


<p>POLITECHNIKA WROCŁAWSKA</p>  <p>Wydział Informatyki i Telekomunikacji</p>	<p>Wydział: Informatyki i Telekomunikacji Kierunek: Cyberbezpieczeństwo Rok Akademicki: 2024/2025 Rok studiów, semestr: 2, 4 Grupa: 1 Termin: pon., 7:30</p>
<p align="center">CBESI0053G Informatyka śledcza – Laboratorium 2</p>	
<p>Prowadzący: mgr inż. Adrian Florek</p>	<p>Autor: 1. Gerard Błaszczuk</p>
<p>Data wykonania ćwiczenia: 10.03.2025</p>	
<p>Data oddania sprawozdania: 16.03.2025</p>	

1. Cel ćwiczenia

Analiza metadanych: ekstrakcja, podejście, metodyki.

2. Odszyfrowanie instrukcji laboratoryjnej

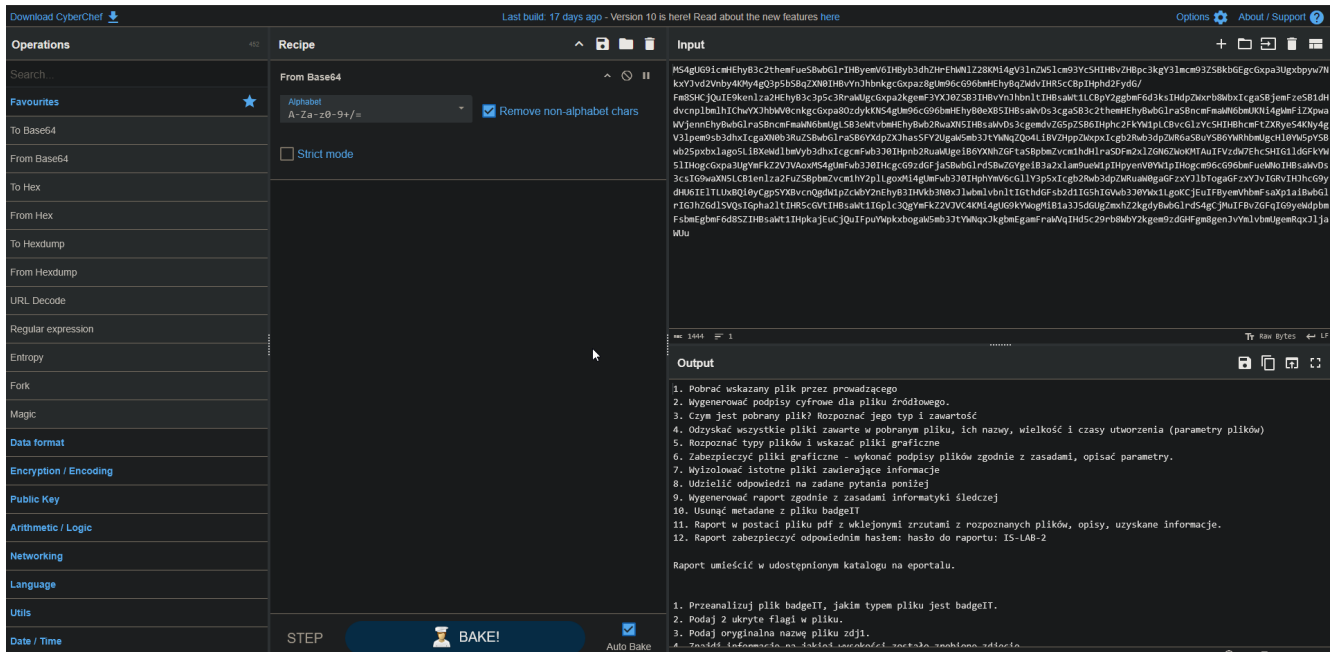
Zadania do sprawozdania:

MS4gUG9icmHEhyB3c2themFueSBwbGlrIHByemV6IHByb3dhZHrEhWNIZ28KMi4gV3I
nZW5lcm93YcSHIHBvZHBpc3kgY3Imcm93ZSBkbGEgcGxpa3Ugxbpyw7NkxYJvd2Vnb
y4KMy4gQ3p5bSBqZXN0IHBvYnJhbGkgcGxpaz8gUm96cG96bmHEhyBqZWdvIHR5cC
BpIHphd2FydG/Fm8SHCjQuIE9kenlza2HEhyB3c3p5c3RraWUgcGxpa2kgemF3YXJ0ZS
B3IHBvYnJhbGltIHBsaWt1LCBpY2ggbmF6d3ksIHdpZWxrb8WbXlcgaSBjemFzeSB1dH
dvcnplbmhlChwYXJhbWV0cnkgcGxpa8OzdykKNS4gUm96cG96bmHEhyB0eXB5IHBs
aWVds3cgaSB3c2themHEhyBwbGlrSBncmFmaWN6bmUKNi4gWmFiZXpwaWVjennE
hyBwbGlrSBncmFmaWN6bmUgLSB3eWtvbmHEhyBwb2RwaXN5IHBsaWVds3cgemd
vZG5pZSB6IHphc2FkYW1pLCBvcGlzYcSHIHBhcmFtZXRYeS4KNy4gV3lpem9sb3dhxlc
gaXN0b3RuZSBwbGlrSB6YXdpZXJhasSFY2UgaW5mb3JtYWNqZQo4LiBVZHppZWxp
xlcbg2Rwb3dpZWR6aSBuYSB6YWRhbmUgcHI0YW5pYSBwb25pxbXlago5LiBXeWdlb
mVyb3dhxlcgcmlFw3J0IHpn2RuaWUgeiB6YXNhZGFtaSBpbmZvcmlhdHlraSDFm2xl
ZGN6ZW0KMTAuIFVzdW7EhcSHIG1ldGFkYW5lIHogcGxpa3UgYmFkZ2VJVAoxMS4gU
mFwb3J0IHcgcG9zdGFjaSBwbGlrSBwZGYgeiB3a2xlam9ueW1pIHpyenV0YW1pIHog
cm96cG96bmFueWN0IHBsaWVds3cslG9waXN5LCB1enlza2FuZSBpbmZvcmlhY2pLg
oxMi4gUmFwb3J0IHphYmV6cGlIY3p5xlcbg2Rwb3dpZWRuaW0gaGFzxYJlbTogaGFzx
YJvIGRvIHJhcG9ydHU6IEITLUXBQi0yCgpSYXBvcnQgdW1pZcWbY2nEhyB3IHVkb3N0
xJlwbmlvbmltIGthdGFsb2d1IG5hIGVwb3J0YWx1LgoKCjEuIFByemVhbmFsaXp1aiBwb
GlrIGJhZGdlSVQslGpha2ltIHR5cGVtIHBsaWt1IGplc3QgYmFkZ2VJVC4KMi4gUG9kYW
ogMiB1a3J5dGUgZmxhZ2kgdyBwbGlrSB4gCjMuIFBvZGFqIG9yeWdpbmFsbmEgdmF6
d8SZIHBsaWt1IHpkajEuCjQuIFpuYWpkxbogaW5mb3JtYWNqxJkgbmEgamFraWVqlHd
5c29rb8WbY2kgem9zdGHFgm8genJvYmVbmUgemRqxJlJaWUu

