IJoFCS (2015) 1, 29-51

The International Journal of
FORENSIC COMPUTER SCIENCE

www.IJoFCS.org

DOI: 10.5769/J201501004 or http://dx.doi.org/10.5769/J201501004

Digital Forensics Analysis for Data Theft

P.S. Lokhande[1] and B.B. Meshram[2]

(1) http://pslokhande.blogspot.in, E-mail: pslokhande@gmail.com

(2) E-mail: bbmeshram@vjti.org

Abstract:Cyber Criminals are using various techniques to attack on computing systems. Not only the professionally Cyber Criminals but also white collar IT employees are also involved in the valuable data theft. Some of the motives behind the data theft are revenge on employer, higher pay offered by a competitor company, or selling valuable data, etc. This work gives step by step approach implemented to extract the digital evidence from the computing systems of employee by whom the data theft is made. The employee used the Windows operating systems and the data in MS word format and excel format was sent to the competitor company by email and the data was also copied from the computer to the pen drive of the employee and then it was deleted from the company's computer. The extensive literature survey is made on Digital Forensic Analysis Process, Digital Forensic Model and various tools and hardware required for forensic set up. We have simulated the investigation process to get the evidence from the suspected employee's computer.

Key words: Digital Forensic, Digital Evidence, Cyber Crime, Indian IT ACT 2000, Forensic tools, Data Theft..

I. Introduction

Data theft is a growing phenomenon primarily caused by system administrators and employees who all are accessing technology such as database servers, desktop computers and devices capable of storing digital information, such as USB flash drives, iPods and even digital cameras. Since employees often spend a maximum amount of time developing contacts, business logic and confidential copyrighted information for the company they work for, they may feel they have some right to the information and are inclined to copy and/or delete part of it when they leave the company, or misuse it while they are still in employment. While most organization have implemented firewall and intrusion detection system, very few take into account the threat from the average employee that copies proprietary data for personal gain or use by another company. A common scenario is where a sales person makes a copy of the contact database for use in their future job.

The Examples of Common Data Theft are as below:

1. Forwarding emails to personal email id from corporate IDs.

Paper submitted on: December 27th, 2015

2. Sending files as attachments from corporate ids with malafide intentions.
3. Copying data on pen drives from computers without the permission of the owner.
4. Selecting, copying and pasting data from websites for financial gain.
5. Helping people to commit offense of Data Theft.
6. Selling or exposing the valuable research in Science and Engineering to the competitor company.

Typically, this is a clear violation of their terms of employment or organization policy about the security of the data.

Section 43(B) of IT Act: According to the amended Information Technology Act, 2000, Crime of data theft under Section 43(B) is stated as- If any person without permission of the owner or any other person who is in charge of a computer, computer system of computer network, downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network or when any information in the form of data is illegally copied or taken from a business or other individual without his knowledge or consent, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. But for such offenses employer must produce Digital Evidence about the suspected employee [1].

Section 66 of IT Act: If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both [1].

2. Literature Survey

2.1 Digital Forensic Process

Digital Forensic Evidence Collection process provides the sequence of evidence collection, it consists of 4 steps as follows [2].

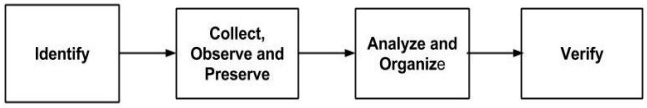

Figure 2.1 Digital Forensic Process Model for Collecting Digital Evidence

i) Identify: Any digital information or artifacts that can be used as evidence. Forensic Examiner first need to identify the Digital equipment such as Computer, Laptop, Mobile phone, iPod, Digital Camera, Storage Drive etc.

ii) Collect, observe and preserve the evidence: Second step consists of collection of seized digital evidence, observation of findings and then preserve in the prescribed format.

iii) Analyze, identify and organize the evidence. : Third stage consists of Analysis of collected digital Evidence, identification of collected Evidences according to the importance of crime and finally Organize the evidence in various categories such as (Browser files, System Log, Windows Registry etc.)

iv) Rebuild the evidence or repeat a situation to verify the same results every time: Verification of collected evidence is an important aspect of digital forensic

2.2 Digital Forensic Analysis Model

Digital Forensic Analysis Model consists of two main elements i) Network Forensics and ii) System Forensics. In Network Forensics IP Tracing, Network Devices Forensics (Router, Switches, Firewall and IPS/IDS Devices) and Session Forensics are suggested. In system forensics five sub-models are suggested a) Browser Log b) Digital Media Forensics c) Memory Forensics d) BIOS forensics f) OF Forensics, which is explained as follows.

a) Browser Log: This is important to get the user browsing history over the internet it provides User History, Cookies, Temporary accessed files and Recent Searches.

b) Digital Media Forensic: All storage media such as HDD, CD, Floppy and Flash Drive holds the digital data which can be seized

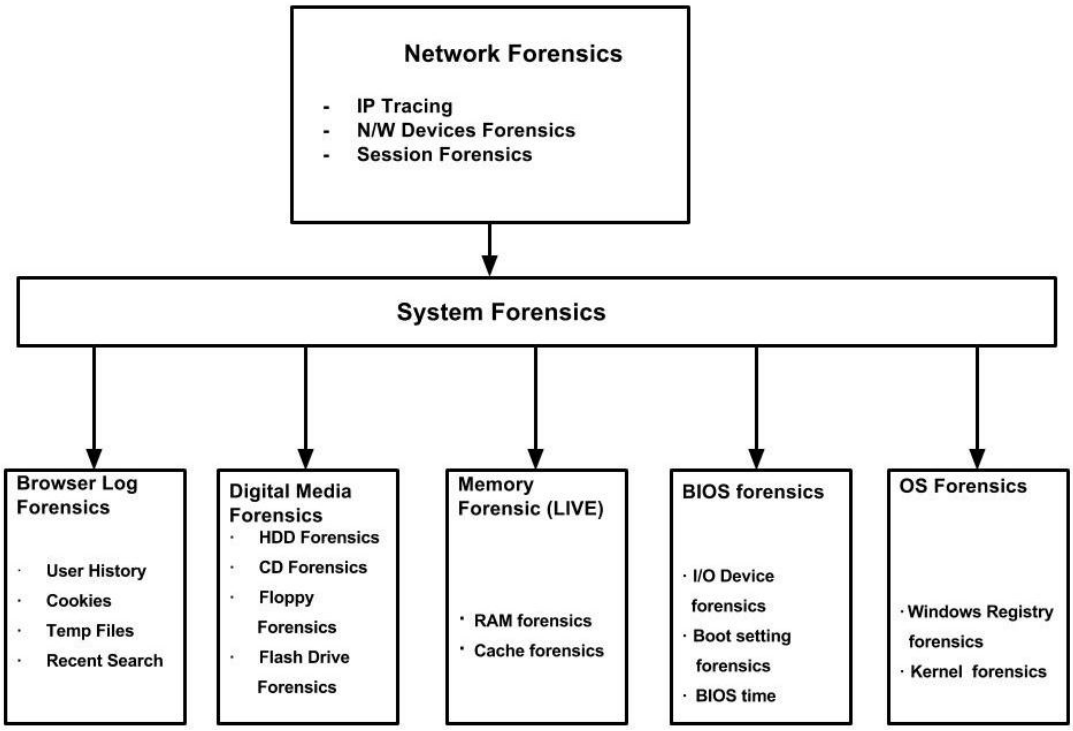

Figure 2.2 Proposed Digital Forensic Model

by accessing HDD Forensics, CD Forensics, Floppy Forensics, and Flash Drive Forensics.

c) Memory Forensics (Live): Computer memory is volatile memory, such as RAM and Cache, to collect the Digital Evidence one must ensure that it should be collected live.

d) BIOS Forensics: It involves collection of Evidence from the BIOS using I/O Device forensics, Boot Setting Forensics and BIOS time.

e) OS Forensics: Operating system of the computing machine is an important source of information, where investigator can get the digital evidence through Windows Registry, Event Viewer Log and doing kernel forensics.

2.3 Tools Available to Collect Digital Evidence

Various tools are used in the extraction of digital evidence from the victim's computer. The tools available in the market are of two types Proprietary tools and open source tools. Some proprietary tools come with hardware attachment. Computer forensics tools classified into various categories some of them mostly used as follows.

2.3.1 Popular Open Source Tools for Forensic Analysis

1) Wireshark: It is open source TCP/IP packet capturing tool used to analyze the traffic in network. Wire shark help you to see what's happening on your network at a microscopic level, Price: Freeware, Vendor: Wire shark Foundation, https://www.wireshark.org/ [4].

2) The Sleuth Kit : It is a collection of command line tools and a C library, which provide user to analyze disk images and recover files from them, Price: Open Source, Vendor: Brian Carrie http://www.sleuthkit.org/ [5].

3) SANS Investigative Forensics Toolkit – SIFT: SANS Investigative Forensics Toolkit or SIFT is a multi-purpose forensic operating system which comes with all the necessary tools used in the digital forensic process. Price: Open source, Vendor: SANS Institute, www.sans.org [6].

4) Volatility: Volatility is the memory forensics framework. It used for incident response and malware analysis. With this tool, you can extract information from running processes, network sockets, network connection, DLLs and registry hives. It also has support for extracting information from Windows crash dump files and hibernation files. Price: Open Source, Vendor: Volatility Foundation. http://code.google.com/p/volatility/ [7].

5) CAINE (Computer Aided INvestigative Environment): It is Linux Live CD consists of many digital forensic tools. CAINE has user-friendly GUI, semi-automated report creation and tools for Mobile Forensics, Network Forensics, Data Recovery and more. Price: Opensource, Vendor: Italian GNU/Linux live distribution created as a Digital Forensics project. http://www.caine-live.net/ [8].

