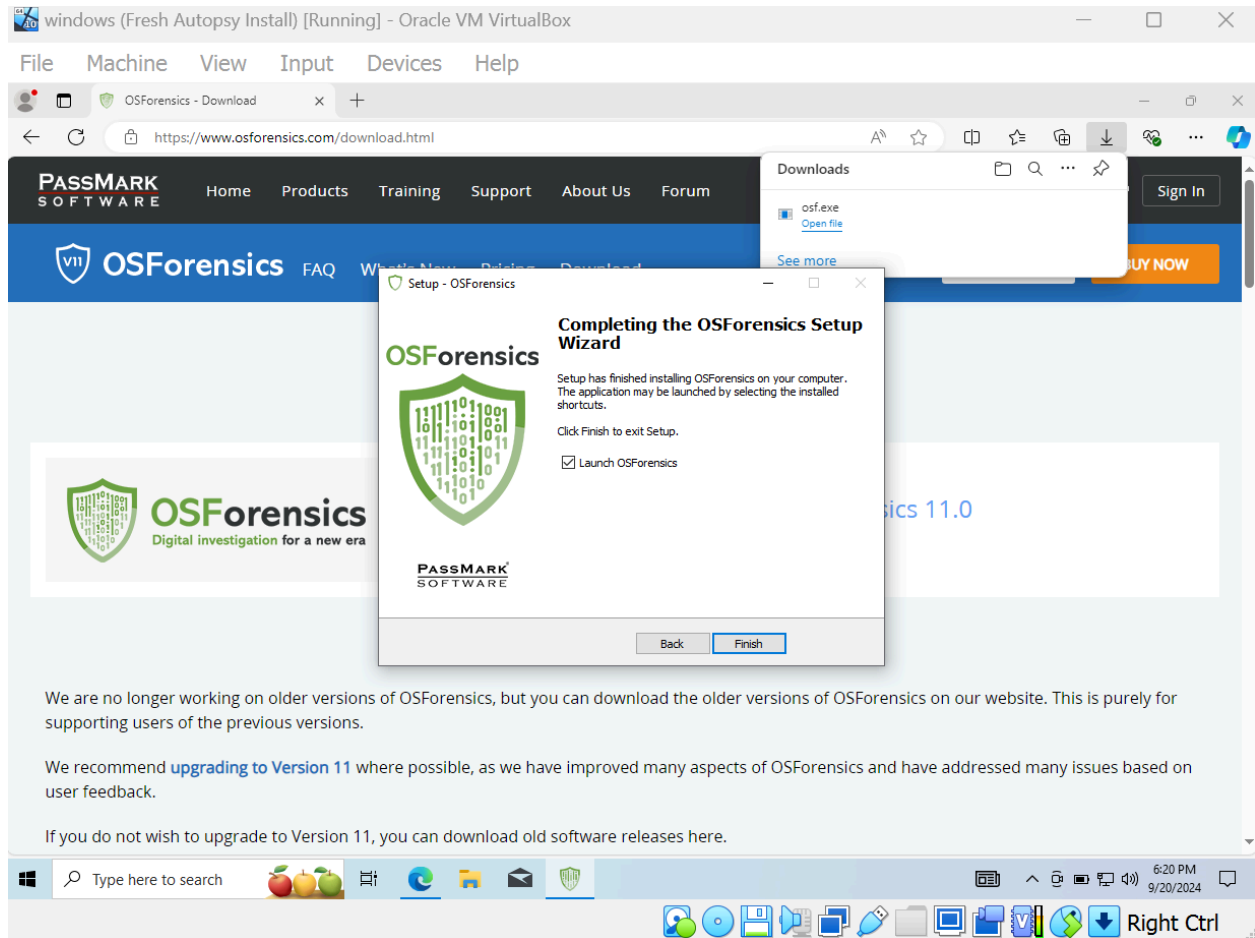


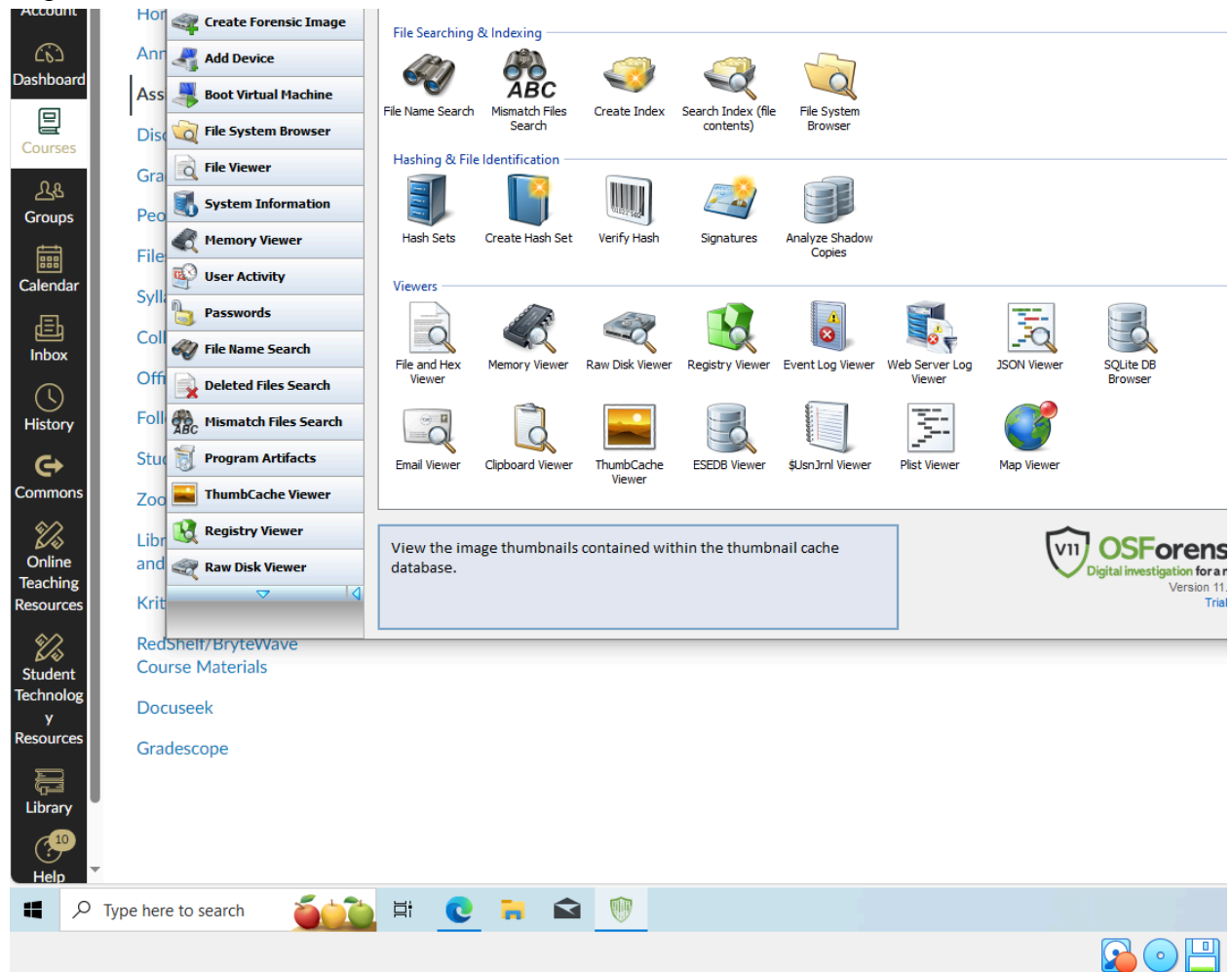
## Task 1: Install OSForensics



Successful installation of OSForensics on the Windows VM.

## Task 2: Hands-on Project 4-3

