których narzędzia informatyki śledczej nie obsługują bezpośrednio. Kolejne fragmenty zawierają również przykłady bezpiecznego montowania (w trybie tylko do odczytu) plików obrazów jako zwykłych systemów plików hosta zabezpieczenia. Dzięki temu możliwe jest uzyskiwanie dostępu oraz przeglądanie ich zawartości za pomocą programów codziennego użytku, takich jak menedżery plików, pakiety biurowe, przeglądarki plików, odtwarzacze multimedialne itp.

Pliki obrazów pozyskanych w celach dowodowych

Podstawą wielu metod i przykładów przedstawianych w tej części jest linuxowe urządzenie pętli (nie mylić z urządzeniem pętli zwrotnej, które jest interfejsem sieciowym). *Urządzenie pętli* to pseudourządzenie, które może być powiązane ze zwykłym plikiem, dzięki czemu staje się on dostępny jako urządzenie blokowe w katalogu */dev*.

Systemy Linux zazwyczaj domyślnie tworzą 8 urządzeń pętli, które mogą nie wystarczyć w przypadku hosta zabezpieczenia. Można tę liczbę zwiększyć podczas uruchamiania systemu w sposób automatyczny albo ręcznie. Aby utworzyć 32 urządzenia pętli, należy dodać podczas uruchomienia `max_loop=32` do wiersza `GRUB_CMDLINE_LINUX_DEFAULT=` w pliku */etc/default/grub*. Po ponownym uruchomieniu powinny być dostępne 32 gotowe do użycia urządzenia pętli. Skrypt sfsimage używa urządzeń pętli do montowania kontenerów dowodowych SquashFS.

Rozdział ten omawia również różne obrazy maszyn wirtualnych, używanych przez popularne systemy wirtualizacji, takie jak QEMU, VirtualBox, VMWare i Microsoft Virtual PC. Opisałem w nim także uzyskiwanie dostępu do systemów plików, szyfrowanych na poziomie systemu operacyjnego, takich jak BitLocker Microsoftu, FileVault Apple, Linux LUKS i VeraCrypt (powstały z rozgałęzienia kolejnych wersji kodu TrueCrypt). Ale zacznijmy od najprostszej formy obrazu – nieprzetworzonego obrazu dysku, uzyskanego za pomocą narzędzia do akwizycji typu dd.

Pliki nieprzetworzonych obrazów dysków oraz urządzenia pętli

Najprostszym przykładem zastosowania urządzenia pętli jest użycie go do nieprzetworzonego obrazu dysku (możliwego do uzyskania za pomocą najprostszego wywołania polecenia `dd`). Komenda `losetup` podłącza i odłącza urządzenia pętli w systemie Linux. W następującym przykładzie tworzy ona urządzenie blokowe z zawartością pliku *image.raw*:

```
# losetup --read-only --find --show image.raw
/dev/loop0
```

W tym przykładzie flagi wskazują, że pętla powinna być tylko do odczytu (`--read-only`). Należy użyć pierwszego dostępnego urządzenia (`--find`), wyświetlając je po wykonaniu tego polecenia (`--show`). Wskazany nazwą plik (*image.raw*) stanie się dostępny jako podłączone do systemu urządzenie blokowe.

Wywołanie polecenia `losetup` bez dodatkowych parametrów wyświetla status wszystkich skonfigurowanych urządzeń pętli. Można więc będzie zobaczyć to utworzone wcześniej:

```
# losetup
NAME       SIZELIMIT OFFSET AUTOCLEAR RO BACK-FILE
/dev/loop0         0      0         0  1 /exam/image.raw
```

Urządzenie */dev/loop0* w tym przypadku wskazuje na */exam/image.raw*, można więc uzyskać dostęp do jego zawartości za pomocą dowolnych narzędzi, które są w stanie pracować z urządzeniami blokowymi. Na przykład polecenie Sleuth Kit `mmls` potrafi wyświetlić tablicę partycji pliku *image.raw* za pomocą urządzenia pętli:

```
# mmls /dev/loop0
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  Meta    0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000000   0000002047   0000002048   Unallocated
02:  00:00   0000002048   0058597375   0058595328   Linux (0x83)
03:  00:01   0058597376   0078129151   0019531776   Linux Swap / Solaris x86
(0x82)
04:  00:02   0078129152   0078231551   0000102400   NTFS (0x07)
05:  00:03   0078231552   0234441647   0156210096   Mac OS X HFS (0xaf)
```

Gdy urządzenie pętli nie jest już potrzebne, można je po prostu odłączyć w następujący sposób:

```
# losetup --detach /dev/loop0
```

Urządzenia pętli dają się dostosowywać i konfigurować. W poprzednim przykładzie z użyciem mmls system plików zaczynał się w sektorze 2048. Można określać przesunięcie początku danych za każdym razem, gdy uruchamiane jest narzędzie do analizy śledczej, ale łatwiej jest mieć osobne urządzenie dla każdej partycji (np. */dev/sda1*). Istnieje możliwość utworzenia oddzielnego urządzenia pętli za pomocą polecenia `losetup` tylko dla wybranej partycji przez podanie odpowiednich flag przesunięcia początku danych (`--offset`) oraz ich rozmiaru (`--sizelimit`). Zwyczajowo jednak stosuje się narzędzie mapowania urządzeń.

