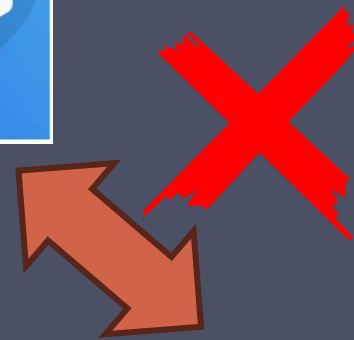


Software Security, Quality and Reliability



- Software quality and reliability



- Software Security

Software Security, Quality and Reliability

- Software quality and reliability:
 - Concerned with the accidental failure of program as a result of some theoretically random, unanticipated input, system interaction, or use of incorrect code
 - Improve using structured design and testing to identify and eliminate as many bugs as possible from a program
 - Concern is not how many bugs, but how often they are triggered

- Software security:
 - Attacker chooses probability distribution, specifically targeting bugs that result in a failure that can be exploited by the attacker
 - Triggered by inputs that differ dramatically from what is usually expected
 - Unlikely to be identified by common testing approaches

Defensive Programming

Defensive Programming

- Designing and implementing software so that it continues to function even when under attack
- Requires attention to all aspects of program execution, environment, and type of data it processes
- Software is able to detect erroneous conditions resulting from some attack
- Also referred to as secure programming
 - Key rule is to never assume anything, check all assumptions and handle any possible error states

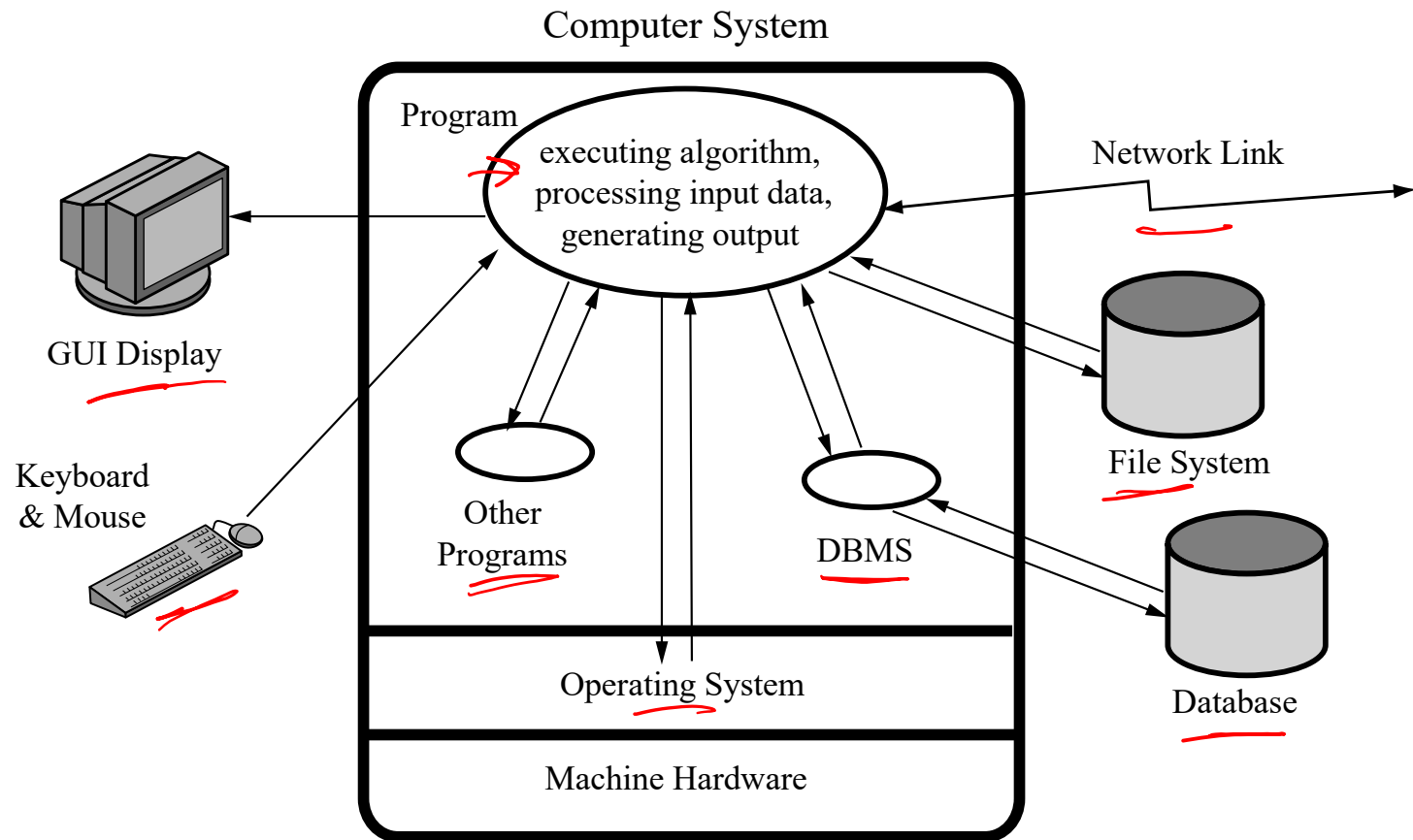


Figure 11.1 Abstract View of Program

Defensive Programming

-  Programmers often make assumptions about the type of inputs a program will receive and the environment it executes in
 - Assumptions need to be validated by the program and all potential failures handled gracefully and safely
-  Requires a changed mindset to traditional programming practices
 - Programmers have to understand how failures can occur and the steps needed to reduce the chance of them occurring in their programs
-  Conflicts with business pressures to keep development times as short as possible to maximize market advantage

Handling Program Input

Handling Program Input

Incorrect handling
of input data is a
very common
failing

Input is any source
of data from
outside and whose
value is not
explicitly known by
the programmer
when the code was
written

Must identify all
data sources

Explicitly validate
assumptions on
size and type of
values before use

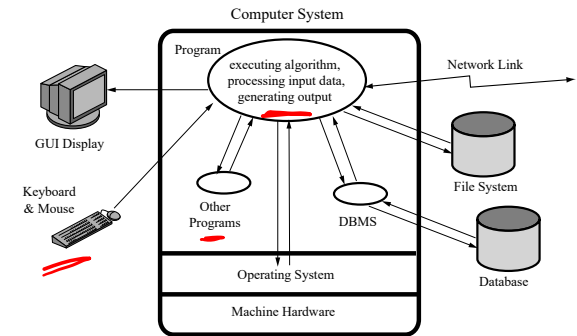


Figure 11.1 Abstract View of Program

Input Size & Buffer Overflow

- Programmers often make assumptions about the maximum expected size of input
 - Allocated buffer size is not confirmed
 - Resulting in buffer overflow
- Testing may not identify vulnerability
 - Test inputs are unlikely to include large enough inputs to trigger the overflow
- Safe coding treats all input as dangerous

Interpretation of Program Input

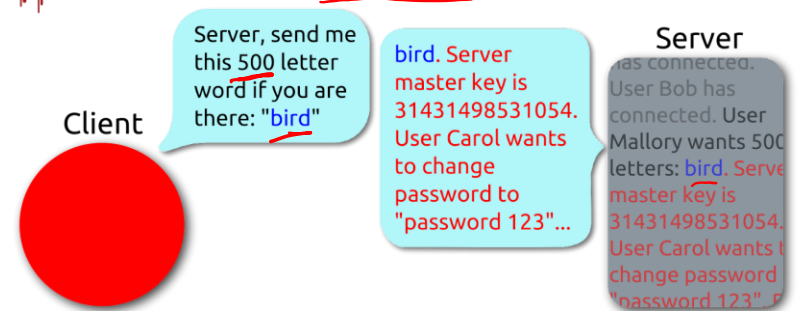
- Program input may be binary or text
 - Binary interpretation depends on encoding and is usually application specific
- There is an increasing variety of character sets being used
 - Care is needed to identify just which set is being used and what characters are being read
- Failure to validate may result in an exploitable vulnerability
- 2014 Heartbleed OpenSSL bug is a recent example of a failure to check the validity of a binary input value



Heartbeat – Normal usage



Heartbeat – Malicious usage



Injection Attacks

Injection Attacks

- Flaws relating to invalid handling of input data, specifically when program input data can accidentally or deliberately influence the flow of execution of the program

Most often occur in scripting languages

- Encourage reuse of other programs and system utilities where possible to save coding effort

```
$name = $_REQUEST['name'];  
$query = "SELECT * FROM suppliers WHERE name = '" . $name . "'";  
$result = mysql_query($query);
```

(a) Vulnerable PHP code

```
$name = $_REQUEST['name'];  
$query = "SELECT * FROM suppliers WHERE name = '" .  
    mysql_real_escape_string($name) . "'";  
$result = mysql_query($query);
```

(b) Safer PHP code

Figure 11.3 SQL Injection Example

SQL Injection Attack Demo

<https://www.codingame.com/playgrounds/154/sql-injection-demo/sql-injection>

```
$name = $_REQUEST['name'];  
$query = "SELECT * FROM suppliers WHERE name = '" . $name . "'";  
$result = mysql_query($query);
```

(a) Vulnerable PHP code

```
$name = $_REQUEST['name'];  
$query = "SELECT * FROM suppliers WHERE name = '" .  
    mysql_real_escape_string($name) . "'";  
$result = mysql_query($query);
```

(b) Safer PHP code

Figure 11.3 SQL Injection Example

query = "SELECT name FROM user where username = ' + username + ' and password = ' + password + '";

query = "SELECT name FROM user where username = 'admin' and password = 'admin123' "; ✓

query = "SELECT name FROM user where username = 'any' and password = '123' or '1'='1'";

Injected SQL

Forensic Science



- Forensic science, also known as criminalistics, is the application of science to criminal and civil laws.
- During criminal investigation in particular, it is governed by the legal standards of admissible evidence and criminal procedure.
- It is a broad field utilizing numerous practices such as the analysis of DNA, fingerprints, bloodstain patterns, firearms, ballistics, and toxicology.
- Forensic scientists collect, preserve, and analyze scientific evidence during the course of an investigation.
- While some forensic scientists travel to the scene of the crime to collect the evidence themselves, others occupy a laboratory role, performing analysis on objects brought to them by other individuals.
- Still others are involved in analysis of financial, banking, or other numerical data for use in financial crime investigation, and can be employed as consultants from private firms, academia, or as government employees.
- In addition to their laboratory role, forensic scientists testify as expert witnesses in both criminal and civil cases and can work for either the prosecution or the defense.

