Introduction to Cyber Forensics

What This Course Is and Is Not

This course discusses

- *Legal and process issues for cyber investigation*
- *The investigation and analysis of computers, file systems and communication activity*
- *What users have done in the past with a subject computer*

This course DOES NOT discuss in detail

- *Forensics of mobile devices such as cell phones and tablets*
  - This is discussed in a different course, IT-S855 / ITMS555
- *Many concepts and some tools are similar*

Objectives

Discuss the field of digital forensics

Explain how to prepare computer investigations and summarize the difference between public-sector and private-sector investigations

Explain the importance of maintaining professional conduct

Describe how to prepare a digital forensics investigation by taking a systematic approach

Objectives

Describe procedures for private-sector digital investigations

Explain requirements for data recovery workstations and software

Summarize how to conduct an investigation, including critiquing a case

How to find information and potential evidence on a disk or solid-state drive

Deleted, hidden, partial, unknown to OS and file system

Explore how cyber forensics extends to network, memory or any digital medium

What Is Forensics?
(Any Kind of Forensics)

The coherent application of methodological investigative techniques to discover past or ongoing criminal, civil, or administrative violations

Involves developing and then testing hypotheses that answer questions about past or present events

Forensics deals primarily what was or is

What happened in the past or what is happening right now

It does not focus on future (i.e., prevention)

What might happen in the future

What is Digital Forensics?

Digital forensics is forensics applied to cyber events

*It **is** the use of digital technology to perform forensic analysis on digital-based events and situations*

e.g., Searching a digital computer for potential evidence

*It is **not** the use of digital technology to perform forensic analysis on non-digital-based events and situations*

e.g., **Not** the use of a computer in DNA analysis on a strand of hair

Note:

"Digital", "cyber" and "computer" are frequently used interchangeably as regards to forensics

For me, "cyber" is the more encompassing word

An Overview of Digital Forensics

Digital forensics

The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation.

In October 2012, an ISO standard for digital forensics was ratified - ISO 27037 Information technology - Security techniques

An Overview of Digital Forensics

The Federal Rules of Evidence (FRE) was created to ensure consistency in federal proceedings

Signed into law in 1973

Many USA states now have rules that map to the FRE

FBI Computer Analysis and Response Team (CART) was formed in 1984 to handle cases involving digital evidence

By late 1990s, CART teamed up with Department of Defense Computer Forensics Laboratory (DCFL)

An Overview of Digital Forensics

The **Fourth Amendment** to the U.S. Constitution protects everyone's right to be secure from search and seizure

*Separate **search warrants** might not be necessary for digital evidence*

Every U.S. legal jurisdiction has case law related to the admissibility of evidence recovered from computers and other digital devices

Digital Forensics and Other Related Disciplines

Investigating digital devices includes:

