Computer Forensics: Issues and Challenges

Dr. Mrs Ashwini Atul Renavikar, Mrs. Anjali Bapat (Deshpande),

[1*]Associated With Symbiosis Skills Professional University And Qa Professional At Shrisoft Pvt. Ltd. Pune Contact Det. : 9890247127 E-Mail: Ashwiinirenavikar@Gmail.Com
[2]quality Management & Benchmarking (Qmb), Symbiosis International (Deemed University), Pune. Contact Det.: 9834748201 Email: Hianjud18@Gmail.Com

[*]**Corresponding author:** Dr. Mrs Ashwini Atul Renavikar
*Associated With Symbiosis Skills Professional University And Qa Professional At Shrisoft Pvt. Ltd. Pune Contact Det. : 9890247127

Introduction

Computer forensics is an application of the scientific method to digital media in order to establish factual information for judicial review. This process often involves investigating computer systems to determine whether they are or have been used for illegal or unauthorized activities.

Who are interested

Criminal prosecutors utilize computer evidence in various crimes, such as homicides, financial fraud, drug-related activities, embezzlement, and child pornography. In civil litigations, personal and business records found on computer systems can be crucial in cases involving fraud, divorce, discrimination, and harassment. Insurance companies can potentially reduce costs by using computer evidence to detect fraud in accident, arson, and workers' compensation cases. Corporations often employ computer forensics specialists to investigate evidence related to sexual harassment, embezzlement, theft, or misappropriation of trade secrets and other internal or confidential information. Law enforcement officials frequently seek assistance with pre-search warrant preparations and post-seizure handling of computer equipment. Additionally, individuals may hire computer forensics specialists to support claims of wrongful termination, sexual harassment, or age discrimination.

How to investigate

It is a detailed science, but broadly speaking, the main phases are often considered to be:

1. Securing the subject system to prevent tampering during the operation.
2. Making a copy of the hard drive, if applicable.
3. Identifying and recovering all files, including those that have been deleted.
4. Accessing and copying hidden, protected, and temporary files.
5. Examining 'special' areas on the drive, such as residue from previously deleted files.
6. Investigating data and settings from installed applications and programs.
7. Assessing the system as a whole, including its structure.
8. Considering general factors related to user activity.
9. Creating a detailed report.

Throughout the investigation, it is crucial to maintain a full audit log of all activities.

Where to search for evidence

Undeleted files, expect some names to be incorrect

–Deleted files

–Windows registry

–Print spool files

–Hibernation files

–Temp files (all those .TMP files!)

–Slack space

–Swap files

–Browser caches

–Alternate partitions

–On a variety of removable media (floppies, ZIP, Jazz, tapes, …) Look for the traces in Event logs

–Are they enabled?

–Review and take copy if possible

–IIS/FTP logs

Five Major Steps in the process of forensic investigation

● Acquire:

- Take pictures and note down observations before disconnecting any wires.
- Unplug the system from the network.
- If possible, freeze the system from the network to save or document current memory, swap files, and CPU registers.

● Collection:

- Ensure the evidence is collected in a manner that maintains its integrity to support the case.
- Methodically identify and label every single item from the suspect's or victim's location.

● Preserve:

- Transportation: - Handle the evidence with extreme care to avoid any alterations.
- Storage: - Keep the evidence in a cool, dry, and appropriate place for electronic evidence.

● Analyze:

- Document the investigation thoroughly, which can be challenging for technical professionals who may not be accustomed to detailed writing.

● Present:

- Use the collected and analyzed evidence in the case.
-

Some Examples

Here are some examples where computer forensics concepts were applied to solve mysteries:

1. **Chandra Levy Case:**

Chandra Levy, a Washington intern, disappeared on April 30, 2001, causing significant concern within the community. Although her whereabouts were initially unknown, she had used the internet and email to arrange travel plans and communicate with her parents. Computer forensics experts traced her online activities, leading the police to her location even after she had been missing for a year.

2. **Child Pornography Cases in Private Schools**:

In several recent cases, authority figures at private schools have been charged with possession of child pornography. These discoveries were made possible through computer forensics. By tracking the buying and selling of pornography online, investigators located individuals involved in these crimes. The evidence gathered from computers served as hard evidence in court, facilitating prosecutions. This has helped remove child pornographers from the education system.

