A Novel Process Framework for Digital Forensics Tools: Based on ISO/IEC 27037:2012

Da-Yu Kao, Central Police University, Taiwan
Guan-Jie Wu, Central Police University, Taiwan
Ying-Hsuan Chiu, Central Police University, Taiwan

The Asian Conference on Business & Public Policy 2014
Official Conference Proceedings

Abstract

Cybercrime has reached unprecedented proportions nowadays. In order to assist digital forensics specialists, many digital forensics tools have been designed from open source programs or business software, which are based on law, policy and practice. Cybercrime examiners often encounter a dilemma in choosing proper tools on the workflow of identifying, collecting, acquiring and preserving digital evidences. This study develops a novel process framework to examine some popular free tools, and proposes a standard evidential suite, which can be performed on the following three periods: prelusion, incident and aftermath. The nature of this framework suggests substantial benefits from using ISO/IEC 27037:2012 approach as a critical reference for digital forensics process. To ensure the quality of evidence collection, this framework may help to clarify the issue at hand, retain most of the useful information, and provide details of how this novel approach links evidence to a verifiable reconstruction of events at the crime scene. This framework allows for a stronger presentation of evidence in a cybercrime case.

Keywords: Criminal Justice Policy, ISO/IEC 27037, Cybercrime, Digital Forensics

1. Introduction

Many banks, institutions, corporations, or businesses often employ data networks to process digital transactions and store any other relevant data. The internet was created to serve the communication needs of a well-defined community. Internet is continuously evolving as the world continues to become more connected every day. However, there is a much wider and varied community of users and services with conflicting interests. Data networks have become the target of frequent attacks to steal electronic files, and lead to loss of credit card information, or other purchasing sensitive information (Vacca, 2014). Cybercrime has impacted our lives (Raghavan, 2014). This unauthorized access of computer system can be internal users or external offenders, a person who would attempt to break into network servers that they have no permission to access. Cybercrime has reached unprecedented proportions nowadays.

When there are some suspicious activities of alert detection on a running system, the system administrator in inner organization should find some human artifacts. If there is something abnormal, that is about time to consider whether the organization should prosecute the offender. When there is an individual complaint or alert detection on abnormal activities, an incident report is necessary to formulate an investigation plan, determine the worth assessment of coordinated resources, and obtain an authorization of search warrant. A security breach is the violation of computer security policies in a system. Responding to a security breach is challenging to keep up with new technologies. The auditing log is an alert to systems administrators, who may or may not choose to pursue further investigation (Vacca, 2014). This growing need of cybercrime investigation and digital forensics has sparked heated debates about tools, terminology, definitions, standards, and other aspects. It should come as no surprise that this study reflects the issue of 'accessing the original data' in the terminology debate. The need of accessing the original data is considered a necessity by internal system administrators and incident response specialists (ISO, 2012). This study presents an approach to implement digital forensics tools and discusses some related issues.

In Section 2, the following literature reviews are discussed: ISO/IEC 27037 Guidelines for Digital Evidence and ACPO Good Practice Guide for Digital Evidence. Section 3 develops a novel process framework on four processes: Identification, Collection, Acquisition and Preservation. The discussions on personnel competency in digital forensics process are presented in Section 4. The conclusion is drawn in Section 5.

2. Review

Cybercrime examiners often encounter a dilemma in choosing proper tools on the workflow of identifying, collecting, acquiring and preserving digital evidences. Agencies used to recommend that investigators just pull the plug on live computers and take everything with them. As cybercrime became more prevalent, data examining operations became flooded. When computers are turned on at a location, forensic technicians frequently perform a live analysis about the software and network before shutting down equipment (Stephenson, 2014). The dispute of live analysis on the original evidence can be settled and based on ISO/IEC 27037: 2012. The follow-

up research will implement a suitable forensic toolkit in a live analysis for internal system administrators or incident response specialists. To have a better understanding in a live analysis, the issues on digital forensics are reviewed below.

