Research, Analysis and Efficiency Measurement of Forensic Tools and Techniques to Detect Criminal Evidence to be used in the Court of Law

GRADUATE PROJECT REPORT

Submitted to the Faculty of
The Department of Computing Sciences
Texas A&M University- Corpus Christi
Corpus Christi, Texas

In Partial Fulfillment of the Requirements for the Degree of
Master of Science in Computer Science

By

Sai Ajay K Garimella
FALL 2007

Committee Members

Dr. Mario Garcia
Committee Chairperson

Dr. David R. Thomas
Committee Member

Dr. Long-Zhuang Li
Committee Member
ABSTRACT

The technological advancements in communications and information exchange have paved the way for an entirely new form of crime called cyber crime. Cyber crime has forced the law enforcement officials to develop new areas of expertise for identifying, preserving, analyzing and presenting evidence to prove the crime in the court of law. Evidence derived from computers has been used in court for almost 30 years. The overall goal of the computer forensics is to provide digital evidence of a specific or general activity.

The act of recovering the data from numerous storage devices like floppy disks, hard drives and removable disks form the base for computer forensics. Though several tools have been developed to undertake the investigation, usage of the proper tool to achieve a particular goal is important as all tools do not work well in all situations. Criminals have taken a step ahead and started using the loopholes of the forensic tools so as to stay undetected. The main idea of this project is to study techniques, methods and strategies used by forensic investigators to identify, preserve, analyze and present the criminal evidence in the court of law. During the course of the project, different categories of memory devices that could be used to store criminal data are studied and the appropriate tools that are used to study those memory devices are tested and results are tabulated. Finally, a recommendation has been made to use proper techniques to identify the criminal activities and evidence.
# TABLE OF CONTENTS

Abstract ........................................................................................................... ii  
Table of Contents ............................................................................................ iii  
List of Figures .................................................................................................. viii  
List of Tables ................................................................................................... xiii  

1. Background and Rationale .............................................................................. 1  
   1.1 What is Computer Forensics? ................................................................. 1  
      1.1.1 Chain of Evidence ....................................................................... 2  
      1.1.2 Data Integrity ............................................................................ 2  
      1.1.3 Data Mirroring ......................................................................... 3  
   1.2 Areas of Application .............................................................................. 3  
      1.2.1 Public Sector ............................................................................ 4  
      1.2.2 Private Sector ........................................................................... 5  
   1.3 Forensic Goals ....................................................................................... 5  
      1.3.1 Identifying ................................................................................ 5  
      1.3.2 Preserving ................................................................................ 6  
      1.3.3 Analyzing ............................................................................... 6  
      1.3.4 Presenting ............................................................................... 7  
   1.4 Forensic Tools in Use .......................................................................... 7  
      1.4.1 PDA Seizure ............................................................................ 7  
      1.4.2 Encase .................................................................................... 8  
      1.4.3 FTK Imager ............................................................................ 10  
      1.4.4 PC Inspector file recovery ......................................................... 10
1.5 Removable Media

1.5.1 Compact Flash Card (CF)

1.5.2 Hitachi Micro Drives

1.5.3 Multi-Media card (MMC)

1.5.4 Secure Digital (SD) card

1.5.5 Memory Stick

2. Narrative

2.1 Previous Work done in the field

2.2 Forensic Investigation Process

2.2.1 Search and Seizure of Evidence

2.2.2 Recovery and Analysis of Data

2.2.3 Presenting the Evidence

2.3 Rules of Computer Forensics

2.3.1 Minimal Handling of the Original

2.3.2 Account for any change

2.3.3 Comply with Rules of Evidence

2.3.4 Do Not Exceed the Knowledge

2.4 Rules of Evidence

2.4.1 Admissibility

2.4.2 Authenticity

2.4.3 Completeness

2.4.4 Reliability

2.4.5 Believable
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.5</td>
<td>Unreadable System files</td>
<td>23</td>
</tr>
<tr>
<td>2.5.1</td>
<td>Windows index.dat file</td>
<td>24</td>
</tr>
<tr>
<td>3.</td>
<td>Research</td>
<td>26</td>
</tr>
<tr>
<td>3.1</td>
<td>Research on Commercial Tools</td>
<td>27</td>
</tr>
<tr>
<td>3.2</td>
<td>Research on Freeware and Shareware Tools</td>
<td>31</td>
</tr>
<tr>
<td>3.2.1</td>
<td>Hashing Tools</td>
<td>32</td>
</tr>
<tr>
<td>3.2.2</td>
<td>Tracing Tools</td>
<td>37</td>
</tr>
<tr>
<td>3.2.3</td>
<td>Source Code Forensic Tools</td>
<td>41</td>
</tr>
<tr>
<td>3.2.4</td>
<td>Online Email Tracking Tools</td>
<td>42</td>
</tr>
<tr>
<td>3.2.5</td>
<td>CD Recovery and Inspection Tools</td>
<td>44</td>
</tr>
<tr>
<td>3.2.6</td>
<td>Recovery Tools</td>
<td>45</td>
</tr>
<tr>
<td>3.2.7</td>
<td>Miscellaneous Tools</td>
<td>54</td>
</tr>
<tr>
<td>3.3</td>
<td>Research on Anti-Forensics</td>
<td>57</td>
</tr>
<tr>
<td>3.3.1</td>
<td>CyberScrub Privacy Suite</td>
<td>62</td>
</tr>
<tr>
<td>3.3.2</td>
<td>Clear History</td>
<td>64</td>
</tr>
<tr>
<td>3.4</td>
<td>Research on Unreadable Index.dat File</td>
<td>66</td>
</tr>
<tr>
<td>3.4.1</td>
<td>DatDetective, A tool to read Index.dat file</td>
<td>67</td>
</tr>
<tr>
<td>4.</td>
<td>Testing and Evaluation</td>
<td>75</td>
</tr>
<tr>
<td>4.1</td>
<td>Testing the Commercial Forensic Tools</td>
<td>75</td>
</tr>
<tr>
<td>4.1.1</td>
<td>Encase</td>
<td>77</td>
</tr>
<tr>
<td>4.1.2</td>
<td>Forensic Tool Kit (FTK)</td>
<td>81</td>
</tr>
<tr>
<td>4.2</td>
<td>Testing the Freeware and Shareware Tools</td>
<td>86</td>
</tr>
<tr>
<td>4.2.1</td>
<td>Testing the Hashing Tools</td>
<td>86</td>
</tr>
</tbody>
</table>
Appendix B: Araxis Merge Tool.................................................................158

Appendix C: List of Files Used to Test Encase and FTK...........................................161
LIST OF FIGURES

Figure 1.1. PDA Seizure screenshot.................................................................8
Figure 1.2. EnCase screenshot.................................................................9
Figure 1.3. PC Inspector File recovery...............................................11
Figure 1.4. Compact Flash card.............................................................13
Figure 1.5. Hitachi Micro drives.........................................................13
Figure 1.6. Multi-Media card...............................................................14
Figure 1.7. Secure Digital (SD) card..................................................15
Figure 1.8. Memory Stick.................................................................15
Figure 2.1 index.dat file Opened with Notepad..................................25
Figure 3.1 Screenshot of CRC32..........................................................33
Figure 3.2 Selection of the Hash value type for a file using DigestIT........35
Figure 3.3 HashCalc Window...............................................................36
Figure 3.4 MD5 Tool Window...............................................................37
Figure 3.5 Visualroute used to ping www.sify.com from my personal computer....39
Figure 3.6 HyperTrace Basic Window Screenshot.................................40
Figure 3.7 Neo Trace URL Window.....................................................41
Figure 3.8 E-mail notification about the e-mail under constant monitoring.....43
Figure 3.9 CD-R Inspector Main Window...........................................45
Figure 3.10 Display of the Root files by the tool....................................47
Figure 3.11 Flash Retriever displaying all the connected flash storage media.........49
Figure 3.12 Flash Retriever provides the option to filter the recovery process........49
Figure 3.13 Retriever Recovery Progress............................................50
Figure 3.14 Flash Retriever Preview and copy of the recovered files.......................50
Figure 3.15 GetDataBack Scan for drives.........................................................52
Figure 3.16 GetDataBack Selecting Source.......................................................52
Figure 3.17 GetDataBack Selecting range and file system.................................53
Figure 3.18 GetDataBack Selecting File System..............................................53
Figure 3.19 GetDataBack Recovery tree.........................................................54
Figure 3.20 Detailed Summary of the computer system being examined...............55
Figure 3.21 Password Recovery Kit recovered password for MS Excel.................56
Figure 3.22 CyberScrub Home Screen..........................................................64
Figure 3.23 Clear History Home Screen.........................................................66
Figure 3.24 Main Window of the tool DatDetective..........................................67
Figure 3.25 File Menu of DatDetective..........................................................69
Figure 3.26 Edit Menu of DatDetective..........................................................69
Figure 3.27 View Menu of DatDetective.........................................................70
Figure 3.28 Help Menu of DatDetective..........................................................70
Figure 4.1 Encase View Pane .................................................................77
Figure 4.2 Deleted files recovered using Encase.............................................89
Figure 4.3 pst file recovered using Encase.......................................................80
Figure 4.4 FTK Basic Screenshot.................................................................81
Figure 4.5 FTK Recovered Deleted Files from SD-Card...................................83
Figure 4.6 FTK’s capability to recognize PIM files..........................................83
Figure 4.7 Misnamed Files recovered by FTK...............................................85
Figure 4.8 Deleted E-mail attachment recovered from .pst file by FTK...............85
Figure 4.9  Comparison of .txt file before and after the deletion of data  ................. 88
Figure 4.10  CRC32 Calculated for an .avi file  ................................................. 88
Figure 4.11  MD5 calculated for the .doc file ...................................................... 90
Figure 4.12  MD5 After deletion of a single full stop from the .doc file .............. 91
Figure 4.13  SHA-1 Calculated for the same .doc file ...................................... 91
Figure 4.14  Various Hash Value types of a single .doc file ............................. 93
Figure 4.15  Different Hash Values of the same .doc file after addition of data .... 94
Figure 4.16  Various Hash Value types for Text String ....................................... 94
Figure 4.17  Hash value calculated for a .doc file ............................................. 96
Figure 4.18  Visualroute used to ping www.sify.com ........................................ 98
Figure 4.19  HyperTrace used to ping www.sify.com ...................................... 100
Figure 4.20  Graph showing the final destination web server in India ............... 102
Figure 4.21  Window showing the list of hops and IP addresses ....................... 103
Figure 4.22  Folder Comparison using Araxis Merge ........................................ 106
Figure 4.23  Comparison of source code files (Original and Modified) ............. 107
Figure 4.24  Comparison of two image files (Original and Modified) ............... 108
Figure 4.25  Summary of the tracked E-mail ..................................................... 110
Figure 4.26  Selection of certain sectors or entire track to be imaged ............... 112
Figure 4.27  Copying the whole track image of the compact disc ..................... 112
Figure 4.28  CD-ROM Hardware Information .................................................... 113
Figure 4.29  Disc report saved in .txt format ................................................. 114
Figure 4.30  Disc Error Summary using CD-R Inspector ................................. 115
Figure 4.31  Searching for the keyword “Texas A&M University”.................116
Figure 4.32  Search result showing the keyword “Texas A&M University”........116
Figure 4.33  Volume Information about the disc..............................................117
Figure 4.34  Analysis of the CD.................................................................118
Figure 4.35  Display of the Lost files by the tool........................................119
Figure 4.36  Display of the deleted content that is been recovered...............120
Figure 4.37  Saving the recovered files on another storage media...............121
Figure 4.38  Flash retriever Preview and copy of the recovered files..........122
Figure 4.39  GetDataBack Recovery tree.................................................124
Figure 4.40  A Sample Recovered image using GetBackData......................124
Figure 4.41  Detailed Summary of the computer system being examined.........127
Figure 4.42  password window of password protected MSExcel sheet.........129
Figure 4.43  Password Recovery Kit recovered password for MS Excel.........129
Figure 4.44  CyberScrub Home Screen......................................................131
Figure 4.45  CyberScrub File Menu..........................................................132
Figure 4.46  CyberScrub Deleted E-mail......................................................132
Figure 4.47  CyberScrub Erase Menu........................................................133
Figure 4.48  CyberScrub Erase Beyond Recovery......................................133
Figure 4.49  CyberScrub Erase All............................................................134
Figure 4.50  CyberScrub Privacy Guard......................................................134
Figure 4.51  CyberScrub Tools.................................................................135
Figure 4.52  Clear History Window............................................................137
Figure 4.53  Clear History Clear Application Tracks.................................137
Figure 4.54  Clear History Clear Browser History……………………………………138
Figure 4.55  Clear History Clearing Junk information………………………………..138
Figure 4.56  Clear History Clearing Windows tracks……………………………………139
Figure 4.57  List of the URLs visited……………………………………………………142
Figure 4.58  Index.dat file from IE History viewed using DatDetective………………….143
Figure 4.59  Cookies related index.dat file opened with DatDetective………………….144
LIST OF TABLES

Table 2.1  Scenario Table……………………………………………………………27
Table 4.1  Encase-SDcard…………………………………………………………….77
Table 4.2  Encase-Thumbdrive………………………………………………………..79
Table 4.3  FTK-SDcard………………………………………………………………81
Table 4.4  FTK-Thumbdrive………………………………………………………….83
Table 4.5  CDR-Inspector Features………………………………………………….111
Table 4.6  List of Passwords tested using Passware Password Recovery Kit……….128
Table 4.7  Comparison of Anti-Forensic Tools………………………………………139
1. BACKGROUND AND RATIONALE

1.1 What is Computer Forensics?

As technology has advanced, the spread of crime through computers has become unavoidable. One of the reasons for this is due to the tremendous awareness about the computer and its usage among the people throughout the world. Also, the exponential increase of various varieties of portable devices fueled increase of the crime rate. Computer forensics is also referred as cyber forensics or Digital forensics. Computer forensics is commonly defined as the collection, preservation, analysis and presenting the computer related evidence to the court of law. Computer forensic examiners follow safe and well-defined methodologies and procedures that are adapted for any particular situation. These procedures include maintaining a chain of evidence, maintaining the integrity of the data source, and creating accurate mirror images of data sources.

There are many branches of forensics like PDA Forensics, Source Code Forensics, Network Forensics, etc., PDA forensics can be defined as applying the forensic computing methodologies to PDA’s which are designed for mobility and hence are compact in size. They are being used by many individuals for both personal as well as for professional purposes. PDA’s vary in both design and are undergoing changes continually due to the introduction of new technologies. The application of computer investigation and analysis techniques to various PDA devices to examine the relevant data contained on them so as to provide the relevant evidence to the court of law summarizes the definition of PDA forensics [Jansen 2004].
1.1.1 Chain of Evidence

The phrase “chain of custody” refers to the accurate auditing and control of original evidence material that could potentially be used for legal purposes [Cybertrust 2005]. The chain of evidence is critical when it comes to dealing with electronic or computer memory related evidence because that sort of evidence is inclined towards easier alteration or destruction. Proving the chain of custody was never broken authenticates the electronic evidence. In order to maintain the chain of evidence, maintenance of frequent logs and proper tracking of the movement and possession of evidence material or source is essential. A forensic investigator must be able to prove that particular data is available at a certain location, at certain time and in certain condition and which can be attained by maintaining a chain of evidence. The strength of the forensic investigation lies on how sophisticated is the chain of evidence.

1.1.2 Data Integrity

When forensic investigation is being performed on a certain data source, it is important to preserve the integrity of this data. In fact, data integrity is the most important aspect of forensics analysis phase as the original data might be needed for subsequent testing and analysis phases. While evidence data is in the possession of the investigator, he must ensure that the original state and condition of data is maintained [Cybertrust 2005]. In order to preserve the data integrity, the analysis of the evidence data should never be performed on the original data source as it might result in irreparable loss of forensics information. Preserving data integrity maintains a credible data source from a legal perspective and allows subsequent investigations to utilize the same base starting point for
performing replication of the analysis. Thus, the best thing to do in order to preserve the
data integrity is to create appropriate mirror copies of all original data.

1.1.3 Data Mirroring

Data mirroring is one of the most important processes of the computer forensics. It is the process of taking a “mirror image” of the storage media. One of the goals of the forensic investigator is to handle the original data as little as possible. In order to achieve this, the forensic investigator creates a mirror image of the original data source and creates any other additional copies if required from this first copy. Thus, the first copy is always termed as the “master copy”. In order to preserve the data integrity, “master copy” is never used for forensic analysis. In this manner, original data needs to be handled only once to create a master copy. Just as the original data is safeguarded from any losses, the additional copies made from the master copy also needs to be properly maintained and strictly handled as they might contain sensitive and/or confidential information [Cybertrust 2005]. While a strict chain of custody does not need to be maintained for data copies, they should be strictly controlled and protected from the original data in a separate physical location.

1.2 Areas of Applications

Computer forensics is primarily used in both the public sector and the private sector. Computer evidence can be used in any case where unauthorized documents such as terrorist literature, financial fraud and child pornography are likely to be found on computer. Insurance companies too hire computer forensics specialists to unearth fake claims, compensation cases etc.,
1.2.1 Public Sector

Computer forensics is used in public sector by government and law enforcement officials to investigate and prosecute crimes. Some of the traditional crimes for which the criminals use computer technology are homicide, theft of confidential government information, financial fraud, auto theft to name a few [Hailey 2003]. A computer can be either a target of a crime, the tool in commission of a crime or as incidental to a crime. Any crime which involves computers in any of the above mentioned way is termed as a “cyber crime”. Military is another important government sector which is to be closely monitored for any cyber crime as crime in this sector might range from destruction of the important information to theft of that information. At any rate, government and law enforcement use of computer forensics is increasing, as more and more criminals are using computer technology.

