Sumário – Tratado de Computação Forense

Capítulo 0 – Introdução à Computação Forense
Deivison Pinheiro Franco – Gustavo Pinto Vilar – Luiz Eduardo Marinho Gusmão – Luiz Rodrigo Grochocki
A Computação Forense
A complexidade e a evolução da computação
Terminologia e conceitos básicos da Computação Forense
Normas técnicas e procedimentos em Computação Forense
Normas técnicas
Procedimento Operacional Padrão (POP) ou Norma Operacional Padrão (NOP)
Os crimes cibernéticos e seus vestígios
Aspectos e temas abordados no Tratado de Computação Forense
Considerações finais. 14
Questões para análise . 15
Referências bibliográficas. 15

Capítulo 1 – Identificação, isolamento, coleta e preservação do vestígio cibernético
Gustavo Pinto Vilar – Luiz Eduardo Gusmão
Os vestígios cibernéticos
Isolamento dos vestígios cibernéticos
Isolamento físico
Isolamento lógico
Registro dos vestígios cibernéticos
Coleta dos vestígios cibernéticos
Preservação dos vestígios cibernéticos
Considerações finais
Questões para análise
Referências bibliográficas

Capítulo 2 – Fundamentos de sistemas de arquivos
Rodrigo Lange
Os sistemas de arquivos
Armazenamento e interpretação de dados
Anatomia e fisiologia das mídias de armazenamento

Discos rígidos mecânicos
Memórias *flash*
Discos ópticos
Particionamento
MBR – *Master Boot Record*
GPT – *GUID Partition Table*
Principais sistemas de arquivos
FAT
NTFS
EXT2/EXT3
EXT4
F2FS
HFS+
GFS e HDFS
Sistema de arquivos em equipamentos de gravação de vídeo (*Digital Video Recorder* – DVR)
Considerações finais
Questões para análise
Referências bibliográficas

Capítulo 3 – Exames em mídias de armazenamento
Rodrigo dos Santos Bacelar Gouveia Barbosa – Luiz Eduardo Marinho Gusmão
As mídias de armazenamento
Programas forenses
Preservação
O destino dos dados
Equipamentos de duplicação forense
Sistemas operacionais forenses
Programas de duplicação forense
Extração de dados
Assinatura de um arquivo
File carving
Análise
Redução
Busca
Análise de linha do tempo
Considerações finais

Questões para análise
Referências bibliográficas

Capítulo 4 – Exames em locais de internet
Gilberto Neves Sudré Filho – Deivison Pinheiro Franco
Os locais de internet
A internet
Camadas e protocolos
Endereçamento
Encontrando o endereço IP
Investigação de crimes cibernéticos
E-mail
Origem e autoria
Vestígios necessários
Análise de e-mail
Anexos de mensagens
Listas de discussão
Páginas web
Domain Name System (DNS)
Análise de sites
Comunicações instantâneas
Salas de bate-papo web
Anonimizadores da navegação e a Deep Web
Proxy
Virtual Private Networks (VPNs)
A Rede TOR
A Deep Web
Redes sociais
Crimes cometidos com o uso de redes sociais
As redes sociais Facebook e Twitter e suas fontes de vestígios cibernéticos para a perícia
Forense Computacional
Características importantes para a perícia
Identificação do ID de um perfil
Vestígios cibernéticos em redes sociais
Ferramentas para Perícia Forense Computacional de redes sociais
Navegadores

Histórico de navegação e *cookies*
Arquivos de histórico e de *cache* e sua localização em disco
Considerações finais
Questões para análise
Referências bibliográficas

Capítulo 5 – Exames em redes de computadores e dados de interceptação telemática
Gabriel Menezes Nunes
As redes de computadores e os dados de interceptação telemática
Equipamentos e protocolos de redes de computadores
Access points
Hubs
Roteadores
Switches
Protocolo DNS
Protocolo FTP
Protocolo HTTP
Protocolo IMAP
Protocolo IP
Protocolo POP3
Protocolo SMB
Protocolo SNMP
Protocolo SMTP
Protocolo TCP
Protocolo TFTP
Protocolo UDP
Fontes de vestígios cibernéticos em redes de computadores
Tráfego de rede
Switches
Roteadores
Servidores de Autenticação
Servidores de *proxy*
Servidores de DHCP
Sistemas de Detecção/Prevenção de Intrusão (IDS/IPS)
Servidores de DNS (***D****omain Name System*)
Firewalls

