RESTRICTED

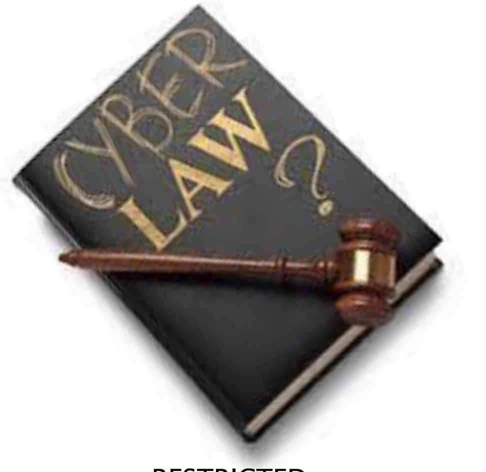
# COLLECTION AND PRESERVATION OF DIGITAL & FORENSIC EVIDENCE IN CYBER CRIME CASES

Presented by:
SSP Jimmy Haguma, CEH, CHFI
Head Electronic Counter Measures - UPF

**Forensics**. Advisory. Security

# SCOPE

- Digital Landscape
- Cyber threat Statistics
- Cyber crimes landscape in Uganda
- Cyber crimes
- Forensic Science
- Principles of Forensic science
- Categories of Forensic science
- Handling of Exhibits
- Digital forensics cryptography
- Challenges
- Call for action
- Netiquettes
- Conclusion



# QUOTE

"It takes 20 years to build a reputation and a few minutes of a cyber-incident to ruin it."

Stephane Nappo, 2018 Global CISO of the year.

# DIGITAL LANDSCAPE

- There are over *200* social networking sites
- Facebook has got over 3 billion users worldwide that post approximately 350 million photos each day
- YouTube has got over *2* billion users, *WhatsApp* at *1.6* billion, *WeChat* at 1.2 billion and photo-sharing app *Instagram* with *1* billion monthly active accounts

# DIGITAL LANDSCAPE ...

- According to 2021 report by App Annie, the average smartphone user worldwide spends 4.2 hours per day
- CIPESA, an African Tech ICT Research Org. estimates it to be 6/7 hours as of August 2022

# QUOTE

"There are only two types of companies: Those that have been hacked and those that will be hacked."

**Robert S. Mueller**

Former Director of the FBI and now Special Counsel into the Russian interference of the USA election

# CYBER THREAT STATISTICS

- 2,200 cyber attacks per day, with a cyber attack happening every 39 seconds on average (source: Astra Security)
- Ransomware accounts for 64% of successful cyber-attacks against the financial sector. (source: PT Security)
- 96% of phishing attacks are delivered via email
- 57% of banking executives identified cyber security as a top priority in 2023. (source: CSI Web)
- Between 2021 and 2023, data breaches rose by 72%, surpassing the previous record (source: Forbes)

# CYBER CRIME LANDSCAPE IN UGANDA

- According to the Police Annual Crime Report of 2023, there was a decrease in crime reported by 1.5%
- A total of **12,892** cases of Economic crimes were reported to Police by the end of 2023, out of which **3,544** cases were taken to Court.
- **2,729** cases were not proceeded with, while **6,619** cases are still under inquiry.
- Out of the total cases taken to Court, **1,132** cases secured convictions, **43** cases were acquitted, **400** cases were dismissed while **1,969** cases are still pending in Court.

# CYBER CRIME LANDSCAPE IN UGANDA …

- A total of **245** cases of Cybercrimes were reported to the Police countrywide in 2023 compared to **286** in 2022, giving a **14.3%** decrease in this crime category**.** By the end of the year, **61** cases were taken to Court, **51** cases were not proceeded with while **133** cases are still under inquiry.

- Out of the total cases taken to Court, **14** cases secured convictions, **01** case was acquitted, **02** cases were dismissed while **44** cases are pending in Court. Cybercrimes led to a loss of approx. **Ugx. 1,5bn** in 2023, out of which **Ugx. 377m** was recovered.

# QUOTE

“Refocus cybersecurity efforts on cyber defender personnel instead of focusing primarily on the technology associated with cyber tools, networks and systems, AND train them to face off against more real threats.”

