

Maria Valencia

CSC 153

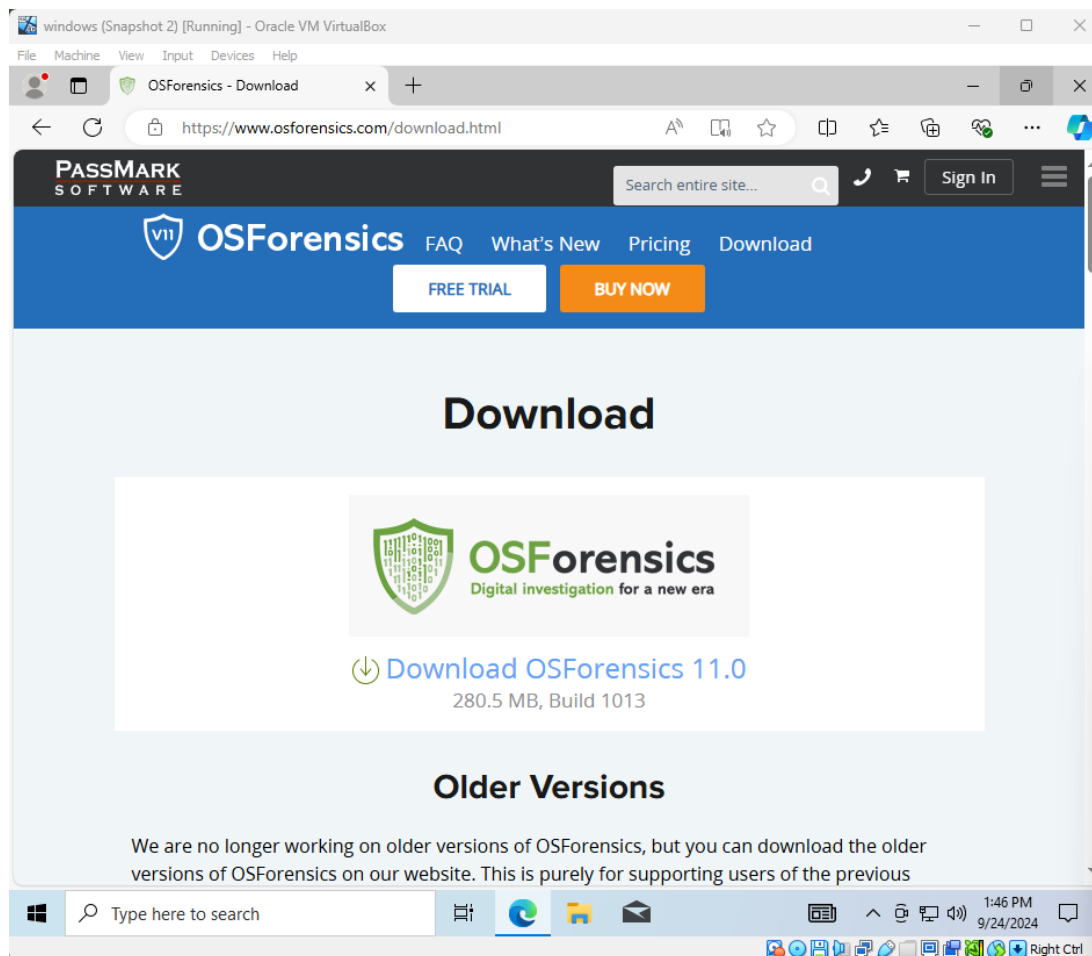
Lab 4

OS Forensics USB case

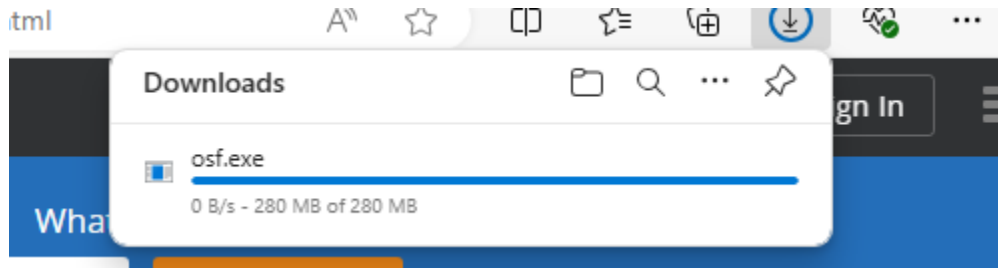
In this lab, I completed the Hands-On project 4-3 on page 190 in the textbook. I was required to install OSForensics on my windows VM and investigated Terry's USB drive.

Task 1:

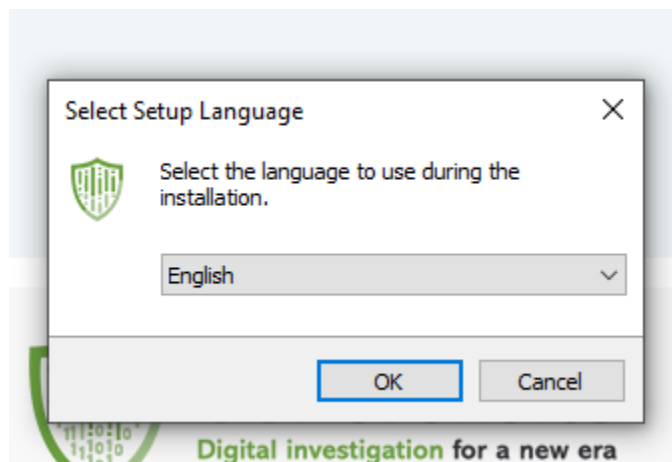
In this task, I installed OSForensics on my windows VM.



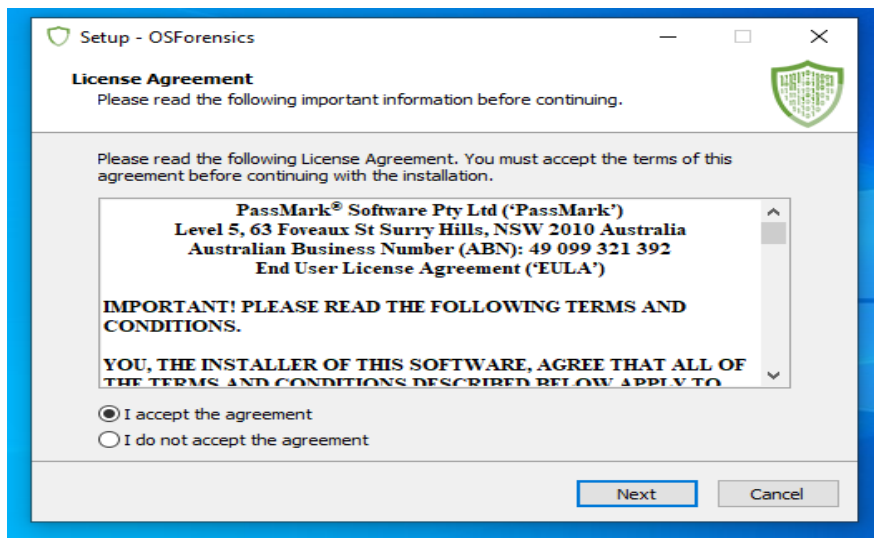
After it was downloaded, I ran the osf.exe from the downloads folder.



