The Guide to Digital Forensics

COURTESY OF ERMProtect Cybersecurity Solutions

What is Digital Forensics?

Digital forensics, sometimes referred to as "computer forensics," is the process of identification, preservation, examination, documentation, and presentation of digital evidence found on a computer, phone, or digital storage media. Essentially, digital artifacts can be collected from all devices that store data such as phones, laptops, hard disks, pen drives, etc.

Digital forensics involves analyzing these digital artifacts in order to find out what happened, how and when it happened, and who was involved in an alleged crime or malfeasance. The results of a digital forensic investigation can then be used as evidence in a court of law.

Types of Digital Forensics

Network Forensics:

Network forensics relates to monitoring a computer network and analyzing the traffic to gather information, evidence, or source of cyberattacks. Network forensics in the context of cyberattacks deals with analyzing the nature of attacks by focusing on attacker activity.

Database Forensics:

Database forensics relates to the forensic analysis of databases and the data they store. Often computer forensic investigators analyze databases to see who accessed the database and what actions were performed over a specific period of time to identify suspicious activities or transactions. They can potentially recover deleted information.

Wireless Forensics:

Wi-Fi networks are lucrative entry points for hackers. Wireless forensics deals with capturing data moving over wireless networks via wireless routers, wireless access points, Wi-Fi switches and other Wi-Fi transmissions. Computer forensic experts often analyze wireless networks to identify rogue or unauthorized devices, malware, intrusions, or infected devices.

Disk Forensics:

Disk forensics involves extracting data from storage media such as hard drives, USB drives, Flash drives, and so on. Computer forensic experts use their knowledge and experience - supplemented with tools, technology, and examination techniques - to recover data from devices even in situations where the devices are physically or logically damaged.

Email Forensics:

Email forensics deals with recovering and analyzing the source and content of emails including deleted emails, calendar entries, contacts, and such. Computer forensic investigators typically analyze email headers, server logs, email sources, attachments in emails, and so on to investigate email-related crimes.

Mobile Forensics:

Mobile forensics deals with the examination and analysis of mobile devices to retrieve stored data such as contacts, logs, SMS, audio and video files, email, web browsing information, location information, social networking messages etc. Mobile forensics has become increasingly important in recent times due to the fact that devices have grown into sophisticated, pocket-sized computers with ever-increasing functionalities and data storage capacities.

Desktop Forensics:

Desktop forensics involves the collection, preservation, analysis, and presentation of evidence found on computers and related storage devices. Forensic computer investigators look deeply into the contents of storage devices, hard drives, emails, documents and other files. They also dig into metadata and also extract data that is hidden or deleted.

Cloud Forensics:

Cloud forensics involves applying the principles and methods of forensic investigation in a cloud environment. This often turns out to be quite complicated because data could be distributed across several cloud servers which, in turn, could be located in various physical locations and even different countries. While performing digital forensic investigations on such a scattered dataset can be challenging, experienced computer forensic investigators have means to tackle these assignments.

Digital Forensics in Investigations

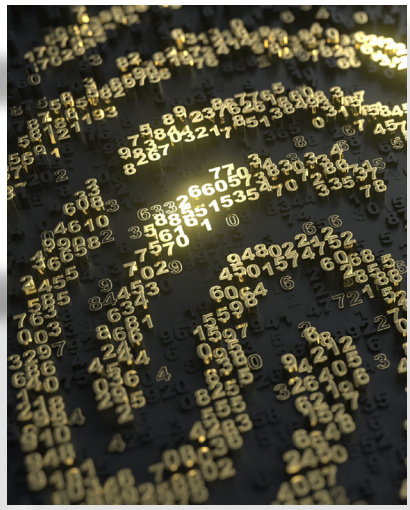
There are broadly two types of investigations where digital forensic expertise is called upon. In both types, investigators must acquire, analyze and preserve information in a manner that will stand up in court:

Public Investigations:

1. Involve criminal or civil cases that will be litigated in court
2. Lawyers rely on digital evidence to support or refute allegations
3. Forensics typically involve investigating activity on computers or devices

Private Investigations:

1. Often involve investigations of alleged misconduct at corporations
2. May also include investigations of data breaches / cyberattacks
3. Forensic evidence helps identify veracity of whistleblower complaints etc.



