
# FORZA: Digital Forensics Investigation Framework That Incorporate Legal Issues

*By*

**Ricci Sze-Chung Ieong**

*Presented At*

The Digital Forensic Research Conference

**DFRWS 2006 USA** Lafayette, IN (Aug 14th - 16th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

**http:/dfrws.org**

# FORZA – Digital Forensics Investigation Framework that incorporate legal issues (DFRWS 2006)

**Ricci IEONG,**
**Founder and Principal Consultant,**
**eWalker Consulting Ltd. (HK)**

# Agenda

- Revisit of two digital forensics cases
- Missing Link between these cases and existing forensics model and framework
- What is the feature of FORZA framework?
- Application of the FORZA framework?
- Benefit of using FORZA?
- Next steps

# Cases revisit

# Case 1: US vs Gorshkov

- **Oct 1999:**
  - Seattle FBI received a complaint from a local Internet Services Provider, Speakeasy
  - Online commerce system intrusion including server hosting and credit card transaction
  - Solicitation for computer security consulting via email from "subbsta"
  - Threat escalation
- **Dec 1999**
  - Speakeasy knocked offline

# Case 1: US vs Gorshkov

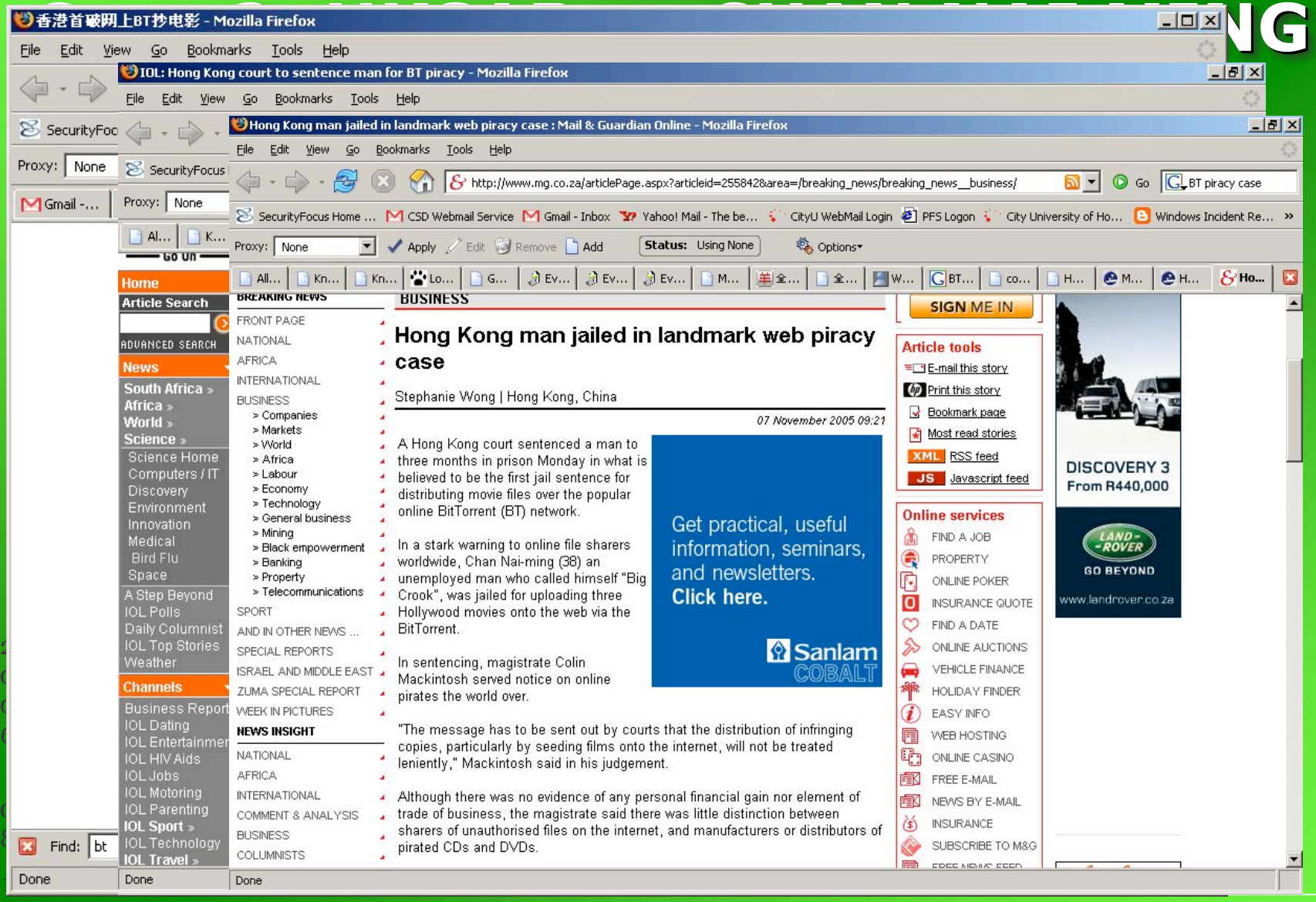
- **Similar timeframe in 1999**
  - FBI received complaint from Online Information Bureau, Vernon, CT
  - The online commerce servers were compromised and credit card information were stolen
  - Solicitation for computer security consulting via email from “subbsta”
  - Origin of attack were found to be generated from CTS in San Diego

# Case 1: US vs Gorshkov

- **What did the FBI do?**
  - Identify the common and difference between the case
  - Collect evidence and information from CTS
  - Confirm that the incident is from tech.net.ru which is from Chelyabinsk Russia
  - Identifies Alexey Ivanov (aka subbsta)

# Case 1: US vs Gorshkov

- **Then what did the FBI do next?**
  - Call Ivanov for security job opportunity
  - Setup Undercover operation
  - Setup Honeypot
- **Using collected user name and passwords, FBI login to suspects' machine (tech.net.ru) and dump out 4 CD-ROM of data.**
- **Afterwards hire experts to perform analysis**
  - Identification of OS
  - Reconstruct system directory overview
  - Determine system control
  - Analyze hacking utilities
  - Analyze of Perl scripts functions
  - Reconstruct the story of tech.net.ru hacking
- **Presentation of the case in court**