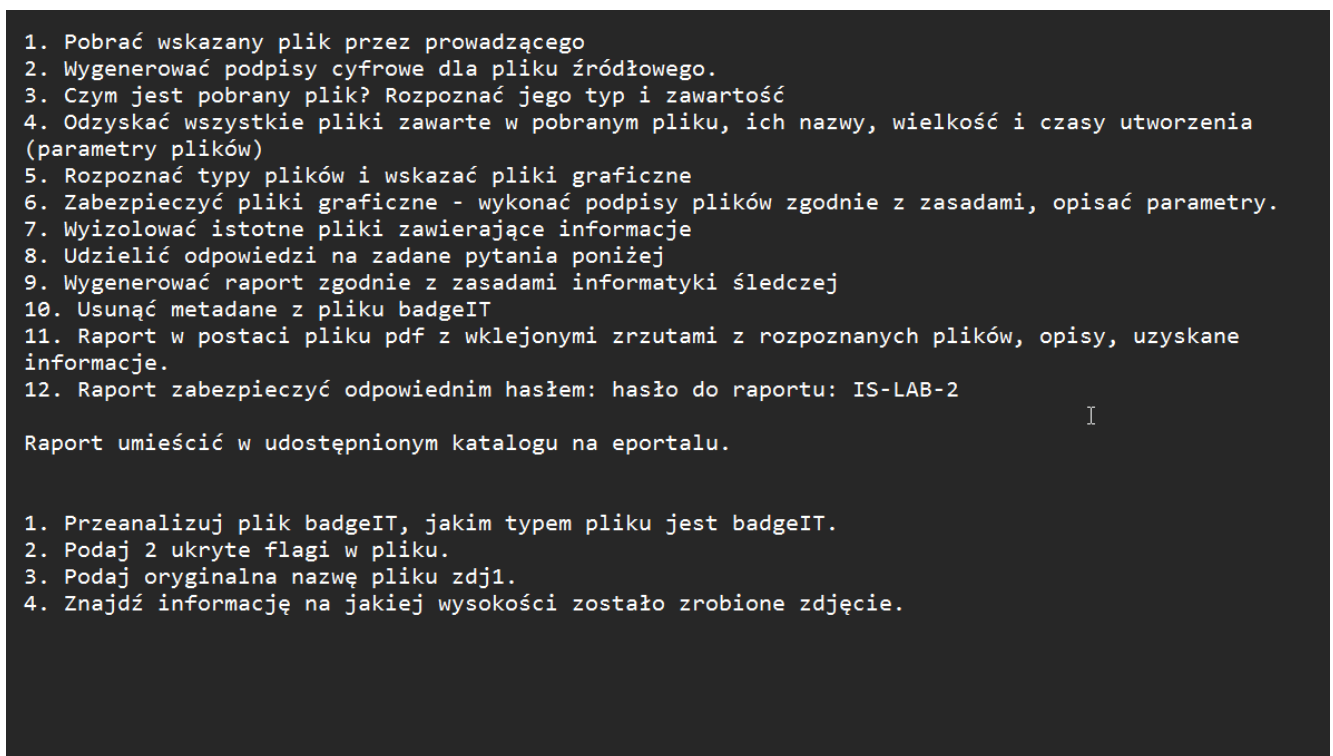
Hasło do pliku:

vasbeznglxnfyrqpmn

Rysunek 1: instrukcja laboratoryjna



Rysunek 2: odszyfrowanie zawartości w programie "CyberChef"



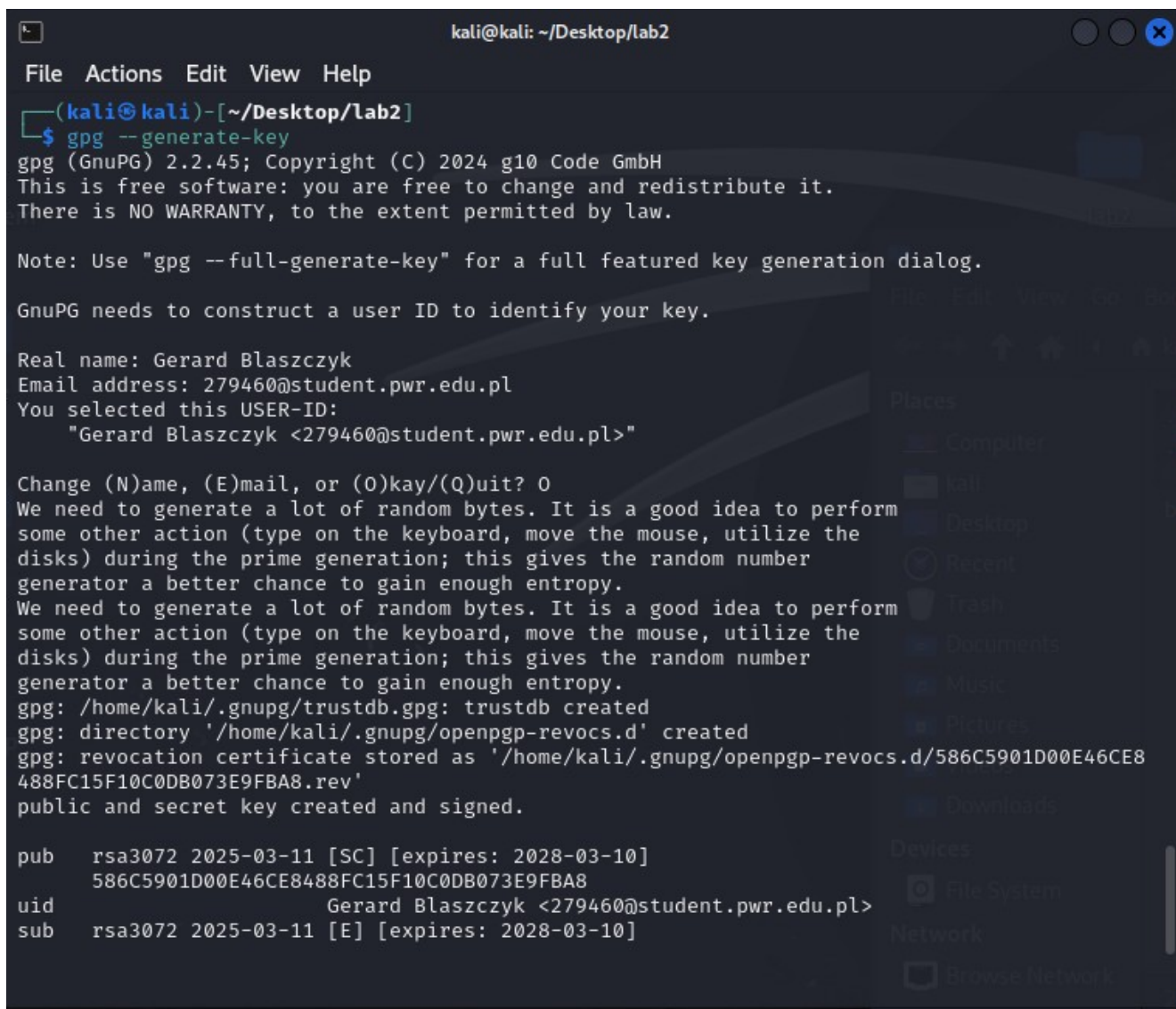
Rysunek 3: odszyfrowana treść instrukcji

