

Informatyka śledcza : gromadzenie, analiza i zabezpieczanie dowodów elektronicznych dla początkujących / William Oettinger. – Gliwice, © 2022

Spis treści

O autorze	11
O recenzencie	12
Wprowadzenie	13
Część I. Gromadzenie dowodów	17
Rozdział 1. Rodzaje dochodzeń w informatyce śledczej	19
Różnice w dochodzeniach z obszaru informatyki śledczej	20
Dochodzenia karne	21
Pierwsi na miejscu zdarzenia	22
Śledztwa korporacyjne	32
Wykroczenie pracowników	33
Szpiegostwo przemysłowe	35
Zagrożenie wewnętrzne	40
Podsumowanie	42
Pytania	42
Materiały dodatkowe	43
Rozdział 2. Proces analizy śledczej	44
Rozważania przed dochodzeniem	45
Stacja robocza dla śledczego	45
Zestaw mobilnego reagowania	47
Oprogramowanie śledcze	50
Szkolenia dla śledczych	53
Analiza informacji o sprawie i zagadnień prawnych	54
Pozyskiwanie danych	56
Łańcuch dowodowy	58
Proces analizy	61
Daty i strefy czasowe	62
Analiza skrótów	62
Analiza sygnatur plików	65
Antywirus	67
Raportowanie wyników	70
Szczegóły do uwzględnienia w raporcie	70
Udokumentuj fakty i okoliczności	71

Podsumowanie raportu	73
Podsumowanie	74
Pytania	74
Materiały dodatkowe	75
Rozdział 3. Pozyskiwanie dowodów	76
Eksploracja dowodów	76
Środowiska do prowadzenia badań kryminalistycznych	79
Walidacja narzędzi	80
Tworzenie sterylnych nośników	85
Zrozumieć blokowanie zapisu	89
Tworzenie obrazów kryminalistycznych	92
Format DD	93
Plik dowodowy EnCase	95
Dyski SSD	95
Narzędzia do obrazowania	96
Podsumowanie	107
Pytania	108
Materiały dodatkowe	109
Rozdział 4. Systemy komputerowe	110
Proces rozruchu	110
Kryminalistyczny nośnik rozruchowy	112
Dyski twarde	115
Partycje w MBR	118
Partycje GPT	121
Host Protected Area (HPA) i Device Configuration Overlays (DCO)	125
Zrozumieć systemy plików	126
System plików FAT	126
Obszar danych	130
Długie nazwy plików	133
Odzyskiwanie usuniętych plików	134
Przestrzeń luzu	135
System plików NTFS	136
Podsumowanie	147
Pytania	147
Materiały dodatkowe	148
Część II. Dochodzenie	149
Rozdział 5. Komputerowy proces śledczy	151
Analiza osi czasu	152
X-Ways	153
Plaso (Plaso Langar Að Safna Öllu)	157
Analiza mediów	168

Wyszukiwanie ciągów znaków	169
Odzyskiwanie usuniętych danych	172
Podsumowanie	174
Pytania	174
Materiały dodatkowe	175
Rozdział 6. Analiza artefaktów systemu Windows	176
Profile użytkowników	177
Rejestr systemu Windows	179
Wykorzystanie konta	181
Ostatnie logowanie/ostatnia zmiana hasła	181
Analiza plików	186
Przeglądanie pamięci podręcznej miniatur	186
Przeglądanie danych z przeglądarek firmy Microsoft	188
Ostatnio używane/ostatnio użyte	189
Zagłądanie do kosza	191
Pliki skrótów (LNK)	192
Odszyfrowywanie list szybkiego dostępu	194
Wpisy Shellbag	195
Funkcja prefetch	197
Identyfikowanie fizycznej lokalizacji urządzenia	198
Określanie strefy czasowej	198
Analiza historii sieci	199
Zrozumieć dziennik zdarzeń WLAN	200
Analiza działania programu	201
UserAssist	201
Pamięć podręczna Shimcache	202
Urządzenia USB/podłączone urządzenia	203
Podsumowanie	205
Pytania	205
Materiały dodatkowe	206
Rozdział 7 Analiza pamięci RAM	207
Podstawowe informacje o pamięci RAM	207
Pamięć o dostępie swobodnym?	208
Źródła danych przechowywanych w pamięci RAM	210
Przechwytywanie zawartości pamięci RAM	212
Przygotowanie urządzenia do przechwytywania	213
Narzędzia do przechwytywania zawartości pamięci RAM	213
Narzędzia do analizy pamięci RAM	217
Bulk Extractor	218
Volix II	222
Podsumowanie	224
Pytania	224
Materiały dodatkowe	225

Rozdział 8. Wiadomości e-mail – techniki śledcze	226
Protokoły poczty elektronicznej	227
Protokół SMTP	227
Protokół POP	228
Protokół IMAP	229
Zrozumieć pocztę internetową	229
Dekodowanie e-maila	230
Format wiadomości e-mail	230
Załączniki	233
Analiza e-maili w aplikacjach pocztowych	234
Microsoft Outlook/Outlook Express	234
Microsoft Windows Live	235
Mozilla Thunderbird	235
Analiza poczty internetowej	237
Podsumowanie	240
Pytania	240
Materiały dodatkowe	241
Rozdział 9. Artefakty internetowe	242
Przeglądarki internetowe	242
Google Chrome	243
Internet Explorer/Microsoft Edge	249
Firefox	256
Media społecznościowe	262
Facebook	265
Twitter	266
Usługodawca	267
Udostępnianie plików w sieciach peer-to-peer	268
Ares	269
eMule	269
Shareaza	271
Chmura obliczeniowa	272
Podsumowanie	275
Pytania	276
Materiały dodatkowe	277
Część III. Raportowanie	279
Rozdział 10. Pisanie raportów	281
Skuteczne robienie notatek	281
Pisanie raportu	283
Przeanalizowane dowody	285
Szczegóły związane z zabezpieczeniem materiałów	286
Szczegóły analizy	286

Załączniki/szczegóły techniczne	287
Podsumowanie	289
Pytania	289
Materiały dodatkowe	290
Rozdział 11 Etyka biegłych	291
Rodzaje postępowań	291
Faza przygotowawcza	293
Curriculum vitae	295
Zeznania i dowody	297
Zachowanie etyczne	299
Podsumowanie	302
Pytania	302
Materiały dodatkowe	303
Odpowiedzi do pytań	305

oprac. BPK