


<b>POLITECHNIKA WROCŁAWSKA</b>  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
<b>CBESI0053G Informatyka śledcza – Laboratorium 4</b>	
Prowadzący: mgr inż. Adrian Florek	Autor: 1. Gerard Błaszczuk
Data wykonania ćwiczenia: 24.03.2025	
Data oddania sprawozdania: <i>dd.mm.rrrr</i>	

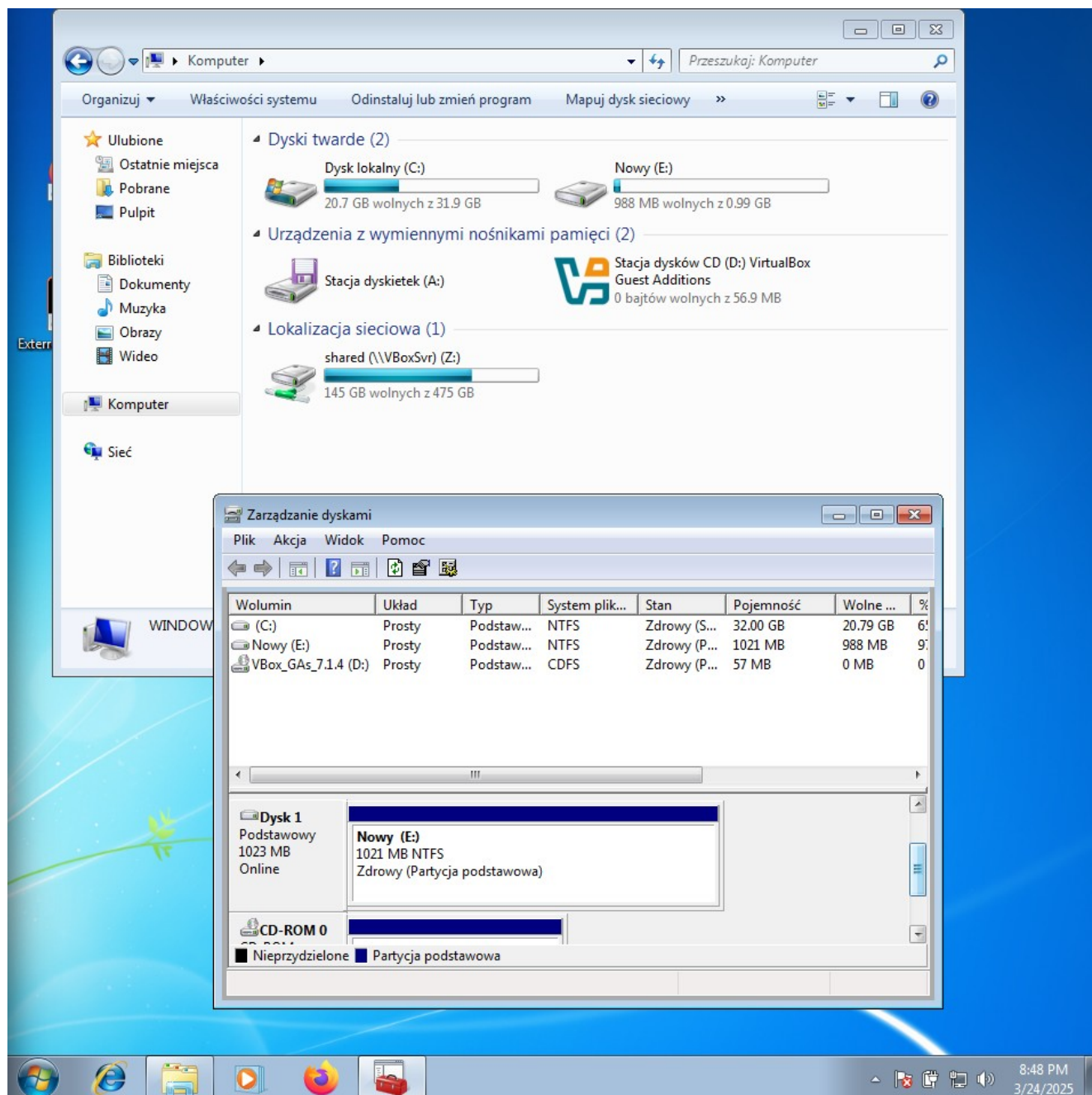
