PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Computer Forensics (ACCD5000)

Anti Forensics Techniques

This Photo by Unknown Author is licensed under CC BY-NC

Lab Activities are based on

TryHackMe, EC Council – CHFI, Digital Forensics Workbook and other Industry Digital Forensic Curriculum

Objectives

In continuation to our lectures, this hands-on Activity helps in providing you an overview of anti-forensic techniques.

ETHICAL STATEMENT

As discussed during our lectures, it is very important to adhere to Personal Ethics, Professional Ethics, Computer Ethics and Business Ethics.

We, the participants and stakeholders in the digital forensics laboratory, recognize the significance of ethical conduct when using digital forensics tools and processes for academic purposes. Our commitment to ethical standards is grounded in the principles of integrity, privacy, and responsible handling of digital data.

The tools and techniques you are exposed to' in this lab is to work only on a virtual machine environment and the purpose is entirely to demonstrate various digital forensic activities. Experimentation with these tools, techniques, and resources is at the discretion of the instructor and institution. If you as a student consider using these tools for educational purposes on an outside environment, you should contact your lecturer prior to any experimentation.

Note: Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

Based on Activity 2, you must have a lab setup working.	☑
So far:	
HoA1: Understand Digital Evidences - Importance of Computer Forensics – Basic Investigation	☑
HoA2: Understand the importance of ensuring DATA Integrity – Computer Forensics Virtual Lab Setup	☑
HoA3: Understand Investigation Process, Ensure integrity of the evidence by calculating, comparing Hash Values	☑
HoA4: Understand Investigation Process – Copying Evidences and ensuring integrity	☑
HoA5: Understand File Systems – Linux, Windows Images and Deleted Files	☑
HoA6: Understand Data Acquisition – dd, E01, RAM – Imaging Methods	☑
Make sure you have acquired the image required to complete your Coursework. If not, contact the lecturer immediately	☑
Make sure the above activities are completed before starting this week's activity	
Task 1: Solid-state drive (SSD) file carving on Windows and Linux file systems	
Task 2: Cracking passwords of various applications	
Task 3: Steg Analysis	
Task 4: Working with ADS	
Task 5: Detecting file-extension mismatch	
Task 6: Unpacking program packers	
Task 7: Coursework (Important) – Work on your Image – Check for AFT	

ICONS Used in this document:

Find out the outcome/ Answers/ Solution and record your reflection

Do research and complete the task. Need referencing/ in-text citations. Shall be included as a part of your coursework.

Recommended Screenshot (with Timestamp) for your Coursework.

Recommended to address this part in your Coursework.

Note: For this activity and other upcoming activities, you shall use any relevant screenshots or discussions to your coursework according to your judgement. I will not be recommending Screenshots/ Recommended part to address in the coursework.

Task 1

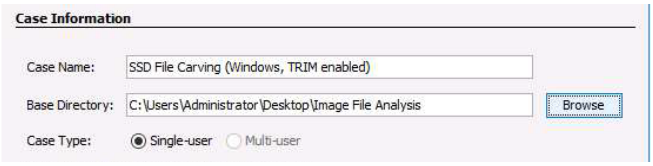
You need Windows 10, Windows Server 2019/ 2022, Autopsy

As a forensic investigator, you should know how to perform SSD file carving on a Windows file system. This lab helps you understand how the TRIM functionality influences the possibility of data recovery on an SSD. It also helps you learn how to recover data from a Windows file system on an SSD when the TRIM functionality is disabled.

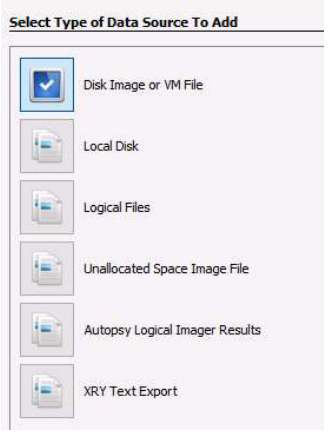
What is File Carving? File carving is a technique to recover files and fragments of files from unallocated hard disk space in the absence of file metadata.

