

Digital Forensics on Future HK Infrastructure

Ricci IEONG, CISSP, CISA, CEH, F.ISFS, ISSAP, ISSMP,
Secretary of Information Security and Forensics Society
Principal Consultant of eWalker Consulting Limited

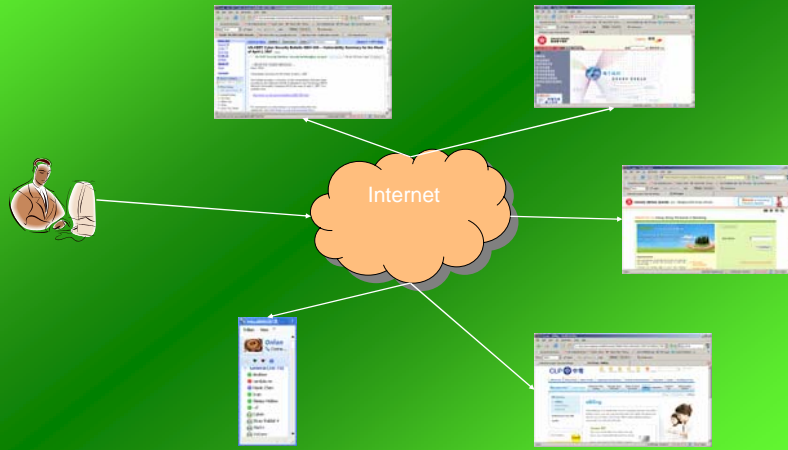


HK IT infrastructure

- **Internet Service Provider**
 - Telcom network
- **Service Content provider**
 - Email Services
 - Web Content Services (e.g. Government Services, Public utilities,
 - eBanking Services



HK IT infrastructure



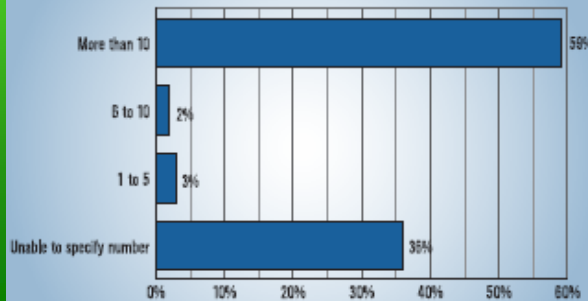
2
0
0
7
0
4
1
6

I
C
T
E
x
p
o
s
e



More Web hacking

Figure 15. Percentage Experiencing Web Site Incidents



CSI/FBI 2008 Computer Crime and Security Survey
Source: Computer Security Institute

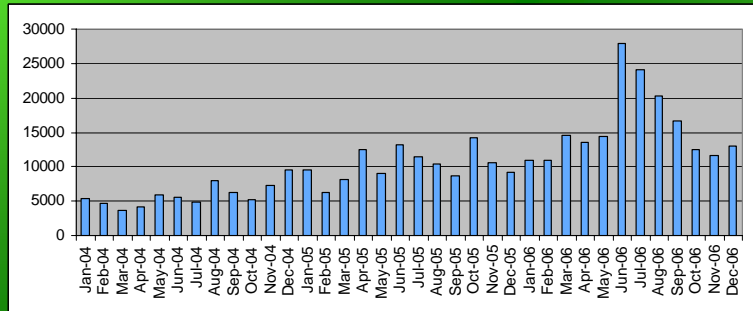
2008: 212 Respondents

2
0
0
7
0
4
1
6

I
C
T
E
x
p
o
s
e



Single IP attack (2004 – 2006)



2
0
0
7
0
4
1
8

I
C
T
E
x
p
o
s
e



Phishing (Dec 06) – By Country



2
0
0
7
0
4
1
8

I
C
T
E
x
p
o
s
e





What is Computer Forensics

Computer Forensics Basics

- **Forensic computing is the process of identifying, preserving, analyzing and presenting digital evidence in a manner that is *legally* acceptable in any legal proceeding**

What a Computer Forensics Investigator do?