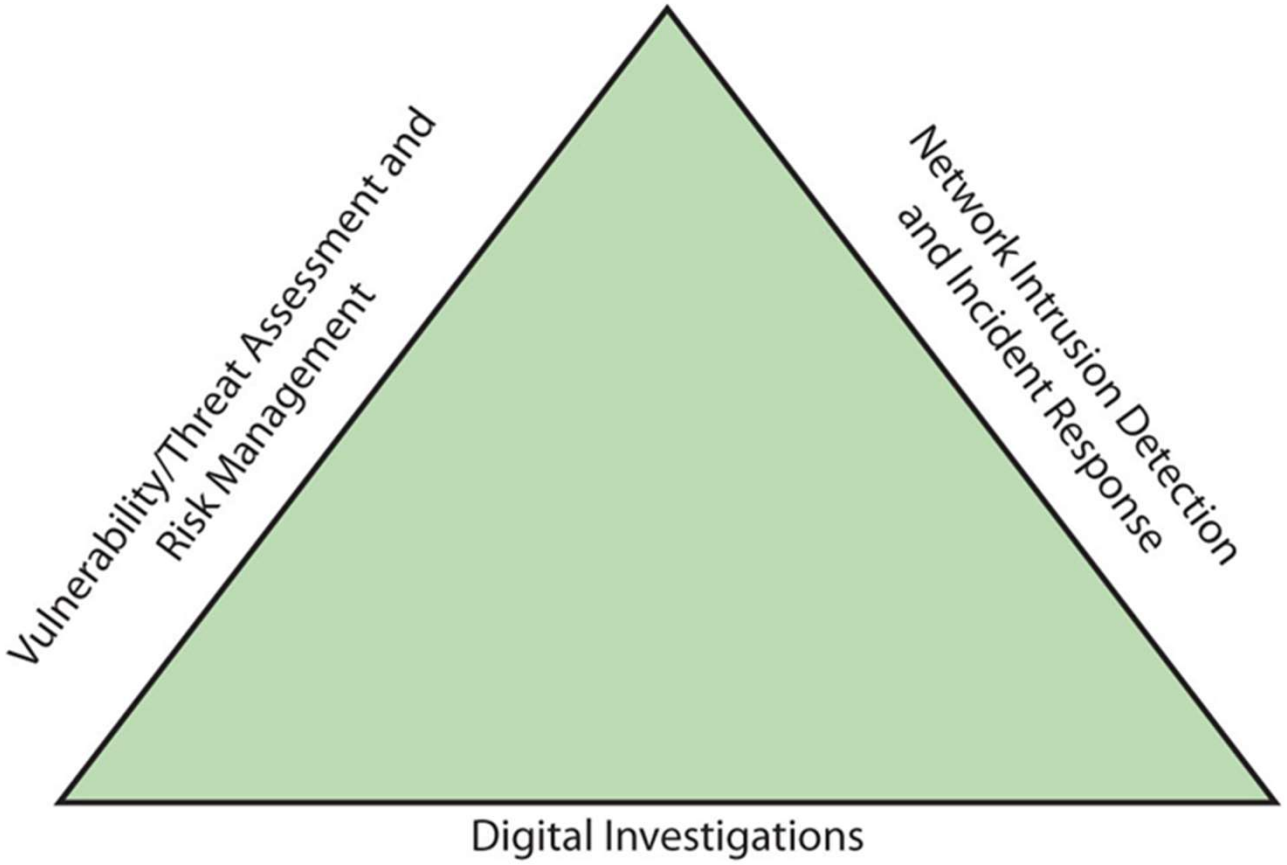
- *Collecting data securely*
- *Examining suspect data to determine details such as origin and content*
- *Presenting digital information to courts*
- *Applying laws to digital device practices*

Digital forensics is different from **data recovery**

- *Which involves retrieving information that was deleted by mistake or lost during events such as a power surge or server crash*

Digital Forensics and Other Related Disciplines

Forensics investigators often work as part of a team, known as the **investigations triad**



