CSU, College of Engineering and Computer Science
Department of Computer Science
CSC 153 – Computer Forensics Principles and Practice

Catherine Nguyen
CSC 153
10/28/2020

Lab 1: Forensic Investigation on Your Own Personal Computer

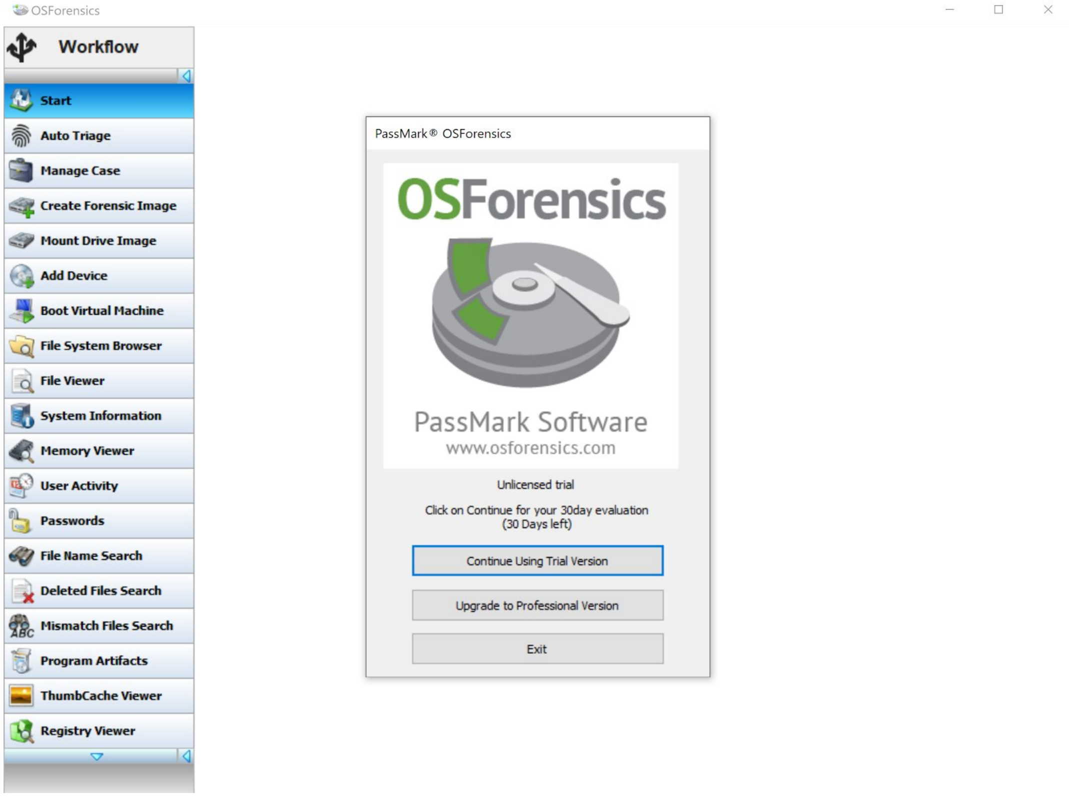
Objectives:

- Become familiar with a forensics tool.
- Become familiar with the basic forensics process.

Instructions:

Do a forensics investigation on your own personal computer using any case management tools (or some other forensics tools) you choose. OSForensics is recommended for this assignment. You may install the trial copy on your own machine. Other tools such as FTK, Sleuthkit/Autopsy_Browser, Encase, ProDiscover Basic, etc. will also work. **In this lab, I decided to use the recommended tool, OSForensics.**

I first started off by downloading the free trial on my laptop which has a 500GB SSD. Once the download was complete, I opened OSForensics and continued with my free trial.

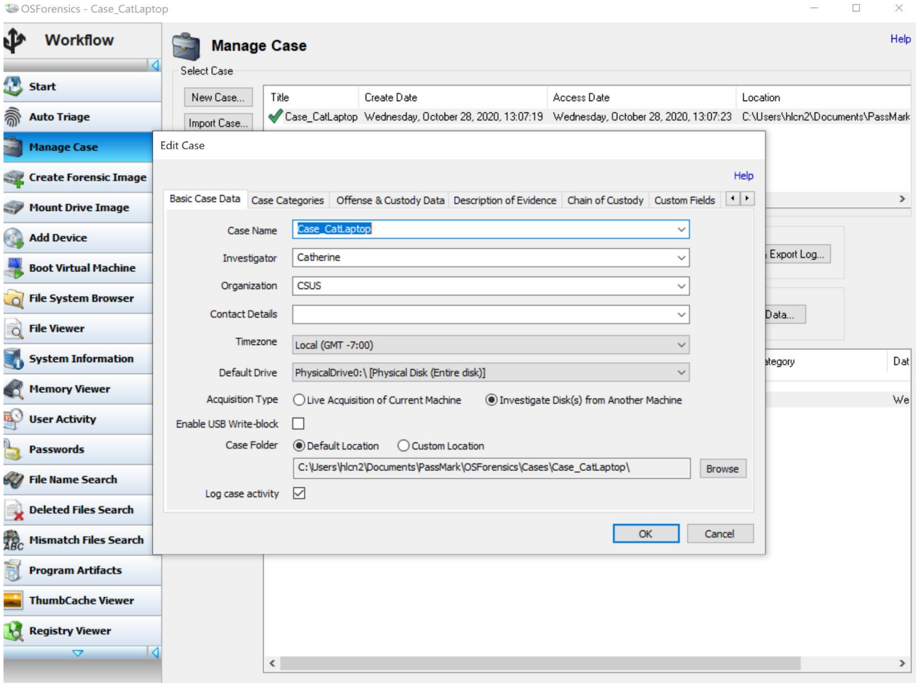


Unlicensed trial

Click on Continue for your 30day evaluation
(30 Days left)

Fig 1: In the progress of downloading OSForensics

The next step was to create a new case, which will allow running all the available features on OSforensics to further this lab's progress.



Manage Case

Select Case

Title	Create Date	Access Date	Location
✓ Case_CatLaptop	Wednesday, October 28, 2020, 13:07:19	Wednesday, October 28, 2020, 13:07:23	C:\Users\hlcn2\Documents\PassMark

Edit Case

Case Name: Case_CatLaptop

Investigator: Catherine

Organization: CSUS

Contact Details:

Timezone: Local (GMT -7:00)

Default Drive: PhysicalDrive0:\ [Physical Disk (Entire disk)]

Acquisition Type: ○ Live Acquisition of Current Machine ● Investigate Disk(s) from Another Machine

Enable USB Write-block: □

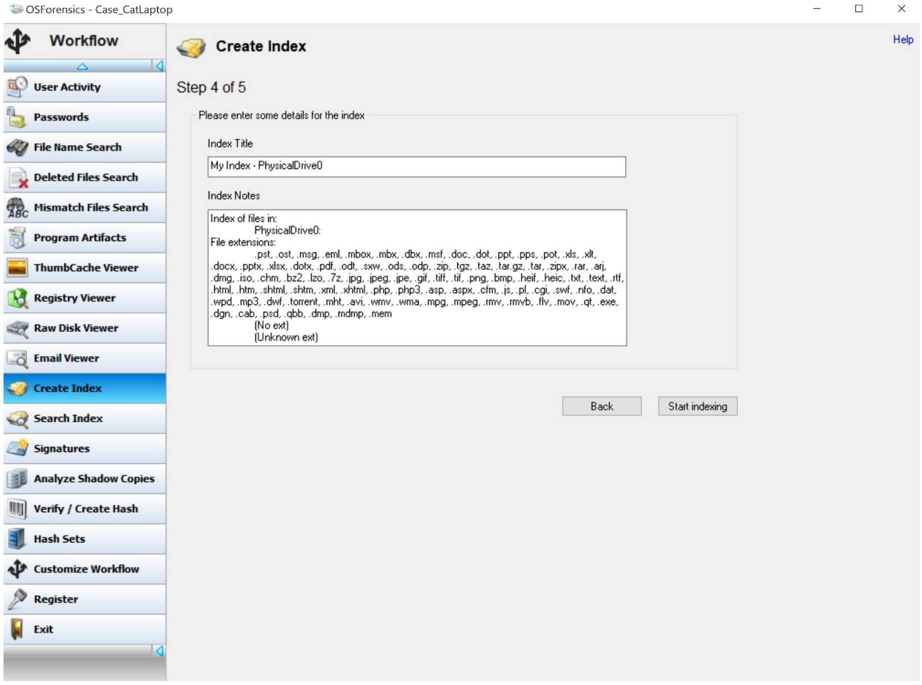
Case Folder: ● Default Location ○ Custom Location

C:\Users\hlcn2\Documents\PassMark\OSForensics\Cases\Case_CatLaptop\

Log case activity: ☑

Fig 2: Process of making a new case.

Next was to create an index of my drive, this would allow me to search index through all my files. I decided to only index my files to save time.



