

Zadanie Struktura dysku

Cel Ogólny Lekcji: Lekcja ma na celu zrozumienie struktury dysku, partycji i systemów plików oraz przegląd narzędzi do analizy i edycji danych na dyskach. Uczestnicy zdobędą wiedzę teoretyczną dotyczącą zarządzania dyskami w systemie Windows oraz praktyczne umiejętności wykorzystywania narzędzi takich jak Active@ Disk Editor, HxD, WinHex.

Cele Szczegółowe:

Uczestnicy dowiedzą się, jak zorganizowane są dyski, partycje i systemy plików, a także jakie są różnice między nimi.

Uczestnicy nauczą się przygotowywać dysk wirtualny oraz podłączać go do maszyny wirtualnej.

Uczestnicy będą w stanie zainstalować oprogramowanie z płyty CD/DVD na maszynie wirtualnej.

Uczestnicy będą w stanie korzystać z narzędzi takich jak Active@ Disk Editor, HxD i WinHex do analizy struktury dysków i plików.

Uczestnicy zidentyfikują partycje na dysku i dowiedzą się, jakie systemy plików są na nich używane.

Uczestnicy będą analizować zawartość dysku, w tym strukturę plików i katalogów.

Uczestnicy sporządzą notatki na temat zastosowania narzędzi takich jak DiskEditor Freeware, HxD i WinHex.

Lekcja ta ma na celu połączenie teorii z praktyką, pozwalając uczestnikom na zdobycie wiedzy teoretycznej oraz umiejętności praktycznych związanych z analizą i edycją danych na dyskach. Uczestnicy zostaną zachęceni do eksploracji i zrozumienia struktury dysków oraz korzystania z odpowiednich narzędzi w celu analizy zawartości dysku.

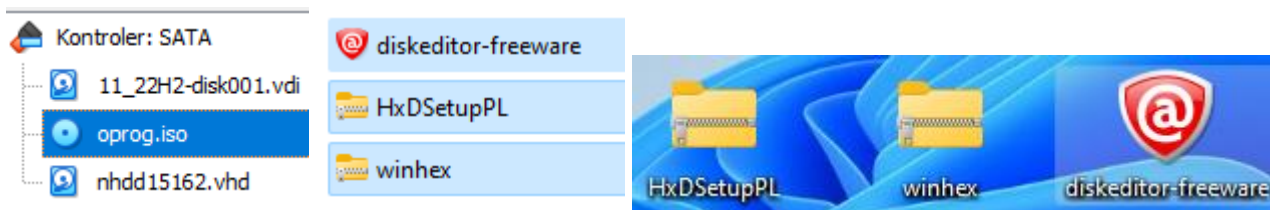
UWAGA: NIE ZAPISUJ ZMIAN W STRUKTURZE DYSKU SYSTEMOWEGO – GROZI UTRATĄ SYSTEMU MASZINY WIRTUALNEJ.

1) Przygotuj folderu z maszyną wirtualną.

W folderze z materiałami o nazwie **2 Struktura dysku** dostępny w <https://tiny.pl/74hzp> znajduje się plik

a) **nhdd15162.zip** należy go pobrać i rozpakować do przygotowanego wcześniej folderu z maszyną wirtualną a następnie skonfigurować i podłączać jako plik drugiego dysku do maszyny wirtualnej.

b) **oprogramowanie.iso** należy go pobrać i podłączyć plik ISO do wirtualnego napędu oraz otworzyć w maszynie wirtualnej płytę cd/dvd gdzie znajduje się oprogramowanie które należy przekopiować (przeciągnąć i upuścić) na pulpit maszyny wirtualnej a następnie je zainstalować.



Każdą czynność wykonaną w zadaniach zgłoś prowadzącemu na etapie wskazanym w zadaniu przez komunikat (zgłoszenie) i jego numer oraz udokumentuj w postaci notatki w zeszycie.

Korzystając z zainstalowanego oprogramowania zidentyfikuj podstawowe elementy struktury podłączonego jako drugi dysk do maszyny wirtualnej dysku.

2) Udokumentuj w zeszycie w sprawozdaniu:

a) jakie partycje z jakimi systemami plików znajdują się na podłączonym dysku jako drugi dysk do maszyny wirtualnej korzystając z oprogramowania Active@ Disk Editor.