- **To dig out the evidence related to computer crime**
- **Preserve the chain of custody of the entire case**
- **To build the case from the fragmented information**

2
0
7
0
4
1
8

I
C
T
E
x
P
o
0
7



General procedures in Forensics Investigation

- **Determine level of volatility**
- **Preserve volatile information**
- **Duplicate the original hard disk to at least 2 copies of hard disk**
- **Search for the obvious evidence**
- **Change the parameters on the system**
 - Restore the deleted files
 - Recover information from the swap drive
 - Remove the back door or trojan horse files
 - Change of some system parameters
- **Document all the steps and response of the system during the Investigation procedure**

2
0
7
0
4
1
8

I
C
T
E
x
P
o
0
7



Goals of Forensics Investigation

- Identify the attackers
- Identify the method/motivation of the attacks
 - Modus Operandi
- Identify the gain of the attacks
 - Damage assessment
- Preserve the evidence
- Present the evidence in a law case

2
0
0
7
0
4
1
6

I
C
T
E
x
P
o
0
7



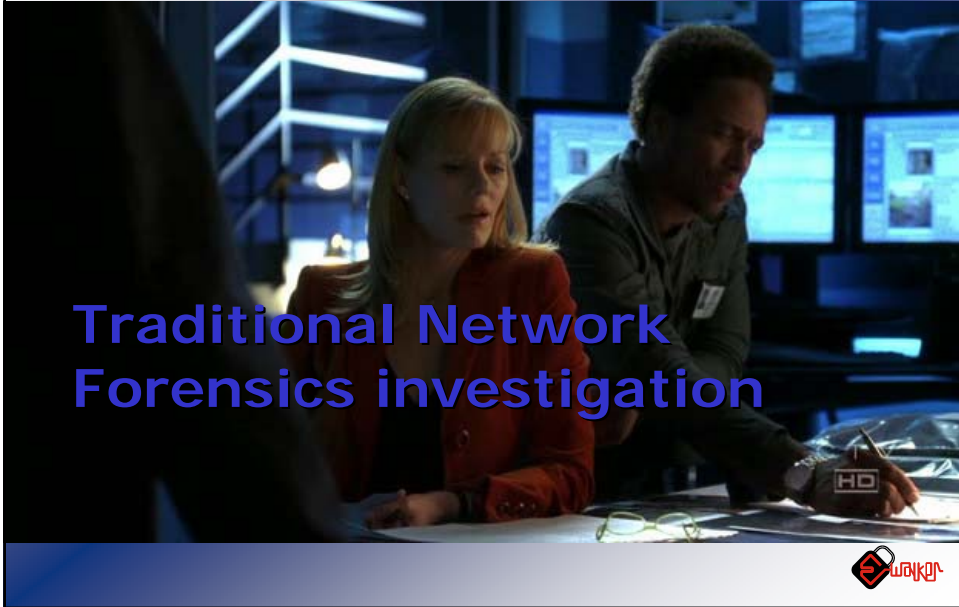
Who Wants Digital Evidence?

- Criminal Prosecutor
- Civil Litigation
- Insurance Companies
- Corporations
- Law Enforcement Officials
- Individuals

2
0
0
7
0
4
1
6

I
C
T
E
x
P
o
0
7





Types of attack

- Scanning/Probing
- Denial of Service
- Unauthorized Access
- Leakage of information
- Virus/Worm Attack
- Web attack – defacement, login attempt
- Intrusion

Potential source of evidence

- System logs
- Network devices logs
- IDS logs
- Web Server logs
- Browser history, cookie, index
- Network information
- Process information

2
0
0
7
0
4
1
8



I
C
T
E
x
P
o
0
7

Log Analysis

- Significant Events Recognition
 - Intrusion detection systems
- Log correlation
- Target Specific
 - Web Defacement Through Known Exploits
 - Web Defacement Through Application Bugs
 - Virii
- Establish Series of Events

2
0
0
7
0
4
1
8



I
C
T
E
x
P
o
0
7

Damage Analysis

- Identify the attacks
- Identify the motivations
- Identify the gains
- Identify the attack paths

