

POLITECHNIKA WROCŁAWSKA  Wydział Informatyki i Telekomunikacji	Wydział: Informatyki i Telekomunikacji Kierunek: Cyber bezpieczeństwo Rok Akademicki: 2024/2025 Rok studiów, semestr: 2, 4 Grupa: 1 Termin: pon., 7:30
--	---

CBESI0053G Informatyka śledcza – Laboratorium 4

Prowadzący: mgr inż. Adrian Florek	Autor: 1. Gerard Błaszczyk
Data wykonania ćwiczenia: 24.03.2025	
Data oddania sprawozdania: <i>dd.mm.rrrr</i>	

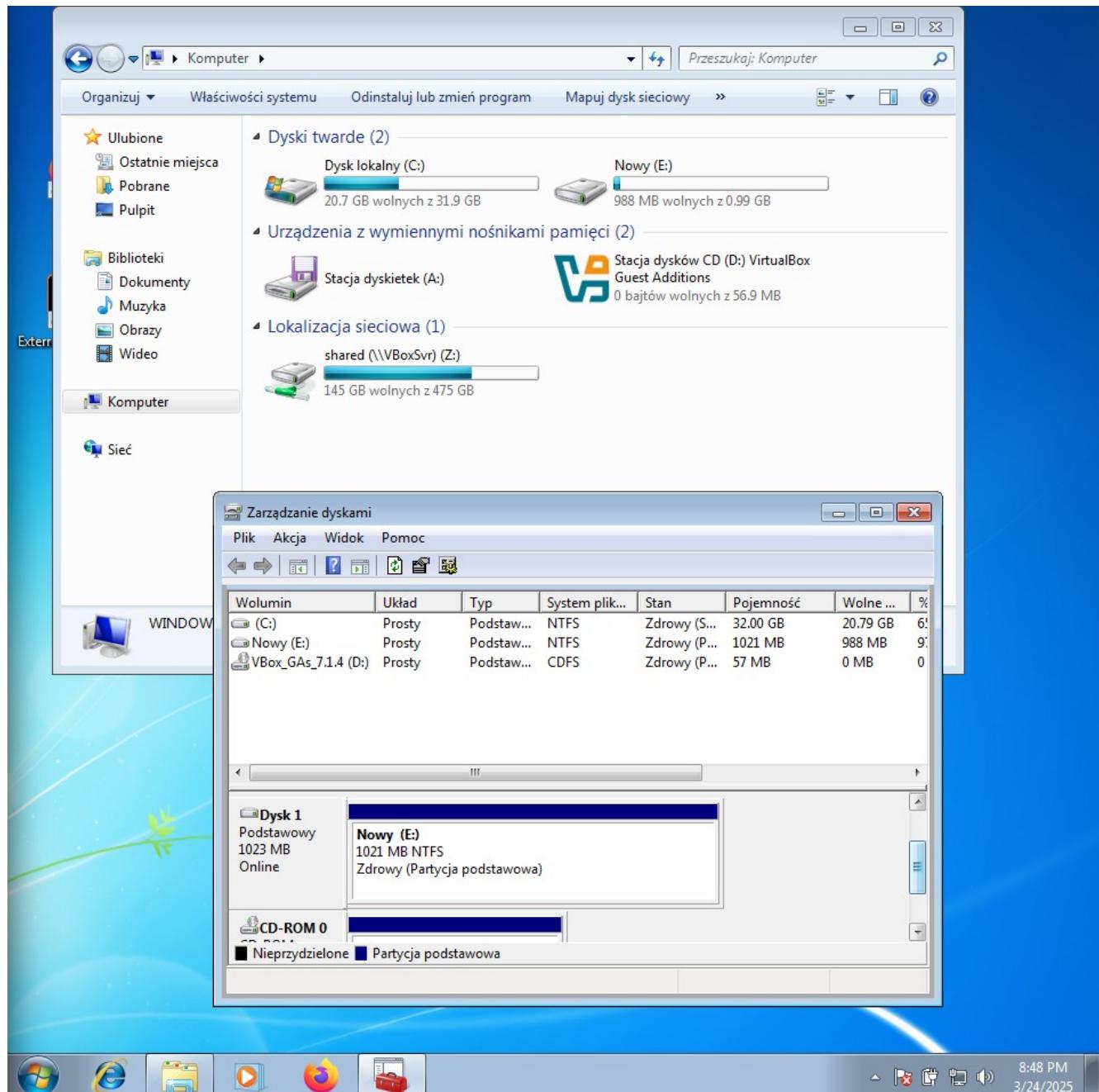
1. Cel ćwiczenia

Tworzenie obrazu nośnika, zapoznanie z programem FTK Imager, automatyzacja tworzenia kopii obrazu.

