

CSE 469: Computer and Network Forensics

Topic 1: Forensics Intro

General Forensic Science

Definition

- Forensic Science is the application of science to those criminal and civil laws that are enforced by police agencies in a criminal justice system.

What is Forensics / Forensic Science

- Chemistry
 - Biology
 - Physics
 - Geology
-
- Places physical evidence into a professional discipline.

History of Forensics / Forensic Science

- Sir Arthur Conan Doyle
- Popularized physical detection methods in a crime scene
- Developed the character Sherlock Holmes
 - Publications from 1887 to 1927

History of Forensics / Forensic Science



ELEMENTARY



Forensics / Forensic Science



Alphonse Bertillon (1853 – 1914)

- Father of Criminal Detection
- Devised the first scientific system of personal identification, using body measurements known as anthropometry in 1879



Francis Galton (1822 – 1911)

- Conducted the first definitive study of fingerprints and their classification.
- 1892 – Treatise entitled *Finger Prints*



Leone Lattes (1887 – 1954)

- Devised a simple procedure for determining the blood type (A,B,O,AB) of a dried bloodstain



Calvin Goddard (1891 – 1955)



- Used a comparison microscope to determine if a bullet was fired from a specific gun
- Published study of “tool marks” on bullets

Sir Alec Jeffreys

- Early 1980s: Restriction Fragment Length Polymorphism (RFLP)
- DNA fingerprinting



Printer & Scanner Forensics



October 12, 2004

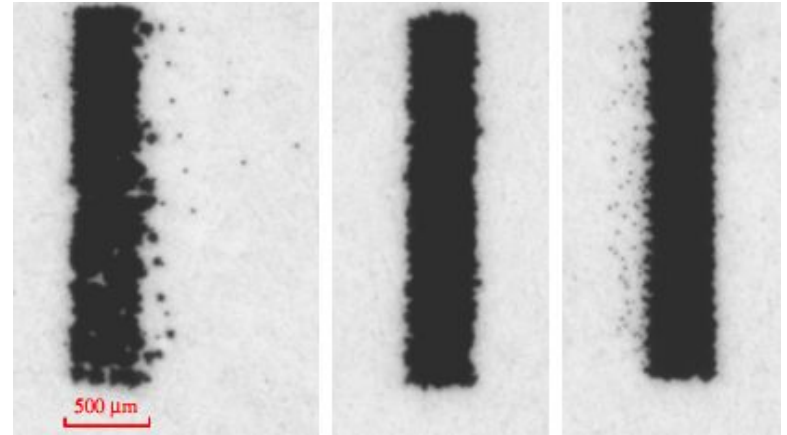
Printer forensics to aid homeland security, tracing counterfeiters

WEST LAFAYETTE, Ind. – Researchers at Purdue University have developed a method that will enable authorities to trace documents to specific printers, a technique law-enforcement agencies could use to investigate counterfeiting, forgeries and homeland security matters.

The technique uses two methods to trace a document: first, by analyzing a document to identify characteristics that are unique for each printer, and second by designing printers to purposely embed individualized characteristics in documents.



"banding"
[Download photo](#)
caption below



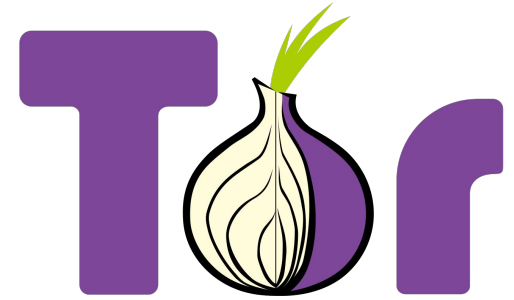
Computer Crime

What is Computer Crime?

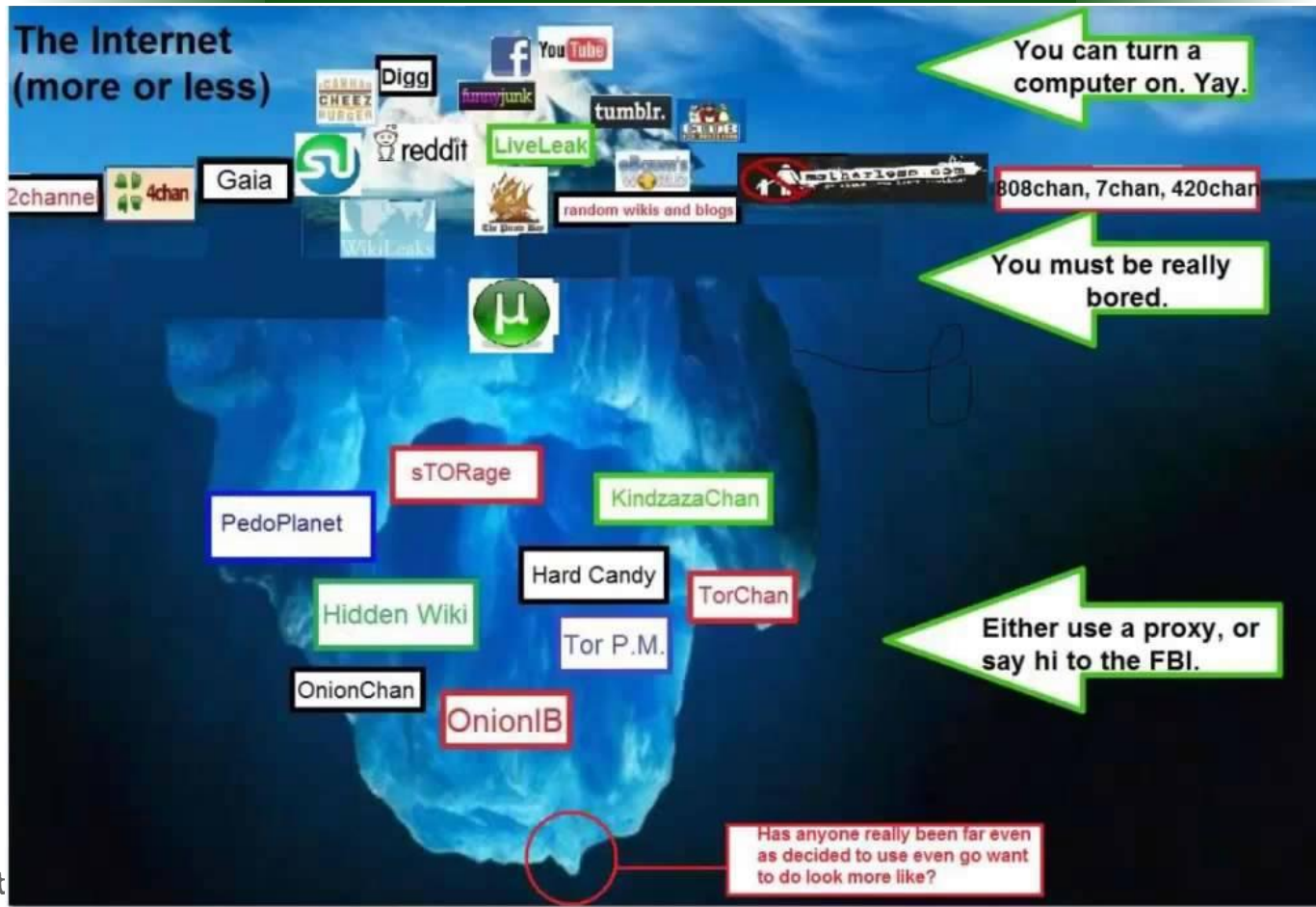
- A crime in which technology plays an important, and often a necessary, part.
- What about the computer?
 - the tool used in an attack
 - the target of an attack
 - used to store data related to criminal activity
- **3 generic categories**
 - Computer assisted
 - e.g., fraud, child pornography
 - Computer specific or targeted
 - e.g., denial of service, sniffers, unauthorized access
 - Computer incidental
 - e.g., customer lists for traffickers

Tor


- The Onion Router
- For anonymous Internet communication
- Bypass censorship
- Host web sites that can only be visited via Tor
- Darknet
 - Not indexed by Google (surface web)
 - Not the same as Deep web (facebook)



Tor



Silk Road



Silk Road

anonymous marketplace


messages(0) | orders(0) | account(\$0.00) | settings |

search

1 day 00 hrs 00 mins 00 secs until **Four Twenty!!!**


Shop by category:

- Drugs(2788)
 - Cannabis(796)
 - Dissociatives(48)
 - Ecstasy(307)
 - Opioids(211)
 - Other(98)
 - Prescription(541)
 - Psychedelics(366)
 - Stimulants(235)
- Apparel(28)
- Books(286)
- Computer equipment(13)
- Digital goods(219)
- Drug paraphernalia(74)
- Electronics(17)
- Fireworks(1)



170\$ pecunix

\$39.23




1 OZ of Jamaican Oil

\$73.91

Need Bitcoins ?