1. Odczytaj i udokumentuj w zeszycie w sprawozdaniu wyświetloną listę dostępnych dysków i partycji.
2. Zidentyfikuj dysk, który jest podłączony jako drugi do maszyny wirtualnej. Na tym dysku znajdują się między innymi partycje oznaczone literą "E:", "G:", "F:".
3. Odczytaj wybrane partycje i zidentyfikuj system plików na partycjach, które są na drugim dysku podłączony do maszyny wirtualnej.

Spodziewany efekt:

Open Data Storage						
Select Physical Disk, Partition or Volume (Logical Drive) and click Open button to open selected items in Disk Editor. More then one item can be selected to open at once.						
Name	Type	File System	Total Size	Offset	Total Sectors	
\\.\PhysicalDrive0	Fixed Disk		1.00 TB		2147483648	
NO NAME (1:)	Volume	FAT32	102 MB		208782	
system (C:)	Volume	NTFS	560 GB		1174415756	
Unallocated Space	Unallocated Space	Unallocated	464 GB	1174624605	972859010	
\\.\PhysicalDrive1	Fixed Disk		127 GB		267380736	
1D1 (E:)	Volume	NTFS	13.2 GB		27760256	
Local Disk (G:)	Volume	NTFS	13.0 GB		27316223	
Local Disk (2:)	Volume	Unknown	9.72 GB		20381696	
Extended Partition	Extended	Extended	91.5 GB	75458560	191922176	
Local Disk (3:)	Volume	Unknown	14.8 GB		31090688	
Local Disk (4:)	Volume	Unknown	11.2 GB		23480320	
Local Disk (F:)	Volume	NTFS	11.8 GB		24723455	
Unallocated Space	Unallocated Space	Unallocated	53.7 GB	1	112621567	

Nazwa	Typ	System plików	Całkowity rozmiar	Wolne miejsce

b) jakie partycje z jakimi systemami plików znajdują się na podłączonym dysku jako drugi dysk do maszyny

Jeśli chcesz użyć polecenia **fsutil fsinfo volumeinfo**, musisz podać literę dysku lub nazwę punktu montowania jako argument. Na przykład, jeśli chcesz sprawdzić informacje o partycji E:, wpisz

fsutil fsinfo volumeinfo E:

(gdzie "E:" to litera dysku partycji). Informacja o systemie plików powinna być wyświetlona.

Jeśli chcesz sprawdzić informacje o partycji bez litery, musisz najpierw znaleźć jej nazwę punktu montowania za pomocą polecenia mountvol. Na przykład, jeśli chcesz sprawdzić informacje o partycji 3 na dysku fizycznym 1, wpisz mountvol i znajdź linię z \?\Volume{GUID}\ na końcu.

mountvol

Następnie skopiuj tę nazwę i wpisz **fsutil fsinfo volumeinfo \?\Volume{GUID}**.

fsutil fsinfo volumeinfo \?\Volume{GUID}

(zgłoszenie) 1

Porównaj w zeszycie informacje uzyskane przez Active@ Disk Editor z informacjami uzyskanych z poleceń mountvol i fsutil.

Active@ Disk Editor, polecenie **mountvol** i **fsutil** to narzędzia dostępne w systemie Windows, które pozwalają na uzyskanie różnych informacji dotyczących dysków i woluminów. Poniżej znajduje się krótka analiza różnic między tymi narzędziami:

1. Active@ Disk Editor:

- Active@ Disk Editor to narzędzie służące do przeglądania i edytowania sektorów dysków na poziomie niskim. Jest to narzędzie zaawansowane, które umożliwia wykonywanie operacji na poziomie bitów na dyskach twardych.
- Dzięki Active@ Disk Editor możesz przeglądać i edytować zawartość konkretnych sektorów dysku, analizować struktury danych na dysku, odzyskiwać dane i wykonywać zaawansowane operacje na dysku.

- Jest to narzędzie bardziej zaawansowane i przeznaczone przede wszystkim dla specjalistów ds. odzyskiwania danych i analizy dysków.

