Taxonomy of Anti-Computer Forensics Threats

Joseph C. Sremack & Alexandre V. Antonov

12 September 2007

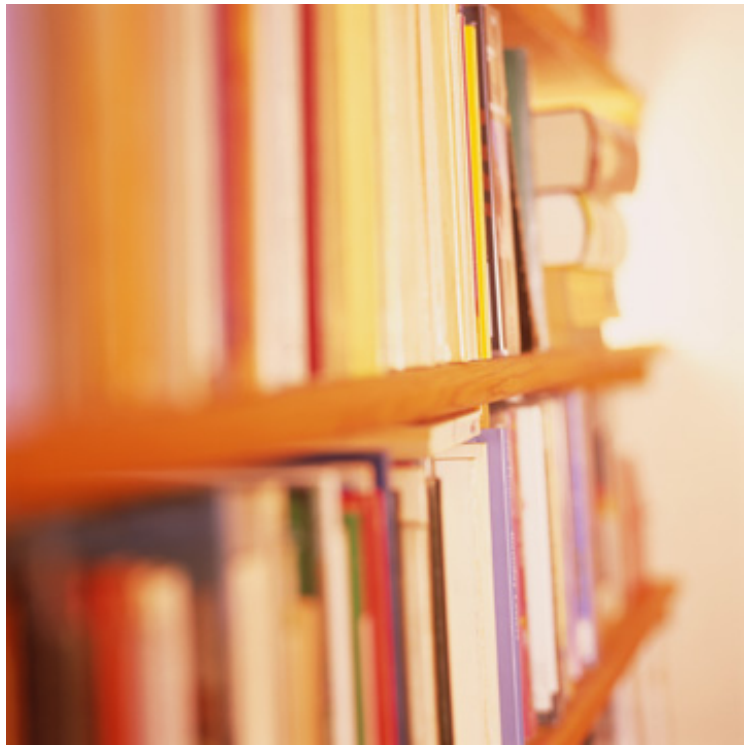
LECG

Overview

1. Introduction
2. Problem Statement
3. High-Level Overview of Investigation Phases
4. Types of Investigations
5. Anti-Forensics
6. Taxonomy of Anti-Forensics Threats
7. Case Study Discussion

Introduction: Who? What? Where?

- Perform computer forensics and data analytics for large-scale corporate civil and criminal investigations.
- Cases typically involve tens to thousands of custodians that require imaging.
- Devices range from PDAs/Blackberries to full data warehouses.
- Most investigations take place within US, although some cases take place in EU and Caribbean.



US Jurisprudence

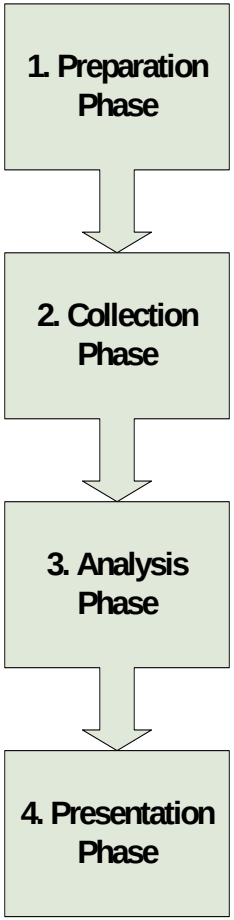
- Most law is based on case law.
- Evidence or expert testimony are typically deemed admissible when they satisfy the Daubert Standard:
  1. Relevant: Evidence/expert "fits" the facts of the case.
  2. Reliable: Evidence/expert's findings are based on sound scientific principles:[1]
     - Empirical testing: the theory or technique must be falsifiable, refutable, and testable.
     - Subjected to peer review and publication.
     - Known or potential error rate and the existence and maintenance of standards concerning its operation.
     - Whether the theory and technique is generally accepted by a relevant scientific community.

1. Wikipedia. "Daubert Standard." http://en.wikipedia.org/wiki/Daubert_Standard. Last updated July 22, 2007.

Problem Statement

- Anti-forensics is a growing issue with potentially catastrophic consequences for investigators.
  - If anti-forensics succeeds, evidence fails Daubert Standard.
  - Significant for case law. Exploiting case law itself can be an anti-forensics technique.
- Anti-forensics threats should be classified, just as they are in other subject areas, e.g. digital security.
- Creating a taxonomy of threats needs to take into account all types of investigations and all types of threats.

Phases in Computer Forensic Investigations



1. Preparation Phase
   - Scoping
   - Interviewing
   - Logistics
2. Collection Phase
   - Acquisition
   - Verification
3. Analysis Phase
   - Keyword searching
   - Log file comparisons
4. Presentation Phase
   - Expert report
   - Court presentation

Requirements for Phases

- Preparation Phase
  - Full scope understood
  - Interviews conducted
  - Determine data points
  - Determine means for analysis
  - Understand venue/audience for analysis findings
- Collection Phase
  - All relevant data are collected
  - Acquired data are verified
  - Full documentation of process
  - Maintain chain-of-custody
- Analysis Phase
  - Performed completely and accurately
  - Findings are verified
  - Industry best practices are applied
  - Court-accepted tools/methodologies employed over novel ones
  - Full documentation
  - Maintain chain-of-custody

Requirements for Phases Cont.