Make sure that Real Time Protection is disabled in Windows 10 virtual machine (if it is running) before beginning this lab.

1. Perform File Carving on Windows File System (Trim Enabled)
2. Login to Windows Server 2019/22.
3. Launch Autopsy and create a New Case, prodie adequate information.



4. Provide the Case Number and Examiner Details (Provide your student id and name).
5. Select Disk Image or VM File in the Add Data Source window and click Next.



6. Select the file task701.dd, and click Open (available in Shared Folder in a compressed folder – named task7).
7. The Add Data Source window now displays the Configure Ingest Modules section which contains a list of options that are checked. Select these options according to your requirement. You may also leave these options set to default.

8. The Add Data Source section appears, displaying the following message: Data Source has been added to the local database. Files are being analyzed. Click Finish.

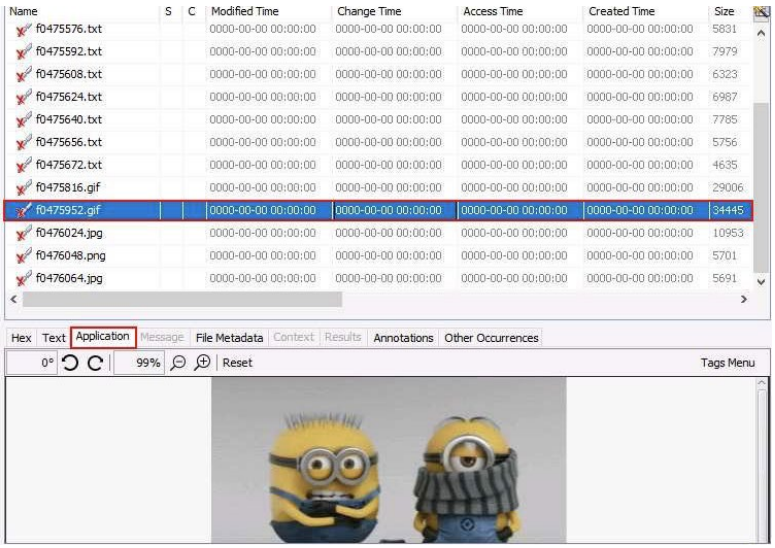
Note: The Autopsy tool will take time to analyze the image file. View the status at the lower-right corner of the Autopsy window. Once the analysis is complete, the status disappears.

9. The application will now take you to its main window. Expand the Data Sources node in the left pane of the window. The Data Sources option lists the name of the image file that you have analyzed (in this case, it is Task701.dd).
10. Click the image file name to view its contents in the right pane of the tool window. The image file contains folders that store data related to files, processes, services, tools, etc., stored/used on a Windows system.
11. Autopsy utilizes most of the virtual machine's resources while scanning the image. The machine might be unresponsive until the scanning is completed. It is recommended not to access the machine until the scanning is completed.
12. You may also view these contents by expanding the image file.
13. You need to recover carved files. The tool takes around 10–15 minutes to analyze the image and attempts to retrieve deleted and carved files from the image.
14. However, since this is a case that involves the use of a TRIM-enabled SSD image file as an evidence file, we observe that the tool does not carve any files. Hence, this demonstrates that file carving is not possible when TRIM is enabled on an SSD image file. You may now close all the windows pertaining to Autopsy.
15. We shall now move to retrieving data from a TRIM-disabled SSD image file. The steps below describe SSD file carving on a Windows file system when TRIM is disabled.
16. Close the Autopsy tool and re-launch it. Create a new case and select the task702.dd file, and click Open and finally analyse.
17. The application now takes you to its main window. Expand the Data Sources node in the left pane. The Data Sources option lists the name of the image file that you have analyzed

