ABSTRACT

Forensic analysis is the process of searching for evidence and preserving it for further examination. Examination of the evidence provides important information about suspect’s behavior which plays crucial role in legal proceedings. This field has gained great attention as there is a noticeable increase in cyber-crime and usage of computers by the suspects. With the importance it has gained lately, the number of users keen on learning computer forensics has increased exponentially. Hence, provision of an environment where in users interested could practice investigations, would be helpful for them in learning the techniques and gaining basic knowledge about carrying forensic investigation.

Many tools are available online for the users that are helpful in conducting forensic investigations. In this research, a comprehensive virtual environment is proposed with some installed open source tools alongside step by step instructions for carrying investigations is provided. This toolkit reduces the user’s effort for installing virtual environment in their workstation as well provides supportive material for conducting basic forensic investigations in that environment.
# TABLE OF CONTENTS

Abstract .................................................................................................................................................. ii

Table of contents ................................................................................................................................... iii

List of figures .......................................................................................................................................... iv

1. Introduction ...................................................................................................................................... 1
   1.1 Digital forensics .......................................................................................................................... 1
      1.1.1 Computer forensics ............................................................................................................. 1
      1.1.2 Network forensics ............................................................................................................ 1
   1.2 Virtual machines ....................................................................................................................... 2
      1.2.1 Uses of virtual machines ................................................................................................. 2

2. Narrative ......................................................................................................................................... 3
   2.1 Problem statement ..................................................................................................................... 3
   2.2 Scope ......................................................................................................................................... 4
   2.3 Benefits of this project .............................................................................................................. 4

3. Proposed system design .................................................................................................................. 5
   3.1 Framework ............................................................................................................................... 5
      3.1.1 Procedure .......................................................................................................................... 5
      3.1.2 System requirements ....................................................................................................... 6
   3.2 Mechanism .................................................................................................................................. 6

4. Implementation .................................................................................................................................. 7
   4.1 Partition Analysis ...................................................................................................................... 7
   4.2 Data Recovery ........................................................................................................................... 16
4.3 Network forensics ......................................................... 25
4.4 File system analysis ..................................................... 45
4.5 Capturing an image ...................................................... 64
4.6 Hash values ............................................................... 65
4.7 Editing using Hex Workshop .......................................... 67
4.8 Graphic images .......................................................... 69
4.9 Web forensics ............................................................. 70
4.10 Email forensics .......................................................... 71
4.11 Data operations .......................................................... 72
4.12 Metadata ................................................................. 73
4.13 Data carving .............................................................. 73
4.14 Volatility ................................................................. 75
5. Testing and evaluation ..................................................... 76
  5.1 Testing on different platforms ....................................... 76
  5.2 Testing different open source tools ................................. 78
  5.3 Testing on different products ....................................... 79
6. Conclusion ....................................................................... 81
Bibliography and references .................................................. 82
LIST OF FIGURES

Figure. 1: Architecture of proposed model .................................................................6
Figure. 2: Opening the testdisk ....................................................................................7
Figure. 3: Displaying testdisk.txt ................................................................................8
Figure. 4: Selecting the disk drive .................................................................................9
Figure. 5: Selecting the partition table type ...............................................................9
Figure. 6: Options to work on partition tables ..........................................................10
Figure. 7: Result obtained after analyzing partition table .........................................11
Figure. 8:Confirmation screen ..................................................................................12
Figure. 9: Result obtained after quick search ............................................................12
Figure. 10: Options to search or write .......................................................................13
Figure. 11: Result of deeper search .............................................................................13
Figure. 12: List of files in NTFS directory ................................................................14
Figure. 13: Result displays any logical tables are obtained by deeper search ..........14
Figure. 14: Confirmation for writing ...........................................................................15
Figure. 15: Confirmation for making changes permanent ...........................................15
Figure. 16: Initializing the PhotoRec ..........................................................................16
Figure. 17: Selecting the appropriate partition .........................................................17
Figure. 18: Options in “Options” tab ........................................................................18
Figure. 19: Options in “File Opt” tab ........................................................................19
Figure. 20: Marking the txt file type .........................................................................20
Figure. 21: Saving the settings ...................................................................................20
Figure. 22: Selecting the appropriate partition and clicking search option ............21
Figure. 23. Selecting the appropriate file type .......................................................... 21
Figure. 24. Choosing the space to be analyzed .......................................................... 22
Figure. 25. Choosing the destination directory .......................................................... 23
Figure. 26. Recovering the lost files ........................................................................... 23
Figure. 27. Retrieved file ............................................................................................ 24
Figure. 28: Initializing wireshark program ................................................................. 25
Figure. 29: Starting the capture operation ................................................................. 26
Figure. 30: Interfaces displayed .................................................................................. 26
Figure. 31: Options in the interface ............................................................................ 27
Figure. 32: Traffic captured in wireshark ................................................................. 27
Figure. 33: Saving the captured traffic ....................................................................... 28
Figure. 34: Observing the summary of the traffic ..................................................... 29
Figure. 35: Displaying summary ................................................................................ 29
Figure. 36: Result displayed with http filter ............................................................. 31
Figure. 37: Summary displayed with http filter ......................................................... 32
Figure. 38: Selecting the filter ................................................................................... 33
Figure. 39: Filtered traffic ......................................................................................... 33
Figure. 40: Setting another filter ............................................................................... 34
Figure. 41: Traffic displayed after setting filters ....................................................... 34
Figure. 42: Traffic displayed after changing the filters ............................................. 35
Figure. 43: Saving the filtered traffic ......................................................................... 36
Figure. 44: Information about the black packet ....................................................... 36
Figure. 45: Options displayed after right-click ......................................................... 37
Figure 46: Traffic with additional column ........................................................................ 37
Figure 47: Options displayed after clicking on analyze .................................................... 38
Figure 48: Tab with expert information displayed .............................................................. 38
Figure 49: Expanding the malformed packets ................................................................. 39
Figure 50: Options displayed for analyzing http traffic .................................................... 40
Figure 51: Tab with http load distribution ....................................................................... 41
Figure 52: Tab with http packet counter ......................................................................... 41
Figure 53: Expanded Packet counter ................................................................................ 42
Figure 54: http requests displayed .................................................................................. 43
Figure 55: Options displayed after right clicking on a packet .......................................... 43
Figure 56: Result of following TCP stream .................................................................... 44
Figure 57. Initializing autopsy .......................................................................................... 45
Figure 58. Opening autopsy in Browser .......................................................................... 46
Figure 59. Creating a new case ....................................................................................... 46
Figure 60. Prompt for adding host .................................................................................. 47
Figure 61. Adding a new host ......................................................................................... 48
Figure 62. Prompt for adding image ................................................................................. 48
Figure 63. Displaying different options available after creating case and adding host ... 49
Figure 64. Adding a new image] ..................................................................................... 49
Figure 65. Confirmation after adding an image ............................................................... 51
Figure 66. Image and File system details ....................................................................... 51
Figure 67. Calculating MD5 ............................................................................................ 52
Figure 68. Options in Host Manager .............................................................................. 53
Figure. 69. Starting the Analyze operation ................................................................. 53
Figure. 70. Searching by the directory name ................................................................. 54
Figure. 71. Searching the file name .............................................................................. 55
Figure. 72. Retrieving all deleted files ........................................................................ 55
Figure. 73. Expanding directories .............................................................................. 56
Figure. 74. Searching by keyword .............................................................................. 57
Figure. 75. Results for keyword search ....................................................................... 57
Figure. 76. Starting the sorting operation ................................................................... 58
Figure. 77. Settings for sorting files ............................................................................ 59
Figure. 78. Path of the index file in which sorted files list is saved .............................. 59
Figure. 79. Opening the Index file .............................................................................. 60
Figure. 80. General file system details ....................................................................... 60
Figure. 81. Searching the data by MFT entry ............................................................... 61
Figure. 82. Displaying status of MFT entries ............................................................... 61
Figure. 83. Searching data by cluster number ............................................................. 62
Figure. 84. Displaying status of cluster entries ............................................................ 62
Figure. 85. Closing the case ....................................................................................... 63
Figure. 86. Validating the image after performing operations ...................................... 63
Figure. 87. Result of validation test ............................................................................. 64
Figure. 88: OVA file importation successfully tested in Mac OS X lion ...................... 76
Figure. 89: OVA file importation successfully tested in Windows 7 ......................... 77
Figure. 90: OVA file importation successfully tested in Linux Ubuntu ..................... 77
Figure. 91: OVA file successfully tested on Oracle VM Virtualbox ............................ 79
Figure 92: .OVA file successfully tested on VMware
1. INTRODUCTION

