

Spis treści

Wprowadzenie	31
Rozdział 1. Zakres informatyki śledczej	33
Popularne mity z dziedziny informatyki śledczej	34
Mit nr 1. Informatyka śledcza i bezpieczeństwo teleinformatyczne to jedno i to samo	34
Mit nr 2. Informatyka śledcza polega na analizowaniu komputerów	34
Mit nr 3. Informatyka śledcza dotyczy dochodzeń w sprawie przestępstw informatycznych	35
Mit nr 4. Informatyka śledcza służy do odzyskiwania usuniętych plików	35
Typy uzyskiwanych dowodów w informatyce śledczej	36
Poczta elektroniczna	36
Pliki graficzne	38
Filmy	39
Odwiedzone witryny i wyrażenia wyszukiwane w internecie	40
Analiza śledcza telefonów komórkowych	41
Analiza śledcza urządzeń IoT	42
Jakie umiejętności powinien posiadać informatyk śledczy?	42
Wiedza z obszaru informatyki	42
Wiedza z zakresu prawa	43
Umiejętności komunikacyjne	43
Znajomość języków	43
Nieustanne kształcenie się	43
Programowanie	44
Poufność	44
Znaczenie informatyki śledczej	44
Możliwości kariery	45
Historia informatyki śledczej	46
Lata 80. — pojawienie się komputerów osobistych	47
Lata 90. — wpływ internetu	47
Pierwsza dekada XXI wieku — kryptowaluty, IoT, szyfrowanie i efekt Edwarda Snowdena	52
Szkolenia i edukacja	53
Szkolenia w organach ścigania	53
Kursy w szkołach średnich	54
Kursy uniwersyteckie	55
Certyfikaty zawodowe	55
Podsumowanie	59
Najważniejsze pojęcia	61
Sprawdzian wiedzy	62

Rozdział 2. System operacyjny Windows i systemy plików	67
Pamięć fizyczna i logiczna	69
Przechowywanie plików	69
Stronicowanie	72
Konwersja plików i formaty liczbowe	74
Konwersja z formatu dwójkowego na dziesiętny	75
Liczby szesnastkowe	75
Konwersja z formatu szesnastkowego na dziesiętny	75
Konwersja z formatu szesnastkowego na ASCII	76
Wykorzystywanie danych szesnastkowych do ustalenia typu pliku	79
Unicode	80
Systemy operacyjne	80
Proces rozruchu	80
System plików w systemie Windows	82
Rejestr systemu Windows	91
Typy danych w rejestrze	93
Przeglądarka rejestru z pakietu FTK	93
Microsoft Office	94
Funkcje systemu Microsoft Windows	95
Windows Vista	95
Windows 7	100
Windows 8.1	112
Windows 10	114
Microsoft Office 365	115
Podsumowanie	115
Ważne pojęcia	116
Sprawdzian wiedzy	120
 Rozdział 3. Sprzęt komputerowy	 125
Dyski twarde	126
SCSI	126
IDE	127
SATA	128
Klonowanie dysków twardych PATA i SATA	130
Urządzenia do klonowania	131
Pamięć wymienna	138
FireWire	138
Pamięć USB	138
Zewnętrzne dyski twarde	139
Karty MMC	141
Podsumowanie	151
Ważne pojęcia	151
Sprawdzian wiedzy	153
Literatura	156

