DIGITAL FORENSICS: THE BASICS

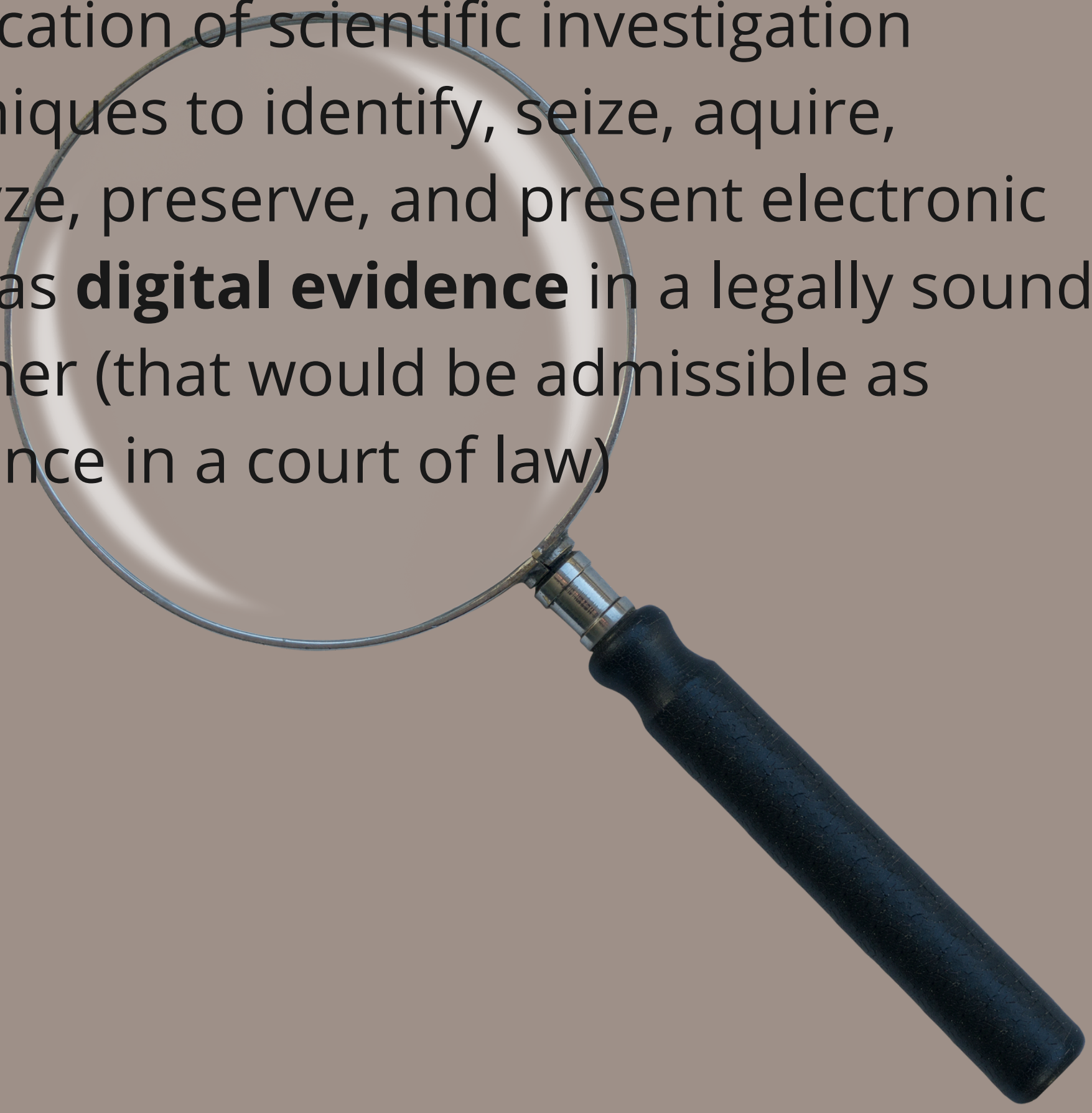
🔍Unveiling the Digital truth

NAMRAH AZAM

NAMRAH AZAM

1. What is digital forensics?

Application of scientific investigation techniques to identify, seize, aquire, analyze, preserve, and present electronic data as **digital evidence** in a legally sound manner (that would be admissible as evidence in a court of law)



NAMRAH AZAM

2. Why digital forensics matters

Digital forensics is important for cyber resilience, incident response, and evidence-based decision-making. It supports the prevention of future attacks, attribution and plays a key role in uncovering critical evidence to ensure accountability and justice in both cybercrime and other investigations.

