



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)

Windows Forensics



[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 windows forensics 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	✓
HoA7: Anti-Forensics Techniques	✓
Make sure the above activities are completed before starting this week's activity	
Task 1: Acquiring Volatile Information from a Live Windows System	
Task 2: Discovering and Extracting Forensic Data from Computer	

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.

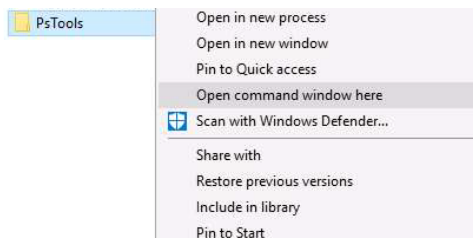
Note: For this activity and other upcoming activities, you shall use any relevant screenshots or discussions to your coursework according to your judgement. I will not be recommending Screenshots/ Recommended part to address in the coursework.

Task 1: Acquiring Volatile Information from a Live Windows System

You need Windows 10, Windows Server 2019/22, PsTools, LogonSessions, NetworkOpenedFiles

Acquiring volatile information from a live system involves obtaining information such as network information and process information about an OS. The objective of this lab is to help you collect volatile information from a live Windows system.

1. Login to your Windows 10 Machine:
2. Our task in this lab is to collect volatile information from a host machine. We will be using Windows Server virtual machine as the host machine and Windows 10 virtual machine as a locally connected machine.
3. Now, switch to Windows Server virtual machine.
4. In Windows Server virtual machine, use Tools from HoA8 Folder or download from Internet sources. Create a Shared Folder in Windows Server and give access to the clients in the network. You will be using the shared folder from your Client Machines.
5. Select the PsTools folder, hold the Shift key on the keyboard, right-click on the selected folder, and then select Open command window here from the context menu.



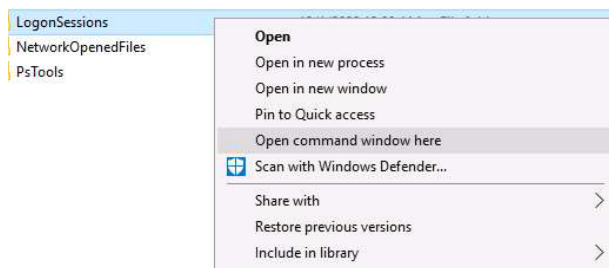
6. The above operation will launch Command Prompt displaying the path of PsTools. Type PsLoggedon64.exe and press Enter.
7. The PsLoggedon License Agreement window will appear. Click Agree to continue.
8. The Command Prompt window will now display two results: Users Logged on locally (here, the local user is the Administrator of the local machine) and Users Logged on via resource shares (in this case, no user is logged on through resource shares; hence, the result displays null in the Users logged on via resource shares section)

9. Now, close the Command Prompt window and launch it with Administrator privileges by right clicking the Start button (Windows icon button) and then clicking on Command Prompt (Admin).
10. We will now run the net sessions command, which will list the IP addresses of all the connected sessions on the host machine (here, Windows Server), the command has listed the IP address of the Windows 10 virtual machine as shown in the following screenshot:

```
C:\Windows\system32>net sessions

Computer          User name          Client Type        Opens Idle time
-----
\\10.10.1.10      Administrator      0 00:02:21
The command completed successfully.
```

11. Select the LogonSessions Tool (Download from Internet or from the Shared folder)



12. The above operation will launch Command Prompt with the path of LogonSessions. Type logonsessions64.exe and press Enter.
13. The LogonSessions License Agreement window will appear. Click Agree to continue.
14. The utility will now list the currently active logon sessions.
15. To list the logon sessions, their types, and the processes running under them, use the -p switch in combination with logonsessions64.exe. All the running processes associated with each session will be displayed under the UPN section:
16. Close the Command Prompt.
17. Now, we will use the net file utility to retrieve information pertaining to all the open shared files with respect to Windows Server virtual machine.
18. To run the net file command, launch it by right clicking the Start button and then clicking Command Prompt (Admin). In the Command Prompt window, type net file and press Enter.

