FORZA: Digital Forensics Investigation Framework That Incorporate Legal Issues

By

Ricci Sze-Chung Ieong

From the proceedings of

The Digital Forensic Research Conference

DFRWS 2006 USA

Lafayette, IN (Aug 14th - 16th)

available at www.sciencedirect.com

SCIENCE DIRECT®

journal homepage: www.elsevier.com/locate/diin

Digital Investigation

FORZA – Digital forensics investigation framework that incorporate legal issues

Ricci S.C. Ieong[*]

eWalker Consulting Ltd, Unit 4 5/F, Block 2 Nan Fung Ind. City, 18 Tin Hau Road, Tuen Mun, Hong Kong, China

Keywords:
Digital forensics investigation framework
Digital forensics
FORZA framework
Forensics principles
Zachman framework
Legal aspects

ABSTRACT

What is Digital Forensics? Mark Pollitt highlighted in DFRWS 2004 [Politt MM. Six blind men from Indostan. Digital forensics research workshop (DFRWS); 2004] that digital forensics is not an elephant, it is a process and not just one process, but a group of tasks and processes in investigation. In fact, many digital forensics investigation processes and tasks were defined on technical implementation details Investigation procedures developed by traditional forensics scientist focused on the procedures in handling the evidence, while those developed by the technologist focused on the technical details in capturing evidence. As a result, many digital forensics practitioners simply followed technical procedures and forget about the actual purpose and core concept of digital forensics investigation.

With all these technical details and complicated procedures, legal practitioners may have difficulties in applying or even understanding their processes and tasks in digital forensics investigations.

In order to break the technical barrier between information technologists, legal practitioners and investigators, and their corresponding tasks together, a technical-independent framework would be required.

In this paper, we first highlighted the fundamental principle of digital forensics investigations (Reconnaissance, Reliability and Relevancy). Based on this principle, we re-visit the investigation tasks and outlined eight different roles and their responsibilities in a digital forensics investigation.

For each role, we defined the sets of six key questions. They are the What (the data attributes), Why (the motivation), How (the procedures), Who (the people), Where (the location) and When (the time) questions. In fact, among all the investigation processes, there are six main questions that each practitioner would always ask.

By incorporating these sets of six questions into the Zachman's framework, a digital forensics investigation framework – FORZA is composed. We will further explain how this new framework can incorporate legal advisors and prosecutors into a bigger picture of digital forensics investigation framework.

Usability of this framework will be illustrated in a web hacking example.

Finally, the road map that interconnects the framework to automatically zero-knowledge data acquisition tools will be briefly described.

[*] Tel.: +852 83387326.
E-mail address: ricci@ewalker.com.hk

1742-2876/$ – see front matter © 2006 DFRWS. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2006.06.004

1. Introduction

What is Digital Forensics? This question has been asked many times and Pollitt highlighted that there is no single answer to this question (Politt, 2004). He mentioned that Digital Forensics is a process, not an elephant, and it is not just one single process, but a group of tasks and processes in investigation.

In the digital forensics investigation practices, there are over hundreds of digital forensics investigation procedures developed all over the world. Each organization tends to develop its own procedures. Some focused on the technology aspects in data acquisition, some focused on data analysis portion of the investigation (Brill and Pollitt, 2006).

As many of these procedures were developed for tackling different technology used in the inspected device, when underlying technology of the target device changes, new procedures has to be developed.

Among those procedures, Lee's (Lee et al., 2001), Casey's (Casey, 2003a), DFRWS (DFRWS, 2001) and Reith, Carr and Gunsch (Reith et al., 2002) procedures are the most frequently quoted procedures. They are known to be the standard procedures in digital forensics investigations. However, discrepancy still lies between them. According to Séamus Ó Ciardhuáin's analysis (Ciardhuáin, 2004), the four procedures were not aligned (Table 1). Instead of difference in definition, the processes they recommend and their coverage were different.

