The International Journal Of Engineering And Science (IJES)
|| Volume || 6 || Issue || 1 || Pages || PP 01-07 || 2017 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Proposed Effective Solution for Cybercrime Investigation in Myanmar

Tin Maung Maung[1], Mie Mie Su Thwin[2]
[1]*Cyber Security Research Lab, UCSY*
[2]*Associate Professor, Cyber Security Research Lab, UCSY*

----------**ABSTRACT**----------
The rapid increase of smart technologies and Internet usage creates new attack surfaces for cybercrime. In society, information is the new challenge for security, privacy, and cybercrime. In this paper, an effective solution has been proposed for cybercrime investigation in Myanmar. The usage of Standard Cyber Laws and Policy for Cybercrime Investigation can provide an ethical, secure and monitored computing environment. This solution provides a secure analysis on both logical and physical data extractions. Acceptable Evidences can be obtained by examining sensible clues from any digital devices such as computer, mobile smart phones, tablets, GPS and IoT devices via traditional or cloud. The most important part of cybercrime investigation is to gather the "relevant" and "acceptable" information for cyber evidence on court. Therefore, investigators need to emphasize how file system timestamps work. This paper emphasizes on the comparative timestamps of the various file and window operating systems.

Keywords: *cloud, cyber evidence, cybercrime forensics, IoT devices and timestamps.*

Date of Submission: 10 January 2017 Date of Accepted: 01 February 2017

I. INTRODUCTION

Cybercrime forensics investigation is not a new field but still based on new practices and new threats encountered; it is an evolving one. Forensic investigation is the vital phase for Cybercrime forensic analysis because the analysis totally depends upon the quality, fine granularity, effectiveness, systematic and legal investigation process being carried out by the computer forensics experts. So, for that purpose the investigations should be systematic, expert, customized and sound enough making it a process been done in less time and therefore causing more relevant information to be collected and subsequently being investigated.

Digital Evidence – 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.

The IT security is the most complex area inside the digital world because there are exposed to a huge number of threats and dozens of malwares (virus, Trojans, spies and worms) come up every single day, including other hundreds of variants. Malwares are becoming more sophisticated by adding rootkits techniques in their codes, by using anti-forensic techniques to hinder the analysis by experts, by abusing of encrypted codes and lots of other tricks. One area of growing concern among forensic examiners is what and where a file has been. While many digital artifacts exist to prove that a file was opened, the most essential piece of information needed is the file's timestamp information. This paper proposes an overall solution that can be followed systematically to produce forensically sound evidence. This solution will support and cover to collect evidence data in different forensics field such as static, cloud and social network environments. The solution is an adaptation or combination of several existing forensic stages. We are going to use some freeware tools, ultimate tools and our own tools in this solution. The purpose of doing this research is to provide an applicable forensics solution for our beloved country Myanmar.

The paper is structured as follows: the subsequent section will briefly discuss some generally accepted solutions, the third section will clarify the related work, section four will introduce the proposed CCFIM solution, the section five will express value of timestamps clue for cybercrime investigation, the section six will present observation on various window operating systems and closing remarks will be made in section seven.

II. BACKGROUND

Many process models have been proposed for digital investigation procedures and researchers have mainly focused on the nature and number of steps involved in the investigations process of cybercrimes.

2.1. Kruse and Heiser Model [1]

The earliest known methodical approach employed to computer forensic. The first phase involves acquiring the data evidence. It is recommended that the data integrity should be ensured. The second step is to check the validity of the collected data by authentication process. The third phase is the analysis of data keeping intact the data integrity and validity. A generalized view of the solution is given in Fig. 1 below.

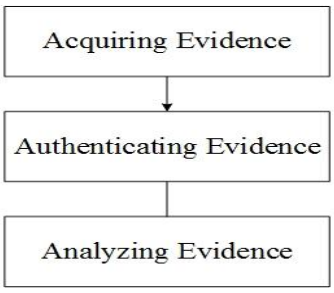

Figure 1. Kruse and Heiser model [1]

2.2. US department of Justice (USDOJ) Model [2]

This model is primarily based on the standard crime scene investigation protocol and comprises of four steps, the collection, examination, analysis, and reporting. The fourth step is reporting or presenting of evidence in the court of law. The simplest schematic workflow is shown in Fig. 2.