Servidores de Aplicação
Análise de registro de logs e tráfego de redes de computadores
PCAP
Wireshark
TCPDump
NetworkMiner
XPlico
DSniff
Cenários de ataques com registro de logs e tráfego de redes de computadores
Análise dos vestígios de um ataque de negação de serviço (DoS/DDoS)
Análise dos vestígios de um ataque de injeção de código SQL (SQL Injection)
Análise dos vestígios de um ataque de inclusão de arquivo local (LFI)
Análise dos vestígios de um ataque de inclusão de arquivo remoto (RFI)
Extração de arquivos com o Wireshark
Extração manual de arquivos com o Wireshark
Extração manual de arquivos com o Network Miner
Captura de tráfego em redes comutadas
Detecção de ataques com o Snort
Visualização de atividades de usuários via DNS
Recuperação de e-mails com o XPlico
Recuperação de chamadas VoIP com o Wireshark
Considerações finais
Questões para análise
Referências bibliográficas

Capítulo 6 – Exames em imagens digitais
Gustavo Henrique Machado de Arruda
As imagens digitais
Formação e armazenamento de imagens digitais
Estrutura básica de uma câmera digital
Formatos de arquivo
Exames periciais em imagens digitais
Detecção de edição ou montagem
Ampliação de imagens
Técnicas de interpolação
Super-resolução
Melhoria e restauração de imagens

Ajustes básicos
Correção de foco e movimento
Ruído periódico
Distorção de lente
Operações aritméticas
Fotogrametria
Considerações finais
Questões para análise
Referências bibliográficas

Capítulo 7 – Exames relacionados à pornografia infanto-juvenil
Mateus de Castro Polastro – Pedro Monteiro da Silva Eleutério
A pornografia infanto-juvenil
Forma de atuação do abusador
Abordagem tradicional
Abordagem virtual
A pedofilia como negócio: as redes de exploração sexual de crianças
Legislação
O que dizem a CF, o ECA e o CP
Técnicas computacionais para identificação de arquivos de pornografia infanto-juvenil
Uso do *hash* criptográfico
Verificação dos nomes dos arquivos
Detecção automática de nudez
Detecção de vídeos de pornografia a partir da identificação de padrões de movimentos e da análise de áudio
Outras técnicas de detecção
Exames em constatação de pornografia infanto-juvenil
Exames em locais de crime e busca e apreensão
Exames em laboratório
Ferramentas de apoio aos exames de constatação de pornografia infanto-juvenil
Ferramentas de apoio para exames em local de crime/busca e apreensão
Ferramentas de apoio para exames em laboratório
Estudo de casos
Cumprimento de mandado de busca e apreensão
Compartilhamento, posse e produção de pornografia infanto-juvenil
Considerações finais
Questões para análise

Referências bibliográficas

Capítulo 8 – Exames em computação embarcada
Pedro Luís Próspero Sanchez
A computação embarcada
Categorização dos sistemas embarcados
Sistemas integrados
Sistemas embutidos
Sistemas embarcados
Sistemas embarcados em veículos de via terrestre
Complexidade dos sistemas embarcados em veículos de via terrestre
Exames em computação embarcada
Especificidades
Abordagem geral
Aquisição de vestígios cibernéticos em computação embarcada
Gravadores de Dados de Eventos (EDR)
Captura de dados contidos no EDR
Valor probatório dos dados do EDR
Especialização profissional
Considerações finais
Questões para análise
Referências bibliográficas

Capítulo 9 – Exames em equipamentos portáteis e telefonia móvel
Alexandre Vrubel – Luiz Rodrigo Grochocki
Os equipamentos portáteis e a telefonia móvel
Equipamentos computacionais portáteis
Telefonia móvel
Configurações dos equipamentos de telefonia móvel
Isolamento, coleta, preservação e transporte
Vestígios físicos
Dados voláteis
Equipamentos pareados
Isolamento e preservação
Coleta de informações
Identificação e documentação
Pré-exame e triagem de materiais

Extração dos dados
Tipos de extração
Extração manual
Extração lógica
Extração física
Extração avançada (*Chip-Off, Micro Read*)
Ferramentas forenses para extração
Metodologia para extração
Cartões SIM
Análise dos dados
Transformando vestígios em evidências
Documentação dos resultados
Considerações finais
Questões para análise
Referências bibliográficas

Capítulo 10 – Exames em computação na nuvem
Joice Ribeiro do Rosário Dantas
A computação na nuvem
Computação na nuvem e a Forense Computacional
Provedores de nuvem e suas políticas
Segurança de dados
Contrato
Principais provedores de computação na nuvem
Computação na nuvem em dispositivos móveis
A Computação Forense e seus desafios na computação na nuvem
Exames em computação na nuvem
Modelos para exames periciais em computação na nuvem
Forense como um serviço em computação na nuvem (Forensic-as-a-Service – FaaS)
Exames em computação na nuvem X MapReduce / Hadoop
Casos recentes envolvendo ambientes de Computação na Nuvem
Considerações finais
Questões para análise
Referências bibliográficas

