Maria Valencia

CSC 153

Lab 5

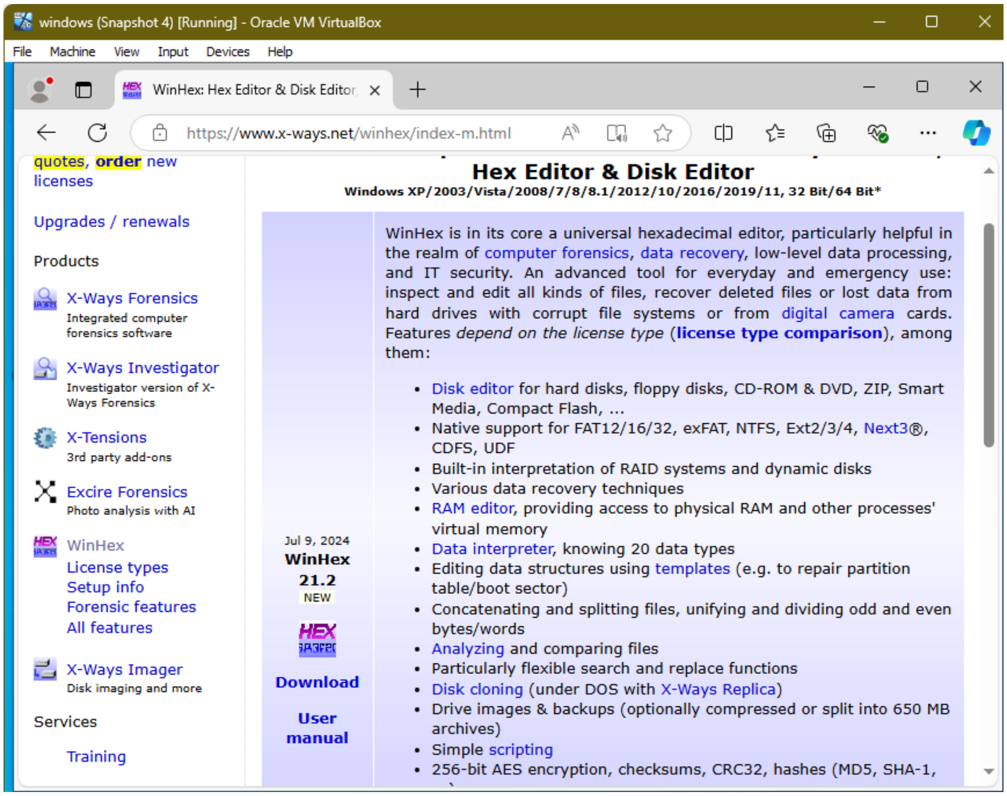
Disk and Registry Analysis

In this lab, I will explore the windows VM disk using WinHex and perform a forensic analysis of the Windows Registry found in the chapter 5 image file using OSForensics.

Task 1:

I will explore the Windows VM's disk using WinHex.

Step 1: I start the Windows VM and download the WinHex installation file.


windows (Snapshot 4) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
WinHex: Hex Editor & Disk Editor
https://www.x-ways.net/winhex/index-m.html

quotes, order new licenses

Upgrades / renewals

Products

X-Ways Forensics
Integrated computer forensics software

X-Ways Investigator
Investigator version of X-Ways Forensics

X-Tensions
3rd party add-ons

Excire Forensics
Photo analysis with AI

WinHex
License types
Setup info
Forensic features
All features

X-Ways Imager
Disk imaging and more

Services

Training

Hex Editor & Disk Editor

Windows XP/2003/Vista/2008/7/8/8.1/2012/10/2016/2019/11, 32 Bit/64 Bit*

Jul 9, 2024
WinHex 21.2
NEW

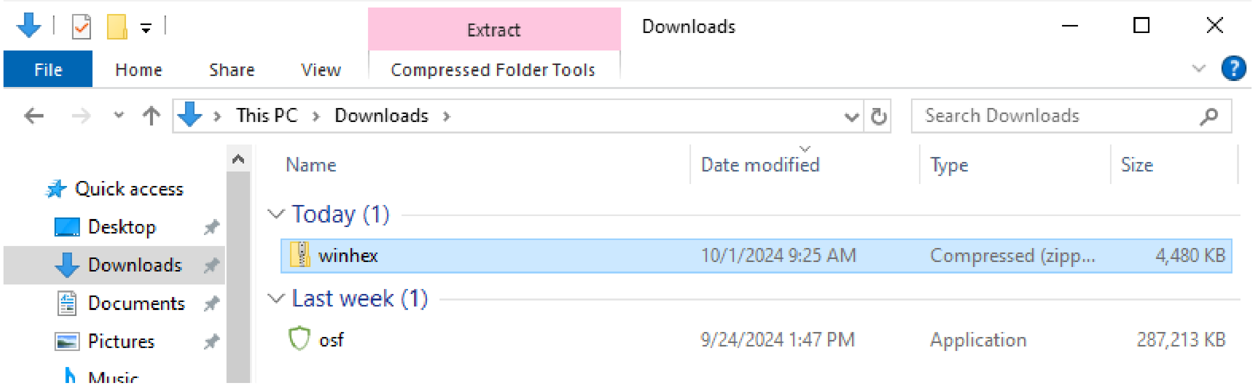
Download

User manual

WinHex is in its core a universal hexadecimal editor, particularly helpful in the realm of computer forensics, data recovery, low-level data processing, and IT security. An advanced tool for everyday and emergency use: inspect and edit all kinds of files, recover deleted files or lost data from hard drives with corrupt file systems or from digital camera cards. Features *depend on the license type* (**license type comparison**), among them:

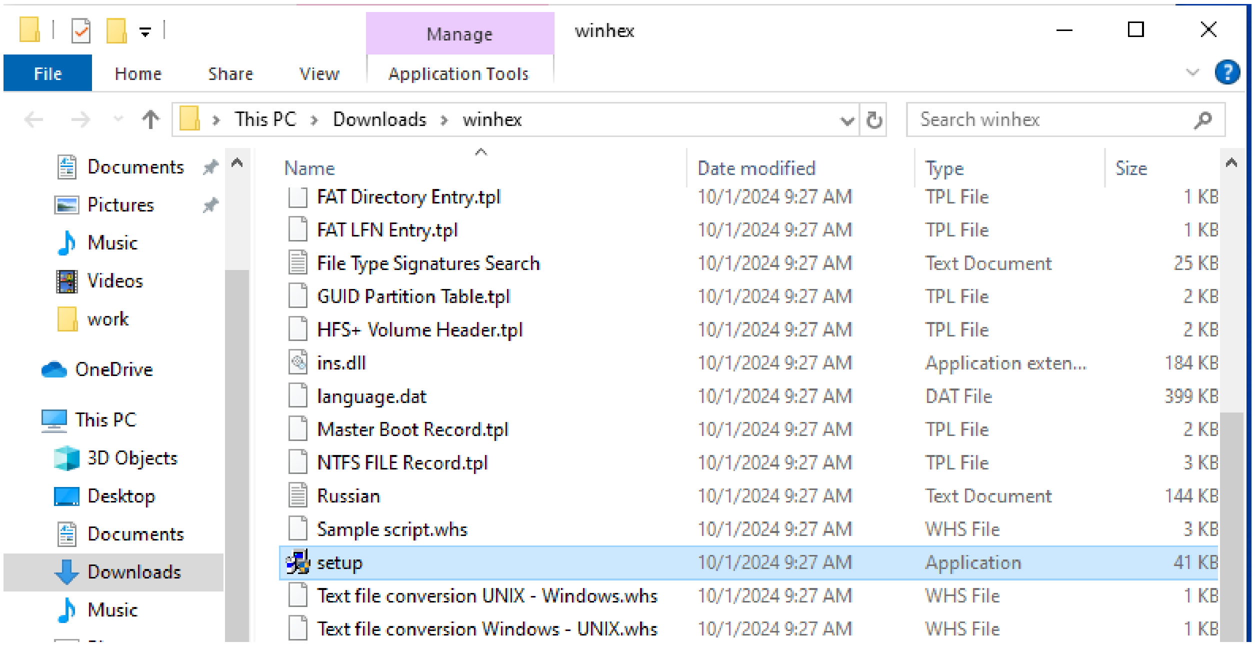
- Disk editor for hard disks, floppy disks, CD-ROM & DVD, ZIP, Smart Media, Compact Flash, ...
- Native support for FAT12/16/32, exFAT, NTFS, Ext2/3/4, Next3®, CDFS, UDF
- Built-in interpretation of RAID systems and dynamic disks
- Various data recovery techniques
- RAM editor, providing access to physical RAM and other processes' virtual memory
- Data interpreter, knowing 20 data types
- Editing data structures using templates (e.g. to repair partition table/boot sector)
- Concatenating and splitting files, unifying and dividing odd and even bytes/words
- Analyzing and comparing files
- Particularly flexible search and replace functions
- Disk cloning (under DOS with X-Ways Replica)
- Drive images & backups (optionally compressed or split into 650 MB archives)
- Simple scripting
- 256-bit AES encryption, checksums, CRC32, hashes (MD5, SHA-1,

Once the zip file was downloaded, I navigated over to my downloads folder and extracted the files.



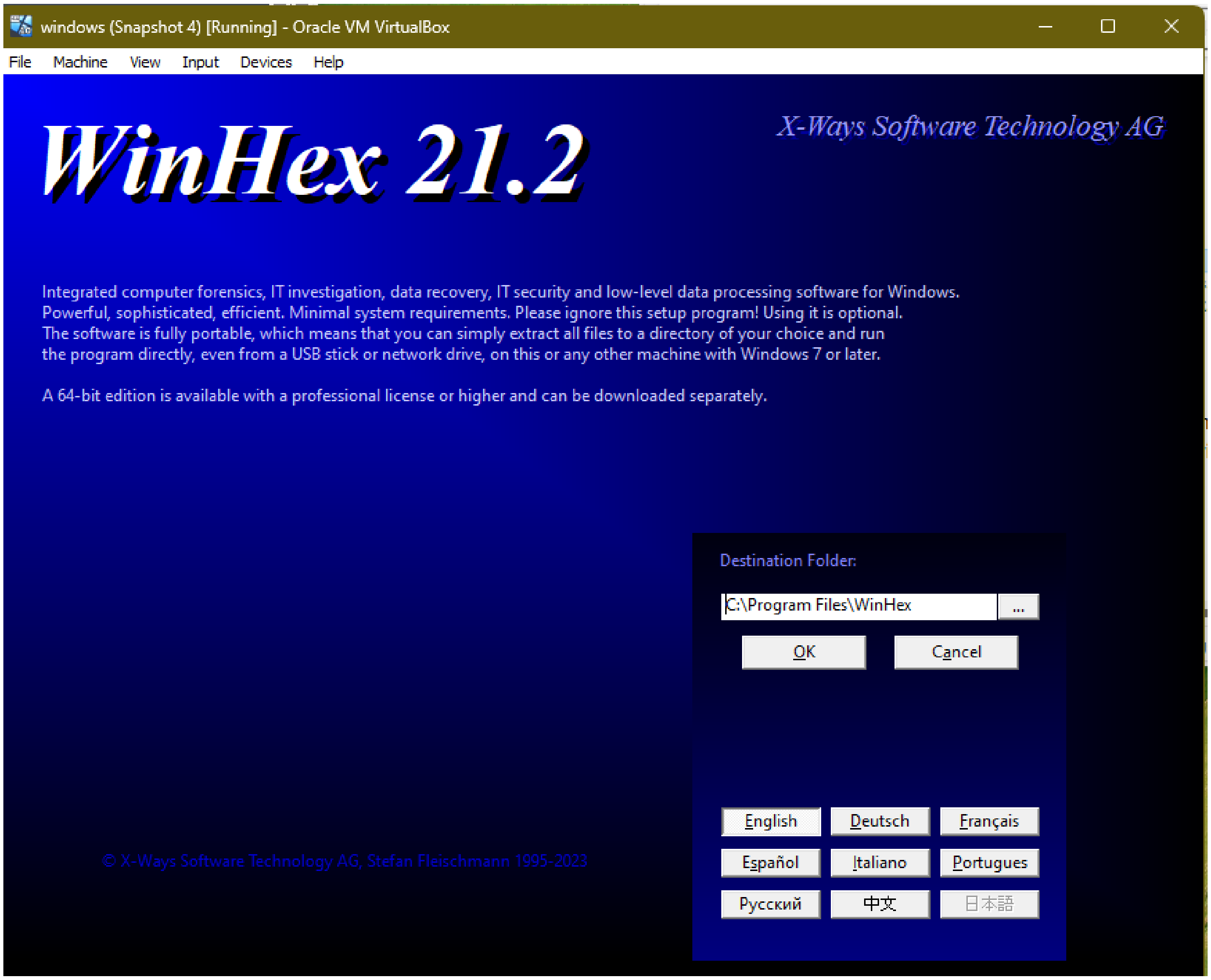
Name	Date modified	Type	Size
Today (1)			
winhex	10/1/2024 9:25 AM	Compressed (zipp...	4,480 KB
Last week (1)			
osf	9/24/2024 1:47 PM	Application	287,213 KB

I then installed WinHex by double clicking the set up application file in the extracted winhex folder within downloads and accepted the UAC prompt.



