Quais tecnologias estão diretamente relacionadas ao incidente?

_____
_____

O suspeito tem acesso ou domínio sobre as tecnologias diretamente relacionadas ao incidente?

_____
_____

Há registros de ações antiforenses em ações criminais iguais ou semelhantes?

_____
_____

O ambiente a ser periciado é propício para ações antiforenses pelo suspeito? Por exemplo, pouco seguro e monitorado.

_____
_____

C - CATÁLOGO DE AMEAÇAS ANTIFORENSES

Classificação	Método Antiforense	ID[8]
Destruição de Evidências	"Limpeza" de arquivos (ou *wipe*)	DE01
	Alteração de atributos de arquivos	DE02
	Destruição de artefatos de atividades de usuários	DE03
	Desmagnetização de mídias	DE04
Ocultação de Evidências	*Slack Space*	OE01
	Alternate Data Streams (ADS)	OE02
	Clusters Adicionais	OE03
	Arquivo $BadClus	OE04
	Atributo $DATA de diretórios	OE05
	Criptografia em arquivos	OE06
	Criptografia em disco	OE07
	Esteganografia	OE08
Eliminação de Fontes de Evidências	Desativação de *Logs*	EF01
	Uso aplicações portáteis	EF02
	Uso de *Live* Distros	EF03
	Uso de *Syscall proxing*	EF04
	Direct Kernel Manipulation (DKOM)	EF05
	Utilização de navegadores "*in-private*"	EF06
Falsificação de Evidências	Modificação de atributos do sistema de arquivos	FE01
	Falsificação de endereço IP – *Spoofing*	FE02
	Sequestro de contas	FE03

[8] Identificador de ameaça antiforense

D - CATÁLOGO DE OCORRÊNCIAS DE AÇÕES ANTIFORENSES

Ação Criminosa	Caso	Ano	Ação antiforense	Descrição
Tráfico de Drogas	Traficante colombiano Juan Carlos Ramírez Abadía[9]	2008	OE08	Mensagens de voz e texto escondidas em arquivos de imagens da gatinha japonesa *Hello Kitty*
Lavagem de dinheiro	Operação Satiagraha da Polícia Federal[10]	2010	OE07	Discos rígidos criptografados apreendidos no apartamento do banqueiro Daniel Dantas.

[9] Informações sobre o caso obtidas em FOLHA (2008)
[10] Informações sobre o caso obtidas em GLOBO (2010)

E - CATÁLOGO DE CONTRAMEDIDAS

ID da ação Antiforense	Contramedidas	Custo
OE01	Verificar *File System Slack Space* e *File Slack Space*, utilizando o *software* forense *Forensic Tool Kit* (FTK) para automatizar a verificação.	Médio
OE02	Verificar ADS utilizando o *software* forense *Forensic Tool Kit* (FTK) para automatizar a verificação.	Médio
OE03	Verificar se *clusters* foram adicionados manualmente a um arquivo já existente para ocultar dados. Comparar o tamanho alocado e o tamanho real de cada arquivo. Caso o tamanho alocado para um arquivo seja maior do que o seu tamanho real, é possível que dados estejam sendo ocultados nele.	Alto
OE04	Verificar a existência de *clusters* rotulados como "ruins" no arquivo $BadClus. Se existir, fazer a sua extração e análise. Utilizar o *software* forense *Forensic Tool Kit* (FTK) como facilitador.	Médio
OE05	Analisar todas as entradas de diretório e verificar se possuem o atributo $DATA. Se algum atributo $DATA for encontrado, o conteúdo dele deve ser analisado.	Alto
OE06	Utilizar ferramentas que analisam o cabeçalho dos arquivos para identificar arquivos encriptados. Se forem encontrados, persuadir o suspeito a fornecer a chave para decifrar os dados.	Médio
	Utilizar ferramentas que analisam o cabeçalho dos arquivos para identificar arquivos encriptados. Se forem encontrados, tentar localizar chaves (ou *passphrases)* no próprio disco periciado.	Alto
	Utilizar ferramentas que analisam o cabeçalho dos arquivos para identificar arquivos encriptados. Se forem encontrados, usar ferramentas para testar frases e palavras derivadas de detalhes pessoais do suspeito obtidas durante o inquérito.	Alto
	Localizar cópias de dados não cifradas deixadas em arquivos de paginação (*swap*), pastas temporárias, lixeira e espaços não alocados.	Médio

