Digital Forensics I: Research problem and roadmap, the next 10 years

Kevin Weaver

September 16th, 2011

Outline

1. Introduction
2. History
   a. 40 Years
3. DFRWS 1
   a. Overview
   b. Speeches
   c. Workshop Discussions
4. The next 10 years
   a. End of a Golden Age?
   b. Challenges ahead
   c. Solutions
5. Conclusion
   a. Similarities
   b. A True Golden Age

Topics for discussion

1. Brief History of Digital Forensics
2. DFRWS 2001 Roadmap
3. Then and Now: What's different and what's changed?
4. Digital forensics research: The next 10 years
5. Conclusion
“Digital forensics” was originally simply data recovery.

- Diversity, in the bad way
- Bad documentation for lots of file types
- Centralized computing facilities, and time-sharing
- No formal tools, training, education


Lasted from 1997-2007


Lasted from 1997-2007

Outline
- Introduction
- History
  - 40 Years
- DFRWS 1
  - Overview
  - Speeches
  - Workshop Discussions
- The next 10 years
  - End of a Golden Age?
  - Challenges ahead
  - Solutions
- Conclusion
  - Similarities
  - A True Golden Age
**Why was it started?**

**Organizational Objectives**
- Initiate Digital Forensics community
- Promote scholarly discussion about Digital Forensics
- Get veterans from law enforcement, military and civilian sectors
- Build foundation for focus of useful research
- Standardize the language used
- Make an excuse to keep talking about Digital Forensics

**Speaker and Topics**
- Dr. Eugene Spafford, Big Computer Forensic Challenges
- Charles Boeckman, A Defensive Info Ops Perspective on Forensic Analysis Requirements
- Chet Hosmer, Digital Forensic Technologies: Are we Overlooking Key Fundamentals?
- David Baker, Digital Forensics
- Dr. John Hoyt, Electronic Crime Technology Program: NIJ/OSnT

**Big Computer Forensic Challenges**

The problems we should be fixing are:
- Technological
- Procedural
- Social
- Legal

**Defensive Info Ops Perspective on Forensic Analysis Requirements**

- Assess **impact** of system compromise
- Assess **scope** of system compromise
- Assess **intelligence value** of collected data
- Perform **Battle Damage Assessment**
Activity concentration

Digital forensics for Defensive purposes is special:

Accuracy must be sacrificed for speed, ensure that missions and mission-critical data can stay within the mission deadline

- Optimize data collection
- Minimize risk of corruption or destruction
- Accommodate operational time constraints

We must be able to analyze active systems.

Digital Forensic Technologies: Are we Overlooking Key Fundamentals?

We have to ask two kinds of questions:

- What are the fundament truths of this thing we call digital evidence?
- What characteristics must be evident across the board for things we deem to be cyberforensic technologies?

Digital Evidence

Questions

- How can we define ownership of data?
- Can digital data provide clues to motive of a crime or incident?
- How do we expand our digital forensic view from disk to network?
- We have to profile, identify, trace and apprehend cybersuspects, but can digital forensics answer who?, or what?, or why? Where? When?
- Are there cyberwitnesses to a cybercrime?

Technologies

We want out of our cybertechnology what we want out of all technology:

- Reliability
- Precision
- Accuracy
- Non-repudiation
- Security
- Flexibility
- Value

But where are the standards? Were the developers certified?

How is digital evidence integrity assured?

Digital Forensics

Ubiquity of technology Even "mundane" crimes have a cyberdimension Critical civilian infrastructure is vulnerable

Move out of after-the-fact mentality
Cybercriminals are adept, determined and isolated: hard to catch outside of the cybersphere.
Detection and Recovery of Hidden Data

Objective
Finding cybercriminals, automating the process of finding them and their data, is of paramount importance.

Research areas
- Categorization
- Detection
- Recovery

Definition of Network Forensics

Objective
Can (and should) digital forensics be applied to live networks? Yes. Makes it a new branch of DFS that requires its own identification and definition.

