Computer Forensics for Law Enforcement

Sogbaike Oluwasegun, Okene Ese David, Esemuede Esther, and Oweh Victor

Delta State Polytechnic
Otefe-Oghara
Delta State, Nigeria.

Corresponding Author: Okene Ese David

Abstract
Prosecuting suspects of computer related crimes is becoming more and more effective as a result of improvements in the methods of carrying out investigations and obtaining evidences from crime scenes. A computer can be used as a tool to perpetuate a crime, a computer can also be the target of a crime, or it can serve as an evidence repository for storing valuable information about a crime. A suspect can be held responsible for a crime when an investigation is still ongoing. Several investigation processes have been proposed but they weren’t able to efficiently address the issue of computer crime, as a result of sophistication and change in paradigm in which computer crimes are been committed. A more general approach to investigating a computer crime scene makes evidence from the crime scene admissible in the court so that suspects can be tied to the crime. This paper explains a recent and general approach of an investigation process that can be used in computer forensics. With this general approach, a computer crime scene can be more effectively investigated. The crime scene conceals detail evidences which are needed to tie a suspect to a crime committed and possibly obtain a conviction.

Keywords: computer forensics, digital evidence, law enforcement, computer crime, investigation, computer forensic model, court of law

INTRODUCTION
Forensic means the use of scientific knowledge or methods in solving crimes. It is the job of the forensics to inform the court. One of the basic principles of forensic is that of Locard’s which states that: when two items or person come in contact there will be an exchange of physical trace. Something is brought, and something is carried away. Meaning that, a suspect can be tied to a crime by detecting these traces.

The continuing technological revolution in communications and information exchange has created an entirely new form of crime: cyber crime or computer crime and also tracking and tracing criminal activity (Mohay et.al 2003). Increase in population of internet users presented a lot of data exchange. Unfortunately many businesses, and even organizations, do not know how to properly protect their sensitive data, thus leaving the door open to criminals (Raca 2005). A computer can play one of three roles in a computer crime. A computer can be the target of the crime, it can be the instrument of the crime, or it can serve as an evidence repository storing valuable information about the crime (Raca 2005, Kadir 2010 & Mohay et.al 2003).

WHAT IS COMPUTER FORENSICS?
Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way effective because of the fast improvement in the manner computer crime is perpetrated.

Computers can be involved in a wide variety of crimes including white-collar crimes (financially motivated nonviolent crime), violent crimes such as murder and terrorism, counterintelligence, economic espionage, counterfeiting, and drug dealing.

A survey by the FBI as documented in (Raca 2005) showed that a huge percentage of unauthorized accesses to organization information are from its employee.

Computer crime has forced the computer and law enforcement professions to develop new areas of expertise and avenues of collecting and analyzing evidence. This is what has developed into the science of computer forensics.

A computer can play one of three roles in a computer crime. A computer can be the target of the crime, it can be the instrument of the crime, or it can serve as an evidence repository storing valuable information about the crime (Raca 2005, Kadir 2010 & Mohay et.al 2003).
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.

The birth of Computer forensic is as a result of the emergence of computer related crimes. Appropriate prosecution of a suspect of a computer related crime was a challenge because availability of evidence in a crime scene without proof of on how it links the suspect to the crime cannot stand in a court of law. Computer forensics provides information to the court on how a suspect is linked to a crime based on evidence from the crime scene.

Computer forensics implies a connection between computers, the scientific method, and crime detection.

Computer forensics as explained in (Mohay et.al 2003) is the identification, preservation and analysis of information stored, transmitted, or produced by a computer system or computer network in order to reason about the validity of hypothesis which attempt to explain the circumstance or cause of an activity under investigation in a manner intended to meet evidentiary requirement.

Evidence is what distinguishes a hypothesis from a groundless assertion. Evidence can conform or disprove a hypothesis, so evidence can be produced in the law court if it satisfies the evidentiary requirement act as stated below (Ryder 2002)

1. Admissible: it conform to certain legal rules before it can be put before the jury
2. Authentic : it must be possible to positively tie evidential material to the incident
3. Complete: it must tell the whole story and not just a particular perspective
4. Reliable: there must be nothing about how the evidence was collected and subsequently handled which causes doubt about its authenticity and veracity
5. Believable: it must be readily believable and understandable to members of jury.

Digital Evidence
Information of probative value that is stored or transmitted in binary form and may be relied upon in court (Mason 2012). It also encompasses any and all digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator (kozushko 2003).

Digital evidence, by its very nature, is fragile and can be altered, damaged, or destroyed by improper handling or examination. For these reasons special precautions should be taken to preserve this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion (NIJ 2004). Because of the composite nature of digital evidence some factor are responsible for making interpretation of digital evidence challenging which are (Raca 2005):

- Too many suspects
- Identifying the crime
- Too much potential evidence
- The evidence is easily contaminated
- Contaminating of some evidence may ruin all

Computer Forensic Model
Several models have been proposed for computer forensic investigation such as Common Process Model for Incident and Computer Forensics, Framework for a Digital Forensic Investigation, A Hierarchical, Objective-Based Framework for the Digital Investigations Process (Yusoff et.al 2011) etc. (Ademu et.al 2011) proposed an approach to computer (digital) forensic investigation enumerating its advantages over the existing models.