6) REGA : Developed by Korea University. Performing collection and analysis of the windows registry hives (GUI application). Price: Freeware, Vendor: Korea University. http://forensic.korea.ac.kr/tools/ [31]

7) Mandiant's Memoryze: Mandiant's Memoryze™ is free memory forensic software that helps incident responders find evil in live memory. Memoryze can acquire and/or analyze memory images and on live systems can include the paging file in its analysis. Price: Freeware: Vendor: Mandiants https://www.fireeye.com/services/freeware/memoryze.html

8) WEFA Tool: Tool developed by Korea University for collection and analysis of the windows web browser (GUI application) Price: Freeware, Vendor: Korea University http://forensic.korea.ac.kr/tools/wefa.html [31]

9) Xplico: Xplico can extract an e-mail message from POP, IMAP or SMTP traffic. Also supports HTTP, SIP, IMAP, TCP, UDP protocols Price: Opensource, Vendor: Xplico http://www.xplico.org [38]

10) MySQL Dump: It is a backup program. It can be used to dump a database or a collection of databases for backup or transfer to another SQL server Price: Opensource, Vendor: Open source Community. www.linux.org

2.3.2 Popular Proprietary Tools for Forensic Analysis

1) ProDiscover Basic: It is a simple digital forensic investigation tool that allows you to image, analyze and report on evidence found on a drive. Once you add a forensic image you can view the data by content or by looking at the clusters that hold the data. Unit Price $50.00, Vendor : The ARC Group, http://www.arcgroupny.com/products/prodiscover-basic/ [9].

2) EnCase: EnCase is multi-purpose forensic platform with many tools for addressing several areas of the digital forensic. This tool can gather data from various devices and unearth potential evidence. It also produces a report based on the evidence. Price: $3,594/- for Ver 7,Vendor: Guidance Software. https://www2.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx [10].

3) Registry Recon: Registry Recon is registry analysis tool. It extracts the registry information from the evidence and then rebuilds the registry representation. It has capability to rebuild registries from both current and previous Windows installations. Price: $599/-, Vendor: Arsenal Recon. https://www.arsenalrecon.com/apps/recon/ [11]

4) Computer Online Forensic Evidence Extractor (COFEE): Computer Online Forensic Evidence Extractor or COFEE is a tool kit developed by Microsoft to gather evidence from Windows systems. It can be installed on a USB pen. Put USB device in the target computer and it gives live analysis. Price: Free to Law and Enforcement Agencies, Vendor: Microsoft. https://cofee.nw3c.org/ [12] and it is not sold to other agencies.

5) HELIX3: HELIX3 is a live CD-based digital forensic suite created to be used in incident response. It comes with many open source digital

forensics tools including hex editors, data carving and password cracking tools. Price: $239 for Pro version, Basic Version is Free, Vendor: E-Fense. http://www.e-fense.com/products.php [13].

6) FTK: It is a multi-purpose tool, FTK5 is a court-cited digital investigations platform built for speed, stability and ease of use. Price: $3995 but basic version is Freeware, Vendor: Forensic Data. http://accessdata.com/ [14].

7) Sqlite: It is database forensic tool used to browse Information from different Sqlite Files .db, .db3, Sqlite, Sqlite3, .fossil, Price: $149.00, Vendor: Freeviewer Software http://www.freeviewer.org/sqlite/forensics/

8) Dump it : This is HDD forensic tool. Dump it generates physical memory dump of Windows machines, 32 bits 64 bit. Can run from a USB flash drive. Price: $190, Vendor: Moon Sols. http://www.moonsols.com/2011/07/18/moonsols-dumpit-goes-mainstream/ [37].

9) NetAnalysis: NetAnalysis® v2 is the industry leading forensic software for the extraction and analysis of Internet browser trace evidence. Used to extract the evidences from Internet Browser. Price: $ 700 approx, Vendor: Digital Detective Group.http://www.digital-detective.net/

10) Aid4Mail: Aid4Mail is a fast, accurate, and easy-to-learn email forensics software provides detailed report and analysis. Price: $299, Vendor: Fookes Software, http://www.aid4mail.com/ [39]

2.4 Tools to Detect the Tempering of Multimedia Data

Multimedia data consists of Text, Image, Audio, and Video which is vital source of digital evidence, there may be chance to alteration or tempering of the data. Some of the tools and techniques available to identify the tempering of multimedia data are as follows.

i) Amped Authenticate. It is image authentication software that offers a complete suite of powerful tools to determine whether an image is an unaltered original, an original generated by a specific device, or the result of manipulation with photo editing software. Price:$46.99 vendor: Amped Software.www.ampedsoftware.com [32].

ii) Checksum: Forensic tool for verification of file content for change. BLAKE2, SHA1 and MD5 hashes are used to verify that a file or group of files has not changed. Price: Freeware, Vendor: Microsoft. www.microsoft.com/en-in/download/details.aspx [35]

iii) File Checksum Integrity Verifier (FCIV) utility: The File Checksum Integrity Verifier (FCIV) is a command-prompt utility that computes and verifies cryptographic hash values of files. FCIV can compute MD5 or SHA-1 cryptographic hash values. These values can be displayed on the screen or saved in an XML file database for later use and verification. Price: Freeware, Vendor: Microsoft [36]

2.5 Digital Forensic Lab Setup

Various hardware equipments are available for field forensic analysis. These hardware equipments are the handy kit for the forensic analyzer, this kit consists of hardware components required for data backup, recovery and imaging. Forensic Hardware kit consists of various posts to facilitate communication to external network or system. Some of the Forensic analysis and acquisition tools available in market are as follows.

a) Hardware Peripherals
b) Forensic Software Applications
c) Evidence Collection Equipments
d) Evidence Preservation Devices
e) Digital Data Investigation Kits
f) Other Assembly Tools
g) The Data Transmission Cables / Connectors

a) Hardware Devices

Digital Forensic Lab.

Roadster Forensic Workstation: This is complete forensic work station, provides data acquisition and analysis facility. This computer forensic

system is built for the road with all the tools necessary to acquire or analyze data from today's common interface technologies including FireWire 1394A/B, USB, IDE, SATA and SCSI.

Figure 2.4 Roadster Forensic acquisition and analysis tool.

With features such as multiple media support, multiple capture mode support, on the fly hashing capabilities, powerful processor for analysis, the Roadster is a versatile and powerful Forensic tool. Cost of the Roadster Forensic acquisition and analysis tool is $75,000/- Vendor: Roadstar [33].

A small digital forensic investigators lab could be limited to one multipurpose forensic works station such as Roadstar and two basic workstations. Investigator can use laptop with Fire Wire (IEEE 139B Standard), USB 2.0 or PCMCIA SATA HDD to create lightweight, mobile forensic workstation. Forensic Tower II X99: The Forensic Tower II X99 includes the NEW Tableau T35689iu Forensic Drive Bridge. The Forensic Tower II comes with a 22" LCD monitor, an Intel® i7 5820k 3.5GHz processor, 32GB of RAM, and additional drives for case and temp locations. Price:$6599, Vendor: Forensic Computers. http://www.forensiccomputers.com/forensic-tower-ii-x99.html.

FREDL: is Forensic Recovery of Evidence Device - Laptop. FREDL is the ultimate solution in mobile forensic imaging convenience and includes UltraKit - the preferred mobile forensic acquisition solution. Latest FREDL can be upgraded to utilize up to 3 internal drives; OS, DATA and an M.2 SSD for cache/database when using Encase or FTK. Price $4999, Vendor: Digital Intelligence. http://www.digitalintelligence.com/products/fredl/

Figure 2.5 Forensic Tower II X99

Figure 2.5 FREDL Mobile forensic imaging Laptop

Cellebrite : The CelleBrite UFED Forensics system is the ultimate standalone device which can be used in the field as well as the forensic lab. The CelleBrite UFED can extract vital data such as phonebook, pictures, videos, text messages, call logs, ESN and IMEI etc. The UFED supports CDMA, GSM, IDEN, and TDMA technologies, and it is compatible with any wireless carrier. The CelleBrite UFED system supports 95% of all cellular phones in the market today, including Smartphones and PDA devices (Palm OS, Microsoft, Blackberry, Symbian). It requires no PC for field use, and can easily store hundreds of phonebooks and content items onto an SD card or USB flash drive The CelleBrite UFED supports all known cellular device interfaces, including serial, USB, infrared, and bluetooth. There is no external software is required, all the functionalities and software are provided inbuilt. Price $13450, Vendor: Cell Brite, http://www.itechdataforensics.com/cellebrite.html.

Figure 2.6 Cellbrite used for cell phone forensic

Deskster Forensic Workstation: The Deskster Forensic Workstation with Dual Xeon Quad Core Processor sets the standard for forensic laboratory systems. The Deskster Forensic Workstation is compatible with all commercial forensic acquisition and analysis software besides Access Data Forensic Tool Kit, which has been provided along with the workstation.
Main features: High speed forensic tool with Drive interfaces IDE, SATA, SCSI, SAS, USB, 1394A/B. Ruggedized Design: Built for the workstations, Large Dual Display 23" wide color, 10TB Raid. Price: $8999, Vendor: Deskster, http://www.itechdataforensics.com/products.html.

Figure 2.7 Deskster Forensic Workstation

Input Devices : Keyboard, Mouse, Scanner. Cost Approx Rs. 3000/-.

Output Devices : CRT & Flat Panel Monitors, Headphones, Printer, Projectors, Sound Card, Graphic Card, LCD Projection Panels, Surround Sound Speakers. Approx Cost Rs. 50,000/-
Processing Devices : Multiple Core Processor, Multiple Processor Motherboard, Chips. Approx Cost RS. 25,000/-

Storage Peripherals : RAM – DDR1 & DDR4, 5 TB & 6 TB - Hard disk drives. Approx Cost Rs.21,000/-

Others Components: Internal/External/PC card modem, Network Card, Laptop Computers, Palmtops, Breadboards. Approx Cost Rs. 35,000/-

b) Forensic Software Applications: As listed in section 2.3

c) Evidence Collection Equipments: HDD of having capacity in TB or higher capacity pen drives, All disk formats supporting live or bootable CDROMS, Mobile device/camera/camcorder memory cards

d) Evidence Preservation Devices: DVD ROM, CD ROM, USB HDD. RF Shield Bags. Approx Cost Rs. 5000/-

e) Digital Data Investigation Kits: Used to copy the data for investigation using write protect feature.

