Computer Forensics & Cyber Crime Security, an investigators experience

By CPA Mustapha B Mugisa, MBA, CFE, CHFI, CEH

Introduction

The use of computers and other digital devices to collect, store, process and produce data is on the rise. This electronically stored information (ESI) is mission critical to government, businesses and individuals. Technology use has permeated everyday life. From mobile devices like phones and laptops to computers, digital television and digital utility meters in our homes, technology is no longer a luxury but a basic necessity of life.

Research indicates that over 95% of all documents are first created using computers. Thanks to Web 2.0, mobile device users capture and process a lot of data on their phones and iPads for upload on social networks which has given rise to big data. Daily electronic mail and phone usage traffic far outstrips postal mail and other hard copy documents. Computer technology now impacts every facet of modern life. Telecom market reports indicate that over 19m Ugandans now own a mobile phone. That is over 53% of the total population.

The crimes, torts and disputes, which carry us to the courtroom, are no exception. Mobile devices and ICTs facilitate the commission of crime on a grand scale. Whereas in a manual system one would have to carry manual paper files, in today's highly automated and digital world, all one needs is a username and password to transfer huge sums of money between accounts. Traditionally, a terrorist had to post a letter through the Postal system and risked delays in delivery or loss in transit. Today, an email can be delivered instantly to over 20 or 100 accomplices!

With cybercrime like identify theft, one does not need to be physically present to commit a crime.

The extent of the problem

Arguably one of the worst types of cybercrime is child pornography. The lack of clear education about the dangers of Internet pornography continues to expose our children to the huge dark industry of on-line pornography. Criminals are able to coordinate their crimes through the Internet regardless of physical location. A company operating cybercrime ring in say Eastern Europe may befriend a Ugandan child found on-line using several social engineering and on-line search tools. Once a target is identified, trust is established, thereafter the child may be "poisoned" to the extent of posing while naked and even uploading personal videos in awkward situations.

Once submitted, such videos and photos are put up for sale in membership pornographic sites. In addition to privacy concerns, the victim may be found by friends or family on such sites which has a lifetime psychological torture and kills self-confidence. For some, it could be used to obtain a ransom, if one is known to be of a certain social standing. Many of the victims prefer to remain silent than report such cases. Even if they reported, the logistics involved in investigating such crimes are enormous. The exact location of the suspects is not clear. Different countries have different cyber laws, leave alone extradition of such criminals is near to impossible, if not impossible even with international support.

According to the 2012 Uganda Police Annual Crime and Road Safety Report, of the 60 cases reported and investigated, a total of UGX 1.5 billion (579,000 USD) was lost through attack vectors like social engineering and phishing to obtain victims' identities which were then used to hack into victim emails and social network profiles. Uganda Police report further shows that in 2014, ATM/VISA frauds caused a loss of over 1.2 billion UGX (460,000 USD) from 700 victims by use of scheming devices installed onto ATMs located in Kampala and other areas. "Cyber-crimes reported in 2013 were 45 cases compared to 62 cases in 2012. However these resulted into a loss of about 18.1 billion UGX (7 Million USD). This implies that more grave losses were made

subsequently despite the reduction in reported cases." The crimes included Electronic frauds, Phishing (password harvesting), Email hacking, pornography/defamation, offensive communication, mobile money frauds, SIM Card swapping and ATM/VISA frauds", the police report notes.

As an investigator, my experience is that most victims in Uganda prefer to suffer silently. This could be partly attributed to the fact that there have been limited successes with cases that have been reported or law enforcement does not offer case summaries and successes made on cases handled.

There is no one who is safe as long as their systems can be accessed via a network, specifically the Internet. With high automation and integration to third party systems using application programming interfaces (APIs) to facilitate ecommerce as well as mobile commerce, there are a plethora of attack vectors, as explained in brief case studies below. In the financial and telecom sectors, of the over 80 cybercrime cases which have been investigated by Summit Consulting Ltd Forensic Services in 2014 in Uganda:

i. 90% of the attacks, where loss of integrity was reported, it involved internal staff at the centre of the crime i.e the attack could not have succeeded without internal staff involvement

ii. 70% of the attacks caused loss of integrity (account manipulations by transferring money from one account to another) and loss of availability (the core application system went off line for 2 to 30 minutes) before, during or after the attack.

iii. The attack on system availability is equally expensive, yet victims rarely quantify the cost.

iv. Over 95% of attacks first originated from someone external of the organisation, by enticing an internal staff

v. No attack on system integrity succeeded by external criminals working alone!

vi. Some internal staff exploited ignorant colleague's username and password. At disciplinary hearing, all suspects denied responsibility for their username and password.

