Digital Forensics

Tim Schulze

Inhaltsverzeichnis

1 Computer Crime Scene Investigation

1.1 Introduction to Digital Forensics

Computer forensics, also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination, is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence. A thorough analysis by a skilled examiner can result in the reconstruction of the activities of a computer user.
In other words, Computer forensics is the collection, preservation, analysis, and presentation of computer-related evidence.
Computer evidence can be useful in criminal cases, civil disputes, and human resources/employment proceedings. The process of acquiring, examining, and applying digital evidence is crucialto the success of prosecuting a cyber criminal.

- White Color Crimes (health care fraud, government fraud including erroneous IRS and Social Security benefit payments, and financial institution fraud)
- Violent Crimee (child pornography, interstate theft)
- Organized Crime (drug dealing, criminal enterprise)

The objective in computer forensics is to recover, analyze, and present computer-based material in such a way that it is **useable as evidence in a court of law**.
Priority: Accuracy > Speed, but efficiently as possible (adhere to stringent guidelines)

1.2 Roles of Computer in a Crime

A computer can be:

- the target of the crime (audit logs and unfamiliar programs should be checked)
- it can be the instrument of the crime (look for password cracking software and password files)
- it can serve as an evidence repository storing valuable information about the crime

1.3 Computer Forensics Specialist(Procedure sequence)

1. Protect the subject computer system during the forensic examination from any possible alteration, damage, data corruption, or virus introduction

2. Discover all files on the subject system. This includes existing normal files, deleted yet remaining files, hidden files, password-protected files, and encrypted files
3. Recover all (or as much as possible) of discovered deleted files
4. Reveal (to the extent possible) the contents of hidden files as well as temporary or swap files used by both the application programs and the operating system
5. Accesses (if possible and if legally appropriate) the contents of protected or encrypted files
6. Analyze all possibly relevant data found in special areas of a disk
7. Print out an overall analysis of the subject computer system, as well as a listing of all possibly relevant files and discovered file data. Further, provide an opinion of the system layout; the file structures discovered; any discovered data and authorship information; any attempts to hide, delete, protect, or encrypt information; and anything else that has been discovered and appears to be relevant to the overall computer system examination.
8. Provide expert consultation and/or testimony

1.4 Use of Computer Forensic Evidence

- Criminal Prosecutors(Strafrechtliche Staatsanwälte): homicides, financial fraud, drug and embezzlement record-keeping, and child pornography
- Civil litigations(Zivilrechtliche Streitigkeiten): personal and business records on divorce, discrimination, and harassment cases (Insurance companies)
- Corporations: sexual harassment, embezzlement, theft or misappropriation of trade secrets, and other internal/confidential information
- Law enforcement officials: require assistance in pre-search warrant preparations and post-seizure handling of the computer equipment
- Individuals: hire computer forensics specialists in support of possible claims of wrongful termination, sexual harassment, or age discrimination (electronic mail systems, on network servers, and on individual employee's computers)

1.5 Use of Computer Forensics in Law Enforcement

If there is a computer on the premises of a crime scene, the chances are very good that there is valuable evidence on that computer. If the computer and its contents are examined (even if very briefly) by anyone other than a trained and experienced computer forensics specialist, the usefulness and credibility of that evidence will be tainted.
Make sure you find someone who not only has the expertise and experience, but also the ability to stand up to the scrutiny and pressure of cross-examination.

1.5.1 Employer Safeguard Program

An unfortunate concern today is the possibility that data could be damaged, destroyed, or misappropriated by a discontented individual Before an individual is informed of their termination, a computer forensic specialist should come on-site and create an exact duplicate of the data on the individual's computer. In this way, should the employee choose to do anything to that data before leaving, the employer is protected.

- What Web sites have been visited
- What files have been downloaded
- When files were last accessed
- Of attempts to conceal or destroy evidence
- Of attempts to fabricate evidence
- That the electronic copy of a document can contain text that was removed from the final printed version
- That some fax machines can contain exact duplicates of the last several hundred pages received
- That faxes sent or received via computer may remain on the computer indefinitely
- That email is rapidly becoming the communications medium of choice for businesses
- That people tend to write things in email that they would never consider writing in a memorandum or letter
- That email has been used successfully in criminal cases as well as in civil litigation
- That email is often backed up on tapes that are generally kept for months or years
- That many people keep their financial records, including investments, on computers

1.6 Computer Forensic Services

- Data seizure(Beschlagnahme)
- Data duplication and preservation(Vervielfältigung und Aufbewahrung)
- Data recovery
- Document searches
- Media conversion