A Structured Process

Digital forensics is a detailed, methodical process. Strict adherence to a methodology could mean the difference between success or failure of a computer forensics investigation. There are broadly five steps that a digital forensic investigation follows:

Step 1 - Identification:

In this very first step, all potential sources of evidence that are capable of storing digital information are identified such as computers, phones, hard drives, pen drives, etc. Forensic experts then identify which of these devices require analysis to meet case objectives.

The scope could range from a single laptop to a complete network. In the event that an entire network is under scrutiny, the investigator must identify any rogue devices on the network that are unknown to the organization. In such cases, the mapping and identification of all the machines and devices in the networked environment becomes a forensic expert's first task.

Step 2 - Preservation:

Next, the scope of materials identified in the first step are isolated, secured, and preserved. Steps are taken to ensure that people do not use these devices so that the evidence is secured. Evidence is handled in a manner that maintains the authenticity, and hence credibility, of data.

Next, an image of the evidence is created. An image is a bit-by-bit copy of the evidence (hard drive, USB device, shared network folder, etc.). Evidence collection concludes when all relevant evidence is imaged. The following aspects are among the many issues to be considered in relation to data collection:

Step 3 - Examination:

This step involves in-depth analysis of all the images or copies of evidence in place. The examination phase is never carried out on the actual evidence so that the original evidence remains intact in the event that something goes wrong. There are different types of data that are of interest to a forensic expert in the examination phase:

- **Saved Data** - This is data that is not deleted or created temporarily and is simply present on the image. This could include files created by various users on the system under investigation and could also include operating system specific files.

- **Temporary Data** - A number of programs on a computer system create temporary files and archived files. For instance, try opening a Microsoft Word document and you will notice in the folder, where the file is located, that a number of temporary files are created that often start with a '~' character or have a ".TMP" extension. Such files represent a snapshot of the original file at some point in time and could be important.

- **Deleted Data** - Data that is deleted is still present on a computer system or device. Deletion only instructs the operating system to "forget" that this data exists and notes that the location occupied by this data is now free to be overwritten. The data remains there until the computer writes new data on that part of the drive. With the right tools, this deleted data can still be extracted as long as it hasn't been overwritten. It is also sometimes possible to reconstruct the file even if it has been partially overwritten. Deleted data is sometimes one of the most important pieces of the forensic puzzle.

- **Metadata** - Metadata is data that describes data. For instance, a file could have related information such as the time of creation of the file, the time it was last modified, the physical location of the file on the hard drive, etc. When data is deleted, it is this metadata that is deleted by the operating system. So, basically, the operating system does not "know" where the data is located anymore. But the fact remains that the data still exists on the drive or storage media.

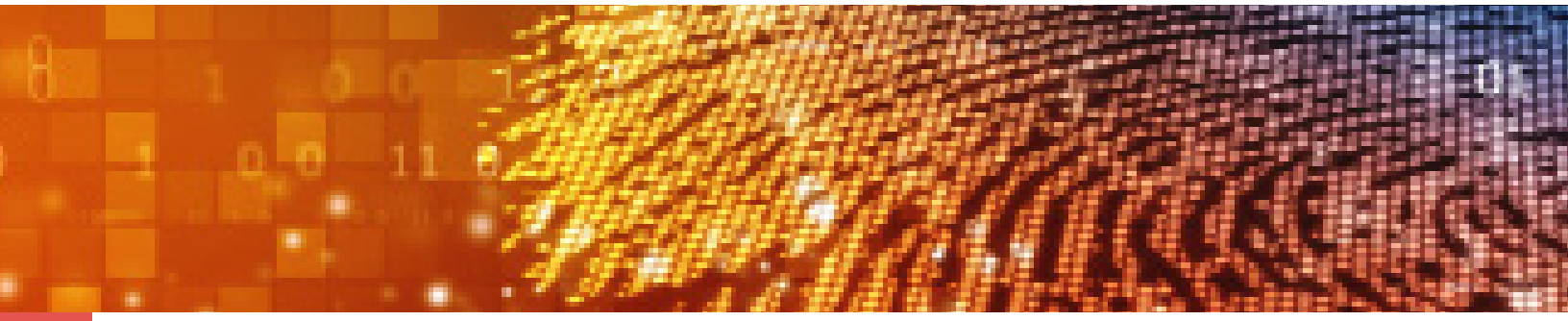
- **Slack Space Data** - Slack space is the area on a hard drive or storage media that is not used by the operating system. Almost every file on a computer system has some associated slack space. If you were given 1.5 gallons of fuel and had 2 canisters of 1 gallon each to fill, one of these would be full and the other would be half-full. The remainder of the second canister, which is the half-empty portion, is the slack space. This slack space on storage media can sometimes contain data that could change the course of a trial.

