Quest Journals
Journal of Research in Humanities and Social Science
Volume 3 ~ Issue 6 (2015) pp:42-46
ISSN(Online) : 2321-9467
www.questjournals.org

Research Paper

Mapping of the emerging digital forensic technologies for crime investigations in Ethiopia: A call for nation security, Safety and sustainability

Gaurav Kataria[(Ph.D.)1], Abhilasha Kataria[(Ph.D.)2]
[1]*Ass Prof. ,School of Law, Wollega University, Nekemte (Ethiopia),*
[1] *Ass Prof. ,School of Law, Wollega University, Nekemte (Ethiopia),*

Received 22 May, 2015; **A**ccepted 15 June, 2015 © The author(s) 2015. Published with open access at **www.questjournals.org**

ABSTRACT:- The use of digital devices like computer, mobile, phablets, tabs etc. are increasing rampantly. The devices are passably connected with all criminal's activities up to some extent. The research paper is discussing about the emerging digital forensic technologies for preventing crime in Ethiopia. There are several software tools like Forensic Kit Tool, Pro Discover, Encase etc. available which are identically useful for investigating crime. In Ethiopia there is no establishment of digital forensic laboratory where such techniques or software tools can be employed. Digital forensics techniques are used in a number of arenas, not just in catching identity thieves and Internet predators. The paper hashed out on digital forensic software tools with some cases study. After surveying the relevant literature authors concluded with policy recommendations.

Keywords:- Digital, Forensic, Software, Crime

I. INTRODUCTION

Not long ago, the incidence of crimes that involved computers or electronic media was negligible. Currently, State and local law enforcement agencies routinely encounter evidence of electronic crimes, including online fraud, child pornography, embezzlement, economic espionage, and cyber stalking. Law enforcement also encounters crimes classified as cyber terrorism. These incidents have included attempts to penetrate electronic systems that control critical infrastructures. The task of investigating and prosecuting electronic crimes and cyber terrorism is complicated by the anonymity afforded perpetrators through the Internet, by a "borderless" environment, and by the variables in Ethiopian and foreign laws. Further, the range of computerized devices encountered during a normal day that may be potential sources of information and evidence and be considered for forensic investigation is vast. In the home, there is the personal computer and the hub or router that connects it to the outside world, probably. A computer games console, a satellite TV box that may have Internet and e-mail capability, the alarm system and control systems for the washing machine and environmental controls, and increasingly other "white goods/' In the car, there is the engine management system and the satellite navigation system, which may include a wireless or Bluetooth communications facility. In the office, there will be networked computer systems, access control systems, and alarm systems. For the individual user, there is the laptop computer and the handheld mobile communications device. The last may seem a strange choice ot words to describe what, to date, has been referred to as the "mobile phone," but that term now no longer really describes the devices we all regularly carry with us. Todays device is more and more a mini computer. In addition to making phone calls, it contains an address book and a diary, can download and play music, can browse the Internet, send e-mail, and act as an SMS-capablc device. The types of information that may contain evidence lie in one of three groups; Active, Archival, and Latent Data. Active data is the information that can be seen on the device, such as data files, programs, and the operating system files. This is the easiest type of data to collect-Archival data is data that has been backed up. This may be stored, for example, on DVDs, CDs, floppies, backup tapes, and hard drives. Latent data is the sort of information that may require

*Corresponding Author: Gaurav Kataria
[1]*Ass Prof. ,School of Law, Wollega University, Nekemte (Ethiopia),*

specialized tools to recover and includes information chat has been deleted or may have been partially overwritten.

II. STATEMENTS OF THE PROBLEM

The digital forensic technologies for crime investigations are emerging proficiencies used in forensics technologies to the examination of digital evidence in support of criminal investigations for offences like —

- Terrorism
- Child Pornography
- Crimes of Violence
- Trade secret theft
- Theft or destruction to intellectual property
- Financial crime
- Property crime
- Internet crimes
- Fraud

Unfortunately Ethiopia has no establishment of forensics laboratory and training centers devoted to the examination of digital evidence in support of criminal investigations.

III. OBJECTIVES

- To provide Information on digital forensics technologies for investigative professionals working for national security
- To explains how to develop the use of digital forensic technologies for controlling crime in Ethiopia.
- To elaborate the function of digital forensic software tools i.e. FKT, Pro Discover, Encase etc.
- To flesh out collection and storage of evidence, staffing, and metrics management.
- To impart the knowledge and experience for digital investigation.
- To Provides guidance on creating and managing a digital forensics laboratory in Ethiopia.
- To give a way to defense professionals, consultant, police or private investigator who is going to be the manager of a unit can have an understanding of the issues that need to be considered when creating a digital forensic laboratory.

