



Maximizing the Potential of Digital Forensics

Clear and focused attention

Moses Kiarie
Thursday, 19 November 2015



© 2015 Deloitte & Touche



Agenda

- “ Case Study
- “ Importance of Digital Forensic
- “ Admissibility of electronic evidence in Kenya
- “ Maximising digital forensic

Case study



Case study

Aaron, an IT expert, and Furaha a relationship manager, work for the same bank

Both Aaron and Furaha are suspected of involvement in fraud costing the bank KES 30 million

It is suspected that Aaron reported on duty as required and accessed the IT room and used an IP address while using the user identity of Furaha.

Case study

Aaron and Furaha are suspected to have colluded and transferred Sh30 million into offshore accounts disguised as forex transactions. This is suspected to have happened at various dates over a period of three months.

The plan was discovered through customer complaints on their account balances.

Case study

You have been called in to investigate.

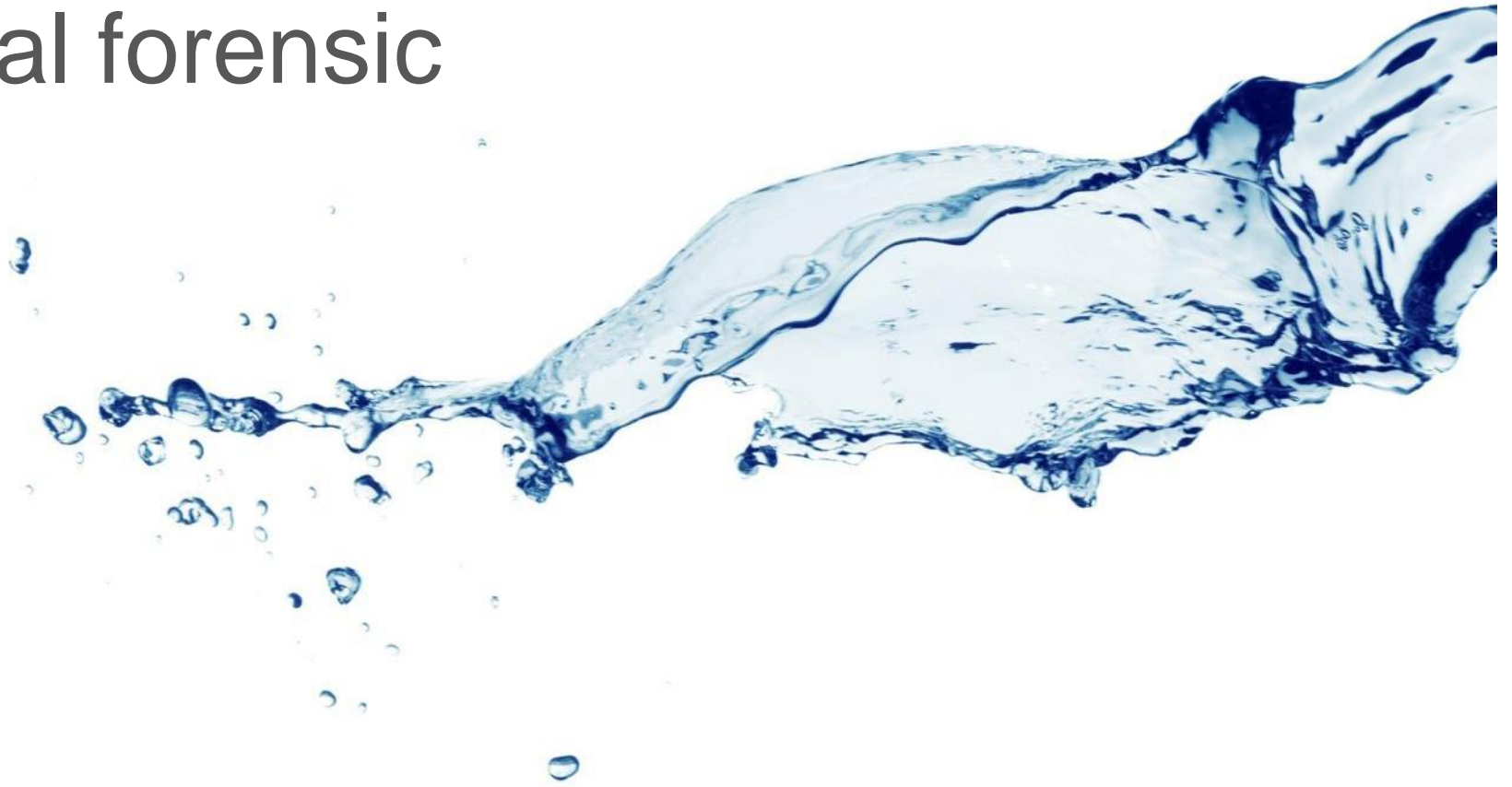
“ What would be the key elements of your investigation plan?