2.1 ISO/IEC 27307 Guidelines for Digital Evidence

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. ISO/IEC 27037 provides guidelines for specific activities in handling potential digital evidence; these processes are: identification, collection, acquisition and preservation of potential digital evidence. This standard ensures that responsible individuals manage potential digital evidence in practical ways that are acceptable worldwide, with the objective to facilitate investigation involving digital devices and digital evidence in a systematic and impartial manner while preserving its integrity and authenticity (ISO, 2012).

As the cybercrime increases in the modern society, the need for digital forensics becomes an integral part of our society, and brings the justice from increasing numbers of the cybercrime. Errors can be made when the examiner investigates cybercrime events. It is essential that digital examiners develop appropriate skills to get round these problems. In order to ensure that the evidence is admissible in court, examiners should take some rigorous procedures on some recommendations (ISO, 2012). There is also an urgent need to set up a standard in the evidence collection issues. Digital forensics is the science of recovering digital evidence from a digital source under forensically sound conditions (Casey, 2011). Forensics is heterogeneous and digital forensics is no exception to this. Digital forensics is a branch of forensic science that is used to encompassing the data investigation in digital devices.

2.2 ACPO Good Practice Guide for Digital Evidence

Every case is different. Forensics is intangible by nature. Investigating human misuse of computers creates some technical puzzles, especially when offenders attempt to conceal their activities on the internet (Casey, 2010). This good practice guide for digital evidence was produced by the ACPO (Association of Chief Police Officers) Crime Business Area and was originally approved by ACPO Cabinet in December 2007. The purpose of this document is to provide guidance not only to assist law enforcement but for all that assists in investigating cyber security incidents and crime. It is updated according to legislative and policy changes. It is also generally adopted by law enforcement agencies all over the world. The principles of digital evidence are listed below (ACPO, 2012).

- Principle 1: No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.
- Principle 2: In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
- Principle 3: An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

- Principle 4: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

3. A Process Framework for Digital Forensics Tools

As the cybercrime increases nowadays, there is an urgent need to set up a standard, which is constructed by extending and unifying the existing approaches. There is a lack of standards in the digital forensics processes. In order to obtain the required evidences that are needed in the court for prosecution, several works have been carried out in the domain of digital forensics process. They can include proactive, active and reactive attitude (Roger & Achille, 2012). None of the proper investigation approaches have taken into consideration three perspectives despite they are linked together in the case management of cybercrime within an organization.

This study tries to provide an in-depth guide to digital forensics from the pioneers of the following processes (see Figure 1 and Table 1): Identification, Collection, Acquisition, and Preservation. There are multiple tools, both free and commercial, that can copy physical memory to a storage device in Window-based or Unix-based system. This section combines 75 free command-line digital forensics tools in a Window-based batch file as a live incident toolkit, which is further categorized into volatile data and non-volatile data (see Table 2-1, 2-2, 2-3, and Table 2-4).