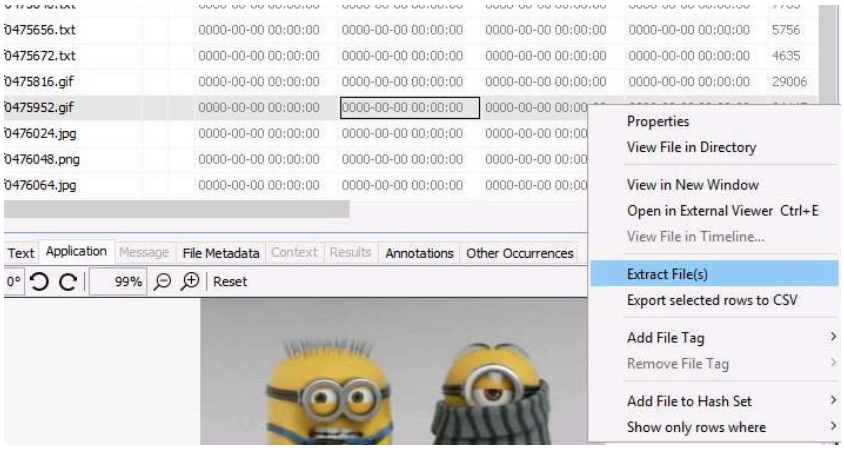
18. Click the image file name to view its contents in the right pane of the tool window. The image file contains folders that store data related to files, processes, services, tools, etc., stored/used on a Windows system.

Name	S	C	Modified Time	Change Time	Access Time	Crea
$OrphanFiles			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000
$CarvedFiles			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000
$Extend			2019-09-09 00:23:18 PDT	2019-09-09 00:23:18 PDT	2019-09-09 00:23:18 PDT	2019
$RECYCLE.BIN			2019-10-04 05:42:29 PDT	2019-10-04 05:42:29 PDT	2019-10-04 05:42:29 PDT	2019
$Unalloc			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000
[current folder]			2019-10-07 16:06:44 PDT	2019-10-07 16:06:44 PDT	2019-10-07 18:14:15 PDT	2019
images			2019-10-07 18:31:12 PDT	2019-10-07 18:31:12 PDT	2019-10-07 18:31:12 PDT	2019
MSI3c953.tmp			2019-10-07 16:06:44 PDT	2019-10-07 16:06:44 PDT	2019-10-07 16:06:44 PDT	2019
Songs			2019-10-04 06:00:00 PDT	2019-10-04 06:00:00 PDT	2019-10-04 06:00:00 PDT	2019
System Volume Information			2019-10-04 05:39:45 PDT	2019-10-04 05:39:45 PDT	2019-10-07 18:14:02 PDT	2019
text			2019-10-07 18:14:21 PDT	2019-10-07 18:14:21 PDT	2019-10-07 18:14:21 PDT	2019
$AttrDef			2019-09-09 00:23:18 PDT	2019-09-09 00:23:18 PDT	2019-09-09 00:23:18 PDT	2019
$BadClus			2019-09-09 00:23:18 PDT	2019-09-09 00:23:18 PDT	2019-09-09 00:23:18 PDT	2019
$BadClus:$Bad			2019-09-09 00:23:18 PDT	2019-09-09 00:23:18 PDT	2019-09-09 00:23:18 PDT	2019

19. To find the carved files, double-click the CarvedFiles folder in the right pane of the window. The tool lists a number of carved files, which are all identified by a cross-mark coupled with a knife icon against the file names.
20. Once the carved files are loaded, you will also find them under the Deleted Files option. Expand the Deleted Files node to find the category All under it. Select All and then scroll down the list of files in the right pane to locate those carved files. Hence, you can alternatively recover those carved files from All under Deleted Files.
21. To view the content of a carved file, select the file. Its content will be displayed in the lower pane of the tool window. Eg: select the file f0475952.gif; the content of this file is displayed in the lower pane of the window.



22. When you select a carved file, the tool will display its content(s) under the Application tab of the lower pane by default. You may also click on the Hex, Text, File Metadata, and other tabs to view the respective data stored under them.
23. Now, to recover the selected carved file, right-click on it and then click Extract File(s) from the context menu.



