Hands-on Projects 4-1

Read the four detective reports and the combined affidavit and warrant for the M57 Patents case. Write a one- to two-page paper describing the evidence the police found and explaining whether they had enough information for the search warrant. Did the information justify taking all the computers and USB drives? Why or why not?

Answer: -

Possession of a cat for the purpose of exploitation is being investigated. The Need for Action I received a call from Aaron Greene, 123 Cloudy Hill Drive, Monterey, CA 93940. Aaron Greene had bought an old computer from a seller on Craig's List, an online classifieds site. When Aaron Greene turned on the computer, she discovered that the previous owner had failed to delete the hard disk drive. She claimed to have discovered kitty exploitation films and images on the computer. Acting Officers were dispatched to Aaron Greene's residence to seize the computer, which Greene had freely released. Greene also mentioned the seller's name: Terry Johnson is a well-known figure in the Further than an email address, there was no other information accessible. Outcome The computer was retrieved, logged as evidence (MT--2009-12--015--EV001), and delivered to the forensics lab.

Kitty exploitation has been discovered on a computer, and an investigation is underway. a reason for Action On the recovered computer (MT--2009--12--015--EV001), forensic tech discovered multiple known kitty exploitation films and photographs, as well as a suspected owner. We believe the original owner of the computer was a local company called M57 Patents, based on the data obtained from the device. Jo was the name of the computer's user (no last name available). Taking Action To find out if Jo was the owner of the files and if there is any other incriminating evidence, more investigation is required. Pat McGoo, the company's owner, has been identified through corporate documents. Rather than obtaining a warrant, we're considering contacting McGoo.

Pat McGoo was contacted, and a voluntary search was approved. The Need for Action After discovering evidence of kitten exploitation on the computer mentioned in previous reports, CoD decided that meeting with McGoo and conducting a voluntary search for as much information as possible would be the best course of action. The decision was made to pursue a warrant only if it was necessary. Detectives have taken action. Gannon had a meeting with McGoo at M57 Patents on Friday. We were allowed to have a private conversation with him. McGoo stated that the computer was most likely stolen after being told it was non--functional. McGoo verified Jo's status as an employee. McGoo was agreeable, but he wanted to consult with an attorney before approving the search.

Jo's USB flash drive has been given a warrant. a reason for Action A USB flash drive, possibly owned by Jo, was used to connect to the computer and possibly used to transfer kitten exploitation material, according to forensic technologists. Taking Action We requested and were granted a warrant to seize the USB thumb drive based on the premise that it belongs to Jo. The warrant was based on information discovered on the computer MT--2009--12--015--EV001. The warrant has been assigned the number MT--2009--12--015--W001. Outcome If we are given permission to search the computers at M57 Patents, we will carry out the warrant and confiscate the thumb drive (if it is in Jo's possession) at that time.

Assuming the thumb drive belongs to Jo, we have requested and received a warrant to seize the thumb drive. The warrant was based upon data found on the computer

MTO2009O12O015OEV001. The warrant has been logged as MTO2009O12O015OW001.If we are granted permission to search computers at M57 Patents, we will execute the warrant and seize the thumb drive (if it is in Jo`s possession) at that time. If not, we will decide about when to execute the warrant.

According to my analysis, the initial investigation was conducted by speaking with MCGoo. I believe it would have been preferable if police had been brought to Jo, since this would have cut down on time and given police a clear image of whether the laptop had been stolen or not. Because there's a potential that someone other than the owner could put the kitty movies and photos on the USB. I believe the police have gathered sufficient evidence to continue their investigation and issue the search warrant on time, and yes, the evidence justifies the seizure of the computer and USB devices.

Hands-on Projects 4-2

You're investigating an internal policy violation when you find an e-mail about a serious assault for which a police report needs to be filed. What should you do? Write a two-page paper specifying who in your company you need to talk to first and what evidence must be turned over to the police.

Answer:-

Case Description:

When the investigator is searching his cabin for proof of an internal policy violation, he may come across evidence of additional crimes that are punishable. The investigator must then call the corporate counsel and provide all of the specifics regarding the evidence obtained from the convict's computer. Determine if the occurrence meets the criteria for a criminal offense. Then, alert management about the employee's criminal activities. We shall attempt to obtain information about the location of the computer from which the message was sent in the event of a policy infringement by issuing attack email. After the investigation is completed, the investigator should provide a report And if we want law enforcement to assist us in locating the person who sent the assault mail, he or she must be arrested. That necessitates strong evidence.

Permission of more investigation and gathering of evidence

Because he is the company's highest official, the Attorney General must be involved in these types of issues. He must be aware of what is going on in the organization. Request that the attorney give you the authority to look through employee files and network records for more evidence. To find the evidence, we'll start by looking for the IP address of the computer that sent the email, and then we'll try to track down the computer's location. However, because IP alone cannot guarantee that you are in the correct location, we must seek out more convincing evidence. We can acquire the name of the individual whose account was created and their email address from the email. Then we'll look for a list of employees who have ever contacted that email address. If the answer is yes, we have a very strong correlation to the person's location. It's also possible that the person didn't send the email from his own ID, but rather from a hacker's account. For this type of circumstance, we'll look for a specific person who can tell us whether someone has hacked their account or not, and if so, we'll try to track down the hacker. We'll bring the email copy to the police station to persuade them of the crime. Provide all relevant information about the email, such as when it was sent and from which account.

Report on the found evidences

The investigator prepares a final report after the investigation, which is a business investigation. The report is then presented to the court, and if the investigator obtains information or proof regarding the offense that is offensive in character, like in this case, the report is presented to the police officer. If the crime involves the internet, we will disclose information about the application utilized by the suspect. This includes crimes such as sending threatening emails or letters, tracking someone without authorisation, and hacking into other computers. If the offence involves child pornography, we will provide over the video and photo files to the police officer. Which of the following is linked to the sending of an assault email in this case? Which of these is a violation of corporate policy? We'll send the email address, which is an assault email. Give all of the account's details, as well as any information discovered throughout the corporate inquiry. If the evidence is good enough, the police will obtain a search warrant for the email address. We receive facts about all the locations from which the account was opened by delivering warrant to the ISP (Internet service provider). The culprit can simply be apprehended with this information.

Corporate investigator and agent of law enforcement

The corporate investigator investigates to see if the employee has done something that is against the company's rules. If he obtains evidence of other crimes that are offensive in nature throughout the course of the investigation. He can submit the report to the police after the investigation is completed. If the police believe the evidence is sufficient for the case, they might request the collection of additional evidence without a warrant. The corporate investigator can then become a law enforcement agent. However, the corporate investigator should avoid acting as a law enforcement agent because it breaches the company's privacy policy.

Since IP addresses do not provide an exact location, we need to find other strong evidence. We may derive the name of the person who created the account from the mail and the email identity of that person. Then we can find the list of employees who have entered email id contact information. If so, we have a very good connection to finding out personally. Individuals may not send mail from their ID, but a hacker can send mail. For this type of situation, we will work with a specific person who can send us information. time, or if we do, we will attempt to locate the hacker. We will take a copy of the email to convince the police of the incident. Provide all requested email information about where their account came from.

The final report is prepared by the prosecutor at the end of the business investigation. The report will then be presented to the court and the prosecutor will provide the report to the police if information or evidence is obtained about a violent crime, such as an incident,. If the criminal is connected to the Internet, we will include information about the criminal's use of the program. This request relates to crimes, such as sending abusive emails, postal services, tracking people without permission, and hacking another device.

Attack email will be sent to us. Provide full account details along with company requirements. If police find convincing enough evidence, they will receive a search warrant by email. By providing the ISP guarantee, we get information about the origin of the account. Suspects will be easily caught using this knowledge. Company Investigator and Law Enforcement Officer.

To find out where the employee is, the corporate investigator asks for something that contradicts corporate policy. During the process of the inquiry, if he gets proof of other aggressive offences. He will send the report to the police after the investigation is finished. If the police deem the facts to be too powerful for their case, they will order more without an order. The corporate researcher will then become the law enforcement officer. However, the company investigator should stop being the law enforcement agent, which breaches company policy privacy.

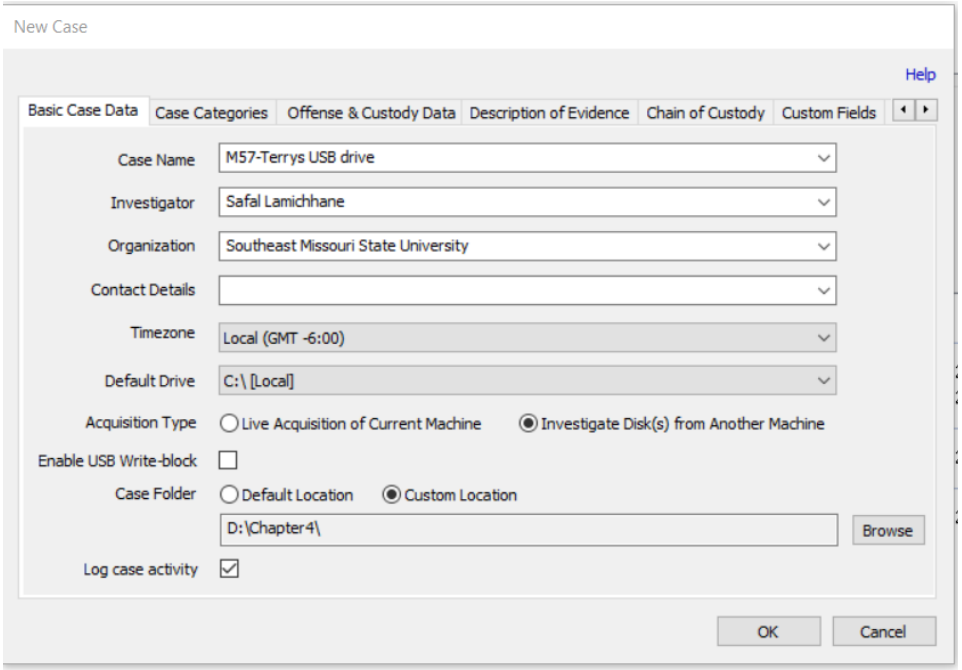
Hands-On Project 4-3

In this project, you examine a USB drive belonging to Terry, the IT person for M57 Patents. Your job is to ascertain whether Terry is involved in anything illicit or against company policy.

