

INTRODUCTION

COMP 597 – Computer Forensics

Digital Forensics & Investigation



Why do we need digital investigation?

- Some type of device that has been involved in an incident or a crime

Digital Forensics & Investigation

FROM THE CASE FILE: TRACKING A KILLER

In late December 2005, 27-year-old Josie Phyllis Brown was reported missing in Baltimore. Digital evidence led investigators to a 22-year-old college student, John Gaumer. Brown met Gaumer on the Internet site MySpace.com and arranged to meet him for a date (Associated Press, 2006). On the night of her disappearance, Brown's mobile telephone records showed that she talked to Gaumer before meeting with him, and police placed her telephone many miles from where he claimed to have left her that night. After the web of evidence converged on Gaumer in February 2006, he led police to her body and admitted to beating Brown to death after their date.

Gaumer used the Internet extensively to communicate and meet potential dates. Part of the evidence against him was a digital recording of "thumping noises, shouting and brief bursts of a woman's muffled screams" apparently created when Gaumer's mobile phone inadvertently dialed Brown's (McMenamin, 2007). In his confession to police, Gaumer stated that he removed her nose, jaw, teeth, and most of her fingertips in an attempt to thwart identification of her body, and that he later sent an e-mail to her account to make it appear that he did not know she was dead.

From: Handbook of Digital Forensics and Investigation, Eoghan Casey

Digital Forensics & Investigation

CASE EXAMPLE (MASSACHUSETTS, 2005–2010)

TJX, the parent company of T.J. Maxx, Marshalls, and other retail stores in the United States, Canada, and Europe, was the target of cyber criminals who stole over 90 million credit and debit card numbers. After gaining unauthorized access to the inner sanctum of the TJX network in 2005, the thieves spent over 2 years gathering customer information, including credit card numbers, debit card details, and drivers' license information. The resulting investigation and lawsuits cost TJX over \$170 million. In 2009, a Ukrainian man named Maksym Yastremskiy was apprehended in Turkey and was convicted to 30 years in prison for trafficking in credit card numbers stolen from TJX. Digital evidence was obtained

with some difficulties from computers used by Yastremskiy, ultimately leading investigators to other members of a criminal group that had stolen from TJX and other major retailers by gaining unauthorized access to their networks. In 2010, Albert Gonzalez was convicted to 20 years in prison for his involvement in breaking into and stealing from TJX. During the years that Gonzalez was breaking into the networks of major retailers, he was paid an annual salary of \$75,000 by the U.S. Secret Service as an undercover informant. Others involved with Gonzalez in the theft of data, sale of credit cards, and laundering of proceeds have received lesser sentences and fines (Zetter, 2010).

From: Digital Evidence and Computer Crime 3rd edition, Eoghan Casey

Digital Forensics & Investigation



The BTK serial killer:

- ▣ Murdered 10 people
- ▣ From 1974 to 1991
- ▣ send taunting letters to police and newspapers
- ▣ Was arrested in 2005

Digital Forensics & Investigation



- Digital Investigation
- Digital Forensics
- Digital Evidence

Locard's Exchange Principle

"Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value."

Digital Investigation



- A process that develops and tests hypotheses through the gathering of evidence to answer questions about digital events

Digital Forensics

- “the use of science or technology in the investigation and establishment of facts or evidence in a court of law”

From: [The American Heritage Dictionary](#)

Digital Evidence

- *any type of data that is saved or transferred using a digital device that can help with the digital investigation*

Digital Evidence



Digital Evidence has:

- legal usage
- investigative usage

Digital Evidence



Used for:

1. what happened when
2. who interacted with whom
3. the origination of a particular item
4. who was responsible
5. determine the intent of a crime

Digital Evidence

- Examples:

- The investigator found an incriminating file
- Searching SMS messages on a murder victim's mobile device

Investigation Process of a digital crime

- ❑ Gather facts
- ❑ Form a hypothesis based on the available evidence
- ❑ Should be objective
- ❑ Follows the laws
- ❑ Always be open to other possibilities