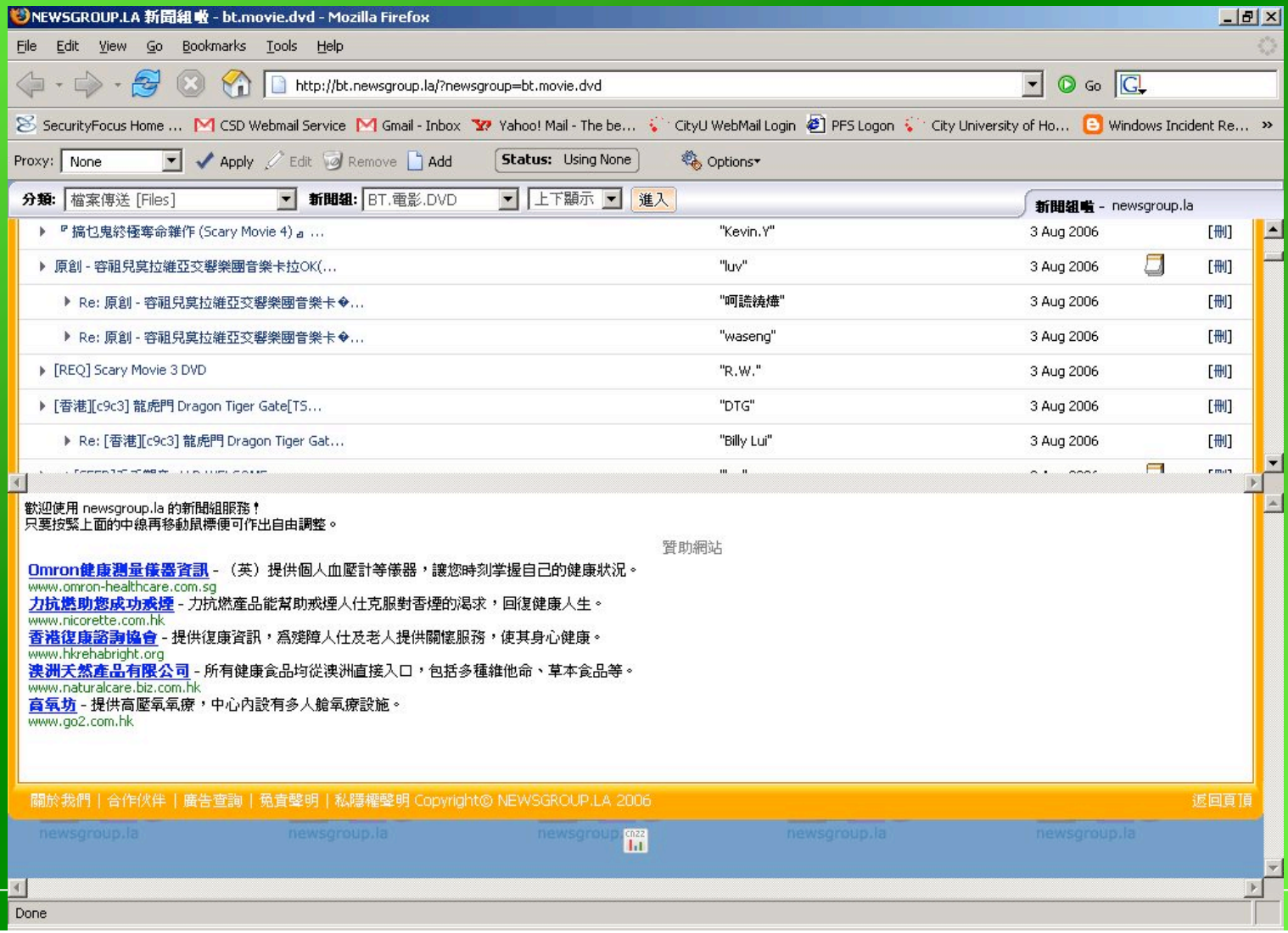

香港首破网上BT抄电影 - Mozilla Firefox
IOL: Hong Kong court to sentence man for BT piracy - Mozilla Firefox
Hong Kong man jailed in landmark web piracy case : Mail & Guardian Online - Mozilla Firefox
http://www.mg.co.za/articlePage.aspx?articleid=255842&area=/breaking_news/breaking_news__business/
BUSINESS
Hong Kong man jailed in landmark web piracy case
Stephanie Wong | Hong Kong, China
07 November 2005 09:21
A Hong Kong court sentenced a man to three months in prison Monday in what is believed to be the first jail sentence for distributing movie files over the popular online BitTorrent (BT) network.
In a stark warning to online file sharers worldwide, Chan Nai-ming (38) an unemployed man who called himself "Big Crook", was jailed for uploading three Hollywood movies onto the web via the BitTorrent.
In sentencing, magistrate Colin Mackintosh served notice on online pirates the world over.
"The message has to be sent out by courts that the distribution of infringing copies, particularly by seeding films onto the internet, will not be treated leniently," Mackintosh said in his judgement.
Although there was no evidence of any personal financial gain nor element of trade of business, the magistrate said there was little distinction between sharers of unauthorised files on the internet, and manufacturers or distributors of pirated CDs and DVDs.
Get practical, useful information, seminars, and newsletters. Click here.
Sanlam COBALT
DISCOVERY 3 From R440,000
LAND ROVER GO BEYOND
www.landrover.co.za

# Case 2: HKSAR vs CHAN NAI MING

# Case 2: HKSAR vs CHAN NAI MING

- **Officer-in-Charge (OC) received information from intelligence team. That complaint was initiated by Copyright Owner that some new torrent of new movies were found in HK newsgroup**
- **10 Jan 2005**
  - A customs officer browsed a HK movie newsgroup and saw a reference to Big Crook having uploaded a file to the BitTorrent newsgroup, which related to a film called "Daredevil".
  - There were images of inlay cards from the film, which had a picture of a statuette superimposed onto them and a .torrent file.
  - The .torrent file was downloaded and activated by the officer and showed the seeder's IP address, where the source seed was located.
  - The officer downloaded the film, as did two of the other downloaders, before the connection was broken
- **11 January 2005**
  - the same procedure was followed with two other films called "Red Planet" and "Miss Congeniality".
- **10 – 11 Jan 2005**
  - Communicated with ISP and Forum for the IP address and account owner of the IP address.
- **12 Jan 2005, 7:00am**
  - Laid ambush outside the defendant's home

# Case 2: HKSAR vs CHAN NAI MING



# Case 2: HKSAR vs CHAN NAI MING

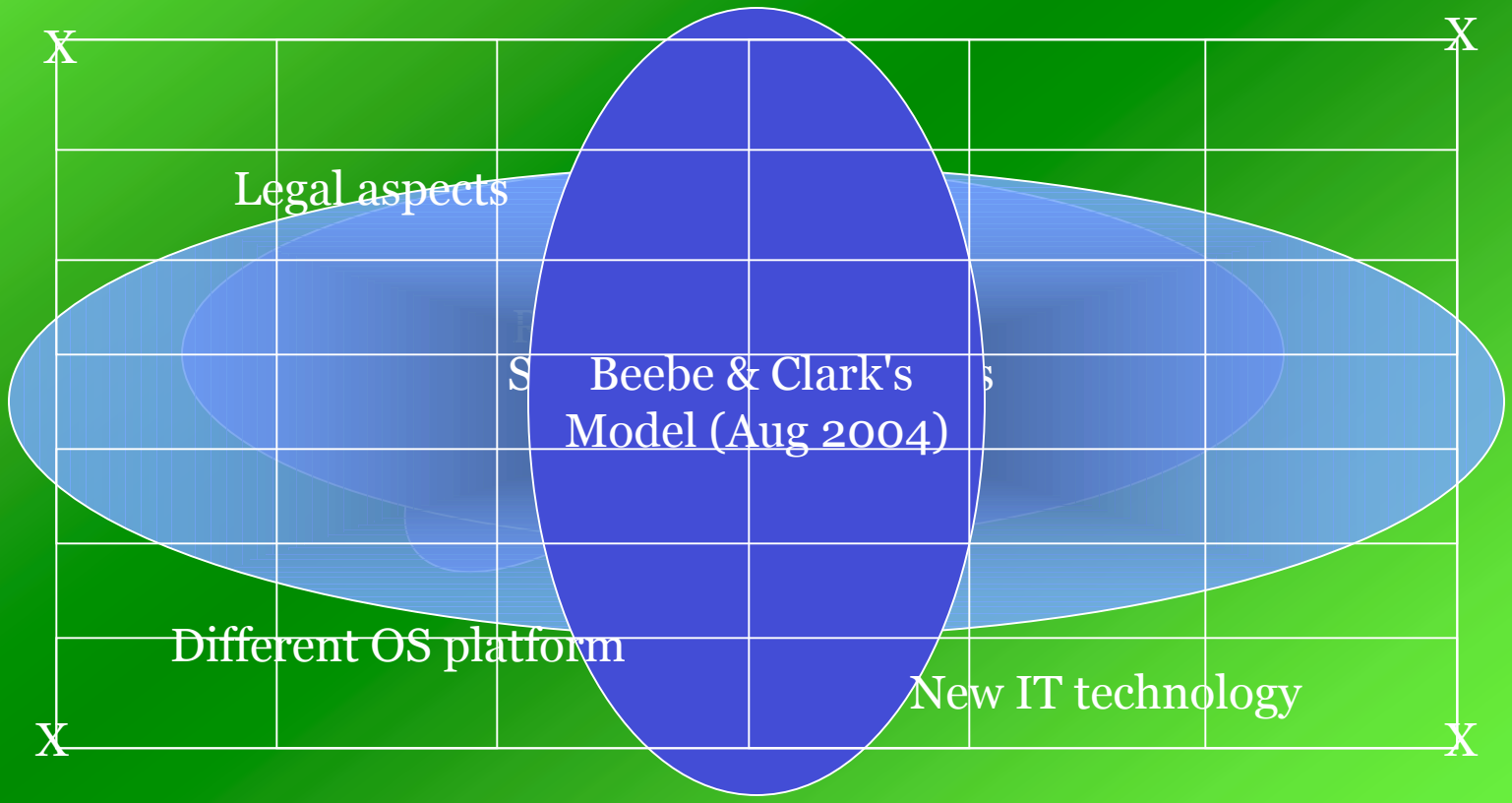
- **Defendant is before this court facing three charges**
  - Section 118(1)(f) of the Copyright Ordinance, Cap 528. of attempting to distribute an infringing copy of a copyright work, other than for the purpose of or in the course of any trade or business, to such an extent as to affect prejudicially the rights of the copyright owner;
  - Three alternative charges of obtaining access to a computer with dishonest intent, contrary to section 161(1) (c) of the Crimes Ordinance, Cap 200.