3. **Workplace Security:**

In the workplace, computer forensics play a crucial role in maintaining security. Employee computers are monitored to ensure no illegal activities occur, and heightened security measures protect company confidential files from outsiders. If security is breached, computer forensics can trace the tampered computer and identify the extracted information, potentially leading to the guilty parties and others involved.

Actual Computer Forensics Cases

Mr. XYZ (Name hidden) is one of the world's most renowned computer forensic specialists. During his tenure as a Special Agent with the Florida Department of Law Enforcement (FDLE), Mr. XYZ (Name hidden) conducted numerous computer forensic examinations, leading to successful criminal prosecutions. His work included uncovering evidence that perpetrators thought they had destroyed and decrypting secured data. Notably, in one case, his examination cleared a defendant of all charges. Since retiring from FDLE, Mr. XYZ (Name hidden) has performed numerous examinations in civil litigation and employment matters. Here are some notable cases:

1. **Corporate Concealment:**

The Board of Directors of a corporation suspected that the president was concealing critical terms of an agreement with another corporation. After Mr. XYZ (Name hidden)'s analysis confirmed their suspicions, the president resigned.

2. **Email Interception:**

A corporation's IT director was suspected of intercepting emails from the CEO and other key employees. Mr. XYZ (Name hidden)'s examination provided proof of these activities, leading to the IT director's resignation.

3. **Client Overbilling:**

An employee quit unexpectedly, raising suspicions that she was overbilling clients and pocketing the profits. An analysis of the company's Macintosh billing system revealed that the employee had deleted hundreds of client records to cover her tracks. Mr. XYZ (Name hidden) successfully recovered all the deleted records.

4. **Personal Use of Company Resources:**

In analyzing a company's computer, Mr. XYZ (Name hidden) discovered that an employee had been using it for personal research on expensive databases.

5. **Competing Business Plan:**

In examining a computer used by a fired employee, Mr. XYZ (Name hidden) found a detailed business plan for a competing business. This plan included information about other employees who would join the new company.

6. **Confidentiality Violation:**

A key employee left a large corporation to start a competing business and formatted his company laptop's hard drive to destroy evidence of violating a confidentiality agreement. Mr. XYZ (Name hidden) recovered emails, letters, memorandums, and business plans from the laptop.

7. **Child Pornography Prosecution:**

Mr. XYZ (Name hidden) was asked by a State Attorney's Office in Florida to review evidence in a child pornography case. His examination of an old IBM PS1 model revealed a dozen child pornography files on the hard drive. However, Mr. XYZ (Name hidden)'s expertise led him to conclude that the defendant was being framed, resulting in dropped charges.

8. **Encrypted Child Pornography:**

In another child pornography case, the defendant admitted to downloading "a few" images months earlier but claimed to have destroyed them. Mr. XYZ (Name hidden)'s examination uncovered a large cache of encrypted files. He successfully broke the password and recovered dozens of child pornographic images, leading the defendant to plead guilty.

9. **Backup Tape Evidence:**

Another defendant denied downloading any child pornography and claimed that deleted files were not pornographic. Mr. XYZ (Name hidden) found numerous backup tapes during the examination. His analysis revealed numerous child pornographic files, further implicating the defendant.

These cases illustrate Mr. XYZ (Name hidden)'s expertise in computer forensics and his significant impact on both criminal and civil investigations.

Forensic Investigation Includes:

- Protection:

- Safeguards the subject computer system during the forensic examination to prevent any alteration, damage, data corruption, or virus introduction.

- Discovery:

- Identifies all files on the subject system, including existing files, deleted but recoverable files, hidden files, password-protected files, and encrypted files.

- Recovery:

- Recovers as many deleted files as possible.

- Revelation:

- Reveals the contents of hidden files and temporary or swap files used by both application programs and the operating system, to the extent possible.

- Access:

- Accesses the contents of protected or encrypted files, if legally permissible.

● Analysis:

- Analyzes all potentially relevant data in special and typically inaccessible areas of a disk, including:
- Unallocated Space: - Currently unused space that may contain remnants of previous data relevant to the investigation.
- Slack Space: - The remnant area at the end of a file in the last assigned disk cluster, which might contain previously created and relevant evidence.

● Documentation:

- Produces an overall analysis of the subject computer system, listing all potentially relevant files and discovered data. This includes providing opinions on the system layout, file structures, discovered data and authorship information, and any attempts to hide, delete, protect, or encrypt information.