2
0
0
7
0
4
1
6



I
C
T
E
x
P
o
0
7

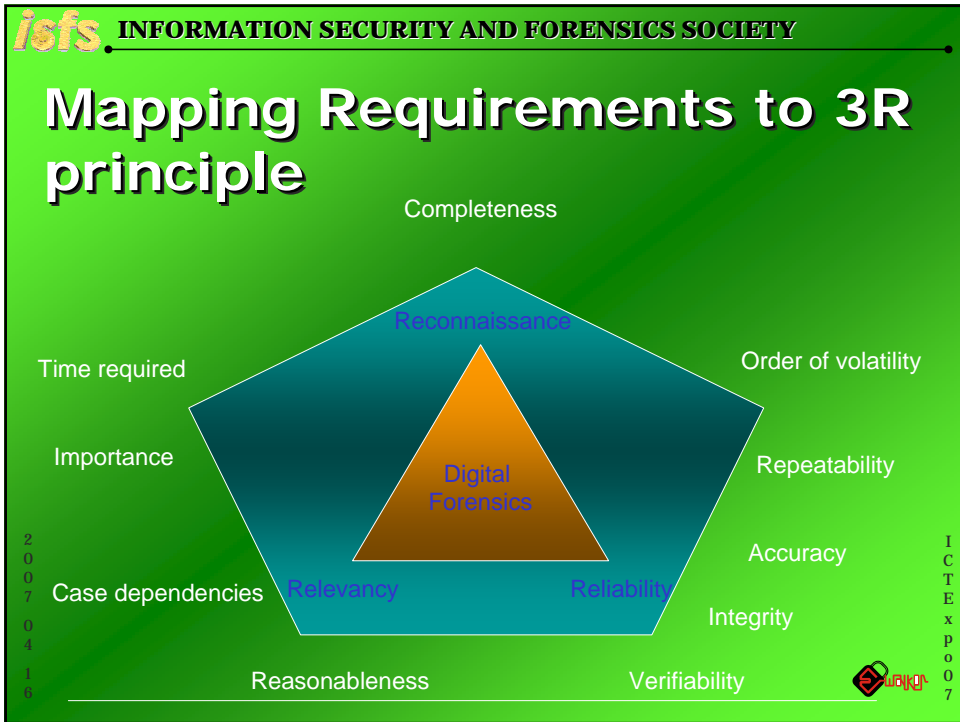
HK Future Infrastructure Change

- Infrastructure change
 - Go mobile
 - Go for free network
- Content change
 - More content driven