Forensic science has several branches of which Digital forensics is one that could be prioritized. With the increase in usage of digital media by the suspects, this field became an interesting topic of research.

1.1 Digital Forensics

Forensic investigations performed on digital sources have gained much importance in the technically advanced world. With the observable increase in crimes using digital sources, this field has emerged as an interesting topic for research. Forensics is a process in which evidence is identified, preserved, analyzed and presented from a source. The ‘source’ can be any digital tool available. Data analyzed about the source is used as evidence in legal proceedings.

1.1.1 Computer forensics

It is branch of digital forensics in which computers are used as source. Investigations are performed on computers which are used by organizations or individuals for information transfer. Computer forensics can be defined as a process of collecting and analyzing data that is stored on a computer which is assumed as suspects computer.

1.1.2 Network forensics

It is a branch of digital forensics in which computers are used as source and investigation is performed on the network. Lately, every computer, either used by a single user or by an organization, is connected to one or the other type of network. Many hacking tools are available which could be used by suspects for committing serious crimes or petty crimes like hacking simple passwords. These crimes can be investigated by carefully observing the network traffic. Capturing network traffic and analyzing captured packets is the primary technique for performing forensic investigation over networks.
1.2 Virtual machines

Virtual machine can be defined as a machine with some resources allocated on the host computer that supports the running of guest operating system on a workstation. This technique hence helps users in operating another computer completely on users system. Hardware and software resources are allocated virtually for running a guest operating system. There are two types of virtual machines; firstly a virtual machine which supports an entire operating system, secondly a virtual machine which is designed for running one process or program. Virtual machine operation does not directly affect the host system.

1.2.1 Uses of virtual machines

There are many uses with the virtual machines.

- For installing or testing new operating systems this is the best option to opt for as new operating systems are usually tough to get used to. Hence, usage of virtual machine would help user in familiarizing with the new operating system. This gives the user to choose whether or not to install the operating system permanently on the workstation.

- For testing new software’s also, virtual machines could be the savior. If a user has lot of sensitive information on the system, usage of some new unknown software’s could cause a threat to the information. To avoid this using virtual machine helps.

- Also, servers can be maintained on a virtual machine. This could reduce the user’s effort of maintaining two different systems.

- Legacy systems can also be installed on the virtual machines. Legacy systems are usually needed for using certain software’s that need support of legacy systems for execution. In organizations with high magnitude, virtual machines could be very useful as several guest operating systems can all be used on one workstation.
2. NARRATIVE

2.1 Problem statement

Forensic investigations are usually performed in controlled environments. For performing or practicing forensic operations, the necessity for a computer that is not in regular use raises. Usually, a computer of this sort is suggestible as some of the operations performed in these investigations might affect the data on the workstation. Some of the operations might result in modification of data or even loss of data completely. Certain operations might change the registry data, modify data in memory, modify log information or even change partitions. Environment in which forensics operations can be freely performed without actually affecting the system data is not freely available for users.

Many forensic tools that are commercial or open source are available. Performing operations on many such tools is usually confusing and time taking. Instructions for the usage of specific tools would be complicated. Though ‘Read me’ files or ‘Instructions of usage’ are made available by the developers, these could be of help partially sometimes but consume time for understanding. Also, some tools consume time to research about their installation.

Performing operations initially on any tool is difficult as users tend to have very little knowledge about the functionality of the tool. Developers provide instructions for performing operations but theoretical information might sometimes fail in providing clear solutions for issues that might come up while operating in run time. Hence, many problems might be observed by users while performing basic forensic investigations. Step by step instructions will not be given by most of the tool developers. Detailed instructions of usage would help users in gaining an idea about the tool which could eventually be of help in working on the tool and performing complicated operations.
2.2 Scope

The scope of this project is observably high. Several open source tools are available online. Open source tools can be developed by any user registered for developing the tool. Hence, these tools can be downloaded and can be developed further. Therefore, providing basic instructions for running these tools and making them available for users would help them in understanding the tool. This would eventually lead to the expansion of the tool by developing new modules with greater understanding of the tool by the users.

2.3 Benefits of this project

This project helps in installing virtual machine on a system without much installation procedure. Time required and steps required would be very less. Image installed in the virtual machine will have all the previous installed software’s. So this importation of a virtual machine can be considered as mobile carrying a complete system by the user in disc. Hence, the need for installing software’s would be greatly reduced as well saves lot of time.

This projects main motto is to provide users with a clear material for performing basic operations using different forensic tools. This material would be of great help to first time users. This material can be used as training material in academia for having students work on these forensics tools without much installation procedures.
3. PROPOSED SYSTEM DESIGN

3.1 Framework

This project helps in understanding some forensic tools and their operations. A virtual environment is provided for working on those tools. This virtual environment helps in avoiding any problems that could be possible with the forensic tools. While performing operations, data could be deleted, log files could be modified and partitions could be changed. Virtual environment therefore provides the flexibility to work with the tools in any way the user wants. Material provided could be helpful for users to perform basic forensic investigations. An image of Windows XP with the forensic tools installed is provided. ‘Instructions to follow’ and software’s are also provided.

3.1.1 Procedure

Following are the steps followed in designing the project.

Step 1: Virtualbox software is installed and windows xp image is installed.

Step 2: Many open source tools are tested and some of them are selected and installed.

Step 3: Instructions for operating those tools are noted and saved.

Step 4: Open Virtual Appliance (.OVA) file is created from that XP image using virtual box options.

