# Informatyka śledcza

**Laboratorium nr 3**

**Spis treści**



## Wstęp

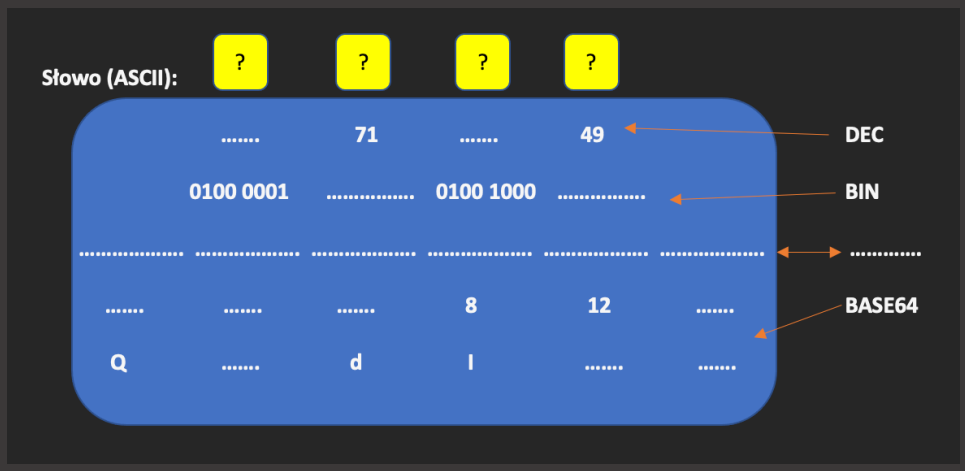
W trakcie tego laboratorium student zaznajomi się z kodowaniem ciągu bajtów za pomocą wygenerowanego ciągu znaków (kodowanie base64) oraz z narzędziami, które pomogą w analizie plików i systemów plików. Z uwagi na szeroki zakres analizy analityków zajmujących się informatyką śledczą wymagana jest niezbędna wiedza umożliwiająca analizę pojedynczych plików oraz ich zawartości. W ramach laboratorium studenci zaznajomią się z podstawowymi narzędziami umożliwiającymi jednostkową analizę ujawnionych „obiektów" systemowych. Utwórz raport z wykonanych zadań i umieść w nim zrzuty ekranu z poszczególnych wykonanych ćwiczeń wraz z opisem dokonanych obserwacji i rezultatów.

## Wykorzystywane narzędzia w trakcie laboratorium:

1. **Base64**
2. **File**
3. **Strings**
4. **GHex**
5. **Pdfinfo**
6. **Mkfs**
7. **Dumpe2fs**
8. **Fsck**

## Zadanie 1 – Base64 jako narzędzie do kodowania i dekodowania.

Korzystając ze zdobytej wiedzy proszę o rozwiązanie zadania:




Korzystając z systemu Linux proszę o utworzenie na pulpicie systemowym pliku o rozszerzeniu .txt oraz zamieszczeniu w nim kliku zdań przykładowego tekstu (używając polskich znaków).
Następnie przy użyciu narzędzia *base64* proszę o zakodowanie wcześniej utworzonego pliku tekstowego oraz rozkodowanie.
Dodatkowo przy użyciu narzędzia *file* sprawdź dane z utworzonego pliku i wskaż system kodowania.
Wykorzystaj narzędzie *strings* do wyświetlenia danych z utworzonego pliku i odpowiedz czy widoczne są różnice pomiędzy narzędziami. W przypadku widocznych różnic, proszę o ich interpretacje.

**Zadanie 2 – W zakładce pliki do przedmiotu Informatyka Śledcza znajduje się katalog File.zip, który zawiera przykładowe pliki o różnych rozszerzeniach.**
Proszę o rozpakowanie katalogu w systemie Linux oraz ustalenie zawartości wypakowanego archiwum zip przy pomocy narzędzia *file* (umożliwi wyświetlenie krótkiej informacji o pliku).
Wykorzystując program *pdfinfo* wyświetl informacje o plikach PDF i odpowiedz na pytania:

- Jaki jest tytuł dokumentów?
- Data wytworzenia pliku?
- Liczba stron?
- Wielkość stron?
- Czy plik zawiera java script?
- Kto jest autorem?
- Jakie oprogramowanie zostało użyte?

