Forensics
Week 2 – Intro to Digital Forensics

Date: 26th September 2025

Course Code: TU856 / TU857 / TU858 yr 4.

TU Dublin – Grangegorman Campus

School of Computer Science

Seoladh Cláraithe / Registered Address
OT Baile Átha Cliath - Teach na Páirce Ghráinseach Ghormáin
191 An Cuarbhóthar Thuaidh, D07 EWV4, Éire

TU Dublin - Park House Grangegorman
191 North Circular Road, D07 EWV4, Ireland

OT Baile Átha Cliath
Gráinseach Ghormáin
D07 H6K8, Éire

TU Dublin
Grangegorman
D07 H6K8, Ireland

~ +353 1 220500
~ tudublin.ie

Overview

- What is a digital forensics?
- Forensic examination
- Anatomy of an investigation
- Digital Forensic Models
- Chain of Custody
- Incidents and Hacking

Slides Created: 15th June 2022
Slides updated: 29th August 2025

Introduction

- In this module we will look at what computer forensics is and what can be achieved.
- A variety of freely available tools will be used for our practical examples (as proprietary tools can be very expensive – but very feature rich and fit for purpose)
- We can’t cover every type of case. The focus is to show how to implement a forensically sound process to examine digital evidence using forensic tools.

What is Digital Forensics?

- Digital forensics is analysis of digital devices to determine what has happened.
- This could be to determine if a crime has been committed. There are different types of infractions, this could be a civil matter or breach of company policy etc.
- Definition:
  - Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation and maintain a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it. (Source: TechTarget: https://www.techtarget.com/searchsecurity/definition/computer-forensics)

Forensic Examinations

- Digital forensics is the practice of collecting, analyzing and reporting on digital data.
- There is usually a specific need for the investigation, ie. Has a particular event occurred?
- Usually a forensic examiner is tasked with performing an examination, the outcome of the investigation needs to be reported back.

- Question: what could be examples of what could be investigated?

Forensic Examinations

- Collecting
  - This is the process of collecting the digital evidence
  - This can be the specific sourcing of a device for examination
  - Data needs to be collected in a forensically sound matter and the order of volatility needs to be carefully considered.
- Analysing
  - This phase is looking at discovering what has happened or what task was performed using a digital device. This is looking to fully understand the transgression and the timeline of the events. The how/when things happened.

Forensic Examinations

- Reporting
  - Creating a document to report our findings to the third party who requested the investigation.
  - This will offer answers to the reason why the third party wanted the investigation.
  - The report needs to be very specific with the process followed.
  - It is important that the conclusions drawn are supported by the results from the investigative process followed.

Forensic Examinations

Questions / Discussion (in-class)

- What are the consequences of not following the collecting, analyzing and reporting on digital data?

- What do we need to know before starting the collecting, analyzing and reporting phase?

OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH
TU DUBLIN
TECHNOLOGICAL UNIVERSITY DUBLIN

The Anatomy of a Digital Investigation

Sources of Digital Evidence

- ***Open computer systems***: Open computer systems are what most people think of as computers—systems comprised of hard drives, keyboards, and monitors such as laptops, desktops, and servers that obey standards.
- These systems, with their ever increasing amounts of storage space, can be rich sources of digital evidence.
- A simple file can contain incriminating information and can have associated properties that are useful in an investigation.
- For example, details such as when a it was created, who likely created it, or that it was created on another computer can all be important.

Sources of Digital Evidence

Computer Systems

- Hard drives, SSDs, removable media (USB, CDs, DVDs).
- Operating system artifacts (Windows Registry, system logs, event logs).
- Application data (email clients, word processors, browsers).

Examples

A company suspects an employee of stealing confidential design files and sending them to a competitor. Investigators seize the employee's workstation for analysis.

Evidence Found on the Computer System

Hard Drive (Primary Storage):

- Recovered deleted CAD files using file carving.
- Located compressed .zip archives with sensitive documents.

Operating System Artifacts:

- Windows Event Logs showed multiple USB device connections late at night.
- Recent files list confirmed access to confidential project folders.

Application Data:

- Email client (Outlook/Thunderbird) contained draft emails with attachments to an external address.
- Browser history showed visits to a competitor's employee portal.

Sources of Digital Evidence

Mobile Devices

- Smartphones and tablets.
- Call logs, SMS/MMS, contacts.
- App data (WhatsApp, Telegram, Signal, etc.).
- GPS and location history.
- Photos, videos, audio recordings.