Step 5: A disc with the virtualbox software for installing in windows, mac and linux is provided and .OVA file is included.

Step 6: Virtualbox software is installed in any system and the .OVA file from the disc is imported to the virtualbox. Image will be created for the user in that system with all the installed tools.
3.1.2 System requirements

Any system that is able to install virtualbox or vmware work station with 10 GB free space of hard disk and 1 GB RAM will be able to create an image of windows XP and will allow users to work on forensic tools installed in it.

3.2 Mechanism

Open Virtual Appliance (.OVA) files are helpful in portability of virtual machines. This OVA file helps in importing a virtual machine from one system to another. A virtual machine created on a system with certain specifications and installations can be exported to an .OVA file. This .OVA file could be used for importing the virtual machine with same specifications, provided all the requirements are satisfied. When double clicked or imported by any virtual machine software, files needed for running a virtual machine are extracted and are associated to the virtual machine software by default. Once after completion of extracting or importing, the .OVA file can be deleted. This is because it extracts and saves all the required files into the virtual machines documents.

![Figure 1. Architecture of proposed model](image-url)
4. IMPLEMENTATION

This project consists of fourteen modules. These modules concentrate on the major forensic investigations done on a suspect’s computer. These modules are selected after extensive research in forensic discussion forums and cases solved.

4.1 Partition analysis

Objective: Retrieving any missing partition using Testdisk

Tool description: It is a tool developed for recovering lost partitions or corrupted partitions. Many operations such as recovering and rebuilding sectors can also be done using this tool.

Step 1: Double click on “shortcut to testdisk_win” located in the “Lab 1 – Partition analysis” folder. In the terminal three options will be displayed as shown in Figure 2.

![Figure 2. Opening the testdisk](image)

“Create” option is for creating a log file named “testdisk.txt”. This log file will be saved in the “testdisk-6.14-WIP” folder. This log file has details about technical features of that system.
“Append” option helps in appending information to the log file. This allows user to add information about different partition to the log file.

“No log” option helps in proceeding without recording any log files. When a disk with read-only option is analyzed this option would be useful.

**Figure. 3.** Displaying testdisk.txt

**Step 2:** Figure 3 displays the “testdisk.txt” file which is created by clicking on “create” option.

After selecting any of the three options and clicking on enter would lead to another screen where different partitions available in the system are displayed as shown in figure 4.
Step 3: Select any one of the displayed partition. If the size of the selected partition is incorrect then the partition can be assumed as corrupt. Select the corrupted partition. Here in this case there is no available corrupted partition. Click on proceed.
**Step 4:** Testdisk checks for the table type and by default highlights it as shown in figure 5. Here the Intel partition table is detected so Intel option is highlighted. Click on enter.

![Testdisk screenshot](image)

**Figure. 6.** Options to work on partition tables

**Step 5:** In the figure 6 there are many options available for the users to select.

“Analyse” – This option analyses the BIOS or OS and retrieves the features. Here the partition table is compared with retrieved characteristics. If any errors are observed testdisk tries to repair them. If no partition table is available then new table is created. When this option is selected partition checks, file system checks and recovery operations are done.

“Advanced” – This option helps in checking with the repairs of NTFS, FAT and ext2/ext3 file systems. This option helps in undeleting files from NTFS, FAT and ext2.

“Geometry” – This option helps in changing disk geometry of the system. Any modifications can be done to the Cylinders, heads and sectors.

“Options” – This option helps in aligning cylinder boundaries and dumping sectors.
“MBR Code” – This option helps in writing the testdisk MBR code to first sector. This helps in repairing the booting. Here overwriting the code to first sector will be done which repairs the code area for booting thus helping in avoiding problems in booting if any.

“Delete” – This option helps in deleting all data from the partition except the MBR code and signature bytes.

![Figure 7: Result obtained after analyzing partition table](image)

**Figure. 7.** Result obtained after analyzing partition table

**Step 6**: Figure 7 is obtained after selecting analyze option.

Here the partitions are listed with some information. In the above screen there are no errors but there might be chance for errors such as “INVALID PARTITION” and repetition of same partition twice.

Here two options will be available.
“Quick search” – This option helps in locating the partitions.

“Backup” – This option helps in creating a backup log file.

**Figure. 8. Confirmation screen**

**Step 7:** Figure 8 displays the confirmation screen. Answer according to the specifications of the computer.

**Figure. 9. Result obtained after quick search**
**Step 8:** Figure 9 shows the result obtained. Here by using the left/right keys bootable characteristic of the partition can be changed. Click on enter to continue.

![Figure 9](image1.png)

**Figure. 10.** Options to search or write

**Step 9:** Figure 10 shows options available to perform. Deeper search helps in locating missing partitions in a deeper manner. Write option helps in saving the partition structure. Click on deeper search.

![Figure 10](image2.png)

**Figure. 11.** Result of deeper search

![Figure 11](image3.png)
**Step 10:** It takes few minutes for analyzing the cylinder which is shown in figure 11. After the completion of analyzing enter ‘p’ to list the files. Figure 12 shows the list of files.

![Image](image1.png)

**Figure. 12.** List of files in NTFS directory

**Step 11:** Enter ‘q’ to quit.

![Image](image2.png)

**Figure. 13.** Result displays any logical tables are obtained by deeper search
Step 12: If there are any new partitions located after the deeper search a write operation can be performed so that the new information can be updated. Clicking on write option which can be observed in figure 13 would lead to figure 14 which ask for confirmation.

![Figure 14. Confirmation for writing](image)

![Figure 15. Confirmation for making changes permanent](image)

Step 13: Figure 15 shows the confirmation screen. Confirming yes would ask user to reboot the system. Rebooting the system would make changes to the partition table permanently.
4.2 Data Recovery

**Objective:** Recovering deleted data from USB drive

**Tool description:** This is a file recovery tool.

**Steps to follow**

**Step 1:** Connect a Flash drive to the computer. For the flash drive to be recognized by the virtual machine, click on “Devices and the USB devices” and select the appropriate device.

**Step 2:** Create a text file with name “2012” in the USB drive.

**Step 3:** Delete the “2012” text file.

**Step 4:** Click on “photorec_win” icon located in “Lab 2 – Data Recovery” and start the operation.

![Figure. 16. Initializing the PhotoRec](image)

**Step 6:** A terminal as shown in the figure 16 will be opened which displays all recognized media connected to the Virtual machine. From the displayed media, select the USB device by using arrow keys. Click on “Proceed” for moving to the next step or click on “Quit” to quit the session.
A note is displayed in the terminal which warns the user to cross check the size of the disk from which the data is to be recovered. If the size displayed of any available media is incorrect, it indicates that the device is corrupted.

**Figure. 17.** Selecting the appropriate partition

**Step 7:** Selecting the USB device and clicking on “Proceed” displays the screen shown in the above figure. Select the appropriate partition from displayed partitions.

As shown in the figure 17 different options are provided for different functionality. Brief description about each option is given.

- **Search:** Selecting this option would start up the process of recovering the lost files.

- **Option:** Selecting this option would display the status of some features which can be modified.

