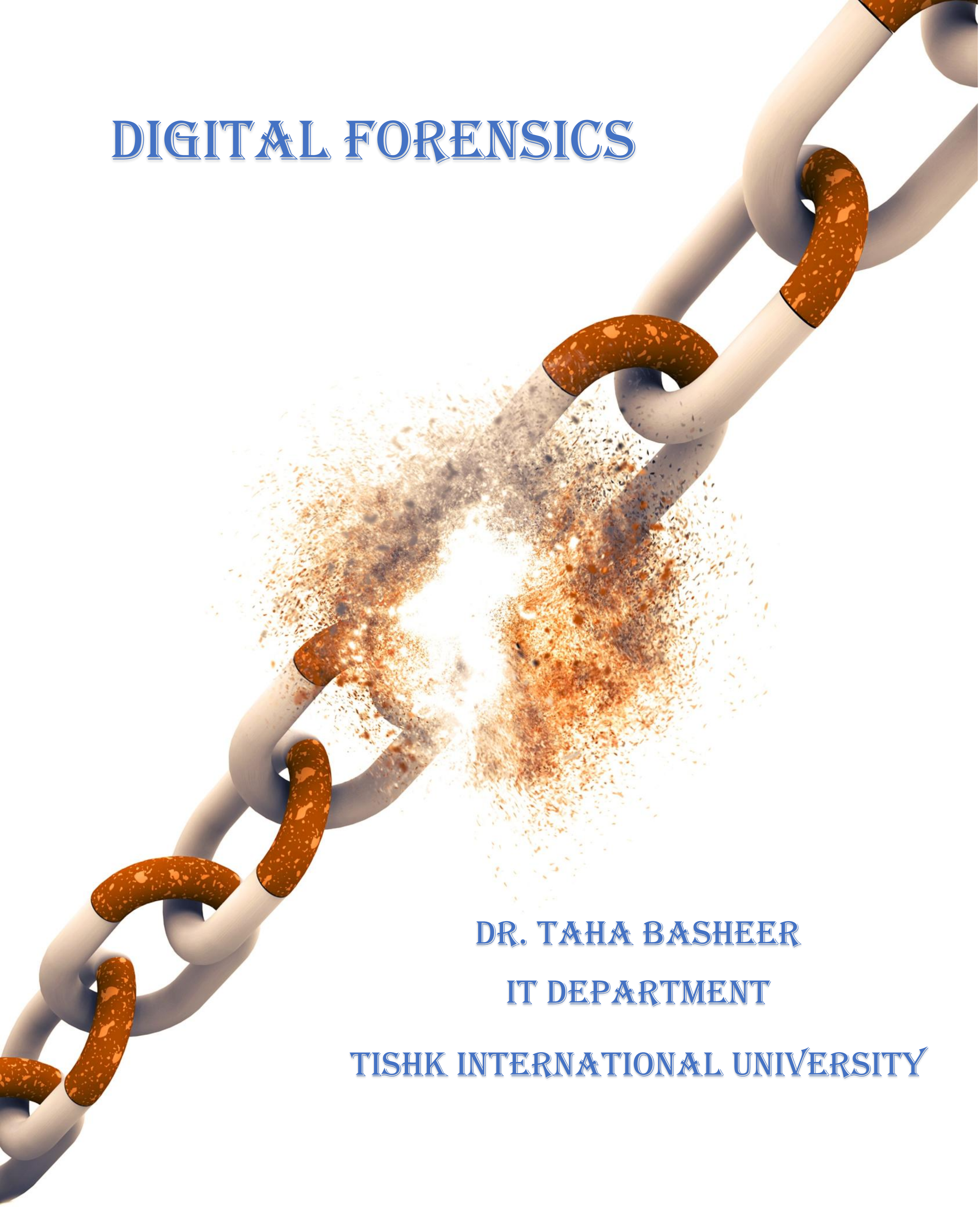
DIGITAL FORENSICS



DR. TAHA BASHEER

IT DEPARTMENT

TISHK INTERNATIONAL UNIVERSITY

Chapter One: Introduction to digital Forensics

Imagine you're called by the police. A company's CEO claims his laptop was hacked and confidential files stolen. You walk into the office — on the desk sits the laptop, a smartphone, and a smartwatch. Where do you begin? What evidence could these devices hold

W*hat clues do you think you could find?"*

This is digital forensics, turning hidden data into legal evidence.

Digital Evidence

Any information stored, transmitted, or received in digital form that can be used in investigation or court.

