

Spis treści

Dystrybucje Linuksa	51
Ewolucja dystrybucji Linuksa	52
Dystrybucje oparte na Debianie	53
Dystrybucje oparte na SUSE	54
Dystrybucje oparte na Red Hacie	55
Dystrybucje oparte na arch Linux	55
Inne dystrybucje	56
Analiza kryminalistyczna systemów Linux	57
DOWODY ZNAJDUJĄCE SIĘ NA NOŚNIKACH PAMIĘCI I W SYSTEMACH PLIKÓW	59
Analiza schematu pamięci i zarządzania woluminem	61
Analiza tablic partycji	61
Zarządca woluminów logicznych	65
Linux Software RAID	70
Analiza kryminalistyczna systemu plików	74
Koncepcja systemu plików w Linuksie	74
Artefakty w systemach plików Linuksa	75
Wyświetlanie i wyodrębnianie danych	78
Analiza ext4	82
Metadane systemu plików — superblok	82
Metadane pliku — i-węzły	85
Wyświetlanie listy plików i wyodrębnianie	87
Analiza btrfs	88
Metadane systemu plików — superblok	89
Metadane pliku — i-węzły	91
Wiele urządzeń i podwoluminów	93
Wyświetlanie listy plików i wyodrębnianie	96
Analiza xfs	98
Metadane systemu plików — superblok	98
Metadane pliku — i-węzły	100
Wyświetlanie listy plików i wyodrębnianie	101
Analiza wymiany systemu Linux	102
Identyfikacja i analiza wymiany	102
Hibernacja	105

Analiza szyfrowania systemu plików	106
Szyfrowanie całego dysku za pomocą LUKS	108
Szyfrowanie katalogów za pomocą eCryptfs	112
Szyfrowanie katalogów za pomocą fscrypt (ext4 directory encryption)	115
Podsumowanie	116
HIERARCHIA KATALOGÓW I ANALIZA KRYMINALISTYCZNA PLIKÓW SYSTEMOWYCH	117
Układ katalogów w Linuksie	117
Hierarchia systemu plików	118
Katalog domowy użytkownika	122
Bazy danych skrótów i NSRL dla Linuksa	128
Typy i identyfikacja plików w systemie Linux	130
Typy plików POSIX	130
Sygnatury i rozszerzenia plików	133
Pliki ukryte	134
Analiza plików z systemu Linux	135
Metadane aplikacji	135
Analiza treści	137
Pliki wykonywalne	138
Awarie i zrzuty rdzenia	140
Zrzuty pamięci procesu	141
Dane dotyczące awarii aplikacji i dystrybucji	144
Awarie jądra	146
Podsumowanie	152
DOWODY ZNAJDUJĄCE SIĘ W LOGACH SYSTEMOWYCH	153
Tradycyjny Syslog	154
Źródło, istotność i priorytet	154
Konfiguracja Sysloga	156
Analiza komunikatów Sysloga	157
Dziennik systemd	159
Funkcje i elementy dziennika systemd	160
Konfiguracja dziennika systemd	161
Analiza zawartości plików dziennika systemd	164
Inne mechanizmy logowania wykorzystywane przez aplikacje i demony	169
Niestandardowe rejestrowanie w Syslogu lub dzienniku systemd	169
Niezależne logi aplikacji serwerowych	171

Niezależne logi aplikacji użytkownika	172
Logi z uruchomienia systemu — ekran logowania Plymouth	174
Logi z jądra i systemu audytu	176
Bufor cykliczny jądra	176
System audytu Linuksa	179
Podsumowanie	184
REKONSTRUKCJA PROCESU ROZRUCHU I INICJALIZACJI SYSTEMU	185
Analiza programów rozruchowych	185
Rozruch z użyciem BIOS-u/MBR oraz GRUB-a	187
Rozruch z użyciem UEFI oraz GRUB-a	189
Konfiguracja GRUB-a	190
Inne programy ładujące	193
Analiza inicjalizacji jądra	194
Parametry przekazywane do jądra w trakcie jego uruchamiania	195
Moduły jądra	197
Parametry jądra	198
Analiza initrd i initramfs	199
Analiza systemd	203
Pliki jednostek systemd	203
Proces inicjalizacji systemd	206
Usługi systemd i demony	208
Aktywacja i usługi na żądanie	210
Planowane uruchomienia poleceń i timery	215
Analiza zasilania i środowiska fizycznego	218
Analiza zasilania i środowiska fizycznego	218
Dowody dotyczące uśpienia, wyłączenia i ponownego uruchomienia	220
Wskaźniki bliskości człowieka	222
Podsumowanie	226
BADANIE ZAINSTALOWANEGO OPROGRAMOWANIA	227
Identyfikacja systemu	228
Informacje o wersji dystrybucji	228
Unikalny identyfikator maszyny	230
Nazwa hosta	230
Analiza instalatora dystrybucji	231
Instalator Debiana	232

