The Evolution of Network Forensics

From Non-Forensic to Forensic Devices

Who am I!

Prof. Kasun De Zoysa, Prof. Samaranayake and Prof Sead Muftic @Georgetown University, USA, 2003

Kasun De Zoysa
Professor in Computer Science
University of Colombo School of Computing

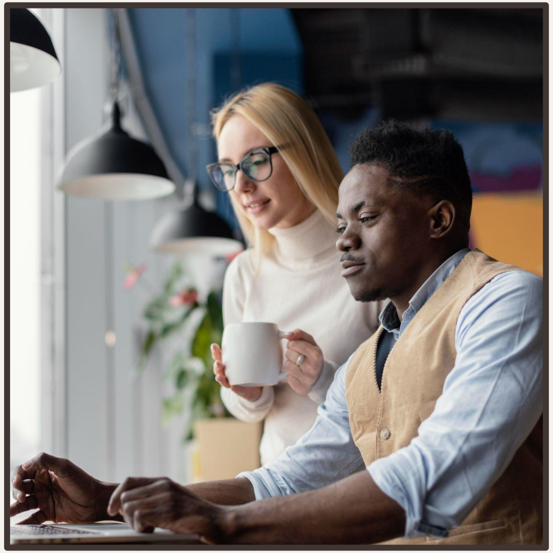
“I’ve seen things you people wouldn’t believe.
Data deleted and wiped coming back to life.
All those … data will never be lost … in time,
we should be able get it all back.”

2003- 2023

01

Introduction

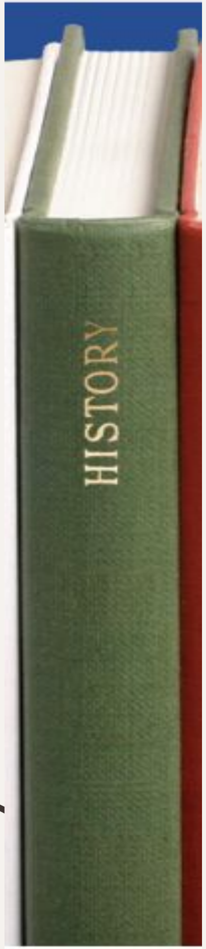
History, Type of Digital Forensic, Forensic Process