# Questions from the two cases

- Did the investigators followed any digital forensics framework?
- Is information collected over network from suspect's location considered to be sufficient evidence?
- What evidence be collected in order to put forward the case?
- When legal aspects should be incorporated?
- If you encountered similar case, what should you do?
- What procedures we should advise a beginner investigator to follow?

# Digital Forensics Models

# Comparison of various Forensics Model



# Forensics Model

- **There are a number of Forensics Investigation Procedures established**
  - Each organization developed their own procedures
  - Due to change of technology, different procedures have been derived
- **Most of them concentrate in the forensics investigation procedures**

# Pollitt's Zachman Forensics Model

- As Politt mentioned, forensics model concentrate on forensics procedures
- Mark Pollitt explained the Zachman's model for forensics.
- But Pollitt also mentioned that Zachman is not good for forensics model.

# Revisit Zachman Forensics Model

- But different roles, framework title could be selected
- In fact, there are other ways to select entities in Zachman Framework

# From Zachman, SABSA to FORZA

# Issues of current forensics model

- But those procedures are a **bit different** from each other because of their **focus in the part of the procedure**.
- **Business owner**, **system owner**, **technical staff** and **legal staff** involvement has not been included.
- Also there is **no unified forensics investigation framework**
- According to security documentation such as ISO13569 and ITIL standard, security documentation should be better organized into:
  - Framework
  - Standard
  - Policy
  - Technical Procedures

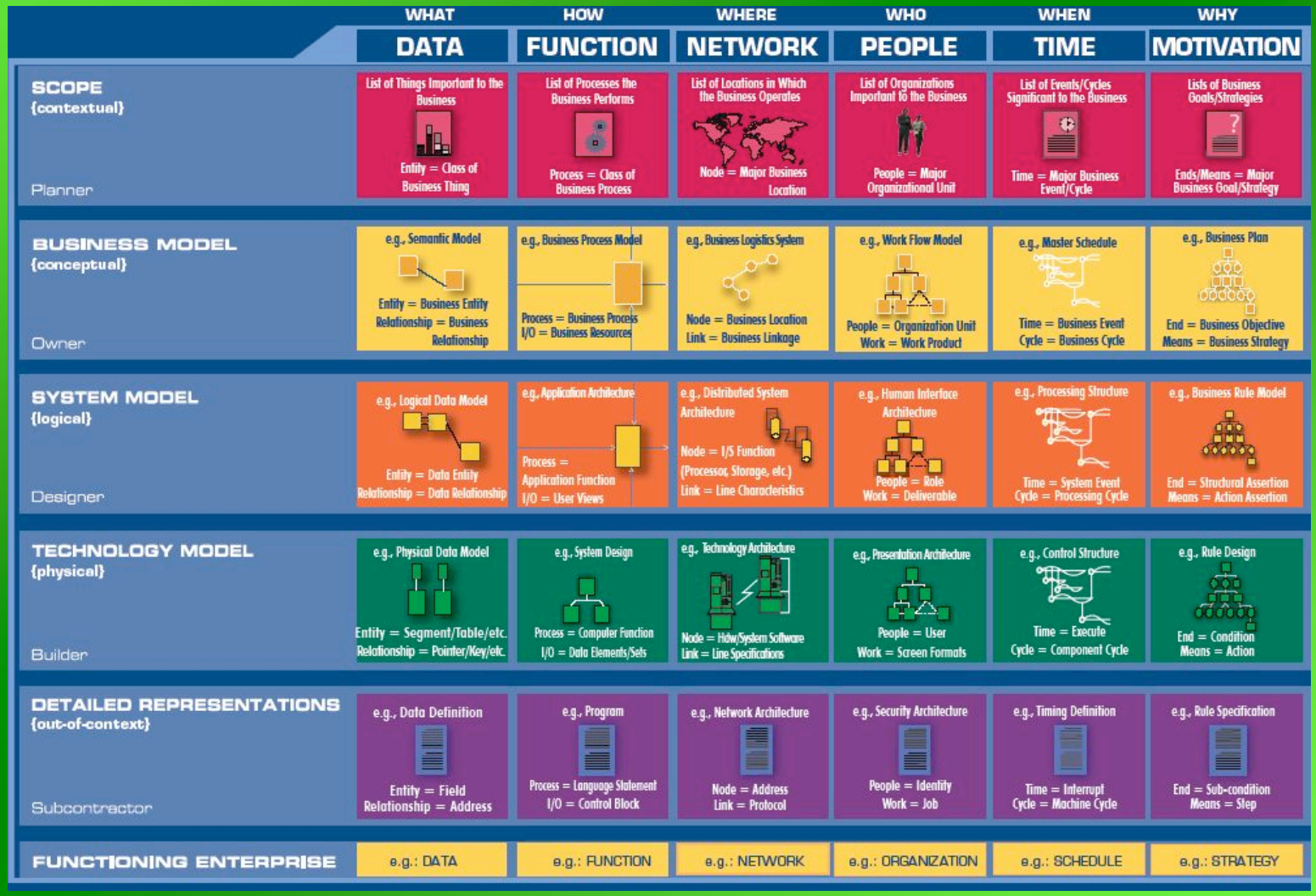
# Zachman Model

- **Zachman model outlines the requirement in developing Enterprise Architecture model.**
- **Requirements are listed as**
  - What
  - Why
  - How
  - When
  - Where
  - Who
- **Roles can be selected based on user**

# Zachman Model (Cont.)

- **Explanation of Zachman model roles, requirement**
  - The Planner View (Scope/Contextual Model)
  - The Owner View (Business/Conceptual Model)
  - The Designer View (System/Logical Model)
  - The Builder View (Technology/Physical Model)
  - The Subcontractor View (Detailed Representations/out-of-context)

# Zachman Framework



# SABSA Model

- Systems and Business Security Architecture (SABSA)
- The Framework has evolved since 1995 as a holistic business-driven approach for delivering cohesive security solutions to business and government.
- SABSA is a model and a methodology for developing risk-driven enterprise information security architectures and for delivering security infrastructure solutions that support critical business initiatives.
- SABSA is a Zachman based Security Model
- the SABSA Matrix also uses the same six questions that are used in the Zachman Framework and which were so eloquently articulated by Rudyard Kipling in his poem 'I Keep Six Honest Serving Men': What, Why and When, How, Where and Who?