Digital Forensics and Other Related Disciplines

Vulnerability/threat assessment and risk management

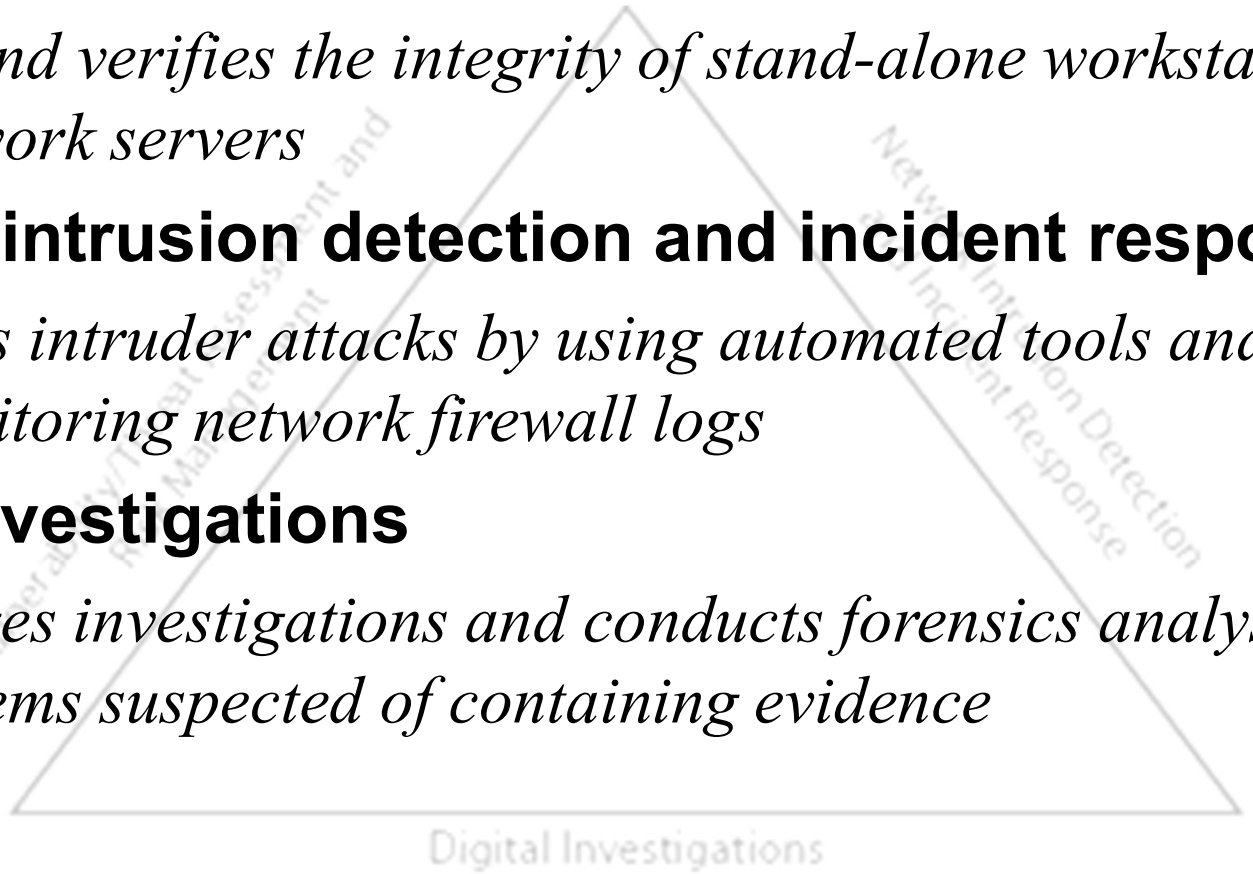
Tests and verifies the integrity of stand-alone workstations and network servers

Network intrusion detection and incident response

Detects intruder attacks by using automated tools and monitoring network firewall logs

Digital investigations

Manages investigations and conducts forensics analysis of systems suspected of containing evidence



A Brief History of Digital Forensics

By the early 1990s, the International Association of Computer Investigative Specialists (IACIS) introduced training on software for digital forensics

IRS created search-warrant programs

ASR Data created Expert Witness for Macintosh and Windows

*This later evolved into **EnCase***

ILook Investigator is currently maintained by the IRS Criminal Investigation Division Electronic Crimes Program

Case Law

Existing statutes have not been able to keep up with the rate of technological change

But they are improving

When statutes don't exist, case law is used

Allows legal counsel to apply previous similar cases to current one to address ambiguity in laws

Forensic examiners need to be:

Somewhat knowledgeable of laws

Familiar with recent court rulings on search and seizure in the electronic environment

Developing Digital Forensics Resources

To supplement your knowledge:

Develop and maintain contact with computing, network, and investigative professionals

Join computer user groups in both the pubic and private sectors

Example: **Computer Technology Investigators Network (CTIN)** meets to discuss problems with digital forensics examiners encounter

Example: **High Tech Crime Investigators Association (HTCIA)** . We used to have a student chapter.

Consult outside experts

Professional Conduct

Maintaining Professional Conduct

Professional conduct - includes ethics, morals, and standards of behavior

An investigator must exhibit a high level of professional behavior

Maintain objectivity

Maintain credibility by maintaining confidentiality

Investigators should also attend training to stay current with the latest technical changes in computer hardware and software, networking, and forensic tools

Maintaining Personal Conduct

Personal conduct - includes ethics, morals, and standards of behavior

If your personal conduct can be called into question, this might affect creditability of your forensic work

Types of Forensic Investigations:
The Nelson Text Perspective

Types of Forensic Investigations: *The Nelson Text Perspective*

Digital investigations fall into two categories:

Public-sector investigations

Government agencies
Article 8 in the Charter of Rights of Canada
U.S. Fourth Amendment search and seizure rules

Private-sector investigations

Private organizations
Company policy violations
Litigation disputes

Public Sector Investigations

Public-sector investigations involve government agencies responsible for criminal investigations and prosecution