Komentarz: instrukcja została zakodowana w Base64.

3. Realizacja odszyfrowanej instrukcji

Zadanie 1. Pobrać plik.

Zadanie 2. Wygenerować podpisy.



```
kali@kali: ~/Desktop/lab2
File Actions Edit View Help
(kali@kali)-[~/Desktop/lab2]
$ gpg --generate-key
gpg (GnuPG) 2.2.45; Copyright (C) 2024 g10 Code GmbH
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

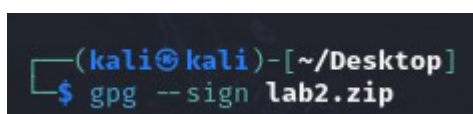
GnuPG needs to construct a user ID to identify your key.

Real name: Gerard Blaszczyk
Email address: 279460@student.pwr.edu.pl
You selected this USER-ID:
  "Gerard Blaszczyk <279460@student.pwr.edu.pl>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? O
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: /home/kali/.gnupg/trustdb.gpg: trustdb created
gpg: directory '/home/kali/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/kali/.gnupg/openpgp-revocs.d/586C5901D00E46CE8
488FC15F10C0DB073E9FBA8.rev'
public and secret key created and signed.

pub  rsa3072 2025-03-11 [SC] [expires: 2028-03-10]
     586C5901D00E46CE8488FC15F10C0DB073E9FBA8
uid                               Gerard Blaszczyk <279460@student.pwr.edu.pl>
sub  rsa3072 2025-03-11 [E] [expires: 2028-03-10]
```

Rysunek 4: generowanie klucza za pomocą programu GPG



```
(kali@kali)-[~/Desktop]
$ gpg --sign lab2.zip
```

Rysunek 5: podpisanie pobranego pliku

Zadanie 3. Czym jest pobrany plik?

Pobrany plik jest archiwum .zip. Potwierdza to sygnatura pliku.

