HORIZONT 3000

Leveraging Digital Forensics in Fraud Investigations

TRAINERS:

JOHN SEMAKULA | CATHERINE NABIFO

Learning outcomes

- Understand what forensics is and the capabilities
- Identify potential sources of evidence and pinpoint electronic evidence
- Understand data storage structures
- Collect and preserve electronic evidence in a forensically sound manner
- Apply forensic techniques to locate and restore hidden or deleted data
- Acquire and analyse forensic data such as email analysis

Digital forensics overview

Forensics is the application of scientific techniques and methodologies to matters of law

Digital forensics is the scientific acquisition, analysis, and preservation of data contained in electronic media whose information can be used as evidence in a court of law

Forms of digital forensics

Computer Forensics

Email Forensics

Network Forensics

Database Forensics

Mobile Forensics

Application of forensics in fraud investigations

- Computer Intrusion
- Identity theft
- E-mail Threats, Harassment, and Stalking
- Online or Economic Fraud
- Theft of Information Assets
- Forgeries of Documents
- Malicious File Identification

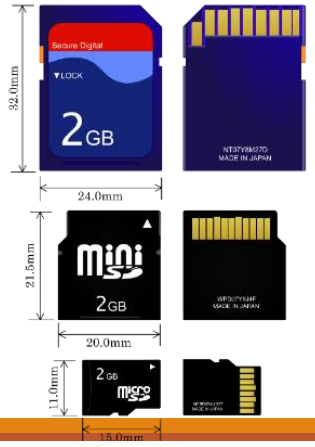
Why Digital Forensics ?

- Fraud perpetration and inappropriate usage of computer resources detection.
- Recovery of Data lost intentionally or accidentally and identification of the cause for data loss.
- Preserving the integrity of the evidence collected
- Evidence in most organizational fraud cases is in digital form. Thus a knowledge of basic forensics is necessary to enable auditors and investigators to efficiently obtain, manage and analyse digital evidence

Fortes of digital forensics

- Image / duplicate / clone storage devices
- Traversing the computer file system
- Recovery of deleted files
- Reconstruction of disk partitions
- Querying the computer registry
- Search slack and unallocated space

Sources of Electronic Evidence



Targeted Data/Information Sources

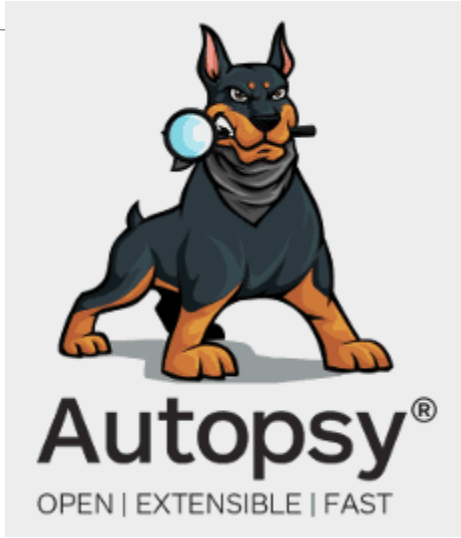
How Computers Work!

- Basic operations
  - Input
  - Out
  - Processing
- File systems
- Operating systems

Computer Forensic Tools

Open source tools

- Helix forensic cd
- The Sleuth Kit (Autopsy)
- WinHex viewer



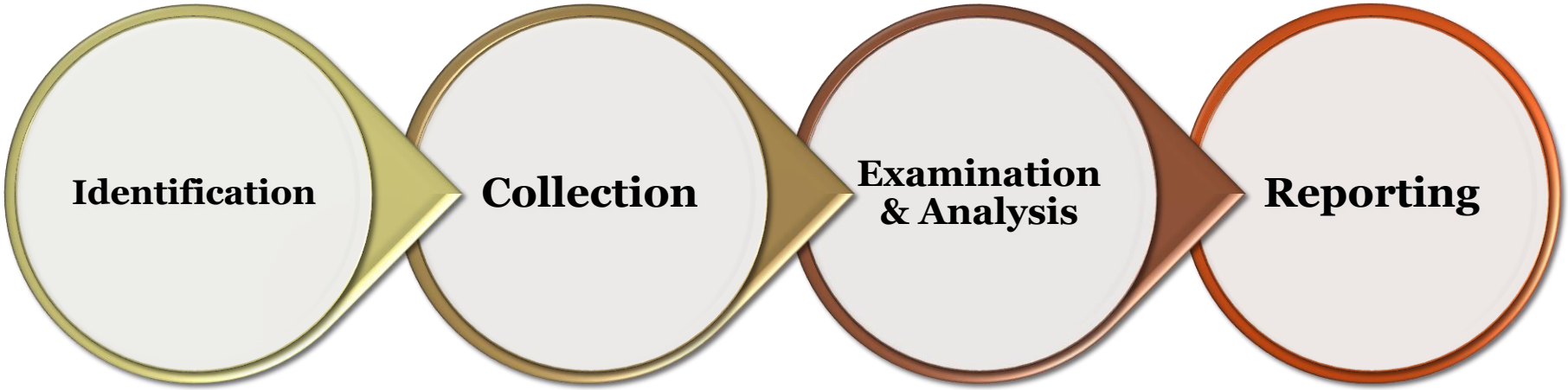
Commercial tools

- Opentext - Encase
- Access Data Forensic Tool Kit
- Paraben Forensic Software
- Cellebrite
- Oxygen forensics

