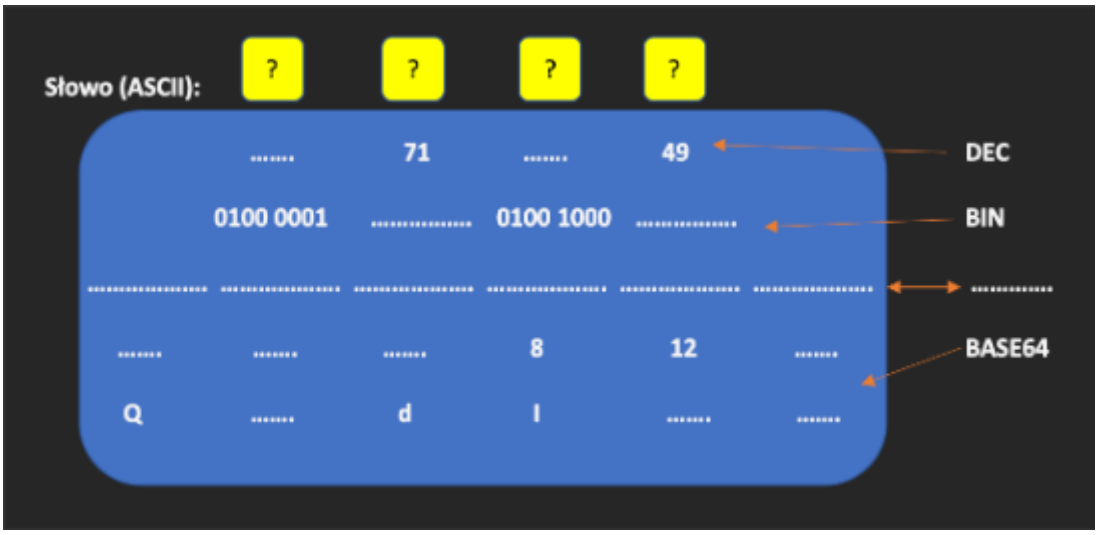

DEC **- 65 71 72 49**

BIN **- 0100 0001 0100 0111 0100 1000 0011 0001**

BASE64 **- QUdIMQ**

ASCII **- AGH1**

Przy użyciu tablic ASCII (polecenia ascii -b ascii –d) oraz polecenia base64 udało się rozszyfrować powyższe hasło

Przykładowy plik:

```
┌──(kali㉿kali)-[~/sledcza/lab_3]
└─$ cat text.txt
Lorem Ipsum Lorem Ipsum
bla vla
test test test

AGH 123
asdasdasd
```

Zakodowany plik:

```
┌──(kali㉿kali)-[~/sledcza/lab_3]
└─$ cat text.txt | base64 -w 10
TG9yZW0gSX
BzdW0gTG9y
ZW0gSXBzdW
0KYmxhIHZs
YSAKdGVzdC
B0ZXN0IHRl
c3QKCkFHSC
AxMjMKYXNk
YXNkYXNkCg
==
```

Odkodowany plik:

```
┌──(kali㉿kali)-[~/sledcza/lab_3]
└─$ echo "TG9yZW0gSX
BzdW0gTG9y
ZW0gSXBzdW
0KYmxhIHZs
YSAKdGVzdC
B0ZXN0IHRl
c3QKCkFHSC
AxMjMKYXNk
YXNkYXNkCg
==" | base64 -d
Lorem Ipsum Lorem Ipsum
bla vla
test test test

AGH 123
asdasdasd
```

```
┌──(kali㉿kali)-[~/sledcza/lab_3]
└─$ file text.txt
text.txt: ASCII text
```

Plik zakodowany jest w ASCII

```
┌──(kali㉿kali)-[~/sledcza/lab_3]
└─$ strings text.txt
Lorem Ipsum Lorem Ipsum
bla vla
test test test
AGH 123
asdasdasd
```

Polecenie strings wyszukuje znaków czytelnych dla ludzi, a polecenie cat wyświetla całą zawartość pliku, nieważne czy będą to znaki czytelne czy nie

Informacje o wypakowanych plikach:

```
┌──(kali㉿kali)-[~/sledcza/lab_3]
└─$ file File.zip
File.zip: Zip archive data, at least v2.0 to extract, compression method=deflate

┌──(kali㉿kali)-[~/sledcza/lab_3]
└─$ file D19910350Lj.pdf
D19910350Lj.pdf: PDF document, version 1.5, 351 pages

┌──(kali㉿kali)-[~/sledcza/lab_3]
└─$ file D2020000211201.pdf
D2020000211201.pdf: PDF document, version 1.5, 18 pages

┌──(kali㉿kali)-[~/sledcza/lab_3]
└─$ file Text
Text: ASCII text, with no line terminators
```