2. **mountvol**:

- **mountvol** jest wierszowym poleceniem systemowym, które pozwala na zarządzanie punktami montowania w systemie plików Windows.
- Możesz użyć **mountvol** do wyświetlania listy dostępnych punktów montowania, tworzenia i usuwania punktów montowania dla woluminów dysków, a także do zarządzania przypisanymi literami dysków.

3. **fsutil**:

- **fsutil** to narzędzie wiersza poleceń, które umożliwia zarządzanie i uzyskiwanie informacji na temat systemu plików NTFS w systemie Windows.
- Możesz użyć **fsutil** do wykonywania różnych operacji na systemie plików NTFS, takich jak defragmentacja, zarządzanie alternatywnymi strumieniami danych, sprawdzanie integralności i wiele innych.
- **fsutil** jest przydatne w kontekście zarządzania systemem plików, a nie dyskami fizycznymi.

Podsumowując, te narzędzia mają zupełnie inne zastosowania:

- **Active@ Disk Editor** jest narzędziem zaawansowanym do analizy i edycji danych na dyskach na poziomie bitów.
- **mountvol** służy do zarządzania punktami montowania i literami dysków w systemie plików.
- **fsutil** koncentruje się na operacjach na systemie plików NTFS, takich jak defragmentacja i zarządzanie strumieniami danych.

Wybór narzędzia zależy od konkretnego zadania, które chcesz wykonać na dyskach i woluminach w systemie Windows.

(zgłoszenie) 2

c) strukturę systemów plików wszystkich zidentyfikowanych partycji użyj:

1. polecenia **dir** w systemie Windows, aby wyświetlić zawartość każdej zidentyfikowanej partycji. Dzięki temu można poznać strukturę plików i katalogów na każdej partycji.

dir E:

2. polecenia **tree** w systemie Windows, aby wyświetlić zawartość każdej zidentyfikowanej partycji. Dzięki temu można poznać strukturę plików i katalogów na każdej partycji.

tree /F E:

(zgłoszenie) 3

d) strukturę wybranego pliku na zidentyfikowanej partycji. Aby wyświetlić szczegółową strukturę wybranego pliku, użyj

1. polecenia **tree** w systemie Windows, na przykład: **tree /F C:\ścieżka\do\pliku\plik.txt**, gdzie "C:\ścieżka\do\pliku\plik.txt" to pełna ścieżka do wybranego pliku.

type E:\E1\E1_0.txt

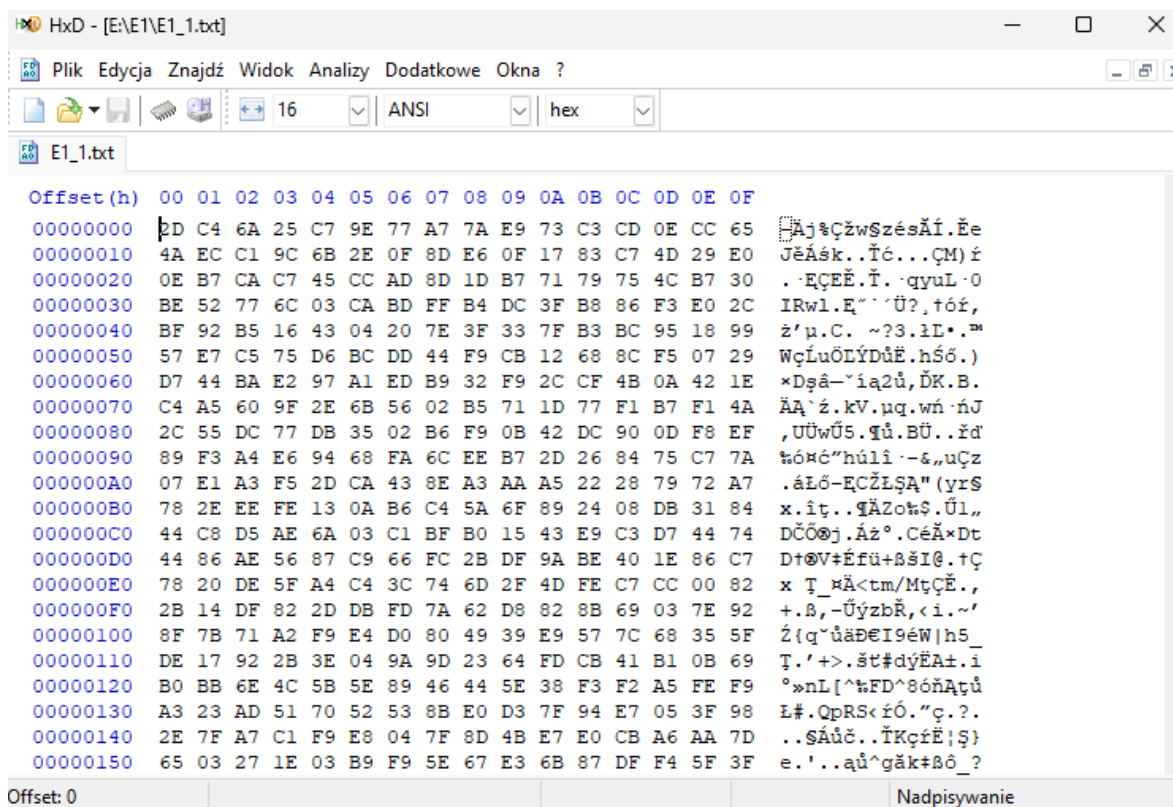
2. polecenia **certutil** w systemie Windows, na przykład: **certutil -encode NazwaPliku PlikWyjściowy.txt**