2
0
0
7
0
4
1
6



I
C
T
E
x
P
o
0
7



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

2
0
0
7
0
4
1
6

I
C
T
E
x
P
o
o
7



FORZA Framework

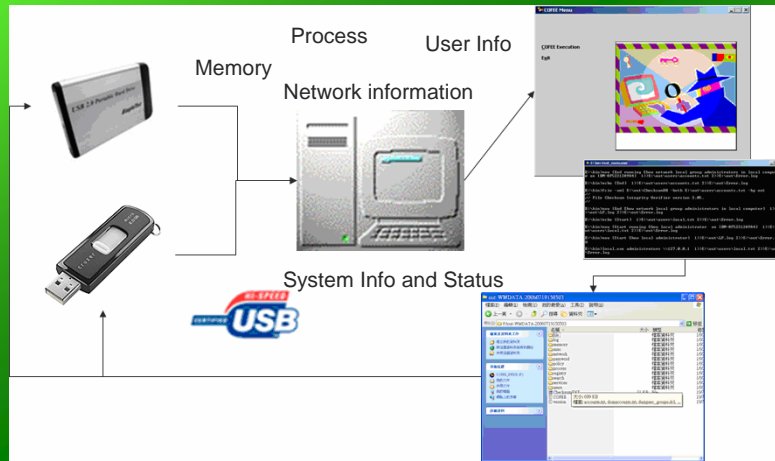
	Who	What	Where	When
Chief Investigator/Officer in Charge (Contextual Investigation Layer)	Investigative Objectives	Investigative Objectives	Initial Participants	Investigative Timeline
System Owner (if any) (Contextual Layer)	System Owner	System Owner	System Owner	System Owner
Legal Advisor (Compliance Advisory Layer)	Legal Advisor	Legal Advisor	Legal Advisor	Legal Advisor
Security/System Architect/Auditor (Conceptual Security Layer)	Security/System Architect/Auditor	Security/System Architect/Auditor	Security/System Architect/Auditor	Security/System Architect/Auditor
IT Forensics Specialists (Technical Preparation Layer)	IT Forensics Specialists	IT Forensics Specialists	IT Forensics Specialists	IT Forensics Specialists
Forensics Investigators/System Administrator/Operator (Collection Layer)	Forensics Investigators/System Administrator/Operator	Forensics Investigators/System Administrator/Operator	Forensics Investigators/System Administrator/Operator	Forensics Investigators/System Administrator/Operator
IT Forensics Specialists (Forensic Preparation Layer)	IT Forensics Specialists	IT Forensics Specialists	IT Forensics Specialists	IT Forensics Specialists
Forensics Investigators/Forensic Analysts (Analysis Layer)	Forensics Investigators/Forensic Analysts	Forensics Investigators/Forensic Analysts	Forensics Investigators/Forensic Analysts	Forensics Investigators/Forensic Analysts
Legal Prosecutor (Presentation layer)	Legal Prosecutor	Legal Prosecutor	Legal Prosecutor	Legal Prosecutor
Legal Prosecutor (Presentation layer)	Legal Presentation Objectives	Legal Presentation Attributes	Legal Presentation Procedures	Legal Jurisdiction Location