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Tekst zdekodowany
00000000	50	4B	03	04	14	00	01	00	08	00	9C	05	66	5A	92	0C	PK.....ś.fZ'.
00000010	67	9C	22	C0	68	00	8A	35	6B	00	07	00	00	00	62	61	gś"Řh.Š5k.....ba
00000020	64	67	65	49	54	95	F2	3F	7B	41	C0	5A	30	F8	80	52	dgeIT•ň?(ARZ0řER
00000030	AF	20	E3	E7	EC	10	28	12	EA	A4	D0	08	8C	C9	75	F3	Ž āçě. (.ęĐ.ŠÉuó
00000040	44	49	8D	30	C6	01	C7	DD	16	6E	D0	D8	FA	C4	A4	72	DIŤ0Ć.ÇÝ.nĐŘúÄxr
00000050	CB	C9	EF	BB	67	15	6C	E9	6D	24	46	19	1C	4F	36	F6	ĚÉd»g.lém\$F..O6ó
00000060	0C	C0	6A	13	79	26	52	A7	3C	32	24	72	DF	8D	BB	99	.Řj.y&R\$<2\$řBŤ»™
00000070	BE	E4	6C	E1	4D	7E	4C	CB	C5	E7	35	C3	A7	77	59	9D	IäláM~LĚĹç5Ă\$wYt
00000080	ED	45	0D	FD	A6	77	98	44	38	46	4C	4C	C4	B2	B6	D5	íE.ý!w.D8FLLÄ,qŮ
00000090	A3	22	21	6E	A8	64	72	F1	52	26	C6	80	87	28	DE	42	L"!n`drńR&Ć€+(ŤB
000000A0	54	F9	D9	1E	FB	2E	1F	43	6F	30	A2	54	9D	D6	AE	9C	TúŮ.ű..Co0`TtÖ@s
000000B0	2A	E9	52	C2	3E	3A	BF	C9	4B	B5	3D	0E	9C	A1	57	0B	*éRÂ>:žÉKµ=.ś`W.
000000C0	AF	73	0E	CF	60	8B	0A	10	3B	03	14	F2	EE	F3	94	04	Žs.Ď`<...;..ňíó".
000000D0	B2	C8	6A	C1	47	C8	B4	27	7E	5E	54	4F	5C	44	52	CB	„ČjÁGČ`'^~TO\DRĚ

Rysunek 6: sygnatura pliku lab2.zip w programie HxD

Zadanie 4. Odzyskać wszystkie pliki zawarte w pobranym pliku, ich nazwy, wielkość i czasy utworzenia (parametry plików)

Archiwum lab2.zip jest zabezpieczone hasłem. Hasło do pliku podane w instrukcji nie działa – jest zaszyfrowane szyfrem Cezara z przesunięciem = 13. Po odkodowaniu otrzymujemy działające hasło: „informatykasledcza”.

Przesunięcie:

13

Tekst:

vasbeznglxnfyrqpmn|

Szyfr Cezara:

informatykasledcza

Rysunek 7: odkodowanie hasła do pliku narzędziem dostępnym na stronie skalkuluj.pl

Po rozszyfrowaniu i wypakowaniu widoczne są dwa pliki:

```
(kali㉿kali)-[~/Desktop/Lab2]
$ ls
badgeIT  zdj1.JPG
```

Rysunek 8: pliki wypakowane z archiwum

Czasy utworzenia i wielkość można uzyskać narzędziem exiftool:

```
(kali@kali)-[~/Desktop/lab2]
$ exiftool badgeIT
ExifTool Version Number      : 13.00
File Name                    : badgeIT
Directory                    : .
File Size                    : 7.0 MB
File Modification Date/Time   : 2025:03:11 05:48:33-04:00
File Access Date/Time        : 2025:03:11 05:48:40-04:00
File Inode Change Date/Time   : 2025:03:11 05:48:33-04:00
```

Rysunek 9: parametry pliku badgeIT

```
(kali@kali)-[~/Desktop/lab2]
$ exiftool zdj1.JPG
ExifTool Version Number      : 13.00
File Name                    : zdj1.JPG
Directory                    : .
File Size                    : 4.1 MB
File Modification Date/Time   : 2025:03:11 05:48:33-04:00
File Access Date/Time        : 2025:03:11 05:48:40-04:00
File Inode Change Date/Time   : 2025:03:11 05:48:33-04:00
```

Rysunek 10: parametry pliku zdj1.JPG

Zadanie 5. Rozpoznać typy plików i wskazać pliki graficzne.

```
kali@kali: ~/Desktop/lab2
File Actions Edit View Help
(kali@kali)-[~/Desktop/lab2]
$ binwalk zdj1.JPG badgeIT

Scan Time:      2025-03-11 09:23:53
Target File:    /home/kali/Desktop/lab2/zdj1.JPG
MD5 Checksum:   f71b24ed38633c341c04863170aaa884
Signatures:     436

DECIMAL      HEXADECIMAL    DESCRIPTION
-----
0            0x0           JPEG image data, EXIF standard
12           0xC           TIFF image data, little-endian offset of first image directory: 8
39851        0x9BAB        TIFF image data, little-endian offset of first image directory: 8

Scan Time:      2025-03-11 09:23:55
Target File:    /home/kali/Desktop/lab2/badgeIT
MD5 Checksum:   7b8c8d02a45eaf74b3ee5e1f964e815c
Signatures:     436

DECIMAL      HEXADECIMAL    DESCRIPTION
-----
0            0x0           JPEG image data, EXIF standard
12           0xC           TIFF image data, big-endian, offset of first image directory: 8
7025861      0x6B34C5       Zip archive data, at least v1.0 to extract, compressed size: 31, uncompressed size: 31, name: text.txt
7026036      0x6B3574       End of Zip archive, footer length: 22

(kali@kali)-[~/Desktop/lab2]
$
```

