

# Tworzenie kopii binarnej nośnika – Szymon Szkarłat

Celem zadania 4 projektu jest wykonanie kopii binarnej nośnika (pendrive'a). Nośnik zawiera dane, które wcześniej przygotowałem.

Na początku sprawdzam jakie urządzenia są podłączone, aby upewnić się, że nośnik jest widoczny przez system.

```
(szymon@szymon)-[~]
$ sudo fdisk -l
Disk /dev/sda: 75 GiB, 80530636800 bytes, 157286400 sectors
Disk model: VMware Virtual S
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: 0x8fc1ea36

Device      Boot    Start        End    Sectors    Size Id Type
/dev/sda1   *          2048    60913663    60911616    29G 83 Linux
/dev/sda2             60915710    62912511    1996802    975M  5 Extended
/dev/sda5             60915712    62912511    1996800    975M 82 Linux swap / Solaris

Disk /dev/sdb: 7,5 GiB, 8053063680 bytes, 15728640 sectors
Disk model: UDisk
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: 0x0005cc9e

Device      Boot    Start        End    Sectors    Size Id Type
/dev/sdb1   *          2048    6397951    6395904     3G  c W95 FAT32 (LBA)
```

Wykonuję polecenie ewfdacquire /dev/sdb1

```
(szymon@szymon)-[~]
$ sudo -s
(root@szymon)-[/home/szymon]
# ewfdacquire /dev/sdb1
ewfdacquire 20140814

Device information:
Bus type:          USB
Vendor:            General
Model:             UDisk
Serial:

Storage media information:
Type:              Device
Media type:        Removable
Media size:        3.2 GB (3274702848 bytes)
Bytes per sector:  512
```

Wprowadzone przeze mnie opcje

```
The following acquiry parameters were provided:
Image path and filename: /home/szymon/USB_image.E01
Case number: image001 001
Description: image
Evidence number: 001
Examiner name: Szymon
Notes:
Media type: removable disk
Is physical: no
EWF file format: EnCase 6 (.E01)
Compression method: deflate
Compression level: none
Acquiry start offset: 0
Number of bytes to acquire: 3.0 GiB (3274702848 bytes)
Evidence segment file size: 1.4 GiB (1493172224 bytes)
Bytes per sector: 512
Block size: 64 sectors
Error granularity: 64 sectors
Retries on read error: 2
Zero sectors on read error: no

Continue acquiry with these values (yes, no) [yes]: yes

Acquiry started at: Dec 29, 2023 16:35:25
This could take a while.

Status: at 1%.
acquired 54 MiB (57606144 bytes) of total 3.0 GiB (3274702848 bytes).
completion in 6 minute(s) and 36 second(s) with 7.8 MiB/s (8186757 bytes/second).
```

Tworzenie kopii zakończyło się sukcesem

```
Status: at 96%.
acquired 2.9 GiB (3168534528 bytes) of total 3.0 GiB (3274702848 bytes).
completion in 9 second(s) with 13 MiB/s (14054518 bytes/second).

Status: at 98%.
acquired 3.0 GiB (3225092096 bytes) of total 3.0 GiB (3274702848 bytes).
completion in 4 second(s) with 13 MiB/s (14115098 bytes/second).

Acquiry completed at: Dec 29, 2023 16:39:16

Written: 3.0 GiB (3274703036 bytes) in 3 minute(s) and 51 second(s) with 13 MiB/s (14176203 bytes/second).
MD5 hash calculated over data: 5bbe910c4bd9da48bf68fa0f892a2ed1
ewfacquire: SUCCESS
```

```
text2.rar.xml
USB_4GB_Kingston.E01
USB_image.E01
USB_image.E02
USB_image.E03
Wideo
```

