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

Kevin Weaver

September 16th, 2011
# Outline

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

1. Brief History of Digital Forensics
Topics for discussion

1. Brief History of Digital Forensics
2. DFRWS 2001 Roadmap
Topics for discussion

1. Brief History of Digital Forensics
2. DFRWS 2001 Roadmap
3. Then and Now: What’s different and what’s changed?
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
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
1. Introduction

2. History
   - 40 Years

3. DFRWS 1
   - Overview
   - Speeches
   - Workshop Discussions

4. The next 10 years
   - End of a Golden Age?
   - Challenges ahead
   - Solutions

5. Conclusion
   - Similarities
   - A True Golden Age
Outline

1. Introduction
2. History
   - 40 Years
3. DFRWS 1
   - Overview
   - Speeches
   - Workshop Discussions
4. The next 10 years
   - End of a Golden Age?
   - Challenges ahead
   - Solutions
5. Conclusion
   - Similarities
   - A True Golden Age
"Digital forensics" was originally simply data recovery.
Hallmarks of the Past

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


Lasted from 1997-2007
Outline

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

Organizational Objectives

- Initiate Digital Forensics community
Why was it started?

Organizational Objectives

- Initiate Digital Forensics community
- Promote scholarly discussion about Digital Forensics
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
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
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
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
Workshop Format

- First, speakers
- Second, roundtable discussions
- Lastly, presentations
Outline

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

1. Dr. Eugene Spafford, Big Computer Forensic Challenges
Speakers and Topics

1. Dr. Eugene Spafford, Big Computer Forensic Challenges
2. Charles Boeckman, A Defensive Info Ops Perspective on Forensic Analysis Requirements
Speakers and Topics

1. Dr. Eugene Spafford, Big Computer Forensic Challenges
2. Charles Boeckman, A Defensive Info Ops Perspective on Forensic Analysis Requirements
3. Chet Hosmer, Digital Forensic Technologies: Are we Overlooking Key Fundamentals?
Speakers and Topics

1. Dr. Eugene Spafford, Big Computer Forensic Challenges
2. Charles Boeckman, A Defensive Info Ops Perspective on Forensic Analysis Requirements
3. Chet Hosmer, Digital Forensic Technologies: Are we Overlooking Key Fundamentals?
4. David Baker, Digital Forensics
<table>
<thead>
<tr>
<th></th>
<th>Speakers and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Dr. Eugene Spafford, Big Computer Forensic Challenges</td>
</tr>
<tr>
<td>2</td>
<td>Charles Boeckman, A Defensive Info Ops Perspective on Forensic Analysis Requirements</td>
</tr>
<tr>
<td>3</td>
<td>Chet Hosmer, Digital Forensic Technologies: Are we Overlooking Key Fundamentals?</td>
</tr>
<tr>
<td>4</td>
<td>David Baker, Digital Forensics</td>
</tr>
<tr>
<td>5</td>
<td>Dr. John Hoyt, Electronic Crime Technology Program: NIJ/OSnT</td>
</tr>
</tbody>
</table>
Big Computer Forensic Challenges

The problems we should be fixing are:

- Technological
Big Computer Forensic Challenges

The problems we should be fixing are:

- Technological
- Procedural
Big Computer Forensic Challenges

The problems we should be fixing are:

- Technological
- Procedural
- Social
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
Defensive Info Ops Perspective on Forensic Analysis Requirements

- Assess **impact** of system compromise
- Assess **scope** of system compromise
Defensive Info Ops Perspective on Forensic Analysis Requirements

- Assess **impact** of system compromise
- Assess **scope** of system compromise
- Assess **intelligence value** of collected data
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 fundamental truths of this thing we call **digital evidence**?
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?
Questions

- How can we define ownership of data?
Questions

- How can we define ownership of data?
- Can digital data provide clues to motive of a crime or incident?
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?
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?
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 cyber suspects, but can digital forensics answer who?, or what?, or why? Where? When?
- Are there cyberwitnesses to a cybercrime?
We want out of our cyber technology what we want out of all technology:
We want out of our cyber technology what we want out of all technology:

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

We want out of our cyber-technology 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

Technology

Ubiquity of technology

Even "mundane" crimes have a cyber dimension

Critical civilian infrastructure is vulnerable

Move out of after-the-fact mentality
Digital Forensics

Technology

Ubiquity of technology
Ubiquity of technology Even "mundane" crimes have a cyberdimension
Digital Forensics