2
0
0
7
0
4
1
6

I
C
T
E
x
P
o
o
7



What information to collect

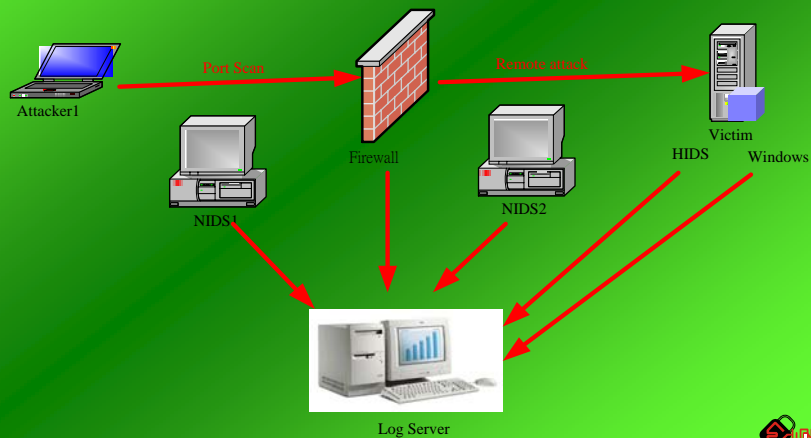


2
0
0
7
0
4
1
6

I
C
T
E
x
p
o
s
i
t
i
o
n



Scenario – Remote Botnet attack



2
0
0
7
0
4
1
6

I
C
T
E
x
p
o
s
i
t
i
o
n



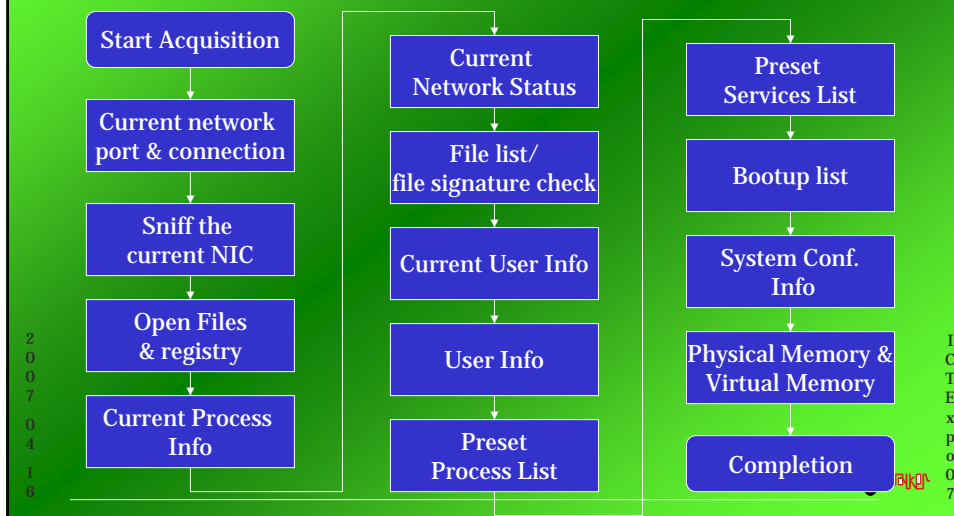
Scenario – Remote Attack

Application Attack Incident

Events Grouped from different devices:

- NIDS1 (Scan / Attack)
- Firewall (Port Scan)
- NIDS2 (Attack)
- HIDS (Attack)
- Windows (Remote Login)

LF Procedures for botnet





isfs INFORMATION SECURITY AND FORENSICS SOCIETY

Technology Improvement

- Operating Systems
- Digital Devices
- Cryptography, Steganography
- Data Volume, Storage Architecture
- Anti-forensics
- Wireless Network

20070418

ICT Expo 07

Forensics Tools

- **Expensive**
 - To purchase
 - To maintain research and development labs
 - To catch up technology advanced
- **Not Yet a Formal Certification**
 - Hard to verify
- **Still Room For Improvement**
 - Intelligent Analysis and Event Correlation

2
0
0
7
0
4
1
6

I
C
T
E
x
p
o
s
e



Legislation

- **Conflicting law**
- **Ambiguous law**
- **Lack of precedent**
- **Not enough technical knowledge and tools**

2
0
0
7
0
4
1
6

I
C
T
E
x
p
o
s
e



Awareness

- **Insufficient Preparation**
- **Ignorance**
- **Insufficient Security Knowledge/Skills**

2
0
0
7
0
4
1
6



I
C
T
E
x
P
o
0
7

Future Direction in Computer Forensics

- **Fast Network based Log correlation and analysis solution**
- **Combination of Forensics Investigation tools with Intrusion Monitoring systems**
- **Live Forensics Investigations Toolkits**
- **More Technical and Legal Training**

2
0
0
7
0
4
1
6



I
C
T
E
x
P
o
0
7

Questions?

Ricci IEONG

[Ricci_ieong \(at\) isfs \(dot\) org \(dot\) hk](mailto:Ricci_ieong@isfs.org.hk)

[Ricci \(at\) ewalker \(dot\) com \(dot\) hk](mailto:Ricci@ewalker.com.hk)



About ISFS



About ISFS

- **Information Security and Forensics Society (ISFS) founded in May 2000 by a group of digital forensics specialists and practitioners**



2
0
0
7
0
4
1
8

I
C
T
E
x
P
o
0
7



Goals

- **to regulate and standardize the practice of information security and forensics professionals;**
- **to conduct examinations and act in such other manner as may be necessary to ascertain whether persons are qualified to be admitted to register as an information security and forensics professional;**
- **to encourage the study of information security and forensics by holding regular training courses and seminars;**
- **to promote public awareness of information security and forensics.**

2
0
0
7
0
4
1
8

I
C
T
E
x
P
o
0
7



Council Members (2006 and 2007)

Chairman	Dr. Hilton CHAN
Vice-Chairman	Mr. David LEUNG
Secretary	Mr. Ricci IEONG
Treasurer	Mr. Michael KWAN
Council Members	Dr. KP CHOW
	Mr. Vitus CHUNG
	Mr. Anthony FUNG
	Dr. W.W. FUNG
	Mr. Vincent IP
	Mr. Collins LEUNG

2
0
0
7
0
4
1
8



I
C
T
E
x
P
o
0
7