ICPAK ANNUAL FORENSIC AUDIT CONFERENCE

Digital Forensics in Fraud & Corruption Investigations

9 October 2014

Leisure Lodge Hotel, Diani

Kenya

Faith Basiye, CFE
Head Group Forensic Services
KCB Banking Group

"This is a truly remarkable attack, but not just in its scope — hackers successfully penetrated one of the most secure organizations on this planet and they stole absolutely nothing of value — no money, no Social Security numbers, no passwords," John Gunn [Vasco Data Security International] in Chicago

On The Menu

- Cyber crime case studies
- Digital Forensics
- Digital Forensic Investigations
- Digital Forensic tools

KCB Making the Difference

Definition

- Cybercrime - Criminal activity committed with the aid of or in the arena of the internet and similar telecommunication technologies

- It is both a new incarnation of old crimes through a new medium and a unique entity all its own

Cyber Attack Threat Trends

- Internet social engineering attacks
- Network sniffers
- Logic bombs
- Worms/ viruses
- Trojans
- Exploited vulnerabilities
- Un-authorized reproduction of computer programs or software piracy

Cyber Attack Threat Trends

- Cyber-threats & bullying
- Automated probes and scans
- GUI intrusion tools
- Automated widespread attacks
- Widespread, distributed denial-of-service attacks
- Industrial espionage
- Executable code attacks (against browsers)

Cyber Attack Threat Trends

- Analysis of vulnerabilities in compiled software without source code
- Widespread attacks on Domain Name Systems (DNS) infrastructure
- Widespread attacks using Network News Transfer Protocol (NNTP) to distribute attack
- "Stealth" and other advanced scanning techniques

Cyber Attack Threat Trends

- Card skimming
- Phishing/ pharming
- Hacking
- Key loggers
- Zero day exploits
- Social networking
- Mobile devices
- Careless employees Malicious insider
- Anti-forensic techniques

It is Real-Global

With love from Russia (JP Morgan Chase & Co)

- 76 million households
- 7 million small businesses
- Highest level of administrative privilege on more than 90 of the banks servers

Syrian Electronic Army EBay

- Personal records of 233 million users compromised

Snowden

- 58,000 Sensitive documents stolen
- Edward Snowden, an American National Security Agency contractor, disclosed classified NSA documents to several media outlets, initiating the NSA leaks, which revealed the operational details of several major internet surveillance programs being conducted by the NSA

Federal Reserve bank

- Hacktivist group Anonymous retrieved the personal information of 4,000 US bank executives

It is Real-Kenya

- Kenya loses close to Kes 2 billion every year due to cybercrime
- In 2013 bank customers lost Kes 1.49 billion
- Hacked KDF twitter account
- Hacked Deputy president William Ruto twitter account
- Hacking of the Integrated Financial Management Information System (IFMIS)
- Ministry of Immigration and registration of persons' website

