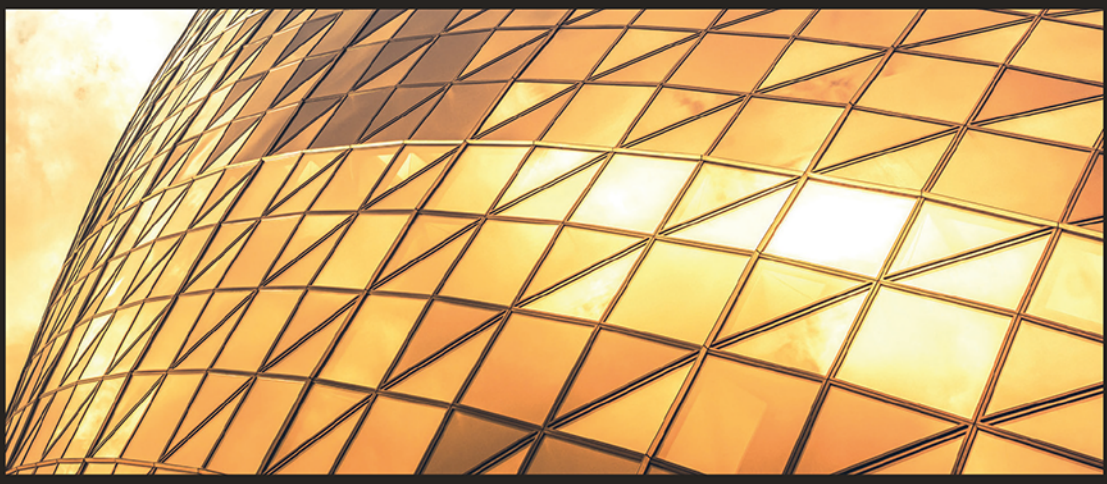
Helion

<packt>



Informatyka śledcza i Kali Linux

Przeprowadź analizy nośników pamięci, ruchu sieciowego i zawartości RAM-u za pomocą narzędzi systemu Kali Linux 2022.x

SHIVA V. N. PARASRAM

Tytuł oryginału: Digital Forensics with Kali Linux Enhance your investigation skills by performing network and memory forensics with Kali Linux 2022.x, 3rd Edition

Tłumaczenie: Grzegorz Kowalczyk

ISBN: 978-83-289-0592-4

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
https://helion.pl/user/opinie/inslk3
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *https://helion.pl* (księgarnia internetowa, katalog książek)

Printed in Poland.

Spis treści

CZĘŚĆ 2.
Podstawowe zagadnienia oraz najlepsze praktyki informatyki śledczej i reagowania na incydenty

CZĘŚĆ 3.
Dochodzenia cyfrowe i reagowanie na incydenty z użyciem narzędzi dostępnych w systemie Kali Linux

CZĘŚĆ 4. Zautomatyzowane narzędzia DFIR

CZĘŚĆ 5. Narzędzia do analizy śledczej połączeń sieciowych

Narzędzia do gromadzenia dowodów cyfrowych

Rozdział 8

W poprzednim rozdziale dowiedziałeś się, że dokumentacja i właściwe procedury postępowania są kluczowymi elementami każdego dochodzenia. Zapewniają one integralność całego dochodzenia poprzez dostarczenie dowodu autentyczności danych oraz zachowanie oryginalnego materiału dowodowego i pełnej dokumentacji postępowania, dzięki czemu otrzymane wyniki są jednoznaczne i powtarzalne (przy użyciu tych samych metod i procedur).

W tym rozdziale skupimy się na zagadnieniach związanych z tworzeniem kopii bitowych nośników cyfrowych, zastosowaniu funkcji skrótu do zapewnienia integralności danych, a także przeprowadzimy szereg ćwiczeń praktycznych mających na celu pozyskiwanie cyfrowego materiału dowodowego z dysków, pamięci RAM i plików stronicowania przy użyciu różnych narzędzi.

Pozyskiwanie i zabezpieczanie cyfrowego materiały dowodowego jest zazwyczaj pierwszym krokiem technicznym w dochodzeniach DFIR, dlatego powinieneś bardzo uważnie zapoznać się z narzędziami i procedurami pozyskiwania dowodów, które omówimy w tym rozdziale. Po ukończeniu tego rozdziału będziesz wiedział, jak przeprowadzać formalne pozyskiwanie dowodów do analizy śledczej, która zostanie omówiona w kolejnych rozdziałach.

W tym rozdziale omówimy następujące zagadnienia:

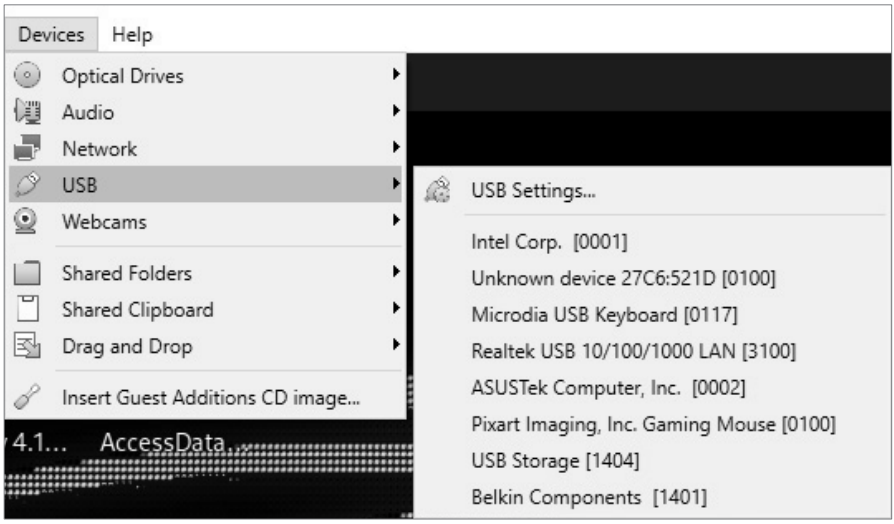
- Zastosowanie polecenia `fdisk` do rozpoznawania partycji.
- Zapewnianie integralności cyfrowego materiału dowodowego przy użyciu kryptograficznych algorytmów generowania funkcji skrótu.
- Tworzenie obrazów binarnych dysków przy użyciu programu DC3DD.
- Tworzenie obrazów binarnych dysków przy użyciu programu DD.
- Tworzenie obrazów binarnych dysków przy użyciu programu Guymager.
- Tworzenie obrazów binarnych dysków i zawartości pamięci przy użyciu programu FTK Imager uruchamianego za pośrednictwem pakietu Wine.

- Tworzenie obrazów binarnych zawartości pamięci RAM i plików stronicowania przy użyciu programu Belkasoft RAM Capturer uruchamianego za pośrednictwem pakietu Wine.

Zastosowanie polecenia fdisk do rozpoznawania partycji

Dla każdego, kto używa systemu Kali Linux jako samodzielnego systemu operacyjnego, proces montowania dysku wymiennego jest prosty. Aby to zrobić, wystarczy podłączyć dysk wymienny do komputera, a następnie uruchomić polecenie `fdisk`. Jeżeli jednak używasz maszyny wirtualnej z systemem Kali Linux, musisz najpierw upewnić się, że wymienny nośnik pamięci został poprawnie rozpoznany przez menedżera VirtualBox. Aby to zrobić, powinieneś wykonać polecenia opisane poniżej:

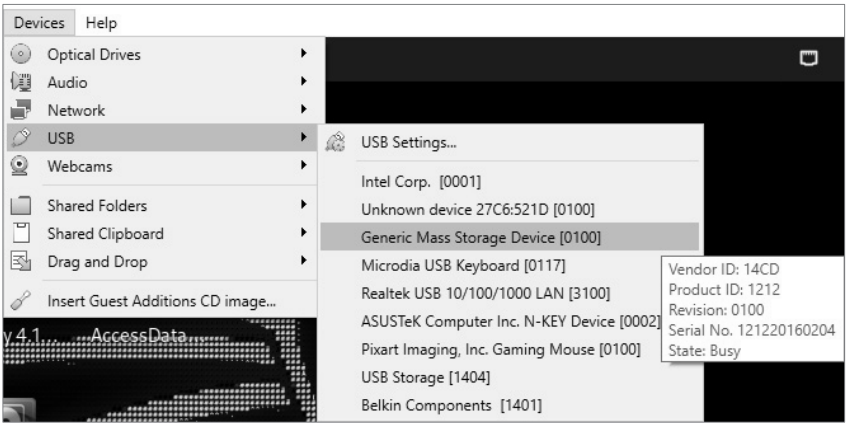
1. W menu okna maszyny wirtualnej VirtualBox z systemem Kali Linux wybierz polecenie *Devices* (urządzenia), a następnie kliknij opcję *USB* (zobacz rysunek 8.1), co spowoduje wyświetlenie listy wszystkich wykrytych urządzeń USB. W celach porównawczych (na później) możesz zrobić zrzut ekranu lub zdjęcie tej listy.



Rysunek 8.1. Menu urządzeń menedżera maszyn wirtualnych VirtualBox

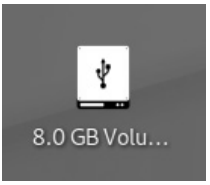
2. Jak łatwo zauważyć, w naszym przykładzie wykrytych zostało osiem urządzeń. Teraz podłącz nośnik pamięci (w naszym przypadku będzie to karta pamięci microSD o pojemności 2 GB) i ponownie wybierz z menu

polecenie *Devices/USB* (urządzenia/USB), aby zobaczyć, czy nowe urządzenie zostało rozpoznane i pojawiło się na liście. Na rysunku 8.2 możesz zauważyć, że na liście USB jest nowe urządzenie, o nazwie *Generic Mass Storage Device [0100]*. Kliknij nazwę tego urządzenia, aby zamontować je w maszynie wirtualnej z systemem Kali Linux.



Rysunek 8.2. Menu urządzeń USB menedżera maszyn wirtualnych VirtualBox

Jeżeli urządzenie zostanie rozpoznane przez VirtualBox i poprawnie zamontowane w maszynie wirtualnej, na pulpicie użytkownika systemu Kali Linux powinna się pojawić ikona tego urządzenia. Na rysunku 8.3 możesz zobaczyć ikonę zamontowanej karty microSD 8 GB, która jest teraz dostępna do użytku.



Rysunek 8.3. Ikona zamontowanego nośnika pamięci widoczna na pulpicie systemu Kali Linux

3. Po zamontowaniu naszego dysku możesz teraz użyć polecenia `fdisk`, aby wyświetlić szczegóły partycji dysku.

Skoro wiesz już, jak zamontować dysk wymienny w systemie Kali Linux, możemy przejść do kolejnego podrozdziału, w którym dowiesz się, jak za pomocą polecenia `fdisk` zidentyfikować wybrany nośnik i jego partycje.

Identyfikacja urządzenia za pomocą polecenia fdisk

Na potrzeby tego przykładu do mojego komputera działającego pod kontrolą systemu Kali Linux podłączyłem przy użyciu zewnętrznego czytnika kart USB 3.0 kartę Sony Pro Duo o pojemności 8 GB. W tym ćwiczeniu możesz użyć dowolnego innego nośnika pamięci masowej, ponieważ cały proces jest dokładnie taki sam, niezależnie od typu używanego urządzenia. Zanim rozpoczniesz tworzenie obrazu binarnego jakiegokolwiek nośnika danych, powinieneś najpierw uruchomić polecenie `sudo fdisk -l`, aby wyświetlić listę wszystkich podłączonych urządzeń pamięci masowej, która pozwoli Ci jednoznacznie zidentyfikować wybrane urządzenie. Jest to konieczne, ponieważ zazwyczaj zamiast nazw urządzeń pamięci masowej będziemy używać ich identyfikatorów.

