IT Forensics & Digital Methods for Investigations

Mauli Shah

Contents

- Case Study
- Digital Forensics
- Digital Evidence
- Need for Computer Forensics

Case Study

The Biggest Hack

About the Hack

- >200 million credit card number stolen
- Heartland Payment Systems, 7-Eleven, and 2 US national retailers hacked
- Heartland Payment Systems lost > 130 million credit and debit card numbers and corresponding credit card data

Modus Operandi

- Visit retail stores to understand workings
- Analyze websites for vulnerabilities
- Hack in using SQL injection
- Inject malware
- Sniff for card numbers and details
- Hide tracks

The hacker underground

- Albert Gonzalez
  - a/k/a “segvec,”
  - a/k/a “soupnazi,”
  - a/k/a “j4guar17”

- Malware, scripts and hacked data hosted on servers in:
  - Latvia
  - Netherlands

Impact of the Hack

- TJX direct costs

$200 million in fines/penalties

$41 million to Visa

$24 million to MasterCard

Digital Forensics – An Insight

Digital Forensics

- “The preservation, identification, extraction, interpretation, and documentation of computer evidence, to include the rules of evidence, legal processes, integrity of evidence, factual reporting of the information found, and providing expert opinion in a court of law or other legal and/or administrative proceeding as to what was found ”

Digital Forensics

- Involves
  - Identification
  - Collection of Evidence
  - Required Documentation
  - Imaging
  - Examination
  - Report Preparation
  - Returning of Evidence

Digital Forensic Examination

- The Digital forensic examination is:
  - Locating digital evidence
  - Evidence can withstand close scrutiny or a legal challenge.

Digital Evidence

- Digital evidence is any information of value that is either stored or transmitted in a binary form, including digital audio, image, and video.

Need for Computer Forensics

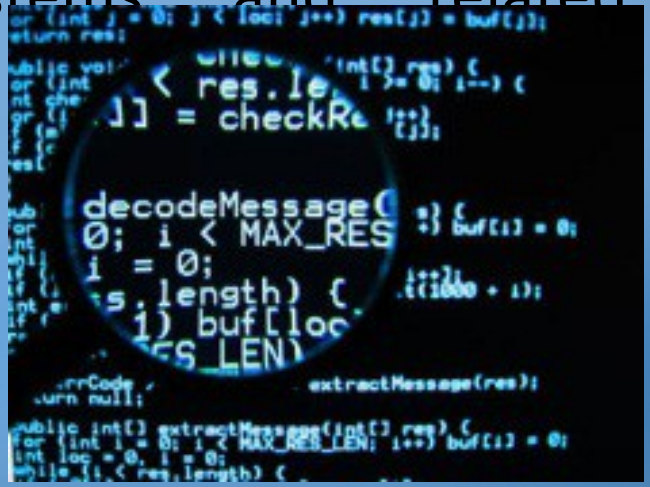
- The growing misuse of computers for criminal activities.
- Increase in the dependence of Internet of various organizations.
- Constantly increase in the Security Incidents.
  - Determining a Security Breach
  - Detection of Disloyal Employees
  - Evidence for Disputed Dismissals
  - Malicious File Identification