A forensic disk controller or hardware write-block device: is a specialized hard disk controller made for read-only access to computer hard drives without the risk of damaging the drive's contents, shown in Figure [34]

Data Copy King: It is a branded data recovery station comes with attachment of SCSI, SATA and IDE Hard Disk along with individual power supply provision as shown in Figure 2.7 (a). Data Copy king is handy small workstation, which can carry at the incident location. Uniqueness of Data Copy king is extraction of data from the various deices with write protection feature. Price: $1450, Vendor: Salvation Data.

Figure2.7(a) Data Copy King

Figure 2.7(b) HDD write block device

HDD Write Block Device: It is pocket size handy equipment used to copy data from Hard Disk drive by providing the write blocker feature. Figure 2.7 (b) shows HDD write block device. Price: $160. Vendor: Ultra Block.

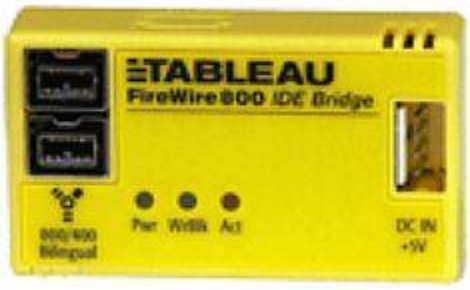

Figure 2.7(c) Forensic Disk Controller, write block device for copying data.

Tableau IDE Bridge (Forensic Disk Controller): This device is similar to HDD Write Blocker but used to provide write block facility to IDE drives. Figure 2.3 (c) shows Tableau IDE Bridge. Price: $190, Vendor: Tableau.

Maintaining OS and required Software Inventories: Operating Systems are essential part of Digital Forensic Lab; investigator must maintain licensed copies of number of various OS. Microsoft OS must include Windows Vista, Windows 7, 8, Windows XP, 2000, NT4.0, NT 3.5, 98, 95 and Dos 6.22. Macintosh Oss must have Mac OS X, 9.x and 8. Linux OSs can include Fedora, Caldera Open Linux, Ubuntu and Debian.

Most high end computer forensic tools can open data files created with popular programs, investigators software inventory of current and older versions of the following programs.

- Microsoft Office 2007, XP,2003, 2000, 97 and 95
- Quicken (for financial investigations)
- Programming Languages: Visual Basic and Visual C++
- Specialized Viewers: ACDSee, Irfan View, Quick View, Thumbs Plus.
- Coral Suite
- Open Office

Forensic Lab Floor Plan Setup: Mid size digital forensic lab have more small workstations at least 6 to 8, and one Multipurpose Forensic Workstation. For safety reasons, the lab should have at least two exists. One or two small cubicles or cabins for supervisors and investigators are more practical in this configuration. One separate space for Library, Software and Hardware stock. One controlled entry exit small cabin having two cupboards to keep Digital Evidence is must. The lab should have at least two controlled exists and no window.

f) Assembly Tools: Required for opening the cabinets and panels. Screwdriver toolkit, Crimping tool, ISO Propane Alcohol, Loose screws etc. Approx Cost Rs 1000/-

g) Data Transmission Cables and Connectors: Various cables and connectors such as RJ 45, RF 11, RJ 58 and Co-Axial cable, Fiber optic cable, BNC connectors, RJ 45 Connectors. Ethernet Cables, Modular Adapters, Ribbon Cables, Din splits Cables, VGA Split Cable, USB

Cables, Audio Cables, Cable Extenders, HDMI 1, 2, 3 Cables, DVI Cables, S Video Cables, DVI to DVI Cable, Serial Cables, Custom Serial Cable, SATA Cables, Optical Fiber Cable, Serial Attached SCSI
Approx Cost Rs. 3000/-

Figure 2.7(d)

2.6 Deleted Data Recovery

There are several techniques to recover the deleted data from the computer. One of the basic method to recover the deleted data is Dos system command.
Purpose: Restores files deleted with the DELETE command.
UNDELETE [d:][path][filename] [/DT|/DS|/DOS]
UNDELETE [/list|/all|/purge[d:]|/status|/load|/U|/S[d:]|/Td:[-entries]]
Various tools available to recover the deleted data is as follows:

2.6.1 Open Source Tools for Deleted Data Recovery

1) Hiren boot: Bootable CD with having utilities related to disk management, Formatting, partitioning, removal of rootkits, recovery of the deleted data etc. Price: Freeware, Vendor: Hiren BootCD org. http://www.hiren.info/pages/bootcd [15].

2) PC INSPECTOR File Recovery: It can recognize data types even when the header is missing recover from deletions, formatting, or even total volume loss. Price: Freeware, Vendor: CONVAR group of companies. http://www.pcinspector.de/ [22].
3) Free Undelete: It undeletes files that have deleted, even if SHIFT-DEL or empty the Recycle Bin. Price: Freeware, Vendor: Recoveronix. http://www.officerecovery.com/freeundelete/ [23]

4) WinHex : This tool is useful for Computer Forensics & Data Recovery Software, Hex Editor & Disk Editor. Price: Freeware, Vendor: X-Ways Software Technology AG. http://www.winhex.com/winhex/index-m.html [24].

5) Wise Data recovery: Recover data from hard drives and removable media such as USB drive, USB Hard Disk. Price: Freeware, Vendor: X-Ways Software Technology AG. http://www.wisecleaner.com/wise-data-recovery.html [25].

6) UndeleteMyFiles Pro : a collection of tools for data recovery, including File Rescue, Media Recover, Deleted File Search, Emergency Disk Image, and Mail Rescue.Price: Freeware, Vendor: Seriousbit. http://seriousbit.com/undeletemyfiles/ [26]

2.6.2 Proprietary Tools for Deleted Data Recovery

1) WinUndelete : is software for deleted files recovery. It can recover deleted files from hard drive, Pen drive, USB external drive, digital camera card, and more. WinUndelete recovers deleted files after emptying the Recycle Bin, or using other deletion actions that bypass the Recycle Bin. Price: $49.95, Vendor: WinRecovery Software. http://www.winundelete.com/ [16].

2) Digital Forensic Framework: This tool is used for digital chain of custody. Recovery hidden of deleted files, quick search for files metadata, and various other things. Price: DFF- Free, DFF PRO- $849, Vendor: ArxSys. http://www.digital-forensic.org/ [17].

3) Active File Recovery: Effectively detect and recover files and disks lost in Windows due to

accidental deletion, disk formatting, virus and other reasons. Price: $29.95, Vendor: LSoft Technologies Inc. http://www.file-recovery.com/ [18].

4) Ontrack EasyRecovery : It gives users a data recovery solution. Protect user data; securely erase data, and recovering deleted files. Price: INR Rs.10, 628.47, Vendor: Kroll Ontrack, http://www.krollontrack.com/data-recovery/recovery-software/ [19].

5) Panda Recovery : Pandora Recovery recovers files permanently removed from Recycle Bin, files deleted using Shift + Delete keys bypassing Recycle Bin and files deleted from DOS prompt. Price: Freeware, Vendor: Pandora Corp. http://www.pandorarecovery.com/ [20].

6) TOKIWA Data Recovery : Data Recovery is freeware and written by TOKIWA to undelete accidentally deleted files even from recycle bin. It supports FAT12, FAT16, FAT32 and NTFS undeletion. Even in both NTFS compressed files and EFS encrypted files. Price: Freeware, Vendor: Tokiwa. http://tokiwa.qee.jp/EN/dr.html [21].

3. Case Study: Confidential Data Theft

The Complaint against its employee was launched by an IT company “Coupon IT” (Name changed to hide identity of Company) located at Mahape, Navimumbai, Maharashtra State, India. This company is working in the field of Discounts Schemes and Coupons for E-Commerce websites. Company top officials stunned to see the strategic plan, Marketing Strategy and Business Logic planned by them were used by their Competitor. After lots of investigation they found that one of their key employees left the company 1 week before and she might have stolen the data from the company computers and transferred it to Competitor Company through email, USB flash drive and Deleted and tempered the database data.

Complaint against her was launched by the company “Coupon IT” at Rabale MIDC Police station, Navimumbai, MS, India. Vide CR No.II 11/2013 Under the provision of IT ACT 43(B) and 66. However this complaint was launched without any evidence therefore the police officers seek my advice and help to obtain the evidence against the suspected employee.
We have adopted following steps for the investigation of this case.

3.1 Data Collection:

Upon receiving the first information about the incident of confidential data theft from IT Company supporting E-Commerce businesses, following process is formulated.
1) Processing Crime and Incident Scene
2) Statement of the complainant.
3) Observation of parameters at crime scene: It includes the physical characteristics of the surrounding area, Computer Network, Internet Service provider, Servers and Computers.
4) Initiating safety measures: Crime scene safety from the electrical, chemical and other hazards.
5) Physical security of any other evidence.

3.2 Questioning:

To establish the link between data theft and company, various key employees of the company was questioned on the following points which, will be used to decide upon the policy of data collection as an evidence.
i) Questioning with the immediate supervisor to know about the confidential files that may be accessed and shared to outsider.
ii) Type of file format (Word, Excel, ppt etc)
iii) Questioned System administrator of the company to know,the internal network structure of the company.
iv) Source of the internet access (Proxy server), IP address range. User authentication details.
v) Existence of mail server for internal and external mailing.
vi) Policies of the Organization / Code of Conduct for Employee.
vii) Various access/ privilege given to whom? Provide the list.