Need bitcoins? Bitcoins for your...

\$0.00




20 Grams of MDMA crystals

\$124.60



HYDRO 10/325 NORCO/LORATAB

\$1.75V...



1oz - "Swazi Red" (Rooibaard)...

\$29.61

News:

- Who's your **favorite?**
- Acknowledging **Heroes**
- A new annonym market **The Army!**
- State of the F Address**

Silk Road

- Silk Road did **\$1.2 billion** worth of business between February of 2011 and July of 2013, the FBI says, earning Dread Pirate Roberts **\$79.8 million** in commissions using current Bitcoin rates.
- Ross Ulbricht (born in 1984), alleged operator of the Silk Road Marketplace, arrested by the FBI on Oct 1, 2013.



= ?



Other Underground Markets

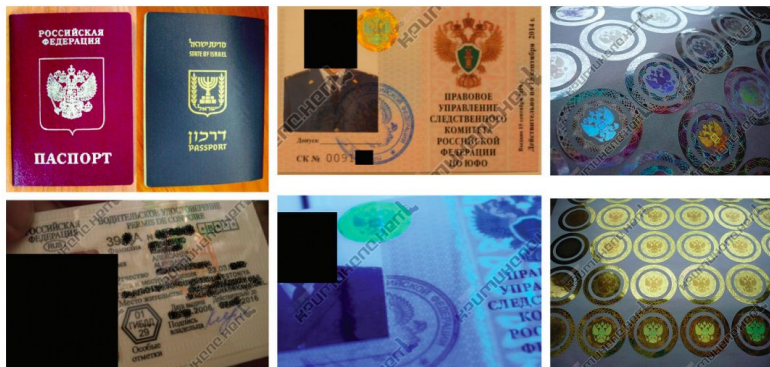
Table 2. Summary of data from the 12 forums.

Name	Subforums	Dates covered	No. of threads
Forum1	Market	Dec. 2010 to Jan. 2011	56
Forum2	Russian speaking carders	Dec. 2010 to Jan. 2011	118
Forum3	Hacking		
Forum4	Buy/Sell		
Forum5	Flea market		
Forum6	Banks		
Forum7	Russian		
Forum8	Verifiers		

(Offering The Best Skin Dumps, Tracks 1/2 Bank Login And Cc Only ...
 Hello brothers,
 I am CC Dumps And Bank Login Vendor.
 We are ready introduce you our service. We have dumps only with ORIGINAL TRACK1+TRACK2. Approval rate
 100% and guarantee they will work good, not for 20% or 100%.
 We accept:
 Western money,
 Liberty reserve,
 PayPal,
 Western union.
 We work 24/7 and have excellent customers support.
 (a)
 > ad New GSM skin for NCR / thumb GSM skin are NCR
 > bo Present to you the invention skin under the NCR.
 > ca Skin installed instead of green antiskin, which cut 45 seconds. After that, the same place skin installed with a
 > cc Continuous operation of the device - the third day.
 > de The transmitted information is encrypted.
 > dn Readability on both sides, with continuous holding readability 99%. Does not read the card when you stop, do not
 > du button labels do any.
 > ha On disorders, wishing to work on rnc, a chip sews most of the files of Russian banks, they have processed
 > ml Lock "smiling" as the original with different viewing angle.
 > od The device looks transparent.
 > pl The rest say photos.
 > se The initial price of the first devices - \$K USD. With a large demand will increase. Work through a guarantee. Completion of the transaction receipt and verification of Paula ustroyevuyu product in
 > sp stock ready to ship.
 > sp Also shares the technology, in whole or in parts, or help you with development. Expensive.
 > sr
 (b)
 > trf



Fake IDs



Ads

BEST QUALITY DUMPS

VISA ALWAYS APPROVED DUMPS ON

Продажа свежих Европейских CC

(a)

Массовые рассылки до 1 миллиарда в день!

ПЕЧАТИ ШТАМПЫ БЕЗ ЛИШНИХ ВОПРОСОВ

(b)

ГОЛОГРАММЫ НАНЕСЕНИЕ ТЕКСТА

(c)

ROYAL SUPPORT2 ICQ: [redacted]

WORLDWIDE DUMPS

GRACO DUMPS

SELLING SERVICE WORLDWIDE

Rent-A-Botnet

КАЧЕСТВЕННЫЙ DDOS СЕРВИС / DDOS SERVICE [QUALITY SERVICE DDOS / DDOS SERVICE]

[Good day dear citizens! доброго времени суток уважаемые жители]

[To your attention a quality service DDOS! У вас вниманию качественный DDOS сервис]

[We the best value for money! У нас наилучшее соотношение цены и качества!]

[Take any project regardless of the subject matter of the target! Берем любые проекты независимо от тематики нишеми!]

[Wholesale customers individual conditions! Оптовые заказчики индивидуальные условия!]

[Average price of service from \$ 50 per night depends on the complexity of the attacked site] в среднем цены на сервис от 50\$ в сутки зависит от сложности атакуемого сайта

Принимая платежей принимаются через системы:

В сети практически круглосуточно!

Команды:

[+] к началу http атаки хоста

[+] к началу icmp атаки хоста

[+] к началу атаки на порт

[+] к началу udp атаки

[+] к началу syn атаки

[+] работа пингов отключена до идеала

Наши контакты:

Иск:

Проверки пройдены:

Сдам/Продам ботнеты Оптика [Rent / Buy Optima botnets]

Цена:

Аренда сутки 30\$

Продажа 100\$ (не барыничаю, продаю свои, на своем [redacted] 4 версии Привата)

На продажу/аренду 12 свободно

Аренд/Продажа только через гарант или по Промокоду (Заранее Админки на счету)

DDOS Услуги, Ddos сервис, Ddos service, ddos Site, ddos атака, ddos attack, заказать Ddos, заказать Ddos, ddos сервис, услуги ddos, заказать ddos

How big is the problem?

- Average armed bank robbery
 - Nets \$7,500 (\$60M annual)
 - 16% of money recovered
 - **80%** of offenders are behind bars
- White collar computer crimes take in about \$10B annually
 - Less than **5%** offenders go to jail
 - Juries consider this a non-violent crime
 - Criminal statutes vary internationally

How big is the problem?

- Billions of pwned accounts.
- Thousands (millions?) of breaches.
- What really scares me:
 - How will the **aggregation** of all my breached information be used against:
 - Me?
 - My family?
 - My employer?
 - My country?
 - My criminal record (or lack thereof)?
 - ...

'--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address pwned?

Generate secure, unique passwords for every account [Learn more at 1Password.com](#)

Why 1Password?

335	5,688,340,657	86,223	93,963,569
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

711,477,622	Onliner Spambot accounts
593,427,119	Exploit.In accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
359,420,698	MySpace accounts
234,842,089	NetEase accounts
164,611,595	LinkedIn accounts
152,445,165	Adobe accounts
131,577,763	Exactis accounts
125,929,660	Apollo accounts

Recently added breaches

242,715	GoldSilver accounts
205,242	Mappery accounts
575,437	Bombuj.eu accounts
36,916	Hub4Tech accounts
66,147,869	You've Been Scraped accounts
66,308	AerServ accounts
776,648	ForumCommunity accounts
265,410	Technic accounts
44,320,330	Data & Leads accounts
9,363,740	Adapt accounts

It Gets
Worse...

