Forensic. Advisory. Fraud

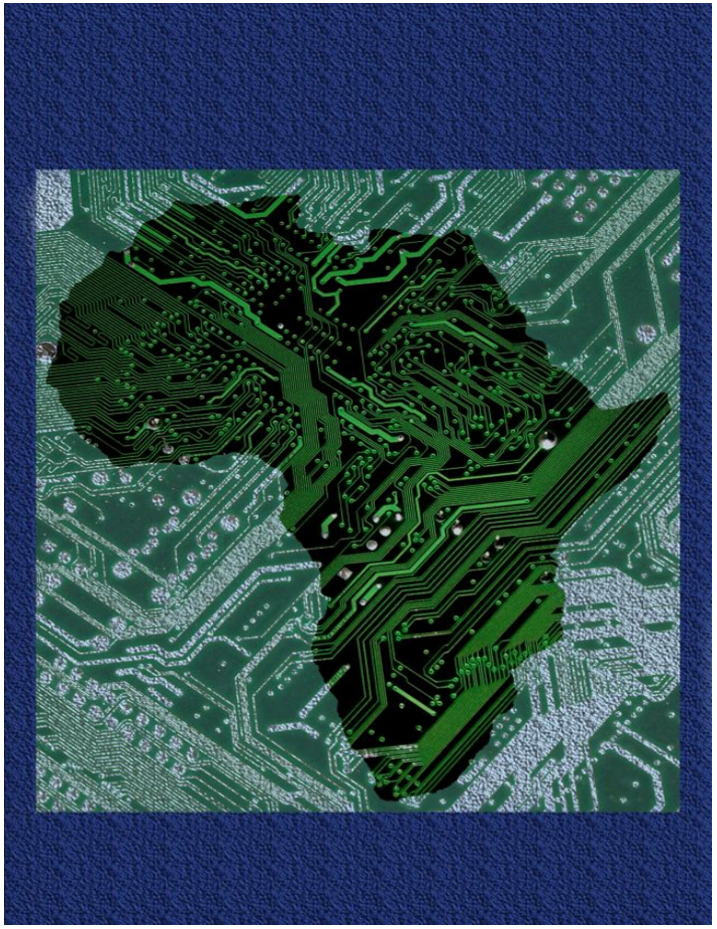
Today's Digital forensics & tools

summit consulting

Improving your condition

Mustapha Mugisa, CISA, CFE, CrFA, MBA

Forensic 2012 and beyond…



www.cits.co.za

summit consulting
www.summitcl.com

Our partners…

cellebrite
mobile data secured

nuix

Guidance SOFTWARE | EnCase

summit consulting

appin

tableau SOFTWARE

Overview

summit consulting

- Background
- Challenges
  - Non Technical
  - Technical
- Current day Cyber Crime
- Digital tools - overview

Background

Digital investigation

Answer questions about digital events

Digital forensic investigation

Answer questions about digital events so the results are admissible in court

Background

summit consulting

What is Forensic Science?

Forensic science involves the "collection, preservation and validation of evidence" as well as the "investigation and analysis of the data, and the preparation of a report for the authorities."

(SANS GIAC Forensics track description)

Background

"Digital evidence is any information of probative value that is either stored or transmitted in a binary form.

This field includes not only computers in the traditional sense but also any digital data format."