### Step 1: Start OS Forensics



I clicked continue using trial version and was met with the landing page of OSF.

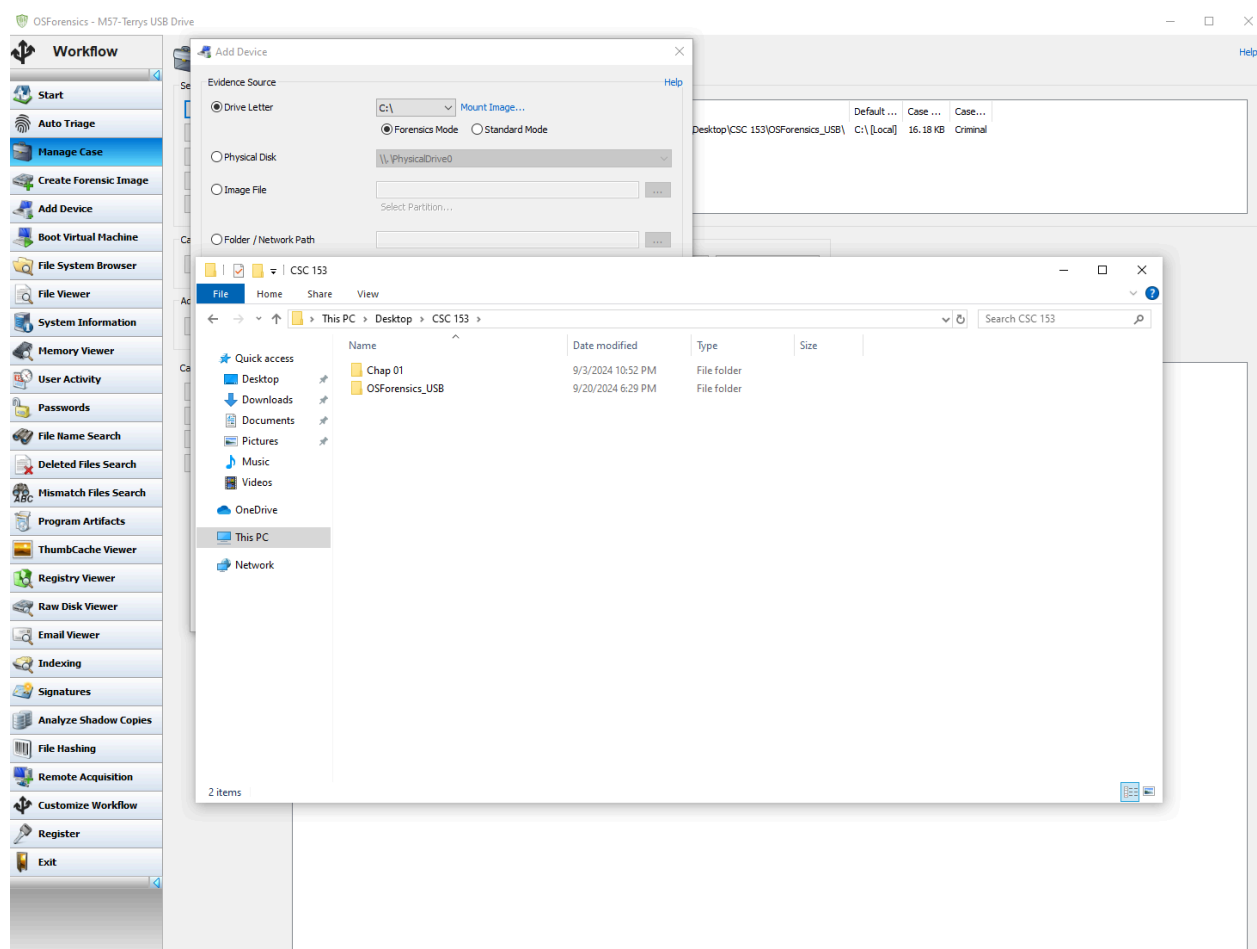
## Step 2 &amp; 3: Create Case and fill in information