IV. RESEARCH QUESTIONS

- Whether the investigators in Ehiopia are equipped with emerging digital forensic technologies.
- Whether the emerging digital forensic technologies are pragmatically applicable in Ethiopia

V. METHODOLOGY

This is a reform oriented qualitative doctrinal Research. In this research, the authors utilized an incremental procedure to explain a need of digital forensic Technologies in Ethiopia for reporting digital evidence items in computer forensic tools. There are different types of digital forensics evidence like storage media evidence, memory evidence, network evidence, and mobile device evidence. Primarily, the authors surveyed the reporting function of computer forensic software tools, which were: FTK, Pro Discover and Uncase as presented in the literature and software review to formulate the data requirements for digital evidence items. Finally, based on the findings, the authors concluded with some policy recommendations.

VI. DIGITAL FORENSIC TECHNOLOGIES AND INVESTIGATION

A digital forensics investigation is conducted for number of reasons but it majorly facilitates criminal investigations and civil litigation investigations. The types of activity commonly considered for criminal investigations include hacking, fraud, distributing viruses, stalking, and blackmail. The second type of activity normally considered to fall into the civil litigation investigation category includes internal disciplinary investigations to gather evidence of system misuse and abuse, or inappropriate behavior that will result in internal disciplinary procedures and potentially the dismissal of a member of staff.

VII. DIGITAL FORENSIC SOFTWARE TOOLS

For more than 30 years, the case of the BTK serial killer went as one of the biggest unsolved mysteries in America. Police spent hundreds of thousands of hours and millions of dollars trying to learn the identity of the man had who killed 10 people in and around Wichita, Kansas, between 1974 and 1991. Then, in a few short hours on February 16, 2005, computer forensicists accomplished what police had failed to do for more than 30 years by identifying the killer as a man named Dennis Rader. The case remains the most famous ever solved by computer forensics. The following some forensic software tools have played a significant role to investigate crimes EnCase is considered one of the best computer forensics packages available because of the software's various component programs. For example, users who wish to examine a suspect's storage media, but do not wish to dedicate the time necessary to make an exact image of the disk, may preview the suspect disk. During this preview, session users may conduct any analysis that could be undertaken if an image of the disk was being examined. Later versions of the software allow for users to save the progress of their forensic examination conducted through the preview method. The true value of this feature becomes apparent in situations in which taking the time to image multiple drives could place an investigation in jeopardy. Consider an investigation involving 15 computers. If each disk requires 30 minutes to image, then the investigator is facing a multi- hour task. However, is it certain that all of these disks contain evidence? If the answer to this is unknown, then first previewing the disk may save hours. In the above example, an investigator could preview the disks, and image only those disks that are important to the case. A second useful feature of the EnCase software is the ability to image a disk (referred to by some users of EnCase as acquiring a disk image) through the use of a network patch cable or a serial cable. While this method of imaging a disk takes longer,the benefit is that the forensic analyst does not have to remove the physical disk from the computer. The EnCase software allows users to create a boot disk that will prevent any data from being written to a suspect's disk during the computer's start-up process. Once the computer is up and running, the forensic analyst can begin making a disk image through either the patch cable or the serial cable.When the image is created, the EnCase software allows the analyst to search the hard drive bv:(l) examining the image files located on the hard drive through a gallery view, (2) examining the files through the use of a hex view (reading the hexadecimal file components), and (3) searching the entire disk for keywords. EnCase also has a reporting feature that allows a forensic analyst to save keyword hits, images, and personal comments into an easy-to-format report that can be printed or e-mailed to attorneys involved in the case.

Forensic Tool Kit (FTK) is produced by Access Data and contains many of the same features as the Encase forensic software. FTK allows users to examine an imaged disk by: (1) examining image files through a gallery view, (2) examining files through a hexadecimal view, and (3) searching the disk for keywords. However, FTK also contains a couple of features. It scans a hard drive looking for various information. It can for example locate deleted email and scan a disk for text strings to use them as a password dictionary to crack encryption. The toolkit also includes a standalone disk imaging program called FTK Imager. The FTK Imager is a simple but concise tool. It saves an image of a hard disk in one file or in segments that may be later on reconstructed.

Pro Discover is a commercial forensic tool made by Technology Pathways that uses its own Pro Discover image file format. Pro Discover can convert a raw image of a disk into a bootable VMware Machine.

