# Informatyka Śledcza - Laboratorium 3

Magdalena Ślusarczyk

## 1 Zadanie 1

#### 1.1 Zakodowane słowo

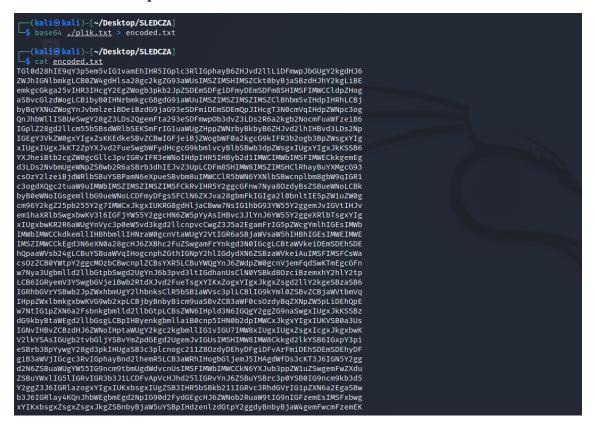
ASCII: AGH1

Decimal: 65 71 72 49

Binary: 01000001 01000111 01001000 00110001

Base64: QUdIMQ

#### 1.2 Kodowanie pliku txt



```
| Space | Spac
```

Komenda file wykrywa typ pliku, strings czyta plik i wypisuje napisy znalezione w pliku.

```
-(kali@kali)-[~/Desktop/SLEDCZA]
—$ file <u>./plik.txt</u>
./plik.txt: UTF-8 Unicode text
 —(kali⊗kali)-[~/Desktop/SLEDCZA]
└$ strings <u>./plik.txt</u>
Litwo! Ojczyzno moja! ty jeste jak zdrowie.
Ile ci trzeba ceni , ten tylko si dowie,
Kto ci straci . Dzi pi kno tw w ca ej ozdobie
Widz i opisuj , bo t skni po tobie.
Panno wi ta, co jasnej bronisz Cz stochowy
I w Ostrej wiecisz Bramie! Ty, co gr
d zamkowy
Nowogr
dzki ochraniasz z jego wiernym ludem!
Jak mnie dziecko do zdrowia powr
ci a cudem
```

# 2 Zadanie 2

### 2.1 Informacje o plikach

#### 2.2 Pdfinfo

```
(<mark>kali⊗kali</mark>)-[~/Desktop/SLEDCZA]
 -$ pdfinfo <u>./D19910350Lj.pdf</u>
                     Akt prawny
                    Władysław Baksza
Microsoft® Word 2013
Author:
Creator:
                     Microsoft® Word 2013
Producer:
                    Tue Oct 12 07:08:08 2021 EDT
Tue Oct 12 07:08:08 2021 EDT
CreationDate:
ModDate:
Tagged:
UserProperties: no
Suspects:
Form:
                    none
JavaScript:
Pages:
Encrypted:
Page size:
                     595.32 x 841.92 pts (A4)
Page rot:
                    2601654 bytes
File size:
Optimized:
   -(kali⊗kali)-[~/Desktop/SLEDCZA]
(kali⊗ kali)-[~/pesktop/sliss

$ pdfinfo _/D2020000211201.pdf
Title: Ustawa z dnia 28 października 2020 r. o zmianie niektórych ustaw w związku z przeciwdzi ałaniem sytuacjom kryzysowym związanym z wystąpieniem COVID-19
Author: RCL
                    Microsoft® Word 2010
Microsoft® Word 2010; modified using iText 2.1.7 by 1T3XT
Sat Nov 28 12:39:52 2020 EST
Producer:
CreationDate:
                     Sat Nov 28 12:40:01 2020 EST
Tagged:
UserProperties: no
                     no
Form:
                     AcroForm
JavaScript:
Pages:
Encrypted:
                     595.32 x 841.92 pts (A4)
Page size:
Page rot:
                     407654 bytes
Optimized:
                    1.5
PDF version:
```

#### 3 Zadanie 3

## 3.1 Informacje o plikach w archiwum w GHex

## 4 Zadanie 4

# 4.1 Różnice między systemami plików

Plik różni się od poprzedniego tym, że jest cały 'wyzerowany' w widoku hex. Po zmianie systemu plików na fat pojawia się informacja o tym, że dysk nie jest uruchamialny.

Po zmianie systemu na ext4 utworzono superbloki na blokach 8193, 24577, 40961, 57345, 73729

## 4.2 Dumpe2fs

Filesystem~UUID:~534c7275-9914-4aa5-833c-d971a1205252

Filesystem magic number: 0xEF53

Block size: 1024 Free blocks: 90319 Checksum type: crc32c Group 12: 4095 free blocks

#### 5 Zadanie 5

Lost+found przechowywuje odzyskane fragmenty z uszkodzonych plików partycji, z której zostało utworzone

```
(kali@ kali)-[~/Desktop/SLEDCZA/mnt/tmp]

$ lost+found newitem

(kali@ kali)-[~/Desktop/SLEDCZA/mnt/tmp]

$ sudo dd if=/dev/zero of=/dev/loop0 count=1 bs=1024 seek=1
1+0 records in
1+0 records out
1024 bytes (1.0 kB, 1.0 KiB) copied, 0.000483408 s, 2.1 MB/s

(kali@ kali)-[~/Desktop/SLEDCZA/mnt/tmp]

$ ls
```