Investigators employ different paradigm for each area when performing analyses. In case of law enforcement, the primary objective of forensic analysis forms the prosecution process. “After the fact” environment is required for forensic analysis in this area. That is, law enforcement can’t act or analyze until there is sufficient reason to believe that a crime has occurred. Computer related evidence is used by the prosecutors on a day to day basis to help convicting criminals involved in fraud, murder, child pornography, drug trafficking and terrorism.

For military operations, however, prosecution forms the secondary objective while continuity of operations forms the primary objective. A real time environment is needed to perform forensic analysis in this area.
1.2.1 **Private Sector**

In the private sector, such as business and industry, computer forensic techniques and methodologies are used to investigate electronic break-ins, embezzlement, improper use of computing resources by employees, and theft of trade secrets among other things. In the field of business and industry, primary objective of analysis is to safeguard availability of service [Hailey 2003]. Prosecution forms the secondary objective in private sector.

1.3 **Forensic Goals**

In technical aspects, the goals of computer forensics can be briefly described as identifying, preserving, analyzing and presenting digital evidence in a manner that preserves the integrity of the evidence so that it can be used effectively in the court of law [McKemmish 1999].

1.3.1 **The Identification of Digital Evidence**

This is the first and foremost step in the forensics process. This can be described as the process of identifying where the evidence is present, what it is, how it is stored and what operating system is being used. This phase of the forensic investigation helps the investigator to understand various aspects of the source of evidence and decide upon the appropriate methodologies and procedures to be used so as to gain evidence. There is a misconception that personal computers are the only candidates where forensic investigation can be performed, but in reality it can extend to any electronic device that is capable of storing information [McKemmish 1999]. The computer forensic examiner must be able to identify the type of information stored in a device and the format in which it is stored so that the appropriate technology can be used to extract it [Pendyala 2006].
1.3.2 The Preservation of Digital Evidence

This is another important phase in the forensics process. This is the process of preserving the integrity of the digital evidence, ensuring the chain of custody is not broken. The data needs to be preserved (copied) on stable media, using reproducible methodologies. There might be some circumstances which arise where the changes to the data are inevitable, but it is important that least amount of changes occurs [McKemmish 1999]. In situations where a change is unavoidable, it is essential to properly document the nature of, reason for the change in order to give necessary explanation to the court. This applies not only to changes made to the data itself, but also includes the physical changes that are made to the particular electronic device to facilitate access to the data [Pendyala 2006].

1.3.3 The Analysis of Digital Evidence

This phase can be explained as the process of extraction, processing and interpretation of digital data. Once the digital data is extracted, digital evidence requires processing to be done on it before it is available to be read by people. The processing of the extracted product may occur as a separate step, or it may be integrated with extraction [Pendyala 2006]. As the analysis cannot be made on the original data source, a mirror image is to be created first. The advantage of mirroring this data is to view it without risk of accidental changes, therefore maintaining the integrity whilst examining the evidence. Analysis of the data being the most critical part of the investigation process, Computer forensics is sometimes described as the critical analysis of a computer hard disk drive after an intrusion or crime.
1.3.4 The Presentation of Digital Evidence

This phase involves the actual presentation in a court of law. It also includes the manner of presenting the evidence, the expertise and qualifications of the presenter and also the credibility of the process employed to produce the evidence [Pendyala 2006]. The feature of the forensic computing that makes it unique when compared to other areas of information technology is the requirement that the final result must be generated from legally accepted methodologies and procedures [McKemmish 1999]. If the matter is presented in court the jury, who may have little or no computer experience, must all be able to understand what is presented and how it relates to the original, otherwise all the efforts to prove the guilt could be futile. Proper application of the appropriate procedures helps in producing digital evidence that proves what happened, when it happened, where it happened, who did it and how they did it.

1.4 Forensic Tools in Use

There are numerous tools available for digital forensics and they range from freeware tools to expensive commercial tools. Forensic tools acquire the data required for the evidence from the device either by physical acquisition or by logical acquisition. Physical acquisition means bit-by-bit copy of an entire physical store. While, logical acquisition means bit-by-bit copy of the logical storage objects (e.g. Directories and files) that reside on the logical store. Some of the Forensic toolkits are:

1.4.1 PDA Seizure

PDA Seizure is a forensic software toolkit offered by Paraben. This allows the forensic examiners to perform various forensic activities on the PDA’s to acquire and
examine the information for both Pocket PC (PPC) and Palm OS platforms. Some of the exciting features of PDA Seizure include the ability to produce an accurate forensic image of Palm and Pocket PC devices, ability to search based on examiner provided search key where it browses through the acquired files to find the required file [Jansen 2004]. It also have the ability to generate reports of its findings. It provides a very good user interface with book-marking capability which helps in organizing the files. Figure 1.1 illustrates the screenshot of the PDA Seizure.

![Figure 1.1 Screenshot of PDA Seizure](image)

### 1.4.2 EnCase

EnCase is a very well known forensic software used for computer forensics. As commercial software it provides many features which helps he examiner in various ways.
Some of its features include search and analysis of the suspect data, data capture and documentation. Though EnCase is very well known for examining PCs, it also support Palm OS devices. One best feature of EnCase tool is that it first creates a bit-stream image called as acquisition file (EnCase evidence file) which is mounted as virtual copy (read-only) [Jansen 2004]. This feature helps in examining the suspicious data while preserving the integrity of the original data source as well as the master copy. It also allows the examiner to highlight various files, folders, or sections of a file which acts as a bookmark and help for any further references. The reporting feature helps to view the information from several perspectives such as acquired files, single files, results obtained when search for a particular object was been made, previously generated reports and the case file created. Figure 1.2 illustrates the screenshot of the Encase toolkit.

Figure 1.2 EnCase toolkit screenshot
1.4.3 FTK IMAGER

Forensic Toolkit (FTK) offers law enforcement and computer security professionals the ability to perform complete and thorough forensic examinations. FTK has some of the powerful features like file filtering and search based on the user given keyword. FTK’s powerful filters help us browse through thousands of files to quickly find the required evidence [Acquisition Data 2005]. Some of the important features associated with FTK are

- View hundreds of different file formats
- FTK imager allows to quickly navigate through acquired images
- Generate audit logs and case reports
- Full text indexing yields instant search results
- Open and analyze all versions of windows registry files.
- Supports various file and acquisition formats.

1.4.4 PC Inspector File Recovery

PC Inspector File Recovery is a freely available forensic tool. This tool serves two main purposes. Firstly, to reveal the contents of all storage media attached to the computer system and, secondly, to recover any deleted data from the media. It recovers lost files and finds partitions automatically, even when the boot sector of the machine has become damaged or erased. Even when a file's header entry is no longer available, PC Inspector File Recovery can recover the file. This program provides an option to save recovered files on network drives. It recovers files with the original time and date stamp.

This tool is very effective at detecting all files resident on a storage device. All unreferenced files are associated with a condition. This condition can either be “good” or
“poor”. The “Find lost data” option of the tool performs a sector-by-sector scan, which includes unallocated space and file slack of the storage media and reveals any files that were either lost or seemed to be deleted. Experiments prove that the probability of viewing or recovering an unreferenced file is higher if the file’s condition was good. The figure 1.3 illustrates how seemingly deleted files are viewed and potentially recovered within the tools interface.
1.5 Removable Media

The evolution of several types of removable storage media created a revolution in the information age. The size of various storage media designed for several handheld devices is noteworthy as they are about the size of a coin. Though small in size, the capacities can be quite large, on the order of gigabytes (GB) of memory. These storage devices are non-volatile and they do not require any battery to retain data [Jansen 2004]. These storage media can be treated as removable disk drive and thus could be imaged and analyzed using most of the forensic tools available in market. Some of the removable media and their characteristics are described in the following subsections

1.5.1 Compact Flash Card

Compact flash memory card is a small solid-state disk card with 50-pin connector with 2 rows and 25pins on each row (edge) of the card. Compact flash cards are designed for PCMCIA-ATA functionality and compatibility. PCMCIA-ATA flash cards are robust and they consume 10% of the power consumed by smaller hard drives. They consist of a 16-bit data bus which serves more like a hard drive rather than a RAM. These are non-volatile and can retain its information once the power is turned off. These use the flash memory technology. Flash memory is a non-volatile computer memory that can be electronically erased and programmed. Flash memory costs far less than EEPROM and therefore become the dominant technology wherever a significant amount of non-volatile, solid-state storage is needed. They are usually the size of a matchbox with dimensions length-36.4mm, width-42.8mm and thickness- 3.3mm to 5mm [Jansen 2004]. Figure 1.4 shows a sample Compact Flash Card.
1.5.2 Hitachi Microdrive

Hitachi microdrive storage media is a very high capacity rotating mass storage device with a 16-bit data bus. Here, the storage media is a small glass disk which requires energy to spin. This is more fragile than a solid state memory. It functions similar to the solid state flash memory card. It is preformatted with a FAT 32 file system. Any storage over 2GB requires FAT 32 [Jansen 2004]. Most cameras and PDA’s support FAT 32 file system. Figure 1.5 shows a sample Hitachi Microdrive.
1.5.3 Multi Media card

A Multi-Media Card (MMC) is a solid-state card with a 7-pin connector. MMC’s have a 1-bit data bus. Just like Compact flash cards, they are designed with flash technology. MMC’s are non-volatile and thus can retain information once the power is turned off from the card. These contain non-moving parts and provide higher data protection when compared to conventional magnetic disks. They are usually of the size of a small postage stamp with dimensions length-32mm, width-24mm and thickness-1.4mm. The reduced version of MMC is RS-MMC, which is approximately one-half the size of the regular MMC [Jansen 2004]. These memory devices are designed specifically for the use in PDA’s such as Mobile phones, Music players, etc. A RS-MMC can be used as a regular MMC when an appropriate adapter is used. Figure 1.6 shows a sample Multi-Media card.

![Multi-Media Card](image)

Figure 1.6 Multi-Media Card

1.5.4 Secure Digital (SD) card

Secure Digital (SD) cards are comparable to the Multi-Media cards in both size as well as solid-state design. SD cards have a 9-pin adapter and a 4-bit data bus which helps in faster data transfer rate. One special feature of the SD card is an erasure-prevention switch when put in the locked mode, helps in preventing accidental deletion of data. They usually are the size of an MMC with dimensions length-32mm, width-24mm and thickness-2.1mm. The extension of the SD card is a mini SD card which is a more compact form of
an SD card with dimensions length-21.5mm, width-20mm and thickness-1.4mm [Jansen 2004]. They can be used as a regular SD card using the suitable SD adapter. Figure 1.7 shows a sample SD card.

![Figure 1.7 Secure Digital (SD) Card](image)

**1.5.5 Memory Stick**

Memory sticks are another kind of compact storage devices which provide solid-state memory. A memory stick is generally the size of a stick of gum with dimensions length-50mm, width-21.45mm and thickness-2.8mm. It has a 10 pin connector with a 1-bit data bus. Just like the SD cards, Memory sticks too have an erasure prevention lock. Memory stick PRO is sophisticated forms of memory sticks with higher capacity as well as data transfer rates [Jansen 2004]. Memory stick Duo is another improvement of Memory stick which is about 2/3rd the size of the regular Memory Stick. Figure 1.8 shows a sample Memory stick pro duo.

![Figure 1.8 Memory Stick PRO](image)
2. NARRATIVE

2.1 Previous Work Done in the Field

The ability to intercept a Palm Pilot PDA password either by monitoring the traffic between the PDA and a workstation with a Palm Pilot cradle or by initiating a synchronization update between the password protected PDA and a second PDA and the ability to analyze image files to detect if a message is hidden in the file using steganography were some of the important research areas in the field of Computer forensics. Niels Provos and Peter Honeyman at the University of Michigan have developed a process using statistically analysis of a JPEG image to detect if there is a steganographic item stored in the JPEG [Provos 2001]. Neil Johnson, a researcher at George Mason University, is working on being able to identify steganographic items in BMP and GIF images files as well as WAV and AU sound files [Johnson 2002].

Another important challenge faced by the forensic investigation team is misnamed file extensions which makes the files unreadable. There were lots of cyber crime related cases which were encountered previously where the criminal changed the file extension to some unreadable format so as to make the file useless. If very few such files were unearthed during the examination, it wouldn’t be a problem to examine all those files individually. Whereas, if large data sources are been examined and large number of such files are been unearthed, it is a very difficult task for the examiner to work on each files individually without being sure if that particular file could help him gain any evidence or not. To avoid this problem, a project called National Software Reference Library (NSRL) was launched with the support of U.S. Department of Justice’s National Institute of Justice(NIJ). NSRL is designed so that it collects software from various sources and the file
profiles related to that software is incorporated into a Reference Data Set (RDS). The RDS is a collection of digital signatures of known, traceable software applications that can be used by law enforcement, government, and industry organizations to review files on a computer by matching file profiles in the RDS [NSRL 2006].

2.2 Forensic Investigation Process

A Computer forensic investigation process proceeds in a series of steps namely search and seizure of evidence, recovery and analysis of evidence and evidence presentation. Each of these steps is explained in a detailed manner in this section.

2.2.1 Search and Seizure of Evidence

By its very nature, digital evidence is volatile and easily corruptible. Thus, the timely identification and the proper seizure and preservation of digital evidence are very important processes during any investigation. If the digital evidence collected is intended to be used in a court of law, investigators must be able to establish its authenticity and integrity beyond reasonable doubt. The practice which is accepted globally for preserving the digital evidence is to make one or more bit-stream images or copies of the original source of data using specialized tools and techniques. This ensures that the original media is not tampered with during the imaging process. Only the duplicate image is then used to perform the analysis process. In situations where it is not possible to retain the original media, two bit-stream images are created and one of the images is preserved and treated as original [Spotlight 2002].
2.2.2 Recovery and Analysis of Data

Data can be stored on various locations within a computer which can be termed as either temporary data or permanent data. Data which is stored at locations such as RAM, temporary directories, slack space etc., is termed temporary data and the data which is stored at the allocated space on the hard disk is termed permanent data. The recovery and analysis process proceeds in four phases namely recovery of the data, searching for active files, searching for deleted files and searching for slack and unallocated space.

Recovery of Data by Taking Stock

This phase involves the process of preparing a full listing of all files on the media, including the directory structure and the hidden files. This listing helps the investigator to determine the way in which the suspect organized his information. This phase also involves the process of identifying various encryptions, data hiding and steganography tools which gives the investigator a hint about the criminal intentions [Spotlight 2002].

Searching for Active Files

At the very first instance during the seizure process, the investigator gets a chance to view the active applications and files. This helps the investigator to get a basic idea of the type of applications the criminal is working upon [Spotlight 2002]. Once a good keyword search tool is used to make a logical and physical search, it helps to understand the characteristics and properties of suspicious files.
Searching for Deleted Files

There might be situations where the suspect might have deleted some important files which might leave some importance evidence. Thus, if the search of active files in unsuccessful, the next priority is to search for deleted files. Whenever, a file is been deleted, the actual content is completely erased from the hard drive only if it is over-written many times. Thus, there are bright chances of recovering those files [Spotlight 2002]. This is a very important phase in gathering useful evidence from deleted files. This could be done using several specialized commercial tools as well as freeware.

Searching Slack and Unallocated Space

Generally, this is the last place to search for the evidence. This represents the ‘nook and cranny’ areas on most storage media created by Windows and DOS due to the mismatch between the actual file size and OS allocated cluster size [Spotlight 2002]. However it is very rare that the file discovered in this area can be recovered entirely. Some criminals may use this place to hide their data so as to keep them unidentified from the investigators. Thus, some very powerful commercial tools are required to unearth the data hidden in this area.

2.2.3 Presenting the Digital Evidence

After the extraction and analysis phase of the digital evidence, proper documentation is necessary to provide the evidence in a coherent, organized and simple-to-understand manner, avoiding confusion. The failure to present the evidence collected in a
technically sound and simple manner in the court of law might result in loosing the court case.

2.3 Rules of Computer Forensics

As the final evidence obtained by the forensics procedure is subject to extensive judicial scrutiny, it is very important to follow legally accepted procedures and rules in order to perform forensics. As the methodology employed is determined by the forensic specialist, the actual process which is applied is to be chosen in such a way that it does not compromise the relevant rules. The rules of forensic computing can be summarized as follows

2.3.1 Minimal Handling of the Original

This is one of the most important rules in the forensic process. It means that the application of computer forensics processes should be kept to an absolute minimum during the examination of the original data source. Any examination that needs to be performed on the original evidence should be conducted in such a way that it does not alter the original data. This can be achieved by duplicating or making a mirror image of the original source of evidence and examining the duplicate data. There are many advantages of this rule. Firstly, it ensures that the integrity of the original data is been preserved in the event of an incorrect or inappropriate process being applied. Secondly, it also allows the examiner to apply several techniques on the duplicated copy when he isn’t sure about the right technique to be applied for that particular case [Ryder 2002]. It also permits multiple forensic specialists to work on the data and finally, it ensures that the original source of evidence is in the perfect state so as to produce it to the court of law.
2.3.2 Account for any Change

Changes are inevitable while performing forensics. During any examination, there might arise a situation where the data needs to be altered or a change becomes inevitable. In such situations, the nature, extent and reason of or such changes should be properly documented and presented during the trial. Here, the examiner must fully understand the nature of the change before that particular change is initiated. Also, the examiner must be able to correctly identify the scope of the change and must be able to give detailed explanation of why that particular change is necessary [Ryder 2002].

2.3.3 Comply With Rules of Evidence

As the final outcome of the forensic process is quite critical, the application of forensic tools and techniques should be undertaken with regard to relevant rules of evidence. One of the fundamental requirements of the forensic computing is the need to ensure that the forensic procedures do not lessen the final admissibility of the final evidence produced. Another important factor related to rules of evidence which is to be considered is that the manner in which the evidence is presented [Ryder 2002]. That is, the method chosen to present the evidence should not alter the meaning of the evidence.