24. A Save window opens, showing the default location where the file will be exported. This default location is the Export sub-folder that exists within the case folder created in the Image File Analysis folder on the Desktop. Click Save to export the file.
25. A pop-up appears, indicating that the file has been extracted. Close the pop-up or click OK.
26. Now, manually navigate to the location where the carved image file has been saved.
27. In this case, we were able to retrieve and view the file's content(s) because it has been acquired from the disk when TRIM was disabled on it. Similarly, you can also retrieve and view the contents of other carved files.
28. **Form a group in the class and discuss about TRIM Feature. Share your thoughts!!! – Recommendations on Disabling and Enabling TRIM Feature. What it is?**

    Submit your thoughts in the Padlet used during the lecture.

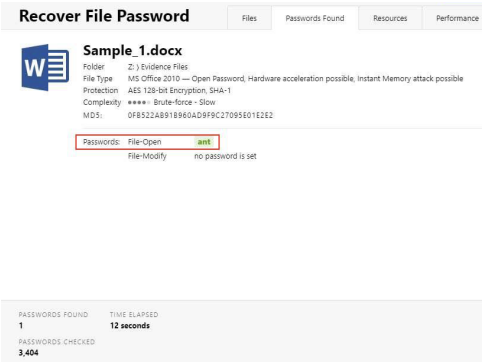
    Make a Group Presentation during the next lecture session.

    Duration: 5 Mins Presentation

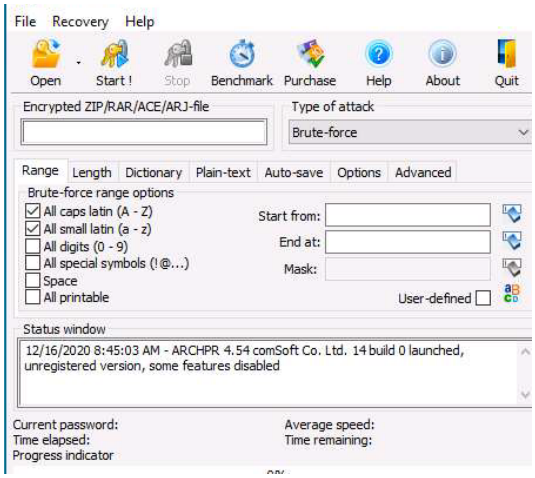
Task 2: Working with Passwords

1. Login to Windows 10 VM.
2. You are free to use any Password Cracking Tools. Write your views in the Discussion Forum and share your work in the Student Shared Folder.
3. Here, the demo is done using Passware Kit Forensic – Demo version.
4. The Passware Kit Forensic GUI appears, as shown in the following screenshot:

5. Click the Recover File Password option from the main window of the tool.
6. Select file Task703.docx, and click Open. (available in our Shared Folder)
7. Upon uploading the file to the application, the Recover File Password window wizard appears, where you need to select the Use Predefined Settings option.
8. The tool will take some time to crack the password. The time required is proportional to the number and types of characters used in the password.
9. After analysis, the tool displays the cracked password, as shown in the screenshot:



10. Now, we shall examine how to crack a compressed password-protected file.
11. You are free to use any Recovery Tools. Write your views in the Discussion Forum and share your work in the Student Shared Folder.
12. To crack the password of a compressed folder, this demo uses Advanced Archive Password Recovery.
13. The Advanced Archive Password Recovery GUI appears, as shown in the following screenshot:



14. Now, set a range for brute-force attack options by checking the options under the Range tab.
15. For the demonstrative purpose of this lab, we are checking the All digits (0-9) option while leaving all the other options unchecked.
16. From the toolbar of the tool window, click Open to add the WinRAR file you wish to crack.
17. An Open window appears. Select the file Compressed_files.rar, and click Open.
18. The tool cracks the password and displays it along with other details.
19. In a real scenario, you must set all the options as you will usually not have any clue regarding the password that protects the file. Therefore, the tool takes a large amount of time for cracking a password, if it is complex in nature. Close the application.
20. Use appropriate tool to crack the password of a password-protected PDF file shared with you. (Confidential.pdf)
21. Document the tool used and the password cracked.