Step 4 - Documentation:

In this phase, an accurate record of all activities undertaken in relation to the investigation is created. This includes details of the methods used for retrieving, copying, storing, and testing data as well as methods used to examine and access evidence. The forensic expert creates a timeline of events that serves as a foundation for the investigation. Good documentation is critical and should demonstrate how the integrity of data was maintained and also prove that proper policies and procedures were adhered to by everyone involved in the investigation. An investigator's failure to accurately document the process could compromise the validity and admissibility of the evidence.

Step 5 - Reporting:

A good report can serve as the invaluable link between the technical and non-technical elements of a case. A report needs to be comprehensive but at the same time it should be simple and offer an easily understandable explanation of the case-relevant evidence. The report is, essentially, the evidence itself in a form that everyone present in court can understand and interpret. At a minimum, a forensic report should identify the data and the events that took place, an independent evaluation of the sequence of events, and a conclusion or opinion at the end. There's a rule of thumb that you need to follow in digital forensics – If You Didn't Write It Down, It Didn't Happen! This is a simple rule to live by when it comes to documenting all the activities involved in the investigation.



Evidence Handling Procedures

Evidence handling is one of the most important aspects of digital forensics because it singlehandedly determines whether evidence will meet the standards necessary to be admissible in a court of law. Evidence needs to be authentic, reliable, and complete in order to be considered legally valid. Here are some key elements that need to be kept in mind in relation to evidence handling:

Policies and Procedures:

It is critical to establish policies and procedures that provide detailed guidance on how potential digital evidence will be recovered, how systems will be prepared before evidence retrieval, where retrieved evidence will be stored, and how these activities will be documented. This ensures that a formal and unambiguous methodology is followed for collecting evidence and ensuring the authenticity of data.

Preparation:

Computer forensic examiners must properly analyze the case at hand to determine where and how evidence will be collected. Protocols and applicable regulatory requirements should be followed for acquiring evidence. The method that will be used to make a copy of the source evidence should also be determined and agreed upon.

Collection:

After identifying what sources of evidence need to be included in scope, the collection process begins where the computer forensic investigator creates a copy of the electronic evidence in order to preserve it. Computer forensic examiners typically make a bit stream backup of all evidence before reviewing or processing it. Bit stream backups are also known as “mirror image” backups and involve backing up all areas of the device/media such that the backup exactly replicates the device/media.

Hashing:

Hashing is a method to ensure the integrity of data acquired by an investigator. A one-way algorithm is created /applied when the investigator images evidence. If the hash value of the data before starting the imaging process matches the hash value of the copy, this demonstrates that the evidence has not been tampered with during the process to ensure its integrity and admissibility in court.

Chain of Custody:

A chain of custody is a paper trial or sequential documentation of the entire evidence-handling process. It details all the steps performed for data collection, sequence of control, transfer, and analysis of evidence to ensure that it can serve as a supporting form of evidence in a court of law. It is very important to maintain the chain of custody to preserve the integrity of the evidence.

Encryption:

All collected electronic data should be encrypted and secured at all times of collection, in transit, and at its destination.

Handling and Transportation:

Each piece of electronic evidence should be stored in its own electronic evidence bag/box for transportation. Smaller devices could be stored together provided they are first labeled and logged. When transporting evidence, extra caution should be taken so that there is no damage or adverse effect from extreme weather conditions.

Tools Used in Forensic Investigations

Various phases of a digital forensic investigation can be significantly aided and made a lot more efficient with the use of forensic tools – both hardware tools and software tools. A very large number of very good tools, both open-source and proprietary, are available in the market today. Each tool supports a specific purpose and phase of the forensic investigation process.

For instance, there are tools for disk data capture, registry analysis, email analysis, mobile device analysis, database analysis, and so on. There are also forensic tools that offer broader functionalities such as network forensic tools and Internet analysis tools.

However, it is important to remember that tools are meant to supplement and support. The real value in a digital forensic investigation is brought to the table by the investigator's expertise and experience.

Furthermore, when using tools, it is a good idea to use multiple tools when trying to validate findings and/or increase the reliability of the evidence. The National Institute of Standards and Technology (NIST) and the National Institute of Justice (NIJ) have established methodologies and guidance on general tool specifications, hardware, test procedures and more that help organizations and investigators decide upon the best set of tools to use depending on the situation and organization.