Characteristic of digital evidence (one or more of the following):

- Easily altered or deleted.
- Large in volume.
- Requires specialized tools to analyze.
- Can have legal weight if properly collected.
- Intangible: It exists as data, not a physical object.
- Volatile: Can be lost or changed when power is turned off or systems are updated.
- Easily replicated: Copies can be made without changing the original.
- Hidden: May reside in unallocated disk space, caches, or metadata.
- Global reach:Often involves data stored across borders or in the cloud.

Have you ever deleted something… and later recovered it?

Sources of Digital Evidence

1. **Computers**
   - Hard drives, browsers, system logs.
   - Example: Registry shows USB devices plugged in.
2. **Smartphones**
   - WhatsApp, SMS, GPS, call logs.
   - Example: Location data proves someone was at the crime scene.
3. **IoT Devices**
   - Smart cameras, smart locks, fitness trackers.
   - Example: A smartwatch shows heart rate spiked at 10:05 PM.
4. **Cloud Services**
   - Google Drive, Dropbox, email servers.
   - Example: A deleted photo recovered from cloud backup.

The amount of information left in each of these places is the basic reason that criminals are caught and found guilty and lawsuits are won or lost. Digital (Electronic) evidence (e-evidence, for short) can play a starring role in the civil, criminal, matrimonial, or workplace cases you investigate.

Like the fingerprint left on the seat adjustment of a car used in a crime, a rogue digital fingerprint always lives on to tell the tale. Computer forensics software makes this process possible by converting an entire hard drive into a single searchable file — called an image — that has no hiding places.

How files stored in computers:

Saving a file (e.g., ***Sand.doc***) in FAT (File Allocation System), for example, system involves 3 steps:

- **FAT entry:** Records location of clusters allocated to the file.
- **Directory entry:** Stores filename, size, FAT link, and metadata
- **Data write:** File content is written to clusters in the data region.

For **Deleting a file (*Sand.doc*) in FAT system:**

1. **FAT entry cleared:** Cluster marked as free.
2. **Dir entry renamed:** First character changed → OS ignores it.

File still intact until overwritten.

- **For permanent removal:** A new file (*Water.doc*) must overwrite the same cluster(s).
- Must be equal or larger in size.

Files are never truly deleted, only marked as gone until replaced

If, for example, Sand.doc filled an entire *cluster* and Water.doc file data took up less space, remnants of **Sand.doc remain and are recoverable**.

The unused portion of the cluster is the slack space. More precisely, it's the portion of the cluster not used by the new file.

When working with operating systems, remember that users have no control over where files are stored, and the larger the hard drive, the lower the chance that deleted data will be overwritten. Even if a file is never saved to a network server, it may still exist on backup media.

Text, voice, and instant messages are always stored digitally by ISPs and phone providers. E-mails, especially when CC and forwarded, spread across multiple servers and drives, making copies multiply like a virus. Forensics work involves locating and recovering these traces.

Can you define digital forensics now?

- Digital forensics is the process of investigating and recovering evidence from digital devices to solve or respond to cybercrimes.
- Purpose: Used to investigate data breaches, identity theft, or other crimes involving technology.

Digital Underworld:

the two dimensions of the digital underworld and what they hold as potential evidence. The contents of both the visible and invisible dimensions can be recovered with forensics tools.

Visible data includes items such as documents, spreadsheets, images, e-mails, folders, programs, log files, and shortcuts. These are typically accessible to the user.

In contrast, **invisible data** is less obvious and may consist of deleted files, hidden folders, file system artifacts, internet history, print spools, system logs, RAM contents, protected storage (like saved credit card details in browsers), and even storage areas outside the normal file system.

Many of these items are not directly created by the user but are generated automatically by the operating system or applications in response to user activity. Both visible and invisible contents can therefore provide valuable e-evidence. In fact, while only about 1% of crimes rely on DNA evidence, more than 50% of cases today involve some form of electronic evidence.

What is my computer doing behind my back?

When files and messages are saved or sent, computer software (that no one ever sees) automatically generates artifacts, or metadata. Metadata exists in virtually every electronic document. It includes information about who created the document, the date it was created, when it was last modified, and more.

Digital communications seem anonymous, but quite the opposite is true

Search engines such as Google, act like unblinking eyes, recording the search terms entered by users. In some cases, this information has been crucial in criminal investigations, even helping to convict murderers. The records usually show IP addresses or cookies rather than personal names, unless the user has registered with identifiable details. However, an IP address alone is often enough to trace activity, since it functions much like a phone number for a computer, identifying it on the network just as a cell number identifies a phone.

Find the IP address of your computer and read much more about IP addresses by visiting http://whatismyipaddress.com

Do you Know?