Brief History of Digital Forensics

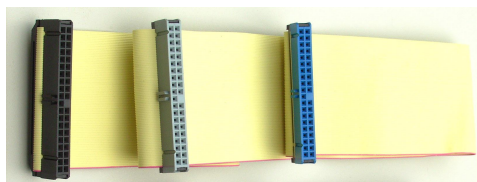
- Roots of digital forensics go back to roughly 1970, but...
 - Originally data recovery
 - Late 1980s - Norton & Mace Utilities provided "Unformat, Undelete."
- Early days were marked by:
 - Diversity — Hardware, Software & Application
 - Proliferation of file formats
 - Heavy reliance on time-sharing and centralized computing
 - Absence of formal process, tools & training
- Forensics of end-user systems was hard, but it didn't matter much.
 - Most of the data was stored on centralized computers.
 - Experts were available to assist with investigations.
 - There wasn't much demand!

Law Enforcement Investigations

- Until **1993**, laws defining computer crimes did not exist
- Analogies between existing law and cyber crime were incomplete and often flawed
- States have since added specific language to their criminal codes to define crimes that involve computers
- Crimes that have proliferated because of computers:
 - Child pornography (Easy access and storage, Anonymity)
 - Child abuse & bullying
 - Financial fraud
 - Identity theft
 - Coordinating drug activity

The Golden Age of Digital Forensics: 1999-2007

- Widespread use of Microsoft Windows, especially Windows XP
- Relatively few file formats:
 - Microsoft Office (.doc, .xls & .ppt)
 - JPEG for images
 - AVI and WMV for video
- Most examinations confined to a single computer belonging to a single subject
- Most storage devices used a standard interface.
 - IDE/ATA
 - USB

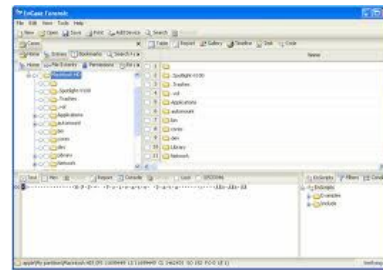


The Golden Age of Digital Forensics: 1999-2007

- This Golden Age gave us good tools and rapid growth.

- Commercial tools:

- FTK
- EnCase



- Open source tools:

- The Sleuth Kit



- Content Extraction Toolkits

Oracle Outside In Technology

Outside In Technology is a suite of software development kits (SDKs) that provides developers with a comprehensive solution to access, transform and control the contents of over 500 unstructured file formats. Each SDK within the suite is optimized to solve a particular problem but they are highly flexible and interoperable. Developers can quickly implement any combination of the Outside In SDKs to provide exactly the right functionality in their application while minimizing integration effort and code footprint. The SDKs offer a wide range of options to give the developer programmatic control of their workflow and output. Thorough documentation and sample applications with source code are included to further accelerate implementation.



Digital Forensics Crisis (1)

1. Dramatically increased costs of extraction and analysis
 - Huge storage, non-removable flash, proliferation of operating systems and file formats, multiple devices and services with important data.
2. Encryption and cloud computing
 - Pervasive encryption, end-user systems don't have the data, RAM-based malware, and new legal challenges.

Digital Forensics Crisis (2)

3. Mobile phones

- Bit-copies can no longer be the gold standard, difficult to validate tools against thousands of phones or millions of apps, no standard extraction protocols.

4. RAM and hardware forensics is really hard

- Malware can hide in many places: disk, BIOS, firmware, RAID controllers, GPU, motherboard...

5. Tools and training simply can't keep up!

Digital Forensics: Basics

Digital Forensics: Objectives (1)

- Digital forensics involves data retrieved from a suspect's:
 - Hard drive
 - Other storage media also:
 - Cell phones
 - Flash drives
 - Cloud services
 - Cars
 - Thermostats
 - Smart speakers

NOTE: The data might be

- Hidden
- Encrypted
- Fragmented
- Deleted
- Outside the normal file structure

Digital Forensics: Objectives (2)

- Figure out *what* happened, *when*, and *who* was responsible.
- Computer forensics is a discipline dedicated to the collection of computer evidence for judicial purposes.
 - Source: EnCase Legal Journal
- Computer forensics involves the preservation, identification, extraction, documentation and interpretation of computer data.
 - Source: Kruse and Heiser, Computer Forensics Incident Response Essentials
- Must be able to show proof

Understanding Digital Forensics

- Digital forensics involves:
 - a. Obtaining and analyzing
 - b. digital information
 - c. for use as evidence
 - d. in civil, criminal, or administrative cases.
- Critical condition:
 - a. Obtaining evidence covered by the **Fourth Amendment to the U.S. Constitution**
 - b. **Protects everyone's rights** to be secure in their person, residence, and property **from search and seizure.**

Fourth Amendment

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.



APR- 4-97 TUE 16:37 P. 02

AD 106 (Rev. 5/97) Affidavit for Search Warrant

United States District Court
WESTERN DISTRICT OF WASHINGTON

MAR 28 1997

CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT TACOMA

**APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT**

CASE NUMBER: 97-5025m

In the Matter of the Search of
(Place, address or brief description of person or property to be searched)

7214 Corredor Road
Vancouver, Washington

I, Jeffrey Gordon, being duly sworn depose and say:

I am a(n) Inspector with the Internal Revenue Service and have reason to believe that () on the person or (X) on the property or premises known as (name, description and/or location)

See Attachment A, attached hereto and incorporated herein

in the Western District of Washington there is now concealed a certain person or property, namely:
(Describe the person or property to be seized)

See Attachment B, attached hereto and incorporated herein

Which is (state type or more basis for search and seizure as forth under Rule 41(b) of Criminal Procedure)

evidence of threats, assaults, obstruction, intimidation, solicitation of murder, false statements, and the unlawful use of false social security numbers

concerning a violation of Titles 26, 42, and 18 United States Code, Section(s) 7212(a), 408, 111, 115, 1505, 1959 and 1001 . The facts to support the issuance of a Search Warrant are as follows:

See attached Affidavit of Jeffrey Gordon, attached hereto and incorporated herein

Continued on the attached sheet and made a part hereof. (X) Yes () No

Signature of Affiant
Jeffrey Gordon
JEFFREY GORDON

Sworn to before me, and subscribed in my presence

March 28, 1997 at 7:02am at Tacoma, Washington
Date City and State

J. KELLEY ARNOLD
United States Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer

USA00 No. 9602582

1

Bottom Line

Searching a person's property
is NOT a trivial matter

Digital Forensics vs Data Recovery

- Data recovery
 - Retrieving data accidentally deleted
 - Damaged or destroyed (fire, power failure, etc.)
 - User WANTS it back
- Digital forensics
 - Retrieving data the user *deliberately obscured*
 - User DOESN'T want it back

Types of Digital Forensics

- Disk Forensics
- Network Forensics
- Email Forensics
- Memory Forensics
- Malware Forensics
- Web Forensics
- Internet of Things (IoT) Forensics
- Cloud Forensics
- Car Forensics
- ...

Where is the evidence?

- Types of data we work with:
 - **Archival**: Data stored on backup tapes.
 - **Active**: Data that is currently seen by the operating system.
 - **Forensic**: Data that has been removed from the operating system's view, also known as unallocated space.

Need to Know

- File system and operating system
 - How a PC saves a file to disk
 - What happens when you delete a file?
 - Data is not changed
 - OS indicates that clusters used by the file are available for reuse
- Understanding Data
 - Hex editor
 - Binary analysis
- Basic OS-level commands are useful and critical

Forensic Tool Kit & System



Forensic Software

- Clean Operating System(s)
- Disk Image Backup Software
- Search & Recovery Utilities
- File Viewing Utilities
- Cracking Software
- Archive & Compression Utilities
- And so on

Public vs Private Sector Investigations

Public Investigations

- **Government agencies** are responsible for criminal investigations and prosecution.
- The law of search and seizure protects the rights of all people, including people suspected of crimes.