Create Index

Step 4 of 5

Please enter some details for the index

Index Title

My Index - PhysicalDrive0

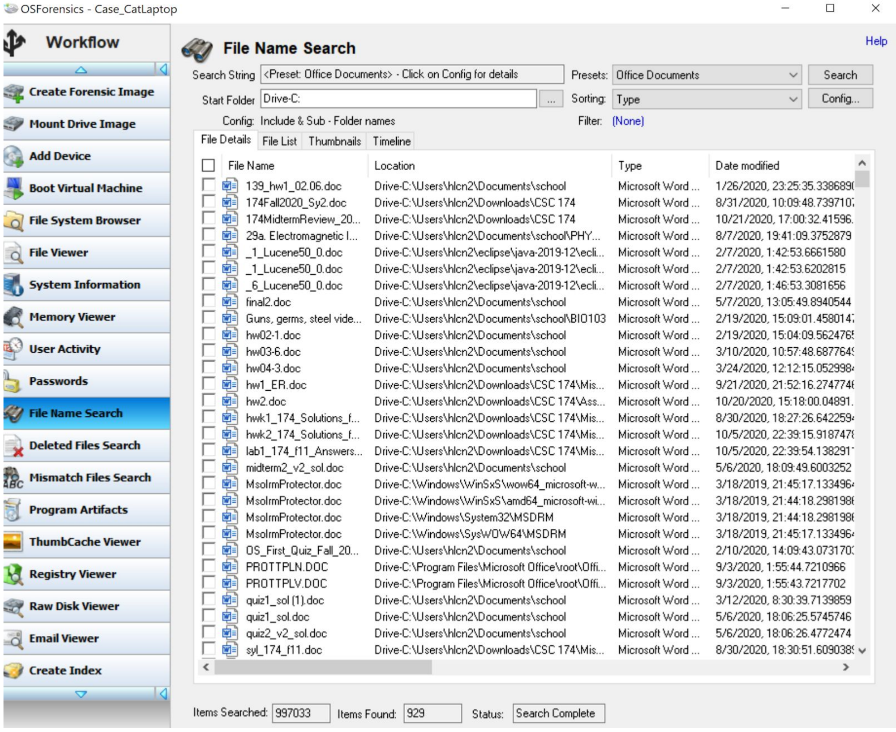
Index Notes

```
Index of files in:
		PhysicalDrive0:
File extensions:
		.pst, .ost, .msg, .eml, .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, .shtm, .xml, .xhtml, .php, .php3, .asp, .aspx, .cfm, .js, .pl, .cgi, .swf, .nfo, .dat,
.wpd, .mp3, .dwf, .torrent, .mht, .avi, .wmv, .wma, .mpg, .mpeg, .rmv, .rmvb, .flv, .mov, .qt, .exe,
.dgn, .cab, .psd, .qbb, .dmp, .mdmp, .mem
		(No ext)
		(Unknown ext)
```

Fig 3: Process of creating an index.

1. **Provide screenshots showing the following information:**

- **Number and type of documents (Word, PowerPoint, Excel, etc)**
  i. To find the number of documents on my laptop I used file name search and changed the preset to office documents. This resulted in 929 files. 39 .dotx, 4 .odt, 649 .pdf, 14 .pot, 38 .ppt, 28 . pptx, 22 .xls, 40 .xlsx.



OSForensics - Case_CatLaptop

File Name Search

Search String: <Preset: Office Documents> - Click on Config for details

Presets: Office Documents

Start Folder: Drive-C:

Sorting: Type

Config: Include & Sub - Folder names

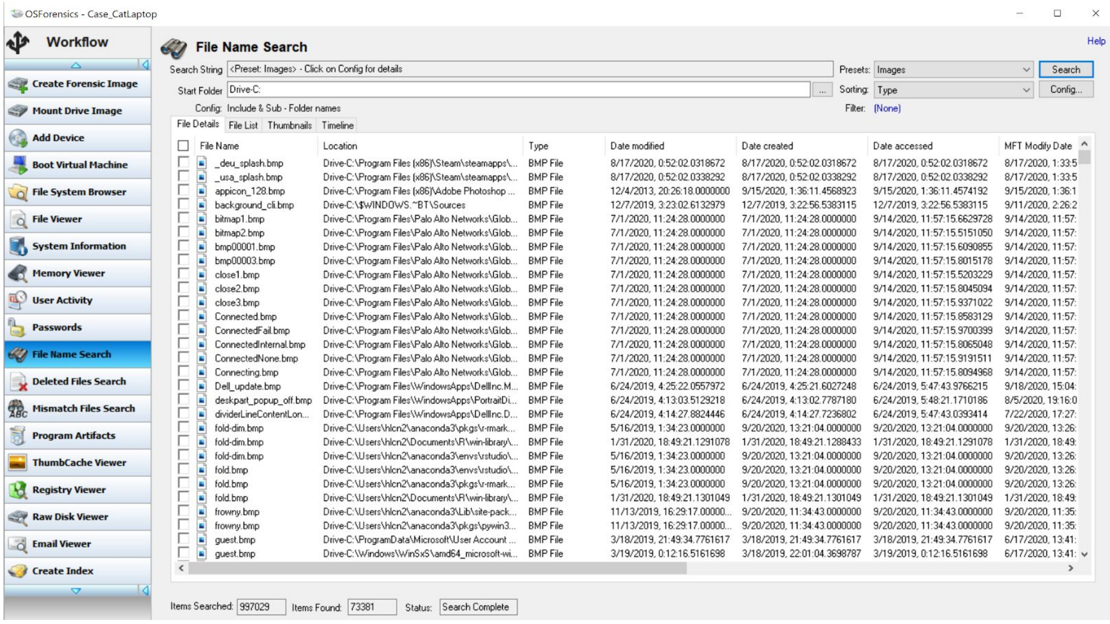
Filter: (None)

☐ File Name	Location	Type	Date modified
139_hw1_02.06.doc	Drive-C:\Users\hlcn2\Documents\school	Microsoft Word ...	1/26/2020, 23:25:35.338689
174Fall2020_Sy2.doc	Drive-C:\Users\hlcn2\Downloads\CSC 174	Microsoft Word ...	8/31/2020, 10:09:48.739710
174MidtermReview_20...	Drive-C:\Users\hlcn2\Downloads\CSC 174	Microsoft Word ...	10/21/2020, 17:00:32.41596.
29a. Electromagnetic I...	Drive-C:\Users\hlcn2\Documents\school\PHY...	Microsoft Word ...	8/7/2020, 19:41:09.3752879
_1_Lucene50_0.doc	Drive-C:\Users\hlcn2\eclipse\java-2019-12\ecli...	Microsoft Word ...	2/7/2020, 1:42:53.6661580
_1_Lucene50_0.doc	Drive-C:\Users\hlcn2\eclipse\java-2019-12\ecli...	Microsoft Word ...	2/7/2020, 1:42:53.6202815
_6_Lucene50_0.doc	Drive-C:\Users\hlcn2\eclipse\java-2019-12\ecli...	Microsoft Word ...	2/7/2020, 1:46:53.3081656
final2.doc	Drive-C:\Users\hlcn2\Documents\school	Microsoft Word ...	5/7/2020, 13:05:49.8940544
Guns, germs, steel vide...	Drive-C:\Users\hlcn2\Documents\school\BIO103	Microsoft Word ...	2/19/2020, 15:09:01.458014
hw02-1.doc	Drive-C:\Users\hlcn2\Documents\school	Microsoft Word ...	2/19/2020, 15:04:09.562476
hw03-6.doc	Drive-C:\Users\hlcn2\Documents\school	Microsoft Word ...	3/10/2020, 10:57:48.687764
hw04-3.doc	Drive-C:\Users\hlcn2\Documents\school	Microsoft Word ...	3/24/2020, 12:12:15.052998
hw1_ER.doc	Drive-C:\Users\hlcn2\Downloads\CSC 174\Mis...	Microsoft Word ...	9/21/2020, 21:52:16.274774
hw2.doc	Drive-C:\Users\hlcn2\Downloads\CSC 174\Ass...	Microsoft Word ...	10/20/2020, 15:18:00.04891.
hwk1_174_Solutions_f...	Drive-C:\Users\hlcn2\Downloads\CSC 174\Mis...	Microsoft Word ...	8/30/2020, 18:27:26.642259
hwk2_174_Solutions_f...	Drive-C:\Users\hlcn2\Downloads\CSC 174\Mis...	Microsoft Word ...	10/5/2020, 22:39:15.918747
lab1_174_f11_Answers...	Drive-C:\Users\hlcn2\Downloads\CSC 174\Mis...	Microsoft Word ...	10/5/2020, 22:39:54.138291
midterm2_v2_sol.doc	Drive-C:\Users\hlcn2\Documents\school	Microsoft Word ...	5/6/2020, 18:09:49.6003252
MsolrmProtector.doc	Drive-C:\Windows\WinSxS\wow64_microsoft-w...	Microsoft Word ...	3/18/2019, 21:45:17.133496
MsolrmProtector.doc	Drive-C:\Windows\WinSxS\amd64_microsoft-wi...	Microsoft Word ...	3/18/2019, 21:44:18.298198
MsolrmProtector.doc	Drive-C:\Windows\System32\MSDRM	Microsoft Word ...	3/18/2019, 21:44:18.298198
MsolrmProtector.doc	Drive-C:\Windows\SysWOW64\MSDRM	Microsoft Word ...	3/18/2019, 21:45:17.133496
OS_First_Quiz_Fall_20...	Drive-C:\Users\hlcn2\Documents\school	Microsoft Word ...	2/10/2020, 14:09:43.073170
PROTTPLN.DOC	Drive-C:\Program Files\Microsoft Office\root\Offi...	Microsoft Word ...	9/3/2020, 1:55:44.7210966
PROTTPLV.DOC	Drive-C:\Program Files\Microsoft Office\root\Offi...	Microsoft Word ...	9/3/2020, 1:55:43.7217702
quiz1_sol (1).doc	Drive-C:\Users\hlcn2\Documents\school	Microsoft Word ...	3/12/2020, 8:30:39.7139859
quiz1_sol.doc	Drive-C:\Users\hlcn2\Documents\school	Microsoft Word ...	5/6/2020, 18:06:25.5745746
quiz2_v2_sol.doc	Drive-C:\Users\hlcn2\Documents\school	Microsoft Word ...	5/6/2020, 18:06:26.4772474
syl_174_f11.doc	Drive-C:\Users\hlcn2\Downloads\CSC 174\Mis...	Microsoft Word ...	8/30/2020, 18:30:51.609038

Items Searched: 997033 Items Found: 929 Status: Search Complete

Fig 4: Search for all the Office Documents on my Laptop.

- **Number of images**
  i. For the number of images, I went into the “File name search” feature and change the preset to images only. That resulted in 73381 image files. Which is a lot more than I expected.



