Computer Forensics and Information Systems Auditing

A presentation to ISACA Kampala Chapter
By Isaac Kayemba, CISA, EnCE
Presentation outline

✓ Computer Forensics Defined
✓ Application of Computer Forensics
✓ Computer Forensics Requirements
✓ Legal Framework impacting on Computer Forensics in Uganda.
✓ Link between Computer Forensic and IT/IS Auditing
Computer Forensics Definition

Computer forensics is the process of extracting information and data from digital storage media using court validated tools and technology and proven forensic best practices to establish its accuracy and reliability for the purpose of reporting on the same as evidence. (ISACA guidelines)
Definition (cont)

What Constitutes Digital Evidence?

• Any information being subject to human intervention or not, that can be extracted from a computer.
• Must be in human-readable format or capable of being interpreted by a person with expertise in the subject.
Definition (cont)

• Computer Forensics Examples
  ✓ Recovering thousands of deleted emails
  ✓ Performing investigation post employment termination
  ✓ Recovering evidence post formatting hard drive
  ✓ Performing investigation after multiple users had taken over the system
Who Uses Computer Forensics?

• **Criminal Prosecutors**
  ✓ Rely on evidence obtained from a computer to prosecute suspects and use as evidence.

• **Civil Litigations**
  ✓ Personal and business data discovered on a computer can be used in fraud, divorce, harassment, or discrimination cases.

• **Private Corporations**
  ✓ Obtained evidence from employee computers can be used as evidence in harassment, fraud, and embezzlement cases.
Who Uses Computer Forensics? (cont)

• Law Enforcement Officials
  ✓ Rely on computer forensics to backup search warrants and post-seizure handling

• Individual/Private Citizens
  ✓ Obtain the services of professional computer forensic specialists to support claims of harassment, abuse, or wrongful termination from employment
Computer Forensic Requirements

• Hardware
  ✓ Familiarity with all internal and external devices/components of a computer
  ✓ Thorough understanding of hard drives and settings
  ✓ Understanding motherboards and the various chipsets used
  ✓ Power connections
  ✓ Memory
Computer Forensic Requirements (cont)

- BIOS
  - Understanding how the BIOS works
  - Familiarity with the various settings and limitations of the BIOS

- Operation Systems
  - Windows,95/98/ME/NT/2000/2003/XP/VISTA/7
  - DOS
  - UNIX,LINUX
  - MAC
Computer Forensic Requirements (cont)

- **Software**
  - Familiarity with most popular software packages such as Office.

- **Forensic Tools**
  - Familiarity with computer forensic techniques and the software packages that could be used
Legal Framework

Uganda's Parliament passed into law the following bills.

- electronic transactions bills
- electronic signature bills.
- The computer misuse bill

Implications

- There is now going to be legal recognition for some of the things we already do electronically,
- the new laws will allow prosecution of cyber/computer related crimes
- Computer Forensic Investigations shall gain prominence
Computer Forensics and IT/IS Auditing

- ISACA recognises the area of computer forensics and thus provides for it in its guidance for the performance of IT Audits.

Refer to:
The ISACA ‘IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals’ (G28, Computer Forensics)
Thank you.......very Much