THE FUTURE OF DIGITAL FORENSICS

SungKyong Un
ETRI

Session ID: CLE-W04
Session Classification: Intermediate
Digital Forensics
DFRWS (2001) defines

The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.
Digital Forensics Procedure

Source: TTAS.KO-12.0058
“Computer Forensics Guideline”
Imaging

HDD Imaging
source: joncrel@flickr

Hardware Duplicator
source: http://www.solstice-inc.com
Recovery
Keyword Search

source: Konrad Andrews@flickr
Registry
Email

WINNING NOTIFICATION
BONO LOTTERY INTERNATIONAL [bono]

FROM THE DESK OF THE PROMOTIONS MANAGER,
INTERNATIONAL PROMOTIONS AWARD DEPARTMENT
Ref: FER/3690/5103/34

Batch: 145-279-382
Winning No: 801/ibs/125

Attr: We happily announce to you the draw of the Bono Lottery International Program held on the 18th of July, 2005. Your name "email address" was attached to ticket number 1232477.
Messenger
Anti-Forensics - Eraser

Automatic Eraser
source: http://www.wiebetech.com

Magnatic Eraser
source: http://www.garner-product.com
Anti-Forensics - Encryption

- **MS BitLocker**
  - Drive Encryption (AES)
  - Windows Vista, 7

- **Apple FileVault**
  - Encrypted File System (AES)
  - Mac OS X v10.3

- **MS Office Encryption Option**
  - Various Algorithm
Anti-Forensics - Countermeasure

88 Node Performance : 200,000,000/sec

GPU based parallel password search
Source : ETRI

FPGA based password search
Source : www.tableau.com
The Present
SmartPhone Forensics
# SmartPhone Forensics

<table>
<thead>
<tr>
<th>Item</th>
<th>Dummy</th>
<th>Smart</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Models</td>
<td>&gt;1,000/Year</td>
<td>&gt;10/Year</td>
</tr>
<tr>
<td>OS</td>
<td>Symbian, Qualcomm</td>
<td>iOS, Android, Windows Mobile, BlackberryOS</td>
</tr>
<tr>
<td>Interface</td>
<td>Various</td>
<td>USB</td>
</tr>
<tr>
<td>Acquisition</td>
<td>Logical, Physical</td>
<td>Logical, Physical, Backup</td>
</tr>
<tr>
<td>Data</td>
<td>Phone book, Call history, SMS, Photo, Schedule</td>
<td>+ Email, Web History, Map, Location, SNS, Message, App, ID/PW</td>
</tr>
<tr>
<td>DB Format</td>
<td>Various</td>
<td>Sqlite</td>
</tr>
<tr>
<td>3rd Party App</td>
<td>-</td>
<td>App Market</td>
</tr>
</tbody>
</table>
Analysis - Briefing
Analysis - Timeline
Analysis – Web Browsing
Analysis – Location & Routing
## Analysis – App

<table>
<thead>
<tr>
<th>Category</th>
<th>App</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone Call</td>
<td>Skype, Viber, Google Voice, ...</td>
</tr>
<tr>
<td>Message</td>
<td>Cacao Talk, iMessage, Twitter DM, Facebook Message, ...</td>
</tr>
<tr>
<td>SNS</td>
<td>Twitter, Facebook, me2day, ...</td>
</tr>
<tr>
<td>Storage</td>
<td>Dropbox, uCloud, SugarSync, Box.net, iCloud, ...</td>
</tr>
<tr>
<td>Key</td>
<td>DataVault, 1Password, Strip, ...</td>
</tr>
</tbody>
</table>
Analysis – Communication Network

Network of Telephone Calls

Quickly identify key phones in networks of calls

source: http://www.i2group.com
Analysis – Social Network
The Future
Problem or Inconvenience

Large Storage $\rightarrow$ Search Space++ $\rightarrow$ 1TB 14H? (20MB/s)

New Device/Service $\rightarrow$ New Tools $\rightarrow$ Buy/Educate? $\rightarrow$ Forensics = Tool Expert?

