Security and Privacy over the Internet

TOOLS REPORT

Name: Sowndarya Krishnamoorthy

Student ID: 104654482

Course Number: 60-564

FTK IMAGER

Statement Of Problem And Tools:

Many times, associations or people don't give much significance to such sort of occurrences and afterward, suffer the real loss of information. Data once deleted from the external or logical drive could not be recovered. To overcome this issue, many data recovery, and disk imaging tools have been created. One such tool is FTK Imager; other software includes Recuva, Undelete, Power Data Recovery, Restoration, Pandora Recovery, etc. These recover and repair files, databases and other storage media and bring back the lost data safely.

Background:

The Forensic Toolkit Imager (FTK Imager) is a business scientific imaging programming bundle circulated by AccessData.

FTK Imager bolsters stockpiling of disk pictures in EnCase's or SMART's file format, and also in raw (dd) format. With Isobuster innovation worked in, FTK Imager images CDs to an ISO/CUE file mix. This likewise incorporates multi and open session CDs.

To prevent coincidental or purposeful control of the first proof, FTK Imager makes a bit-for-bit duplicate picture of the media. The forensic image is indistinguishable all around to the first, including file slack and disk unallocated space. This permits you to store the original media away, safe from damage while the examination continues utilizing the picture.

After you make a picture of the information, you can then utilize FTK to perform a finish and careful measurable examination and make a report of your discoveries.

Overview:

The FTK toolbox incorporates a standalone disk imaging program called FTK Imager. The FTK Imager can spare a picture of a hard disk in one document or in portions that might be later remade.

- It ascertains MD5 hash values and affirms the trustworthiness of the information before shutting the records.
- It generates Secure Hash Algorithm (SHA-1) hash reports for disk files and images to provide integrity and check whether the image has remained unchanged after recovery.

- It previews the forensic data stored on the local system or on a network drive and exports the files and folders.
- In expansion to the FTK Imager apparatus can mount gadgets (e.g., drives) and recuperate erased records.
- It can also function as a RAM analyzer and stores the results in .mem format.

FTK Imager can additionally make exact duplicates (forensic pictures) of system information without rolling out improvements to the original evidence.

Installation:

FTK Imager can be introduced to the system where it will be utilized, or it can be keep running from a compact gadget such as a USB thumb drive associated with a machine in the field, so there is no compelling reason to introduce it in a suspect's system.

Install FTK Imager User Interface to a local hard drive when you mean to connect evidence hardware to the system for analyzing the imaging evidence.

WORKING WITH EVIDENCE:

Utilize FTK Imager to preview evidence preceding making the picture file(s). You can then picture the whole evidence object, or pick particular things to add to a Custom Content (AD1) picture.

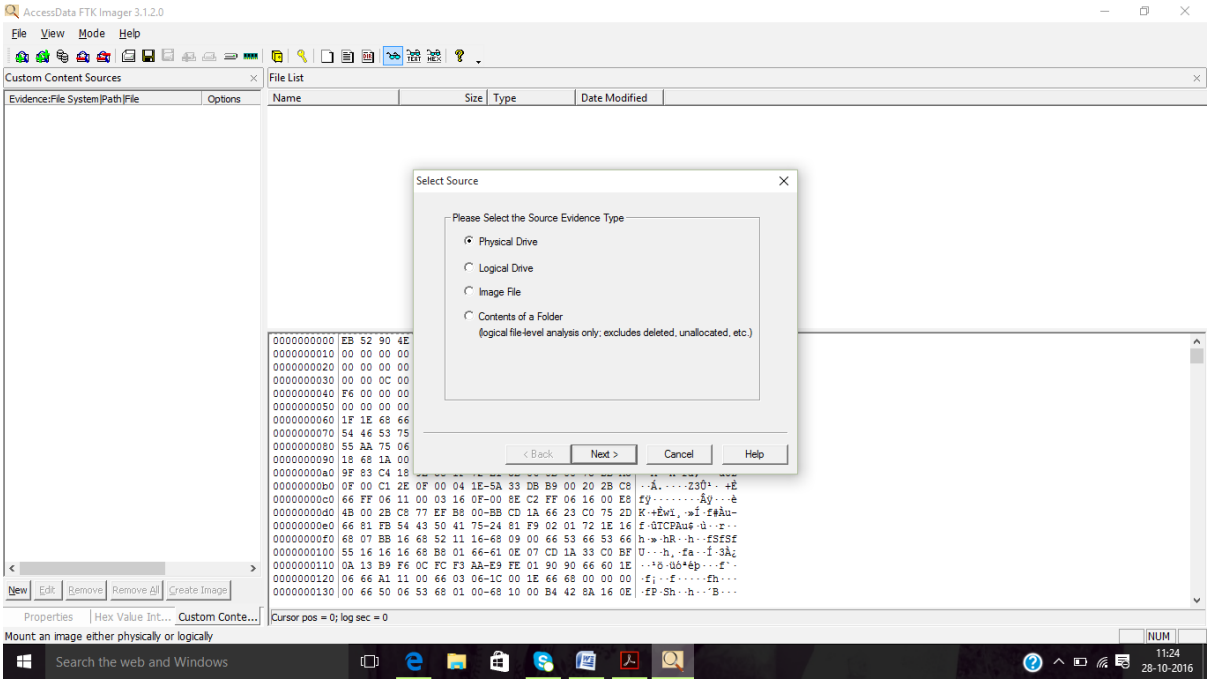
Adding Evidence Item:

Single evidence item or several at one time can be added.

