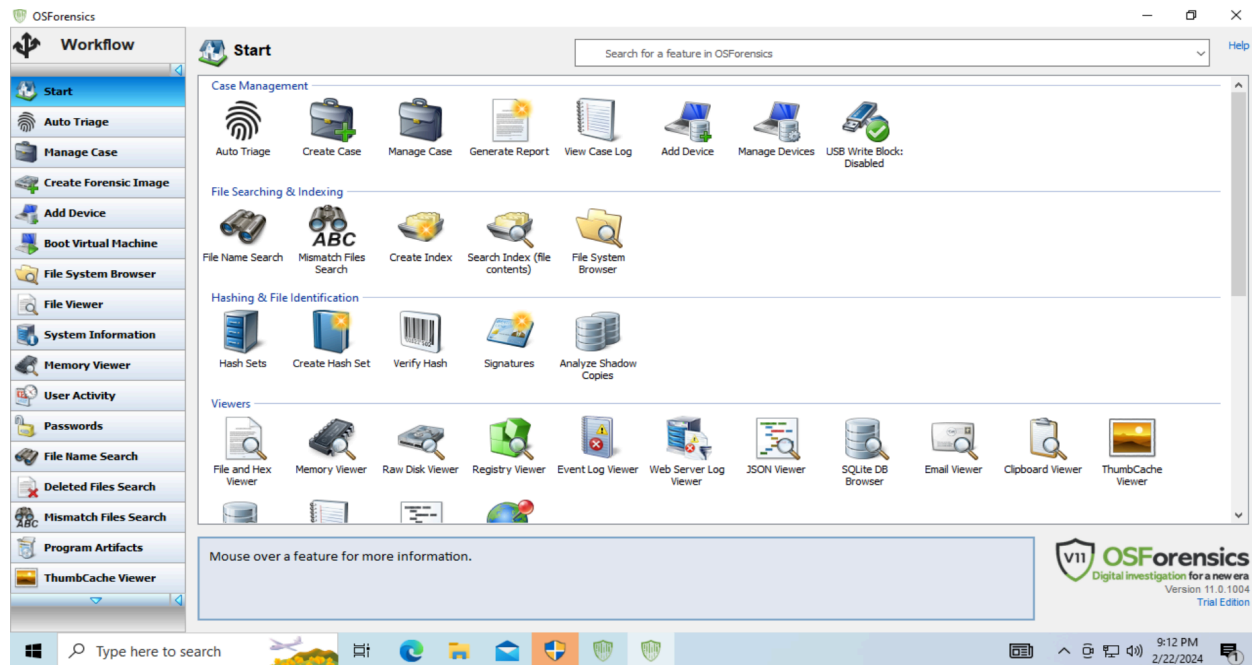


Task 1:




In this step, I have successfully downloaded OSforensics.

Task 2:

New Case

The 'New Case' dialog box is open, showing various input fields for case information. The fields are organized into sections: Chain of Custody, Custom Fields, and Case Narrative. The Case Narrative section is expanded, showing fields for Case Name, Case Type, Investigator, Organization, Contact Details, Timezone, Display Date Format, Default Drive, Acquisition Type, Case Folder, and checkboxes for Log case activity and Enable USB Write-block. The Case Name is 'M57-Terrys USB Drive', Case Type is 'Criminal', Investigator is 'Timothy Doan', Organization is 'Google', Contact Details is '916-540-9379', Timezone is 'Local (UTC -8:00) Pacific Time (US & Canada)', Display Date Format is '2/23/2024 (Default)', Default Drive is 'C: \ [Local]', Acquisition Type is 'Investigate Disk(s) from Another Machine', Case Folder is 'C: \Users\timothyd\Documents\PassMark\OSForensics\Cases\M57-Terrys USB [', Log case activity is checked, and Enable USB Write-block is unchecked. The dialog has 'OK' and 'Cancel' buttons at the bottom right.

In this step, I am in OSForensics and starting a new case. I am filling out the inputs to start the case.

 Add Device ×

Evidence Source [Help](#)

☐ Drive Letter C:\ Mount Image...
☒ Forensics Mode ☐ Standard Mode

☐ Physical Disk \\.\PhysicalDrive0

☒ Image File C:\Users\timothyd\Desktop\chapter04-Terry_work_usb.E01 ...
Partition: <entire image file>

☐ Folder / Network Path ...

☐ File Path ...

☐ Volume Shadow Copy ...
Select Shadow...

