ICPAK

Credibility . Professionalism . AccountAbility

INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS OF KENYA

Forensic Audit Workshop

18th – 19th October 2017

Waterbuck Hotel - Nakuru

It Tools, Techniques and Use of Technology as drivers for Fraud detection and Investigation

CPA Kennedy Waituika, CFE

Credibility . Professionalism . AccountAbility

Technology – is it important in Fraud Prevention and Detection?

How do I control the cost without increasing risk?

How do I analyse and review large amounts of data quickly and efficiently?

How can I identify, preserve and capture relevant information and records?

When can we apply technology

- Proactive- Use of technology to detect fraud on a continuous basis. Analytics, Intelligence Analysis and Monitoring.

- Reactive- use of technology to respond to incidences of fraud/Investigation. Extracting information, analyzing data, preserving information for court purposes

Who uses Technology

- Organisations – Proactive fraud detection using data analytics, Performing special audits in regard to a range of criminal activity: theft, embezzlement, misappropriation of trade secrets;
- Law enforcement - Require F-tech services in pre-search warrant preparations and post seizure handling of computer equipment;
- Individuals - Hire computer forensic specialists in support pf possible claims of: wrongful dismissal, harassment or discrimination; and
- Civil litigators - Make use of personal and business records found on computer systems that support: fraud and harassment cases.

Most of our activities nowadays (including fraud) leave a digital footprint – Importance of Forensic Technology and related technology can only increase.

What are the trends in technology-based fraud?

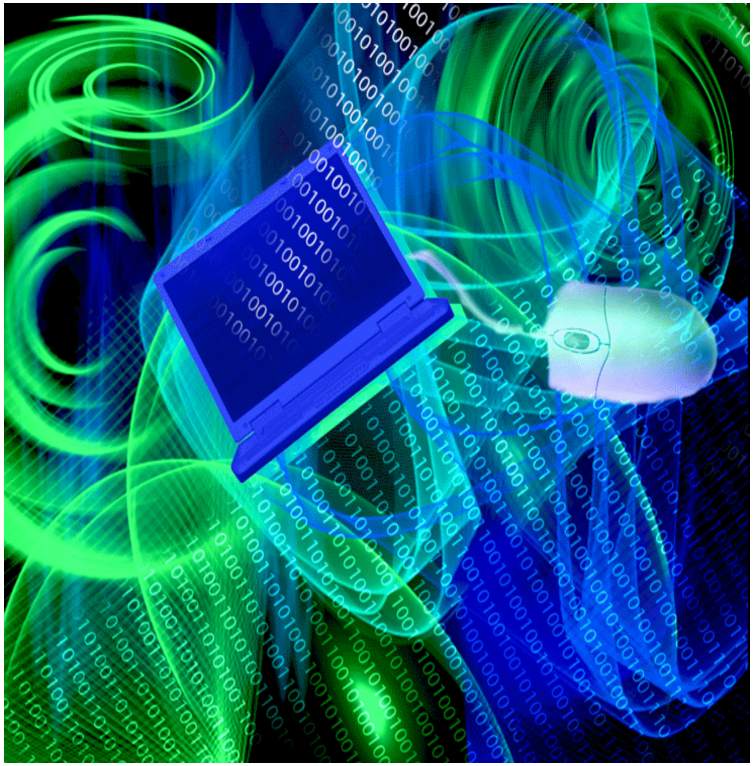
- Fraudsters have embraced technology and use it to perpetrate fraud from even remote locations.
- Some of the new trends in technology based fraud include:

✓Use of spyware to steal information e.g. bank transfer passwords;

