



Cybersecurity & Digital Forensics

Legal and Ethical issues Related to Digital Forensics

Catherine Bwire

(ITIL, CISA, CISM, CCNA, CEH, ISO27001, ISO27701 LI)

Department of Computing & Technology

Faculty of Engineering, Design & Technology

2025

A Complete Education for A Complete Person

P.O. Box 4, Mukono, Uganda, Plot 67-173, Bishop Tucker Road, Mukono Hill | Tel: +256 (0) 312 350 800 Email: info@ucu.ac.ug Web: <https://ucu.ac.ug>
Founded by the Province of the Church of Uganda. Chartered by the Government of Uganda



Lecture Introduction



- Digital Forensics is a vital tool in the fight against Cyber Crime, but it also raises legal and Ethical issues that need to be addressed.
- The legal issues related to Digital Forensics revolve around the admissibility of digital evidence in court, the Chain of Custody and the qualifications of the forensic examiner..

A Complete Education for A Complete Person

P.O. Box 4, Mukono, Uganda, Plot 67-173, Bishop Tucker Road, Mukono Hill | Tel: +256 (0) 312 350 800 Email: info@ucu.ac.ug Web: <https://ucu.ac.ug>
Founded by the Province of the Church of Uganda. Chartered by the Government of Uganda





Legal and Ethical issues

a) Admissibility of digital evidence in court

Digital Forensics involves the collecting, preserving, analyzing, and presenting digital evidence in court.

Therefore, to be admissible in court, evidence must be collected lawfully and preserved without changing or damaging it.

Additionally, a certified professional must analyze the evidence



Legal and Ethical issues

b) Chain of Custody

The Chain of Custody is another legal concern, as it must be documented and maintained for evidence to be admissible.

1. What is the Chain of Custody?
2. Why is it key in digital forensics investigations?



Legal and Ethical issues

b) Other Legal and Ethical Issues

Ethical issues related to Digital Forensics mainly involve;

a) privacy and confidentiality

The Digital Forensics investigator must respect the privacy of the individual and only collect data that is relevant to the investigation.

a) the use of forensic technology

Forensic Technology can be good, powerful and intrusive – Collecting data without individuals knowledge or consent. It is important that these are used responsibly and used only when necessary.

a) and the use of data collected.

The Forensic examiner must maintain the individual's confidentiality and ensure that the data is only used for the intended purpose.

We shall get to understand these better when we get to the Case studies and labs.



A Complete Education for A Complete Person
 P.O. Box 4, Mukono, Uganda, Plot 67-173, Bishop Tucker Road, Mukono Hill | Tel: +256 (0) 312 350 800 Email: info@ucu.ac.ug Web: <https://ucu.ac.ug>
 Founded by the Province of the Church of Uganda. Chartered by the Government of Uganda

Case Study: - Assignment 1

Facebook Cambridge Analytica Scandal Submission due date: s
 (7th February 2025 23:59hrs)

In 2018, it was discovered that Facebook had allowed the political consulting firm Cambridge Analytica to access the personal data of millions of users without their consent. This raised ethical issues about the use of personal data and the responsibility of companies to protect users' privacy. Digital Forensics was used to investigate the data breach and determine the extent of damage.

Questions:

1. What are some of the sensitive and personal data that may be collected during a digital Forensics Investigation?
2. How does Uganda's data privacy law address this type of case, and what rights does it grant to individuals? (Describe each of the rights in the context of the scenario mentioned above)
3. Discuss the role of the General Data Protection Regulation (GDPR) in addressing data privacy issues. How might the GDPR have influenced the outcome of the Cambridge Analytica case if it had been in effect at the time?



A Complete Education for A Complete Person
 P.O. Box 4, Mukono, Uganda, Plot 67-173, Bishop Tucker Road, Mukono Hill | Tel: +256 (0) 312 350 800 Email: info@ucu.ac.ug Web: <https://ucu.ac.ug>
 Founded by the Province of the Church of Uganda. Chartered by the Government of Uganda



What is Digital Evidence?

Digital Evidence is defined as any type of file stored on a device, such as a text file, a document, an image or an executable file.

It is any information of probative value that is either stored or transmitted in a digital form.

Locard's Exchange principle states that everyone who enters and exits a crime scene leaves something of themselves behind.



What is Digital Evidence?

Digital information can be gathered:

- From the media
- From the live capture of packets being transmitted
- From any other electronic source





Sources of Digital Evidence

Digital Evidence is found in files such as :

- Emails
- Log files
- Internet browser histories, cookies
- Graphic files
- Server logs



Sources of Digital Evidence *continued*

- Hard Disk

Mainly evidence that is gathered from hard disks of the seized system.

The data is stored in different file formats such as text, pictures, video files, computer program files etc.

- Thumb Drive

Thumb drive is another important electronic storage device with USB connection





Sources of Digital Evidence *continued*

- Memory Card

Memory card is a removeable electronic storage device, used in many devices such as digital cameras, PDAs, computers etc.

Data present in the memory card is not lost when power is turned off as it is a secondary storage

- Smart Card

A smart Card has memory and stores encryption keys or password and digital certificates



Sources of Digital Evidence *continued*

- Dongle

A copy protection device provided with software that is plugged into a computer port.

- Biometric Scanner

It is a device connected to a computer system that identifies the physical characteristics of an individual mainly for identification purposes





Sources of Digital Evidence *continued*

- Digital Camera – Images and videos

Evidence is found in images, removable cartridges, videos, sound, date and time stamp

- Modem

It is used by computers to communicate over telephone lines.

Evidence is found on the device itself.

- Printer

Printers contain memory buffers and store data.



Sources of Digital Evidence *continued*

- Scanner

It is an optional device connected to a computer, which scans documents and transmits to a computer network.

Even physical marks and damages on the scanner can become evidence





Characteristics of Digital Evidence

- Admissible

Evidence must be admissible in the courts of law and must be related to the fact being proved.

- Authentic

Evidence must be real and related to the incident

- Complete

Evidence must prove the attacker's action or his innocence



Characteristics of Digital Evidence *continued*

- 10 Reliable

There must be no doubt about the authenticity or veracity of the evidence

- 10 Believable

Evidence must be clear and understandable by the judges/jury

- 10 Reproducible

Evidence must be reproducible





**UGANDA CHRISTIAN
UNIVERSITY**
A Centre of Excellence in the Heart of Africa



NEXT TOPICS:

1. Basic Concepts of digital forensics and Digital Evidence
2. Rule of evidence and antiforensics



Uganda Christian University

P.O. Box 4 Mukono, Uganda

Tel: 256-312-350800

<https://ucu.ac.ug/> Email: info@ucu.ac.ug

[f](#) @ugandachristianuniversity [t](#) @UCUniversity

[v](#) @UgandaChristianUniversity



Department of Computing & Technology

FACULTY OF ENGINEERING, DESIGN AND TECHNOLOGY

Tel: +256 (0) 312 350 863 | WhatsApp: +256 (0) 708 114 300

[f](#) @ucuc Computeng [t](#) @ucu_ComputEng

<https://cse.ucu.ac.ug/> Email: dct-info@ucu.ac.ug



A Complete Education for A Complete Person

P.O. Box 4, Mukono, Uganda, Plot 67-173, Bishop Tucker Road, Mukono Hill | Tel: +256 (0) 312 350 800 Email: info@ucu.ac.ug Web: <https://ucu.ac.ug>
Founded by the Province of the Church of Uganda. Chartered by the Government of Uganda