Fourth Amendment to the U.S. Constitution

Restricts government ***search and seizure***

The Department of Justice (DOJ) updates information on computer search and seizure regularly

Private-sector investigations focus more on policy violations

Public Sector Investigations

When conducting public-sector investigations, you must understand laws on computer-related crimes including:

- *Standard legal processes*
- *Guidelines on search and seizure*
- *How to build a criminal case*

The Computer Fraud and Abuse Act was passed in 1986

- *Specific state laws were generally developed later*

Public Sector Investigations
Following Legal Processes

A criminal investigation usually begins when someone finds evidence of or witnesses a crime

*Witness or victim makes an **allegation** to the police*

Police interview the complainant and writes a report about the crime

Report is processed and management decides to start an investigation or log the information in a police record

This record is a historical database of previous incidents and crimes

Public Sector Investigations

Following Legal Processes

Digital Evidence First Responder (DEFR)

Arrives on an incident scene, assesses the situation, and takes precautions to acquire and preserve evidence

Digital Evidence Specialist (DES)

Has the skill to analyze the data and determine when another specialist should be called in to assist

Affidavit - a sworn statement of support of facts about or evidence of a crime

*Can include **exhibits** that support the allegation*

Private Sector Investigations

Private-sector investigations involve private companies and lawyers who address company policy violations and litigation disputes

Example: wrongful termination, misuse of company items

Businesses strive to minimize or eliminate litigation

Private-sector crimes can involve:

E-mail harassment, falsification of data, gender and age discrimination, embezzlement, sabotage, and industrial espionage

Private Sector Investigations

Businesses can reduce the risk of litigation by publishing and maintaining policies that employees find easy to read and follow

Most important policies define rules for using the company's computers and networks

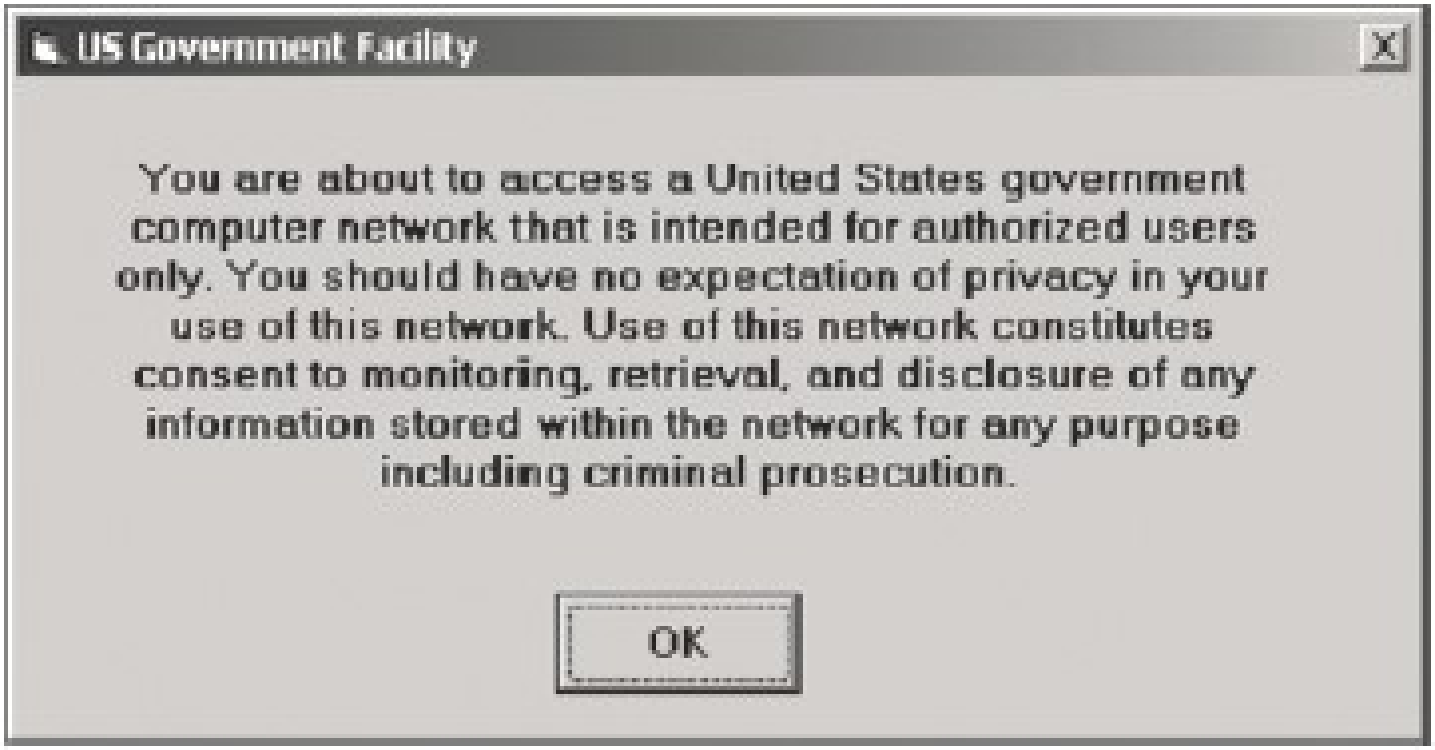
Known as an "Acceptable use policy"