APR - 4-97 TIME 16:37 P.02

FD-204 (Rev. 7-16-93) Affidavit for Search Warrant

United States District Court
WESTERN DISTRICT OF WASHINGTON

CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT TACOMA

MAR 28 1997

APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT

CASE NUMBER: 97-5025m

In the Matter of the Search of
(Place address or kind description of person or property to be searched)

7214 Corregidor Road
Vancouver, Washington

I, Jeffrey Gordon, being duly sworn depose and say:

I am AKA Inspector with the Internal Revenue Service and have reason to believe that () on the person or (X) on the property or premises known as (place, description, exact location)

See Attachment A, attached hereto and incorporated herein

in the Western District of Washington there is now concealed a certain person or property, namely:
(describe in person or property to be searched)

See Attachment B, attached hereto and incorporated herein

which it seems me or seems best to search and seizure on (state statute Rule 153(a) of Criminal Procedure)

evidence of threats, assaults, obstructions, intimidation, solicitation of murder, false statements, and the unlawful use of force against justice numbers

concerning a violation of Titles 26, 42, and 18 United States Code, Section(s) 7212(a), 408, 111, 115, 1505, 1559 and 1001 . The facts to support the issuance of a Search Warrant are as follows:

See attached Affidavit of Jeffrey Gordon, attached hereto and incorporated herein

Continued on the attached sheet and made a part hereof.

(X) Yes () No

[Signature]
Signature of Affiant
JEFFREY GORDON

Sworn to before me, and subscribed in my presence

March 28, 1997 at Tacoma, Washington
Date City and State

J. KELLEY ARNOLD
United States Magistrate Judge
Name and Title of Judicial Officer

[Signature]
Signature of Judicial Officer

USDCM No. 9602582

Public Investigations

- Public investigation == Law enforcement agency investigation
 - Need to understand laws on computer-related crimes: local city, county, tribal, state/province, and federal.
 - Understand the standard legal process.
 - How to build a criminal case.

Public Investigations

- Historically, computers and networks were seen only as *tools* that could be used to commit crimes of more traditional natures.
 - Analogies between existing law and cyber crime were incomplete and often flawed.
 - States have since added specific language to their criminal codes to define crimes that involve computers.

Criminal Legal Process

- A criminal case follows three stages:
 1. Complaint: Someone files a complaint.
 2. Investigation: A specialist investigates the complaint.
 3. Prosecution : Prosecutor collects evidence and builds a case.

Levels of Law Enforcement Expertise

1. Level 1 (street police officer)
 - Acquiring and seizing digital evidence
2. Level 2 (detective)
 - Managing high-tech investigations
 - Teaching the investigator what to ask for
 - Understanding computer terminology
 - What can and cannot be retrieved from digital evidence
3. Level 3: (digital forensics expert)
 - Specialist training in retrieving digital evidence

Private Sector Investigations

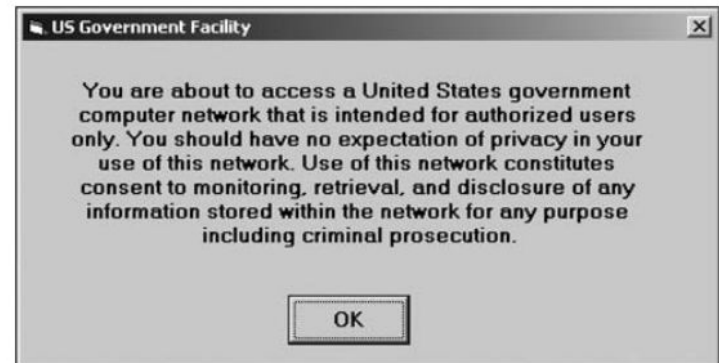
- Deals with private organizations are not governed directly by criminal law or the Fourth Amendment...
- But by **internal policies** that define expected employee behavior and conduct in the workplace.
- Private investigations are usually conducted in civil cases...
- However, a civil case can escalate into a criminal case...
- And a criminal case can be reduced to a civil case.

Private Sector Investigations

- Guiding principle:
 - Business must continue with minimal interruption from the investigation.
- Corporate computer crime examples:
 - Email-harassment
 - Falsification of data
 - Gender/age/... discrimination
 - Embezzlement
 - Industrial espionage

Organizations' Responsibilities

- Organizations must help prevent and address computer crime by:
 - Establishing company policies for acceptable use of systems.
 - Bring your own device (BYOD)
 - Clearly defining what distinguishes private property and company property.
 - Display warning banners.



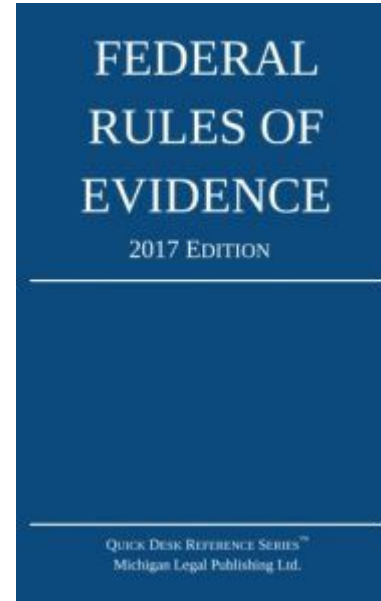
Public vs Private Investigations

- Public investigations search for evidence to support criminal allegations.
- Private investigations search for evidence to support allegations of abuse of a company's assets and criminal complaints.

Rules of Evidence

Rules of Evidence

- Authenticity
- Admissibility
- Completeness
- Reliability / Accuracy



Rules of Evidence: Authenticity

- Can we explicitly link files, data to specific individuals and events?
- Typically uses:
 - Access control
 - Logging, audit logs
 - Collateral evidence
 - Crypto-based authentication
 - Non-repudiation

Rules of Evidence: Admissibility

- Legal rules which determine whether potential evidence can be considered by a court.
 - Common / civil code traditions
 - Adversarial / inquisitorial trials
 - “Proving” documents, copies
- US: 4th amendment rights / Federal Rules of Evidence
- UK: PACE, 1984; “business records” (s 24 CJA, 1988) etc

Rules of Evidence: Completeness

- Evidence must tell a complete narrative of a set of particular circumstances, setting the context for the events being examined so as to avoid “any confusion or wrongful impression.”
- If an adverse party feels evidence lacks completeness, they may require introduction of additional evidence “to be considered contemporaneously with the [evidence] originally introduced.”
 - Wex Legal Dictionary / Encyclopedia. Doctrine of Completeness. Legal Information Institute at Cornell University Law School. URL: https://www.law.cornell.edu/wex/doctrine_of_completeness.

Rules of Evidence: Accuracy

- Reliability of the *computer process* that created the content **not** the data content itself.
- Can we explain how an exhibit came into being?
 - What does the computer system do?
 - What are its inputs?
 - What are the internal processes?
 - What are the controls?

Chain of Custody

- When you are given an original copy of media to deal with, you need to document the handling:
 - Where it was stored
 - Who had access to it and when
 - What was done to it
- Shows that the **integrity** of evidence/data was preserved and not open to compromise.
- Route the evidence takes from the time you find it until the case is closed or goes to court.

Time Attributes

- Allow an investigator to develop a timeline of the incident
- M-A-C
 - mtime: Modified time
 - Changed by modifying a file's content.
 - atime: Accessed time
 - Changed by reading a file or running a program.
 - ctime : changed time
 - Keeps track of when the meta-information about the file was changed (e.g., owner, group, file permission, or access privilege settings).
 - Can be used as approximate *dtime* (deleted time).

The Forensic Process

Forensics Process/Flow (AAA)

- **A**cquisition/Preparation/Preservation
 - Copy the evidence/data without altering or damaging the original data or scene.
- **A**uthentication/Identification
 - Prove that the recovered evidence/data is the same as the original data.
- **A**nalysis/Examination/Evaluation
 - Analyze the evidence/data without modifying it.
- Reporting/ Presentation/ Documentation/ Interpretation

Acquisition

- Confirm the **authority** to conduct analysis/search of media.
- Verify the **purpose** of the analysis and the clearly defined **desired results**.
- Ensure that all software tools utilized for the analysis are **tested and widely accepted** for use in the forensics community.
- Make a **forensic/exact image** of the target media.