**Hon. Nickolas Guertin**
Director, Operational Test and Evaluation
April 2023

# CYBER CRIMES

- **Identity Theft**
- Online Auction Fraud
- Crimes Against Children
- Crimes Against Seniors
- Gambling
- Money Laundering
- Narcotics
- Prostitution
- Hacking
- Network Intrusions
- Virus Distribution
- E-mail Scams
- Theft of Intellectual Property
- Piracy
- Harassment
- Stalking
- Homicide
- Terrorism

…and the list goes on!

***Can you name a crime that would not involve electronic evidence*** ?

# CYBER CRIMES …

- Internet frauds – identity thefts, password harvesting, foot-printing, social engineering.
- Health care frauds i.e. medical care schemes
- Financial frauds – Salami techniques (Banks), Payment cards frauds & insurance schemes, Telecom frauds – mobile money, SIM card swapping, unsolicited SMS or voice calls, VIOP interceptions
- Ponzi schemes – Capital Chicken, Telex free
- Domain Hosting frauds – website cloning and hacking
- Intellectual property infringement refer to case Uganda vs CITI Cable firm

# CYBER CRIMES..

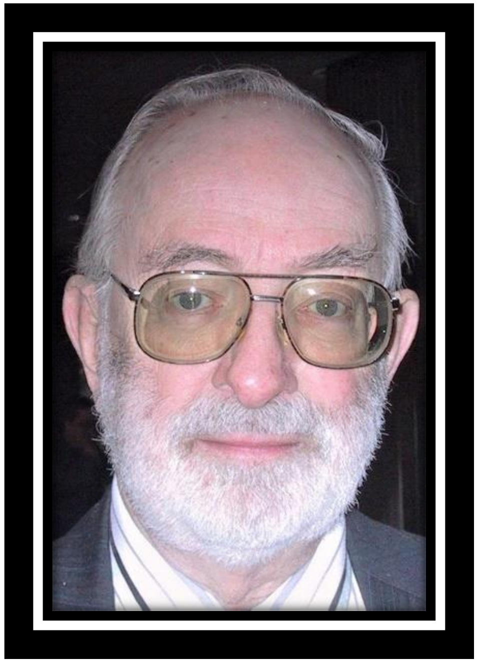
ft, Robinhood Byamukama, Guster Nsubuga and their accomplice hack into the URA system. Illustrations by
izera

Uganda Vs Gaster Nsubuga (HCT-00-AC-SC-0084-2012)

Uganda Vs Ivan Ganchev & others

(Criminal Case N. 865 of 2012)

# QUOTE



"Physical evidence cannot be intimidated. It does not forget. It doesn't get excited at the moment something is happening like people do. It sits there and waits to be detected, preserved, evaluated, and explained."

Dr. Herbert Leon MacDonnell,
*The Evidence Never Lies, 1984*.

# FORENSIC SCIENCE ...

- **Forensic scientists** collect, preserve, and analyze scientific evidence during the course of an investigation.
- 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

# PRINCIPLES OF FORENSIC SCIENCE

- Principles of forensics sciences
  - Law of Individuality
  - Principle of Exchange
  - Law of progressive change
  - Law of comparison
  - Law of Analysis
  - Law of Probability
  - Law of circumstantial facts