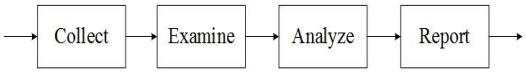

Figure 2. USDOJ model

2.3. Systemic Digital Forensic Investigation (SRDIFM) Model [3]

Agarwal and colleagues in 2011 proposed a systemic approach to digital forensic investigation. There are 11 phases in this model named Preparation, securing the scene, survey and recognition, documentation of scene, communication shielding, evidence (both volatile and non-volatile) collection, preservation, examination, analysis, presentation, result and review (Fig.3).

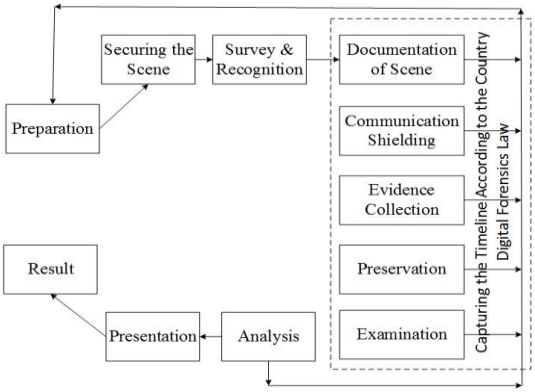

Figure 3. A systematic digital forensic investigation model

III. RELATED WORK

The purpose of this research was to develop a digital forensics framework that will serve as a blueprint for Kenyan courts of laws in apprehending digital criminals. Existing DF models were surveyed and then adopted to create a specific application framework. The finding can be used by both government and private agencies in developing countries like Kenya as a guide in providing Digital Forensics services whether Internal investigation, disciplinary hearing or court case. [4]

This paper aims at defining a new approach to the problem of evidence examination, studying the practical experience of a case study within the Italian legal system concerning techniques of forensic computer analysis based on command line. There are consist of six phases; Creating hash code phase, Image copy phase, Data recovery/data carving phase, Disk analysis phase, Mount partition phase and Files system analysis. In this paper the forensic analysis focuses on non-volatile memory. The future work concerns the normalization of the model

to the other legislations, defining e new model in relation to different types of media such as mobile phone, tablet and volatile memory and into a cloud computing. [5]

A Generic Computer Forensic Investigation Model (GCFIM) based on the grouping of the overlapping and similar phases, Phase 1 of GCFIM is known as Pre-Process. And Phase 2 is Acquisition & Preservation phase. Next phase is Analysis and after that Presentation phase comes. Last Phase is Post-Process phase. This phase relates to the proper closing of the investigation exercise and the lesson can be learnt and used for improvement of the future investigations. [6]

Domain Specific Cyber-Forensic Investigation Process Model (DSCFIPM) can serve the purpose of laying foundation for providing secure and monitored computing environment to university students and employees. This model includes the tailoring of existing process models to the particular domain of higher education institutes. With the growing access of computing resources and internet to the students, employees and overall citizens, it is the need of time that organizations should establish and maintain their cyber forensics analysis policy along with whole process to be followed in case of any cybercrime scene reporting. [7]

This paper has discussed how the stages on Digital Forensics Readiness (DFR) within the solution of the preservation of digital evidence. Minimize the duration and cost of the investigation, it has proposed a new scheme called Digital Forensics Readiness Schema (DFRS). In principle, DFRS have to accommodate the interests and the need to conduct an investigation in order to readiness digital forensic process. [8]

As forensic examiners, there is no shortage of techniques to prove that something occurred and when it occurred. However, being able to prove the Why, How and most importantly, when a specific file(s) was created or used goes further to prove who was behind the keyboard during the time of the incident than merely finding the file(s) and determining that the case is solved. This paper includes compares and experimental results of file system timestamps work not only between NTFS, FAT32 and exFAT, but also between Windows Operating Systems testing with Window XP, Window 7, Window 8. [9]

From the proposed solutions mentioned above, the following can be seen quite clearly:

- Each of the proposed models builds on the experience of the previous,
- Some of the models have similar approaches,
- Some of the models focus on different areas of the investigation.

Perhaps the best way to balance the process is to ensure the focus remains on achieving the overriding goal: to produce concrete evidence suitable for presentation in a court of law.