Aby to zrobić, otwórz nowe okno terminala, wpisz polecenie pokazane poniżej i naciśnij klawisz *Enter*:

```
sudo fdisk -l
```

Na rysunku 8.4 wewnętrzny dysk komputera jest wymieniony jako urządzenie `sda`, a podłączona karta Sony Pro Duo jest wymieniona jako urządzenie `sdb`.

```
┌──(cfsi㉿Research)-[~]
└─$ sudo fdisk -l
[sudo] password for cfsi:
Disk /dev/sda: 372.61 GiB, 400088457216 bytes, 781422768 sectors
Disk model: ST3400832NS
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0×ab60b093

Device     Boot     Start       End   Sectors   Size Id Type
/dev/sda1  *         2048 779421695 779419648 371.7G 83 Linux
/dev/sda2       779423742 781422591   1998850   976M  5 Extended
/dev/sda5       779423744 781422591   1998848   976M 82 Linux swap / Solaris


Disk /dev/sdb: 7.45 GiB, 8002732032 bytes, 15630336 sectors
Disk model: Multi-Card
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0×0fe98fd2

Device     Boot Start      End  Sectors  Size Id Type
/dev/sdb1  *     4476 15618427 15613952  7.4G  c W95 FAT32 (LBA)

┌──(cfsi㉿Research)-[~]
└─$
```

Rysunek 8.4. Przykładowe wyniki działania polecenia fdisk -l

Jak widać na rysunku 8.4, szczegółowe informacje o mojej karcie Sony Pro Duo są następujące:

- **Identyfikator dysku**: `sdb`.
- **Pojemność karty**: 7,4 GB.
- **Rozmiar sektora**: 512 bajtów.
- **System plików**: FAT32.

Jak widać na poprzednim rysunku, system Kali Linux rozpoznał dwa urządzenia:

- `sda` — to główny dysk twardy mojego komputera, podzielony na trzy partycje.
- `sdb` — nośnik pamięci masowej (czyli nasza karta), którego obraz binarny będziemy tworzyć.

Użytkownicy systemu Windows z pewnością zauważą, że rozpoznawanie dysków i partycji oraz konwencje nazewnictwa w systemie Kali Linux (a w zasadzie również we wszystkich innych dystrybucjach systemu Linux) różnią się od tych stosowanych w systemie Windows.

Typowe urządzenia w systemie Linux są adresowane lub rozpoznawane jako `/dev/sda`, `/dev/sdb` itd., podczas gdy dyski w systemie Windows są zwykle rozpoznawane jako `Disk 0`, `Disk 1` itd.

- `/dev` — to początek nazwy ścieżki dla wszystkich urządzeń i dysków w systemie Linux, które mogą być odczytywane lub zapisywane.
- `/sda` — określa urządzenia z interfejsami SCSI (ang. *Small Computer Systems Interface*), SATA i USB.

Pierwsze znaki, `sd`, oznaczają sterownik SCSI, a po nich następuje litera (na przykład `a`, `b` itd.) reprezentująca kolejny numer dysku, np.:

- `sda` — pierwszy podłączony dysk (inaczej dysk `0`).
- `sdb` — drugi podłączony dysk lub nośnik pamięci masowej.

W systemie Windows wyróżniamy partycje podstawowe, logiczne i rozszerzone, ale w systemie Linux partycje dysku są identyfikowane jako numery następujące po literze dysku:

- `sda1` — partycja `1` na pierwszym dysku (`sda`).
- `sda2` — partycja `2` na pierwszym dysku.
- `sdb1` — partycja `1` na drugim dysku (`sdb`).
- `sdb2` — partycja `2` na drugim dysku.

Więcej szczegółowych informacji na temat konwencji nazewnictwa urządzeń w systemie Linux można znaleźć na stronie *https://www.dell.com/support/kbdoc/pl-pl/000132092/ubuntu-linux-postanowienia-dotyczące-urządzeń-urządzenia-dysku-twardego-i#Linux_device_naming_convention*.

Wiesz już, jak zidentyfikować dyski i partycje w systemie plików Linux. W kolejnym podrozdziale dowiesz się, jak przy użyciu funkcji skrótu kryptograficznego zapewnić integralność cyfrowego materiału dowodowego.

Zastosowanie silnych algorytmów funkcji skrótu do zapewnienia integralności dowodów cyfrowych

Aby upewnić się, że cyfrowy materiał dowodowy nie został w żaden sposób zmodyfikowany, przed i po utworzeniu binarnego obrazu dowodowego nośnika pamięci powinieneś obliczyć dla niego wartość skrótu przy użyciu odpowiednio silnego algorytmu kryptograficznego. Algorytmy obliczające wartości kryptograficznych funkcji skrótu (hasze) zwykle generują wyniki w postaci ciągu znaków szesnastkowych (*a – f* i *0 – 9*) o różnej długości (w zależności od rodzaju użytego algorytmu).

Obecnie najczęściej wykorzystywane są następujące algorytmy kryptograficzne:

- MD5 (ang. *Message Digest 5*).
- SHA-1 (ang. *Secure Hash Algorithm version 1*).
- SHA-256, czyli algorytm z grupy SHA-2, generujący wynik o długości 256 bitów.

Uwaga

Więcej szczegółowych informacji na temat kryptograficznych funkcji skrótów można znaleźć na stronie *https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm*.

W systemie Kali Linux do obliczania wartości kryptograficznych funkcji skrótu możemy użyć poleceń `md5sum`, `sha1sum` lub `sha256sum`. Parametrem wywołania tych poleceń powinna być ścieżka urządzenia, czyli nośnika pamięci, którego skrót chcesz obliczyć. Na przykład, aby utworzyć skrót SHA-256 wybranego dysku, powinieneś użyć polecenia pokazanego poniżej, gdzie `sdx` reprezentuje identyfikator dysku:

```
sha256sum /dev/sdx
```

Choć przed chwilą wspomniałem o poleceniu `md5sum`, zalecałbym jednak użycie silniejszego algorytmu, takiego jak SHA-1 lub SHA-256, ponieważ MD5 jest znacznie starszy i teoretycznie może być podatny na kolizje:

- MD5 — rozmiar skrótu: 128 bitów.
- SHA-1 — rozmiar skrótu: 160 bitów.
- SHA-256 — rozmiar skrótu: 256 bitów
- SHA-3 — rozmiar skrótu: 256 bitów (ale sam algorytm jest szybszy niż SHA-2).

Aby obliczyć wartość skrótu MD5 dla mojej karty Pro Duo (`sdb`), użyłem następującego polecenia:

```
sudo md5sum /dev/sdb
```

Aby obliczyć wartość skrótu SHA-1 dla mojej karty Pro Duo (`sdb`), użyłem następującego polecenia:

```
sudo sha1sum /dev/sdb
```

Aby obliczyć wartość skrótu SHA-256 dla mojej karty Pro Duo (`sdb`), użyłem następującego polecenia:

```
sudo sha256sum /dev/sdb
```

Na rysunku 8.5 pokazano przykładowe wyniki działania wszystkich trzech poleceń. Zwróć uwagę, że skrót SHA-256 jest najdłuższy.

Rysunek 8.5. Przykładowe wyniki działania trzech różnych poleceń obliczających wartości skrótów

Ważna uwaga

Podczas tworzenia obrazu binarnego dysku lub innego nośnika pamięci wartość skrótu kryptograficznego oryginalnego pliku musi zawsze odpowiadać wartości skrótu utworzonego obrazu binarnego, co zapewnia integralność oryginalnego nośnika i jego kopii bitowej (obrazu binarnego).

Teraz już wiesz, jak zidentyfikować poszczególne dyski i który dysk ma być obrazowany (`sdb`), możemy więc rozpocząć tworzenie obrazu binarnego za pomocą programu DC3DD. W naszym przykładzie do zilustrowania sposobu działania programu DC3DD użyłem starszego typu karty pamięci Pro Duo o pojemności 8GB, ale możesz użyć dowolnego dysku lub innego nośnika pamięci masowej. Pamiętaj, aby przed rozpoczęciem użyć polecenia `fdisk -l`, żeby zidentyfikować dyski i partycje.

Tworzenie obrazów binarnych nośników pamięci za pomocą programu DC3DD

Pierwszym narzędziem, którego użyjemy do tworzenia obrazu binarnego, jest DC3DD. Co ciekawe, program ten został opracowany przez centrum ds. cyberprzestępczości amerykańskiego Departamentu Obrony (ang. *Department of Defense Cyber Crime Center*). DC3DD to nieco bardziej rozbudowana wersja bardzo popularnego, linuksowego narzędzia DD (ang. *Data Dump*), powszechnie używanego do tworzenia kopii bitowych zawartości dysków i innych nośników danych.

Program DD posiada między innymi następujące możliwości:

- Tworzenie kopii bitowych i klonowanie dysków i innych nośników danych.
- Kopiowanie partycji dysków.
- Kopiowanie folderów i plików.
- Sprawdzanie dysku twardego pod kątem błędów.
- Bezpieczne usuwanie (nadpisywanie) wszystkich danych na dyskach twardych i innych nośnikach danych.

DC3DD jest aktualizowany przy każdej aktualizacji bazowego programu DD. DC3DD oferuje praktycznie wszystkie funkcje bazowego programu DD oraz posiada kilka dodatkowych, bardzo użytecznych możliwości:

- Haszowanie danych „w locie” przy użyciu różnych algorytmów kryptograficznych, takich jak MD5, SHA-1, SHA-256 i SHA-512.
- Mechanizm monitorowania postępu procesu tworzenia obrazu binarnego.
- Zapisywanie dziennika błędów do pliku.
- Dzielenie plików wyjściowych.
- Weryfikacja utworzonych plików.
- Wymazywanie plików wyjściowych (przy użyciu zadanego wzorca).

Pakiet DC3DD nie jest domyślnie dostępny w systemie Kali Linux, zatem musisz go samodzielnie zainstalować ręcznie. Aby to zrobić, najpierw zaktualizujemy naszą wersję Kali Linux za pomocą polecenia `apt-get update`, tak jak pokazano na rysunku 8.6.

```
┌──(cfsi㉿Research)-[~]
└─$ sudo apt-get update
Get:1 http://kali.download/kali kali-rolling InRelease [30.6 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [18.7 MB]
Get:3 https://dl.google.com/linux/chrome/deb stable InRelease [1,811 B]
Get:4 https://dl.google.com/linux/chrome/deb stable/main amd64 Packages [1,095 B]
25% [2 Packages 7,005 kB/18.7 MB 37%]                          187 kB/s 5min 3s
```

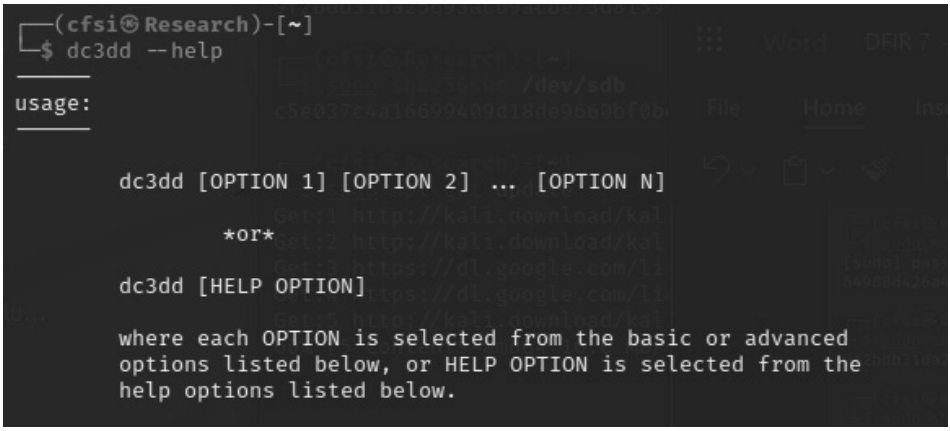
Rysunek 8.6. Aktualizowanie systemu Kali Linux

Po zakończeniu aktualizacji systemu Kali Linux możesz ręcznie zainstalować pakiet DC3DD, wykonując polecenie `sudo apt-get install dc3dd`, tak jak pokazano na rysunku 8.7.

```
┌──(cfsi㉿Research)-[~]
└─$ sudo apt-get install dc3dd
[sudo] password for cfsi:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  dc3dd
0 upgraded, 1 newly installed, 0 to remove and 749 not upgraded.
Need to get 121 kB of archives.
After this operation, 501 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 dc3dd amd64 7.2.646-5
+b1 [121 kB]
Fetched 121 kB in 1s (151 kB/s)
Selecting previously unselected package dc3dd.
(Reading database ... 312296 files and directories currently installed.)
Preparing to unpack .../dc3dd_7.2.646-5+b1_amd64.deb ...
Unpacking dc3dd (7.2.646-5+b1) ...
Setting up dc3dd (7.2.646-5+b1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for kali-menu (2022.3.1) ...
```

Rysunek 8.7. Instalowanie pakietu dc3dd

Program DC3DD jest narzędziem konsolowym (czyli uruchamianym i działającym z poziomu wiersza poleceń konsoli). Aby go uruchomić, powinieneś otworzyć nowe okno terminala i wykonać polecenie `dc3dd`. Na początek zalecam jednak wykonanie polecenia `dc3dd --help`, które wyświetli na ekranie listę dostępnych opcji tego programu, tak jak pokazano na rysunku 8.8.