Examples

Police are investigating a drug trafficking case. A suspect's smartphone is seized during an arrest.

Evidence Found on the Mobile Device

Call Logs & Contacts

- Recovered call history showing frequent late-night calls to a known dealer.
- Contacts list contained aliases matching code names from surveillance.

Messaging Apps

- WhatsApp chats revealed discussions about "deliveries" with timestamps matching observed movements.
- Deleted Telegram messages were partially recovered from the device's database files.

Location Data

- GPS history showed repeated visits to a warehouse used as a stash location.
- Google Maps "Timeline" confirmed travel routes consistent with drug drop-offs.

Multimedia Evidence

- Photos of packaged substances stored in the gallery.
- A voice memo discussing transaction amounts.

Sources of Digital Evidence

Network Sources

- Network logs (routers, firewalls, intrusion detection/prevention systems).
- Server logs (web servers, DNS, email servers).
- Packet captures (PCAPs) from monitoring tools like Wireshark.
- Cloud services (Google Drive, iCloud, Dropbox).

Examples

A financial institution reports a suspected cyber intrusion where attackers may have accessed customer data. Forensic investigators analyze the organization's network logs.

Evidence Found in Network Sources

Firewall Logs

- Detected multiple failed login attempts from foreign IPs, followed by a successful login at 3:12 AM.

Intrusion Detection System (IDS) Alerts

- Flagged abnormal outbound traffic patterns — large encrypted data transfers to an unknown server.

Web Server Logs

- Showed exploitation of a vulnerable login form (SQL injection attack).
- Logs included attacker's IP address and request payloads.

Packet Capture (PCAP)

Analysis of packet data revealed exfiltration of customer records (names, account numbers).

Sources of Digital Evidence

Internet & Online Services

- Social media platforms (Facebook, Instagram, Twitter/X, TikTok).
- Messaging services (Slack, Discord, Teams).
- Forums, blogs, websites.
- Cloud-hosted virtual machines or SaaS platforms.

Example

Investigators are looking into an online harassment case where a victim reported receiving threatening messages on Twitter/X and Discord.

Evidence Found Online

Social Media (Twitter/X)

- Threatening posts traced back to an account using a pseudonym.
- Metadata analysis (IP logs from Twitter) showed login locations matching the suspect's home Wi-Fi.

Messaging Service (Discord)

- Private chat logs revealed the suspect coordinating with others about targeted harassment.
- Deleted messages were recovered from Discord's database export, provided via legal request.

Cloud Storage (Google Drive)

- Investigators found stored documents containing screenshots of planned attacks and doxxing material.
- File timestamps confirmed they were created on the suspect's Google account.

Sources of Digital Evidence

Removable & External Devices

- USB drives, SD cards, external HDDs/SSDs.
- IoT devices (smart TVs, smart speakers, wearables like Fitbit/Apple Watch).
- Vehicle infotainment systems (GPS routes, Bluetooth logs).

Example

During a corporate fraud investigation, forensic analysts search an employee's office and find a USB flash drive hidden in a drawer.

Evidence Found on the Device

File Storage

- Contained encrypted spreadsheets with detailed records of unauthorized financial transfers.
- File names matched projects the employee had access to internally.

Timestamps

- Metadata showed the files were last modified outside of office hours.
- "Date accessed" entries matched days when suspicious transactions occurred.

Deleted Data

- Forensic carving recovered deleted PDFs with company bank account details.

Connection History

- Windows registry on the suspect's workstation confirmed the same USB drive was plugged into their computer multiple times.

Sources of Digital Evidence

Peripheral Devices

- Printers (spool files, cached documents).
- Scanners, copiers (stored images).
- Surveillance cameras/DVRs.

Example

A law enforcement team is investigating an intellectual property theft case. The suspect works in a design firm and frequently prints confidential blueprints.

Evidence Found on Peripheral Devices

Printers & Copiers

- Analysis of the printer's internal storage (spool files and logs) revealed copies of sensitive blueprints.
- Metadata in the print job showed the username of the suspect's workstation and timestamps.

Scanners

- Scanned PDFs stored on a shared network scanner contained confidential documents.
- Logs showed the scanner was accessed at odd hours when office staff were absent.

Other Peripherals (e.g., Smart Cameras, USB Devices)

- Surveillance cameras confirmed the suspect accessing restricted areas.
- A connected USB drive to the copier contained drafts of sensitive design files.