3.3 Computer Seizure and Forensic Analysis and Validation

3.3.1 Seizure and Data Analysis: The Collection phase of computer forensics is finalized when artifacts considered to be of evidentiary value are identified and collected. Normally these artifacts are digital data in the form of disk drivers, Flash memory drives and other forms of digital media [2]. Based on the input received from the other employees of victim company it is known that the Computer, Internet, Email (Gmail account), Mobile phone (Blackberry Make) and USB drive was used by the employee who committed data theft.

3.3.2 Devices from Which Data is Extracted
Identification of Digital Devices from which data is to be extracted is an important task, as this data is considered as evidence in the court. Following are the general task investigator need to perfume during the working with digital devices [3].
1) Identify Digital artifact that can be used as evidence.
2) Analyze, identify and organize evidence.
3) Plan the methodology to extract the data.
4) Collect, preserve and document evidence.
a) Based on the input of employees and system admin of the company it's clear that the employee who steal the data which is classified, confidential and carries secret business planning. This type of data mostly reside on the system of the employee who is handling this important portfolio. Hence we decided to have thorough scanning of computer system.
b) According the company the secret business tactics were known to the competitor. Various ways to share the same from the company computer system are Sharing data through email, copying data on USB drive.As company system doesn't have DVD writer hence above two possibilities are there.

c) Proxy server log: To prove that employee who steal data was using company internet facility, we need to collect and preserve the proxy server log for her ip address and various sites used. Proxy server was installed with Linux operating Systems.

Log is a valuable source of information. Logs records not only access information , but also shows various system configuration errors and consumption of various resources.
Log can be accessed through the path
To display log file in real time, apply the following procedure and commands to get the access.log file.
tail –f
/var/log/squid/access.log
To view the log file text editor can be used
vi
/var/log/squid/access.log

Figure 3.1 Proxy Server Log

So that we get the following output as Figure 3.1. Fig 3.1 shows snapshot of log file of proxy server, which prints the IP address of the system(192.168.0.68) and time stamp record of accessed websites(gmail, tubemogul.co.in , bing.com) and services by the user. Log analysis

shows that the suspect employee accessed company email service through POP email client(Outlook) and private email service i.e gmail on a particular time and date.

d) Employees Computer: Most crucial evidence to prove the data theft crime is to collect data from the employee computer. To prove that employee accessed the classified files and used private email service (Gmail) other than corporate email account.

3.3.3 Computer Internet Browser Data

To extract the internet browser data we used WEFA browser forensic analyzer tool, this tool is used to get the history of browser, cookies information, download list, Search information, local files opened and uploaded, extraction of temporary internet files and time line of events. We will see how WEFA tool is used in the current case to extract the digital evidence. The following activities are performed in order to get the internet browser data:

1) Browser History: We used WEFA (Web Browser Forensic Analyzer) Tool to collect evidence from web browser, which provided us the various information such as; various web sites visited, files downloaded, the local files accessed from computer system, active time on the internet, various searches performed etc.

To open the WEFA tool click on the Start menu of Windows > from the program menu select WEFA > click ok to open it.

Upon opening the tool investigator need to create the new case in to WEFA tool by providing name of Investigator, Case Number, Description and path to store the case. Figure 3.2 Shows Creation of new case in WEFA tool.

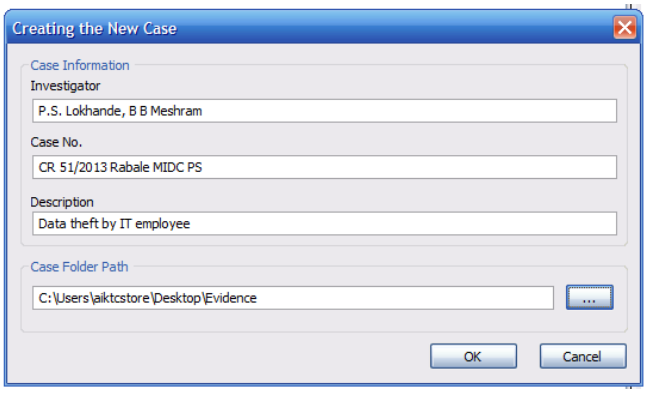

Figure 3.2 Creating new case in WEFA to collect evidence from web browsers.

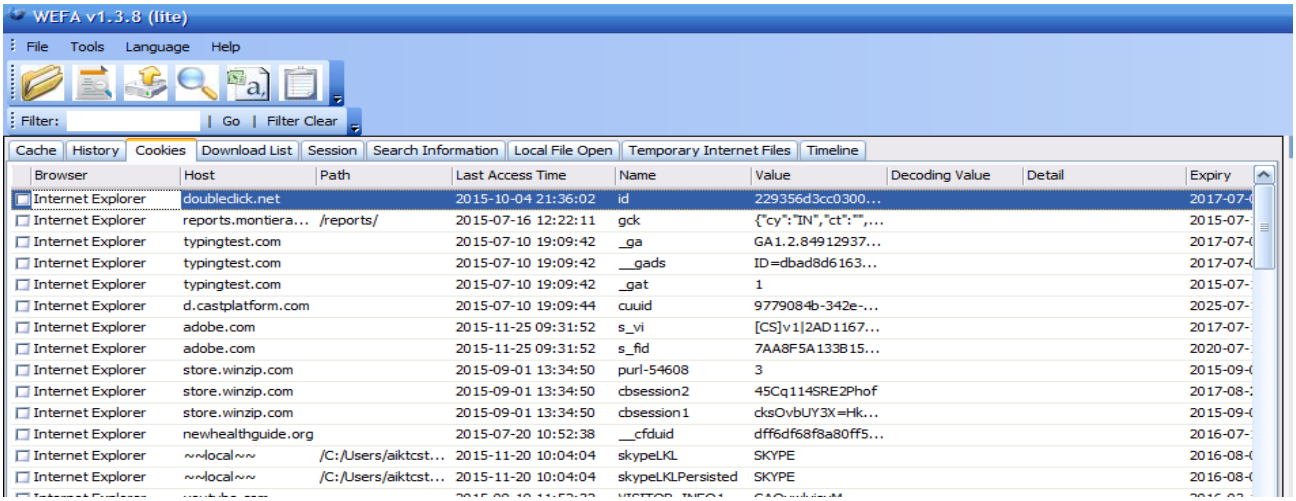

Figure. 3.3 Extracting cookies with all details

2) Extracting Cookies through WEFA tool.

Cookies are the great source of data such as record of users browsing activity, logging in, pages visited in past, the form content which was accessed by the user. Information extracted through cookies are vital information required to prove the involvement of suspect in the crime

Various stored cookies on the system can be extracted with the help of WEFA tool. To extract cookies click on FILE> CREATE NEW CASE> Enter the details such as Investigator name case

no, Case folder path and click ok, then click on Cookies menu, you will get the following information about cookies. Evidence captured through cookies is, type of browser used, Name of host website " doubleclick.net", the competitor website, WinZip application website to compress the bundle of confidential files , last access time, session id and cookie expiry time on the local machine. All these detail are useful to establish the motive of the suspect employee that she is involved in to the data theft act and continuously accessing the computer resources and confidential files.

3) Backing up Web Browser Log Files: Complete backup of web browser files can be taken as evidence. Log file of Web Browser can be accessed through WEFA tool Click on FILE >Collection of WEB BROWSER LOG FILE > Select the Acquisition Target and click OK.
WEFA tool provided web browser files in the form of cache; investigator can take the backup of web browser cache by clicking on Cache tab.
Procedure to collect web browser file backup.
Click on File>Click on the option Analysis of Web Browser Log Information> select the current

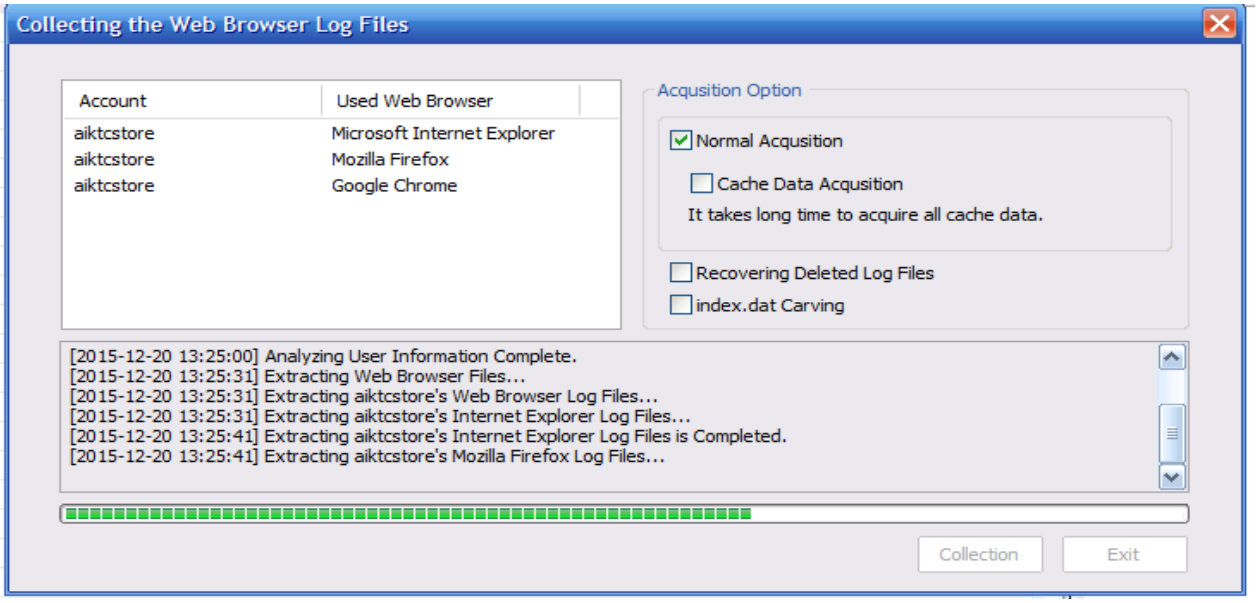

Figure 3.4 Web browser file backup window.

system > click OK. This will collect all log information of web Browser.
To Collect the Web Browser Log information: Click on File menu> Select Collection of Web Browser Log File Provide path to store the file and Click Continue.
The backed up of web browser contains vital information that can be used as an evidence such as Name of web site, browser name, visit time, total number of time the website visited, type of web site i.e. email, news, media etc, title of the web page accessed. It was observed that the official email of the company and private email service i.e. gmail.com was used frequently and number of times. It also contain the information of the local files accessed i.e. files from the computer and activity time on the particular web site.