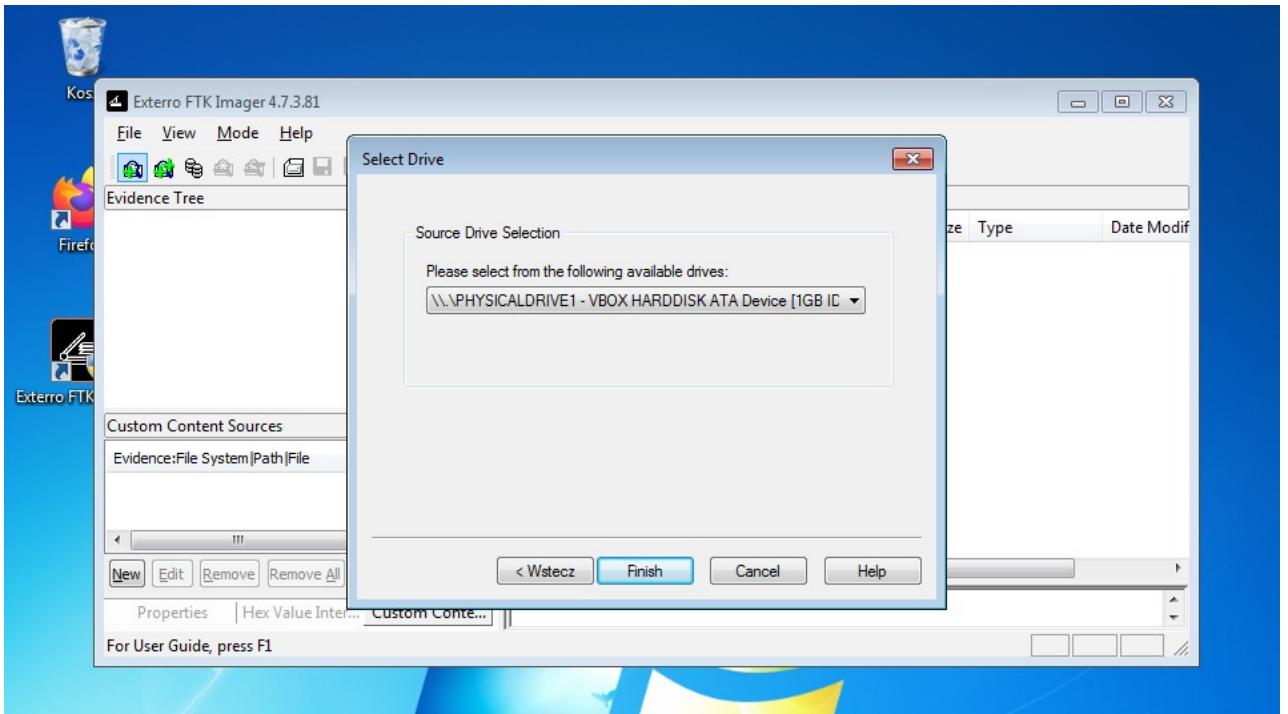
2. Realizacja instrukcji laboratoryjnej

1. Zapoznaj się z programem FTK Imager

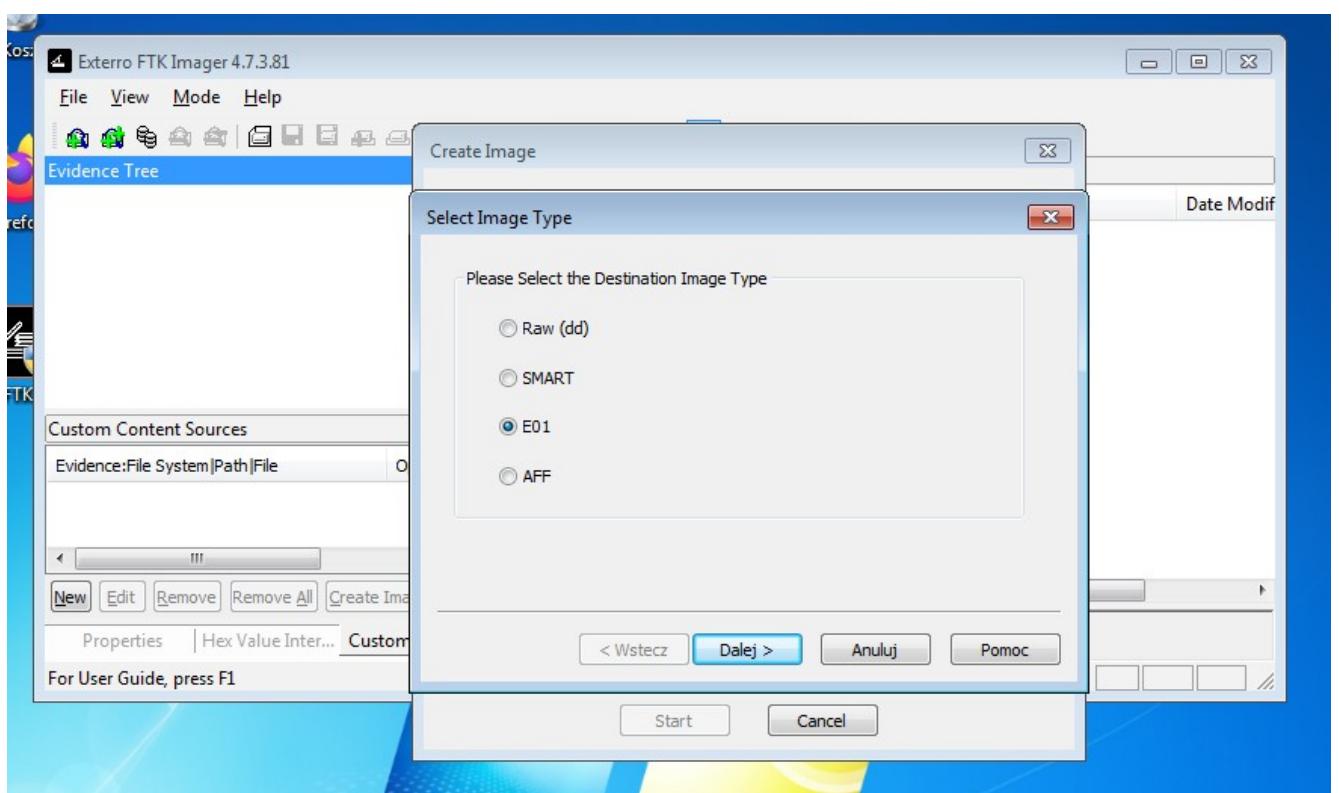
a) Za pomocą FTK Imager utwórz obraz nośnika, Wybierz format E01