Investigation Process of a digital crime

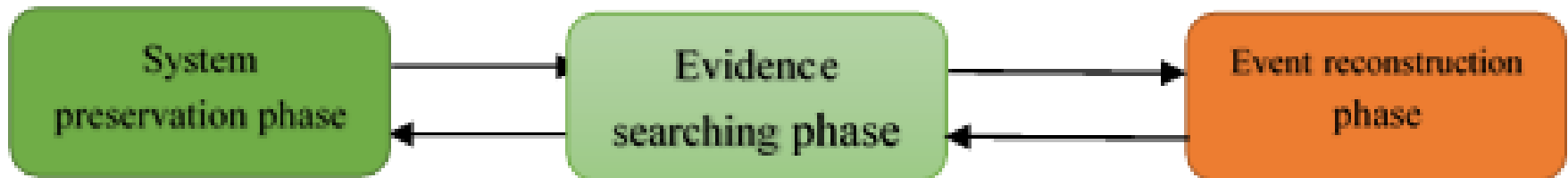


Example:

- We are at the office and there is no more coffee
- Who drank the last cup of coffee?

Investigation Process of a digital crime

Three major phases:



System preservation phase



- We want to reduce the amount of evidence that may be overwritten
- It is a continuous process

Evidence Searching Phase



- Live analysis
- Dead analysis

Evidence Searching Phase

- Search for evidence: looking for data to support or refute (easier) hypotheses
 - ▣ salvage deleted data
 - ▣ special files
 - ▣ filter out irrelevant data
 - ▣ extract embedded metadata

Evidence Searching Phase



1. Define the general characteristics of the object
2. Define the initial locations to search for

Evidence Searching Phase

Search criteria can be based on:

- ❑ file extensions
- ❑ names
- ❑ Keyword
- ❑ temporal data
- ❑ Message digest value
- ❑ Content signatures

Event Reconstruction



- use the evidence to determine what are the events that occurred in the system

Event Reconstruction



- Relational Analysis
- Functional Analysis
- Temporal Analysis

Event Reconstruction

FROM THE CASE FILE: TRACKING A KILLER

In late December 2005, 27-year-old Josie Phyllis Brown was reported missing in Baltimore. Digital evidence led investigators to a 22-year-old college student, John Gaumer. Brown met Gaumer on the Internet site MySpace.com and arranged to meet him for a date (Associated Press, 2006). On the night of her disappearance, Brown's mobile telephone records showed that she talked to Gaumer before meeting with him, and police placed her telephone many miles from where he claimed to have left her that night. After the web of evidence converged on Gaumer in February 2006, he led police to her body and admitted to beating Brown to death after their date.

Gaumer used the Internet extensively to communicate and meet potential dates. Part of the evidence against him was a digital recording of "thumping noises, shouting and brief bursts of a woman's muffled screams" apparently created when Gaumer's mobile phone inadvertently dialed Brown's (McMenamin, 2007). In his confession to police, Gaumer stated that he removed her nose, jaw, teeth, and most of her fingertips in an attempt to thwart identification of her body, and that he later sent an e-mail to her account to make it appear that he did not know she was dead.