2.3.4 Do Not Exceed the Knowledge

The forensic examiner should not carry out any examination procedure that is beyond their current knowledge level or understanding. To achieve this, the examiner should carry out a self assessment in order to understand his level of knowledge and skill. On reaching this point, the examiner can choose to cease any further advancement in the forensic process and let more experienced professional to carry out the further examination. Essentially, sophisticated computer forensic examinations should be undertaken by
extremely skilled and qualified professionals who have appropriate level of training [Ryder 2002]. Finally, Computer forensic staff requires continual training to get used to the advancements in the technology.

2.4 Rules of Evidence

Evidence must be competent, relevant and material to the issue. There are five rules of evidence which help the evidence to be valid in the court of law. They are explained below

2.4.1 Admissibility

The evidence which is gathered should be in such a way that it should be admissible in the court of law. Cyber laws differ based on the country the crime was committed in. Thus, the gathered evidence must meet all the requirements of the court of law in which the particular case is being fought.

2.4.2 Authenticity

Authentication means showing a true copy of the original. If the evidence can’t be tied positively to the particular incident, it can be used to prove nothing. It should be proved in the court of law that the evidence relates to the incident in a relevant way.

2.4.3 Completeness

The evidence collected, which just shows one perspective of the incident is useless. The evidence should be collected in such a way that it can help prove the attacker’s actions and for completeness, it is also necessary to consider and evaluate all evidence available to the investigators and retain that which may contradict or otherwise diminish the reliability
of other potentially incriminating evidence held about the suspect. It is also vital to collect the evidence that eliminates alternative suspects [Ryder 2002].

2.4.4 Reliability

The evidence collected and analysis procedures must not cast doubt on the evidence’s authenticity and veracity [Ryder 2002]. To maintain the reliability, the forensics investigation must proceed according to the legal procedures and rules.

2.4.5 Believable

The evidence that is presented in the court should be clear, easy to understand and believable by a jury. Presenting a binary dump of data to the jury would be meaningless when the jury doesn’t know what it exactly means. Similarly, if the formatted version is presented which can be easily read and understood by a jury, unless the actually relationship of this formatted version to the original binary is shown, there’s no way for the jury to know whether the evidence is faked [Ryder 2002].

2.5 Unreadable System files

There are numerous files used by the operating system for the proper running of the computer system. System files are the hardest working files in the computer: they literally “drive” the computer and house the “drivers” for the mouse, printer, and monitor, among others [Windows 1999]. Every application that is installed has its own set of system files which drive the application and any malfunction related to the application is strongly related to the malfunction of its system files. Some of the system files used by a windows operating system have extensions such as .386, .com, .dll, .drv, .vxd, etc.,. Most of these
system files are unreadable by the user as they are in the computer understandable language.

2.5.1 Windows Index.dat file

In Microsoft Windows Operating systems, index.dat file is used by the Internet Explorer Web browser. The index.dat file runs as an active database, as long as windows is active. It functions as the database for redundant information such as URLs, search queries and recently opened files [Wikipedia 2007]. In the Internet explorer, every Web address visited is sorted in the index.dat file, allowing internet explorer to attempt to find an appropriate match when a user types in an edit field. Separate index.dat files exist for the Internet Explorer history, cache and cookies. Along with the browsing history, e-mail that has been sent or received through Outlook or Outlook express is also being looged.

Index.dat files can be a major source of evidence in some of the cases such as phishing, child pornography, bank fraud, etc., Though the temporary internet files are been deleted the index.dat files remain behind and continue to grow. But, as these files are in unreadable format, these could not be used in gathering evidence. A method that helps in parsing the index.dat file and printing the same in human readable form would greatly help the forensic investigators in gathering evidence related to the criminal activities on the web and present the same to the court of law.

This research concentrates on the method to deploy the index.dat file. This part of research might involve the development of a tool which serves this purpose.

Some of the locations in Windows 2000 and XP where these “index.dat” files can be found are [Acesoft 2006].
Figure 2.1 is a screenshot of the “index.dat” file obtained from a laptop. This screenshot depicts the unread ability of the “index.dat” file when opened with a notepad. The source of the “index.dat” file was \Documents and Settings\Ajay\Local Settings\History\History.IE5\index.dat

Figure 2.1 index.dat file opened with a notepad
3. RESEARCH

This research mainly concentrates on comparison and analysis of forensic commercial, freeware and Anti-Forensic tools which are regularly used by various forensic investigators. Some of the commercial and freeware tools which have been used in this research are Encase, FTK Imager, PC Inspector file recovery, VisualRoute, CD-R Inspector, etc. Throughout this research, all the standardized rules and procedures discussed in the first two sections of this report have been followed.

Each of these tools has been tested for various scenarios and the results are tabulated. By the end of this phase of the research, the scope of each of the above mentioned tools would be clearly explained. As a part of this research, each of these tools has been tested for various scenarios, file formats and conditions. The scenarios for which these tools have been tested and evaluated are explained in a detailed manner in this section of this report.

This research also concentrates on various techniques that could be used in deploying the index.dat files from a computer working on the Windows operating system. In this research, a tool which parses the index.dat file and generates the output in the user readable format has been developed. Some of the user readable format could be in .txt, .xls formats. This phase of the project greatly helps the investigators in gathering very sensitive and important evidence related to the criminals involved in pornography, bank fraud, etc., This section briefly describes the work done as a part of this research on various kinds of tools such as Commercial, Freeware/Shareware, Anti-Forensic tools and DatDetective(Tool developed to read index.dat files).
3.1 Research on Commercial Tools

Commercial tools play a vital role in administering the criminal justice in cyber crimes. All the Law enforcement agencies worldwide mainly depend on expensive commercial tools like Encase, FTK, etc., The prime reason for this is because of the bundle of features each of these tools provide. Two of the commercial tools named Encase and FTK have been discussed in the “Narrative” section of this report. These two tools are the most widely used tools in cyber forensics. Each of these tools has been tested on two of the most widely used removable media, SD-Card and Thumbdrive. Each of the tools has been tested separately on both these removable media based on several scenarios. A brief summary of the scenarios is shown in table 2.1.

Table 2.1 Scenario Table

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Acquisition</td>
<td>To determine if the tool is able to acquire the contents of the device</td>
</tr>
<tr>
<td>Personal Information management applications</td>
<td>To determine if the tool can find information related to Personal Information management applications such as calendar, contacts, e-mails, etc.,</td>
</tr>
<tr>
<td>Web-Email applications</td>
<td>To determine if the tool can find a visited website and exchanged e-mail message information from the system cache.</td>
</tr>
<tr>
<td>Graphic File Formats</td>
<td>To determine of the tool can find all the graphic formatted files acquired from the device.</td>
</tr>
<tr>
<td>Common Compressed file formats</td>
<td>To determine if the tool can find the files located inside the compressed files like .zip and .rar</td>
</tr>
<tr>
<td>Other compressed file formats</td>
<td>To determine if the tool can find the files located inside usual file formats such as .tar, .gz, etc.,</td>
</tr>
<tr>
<td>Deleted Files</td>
<td>To determine if the tool can recover the deleted files from the device.</td>
</tr>
<tr>
<td>Misnamed files</td>
<td>To determine if the tool can recognize file types by headers rather than their extensions.</td>
</tr>
<tr>
<td>Memory cards</td>
<td>To determine of the tool can acquire files stored on a memory card and see if the deleted and misnamed files could be recovered.</td>
</tr>
<tr>
<td>Imaging</td>
<td>To determine if the tool can be used to create a bit-by-bit image of the suspect memory source.</td>
</tr>
<tr>
<td>MD5 Hash</td>
<td>To determine if the tool has the option to determine the MD5 has of the suspects system.</td>
</tr>
<tr>
<td>Summary Printout</td>
<td>To determine of the tool could display the summary of the analysis.</td>
</tr>
</tbody>
</table>
Each of the above mentioned scenarios are designed in such a way that they provide crucial information about the performance of the tool which helps us in evaluating the tool for a particular scenario without any ambiguity. At the end of this phase of research, it is determined if the tool is worth to be used in a particular scenario and also determine the best combination of the tools which could be used to gather the evidence in a particular scenario. The designing of each of the scenarios is explained in a detailed manner below.

Device Acquisition

In order to test for device acquisition, the tool is to be installed on the forensic workstation and various devices which are to be tested are connected to the workstation and acquire the contents. By verifying the information obtained with the information actually on the device, the performance of the tool for this particular scenario is clearly determined.

Personal Information Management applications

By creating various PIM files on the memory device and running the tool on that particular device, it can be determined if they are been found. Some of the files have been deleted and the tool is being run to see if they are been recovered by the tool.

Web-Email applications

By using the system of interest (system used for investigation) to configure itself to the e-mail application such as MS Outlook, the cache (.pst file) is loaded on the systems.
hard drive. When this system is examined using the tool, the tool is expected to find and report the most recent web, web-mail and e-mail activity.

If some of the e-mail and source of the recent Web logins on the system are detected and deleted they are re-examined with the tool to determine if the tool is able to detect and recover them. This gives an idea about the capability of the tool in recovering deleted e-mail contents.

Graphic File Formats

The memory device is loaded with compilation of various graphics formatted files with extensions like .bmp, .jpg, .gif, etc., and all the tools are run on the device to see if they find and display them.

Common compressed file formats

Various files with different extensions like .txt, .bmp, .exe, etc., are included in a folder and the folder is compressed into a common compressed file format like .zip. This is loaded onto the memory device and all the tools are run on this device to determine if the tools detect the files contained inside the compressed folder.

Other Compressed file formats

Various files with different extensions like .txt, .bmp, .exe, etc., are included in a folder and the folder is compressed into an unusual compressed file format like .rar, .tar, .gz, etc.,. This is loaded onto the memory device and all the tools are run on this system to determine if the tools detect the files contained inside the compressed folder.
**Deleted files**

Some of the files are copied onto the memory device and they are later deleted. All the tools are been run on the device to see if the tool is able to recover the deleted files.

**Misnamed files**

The file extensions for some of the files which are present on the memory device are changed. For example, a file name with an extension .jpg is changed to a file with extension .txt. Now all the tools are run on the device to see if the tool is able to detect the misnamed files. This is achieved if the tool has the capability to find any mismatches between the file signatures and file content.

**Memory Card**

Several files with various extensions like .jpg, .txt, .mp3, etc., are copied onto the memory card and is connected to the forensic workstation using suitable memory card adapter. Various tools are run on the memory card to determine if the tools are able to acquire individual files stored on the system and also to determine of the files deleted from the memory card could be acquired.

**Microsoft Outlook .pst file**

The Personal Folders (.pst) files are also called as data file which is personally stored on a computer. These kinds of files are mostly used with Microsoft Windows products like Microsoft Outlook which stores messages, calendar, e-mail contents, etc.,
**Imaging**

The memory device is connected to the forensics workstation and various tools are used on the data source to make a bit-by-bit copy of that data source and the observations are noted. This process not only copies the contents but also copies the contents of the slack and unallocated space.

**MD5 Hash**

MD5 is a widely used Cryptographic hash function with a 128-bit hash value which is commonly used to check the integrity of the files [Wikipedia1 2007]. Various tools are tested on the memory device to determine if they could determine the MD5 hash value of the device.

**Summary Printout**

After the completion of the investigation on the memory device, all the tools are tested to see if they have an option to print the complete summary of the investigation performed using that tool.

The testing scenarios along with the obtained results are been discussed in the testing and evaluation section of this report.

### 3.2 Research on Freeware and Shareware Tools

There are several freeware and shareware tools which serve as lifesavers and cheapest alternatives to the highly expensive commercial forensic tools. A good forensic investigator should never depend on just one tool but always be ready with several other
tools which might be helpful when the prime tool fails to work at the moment. There exist several Freeware and Shareware tools available on the web which have been very helpful to several law enforcement agencies throughout the world. As small organizations wouldn’t be able to afford highly expensive commercial tools, the only possible choice for them is to depend on the shareware and freeware tools. Some of the freeware and shareware tools which are most useful in forensic investigation are been categorized and listed below. Each of these tools has been implemented as a part of this research and the report of each of them is listed in detailed manner in this section.

3.2.1 Hashing Tools

In Forensic terms, the process of creating an exact duplicate of the original suspect’s evidentiary media is termed as “Imaging”. Every copy of the evidentiary media including the duplicate images is to be calculated for their Hash value. A small alteration to any type of evidence, whether it’s a digital evidence or typical identifying evidence, changes the overall character of the evidence and is reflected on the corresponding hash value. There are two main types of hash values which are used by a typical forensic investigator; they are Message Digest Algorithm 5 (MD5) and Secure Hash Algorithm 1 (SHA1). MD5 produces a 30 bit unique value and SHA1 produces a 40 bit unique value. The hash values can be calculated for the drive as a whole or just for a file or a folder with set of files in it [Latent Technology 2006].

Four of the freeware and shareware Forensic Hashing tools are been studied as a part of this research. They are CRC32, DigestIT, HashCalc and MD5.
CRC32

CRC32 can be used as a Forensic tool which performs the Cyclic Redundancy Checksum (CRC) value. A CRC is a “digital signature” representing data. The most common CRC is CRC32 in which digital signature is a unique 32 bit number. CRC32 is a freeware forensic tool which helps a forensic investigator to calculate the CRC value of a single file or a disk drive which helps him in determining the integrity of the data. When a CRC check is been made on the same file several times, the same CRC32 value is expected unless any changes are been made in the file. A minute change of even 1 byte changes the CRC32 value [Friesen 2001]. Figure 3.1 is a basic screenshot of CRC32.

![Figure 3.1 Screenshot of CRC32](image)

The testing scenario and the results for this tool are been listed in the “Testing and Evaluation” section of this report.
**DigestIT**

DigestIT is a freeware cyber forensic tool which allows the law enforcement official to calculate the MD5 or SHA-1 checksum of any single file or set of files. Once this tool is installed on any forensic workstation, the hash signature for a selected file can be easily calculated by just right clicking on the file and selecting the “DigestIT” option from menu. One of the best features of this tool is that DigestIT not only calculates MD5, SHA-1 hash value and verifies the hash value but also verify a file against a signature. These features of the tool help the law enforcement official to determine if the file has been tampered with since the original Hash checksum value was been generated. This feature of the tool is important as even a small minute change of even 1 byte might make the whole evidentiary source useless. It is also necessary that this Hash checksum value is to be calculated for the images and not the original evidentiary source from time to time in order to detect any tampering done to those sources [Ballard 2004]. Summary of this tool is listed below. Figure 3.2 illustrates the implementation of DigestIT.
Figure 3.2 Selection of the Hash value type for a file using DigestIT

The testing scenario and the results for this tool are been listed in the “Testing and Evaluation” section of this report.

HashCalc

HashCalc is a freeware cyber forensic tool which is used to calculate the Hash checksum values for a single file or set of files. This tool is not only helpful in calculating Message Digest (MD) values but also useful in calculating Checksum values and Hash Message Authentication Code (HMAC) values for any file. The major important feature of this tool is that it supports 12 well known and documented hash and checksum algorithms such as MD2, MD4, MD5, SHA1, PANAMA, TIGER, etc.. This tool is more helpful for any forensic investigator as it not only calculates the two basic hash checksum values such as MD5 and SHA-1 but also various other checksum values [SlavaSoft 2007]. The more
the number of checksum values generated for the file, the better it can be monitored for any
tampering occurred for that file. Figure 3.3 illustrates the basic screenshot of HashCalc.

![Figure 3.3 HashCalc Window](image)

The testing scenario and the results for this tool are been listed in the “Testing and Evaluation” section of this report.

**MD5**

MD5 is a basic utility program developed by RSA Data Security Inc. This tool has
the very basic feature of calculating the MD5 hash value of a selected file [Rivest 1991].
This tool can be used for only one reason that it is very small and the executable file can be
stored easily even in the thumb drive or also as an e-mail attachment. This tool being one
of the oldest tools is used in rare cases as many more sophisticated tools have come up.
Figure 3.4 illustrates the basic screenshot of MD5 tool.
The testing scenario and the results for this tool are been listed in the “Testing and Evaluation” section of this report.

As a part of this research, HashCalc seemed to be the best freeware tool that could be used by a Forensic Investigator as it provides higher number of features required to detect the file tampering.

3.2.2 Tracing Tools

Tracing tools are used by several law enforcement officials and network administrators to monitor the entire trace route from one system to anywhere on the web. These tools can also be used in tracking the connectivity problems, finding out where the spam goes from, running the whois queries for all the routing nodes and finding their IP addresses and corresponding domain names. As web based crime is increasing at an alarming rate, there is a need to keep track of the fraud websites and their activities. There are many such instances where a law enforcement official would be interested to know the geographical location of a web server or an IP address. There are tools existing that even show a visual representation of the packet hops using a graph. Some of such tools are been
studied as a part of this research and the description and summary of each of them are been listed in this section of the report.

**Visual Route**

Visual route can be used by network administrators or law enforcement officials to determine the information about a website or an IP address. This also shows the detailed information of the hops made by the packets from the computer from which the website is pinged before it reaches the destination address. This tool helps to know the route which the packets take from the personal computer to reach the destination which helps the investigators to know the different privately used systems and servers from which the data is passing from [Visualware 2007]. Visual route provides a very easy to use interface and a graphical representation of the packet route. User can easily gather information about an IP address or a website including the visual graphical location. This tool has been tested vigorously for its features and the observations are been listed in this section of the report. Figure 3.5 illustrates the basic screenshot of the visual route when it is been used to ping a website.
Figure 3.5 Visualroute used to ping [www.sify.com](http://www.sify.com) from my personal computer

The testing scenario and the results for this tool are been listed in the “Testing and Evaluation” section of this report.