Practitioners Tip

- System administrators who find child pornography on computers in their workplace are in a perilous position.
- Simply deleting the contraband material and not reporting the problem may be viewed as criminally negligent.
- A system administrator who did not muster his employer's support before calling the police to report child pornography placed on a server by another employee was disavowed by his employer, had to hire his own lawyer, testify on his own time, and ultimately find a new job.
- Well-meaning attempts to investigate child pornography complaints have resulted in the system administrator being prosecuted for downloading and possessing illegal materials themselves.
- Therefore, in addition to being technically prepared for such incidents, it is important for organizations and system administrators to have clear policies and procedures for responding to these problems

Principles of Digital Forensics

- Forensic Science provides a large body of proven investigative techniques and methods for achieving the ends that are referenced extensively in this text.
- By *forensic* we mean a characteristic of evidence that satisfies its suitability for admission as fact and its ability to persuade based upon proof (or high statistical confidence).

Evidence Exchange

- The main goals in any investigation are to follow the trails that offenders leave during the commission of a crime and to tie perpetrators to the victims and crime scenes.
- Although witnesses may identify a suspect, tangible evidence of an individual's involvement is usually more compelling and reliable.
- Forensic analysts are employed to uncover compelling links between the offender, victim, and crime scene.
- According to **Locard's Exchange Principle**, contact between two items will result in an exchange.
- This principle applies to any contact at a crime scene, including between an offender and victim, between a person with a weapon, and between people and the crime scene itself.
- There will always be evidence of the interaction, although in some cases it may not be detected easily (note that absence of evidence is not evidence of absence).
- This transfer occurs in both the physical and digital realms and can provide links between them

Evidence Exchange (example)

- In computer intrusions, the attackers will leave multiple traces of their presence throughout the environment, including in the le systems, registry, system logs, and network-level logs.
- Furthermore, the attackers could transfer elements of the crime scene back with them, such as stolen user passwords or in a file or database. Such evidence can be useful to link an individual to an intrusion.
- In an e-mail harassment case, the act of sending threatening messages via a Web-based e-mail service such as Hotmail can leave a number of traces. The Web browser used to send messages will store les, links, and other information on the sender's hard drive along with date-time related information.
- Forensic analysts may find an abundance of information relating to the sent message on the offender's hard drive, including the original message contents.
- Additionally, investigators may be able to obtain related information from Hotmail, including Web server access logs, IP addresses, and possibly the entire message in the sent mail folder of the offender's e-mail account.

Evidence Characteristics

- The exchanges that occur between individual and crime scene produce trace evidence belonging to one of two general categories: (i) evidence with attributes that fit in the group called *class characteristics* and (ii) evidence with attributes that fall in the category called *individual characteristics*.
- Class characteristics are common traits in similar items whereas individual characteristics are more unique and can be linked to a specific person or activity with greater certainty.
- Consider the physical world example of a shoe print left under a window at a crime scene.
- Forensic analysis of those impressions might only reveal the make and model of the shoe, placing it in the class of all shoes of the same make and model.
- If a suspect was found to be in possession of a pair of the same make and model, a tenuous circumstantial link can be made between the suspect and the wrongdoing. If forensic analysis uncovers detailed wear patterns in the shoe prints and finds identical wear of the suspect's soles, a much stronger link is possible.
- The margin of error is significantly reduced by the discovery of an individual characteristic, making the link much less circumstantial and harder to refute

Forensics Soundness

- In order to be useful in an investigation, digital evidence must be preserved and examined in a forensically sound manner.
- Some practitioners of digital forensics think that a method of preserving or examining digital evidence is only forensically sound if it does not alter the original evidence source in any way. This is simply not true. Traditional forensic disciplines such as DNA analysis show that the measure of forensic soundness does not require the original to be left unaltered.
- When samples of biological material are collected, the process generally scrapes or smears the original evidence.
- Forensic analysis of the evidential sample further alters the sample because DNA tests are destructive. Despite the changes that occur during preservation and processing, these methods are considered forensically sound and DNA evidence is regularly admitted as evidence.

Forensics Soundness (example)

- In digital forensics, the routine task of acquiring data from a hard drive, even when using a hardware write-blocker, alters the original state of the hard drive.
- Such alterations can include making a hidden area of the hard drive accessible, or updating information maintained by Self-Monitoring, Analysis, and Reporting Technology (S.M.A.R.T.) on modern hard drives.
- Furthermore, most methods of acquiring the contents of memory on live computer systems and mobile devices alter or overwrite portions of memory, but this is a generally accepted practice in digital forensics.
- In fact, courts are starting to compel preservation of volatile computer data in some cases, which requires digital investigators to preserve data on live systems.
- In Columbia Pictures Indus. v. Bunnell, for example, the court held that random access memory (RAM) on a Web server could contain relevant log data and was therefore within the scope of discoverable information in this case.