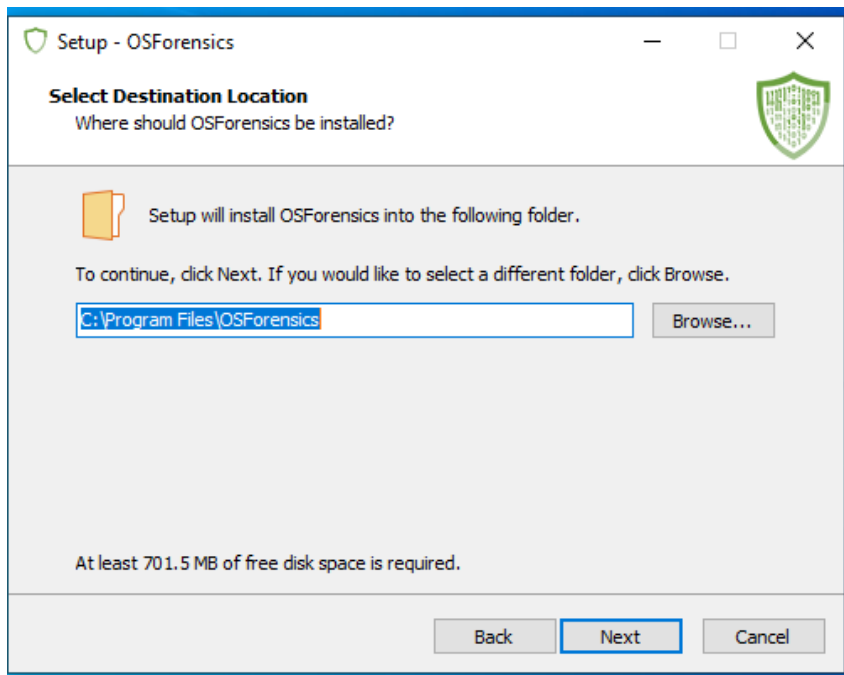
I accepted the UAC prompt and selected English.



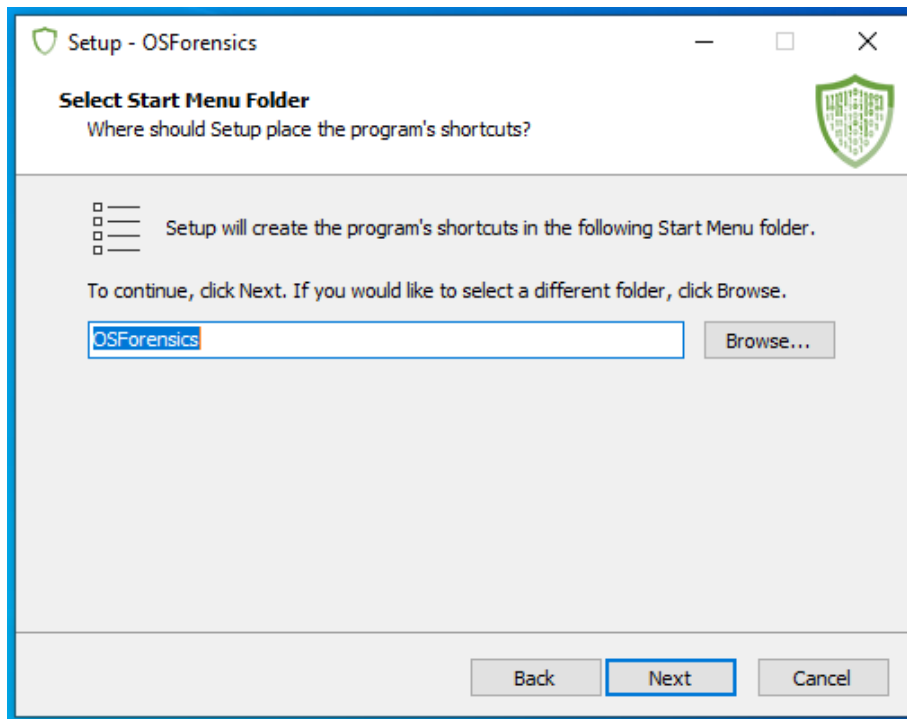
I accepted the License Agreement and pressed on next.



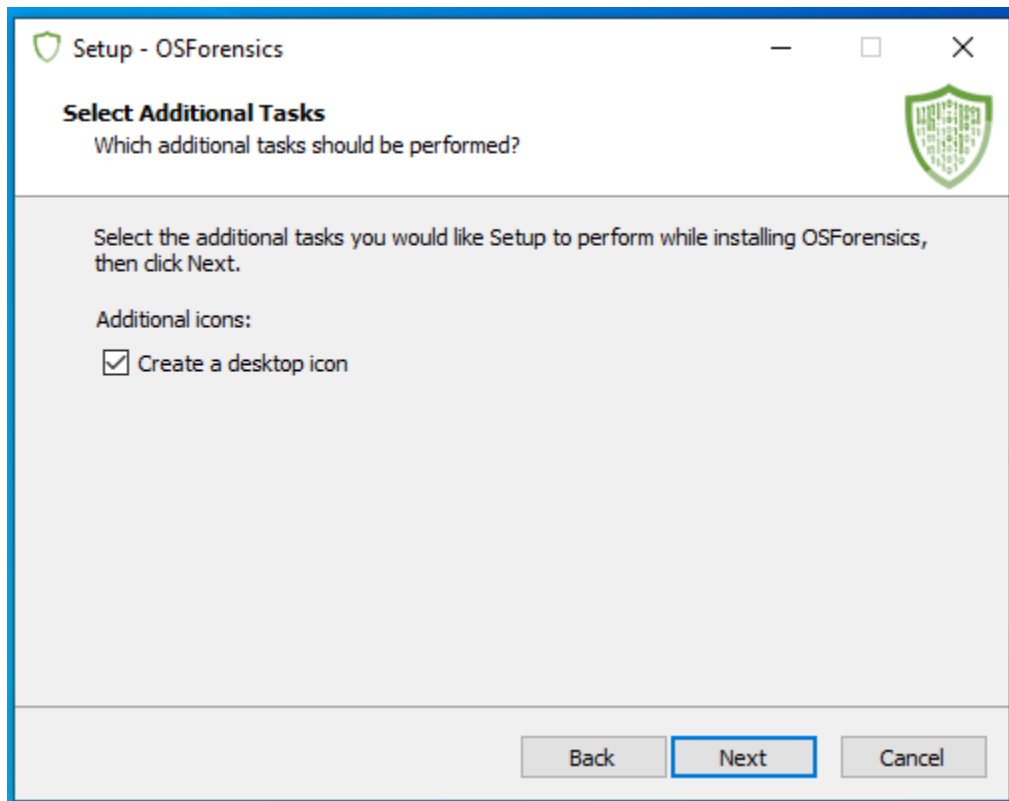
Then I selected the installation location and pressed next.