Origins of forensic science and early methods

- The ancient world lacked standardized forensic practices, which enabled criminals to escape punishment.
- Criminal investigations and trials relied heavily on forced confessions and witness testimony.
- However, ancient sources do contain several accounts of techniques that foreshadow concepts in forensic science developed centuries later.

Locard's Exchange Principle

- In forensic science, Locard's principle holds that the perpetrator of a crime will bring something into the crime scene and leave with something from it, and that both can be used as forensic evidence.
- Dr. Edmond Locard (1877–1966) was a pioneer in forensic science who became known as the Sherlock Holmes of Lyon, France.
- He formulated the basic principle of forensic science as: "Every contact leaves a trace".
- It is generally understood as "with contact between two items, there will be an exchange."
- Paul L. Kirk expressed the principle as follows:
 - Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him.
 - Not only his fingerprints or his footprints, but his hair, the fibres from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects.
 - All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value.



Edmond Locard's (Sherlock Holmes of France) Principle

Every contact by a criminal
leaves behind a trace.



- **Fragmentary** or **trace evidence** is any type of material left at (or taken from) a crime scene, or the result of **contact** between two surfaces, such as shoes and the floor covering or soil, or fibres from where someone sat on an upholstered chair.
- When a crime is committed, fragmentary (or trace) evidence needs to be collected from the scene.
- A team of specialised police technicians goes to the scene of the crime and seals it off.
- They record video and take photographs of the crime scene, victim/s (if there are any) and items of evidence.
- If necessary, they undertake ballistics examinations.
- They check for foot, shoe, and tire mark impressions, plus hair as well as examine any vehicles and check for fingerprints – whole or partial.

Principle of Exchange

According to this, when a criminal or his instrument of crime come in contact with the victim or the objects surrounding him, they leave traces, and the criminal or his instrument picks up traces from the same contact.

– Edmond Locard

What is computer/digital/cyber forensics?

- Cyber forensics is the discovery, analysis, and reconstruction of evidence extracted from any element of Computer systems, Computer networks, Computer media, and Computer peripherals that allow investigators to solve a crime.
- Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery, investigation, examination, and analysis of material found in digital devices, often in relation to mobile devices and computer crime.
- The term "digital forensics" was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data.



Media types used for computer forensic analysis: a Fujifilm FinePix digital camera, two flash memory cards, a USB flash drive, a 5GB iPod, a CD-R or DVD recordable, and a Mini CD.

<https://en.wikipedia.org/wiki/File:PersonalStorageDevices.agr.jpg>













Nature of Digital Evidence

- Physical Form
- Virtual Locations / Paths
- Volatile vs Non-volatile

Application and Uses



- Digital forensics investigations have a variety of applications.
- The most common is to support or refute a hypothesis before criminal or civil courts.
- Criminal cases involve the alleged breaking of laws that are defined by legislation and enforced by the police and prosecuted by the state, such as murder, theft, and assault against the person.
- Civil cases, on the other hand, deal with protecting the rights and property of individuals (often associated with family disputes), but may also be concerned with contractual disputes between commercial entities where a form of digital forensics referred to as electronic discovery (ediscovery) may be involved.
- Forensics may also feature in the private sector, such as during internal corporate investigations or intrusion investigations (a special probe into the nature and extent of an unauthorized network intrusion).
- As well as identifying direct evidence of a crime, digital forensics can be used to attribute evidence to specific suspects, confirm alibis or statements, determine intent, identify sources (for example, in copyright cases), or authenticate documents.
- Investigations are much broader in scope than other areas of forensic analysis (where the usual aim is to provide answers to a series of simpler questions), often involving complex time-lines or hypotheses.



- Digital forensics is commonly used in both criminal law and private investigation.
- Traditionally it has been associated with criminal law, where evidence is collected to support or oppose a hypothesis before the courts.
- As with other areas of forensics this is often a part of a wider investigation spanning a number of disciplines.
- In some cases, the collected evidence is used as a form of intelligence gathering, used for other purposes than court proceedings (for example to locate, identify or halt other crimes).
- In civil litigation or corporate matters digital forensics forms part of the electronic discovery (or eDiscovery) process.
- Forensic procedures are similar to those used in criminal investigations, often with different legal requirements and limitations.
- Outside of the courts digital forensics can form a part of internal corporate investigations.
- A common example might be following unauthorized network intrusion.
- A specialist forensic examination into the nature and extent of the attack is performed as a damage limitation exercise, both to establish the extent of any intrusion and in an attempt to identify the attacker.

Subdivisions and Branches

- Digital forensics is the application of proven scientific methods and techniques in order to recover data from electronic / digital media. Digital Forensic specialists work in the field as well as in the lab.
- Digital forensics investigation is not restricted to retrieve data merely from the computer, as laws are breached by the criminals and small digital devices (e.g. tablets, smartphones, flash drives) are now extensively used.
- Some of these devices have volatile memory while some have non-volatile memory.
- Sufficient methodologies are available to retrieve data from volatile memory, however, there is lack of detailed methodology or a framework for data retrieval from non-volatile memory sources.
- Also, the technical aspect of an investigation is divided into several sub-branches related to the type of digital devices involved:
 - computer forensics, network forensics, forensic data analysis, and mobile device forensics, router forensics.
- Depending on the type of devices, media or artifacts, digital forensics investigation is branched into various types.

Digital Forensic Categories / Subdivisions / Branches

- Computer Forensics
- Mobile Device Forensics
- Network Forensics [Logs]
- Forensic Data Analysis
- Digital Image Forensics
- Database Forensics
- Cloud Forensics
- IoT Forensics
- Dark Web Forensics
- Audio Analysis/Forensics
- Video Analysis/Forensics
- E-Mail Forensics

- **Computer forensics**

- The goal of computer forensics is to explain the current state of a digital artifact; such as a computer system, storage medium or electronic document.
- The discipline usually covers computers, embedded systems (digital devices with rudimentary computing power and onboard memory) and static memory (such as USB pen drives).
- Computer forensics can deal with a broad range of information; from logs (such as internet history) through to the actual files on the drive.
- In 2007 prosecutors used a spreadsheet recovered from the computer of Joseph Edward Duncan to show premeditation and secure the death penalty.
- Sharon Lopatka's killer was identified in 2006 after email messages from him detailing torture and death fantasies were found on her computer.

- **Mobile device forensics**

- Mobile device forensics is a sub-branch of digital forensics relating to recovery of digital evidence or data from a mobile device.
- Mobile device forensics is the scientific examination and evaluation of evidence found in mobile phones, e.g. Call History and Deleted SMS, and includes SIM Card Forensics.
- It differs from Computer forensics in that a mobile device will have an inbuilt communication system (e.g. GSM) and, usually, proprietary storage mechanisms.
- Investigations usually focus on simple data such as call data and communications (SMS/Email) rather than in-depth recovery of deleted data.
- SMS data from a mobile device investigation helped to exonerate Patrick Lumumba in the murder of Meredith Kercher.
- Mobile devices are also useful for providing location information; either from inbuilt gps/location tracking or via cell site logs, which track the devices within their range.
- Such information was used to track down the kidnappers of Thomas Onofri in 2006.

- **Network forensics**

- Network forensics is concerned with the monitoring and analysis of computer network traffic, both local and WAN/internet, for the purposes of information gathering, evidence collection, or intrusion detection.
- Traffic is usually intercepted at the packet level, and either stored for later analysis or filtered in real-time.
- Unlike other areas of digital forensics network data is often volatile and rarely logged, making the discipline often reactionary.

- **Forensic data analysis**
 - Forensic Data Analysis is a branch of digital forensics. It examines structured data with the aim to discover and analyze patterns of fraudulent activities resulting from financial crime.
- **Digital image forensics**
 - Digital image forensics (or forensic image analysis) is a branch of digital forensics that deals with examination and verification of an image's authenticity and content.
 - These can range from Stalin-era airbrushed photos to elaborate deepfake videos.
 - This has broad implications for a wide variety of crimes, for determining the validity of information presented in civil and criminal trials, and for verifying images and information that are circulated through news and social media.
- **Forensic video analysis** is the scientific examination, comparison and evaluation of video in legal matters.

- **Database forensics**

- Database forensics is a branch of digital forensics relating to the forensic study of databases and their metadata.
- Investigations use database contents, log files and in-RAM data to build a timeline or recover relevant information.

- **IoT Forensics**

- IoT forensics is a branch of Digital forensics that has the goal of identifying and extracting digital information from devices belonging to the Internet of things field, to be used for forensics investigations as potential source of evidence.

Digital Forensic Standards & Frameworks

- Since 2000, in response to the need for standardization, various bodies and agencies have published guidelines for digital forensics.
 1. The Scientific Working Group on Digital Evidence (SWGDE) produced a 2002 paper, Best practices for Computer Forensics.
 2. This was followed, in 2005, by the publication of an ISO standard (ISO 17025, General requirements for the competence of testing and calibration laboratories).
 3. NIST

Forensic Lab Setup

- Laws & Regulations
- Types of Incidents
- Important Numbers / Emergency Contacts
- Physical Location
- Team Members & Personnel
- Forensic Expertise
- HVAC & Lighting
- Building Structure
- Tools
 - Hardware
 - Forensic Machines
 - Cables & Connectors
 - Software
 - Write Blocker
 - Duplicator
 - Storage
 - Data & Equipment

Digital Forensic Process

- The typical forensic process encompasses the **seizure**, forensic **imaging (acquisition)**, and **analysis** of digital media, followed with the production of a **report** of the collected evidence.



