VENSELVAM
REG NO:231901061

EXP NO: 1

Study of Computer Forensics and different tools used for forensic investigation

Aim :

Study of Computer Forensics and different tools used for forensic investigation

What Is Digital Forensics?

Digital forensics is the field of determining who was responsible for a digital intrusion or other computer crime. It uses a wide range of techniques to gain attribution to the perpetrator.

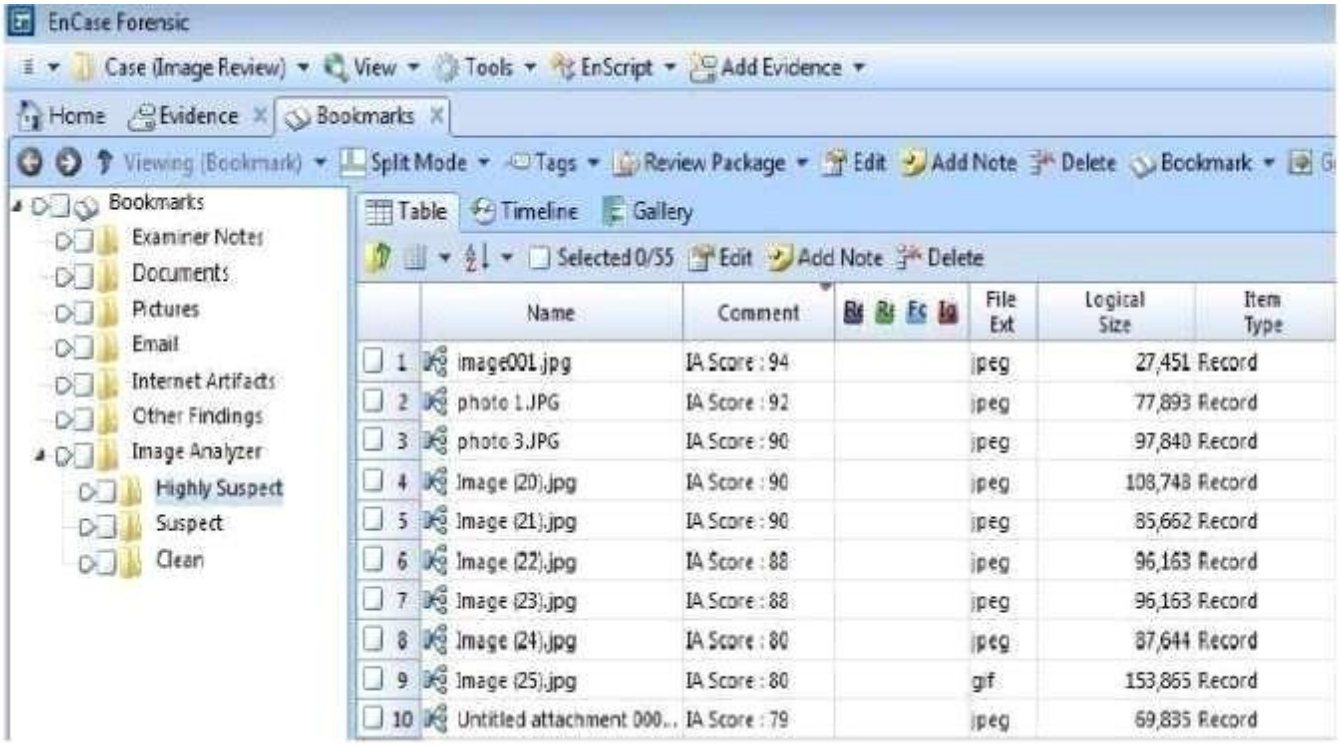
It relies upon the fundamental concept that whenever a digital intrusion or crime is committed, the perpetrator inadvertently leaves a bit of themselves behind for the investigator to find. These "bits" could be entries in log files, changes to the registry, hacking software, malware, remnants of deleted files, etc. All of these can provide clues and evidence to determine their identity and lead to the capture and arrest of the hacker.

As a hacker, the more you know and understand about digital forensics, the better you can evade the standard forensic techniques and even implement anti-forensic measures to throw off the investigator.

