

Computer Forensics What is It and When Should You Use It?

Robert Ono, IT Security Coordinator, UC Davis
Tye Stallard, Security Administrator, UC Davis

February 2009

Discussion Topics

- ▶ Define “computer forensics”
- ▶ Computer forensics team workflow
- ▶ Computer forensics methodology and tools
- ▶ Where to apply computer forensics?
- ▶ How to start a computer forensics program?

Computer Forensics

- ▶ Application of computer investigation and analysis techniques to collect evidence.
- ▶ Structured and objective investigation – think CSI
- ▶ Preservation of digital artifacts

Use of Computer Forensics

- ▶ Policy violations
- ▶ Federal and/or state law violation
- ▶ Research misconduct
- ▶ Preliminary analysis of incident
 - ▶ unknown if a crime has been committed

Insider Motivations

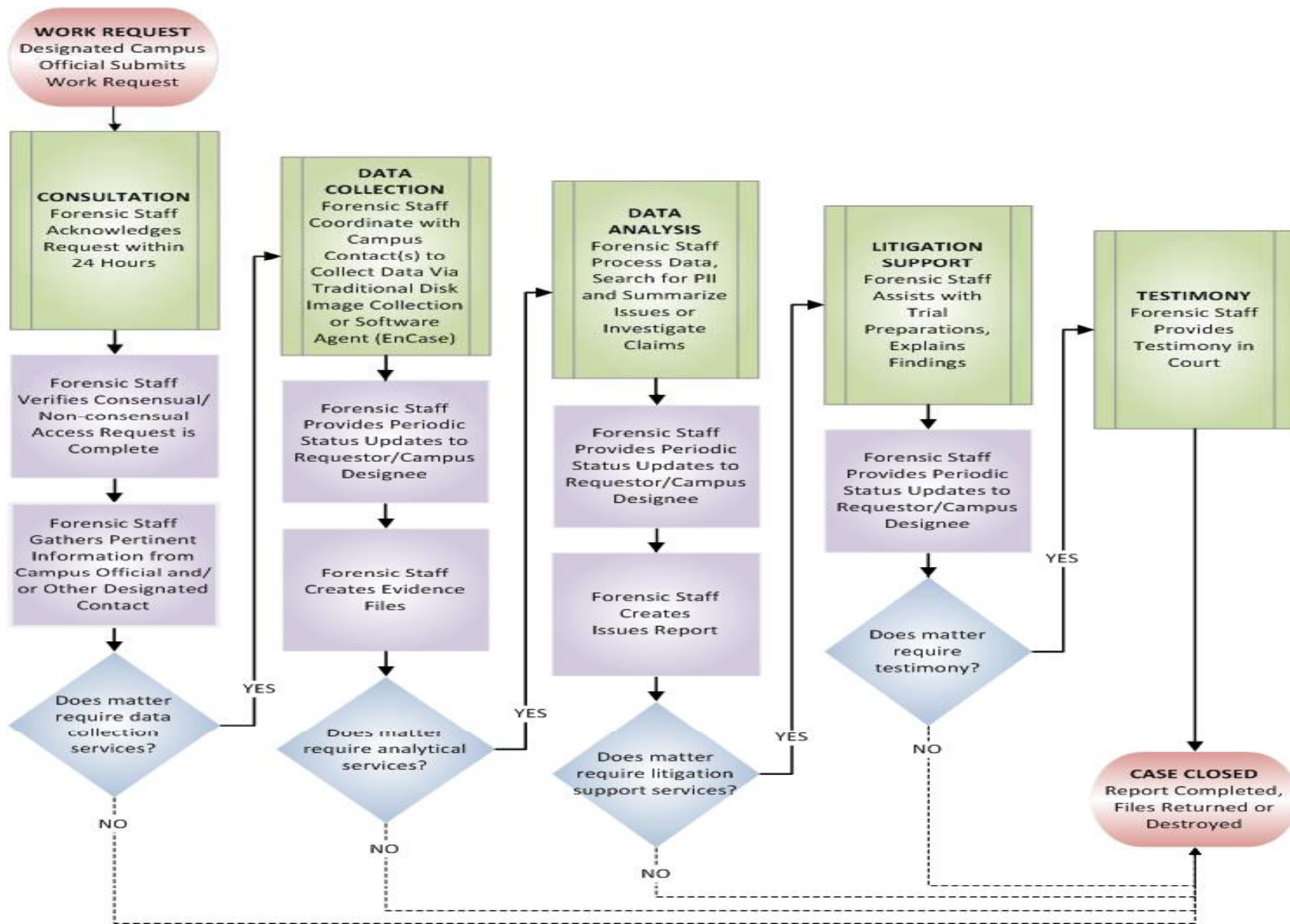
- ▶ Intentional
 - ▶ Disgruntled
 - ▶ Terminated
 - ▶ Personal Gain
- ▶ Unintentional
 - ▶ Complacency
 - ▶ New
 - ▶ Untrained



When Should You Use It?