- **Paranoid feature:** This feature will be ‘on’ by default and will have “Brute force disabled”. This feature can be turned off as well the Brute force option can be enabled or disabled.
This paranoid feature helps in verifying the recovered files. If a file is found invalid it simply ignores the file. Enabling the Brute force feature would help in having deeper search about lost files. This would take much time. This option will be used for recovering files when disabled brute force feature do not yield good results.

*Keep corrupted files:* This option will be “no” by default which could be changed to “yes”. Enabling this option would help in keeping recovered corrupt files without ignoring.

*Expert mode:* This option is used by the investigators in performing complex recovery using partitions. Enabling this option helps experts in choosing the size and the offset.

*Low memory:* Recovery with less memory is achieved by enabling this option. This option helps workstations with less memory.

![Figure. 18. Options in “Options” tab.](image)

**File Opt:** Selecting this option helps in choosing the file types the user wants to recover. PhotRec supports many file types which can be observed by scrolling down. If a user wants to recover only specific type of files, this option would be helpful.
**Figure. 19.** Options in “File Opt” tab.

**Quit:** Selecting this option would redirect to the screen where media for recovering files can be chosen.

**Step 8:** Click on “File Opt”. List of file types are displayed as shown in figure 19. Tap “s” for disabling all file types. Here, text files are needed for recovery, hence scroll down till file extension “txt” is found, which is shown in figure 20 and then hit right arrow which marks the “txt” file type.
Figure. 20. Marking the txt file type

Tap “b” for saving the file settings. This would lead to figure 21.

Figure. 21. Saving the settings
Step 9: Click on “Ok” and then click on “Quit”. Select the appropriate partition from the displayed options which are shown in figure 22 and click “Search”.

![Figure 22. Selecting the appropriate partition and clicking search option](image)

Step 10: Select the file system type from the displayed options which are shown in figure 23. In PhotoRec the two file system types are listed “ext2/ext3” and “other”. Select the appropriate one and hit “enter”.

![Figure 23. Selecting the appropriate file type](image)
Step 11: Two options will be displayed as shown in figure 24. These options allow users to choose the space to be analyzed. Clicking on “Free” space would analyze only the deleted or lost files. Clicking on “whole” would analyze all the files including the deleted files and files which are currently on USB drive.

Here click on “Free” since the file required is deleted.

Figure. 24. Choosing the space to be analyzed
Step 11: As shown in the figure 25, the directory where the recovered files are to be saved can be chose. Clicking on arrows changes the directory. After selecting the directory, click “c”, this confirms the destination.

Figure. 25. Choosing the destination directory

Figure. 26. Recovering the lost files.
Step 12: Analyzing and recovering file takes some time, figure 26 shows the process of recovering files. A directory named “recup_dir.1” will be created in the destination folder, in which the recovered files are saved, which is shown in figure 27. For each recovery different directory is created.

Figure. 27. Retrieved file

This is the process for recovering a deleted/lost file from USB. This mechanism can be implemented on any drive.
4.3 Network forensics

**Objective:** Performing basic network forensics using wireshark

**Tool description:** This tool is popular traffic capturing software for analyzing traffic. Many operations can be performed on the captured traffic.

**Capturing a session**

Double click on the “wireshark” icon located in “Lab 3 – Network forensics” to start the Wireshark. A wireshark window as shown in figure 28 will be opened.

![Figure 28. Initializing wireshark program](image)

Click on capture option shown in figure 29 and select interfaces from the displayed options which are shown in figure 30.
Click on options which are displayed, these options are shown in figure 31 and verify if capture is promiscuous mode is checked or not. After checking it click on start.
Figure. 31. Options in the interface

Go to internet explorer and open any website. One can observe some traffic captured in Wireshark as shown in figure 32.

Figure. 32. Traffic captured in Wireshark
Go to capture and click on stop. Later go to File and click on Save as and save the file with name “firstoutput”. This operation can be observed in figure 33.

Figure. 33. Saving the captured traffic

This is how a session is captured using wireshark.

Analyzing a session

For analyzing the session which is captured double click on firstoutput file or go to file and click on open and browse for the firstoutput file.

For finding the summary of the session go to statistics and click on summary. This operation can be observed figure 34.
Figure. 34. Observing the summary of the traffic

New tab will be opened after clicking on summary, as shown in figure 35.

Figure. 35. Displaying summary
From the summary tab many details about the captured session can be known.

In the summary under section File user can observe general information about the session such as name and length of the captured session, packet size limit etc.

Under the section Time, one can observe the timestamp when the first packet was sent and the timestamp when the last packet was sent. And also time elapsed for the session is displayed.

Under the section Display, one can observe if any display filters are used. Here in our case no display filter is used.

In the bottom of the summary tab one can observe some important information that could help forensic investigators in knowing the network functioning.

One can observe total bytes that are transferred during the session and the average transfer rate. This could help investigators in finding any network delays or anomalies.
Preparing a display filter

Display filters help in ignoring all information other than what is required. These display filters help investigators to deal with the information they wanted and investigate what happened in the transaction.

There are many redefined filters which can be used. In the Figure 36 http filter is used.

![Figure 36: Result displayed with http filter](image)

Clicking on the statistics and summary would give summary about the session filtered with filter used by the user.
In the Figure 37, user can observe under section Display, http is named as display filter. One can observe difference between captured packets and displayed packets and also the sizes transferred.

In some cases investigators are interested in knowing the transaction only between specified source and destination addresses. In that case a filter can be build.

Here in our session two ip addresses are considered. Right click on the ip address to build the filter with and select prepare a filter and click on selected. This operation can be observed in figure 38.
Figure. 38. Selecting the filter

Figure. 39. Filtered traffic

In the Figure 39 since the IP address was selected from source the filter considered it as ip.src. This can be modified.
Now right click on other IP address to analyze the traffic.

**Figure. 40.** Setting another filter

Instead of selecting the “selected” from the list select the “…and selected”. This option can be observed in figure 40.

**Figure. 41.** Traffic displayed after setting filters
In the Figure 41 filter is developed between 10.2.xx as source and 74.125.xx as destination. To get the requests and responses the filter has to be modified as ip.src to ip.addr and ip.dst to ip.addr.

**Figure. 42.** Traffic displayed after changing the filters

This filter can be saved following the same steps followed in capturing the session. Go to file click on save as and save it as filter1. Important thing is to select “Displayed” while saving the file. If captured is selected then whole session will be saved which is unnecessary.
After saving the filtered session user have to save the filter applied for documentation purpose. This is how a customized filter is built. This operation is shown in figure 43.

Black packets displayed signify bad traffic, one of the black packets can be observed in figure 44. Selecting on the black packet and expand the [SEQ/ACK analysis] would give more detailed information about the packet.

Figure. 43. Saving the filtered traffic

Figure. 44. Information about the black packet
Customizing columns

Wireshark can be customized for displaying the columns that will make investigation easier.

Figure 45. Options displayed after right-click

Expand any of the protocols and right click on the information as shown in the figure 45 to display in the column and click on “Apply as column”. In the Figure 45 “destination port” is selected and is being applied as column.