OSForensics - Case_CatLaptop

File Name Search

Search String: <Preset: Images> - Click on Config for details

Presets: Images

Start Folder: Drive-C:

Sorting: Type

Config: Include & Sub - Folder names

Filter: (None)

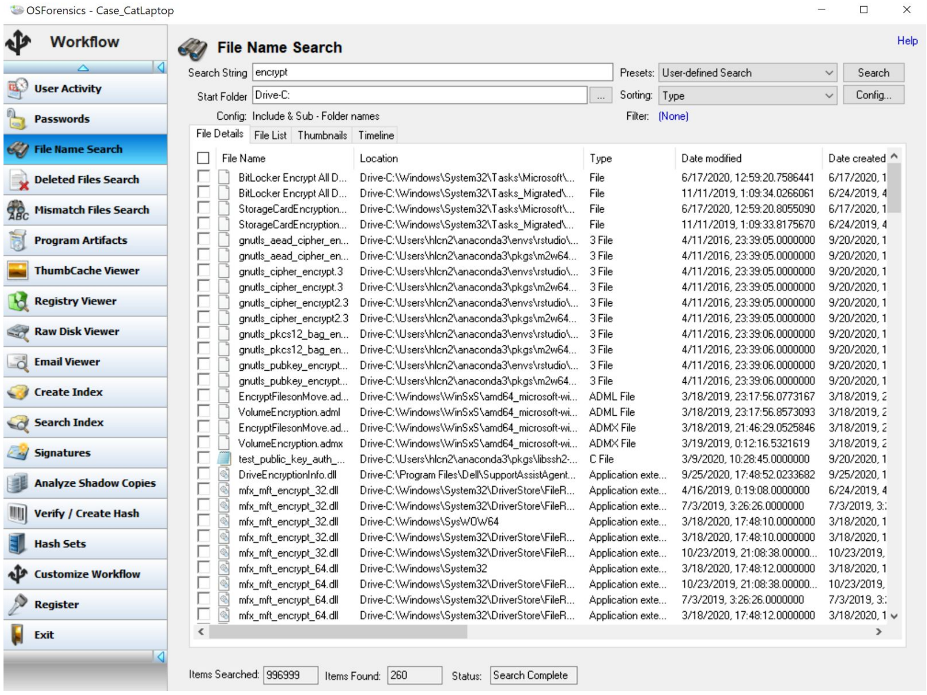
☐ File Name	Location	Type	Date modified	Date created	Date accessed	MFT Modify Date
_deu_splash.bmp	Drive-C:\Program Files (x86)\Steam\steamapps\...	BMP File	8/17/2020, 0:52:02.0318672	8/17/2020, 0:52:02.0318672	8/17/2020, 0:52:02.0318672	8/17/2020, 1:33:5
_usa_splash.bmp	Drive-C:\Program Files (x86)\Steam\steamapps\...	BMP File	8/17/2020, 0:52:02.0338292	8/17/2020, 0:52:02.0338292	8/17/2020, 0:52:02.0338292	8/17/2020, 1:33:5
appicon_128.bmp	Drive-C:\Program Files (x86)\Adobe Photoshop ...	BMP File	12/4/2013, 20:26:18.0000000	9/15/2020, 1:36:11.4568923	9/15/2020, 1:36:11.4574192	9/15/2020, 1:36:1
background_cli.bmp	Drive-C:\$WINDOWS.~BT\Sources	BMP File	12/7/2019, 3:23:02.6132979	12/7/2019, 3:22:56.5383115	12/7/2019, 3:22:56.5383115	9/11/2020, 2:26:2
bitmap1.bmp	Drive-C:\Program Files\Palo Alto Networks\Glob...	BMP File	7/1/2020, 11:24:28.0000000	7/1/2020, 11:24:28.0000000	9/14/2020, 11:57:15.6629728	9/14/2020, 11:57:
bitmap2.bmp	Drive-C:\Program Files\Palo Alto Networks\Glob...	BMP File	7/1/2020, 11:24:28.0000000	7/1/2020, 11:24:28.0000000	9/14/2020, 11:57:15.5151050	9/14/2020, 11:57:
bmp00001.bmp	Drive-C:\Program Files\Palo Alto Networks\Glob...	BMP File	7/1/2020, 11:24:28.0000000	7/1/2020, 11:24:28.0000000	9/14/2020, 11:57:15.6090855	9/14/2020, 11:57:
bmp00003.bmp	Drive-C:\Program Files\Palo Alto Networks\Glob...	BMP File	7/1/2020, 11:24:28.0000000	7/1/2020, 11:24:28.0000000	9/14/2020, 11:57:15.8015178	9/14/2020, 11:57:
close1.bmp	Drive-C:\Program Files\Palo Alto Networks\Glob...	BMP File	7/1/2020, 11:24:28.0000000	7/1/2020, 11:24:28.0000000	9/14/2020, 11:57:15.5203229	9/14/2020, 11:57:
close2.bmp	Drive-C:\Program Files\Palo Alto Networks\Glob...	BMP File	7/1/2020, 11:24:28.0000000	7/1/2020, 11:24:28.0000000	9/14/2020, 11:57:15.8045094	9/14/2020, 11:57:
close3.bmp	Drive-C:\Program Files\Palo Alto Networks\Glob...	BMP File	7/1/2020, 11:24:28.0000000	7/1/2020, 11:24:28.0000000	9/14/2020, 11:57:15.9371022	9/14/2020, 11:57:
Connected.bmp	Drive-C:\Program Files\Palo Alto Networks\Glob...	BMP File	7/1/2020, 11:24:28.0000000	7/1/2020, 11:24:28.0000000	9/14/2020, 11:57:15.8583129	9/14/2020, 11:57:
ConnectedFail.bmp	Drive-C:\Program Files\Palo Alto Networks\Glob...	BMP File	7/1/2020, 11:24:28.0000000	7/1/2020, 11:24:28.0000000	9/14/2020, 11:57:15.9700399	9/14/2020, 11:57:
ConnectedInternal.bmp	Drive-C:\Program Files\Palo Alto Networks\Glob...	BMP File	7/1/2020, 11:24:28.0000000	7/1/2020, 11:24:28.0000000	9/14/2020, 11:57:15.8065048	9/14/2020, 11:57:
ConnectedNone.bmp	Drive-C:\Program Files\Palo Alto Networks\Glob...	BMP File	7/1/2020, 11:24:28.0000000	7/1/2020, 11:24:28.0000000	9/14/2020, 11:57:15.9191511	9/14/2020, 11:57:
Connecting.bmp	Drive-C:\Program Files\Palo Alto Networks\Glob...	BMP File	7/1/2020, 11:24:28.0000000	7/1/2020, 11:24:28.0000000	9/14/2020, 11:57:15.8094968	9/14/2020, 11:57:
Dell_update.bmp	Drive-C:\Program Files\WindowsApps\DellInc.M...	BMP File	6/24/2019, 4:25:22.0557972	6/24/2019, 4:25:21.6027248	6/24/2019, 5:47:43.9766215	9/18/2020, 15:04:
deskpart_popup_off.bmp	Drive-C:\Program Files\WindowsApps\PortraitDi...	BMP File	6/24/2019, 4:13:03.5129218	6/24/2019, 4:13:02.7787180	6/24/2019, 5:48:21.1710186	8/5/2020, 19:16:0
dividerLineContentLon...	Drive-C:\Program Files\WindowsApps\DellInc.D...	BMP File	6/24/2019, 4:14:27.8824446	6/24/2019, 4:14:27.7236802	6/24/2019, 5:47:43.0393414	7/22/2020, 17:27:
fold-dim.bmp	Drive-C:\Users\hlcn2\anaconda3\pkgs\r-rmark...	BMP File	5/16/2019, 1:34:23.0000000	9/20/2020, 13:21:04.0000000	9/20/2020, 13:21:04.0000000	9/20/2020, 13:26:
fold-dim.bmp	Drive-C:\Users\hlcn2\Documents\R\win-library\...	BMP File	1/31/2020, 18:49:21.1291078	1/31/2020, 18:49:21.1288433	1/31/2020, 18:49:21.1291078	1/31/2020, 18:49:
fold-dim.bmp	Drive-C:\Users\hlcn2\anaconda3\envs\rstudio\...	BMP File	5/16/2019, 1:34:23.0000000	9/20/2020, 13:21:04.0000000	9/20/2020, 13:21:04.0000000	9/20/2020, 13:26:
fold.bmp	Drive-C:\Users\hlcn2\anaconda3\envs\rstudio\...	BMP File	5/16/2019, 1:34:23.0000000	9/20/2020, 13:21:04.0000000	9/20/2020, 13:21:04.0000000	9/20/2020, 13:26:
fold.bmp	Drive-C:\Users\hlcn2\anaconda3\pkgs\r-rmark...	BMP File	5/16/2019, 1:34:23.0000000	9/20/2020, 13:21:04.0000000	9/20/2020, 13:21:04.0000000	9/20/2020, 13:26:
fold.bmp	Drive-C:\Users\hlcn2\Documents\R\win-library\...	BMP File	1/31/2020, 18:49:21.1301049	1/31/2020, 18:49:21.1301049	1/31/2020, 18:49:21.1301049	1/31/2020, 18:49:
frowny.bmp	Drive-C:\Users\hlcn2\anaconda3\Lib\site-pack...	BMP File	11/13/2019, 16:29:17.00000...	9/20/2020, 11:34:43.0000000	9/20/2020, 11:34:43.0000000	9/20/2020, 11:35:
frowny.bmp	Drive-C:\Users\hlcn2\anaconda3\pkgs\pywin3...	BMP File	11/13/2019, 16:29:17.00000...	9/20/2020, 11:34:43.0000000	9/20/2020, 11:34:43.0000000	9/20/2020, 11:35:
guest.bmp	Drive-C:\ProgramData\Microsoft\User Account ...	BMP File	3/18/2019, 21:49:34.7761617	3/18/2019, 21:49:34.7761617	3/18/2019, 21:49:34.7761617	6/17/2020, 13:41:
guest.bmp	Drive-C:\Windows\WinSxS\amd64_microsoft-wi...	BMP File	3/19/2019, 0:12:16.5161698	3/18/2019, 22:01:04.3698787	3/19/2019, 0:12:16.5161698	6/17/2020, 13:41:

Items Searched: 997029 Items Found: 73381 Status: Search Complete

Fig 5: Search for all image files.

- **Number and types of encrypted files**

  i. I am not sure if this is the correct way to search for encrypted files, but this was the best I could do. Fig 6. There were 260 encrypted files. However, If I change the preset into encrypted I get 0 results. Fig 7.