Rozdział 4. Zbieranie dowodów w laboratorium informatyki śledczej	157
Wymagania dotyczące laboratorium	158
ASCLD	158
ASCLD/LAB	158
Wytyczne ASCLD/LAB z zakresu zarządzania laboratorium kryminalistycznym	159
ISO/IEC 17025:2017	160
SWGDE	160
Prywatne laboratoria informatyki śledczej	161
Laboratorium zbierania dowodów	162
Laboratorium przygotowywania e-maili	162
Inwentaryzacja materiałów	162
Systemy informatyczne dla laboratoriów	163
Hosting	163
Wymagania stawiane laboratorium informatyki śledczej	164
Układ laboratorium	164
Zarządzanie laboratorium	184
Dostęp do laboratorium	185
Pozyskiwanie dowodów z urządzeń	187
Korzystanie z dd	187
Stosowanie wyrażeń regularnych GREP	188
Skimmery	195
Steganografia	198
Podsumowanie	198
Ważne pojęcia	199
Sprawdzian wiedzy	201
Rozdział 5. Dochodzenia z wykorzystaniem internetu	205
Praca pod przykrywką	206
Budowanie tożsamości	207
Tworzenie kont e-mailowych	208
Ukrywanie tożsamości	210
Dochodzenia dotyczące dark webu	212
Platforma OSINT	213
Tor	214
Invisible Internet Project	214
Freenet	215
SecureDrop	215
Sklepy w dark webie	215
Waluty wirtualne	217
Bitcoin	217
Venmo i Vicemo	218
Dowody z witryn	219
Archiwa witryn	219
Statystyki dotyczące witryn	219

Sprawdzanie podejrzanego	221
Wyszukiwanie danych osobowych	221
Grupy hobbystyczne i grupy użytkowników	224
Szukanie skradzionej własności	226
Przestępstwa w internecie	239
Kradzież tożsamości	240
Karty kredytowe na sprzedaż	240
Elektroniczne karty medyczne	240
Dochodzenia przeciwko podróbkom i rozpowszechnianiu broni	241
Cybernękanie	241
Sieci społecznościowe	241
Przechwytywanie komunikacji internetowej	242
Używanie zrzutów ekranu	242
Wykorzystywanie filmów	243
Wyświetlanie plików cookie	244
Używanie rejestru systemu Windows	245
Przeglądarka Edge	246
Podsumowanie	246
Ważne pojęcia	247
Sprawdzian wiedzy	249
Rozdział 6. Dokumentowanie dochodzenia	255
Uzyskiwanie dowodów od dostawców usług	255
Dokumentowanie miejsca zdarzenia	257
Zajmowanie dowodów	258
Analizy na miejscu zdarzenia	258
Wyposażenie policjanta techniki kryminalistycznej	259
Dokumentowanie dowodów	260
Uzupełnianie formularza łańcucha dowodowego	260
Wypełnianie arkusza informacji o komputerze	261
Wypełnianie arkusza dotyczącego dysku twardego	263
Wypełnianie arkusza dotyczącego serwera	263
Narzędzia do dokumentowania dochodzenia	265
FragView	265
Przydatne aplikacje mobilne	265
Pisanie raportów	266
Strefy czasowe i zmiana czasu	267
Pisanie kompletnego raportu	268
Udział biegłych w procesie	272
Biegły sądowy	273
Zadania biegłego	273
Przygotowania biegłego do procesu	273
Podsumowanie	275
Ważne pojęcia	276
Sprawdzian wiedzy	277

Rozdział 7. Dopuszczalność dowodów elektronicznych	281
Historia i struktura amerykańskiego systemu prawnego	282
Źródła systemu prawnego Stanów Zjednoczonych	283
Omówienie systemu sądowego Stanów Zjednoczonych	284
W sali sądowej	288
Dopuszczalność dowodów	291
Prawo konstytucyjne	292
Pierwsza poprawka	292
Pierwsza poprawka a internet	292
Czwarta poprawka	295
Piąta poprawka	309
Szósta poprawka	311
Ustawy Kongresu	311
Ustawa CLOUD (Clarifying Lawful Overseas Use of Data)	318
Zasady dopuszczalności dowodów	319
Obrona w sprawach karnych	324
Kalifornijska ustawa o ochronie prywatności konsumentów	325
Reguła 23 NYCRR 500 NYDFS	325
Kanadyjska ustawa o ochronie danych osobowych i dokumentach elektronicznych	326
Błędy w informatyce śledczej	327
Pornografia w sali szkolnej	327
Struktura systemu prawnego w Unii Europejskiej	327
Źródła prawa europejskiego	328
Struktura prawa Unii Europejskiej	328
Azjatyckie przepisy o ochronie prywatności	335
Chiny	335
Indie	335
Podsumowanie	336
Ważne pojęcia	337
Sprawdzian wiedzy	341
Rozdział 8. Analiza śledcza sieci i reagowanie na incydenty	345
Używane narzędzia	346
Urządzenia sieciowe	347
Serwery proxy	348
Serwery WWW	348
Serwery DHCP	351
Dzienniki DHCP	354
Koncentrator	354
Przełącznik	354
Serwery SMTP	355
Serwery DNS	357
Plik hosts	358
Protokół DNS	358
ICANN	358

