Informatyka Śledcza - Laboratorium 4

Magdalena Ślusarczyk

1 Przygotowanie do odzyskiwania danych

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo dc3dd wipe=/dev/sdb1

dc3dd 7.2.646 started at 2021-11-27 13:28:16 -0500
compiled options:
command line: dc3dd wipe=/dev/sdb1
device size: 7561952 sectors (probed),    3,871,719,424 bytes
sector size: 512 bytes (probed)
  3871719424 bytes ( 3.6 G ) copied ( 100% ),  520 s, 7.1 M/s

input results for pattern `00':
   7561952 sectors in

output results for device `/dev/sdb1':
   7561952 sectors out

dc3dd completed at 2021-11-27 13:36:56 -0500
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo dc3dd if=/dev/sdb1 of=./file.dd hash=md5                    148 ✕ 3 ⚙

dc3dd 7.2.646 started at 2021-11-27 14:09:19 -0500
compiled options:
command line: dc3dd if=/dev/sdb1 of=./file.dd hash=md5
device size: 7561952 sectors (probed),    3,871,719,424 bytes
sector size: 512 bytes (probed)
  3871719424 bytes ( 3.6 G ) copied ( 100% ),  341 s, 11 M/s

input results for device `/dev/sdb1':
   7561952 sectors in
   0 bad sectors replaced by zeros
   b5ec18dd0fbf1a1447cd241e6af0de4e (md5)

output results for file `./file.dd':
   7561952 sectors out

dc3dd completed at 2021-11-27 14:15:00 -0500
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo md5sum /dev/sdb1                                            1 ✕ 4 ⚙
b5ec18dd0fbf1a1447cd241e6af0de4e  /dev/sdb1

┌──(kali㉿kali)-[~/Desktop]
└─$ md5sum ./file.dd                                                   4 ⚙
b5ec18dd0fbf1a1447cd241e6af0de4e  ./file.dd
```

2 Foremost

Pliki odzyskane z obrazu:

```
┌──(root💀kali)-[/home/kali/Desktop/output_file]
└─# ls -Rl
.:
total 20
-rw-r--r-- 1 root root 1098 Nov 27 14:39 audit.txt
drwxr-xr-- 2 root root 4096 Nov 27 14:38 exe
drwxr-xr-- 2 root root 4096 Nov 27 14:38 jpg
drwxr-xr-- 2 root root 4096 Nov 27 14:38 png
drwxr-xr-- 2 root root 4096 Nov 27 14:38 zip

./exe:
total 1296
-rw-r--r-- 1 root root 1327104 Nov 27 14:38 00040520.exe

./jpg:
total 596
-rw-r--r-- 1 root root  93696 Nov 27 14:38 00043224.jpg
-rw-r--r-- 1 root root 120517 Nov 27 14:38 00043408.jpg
-rw-r--r-- 1 root root 157703 Nov 27 14:38 00043648.jpg
-rw-r--r-- 1 root root  72338 Nov 27 14:38 00043960.jpg
-rw-r--r-- 1 root root 158818 Nov 27 14:38 00044104.jpg

./png:
total 40
-rw-r--r-- 1 root root 16810 Nov 27 14:38 00040640.png
-rw-r--r-- 1 root root 16810 Nov 27 14:38 00043040.png

./zip:
total 40
-rw-r--r-- 1 root root 37319 Nov 27 14:38 00043144.zip
```

Pliki odzyskane bezpośrednio z dysku:

```
┌──(root💀kali)-[/home/kali/Desktop/output_disc]
└─# ls -Rl
.:
total 20
-rw-r--r-- 1 root root 1098 Nov 27 14:46 audit.txt
drwxr-xr-- 2 root root 4096 Nov 27 14:42 exe
drwxr-xr-- 2 root root 4096 Nov 27 14:42 jpg
drwxr-xr-- 2 root root 4096 Nov 27 14:42 png
drwxr-xr-- 2 root root 4096 Nov 27 14:42 zip

./exe:
total 1296
-rw-r--r-- 1 root root 1327104 Nov 27 14:42 00040520.exe

./jpg:
total 596
-rw-r--r-- 1 root root  93696 Nov 27 14:42 00043224.jpg
-rw-r--r-- 1 root root 120517 Nov 27 14:42 00043408.jpg
-rw-r--r-- 1 root root 157703 Nov 27 14:42 00043648.jpg
-rw-r--r-- 1 root root  72338 Nov 27 14:42 00043960.jpg
-rw-r--r-- 1 root root 158818 Nov 27 14:42 00044104.jpg

./png:
total 40
-rw-r--r-- 1 root root 16810 Nov 27 14:42 00040640.png
-rw-r--r-- 1 root root 16810 Nov 27 14:42 00043040.png