# CATEGORIES OF FORENSIC SCIENCE

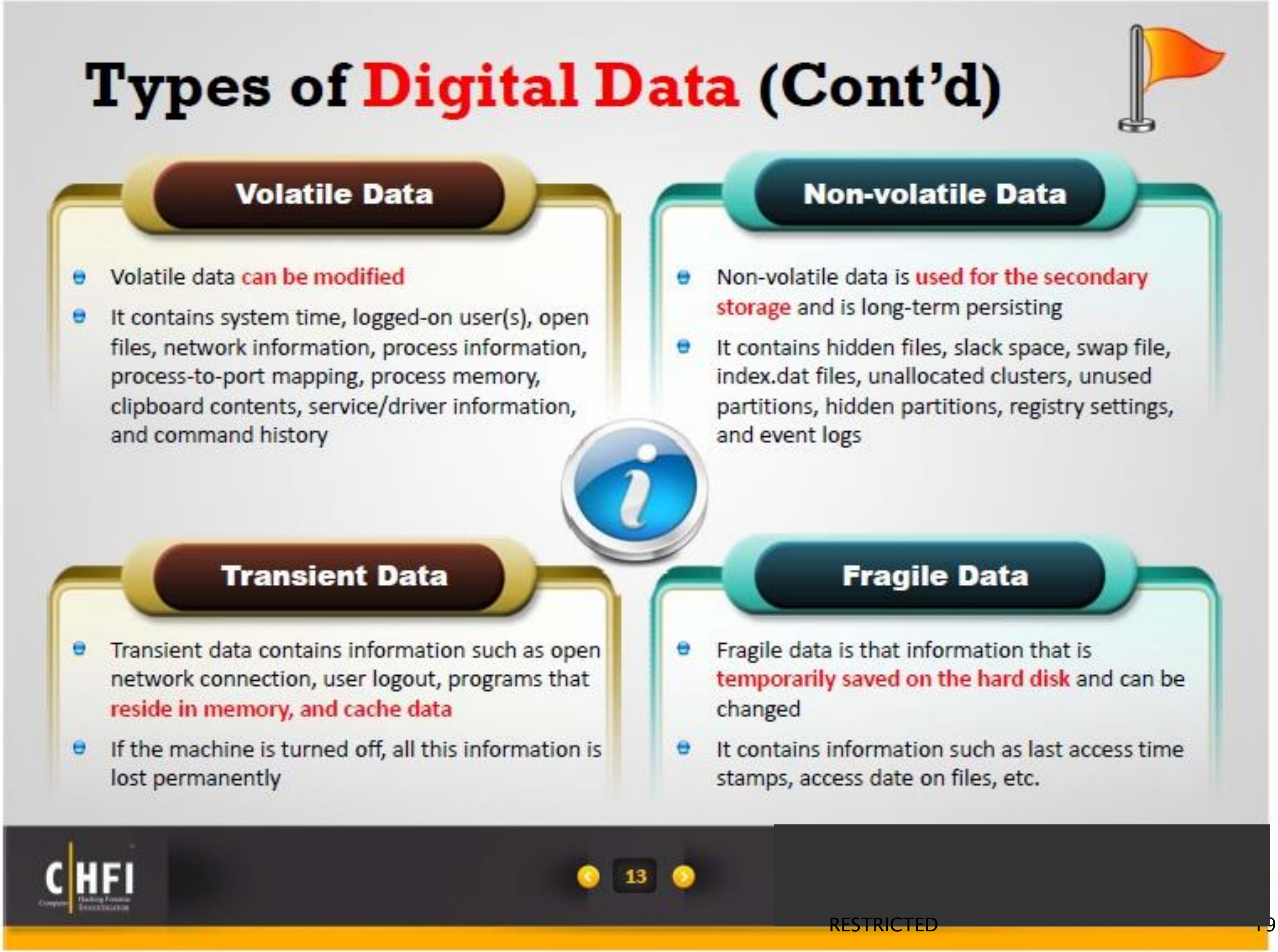
- Criminal Identification
  - Scenes of Crime
  - Photography
  - Finger Prints
- Questioned Documents
- Ballistics
- Computer crimes (Digital forensics)
- Chemical, Biology, Radiology & Nuclear e- Analysis
  - Toxicology
  - Explosives and Residues
  - Foods Water, Drugs & Environment
  - DNA &Serology

# Definition of Digital Evidence

- Digital evidence is defined as "any information of **probative value** that is either stored or transmitted in a digital form"
- Digital information can be **gathered** while examining digital storage media, monitoring the network traffic, or making the duplicate copies of digital data found during forensics investigation

Digital evidence is found in files such as:

- Graphics files
- Audio and video recording and files
- Internet browser histories
- Server logs
- Word processing and spreadsheet files
- Emails
- Log files



