Cyber Forensics

The Fascinating World of Digital Evidence

Introduction

Eric Katz

Law Enforcement Coordinator

Purdue Cyber Forensics Lab

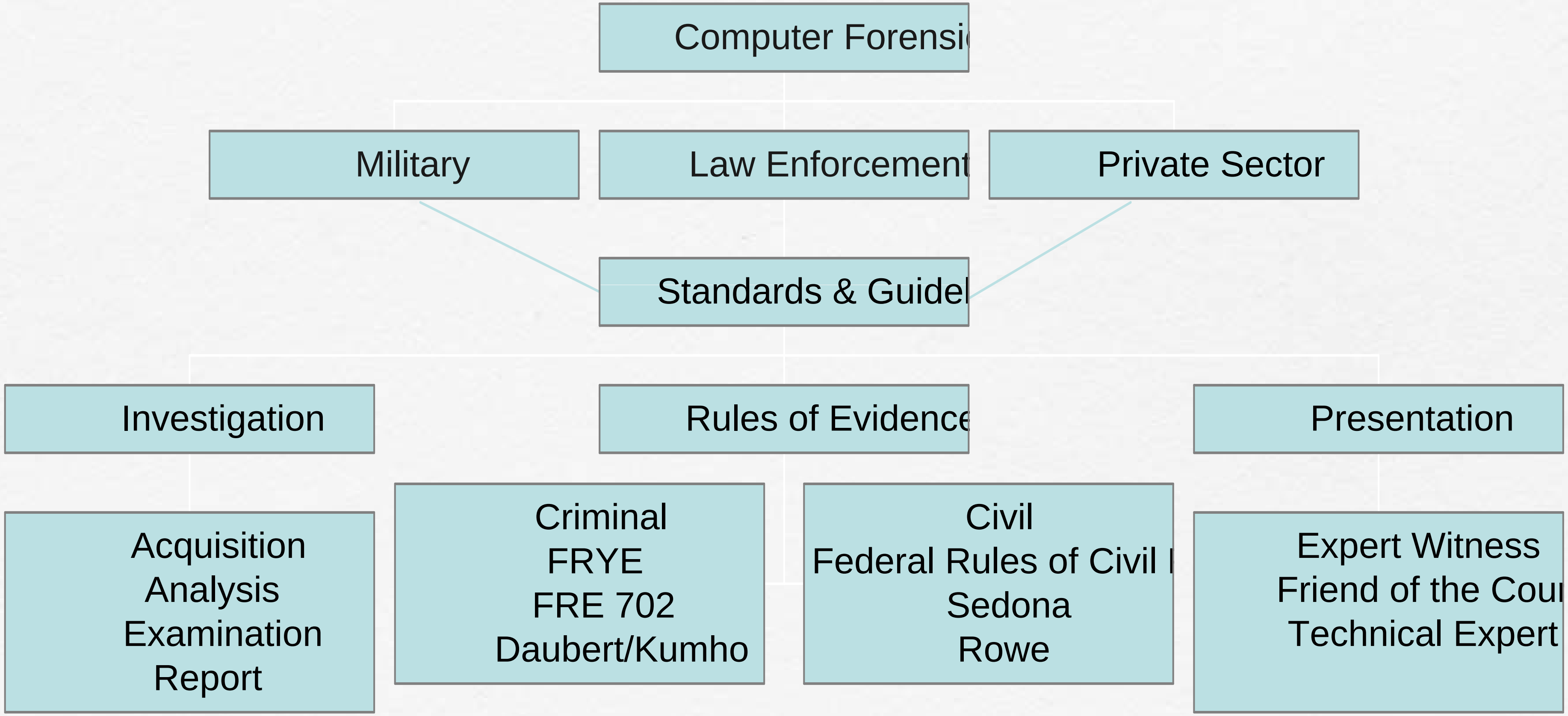
Dept. of Computer & Information Technology

Caveat

- Warning: This lecture will **not** make you a certified digital forensics technician. This lexture is designed to provide an introduction to this field from both a theoretical and practical perspective.
- Digital forensics is a maturing scientific field with many sub-disciplines.