**HyperTrace**

AnalogX HyperTrace is a freeware tracing tool used to find out how exactly information gets from one point to another and to know about the machines through which the packets go through. HyperTrace is a graphical version of traceroute program [AnalogX 2001]. This tool is been tested for its features and performance and the observations, screenshots are listed in this section of the report. Figure 3.6 illustrates the basic screenshot of HyperTrace.
Neo Trace

Neo Trace is another useful tracing tool which provides graphical representation of the traceroute. It not only gives the information about the hops but also provides better feedback than many other tracing tools. Neo trace pro also includes hacker reporting to hacker watch, mail server tracing and powerful map engine. This tool is quite helpful in determining the web server location. Most of the cases related to fraud websites, etc., can be studied carefully by understanding the web server location [NeoTrace 2001]. This tool is been implemented and tested for its features and are listed in this section of the report. Figure 3.7 illustrates the basic screenshot of NeoTrace.
The testing scenario and the results for this tool are been listed in the "Testing and Evaluation" section of this report.

After testing the various features of the three tracing tools discussed above, the tracing tool named “Visual Route” seems to be the best among them as it displayed various important features required by a forensic investigator.

3.2.3 **Source Code Forensic Tools**

Source Code theft have been a biggest threat to the corporate sector since its evolution. Criminal cases related to source code theft have been increasing at an alarming rate worldwide as they involve losses to the Information Technology industry in millions. In spite of various strict rules and regulations framed by Software companies, offenders find their ways to steal the source code in some or the other way and use them for their personal benefits incurring huge losses to the software industry. These factors helped in creating another branch of computer forensics called “Source Code Forensics”. There is a very high requirement for a tool to prove the source code theft and prove the guilt of the offender in the court of law. One such tool is been studied as a part of this research and it is
been tested to study its features and the details of the tool are been listed in this section of the report.

**Araxis Merge**

Araxis Merge is a two-way or three-way file/folder comparison and merging application. It is used to compare and merge source code, web pages, images, text files, etc., It can be used by Law enforcement officials to detect every change made to an original document by comparing both the original as well as the modified version of it. It can also be used to compare, understand and combine several source file versions [Merge 2007]. This tool has been tested vigorously as a part of this research for its features.

The testing scenario and the results for this tool are been listed in the “Testing and Evaluation” section of this report.

**3.2.4 Online E-mail Tracking Tools**

As present day criminals are getting updated with latest trends and technologies, the use of e-mail as a communication media have increased tremendously. Billions of E-mail messages are sent and received everyday worldwide. This turned out to be a challenge to the law enforcement officials to track the people sending and receiving the e-mails. In most of the criminal cases, the information about the geographical location of the recipient of the e-mail serves as a very important evidence and clue in tracking the criminal. Though there are several online and offline tools available to monitor the e-mails, an online e-mail tracking tool has been used in this research which is tested for its features and the observations are documented in this section of the report.
Readnotify

The online tool available at www.readnotify.com is used to monitor the e-mails. Readnotify is a paid service which provides numerous features for a reasonable price. This tool provides many useful features for a law enforcement official to gather required evidence related to the offender. This tool prompts the user to register an e-mail address which would be used to send the e-mail messages to others. After this process, any e-mail which needs to be tracked can be sent with a suffix “.readnotify.com” (For example: abcdefg@yahoo.com.readnotify.com). This e-mail would be closely monitored and the updates are stored and can be checked on the Readnotify website. The updates are also sent to the users primary e-mail address that is been registered with the Readnotify service [ReadNotify 2007]. This tool is been used as a part of this research to test for its features and the observations are been listed in this section of the report along with the screenshots, testing procedure and the summary of the tool. Figure 3.8 illustrates the sample E-mail notification about the tracked E-mail.

Figure 3.8 E-mail notification about the e-mail under constant monitoring

As the crime rate related to web and e-mails are increasing at an alarming rate, there is a necessity for such tools to track the offenders. This tool is being used by majority of the law enforcement agencies worldwide in criminal cases related to phishing, Child
Pornography through E-mails, bank frauds, etc.,. This tool seems to be a highly useful tool in the field of cyber forensics.

The testing scenario and the results for this tool are been listed in the “Testing and Evaluation” section of this report.

3.2.5 CD Recovery and Inspection Tools

One of the most widely used data storage media are CDs and DVDs. These still remain as the favorite data storage media for criminals to store and transport their data easily. Some of the reasons why CDs and DVDs are been used for data storage are their efficiency, portability, higher storage capacity, cheap, etc., Thousands of files of all types could be stored on a single disk and can be transported from one place to another without many hassles. Thus, there is a need for a forensic tool which can both recover the data from these storage media easily and can also analyze the data present on it easily and reduce the investigation time for the investigator. As a part of this research, one of such tools namely “Arrowkey CD-R Inspector” is been studied thoroughly and the results are been listed in this section of the report along with the screenshots and the summary of the tool.

CD-R Inspector

CD-R Inspector is a shareware forensic tool developed by InfinaDyne formerly known as Arrowkey. This tool is highly powerful in inspecting suspect’s CD’s and DVD’s. This tool provides various options for a complete diagnosis of a CD or DVD [InfinaDyne 2007]. Some of the important features of the tool are been explained in detailed manner in
this section of the report and also all the other features are been tested and the results are been tabulated along with the summary of the tool.

This tool is been studied and tested using a Compact Disc (CD). A 700MB compact disc has been filled with random data upto 418MB which contained several files such as .bmp, .wav, .midi, .mp3, .jpeg, .doc, .txt, etc., Figure 3.9 illustrates the CD-R Inspector main window.

![CD-R Inspector Main Window](image)

Figure 3.9  CD-R Inspector Main Window

The testing scenario and the results for this tool are been listed in the “Testing and Evaluation” section of this report.

### 3.2.6 Recovery Tools

Recovery tools play a vital role in cyber crime investigation. In majority of the cases in which the criminal has a prior knowledge about being caught takes all possible measures to eliminate the data and as a part of these trails he would delete the data from the hard drive, making it inaccessible by any other user. This is when the recovery tools come
into action during the cyber forensic investigation. One of the most essential categories of the tools required by a forensic investigator would be data recovery tools. There might be several other instances where these tools would be used. For example, to undelete the data that got accidentally deleted from the storage media. Several recovery tools have been studied as a part of the research but only some of them are been implemented and tested. The tools that are been studied tested are listed in this section of the report.

**PC Inspector File Recovery**

PC Inspector file recovery is a freeware data recovery program that supports two file systems, FAT 12/16/32 and NTFS. It has some of the best features that a forensic recovery tool is supposed to have. Some of its prime features are display of the root data, recovery and display of the deleted content on the storage media and recovery and display of the lost content still present on the storage media [PCI 2007]. This tool has been implemented and tested as a part of this research and the details are listed in this report along with the screenshots. Figure 3.10 illustrates the display of the root files by the tool.
The testing scenario and the results for this tool are been listed in the “Testing and Evaluation” section of this report.

**Flash Retriever**

Storage capacity has been increasing tremendously and so is the portability of the storage media. Even more than 150GB worth data could be carried in a portable storage device. Thus, the use of small flash memory cards in digital cameras, music players, etc., took its way. There is a very high necessity for a forensic tool which is capable of retrieving data from such small storage media.
InfinaDyne’s “Flash Retriever” is a small and easy to use tool which is capable of successfully recovering pictures, movies, sounds, etc., from Smart media, Memory stick, CompactFlash and all other flash memory cards. This tool has been implemented and tested as a part of this research and the details are listed in this section of the report along with the screenshots and the summary of the tool.

This tool works in four steps. In Step1, the tool displays all the flash media attached to the workstation which could be recovered. In step2, the tool gives the user an option to filter the recovery process by providing an option to either check or uncheck various attributes such as recover deleted files, Intensive search for all files, Include incomplete files, types of files present(jpeg, mpeg, avi, mp3, other, etc.). In step3, the tool carries out the recovery process on the media and displays the recovered content. In step4, tool provides an option to the user to preview the recovered content and also copy the selected content onto a different media [InfinaDyneFR 2007]. Figures 3.11 thru 3.14 illustrates the various steps involved in Flash Retriever.
Figure 3.11 Step 1: Flash Retriever displaying all the connected flash storage media

Figure 3.12 Step 2: Flash Retriever provides the option to filter the recovery process
Figure 3.13 Step3: Flash Retriever Recovery Progress

Figure 3.14 Step4: Flash Retriever Preview and copy of the recovered files
The testing scenario and the results for this tool are listed in the “Testing and Evaluation” section of this report.

**GetDataBack**

GetDataBack is another forensic recovery tool which is used to recover various types of data from all kinds of storage media which was been deleted either accidentally or intentionally. This tool was developed by Runtime software to foster the needs of forensic researcher to recover the deleted content from a storage media and unearth the evidence. This tool has some of the most important features a forensic recovery tool should possess. This tool has been implemented and tested as a part of this research and the details are listed in this section of the report along with the screenshots and summary of the tool.

GetDataBack works in five steps. In Step1, the tool scans for various drives on the system and displays it to the user so that one or all of the drives which are to be recovered could be selected. In Step2, the tool allows the user to select one of the drives which is to be recovered and also displays the contents of that particular drive which has been selected. In Step3, the user is given an option to select the range and the file system. The range here implies the range of the sectors which are to be searched for to recover the data. User can also opt to select the entire drive to be recovered. In Step4, the user is given an option to select the file system. In Step5, the tool recovers and displays all the recovered content from the disk [Runtime 2007]. Figures 3.15 thru 3.19 illustrate the various steps involved in the data recovery using GetDataBack.
Figure 3.15 Step 1: GetDataBack Scan for drives

Figure 3.16 Step 2: GetDataBack Selecting Source
Figure 3.17 Step 3: GetDataBack Selecting range and file system

Figure 3.18 Step 4: GetDataBack Selecting File System
The testing scenario and the results for this tool are been listed in the “Testing and Evaluation” section of this report.

3.2.7 Miscellaneous Tools

This section describes the details of various miscellaneous tools used by a forensic investigator. Some of these tools which are studied as a part of this research are Belarc Advisor, Bad Copy, Password Recovery Kit and Invisible Secret. Each of these tools is been tested vigorously and the observations are documented in this section of the report.

Belarc Advisor

Any Forensic examiner needs to have a detailed record of the installed software and hardware including the Microsoft hotfixes and their serial numbers for the computer system.
that is being imaged for examination. This tool analyzes machine’s weak points by looking at the updates of the anti virus software and at the elements which prove that all the security flaws have been patched. Belarc Advisor gives a detailed profile of all the hardware and software packages installed on the computer. This tool has been tested vigorously as a part of this research and the details are listed in this report along with the screenshots. Figure 3.20 illustrates the detailed summary of the computer system that has been examined.

This tool has been installed on a personal computer and the summary of all the hardware, software and operating system components installed on the computer is obtained by running the tool.

Figure 3.20 Detailed Summary of the computer system being examined

The testing scenario and the results for this tool are been listed in the “Testing and Evaluation” section of this report.
Passware Password Recovery Kit

Passware password recovery kit is a powerful password recovery tool covering passwords for the most popular MS office application files such as Excel, Word, Windows XP/NT, Rar, Winzip, Access, Outlook, Adobe Acrobat, Quicken, WordPerfect, VBA, etc. This kit is capable of recovering passwords for opening, workbooks and worksheets, personal folder files, form designs and databases and for accessing user accounts. This tool has been tested for password recovery on various possible files and the details are listed in this report along with the screenshots. Figure 3.21 illustrates the recovered password using the tool.

Figure 3.21 Password Recovery Kit recovered password for MS Excel

The testing scenario and the results for this tool are been listed in the “Testing and Evaluation” section of this report.
3.3 Research on Anti-Forensics

Attempts to negatively affect the existence, amount and/or quality of evidence from a crime scene, or make the analysis and examination or evidence difficult or impossible to conduct [Rogers 2006]. Every technology can be seen in the positive as well as negative perspective. The proper use or the misuse of the technology depends on the purpose for which it is being used. Along with the recent advancements in various computer forensic tools, Antiforensics is also gaining a lot of importance. While researchers in computer forensics field are striving hard to discover various methods and tools to gather evidence in order to prove the crime in the court of law, offenders are trying to develop various antiforensic tools and also make use of the flaws in the digital devices to mislead the law enforcement officials. There are several antiforensic tools available for sale on the web, some of them being highly powerful when compared to their forensic counterparts. In some circumstances, Antiforensic tools can be used to take proper care to securely hide or delete the information before it goes into the hands of offenders. Some of the instances where Antiforensics can be used for a good cause are:

- Use of Antiforensics in defense to securely hide/delete the sensitive and confidential information.
- Use of Antiforensics in securing the system by hiding/deleting the information before it reaches the hackers and offenders.

Use of Antiforensics in Defense Department

One of the departments in any country which usually carries the most sensitive and confidential information about national security is defense department. There are several cases where the government officials belonging to defense department travel on an official
work to several places and several countries too sometimes. Thus, they need to be very careful about the information they carry in their laptops and other digital devices as they could serve as hints to the anti-social elements and could leak highly sensitive information relate to national security. Every defense department professional who uses the computer need not be a computer techie and so might not be aware of the loopholes of the operating system and the other applications which are being run on that computer. Thus, it is an important task to educate the defense professionals with different ways of securing the data on their digital devices. Some of the various locations in the operating system as well as the computer which are to be regularly monitored and cleaned as they serve as the safe storage for where some important information are:

- **Windows Swap File**
  To execute any program in windows, it first needs to be loaded onto the main memory (RAM). When multiple programs run simultaneously in windows, there are pretty good chances that they don’t fit on the computer’s RAM and so windows maintains a special file on the hard drive called Swap File which serves as a virtual memory to simulate RAM. The data is moved from real memory to this swap file and moved back to the real memory once free space is been found on the real memory [SwapFile 2007].

- **Windows Application Logs**
  On a windows system, all the reporting services write the event messages to the windows application log. The information written o the application log
can be used to find out about the events that are generated by the report server applications running on the local system [Windows Application Log 2007].

- Windows temporary files
  These are the files that start with a tilde (~) character or with an extension .TMP. These files are been created by windows and survive until windows session exists and they closedown as soon as the windows session is closed. But sometimes due to the irregular exit from the windows session like restarting the computer without closing the windows session, they remain on the hard drive until they are been removed [Windows Temporary Files 2005].

- Windows Recycle Bin
  All the content that is been deleted from windows reaches the recycle bin. These files reside there until they are been removed. The contents of the recycle bin can be restored at any time. Thus this serves as another important area in windows that needs monitoring and cleaning.

- Windows Registry Backups
  Windows registry holds all the important information about the computer. It holds the information about the type of hardware installed, the software installed etc., Usually, the registry back is made by users to save the registry information as it might be helpful in restoring the system to a safer state.
when the system crashes. Thus this is one important item which is to be monitored and the information is to be cleared [Registry 2007].

- **Windows Clipboard Data**

  A windows clipboard is a set of functions that enables applications to transfer data. As all the applications have the access to the clipboard, the information can be transferred easily between different applications or within the application [Clipboard 2007]. An example of the usage of the clipboard is the copy (Ctrl+C) and paste (Ctrl+V) functions in the windows.

- **Windows Recent Document history**

  Windows maintains a history of recently opened or accessed documents.

- **Windows Run History**

  Windows maintains a history of recently typed in commands or paths

- **Windows Find files history**

  Windows maintains a history of the recently searched files using the Find files feature

- **History related to Windows media player**

- **History related to Windows media player playlists in media library**

- **History related to Yahoo, MSN and AOL instant messenger contacts**

- **Netscape navigator temporarily typed URLs, Files, cache and history**

- **Netscape Navigator Cookies**

- **Netscape mail history of sent and deleted e-mails**

- **Netscape mail hidden files**

60
• Deleted filenames sizes and attributes from drive directory structures
• Microsoft Internet explorer history of visited URL’s, index.dat files, cache and history
• Microsoft Internet explorer’s autocomplete memory of form posts and passwords
• Microsoft internet explorer’s cookies
• Microsoft internet explorer’s internet components
• Microsoft internet explorer’s download folder memory
• Microsoft internet explorer’s Favorites list
• Microsoft Outlook Express .pst file
• Free slack from all file tips
• All free unallocated space on all hard drives
• Evidence of activity in many other programs using plug-in modules
• Slack space and deleted entries in the windows registry
• Timestamps (Created and modified dates and times) on all files and folders.
• Windows registry streams

**Antiforensic Tools**

Forensic investigation tools as necessary to gather the traces of the digital evidence from the suspect’s digital media and on the other hand its counterpart, the Antiforensic tools are used in sensitive government areas to securely hide/delete the confidential data before it reaches the hands of the offenders. Some of the Antiforensic tools like Clear
History and Cyber Scrub are helpful in carrying out this task and are explained in detailed manner in the following section.

### 3.3.1 CyberScrub Privacy Suite

CyberScrub Privacy suite is a high level military grade application developed to securely and completely eliminate all the required sensitive information on a computer. It not only works well for securely eliminating the files created as a result of offline activities but also the ones created as a result of online activities such as internet browsing and E-mail’s. CyberScrub products are been used by many important government departments in US such as US Department of Defense, US Air Force and Army and many other large companies. It has also bagged the prestigious ZDNet5 Star Editors pick. CyberScrub Privacy Suite is been published by CyberScrub LLC and is a shareware. Trial version can be downloaded for free from the website [http://www.cyberscrub.com/](http://www.cyberscrub.com/) and the full version can be purchased for $49.95 from the same website. CyberScrub is clean with no adware, spyware or any kind of malware [CyberScrub 2002]. This tool has been tested vigorously as a part of this research and the details are listed in this report along with the screenshots and the summary of the tool. Figure 3.22 illustrates the sample home screen of Cyber Scrub.

