An Event-Based Digital Forensic Investigation Framework

By

Brian Carrier, Eugene Spafford

Presented At

The Digital Forensic Research Conference

DFRWS 2004 USA  Baltimore, MD (Aug 11th - 13th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http://dfrws.org
An Event-based Digital Forensic Investigation Framework

Brian D. Carrier
Eugene H. Spafford

DFRWS 2004
Outline

- Basic concepts
- The big picture of investigations
- Digital crime scene investigation
- Summary
Digital Data & Objects

• **Digital data**: Data represented in a numerical form

• **Digital object**: A discrete collection of digital data

• All digital data has a physical form
  – Magnetic Fields
  – Voltage Levels
States & Events

• **State:** The value of an object’s characteristics

• **Event:** An occurrence that changes the state of one or more objects
  – Cause: An object whose state was used by the event
  – Effect: An object whose state was changed by an event
Basic Event: Appending a File

Causes
- notepad
- file1.txt
- OS

Effects
- file1.txt

E
Incidents & Investigations

• **Incident/Crime**: An event that violates a policy or law

• **Investigation**: A process that develops and tests hypotheses to answer questions about events that occurred
Evidence

• There is evidence of an event if the effect objects still exist

• **Digital Evidence**: A digital object that contains reliable information that supports or refutes a hypothesis about the incident
  – A hard disk is physical evidence
What about “Forensics”?

• “Relating to the use of science or technology in the investigation and establishment of facts or evidence in a court of law”
  – American Heritage Dictionary

• Digital Investigation vs. Digital Forensic Investigation: The legal requirements
Digital Forensic Investigation

A process that uses science and technology to examine digital objects and that develops and tests theories, which can be entered into a court of law, to answer questions about events that occurred.
The Big Picture
Digital Crime
Scene Investigation
Digital Crime Scene Investigation

• Goal: To determine what digital events occurred by recognizing digital evidence

• Three Phases:
  – Crime Scene Preservation & Documentation
  – Evidence Search & Documentation
  – Event Reconstruction & Documentation
Phase 1: Digital Crime Scene Preservation & Documentation
Scene Preservation & Documentation

- **Goal:** Preserve the state of as many digital objects as possible and document the crime scene.

- **Methods:**
  - Shut system down and copy it
  - Unplug from network & kill processes
  - Do nothing
Is it Necessary?

- An investigation does not need preservation
- A forensic investigation may need preservation
- Are bitwise-images needed?
  - Do we take buildings as evidence?
- Legal requirements dictate the technical requirements of this phase
Phase 2:
Digital Evidence Searching and Documentation
Evidence Searching & Doc

• Need to find evidence of events
• Goal: To recognize the digital objects that may contain information about the incident and document them.
Existing Research (1)

- Target definition
  - Stallard & Levitt - *Automated Analysis for Digital Forensic Science: Semantic Integrity Checking*
  - Carrier & Spafford - *Defining Searches of Digital Crime Scenes*
  - Manually - experience and training
  - Stego & malware signatures
  - Many others....
Existing Research (2)

• Extraction
  – All current “forensic” tools
  – Carrier - *Defining Digital Forensic Examination and Analysis Tools*

• Comparison
  – Visual (most tools)
  – Equality (keyword searching)
Phase 3:
Digital Event Reconstruction and Documentation
Event Reconstruction

- Need to translate evidence into events
- Goal: To determine and document the events for which evidence exists and has been collected
- Not currently supported by many tools
Evidence Examination

Role Classification

(A) \( X \)

(B) \( X \)

\( E_i \)

\( X' \)

\( Z \)

\( E_i \)

\( Y \)

\( E_j \)

\( B \)

\( W \)

\( E_m \)

\( Z \)

\( E_n \)

\( W \)

\( Y \)

\( E_k \)

\( B \)

\( D \)
Event Construction  Event Sequencing

(A)  (B)

X  X'  X'  X

Y  E_1  E_1  E_1

Z  E_2  W  W

W  W'
Existing Research

- Carney & Rogers - *The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction* - IJDE
- Carrier & Spafford - *Defining Digital Crime Scene Event Reconstruction* - JFS
- Gladyshev & Patel - *Finite State Machine Approach to Digital Event Reconstruction* - JDI
- Stephenson - *Modeling of Post-Incident Root Cause Analysis* - IJDE
Conclusion

• High-level phases based on investigation goals:
  – Digital Crime Scene Preservation
  – Digital Evidence Search
  – Digital Event Reconstruction

• Similar to physical crime scene investigation