# Types of Digital Data (Cont'd)

## Volatile Data

- Volatile data **can be modified**
- It contains system time, logged-on user(s), open files, network information, process information, process-to-port mapping, process memory, clipboard contents, service/driver information, and command history

## Non-volatile Data

- Non-volatile data is **used for the secondary storage** and is long-term persisting
- It contains hidden files, slack space, swap file, index.dat files, unallocated clusters, unused partitions, hidden partitions, registry settings, and event logs

## Transient Data

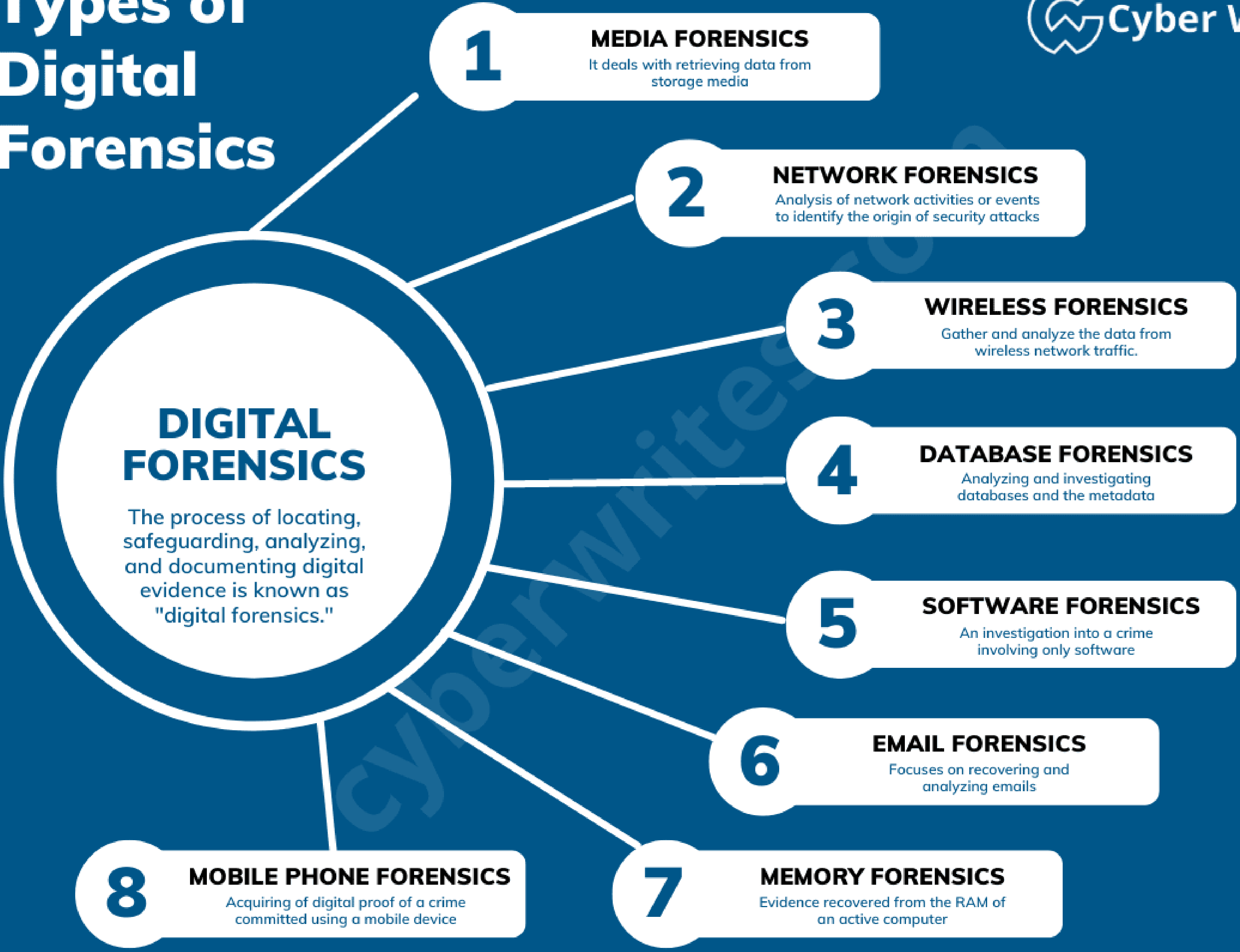
- Transient data contains information such as open network connection, user logout, programs that **reside in memory, and cache data**
- If the machine is turned off, all this information is lost permanently

## Fragile Data

- Fragile data is that information that is **temporarily saved on the hard disk** and can be changed
- It contains information such as last access time stamps, access date on files, etc.