In this paper, we present an effective solution for Cybercrime Investigation in Myanmar. This solution can even support non-technical person well handle for Cybercrime Forensics in Myanmar. Each stage of our Proposed Solution can support Cybercrime investigator to get the must to do list and facing decision choice for possible different environments. Evidences are the needle in the haystack. Therefore, this proposed solution assists for seizing relevant and meaningful evidence and reduces or saves time and cost consuming. It is from existing gaps that we developed a solution that will provide guidance in digital forensics processes, particularly in developing countries like Myanmar.

IV. THE PROPOSED APPLICABLE CCFIM SOLUTION

4.1. PROBLEM STATEMENT

In Myanmar, a widespread crime being perpetuated by using mobile phones like terrorism, drug trafficking, money laundering, extortion, fraud, hate messages, and incitement are on increase. But more often than not evidence presented before Myanmar courts of laws are inadmissible due to lack of proper Digital Forensics solution. Ministry of Transport and Communication published some regulatory policies like requiring all mobile subscribers to register their SIM card before 01 April 2017. In Myanmar, ICT is rapidly developing with international service provider such as Telenor, Ooredoo. Internet is widely used to share information and easily then its impact is large. It is very important that the gathered information need not only to be fast but also to be in correct manner.

Therefore, this solution is important in investigating cybercrimes using ICT in Myanmar. The primary objective of this solution is to carry out an organized and structured investigation in order to preserve, identify, extract, document and interpret information that is then utilized to prevent, detect and solve cybercrimes. There is no research about which Cybercrime Investigation System is important and effective for Cyber Security in Myanmar.

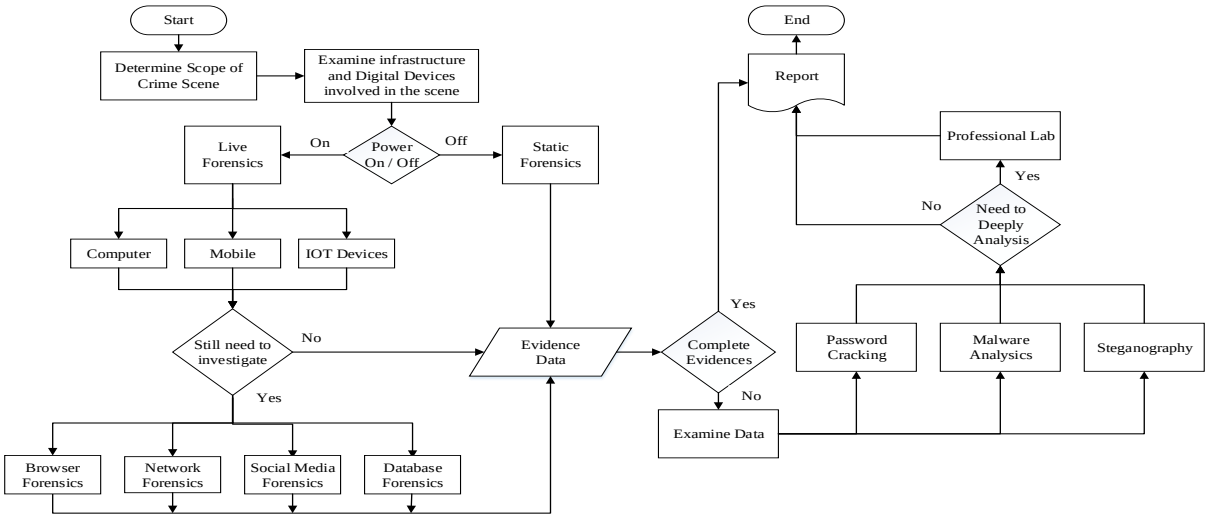

Figure 4. The Proposed Solution

4.2. The Proposed Solution

As the ICT sector grows in Myanmar, services will evolve and risks will increase. For example, online-banking, ecommerce, e-government, email, social networking and online shopping, etc. Therefore, a high-level solution of the overall solution(CCFIM) is proposed to support Cybercrime Forensics Investigation in Myanmar.

As a very first step, we do need to determine the scope of the Crime Scene and then examine infrastructure and digital devices involved in the scene. After that we investigate the static or live forensics according to the device status.