The Digital forensic investigation process was generalized into 4 tier iterative approach. The entire digital forensic investigation process can be conceptualized as occurring iteratively in four different phases. The first tier which is the preparation or inception phase occurs over the course of an investigation from assessment to final presentation phase. The first tier will have 4 rules for digital forensic investigation which involves preparation, identification, authorization and communication. The second tier will have rules such as collection, preservation and documentation, the third tier will have rules consisting examination, exploratory testing, and analysis, the 4th tier which is the presentation phase have rules such as result, review and report as shown in fig 1.
Fig 1: Proposed digital forensic investigation Model (Ademu et.al 2011)

The proposed model of fig 1 allows the much needed interaction of investigators with other resources for carrying out the investigation, capturing the expertise of investigation as a basis for the development of advanced tools incorporating techniques such as automated digital evidence collection. But also clearly state that Generality of this approach is not explicit. It must be applied in the context of a crime before it will be possible to make clear the details of the process. However (Yusoff et.al 2011) outlined some existing computer forensic investigation models grouping similar phases shared by each models upon completion realized that phases can be grouped into five (5) generic grouping namely, pre-process, acquisition & preservation, analysis, presentation and post-process forming the basis for proposing the generic computer forensic investigation model (GCFIM) as shown in fig 2 below

Fig 2: Proposed generic computer forensics investigation model (Yusoff 2011 et.al)

Pre-Process: The tasks performed in this phase relates to all of the works that need to be done prior to the actual investigation and official collection of data. Among the tasks to be performed are getting the necessary approval from relevant authority, preparing and setting-up of the tools to be used, etc.

Acquisition & Preservation: Tasks performed under this phase related to the identifying, acquiring, collecting, transporting, storing and preserving of data. In general, this phase is where all relevant data are captured, stored and be made available for the next phase.

Analysis: This is the main and the center of the computer forensic investigation processes. It has the most number of phases in its group thus reflecting the focus of most models reviewed are indeed on the analysis phase Various types of analysis are performed on the acquired data to identify the source of crime and ultimately discovering the person responsible of the crime.

Presentation: The finding from analysis phase are documented and presented to the authority. Obviously, this phase is crucial as the case must not only be presented in a manner well understood by the party presented to, it must also be supported with adequate and acceptable evidence. The main output of this phase is either to prove or refute the alleged criminal acts

Post-Process. This phase relates to the proper closing of the investigation exercise. Digital and physical evidence need to be properly returned to the rightful owner and kept in safe place, if necessary. Review of the investigative process should be done so that the lesson can be learnt and used for improvement of the future investigations.

(Ademu et.al 2011) did not admit that the proposed computer forensic model possess any degree of generality and (Yusoff et.al 2011) didn’t state the
degree of generality but from discovery of the 5 (five) phases uniquely shared by all examined computer forensic investigation model, the generic computer forensic investigation model (GCFIM) is truly generic and general as stated by security monitoring solution(blog) in this statement “the GCFIM model is a perfect generic model, that any computer security incidence response team (CSIRT) and forensics investigators can start with when creating its own incident response processes. It seems that the main stream or flow of this model can be easily recognizable in incident response processes which contains forensics investigation”

LAW ENFORCEMENT
Computers may also contain important information for intelligence gathering purposes. Much more computer crime exists than law enforcement acknowledges or identifies, and there are many techniques that law enforcement is largely unaware of. Computer-based evidence is now routinely becoming common in court proceedings, Cases are frequently decided on evidence obtained from computer systems.

Computer forensics is about evidence from computers that is sufficiently reliable to stand up in court and be convincing. Computer forensics a relatively new discipline to the courts in Nigeria and many of the existing laws used to prosecute computer-related crimes, legal precedents, and practices related to computer forensics are in a state of flux. New court rulings are issued that affect how computer forensics is applied. Security professionals need to consider their policy decisions and technical actions in the context of existing laws. For instance, you must have authorization before you monitor and collect information related to a computer intrusion.

CONCLUSION
Computer forensics is routinely employed by law enforcement, by government and by commercial organization. Investigating a computer crime scene with a reliable investigation approach is a concern in computer forensics because computer crime has become really advanced and sophisticated.

A computer crime scene properly investigated using the generic computer forensic model can produce digital evidence that can be tied to the suspect by showing and explaining how the suspect is involved in the crime. The evidence is then admissible in the court by satisfying the evidential requirement and then can be tied to the suspect.

REFERENCES
George Mohay Alison Anderson; Byron Collie; Oliver De Vel; Rod Mckemmish; (2003). Computer and Intrusion forensics. Artech House Inc.


Karen Ryder (2002): Computer Forensics – We’ve had an incident, who do we get to investigate? SANS Institute Info Sec Reading Room


http://searchsecurity.techtarget.com/definition/computer-forensics accessed 19/10/2013