● Expert Consultation:

- Provides expert consultation and/or testimony as required.

Skills required
Computer forensics is not a task to be undertaken lightly by just any IT worker. Instead, it requires specialized skills and meticulous, documented procedures. A forensics expert knows what signs to look for and can identify additional sources of relevant evidence, including earlier files and even data from reformatted disks, which can often be fully recovered. Moreover, computer data can be precisely replicated for analysis and processing without damaging the original data.

Any type of data can serve as evidence, including text documents, graphical images, calendar files, databases, spreadsheets, audio and video files, websites, and application programs. Even viruses, Trojan horses, and spyware can be secured and investigated. Email records and instant messaging logs are valuable sources of evidence in litigation because people tend to be more casual in their electronic communications than in hard-copy correspondence such as written memos and letters.

Digital data can be searched quickly and easily by machines, whereas paper documents must be examined manually. However, like other information used in a case, the results of a computer forensics investigation must adhere to accepted standards of evidence as codified in state and federal law. This requires investigators to take special care to protect evidence and preserve its original state, ensuring that suspect files are not altered or damaged through improper handling.

Computer forensics is a component of the broader concept of electronic discovery, which involves seeking, locating, securing, and searching data from a specific computer or network with the intent of using it as evidence in a civil or criminal legal case. Court-ordered or government-sanctioned hacking to obtain evidence can also be considered a form of electronic discovery. In general, electronic discovery refers to the overall process, while computer forensics is concerned with specific procedures and technical details.

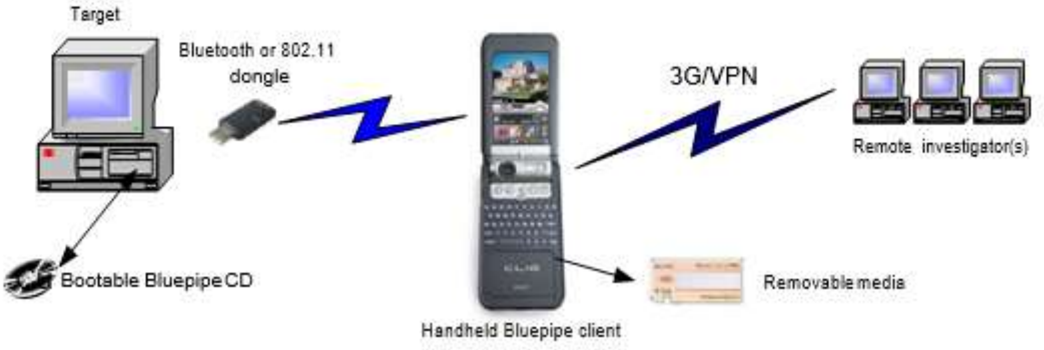
How Windows remembers links
Operating systems such as Windows keep track of various devices—disk-on-keys, printers, cameras, headphones, mobile phones, and more—that users connect to them. These devices can connect via physical or wireless ports using a variety of protocols, including wired protocols like USB and Firewire, and wireless protocols like IrDA, Wi-Fi, and Bluetooth.

The information Windows stores about these devices varies depending on the device and protocol, but users can typically access information about devices previously connected to a computer. For instance, you can find out that a user connected an encrypted disk-on-key to "Joe's" computer, with details such as the manufacturer (Kingston) and the key size (128 MB). Metadata describing this information can be retrieved even years after the device was connected.

This data is invaluable to security professionals who use it to understand how computers are used within organizations.

For example, a Chief Security Officer (CSO) conducting a risk assessment or investigating an incident would find such information useful. However, unauthorized individuals could also exploit this information to learn about an organization's device usage, potentially breaching the company's privacy.

Modern hardware devices contain information that helps the operating system find appropriate drivers to handle the device. This is true for all modern ports—USB, Firewire (IEEE 1394), Bluetooth, PCI, and PCMCIA.
Inputs required:



1. **Computer Time and Date Settings**

The accuracy of the time and date stamps on files is crucial in cases involving computer evidence. This accuracy is directly linked to the time and date stored in the CMOS chip of the computer. Thus, documenting the accuracy of these settings on the seized computer is essential. Without this information, validating the times and dates associated with relevant files is almost impossible. It is recommended to compare the current time and date with those stored in the computer, which can be obtained from reliable sources like the telephone company or online services such as [Greenwich Mean Time](http://wwp.greenwichmeantime.com/). Before checking the time and date, creating a bitstream backup of the computer hard drive is crucial. Free software is available online to help document system time and date settings.

