FORZA

Digital forensics investigation framework that incorporate legal issues

Ricci S.C. Ieong
Presentation Outline

1. Introduction
2. Fundamental principle in digital forensics investigation procedures
3. FORZA framework – the link to bind them all
4. Bringing legal aspects into the picture
5. Applying FORZA framework
6. Future work
Introduction

What is Digital Forensics?
WHEN DOES LIFE BEGIN?

AT THE MOMENT OF CONCEPTION.

AT BIRTH.

WHEN YOU GET YOUR DRIVE'S LICENSE.
What is Digital Forensics?

There is no single answer to this question (Politt, 2004)
For this course

“the application of proven scientific methods and techniques in order to recover data from electronic or digital media”
Why this difference

- 100+ DFIP
- Technology vs. data analysis aspects
- Each organization has its own procedures
- Technology changes → new procedures.
<table>
<thead>
<tr>
<th>Lee’s</th>
<th>Casey’s</th>
<th>DFRWS</th>
<th>Reith et al.</th>
</tr>
</thead>
</table>

Frequently Used Procedures:
Their definition, the processes they recommend and their coverage were different.

<table>
<thead>
<tr>
<th>Term in new model</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Lee et al.</td>
</tr>
<tr>
<td>Awareness</td>
<td>Recognition, identification</td>
</tr>
<tr>
<td>Authorisation</td>
<td>Collection and preservation</td>
</tr>
<tr>
<td>Planning</td>
<td>Search/identification</td>
</tr>
<tr>
<td>Notification</td>
<td>Collection</td>
</tr>
<tr>
<td>Transport</td>
<td>Examination</td>
</tr>
<tr>
<td>Storage</td>
<td>Hypothesis</td>
</tr>
<tr>
<td>Examination</td>
<td>Presentation</td>
</tr>
<tr>
<td>Hypothesis</td>
<td>Proof/defence</td>
</tr>
<tr>
<td>Presentation</td>
<td>Reporting and presentation</td>
</tr>
<tr>
<td>Proof/defence</td>
<td>Decision</td>
</tr>
<tr>
<td>Dissemination</td>
<td>Decision</td>
</tr>
</tbody>
</table>
Ciardhuáin’s extended model

• His DF procedures have been extended to cover a wider prospective and area

• Does not cover “the gap between technical aspects of digital forensics and judicial process”
The CEM Gap (Losavio and Adams, 2006).

- Digital evidence and digital forensics practices
- technical procedures and knowledge

- difficult for them to learn or even to follow technical procedures
- Data Relevance (non-repudiable)
Fundamental principle in DFIP

Reconnaissance

Digital Forensics

Relevancy

Reliability

Fig. 2 – Digital Forensics Investigation Fundamentals.
Fundamental principle in DFIP

Reconnaissance: exhaust different methods, practices and tools that were developed for particular operating environment to collect, recover, decode, discover, extract, analyze and convert data that are kept on different storage media to readable evidence.
**Fundamental principle in DFIP (Cont.)**

**Reliability:** Chain of evidence should be preserved during extracting, analyzing, storing and transporting of data. This will be in general considered as the non-repudiation feature of digital forensics.
Fundamental principle in DFIP (Cont.)

Relevancy: relevancy of the evidence with the case affects the weight and usefulness of the evidence. The legal practitioner’s advise will save time and cost.
An overall framework should be derived to link the practitioners and their procedures all together.
Zachman EA framework

• There are Planner, Owner, Designer, Builder and Subcontractor

• In a typical DFIP, system owners, digital forensics investigators and legal practitioners are expected to be involved.
## Expanded Role of SO, DFI and LP

<table>
<thead>
<tr>
<th>Case Leader</th>
<th>System/Business Owner</th>
<th>Legal Advisor</th>
<th>Security/System Architect/Auditor</th>
</tr>
</thead>
<tbody>
<tr>
<td>DF Specialist</td>
<td>DFI/System Admin. /Operator</td>
<td>DF Analyst</td>
<td>Legal Prosecutor</td>
</tr>
</tbody>
</table>

These roles are different in nature but could be handled by the same person if required.
• **The Case Leader:**
  
  – Is the planner and the case leader
  
  – Determines whether to proceed forward or not.
Expanded Roles (Cont.)

