UKACC International Conference on Control 2012
Cardiff, UK, 3-5 September 2012

# Overview on Computer Forensics Tools

Raza Hasan
Computer Engineering Department
Sir Syed University of Engineering & Technology
Karachi, Pakistan
raza_6@hotmail.com

Salman Mahmood
Computer Engineering Department
Sir Syed University of Engineering & Technology
Karachi, Pakistan
salmanm@ssuet.edu.pk

Akshyadeep Raghav
School of Computing
Staffordshire University
Stafford, UK
akshyadeep@gmail.com

***Abstract*— Different tools are used to aid the investigation process. The need of specialized software is required for the acquisition and examination of data gathered from the crime scene. To abide by chain of custody proper crime scene reconstruction or image is acquired from the original source that can be admissible to the court. This paper focuses on the various hardware and software tools that are widely used during a Computer Forensics Investigation.**

***Keywords-component; Computer; Forensics; Investigation; Hardware; Software; Crime; Tool;***

## I. INTRODUCTION

A computer crime is defined as a criminal act in which people commit the offence using the digital knowledge stored in the computer system. To investigate the computer based crime a new field of specialization - forensic computing has been developed, which is the process of computer investigation and analysis technique to gather evidence in a manner that is legally acceptable [1].

Computers and internet continue to spread and occupy our lives by increasing the potential of harm caused by it through increased number of computer crimes. To deal with this rise, new and advance methods of investigations are required. Electronic evidence in the form of data or information of investigative importance is stored or transmitted digitally by means of electronic devices. Electronic evidence by its nature is very fragile. It can be damaged, destroyed or altered by improper handling and examination. For this reason, special precautions or set of rules have to be followed in acquiring, analyzing and reporting this type of evidence, failure to do so may result an inaccurate conclusion. Electronic evidence poses special challenges regarding its admissibility in court [2].

An important tool used by investigators to safeguard evidence, is called chain of custody. Essentially, this means accounting for those who has touched a given piece of evidence, when they touch it and what they did to evidence. It's a way of demonstrating that evidence hasn't been damaged or tampered with while in the care of the investigator. In the book, Criminalistics: An Introduction to Forensic Science, Richard Saferstein notes in 7th Edition (July 31, 2000), "Failure to substantiate the evidence's chain of custody may lead to serious questions regarding the authenticity and integrity of the evidence and the examinations rendered upon it (pg. 48)." As one would imagine, changes to the chain of custody can quickly ruin a case [3].

The paper is organized as follows: Section II describes the scenerio on which the investigation focuses. Section III describes the Hardware tools used in the investigation. Section IV describes the Software tools used in the investigation. Section V concludes the paper.

## II. SCENERIO

The use of computer forensics may be able to show a pattern of activity that will aid in a lawsuit. Through the use of e-mails, deleted data, and other items found during an investigation, the computer forensics specialist can piece together a history of the prior employee's computer usage and this type of information is very useful in a court.

For example, in an Advertising company they have recently hired a new salesman. Six months after his hire, he leaves the company and forms a competing interest, sending letters or client contacts to another competitive company. The organisation might think this a bit odd and contact an attorney to consider filing a suit. What has occurred is a virtual theft; the salesman stole a copy of your client database. Note that this is a VIRTUAL theft, since you were not deprived of any property (he didn't delete it, just copied it) you will likely not be able to prosecute him criminally.

In order to prove him guilty under law the use of Computer Forensics could be put to practise. The Computer Forensics Tools are of two kinds Hardware tools and Software tools. Data recovery is as much art as it is science. Using industry standard tools, computer data once thought to be lost is restored either in full or at least in part.

When a file is deleted, the space it occupied on the hard drive is not initially overwritten. Additionally, there are snippets of data, previous versions of documents, and other content that may be scattered throughout the hard drive. Computer Forensics experts can recover the lost

data. Sometimes this is a simple undelete whereas other times it takes a considerable amount of effort to piece the file back together. In addition to recovering deleted files, we can also break password protected files (such as a Word document for example) and in some cases encrypted files [4].

In order to carry out these procedures of retrieval of data a Computer Forensics expert would use various Hardware and Software Tools, which would be discussed in next section.