Computer Forensics Types

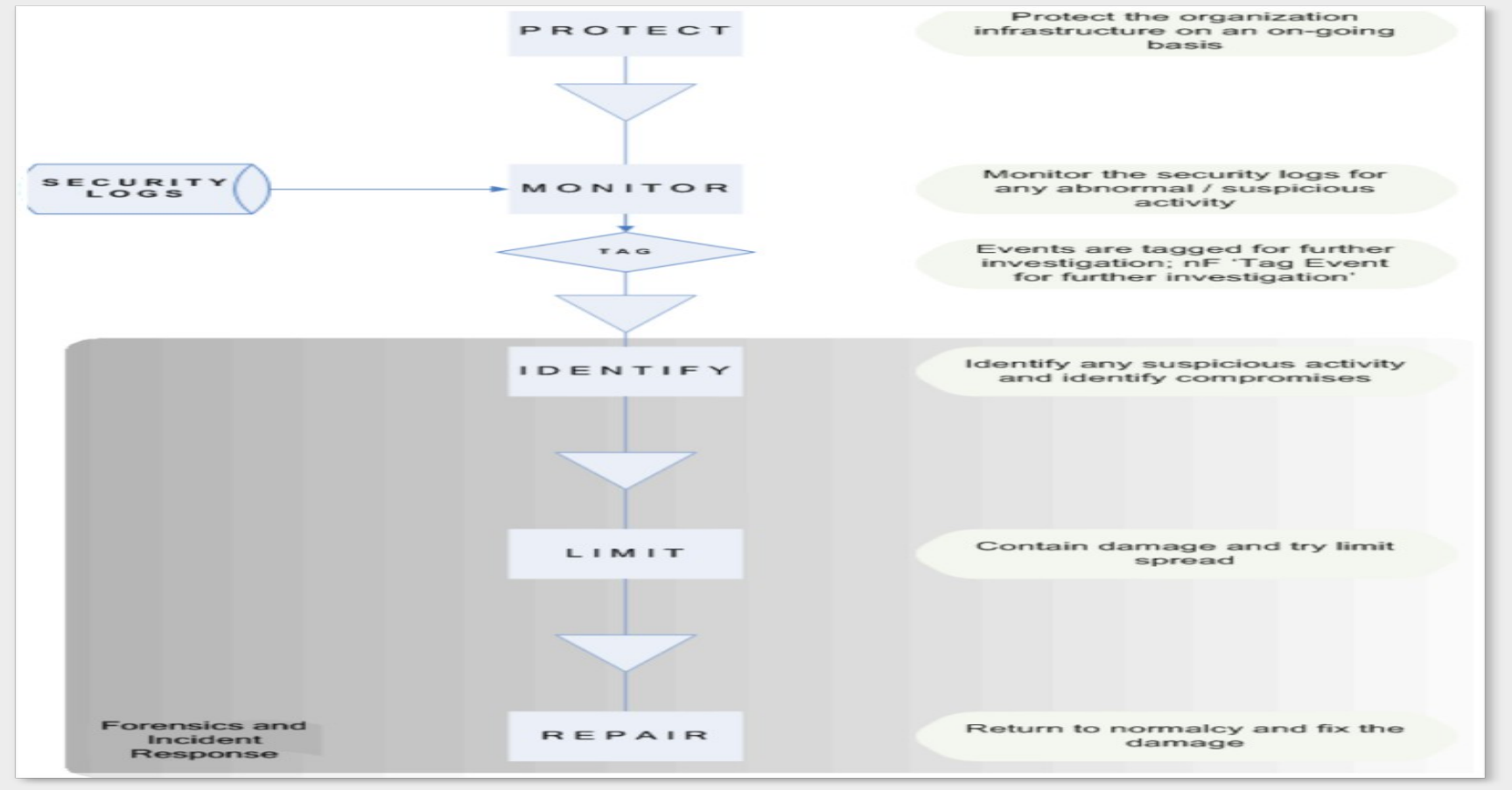
- Disk Forensics
  - Recover, Analyze file access and logs.
- System Forensics
  - O/S Dependent
- Network Forensics
  - Includes ID systems
- Internet Forensics
  - Includes ISP logs etc.
- Mobile Forensics

Incidence Response and Digital Forensics

- The need for computer forensics is determined by the type of incident.
- It is used for all types of security and criminal incidents which involve computer systems and related technologies.



Incidence Response and Digital Forensics



Computer Forensics & IT Audit

- Incorporate computer forensic services
- Cases are requiring computer forensics
- IT Auditors have:
  - authority
  - technical know how

Computer Forensics & IT Audit

IT Auditor's Role

(Forensic Specialist)

- Determine if reason for computer forensics is appropriate.
- Identify where additional digital evidence may reside.

Client's Role

- Determine when to use Computer Forensic Services:
- Identify where digital evidence may reside.

Collection of Evidence

IT Auditor's Role

- Help Client Secure the computer to be examined
- Require and Complete Necessary Forms
- Securely Collect Computer from Client

Client's Role

- Ensure that computer to be examined remains secure until collected
- Notify Appropriate Personnel
- Complete Chain of Custody Form

Forensics Tools

- Tools and Vendors include:
  - EnCase
  - Helix
  - FTK Imager

EnCase

- Considered the leader in stand-alone forensics analysis.
- Widely accepted in court.
- Facilitates examination of files, including deleted files and unallocated data.
- Produces reports and extracts without altering the original data.

Do’s and Don'ts

- Collection
  - Do not disturb the computer in question.
  - Computer is off, Leave it off
  - Computer is on, Leave it on
  - Do not run any programs on the computer.
  - Do not make any changes
  - Do Not Insert Anything Into The Computer
  - Secure the computer
  - Unplug the system from the network

Challenges faced

- Identification of an Incident
- Timeliness
- Digital Data is an Abstraction
- Digital Evidence easily manipulated
- Distributed nature of Evidence


Questions