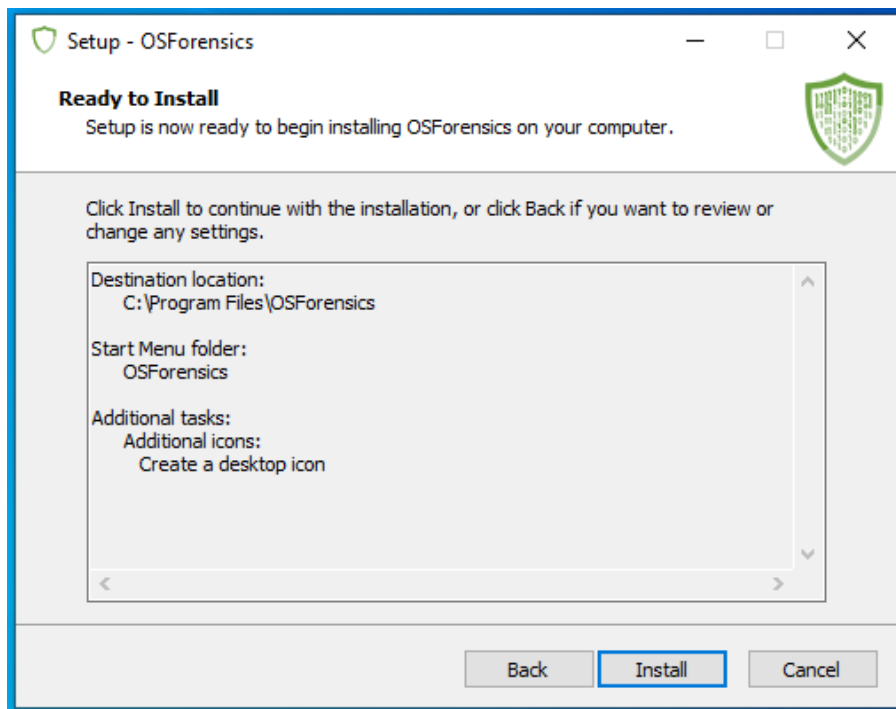
I selected the start menu folder and selected next.



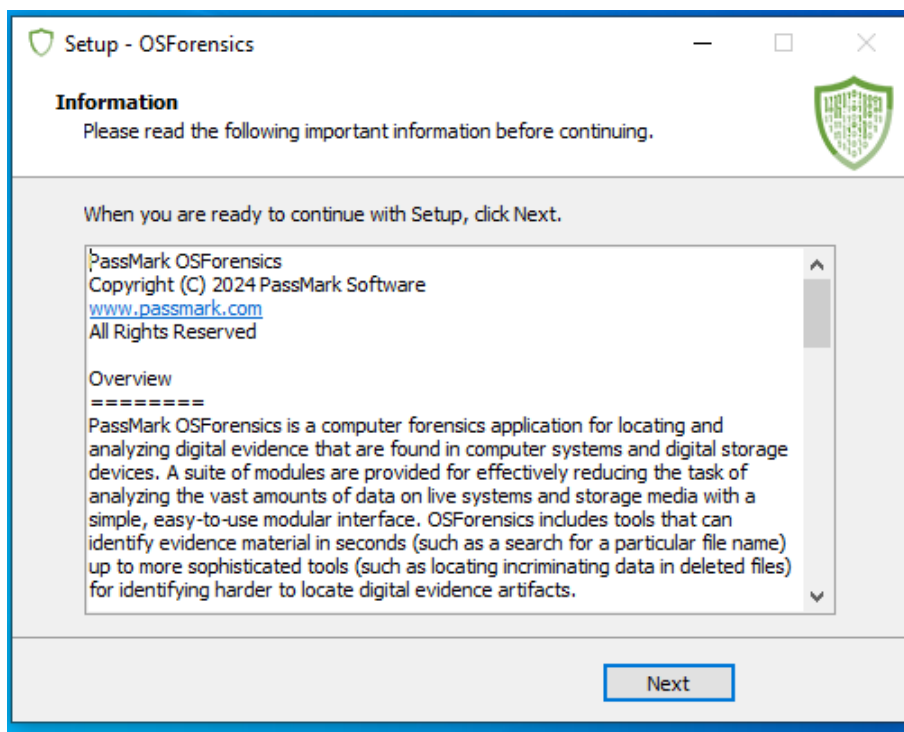
I selected additional tasks create desktop icon and pressed next.



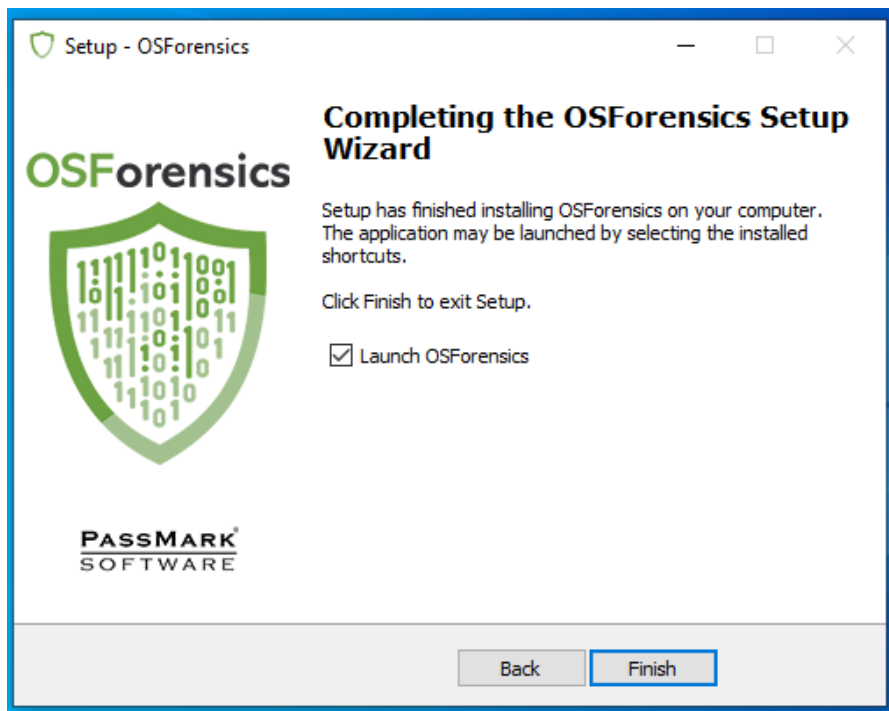
Then, I selected Install.



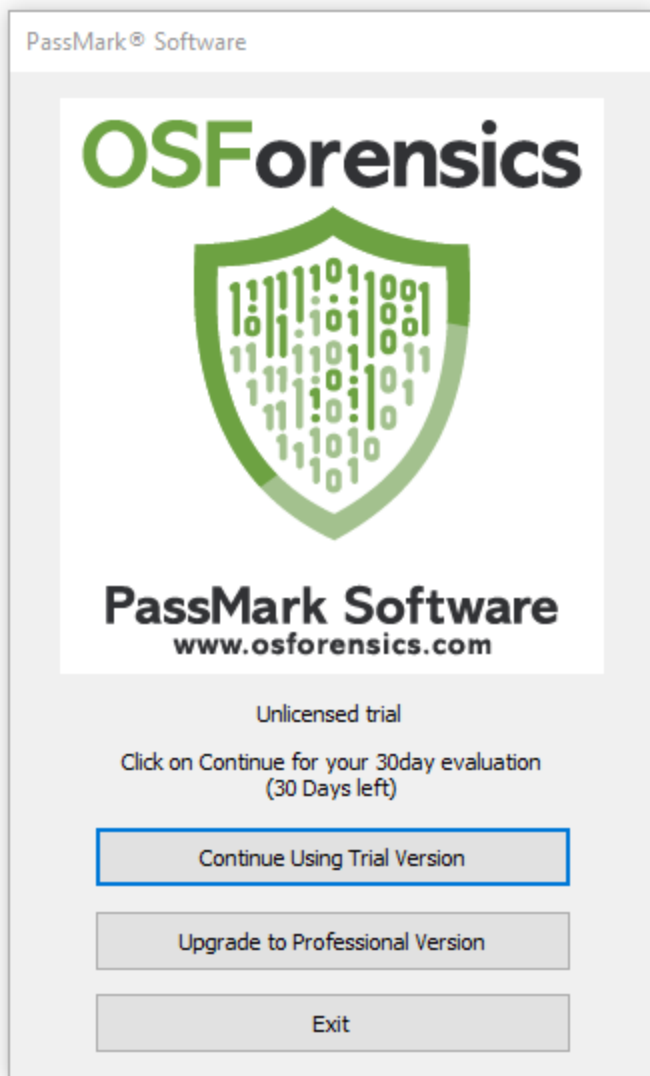
Once installed, I selected next.