Name	Date modified	Type	Size
FAT Directory Entry.tpl	10/1/2024 9:27 AM	TPL File	1 KB
FAT LFN Entry.tpl	10/1/2024 9:27 AM	TPL File	1 KB
File Type Signatures Search	10/1/2024 9:27 AM	Text Document	25 KB
GUID Partition Table.tpl	10/1/2024 9:27 AM	TPL File	2 KB
HFS+ Volume Header.tpl	10/1/2024 9:27 AM	TPL File	2 KB
ins.dll	10/1/2024 9:27 AM	Application exten...	184 KB
language.dat	10/1/2024 9:27 AM	DAT File	399 KB
Master Boot Record.tpl	10/1/2024 9:27 AM	TPL File	2 KB
NTFS FILE Record.tpl	10/1/2024 9:27 AM	TPL File	3 KB
Russian	10/1/2024 9:27 AM	Text Document	144 KB
Sample script.whs	10/1/2024 9:27 AM	WHS File	3 KB
setup	10/1/2024 9:27 AM	Application	41 KB
Text file conversion UNIX - Windows.whs	10/1/2024 9:27 AM	WHS File	1 KB
Text file conversion Windows - UNIX.whs	10/1/2024 9:27 AM	WHS File	1 KB

I followed the installation wizard accepting the default destination folder. Pressed OK and then Yes to the set-up pop up and shortcut windows.



windows (Snapshot 4) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
WinHex 21.2
X-Ways Software Technology AG

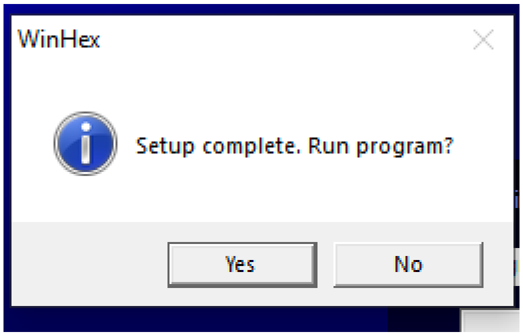
Integrated computer forensics, IT investigation, data recovery, IT security and low-level data processing software for Windows. Powerful, sophisticated, efficient. Minimal system requirements. Please ignore this setup program! Using it is optional. The software is fully portable, which means that you can simply extract all files to a directory of your choice and run the program directly, even from a USB stick or network drive, on this or any other machine with Windows 7 or later.

A 64-bit edition is available with a professional license or higher and can be downloaded separately.

Destination Folder: C:\Program Files\WinHex

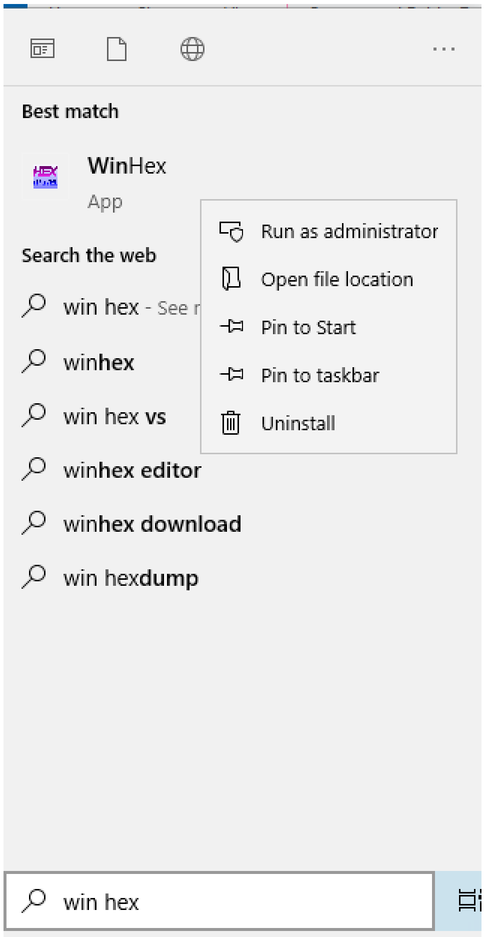
© X-Ways Software Technology AG, Stefan Fleischmann 1995-2023

Once the installation was completed, I selected NO to not start the program yet.

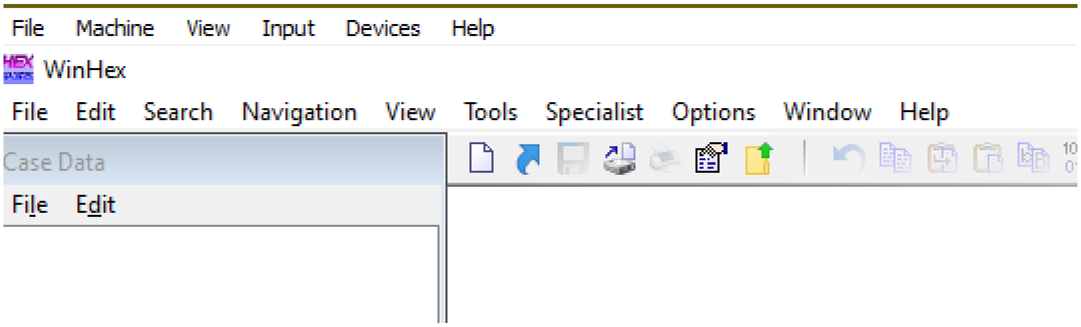


Setup complete. Run program?

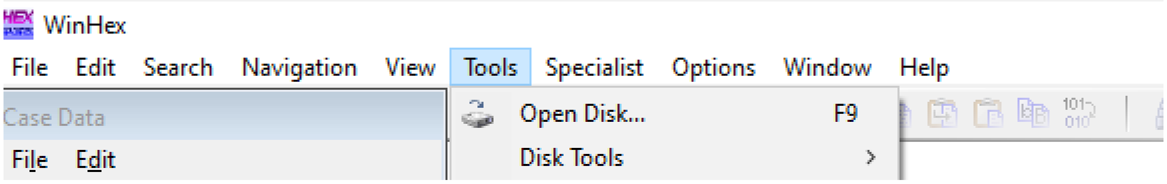
I start winhex by searching for the application in the windows search bar and launch it as administrator.



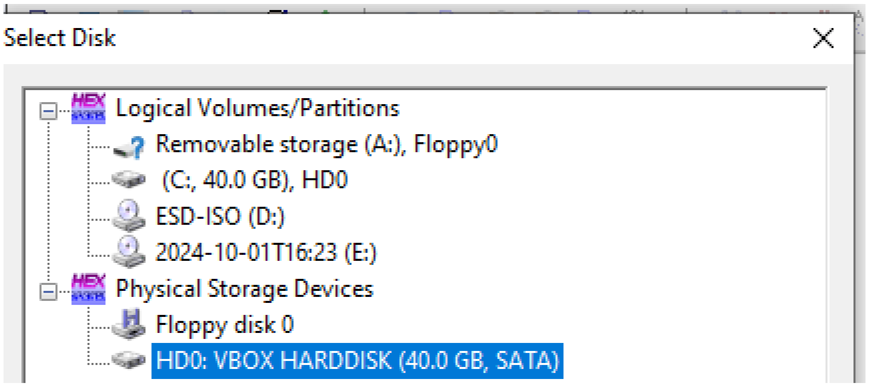
Program Runs!


File Machine View Input Devices Help
WinHex
File Edit Search Navigation View Tools Specialist Options Window Help
Case Data
File Edit

Step 2: I opened the Windows VM disk in WinHex by selecting the Tools menu and open disk option.

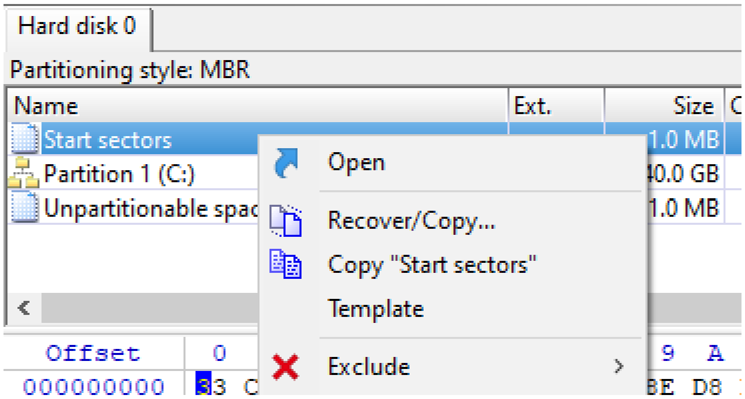


I select the HD0: VBOX HARDDISK and pressed ok.

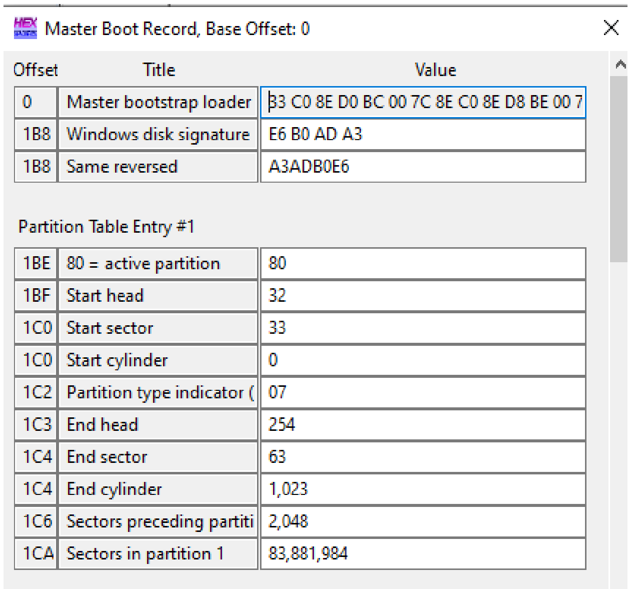


Step 3: I used WinHex's built-in templates to draw the master boot record.

I selected "Start Sectors" and right clicked and selected template.



I observed the master boot record template launched (1st partition entry offset 1BE is 80). Head is at offset 1BF with a value of 32.



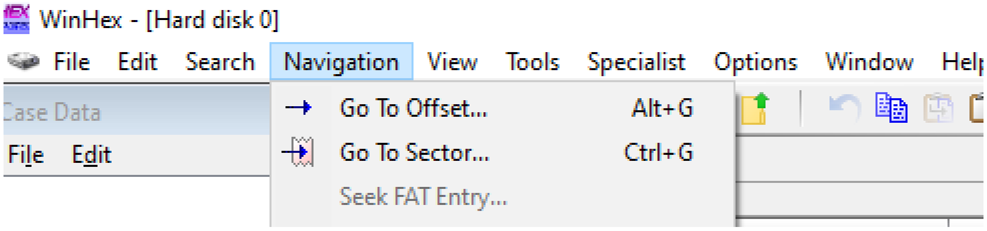
Master Boot Record, Base Offset: 0

Offset	Title	Value
0	Master bootstrap loader	33 C0 8E D0 BC 00 7C 8E C0 8E D8 BE 00 7
1B8	Windows disk signature	E6 B0 AD A3
1B8	Same reversed	A3ADB0E6

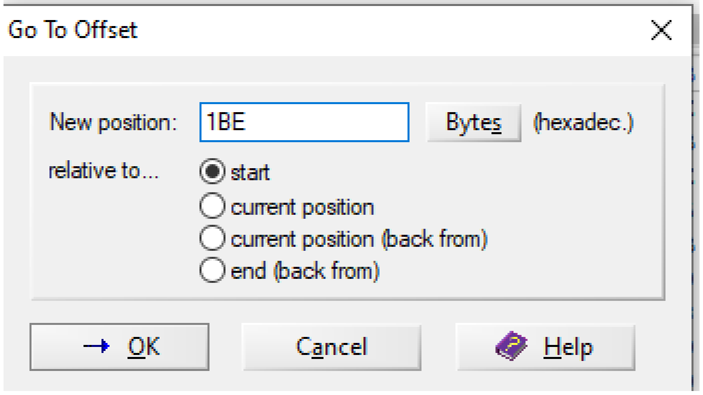
Partition Table Entry #1

Offset	Title	Value
1BE	80 = active partition	80
1BF	Start head	32
1C0	Start sector	33
1C0	Start cylinder	0
1C2	Partition type indicator (	07
1C3	End head	254
1C4	End sector	63
1C4	End cylinder	1,023
1C6	Sectors preceding partiti	2,048
1CA	Sectors in partition 1	83,881,984

I used the Go To function to jump to the first partition table entry. Selected Navigate from the menu and chose “Go to Offset”.