Although with Ciardhuáin's extended model, digital forensics procedures have been extended to cover a wider prospective and area, one core issue have not been solved. That is the gap between technical aspects of digital forensics and judicial process (Losavio and Adams, 2006).

According to Losavio and Adams' research, they concluded that there is a wide gap between the technical specialists and the legal practitioners.

Many of them understand that they need to get familiar with digital evidence and digital forensics practices. However, they consider that the technical procedures and knowledge are difficult for them to learn or even to follow.

Legal practitioners do not need to understand exactly the procedures in "dissecting" the hard disk before he can make use of the user records in the computer as an admissible evidence. They only need to know whether the data are relevant to the case and non-repudiatable. Thus, they found themselves lost in the details without understanding the fundamental principle in digital forensics investigation procedures.

2. Fundamental principle in digital forensics investigation procedures

In IT Security field, there are a lot of technological aspects, such as access control, biometrics, encryption, network security, security algorithm, etc. Each of them has its specific methodology and school of thoughts, but they all rely on one set of fundamental principles. That is, the core IT Security fundamentals – Confidentiality, Integrity and Availability (Fig. 1).

With this core principle, different areas of IT Security are linked together. IT Security development, assessment and audit view across different organizations all rely on the core IT Security fundamental principle.

Similarly, digital forensics investigation should also have a core principle that enables the practitioners to view the underlying concept across different digital forensics investigation procedures. Digital Forensics Investigation is a process to determine and relate extracted information and digital evidence to establish factual information for judicial review. To accomplish this requirement, its fundamental principle includes *Reconnaissance, Reliability, and Relevancy* (Fig. 2).

- *Reconnaissance*. Similar to what needs to be performed before ethical hacking, a digital forensics investigator needs to exhaust different methods, practices and tools that were developed for particular operating environment to collect, recover, decode, discover, extract, analyze and convert data that kept on different storage media to readable evidence. No matter where data are stored, digital forensics

Table 1 – A comparison table between different digital forensics investigation model extracted from Séamus Ó Ciardhuáin's analysis

Term in new model	Model			
	Lee et al.	Casey	DFRWS	Reith et al.
Awareness				Identification
Authorisation				
Planning				Preparation
Notification				
Search/identification	Recognition, identification	Recognition	Identification	
Collection	Collection and preservation	Preservation, collection, documentation	Preservation, collection	Preservation, collection
Transport				
Storage				
Examination	Individualization	Classification, comparison, individualization	Examination	Examination
Hypothesis	Reconstruction	Reconstruction	Analysis	Analysis
Presentation	Reporting and presentation		Presentation	Presentation
Proof/defence			Decision	
Dissemination				

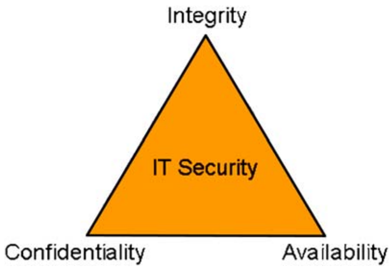

Fig. 1 – IT Security fundamentals.

investigators should be revealing, and focusing retrieval of the truth behind the data.

- *Reliability*. Extracting of data is not simply copying of data using Windows Explorer or saving files to a disk. Chain of evidence should be preserved during extracting, analyzing, storing and transporting of data. In general, chain of evidence, time, integrity of the evidence and the person relationship with the evidence could be collectively considered as the non-repudiation feature of digital forensics. If the evidence cannot be repudiated and rebutted, then the digital evidence would be reliable and admissible for judicial review.
- *Relevancy*. Even though, evidence could be admissible, relevancy of the evidence with the case affects the weight and usefulness of the evidence. If the legal practitioner can advise on what should be collected during the process, time and cost spent in investigation could be controlled better.

In the world of ''The Lord of the Rings'', the invisible ring is known to be the ring to rule them all and the ring to find them all. In digital forensics investigation world, after establishing the ''One Ring'', we have to determine how to ''find them all''. An overall framework should be derived to link the practitioners and their procedures all together.