Task 3: Steg Analysis

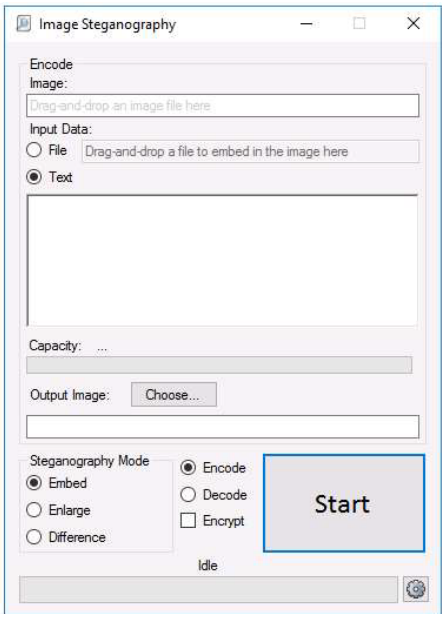
As an expert forensic investigator, you must be able to detect and analyze steganography files.

What is Steganography? Steganography is the process of hiding information or a file within another file. In other words, it is the process of disguising a harmful file as a safe file.

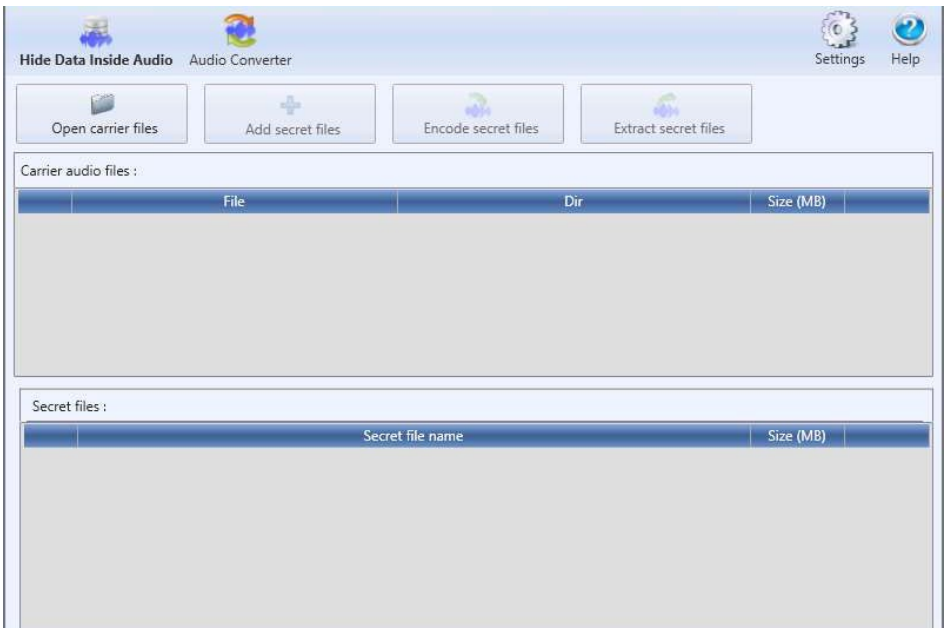
The objective of this lab is to help you analyze files hidden using steganography and find their impact on a system or network.

Make sure that Real Time Protection is disabled in Windows 10 virtual machine.

1. Login to Windows Server 2019/22.
2. You are free to use any Steganography Tools. Write your views in the Discussion Forum and share your work in the Student Shared Folder.
3. Here, the demo is done using StegSpy – Demo version.
4. Select task703.png and click the Open button. (available in Shared Folder)
5. The tool will scan the file and display the type of steganography technique used to hide another file in it.
6. Did you find anything suspicious? Discuss with you class during the next lecture or record your outcomes and discussions in the Forum.
7. Did you tried using any online steganography detection tools? List and discuss in the forum.
8. Let's attempt to decode the content hidden in the image.
   Note: We must keep attempting the use of various tools to detect the data hidden in the image.
9. In this lab, we will use Image Steganography and OpenStego to uncover the hidden data. However, as stated earlier, you are free to use your own selection of tools.
10. Open Image Steganography and launch.
11. The main window of Image Steganography appears, as shown in the following screenshot:



12. Select the Decode option to extract the hidden file from the suspicious file.
13. The tool will attempt to analyze the file and display the result if it could decipher it; else, it will display a message indicating that the provided image is either corrupt or invalid.
14. What outcome did you get? Did you manage to decipher the hidden file?
15. Try with other tools as well and record your outcomes. (Like OpenStego)
16. During investigation, you might also come across audio files that contain hidden data. Now, let's extract hidden data from an audio file using DeepSound. Again, you are free to use any tools.
17. Open DeepSound and launch the application.
18. The DeepSound GUI appears as shown in the following screenshot:



19. Click the Open carrier files button to add the file containing steganography.
20. Note that, the shared folder has a number of audio files. You need to analyse the folder and choose the file that you think is altered/ modified or suspicious.
21. Document your steps and justify your reasons.
22. Open the suspicious audio file, and click the Open button.
23. Click the Extract secret files button to start extracting the hidden files or data.
24. Post extraction, the tool will generate a message displaying the location of the extracted file. Click OK.
25. To view the hidden file that was extracted in the previous step, navigate to the location.
26. Did you manage to successfully identify the suspicious file and extract the hidden information? If not, continue
27. In this manner, you can detect and analyze data hidden in files of various format using steganography.

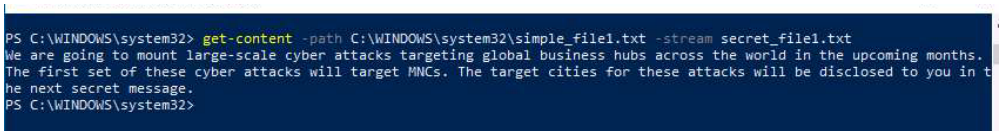
Task 4: Working with ADS

As an expert forensic investigator, you must know how to extract information from hidden ADS. The use of Alternate Data Streams (ADS) is an anti-forensics technique that allows attackers to hide data in Windows NTFS; occasionally, these hidden Alternate Data Streams can be used to remotely exploit a web server. The objective is to help you learn how to detect ADS.

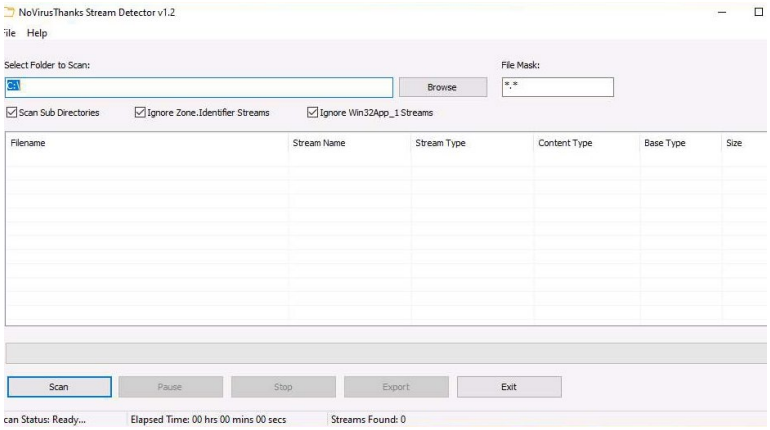
Make sure that Real Time Protection is disabled in Windows 10 virtual machine.

1. Login to Windows 10. Copy the files in ADS Folder in your VM.
2. Launch PowerShell.
3. To identify hidden ADS through PowerShell, enter the command
   gci -recurse | % { gi $_.FullName -stream * } | where stream -ne ':$Data'
   press Enter.
4. Now, navigate to the path where the text files simple_file1.txt and simple_file2.txt reside and open them.
5. The files, when opened, display the data they contain, but hidden alternate data streams cannot be viewed through Windows Explorer.
6. We shall now extract the hidden stream attached to the first file, i.e., simple_file1.txt.