Informacje o plikach pdf:

```
┌──(kali㉿kali)-[~/sledcza/lab_3]
└─$ pdfinfo D19910350Lj.pdf
Title:          Akt prawny
Author:         Władysław Baksza
Creator:        Microsoft® Word 2013
Producer:       Microsoft® Word 2013
CreationDate:   Tue Oct 12 07:08:08 2021 EDT
ModDate:        Tue Oct 12 07:08:08 2021 EDT
Custom Metadata: no
Metadata Stream: no
Tagged:         yes
UserProperties: no
Suspects:       no
Form:           none
JavaScript:     no
Pages:          351
Encrypted:      no
Page size:      595.32 x 841.92 pts (A4)
Page rot:       0
File size:      2601654 bytes
Optimized:      no
PDF version:    1.5
```

```
┌──(kali㉿kali)-[~/sledcza/lab_3]
└─$ pdfinfo D2020000211201.pdf
Title:          Ustawa z dnia 28 października 2020 r. o zmianie niektórych ustaw w związku z przeciwdziałaniem syt
uacjom kryzysowym związanym z wystąpieniem COVID-19
Author:         RCL
Creator:        Microsoft® Word 2010
Producer:       Microsoft® Word 2010; modified using iText 2.1.7 by 1T3XT
CreationDate:   Sat Nov 28 12:39:52 2020 EST
ModDate:        Sat Nov 28 12:40:01 2020 EST
Custom Metadata: no
Metadata Stream: yes
Tagged:         yes
UserProperties: no
Suspects:       no
Form:           AcroForm
JavaScript:     no
Pages:          18
Encrypted:      no
Page size:      595.32 x 841.92 pts (A4)
Page rot:       0
File size:      407654 bytes
Optimized:      no
PDF version:    1.5
```

Dokument D19910350Lj.pdf:

Tytuł: Akt prawny
Data utworzenia pliku 12.10.2021
Liczba stron: 351
Wielkość stron: A4 (595.32 x 841.92 pts)
Plik nie zawiera JavaScript
Autor: Władysław Baksza
Użyte oprogramowanie: Microsoft Word 2013

Dokument D2020000211201.pdf:

Tytuł: Ustawa z dnia 28 października 2020 r. o zmianie niektórych ustaw w związku z przeciwdziałaniem sytuacjom kryzysowym związanym z wystąpieniem COVID-19

Data utworzenia pliku 28.11.2020
Liczba stron: 18
Wielkość stron: A4 (595.32 x 841.92 pts)
Plik nie zawiera JavaScript
Autor: RCL
Użyte oprogramowanie: Microsoft Word 2010

GHEX:

ghex File.zip

Informacje o rozszerzeniu zawiera pierwszy wiersz: Dla ZIP jest to 0x04034b50 PK.. (little endian), dla PDF jest to %PDF + wersja (Dla D2020000211201.pdf 25 50 44 46 2D 31 2E 35 czyli %PDF-1.5), dla RAR jest to Rar! (52 61 72 21), a plik txt nie zawiera informacji o rozszerzeniu, a jedynie zawartość pliku (można powiedzieć, że .txt jest umowne i nie jest wymagane)

W ramach plików archiwum, nie jesteśmy w stanie wyświetlić zawartości plików, możemy jedynie wyświetlić ich nazwy. Wyświetlenie zawartości jest niemożliwe, ponieważ archiwa zip i rar używają kompresji.

Nowo utworzony plik zawiera same 0
po zmianie systemu pliku dla tego pliku, dodał się header FAT16
Po zmianie na ext4, system plików FAT16 został usunięty
Superbloki zostały utowrzone na: 8193, 24577, 40961, 57345, 73729

```
┌──(kali㉿kali)-[~/sledcza/lab_3]
└─$ mkfs.fat sfile.raw
mkfs.fat 4.2 (2021-01-31)
```

```
┌──(kali㉿kali)-[~/sledcza/lab_3]
└─$ mkfs.ext4 sfile.raw
mke2fs 1.46.6-rc1 (12-Sep-2022)
sfile.raw contains a vfat file system
Proceed anyway? (y,N) y
Discarding device blocks: done
Creating filesystem with 102400 1k blocks and 25584 inodes
Filesystem UUID: 0607b418-5266-419d-92dc-be4c14047fae
Superblock backups stored on blocks:
        8193, 24577, 40961, 57345, 73729

Allocating group tables: done
Writing inode tables: done
Creating journal (4096 blocks): done
Writing superblocks and filesystem accounting information: done
```

Sfile.raw:

Magic Number: 0xEF53
Filesystem UUID: 0607b418-5266-419d-92dc-be4c14047fae
Block Size: 1024
Free blocks: 90319
Checksum type: crc32c