<https://www.uco.edu/programs/microcredentials/digital-evidence>

- A digital forensic investigation commonly consists of 3 stages:
 - acquisition or imaging of exhibits, analysis, and reporting.
- Ideally acquisition involves capturing an image of the computer's volatile memory (RAM) and creating an exact sector level duplicate (or "forensic duplicate") of the media, often using a **write blocking** device to prevent modification of the original.
 - However, the growth in size of storage media and developments such as cloud computing have led to more use of **'live' acquisitions** whereby a 'logical' copy of the data is acquired rather than a complete image of the physical storage device.
 - Both acquired image (or logical copy) and original media/data are **hashed** (using an algorithm such as SHA-1 or MD5) and the values compared to verify the copy is accurate.
- During the analysis phase an investigator recovers evidence material using a number of different methodologies and tools.
 - In 2002, an article in the International Journal of Digital Evidence referred to this step as "an in-depth systematic search of evidence related to the suspected crime."
 - In 2006, forensics researcher Brian Carrier described an "intuitive procedure" in which obvious evidence is first identified and then "exhaustive searches are conducted to start filling in the holes."
 - The actual process of analysis can vary between investigations, but common methodologies include conducting keyword searches across the digital media (within files as well as unallocated and slack space), recovering deleted files and extraction of registry information (for example to list user accounts, or attached USB devices).
 - The evidence recovered is analysed to reconstruct events or actions and to reach conclusions, work that can mostly be performed by specialised staff.
- When an investigation is complete the data is presented, usually in the form of a written report, in lay persons' terms.

DIGITAL FORENSICS

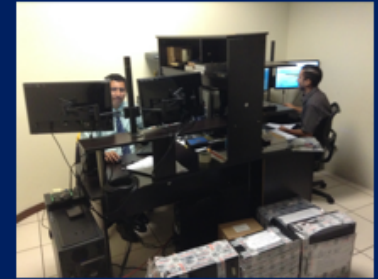
Identification

Where is the evidence? In which country?
Which device(s) does it need to be gathered from?
Is the data "at rest" or "in transit"?



Preservation

How will the data be accessed? Which legislation applies?
Is the action proportionate, lawful, accountable and necessary?



Analysis

Are the required technical and people skills available
to acquire, analyse and exploit the evidence in a
timely manner with full chain-of-custody?

Documentation

Ensure EVERYTHING is documented to prevent losing
evidence due to legal or procedural mistakes

Presentation

Evidence should be presented accurately, concisely
and clearly. Can the judge and/or jury understand it?
Can it be tested and challenged by the defence?



An example of an image's Exif metadata that might be used to prove its origin

https://en.wikipedia.org/wiki/File:En_exif_data.png

Camera manufacturer	Canon
Camera model	Canon EOS 400D DIGITAL
Exposure time	1/60 sec (0.016666666666667)
F-number	f/4.5
ISO speed rating	400
Date and time of data generation	11:06, August 27, 2010
Lens focal length	31 mm
Show extended details	

Forensic Report

- Title Page [Case number/title, reporting date, number of pages, examiner name]
- Case Summary
- Evidence Details or Particulars
- Tools Used
- Methodology / Steps
- Forensic Analysis & Findings
- Forensic Investigator/Examiner Signature
- Images of Evidentiary Items
- Chain of Custody

Development of Digital Forensic Tools

- During the 1980s, very few specialized digital forensic tools existed.
- Consequently, investigators often performed live analysis on media, examining computers from within the operating system using existing **sysadmin tools** to extract evidence.
- This practice carried the **risk of modifying data** on the disk, either inadvertently or otherwise, which led to claims of **evidence tampering**.
- A number of tools were created during the early 1990s to address the problem.
- The need for such software was first recognized in 1989 at the Federal Law Enforcement Training Center, resulting in the creation of IMDUMP (by Michael White) and in 1990, SafeBack (developed by Sydex).
- Similar software was developed in other countries; DIBS (a hardware and software solution) was released commercially in the UK in 1991, and Rob McKemmish released Fixed Disk Image free to Australian law enforcement.
- These tools allowed examiners to create an **exact copy** of a piece of digital media to work on, leaving the **original disk intact for verification**.
- By the end of the 1990s, as demand for digital evidence grew, more **advanced commercial tools** such as **EnCase** and **FTK** were developed, allowing analysts to examine copies of media without using any live forensics.
- More recently, a trend towards "live memory forensics" has grown, resulting in the availability of tools such as WindowsSCOPE.
- The same progression of tool development has occurred for **mobile devices**; initially investigators accessed data directly on the device, but soon specialist tools such as **Cellebrite**, **XRY** or Radio Tactics Aceso appeared.

<https://interworks.com/blog/bstephens/2016/02/05/what-digital-forensics/>



Digital Forensic Tools

- Building Structure
- Tools
 - Hardware
 - Forensic Machines
 - Cables & Connectors
 - Software
 - Write Blocker
 - Duplicator
 - Storage
 - Data & Equipment

Mobile phones in an Evidence bag
<https://en.wikipedia.org/wiki/File:Mobiles.JPG>



A portable Tableau write-blocker attached to a hard drive
https://en.wikipedia.org/wiki/File:Portable_forensic_tableau.JPG



Limitations

- Encryption
 - One major limitation to a forensic investigation is the use of encryption; this disrupts initial examination where pertinent evidence might be located using keywords.
 - Laws to compel individuals to disclose encryption keys are still relatively new and controversial but always more frequently there are solutions to brute force passwords or bypass encryption, such as in smartphones or PCs where by means of bootloader techniques the content of the device can be first acquired and later forced in order to find the password or encryption key.
- Steganography
- Cloud Computing/Forensics
 - Jurisdiction
 - Virtualization
 - Elasticity

Anti-Forensic Techniques

- Passwords
- Encryption
- Jurisdiction
- Proxy Chaining
- Steganography
- NTFS Data Streams

Data hiding

- Data hiding is the process of making data difficult to find while also keeping it accessible for future use.
- "Obfuscation and encryption of data give an adversary the ability to limit identification and collection of evidence by investigators while allowing access and use to themselves."
- Some of the more common forms of data hiding include encryption, steganography and other various forms of hardware/software based data concealment.
- Each of the different data hiding methods makes digital forensic examinations difficult.
- When the different data hiding methods are combined, they can make a successful forensic investigation nearly impossible.
- Encryption
- Steganography
- Other forms of data hiding

Data hiding: Encryption

- One of the more commonly used techniques to defeat computer forensics is data encryption.
- In a presentation given on encryption and anti-forensic methodologies, the Vice President of Secure Computing, Paul Henry, referred to encryption as a "forensic expert's nightmare".
- The majority of publicly available encryption programs allow the user to create virtual encrypted disks which can only be opened with a designated key.
 - Through the use of modern encryption algorithms and various encryption techniques these programs make the data virtually impossible to read without the designated key.
- File level encryption encrypts only the file contents.
 - This leaves important information such as file name, size and timestamps unencrypted.
 - Parts of the content of the file can be reconstructed from other locations, such as temporary files, swap file and deleted, unencrypted copies.
- Most encryption programs have the ability to perform a number of additional functions that make digital forensic efforts increasingly difficult.
 - Some of these functions include the use of a keyfile, full-volume encryption, and plausible deniability.
 - The widespread availability of software containing these functions has put the field of digital forensics at a great disadvantage.

Data hiding: Steganography

- Steganography is a technique where information or files are hidden within another file in an attempt to hide data by leaving it in plain sight.
- "Steganography produces dark data that is typically buried within light data (e.g., a non-perceptible digital watermark buried within a digital photograph)."
- While some experts have argued that the use of steganography techniques is not very widespread and therefore the subject shouldn't be given a lot of thought, most experts agree that steganography has the capability of disrupting the forensic process when used correctly.
- According to Jeffrey Carr, a 2007 edition of Technical Mujahid (a bi-monthly terrorist publication) outlined the importance of using a steganography program called Secrets of the Mujahideen. According to Carr, the program was touted as giving the user the capability to avoid detection by current steganalysis programs. It did this through the use of steganography in conjunction with file compression.

Data hiding: Other forms of data hiding

- Other forms of data hiding involve the use of tools and techniques to hide data throughout various locations in a computer system.
 - Some of these places can include "memory, slack space, hidden directories, bad blocks, alternate data streams, (and) hidden partitions."
- One of the more well known tools that is often used for data hiding is called Slacker (part of the Metasploit framework).
 - Slacker breaks up a file and places each piece of that file into the slack space of other files, thereby hiding it from the forensic examination software.
- Another data hiding technique involves the use of bad sectors.
 - To perform this technique, the user changes a particular sector from good to bad and then data is placed onto that particular cluster.
 - The belief is that forensic examination tools will see these clusters as bad and continue on without any examination of their contents.

Artifact wiping

- The methods used in artifact wiping are tasked with permanently eliminating particular files or entire file systems.
- This can be accomplished through the use of a variety of methods that include disk cleaning utilities, file wiping utilities and disk degaussing/destruction techniques.
- Disk cleaning utilities
- File wiping utilities
- Disk degaussing / destruction techniques

Artifact wiping: Disk cleaning utilities

- Disk cleaning utilities use a variety of methods to overwrite the existing data on disks .
- The effectiveness of disk cleaning utilities as anti-forensic tools is often challenged as some believe they are not completely effective.
- Experts who don't believe that disk cleaning utilities are acceptable for disk sanitization base their opinions of current DOD policy, which states that the only acceptable form of sanitization is degaussing.
- Disk cleaning utilities are also criticized because they leave signatures that the file system was wiped, which in some cases is unacceptable.
- Some of the widely used disk cleaning utilities include DBAN, srm, BCWipe Total WipeOut, KillDisk, PC Inspector and CyberScrubs cyberCide.
- Another option which is approved by the NIST and the NSA is CMRR Secure Erase, which uses the Secure Erase command built into the ATA specification.