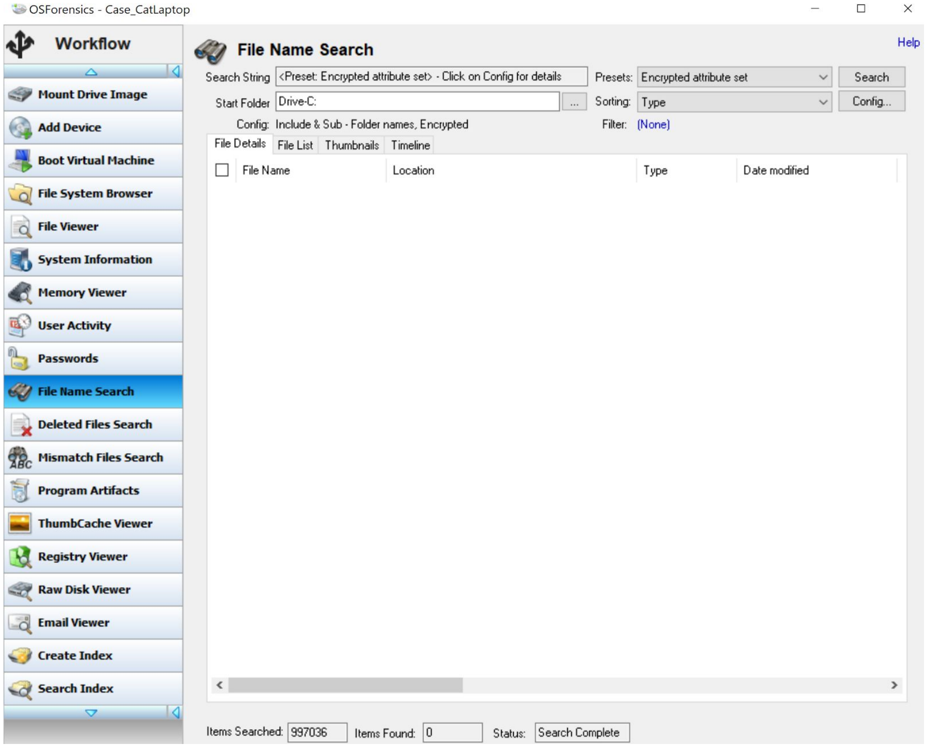


Search String: encrypt
Presets: User-defined Search
Start Folder: Drive-C:
Sorting: Type
Config: Include & Sub - Folder names
Filter: (None)

□	File Name	Location	Type	Date modified	Date created
□	BitLocker Encrypt All D...	Drive-C:\Windows\System32\Tasks\Microsoft\...	File	6/17/2020, 12:59:20.7586441	6/17/2020, 1
□	BitLocker Encrypt All D...	Drive-C:\Windows\System32\Tasks_Migrated\...	File	11/11/2019, 1:09:34.0266061	6/24/2019, 4
□	StorageCardEncryption...	Drive-C:\Windows\System32\Tasks\Microsoft\...	File	6/17/2020, 12:59:20.8055090	6/17/2020, 1
□	StorageCardEncryption...	Drive-C:\Windows\System32\Tasks_Migrated\...	File	11/11/2019, 1:09:33.8175670	6/24/2019, 4
□	gnutls_aead_cipher_en...	Drive-C:\Users\hlcn2\anaconda3\envs\rstudio\...	3 File	4/11/2016, 23:39:05.0000000	9/20/2020, 1
□	gnutls_aead_cipher_en...	Drive-C:\Users\hlcn2\anaconda3\pkgs\m2w64...	3 File	4/11/2016, 23:39:05.0000000	9/20/2020, 1
□	gnutls_cipher_encrypt.3	Drive-C:\Users\hlcn2\anaconda3\envs\rstudio\...	3 File	4/11/2016, 23:39:05.0000000	9/20/2020, 1
□	gnutls_cipher_encrypt.3	Drive-C:\Users\hlcn2\anaconda3\pkgs\m2w64...	3 File	4/11/2016, 23:39:05.0000000	9/20/2020, 1
□	gnutls_cipher_encrypt2.3	Drive-C:\Users\hlcn2\anaconda3\envs\rstudio\...	3 File	4/11/2016, 23:39:05.0000000	9/20/2020, 1
□	gnutls_cipher_encrypt2.3	Drive-C:\Users\hlcn2\anaconda3\pkgs\m2w64...	3 File	4/11/2016, 23:39:05.0000000	9/20/2020, 1
□	gnutls_pkcs12_bag_en...	Drive-C:\Users\hlcn2\anaconda3\envs\rstudio\...	3 File	4/11/2016, 23:39:06.0000000	9/20/2020, 1
□	gnutls_pkcs12_bag_en...	Drive-C:\Users\hlcn2\anaconda3\pkgs\m2w64...	3 File	4/11/2016, 23:39:06.0000000	9/20/2020, 1
□	gnutls_pubkey_encrypt...	Drive-C:\Users\hlcn2\anaconda3\envs\rstudio\...	3 File	4/11/2016, 23:39:06.0000000	9/20/2020, 1
□	gnutls_pubkey_encrypt...	Drive-C:\Users\hlcn2\anaconda3\pkgs\m2w64...	3 File	4/11/2016, 23:39:06.0000000	9/20/2020, 1
□	EncryptFilesonMove.ad...	Drive-C:\Windows\WinSxS\amd64_microsoft-wi...	ADML File	3/18/2019, 23:17:56.0773167	3/18/2019, 2
□	VolumeEncryption.adml	Drive-C:\Windows\WinSxS\amd64_microsoft-wi...	ADML File	3/18/2019, 23:17:56.8573093	3/18/2019, 2
□	EncryptFilesonMove.ad...	Drive-C:\Windows\WinSxS\amd64_microsoft-wi...	ADMX File	3/18/2019, 21:46:29.0525846	3/18/2019, 2
□	VolumeEncryption.admx	Drive-C:\Windows\WinSxS\amd64_microsoft-wi...	ADMX File	3/19/2019, 0:12:16.5321619	3/18/2019, 2
□	test_public_key_auth_...	Drive-C:\Users\hlcn2\anaconda3\pkgs\libssh2-...	C File	3/9/2020, 10:28:45.0000000	9/20/2020, 1
□	DriveEncryptionInfo.dll	Drive-C:\Program Files\Dell\SupportAssistAgent...	Application exte...	9/25/2020, 17:48:52.0233682	9/25/2020, 1
□	mfx_mft_encrypt_32.dll	Drive-C:\Windows\System32\DriverStore\FileR...	Application exte...	4/16/2019, 0:19:08.0000000	6/24/2019, 4
□	mfx_mft_encrypt_32.dll	Drive-C:\Windows\System32\DriverStore\FileR...	Application exte...	7/3/2019, 3:26:26.0000000	7/3/2019, 3:
□	mfx_mft_encrypt_32.dll	Drive-C:\Windows\SysWOW64	Application exte...	3/18/2020, 17:48:10.0000000	3/18/2020, 1
□	mfx_mft_encrypt_32.dll	Drive-C:\Windows\System32\DriverStore\FileR...	Application exte...	3/18/2020, 17:48:10.0000000	3/18/2020, 1
□	mfx_mft_encrypt_32.dll	Drive-C:\Windows\System32\DriverStore\FileR...	Application exte...	10/23/2019, 21:08:38.00000...	10/23/2019,
□	mfx_mft_encrypt_64.dll	Drive-C:\Windows\System32	Application exte...	3/18/2020, 17:48:12.0000000	3/18/2020, 1
□	mfx_mft_encrypt_64.dll	Drive-C:\Windows\System32\DriverStore\FileR...	Application exte...	10/23/2019, 21:08:38.00000...	10/23/2019,
□	mfx_mft_encrypt_64.dll	Drive-C:\Windows\System32\DriverStore\FileR...	Application exte...	7/3/2019, 3:26:26.0000000	7/3/2019, 3:
□	mfx_mft_encrypt_64.dll	Drive-C:\Windows\System32\DriverStore\FileR...	Application exte...	3/18/2020, 17:48:12.0000000	3/18/2020, 1

Items Searched: 996999 Items Found: 260 Status: Search Complete

Fig 6: Search for files with “encrypt”.



Search String: <Preset: Encrypted attribute set> - Click on Config for details
Presets: Encrypted attribute set
Start Folder: Drive-C:
Sorting: Type
Config: Include & Sub - Folder names, Encrypted
Filter: (None)

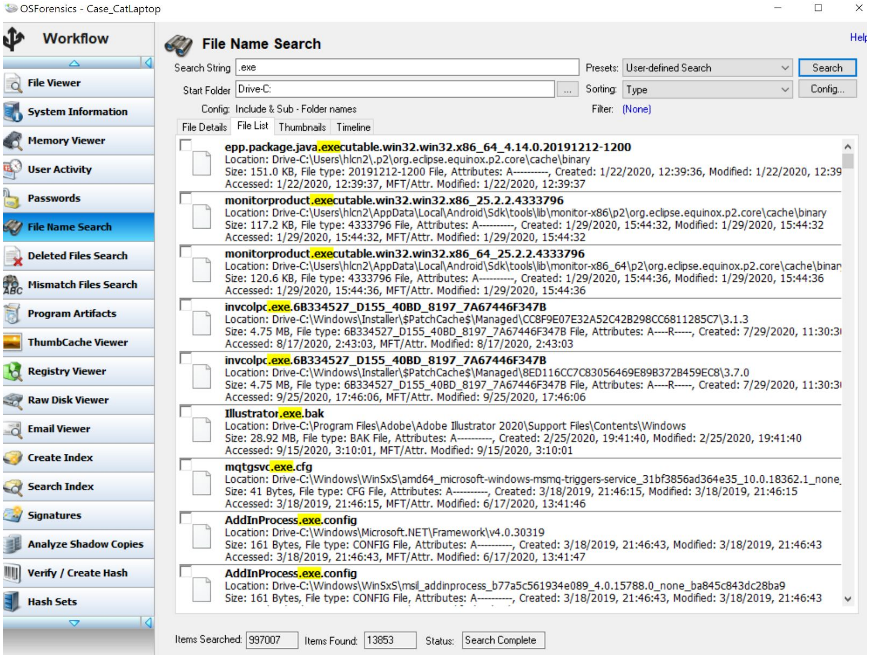
□	File Name	Location	Type	Date modified

Items Searched: 997036 Items Found: 0 Status: Search Complete

Fig 7: Search for the encrypted attributed set files.