Technology

Ubiquity of technology Even "mundane" crimes have a cyberdimension Critical civilian infrastructure is vulnerable
Ubiquity of technology Even "mundane" crimes have a *cyber*dimension Critical civilian infrastructure is vulnerable Move out of after-the-fact mentality
Electronic Crime Technology Program: NIJ/OSnT

National Institute of Justice, Office of Science and Technology
Electronic Crime Technology Program: NIJ/OSnT

National Institute of Justice, Office of Science and Technology

- Tools and technology development
- Technical assistance
- Standards, certification and training
- Policy and legal issues
- Outreach and education

Cyercriminals are adept, determined and isolated: hard to catch outside of the cybersphere.
Foundations
- Framework for Digital Forensic Science
- Trustworthiness of Digital Evidence
- Definition of Network Forensics

Challenges
- Detection and Recovery of Hidden Data
Framework for Digital Forensic Science

Objective
Help research area become an effective and useful lexicon containing clear definitions and terminology.
Framework for Digital Forensic Science

Objective

Help research area become an effective and useful lexicon containing clear definitions and terminology.

Research areas

- Definition
Framework for Digital Forensic Science

<table>
<thead>
<tr>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help research area become an effective and useful lexicon containing clear definitions and terminology.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Research areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Definition</td>
</tr>
<tr>
<td>• Process</td>
</tr>
</tbody>
</table>
Framework for Digital Forensic Science

Objective
Help research area become an effective and useful lexicon containing clear definitions and terminology.

Research areas
- Definition
- Process
- Expertise
Timeline

- 2001: DIP
- 2002: Definition
- 2003: Expertise
Trustworthiness of Digital Evidence

Objective

Find and eliminate those aspects of digital technology that makes people distrust investigations. Specifically law- and policymakers. Be able to explain exactly what happens from raw bits to visual display. Assure those who ask that the integrity of the information is unquestioned.
Trustworthiness of Digital Evidence

Objective
Find and eliminate those aspects of digital technology that makes people distrust investigations. Specifically law- and policymakers. Be able to explain exactly what happens from raw bits to visual display. Assure those who ask that the integrity of the information is unquestioned.

Research areas
- Anti-tampering
Trustworthiness of Digital Evidence

Objective

Find and eliminate those aspects of digital technology that makes people distrust investigations. Specifically law- and policymakers. Be able to explain exactly what happens from raw bits to visual display. Assure those who ask that the integrity of the information is unquestioned.

Research areas

- Anti-tampering
- Correctness
Trustworthiness of Digital Evidence

Objective

Find and eliminate those aspects of digital technology that makes people distrust investigations. Specifically law- and policymakers. Be able to explain exactly what happens from raw bits to visual display. Assure those who ask that the integrity of the information is unquestioned.

Research areas

- Anti-tampering
- Correctness
- Procedure
Detection and Recovery of Hidden Data

Objective

Finding *cyber*criminals, automating the process of finding them and their data, is of paramount importance.
Detection and Recovery of Hidden Data

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

Research areas
- Categorization
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
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
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
Timeline
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
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
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
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
1. Introduction

2. History
   - 40 Years

3. DFRWS 1
   - Overview
   - Speeches
   - Workshop Discussions

4. The next 10 years
   - End of a Golden Age?
   - Challenges ahead
   - Solutions

5. Conclusion
   - Similarities
   - A True Golden Age
There was a Golden Age?

- Windows XP
There was a Golden Age?

- Windows XP
- Lack of filetype diversity
There was a Golden Age?

- Windows XP
- Lack of filetype diversity
- Small-scale investigations
There was a Golden Age?

- Windows XP
- Lack of filetype diversity
- Small-scale investigations
- Standardized hardware
There was a Golden Age?

- Windows XP
- Lack of filetype diversity
- Small-scale investigations
- Standardized hardware
- Decent recovery tools
There was a Golden Age?

- Windows XP
- Lack of filetype diversity
- Small-scale investigations
- Standardized hardware
- Decent recovery tools
- Academic and research boom
And now it’s ending?

- Slower analysis
And now it’s ending?

- Slower analysis
- Great diversity
And now it’s ending?

- Slower analysis
- Great diversity
- Multiple analyses
And now it’s ending?

- Slower analysis
- Great diversity
- Multiple analyses
- Encryption
And now it’s ending?

- Slower analysis
- Great diversity
- Multiple analyses
- Encryption
- Cloud computing
And now it’s ending?