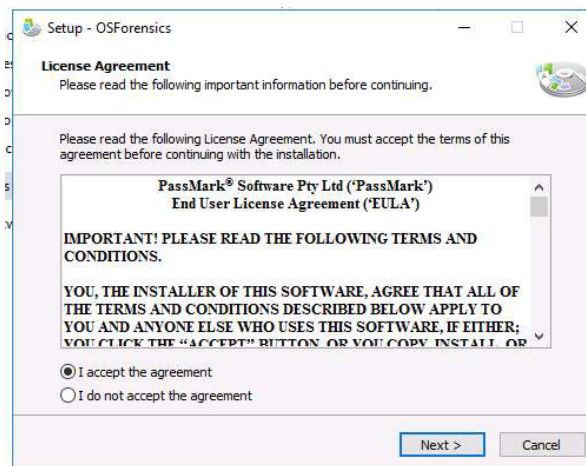
```
C:\Windows\system32>net file_
```

19. The net file command will now display the Path of the shared folder from the local machine which is accessed by other machines (here, Windows 10 virtual machine); it also displays the Username of the user account that is remotely accessing ANY folder along with the ID and Locks that are associated:
20. For further analysis, you can use NetworkOpenedFiles to obtain more information regarding the shared network folder/drive, such as IP Address, Host Name, and Permissions.
21. NetworkOpenedFiles is a utility for Windows that lists all the files that are currently open on the host machine (only those files that have been opened via remote login will be displayed). With the help of this tool, an investigator can identify suspicious files that are currently open on a host machine and have been opened via remote login.
22. Before running NetworkOpenedFiles, switch to Windows 10 virtual machine and navigate to our Shared Folder that you created in your Server machine earlier and paste the Infected.pdf file from our "SOAC Shared Folder". Open the file Infected.pdf.
23. Run NetworkOpenedFiles,
24. The NetworkOpenedFiles window appears, displaying the shared folders and files that have been accessed, along with information such as the IP Address of the computer on which they have been remotely opened, the User (name of the user account) accessing the folders and file(s), and the Host Name of the computer from which the listed folders and file(s) have been opened (in this case, the Host Name section would reflect Windows 10 virtual machine's name).
25. The tool displays the folders and Files and the file Infected.pdf because they have been opened remotely from another computer.
26. A Properties window will now open, displaying all the details pertaining to the file Infected.pdf.
27. For the demonstrative purpose of this lab, the suspicious file has been represented as Infected.pdf. In the real time, the suspicious file may bear any name. In this manner, you can also determine other files/folders that are currently open on the host machine.

Task 2: Discovering and Extracting Forensic Data from Computers

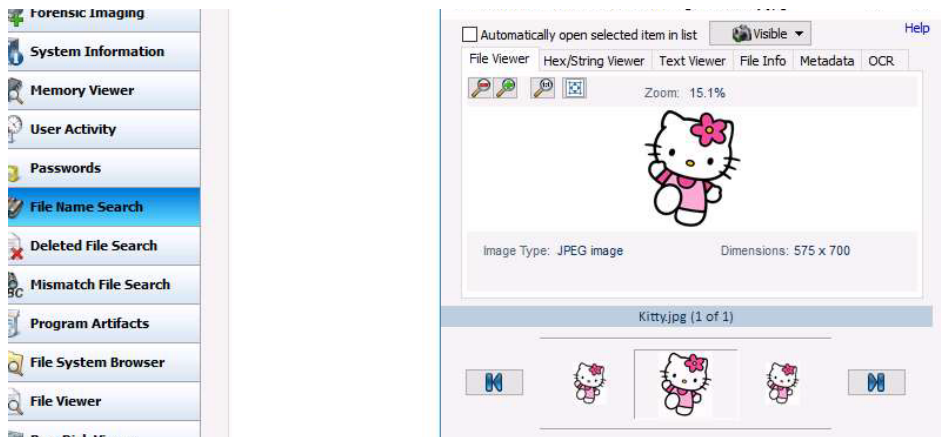
During forensic investigation, the investigator must identify any suspicious activity on the target system and extract evidence that could be useful for investigation. The objective of this lab is to help you learn how to investigate a suspect's computer to locate evidence for a crime.