3. FORZA framework – the link to bind them all

Back to the basic rule, a framework depends on the participants in the organization. For instance, in Zachman framework (Zachman) for enterprise architecture, there are Planner, Owner, Designer, Builder and Subcontractor.

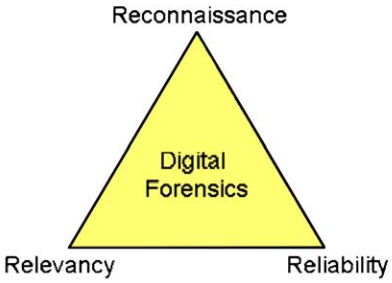

Fig. 2 – Digital Forensics Investigation Fundamentals.

In a typical digital forensics investigation process, system owners, digital forensics investigators and legal practitioners are expected to be involved. However, if we further separate the roles and responsibilities of these participants, they could be further categorized into eight individual roles of participants in investigation. These roles are different in nature but could be handled by the same person if required.

- Case leader
- System/business owner
- Legal advisor
- Security/system architect/auditor
- Digital forensics specialist
- Digital forensics investigator/system administrator/operator
- Digital forensics analyst
- Legal prosecutor

The *case leader* is the planner and orchestra of the entire digital investigation process. He will be leading the case and determining whether it should proceed forward or not.

The *system/business owner* is the owner of the system being inspected. He/she is usually the victim and sponsor of the case. For instance, if the case is a web hacking case, his/her system could be affected and he/she would have to contact police for investigation. In some occasion, owner can also be the suspect of the case. For example, if it is an illegal sharing of music files case, the owner will be the suspect of the case.

Legal Advisor is the first legal practitioner the case leader would seek for legal advice. He/she would advise the case leader whether it is applicable to proceed forward for legal disputes. As digital forensics investigation is a process for collecting relevant evidence for legal dispute, if case leader could seek legal advice and determine whether it is feasible to present the case in litigation at earlier stage of an investigation, time and expenses could be reduced. Besides, investigator can concentrate more on seeking data from the devices that are relevant to the dispute.

Even with legal advice, case leader should explore and understand more about the system and security design of the system to be inspected. In large corporation, *system/solution architect, security consultant and internal auditor* should be interviewed. Through these discussions, case leader would be able to estimate the scope of the case and extract the security controls design that have been implemented in the systems.

Then the case leader could assign or hire proper *digital forensics specialists* to plan the entire operations. Digital forensics investigation is not a static process. Depending on the business nature, system design and legal advice, different methods of investigation would be formulated. Thus, digital forensics specialists should reconsider all the inputs and requirements from legal advice to plan the entire investigation strategy. He/she should also decide whether it is necessary to contact third party vendors or external consultant to perform specific part of investigation.

Afterwards, digital forensics specialists would provide the defined strategy to the *digital forensics investigator*. The main responsibilities of the investigator is to collect, extract, preserve and store the digital evidence from the systems. Depending on the system owner arrangement, sometimes, digital forensics investigator may not be permitted to directly operate the system. System administrator or operators in the company may be requested to follow the documented strategy to act as the hand of investigator to perform the data acquisition process.

From the collected evidence, *digital forensics analyst* would have to extract relevant data, analyze them against the hypothetical model proposed for investigation. Analysts may also have to perform various tests to prove/disprove the hypothetical model that emulate the case. They also have to reconstruct the timeline of the case based on the extracted data.

With the extracted information, timeline and relevant information, case leader would discuss again with legal practitioner to determine whether litigation process should continue. This type of practitioner is normally the *legal prosecutor* or councilor. He/she would advise the case leader whether the collected evidence is sufficient, relevant, admissible and favorable to which party. He/she should also propose to the case leader the most feasible legal system to choose. Sometimes, a case can be presented as civil, criminal litigation or even as arbitration case. Legal prosecutor should choose the most suitable arena and lead the case from onwards in the litigation process. The entire process flow is described in Fig. 3.