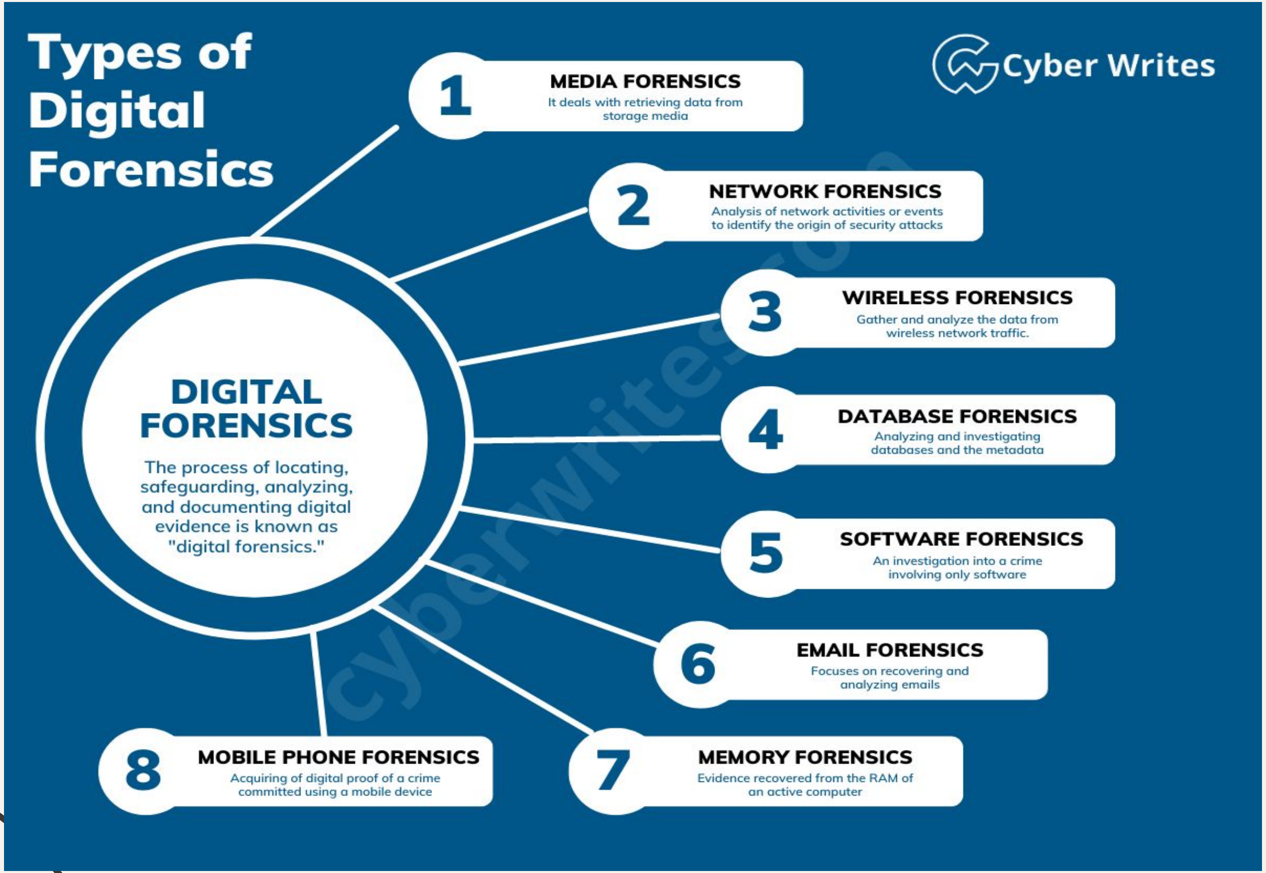
800,944

FBI’s internet crime records in year 2022

(https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf)



1978	The Florida Computer Act
1980s	Rapid growth in Digital Forensics Field
1990s	Adaptive Growth, implemented in various sectors
1970-1980	Federal Law Enforcement
1984	Operation started by FBI Computer Analysis and Response Team (CART)
1994-1995	Modern British digital forensic methodology developed.
1998	Good practice guide- Association of Chief Police Officers , UK