To add an evidence –

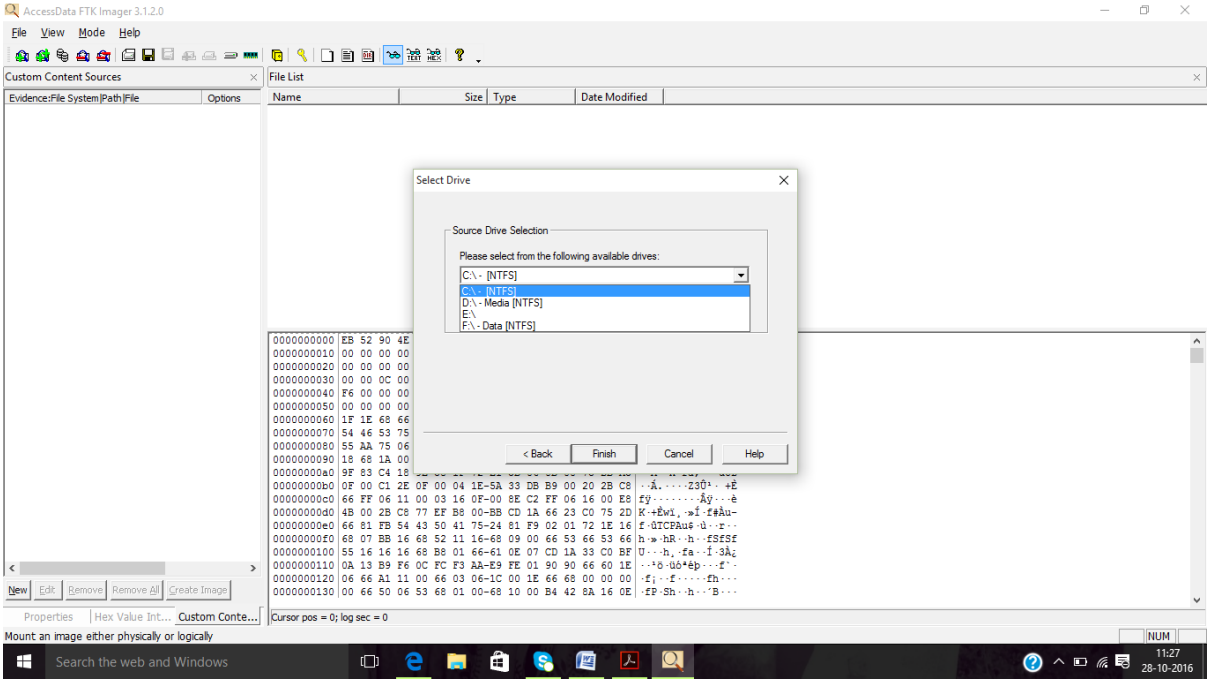
1. Perform one of the following:
    - Click File > Add Evidence Item.
    - Click Add Evidence Item button on the Toolbar.
2. Choose the source type you want to preview, and then click Next.
3. Select the drive or browse to the source you want to preview, and then click Finish.
The evidence item appears in the Evidence Tree.
4. Repeat these steps to include more evidence items.

Screenshot: After selecting Add Evidence Item button, choose the source



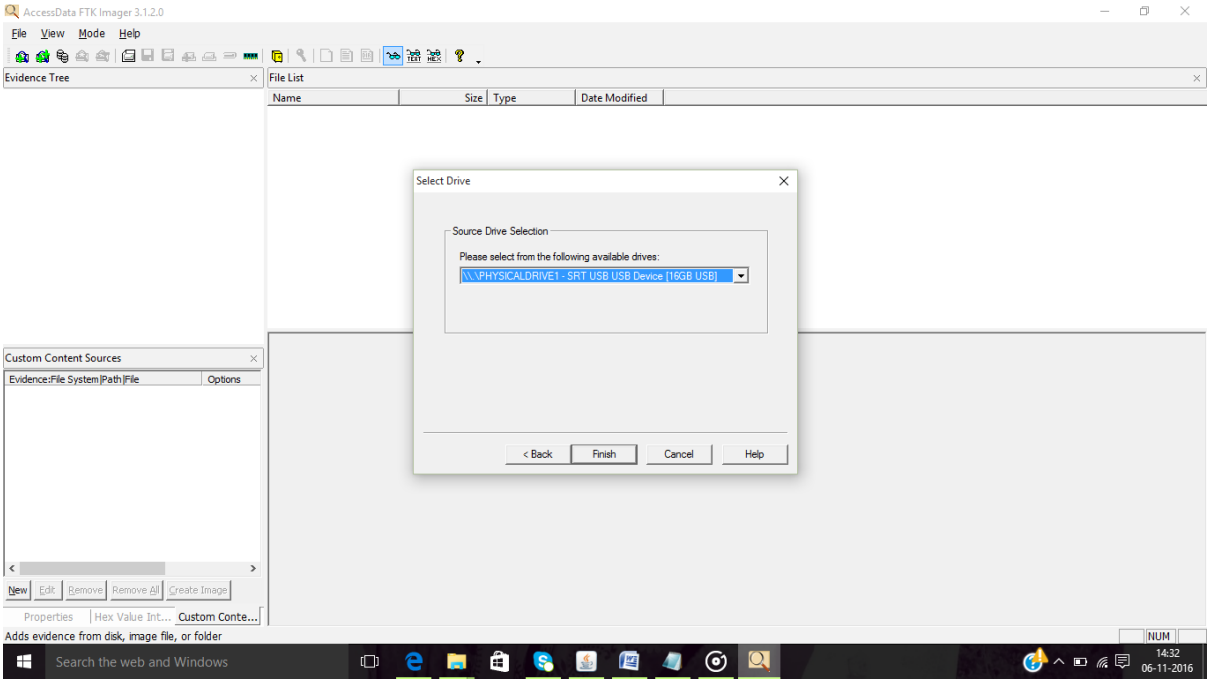
The source for evidence type can be selected among- Physical (external drives attached to the system), Logical drive (drives mounted in the system), Image file or contents of a folder.

Screenshot: If Logical Drive was selected as Source it displays the following screen



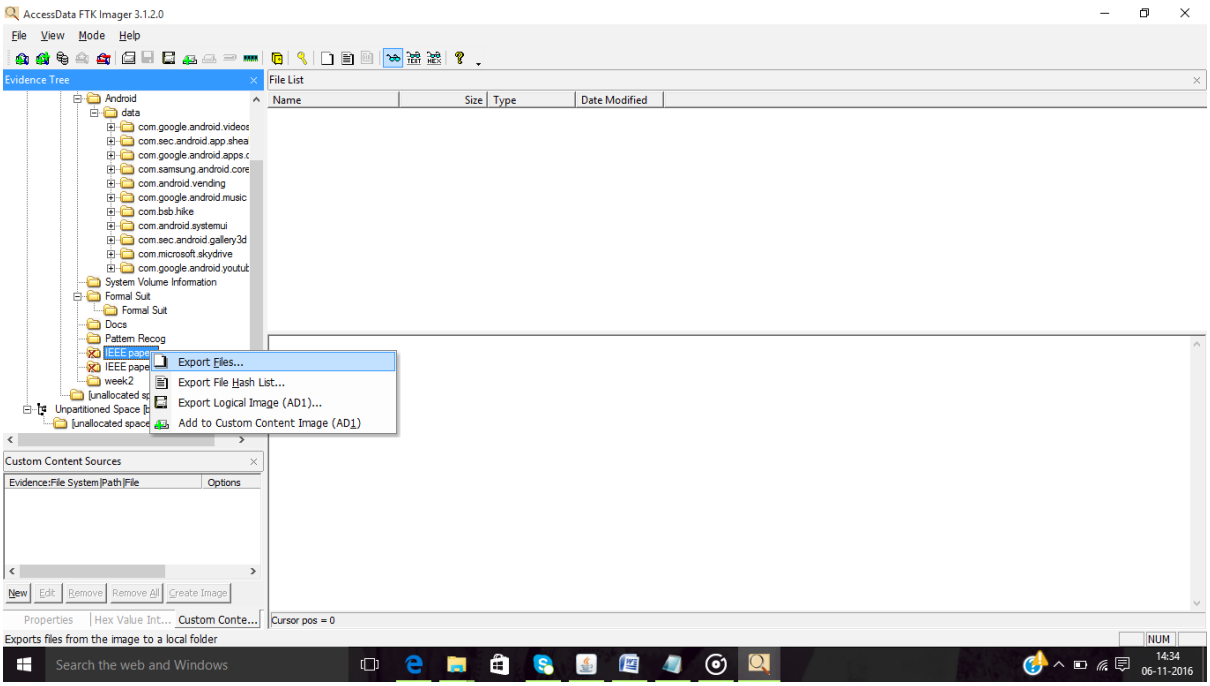
If Image file or Contents of a folder option is selected, you can browse to a specific folder and choose the contents.

