DIGITAL FORENSICS TOOLS

Gennifer Dominic[1], Shivkumar Goel[2]

[1]PG Student, Vivekanand Education Society's Institute of Technology, Dept. of MCA, Mumbai, India
[2]Deputy HOD/Assistant Professor, Vivekanand Education Society's Institute of Technology, Dept. of MCA, Mumbai, India

***

Abstract - *Computer use has grown, and computer crime has also risen at the same time. This article will tackle a very significant topic in the computing world, even more so provided that the Data Forensics field has had tremendous development over time. The immense meaning and quality of the information that is stored in a computing system on a single hard disk create considerable concern in certain people who commit immoral activities such as fraud and modification of information by the use of the Internet as a large network. These techniques used in Computer Forensics are technologies or essential software devoted to collecting information for use as proof or evidence needed by any legal action, where the major crime scenes may be assumed to be the computers and the network it is linked to. Therefore, continue to evaluate methods that fulfill criteria and functions in the above field only for processes. This work is thus based on an empirical, bibliographic, statistical, and correlational study; as it has gathered accurate knowledge from literature sources such as books and academic papers; besides providing a robust methodological method.*

***Key Words*: Digital Crime, Computer Forensic, Security, Risks, Information.**

1. INTRODUCTION

Computer crime is defined as a criminal act in which people commit the offense using the digital knowledge stored in the computer system. To investigate a computer-based crime a new field of specialization - forensic computing has been developed, which is the process of computer investigation and analysis techniques to gather evidence in a legally acceptable manner. [1]. As technology has advanced, all processes have been automated thanks to the exponential development of computer software and the great protection of digital information storage devices or networks, but several types of vulnerabilities are also reported, which should be treated with great caution to avoid cyber fraud victims[6]. New and advanced investigative approaches are required to tackle this increase. Electronic content, in the form of investigative data or information, is processed or digitally distributed by electronic devices. In its definition, the electronic proof is very fragile. Inappropriate handling and inspection can damage, kill, or change it. For this purpose, in collecting, evaluating, and recording this form of data, specific measures or collection of guidelines must be followed; failure to do so may result in an incorrect inference. That is why the Digital Forensics' role is of tremendous significance because, since its inception, it has acted as help to justice today, it faces obstacles and guarantees the facts by evidence or electronic proof that may become a major part in a judicial proceeding. It will also encourage any accident to be corrected more quickly and will prevent repeated incidents in the future.

2. Hardware Tools

A specialist in data forensics would be aware of the interior of a computer network and learn it. Before they could operate on data retrieval software, one could know the inside and outside of the system. They should know the hard drives well and their configurations well. A Forensics professional may use several hardware devices, FRED is the most popular hardware system used by most investigators. FRED stands for Proof Computer retrieval forensics. The forensic workstation FRED families are tightly interconnected, scalable, and modular forensic systems.

2.1 Fred System

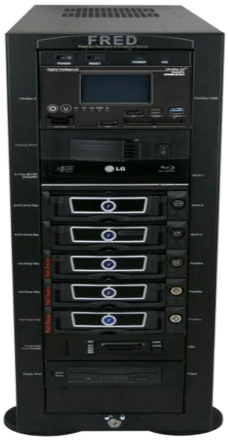
FRED devices are designed for collection and analysis at stationary laboratories. Simply detach and plug the hard drive(s) into FRED from the suspect device and collect digital evidence. FRED can collect data directly from hard drives and storage systems IDE / EIDE / ATA / SATA / ATAPI / SAS / Firewire / USB and store forensic images on Blu-Ray, DVD, CD, or hard drives.

Also, FRED is capable of archiving or collecting information from DLT-V4 tapes with the available tap drive. Both FRED systems have UltraBay connections, front panel connections, and interchangeable drive trays, and there is no need to open the operating door to mount drives or crawl around the device's back.

2.1.1 Dual Xeon Quad Core Speed (8 Processors)

Traditionally, dual processor device architectures have been "application-centric" with aging chipsets, low memory capacity, low I / O capacity, and minimal peripheral support. Digital Intelligence has developed the first Dual Processor device with all the performance, reliability, and stable specifications of a Forensic Evidence Recovery System (FRED) [2].