Rysunek 8.8. Opcje pomocy programu dc3dd

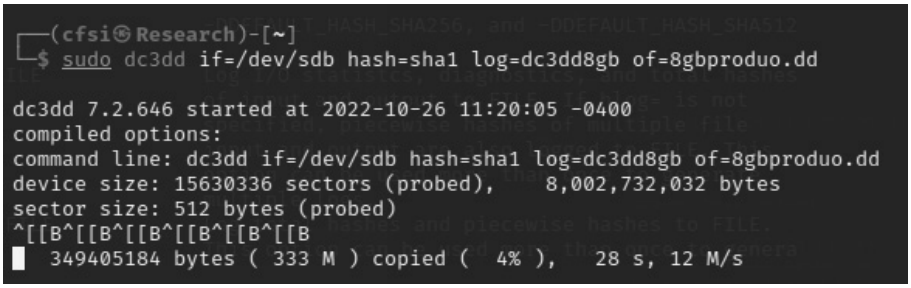
Jak pokazano na rysunku 8.8, typowe wywołanie programu DC3DD wygląda następująco:

dc3dd *[opcja 1] [opcja 2] … [opcja n]*

Aby utworzyć obraz binarny mojej karty pamięci o pojemności 8 GB, użyłem następującego polecenia:

```
sudo dc3dd if=/dev/sdb hash=sha1 log=dc3dd8gb of=8gbproduo.dd
```

Wyniki działania tego polecenia zostały pokazane na rysunku 8.9.



Rysunek 8.9. Tworzenie obrazu binarnego karty pamięci za pomocą programu dc3dd

Poniżej zamieszczam krótki opis poszczególnych argumentów wywołania polecenia dc3dd, pokazanego na rysunku 8.9:

- `if` (ang. *input file*) — określa nazwę *pliku wejściowego*, czyli inaczej mówiąc, wskazuje nośnik, którego obraz binarny będziemy tworzyć.
- `hash` — wskazuje algorytm kryptograficzny, którego będziemy używać do weryfikacji integralności utworzonego obrazu. Jak widać, w tym przykładzie użyłem nieco starszego algorytmu MD5.
- `log` — określa nazwę pliku dziennika, w którym zapisywane będą informacje o nośniku wejściowym i przebieg procesu tworzenia obrazu binarnego, w tym wszystkie błędy (o ile się takie pojawią).
- `of` (ang. *output file*) — określa nazwę pliku obrazu binarnego tworzonego przez program DC3DD. Choć w tym przykładzie plik obrazu wyjściowego będzie tworzony w formacie *.dd*, program DC3DD obsługuje również inne formaty binarne, w tym *.img*, którego użyjemy w kolejnym przykładzie.

Wykrytą pojemność źródłowego nośnika pamięci (podawaną w liczbie sektorów oraz w bajtach) powinieneś zanotować, a następnie porównać z wynikami wyjściowymi. Po zakończeniu procesu tworzenia obrazu binarnego wyświetlane są parametry wejściowe i wyjściowe.

Na rysunku 8.10 pokazano raport wyświetlany po zakończeniu procesu tworzenia obrazu binarnego, na którym możesz zobaczyć informacje o statusie, ilości skopiowanych danych, czasie, który upłynął (w sekundach) oraz prędkości procesu tworzenia obrazu (w Mbps).

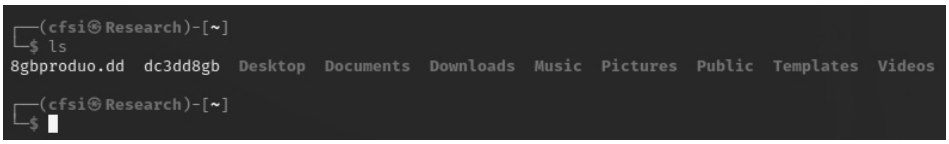
```
┌──(cfsi㉿Research)-[~]
└─$ sudo dc3dd if=/dev/sdb hash=sha1 log=dc3dd8gb of=8gbproduo.dd

dc3dd 7.2.646 started at 2022-10-26 11:20:05 -0400
compiled options:
command line: dc3dd if=/dev/sdb hash=sha1 log=dc3dd8gb of=8gbproduo.dd
device size: 15630336 sectors (probed),    8,002,732,032 bytes
sector size: 512 bytes (probed)
^[[B^[[B^[[B^[[B^[[B^[[B
  8002732032 bytes ( 7.5 G ) copied ( 100% ),  647 s, 12 M/s

input results for device `/dev/sdb':
   15630336 sectors in
   0 bad sectors replaced by zeros
   9f2bdb31da25693acb9acbe73d815996cd7e293b (sha1)

output results for file `8gbproduo.dd':
   15630336 sectors out

dc3dd completed at 2022-10-26 11:30:52 -0400
```

Rysunek 8.10. Przykładowe wyniki działania polecenia dc3dd

Im większy rozmiar dysku lub innego nośnika pamięci, którego obraz binarny tworzymy, tym więcej czasu zabierze taki proces. Ale nie ma tego złego, co by na dobre nie wyszło — w międzyczasie możesz zaparzyć sobie filiżankę aromatycznej kawy albo rzucić okiem na inne wspaniałe książki wydawnictwa Helion, które znajdziesz pod adresem *https://helion.pl/*.

Analizując wyniki działania pokazane na rysunku 8.10, możesz się przekonać, że zobrazowana została ta sama liczba sektorów (15630336) i żadne uszkodzone sektory nie zostały zastąpione zerami. Widać również, że dla obrazu utworzony został skrót SHA1, co zapewnia, że utworzona została dokładna kopia nośnika źródłowego.

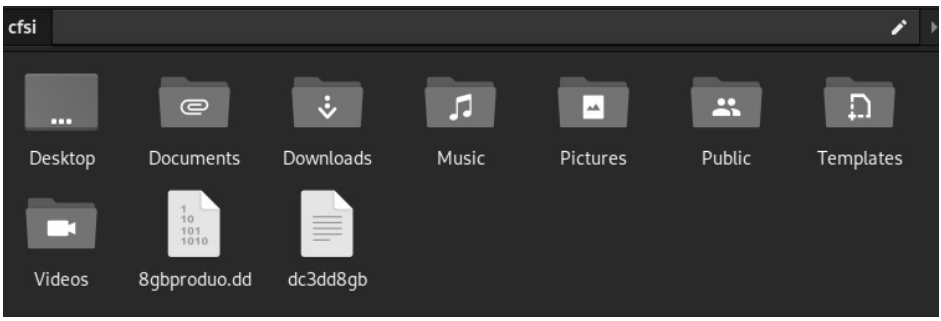
Aby wyświetlić zawartość katalogu, w którym zapisany został utworzony wyjściowy obraz binarny, możesz użyć polecenia `ls`. Jak widać na rysunku 8.11, w moim przykładowym katalogu zostały utworzone dwa pliki: plik obrazu *8gbproduo.dd* i plik dziennika *dc3dd8gb*:



Rysunek 8.11. Lista plików w katalogu wyjściowym, wyświetlona przy użyciu polecenia ls

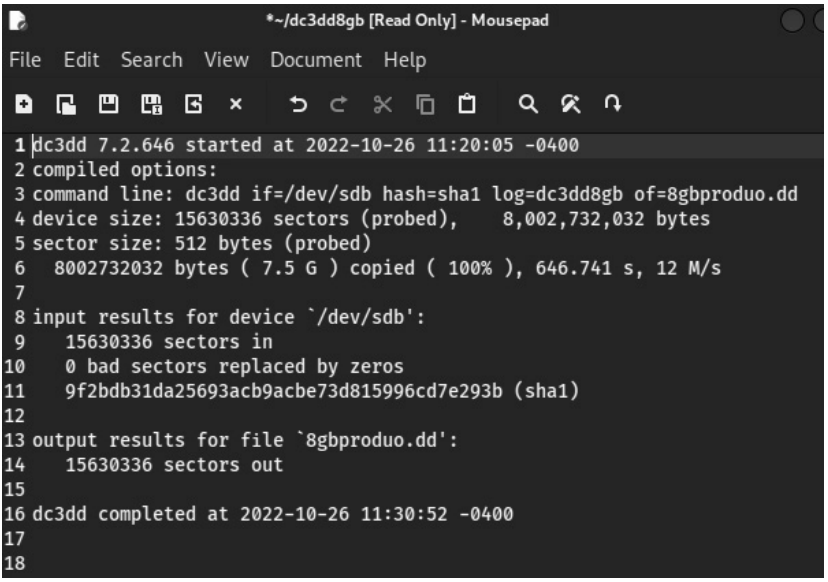
Aby uzyskać dostęp do utworzonego obrazu binarnego i pliku dziennika, powinieneś przejść do katalogu wyjściowego (w naszym przykładzie */home*). Aby to zrobić, kliknij ikonę folderu znajdującą się w lewym górnym rogu pulpitu, a następnie wybierz opcję *Open Folder* (otwórz folder).

W moim folderze domowym pierwszy plik, *8gbproduo.dd*, to plik obrazu binarnego utworzony przez program DC3DD (przypomnij sobie parametr `of=8gbproduo.dd`). Drugi plik, *dc3dd8gb*, to plik dziennika utworzony przy użyciu parametru `log=dc3dd8gb` (zobacz rysunek 8.12).



Rysunek 8.12. Plik obrazu i plik dziennika utworzone w moim folderze domowym

Pamiętaj, aby zachować plik dziennika, który zawiera zapis procesu tworzenia obrazu i jego podsumowanie, tak jak pokazano na rysunku 8.13.



Rysunek 8.13. Przykładowa zawartość pliku dziennika

W rozdziale 12., „Pakiet Autopsy Forensic Browser", i rozdziale 13., „Przeprowadzanie dochodzeń cyfrowych przy użyciu pakietu Autopsy 4", przeanalizujemy pozyskane obrazy binarne za pomocą pakietu Autopsy; warto jednak pamiętać, że w razie potrzeby możesz skopiować lub sklonować obrazy binarne bezpośrednio na inny nośnik.

Aby to zilustrować, spróbujemy sklonować pozyskany wcześniej obraz binarny (*8gbproduo.dd*) na nowy dysk, oznaczony jako `sdc`. Polecenie, za pomocą którego możemy wykonać takie zadanie, byłoby następujące:

```
dc3dd if=8gbproduo.dd of=/dev/sdc log=drivecopy.log
```

Jeżeli chcesz skopiować obraz binarny bezpośrednio na nowy dysk, powinieneś się upewnić, że rozmiar dysku docelowego jest równy lub większy niż rozmiar pliku obrazu.

Weryfikacja wartości skrótu kryptograficznego obrazów binarnych

Aby zweryfikować wartość skrótu kryptograficznego dysku `sdb`, możesz użyć następującego polecenia:

```
sudo sha1sum /dev/sdb
```

Przykładowy wynika działania takiego polecenia został pokazany na rysunku 8.14.

```
┌──(cfsi㉿Research)-[~]
└─$ sudo sha1sum /dev/sdb
[sudo] password for cfsi:
3b36efe65704c140b48df6dea3811c73b6091c0d  /dev/sdb
```

Rysunek 8.14. Przykładowy wynik działania polecenia sha1sum

Alternatywnie możesz również użyć następującego polecenia:

```
cat 8gbproduo.dd | sha1sum
```

Przykładowy wynik działania takiego polecenia został pokazany na rysunku 8.15.

```
┌──(cfsi㉿Research)-[~]
└─$ cat 8gbproduo.dd | sha1sum
9f2bdb31da25693acb9acbe73d815996cd7e293b  -
```

Rysunek 8.15. Przykładowy wynik działania polecenia cat sha1sum

Wymazywanie dysku za pomocą programu DC3DD

Widziałeś już próbkę możliwości programu DC3DD jako znakomitego narzędzia do tworzenia obrazów binarnych, ale chciałbym również pójść o krok dalej i przedstawić Ci jego możliwości jako narzędzia do wymazywania danych.