# SABSA Model (Cont.)

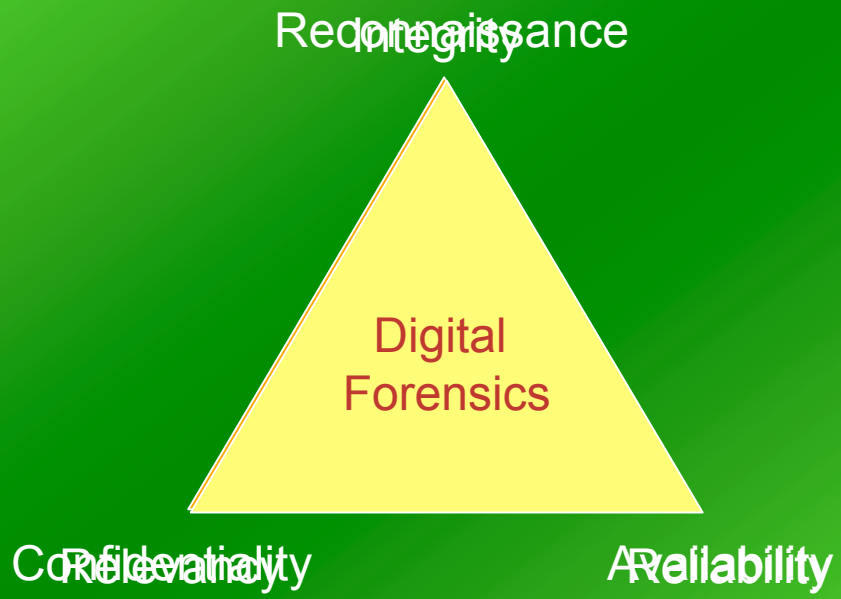
- **Explanation of SABSA model roles, requirement**
  - The Business View (Contextual Security Architecture)
  - The Architect's View (Conceptual Security Architecture)
  - The Designer's View (Logical Security Architecture)
  - The Builder's View (Physical Security Architecture)
  - The Tradesman's View (Component Security Architecture)
  - The Facilities Manager's View (Operational Security Architecture)

# SABSA Matrix

| | Assets (What) | Motivation (Why) | Process (How) | People (Who) | Location (Where) | Time (When) |
|---|---|---|---|---|---|---|
| Contextual | The Business | Business Risk Model | Business Process Model | Business Organization and Relationships | Business Geography | Business Time Dependencies |
| Conceptual | Business Attributes Profile | Control Objectives | Security Strategies and Architectural Layering | Security Entity Model and Trust Framework | Security Domain Model | Security-Related Lifetimes and Deadlines |
| Logical | Business Information Model | Security Policies | Security Services | Entity Schema and Privilege Profiles | Security Domain Definitions and Associations | Security Processing Cycle |
| Physical | Business Data Model | Security Rules, Practices and Procedures | Security Mechanisms | Users, Applications and the User Interface | Platform and Network Infrastructure | Control Structure Execution |
| Component | Detailed Data Structures | Security Standards | Security Products and Tools | Identities, Functions, Actions and ACLs | Processes, Nodes, Addresses and Protocols | Security Step Timing and Sequencing |
| Operational | Assurance of Operational Continuity | Operational Risk Management | Security Service Management and Support | Application and User Management and Support | Security of Sites, Networks and Platforms | Security Operations Schedule |

# FORZA Framework

# Attributes in Digital Forensics



# FORensics-ZAchman Model

- FORZA framework is derived based on Zachman
- It is an extended model that covers various forensics model using Zachman model.
- Focus more on the static attributes of the forensics aspects

# FORZA Framework

- **Roles in Digital Forensics**
  - Investigator in Chief/Officer in Charge (Contextual Investigation Layer)
  - System Owner (Contextual Layer)
  - Legal Advisor (Compliance Advisory Layer)
  - Security/System Architect/Auditor (Conceptual Security Layer)
  - IT Forensics Specialists (Technical Preparation Layer)
  - Forensics Investigators/System Administrator/Operator (Collection Layer)
  - Forensics Investigators/Forensics Analysts (Analysis Layer)
  - Legal Prosecutor (Presentation layer)

# FORZA Framework

| | Why | What | How | Where | Who | When |
|---|---|---|---|---|---|---|
| | Motivation | Data | Function | Network | People | Time |
| Chief Investigator/Officer in Charge (Contextual Investigation Layer) | Investigation Objectives | Event Nature | Requested Initial Investigation | Investigation Geograhy | Initial Participants | Investigation Timeline |
| System Owner (if any) (Contextual Layer) | Business Objectives | Business & Event Nature | Business & System Process Model | Business Geography | Organization & Participants relationship | Business & Incident Timeline |
| Legal Advisor (Compliance Advisory Layer) | Legal Objectives | Legal Background and preliminary issues | Legal Procedures for further investigation | Legal Geography | Legal Entities & 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 |
| IT 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 (Collection 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 (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 (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 |

# How to integrate current model

- **Incorporate various forensics investigation procedures**
- **Focus on forensics investigation aspects. More towards forensics investigation process**
- **Basic concept derived on the core aspects of forensics investigation**
  - Collection of digital evidence related to the case and suitable to legal consideration
  - Preservation of digital evidence
  - Reconstruct timeline and preserve chain of custody

# Investigator in Chief/Office in Charge (Contextual Investigation Layer)

| Why | What | How | Where | Who | When |
|---|---|---|---|---|---|
| **Motivation** | **Data** | **Function** | **Network** | **People** | **Time** |
| Investigation Objectives<br><br>**- what is the purpose of this investigation**<br>**- what is the potential incident**<br>**- what are the needs of the requester** | Event Nature<br><br>**- What is the nature of the reported event?**<br>**- IT system as: (Donn Parker's proposed categories)**<br>**- Object of crime**<br>**- Subject of crime**<br>**- Tools for conducting or planning a crime**<br>**- Symbol of computer used to intimidate or deceive**<br>**- IT system as major source/minor source of evidence?**<br>**- What functions has been disrupted?** | Requested Initial Investigation<br><br>**- What needs to be performed in this investigation**<br>**- What preliminary investigation should be performed and what information should be collected** | Investigation Geograhy<br><br>**- The geographical location of the reported event?** | Initial Participants<br><br>**- Who reported the case?**<br>**- Who is/are the suspects and victims?**<br>**- Who is the owner of the system?**<br>**- Who should be in the operation team for this case?**<br>**- What other resources required?** | Investigation Timeline<br><br>**- When event is reported?**<br>**- Any other similar event reported?**<br>**- When to call for action?** |