By traditional digital forensics it is focused on examining a duplicate called copy of disk to take out memory contents, like the files which are deleted, history of web browsing, file fragments, network connections, opened files, user login history, etc. In static analysis, different kind of software and hardware tools are used for memory dumping and sorting of evidence data for analysis and presentation purpose.

Live Forensics Investigation flow depends on the situation and cases to be investigated. Without any specific requirement, a typical live forensics investigation flow can be depicted in solution. The most important information to be verified and identified during the investigation is to identify the target machine being used for illegal upload of identified matter together with the identity of the user, current user and any web related account information. According to this requirement, the live forensics toolkits should be formulated to collect relevant data.

Firstly, capture physical and virtual memory and then examine the current network connections. Secondly, investigate the files and registry information and current execution process information. After that, collect the current connected network, IP address, and check the network status such as current network path and network broadband device configuration. Also, investigate the current user information and system configuration. Moreover, preset the process and service list and also collect file and directory information and event log.

Therefore, forensic examiner can extract current process lists, CPU, Cache, Memory, Network information, Data sharing and transfer archival media, RAM and Storage device image, text messages, call histories and address books from various makes and models of computer, mobile smart phones, tablets, GPS and IoT devices that can serve as cyber evidence. For some circumstances, there will be more to investigate information about Internet Forensics Usage, inspector can extract specifies evidence data from Web browsers, chat, email, and social networking sites. These investigations assist in the recovery of Internet and application data from computers as well as smart devices data that are used to conduct these transactions.

As a result of storage device imaging for static forensics, inspector can examine or analyze such as malicious software, advanced persistent threat and stenography process. If there is some sample still need to investigate, examine at Professional Forensics Lab and extract the secret information and analyze these data and send to the court.

V. IMPORTANCE OF TIMESTAMPS CLUE FOR CYBERCRIME INVESTIGATION

Digital/ Electronic evidence is extremely volatile. Once the evidence is contaminated it cannot be de-contaminated. Chain of Custody is crucial. The courts acceptance is based on the best evidence principle. With computer data, printouts or other output readable by sight, and bit stream copies adhere to this principle. With all

of this information, investigators can then provide a "What" the file is, "Where" the file resides, "Why" it could be residing there, "How" it got on the device and most importantly narrow the "Who" put it there.
For example, if forensicator notices establishment of suspicious network connections, firstly, lookup the IP address and port number. After that check the process ID timestamp. Next, examiner gets the process name and times stamps according to the parent process ID. Finally, know the associated entities for open registry keys, open files and associated DLLs. Therefore, file timestamp is one of the key factors for cybercrime investigation.

5.1. Timestamping Definitions

Before going in depth for the knowledge and datasets, it is key that specific definitions of timestamp be understood.

- Creation Time (C): This is the time the file was created (Carrier, 2006).
- Modified Time (M): Time content of a file was last modified (Lee, 2015).
- MFT modified Time (B): Time that the metadata of the file was last modified (NTFS) and is not showing in Windows under Properties. (Carrier, 2006).
- Accessed Time (A): Approximate time file data was last accessed (Lee, 2015).

5.2. FAT Filesystem

One of the most universal file systems across all four OS platforms is the File Allocation Table, or FAT. The MAC timestamps for FAT as being a 16-bit value where 7 bits are related to the year, 4 bits for month and 5 bits for the day. The same concept with a 16-bit value being used for hours, minutes and seconds.

5.3. ExFAT Filesystem

One of the more recent file systems created in 2006, exFAT is also known as FAT64 (Rusinovich et. al.). The creation of this file system was largely pushed by those in the film industry requesting a file system that could perform continuous recording in a single file that was not restricted to previous FAT file size restrictions.

5.4. NTFS Filesystem

New Technology File System(NTFS) employs B-tree indexing for providing efficient storage of many files and fast lookups, which changes in a structure of the directory when file commands are operated. Like other components of filesystem, the directory index also leaves important traces in the process of file system operation.

VI. OBSERVATIONS AND FINDINGS

File timestamps will be gathered using FTK Imager version 3.4.2.6 and Belkasoft Evidence Center Ultimate 7.5.

6.1. Observations 1 – XP, Win7, Win8, Win 10 Standalone

6.1.1. File Creation

Creation of Test.txt on all four boxes yielded this information pertaining to C, M, A, and B dates respectively.