In order to bind roles, responsibilities and procedures together, a technology-independent digital forensics investigation framework would be required. Through the Zachman framework derivatives – FORensics ZAchman framework (FORZA) framework,[1] these eight roles and their responsibilities are linked together. High-level outline of the framework is shown in Table 2.

Similar to the nature and concept of Systems and Business Security Architecture (SABSA) framework,[2] layers are interconnected to each other through sets of six categories of questions namely:

- What (the data attributes);
- Why (the motivation);
- How (the procedures);
- Who (the people);
- Where (the location), and
- When (the time).

These questions are not just tailored for SABSA, they have also been considered in various digital forensics investigation procedures.

4. Bringing legal aspects into the picture

One of the advancements of this framework is its coverage. Through this framework, different standards and procedures could be linked together in a more holistic way. Digital forensics investigation is no longer viewed from pure technical aspects. Business, system and legal aspects are incorporated.

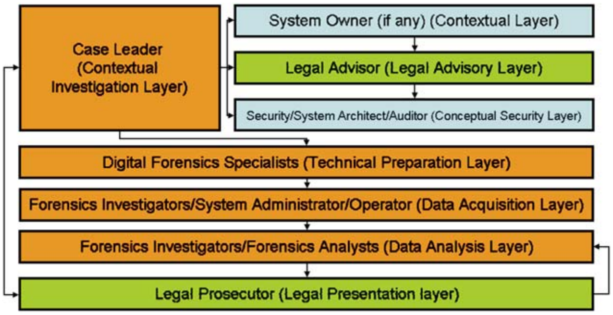
Case Leader (Contextual Investigation Layer)
System Owner (if any) (Contextual Layer)
Legal Advisor (Legal Advisory Layer)
Security/System Architect/Auditor (Conceptual Security Layer)
Digital Forensics Specialists (Technical Preparation Layer)
Forensics Investigators/System Administrator/Operator (Data Acquisition Layer)
Forensics Investigators/Forensics Analysts (Data Analysis Layer)
Legal Prosecutor (Legal Presentation layer)

Fig. 3 – Process flow between the roles in digital forensics investigation.

Besides, legal advisor and prosecutor can play a much active and systematic role in the entire digital forensics investigation. According to the framework, legal practitioner would be acting as the role of Legal Advisor and/or the Legal Prosecutor.

As a Legal Advisor, he/she can focus on the following questions.

Legal objectives (Why)
- What is the purpose of the dispute?
- What is the law of dispute?
- Is the case criminal or civil case?

Legal background and preliminary issues (What)
- What is/are the relevant law/ordinance?
- Which sections of the ordinance should be referred to?
- What are the key elements in the ordinance?
- What is the required and related information?
- What data should be collected?
- What are the issues of law and issues of fact?

Legal procedures for further investigation (How)
- Is there any injunction action (e.g. Anton Pillar Injunction) required?
- Is any warrant, search warrant required?
- Any actions required to be applied for protecting the evidence?

Legal geography (Where)
- Is that within jurisdiction of the country?

Legal entities and participants (Who)
- Who is/are the claimant/respondent?
- Who are the Legal Councilor, Prosecutor, Legal Staff and other legal staff?

Legal timeframe (When)
- What is the time limit of the case?
- Is that within the time bar limit?
- What is the time span of the case?
- What is the usual time and cost of similar cases?

Based on the legal advice, case leader concentrate on the issues of matter and dig out the relevant evidence. After the forensics analysis procedures, case leader would have

[1] FORZA – a Zachman based digital forensics investigation framework, unpublished, 2006.
[2] SABSA is a derivative from Zachman framework for developing Enterprise Security Architecture.