Rysunek 11: wynik badania plików programem binwalk

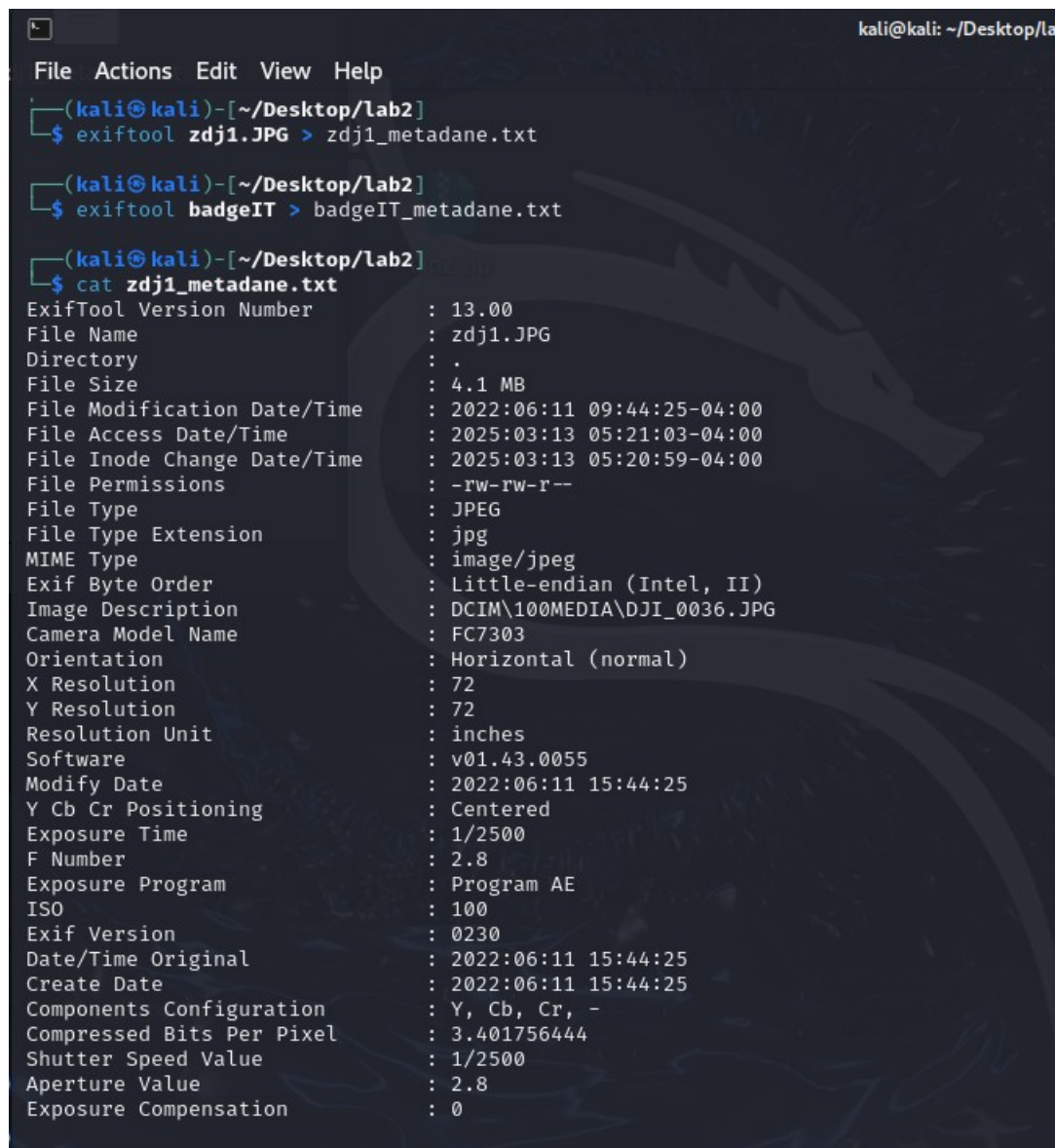
Program Binwalk pokazuje, że oba pliki są plikami graficznymi typu .jpg. Dodatkowo, w pliku badgeIT jest ukryte archiwum .zip, a także plik .txt.