# System Owner (if any) (Contextual Layer)

| Why | What | How | Where | Who | When |
|---|---|---|---|---|---|
| **Motivation** | **Data** | **Function** | **Network** | **People** | **Time** |
| Business Objectives<br><br>**- What is the nature of the business**<br>**- What is purpose of system** | Business & Event Nature<br><br>**- What is the business of the company**<br>**- What is the purpose of the data/asset**<br>**- What are the affected data and systems?**<br>**- What data and systems should be protected?**<br>**- How is the events (Security incidents) happened?** | Business & System Process Model<br><br>**- What is the business process that required the affected system?**<br>**- What is the role of the affected information system in the business process?**<br>**- What function has been affected?**<br>**- What is the relationship between the information system with the reported event?** | Business Geography<br><br>**- The location/office of the source of identified issues**<br>**- Any other location of office, server room?** | Organization & Participants relationship<br><br>**- Who should be the responsible people (System admin, support, owner)?**<br>**- Any IT Security Architect/Solution Architect or Internal IT Auditor in the organization?**<br>**- Any Organization Chart**<br>**- What is the relationship between the organization with the reporting person, suspected participants?** | Business & Incident Timeline<br><br>**- When the system started operating?**<br>**- When is the event first reported?** |

# Legal Advisor/Compliance Manager/Disciplinary Board (Compliance Advisory Layer)

| Why | What | How | Where | Who | When |
|---|---|---|---|---|---|
| **Motivation** | **Data** | **Function** | **Network** | **People** | **Time** |
| Legal Objectives<br><br>**- What is the purpose of the dispute?**<br>**- What is the law of dispute?**<br>**- Is the case criminal or civil case?**<br>**- Determine should client/third-party be asked to preserve digital evidence?**<br>**- Suggest whether client should report to law enforcement agencies or institute private prosecution** | Legal Background and preliminary issues<br><br>**- What are the relevant law/ordinance**<br>**- What is the required and related information**<br>**- What data is required to be collected**<br>**- What is the issues of law and issues of fact**<br>**- Identify the facts and determine any gaps in the facts**<br>**- Identify which facts are probably agreed**<br>**- Identify which acts are probably in dispute**<br>**- Identify which facts you need evidence for**<br>**- Identify which facts you have evidence of**<br>**- Identify what is the case against the claimant/respondent?** | Legal Procedures for further investigation<br><br>**- What sections of the ordinance should be referred to?**<br>**- What are the key elements in the ordinance?**<br>**- Is there any injunction required?**<br>**- Is any warrant, search warrant required?**<br>**- Request preservation of evidence by client or by third party**<br>**- Formulate the required facts into search criteria.**<br>**- How can the evidence be admissible at trial?** | Legal Geography<br><br>**- Is that within jurisdiction of the country?**<br>**- What are the law governing the case?**<br>**- Does local court have the jurisdiction?** | Legal Entities & Participants<br><br>**- Who are the claimant/respondent?**<br>**- Who are the Legal Council, Prosecutor, Legal Staff?**<br>**- Who are likely to be the witnesses for the claimant and respondent?**<br>**- Who are likely to be experts and what are their credentials?** | Legal Timeframe<br><br>**- When was the offence first discovered / when was the matter of the information arose?**<br>**- When was the cause of action accrued?**<br>**- What is the time limit of the case?**<br>**- Is that within the time bar limit?**<br>**- What is the time span of the case?**<br>**- What are teh crucial dates for interlocutory proceedings?** |

eWalker Consulting Ltd.

# Security/System Architect/Auditor (Conceptual Security Layer)

| Why | What | How | Where | Who | When |
|---|---|---|---|---|---|
| **Motivation** | **Data** | **Function** | **Network** | **People** | **Time** |
| System/Security Control Objectives<br><br>**- What kind of security controls have been implemented to protect the information system/data?**<br>**- What is the security design model, risk management model?**<br>**- What is the missing security control that would lead to the issues?** | System Information and Security Control Model<br><br>**- What is the Security Control and System Information Model?**<br>**- What data/system has been involved?**<br>**- What is the data classification scheme and risk assessment scheme implemented?**<br>**- What protection scheme has been implemented?**<br>**- What Operating Systems are used?**<br>**- Is data encryption implemented?**<br><br>**- What kind of data lost?**<br>**- What event logging mechanism has been enabled?** | Security Mechanisms<br><br>**- How and what kind of security functions/policy being implemented?**<br>**- Which security functions detected the events? (e.g. Profile Detection, Anomalous detection, complaints, system monitoring or audit analysis?)** | Security Domain and Network Infrastructure<br><br>**- Is there any security domain and protection zone?**<br>**- Is the network infrastructure defined? (Network diagram, Firewall, IDS, and other security solution)**<br>**- Where is the location within the infrastructure?** | Users and Security Entity Model<br><br>**- What is the entities and their inter-relationship models?**<br>**- What is the roles and privilege of the entities?**<br>**- User Identity, Privileges and ACL of users**<br>**- Any people violating the rules or introducing the events to the system?** | Security Timing and Sequencing<br><br>**- When is the security protection implemented?**<br>**- Any time-dependency of the security protection mechanism?**<br>**- Is time synchronized implemented in the infrastructure?**<br>**- Any time-pattern of the identified incident?** |

# IT Forensics Specialists (Technical Preparation Layer)

| Why | What | How | Where | Who | When |
|---|---|---|---|---|---|
| **Motivation** | **Data** | **Function** | **Network** | **People** | **Time** |
| Forensics Investigation Strategy Objectives<br><br>**- With the specific requirement, what information should be collected?**<br>**- What mechanism, procedures should be adopted in this investigation process?** | Forensics Data Model<br><br>**- What is the hypothesis of the issue?**<br>**- What is the data that needs to be collected?**<br>**- What is the possible hidden data? Any hidden information needs to be collected**<br>**- What files (such as data files, log files) need to be collected?**<br>**- Any other events need to be collected**<br>**- What media needs to be captured?**<br>**- Is the data or media commonly used and previously captured type?**<br>**- What is the approved hardware/software that can be supported** | Forensics Strategy Design<br><br>**- What extraction procedures should be used for extracting the information?**<br>**- How to capture live/production information before turning off the machine**<br>**- How to capture data from the machine?**<br>**- Any specific investigation procedures need to be performed on the device?**<br>**- Reconstruct the hypothesis**<br>**- What tools could be used for extracting data from the media?**<br>**- Should ISP administrators be contact to preserve logs for collection?**<br>**- Should warrant would be required to ask ISP to expose IP address** | Forensics Data Geography<br><br>**- Where can the data be collected? (from ISP, media, volatile memory?)**<br>**- Where is the suspected source and target IP address of the event?**<br>**- is the network service provider, DNS located in the same location?**<br>**- Any suspected proxy server?** | Forensics Entity Model<br><br>**- Who should be the involved people**<br>**- Who should be interviewed**<br>**- Is 3rd party expert or vendor required to help in conducting the data collection or analysis?** | Hypothetical Forensics Event Timeline<br><br>**- when the event happen**<br>**- when the event start**<br>**- when the event completed**<br>**- Define the sequence of the collection activities** |

eWalker Consulting Ltd.