- **Number of executable files**

  i. The number of executable files on my drive is 13853 out of the 997007 searched. I used ".exe" to search for them. Not sure if this is the correct way to get these files, but this is what I did.



Search String: .exe
Presets: User-defined Search
Start Folder: Drive-C:
Sorting: Type
Config: Include & Sub - Folder names
Filter: (None)

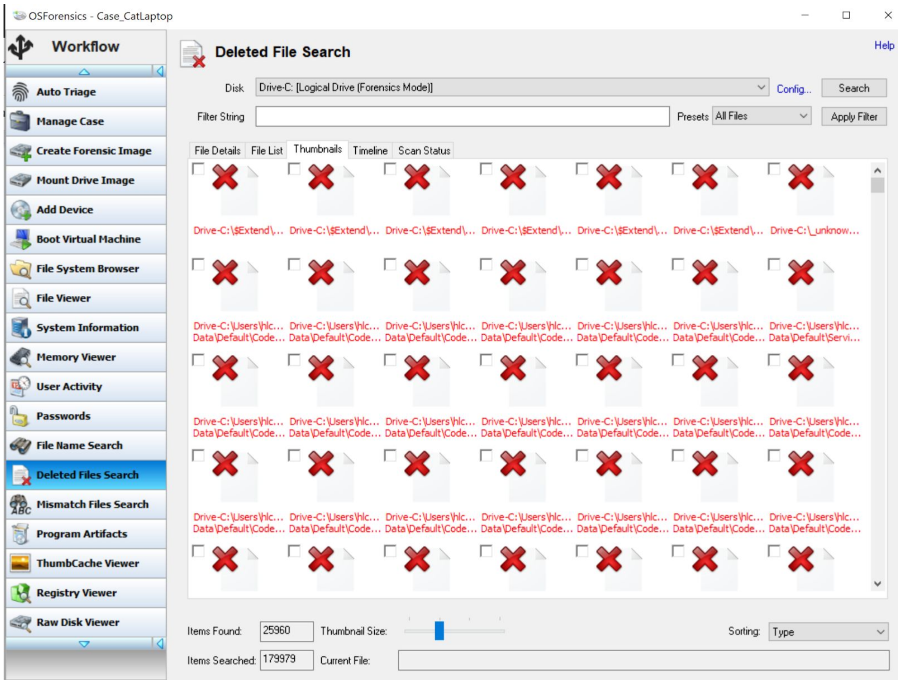
```
epp.package.java.executable.win32.win32.x86_64_4.14.0.20191212-1200
Location: Drive-C:\Users\hlcn2\.p2\org.eclipse.equinox.p2.core\cache\binary
Size: 151.0 KB, File type: 20191212-1200 File, Attributes: A----------, Created: 1/22/2020, 12:39:36, Modified: 1/22/2020, 12:39
Accessed: 1/22/2020, 12:39:37, MFT/Attr. Modified: 1/22/2020, 12:39:37
monitorproduct.executable.win32.win32.x86_25.2.2.4333796
Location: Drive-C:\Users\hlcn2\AppData\Local\Android\Sdk\tools\lib\monitor-x86\p2\org.eclipse.equinox.p2.core\cache\binary
Size: 117.2 KB, File type: 4333796 File, Attributes: A----------, Created: 1/29/2020, 15:44:32, Modified: 1/29/2020, 15:44:32
Accessed: 1/29/2020, 15:44:32, MFT/Attr. Modified: 1/29/2020, 15:44:32
monitorproduct.executable.win32.win32.x86_64_25.2.2.4333796
Location: Drive-C:\Users\hlcn2\AppData\Local\Android\Sdk\tools\lib\monitor-x86_64\p2\org.eclipse.equinox.p2.core\cache\binar
Size: 120.6 KB, File type: 4333796 File, Attributes: A----------, Created: 1/29/2020, 15:44:36, Modified: 1/29/2020, 15:44:36
Accessed: 1/29/2020, 15:44:36, MFT/Attr. Modified: 1/29/2020, 15:44:36
invcolpc.exe.6B334527_D155_40BD_8197_7A67446F347B
Location: Drive-C:\Windows\Installer\$PatchCache$\Managed\CC8F9E07E32A52C42B298CC6811285C7\3.1.3
Size: 4.75 MB, File type: 6B334527_D155_40BD_8197_7A67446F347B File, Attributes: A----R-----, Created: 7/29/2020, 11:30:3
Accessed: 8/17/2020, 2:43:03, MFT/Attr. Modified: 8/17/2020, 2:43:03
invcolpc.exe.6B334527_D155_40BD_8197_7A67446F347B
Location: Drive-C:\Windows\Installer\$PatchCache$\Managed\8ED116CC7C83056469E89B372B459EC8\3.7.0
Size: 4.75 MB, File type: 6B334527_D155_40BD_8197_7A67446F347B File, Attributes: A----R-----, Created: 7/29/2020, 11:30:3
Accessed: 9/25/2020, 17:46:06, MFT/Attr. Modified: 9/25/2020, 17:46:06
Illustrator.exe.bak
Location: Drive-C:\Program Files\Adobe\Adobe Illustrator 2020\Support Files\Contents\Windows
Size: 28.92 MB, File type: BAK File, Attributes: A----------, Created: 2/25/2020, 19:41:40, Modified: 2/25/2020, 19:41:40
Accessed: 9/15/2020, 3:10:01, MFT/Attr. Modified: 9/15/2020, 3:10:01
mqtgsvc.exe.cfg
Location: Drive-C:\Windows\WinSxS\amd64_microsoft-windows-msmq-triggers-service_31bf3856ad364e35_10.0.18362.1_none_
Size: 41 Bytes, File type: CFG File, Attributes: A----------, Created: 3/18/2019, 21:46:15, Modified: 3/18/2019, 21:46:15
Accessed: 3/18/2019, 21:46:15, MFT/Attr. Modified: 6/17/2020, 13:41:46
AddInProcess.exe.config
Location: Drive-C:\Windows\Microsoft.NET\Framework\v4.0.30319
Size: 161 Bytes, File type: CONFIG File, Attributes: A----------, Created: 3/18/2019, 21:46:43, Modified: 3/18/2019, 21:46:43
Accessed: 3/18/2019, 21:46:43, MFT/Attr. Modified: 6/17/2020, 13:41:47
AddInProcess.exe.config
Location: Drive-C:\Windows\WinSxS\msil_addinprocess_b77a5c561934e089_4.0.15788.0_none_ba845c843dc28ba9
Size: 161 Bytes, File type: CONFIG File, Attributes: A----------, Created: 3/18/2019, 21:46:43, Modified: 3/18/2019, 21:46:43
```

Items Searched: 997007 Items Found: 13853 Status: Search Complete

Fig 8: Search for files including ".exe".

- **Number of deleted files**

  i. The number of deleted files I had amazed me. I have exactly 25960 files deleted out of the 179979 files searched. To get here I used the Deleted File Search feature and searched my whole drive.

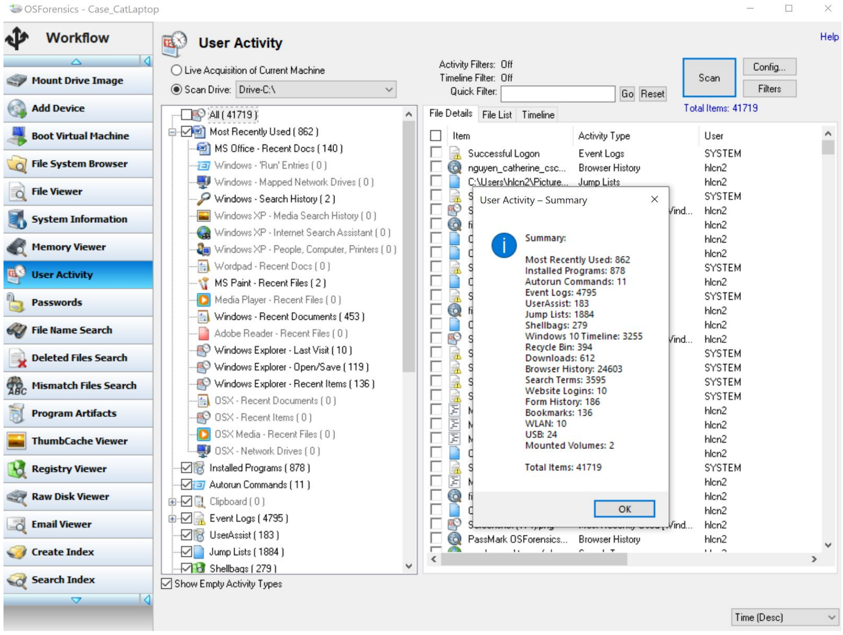


Disk: Drive-C: [Logical Drive (Forensics Mode)]
Filter String:
Presets: All Files
Items Found: 25960
Items Searched: 179979
Sorting: Type
Current File:

Fig 9: Files found in the Deleted File Search.

- **Recently visited web sites**

i. This is my user activity summary. By the looks of it, I have been up to a lot since I had this laptop.