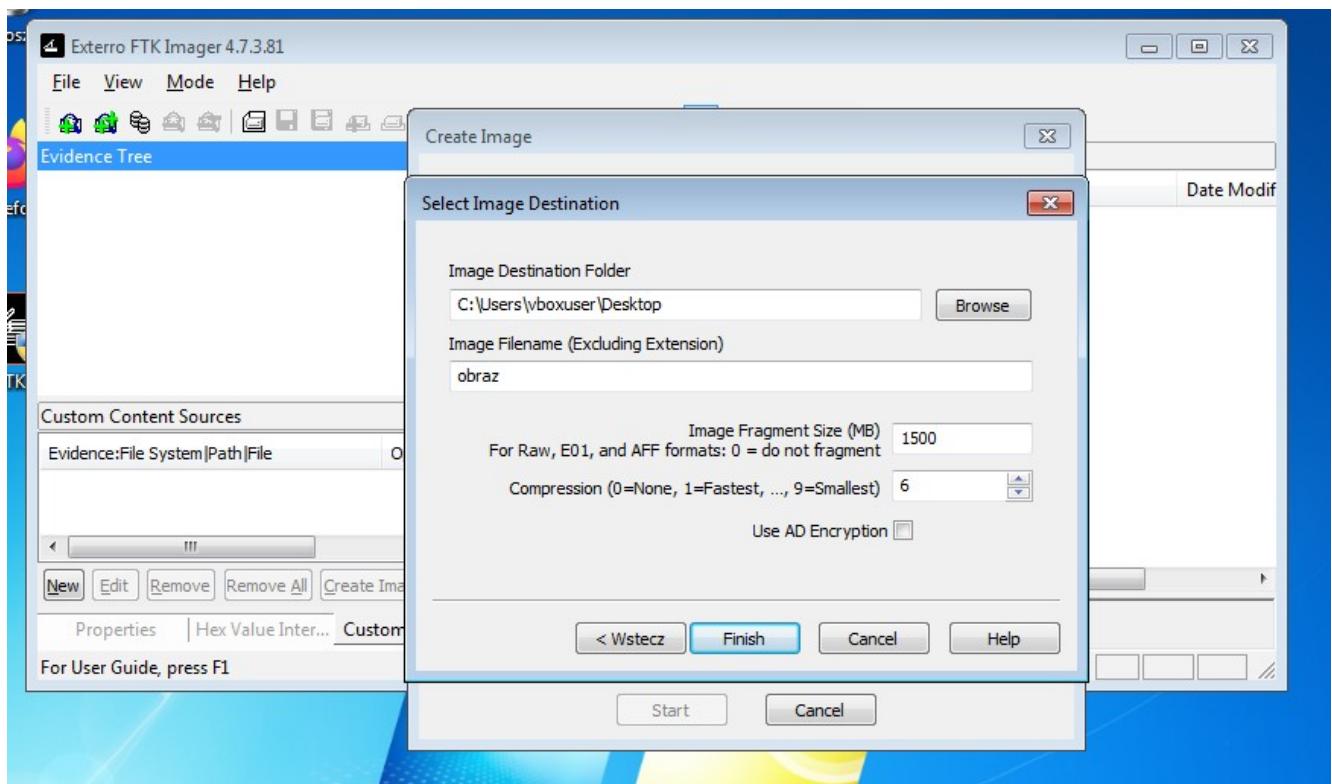
Rysunek 1: Zimportowanie wirtualnego dysku (1GB) do systemu plików