# 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

# DIGITAL FORENSICS METHODOLOGY

- Digital forensics is the process of storing, analyzing, retrieving, and preserving electronic data that may be useful in an investigation.
- It includes data from hard drives in computers, mobile phones, smart appliances, vehicle navigation systems, electronic door locks, and other digital devices

- Seizure *(search authority)*
- Documentation of seized items *(chain of custody)*
- Delivery to the laboratory *(evidence storage)*
- Assigning of the case to Investigating officer
- Imaging & Acquisition
- Generation of forensic report

# DIGITAL FORENSIC TOOLS

- Encase
- SANS Toolkit
- FTK (forensic tool kit)
- IEF (Internet Evidence Finder)
- UFED Touch
- Wire shark/Caine and Able

# DIGITAL FORENSIC LAB

# ROLE OF SOCO (SCENES OF CRIME OFFICER)

- Identifying and Gathering Evidence
- Documenting Evidence
- Preserving Evidence
- Testing Evidence for authenticity and validity
- Reporting findings in courts of law (Testifying)

# HANDLING OF EXHIBITS

- **Chain of custody,** refers to the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence

- **Evidence management** is the administration and control of evidence related to an event so that it can be used to prove the circumstances of the event, and so that this proof can be tested by independent parties with confidence that the evidence provided is the evidence collected & is related to the event.

# HANDLING OF EXHIBITS

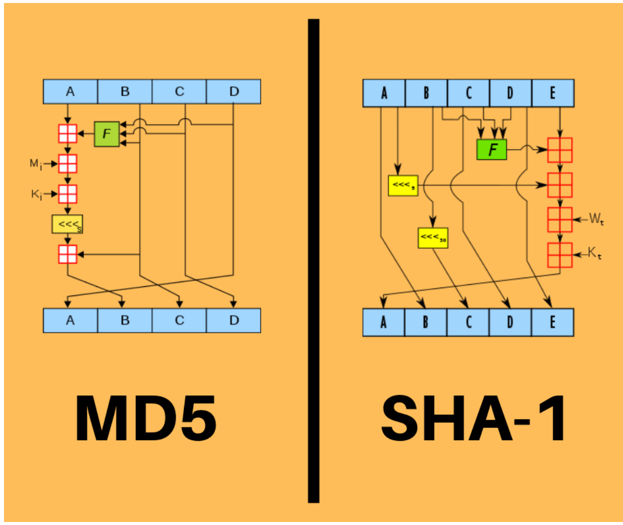
- Before you package computer hardware & other storage devices
  - Check to see if the original packaging is available
  - Use non-static packing material
  - Cushion well
- Preserve other forms of evidence at the scene. Namely;
  - Latent prints
  - DNA
  - Trace evidence

