

# Spis treści |

|                                                              |           |
|--------------------------------------------------------------|-----------|
| <b>O autorze .....</b>                                       | <b>11</b> |
| <b>O recenzencie .....</b>                                   | <b>12</b> |
| <b>Wprowadzenie .....</b>                                    | <b>13</b> |
| <b>Rozdział 1</b>                                            |           |
| <b>Rodzaje dochodzeń w informatyce śledczej .....</b>        | <b>17</b> |
| Różnice w dochodzeniach z obszaru informatyki śledczej ..... | 18        |
| Dochodzenia karne .....                                      | 20        |
| Pierwsi na miejscu zdarzenia .....                           | 20        |
| Śledczy .....                                                | 21        |
| Technik kryminalistyki .....                                 | 21        |
| Nielegalne zdjęcia .....                                     | 23        |
| Stalking .....                                               | 26        |
| Spiskowanie .....                                            | 29        |
| Śledztwa korporacyjne .....                                  | 31        |
| Wykroczenia pracowników .....                                | 32        |
| Szpiegostwo przemysłowe .....                                | 35        |
| Zagrożenie wewnętrzne .....                                  | 40        |
| Studia przypadków .....                                      | 43        |
| Sprawa Dennisa Radera .....                                  | 43        |
| Silk Road .....                                              | 44        |
| Atak terrorystyczny w San Bernardino .....                   | 46        |
| Kradzież własności intelektualnej .....                      | 48        |
| Podsumowanie .....                                           | 49        |
| Pytania .....                                                | 49        |
| Materiały dodatkowe .....                                    | 50        |
| <b>Rozdział 2</b>                                            |           |
| <b>Proces analizy śledczej .....</b>                         | <b>51</b> |
| Rozważania przed dochodzeniem .....                          | 51        |
| Stacja robocza dla śledczego .....                           | 52        |
| Zestaw mobilnego reagowania .....                            | 54        |

|                                                         |    |
|---------------------------------------------------------|----|
| Oprogramowanie śledcze .....                            | 57 |
| Szkolenia dla śledczych .....                           | 61 |
| Analiza informacji o sprawie i zagadnień prawnych ..... | 62 |
| Pozyskiwanie danych .....                               | 65 |
| Łańcuch dowodowy .....                                  | 67 |
| Proces analizy .....                                    | 71 |
| Daty i strefy czasowe .....                             | 71 |
| Analiza skrótów .....                                   | 72 |
| Analiza sygnatur plików .....                           | 74 |
| Antywirus .....                                         | 76 |
| Raportowanie wyników .....                              | 80 |
| Szczegóły do uwzględnienia w raporcie .....             | 80 |
| Udokumentuj fakty i okoliczności .....                  | 82 |
| Podsumowanie raportu .....                              | 83 |
| Podsumowanie .....                                      | 84 |
| Pytania .....                                           | 84 |
| Materiały dodatkowe .....                               | 85 |

### Rozdział 3

|                                                          |           |
|----------------------------------------------------------|-----------|
| <b>Pozyskiwanie dowodów .....</b>                        | <b>86</b> |
| Eksploracja dowodów .....                                | 86        |
| Środowiska do prowadzenia badań kryminalistycznych ..... | 89        |
| Walidacja narzędzi .....                                 | 90        |
| Tworzenie sterylnych nośników .....                      | 95        |
| Zrozumieć blokowanie zapisu .....                        | 99        |
| Tworzenie obrazów kryminalistycznych .....               | 102       |
| Format DD .....                                          | 104       |
| Plik dowodowy EnCase .....                               | 105       |
| Dyski SSD .....                                          | 106       |
| Narzędzia do obrazowania .....                           | 107       |
| Podsumowanie .....                                       | 120       |
| Pytania .....                                            | 121       |
| Materiały dodatkowe .....                                | 122       |

### Rozdział 4

|                                          |            |
|------------------------------------------|------------|
| <b>Systemy komputerowe .....</b>         | <b>123</b> |
| Proces rozruchu .....                    | 123        |
| Kryminalistyczny nośnik rozruchowy ..... | 126        |
| Dyski twarde .....                       | 129        |
| Partycje w MBR .....                     | 132        |

|                                                                       |     |
|-----------------------------------------------------------------------|-----|
| Partycje GPT .....                                                    | 135 |
| Host Protected Area (HPA) i Device Configuration Overlays (DCO) ..... | 139 |
| Zrozumieć systemy plików .....                                        | 140 |
| System plików FAT .....                                               | 140 |
| Obszar danych .....                                                   | 145 |
| Długie nazwy plików .....                                             | 147 |
| Odzyskiwanie usuniętych plików .....                                  | 148 |
| Przestrzeń luzu .....                                                 | 150 |
| System plików NTFS .....                                              | 151 |
| Podsumowanie .....                                                    | 161 |
| Pytania .....                                                         | 162 |
| Materiały dodatkowe .....                                             | 163 |