Rysunek 2: Tworzenie obrazu dysku

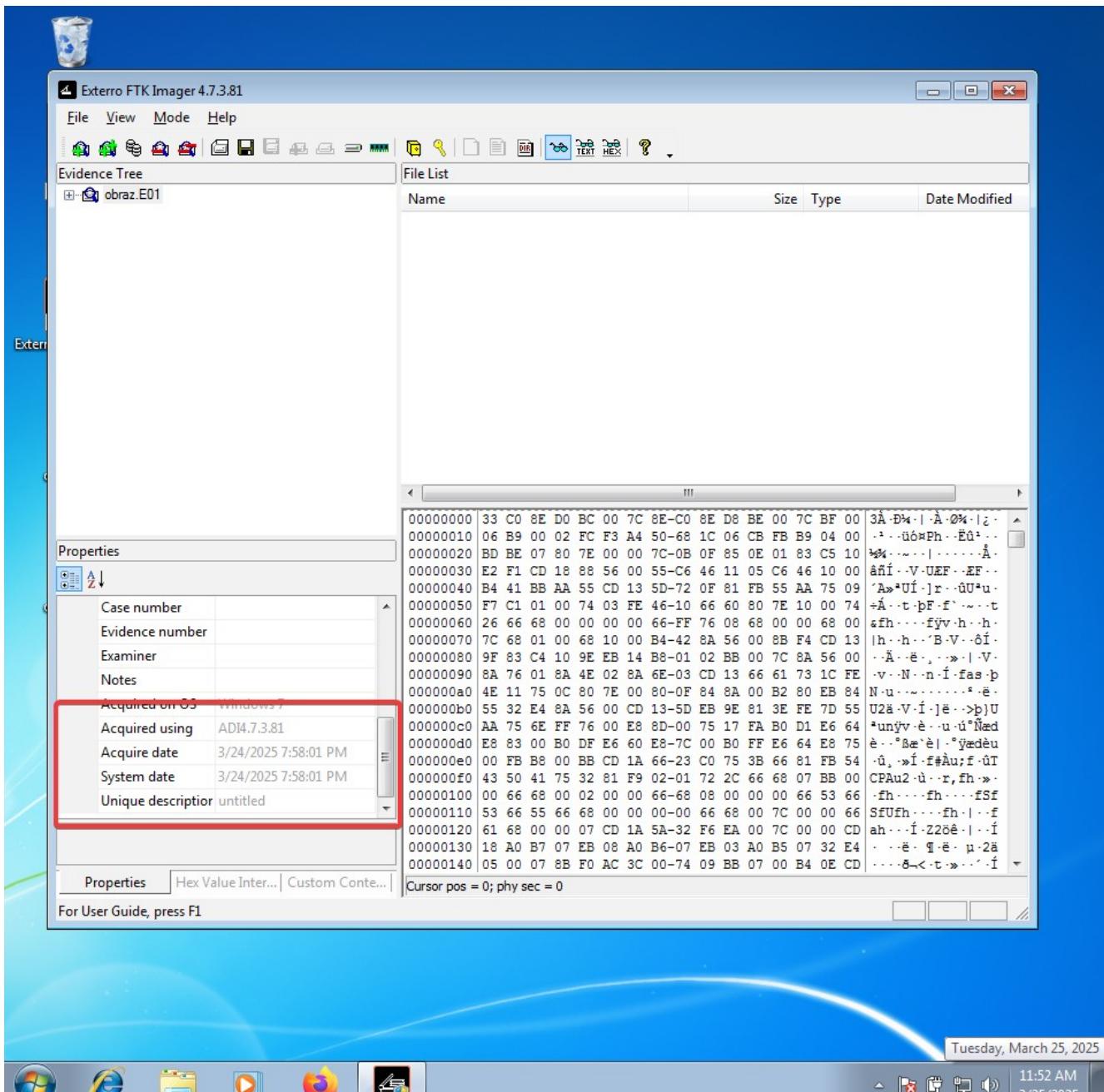


Rysunek 3: Tworzenie obrazu dysku



Rysunek 4: Tworzenie obrazu dysku

b) Po utworzeniu obrazu otwórz go w FTK Imager i sprawdź metadane (data utworzenia, hash).



Rysunek 5: Wyświetlenie daty utworzenia

Drive/Image Verify Results	
obraz.E01	
Name	obraz.E01
Sector count	2097152
MD5 Hash	
Computed hash	9736c1a75e706264d3166385cc0bfaf
Stored verification hash	9736c1a75e706264d3166385cc0bfaf
Report Hash	9736c1a75e706264d3166385cc0bfaf
Verify result	Match
SHA1 Hash	
Computed hash	61643dc8d313955f5792024f8ee6f7fa6599bab6
Stored verification hash	61643dc8d313955f5792024f8ee6f7fa6599bab6
Report Hash	61643dc8d313955f5792024f8ee6f7fa6599bab6
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image
Close	

Rysunek 6: Wyświetlenie MD5 oraz SHA1

c) Zweryfikuj integralność obrazu

Weryfikacja pokazana na rysunku 6 – porównanie skrótów obrazu z oryginalnym skrótem stworzonym przy pierwotnym tworzeniu obrazu.

- Jakie są różnice między formatem surowym a E01?

format surowy nie obsługuje kompresji ani zachowania metadanych w przeciwieństwie do E01, natomiast jest bardziej uniwersalny.