I entered 1BE in the New Position field and pressed OK.

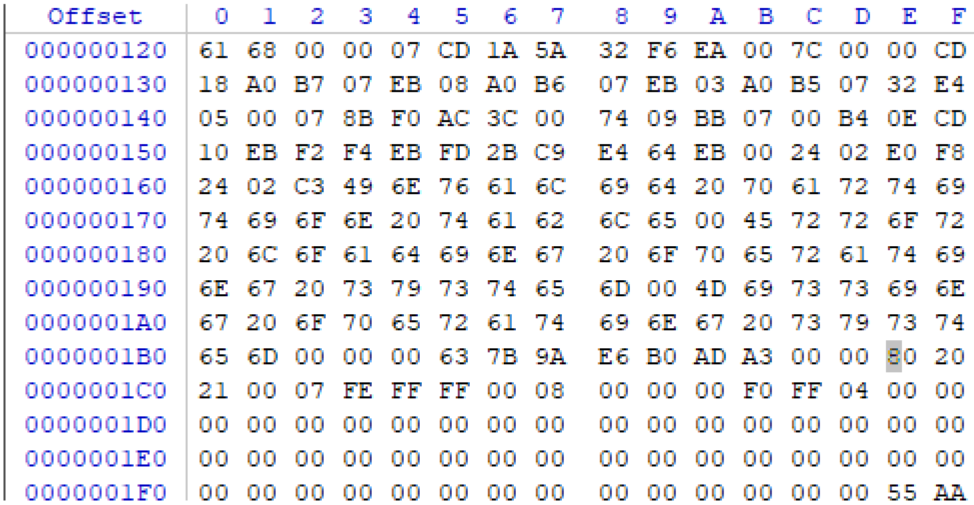


New position: 1BE Bytes (hexadec.)

relative to...

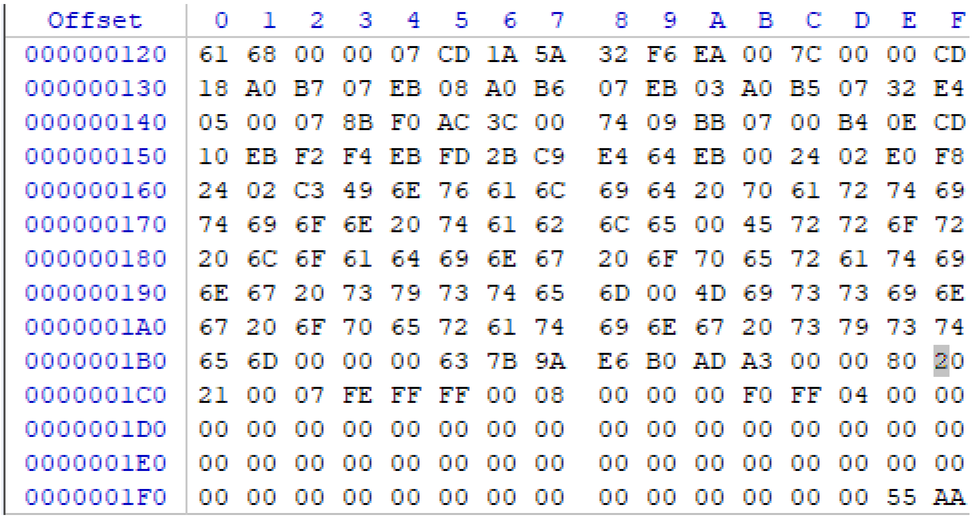
● start
○ current position
○ current position (back from)
○ end (back from)

I observed the cursor is set to Offset position 1BE in the main pane with the value 80. This is the same number that WinHex’s MBR template identified.



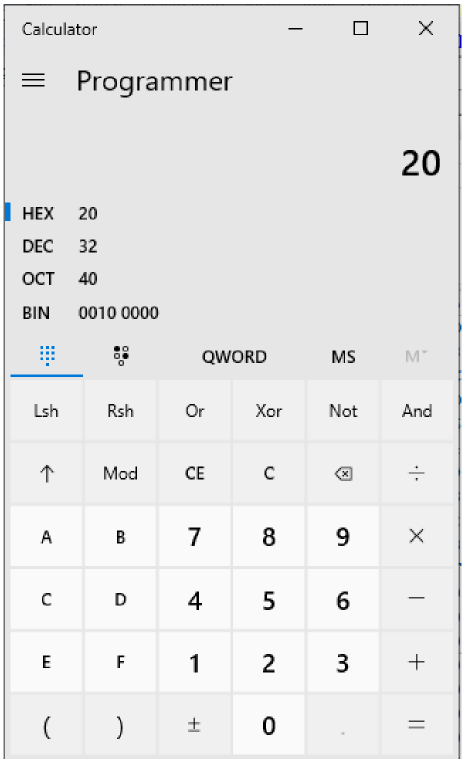
```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
000000120  61 68 00 00 07 CD 1A 5A  32 F6 EA 00 7C 00 00 CD
000000130  18 A0 B7 07 EB 08 A0 B6  07 EB 03 A0 B5 07 32 E4
000000140  05 00 07 8B F0 AC 3C 00  74 09 BB 07 00 B4 0E CD
000000150  10 EB F2 F4 EB FD 2B C9  E4 64 EB 00 24 02 E0 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  E6 B0 AD A3 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
```

Using navigate to offset again, I went to offset 1BF which is the next byte. I observed the value is 20 and not 32 as described in the template.



```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
000000120  61 68 00 00 07 CD 1A 5A  32 F6 EA 00 7C 00 00 CD
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  E6 B0 AD A3 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
```

The 20 value is hexadecimal while the 32 value from the template is in decimal. I converted hexadecimal 20 into decimal using Windows calculator. So I launched the calculator, switched to programmer mode, selected hex and entered 20. I observed that the DEC value is 32!



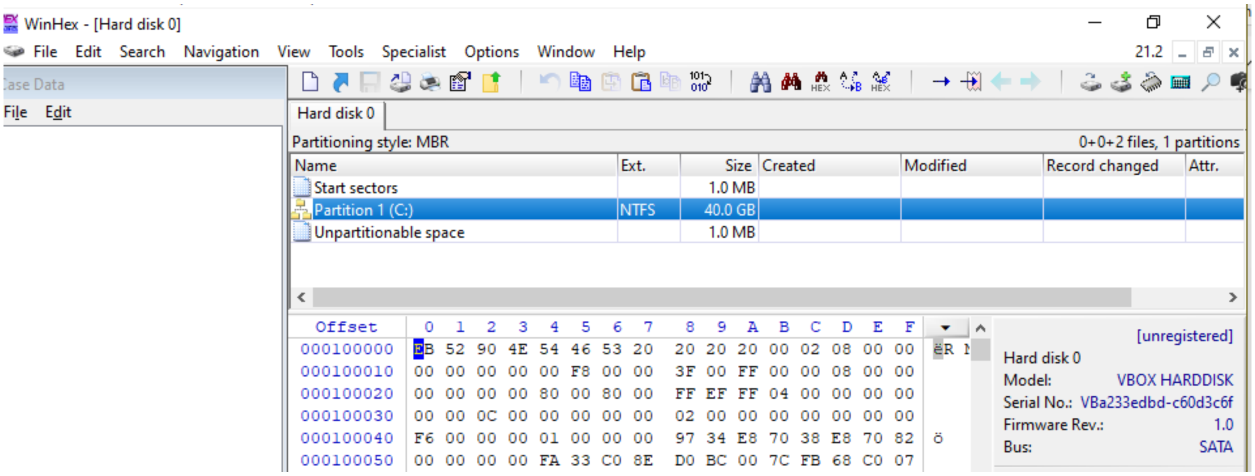
Calculator

Programmer

20

HEX	20
DEC	32
OCT	40
BIN	0010 0000

Step 4: I selected the partition 1(C:) and observed the NTFS file system.



WinHex - [Hard disk 0]

Partitioning style: MBR

0+0+2 files, 1 partitions

Name	Ext.	Size	Created	Modified	Record changed	Attr.
Start sectors		1.0 MB				
Partition 1 (C:)	NTFS	40.0 GB				
Unpartitionable space		1.0 MB				

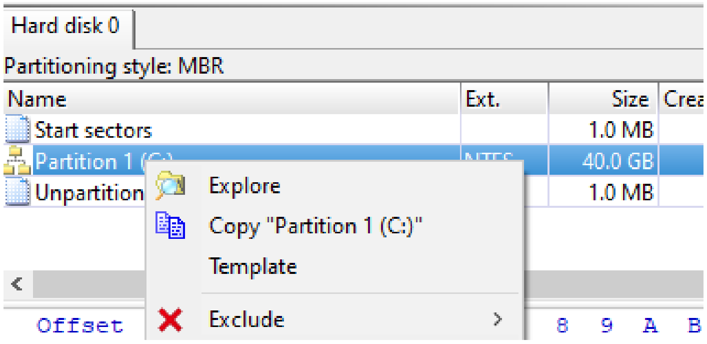
```
   Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
000100000    EB 52 90 4E 54 46 53 20  20 20 20 00 02 08 00 00   ëR N
000100010    00 00 00 00 00 F8 00 00  3F 00 FF 00 00 08 00 00
000100020    00 00 00 00 80 00 80 00  FF EF FF 04 00 00 00 00
000100030    00 00 0C 00 00 00 00 00  02 00 00 00 00 00 00 00
000100040    F6 00 00 00 01 00 00 00  97 34 E8 70 38 E8 70 82   ö
000100050    00 00 00 00 FA 33 C0 8E  D0 BC 00 7C FB 68 C0 07
```

[unregistered]

Hard disk 0

Model:	VBOX HARDDISK
Serial No.:	VBa233edbd-c60d3c6f
Firmware Rev.:	1.0
Bus:	SATA

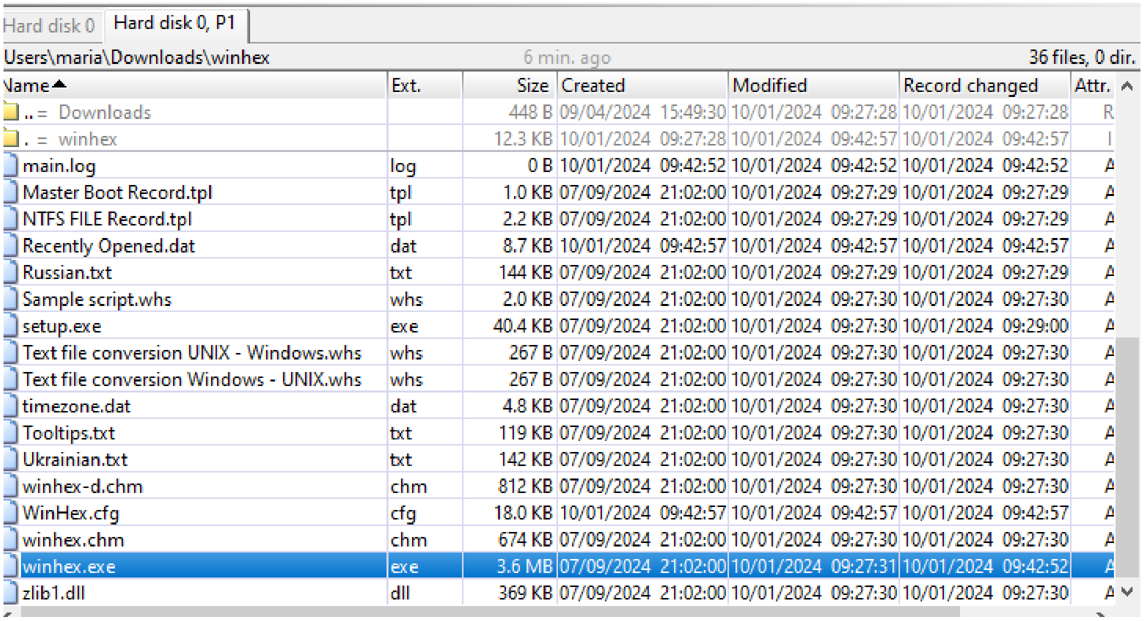
Step 5: I selected Partition 1 (C:) , right clicked and selected explore.