User Activity

○ Live Acquisition of Current Machine
● Scan Drive: Drive-C:\

Activity Filters: Off
Timeline Filter: Off
Quick Filter:

Total Items: 41719

```
□ All ( 41719 )
☑ Most Recently Used ( 862 )
    MS Office - Recent Docs ( 140 )
    Windows - 'Run' Entries ( 0 )
    Windows - Mapped Network Drives ( 0 )
    Windows - Search History ( 2 )
    Windows XP - Media Search History ( 0 )
    Windows XP - Internet Search Assistant ( 0 )
    Windows XP - People, Computer, Printers ( 0 )
    Wordpad - Recent Docs ( 0 )
    MS Paint - Recent Files ( 2 )
    Media Player - Recent Files ( 0 )
    Windows - Recent Documents ( 453 )
    Adobe Reader - Recent Files ( 0 )
    Windows Explorer - Last Visit ( 10 )
    Windows Explorer - Open/Save ( 119 )
    Windows Explorer - Recent Items ( 136 )
    OSX - Recent Documents ( 0 )
    OSX - Recent Items ( 0 )
    OSX Media - Recent Files ( 0 )
    OSX - Network Drives ( 0 )
☑ Installed Programs ( 878 )
☑ Autorun Commands ( 11 )
☑ Clipboard ( 0 )
☑ Event Logs ( 4795 )
☑ UserAssist ( 183 )
☑ Jump Lists ( 1884 )
☑ Shellbags ( 279 )
☑ Show Empty Activity Types
```

Item	Activity Type	User
Successful Logon	Event Logs	SYSTEM
nguyen_catherine_csc...	Browser History	hlcn2
C:\Users\hlcn2\Picture...	Jump Lists	hlcn2
PassMark OSForensics...	Browser History	hlcn2

User Activity – Summary

Summary:

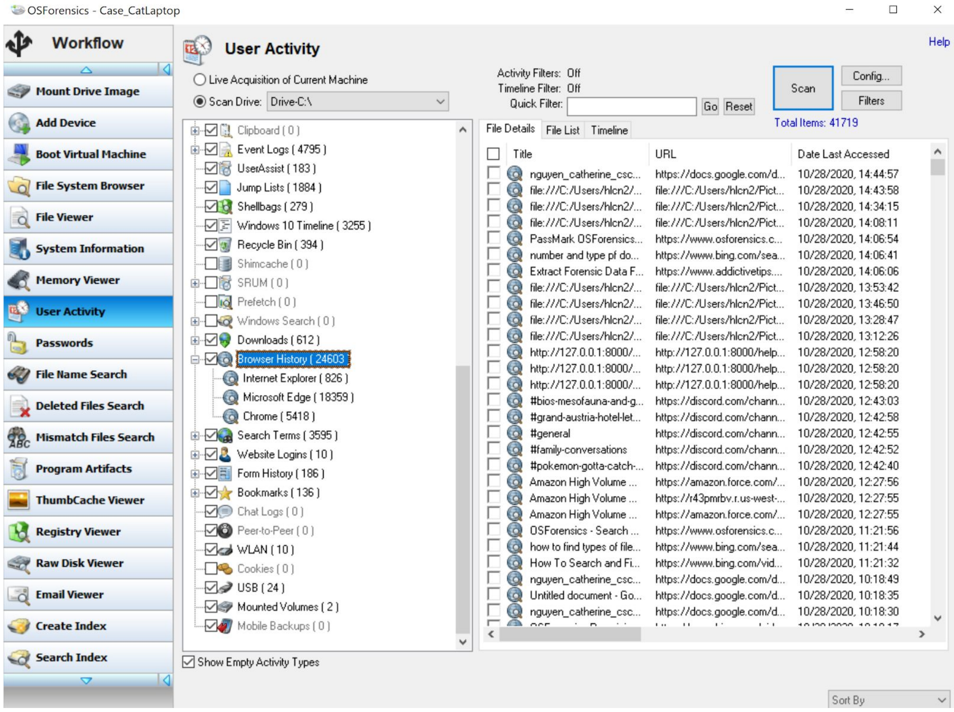
Most Recently Used: 862
Installed Programs: 878
Autorun Commands: 11
Event Logs: 4795
UserAssist: 183
Jump Lists: 1884
Shellbags: 279
Windows 10 Timeline: 3255
Recycle Bin: 394
Downloads: 612
Browser History: 24603
Search Terms: 3595
Website Logins: 10
Form History: 186
Bookmarks: 136
WLAN: 10
USB: 24
Mounted Volumes: 2

Total Items: 41719

Time (Desc)

Fig 10: User Activity Summary.

ii. Here is an even closer look at my browser history. A total of 24603 browsers and the browser I use the most is Microsoft edge with 18,000+ browsers. Second is Chrome with 5,000 plus and last is Internet Explorer with 800+ browsers. This makes sense because I rarely use internet explorer and I've moved on from Google Chrome and have been using Microsoft Edge ever since.



User Activity

○ Live Acquisition of Current Machine
● Scan Drive: Drive-C:\

Activity Filters: Off
Timeline Filter: Off
Quick Filter:

Total Items: 41719

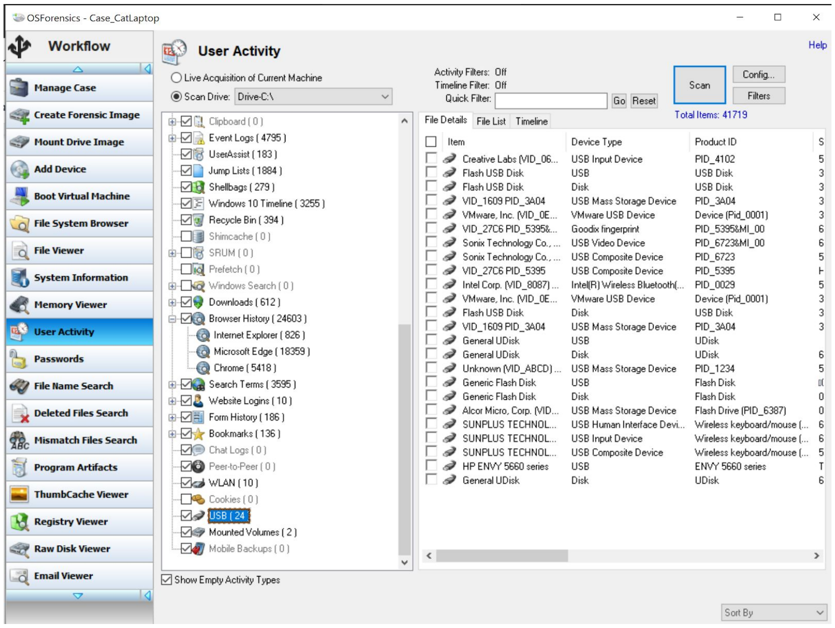
```
☑ Clipboard ( 0 )
☑ Event Logs ( 4795 )
☑ UserAssist ( 183 )
☑ Jump Lists ( 1884 )
☑ Shellbags ( 279 )
☑ Windows 10 Timeline ( 3255 )
☑ Recycle Bin ( 394 )
□ Shimcache ( 0 )
□ SRUM ( 0 )
□ Prefetch ( 0 )
□ Windows Search ( 0 )
☑ Downloads ( 612 )
☑ Browser History ( 24603 )
    Internet Explorer ( 826 )
    Microsoft Edge ( 18359 )
    Chrome ( 5418 )
☑ Search Terms ( 3595 )
☑ Website Logins ( 10 )
☑ Form History ( 186 )
☑ Bookmarks ( 136 )
☑ Chat Logs ( 0 )
☑ Peer-to-Peer ( 0 )
☑ WLAN ( 10 )
□ Cookies ( 0 )
☑ USB ( 24 )
☑ Mounted Volumes ( 2 )
☑ Mobile Backups ( 0 )
☑ Show Empty Activity Types
```

Title	URL	Date Last Accessed
nguyen_catherine_csc...	https://docs.google.com/d...	10/28/2020, 14:44:57
file:///C:/Users/hlcn2/...	file:///C:/Users/hlcn2/Pict...	10/28/2020, 14:43:58
file:///C:/Users/hlcn2/...	file:///C:/Users/hlcn2/Pict...	10/28/2020, 14:34:15
file:///C:/Users/hlcn2/...	file:///C:/Users/hlcn2/Pict...	10/28/2020, 14:08:11
PassMark OSForensics...	https://www.osforensics.c...	10/28/2020, 14:06:54
number and type pf do...	https://www.bing.com/sea...	10/28/2020, 14:06:41
Extract Forensic Data F...	https://www.addictivetips....	10/28/2020, 14:06:06
file:///C:/Users/hlcn2/...	file:///C:/Users/hlcn2/Pict...	10/28/2020, 13:53:42
file:///C:/Users/hlcn2/...	file:///C:/Users/hlcn2/Pict...	10/28/2020, 13:46:50
file:///C:/Users/hlcn2/...	file:///C:/Users/hlcn2/Pict...	10/28/2020, 13:28:47
file:///C:/Users/hlcn2/...	file:///C:/Users/hlcn2/Pict...	10/28/2020, 13:12:26
http://127.0.0.1:8000/...	http://127.0.0.1:8000/help...	10/28/2020, 12:58:20
http://127.0.0.1:8000/...	http://127.0.0.1:8000/help...	10/28/2020, 12:58:20
http://127.0.0.1:8000/...	http://127.0.0.1:8000/help...	10/28/2020, 12:58:20
#bios-mesofauna-and-g...	https://discord.com/chann...	10/28/2020, 12:43:03
#grand-austria-hotel-let...	https://discord.com/chann...	10/28/2020, 12:42:58
#general	https://discord.com/chann...	10/28/2020, 12:42:55
#family-conversations	https://discord.com/chann...	10/28/2020, 12:42:52
#pokemon-gotta-catch-...	https://discord.com/chann...	10/28/2020, 12:42:40
Amazon High Volume ...	https://amazon.force.com/...	10/28/2020, 12:27:56
Amazon High Volume ...	https://r43pmrbv.r.us-west-...	10/28/2020, 12:27:55
Amazon High Volume ...	https://amazon.force.com/...	10/28/2020, 12:27:55
OSForensics - Search ...	https://www.osforensics.c...	10/28/2020, 11:21:56
how to find types of file...	https://www.bing.com/sea...	10/28/2020, 11:21:44
How To Search and Fi...	https://www.bing.com/vid...	10/28/2020, 11:21:32
nguyen_catherine_csc...	https://docs.google.com/d...	10/28/2020, 10:18:49
Untitled document - Go...	https://docs.google.com/d...	10/28/2020, 10:18:35
nguyen_catherine_csc...	https://docs.google.com/d...	10/28/2020, 10:18:30

Sort By

Fig 11: User Activity - Browser History.