- W jakich sytuacjach lepiej stosować E01 zamiast DD?

kiedy ważne jest zachowanie metadanych, dla efektywnego przechowywania, dla chęci łatwego weryfikowania integralności

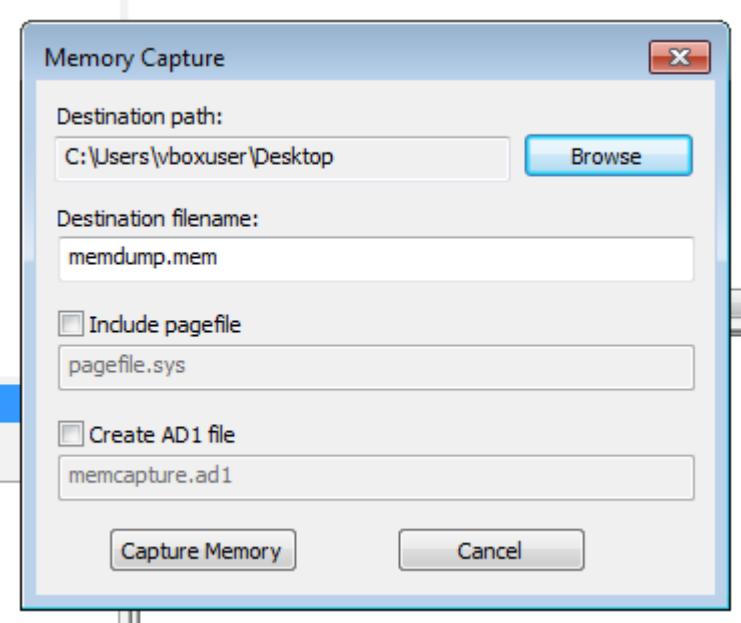
- Przeanalizuj nagłówek partycji, jaki ma identyfikator?

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Tekst zdekodowany
00000000	45 56 46 09 0D 0A FF 00 01 01 00 00 00 68 65 61	EVF.....he
00000010	64 65 72 00 00 00 00 00 00 00 00 00 00 B9 00 00	der.....a...
00000020	00 00 00 00 00 AC 00 00 00 00 00 00 00 00 00 00n.....
00000030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