Cybercrime and the law

Government of Uganda passed three critical laws i.e. the Uganda Cyber Laws namely (i) Computer Misuse Act, 2011; (2) Electronic Transactions Act, 2011; and (3) Electronic Signatures Act, 2011.

The Computer Misuse Act provides for the safety of electronic transactions and information systems; to prevent unlawful access, abuse or misuse of information systems including computers and to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment and to provide for other related matters.

The need for cyber laws in Uganda and elsewhere in the world is four fold:

i. Tackle cyber crimes
ii. Address intellectual property rights and copyrights protection
iii. Enable e-commerce and facilitate trade
iv. Regulate the use of electronic signatures to ensure security (confidentiality, integrity and availability) of communication and non-repudiation

However, successful prosecution of cybercrime cases remains a challenge.

The new field of computer forensic entails the identification, preservation, extraction, interpretation and presentation of computer-related evidence. Without using the right tools and techniques to preserve, examine and extract data, law enforcement officers run the risk of losing something important, rendering what you find inadmissible, or even causing spoliation of evidence. Some of the major challenges in prosecuting cybercrime

cases are the lack of standard operating procedures (SOPs) pertaining to cybercrime investigation process in Uganda. The fact that the law always lags behind technology advancement, means that some of the key stakeholders in the prosecution are not on the same page.

In Uganda, under the criminal justice system the burden of proof in a criminal matter lies upon the prosecution, which must prove all constituent components of the case. Unlike in civil matters, the standard of proof in a criminal case is beyond reasonable doubt. The main purpose of investigating any crime is to collect sufficient & legally admissible evidence to ensure conviction of offenders. The requirements of evidence in cybercrimes are not different, but its nature has made collection of evidence a specialized job.

Cybercrime investigation in Uganda fails due to poor first response procedures which often lead to spoliation of evidence making authentication of electronic evidence a tough call for any forensic examiner.

The Encase Legal Journal, 5th Edition (can be accessed via Google) provides the best case law and cybercrime investigation guidelines for effective prosecution or defense. I invite all of you to read a copy.

Briefly, prosecution must prove the following three key ingredients in the offense of electronic crime causing financial loss beyond reasonable doubt:

i. There was dishonesty by the accused person
ii. That the dishonesty was deliberate with intent to secure unlawful gain
iii. That use of a digital device was involved in (i) and or (ii) above.

Without clear standard operating procedures, public awareness for effective first responder to preserve the crime scene for computer evidence, it is difficult, to prove the charges. And that is why most cyber related cases have by far failed at prosecution.

I will mention a few. Aliases have been used and some facts omitted to ensure confidentiality.

Case 1: The web phishing case

1.1 The facts in brief

i. A businessman based in Kampala approached an IT company for computer maintenance services. A service level agreement (SLA) was signed, specifying clear terms and responsibilities for each party.
ii. During the course of the work, unknown to the client, the IT Company outsourced part of the work to an external consultant who discovered the nature of transactions the client deals in in. Specifically, he noted that the client supplied some imported products to several companies purchased from a specific company in the US.
iii. Using free Internet tools, the suspect (computer consultant) copied the website of the US supplier and made the replica look exactly like the genuine one and also advertised all the products the company sells. He then sent a link to the victim via a cloud (anonymous) email address, who unknowingly placed orders through the rogue website.
iv. In the process, payment instructions were exchanged. The first was a bidding security payment of US $90,000. Thereafter, the victim was further asked to pay US $250,000 as part of tax clearance, PVO and inspection, among others. The victim provided evidence as having paid this money to the account provided by the suspect.
v. Before the goods could be shipped, the victim was further asked to make more payments, which aroused his suspicious. The genuine company never asked for this kind of payment, though at first he had thought of a change of process.

vi. The victim engaged Summit Consulting Ltd to help in the investigation. As a first step, Summit Consulting advised the client to report the matter to Police, considering the criminal nature of case.

1.2 The investigation

i. Since we did not know the suspect, yet, we started by getting the emails received in the victim's inbox. We were able to obtain the suspect's email header (has information about the senders IP address and the email path from origin to destination) as well as bank account information and the fake website that had been created. Using WHOIS.com and other cyber forensic investigation tools, we established the details of the webmaster, and key details like email address, name, mobile phone number among others.

ii. SCL gave this information to Uganda Police, who then obtained a court order for a call log printout from the telecom company. Together with the email header information, the physical location of the suspect's office was established. After obtaining the search warrant, police visited the suspect's offices in Kampala. Key information like payment papers (invoices to the victim), registration details of the web site, etc are seized. The key omission made was the failure to seize the physical computers at the offices. Apparently, the search warrant had not specified seizure of the computers and digital devices. On return, with appropriate instruments for seizure, the office was found empty. All computers had been removed!

iii. However, after analysis of the call log patterns in addition to satellite geolocation technology, the suspects' home address is ascertained. The details are given to police who visit and fortunately seize three laptop computers and mobile phones. These are forensically processed to establish whether the emails send to the victim originated from the laptop. An image of the suspect laptop is created and verified using a MD5, among others and

analyzed using both Encase Forensic Software and Paraben Forensic Software at Summit Consulting Ltd computer forensic & training lab.