## 1. Cel ćwiczenia

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

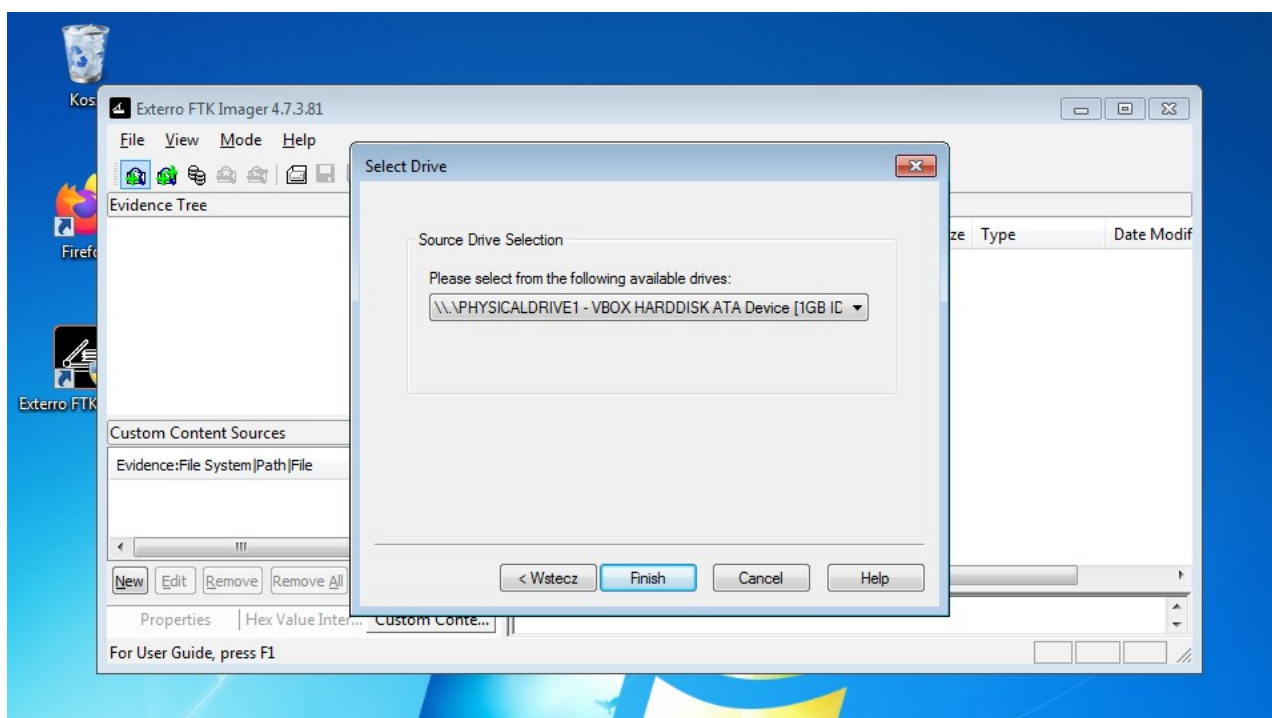
## 2. Realizacja instrukcji laboratoryjnej

### 1. Zapoznaj się z programem FTK Imager

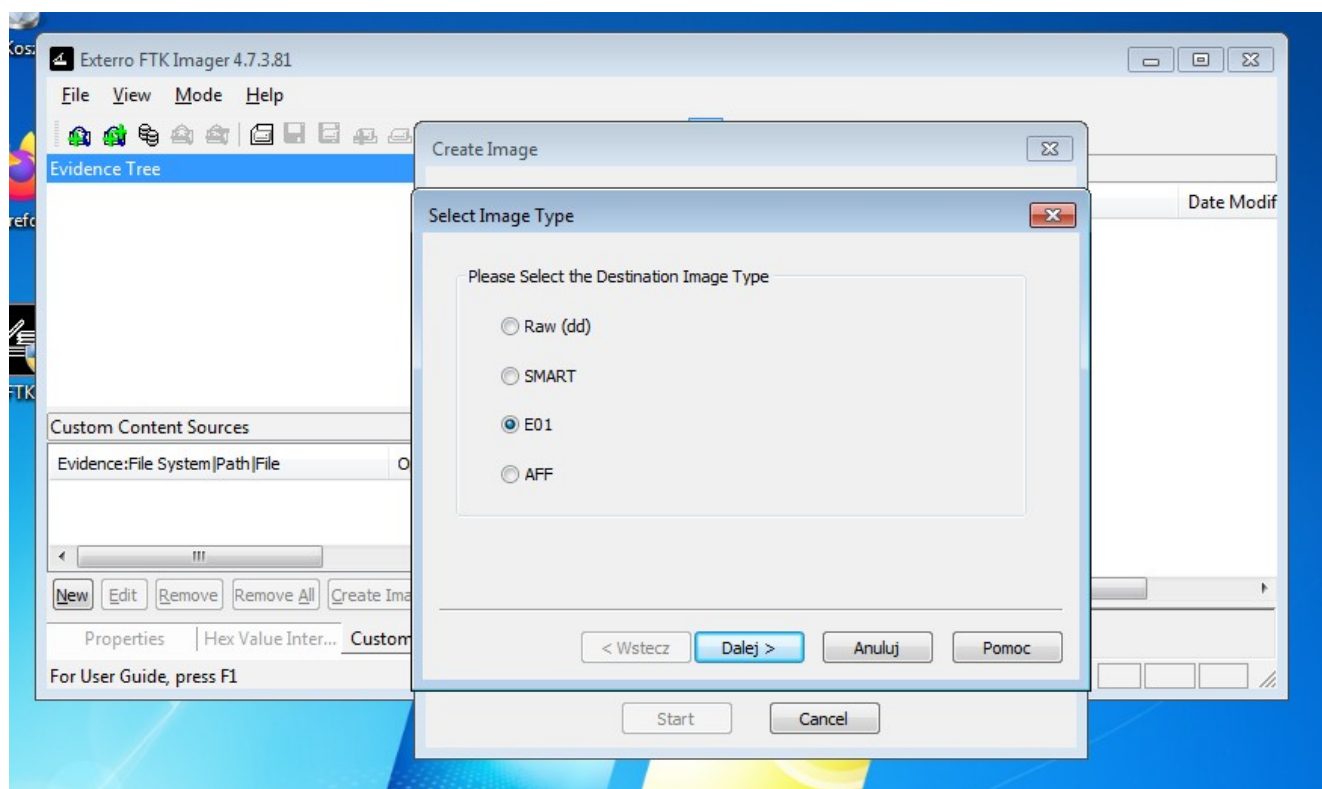
a) Za pomocą FTK Imager utwórz obraz nośnika, Wybierz format E01