The 2004 Kobe Bryant case was the first high-profile U.S. criminal case involving cell phone text messages. A judge granted Bryant's attorneys access to cell phone text messages sent among three people — including the accuser — in the hours after the alleged attack. The judge ordered AT&T to produce the records of one of the accuser's friends to whom she sent text messages.

Objectives & Benefits of Digital Forensics

1. Reveal the truth (who did what, when, how).
2. Support law enforcement in court.
3. Recover lost or hidden data.
4. Strengthen cybersecurity by learning from attacks.
5. Hold people accountable.

"Which of these would motivate YOU most if you were a digital investigator: uncovering truth, fighting crime, or protecting systems?"

Activity: Take a sheet of paper (or use any paint app)

1. Draw **yourself** in the center of the page.
2. Around your picture, draw or write **all the digital devices** you use every day — for example:
   - Laptop
   - Smartphone
   - Cloud accounts
   - Smartwatch
   - Game console
   - Smart TV
3. For **each device**, write:
   - **What kind of data** it stores (e.g., photos, chats, GPS, browsing history, documents).
   - **How that data** could be used as **digital evidence** in an investigation.

Sharing & Discussion:

- Be ready to share your digital map with your classmates
- Think about surprising examples — for instance, **did you know your smart TV might record what you watch?**
- Discuss how everyday devices can reveal more about us than we realize.

Chapter 2: Suiting Up for a Lawsuit

Imagine this: A local company reports that their confidential customer data was stolen. The police raid the suspect's apartment and find a single USB flash drive on his desk. That USB could hold the key to the whole case. But here's the problem: if we mishandle it even once — if the evidence is not documented, if it's touched without permission, if it disappears for an hour — the entire case could collapse in court. The hacker could walk free.

Why Law Matters in Digital Forensics

- Digital forensics isn't just "tech work" — it's *legal evidence handling*.
- Evidence is useless if it's not admissible in court.
- Judges don't care how "smart" your tool is if you didn't follow procedure.

Determining the Admissibility of Electronic Evidence

Digital evidence must be handled according to the **rules of evidence** that apply in a given jurisdiction.

Figure 2.1 illustrates the **step-by-step reasoning** a court or legal professional follows to decide whether **e-evidence** (electronic evidence) can be admitted in trial.

Step 1: Is the Evidence Relevant?

- **Question:** Does the evidence have any tendency to make a fact more or less possible than it would be without the evidence?
- **Meaning:** The data must help prove or disprove an important element of the case.
- **Example:** A text message confirming a meeting between a suspect and victim is *relevant*.
- **If "No"** → The evidence is **inadmissible** — irrelevant data cannot be used in court

Step 2: Is the Probative Value Outweighed by Specific Risks?

- **Probative value** means the strength or usefulness of the evidence in proving something important.
- However, even relevant evidence may be excluded if it causes **risks**, such as:
    - Wasting time or confusing the jury
    - Misleading or unfairly influencing the case
    - Overcomplicating issues
- **Example:** Presenting hundreds of irrelevant browsing logs might distract the jury rather than clarify the issue.
- **If "Yes"** → The evidence is **inadmissible** (its risks outweigh its usefulness).

Step 3: Is There Any Exclusion That Applies?

- Even if the evidence is relevant and not misleading, it might still fall under **legal exclusions**
- Common exclusions include:
    - **Illegally obtained evidence** (e.g., through unauthorized hacking or without a warrant).
    - **Hearsay(rumors)** rules (statements made outside of court used to prove the truth of the matter).
    - **Privilege violations** (e.g., attorney-client communications).
- **If "Yes"** → The evidence is **probably inadmissible**, unless an **exception** applies (for example, consent or a public safety exception).

Step 4: Final Decision – Admissible Unless the Judge Decides Otherwise

- If the evidence passes all the above tests — it is relevant, its probative value is not outweighed by risks, and no exclusion applies — then it is generally **admissible**.
- However, the **judge** retains final discretion.
    - A judge may still exclude evidence if admitting it would be unfair or contrary to procedural justice.
- Thus, the outcome is **"Admissible unless the judge decides it's not.**