I pressed finish to complete the installation process.



OSForensics was launched and I selected “Continue Using Trial Version”

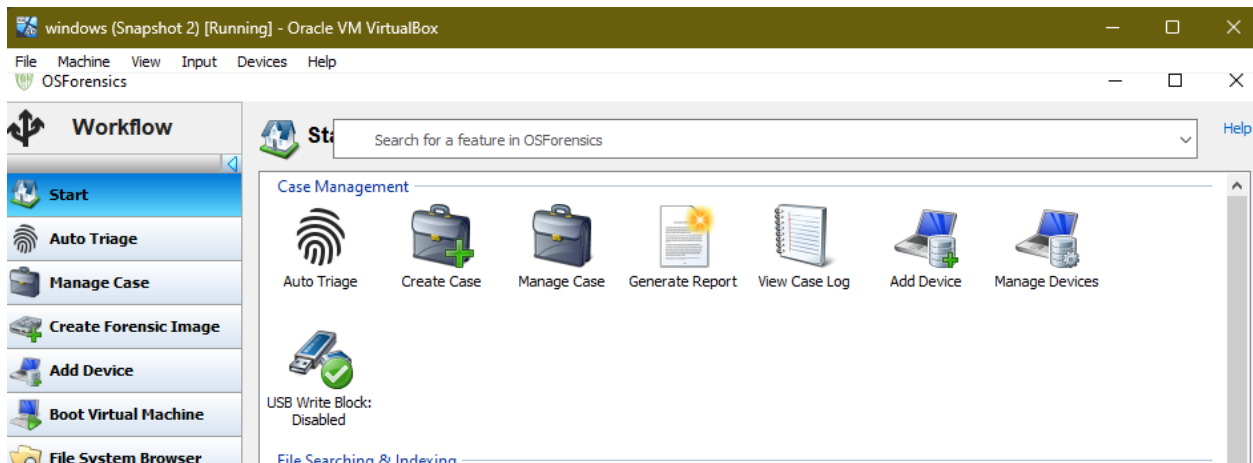


Task 2:

In this task, I complete the Hands-on project 4-3 from the textbook using the provided "Chapter04-Terry_work_usb.E01"

Step1: was completed in task 1

Step 2: I clicked "create case"



Step3: In the new case dialog box, I entered my name in the investigator text box . In the case name text box, I put “m57-Terrys USB drive”. Then I filled in the contact details and the organization and clicked “Investigate Disk(s) from Another machine”.

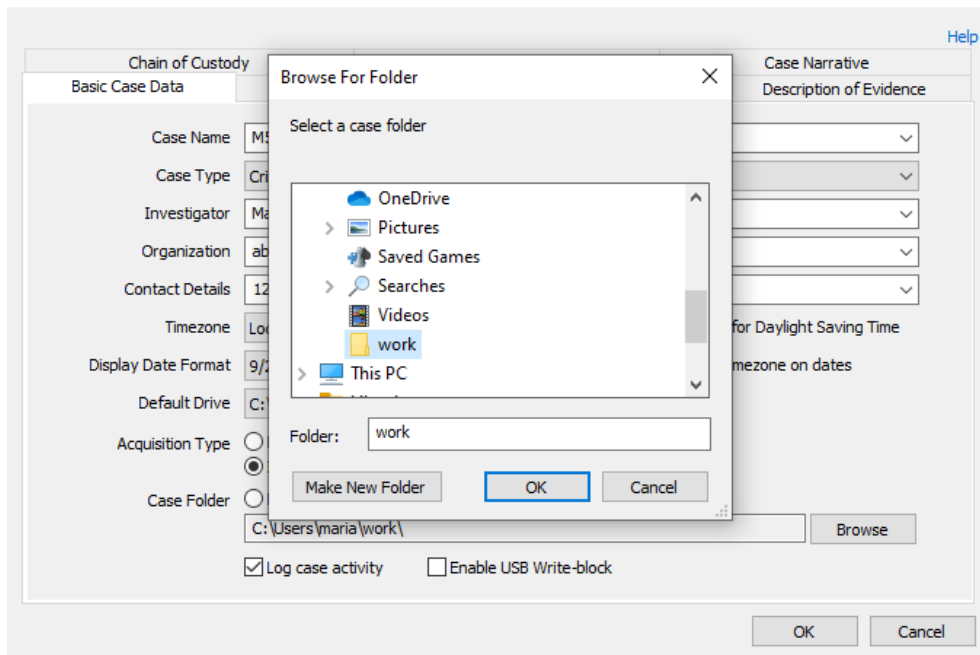
New Case

Chain of Custody		Custom Fields		Case Narrative
Basic Case Data		Case Categories	Offense & Custody Data	Description of Evidence
Case Name	M57-terrrys USB drive			
Case Type	Criminal			
Investigator	Maria			
Organization	abc			
Contact Details	123			
Timezone	Local (UTC -7:00) Pacific Time (US & Canada)	<input checked="" type="checkbox"/>	Account for Daylight Saving Time	
Display Date Format	9/24/2024 (Default)	<input type="checkbox"/>	Display timezone on dates	
Default Drive	C:\ [Local]			
Acquisition Type	<input type="radio"/> Live Acquisition of Current Machine <input checked="" type="radio"/> Investigate Disk(s) from Another Machine			
Case Folder	<input checked="" type="radio"/> Default Location <input type="radio"/> Custom Location C:\Users\maria\Documents\PassMark\OSForensics\Cases\M57-terrrys USB drive <input type="button" value="Browse"/>			
<input checked="" type="checkbox"/> Log case activity		<input type="checkbox"/> Enable USB Write-block		