Table 2 – A high-level view of the FORZA framework

	Why (motivation)	What (data)	How (function)	Where (network)	Who (people)	When (time)
Case leader (contextual investigation layer)	Investigation objectives	Event nature	Requested initial investigation	Investigation geography	Initial participants	Investigation timeline
System owner (if any) (contextual layer)	Business objectives	Business and event nature	Business and system process model	Business geography	Organization and participants relationship	Business and incident timeline
Legal advisor (legal advisory layer)	Legal objectives	Legal background and preliminary issues	Legal procedures for further investigation	Legal geography	Legal entities and participants	Legal timeframe
Security/system architect/ auditor (conceptual security layer)	System/Security control objectives	System information and security control model	Security mechanisms	Security domain and network infrastructure	Users and security entity model	Security timing and sequencing
Digital forensics specialists (technical preparation layer)	Forensics investigation strategy objectives	Forensics data model	Forensics strategy design	Forensics data geography	Forensics entity model	Hypothetical forensics event timeline
Forensics investigators/system administrator/operator (data acquisition layer)	Forensics acquisition objectives	On-site forensics data observation	Forensics acquisition/ seizure procedures	Site network forensics data acquisition	Participants interviewing and hearing	Forensics acquisition timeline
Forensics investigators/ forensics analysts (data analysis layer)	Forensics examination objectives	Event data reconstruction	Forensics analysis procedures	Network address extraction and analysis	Entity and evidence relationship analysis	Event timeline reconstruction
Legal prosecutor (legal presentation layer)	Legal presentation objectives	Legal presentation attributes	Legal presentation procedures	Legal jurisdiction location	Entities in litigation procedures	Timeline of the entire event for presentation

a much clearer picture of the case and be able to determine and perform review with the legal prosecutor. Usually, the legal prosecutor would take the input from the case leader, forensics analysts, reconstruct the case and present that using legal viewpoint. Thus, Legal Prosecutor would focus on the following questions:

Legal presentation objectives (Why)
- Should the case proceed or close?
- Is sufficient evidence collected?
- Which litigation mechanism should be used?

Legal presentation attributes (What)
- What charge should be issued?
- What information should be included/excluded?
- What evidence should be presented?
- Which piece of evidence is relevant and admissible?

Legal presentation procedures (How)
- What litigation scheme should be used? (International Arbitration, local litigation?)
- What tactic should be applied in the litigation procedure?

Legal jurisdiction location (Where)
- Where should be the place of litigation?
- Where should be the place of enforcement?
- Where should be the place of hearing?

Entities in litigation procedures (Who)
- Which witnesses should be called?
- Should any expert witnesses be called?
- Which Judge, Council and Arbitrator are involved?

Timeline of entire event for presentation (When)
- Is the entire story board re-constructed?
- Any timeline missing in the evidence?
- When should the case be presented?

5. Applying FORZA framework

No framework could be applied without testing its applicability. As an illustration, we handle a web hacking case by using the FORZA framework.

5.1. *Contextual investigation layer*

Assuming a corporate web system was reported to be hacked, the case leader (such as the law enforcement team for criminal investigation) after receiving the report of the case would:

- Determine the motivation (Why) of this case. He will confirm the type of reported case and determine whether an investigation is required.
- Identify the involved parties (Who). He will identify the involved parties such as suspects, witnesses, system owner and the victims and the person reporting the case. He will also identify the relationship between the person reporting the case and the owner of the systems.

- Confirm the time of the incident (When). He will also confirm the reporting time, start time and end time of the web hacking case.
- Verify the location of the case (Where). He will determine the suspected geographical location of the web attack.
- Determine the reported event nature (What). As the case is being confirmed to be web hacking case, the victim machine would be the object/victim of the event. The web services would probably be disrupted.
- Plan the next step procedure (How). This action leads to the next layer in the framework. The case leader has to plan the next step action. If the case leader decided to proceed forward, he/she would have to consider which investigation team needs to be assigned to the tasks.

