Digital Forensic:
Brief Intro & Research challenge

Aung Thu Rha Hein (g5536871)

4th February 2014
Content

• What is Digital Forensic
• Examples Of DF Cases
• Digital Forensic Branches
• Use of Digital Forensic
• Methodology
• Tools
• Research Challenge
• Future Challenge
• Discussion & Conclusion
Digital Forensic

- preservation, identification, extraction, interpretation & documentation of computer evidence which can be used in the court of law.

- **Goal**: To explain the current state of digital artifact
Examples Of DF Cases

August 6, 2009 DDoS attacks To Social Sites

We had network issues today related to a denial-of-service attack. Service now is restored for most people and we're investigating further.
Examples Of DF Cases/2

- BTK Killer
  - serial killer arrested by investigating letters sent via floppy disk

- David Riley
  - Air Force Major sent images of child pornography over internet
Digital Forensic Branches

➔ Disk Forensic
  ◆ Flash, HDD, USB Device

➔ Network Forensic
  ◆ monitoring and analyzing network traffic

➔ Memory Forensic
  ◆ analysis of system dump

➔ Mobile Forensic
  ◆ acquire deleted or undeleted data

➔ Cloud Forensic
  ◆ forensic network analysis on Cloud computing architecture
Use of Digital Forensic

→ **Criminal Investigations**
  ◆ Child Pornography, identify thief, e-Crimes

→ **Civil Litigation**
  ◆ eDiscovery

→ **Intelligence**
  ◆ Terrorist attacks
Methodology

- Basic Methodology

Acquire Evidence → Authenticate evidence → Analyze Data

Identification Phase → Acquisition of Evidence → Authentication of Evidence → Analysis Phase → Presentation Phase
● 3 standard methodologies & the detailed process varies
  ○ Basic Forensic Methodology
  ○ Cyber Tool Online Search For Evidence (CTOSE)
  ○ Data Recovery UK (DRUK)
● the recommended methodology$^6$ combines the practice from 3 standards
● there are more than dozen DF frameworks

## Taxonomy of DF Methodology

<table>
<thead>
<tr>
<th>No</th>
<th>Digital Forensic Investigation Framework</th>
<th>No of Phases</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Computer Forensic Process (M.Pollitt, 1995)</td>
<td>4 processes</td>
</tr>
<tr>
<td>2</td>
<td>Generic Investigative Process (Palmer, 2001)</td>
<td>7 classes</td>
</tr>
<tr>
<td>3</td>
<td>Abstract Model of the Digital Forensic Procedure (Reith, Carr, &amp; Gunsch, 2002)</td>
<td>9 components</td>
</tr>
<tr>
<td>4</td>
<td>An Integrated Digital Investigation Process (Carrier &amp; Spafford, 2003)</td>
<td>17 phases</td>
</tr>
<tr>
<td>5</td>
<td>End-to-End Digital Investigation (Stephenson, 2003)</td>
<td>9 steps</td>
</tr>
<tr>
<td>6</td>
<td>Enhance Integrated Digital Investigation Process (Baryamureeba &amp; Tushabe, 2004)</td>
<td>21 phases</td>
</tr>
<tr>
<td>7</td>
<td>Extended Model of Cybercrime Investigations (Ciardhuin, 2004)</td>
<td>13 activities</td>
</tr>
<tr>
<td>8</td>
<td>Hierarchical, Objective-based Framework (Beebe &amp; Clark, 2004)</td>
<td>6 phases</td>
</tr>
<tr>
<td>9</td>
<td>Event-based Digital Forensic Investigation Framework (Carrier &amp; Spafford, 2004)</td>
<td>16 phases</td>
</tr>
<tr>
<td>10</td>
<td>Forensic Process (Kent K., Chevalier, Grance, &amp; Dang, 2006)</td>
<td>4 processes</td>
</tr>
<tr>
<td>11</td>
<td>Investigation Framework (Kohn, Eloff, &amp; Oliver, 2006)</td>
<td>3 stages</td>
</tr>
<tr>
<td>12</td>
<td>Computer Forensic Triage Process Model (K.Rogers, Goldman, Mislav, Wedge, &amp; Debrotta, 2006)</td>
<td>4 phases</td>
</tr>
<tr>
<td>13</td>
<td>Investigative Process Model (Freiling &amp; Schwittay, 2007)</td>
<td>4 phases</td>
</tr>
</tbody>
</table>
## Digital Forensic Tools