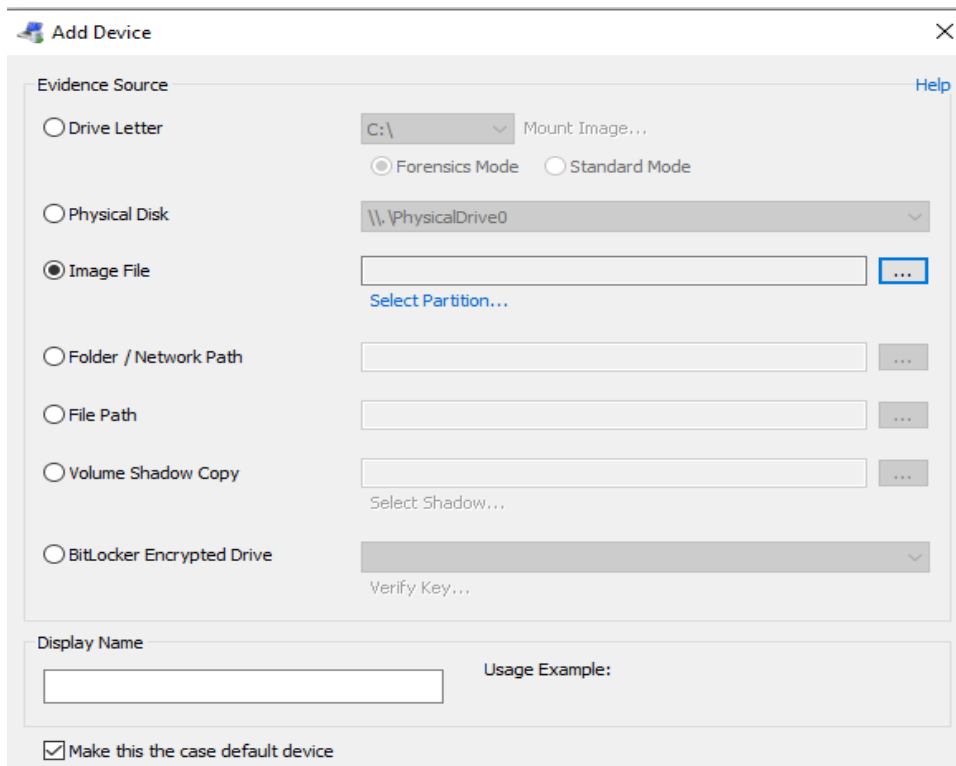
OK Cancel

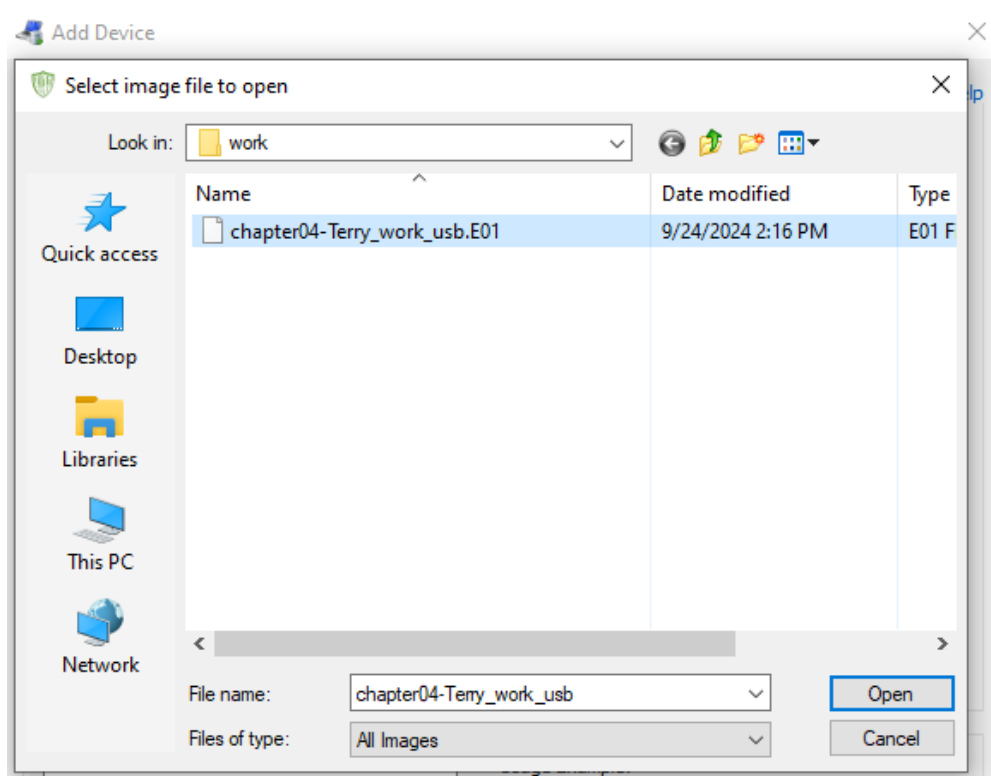
Step 4: In the same tab, I clicked custom location for the case folder and chose my work folder and clicked ok twice.

New Case

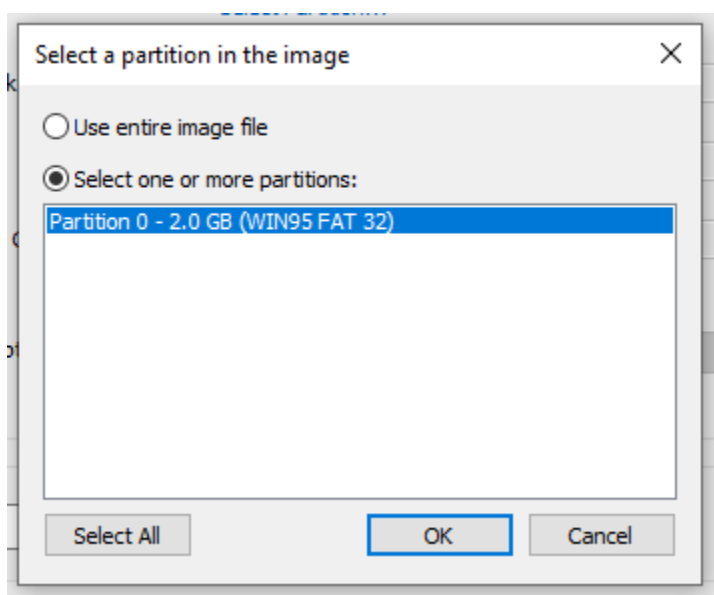


Step 5: I clicked add device and clicked the image file option button. Then chose the folder I copied the images to (chapter04-terry_work_usb.E01) and clicked open.





Step 6: I left the default option for the partition and clicked OK twice.



Add Device

×

Evidence Source

Help

☐ Drive Letter

C:\

Mount Image...

☐ Physical Disk

\\.\PhysicalDrive0

☒ Image File

C:\Users\maria\work\chapter04-Terry_work_usb.E01

...

Partition: 0

☐ Folder / Network Path

...

☐ File Path

...

☐ Volume Shadow Copy

...

Select Shadow...

☐ BitLocker Encrypted Drive

...

Verify Key...

Display Name

chapter04-Terry_work_usb

Usage Example:
"chapter04-Terry_work_usb:\dir\file.ext"

☒ Make this the case default device

windows (Snapshot 2) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

OSForensics - M57-terrys USB drive

Workflow

Start

Auto Triage

Manage Case

Create Forensic Image

Add Device

Boot Virtual Machine

File System Browser

File Viewer

System Information

Memory Viewer

User Activity

Passwords

File Name Search

Deleted Files Search

Manage Case

Help

Select Case

New Case...

Import Case

Load Case

Export Case

Delete Case

Title	Create Date	Access Date	Location	Default ...	Case ...
✓ M57-terrys USB drive	9/24/2024, 14:12:43	9/24/2024, 14:12:43	C:\Users\maria\work\	C:\[Local]	16.18 KB

Case Properties

Edit Case Details...

Edit Narrative...

Edit Categories...

Manage Devices...

Case Exports

Generate Report...

View & Export Log...

Add to Case

Device...

Attachment...

Photos of Evidence...

External Report...

Notes...

Clipboard Data...