Screenshot: If Physical Drive was selected as Source it displays the following screen



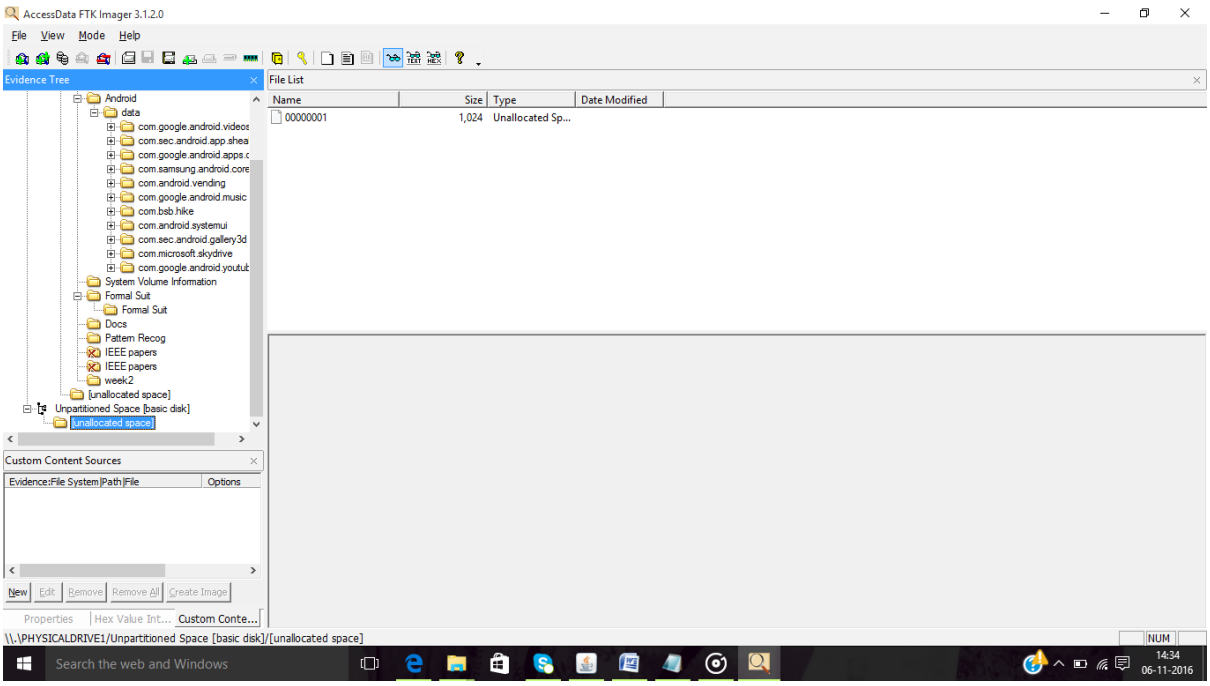
After selecting the physical drive, the connected USB can be detected. Select the USB drive to access lost files and recover data.

Screenshot: Export the files which have been deleted in the USB drive



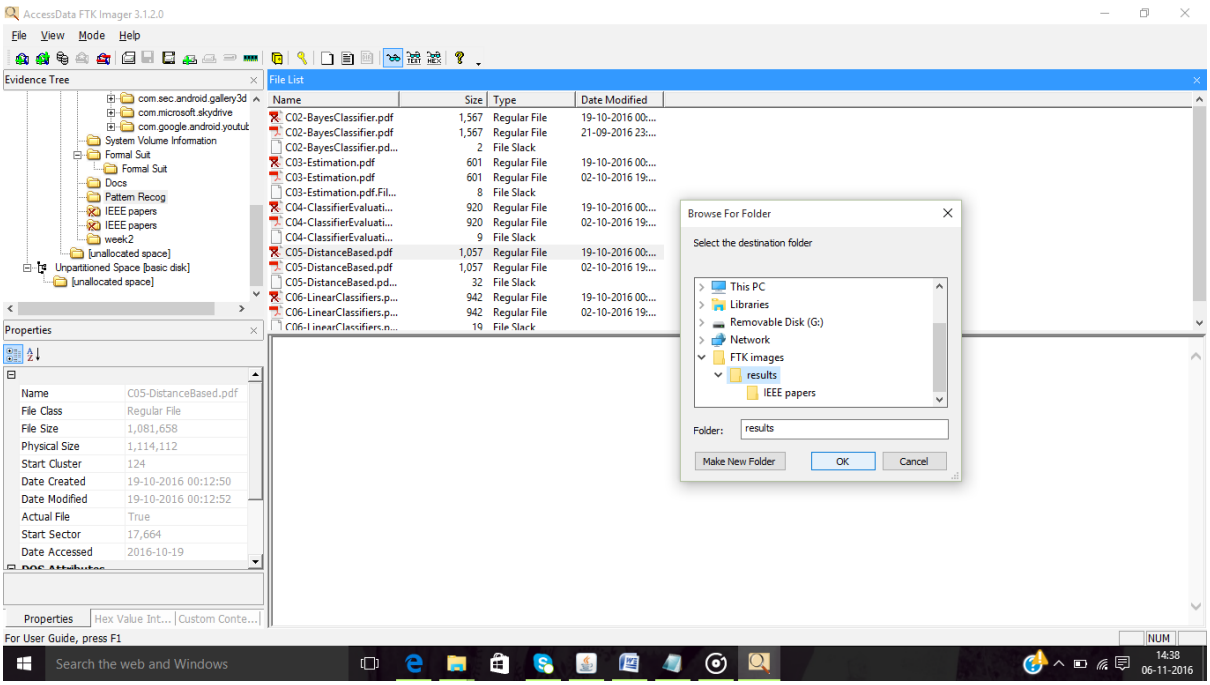
Access all the folders and files recovered in the USB drive, and select the required file to export it to the specified path.

