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

```
┌──(kali㉿kali)-[~/Desktop/SLEDCZA]
└─$ base64 ./plik.txt > encoded.txt

┌──(kali㉿kali)-[~/Desktop/SLEDCZA]
└─$ cat encoded.txt
TGl0d28hIE9qY3p5em5vIG1vamEhIHR5IGplc3RlIGphayB6ZHJvd2llLiDFmwpJbGUgY2kgdHJ6
ZWJhIGNlbmkgLCB0ZW4gdHlsa28gc2kgZG93aWUsIMSZIMSHIMSZCkt0byBjaSBzdHJhY2kgLiBE
emkgcGkga25vIHR3IHcgY2EgZWogb3pkb2JpZSDEmSDFgiDFmyDEmSDFm8SHIMSFIMWCCldpZHog
aSBvcGlzdWogLCBibyB0IHNrbmkgcG8gdG9iaWUuIMSZIMSZIMSZIMSZClBhbm5vIHdpIHRhLCBj
byBqYXNuZWogYnJvbmlzeiBDeiBzdG9jaG93eSDFmiDEmSDEmQpJIHcgT3N0cmVqIHdpZWNpc3og
QnJhbWllISBUeSwgY28gZ3LDs2QgemFta293eSDFmwpOb3dvZ3LDs2R6a2kgb2NocmFuaWFzeiB6
IGplZ28gd2llcm55bSBsdWRlbSEKSmFrIG1uaWUgZHppZWNrbyBkbyB6ZHJvd2lhIHBvd3LDs2Np
IGEgY3VkZW0gxYIgxZsKKEdkeSBvZCBwIGFjeiBjZWogbWF0a2kgcG9kIFR3b2ogb3BpZWsgxYIg
xIUgxIUgxJkKT2ZpYXJvd2FueSwgbWFydHcgcG9kbmlvcyBlbSBwb3dpZWsgxIUgxYIgxJkKSSB6
YXJheiBtb2cgZW0gcGllc3pvIGRvIFR3eWNoIHdpIHR5IHByb2d1IMWCIMWbIMSFIMWECkkgemEg
d3LDs2NvbmUgeWNpZSBwb2R6aSBrb3dhIEJvZ3UpLCDFm8SHIMW8IMSZIMSHClRhayBuYXMgcG93
csOzY2lzeiBjdWRlbSBuYSBPamN6eXpueSBvbm8uIMWCClR5bWN6YXNlbSBwcnplbm8gbW9qIGR1
c3ogdXQgc2tuaW9uIMWbIMSZIMSZIMSZIMSFCkRvIHR5Y2ggcGFnw7Nya8OzdyBsZSBueWNoLCBk
byB0eWNoIGsgemllbG9ueWNoLCDFmyDFgsSFClN6ZXJva28gbmFkIGIga2l0bnltIE5pZW1uZW0g
cm96Y2kgZ25pb255Y2g7IMWCxJkgxIUKRG8gdHljaCBww7NsIG1hbG93YW55Y2ggemJvIGVtIHJv
em1haXRlbSwgxbwKV3l6IGFjYW55Y2ggcHN6ZW5pYyAsIHBvc3JlYnJ6YW55Y2ggeXRlbTsgxYIg
xIUgxbwKR2R6aWUgYnVyc3p0eW5vd3kgd2llcnpvcCwgZ3J5a2EgamFrIG5pZWcgYmlhIGEsIMWb
IMWbIMWCCkdkemllIHBhbmllIHNraW0gcnVtaWUgY2VtIGR6aSBjaWVsaW5hIHBhIGEsIMWEIMWE
IMSZIMWCCkEgd3N6eXN0a28gcHJ6ZXBhc2FuZSwgamFrYnkgd3N0IGcgLCBtaWVkeiDEmSDEhSDE
hQpaaWVsb24gLCBuYSBuaWVqIHogcnphZGthIGNpY2hlIGdydXN6ZSBzaWVkeiAuIMSFIMSFCsWa
csOzZCB0YWtpY2ggcMOzbCBwcnplZCBsYXR5LCBuYWQgYnJ6ZWdpZW0gcnVjemFqdSwKTmEgcGFn
w7Nya3Ugbmlld2llbGtpbSwgd2UgYnJ6b3pvd3ltIGdhanUsClN0YSBkd8OzciBzemxhY2hlY2tp
LCB6IGRyemV3YSwgbGVjeiBwb2RtdXJvd2FueTsgxYIKxZogxYIgxJkgxZsgd2llY2kgeSBzaSB6
IGRhbGVrYSBwb2JpZWxhbmUgY2lhbnksClR5bSBiaWVsc3plLCBlIG9kYml0ZSBvZCBjaWVtbmVq
IHppZWxlbmkgxbwKVG9wb2xpLCBjbyBnbyBicm9uaSBvZCB3aWF0csOzdyBqZXNpZW5pLiDEhQpE
w7NtIG1pZXN6a2Fsbnkgbmlld2llbGtpLCBsZWN6IHpld3N6IGQgY2ggZG9naSwgxIUgxJkKSSBz
dG9kbyBtaWEgd2llbGsgLCBpIHByenkgbmllaiB0cnp5IHN0b2dpIMWCxJkgxYIgxIUKVSB0a3Us
IGNvIHBvZCBzdHJ6ZWNoIHptaWUgY2kgc2kgbmllIG1vIGU7IMW8xIUgxIUgxZsgxIcgxJkgxbwK
V2lkYSAsIGUgb2tvbGljYSBvYmZpdGEgd2UgemJvIGUsIMSHIMW8Ckkgd2lkYSB6IGxpY3pi
eSBrb3BpYywgY28gd3pkIHUgaSB3c3plcnogc211Z8OzdyDEhyDFgiDFvArFmiDEhSDEmSDEhyDF