5.2. *Contextual layer*

The case leader will then seek input from the *system owner* or his representative. He would have to perform an interview with the system owner and person who report the case to:

- Understand the business nature of the company and the business objectives (Why) of the affected system.
- Determine the business and event nature (What). He will discuss with the system owner and understand the data or system being affected and how does the event happen.
- Confirm business and system process model (How). After knowing the business and system nature, he also has to understand the criticality of the system to the business and what function has been affected.
- Explore the business geography (Where). He also has to explore and determine whether all servers are located in one location and whether the victim network is widely spread across various offices.
- Determine the business and incident timeline (When). Other than determining when the system was first operated, and event was first reported, case leader also has to determine how long the investigation can last.
- Understand organization and participants' relationship (Who). The case leader has to understand the organization structure, identify the participants, system supports, security administrator of the organization and also seek the input from the business person who they suspected to be the attacker.

5.3. *Legal advisory layer*

After understanding the background of the web hacking case, the case leader should seek *legal adviser* to determine:

- The legal objectives (Why) of this case. For instance, in Hong Kong, the case leader who is the HK Police Force investigation team will have to check with prosecutors from Department of Justice to determine whether this hacking case should be brought to court.
- Legal background and preliminary issues (What) of this case. Legal advisor would provide the background idea on what is the necessary and sufficient information, what is the relevant law and ordinance to be incorporated. Besides, they should determine the issues of law and issues of fact.
- Legal Geography and Jurisdiction (Where). Legal advisor should also advise the investigators whether the case would be within the geographical jurisdiction. In most web hacking case, the source of the attacker is outside the country. So it may not be worthwhile to proceed in the litigation process.
- Legal Entities and Participants (Who) of this case. Legal advisor and the investigators have to prepare the preliminary list of entities, participants of this case. That includes the claimant, respondent, legal council. If the case is to be proceeded through arbitration or mediation, arbitrator or mediator could also be considered.
- Legal Timeframe (When) of this case. In most cases, time span and monetary gain/spent were the determination factor. Legal advisor should advise the investigator and the owner how much time would be needed in this case and whether there is any time bar limit in the litigation.
- Legal Procedures for further investigation (How) of this case. After identifying the necessary background about the case, the legal advisor and the investigator can confirm whether the case should be eligible for litigation. If legal process would not be required, investigator may simply concentrate on identification of the root case of the web hacking.

5.4. *Conceptual security layer*

After seeking legal advice, the case leader would explore and understand further the design of the information system and the relevant security controls, from the system owner recommended technical staff. The case leader would:

- Explore the System/Security Control Objectives (Why) that has been implemented to protect against external attacks. Case leader may also explore why hacker can compromise the server.
- Understand the System information and security control model (What). Data and process model of the system, risk assessment scheme, data classification scheme, operating systems, data protection scheme and audit-logging facilities should be collected. Case leader should also determine from the technical staff what data have been lost.
- Collect the implemented Security Mechanisms details (How). Detail security functions or policies within the systems should be explored. Relevant audit information (e.g. Profile Detection, Anomalous Intrusion Detection, System log monitoring, etc.) could be collected.
- Explore the Security Domain and Network Infrastructure (Where). In most organizations, firewall, protection zone would be implemented. In the previous interviews with the owner, case leader may have identified other connected network. Case leader should collect the network diagram and explore the other related systems within this case. For example, logs in other networking devices would also be one source of information input.
- Determine the User and Security Entity Model (Who). At this stage of the investigation, the case leader should also

explore the inter-relationship model of entities within the organization. Sometimes, web hacking could be performed through internal user accounts. So user identity, privileges, access control list and previous violation events or records should be collected.
- Determine the Security Timing and Sequencing (When). Security controls and protection scheme may not have been implemented when the system was first designed. So case leader should determine whether the security controls have been implemented before reporting of the first event, and if time synchronization mechanism has been implemented. Besides, technical support staff may also be able to provide some information whether there is any occurrence time pattern of the reported event.