Authentication

- Protect the **integrity** of the evidence.
- Maintain **control** until final disposition.
- At Booting, HD disconnection and HD Lock.
- **Verify** the forensic/exact image.

Analysis

What?

- The Operating System
- Services
- Applications/processes
- Hardware
- File System
 - Deleted/Hidden Files/NTFS Streams
- Published Shares/Permissions
- Password Files
- Network Architecture/Trusted Relationships

Issues

- Searching Access Controlled Systems
- Virus Infection
- Formatted Disk
- Corrupted Disk
- DiskWipe or Degaussed Media
- Defragmented Disk
- Cluster Boundaries
- Evidence Eliminator

Reporting/Documentation

- The way you communicate the results of your forensic examination of the evidence.
 - Must be written so non-technical personnel can understand.
 - Must be admissible in court.
- Document **EVERYTHING!**
 - The reason you do anything.
 - All details of the scene.
 - Take screenshots or copy files.
 - All applications on the systems.

Note: The textbook has an entire chapter (14) dedicated to report writing... that's how important it is!

Forensics Process/Flow (AAA)

- Acquisition/Preparation/Preservation
 - Acquire the evidence/data without altering or damaging the original data or scene.
- Authentication/Identification
 - Authenticate that the recovered evidence/data is the same as the original data.
- Analysis/Examination/Evaluation
 - Analyze the evidence/data without modifying it.
- Reporting/ Presentation/ Documentation/ Interpretation

A Model for Digital Forensics

- **Role** of digital forensics professional is to gather evidence to prove that a suspect *committed a crime* or *violated a company policy*.
- Need a systematic approach: procedures and checklists.

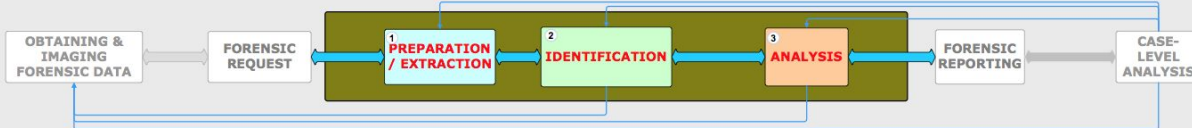


DIGITAL FORENSIC ANALYSIS METHODOLOGY

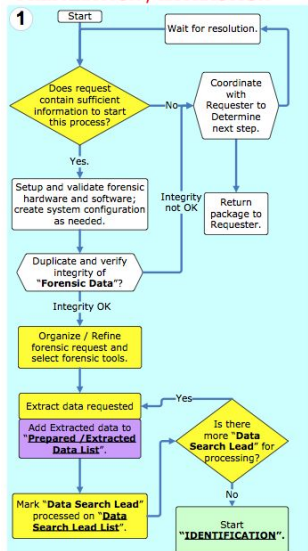
Last updated: August 22, 2007



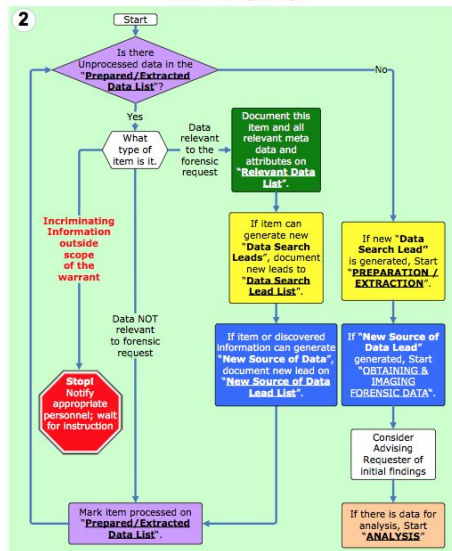
PROCESS OVERVIEW



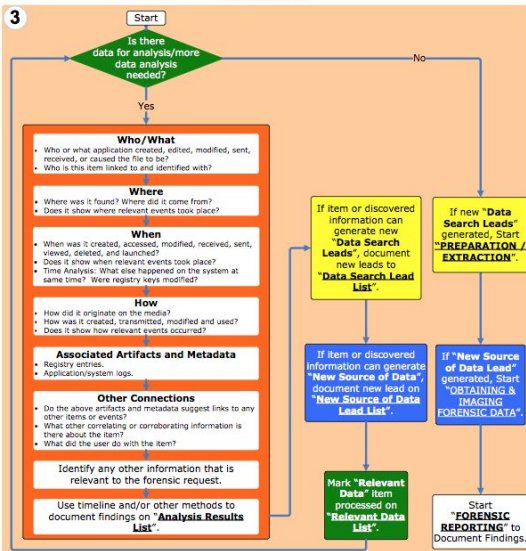
PREPARATION / EXTRACTION



IDENTIFICATION



ANALYSIS



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

LISTS

Search Leads	Comments/Notes/Messages
<p>Data Search Leads</p> <p>Generally this involves opening a case file in the list of drives and importing forensic image file. This could also include recreating a network environment or database to mirror the original environment.</p> <p>Sample Data Search Leads:</p> <ul style="list-style-type: none"> Identify and extract all email and deleted items. Search media for evidence of child pornography. Configure and load seized database for data mining. Recover all deleted files and index drive for review by case agent/forensic examiner. 	<p>Use this section as needed.</p> <p>Sample Note:</p> <p>Please notify case agent when forensic data preparation is completed.</p>

Extracted Data	Comments/Notes/Messages
<p>Prepared / Extracted Data</p> <p>Prepared / extracted data is a list of items that are prepared or extracted to allow identification of data pertaining to the forensic request.</p> <p>Sample Prepared / Extracted Data items:</p> <ul style="list-style-type: none"> Processed hard drive image using Encase or FTK to allow a case agent to stage the contents. Exported registry files and installed registry viewer to allow examiner to examine registry entries. A seized contents file is loaded on a database server ready for data mining. 	<p>Use this section as needed.</p> <p>Sample Note:</p> <p>Numerous files located in C:\Windows\Directory have .avi extensions but are actually Excel spreadsheets.</p>