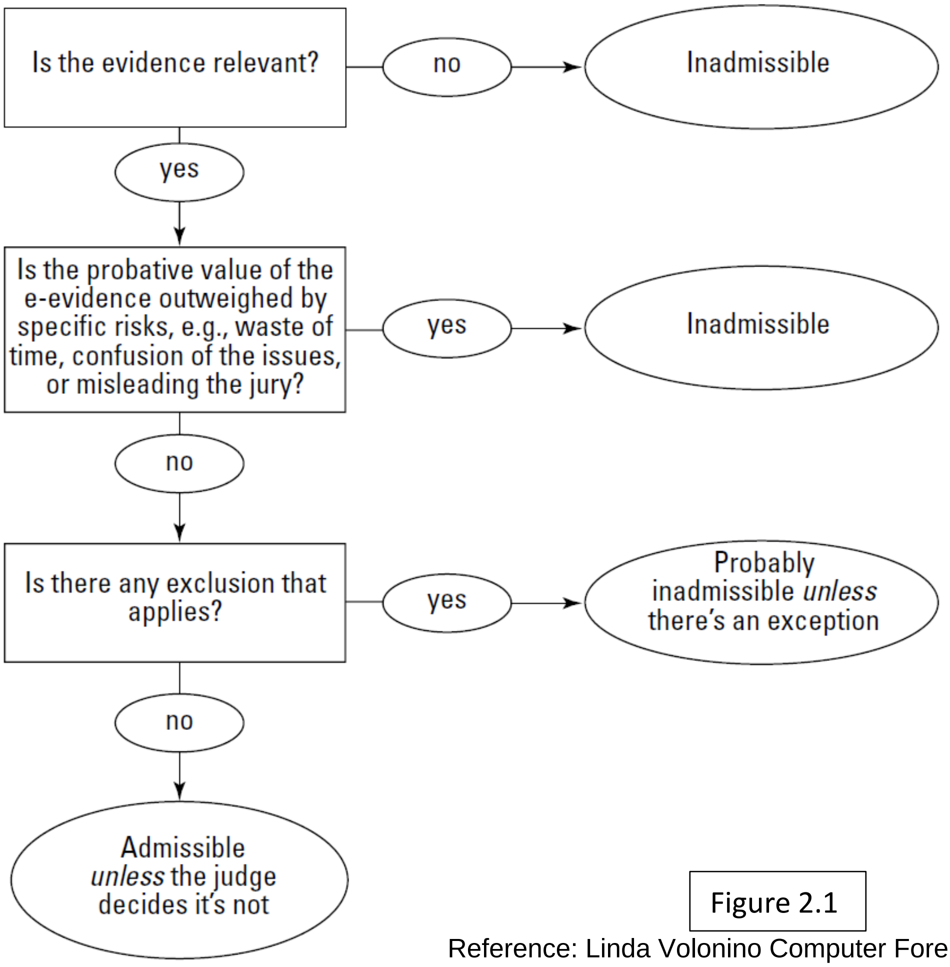

Is the evidence relevant?
no
Inadmissible
yes
Is the probative value of the e-evidence outweighed by specific risks, e.g., waste of time, confusion of the issues, or misleading the jury?
yes
Inadmissible
no
Is there any exclusion that applies?
yes
Probably inadmissible *unless* there's an exception
no
Admissible *unless* the judge decides it's not

Figure 2.1

Reference: Linda Volonino Computer Forensics for Dummies

Group Game: "The Voice Case"

A digital audio clip has been leaked online.
The clip **seems** to contain a person confessing to a crime.
Two teams will battle to **convince the judge** (the trainer or audience) of their side.

- **Red Team = Prosecution** (They argue the audio *is valid evidence*.)
- **Blue Team = Defense** (They argue the audio *cannot be trusted*.)

Legal Reflection: The Balance of Truth and Rights

- Law tries to balance **finding truth** with **protecting fairness**.
- Digital evidence can be misleading: manipulated audio, deepfakes, or incomplete data.
- A good forensic expert must **communicate findings clearly**, acknowledging uncertainty.

Digital Evidence handling Procedure:

In digital forensics, both sides of a case (prosecutor/defense or plaintiff/defendant) must be able to defend their methods, interpretations, and conclusions. The integrity of electronic evidence depends on following a **standardized, defensible approach** for data handling and preservation.

Core steps in handling e-evidence:

1. **Pre-Investigation Preparation** – plan procedures, tools, and scope.
2. **Acquisition and Preservation** – collect evidence without altering or damaging the source.
3. **Authentication** – verify that the acquired copy is identical to the original (e.g., through hash values).
4. **Analysis** – examine files, logs, and artifacts without modification. Errors here can destroy a case.
5. **Production and Reporting** – present findings clearly and systematically in reports and in court.

Tampering with e-discovery can cost more than failing to comply with requests to produce ESI. For overwriting files and concealing e-evidence, the court punished Morgan Stanley with a $1.6 billion fine in 2005.