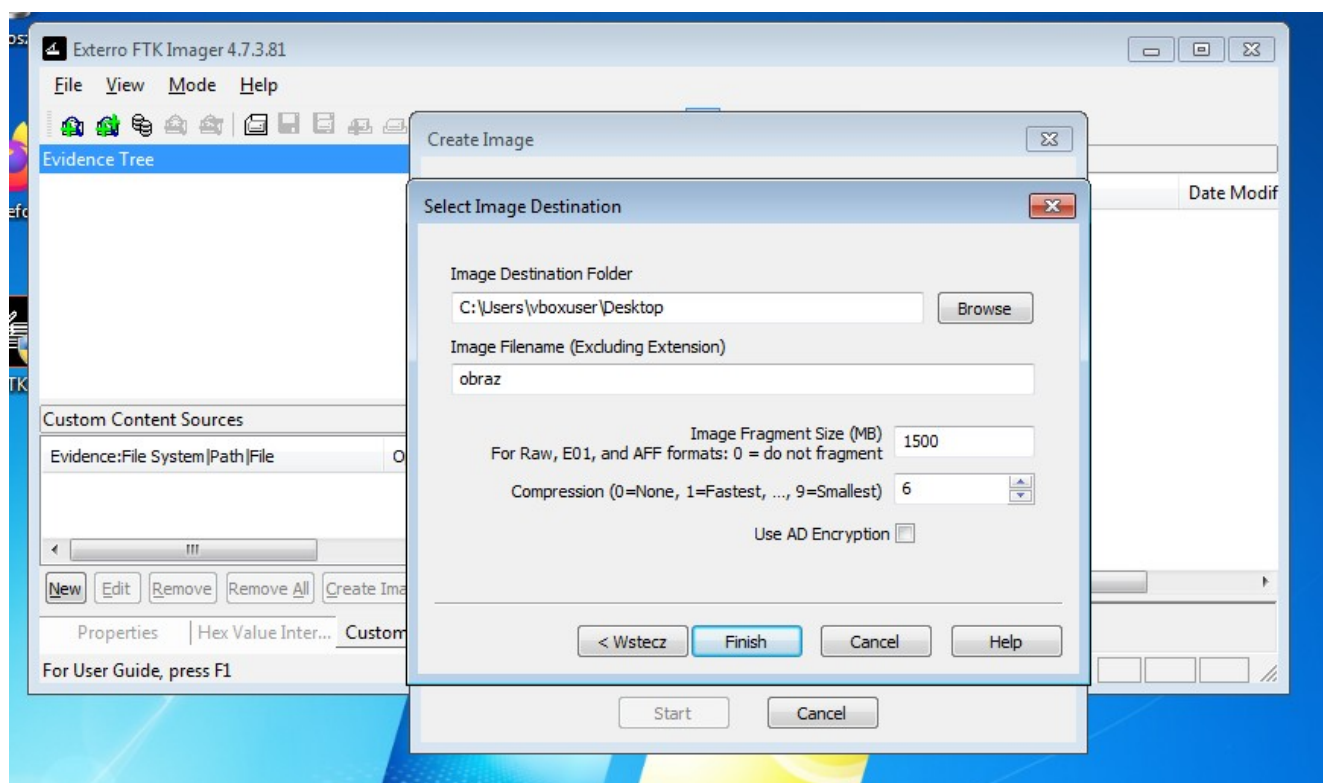
Rysunek 1: Zaimportowanie wirtualnego dysku (1GB) do systemu plików