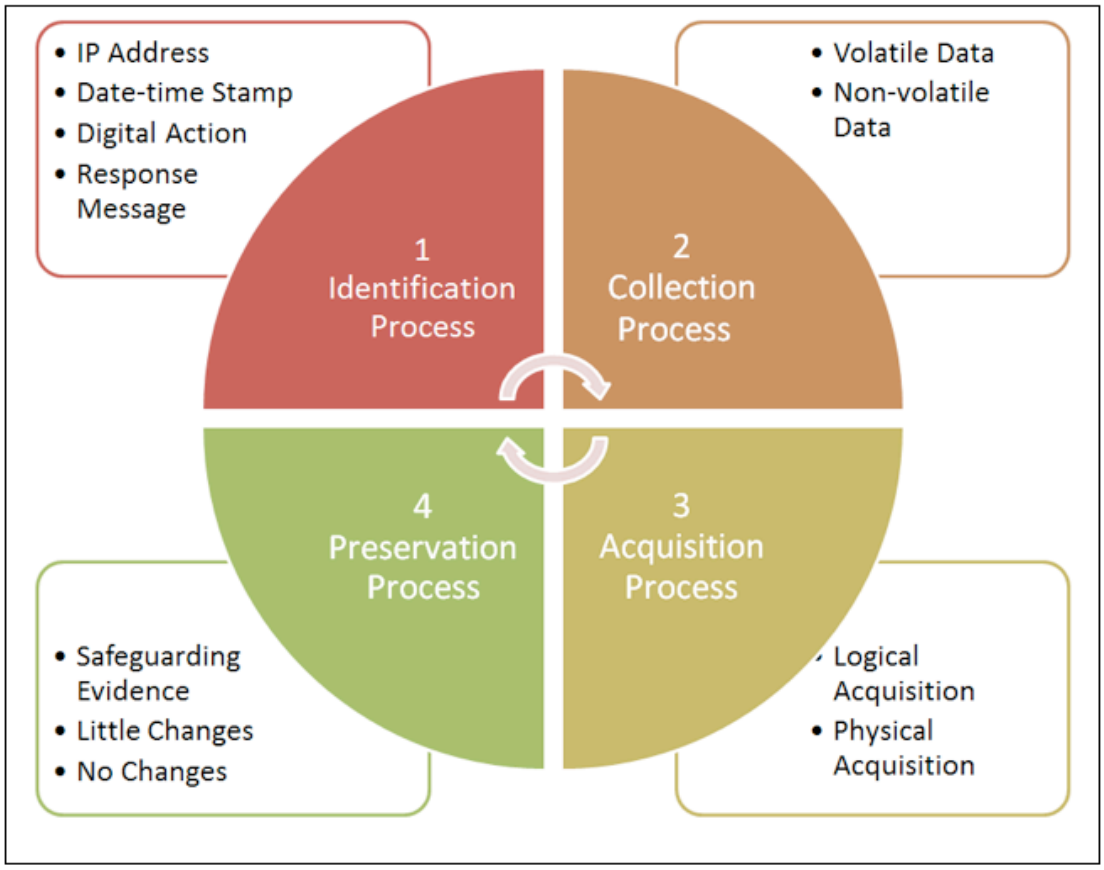

Figure 1: A Process Framework for Digital Forensics

Table 1: The Framework Concern for Digital Forensics

Concern / Process	Period			Goal
	Prelusion	Incident	Aftermath	
Identification	Log Identification (IP Address and Date-time Stamp)	Incident Identification (Digital Action)	Evidence Identification (Response Message)	Identify Relevant Evidence to the Incident
Collection	Network Collection (Volatile Data)	Real-time Memory Collection (Volatile Data)	Host Image Collection (Non-volatile Data)	Gather Evidential Items to Prove Something
Acquisition	Prelusion Detection (Logical Acquisition)	Incident Investigation (Physical Acquisition)	Aftermath Forensics (Physical Acquisition)	Adopt Suitable Methods to Produce a Copy
Preservation	Safeguarding Evidence	Little Changes	No Changes	Maintain the Reasonable Integrity of the Evidence

To quickly process data, the computer needs to move the data from the slow hard drive into the faster random access memory (RAM). We examine volatile memory and its role in live forensics. Live forensics is the relatively new concept of gathering evidence while the computer is in operation, unlike dead forensics. There is a considerable amount of very important information in RAM that is part of the live data related to both the operating system and the running programs. Collecting live data is not the end of the process. Live forensics has the potential for gathering much more timely evidence than dead forensics (Stephenson, 2014).

These tables have illustrates the four-element observation of auditing log in digital forensics tools. Their outputs are also explored from the four elements of auditing logs: IP Address, Date-time Stamp, Digital Action, and Response Message. These four elements are the key to prosecute any offenders.

3.1 Identification Process: Identify Relevant Evidence to the Incident

The identification process should identify electronic storage devices, which may contain potential digital evidence relevant to the incident. The identification process involves the search for, recognition and documentation of potential digital artifacts (ISO, 2012). Information required to keep track of these states can grouped into log identification, incident identification, and evidence identification. Always keep in mind the four elements of auditing logs within any network or computer: IP Address, Date-time Stamp, Digital Action, and Response Message (Johnson, 2013). These four elements are composed of the facts behind the evidence, which can be further identified into the different logs audited.