Partitioning style: MBR

Name	Ext.	Size	Crea
Start sectors		1.0 MB	
Partition 1 (C:)	NTFS	40.0 GB	
Unpartition		1.0 MB	

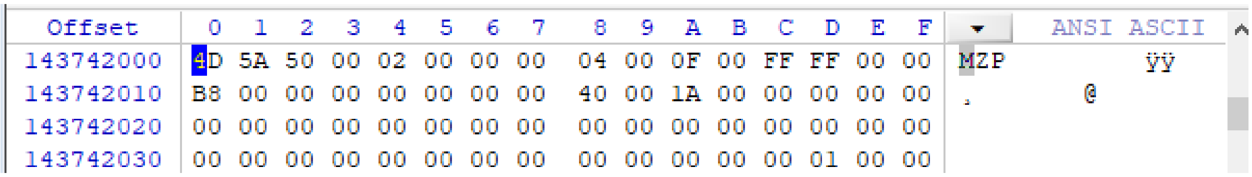
I observed the file directory of the hard disk that was displayed. Using that directory, I navigated to the downloads folder where WinHex was unzipped and selected the WinHex.exe file.



Users\maria\Downloads\winhex 6 min. ago 36 files, 0 dir.

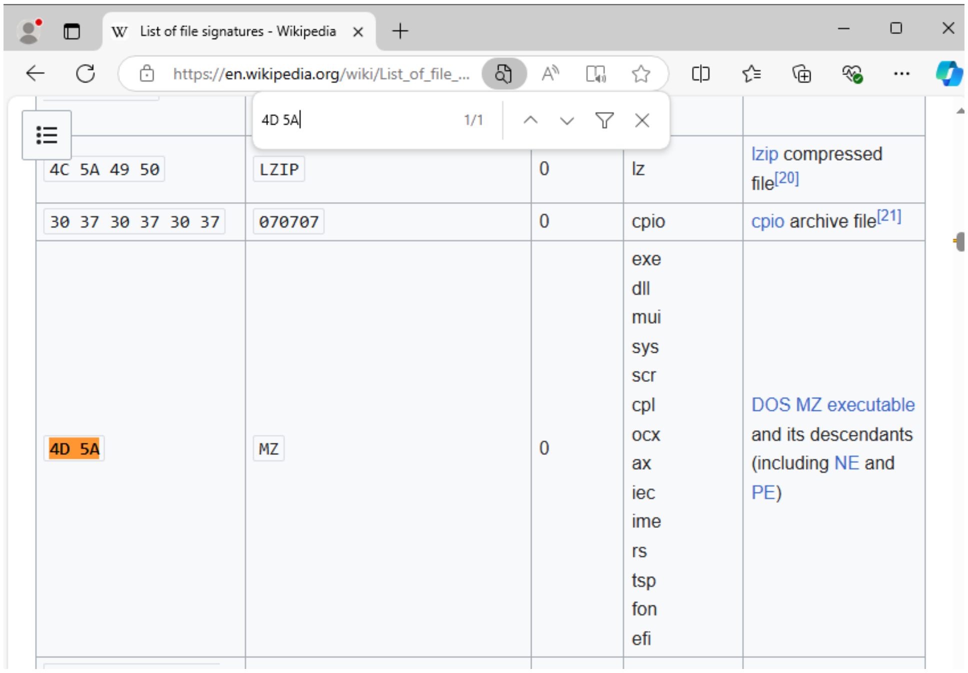
Name	Ext.	Size	Created	Modified	Record changed	Attr.
.. = Downloads		448 B	09/04/2024 15:49:30	10/01/2024 09:27:28	10/01/2024 09:27:28	R
. = winhex		12.3 KB	10/01/2024 09:27:28	10/01/2024 09:42:57	10/01/2024 09:42:57	I
main.log	log	0 B	10/01/2024 09:42:52	10/01/2024 09:42:52	10/01/2024 09:42:52	A
Master Boot Record.tpl	tpl	1.0 KB	07/09/2024 21:02:00	10/01/2024 09:27:29	10/01/2024 09:27:29	A
NTFS FILE Record.tpl	tpl	2.2 KB	07/09/2024 21:02:00	10/01/2024 09:27:29	10/01/2024 09:27:29	A
Recently Opened.dat	dat	8.7 KB	10/01/2024 09:42:57	10/01/2024 09:42:57	10/01/2024 09:42:57	A
Russian.txt	txt	144 KB	07/09/2024 21:02:00	10/01/2024 09:27:29	10/01/2024 09:27:29	A
Sample script.whs	whs	2.0 KB	07/09/2024 21:02:00	10/01/2024 09:27:30	10/01/2024 09:27:30	A
setup.exe	exe	40.4 KB	07/09/2024 21:02:00	10/01/2024 09:27:30	10/01/2024 09:29:00	A
Text file conversion UNIX - Windows.whs	whs	267 B	07/09/2024 21:02:00	10/01/2024 09:27:30	10/01/2024 09:27:30	A
Text file conversion Windows - UNIX.whs	whs	267 B	07/09/2024 21:02:00	10/01/2024 09:27:30	10/01/2024 09:27:30	A
timezone.dat	dat	4.8 KB	07/09/2024 21:02:00	10/01/2024 09:27:30	10/01/2024 09:27:30	A
Tooltips.txt	txt	119 KB	07/09/2024 21:02:00	10/01/2024 09:27:30	10/01/2024 09:27:30	A
Ukrainian.txt	txt	142 KB	07/09/2024 21:02:00	10/01/2024 09:27:30	10/01/2024 09:27:30	A
winhex-d.chm	chm	812 KB	07/09/2024 21:02:00	10/01/2024 09:27:30	10/01/2024 09:27:30	A
WinHex.cfg	cfg	18.0 KB	10/01/2024 09:42:57	10/01/2024 09:42:57	10/01/2024 09:42:57	A
winhex.chm	chm	674 KB	07/09/2024 21:02:00	10/01/2024 09:27:30	10/01/2024 09:27:30	A
winhex.exe	exe	3.6 MB	07/09/2024 21:02:00	10/01/2024 09:27:31	10/01/2024 09:42:52	A
zlib1.dll	dll	369 KB	07/09/2024 21:02:00	10/01/2024 09:27:30	10/01/2024 09:27:30	A

With the file selected, i selected the first two bytes and observed the ASCII representation is "MZ".



```
  Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F    ANSI ASCII
143742000   4D 5A 50 00 02 00 00 00  04 00 0F 00 FF FF 00 00   MZP         ÿÿ
143742010   B8 00 00 00 00 00 00 00  40 00 1A 00 00 00 00 00   ¸       @
143742020   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
143742030   00 00 00 00 00 00 00 00  00 00 00 00 00 01 00 00
```

I opened a browser and navigated to https://en.wikipedia.org/wiki/List_of_file_signatures and searched the pattern "4D 5A". I observed that this byte set represents DOS MZ executable files.

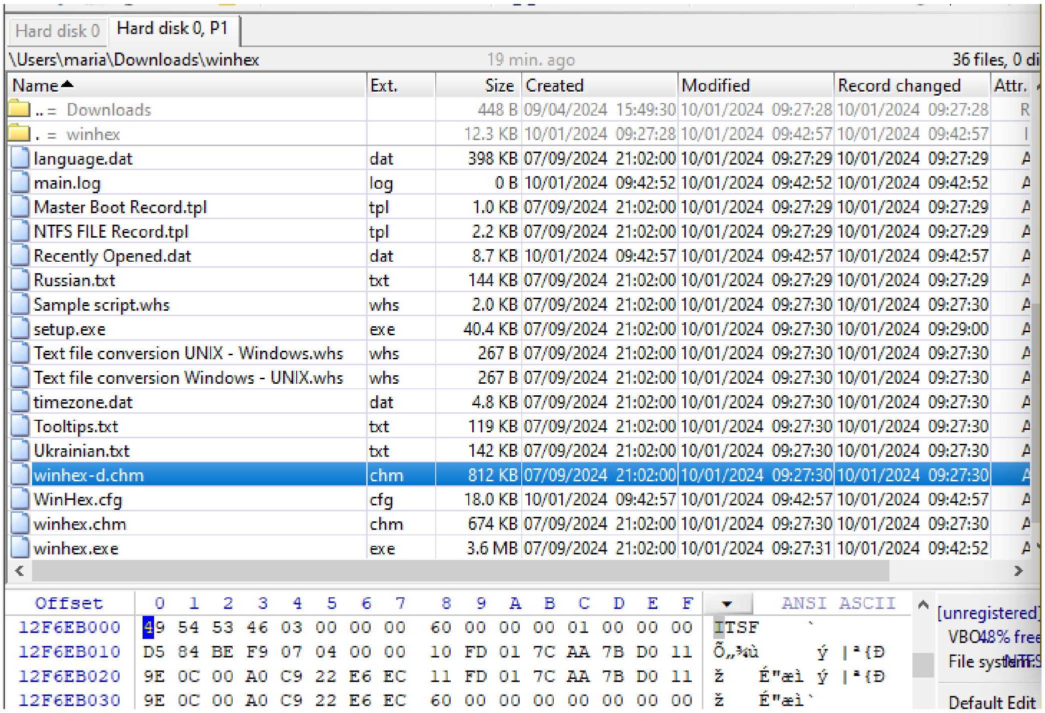


List of file signatures - Wikipedia
https://en.wikipedia.org/wiki/List_of_file_...
4D 5A
1/1

4C 5A 49 50	LZIP	0	lz	lzip compressed file[20]
30 37 30 37 30 37	070707	0	cpio	cpio archive file[21]
4D 5A	MZ	0	exe dll mui sys scr cpl ocx ax iec ime rs tsp fon efi	DOS MZ executable and its descendants (including NE and PE)

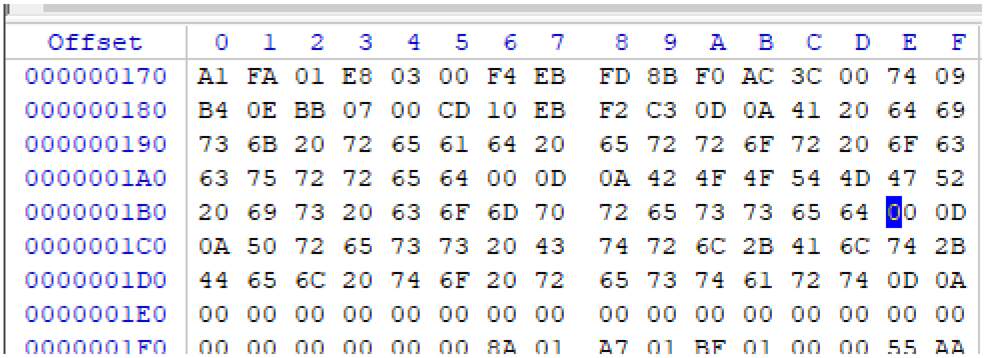
Step 6: I then found another file structure from the previous step.

I chose the winhex-d.chm file which is a MS Windows HTML data file . The ASCII representation is "ITSF", and the bytes were 00 00. This is because it is a null file.