*Rysunek 2: Tworzenie obrazu dysku*

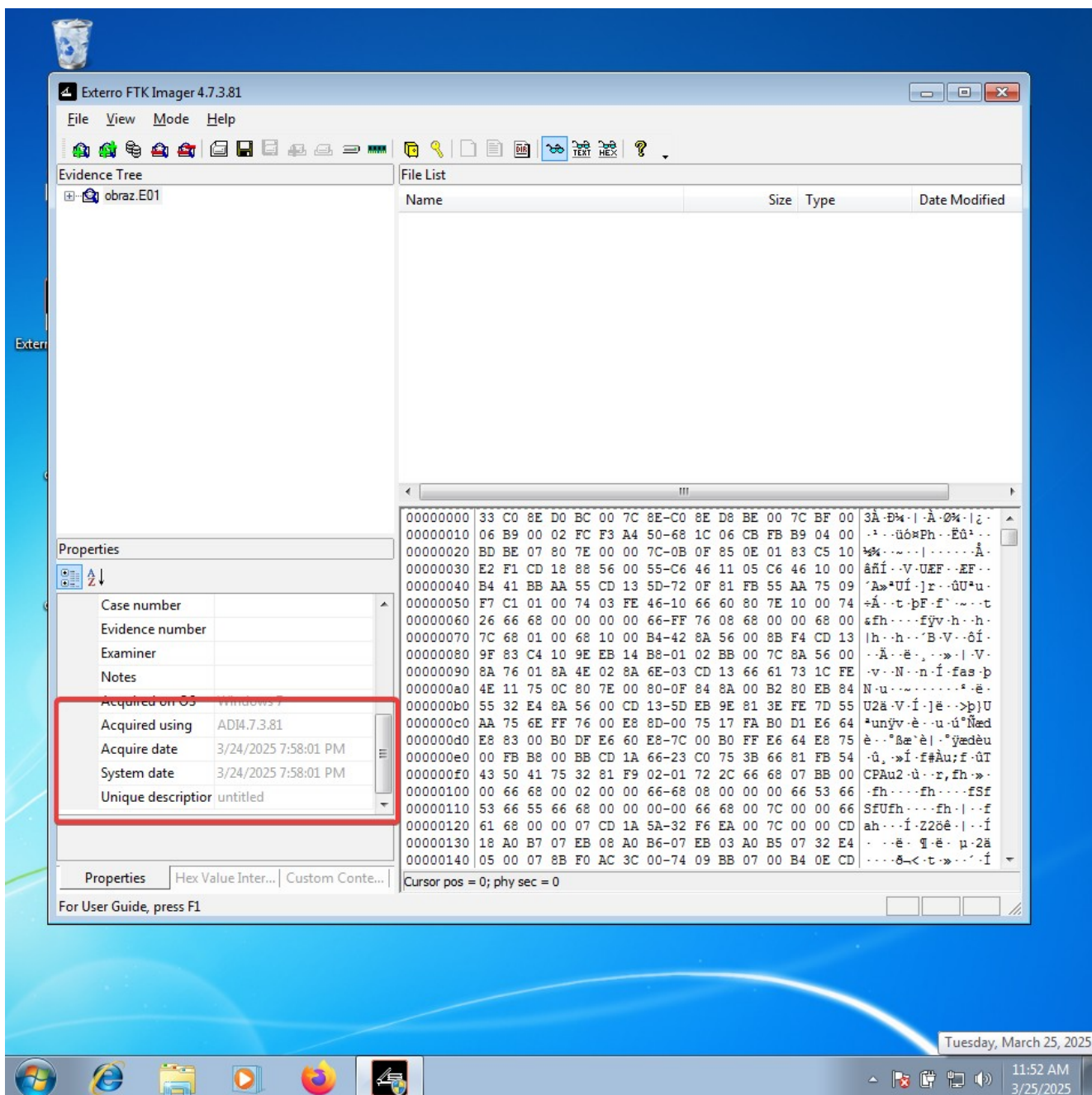


*Rysunek 3: Tworzenie obrazu dysku*

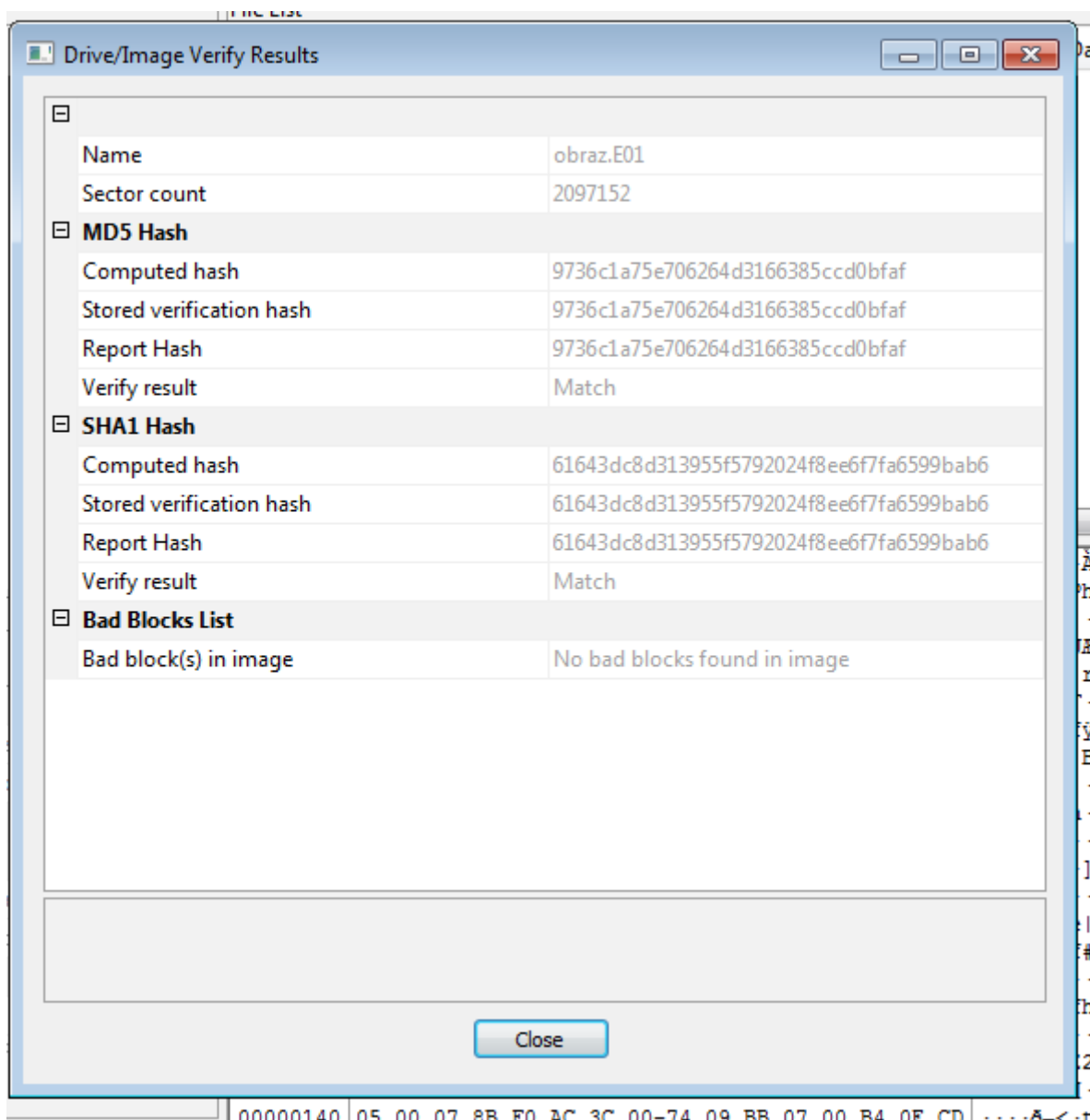


*Rysunek 4: Tworzenie obrazu dysku*

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



Rysunek 5: Wyświetlenie daty utworzenia



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