From: Handbook of Digital Forensics and Investigation, Eoghan Casey

Evidence Characteristics



- class characteristics
- Individual characteristics

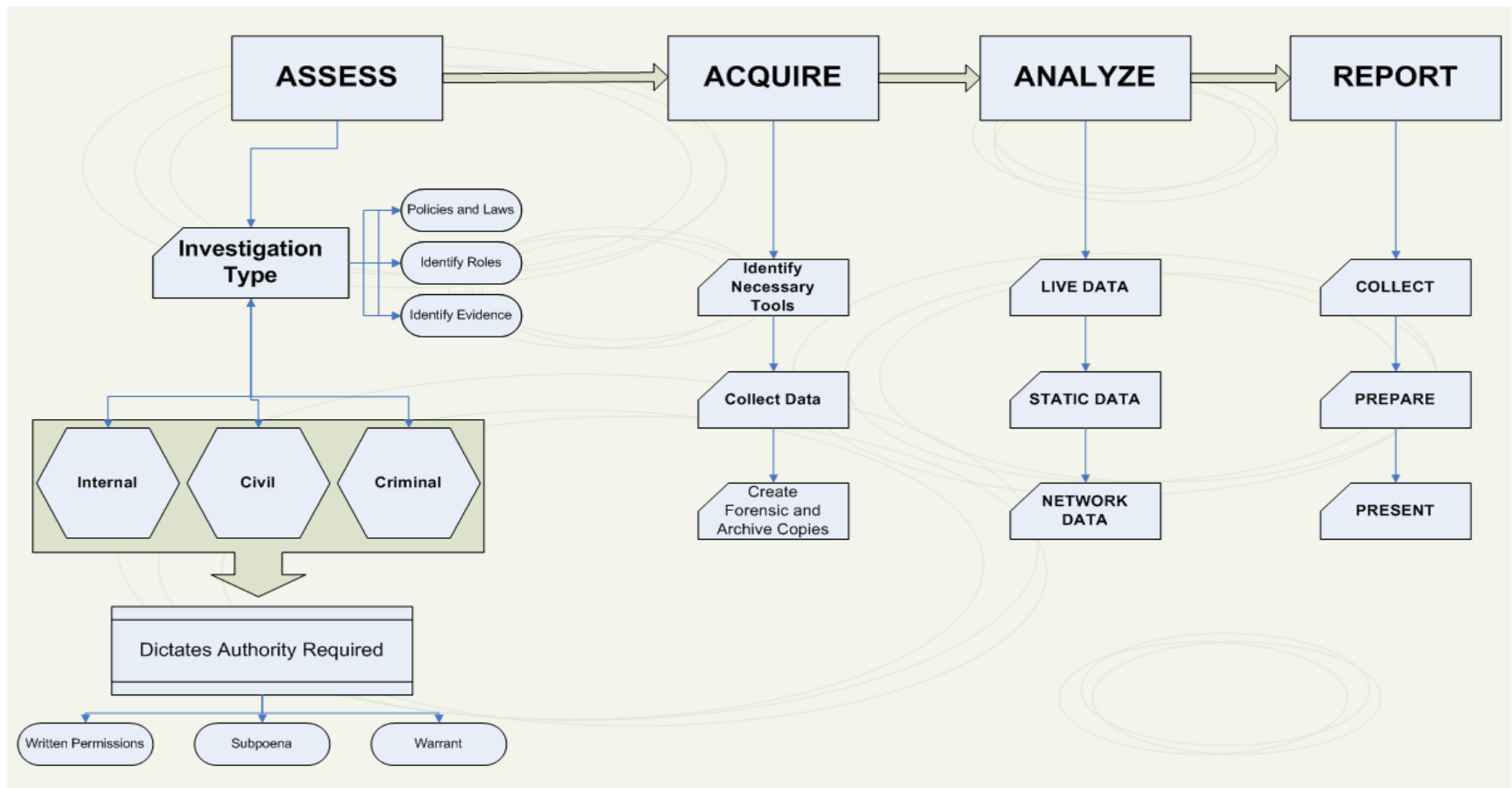
Investigation Process of a digital crime



Example:

- We are asked to search for child pornography on a personal computer. What do we need to do?

Investigation Process of a digital crime



From: Digital Archaeology: The Art and Science of Digital Forensics



General Investigation Guidelines

General Investigation Guidelines

- Preservation
- Isolation
- Correlation
- Logging

Forensic Soundness



Digital evidence used:

- ☐ Is what you claim
- ☐ Has not been altered or substituted since collection

Forensic Soundness

Process:

- a) Documentation of the acquisition process
- b) Documenting unique characteristics of the evidence
- c) Showing continuous possession and control throughout its lifetime
- d) Copy important data, put the original in a safe place, and analyze the copy


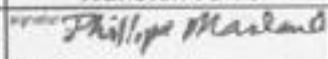
Forensic Soundness



Things to prevent:

- ▣ Misidentification of evidence
- ▣ Contamination of evidence
- ▣ Loss of evidence

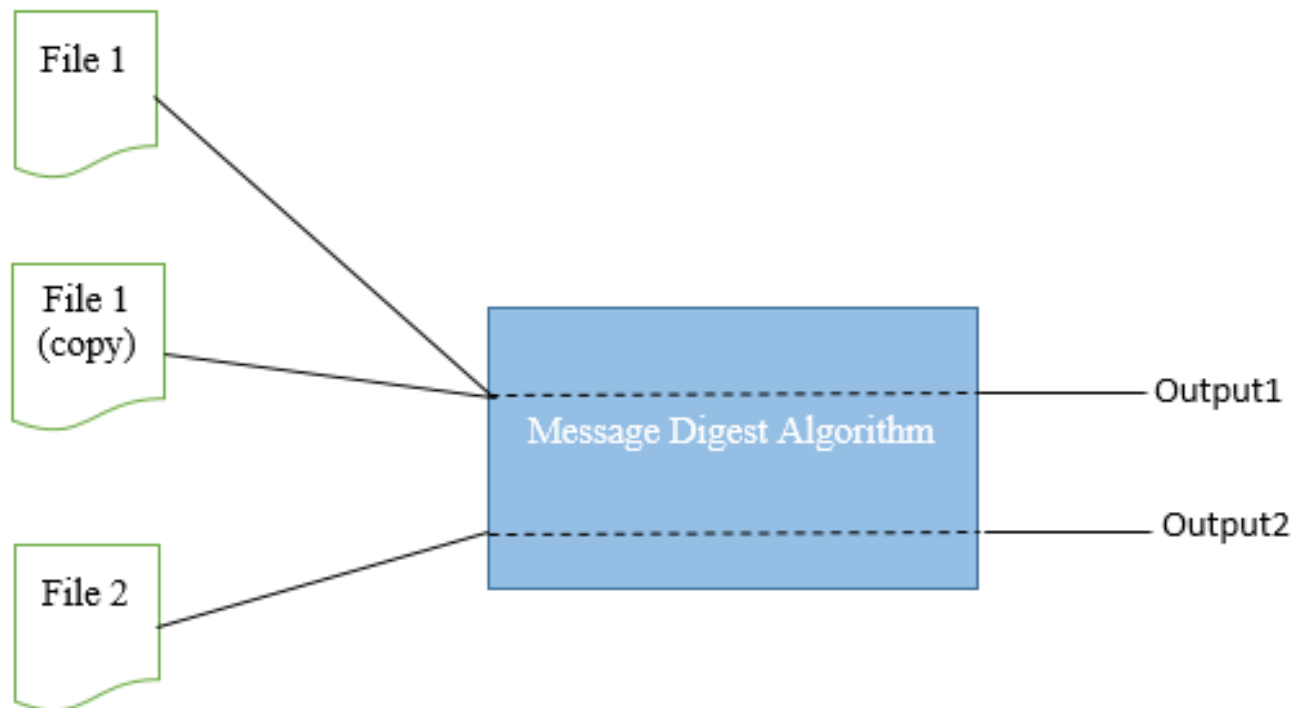
Forensic Soundness – Chain of Custody

cmdLabs Continuity of Possession Form				
Case Number:	2010-05-27-00X		Client/Case Name:	Digifinger Intrusion
Evidence Type:	hard drive		Evidence Number:	0023
Details:	Mac storage <network share>			
Date of Transfer	Transferred From	Transferred To	Location of Transfer	Action Taken by Recipient
5/27/10	<small>signature</small>  <small>print name</small> Sam Spade	<small>signature</small>  <small>print name</small> Philip Maulou	Digifinger HQ Linthicum MD	Collected evidence for examination
	<small>signature</small> <small>print name</small>	<small>signature</small> <small>print name</small>		

From: Digital Evidence and Computer Crime 3rd edition, Eoghan Casey

Forensic Soundness – Evidence Integrity

- How do we show that the digital evidence was not altered from the time it was collected?