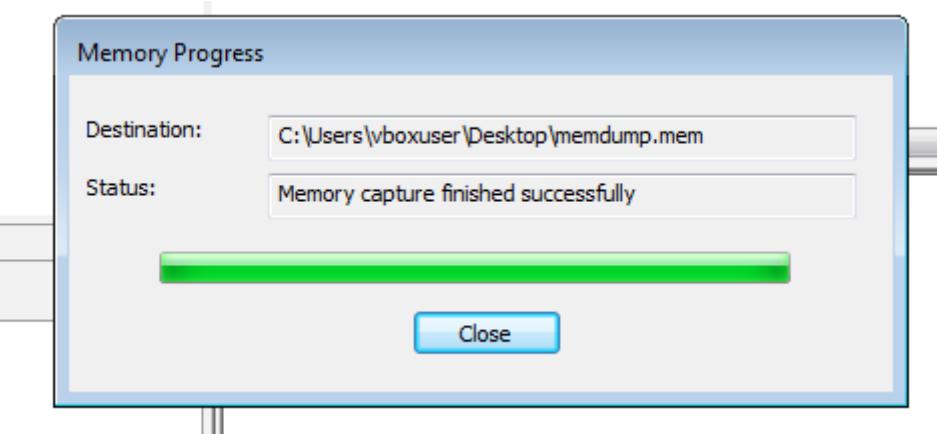
Rysunek 7: Sygnatura pliku obrazu

plik ma nagłówek: 45 56 46

d) Zrób zrzut pamięci



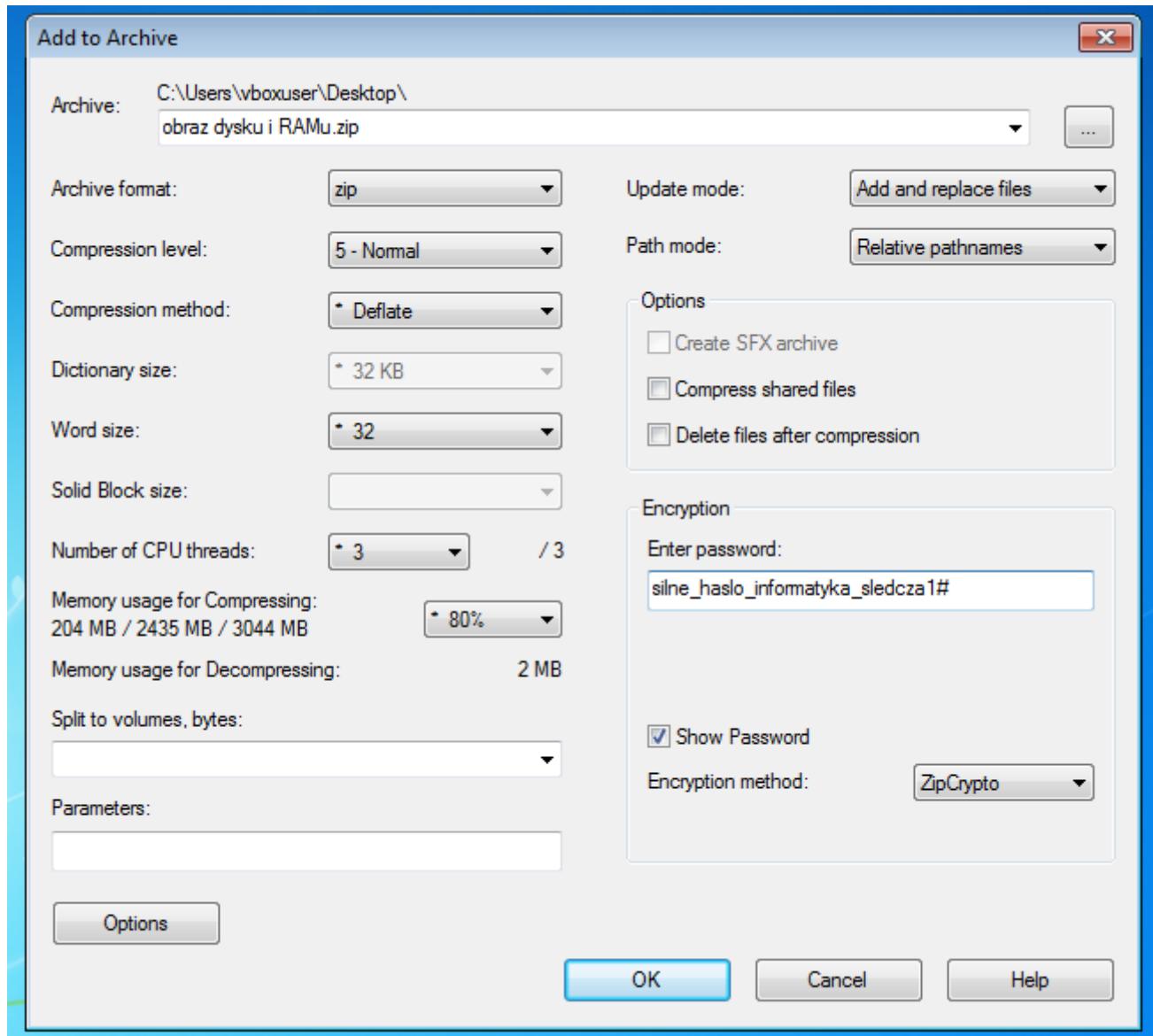