- **Types of external devices (eg. USB, printer, etc.) connected to the computer**
  i. Based on OSForensics it seems that I have had a total of 24 external devices that have come in contact with my laptop. To find this, I used the User Activity feature and clicked on "USB" which then showed me all the previous external devices.



○ Live Acquisition of Current Machine
● Scan Drive: Drive-C:\

Activity Filters: Off
Timeline Filter: Off
Quick Filter:

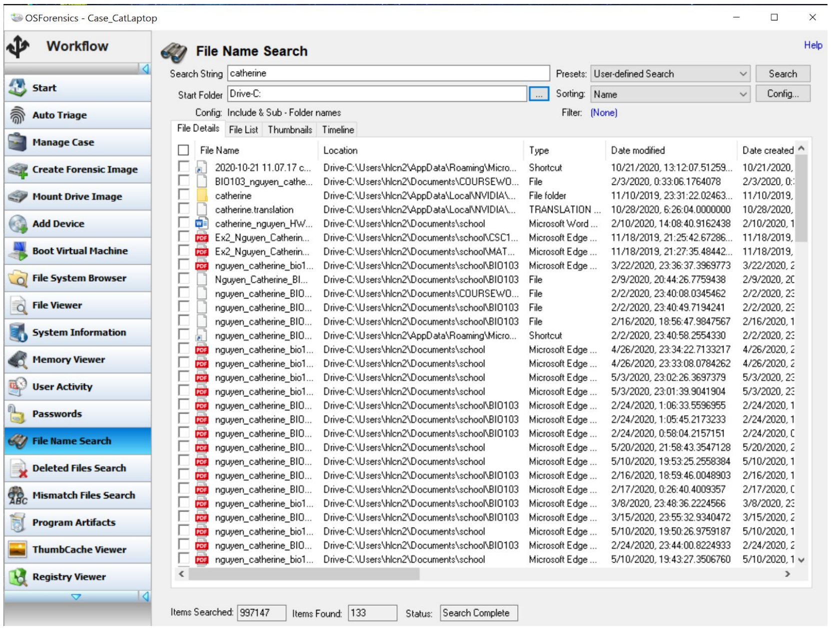
Total Items: 41719

Item	Device Type	Product ID	S
Creative Labs (VID_06...	USB Input Device	PID_4102	5
Flash USB Disk	USB	USB Disk	3
Flash USB Disk	Disk	USB Disk	3
VID_1609 PID_3A04	USB Mass Storage Device	PID_3A04	3
VMware, Inc. (VID_0E...	VMware USB Device	Device (Pid_0001)	3
VID_27C6 PID_5395&...	Goodix fingerprint	PID_5395&MI_00	6
Sonix Technology Co., ...	USB Video Device	PID_6723&MI_00	6
Sonix Technology Co., ...	USB Composite Device	PID_6723	5
VID_27C6 PID_5395	USB Composite Device	PID_5395	H
Intel Corp. (VID_8087) ...	Intel(R) Wireless Bluetooth(...	PID_0029	5
VMware, Inc. (VID_0E...	VMware USB Device	Device (Pid_0001)	3
Flash USB Disk	Disk	USB Disk	3
VID_1609 PID_3A04	USB Mass Storage Device	PID_3A04	3
General UDisk	USB	UDisk	
General UDisk	Disk	UDisk	6
Unknown (VID_ABCD) ...	USB Mass Storage Device	PID_1234	5
Generic Flash Disk	USB	Flash Disk	[illegible]
Generic Flash Disk	Disk	Flash Disk	0
Alcor Micro, Corp. (VID...	USB Mass Storage Device	Flash Drive (PID_6387)	0
SUNPLUS TECHNOL...	USB Human Interface Devi...	Wireless keyboard/mouse (...	6
SUNPLUS TECHNOL...	USB Input Device	Wireless keyboard/mouse (...	6
SUNPLUS TECHNOL...	USB Composite Device	Wireless keyboard/mouse (...	5
HP ENVY 5660 series	USB	ENVY 5660 series	T
General UDisk	Disk	UDisk	6

☑ Show Empty Activity Types

Fig 12: User Activity - USB

2. **Do a search to determine the number of times your name appears, and typical places your name appeared.**
   - This was the best I could do when it came to searching for my name. Out of the 990,000+ files I was only able to find my name in 133 files. This makes sense because a majority of my files are usually on google docs. Unfortunately, this is my only file names. The typical places my name appeared were in school-related files.



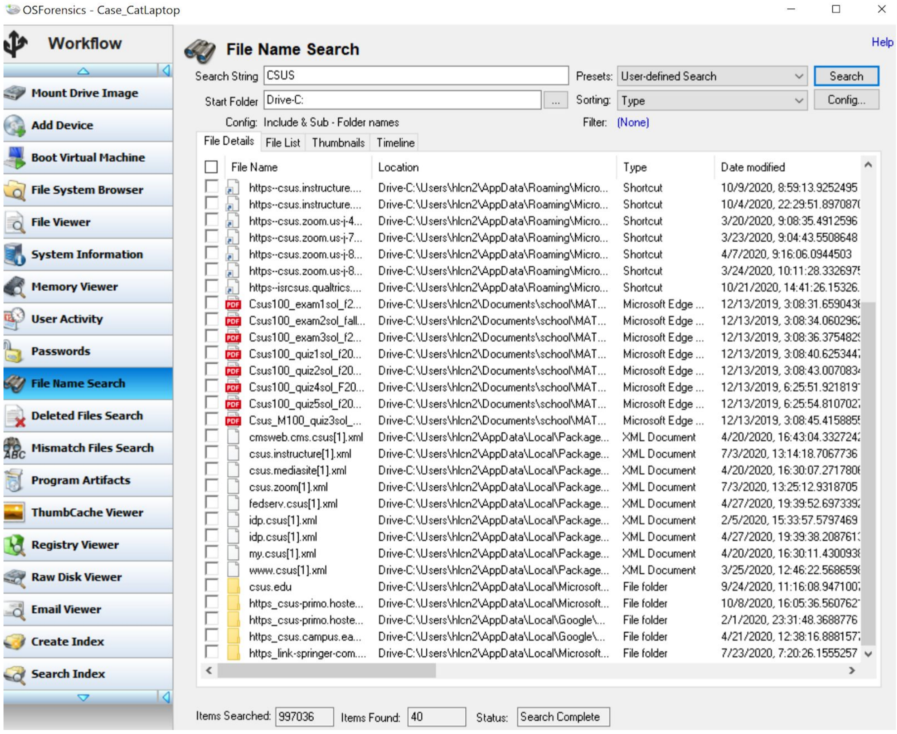
Search String: catherine
Start Folder: Drive-C:
Config: Include & Sub - Folder names
Presets: User-defined Search
Sorting: Name
Filter: (None)

File Name	Location	Type	Date modified	Date created
2020-10-21 11.07.17 c...	Drive-C:\Users\hlcn2\AppData\Roaming\Micro...	Shortcut	10/21/2020, 13:12:07.51259...	10/21/2020,
BIO103_nguyen_cathe...	Drive-C:\Users\hlcn2\Documents\COURSEWO...	File	2/3/2020, 0:33:06.1764078	2/3/2020, 0:
catherine	Drive-C:\Users\hlcn2\AppData\Local\NVIDIA\...	File folder	11/10/2019, 23:31:22.02463...	11/10/2019,
catherine.translation	Drive-C:\Users\hlcn2\AppData\Local\NVIDIA\...	TRANSLATION ...	10/28/2020, 6:26:04.0000000	10/28/2020,
catherine_nguyen_HW...	Drive-C:\Users\hlcn2\Documents\school	Microsoft Word ...	2/10/2020, 14:08:40.9162438	2/10/2020, 1
Ex2_Nguyen_Catherin...	Drive-C:\Users\hlcn2\Documents\school\CSC1...	Microsoft Edge ...	11/18/2019, 21:25:42.67286...	11/18/2019,
Ex2_Nguyen_Catherin...	Drive-C:\Users\hlcn2\Documents\school\MAT...	Microsoft Edge ...	11/18/2019, 21:27:35.48442...	11/18/2019,
nguyen_catherine_bio1...	Drive-C:\Users\hlcn2\Documents\school\BIO103	Microsoft Edge ...	3/22/2020, 23:36:37.3969773	3/22/2020, 2
Nguyen_Catherine_BI...	Drive-C:\Users\hlcn2\Documents\school\BIO103	File	2/9/2020, 20:44:26.7759438	2/9/2020, 20
nguyen_catherine_BIO...	Drive-C:\Users\hlcn2\Documents\COURSEWO...	File	2/2/2020, 23:40:08.0345462	2/2/2020, 23
nguyen_catherine_BIO...	Drive-C:\Users\hlcn2\Documents\school\BIO103	File	2/2/2020, 23:40:49.7194241	2/2/2020, 23
nguyen_catherine_BIO...	Drive-C:\Users\hlcn2\Documents\school\BIO103	File	2/16/2020, 18:56:47.9847567	2/16/2020, 1
nguyen_catherine_BIO...	Drive-C:\Users\hlcn2\AppData\Roaming\Micro...	Shortcut	2/2/2020, 23:40:58.2554330	2/2/2020, 23
nguyen_catherine_bio1...	Drive-C:\Users\hlcn2\Documents\school	Microsoft Edge ...	4/26/2020, 23:34:22.7133217	4/26/2020, 2
nguyen_catherine_bio1...	Drive-C:\Users\hlcn2\Documents\school	Microsoft Edge ...	4/26/2020, 23:33:08.0784262	4/26/2020, 2
nguyen_catherine_bio1...	Drive-C:\Users\hlcn2\Documents\school	Microsoft Edge ...	5/3/2020, 23:02:26.3697379	5/3/2020, 23
nguyen_catherine_bio1...	Drive-C:\Users\hlcn2\Documents\school	Microsoft Edge ...	5/3/2020, 23:01:39.9041904	5/3/2020, 23
nguyen_catherine_BIO...	Drive-C:\Users\hlcn2\Documents\school\BIO103	Microsoft Edge ...	2/24/2020, 1:06:33.5596955	2/24/2020, 1
nguyen_catherine_BIO...	Drive-C:\Users\hlcn2\Documents\school\BIO103	Microsoft Edge ...	2/24/2020, 1:05:45.2173233	2/24/2020, 1
nguyen_catherine_BIO...	Drive-C:\Users\hlcn2\Documents\school\BIO103	Microsoft Edge ...	2/24/2020, 0:58:04.2157151	2/24/2020, 0
nguyen_catherine_BIO...	Drive-C:\Users\hlcn2\Documents\school	Microsoft Edge ...	5/20/2020, 21:58:43.3547128	5/20/2020, 2
nguyen_catherine_BIO...	Drive-C:\Users\hlcn2\Documents\school	Microsoft Edge ...	5/10/2020, 19:53:25.2558384	5/10/2020, 1
nguyen_catherine_BIO...	Drive-C:\Users\hlcn2\Documents\school\BIO103	Microsoft Edge ...	2/16/2020, 18:59:46.0048903	2/16/2020, 1
nguyen_catherine_BIO...	Drive-C:\Users\hlcn2\Documents\school\BIO103	Microsoft Edge ...	2/17/2020, 0:26:40.4009357	2/17/2020, 0
nguyen_catherine_bio1...	Drive-C:\Users\hlcn2\Documents\school\BIO103	Microsoft Edge ...	3/8/2020, 23:48:36.2224566	3/8/2020, 23
nguyen_catherine_BIO...	Drive-C:\Users\hlcn2\Documents\school\BIO103	Microsoft Edge ...	3/15/2020, 23:55:32.9340472	3/15/2020, 2
nguyen_catherine_bio1...	Drive-C:\Users\hlcn2\Documents\school	Microsoft Edge ...	5/10/2020, 19:50:26.9759187	5/10/2020, 1
nguyen_catherine_BIO...	Drive-C:\Users\hlcn2\Documents\school\BIO103	Microsoft Edge ...	2/24/2020, 23:44:00.8224933	2/24/2020, 2
nguyen_catherine_bio1...	Drive-C:\Users\hlcn2\Documents\school	Microsoft Edge ...	5/10/2020, 19:43:27.3506760	5/10/2020, 1