giB3aWVjIGcgc3RvIGphayBnd2lhemR5LCB3aWRhIHogbGljemJ5IHAgdWfDs3cKT3J6IGN5Y2gg
d2N6ZSBuaWUgYW55IG9ncm9tbmUgdWdvcnUsIMSFIMWbIMWCCkN6YXJub3ppZW1uZSwgemFwZXdu
ZSBuYWxlIG5lIGRvIGR3b3J1LCDFvApVcHJhd25lIGRvYnJ6ZSBuYSBrc3p0YSB0IG9ncm9kb3d5
Y2ggZ3J6IGRlazogxYIgxIUKxbsgxIUgZSB3IHR5bSBkb211IGRvc3RhdGVrIG1pZXN6a2EgaSBw
b3J6IGRlay4KQnJhbWEgbmEgd2NpIG90d2FydGEgcHJ6ZWNob2RuaW9tIG9nIGFzemEsIMSFxbwg
xYIKxbsgxZsgxZsgxJkgZSBnbyBjaW5uYSBpIHdzenlzdGtpY2ggdyBnbyBjaW4gemFwcmFzemEK
```

```
└─$ base64 -d encoded.txt > decoded.txt

┌──(kali㉿kali)-[~/Desktop/SLEDCZA]
└─$ cat decoded.txt
Litwo! Ojczyzno moja! ty jeste jak zdrowie. ś
Ile ci trzeba ceni , ten tylko si dowie, ę ć ę
Kto ci straci . Dzi pi kno tw w ca ej ozdobie ę ł ś ę ść ą ł
Widz i opisuj , bo t skni po tobie. ę ę ę ę
Panno wi ta, co jasnej bronisz Cz stochowy Ś ę ę
I w Ostrej wiecisz Bramie! Ty, co gród zamkowy ś
Nowogródzki ochraniasz z jego wiernym ludem!
Jak mnie dziecko do zdrowia powróci a cudem ł ś
(Gdy od p acz cej matki pod Twoj opiek ł ą ą ę
Ofiarowany, martw podnios em powiek ą ł ę
I zaraz mog em pieszo do Twych wi ty progu ł ś ą ń
I za wrócone ycie podzi kowa Bogu), ść ź ę ć
Tak nas powrócisz cudem na Ojczyzny ono. ł
Tymczasem przeno moj dusz ut sknion ś ę ę ą
Do tych pagórków le nych, do tych k zielonych, ś łą
Szeroko nad b kitnym Niemnem rozci gnionych; łę ą
Do tych pól malowanych zbo em rozmaitem, ż
Wyz acanych pszenic , posrebrzanych ytem; ł ą ż
Gdzie bursztynowy wierzop, gryka jak nieg bia a, ś ś ł
Gdzie panie skim rumie cem dzi cielina pa a, ń ń ę ł
A wszystko przepasane, jakby wst g , miedz ę ą ą
Zielon , na niej z rzadka ciche grusze siedz . ą ą
Śród takich pól przed laty, nad brzegiem ruczaju,
Na pagórku niewielkim, we brzozowym gaju,
Sta dwór szlachecki, z drzewa, lecz podmurowany; ł
Ś ł ę ś wieci y si z daleka pobielane ciany,
Tym bielsze, e odbite od ciemnej zieleni ż
Topoli, co go broni od wiatrów jesieni. ą
Dóm mieszkalny niewielki, lecz zewsz d ch dogi, ą ę
I stodo mia wielk , i przy niej trzy stogi łę ł ą
U tku, co pod strzech zmie ci si nie mo e; żą ą ś ć ę ż
Wida , e okolica obfita we zbo e, ć ż ż
I wida z liczby kopic, co wzd u i wszerz smugów ć ł ż
Ś ą ę ć ł wiec g sto jak gwiazdy, wida z liczby p ugów
Orz cych wcze nie any ogromne ugoru, ą ś ł
Czarnoziemne, zapewne nale ne do dworu, ż
Uprawne dobrze na kszta t ogrodowych grz dek: ł ą
Ż ą e w tym domu dostatek mieszka i porz dek.
Brama na wci otwarta przechodniom og asza, ąż ł
Ż ś ś ę e go cinna i wszystkich w go cin zaprasza
```