- Expert witness services

PROVIDE EXPERT CONSULTATION AND EXPERT WITNESS SERVICES

COMPUTERS

Expert Testimony

- Has testified multiple times as an expert witness in computers and computer forensics in circuit court
- Regularly testify as an expert witness in computers and computer forensics in federal court for U.S. attorney's offices

Computer Expertise

- Belongs to the Computer Crime Investigators Association
- Trained in the forensic examination of computers (PC & Mac), having conducted examinations in countless cases including child exploitation, homicide, militia, software piracy, and fraud
- Has testified in state and federal courts as an expert in computers, computer forensics, the Internet, and America Online; often as an expert witness for U.S. attorney's offices
- Is thoroughly familiar with both computer hardware and software, having written software and repaired and assembled computers
- Teaches computer crime investigation, including computer search and seizure, for the Institute of Police Technology and Management
- Regularly consults with law enforcement officers in the search and seizure of computers
- Has provided forensic training to numerous law enforcement officers and corporate security officers
- Regularly consulted by other forensic examiners for advice in difficult cases

Training Given as Expert in Computer Crimes

- Law Enforcement and Corrections Technology Symposium and Exhibition
- Bureau of Justice Statistics/Justice Research Statistics Association

Electronic Surveillance

- Theft by employees or others
  - Time
  - Property
  - Propriety information and trade secrets
- Embezzlement
- Inappropriate employee actions
- Burglary

Your computer forensics expert's experience should include installing cameras in every imaginable location (indoors and outdoors, offices, homes, warehouses, stores, schools, or vehicles) for every conceivable crime (theft, burglaries, homicides, gambling, narcotics, prostitution, extortion, or embezzlement) under every conceivable circumstance (controlled settings, hostage crisis, or court-ordered covert intrusion).

If you need to know what your employees are doing on your time and on your premises, your computer forensics experts should be able to covertly install video monitoring equipment so that you can protect your interests. This even includes situations where employees may be misusing company computers. By using video surveillance to document employees who are stealing time, property, or secrets from you, you should protect yourself if you plan to take appropriate action against the employees.

Child Exploitation

- Child sexual exploitation
- Child pornography
  - Manufacture
  - Use
  - Sale
  - Trading
  - Collection
  - Child erotica
- Use of computers in child exploitation
- Search and seizure
- Victim acquisition
- Behavior of preferential and situational offenders
- Investigation
  - Proactive
  - Reactive [4]

- Computer evidence service options
  - Standard service
  - On-site service
  - Emergency service
  - Priority service
  - Weekend service
- Other miscellaneous services
  - Analysis of computers and data in criminal investigations
  - On-site seizure of computer data in criminal investigations
  - Analysis of computers and data in civil litigation.
  - On-site seizure of computer data in civil litigation
  - Analysis of company computers to determine employee activity
  - Assistance in preparing electronic discovery requests
  - Reporting in a comprehensive and readily understandable manner
  - Court-recognized computer expert witness testimony
  - Computer forensics on both PC and Mac platforms
  - Fast turnaround time

1.7 Problems with Computer Forensic Evidence

Computer evidence is like any other evidence. It must be:

- Authentic
- Accurate
- Complete
- Convincing to juries
- In conformity with common law and legislative rules (i.e., admissible)

There are also special problems:

- Computer data changes moment by moment.
- Computer data is invisible to the human eye; it can only be viewed indirectly after appropriate procedures.
- The process of collecting computer data may change it—in significant ways. The processes of opening a file or printing it out are not always neutral.

- Computer and telecommunications technologies are always changing so that forensic processes can seldom be fixed for very long [5].

1.8 The Forensic Technican

standard disk repair, network testing

- The scene of crime has to be frozen; that is, the evidence has to be collected as early as possible and without any contamination.
- There must be continuity of evidence, sometimes known as chain of custody; that is, it must be possible to account for all that has happened to the exhibit between its original collection and its appearance in court, preferably unaltered.
- All procedures used in examination should be auditable; that is, a suitably qualified independent expert appointed by the other side in a case should be able to track all the investigations carried out by the prosecution's experts [5].

Key features

- Careful methodology of approach, including record keeping
- A sound knowledge of computing, particularly in any specialist areas claimed
- A sound knowledge of the law of evidence
- A sound knowledge of legal procedures
- Access to and skill in the use of appropriate utilities [5]

1.9 Subject Matter of Computer Forensics

- Authenticity: Does the material come from where it purports?
- Reliability: Can the substance of the story the material tells be believed and is it consistent? In the case of computer-derived material, are there reasons for doubting the correct working of the computer?
- Completeness: Is the story that the material purports to tell complete? Are there other stories that the material also tells that might have a bearing on the legal dispute or hearing
- Freedom from interference and contamination: Are these levels acceptable as a result of forensic investigation and other post-event handling?