Digital Forensics in the Corporate World

Ernesto F. Rojas CISSP, DFCP, CCFP

Assistant Director, Cyber Security Institute

University of Houston Clear Lake

UHCL

The choice is clear.

Biggest Data Breaches of 2014*

eBay – 145 million customer names, passwords, email addresses, physical addresses, phone numbers and date of birth

Michaels Stores – 3.0 million payment card numbers

Montana Department of Public Health – Server with 1.3 million names, addresses, dates of birth, and SSN

Variable Annuity Life Insurance Co. – Information on 774,723 of the company's customers, including SSN.

Spec's – Information on 550 thousand customers. Customer names, credit and debit cards, card expiration dates, card security codes, bank account numbers from checks, and driver license numbers

St. Joseph Health System – 405 thousand patient records

*as of July 2014

What is Digital Forensics

NIST Publication SP 800-86 Published in August of 2006

Defines it as: “the application of science to the identification, collection, examination and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data”.

Corporate Forensics

Investigating Crimes Internally

Internal Policy Violations

Reconstructing Computer Security Incidents

Troubleshooting Operational Problems

Recovering from System damage

Preventing Protected and Sensitive data from leaving

and many other uses ….

Forensic Steps

Collection – Identifying, labeling, recording and acquiring data while preserving integrity of the data

Examination – forensically processing collected data using a combination of automated and manual methods and assessing and extracting data of particular interest, while preserving the integrity of the data

Analysis – analyzing the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the that were the impetus for performing the collection and examination

Reporting – reporting the results of the analysis, which may include describing the actions used, explaining how tools and procedures were selected, determining other actions need to be performed and providing recommendations for improvement

Guidance Tools

To implement an internal corporate digital forensics practice:

- NIST SP 800-86 guidelines
- Develop a training regimen with a mix of sources
- Identify a staff with appropriate credentials
- Define roles and responsibilities
- Develop staff training and skills
- Integrate into the information life cycle

Differences in Forensics

Digital Forensics for Legal Cases

- Involves data recovery, deleted files and version recovery
- Focused on time slice, subject of dispute and custodians
- Based on facts of the case and specifics
- Designed to present information in a court of law

Digital Forensics for Corporate Incidents

- Analysis of operating systems, network traffic and data
- Focused on discovering the how and why of the incident
- Based on developing and finding the source of the incident
- Designed to present information in a court of law if necessary

Corporate Incidents

Components of an Incident Investigation

- Operating system information
  - volatile and non-volatile data
- Network Traffic
- Application Data

Recommendations

- Organizations should use a consistent forensic process
- Organizations should be proactive in collecting useful data
- Analysts should use a data collection standard based process
- Analysts should use a methodical approach to studying the data
- Analysts should review their processes and practices

Logs

In corporate incident response the importance of log files is significant:

- System events
- Audit records
- Application events
- Command history
- Recently accessed files

Priority in Collections

The process of collecting information in an incident has to flow from most volatile to least volatile as follows:

- Network connections
- Login sessions
- Contents of memory
- Running processes
- Open files
- Network configuration
- Operating system time

Once this portion of the collection is completed then the non-volatile data can be collected once the system has been shut down.

UHCL-CSI Program

Starting in the Fall 2014

- **Introduction to Forensics**
- **Data Collection**
- **Digital Forensics Level 1**

Offered in a Weekend Program

Friday/Saturday

Thank you!

Questions?

Ernesto F. Rojas CISSP, DFCP, CCFP
rojase@UHCL.edu
http://www.uhcl.edu/sce/csi