Types of Investigation

- Criminal
  - Government agency is the plaintiff
  - Accused is the defendant
- Civil
  - A dispute between two entities (public or private)
  - Either side can be the plaintiff or defendant

More Investigation Types

- Internal
  - An inquiry held within the confines of an organization (civil or federal) that is not meant for public review
  - May or may not be civil or criminal, but assume it could

Frameworks / Models

The following models will be discussed:

- DFRWS Digital Forensics Model: Evidence Handling Framework
- The Basic Model (Kruse and Heiser)
- The Casey Model

DFRWS Digital Forensics Model: Evidence Handling Framework

OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH
TU DUBLIN
TECHNOLOGICAL UNIVERSITY DUBLIN

Origin & Definition

The DFRWS model, introduced in 2001 by Gary Palmer at the inaugural DFRWS, provides a structured, technology-neutral process for digital forensic investigations. It outlines seven core phases:

- Identification
- Preservation
- Collection
- Examination
- Analysis
- Presentation
- Decision

Source: https://dfrws.org/wp-content/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research.pdf

DFRWS phases

- **Identification** – Recognizing potential digital evidence (e.g., cases, anomalies, system artifacts).
- **Preservation** – Safeguarding integrity via imaging, chain-of-custody, timestamp synchronization.
- **Collection** – Acquiring evidence using approved methods and tools, and ensuring legal authority.
- **Examination** – Applying pattern matching, hidden-data recovery, validation, and filtering techniques.
- **Analysis** – Interpreting the extracted evidence using statistical methods, data mining, or timelines.
- **Presentation** – Documenting findings, offering expert testimony, and suggesting responses.
- **Decision** – Enabling final determination by legal or management authorities.

DFRWS

- The importance of this model.
- The DFRWS model remains a cornerstone in digital forensics, ensuring that investigations are conducted in a systematic, repeatable, and legally-defensible manner.
- It was the first formal, academic forensic process model, widely referenced across academic and practical domains.
- Serves as a foundation for many modern standards, including ISO, NIST, and forensic methodologies used in criminal and corporate contexts.