## III. HARDWARE TOOLS

A Computer Forensics expert should be aware and familiar with the inside of a computer system. One should know the inside and outside of the system before they could work on the tools to retrieve data. They should have a good knowledge of the hard drives and their settings. There are many hardware tools that could be used by a Forensics expert, this section would be addressing and discussing about FRED in this chapter. FRED is the most common hardware device used by most investigators. FRED stands for Forensic Recovery of Evidence Device. The FRED families of forensic workstations are highly integrated, flexible and modular forensic platforms and now include DI's exclusive ***UltraBay Write Protected Imaging Bay***. There are a lot of versions of FRED like FRED SR, FRED L, etc... [5]

### *A. FRED System*

FRED systems are optimized for stationary laboratory acquisition and analysis. Simply remove the hard drive(s) from the suspect system and plug them into FRED and acquire the digital evidence. FRED will acquire data directly from IDE/EIDE/ ATA/SATA/ATAPI/SCSI I/SCSI II/SCSI III hard drives and storage devices and save forensic images to DVD, CD or hard drives. FRED systems also acquire data from floppies, 100/250/750 MB ZIP cartridges, CD-ROM, DVD-ROM, Compact Flash, Micro Drives, Smart Media, Memory Stick, Memory Stick Pro, xD Cards, Secure Digital Media and Multimedia Cards. Furthermore, with the optional tape drive FRED is capable of archiving to or acquiring evidence from 4mm DAT tapes. With the RAID option FRED has an incredible 1.6 TB (1600 GB) of internal RAID storage. All FRED systems include the UltraBay, custom front panel connections, and removable drive trays so there is no need to open up the processing system to install drives or crawl around the back of the unit to attach devices. Fig 1 illustrates a FRED system; its estimate cost would be $5999.00 [5].

Figure 1. FRED System [5]

#### *1) The UltraBay II*

The UltraBay II can be used to acquire a forensically sound image of IDE, SATA, SCSI, USB and Firewire using your choice of Forensic Imaging software. Furthermore, drives may be connected/ removed from the UltraBay II without having to shut down the workstation or leaving the GUI. The UltraBay II is exclusively available with Digital Intelligence FRED systems and is not available separately or from any other source. Fig 2 illustrates an UltraBay [5].


Figure 2. UltraBay II

FRED systems come with two high capacity hard drives. One of these drives is used for your forensic acquisition and processing tools and the other drive as a work drive for restoring and processing digital evidence. With multiple boot menu options FRED can be booted into data acquisition mode and PDBlock loaded automatically, write protecting the suspect hard drive.

Another boot option can be configured to place the FRED in data analysis mode with full access to your forensic analysis tools. FRED systems even come with Linux 9.1 Professional pre-configured! Both hard drives are supplied in removable trays with front panel switches for master/slave configuration [5].

FRED systems have inbuilt network functionality. All FRED systems can be connected directly to a network (10/100/1000 Mb Ethernet) for use as a standard workstation or file server when not processing or acquiring data.

The FRED Systems are usually stationary system used in the Forensics labs. There are other portable devices like the FRED – L, Ultrakit etc. FRED –L is the first laptop member of the FRED family. It as got a price tag of $4999. Though the specifications are less compared to the FRED system usually, FRED-L comes complete with an UltraKit for the ultimate mobile field forensic acquisition kit [5].

#### *2) FRED – L*

The FRED-L forensic laptop and the included UltraKit work together to quickly, efficiently, and securely image IDE, SATA, and SCSI hard drives in a forensically sound manner. FRED-L is built on the very latest and fastest Intel Core i7-2720QM (2.2GHz, 6MB L3 Cache) Processor with up to 8 GB RAM, built-in FireWire 1394a, USB 2.0, Wireless 802.11 a/b/g/n, and Gigabit (10/100/1000 Mb/s) Ethernet support. This support is provided completely via integrated laptop components and is in no way reliant on add-on or auxiliary cards or devices.

The FRED-L has inbuilt network functionality like FRED systems. FRED-L also has the ability to connect directly to a

10Mb, 100Mb, or even Gigabit Ethernet networks for use as a standard laptop when not processing or acquiring data. FRED-L also includes integrated 802.11b/g wireless capabilities. With the addition of Network Analysis software (Packet Analyzer), FRED-L can also be used to monitor network traffic and

communications at the crime scene [5]. Fig 3 illustrates the FRED-L System.