1. Start OSForensics. If necessary, click OK or Yes in the UAC message box. In the OSForensics message box, click Continue Using Trial Version.

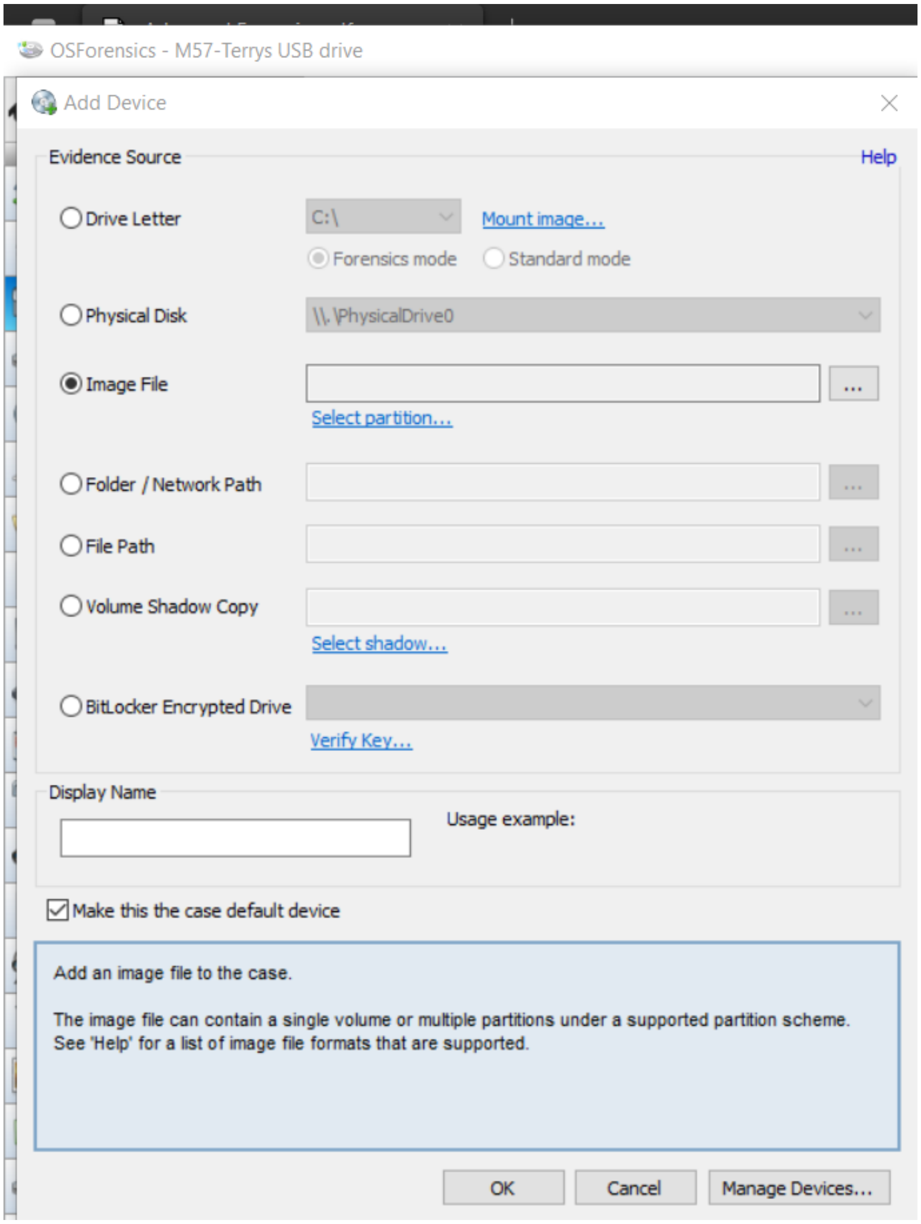
2. Click Start in the left pane, if necessary. In the right pane, click Create Case.

3. In the New Case dialog box, enter your name in the Investigator text box. In the Case Name text box, type M57-Terrys USB drive. Fill in the contact details and the organization, and then click Investigate Disk(s) from Another Machine.



Case Name: M57-Terrys USB drive
Investigator: Safal Lamichhane
Organization: Southeast Missouri State University
Contact Details:
Timezone: Local (GMT -6:00)
Default Drive: C:\ [Local]
Acquisition Type: ○ Live Acquisition of Current Machine ● Investigate Disk(s) from Another Machine
Enable USB Write-block: □
Case Folder: ○ Default Location ● Custom Location
D:\Chapter4\
Log case activity: ☑

4. Click Custom Location for the case folder. Click the Browse button on the lower right, navigate to and click your work folder, and then click OK twice. You should see the Manage Case window.



○ Drive Letter C:\ (● Forensics mode ○ Standard mode)

○ Physical Disk \\.\PhysicalDrive0

● Image File

○ Folder / Network Path

○ File Path

○ Volume Shadow Copy

○ BitLocker Encrypted Drive

☑ Make this the case default device

Add an image file to the case.

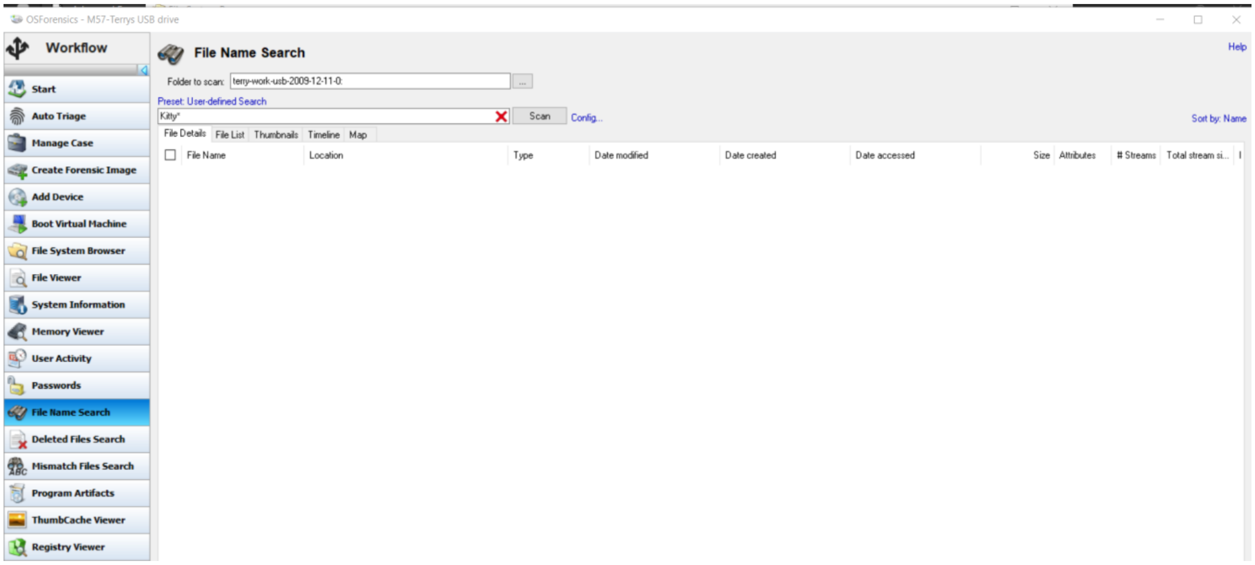
The image file can contain a single volume or multiple partitions under a supported partition scheme. See 'Help' for a list of image file formats that are supported.

5. Click the Add Device button to open the “Select device to add” dialog box, and then click the Image File option button. Click the browse button, navigate to the folder you copied images to, and click terry-work-usb-2009-12-11.E01. Click Open.

6. In the message box asking which partition to use, leave the default setting for using the entire image file, and then click OK. Click OK to close the “Select device to add” dialog box.

7. Click the terry-work-usb-2009-12-11.E01 filename at the lower right, and then click the Open button to the left to open the File System Browser window.

8. Click the File Name Search icon in the File System Browser window or the left pane of the main window. In the Search String text box, type kitty*. On the far right, click the Search button. Notice that the “kitty porn” isn’t on his USB drive.