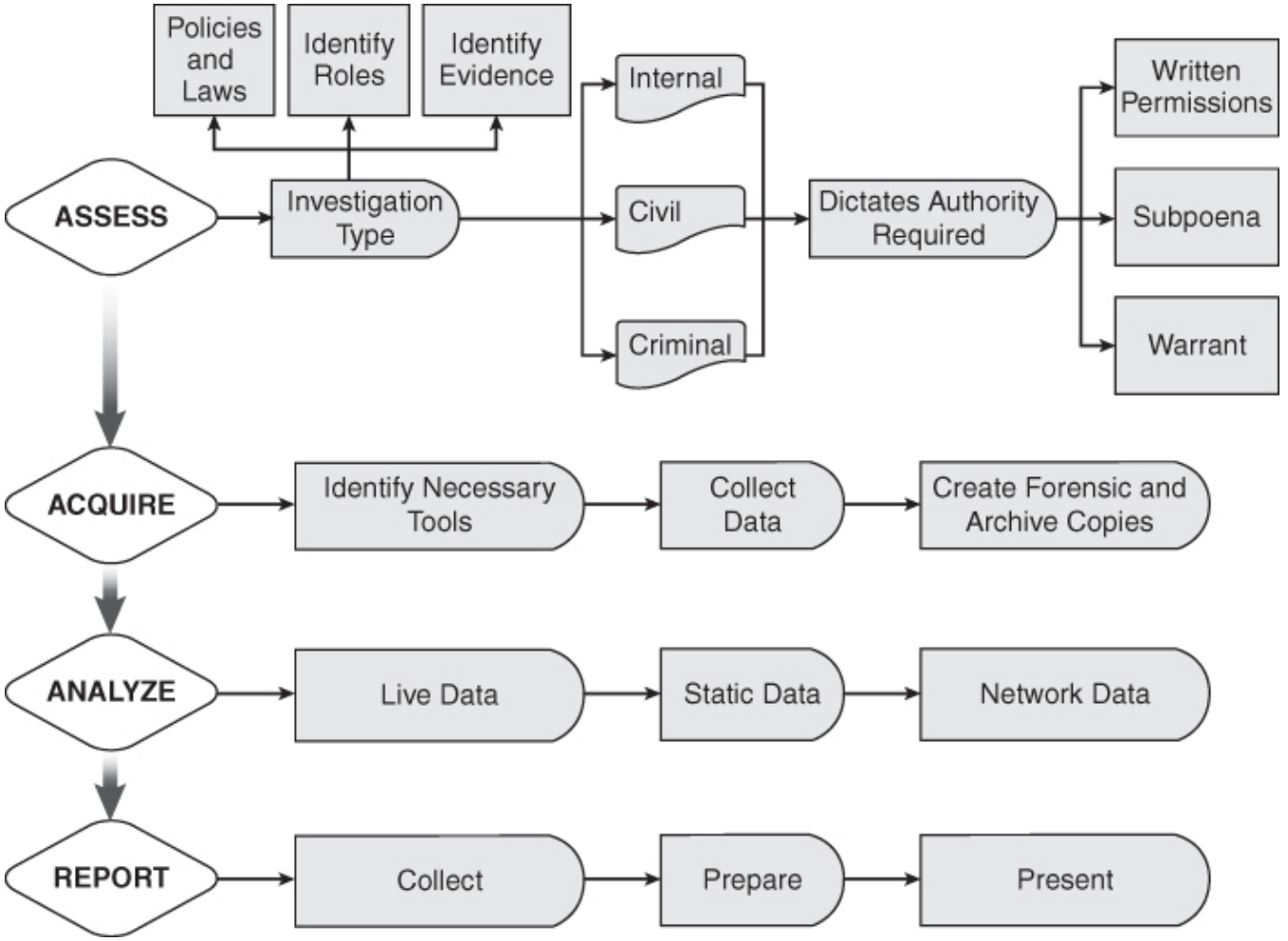
The Basic Model (Kruse and Heiser)

- Assess
- Acquire
- Analyze
- Report

The Casey Model

- Revision of the basic model by Eoghan Casey
  - Identification/Assessment
  - Collection/Acquisition
  - Preservation
  - Examination
  - Analysis
  - Reporting

Casey Model


Policies and Laws
Identify Roles
Identify Evidence
Internal
Written Permissions
ASSESS
Investigation Type
Civil
Dictates Authority Required
Subpoena
Criminal
Warrant
ACQUIRE
Identify Necessary Tools
Collect Data
Create Forensic and Archive Copies
ANALYZE
Live Data
Static Data
Network Data
REPORT
Collect
Prepare
Present

Casey Model - Identification/Assessment

- Define the scope of the examination
- Collect all legal documentation needed
- Get any permissions required for resources not covered by warrants
- Identify the tools required
- Identify the personnel needed
- Identify the stakeholders

Casey Model - Collection/Acquisition

- Collection methods must assure:
  - Data is authentic
  - Sources of data are reliable
  - Nothing was modified throughout the process
  - All tools used are valid
  - Personnel are qualified to do their jobs
  - Enough evidence exists to prove a point
  - Conclusions are valid

Casey Model - Preservation

- NEVER work on original data sources
- Forensically sound copies must be identical to originals
- Media used to store copies must be uncontaminated
- A chain of custody must be maintained

Casey Model - Examination

- All possible sources of data must be examined
  - File system
  - Slack space
  - Unallocated space
  - Hidden partitions
- All tools used must be tested and verified

Casey Model - Analysis

- People other than the investigator may be called upon to examine data
- Technique is as critical as the tools used
- Exculpatory evidence is as critical as incriminating evidence

Casey Model - Reporting

- Actually begins when the assignment is accepted
- First response documentation
- Case documentation
- Process documentation
- Analysis and conclusion

Understanding Scope

- Defines precisely what can be searched and what is being looked for
- Can vary with the type of investigation
- Must never be exceeded

Understanding Scope

- Internal Investigations
- Civil Investigations
  - Intrusions
  - DOS Attacks
  - Malicious Code
  - Malicious Communication
  - Misuse of Resources

Possible Computer Crimes

- Auction or online retail fraud
- Child Pornography
- Child Endangerment
- Counterfeiting
- Cyberstalking
- Forgery
- Identity Theft
- Piracy
- Prostitution
- Theft of Services

The Stakeholders

- Principles (accused and accuser)
- Decision makers
- Mediator
- Regulators
- Management
- Process owners