3.4 Email Forensics

We suspected the company computer from which the files were sent by the suspected employee with the help of Gmail email to the competitor email address.

Forensic of email involve the acquisition of evidences from both sides. Examining email headers: This is to gather information about the e-mail and track the suspect to the email's originating location. The Primary other information includes the date and time of the message was sent, filenames of any attachments and unique message number if available.

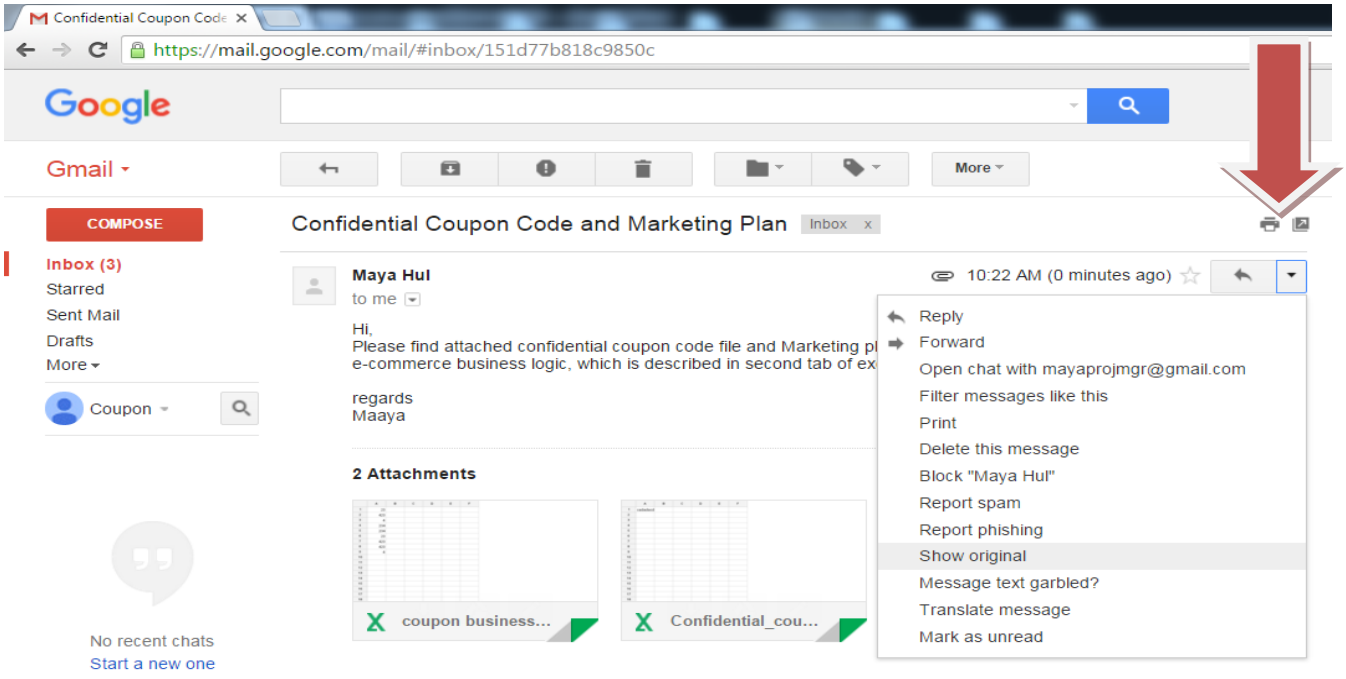

Figure 3.5: Extracting email headers from gmail

Extracting Email Header of Gmail:

1. Log into your Gmail Account.
2. Open the Email whose headers you want to view.
3. Locate Reply at the top right of the message pane.
4. You will see a little arrow pointing down next to Reply. Click on this down arrow next to Reply.
5. A drop down menu will open up. Select Show original in this menu.

The full headers will now appear in a new window as shown in figure 3.6. Figure shows email header copied from gmail (The email addresses are not real addresses). After clicking on show original option you will get the following information as shown in figure 3.6. A message header, in above Figure 3.6 provided lots of information line number 1-4 shows the email servers through which the message travelled.

Line 1 identifies recipient's email address.

Line 2 lists the IP address of the email server that sent the message.

Line 3 shows return path, whith an address the Gmail email system use to send reply message.

Line 4 shows type of email service that sent the message.

```
1) Delivered-To: couponecommerce@gmail.com

2) Received: by 10.79.24.133 with SMTP id 127csp808440ivy;
        Thu, 24 Dec 2015 20:52:54 -0800 (PST)
X-Received: by 10.107.166.13 with SMTP id p13mr61497ioe.179.1451019174356;
        Thu, 24 Dec 2015 20:52:54 -0800 (PST)

3) Return-Path: mayaprojmgr@gmail.com

4) Received: from mail-io0-x243.google.com (mail-io0-x243.google.com.
[2607:f8b0:4001:c06::243])
        by mx.google.com with ESMTPS id o13si8824474ioo.4.2015.12.24.20.52.54
        for <couponecommerce@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Thu, 24 Dec 2015 20:52:54 -0800 (PST)
Received-SPF: pass (google.com: domain of mayaprojmgr@gmail.com designates
2607:f8b0:4001:c06::243 as permitted sender) client-ip=2607:f8b0:4001:c06::243;
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of mayaprojmgr@gmail.com designates
2607:f8b0:4001:c06::243 as permitted sender)
```

Figure 3.6: An email header with line number added.

```
--001a113507347150b30527b1bad0
Content-Type: application/vnd.openxmlformats-officedocument.spreadsheetml.sheet;
        name="Confidential_coupon_ecommerce file.xlsx"
Content-Disposition: attachment;
        filename="Confidential_coupon_ecommerce file.xlsx"
Content-Transfer-Encoding: base64
X-Attachment-Id: f_iil7cm581
```

Figure: 3.7 Evidence of confidential file sent as an attachment

Figure 3.7 shows evidence collected from the email to prove the confidential file is used and attached. It gives the information such as content type (attachment type) as MS office Spreadsheet, Content Disposition as an attachment, with its file name("Confidential_coupon_ecommerce file.xls") and the attachment ID (f_iil7cm581).

By performing the email forensics we established the link between suspects email and the competitor company email address by acquiring the evidences from the both email addresses.

Through the email header forensic we got following information

1) Suspect Accessed email to send confidential data to competitor company, time of email service matched with the system time, proxy server login session timing and Browser history.

2) Browser forensic showed the confidential file accessed at a particular time, which was matched with the time of email server time.

3) Name of Confidential uploaded files from the company computer was matched.

3.5 Hard Disk Data:

HDD is the main source of various forms of data which can be used as an evidence. As expected files having classified information and business secrets were deleted by accused employee. We are successful to recover most of the files with the help of various tools such as Active file recovery, Hiren Boot etc.

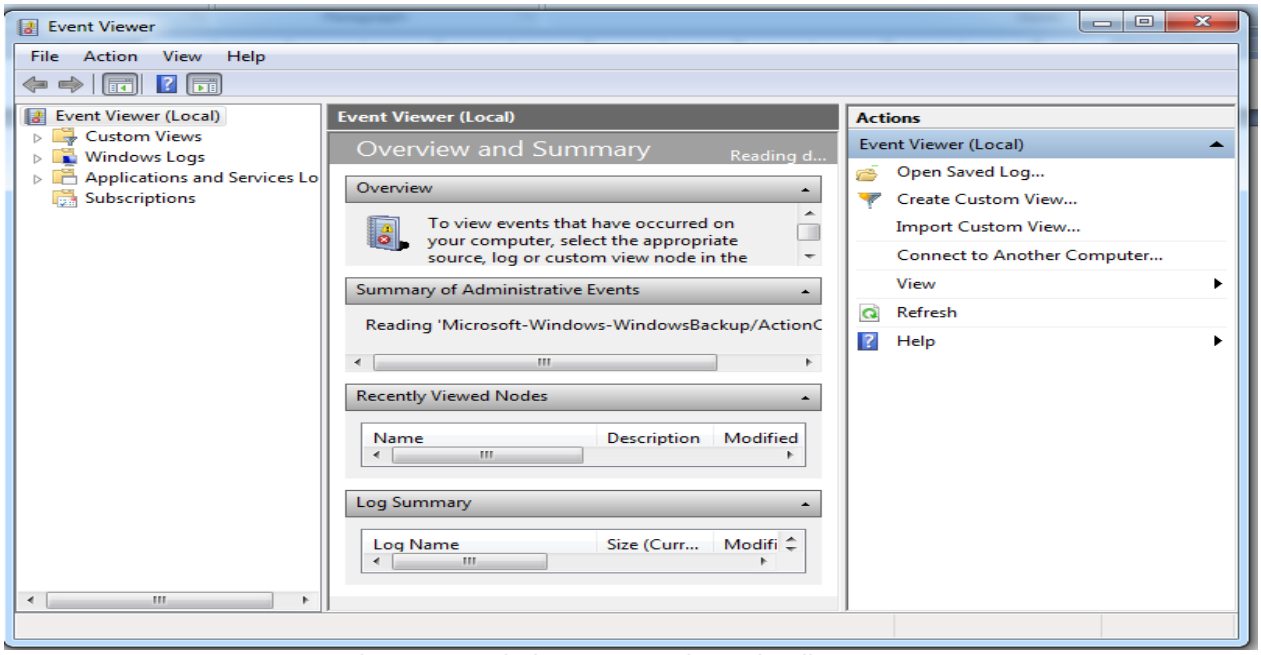

Figure 3.8 Windows Event Viewer landing page.