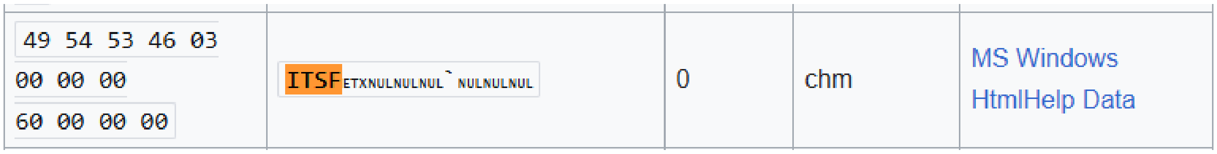


Name	Ext.	Size	Created	Modified	Record changed	Attr.
.. = Downloads		448 B	09/04/2024 15:49:30	10/01/2024 09:27:28	10/01/2024 09:27:28	R
. = winhex		12.3 KB	10/01/2024 09:27:28	10/01/2024 09:42:57	10/01/2024 09:42:57	I
language.dat	dat	398 KB	07/09/2024 21:02:00	10/01/2024 09:27:29	10/01/2024 09:27:29	A
main.log	log	0 B	10/01/2024 09:42:52	10/01/2024 09:42:52	10/01/2024 09:42:52	A
Master Boot Record.tpl	tpl	1.0 KB	07/09/2024 21:02:00	10/01/2024 09:27:29	10/01/2024 09:27:29	A
NTFS FILE Record.tpl	tpl	2.2 KB	07/09/2024 21:02:00	10/01/2024 09:27:29	10/01/2024 09:27:29	A
Recently Opened.dat	dat	8.7 KB	10/01/2024 09:42:57	10/01/2024 09:42:57	10/01/2024 09:42:57	A
Russian.txt	txt	144 KB	07/09/2024 21:02:00	10/01/2024 09:27:29	10/01/2024 09:27:29	A
Sample script.whs	whs	2.0 KB	07/09/2024 21:02:00	10/01/2024 09:27:30	10/01/2024 09:27:30	A
setup.exe	exe	40.4 KB	07/09/2024 21:02:00	10/01/2024 09:27:30	10/01/2024 09:29:00	A
Text file conversion UNIX - Windows.whs	whs	267 B	07/09/2024 21:02:00	10/01/2024 09:27:30	10/01/2024 09:27:30	A
Text file conversion Windows - UNIX.whs	whs	267 B	07/09/2024 21:02:00	10/01/2024 09:27:30	10/01/2024 09:27:30	A
timezone.dat	dat	4.8 KB	07/09/2024 21:02:00	10/01/2024 09:27:30	10/01/2024 09:27:30	A
Tooltips.txt	txt	119 KB	07/09/2024 21:02:00	10/01/2024 09:27:30	10/01/2024 09:27:30	A
Ukrainian.txt	txt	142 KB	07/09/2024 21:02:00	10/01/2024 09:27:30	10/01/2024 09:27:30	A
winhex-d.chm	chm	812 KB	07/09/2024 21:02:00	10/01/2024 09:27:30	10/01/2024 09:27:30	A
WinHex.cfg	cfg	18.0 KB	10/01/2024 09:42:57	10/01/2024 09:42:57	10/01/2024 09:42:57	A
winhex.chm	chm	674 KB	07/09/2024 21:02:00	10/01/2024 09:27:30	10/01/2024 09:27:30	A
winhex.exe	exe	3.6 MB	07/09/2024 21:02:00	10/01/2024 09:27:31	10/01/2024 09:42:52	A

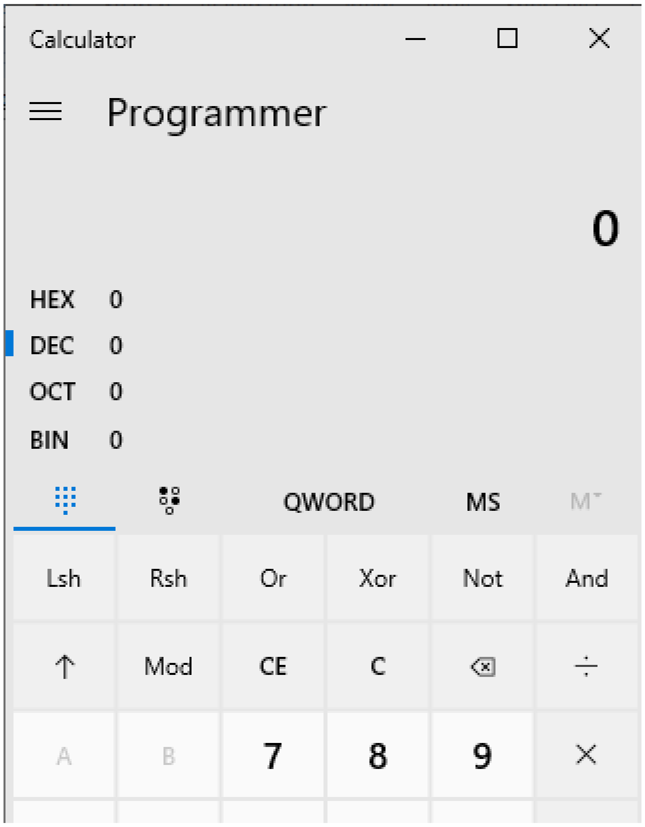
```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F     ANSI ASCII
12F6EB000  49 54 53 46 03 00 00 00  60 00 00 00 01 00 00 00  ITSF    `
12F6EB010  D5 84 BE F9 07 04 00 00  10 FD 01 7C AA 7B D0 11  Õ„¾ù      ý |ª{Ð
12F6EB020  9E 0C 00 A0 C9 22 E6 EC  11 FD 01 7C AA 7B D0 11  ž   É"æì ý |ª{Ð
12F6EB030  9E 0C 00 A0 C9 22 E6 EC  60 00 00 00 00 00 00 00  ž   É"æì`
```



```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
000000170  A1 FA 01 E8 03 00 F4 EB  FD 8B F0 AC 3C 00 74 09
000000180  B4 0E BB 07 00 CD 10 EB  F2 C3 0D 0A 41 20 64 69
000000190  73 6B 20 72 65 61 64 20  65 72 72 6F 72 20 6F 63
0000001A0  63 75 72 72 65 64 00 0D  0A 42 4F 4F 54 4D 47 52
0000001B0  20 69 73 20 63 6F 6D 70  72 65 73 73 65 64 00 0D
0000001C0  0A 50 72 65 73 73 20 43  74 72 6C 2B 41 6C 74 2B
0000001D0  44 65 6C 20 74 6F 20 72  65 73 74 61 72 74 0D 0A
0000001E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001F0  00 00 00 00 00 00 8A 01  A7 01 BF 01 00 00 55 AA
```



49 54 53 46 03 00 00 00 60 00 00 00	ITSFETXNULNULNUL` NULNULNUL	0	chm	MS Windows HtmlHelp Data



Calculator

Programmer

0

HEX 0

DEC 0

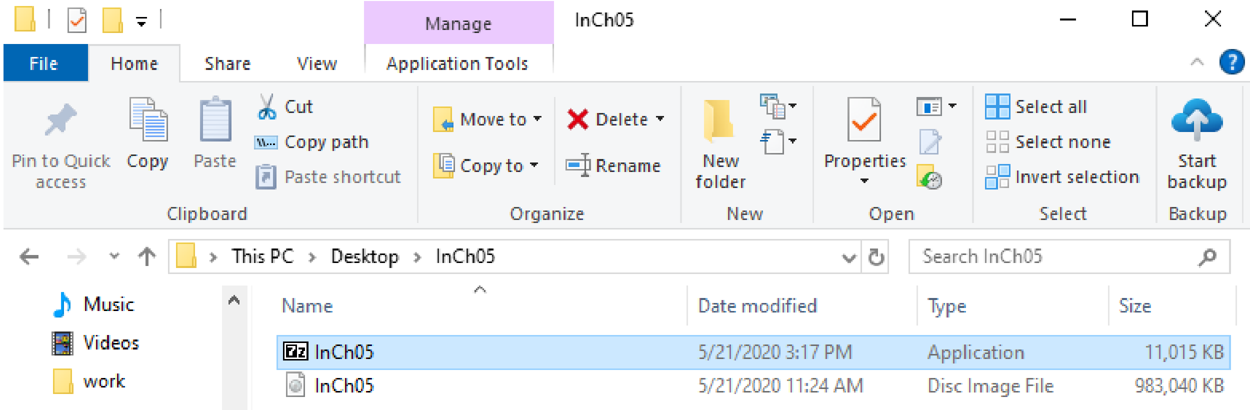
OCT 0

BIN 0

Task 2:

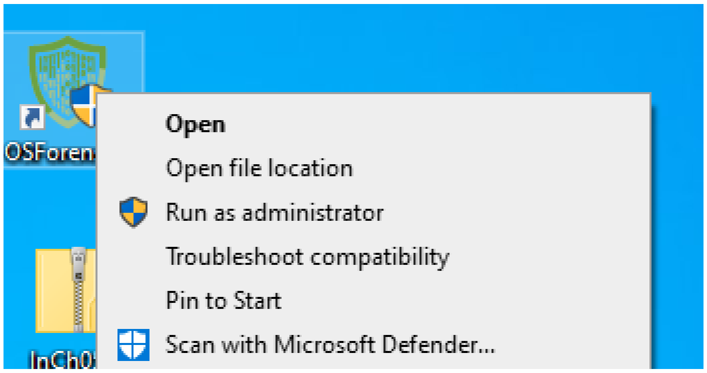
This task will use the textbook provided file and my windows VM to explore the subject image registry file in OSForensics.

Step 1: I downloaded “InChp05.zip” to the VM and extracted the file. Then I ran it to extract the image file.

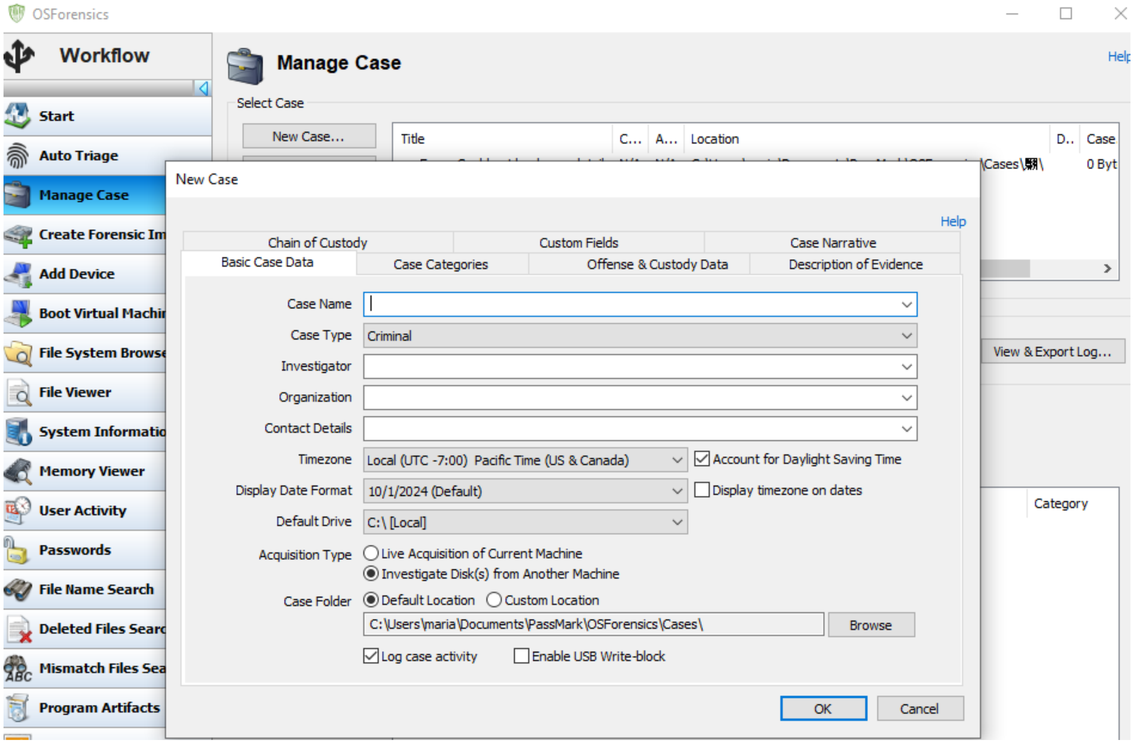


Name	Date modified	Type	Size
InCh05	5/21/2020 3:17 PM	Application	11,015 KB
InCh05	5/21/2020 11:24 AM	Disc Image File	983,040 KB

Step 2: I started the OSForensics as administrator and accepted the UAC prompt.