This machine is based on a 64-bit Xeon Motherboard dual-processor with excellent versatility, optimized peripheral support, and performance well above anything commonly seen in a Forensic Workstation.



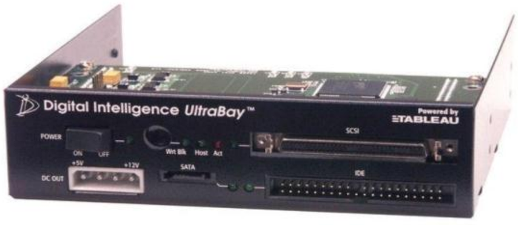
[Fig 2.1.1]

During the imaging cycle selected FRED systems to use our ventilated image shelf for full drive cooling:

- Integrated Retractable picture shelf (when not in service, it retracts entirely to the system).
- Dual ventilators for full surface coverage and cooling.
- Turn on / off to monitor airflow.

2.1.2 The UltraBay II

Using your choice of Forensic Imaging tools, UltraBay 11 will acquire a forensically sound image of IDE, SAT A, SCSI, USB, and Firewire. Additionally, drives can be connected/removed from UltraBay IT without the need to shut down the workstation or leave the Interface. The UltraBay 11 is available exclusively with FRED Digital Intelligence systems and is not available independently or from any other source[1].



[Fig 2.1.2]

Two high volume hard drives come with FRED systems. One of such drives is used as a working drive to retrieve and process recorded evidence with the forensic collection and retrieval equipment, and the other drive. FRED can be booted into data acquisition mode with several boot menu options, and PDBlock enabled automatically, writing to secure the suspect hard disk.

With complete access to your forensic analysis software, you can configure another boot option to put the FRED in the data analysis model. FRED devices only come with pre-configured Linux 9.1 Professional! For master/slave setup, both hard drives are supplied in removable trays with front panel switches.

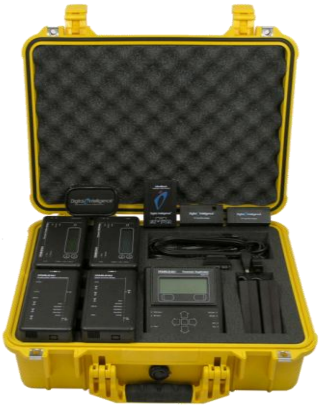
The FRED systems are typically stationary devices that are used in Forensics laboratories. There are other mobile apps such as FRED-L, Ultra kit, etc. FRED -L is the FRED family's first Laptop leader. Although the requirements are generally fewer compared to the FRED device, FRED-L comes complete with an UltraKit for the ultimate handheld field discovery forensic kit.

2.1.3 Ultrakit III

The UltraKit III is a compact kit that contains a full family of UltraBlock hardware writes blockers along with adapters and connections that can be used to create a forensically sound picture of nearly any hard drive or storage unit you may encounter.

Just pick the correct Write Secured UltraBlock and add it to the source drive, and use your desktop or laptop to provide a forensically secured disk file to an internal drive or externally attached computer enclosure.

The UltraKit consists of a Write Safe UltraBlock-l DE, UltraBlock-SAT A, UltraBlock-SCSI, and a Write Enabled UltraBlock-iDE. FRED-L is intended to be used on electronic crime scenes "On-Site" Delete the hard drive(s) from the suspect device, and connect them in the UltraKit to the correct write blocker. On the acquisition drive connected to the Read / Write UltraBlock, you can then use the FRED-L program to build your image file(s) easily and efficiently.



[Fig 2.1.3]

There are several other hardware tools, such as UltraBlock Forensic card reader, Photo MASSter Solo, FastBloc, Acard, etc. Each hardware interface is used as its software and the hardware is used depending on the situation of the investigation. Hardware available for computer forensics involves workstations and blockers including write blockers needed to avoid proof contamination.

3. Software Tools

3.1 EnCase

EnCase Forensic, the industry-standard solution for computer science, is for forensic professionals who need to use a repeatable and defensible procedure to perform reliable, forensically sound data collection and investigations. The tested, successful, and trustworthy EnCase Forensic software allows reviewers to gather data from a wide range of resources, discover potential information at the disc level through forensic analysis, and produce comprehensive reports on their findings while maintaining the information's credibility[3].