Artifact wiping: File wiping utilities

- File wiping utilities are used to delete individual files from an operating system.
- The advantage of file wiping utilities is that they can accomplish their task in a relatively short amount of time as opposed to disk cleaning utilities which take much longer.
- Another advantage of file wiping utilities is that they generally leave a much smaller signature than disk cleaning utilities.
- There are two primary disadvantages of file wiping utilities, first they require user involvement in the process and second some experts believe that file wiping programs don't always correctly and completely wipe file information.
- Some of the widely used file wiping utilities include BCWipe, R-Wipe & Clean, Eraser, Aevita Wipe & Delete and CyberScrubs PrivacySuite.
- On Linux tools like shred and srm can be also used to wipe single files.
- SSDs are by design more difficult to wipe, since the firmware can write to other cells therefore allowing data recovery.
- In these instances ATA Secure Erase should be used on the whole drive, with tools like hdparm that support it.

Artifact wiping: Disk degaussing / destruction techniques

- Disk degaussing is a process by which a magnetic field is applied to a digital media device.
- The result is a device that is entirely clean of any previously stored data.
- Degaussing is rarely used as an anti-forensic method despite the fact that it is an effective means to ensure data has been wiped.
- This is attributed to the high cost of degaussing machines, which are difficult for the average consumer to afford.
- A more commonly used technique to ensure data wiping is the physical destruction of the device.
- The NIST recommends that "physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverizing, shredding and melting.

Trail obfuscation

- The purpose of trail obfuscation is to confuse, disorient, and divert the forensic examination process.
- Trail obfuscation covers a variety of techniques and tools that include "log cleaners, spoofing, misinformation, backbone hopping, zombied accounts, trojan commands."
- One of the more widely known trail obfuscation tools is Timestomp (part of the Metasploit Framework).
 - Timestomp gives the user the ability to modify file metadata pertaining to access, creation and modification times/dates.
 - By using programs such as Timestomp, a user can render any number of files useless in a legal setting by directly calling into question the files' credibility.
- Another well known trail-obfuscation program is Transmogrify (also part of the Metasploit Framework).
 - In most file types the header of the file contains identifying information.
 - A (.jpg) would have header information that identifies it as a (.jpg), a (.doc) would have information that identifies it as (.doc) and so on.
 - Transmogrify allows the user to change the header information of a file, so a (.jpg) header could be changed to a (.doc) header.
 - If a forensic examination program or operating system were to conduct a search for images on a machine, it would simply see a (.doc) file and skip over it.

Attacks against computer forensics

- In the past anti-forensic tools have focused on attacking the forensic process by destroying data, hiding data, or altering data usage information.
- Anti-forensics has recently moved into a new realm where tools and techniques are focused on attacking forensic tools that perform the examinations.
- These new anti-forensic methods have benefited from a number of factors to include well documented forensic examination procedures, widely known forensic tool vulnerabilities, and digital forensic examiners' heavy reliance on their tools.
- During a typical forensic examination, the examiner would create an image of the computer's disks.
 - This keeps the original computer (evidence) from being tainted by forensic tools.
 - Hashes are created by the forensic examination software to verify the integrity of the image.
 - One of the recent anti-tool techniques targets the integrity of the hash that is created to verify the image.
 - By affecting the integrity of the hash, any evidence that is collected during the subsequent investigation can be challenged.

Forensic Jobs

- Government, Military, Law Enforcement Agencies
- Private sector companies
- Designations:
 - Forensic Examiner / Specialist / Scientist / Manager
- Relevant Degree, Certifications and Experience



Digital Forensic Certifications

- There are several computer forensics certifications available, such as the ISFCE Certified Computer Examiner, Digital Forensics Investigation Professional (DFIP) and IACRB Certified Computer Forensics Examiner.
- The top vendor independent certification (especially within EU) is considered the CCFP - Certified Cyber Forensics Professional.
- Others, worth to mention for USA or APAC are: The International Association of Computer Investigative Specialists offers the Certified Computer Examiner program. The International Society of Forensic Computer Examiners offers the Certified Computer Examiner program.
- Many commercial based forensic software companies are now also offering proprietary certifications on their products.
 - For example, Guidance Software offering the (EnCE) certification on their tool EnCase, AccessData offering (ACE) certification on their tool FTK, PassMark Software offering certification on their tool OSForensics, and X-Ways Software Technology offering (X-PERT) certification for their software, X-Ways Forensics.
- Tool Specific: EnCase, AccessData FTK, Cellebrite
- General: CHFI (Certified Hacking Forensic Investigator by EC-Council), Mile2, eLearnSecurity, SANS GIAC and many more

DIGITAL FORENSICS

Computer forensics (also known as computer forensic science) is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail.

Evidence from computer forensics investigations is usually subjected to the same guidelines and practices of other digital evidence. It has been used in a number of high-profile cases and is accepted as reliable within U.S. and European court systems.

Overview

In the early 1980s, personal computers became more accessible to consumers, leading to their increased use in criminal activity (for example, to help commit fraud). At the same time, several new "computer crimes" were recognized (such as cracking). The discipline of computer forensics emerged during this time as a method to recover and investigate digital evidence for use in court. Since then, computer crime and computer-related crime has grown, with the FBI reporting a suspected 791,790 internet crimes alone in 2020, a 69% increase over the amount reported in 2019. Today, computer forensics is used to investigate a wide variety of crime, including child pornography, fraud, espionage, cyberstalking, murder, and rape. The discipline also features in civil proceedings as a form of information gathering (for example, Electronic discovery)

Forensic techniques and expert knowledge are used to explain the current state of a digital artifact, such as a computer system, storage medium (e.g., hard disk or CD-ROM), or an electronic document (e.g., an email message or JPEG image). The scope of a forensic analysis can vary from simple information retrieval to reconstructing a series of events. In a 2002 book, *Computer Forensics*, authors Kruse and Heiser define computer forensics as involving "the preservation, identification, extraction, documentation and interpretation of computer data". They go on to describe the discipline as "more of an art than a science", indicating that forensic methodology is backed by flexibility and extensive domain knowledge. However, while several methods can be used to extract evidence from a given computer, the strategies used by law enforcement are fairly rigid and lack the flexibility found in the civilian world.

Digital forensics

Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery, investigation, examination, and analysis of material found in digital devices, often in relation to mobile devices and computer crime. The term "digital forensics" was originally used as a synonym for computer forensics but has expanded to cover investigation of all

devices capable of storing digital data. With roots in the personal computing revolution of the late 1970s and early 1980s, the discipline evolved in a haphazard manner during the 1990s, and it was not until the early 21st century that national policies emerged.

Digital forensics investigations have a variety of applications. The most common is to support or refute a hypothesis before criminal or civil courts. Criminal cases involve the alleged breaking of laws that are defined by legislation and enforced by the police and prosecuted by the state, such as murder, theft, and assault against the person. Civil cases, on the other hand, deal with protecting the rights and property of individuals (often associated with family disputes), but may also be concerned with contractual disputes between commercial entities where a form of digital forensics referred to as electronic discovery (ediscovery) may be involved.

Forensics may also feature in the private sector, such as during internal corporate investigations or intrusion investigations (a special probe into the nature and extent of an unauthorized network intrusion).

The technical aspect of an investigation is divided into several sub-branches related to the type of digital devices involved: computer forensics, network forensics, forensic data analysis, and mobile device forensics. The typical forensic process encompasses the seizure, forensic imaging (acquisition), and analysis of digital media, followed with the production of a report of the collected evidence.

As well as identifying direct evidence of a crime, digital forensics can be used to attribute evidence to specific suspects, confirm alibis or statements, determine intent, identify sources (for example, in copyright cases), or authenticate documents. Investigations are much broader in scope than other areas of forensic analysis (where the usual aim is to provide answers to a series of simpler questions), often involving complex time-lines or hypotheses.

History

Prior to the 1970s, crimes involving computers were dealt with using existing laws. The first computer crimes were recognized in the 1978 Florida Computer Crimes Act, which included legislation against the unauthorized modification or deletion of data on a computer system. Over the next few years, the range of computer crimes being committed increased, and laws were passed to deal with issues of copyright, privacy/harassment (e.g., cyber bullying, happy slapping, cyber stalking, and online predators), and child pornography. It was not until the 1980s that federal laws began to incorporate computer offences. Canada was the first country to pass legislation in 1983. This was followed by the US Federal Computer Fraud and Abuse Act in 1986, Australian amendments to their crimes acts in 1989, and the British Computer Misuse Act in 1990.

1980s–1990s: Growth of the field

The growth in computer crime during the 1980s and 1990s caused law enforcement agencies to begin establishing specialized groups, usually at the national level, to handle the technical aspects of investigations. For example, in 1984, the FBI launched a Computer Analysis and Response Team and the following year a computer crime department was set up within the British Metropolitan Police fraud squad. As well as being law enforcement professionals, many of the early members of these groups were also computer hobbyists and became responsible for the field's initial research and direction.

One of the first practical (or at least publicized) examples of digital forensics was Cliff Stoll's pursuit of hacker Markus Hess in 1986. Stoll, whose investigation made use of computer and network forensic techniques, was not a specialized examiner. Many of the earliest forensic examinations followed the same profile.

Throughout the 1990s, there was high demand for these new, and basic, investigative resources. The strain on central units led to the creation of regional, and even local, level groups to help handle the load. For example, the British National Hi-Tech Crime Unit was set up in 2001 to provide a national infrastructure for computer crime, with personnel located both centrally in London and with the various regional police forces (the unit was folded into the Serious Organised Crime Agency (SOCA) in 2006).