Zadanie 6. Wyizolować istotne pliki zawierające informacje.

-----w tym momencie następuje aktualizacja pliku archiwum na nowsze, zgodnie z informacją podaną na platformie Teams-----

-----plik został ponownie podpisany-----

Metadane plików można pozyskać programem exiftool a następnie zapisać do pliku.



```
kali@kali: ~/Desktop/lab2
File Actions Edit View Help
(kali@kali)-[~/Desktop/lab2]
$ exiftool zdj1.JPG > zdj1_metadane.txt

(kali@kali)-[~/Desktop/lab2]
$ exiftool badgeIT > badgeIT_metadane.txt

(kali@kali)-[~/Desktop/lab2]
$ cat zdj1_metadane.txt
ExifTool Version Number      : 13.00
File Name                    : zdj1.JPG
Directory                    : .
File Size                     : 4.1 MB
File Modification Date/Time   : 2022:06:11 09:44:25-04:00
File Access Date/Time        : 2025:03:13 05:21:03-04:00
File Inode Change Date/Time   : 2025:03:13 05:20:59-04:00
File Permissions              : -rw-rw-r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
Exif Byte Order               : Little-endian (Intel, II)
Image Description             : DCIM\100MEDIA\DJI_0036.JPG
Camera Model Name             : FC7303
Orientation                   : Horizontal (normal)
X Resolution                  : 72
Y Resolution                  : 72
Resolution Unit               : inches
Software                      : v01.43.0055
Modify Date                   : 2022:06:11 15:44:25
Y Cb Cr Positioning          : Centered
Exposure Time                 : 1/2500
F Number                      : 2.8
Exposure Program              : Program AE
ISO                           : 100
Exif Version                  : 0230
Date/Time Original            : 2022:06:11 15:44:25
Create Date                   : 2022:06:11 15:44:25
Components Configuration     : Y, Cb, Cr, -
Compressed Bits Per Pixel     : 3.401756444
Shutter Speed Value           : 1/2500
Aperture Value                : 2.8
Exposure Compensation         : 0
```

Rysunek 12: ekstrakcja informacji za pomocą exiftool i zapis do pliku

Zadanie 8. Udzielić odpowiedzi na zadane pytania poniżej:

1. Przeanalizuj plik badgeIT, jakim typem pliku jest badgeIT.
Odpowiedz: udzielona w zadaniu 5.
2. Podaj 2 ukryte flagi w pliku.
Ekstrakcja plików za pomocą narzędzia binwalk:

```
File Actions Edit View Help
(kali@kali)-[~/Desktop/lab2]
$ binwalk -e -D '*.*' badgeIT
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, EXIF standard
12	0xC	TIFF image data, big-endian, offset of first image directory: 8
7025861	0x6B34C5	Zip archive data, at least v1.0 to extract, compressed size: 31, uncompressed size: 31, name: text.txt
7026036	0x6B3574	End of Zip archive, footer length: 22

```
(kali@kali)-[~/Desktop/lab2]
$
```

Rysunek 13: ekstrakcja ukrytych plików z badgeIT

Komentarz: opcja -D '*.*' użyta, ponieważ bez niej program dokonywał ekstrakcji tylko pliku .zip.

```
File Actions Edit View Help
(kali@kali)-[~/Desktop/lab2/_badgeIT.extracted]
$ cat text.txt
Informatyka sledcza jest fajna
(kali@kali)-[~/Desktop/lab2/_badgeIT.extracted]
$
```

Rysunek 14: flaga 1

```
Keywords : 3d, background, Firewall, Encryption, Anti-virus, Cybersecurity, Hacker, Data, protection, Authentication, Network, security, Intrusion, detection, Malware, Vulnerability, Threat, Internet, Passwords, breach, Phishing, Spam, Spoofing, Ransomware, DDoS, attack, render
URL : Trust, but verify... and then hex dump :)
```

Rysunek 15: flaga 2 (URL)

3. Podaj oryginalną nazwę pliku zdj1.