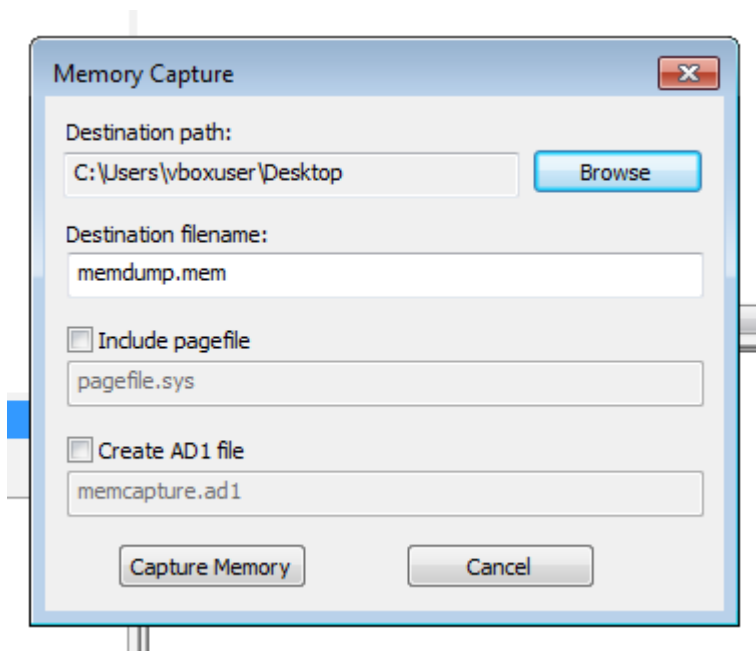
- **Przeanalizuj nagłówki partycji, jaki ma identyfikator?**

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	EVE....`.....hea
00000010	64	65	72	00	00	00	00	00	00	00	00	00	00	B9	00	00	der.....ą..
00000020	00	00	00	00	00	AC	00	00	00	00	00	00	00	00	00	00	.....7.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