Aby zmapować tablicę partycji, można zastosować dmsetup wywołane ręcznie, tak jak zostało to opisane w części „RAID i systemy wielodyskowe" na stronie 185. Narzędzie kpartx automatyzuje jednak tworzenie urządzeń partycji dla danego pliku obrazu. Zabezpieczony dowodowo obraz, zawierający cztery partycje, został użyty w następnym przykładzie w celu zademonstrowania działania narzędzia kpartx. Mapuje ono poszczególne partycje na utworzone w tym celu urządzenia:

```
# kpartx -r -a -v image.raw
add map loop0p1 (252:0): 0 58595328 linear /dev/loop0 2048
add map loop0p2 (252:1): 0 19531776 linear /dev/loop0 58597376
```

```
add map loop0p3 (252:2): 0 102400 linear /dev/loop0 78129152
add map loop0p4 (252:3): 0 156210096 linear /dev/loop0 78231552
```

Jak widać, narzędzie kpartx odczytuje tablicę partycji dysku lub pliku obrazu. Tworzy następnie urządzenie pętli dla całego obrazu, po czym kolejne urządzenia mapowania dla poszczególnych partycji. Flaga `-r` zapewnia, że pętla odpowiadająca dyskowi oraz mapowania partycji są dostępne tylko do odczytu. Flaga `-a` nakazuje kpartx mapować wszystko, co znajdzie. Użycie flagi `-v` zwiększającej liczbę wypisywanych informacji pozwala udokumentować dane wyjściowe polecenia i wskazać, co zostało zmapowane.

W tym przykładzie tworzone jest urządzenie pętli (*/dev/loop0*) z zawartością całego pliku obrazu. Umożliwia ono bezpośredni dostęp do jego zawartości przez urządzenie blokowe. Ponadto urządzenia partycji są udostępniane w katalogu */dev/mapper*. Można więc uzyskać do nich dostęp za pomocą narzędzi informatyki śledczej pracujących z całymi partycjami, bez konieczności określania jakichkolwiek przesunięć początkowych danych. Oto przykładowe polecenia z pakietu Sleuth Kit dla kilku wybranych partycji:

```
# fsstat /dev/mapper/loop0p1
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: Ext4
Volume Name:
Volume ID: d4605b95ec13fcb43646de38f7f49680
...
# fls /dev/mapper/loop0p3
r/r 4-128-1:    $AttrDef
r/r 8-128-2:    $BadClus
r/r 8-128-1:    $BadClus:$Bad
r/r 6-128-1:    $Bitmap
r/r 7-128-1:    $Boot
d/d 11-144-2:   $Extend
r/r 2-128-1:    $LogFile
r/r 0-128-1:    $MFT
...
# fsstat /dev/mapper/loop0p4
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: HFS+
File System Version: HFS+
...
```

Zmapowany na urządzenie, zawarty w obrazie system plików może być bezpiecznie zamontowany w trybie tylko do odczytu. Umożliwia to dostęp do jego zawartości za pomocą standardowego menedżera plików, aplikacji i innych narzędzi do analizy plików. Można zamontować i odmontować partycje urządzenia pętli metodą pokazaną w kolejnym przykładzie:

```
# mkdir p3
# mount --read-only /dev/mapper/loop0p3 p3
# mc ./p3
...
# umount p3
# rmdir p3
```

W tym przypadku katalog *p3* reprezentujący partycję został utworzony w tym samym katalogu, w którym zapisany jest plik nieprzetworzonego obrazu. Następnie *p3* został użyty jako punkt montowania. (Wybrany punkt montowania może znajdować się w dowolnym miejscu systemu plików hosta zabezpieczenia). Midnight Commander (`mc`) to tekstowy menedżer plików (klon Norton Commandera) użyto go w tym przykładzie do przeglądania plików zamontowanej partycji. Jeśli punkt montowania nie jest już potrzebny, polecenie `umount` odmontowuje system plików. (To polecenie jest napisane poprawnie, tylko z jednym *n* w środku w porównaniu z angielskim *unmount*). Komenda `rmdir` usuwa katalog będący wcześniej punktem montowania. Opisana procedura prezentuje tradycyjny, unixowy sposób montowania i odmontowywania systemu plików w systemie hosta. Jeśli pętla odpowiadająca dyskowi oraz mapowania partycji nie są już potrzebne, można je wszystkie usunąć, używając kpartx z flagą (`-d`) wraz z nazwą pliku obrazu. Odbywa się to w następujący sposób:

```
# kpartx -d image.raw
loop deleted : /dev/loop0
```

Należy zwrócić uwagę, że to usunięcie nie ma wpływu na zawartość obrazu dysku. To pętla i mapowania są usuwane, a nie obraz dysku. Nie jest on również modyfikowany. Jeśli nieprzetworzony obraz ma uszkodzoną lub nadpisaną tablicę partycji, można przeszukać go pod kątem zawartych systemów plików i użyć dmsetup do ich ręcznego zmapowania jako urządzeń (za pomocą tablic dmsetup). Podczas tworzenia, montowania, odmontowywania lub odłączania urządzenia pętli wymagane są uprawnienia roota. Są one również potrzebne do bezpośredniej pracy z urządzeniami */dev/loopX* za pomocą narzędzi informatyki śledczej. Przykłady pokazane w tej części były uruchamiane przez użytkownika root. Miało to na celu zmniejszenie złożoności zapisanych poleceń, ułatwiając w ten sposób ich zrozumienie. Poprzedzanie poleceń komendą `sudo` może być używane przez zwykłych użytkowników do uruchamiania poleceń w sposób uprzywilejowany.

Pliki obrazów w formatach dowodowych

Pakiet oprogramowania ewflib zawiera narzędzie o nazwie ewfmount do „montowania" zawartości obrazów w formatach dowodowych, dzięki czemu ich zawartość staje się dostępna za pośrednictwem zwykłego pliku nieprzetworzonego obrazu.

Kolejny przykład prezentuje grupę plików **.e01*. Polecenie `mkdir` tworzy punkt montowania `raw`, w którym zostanie udostępniony plik nieprzetworzonego obrazu: