

SZCZEGÓŁOWY SPIS TREŚCI

OD TŁUMACZA	vii
PRZEDMOWA	xvii
WPROWADZENIE	xix
Dlaczego napisałem tę książkę	xix
Co wyróżnia tę książkę	xx
Dlaczego warto korzystać z linii poleceń	xx
Docelowi czytelnicy i wymagania	xxii
Kto powinien przeczytać tę książkę	xxii
Niezbędna wiedza	xxii
Preinstalowana platforma i oprogramowanie	xxii
Jak zorganizowana jest ta książka	xxii
Zakres tej książki	xxv
Konwencje i format	xxv
0	
OGÓLNY ZARYS INFORMATYKI ŚLEDCZEJ	1
Historia informatyki śledczej	1
Koniec wieku XX	1
2000–2010	2
2010–obecnie	3
Główne kierunki i wyzwania cyfrowego zabezpieczenia	4
Zmiany rozmiaru, lokalizacji i złożoności dowodu	4
Problem wielu jurysdykcji	5
Przemysł, środowisko akademickie i współpraca z organami ścigania	5
Zasady cyfrowego śledztwa post mortem	6
Standardy informatyki śledczej	6
Publikacje recenzowane	7
Branżowe wytyczne i najlepsze praktyki	8
Zasady stosowane w tej książce	9
1	
OMÓWIENIE NOŚNIKÓW DANYCH	11
Magnetyczne nośniki danych	12
Dyski twarde	12
Taśmy magnetyczne	13
Starsze pamięci magnetyczne	15

Pamięć nielotna	15
Dyski półprzewodnikowe (SSD)	16
Napędy USB flash	17
Wymienne karty pamięci	18
Starsze typy pamięci nielotnej	20
Dyski optyczne	20
Płyty kompaktowe	21
Digital Versatile Discs	22
Płyty Blu-ray	23
Starsze dyski optyczne	23
Interfejsy i złącza	23
Serial ATA	24
Serial Attached SCSI i Fibre Channel	26
Non-Volatile Memory Express	28
Universal Serial Bus	30
Thunderbolt	32
Interfejsy starszego typu	33
Polecenia, protokoły i mostki	35
Polecenia ATA	36
Polecenia SCSI	37
Polecenia NVMe	38
Mostkowanie, tunelowanie i przekazywanie	39
Tematy specjalne	40
Obszary dysku DCO i HPA	40
Obszar serwisowy dysku	41
USB Attached SCSI Protocol	41
Advanced Format 4Kn	42
NVMe Namespaces	46
Solid State Hybrid Disks	48
Podsumowanie	48

2

LINUX – PLATFORMA ZABEZPIECZENIA DOCHODZENIOWO-ŚLEDZCEGO

49

Linux i OSS w kontekście dochodzeniowo-śledczym	50
Korzyści stosowania Linuxa i OSS w laboratoriach informatyki śledczej	50
Niewygody stosowania Linuxa i OSS w laboratoriach informatyki śledczej	51
Jądro Linuxa i urządzenia pamięci masowej	52
Wykrywanie urządzeń przez jądro systemu	52
Urządzenia pamięci masowej w katalogu /dev	54
Inne urządzenia specjalne	55
Jądro Linuxa i systemy plików	56
Obsługa systemów plików przez jądro systemu	56
Montowanie systemów plików w systemie Linux	56
Dostęp do systemów plików za pomocą narzędzi śledczych	58
Dystrybucje i powłoki systemu Linux	58
Dystrybucje Linuxa	59
Powłoka	59
Wywołanie komendy	59
Przesyłanie łączami i przekierowania	60
Podsumowanie	60

3

FORMATY OBRAZÓW DOWODOWYCH	61
Obrazy nieprzetworzone (<i>raw</i>)	62
Tradycyjne dd	62
Warianty dd do zastosowań dochodzeniowo-śledczych	63
Narzędzia do odzyskiwania danych	64
Formaty dowodowe	64
EnCase EWF	64
FTK SMART	65
AFF	65
SquashFS jako kontener dowodowy	65
Podstawy SquashFS	65
Kontenery dowodowe SquashFS	66
Podsumowanie	69