OXYGEN FORENSICS
Helping good people make this world safer

opentext™ | EnCase™

Digital Forensic Process



Gathering & Preserving Electronic Evidence

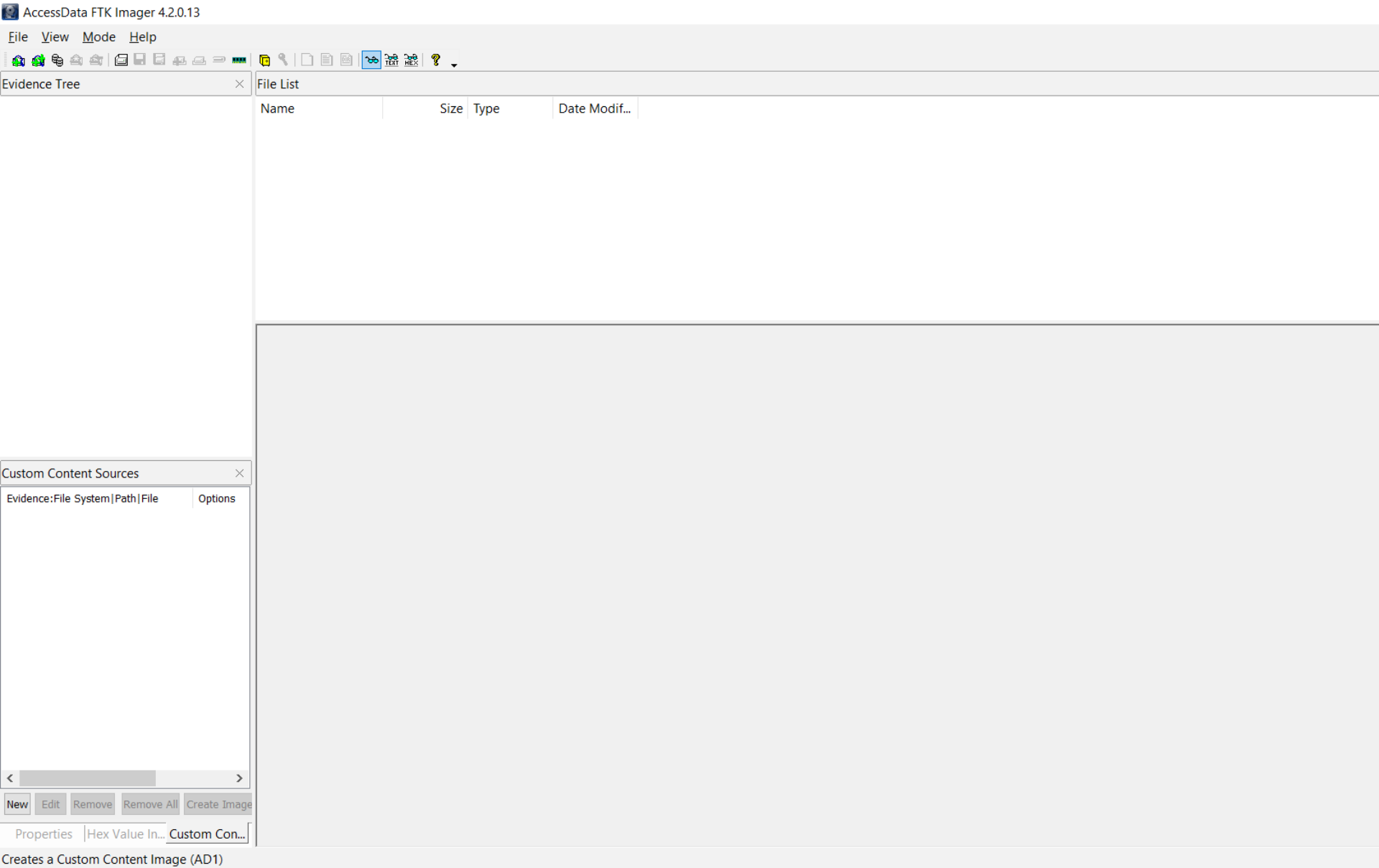
- Legal right to search and seize and scope of search
- System inspection; connections; network; power considerations
- Caution – safety and security
- Document who is involved, state of crime scene
- Protected content e.g. medical content; lawyers - attorney client privileges
- Best evidence rule – proper hash validation where original isn't available
- Order of volatility; Encryption

GATHERING AND PRESERVING ELECTRONIC EVIDENCE

Ensure that the chain of custody is maintained

Device Forensic Imaging

Forensic Imaging



Practical Session

Further reading

- **How Computers Work, Compilation Video of Basics Explained**

  https://www.youtube.com/watch?v=Rv73ki6fTuo

- **How do SSDs Work**

  https://www.youtube.com/watch?v=5Mh30886qpg

- **Forensic Acquisition in Windows - FTK Imager**

  https://www.youtube.com/watch?v=TkG4JqUcx_U

- FTK Imager User guide

- Kearns, G. (2015) 'Computer Forensic Projects for Accountants', *Journal of Digital Forensics, Security and Law* [Preprint]. Available at: https://doi.org/10.15394/jdfsl.2015.1203.

- Pearson, T.A. and Singleton, T.W. (2008) 'Fraud and Forensic Accounting in the Digital Environment', *Issues in Accounting Education*, 23(4), pp. 545–559. Available at: https://doi.org/10.2308/iace.2008.23.4.545.

- Coglitore, F.J. & Matson, D.M. (2007). The use of computer-assisted auditing techniques in the auditing course: Further evidence. Journal of Forensic Accounting, VIIII, 201-226.


thank
you