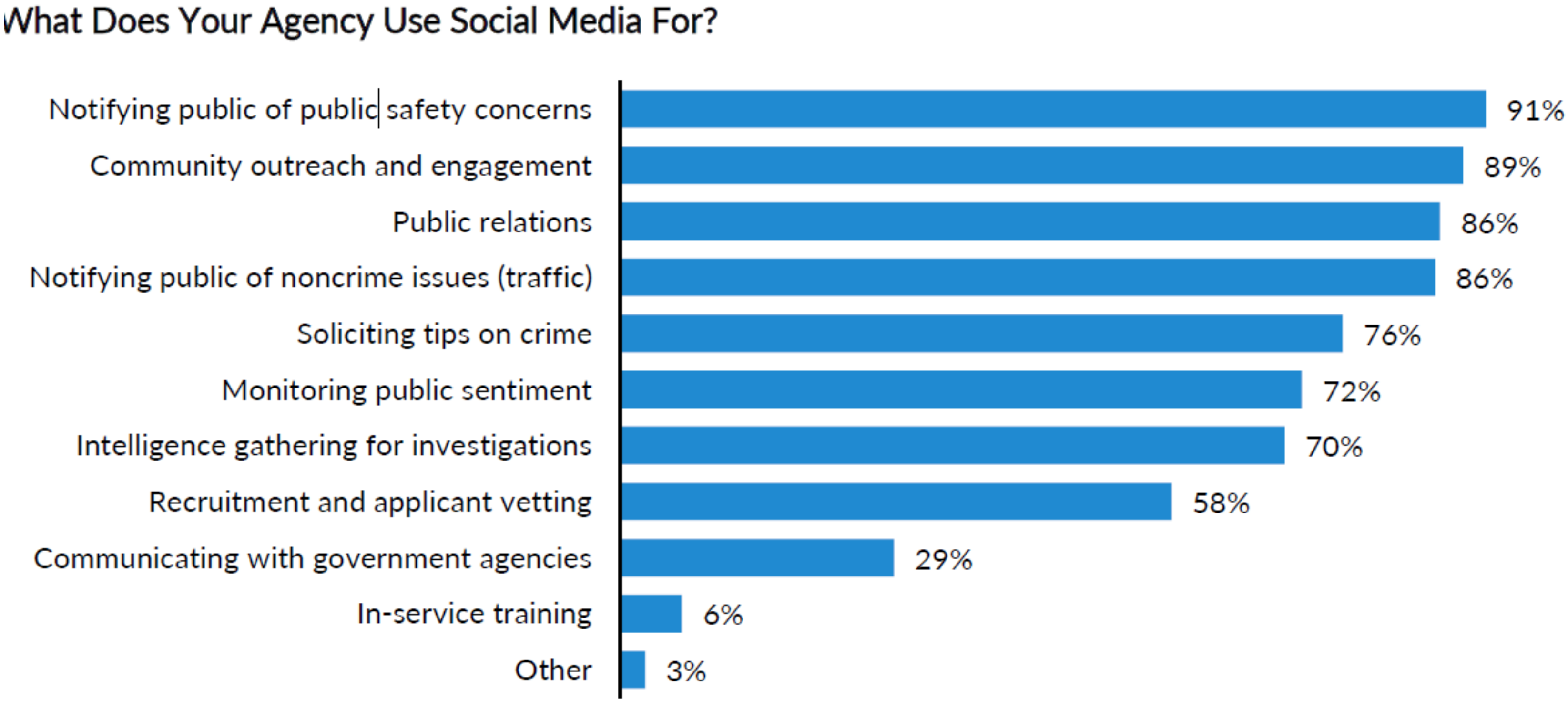
✓Remote access of an organization's system;

✓Phishing of emails; and

✓Tampering of electronic records.



Rising importance of social media and cloud data



Vhat Does Your Agency Use Social Media For?

Source: 2016 Law Enforcement Use of Social Media Survey - International Association of Chiefs of Police and the Urban Institute