☐ BitLocker Encrypted Drive Drive-C:\ Verify Key...

Display Name

chapter04-Terry_work_usb Usage Example:
"chapter04-Terry_work_usb:\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.

OK Cancel Manage Devices...

In this step, I am adding a device to this case and then adding Terry's work usb.



File Name Search


Device to Scan:

Preset: User-defined Search

Sort by: File Name

File Details	File List	Thumbnails	Timeline	Map		
<input type="checkbox"/>	File Name	Location	Type	Date Modified	Date Created	Date Accessed

I am in Terry's work usb and am searching for files that have kitty in their name. After doing this search, nothing is coming up.



Indexing

Step 1 of 5

What types of files would you like to index?


☒ Use Pre-defined File Types

- ☒ E-mails ☒ Attachments
- ☒ Office + PDF documents
- ☒ ZIP and compressed archives
- ☒ Images
- ☒ Plain text files
- ☒ Web files + XML
- ☒ Video, audio and other media
- ☒ 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
- ☒ Windows Event Log files

☐ Use previously saved configuration:

Configuration	File Types

In this step, I am in the create index tab and checking all the boxes.

 **Indexing**

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:	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

In this step, I am adding Terry's work usb so that it can be indexed.

 **Indexing**

Create Index Search Index

Step 5 of 5

Start Time	Thu Feb 22 22:10:49 2024	Finish Time	
Files Indexed	27	Time Elapsed	00:00:13
Emails Indexed	0	Peak Phys. Mem. Used	174 MB
Alerts	0	Peak Virt. Mem. Used	8732 MB
Warnings	0	Max File & Emails	2500
Total Bytes	8.43 MB	Unique Words	70059