# Forensics Investigators/System Administrator /Operator (Collection Layer)

| Why | What | How | Where | Who | When |
|---|---|---|---|---|---|
| **Motivation** | **Data** | **Function** | **Network** | **People** | **Time** |
| Forensics Acquisition Objectives<br><br>**- How should the forensics investigation be performed?**<br>**- With what procedures and mechanism, should the investigation be processed?**<br>**- With what tools should be used in the investigation** | On-site Forensics Data Observation<br><br>**- What data reduction techniques being implemented?**<br>**- Any specific volatile information needs to be collected?**<br>**- Is the data to be captured live data?**<br>**- Is the event still ongoing?**<br>**- Is data being deleted?**<br>**- Any trojan or backdoor identified** | Forensics Acquisition/Seizure Procedures<br><br>**<u>Preparation</u>**<br>**- Sterize the storage media**<br>**- Copy the image using forensically sound system. (i.e. using commercial or open-source imaging technologies). Determine whether cloning of deleted information required?**<br>**- Perform on-site live data forensics investigation (Live data if necessary)**<br>**- Perform network monitoring (if necessary)**<br>**- Is Forensics Best Practices followed?**<br><br>**<u>Documentation</u>**<br>**- Document the scene**<br>**- Photo the scene**<br>**- Document the time/date stamp**<br>**- Document the Investigation procedures**<br>**- Create the inventory list**<br><br>**<u>Preservation and Duplication</u>**<br>**- Generate digital image**<br>**- Store the capture information**<br>**- Perform the cryptographic checksum for integrity preservation**<br><br>**<u>Transportation</u>**<br>**- Protect the evidence during transportation** | Site Network Forensics Data Acquisition<br><br>**- Is any other systems within the network being affected?**<br>**- Any other network devices affected?**<br>**- What is the actual network infrastructure?**<br>**- Any network devices forensics data to be collected?**<br>**- Is sniffing permitted to be implemented?**<br>**- Where is the backdoor connected (if any)** | Participants Interviewing and Hearing<br><br>**- Who should be interviewed?**<br>**- Rebuild the story board and events based on interviews** | Forensics Acquisition Timeline<br><br>**- What is the chain of custody**<br>**- What is the timeline created?** |

# Forensics Investigators/Forensics Analysts (Analysis Layer)

| Why | What | How | Where | Who | When |
|---|---|---|---|---|---|
| **Motivation** | **Data** | **Function** | **Network** | **People** | **Time** |
| Forensics Examination Objectives<br><br>**- Based on the collected information, what are the critical information that should be identified to prove the case?**<br>**- What needs to be search and extracted from the collected information?** | Event Data Reconstruction<br><br>**- What data, information to be extracted for analysis?**<br>**- Any damaged digital evidence?**<br>**- Any encrypted data relevant to investigation?**<br>**- What data needs to be searched?**<br>**- Extract user accounts information**<br>**- What is the statistical information**<br>**- What is the protocol information** | Forensics Analysis Procedures<br><br>**- Extract and examine the cloned image**<br>**- Analyze the case based on the hypothesis?**<br>**- Review the Internet activity history and log files**<br>**- Review data and compile an analysis report**<br>**- Prepare Expert Testimony**<br>**- Outline the Search space**<br>**- Search for keywords or search for specific files/image/video/audio file**<br>**- Correlate the identified activities between device logs**<br>**- Perform reverse-engineering of the identified code**<br>**- Perform any Pattern Matching** | Network Address Extraction and Analysis<br><br>**- Any identified IP address collected?**<br>**- Reconstruct the network path of the events** | Entity and Evidence Relationship Analysis<br><br>**- Any user accounts identified?**<br>**- Any user specific information identified?**<br>**- Any phone number identified?**<br>**- Any Email address?**<br>**- Who is the person related?**<br>**- User accounts and user entity relationship** | Event Timeline Reconstruction<br><br>**- Compare the hypothesis with the collected digital evidence time line**<br>**- Reconstruct the timeline**<br>**- Determine the time the suspect first appear and the start time of the event** |

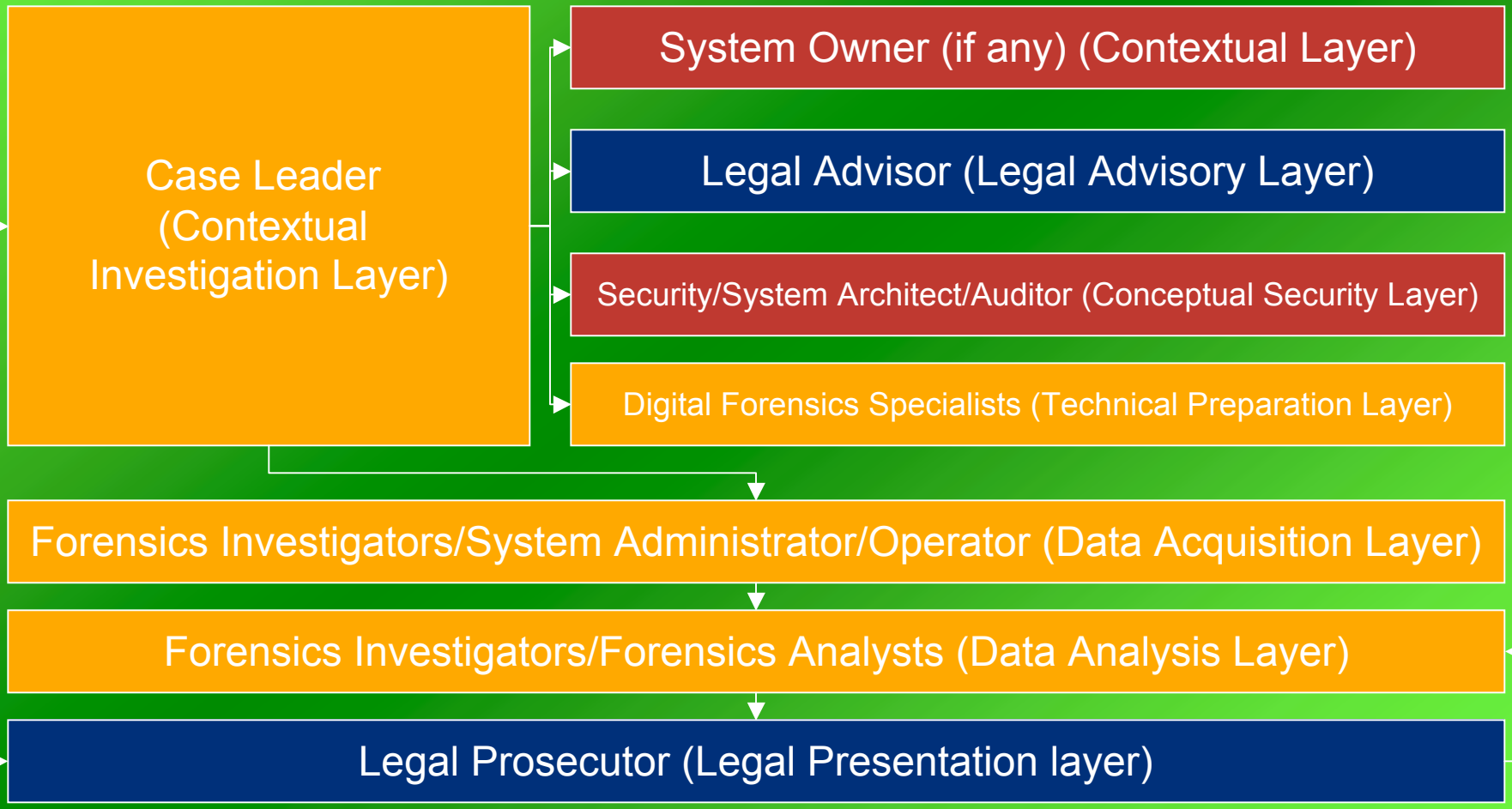
# Legal Prosecutor/Compliance Manager/Disciplinary Board (Presentation layer)