Use of technology to detect fraud on a continuous basis

Technology tools available – Data Analytics

ACL

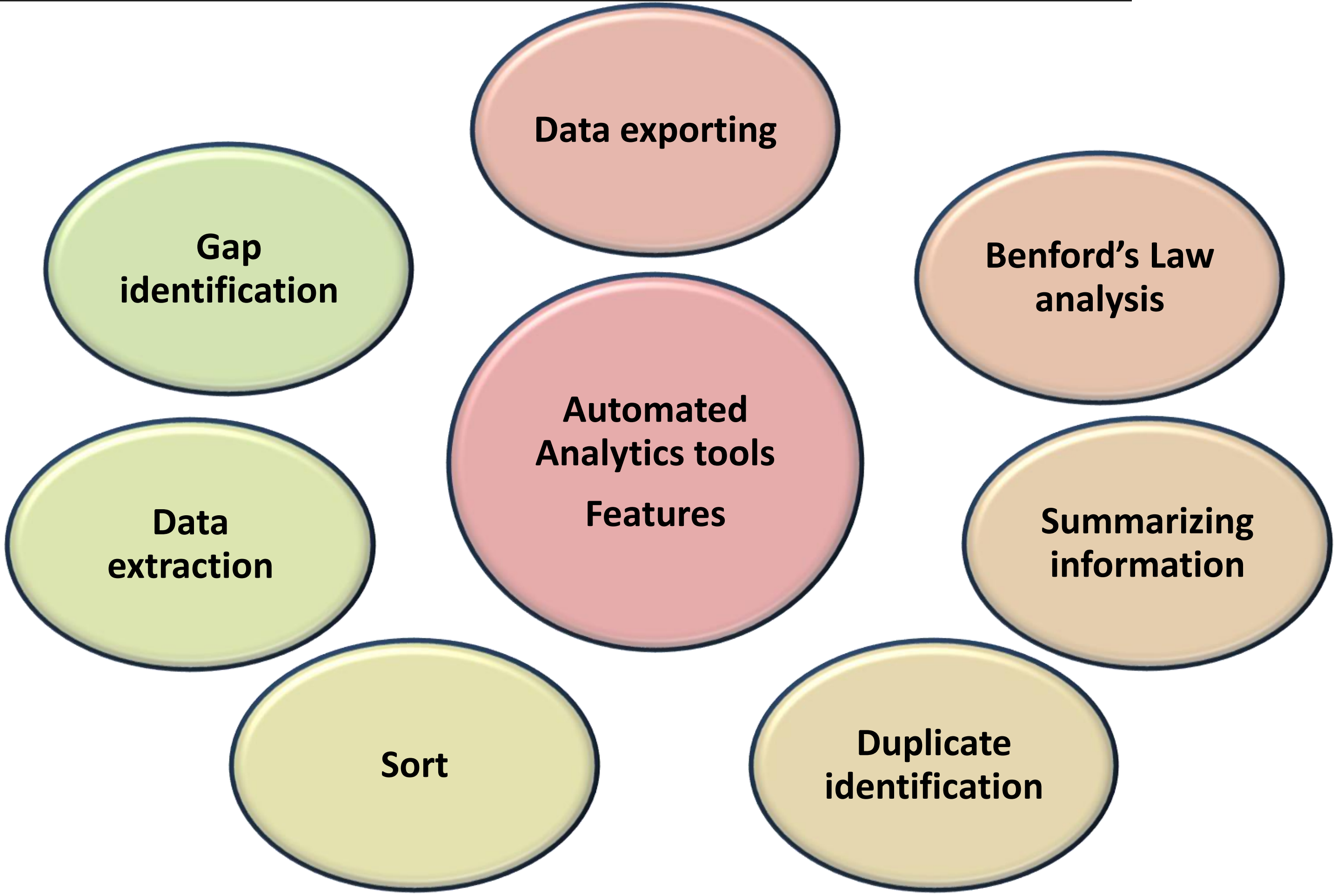
IDEA

Interactive Data Extraction and Analysis

ActiveData for Excel

Microsoft Excel

Analytics tools - Capabilities



Automated Analytics tools

Features

Data exporting

Benford’s Law analysis

Summarizing information

Duplicate identification

Sort

Data extraction

Gap identification

Data Analytics- Types of Data That Can Be Analyzed

Relevant data comes from numerous sources and takes numerous forms:

- Accounting and financial data
- Human resources data
- Customer data
- Vendor data
- Internal communications and documents
- External benchmarking data

Analytical Techniques for Fraud Detection

Prior to analysis, the special auditor must consider:

Which areas can fraud occur?

What fraudulent activity would look like in the data?

What data sources are required to test for indicators of fraud?

Analytical Techniques for Fraud Detection

The following analytical techniques are effective in detecting Fraud

Statistical parameters

Calculation of statistical parameters (e.g., averages, standard deviations, high/low values) – to identify outliers that could indicate fraud.

Benford’s law

Digital analysis using Benford’s Law – to identify unexpected occurrences of digits in naturally occurring data sets.

Stratification

Stratification of numbers – to identify unusual (i.e., excessively high or low) entries.

Classification

Classification – to find patterns amongst data elements.