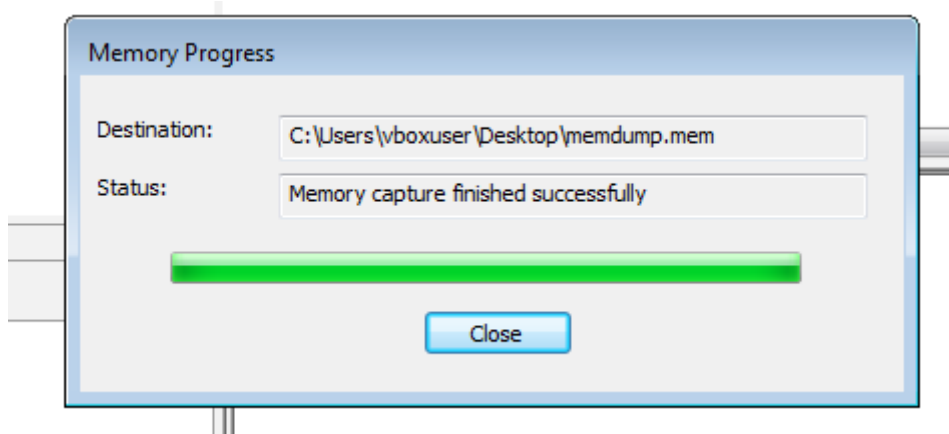
Rysunek 7: Sygnatura pliku obrazu

plik ma nagłówek: 45 56 46

d) Zrób zrzut pamięci



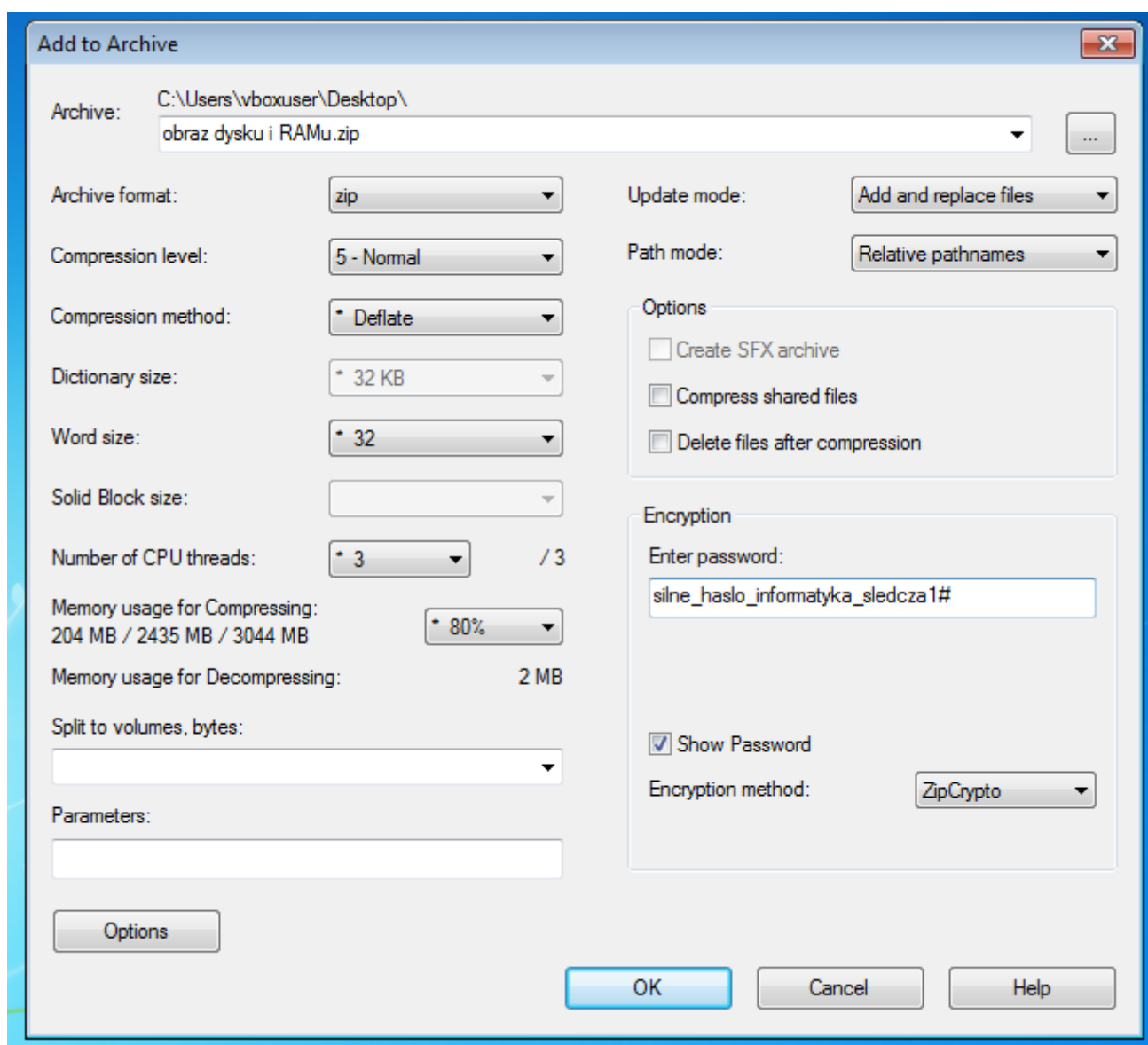