OSForensics - M57-Terrys USB drive

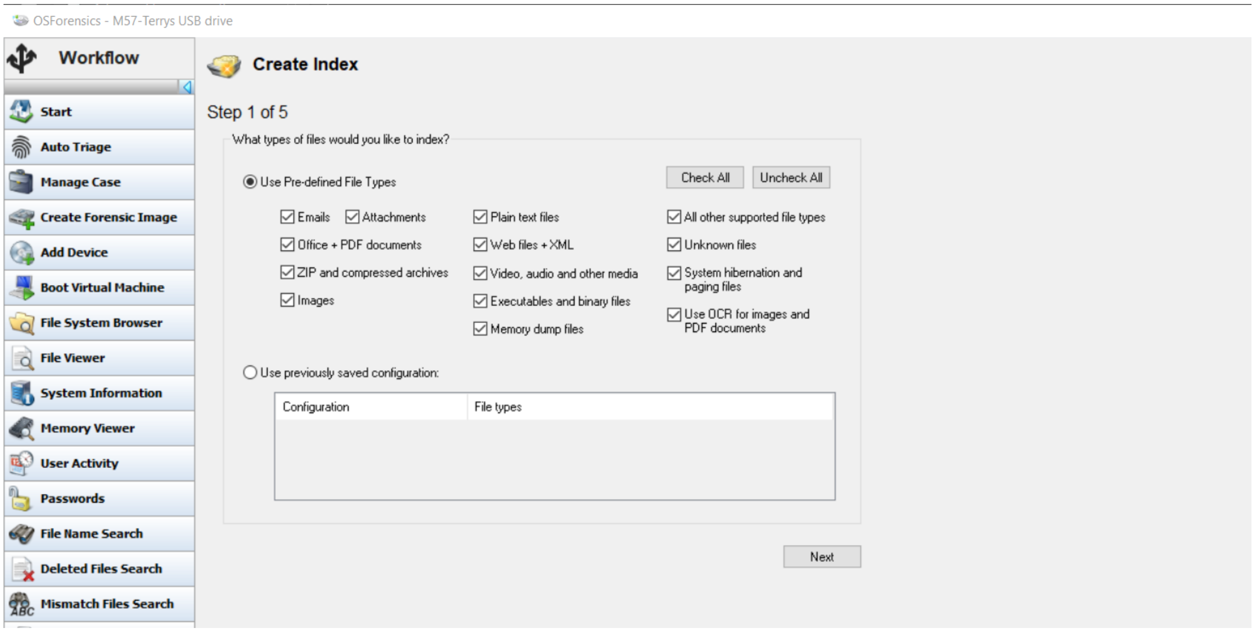
File Name Search

Folder to scan: terry-work-usb-2009-12-11-0:

Preset: User-defined Search

Kitty*

9. Click the Create Index button in the left pane. (Note: You might have to click New Index if the window is showing the results from the index of Charlie’s USB drive.) In the Step 1 of 5 window, click the Use Pre-defined File Types option button, click all the file types listed, and then click Next.



Create Index

Step 1 of 5

What types of files would you like to index?

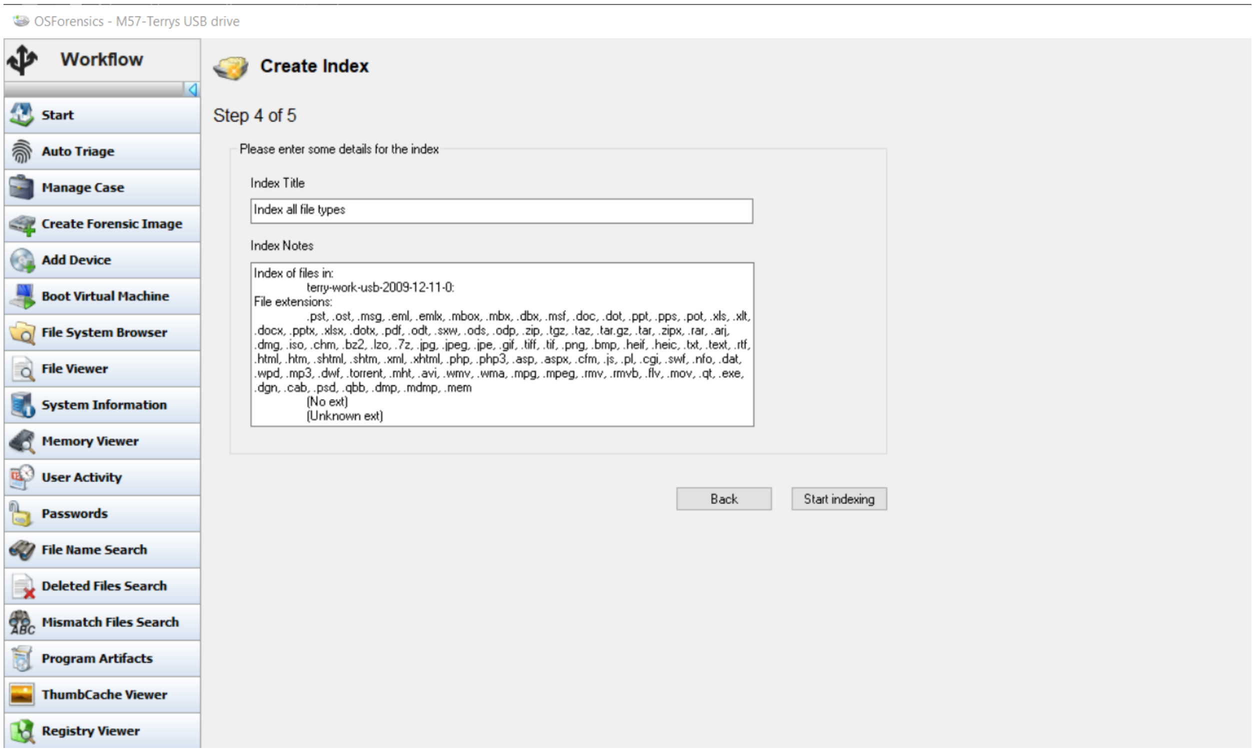
● Use Pre-defined File Types

☑ Emails ☑ 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

○ Use previously saved configuration:

10. In the Step 2 of 5 window, click Charlie’s USB image and click Remove to delete it from the list box, if necessary. Click Add, click terry-work-usb-2009-12-11.E01, click OK, and then click Next.

11. In the Step 3 of 5 window, type Index all file types in the Index Title text box, and then click Start Indexing. When the indexing is finished, which might take up to an hour, click OK in the message box.



Create Index

Step 4 of 5

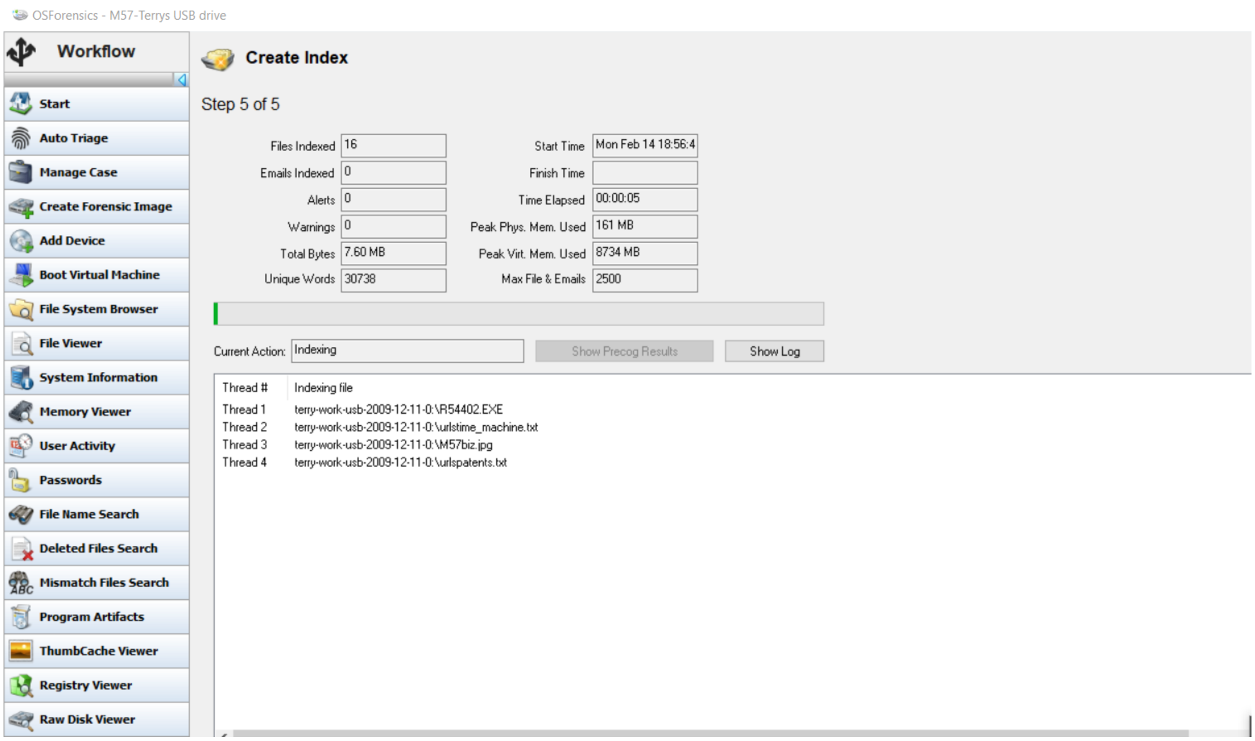
Please enter some details for the index

Index Title: Index all file types

Index Notes:

```
Index of files in:
            terry-work-usb-2009-12-11-0:
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, .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)
```

12. Click the Open Log button at the lower right, and examine the log. Notice whether any errors were reported and the number of files processed, and then close the log.