- ▶ Anytime there are digital artifacts
 - ▶ Determine scope of data collection
 - ▶ Preserve data to nullify accusations of spoliation
 - ▶ Corroboration to improve argument of authenticity
- ▶ Courts
 - ▶ Anticipation of litigation
 - ▶ Anticipation of obstruction of justice





Relevant Policies and Laws

- ▶ UC Electronic Communications Policy
 - ▶ Privacy and Access
- ▶ Applicable state laws
- ▶ Federal Rules of Civil Procedure
- ▶ Government searches and privacy
 - ▶ Fourth Amendment
 - ▶ Wiretap Act 1968
 - ▶ Electronic Communications Privacy Act 1987
 - ▶ Patriot Act 2001 and 2006

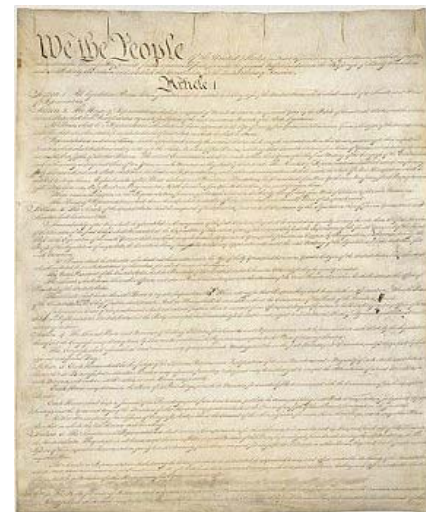


Relevant Policies and Laws

Fourth Amendment, US Constitution

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

- Judicial sanction
- Probable cause
- Defined scope



Methodology

- ▶ Preparation
- ▶ Collection
- ▶ Preservation
- ▶ Extraction
- ▶ Identification
- ▶ Analysis
- ▶ Reporting

What's In the Computer Forensics Toolkit?

- ▶ Hardware
 - ▶ Wide variety of interfaces
 - ▶ Integrity preserving devices
- ▶ Software
 - ▶ Wide variety of formats to parse
- ▶ Training





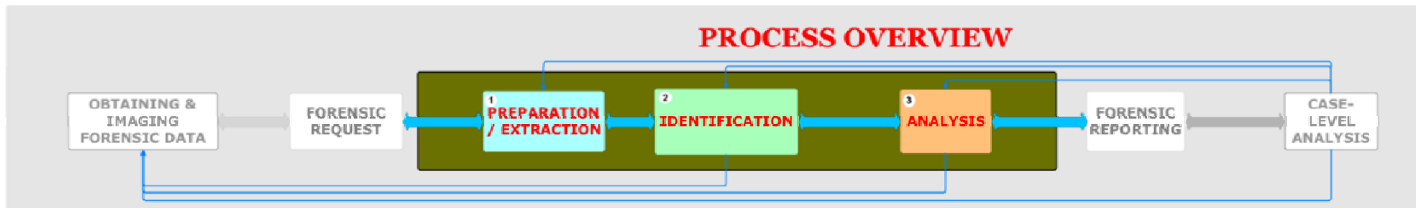
DIGITAL FORENSIC ANALYSIS METHODOLOGY



1.08 | 4/28/14 | Page 27 | 2017

LISTS

PROCESS OVERVIEW



Search Leads	
Data Search Leads	Comments/Notes/Message
<p>Generally, this involves opening a case file in the tool of choice and exporting forensic image file. This could also include recovering a network environment or database to mirror forensic environment.</p> <p>Example Data Search Leads:</p> <ul style="list-style-type: none"> Identify and extract all email and deleted items. Search results for evidence of child pornography. Configure and load external database for data mining. Review all Available files and index files for review by case agent/forensic examiner. 	<p>Use this section as needed.</p> <p>Example Note:</p> <p>Created empty case agent when forensic data was reviewed.</p>