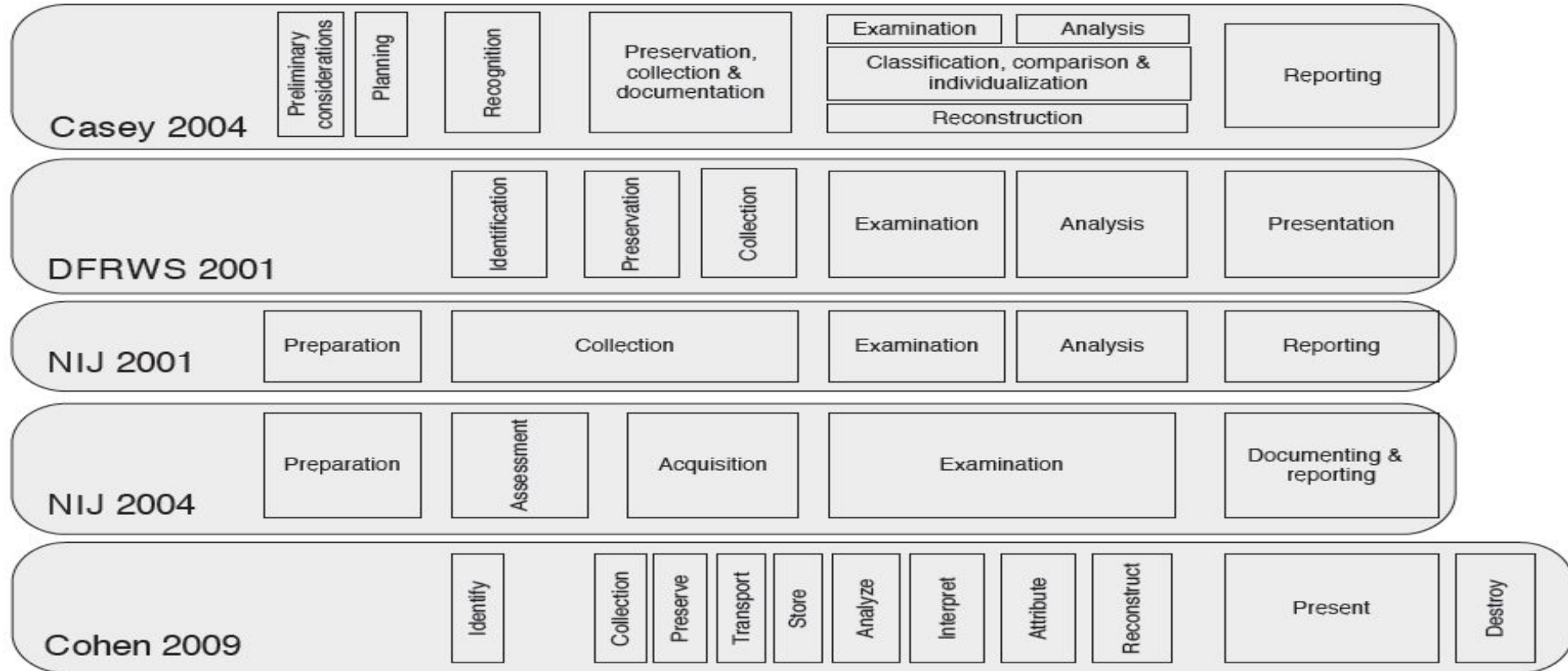
Relevant Data	Comments/Notes/Messages
<p>Relevant Data</p> <p>Relevant Data List is a list of data that is relevant to the forensic request. For example:</p> <ul style="list-style-type: none"> If the forensic request is finding information relating credit card fraud, any credit card number, image of credit card, email discussing online credit card, web cache that shows the date, time and search terms used to find credit card, website. If the forensic request is finding information relating to a specific person, any information that identifies the person, any information that identifies the person's location, any information that identifies the person's activities. 	<p>Use this section as needed.</p> <p>Sample Note:</p> <p>Relevant Data List is a list of items that are relevant to the forensic request. For example: If the forensic request is finding information relating to a specific person, any information that identifies the person, any information that identifies the person's location, any information that identifies the person's activities.</p>

New Source of Data Leads	Comments/Notes/Messages
<p>New Source of Data Leads</p> <p>New Source of Data Lead List is a list of data that should be analyzed to corroborate or further investigative efforts.</p> <p>Sample New Source of Data Leads:</p> <ul style="list-style-type: none"> Email address: [redacted]@com. Server logs from FTP server. Search information for an IP address. Transaction log from server. 	<p>Use this section as needed.</p> <p>Sample Note:</p> <p>Relevant Data List is a list of items that are relevant to the forensic request. For example: If the forensic request is finding information relating to a specific person, any information that identifies the person, any information that identifies the person's location, any information that identifies the person's activities.</p>

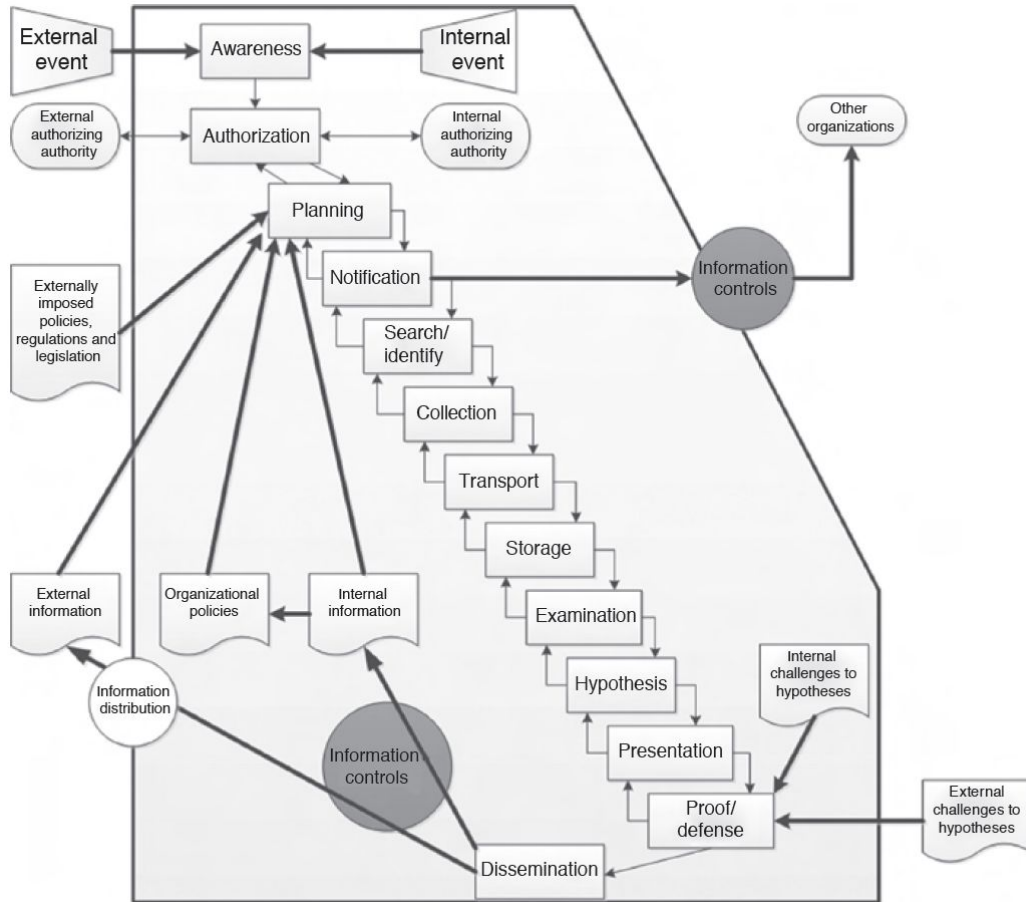
Analysis Results	Comments/Notes/Messages
<p>Analysis Results</p> <p>Analysis Results List is a list of meaningful data that answers the who, what, when, where and how questions in analyzing the forensic request.</p> <p>Sample Analysis Results:</p> <ul style="list-style-type: none"> Relevant Data List is a list of items that are relevant to the forensic request. Relevant Data List is a list of items that are relevant to the forensic request. Relevant Data List is a list of items that are relevant to the forensic request. 	<p>Use this section as needed.</p> <p>Sample Note:</p> <p>Relevant Data List is a list of items that are relevant to the forensic request. For example: If the forensic request is finding information relating to a specific person, any information that identifies the person, any information that identifies the person's location, any information that identifies the person's activities.</p>

Copyright © 2007 by [redacted]