Figure 46. Traffic with additional column
Expert Info Composite

This gives expert information about the traffic.

Import any captured session and click on analyze and then click on Expert info composite. This operation is shown in figure 47.

Figure. 47. Options displayed after clicking on analyze

Figure. 48. Tab with expert information displayed
This expert info composite, helps in knowing what kind of traffic investigators are dealing with.

In the figure 48, there is a malformed packet which is a GIF image.

![Figure 48: Malformed Packet with GIF Image](image)

**Figure. 49.** Expanding the malformed packets

Similarly, there are warnings tab, notes tab, chats tab and details tab, which can be observed in figure 49. These tabs are very important for an investigator to carry on the investigation.

If there is anything wrong with the network warnings help in detecting that.

Notes tab helps in getting detailed information about some of the transactions happened.

Chats tab gives the information about the conversation happened between the servers and the clients.

Details tab gives information about all the transactions.
Analyzing http traffic

Most of the secure transactions happen with http. There are some options developed for observing the traffic with http protocol. Open any captured session and click on statistics and select http, as shown in figure 50, which gives the user three options load distribution, packet counter and requests.

Figure. 50. Options displayed for analyzing http traffic
Click on load distribution and click on create stat

![Figure 51. Tab with http load distribution](image)

It displays the http requests sent and http responses received, which can be observed in figure 51.

Now close the load distribution and select the packet counter as shown in figure 52.

![Figure 52. Tab with http packet counter](image)
Expanding the HTTP request packets and HTTP response packets gives some more information.

**Figure. 53.** Expanded Packet counter

As displayed in the figure 53 there are 24 HTTP GET request packets, 19 HTTP SUCCESS Response packets and 5 HTTP REDIRECTED response packets.

Now close the packet counter and go to Requests.
This gives information about the requests sent by the client to different servers with some detailed information, which can be observed in figure 54. One important function provided by Wireshark is to follow the TCP stream. Right click on any packet and select follow TCP stream.

Figure. 54. http requests displayed

Figure. 55. Options displayed after right clicking on a packet
**Figure. 56.** Result of following TCP stream

By selecting options from dropdown list in the bottom, the user can see the request form client to server and response from server to client, this can be observed in figure 56. This Follow TCP stream could help bad people in stealing passwords from insecure websites.
4.4 File System Analysis

Objective: Analyzing a sample file system

Tool description: Sleuth kit is a Linux tool which supports analyzing file systems. Autopsy supports sleuth kit in providing Graphical User Interface.

Step 1: Open folder “Lab 4 – File System Analysis” and double click on “cygwin terminal”. Change the directory to “autopsy” using the following command “cd /usr/local/autopsy-2.24”. After entering the directory, enter the following command “./autopsy”, this initializes the autopsy forensic browser, which can be observed in figure 57.

![Figure 57. Initializing autopsy](image)

Step 2: Copy and paste the displayed URL “http://localhost:9999/autopsy” in Internet explorer. This opens up Autopsy Forensic Browser 2.24 in Internet explorer, which is shown in figure 58.
Step 3: For opening an existing case, “Open Case” option can be used. A case which is in progress can be saved and can be opened using this option.

Here operation is working on a new case so click on “New Case”.

Figure. 58. Opening autopsy in Browser

Figure. 59. Creating a new case
**Step 4:** Fill out the details in appropriate blank spaces shown in figure 59 and click on “New Case”, which creates a new case. An investigation can have many investigators, thus many blanks are made available under the option of ‘Investigator names’.

![Figure. 60. Prompt for adding host](image)

**Step 5:** From the dropdown box shown in figure 60, select the name of the current investigator. For adding a host, click on “Add Host”.
Figure. 61. Adding a new host

**Step 6:** Fill out the information in the blanks which are shown in figure 61. Here, Additional options for Time are provided. Time zone can be selected and adjustment can be made. After filling out the information, click on “Add host”.

Figure. 62. Prompt for adding image
Step 7: Proceed for adding image by clicking on “Add Image”, which can be observed in figure 62. This is the image on which analysis will be done for finding any evidence.

Figure. 63. Displaying different options available after creating case and adding host

Step 8: Several options will be displayed as shown in figure 63. Click on “Add Image File”.

Figure. 64. Adding a new image
**Step 9:** Enter the path where the image is stored.

Here, in this lab, “/usr/local/8-jpeg-search/8-jpeg-search/8-jpeg-search.dd” is the path where the image is stored. More of these images can be found at “http://dftt.sourceforge.net/”.

Since this image is a partition, click on “Partition”.

For performing analyze operation on any image, it has to be imported to a directory specified during the installation. Import method has three options to import the image to the directory.

**Symlink:** Symlink is the Symbolic Link which refers to the address location where the image is stored.

**Copy:** Selecting this option copies the image from the original location and creates a copy in the evidence folder.

**Move:** Selecting this option moves the image from the source directory to the destination directory.

When moving or copying the file is not needed, so select Symlink from the given options and click on “Next”.
Step 10: If the provided path is correct, then the Confirmation message will be displayed as shown in figure 65. If not, provided path might be incorrect. Click on “Next” to confirm the image provided is correct and to proceed.

Figure. 65. Confirmation after adding an image

Figure. 66. Image and File system details
Step 11: Options are provided for protecting the Data Integrity of the image. A hash value calculated can be useful in verifying if the integrity of the image is protected or not i.e. any changes are made to the image or not.

Select the option for “calculating the hash value for this image”.

In the file system details, autopsy by default identifies the Mount Point and File System Type. If identified information is incorrect, then user is given the flexibility to modify the information.

After verifying the information click “Add”.

![Image showing MD5 calculation](image.png)

**Figure. 67. Calculating MD5**

Step 12: A hash value will be calculated for the image, which can be observed in figure 67. After viewing the information click “Ok” to proceed.
Step 13: “Case Gallery” and “Host Gallery” helps the investigator to jump to any other case or host. Host manager will have the permissions to perform any operation on the current image. Here operation is analyzing the image. “Analyze” option displayed in figure 68, would help in analyzing the image file.

Figure 68. Options in Host Manager

Figure 69. Starting the Analyze operation
Step 14: Many operations can be performed on the imported image. Options can be observed in figure 69.

“File Analysis” option is useful in analyzing the files and directories which are part of the imported image. The Information about the deleted files can also be obtained. It provides the functionality to view data in ASCII, HEX and ASCII Strings. Notes can be added and also data can be exported.

Directory Seek: This option allows users to enter the name of the directory which they wish to analyze. Directory name could be a random or educated guess. Results could be observed in figure 70.

![Figure 70. Searching by the directory name](image-url)
**File Name Search:** This option allows user to search by the file name in the image. If the investigator is searching for any file name in particular, this option would be much helpful. Result of this operation could be observed in figure 71.

![Figure 71. Searching the file name](image)

**All Deleted Files:** This option allows users to display the deleted files from the image. Result can be observed in figure 72.