Program DC3DD może bezpiecznie wymazywać dane i kasować dyski poprzez nadpisywanie danych na trzy sposoby:

- Nadpisywanie danych i wypełnianie dysków zerami. Aby to zrobić, powinieneś wykonać następujące polecenie:

  ```
  dc3dd wipe=/dev/sdb
  ```

  Na rysunku 8.16 pokazano przykładowe wyniki działania tego polecenia.

```
┌──(cfsi㉿Research)-[~]
└─$ sudo dc3dd wipe=/dev/sdb
[sudo] password for cfsi:

dc3dd 7.2.646 started at 2022-10-27 10:09:33 -0400
compiled options:
command line: dc3dd wipe=/dev/sdb
device size: 15630336 sectors (probed),    8,002,732,032 bytes
sector size: 512 bytes (probed)
 4541087744 bytes ( 4.2 G ) copied ( 57% ),  122 s, 35 M/s
```

Rysunek 8.16. Przykładowe wyniki działania polecenia dc3dd wipe

- Nadpisywanie danych i wypełnianie dysków wzorcem szesnastkowym przy użyciu opcji `pat`. Aby to zrobić, powinieneś wykonać następujące polecenie:

  `dc3dd wipe=/dev/sdb pat=10101010`

  Na rysunku 8.17 pokazano przykładowe wyniki działania tego polecenia.

```
┌──(cfsi㉿Research)-[~]
└─$ sudo dc3dd wipe=/dev/sdb pat=10101010

dc3dd 7.2.646 started at 2022-10-26 12:33:29 -0400
compiled options:
command line: dc3dd wipe=/dev/sdb pat=10101010
device size: 15630336 sectors (probed),    8,002,732,032 bytes
sector size: 512 bytes (probed)
  8002732032 bytes ( 7.5 G ) copied ( 100% ),  715 s, 11 M/s

input results for pattern `10101010':
   15630336 sectors in

output results for device `/dev/sdb':
   15630336 sectors out

dc3dd completed at 2022-10-26 12:45:24 -0400
```

Rysunek 8.17. Przykładowe wyniki działania polecenia dc3dd z szesnastkowym wzorcem nadpisywania

- Nadpisywanie danych i wypełnianie dysków wzorcem tekstowym za pomocą opcji `tpat`. Aby to zrobić, powinieneś wykonać następujące polecenie:

  `dc3dd wipe=/dev/sdb tpat=CFSI`

  Na rysunku 8.18 pokazano przykładowe wyniki działania tego polecenia.

```
┌──(cfsi㉿Research)-[~]
└─$ sudo dc3dd wipe=/dev/sdb tpat=CFSI
[sudo] password for cfsi:

dc3dd 7.2.646 started at 2022-10-26 12:56:38 -0400
compiled options:
command line: dc3dd wipe=/dev/sdb tpat=CFSI
device size: 15630336 sectors (probed),    8,002,732,032 bytes
sector size: 512 bytes (probed)
  8002732032 bytes ( 7.5 G ) copied ( 100% ),  714 s, 11 M/s

input results for pattern `CFSI':
   15630336 sectors in

output results for device `/dev/sdb':
   15630336 sectors out

dc3dd completed at 2022-10-26 13:08:32 -0400
```

Rysunek 8.18. Przykładowe wyniki działania polecenia dc3dd z tekstowym wzorcem nadpisywania

Wiesz już, jak używać polecenia `dc3dd` i jak wykorzystywać je do bezpiecznego usuwania danych z nośników. W kolejnym podrozdziale przyjrzyjmy się podobnemu programowi, o nazwie DD, który również może być wykorzystywany do tworzenia binarnych obrazów dysków oraz czyszczenia zawartości nośników danych.

Tworzenie obrazów binarnych nośników pamięci za pomocą programu DD

Zanim zaczniemy korzystać z programu DD, chciałbym ponownie zwrócić uwagę na jedną z funkcji programu DD, jaką jest możliwość bezpiecznego czyszczenia danych, partycji i dysków — ze względu na te możliwości program DD jest nieco z pewną emfazą nazywany **destruktorem danych** (ang. *data destroyer*). Kiedy chcesz skorzystać z programów DD i DC3DD, zawsze powinieneś najpierw zidentyfikować odpowiednie urządzenia, partycje, pliki wejściowe i wyjściowe oraz parametry wywołania tych poleceń.

W przykładach zastosowania programu DC3DD omawianych w tym podrozdziale będę używał nieco starszego, ale nadal w pełni funkcjonalnego dysku flash 2 GB.

Zamiast DC3DD możesz również użyć narzędzia DD, ponieważ oba polecenia i sposób ich użycia są bardzo podobne.

Na początek możesz upewnić się, że masz dostęp do polecenia `dd`. Aby to zrobić, po prostu uruchom polecenie `dd –help` (zobacz rysunek 8.19). Jeżeli polecenie `dd` nie jest dostępne, zaktualizuj swój system Kali Linux, uruchamiając polecenie `apt-get update`, a następnie ponownie spróbuj uruchomić polecenie `dd --help`.

Aby utworzyć obraz binarny mojego dysku, użyłem następującego polecenia:

```
dd if=/dev/sdb of=produo8g b.img bs=65536 conv=noerror,sync
```

Na rysunku 8.20 pokazano wyniki działania tego polecenia.

Poniżej znajdziesz krótki opis poszczególnych opcji wywołania tego polecenia:

- `if` — nazwa pliku wejściowego (urządzenie `sdb`).
- `of` — nazwa pliku wyjściowego (nazwa obrazu binarnego, który chcemy utworzyć).

```
root@kali:~# dd --help
Usage: dd [OPERAND]...
  or:  dd OPTION
Copy a file, converting and formatting according to the operands.

  bs=BYTES        read and write up to BYTES bytes at a time (default: 512);
                  overrides ibs and obs
  cbs=BYTES       convert BYTES bytes at a time
  conv=CONVS      convert the file as per the comma separated symbol list
  count=N         copy only N input blocks
  ibs=BYTES       read up to BYTES bytes at a time (default: 512)
  if=FILE         read from FILE instead of stdin
  iflag=FLAGS     read as per the comma separated symbol list
  obs=BYTES       write BYTES bytes at a time (default: 512)
  of=FILE         write to FILE instead of stdout
  oflag=FLAGS     write as per the comma separated symbol list
  seek=N          skip N obs-sized blocks at start of output
  skip=N          skip N ibs-sized blocks at start of input
  status=LEVEL    The LEVEL of information to print to stderr;
                  'none' suppresses everything but error messages,
                  'noxfer' suppresses the final transfer statistics,
                  'progress' shows periodic transfer statistics

N and BYTES may be followed by the following multiplicative suffixes:
c =1, w =2, b =512, kB =1000, K =1024, MB =1000*1000, M =1024*1024, xM =M,
GB =1000*1000*1000, G =1024*1024*1024, and so on for T, P, E, Z, Y.

Each CONV symbol may be:

  ascii     from EBCDIC to ASCII
  ebcdic    from ASCII to EBCDIC
  ibm       from ASCII to alternate EBCDIC
  block     pad newline-terminated records with spaces to cbs-size
  unblock   replace trailing spaces in cbs-size records with newline
  lcase     change upper case to lower case
  ucase     change lower case to upper case
  sparse    try to seek rather than write the output for NUL input blocks
  swab      swap every pair of input bytes
```

Rysunek 8.19. Ekran pomocy polecenia dd

```
┌──(cfsi㉿Research)-[~]
└─$ sudo dd if=/dev/sdb of=ddproduo8gb.img bs=512 conv=noerror,sync
15630336+0 records in
15630336+0 records out
8002732032 bytes (8.0 GB, 7.5 GiB) copied, 104.02 s, 76.9 MB/s

┌──(cfsi㉿Research)-[~]
```

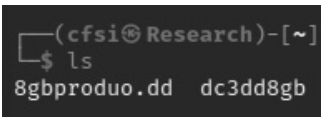
Rysunek 8.20. Tworzenie obrazu dysku przy użyciu polecenia dd

- `bs` — rozmiar bloku (domyślny rozmiar to 512 bajtów).
- `conv=noerror, sync` — opcja `noerror` powoduje, że polecenie `dd` będzie kontynuowało tworzenie obrazu, nawet jeżeli wystąpią jakieś błędy odczytu; jeżeli wystąpią błędy, odpowiednie bloki zostaną wypełnione zerami (opcja `sync`).

W poprzednim poleceniu ustawiłem rozszerzenie pliku wyjściowego na *.img*; w zależności od potrzeb możesz jednak użyć innego formatu, takiego jak *.iso*, podając odpowiednie rozszerzenie nazwy pliku za pomocą opcji `of`.

Listę utworzonych plików możesz przeglądać za pomocą polecenia `ls`. W naszych przykładach utworzyliśmy do tej pory dwa obrazy.

Przykładowe wyniki działania polecenia `ls` zostały pokazane na rysunku 8.21.



Rysunek 8.21. Pliki pozyskiwania dowodów w katalogu domowym

W kolejnym podrozdziale poznasz inne, bardzo popularne narzędzie do tworzenia binarnych obrazów nośników danych, czyli program Guymager, który oferuje bardzo podobną funkcjonalność jak narzędzia omawiane przed chwilą, ale wyposażony jest w graficzny interfejs użytkownika (ang. *Graphical User Interface* — GUI).

Tworzenie obrazów dysków za pomocą programu Guymager

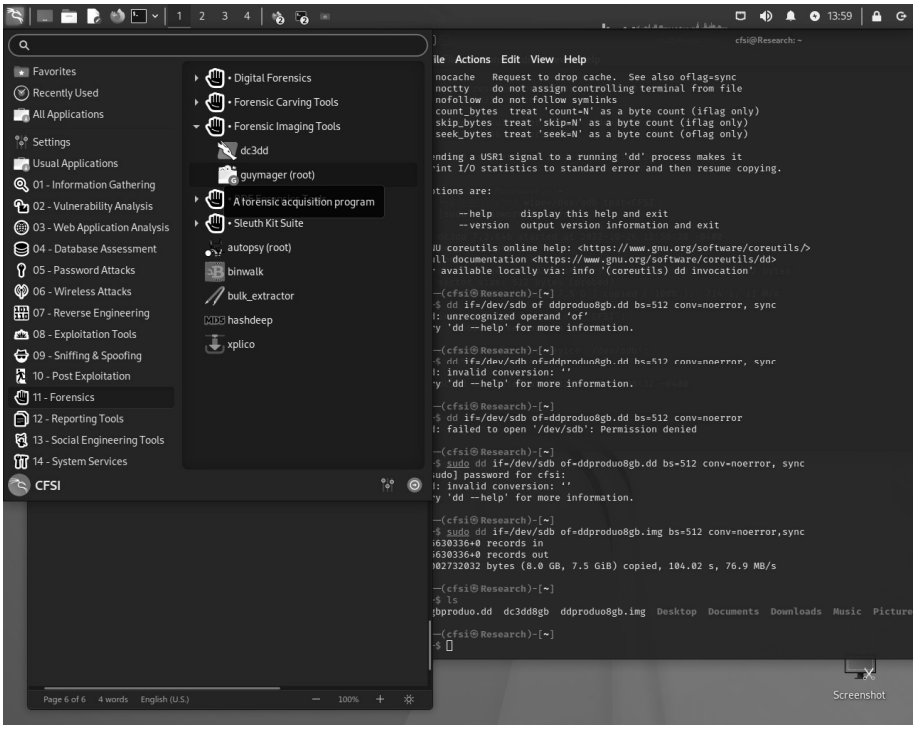
Guymager to kolejne narzędzie do tworzenia binarnych obrazów dysków i innych nośników danych, które może być używane do tworzenia kopii bitowych, a także do klonowania dysków. Opracowany przez Guya Vonckena program Guymager jest całkowicie bezpłatny i udostępniany jako oprogramowanie open source. Program ma wiele funkcji takich samych jak DC3DD i jest dostępny tylko na platformie Linux. Choć niektórzy analitycy preferują narzędzia konsolowe, to jednak program Guymager został wyposażony w wygodny, graficzny interfejs użytkownika i dlatego program ten może być nieco częściej wybierany przez początkujących lub nieco mniej doświadczonych użytkowników.

W tym przykładzie użyję tego samego 2-gigabajtowego dysku flash, którego używałem w poprzednich przykładach DC3DD, dzięki czemu na końcu będziemy mogli porównać otrzymane wyniki. Przypominam, że podczas tworzenia binarnych obrazów dysków i innych nośników danych, które stanowią materiał dowodowy dla dochodzeń cyfrowych, powinieneś zawsze używać urządzeń blokujących zapis, aby uniknąć przypadkowego nadpisywania bądź modyfikacji oryginalnych plików dowodowych.