During this period, the science of digital forensics grew from the ad-hoc tools and techniques developed by these hobbyist practitioners. This is in contrast to other forensics disciplines, which developed from work by the scientific community. It was not until 1992 that the term "computer forensics" was used in academic literature (although prior to this, it had been in informal use); a paper by Collier and Spaul attempted to justify this new discipline to the forensic science world. This swift development resulted in a lack of standardization and training. In his 1995 book, *High-Technology Crime: Investigating Cases Involving Computers*, K. Rosenblatt wrote the following:

Seizing, preserving, and analyzing evidence stored on a computer is the greatest forensic challenge facing law enforcement in the 1990s. Although most forensic tests, such as fingerprinting and DNA testing, are performed by specially trained experts the task of collecting and analyzing computer evidence is often assigned to patrol officers and detectives.

2000s: Developing standards

Since 2000, in response to the need for standardization, various bodies and agencies have published guidelines for digital forensics. The Scientific Working Group on Digital Evidence (SWGDE) produced a 2002 paper, *Best practices for Computer Forensics*, this was followed, in 2005, by the publication of an ISO standard (ISO 17025, General requirements for the competence of testing and calibration laboratories). A European-led international treaty, the Convention on Cybercrime, came into force in 2004 with the aim of reconciling national computer crime laws, investigative techniques, and international co-operation. The treaty has been signed by 43 nations (including the US, Canada, Japan, South Africa, UK, and other European nations) and ratified by 16.

The issue of training also received attention. Commercial companies (often forensic software developers) began to offer certification programs, and digital forensic analysis was included as a topic at the UK specialist investigator training facility, Centrex.

In the late 1990s, mobile devices became more widely available, advancing beyond simple communication devices, and were found to be rich forms of information, even for crime not traditionally associated with digital forensics. Despite this, digital analysis of phones has lagged behind traditional computer media, largely due to problems over the proprietary nature of devices.

Focus has also shifted onto internet crime, particularly the risk of cyber warfare and cyberterrorism. A February 2010 report by the United States Joint Forces Command concluded the following:

Through cyberspace, enemies will target industry, academia, government, as well as the military in the air, land, maritime, and space domains. In much the same way that airpower transformed the

battlefield of World War II, cyberspace has fractured the physical barriers that shield a nation from attacks on its commerce and communication.

The field of digital forensics still faces unresolved issues. A 2009 paper, "Digital Forensic Research: The Good, the Bad and the Unaddressed" by Peterson and Shenoi, identified a bias towards Windows operating systems in digital forensics research. In 2010, Simson Garfinkel identified issues facing digital investigations in the future, including the increasing size of digital media, the wide availability of encryption to consumers, a growing variety of operating systems and file formats, an increasing number of individuals owning multiple devices, and legal limitations on investigators. The paper also identified continued training issues, as well as the prohibitively high cost of entering the field.

Development of forensic tools

During the 1980s, very few specialized digital forensic tools existed. Consequently, investigators often performed live analysis on media, examining computers from within the operating system using existing sysadmin tools to extract evidence. This practice carried the risk of modifying data on the disk, either inadvertently or otherwise, which led to claims of evidence tampering. A number of tools were created during the early 1990s to address the problem.

The need for such software was first recognized in 1989 at the Federal Law Enforcement Training Center, resulting in the creation of IMDUMP (by Michael White) and in 1990, SafeBack (developed by Sydex). Similar software was developed in other countries; DIBS (a hardware and software solution) was released commercially in the UK in 1991, and Rob McKemmish released Fixed Disk Image free to Australian law enforcement. These tools allowed examiners to create an exact copy of a piece of digital media to work on, leaving the original disk intact for verification. By the end of the 1990s, as demand for digital evidence grew, more advanced commercial tools such as EnCase and FTK were developed, allowing analysts to examine copies of media without using any live forensics. More recently, a trend towards "live memory forensics" has grown, resulting in the availability of tools such as WindowsSCOPE.

More recently, the same progression of tool development has occurred for mobile devices; initially investigators accessed data directly on the device, but soon specialist tools such as XRY or Radio Tactics Aceso appeared.

Cybersecurity

Computer forensics is often confused with cybersecurity. Cybersecurity is about prevention and protection, while computer forensics is more reactionary and active, involving activities such as tracking and exposing. System security usually encompasses two teams, cybersecurity and computer forensics, which work together. A cybersecurity team creates systems and programs to protect data; if these fail, then the computer forensics team recovers the data and performs the investigation into the intrusion and theft. Both areas require knowledge of computer science.

Computer-related crimes

Computer forensics are used to convict those involved in physical and digital crimes. Some of these computer-related crimes include interruption, interception, copyright infringement, and fabrication. Interruption relates to the destruction and stealing of computer parts and digital files. Interception is the unauthorized access of files and information stored on technological devices. Copyright Infringement is using, reproducing, and distributing copyrighted information, including software piracy. Fabrication is accusing someone of using false data and information put in the system through an unauthorized source. Examples of interceptions are the Bank NSP case, Sony.Sambandh.com case, and business email compromise scams.

Use as evidence

In court, computer forensic evidence is subject to the usual requirements for digital evidence. This requires that information be authentic, reliably obtained, and admissible. Different countries have specific guidelines and practices for evidence recovery. In the United Kingdom, examiners often follow Association of Chief Police Officers guidelines that help ensure the authenticity and integrity of evidence. While voluntary, the guidelines are widely accepted in British courts.

Computer forensics has been used as evidence in criminal law since the mid-1980s, some notable examples include:

- **BTK Killer:** Dennis Rader was convicted of a string of serial killings that occurred over a period of sixteen years. Towards the end of this period, Rader sent letters to the police on a floppy disk. Metadata within the documents implicated an author named "Dennis" at "Christ Lutheran Church"; this evidence helped lead to Rader's arrest.
- **Joseph Edward Duncan:** A spreadsheet recovered from Duncan's computer contained evidence that showed him planning his crimes. Prosecutors used this to show premeditation and secure the death penalty.
- **Sharon Lopatka:** Hundreds of emails on Lopatka's computer lead investigators to her killer, Robert Glass.
- **Corcoran Group:** This case confirmed parties' duties to preserve digital evidence when litigation has commenced or is reasonably anticipated. Hard drives were analyzed by a computer forensics expert who could not find relevant emails the Defendants should have had. Though the expert found no evidence of deletion on the hard drives, evidence came out that the defendants were found to have intentionally destroyed emails, and misled and failed to disclose material facts to the plaintiffs and the court.
- **Dr. Conrad Murray:** Dr. Conrad Murray, the doctor of the deceased Michael Jackson, was convicted partially by digital evidence on his computer. This evidence included medical documentation showing lethal amounts of propofol.

Forensic process

Computer forensic investigations usually follow the standard digital forensic process or phases: acquisition, examination, analysis, and reporting. Investigations are performed on static data (i.e. acquired images) rather than "live" systems. This is a change from early forensic practices where a lack of specialist tools led to investigators commonly working on live data.

Forensic process

A digital forensic investigation commonly consists of 3 stages: acquisition or imaging of exhibits, analysis, and reporting. Ideally acquisition involves capturing an image of the computer's volatile memory (RAM) and creating an exact sector level duplicate (or "forensic duplicate") of the media, often using a write blocking device to prevent modification of the original. However, the growth in size of storage media and developments such as cloud computing have led to more use of 'live' acquisitions whereby a 'logical' copy of the data is acquired rather than a complete image of the physical storage device. Both acquired image (or logical copy) and original media/data are hashed (using an algorithm such as SHA-1 or MD5) and the values compared to verify the copy is accurate.

An alternative (and patented) approach (that has been dubbed 'hybrid forensics' or 'distributed forensics') combines digital forensics and ediscovery processes. This approach has been embodied in a commercial tool called ISEEK that was presented together with test results at a conference in 2017.

During the analysis phase an investigator recovers evidence material using a number of different methodologies and tools. In 2002, an article in the International Journal of Digital Evidence referred to this step as "an in-depth systematic search of evidence related to the suspected crime." In 2006, forensics researcher Brian Carrier described an "intuitive procedure" in which obvious evidence is first identified and then "exhaustive searches are conducted to start filling in the holes."

The actual process of analysis can vary between investigations, but common methodologies include conducting keyword searches across the digital media (within files as well as unallocated and slack space), recovering deleted files and extraction of registry information (for example to list user accounts, or attached USB devices).

The evidence recovered is analysed to reconstruct events or actions and to reach conclusions, work that can often be performed by less specialised staff. When an investigation is complete the data is presented, usually in the form of a written report, in lay persons' terms.

Application

Digital forensics is commonly used in both criminal law and private investigation. Traditionally it has been associated with criminal law, where evidence is collected to support or oppose a hypothesis before the courts. As with other areas of forensics this is often a part of a wider investigation spanning a number of disciplines. In some cases, the collected evidence is used as a form of intelligence gathering, used for other purposes than court proceedings (for example to locate, identify or halt other crimes). As a result, intelligence gathering is sometimes held to a less strict forensic standard.

In civil litigation or corporate matters digital forensics forms part of the electronic discovery (or eDiscovery) process. Forensic procedures are similar to those used in criminal investigations, often

with different legal requirements and limitations. Outside of the courts digital forensics can form a part of internal corporate investigations.

A common example might be following unauthorized network intrusion. A specialist forensic examination into the nature and extent of the attack is performed as a damage limitation exercise, both to establish the extent of any intrusion and in an attempt to identify the attacker. Such attacks were commonly conducted over phone lines during the 1980s, but in the modern era are usually propagated over the Internet.

The main focus of digital forensics investigations is to recover objective evidence of a criminal activity (termed *actus reus* in legal parlance). However, the diverse range of data held in digital devices can help with other areas of inquiry.