| Why | What | How | Where | Who | When |
|---|---|---|---|---|---|
| **Motivation** | **Data** | **Function** | **Network** | **People** | **Time** |
| Legal Presentation Objectives<br><br>**- Should the case be proceed or close?**<br>**- Is sufficient evidence collected?**<br>**- Which litigation mechanism should be used?**<br>**- Determine the chances of success?**<br>**- Determine if it is worth proceeding in this matter?** | Legal Presentation Attributes<br><br>**- What charge should be issued?**<br>**- What information should be included/excluded ?**<br>**- What evidence should be presented?**<br>**- How strong is the evidence?** | Legal Presentation Procedures<br><br>**- What litigation scheme should be used? (International Arbitration, local litigation?)**<br>**- What tactic should be used in the litigation procedure?**<br>**- Determine the civil and criminal interlocutory remedies needed?** | Legal Jurisdiction Location<br><br>**- Where should be the place of litigation?**<br>**- Where should be the place of enforcement?**<br>**- Where should be the place of hearing?** | Entities in Litigation Procedures<br><br>**- Which witnesses should be called?**<br>**- Any expert witnesses should be called?**<br>**- Which Judge, Council, Arbitrator involved?** | Timeline of the entire event for Presentation<br><br>**- Is the entire story board re-created?**<br>**- When should the case be presented?**<br>**- Any timeline missing in the evidence?** |

# Feature of FORZA model

- Divide the digital forensics investigation aspects into different roles
- Incorporate various digital forensics investigation procedures together
- Formulate information needed to be collected under 6 easy to remember category

# Flow in FORZA



# Benefit of the framework

- Cover various aspects of Digital Forensics aspects
- Include IT, investigator and legal aspects into the digital forensics investigation
- Provide a framework with scope of investigation
- Unified various procedures and produce a framework that enables systematic approach of digital forensics investigation.
- Enable less experience user to carry out investigation
- Assist digital forensics procedures to be developed for new cases

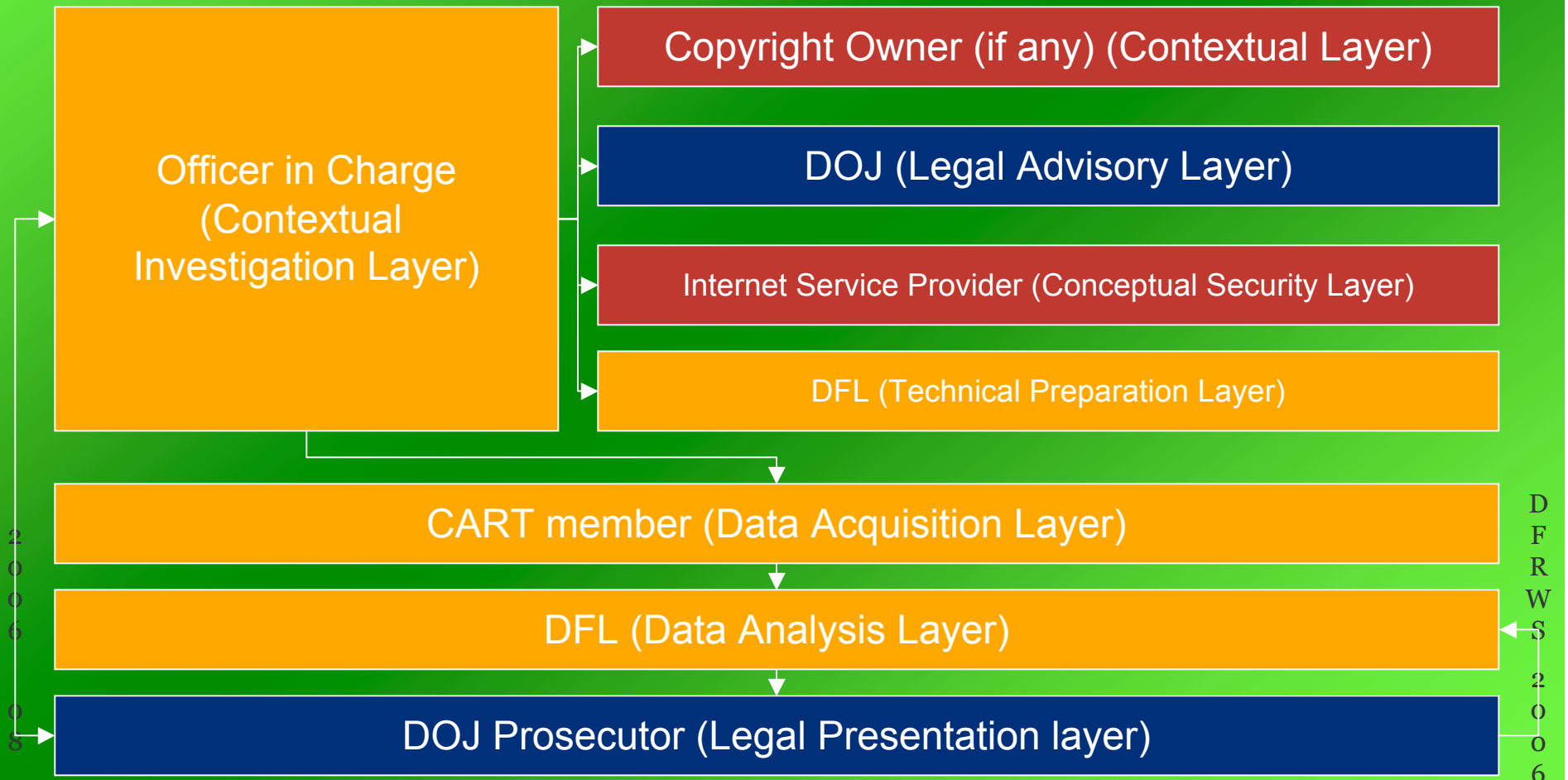
# Weakness of the framework

- Spectrum in the model is wide
- Difficult to be adopted if digital forensics cookbook has been developed
- Too new to be adopted. More comments and feedbacks from different law enforcement team to enhance this dynamic framework is required
- No specific technology dependent methodology and solution is included
- No ready to use digital forensics cookbook could be used

# Revisit of BT case

eWalker Consulting Ltd.

# The Flow of BT case in FORZA



# Case 2: BT case

- Officer-in-Charge (OC) received information from intelligence team. That complaint was initiated by Copyright Owner that some new torrent of new movies were found in HK newsgroup
- OC discussed with Copyright Owner what's nature of their complaint? And what did the Copyright Owner wish to perform?
- Then OC discussed with IT folks and search for some background about Bit Torrent
- OC then discussed with Prosecutors which law would be applicable for this new case and what is the necessary information should be collected as evidence. (in HK, only the uploader/illegal publishing would be charged for criminal offense)
- OC then discussed with Forensics specialists about the methods to collect those evidence and the constrains in the methods used for collecting information.
- OC then planned and coordinate resources for conducting the actions.