Documentation

- General case documentation
- Procedural documentation
- Process documentation
- Timelines
  - Case timeline
  - Process timeline
- Chain of custody

Case Documentation

- Contact information for everyone involved
- First response documentation
  - Notes
  - Photographs
  - Videos
- All legal authorizations

Procedural Documentation

- Every task that was performed related to the investigation (not process)
- Summary of events
- List of equipment seized
- What steps were taken and what tools were used
- Detailed analysis of the data

Process Documentation

- User manuals
- Installation manuals
- README files
- Update history logs
- Results of testing

Timeline

- Case timeline
  - Systematic analysis of what transpired
  - Times and dates of related events
  - MAC data of files involved
- Procedural timeline
  - Detailed list of steps taken
  - Times and dates each step began and ended

Chain of Custody

- Begins when evidentiary materials are first seized
  - Time and date taken
  - From whom and where
  - Complete description of each item
- Every time an item changes hands, time, date and people involved
- There can be no gaps in history

Three Incidents

- **MILNET:** Via independent data carrier (Tymnet), a KGB-employed hacker seemed to have easily entered MILNET. It was discovered by chance in 1986 by a programmer at UC Berkeley.

- **Morris Worm:** In 1988, Cornell student Robert Morris released the worm (self-replicating computer program), which quickly spread to over 6000 computers, causing millions in damages.
  - Convicted for violating Computer Fraud and Abuse Act

- **AT&T crash:** The crash occurred due to a software failure, demonstrating the vulnerability of telephone system. It was the result of self-named Legion of Doom, which may or may not have been a hacking menace.

Three Incidents

- Secret Service investigated, getting leads from the bragging of some and disclosure of a critical safety document by one.
- Federal law enforcement believed that the business, Steve Jackson's Games, was a critical player in these actions, but it was only one employee. Their overreaction embarrassed the agency.
- Early hackers included:
  - Kevin Mitnick (perhaps the most famous)
  - cOmrade (first teen to be incarcerated for hacking)
  - Terminus (Unix programmer & AT&T minicomputer expert)
  - Shadowhawk (breaking and entering into U.S. Missile Command)

Phreakers: Yesterday's Hackers

- **Phreaking:** Manipulation of telecommunications carriers to gain knowledge of telecommunications, and/or theft of applicable services
  - Illegal use, manipulation of access codes, access tones, PBXs, or switches
- Methods
  - Social engineering, like shoulder surfing, stealing codes while people are dialing
  - Use of blue boxes, devices that deceived switching system to put through a call for free
  - Some approaches became dated due to changes in phone equipment. New strategies were constantly developed, such as with the theft and sale of stolen access codes ("call-sell" operations).

Evolution in the Hacking Community

- In the 1960s, “hacking” by MIT students was more benign. Hackers would look for computer shortcuts, engage in clever pranks; would "hack" a way at a problem until solution was found.
  - Those with criminal intentions were initially called "crackers."
  - “Hacking” now refers to both benign and criminal activities.

Initially:

- Hacking was conducted via role-playing games, by young, socially inept individuals fascinated with computer technology.
- Some advocated anti-establishment ideology, but others were motivated to hack telephone exchanges because of the costs associated with downloading.

Contemporary Hacking Communities

- Most of the original ideology is gone.
- Contemporary motivation includes:
  - Profit, economic goals (like theft)
  - Revenge (for example, by insiders such as disgruntled employees)
  - Personal notoriety
  - Relief from boredom
  - Informational voyeurism (what's there to see?)
  - Intellectual challenge (hacking as a way to mine for knowledge)
  - Sexual gratification (stalking, harassment)
  - Political goals (the aims of terrorists and spies)

Hierarchy of Contemporary Cyber-Criminals

- **Script kiddies**
  - Inexperienced hackers who use others' programs (like scripts) to exploit vulnerabilities and compromise computer systems, but they don't understand these programs
  - Also known as skidiots, skiddie, or Victor Skill Deficiency (VSD)

- **Cyberpunks**
  - Name used by law enforcement for those who wreak havoc on the Internet
  - Not its original, more benign meaning

- **Hackers/Crackers**
  - Sophisticated computer criminals

- **Cyber-criminal organizations**
  - Greater threat

Social Engineering

- Social engineering takes advantage of people who use technology.
  - Insiders may be the most dangerous, whether by accident or intentionally
  - Can reduce risks through security awareness training

Questions