Evidence

CIS8630 Business Computer Forensics and Incident Response
Richard Baskerville

Agenda

- About Evidence
- Forensics Methodology
- Federal Rules of Civil Procedure
- Document Retention
About Evidence

Motivation: Incident Evidence

- Admissible evidence for policy enforcement, civil procedure, criminal prosecution or defense
- Managerial evidence for designing corrective actions, future policies, systems, etc.
  - Evidence-based Management
  - Evidence related to the incident
  - Evidence related to other relevant incidents
Locard’s Exchange Principle (1920)

- A criminal and a crime scene exchange physical information: the criminal’s presence leaves traces of evidence, and criminals carry traces of evidence away.
  - Edmund Locard (first forensic lab in Lyons)

Evidence Quality

- Admissible
- Authentic (related to the incident)
- Complete (cannot be selective)
- Reliable (has integrity & chain of custody)
- Believable (relevant & understandable)
Evidence-Collection

- Reactive evidence collection
  - Incident has happened, and that someone wants to know more about that occurrence

- Pro-Active evidence collection
  - Monitoring setting for expected incident
  - Admissibility issues for entrapment (honeypots)

Forensics Methodology
Forensics Methodology

<table>
<thead>
<tr>
<th>Functions</th>
<th>Identification</th>
<th>Response Design</th>
<th>Preservation</th>
<th>Collection</th>
<th>Examination</th>
<th>Analysis</th>
<th>Presentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Goals</td>
<td>Recognizing an incident from indicators and determining its type</td>
<td>Prepare and design approach</td>
<td>Isolate, secure and preserve the state of physical and digital evidence</td>
<td>Record the physical scene and duplicate digital evidence</td>
<td>Search, location, and identification of relevant evidence</td>
<td>Determine significance, reconstruct fragments of data and draw conclusions</td>
<td>Summarize and provide explanation of conclusions</td>
</tr>
<tr>
<td>Tasks</td>
<td>• Profile detection • Anomalous detection • Complaints • Audit analysis • System monitoring</td>
<td>• Prepare tools • Search warrants</td>
<td>• Case management • Chain of custody</td>
<td>• Imaging • Lossless compression • Sampling • Data recovery</td>
<td>• Filtering • Pattern matching • Hidden data discovery • Hidden data extraction</td>
<td>• Statistical • Protocols • Data Mining</td>
<td>• Documentation • Expert testimony • Interpretation • Clarification • Recommendations</td>
</tr>
<tr>
<td>Constraints</td>
<td>Impact on victims &amp; bystanders</td>
<td>Legal authority, Traceability</td>
<td>Legal authority, Traceability</td>
<td>Legal authority, Traceability</td>
<td>Legal authority, Traceability</td>
<td>Legal authority, Traceability</td>
<td></td>
</tr>
</tbody>
</table>

Adapted from Mark M. Pollitt “Six blind men from Indostan”, Keynote Address: DFRWS 2004 Program and Proceedings

Identification

- Determining an incident has occurred
- Classifying the incident
- Determining possible sources of evidence
Response Design

- Assemble resources (capable people & tools)
- Obtain/ensure authorization
- Law enforcement requires search warrants
- Corporations cannot violate privacy
  - E.g., searching personal property of employees
  - E.g., unauthorized downloading of personal data

Preservation

- Freezing the scene: Snapshot
- Remove external avenues of change
  - Pull the plug? Prevents self-destruct scripts.
  - Normal shut down? Writes buffers to disks.
  - Live image? Yes, if full disk encryption is open.
- Making photographs, notes, etc.
  - Photograph screen before powering down
- Establishing chain of custody

(Adapted from Colin Armstrong (2005), CF601 Notes, Curtin University)
Collection

- Use accepted methods and practices
- Collect everything first time
- Document everything
- Follow an order of volatility
  - Minimize lost/corrupted data
- Seizing media, devices, logs, etc.
  - Corporate quick-and-dirty imaging?
- Network-based collection and imaging

(Adapted from Colin Armstrong (2005), CF601 Notes, Curtin University)

Examination

- Contamination control
  - Never work on originals
  - Use isolated examination workstations
    - (Virus Contaminated Evidence)
- Maintain chain of custody
- Searching captured material for relevant evidence
- Requires knowledge of purpose (incident)
  - No pointless rummaging