VIII. THE FAMOUS CASES SOLVED BY DIGITAL FORENSIC TECHNOLOGIES

The BTK Killer The case started on January 15, 1975, when Dennis Rader strangled to death four members of the Otero family. Over the next 15 years, he would admit to binding and killing six more victims, all female. As he was murdering victims, Rader taunted police by sending them bizarre notes. His first letter was stuck in an engineering book in the Wichita Public Library. In that note, Rader claimed responsibility for the Otero murders, providing details only known by police. He also promised more murders and suggested a nickname for himself – BTK (Bind, Torture, Kill). Rader went on to write many other letters to police, including twisted poems, puzzles and pictures. Sometimes he would send the letters straight to the police, other times he would mail them to the media or hide them somewhere. Police even suspected that he placed references to himself in the newspaper's classified section. Local police, working with the FBI, spent thousands of hours studying these communications. They hired the best criminal psychologists, followed up on every possible lead and interviewed thousands of suspects. Even with this staggering collection of evidence, however, police were unable to tie any of the murders to Rader. It was not until 2004, after more than 10 years of complete silence from the killer, that police finally caught a break. That year, Rader resumed his communications with police. He eventually sent them a Word document on a floppy disk that computer forensics experts immediately examined. By using EnCase forensics software, police were able to pull up a Word document that had been deleted. The document contained metadata that revealed it had last been modified by someone named “Dennis” at Christ Lutheran Church. A quick search of the church's website revealed that Dennis Rader functioned as president of the church's congregation council. By checking Rader's background and examining DNA evidence, police were able to quickly link him with the BTK murders. Rader originally pleaded not guilty to the murders, but he later confessed, providing hours of testimony filled with excruciating detail. Today, computer forensics is used more than ever to solve murder, kidnapping, rape, fraud and embezzlement cases. Investigators routinely dig up information that was thought to be long gone on computers, cell phones, Web chats and networks. The tools they use are also growing more advanced every day. In the digital age, computer forensics experts are more valuable than ever – just ask Dennis Rader. You'll find him in Kansas's El Dorado Correctional Facility. His earliest possible release date is February 26, 2180.

A. **Dr. Conrad Murray** One of the higher-profile cases of the last few years is that of Michael Jackson's physician. Now, his case wasn't entirely decided by computer forensics, but it certainly didn't help him that investigators were able to find medical documentation on his computer showing that he authorized lethal amounts of propofol for the deceased pop star.

B. **Krenar Lusha** When his laptop was searched by UK computer forensics experts, they discovered that he had downloaded instructions on how to do a number of frightening things – like build suicide belts and other types of explosives. He also commonly had live chats with people where he talked about being a terrorist and wanting to see Americans and Jews killed. All of this led to a search of his apartment, where officers found bomb-making equipment and other weaponry. Needless to say, he won't be trying it out anytime soon.

C. **Matt Baker** While not a famous case, this one goes to show you that when you use a computer for crime, the evidence doesn't just fade with time. The story started when Mr. Baker's wife overdosed on sleeping pills and left a suicide note – everyone accepted that she had simply killed herself. But after four years of investigating and analyzing Mr. Baker's computer, it was discovered that he had done research about overdosing on sleeping pills and visited a number of pharmaceutical websites shortly before his wife's "suicide." Couple this with damning evidence about his personal character (also obtained from his computer) and Matt Baker was sentenced to 65 years in prison.

D. **Krenar Lusha** When his laptop was searched by UK computer forensics experts, they discovered that he had downloaded instructions on how to do a number of frightening things – like build suicide belts and other types of explosives. He also commonly had live chats with people where he talked about being a terrorist and wanting to see Americans and Jews killed. All of this led to a search of his apartment, where officers found bomb-making equipment and other weaponry. Needless to say, he won't be trying it out anytime soon.

E. **Sharon Lopatka** In a show of one of the ways computer forensics can be used to benefit someone, investigators found hundreds of emails on Ms. Lopatka's computer that eventually led them to the man that killed her – Robert Glass.

F. **Corcoran Group** This one is interesting because a lack of evidence led to convictions. How so? After the case began, a computer forensics expert was tasked with looking through computer files for evidence of wrongdoing. He didn't find that evidence, but what he did find was just as interesting – emails and other files that should have been there were just gone. Even though he couldn't prove that the defendants deleted emails, the judge ruled that they were intentionally trying to hide evidence and mislead the court.

IX. DIGITAL FORENSIC INVESTIGATION ARENA

Investigation for single computer: For the laptop and the stand-alone personal or work computer, the investigation into a single computer is probably the easiest type undertaken. Even here, the level of difficulty is growing as PCs become more powerful and the size of the storage media increases, and as the ways in which they connect to networks increase and become less obvious (\ViFi,WiMax,and Bluetooth). When dealing with a single PC, elements to be considered include- The PC, Peripheral devices, Storage media, associated material. Invetigation for networked computer: Network forensics deals with the capture, recording, and analysis of network events in order to discover evidence and to determine the source of an incident or network-related problem. Network forensics mainly deals with information related to networks on a number of different levels, such as topology, the configuration of the network and the individual elements, network traffic, and the relevant hardware devices that form the network.

