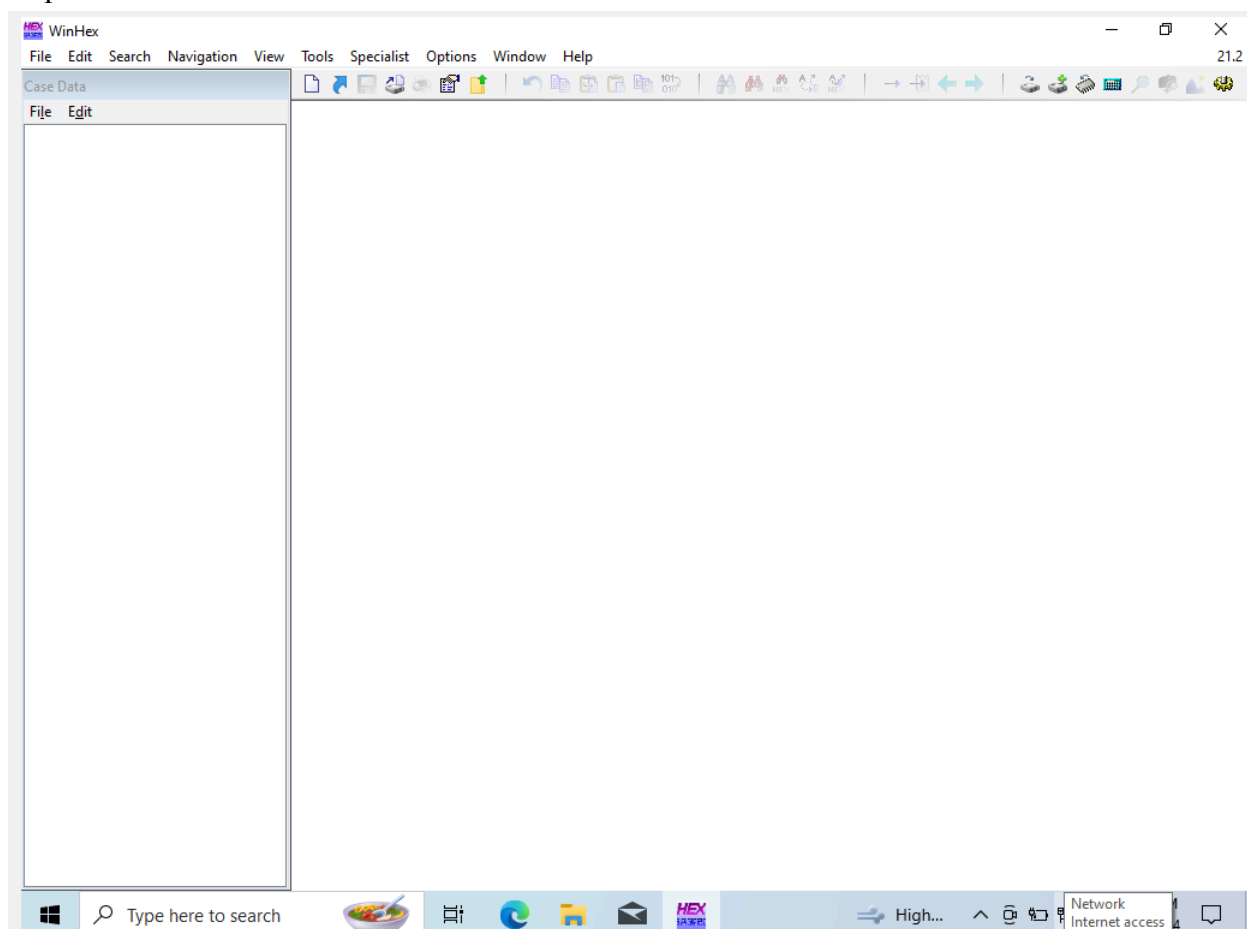


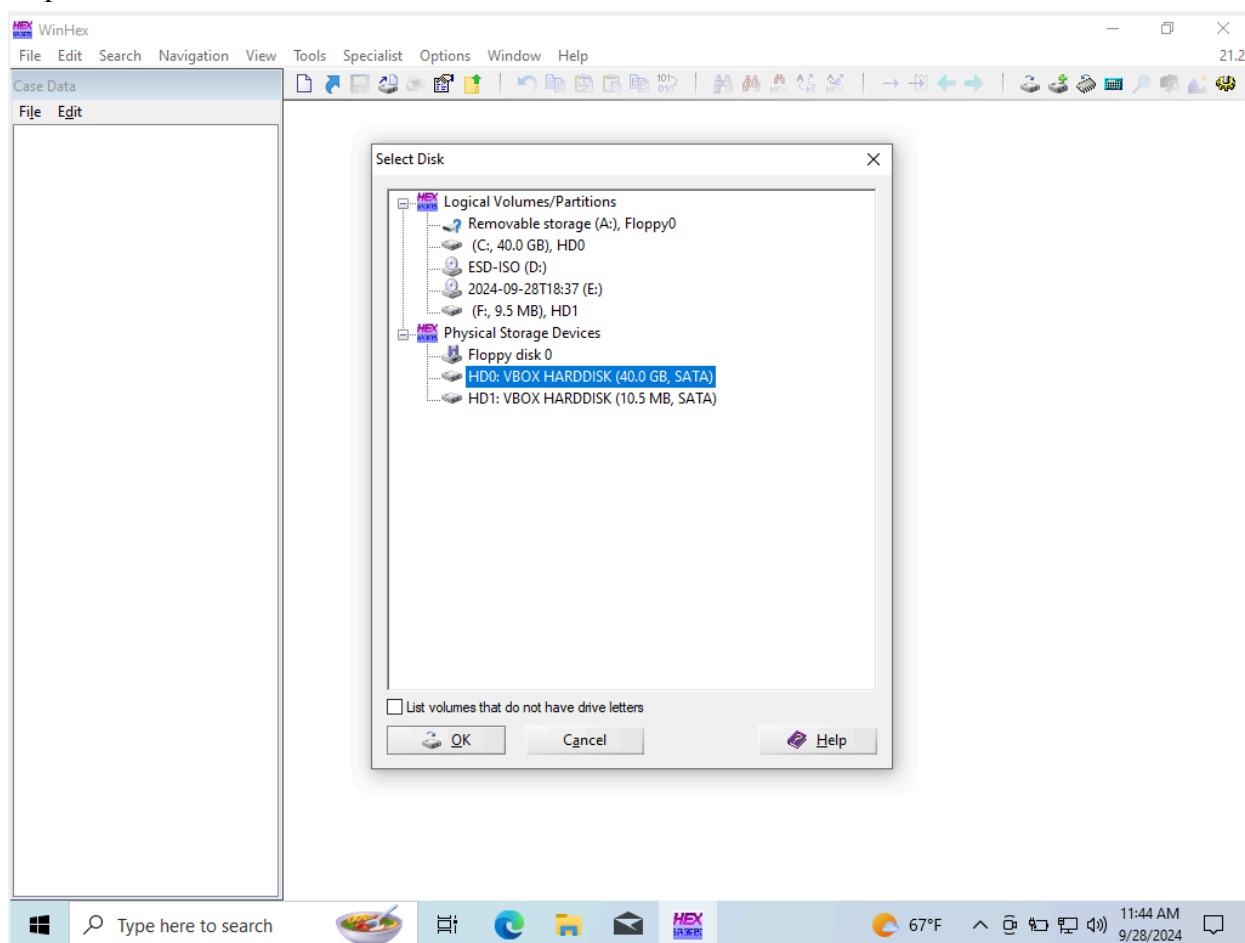
## Task 1: Disk Exploration

### Step 1: Install WinHex



Successful installation of WinHex onto the Windows VM.

