Arriving at an Anti-forensics Consensus

Examining How to Define and Control the Anti-forensics Problem

Ryan Harris
CERIAS, Purdue University
DFRWS 2006
What is the problem?

- Lack of agreement about how to define anti-forensics
- No way to classify anti-forensic methods
Some current views of anti-forensics

- Ways to “avoid detection” or “break industry tools”  
  Foster & Liu

- Hiding a system intrusion attempt  
  Shirani
Based on Saferstein’s definition

- **Anti-forensics:**

  “Methods used to prevent (or act against) the application of science to those criminal and civil laws that are enforced by police agencies in a criminal justice system.”
Viewing anti-forensics differently

- Ways to “...limit the identification, collection, collation and validation of electronic data...” Peron & Legary

- “Attempting to limit the quantity and quality of forensic evidence...” Grugg
Evidence and process based definition

- Anti-forensics:
  
  Any attempts to compromise the availability or usefulness of evidence to the forensics process.
Categorizing anti-forensic methods

<table>
<thead>
<tr>
<th>Peron &amp; Legary</th>
<th>Rogers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hiding</td>
<td>Data hiding</td>
</tr>
<tr>
<td>Destroying</td>
<td>Artifact wiping</td>
</tr>
<tr>
<td>Preventing from being created</td>
<td></td>
</tr>
<tr>
<td>Manipulating</td>
<td>Trail obfuscation</td>
</tr>
<tr>
<td></td>
<td>Attacks against the process &amp; tools</td>
</tr>
</tbody>
</table>
Proposed categories

- Evidence Destruction
- Evidence Hiding
- Evidence Source Elimination
- Evidence Counterfeiting
Evidence Destruction

- Dismantling evidence or making it unusable to the investigative process

- Physical example: Wiping fingerprints

- Digital example: Wiping a filesystem
Evidence Hiding

- Removing evidence from view
- Physical example: throwing a gun into the sewer
- Digital example: Steganography
Evidence Source Elimination

- Neutralizing evidentiary sources
- Physical example: Wearing gloves during a crime
- Digital example: Disabling audit trails
Evidence Counterfeiting

- Creating a “faked” version of the evidence

- Physical example: planting fingerprints

- Digital example: Using a different user’s account
Anti-forensic attacks - human element

- Alert investigators
- Education
- Real world experience
- “Thinking outside the box”
Anti-forensic attacks - tool dependence

- Tool assumptions
- Implementation bugs
Anti-forensic attacks - physical/logical

- Storage space
- Time
- Money
Presentation references


Questions/Comments?