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

1. Cel ćwiczenia

Analiza metadanych: ekstrakcja, podejście, metodyki.

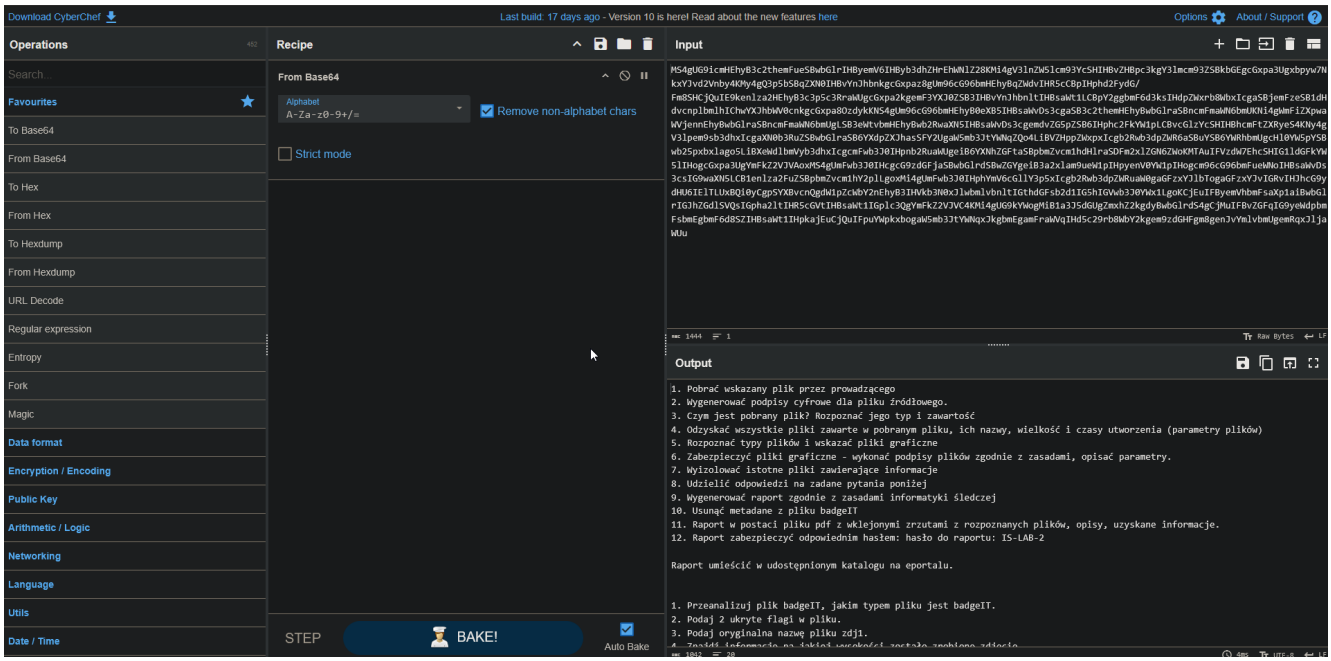
2. Odszyfrowanie instrukcji laboratoryjnej

Zadania do sprawozdania:

MS4gUG9icmHEhyB3c2themFueSBwbGlrIHByemV6IHByb3dhZHrEhWNlZ28KMi4gV3l
nZW5lcm93YcSHIHBvZHBpc3kgY3lmcm93ZSBkbGEgcGxpa3Ugxbpyw7NkxYJvd2Vnb
y4KMy4gQ3p5bSBqZXN0IHBvYnJhbnkgcGxpaz8gUm96cG96bmHEhyBqZWdvIHR5cC
BpIHphd2FydG/Fm8SHCjQuIE9kenIza2HEhyB3c3p5c3RraWUgcGxpa2kgemF3YXJ0ZS
B3IHBvYnJhbnItIHBsaWt1LCBpY2ggbmF6d3ksIHdpZWxrb8WbxlcgaSBjemFzeSB1dH
dvcnplbmlhICHwYXJhbWV0cnkgcGxpa8OzdykKNS4gUm96cG96bmHEhyB0eXB5IHBs
aWvDs3cgaSB3c2themHEhyBwbGlraSBncmFmaWN6bmUKNi4gWmFiZXpwaWVjennE
hyBwbGlraSBncmFmaWN6bmUgLSB3eWtvbmHEhyBwb2RwaXN5IHBsaWvDs3cgemd
vZG5pZSB6IHphc2FkYW1pLCBvcGlzYcSHIHBhcmFtZXRyeS4KNy4gV3lpem9sb3dhxlc
gaXN0b3RuZSBwbGlraSB6YXdpZXJhasSFY2UgaW5mb3JtYWNqZQo4LiBVZHppZWxp
xlcgb2Rwb3dpZWR6aSBuYSB6YWRhbmUgcHl0YW5pYSBwb25pxbxlago5LiBXeWdlb
mVyb3dhxlcgcmFwb3J0IHpnb2RuaWUgeiB6YXNhZGFtaSBpbmZvcm1hdHlraSDFm2xl
ZGN6ZWoKMTAuIFVzdW7EhcSHIG1ldGFkYW5lIHogcGxpa3UgYmFkZ2VJVAoxMS4gU
mFwb3J0IHcgcG9zdGFjaSBwbGlrdSBwZGYgeiB3a2xlam9ueW1pIHpyenV0YW1pIHog
cm96cG96bmFueWNolHBsaWvDs3csIG9waXN5LCB1enlza2FuZSBpbmZvcm1hY2plLg
oxMi4gUmFwb3J0IHphYmV6cGlIY3p5xlcgb2Rwb3dpZWRuaW0gaGFzxYJlbTogaGFzx
YJvIGRvIHJhcG9ydHU6IElTLUxBQi0yCgpSYXBvcnQgdW1pZcWbY2nEhyB3IHVkb3N0
xJlwbmlvbnltIGthdGFsb2d1IG5hIGVwb3J0YWx1LgoKCjEuIFByemVhbmFsaXp1aiBwb
GlrIGJhZGdlSVQsIGpha2ltIHR5cGVtIHBsaWt1IGplc3QgYmFkZ2VJVC4KMi4gUG9kYW
ogMiB1a3J5dGUgZmxhZ2kgdyBwbGlrdS4gCjMuIFBvZGFqIG9yeWdpbmFsbmEgbmF6
d8SZlHBsaWt1IHpkajEuCjQuIFpuYWpkxbogaW5mb3JtYWNqxJkgbmEgamFraWVqIHd
5c29rb8WbY2kgem9zdGHFgm8genJvYmlvbmUgemRqxJljaWUu

Hasło do pliku:
vasbezngIxnfyrqpmn

Rysunek 1: instrukcja laboratoryjna



Rysunek 2: odszyfrowanie zawartości w programie "CyberChef"

```
1. Pobrać wskazany plik przez prowadzącego
2. Wygenerować podpisy cyfrowe dla pliku źródłowego.
3. Czym jest pobrany plik? Rozpoznać jego typ i zawartość
4. Odzyskać wszystkie pliki zawarte w pobranym pliku, ich nazwy, wielkość i czasy utworzenia
(parametry plików)
5. Rozpoznać typy plików i wskazać pliki graficzne
6. Zabezpieczyć pliki graficzne - wykonać podpisy plików zgodnie z zasadami, opisać parametry.
7. Wyizolować istotne pliki zawierające informacje
8. Udzielić odpowiedzi na zadane pytania poniżej
9. Wygenerować raport zgodnie z zasadami informatyki śledczej
10. Usunąć metadane z pliku badgeIT
11. Raport w postaci pliku pdf z wklejonymi zrzutami z rozpoznanych plików, opisy, uzyskane
informacje.
12. Raport zabezpieczyć odpowiednim hasłem: hasło do raportu: IS-LAB-2

Raport umieścić w udostępnionym katalogu na eportalu.


1. Przeanalizuj plik badgeIT, jakim typem pliku jest badgeIT.
2. Podaj 2 ukryte flagi w pliku.
3. Podaj oryginalna nazwę pliku zdj1.
4. Znajdź informację na jakiej wysokości zostało zrobione zdjęcie.
```