The Computer Forensics Tools & Techniques Catalog is a great resource at https://toolcatalog.nist.gov

How to Pick a Digital Forensics Firm

If you are looking to hire an external Digital Forensics expert or firm, here are some things to consider when making a final choice:

- Analyze if the computer forensics company or expert has experience in the platforms and systems that potentially fall within the scope of the investigation. There could be situations where a very competent computer forensics examiner might not be the right choice for your environment because it might be her/his first time viewing a specific technology in your environment.

- Assess the computer forensic team's and company's qualifications. There are several digital forensics certifications available today that are widely acknowledged and highlight expertise in forensic techniques and procedures, standards of practice, and ethical principles such as:

  - **PCI Forensic Investigator (PFI)**
  - **Encase Certified Examiner (ENCE)**
  - **Certified Computer Forensic Examiner (CCFE)**
  - **Certified Cyber Forensics Professional**
  - **GIAC Forensic Examiner (GCFE)**
  - **GIAC Forensic Analyst**
  - **GIAC Network Forensic Analyst**
  - **GIAC Advanced Smartphone Forensics**

Employees holding one or more of these certifications are well-trained in the digital forensics process. Also look to see if the firm or its employees have experience in Expert Witness Testimony.

- Check to see if the computer forensic company has good references. Also, ask for sample deliverables of work to verify the quality.

- Verify if the firm is willing to testify in court in criminal or civil cases if necessary, before the investigation begins. This is where a firm's experience in expert witness testimony can be critical.

- Inquire into the firm's infrastructure to ensure that they have a well-equipped digital forensics laboratory and if they regularly upgrade their software and equipment with time.

Legal Considerations

Computer forensic investigators must discover evidence to support or refute an allegation in a trial in a lawful manner. Legal issues include the method used to obtain the evidence, the right to access it, and the manner in which it is examined.

Before seizing a computer or other electronic device, investigators need to examine whether the Fourth Amendment requires a search warrant. The investigation team needs to know what constitutes a legal search, what telecommunications can lawfully be intercepted or examined, and what privacy rights employees or others involved in the investigation possess.

There may also be situations where data resides across borders, such as in cases involving datacenters operated by a cloud service provider. In such cases, appropriate legal steps need to be followed which factor in regulations and privacy laws that apply to the other country regarding the retrieval of relevant data from their data centers.

These legal issues are the reason that forensic investigators typically work alongside the client's General Counsel, prosecutors or outside lawyers who specialize in laws and regulations impacting their investigations.

ERMProtect
Cybersecurity Solutions

Glossary

Backup
A backup is a copy of computer data taken and stored elsewhere so that it may be used to restore the original after a data loss event.

Bit-by-bit copy
A bit-for-bit copy of a digital file is a copy where each bit of that copy is identical to the corresponding bit in the original. It is used to create an exact copy of data.

Cloud service providers
Cloud service providers are companies that offer network services, infrastructure, application, or storage services. Cloud service is made available to users on demand via the Internet and companies typically have to pay only for the amount of cloud services they use.

Datacenter
A large group of networked computer servers typically used by organizations for the remote storage, processing, or distribution of large amounts of data.

Email Header
The email header is a small piece of code that contains information about the sender, recipient, the email's route to get to the inbox and other authentication details.

FBI
The FBI is a government agency in the United States that investigates crimes in which a national law is broken or in which the country's security is threatened.

Fourth Amendment
The Fourth Amendment to the United States Constitution is part of the Bill of Rights that prohibits unreasonable searches and seizures.

Forensics
Is related to scientific methods of solving crimes, involving examining the objects or substances that are involved in the crime.

Hard drive
Hard drive is the device that stores all the data magnetically so that it stays on the drive even after power supply is turned off.

Hashing
Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string.

Inadmissible
If something is inadmissible it means that it is not accepted as valid evidence in court.

Investigator
A person who carries out a formal inquiry to examine a crime, dispute, statement etc. in order to discover the truth.

Lawsuit
A lawsuit is a case in a court of law which concerns a dispute between two people or organizations.

Physical Surveillance
Physical surveillance is the monitoring of behavior, activities to gather information and evidence on the suspects they are hired to follow.

RAM
RAM is an acronym for random access memory and is a type of computer data storage. A RAM device makes it possible to access data in random order, which makes it very fast to find a specific piece of information.

Shared Network Folder
Shared network folder is a directory or folder made accessible to multiple users on a computer network.