(Adapted from Colin Armstrong (2005), CF601 Notes, Curtin University)
Analysis

- Collate, group and classify evidence
- Use graphics, spreadsheets, etc.
- Reconstruct the incident

(Adapted from Colin Armstrong (2005), CF601 Notes, Curtin University)

Presentation

- Written Report
  - Can be in electronic form
  - Can include DVD, CDs, etc.
- Testimony
  - Depositions
  - Courtroom
Federal Rules of Criminal Procedure

Federal Rules of Civil Procedure

(If not covered in previous session)

- Rule 16: Pretrial Conferences; Scheduling; Management.
- Rule 26: General Provisions Governing Discovery; Duty of Disclosure.
- Rule 34: Production of Documents, Electronically Stored Information, and Things and
- Rule 37: Failure to Make Disclosures or Cooperate in Discovery; Sanctions.
Rule 16: Pretrial Conferences; Scheduling; Management.

- Comment: the judge shall enter a scheduling order that limits the time to file motions and complete discovery, etc. The scheduling order includes provisions for disclosure or discovery of electronically stored information, agreements among the parties for privilege or protection, and the dates for conferences before trial.
- Rule 16 alerts the court to needs for discovery of electronically stored information early in the litigation.

Rule 26: General Provisions Governing Discovery; Duty of Disclosure.

- Comment: A responding party should produce electronically stored information that is relevant, not privileged, and reasonably accessible. The responding party must also identify, by category or type, the sources containing potentially responsive information that it is neither searching nor producing. The identification should provide enough detail to enable the requesting party to evaluate the burdens and costs of providing the discovery and the likelihood of finding responsive information on the identified sources.
Rule 34: Production of Documents, Electronically Stored Information, Tangible Things or Entry Upon Land for Inspection

- Comment: Any party may serve on any other party a request to produce any electronically stored information which are in the possession of the party upon whom the request is served; or permit entry for the purpose of inspection or sampling any designated object.

- Rule 34 requires a party producing electronically stored information to translate it into reasonably usable form and that parties may request an opportunity to test or sample materials in addition to inspecting and copying them.

Rule 37: Failure to Make Disclosures or Cooperate in Discovery; Sanctions.

- Formerly (f), now (e) Electronically stored information. A court may not impose sanctions on a party for failing to provide electronically stored information lost as a result of the routine, good faith operation of an electronic information system.

- Good faith involves modifying or suspending that routine operation to prevent the loss of information subject to a preservation obligation. Preservation obligations (i.e., a "litigation hold") mean a party is under a duty to preserve information because of pending or reasonably anticipated litigation. It means that a party is not permitted to exploit routine IS operation to thwart discovery obligations.
Guideline 1: A reasonable anticipation of litigation arises when an organization is on notice of a credible probability that it will become involved in litigation, seriously contemplates initiating litigation, or when it takes specific actions to commence litigation.

Guideline 2: Adopting and consistently following a policy or practice governing an organization's preservation obligations are factors that may demonstrate reasonableness and good faith.

Guideline 3: Adopting a process for reporting information relating to a probable threat of litigation to a responsible decision maker may assist in demonstrating reasonableness and good faith.

Guideline 4: Determining whether litigation is or should be reasonably anticipated should be based on a good faith and reasonable evaluation of relevant facts and circumstances.

Guideline 5: Evaluating an organization's preservation decisions should be based on the good faith and reasonableness of the decisions undertaken (including whether a legal hold is necessary and how it should be executed) at the time they are made.

Guideline 6: The duty to preserve involves reasonable and good faith efforts, taken as soon as is practicable and applied proportionately, to identify and, as necessary, notify persons likely to have relevant information to preserve the information.

Guideline 7: Factors that may be considered in determining the scope of information that should be preserved include the nature of the issues raised in the matter, the accessibility of the information, the probative value of the information, and the relative burdens and costs of the preservation effort.