2. **Hard Disk Partitions**

The potential for hidden or missing data exists with computer hard disk drives. Therefore, documenting the make, model, and size of all hard disk drives in the seized computers is vital. This involves a physical examination of the hard disk drive and documenting the factory information recorded on the outside. Tools like DOS FDISK or PartInfo should be used to document the number and size of partitions, ensuring hidden partitions and data are found and documented. PartInfo is available with Partition Magic Software, which can be purchased at most computer stores.

3. **Operating System and Version**

A seized computer may use one or more operating systems, which should be documented. For DOS and Windows-based systems, this can be determined by examining the boot sector of each partition or using programs like Norton Utilities. The findings should be noted, and the software and version used should be documented and retained.

4. **Data and Operating System Integrity**

The integrity of the operating system, directory, FAT, and data storage areas directly affects the accuracy of any data found. Running programs like DOS ScanDisk and DOS ChkDisk can document this integrity. Any errors found should be documented, and corrective actions taken should be recorded. The version of the software used should also be retained and stored with the documentation.

5. **Computer Virus Evaluation**

To prevent introducing viruses into seized computer storage devices, all processing software should be scanned by NIST-certified virus scanning utilities like McAfee, Norton, or Dr. Solomon. Ideally, two separate virus scanning utilities should be used, and the results documented. The seized computer hard drives and floppy disks should also be scanned, and any viruses found should be documented and, if necessary, removed. The software versions used should be retained and stored with the documentation. Note that some virus scanning programs automatically search inside compressed files, while others do not, which should be considered during documentation creation.

6. **File Catalog**

Files stored on the computer hard drives and floppy disks should be listed and cataloged, including their creation and update dates and times. Sorting files by date and time can provide valuable leads and help document conspiracies when evaluated across multiple computers seized in the same case. NTI's FileList Pro program is ideal for this purpose, supporting various Windows systems and documenting long file names and deleted files. The output can be sorted by creation date, last modified date, and last accessed date, aiding in documenting computer hard disk drive content and usage patterns.

7. Software Licensing

Law enforcement agencies often face funding challenges, leading to the use of unlicensed software in processing computer-related evidence. This can jeopardize a case if discovered by the defense. It is crucial to use licensed software, document this fact, and register the software after purchase. Some software companies offer free or discounted forensic software to law enforcement agencies. Ensuring proper licensing avoids credibility and legal issues.

8. Retention of Software, Input Files, and Output Files

Software is frequently updated, making it important to retain the exact version and copy of the software used in processing computer evidence. This ensures the ability to duplicate results if needed, preventing doubts about the accuracy of the processing and addressing defense claims of evidence tampering. It is recommended to archive the source files, text search files, output files, and forensic software on the same storage device until after trial or until all appeal possibilities are exhausted. Jazz Disks (by Iomega) or similar external storage devices are suitable for this purpose. Documentation should list the software used, names of source files, output files, and software versions, matching the contents of the archive disk.

Steganography

Steganography is the art of concealed or hidden writing, aiming at covert communication to conceal a message from third parties. Unlike cryptography, which focuses on making a message unreadable to third parties without hiding the communication's existence, steganography conceals the actual message itself. While steganography and cryptography are distinct, they share analogies, leading some to classify steganography as a form of cryptography due to its hidden communication aspect.

One famous example of steganography is found in Da Vinci's Mona Lisa painting, showcasing hidden messages within the artwork. Techniques like these were prevalent in ancient times, particularly during the peak of steganography around 1400 BC, coinciding with high civilization levels in places like Egypt, India, and China.

Although the term "steganography" was coined in the late 15th century, its use dates back millennia. Historical methods include hiding messages on wax writing tablets' backs, inscribing them on animals like rabbits, or even tattooing them on slaves' scalps. Invisible ink, used for both amusement and espionage, has been a longstanding steganographic tool. Microdots and microfilm, popular in war and espionage narratives, emerged after photography's invention.