### Features of CyberScrub Privacy Suite

- The settings of this application can be configured so that it automatically removes all the evidence related to the online activity either at the start of the computer or
during the shut down process. This could be done using the ‘Scheduler’ option in
the tools menu.

• Data encryption can be done using a feature called “safe” which could be accessed
from the main screen. This helps in protecting the sensitive data using the most
secure and sophisticated methods.

• The E-mails deleted can be made non-recoverable using the “Deleted E-mail”
button from the main screen.

• Erasing files or folders can be done securely by simple drag and drop procedure and
selecting “Erase all” feature.

• Access to the CyberScrub Privacy Suite can be restricted using an entry password
feature.

• Log file is maintained which records all the operations performed and errors
occurred during the particular operation.

• Files or folders can be erased securely from the hard drive using the “Erase beyond
recovery” feature so that even sophisticated recovery tools fail to recover the files.

• All evidence related to the online activity can be removed permanently by running
the feature called “Privacy Guard”.

The testing scenario and the results for this tool are been listed in the “Testing and
Evaluation” section of this report.
3.3.2 Clear History

Clear History is another Anti Forensic tool which helps the forensic investigators to erase the data securely before it gets into the hands of the offenders and they could misuse it. Clear History is a freeware Antiforensics tool helpful in not only eliminating the web history but also in eliminating the files generated as a part of the offline activity on the stand alone computer such as temporary files. Clear History can also be used as a junk remover. This tool was developed by Clear History Software and can be downloaded for free from http://www.clear-history.net. This tool is clean and does not contain adware, spyware or any other kind of malware [Clear History]. This tool has been tested vigorously as a part of this research and the details are listed in this report along with the screenshots and the summary of the tool. Figure 3.23 illustrates the basic screenshot of Clear History.
Features of Clear History

- User friendly interface
- It has the ability to clear the search history, location bar history, browsing history, etc.,
- It has the ability to clear the cache, download history and the cookies. It also provides user an option to exclude any of the cookies from deletion.
- It has the ability to erase the locked windows files such as index.dat
- It has the ability to clear history from MS Office applications, Windows applications and autocomplete forms.
- It not only clears the Internet explorer history files but also works well with the Firefox history.
- It gives the user an option to select the particular files that are to be erased and also can erase the files beyond recovery even by the most sophisticated recovery tools.
- It can erase other tracks such as WinZip, WinRar, Windows Media player, Microsoft WordPad and Media player classic.
- It also has features to erase windows tracks such as recent documents, run history, find/search history, clipboard history and open-save dialog history.
The testing scenario and the results for this tool are been listed in the “Testing and Evaluation” section of this report.

3.4 Research on Unreadable Windows index.dat files

Though there are many unreadable files on the system which could be used for investigation, main focus has been laid on one of the files called “index.dat” throughout this research.
3.4.1 DatDetective, A Tool To Read index.dat Files

A tool has been developed as a part of this research which parses through the index.dat files and displays the contents of the file in the user readable form i.e., it converts the computer readable form of the index.dat file into general English language.

This tool is been named “DatDetective”. Figures 3.24 thru 3.28 illustrates the various screenshots of the menu items of DatDetective.

Figure 3.24 Main Window of the tool DatDetective

About DatDetective

The tool is named “DatDetective”. This tool has a user friendly GUI and gives options to the investigator to open the index.dat file from any location on the hard drive and display its contents. It also has the capability to search for the index.dat files on the disk if the investigator isn’t sure about the specific location. The features of this tool are listed below.

- The tool, DatDetective is designed to provide the investigator a very friendly GUI
• DatDetective has a menu bar with various items such as File, Edit, View and Help
• DatDetective provides an option to the investigator to select an index.dat file from any location on the hard drive.
• DatDetective also provides an option to the investigator to search for the index.dat files on the hard drive if the investigator isn’t sure about the accurate location.
• DatDetective provides an option to the user to save the results obtained in the form of a .csv, .txt or .doc. This helps the investigator to analyze the file more accurately and also print the results.
• DatDetective provides an option to ‘copy’ only selected row from the result obtained and paste it elsewhere in any other application.
• DatDetective provides an option to the investigator to change the size of the main window of the tool using the “view” item in the “menu” bar.
• DatDetective is designed to provide “Help” menu to provide support to the investigators in explaining the steps to be followed while using the tool and other general information about the index.dat file.

The Menu bar of the DatDetective has several Menus such as “File”, “Edit”, “View” and “Help”. Each of them has sub menu items. They are

**File Menu**

- **Open**
  - Open an existing file from a given location
- **Find**
  - Scans the hard disk for the selected index.dat files
- **Close**
  - Closes an already opened file
Save as  This provides an option to save the report in any of the forms such as .csv, .doc or .txt.

Exit  This exits DatDetective

Figure 3.25 File Menu of DatDetective

Edit Menu

Copy  Copies data from the document to the clipboard

Figure 3.26 Edit Menu of DatDetective
**View Menu**

**Full Screen**  
Main window of the tool is being shown as a full screen

**Half Size**  
Main window is half the screen size

**Normal Size**  
Main window is of normal size

![Full Screen Menu](image)

*Figure 3.27 View Menu of DatDetective*

**Help menu**

**Help Topics**  
This explains the basic details of index.dat files and explains the steps involved in using DatDetective

**About DatDetective**  
This has the details of the developers of the tool.

![Help Menu](image)

*Figure 3.28 Help Menu of DatDetective*
This tool has been vigorously tested in various conditions and scenarios as it plays an important role in gathering evidence which could be used in a court of law. Various testing scenarios used to test this tool are discussed in detail in the “Testing and Evaluation” section of this report.

**Technology Used For Development of the Tool**

Java is been used to develop the tool, DatDetective. JDK 1.5 is been downloaded from the Sun Microsystems website at [http://java.sun.com](http://java.sun.com). Java Applets have been used to create the front-end to the tool. Some of the reasons for using Java as a programming language to develop the tool are

- It implements the object oriented programming methodology
- It is platform independence
- It is designed to execute code from remote sources securely

**System Requirements to implement the tool**

The system requirements for the forensic workstation using the tool, DatDetective are

- Hard Drive – 10GB
- RAM – 16MB
- Java J2SDK 1.5
Working of The Tool

Step1: Index.dat file can be opened using the menu item called “Open” from File menu. Using this, the user can select the index.dat file at a specific location on the hard drive. Index.dat can also be searched on the hard drive using the menu item called “Find” from in File menu.

Step2: Once the index.dat file is been selected, the tool displays the contents of the index.dat file in another window inside the main window.

Step 3: The displayed results can be saved on the computer hard drive in any of the three forms such as .csv, .doc or .txt using the “Save as” menu item from the File menu. Once the “Save as” menu item is selected, a dropdown list is displayed which gives an option to select among the file types (.csv, .doc or .txt) in which the result is to be saved.

Step 4: In order to close the result window, “Close” menu item from the File menu can be used.

Step 5: In order to copy just a small portion of the result obtained onto the clipboard, “copy” menu item from the Edit menu can be used.

Step 6: To Exit the tool, “Exit” menu item from the File menu can be used.

Uses of DatDetective

DatDetective can be used in various areas such as Universities, Home, by Law enforcement agencies, etc., to track the browsing habits of the students, children and offenders respectively. The areas in which this tool can be used are described next.
Universities

Every university frames several policies and rules for the students and staff using the computers on-campus. One of the common policies being a ban on the visit of improper URLs such as pornographic sites. Thus, DatDetective can be used in the universities to track the browsing habits of the students and staff so that they could be appropriately punished if found breaking the university policies. Every university provides a username for every computer user on-campus and one of the wonderful features of the tool is that it displays a report of all the URLs visited along with the name of the user who visited the URL.

Home

As internet is getting widespread, it became one of the basic necessities of every household. Thus, the rate at which young children viewing pornographic sites is increasing at an alarming rate. Thus, it is necessary for the parents to keep an eye on their children’s browsing habits. DatDetective could be used by parents to monitor the browsing habits of their children at home.

Use of DatDetective by Law Enforcement Officials

DatDetective could be used by Law enforcement agencies to gather the evidence from suspect’s computer to prove the guilt in the court of law. Most of the present day criminal cases in someway or the other involves the evidence related to the browsing history of the offender. In most of the cases, the offender also tries to erase the evidence related to browsing history by deleting the temporary internet files, cookies, etc., Thus,
DatDetective could be used to study the locked windows file such as index.dat to gather the evidence related to the browsing history.

The testing scenario and the results for this tool are been listed in the “Testing and Evaluation” section of this report.
4. TESTING AND EVALUATION

Testing plays an important role in this research project. The testing phase in this research project is sub classified into four parts. First part of the testing concentrates on testing the commercial tools used in this research. Second part concentrates on testing various freeware and shareware tools. Third part concentrates on testing the Anti-forensic tools and the fourth part concentrates on testing the tool, DatDetective that is been developed as a part of this research. Various testing scenarios along with the testing results have been explained in this part of the document.

4.1 Testing Commercial Forensic Tools

Two of the Commercial Forensic tools have been discussed in this report. They are Encase and FTK. These tools have been tested on two of the storage media such as SD-Card and Thumbdrive. The brief summary of the test cases for each of the storage media is as follows.

SD-Card

Test case 1: SD-Card has been plugged inside the camera and it is been used to capture images onto the SD-Card. Now after the image capturing process has been completed, some of the files have been deleted and the details and description of the deleted files have been noted before deletion so as to make sure that the tool is able to recover all these deleted files.
**Test Case 2:** Several Assorted files of various categories such as .txt, .bmp, .jpeg, .avi, .mp3, misnamed files, deleted files etc., are been loaded onto the SD-Card and some of this content has been deleted and tested using the tool to determine if it is able to recognize and display all the content of the SD-Card along with the deleted content.

**Test Case 3:** This test case mainly concentrates on testing the Outlook file namely “.pst”. The .pst file has been grown in size with e-mails, contacts, calendar, etc., and some of its content is been deleted and details have been noted before it is been tested. This .pst file has been loaded on to the SD-Card to determine if the deleted content could be recovered using the tool.

**Thumbdrive**

**Test Case 1:** Several Assorted files of various categories such as .txt, .bmp, .jpeg, .avi, .mp3, misnamed files, deleted files etc., are been loaded onto the Thumbdrive and some of this content has been deleted and tested using the tool to determine if it is able to recognize and display all the content of the storage media along with the deleted content.

**Test Case 2:** This test case mainly concentrates on testing the Outlook file namely “.pst”. The .pst file has been grown in size with e-mails, contacts, calendar, etc., and some of its content is been deleted and details are been noted before it is been tested. This .pst file has been loaded on to the Thumbdrive to determine if the deleted content could be recovered using the tool.
4.1.1 Encase

Encase is a commercial Forensic tool which has been studied for its features on two storage media SD-Card and Thumbdrive and the results are tabulated below. Figure 4.2 illustrates the Encase View Pane and Figure 4.2 illustrates the deleted files recovered using Encase. Table 4.1 illustrates the results obtained during the study of Encase on SDcard.

Table 4.1 Encase-SDCard

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Result</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is Encase able to recover all the image files from SD card which are deleted using camera’s inbuilt “delete” option</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>Is Encase able to recover all the</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td><strong>Video files</strong> from SD card which are deleted using camera’s inbuilt “delete” option</td>
<td>Is Encase able to recover all the <strong>image files</strong> from SD card which are deleted using Windows</td>
<td>NO</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Is Encase able to recover all the <strong>Video files</strong> from SD card which are deleted using camera’s inbuilt “delete” option</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>Is Encase able to recover all the <strong>image files</strong> from SD card which are deleted using Windows</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>Is Encase able to recover the <strong>.pst</strong> file</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>Is Encase able to recover the Personal Information Management files related to Outlook <strong>.pst</strong> file</td>
<td>NOT ALL</td>
<td>Size of the .pst file before and after deletion of e-mails and PIM’s didn’t change. But still tool was able to recover few but not all</td>
</tr>
<tr>
<td>Is Encase able to recover all the e-mails deleted from the <strong>.pst</strong> file when the <strong>.pst</strong> file is on the SD-Card</td>
<td>NOT ALL</td>
<td>Size of the .pst file before and after deletion of e-mails and PIM’s didn’t change. But still tool was able to recover few but not all</td>
</tr>
<tr>
<td>Is Encase able to recover all the e-mail deleted from <strong>.pst</strong> file when the <strong>.pst</strong> file is on the computer with windows OS</td>
<td>NOT ALL</td>
<td>Size of the .pst file before and after deletion of e-mails and PIM’s didn’t change. But still tool was able to recover few but not all</td>
</tr>
<tr>
<td>No. of E-mails deleted/No. of E-mails recovered</td>
<td>4/2</td>
<td>-</td>
</tr>
<tr>
<td>Attachments related to the deleted E-mails Recovered?</td>
<td>Yes</td>
<td>Attachments were been recovered only for those e-mails which were been recovered</td>
</tr>
<tr>
<td>Device Acquisition</td>
<td>YES</td>
<td>Tool provided Device Acquisition feature</td>
</tr>
<tr>
<td>Graphic File Formats</td>
<td>YES</td>
<td>Tool could recognize and recover various graphic file formats</td>
</tr>
<tr>
<td>Common Compressed file formats</td>
<td>YES</td>
<td>Tool could recognize and recover various compressed file format</td>
</tr>
<tr>
<td>Other compressed file formats</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>Deleted Files</td>
<td>YES</td>
<td>Tool could successfully recover all the deleted content</td>
</tr>
<tr>
<td>Misnamed files</td>
<td>NOT ALL</td>
<td>Tool was able to recognize most of the misnamed files but it failed to recognize few signatures like mp3 and files like mp3 file misnamed as gif</td>
</tr>
<tr>
<td>Imaging</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>MD5 Hash</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>Summary Printout</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>Any Unknown File Types</td>
<td>YES</td>
<td>Mp3</td>
</tr>
<tr>
<td>Any File types Unrecognized</td>
<td>YES</td>
<td>An Mp3 File converted to GIF</td>
</tr>
</tbody>
</table>
Figure 4.2 Deleted files recovered using Encase

Figure 4.3 illustrates the .pst file recovered using Encase. Table 4.2 illustrates the results obtained during the study of Encase on Thumbdrive.

Table 4.2 Encase-Thumbdrive

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Result</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is Encase able recognize and read “.pst” file</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>Is Encase able to recover the Personal Information Management files related to Outlook “.pst” file</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>Is Encase able to recover all the e-mails and PIM’s deleted from the “.pst” file when the “.pst” file is on the Thumbdrive</td>
<td>NOT ALL</td>
<td>Size of the .pst file before and after deletion of e-mails and PIM’s didn’t change. But still tool was able to recover few but not all</td>
</tr>
<tr>
<td>Is Encase able to recover all the e-mails and PIM’s deleted from “.pst” file when the “.pst” file is on the computer with windows OS</td>
<td>NOT ALL</td>
<td>Size of the .pst file before and after deletion of e-mails and PIM’s didn’t change. But still tool was able to recover few e-mails but not all</td>
</tr>
<tr>
<td>No. of E-mails deleted/No. of E-mails recovered</td>
<td>4/2</td>
<td>-</td>
</tr>
<tr>
<td>Feature</td>
<td>Status</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Attachments related to the deleted E-mails Recovered?</td>
<td>Yes</td>
<td>Attachments were been recovered only for those e-mails which were been recovered</td>
</tr>
<tr>
<td>Device Acquisition</td>
<td>YES</td>
<td>Tool provided Device Acquisition feature</td>
</tr>
<tr>
<td>Graphic File Formats</td>
<td>YES</td>
<td>Tool could recognize and recover various graphic file formats</td>
</tr>
<tr>
<td>Common Compressed file formats</td>
<td>YES</td>
<td>Tool could recognize and recover various compressed file format</td>
</tr>
<tr>
<td>Other compressed file formats</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Deleted Files</td>
<td>YES</td>
<td>Tool could successfully recover all the deleted content</td>
</tr>
<tr>
<td>Misnamed files</td>
<td>NOT ALL</td>
<td>Tool was able to recognize most of the misnamed files but it failed to recognize few signatures like mp3 and files like mp3 file misnamed as gif</td>
</tr>
<tr>
<td>Imaging</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>MD5 Hash</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Summary Printout</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Any Unknown File Types</td>
<td>YES</td>
<td>An Mp3 File converted to GIF</td>
</tr>
<tr>
<td>Any File types Unrecognized</td>
<td>YES</td>
<td></td>
</tr>
</tbody>
</table>
4.1.2 Forensic Tool Kit (FTK)

FTK is a commercial Forensic tool which has been studied for its features on two storage media SD-Card and Thumbdrive and the results are tabulated below. Figure 4.4 illustrates the FTK basic screenshot and Figure 4.5 illustrates the deleted files recovered using FTK, Figure 4.6 illustrates the FTK’s capability to recognize PIM files, Figure 4.7 illustrates misnamed files recovered by FTK and Figure 4.8 illustrates the deleted E-mail attachment recovered from .pst file by FTK. Table 4.3 illustrates the results obtained during the study of FTK on SDcard and Table 4.4 illustrates the results obtained during the study of FTK on Thumbdrive.