Screenshot: Unallocated space in the drive is also displayed



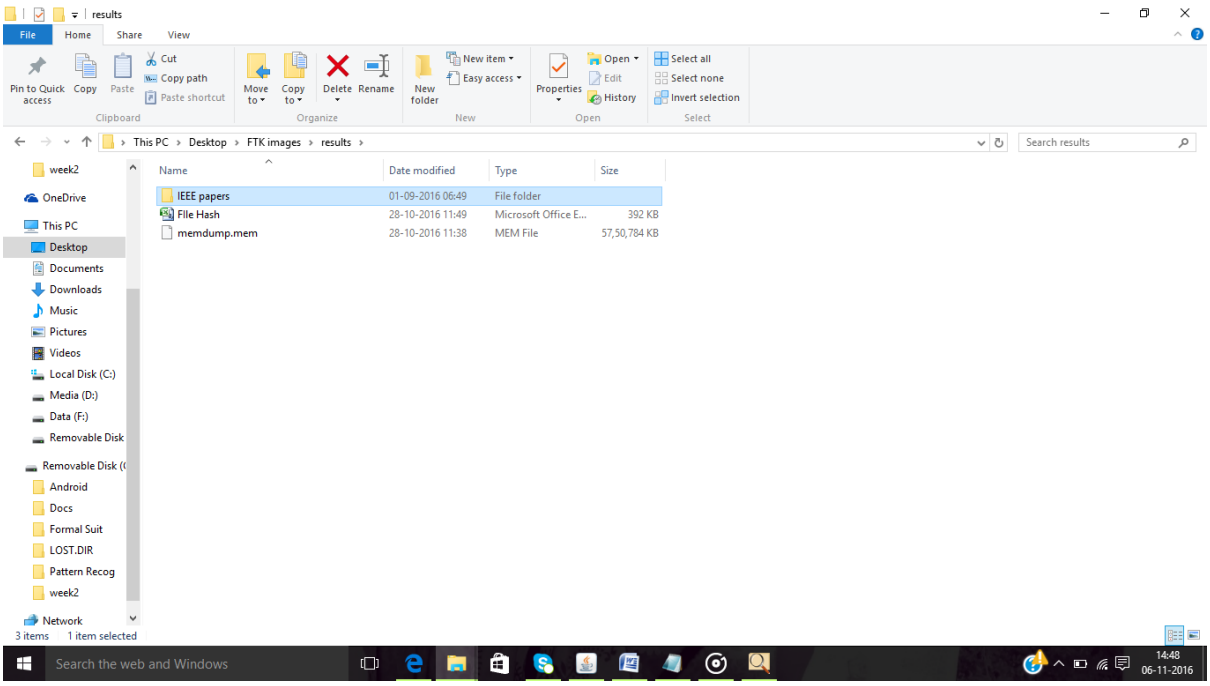
Sometimes, the data can be hidden in the unallocated space of the drive while portioning it. However, all the hidden data and lost files can be recovered through FTK Imager and display the contents in the UI.

Screenshot: View the file properties in Properties column and export it to specified path



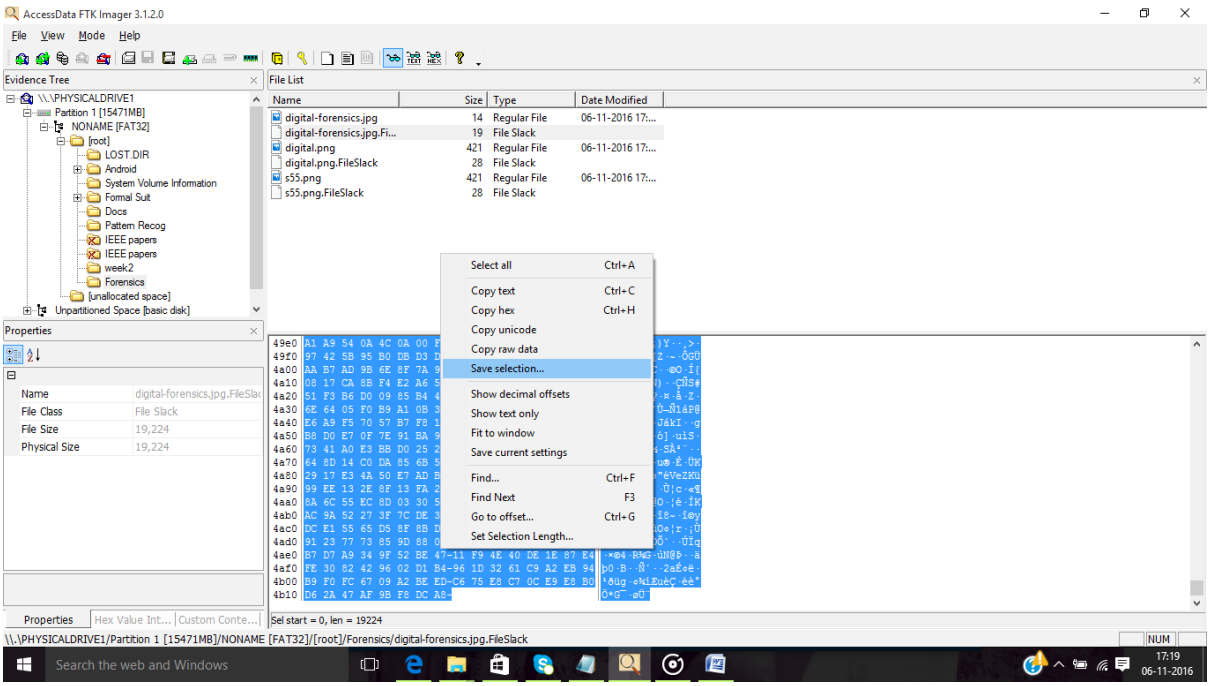
The left corner panel displays the file properties for each of the file present in the drive. It gives details like file history, last modified date, size etc.

Screenshot: File deleted in the drive recovered to the specified folder



The IEEE papers folder and its contents were deleted on the USB drive. Using FTK Imager, it can be recovered to the specified path without any data loss.