Table 1. File Creation on Standard Systems

Date	Win XP	Win 7	Win 8.1	Win 10
C	10/30/2016 04:17:10	10/30/2016 07:36:55	10/30/2016 04:56:31	10/30/2016 04:14:19
M	10/30/2016 04:17:10	10/30/2016 07:36:55	10/30/2016 04:56:31	10/30/2016 04:14:19
A	10/30/2016 04:17:10	10/30/2016 07:36:55	10/30/2016 04:56:31	10/30/2016 04:14:19
B	10/30/2016 04:17:33	10/30/2016 07:37:14	10/30/2016 04:56:50	10/30/2016 04:14:35

6.1.2. Copy and Paste

Files were created on:\Users\%USERNAME %\Desktop. From there they were right-clicked, copied and pasted in the C:\Users\%USER NAME%\MyDocuments folder. The following information was recorded.

Table 2. Copying of files on Machines

Date	Win XP	Win 7	Win 8.1	Win 10
C	10/30/2016 04:20:22	10/30/2016 07:41:54	10/30/2016 05:22:00	10/30/2016 04:56:14
M	10/30/2016 04:17:10	10/30/2016 07:36:55	10/30/2016 04:56:31	10/30/2016 04:14:19
A	10/30/2016 04:20:22	10/30/2016 07:41:54	10/30/2016 05:22:00	10/30/2016 04:56:14
B	10/30/2016 04:17:33	10/30/2016 07:41:54	10/30/2016 04:56:50	10/30/2016 04:14:35

6.1.3. Cut and Paste

Files were created on the C:\Users\%USER NAME%\Desktop. They were then right-clicked, cut and pasted to C:\Users \%USERNAME% \MyDocuments\EXAMPLE folder. The following information was recorded.

Table 3. Moving of file on Machines

Date	Win XP	Win 7	Win 8.1	Win 10
C	10/30/2016 04:17:10	10/30/2016 07:36:55	10/30/2016 04:56:31	10/30/2016 04:14:19
M	10/30/2016 04:17:10	10/30/2016 07:36:55	10/30/2016 04:56:31	10/30/2016 04:14:19
A	10/30/2016 04:17:10	10/30/2016 07:36:55	10/30/2016 04:56:31	10/30/2016 04:14:19
B	10/30/2016 04:25:50	10/30/2016 07:45:48	10/30/2016 05:38:18	10/30/2016 05:23:55

6.2. Observations 2 – Cross OS Win 10 to Win 7 via exFAT

Table 4. Cross OS Win 10 to Win 7 via exFAT

Date	Win 10	Win 7
C	9/4/2016 18:08:05	9/4/2016 23:08:05
M	9/8/2016 13:42:37	9/8/2016 08:42:38
A	9/8/2016 16:59:20	9/8/2016 23:08:05
B	9/4/2016 19:59:20	9/4/2016 18:08:05

6.3. Observations 3 – Win 7 to NTFS and FAT32 Partitions

Table 5. Win 7 to NTFS and FAT32

Date	NTFS		FAT 32
	CUT	COPY	
C	9/26/2016 07:36:55	9/26/2016 07:41:54	9/26/2016 13:24:01 CST
M	9/26/2016 07:36:55	9/26/2016 07:36:55	9/26/2016 10:44:20CST
A	9/26/2016 07:45:48	9/26/2016 07:41:54	9/26/2016
B	9/26/2016 07:45:48	9/26/2016 07:41:54	N/A

6.4. Observations 4 – Win 7 to NTFS and FAT32 Partitions

Table 6. Win 8 to NTFS and FAT32

Date	NTFS		FAT 32
	CUT	COPY	
C	11/6/2016 11:05:42	11/6/2016 11:49:01	11/6/2016 06:35:42 CST
M	11/6/2016 10:40:00	11/7/2016 10:36:56	11/6/2016 06:10:00 CST
A	11/6/2016 11:10:18	11/6/2016 11:18:43	11/6/2016
B	11/6/2016 11:10:18	11/6/2016 11:18:43	N/A