![FTK Basic Screenshot](image)

**Table 4.3 FTK-SDCard**

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Result</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is FTK able to recover all the <strong>image files</strong> from SD card which are deleted using camera’s inbuilt</td>
<td>YES</td>
<td>-</td>
</tr>
</tbody>
</table>

81
<table>
<thead>
<tr>
<th>“delete” option</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Is FTK able to recover all the <strong>Video files</strong> from SD card which are deleted using camera’s inbuilt “delete” option</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>Is FTK able to recover all the <strong>image files</strong> from SD card which are deleted using Windows</td>
<td>YES</td>
<td>All Image files recovered and viewed</td>
</tr>
<tr>
<td>Is FTK able to recover all the <strong>Video files</strong> from SD card which are deleted using camera’s inbuilt “delete” option</td>
<td>NO</td>
<td>One video file got overwritten and could be recovered but could not be viewed</td>
</tr>
<tr>
<td>Is FTK able to recognize and read “.pst” file</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>Is FTK able to recover the Personal Information Management files related to Outlook “.pst” file</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>Is FTK able to recover all the e-mails deleted from the “.pst” file when the “.pst” file is on the SD-Card</td>
<td>NOT ALL</td>
<td>Size of the .pst file before and after deletion of e-mails and PIM’s didn’t change. But still tool was able to recover all the deleted e-mails except for one.</td>
</tr>
<tr>
<td>Is FTK able to recover all the e-mail deleted from “.pst” file when the “.pst” file is on the computer with windows OS</td>
<td>NOT ALL</td>
<td>Size of the .pst file before and after deletion of e-mails and PIM’s didn’t change. But still tool was able to recover few but not all</td>
</tr>
<tr>
<td>No. of E-mails deleted/No. of E-mails recovered</td>
<td>4/3</td>
<td>-</td>
</tr>
<tr>
<td>Attachments related to the deleted E-mails Recovered?</td>
<td>Yes</td>
<td>Attachments were been recovered only for those e-mails which were been recovered</td>
</tr>
<tr>
<td>Device Acquisition</td>
<td>YES</td>
<td>Tool provided Device Acquisition feature</td>
</tr>
<tr>
<td>Graphic File Formats</td>
<td>YES</td>
<td>Tool could recognize and recover various graphic file formats</td>
</tr>
<tr>
<td>Common Compressed file formats</td>
<td>YES</td>
<td>Tool could recognize and recover various compressed file format</td>
</tr>
<tr>
<td>Other compressed file formats</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>Deleted Files</td>
<td>YES</td>
<td>Tool could successfully recover all the deleted content</td>
</tr>
<tr>
<td>Misnamed files</td>
<td>NOT ALL</td>
<td>Tool was able to recognize most of the misnamed files but it failed to recognize few signatures like mp3 and files like mp3 file misnamed as gif</td>
</tr>
<tr>
<td>Imaging</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>MD5 Hash</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>Summary Printout</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>Any Unknown File Types</td>
<td>YES</td>
<td>1) .Midi file extension changed to .jpg 2) .mp3 changed to .gif</td>
</tr>
<tr>
<td>Any File types Unrecognized</td>
<td>YES</td>
<td>.au, .mp3, .ra</td>
</tr>
</tbody>
</table>
Figure 4.5 FTK Recovered Deleted Files from SD-Card

Figure 4.6 FTK’s capability to recognize PIM files

Table 4.4 FTK-Thumbdrive

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Result</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is FTK able recognize and read “.pst” file</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>Is FTK able to recover the</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>Personal Information Management files related to Outlook &quot;.pst&quot; file</td>
<td>YES</td>
<td>Size of the .pst file before and after deletion of e-mails and PIM’s didn’t change. But still tool was able to recover few but not all</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Is FTK able to recover all the e-mails and PIM’s deleted from the &quot;.pst&quot; file when the &quot;.pst&quot; file is on the Thumbdrive</td>
<td>NO</td>
<td>Size of the .pst file before and after deletion of e-mails and PIM’s didn’t change. But still tool was able to recover few e-mails but not all</td>
</tr>
<tr>
<td>No. of E-mails deleted/No. of E-mails recovered</td>
<td>4/3</td>
<td>-</td>
</tr>
<tr>
<td>Attachments related to the deleted E-mails Recovered?</td>
<td>YES</td>
<td>Attachments were been recovered only for those e-mails which were been recovered</td>
</tr>
<tr>
<td>Device Acquisition</td>
<td>YES</td>
<td>Tool provided Device Acquisition feature</td>
</tr>
<tr>
<td>Graphic File Formats</td>
<td>YES</td>
<td>Tool could recognize and recover various graphic file formats</td>
</tr>
<tr>
<td>Common Compressed file formats</td>
<td>NOT ALL</td>
<td>Tool could recognize and recover various compressed file format</td>
</tr>
<tr>
<td>Other compressed file formats</td>
<td>NOT ALL</td>
<td>-</td>
</tr>
<tr>
<td>Deleted Files</td>
<td>YES</td>
<td>Tool could successfully recover all the deleted content</td>
</tr>
<tr>
<td>Misnamed files</td>
<td>YES</td>
<td>Tool was able to recognize most of the misnamed files but it failed to recognize few signatures like mp3 and files like mp3 file misnamed as gif</td>
</tr>
<tr>
<td>Imaging</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>MD5 Hash</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>Summary Printout</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>Any Unknown File Types</td>
<td>YES</td>
<td>1) Midi file extension changed to .jpg 2) mp3 changed to .gif</td>
</tr>
<tr>
<td>Any File types Unrecognized</td>
<td>YES</td>
<td>.au, .mp3, .ra</td>
</tr>
</tbody>
</table>
Figure 4.7 Misnamed Files recovered by FTK

Figure 4.8 Deleted E-mail attachment recovered from .pst file by FTK
4.2 Testing Freeware and Shareware Tools

Various Freeware and Shareware tools that are been studied as a part of this research are tested vigorously for their features and the results along with the testing scenarios are as follows.

4.2.1 Testing the Hashing Tools

Four hashing tools have been studied during this research and their results and testing scenarios are as follows.

CRC32

CRC32 is a hashing tool which has been studied as a part of this research. The testing scenario and the results are as follows. Figure 4.9 illustrates the comparison of the same .txt file before and after the deletion of a single byte of data and Figure 4.10 illustrates the CRC32 value calculated for an .avi file.

Testing Scenario

- Scenario1: A text file with extension “.txt” is to be checked thrice for its CRC32 value before making any changes on it to see if the tool displays the same CRC32 values all the three times.

- Scenario2: The same image file residing on different computers is to be checked for CRC32 value. This process has been followed for several different types of files such as .txt, .gif, .wav, .mp3, etc.
• Scenario 3: Small changes are been made in the .txt file such as adding an extra blank space on the last line. Changing the line feed, etc., and this is tested for CRC value to see if it displays any changes.

• Scenario 4: The filename of a file is to be changed and the effect og this change on the CRC32 value is been checked.

Observations

• The tool, CRC32 displayed the same CRC value when the same .txt file has been calculated for CRC value thrice.

• The same image file residing on different computers has been checked for CRC32 value and it turned out to be the same. This process has been checked for several different types of files such as .txt, .gif, .wav, .mp3, etc.,.

• Small changes are been made in the .txt file such as adding an extra blank space on the last line. Changing the line feed, etc., and this is tested for CRC value and it showed a change when compared to the original file. Screenshot of the same is listed below.

• The change of filename did not show any effect on the CRC value of the file.
Figure 4.9 Comparison of the same .txt file before and after the deletion of a single byte of data

Figure 4.10 CRC32 Calculated for an .avi file
DigestIT

DigestIT is a hashing tool which has been studied as a part of this research. The testing scenario and the results are as follows. Figure 4.11 illustrates the MD5 calculated for the .doc file, Figure 4.12 illustrates the MD5 After deletion of a single full stop from the .doc file and Figure 4.13 illustrates the SHA-1 Calculated for the same .doc file.

Testing Scenario

- Scenario 1: A MS-Word with an extension “.doc” is to be selected for the test and is to be tested for its hash value before and after deletion of a single character in it to note the effect of deletion of a single character in the document.
- Scenario 2: With the help of Scenario 1, the tool is to be tested if it is able to display both the hash values, MD5 and SHA1.
- Scenario 3: The tool is to be tested on bigger files to check if it takes large amount of time in calculating its hash values.

Observations

- DigestIT is a very easy to use tool which gets installed easily on the windows system.
- There are no hassles observed in running this tool, any file can be selected to view its MD5 or SHA-1 value.
- One noticeable advantage of this tool is that it calculates two hash values which is always helpful and necessary for a law enforcement official in a case where one of the algorithm is compromised by the offender.
• MD5 and SHA-1 are been calculated for several file types and tool returned the appropriate results for each.

• Several tests are been done to test the credibility of the tool. The tool has been tested for the same .doc file before and after the deletion of one single character from the file and it returned different hash values. The screenshots related to this are included in this section of this report.

• DigestIT has an option to copy or save the results obtained and it provides the option to save the results in any format specified by the user.

• Time taken to generate the hash value is been observed to be very less even for bigger sized files.

Figure 4.11 MD5 calculated for the .doc file
Figure 4.12 MD5 After deletion of a single full stop from the .doc file

Figure 4.13 SHA-1 Calculated for the same .doc file
**HashCalc**

HashCalc is a hashing tool which has been studied as a part of this research. The testing scenario and the results are as follows. Figure 4.14 illustrates various hash value types of a single .doc file, Figure 4.15 illustrates different hash values of the same .doc file after addition of some content to it and Figure 4.16 illustrates various hash value types for Text String.

**Testing Scenario**

- **Scenario1:** This tool is to be tested to see if it is capable of display any other hash values other than just MD5 and SHA1. These tests are to be implemented on various files such as music, video, audio, image, MS-Office, etc.,

- **Scenario2:** This tool is to be tested to find out if it takes larger amount of time to check the hash values for larger sized files.

- **Scenario3:** This tool is to be tested to see if it has the capability to save the result in user defined format.

**Observations**

- HashCalc is a freeware tool which could be downloaded and installed easily.

- This tool supports not only the famous MD5 and SHA-1 hash value types but also 10 other hash and checksum value types. This could be observed in the screenshot above.

- It supports two modes of calculations such as Hash/Checksum and HMAC.
• This tool worked well on various file types such as music, video, audio, image, MS-Office, etc.,
• This tool worked swiftly for even larger sized files upto 10GB.
• This tool provides the rare ability to display the various Hash values for Text String, data file and Hex String. The screenshots of the same are displayed in this section.
• This tool also calculates the HMAC value calculated using a cryptographic hash function in combination with a secret key.
• The only drawback which was been observed was that this tool doesn’t have the capability to save the result in the form of a file. In most of the cases this feature would be very necessary for a law enforcement official to save the results from time to time.

Figure 4.14 Various Hash Value types of a single .doc file
Figure 4.15 Different Hash Values of the same .doc file after addition of some content to it

Figure 4.16 Various Hash Value types for Text String
MD5

MD5 is a hashing tool which has been studied as a part of this research. The testing scenario and the results are as follows. Figure 4.17 illustrates the MD5 Hash value calculated for a .doc file.

Testing Scenario

- Scenario1: This tool is to be tested to see if it has the capability to check the hash values for multiple files at a time.
- Scenario2: This tool is to be tested on a basic “.doc” file to see if it can display SHA1 value also along with the MD5 value.
- Scenario3: This tool is to be tested to see if it has the capability to save the results in the user defined file format.

Observations

- MD5 is a very basic tool which has only one feature of calculating the MD5 hash value of a file.
- MD5 doesn’t have the ability to calculate the hash value of multiple files. It just calculates the hash value of a single file at a time.
- MD5 doesn’t have the ability to calculate the SHA-1 hash value of a file.
- MD5 doesn’t have the ability to save the results in the form of a file.
- MD5 worked well only for basic file types but not too many.
Based on the tests results and observations, HashCalc seemed to be the best freeware tool that could be used by a Forensic Investigator as it provides higher number of features required to detect the file tampering.

### 4.2.2 Testing the Tracing Tools

Three tracing tools have been studied during this research and their results and testing scenarios are as follows.

**Visual Route**

Visual Route is a tracing tool which has been studied as a part of this research. The testing scenario and the results are as follows.
Testing Scenario

Scenario: Visualroute is to be implemented as a part of this research from a computer to ping several websites to know the route which the packet takes, any packet loss that occurs, the locations of the intermediate hops and their geographical location, average pinging time, minimum pinging time and maximum pinging time. These tests are been done by pinging a website called www.sify.com whose webserver is located in India. The detailed observations of this test are listed in this section of the report. Figure 4.18 illustrates the screenshot when Visualroute was used to ping www.sify.com from a personal computer.

Observations

- Visualroute was been implemented to ping various websites and the tool was successful in tracing the route and also provided the geographical locations of all the intermediate IP addresses.
- Tool successfully reported the IP location.
- Tool successfully reported the domain whois lookups.
- Tool also provided the ICMP and UDP traceroutes.
- This tool provided an option to provide the snapshot of the report either in text format, jpeg format or the html report.
- This tool provides DNS connectivity analysis.
HyperTrace

HyperTrace is a tracing tool which has been studied as a part of this research. The testing scenario and the results are as follows.

Testing Scenario

- Scenario: This tool is to be tested for various features to see if it provides the features such as number of hops, intermediate IP addresses, response time, Machine name and the percentage loss at that particular point, ability to copy the results in the user defined file format, ability to provide graphical representation of the packet hops and web server location. These tests are been done by pinging a website called www.sify.com whose webserver is located in India. Figure 4.19 illustrates the screenshot when HyperTrace was used to ping www.sify.com.
Observations

- HyperTrace is a very basic tracing program used to trace the route in which the packets pass to reach the destination.

- This tool provided the number of hops, intermediate IP addresses, response time, Machine name and the percentage loss at that particular point.

- This tool provided the feature to copy the results to the clipboard but didn’t provide the option to save the results in the user specified format.

- HyperTrace can also be used to find out about the connectivity problems. For example if there is a 50% loss at any point in the route then it is clear that the connectivity problem exists at that point.

- It didn’t provide the graphical geographical representation of the traceroute using maps.

- This tool didn’t provide the network details unlike the other tool, Virtual route.

- This tool provided the response times but failed to provide the summary details such as minimum, maximum and average response times.

- This tool didn’t seem to be having many features as it worked nothing more than the “Tracert” command in the windows command line.
Neo Trace

NeoTrace is a tracing tool which has been studied as a part of this research. The testing scenario and the results are as follows.

Testing Scenario

Scenario: This tool is been tested to see if it provides the features such as number of hops, intermediate IP addresses, response time, Machine name and the percentage loss at that particular point, ability to copy the results in the user defined file format, ability to provide graphical representation of the packet hops and web server location. These tests are been done by pinging a website called www.sify.com whose webserver is
located in India. Figure 4.20 illustrates the graph showing the final destination web server in India and Figure 4.21 illustrates the window showing the list of hops and IP addresses.

**Observations**

- Neo Trace was successful in displaying the summary of hops taken when a sample website [www.sify.com](http://www.sify.com) is pinged from Corpus Christi, Texas.
- Neo Trace was successful in displaying the graph with intermediate hops when the website [www.sify.com](http://www.sify.com) was been pinged from Corpus Christi, Texas.
- This tool was successful in displaying the time taken at each intermediate node but failed to display the summary of the minimum, maximum and average hop time.
- This tool was successful in displaying the network information related to the final destination.
- This tool has the capability to integrate with the web browser and it can be run directly from the web browser while the website is being viewed.
- This tool finds its major advantage in criminal cases related to fraud websites where the exact location of the web server could be identified.
- This tool couldn’t save the results in the user specified format.
- This tool was successful in displaying the details of the registrant who registered the required domain name.
Figure 4.20 Graph showing the final destination web server in India
After testing the various features of the three tracing tools discussed above, the tracing tool named “Visual Route” seems to be the best among them as it displayed various important features required by a forensic investigator.
4.2.3 Testing the Source Code Forensic Tool

One Source Code Forensic tool has been studied during this research and the results and testing scenarios are as follows.

Araxis Merge

Araxis Merge is a Source Code forensic tool which has been studied as a part of this research. The testing scenario and the results are as follows.

Testing Scenario

- Scenario1: In order to test the “folder comparison” feature of the Araxis Merge, two folders have been created where one of them is considered as the original folder and the other one is considered as the modified folder, both containing image files in them. The modified folder is been added with 5 additional image files and these two folders are stored at different locations on the hard drive. In the screenshot shown in figure 4.22, the left pane indicates the location (Location 1) of the original folder and the right pane indicates the location (Location 2) of the modified folder. The tool is tested to see if it successfully highlighted the files which were been added as well as deleted in either of the folders.

- Scenario2: In order to test the “File comparison” feature of the Araxis Merge, two program files (.C files) were created and prepared for testing. One of them is considered as the original file and the other one is the modified version of the original file. In the screenshot shown figure 4.23, the left pane indicates the original file and the right pane indicates the modified file. The tool is tested to see if it was successful in determining all the changes made to the original file.
• Scenario3: In order to test the “Image comparison” feature of the Araxis Merge, two image files are been created and prepared for testing. One of the image files is considered as an original file and the other one as a modified version of the original image file. In the screenshot shown in figure 4.24, the left pane indicates the original image file and the right pane indicates the modified version. The tool is been tested to see if it was successful in highlighting the pixels which were been changed.

Observations

• The tool was successful in comparing files and in merging them.

• The tool was successful in comparing not only text files but also image files and it successfully showed the pixels which were modified.

• The tool was successful in not only making a two way comparison but also 3 way file comparison.

• The tool was successful in making a folder hierarchy comparison and clearly depicted where exactly the change occurred.

• The tool was successful in making a three way folder comparison.

• The tool was successful in generating file comparison reports in either html format or xml format.

• The tool was successful in displaying the ability to print a hard copy of the file and folder comparisons.

• The tool was successful in providing the comparison statistics mentioning the number of additions made to the original file, number of removals made and total number of changes made to the original file.
The tool displayed the very important feature called “bookmark” which helps the forensic investigator in book marking the important observations made during the file comparison and it also helps the investigator in understanding the case easily even if the case is being studied after reasonably long time after the analysis was been made.