![Figure 72. Retrieving all deleted files](image)
**Expand Directories:** This option allows users to view the directories in tree wise fashion. Expanded tree can be observed in figure 73.

![Figure 73. Expanding directories](image)

**Step 15: “Keyword Searching”** option helps investigators in searching the image by keywords. A text box is available for investigators to enter the keyword, which can be observed in figure 74. This option helps users in searching for any deleted files or any specific files. Investigators are provided flexibility to have the search to be case sensitive or case insensitive, ASCII or UNICODE.
Figure. 74. Searching by keyword

After the search is completed, results will be displayed. To obtain these results, search for the keyword is done and if it matches any, the list is displayed, as shown in figure 75. On clicking the ‘retrieved file name’, output can be viewed in ASCII, HEX and ASCII strings. Retrieved file can be exported.

Figure. 75. Results for keyword search
Step 16: “File Type Sorting”

This option allows investigators in sorting the data by file types. This reduces the burden on investigators to sort the information.

![Figure 76. Starting the sorting operation](image)

Several options are provided to the user in sorting file types, these options can be observed in figure 76. Saving unknown files data can be an option, as well a copy can be saved in the directory or graphic images can be saved etc.
Figure. 77. Settings for sorting files

These sorted file types can be viewed by clicking on “View Sorted Files”.

Figure. 78. Path of the index file in which sorted files list is saved
Current version of autopsy does not support viewing the sorted files in the browser, this information can be observed in figure 78. Instead, the sorted files can be viewed using the “index.html” file. Figure 79 shows the opened html file.

![Opening the Index file](image)

**Figure. 79. Opening the Index file**

**Step 17:** Clicking on “Image Details” displays the General File System Details of the imported image, which can be observed in figure 80.

![General file system details](image)

**Figure. 80. General file system details.**
Step 18: “Meta Data” option helps investigator in searching for the data using MFT Entry numbers, as shown in figure 81. This mode helps in gathering detailed information about the file.

![Figure. 81. Searching the data by MFT entry](image)

Clicking on Allocation List could display the files in MFT sorted order as shown in figure 82.

![Figure. 82. Displaying status of MFT entries](image)
Step 19: “Data Unit Mode” helps investigator in searching the data based on the area the data occupied in the disk. This mode helps in searching for deleted files. Cluster number can be provided for searching a file which can be observed in figure 83.

**Figure. 83.** Searching data by cluster number

Clicking on “Allocation list” would display the clusters, as shown in figure 84 and its status indicating if it is allocated or not.

**Figure. 84.** Displaying status of cluster entries
Step 20: Clicking on “Close” would close the case and leads to the Host Manager page as shown in figure 85.

Figure. 85. Closing the case

“Image integrity” option could be helpful in verifying if the integrity of image is protected or not.

Figure. 86. Validating the image after performing operations
Clicking on “Validate” option which can be observed in figure 86, cross checks the previous and current MD5 values. If matched, integrity is maintained. Figure 87 is an example of a successful validation test.

![Figure 87. Result of validation test](image)

After completion of validation, close the host and the case.

### 4.5 Capturing an image

**Objective:** Capturing an Image using ProDiscover

**Tool description:** ProDiscover supports capturing the evidence and analyzing the evidence.

**Step 1:** Connect a Flash drive to the computer. For the flash drive to be recognized by the virtual machine, click on “Devices and the USB devices” and select the appropriate device.

**Step 2:** Create a folder HAPPY NEW YEAR in the USB device and create a text file with name 2012.

**Step 3:** Delete the HAPPY NEW YEAR folder.
Step 4: Click on Prodiscover icon and start the operation.

Step 5: Enter the Project name and description for documentation purpose.

Step 6: Click on Capture image located on the top and select the appropriate Source Drive from the dropdown menu.

Step 7: Click on the double arrow located below the source drive and select the destination and create a new folder with name “recovery” and name a file as “data”. Fill all the necessary data to proceed.

Step 8: If the data that is to be recovered is large then split option can be used. Fill the technician name, image number and description and click ok. Capturing the image starts and takes few moments for completing.

Step 9: Click ok and go to the destination folder specified. In the folder two files named data.eve and IOLogerrors will be found.

The process of capturing image is completed. For verifying the correctness of the image, open the image with prodiscover and look for the folder named “HAPPY NEW YEAR” and text file named “2012”.

4.6 Hash values

Objective: Generating hash values

Tool description: Quickhash GUI provides user interface for calculating hash values using different algorithms.

Text Hashing

Step 1: Click on “QuickHash” shortcut located in “Lab 6 – Hash values” folder.
**Step 2:** Choose the hash algorithm from given options MD5, SHA-1, SHA-256 and SHA-512. After choosing an algorithm, enter any text in the “Text Hashing” pane where it says “Enter text to hash....” And click on “Generate Hash”. A hash value for the chosen algorithm will be calculated and displayed below the “Generate Hash” tab.

**Step 3:** Note down the Hash value obtained. Now modify the entered text by deleting a letter or word or sentence.

**Step 4:** Re-enter the original text and generate hash value with the same algorithm and observe the hash value. Both the hash values will be same. This is to maintain the integrity of the data.

**File Hashing**

**Step 5:** File hashing is same as text hashing. Here hashing will be done on the given file. Click on select file and browse for any file and click open. A hash value will be generated in the “File Hashing” pane. Note down the value.

**Step 6:** Make some modifications to the file by adding or erasing data. Calculate the hash value and compare it to the original one.

**Step 7:** Restore the file back to original and generate the hash value and compare it to the noted value. Those values match.

Note: Renaming the file does not have any effect on the Hash value.

**Recursive Directory Hashing**

**Step 8:** This helps in hashing an entire directory. Select the option of saving the hash values to a .CSV file or .HTML file. Click on select directory and browse for a directory which has more
than 3 files in it. After selecting the directory, enter a file name to save the log file and remember the destination of html file. Open the html file.

Hash values for all the files located in the directory will be calculated and will be saved to the html file.

**Copy and Hash files**

**Step 9:** This option helps in copying files from a source to a destination and calculates the hash value before copying and after copying. Thus, helping in secure data transfer.

Select a source directory from which the files are to be copied and destination directory in which those files are to be pasted. Click on Go and then click on proceed.

Name the file to be saved.

Open the .CSV file and observe the data. Source hash and Dest hash values will be the same, which indicates that the copying is done while maintaining integrity.

Repeat the whole lab by choosing different algorithms.

**4.7 Editing using Hex Workshop**

**Objective:** Edit a file using Hex Workshop

**Tool description:** Hex workshop is a hexadecimal values editor.

**Step 1:** Open a text document and enter a continuous string of c’s and save it as “trail.txt” on the desktop.
Step 2: Click on “Hex Workshop Hex Editor” icon located in the folder “lab 7 – Hex Workshop”. Click on “File”, click on “Open” and browse for the text file “trail.txt” which is saved on desktop.

Step 3: A window will be opened in which a string of ‘0’s , numbers and alphabets are displayed. These are divided into three types. The set which is on left is called “Offset Area”. The set in the middle is called “Hex Area” and the set to the right is called “Text area”. The values in the Hex area and Text area matches. In the figure, each 63 in Hex Area represents a ‘c’ in Text area.