The screenshot shows the OSForensics application interface. On the left is a 'Workflow' sidebar with various tools like 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, Mismatch Files Search, Program Artifacts, ThumbCache Viewer, Registry Viewer, and Raw Disk Viewer. The 'Manage Case' window is open, displaying a 'New Case' dialog box. The dialog box has tabs for 'Chain of Custody', 'Custom Fields', and 'Case Narrative'. The 'Chain of Custody' tab is active, showing 'Basic Case Data' and 'Case Categories'. The 'Basic Case Data' section includes fields for Case Name, Case Type, Investigator, Organization, Contact Details, Timezone, Display Date Format, Default Drive, Acquisition Type, Case Folder, Log case activity, and Enable USB Write-block. The 'Case Categories' section includes Offense & Custody Data and Description of Evidence. The 'Case Narrative' tab is also visible, showing a 'Description of Evidence' section. The 'New Case' dialog box is currently open, showing the following information:

Chain of Custody	Custom Fields	Case Narrative
Basic Case Data	Case Categories	Offense & Custody Data
Case Name	M57-Terrys USB Drive	
Case Type	Criminal	
Investigator	Jessica Villanueva	
Organization	M57 Patents	
Contact Details		
Timezone	Local (UTC -7:00) Pacific Time (US & Canada)	<input checked="" type="checkbox"/> Account for Daylight Saving Time
Display Date Format	9/21/2024 (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\jessica_win\Documents\PassMark\OSForensics\Cases\M57-Terrys US	
Log case activity	<input checked="" type="checkbox"/>	
Enable USB Write-block	<input type="checkbox"/>	

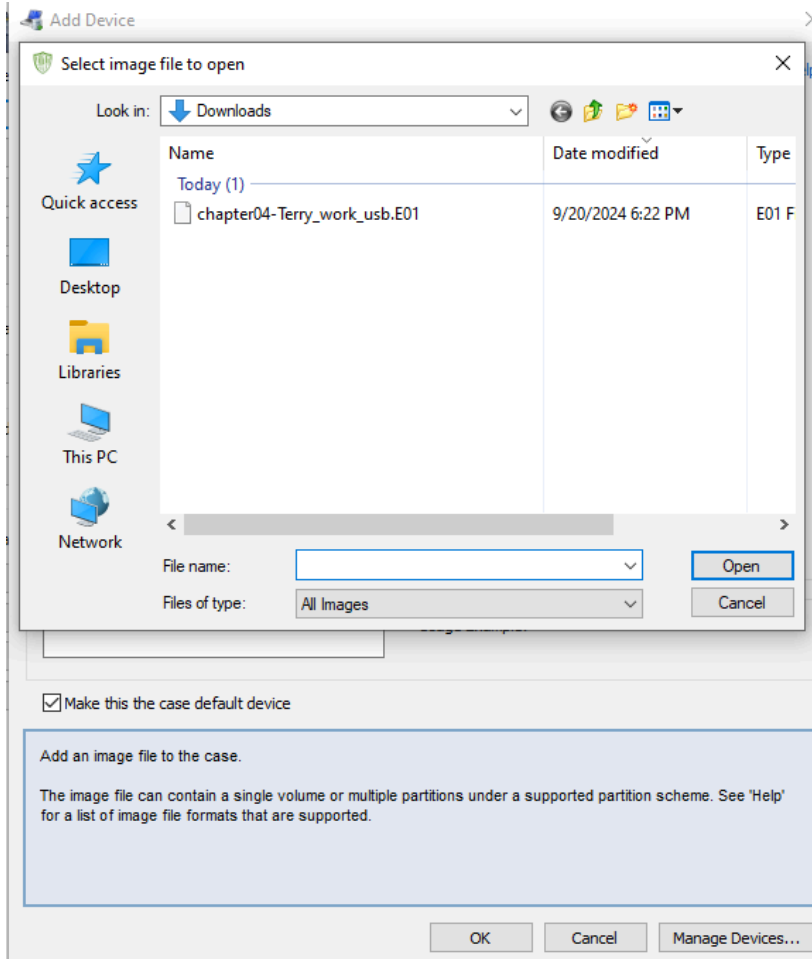
I entered the appropriate information and included my investigator name.

## Step 4: Select case file



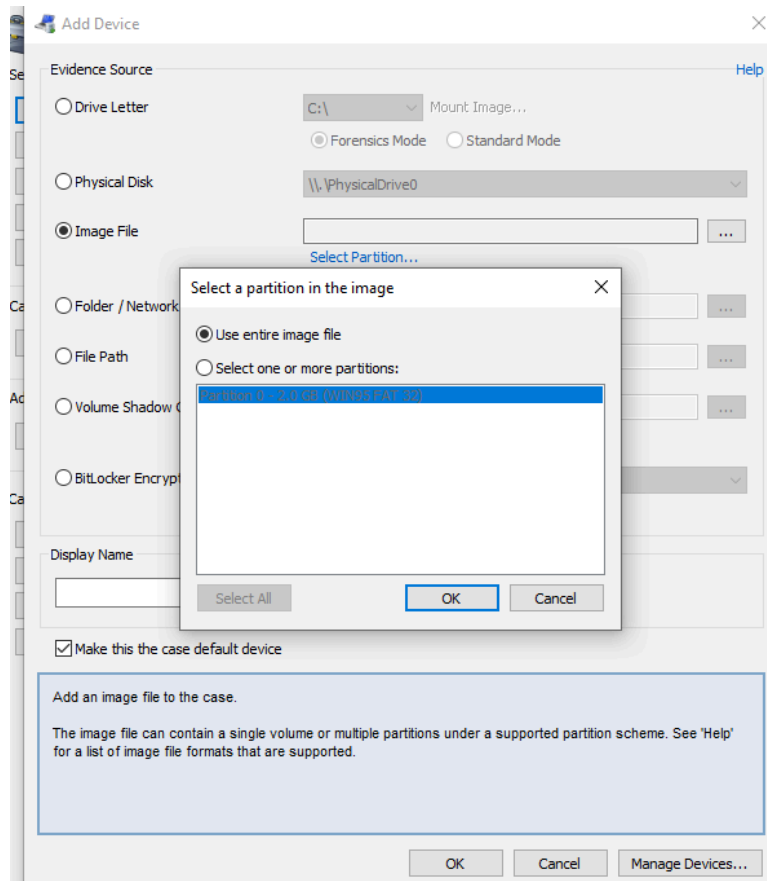
I created a new case folder to select for the case.