Other Process Models



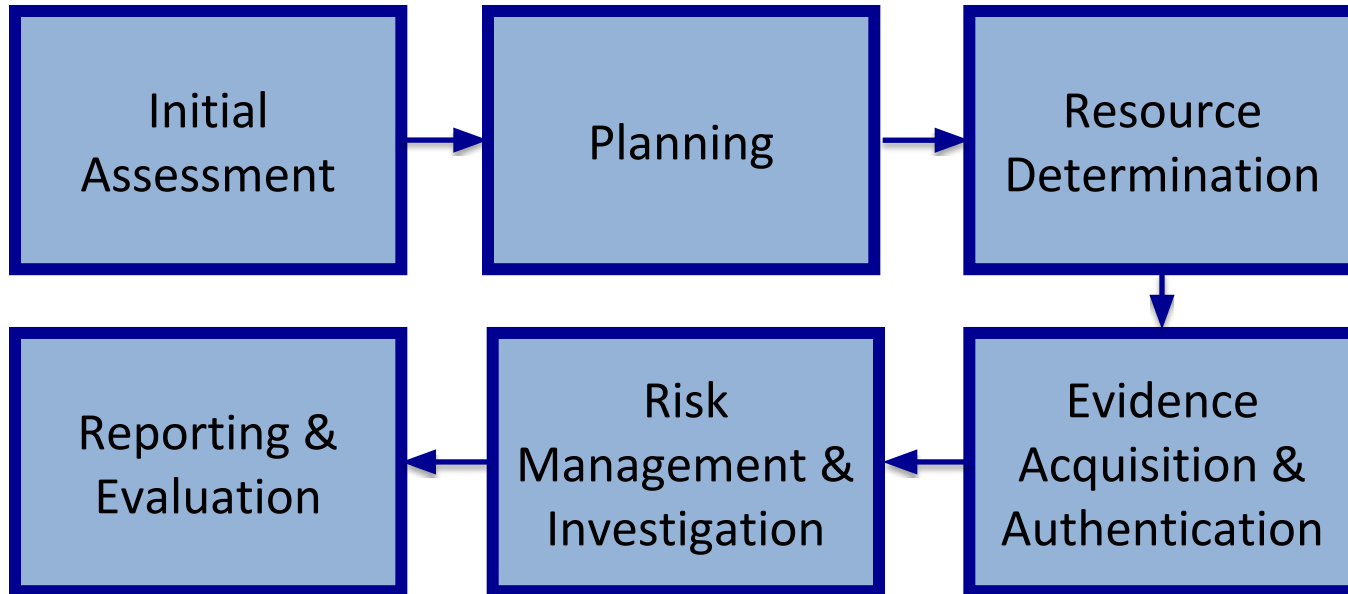
Ó Ciardhuáin's Extended Model



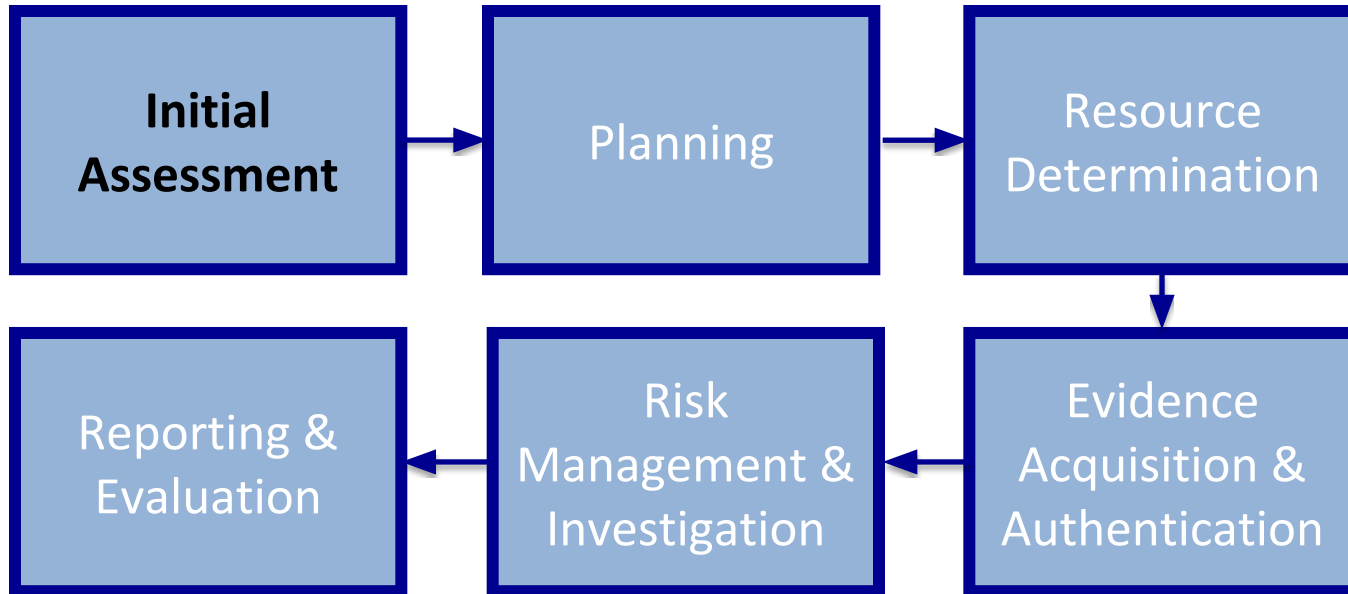
Systematic Approach

- Initial Assessment
- Planning
 - Preliminary design
 - Detailed checklist
- Resource determination
- Evidence acquisition and authentication
- Risk identification and mitigation
- Investigation
 - Evidence analysis and recovery
- Reporting and Evaluation

Systematic Approach



Systematic Approach



Initial Assessment

- Systematically outline the case details
 - Situation:
 - Nature of the case:
 - Specifics of the case:
 - Type of evidence:
 - Operating system:
 - Known disk format:
 - Location of evidence:

Initial Assessment

- Situation: Employee abuse case
- Nature of the case: Side business conducted on the employer's computer
- Specifics of the case: ... Co-workers have complained that he's been spending too much time on his own business and not performing his assigned work duties ...
- Type of evidence: USB flash drive
- Operating system: Windows XP
- Known disk format: FAT16
- Location of evidence: one USB flash drive recovered from the employee's assigned computer

Systematic Approach



Planning

- A basic investigation **plan** should include the following activities:
 - How to collect the targeted evidence
 - Prepare an evidence form and establish a chain of custody
 - How to transport the evidence to a digital forensics lab
 - How to secure evidence in an approved secure container

Planning: Custody Form

- An evidence custody form helps you document what has been done with the original evidence and its forensics copies
- Two types
 - Single-evidence form
 - Lists each piece of evidence on a separate page
 - Multi-evidence form

Single-Evidence Form

Metropolis Police Bureau					
High-tech Investigations Unit					
This form is to be used for only one piece of evidence. Fill out a separate form for each piece of evidence.					
Case No.:				Unit Number:	
Investigator:					
Nature of Case:					
Location where evidence was obtained:					
Item # ID	Description of evidence:	Vendor Name		Model No./Serial No.	
Evidence Recovered by:				Date & Time:	
Evidence Placed in Locker:				Date & Time:	
Evidence Processed by		Disposition of Evidence			Date/Time
Page __ of __					

Chain-of- Evidence Form

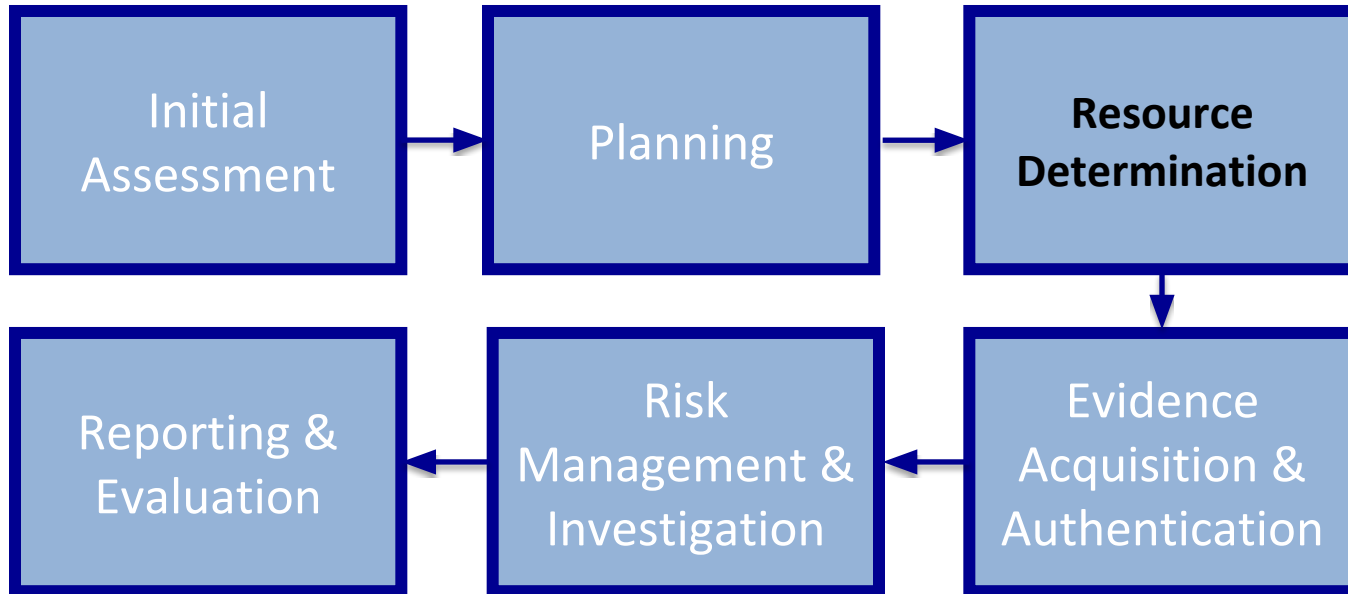
Corporation X Security Investigations			
Case No.:		Investigating Organization:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			
	Description of evidence:	Vendor Name	Model No./Serial No.
Item #1			
Item #2			
Item #3			
Item #4			
Item #5			
Item #6			
Item #7			
Item #8			
Item #9			
Item #10			
Evidence Recovered by:			Date & Time:
Evidence Placed in Locker:			Date & Time:
Item #	Evidence Processed by	Disposition of Evidence	Date/Time
			Page ___ of ___

This form is to be used for one to ten pieces of evidence.