Rysunek 8: Tworzenie zrzutu pamięci



Rysunek 9: Tworzenie zrzutu pamięci

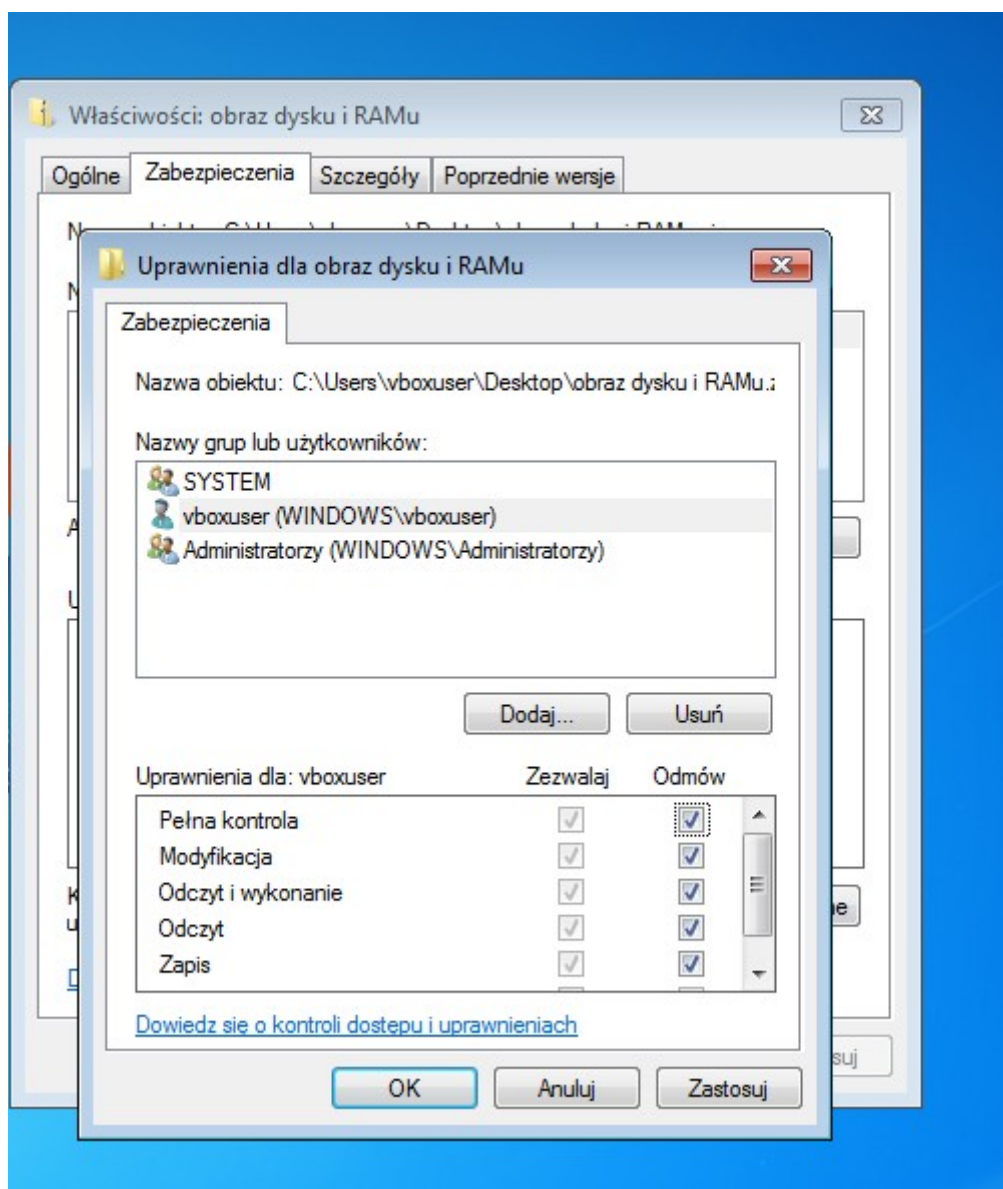
e) Zabezpiecz obraz nośnika przed nieautoryzowanym dostępem.