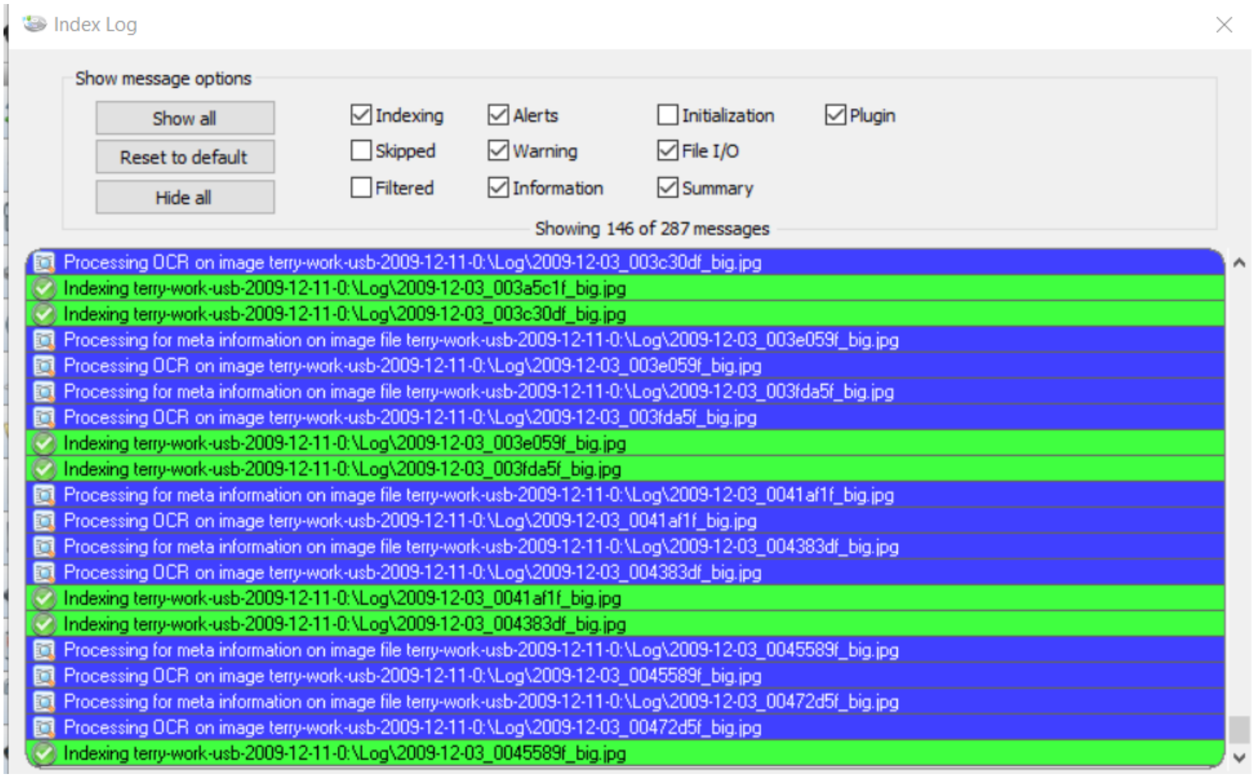
Create Index

Step 5 of 5

Files Indexed	16	Start Time	Mon Feb 14 18:56:4
Emails Indexed	0	Finish Time	
Alerts	0	Time Elapsed	00:00:05
Warnings	0	Peak Phys. Mem. Used	161 MB
Total Bytes	7.60 MB	Peak Virt. Mem. Used	8734 MB
Unique Words	30738	Max File & Emails	2500

Current Action: Indexing

Thread #	Indexing file
Thread 1	terry-work-usb-2009-12-11-0:\R54402.EXE
Thread 2	terry-work-usb-2009-12-11-0:\urlstime_machine.txt
Thread 3	terry-work-usb-2009-12-11-0:\M57biz.jpg
Thread 4	terry-work-usb-2009-12-11-0:\urlspatents.txt

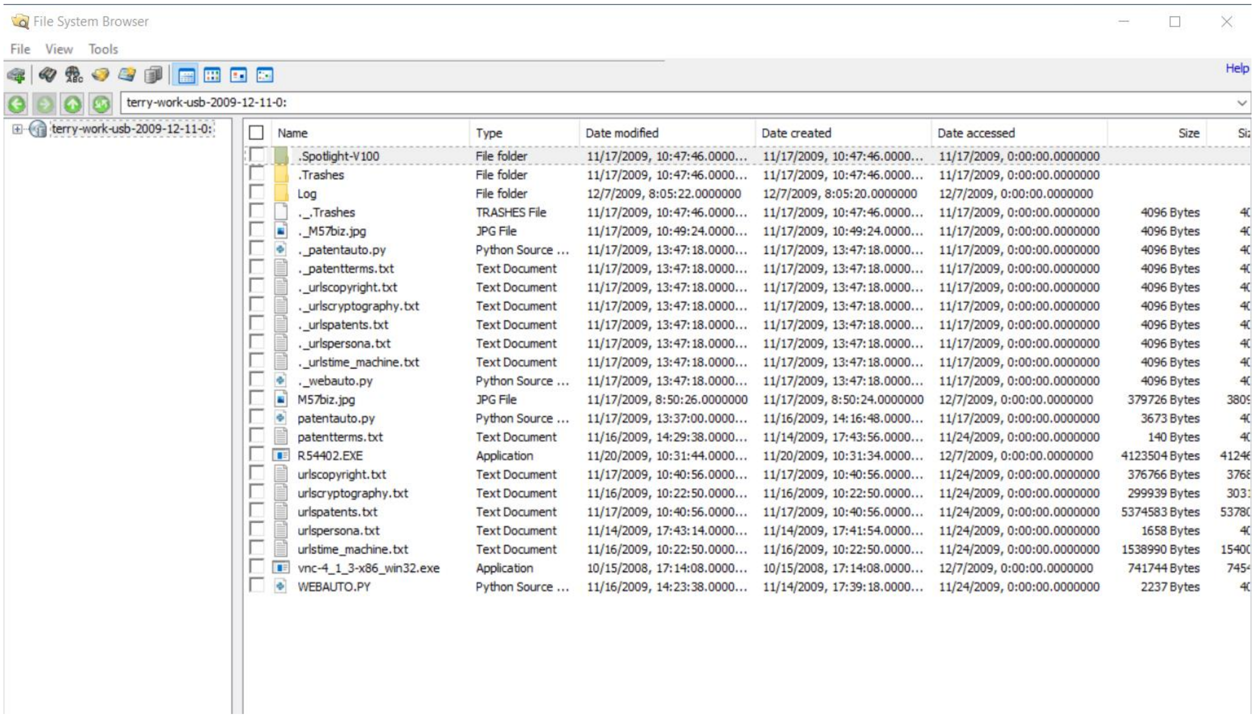


☑ Indexing ☑ Alerts □ Initialization ☑ Plugin
□ Skipped ☑ Warning ☑ File I/O
□ Filtered ☑ Information ☑ Summary

Showing 146 of 287 messages

```
Processing OCR on image terry-work-usb-2009-12-11-0:\Log\2009-12-03_003c30df_big.jpg
Indexing terry-work-usb-2009-12-11-0:\Log\2009-12-03_003a5c1f_big.jpg
Indexing terry-work-usb-2009-12-11-0:\Log\2009-12-03_003c30df_big.jpg
Processing for meta information on image file terry-work-usb-2009-12-11-0:\Log\2009-12-03_003e059f_big.jpg
Processing OCR on image terry-work-usb-2009-12-11-0:\Log\2009-12-03_003e059f_big.jpg
Processing for meta information on image file terry-work-usb-2009-12-11-0:\Log\2009-12-03_003fda5f_big.jpg
Processing OCR on image terry-work-usb-2009-12-11-0:\Log\2009-12-03_003fda5f_big.jpg
Indexing terry-work-usb-2009-12-11-0:\Log\2009-12-03_003e059f_big.jpg
Indexing terry-work-usb-2009-12-11-0:\Log\2009-12-03_003fda5f_big.jpg
Processing for meta information on image file terry-work-usb-2009-12-11-0:\Log\2009-12-03_0041af1f_big.jpg
Processing OCR on image terry-work-usb-2009-12-11-0:\Log\2009-12-03_0041af1f_big.jpg
Processing for meta information on image file terry-work-usb-2009-12-11-0:\Log\2009-12-03_004383df_big.jpg
Processing OCR on image terry-work-usb-2009-12-11-0:\Log\2009-12-03_004383df_big.jpg
Indexing terry-work-usb-2009-12-11-0:\Log\2009-12-03_0041af1f_big.jpg
Indexing terry-work-usb-2009-12-11-0:\Log\2009-12-03_004383df_big.jpg
Processing for meta information on image file terry-work-usb-2009-12-11-0:\Log\2009-12-03_0045589f_big.jpg
Processing OCR on image terry-work-usb-2009-12-11-0:\Log\2009-12-03_0045589f_big.jpg
Processing for meta information on image file terry-work-usb-2009-12-11-0:\Log\2009-12-03_00472d5f_big.jpg
Processing OCR on image terry-work-usb-2009-12-11-0:\Log\2009-12-03_00472d5f_big.jpg
Indexing terry-work-usb-2009-12-11-0:\Log\2009-12-03_0045589f_big.jpg
```

13. Click the Manage Case button in the left pane. In the lower-right pane, double-click Terrys USB under the Devices heading, open any text or picture files, and examine them.