Po zweryfikowaniu za pomocą odpowiedniego polecenia, stwierdzam, że kopia binarna została prawidłowo wykonana. Wartości MD5 hash są takie same.

```
(root@szymon)-[/home/szymon]  
# ewfverify USB_image.E01
```

```
ewfverify 20140814
```

```
Verify started at: Dec 29, 2023 17:45:58  
This could take a while.
```

```
Status: at 24%.
```

```
verified 761 MiB (798556160 bytes) of total 3.0 GiB (3274702848 bytes).  
completion in 12 second(s) with 195 MiB/s (204668928 bytes/second).
```

```
Status: at 55%.
```

```
verified 1.7 GiB (1819148288 bytes) of total 3.0 GiB (3274702848 bytes).  
completion in 6 second(s) with 223 MiB/s (233907346 bytes/second).
```

```
Status: at 86%.
```

```
verified 2.6 GiB (2841477120 bytes) of total 3.0 GiB (3274702848 bytes).  
completion in 1 second(s) with 240 MiB/s (251900219 bytes/second).
```

```
Verify completed at: Dec 29, 2023 17:46:11
```

```
Read: 3.0 GiB (3274702848 bytes) in 13 second(s) with 240 MiB/s (251900219 bytes/second).
```

```
MD5 hash stored in file: 5bbe910c4bd9da48bf68fa0f892a2ed1
```

```
MD5 hash calculated over data: 5bbe910c4bd9da48bf68fa0f892a2ed1
```

```
ewfverify: SUCCESS
```



## Informacje o obrazie

```
(root@szymon)-[/home/szymon]
# ewfinfo USB_image.E01
ewfinfo 20140814

Acquiry information
Case number:          001
Description:          image
Examiner name:       Szymon
Evidence number:     001
Acquisition date:    Fri Dec 29 16:35:25 2023
System date:         Fri Dec 29 16:35:25 2023
Operating system used: Linux
Software version used: 20140814
Password:            N/A
Model:               UDisk

EWF information
File format:         EnCase 6
Sectors per chunk:   64
Error granularity:   64
Compression method:  deflate
Compression level:   no compression

Media information
Media type:          removable disk
Is physical:         no
Bytes per sector:    512
Number of sectors:   6395904
Media size:          3.0 GiB (3274702848 bytes)

Digest hash information
MD5:                 5bbe910c4bd9da48bf68fa0f892a2ed1
```

### Przedstawione informacje:

- Numer sprawy (Case number): 001
- Opis (Description): obraz (image)
- Imię egzaminatora (Examiner name): Szymon
- Numer dowodu (Evidence number): 001
- Data pozyskania (Acquisition date): Fri Dec 29 16:35:25 2023
- Data systemowa (System date): Fri Dec 29 16:35:25 2023
- Użyty system operacyjny (Operating system used): Linux
- Użyta wersja oprogramowania (Software version used): 20140814
- Hasło (Password): N/A
- Model: UDisk
- Format pliku (File format): EnCase 6
- Sektory na kawałek (Sectors per chunk): 64
- Granulacja błędu (Error granularity): 64
- Metoda kompresji (Compression method): deflate
- Poziom kompresji (Compression level): brak kompresji

- Typ nośnika (Media type): dysk wymienny (removable disk)
- Fizyczny (Is physical): nie (no)
- Bajtów na sektor (Bytes per sector): 512
- Ilość sektorów (Number of sectors): 6395904
- Rozmiar nośnika (Media size): 3.0 GiB (3274702848 bajtów)
- Wartość funkcji skrótu, czyli MD5 wynosi: 5bbe910c4bd9da48bf68fa0f892a2ed1

Wykonanie polecenia fsstat

```
(szymon@szymon)-[~]
$ fsstat USB_image.E01
FILE SYSTEM INFORMATION

File System Type: FAT32

OEM Name: MSDOS5.0
Volume ID: 0x4b5b179
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory):
File System Type Label: FAT32
Next Free Sector (FS Info): 168496
Free Sector Count (FS Info): 6227408

Sectors before file system: 2048

File System Layout (in sectors)
Total Range: 0 - 6395903
* Reserved: 0 - 3921
** Boot Sector: 0
** FS Info Sector: 1
** Backup Boot Sector: 6
* FAT 0: 3922 - 10152
* FAT 1: 10153 - 16383
* Data Area: 16384 - 6395903
** Cluster Area: 16384 - 6395903
*** Root Directory: 16384 - 16391
```