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

```
┌──(kali㉿kali)-[~/Desktop/SLEDCZA]
└─$ file ./plik.txt
./plik.txt: UTF-8 Unicode text

┌──(kali㉿kali)-[~/Desktop/SLEDCZA]
└─$ strings  ./plik.txt
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

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

┌──(kali㉿kali)-[~/Desktop/SLEDCZA]
└─$ file ./D19910350Lj.pdf
./D19910350Lj.pdf: PDF document, version 1.5

┌──(kali㉿kali)-[~/Desktop/SLEDCZA]
└─$ file ./D20200000211201.pdf
./D20200000211201.pdf: PDF document, version 1.5
```

2.2 Pdfinfo

```
┌──(kali㉿kali)-[~/Desktop/SLEDCZA]
└─$ pdfinfo ./D19910350Lj.pdf                                                1 ✕ 1 ⚙
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
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)-[~/Desktop/SLEDCZA]
└─$ pdfinfo ./D20200000211201.pdf                                                1 ⚙
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
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
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
```

3 Zadanie 3

3.1 Informacje o plikach w archiwum w GHex

```
0028BA4B  00 00 00 00 00 00 00 00 00 A4 81 00 00 00 00 44 31 39 39 31 30 33 35 30 4C 6A 2E 70 64  ...............D19910350Lj.pd
0028BA68  66 55 54 05 00 03 C1 15 81 61 75 78 0B 00 01 04 E8 03 00 00 04 E8 03 00 00 50 4B 01 02  fUT......aux.............PK..
0028BA85  1E 03 14 00 00 00 08 00 2E 5D 62 53 68 01 F0 16 D5 4B 05 00 66 38 06 00 12 00 18 00 00  .........]bSh....K..f8.......
0028BAA2  00 00 00 00 00 00 00 A4 81 C9 6D 23 00 44 32 30 32 30 30 30 30 32 31 31 32 30 31 2E 70  ..........m#.D2020000211201.p
0028BABF  64 66 55 54 05 00 03 D7 15 81 61 75 78 0B 00 01 04 E8 03 00 00 04 E8 03 00 00 50 4B 01  dfUT......aux.............PK.
0028BADC  02 1E 03 0A 00 00 00 00 00 88 5E 62 53 32 D1 4D 78 04 00 00 00 04 00 00 00 04 00 18 00  ..........^bS2.Mx............
0028BAF9  00 00 00 00 01 00 00 00 A4 81 EA B9 28 00 54 65 78 74 55 54 05 00 03 5F 18 81 61 75 78  ............(.TextUT..._..aux
0028BB16  0B 00 01 04 E8 03 00 00 04 E8 03 00 00 50 4B 05 06 00 00 00 00 03 00 03 00 F7 00 00 00  .............PK..............
0028BB33  2C BA 28 00 00 00                                                                       ,.(...
```

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