New Environment $\rightarrow$ Internet $\rightarrow$ Cloud Computing $\rightarrow$ Smart Phone
(Blog, Cafe, SNS) (Seizure & Search Warrant?)

Binary Search $\rightarrow$ Index Search $\rightarrow$ What if keyword is not known?
New Viewpoint

Investigating the case, not the device  →  Need information, not data

Multiple device/services per user  →  Need multi(source) data integration

Continuous device/service creation/change  →  Need a framework to host

Multiple remote sites  →  Need mobility & connectivity

Volatile evidences  →  Need acquisition method & third party attestation
The Future of Digital Forensics

Data Centric Analysis  →  Conduct Centric Analysis

Forensic Tools  →  Forensic Services
Conduct Centric Analysis

- Multi-source Evidence Acquisition
- Relationship Analysis
- Intuitive Analysis
- Automatic Analysis Based on the Profile
Forensic Services

- Parallel/Distributed Platform for Large Data Handling
- Adapting Fast Changing Device/Tools
- User Mobility & Connectivity
Forensic Cloud: Forensics as a Service

Forensic Cloud Technology Framework

Presentation Layer
- Multi-vision GUI
- Mobile GUI
- Web GUI

Front-End Layer
- Real-time Digital Forensic Service
- e-Discovery Service
- Visualization
- Analysis Automation
- e-Discovery
- Review/Reporting

Data Processing Layer
- Forensic Index
- Data Categorization
- File/Memory Analysis
- PW/Anti-Forensic
- Forensic VFS
- Forensic File Filter
- Multi-source Acquisition
- Online Forensic Data Acquisition
- Attestation

Platform Layer
- Single Platform (Win/Linux)
- Distributed Platform (Cloud/Grid)
- Centralized Repository
Forensic Cloud: Forensics as a Service

Forensic Cloud Technology Framework

Client Layer
- **Mobile Support** ➔ **User Mobility/Connectivity**

Front-End Layer
- **Visualization** ➔ **Intuitive Analysis**

Data Processing Layer
- **Parallel/Distributed Computing** ➔ **Core Function Acceleration**

Platform Layer
- Single Platform (Win/Linux)
- Distributed Platform (Cloud/Grid)
- Centralized Repository

Visual Analytics
- Forensic Cloud Technology Framework
- Real-time Digital Forensic Service
- e-Discovery Service
- Password/Anomaly Detection
- Antiforensic Techniques
- Remote Image Collection
- Online Forensic Data Collection
- System File/Physical Memory Analysis
- Forensic Index/High-Speed Search Techniques
- Multi-Source Data Acquisition/Transformation Techniques
- Mobile Support ➔ User Mobility/Connectivity

Intuitive Analytics
- Visualization ➔ Intuitive Analysis
- Parallel/Distributed Computing ➔ Core Function Acceleration
- Forensic Cloud Technology Framework
- Real-time Digital Forensic Service
- e-Discovery Service
- Password/Anomaly Detection
- Antiforensic Techniques
- Remote Image Collection
- Online Forensic Data Collection
- System File/Physical Memory Analysis
- Forensic Index/High-Speed Search Techniques
- Multi-Source Data Acquisition/Transformation Techniques
- Mobile Support ➔ User Mobility/Connectivity

Accelerate Analysis
- Acceleration ➔ Intuitive Analysis
- Parallel/Distributed Computing ➔ Core Function Acceleration
- Forensic Cloud Technology Framework
- Real-time Digital Forensic Service
- e-Discovery Service
- Password/Anomaly Detection
- Antiforensic Techniques
- Remote Image Collection
- Online Forensic Data Collection
- System File/Physical Memory Analysis
- Forensic Index/High-Speed Search Techniques
- Multi-Source Data Acquisition/Transformation Techniques
- Mobile Support ➔ User Mobility/Connectivity
Forensic Cloud: Forensics as a Service
Forensic Cloud: Forensics as a Service

source: http://en.wikipedia.org/wiki/File:Sun_Modular_Datacenter_SunEBC.JPG