Screenshot: Hex values are selected and saved to an image format



The hex values present on the drive are selected and can be used to reproduce the image file. Select ‘Save Selection’ option after analyzing the hex values and save it as .jpeg file. The hex values contain the header information in the first row and RGB values in the content.

Removing All Evidence Items:

All evidence items can be removed at once by performing one of the following-

Either click File ->Remove All Evidence Items or click Remove All Evidence Items button on the toolbar.

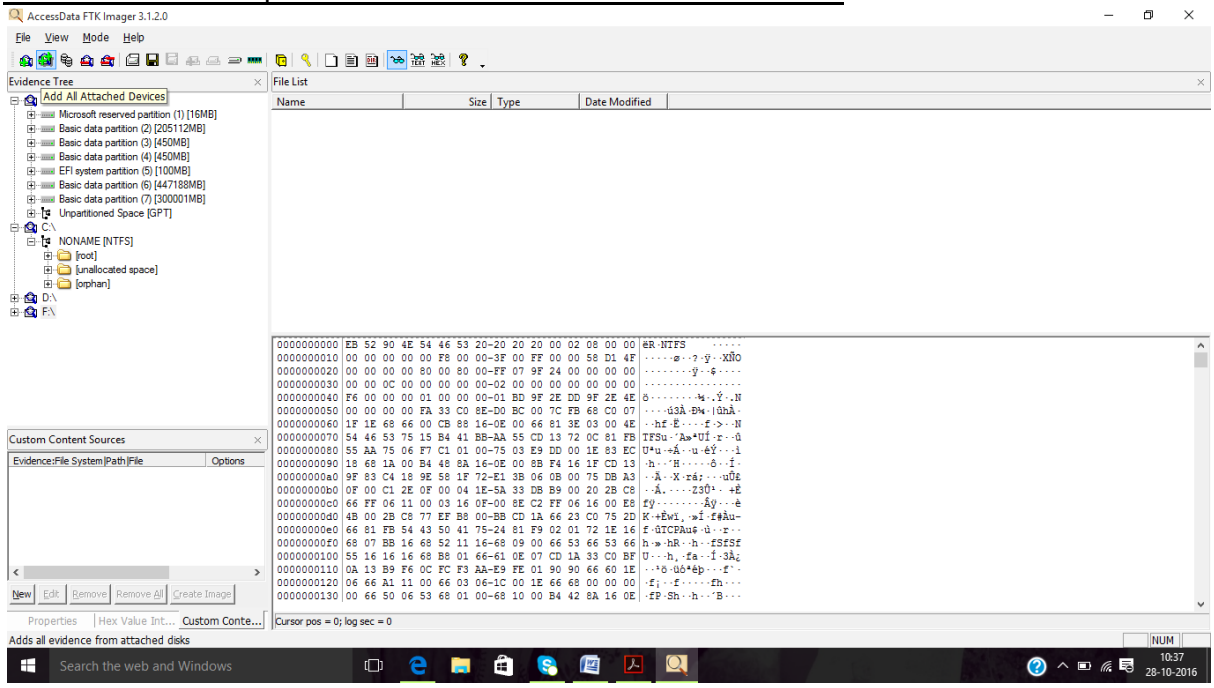
Adding All Attached Devices (Auto-mount):

To add data from all of the devices attached to a machine-

Either Click File -> Add All Attached Devices or click Add All Attached Devices button on the Toolbar.

It examines all associated physical and logical drives for media. If no media is available in a connected drive such as CD-or DVD-ROM or a DVD-RW, the drive is skipped.

Screenshot: Cursor placed over Add All Attached Devices button

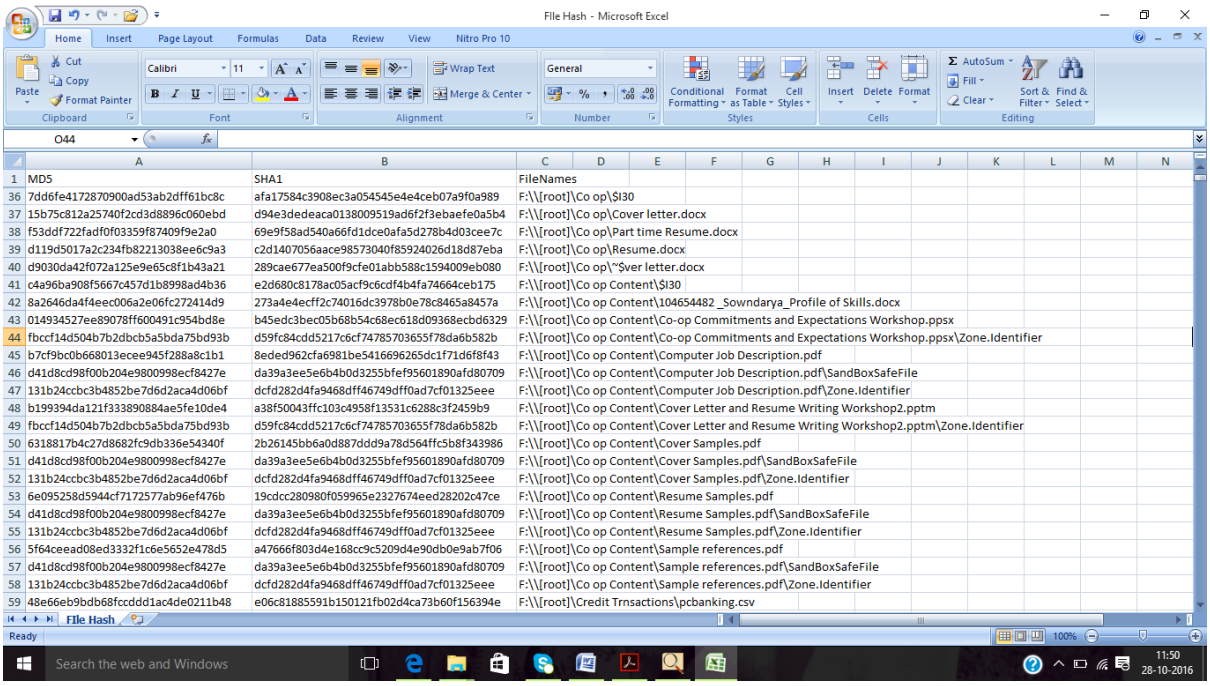


Exporting Files:

FTK Imager allows the recovered files to be exported to a destination folder. The File menu has various exporting options such as- Export Files, Export File Hash List, Export Directory Listing, and Export Disk Images.