1. Login to Server virtual machine
2. Navigate to our shared folder and search for OSForensics (Alternate: Download from Internet).
3. Launch the setup and follow the wizard-driven installation instructions to complete the installation of the tool.

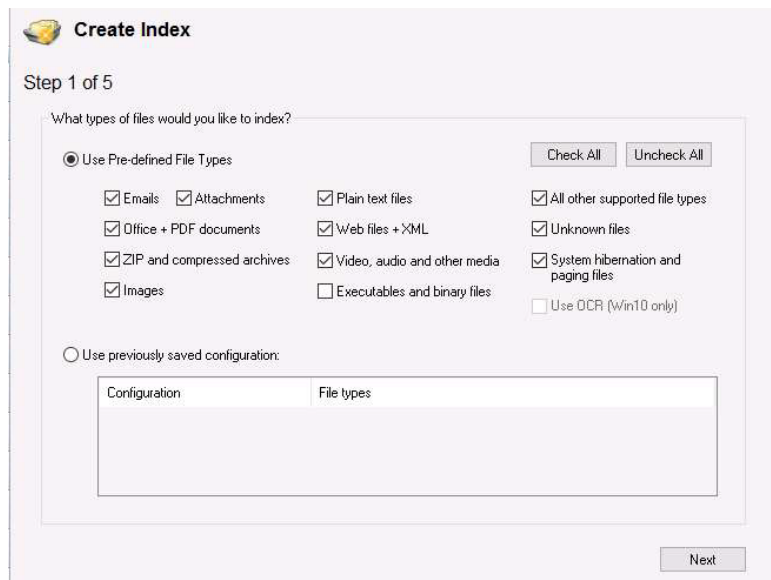


4. If an Open File - Security Warning pop-up appears, click Run.
5. OSForensics GUI appears, along with PassMark OSForensics pop-up. In the pop-up, click Continue Using Trial Version.
6. Our first task is to create a case using this tool. Click the Create Case icon in the tool's main window to create a new case.
7. A New Case window appears; fill out the required fields in the window. Ensure that you select the radio button for the Live Acquisition of Current Machine option in the Acquisition Type category. You may choose to save the new case folder either in Default or Custom locations. Click OK.
8. In this lab, we have set the default location for the case folder.
9. A new case is created:
10. The OSForensics tool can help investigators in searching and locating files on a system. To start searching for files, click File Name Search in the left pane of the window.

11. To locate files, type a file name or its extension in the Search String field under the File Name Search section. Alternatively, you may select the file type from the Presets drop-down list.
12. In this lab, we will be searching for image files. So, choose the Images option from the Presets drop-down list.
13. In the Start Folder field, specify the path to search for image files by clicking the ellipsis button and choosing the location (here, we are specifying the location of our shared folder. (Note that connecting to the soac network is not advisable. Hence, copy the Evidence File into your machine and choose that location) click the Search button.
14. The File Name Search section now displays the list of files contained in the selected location.
15. By default, the tool displays these files under the File Details tab. You may also view this list of files under the File List and Thumbnails tabs by clicking on them.
16. The Timeline tab allows you to view/sort files according to their modified, accessed, or created times.
17. Alternatively, if you wish to search only for a single image on the entire system, select Images from the Presets drop-down menu, enter the name of the desired image file in the Search String field, and then click Search, as shown in the screenshot below. Here, we are searching for the JPEG image file named Kitty.
18. The tool will search for the specified image file and display the search result in the File Name Search section under the File Details tab. The search result will be displayed along with the path/location where the searched file is stored.
19. To view the image, double-click it. The tool will display the image through a pop-up, as shown in the following screenshot:

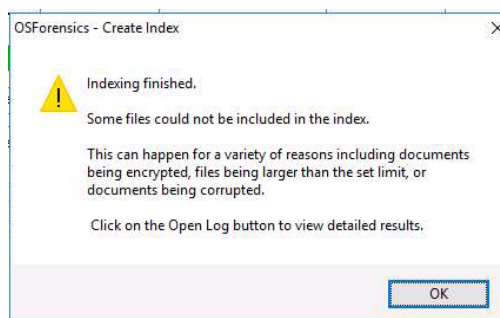


20. Similarly, the tool also allows you to search for all the image files that are present on a disk partition. For demonstrative purposes and to save time, we have confined our search operation mostly to the Image Files sub-folder within the Evidence Files folder.
21. We will now proceed to the task of creating an index of files. Here, we demonstrate the creation of an index for image files. Creating an index of files helps investigators expedite their file search.
22. To start creating an index of files, click Create Index in the left pane of the tool window.



23. The Create Index section appears in the right pane. In this section, select the Use Pre-defined File Types option for creating the index and check the required options listed under it for selecting the file types that you wish to index (here, we have selected the Images option). Then, click Next.
24. Now, click the Add button to select the target drive or folder in which the files which you wish to index are stored.

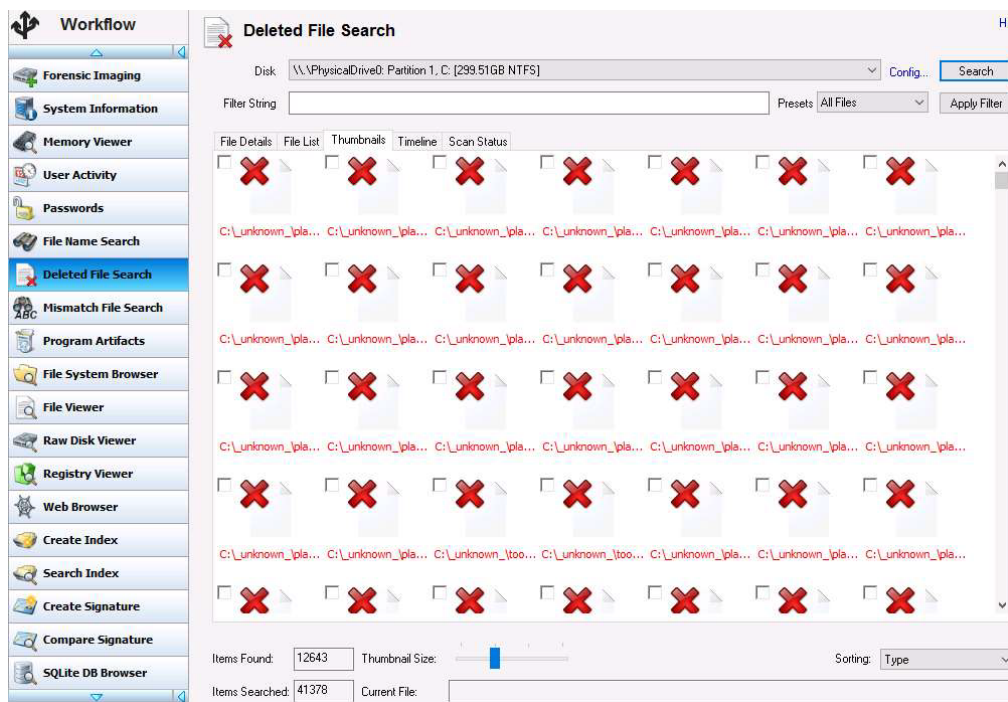
25. When you click the Add button, the Add Start Location pop-up appears. From this pop-up, select the Specific Folder radio button, and click the ellipsis button to provide the path to the target folder. For this lab, select folder where you copied your image/ evidence files and click the OK button.
26. The Start Folder is now configured. Click Next.
27. In the Step 3 of the wizard, select the Don't Know (Pre-Scan Required) option, ensure that the Use RAM drive for temporary files to speed up indexing option is checked, and click Next.
28. In Step 4 of the wizard, specify an Index Title, enter Index Notes (optional), and then click Start Indexing.
29. The application will now start performing a pre-scan on the specified folder.
30. If a Maximum page limit in Free Version dialog box appears while scanning, click OK to close it.