Planning: High-Tech Investigations

- Develop formal procedures and informal checklists
 - To cover *all issues* important to high-tech investigations
 - Employee Termination Cases
 - Internet Abuse Investigations
 - Email Abuse Investigations
 - Attorney-Client Privilege Investigations
 - Must keep all findings confidential
 - Media Leak Investigations
 - Espionage Investigations

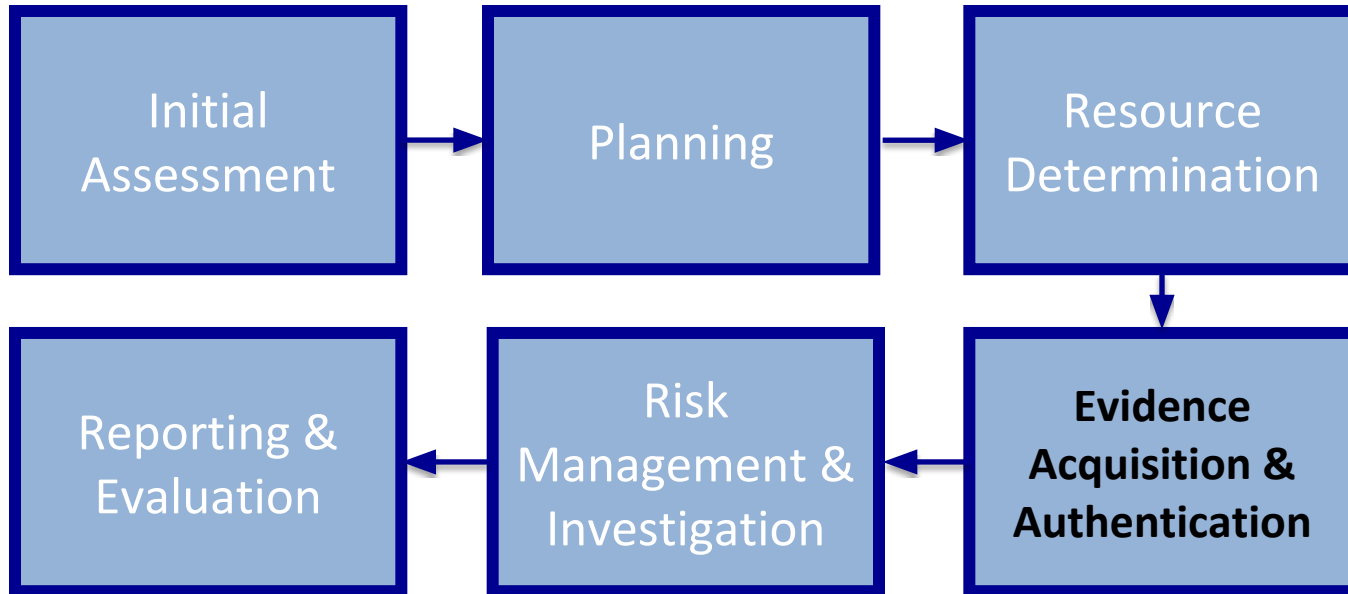
Systematic Approach



Resources

- Gather resources identified in investigation plan
 - Software / hardware
- Items needed
 - Original storage media
 - Evidence custody form
 - Evidence container for the storage media
 - Bit-stream imaging tool
 - Forensic workstation to copy and examine your evidence
 - Securable evidence locker, cabinet, or safe (evidence bag)

Systematic Approach



Acquisition and Authentication

- Maintaining the integrity of the evidence
 - Avoid damaging the evidence
 - Preserve the original evidence
- Steps (example):
 - Place the evidence in a secure container
 - Complete the evidence custody form
 - Create forensics copies
 - Carry the evidence to the digital forensics lab
 - Secure evidence by locking the container

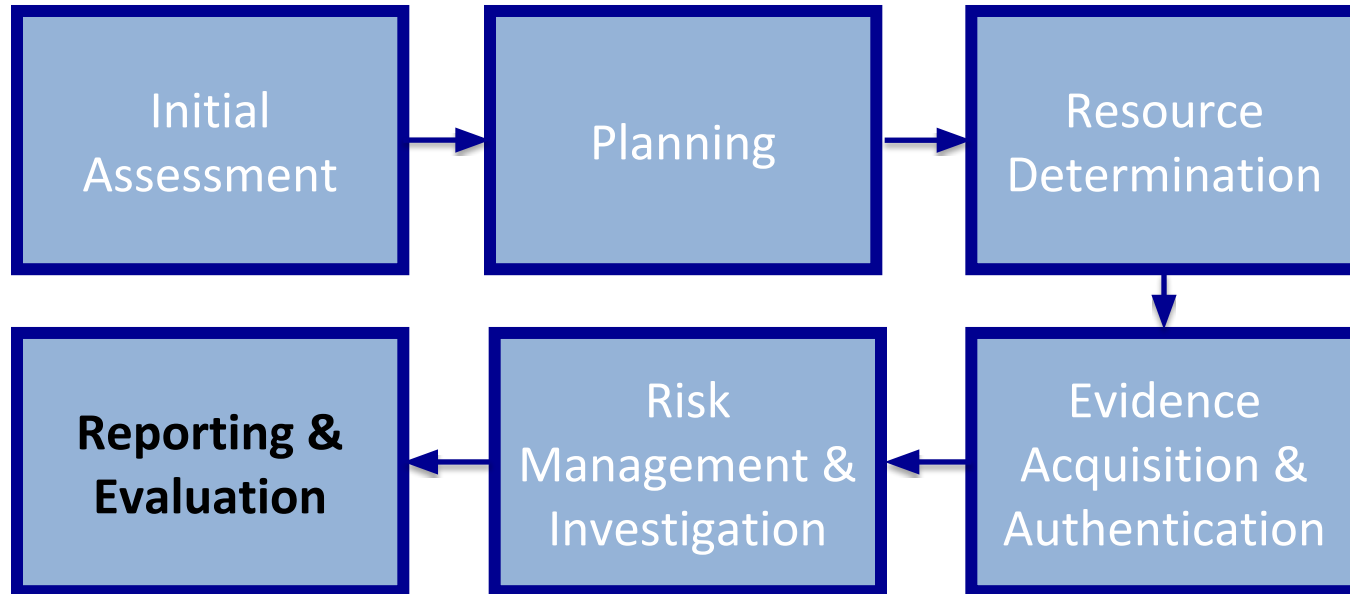
Systematic Approach



Investigation: Discovery, Extraction, and Analysis

- **Discover** and **Extract** data from:
 - Deleted files, File fragments and Complete files
 - Deleted files linger on the disk until new data is saved on the same physical location
- **Analyze** the data
 - Search for information related to the case
 - Can be most time-consuming task
 - Should follow the rules of evidence

Systematic Approach



Reporting and Documentation

- Need to produce a final report
 - State what you did and what you found
- **Repeatable findings**
 - Repeat the steps and produce the same result
- Report should show **conclusive evidence**
 - Suspect *did* or *did not* commit a crime or violate a company policy

Systematic Approach