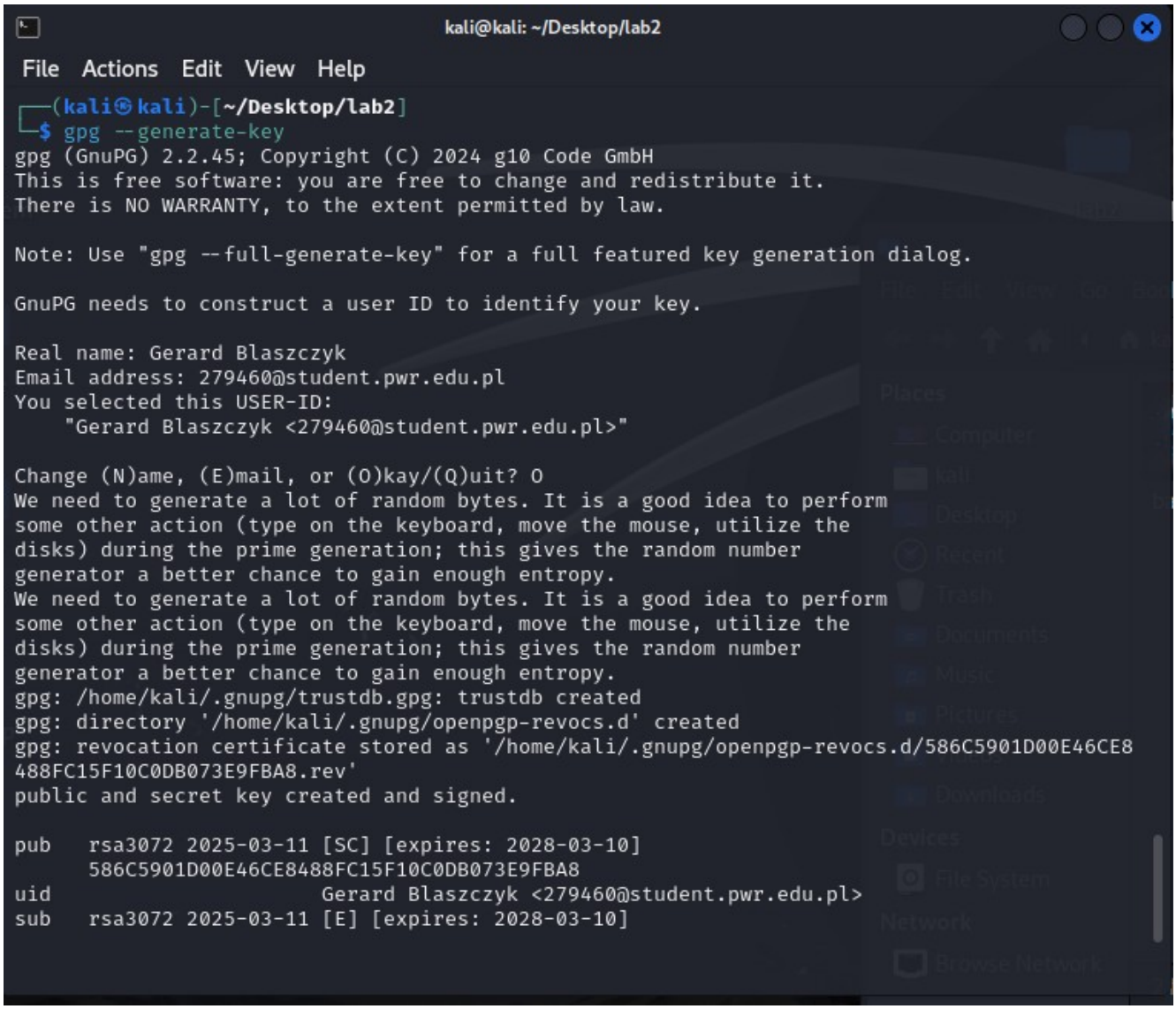
Rysunek 3: odszyfrowana treść instrukcji

Komentarz: instrukcja została zakodowana w Base64.

3. Realizacja odszyfrowanej instrukcji

Zadanie 1. Pobrać plik.

