BIG DATA ANALYTICS IN FORENSIC AUDIT

Presented in Mombasa

Uphold public interest

Nasumba Kwatukha Kizito

CPA,CIA,CISA,CISI,CRMA,CISM,CISSP,CFE,IIK

Internal Audit, Risk and Compliance

Strathmore University

Uphold public interest

Menu .....

- Introduction
- Big Data
- Conclusion
- Question and Answer

Why Data .....

1. Support facts of the case
2. Help secure admissibility
3. Understand modus operandi
4. Punching board by the legal team

Admissibility test....

Documents are relevant to the case- Check papers; check recommendations and check the purpose

Relevant to the case at Hand - Avoid decoys

Reliable – trace the source and authenticity

Ways of analysis and investigation ....

- Covert
- Overt
- Follow facts at a distance and understand the deal breaker
- Be in the shoe of the cross examiner and the accused

Data Analytics ....

Data Analytics is....

Data analytics is the pursuit of extracting meaningful information from raw data using specialized computer systems.

Business intelligence and Artificial intelligence

It is not evidence in itself but provides information to be corelated

Forensic is....

Application of techniques to get an admission: Co-relate facts with the witness some are hostile and some are not

Ultimate consumer of any investigation are the courts and so **data and facts** become very critical

There needs to be a difference between Audit; Special Audit and Investigation

Forensic Data Analysis ....

Forensic Data Analysis (FDA) is a branch of Digital **forensics**. It examines structured **data** with regard to incidents of financial crime. The aim is to discover and analyze patterns of fraudulent activities.

Importance of Forensic Data Analytics.....

- Reserving Digital Data in its original format
- It is a critical game changer in any investigation
- Helps in decision making (Critical)
- Remember that proof is beyond reasonable doubt

Steps in Forensic Data Analytics .....

1. Formulate Objectives- based on hypothesis
2. Make a decision on the objectives-shut the computer
3. Identify the Unanswered questions through imaging
4. Determine where to get the data
5. What technology to use in getting the data
6. Implementation Plan
7. Remember to avoid decoys and re-adjust accordingly

Where to get the data .....

1. Computers: Switch off immediately to reserve data ; be good at imaging and Analyse with forensic tools

2. Phones- Data administrator remotely

3. Networks :Net Maps. Reserve the ports

4. Cloud storage : review the storage arrangement

Forensic Data Collection .....

Is the process of preserving or collecting data from a computer or electronic device for later analysis and investigation.

Tools for Forensic Data Collection .....

A good analytical tool should be able to store data in its original form. Some of them include;

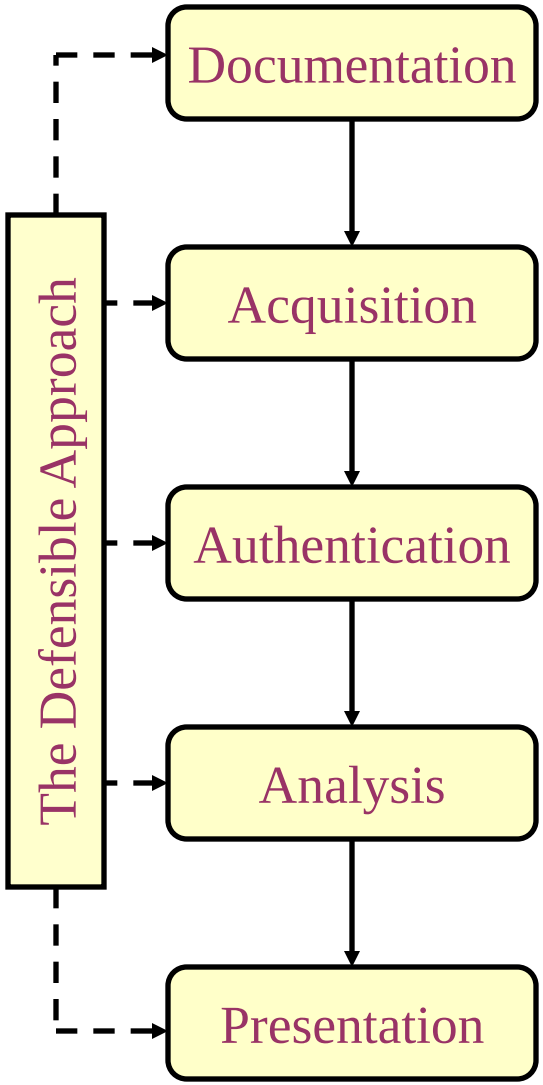
- Forensic tool kit-FTK
- ProDiscover Forensic
- Volatility Framework
- The Sleuth Kit (+Autopsy)
- Encase
- X-Ways Forensics