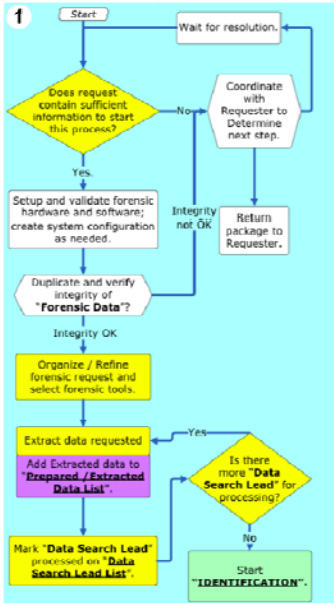
Extracted Data	
Prepared / Extracted Data	Comments/Notes/Message
<p>Prepared / Extracted Data List is a list of items that are prepared or extracted to allow identification of Data pertaining to the forensic request.</p> <p>Example Prepared / Extracted Data items:</p> <ul style="list-style-type: none"> Recreated hard drive image using Sector or PFX to allow a case agent to image the contents. Exported registry files and external registry content to allow a forensic examiner to examine registry entries. Loaded database files to loaded on a database server ready for data mining. 	<p>Use this section as needed.</p> <p>Example Message:</p> <p>Various files located in C:\Program\Directory have all extensions but are actually .exe files.</p>

Relevant Data	
Relevant Data	Comments/Notes/Message
<p>Relevant Data List is a list of data that is relevant to the forensic request. For example:</p> <ul style="list-style-type: none"> If the forensic request is finding information relating credit card fraud, any credit card numbers, images of credit cards, links discussing making credit card, and items that show the card, time and search term used to find credit card numbers program, the relevant Data are identified. In addition, victim information associated credit numbers case for purpose of victim notification. 	<p>Use this section as needed.</p> <p>Example Note:</p> <p>Attachment in training and message with list of URLs in L. Make sure an extension before exporting and identify and reviewed 13 items containing data to control.</p>

New Data Source Leads	
New Source of Data Leads	Comments/Notes/Message
<p>New Source of Data Lead List is a list of data that should be reviewed by investigative or further investigation efforts.</p> <p>Example New Source of Data Leads:</p> <ul style="list-style-type: none"> Local address: 104001001.com Server logs from PFX server. Database information for an IP address. Transaction logs from server. 	<p>Use this section as needed.</p> <p>Example Note:</p> <p>During forensic analysis of server logs from credit card that a email message revealed that local Data was taken from program on credit card printing machine.</p>

Analysis Results	
Analysis Results	Comments/Notes/Message
<p>Analysis Results List is a list of reviewed data that analyzed the who, what, when, where and how questions to satisfy the forensic request.</p> <p>Example Analysis Results:</p> <p>Sample Message:</p> <p>IP Address: 104001001.com</p> <p>Server logs from PFX server.</p> <p>Database information for an IP address.</p> <p>Transaction logs from server.</p>	<p>Use this section as needed.</p> <p>Example Note:</p> <p>Sample Message:</p> <p>IP Address: 104001001.com</p> <p>Server logs from PFX server.</p> <p>Database information for an IP address.</p> <p>Transaction logs from server.</p>

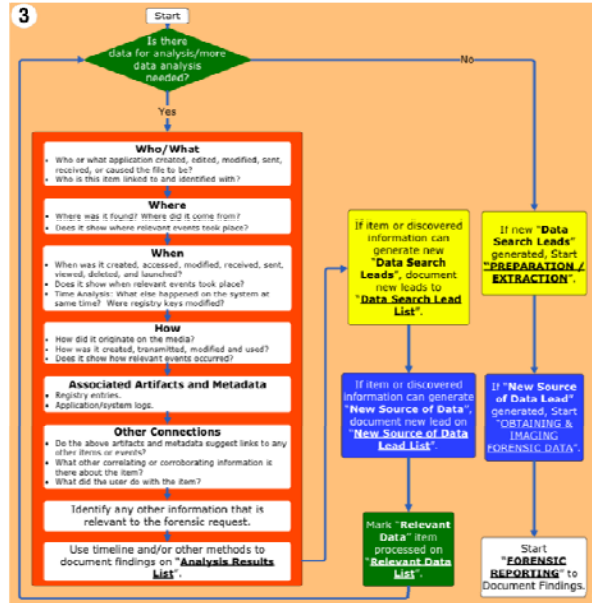
1 PREPARATION / EXTRACTION



2 IDENTIFICATION



3 ANALYSIS



Return On Investment (Determines when to stop the process. Typically, after enough evidence is obtained for preservation, the value of additional forensic analysis diminishes.)

Where's the Data?