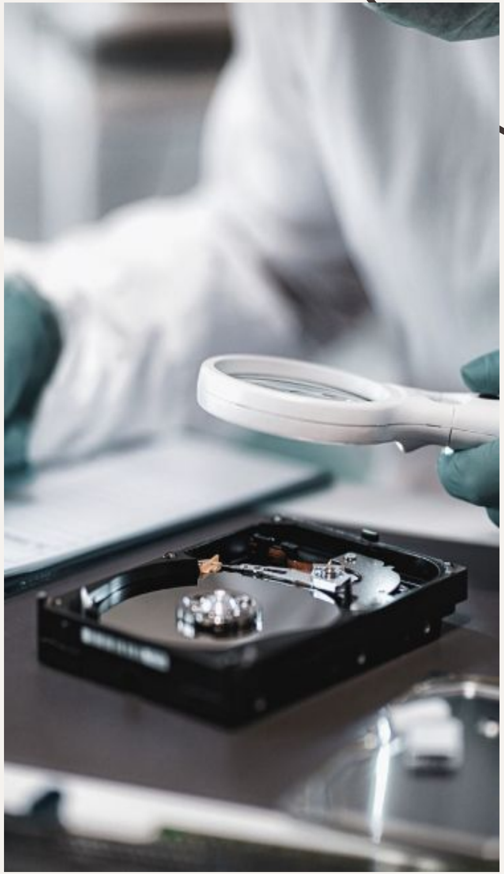
Types of Digital Forensics

Cyber Writes

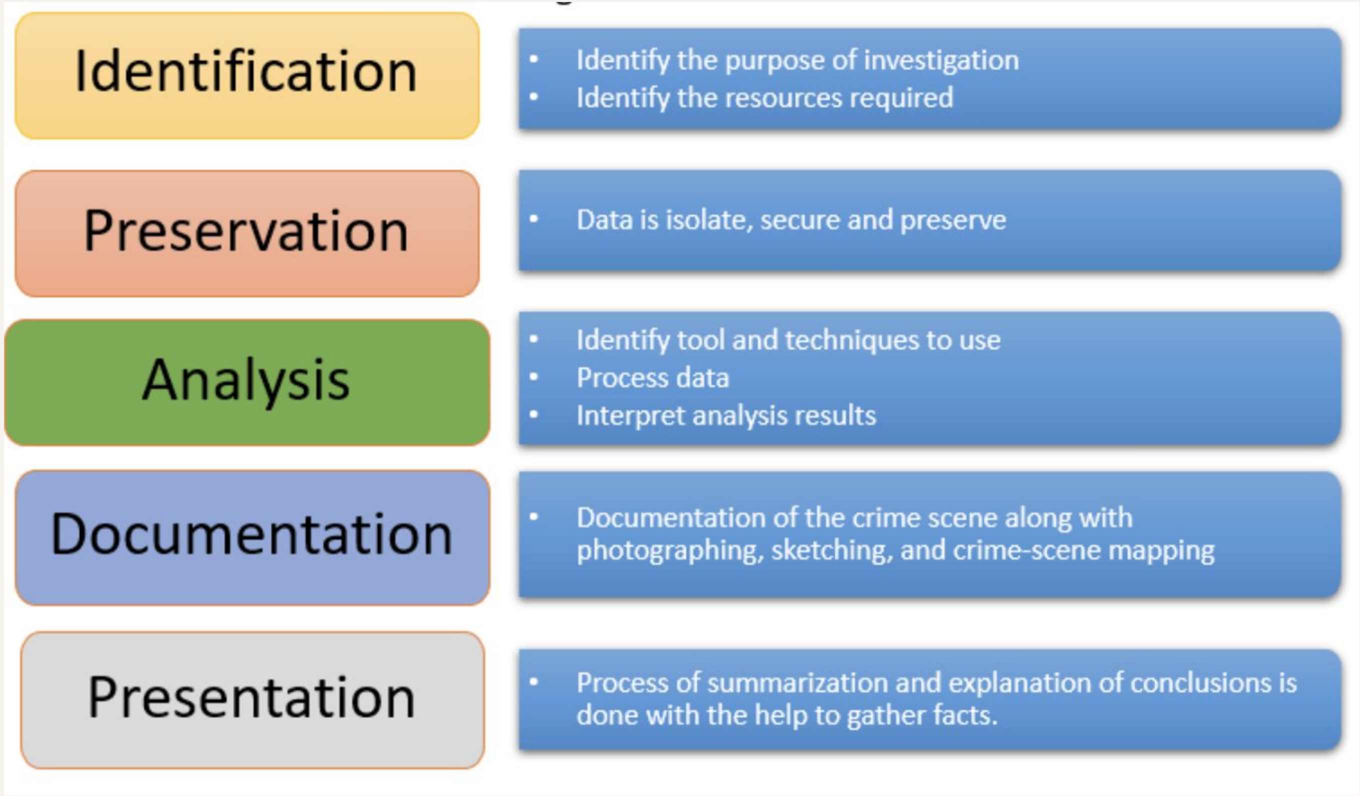
DIGITAL FORENSICS

The process of locating, safeguarding, analyzing, and documenting digital evidence is known as "digital forensics."

1. **MEDIA FORENSICS** – It deals with retrieving data from storage media
2. **NETWORK FORENSICS** – Analysis of network activities or events to identify the origin of security attacks
3. **WIRELESS FORENSICS** – Gather and analyze the data from wireless network traffic.
4. **DATABASE FORENSICS** – Analyzing and investigating databases and the metadata
5. **SOFTWARE FORENSICS** – An investigation into a crime involving only software
6. **EMAIL FORENSICS** – Focuses on recovering and analyzing emails
7. **MEMORY FORENSICS** – Evidence recovered from the RAM of an active computer
8. **MOBILE PHONE FORENSICS** – Acquiring of digital proof of a crime committed using a mobile device