**Zadanie 3 – Właściwości narzędzia GHex**
W ramach ćwiczeń proszę o zainstalowanie narzędzia GHex oraz przeprowadzenie analizy pobranego archiwum oraz udzielenia odpowiedzi na pytania:

- Który wiersz zawiera informacje o pliku (rozszerzeniu)?
- Proszę o podanie sygnatury reprezentowanej nazwy pliku (plik.rar) w HEX-ie (GHex).

- Czy w ramach pliku archiwum jesteśmy w stanie odczytać jego zawartość? Jeśli tak to proszę ją wyświetlić, jeśli nie, to dlaczego?

## Zadanie 4 – Różnice pomiędzy systemami plików?

Wykonaj polecenie:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ dd if=/dev/zero of=sfile.raw count=100 bs=1M
100+0 records in
100+0 records out
104857600 bytes (105 MB, 100 MiB) copied, 0.0689166 s,
1.5 GB/s
```

Zweryfikuj zawartość nowo utworzonego pliku w GHexie i opisz, czym różni się od poprzednio badanego pliku?
Wykonaj polecenie *mkfs* i sprawdź, co zmieniło się w strukturze pliku (GHex)?:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ mkfs.fat sfile.raw
```

Następnie zmień w utworzonym pliku system plików na ext4 i podaj, gdzie zostały utworzone superbloki?

Dzięki zastosowaniu narzędzia *dumpe2fs* wyświetl i wymień najistotniejsze informacje takie jak:

- „magiczny numer" badanego obrazu
- numer UUID
- wielkość bloku
- liczbę wolnych bloków
- podaj checksum typ
- ile wolnych bloków zawiera grupa nr 12?

*fsck* posiada ciekawą zdolność do wyświetlenia informacji z badanego nośnika:

- podaj, ile bloków zostało zużytych w %?

## Zadanie 5 – Znaczenie superbloku w odzyskiwaniu danych.

W tym zadaniu należy wykorzystać przygotowany obraz .raw, który należy zamontować w systemie:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo losetup --find --show sfile.raw
[sudo] password for kali:
/dev/loop1
```

Mając przygotowane środowisko loop1 wykonaj polecenie do zamontowania pliku:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo mount /dev/loop1 /mnt/hgfs
```

Proszę o sprawdzenie uprawnień (ls -li) oraz odpowiedz na pytanie, do czego służy „plik" lost+found?
Posiadając wiedzę na temat numerów super bloków utwórz w zamontowanym obrazie nowy plik:

```
┌──(kali㉿kali)-[/mnt/hgfs]
└─$ sudo touch newitem
[sudo] password for kali:

┌──(kali㉿kali)-[/mnt/hgfs]
└─$ ls
lost+found  newitem
```

Wykorzystaj polecenie dd do wyczyszczenia danych i zastąpienia ich zerami:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo dd if=/dev/zero of=/dev/loop1 count=1 bs=1024 seek=1
1+0 records in
1+0 records out
1024 bytes (1.0 kB, 1.0 KiB) copied, 0.000163334 s, 6.3 MB/s
```

Sprawdź, czy w katalogu z danymi z obrazu nadal znajduje się utworzony nowy plik?

Odmontuj obraz oraz spróbuj zamontować go ponownie i odpowiedz na pytanie:

- Czy w trakcie odmontowania wystąpił błąd? Jeśli tak, to jakie było rozwiązanie?
- Czy w trakcie ponownego montowania pliku wystąpił problem? Jeśli tak, to dlaczego?

Przy użyciu narzędzia *fsck* odzyskaj wcześniej skasowane dane (wpisz w poleceniu numer superbloku).

```
┌──(kali㉿kali)-[/mnt/hgfs]
└─$ sudo fsck -f -y -b 8193 /dev/loop1 /mnt/hgfs
fsck from util-linux 2.37.2
e2fsck 1.46.4 (18-Aug-2021)
e2fsck 1.46.4 (18-Aug-2021)
fsck.ext2: Is a directory while trying to open /mnt/hgfs
```

Wyświetl rezultat z odzyskanych danych i umieść go w raporcie z ćwiczenia numer 3.

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