Capítulo 11 – Exames em detecção de intrusão

Luiz Fernando dos Santos – Leandro Bezerra Di Barcelos

A detecção de intrusão

Contextualização sobre os sistemas de detecção de intrusão

- Modelo conceitual
- IDSs baseados em rede e em *host*
- IDS x *firewall*
- IDS x IPS
- Metodologias de detecção

Intrusões

- Em máquinas individuais
- Em redes de computadores
- Dispositivos móveis
- Nuvem

Casos reais

- RAT (*Remote Administration Tool*)

Estudo de caso

Coleta inicial

- Checklists
- Linha do tempo

Coleta de dados

- Coleta de dados voláteis
- Duplicação forense
- Evidência de rede
- Serviços

Análise de dados

- Windows
- macOS

Considerações finais

Questões para análise

Referências bibliográficas

Capítulo 12 – Exames em *malwares*

Rafael Eduardo Barão – Gustavo Pinto Vilar

Os *malwares*

O que é um malware

Classes de malwares

- Spyware

- Backdoor
- Worm
- Bot
- Cavalo de tróia
- Rootkit
- Vírus

Objetivos da análise de malware no contexto pericial

- Software suspeito
- Ataques utilizando malwares
- Malware como elemento secundário

Tipos de análise

- Análise estática
- Análise dinâmica
- Análise *post-mortem* (de malware)
- Antianálise

Como identificar um malware

- VirusTotal
- Autoruns
- Arquivos de prefetch

Análise estática

- Strings
- Formato PE (*Portable Executable*)
- PEview
- Dependency walker
- Resource Hacker

Análise dinâmica

- Procedimentos recomendados em ambiente virtuais
- Process Explorer
- Process monitor
- Network Monitor
- TCPView

Análise avançada

- IDA
- OllyDbg

Considerações finais

Questões para análise

Referências bibliográficas

Capítulo 13 – Exames em dados criptografados

Luciano Lima Kuppens

Os dados criptografados

Conceitos de criptografia

- Noções básicas e nomenclatura utilizada
- Chave versus senha

Como detectar dados criptografados

- Arquivos criptografados
- Discos virtuais criptografados
- Discos completamente criptografados

Métodos para a decifragem de dados

- Recuperação direta
- Pré-computado
- Força bruta
- Dicionário
- Probabilístico
- Híbrido

Ferramentas para a decifragem de dados

- Aceleradores
- Aplicativos

Processo de decifragem de dados

- Identificação dos recursos compatíveis
- Ordem e parâmetros dos métodos de decifragem
- Finalização do caso

Considerações finais

Questões para análise

Referências bibliográficas

Capítulo 14 – Técnicas antiforenses

Diego Fuschini Camargo – Tony Rodrigues

A antiforense

Antiforense computacional

Leis e fundamentos da Computação Forense

Classificação das técnicas antiforenses

- Ocultação, ofuscação e encriptação de dados
- Deleção ou destruição de dados

Falsificação de dados
Prevenção à análise
Obstrução à coleta de vestígios
Subversão de ferramentas
Considerações finais
Questões para análise
Referências bibliográficas

Capítulo 15 – Segurança e defesa cibernética
Eder Luís Oliveira Gonçalves – Gabriel Menezes Nunes – Deivison Pinheiro Franco
O espaço cibernético
Segurança cibernética
A importância da segurança cibernética
Defesa cibernética
Guerra cibernética
Digital attack map
Norse IPViking
Cyberthreat Real-Time Map
Armas cibernéticas
Zero day
Inteligência cibernética
Ferramentas de inteligência cibernética
Coleta de informações
Segurança e defesa cibernética na Computação Forense
Normatização
Laboratório
Capacitação
Desafios
Considerações finais
Questões para análise
Referências bibliográficas

Capítulo 16 – Noções de direito cibernético
Patricia Peck Pinheiro – Luiz Rodrigo Grochocki
O direito cibernético
O direito aplicado à tecnologia
A evolução da prova no direito digital

Requisitos para obtenção da prova digital. 543
A prova pericial no novo Código de Processo Civil
Privacidade e Segurança Pública
Crimes cibernéticos
Divisão didática dos crimes cibernéticos
Características dos crimes cibernéticos
Considerações finais
Questões para análise
Referências bibliográficas

Capítulo 17 – Documentos processuais – laudos, pareceres e relatórios
Luiz Rodrigo Grochocki – Deivison Pinheiro Franco
Os documentos processuais
Laudo pericial em Computação Forense
Estrutura básica recomendável para um laudo pericial
Parecer técnico em Computação Forense. 578
Estrutura básica recomendável para um parecer técnico
Relatório técnico em Computação Forense
Estrutura básica recomendável para um relatório técnico em Computação Forense
Considerações finais
Questões para análise
Referências bibliográficas

Organizador e Autores