Zadanie 2. Wygenerować podpisy.

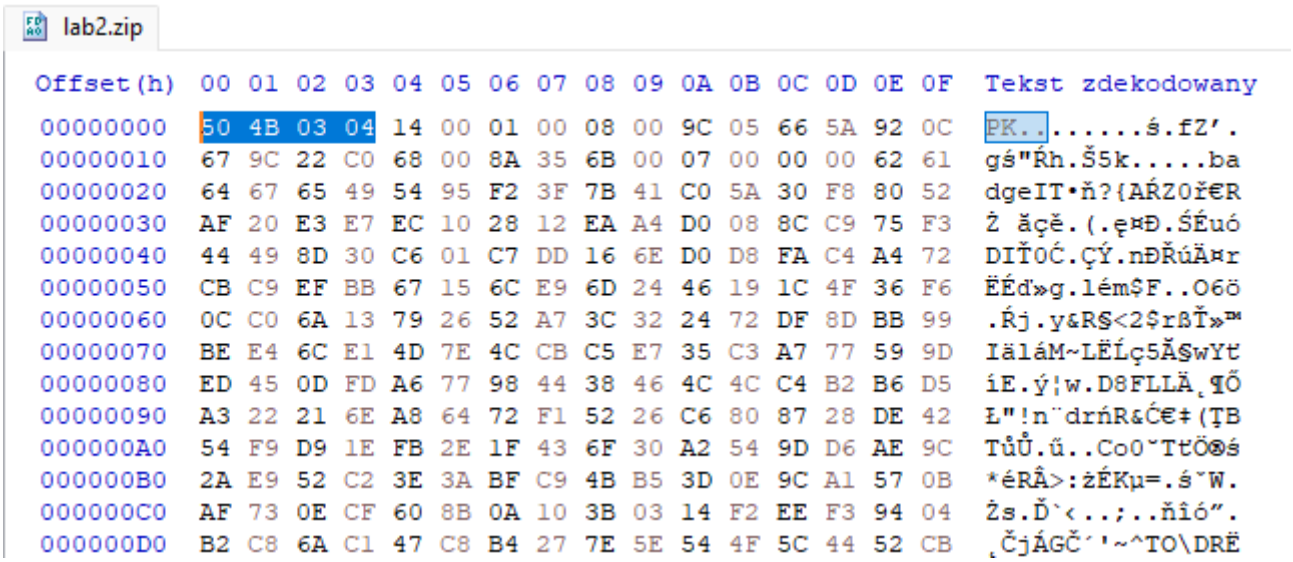


Rysunek 4: generowanie klucza za pomocą programu GPG

Rysunek 5: podpisanie pobranego pliku

Zadanie 3. Czym jest pobrany plik?