“ What evidence would you collect?

“ Which experts would you want as part of the team?

Introduction and importance

Digital forensic



Why digital forensic?



Why digital forensic?

Social Media



Instagram

News headlines

Bank employee
manipulates
system to defraud
customers

Student charged with
computer fraud in
grade-changing case

US Internal Revenue Service admits to much bigger
attack using stolen information ↗

September 2015

The US Internal Revenue Service (IRS) has revised the number of people
affected by scammers using stolen data back in May....

Infidelity website among latest breaches ↗

August 2015

As many as 37 million users of the Ashley Madison dating site – which
targets people looking to have extra-marital affairs – have had their
account details stolen by hackers....

Why digital forensic?

It takes a wide variety of skills and disciplines to move through a successful financial investigation

You don't need to be a computer forensics expert but you should understand:

**What they do,
how they do it; and
the tools of the trade**

Why digital forensic?

Whether your expertise is in law, audit or another anti-fraud field, as a fraud fighting professional you know how important digital evidence has become in fraud investigations

Admissibility of electronic evidence in Kenya



Laws of Kenya

Some of the relevant laws:

“ Evidence Act (CAP 80)

“ Kenya Information and Communications Act (CAP 411A)



Laws of Kenya . Evidence Act

The Evidence Act

- “ **Section 78A: Admissibility of electronic and digital evidence** - electronic messages and digital material shall be admissible as evidence
- “ **Section 106B: Admissibility of electronic records** – an electronic recording in a computerized system shall be deemed to be a document and admissible as evidence in Court if it meets the requirements



Laws of Kenya . Evidence Act

Section 78A requirements:

- “ The reliability of the manner in which the electronic and digital evidence was **generated, stored or communicated**;
- “ The reliability of the manner in which the **integrity** of the **electronic and digital evidence was maintained**;
- “ The manner in which the **originator** of the electronic and digital evidence was **identified**; etc

Laws of Kenya . Conclusion

- “ Electronic evidence acquired by an investigator is admissible in Court
- “ However, it must be adduced in accordance with the stringent rules provided in the Evidence Act

Maximising digital forensic



Digital forensic capabilities

- “ Deleted files and other data that has not been overwritten
- “ Temporary auto-save files
- “ Print-spool files
- “ Websites visited, even where the browser history and cache have been deleted
- “ Financial-based Internet transactions
- “ Documents, letters, and images created, modified, or accessed on the computer
- “ The time and date information about files

Digital forensic . Caveats

Digital evidence is more volatile than paper information; therefore, it can be easily altered or destroyed.

” Integrity must be preserved.

” If files are destroyed, it can give rise to a claim of *spoliation of evidence*.

Question

Turning on or tuning off a computer has little effect on the files contained on the computer system.

A. True

B. False

Explain



Digital forensic

If authenticity is not supported or proven, evidence will be inadmissible.

To be admissible, evidence must be:

- ” Relevant
- ” Material
- ” Established as authentic
- ” Legally obtained

Digital forensic . stages

- “ Seizing
- “ Imaging
- “ Analyzing
- “ Reporting and testifying



Digital forensic . Seizing

Document the scene with photographs or a diagram

Two %Golden Rules+should be followed:

1. %If the computer is off, don't turn it on.+
2. %Don't peek through the files.+

Digital forensic . Imaging

Image acquisition involves using a standalone hard drive duplicator; or

Similar device to duplicate a computer's entire drive without altering it.

Digital forensic . Analysing

Most time consuming phase

Best to use a combination of various forensic tools during the analysis phase.

Fraud examiners should look for both incriminating and exonerating evidence

Primary concern is to maintain the integrity of the data at all times.

Conclusion

- “ Importance of digital forensics
- “ Admissibility of digital evidence
- “ Maximising digital forensic

Deloitte.