#### 1. Informacje o systemie plików:

- Typ systemu plików: FAT32
- OEM Name: MSDOS5.0
- ID woluminu: 0x4b5b179
- Etykieta woluminu (sektor rozruchowy): NO NAME
- Etykieta woluminu (katalog główny): (pusty)
- Etykieta typu systemu plików: FAT32
- Następny wolny sektor (FS Info): 168496
- Liczba wolnych sektorów (FS Info): 6227408
- Liczba sektorów przed systemem plików: 2048

## 2. Struktura systemu plików (w sektorach):

- Zarezerwowane:

- Zakres: 0 - 3921
- Sektor rozruchowy: 0
- Sektor informacji o systemie plików (FS Info): 1
- Zapasowy sektor rozruchowy: 6

- FAT 0: 3922 – 10152

- FAT 1: 10153 – 16383

- Obszar danych: 16384 - 6395903

- Obszar klastra: 16384 - 6395903
- Katalog główny: 16384 - 16391

Zawartość kopii binarnej – pliki, które wcześniej umieściłem na pendrive

```
(szymon@szymon)-[~]  
$ fls USB_image.E01  
d/d 5: System Volume Information  
r/r 10: Instrukcja obsługi INNO View 6S (EN).pdf  
r/r 14: T-REC-G.984.1-200803-I !! PDF-E.pdf  
r/r * 15: _alka.pdf  
r/r * 16: _alka.pdf  
r/r * 19: lalka.pdf.opdownload  
r/r 20: lalka.pdf  
r/r * 25: ee10-2020-czerwiec-egzamin-zawodowy-pisemny.pdf  
r/r * 31: ee10-2020-czerwiec-egzamin-zawodowy-pisemny.pdf.opdownload  
r/r 36: ee10-2020-czerwiec-egzamin-zawodowy-pisemny.pdf  
r/r * 42: ee10-2020-czerwiec-egzamin-zawodowy-pisemny-odpowiedzi.pdf  
r/r * 49: ee10-2020-czerwiec-egzamin-zawodowy-pisemny-odpowiedzi.pdf.opdownload  
r/r 55: ee10-2020-czerwiec-egzamin-zawodowy-pisemny-odpowiedzi.pdf  
r/r * 58: Manchester_Route_Map.jpg  
r/r * 62: Manchester_Route_Map.jpg.opdownload  
r/r 65: Manchester_Route_Map.jpg  
r/r * 70: Europa_w_czasach_Napoleona_(Ultima_Thule).png  
r/r * 76: Europa_w_czasach_Napoleona_(Ultima_Thule).png.opdownload  
r/r 81: Europa_w_czasach_Napoleona_(Ultima_Thule).png  
r/r 84: IMG_20230801_104010.jpg  
r/r 87: IMG_20230929_164918.jpg  
r/r 91: Cat.Goes.Fishing.Build.11957298.zip  
r/r 93: zad4_sito.py  
r/r 96: python-3.12.0-amd64.exe  
v/v 102072323: $MBR  
v/v 102072324: $FAT1  
v/v 102072325: $FAT2  
V/V 102072326: $OrphanFiles
```

## Informacje o obrazie

```
(szymon@szymon)-[~] USB_image
$ img_stat USB_image.E01
IMAGE FILE INFORMATION
-----
Image Type:          ewf
Size of data in bytes: 3274702848
Sector size:         512
MD5 hash of data:     5bbe910c4bd9da48bf68fa0f892a2ed1
```