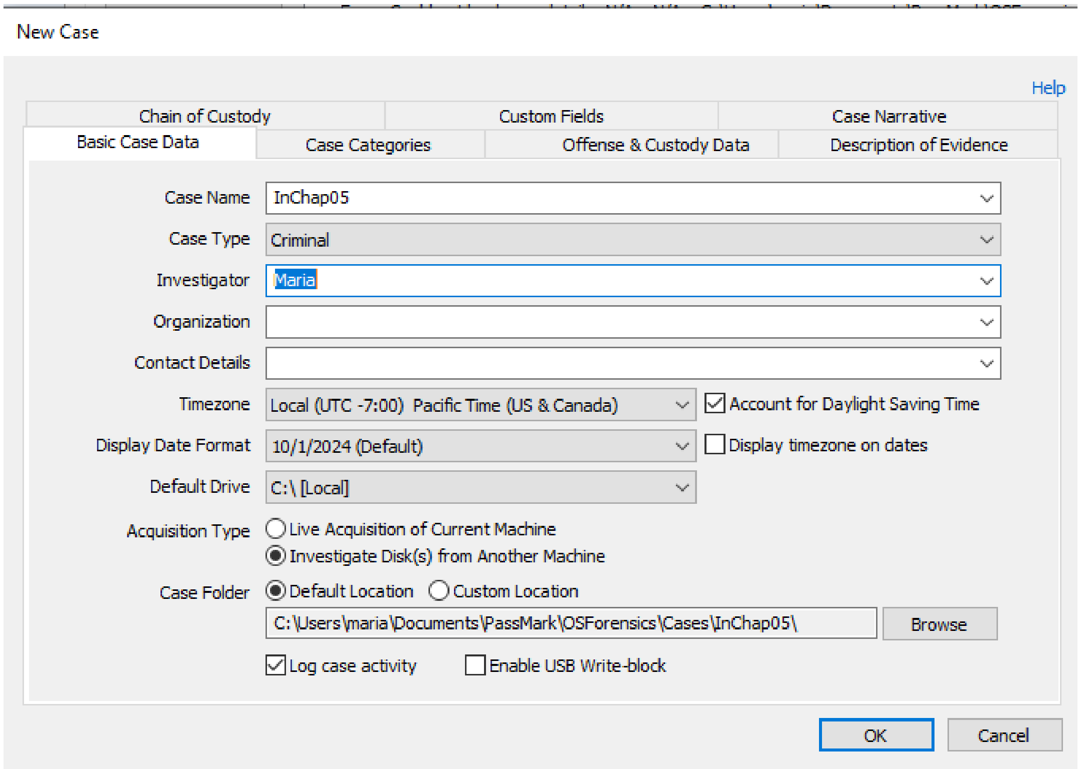


With OSForensics open, I created a new case by selecting Manage case -> new case



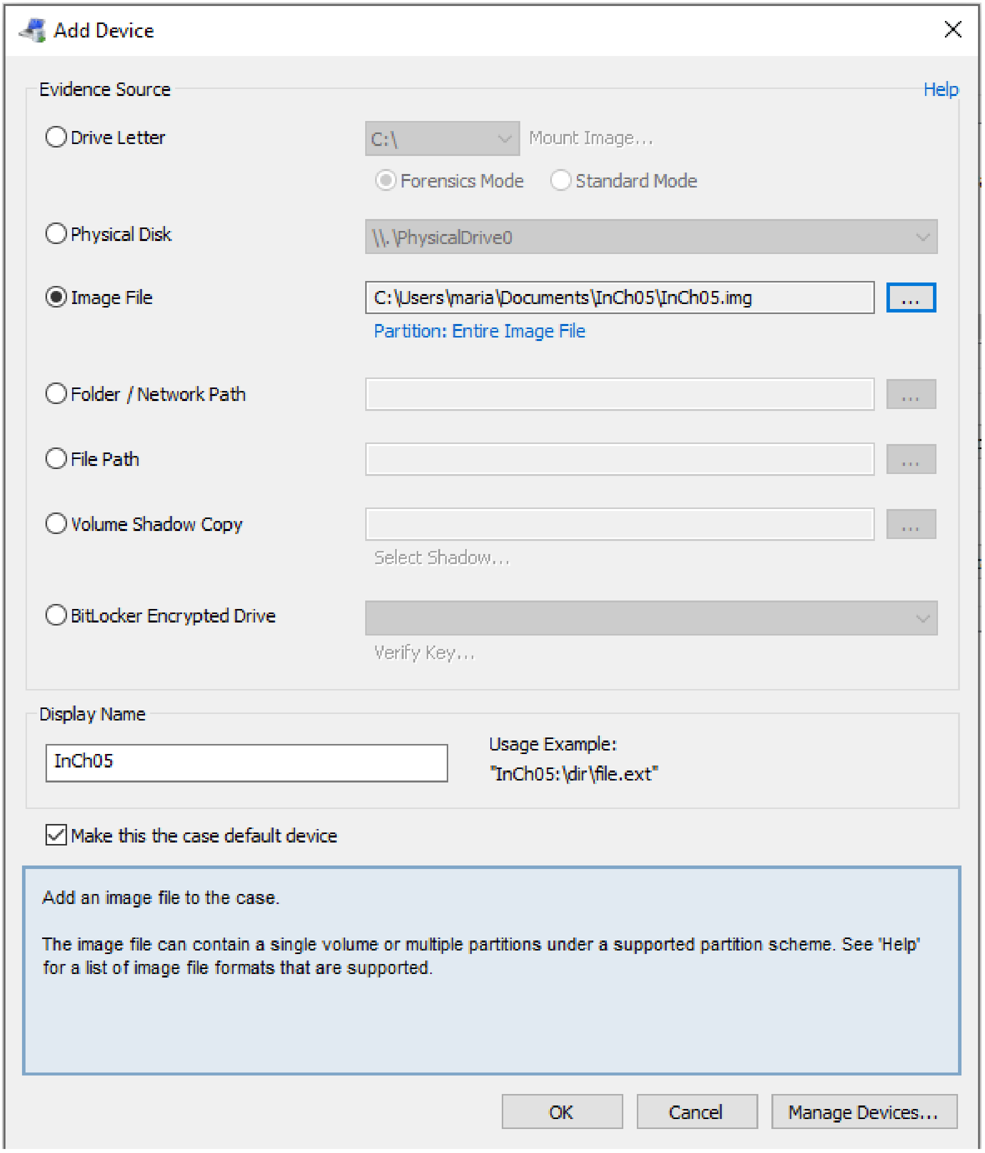
Case Name
Case Type: Criminal
Investigator
Organization
Contact Details
Timezone: Local (UTC -7:00) Pacific Time (US & Canada) ☑ Account for Daylight Saving Time
Display Date Format: 10/1/2024 (Default) □ Display timezone on dates
Default Drive: C:\ [Local]
Acquisition Type: ○ Live Acquisition of Current Machine ● Investigate Disk(s) from Another Machine
Case Folder: ● Default Location ○ Custom Location
C:\Users\maria\Documents\PassMark\OSForensics\Cases\
☑ Log case activity □ Enable USB Write-block

I then completed the New case Fields



Case Name: InChap05
Case Type: Criminal
Investigator: Maria
Organization
Contact Details
Timezone: Local (UTC -7:00) Pacific Time (US & Canada) ☑ Account for Daylight Saving Time
Display Date Format: 10/1/2024 (Default) □ Display timezone on dates
Default Drive: C:\ [Local]
Acquisition Type: ○ Live Acquisition of Current Machine ● Investigate Disk(s) from Another Machine
Case Folder: ● Default Location ○ Custom Location
C:\Users\maria\Documents\PassMark\OSForensics\Cases\InChap05\
☑ Log case activity □ Enable USB Write-block

With the add device open (it automatically opened, i did not need to click device...), I selected image file for the evidence source and navigate to the img file and pressed OK.



Add Device

Evidence Source

○ Drive Letter — C:\ — Mount Image...

● Forensics Mode ○ Standard Mode

○ Physical Disk — \\.\PhysicalDrive0

● Image File — C:\Users\maria\Documents\InCh05\InCh05.img

Partition: Entire Image File

○ Folder / Network Path

○ File Path

○ Volume Shadow Copy — Select Shadow...

○ BitLocker Encrypted Drive — Verify Key...

Display Name: InCh05

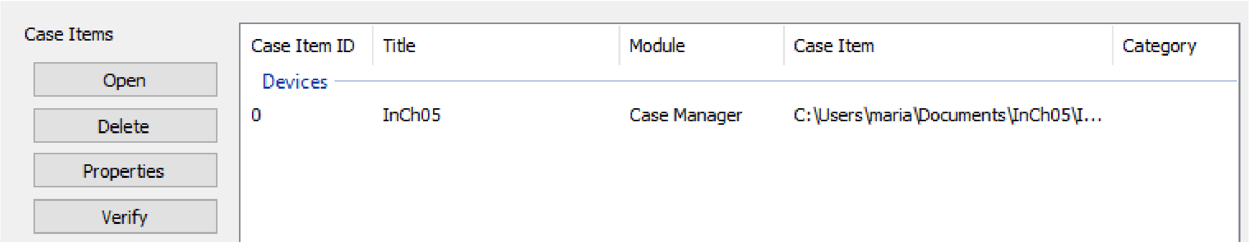
Usage Example:
"InCh05:\dir\file.ext"

☑ Make this the case default device

Add an image file to the case.

The image file can contain a single volume or multiple partitions under a supported partition scheme. See 'Help' for a list of image file formats that are supported.

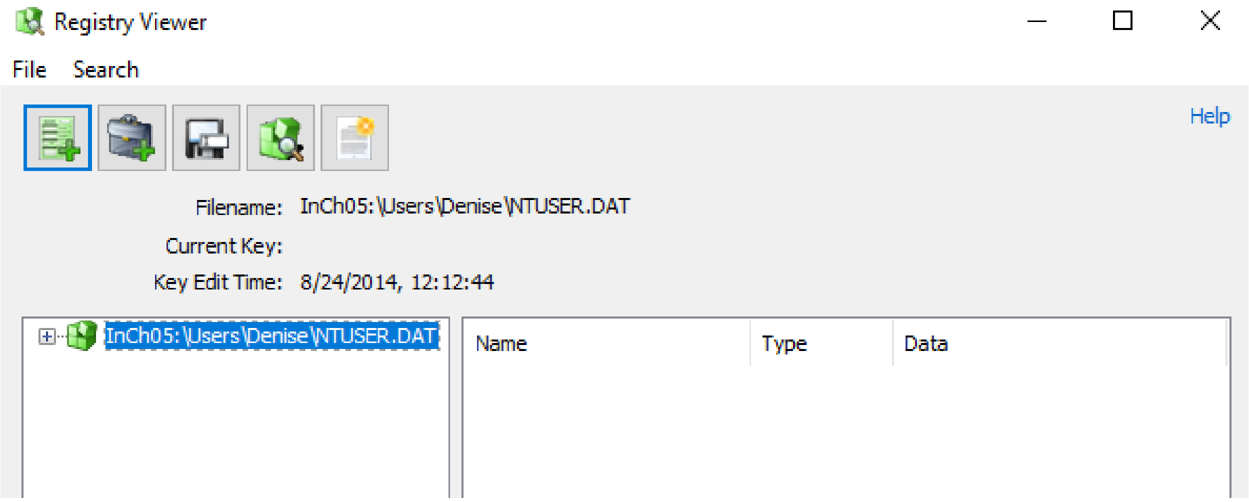
The img file now shows up on the case items section.



Case Items

Case Item ID	Title	Module	Case Item	Category
Devices				
0	InCh05	Case Manager	C:\Users\maria\Documents\InCh05\I...	

Step 3: I selected the registry viewer on the left navigation pane to launch the viewer. I observed the image file was auto mounted and an NTUSER.DAT file for the user Denise was detected. and I opened the file.



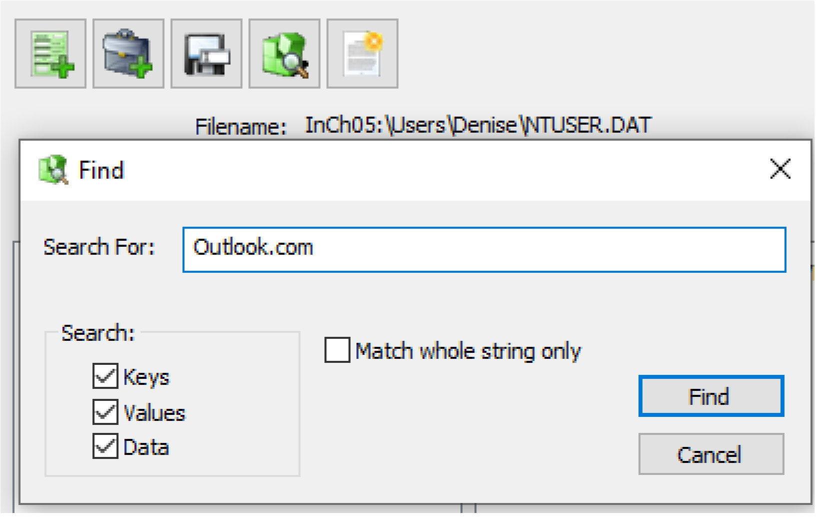
Filename: InCh05:\Users\Denise\NTUSER.DAT

Current Key:

Key Edit Time: 8/24/2014, 12:12:44

InCh05:\Users\Denise\NTUSER.DAT

I selected the find key/value button and searched for outlook.com.