6.5. Observations 5 – Win10 to NTFS and FAT32 Partitions

Table 7. Win 10 to NTFS and FAT32

Date	NTFS		FAT 32
	CUT	COPY	
C	9/26/2016 07:36:55	9/26/2016 07:41:54	9/26/2016 13:24:01 CST
M	9/26/2016 07:36:55	9/26/2016 07:36:55	9/26/2016 10:44:20CST
A	9/26/2016 07:45:48	9/26/2016 07:41:54	9/26/2016
B	9/26/2016 07:45:48	9/26/2016 07:41:54	N/A

6.6. Findings

The most affected B Attribute which is the MFT Entry Modified time. That's why Forensics Experts need to be take into account upon this attribute. The value of the Attribute B changes according to the processing nature of the files. The A Attribute as the file's Access Times attribute of exFAT thumb drive is untrusted because NTFS resolved to the same time as B Attribute, which is the MFT modified timestamp. So, when doing forensic analysis, the files should require further analysis to determine true times.

VII. CONCLUSION

This solution has been developed to be a modular system. It is very extensible when a new tool or module develops in it. It could be plugged into the solution easily. New forensic challenges arise with the introduction of newly released and latest operating systems. While on one hand, these newly released versions of Windows are aimed at making things easier for users, many of the functions. Having the capability of knowing when the file was created and what else was created around it or during the modification time or MFT content change time could open an entirely new window that would have been missed through timeline analysis or more traditional forensic examinations.

REFERENCES

[1] W. G. Kruse and J. G. Heiser, Computer Forensics: Incident Response Essentials, 1st ed., Addison Wesley, 2002.

[2] M. Reith, C. Carr, and G. Gunsch, "An examination of digital forensic models," IJDE, vol. 1, issue 3, 2002.

[3] A. Agarwal, M. Gupta, S. Gupta, and S. C. Gupta, "Systematic digital forensic investigation model," IJCSS, vol. 5, issue 1, pp. 118-131, 2011.

[4] Obwaya Mogire, "Digital Forensics Solution for KENYAN Courts of Laws," 2011.

[5] Gianni Fenu and Fabrizio Solinas, "Computer Forensics Investigation an Approach to Evidence in Cyberspace," 2013, Italy.

[6] Yunus Yusoff, Roslan Ismail and Zainuddin Hassan, "Common Phases of Computer Forensics Investigation Models", IJCSITvol. 3, no. 3, 2011.

[7] Rabil Shafique Satti and Fakeeha Jafari, "Domain Specific Cyber Forensic Investigation Process Model", Journal of Advances in Computer Networks, Vol. 3, No.1, March 2015.

[8] Ahmad Luthfi and Yudi Prayudi, "Process Model of Digital Forensics Readiness Scheme (DFRS) as a Recommendation of Digital Evidence Preservation", IEEE, 2015.

[9] Tony Knutson and Richard Carbone, "Filesystem Timestamps: What Makes Them Tick?" GIAC GCFA Gold Certification 2016.

[10] Esan P. Panchal, "Extraction of Persistence and Volatile Forensics Evidences from Computer System", International Journal of Computer Trends and Technology(IJCTT)-volume Issue5-May 2013.

[11] Gyu-Sang Cho, "NTFS Directory Index Analysis for Computer Forensics," IEEE, 2015.

[12] Lei Chan, Lanchuan Xu, Xiaohui Yuan and Narasimha Shshidhar," Digital Forensics in Social Networks and the Cloud," IEEE, 2015

[13] Shams Zawoad and Ragib Hasan, "FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things," IEEE, 2015.

[14] Brian Carrier, "File System Forensic Analysis", 2005, USA.

Biographies and Photographs

Name – Mr. Tin Maung Maung
Age – 33
Material Status - Married
Graduated B.Sc., Defense Service Academy, M.Sc., University of Computer Studies(Yangon)
Current Education – Ph.D. Research Candidate, Cyber Security Research Lab, University of Computer Studies, Yangon (UCSY)
Nationality – Myanmar
Working Experiences – Technical staff at Myanmar Airforce, Research interest is in cyber forensics, information security and Internet of Things(IoT)

Name – Dr. Mie Mie Su Thwin
Age – 45
Material Status – Single
Graduated – Ph.D Computer Science, University of Computer Studies, Yangon
Working Experiences – Associate Professor (20 years), mmCERT (6 years)