4

PLANOWANIE I PRZYGOTOWANIA	71
Dbalność o ścieżkę audytu	72
Zarządzanie zadaniami	72
Historia wiersza poleceń	75
Rejestratory terminali	77
Audyt systemu Linux	78
Organizowanie zebranych dowodów i danych z wyjścia poleceń	79
Konwencje nazewnictwa dla plików i katalogów	79
Skalowalna struktura katalogów śledztwa	82
Zapisywanie wyjścia poleceń za pomocą przekierowania	84
Ocena logistyczna infrastruktury zabezpieczenia	85
Rozmiary obrazów i wymagane miejsce na dysku	85
Kompresja plików	87
Pliki rzadkie	87
Zgłaszane rozmiary plików i obrazów	88
Przenoszenie i kopiowanie obrazów dowodowych	89
Szacowanie czasów ukończenia zadań	90
Wydajność i wąskie gardła	90
Ciepło i czynniki środowiskowe	93
Ustanawianie ochrony przed zapisem	96
Sprzętowe blokery zapisu	97
Programowe blokery zapisu	100
Linuxowe bootowalne płyty CD do informatyki śledczej	101
Nośniki z trybami fizycznego dostępu tylko do odczytu	103
Podsumowanie	104

5

PODŁĄCZANIE BADANEGO NOŚNIKA DO HOSTA ZABEZPIECZENIA	105
Badanie podejrzanego sprzętu komputerowego	106
Analiza sprzętowej konfiguracji komputera i usuwanie dysku	106
Inspekcja sprzętu w badanym komputerze	106
Podłączenie zabezpieczonego dysku do hosta śledczego	107

Przegląd sprzętu hosta zabezpieczenia	107
Identyfikacja podejrzanego napędu	109
Sprawdzanie informacji zwracanych przez badany dysk	111
Dokumentowanie danych identyfikacyjnych urządzenia	111
Sprawdzanie możliwości i funkcji dysku za pomocą hdparm	113
Wydobycie danych SMART za pomocą smartctl	116
Włączanie dostępu do ukrytych sektorów	122
Usuwanie DCO	122
Usuwanie HPA	125
Dostęp do obszaru serwisowego dysku	126
Zabezpieczenie hasłem ATA i dyski samoszyfrujące	129
Identyfikacja i odblokowanie dysków chronionych hasłem ATA	130
Identyfikacja i odblokowanie dysków samoszyfrujących Opal	132
Szyfrowane pendrive'y	136
Podłączanie nośników wymiennych	137
Napędy optyczne	137
Napędy taśmowe	139
Karty pamięci	141
Podłączanie innych nośników	142
Apple Target Disk Mode	142
NVMe SSD	143
Inne urządzenia z dostępem do bloków lub znaków	145
Podsumowanie	145

6

POZYSKIWANIE OBRAZU DOWODOWEGO 147

Pozyskanie obrazu za pomocą narzędzi typu dd	148
Standardowe, unixowe dd i GNU dd	149
Programy dcfldd i dc3dd	151
Pozyskanie obrazów w formatach dowodowych	152
Narzędzie ewfacquire	152
AccessData ftkimager	154
Kontener dowodowy SquashFS	155
Pozyskiwanie obrazu z jednoczesnym zapisem w kilku miejscach	156
Zastosowanie kryptografii podczas zabezpieczania dowodów cyfrowych	157
Podstawy kryptograficznych funkcji skrótu	157
Okna haszowania	159
Podpisywanie obrazu za pomocą PGP lub S/MIME	161
Znaczniki czasu RFC-3161	164
Obsługa awarii i błędów dysku	166
Obsługa błędów w narzędziach informatyki śledczej	166
Narzędzia do odzyskiwania danych	168
SMART i błędy jądra	170
Inne metody w przypadku awarii dysku	171
Uszkodzone dyski optyczne	172
Pozyskiwanie obrazu nośnika przez sieć	173
Zdalne pozyskiwanie obrazów dowodowych za pomocą rdd	173
Bezpieczne, zdalne tworzenie obrazu za pomocą ssh	175
Zdalne pozyskiwanie do kontenera dowodowego SquashFS	177
Pozyskiwanie obrazu zdalnego dysku w formatach EnCase i FTK	178
Zabezpieczanie działającego systemu za pomocą migawek Copy-On-Write	179