Case Items

Open

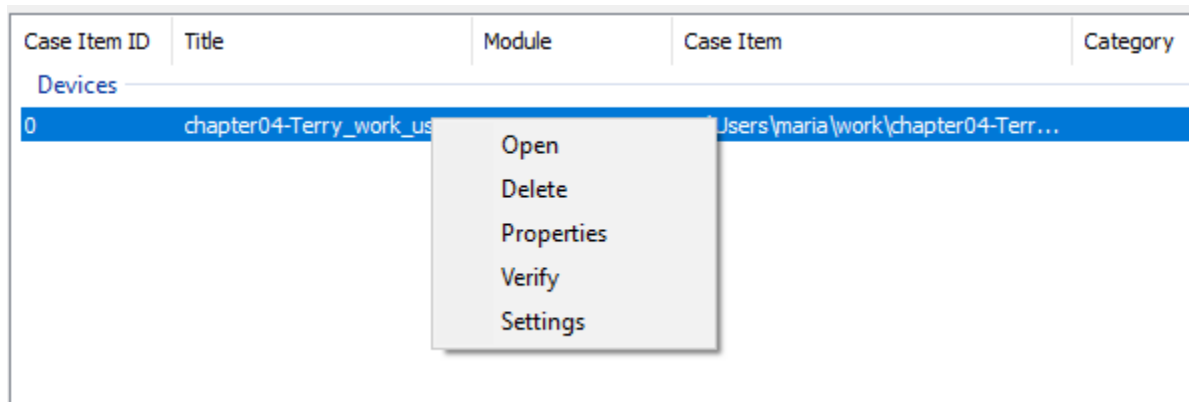
Delete

Properties

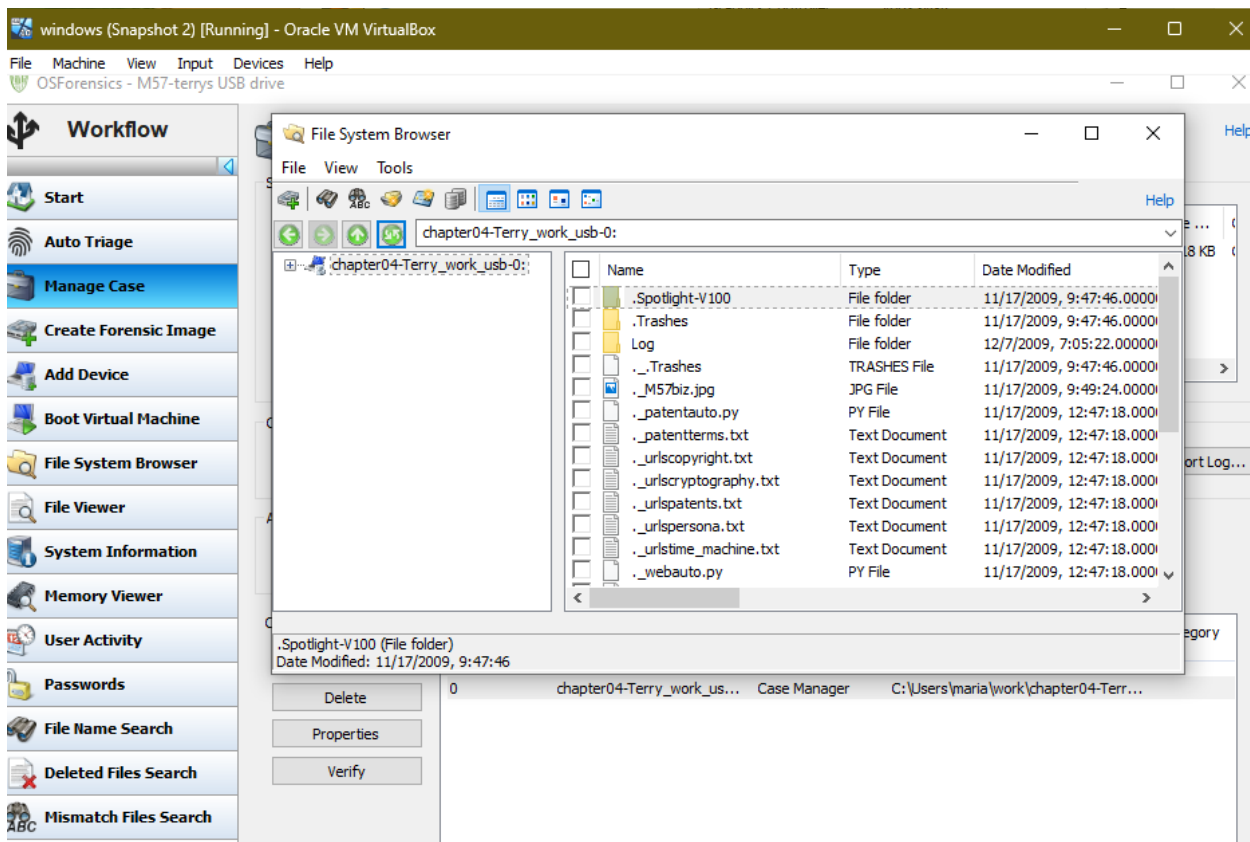
Verify

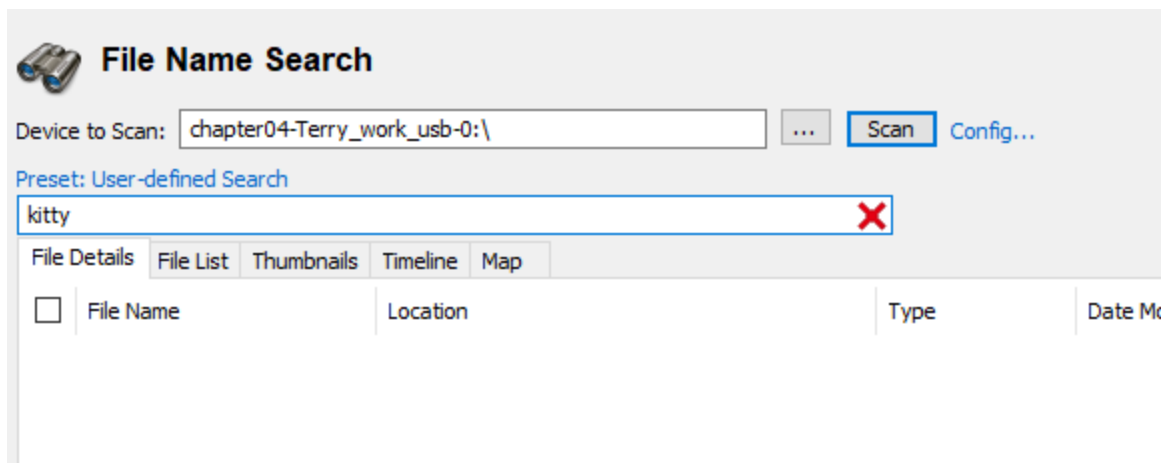
Case Item ID	Title	Module	Case Item	Category
Devices				
0	chapter04-Terry_work_us...	Case Manager	C:\Users\maria\work\chapter04-Terr...	

Step 7: I clicked the “chapter04-terry_work_usb” and clicked open.