Forensic Process



Identification

- Identify the purpose of investigation
- Identify the resources required

Preservation

- Data is isolate, secure and preserve

Analysis

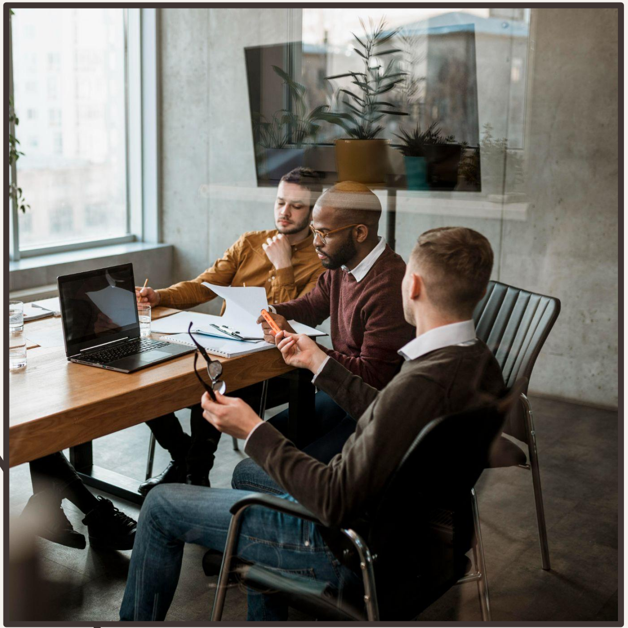
- Identify tool and techniques to use
- Process data
- Interpret analysis results

Documentation

- Documentation of the crime scene along with photographing, sketching, and crime-scene mapping

Presentation

- Process of summarization and explanation of conclusions is done with the help to gather facts.



02

Network Forensic

Non Forensic Devices,
Forensically Sound Devices

Network Forensics

The monitoring, capture, storing and analysis of network activities or events in order to discover the source of security attacks, intrusions or other problem incidents, i.e. worms, virus or malware attacks, abnormal network traffic and security breaches.

Non-forensic Devices

non-forensic devices are general-purpose devices used for regular, everyday purposes such as mobile phones, laptops, switches, routers etc.

Forensically Sound Devices

Any digital devices that have been specifically designed, configured, and maintained in a manner that ensures the integrity, preservation, and secure handling of digital evidence for forensic purposes.

Network Devices

Non-Forensic

- Routers
- Switches
- Access Points
- Firewalls
- Load Balancers
- Proxy Servers
- etc

Forensically Sound

- Network TAPs (Test Access Points)
- Forensic Packet Capture
- Forensic Firewalls
- Network Time Servers (NTP Servers)
- Secure Logging Servers
- Hardware Security Modules

03

Forensically Sound Devices

Chain of Custody, Immutability, Timestamping, Access Control, Authentication, Compliance with Legal Standards

Features of Forensically Sound Devices

- Chain of Custody (Cryptographic Hashing)
- Immutability (Write-Blocking)
- Timestamping and Device State
- Access Control and Authentication
- Compliance with Legal Standards (Digital Signatures)

Chain of Custody

Maintain a detailed chain of custody log, documenting who has had possession of the device, logs or images at all times.

Hashing

Generate cryptographic hashes of the original data. This provides a unique fingerprint of the data, allowing for later verification of its integrity.

Immutability

Immutability is a crucial concept in digital forensics. It refers to the state of data or evidence that cannot be altered, deleted, or modified once it has been captured or acquired.

Timestamping and Device State

Timestamping and documenting the device state are essential practices in digital forensics to ensure the accuracy, reliability, and integrity of evidence.

Access Control and Authentication

Access control and authentication are crucial security measures in digital forensics, ensuring that only authorized individuals or entities can access and interact with the devices.

Compliance with Legal Standards

Adhering to established laws, regulations, and ethical guidelines is essential for ensuring the admissibility and credibility of digital evidence in court.

04

What's Next?

AI and Blockchain

AI for Network Forensic

Using Artificial Intelligence (AI) for network forensics involves leveraging machine learning algorithms and other AI techniques to analyze and extract meaningful information from network data.

What can we do?