OE07	Obtenção dos volumes criptografados quando ainda estão montados.	Médio
	Obtenção da chave criptográfica do volume.	Alto
OE08	Busca por ferramentas ou aplicações de esteganografia no computador do suspeito. Se forem encontradas, indagar o suspeito sobre sua utilização.	Baixo
	Analisar o conteúdo de arquivos com ferramentas de detecção automatizada, como *stegdetect*.	Alto

F - MODELO DE RELATÓRIO DE MODELAGEM DE AMEAÇAS

I. Objetivo

[Descrever de forma sucinta o propósito do processo de modelagem, delimitando sua abrangência]

II. Processo de modelagem de ameaças antiforenses

[Registrar as informações coletadas durante o processo de modelagem de ameaças]

a. Compreensão do caso investigado

b. Fontes de evidências digitais

c. Ameaças antiforenses identificadas

d. Riscos das ameaças antiforenses

Ameaça antiforense	Risco

e. Contramedidas e custo de aplicação

Ameaça antiforense	Contramedidas	Custo

f. Estratégia de mitigação

Ameaça antiforense	Contramedida	Estratégia de mitigação

III. Contramedidas recomendadas

Ameaça antiforense	Contramedida	Descrição

IV. Considerações finais sobre o procedimento

[Fazer uma análise do resultado do processo de modelagem de ameaças]

G - ESTUDO DE CASO 01: RELATÓRIO DE MODELAGEM DE AMEAÇAS

I. Objetivo

Registar os resultados da aplicação do processo de modelagem de ameaças antiforenses adotado em procedimento pericial durante operação busca e apreensão em empresa localizada no Estado do Pará, com fins de apurar crime de exploração e abuso sexual de criança ou adolescente.

II. Processo de modelagem de ameaças antiforenses

a) Compreensão do caso investigado

Envolvia um funcionário, lotado na Gerência de Informática, com conhecimentos avançados de informática, sem antecedentes criminais e com idade aproximada de 30 anos. Em termos de equipamentos computacionais, a operação previa apenas a apreensão do computador de uso diário do funcionário.

b) Fontes de evidências digitais

Arquivos de imagem e vídeo produzidos pelo usuário armazenados no disco rígido do computador.

c) Ameaças antiforenses identificadas

- *Slack Space*
- *Alternate Data Streams* (ADS)
- *Clusters* Adicionais
- Arquivo $BadClus
- Atributo $DATA de diretórios
- Criptografia em arquivos
- Criptografia em disco
- Esteganografia

d) Riscos das ameaças antiforenses

Ameaça antiforense	Risco
Slack Space	Baixo
Alternate Data Streams (ADS)	Médio
Clusters Adicionais	Baixo
Arquivo $BadClus	Baixo
Atributo $DATA de diretórios	Baixo
Criptografia em arquivos	Alto
Criptografia em disco	Alto
Esteganografia	Médio

e) Contramedidas X Custo de aplicação

Ameaça antiforense	Contramedidas	Custo
Slack Space	Verificar *File System Slack Space* e *File Slack Space*, utilizando o *software* forense *Forensic Tool Kit* (FTK) para automatizar a verificação (CM1).	Médio
Alternate Data Streams (ADS)	Verificar ADS utilizando o *software* forense *Forensic Tool Kit* (FTK) para automatizar a verificação (CM2).	Médio
Clusters Adicionais	Verificar se *clusters* foram adicionados manualmente a um arquivo já existente para ocultar dados. Comparar o tamanho alocado e o tamanho real de cada arquivo. Caso o tamanho alocado para um arquivo seja maior do que o seu tamanho real, é possível que dados estejam sendo ocultados nele (CM3).	Alto
Arquivo $BadClus	Verificar a existência de *clusters* rotulados como "ruins" no arquivo $BadClus. Se existir, fazer a sua extração e análise. Utilizar o *software* forense *Forensic Tool Kit* (FTK) como facilitador (CM4).	Médio