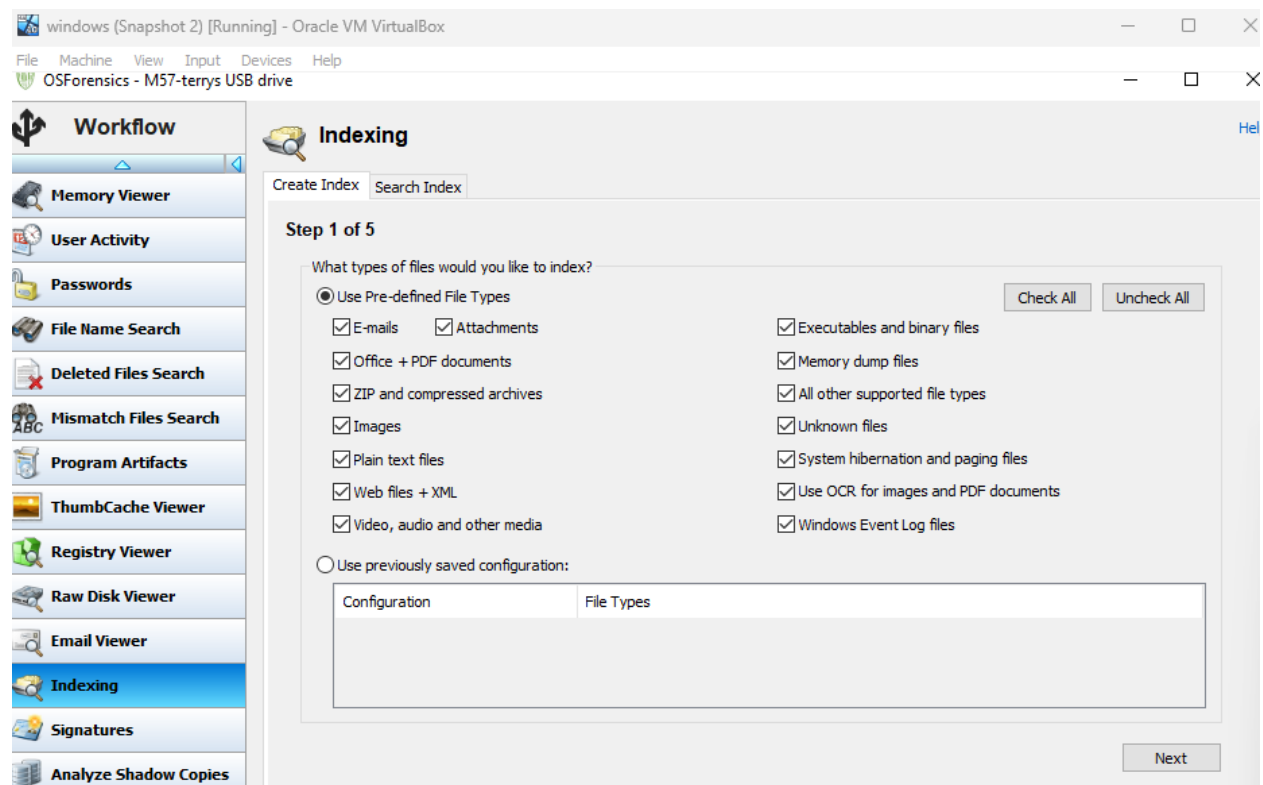


Step 8: I clicked “File name Search” and searched “kitty”





Step 9: I clicked the indexing button in the left pane and clicked next.



Step 10: I clicked Add and chose terrys usb to add and clicked ok and next.

Create Index Search Index

Step 2 of 5

Which drive(s) or folder(s) would you like to index?

File Details	Type
--------------	------

Add... Remove

Advanced settings (optional)

File extensions	Edit	Precognitive search	Edit
Skip files/folders	Edit	Binary string extraction	Edit
Languages & Stemming	Edit	Email attachments	Edit

Back Next

Create Index Search Index

Step 2 of 5

Which drive(s) or folder(s) would you like to index?

File Details	Type
--------------	------

Add... Remove

Advanced settings (optional)

File extensions	Edit	Precognitive search	Edit
Skip files/folders	Edit	Binary string extraction	Edit
Languages & Stemming	Edit	Email attachments	Edit

Back Next

Add Start Location

☒ Whole Drive chapter04-Terry_work_usb-0:\

Drive indexing options: Index files only

☐ Specific Folder chapter04-Terry_work_usb-0:\

OK Cancel

Create Index Search Index

Step 2 of 5

Which drive(s) or folder(s) would you like to index?

File Details	Type
chapter04-Terry_work_usb-0:	Folder

Add... Remove

Advanced settings (optional)

File extensions	Edit	Precognitive search	Edit
Skip files/folders	Edit	Binary string extraction	Edit
Languages & Stemming	Edit	Email attachments	Edit

Back Next

Step 11: Here, I clicked small and next. Then i clicked start indexing with “index all file types” in the index title text box and clicked ok.

Create Index Search Index

Step 3 of 5

Memory optimization / Indexing limits

Estimate the number of files (and size) being indexed. This will help optimize memory usage and index more efficiently.

☒ Small
☐ Medium
☐ Large
☐ Extreme
☐ Don't know (Pre-scan required)
☐ Custom Edit

Max number of files = 10,000
Max file size* = 4 MB
Estimated RAM required: 1,320 MB (1.3 GB)
Available RAM: 1,340 MB (1.3 GB)

*Max file size does not apply to some file formats

Select number of threads: 4

☒ Use RAM drive for temporary files to speed up indexing

Back Next

Create Index

Search Index

Step 4 of 5

Please enter some details for the index

Index Title

index all file types

Index Notes

Index of files in:
chapter04-Terry_work_usb-0:
File extensions:
.pst, .ost, .msg, .eml, .emlx, .mbox, .mbx, .dbx, .msf, .doc, .dot, .ppt, .pps, .pot, .xls, .xlt, .docx, .pptx, .xlsx, .dotx, .pdf, .odt, .sxw, .ods, .odp, .zip, .tgz, .taz, .tar.gz, .tar, .zipx, .rar, .arj, .dmg, .iso, .chm, .bz2, .lzo, .7z, .jpg, .jpeg, .jpe, .gif, .tiff, .tif, .png, .bmp, .heif, .heic, .txt, .text, .rtf, .html, .htm, .shhtml, .shhtml, .xml, .xhtml, .php, .php3, .asp, .aspx, .cfm, .js, .pl, .cgi, .swf, .nfo, .dat, .wpd, .mp3, .mp4, .m4v, .dwm, .torrent, .mht, .avi, .wmv, .wma, .mpg, .mpeg, .rmv, .rmvb, .flv, .mov, .qt, .exe, .dgn, .cab, .psd, .qbb, .dmp, .mdmp, .mem, .evtx
(No ext)
(Unknown ext)
(System hibernation and page files)

Back

Start Indexing

windows (Snapshot 2) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

OSForensics - M57-terrys USB drive

Workflow

Memory Viewer

User Activity

Passwords

File Name Search

Deleted Files Search

Mismatch Files Search

Program Artifacts

ThumbCache Viewer

Registry Viewer

Raw Disk Viewer

Email Viewer

Indexing

Signatures

Analyze Shadow Copies

File Hashing

Remote Acquisition

Customize Workflow

Register

Exit

Indexing

Create Index

Search Index

Step 5 of 5

Start Time

Tue Sep 24 15:09:14 2024

Finish Time

Files Indexed

22

Time Elapsed

00:00:36

Emails Indexed

0

Peak Phys. Mem. Used

184 MB

Alerts

0

Peak Virt. Mem. Used

8732 MB

Warnings

0

Max File & Emails

2500

Total Bytes

8.38 MB

Unique Words

70019

Current Action:

Indexing - Processing file

Show Log

Thread #

Indexing file

Thread 1

Thread 2

Thread 3

Thread 4

<< New Index

Save configuration

Show Precog Results

Cancel

Type here to search


99°F

3:09 PM

9/24/2024

Right Ctrl

Step 12: After the indexing is completed, I clicked open log and examined the log. Then I closed the log.