Grupa 12 zawiera 4095 wolnych bloków

```
Group 12: (Blocks 98305-102399) csum 0×b39d [INODE_UNINIT, ITABLE_ZEROED]
  Block bitmap at 271 (bg #0 + 270), csum 0×0189a663
  Inode bitmap at 284 (bg #0 + 283), csum 0×00000000
  Inode table at 6189-6680 (bg #0 + 6188)
  4095 free blocks, 1968 free inodes, 0 directories, 1968 unused inodes
  Free blocks: 98305-102399
  Free inodes: 23617-25584
```

```
┌──(kali㉿kali)-[~/sledcza/lab_3]
└─$ dumpe2fs sfile.raw
dumpe2fs 1.46.6-rc1 (12-Sep-2022)
Filesystem volume name:   <none>
Last mounted on:          <not available>
Filesystem UUID:          0607b418-5266-419d-92dc-be4c14047fae
Filesystem magic number:  0xEF53
Filesystem revision #:    1 (dynamic)
Filesystem features:      has_journal ext_attr resize_inode dir_i
rge_file huge_file dir_nlink extra_isize metadata_csum
Filesystem flags:         signed_directory_hash
Default mount options:    user_xattr acl
Filesystem state:         clean
Errors behavior:          Continue
Filesystem OS type:       Linux
Inode count:              25584
Block count:              102400
Reserved block count:     5120
Overhead clusters:        12067
Free blocks:              90319
Free inodes:              25573
First block:              1
Block size:               1024
Fragment size:            1024
Group descriptor size:    64
Reserved GDT blocks:      256
Blocks per group:         8192
Fragments per group:      8192
Inodes per group:         1968
Inode blocks per group:   492
Flex block group size:    16
Filesystem created:       Sun Dec  4 11:34:33 2022
Last mount time:          n/a
Last write time:          Sun Dec  4 11:34:33 2022
Mount count:              0
Maximum mount count:      -1
Last checked:             Sun Dec  4 11:34:33 2022
Check interval:           0 (<none>)
Lifetime writes:          279 kB
Reserved blocks uid:      0 (user root)
Reserved blocks gid:      0 (group root)
First inode:              11
Inode size:               256
Required extra isize:     32
Desired extra isize:      32
Journal inode:            8
Default directory hash:   half_md4
Directory Hash Seed:      d5d66d3f-247b-455f-9a16-5d7caa6c81b0
Journal backup:           inode blocks
Checksum type:            crc32c
Checksum:                 0xd5dfefaa
Journal features:         (none)
Total journal size:       4096k
```

Badanie nośnika:

Utworzenie z sfile.raw urządzenie loop:

```
┌──(kali㉿kali)-[~/sledcza/lab_3]
└─$ sudo losetup --find --show sfile.raw
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
/dev/loop0
```

```
┌──(kali㉿kali)-[~/sledcza/lab_3]
└─$ sudo fsck -n -v /dev/loop0
fsck from util-linux 2.38.1
e2fsck 1.46.6-rc1 (12-Sep-2022)
/dev/loop0: clean, 11/25584 files, 12081/102400 blocks
```

11,8% Bloków jest zajęte

Przy odmontowaniu urządzenia nie wyskoczył błąd
Przy zamontowaniu urządzenia wyskoczył błąd, ponieważ całe urządzenie zostało nadpisane zerami

```
┌──(root㉿kali)-[/mnt]
└─# fsck -f -y -b 8193 /dev/loop0 /mnt/sfile
fsck from util-linux 2.38.1
e2fsck 1.46.6-rc1 (12-Sep-2022)
e2fsck 1.46.6-rc1 (12-Sep-2022)
fsck.ext2: Is a directory while trying to open /mnt/sfile

The superblock could not be read or does not describe a valid ext2/ext3/ext4
filesystem.  If the device is valid and it really contains an ext2/ext3/ext4
filesystem (and not swap or ufs or something else), then the superblock
is corrupt, and you might try running e2fsck with an alternate superblock:
    e2fsck -b 8193 <device>
 or
    e2fsck -b 32768 <device>

Superblock needs_recovery flag is clear, but journal has data.
Recovery flag not set in backup superblock, so running journal anyway.
/dev/loop0: recovering journal
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
Block bitmap differences:  +(8193--8450) +(24577--24834) +(40961--41218) +(57345--57602) +(73729--73986)
Fix? yes

Free inodes count wrong for group #0 (1957, counted=1956).
Fix? yes

Free inodes count wrong (25573, counted=25572).
Fix? yes

Padding at end of inode bitmap is not set. Fix? yes


/dev/loop0: ***** FILE SYSTEM WAS MODIFIED *****
/dev/loop0: 12/25584 files (0.0% non-contiguous), 12081/102400 blocks
```

Dane zostały odzyskane