## Step 2: Load the Virtual Hard Disk



I gave WinHex administrator privileges and loaded the disk.

### Step 3: Examine the Master Boot Record

The screenshot displays a hex editor window showing the Master Boot Record (MBR) at Sector 0 of 83,886,080. The hex data is displayed in columns 0-15, with corresponding ASCII values on the right. The right pane shows disk information for 'Hard disk 0' (VBOX HARDDISK) with a capacity of 40.0 GB and 512 bytes per sector. The status bar shows the current position at Offset 18F, Sector 0.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
000000130	18	A0	B7	07	EB	08	A0	B6	07	EB	03	A0	B5	07	32	E4
000000140	05	00	07	8B	F0	AC	3C	00	74	09	BB	07	00	B4	0E	CD
000000150	10	EB	F2	F4	EB	FD	2B	C9	E4	64	EB	00	24	02	E0	F8
000000160	24	02	C3	49	6E	76	61	6C	69	64	20	70	61	72	74	69
000000170	74	69	6F	6E	20	74	61	62	6C	65	00	45	72	72	6F	72
000000180	20	6C	6F	61	64	69	6E	67	20	6F	70	65	72	61	74	69
000000190	6E	67	20	73	79	73	74	65	6D	00	4D	69	73	73	69	6E
0000001A0	67	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74
0000001B0	65	6D	00	00	00	63	7B	9A	EF	D3	D6	EF	00	00	80	20
0000001C0	21	00	07	FE	FF	FF	00	08	00	00	00	F0	FF	04	00	00
0000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA
000000200	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000210	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000220	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000230	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000240	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000250	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000260	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000270	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000280	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000290	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000002A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000002B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

I have navigated to the first partition and start head and verified that the values are the same as in the template.

### Step 4: Identify the File System

The screenshot shows a disk partitioning tool interface. At the top, it displays 'Hard disk 0' and 'Partitioning style: MBR'. Below this, a table lists the partitions:

Name	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector
Start sectors		1.0 MB					
Partition 1 (C:)	NTFS	40.0 GB					2,0
Unpartitionable space		1.0 MB					83,884,0

Below the table, a hex editor view shows the raw data of the selected sector (Sector 2,048 of 83,886,080). The hex data is displayed in columns, and the corresponding ASCII characters are shown to the right. The file system signature 'NTFS' is visible in the hex data.

On the right side, a properties panel for 'Hard disk 0' is shown:

- Model: VBOX HARDDISK
- Serial No.: VB3940070e-ba99833e
- Firmware Rev.: 1.0
- Bus: SATA
- Default Edit Mode: original
- State: original
- Undo level: 0
- Undo reverses: n/a
- Total capacity: 40.0 GB (42,949,672,960 bytes)
- Bytes per sector: 512
- Surplus sectors at end: 2048
- Partition: 1
- Relative sector No.: 0
- Mode: hexadecimal
- Offsets: hexadecimal
- Byte: 0
- Win: 8 Bit (±): -21
- Win: 16 Bit (±): 21,227
- Clip: 32 Bit (±): 1,318,081,259
- Binary: 11101011

The bottom status bar shows 'Sector 2,048 of 83,886,080', 'Offset: 100000', '= 235', and 'Block:'. The taskbar at the bottom includes icons for a web browser, file explorer, and other applications, along with the system clock showing '11:53 AM 9/28/2024'.

I selected Partition 1 (C:) with its NTFS file system.