## Step 5: Add device



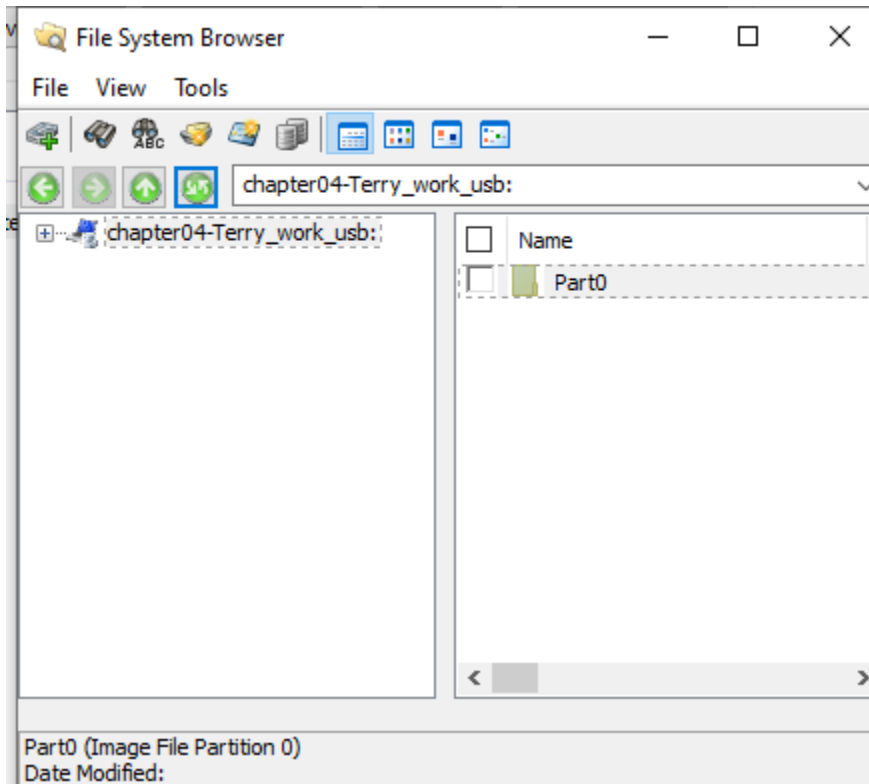
I selected the proper case files to open.

## Step 6: Default settings



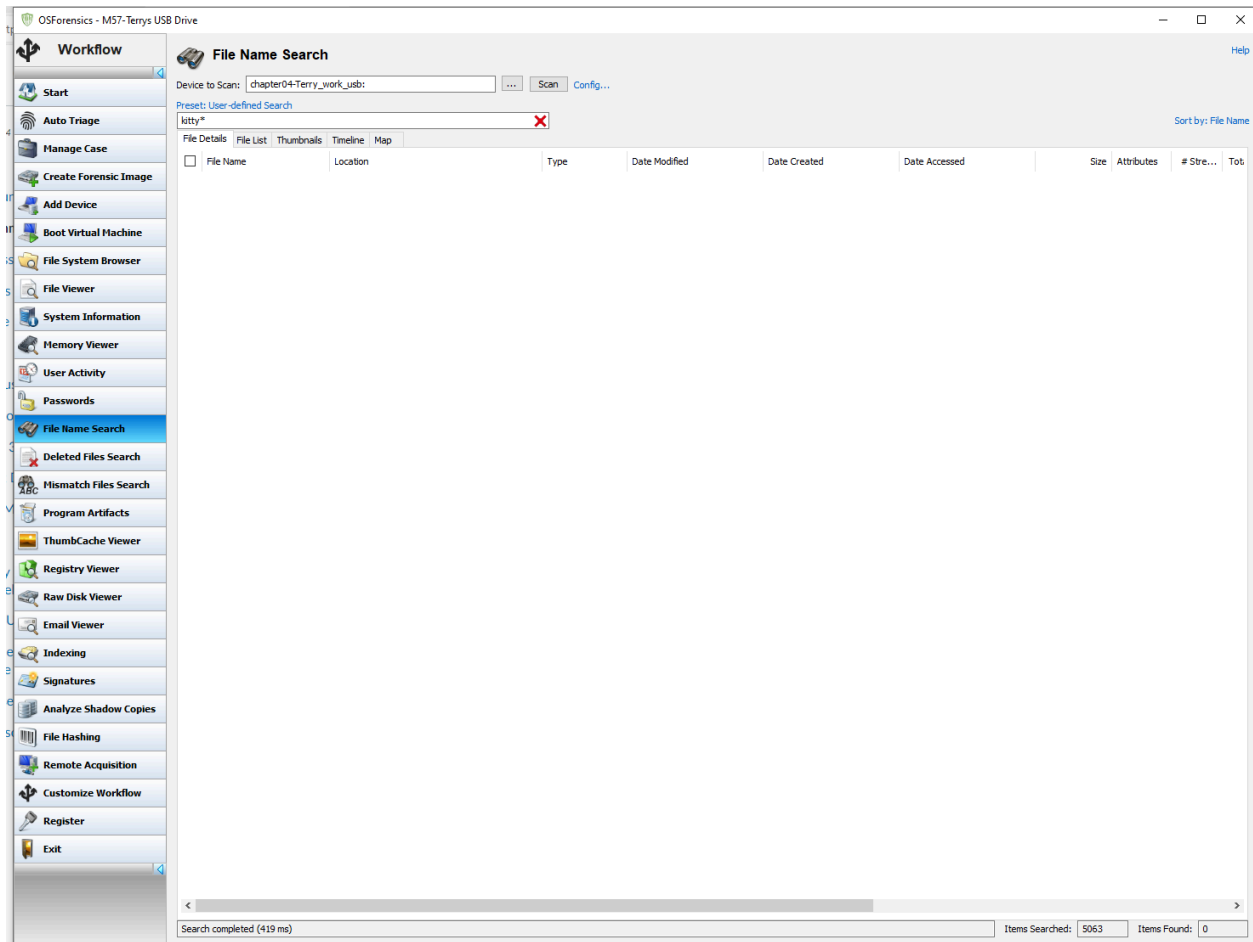
I chose the default settings (use entire image file) as the instructions said to.