## Rozdział 5

|                                                      |            |
|------------------------------------------------------|------------|
| <b>Komputerowy proces śledczy .....</b>              | <b>164</b> |
| Analiza osi czasu .....                              | 164        |
| X-Ways .....                                         | 166        |
| Plaso (Plaso Langer Að Safna Öllu) .....             | 170        |
| Analiza mediów .....                                 | 181        |
| Wyszukiwanie ciągów znaków .....                     | 183        |
| Odzyskiwanie usuniętych danych .....                 | 185        |
| Podsumowanie .....                                   | 188        |
| Pytania .....                                        | 188        |
| Materiały dodatkowe .....                            | 189        |
| Ćwiczenia .....                                      | 189        |
| Zbiór danych .....                                   | 189        |
| Wymagane oprogramowanie .....                        | 190        |
| Ćwiczenie z analizy wiadomości e-mail .....          | 190        |
| Ćwiczenie z analizy obrazów kryminalistycznych ..... | 190        |

## Rozdział 6

|                                                          |            |
|----------------------------------------------------------|------------|
| <b>Analiza artefaktów systemu Windows .....</b>          | <b>191</b> |
| Profile użytkowników .....                               | 192        |
| Rejestr systemu Windows .....                            | 194        |
| Wykorzystanie konta .....                                | 196        |
| Ostatnie logowanie/ostatnia zmiana hasła .....           | 196        |
| Analiza plików .....                                     | 202        |
| Przeglądanie pamięci podręcznej miniatur .....           | 202        |
| Przeglądanie danych z przeglądarki firmy Microsoft ..... | 204        |
| Ostatnio używane/ostatnio użyte .....                    | 206        |

|                                                        |     |
|--------------------------------------------------------|-----|
| Zagłębienie do kosza .....                             | 208 |
| Pliki skrótów (LNK) .....                              | 209 |
| Odszyfrowywanie list szybkiego dostępu .....           | 210 |
| Wpisy Shellbag .....                                   | 212 |
| Funkcja prefetch .....                                 | 214 |
| Identyfikowanie fizycznej lokalizacji urządzenia ..... | 215 |
| Określanie strefy czasowej .....                       | 215 |
| Analiza historii sieci .....                           | 216 |
| Zrozumieć dziennik zdarzeń WLAN .....                  | 217 |
| Analiza działania programu .....                       | 218 |
| UserAssist .....                                       | 218 |
| Pamięć podręczna Shimcache .....                       | 219 |
| Urządzenia USB/podłączone urządzenia .....             | 220 |
| Podsumowanie .....                                     | 222 |
| Pytania .....                                          | 223 |
| Materiały dodatkowe .....                              | 224 |
| Ćwiczenie .....                                        | 224 |
| Zbiór danych .....                                     | 224 |
| Wymagane oprogramowanie .....                          | 224 |
| Scenariusz .....                                       | 224 |

## Rozdział 7

|                                                           |            |
|-----------------------------------------------------------|------------|
| <b>Analiza pamięci RAM .....</b>                          | <b>226</b> |
| Podstawowe informacje o pamięci RAM .....                 | 226        |
| Pamięć o dostępie swobodnym? .....                        | 227        |
| Źródła danych przechowywanych w pamięci RAM .....         | 230        |
| Przechwytywanie zawartości pamięci RAM .....              | 232        |
| Przygotowanie urządzenia do przechwytywania .....         | 232        |
| Narzędzia do przechwytywania zawartości pamięci RAM ..... | 233        |
| Narzędzia do analizy pamięci RAM .....                    | 237        |
| Bulk Extractor .....                                      | 237        |
| Volix II .....                                            | 241        |
| Podsumowanie .....                                        | 244        |
| Pytania .....                                             | 245        |
| Materiały dodatkowe .....                                 | 246        |

## Rozdział 8

|                                                   |            |
|---------------------------------------------------|------------|
| <b>Wiadomości e-mail — techniki śledcze .....</b> | <b>247</b> |
| Protokoły poczty elektronicznej .....             | 248        |
| Protokół SMTP .....                               | 248        |
| Protokół POP .....                                | 249        |

|                                                |     |
|------------------------------------------------|-----|
| Protokół IMAP .....                            | 250 |
| Zrozumieć pocztę internetową .....             | 250 |
| Dekodowanie e-maila .....                      | 251 |
| Format wiadomości e-mail .....                 | 251 |
| Załączniki .....                               | 255 |
| Analiza e-maili w aplikacjach pocztowych ..... | 256 |
| Microsoft Outlook/Outlook Express .....        | 256 |
| Microsoft Windows Live .....                   | 256 |
| Mozilla Thunderbird .....                      | 257 |
| Analiza poczty internetowej .....              | 259 |
| Podsumowanie .....                             | 263 |
| Pytania .....                                  | 263 |
| Materiały dodatkowe .....                      | 264 |
| Ćwiczenie .....                                | 264 |
| Zbiór danych .....                             | 264 |
| Wymagane oprogramowanie .....                  | 264 |
| Scenariusz .....                               | 265 |
| Konta e-mailowe .....                          | 265 |