1.3 Key issues/ evidence

i. The payment documents for fake website registration and hosting are in the names of the suspect, who we established was a consultant attached to a computer maintenance company working with our client.
ii. Confirmed that the seized laptop with the suspect sent out the emails, which also provided the bank details where money was deposited
iii. Pictures and documents posted on the fake website, were found to contain artefacts in the metadata of the author, which were those of the suspect
iv. Court order to verify bank documents and details on which money was deposited was issued and found to that the bank account opening forms had photos of the fraudster, with a relative as a co-shareholder in the company.

1.4 The charge

The suspect was charged with electronic fraud contrary to section 19 of the Computer Misuse Act, 2011 laws of Uganda. This carried punishment of up to 15 years. Also the victim will pursue civil proceedings to recover his money under civil law.

1.5 Issues and lessons to consider

i. Effective working relationship with Police and private company – each party handled their area of expertise.
ii. The suspect was an amateur. He used true identities for bank account information, on-line hosting, mobile phone and physical office.
iii. Working swiftly is recommended given the volatile nature of computer evidence. Forensic tools help recover even deleted evidence.
iv. The rules of evidence that apply to physical evidence apply to digital evidence. Cyber criminals are making a fortunate in their schemes. Unfortunately, it is

difficult to prosecute this people. Once one loses money, recovery is very difficult and a long process! This case has been running since late 2013, and civil procedures for damages are yet to commence!

v. Not everyone can investigate cybercrime or process digital evidence.

2. Case study: Theft or loss of confidential information at a financial institution

Scenario 1: A business rival obtains confidential information (e.g. tender quotations, business plans, database of customer top customers & transactions, list of clients etc) through hacking including social engineering. He then uses the information for the benefit of his own business (e.g. quoting lower rates for the tender) and or sales it to competitors for use.

Scenario 2: A criminal obtains confidential financial institution or hospital information by hacking or social engineering and threatens to make the information public unless the victim pays him money.

Scenario 3: A disgruntled employee steals confidential company information and mass emails it to the victim's rivals and also posts it to the numerous websites and newsgroups; and promotes it via social networks using fake profiles.

Required:

1. Which law/s is most applicable under each scenario?
2. Who is liable?
3. What is their motive?
4. What is the modus operandi?
5. How would you approach the investigation? Which evidence would you collect, how and where would you find it?

Answers| case study 1

1. The relevant law, for each scenario
    a) Constitution
    b) Penal code
    c) Computer Misuse Act, 2011
2. Who is liable?
    a. Scenario 1: The persons who steal the information as well as the persons who misuse the stolen information.
    b. Scenario 2: The persons who steal the information as well as the persons who threaten the victim and extort money.
    c. Scenario 3: The disgruntled employee as well as the persons who help him in stealing and distributing the information.
3. The motive?
    a. Scenario 1: Illegal financial gain.
    b. Scenario 2: Illegal financial gain.
    c. Scenario3: Revenge.
4. Modus Operandi

Scenario 1: The suspect could hire a skilled hacker to break into the victim systems. The hacker could also use social engineering techniques.

Illustration a: A very good looking woman went to meet the system administrator (sa) of a large company. She interviewed the SA for a “magazine article”.

During the interview she flirted a lot with the sysadmin and while leaving she “accidentally” left her pen drive at the sysadmin’s room. The sysadmin accessed the pen drive and saw that it contained many photographs of the lady. He did not realize that the photographs were Trojanized! Once the Trojan was in place, a lot of sensitive information was stolen very easily.

Illustration b: The system administrator (sa) of a large manufacturing company received a beautifully packed CD ROM containing "security updates" from the company that developed the operating system that ran his company's servers.

He installed the "updates" which in reality were Trojanized software. For 3 years after that a lot of confidential information was stolen from the company's systems!

Scenario 2: Same as scenario 1.

Scenario 3: The disgruntled employee would usually have direct or indirect access to the information. He can use his personal computer or a cyber café to spread the information.

Investigation approach – scenario 1

1. Understand the issues
    a. What happened? When?
    b. Are there any suspects? If yes, who? Do they pass the predication test?
    c. Which evidence do we need?
    d. What is at risk?
    e. Possible places for evidence

References

1. Encase legal journal, 5th Edition
2. Summit Consulting Ltd cybercrime cases by Mustapha B Mugisa @www.summitcl.com
3. Cybercrime and digital evidence, Indian perspective