# HANDLING OF EXHIBITS

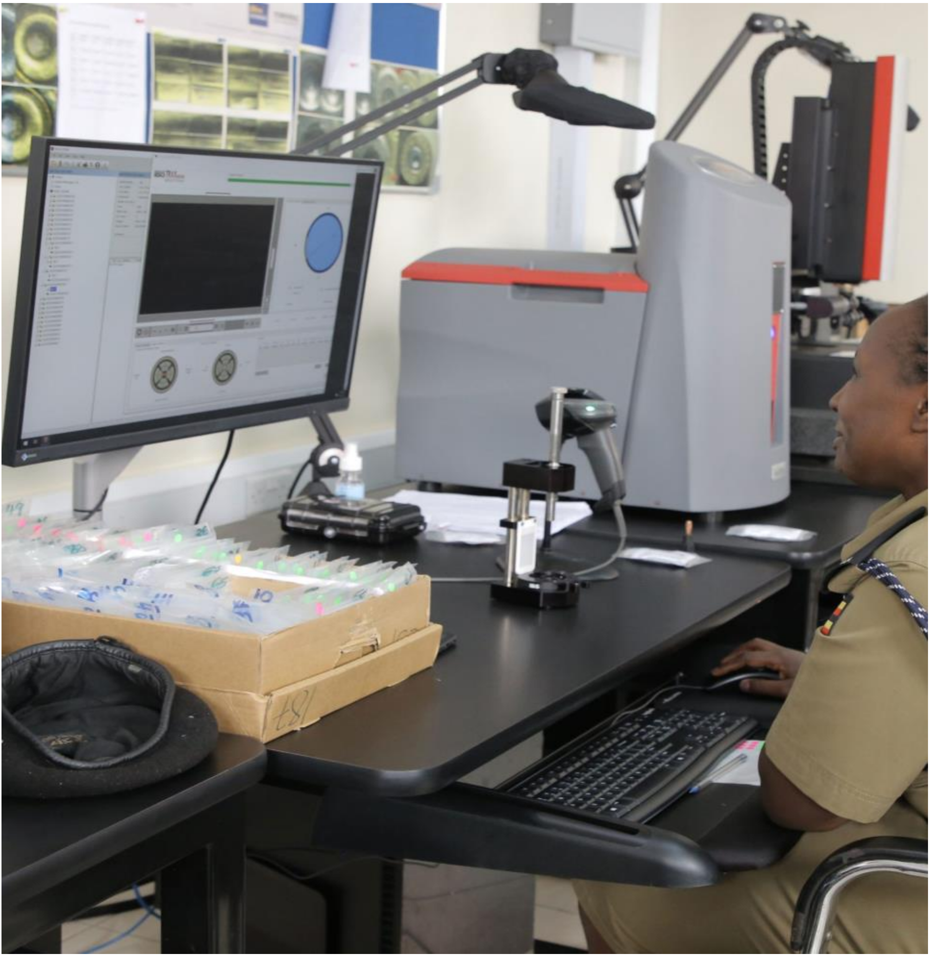
- Document the scene you are leaving
  - Photograph
  - Videotape
- You should have “**before**” and “**after**” documentation
  - This Counters accusations of “trashing the place”

# DIGITAL FORENSICS CRYPTOGRAPHY

- Certifying digital evidence is not about obtaining a specific certification but rather following established protocols and best practices to ensure that the evidence is handled in a way that maintains its integrity and admissibility in legal proceedings.
- The court will determine whether the digital evidence is admissible.
- To be admissible, evidence must meet certain legal standards, including relevance and reliability.