Items Searched: 997147 Items Found: 133 Status: Search Complete

Fig 13: Search for files including my name "Catherine".

3. **Do a search to determine the number of times CSUS or Sac State appeared and typical places where it appeared.**
    - Surprisingly there are not many csus or sac state files. This might be due to my lack of knowledge in conducting a concise search. I assume I need to "Search Index", but the time it took to create an index was too much for someone impatient. So the best I could do was search for file names. This resulted in 40 files with "csus" and 0 files with "sac state" included.



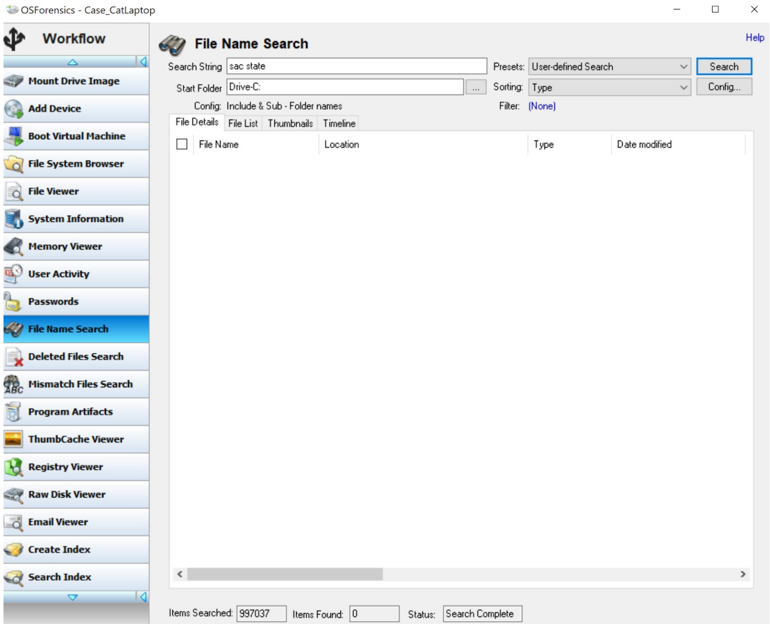
File Name Search

Search String: CSUS
Presets: User-defined Search
Start Folder: Drive-C:
Sorting: Type
Config: Include & Sub - Folder names
Filter: (None)

File Name	Location	Type	Date modified
https--csus.instructure....	Drive-C:\Users\hlcn2\AppData\Roaming\Micro...	Shortcut	10/9/2020, 8:59:13.9252495
https--csus.instructure....	Drive-C:\Users\hlcn2\AppData\Roaming\Micro...	Shortcut	10/4/2020, 22:29:51.897087(
https--csus.zoom.us-j-4...	Drive-C:\Users\hlcn2\AppData\Roaming\Micro...	Shortcut	3/20/2020, 9:08:35.4912596
https--csus.zoom.us-j-7...	Drive-C:\Users\hlcn2\AppData\Roaming\Micro...	Shortcut	3/23/2020, 9:04:43.5508648
https--csus.zoom.us-j-8...	Drive-C:\Users\hlcn2\AppData\Roaming\Micro...	Shortcut	4/7/2020, 9:16:06.0944503
https--csus.zoom.us-j-8...	Drive-C:\Users\hlcn2\AppData\Roaming\Micro...	Shortcut	3/24/2020, 10:11:28.332697!
https--isrcsus.qualtrics....	Drive-C:\Users\hlcn2\AppData\Roaming\Micro...	Shortcut	10/21/2020, 14:41:26.15326.
Csus100_exam1sol_f2...	Drive-C:\Users\hlcn2\Documents\school\MAT...	Microsoft Edge ...	12/13/2019, 3:08:31.659043(
Csus100_exam2sol_fall...	Drive-C:\Users\hlcn2\Documents\school\MAT...	Microsoft Edge ...	12/13/2019, 3:08:34.060296:
Csus100_exam3sol_f2...	Drive-C:\Users\hlcn2\Documents\school\MAT...	Microsoft Edge ...	12/13/2019, 3:08:36.375482!
Csus100_quiz1sol_f20...	Drive-C:\Users\hlcn2\Documents\school\MAT...	Microsoft Edge ...	12/13/2019, 3:08:40.625344:
Csus100_quiz2sol_f20...	Drive-C:\Users\hlcn2\Documents\school\MAT...	Microsoft Edge ...	12/13/2019, 3:08:43.007083
Csus100_quiz4sol_F20...	Drive-C:\Users\hlcn2\Documents\school\MAT...	Microsoft Edge ...	12/13/2019, 6:25:51.921819
Csus100_quiz5sol_f20...	Drive-C:\Users\hlcn2\Documents\school\MAT...	Microsoft Edge ...	12/13/2019, 6:25:54.810702:
Csus_M100_quiz3sol_...	Drive-C:\Users\hlcn2\Documents\school\MAT...	Microsoft Edge ...	12/13/2019, 3:08:45.415885!
cmsweb.cms.csus[1].xml	Drive-C:\Users\hlcn2\AppData\Local\Package...	XML Document	4/20/2020, 16:43:04.332724:
csus.instructure[1].xml	Drive-C:\Users\hlcn2\AppData\Local\Package...	XML Document	7/3/2020, 13:14:18.7067736
csus.mediasite[1].xml	Drive-C:\Users\hlcn2\AppData\Local\Package...	XML Document	4/20/2020, 16:30:07.271780(
csus.zoom[1].xml	Drive-C:\Users\hlcn2\AppData\Local\Package...	XML Document	7/3/2020, 13:25:12.9318705
fedserv.csus[1].xml	Drive-C:\Users\hlcn2\AppData\Local\Package...	XML Document	4/27/2020, 19:39:52.697339:
idp.csus[1].xml	Drive-C:\Users\hlcn2\AppData\Local\Package...	XML Document	2/5/2020, 15:33:57.5797469
idp.csus[1].xml	Drive-C:\Users\hlcn2\AppData\Local\Package...	XML Document	4/27/2020, 19:39:38.208761:
my.csus[1].xml	Drive-C:\Users\hlcn2\AppData\Local\Package...	XML Document	4/20/2020, 16:30:11.430093!
www.csus[1].xml	Drive-C:\Users\hlcn2\AppData\Local\Package...	XML Document	3/25/2020, 12:46:22.568659!
csus.edu	Drive-C:\Users\hlcn2\AppData\Local\Microsoft...	File folder	9/24/2020, 11:16:08.947100:
https_csus-primo.hoste...	Drive-C:\Users\hlcn2\AppData\Local\Microsoft...	File folder	10/8/2020, 16:05:36.560762
https_csus-primo.hoste...	Drive-C:\Users\hlcn2\AppData\Local\Google\...	File folder	2/1/2020, 23:31:48.3688776
https_csus.campus.ea...	Drive-C:\Users\hlcn2\AppData\Local\Google\...	File folder	4/21/2020, 12:38:16.888157:
https_link-springer-com....	Drive-C:\Users\hlcn2\AppData\Local\Microsoft...	File folder	7/23/2020, 7:20:26.1555257

Items Searched: 997036 Items Found: 40 Status: Search Complete

Fig 14: Search for files with "CSUS"



File Name Search

Search String: sac state
Presets: User-defined Search
Start Folder: Drive-C:
Sorting: Type
Config: Include & Sub - Folder names
Filter: (None)

File Name	Location	Type	Date modified

Items Searched: 997037 Items Found: 0 Status: Search Complete

Fig 15: Search for files with "Sac State"

4. **Any surprising information you least expected to find.**
    - **I am surprised to find out that I don't have any files that are encrypted and that my browser activity is high. Also, I am surprised that my laptop is familiar with only 10 wifis.**

Conclusion: This lab was really fun. At first, I was worried. Since this tool is new to me and I was not sure I would be able to figure out how to use it for this lab. Hopefully what I have turned in is acceptable. I have learned a lot from this.