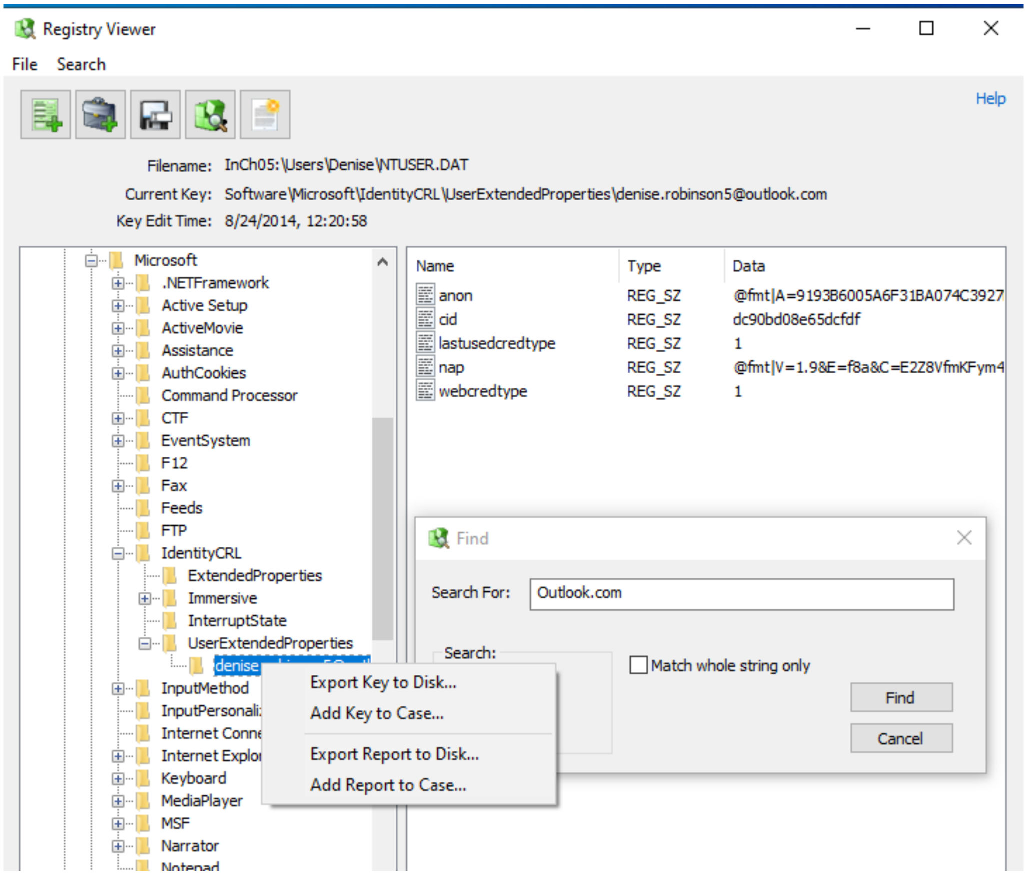
Filename: InCh05:\Users\Denise\NTUSER.DAT

Search For: Outlook.com

Search:
☑ Keys
☑ Values
☑ Data

□ Match whole string only

I right clicked the key and selected add key to case.



Filename: InCh05:\Users\Denise\NTUSER.DAT

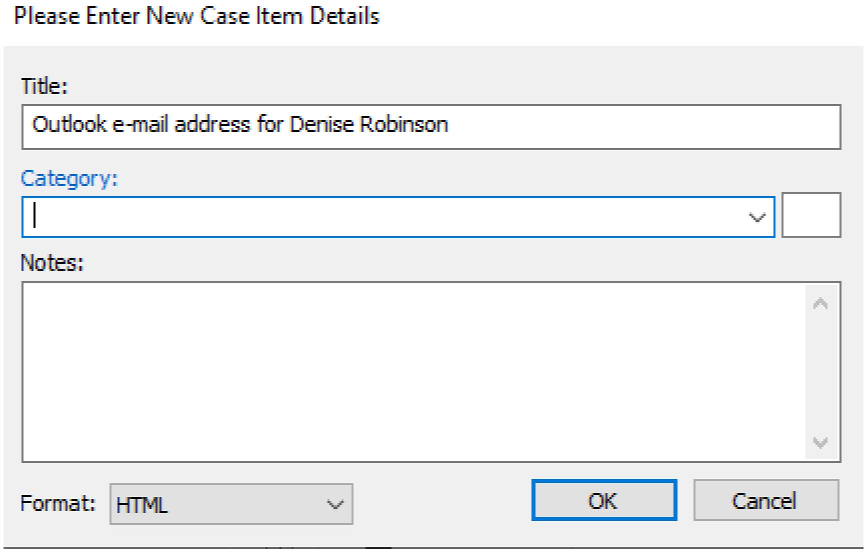
Current Key: Software\Microsoft\IdentityCRL\UserExtendedProperties\denise.robinson5@outlook.com

Key Edit Time: 8/24/2014, 12:20:58

Name	Type	Data
anon	REG_SZ	@fmt|A=9193B6005A6F31BA074C3927
cid	REG_SZ	dc90bd08e65dcfdf
lastusedcredtype	REG_SZ	1
nap	REG_SZ	@fmt|V=1.9&E=f8a&C=E2Z8VfmKFym4
webcredtype	REG_SZ	1

Search For: Outlook.com

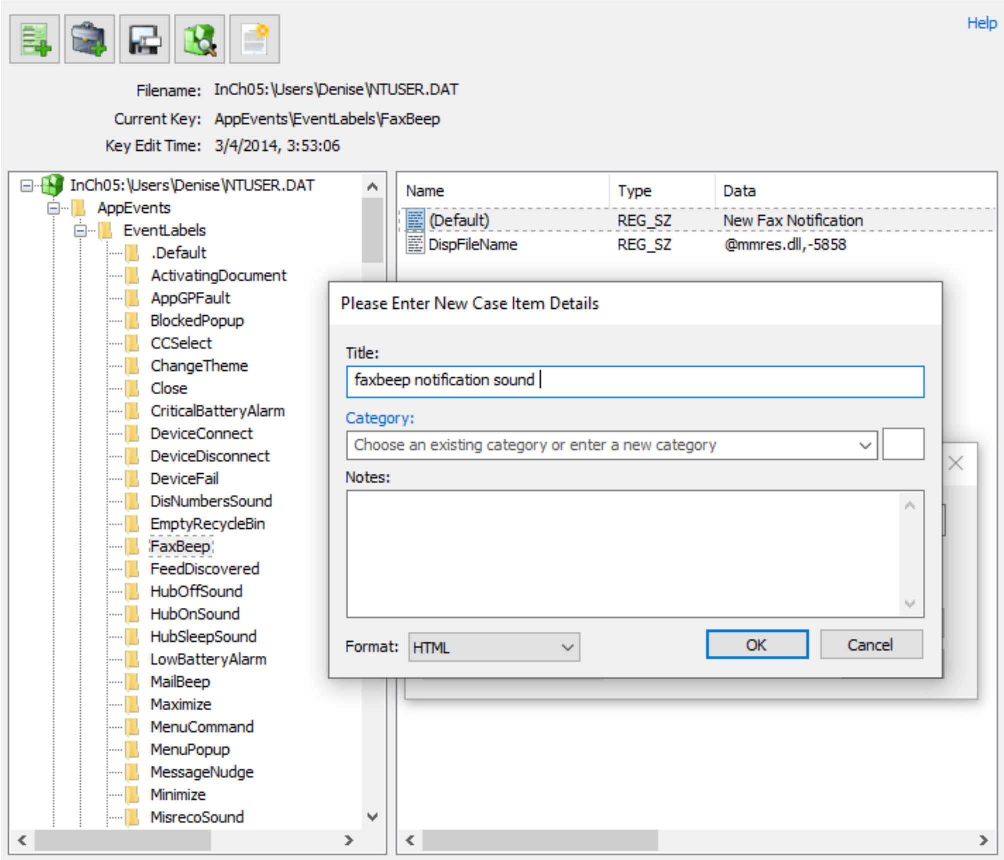
I then entered the title in the new case items details window



Title: Outlook e-mail address for Denise Robinson

Format: HTML

I then explored the register manually and found 3 other keys I found interesting and added them to the case.

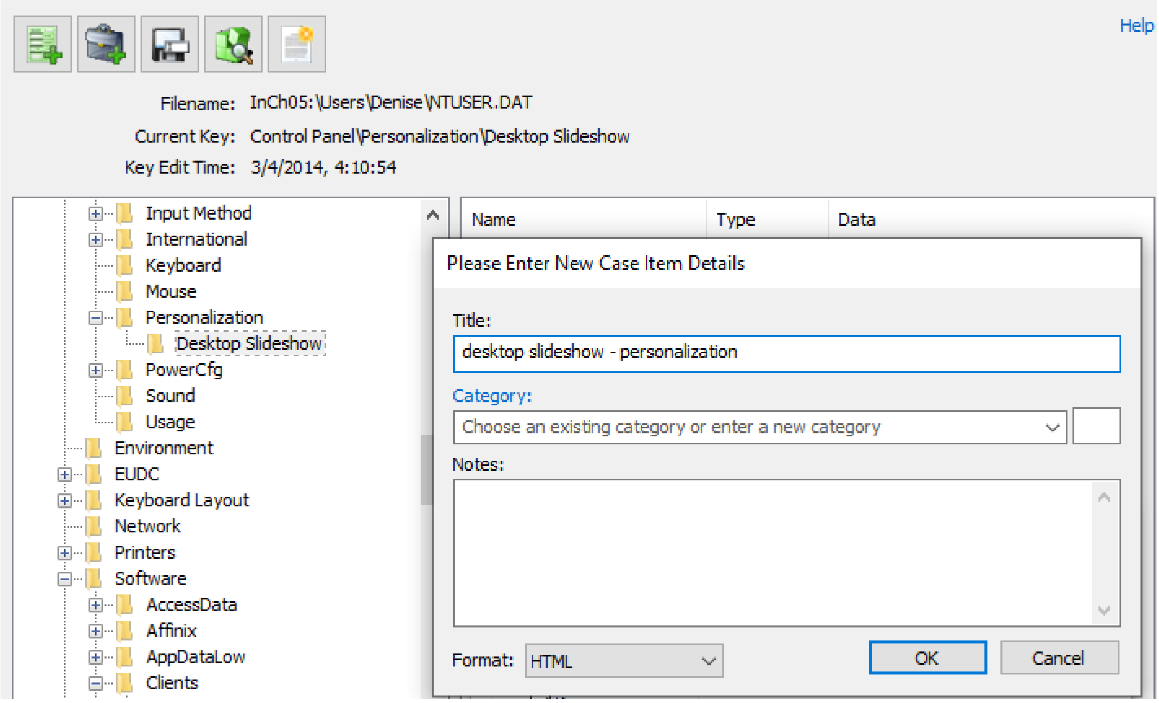


Filename: InCh05:\Users\Denise\NTUSER.DAT
Current Key: AppEvents\EventLabels\FaxBeep
Key Edit Time: 3/4/2014, 3:53:06

Name	Type	Data
(Default)	REG_SZ	New Fax Notification
DispFileName	REG_SZ	@mmres.dll,-5858

Title: faxbeep notification sound

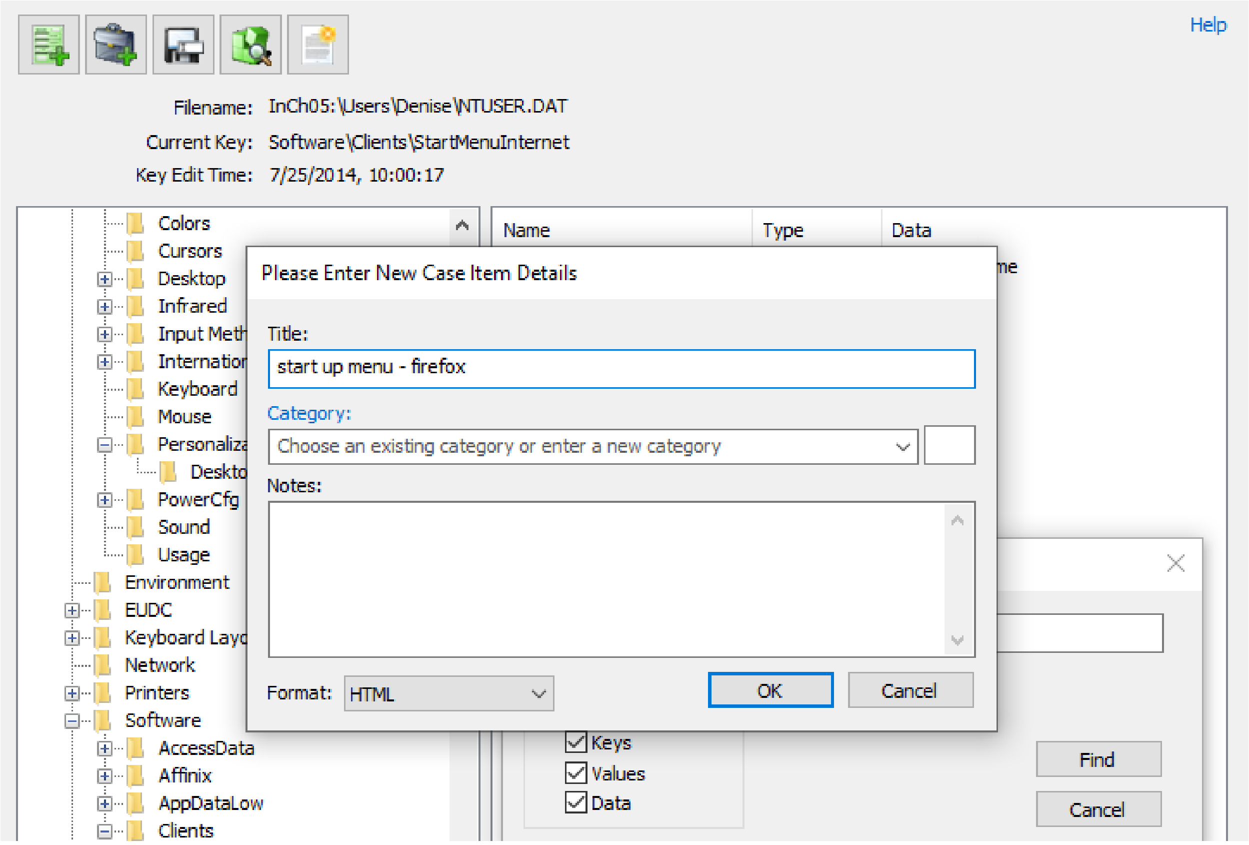
Format: HTML



Filename: InCh05:\Users\Denise\NTUSER.DAT
Current Key: Control Panel\Personalization\Desktop Slideshow
Key Edit Time: 3/4/2014, 4:10:54