1) Deleted files: Received with the help of tools, we found that the classified files were deleted by the employee after uploading it to her private email.

2) Event viewer backup: This is just like a black box of the system, data extracted from the Event Viewer helped us to establish the link user activity on the system and her involvement in stealing the data. It can be started by typing event viewer into the Start Menu search box. Also, it can be opened by going

Control Panel -> System and Security -> Administrative Tools -> Event Viewer.
Following Figure 3.9 shows Microsoft file opened several times to access the data.

A copied event log for a specific entry may look like as shown in figure 3.10.

Event log provided the evidence required in proving that the suspect user accessed the confidential files several times (Microsoft Office 12 Sessions) with the date and time of access (SystemTime=2015-11-25 05:43:51) with event ID (Event ID: 7000). It also shows that after accessing the confidential file suspect accessed the private email service, which can be proved by SMTP service logs in the event viewer.

Tracking SMTP service in event viewer

Click Start > Programs>Administrative tools then click Event Viewer
In the console tree click > System Log double click log entry to open event property.
From View menu click Filter and type SMTP
In System Log Properties >select Event Source List > Select SMTPSVC
In the category list, click View all events for SMTP service by keeping default setting at All
This log shows the event ID, time of service access and event record ID. Which supports the claim that suspect used email service.

3.6 RAM Data:

As computer was switched off RAM data was not recovered.
3.6.1 Windows Registry Data: is a hierarchical database that stores low-level settings for the Microsoft Windows operating system and for applications that opt to use the Registry. The kernel, device drivers, services, Security Accounts Manager (SAM), and user interface call use it.

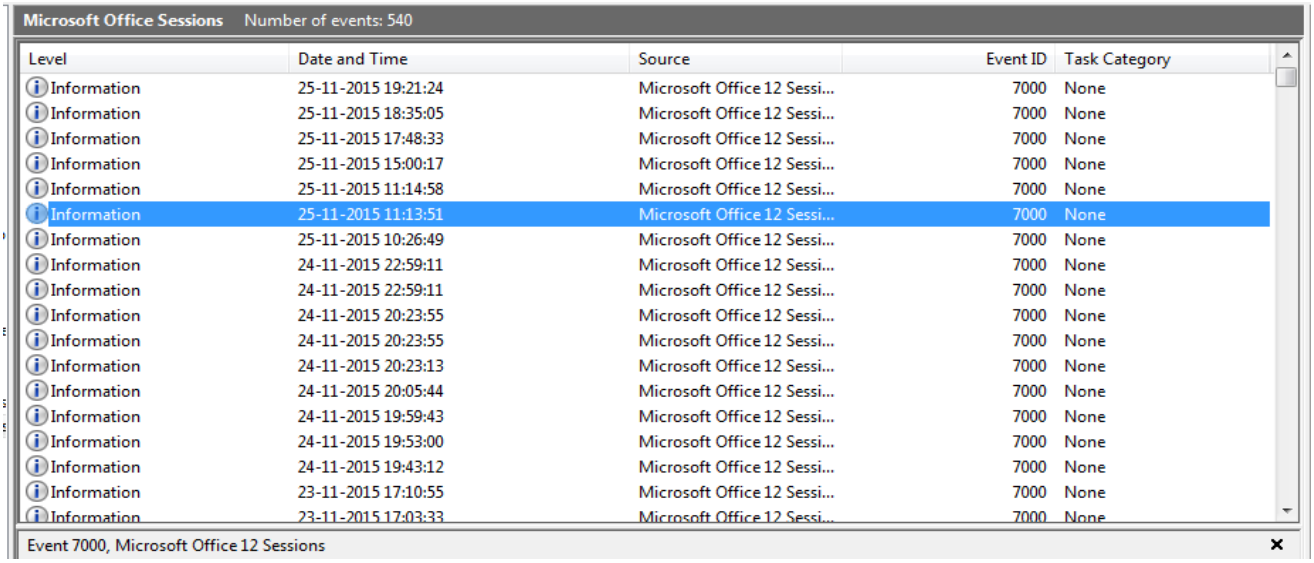

Figure 3.9 Application Event log shows the history of MS Word file opened.

3.7 Windows Registry Data: is a hierarchical database that stores low-level settings for the Microsoft Windows operating system and for applications that opt to use the Registry. The kernel, device drivers, services, Security Accounts Manager (SAM), and user interface can all use the Registry.

3.7.1 Windows Registry Backups from the Command Line: The most technical method of backing up the Windows registry involves using command prompt. To do this, we used the "Console Registry Tool", REG.exe. Performing Windows registry backups in this fashion is usually done when a user would like to automate the process with programming scripts.

To use the Console Recovery Tool, open a command prompt by typing "cmd.exe" into the "Run" dialog in your Start menu, you will get the registry hierarchy.

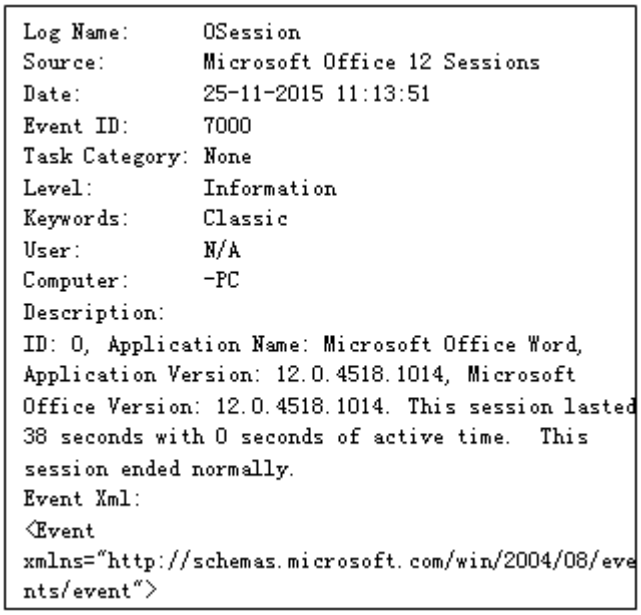

Figure 3.10 Event Log

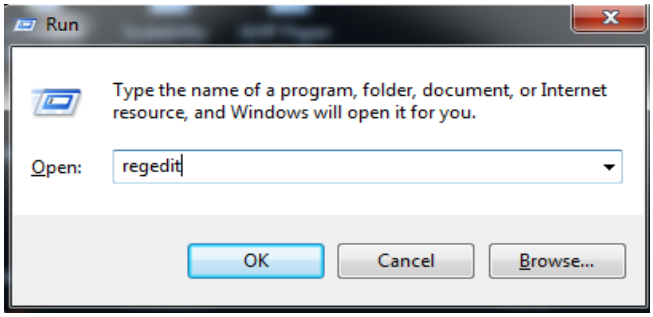

Figure 3.11 Opening registry editor in windows.

The command you type should look like as follows

REG EXPORT [KEY TO EXPORT] [WHERE TO SAVE IT]

For example, if you would like to export the key “HKEY_CURRENT_USER\Software” and save it to “C:\Windows\Backups” you would type the following:

```
REG EXPORT HKEY_CURRENT_USER\Software C:\Windows\Backups
```

If you would like to view the backup, simply navigate to where you have chosen to store it on your computer (C:\Windows\Backups in this example). If you would like to know more about what you can do with the Console Registry tool, you can type “reg /?” for help on using the tool.

3.7.2 MRU List: MRU, or 'most recently used' lists contain entries made due to specific actions performed by the user. There are numerous MRU lists located throughout various Registry keys. The Registry maintains these lists of items in case the user returns to them in the future. It is basically similar to how the history and cookies act to a web browser. One example of an MRU list located in the Windows Registry is the RunMRU key. When a user types a command into the 'Run' box via the Start menu, the entry is added to this Registry key. The location of this key is HKCU\Software\Microsoft\Windows\ CurrentVersion\Explorer\RunMRU and its contents can be seen in Figure 3.12 The chronological order of applications executed via 'Run' can be determined by looking at the Data column of the 'MRUList' value. The first letter of this is 'c', which tells us that the last command typed in the 'Run' window was to execute notepad. Also, the LastWrite time of the RunMRU key will correlate with the last application executed in 'Run'.