certutil -encode E:\E1\base.txt E:\PlikWyjściowy.txt

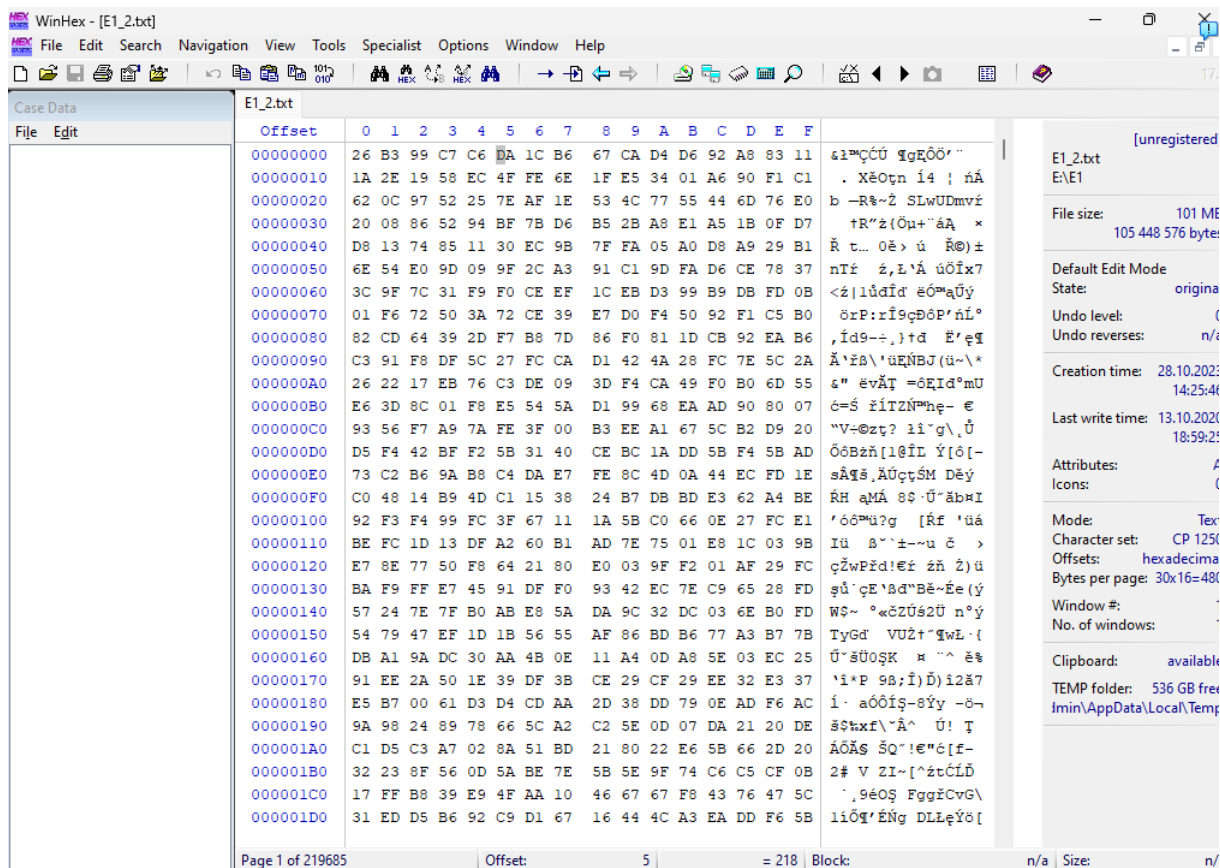
3. polecenia **format-hex** w powershell jeśli chcesz zobaczyć strukturę pliku w formacie heksadecymalnym. To polecenie wyświetli dane binarne pliku w postaci heksadecymalnej i ASCII. Możesz też zapisać wynik polecenia do pliku XML, używając