./zip:
total 40
-rw-r--r-- 1 root root 37319 Nov 27 14:42 00043144.zip
```

Metadane przykładowego odzyskanego obrazu:

```
┌──(root💀kali)-[/home/kali/Desktop/output_disc/jpg]
└─# exiftool ./00043224.jpg
ExifTool Version Number         : 12.34
File Name                       : 00043224.jpg
Directory                       : .
File Size                       : 92 KiB
File Modification Date/Time     : 2021:11:27 14:42:49-05:00
File Access Date/Time           : 2021:11:27 14:42:49-05:00
File Inode Change Date/Time     : 2021:11:27 14:42:49-05:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.02
Exif Byte Order                 : Big-endian (Motorola, MM)
Photometric Interpretation      : RGB
Image Description               : G. [Gaston] Massiot et Compagnie (French photographic firm, active ca. 1899-1940);
Abbreviated G. Massiot & Cie; also Radiguet & Massiot (from 1899-1905); Aerial topographic view of Nice, France; Nice
, France - Panorama; Overall view, imaged from lantern slide; ca. 1899-before 1909 (creation); black and white film;
glass; 4 in (height) x 3.25 in (width); University of Notre Dame, Architecture Library (South Bend, Indiana, United S
```

3 Recoverjpeg

Program recoverjpeg odzyskuje jedynie obrazy.

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# recoverjpeg /dev/sdb1
Restored 5 pictures
```

Porównanie metadanych:

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# exiftool ./output_disc/jpg/00043224.jpg > meta_recoverjpeg

┌──(root💀kali)-[/home/kali/Desktop]
└─# exiftool ./image00000.jpg > meta_recoverjpeg

┌──(root💀kali)-[/home/kali/Desktop]
└─# diff meta_foremost meta_recoverjpeg
2,3c2,3
< File Name                     : 00043224.jpg
< Directory                     : ./output_disc/jpg
---
> File Name                     : image00000.jpg
> Directory                     : .
5,7c5,7
< File Modification Date/Time   : 2021:11:27 14:42:49-05:00
< File Access Date/Time         : 2021:11:27 14:59:16-05:00
< File Inode Change Date/Time   : 2021:11:27 14:42:49-05:00
---
> File Modification Date/Time   : 2021:11:27 15:03:19-05:00
> File Access Date/Time         : 2021:11:27 15:03:19-05:00
> File Inode Change Date/Time   : 2021:11:27 15:03:19-05:00
```

4 Scalpel

Odkomentowałam linie dla plików jpg, png, zip.

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# scalpel ./file.dd                                                                                    2 ⚙
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/home/kali/Desktop/file.dd"

Image file pass 1/2.
./file.dd: 100.0% |*************************************************************************|    3.6 GB    00:00 ETA
Allocating work queues ...
Work queues allocation complete. Building carve lists ...
Carve lists built.  Workload:
jpg with header "\xff\xd8\xff\x3f\x3f\x3f\x45\x78\x69\x66" and footer "\xff\xd9" ⟶ 1 files
jpg with header "\xff\xd8\xff\x3f\x3f\x3f\x4a\x46\x49\x46" and footer "\xff\xd9" ⟶ 9 files
png with header "\x50\x4e\x47\x3f" and footer "\xff\xfc\xfd\xfe" ⟶ 0 files
zip with header "\x50\x4b\x03\x04" and footer "\x3c\xac" ⟶ 51 files
Carving files from image.
Image file pass 2/2.
./file.dd: 100.0% |*************************************************************************|    3.6 GB    00:00 ETA
Processing of image file complete. Cleaning up ...
Done.
Scalpel is done, files carved = 61, elapsed = 14 seconds.
```

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# ls -Rl ./scalpel-output                                                                              2 ⚙
./scalpel-output:
total 16
-rw-r--r-- 1 root root 3757 Nov 27 15:21 audit.txt
drwxr-xr-x 2 root root 4096 Nov 27 15:21 jpg-0-0
drwxr-xr-x 2 root root 4096 Nov 27 15:21 jpg-1-0
drwxr-xr-x 2 root root 4096 Nov 27 15:21 zip-3-0

./scalpel-output/jpg-0-0:
total 5028
-rw-r--r-- 1 root root 5147917 Nov 27 15:21 00000000.jpg