Research areas
- Definition
- Performance
- Paradigm Distinctions

Outline
- Introduction
- History
- 40 Years
- DFRWS 1
  - Overview
  - Speeches
  - Workshop Discussions
- The next 10 years
  - End of a Golden Age?
  - Challenges ahead
  - Solutions
- Conclusion
  - Similarities
  - A True Golden Age
<table>
<thead>
<tr>
<th>Outline</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Introduction</strong></td>
</tr>
<tr>
<td><strong>History</strong></td>
</tr>
<tr>
<td>40 Years</td>
</tr>
<tr>
<td><strong>DFRWS 1</strong></td>
</tr>
<tr>
<td>Overview</td>
</tr>
<tr>
<td>Speeches</td>
</tr>
<tr>
<td>Workshop Discussions</td>
</tr>
<tr>
<td><strong>The next 10 years</strong></td>
</tr>
<tr>
<td>End of a Golden Age?</td>
</tr>
<tr>
<td>Challenges ahead</td>
</tr>
<tr>
<td>Solutions</td>
</tr>
<tr>
<td><strong>Conclusion</strong></td>
</tr>
<tr>
<td>Similarities</td>
</tr>
<tr>
<td>A True Golden Age</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>There was a Golden Age?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP</td>
</tr>
<tr>
<td>Lack of filetype diversity</td>
</tr>
<tr>
<td>Small-scale investigations</td>
</tr>
<tr>
<td>Standardized hardware</td>
</tr>
<tr>
<td>Decent recovery tools</td>
</tr>
<tr>
<td>Academic and research boom</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>And now it’s ending?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slower analysis</td>
</tr>
<tr>
<td>Great diversity</td>
</tr>
<tr>
<td>Multiple analyses</td>
</tr>
<tr>
<td>Encryption</td>
</tr>
<tr>
<td>Cloud computing</td>
</tr>
<tr>
<td>Hidden malware</td>
</tr>
<tr>
<td>Legal trouble</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Problems with today’s models</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evidence-oriented design creates tools that are:</td>
</tr>
<tr>
<td>Designed for finding evidence, not assisting in investigations</td>
</tr>
<tr>
<td>Designed to find evidence of crimes where the evidence is a crime itself</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reverse Engineering, Monolithic Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RE</strong></td>
</tr>
<tr>
<td>Lack of standards, lack of automation. Each project becomes stand-alone, can’t save or exchange data for use in other projects</td>
</tr>
<tr>
<td><strong>All-in-one Apps</strong></td>
</tr>
<tr>
<td>Developers, companies release packaged, bundled software and tools</td>
</tr>
</tbody>
</table>
Lack of Communication

Lots of academic activity, but everybody’s keeping to themselves:
- Open-source tools
- License tech to a vendor
- Vendors read the papers

Forensic data abstraction

Garfinkel suggests these additions:
- Signature metrics
- File metadata
- File system metadata
- Application profiles
- User profiles
- Internet and social network info

Platforms

Forensic software developed in several languages: Java, Perl, C/C++, Python to name a few. Other disciplines put out platforms to handle this issue: Apache, Eclipse, .NET

Alternative models

Currently using the “Visibility, Filter and Report” model. Make a platform with this first, but try to move on:
- Stream-based disk forensics
- Stochastic analysis
- Prioritized analysis

Large-scale research

Research isn’t being done on a large enough scale. Many fail when given very large data sets. Techniques don’t work when run in data-rich environments. Need to increase scale of testing during research.
Further abstraction

After getting used to new abstraction techniques, can start abstracting even further, developing new forensic techniques, tools and procedures.

- Identity Management
- Data visualization and advanced user interfaces
- Visual analytics
- Collaboration
- Autonomous operation

Outline

Introduction
- History
  - 40 Years
- DFRWS 1
  - Overview
  - Speeches
  - Workshop Discussions
- The next 10 years
  - End of a Golden Age?
  - Challenges ahead
  - Solutions
- Conclusion
  - Similarities
  - A True Golden Age

Similarities

All of the papers I read indicated the same thing: the forensics community is currently too disconnected and needs to focus on a unified forensic definition. Both gave suggestions about what that focus should be, too. In the case of the first paper, there were many suggestions about a variety of topics.

A sense of adventure

Garfinkel’s paper was a little bit exagerrated and whiny (Personal take). Necessity is the mother of invention. Easy doesn’t mean good.
References

- "Digital Forensics Research: The next 10 years", Simson L. Garfinkel
- "Effective Digital Forensics Research is Investigator-Centric", Robert Walls, Brian Levine, Marc Liberatore, Clay Shields