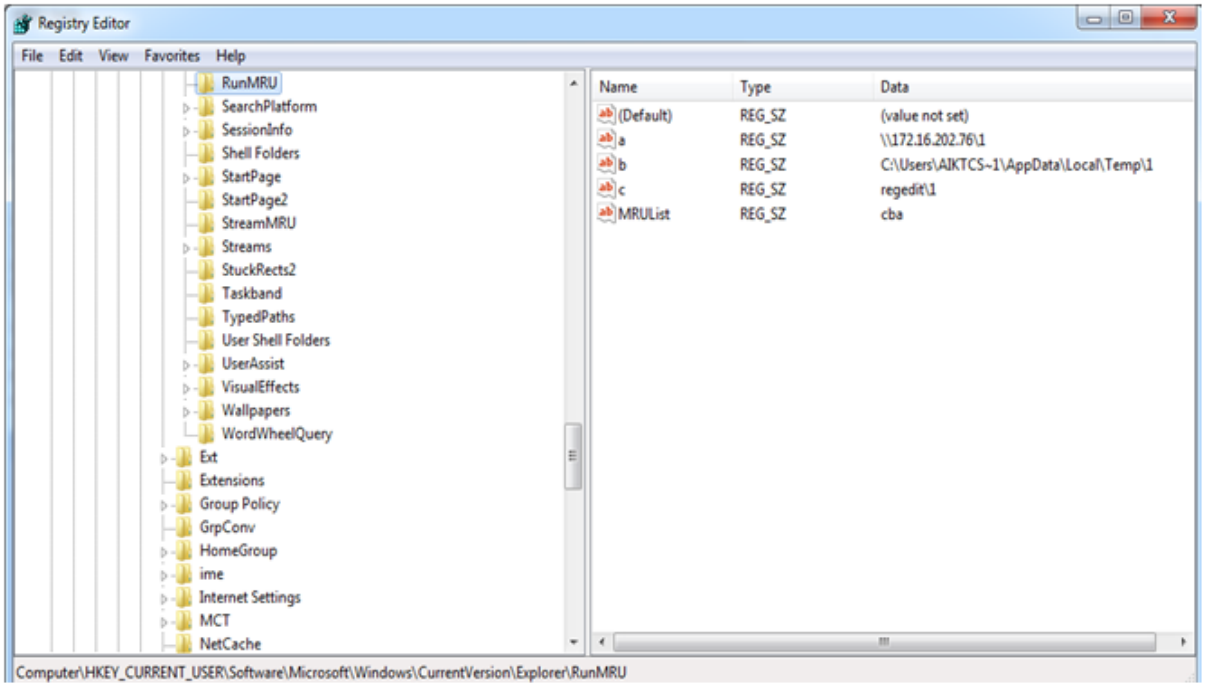

Figure 3.12 MRU List of windows registry

3.7.3 USB Drive: Anytime a device is connected to the Universal Serial Bus (USB), drivers are queried and the device's information is stored into the Registry (i.e., thumb drives).

The first important key is HKLM\SYSTEM\ControlSet00x\Enum\USBSTOR. This key stores the contents of the product and device ID values of any USB device that has ever been connected to the system. Figure 3.13 reveals the contents of this key. The serial

numbers of these devices are a unique value assigned by the manufacturer, much like the MAC address of a network interface card. Therefore, a particular USB device can be identified to determine whether or not it has been connected to other Windows systems.

3.8 Internet Explorer

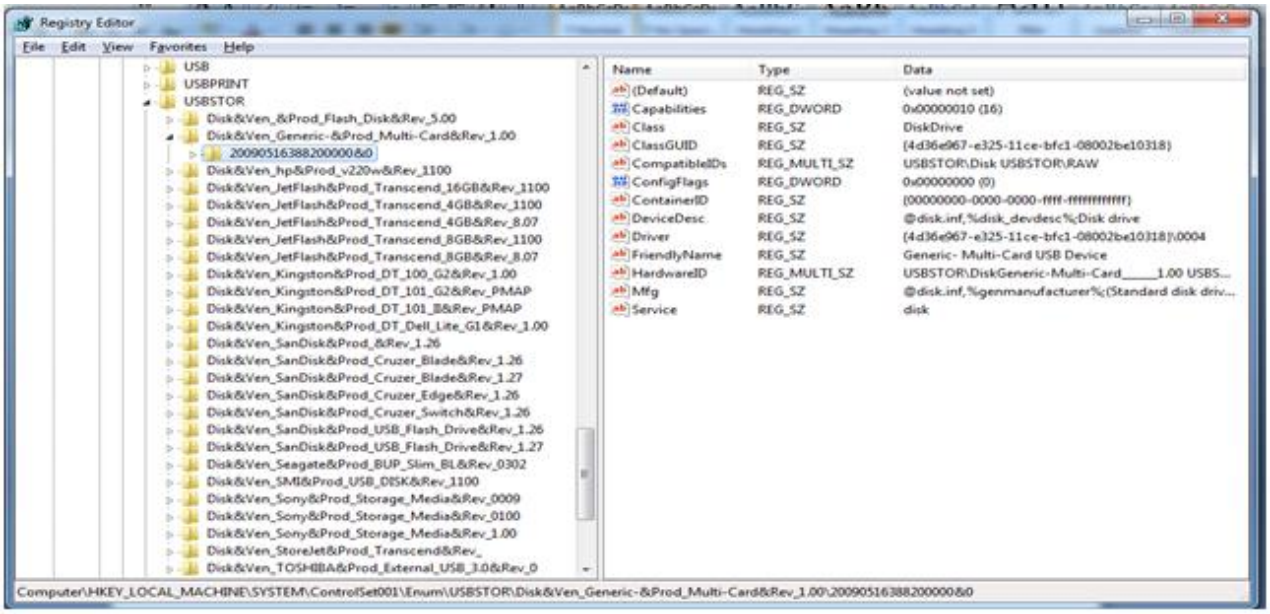

Figure 3.13 USB Drives connected to system and their unique serial numbers

Internet Explorer is the native web browser in Windows operating systems. It utilizes the Registry extensively for storage of data. Internet Explorer stores its data in the HKCU\Software\Microsoft\Internet Explorer key.

There are three subkeys within the Internet Explorer key that are most important for Digital Evidence collection.

1) HKCU\Software\Microsoft\ Internet Explorer\Main.

This key stores the user's settings in Internet Explorer. It contains information like search bars, start page, form settings, etc.

2) The second and most important key is HKCU\Software\Microsoft\Internet Explorer\TypedURLs.

This key shows the content of various URL's typed by the used of system. TypedURLs key screen shot is shown in Figure 4 which, demonstrates the content of what the TypedURLs key displays.

3) The third subkey is HKCU\Software\Microsoft\ Internet Explorer\Download Directory.

This key reveals the last directory used to store a downloaded file from Internet Explorer, giving the examiner an idea as to the location of where the user stores their files.

As an evidence typed URL's provided the information such as official email server accessed (http://123.63.189.168) Websites visited such as competitor web site (coupondunia.in) private email service (Gmail and yahoo) online searching through www.google.com.

Registry Backup: Backing up windows Registry: One can back up the selected branch of windows registry but it is advisable to take the complete backup shown in fig 3.12.

i) To open Registry editor Click Start >type regedit in command box and press enter
ii) You will get Registry Editor application window, click it to open the registry editor
iii) Once the registry editor is opened click on file menu > Select Export option to backup
iv) New window of Export Registry File will open > give appropriate file name to identify

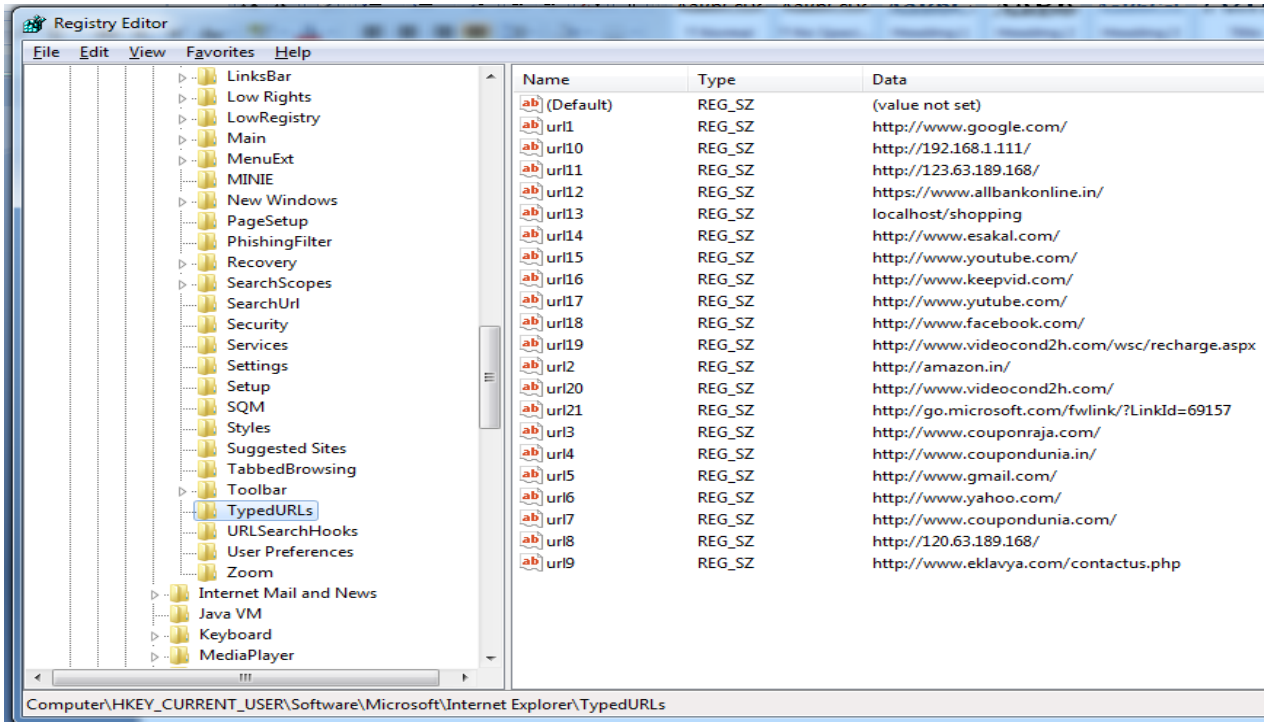

Fig 3.14. Typed URL's record in registry editor.

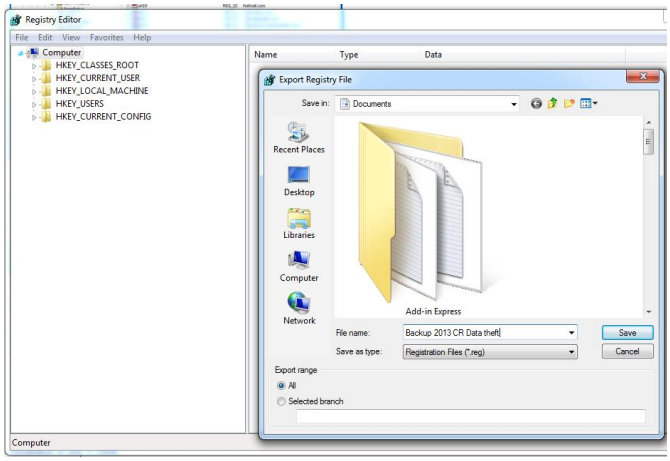

Fig 3.15 Backing up of full Windows registry with all keys.