- Presentation Phase
  - All relevant information presented clearly
  - Analysis conforms to rules of admissibility

- Overall
  - Follow rules of admissibility
  - Findings are convincing and based on best practices
  - Full process is documented
  - Performed timely and accurately

Types of Computer Forensic Investigations

All try to answer the "Who, What, Where, When, and How?" question.

- Internal
  - Resolve an event outside of court of law.
  - Less rigor usually required, except when public disclosure required.
- Civil
  - Performed for court of law for some violation of civil liberties.
  - Requires preponderance of evidence.
- Criminal
  - Performed for court of law for breaking of societal law.
  - Requires proof beyond a shadow of doubt.
  - Often performed exclusively by law enforcement.

Anti-Forensics Defined

Def.: The practice of thwarting a proper forensic investigation.

Any activity that *intentionally* aims to deceive or impede the investigation is classified as anti-forensics.

Two classes of threats posed by anti-forensics:

1. Threats to digital evidence
2. Threats to legal process/admissibility

Digital Evidence Anti-Forensics

We have identified four main classes of threats to digital evidence:

1. Data Preservation: Preserving the potential evidence in its original state, including not creating new evidence.
2. Data Counterfeiting: Creating false and/or misleading evidence.
3. Data Hiding: Moving evidence to location undiscoverable by investigator.
4. Data Destruction: Destroying evidence, either completely or to un-analyzable state.

Two subclasses exist for each

1. Physical
2. Technical

Digital Evidence Anti-Forensics Taxonomy

Class	Subclass	Example
Evidence Preservation	Technical	Prevention from writing to hard drive.
Evidence Preservation	Physical	Installation of data gathering equipment that does not communicate with host network, such as a silent sniffer.
Evidence Destruction	Technical	Deletion of log file entries.
Evidence Destruction	Physical	Chemical, magnetic, mechanical destruction of media containing evidence.
Evidence Hiding	Technical	Use of encryption or steganography.
Evidence Hiding	Physical	Use of smart cards or hardware cryptographic modules.
Evidence Counterfeiting	Technical	Creation of misleading log file entries.
Evidence Counterfeiting	Physical	Physical replacement of system hard drive with a ghost image of the original hard drive with non-incriminating digital evidence.

Legal Process Anti-Forensics

The idea is to use legal boundaries and restrictions against the investigator.

Intentionally thwarting forensic investigation by exploiting legal process is becoming more prevalent.

Several Classes Exist

1. Sufficient Doubt: Creating doubt regarding “who” and/or “how” of an investigation.
2. Crossing Jurisdictions: Limiting what evidence can be captured due to inability to access data in one or more jurisdictions.
3. Privacy: Limiting what evidence can be captured due to privacy laws.
4. Significant Changes in Scientific Foundation: Relying on recent scientific breakthroughs to undermine established forensic process.

Legal Process Anti-Forensics Taxonomy

Class	Example
Sufficient Doubt	Perform crime from publicly-accessible or virus-infected computer.
Crossing Jurisdictions	Perform crime from a jurisdiction with no extradition and no working relationship with target jurisdiction.
Privacy	EU laws prevent certain EU citizen personal data from being sent to non-EU countries.
Significant Changes in Scientific Foundation	Recent proofs in weakness in SHA-1 and MD5.

Taxonomy Considerations for Different Types of Cases

Internal

All digital evidence anti-forensics threats apply, but the legal process threats do not. Legal process may become important if internal investigation later leads to civil or criminal investigation.

Civil

All digital evidence anti-forensics threats apply, and the legal process threats apply. The legal process becomes important insofar as some data may be inaccessible, but sufficient doubt does not apply so long as a preponderance of evidence still exists.

Criminal:

All digital evidence anti-forensics threats apply, and the legal process threats apply. Legal process extremely important, since any doubt can make evidence inadmissible.

Case Study: International Intellectual Property Theft

Medical manufacturer ("A") whose former CEO left to form Competitor ("B"). Believed that IP being leaked through employees at previous company.

B located outside of US in country with no extradition/poor data export laws (crossing jurisdictions).

Installed traffic capturing devices for email and instant messages at three sites: US, EU, and Latin America.

Traffic analysis showed missing data from Latin American site, which was due to IT staff stealing equipment before leaving company (physical evidence hiding).

Later analysis established some suspects and allowed A to mitigate.

Future Work

1. Expand taxonomy to include unintentional threats.

2. Investigate social threats to forensics, such as collusion and other forms of social engineering.

3. Develop better controls for forensic process.