Move the cursor to any of the values in the text or hex, automatically another cursor highlights the respective hex or text value.

Step 4: Click on some value in the Hex Area and change the number to “64” and observe the respective change happened in Text area.

In the figure it can be observed that the value highlighted in red are the changed ones and modifying the value to ‘64’ made the text change to ‘d’.

Step 5: Similarly, make a change in text area. Enter “s” and observe the change in the Hex area.

Step 6: Searching for a specific term in a file happens all the time. To do so there are two ways to do it. Go to “edit” and click on “Goto”. Here two options are provided for searching. Dec or Hex. Dec takes natural numbers and Hex takes hexadecimal numbers.

Enter a value in Offset, select Dec and click “Go”.

Step 7: Now select “Hex” and enter some value in the offset.

Click on “Go”.

Step 8: Make a change in the location obtained after the “Goto” operation.
Save the file. Answer “yes” for saving a backup file. Close the Hex Workshop. Now open the original text file and observe the data.

The data modified can be observed. This can be done with any kind of files. Try it with different file formats.

4.8 Graphic images

Objective: Playing with the header files of graphic files

Tool description: Hex Workshop supports editing hexadecimal values.

Step 1: Click on “Hex Workshop Hex Editor” icon located in the “Lab 8 – Graphic Files”. Click on “File”, click on “Open” and browse for the “PNG” file located in the “Lab 8 – Graphic Files” folder.

Step 2: Make many changes to the values in the “Hex Area” and save the file. Click on “Yes” to make a backup copy of the file.

Step 3: Open the saved file using any image viewer software. It does not get opened.

Step 4: Open the saved backup copy of file. Click on Save as and name the file with its original name along with its extension. This replaces the modified copy with the original copy.

Step 5: Open the original file again. Modify the first 5 values in the “Hex Area” and save the copy. Open the file and observe.

Step 6: The modified file cannot be opened. Either following step 4 or modifying the value manually could help in opening the image. Use different file types and follow the same procedure and observe.
4.9 Web Forensics

**Objective:** Retrieving browser history using web historian

**Tool description:** This tool retrieves web history from different browsers.

**Step 1:** Click on “Mandiant Web Historian” icon located in “Lab 9 – Web Forensics”.

**Step 2:** Click on “File” and click on “Options”

Change the Default Saved file format to “HTML”. Select the browser for which the history is to be retrieved. Select each browser at a time which could increase the performance and avoids software hanging. Click “Ok”.

**Step 3:** If the location of the file where the browser history is saved is known select “Specify a browser history file:” and enter the path of the file or browse for the file.

If the file where browser history is saved is not known then select “Find Browser history files”. Better option here is to select the Find browser history files, because it could find files saved in different locations which user could not be aware of.

**Step 4:** Specify a directory in which the search has to be done for the browser history files. Click on process. This would take time because search will be done for the appropriate files. Choose the destination and name the file.

**Step 5:** Close the Mandiant Web Historian and open the destination folder. An html file and a folder named “XXXXX_Files” will be created.

Open the html file. Browsing history will be displayed.

On the bottom of the page tabs with names 1 Internet Explorer, 2 Internet Explorer and so on can be found. Each tab refers to a different location where the history is saved.

In the “XXXXX_Files”, many html pages are created each referring to a different location where the browser history is saved.
4.10 Email forensics

**Objective:** Basic operations on email forensics

**Tool description:** FTK imager provides many functionalities in which email forensics is an important one.

**Step 1:** .PST files of Outlook are used for conducting forensic investigations on emails send by a suspect. Simple mechanism is described for creating a .PST file.

Click on “File” and then click on “export and import”.

**Step 2:** Select “Export to file” and click next.

**Step 3:** Select .PST which is the Personal Folder File and click “Next”.

**Step 4:** Browse for the location to save and name the new .PST file.

**Step 5:** Click finish and go to the destination directory and verify whether the .PST file is saved or not. Copy the .PST file and save it in the folder “Lab 10 – Email forensics”

**Step 6:** Click on “Forensic Toolkit” icon in “Lab 10 – Email Forensics” folder. An error will be displayed, ignore the error by clicking “Ok”.

**Step 7:** Start a new case and fill in the details required. Make sure to note the specified “Case Path”, because all the data will be exported to that folder.

**Step 8:** Click on “Next” till “Refine Case” is found. Select the “Email Emphasis” and click “Next” until “Add Evidence” is found. Click on “Add Evidence” and browse for the “.PST” file and click “Next” and follow till the following screen is displayed.

**Step 9:** In the “Overview” tab, files are listed based on categories. Go to the “Explore” tab which provides a tree view of the .PST file.

This view provides the functionality of showing the Directories in a tree wise view on the top-left, Content of the message in the top-right and list of messages in the bottom pane.
Step 10: Click on “Graphics” tab. This tab is useful in viewing the images which are contained in the imported .PST file. This view is useful in particular for any images or graphic files in the emails. Most of the times these images help in finding the behavior of the suspect.

4.11 Data Operations

Objective: Observe the result of data operations using Hex Workshop

Tool description: Hex workshop supports editing hexadecimal values.

Step 1: Click on “Hex Workshop Hex Editor” icon located in “Lab 11 – Data operations” folder. Click “Open” and browse for any text file.

Step 2: By default the icons for doing the shift operations will not be displayed. To perform the operations click on “Tools”, click on “Operations” and then many options will be displayed for the user to select.

Step 3: Select the “Byte Flip” from the list of “Operations”. Observe the values in the Hex Area and figure out the mechanism of “Byte Flip” operation.

Step 4: Save this file as “Byte Flip”, open the file and observe the data.

Step 5: Performing a “Byte Flip” operation again sets the bytes back in order.

Step 6: Open the text file again and perform “Inverse Bits” operation. Observe the values in the Hex Area and figure out the mechanism of “Inverse Bits” operation.

Step 7: Save it to a text file, open the text file and observe the data.

Step 8: Open the original text file back and perform each operation listed. AND, OR, XOR, UPPER CASE, LOWER CASE, INVERSE CASE and save the files and observe the changes being done to the data and the Hex values.
4.12 Metadata

Objective: Reading, writing and other operations on Metadata

Tool description: Exiftool is a command line tool for extracting information about data files.

Step 1: Click on “Command Prompt” located in “Lab 12 - Metadata” and go to the folder using the command “cd Desktop\Lab 12\exiftool”.

Step 2: Copy the file which is to be investigated and paste it in the folder “exiftool” which is located in “Lab 12 - Metadata” folder.

Step 3: In the command prompt execute the following command and observe the printed information. “exiftool –a –u –g1 filename”. Here the filename has to include its extension.

Do the same with different files and observe the data retrieved.

Step 4: To print the information of all pictures in a directory execute the following command. “exiftool –r foldername”. This folder has to be placed in the “exiftool” directory.

Step 5: Go to

“http://www.sno.phy.queensu.ca/~phil/exiftool/exiftool_pod.html#reading_examples”, use the commands and observe the metadata.