Figure 3. FRED - L

*3)* ***Ultrakit III***

The UltraKit is portable kit which contains a complete family of hardware write blockers for use in acquiring a forensically sound image of virtually any hard drive you may encounter (eSATA IDE / SATA, UltraBlock SCSI, UltraBlock USB and an UltraBlock Forensic Card Reader). The UltraKit contains all the write blockers, cables, adapters, and power supplies necessary for use in acquiring images in the field using a standard laptop with FireWire or USB support. Fig 4 illustrates the Ultrakit which comes along with the FRED-L system. An Ultrakit would cost approximately $1369.


Figure 4. Ultrakit

The UltraKit consists of a Write Protected UltraBlock-IDE, UltraBlock-SATA, UltraBlock-SCSI, and a Write Enabled UltraBlock-IDE. FRED-L is designed for use "On Location" at electronic crime scenes. Remove the hard drive(s) from the suspect system and attach them to the appropriate write blocker in the UltraKit. You can then use the FRED-L system to quickly and efficiently create your image file(s) on the acquisition drive attached to the Read/Write UltraBlock. Using the Read/Write UltraBlock device allows you to utilize faster, larger, less costly desktop drives to receive your forensic images. No more worrying about the problems encountered trying to configure parallel devices on suspect equipment in order to use external backup devices. No worries about installing a SCSI adapter into a suspect's computer [5].

With multiple boot menu options, FRED-L is not limited to use as a Forensic Imaging tool. FRED-L can be booted into DOS 6.22, Windows 98 (Standalone DOS), or Windows XP and Windows 7 and will support any forensic tools which run within those environments. FRED-L also comes complete with a fully configured installation of Suse Linux 9.1 Professional. Capable of configuration with the fastest Intel Centrino Pentium-M mobile processors (2 GHz and beyond), and with an impressive memory capacity (up to 2 GB), FRED-L is also a very formidable processing platform.

There are many more hardware devices that are used for investigation purposes like UltraBlock Forensics card reader, Image MASSter Solo, FastBloc, Acard, etc... , Each Hardware device as its own functionalities and depending on the investigation scenario the hardware's is used. Hardware required for computer forensics include workstations and blockers such as write blockers needed to prevent contamination of evidence [6].

## IV. SOFTWARE TOOLS

The Software Tools used in Computer Forensics is usually based on the type of investigation that is carried out. If it is a data recovery investigation then Data Recovery Tools are used, each software tools as its own purpose and its own results. Computer forensics software tools would be characterised into Data Recovery Tools, Partition Tools, Disk Clone Tools, Recovery Tools, Testing Tools, RAM Test utility, System Speed Test, Hard Disk Tools, System Information Tools, Dos Tools and Other Tools. Each Tool as a variety of software's below is few examples of and some description on them. The tools are listed below according to the category of the job.

### *A.* ***Stealth™ Suite***

The Stealth™ Suite is used to assess activity on a computer hard disk drive without the user needing a forensic background. This set of tools helps identify whether or not a targeted computer system was used to access inappropriate information [7] [8].

### *B.* ***Computer Incident Response Suite***

These suites of tools are often used in corporate and government investigations and security risk reviews. This suite is optimized for the lowest cost forensic platform for DOS and Windows processing, DOS. Many of the tools also have version that can be run on a Windows OS. This should be one of your first forensic toolsets. It also makes an excellent set of tools to cross-validate your findings before you go before the court or the board [7] [8].

### *C.* ***Data Elimination Suite™***

This Suite allows you to remove information from a drive and cross-validate that the information has been removed.

This is our most popular suite of software tools for the high assurance government or corporate environment. This suite of tools has been tested and certified by the US Department of

Defence. It eliminates classified data 'leakage' and verifies that the data was properly eliminated [7] [8].

### *D. TextSearch Suite*

TextSearch NT and TextSearch Plus have both been upgraded. TextSearch NT is used to process Windows NT/2000/XP-based computer systems from a DOS command line. The upgraded program provides the same popular interface and features as TextSearch Plus but it identifies many compressed and graphics files using the file header signature, giving the investigator a listing of files that could store information in a compressed or graphic format.

Also included in this suite is HexSearch. This tool provides a similar interface as TextSearch Plus while allowing the user to search for hexadecimal strings, such as file headers, non-printing characters, and more [7] [8].