./scalpel-output/jpg-1-0:
total 45816
-rw-r--r-- 1 root root 5199618 Nov 27 15:21 00000001.jpg
-rw-r--r-- 1 root root 5198714 Nov 27 15:21 00000002.jpg
-rw-r--r-- 1 root root 5225627 Nov 27 15:21 00000003.jpg
-rw-r--r-- 1 root root 5223735 Nov 27 15:21 00000004.jpg
-rw-r--r-- 1 root root 5222447 Nov 27 15:21 00000005.jpg
-rw-r--r-- 1 root root 5199128 Nov 27 15:21 00000006.jpg
-rw-r--r-- 1 root root 5229489 Nov 27 15:21 00000007.jpg
-rw-r--r-- 1 root root 5201320 Nov 27 15:21 00000008.jpg
-rw-r--r-- 1 root root 5196624 Nov 27 15:21 00000009.jpg

./scalpel-output/zip-3-0:
total 3560
-rw-r--r-- 1 root root 81202 Nov 27 15:21 00000010.zip
-rw-r--r-- 1 root root 81157 Nov 27 15:21 00000011.zip
-rw-r--r-- 1 root root 81107 Nov 27 15:21 00000012.zip
-rw-r--r-- 1 root root 80067 Nov 27 15:21 00000013.zip
-rw-r--r-- 1 root root 79695 Nov 27 15:21 00000014.zip
-rw-r--r-- 1 root root 79472 Nov 27 15:21 00000015.zip
-rw-r--r-- 1 root root 78625 Nov 27 15:21 00000016.zip
-rw-r--r-- 1 root root 78273 Nov 27 15:21 00000017.zip
-rw-r--r-- 1 root root 77813 Nov 27 15:21 00000018.zip
-rw-r--r-- 1 root root 77763 Nov 27 15:21 00000019.zip
-rw-r--r-- 1 root root 77362 Nov 27 15:21 00000020.zip
-rw-r--r-- 1 root root 77099 Nov 27 15:21 00000021.zip
-rw-r--r-- 1 root root 76201 Nov 27 15:21 00000022.zip
-rw-r--r-- 1 root root 75837 Nov 27 15:21 00000023.zip
-rw-r--r-- 1 root root 75544 Nov 27 15:21 00000024.zip
-rw-r--r-- 1 root root 75371 Nov 27 15:21 00000025.zip
-rw-r--r-- 1 root root 75163 Nov 27 15:21 00000026.zip
-rw-r--r-- 1 root root 74907 Nov 27 15:21 00000027.zip
```

Scalpel odzyskał każdy plik z archiwum osobno, podczas gdy poprzednie programy odzyskały spakowane archiwum.

5 Bulk extractor

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# ls -Rl ./bulk                                                    2 ⚙
./bulk:
total 168
-rw-r--r-- 1 root root     0 Nov 27 15:27 aes_keys.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 alerts.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 ccn_histogram.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 ccn_track2_histogram.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 ccn_track2.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 ccn.txt
-rw-r--r-- 1 root root   841 Nov 27 15:27 domain_histogram.txt
-rw-r--r-- 1 root root 12541 Nov 27 15:27 domain.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 elf.txt
-rw-r--r-- 1 root root   186 Nov 27 15:27 email_domain_histogram.txt
-rw-r--r-- 1 root root   193 Nov 27 15:27 email_histogram.txt
-rw-r--r-- 1 root root   876 Nov 27 15:27 email.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 ether_histogram.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 ether.txt
-rw-r--r-- 1 root root 11208 Nov 27 15:27 exif.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 find_histogram.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 find.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 gps.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 httplogs.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 ip_histogram.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 ip.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 jpeg_carved.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 json.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 kml.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 ntfsusn_carved.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 pii_teamviewer.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 pii.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 rar.txt
-rw-r--r-- 1 root root 48840 Nov 27 15:27 report.xml
-rw-r--r-- 1 root root     0 Nov 27 15:27 rfc822.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 sin.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 sqlite_carved.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 telephone_histogram.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 telephone.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 unrar_carved.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 unzip_carved.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 url_facebook-address.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 url_facebook-id.txt
-rw-r--r-- 1 root root  2236 Nov 27 15:27 url_histogram.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 url_microsoft-live.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 url_searches.txt
-rw-r--r-- 1 root root   780 Nov 27 15:27 url_services.txt
-rw-r--r-- 1 root root 19239 Nov 27 15:27 url.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 vcard.txt
-rw-r--r-- 1 root root  6756 Nov 27 15:27 windirs.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 winlnk.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 winpe_carved.txt
-rw-r--r-- 1 root root 15755 Nov 27 15:27 winpe.txt
-rw-r--r-- 1 root root     0 Nov 27 15:27 winprefetch.txt
-rw-r--r-- 1 root root 20556 Nov 27 15:27 zip.txt
```

6 Podsumowanie

Osobiście najbardziej zadowoliło mnie działanie programu foremost, ponieważ program ten był łatwy w użyciu, nie trzeba było zmieniać żadnych ustawień i odzyskał wszystkie usunięte pliki.