Atributo $DATA de diretórios	Analisar todas as entradas de diretório e verificar se possuem o atributo $DATA. Se algum atributo $DATA for encontrado, o conteúdo dele deve ser analisado (CM5).	Alto
Criptografia em arquivos	Utilizar ferramentas que analisam o cabeçalho dos arquivos para identificar arquivos encriptados. Se forem encontrados, persuadir o suspeito a fornecer a chave para decifrar os dados (CM6).	Médio
	Utilizar ferramentas que analisam o cabeçalho dos arquivos para identificar arquivos encriptados. Se forem encontrados, tentar localizar chaves (ou *passphrases)* no próprio disco periciado (CM7).	Alto
	Utilizar ferramentas que analisam o cabeçalho dos arquivos para identificar arquivos encriptados. Se forem encontrados, usar ferramentas para testar frases e palavras derivadas de detalhes pessoais do suspeito obtidas durante o inquérito (CM8).	Alto
	Localizar cópias de dados não cifradas deixadas em arquivos de paginação (*swap*), pastas temporárias, lixeira e espaços não alocados (CM9).	Médio
Criptografia em disco	Obtenção dos volumes criptografados quando ainda estão montados (CM10).	Médio
	Obtenção da chave criptográfica do volume (CM11).	Alto
Esteganografia	Busca por ferramentas ou aplicações de esteganografia no computador do suspeito. Se forem encontradas, indagar o suspeito sobre sua utilização (CM12).	Baixo
	Analisar o conteúdo de arquivos com ferramentas de detecção automatizada, como s*tegdetect* (CM13).	Alto

f) Estratégia de Mitigação

Ameaça antiforense	Contramedida	Estratégia de mitigação
Slack Space	CM1	Aceitar
Alternate Data Streams (ADS)	CM2	Mitigar
Clusters Adicionais	CM3	Aceitar
Arquivo $BadClus	CM4	Aceitar
Atributo $DATA de diretórios	CM5	Aceitar
Criptografia em arquivos	CM6	Mitigar
	CM7	Aceitar

	CM8	Aceitar
	CM9	Mitigar
Criptografia em disco	CM10	Mitigar
	CM11	Mitigar
Esteganografia	CM12	Mitigar
	CM13	Aceitar

III. Contramedidas recomendadas

Ameaça antiforense	Contramedida	Descrição
Alternate Data Streams (ADS)	CM2	Verificar ADS utilizando o *software* forense *Forensic Tool Kit* (FTK) para automatizar a verificação.
Criptografia em arquivos	CM6	Utilizar ferramentas que analisam o cabeçalho dos arquivos para identificar arquivos encriptados. Se forem encontrados, persuadir o suspeito a fornecer a chave para decifrar os dados.
	CM9	Localizar cópias de dados não cifradas deixadas em arquivos de paginação (*swap*), pastas temporárias, lixeira e espaços não alocados.
Criptografia em disco	CM10	Obtenção dos volumes criptografados quando ainda estão montados.
	CM11	Obtenção da chave criptográfica do volume
Esteganografia	CM12	Busca por ferramentas ou aplicações de esteganografia no computador do suspeito. Se forem encontradas, indagar o suspeito sobre sua utilização.

IV. Considerações finais sobre o procedimento

A ameaça criptografia em arquivos não foi confirmada, portanto as contramedidas CM6 e CM9 foram aplicadas parcialmente. Não foram identificadas ameaças de esteganografia com o uso da busca por ferramentas ou aplicações conhecidas para esse fim. A ameaça de criptografia de disco também não foi confirmada, embora a contramedida CM10 tenha sido aplicada preventivamente, considerando que a confirmação da ameaça só seria possível após o acesso ao computador. Cabe ressaltar que apenas a contramedida CM10 foi aplicada no local de apreensão do equipamento, as demais foram aplicadas em laboratório pericial.

H - ESTUDO DE CASO 02: RELATÓRIO DE MODELAGEM DE AMEAÇAS

I. Objetivo

Registar os resultados da aplicação do processo de modelagem de ameaças antiforenses adotado em procedimento pericial em notebook apreendido, com fins de apurar exploração de jogo de azar (jogo do bicho).