Podobnie jak to robiliśmy w poprzednich ćwiczeniach z DD i DC3DD, przed rozpoczęciem powinieneś najpierw upewnić się, że znasz nazwy urządzeń podłączonych do Twojego komputera. Możesz to zrobić za pomocą polecenia `fdisk -l` lub `sudo fdisk -l`.

Uruchamianie programu Guymager

Program Guymager możesz uruchomić, korzystając z menu systemu Kali Linux. Aby to zrobić, rozwiń menu *Applications* (aplikacje) znajdujące się w lewej górnej części pulpitu, a następnie wybierz opcję *11 – Forensics/Forensic Imaging Tools* (narzędzia śledcze/narzędzia do tworzenia binarnych obrazów nośników danych), jak to zostało pokazane na rysunku 8.22.

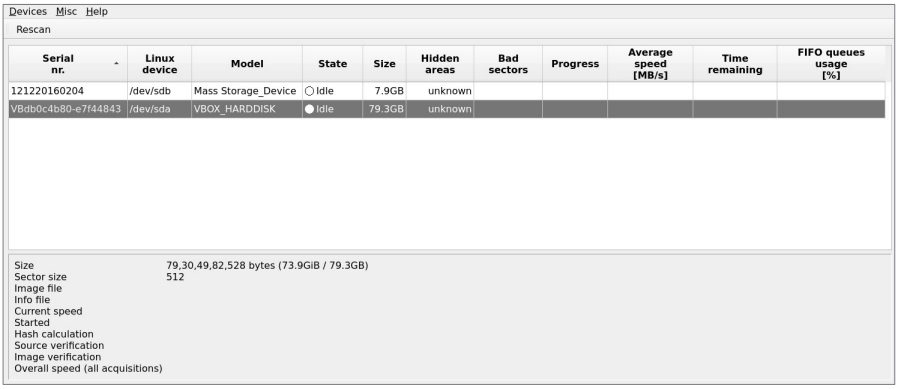


Rysunek 8.22. Menu Forensics w systemie Kali Linux

Po uruchomieniu programu Guymager na ekranie wyświetlona zostanie lista wykrytych dysków podłączonych do Twojego systemu Kali Linux. Jak pokazano na rysunku 8.23, program wyświetla szczegółowe dane o moim dysku flash 2 GB, którego używam w tym przykładzie. Możemy tutaj zobaczyć między innymi takie informacje jak:

- *Linux device* (nazwa urządzenia w systemie Linux) — mój dysk został rozpoznany jako `/dev/sdb`.

- *Model* (model urządzenia) — `USB_Flash_Memory`.
- *State* (stan urządzenia) — obecnie wyświetlany jako `Idle` (bezczynny), ponieważ proces tworzenia obrazu jeszcze się nie rozpoczął.
- *Size* (rozmiar) — `2.0GB`.
- *Serial numer* (numer seryjny) — `001CC0C60D...` (numer seryjny jest unikalny dla każdego dysku).
- *Hidden areas* (ukryte obszary) — `unknown` (nieznane).



Rysunek 8.23. Interfejs użytkownika programu Guymager

Jeżeli dane urządzenie nie zostało wykryte lub chcesz dodać kolejne urządzenia, upewnij się, że takie urządzenie zostało poprawnie podłączone, i naciśnij przycisk *Rescan* (skanuj ponownie) znajdujący się w lewym górnym rogu okna aplikacji, aby rozpocząć proces ponownego wykrywania podłączonych urządzeń.

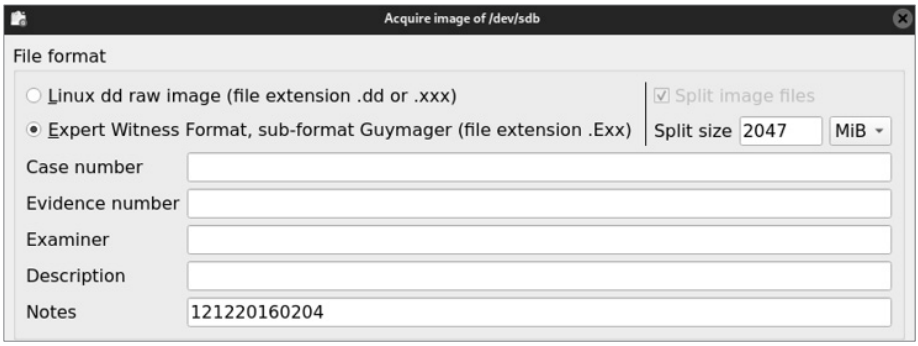
Tworzenie binarnych obrazów nośników danych za pomocą programu Guymager

Aby rozpocząć proces tworzenia binarnego obrazu dysku lub innego nośnika danych, odszukaj żądany dysk na liście wykrytych urządzeń, a następnie kliknij go prawym przyciskiem myszy (w tym przykładzie jest to urządzenie `/dev/sdb`) i z menu podręcznego wybierz polecenie *Acquire image* (pozyskaj obraz). Zwróć uwagę, że opcja *Clone device* (klonuj urządzenie) jest również dostępna (zobacz rysunek 8.24) — możesz jej użyć, jeżeli na przykład chcesz sklonować dysk dowodowy. Pamiętaj, że (jak już wspominałem wcześniej) podczas klonowania pojemność dysku docelowego musi być równa lub większa niż pojemność źródłowego (oryginalnego) dysku dowodowego.

Rysunek 8.24. Opcje tworzenia obrazu i klonowania nośników w programie Guymager

Zanim rozpoczniesz właściwy proces tworzenia obrazu dysku, zostaniesz poproszony o wprowadzenie kilku informacji o sobie i tworzonym obrazie (czyli potencjalnie materiale dowodowym):

- Grupa opcji *File format* (format pliku), zobacz rysunek 8.25:
  - *File extensions* (rozszerzenia plików) — *.dd*, *.xxx* lub *.Exx*.
  - *Split size* (rozmiar fragmentów) — pozwala na zdefiniowanie rozmiaru kolejnych części tworzonego obrazu dysku.
  - *Case management information* (informacje o sprawie) — jeżeli tworzysz obraz dysku lub innego nośnika danych na potrzeby dochodzenia cyfrowego, możesz tutaj wpisać takie informacje jak *Case number* (numer sprawy), *Evidence number* (numer dowodu), *Examiner* (imię i nazwisko analityka), *Description* (opis sprawy) i *Notes* (notatki, informacje dodatkowe).



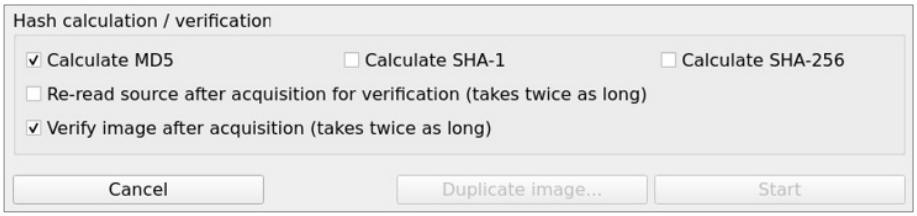
Rysunek 8.25. Opcje formatu tworzonego binarnego obrazu nośnika danych

- Grupa opcji *Destination* (miejsce docelowe), zobacz rysunek 8.26:
  - *Image directory* (katalog obrazu) — nazwa katalogu, w którym zapisany zostanie tworzony obraz i plik dziennika (plik informacyjny).
  - *Image filename* (nazwa pliku obrazu) — nazwa pliku tworzonego obrazu nośnika danych.

Rysunek 8.26. Opcje wyboru miejsca, w którym zostanie zapisany tworzony obraz nośnika danych

Weryfikacja obrazu za pomocą obliczania funkcji skrótu

Program Guymager obsługuje kilka algorytmów funkcji skrótu kryptograficznego, umożliwiając badaczowi wybór spośród takich popularnych algorytmów jak MD5, SHA-1 i SHA-256 (zobacz rysunek 8.27).



Rysunek 8.27. Opcje wyboru algorytmu skrótu kryptograficznego w programie Guymager

Opcja *Re-read source after acquisition for verification* (ponowny odczyt nośnika źródłowego w celu weryfikacji po utworzeniu obrazu) umożliwia weryfikację poprawności odczytu danych z nośnika źródłowego.

Opcja *Verify image after acquisition* (weryfikuj obraz po utworzeniu) weryfikuje poprawność utworzonego obrazu i jego zgodność z oryginalnym nośnikiem danych.

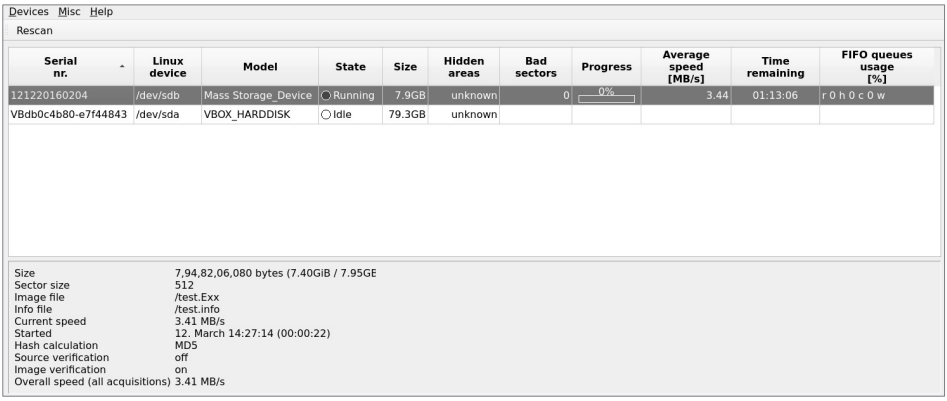
W prawej dolnej części okna pokazanego na rysunku 8.27 znajdują się dwa nieaktywne przyciski. Pierwszy z tych przycisków, *Duplicate image...* (utwórz duplikat obrazu), pozwala na tworzenie duplikatów utworzonego obrazu bez konieczności powtarzania od początku całego procesu wprowadzania danych.

Tworząc nowy obraz nośnika danych, zawsze warto określić katalog, w którym zostanie zapisany plik obrazu. Aby to zrobić, w grupie opcji *Destination* (miejsce docelowe) naciśnij przycisk *Image directory* (katalog obrazu) i wybierz żądaną lokalizację. W naszym przykładzie jako lokalizację dla obrazu i pliku dziennika wybrałem katalog *Desktop*.

Rysunek 8.28 pokazuje dane, których użyłem do utworzenia mojego przykładowego obrazu dysku, po wybraniu katalogu *Desktop* jako katalogu docelowego oraz algorytmów haszujących MD5 i SHA-1.

Rysunek 8.28. Opcje folderu docelowego dla tworzonego obrazu nośnika danych

Po kliknięciu przycisku *Start* (zobacz rysunek 8.29) stan procesu zmienia się z *Idle* (bezczynny) na *Running* (uruchomiony). W polu *Progress* (postęp) wyświetlany jest teraz także pasek postępu.



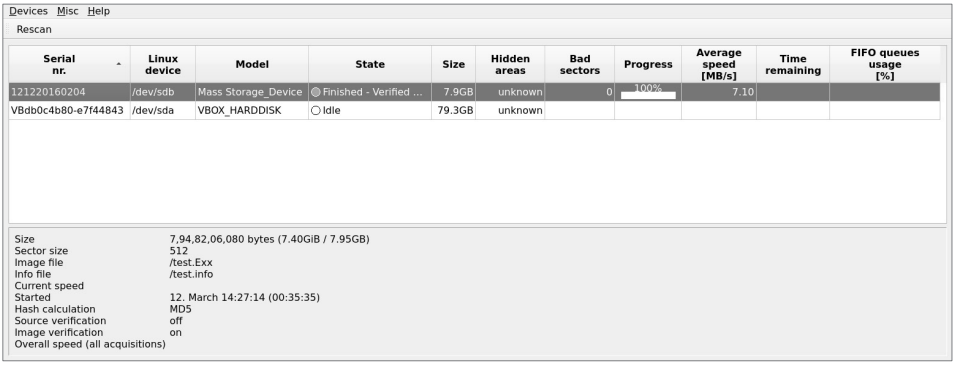
Rysunek 8.29. Postęp procesu tworzenia obrazu binarnego nośnika danych

Jeżeli przyjrzysz się bliżej szczegółom w lewym dolnym rogu ekranu, zobaczysz rozmiar obrazu, ścieżkę docelowej lokalizacji obrazu i pliku dziennika, nazwę i rozszerzenie nazwy obrazu, bieżącą prędkość przetwarzania danych i rodzaj wybranych funkcji skrótu kryptograficznego. Możesz również zauważyć, że weryfikacja obrazu jest włączona (zobacz rysunek 8.30).