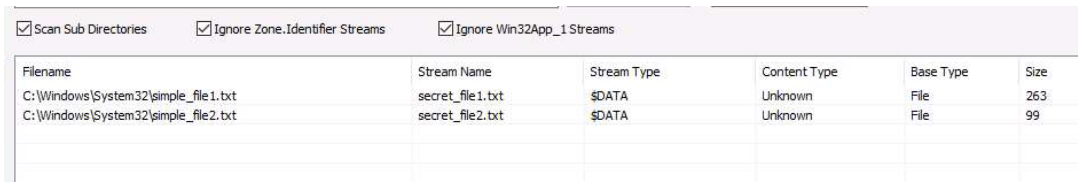
7. To extract the hidden stream, execute the command in Windows PowerShell get-content -path C:\WINDOWS\system32\simple_file1.txt -stream secret_file1.txt
8. PowerShell will extract and display the content stored in the hidden stream as shown in the following screenshot:



9. Similarly, we will now extract the hidden stream attached to the second file, i.e., simple_file2.txt.
10. Go to Moodle, and check for Important Folder in Assessments Tab. The documents in there has your Phone Pins that are required for your Coursework. All the best.
11. Lets use another tool, NoVirusThanks Stream Detector to detect streams. Again, you are free to use any tools.



12. Lets scan the folder. (I am using C:Windows – You shall use the folder that you work with~) A Browse for Folder window will appear. Navigate and select the directory that you wish to scan for ADS and click OK.
13. Click Scan to run a scan on the directory.
14. The tool scans for ADS files. Upon completing the scan, it displays the streams present in the directory with details such as Stream Name, Filename (names of the files in which those streams exist), and Size of the files.



15. Export the file to Desktop. Navigate to Desktop and open the file to view the details of the files containing ADS. In this manner, you can detect streams on a machine and view them.

Task 5: File Extension Mismatch

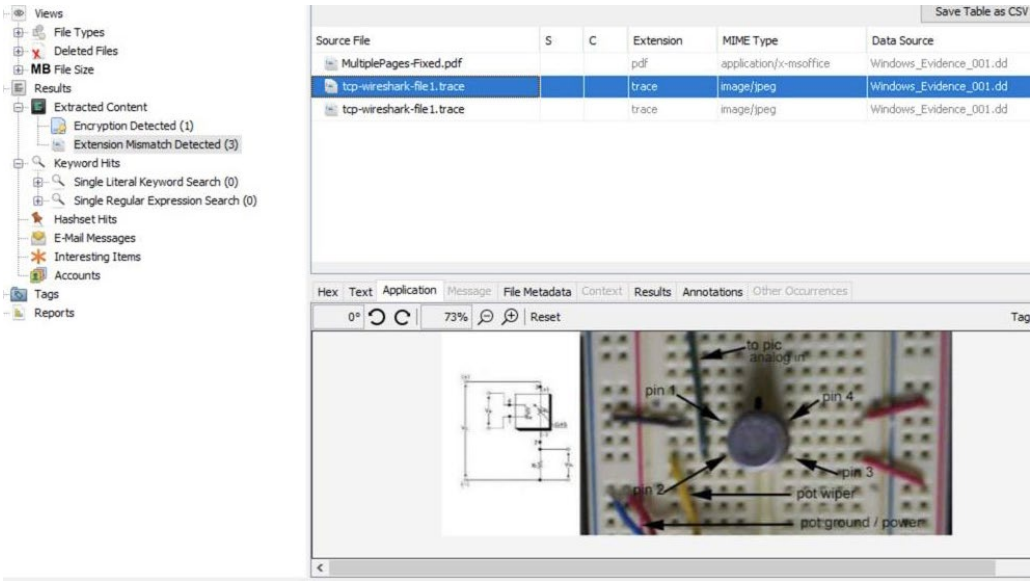
A file extension is an identifier specified as a suffix at the end of a filename. It helps identify the file type in operating systems such as Windows. The objective of this lab is to help you learn how to detect file-extension mismatch.