👨‍💼 For businesses: protects reputation, reduces downtime, and aids compliance

🔍 For investigators: a powerful tool to bring truth and accountability in the digital era

3. Digital forensics process

1. Identify	Recognizing and identifying potential sources of digital evidence.
2. Seize	Physically or logically isolating electronic devices to prevent data loss and maintain integrity of evidence.
3. Aquire	Extracting stored data from the seized device (making forensically sound copies, i.e. disk imaging).
4. Preserve	Ensuring integrity of evidence to prevent tampering (i.e. digital fingerprints hash digests)
5. Analyze	Examining data for evidence (i.e. logs, files, metadata).
6. Present	Report the findings of a forensic investigation to relevant stakeholders through documentation and/or court proceedings.

🔑 Key Principle: chain of custody ensures evidence is admissible

📝 Note: Some steps may vary in order depending on the situation
Example: In a time-critical incident response, preliminary analysis might be done before full preservation to contain an ongoing cyberattack.

NAMRAH AZAM

NAMRAH AZAM

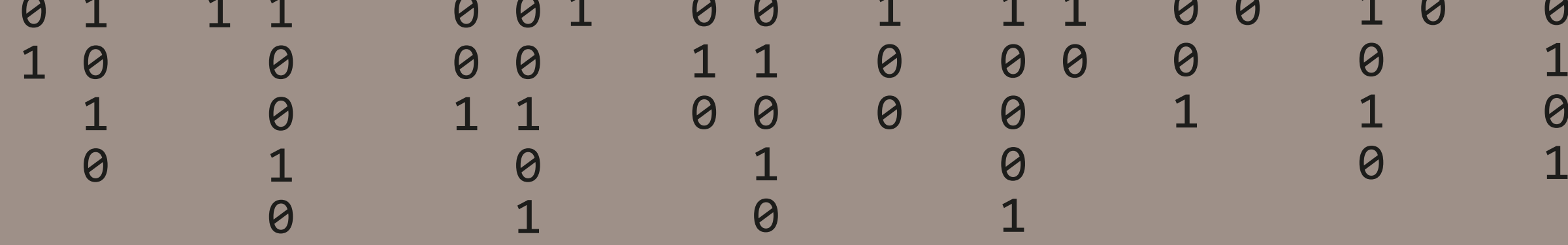
4. Real-world applications

💻 Cybercrime investigations: identifying hackers, data theft, ransomware, attribution etc.

⚖️ Legal Cases: Evidence for fraud, harassment, or intellectual property theft.

🏛️ Corporate Security: Incident response, reversing, breach and malware analysis

🚨 National Security: Tracking advanced persistent threats (APTs) and terrorism-related activities.



5. Tools & Techniques

Common techniques:

- File recovery: carving and retrieving data
- Log analysis: tracking access and changes
- Timeline reconstruction: creating a chronological event timeline
- Network forensics: analyzing traffic and packet data
- Malware analysis: examining malicious software

Popular tools:

- EnCase, FTK, X-ways for imaging and analysis
- Autopsy analyzing disk images, recovering deleted files, and extracting artifacts
- Wireshark for network analysis
- Volatility for memory analysis

NAMRAH AZAM

6 Challenges in digital forensics

🔐 Encryption: securing access to encrypted devices

💾 Volume of data: analyzing massive datasets efficiently

🥷 Anti-forensics techniques: detecting tampered data, erased evidence, or techniques used to obscure digital traces (file obfuscation or time-stamping manipulations)

⚖️ Legal & privacy issues: Handling evidence according to jurisdictional laws and privacy regulations to ensure admissibility in court

NAMRAH AZAM

7 Trends & Innovations

🌐 Cloud forensics: evidence collection from cloud platforms (AWS, Azure, Google Cloud)

🤖 AI integration: automating to process large-scale data faster and to find relevant evidence

📲 Mobile forensics: gain access to phones in order to extract and analyze smartphone data (messages, GPS data, pictures).

🔐 Blockchain investigations: tracing cryptocurrency transactions

🚗 Car forensics: investigating digital systems in modern vehicles (event data recorders, GPS logs, and onboard diagnostics)

LETS CONNECT!

Let us connect if you want to learn more about digital forensics or if you are interested in enhancing your cyber defense strategy!

NAMRAH AZAM