□	Name	Type	Date modified	Date created	Date accessed	Size	Si
□	.Spotlight-V100	File folder	11/17/2009, 10:47:46.0000...	11/17/2009, 10:47:46.0000...	11/17/2009, 0:00:00.0000000		
□	.Trashes	File folder	11/17/2009, 10:47:46.0000...	11/17/2009, 10:47:46.0000...	11/17/2009, 0:00:00.0000000		
□	Log	File folder	12/7/2009, 8:05:22.0000000	12/7/2009, 8:05:20.0000000	12/7/2009, 0:00:00.0000000		
□	._.Trashes	TRASHES File	11/17/2009, 10:47:46.0000...	11/17/2009, 10:47:46.0000...	11/17/2009, 0:00:00.0000000	4096 Bytes	40
□	._M57biz.jpg	JPG File	11/17/2009, 10:49:24.0000...	11/17/2009, 10:49:24.0000...	11/17/2009, 0:00:00.0000000	4096 Bytes	40
□	._patentauto.py	Python Source ...	11/17/2009, 13:47:18.0000...	11/17/2009, 13:47:18.0000...	11/17/2009, 0:00:00.0000000	4096 Bytes	40
□	._patentterms.txt	Text Document	11/17/2009, 13:47:18.0000...	11/17/2009, 13:47:18.0000...	11/17/2009, 0:00:00.0000000	4096 Bytes	40
□	._urlscopyright.txt	Text Document	11/17/2009, 13:47:18.0000...	11/17/2009, 13:47:18.0000...	11/17/2009, 0:00:00.0000000	4096 Bytes	40
□	._urlscryptography.txt	Text Document	11/17/2009, 13:47:18.0000...	11/17/2009, 13:47:18.0000...	11/17/2009, 0:00:00.0000000	4096 Bytes	40
□	._urlspatents.txt	Text Document	11/17/2009, 13:47:18.0000...	11/17/2009, 13:47:18.0000...	11/17/2009, 0:00:00.0000000	4096 Bytes	40
□	._urlspersona.txt	Text Document	11/17/2009, 13:47:18.0000...	11/17/2009, 13:47:18.0000...	11/17/2009, 0:00:00.0000000	4096 Bytes	40
□	._urlstime_machine.txt	Text Document	11/17/2009, 13:47:18.0000...	11/17/2009, 13:47:18.0000...	11/17/2009, 0:00:00.0000000	4096 Bytes	40
□	._webauto.py	Python Source ...	11/17/2009, 13:47:18.0000...	11/17/2009, 13:47:18.0000...	11/17/2009, 0:00:00.0000000	4096 Bytes	40
□	M57biz.jpg	JPG File	11/17/2009, 8:50:26.0000000	11/17/2009, 8:50:24.0000000	12/7/2009, 0:00:00.0000000	379726 Bytes	3809
□	patentauto.py	Python Source ...	11/17/2009, 13:37:00.0000...	11/16/2009, 14:16:48.0000...	11/17/2009, 0:00:00.0000000	3673 Bytes	40
□	patentterms.txt	Text Document	11/16/2009, 14:29:38.0000...	11/14/2009, 17:43:56.0000...	11/24/2009, 0:00:00.0000000	140 Bytes	40
□	R54402.EXE	Application	11/20/2009, 10:31:44.0000...	11/20/2009, 10:31:34.0000...	12/7/2009, 0:00:00.0000000	4123504 Bytes	41246
□	urlscopyright.txt	Text Document	11/17/2009, 10:40:56.0000...	11/17/2009, 10:40:56.0000...	11/24/2009, 0:00:00.0000000	376766 Bytes	3768
□	urlscryptography.txt	Text Document	11/16/2009, 10:22:50.0000...	11/16/2009, 10:22:50.0000...	11/24/2009, 0:00:00.0000000	299939 Bytes	3031
□	urlspatents.txt	Text Document	11/17/2009, 10:40:56.0000...	11/17/2009, 10:40:56.0000...	11/24/2009, 0:00:00.0000000	5374583 Bytes	53780
□	urlspersona.txt	Text Document	11/14/2009, 17:43:14.0000...	11/14/2009, 17:41:54.0000...	11/24/2009, 0:00:00.0000000	1658 Bytes	40
□	urlstime_machine.txt	Text Document	11/16/2009, 10:22:50.0000...	11/16/2009, 10:22:50.0000...	11/24/2009, 0:00:00.0000000	1538990 Bytes	15400
□	vnc-4_1_3-x86_win32.exe	Application	10/15/2008, 17:14:08.0000...	10/15/2008, 17:14:08.0000...	12/7/2009, 0:00:00.0000000	741744 Bytes	7454
□	WEBAUTO.PY	Python Source ...	11/16/2009, 14:23:38.0000...	11/14/2009, 17:39:18.0000...	11/24/2009, 0:00:00.0000000	2237 Bytes	40

14. Scroll to the bottom of the left pane, and click the Exit button. Write a one- to two-page paper explaining the importance of the files you examined. How might they affect a patent case? When you're finished, exit OSForensics.

The information on Terry's pen drive has been examined. The following information is contained on the Pen drive.

1) Photographs: On the pen drive, we discovered Terry's personal and family photographs. Pictures on a pen drive are not a problem.

2) Third-party software: I also made a note of certain executable third-party software files on the pen drive. These executable files are unnecessary because they can be used by third-party applications and may contain dangerous or virus code.

3) Video Files: I discovered a small bit of video footage on the pen drive. Terry made this video for himself. So there's no video issue. It's no problem.

4) Business Documents: I also saw some presentations and pen drive documents related to the company. These are classified materials that can only be accessed on company computers. It's not okay because these records are on Terry's pen drive.

5) Pdf files: were also included on the pen drive. These pdf files are related to cutting-edge technology as well as some educational topics. There are no issues with these pdf files. Because these pdf files are open source, anyone can see them.

We can deduce that Terry's is guilty of storing company-related private material on his pen drive based on the contents of Terry's pen drive. If this pen drive ends up in the hands of another corporation, it will cause significant damage to the current one.

Hands-On Project 4-4

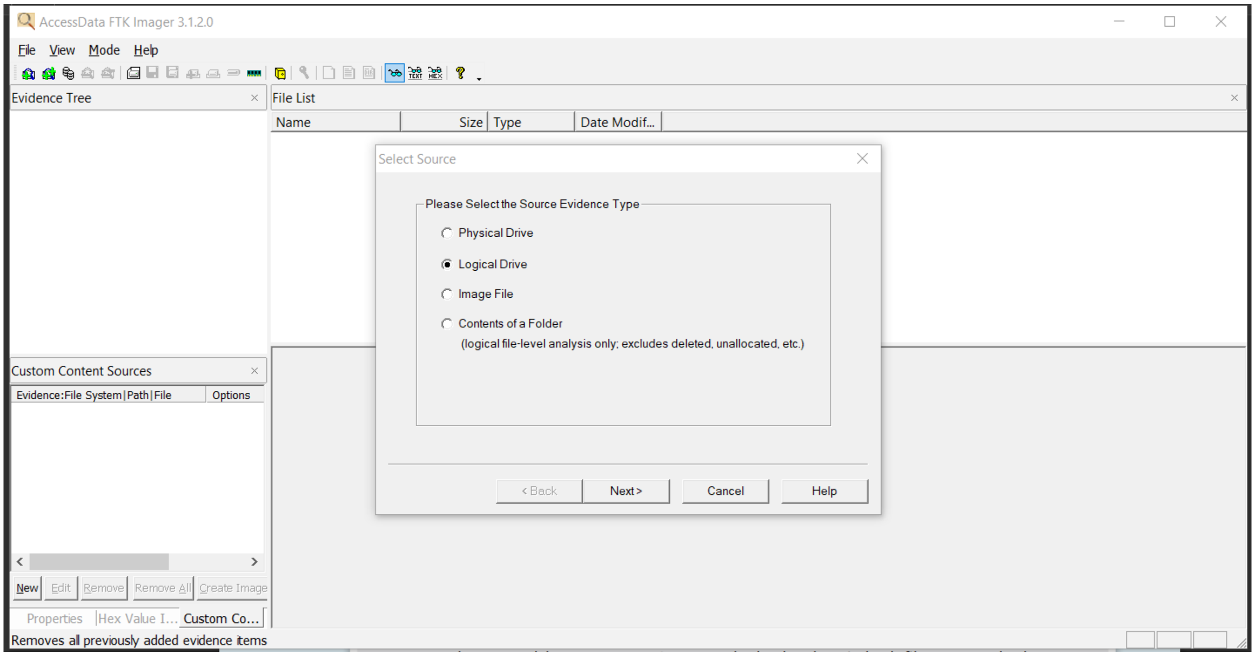
In this project, you create a file on a USB drive and calculate its hash value in FTK Imager Lite. Then you change the file and calculate the hash value again to compare the files. You need a Windows computer and a USB drive.

1. Create a folder called C4Prj04 on your USB drive, and then start Notepad.

2. In a new text file, type This is a test of hash values. One definition of a forensic hash is that if the file changes, the hash value changes.

3. Save the file as hash1.txt in the C4Prj04 folder on your USB drive, and then exit Notepad.

4. Start FTK Imager Lite (clicking OK or Yes in the UAC message box, if necessary), and click File, Add Evidence Item from the menu. In the Select Source dialog box, click the Logical Drive option button, and then click Next.