- **Attribution**
- Meta data and other logs can be used to attribute actions to an individual. For example, personal documents on a computer drive might identify its owner.
- **Alibis and statements**
- Information provided by those involved can be cross checked with digital evidence. For example, during the investigation into the Soham murders the offender's alibi was disproved when mobile phone records of the person he claimed to be with showed she was out of town at the time.
- **Intent**
- As well as finding objective evidence of a crime being committed, investigations can also be used to prove the intent (known by the legal term *mens rea*). For example, the Internet history of convicted killer Neil Entwistle included references to a site discussing How to kill people.
- **Evaluation of source**
- File artifacts and meta-data can be used to identify the origin of a particular piece of data; for example, older versions of Microsoft Word embedded a Global Unique Identifier into files which identified the computer it had been created on. Proving whether a file was produced on the digital device being examined or obtained from elsewhere (e.g., the Internet) can be very important.
- **Document authentication**
- Related to "Evaluation of source," meta data associated with digital documents can be easily modified (for example, by changing the computer clock you can affect the creation date of a file). Document authentication relates to detecting and identifying falsification of such details.

Limitations

One major limitation to a forensic investigation is the use of encryption; this disrupts initial examination where pertinent evidence might be located using keywords. Laws to compel individuals to disclose encryption keys are still relatively new and controversial. but always more frequently there are solutions to brute force passwords or bypass encryption, such as in smartphones or PCs where by means of bootloader techniques the content of the device can be first acquired and later forced in order to find the password or encryption key.

Legal considerations

The examination of digital media is covered by national and international legislation. For civil investigations, in particular, laws may restrict the abilities of analysts to undertake examinations. Restrictions against network monitoring, or reading of personal communications often exist. During criminal investigation, national laws restrict how much information can be seized. For example, in the United Kingdom seizure of evidence by law enforcement is governed by the PACE act. During its existence early in the field, the "International Organization on Computer Evidence" (IOCE) was one agency that worked to establish compatible international standards for the seizure of evidence.

In the UK the same laws covering computer crime can also affect forensic investigators. The 1990 Computer Misuse Act legislates against unauthorised access to computer material; this is a particular concern for civil investigators who have more limitations than law enforcement.

An individual's right to privacy is one area of digital forensics which is still largely undecided by courts. The US Electronic Communications Privacy Act places limitations on the ability of law enforcement or civil investigators to intercept and access evidence. The act makes a distinction between stored communication (e.g. email archives) and transmitted communication (such as VOIP). The latter, being considered more of a privacy invasion, is harder to obtain a warrant for. The ECPA also affects the ability of companies to investigate the computers and communications of their employees, an aspect that is still under debate as to the extent to which a company can perform such monitoring.

Article 5 of the European Convention on Human Rights asserts similar privacy limitations to the ECPA and limits the processing and sharing of personal data both within the EU and with external countries. The ability of UK law enforcement to conduct digital forensics investigations is legislated by the Regulation of Investigatory Powers Act.

Digital evidence

When used in a court of law digital evidence falls under the same legal guidelines as other forms of evidence; courts do not usually require more stringent guidelines. In the United States the Federal Rules of Evidence are used to evaluate the admissibility of digital evidence, the United Kingdom PACE and Civil Evidence acts have similar guidelines and many other countries have their own laws. US federal laws restrict seizures to items with only obvious evidential value. This is acknowledged as not always being possible to establish with digital media prior to an examination.

Laws dealing with digital evidence are concerned with two issues: integrity and authenticity. Integrity is ensuring that the act of seizing and acquiring digital media does not modify the evidence (either the original or the copy). Authenticity refers to the ability to confirm the integrity of information; for example that the imaged media matches the original evidence. The ease with which digital media can be modified means that documenting the chain of custody from the crime scene, through analysis and, ultimately, to the court, (a form of audit trail) is important to establish the authenticity of evidence.

Attorneys have argued that because digital evidence can theoretically be altered it undermines the reliability of the evidence. US judges are beginning to reject this theory, in the case US v. Bonallo the court ruled that "the fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness." In the United Kingdom guidelines such as those issued by ACPO are followed to help document the authenticity and integrity of evidence.

Digital investigators, particularly in criminal investigations, have to ensure that conclusions are based upon factual evidence and their own expert knowledge. In the US, for example, Federal Rules of Evidence state that a qualified expert may testify "in the form of an opinion or otherwise" so long as:

- (1) the testimony is based upon sufficient facts or data,
- (2) the testimony is the product of reliable principles and methods, and
- (3) the witness has applied the principles and methods reliably to the facts of the case.

The sub-branches of digital forensics may each have their own specific guidelines for the conduct of investigations and the handling of evidence. For example, mobile phones may be required to be placed in a Faraday shield during seizure or acquisition to prevent further radio traffic to the device. In the UK forensic examination of computers in criminal matters is subject to ACPO guidelines. There are also international approaches to providing guidance on how to handle electronic evidence. The "Electronic Evidence Guide" by the Council of Europe offers a framework for law enforcement and judicial authorities in countries who seek to set up or enhance their own guidelines for the identification and handling of electronic evidence.

Investigative tools

The admissibility of digital evidence relies on the tools used to extract it. In the US, forensic tools are subjected to the Daubert standard, where the judge is responsible for ensuring that the processes and software used were acceptable. In a 2003 paper Brian Carrier argued that the Daubert guidelines required the code of forensic tools to be published and peer reviewed. He concluded that "open source tools may more clearly and comprehensively meet the guideline requirements than would closed source tools." In 2011 Josh Brunty stated that the scientific validation of the technology and software associated with performing a digital forensic examination is critical to any laboratory process. He argued that "the science of digital forensics is founded on the principles of repeatable processes and quality evidence therefore knowing how to design and properly maintain a good validation process is a key requirement for any digital forensic examiner to defend their methods in court." "

Computer forensics lab

The computer forensic lab is a safe and protected zone where electronic data can be managed, preserved, and accessed in a controlled environment. There, there is a very much reduced risk of damage or modification to the evidence. Computer forensic examiners have the resources needed to elicit meaningful data from the devices that they are examining.

Techniques

A number of techniques are used during computer forensics investigations, and these include the following:

- Cross-drive analysis

- This is a forensic technique that correlates information found on multiple hard drives, and has been used to identify social networks and perform anomaly detection.
- Live analysis
 - The examination of computers from within the operating system using custom forensics or existing sysadmin tools to extract evidence. The practice is useful when dealing with Encrypting File Systems, for example, where the encryption keys may be collected and, in some instances, the logical hard drive volume may be imaged (known as a live acquisition) before the computer is shut down.
- Deleted files
 - A common technique used in computer forensics is the recovery of deleted files. Modern forensic software have their own tools for recovering or carving out deleted data. Most operating systems and file systems do not always erase physical file data, allowing investigators to reconstruct it from the physical disk sectors. File carving involves searching for known file headers within the disk image and reconstructing deleted materials.
- Stochastic forensics
 - A method which uses stochastic properties of the computer system to investigate activities lacking digital artifacts. Its chief use is to investigate data theft.
- Steganography
 - One of the techniques used to hide data is via steganography, the process of hiding data inside of a picture or digital image. An example would be to hide pornographic images of children or other information that a given criminal does not want to have discovered. Computer forensics professionals can fight this by looking at the hash of the file and comparing it to the original image (if available.) While the images appear identical upon visual inspection, the hash changes as the data changes.

Mobile device forensics

- **Phone Logs:** Phone companies usually keep logs of calls received, which can be helpful when creating timelines and gathering the locations of persons when the crime occurred.
- **Contacts:** Contact lists help narrow down the suspect pool due to their connections with the victim or suspect.
- **Text messages:** Messages contain timestamps and remain in company servers indefinitely, even if deleted on the original device. Because of this, messages act as crucial records of communication that can be used to convict suspects.
- **Photos:** Photos can be critical in either supporting or disproving alibis by displaying a location or scene along with a timestamp of when the photo was taken.
- **Audio Recordings:** Some victims might have been able to record pivotal moments of the struggle, like the voice of their attacker or extensive context of the situation.

Branches

Digital forensics investigation is not restricted to retrieve data merely from the computer, as laws are breached by the criminals and small digital devices (e.g. tablets, smartphones, flash drives) are now extensively used. Some of these devices have volatile memory while some have non-volatile memory.

Sufficient methodologies are available to retrieve data from volatile memory, however, there is lack of detailed methodology or a framework for data retrieval from non-volatile memory sources. Depending on the type of devices, media or artifacts, digital forensics investigation is branched into various types.

- **Computer forensics**

- The goal of computer forensics is to explain the current state of a digital artifact; such as a computer system, storage medium or electronic document. The discipline usually covers computers, embedded systems (digital devices with rudimentary computing power and onboard memory) and static memory (such as USB pen drives).
- Computer forensics can deal with a broad range of information; from logs (such as internet history) through to the actual files on the drive. In 2007 prosecutors used a spreadsheet recovered from the computer of Joseph Edward Duncan to show premeditation and secure the death penalty. Sharon Lopatka's killer was identified in 2006 after email messages from him detailing torture and death fantasies were found on her computer.

- **Mobile device forensics**

- Mobile device forensics is a sub-branch of digital forensics relating to recovery of digital evidence or data from a mobile device. It differs from Computer forensics in that a mobile device will have an inbuilt communication system (e.g. GSM) and, usually, proprietary storage mechanisms. Investigations usually focus on simple data such as call data and communications (SMS/Email) rather than in-depth recovery of deleted data. SMS data from a mobile device investigation helped to exonerate Patrick Lumumba in the murder of Meredith Kercher.
- Mobile devices are also useful for providing location information; either from inbuilt gps/location tracking or via cell site logs, which track the devices within their range. Such information was used to track down the kidnappers of Thomas Onofri in 2006.