The Digital Forensic Tools

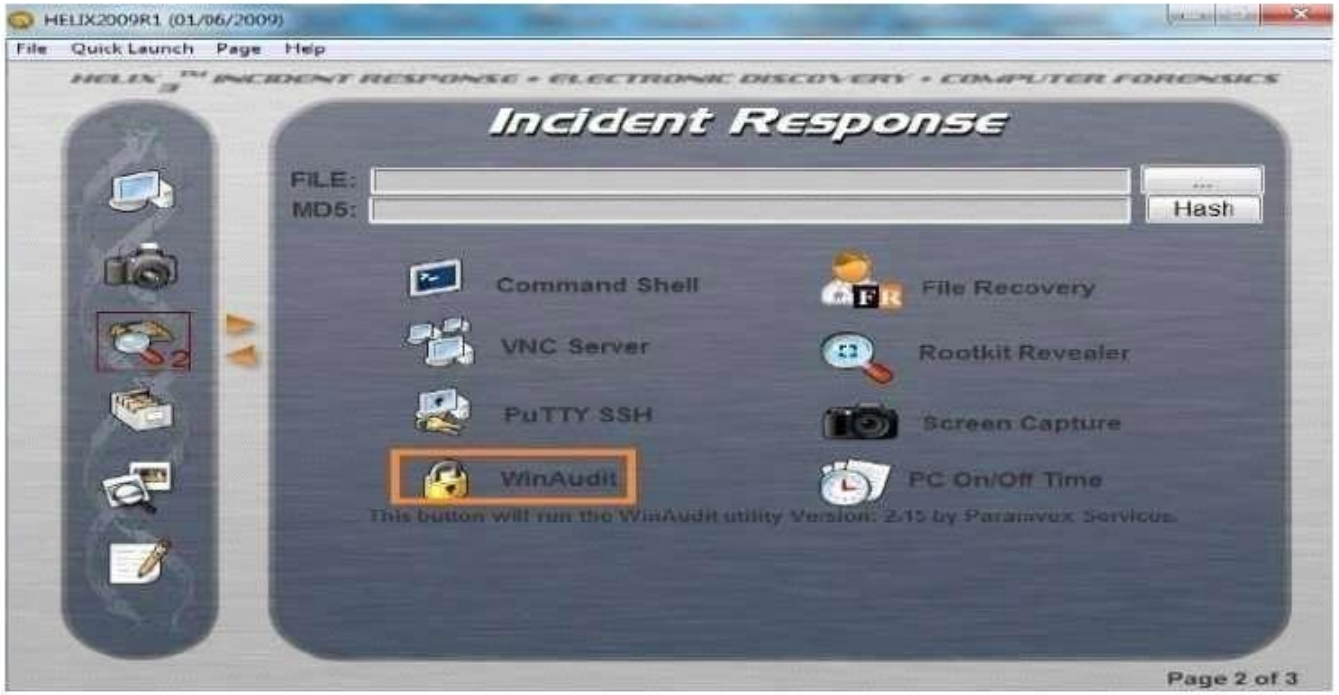
Just like in hacking, there are a number of software tools for doing digital forensics. For the hacker, becoming familiar with these tools and how they work is crucial to evading them. Most digital forensic investigators rely upon three major commercial digital forensic suites.

- Guidance Software's EnCase Forensic
- Access Data's Forensic Tool Kit (FTK)
- Prodiscover



These three suites are comprised of multiple tools and reporting features and can be fairly expensive. While these suites are widely used by law enforcement, they use the same or similar techniques as the free open-source suites without the fancy interfaces. By using the open-source and free suites, we can come to understand how such tools as EnCase work without the expense. EnCase is the most widely used tool by law enforcement, but not necessarily the most effective and sophisticated. These tools are designed for user-friendliness, efficiency, certification, good training, and reporting. There are a number of the free, open-source forensic suites, including the following three.

- The Sleuthkit Kit (TSK)
- Helix
- Knoppix



The Forensic Tools Available in BackTrack

In addition, there are a large number of individual tools that are available for digital forensics, some of which are available in our BackTrack and Kali distributions

Some of the better tools in BackTrack include the following, among many others

- sleuthkit
- truecrypt
- hexedit
- autopsy
- iphoneanalyzer
- rifiuti2
- ptk
- exiftool
- evtparse.pl
- fatback
- scalpel
- dc3dd
- driftnet
- timestomp

Forensics Field Tools

- **FTKImager**

Forensic disk imager and file recovery.

- **Log Parser Lizard GUI**

Flexible and powerful log file parser. It also does much much more.

- **Noxcivis Field Toolkit**

The Noxcivis Field Toolkit (NFT) is a free and open interface that allows forensic examiners and collection teams to collect information from a computer.

- **Active@ Partition Recovery**

Recover deleted partitions.

- **Autopsy :**

Forensics tool. Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools. It can be used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card.

Result:

Thus, the forensic tools executed successfully, and the evidence was captured and analyzed accurately.