Line of authority - states who has the legal right to initiate an investigation, who can take possession of evidence, and who can have access to evidence

Private Sector Investigations

Business can avoid litigation by displaying a **warning banner** on computer screens

Informs end users that the organization reserves the right to inspect computer systems and network traffic at will



Private Sector Investigations

Sample text that can be used in internal warning banners:

Use of this system and network is for official business only

Systems and networks are subject to monitoring at any time by the owner

Using this system implies consent to monitoring by the owner

Unauthorized or illegal users of this system or network will be subject to discipline or prosecution

Private Sector Investigations

Businesses are advised to specify an **authorized requester** who has the power to initiate investigations

Examples of groups with authority

- *Corporate security investigations*
- *Corporate ethics office*
- *Corporate equal employment opportunity office*
- *Internal auditing*
- *The general counsel or legal department*

Private Sector Investigations

During private investigations, you search for evidence to support allegations of violations of a company's rules or an attack on its assets

Three types of situations are common:

Abuse or misuse of computing assets

E-mail abuse

Internet abuse

A private-sector investigator's job is to minimize risk to the company

Private Sector Investigations

The distinction between personal and company computer property can be difficult with cell phones, smartphones, personal notebooks, and tablet computers

Bring your own device (BYOD) environment

Some companies state that if you connect a personal device to the business network, it falls under the same rules as company property

Types of Forensic Investigations:
Another Perspective

Types of Forensic Cases

Involves obtaining and analyzing digital information for use as evidence in "cases"

Three types of "cases"

- ***Administrative***
- ***Civil***
- ***Criminal***

A Little Bit of Law

Administrative Cases

Violation of some enterprise rule

Usually by a member of the enterprise

Remedy is pursued by and at the discretion of the enterprise

Arbiter comes from within the enterprise

There often is no arbiter

A Little Bit of Law
Civil Cases

Violation of a civil law

A wrong that damages a private citizen or enterprise

The alleged wrong is often committed by an entity that is not a member of the enterprise

The entity can be either a person or another enterprise

Remedy is pursued by and at discretion of damaged party

Arbiter is neither a member of the enterprise nor the entity

e.g., civil court case on patent infringement

Arbiter is usually a civil court judge, jury or legal referee

A Little Bit of Law
Criminal Cases

Criminal

Violation of a criminal law

An offense against the public

Remedy is pursued by & at discretion of the state, which represents the public

Arbiter is usually a legal referee, judge or jury

A Little Bit of Law
Reprise

Administrative: *What's the Violation? The Remedy?*

Violation of some enterprise rule

Remedy pursued by & at the discretion of the enterprise

Civil: *What's the Violation? The Remedy?*

Violation of a civil law

A wrong that damages a private citizen or enterprise

Remedy is pursued by & at discretion of damaged party

Criminal: *What's the Violation? The Remedy?*

Violation of a criminal law

An offense against the public

Remedy is pursued by & at discretion of the state

Forensics and the Law

Our study of forensics focuses on technology

But forensics is closely coupled to legal or organizational rules

Consequently, we must consider

Legal issues

The law (criminal, civil, or both)

Administrative issues

Rules that apply within organizations (e.g., corporate policy)

Criminal Investigations

In criminal investigations a crime is presumed to have been committed

The public is presumed to have been wronged

Protecting evidence always trumps such activities as getting system(s) back in operation