Size	7,94,82,06,080 bytes (7.40GiB / 7.95GB)
Sector size	512
Image file	/test.Exx
Info file	/test.info
Current speed	3.49 MB/s
Started	12. March 14:27:14 (00:02:51)
Hash calculation	MD5
Source verification	off
Image verification	on
Overall speed (all acquisitions)	3.49 MB/s

Rysunek 8.30. Szczegóły procesu tworzenia obrazu nośnika danych w programie Guymager

Po zakończeniu procesu tworzenia obrazu kolor przycisku w polu *State* (stan) zmienia się z niebieskiego na zielony, wskazując, że proces został zakończony, oraz wyświetlona zostaje informacja *Finished — Verified & ok* (gotowe — zweryfikowane), o ile włączyłeś odpowiednie opcje weryfikacji w panelu *Hash verification/calculation* (weryfikacja/obliczanie skrótów), a na pasku postępu wyświetlana jest wartość 100% (zobacz rysunek 8.31).



Rysunek 8.31. Program Guymager zakończył proces tworzenia obrazu nośnika danych

Nasz przykładowy plik obrazu oraz plik dziennika znajdują się na pulpicie, ponieważ taką lokalizację wybrałem przed rozpoczęciem tworzenia obrazu. W kolejnym podrozdziale przyjrzymy się plikowi dziennika i sprawdzimy wyniki haszowania obrazu.

Zawartość pliku .info

Dwukrotne kliknięcie pliku dziennika z rozszerzeniem *.info* pozwoli Ci sprawdzić różne informacje dotyczące przebiegu procesu tworzenia obrazu nośnika danych oraz zobaczyć wartości obliczonych funkcji skrótów kryptograficznych.

Plik *.info* utworzony przez program Guymager zawiera znacznie więcej informacji niż plik dziennika wygenerowany przez DC3DD (np. znajdziesz tam również informacje, które wprowadziłeś w polach opisu sprawy).

Przyjrzyjmy się teraz bliżej informacjom o haszowaniu nośnika źródłowego oraz obrazu, które znajdują się w pliku *.info*.

W naszym przykładzie możesz łatwo zauważyć, że skróty MD5 i SHA-1 zostały utworzone i zweryfikowane, jak pokazano na rysunku 8.32.

```
MD5 hash                    : 7d9171d9c5aabf743799ce4a323a9d45
MD5 hash verified source    : --
MD5 hash verified image     : 7d9171d9c5aabf743799ce4a323a9d45
SHA1 hash                   : --
SHA1 hash verified source   : --
SHA1 hash verified image    : --
SHA256 hash                 : --
SHA256 hash verified source: --
SHA256 hash verified image : --
Image verification OK. The image contains exactly the data that was written.
```

Rysunek 8.32. Wyniki haszowania utworzonego obrazu zapisane w pliku dziennika

Na tym zakończę opis procesu tworzenia obrazów binarnych dysków i innych nośników danych za pomocą programu Guymager, który jest znacznie prostszy w użyciu niż programy `dc3dd` i `dd`, działające z poziomu wiersza poleceń.

W następnym podrozdziale poznasz program FTK Imager, czyli kolejne narzędzie do tworzenia obrazów dysków i nośników danych, którego możesz używać w systemie Kali Linux.

Tworzenie obrazów nośników danych i pamięci operacyjnej za pomocą programu FTK Imager uruchamianego za pośrednictwem pakietu Wine

Istnieje wiele narzędzi do tworzenia obrazów dysków, zawartości pamięci operacyjnej i innych nośników danych, z których możesz korzystać na platformie Windows. Utworzone w ten sposób obrazy binarne możesz następnie otworzyć na komputerze lub maszynie wirtualnej działającej pod kontrolą systemu Kali Linux w celu dalszej analizy, używając na przykład pakietu **Volatility 3** do analizy zrzutu pamięci i pakietu

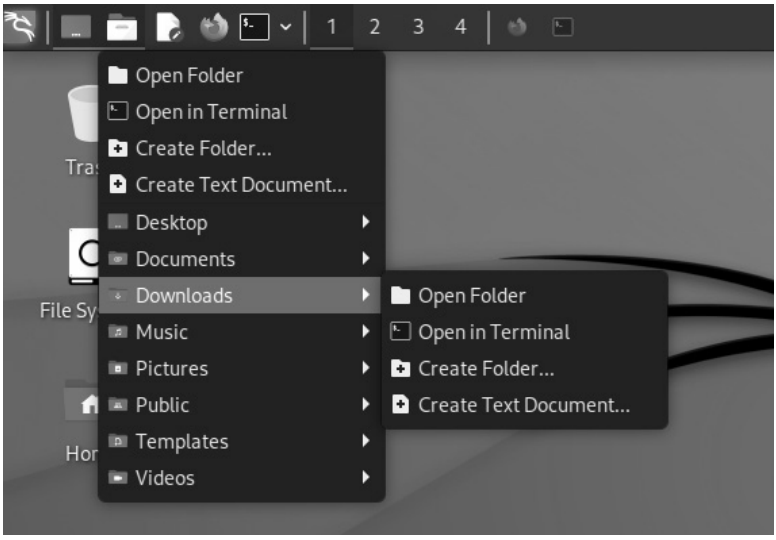
Autopsy do analizy zawartości dysku. Zanim jednak przejdziemy do tych zagadnień, dowiesz się, jak za pośrednictwem pakietu Wine zainstalować w systemie Kali Linux program FTK Imager.

Instalowanie programu FTK Imager

Program **FTK Imager** jest darmowym narzędziem przeznaczonym dla systemu Windows, które umożliwia tworzenie binarnych obrazów zawartości pamięci RAM, pliku stronicowania, dysków i innych nośników danych.

Aby zainstalować program FTK Imager w systemie Kali Linux, powinieneś wykonać polecenia opisane poniżej:

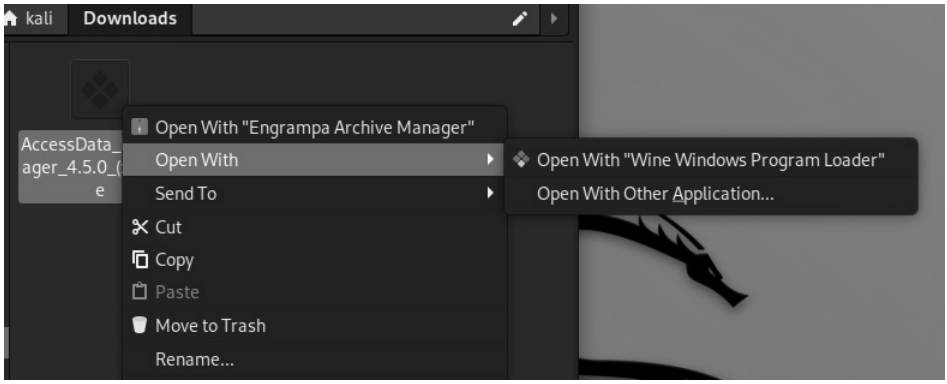
1. Pobierz program FTK Imager ze strony internetowej programu, dostępnej pod adresem *https://www.exterro.com/ftk-imager*. Wypełnij formularz rejestracji i naciśnij przycisk *Submit* (prześlij), a na ekranie pojawi się link umożliwiający pobranie aplikacji.
2. Po zakończeniu pobierania kliknij ikonę folderu *Home* (folder domowy użytkownika), przejdź do katalogu *Downloads* (pobrane), a następnie wybierz opcję *Open Folder* (otwórz folder), jak pokazano na rysunku 8.33.



Rysunek 8.33. Otwieranie folderu Downloads w systemie Kali Linux

3. Teraz kliknij prawym przyciskiem myszy pobrany plik *AccessData_FTK_Imager*, z menu podręcznego wybierz polecenie *Open With* (otwórz za pomocą), a następnie wybierz opcję *Open with "Wine Windows*

Program Loader" (otwórz za pomocą programu „Wine Windows Program Loader"), jak pokazano na rysunku 8.34.



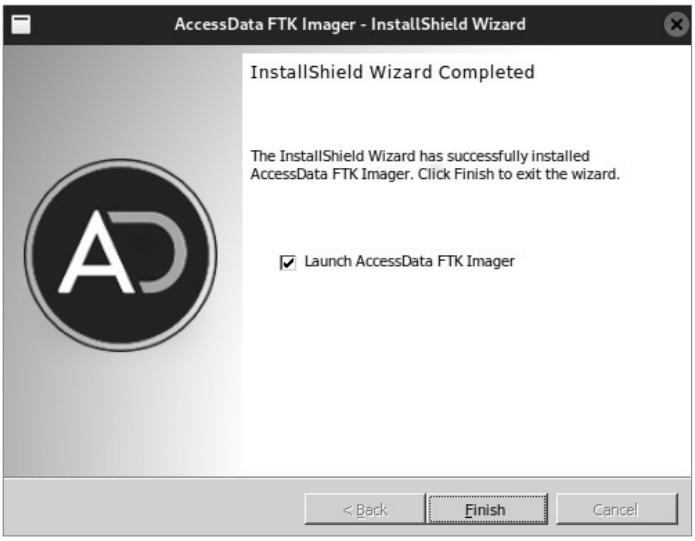
Rysunek 8.34. Uruchamianie programu instalacyjnego pakietu FTK Imager za pośrednictwem Wine

4. Instalator rozpocznie teraz instalację programu FTK Imager w Twoim systemie Kali Linux (zobacz rysunek 8.35). Aby kontynuować, naciśnij przycisk *Next* (dalej).

Rysunek 8.35. Instalator programu FTK Imager

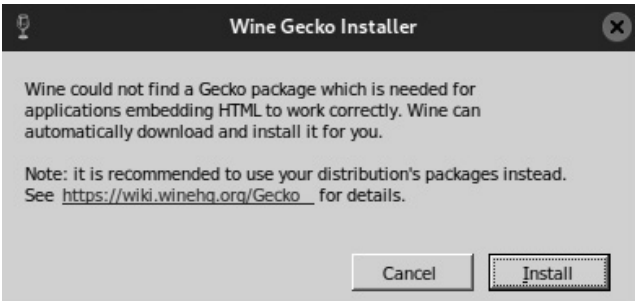
5. Zaakceptuj umowę licencyjną, następnie zaakceptuj domyślny folder docelowy, naciskając przycisk *Next* (dalej), a następnie naciśnij przycisk

Install (instaluj). Po zakończeniu instalacji naciśnij przycisk *Finish* (zakończ), aby uruchomić program FTK Imager, jak pokazano na rysunku 8.36.



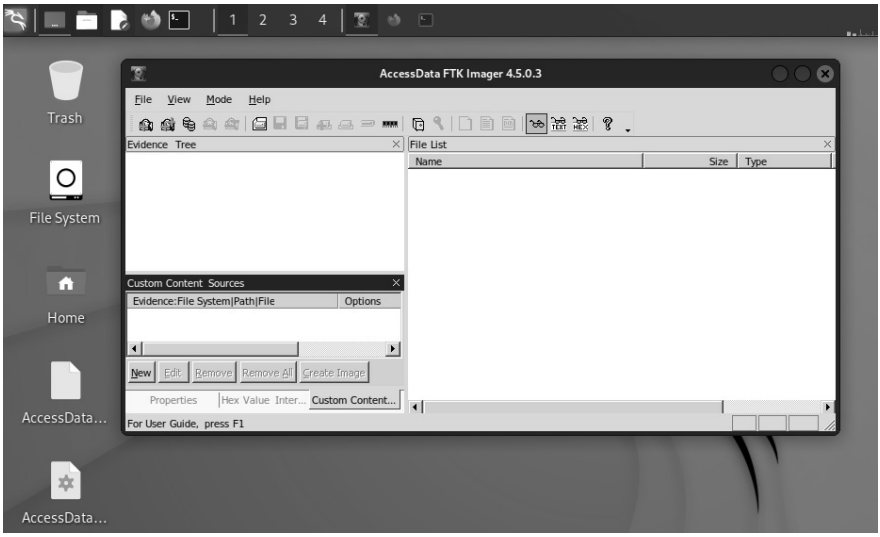
Rysunek 8.36. Zakończenie procesu instalowania pakietu FTK Imager

6. Na ekranie może teraz się pojawić prośba o pobranie pakietu instalatora Wine Gecko (zobacz rysunek 8.37), który jest wymagany do prawidłowego działania niektórych aplikacji. Aby go zainstalować, naciśnij przycisk *Install* (zainstaluj).