Computer Forensics

Fundamentals



Computer Forensi

Military

Law Enforcement

Private Sector

Standards & Guidel

Investigation

Rules of Evidence

Presentation

Acquisition
Analysis
Examination
Report

Criminal
FRYE
FRE 702
Daubert/Kumho

Civil
Federal Rules of Civil I
Sedona
Rowe

Expert Witness
Friend of the Cour
Technical Expert

Digital Forensic Science

- Digital Forensic Science (DFS):

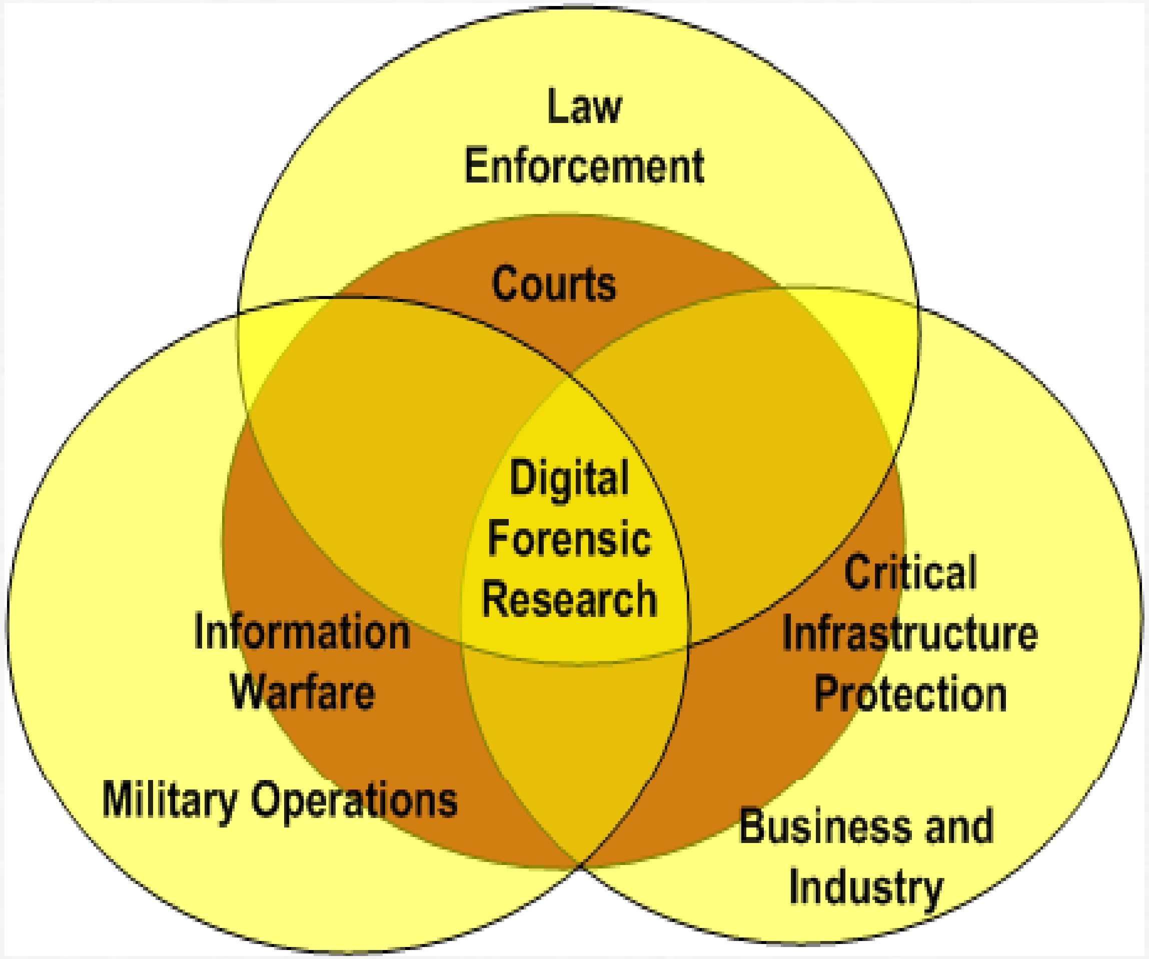
> “The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.”