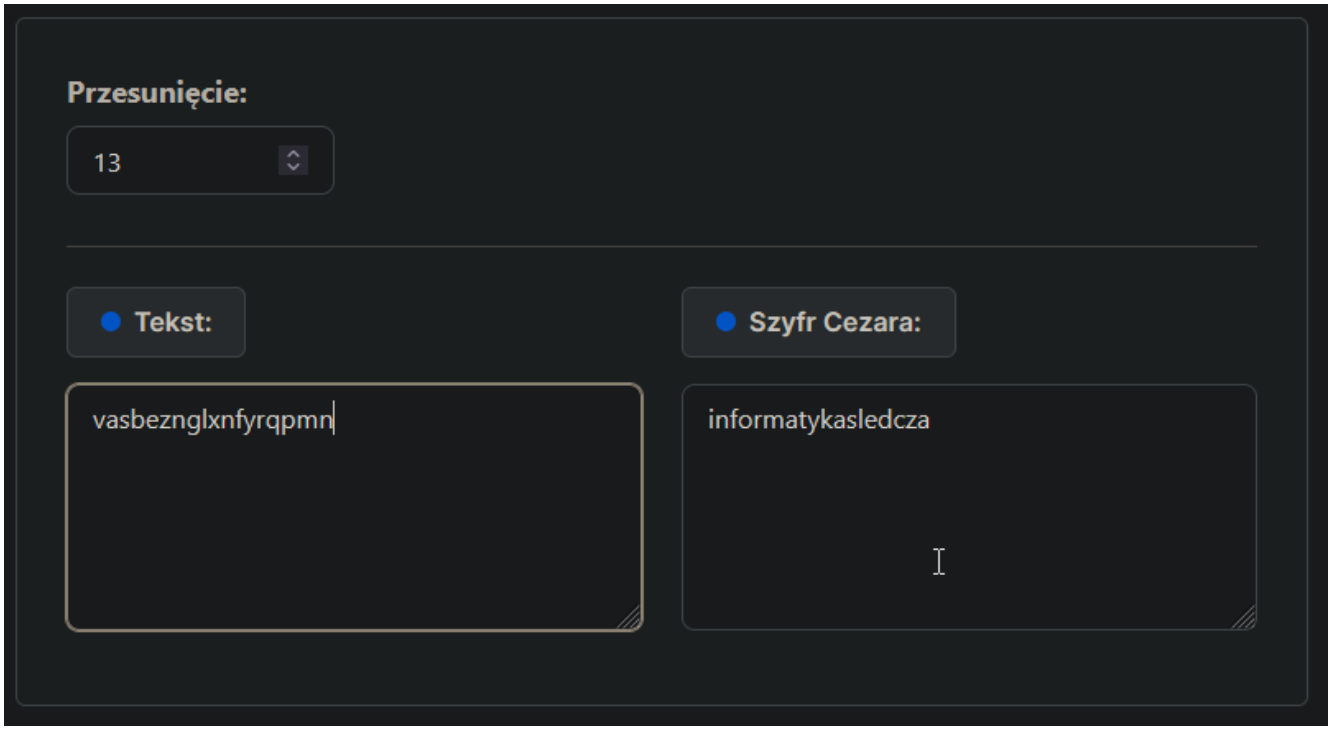
Pobrany plik jest archiwum .zip. Potwierdza to sygnatura pliku.



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 intrukcji nie działa – jest zaszyfrowane szyfrem Cezara z przesunięciem = 13. Po odkodowaniu otrzymujemy działające hasło: „informatykasledcza”.

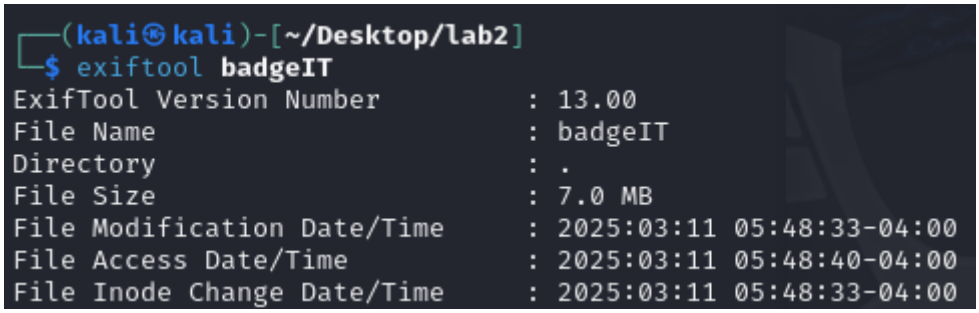


Rysunek 7: odkodowanie hasła do pliku narzędziem dostępnym na stronie skalkuluj.pl

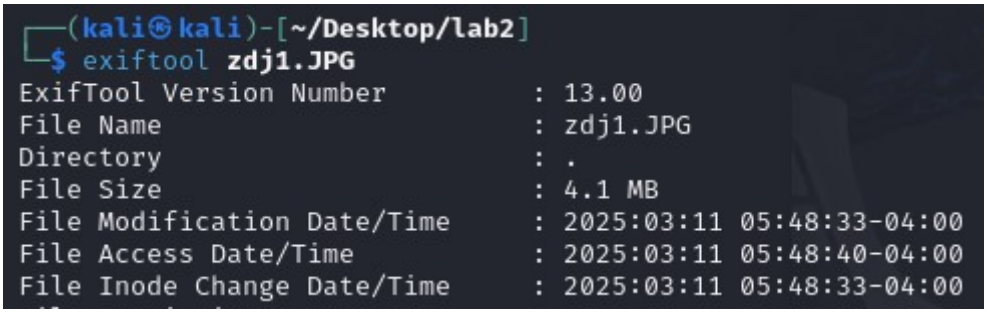
Po rozszyfrowaniu i wypakowaniu widoczne są dwa pliki:

Rysunek 8: pliki wypakowane z archiwum

Czasy utworzenia i wielkość można uzyskać narzędziem exiftool:

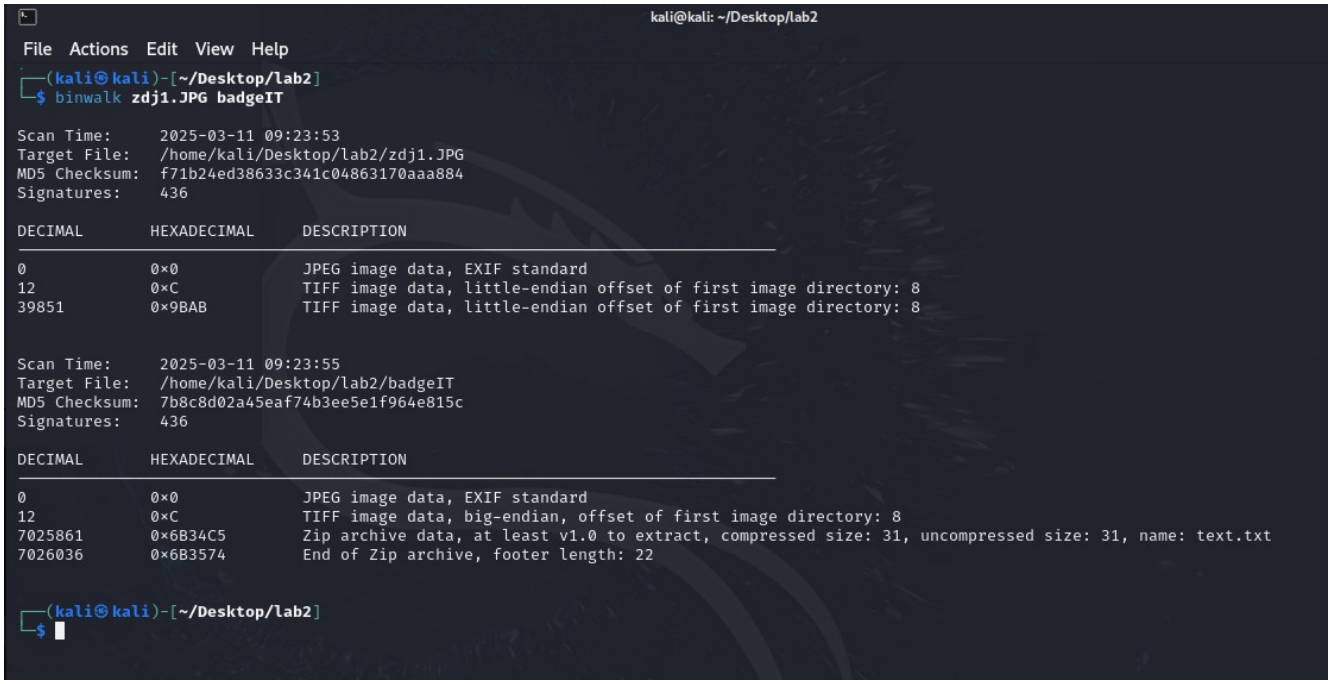


Rysunek 9: parametry pliku badgeIT



Rysunek 10: parametry pliku zdj1.JPG

Zadanie 5. Rozpoznać typy plików i wskazać pliki graficzne.