5.5. *Technical presentation layer*

As all business, system and legal background has been collected and forensics investigation objective being confirmed, the case leader could assign relevant digital forensics specialists to plan before on-site investigation. The Digital Forensics Specialists should:

- Understand the objective and plan the relevant Forensics Investigation Strategy Objectives (Why).
- Determine the Forensics Data Model (What). After knowing the strategy objectives of the forensics investigation, specialists should be able to draw the hypothesis of the why web hacking would happen and determine what logs should be collected from the web sites.
- Explore Geography location within the Forensics Data Model (Where). In this case, the IP addresses of the source attacker, the owner of the network and the login account information should be consolidated into the Forensics Data Model.
- Draft the entity lists for the Forensics Entity Model (Who). Web hacking cannot happen without human intervention. Specialists with the hypothetical data model should be able to outline the involved entities relationship and list the parties to be interviewed. In addition, specialists should determine whether external third party experts or vendors should be introduced to help in conducting data collection or analysis.
- Propose a Hypothetical Forensics Event Timeline (When). Confirmation of the time when hacker first penetrated into the systems would be crucial to the entire investigation.
- Define the Forensics Strategy (How). With Data, Entity Models and timeline defined, specialists could outline the data acquisition and analysis procedures and requirement. Offline data collection or live production information could be decided. Tools and media for data acquisition could also be selected.

5.6. *Data acquisition layer*

Based on the strategies and tasks outlined by the digital forensics specialists, forensics investigators, system administrators or operators could follow strictly the outline procedures. The investigators should:

- Understand the Forensics Acquisition Objectives (Why) assigned by the forensics specialists. In this case, the investigators should check the log files from the servers and the hacked servers.
- Perform on-site Forensics Data Observation (What). When the investigators go on-site, they should determine whether the hypothesis is the same as the real-situation. They should also observe whether the reported web hacking activities are still observable on network and whether network data capturing is required. Investigators should also observe and verify whether any potential data lost happened in the system.
- Interview participants and witnesses identified (Who). Investigators should interview both internal staff and suspected parties identified from the ISP.
- Perform Forensics Acquisition and Seizure Procedures (How). The investigators should clone the log files, disk image from the compromised machine and the victim machine if any based on the defined strategies.
- Perform site network forensics data acquisition (Where). The investigators should collect network devices' logs, activities, network access control lists, IDS, firewall, router activities log. If the web hacker is suspected to be online, live network capturing would also be required.
- Keep the forensics acquisition timeline and chain of custody (When). In a forensics investigation process, all the activities performed and its performed time should be recorded.

5.7. *Data analysis layer*

After the necessary data being collected and transported to the digital forensics laboratory for further analysis and investigation, digital forensics analysts would have to extract relevant information and review them according to the hypothetical model. They would have to:

- Extract information that is critical for proving the case which matches the Forensics Examination Objectives (Why).
- Reconstruct the Event Data based on the extracted data (What). Analysts should reconstruct the data schema based on the extracted information and extract user account information, statistics and other system information.
- Extract Network information (Where). Network address, network path and captured network live data, as well as all network logs would also be extracted for analysis.
- Extract Entity, accounts information and rebuilding the relationship linkage (Who). User accounts, phone number, emails, organization charts would be collectively analyzed.
- Analyze the extracted data based on forensics analysis procedures (How). Analysts should define the searching criteria to find out the hacking mechanism and compare that against the hypothesis.
- Reconstruct the event timeline (When) of the hacking activity. Analysts would have to determine whether the chain of evidence and timeline of the events are consistent.