Forensic investigation…

In forensic, each point you write, provide evidence

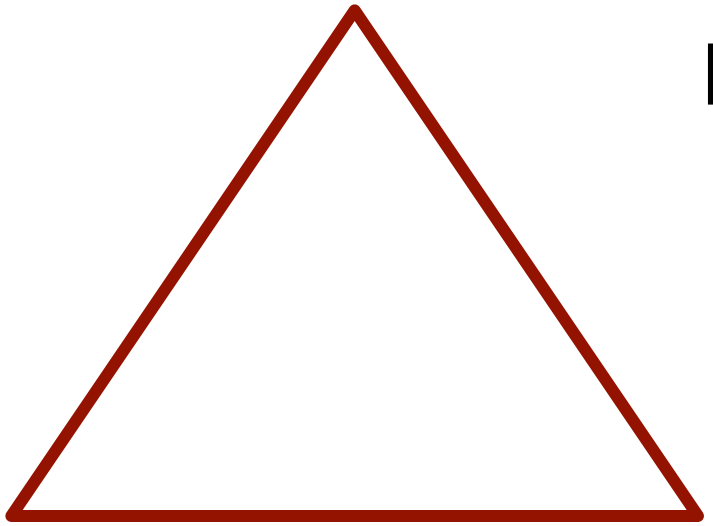
Very **adversarial** in nature

Are reactive other than proactive

Outcome assumption: ***the case will be determined in court***

It's all about facts seeking and no other.

Proving guilt…



Who, what, where, when, how?

Background

Reasons for a forensic analysis

- ID the perpetrator.
- ID the method/ vulnerability
- Conduct a damage assessment
- Preserve the evidence for legal action

Forensic investigation…

- Everything is material. Need great care & accuracy.
- Establish facts with evidence. ***Working documents*** must withstand detailed scrutiny.

Basic mistakes like **arithmetic errors** in reports, **straying outside expertise**, lack of objectivity, etc = no work done.

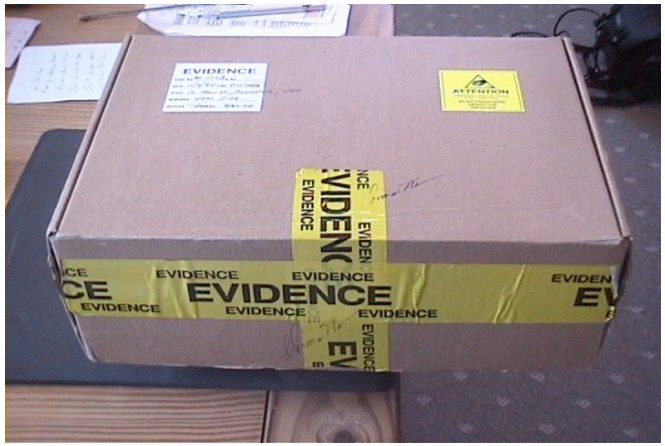
Investigative auditing…

- Detailed examination or enquiry
- Internal audit approach may be used
- **Legal recourse** is not presumed

Involves enquiry to establish facts, with no intention for a legal recourse.

Challenges – non technical

- Prevent cross contamination during exam
- Wide acceptance of investigative techniques?



Challenges - non technical

Proof of Scientific Rigor

Judges, and prosecutors must have confidence in tools and techniques used in digital crime cases.

Digital forensics tools and techniques

must go through a lengthy process

of establishing legitimacy in the courtroom, as other forensic tools had to.

These days, DNA evidence, for example, is routinely accepted as powerful and convincing evidence, but this was not always so.

Challenges – non technical

summit consulting

Legal Landscape

Building the bridge between IT & Legal

Challenges – non technical

Legal landscape

- Mandate
- Jurisdiction
- Privacy
- Politics

Regulatory landscape

① The Constitution of the Republic of Uganda, 1995 (as amended)

② The Computer Misuse Act, 2011

③ The Electronic Transactions Act, 2010

④ The Electronic (Digital) Signature Act, 2010

⑤ The Electronic Media Act, 1996 (Cap 104)

⑥ The Communications Act, 1997

⑦ Access to Information Act, 2004

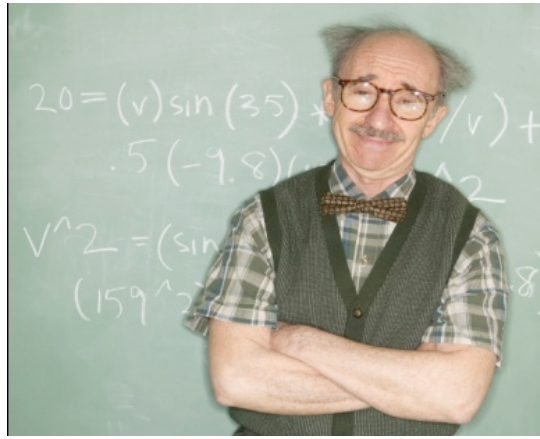
⑧ The Copyrights and Neighbouring Rights Act. 2006