Rysunek 11: wynik badania plików programem binwalk

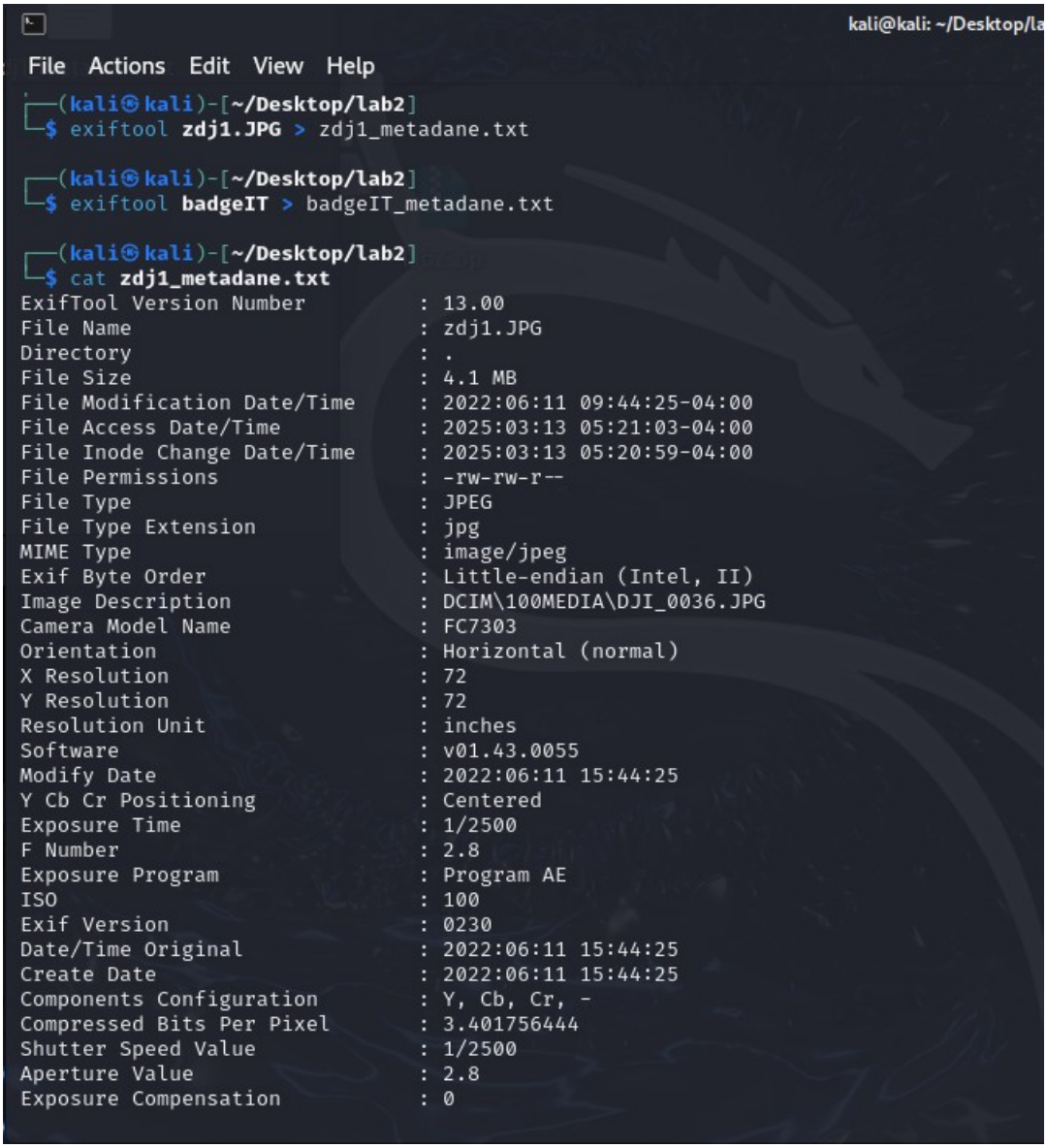
Program Binwalk pokazuje, że oba pliki są plikami graficznymi typu .jpg. Dodatkowo, w pliku badgeIT jest ukryte archiwum .zip, a także plik .txt.

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 pozystać programem exiftool a następnie zapisać do pliku.



