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 Authorisation				Identification
Planning Notification				Preparation
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 Dissemination			Decision	