The screenshot below explains one example of exporting using File Hash List option:

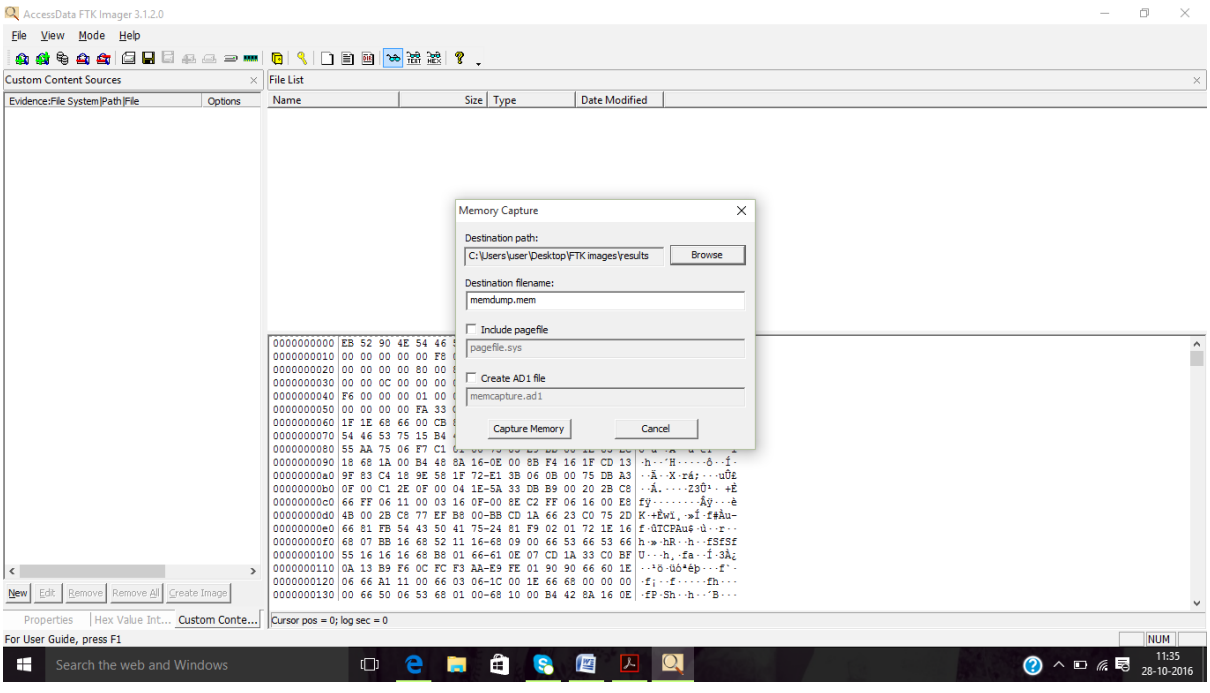
Screenshot: Exporting hash values of a selected logical drive using Export File Hash List option



The hash values of all the content on the logical drive are exported and saved in .csv format. The hashing algorithms are MD5 (Message Digest) and SHA1 (Secure Hash Algorithm).