Zabezpieczanie nośników wymiennych	180
Karty pamięci	180
Dyski optyczne	181
Taśmy magnetyczne	183
RAID i systemy wielodyskowe	185
Zabezpieczanie zastrzeżonych układów RAID	185
JBOD i RAID-0 – striping dysków	186
Microsoft Dynamic Disks	188
RAID-1 – mirroring dysków	189
Linux RAID-5	190
Podsumowanie	192

7

OPEROWANIE OBRAZAMI DOWODOWYMI	193
Zastosowania kompresji obrazów	194
Standardowe, linuxowe narzędzia do obsługi kompresji	194
Format skompresowany EnCase EWF	195
Format skompresowany FTK SMART	196
Kompresja wbudowana w AFFlib	196
Skompresowane kontenery dowodowe SquashFS	197
Operowanie podzielonymi obrazami	198
Polecenie GNU split	198
Podział obrazów podczas akwizycji	200
Dostęp do zawartości podzielonego obrazu	201
Ponowne składanie podzielonych obrazów	202
Sprawdzanie integralności obrazów dowodowych	203
Sprawdzanie kryptograficznego skrótu utworzonego podczas zabezpieczenia	204
Ponowne obliczanie haszy obrazów dowodowych	204
Kryptograficzne skróty podzielonych obrazów nieprzetworzonych	206
Znajdowanie niepasujących do siebie okien haszowania	206
Sprawdzanie poprawności podpisów cyfrowych i znaczników czasu	207
Przekształcanie formatów obrazów	209
Zamiana obrazów nieprzetworzonych	209
Konwersja z formatu EnCase/E01	212
Konwersja formatu FTK	215
Konwersja formatu AFF	216
Kryptograficzne zabezpieczanie obrazu	218
Szyfrowanie GPG	219
Szyfrowanie OpenSSL	220
Wbudowane szyfrowanie w formatach dowodowych	222
Uniwersalne szyfrowanie dysków	224
Klonowanie i powielanie dysków	226
Przygotowanie kłona dysku	226
Użycie HPA do powielenia liczby sektorów nośnika	227
Zapis obrazu na klonie dysku	228
Przesyłanie i przechowywanie obrazów	229
Zapis na nośniku wymiennym	229
Niedrogie dyski do przechowywania i przenoszenia danych	230
Przesyłanie dużych ilości danych przez sieć	230
Bezpieczne zamazywanie i usuwanie danych	231
Usuwanie pojedynczych plików	232

Bezpieczne zamazywanie zawartości nośników danych	232
Wykorzystanie komendy ATA Security Erase Unit	234
Niszczenie kluczy szyfrowania dysków	235
Podsumowanie	236

8

UZYSKIWANIE DOSTĘPU DO ZAWARTOŚCI NIETYPOWYCH OBRAZÓW 237

Pliki obrazów pozyskanych w celach dowodowych	238
Pliki nieprzetworzonych obrazów dysków oraz urządzenia pętli	238
Pliki obrazów w formatach dowodowych	241
Przygotowanie obrazów startowych za pomocą xmount	244
Obrazy maszyn wirtualnych (VM)	245
QEMU QCOW2	246
VirtualBox VDI	248
VMWare VMDK	249
Microsoft VHD	250
Systemy plików szyfrowane z poziomu systemu operacyjnego	252
Microsoft BitLocker	252
Apple FileVault	258
Linux LUKS	261
TrueCrypt i VeraCrypt	264
Podsumowanie	268

9

WYODRĘBNIANIE PODZBIORÓW DANYCH Z OBRAZÓW DOWODOWYCH 269

Określanie układu partycji oraz typów systemów plików	270
Schematy partycjonowania	270
Tablice partycji	272
Identyfikacja systemów plików	273
Wyodrębnianie zawartości partycji	274
Wyodrębnianie poszczególnych partycji	274
Znajdowanie i wyodrębnianie usuniętych partycji	276
Identyfikowanie i wyodrębnianie przestrzeni między partycjami	278
Wydobycie sektorów z obszarów HPA i DCO	279
Wydobywanie innych fragmentarycznych danych	280
Wyodrębnianie slack space z systemów plików	281
Wyodrębnianie nieprzydzielonych bloków systemu plików	282
Ręczne wyodrębnianie za pomocą przesunięć	282
Podsumowanie	284

UWAGI KOŃCOWE 285

DODATEK OD TŁUMACZA 287

INDEKS 289