The tool was making a clear color-coded side by side file and folder comparison which is helpful in easily pinpointing the changes between both the files.

In the screenshot shown in figure 4.22, the left pane indicates the location (Location 1) of the original folder and the right pane indicates the location (Location 2) of the modified folder. The tool successfully highlighted the files which were been added as well as deleted in either of the folders.

Figure 4.22 Folder Comparison using Araxis Merge

In the screenshot shown below, the line mentioned as the “line modified” in the right pane indicates the line which is been modified and a line is drawn to the
corresponding original line on to the left pane. The tool could also highlight the line which is been added to the original.

![Figure 4.23 Comparison of source code files (Original and Modified)](image)

In the screenshot shown below, the left pane indicates the original image file and the right pane indicates the modified version. The tool was successful in highlighting the pixels which were been changed. In the screenshot shown below, the red circle in the original image on the left pane is lighter when compared to the red circle on the image on the right pane. This is a clear indication that the original image didn’t have any red circles on them but in the modified version and bookmark was been made on the image.
4.2.4 Testing the Online E-mail Tracking Tool

An online e-mail tracking tool has been studied during this research and the results and testing scenarios are as follows.

Testing Scenario

- Scenario: An E-mail address “ajay.readnotify@gmail.com” has been created as a part of this research and the e-mail sent to this e-mail address is been tracked. Another E-mail ID, ajay.gugu@gmail.com is been registered to obtain the Readnotify services and this serves as a primary e-mail address. An E-mail has been sent from the primary E-mail address to the E-mail ID that is to be tracked. The E-mail that is to be tracked was been sent on 8th OCT 2007 at about 2:47am (American Central Time). A close acquaintance is
been asked to open the e-mail from a city called Hyderabad in India and the e-mail was
been opened on 8th OCT 2007 approximately at 3:07am (American Central time) and it was
been read for approximately 8 minutes. At about 3:10am on 8th OCT 2007, the e-mail
tracking summary was been studied and it returned precise results. The tool was successful
in determining the geographical location including the IP address of the computer on which
it was been opened. Figure 4.25 illustrates summary of the tracked E-mail. The
observations are as follows.

**Observations**

- The tool was successful in recording the details about when the e-mail was opened
  and read.
- The tool was successful in determining the duration of time for which the e-mail
  was been read.
- The tool was successful in determining if the e-mail was forwarded to anybody else.
- The tool provided the date and time of each opening and re-opening of the e-mail
  by all recipients.
- The tool provided a separate breakdown activity for each reader including the
  people the e-mail was been forwarded to.
- The tool provided the detailed information about the recipients IP address and the
  name of the ISP.
- The tool provided the approximate geographical location of the recipient. The tool
  approximately mentioned the geographical location where the e-mail was been
  opened as a city called Mumbai, India which is approximately about 320 miles
  away from the actual location (Hyderabad, India) where the e-mail was opened.
• The tool was successful in determining the URL web clicks made from the e-mail by the recipient.
• The tool was successful in determining the list of languages the recipient understands based on the language that has been set on the computer on which the e-mail was been opened.
• The tool was successful in determining the browser information of the recipient.
• The tool was successful in sending subsequent notifications when the message was re-opened and forwarded.
• This tool provides certified proof of sending and receiving the e-mail and this can be used as evidence in the court of law.
• This tool also provides certified proof of e-mail rendering and this can be used as an evidence to prove the guilt of an offender in the court of law.

Figure 4.25 Summary of the tracked E-mail
4.2.5 Testing the CD Recovery and Inspection Tool

One CD-R recovery tool called CDR Inspector has been studied during this research and their results and testing scenarios are as follows.

CD-R Inspector

CD-R Inspector is a CD recovery and inspection tool which has been studied as a part of this research. The testing scenario and the results are illustrated in the table 4.5.

Testing Scenario

• Scenario: This tool is been studied and tested using a Compact Disc (CD). A 700MB compact disc has been filled with random data upto 418MB which contained several files such as .bmp, .wav, .midi, .mp3, .jpeg, .doc, .txt, etc.,.

Observations

• This tool is been implemented and tested for various features and the results are tabulated below.

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>YES/NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete CD Imaging</td>
<td>Yes</td>
</tr>
<tr>
<td>Volume information</td>
<td>Yes</td>
</tr>
<tr>
<td>Hardware information</td>
<td>Yes</td>
</tr>
<tr>
<td>DVD media recovery</td>
<td>Yes</td>
</tr>
<tr>
<td>File examination</td>
<td>Yes</td>
</tr>
</tbody>
</table>
CD-R Inspector was successful in making a complete or partial image of the compact disk or a DVD. This tool gave an option to select only certain sectors which would be imaged. Figure 4.26 illustrates the selection of certain sectors or entire track to be imaged. Figure 4.27 illustrates the copying of the whole track image of the compact disc.

Figure 4.26 Selection of certain sectors or entire track to be imaged

Figure 4.27 Copying the whole track image of the compact disc
The tool has been used to check the hardware information of the CD-ROM hardware information which is been used to read/access the disc. The tool was successful in displaying the hardware information accurately. Figure 4.28 illustrates the CD-ROM Hardware Information.

![CD-ROM Hardware Information](image)

**Figure 4.28  CD-ROM Hardware Information**

- The tool was successful in saving the whole disc report in the user specified format.

In this research, the disc report is been stored in .txt format. This report gave complete information about all the files and folders present on the disc. Figure 4.29 illustrates the Disc report saved in .txt format.
The “Error summary” option of the CD-R Inspector tests the readability of the CD/DVD. CD-R Inspector displays a graphical representation of the timing measurement from the disc. On selecting the “Error Summary” option, the tool displays a percentage of “recoverable” sectors and a percentage of “unrecoverable” sectors. This refers to what the device has found while reading the disc. A “recoverable” sector can be defined as a sector which could be read by the CD device by performing some error recovery upon the data. One drawback of this option is that this tool scans even those areas on the disc which are left out without writing data on it and thus it returns an error reading those areas of the disc.

Figure 4.30 illustrates the Graphical Representation of the Disc Error Summary using CD-R Inspector.
Another important feature of the tool, CD-R Inspector is that it can be used to search for content on the disc without opening any file or document on the disc. This is somewhat similar to a keyword search but the tool has a sophisticated option to specify only certain sectors which should be searched for the specified keyword. After the search, the tool returns the search result along with the sector information where the content resided. In this research, the tool is been tested to search for the sectors on the CD which has 2108 files and 205 folders for the keyword “Texas A&M University” and the tool successfully returned the accurate result. Figure 4.31 illustrates the Searching for the keyword “Texas A&M University” and Figure 4.32 Search result showing the keyword “Texas A&M University”.

Figure 4.30 Graphical Representation of the Disc Error Summary using CD-R Inspector
This tool has the capability to display the result for “Volume information” of the tool. This feature has been implemented and tested on the CD which was been used for the research and the tool displayed accurate results. Figure 4.33 illustrates the volume Information about the disc.
This tool has a feature to make an analysis of the disc and display the information related to various tracks on the disc and detailed information about each of them. It is capability of giving information even about the number of blocks that were been written on the each track of the disc. This feature was been tested on the CD which was been used in this research and the tool was successful in displaying the accurate information. The tool was successful in giving information about various tracks on the CD and also some information about the CD burning software that was been used to write the contents onto the CD. Figure 4.34 illustrates the analysis of the CD.
4.2.6 Testing the Recovery Tools

Three recovery tools have been studied during this research and their results and testing scenarios are as follows.

PC Inspector File Recovery

PC Inspector File Recovery is a forensic recovery tool which has been studied as a part of this research. The testing scenario and the results are as follows.

Testing Scenario

- Scenario: This tool was been implemented on a USB Flash drive which was been loaded with certain data on it. Some of the contents are been deleted from the storage media to test the recovery feature of the tool. Forensic read-only device has
been used to study the USB Flash drive to avoid any disturbances in the storage media while re-booting it. The details of the deleted content are been noted down before the examination to see if the tool could recover all the content or not.

**Observations**

- The tool successfully displayed all the content that is been lost from the storage media. Figure 4.35 illustrates the display of the lost files by the tool.

![Figure 4.35 Display of the Lost files by the tool](image-url)
The tool successfully displayed and recovered all the content that has been deleted from the storage media. This recovered data is the same as the data that has been deleted from the storage media. The tool also provided an option to save the recovered content onto another storage media and this feature has been successfully tested in this research. The storage of the recovered data on another media helps in preventing the duplication of the data on the same storage media which is been recovered. Figure 4.36 illustrates the display of the deleted content that has been recovered.

![Recovered Files](image)

Figure 4.36 Display of the deleted content that is been recovered

- The tool was successful in saving the recovered files onto another storage media. This is been shown in the screenshot below.

- The tool failed to generate reports about the findings.
Flash Retriever

Flash Retriever is a Forensic recovery tool which has been studied as a part of this research. The testing scenario and the results are as follows.

Testing Scenario

- Scenario: This tool was been implemented on a USB Flash drive which was been loaded with certain data (various kinds of files like .jpeg, .avi, zip, rar, tar, etc.,) on it. Some of the contents are been deleted from the storage media to test the recovery feature of the tool. Forensic read-only device has been used to study the USB Flash drive to avoid any disturbances in the storage media while re-booting it. The details of the deleted content are

Figure 4.37 Saving the recovered files on another storage media
been noted down before the examination to see if the tool could recover all the content or not.

**Observations**

- This tool was successful in recovering not only files such as jpeg, avi, bmp, etc., but also files like zip, rar, tar, etc.,
- This tool provided an option to copy the recovered content onto another disk.
- This tool failed to provide reporting option where it could provide the summary report of the findings.
- This tool has the inbuilt feature to view the recovered content such as jpeg, bmp, etc., Figure 4.38 illustrates the preview and copy of the recovered files by the tool.

![Flash Retriever](image)

Figure 4.38 Step4: Flash retriever Preview and copy of the recovered files
GetDataBack

GetDataBack is a Forensic recovery tool which has been studied as a part of this research. The testing scenario and the results are as follows.

Testing Scenario

- Scenario: This tool was been implemented on a USB Flash drive which was been loaded with certain data (various kinds of files like .jpeg, .avi, zip, rar, tar, etc.,) on it. Some of the contents are been deleted from the storage media to test the recovery feature of the tool. Forensic read-only device has been used to study the USB Flash drive to avoid any disturbances in the storage media while re-booting it. The details of the deleted content are been noted down before the examination to see if the tool could recover all the content or not.

Observations

- The tool successfully recovered all the data that has been deleted from the storage media (USB Flash drive).
- The tool worked pretty well for NTFS and FAT file systems.
- The tool seemed to be very easy to use.

Figure 4.39 and Figure 4.40 illustrates the GetDataBack recovery tree and a sample recovered image using the tool respectively.
Figure 4.39 Step 5: GetDataBack Recovery tree

Figure 4.40 A Sample Recovered image using GetBackData
4.2.7 Testing the Miscellaneous Tools

Two miscellaneous forensic tools have been studied during this research and their results and testing scenarios are as follows.

Belarc Advisor

Belarc Advisor is a forensic tool which has been studied as a part of this research. The testing scenario and the results are as follows.

Testing Scenario

• Scenario: This tool has been installed on a personal computer and the summary of all the hardware, software and operating system components installed on the computer is obtained by running the tool.

Observations

• This tool was successful in determining the following details about the computer system that has been examined.
  • Operating System
  • System Model
  • Processor
  • Main Circuit Board
  • Drives
  • Memory Modules
  • Local drive volumes
• Network Drives
• Users and their last logon information
• Printers installed on the computer
• Controllers
• Display
• Bus Adapters
• Multimedia
• Communications
• Other devices
• Virus Protection
• Missing Microsoft security hotfixes
• Installed Microsoft hotfixes
• Software licenses
• Software versions installed on the computer

This tool is very helpful for forensic investigators in reducing the time they spend to individually study the details of the hardware and software components and prepare a detailed report of the same. Figure 4.41 illustrates the detailed Summary of the computer system that is being examined.
Passware Password Recovery Kit

Passware Password Recovery Kit is a forensic password recovery tool which has been studied as a part of this research. The testing scenario and the results are as follows.

Test Scenario

- Scenario: Passware Password Recovery Kit has been tested on various file types such as MS Excel, MS Outlook, MS Word, MS Access, Winzip, Winrar, Adobe acrobat, etc., that are password protected and the results are been tabulated in this section of the report along with the passwords that are been recovered by the tool. These test results are tabulated in the observations section of this report.
Observations

- Summary of the results obtained when various password protected files are been tested with the tool are as shown in table 4.6.

Table 4.6 various file types tested and the passwords recovered

<table>
<thead>
<tr>
<th>Password Protected File Tested</th>
<th>Password Recovered</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS Excel</td>
<td>amphitheater</td>
</tr>
<tr>
<td>MS Word</td>
<td>anthropology321</td>
</tr>
<tr>
<td>MS Outlook</td>
<td>Dave4password</td>
</tr>
<tr>
<td>MS Powerpoint</td>
<td>Univer5sity</td>
</tr>
<tr>
<td>MS Access</td>
<td>1bombard6</td>
</tr>
<tr>
<td>Winzip</td>
<td>park007</td>
</tr>
<tr>
<td>Winrar</td>
<td>Roster4</td>
</tr>
<tr>
<td>Adobe Acrobat</td>
<td>Graduat567ion</td>
</tr>
<tr>
<td>Word Perfect</td>
<td>Simplicity</td>
</tr>
</tbody>
</table>

The tool successfully recovered the passwords for the file types that were been tested.

- The tool took no time to recover the passwords which are dictionary words.
- The tool took reasonably long time (1hr 12mins) to recover few passwords like “Graduat567ion”.
- The tool implemented various methods to recover the passwords such as Dictionary attack, Brute-force method, Xieve optimization, etc.,
- The tool provided the customization option to filter the searching method which seemed to be useful in certain cases.
Figure 4.42 Screenshot showing the password window when password protected MSExcel sheet has been opened

Figure 4.43 Password Recovery Kit recovered password for MS Excel
4.3 Testing the Anti-Forensic Tools Used in the Research

Two Anti-Forensic tools have been studied during this research and their results and testing scenarios are as follows.

4.3.1 Testing the CyberScrub Privacy Suite

CyberScrub is an Anti-Forensic tool which was been studied during this research and the test scenarios along with the results, observations and screenshots are been listed in this section of the report.

Test Scenario

- Scenario: Two systems are been selected to evaluate the performance of the forensic tool CyberScrub Privacy Suite. Before starting the evaluation phase, the details of all the history files residing on those computers are been categorized and noted down in an excel sheet to prove the reliability of the tool. After the list of the files is been made, the tool was run on the designated system and the observations are tabulated in this section of the report. Figures 4.44 thru 4.51 illustrates various screenshots if Cyberscrub.

Observations

- This tool was successful in automatically removing all evidence related to the online activity and his was successfully performed using the scheduler option in the tools menu.
- This tool was successful in encrypting the data using a feature called “safe”.
• This tool was successful in making the deleted e-mails non-recoverable using the “Deleted E-mail” option.

• This tool successfully deleted the files and folders securely by drag and drop procedure.

• This tool successfully provided an option to secure the entry into the tool using an entry password feature.

• This tool was successful in maintaining a log file of all the operations performed during the particular session.

• This tool was successful in deleting the files and folder beyond the recovery using “Erase beyond recovery” feature so that even sophisticated recovery tools fail to recover the files.

• This tool was successful in removing all the evidence related to the online activity permanently by running the feature called “Privacy Guard”.

![CyberScrub Home Screen](image)

Figure 4.44 CyberScrub Home Screen
Figure 4.45  CyberScrub File Menu

Figure 4.46  CyberScrub Deleted E-mail
Figure 4.47  CyberScrub Erase Menu

Figure 4.48  CyberScrub Erase Beyond Recovery
Figure 4.49 CyberScrub Erase All

Figure 4.50 CyberScrub Privacy Guard
4.3.2 Testing the Clear History

Clear History is an Anti-Forensic tool which was been studied during this research and the test scenarios along with the results, observations and screenshots are been listed in this section of the report.

Test Scenario

- Scenario: Two systems are been selected to evaluate the performance of the forensic tool Clear History. Before starting the evaluation phase, the details of all the history files residing on those computers are been categorized and noted down in an excel sheet to prove the reliability of the tool. After the list of the files is been made, the tool was
run on the designated system and the observations are tabulated in this section of the report.

Figure 4.52 thru 4.56 illustrates various screenshots of Clear History.

**Observations**

- This tool was successful in clearing the search history, location bar history, etc.,
- This tool was successful in clearing the cache, download history and the cookies.
- This tool was successful in erasing even the locked windows file such as index.dat.
- This tool was successful in clearing the history from MS Office applications, Windows applications and Autocomplete forms.
- This tool was successful in clearing history related to IE as well as Mozilla Firefox.
- This tool was successful in erasing the files beyond recovery by various commercial tools.
- This tool was successful in erasing other tracks such as WinZip, WinRar, Windows Media player, Microsoft WordPad and Media player classic.
- This tool was successful in erasing windows tracks such as recent documents, run history, find/search history, clipboard history and open-save dialog history.
Figure 4.52 Clear History Window

Figure 4.53 Clear History Clear Application Tracks
Figure 4.54  Clear History Clear Browser History

Figure 4.55  Clear History Clearing Junk information
### 4.3.3 Comparison of both the Anti-Forensic Tools

The summary of the comparison of both the Anti-Forensic tools is been listed in this section of the report in this section. Table 4.7 illustrates the comparison of both the Anti-Forensic tools.