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

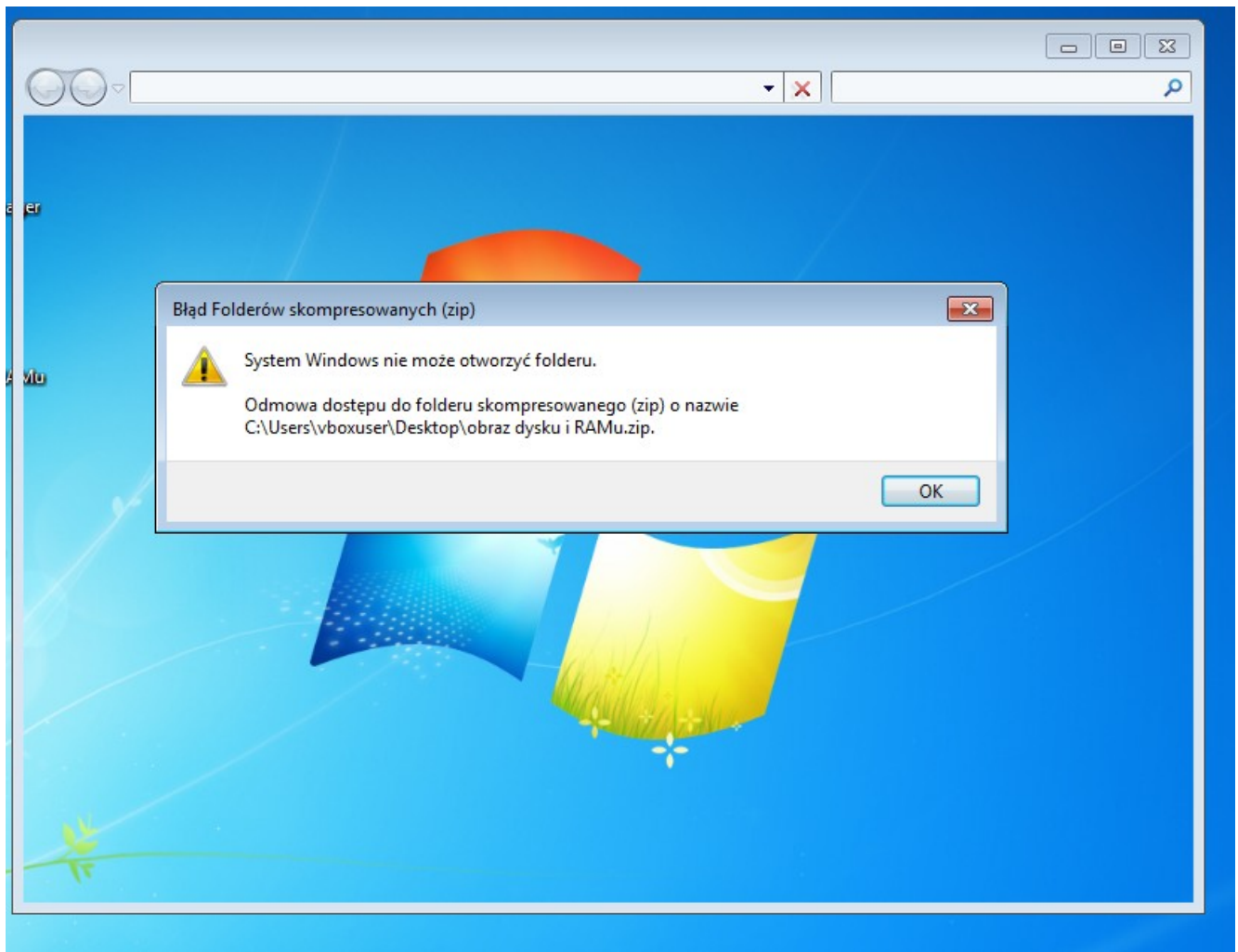


*Rysunek 10: tworzenie archiwum z obrazem dysku i zrzutem pamięci*

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

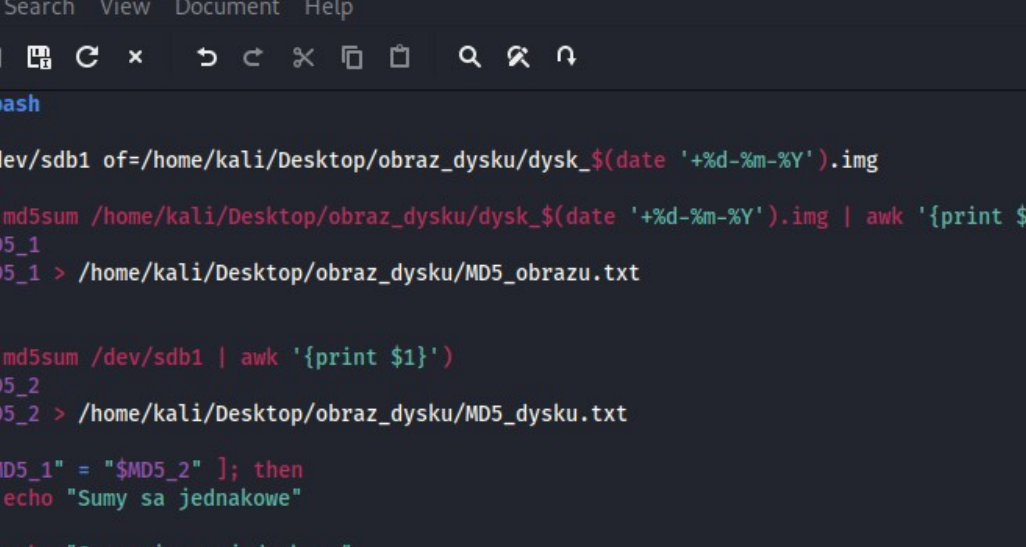


*Rysunek 11: Odbieranie uprawnień dostępu do pliku*



*Rysunek 12: Próba otworzenia 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.**



The screenshot shows a terminal window titled '~/.Desktop/skrypt.sh - Mousepad'. The window has a menu bar with 'File', 'Edit', 'Search', 'View', 'Document', and 'Help'. Below the menu is a toolbar with icons for file operations. The terminal content is a shell script with 19 lines:

```

1 #!/bin/bash
2
3 dd if=/dev/sdb1 of=/home/kali/Desktop/obraz_dysku/dysk_$(date '+%d-%m-%Y').img
4
5 MD5_1=$(md5sum /home/kali/Desktop/obraz_dysku/dysk_$(date '+%d-%m-%Y').img | awk '{print $1}')
6 echo $MD5_1
7 echo $MD5_1 > /home/kali/Desktop/obraz_dysku/MD5_obrazu.txt
8
9
10 MD5_2=$(md5sum /dev/sdb1 | awk '{print $1}')
11 echo $MD5_2
12 echo $MD5_2 > /home/kali/Desktop/obraz_dysku/MD5_dysku.txt
13
14 if [ "$MD5_1" = "$MD5_2" ]; then
15     echo "Sumy sa jednakowe"
16 else
17     echo "Sumy nie sa jednakowe"
18 fi
19

```

**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.