Examples of analysis – analytics tests

Cash

- ✓ Identify cash transactions just below certain approval thresholds.
- ✓ Identify a series of cash disbursements to one specific vendor or staff at specific time
- ✓ Identify Cash transactions approved by one particular staff

Procurement

- ✓ Identify transactions with vendors not on prequalified list by matching list of prequalified supplies with all vendors paid in the period.
- ✓ Identify vendors with similar addresses or contact information
- ✓ Identify vendors with bank details or contact information with staff member

Examples of analysis – analytics tests

Payroll

- ✓ Ghost workers
- ✓ Unreasonable overtime
- ✓ Double payments – employees with similar bank accounts

Invoicing/payments

- ✓ Multiple invoices with same item description
- ✓ Invoice with same amount, paid on the same day
- ✓ Multiple invoices with same PO reference, same date
- ✓ Invoice with PO numbers outside current range
- ✓ POs with numbers outside range for particular period

Examples of analysis – analytics tests

Cash

- ✓ Identify cash transactions just below certain approval thresholds.
- ✓ Identify a series of cash disbursements to one specific vendor or staff at specific time
- ✓ Identify Cash transactions approved by one particular staff

Procurement

- ✓ Identify transactions with vendors not on prequalified list by matching list of prequalified supplies with all vendors paid in the period.
- ✓ Identify vendors with similar addresses or contact information
- ✓ Identify vendors with bank details or contact information with staff member

Examples of analysis – Benford Analysis

States that the leading digit in some numerical series is follows an exponential rather than normal distribution

Applies to a wide variety of figures: financial results, electricity bills, street addresses, stock prices, population numbers, death rates, lengths of rivers

Leading Digit	Probability
1	30.1 %
2	17.6 %
3	12.5 %
4	9.7 %
5	7.9 %
6	6.7 %
7	5.8 %
8	5.1 %
9	4.6 %

Using Data Analytics for Fraud Auditing – points to note

- Effective data analysis requires:
- Translating knowledge of organization and common fraud indicators into analytics tests
- Effectively using technological tools
- Resolving errors in data output due to incorrect logic or scripts
- Applying fraud investigation skills to the data analysis results to detect potential instances of fraud
- Data analysis techniques alone are unlikely to detect fraud; human judgment is needed to decipher results.

Reactive- use of technology to respond to incidences of fraud/Investigation

Potential sources of electronic evidence

- Digital evidence recovery will be used in investigations where potentially relevant information may reside on electronic media e.g.

✓ Desktop computers;

✓ Laptops;

✓ T24 Servers

✓ File and corporate servers;

✓ Mobile devices (such as PDAs, phones etc); and

✓ Portable media (such as memory cards, DVD etc.)

✓ Printers and scanners

✓ Cloud storage

Possible types of systems and data

- An investigation team will likely come across the following types of data:
  - Operating system log files
  - Emails and instant messages;
  - Documents e.g. Word, PDF, PowerPoint
  - Multimedia files e.g. JPEG, TIFF, AVI, MP4
  - Relational data e.g. Access database, SQL dump
  - SMS and chat messages
  - Internet history
  - Print spoolers
  - Temporary files and or auto recovery files

Technology tools available – digital forensics

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

Phases of Digital Forensics

Three Phases:

- Preserve & Document Scene
- Analyze/Search & Document Data
- Reconstruct & Document Fraud Event

Extract, process, interpret

- Work on the imaged data or “safe copy”
- Data extracted may be in binary form
- Process data to convert it to understandable form
  - Reverse-engineer to extract disk partition information, file systems, directories, files, etc
  - Software available for this purpose
- Interpret the data – search for key words, phrases, etc.

Technology tools available – digital forensics

- Forensic Explorer – data extraction
- Nuix – very powerful for analyzing emails
- Access Data’s Forensic Toolkit (FTK)
- EnCase Cybersecurity
- EnCase eDiscovery
- EnCase Portable
- EnCase Forensic
- ArcSight Logger
- Netwitness Investigator
- Quest Change Auditor
- Cellebrite
- Physical Analyzer
- Lantern

Digital Forensics Capabilities

- Recover deleted files
- Find out what external devices have been attached and what users accessed them
- Determine what programs ran
- Recover webpages
- Recover emails and users who read them
- Recover chat logs
- Determine file servers used
- Discover document’s hidden history
- Recover phone records and SMS text messages from mobile devices
- Find malware and data collected
- Analytics of both structured and unstructured data

Key characteristics of electronic evidence

Digital evidence differs from other types of evidence in that it:

- Is intangible;
- Is volatile;
- Is susceptible to manipulation;
- Can be located in any country in the world;
- Requires examination via the use of computer technology; and
- Tends to be transient in nature.