5.8. *Legal presentation layer*

After extracting and analyzing the information collected from the victim, together with the IP address information from the network service providers, legal prosecutor has to discuss with the case leader and the system owner on:

- Legal Presentation Objectives (Why). From the extracted relevant information and analysis report, legal prosecutor would be able to determine whether the case can be taken to litigation process or to be closed and whether sufficient evidence has been collected.
- Legal Presentation Attributes (What). Legal prosecutor should consider what he would like to present in the litigation, whether the data are relevant and admissible. He should also let the analysts know whether additional evidence would be required.
- Legal Presentation Procedures (How). Legal prosecutors need to define the arena for litigation. For the hacking case, criminal prosecution would be applied. Also the tactics used in the litigation procedures have to be considered.
- Legal Jurisdiction Location (Where). As criminal prosecution procedures would be processed, legal jurisdiction location has been confirmed.
- Entities in Litigation Procedures (Who). For criminal prosecution, legal prosecutor has to define the witness list order and the interlocutory question list.
- Timeline of entire event for Presentation (When). Legal prosecutors should also draft the entire story board of the case based on the presented evidence and determine if there is any piece of timeline information is missing.

6. Future work

As the next step, we have already started to incorporate the framework questions together with the necessary workflow to an intelligence data acquisition scripts generator. Using this framework, questions and answers in a digital forensics investigation could be systematically thought through. Then based on the provided answers, scripts would be tuned to collect and extract relevant information from seized devices.

By these automatic scripts, investigators can perform fast and zero-knowledge data acquisition.

Thus, FORZA framework will be formulated as a semi-automatic investigation toolbox.

REFERENCES

Brill AE, Pollitt M. The evolution of computer forensic best practices: an update on programs and publications. Journal of Digital Forensic Practice 2006;1:3–11.

Casey E. Digital evidence and computer crime – forensic science, computers and the internet. Cambridge: Academic Press; 2003a. p. 265.

Ciardhuáin Séamus Ó. An extended model of cybercrime investigations. International Journal of Digital Evidence Summer 2004;3(1).

DFRWS. Report from the first digital forensic research workshop. DTR-T001-01 FINAL A road map for digital forensic research; 2001 <http://www.dfrws.org> [final version, November 6, 2001].

Lee HC, Palmbach TM, Miller MT. Henry Lee's crime scene handbook. San Diego: Academic Press; 2001.

Losavio M, Adams J. Gap analysis: judicial experience and perception of electronic evidence. Journal of Digital Forensic Practice 2006;1:13–7.

Politt MM. Six blind men from Indostan. Digital forensics research workshop (DFRWS); 2004.

Reith M, Carr C, Gunsch G. An examination of digital forensic models. International Journal of Digital Evidence Fall 2002;1(3): 1–12.

Zachman J. Enterprise architecture: a framework, <www.zifa.com>.

Further reading

Beebe NL, Clark JG. A hierarchical, objectives-based framework for the digital investigations process. Digital forensics research workshop (DFRWS); 2004.

Casey E, editor. Handbook of computer crime investigation. London: Academic Press; 2003b.

Marsico CV. CERIAS tech report 2005-27, digital music device forensics. Center for Education and Research in Information Assurance and Security, Purdue University; 2005.

Sherwood J, Clark A, Lynas D. SABSA white paper – enterprise security architecture. SABSA, <http://www.sabsa-institute.org/>; 2005.

U.S. Department of Justice. Electronic crime scene investigation – a guide for first responders; 2001.

U.S. Department of Justice. Forensic examination of digital evidence: a guide for law enforcement; 2004.

Ricci Ieong is the founder and Principal Security Consultant of eWalker Consulting Limited where he leads the IT Security planning, IT Security assessment, Digital Forensics Investigation, penetration test and IT audit project as well as security management solution design projects. Prior starting his own company, he was the Security Lead of HPS Consulting and Integration in Hong Kong, Deputy Manager of ITPSA Security Services in HP and the HK e-Security Center. He has been with HP since December 2000 and has over 6 years of experience in IT Security area specialized in Security Risk Assessment, IT Audit, Ethical Hacking and Penetration Test, Smart Card and Biometrics System deployment and Computer Forensics Investigation. He is also the founding member and secretary of Information Security and Forensics Society of Hong Kong.