

Spis treści

O autorach	9
Podziękowania	11
Wprowadzenie	13
ROZDZIAŁ 1. Informatyka śledcza i narzędzia typu open source	17
Wprowadzenie	17
Czym jest informatyka śledcza?	18
Cele dochodzeń informatyki śledczej	19
Proces cyfrowej analizy śledczej	20
Czym jest open source?	21
Oprogramowanie darmowe a otwarte	22
Licencje open source	22
Zalety korzystania z oprogramowania open source	23
Edukacja	23
Przenośność i elastyczność	24
Cena	24
Inne zalety	25
Podsumowanie	26
Bibliografia	26
ROZDZIAŁ 2. Platforma robocza typu open source	27
Przygotowanie stanowiska badawczego	27
Budowanie pakietów oprogramowania	27
Instalowanie interpreterów	28
Praca z binarnymi obrazami nośników danych	28
Praca z systemami plików	29
Stacja robocza z systemem Linux	29
Rozpakowywanie pakietów oprogramowania	30
Pakiet GNU Build System	31
Systemy kontroli wersji pakietów oprogramowania	35
Instalowanie interpreterów	36
Praca z binarnymi obrazami nośników danych	38
Stacja robocza z systemem Windows	46
Budowanie pakietów oprogramowania	47
Instalowanie interpreterów	49

Praca z binarnymi obrazami nośników danych	52
Praca z systemami plików	56
Podsumowanie	58
Bibliografia	59
ROZDZIAŁ 3. Analiza zawartości dysku i systemu plików	61
Analiza zawartości nośników danych — pojęcia podstawowe	61
Abstrakcyjny model systemu plików	62
Pakiet The Sleuth Kit	64
Instalowanie pakietu The Sleuth Kit	65
Narzędzia pakietu	66
Podział na partycje i konfiguracja dysków	77
Identyfikacja i odtwarzanie partycji	78
Macierze RAID	79
Kontenery specjalne	80
Obrazy dysków maszyn wirtualnych	80
Kontenery obrazów binarnych	81
Haszowanie	83
Data carving — odzyskiwanie danych z niealokowanej przestrzeni nośnika danych	85
Foremost	86
Tworzenie binarnych kopii nośników danych	88
Skasowane dane	89
File slack — niewykorzystana przestrzeń na końcu pliku	90
Polecenie dd	92
Polecenie dcfldd	94
Polecenie dc3dd	95
Podsumowanie	96
Bibliografia	96
ROZDZIAŁ 4. Systemy plików i artefakty w systemie Windows	97
Wprowadzenie	97
Systemy plików obsługiwane w systemie Windows	97
System plików FAT	98
System plików NTFS	99
Systemy plików — podsumowanie	107
Rejestr	107
Dzienniki zdarzeń	114
Pliki prefetch	118
Pliki skrótów	120
Pliki wykonywalne	121
Podsumowanie	125
Bibliografia	125

ROZDZIAŁ 5. Systemy plików i artefakty w systemie Linux	127
Wprowadzenie	127
Systemy plików obsługiwane w systemie Linux	127
Warstwa systemu plików	129
Warstwa nazw plików	132
Warstwa metadanych	134
Warstwa jednostek danych	136
Narzędzia księgujące	136
Skasowane dane	137
Menedżer dysków logicznych systemu Linux	137
Proces uruchamiania systemu Linux i jego usług	138
System V	139
BSD	141
Organizacja systemu Linux i artefakty	141
Partycjonowanie	141
Hierarchia systemu plików	141
Pojęcie właściciela plików oraz prawa dostępu do plików	141
Atrybuty plików	143
Pliki ukryte	143
Katalog /tmp	144
Konta użytkowników	144
Katalogi domowe użytkowników	147
Historia poleceń powłoki	149
SSH	149
Artefakty menedżera okien środowiska GNOME	150
Logi (dzienniki zdarzeń)	152
Logi aktywności użytkownika	152
Syslog	153
Przetwarzanie logów z poziomu wiersza poleceń konsoli	155
Zaplanowane zadania	158
Podsumowanie	158
Bibliografia	158
ROZDZIAŁ 6. Systemy plików i artefakty w systemie Mac OS X	159
Wprowadzenie	159
Artefakty systemu plików w Mac OS X	159
Podstawowe struktury systemu HFS+	160
Artefakty systemu operacyjnego Mac OS X	166
Pliki .plist	167
Bundles	167
Uruchamianie systemu i usług	168
Rozszerzenia jądra systemu — kexts	169
Konfiguracja połączeń sieciowych	169