- ▶ New Survey reveals one-third of employees use personal email one or twice a week for business purposes
- ▶ Nearly 60 percent use personal email at work with employer provided email is down

Source: AP Alert – Business (Market Wire), April 16, 2007

Location	Potential source	What you might find	Who to ask first
Victim computer	<ul style="list-style-type: none"> ■ Operating system logs ■ Application logs ■ Security logs ■ .ini files ■ Contraband files 	<ul style="list-style-type: none"> ■ Date and time stamps ■ User names and passwords ■ Connection information ■ IP addresses ■ Node names 	<ul style="list-style-type: none"> ■ Victim ■ Network administrator or installer
Victim-side firewall or router, Syslog server	<ul style="list-style-type: none"> ■ Firewall logs ■ DHCP logs ■ NAT/PAT logs ■ Proxy logs 	<ul style="list-style-type: none"> ■ Address translations ■ Date and time stamps ■ User names and passwords ■ Connection information ■ IP addresses ■ Node names 	<ul style="list-style-type: none"> ■ Victim ■ Network administrator or installer
Victim ISP	<ul style="list-style-type: none"> ■ Firewall logs ■ DHCP logs ■ NAT/PAT logs ■ Proxy logs 		<ul style="list-style-type: none"> ■ Victim ISP
Source ISP	<ul style="list-style-type: none"> ■ Firewall logs ■ DHCP logs ■ NAT/PAT logs ■ Proxy logs 		<ul style="list-style-type: none"> ■ Source ISP
Source-side firewall, router, Syslog server	<ul style="list-style-type: none"> ■ Firewall logs ■ DHCP logs ■ NAT/PAT logs ■ Proxy logs 		<ul style="list-style-type: none"> ■ Owner ■ Operator ■ Network administrator
Source computer	<ul style="list-style-type: none"> ■ Operating system logs ■ Application logs ■ Security logs ■ .ini files ■ Contraband files 	<ul style="list-style-type: none"> ■ Date and time stamps ■ User names and passwords ■ Connection information ■ IP addresses ■ Node names 	<ul style="list-style-type: none"> ■ Owner ■ Operator ■ Network administrator

General Incident Considerations

- ▶ Restrict access to area/systems
- ▶ Create a timeline
- ▶ Document environment and actions
- ▶ Pull the plugs? Which plugs?
- ▶ Bag and tag?
- ▶ Prepare to accept disk image(s)
- ▶ Image disk(s)
- ▶ Discover boot order

General Incident Considerations

- ▶ Disk analysis
 - ▶ Need incident details prior to initiating data search
- ▶ Maintain chain of custody
- ▶ Extent of analysis

“The New E-spionage Threat”

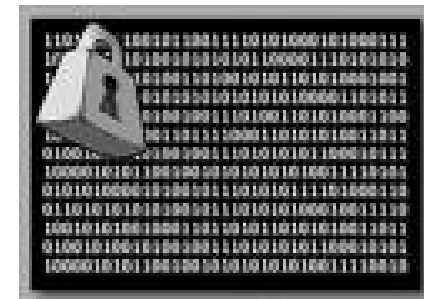
- ▶ Spear phishing
 - ▶ Email targets high profile executives
 - ▶ Executives are enticed them to a Web site
 - ▶ Victim downloads a program
 - ▶ Key logger is installed

BusinessWeek, April 10, 2008

Better Business Bureau, February 2007

Threats to Forensics

- ▶ Cryptography
- ▶ Disk wiping
- ▶ Anti-Forensics
- ▶ Cloud computing
 - ▶ GDrive
- ▶ Data overload



What's This Going to Cost?

Standalone Forensics SW	\$ 5,000
NW Acquisition SW	\$195,000
Hardware	\$ 12,000
Training with Travel (for 2 positions)	\$ 15,000
Secure Forensics Facility	Depends
Forensics Staff	Depends



Can This Work be Outsourced?

- ▶ Availability
- ▶ Confidentiality
 - ▶ Privileged work product?
- ▶ Bias
 - ▶ Independence
 - ▶ Work for hire
- ▶ Liability

Can This Work be Outsourced?

- ▶ Advantages

- ▶ Independence of expert

- ▶ Disadvantages

- ▶ Without clear expectations and authorities, each incident can be bureaucratic, slow and expensive

Summary

- ▶ Forensics is a methodology driven process
- ▶ Preparation helps to manage costs and liability
- ▶ Technology constantly changes
 - ▶ Motivations for misuse of electronic resources do not

Questions

References

- ▶ Open Source tools
 - ▶ www.opensourceforensic.org
- ▶ Commercial tools, training and/or services
 - ▶ www.accessdata.com
 - ▶ www.forensics-intl.com (New Technologies, Inc)
 - ▶ www.guidancesoftware.com
 - ▶ www.sans.org