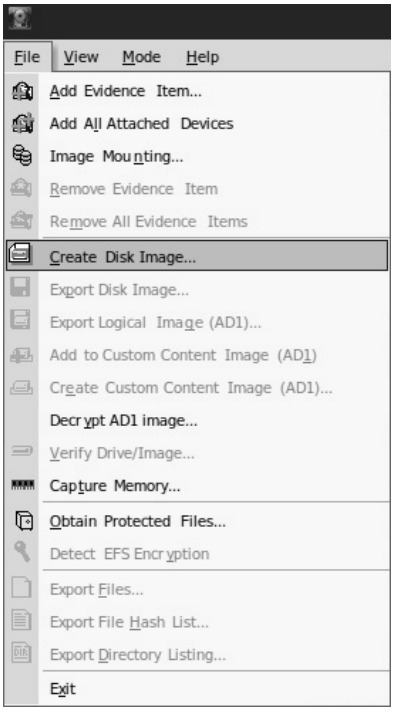
Rysunek 8.37. Instalator pakietu Wine Gecko

Jeżeli wszystko poszło zgodnie z oczekiwaniami, program FTK Imager powinien teraz zostać uruchomiony i na ekranie powinno się pojawić jego okno, pokazane na rysunku 8.38.



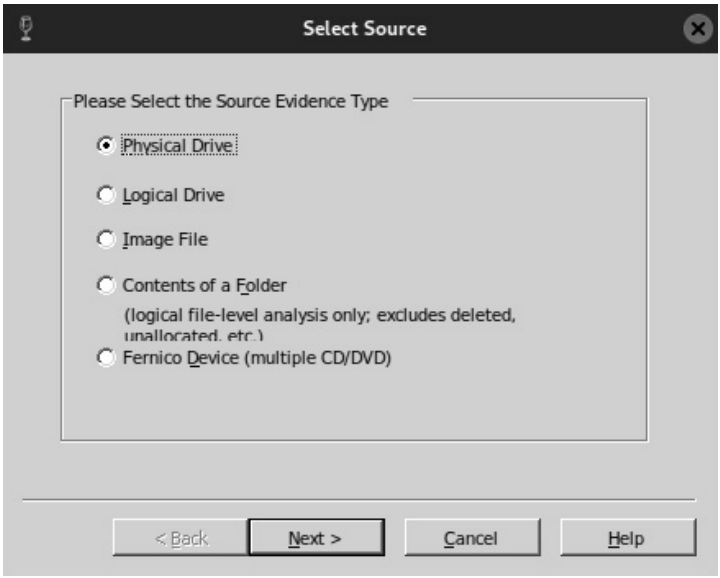
Rysunek 8.38. Interfejs programu FTK Imager uruchomionego w systemie Kali Linux

7. Aby wyświetlić opcje tworzenia obrazów binarnych, kliknij menu *File* (plik), które zostało pokazane na rysunku 8.39.



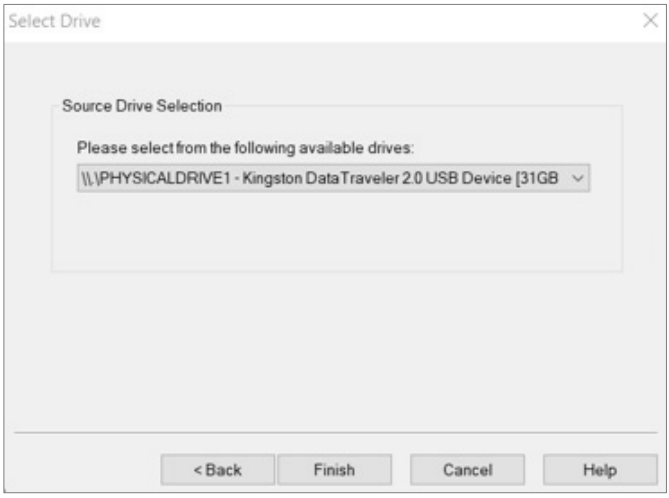
Rysunek 8.39. Menu File w programie FTK Imager

8. W menu *File* (plik) dostępnych jest kilka opcji umożliwiających pozyskiwanie i analizę cyfrowego materiału dowodowego. Opcja *Create Disk Image...* (utwórz obraz dysku) pozwala na tworzenie binarnych obrazów dysków fizycznych i logicznych, zawartości folderów oraz płyt CD i DVD. Kliknij tę opcję, a na ekranie pojawi się okno pozwalające na wybranie źródłowego nośnika danych, pokazane na rysunku 8.40.

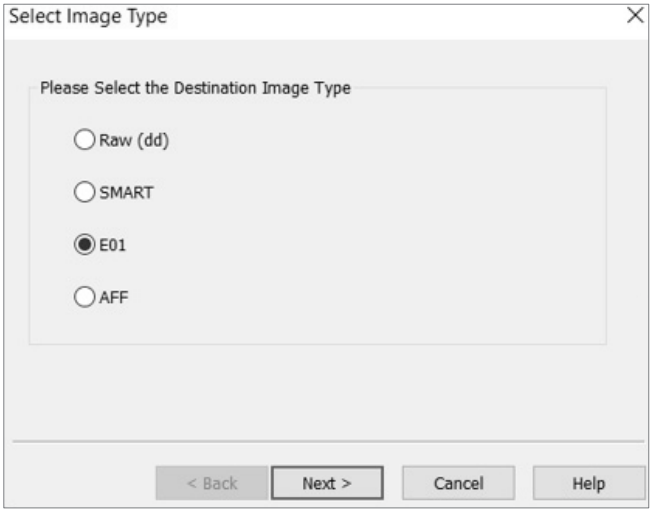


Rysunek 8.40. Wybór źródłowego nośnika danych w programie FTK Imager

9. Naciśnij przycisk *Next* (dalej), aby kontynuować. W naszym przykładzie wybrałem fizyczny dysk Kingston o pojemności 32 GB, jak to zostało pokazane na rysunku 8.41 (oczywiście na swojej maszynie możesz wybrać dowolny inny dysk). Po dokonaniu wyboru naciśnij przycisk *Finish* (zakończ).
10. Następnie musisz wybrać miejsce docelowe do zapisania pliku obrazu. Naciśnij przycisk *Add* (dodaj), wybierz typ obrazu (*Raw*, *SMART*, *E01* lub *AFF*, jak pokazano na rysunku 8.42), a następnie naciśnij przycisk *Next* (dalej).
11. Na ekranie pojawi się okno dialogowe *Evidence Item Information* (informacje o dowodzie cyfrowym), pokazane na rysunku 8.43. Wypełnij pola formularza, a następnie naciśnij przycisk *Next* (dalej).
12. Na koniec wybierz folder docelowy obrazu i wpisz nazwę obrazu wraz z rozszerzeniem (zobacz rysunek 8.44).

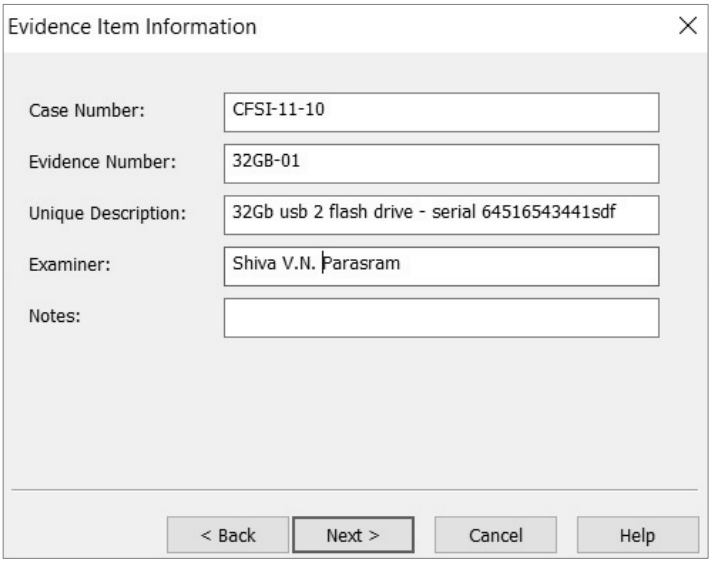


Rysunek 8.41. Wybór źródłowego dysku fizycznego

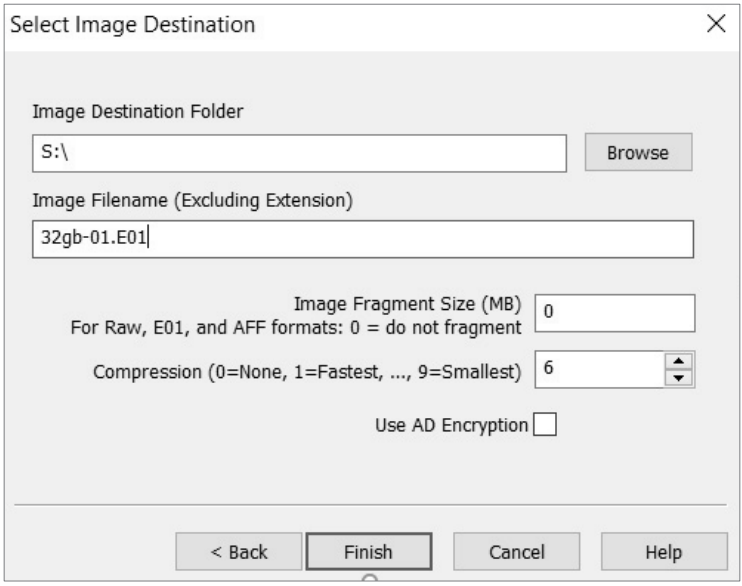


Rysunek 8.42. Wybór formatu obrazu binarnego

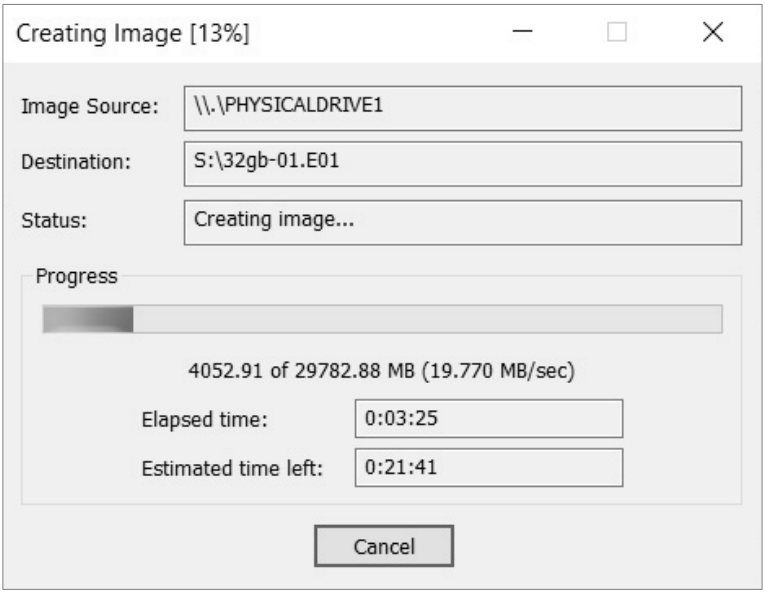
Opcję rozmiaru fragmentu pliku obrazu ustawiłem na wartość 0, dzięki czemu program nie będzie fragmentować ani dzielić pliku obrazu na kilka części. Aby rozpocząć proces tworzenia obrazu, naciśnij przycisk *Finish* (zakończ), a następnie przycisk *Start*. Przebieg procesu tworzenia obrazu pokazano na rysunku 8.45.