Select Source

Please Select the Source Evidence Type

○ Physical Drive

● Logical Drive

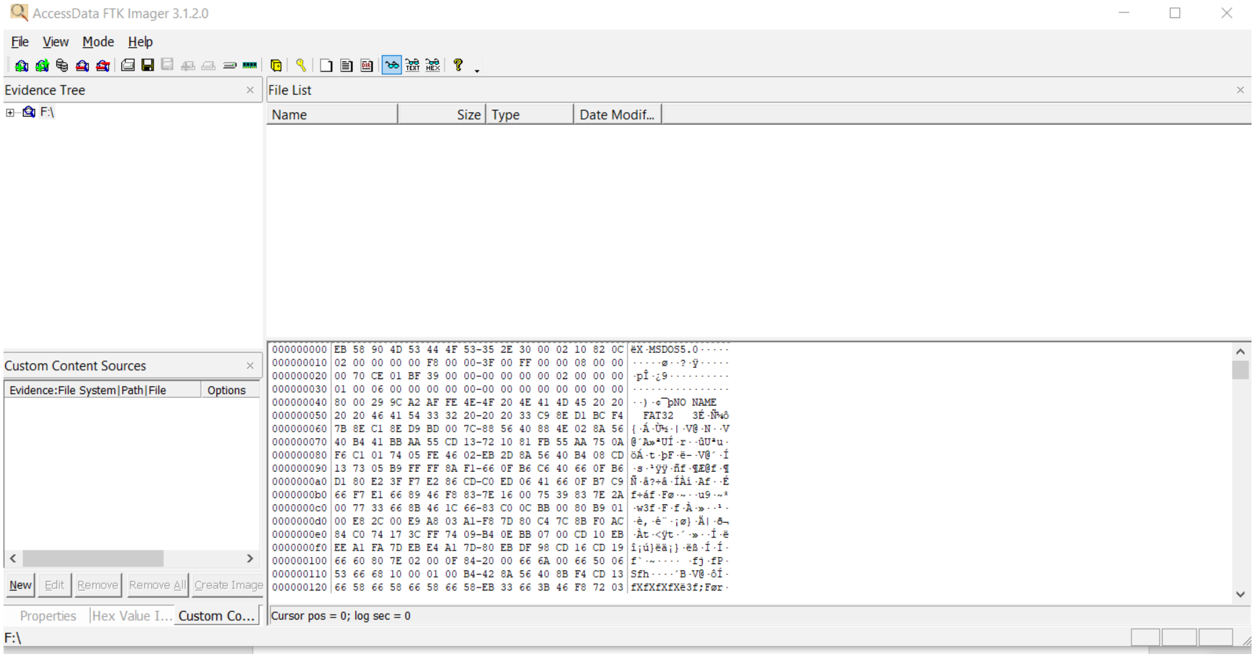
○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

< Back | Next > | Cancel | Help

Removes all previously added evidence items

5. In the Select Drive dialog box, click the Source Drive Selection list arrow, click to select your USB drive, and then click Finish.

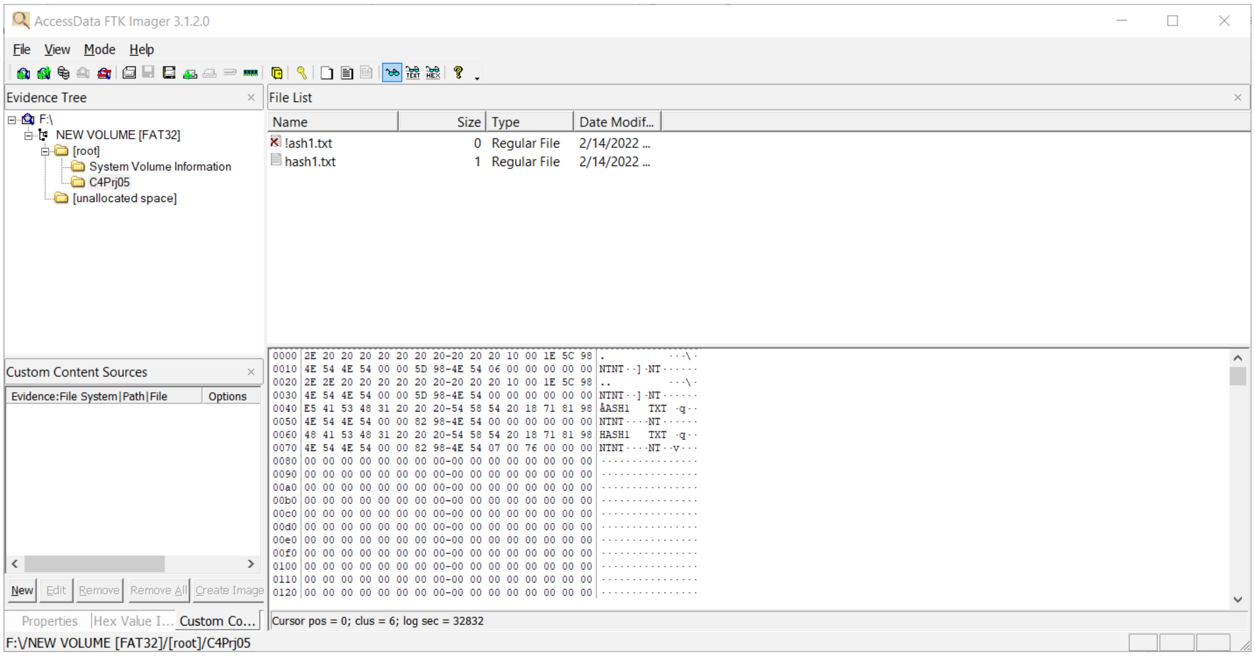


```
000000000 EB 58 90 4D 53 44 4F 53-35 2E 30 00 02 10 82 0C ëX·MSDOS5.0·····
000000010 02 00 00 00 00 F8 00 00-3F 00 FF 00 00 08 00 00 ·····ø··?·ÿ·····
000000020 00 70 CE 01 BF 39 00 00-00 00 00 00 02 00 00 00 ·pÎ·¿9··········
000000030 01 00 06 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000000040 80 00 29 9C A2 AF FE 4E-4F 20 4E 41 4D 45 20 20 ··)·¢¯þNO NAME  
000000050 20 20 46 41 54 33 32 20-20 20 33 C9 8E D1 BC F4   FAT32   3É·Ñ¼ô
000000060 7B 8E C1 8E D9 BD 00 7C-88 56 40 88 4E 02 8A 56 {·Á·Ù½·|·V@·N··V
000000070 40 B4 41 BB AA 55 CD 13-72 10 81 FB 55 AA 75 0A @´A»ªUÍ·r··ûUªu·
000000080 F6 C1 01 74 05 FE 46 02-EB 2D 8A 56 40 B4 08 CD öÁ·t·þF·ë-·V@´·Í
000000090 13 73 05 B9 FF FF 8A F1-66 0F B6 C6 40 66 0F B6 ·s·¹ÿÿ·ñf·¶Æ@f·¶
0000000a0 D1 80 E2 3F F7 E2 86 CD-C0 ED 06 41 66 0F B7 C9 Ñ·â?÷â·ÍÀí·Af··É
0000000b0 66 F7 E1 66 89 46 F8 83-7E 16 00 75 39 83 7E 2A f÷áf·Fø·~··u9·~*
0000000c0 00 77 33 66 8B 46 1C 66-83 C0 0C BB 00 80 B9 01 ·w3f·F·f·À·»··¹·
0000000d0 00 E8 2C 00 E9 A8 03 A1-F8 7D 80 C4 7C 8B F0 AC ·è,·é¨·¡ø}·Ä|·ð¬
0000000e0 84 C0 74 17 3C FF 74 09-B4 0E BB 07 00 CD 10 EB ·Àt·<ÿt·´·»··Í·ë
0000000f0 EE A1 FA 7D EB E4 A1 7D-80 EB DF 98 CD 16 CD 19 î¡ú}ëä¡}·ëß·Í·Í·
000000100 66 60 80 7E 02 00 0F 84-20 00 66 6A 00 66 50 06 f`·~···· ·fj·fP·
000000110 53 66 68 10 00 01 00 B4-42 8A 56 40 8B F4 CD 13 Sfh····´B·V@·ôÍ·
000000120 66 58 66 58 66 58 66 58-EB 33 66 3B 46 F8 72 03 fXfXfXfXë3f;Før·
```

Cursor pos = 0; log sec = 0

F:\

6. In the upper-left pane, click to expand the USB drive and continue expanding until you can click the C4Prj04 folder. In the upper-right pane, you should see the hash1.txt file you created.