## Step 5: Identify File Type

4D 5A

Also found: [4c 5a](#)

4F 52 4D ?? ?? ?? ??	FORM????AIF			Audio Interchange File Format
41 49 46 46			iff	
4C 5A 49 50	LZIP	0	lz	<a href="#">lzip compressed file</a> <sup>[20]</sup>
30 37 30 37 30 37	070707	0	cpio	<a href="#">cpio archive file</a> <sup>[21]</sup>
4D 5A	MZ	0	exe dll mui sys scr cpl ocx ax iec ime rs tsp fon efi	<a href="#">DOS MZ executable</a> and its descendants (including <a href="#">NE</a> and <a href="#">PE</a> )
53 4D 53 4E 46 32 30 30	SMSNF200	0	ssp	<a href="#">SmartSniff Packets File</a> <sup>[22]</sup>
5A 4D	ZM	0	exe	<a href="#">DOS ZM executable</a> and its descendants (rare)

I identified winhex.exe's file type to be a DOS MZ executable file.

### Step 6: Identify another file

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		ANSI	
0CFD1C000	45	56	46	09	0D	0A	FF	00	01	01	00	00	00	68	65	61	EVF	ÿ	
0CFD1C010	64	65	72	32	00	00	00	00	00	00	00	00	00	03	01	00	der2		
0CFD1C020	00	00	00	00	00	F6	00	00	00	00	00	00	00	00	00	00			

45 56 46 32	EVF2	0	Ex01	EnCase EWF version 2 format
45 56 46	EVF	0	e01	EnCase EWF version 1 format

I examined the case file from the previous lab and cross referenced it with the Wikipedia page to find that is an EnCase file type. The Hex byte value “45 56 46” has the ASCII representation of “EVF”.

## Task 2: Windows Registry

### Step 1: Download the subject image

This PC > Downloads > InCh05					Search InCh05
Name	Date modified	Type	Size		
InCh05	9/28/2024 12:14 PM	Application	11,015 KB		
InCh05	5/21/2020 11:24 AM	Disc Image File	983,040 KB		

Successfully downloaded the image file.

### Step 2: Create a Case

Manage Case					Hel
Select Case					
New Case...	Title	Create Date	Access Date	Location	
Import Case	✓ InChap05	9/28/2024, 12:19:06	9/28/2024, 12:19:06	C:\Users\jessica_win\Documents\PassMark\OSForensics\Ce	
Load Case	M57-Terrys USB Drive	9/20/2024, 18:29:05	9/28/2024, 12:17:38	C:\Users\jessica_win\Desktop\CSC 153\OSForensics_USB\	
Export Case	M57-Terrys USB Hard Drive	9/22/2024, 20:13:41	9/22/2024, 20:13:41	C:\Users\jessica_win\Desktop\CSC 153\USB\	
Delete Case					



Successfully created a case.

### Step 3: Investigate the Registry

Case Item ID	Title	Module	Case Item	Category
<b>Exported Items</b>				
1	Outlook e-mail address for...	Registry Viewer	RV 2024-09-28 19-26-29.html	
2	Denise Robinson's FTK Im...	Registry Viewer	RV 2024-09-28 19-33-33.html	
3	Denise Robinson's Notepa...	Registry Viewer	RV 2024-09-28 19-34-53.html	
4	Denise Robinson's Zoom A...	Registry Viewer	RV 2024-09-28 19-35-30.html	

I added four total keys after searching.

### Step 4: Generate a Report

**PassMark Software**  
www.osforensics.com

#### Uncategorized

##### Registry Artifacts

Case Item ID	Title	Date Added (UTC-7:00)	Additional Details
1	Outlook e-mail address for Denise Robinson	9/28/2024, 12:26:30	Filename: RV 2024-09-28 19-26-29.html Notes:
2	Denise Robinson's FTK Imager Application	9/28/2024, 12:33:33	Filename: RV 2024-09-28 19-33-33.html Notes:
3	Denise Robinson's Notepad Contents	9/28/2024, 12:34:53	Filename: RV 2024-09-28 19-34-53.html Notes:
4	Denise Robinson's Zoom Application	9/28/2024, 12:35:30	Filename: RV 2024-09-28 19-35-30.html Notes:

#### Case Narrative

[Case Info](#)

Case Materials

#### Categories

[Uncategorized](#)

The keys that I added in the previous step are now displayed in the report generated through OS Forensics.