Ukryte katalogi	171
Zainstalowane aplikacje	171
Pliki wymiany i hibernacji	171
Dzienniki systemowe	171
Artefakty związane z aktywnością użytkownika w Mac OS X	172
Katalogi domowe użytkowników	173
Podsumowanie	181
Bibliografia	181
ROZDZIAŁ 7. Artefakty internetowe	183
Wprowadzenie	183
Artefakty przeglądarek sieciowych	183
Przeglądarka Internet Explorer	184
Przeglądarka Firefox	188
Przeglądarka Chrome	196
Przeglądarka Safari	199
Artefakty poczty elektronicznej	203
Pliki PST	204
Formaty mbox i maildir	206
Podsumowanie	210
Bibliografia	210
ROZDZIAŁ 8. Analiza plików	211
Podstawowe zagadnienia analizy plików	211
Identyfikacja zawartości plików	212
Analiza zawartości plików	214
Wyodrębnianie metadanych	216
Zdjęcia i inne pliki graficzne	218
Pliki w formacie JPEG	221
Pliki w formacie GIF	228
Pliki w formacie PNG	229
Pliki w formacie TIFF	229
Pliki audio	230
Pliki w formacie WAV	230
Pliki w formacie MPEG-3/MP3	230
Pliki w formacie MPEG-4 Audio (AAC/M4A)	231
Pliki w formacie ASF/WMA	233
Pliki wideo	234
Pliki w formatach MPEG-1 i MPEG-2	234
Pliki w formacie MPEG-4 Video (MP4)	234
Pliki w formacie AVI	235
Pliki w formacie ASF/WMV	236
Pliki w formacie MOV (Quicktime)	236
Pliki w formacie MKV	237

Pliki archiwum	237
Pliki w formacie ZIP	238
Pliki w formacie RAR	239
Pliki w formacie 7-zip	240
Pliki w formatach TAR, GZIP oraz BZIP2	241
Pliki dokumentów	242
Dokumenty pakietu Office (OLE Compound Files)	242
Dokumenty pakietu Office w formacie Open XML	247
Pliki w formacie ODF (OpenDocument Format)	250
Pliki w formacie RTF (Rich Text Format)	251
Pliki w formacie PDF	252
Podsumowanie	255
Bibliografia	256
ROZDZIAŁ 9. Automatyzacja procesów analizy śledczej	257
Wprowadzenie	257
Graficzne środowiska wspomagające analizę śledczą	257
PyFLAG	258
DFF — Digital Forensics Framework	268
Automatyzacja procesu identyfikacji i wyodrębniania artefaktów	278
Pakiet fiwalk	278
Chronologia zdarzeń	280
Względne znaczniki czasu	283
Pośrednie znaczniki czasu	285
Osadzone znaczniki czasu	287
Periodyczność	288
Częstość występowania i zdarzenia LFO	289
Podsumowanie	291
Bibliografia	292
DODATEK A. Inne bezpłatne narzędzia wspomagające analizę śledczą i powtórzeniową	293
Wprowadzenie	293
Rozdział 3. Analiza zawartości dysku i systemu plików	294
FTK Imager	294
ProDiscover Free	295
Rozdział 4. Artefakty systemu Windows	296
Windows File Analyzer	296
Event Log Explorer	297
LogParser	298
Rozdział 7. Artefakty internetowe	299
Narzędzia Nira Sorfera (Nirsoft)	299
Narzędzia Woanware	300