Rysunek 8: Tworzenie zrzutu pamięci



Rysunek 9: Tworzenie zrzutu pamięci

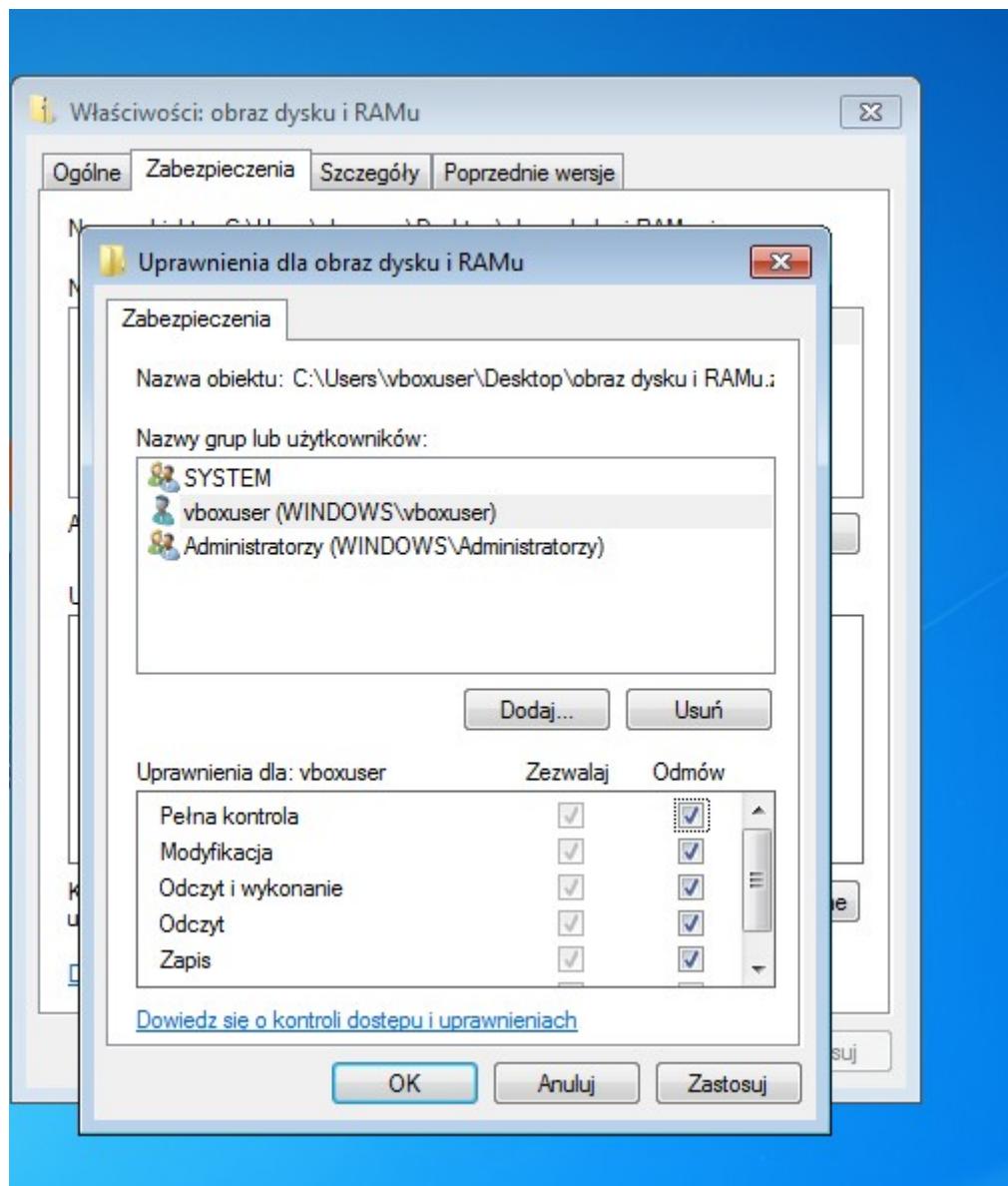
e) Zabezpiecz obraz nośnika przed nieautoryzowanym dostępem.