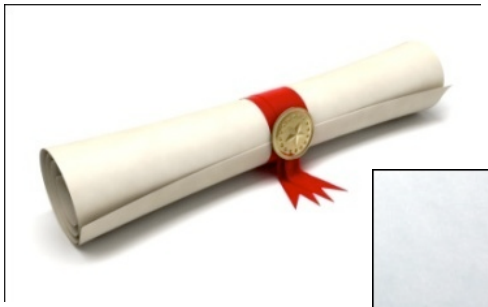
⑨ The Penal Code Act Cap 120 (Causing Financial Loss)

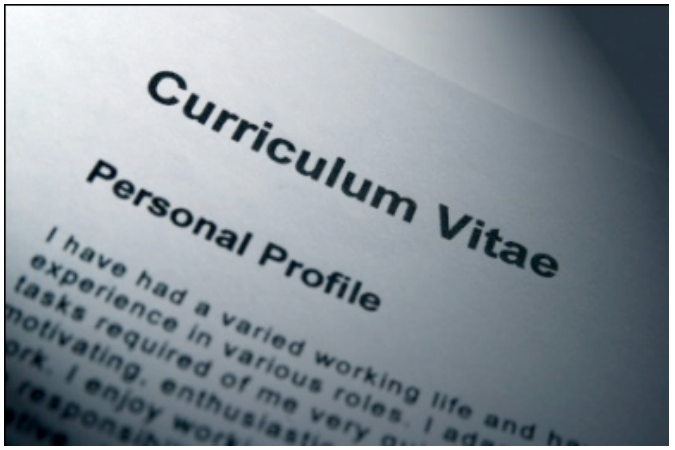
Challenges – Non Technical

Human Recourses

- Team Management
- Centralization of Forensic Skill
- Training
- Certification
- Personnel retention







Challenges – Non Technical

summit consulting

Forensic Event Preparation

- Tools
- Response Times
- Process, Policy & Procedure
- Lab Accreditation
- Workload & Data volumes
- Evidence Storage

Challenges – Technical

summit consulting

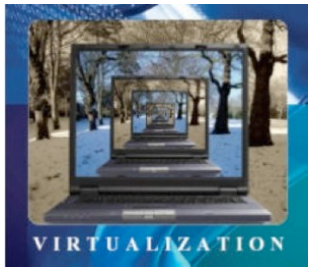
Peer 2 Peer Comms

SopCast © deliver your media to the world!

Challenges – Technical

Data Hiding

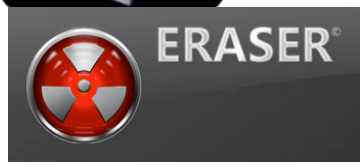
Virtualization



Use of VMs

Steganography

Encryption



Wiping Tools

WHITE CANYON SOFTWARE

Challenges – Technical

Roaming users

Across the wire Investigations

Wireless Investigation (802.x, GSM, Bluetooth…..)