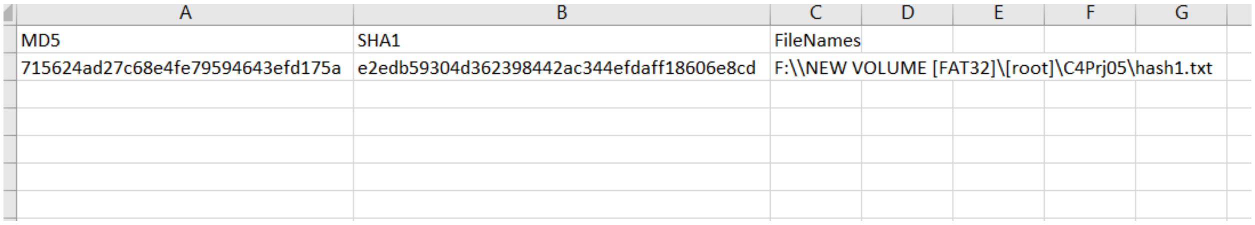
Name	Size	Type	Date Modif...
!ash1.txt	0	Regular File	2/14/2022 ...
hash1.txt	1	Regular File	2/14/2022 ...

```
0000 2E 20 20 20 20 20 20 20-20 20 20 10 00 1E 5C 98 .           ···\·
0010 4E 54 4E 54 00 00 5D 98-4E 54 06 00 00 00 00 00 NTNT··]·NT······
0020 2E 2E 20 20 20 20 20 20-20 20 20 10 00 1E 5C 98 ..          ···\·
0030 4E 54 4E 54 00 00 5D 98-4E 54 00 00 00 00 00 00 NTNT··]·NT······
0040 E5 41 53 48 31 20 20 20-54 58 54 20 18 71 81 98 åASH1   TXT ·q··
0050 4E 54 4E 54 00 00 82 98-4E 54 00 00 00 00 00 00 NTNT····NT······
0060 48 41 53 48 31 20 20 20-54 58 54 20 18 71 81 98 HASH1   TXT ·q··
0070 4E 54 4E 54 00 00 82 98-4E 54 07 00 76 00 00 00 NTNT····NT··v···
0080 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0090 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0100 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0110 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0120 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
```

Cursor pos = 0; clus = 6; log sec = 32832

F:\/NEW VOLUME [FAT32]/[root]/C4Prj05

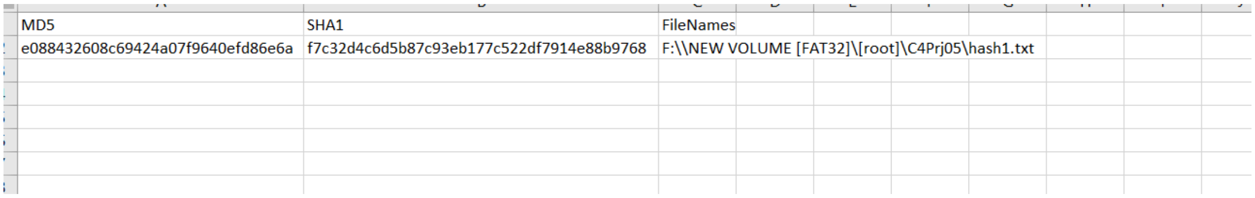
7. Right-click the file and click Export File Hash List. Save the file as original hash in the C4Prj04 folder on your USB drive. FTK Imager Lite saves it as a .csv file. Exit FTK Imager Lite, and start Notepad.



A	B	C	D	E	F	G
MD5	SHA1	FileNames				
715624ad27c68e4fe79594643efd175a	e2edb59304d362398442ac344efdaff18606e8cd	F:\\NEW VOLUME [FAT32]\[root]\C4Prj05\hash1.txt				

8. Open hash1.txt in Notepad. Add one letter to the end of the file, save it, and exit Notepad.

9. Start FTK Imager Lite again. Repeat Steps 4 to 7 (but without starting Notepad), but this time when you export the file hash list, save the file as changed hash.



MD5	SHA1	FileNames
e088432608c69424a07f9640efd86e6a	f7c32d4c6d5b87c93eb177c522df7914e88b9768	F:\\NEW VOLUME [FAT32]\[root]\C4Prj05\hash1.txt

10. Open the original hash and changed hash files on your USB drive in Excel or another spreadsheet program. Compare the hash values in both files to see whether they're different, and then exit Excel and FTK Imager Lite.

From the project hash value is different when adding letter and removing from the file.

Hands-On Project 4-5

In this project, you create a file on your USB drive and calculate its hash values in FTK Imager Lite. Then you change the filename and extension and calculate the hash values again to compare them. You need a Windows computer and a USB drive.

1. Create a folder called C4Prj05 on your USB drive, and then start Notepad.

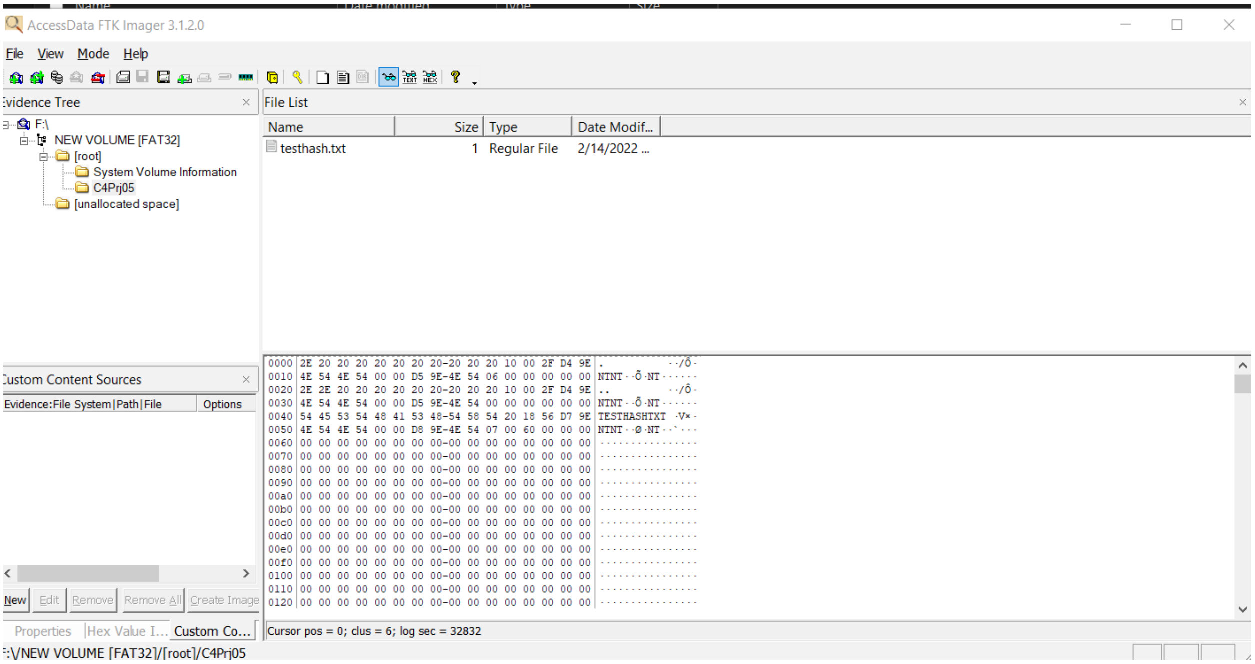
2. In a new text file, type This project shows that the file, not the filename, has to change for the hash value to change.

3. Click File, Save As from the menu, and save the file as testhash.txt in the C4Prj05 folder on your USB drive. Exit Notepad, and start FTK Imager Lite (clicking OK or Yes in the UAC message box, if necessary).

4. Click File, Add Evidence Item from the menu. In the Select Source dialog box, click the Logical Drive option button, and then click Next.

5. In the Select Drive dialog box, click the Source Drive Selection list arrow, click to select your USB drive, and then click Finish

6. In the upper-left pane, click to expand your USB drive and continue expanding until you can click the C4Prj05 folder. In the upper-right pane, you should see the testhash.txt file you created.



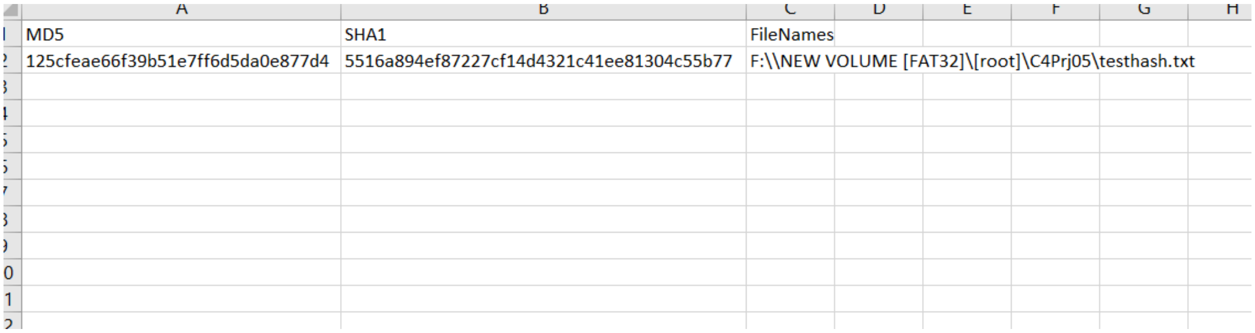
Name	Size	Type	Date Modif...
testhash.txt	1	Regular File	2/14/2022 ...

```
0000  2E 20 20 20 20 20 20 20-20 20 20 10 00 2F D4 9E  .         ··/Ô·
0010  4E 54 4E 54 00 00 D5 9E-4E 54 06 00 00 00 00 00  NTNT··Õ·NT······
0020  2E 2E 20 20 20 20 20 20-20 20 20 10 00 2F D4 9E  ..        ··/Ô·
0030  4E 54 4E 54 00 00 D5 9E-4E 54 00 00 00 00 00 00  NTNT··Õ·NT······
0040  54 45 53 54 48 41 53 48-54 58 54 20 18 56 D7 9E  TESTHASHTXT ·V×·
0050  4E 54 4E 54 00 00 D8 9E-4E 54 07 00 60 00 00 00  NTNT··Ø·NT··`···
0060  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0070  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0080  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0090  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
00a0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
00b0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
00c0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
00d0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
00e0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
00f0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0100  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0110  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0120  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
```

Cursor pos = 0; clus = 6; log sec = 32832

:\NEW VOLUME [FAT32]/[root]/C4Prj05

7. Right-click the file and click Export File Hash List. Save the file as original hash value in the C4Prj05 folder on your USB drive. FTK Imager Lite saves it as a .csv file.