# Case 2: BT case

- OC setup a monitoring team for monitoring the new torrent upload in newsgroup
- OC found a frequent uploader of movies posted a new torrent of the film he prepared into one of the newsgroup OC monitored
- OC then initiated the action by
  - Immediately collected the IP address owner information from the newsgroup forum and ISP
  - Immediately started downloading the movie
  - Immediately sent the troop to the location of the uploader home.
- During the uploading time, the troop entered to the uploader home and found the computer for uploading the movie together with the VCD related to this case.

# Next Step in the model

- Develop a dynamic FORZA flow model to forensics investigation tools
- Apply the FORZA framework into forensics investigation tools

# Questions?

# Backup Slides

# DFRWS' Framework

| IDENTIFICATION | PRESERVATION | COLLECTION | EXAMINATION | ANALYSIS | PRESENTATION |
|---|---|---|---|---|---|
| **Event/Crime Detection** | **Case Management** | **Preservation** | **Preservation** | **Preservation** | Documentation |
| Resolve Signature | Imaging Technologies | **Approved Methods** | **Traceability** | **Traceability** | Expert Testimony |
| Profile Detection | **Chain of Custody** | Approved Software | Validation Techniques | Statistical | Clarification |
| Anomalous Detection | **Time Synch.** | Approved Hardware | Filtering Techniques | Protocols | Mission Impact Statement |
| Complaints | | **Legal Authority** | Pattern Matching | Data Mining | Recommended Countermeasure |
| System Monitoring | | Lossless Compression | Hidden Data Discovery | Timeline | Statistical Interpretation |
| Audit Analysis | | Sampling | Hidden Data Extraction | **Link** | |
| | | Data Reduction | | Spatial | |
| | | Recovery Techniques | | | |

**Figure 2. The DFRWS Digital Investigative Framework**

# From Incident Response

- **In the book Incident Response, an "incident response methodology" is given with the following phases:**
  - **Pre-incident Preparation:** Prepare for an incident with proper training and infrastructure.
  - **Detection of the Incident:** Identify a suspected incident.
  - **Initial Response:** Verify that the incident has occurred and collect volatile evidence.
  - **Response Strategy Formulation:** Determine a response based on the known facts.
  - **Duplication:** Create a backup of the system.
  - **Investigation:** Investigate the system to identify who, what, and how.
  - **Secure Measure Implementation:** Isolate and contain the suspect system before it is rebuilt.
  - **Network Monitoring:** Observe the network to monitor attacks and identify additional attacks.
  - **Recovery:** Restore the system to its original state with additional security measures added.
  - **Reporting:** Document the response steps and remedies taken.
  - **Follow-up:** Review the response and adjust accordingly.

# DOJ's Electronic Crime Scene Investigation Guide

- **The U.S. Department of Justice (DOJ) published a process model in the Electronic Crime Scene Investigation Guide**
  - **Preparation:** Prepare equipment and tools to perform needed tasks during an investigation.
  - **Collection:** Search for and collect electronic evidence.
    - **Secure and Evaluate the Scene:** Secure the scene to ensure the safety of people and the integrity of evidence. Potential evidence should be identified in this phase.
    - **Document the Scene:** Document the physical attributes of the scene including photos of the computer.
    - **Evidence Collection:** Collect the physical system or make a copy of the data on the system.
  - **Examination:** A technical review of the system for evidence.
  - **Analysis:** The Investigation team reviews the examination results for their value in the case.
  - **Reporting:** Examination notes are created after each case.

# Séamus' "An Extended Model of Cybercrime Investigations"

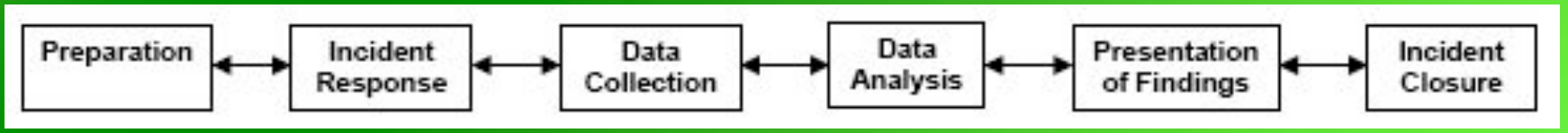
- **Based on Séamus Ó Ciardhuáin, "An Extended Model of Cybercrime Investigations", International Journal of Digital Evidence Summer 2004, Volume 3, Issue 1**
  - Lee's Model
  - Casey's Model
  - DFRWS Model
  - Reith, Carr and Gunsch Model
- **Séamus also proposed an extended model**

# Séamus' "An Extended Model of Cybercrime Investigations"

| *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 | | | | |

# Nicole Lang Beebe and Jan Guynes Clark's Model

- Nicole Lang Beebe and Jan Guynes Clark, "A Hierarchical, Objectives-Based Framework for the Digital Investigations Process, Digital Forensics Research Workshop (DFRWS), Baltimore, Maryland, August 2004



| | Prep. | Incident Response | Data Collect. | Data Analysis | Findings Present. | Incident Closure |
|---|---|---|---|---|---|---|
| **Palmer, 2001 (DFRWS model)** | | | | | | |
| Identification | | ✓ | | | | |
| Preservation | | | ✓ | | | |
| Collection | | | ✓ | | | |
| Examination | | | | ✓ | | |
| Analysis | | | | ✓ | | |
| Presentation | | | | | ✓ | |
| Decision | | | | | | ✓ |
| **Department of Justice, 2001** | | | | | | |
| Collection | | | ✓ | | | |
| Examination | | | | ✓ | | |
| Analysis | | | | ✓ | | |
| Reporting | | | | | ✓ | |
| **Reith et al, 2002 (Abstract Model)** | | | | | | |
| Identification | | ✓ | | | | |
| Preparation [for the current investigation] | | ✓ | | | | |
| Approach strategy | | ✓ | | | | |
| Preservation | | | ✓ | | | |
| Collection | | | ✓ | | | |
| Examination | | | | ✓ | | |
| Analysis | | | | ✓ | | |
| Presentation | | | | | ✓ | |
| Returning evidence | | | | | | ✓ |
| **Mandia et al, 2003** | | | | | | |
| Pre-incident preparation | ✓ | | | | | |
| Detection of incidents | | ✓ | | | | |
| Initial response | | ✓ | | | | |
| Formulate response strategy | | ✓ | | | | |
| Data collection | | | ✓ | | | |
| Data analysis | | | | ✓ | | |
| Reporting | | | | | ✓ | |
| **Carrier and Spafford, 2003** | | | | | | |
| Readiness | ✓ | | | | | |
| Deployment | | ✓ | | | | |
| Digital crime scene investigation | | | ✓ | ✓ | ✓ | |
| Preservation | | | ✓ | | | |
| Survey | | | | ✓ | | |
| Documentation | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Search and collection | | | ✓ | ✓ | | |
| Reconstruction | | | | ✓ | | |
| Presentation | | | | | ✓ | |
| Review | | | | | | ✓ |
| **Nelson et al, 2004** | | | | | | |
| Initial assessment | | ✓ | | | | |
| Approach strategy ("design") | | ✓ | | | | |
| Resource determination | | ✓ | | | | |
| Copy evidence | | | ✓ | | | |
| Risk identification & mitigation | | ✓ | | | | |
| Test approach strategy ("design") | | | ✓ | ✓ | | |
| Data analysis and recovery | | | | ✓ | | |
| Data investigation | | | | ✓ | | |
| Report | | | | | ✓ | |
| Critique | | | | | | ✓ |