Pliki można zabezpieczyć dodając je do archiwum zip z silnym hasłem, za pomocą programu 7zip.

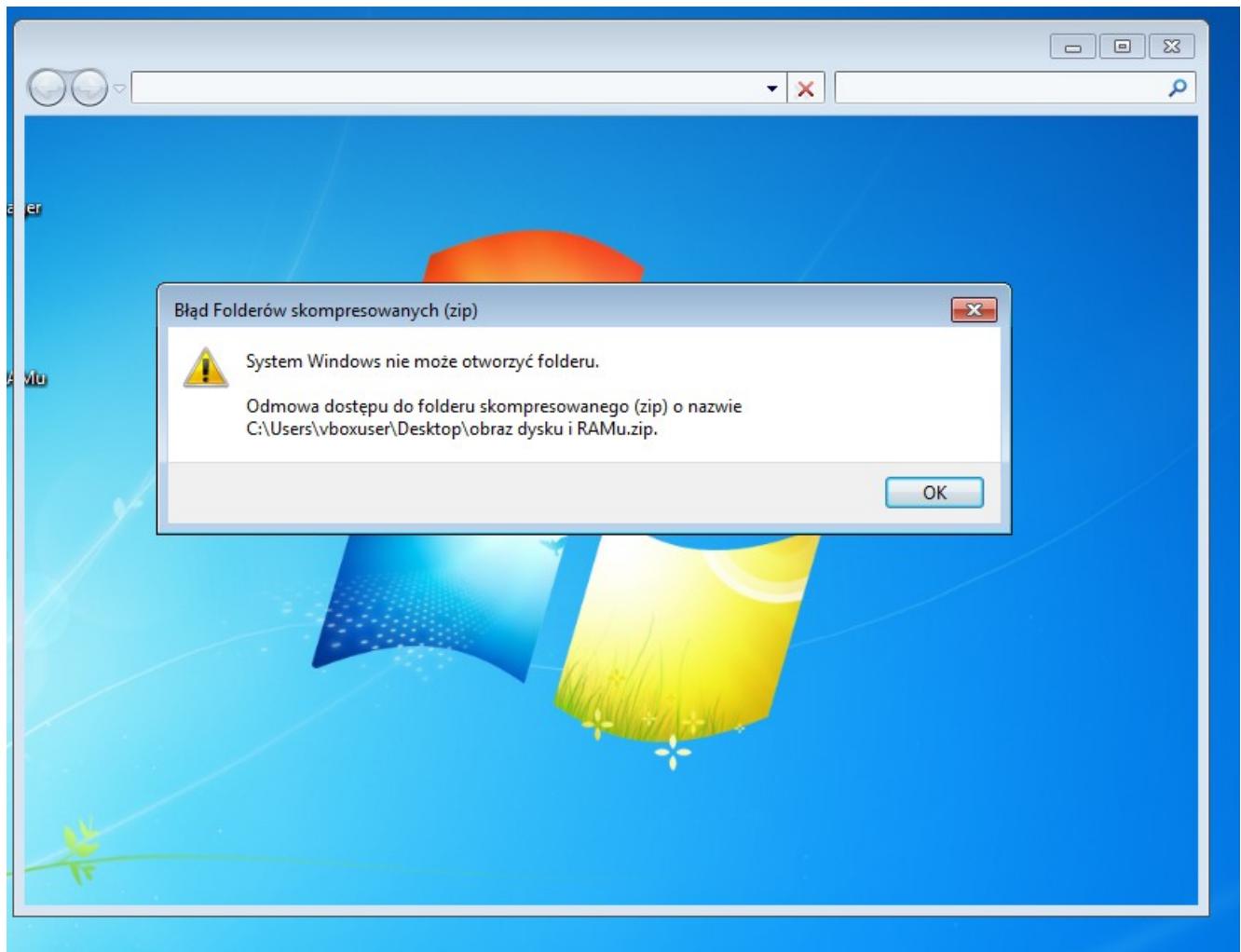


Rysunek 10: tworzenie archiwum z obrazem dysku i zrzutem pamięci

Ponadto, można pobawić jakichkolwiek praw do pliku kontom nie-administratorskim

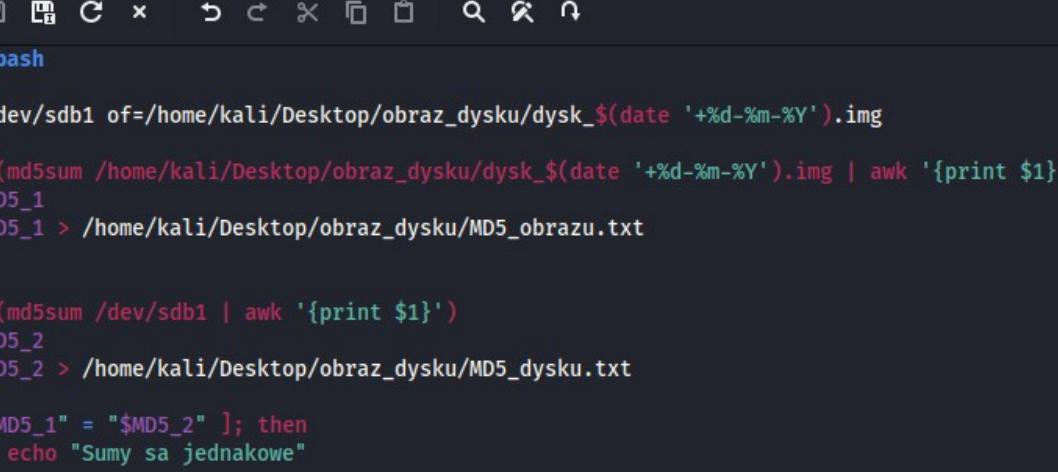


Rysunek 11: Odbieranie uprawnień dostępu do pliku



Rysunek 12: Próba otwarcia pliku jako zwykły użytkownik

2. Napisz skrypt w bashu, który automatycznie utworzy kopie obrazu. Skrypt powinien zapisać datę wykonania kopii w nazwie pliku a następnie wygenerować, porównać i zapisać do pliku sumy kontrolne obrazów.



```
#!/bin/bash
dd if=/dev/sdb1 of=/home/kali/Desktop/obraz_dysku/dysk_$(date '+%d-%m-%Y').img
MD5_1=$(md5sum /home/kali/Desktop/obraz_dysku/dysk_$(date '+%d-%m-%Y').img | awk '{print $1}')
echo $MD5_1 > /home/kali/Desktop/obraz_dysku/MD5_obrazu.txt
MD5_2=$(md5sum /dev/sdb1 | awk '{print $1}')
echo $MD5_2 > /home/kali/Desktop/obraz_dysku/MD5_dysku.txt
if [ "$MD5_1" = "$MD5_2" ]; then
    echo "Sumy sa jednakowe"
else
    echo "Sumy nie sa jednakowe"
fi
```

Rysunek 13: skrypt do tworzenia i sprawdzenia integralności obrazu dysku

```
Sumy sa jednakowe

└─(kali㉿kali)-[~/Desktop]
$ sudo ./skrypt.sh
2091008+0 records in
2091008+0 records out
1070596096 bytes (1.1 GB, 1021 MiB) copied, 4.47922 s, 239 MB/s
e6ec768916b6c359f930d210f1ba279c
e6ec768916b6c359f930d210f1ba279c
Sumy sa jednakowe

└─(kali㉿kali)-[~/Desktop]
$ ls obraz_dysku/
dysk_25-03-2025.img  MD5_dysku.txt  MD5_obrazu.txt

└─(kali㉿kali)-[~/Desktop]
$ cat obraz_dysku/MD5_dysku.txt
e6ec768916b6c359f930d210f1ba279c

└─(kali㉿kali)-[~/Desktop]
$ cat obraz_dysku/MD5_obrazu.txt
e6ec768916b6c359f930d210f1ba279c

└─(kali㉿kali)-[~/Desktop]
$ █
```

Rysunek 14: działanie skryptu

- a) W systemie Linux zamontuj obraz w trybie tylko do odczytu

```
(kali㉿kali)-[~/Desktop/obraz_dysku]  
└─$ sudo mount -o ro dysk_25-03-2025.img /mnt
```

Rysunek 15: montowanie obrazu w trybie do odczytu

Wnioski: Zarówno system Windows jak i Linux oferują możliwość tworzenia obrazów dysków, co jest przydatne gdy potrzebna jest redundancja dowodów cyfrowych. Obrazy dysków powinny być zabezpieczane oraz powinno się dokonywać sprawdzania ich integralności z dyskiem oryginalnym.