# Informatyka śledcza

**Laboratorium nr 1**

## Spis treści



## Wstęp

Przygotowane zadania mają na celu zaznajomienie uczestników laboratorium z podstawowymi funkcjami oraz narzędziami wykorzystywanymi w informatyce śledczej. Pierwsze laboratorium skupiać się będzie na pozyskiwaniu i analizie danych z nośnika typu pendrive. W tym celu zostały udostępnione pliki pod nazwą USB_4GB_Kingston.E01 oraz LAB_1.img, które zawierają wiele informacji niezbędnych do rozwiązania niniejszego laboratorium. Ostatecznym etapem jest utworzenie przez studenta kopii własnego nośnika danych oraz poddania go analizie przy pomocy przedstawionych narzędzi.

**Wykorzystywane narzędzia w trakcie laboratorium:**

1. System Linux
2. *Md5sum* oraz *Sha1sum*
3. *Mmls*
4. *Fsstat*
5. *Fls*
6. *EwfTools* (*sudo apt install libewf-dev ewf-tools*)

**Zadanie 1 – Instalacja środowiska wirtualnego (Kali/SIFT lub innej dystrybucji Linux), oraz pobranie pliku z rozszerzeniem E01 (załącznik zostanie udostępniony w trakcie laboratorium).**

W trakcie laboratorium zostanie udostępniony plik z rozszerzeniem E01. Plik zawiera informacje, które są niezbędne do przeprowadzenia analizy śledczej. Jednakże, aby wyświetlić interesujące nas dane, potrzebne będzie utworzenie odpowiedniego środowiska wirtualnego. W tym celu należy pobrać i zainstalować program VirtualBox (https:// www.virtualbox.org/wiki/Downloads) lub równorzędny oraz pobrać obraz jednej z dystrybucji Linux (polecany Kali - https://www.kali.org).

agh.edu.pl

**Zadanie 2 – Analiza pobranego obrazu (plik .E01).**

Pobrany plik *USB_4GB_Kingston.E01* zawiera informacje o trzech partycjach, które należy wyświetlić przy pomocy dedykowanych programów. W pierwszej kolejności odpowiedz na pytanie:

1. Jaka jest wartość skrótu dla funkcji haszującej md5 i sha-1?

Proszę przy pomocy polecenia *mmls* o wyświetlenie i podanie odpowiedzi na pytania:

1. W jakim przedziale sektorów znajduje się niealokowana pamięć?
2. W której partycji znajdują się pliki systemowe?
3. Proszę o podanie początku i końca sektora należącego do partycja Win95?

Przy pomocy narzędzia *fsstat* proszę o wyświetlenie i odpowiedź na pytania:

1. Jaki system plików zaczyna się w sektorze 0000000128 analizowanego pliku?
2. Jaka jest wielkość sektora oraz klastra w badanym obszarze?

Narzędzie *fls* posiada funkcje umożliwiającą wyświetlanie informacji o plikach znajdujących się w partycji Win95.

1. Wypisz wszystkie pliki głównego katalogu USB_4GB_Kingston.E01.
2. Wypisz wszystkie plik znajdujące się w folderze „1”.

EwfTools jest darmowym narzędziem do tworzenia i analizy danych cyfrowych pomocnych w informatyce śledczej.

Przy użyciu funkcji znajdujących się w *EWFTools/ewfinfo* wyświetl informacje o pliku oraz odpowiedz na poniższe pytania.

1. Pod jaki numer sprawy podlega badany nośnik?
2. Jaka jest nazwa osoby tworzącej obraz dysku?
3. Kiedy plik został utworzony?
4. Numer seryjny fizycznego dysku oraz nazwa modelu?
5. Wskaż format plików?
6. Proszę o podanie metody kompresji pliku?
7. Jaka jest pełna wielkość badanego nośnika (w bajtach)?
8. Jaki poziom kompresji został wskazany przy tworzeniu pliku?

**Zadanie 3 – Analiza pobranego obrazu (LAB_1.img).**

1. Wczytaj za pomocą polecenia *mmls* i podaj liczbę sektorów *gpt_load_table*.
2. Proszę o podanie sektora startowego *gpt_load: 0.*
3. Ile niealokowanych sektorów znajduję się w obrazie? Podaj ich sektory startowe oraz końcowe.
4. Podaj ujawnione woluminy.
5. Wykorzystując polecenie *mmstat* wyświetl informacje tablicy partycji.
6. Przy wykorzystaniu narzędzia fsstat wyświetl informacje o woluminie „ntfs” oraz podaj „Volume Serial Number” oraz informacje o wersji („Version”).

**Zadanie 4 – Pozyskanie obrazu nośnika przy użyciu narzędzia ewfacquire.**

Przy wykorzystaniu dowolnego pendriva proszę o sporządzenie jego kopii binarnej przy pomocy narzędzia *ewfacquire* oraz wyświetlenie najistotniejszych informacji.

W tym celu sprawdź swój podłączony nośnik:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo fdisk -l
[sudo] password for kali:


Disk /dev/sda: 152 GiB, 163208757248 bytes, 318767104 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: 0x9cca7389

Device     Boot     Start       End   Sectors  Size Id Type
/dev/sda1  *         2048 316766207 316764160  151G 83 Linux
/dev/sda2       316768254 318765055   1996802  975M  5 Extended
/dev/sda5       316768256 318765055   1996800  975M 82 Linux swap / Solaris


Disk /dev/sdb: 3.62 GiB, 3881828352 bytes, 7581696 sectors
Disk model: USB DISK 2.0
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: 0x00000000

Device     Boot Start     End Sectors  Size Id Type
/dev/sdb1           1 7581695 7581695  3.6G  b W95 FAT32
```

Postępuj zgodnie z wymuszonymi krokami przez program.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo ewfacquire /dev/sdb
ewfacquire 20140807

Device information:
Bus type:    USB
Vendor:     Wilk
Model:     USB DISK 2.0
Serial:     0D7117891080

Storage media information:
Type:       Device
Media type:    Removable
Media size:    3.8 GB (3881828352 bytes)
Bytes per sector:   512

Acquiry parameters required, please provide the necessary input
Image path and filename without extension:
```

Sprawdź poprawność wykonanego obrazu:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo ewfverify 2022 USB 4GB 001.E01
ewfverify 20140807

Verify started at: Oct 04, 2022 20:48:35
This could take a while.

Status: at 39%.
        verified 1.4 GiB (1530003456 bytes) of total 3.6 GiB (3881828352 bytes).
        completion in 6 second(s) with 370 MiB/s (388182835 bytes/second).

Status: at 95%.
        verified 3.4 GiB (3715563520 bytes) of total 3.6 GiB (3881828352 bytes).
        completion in 0 second(s) with 462 MiB/s (485228544 bytes/second).

Verify completed at: Oct 04, 2022 20:48:43

Read: 3.6 GiB (3881828352 bytes) in 8 second(s) with 462 MiB/s (485228544 bytes/second).

MD5 hash stored in file:   fd1e436c26276d0731361b0b5f339053
MD5 hash calculated over data:   fd1e436c26276d0731361b0b5f339053

ewfverify: SUCCESS
```

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