Investigation for Mobile and Tabs: When dealing with the handheld device, a set of additional considerations must be addressed to ensure that any evidence they contain is captured in a manner that makes it useable in any criminal or civil action. The term "handheld device" is used to describe a range of devices that continues to expand. It includes electronic organizers, personal digital assistants (PDAs), mobile phones (cell phones) and increasingly, as they reduce in size, devices that would previously have been called laptop computers. An increasing convergence in the capabilities of small devices is underway, and the distinction between the whole range of handheld devices is shrinking.

In addition to the types of devices previously detailed, a number of other electronic devices fall into the handheld group that might be encountered during searches, which may contain evidence relevant to the investigation. These include pagers, digital cameras, and MP3 and MP4 players.

Electronic organizers and PDAs range from very small and very cheap devices that may contain anything from a few telephone entries to expensive devices that have as much processing power and storage as the desktop PC of only a few years ago. These devices work on a range of operating systems, such as Linux, Windows CE, the Halm OS, and the Svmbian OS. Mobile (cell) phones range from devices capable of making phone calls and storing a small list of phone numbers to modern 3G-capable devices that have the full functionality of a PDA.

Small laptops such as the Nokia Lumia, the Toshiba Libretto, and the HTC "Shift" are fully functional laptops that have been reduced in size to the point where they are treated very much like other handheld devices.

X. CONCLUSION AND POLICY RECOMMENDATIONS

- A quality digital investigation system should be encouraged. Professional crime investigation systems should examine the need for fully trained and qualified forensic experts with competent investigative and support staffs. Specifically, Govt. should reexamine their current digital investigation systems to determine whether they can conduct appropriate, timely, and reliable investigations or not.
- Digital Forensic laboratories should be established.
- An organized attempt should be made to determine the quantity of forensic service providers outside crime laboratories by Ethiopian Government.
- There should be outreach to all forensic service providers, including noncrime lab providers, to advise them of professional and governmental assistance programs.
- The needs of the forensic community should be monitored on an ongoing, systematic basis.
- Professional models for training and establishing competency should be encouraged.
- Quality graduate education in forensic science programs should be encouraged. A program to eliminate or forgive student loans for graduates who obtain full-time employment in public forensic science institutions is one alternative that should be considered.
- Forensic community supports accreditation of organizations and certification of practitioners.
- A formal mechanism, such as an advisory board or focus group, should be established to facilitate coordination and collaboration between Federal laboratories and the forensic community.
- The forensic science organizations support the creation of a National Forensic Science Commission to assess the needs of the forensic science community and to stimulate public awareness of and interest in the uses of forensic technology to solve crimes. The commission should be tasked to undertake a comprehensive review of the role of forensic science in the criminal justice system, cost/benefit analysis of the value of forensic science to the administration of justice, needs of forensic science providers, and policy issues with respect to forensic science.

REFERENCE

[1]. Duwairi, A., Manimaran, G.: Novel Hybrid Schemes Employing Packet Marking and Logging for IP Traceback. IEEE Trans. Parallel and Dist. Sys. 17(5). 403-418 (2006)

[2]. Jing, Y.N., Tu. P.. Wang. X.P., Zhang. G.D.: Distributed log based scheme. In: Proc of 5th Int" I. Conf. on Computer and Information Technology (2005)

[3]. Gong. C., Sarac, K.: A More Practical Approach for Single-Packet IP Traceback using Packet Marking and Logging. IEEE Trans. Parallel and Dist. Sys. 19(10), 1310-1324 (2008)

[4]. Jing. W.X., Lin, X.Y.: IP Traceback based on Deterministic Packet Marking and Logging. In: Proc. IEEE Int'l. Conf. on Scalable Computing and Comm.. pp. 178-182 (2009)

[5]. Paruchuri. V., Durresi, A., Kannan, R.. Iyengar, S.S.: Authentic Autonomous Traceback. In: Proc. 18th Int'l Conf. Adv. Info. Networking and Appln., pp. 406-413 (2004)

[6]. Gao, Z., Ansari, N.: A practical and robust inter-domain marking scheme for IP trace- back. Computer Networks 51 (3), 732-750 (2007)

[7]. Korkmaz. T., et al.: Single packet IP traceback in AS-level partial deployment scenario. Int. J. Security and Networks 2(1/2), 95-108 (2007)

[8]. Castelucio, A.. Ziviani, A., Salles, R.M.: An AS-level Overlay Network for IP Traceback. IEEE Network. 36-41 (2009)

[9]. Carrier, B.. Shields, C.: The Session Token Protocol for Forensics and Traceback. ACM Trans, on Info. System Security 7(3), 333-362 (2004)

[10]. Demir, O., Ping, J., Kim, J.: Session Based Packet Marking and Auditing for Network Forensics. Int'l. Journal of Digital Evidence 6(1), 1-15 (2007)

[11]. Cohen, MX: Source attribution for network address translated forensic captures. Digit. Investig. 5(3-4). 138-145 (2009)