3.1.1 IP Address

- Network access: Take care more on the accesses to the systems and networks.
- Unexplained accounts: Watch out the unexplained administration/user accounts and their IP addresses

3.1.2 Date-time Stamp

- Malicious files: Rename malicious executable files with normal file names, and modify their date-time stamps.
- IP address: The date-time stamp is often followed by the source and destination IP address.

3.1.3 Digital Action

- Alerts or alarms: During initial response efforts always notice the alerts or alarms of unusual actions in Firewall, Intrusion Detection System (IDS), or anti-virus products.
- Unusual actions: Suspicious entries of unusual actions in the system or network activities.

3.1.4 Response Message

- Successful login: Examine the file metadata of unfamiliar new files or filenames in system directories.

- Unsuccessful attempts: Keep eyes on (more than three) excessive unsuccessful login attempts.

3.2 Collection Process: Gather Evidential Items to Prove Something

The collection process gathers the physical items that contain potential digital evidence (ISO, 2012). Information required to keep track of these states can grouped into network collection (between application programs and translation servers), real-time memory collection (volatile vs. non-volatile data), and host image collection. The network log is usually hidden, but it appears automatically if a serious problem occurs. Collection is the digital evidence handling process where devices that may contain potential digital evidence are removed from their original location to a laboratory or another controlled environment for later acquisition and analysis (ISO, 2012). The collection process includes documenting the whole approach, as well as the packaging of these devices prior to transportation. Mobile phones and PDAs should be secured and prevented from receiving or transmitting data once they are identified and collected as evidence (Johnson, 2013).

3.2.1 Volatile Data

The volatility of the data should be identified to ensure the correct order of the collection and acquisition processes to obtain the best evidence. How to collect digital evidence at the incident scene is a topic constantly under debate, and no single right answer exists. Some first responders might immediately access the original data (i.e. volatile/non-volatile data collection), shut down the computer (i.e., a clean shutdown), literally pull the plug (i.e., a dirty shutdown), disconnect the computer from the network, or do nothing at all (Malin, Casey & Aquilina, 2008). However, some

crucial information is still lost no matter what kinds of actions examiners may take.

(1) System Details

The critical system details of volatile data can illustrate how the system was compromised and how the evidence was recorded. Examples include date-time stamps, network status, opening port, and running process. The system details of volatile data in live analysis are illustrated to match the four elements of auditing logs in Table 2-1.

Table 2-1: System Details of Volatile Data in Live Analysis

Type	Sub-type	No	Tool's Command	IP Address	Date-time Stamp	Digital Action	Response Message
1-1. System Details	1-1-1. Date-time Stamps	1	date /t		V		
		2	time /t		V		
	1-1-2. Network Status	3	tcpvcon	V		V	V
		4	netstat -an -p tcp	V		V	V
		5	netstat -an	V		V	V
		6	netstat -s				V
		7	net view	V			
		8	net session	V		V	
		9	net use	V		V	V
		10	NetResView /stext	V			V
		11	psfile			V	
		12	net share				V
		13	net file			V	
		14	OpenedFilesView /stext		V		V
	1-1-3. Opening Port	15	fport -p			V	V
		16	getport			V	V
		17	cports /stext	V		V	V
	1-1-4. Running Process	18	Pslist			V	
		19	Psservice config			V	
		20	Handle			V	V
		21	listdlls				V
		22	psgetsid				V
		23	pulist			V	

(2) Ephemeral Information

The ephemeral information of volatile data can demonstrate the insight of the infection. Examples include login user, auto run and table information. The ephemeral information of volatile data in live analysis is illustrated to match the four elements of auditing logs in Table 2-2.

Table 2-2: Ephemeral Information of Volatile Data in Live Analysis

Type	Sub-type	No	Tool's Command	IP Address	Date-time Stamp	Digital Action	Response Message
1-2. Ephemeral Information	1-2-1. Login User	24	Whoami				V
		25	net accounts				V
		26	userdump				V
		27	net user				V
		28	net localgroup				V
		29	psloggedon		V		V
		30	joa				V
		31	UserProfilesView /stext		V		V
	1-2-2. Autorun	32	Autorunsc				V
		33	net start				V
		34	WhatInStartup /stext		V		V
	1-2-3. Table Information	35	route print -4	V			V
		36	route print -6	V			V
		37	arp –a	V			V

3.2.2 Non-volatile Data

Non-volatile data means the data is storage in electrically addressed systems (ex: read-only memory) and mechanically addressed systems (ex: hard disks, optical disc, magnetic tape, holographic memory, and such). Electrically addressed systems are expensive, but fast; whereas mechanically addressed systems are cheap, but are slow.