II. Processo de modelagem de ameaças antiforenses

a) Compreensão do caso investigado

Envolvia um indivíduo, aposentado, com idade aproximada de 60 anos, nível escolaridade fundamental e sem antecedentes criminais. O indivíduo é acusado de ser apontador de jogo do bicho ("cambista"). O exame pericial focava na busca de informações relacionadas à operação do jogo do bicho em notebook apreendido em pose do indivíduo.

b) Fontes de evidências digitais

Arquivos produzidos pelo usuário.

c) Ameaças antiforenses identificadas

- *Slack Space*
- *Alternate Data Streams* (ADS)
- *Clusters* Adicionais
- Arquivo $BadClus
- Atributo $DATA de diretórios
- Criptografia em arquivos
- Criptografia em disco
- Esteganografia

d) Riscos das ameaças antiforenses

Ameaça antiforense	Risco
Slack Space	Baixo
Alternate Data Streams (ADS)	Baixo
Clusters Adicionais	Baixo

Arquivo $BadClus	Baixo
Atributo $DATA de diretórios	Baixo
Criptografia em arquivos	Médio
Criptografia em disco	Médio
Esteganografia	Baixo

e) Contramedidas X Custo de aplicação

Ameaça antiforense	Contramedidas	Custo
Slack Space	Verificar *File System Slack Space* e *File Slack Space*, utilizando o *software* forense *Forensic Tool Kit* (FTK) para automatizar a verificação (CM1).	Médio
Alternate Data Streams (ADS)	Verificar ADS utilizando o *software* forense *Forensic Tool Kit* (FTK) para automatizar a verificação (CM2).	Médio
Clusters Adicionais	Verificar se *clusters* foram adicionados manualmente a um arquivo já existente para ocultar dados. Comparar o tamanho alocado e o tamanho real de cada arquivo. Caso o tamanho alocado para um arquivo seja maior do que o seu tamanho real, é possível que dados estejam sendo ocultados nele (CM3).	Alto
Arquivo $BadClus	Verificar a existência de *clusters* rotulados como "ruins" no arquivo $BadClus. Se existir, fazer a sua extração e análise. Utilizar o *software* forense *Forensic Tool Kit* (FTK) como facilitador (CM4).	Médio
Atributo $DATA de diretórios	Analisar todas as entradas de diretório e verificar se possuem o atributo $DATA. Se algum atributo $DATA for encontrado, o conteúdo dele deve ser analisado (CM5).	Alto
Criptografia em arquivos	Utilizar ferramentas que analisam o cabeçalho dos arquivos para identificar arquivos encriptados. Se forem encontrados, persuadir o suspeito a fornecer a chave para decifrar os dados (CM6).	Médio
	Utilizar ferramentas que analisam o cabeçalho dos arquivos para identificar arquivos encriptados. Se forem encontrados, tentar localizar chaves (ou *passphrases)* no próprio disco periciado (CM7).	Alto

	Utilizar ferramentas que analisam o cabeçalho dos arquivos para identificar arquivos encriptados. Se forem encontrados, usar ferramentas para testar frases e palavras derivadas de detalhes pessoais do suspeito obtidas durante o inquérito (CM8).	Alto
	Localizar cópias de dados não cifradas deixadas em arquivos de paginação (*swap*), pastas temporárias, lixeira e espaços não alocados (CM9).	Médio
Criptografia em disco	Obtenção dos volumes criptografados quando ainda estão montados (CM10).	Médio
	Obtenção da chave criptográfica do volume (CM11).	Alto
Esteganografia	Busca por ferramentas ou aplicações de esteganografia no computador do suspeito. Se forem encontradas, indagar o suspeito sobre sua utilização (CM12).	Baixo
	Analisar o conteúdo de arquivos com ferramentas de detecção automatizada, como s*tegdetect* (CM13).	Alto

f) Estratégia de Mitigação

Ameaça antiforense	Contramedida	Estratégia de mitigação
Slack Space	CM1	Aceitar
Alternate Data Streams (ADS)	CM2	Aceitar
Clusters Adicionais	CM3	Aceitar
Arquivo $BadClus	CM4	Aceitar
Atributo $DATA de diretórios	CM5	Aceitar
Criptografia em arquivos	CM6	Mitigar
	CM7	Aceitar
	CM8	Aceitar
	CM9	Mitigar
Criptografia em disco	CM10	Mitigar
	CM11	Aceitar
Esteganografia	CM12	Aceitar
	CM13	Aceitar