To get systems back online quickly, you almost certainly will destroy evidence

Default: Treat every case as if it will end up in criminal court

Need to make an early assessment about this

Nice in theory but not practical in many cases

Civil Investigations

In civil investigations there may or may not be a crime

Another private entity may feel or have been wronged

Protecting evidence usually trumps getting the system(s) back in operation

Default: Treat most cases as if it will end up in civil court

Notice that the emphasis on protecting evidence is not quite as strong as in the criminal case

Administrative Investigations

In administrative investigations there often is no crime

Instead, there may be a violation of corporate policy

Getting the system(s) back in operation is often more important than securing evidence

To get systems back online quickly, you almost certainly will destroy evidence

Tension

There is always tension between:

The need to get systems restored and operational and

The need to protect evidence

This tension is complicated -- even more so because a violation can morph between *administrative*, *civil* and *criminal* violations

Morphing

A civil or administrative investigation can escalate to a criminal case

A private investigation involving unauthorized used of a corporate computer by an employee may uncover the theft of corporate funds

Conversely a criminal or civil case can become an administrative case if the evidence of a crime or civil violation is weak

Some Legal History

The first laws in the U.S.A. defining computer crimes appeared in 1993

The first of these were state laws

Some states modified existing laws by extended their definitions of crimes such as burglary and theft to include the use of computers for malicious activities

Other states created new laws, leaving their existing laws as is

There are now federal, state, county, and city laws in the U.S.

Some of these laws have yet to be tested in the courts

Legal Jurisdictions

An incident committed in Chicago may not be a city or federal crime but might be an Illinois state crime

Laws and the rules by which forensic investigations must be conducted will vary depending on the legal jurisdiction

Thus, the digital forensic expert must be aware of the laws and likely jurisdiction issues at the beginning of an investigation

Investigation & Individual Rights

There is also frequent and ongoing tensions between

The need to investigate an incident and

An individual's rights

Criminal law in the U.S. protects the rights of the suspect via the U.S. Constitution's Fourth Amendment

Many other countries have laws or rules similar to the 4th Amendment

United States Constitution
Fourth Amendment

The U.S. protects the rights of the all citizens via the U.S. Constitution's 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.***"

In the past, actions by the U. S. federal government may have conflicted with this

Other Countries

Many other countries have similar laws or rules similar to those of the U.S. Constitution

Canadian Charter of Rights and Freedoms

> *"8. Everyone has the right to be secure against unreasonable search or seizure."*

When reading the

> *U.S. Constitution's Fourth Amendment or the Canadian Charter of Rights and Freedoms,*

What question should you ask?

Application of Fourth Amendment

The *Fourth Amendment* applies to public investigations

It often does not apply to private organizations

- *The computer supplied by your employer and used by you both at work and home is not protected*
- *Your personally owned computer, when connected to your company's network is not protected - in Illinois*
- *Your personally owned computer, when not network connected or connected to a public ISP is probably protected*

Search Warrants

Search **Warrant** (required by 4th Amendment)

A legal document that allows law enforcement to search, seize or monitor specified items:

e.g., Office, Home, Telephone, Computer, Place of Business…

For evidence relating to a specified alleged crime

A presumed independent judge must be convinced beforehand that a search warrant is appropriate

A Little USA History

Fourth Amendment Violations

In times of national crisis the U.S. Government has passed laws and/or operated in ways that many say violate the 4th Amendment

Examples

Alien & Sedition Acts: 1798 (John Adams president)

Suspension of Habeas Corpus

1862 (Abraham Lincoln) & early1870s (Ulysses S. Grant president)

Palmer Raids - ~1918 (Woodrow Wilson president)

Japanese Internment - ~1942 (Franklin Roosevelt president)

Patriot Act - 2001 (George W. Bush president)

Alien & Sedition Acts

Enacted in 1798 (John Adams)

In response to an undeclared naval war with France

Extended citizenship naturalization to 14 years

Deport any resident alien considered "dangerous to the peace and safety of the United States"

Apprehend & deport resident aliens if their home countries were at war with the U. S.