(1) Host Settings

The host settings of non-volatile data can reveal the status and settings of the examined system. Examples include IP configuration, system configuration and system files. The host settings of non-volatile data in live analysis are illustrated to match the four elements of auditing logs in Table 2-3.

Table 2-3: Host Settings of Non-volatile Data in Live Analysis

Type	Sub-type	No	Tool's Command	IP Address	Date-time Stamp	Digital Action	Response Message
2-1. Host Setting	2-1-1. IP Configuration	38	hostname				V
		39	ipconfig/all	V		V	V
	2-2-2. System Configuration	40	systeminfo	V	V		V
		41	net config				V
		42	psinfo		V		V
		43	awatch /stext	V		V	V
	2-2-3. System Files	44	myuninst /stext				V
		45	dir /t:c /s %windir%				V
		46	dir /t:c /s "C:\Program Files (x86)\"				V
		47	dir /t:c /s "C:\Program Files\"				V

(2) Auditing Logs

The auditing logs of non-volatile data can support the understanding of the infection. Examples include used log, cache view and stored password. The auditing logs of volatile data in live analysis are illustrated in Table 2-2.

Table 2-4: Auditing Logs of Non-volatile Data in Live Analysis

Type	Sub-type	No	Tool's Command	IP Address	Date-time Stamp	Digital Action	Response Message
2-2. Auditing Logs	2-3-1. Used Log	48	recentfilesview /stext		V		V
		49	usbdeview /stext		V		V
		50	auditpol				V
		51	Psloglist		V		V
		52	faview /stext	V	V		V
		53	schtasks /Query		V	V	
		54	SkypeLogView /stext		V	V	V
		55	mzcv /stext	V	V	V	
		56	Mozillahistoryview /stext	V	V	V	
		57	MyLastSearch /stext		V	V	
		58	browsinghistoryview /stext	V	V	V	
		59	iehv /stext	V	V	V	
	2-3-2. Cache View	60	insideClipboard /stext				V
		61	chromecacheview /stext	V	V	V	
		62	Mozillacacheview /stext	V	V	V	
		63	IECacheView /stext	V	V	V	
		64	OperaCacheView /stext	V	V	V	
	2-3-3. Stored Password	65	dialupass /stext	V			V
		66	chromepass /stext	V	V		V
		67	mailpv /stext	V			V
		68	iepv /stext	V			V
		69	mspass /stext				V
		70	netpass /stext		V		V
		71	pspv /stext				V
		72	PstPassword /stext		V		V
		73	PwDump7				V

		74	VNCPassView /stext				V
		75	WirelessKeyView /stext		V		V

3.3 Acquisition Process: Adopt Suitable Methods to Produce a Copy

The acquisition process creates a copy of data within a defined set (ISO, 2012). Cloning is the preferred method of data acquisition. The acquisition process involves creating a digital evidence copy (e.g. complete hard disk, partition, selected files) within a defined set, and minimizing the damage to the potential digital evidence (ISO, 2012). The examiner should adopt a reliable acquisition method based on the suitable situation, cost and time, and document the decision for using a particular method or tool appropriately. Information required to keep track of these states can grouped into logical acquisition and physical acquisition.

3.3.1 Logical Acquisition

During logical acquisition, active files and non-file-based allocated space on the digital storage media may be copied; deleted files and unallocated space may not be copied, depending on the method used (ISO, 2012).

3.3.2 Physical Acquisition

There may be instances in which it is not feasible or permissible to create a physical acquisition of an evidence source, such as when the source is too large or the time is limited.