Bot Evolution

Advanced Web Threats Java-based Web applications

7.6 percent of organisations reported exploits of their wireless systems.
CSI's 14th annual security survey 2009

Packet Injection

Challenges – Technical

summit consulting

Cloud Computing, Storage & data volumes

Current Day Cyber Crime

Rise of the Insider Threats

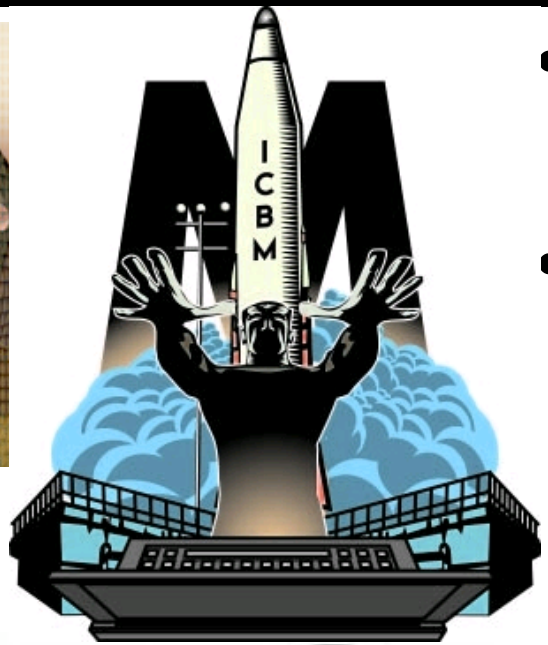
45% organisation stated the majority of their financial losses in the past year were due to actions by insiders

CSI's 14th annual security survey
December 2011

Current Day Cyber Crime

- IP Theft
- Identification Theft
- Phishing Masquerading
- Spam
- Anonymous Slandering
- Spy ware / Virus / Malware / Bots
- IT related sex offenses

Current Day Cyber Crime



- Bandwidth Theft
- Information Warfare
  DOS Key
  Infrastructure
- Organized Crime
- Piracy
- Credit Card Fraud

Common ICT frauds -- telecom

- IR/IC (International Roaming and Interconnect)
- Revenue leakages during provisioning and switching
- International Mobile Subscriber Identity/ Integrated Services Digital Network (MSI)/ISDN mapping - serial theft
- Post paid billing (this is usually manual)
- Local call Leakages through the IN (i.e Regional, National or International sipping through a Local Call)
- Call Detail Record (CDR) manipulations
- Mobile Money – interceptions
- Profile switching – prepaid vs post paid
- Theft by seconds – pay for 60s, use 55s

The faces of fraud - banking

summit consulting

- Fictitious Client Accounts & Transaction Replication
- Key Loggers (Lakeside Logger) == auto database jobs in background
- Syndicated Inter-Branch Withdrawals using fake Identities & Falsification of Client Identities
- Alteration Loan Parameters (Principal Installments, Interest etc)
- Steganographic Manipulation of Client Photos, Signatures or Thumb Prints
- Identity theft (ATM, PCI, etc) & Perpetual Overdrafts
- Salami Techniques (a dollar here, a dollar there etc)
- Electronic Scavenging - searching for residual data left in a computer

summit consulting

Some common forensic tools

1. EnCase - Acquisition & Analysis (while maintaining state), data recovery
2. LinkAlyzer - Analyzing Link Files
3. FlexHEX Editor or EditPad Pro 6+
4. Hexa Data Interpreter
5. PmExplorer – GSM key decoder (Nokia phones)
6. RevEnge - Hex viewer designed with Reverse Engineering – performs decompression, SMS GSM PDU 7 file decoder etc
7. Stegadetect – testing for existence of stega content
1. DB Visualizer version 6.5, Win NT version
8. Db forge for SQL SERVER version 4.5 , Win NT version
9. SQL Image Viewer Version
10. SQL Data Sets Version
11. Apex SQL 4.0

Fear nothing!

mmugisa@summitcl.com

+256712984585

q & a?

summit consulting

Contact:

Summit Consulting Ltd
Forensic. Advisory. Fraud
Plot 5, Kategro Road, Kira Road, Opp. British High Commission
P.O. Box 40292
Kampala, Uganda
P: +256 414 231136
M: +256 712 984585/ 0782610333
E: mmugisa@summitcl.com
Web: www.sbreview.net or www.summitcl.com
Skype ID: *mmugisa*.
Gtalk: *mugisa1*

Forensic. Advisory. Fraud.

Improve YOUR Condition!