format-hex -path E:\E1\base.txt | export-clipxml E:\PlikWyjściowy.xml

4. programu HxD aby otworzyć strukturę plik E:\E1\E1_1.txt



5. programu WinHex aby otworzyć strukturę plik E:\E1\E1_2.txt



(zgłoszenie) 4

e) wykonaj krótką notatkę, w której opisz zastosowanie zainstalowanych programów.

Przeglądając zawartość partycji, zidentyfikuj zainstalowane programy lub aplikacje na dysku.

Wykonaj listę tych programów i napisz krótkie notatki na temat ich zastosowania lub przeznaczenia.

Notatka opisująca zastosowanie trzech programów: DiskEditor Freeware, WinHex i HxD:

1. DiskEditor Freeware:

- **Zastosowanie:** DiskEditor Freeware to narzędzie umożliwiające analizę i edycję danych na dyskach na poziomie bitów. Jest przydatne w dziedzinie odzyskiwania danych, analizy dysków twardych, badania uszkodzonych sektorów i innych zastosowań związanych z manipulacją danymi na niskim poziomie.

Cechy:

- Przeglądanie i edycja danych na dyskach twardych.
- Obsługa różnych systemów plików.
- Możliwość odzyskiwania danych z uszkodzonych dysków.

- Wykorzystywane przez profesjonalistów ds. bezpieczeństwa, odzyskiwania danych i analizy dysków.

2. WinHex:

- **Zastosowanie:** WinHex to zaawansowane narzędzie do analizy i edycji danych na dyskach twardych oraz innych nośnikach. Jest wykorzystywane w dziedzinach takich jak odzyskiwanie danych, badanie komputerów w celach śledczych oraz analiza struktur plików.

Cechy:

- Przeglądanie i edycja danych na poziomie bitów.
- Obsługa różnych formatów plików i systemów plików.
- Zaawansowane narzędzia do analizy struktur danych.
- Wykorzystywane przez profesjonalistów w dziedzinie informatyki śledczej.

3. HxD:

- **Zastosowanie:** HxD to edytor szesnastkowy i dziesiętny, który umożliwia przeglądanie i edycję plików w formie szesnastkowej lub dziesiętnej. Jest używany przez programistów, hobbystów i profesjonalistów w różnych dziedzinach do analizy i edycji danych w plikach.

Cechy:

- Przeglądanie i edycja plików w formie szesnastkowej i dziesiętnej.
- Obsługa dużych plików.
- Możliwość wykonywania operacji na plikach binarnych.
- Często stosowany przy analizie struktur plików i kodu.

Wszystkie te narzędzia są przydatne w analizie i edycji danych na poziomie bitów, ale różnią się poziomem zaawansowania i zastosowaniami. DiskEditor Freeware i WinHex są bardziej zaawansowane i znacznie wykorzystywane w profesjonalnych zastosowaniach, podczas gdy HxD jest bardziej dostępny dla programistów i hobbystów.

(zgłoszenie) 5

Powyższe polecenia i kroki pomogą w dokładnym udokumentowaniu informacji dotyczących dysku, partycji, systemów plików, struktury plików i zainstalowanych programów na drugim dysku maszyny wirtualnej. Dzięki temu uczniowie będą mieli kompletną informację na temat zawartości tego dysku.