### *E. NTI Secure ToolKit*

This software is used to secure sensitive files stored on portable and desktop computers. Because it uses NIST tested and approved AES 256 encryption, it qualifies for government use with classified 'Secret' level data. This software exceeds commercial security requirements and it is much easier to use than PGP. It includes a management tool so that corporate information is not lost to the corporation. An export license may be required for locations outside the United States [7] [8].

### *F. SafeBack 3.0*

The industry standard for making evidence grade bit-stream backups of hard drives has gotten even better with version 3.0 [7] [8].

### *G. Guidance Software Encase*

Most of the software's are packed in suites. EnCase Forensic has become the industry standard tool for uncovering, analyzing and presenting forensic data. Used by investigators in law enforcement, government, small businesses, consulting firms and corporations, EnCase Forensic provides a robust way to authenticate, search and recover computer evidence rapidly and thoroughly.

Computer evidence recovered with EnCase has been admitted into thousands of court proceedings in several countries and jurisdictions, and the EnCase software has been validated by the courts in several published decisions. [CGFI] The following are the advanced features of EnCase:

- Extracts messages from Microsoft PST files.
- Spans multiples Redundant Array of Inexpensive Disk (RAID) volumes.
- Supports NTFS compression and Access Control List (ACL) of files.
- Provides advanced language support.

Several software vendors have recently introduced computing investigation tools that work in Windows. The command line DOS tools you explored in the previous section require a strong understanding of MS-DOS and the various file systems. Because GUI (Graphical User Interface) forensics tools do not require the same level of knowledge, they can simplify computer forensics investigations. These GUI tools have also simplified training for beginning examiners in computer forensics. However DOS forensics should also be known because there are rare cases when the GUI tool would miss out critical evidence and this could be got using a DOS tool [7][8][9].

## V. CONCLUSION

This paper focuses on the most essential and widely used Hardware tools, there are many more tools used but the main focus was on mainly the ones that are quite common. Also, discussed on the Software tools used but not in depth, as the paper focuses on mainly the ones that are quite common in a Computer Forensics Investigation as there are other softwares as well but due to the scope of this paper it was inadequate to cover all the software tools, given a brief description of a few software's that are used for evidence collection.

The paper attempts to give the audience to increase the level of understanding with the wide range of tools used for Computer Forensics Investigations.

## ACKNOWLEDGMENT

Special thanks to all other faculty members for helping during the research and giving their valuable suggestion and guidance.

## REFERENCES

[1] Hasan, R.; Raghav, A.; Mahmood, S.; Hasan, M.A.; , "Artificial Intelligence Based Model for Incident Response," *Information Management, Innovation Management and Industrial Engineering (ICIII), 2011 International Conference on* , vol.3, no., pp.91-93, 26-27 Nov.2011.
doi:10.1109/ICIII.2011.307
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6114714&isnumber=6114683

[2] J. Ashcroft, "*Electronic Crime Scene Investigation: a Guide for LawEnforcement*", 2001.

[3] J. Rory, "Practical Handbook For Private Investigators", ISBN 0-8493-0290-0 Timothy E. Wright, 2000, Field Guide, 2001.

[4] J. Nerlinger, Jr., Jatero Consulting & Development, URL:http://www.jatero.com, retrieved 23 December 2011.

[5] Digital Intelligence, URL:http://www.digitalintelligence.com, retrieved 23 January 2012.

[6] Bill Nelson, Amelia Phillips, Frank Enfinger, Chris Steuart, *Computer Forensics and Investigation*, Cengage Learning, 2010 ISBN: 1435498836, 9781435498839.

[7] J. Wiles, K. Cardwell, A. Reyes,*"The Best Damn Cybercrime and Digital Forensics Book Period"*, 1st Edition, Syngress, 26 Nov 2007, ISBN: 9781597492287.

[8] D. Shinder; M. Cross;, "*Scene of the Cybercrime*", Syngress, 2 edition, June 20, 2008, ISBN: 978-1597492768.

[9] A. Phillips; B. Nelson; F. Enfinger; C. Steuart, "*Guide to Computer Forensics and Investigations*", Course Technology, 2nd edition, September 28, 2009 , ISBN:978-0619217068.