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

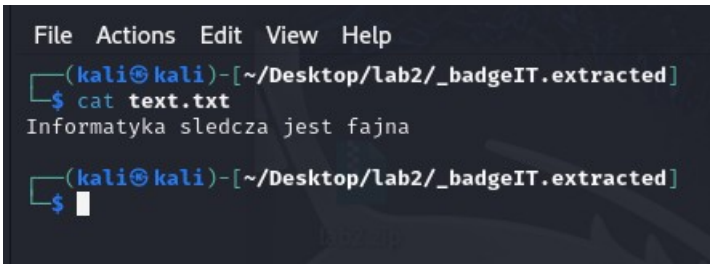
Zadanie 8. Udzielić odpowiedzi na zadane pytania poniżej:

1. Przeanalizuj plik badgeIT, jakim typem pliku jest badgeIT.
   Odpowiedz: udzielona w zadaniu 5.

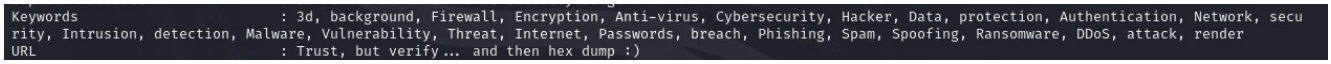
2. Podaj 2 ukryte flagi w pliku.
   Ekstrakcja plików za pomocą narzędzia binwalk:

Rysunek 13: ekstrakcja uktytych plików z badgeIT

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

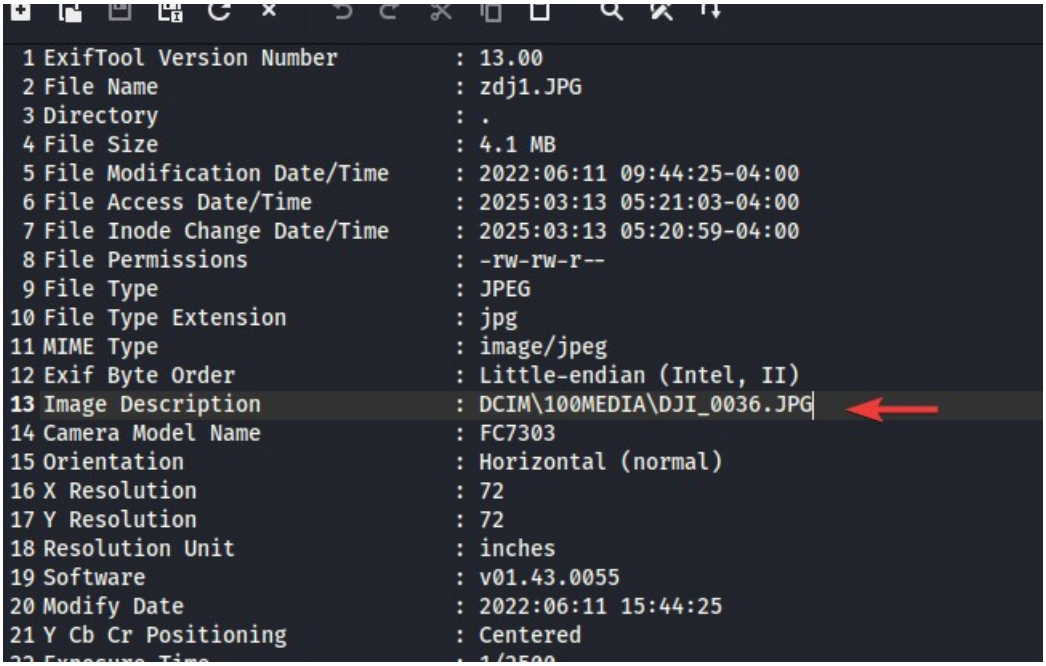


Rysunek 14: flaga 1



Rysunek 15: flaga 2 (URL)

3. Podaj oryginalna nazwę pliku zdj1.



Rysunek 16: oryginalna nazwa pliku zdj1

4. Znajdź informację na jakiej wysokości zostało zrobione zdjęcie.

```
106 Image UID 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                    : 4000×2250
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                      : 4096×4096
Megapixels                      : 16.8

┌──(kali㉿kali)-[~/Desktop/lab2]
└─$
```

Rysunek 18: usuwanie metdadanych 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 dodawkowych informacji o plikach, a także na znajdowanie plików ukrytych.