3.4 Preservation Process: Maintain the Reasonable Integrity of the Evidence

The preservation process maintains and safeguards the integrity and/or original condition of the potential digital evidence (ISO, 2012). It should be initiated and maintained throughout the digital evidence handling processes, starting from the identification of the digital devices that contain potential digital evidence. Information required to keep track of these states can grouped into safeguarding evidence, little changes and no changes.

3.4.1 Safeguarding Evidence

In order to facilitate a useful investigation with minimal interruption of inner organization activities, a fast and methodical intervention must be committed to safeguard potential digital evidence and digital devices (Roger & Achille, 2012).

3.4.2 Little Changes

Mostly open source tools acquire network connections, execute commands in memory, and make other alternations on the affected machine. It may cause alteration in volatile data. Modification of memory content is unavoidable while examiners perform live forensic analysis to collect evidence. The rationale actions should be documented if unavoidable changes were made.

3.4.3 No Changes

The preservation process involves the safeguarding of potential digital evidence and digital devices that may contain potential digital evidence from tampering or spoliation. It is better to be no spoliation to the data itself or any metadata associated with it.

4. Personnel Competency in Digital Forensics Process

As ICT devices continue to update, people must adopt new principles, methods or tools to keep in good status of handling cybercrime issues. This section describes an adjustment approach composed of two concepts in digital forensics process: core capability and dynamic capability. The details of core capability and dynamic capability are described as follows (see Figure 2).