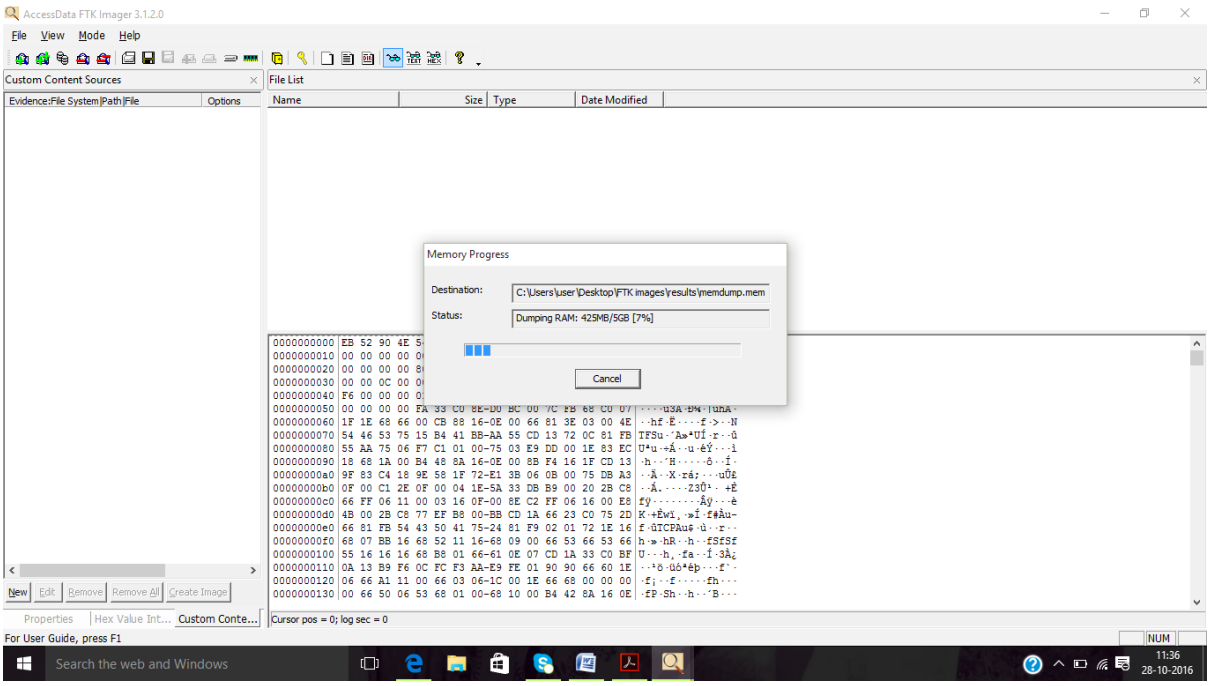
CAPTURING MEMORY

Screenshot: Browse the destination path to save the memory dump

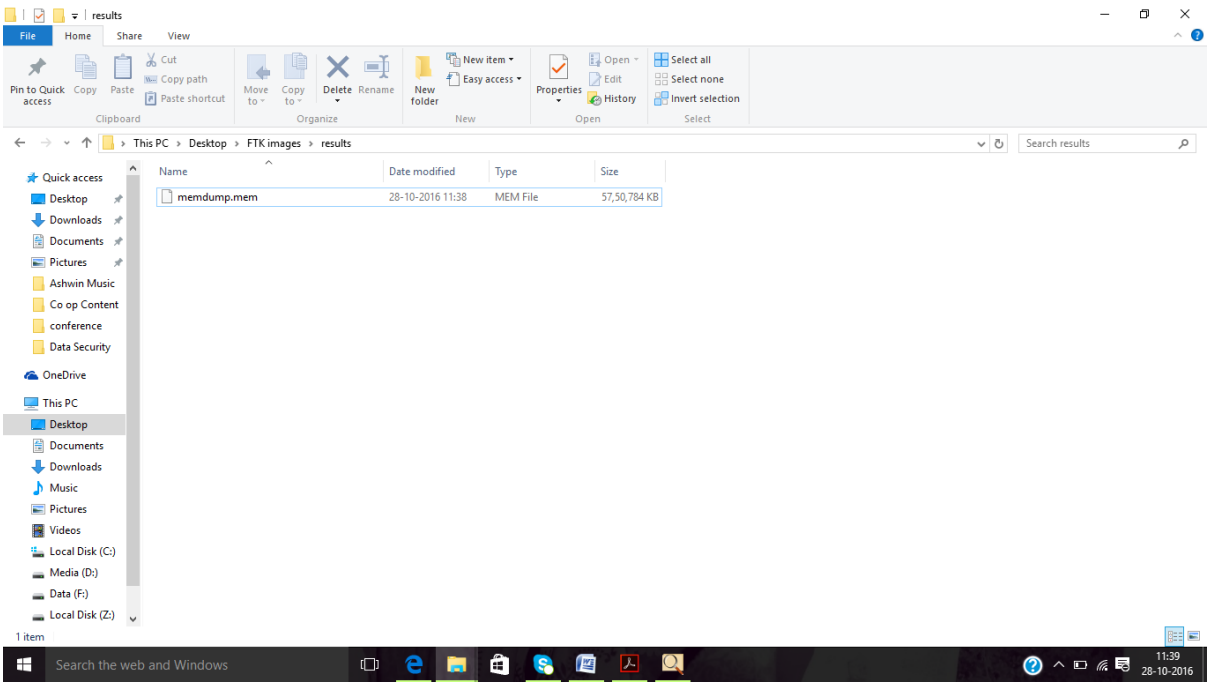


FTK Imager can also capture memory and save it as a dump file (.mem format) to the specified path.

Screenshot: FTK Imager captures and dumps RAM



Screenshot: After dumping successfully, the results are stored in the destination folder



The dump file is in .mem format which requires any other RAM analyzer tool to investigate it.

RELATED TOOLS:

COMPARISON OF FTK Imager with VOLATILITY:-

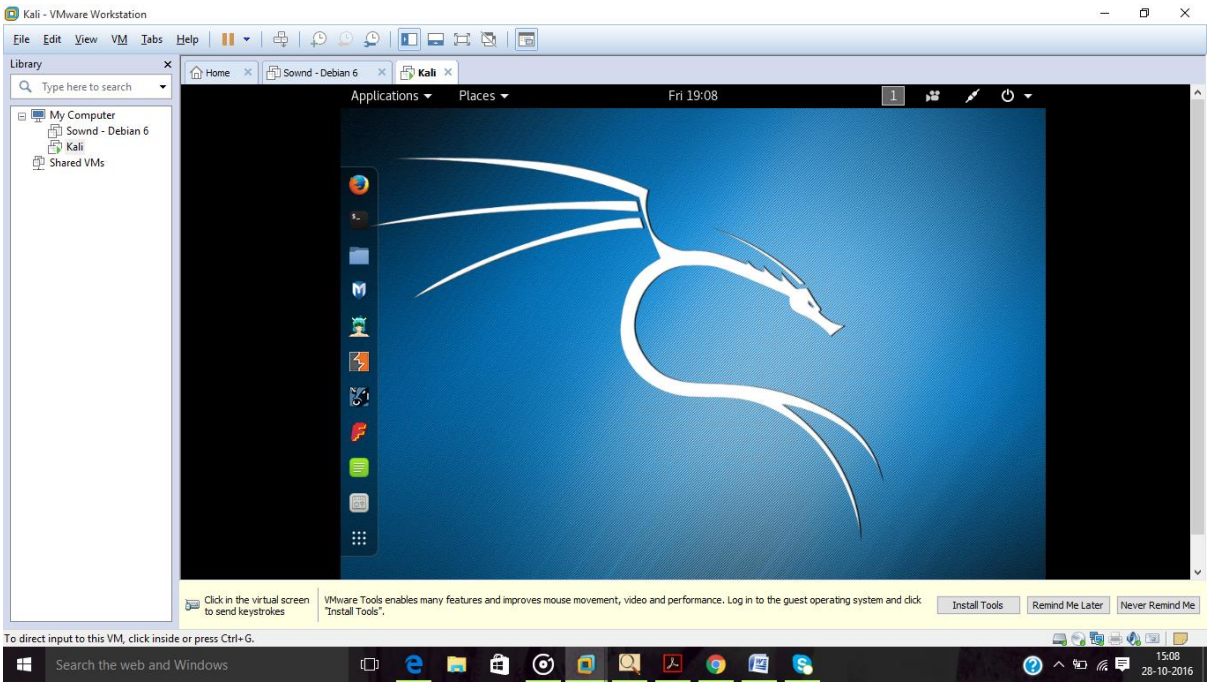
Kali Linux OS is used for penetration testing and digital forensics. It has many cyber attack management tool which includes the volatility tool as well. Enter into the virtual machine and load the .iso file to boot the Kali Linux operating system.

Volatility tool is used to capture and analyze the system RAM. The dump files such as raw dump, crash dump, and virtual machine dump can be traced through Volatility.

It has many functions other than analyzing the memory. Few such functions are-

- It can view all the processes which are currently running (pstree command) and associated dlls (dlllist command).
- Memory files can be dumped using memdump command and all dll using dlldump.
- It is used for scanning malware analysis, root kit activities (psscan command), the profile of kernel structures and system addresses.
- The TCP connection can also be checked while active memory dumps using connections and sockets command.