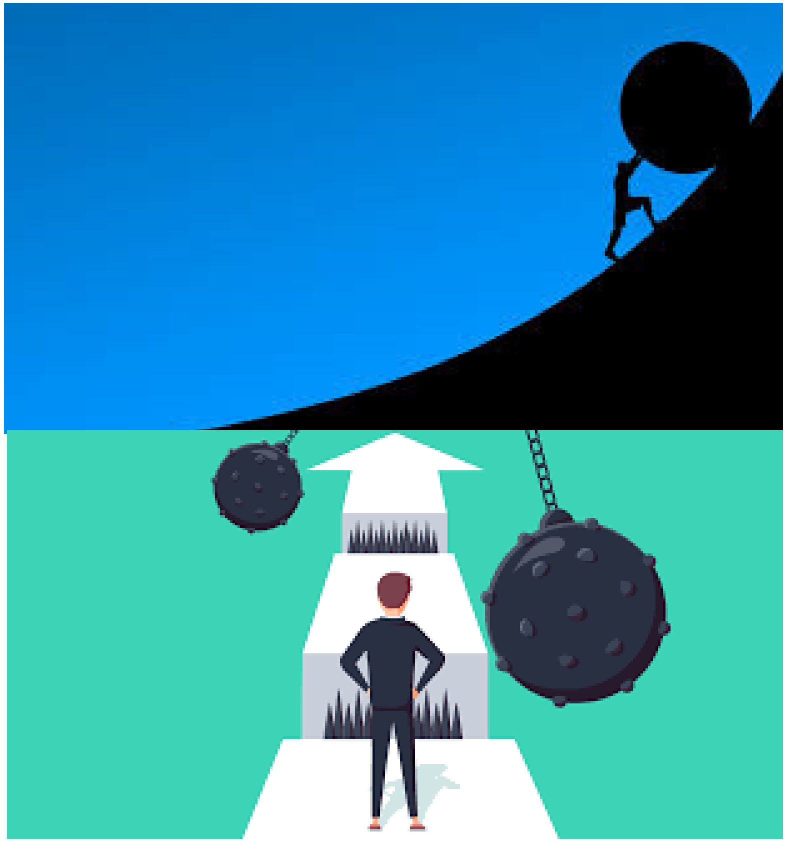


# BALISTIC & AFIS LAB



# CHALLENGES

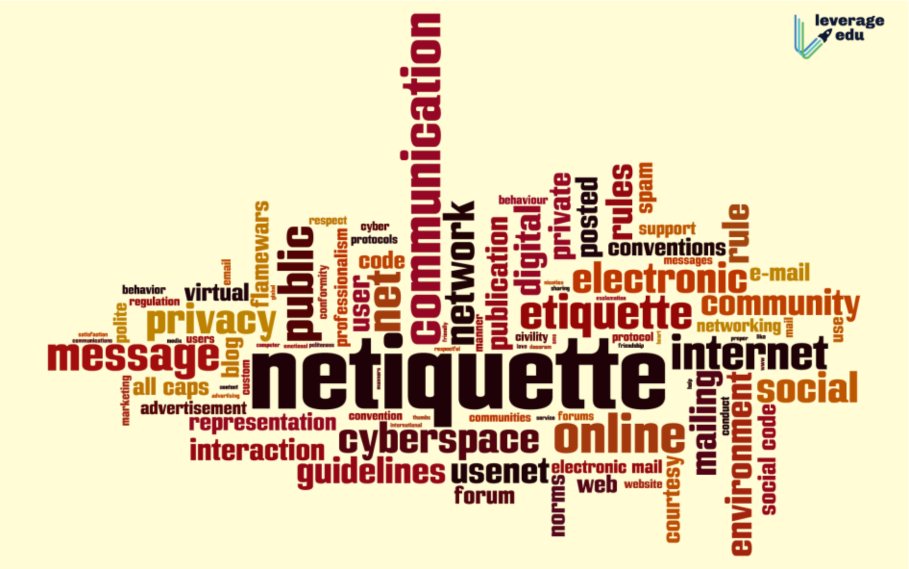
- Funding gaps
- Jurisdictional bottlenecks
- Consumer/user ignorance
- Skill gaps due to evolving technologies
- Inadequate digital forensic facilities



# CALL FOR ACTION

- Cooperation and collaboration with regional blocs such as EAPCCO & Interpol
- Harmonisation of legal frameworks at national, sub-regional, regional and international levels
- Domestic coordination. NISG & UG-CERT (National Information Security Group)
- Meaning engagement that influence global rules, norms and principles for responsible state behavior in cyberspace
- Development of cybersecurity expertise through innovation hubs, centres of excellence, upskilling, research and development

# NETIQUETTES



- Schedule breaks
- Unplug completely
- Consider noise-canceling devices
- Adjust or turn off notifications
- Reward yourself for focus
- Stop valuing the wrong things
- Stay informed and educated

# CONCLUSION

- A chain is as strong as its weakest link.
- Therefore, a breach from one person in a distributed environment will be to the detriment of the entire organization.
- Your passwords are like under garments, please change them regularly

THANK
YOU
GRACIAS
ARIGATO
SHUKURIA
DANKSCHEEN
BÎYAN
SHUKRIA
TASHAKKUR ATU
YÁQHANYELAY
SUKSAMA
GRAZIE
MEHRBANI
BOLZÏN
MERCI
JUSPAXAR
GOZAIMASHITA
EFCHARISTO