Traceroute	359
Routery	359
Systemy wykrywania włamań	368
Zapory	369
Porty	370
Omówienie modelu OSI	371
Warstwa fizyczna	371
Warstwa łącza danych	372
Warstwa sieciowa	372
Warstwa transportowa	373
Warstwa sesji	374
Warstwa prezentacji	374
Warstwa aplikacji	374
Wprowadzenie do usług VoIP	376
Protokół VoIP	376
Wady telefonii VoIP	376
System PBX	376
Protokół SIP	378
STUN	378
Reagowanie na incydenty	378
STIX, TAXII i Cybox	379
Ataki APT	380
APT10	380
Łańcuch etapów cyberataku	381
Wskaźniki naruszeń	384
Badanie ataku sieciowego	387
Pamięć RAM	388
AmCache	388
ShimCache	388
ShellBags	389
Usługa VSC	389
Narzędzia EDR	389
Kibana	389
Log2Timeline i Plaso	390
Stacja robocza SANS SIFT	390
Rejestr systemu Windows	392
Podsumowanie	394
Ważne pojęcia	395
Sprawdzian wiedzy	397
Rozdział 9. Analiza śledcza urządzeń mobilnych	401
Sieć komórkowa	403
Stacja bazowa	404
Stacja abonencka	407
Typy sieci komórkowych	412

Analiza śledcza kart SIM	415
Rodzaje dowodów	418
Specyfikacje urządzeń	419
Pamięć i procesor	419
Akumulatory	419
Inny sprzęt	419
Mobilne systemy operacyjne	420
Android	420
System operacyjny Symbian	429
BlackBerry 10	429
Windows Phone	430
Standardowe procedury operacyjne dotyczące dowodów z telefonów mobilnych	430
NIST	430
Analiza śledcza telefonów	435
Narzędzia do analizy śledczej telefonów komórkowych	435
Badania logiczne i fizyczne	437
Ręczne badanie telefonów komórkowych	437
Zestawy do flashowania	438
Dostawcy usług GPS	439
Satelitarne usługi telekomunikacyjne	439
Kwestie prawne	439
Agencja NCIC	440
Inne urządzenia mobilne	442
Tablety	442
Śledzenie GPS	443
Dokumentowanie dochodzenia	444
Podsumowanie	444
Ważne pojęcia	445
Sprawdzian wiedzy	449
Rozdział 10. Analiza aplikacji mobilnych w dochodzeniach	453
Analizy statyczne i dynamiczne	454
Analiza statyczna	454
Analiza statyczna — przegląd kodu	456
Analiza dynamiczna	458
Wprowadzenie do narzędzia Debookey	459
Aplikacje randkowe	467
Tinder	467
Grindr	471
Aplikacje do wspólnych przejazdów	475
Uber	475
Komunikatory	478
Skype	478
Podsumowanie	481
Ważne pojęcia	481
Sprawdzian wiedzy	482