Key characteristics of electronic evidence

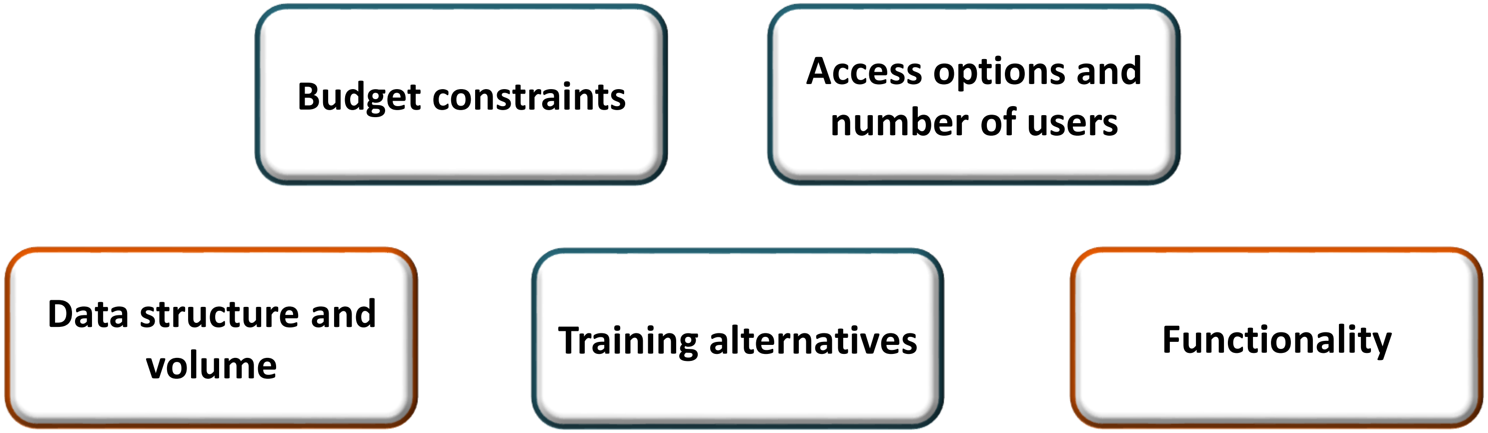
Digital evidence differs from other types of evidence in that it:

- Is intangible;
- Is volatile;
- Is susceptible to manipulation;
- Can be located in any country in the world;
- Requires examination via the use of computer technology; and
- Tends to be transient in nature.

Considerations when selecting a technology tool

Prior to selection of a suitable automate tool, management must consider certain factors affecting the organization.

The considerations include:



Budget constraints

Access options and number of users

Data structure and volume

Training alternatives

Functionality

The rules of evidence – why we need to be careful

- Admissible

✓ Does it meet the standards of a set of legal rules used by the legal system?

- Relevant

✓ Does the material make some fact that is of consequence to the legal dispute more or less probable that it otherwise would be?

- Authentic

✓ Does the material come from where it purports?

- Reliability:

✓ Are there reasons for doubting the correct working of the computer?

✓ Are we able generate accurate copies of records in both human readable and electronic form?

- Completeness:

✓ Is the story that the material purports to tell complete?

✓ Are there other stories that the material also tells that might have a bearing on the legal dispute or hearing?

Something to think about

….What fraud has that data analytics can never account for is the human behavior element…without having someone who has an expertise in knowing how fraudsters operate as well as someone who understands victimology, significant weaknesses are developed..

Where to find these tools

ACL
    http://www.acl.com/Default.aspx?bhcp=1

Eraser
    http://www.heidi.ie/eraser/

Private Disk
    http://www.private-disk.net/

HashCalc
    http://www.slavasoft.com/hashcalc/index.htm

PC Inspector
    http://www.download.com/3000-2242-10066144.html

VeriSign
    http://www.verisign.com

HandyBits Encryption
    http://www.handybits.com/

EnCase
    http://www.handybits.com/

IP tracking
    http://www.whatismyipaddress.com

Where to find these tools

Spector
http://www.spectorsoft.com/
Stolen ID Search
https://www.stolenidsearch.com/
Abika Background Check
http://www.abika.com/
Guide to Log Management
http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf
NetWitness
http://www.netwitness.com/
GASP Std V 7.0 Free Software
http://www.bsa.org/usa/antipiracy/Free-Software-Audit-Tools.cfm
Federal Guidelines for Searches
http://www.cybercrime.gov/searchmanual.htm
Recuva
www.piriform.com/recuva
DLP-Data loss prevention
www.websense.com

Contacts

Kennedy Waituika
Mob: +254 720572405
Email: kenwaituika@gmail.com