III. Contramedidas recomendadas

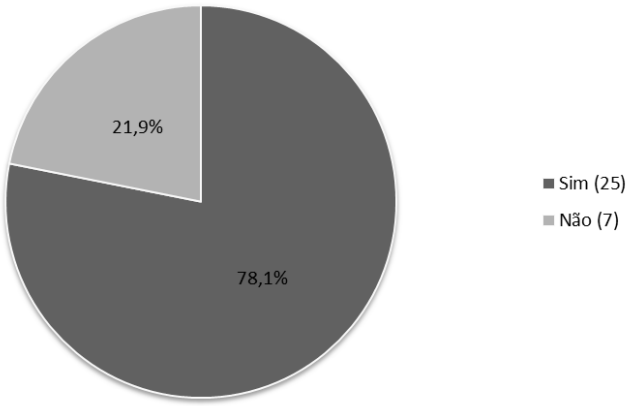
Ameaça antiforense	Contramedida	Descrição
Criptografia em arquivos	CM6	Utilizar ferramentas que analisam o cabeçalho dos arquivos para identificar arquivos encriptados. Se forem encontrados, persuadir o suspeito a fornecer a chave para decifrar os dados.
	CM9	Localizar cópias de dados não cifradas deixadas em arquivos de paginação (*swap*), pastas temporárias, lixeira e espaços não alocados.
Criptografia em disco	CM10	Obtenção dos volumes criptografados quando ainda estão montados.

IV. Considerações finais sobre o procedimento

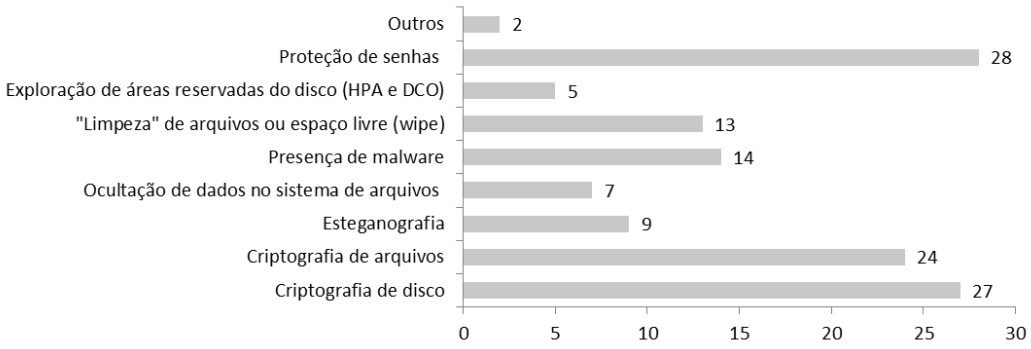
A ameaça criptografia em arquivos não foi confirmada, portanto as contramedidas CM6 e CM9 foram aplicadas parcialmente. Não foi possível aplicar a contramedida CM10, pois o equipamento foi encaminhado para exame pericial desligado. No entanto, não houve prejuízo ao processo pericial, visto que, a ameaça criptografia de disco não foi confirmada.

I – RESULTADO DA PESQUISA SOBRE A GESTÃO DE RISCOS NO PROCESSO PERICIAL EM INFORMÁTICA[11]

1. Você considera riscos de ameaças antiforenses antes de iniciar os procedimentos periciais?

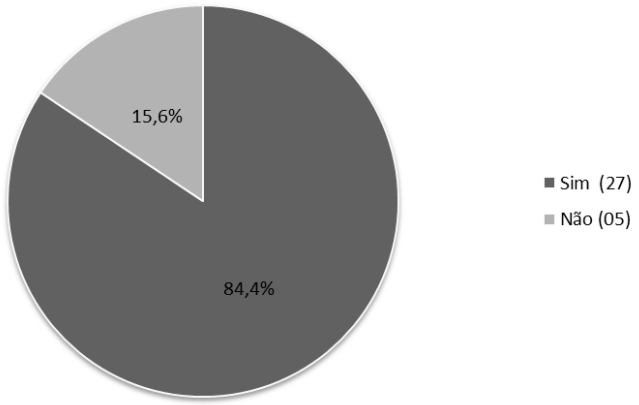


2. Quais dessas ameaças antiforenses você considera preocupantes?



[11] Pesquisa realizada para diagnosticar o estado da gestão de riscos no processo pericial e as ameaças identificadas pelos peritos no exercício da sua atividade.

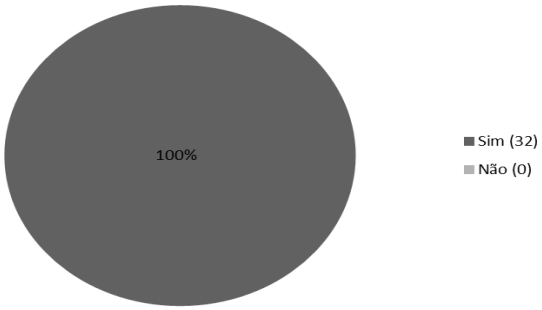
3. Você tem conhecimento de ocorrências de ameaças antiforenses em procedimentos periciais anteriores?