Criminal to publish "false, scandalous, and malicious writing" against the U. S. government or its officials

All repealed or "sunsetted" in 1800 or 1801

Habeas Corpus*

Latin: "You shall have the body"

Requires that a person charged with a crime to be brought before a court:

To hear what he/she has been charged with and

To determine, by an independent judge, whether the government has the right to continue detaining them

The individual being held or their representative can petition the court for such a writ

U.S. Constitution, Article 1, Section 9

"The privilege of the Writ of Habeas Corpus shall not be suspended unless, when in Cases of Rebellion or Invasion the public safety may require it."

Suspension of Habeas Corpus*

Suspended in 1862 by Abraham Lincoln for the state of Maryland and parts of some midwestern states

Occurred during U. S. War Between the States (i.e., "Civil War")

Suspended again in early 1870s by President Grant

In parts of South Carolina during the fight against the Ku Klux Klan

Palmer Raids

1918-1920 (President Woodrow Wilson)

Occurred between Nov. 1919 and Feb. 1920)

Shortly after World War I

A. Mitchell Palmer was U.S. Attorney General

There were a number of labor and political tensions, anarchist movements and bombings

The Palmer Raids consisted of a number of large-scale raids on groups of persons considered dissidents

"Red scare" was an issue

The Government arrested over 5000 individuals and deported over 500

The U. S. courts ended the raids in 1920

Japanese Internment

1942 (President Franklin Roosevelt)

During World War II starting about 70 days after Imperial Japan's attack on Pearl Harbor (7 Dec 1941)

Forced the relocation and internment of U.S. citizens and residents of the U.S. if they were partially or wholly of Japanese decent

About 120,000 were sent to "War Relocation Camps"

Justified as a military necessity

Interestingly, the Japanese residents of Hawaii were not "relocated"

In 1988 the U.S. government officially apologized and over $1.6 billion were paid in reparations

Fourth Amendment Violations

Patriot Act - 2001 (President George W. Bush)

- *Passed by U.S. Congress*
- *Section 213: "Authority for Delaying Notice of the Execution of a Warrant"*
  - Gave the federal government increased ability of the to commit surveillance on citizens without proper search warrants

Many of Act's provisions were "sunset" at end of 2005

U.S. Congress reauthorized the Patriot Act in 2006

- *Modest changes*

Search Warrants

The U.S. Presidency has apparently approved certain government agencies executing telephone monitoring in certain circumstances without obtaining warrants

Big "dust-up" in 2006

Continues to be controversial

Also, some argue that the Guantanomo incarcerations violate the writ of habeas corpus

The U.S. supreme Court agreed in some specific cases

And into the future…

End of history lesson!

To Record or Not To Record?

Remember that anything you write down or otherwise record is subject to subpoena

U. S. President Richard Nixon found this out the hard way

i.e., the Watergate tapes & recent H.R. Haldeman records re. Vietnam

Any notes that you make are fair game

Suppose that you have a check list that you use for all your forensic investigations (Seems like a good idea -- right?)

For any investigation, many of the items may not be applicable

Your check off the items that you do in your investigation that you judge to be applicable

Your check list may be subpoenaed

You may be asked in open court why you didn't do one of the unchecked list items

Corporate Investigations

Industrial Espionage

Selling of sensitive company information to competitors

Could be committed by any employee with computer access

National Espionage

Illegally seeking sensitive company or government information by foreign entities

Company Policies

Can be set forth on company computers and networks

Provides a "line of authority" to conduct investigations.

Corporate Investigations

Line of Authority

States in writing who has the corporate right to initiate a corporate investigation

Authorized Requestor

Person or organization authorized to conduct security-related investigations

- Corporate security organization
- Corporate ethics office
- Corporate equal opportunity office
- Internal auditing organization
- The General Counsel
- Legal department

Corporate Investigations

Warning banner

Often provided by company

Informs user that the organization reserves the right to inspect the computer & network traffic

Banner examples

"Access to this system and network is restricted."

"Use of this system & network is for official business use only."

"Systems and networks are subject to monitoring at any time by the owner."

"Using this system implies consent to monitoring by the owner."

"Unauthorized or illegal users of this system or network will be subject to discipline or prosecution."

Wrap-Up
Administrative, Civil & Criminal Issues

This is a course in forensic sciences and technologies

It is not a course devoted to administrative, civil and criminal procedures, policies and laws

Therefore, we will focus on technology and science for almost all of this course after today

But because the above issues determine how technology is applied, we'll return from time to time to these topics in the context of using forensic technologies