## Zawartość pendrive'a

Dysk USB (D:) >					Przeszukaj: Dysk
Sortuj Wyświetl Wysuń					
Nazwa	Data modyfikacji	Typ	Rozmiar		
Cat.Goes.Fishing.Build.11957298.zip	29.12.2023 14:57	Folder skompresowa...	33 759 KB		
ee10-2020-czerwiec-egzamin-zawodowy-pise...	29.12.2023 14:37	Adobe Acrobat Docu...	2 332 KB		
ee10-2020-czerwiec-egzamin-zawodowy-pise...	29.12.2023 14:37	Adobe Acrobat Docu...	278 KB		
Europa_w_czasach_Napoleona_(Ultima_Thule).p...	29.12.2023 14:42	Plik PNG	1 032 KB		
IMG_20230801_104010.jpg	29.12.2023 14:50	Plik JPG	3 920 KB		
IMG_20230929_164918.jpg	29.12.2023 14:47	Plik JPG	4 386 KB		
Instrukcja obsługi INNO View 6S (EN).pdf	29.12.2023 14:12	Adobe Acrobat Docu...	1 094 KB		
lalka.pdf	29.12.2023 14:34	Adobe Acrobat Docu...	2 838 KB		
Manchester_Route_Map.jpg	29.12.2023 14:41	Plik JPG	246 KB		
python-3.12.0-amd64.exe	27.10.2023 12:25	Aplikacja	25 887 KB		
T-REC-G.984.1-200803-III!PDF-E.pdf	29.12.2023 14:14	Adobe Acrobat Docu...	252 KB		
zad4_sito.py	29.12.2023 15:00	Python Source File	1 KB		

## Wykonanie kopii binarnej za pomocą polecenia ds3dd

```
(szymon@szymon)-[~/Pulpit]
$ sudo dc3dd if=/dev/sdb1 hash=md5 log=dc3ddusb of=usb_image.dd

dc3dd 7.2.646 started at 2023-12-29 18:12:51 +0100
compiled option
```

Utworzenie kopii binarnej w ten sposób przynosi taki sam efekt i zwraca takie same wyniki oraz informacje o kopii binarnej nośnika jakim jest pendrive.

Podsumowując, proces tworzenia kopii binarnych jest niezwykle ważny i kluczowy, nie tylko podczas analizy plików pozyskanych podczas śledztwa, ale również podczas codziennych czynności. Umiejętność tworzenia kopii binarnej przydaje się podczas sytuacji, gdy nie chcemy pracować na nośniku w sposób bezpośredni, a chcemy jedynie przeprowadzić analizę zawartości nośnika. Dodatkowo, tworzenie kopii bezpieczeństwa danych z nośnika pendrive'a ma wiele praktycznych zastosowań i jest dobrym zwyczajem z punktu widzenia zarządzania informacjami oraz utrzymania bezpieczeństwa danych. Oto kilka głównych powodów, dla których warto posiadać umiejętność tworzenia kopii bezpieczeństwa białej kopii pendrive'a:

1. Zabezpieczenie przed utratą danych: W przypadku awarii pendrive'a, utraty lub uszkodzenia fizycznego, posiadanie kopii danych pozwala uniknąć trwałej utraty informacji.
2. Ochrona przed przypadkowym usunięciem: Przy korzystaniu z pendrive'a zawsze istnieje ryzyko przypadkowego usunięcia ważnych plików. Regularne tworzenie kopii danych pozwala na przywrócenie utraconych informacji.
3. Zabezpieczenie przed atakami ransomware: W przypadku ataków ransomware, kiedy pliki na pierwotnym nośniku stają się niedostępne, posiadanie kopii danych na innym nośniku pozwala na przywrócenie informacji bez konieczności płacenia okupu.
4. Łatwiejsza migracja danych: Kopie zapasowe ułatwiają przenoszenie danych między różnymi urządzeniami lub systemami operacyjnymi, co może być przydatne przy aktualizacji lub wymianie sprzętu.
5. Zachowanie ważnych dokumentów i danych: Pendrive'y są często używane do przechowywania ważnych dokumentów biznesowych, projektów czy zdjęć. Kopie bezpieczeństwa zapewniają ochronę przed utratą niezastąpionych informacji.
6. Zarządzanie wersjami plików: Tworzenie regularnych kopii bezpieczeństwa umożliwia śledzenie zmian w plikach, co może być przydatne w przypadku konieczności powrotu do wcześniejszych wersji.

W skrócie, umiejętność tworzenia kopii bezpieczeństwa pendrive'a pomaga w zminimalizowaniu ryzyka utraty danych, a także zwiększa ogólne bezpieczeństwo i spokój umysłu użytkownika.