4.13 Data carving

Objective: Data carving using DFF

Tool description: Digital Forensics Framework is a tool developed for analyzing and investigating evidence.

Step 1: Click on “DFF (gui)” icon located in “Lab 13 – Data carving” folder.

Step 2: Click on “File” and then on “Evidence files”.
Step 3: Click on the “+” sign and browse all the way to “11-carve-fat.dd” which is located in the “Lab 13 – Data carving” folder.

Click “Open” and then click “Ok”. This imports the dump into DFF.

Step 4: Click on “Logical Files” which is located on the Left side.

Step 5: In the middle pane mark the box beside “11-carve-fat.dd” file and right click on it. Click on “Open with” then click on “Search” and the select “carvergui”. A new tab named “carver-gui <11-carve-fat.dd>” will be opened.

Step 6: In the “carver-gui <11-carve-fat.dd>” tab, click on ”application/images” and then “+” sign to expand the tree to view the types of images. Select all the required file types and click “Start”. “Overall progress” shows the status of the carving in percentage.

Step 7: Go back to the “Browser” tab. Click on “+” to expand “Logic files” then on “11-carve-fat.dd” then on “carved” and then select any of the file types. In the middle pane many files will be displayed.

Step 8: Select any one of the files from the middle pane and right click on it. From the displayed options click on “Relevant module” and then select “pictures”.

Step 9: Click “OK” in the “Apply module pictures” window. A new tab named “viewerimage” will be opened. Images can be viewed by clicking arrows displayed in the tab.

This is the process of data carving from a raw image. Follow the same procedure again with another test image which can be downloaded from the following link “http://dftt.sourceforge.net/test12/index.html”.
4.14 Volatility

**Objective:** Exploring volatile memory of an image

**Tool description:** Digital Forensics Framework is a tool developed for analyzing and investigating evidence.

**Step 1:** Click on “DFF (gui)” icon located in “Lab 14 – Volatility” folder.

**Step 2:** Click on “File” and then on “Evidence files”.

**Step 3:** Click on the “+” sign and browse all the way to “be2.vmem” which is located in the “Lab 14 - Volatility” folder.

**Step 4:** Click on “Logical Files” located in the left pane, a file will be displayed in the middle pane. Right click on the file displayed in the middle pane and click “Open with” and then click on “Volatile memory” and select “Volatility”.

**Step 5:** Click on “file” in the Arguments and click “OK”.

**Step 6:** Expand “Logical files” and then expand “be2.vmem” and click on “volatility”. It displays the processes that are running while acquiring the data.

Similarly, repeat **Step 5**, by selecting different Arguments displayed and observe the information. More memory dumps can be found at “https://code.google.com/p/volatility/wiki/FAQ#Are_there_any_public_memory_samples_available_that_I_can_use_for”. Download some of the memory dumps and perform similar operations.
5. TESTING AND EVALUATION

5.1 Testing on different platforms

VirtualBox can be installed on different operating systems. Hence, the .OVA file has to be successfully imported by the virtualbox in all operating systems. For testing, the same procedure is followed for importing the .OVA file in all widely used platforms. Importation procedure for all the platforms is similar. Figures 88, 89 and 90 are the screenshots obtained after testing the project in different operating systems.

![Screenshot of VirtualBox on Mac OS X Lion](image)

**Figure. 88.** .OVA file importation successfully tested in Mac OS X lion
**Figure. 89.** OVA file importation successfully tested in Windows 7

**Figure. 90.** OVA file importation successfully tested in Linux Ubuntu
5.2 Testing different open source tools

FTimes
This is an open source tool which is primarily concerned with collecting evidence. This is one of the mostly used data recovery tool. This tool is complicated in installing and also compiling. This is developed in C language and execution of this tool requires C knowledge. Basic compilation and commands are required for using this tool.

Pyflag
This is an open source tool developed in python. This tool is popular in dealing with network forensics. This tool uses pcap files and captures network traffic. But wireshark being most extensively used and user friendly makes it more popular than this tool.

Pasco
This is an open source tool used by the investigators who work on internet explorer history forensics. This tool can retrieve history from the index.dat file of internet explorer. This tool is supported by cygwin in windows. This is also a command line tool executed with many commands.

Galleta
This is an open source tool which could retrieve web browsing history from all the web browsers. This retrieval of history plays a major role in investigating suspect’s activities in web forensics. Issue with this tool is it does not support windows32 systems.

Volatility
Volatility is an open source tool which concentrates on volatile memory forensics. It is useful in analyzing the RAM. Volatile memory forensics is a field in forensics which has much scope for research. This tool is one of the most popular tools for analyzing volatile memory.
Tcpdump

This is a tool developed in C/C++. This is a command line tool. Lots of commands are needed for capturing network traffic. Wireshark having all the functionalities with a great interface makes it more popular in analyzing network traffic.

5.3 Testing on different products

In this project, VirtualBox software is used to develop and perform operations. This is an open source tool which is available online at no cost. VMWare is a commercial product which assists users in providing virtual machines. VMWare supports importing .OVA files. So the exported OVA file is tested on VMWare. Figures 91 and 92 are screenshots obtained after testing the .OVA file in virtualbox and VMWare.

Oracle VM Virtualbox

![Oracle VM Virtualbox](image)

Figure. 91. .OVA file successfully tested on Oracle VM Virtualbox
Disc created with the virtualbox software and XP is tested on different platforms and then for end user testing, disc is provided to some selected users. From the feedback obtained changes were done to allow the user utmost comfort in using the Disc and installing the image. Pre-installed tools were used by the users with the help of training material and feedback is obtained.

Figure 92. OVA file successfully tested on VMWare
6. CONCLUSION

In this project, a toolkit a mobile work station for installing and performing basic forensic investigations is developed. This project would be a great contribution to the faculty and students in the field of computer forensics. Portability of the disc is one of the important features. Extensive research is done on the huge database of available open source forensic tools. Forums were visited, popular cases which were solved using forensic techniques were observed. Based on the efficiency and user friendliness some of the tools were selected and tested. Information about each tool is obtained by visiting the tools website. Materials for performing basic functions using those forensic tools are provided. All the tools for which the material is provided are tested on the image, which is provided in the disc.

After generation of the disc with the XP image, in which forensic tools are pre-installed testing phase was carried out. Different operating systems were considered and many computers were used for the purpose of testing. Disc was made available to some users, by whom the testing was done. Feedback from them was obtained and changes were made to improve the user friendliness of the material provided for installing the image and using the tools. This project is useful for users in multiple ways. Major advantage of the project is providing learning experience for the users. Expanding this project could help users in performing various operations on several forensic tools without any prior knowledge about the tools. Availability of many more forensic tools improves the scope of expanding the project to further level. This project can be helpful to develop a similar project with different operating systems which are widely used.
BIBLIOGRAPHY AND REFERENCES


• [http://www2.opensourceforensics.org/](http://www2.opensourceforensics.org/)
• [https://www.virtualbox.org/](https://www.virtualbox.org/)