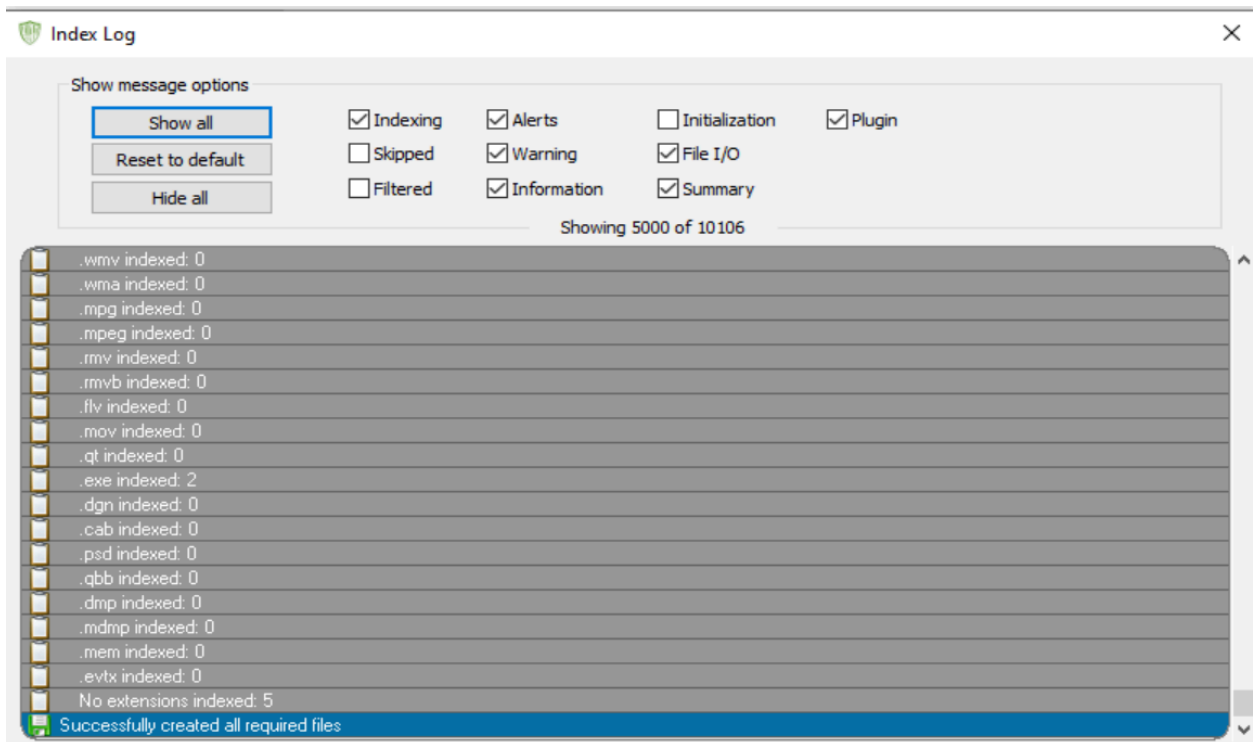
Current Action: Indexing Show Log

Thread #	Indexing file
Thread 1	chapter04-Terry_work_usb:\Part0\Log\2009-12-03_0005425f_big.jpg
Thread 2	chapter04-Terry_work_usb:\Part0\Log\2009-12-03_0007171f_big.jpg
Thread 3	chapter04-Terry_work_usb:\Part0\Log\2009-12-03_000e6a1f_big.jpg
Thread 4	chapter04-Terry_work_usb:\Part0\Log\2009-12-03_0013e85f_big.jpg

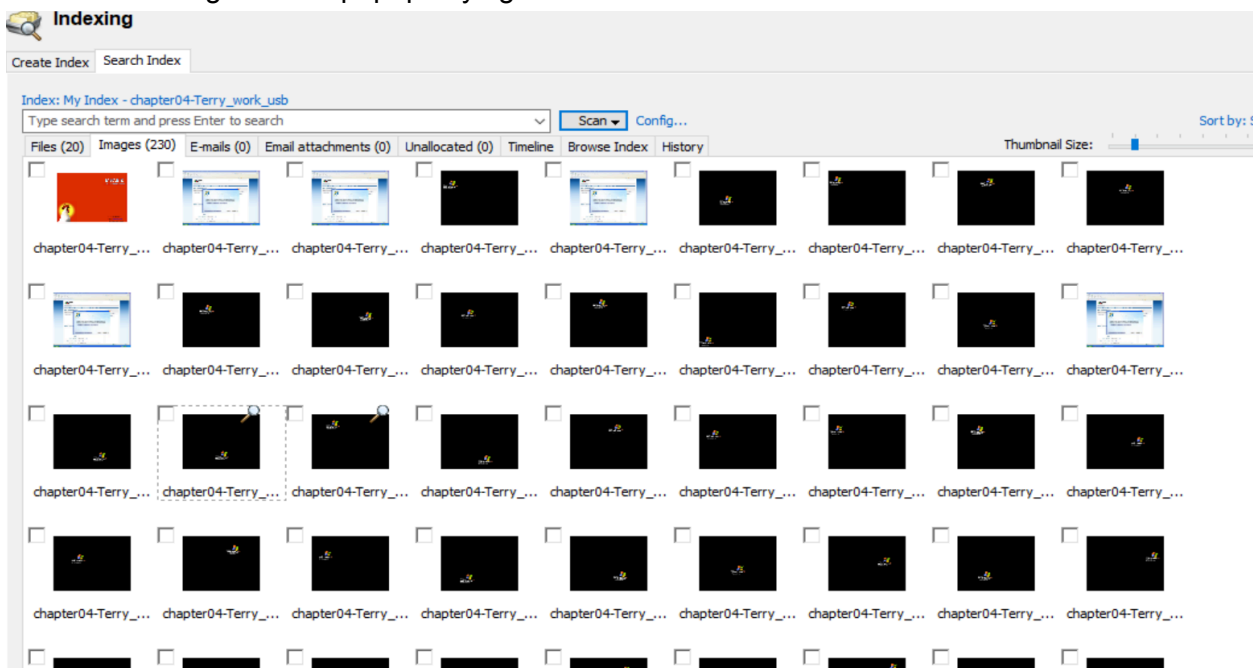
< >

<< New Index Save configuration Show Precog Results Cancel

In this step, I am indexing the usb drive.



The USB drive has finished indexing and now I am looking at the logs. There seems to be no errors but it did give me a popup saying that it couldn't index some files for some reason.



I am now able to look through the image and text files that were indexed on her usb drive.

Report:

Upon indexing Terry's usb drive and examining the image and txt files, I was not able to find any evidence that Terry was involved in any illicit or illegal activity that is against company policy.

When looking through her image files, I just see screenshots of some emails and Internet Explorer pop ups. After looking through that, I looked through her txt files and wasn't able to find anything suspicious either. Most of these files just contain links or work notes it seems like.

These files I have examined are important because they can either prove an employee's innocence, or prove that an employee is doing things that are against the company's policy. In this case, these files have proven Terry's innocence and that she wasn't doing anything that will go against her company's policies.