Steganography conceals the hidden message while revealing that communication is occurring between two parties. The process typically involves embedding a secret message within a carrier, forming the steganography medium. Encryption of the hidden message and randomization in the steganography scheme may employ a steganography key.In summary:
steganography_medium = hidden_message + carrier + steganography_key

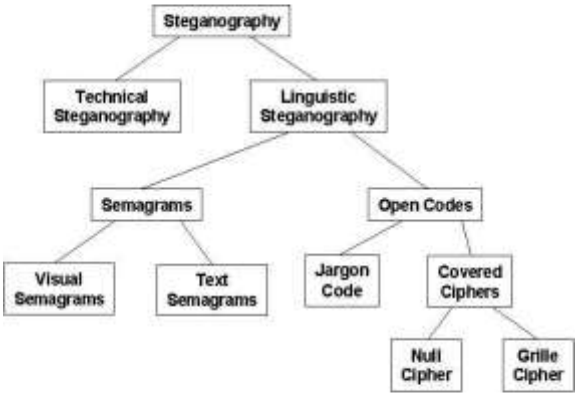


Figure above shows a common taxonomy of steganographic techniques

Technical steganography employs scientific methods to conceal a message, including techniques like invisible ink, microdots, and size-reduction methods.

Linguistic steganography hides messages in carriers in non-obvious ways, categorized as semagrams or open codes.

- Semagrams use symbols or signs to hide information. Visual semagrams use everyday objects or innocuous symbols, like doodles or item positioning, to convey a message. Text semagrams modify carrier text appearance subtly, like font changes, spacing, or letter flourishes.
- Open codes hide messages within legitimate carrier messages, not obvious to unsuspecting observers. The overt communication is the carrier, while the covert communication is the hidden message. This category includes jargon codes and covered ciphers.
- Jargon codes use language understood by a group but meaningless to others, like warchalking symbols or specialized terminology.
- Cue codes, a subset of jargon codes, use prearranged phrases with special meanings.
- Covered or concealment ciphers openly hide messages in carriers, recoverable by those who know the concealment method. A grille cipher uses a template to cover the carrier, revealing the hidden message through template openings. A null cipher hides messages according to specific rules, such as reading every fifth word or focusing on specific characters within words.

In the digital age, steganography has found its place in storing and transmitting data on computers and networks. Steganography applications allow hiding any binary file within another binary file, with image and audio files being the most common carriers.

One crucial application of steganography in the digital world is digital watermarking. Here, authors can embed hidden messages in files to assert ownership of intellectual property or ensure content integrity. For instance, an artist can embed a watermark in their original artwork posted online. If someone claims ownership of the work, the artist can prove ownership by recovering the watermark. Digital watermarking, while conceptually similar to steganography, typically serves different technical goals. It involves inserting a small amount of repetitive information into the carrier, doesn't require hiding the watermarking information, and allows for the watermark to be removed while maintaining carrier integrity.

However, steganography also has nefarious applications, including hiding records of illegal activities, financial fraud, industrial espionage, and facilitating communication among criminal or terrorist organizations.

Forensic tools available

Hardware tools: IMAGE MASTER Hand held disk imager.

Software tools: Encase Computer forensic software from Guidance Software' Ontrack Data recovery software SuprSCAB Forensic software. Logic Cube Hardware disk duplication. Mailbag assistant E-mail organizer.

Digital Guards Intrusion detection tools

Summary

With the world becoming more and more IT savvy it is needless to say that there will be more and more crimes with the help of computers. It is not possible to stop those. Instead, the computer forensics arena can be broadened to encompass wider area of crimes, to prevent the crimes and if there are nay, investigate them in a more scientific and methodic way. People with a strong IT background and with good investigating skills can take up computer forensics as a career.

References and bibliography Research papers and articles

'How Windows remembers your connections' by Zvi Gutterman and Avner Rosenan (Zvi is founder and CTO of Safend. Avner is a Team Leader in the R&D group.)

'Reproducibility of Digital Evidence in Forensic Investigations' by Lei Pan and Lynn M. Batten, School of IT, Deakin

University,Melbourne, Australia(August 19, 2005)

Books

Digital Evidence and Computer Crime (E. Casey, Academic Press) Computer Forensics and Privacy (M. Caloyannides, Artech House) Handbook of Computer Crime Investigation: Forensic Toolsand Technology by Eoghan Casey.

URLs

1. http://www.dfrws.org
2. http://www.ijde.org/ (International Journal of Digital Evidence) http://vip.poly.edu/kulesh/forensics/list.htm http://www.tucofs.com/tucofs/tucofs.asp