## Rozdział 9

|                                                       |            |
|-------------------------------------------------------|------------|
| <b>Artefakty internetowe .....</b>                    | <b>266</b> |
| Przeglądarki internetowe .....                        | 266        |
| Google Chrome .....                                   | 267        |
| Internet Explorer/Microsoft Edge (stara wersja) ..... | 274        |
| Firefox .....                                         | 282        |
| Media społecznościowe .....                           | 288        |
| Facebook .....                                        | 291        |
| Twitter .....                                         | 292        |
| Usługodawca .....                                     | 293        |
| Udostępnianie plików w sieciach peer-to-peer .....    | 294        |
| Ares .....                                            | 295        |
| eMule .....                                           | 296        |
| Shareaza .....                                        | 298        |
| Chmura obliczeniowa .....                             | 299        |
| Podsumowanie .....                                    | 302        |
| Pytania .....                                         | 303        |
| Materiały dodatkowe .....                             | 304        |

**Rozdział 10**

|                                                                  |            |
|------------------------------------------------------------------|------------|
| <b>Śledztwa w sieci</b> .....                                    | <b>305</b> |
| Śledztwa pod przykrywką .....                                    | 305        |
| Platforma do pracy pod przykrywką .....                          | 307        |
| Tożsamość w sieci .....                                          | 308        |
| Wyszukiwanie informacji o podejrzanym .....                      | 313        |
| Rejestracja czynności wykonywanych w toku śledztwa w sieci ..... | 321        |
| Podsumowanie .....                                               | 327        |
| Pytania .....                                                    | 328        |
| Materiały dodatkowe .....                                        | 330        |

**Rozdział 11**

|                                                     |            |
|-----------------------------------------------------|------------|
| <b>Podstawy działania sieci komputerowych</b> ..... | <b>331</b> |
| Model Open Source Interconnection (OSI) .....       | 332        |
| Warstwa fizyczna (warstwa 1) .....                  | 332        |
| Warstwa łącza danych (warstwa 2) .....              | 333        |
| Warstwa sieciowa (warstwa 3) .....                  | 334        |
| Warstwa transportowa (warstwa 4) .....              | 334        |
| Warstwa sesji (warstwa 5) .....                     | 335        |
| Warstwa prezentacji (warstwa 6) .....               | 335        |
| Warstwa aplikacji (warstwa 7) .....                 | 335        |
| Enkapsulacja .....                                  | 335        |
| TCP/IP .....                                        | 336        |
| IPv4 .....                                          | 338        |
| IPv6 .....                                          | 340        |
| Protokoły warstwy aplikacji .....                   | 342        |
| Protokoły warstwy transportowej .....               | 343        |
| Protokoły warstwy internetowej .....                | 343        |
| Podsumowanie .....                                  | 345        |
| Pytania .....                                       | 346        |
| Materiały dodatkowe .....                           | 347        |

**Rozdział 12**

|                                                       |            |
|-------------------------------------------------------|------------|
| <b>Pisanie raportów</b> .....                         | <b>348</b> |
| Skuteczne robienie notatek .....                      | 348        |
| Pisanie raportu .....                                 | 350        |
| Przeanalizowane dowody .....                          | 353        |
| Szczegóły związane z zabezpieczeniem materiałów ..... | 354        |
| Szczegóły analizy .....                               | 354        |
| Załączniki/szczegóły techniczne .....                 | 355        |

|                           |     |
|---------------------------|-----|
| Podsumowanie .....        | 357 |
| Pytania .....             | 357 |
| Materiały dodatkowe ..... | 358 |

## **Rozdział 13**

### **Etyka biegłych .....** 359

|                           |     |
|---------------------------|-----|
| Rodzaje postępowań .....  | 359 |
| Faza przygotowawcza ..... | 362 |
| Curriculum vitae .....    | 363 |
| Zeznania i dowody .....   | 365 |
| Zachowanie etyczne .....  | 368 |
| Podsumowanie .....        | 371 |
| Pytania .....             | 371 |
| Materiały dodatkowe ..... | 372 |

### **Odpowiedzi do pytań .....** 373

|                   |     |
|-------------------|-----|
| Rozdział 1 .....  | 373 |
| Rozdział 2 .....  | 373 |
| Rozdział 3 .....  | 373 |
| Rozdział 4 .....  | 374 |
| Rozdział 5 .....  | 374 |
| Rozdział 6 .....  | 374 |
| Rozdział 7 .....  | 374 |
| Rozdział 8 .....  | 375 |
| Rozdział 9 .....  | 375 |
| Rozdział 10 ..... | 375 |
| Rozdział 11 ..... | 376 |
| Rozdział 12 ..... | 376 |
| Rozdział 13 ..... | 376 |