Forensic Soundness – Evidence Integrity



- MD5
- SHA-1
- SHA-256

Forensic Soundness – Evidence Integrity

- Why message digest algorithm on its own does not indicate that the evidence is reliable?

Isolate



- *isolate* the analysis environment from both the suspect data and the outside world

Correlate

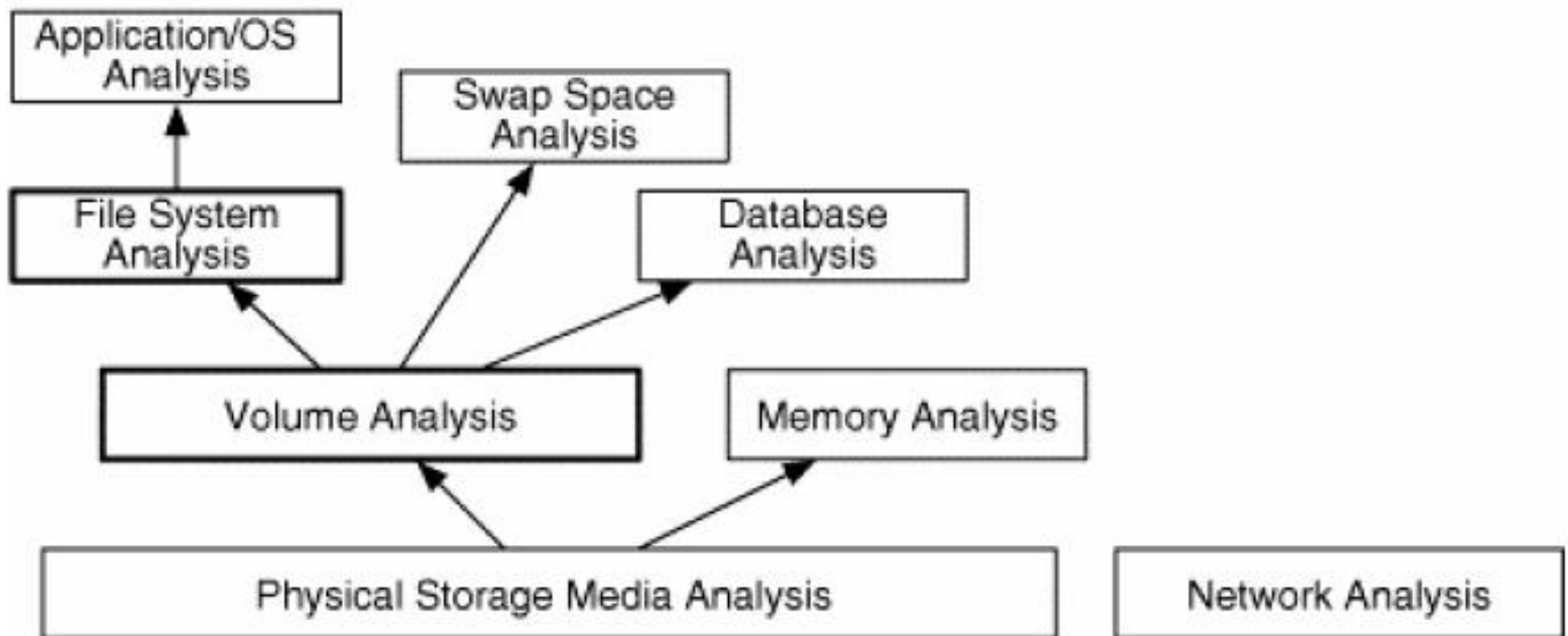


- correlate data with other independent sources



Data Analysis

Data Analysis



File System Forensic Analysis, 2nd edition, Brian Carrier

References



1. File System Forensic Analysis, 2nd edition, Brian Carrier, 2005.
2. Handbook of Digital Forensics and Investigation, Eoghan Casey, 2009.
3. Digital Evidence and Computer Crime, 3rd edition, Eoghan Casey, 2011.
4. Digital Archaeology: The Art and Science of Digital Forensics, Michael W Graves, 2013.