• The system/business owner:
  – Is the owner of the system being inspected.
  – Can be the victim or the suspect of the case.
Expanded Roles (Cont.)

• **Legal Advisor:**
  – Is a legal practitioner
  – Advise the case for legal disputes.

• **system/solution architect, security consultant and internal auditor**
• Understands more about the system and security design
• Should be interviewed in large corporation
• Will help case leader to be able to estimate the scope of the case and extract the security
• controls design that have been implemented in the systems.
Expanded Roles (Cont.)

• **System/ solution architect, security consultant and internal auditor**
  - Understands more about the system and security design
  - Should be interviewed in large corporation
  - Will help case leader to be able to estimate the scope of the case and extract the security controls design that have been implemented in the systems.
Expanded Roles (Cont.)

• Digital forensics specialist:
  – Plan the entire operations because the process is not static.
  – Formulates different methods of investigation.
  – Should reconsider all the inputs and requirements from legal.
  – Should also decide whether it is necessary to contact third party vendors or external consultant to perform specific part of investigation.
Expanded Roles (Cont.)

• Digital forensics investigator (Sys. Admin.):
  – Gets the defined strategy provided by the DFS.
  – Collect, extract, preserve and store the digital evidence
  – If not permitted to directly operate the system, system administrator in the company shall do it.
Expanded Roles (Cont.)

• Digital forensics analyst:
  – Extract relevant data, analyze them against the hypothetical model proposed for investigation.
  – Analyst(s) may also have to perform various tests to prove/disprove the hypothetical model that emulate the case.
  – Reconstruct the timeline based on the extracted data
Expanded Roles (Cont.)

• Legal Practitioner:
  – Give the CL whether litigation process should continue.
  – Determine whether the collected evidence is sufficient, relevant, admissible and Favorable
  – Should propose to the CL the most feasible legal system to choose: civil, criminal litigation or as arbitration case.
  – Choose the most suitable arena and lead the case
Fig. 3 - Process flow between the roles in digital forensics investigation.
What is Framework?
What is Framework?

Broad overview, outline, or skeleton of interlinked items which supports a particular approach to a specific objective, and serves as a guide that can be modified as required by adding or deleting items.

Source: http://www.businessdictionary.com/definition/framework.html
FORensics Zachman (FORZA)

FORZA framework

A technology-independent digital forensics investigation framework
<table>
<thead>
<tr>
<th>Role/Role Title</th>
<th>Why (motivation)</th>
<th>What (data)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case leader (contextual investigation layer)</td>
<td>Investigation objectives</td>
<td>Event nature</td>
</tr>
<tr>
<td>System owner (if any) (contextual layer)</td>
<td>Business objectives</td>
<td>Business and event nature</td>
</tr>
<tr>
<td>Legal advisor (legal advisory layer)</td>
<td>Legal objectives</td>
<td>Legal background and preliminary issues</td>
</tr>
<tr>
<td>Security/system architect/auditor (conceptual security layer)</td>
<td>System/Security control objectives</td>
<td>System information and security control model</td>
</tr>
<tr>
<td>Digital forensics specialists (technical preparation layer)</td>
<td>Forensics investigation strategy objectives</td>
<td>Forensics data model</td>
</tr>
<tr>
<td>Forensics investigators/system administrator/operator (data acquisition layer)</td>
<td>Forensics acquisition objectives</td>
<td>On-site forensics data observation</td>
</tr>
<tr>
<td>Forensics investigators/forensics analysts (data analysis layer)</td>
<td>Forensics examination objectives</td>
<td>Event data reconstruction</td>
</tr>
<tr>
<td>Legal prosecutor (legal presentation layer)</td>
<td>Legal presentation objectives</td>
<td>Legal presentation attributes</td>
</tr>
</tbody>
</table>
FORZA framework (Cont.)

