Informatyka śledcza

Laboratorium nr 4

agh.edu.pl

Spis treści

Wstęp

Laboratorium ma na celu zapoznanie studenta z narzędziami do odzyskiwania danych oraz analizą rejestru systemu Windows. Zadania przedstawiać będą praktyczne operacje odzwierciadlające schemat odzyskiwania danych, które zostały usunięte oraz mogły zostać nadpisane w fizycznym nośniku lub jego obrazie binarnym. W trakcie wykonywanych ćwiczeń zostaną przedstawione 5 darmowe narzędzia do odzyskiwania informacji, które posiadają swoje wyjątkowe właściwości.

Wykorzystywane narzędzia w trakcie laboratorium:

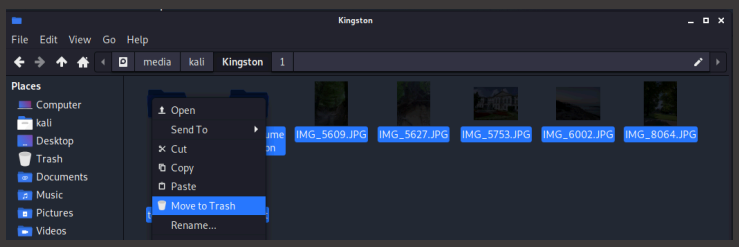
1. Foremost
2. Recoverjpeg
3. Scalpel
4. Bulk_Extractor
5. Regripper

Zadanie 1 – Przygotowanie do odzyskiwania danych

- W ramach zajęć proszę o przygotowanie czystego pendriva, na którym należy umieścić kilka zdjęć zrobionych telefonem z metadanymi (takimi jak np. położenie), kilka plików tekstowych, kilka plików rar, jeden lekki program .exe, kilka plików doc, oraz pdf. Przed rozpoczęciem kopiowania danych na pendriva należy go wyczyścić narzędziem *dc3dd*.

sudo dc3dd wipe=/dev/sdbx

- Następnie proszę usunąć przekopiowane dane z nośnika *sdbx*.



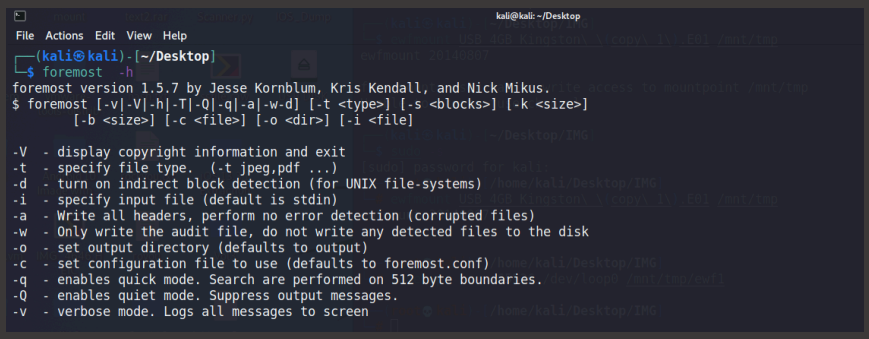
- Przenieś dowolny plik o rozmiarze około 100 MB na nośnik *sdbx*.

- Wykonaj kopie binarną nośnika *sdbx* (dc3dd).

- Wykorzystując narzędzie *md5sum* sprawdź poprawność wykonania kopii.

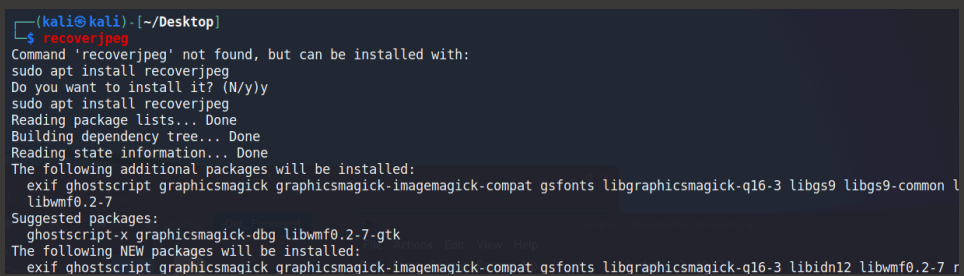
Zadanie 2 – Foremost

Wykorzystaj narzędzie *foremost* do próby odzyskania jak największej ilości danych z nowo utworzonego obrazu (*.dd*) oraz fizycznego urządzenia (*/dev/sdbx*). Proszę o przedstawienie uzyskanego rezultatu w postaci dokumentacji graficznej oraz opisu z analizy pozyskanych danych. Użyj programu *exiftool* do sprawdzenia, czy odzyskane pliki fotograficzne posiadają metadane, sprawdź poprawność współrzędnych GPS. Opisz swoje spostrzeżenia.



Zadanie 3 – Recoverjpeg

Proszę o zainstalowanie programu recoverjpeg:



Wykorzystując nowy program (recoverjpeg), użyj go do odzyskania danych z fizycznego urządzenia */dev/sdbx*. Opisz efekt pozyskanych danych (wraz z metadanymi) w porównaniu do programu *foremost*.