- Slower analysis
- Great diversity
- Multiple analyses
- Encryption
- Cloud computing
- Hidden malware
And now it’s ending?

- Slower analysis
- Great diversity
- Multiple analyses
- Encryption
- Cloud computing
- Hidden malware
- Legal trouble
Outline

1. Introduction
2. History
   - 40 Years
3. DFRWS 1
   - Overview
   - Speeches
   - Workshop Discussions
4. The next 10 years
   - End of a Golden Age?
   - Challenges ahead
   - Solutions
5. Conclusion
   - Similarities
   - A True Golden Age
Problems with today’s models

Evidence-oriented design creates tools that are:

- Designed for finding evidence, not assisting in investigations
Problems with today’s models

Evidence-oriented design creates tools that are:

- Designed for finding evidence, not assisting in investigations
- Designed to find evidence of crimes where the evidence is a crime itself
Reverse Engineering, Monolithic Applications

RE
Lack of standards, lack of automation. Each project becomes stand-alone, can’t save or exchange data for use in other projects.
Reverse Engineering, Monolithic Applications

RE
Lack of standards, lack of automation. Each project
becomes stand-alone, can’t save or exchange data for
use in other projects

All-in-one Apps
Developers, companies release packaged, bundled
software and tools
Lack of Communication

Lots of academic activity, but everybody’s keeping to themselves:

- Open-source tools
Lack of Communication

Lots of academic activity, but everybody’s keeping to themselves:

- Open-source tools
- License tech to a vendor
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
Outline

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

Not enough abstraction types
Currently, we have:

- Disk images
Forensic data abstraction

Not enough abstraction types
Currently, we have:
- Disk images
- Packet capture files

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

Not enough abstraction types
Currently, we have:

- Disk images
- Packet capture files
- Files
Forensic data abstraction

Not enough abstraction types
Currently, we have:

- Disk images
- Packet capture files
- Files
- File signatures
Forensic data abstraction

Not enough abstraction types
Currently, we have:

- Disk images
- Packet capture files
- Files
- File signatures
- Extracted name entities
Forensic data abstraction

Not enough abstraction types
Currently, we have:
- Disk images
- Packet capture files
- Files
- File signatures
- Extracted name entities

Garfinkel suggests these additions:
- Signature metrics
Forensic data abstraction

Not enough abstraction types
Currently, we have:
- Disk images
- Packet capture files
- Files
- File signatures
- Extracted name entities

Garfinkel suggests these additions:
- Signature metrics
- File metadata
Forensic data abstraction

Not enough abstraction types
Currently, we have:
- Disk images
- Packet capture files
- Files
- File signatures
- Extracted name entities

Garfinkel suggests these additions:
- Signature metrics
- File metadata
- File system metadata
Forensic data abstraction

Not enough abstraction types

Currently, we have:

- Disk images
- Packet capture files
- Files
- File signatures
- Extracted name entities

Garfinkel suggests these additions:

- Signature metrics
- File metadata
- File system metadata
- Application profiles
Forensic data abstraction

Not enough abstraction types
Currently, we have:
- Disk images
- Packet capture files
- Files
- File signatures
- Extracted name entities

Garfinkel suggests these additions:
- Signature metrics
- File metadata
- File system metadata
- Application profiles
- User profiles
Forensic data abstraction

Not enough abstraction types
Currently, we have:
- Disk images
- Packet capture files
- Files
- File signatures
- Extracted name entities

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.
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
Currently using the "Visibility, Filter and Report" model. Make a platform with this first, but try to move on:

- Stream-based disk forensics
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
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
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
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
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
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

1. Introduction

2. History
   - 40 Years

3. DFRWS 1
   - Overview
   - Speeches
   - Workshop Discussions

4. The next 10 years
   - End of a Golden Age?
   - Challenges ahead
   - Solutions

5. Conclusion
   - Similarities
   - A True Golden Age
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.
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.
Outline

1. Introduction

2. History
   - 40 Years

3. DFRWS 1
   - Overview
   - Speeches
   - Workshop Discussions

4. The next 10 years
   - End of a Golden Age?
   - Challenges ahead
   - Solutions

5. Conclusion
   - Similarities
   - A True Golden Age
A sense of adventure

Garfinkel’s paper was a little bit exaggerated and whiny (Personal take).
A sense of adventure

Garfinkel’s paper was a little bit exaggerated and whiny (Personal take). Necessity is the mother of invention.
Garfinkel’s paper was a little bit exaggerated 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