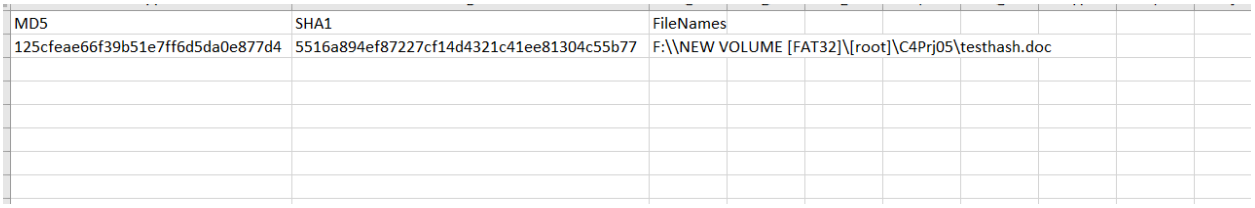
A	B	C	D	E	F	G	H
MD5	SHA1	FileNames					
125cfeae66f39b51e7ff6d5da0e877d4	5516a894ef87227cf14d4321c41ee81304c55b77	F:\\NEW VOLUME [FAT32]\[root]\C4Prj05\testhash.txt					

8. Click to select your USB drive in the upper-left pane, if necessary, and then click File, Remove Evidence Item from the menu. Exit FTK Imager Lite.

9. Open File Explorer. Right-click the testhash.txt file on your USB drive, and rename it as testhash.doc. In the warning message about the change in extension, click Yes.

10. Start FTK Imager Lite. Follow Steps 4 to 7, but this time when you export the file hash list, save the file as changed hash value. Exit FTK Imager Lite.

11. Open original hash value and changed hash value in Excel or another spreadsheet program. Compare the hash values in both files to see whether they’re different, and then exit Excel



MD5	SHA1	FileNames
125cfeae66f39b51e7ff6d5da0e877d4	5516a894ef87227cf14d4321c41ee81304c55b77	F:\\NEW VOLUME [FAT32]\[root]\C4Prj05\testhash.doc

From the project, hash value is not changed when you change the extension.

Anti-Forensics: Techniques

Safal Lamichhane

Department of Computer Science, Southeast Missouri State University

Cy 620: Advanced Computer Forensics

Instructor’s name: Dr. Mario Garcia

February 14, 2022

Abstract: **Anti-forensics (AF) helps in the digital investigation process. AF is the tactic that is taken to help in digital investigation. AF tools and techniques help in erasing information, creating chaffs that waste time and hide information from the investigator. It also makes fake evidence that implicates an innocent person. It exploits implementation bugs in tools and leaves certain data that cause CFT to reveal their use to the attacker. There are some traditional AF tools like disk sanitizers. It was created to protect the privacy of the user. This paper describes traditional AF techniques like disk sanitization utilities. It discusses how by exploiting bugs in forensic tools. This paper also shows the effectiveness of these tools for defeating CFTs. AF procedures are employed to delay digital information rather than prevent its discovery. AF is used to remove the traces or evidence so that it will be hard for the investigators to collect the evidence from digital computers. Generally, AF is used for delaying or misdirecting any investigations so that it will be hard for the investigators to catch the criminals.**

Keywords**: Anti-Forensic, cybercrime, EnCase, hacker Tools, data hiding, attacks on computer forensics tools, privacy.**

Table of Contents

Introduction

In the present generation, computers have become a part of our day-to-day life whether you are eating or sleeping. They have made life easy for everyone due to their broad use. But, due to those different capabilities, computers have also become a tool for criminals which they can misuse. While doing crime, there are two prospects: one without leaving traces and evidence, another by clearing the evidence such that that evidence is untraceable. Forensics means utilizing certain tools and techniques for investigation in a crime. So, we can say that computer forensics refers to a computer system that is gathered from the crime scene. That computer system is later investigated and analyzed in search of some evidence. Nowadays, different crime takes place using digital evidence, due to which courts and laws also accept those evidence as an eyewitness. So, both criminals and investigators both try to retrieve and destroy. Destroy the evidence by criminals to make the investigation even harder. This is called Anti-forensic. Thus, we can say ATF is the countermeasures that are taken to make the investigation harder and misrepresent the evidence to gain more time to escape to prevent getting caught.

AF Techniques

Artifact Wiping

This technique is used to attempt data sanitization, where sanitization is the process of deliberately, and irreversibly removing or destroying the data stored on memory [2]. It can be achieved in various ways.

We might think that using shift+del to delete files permanently makes those data deleted, but the fact is that data can be easily tracked down and recovered. It is because when you delete those files they won't be deleted from the hard drive but are shifted or de-allocated making the space where the data was before empty. There are various open-source tools like Eraser, PGP wipe for data sanitization.

This technique is more preferred due to its time consuming which is less and is more efficient but there are some limitations to it. Some data wiping is hard to achieve. Deleting a file from the other file system structures such as journal files and page file is hard [3].

Data Hiding

It is one of the oldest methods. In this method, we believe that one investigator can give a limited time and a resource to one case. So, with a huge amount of material to search given the size of the hard disk of modern computers is hard. There are many ways of hiding the data. One is the relocation of data. The target data is stored at a location that a user thinks will not be examined by the investigator. Another way is transferring data into portable storage and wiping it from the computer. This method has a drawback that relocating leave behind a record of data transferred into automated logs and computers also update the system logs when the portable storage devices are connected to it.

Another way is making the data invisible concealing the fact that there is still data hidden but exists. It can be achieved by steganography or streaming. The steganography method hides files and information into another file. It was used generally to hide the images. But, now many advanced techniques are using various file formats. Streaming files use a table entry of a single primary file which can associate more than one file. When forensic tools are run, they will show only a primary file. If files are not compressed or encoded before streaming, streamed files can be found by keyword or other searches.

Lastly, data hiding can also be achieved by altering file extensions. For instance, if the .doc file is converted into .exe then hiding is achieved as the investigator will be likely to look .doc file. This can be recovered however with the help of signature analysis which finds out the actual file types.

Trail obfuscation

This technique is also called counterfeiting. It means to imitate to forge. This method is used to confuse and mislead the investigation.

It can be achieved in various ways. One is Defragmentation. This technique uses the old concept of artificial wiping to confuse the ongoing investigation. As we know it is very difficult to store large files in one contiguous space. And we know that the file is stored in different locations in part. It helps in achieving rewriting and erasing the files all over the disks which disrupts data in the space that is allotted. And it will eventually lead to destroying any traces in those locations. So, it does not delete files like artificial wiping but destroys any residual data that may be present.

This technique raises suspicions when it is discovered that it was done after the system was being analyzed by the investigator. It is said that too much use of this tool may lead to more suspicion as it is recommended only to do one a year or in 6 months.

Another way is by attacking the credibility of the evidence in the question. It is commonly done by modifying the Metadata. Timestamps are one type of metadata that shows when the document was created, last accessed, or modified. Hence, altering this make the investigation harder as the data may seem irrelevant to investigators.

Investigators can find out about tampering by using time-based data forensics by analyzing both differences and similarities among various pieces of evidence with the metadata. It is also called a cross-reference time-based forensic scheme which finds both malicious activities and detects tampering of the file stamps.

The attack against computer forensics tools (CFTs) and process

This is the most recent approach and most dangerous one. Attackers or criminals will be an advantage using this method as they will know in prior what kinds of tools can be used by the investigators to capture their malicious activities. As all the forensic tools along with their procedures are well known, their vulnerabilities can be easily determined if an attacker can grab a hand on that tool.

Among the six phases in process of digital forensics describe by palmer, this technique attacks the analysis phase which is the most crucial phase. This phase relies completely on CFTs and the expertise of the investigator and finds out or validates based on evidence that is provided. Attackers will use the vulnerability of those tools relating validation of data. They will use buffer overflow attacks which can damage the functioning of CFTs.

DoS(Denial of Service) attacks the availability. In anti-forensic, it targets resources that are used by CFT. Those resources if accepts any input, then they are likely to be vulnerable to DoS attack. There are various ways of launching a Dos attack. There is also ReDoS(Regular Expression Denial of Service). Regular expressions are used for pattern matching to validate the input. They are most useful in intrusion detection systems where pattern matching is carried out by a special machine.[1]

Conclusion

Various tools are used by the Counter- Forensics. The forensic tool is not able to recover the files. By using the artifact wiping tool, the forensic tool could show the random results for timestamp value. There are no standard measures to prevent an attack on forensic tools. One forensic tool is better in certain scenarios whereas that will be not better in certain scenarios and is simply dependent on the nature of AF implemented. Aperio is one type of tool which finds or hunts traces of counter-forensic tool usage[3]. But even if traces can be found, we cannot recover the data.

Bibliography

1. Anti-Forensics Techniques: An Analytical *Review* - *Researchgate*.

   https://www.researchgate.net/publication/275155942_AntiForensics_Techniques_An_Analytical_Review.

2. University of California - Riverside," Security using Data Sanitization", Available: http://cnc.ucr.edu/security/datasan.html , Aug 05, 2011
3. Geiger," Counter-Forensic Tools: Analysis and Data Recovery" , 18th Annual FIRST Conference, Jun 25-30, 2006.
4. Adrian T.N. Palmer, "Computer Forensics –The six steps ", U.K. Electronic Evidence, Vol.3 No.1, Dec 2004.