Step 7: Click filename



I opened the File System Browser Window.

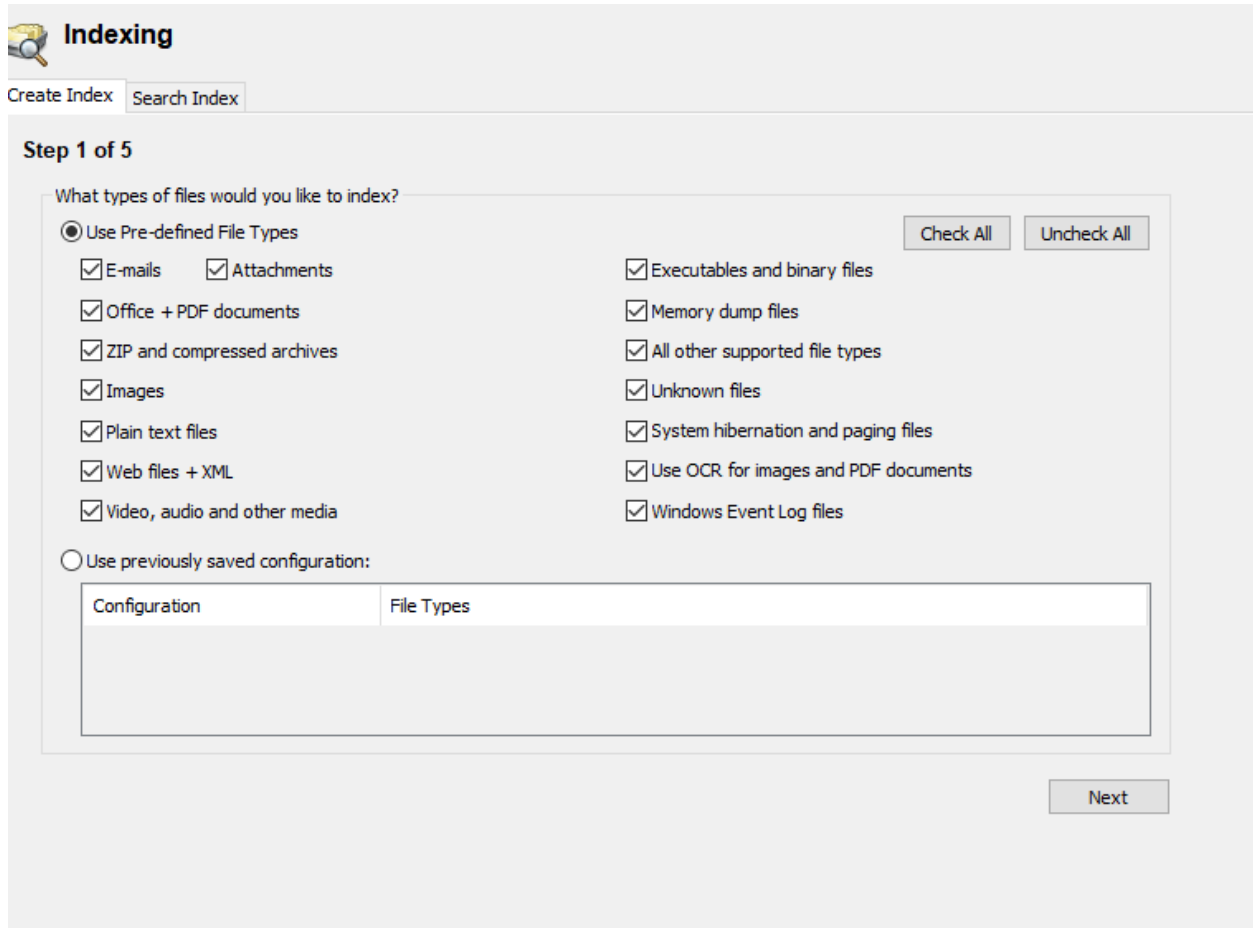
## Step 8: File Name Search



I searched for "kitty\*" and no results came up, indicating that the device is clean.



## Step 9: Create Index



The screenshot shows the Windows Indexing Control Panel window. At the top, there's a title bar with the word "Indexing" and a magnifying glass icon. Below the title bar, there are two tabs: "Create Index" (selected) and "Search Index". The main content area is titled "Step 1 of 5" and contains the question "What types of files would you like to index?". There are two radio buttons: "Use Pre-defined File Types" (selected) and "Use previously saved configuration:". To the right of the "Use Pre-defined File Types" radio button are two buttons: "Check All" and "Uncheck All". Below the radio buttons are two columns of checkboxes, all of which are checked. The first column includes: "E-mails", "Attachments", "Office + PDF documents", "ZIP and compressed archives", "Images", "Plain text files", "Web files + XML", and "Video, audio and other media". The second column includes: "Executables and binary files", "Memory dump files", "All other supported file types", "Unknown files", "System hibernation and paging files", "Use OCR for images and PDF documents", and "Windows Event Log files". At the bottom right of the window is a "Next" button.