**Table 4.7 Comparison of Anti-Forensic Tools**

<table>
<thead>
<tr>
<th>Testing Criteria</th>
<th>CyberScrub Privacy Suite</th>
<th>Clear History</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUI Interface</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Is tools able to erase windows tracks</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Is tool able to erase deleted E-mail content</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Is tool able to erase contents beyond recovery</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Feature</td>
<td>CyberScrub</td>
<td>Clear History</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Access control facility to access the tool</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Remove junk data on the windows such as .tmp,.bak,etc.,</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Drag and drop option</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Task scheduler</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>‘Undelete’ or ‘undo’ facility which can be used to undo the previous task</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Maintain a log file with log of operations performed</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Capability to erase the locked windows files such as index.dat</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Erase the contents of slack space of existing files beyond the recovery</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Capability to erase the free(unused) disk space</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Freeware or Commercial</td>
<td>Shareware</td>
<td>Freeware</td>
</tr>
</tbody>
</table>

Thus, the results indicate that though both the tools ‘CyberScrub’ as well as ‘Clear History’ work almost similarly, the tool names CyberScrub is functionally sound when compared to the tool Clear History. There are several freeware tools available in online which can do the basic operations such as erasing the history files on the computer but one excellent feature of CyberScrub is that it has the capability to erase the slack space of the existing file as well as the unused (free) disk space on the hard drive beyond the recovery which is done by very few tools. Thus, it is necessary for the crucial government departments such as Defense Department to use such tools to keep the confidential and sensitive data safe and secure by erasing them beyond the recover on a regular basis.
4.4 Testing DatDetective, A Tool To Read index.dat Files

DatDetective is a tool that was been developed as a part of this research which parses through the index.dat files and displays the contents of the file in the user readable form i.e., it converts the computer readable form of the index.dat file into general English language. This tool has been tested for its features and performance and test scenarios along with the results, observations and screenshots are been listed in this section of the report.

Test Scenario 1: Windows Internet Explorer History index.dat File

The history of all the browsing is stored in the index.dat file located at \Documents and Settings\<Username>\Local Settings\History\History.IE5\index.dat in the subject system. The browsing history is also been monitored during that week. This file is been retrieved and is tested using the tool, DatDetective. In this phase of testing, the tool reported the browsing history in a user readable format.

The system on which the tool is assumed to be tested is prepared for this testing about more than 3 months before the tool is been tested. The system is used to visit several Web pages including the standard URLs before the tool is been tested. During this process “administrator” account is been used to login to the computer to visit the websites. All the websites that are been visited are noted down to test the integrity of the tool. After this phase, a backup of index.dat files is been made and stored at a secure location until it is been tested. Figure 4.57 illustrates the list of the URLs visited and Figure 4.58 illustrates Index.dat file from IE History viewed using DatDetective.
Observations:

After the tool is made ready, it is used to test the index.dat that is saved for examination which was obtained from the source C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\index.dat

- The tool displayed all the URLs that have been visited during the testing phase.
- The tool displayed many attributes for each of the URL visited such as URL Type, Data, Modified time, Accessed time, File name and catch directory.
- Apart from the URL that have been visited during the testing phase, the tool also displayed several other URLs that are related to the primary URLs visited.
- The URL accessed time displayed by the tool, DatDetective during the study of index.dat file is exactly the same as the time noted down during the URL visit.
Test Scenario 2: Cookies Related Index.dat file

The subject system is used to visit several websites which created cookies on the system. As a result of this, the information related to the cookies is stored in the index.dat file located at `\Documents and Settings\<Username>\Cookies\index.dat`. A backup of this file is made and is stored in a secured location until further testing with the tool. In this phase of testing, the tool reported the information related to the cookies in a user readable format. In the subject system the index.dat file was been retrieved from the location `\Documents and Settings\Administrator\Cookies\index.dat`. Figure 4.59 illustrates the Cookies related index.dat file opened with DatDetective.
Figure 4.59 Cookies related index.dat file opened with DatDetective

Observations:

In this phase of testing, the index.dat file is obtained from C:\Documents and Settings\Administrator\Cookies\index.dat and is tested using the tool. The following observations are been made during this phase of testing.

- The tool displayed all the cookies that were been loaded on the system in the cookies folder. The cookies were related to the websites visited during the testing phase.

- All the URLs displayed during the display of cookies related index.dat file are exactly the same as the URLs displayed in the index.dat file found at the IE History folder.

- The time displayed for this index.dat file is the same as the time displayed for the index.dat file stored at IE History folder.
Test Scenario 3: Index.dat files After the Deletion of the Temporary Internet files

The temporary internet files are been deleted in the subject system and the index.dat file located at Documents and Settings\Administrator\Local Settings\History\History.IE5\index.dat is retrieved and tested with the tool. The observations made at this stage are as been listed below.

Observations:

- There was no change in the data resided on the index.dat files and thus this proves that the deletion of the temporary internet files does not make a difference to the data residing on the index.dat files.

Test Scenario 4: Index.dat files After the “Autocomplete” is Turned “OFF” in Windows

The “Autocomplete” option in the “Windows” operating system is handy or at times irritating for the user. As the user begins to type something – Web site or Internet explorer, for instance a credit card number into an online form, Windows XP sends down a little box with the list of all the items that were been typed previously [Rathbone 2006]. The index.dat files in the Windows XP operating system is said to be linked with the Autocomplete option. Hence the index.dat files are been tested after the Autocomplete option is turned off in the subject system. Thus, AutoComplete is turned off and several other websites are been visited and also noted down simultaneously to test the integrity of
the tool. After this process is complete, the index.dat file is been made a backup and it is tested with the tool. The observations are noted down after this phase of testing. All the testing in this phase is done by hand and a test program is used to do achieve this task. A summary of all test results is listed below.

**Observations:**

- Tool was not able to display the URLs visited after the Autocomplete is turned OFF.
5. CURRENT AND FUTURE CHALLENGES

As the technology is taking a big leap towards advancement, new and difficult challenges are been posed to forensic examiners. Though all the changes might not be technical in nature, they must also deal with issues of resourcing, procedure and policy. Some of the technical challenges faced by the forensic examiners are:

5.1 Operating Systems

There has been a rapid advancement in operating system design, implementation and functionality. Previously when the operating system used text based interface like DOS which were simple in style as well as implementation. Performing forensics on such operating system was easier when compared to the present day sophisticated operating systems using a graphical user interface (GUI). When DOS was the predominant operating system for PC’s things were much easier for a forensic specialist as the DOS OS could be installed on a floppy disk and the suspicious system could be booted using the OS residing in the floppy. But, the present day operating systems are very complicated in their design and robustness to perform forensics on them. Evolution of the operating systems which support plug and play devices are also complicated candidates to work on [McKemmish 1999].

5.2 Data Volume

This is one major problem faced by the forensic staff in the present days. The result of the advancement in the current technologies and the demand for larger storage capacity is the emergence of very high storage capacity disks. As the storage capacity of the disks is increasing exponentially, the permanent data stored on those disks is increasing which
presents the forensic examiner with new set of problems. The accurate and proper processing of these large volumes of data provides is the biggest challenge to the forensic examiner [McKemmish 1999]. This is because it takes a lot of effort and time to properly examine these large volumes of data to identify and retrieve the necessary evidence in a form that is legally accepted.

5.3 Digital Evidence

The recent advancements in microelectronics have put forensic examiners in a fit. With these advancements, the size of the microprocessor chips and the storage media have reduced tremendously as they are to be used in small electronic devices such as organizers, cell phones, etc., One such technical advancements could be a “smart card” which not only store large amounts of data but also process and store the data securely on a single chip [McKemmish 1999]. This adds few more complications to forensic examination process.

5.4 Encryption

Improvements in advanced technologies combined with cryptographic techniques to keep the system and data secure have been very useful for the genuine users as well as for the offenders. There have been several cases where offenders use several encryption techniques to carry out their activities so as to stay away from being caught. Advancements in the information age have brought several freely available encryption software to be easily available to everybody through internet which became a major barrier to the forensic examiners [McKemmish 1999].
5.5 Challenges posed by Anti-Forensic tools

Along with the rapid growth of computer forensic tools, Anti-forensic tools also came into existence and are increasing at an alarming rate which might turn as a threat to the computer forensic tools. Some of the upcoming anti-forensic tools which might provide the offenders a chance to escape from the crime are listed below.

5.5.1 TimeStomp

Every file on the computer is maintained with timestamp values such as Created, modified, accessed and entry modified. In most of the cases involving cyber crime, these time stamps play a crucial role which determines the creator of the file, time of creation and the last accessed date and time [Metasploit 2007]. This might prove to be very crucial evidence in the court of law. Thus, to keep the crime covered, there is an Anti-forensic tool called TimeStomp which is coming up so as to modify the time stamps of a file without being detected even by the most promising computer forensic tools. Once this tool pops up then there would definitely be a need to upgrade all the computer forensic tools to detect such timestamp changes for all the computer files.

5.5.2 Slacker

In computer terminology, Slack space is the space between the end of the file and the end of the cluster or sector used by that file [SlackSpace 2007]. One important drawback of most of the forensic tools is their inability to search for the contents residing in the slack space. With the advent of the powerful Anti-forensic tool called slacker, the files could be hidden within the slack space of the NTFS file system [Metasploit 2007].
5.5.3 Transmogrify

Transmogrify is another powerful anti-forensic tool which helps has the ability to change the file extensions. This can mask and unmask the files as any file type [Metasploit1 2007]. This has the ability to beat even the file signaturing capabilities of the most powerful forensic tools such as ENCASE and FTK. If this comes into existence, it would be the tough time for the forensic experts to trace out the evidence files which are been masked from a really huge hard drive as examining every file on the hard disk is a practically impossible task.

Thus, there is a very high necessity for all the commercial tools to regularly monitor the loopholes and bugs in the tool and upgrade themselves so that they would be able to meet the requirements of the present day cyber crime and to face the upcoming powerful forensic tools.
6. CONCLUSION

As the cyber awareness has been increasing at a rapid pace, the rate at which cyber crimes are increasing is rising tremendously. There are several challenges faced by Law enforcement officials in solving the cases and proving the guilt in the court of law. Thus, every law enforcement official should keep updating himself with the upcoming technologies and must have knowledge of all the tools available which might help him in solving the case as use of proper combination of tools always plays a key role in gathering the evidence. There is an immediate need for all the countries worldwide to come up with some standardized cyber laws which helps the law enforcement officials in administering the criminal justice. It is high time for any government to provide enough resources for carrying out research in this area so as to keep themselves updated with the technology and face new challenges that are coming up in Digital Forensics.


APPENDIX A : DatDetective

List of Websites Visited before testing DatDetective
<table>
<thead>
<tr>
<th>No</th>
<th>Name</th>
<th>URL</th>
<th>Modified Date</th>
<th>Accessed Date</th>
<th>Fsize</th>
<th>Cache Info</th>
</tr>
</thead>
</table>

157
APPENDIX B: Araxis Merge Tool

Original Program used to test Araxis Merge Tool

//FCFS

#include<stdio.h>
#include<stdlib.h>

void main()
{

int tot,i;

struct process p[20]
{

int burst;
int artime;
};

printf("Enter the total number of Processes:");
scanf("%d",&tot);

printf("Enter the burst time for the processes:");

for(i=0;i<tot;i++)
{
scanf("%d", &p[i].burst);
}

printf("Enter the Arrival time for the Processes:")

for(i=0;i<tot;i++)
{

}
scanf("%d", &p[i].artime);
}

printf("The Burst times for processes are:\n");
for(i=0;i<tot;i++)
{
 printf("The Burst time for Process p[%d] is %d",i,p[i].burst);
}

printf("The Arrival times for Processes are:\n");
for(i=0;i<tot;i++)
{
 printf("The arrival time for process p[%d] is %d",i,p[i].artime);
}


Modified Program Used to test Araxis Merge tool
/*    FCFS   */
#include<stdio.h>
#include<stdlib.h>

void main()
{

 int total,i;

 struct process p[20]
 {

 int burstime;
 int artime;


printf("Enter the total number of Processes:");
scanf("%d",&total);

printf("Enter the burstime time for the processes:");

for(i=0;i<total;i++)
{
    scanf("%d", &p[i].burstime);
}

printf("Enter the Arrival time for the Processes:");

for(i=0;i<total;i++)
{
    scanf("%d", &p[i].artime);
}

printf("The burstime times for processes are:\n");

for(i=0;i<total;i++)
{
    printf("The burstime time for Process p[%d] is %d",i,p[i].burstime);
    printf("The burst times for the processes are been displayed above");
}
printf("The Arrival times for Processes are:\n");

for(i=0;i<total;i++)
{
    printf("The arrival time for process p[%d] is %d",i,p[i].artime);
    printf("The arrival times for the processes are been displayed above");
}

APPENDIX C: List of Files used for testing Encase and FTK

1. Audio Files:
   A. MIDI Files:
      a) MIDI_alkaseltzer
      b) MIDI_coca_cola
      c) MIDI_itsslinky
      d) MIDI_nokia_tune
   B. MP3_Files
      a) MP_aladdin_goodbye
      b) MP_bugs_mail
      c) MP_cant_takeit
      d) MP_doh
      e) MP_hello_butthead
      f) MP_mail_here
   C. AU Files
      a) AU_bart_laugh
      b) AU_i_want_you
      c) AU_sorry_i_asked
   D. Real Audio Files
      a) RA_daffy_duck_show
      b) RA_hakuna_matata
      c) RA_hula_song
   E. WAV_Files
      a) WAV_aladdin_goodbye
      b) WAV_ahw_man
      c) WAV_bugs_bye
      d) WAV_bugs_mail
      e) WAV_bunny_awful
      f) WAV_bunny_troubles
      g) WAV_cant_takeit
      h) WAV_despicable

2. Video Files
   a) Vid_Clock
   b) Vid_Coffee
   c) Vid_Houston
3. Deleted Files
   
a) Deleted_AU_Sorry_To_Ask
b) Deleted_BMP_Bus_Shelter
c) Deleted_BMP_Staircase
d) Deleted_BMP_Tortoise
e) Deleted_GIF_bearfish
f) Deleted_GIF_bee
g) Deleted_GIF_Elephant
h) Deleted_JPG_ECDC
i) Deleted_JPG_Lamp
j) Deleted_JPG_Swimming Pool
k) Deleted_MIDI_coke
l) Deleted_MP_I_cant_takeit
m) Deleted_RA_Lion_King
n) Deleted_RAR_Folder
o) Deleted_TAR_Folder
p) Deleted_Text
q) Deleted_Vid_Cigarette
r) Deleted_WAV_BugsBye
s) Deleted_Word
t) Deleted_Zip_Folder

4. IMAGE FILES
   
   A. JPEG Files
      
a) JPG_Beach_Road
b) JPG_Bench
c) JPG_Bus_Shelter
d) JPG_Dolphins
e) JPG_ECDC
f) JPG_Fishes
g) JPG_Lamp
h) JPG_Staircase
i) JPG_Swimming_Pool
j) JPG_Tortoise

   B. BMP Files
      
a) BMP_Beach_Road
b) BMP_Bench
c) BMP_Bus_Shelter
d) BMP_Dolphins
e) BMP_ECDC
f) BMP_Fishes
g) BMP_Lamp
h) BMP_Staircase
i) BMP_Swimming_Pool
j) BMP_Tortoise
C. GIF Files
   a) GIF_bear
   b) GIF_bearfish
   c) GIF_bee
   d) GIF_Cat
   e) GIF_cheetah
   f) GIF_dinosaur
   g) GIF_Elephant
   h) GIF_horse
   i) GIF_HorseRun
   j) GIF_spider

5. Misnames Files
   a) BMP_Lamp (BMP-> MIDI)
   b) GIF_dinosaur ( GIF ->TXT)
   c) JPG_ECDC (JPG->WAV)
   d) MIDI_nokia_tune (MIDI->JPG)
   e) MP_aladdin_goodbye (MP->GIF)
   f) RAR Files (RAR->.PST)
   g) TAR Files (TAR->.AVI)
   h) Text1 (Txt ->MP3)
   i) Vid_Clock (Vid->TXT)
   j) WAV_awh_man (WAV->BMP)
   k) Word1 (DOC->JPG)
   l) ZIP Files (ZIP->TAR)

6. TAR Files
   a) TAR_AU_sorry_i_asked
   b) TAR_BMP_Fishes
   c) TAR_GIF_bearfish
   d) TAR_JPG_ECDC
   e) TAR_MIDI_coca_cola
   f) TAR_MP_hello_butthead
   g) TAR_RA_hakuna_matata
   h) TAR_Text
   i) TAR_WAV_awh_man
   j) TAR_Word

7. ZIP Files
   k) ZIP_AU_sorry_i_asked
   l) ZIP_BMP_Fishes
   m) ZIP_GIF_bearfish
   n) ZIP_JPG_ECDC
   o) ZIP_MIDI_coca_cola
   p) ZIP_MP_hello_butthead
7. RAR Files
   a) RAR_AU_sorry_i_asked
   b) RAR_BMP_Fishes
   c) RAR_GIF_bearfish
   d) RAR_JPG_ECDC
   e) RAR_MIDI_coca_cola
   f) RAR_MP_hello_butthead
   g) RAR_RA_hakuna_matata
   h) RAR_Text
   i) RAR_WAV_ahh_man
   j) RAR_Word

8. Text Files
   a) Bad Stuff
   b) Good Stuff
   c) Introduction_text
   d) Text1
   e) Text2
   f) Text3
   g) Text4
   h) Text5
   i) Text6
   j) Welcome_text

9. Word Documents Files
   a) Bad Stuff
   b) Good Stuff
   c) Introduction
   d) Welcome
   e) Word1
   f) Word2
   g) Word3
   h) Word4
   i) Word5
   j) Word6