Raspberry Pi Raspian	234
Fedora Anaconda	235
SUSE YaST	236
Arch Linux	237
Analiza formatów plików pakietów	238
Format pakietu binarnego w Debianie	238
Menedżer pakietów Red Hat	242
Pakiety Arch Pacman	245
Analiza systemów zarządzania pakietami	247
Debian apt	248
Fedora dnf	251
SUSE zypper	253
Arch Pacman	255
Analiza uniwersalnych pakietów oprogramowania	258
ApplImage	259
Flatpak	262
Snap	264
Centra oprogramowania i interfejsy graficzne	266
Inne metody instalacji oprogramowania	267
Ręcznie skompilowane i zainstalowane oprogramowanie	268
Pakiety języków programowania	269
Wtyczki do aplikacji	269
Podsumowanie	270
IDENTYFIKACJA ARTEFAKTÓW ZWIĄZANYCH Z KONFIGURACJĄ SIECI	271
Analiza konfiguracji sieci	272
Interfejsy i adresowanie w Linuksie	272
Menedżery sieci i konfiguracja specyficzna dla dystrybucji	275
Zapytania DNS	278
Usługi sieciowe	281
Analiza sieci bezprzewodowej	284
Artefakty związane z Wi-Fi	284
Artefakty związane z Bluetooth	289
Artefakty WWAN	291
Artefakty związane z bezpieczeństwem sieci	294
WireGuard, IPsec i OpenVPN	294

Zapory systemu Linux i kontrola dostępu na podstawie adresu IP	297
Ustawienia proxy	300
Podsumowanie	302
ANALIZA KRYMINALISTYCZNA CZASU I LOKALIZACJI	303
Analiza konfiguracji czasu w systemie Linux	303
Formaty czasu	303
Strefy czasowe	306
Czas letni i czas przestępny	307
Synchronizacja czasu	308
Znaczniki czasu i kryminalistyczne osie czasu	311
Internacjonalizacja	313
Ustawienia regionalne i językowe	313
Układ klawiatury	315
Linux i położenie geograficzne	318
Historia lokalizacji geograficznej	318
Usługa geolokalizacji GeoClue	320
Podsumowanie	322
REKONSTRUKCJA PROCESU LOGOWANIA ORAZ AKTYWNOŚCI W ŚRODOWISKU GRAFICZNYM	323
Analiza logowania i sesji w systemie Linux	324
Stanowiska i sesje	325
Logowanie do powłoki	329
X11 i Wayland	333
Logowanie w środowisku graficznym	335
Autentykacja i autoryzacja	339
Pliki użytkowników, grup i haseł	340
Podwyższanie uprawnień	345
GNOME Keyring	348
KDE Wallet Manager	351
Uwierzytelnianie biometryczne za pomocą odcisku palca	353
GnuPG	354
Artefakty pochodzące ze środowisk graficznych systemu Linux	356
Ustawienia i konfiguracja środowiska	356
Dane ze schowka	360
Kosze	362

Zakładki i ostatnie pliki	363
Miniatury obrazów	365
Dobrze zintegrowane ze środowiskiem graficznym aplikacje	368
Inne artefakty występujące w środowiskach graficznych	369
Dostęp przez sieć	372
SSH	372
Pulpit zdalny	375
Sieciowe systemy plików i usługi chmurowe	377
Podsumowanie	380
ŚLADY POZOSTAWIANE PRZEZ URZĄDZENIA PERYFERYJNE	381
Urządzenia peryferyjne w systemie Linux	381
Zarządzanie urządzeniami w Linuksie	382
Identyfikacja urządzeń USB	383
Identyfikacja urządzeń PCI i Thunderbolt	385
Drukarki i skanery	387
Analiza drukarek i historii drukowania	387
Analiza urządzeń skanujących i historii skanowania	390
Pamięć zewnętrzna	391
Identyfikacja nośnika pamięci	391
Dowody montażu systemu plików	393
Podsumowanie	394
POSŁOWIE	395
A	
LISTA PLIKÓW I KATALOGÓW DO SPRAWDZENIA W TRAKCIE ŚLEDZTWA	398
SKOROWIDZ	416