Title: desktop slideshow - personalization

Format: HTML



Filename: InCh05:\Users\Denise\NTUSER.DAT

Current Key: Software\Clients\StartMenuInternet

Key Edit Time: 7/25/2014, 10:00:17

Please Enter New Case Item Details

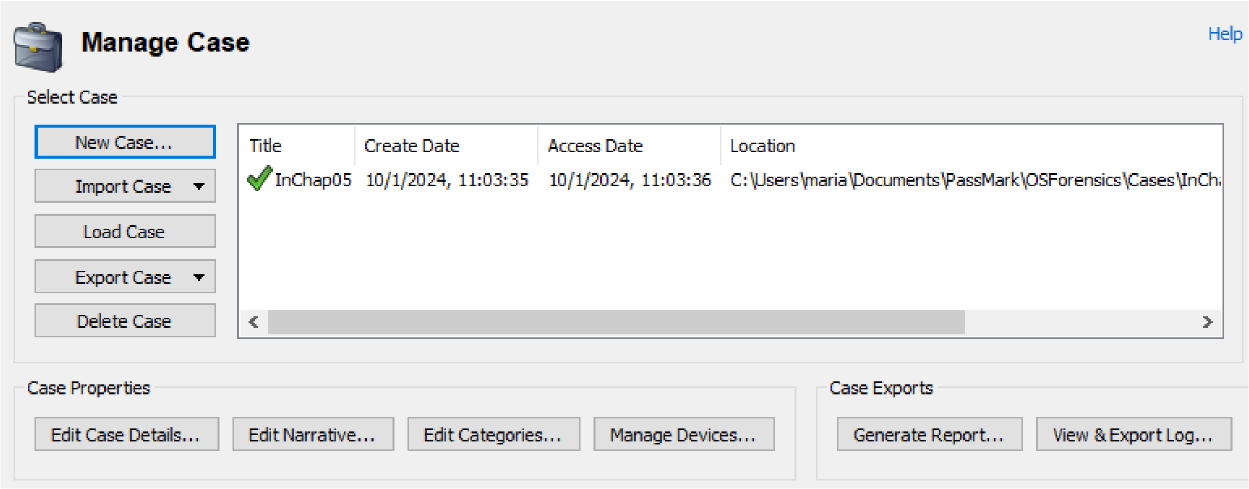
Title: start up menu - firefox

Category: Choose an existing category or enter a new category

Notes:

Format: HTML

Step 4: With the registry viewer closed, while in manage case, I selected generate report.

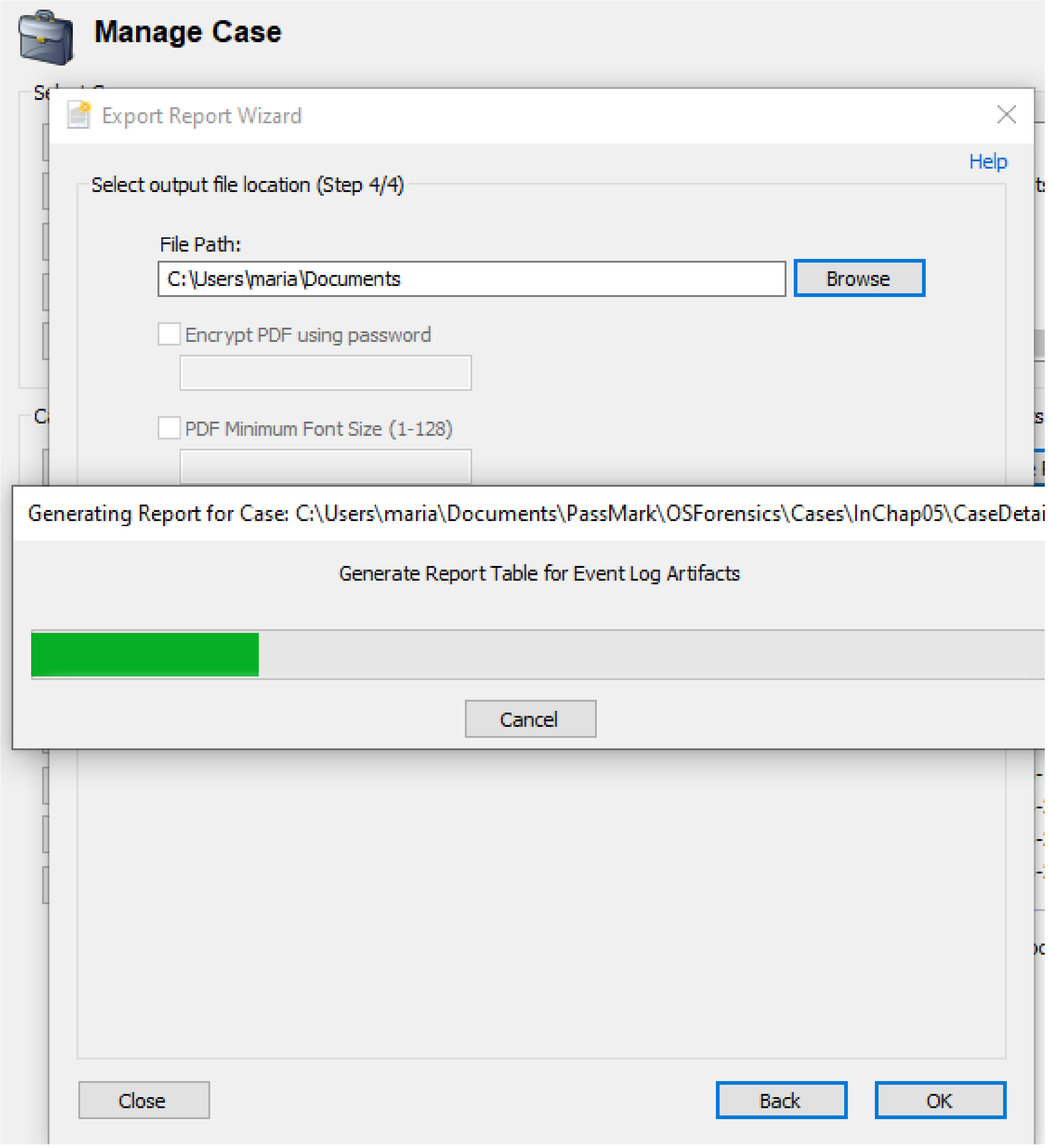


Manage Case

Select Case

Title	Create Date	Access Date	Location
✓ InChap05	10/1/2024, 11:03:35	10/1/2024, 11:03:36	C:\Users\maria\Documents\PassMark\OSForensics\Cases\InCh

I pressed Ok when the export report setting window launched to create the HTML report. I allowed the report to finish creating.



Select output file location (Step 4/4)

File Path: C:\Users\maria\Documents

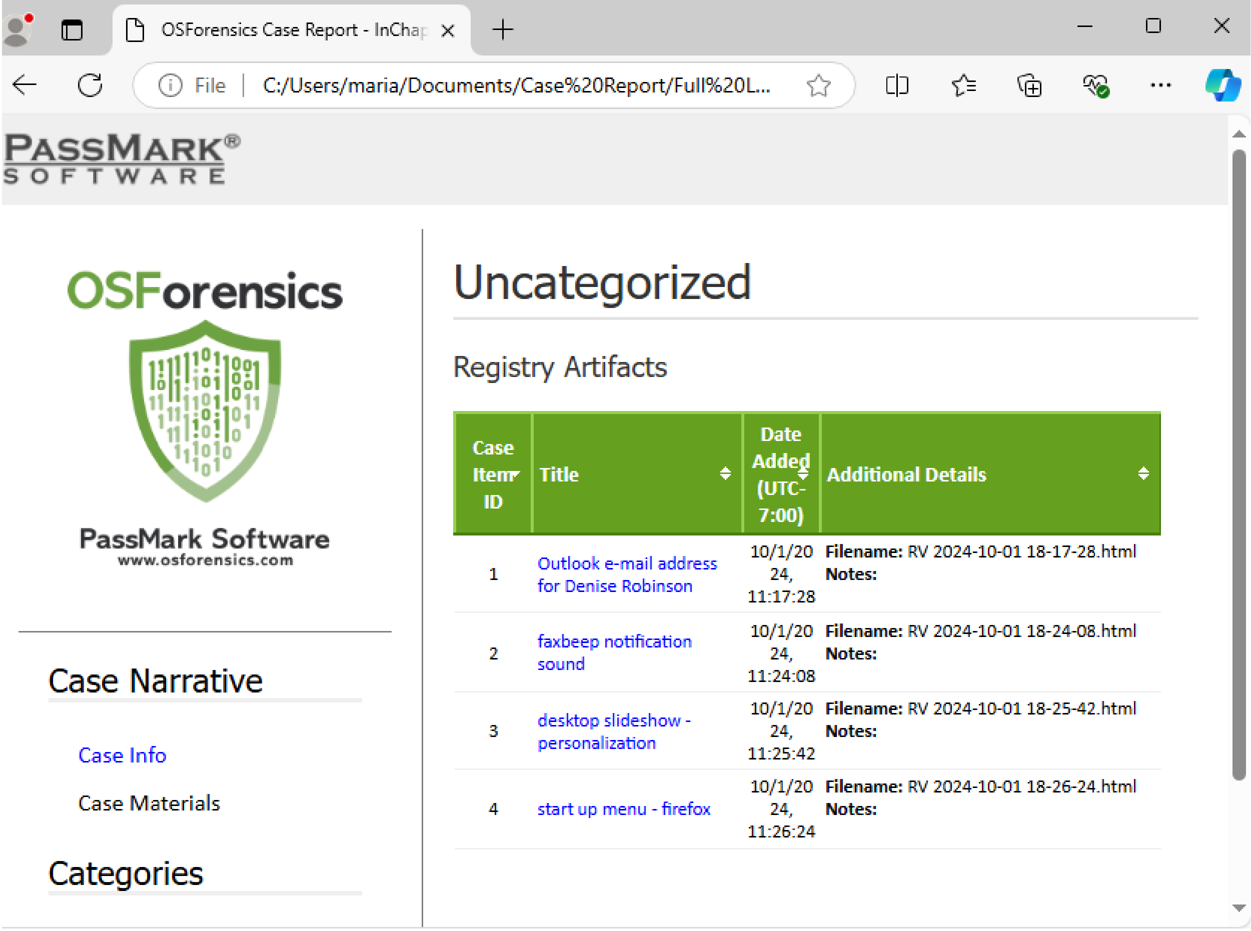
□ Encrypt PDF using password

□ PDF Minimum Font Size (1-128)

Generating Report for Case: C:\Users\maria\Documents\PassMark\OSForensics\Cases\InChap05\CaseDetai

Generate Report Table for Event Log Artifacts

I reviewed the report and navigated to the 4 registry artifacts I found and added to my case.



Uncategorized

Registry Artifacts

Case Item ID	Title	Date Added (UTC-7:00)	Additional Details
1	Outlook e-mail address for Denise Robinson	10/1/2024, 11:17:28	**Filename:** RV 2024-10-01 18-17-28.html **Notes:**
2	faxbeep notification sound	10/1/2024, 11:24:08	**Filename:** RV 2024-10-01 18-24-08.html **Notes:**
3	desktop slideshow - personalization	10/1/2024, 11:25:42	**Filename:** RV 2024-10-01 18-25-42.html **Notes:**
4	start up menu - firefox	10/1/2024, 11:26:24	**Filename:** RV 2024-10-01 18-26-24.html **Notes:**