Computer Forensics Procedure

- Verify Legal Authority
- Search warrants
- Photographing
- Documentation

- Hash verification
- CRC/MD5/SHA1
- Documentation

- Interpret and report
- Present and defend



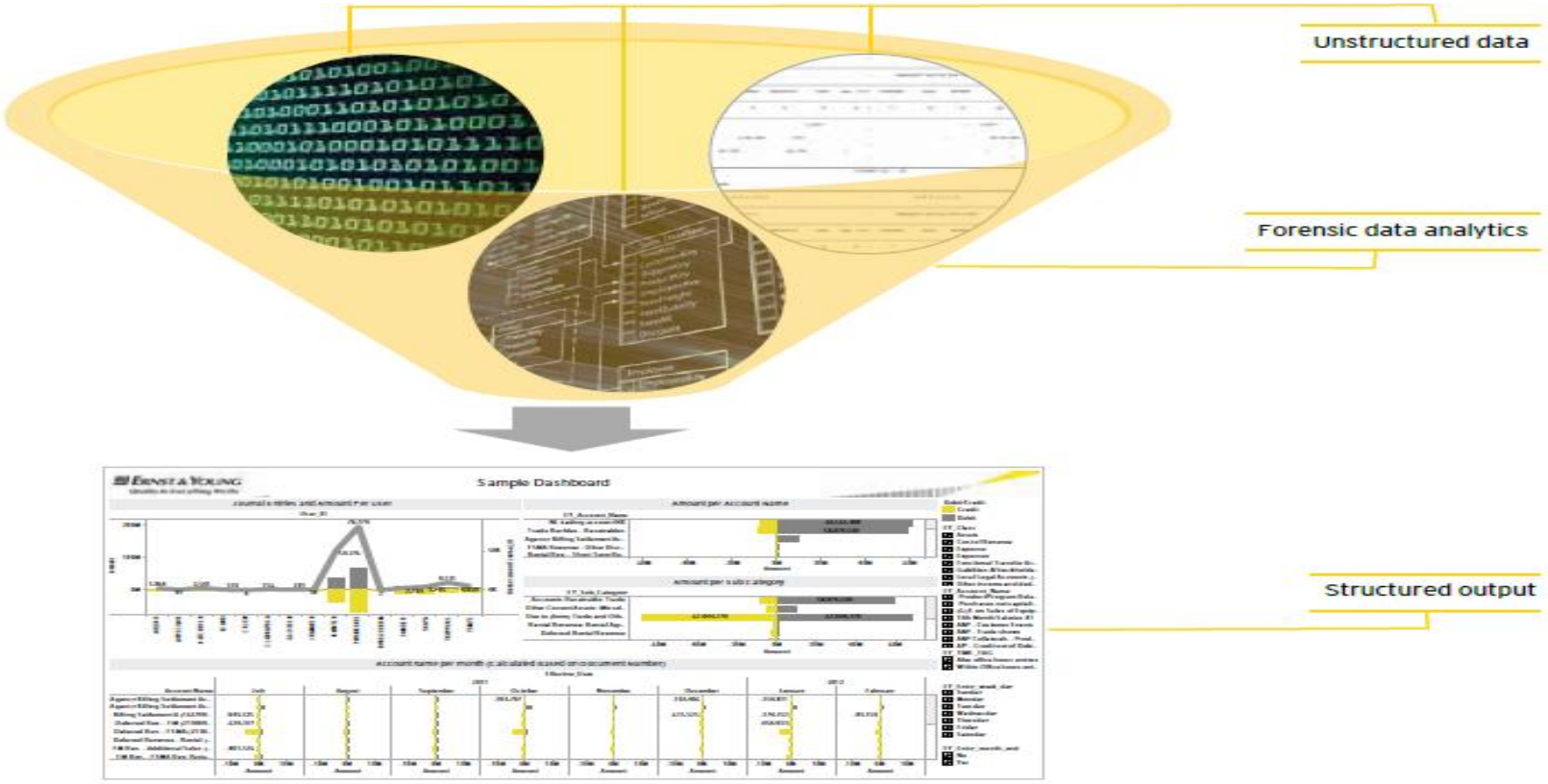
- Location, date, time, witnesses
- System information, status
- Physical evidence collected

- Forensically wipe storage drive
- Bit-stream Imaging
- Documentation
- **Chain of custody**

- Retain the integrity
- Filtering out irrelevant data
- What could/could not have happened
- Be objective and unbiased
- Documentation

Out Puts;

- *"The key to identify fraud lies in the ability to comprehend what lies beneath."*



Out put uses....

- Audit Purposes: Decision Making
- Investigative Purposes: As Evidence where it has to be **admissible,** hence reliable, original, consistent
- Also confirm if you are admissible yourself and the methodology is acceptable

Approaches in Data Analysis.....

- Link Analysis – Evaluates relationships
- Social Network Analysis – Evaluates relationships in network theory among groups of people
- Concept Clustering Analysis – Grouping Similar entities and clusters to identify anomalies
- Sentiments Analysis – Identify and extract subjective information

How is Data Analytics useful in Fraud Prevention ....

- Proactive fraud prevention management
- Controlling the magnitude of fraud in a reactive set up
- Effective and focused internal controls
- Improving regulatory and compliance environment

Value of Forensic Analytics....

"The greatest value of forensic analytics is when it forces us to notice what we did not expect to see."

Useful in secretive Investigation

Q & A ?

Nasumba Kwatukha Kizito

CPA,CIA,CISA,CISI,CRMA,CISM,CISSP,CFE,IIK

Executive Director

Internal Audit, Risk and Compliance

Strathmore University