- **Network forensics**

- Network forensics is concerned with the monitoring and analysis of computer network traffic, both local and WAN/internet, for the purposes of information gathering, evidence collection, or intrusion detection. Traffic is usually intercepted at the packet level, and either stored for later analysis or filtered in real-time. Unlike other areas of digital forensics network data is often volatile and rarely logged, making the discipline often reactionary.
- In 2000 the FBI lured computer hackers Aleksey Ivanov and Gorshkov to the United States for a fake job interview. By monitoring network traffic from the pair's computers, the FBI identified passwords allowing them to collect evidence directly from Russian-based computers.

- **Forensic data analysis**

- Forensic Data Analysis is a branch of digital forensics. It examines structured data with the aim to discover and analyze patterns of fraudulent activities resulting from financial crime.

- **Digital image forensics**
- Digital image forensics (or forensic image analysis) is a branch of digital forensics that deals with examination and verification of an image's authenticity and content. These can range from Stalin-era airbrushed photos to elaborate deepfake videos. This has broad implications for a wide variety of crimes, for determining the validity of information presented in civil and criminal trials, and for verifying images and information that are circulated through news and social media.
- **Database forensics**
- Database forensics is a branch of digital forensics relating to the forensic study of databases and their metadata. Investigations use database contents, log files and in-RAM data to build a timeline or recover relevant information.
- **IoT Forensics**
- IoT forensics is a branch of Digital forensics that has the goal of identifying and extracting digital information from devices belonging to the Internet of things field, to be used for forensics investigations as potential source of evidence.

Volatile data

Volatile data is any data that is stored in memory, or exists in transit, that will be lost when the computer loses power or is turned off. Volatile data resides in registries, cache, and random access memory (RAM). The investigation of this volatile data is called "live forensics".

When seizing evidence, if the machine is still active, any information stored solely in RAM that is not recovered before powering down may be lost. One application of "live analysis" is to recover RAM data (for example, using Microsoft's COFEE tool, WinDD, WindowsSCOPE) prior to removing an exhibit. CaptureGUARD Gateway bypasses Windows login for locked computers, allowing for the analysis and acquisition of physical memory on a locked computer.

RAM can be analyzed for prior content after power loss, because the electrical charge stored in the memory cells takes time to dissipate, an effect exploited by the cold boot attack. The length of time that data is recoverable is increased by low temperatures and higher cell voltages. Holding unpowered RAM below -60 °C helps preserve residual data by an order of magnitude, improving the chances of successful recovery. However, it can be impractical to do this during a field examination.

Some of the tools needed to extract volatile data, however, require that a computer be in a forensic lab, both to maintain a legitimate chain of evidence, and to facilitate work on the machine. If necessary, law enforcement applies techniques to move a live, running desktop computer. These include a mouse jigglers, which moves the mouse rapidly in small movements and prevents the computer from going to sleep accidentally. Usually, an uninterruptible power supply (UPS) provides power during transit.

However, one of the easiest ways to capture data is by actually saving the RAM data to disk. Various file systems that have journaling features such as NTFS and ReiserFS keep a large portion of the RAM

data on the main storage media during operation, and these page files can be reassembled to reconstruct what was in RAM at that time.

Analysis tools

A number of open source and commercial tools exist for computer forensics investigation. Typical forensic analysis includes a manual review of material on the media, reviewing the Windows registry for suspect information, discovering and cracking passwords, keyword searches for topics related to the crime, and extracting e-mail and pictures for review. Autopsy (software), Belkasoft Evidence Center, COFEE, EnCase are the some of tools used in Digital forensics.

Jobs in computer forensics

Digital forensics analyst

A digital forensics analyst is responsible for preserving digital evidence, cataloging collected evidence, analyzing evidence in a manner relevant to the ongoing case, responding to cyber breaches (usually in a corporate context), writing reports containing findings, and testifying in court. A digital forensic analyst may alternatively be referred to as a computer forensic analyst, digital forensic examiner, cyber forensic analyst, forensic technician, or other similarly named titles, although these roles perform the same duties.

Certifications

There are several computer forensics certifications available, such as the ISFCE Certified Computer Examiner, Digital Forensics Investigation Professional (DFIP) and IACRB Certified Computer Forensics Examiner.

The top vendor independent certification (especially within EU) is considered the CCFP - Certified Cyber Forensics Professional.

Others, worth to mention for USA or APAC are: The International Association of Computer Investigative Specialists offers the Certified Computer Examiner program.

The International Society of Forensic Computer Examiners offers the Certified Computer Examiner program.

Many commercial based forensic software companies are now also offering proprietary certifications on their products. For example, Guidance Software offering the (EnCE) certification on their tool EnCase, AccessData offering (ACE) certification on their tool FTK, PassMark Software offering certification on their tool OSForensics, and X-Ways Software Technology offering (X-PERT) certification for their software, X-Ways Forensics.

Anti-computer forensics

Anti-computer forensics or counter-forensics are techniques used to obstruct forensic analysis.

Definition

Anti-forensics has only recently been recognized as a legitimate field of study.

One of the more widely known and accepted definitions comes from Marc Rogers of One of the earliest detailed presentations of anti-forensics, in Phrack Magazine in 2002, defines anti-forensics as "the removal, or hiding, of evidence in an attempt to mitigate the effectiveness of a forensics investigation".

A more abbreviated definition is given by Scott Berinato in his article entitled, The Rise of Anti-Forensics. "Anti-forensics is more than technology. It is an approach to criminal hacking that can be summed up like this: Make it hard for them to find you and impossible for them to prove they found you." Neither author takes into account using anti-forensics methods to ensure the privacy of one's personal data.

Sub-categories

Anti-forensics methods are often broken down into several sub-categories to make classification of the various tools and techniques simpler. One of the more widely accepted subcategory breakdowns was developed by Dr. Marcus Rogers. He has proposed the following sub-categories: data hiding, artifact wiping, trail obfuscation and attacks against the CF (computer forensics) processes and tools. Attacks against forensics tools directly has also been called counter-forensics.

Purpose and goals

Within the field of digital forensics there is much debate over the purpose and goals of anti-forensic methods. The conventional wisdom is that anti-forensic tools are purely malicious in intent and design. Others believe that these tools should be used to illustrate deficiencies in digital forensic procedures, digital forensic tools, and forensic examiner education. This sentiment was echoed at the 2005 Blackhat Conference by anti-forensic tool authors, James Foster and Vinnie Liu. They stated that by exposing these issues, forensic investigators will have to work harder to prove that collected evidence is both accurate and dependable. They believe that this will result in better tools and education for the forensic examiner. Also, counter-forensics has significance for defence against espionage, as recovering information by forensic tools serves the goals of spies equally as well as investigators.

Data hiding

Data hiding is the process of making data difficult to find while also keeping it accessible for future use. "Obfuscation and encryption of data give an adversary the ability to limit identification and collection of evidence by investigators while allowing access and use to themselves."

Some of the more common forms of data hiding include encryption, steganography and other various forms of hardware/software based data concealment. Each of the different data hiding methods makes digital forensic examinations difficult. When the different data hiding methods are combined, they can make a successful forensic investigation nearly impossible.

Encryption

One of the more commonly used techniques to defeat computer forensics is data encryption. In a presentation given on encryption and anti-forensic methodologies, the Vice President of Secure Computing, Paul Henry, referred to encryption as a "forensic expert's nightmare".

The majority of publicly available encryption programs allow the user to create virtual encrypted disks which can only be opened with a designated key. Through the use of modern encryption algorithms and various encryption techniques these programs make the data virtually impossible to read without the designated key.

File level encryption encrypts only the file contents. This leaves important information such as file name, size and timestamps unencrypted. Parts of the content of the file can be reconstructed from other locations, such as temporary files, swap file and deleted, unencrypted copies.

Most encryption programs have the ability to perform a number of additional functions that make digital forensic efforts increasingly difficult. Some of these functions include the use of a keyfile, full-volume encryption, and plausible deniability. The widespread availability of software containing these functions has put the field of digital forensics at a great disadvantage.

Steganography

Steganography is a technique where information or files are hidden within another file in an attempt to hide data by leaving it in plain sight. "Steganography produces dark data that is typically buried within light data (e.g., a non-perceptible digital watermark buried within a digital photograph)." While some experts have argued that the use of steganography techniques is not very widespread and therefore the subject shouldn't be given a lot of thought, most experts agree that steganography has the capability of disrupting the forensic process when used correctly.

According to Jeffrey Carr, a 2007 edition of Technical Mujahid (a bi-monthly terrorist publication) outlined the importance of using a steganography program called Secrets of the Mujahideen. According to Carr, the program was touted as giving the user the capability to avoid detection by current steganalysis programs. It did this through the use of steganography in conjunction with file compression.

Other forms of data hiding

Other forms of data hiding involve the use of tools and techniques to hide data throughout various locations in a computer system. Some of these places can include "memory, slack space, hidden directories, bad blocks, alternate data streams, (and) hidden partitions."

One of the more well known tools that is often used for data hiding is called Slacker (part of the Metasploit framework). Slacker breaks up a file and places each piece of that file into the slack space of other files, thereby hiding it from the forensic examination software. Another data hiding technique involves the use of bad sectors. To perform this technique, the user changes a particular sector from good to bad and then data is placed onto that particular cluster. The belief is that forensic examination tools will see these clusters as bad and continue on without any examination of their contents.

Artifact wiping

The methods used in artifact wiping are tasked with permanently eliminating particular files or entire file systems. This can be accomplished through the use of a variety of methods that include disk cleaning utilities, file wiping utilities and disk degaussing/destruction techniques.

Disk cleaning utilities

Disk cleaning utilities use a variety of methods to overwrite the existing data on disks. The effectiveness of disk cleaning utilities as anti-forensic tools is often challenged as some believe they are not completely effective. Experts who don't believe that disk cleaning utilities are acceptable for disk sanitization base their opinions of current DOD policy, which states that the only acceptable form of sanitization is degaussing. Disk cleaning utilities are also criticized because they leave signatures that the file system was wiped, which in some cases is unacceptable. Some of the widely used disk cleaning utilities include DBAN, srm, BCWipe Total WipeOut, KillDisk, PC Inspector and CyberScrubs cyberCide. Another option which is approved by the NIST and the NSA is CMRR Secure Erase, which uses the Secure Erase command built into the ATA specification.

