Digital Forensic Investigations
COS783
Standardising the Digital Forensic Investigation Process: ISO27043

Prof HS Venter
hventer@cs.up.ac.za
Copyright © HS Venter (2015)

Digital Forensic Process

• Digital Evidence
  – Acquisition
  – Preservation
  – Examination
  – Analysis
  – Presentation

• Primary Components
  – High-Tech Issues
  – Legal and Ethical Issues
**Digital Forensic Process Models**

- The digital forensic process model proposed at DFRWS in 2001 included 7 phases:
  1. Identification,
  2. Preservation,
  3. Collection,
  4. Examination,
  5. Analyses,
  6. Presentation,
  7. Decision.

- Reith, Carr, and Gunsch proposed abstract model, which includes 9 phases:
  - 1. Identification,
  - 2. Preparation,
  - 3. Approach strategy,
  - 4. Preservation,
  - 5. Collection,
  - 6. Examination,
  - 7. Analysis,
  - 8. Presentation,
Digital Forensic Process Models

• The U.S. Department of Justice (DOJ) process model with 8 phases:
  1. Preparation,
  2. Recognition and identification,
  3. Documentation of the crime scene,
  4. Collection and preservation,
  5. Packaging and transportation,
  6. Examination,
  7. Analysis,
  8. Reporting.

• Model proposed by Carrier and Spafford includes 17 phases organized into five groups. Five groups proposed are:
  1. Readiness Phases,
  2. Deployment Phases,
  3. Physical Crime Scene Investigation Phases,
  4. Digital Crime Scene Investigation Phases,
  5. Review Phase.
Digital Forensic Process Models • Mandia and Prosise have proposed digital forensic process, known as incident model, containing following phases:
  1. Pre-incident Preparation,
  2. Detection of the Incident,
  3. Initial Response,
  4. Response Strategy Formulation,
  5. Duplication (System backup),
  6. Investigation,
  7. Secure Measure Implementation (Isolation and containing the suspect system),
  8. Network Monitoring,
  9. Recovery (Recovery of the suspect system to original phase),
 10. Reporting,
 11. Follow-up.

Digital Forensic Process Models • First tier phases proposed by Beebe and Clark include 6 phases:
  1. Preparation,
  2. Incident response,
  3. Data collection,
  4. Data analyses,
  5. Findings presentation,
  6. Closure.
Digital Forensic Process Models

- Cuadr Huain proposed 13 phases:
  1. Awareness
  2. Authorization
  3. Planning
  4. Notification
  5. Search for and identify evidence
  6. Collection of evidence
  7. Transport of evidence
  8. Storage of evidence
  9. Examination of evidence
  10. Hypothesis
  11. Presentation of hypothesis
  12. Proof/Defense of hypothesis
  13. Dissemination of information

- Cohen proposed process model that includes 11 phases:
  1. Identification,
  2. Collection,
  3. Preservation,
  4. Transportation,
  5. Storage,
  6. Analysis,
  7. Interpretation,
  8. Attribution
  9. Reconstruction,
  10. Presentation,
  11. Destruction.
ISO/IEC 27043 – need for standardisation

- Disparities in current models
- Acknowledged on international level
- Proposed after ISO/IEC 27037: Guidelines for identification, collection, acquisition, and preservation of digital evidence
- Need for ‘umbrella’ standard
- Covering width, not depth
- Research: Harmonise current process models
- Tested on real-world cases