Features

- Acquire from Almost Anywhere: Acquire data from disk or RAM, records, images, email, webmail, site objects, web history and cache, restoration of HTML pages, chat sessions, compressed files, backup files, encrypted files, Attacks, workstations, servers, and version 7: smartphones and tablets.
- Advanced Analysis: Recover files and partitions, detect deleted files by parsing event logs, analyzing file signatures and hash analysis, even in compounded files or unallocated disc space.
- Improved Productivity: Examiners should be able to display reports as data is being processed. Once the image files have been created, examiners can simultaneously search for and analyze multiple drives or media.

3.2 X-Ways Forensics:- Integrated computer forensic software

Forensics on X-Ways is an innovative operating method for computer forensic examiners. Runs under the XP/2003/vista/7/8.1/2012*,32 Bit/64 Bit, Standard / PE / FE variant. Similar to its rivals, X-ways forensics is more effective to use for a while, always run quicker, is not as resource-hungry, discovers missing files, and scan hits that the rival will lack[4]. It's made by the German industry and it comes at a fraction of the size! X-Ways forensics is fully portable and runs a USB stick without installation on any given Windows system. XWays Forensics is based on the WinHex hex and disc editor and is part of an effective working flow model where computer forensic examiners exchange data and use XWays investigators to communicate with researchers.

X-Ways Forensics manages your cases separately and will allow you to identify all sources and pieces of evidence related to your case. It creates a tree-like structure for each of your cases where you can freely add drives, images, and any other file. For every item, notes and pieces of evidence found will be recorded separately.

Features

- Disk cloning and imaging.
- Partitioning and file system architectures can be read inside raw (.dd) image files, ISO, VHD, VHDX, VDI, and VMDK images.
- Complete access to drives, RAIDs, and photographs larger than 2 TB in size (more than 232 sectors) with sector sizes up to 8 KB.
- Superimposition of sectors, e.g. with corrected partition tables or file system data structures to parsing file systems completely despite data corruption, without altering the original disk or image.
- Different methods for data recovery, lightning-fast, and efficient carving of files.

3.3 Forensic ToolKit (FTK)

FTK is also a window-based automated forensic software that can create forensic backups and "delete" the evidence, FTK is simple to use and allows an investigator the ability to access Current, Latent, and Archival data without changing the evidence. Law enforcement also makes heavy use of FTK to process digital data.

FTK is a court-accepted platform for automated investigations, designed for speed, automation, and scalability of the business level. Known for its elegant interface, email review, personalized views of data, and reliability, FTK offers the foundation for smooth expansion such that the computer forensics system will expand with the needs of the business.

It gives investigators an aggregation of the most common forensic tools in one place. Whether you are trying to crack a password, analyze emails, or look for specific characters in files, FTK has got you covered[5].

Features

- Easy-to-use GUI with automated preprocessing of forensic data.
- Flexibility: Available as a perpetual or subscription license.
- Comprehensive: volatile memory analysis.
- Add-on Cerberus: for automated malware analysis and triage.
- Password cracking: through PRTK/DNA.
- Visualization: capabilities allow a graphic analysis of file and email data.

4. CONCLUSION

This paper focuses on the most essential and widely used hardware tools and software tools, many more tools are used, but mainly those that are quite common were the main focus. Also discussed on the software tools used but not in detail, as the paper focuses primarily on those that are very typical in a Computer Forensics Investigation when there are other applications as well, but due to the nature of this paper, it was impractical to cover all the software tools, despite a short overview of certain devices that are used to gather evidence.

REFERENCES

[1] R. Hasan and S. Mahmood, "Overview on Computer Forensics Tools," p. 5.

[2] "Digital Intelligence's FRED DX." https://www.insectraforensics.com/Digital-Intelligences-FRED-DX/en.

[3] "EnCase Forensic V7, Forensic Analysis Tool | SECURE INDIA." https://www.secureindia.in/?page_id=1105.

[4] S. Preeti, "Tool and Techniques for Computer Forensics."

[5] "FTK Forensic Toolkit Overview," Infosec Resources. https://resources.infosecinstitute.com/category/computerforensics/introduction/commercial-computer-forensics-tools/ftk-forensic-toolkit-overview/.

[6] N. Loja, R. Morocho, and J. Novillo, "Digital Forensic Tools."