31. Once the indexing is completed, OSForensics - Create Index window appears, click OK. The application also changes the status of the indexing process to Finished, as can be seen in the Current Action field.
32. We will now search the indexed files. To search for the indexed files, select Search Index from the left pane of the tool window. The Search Index section now appears in the tool window. The index field at the top displays the name of the case we created. Click Search. The tool will load the image files that you have indexed under the Images tab.
33. The trial version of OSForensics returns a limited number of results. So, if the search results exceed this number, an OSForensics - Notice pop-up might appear, where you need to click OK.
34. Similarly, you can also index other files such as emails and search for them using the Search Index option. In that case, the indexed emails will be displayed under the Emails tab.

35. Now, we will gather all the user activities that occurred on the system.
36. Click User Activity in the left pane to scan for evidence such as browsed websites, USB drives, recent downloads, and wireless networks.
37. In this lab, we will scan for activities that took place in the C: drive. Select the Scan Drive radio button, ensure that the C: drive is selected from the Scan Drive drop-down menu, and then click Scan to scan for activities such as browsed websites, USB drives, recent downloads, and wireless networks in the drive.
38. If any Warning pop-ups appear, click Yes. If an OSForensics Error appears during the scan, click OK.
39. If a Select device to add window appears, click OK.
40. The application takes some time to scan, and upon completion of the scan, a User Activity - Summary window pops up, displaying a summary of information pertaining to user activity such as Browser History, Downloads, Most Recently Used, and Installed Programs. Click OK to close the User Activity – Summary.
41. If you wish to save any of the above user-activity information on your system, such as Browser History, then scroll down the items list in the left pane below the Scan Drive option and expand the Browser History node. Select the browser for which you wish to retrieve the history (Here, we are selecting Chrome). The browser history pertaining to this browser will be displayed in the right pane of the tool window.
42. To retrieve the entire browser history, select any one of the files in the right pane and right click it. From the context menu, click Export list of all results to, and from the resulting drop-down menu, click txt.
43. An Export List to... window will appear. Navigate to C:\Users\Administrator\Documents\PassMark\OSForensics\Cases\Case 75, name the file (here, we are naming it as Browsing History), and click Save to export the browsing history.
44. Since this is a trial version of the OSForensics tool, the number of items you can export to your system is limited. So, if the User Activity export limit in Trial Version pop-up appears, click OK to close it. If you wish to export all the files, you need to upgrade to the professional version of the tool.

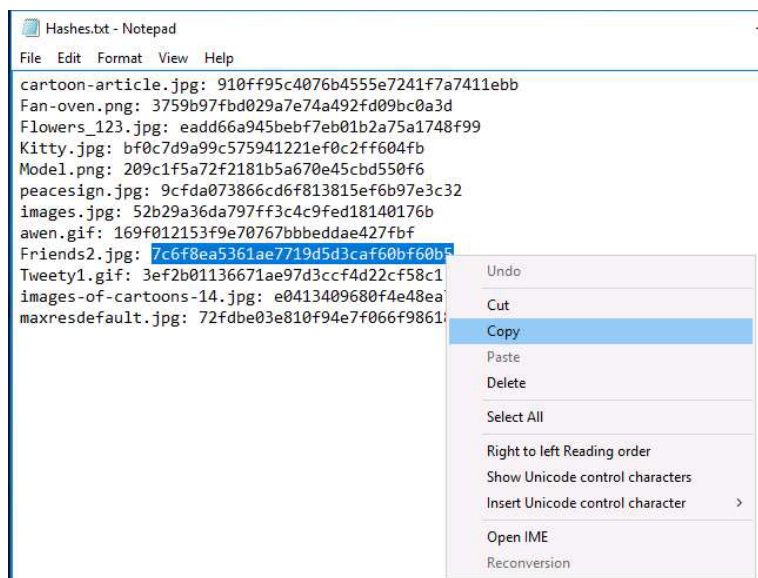
45. The history will be exported and saved to a text file. Navigate to the case folder and double-click the Browsing History file to view the information stored in it.
46. We will now examine how to recover deleted files using this tool.
47. To recover deleted files from the file system, click Deleted File Search in the left pane, select a disk on which you wish to perform the deleted file search from the Disk drop-down menu (here, we are choosing Partition 1, C:), and click the Search button.
48. The application will run a scan on the selected drive, retrieve the deleted files, and display them under the Thumbnails tab shown in the following screenshot:



49. Alternatively, you can view the retrieved files under the File Details tab or File List tab. Under the Scan Status tab, you will see all the details pertaining to the scan.
50. To save and view contents of the deleted files that have been retrieved by the tool, follow the same procedure as described in the above steps and name the file being exported as Recovered Deleted Files.
51. We will now detect files with an extension mismatch. For this, we will be using the Mismatch File Search feature. This feature is helpful in cases where an attacker has saved malicious files to a system by modifying their extensions.
52. To locate files having contents that do not match the file extensions, click Mismatch File Search in the left pane of the tool window. The tool will display the Mismatch File Search section in the right pane:

53. Click the Ellipsis button pertaining to the Start Folder field to provide the location in which files with extension mismatch are to be searched for. For this task, we will be searching for files with extension mismatch in the Image Files folder. So, provide the location of the Evidence Files and click the Search button.
54. The tool will scan the selected directory and display all the files with extension mismatch under the File Details tab by default. Click on the File List tab for the ease of viewing the files and their details:
55. We will now proceed to the task of viewing running processes on the system.
56. To view the processes running on the system, click Memory Viewer in the left pane of the tool window. The tool will now display the Memory Viewer section.
57. If an OSForensics – Warning pop-up appears, click OK.
58. Select a Process from the list of running processes, and then select the Memory Space tab to view the complete memory details of that process.
59. To view the process information pertaining to the selected file, click on the Process Info tab. The information pertaining to that process will be displayed
60. We will now proceed to the task of viewing system information.
61. To retrieve detailed information about the core components of the system, click System Information. The tool will display the System Information section.
62. From the List drop-down menu, select any of the options based on the type of information you wish to retrieve and then click Go. The options displayed in the list drop-down menu are Basic DOS Commands, Basic system information, System Information From Registry, BitLocker Detection, Recover BitLocker Keys, Python Scripts, and All commands.
63. Here, we select All Commands from the List drop-down menu. Ensure that the radio button against Live Acquisition of Current Machine option is selected and then click Go.
64. Since we have selected the All Commands option, upon clicking Go, the application will display all the commands that were executed on the system and their respective outputs under the Result 1 – All Commands (Live) tab
65. We will now proceed to the task of verifying the integrity of files by calculating their hash values.

66. To verify the integrity of files by calculating their hash values, click Verify/Create Hash from the left pane of the window. The Verify/Create Hash section will now appear in the window. Ensure that the File option is selected.
67. Click the Ellipsis button to specify a File to calculate its hash value. Here, we are specifying the file Friends2.jpg from the location of Evidence Files to calculate its hash value. From the Hash Function dropdown, select MD5, and from the Secondary Hash Function dropdown, select SHA1. Then, click Calculate.
68. The file's hash value appears in the Calculated Hash section in both the Primary Hash Function (MD5) as well as Secondary Hash Function (SHA-1) fields:
69. To verify the integrity of the Friends2.jpg file, we can input its pre-existing hash value in the Comparison Hash field. Navigate to Evidence Files and open the file Hashes.txt, which contains the pre-existing hashes of some of the image files. Copy the hash value for the Friends2.jpg file.



70. Now, paste the copied hash value of the Friends2.jpg file in the Comparison Hash field. You will see that a tick mark appears against the Comparison Hash field, which indicates that the pre-existing and calculated MD5 hash values of the selected file match with each other. This implies that the file's integrity is intact.
71. Conversely, if the file's integrity is not intact, the tool will generate a warning icon in the form of a cross mark, indicating that the file has been tampered with to act as a payload for an attack.

72. In this manner, you can perform investigation on a system or the folders and partitions within the system to gather data of interest to the forensic investigation.

73. Close all open windows.

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 in Windows Forensics Technique.
3. Rate yourself: Understanding on Windows Forensics, its tools and analysis

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