Harmonisation effort

<table>
<thead>
<tr>
<th>The Harmonised model</th>
<th>DFIRIS (13)</th>
<th>Rappo et al. (14)</th>
<th>BS5014</th>
<th>Carrier et al. (15)</th>
<th>Mandia et al. (16)</th>
<th>Bennett et al. (17)</th>
<th>Cofer (10)</th>
<th>Sequeira (18)</th>
<th>AIPDC (19)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process</td>
<td>1 Incident</td>
<td>1 Identification</td>
<td>2.2 Investigation</td>
<td>3.2.1 Analysis</td>
<td>4.1 Incident</td>
<td>5.1 Response</td>
<td>6.1 Preservation</td>
<td>7.1 - 7.3</td>
<td>8.1 - 8.3</td>
</tr>
<tr>
<td></td>
<td>1 Incident</td>
<td>1 Identification</td>
<td>2.2 Investigation</td>
<td>3.2.1 Analysis</td>
<td>4.1 Incident</td>
<td>5.1 Response</td>
<td>6.1 Preservation</td>
<td>7.1 - 7.3</td>
<td>8.1 - 8.3</td>
</tr>
<tr>
<td></td>
<td>1 Incident</td>
<td>1 Identification</td>
<td>2.2 Investigation</td>
<td>3.2.1 Analysis</td>
<td>4.1 Incident</td>
<td>5.1 Response</td>
<td>6.1 Preservation</td>
<td>7.1 - 7.3</td>
<td>8.1 - 8.3</td>
</tr>
<tr>
<td></td>
<td>1 Incident</td>
<td>1 Identification</td>
<td>2.2 Investigation</td>
<td>3.2.1 Analysis</td>
<td>4.1 Incident</td>
<td>5.1 Response</td>
<td>6.1 Preservation</td>
<td>7.1 - 7.3</td>
<td>8.1 - 8.3</td>
</tr>
<tr>
<td></td>
<td>1 Incident</td>
<td>1 Identification</td>
<td>2.2 Investigation</td>
<td>3.2.1 Analysis</td>
<td>4.1 Incident</td>
<td>5.1 Response</td>
<td>6.1 Preservation</td>
<td>7.1 - 7.3</td>
<td>8.1 - 8.3</td>
</tr>
<tr>
<td></td>
<td>1 Incident</td>
<td>1 Identification</td>
<td>2.2 Investigation</td>
<td>3.2.1 Analysis</td>
<td>4.1 Incident</td>
<td>5.1 Response</td>
<td>6.1 Preservation</td>
<td>7.1 - 7.3</td>
<td>8.1 - 8.3</td>
</tr>
<tr>
<td></td>
<td>1 Incident</td>
<td>1 Identification</td>
<td>2.2 Investigation</td>
<td>3.2.1 Analysis</td>
<td>4.1 Incident</td>
<td>5.1 Response</td>
<td>6.1 Preservation</td>
<td>7.1 - 7.3</td>
<td>8.1 - 8.3</td>
</tr>
<tr>
<td></td>
<td>1 Incident</td>
<td>1 Identification</td>
<td>2.2 Investigation</td>
<td>3.2.1 Analysis</td>
<td>4.1 Incident</td>
<td>5.1 Response</td>
<td>6.1 Preservation</td>
<td>7.1 - 7.3</td>
<td>8.1 - 8.3</td>
</tr>
<tr>
<td></td>
<td>1 Incident</td>
<td>1 Identification</td>
<td>2.2 Investigation</td>
<td>3.2.1 Analysis</td>
<td>4.1 Incident</td>
<td>5.1 Response</td>
<td>6.1 Preservation</td>
<td>7.1 - 7.3</td>
<td>8.1 - 8.3</td>
</tr>
<tr>
<td></td>
<td>1 Incident</td>
<td>1 Identification</td>
<td>2.2 Investigation</td>
<td>3.2.1 Analysis</td>
<td>4.1 Incident</td>
<td>5.1 Response</td>
<td>6.1 Preservation</td>
<td>7.1 - 7.3</td>
<td>8.1 - 8.3</td>
</tr>
</tbody>
</table>

8/13/2015 8/13/2015
ISO/IEC 27043 roadmap

- October 2010 (Berlin, Germany): Proposal
- April 2011 (Singapore): SP
- October 2011 (Stockholm, Sweden): WD1
- April 2012 (Nairobi, Kenya): WD2
- October 2012 (Rome, Italy): CD1
- April 2013 (Sophia Antipolis, France): CD2
- October 2013 (Incheon, Korea): DIS
- April 2015 (Hong Kong): FDIS
- October 2015 (Mexico): IS
- March 2015: published

ISO/IEC 27043

- Incident investigation principles and processes
- Why not “[Digital] [forensic] investigation principles and [process]”? 
- Digital: should also include the physical investigation
- Forensic: has a legal connotation; standard should not promote legal issues
- Principles: ‘umbrella’ standard – include general principles as well 
- Processes: Defined in another ISO standard
Classes of processes

• Novel contribution:
  – Readiness processes class
  – Concurrent processes class

• Harmonisation of current process models
  – Initialisation processes class
  – Acquisitive processes class
  – Investigative processes class
Readiness processes

Planning processes group

Implementation processes group

Assessment processes group

Input to the rest of the digital investigation (to the incident detection process within the initialization processes class in Figure 5)

CONCURRENT PROCESSES

Planning processes group

Scenario definition

Identification of potential digital evidence sources

Planning pre-incident collection, storage and handling of data representing potential digital evidence

Planning pre-incident analysis of data representing potential digital evidence

Defining system architecture

Defining incident analysis
Readiness processes

- Planning processes group
- Implementation processes group
- Assessment processes group

Input to the rest of the digital investigation (to the incident detection process within the initialization processes class in Figure 5)
Readiness processes

Input to the rest of the digital investigation (to the incident detection process within the initialization processes class in Figure 5)

Plan processes group

Implementation processes group

Assessment processes group

Implementing pre-incident analysis of data representing potential digital evidence

Implementing incident detection

Assessment of implementation

Changes needed?

yes

no

Implementation of assessment results

8/13/2015
Readiness processes
**Initialisation processes**

- Concurrent processes class
- Readiness processes class
  - Initialization processes class
- Acquisitive processes class
- Investigative processes class

---

**Acquisitive processes**

- Concurrent processes class
- Readiness processes class
  - Initialization processes class
- Acquisitive processes class
- Investigative processes class
Investigative processes

Concurrent processes class

Readiness processes class

Initialization processes class

Acquisitive processes class

Investigative processes class

Investigative processes

Concurrent processes

Investigative processes

Input from acquisitive processes in Figure 6

Optional process iteration to Figure 6

Potential digital evidence acquisition

Digital evidence management and analysis

Investigation closure

Reporting

Presentation
Applicability to other standards
Conclusion

• Harmonisation effort
• ISO/IEC 27043 is an ‘umbrella standard'
• Many other standards involved
• Will discuss these in the next lecture