```
1 ExifTool Version Number      : 13.00
2 File Name                    : zdj1.JPG
3 Directory                    : .
4 File Size                    : 4.1 MB
5 File Modification Date/Time   : 2022:06:11 09:44:25-04:00
6 File Access Date/Time        : 2025:03:13 05:21:03-04:00
7 File Inode Change Date/Time   : 2025:03:13 05:20:59-04:00
8 File Permissions              : -rw-rw-r--
9 File Type                    : JPEG
10 File Type Extension          : jpg
11 MIME Type                    : image/jpeg
12 Exif Byte Order               : Little-endian (Intel, II)
13 Image Description             : DCIM\100MEDIA\DCI_0036.JPG ←
14 Camera Model Name             : FC7303
15 Orientation                   : Horizontal (normal)
16 X Resolution                  : 72
17 Y Resolution                  : 72
18 Resolution Unit               : inches
19 Software                      : v01.43.0055
20 Modify Date                   : 2022:06:11 15:44:25
21 Y Cb Cr Positioning          : Centered
22 Exposure Time                 : 1/2500
```

Rysunek 16: oryginalna nazwa pliku zdj1

4. Znajdź informację na jakiej wysokości zostało zrobione zdjęcie.

```
106 Image ID List      : (Binary data 66 bytes, use -b option to extract)
107 Total Frames       : 1
108 Image Width        : 4000
109 Image Height       : 2250
110 Encoding Process   : Baseline DCT, Huffman coding
111 Bits Per Sample     : 8
112 Color Components    : 3
113 Y Cb Cr Sub Sampling : YCbCr4:2:2 (2 1)
114 Aperture           : 2.8
115 Image Size         : 4000x2250
116 Megapixels         : 9.0
117 Scale Factor To 35 mm Equivalent: 5.3
118 Shutter Speed      : 1/2500
119 Thumbnail Image     : (Binary data 13219 bytes, use -b option to extract)
120 GPS Altitude        : 147.9 m Above Sea Level|
121 GPS Latitude        : 51 deg 6' 23.25" N
122 GPS Longitude       : 17 deg 7' 12.34" E
123 Preview Image      : (Binary data 277176 bytes, use -b option to extract)
124 Circle Of Confusion : 0.006 mm
125 Field Of View       : 73.7 deg
126 Focal Length        : 4.5 mm (35 mm equivalent: 24.0 mm)
127 GPS Position        : 51 deg 6' 23.25" N, 17 deg 7' 12.34" E
```

Rysunek 17: wysokość na której wykonano zdjęcie

Zadanie 9. Wygenerować raport zgodnie z zasadami informatyki śledczej.

...

Zadanie 10. Usunąć metadane z pliku badgeIT.

```
File Actions Edit View Help
(kali@kali)-[~/Desktop/lab2]
$ exiftool -all= badgeIT
1 image files updated

(kali@kali)-[~/Desktop/lab2]
$ exiftool badgeIT
ExifTool Version Number      : 13.00
File Name                    : badgeIT
Directory                    : .
File Size                    : 7.0 MB
File Modification Date/Time   : 2025:03:13 06:32:56-04:00
File Access Date/Time        : 2025:03:13 06:32:57-04:00
File Inode Change Date/Time   : 2025:03:13 06:32:56-04:00
File Permissions              : -rw-rw-r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
DCT Encode Version           : 100
APP14 Flags 0                : [14]
APP14 Flags 1                : (none)
Color Transform               : YCbCr
Image Width                  : 4096
Image Height                 : 4096
Encoding Process              : Baseline DCT, Huffman coding
Bits Per Sample              : 8
Color Components              : 3
Y Cb Cr Sub Sampling         : YCbCr4:4:4 (1 1)
Image Size                   : 4096x4096
Megapixels                   : 16.8

(kali@kali)-[~/Desktop/lab2]
$
```

Rysunek 18: usuwanie metadanych z pliku badgeIT

Zadanie 11. Raport w postaci pliku pdf z wklejonymi zrzutami z rozpoznanych plików, opisy, uzyskane informacje.

...

Zadanie 12. Raport zabezpieczyć odpowiednim hasłem: hasło do raportu: IS-LAB-2

...

4. Wnioski

Analiza plików odpowiednimi narzędziami pozwala na odkrycie dodatkowych informacji o plikach, a także na znajdowanie plików ukrytych.