Select the data drive path i.e D:\ reg_bkp or E:\reg_bkp, where you wanted to store the backup and click Save to backup all registry data as an evidence. Figure 3.15 shows the registry backup procedure.

4. Evidence Handling

After collection of evidence from the various sources, the first role of investigator is to process the all evidences by following standard procedure as given below.

4.1 Evidence Identification:

Identification of Digital Evidence includes the deciding the act of employee who steal the data and transferred to Competitor company. Identify the case requirement, which involves determining the type of case, the investigator can assess the case as follows.

- Situation: Data theft by employee
- Nature of case: Data uploaded to competitor account.
- Type of Evidence: Employee assigned Computer HDD, Email, Browser Log.
- Operating System: Windows XP
- Location of Evidence: Company premises, Company Proxy server, N/W

Based on the details investigator can determine case requirement and identify the evidences required.

4.2 The investigation

During most investigations, an individual's web browsing activity often provides investigative leads. In this investigation, we will begin our analysis by reconstructing the web browsing ctivity in order to help prove Our investigation will utilize System commands and and open source tools that you can use to analyze the data provided for this incident.

4.3 Internet Activity File Formats

One web browser we encountered during computer related investigations Google Chrome.These browsers saves the web browsing activity (also known as web browsing history) in their own unique formats.

System Registry Backup: To know the various external devices configured for the employees system.

Event Viewer: To know the active time and system related applications access.

Following methodology implemented to extract the evidence from the employees computer.

1. Backing up windows registry
2. Backing up event viewer
3. Backing up browser contents
4. Extracting data from cookies
5. Proxy server log
6. User activities in web browser
7. Deleted Data Recovery Tool

4.4 Collection and Preservation

Extracted data is collected and mapped to the user activity to prove intention of the accused user i.e. stealing the classified data and then transferring the same to Competitor Company. Extracted data is collected which is as shown in table 4. The seized evidence is divided in to 5 exhibits and separated as Proxy Server Log, Deleted Data Recovery, Web Browser Data, Event Viewer and Windows Registry data which can be used to prove the data theft crime. Detailed mapping of evidence and related activity to be proved is shown in above table 4.

Table: 4. Mapping of Evidence to prove the crime

Sr. No	Exhibit No	Evidence Source	Mapping to be used to prove
01	I	Proxy Server Log	To prove that the user was online. User accessed private email service (Gmail), date time and IP of the system. Time stamp details of the proxy server log were captured which shows the suspect employees machines IP address and login details. Search history of websites accessed.
02	II	Deleted Data Recovery	Proves that user tempered with the classified information files. Recovered files are the confidential business secret files, which was deleted by the suspect employee after downloading it from the official email id to the system. These files are recovered by the deleted data recovery tools.
03	III	Web Browser Data	Shows user online activity, various websites accessed, various files downloaded, Confidential files opened etc. Backup of web browser provides the information used to prove the suspect handled the confidential files, web browser forensic provided the information such as local files accessed , files uploaded and downloaded, various sites accessed and search history.
04	IV	Event Viewer	Shows the user activity as applications opened and resources used etc. Proves the involvement of user in theft. Opened the Ms word and Ms Excel application number of times, also event viewer shows the access of SMTP service which proves the suspect accessed the email , which was matched with the time

			and date of proxy server and web browser access details.
05	V	Windows Registry Data	Proves that specific USB drive(with serial number) connected to computer system, owned by accused employee. MRU list gives complete details about the Most Recent activity of user on the computer system. Also shows typed URL's record.

Police Department Evidence Seizure Report Format				
Crime Record No	CR No 51/2013	Police Stn.	Rabale MIDC	
Name of Investigating Officer:	Mr. Barve, Mr Sarfare			
Nature of Case	Data theft from the employeers computer, Under the provision of IT ACT 43(B).			
Location of Evidence	Mahapem MIDC, Mahape Shil road, Navimumbai			
Seized item ID	Detail of Evidence	Company / Make	Remark	Model No./Sr. No
CR/51/2013/01	Computer system (CPU, HDD, CD Drive, Mother Board) of suspect employee	HP	Working	PC/AT P-IV XXX-0123-768
CR/51/2013/02	USB Drive	Sony	Working	2GB USB
Evidence Seized By	IO, Rabale MIDC PS		Date and Time	10/10/2013
Evidence sealed and preserved By	IO, Rabale PS, AIO, Rabale MIDC PS		Date and Time	10/10/1013
Evidence Processed By	Disposition of Evidence			Date/Time
Company Hardware engineer	Sealed as per procedure			10/10/2013 04:15 pm
Cyber Crime Expert				

Figure 4.1 Final report format with evidence collection, identification and seizure details

4.5 Preservation of data:

Data is preserved on the DVD and one Hard disk drive. All preserved data is assigned unique Exhibits number as per the Police dept manual. To ensure the data is to be intact at least for 5 years, special antistatic packaging was used to seal the evidences. Finally all antistatic packaging were padded with padding material and kept in box, which is finally sealed with cotton cloth.

4.6 Report

A final report consisting of the First information Report of complainant along with the statement of employees and accused employee is prepared is shown in figure 4.1. All evidences are analyzed and preserved to be present in the court of law. Final report of evidence seizure is made as per the following format.

5. Conclusion

The Chart of Cyber Crime is day by day increasing, Law and enforcement agency is finding it difficult to tackle such cases due to lack of required technical manpower, who can investigate such cases. Most of the time Cyber Crime related cases are not investigated properly due to the non awareness of various tool and techniques used to seize the evidence.

We have designed Digital Forensic Model to check the various parameters required for the digital forensic analysis. This paper also provides the information on how to set up the Digital Forensic Laboratory, along with the required peripherals and software's. Then we have simulated the real life case study on data theft by the employee from IT company's computer system.

Here through this real life case study, we tried to make the reader familiar with the step by step approach in collection of Digital Evidence and various open source and proprietary tools to be used in Digital Forensic Evidence collection and analysis.

Declaimer: To keep the confidentiality of the Data Theft case, company names, person names and addresses used in this paper are changed.

Acknowledgement: We are thankful to the Mr. Ramchandra Deshmukh (Senior Police Inspector), Inquiry Officer Mr. Barve (Police Inspector), Asst. Inquiry Officer Mr. Pradeep Sarfare, (Sub Inspector) Rabale MIDC Police Station, Navi Mumbai, MS, India, for allowing us to work on this Digital Evidence collection assignment.

References

[1] The Information Technology Act 2000, The Gazette of the India, Ministry of Law, Justice and Company Affairs. June 2000
[2] Christopher L.T. Brown, “Computer Evidence Collection and Preservation”, Networking and Security, Searisem Firewall Media, ISBN- 81-318-0015-6, 2007.
[3] Nelson, Philips, Enfinger, Steuart, “ Computer Forensics and Investigations”, Cengage Learning India Pvt. Ltd., ISBN- 978-81-315-0877-3, 2011.
[4] Wireshark: https://www.wireshark.org/about.html
[5] Sluthkit Collection of Forensic Tools: http://www.sleuthkit.org/
[6] SANS Investigative Forensics Toolkit: www.sans.org
[7] Volatility- memory forensics framework: http://code.google.com/p/volatility/
[8] CAINE- Computer Aided INvestigative Environment: http://www.caine-live.net/
[9] Prodiscover basic: http://www.arcgroupny.com/products/prodiscover-basic/
[10] EnCase :https://www2.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx
[11] Registry Rcon: http://arsenalrecon.com/apps/recon/
[12] COFEE: https://cofee.nw3c.org/
[13] HELIX3: http://www.e-fense.com/products.php
[14] FTK: http://accessdata.com/
[15] Hiren Boot: http://www.hiren.info/pages/bootcd
[16] WinUndelete: http://www.winundelete.com/
[17] Digital Forensic Framework: http://www.digital-forensic.org/
[18] Active File Recovery: http://www.file-recovery.com/
[19]Ontrack Easy Recovery: http://www.krollontrack.com/data-recovery/recovery-software/
[20] Panda Recovery: http://www.pandorarecovery.com/
[21] TOKIWA Data Recovery: http://tokiwa.qee.jp/EN/dr.html
[22] Pcinspector tool : http://www.pcinspector.de/default.htm?language=1
[23] Free Undelete tool: http://www.officerecovery.com/freeundelete/
[24] WinHex Data recovery tool : http://www.winhex.com/winhex/index-m.html
[25] Wise Data Recovery: http://www.wisecleaner.com/wise-data-recovery.html
[26] UndeleteMyFiles Pro: http://seriousbit.com/undeletemyfiles/
[27] Steller Phonix Data Recovery: http://www.stellarinfo.com/windows-data-recovery.php
[28] R-Studio Data Recovery: http://www.r-studio.com/
[29] Data Rescue PC: https://www.prosofteng.com/data-rescue-pc-3/
[30] Seagate File recovery: http://www.seagate.com/in/en/services-software/seagate-recovery-services/recover/
[31] REGA Tool : http://forensic.korea.ac.kr/
[32] Amped Authenticate Image tempering detection tool:http://ampedsoftware.com/authenticate
[33] Roadster Forensics acquisition and analysis tool : http://www.itechdataforensics.com/ Roadster.html
[34] Forensic Disk Controller: https://en.wikipedia.org/wiki/Forensic_disk_controller
[35] File Tempering: http://corz.org/windows/software/checksum/
[36] File Checksum Utility by Microsoft: https://support.microsoft.com/en-us/kb/841290
[37] Dump it HDD Forensic Tool: http://www.moonsols.com/2011/07/18/moonsols-dumpit-goes-mainstream
[38] Xplico Email forensic Tool: http://www.xplico.org
[39] Aid4Mail Email forensic application: http://www.aid4mail.com/