1. Login to Windows Server 2019/22.
2. Launch Autopsy and create a New Case.
3. Select the task70501.dd image file and configure Ingest Modules and check File Type Identification, Extension Mismatch Detector and Embedded File Extractor options.
4. The tool will now take you to its main window. Expand the Data Sources node in the left pane of the window. The Data Sources option will list the name of the image file you have analyzed.

   Autopsy utilizes most of the virtual machine's resources while scanning the image. The machine might be unresponsive until the scanning is completed. It is recommended not to access the machine until the scanning is 100% completed.

5. Click the image filename to view its contents in the right pane of the tool window. It includes all the necessary operating system data.
6. To view the files that have been detected with an extension mismatch, click the Extension Mismatch Detected category in the left pane. The tool will then display the files with extension mismatch in the right pane of the window.
7. Did you notice anything?
8. The Extension column in the right pane of the window displays the modified extensions of the files, while the MIME Type column displays their original extensions. As the extensions of the files have been modified, it means that they have been tampered with.

9. To view the content(s) of a file with extension mismatch, select the file; its contents will be displayed in the lower pane of the window, (here, we have selected the file tcp-wireshark-file1.trace. Selecting this file displays the image of an electronic circuit in the lower pane of the window. As can be seen in the screenshot below, .trace is the modified extension of this file, while .jpeg is its original extension.



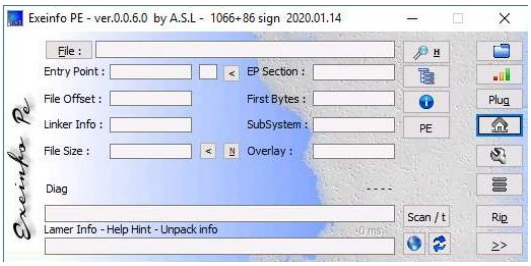
10. When you select an image file, the tool will show you its content(s) under the Application tab of the lower pane of the window by default. You may also click on the Hex, Text, File Metadata, and other tabs to view the respective data stored under them.
11. In this manner, you can identify files with tampered extensions, view their original extensions, and perform further analysis if required.

Task 6: Program Packers

Using program packers is an effective anti-forensics technique for an attacker to prevent malicious programs on a system from being detected. The objective of the lab is to help you learn how to unpack packed program files.

1. Login to Windows Server 2019/22.
2. In this lab, our first task is to identify the packer used to pack a file named Infected.exe.

3. We will use ExeInfo PE to perform this task. You are free to use any tools.



4. The Open EXE,DLL file window will appear. Open the file Infected.exe (Shared in our Folder)

   For the demonstrative purpose of this lab, the target evidence file has been named Infected.exe. In a real scenario, a malicious program file might bear a name that appears normal. Attackers disguise malicious files as normal files by using program packing tools so that they remain undetected by the firewall and anti-malware software on a system.

5. The tool's main window will now display the details of the application that was used to pack the selected executable file (i.e., Infected.exe).
6. Could you see any details about the selected executable file? Which tool was it using? Use the same tool.
7. For me, it is tool UPX. Therefore, I will be using the same tool (UPX) to unpack it.
8. Open UPX in CLI.
9. To unpack the target file, i.e., Infected.exe and save it as Unpacked.exe, run the command
   upx.exe -d -o "C:\ "Give the Path" \Unpacked.exe" "C:\ "Give the Path" \Infected.exe".
10. The UPX tool unpacks the file successfully
11. The packed file has now been unpacked as unpacked.exe and saved to the stated directory.
12. This Unpacked.exe file is the original (uncompressed) file that was packed, and you can observe that its size is greater than that of the packed file.
13. In this manner, you can detect the packers used to pack files and unpack them using suitable tools.

Overall Reflection

Record your reflection via Moodle – Group Discussion.

1. Understanding on the concepts discussed in the lecture and its relation to the activity done.
2. Understanding about various tools used Anti Forensics Techniques.
3. Rate yourself: Understanding on AFT, its tools and analysis

----------End of Activity----------