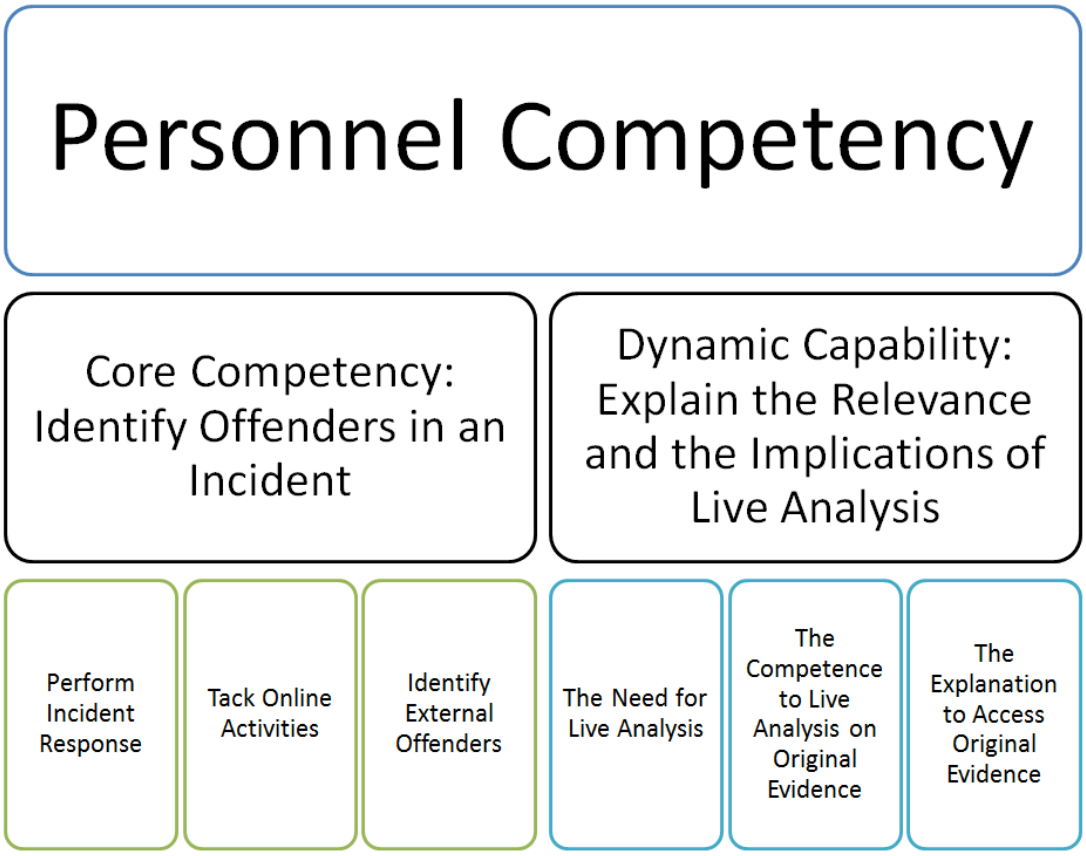

Figure 2: Personnel Competency in Digital Forensics Process

4.1 Core Competency: Identify Offenders in an Incident

It is not easy for criminal investigators to jump to conclusions. The gathering information of IP address, date-time stamp, digital action and response message is just a starting point for the investigation. Digital Action and Response Message are the only way to make sure what really happened. Additional clues must be identified and analyzed by technical experts and forensic investigators. There is no agreement in performing different tasks in the associated achievement of investigation goal. Core competency is essentially what a cyber-investigator does well that distinguishes it from other investigators. The concept of core competency includes the concept of

competitive advantage and the key ability that an agency has acquired (Prahalad & Hamel, 1990).

4.1.1 Perform Incident Response

The tools, methods, and disciplines used to perform incident response vary day by day. The incident response requires the legal disciplines and public relations to effectively handling an incident (Luttgens & Pepe, 2014). Reconstructing an event is a necessary process in forensics investigations. Because examiners have limited resources, it does not make sense to collect large volumes of data that may never have enough time to examine later. This study shows several ways to leverage strings to prove or disprove that certain actions took place on a computer system (Ligh, Case, Levy & Walters, 2014).

4.1.2 Tack Online Activities

The focus of many forensic investigations is tracking a suspect's activities based on artifacts created by web browsers, address books, email and chat clients, word processors, social media applications, and calendars (Ligh, Case, Levy & Walters, 2014). Examiners have to accomplish their activities faster than ever. In order to assist digital forensics specialists, many digital forensics tools have been designed from open source programs or business software, which are based on law, policy and practice.

4.1.3 Identify External Offenders

Since the internet is widely used for daily routine activities by all kinds of businesses, law enforcement agents have enacted stiffer penalties for hackers. We need to identify the threats posed to the network from external offenders when those from internal users are easily traceable (Vacca, 2014).

4.2 Dynamic Capability: Explain the Relevance and the Implications of Live Analysis

Dynamic capability refers to the capacity of an organization to purposefully create, extend, or modify its resource base (Prahalad & Hamel, 1990). Dynamic capability is the agency's ability to integrate, build, and reconfigure internal and external competences to address rapidly changing environments. Dynamic capability is distinct from core competency or operational capability, which pertain to the current operations of a law enforcement agency. Devices containing potential digital evidence may be in one of two states: when the system is powered on or when the system is powered off (ISO, 2012). Digital forensics is separated by dead analysis and live analysis, which identify that the system is boot or not at that time (Yadav, 2011). If the system is boot then it called live analysis. Dead analysis may lose data or information due to shutdown of digital device or removal the plug. In fact, courts are starting to compel preservation of volatile computer data in some cases, which requires digital examiners to preserve data on live systems (Casey, 2011).

4.2.1 The Need for Live Analysis

When a computer is involved in an incident, there are several choices to proceed during an investigation. Sometimes system administrators cannot afford to remove the computer from the network. A traditional forensic duplication cannot be acquired because a proper backup server cannot be swapped in its place. The data currently in memory may be the only evidence of the incident. A live response process contains information such as the current network connections, running processes, and open files. The live incident response process has become a technique for collecting and analyzing forensically sound evidence. Once the memory data has been collected, there are a variety of techniques to extract evidential data from it. The above tools provide the ability to extract meaningful information from the memory data, such as running processes, dump user passwords, dump contents of open files, and many other items (Stephenson, 2014).

4.2.2 The Competence to Live Analysis on Original Evidence

The process of live analysis becomes an important issue in a security breach. This is applicable especially in a live response scenario of malware investigation. Different approaches and tools are required, depending on the state of the device (ISO, 2012). When the volatile evidence is necessary, there are countless tools that can be part of live collection. The choice of which tools to include must be based on the each case (Stephenson, 2014). Since each case is different, it is almost impossible to create a manual which can cover all possibilities. The cybercrime investigation is contingent upon various situational factors, including the capabilities and behaviors of offenders, and the investigator's preferred style. There is no best way of investigation. An investigation style that is effective in some situations may not be successful in others. Investigators who are very effective at one place and time may become unsuccessful either when they have transplanted to another situation or when the factors around them change.