KCB Making the Difference

Digital Forensics

Digital Forensics

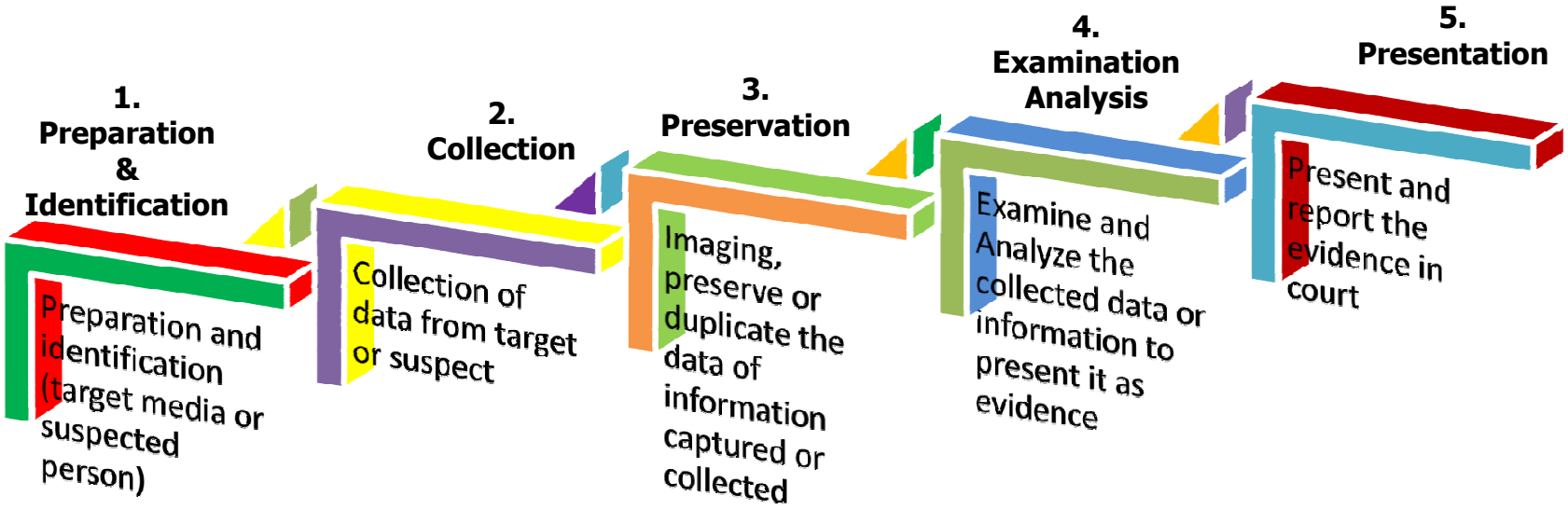
- Recovery and investigation of material found in digital devices in relation to computer crime
- The main objective is to reconstruct a past event
- Used to support or refute a hypothesis before criminal or civil courts or internal organization investigations

Electronic Evidence

Electronic evidence is information and data of investigative value based on the scope of your investigation that is stored on or transmitted by an electronic device

- Often latent in the same sense as fingerprints or DNA
- Can transcend borders with ease
- Is fragile and can easily be altered, damaged or destroyed
- Can be time sensitive

Digital Forensics Lifecycle



Where the Fun Begins

- Secure the suspect
- Secure the electronic media
- Check the electronic media to see if they are connected to a network or a phone line
- Photograph the connections, the digital media and its surroundings, the screen
- Disconnect printer and all peripherals (let it finish if printing

Where the Fun Begins

- Place evidence tape over the drives
- Search area around digital media for passwords, notes, user names, etc
- Seize other disks, CDs, external drives, manuals
- If computer is on turn them off by pulling the power code from the rear of the computer (for Windows only)

Where is the Evidence

- Internet history files
- Temp. Internet files (caches, Cookies)
- Slack/ Unallocated space
- Buddy lists, personal profiles, chat room records
- Settings, folder structure, file names
- File storage data
- Software/ hardware
- File sharing ability
- Emails

Tools Description

Digital Forensic Tools

- Computer/Live Forensics– Encase, FTK, Sleuth Kit, Autopsy
- Network Forensics - Wireshark, tcpflow, Network Miner
- Mobile Forensics – Blacklight, Cellebrite Mobile Forensics, SAFT Mobile
- Database Forensics - ACL, Idea and Arbutus

Common Digital Analysis Types

- Media Analysis- From a storage device
- Media Management Analysis- Analysis of the management system used to organize media
- File system analysis- analysis of the file system data inside of a partition or disk
- Application Analysis- analysis of data inside of a file

Common Digital Analysis Types

- Network analysis- analysis of data on a communications network
- OS Analysis- Analysis that examines the configuration files and output data of the OS to determine what events may have occurred
- Executable Analysis- Analysis of digital objects that can cause an event to occur

Common Digital Analysis Types

- Image Analysis- Analysis of images looking for information where picture was taken and who or what is in the picture
- Video Analysis- examines video for identity of objects in the video and location where it was shot


Thank You!

Faith Basiye, CFE, CPS(K)

Head of Group Forensic Services

KCB Bank Group

Email: fbasiye@kcb.co.ke

Cell:+254721240108

Direct line: +254203270848