Rozdział 11. Analiza śledcza zdjęć	485
Organizacja NCMEC	487
Organizacja Project VIC	488
Studia przypadku	488
Selfie z Facebooka	488
Jak złapać pedofila?	488
Szantaż	489
Czym jest zdjęcie cyfrowe?	489
Aplikacje i usługi z dziedziny fotografii cyfrowej	490
Analiza plików ze zdjęciami	491
EXIF	492
Dopuszczalność dowodów	495
Federalne reguły dowodowe	495
Zdjęcia analogowe i cyfrowe	495
Studia przypadków	496
Ogólnosiwiatowe poszukiwania	497
Jednostka rozpoznawania twarzy w nowojorskiej policji	498
Podsumowanie	498
Ważne pojęcia	499
Sprawdzian wiedzy	500
 Rozdział 12. Analiza śledcza komputerów Mac	 503
Krótką historia	504
Komputery Macintosh	504
Mac mini z systemem OS X Server	504
iPod	505
iPhone	506
iPad	507
iPad Pro	508
Apple Watch	508
Urządzenia firmy Apple z obsługą Wi-Fi	510
Apple TV	510
AirPort Express	511
AirPort Extreme	511
AirPort Time Capsule	511
Systemy plików w komputerach Macintosh	512
System HFS	512
HFS+	513
APFS	514
Analiza śledcza komputerów Mac	518
Czas epoki	520
DMG	521
Pliki PLIST	522

Bazy SQLite	524
Pliki poczty elektronicznej	524
Plik hibernacji	524
Systemy operacyjne w komputerach Macintosh	524
macOS Catalina	525
Narzędzie FileVault	526
Narzędzie dyskowe	526
Funkcja pęku kluczy w systemie macOS	526
Pęk kluczy iCloud	526
Kilka wyświetlaczy	527
Powiadomienia	527
Tagi	527
Safari	527
Tryb Target Disk Mode i klonowanie urządzeń	529
Urządzenia mobilne firmy Apple	530
iOS	531
Urządzenia firmy Apple w środowisku korporacyjnym	549
Akumulator	549
Analiza śledcza komputerów Mac	549
Studia przypadków	551
Znajdź mój iPhone	551
Poszukiwany haktywista	552
Michael Jackson	552
Skradziony iPhone	552
Nalot na handlarzy narkotyków	552
Proces o morderstwo	552
Podsumowanie	553
Ważne pojęcia	553
Sprawdzian wiedzy	557
Rozdział 13. Studia przypadków	561
Silk Road	562
Geneza powstania serwisu Silk Road	562
Groźenie śmiercią	565
Zablokowanie serwisu Silk Road	565
Aresztowanie Ulbrichta	566
Postępowanie przedprocesowe w sprawie Rossa Ulbrichta	567
Proces Rossa Ulbrichta	569
Dowody z laptopa	569
Werdykt	571
Masakra w Las Vegas	571
Zacarias Moussaoui	572
Informacje wstępne	573
Dowody elektroniczne	574

Sprzeciwy doradcy	575
Pismne oświadczenie pod przysięgą oskarżenia	576
Rekwizyty	577
Seryjny morderca BTK	578
Profil mordercy	578
Dowody	579
Cybernękani	579
Federalne przepisy przeciwko nękaniu	580
Stanowe przepisy przeciwko nękaniu	580
Sygnały ostrzegawcze związane z cybernękaniem	580
Czym jest cybernękani?	580
Phoebe Prince	581
Ryan Halligan	581
Megan Meier	582
Tyler Clementi	582
Sport	584
Podsumowanie	585
Ważne pojęcia	586
Sprawdzian wiedzy	586
Zadanie	593
Rozdział 14. Analiza śledcza internetu rzeczy i nowe technologie	595
Sieć 5G	596
Wi-Fi 6	599
Sieci kratowe Wi-Fi	599
Shodan	600
Botnet Mirai	600
Kopanie kryptowalut	601
Alexa	601
Mikrochip	602
Narzędzia śledzące aktywność fizyczną	603
Apple Watch	604
Kamery sportowe	606
Bezpieczeństwo policji	606
Pojazdy policyjne	608
Analiza śledcza pojazdów	609
Prosta metoda znajdowania zaawansowanych urządzeń	610
Podsumowanie	611
Ważne pojęcia	611
Sprawdzian wiedzy	613
Klucz odpowiedzi	617