• Layers are interconnected to each other through sets of six categories of questions:
  – What (the data attributes)
  – Why (the motivation)
  – How (the procedures)
  – Who (the people)
  – Where (the location)
  – When (the time)
Bringing legal aspects into the picture

- This framework expanded its coverage
- Different standards and procedures could be linked together in a holistic way.
- DFI is no longer pure technical but business, system and legal aspects are incorporated.
- Legal advisors and prosecutor can play a much active and systematic role in the entire DFI.
Legal Advisor questions

Legal objectives (Why)
purpose - law of dispute - criminal or civil

Legal background and preliminary issues (What)
relevant law – referral section - key elements - required and related info - collection items - issues of law and issues of fact

Legal procedures for further investigation (How)
any injunction action required - any warrant, search warrant - Any actions required for protecting the evidence?
Legal Advisor questions (Cont.)

Legal geography (Where)
within country jurisdiction

Legal entities and participants (Who)
the claimant/respondent- Legal Councilor, Prosecutor, Legal Staff

Legal timeframe (When)
time limit - time bar limit - time span - time and cost of similar cases
Legal Prosecutor Questions

Legal presentation objectives (Why)
- proceed or close - is evidence sufficient? - Which litigation mechanism?

Legal presentation attributes (What)
- What charge? - information to be included/excluded? – evidence -
- Which piece of evidence is relevant and admissible?
Legal Prosecutor Questions (cont.)

Legal presentation procedures (How)

- litigation scheme (International Arbitration, local litigation?)

- applied tactic in the litigation procedure?

Legal jurisdiction location (Where)

- place of litigation? - place of enforcement? - place of hearing?
Legal Prosecutor Questions (cont.)

Entities in litigation procedures (Who)

Timeline of entire event for presentation (When)
- story board re-constructed? - missing timeline? - presentation time?
Applying FORZA framework

Handling a web hacking case by using the FORZA framework.
5.1 Contextual investigation layer

Case Leader:

- Determine the motivation (Why)
  - Confirm the type / investigation is required?

- Identify the involved parties (Who)
  - Identify the involved parties and relationship

- Confirm the time of the incident (When)
  - Confirm the reporting time, start time and end time
5.1 Contextual investigation layer (Cont.)

Case Leader:

• Verify the location of the case (Where)
  – suspected geographical location

• Determine the reported event nature (What)
  – the victim machine, disrupted services

• Plan the next step procedure (How)
  – The CL has to plan the next step action and investigation team
5.2 Contextual layer

The system owner or his representative (interviewer CL)

• Business nature and the business objectives (Why) of the system

• Determine the business and event nature (What)
  – understand affected data and how it happened

• Confirm business and system process model (How)
  – Understand system criticality and what functions affected

• Explore the business geography (Where)
  – Are all servers are located in one location or widely spread
5.2 Contextual layer (cont.)

The system owner or his representative (interviewer CL)

- Determine the business and incident timeline (When).
  - When the system was first operated, and event was first reported, how long the investigation can last.
- Understand organization and participants’ relationship (Who)
  - Understand the organizational structure, identify the participants, system supports, security administrator and also seek the input from the business person who they suspected to be the attacker
5.3 Legal advisory layer

Legal adviser to determine:

• The legal objectives (Why)
  – check whether the case be brought to court.

• Legal background and preliminary issues (What)
  – background idea on the necessary and sufficient information,
    which law and ordinance to be incorporated

• Legal Geography and Jurisdiction (Where)
  – Is the case within the geographical jurisdiction or outside
5.3 Legal advisory layer (cont.)

Legal adviser to determine:

• Legal Entities and Participants (Who)
  – Claimant, respondent, legal council.

• Legal Timeframe (When)
  – time span and monetary gain/spent are the determinants.

• Legal Procedures for further investigation (How)
  – is the case eligible for litigation
5.4. Conceptual security layer

The case leader would:

• Explore the System/Security Control Objectives (Why)
  – implemented protection and why hacker can compromise

• Understand the System information and security control model (What)
  – Data and process model, risk assessment, lost data
  – data classification, OS, data protection scheme and audit-loggin

• Collect the implemented Security Mechanisms details (How)
  – explore security functions or policies
  – Collect relevant audit information
5.4. Conceptual security layer (cont.)