**Indexing**Help

Create IndexSearch Index

Step 5 of 5

Start Time
Tue Sep 24 15:09:14 2024

Finish Time
Tue Sep 24 15:31:19 2024

Files Indexed
2500

Time Elapsed
00:22:05

Emails Indexed
0

Peak Phys. Mem. Used
192 MB

Alerts
7

Peak Virt. Mem. Used
8747 MB

Warnings
4

Max File & Emails
2500

Total Bytes
48.42 MB


Unique Words
74580

Current Action: Finished (Some files could not be indexed - see indexer log)Show Log

Thread #	Indexing file
Thread 1	{Finished}
Thread 2	{Finished}
Thread 3	{Finished}
Thread 4	{Finished}

< >

<< New IndexSave configurationShow Precog ResultsCancel

Index Log×

Show message options

Show allReset to defaultHide all


☒ Indexing☐ Skipped☐ Filtered


☒ Alerts☒ Warning☒ Information


☐ Initialization☒ File I/O☒ Summary


☒ Plugin


Showing 5000 of 10109


 .wmv indexed: 0


 .wma indexed: 0


 .mpg indexed: 0


 .mpeg indexed: 0


 .rmv indexed: 0


 .rmvb indexed: 0


 .flv indexed: 0


 .mov indexed: 0


 .qt indexed: 0


 .exe indexed: 2


 .dgn indexed: 0


 .cab indexed: 0


 .psd indexed: 0


 .qbb indexed: 0

 .dmp indexed: 0

 .mdmp indexed: 0

 .mem indexed: 0

 .evtx indexed: 0

 No extensions indexed: 5

Successfully created all required files

Step 13: I then clicked manage case and double-clicked terry's usb and opened files to examine them.

The image shows two windows from the OSForensics application. The top window is titled 'Manage Case' and displays a table of cases. The bottom window is titled 'File System Browser' and shows the contents of a USB drive.

Manage Case Window:

Select Case Table:

Title	Create Date	Access Date	Location	Default ...	Case ...
✓ M57-terrys USB drive	9/24/2024, 14:12:43	9/24/2024, 14:12:43	C:\Users\maria\work\	C:\ [Local]	16.18 KB

Case Properties: Edit Case Details... Edit Narrative... Edit Categories... Manage Devices...

Case Exports: Generate Report... View & Export Log...

Add to Case: Device... Attachment... Photos of Evidence... External Report... Notes... Clipboard Data...

Case Items Table:

Case Item ID	Title	Module	Case Item	Category
Indexes				
1	index all file types	Create Index	index all file types	Images
Devices				
0	chapter04-Terry_work_us...	Case Manager	C:\Users\maria\work\chapter04-Terr...	

File System Browser Window:

chapter04-Terry_work_usb-0:

Name	Type	Date Modified	Date Created	Date Accessed
..Spotlight-V100	File folder	11/17/2009, 9:47:46.0000000	11/17/2009, 9:47:46.0000000	11/16/2009, 23:00:00.0000000
..Trashes	File folder	11/17/2009, 9:47:46.0000000	11/17/2009, 9:47:46.0000000	11/16/2009, 23:00:00.0000000
Log	File folder	12/7/2009, 7:05:22.0000000	12/7/2009, 7:05:20.0000000	12/6/2009, 23:00:00.0000000
..Trashes	TRASHES File	11/17/2009, 9:47:46.0000000	11/17/2009, 9:47:46.0000000	11/16/2009, 23:00:00.0000000
..M57biz.jpg	JPG File	11/17/2009, 9:49:24.0000000	11/17/2009, 9:49:24.0000000	11/16/2009, 23:00:00.0000000
..patentauto.py	PY File	11/17/2009, 12:47:18.0000000	11/17/2009, 12:47:18.0000000	11/16/2009, 23:00:00.0000000
..patentterms.txt	Text Document	11/17/2009, 12:47:18.0000000	11/17/2009, 12:47:18.0000000	11/16/2009, 23:00:00.0000000
..urlscopyright.txt	Text Document	11/17/2009, 12:47:18.0000000	11/17/2009, 12:47:18.0000000	11/16/2009, 23:00:00.0000000
..urlscryptography.txt	Text Document	11/17/2009, 12:47:18.0000000	11/17/2009, 12:47:18.0000000	11/16/2009, 23:00:00.0000000
..urlspatents.txt	Text Document	11/17/2009, 12:47:18.0000000	11/17/2009, 12:47:18.0000000	11/16/2009, 23:00:00.0000000
..urlspersona.txt	Text Document	11/17/2009, 12:47:18.0000000	11/17/2009, 12:47:18.0000000	11/16/2009, 23:00:00.0000000
..urlstime_machine.txt	Text Document	11/17/2009, 12:47:18.0000000	11/17/2009, 12:47:18.0000000	11/16/2009, 23:00:00.0000000
..webauto.py	PY File	11/17/2009, 12:47:18.0000000	11/17/2009, 12:47:18.0000000	11/16/2009, 23:00:00.0000000
M57biz.jpg	JPG File	11/17/2009, 7:50:26.0000000	11/17/2009, 7:50:24.0000000	12/6/2009, 23:00:00.0000000
patentauto.py	PY File	11/17/2009, 12:37:00.0000000	11/16/2009, 13:16:48.0000000	11/16/2009, 23:00:00.0000000
patentterms.txt	Text Document	11/16/2009, 13:29:38.0000000	11/14/2009, 16:43:56.0000000	11/23/2009, 23:00:00.0000000
RS4402.EXE	Application	11/20/2009, 9:31:44.0000000	11/20/2009, 9:31:34.0000000	12/6/2009, 23:00:00.0000000
urlscopyright.txt	Text Document	11/17/2009, 9:40:56.0000000	11/17/2009, 9:40:56.0000000	11/23/2009, 23:00:00.0000000
urlscryptography.txt	Text Document	11/16/2009, 9:22:50.0000000	11/16/2009, 9:22:50.0000000	11/23/2009, 23:00:00.0000000
urlspatents.txt	Text Document	11/17/2009, 9:40:56.0000000	11/17/2009, 9:40:56.0000000	11/23/2009, 23:00:00.0000000
urlspersona.txt	Text Document	11/14/2009, 16:43:14.0000000	11/14/2009, 16:41:54.0000000	11/23/2009, 23:00:00.0000000
urlstime_machine.txt	Text Document	11/16/2009, 9:22:50.0000000	11/16/2009, 9:22:50.0000000	11/23/2009, 23:00:00.0000000
vnc-4_1_3-x86_win32.exe	Application	10/15/2008, 17:14:08.0000000	10/15/2008, 17:14:08.0000000	12/6/2009, 23:00:00.0000000
WEBAUTO.PY	PY File	11/16/2009, 13:23:38.0000000	11/14/2009, 16:39:18.0000000	11/23/2009, 23:00:00.0000000

..urlstime_machine.txt (Text Document)
Date Modified: 11/17/2009, 12:47:18 Size: 4.00 KB