**Indexing**

Create Index Search Index

**Step 1 of 5**

What types of files would you like to index?

☒ Use Pre-defined File Types ☐ Use previously saved configuration:

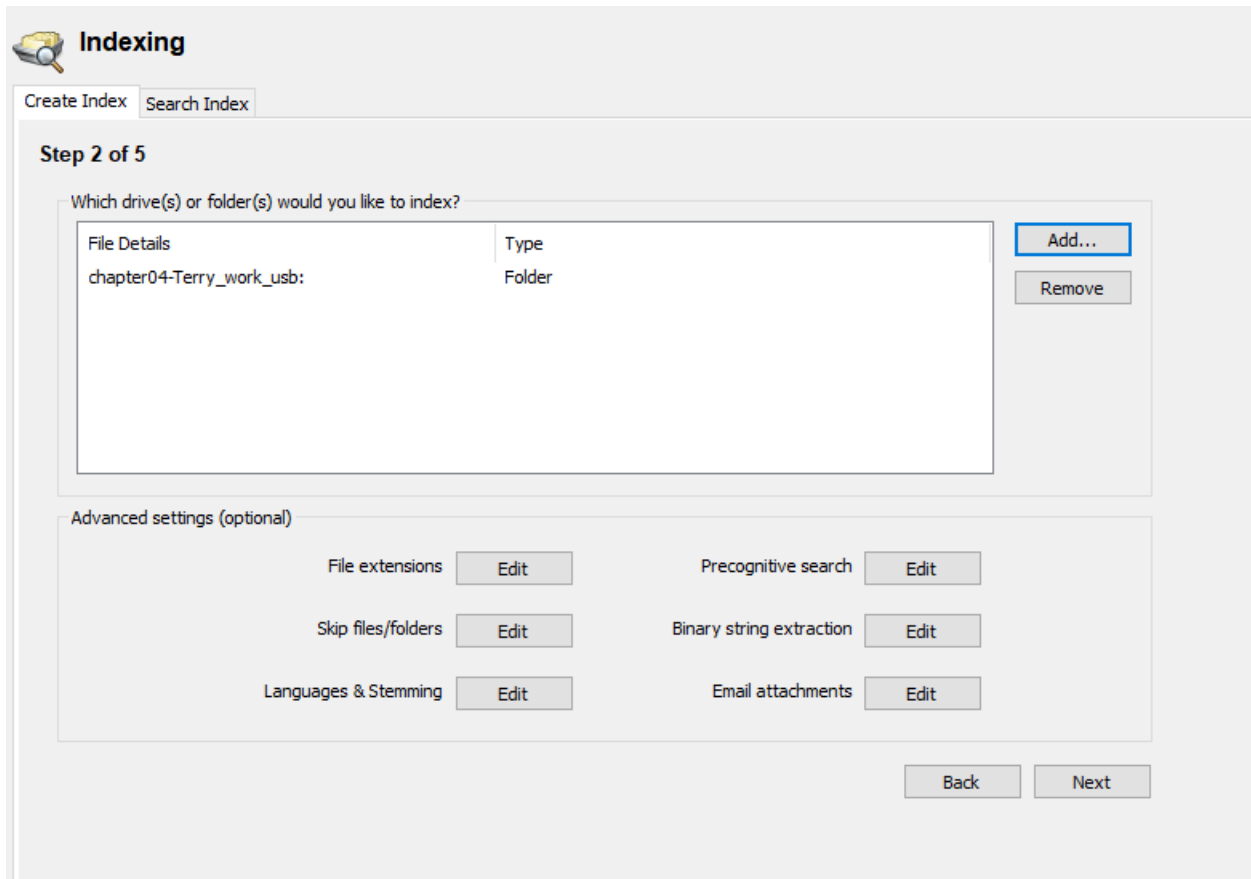
Check All Uncheck All

<input checked="" type="checkbox"/> E-mails	<input checked="" type="checkbox"/> Executables and binary files
<input checked="" type="checkbox"/> Attachments	<input checked="" type="checkbox"/> Memory dump files
<input checked="" type="checkbox"/> Office + PDF documents	<input checked="" type="checkbox"/> All other supported file types
<input checked="" type="checkbox"/> ZIP and compressed archives	<input checked="" type="checkbox"/> Unknown files
<input checked="" type="checkbox"/> Images	<input checked="" type="checkbox"/> System hibernation and paging files
<input checked="" type="checkbox"/> Plain text files	<input checked="" type="checkbox"/> Use OCR for images and PDF documents
<input checked="" type="checkbox"/> Web files + XML	<input checked="" type="checkbox"/> Windows Event Log files
<input checked="" type="checkbox"/> Video, audio and other media	

Next

I selected the pre-defined file types as instructed and proceeded.

## Step 10: Select USB image



The screenshot shows the 'Indexing' window of a software application. At the top, there is a 'Create Index' button and a 'Search Index' button. Below this, the window is titled 'Step 2 of 5'. The main question is 'Which drive(s) or folder(s) would you like to index?'. A table lists the selected item: 'chapter04-Terry\_work\_usb:' under 'File Details' and 'Folder' under 'Type'. To the right of the table are 'Add...' and 'Remove' buttons. Below the table is an 'Advanced settings (optional)' section with six settings, each with an 'Edit' button: 'File extensions', 'Precognitive search', 'Skip files/folders', 'Binary string extraction', 'Languages & Stemming', and 'Email attachments'. At the bottom right are 'Back' and 'Next' buttons.