The case leader would:

- Explore the Security Domain and Network Infrastructure (Where)
  - implement protection zone
  - Collect the network diagram

- Determine the User and Security Entity Model (Who)
  - explore the inter-relationship model of entities
  - get user identity, privileges, access control and previous violation events or records should be collected.
5.4. Conceptual security layer (cont.)

The case leader would:

• Determine the Security Timing and Sequencing (When)
  
  – determine security controls implementation time
  
  – technical support staff may provide any occurrence time pattern of the reported event.
5.5. Technical presentation layer

The Digital Forensics Specialists should:

• Plan the relevant Forensics Investigation Strategy Objectives (Why)
• Determine the Forensics Data Model (What)
  – draws the hypothesis of the why the hack happened
  – what logs should be collected from the web sites
• Explore Geography location within the Forensics Data Model (Where)
  – the IP addresses of the source attacker,
  – network owner, login account info.
5.5. Technical presentation layer (cont.)

The Digital Forensics Specialists should:

• Draft the entity lists for the Forensics Entity Model (Who)
  – outline involved entities relationship, list the interviewees
  – do we need third party for data collection or analysis?

• Propose a Hypothetical Forensics Event Timeline (When)
  – confirmation when hacker first penetrated into the systems

• Define the Forensics Strategy (How)
  – outline the data acquisition and analysis procedures and requirement
  – Offline or live data collection
  – Tools and media should be selected
5.6. Data acquisition layer

Forensics investigators should:

• Understand the Forensics Acquisition Objectives (Why)
  – check the log files from the servers and the hacked servers.

• Perform on-site Forensics Data Observation (What)
  – hypothesis is true or not
  – hacking activities still observable or data capturing is needed
  – Observe and verify any loss of potential data

• Interview participants and witnesses identified (Who)
  – interview both internal staff and suspects identified from the ISP.
5.6. Data acquisition layer (cont.)

Forensics investigators should:

- Perform Forensics Acquisition and Seizure Procedures (How)
  - 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)
  - collect network devices’ logs, activities, network access control lists, IDS, firewall, router activities log or make live network capturing

- Keep the forensics acquisition timeline and chain of custody (When)
  - all the activities and its time stamp should be recorded.
5.7. Data analysis layer

Digital forensics analysts 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)
  – reconstruct the data schema based on the extracted information and user account information, statistics and other system information.

• Extract Network information (Where)
  – Network address, network path and captured network live data, all network
5.7. Data analysis layer (cont.)

Digital forensics analysts would have to:

- Extract Entity, accounts information and rebuilding the relationship linkage (Who)
  - User accounts, phone number, emails, organization charts
- Analyze the extracted data based on forensics analysis procedures (How)
  - define the criteria to relate the hacking mechanism and the hypothesis.
- Reconstruct the event timeline (When)
  - determine whether the consistency of the timeline of evidence
5.8. Legal presentation layer

Legal prosecutor has to discuss with the CL:

• Legal Presentation Objectives (Why)
  – whether take litigation or close
  – are there sufficient evidence

• Legal Presentation Attributes (What)
  – what to present in the litigation, data relevance and admissibility.
  – let the analysts know whether additional evidence would be required.

• Legal Presentation Procedures (How).
  – define the arena for litigation(for this case criminal prosecution)
  – litigation tactics have to be considered.
5.8. Legal presentation layer (cont.)

Legal prosecutor has to discuss with the CL:

• Legal Jurisdiction Location (Where)
  – legal jurisdiction location has to be confirmed.

• Entities in Litigation Procedures (Who)
  – define the witness list and the interlocutory (temporary) questions.

• Timeline of entire event for Presentation (When)

• draft the entire story board of the case based on the evidence and determine if there something missing
6. Future work

• 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.
6. Future work

• 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 semiautomatic investigation toolbox.