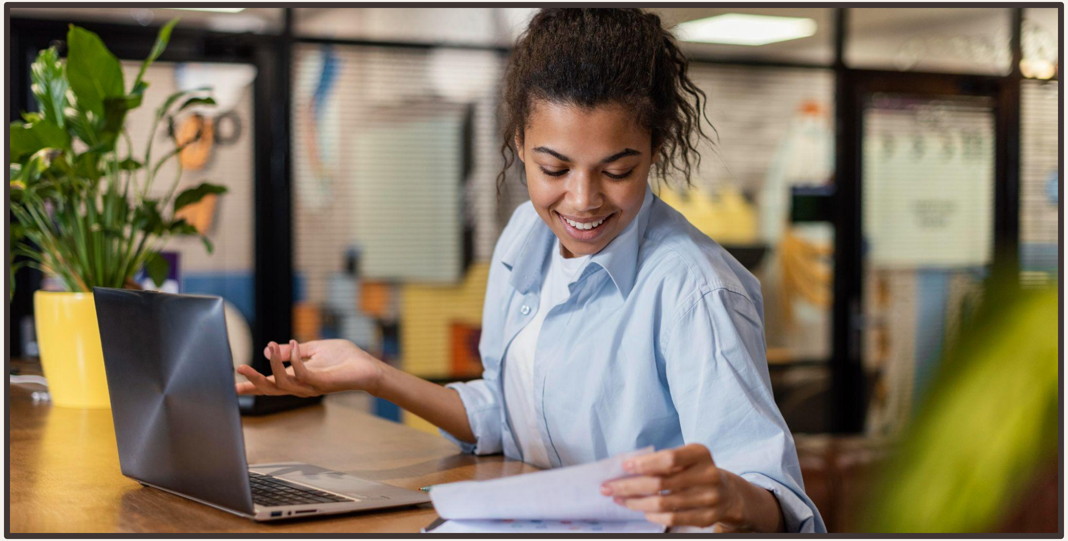
Anomaly Detection

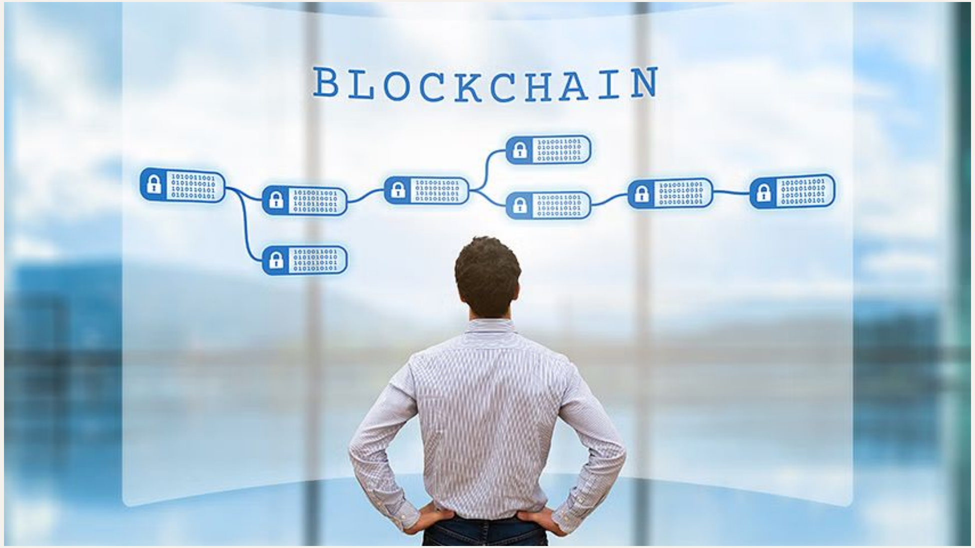
Behavioral Analysis

Pattern Recognition

Threat Intelligence

Incident Response





Blockchain

Blockchain technology can enhance the integrity and traceability of digital evidence.

Hence it can be used to create a forensically sound device.

Blockchain Makes Forensically Sound Devices

Chain of Custody

Each time the device or its data changes, record it on the blockchain, including details such as timestamps, identities of individuals involved, and the condition of the device.

Hashing

Hash device logs and critical data at regular intervals and store these hashes on the blockchain.

Digital Signatures

Require digital signatures for critical device actions, such as firmware updates or data access. These signatures can be recorded on the blockchain to ensure that only authorized actions are taken.

Thanks

Do you have any questions?

kasun@ucsc.cmb.ac.lk
+94773832923
University of Colombo School of Computing

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, infographics & images by **Freepik**