Zadanie 4 – Scalpel

- Zainstaluj program *scalpel* (domyślnie zainstalowany w dystrybucji Kali Linux). Przejdź do pliku *scalpel*.conf:

```
┌──(kali㉿kali)-[/]
└─$ cd /etc/scalpel

┌──(kali㉿kali)-[/etc/scalpel]
└─$ ll
total 12
-rw-r--r-- 1 root root 8669 Apr 21  2020 scalpel.conf
```

- Edytuj plik konfiguracyjny (*scalpel.conf*) w taki sposób, aby odzwierciedlić rozszerzenia plików znajdujących się w naszym zainteresowaniu. Zmiany polegają na odznaczeniu # z poszczególnych typów rozszerzeń.

- Użyj programu *scalpel* z podpiętym plikiem konfiguracyjnym do odzyskania informacji z kopii nośnika *(.dd)*.

- Porównaj rezultaty z poprzednio używanymi programami.

Zadanie 5 – Bulk_Extractor

Zainstaluj program *bulk_extractor* (domyślnie zainstalowany w dystrybucji Kali Linux):

```
kali@kali: ~/Desktop/IMG
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/Desktop/IMG]
└─$ bulk_extractor -h
bulk_extractor version 1.6.0
Usage: bulk_extractor [options] imagefile
  runs bulk extractor and outputs to stdout a summary of what was found where

Required parameters:
   imagefile      - the file to extract
 or  -R filedir   - recurse through a directory of files
                    HAS SUPPORT FOR E01 FILES
                    HAS SUPPORT FOR AFF FILES
   -o outdir      - specifies output directory. Must not exist.
                    bulk_extractor creates this directory.
Options:
   -i             - INFO mode. Do a quick random sample and print a report.
   -b banner.txt- Add banner.txt contents to the top of every output file.
   -r alert_list.txt  - a file containing the alert list of features to alert
                        (can be a feature file or a list of globs)
                        (can be repeated.)
   -w stop_list.txt   - a file containing the stop list of features (white list
                        (can be a feature file or a list of globs)s
                        (can be repeated.)
   -F <rfile>     - Read a list of regular expressions from <rfile> to find
   -f <regex>     - find occurrences of <regex>; may be repeated.
```

- Wykorzystaj narzędzie do pozyskania danych z kopii nośnika (*.dd*).

- Przeanalizuj uzyskane wyniki z odzyskanych informacji.

Zadanie 6 – Podsumowanie odzyskiwania danych

Proszę o przeprowadzenie szczegółowego porównania uzyskanych rezultatów z odzyskiwania informacji z nośnika/kopii (.dd). Należy zamieścić w raporcie preferowane narzędzie wraz z uzasadnieniem oraz umieścić informacje o napotkanych trudnościach w trakcie tego laboratorium.

Zadanie 7 – Analiza rejestru systemu Windows

Pobierz z platformy UPEL pliki rejestru systemu Windows (NTUSER.DAT, SAM, SECURITY, SOFTWARE, SYSTEM, UsrClass.dat).

1. Przeanalizuj plik NTUSER.DAT i odpowiedz na pytania:
- Czy są jakiekolwiek ślady używania Adobe Acrobat?
- Jakie aplikacje są skojarzone z kluczem ApplicationAssociationToasts?
- Czy znaleziono dane o kompatybilności aplikacji w AppCompatFlags?
- Jakie są ostatnie czasy zapisu dla Applets?
- Czy istnieje klucz AppSpecific dla Microsoft IntelliPoint?
- Jakie pliki zostały ostatnio otwarte za pomocą iexplore.exe?
- Jakie są ustawienia środowiska użytkownika?
- Czy znaleziono informacje o Office Internet Server Cache?
- Czy istnieją jakiekolwiek ślady użycia WinRAR?
- Jakie strony internetowe zostały ostatnio wpisane przez użytkownika?
- Jakie są ostatnie czasy dostępu do wpisanych adresów URL?
- Czy są jakiekolwiek informacje o zainstalowanym oprogramowaniu Spotify?

2. Przeanalizuj plik SAM oraz podaj 10 najciekawszych informacji znajdujących się w tym pliku.

3. Przeanalizuj plik SECURITY oraz podaj 10 najciekawszych informacji znajdujących się w tym pliku.

4. Przeanalizuj plik SOFTWARE oraz podaj 10 najciekawszych informacji znajdujących się w tym pliku.

5. Przeanalizuj plik SYSTEM oraz podaj 10 najciekawszych informacji znajdujących się w tym pliku.

6. Przeanalizuj plik UsrClass.dat oraz podaj 10 najciekawszych informacji znajdujących się w tym pliku.

**Uwaga, nie wszystkie informacje mogą znajdować się wewnątrz załączonych plików.*

Rozwiązania zadań muszą zawierać zrzuty ekranów ze wszystkich wykonanych elementów oraz szczegółowy opis uzyskanych rezultatów.