Guideline 8: In circumstances where issuing a legal hold notice is appropriate, such a notice is most effective when the organization identifies the custodians and data stewards most likely to have relevant information, and when the notice:
   - (a) Communicates in a manner that assists persons in taking actions that are, in good faith, intended to be effective
   - (b) Is in an appropriate form, which may be written
   - (c) Provides information on how preservation is to be undertaken
   - (d) Is periodically reviewed and, when necessary, reissued in either its original or an amended form, and
   - (e) Addresses features of relevant information systems that may prevent retention of potentially discoverable information.

Guideline 9: An organization should consider documenting the legal hold policy, and, when appropriate, the process of implementing the hold in a specific case, considering that both the policy and the process may be subject to scrutiny by opposing parties and review by the court.

Guideline 10: Compliance with a legal hold should be regularly monitored.

Guideline 11: Any legal hold policy, procedure, or practice should include provisions for releasing the hold upon the termination of the matter at issue so that the organization can adhere to policies for managing information through its useful lifecycle in the absence of a legal hold.
Actually document “destruction” policies
Must be formal
Unnecessary retention increases E-Discovery costs
Must conform with document retention laws
  ▪ Sarbox criminalizes records destruction with intent to prevent availability for official proceedings.
  ▪ IRS
  ▪ SEC
    – Rule 17a-4 of SEC act: preserve email for 3 years
  ▪ Legal Holds (duty to preserve)
Document Retention Constraints

Examples

<table>
<thead>
<tr>
<th>Type of Record</th>
<th>Retention Period (years)</th>
<th>Law/Policy (source)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditors' reports</td>
<td>P</td>
<td>CCH Recommends</td>
</tr>
<tr>
<td>Cancelled checks, generally</td>
<td>3</td>
<td>UPPBRA</td>
</tr>
<tr>
<td>Employee payroll records (W-2, W-4, annual earnings records, etc.)</td>
<td>3</td>
<td>FLSA, UPPBRA</td>
</tr>
<tr>
<td>Payroll journal</td>
<td>3</td>
<td>FLSA, UPPBRA</td>
</tr>
<tr>
<td>Petty cash vouchers</td>
<td>3</td>
<td>UPPBRA</td>
</tr>
<tr>
<td>Annual reports</td>
<td>P</td>
<td>CCH Recommends</td>
</tr>
<tr>
<td>Contracts</td>
<td>Expiration +7</td>
<td>CCH Recommends</td>
</tr>
<tr>
<td>General, routine correspondence</td>
<td>3</td>
<td>UPPBRA</td>
</tr>
<tr>
<td>Employment Applications</td>
<td>1</td>
<td>Title VII, ADA</td>
</tr>
<tr>
<td>Employee earnings/payroll records</td>
<td>3</td>
<td>FLSA</td>
</tr>
<tr>
<td>Employee files</td>
<td>4</td>
<td>SSA, FLSA, ERISA,</td>
</tr>
<tr>
<td>Employment contracts</td>
<td>Expiration +3</td>
<td>FLSA</td>
</tr>
<tr>
<td>Form I-9 &amp; Control Act</td>
<td>3</td>
<td>Immigration Reform</td>
</tr>
<tr>
<td>Garnishments</td>
<td>7</td>
<td>FLSA</td>
</tr>
<tr>
<td>Medical or exposure to toxic substances records</td>
<td>30</td>
<td>OSHA</td>
</tr>
<tr>
<td>Pension documents/profit sharing plans</td>
<td>6</td>
<td>ERISA</td>
</tr>
<tr>
<td>Employee pension records, including service, eligibility, personal information, pensions paid</td>
<td>6</td>
<td>ERISA, ESA</td>
</tr>
<tr>
<td>Time cards/sheets</td>
<td>3</td>
<td>FLSA</td>
</tr>
<tr>
<td>Income tax returns and cancelled checks (federal, state and local)</td>
<td>6</td>
<td>IRS Code</td>
</tr>
<tr>
<td>Payroll tax returns</td>
<td>4</td>
<td>IRS Code</td>
</tr>
</tbody>
</table>

Document Retention Issues

- Must be applied regularly and consistently
  - Selective application is defeating

- Issues
  - Backup copies
  - Workstation drives
  - Mobile devices
    - Laptop drives
    - PDA-Phones
  - Practical
    - "Destroy after" locations
Evidence

CIS8630 Business Computer Forensics and Incident Response
Richard Baskerville