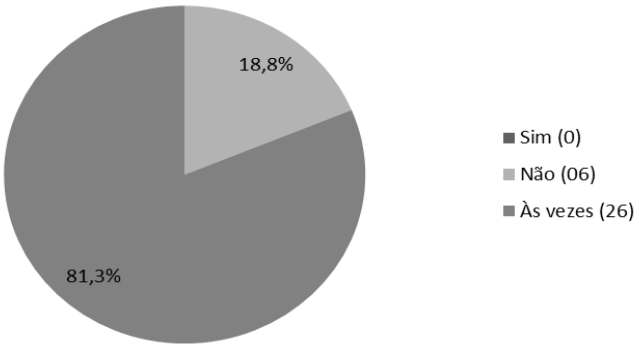
4. Quais ameaças já foram identificadas em pocedimentos periciais anteriores?

Criptografia de disco (BitLocker), HPA/DCO, senha ATA, ADS
Wipe remoto de dispositivos Apple.
Criptografia de discos
Exploração de áreas reservadas do disco (HPA e DCO), Criptografia de disco, Criptografia de arquivos.
Wipe, criptografia de disco, bloqueio de acesso por senha.
criptografia
Criptografia do disco por hardware
Criptografia de disco e arquivo
proteção por senhas, "Limpeza" de arquivos
criptografia de disco;
Wipe, criptografia e esteganografia.
criptografia e uso de senhas
criptografia de disco e arquivos
Criptografia de disco, criptografia de arquivos, presença de malware
Proteção por senha, wipe de arquivos, criptografia de armazenamento de dispositivos móveis (celulares).
Criptografia de disco e proteção por senhas
Criptografia de disco e arquivos, wipe, proteção por senhas
Criptografia de disco, e de arquivos. Proteção por senha. Esteganografia.
HPA e criptografia de disco
Destruição física da mídia de armazenamento, ocultação de arquivos, utilização de senhas, desativação de logs de sistemas, etc
Arquivos ocultos e Arquivos protegidos por senha
Criptografia
Criptografia de arquivos, proteção por senhas
presença de malware
Criptografia e compactação com senha.
Criptografia, programas de limpeza (ccleaner)

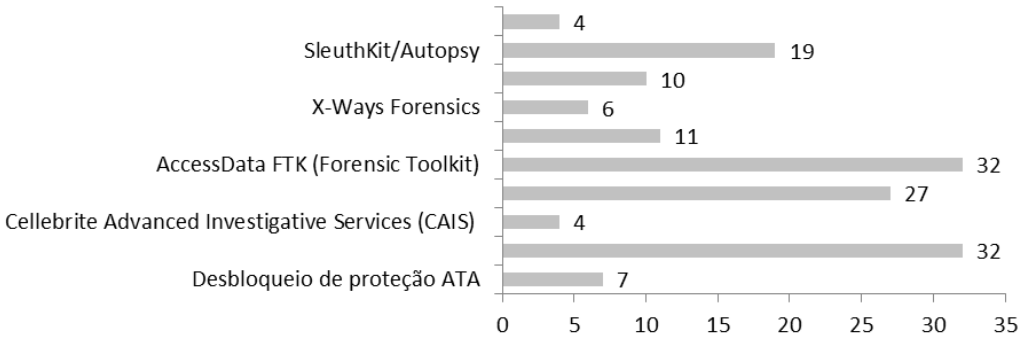
5. Aspectos relacionados ao suspeito (nível de conhecimento técnico, condições financeiras, motivação, oportunidade, etc.) podem influenciar a probabilidade de ocorrência de uma ameaça antiforense?