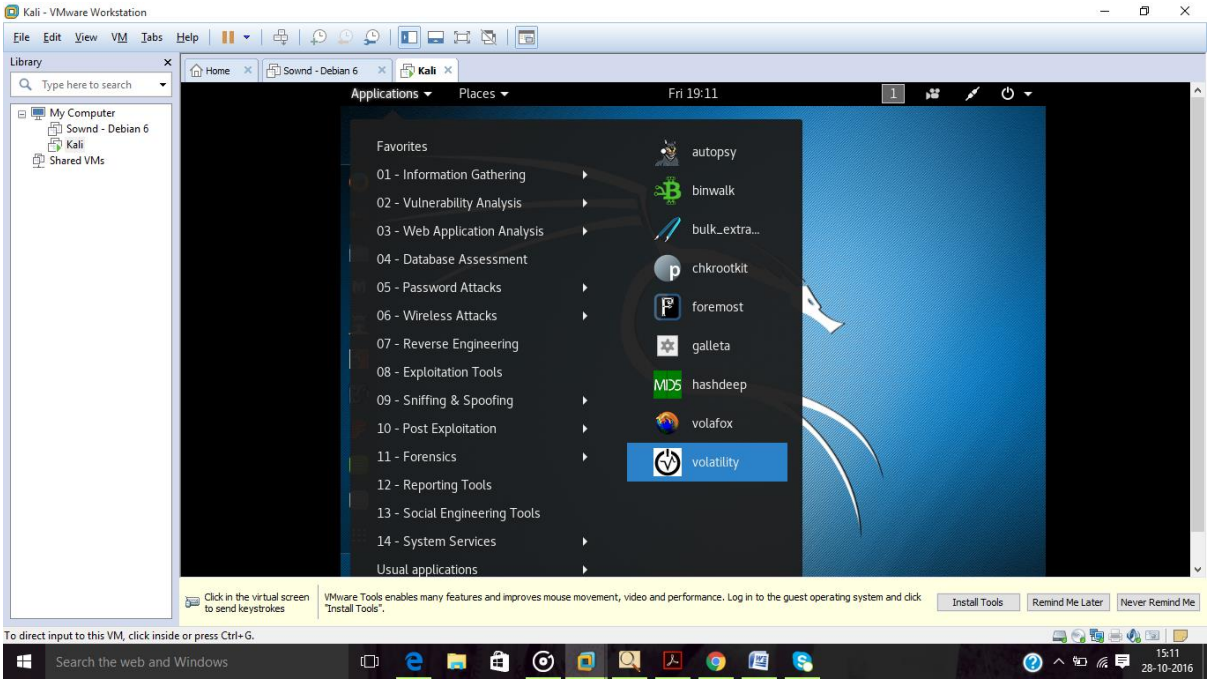
Screenshot: After entering virtual machine, Kali Linux OS getting loaded



Volatility tool is installed in the Kali Linux OS under forensic tools option. Access it through -

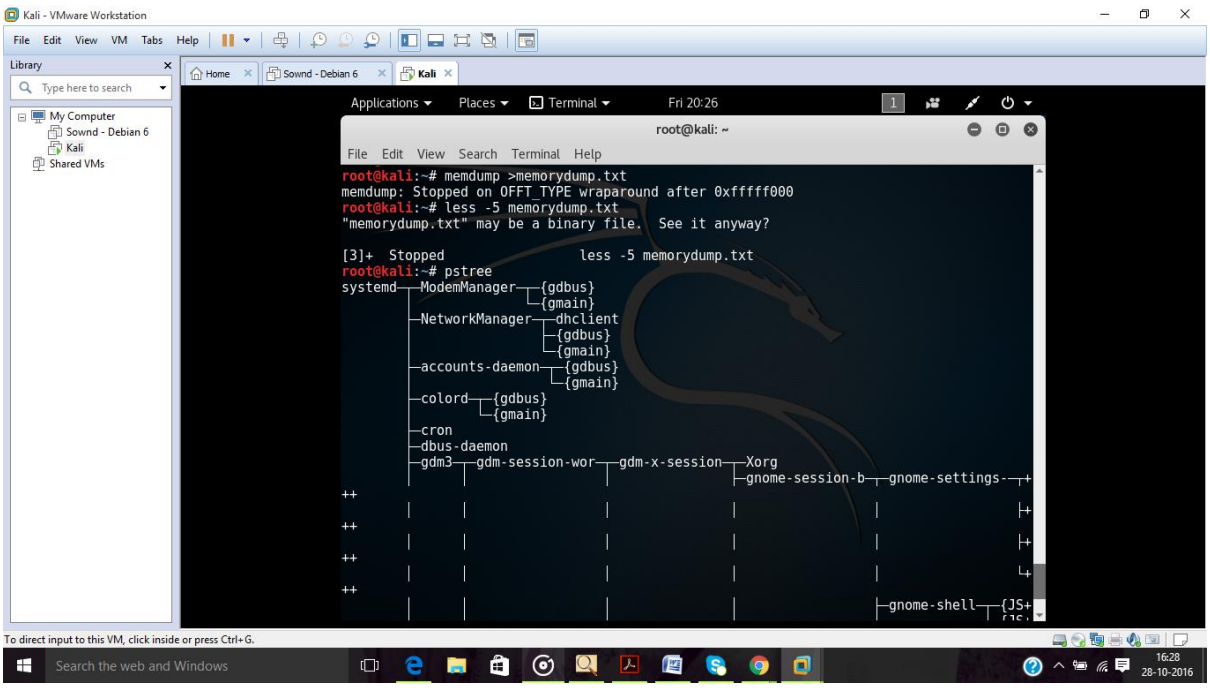
Applications-> Forensic Tools -> Volatility

Screenshot: Accessing Volatility Tool



Volatility is opened from Forensics tools option. The Kali Linux has various other cryptanalytic tools installed in it such as Information Gathering tools, Vulnerability Analysis tools, Web Application Analysis tools, Database Assessment tools, Password Attacks tools, Wireless Attacks tools, Reverse Engineering tools, Exploitation tools, Sniffing and Spoofing tools, Post Exploitation tools, Reporting tools, Social Engineering tools and System Services.

Screenshot: Capturing memory using Volatility



In the command line prompt, enter the command ‘memdump’ to capture the memory. This can be loaded into a file (memorydump.txt) through ‘memdump > memorydump.txt’ command. The file can also be viewed through commands like cat or view or ‘less -10

memorydump.txt'. The volatility also displays all the processes currently running by using 'pstree' command.

Thus, FTK Imager and Volatility has the similar function to capture the memory.

Disadvantage of FTK Imager:

A hardware-based writing blocking device must be used to create a forensic image of the suspect's hard drive in order to ensure that operating system doesn't change the suspect's hard drive when it is been attached to the computer.

REFERENCES AND CITATIONS:

Bibliography

AccessData, C. (2016). *Installing FTK Imager*. Retrieved 2016, from AccessData: http://accessdata.com/product-download/digital-forensics/ftk-imager-lite-version-3.1.1

Infosec, R. (2016). *Volatility*. Retrieved from Info Sec Institute: http://resources.infosecinstitute.com/memory-forensics-and-analysis-using-volatility/

Kali. (2010, October 16). *Kali Linux Installation*. Retrieved from Kali: https://www.kali.org/downloads/

Martin, J. (Director). (2013). *https://www.youtube.com/watch?v=tFjQ9NuP33w* [Motion Picture].

Sammons, J. (2016). *Digital Forensics with the AccessData Forensic Toolkit(FTK).* McGraw-Hill Education.