Rysunek 8.43. Wypełnianie informacji o obrazie binarnym



Rysunek 8.44. Wybieranie folderu, w którym zostanie utworzony obraz binarny



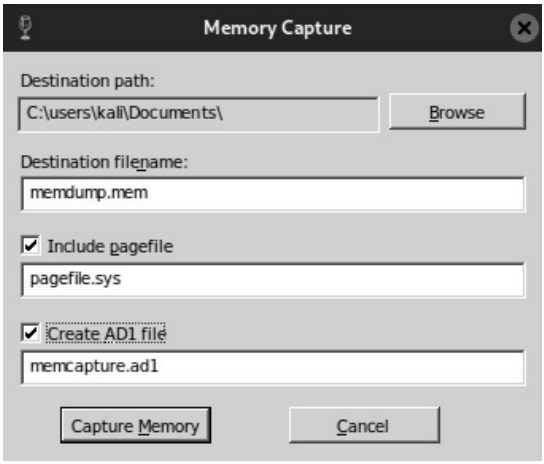
Rysunek 8.45. Proces tworzenia obrazu binarnego dysku za pomocą programu FTK Imager

Utworzony obraz dysku można teraz analizować za pomocą różnych narzędzi, takich jak Autopsy czy Volatility, które zostaną bardziej szczegółowo omówione w rozdziale 10., „Analiza śledcza zawartości pamięci przy użyciu pakietu Volatility 3", oraz w rozdziale 11., „Analiza artefaktów systemowych, malware i oprogramowania ransomware".

Tworzenie obrazów zawartości pamięci RAM za pomocą programu FTK Imager

Za pomocą programu FTK Imager możemy również utworzyć obraz binarny zawartości pamięci RAM oraz pliku stronicowania działającego systemu. Aby to zrobić, powinieneś wykonać polecenia opisane poniżej:

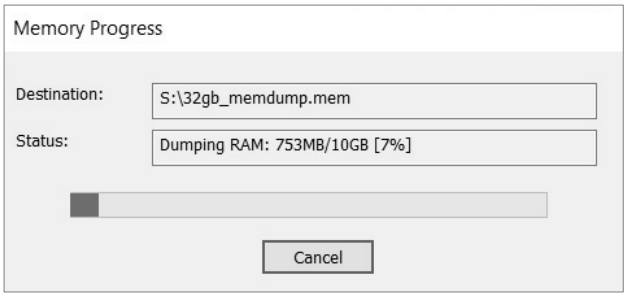
1. Z menu głównego wybierz polecenie *File/Memory Capture* (plik/przechwytywanie pamięci). Na ekranie pojawi się okno dialogowe Memory Capture, pokazane na rysunku 8.46.



Rysunek 8.46. Tworzenie obrazu zawartości pamięci i pliku stronicowania za pomocą programu FTK Imager

2. Teraz wybierz ścieżkę docelową i wpisz nazwę pliku obrazu zawartości pamięci (*.mem*). Aby dołączyć plik stronicowania, zaznacz opcję *Include pagefile* (dołącz plik stronicowania).
3. Naciśnij przycisk *Capture Memory* (przechwyć pamięć), aby rozpocząć proces tworzenia obrazu zawartości pamięci.

Pasek stanu poinformuje Cię o zakończeniu procesu (zobacz rysunek 8.47). Zwykle nie zajmuje to zbyt wiele czasu, zwłaszcza w porównaniu z procesem tworzenia obrazu dysku twardego. Pamiętaj, że tworzenie zrzutu pamięci w maszynie wirtualnej może być problematyczne; jednak opcji tej bez problemu możesz używać na komputerze działającym pod kontrolą systemu Kali Linux z zainstalowanym pakietem Wine lub na dowolnej maszynie z systemem Windows.



Rysunek 8.47. Proces tworzenia obrazu zawartości pamięci za pomocą programu FTK Imager

Jak sam się mogłeś przekonać, tworzenie obrazu zawartości pamięci za pomocą programu FTK Imager jest dosyć proste. W następnym podrozdziale poznasz kolejne narzędzie, RAM Capturer, którego również możesz używać do tworzenia obrazów zawartości pamięci RAM.

Tworzenie obrazów pamięci RAM i plików stronicowania za pomocą programu Belkasoft RAM Capturer

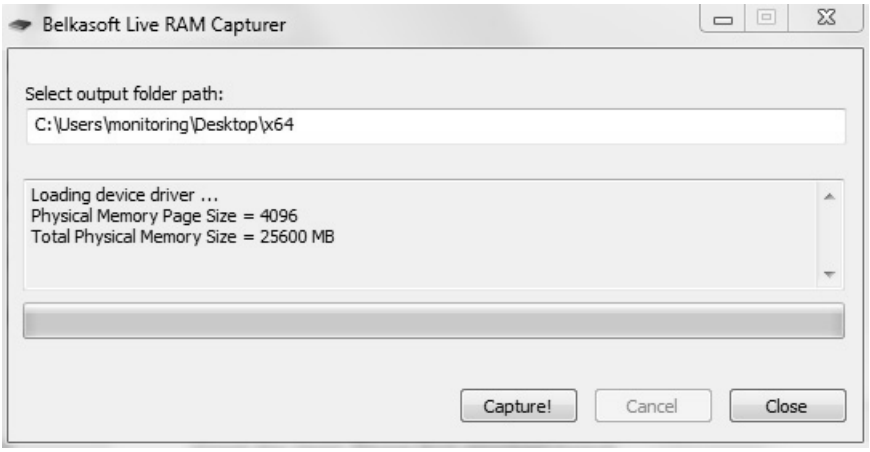
Belkasoft to firma, która od wielu lat tworzy specjalistyczne narzędzia dla informatyki śledczej, a także oferuje pakiet narzędzi do tworzenia obrazów i analizy śledczej nośników danych. Jednym z takich narzędzi jest bezpłatny program RAM Capturer, który można pobrać ze strony *https://belkasoft.com/ram-capturer*. Narzędzie to najlepiej sprawdza się w systemie Windows, ale chciałem o nim tutaj wspomnieć ze względu na jego popularność i szybkość działania.

Po wejściu na stronę *https://belkasoft.com/ram-capturer* naciśnij przycisk *Download Now* (pobierz teraz), wpisz swój adres e-mail i naciśnij przycisk *Proceed* (rozpocznij). W ciągu 24 godzin powinieneś otrzymać wiadomość e-mail z linkiem do pobrania programu.

Po pobraniu i rozpakowaniu programu na komputerze z systemem Windows wybierz odpowiednią wersję (`x86` lub `x64`) i uruchom program.

Graficzny interfejs użytkownika programu Belkasoft RAM Capturer jest naprawdę bardzo prosty. Aby utworzyć plik obrazu zawartości pamięci, wpisz ścieżkę do folderu, w którym ma zostać zapisany plik, następnie naciśnij przycisk *Capture!* (przechwyć); zobacz rysunek 8.48.

Proces tworzenia obrazu zawartości pamięci zajmuje zwykle kilka minut, a po jego zakończeniu możesz używać innych narzędzi do obliczenia wartości wybranej funkcji skrótu kryptograficznego czy przeprowadzenia analizy. To tyle, co chciałem Ci przekazać na temat programu RAM Capturer, będącego jednym z najprostszych dostępnych narzędzi do pozyskiwania zawartości pamięci RAM.



Rysunek 8.48. Tworzenie obrazu zawartości pamięci za pomocą programu Belkasoft Live RAM Capturer

Podsumowanie

W tym rozdziale omówiliśmy kilka narzędzi do tworzenia obrazów zawartości dysków i innych nośników danych, które są dostępne bezpośrednio w systemie Kali Linux, oraz narzędzie o nazwie FTK Imager, które jest natywnie przeznaczone dla systemu Windows, ale może być zainstalowane w systemie Kali Linux za pośrednictwem pakietu Wine. Dowiedziałeś się, dlaczego najpierw za pomocą polecenia `fdisk -l` musisz dokonać identyfikacji urządzeń, aby można było później utworzyć pełną kopię bitową nośnika dowodowego. Do przeprowadzenia analizy śledczej niezbędne jest wykonanie obrazu binarnego (kopii bitowej) materiału dowodowego i do tego celu używaliśmy takich narzędzi jak DC3DD, DD i Guymager.

Najpierw użyliśmy programu DC3DD, będącego rozbudowaną wersją popularnego narzędzia DD. Program DC3DD to narzędzie działające z poziomu wiersza poleceń konsoli, za pośrednictwem którego wykonaliśmy sporo zadań, takich jak tworzenie obrazu zawartości nośników danych, haszowanie obrazu i jego weryfikacja oraz czyszczenie dysku. Podobne zadania wykonywaliśmy również przy użyciu programu DD, który jest bardzo zbliżony do DC3DD.

Trzeci program, Guymager, ma wbudowane możliwości opisywania tworzonego obrazu metadanymi i funkcjonalnie jest bardzo podobny do DC3DD, z tym że jest wyposażony w graficzny interfejs użytkownika i dlatego jest częściej wybierany przez początkujących i mniej doświadczonych użytkowników.

Wszystkie narzędzia omówione w tym rozdziale działają dokładnie i bardzo rzetelnie. Jeżeli nie masz zbyt wielu doświadczeń w pracy z programami konsolowymi, takimi jak DD i DC3DD, program Guymager może być dla Ciebie łatwiejszym w użyciu narzędziem, biorąc pod uwagę to, że wszystkie jego opcje, w tym klonowanie czy odczytywanie dziennika tworzenia obrazu, są łatwo dostępne za pośrednictwem graficznego interfejsu użytkownika. W przypadku bardziej zaawansowanych zastosowań, takich jak wymazywanie dysku, warto jednak użyć programu DC3DD, ale jak zawsze ostateczny wybór należy do Ciebie.

W tym rozdziale przyjrzeliśmy się również programom FTK Imager i Belkasoft Ram Capturer. FTK Imager jest natywnie przeznaczony dla systemu Windows, ale można go łatwo zainstalować w systemie Kali Linux za pośrednictwem pakietu Wine. Program FTK Imager pozwala na tworzenie obrazów zawartości pamięci RAM, dysków twardych i innych nośników danych, podczas gdy program Belkasoft RAM Capturer (również przeznaczony dla systemu Windows) tworzy tylko obraz zawartości pamięci RAM.

Myślę, że poszło nam całkiem nieźle jak na pierwsze spotkanie z narzędziami śledczymi dostępnymi w systemie Kali Linux! W kolejnym rozdziale przejdziemy do omawiania narzędzi pozwalających na analizowanie i odzyskiwanie plików. To będzie naprawdę ekscytujące!

Kali Linux: Twój najlepszy partner w cyfrowej dochodzeniówce!

Aby pomyślnie przeprowadzić dochodzenie cyfrowe, poza specjalnymi umiejętnościami i wiedzą techniczną musisz dysponować odpowiednimi narzędziami. Z rozwoju technologii korzystają również przestępcy, którzy popełniają swoje występki na wiele dotychczas nieznanych sposobów. W tych warunkach bezcenną pomoc możesz znaleźć w Kali Linuksie — potężnym systemie specjalnie przygotowanym do prowadzenia testów penetracyjnych i dochodzeń w informatyce śledczej.

Ta książka pomoże Ci w doskonaleniu umiejętności potrzebnych na każdym etapie dochodzenia cyfrowego, od zbierania dowodów, poprzez ich analizę, po tworzenie raportów. Dzięki wielu wskazówkom i praktycznym ćwiczeniom przyswoisz techniki analizy, ekstrakcji danych i raportowania przy użyciu zaawansowanych narzędzi. Poznasz różne systemy przechowywania plików i nauczysz się wyszukiwać urządzenia sieciowe za pomocą skanerów Nmap i Netdiscover. Zapoznasz się też ze sposobami utrzymywania integralności cyfrowego materiału dowodowego. Znajdziesz tu ponadto omówienie kilku bardziej zaawansowanych tematów, takich jak pozyskiwanie ulotnych danych z sieci, nośników pamięci i systemów operacyjnych.

Z książki dowiesz się:

- jak przygotować system Kali Linux do pracy na różnych platformach sprzętowych
- po co w analizach DFIR bada się zawartość RAM, a także systemy plików i nośniki danych
- jak używać narzędzi takich jak Scalpel, Magic Rescue, Volatility 3 czy Autopsy 4
- czym jest ransomware i jak korzystać z artefaktów systemowych w dochodzeniach DFIR
- jak za pomocą narzędzi NFAT przechwytywać pakiety i analizować ruch sieciowy
- jak odpowiednio reagować na ataki ransomware

Shiva V. N. Parasram od niemal 20 lat zajmuje się cyberbezpieczeństwem i szacowaniem ryzyka. Specjalizuje się w testach penetracyjnych i reagowaniu na incydenty bezpieczeństwa. Jest też znany z wartościowych, zaawansowanych szkoleń z zakresu cyberbezpieczeństwa, również dla ISACA, ISC2, uniwersytetów i różnych agencji bezpieczeństwa.

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl
KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-289-0592-4
9 788328 905924
Cena: 99,00 zł