File wiping utilities

File wiping utilities are used to delete individual files from an operating system. The advantage of file wiping utilities is that they can accomplish their task in a relatively short amount of time as opposed to disk cleaning utilities which take much longer. Another advantage of file wiping utilities is that they generally leave a much smaller signature than disk cleaning utilities. There are two primary disadvantages of file wiping utilities, first they require user involvement in the process and second some experts believe that file wiping programs don't always correctly and completely wipe file information. Some of the widely used file wiping utilities include BCWipe, R-Wipe & Clean, Eraser, Aevita Wipe & Delete and CyberScrubs PrivacySuite. On Linux tools like shred and srm can be also used to wipe single files. SSDs are by design more difficult to wipe, since the firmware can write to other cells therefore allowing data recovery. In these instances ATA Secure Erase should be used on the whole drive, with tools like hdparm that support it.

Disk degaussing / destruction techniques

Disk degaussing is a process by which a magnetic field is applied to a digital media device. The result is a device that is entirely clean of any previously stored data. Degaussing is rarely used as an anti-forensic method despite the fact that it is an effective means to ensure data has been wiped. This is attributed to the high cost of degaussing machines, which are difficult for the average consumer to afford.

A more commonly used technique to ensure data wiping is the physical destruction of the device. The NIST recommends that "physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverizing, shredding and melting."

Trail obfuscation

The purpose of trail obfuscation is to confuse, disorient, and divert the forensic examination process. Trail obfuscation covers a variety of techniques and tools that include "log cleaners, spoofing, misinformation, backbone hopping, zombied accounts, trojan commands."

One of the more widely known trail obfuscation tools is Timestomp (part of the Metasploit Framework). Timestomp gives the user the ability to modify file metadata pertaining to access, creation and modification times/dates. By using programs such as Timestomp, a user can render any number of files useless in a legal setting by directly calling into question the files' credibility.

Another well known trail-obfuscation program is Transmogrify (also part of the Metasploit Framework). In most file types the header of the file contains identifying information. A (.jpg) would have header information that identifies it as a (.jpg), a (.doc) would have information that identifies it as (.doc) and so on. Transmogrify allows the user to change the header information of a file, so a (.jpg) header could be changed to a (.doc) header. If a forensic examination program or operating system were to conduct a search for images on a machine, it would simply see a (.doc) file and skip over it.

Attacks against computer forensics

In the past anti-forensic tools have focused on attacking the forensic process by destroying data, hiding data, or altering data usage information. Anti-forensics has recently moved into a new realm where tools and techniques are focused on attacking forensic tools that perform the examinations. These new anti-forensic methods have benefited from a number of factors to include well documented forensic examination procedures, widely known forensic tool vulnerabilities, and digital forensic examiners' heavy reliance on their tools.

During a typical forensic examination, the examiner would create an image of the computer's disks. This keeps the original computer (evidence) from being tainted by forensic tools. Hashes are created by the forensic examination software to verify the integrity of the image. One of the recent anti-tool techniques targets the integrity of the hash that is created to verify the image. By affecting the integrity of the hash, any evidence that is collected during the subsequent investigation can be challenged.

Physical

To prevent physical access to data while the computer is powered on (from a grab-and-go theft for instance, as well as seizure from Law Enforcement), there are different solutions that could be implemented:

- Software frameworks like USBGuard or USBKill implements USB authorization policies and method of use policies. If the software is triggered, by insertion or removal of USB devices, a specific action can be performed. After the arrest of Silk Road's administrator Ross Ulbricht, a number of proof of concept anti-forensic tools have been created to detect seizing of the computer from the owner to shut it down, therefore making the data inaccessible if full disk encryption is used.
- Hardware cable anchors using the Kensington Security Slot to prevent stealing by opportunistic thieves.
- Hardware kill cables like BusKill that lock, shutdown, or wipe data when ejected

- Use of chassis intrusion detection feature in computer case or a sensor (such as a photodetector) rigged with explosives for self-destruction. In some jurisdictions this method could be illegal since it could seriously maim or kill an unauthorized user and could consist in destruction of evidence.
- Battery could be removed from a laptop to make it work only while attached to the power supply unit. If the cable is removed, shutdown of the computer will occur immediately causing data loss. In the event of a power surge the same will occur though.

Some of these methods rely on shutting the computer down, while the data might be retained in the RAM from a couple of seconds up to a couple minutes, theoretically allowing for a cold boot attack. Cryogenically freezing the RAM might extend this time even further and some attacks on the wild have been spotted. Methods to counteract this attack exist and can overwrite the memory before shutting down. Some anti-forensic tools even detect the temperature of the RAM to perform a shutdown when below a certain threshold.

Attempts to create a tamper-resistant desktop computer has been made (as of 2020, the ORWL model is one of the best examples). However, security of this particular model is debated by security researcher and Qubes OS founder Joanna Rutkowska.

Use by criminals

While the study and applications of anti-forensics are generally available to protect users from forensic attacks of their confidential data by their adversaries (eg investigative journalists, human rights defenders, activists, corporate or government espionage), Mac Rogers of Purdue University notes that anti-forensics tools can also be used by criminals.

Rogers uses a more traditional "crime scene" approach when defining anti-forensics. "Attempts to negatively affect the existence, amount and/or quality of evidence from a crime scene, or make the analysis and examination of evidence difficult or impossible to conduct."

Effectiveness of anti-forensics

Anti-forensic methods rely on several weaknesses in the forensic process including: the human element, dependency on tools, and the physical/logical limitations of computers. By reducing the forensic process's susceptibility to these weaknesses, an examiner can reduce the likelihood of anti-forensic methods successfully impacting an investigation. This may be accomplished by providing increased training for investigators, and corroborating results using multiple tools.



FTPS (File Transfer Protocol Secure)

Ensuring Secure and Reliable File Transfers

Introduction to FTPS

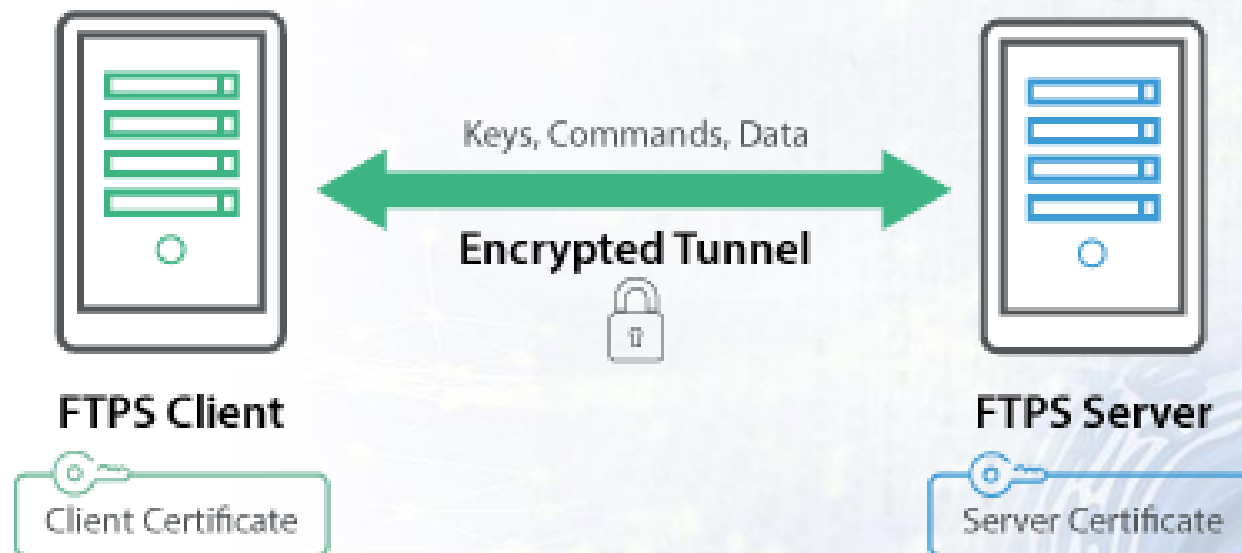
- FTPS is a secure file transfer protocol that combines the traditional FTP protocol with the security features of SSL/TLS encryption.
- It provides a secure and reliable method for transferring files over a network, ensuring data integrity and confidentiality.
- FTPS is widely used in various industries, including banking, healthcare, and e-commerce, where secure file transfers are crucial.



How FTPS Works?

- FTPS utilizes SSL/TLS encryption to secure the communication between the client and the server.
- SSL/TLS establishes a secure and encrypted connection, preventing unauthorized access and eavesdropping.
- FTPS supports both implicit and explicit modes, offering flexibility in choosing the level of security required.

FTPS working



Key Features of FTPS

- **Encryption:** FTPS uses SSL/TLS encryption to protect data during transit, safeguarding it from interception and tampering.
- **Authentication:** FTPS provides strong authentication mechanisms, ensuring that only authorized users can access and transfer files.
- **Data Integrity:** Through SSL/TLS, FTPS guarantees the integrity of transferred files, detecting any unauthorized modifications.
- **Portability:** FTPS is supported by various operating systems and FTP client software, making it widely compatible and accessible.

Benefits of Using FTPS

Enhanced Security: FTPS offers a higher level of security compared to standard FTP, making it suitable for sensitive data transfers.

Compliance with Regulations: FTPS helps organizations meet regulatory requirements for data protection, such as HIPAA and GDPR.

Reliability: FTPS ensures the reliable delivery of files, minimizing errors and interruptions during transfers.

Flexibility: With implicit and explicit modes, FTPS allows organizations to choose the level of security that best suits their needs.