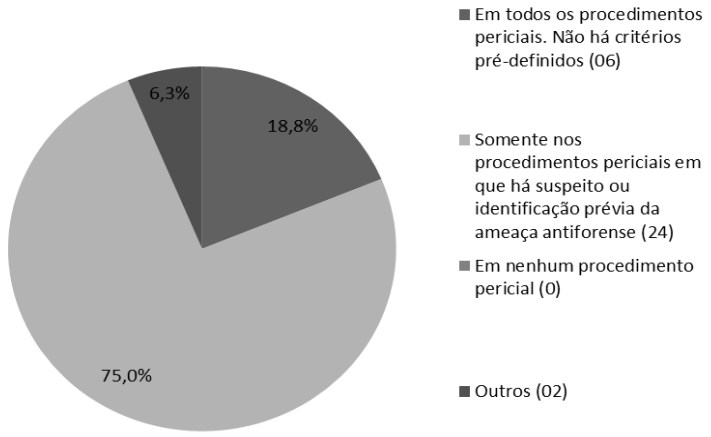
6. Na realização do processo pericial, você tem conhecimento prévio do perfil do suspeito/atacante?



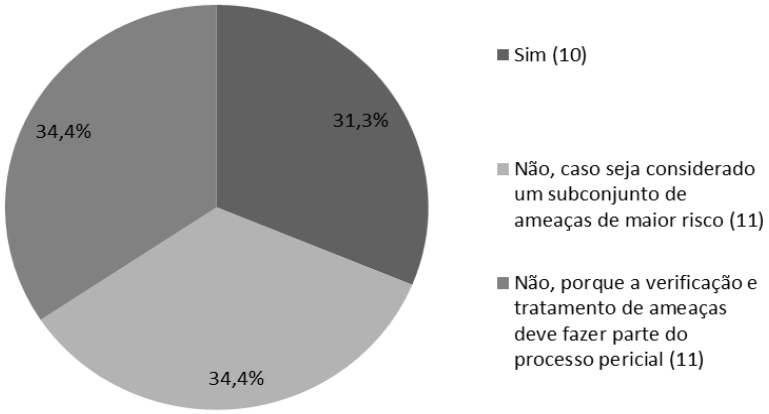
7. No seu local de trabalho, quais dessas ferramentas/serviços você tem à sua disposição?



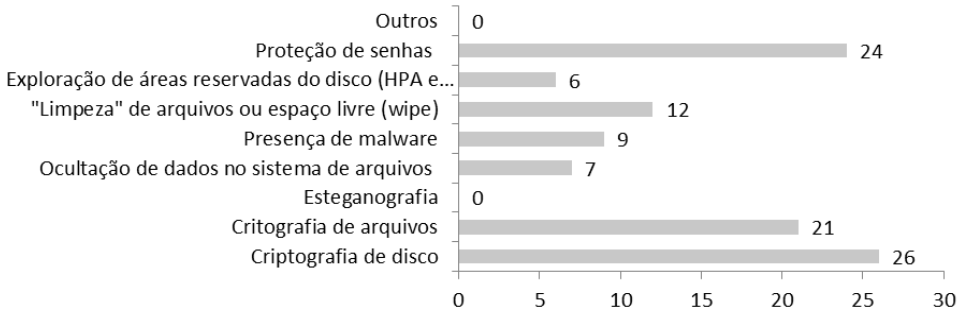
8. Em quais situações você faz uso de ferramentas ou métodos para tratamento de ameaças antiforenses?



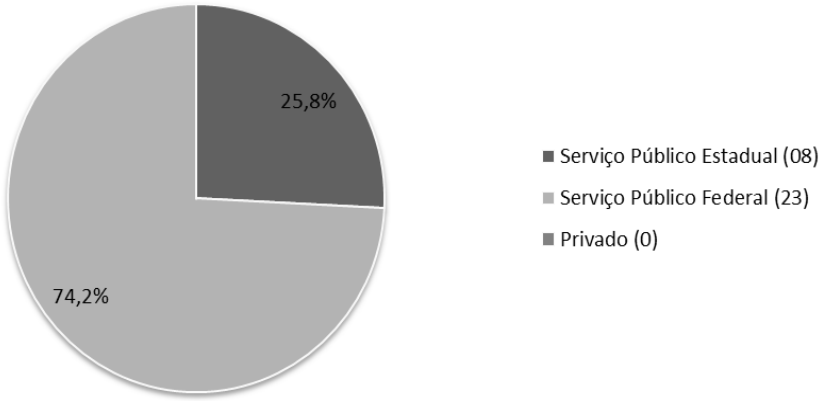
9. Você considera que o tempo necessário para verificar e tratar as ameaças antiforenses inviabilizaria a realização tempestiva do exame pericial?



10. Quais ameaças antiforenses costumam ser verificadas durante os procedimentos periciais?



11. Em qual âmbito você atua?



12. Qual é o seu estado de atuação?