File Details	Type
chapter04-Terry_work_usb:	Folder

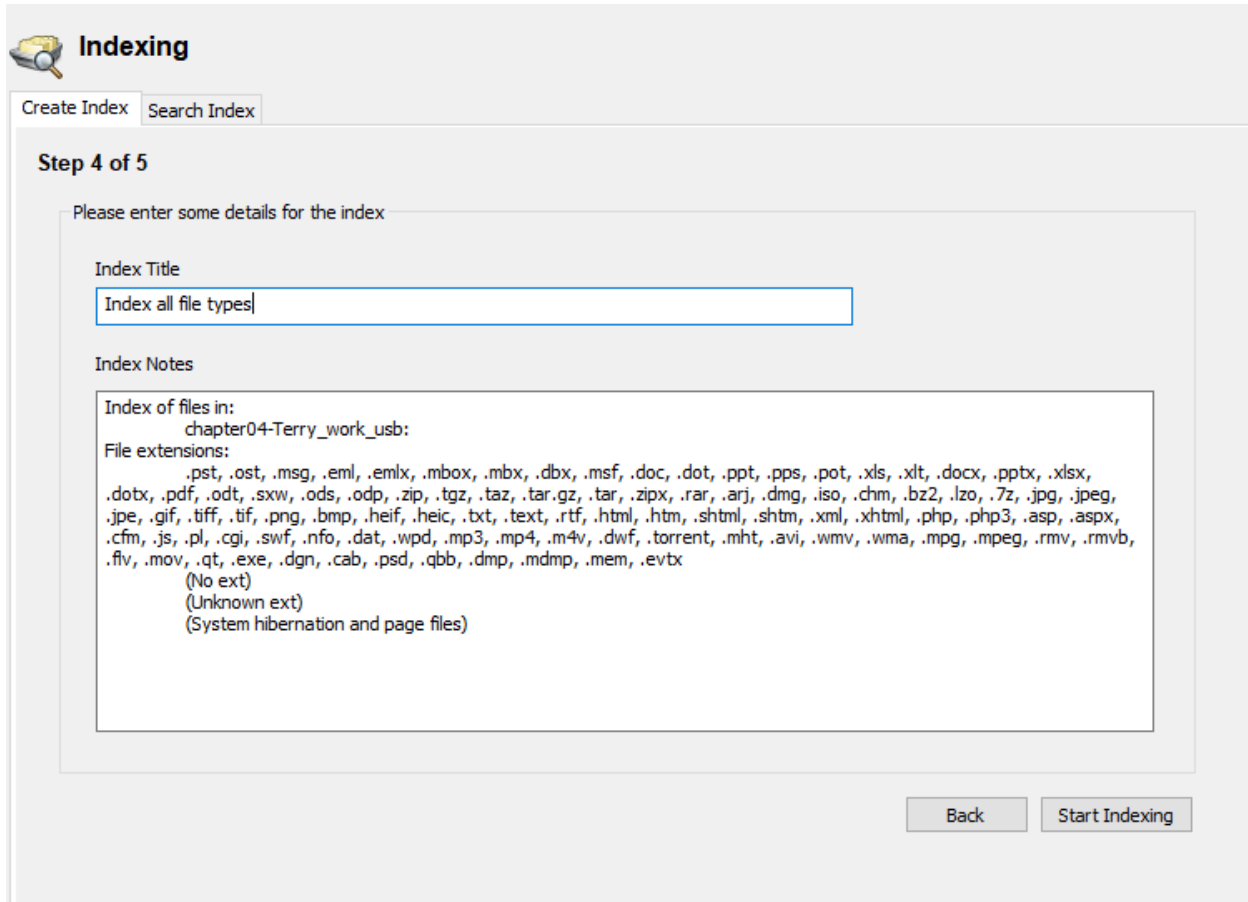
Advanced settings (optional)

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

Back Next

I selected the correct drive to index.

## Step 11: Index all File types



**Indexing**

Create Index Search Index

**Step 4 of 5**

Please enter some details for the index

Index Title

Index all file types

Index Notes

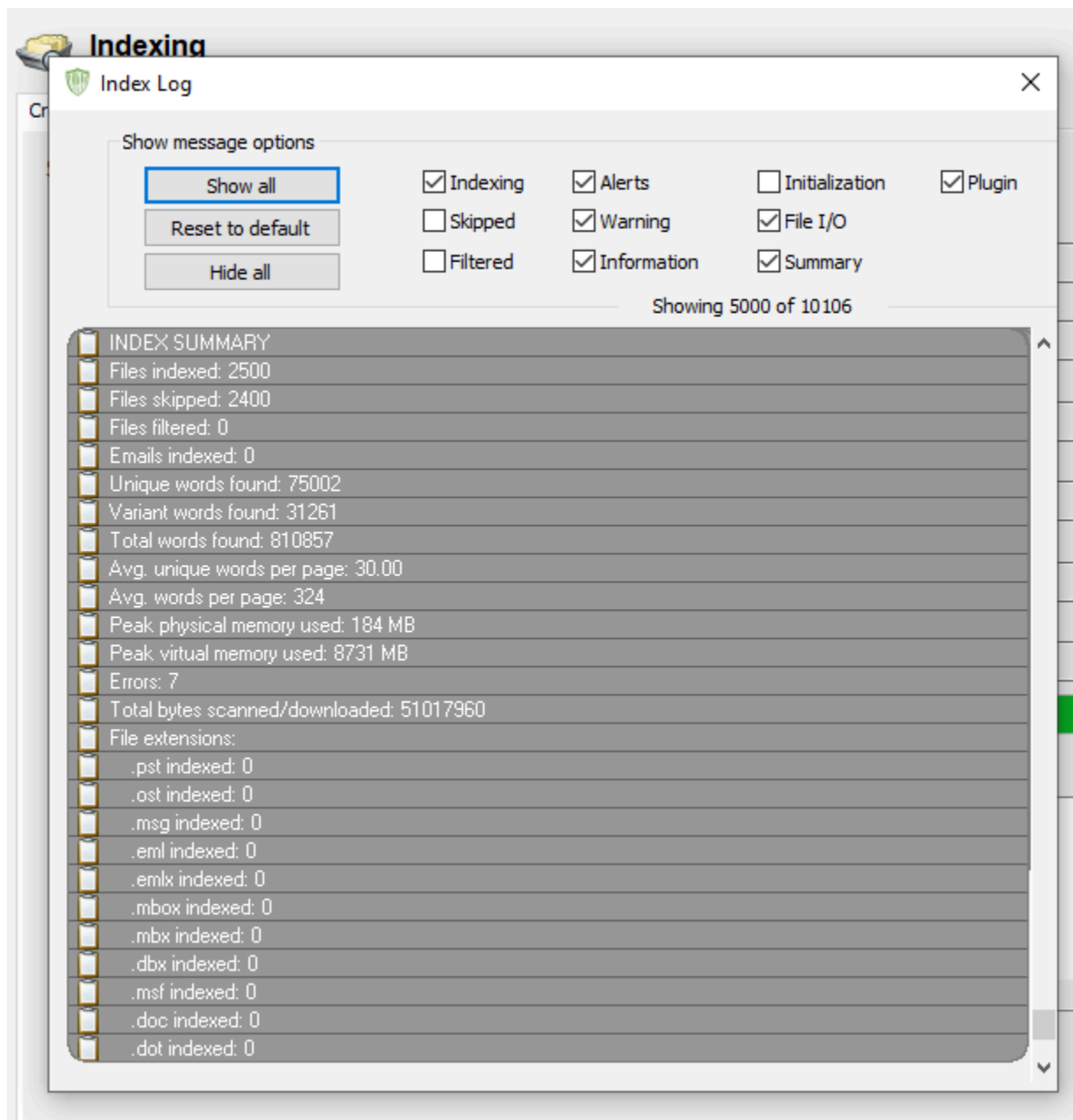
Index of files in:  
chapter04-Terry\_work\_usb:

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, .shtml, .shml, .xml, .xhtml, .php, .php3, .asp, .aspx,  
.cfm, .js, .pl, .cgi, .swf, .nfo, .dat, .wpd, .mp3, .mp4, .m4v, .dwf, .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

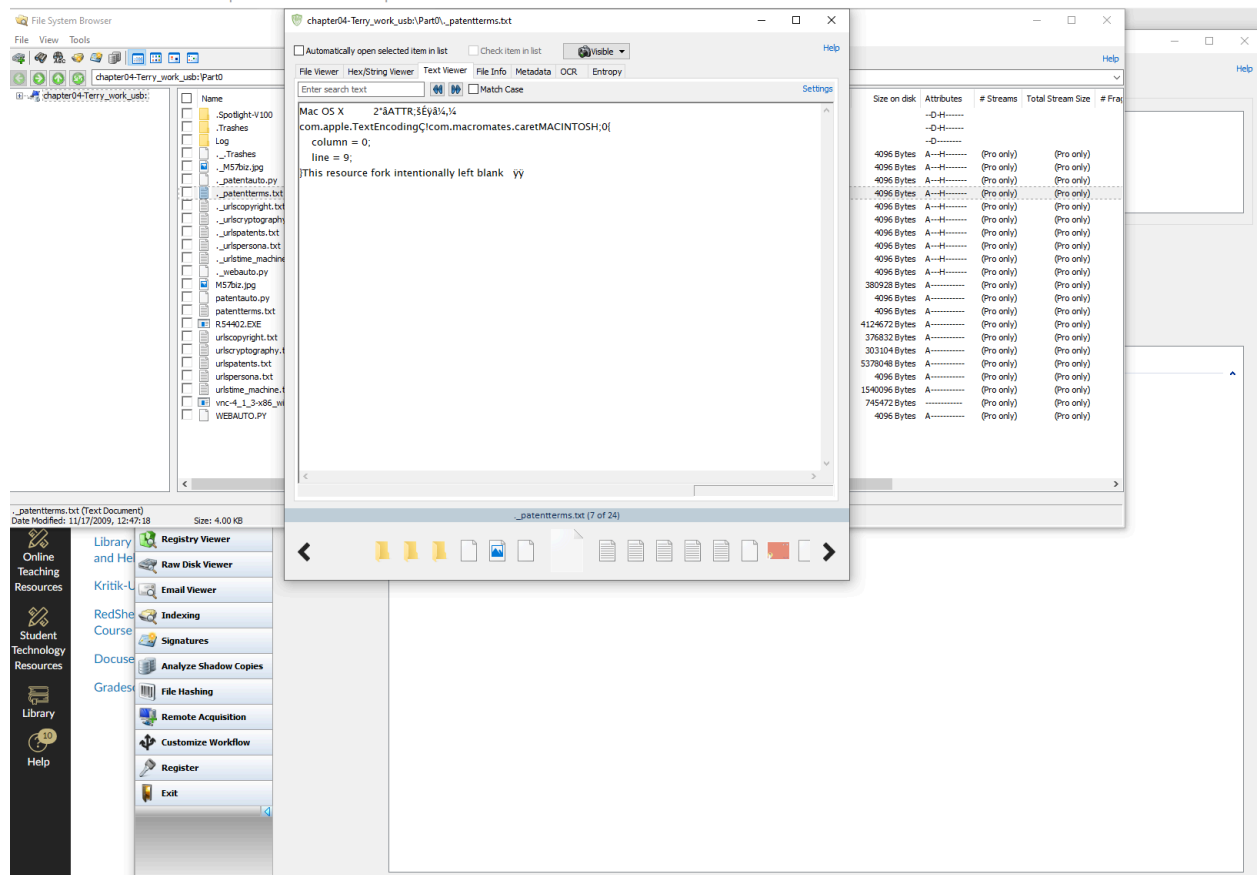
I renamed the index appropriately.

## Step 12: Examine Log



After the index, no errors were reported and it was able to process 2500 files since that is the maximum allowed while using the free trial.

### Step 13: Manage Case



I examined some of the files on the drive and there doesn't seem to be any criminal activity on the drive. The files seem to be related to work or logs.