4.2.3 The Explanation to Access Original Evidence

It is no longer possible to ignore the volatile data of computer memory during a subsequent analysis. With the rise of challenges in the digital forensic investigation field, some interesting problems are looming on the horizon for both victims and examiners. It is no longer sufficient to collect the non-volatile data of digital evidence when examiners pull the plug and take the computer back to the lab. In circumstances where a person finds it necessary to access the original data held on a computer or on storage media, that person must be competent to do so and be able to explain the relevance and the implications of their actions (ACPO, 2012).

5. Conclusion

Security breaches become a part of life nowadays. When cyber threats originate from malicious offenders or trusted insiders, the need to quickly assess and appropriately respond is essential. To uncover the truth, Cyber-crime investigations should be founded on the latest information technology. Often the criminals' activities have left behind a communication trail on the networks used to connect to the crime scene. It is possible to extract clues from these locations as well. However, proving the

offender has caused the damage to the system is a tough job. This framework allows for a stronger presentation of evidence in a cybercrime case. It is crucial to use some toolkits and perform a forensic analysis of the compromised computer. Examiners should propose a handful of realistic questions, explore some approaches to execute it, and uncover potential information to answer them. To ensure the quality of evidence collection, this framework may help to clarify the issue at hand, retain most of the useful information, and provide details of how this novel approach links evidence to a verifiable reconstruction of events at the crime scene.

Acknowledgments
This research was partially supported by The Henry C. Lee Forensic Science Foundation.

References

ACPO (Association of Chief Police Officers). (2012). ACPO Good Practice Guide for Digital Evidence. *Retrieved April 24, 2014, from* http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

Bashir, M. S., & Khan, M. N. A. (2013). Triage in Live Digital Forensic Analysis. *The International Journal of Forensic Computer Science,* l(1), 35-44.

Casey, E. (2010). *Handbook of Digital Forensics and Investigation.* Burlington, MA: Elsevier Academic Press.

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (Third Edition)*. Waltham, MA: Elsevier Inc.

ISO (International Organization for Standardization). (2012). *ISO/IEC 27037:2012 - Information Technology: Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence.* Switzerland: ISO Office.

Johnson, L. (2013). *Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response.* Burlington, MA: Elsevier Inc.

Ligh, M. H., Case, A., Levy, J. & Walters, A. (2014). *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory.* Indianapolis. IN: John Wiley & Sons, Inc.

Luttgens, J. T., & Pepe, M. (2014). Incident Response & Computer Forensics (Third Edition). New York: McGraw-Hill Education.

Malin, C. H., Casey, E. & Aquilina, J. M. (2008). *Malware forensics: Investigating and Analyzing Malicious Code*. Burlington, MA: Elsevier Inc.

NIST Cloud Computing Forensic Science Working Group. (2014). NIST Cloud Computing Forensic Science Challenges (Draft NISTIR 8006). *Retrieved April 24, 2014, from* http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf.

Prahalad, C. K. & Hamel, G. (1990). The Core Competence of the Corporation. *Harvard Business Review*, 68(3), pp. 79–91.

Raghavan, S. (2014). *A Framework for Identifying Associations in Digital Evidence Using Metadata.* Dissertation, Brisbane: Queensland University of Technology.

Roger, A. E., & Achille, M. M. (2012). Multi-Perspective Cybercrime Investigation Process Modeling, *International Journal of Applied Information Systems*, 2(2). New York: Foundation of Computer Science.

Stephenson, P. (2014). *Official (ISC)2® Guide to the CCFP CBK*, Auerbach Publications.

Vacca, J. R. (2014). *Network and System Security (Second Edition)*. Burlington, MA: Elsevier Inc.

Yadav, S. (2011). Analysis of Digital Forensic and Investigation. *VSRD International Journal of Computer SCI. & Information Technology*, 1 (3), 171-178.

Contact email: camel@mail.cpu.edu.tw