<table>
<thead>
<tr>
<th>Tools</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forensic Toolkit <strong>AccessData</strong> Group, LLC</td>
<td>Multipurpose tool (acquisition, verification, searching, reporting, wiping, etc.)</td>
</tr>
<tr>
<td>SMART &amp; SMART for Linux <strong>ASR Data, Data Acquisition and Analysis, LLC</strong></td>
<td>Multipurpose tool (acquisition, verification, searching, reporting, wiping, etc.)</td>
</tr>
<tr>
<td><strong>Softblock, Macquisition</strong>, Blacklight BlackBag Technologies, Inc.</td>
<td>Multiple Macintosh forensic tools</td>
</tr>
<tr>
<td><strong>Raptor</strong> Forward Discovery, Inc.</td>
<td>Linux-based acquisition and preview tool</td>
</tr>
</tbody>
</table>
# Research Challenges

- DF research is trending from 1997-2007
- After 2007, Digital forensic meets with many challenges

### Characteristics comparison

<table>
<thead>
<tr>
<th>Era</th>
<th>OS</th>
<th>File Format</th>
<th>Computing Architecture</th>
<th>Storage Architecture</th>
<th>Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1997-2007</strong></td>
<td>Windows Dominance</td>
<td>few file formats</td>
<td>PC, Centralized</td>
<td>standard cable interfaces</td>
<td>commercial tools are working</td>
</tr>
<tr>
<td><strong>2007- recent</strong></td>
<td>increasing OSs</td>
<td>Various file formats</td>
<td>Client/Server, Cloud</td>
<td>Flash, Cloud Storage</td>
<td>can’t catch up with req</td>
</tr>
</tbody>
</table>

**Other Introduced Issues**: Storage Size, pervasive encryption, legal challenges
Research Challenges/2

- **Evidence-oriented design** influences today’s DF research
  - find evidence instead of assisting investigation
  - not think of cyber-crime, i.e tools are not for hacking cases
  - not possible to perform short-time analysis
  - not capable of generating data from residual file

- **Visibility, Filter, Report Model**
  - data recover before making analysis
  - not possible to do parallel processing

- no standard for reverse engineering
- ‘application instead of tools’ concept by vendors
- lost academic research

[2] 2010, Digital forensics research: The next 10 years
Research Challenges/3

- 2013 survey takes part in 4 categories:
  - Demographics, Forensic Capabilities, Future Challenge, Legislative Concerns
- more than 50% of participants: 3 years of DF experience
- Current DF tools & Capabilities:
  - Importance: more than 98% ranks as 4 out of 5
  - Key Limitations: Data Volume, Time, Tool Capability
  - Tool Capability: not clear result
- Technology that least concerns: malware, steganography

<table>
<thead>
<tr>
<th></th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Researchers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cloud Computing</td>
</tr>
<tr>
<td></td>
<td>Encryption = Pace of Technology</td>
</tr>
<tr>
<td>Practitioners</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anti-Forensics</td>
</tr>
<tr>
<td></td>
<td>Encryption</td>
</tr>
<tr>
<td></td>
<td>Cloud Computing</td>
</tr>
<tr>
<td>Overall</td>
<td>Anti-Forensics</td>
</tr>
<tr>
<td></td>
<td>Cloud Computing</td>
</tr>
<tr>
<td></td>
<td>Encryption</td>
</tr>
</tbody>
</table>

[3] 2013, Challenges to Digital Forensic
Future Challenge

- Challenge: Investigation & Analysis Time
- Mobile and Network Forensic will be trending
- Should adopt standards for case data, data abstractions and composable models
- More data abstractions should create
- Should standardise development diversity
- Alternative analysis model: parallel processing, stochastic analysis ...
- Doesn’t work in small-scale dataset
- Standardized test data
Discussion & Conclusion

- The importance of DF
- DF has been in “Golden Age” and it is over
- encounters many research challenges
- needs a clear research plan/agenda

Thank you...
Questions?
References