Source: (2001). Digital Forensic Research Workshop (DFRWS)

Communities

- There at least 3 distinct communities within Digital Forensics
    - Law Enforcement
    - Military
    - Business & Industry
        - Possibly a 4th – Academia

Digital Forensic Science



Community Objectives

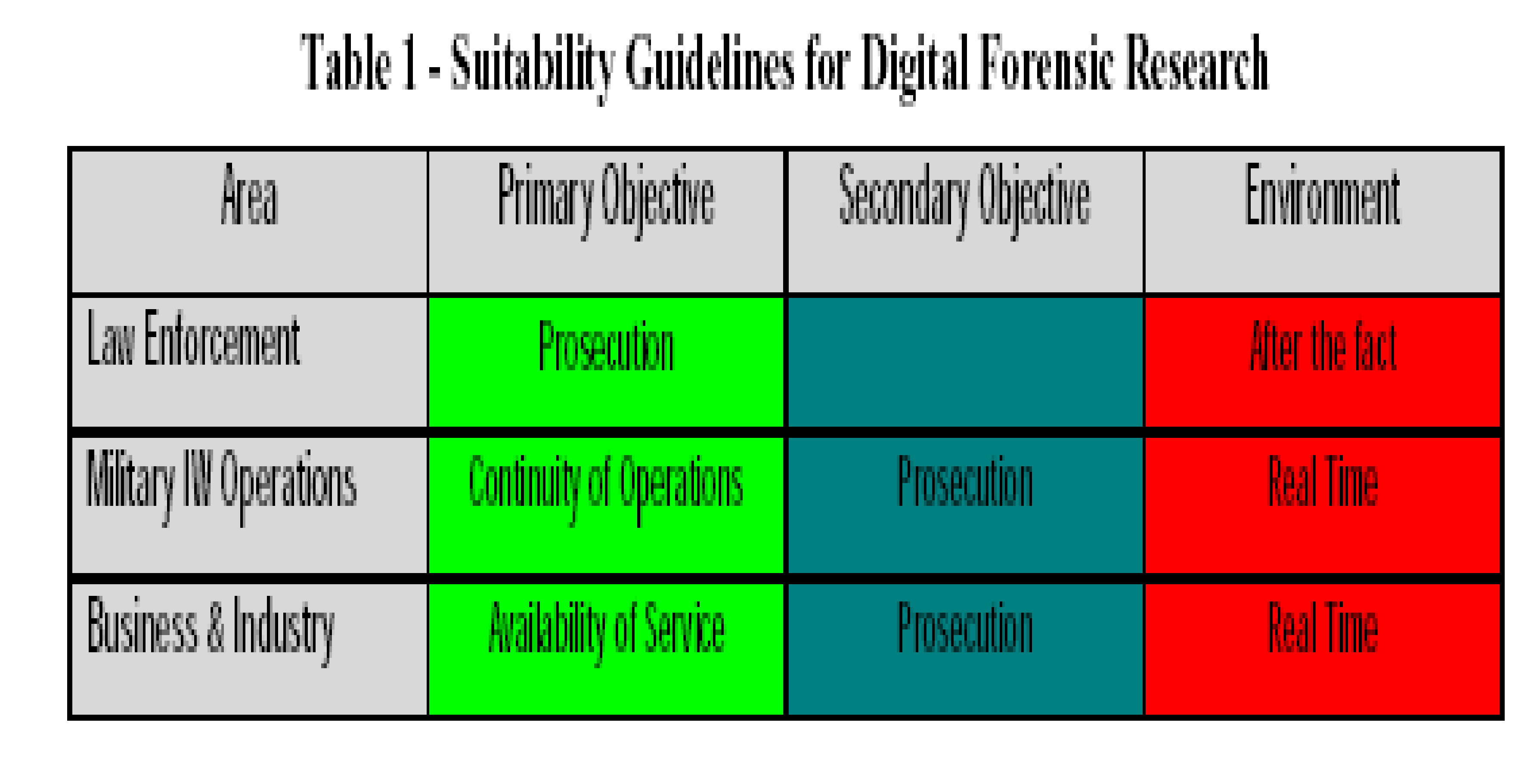


Table 1 - Suitability Guidelines for Digital Forensic Research

Area	Primary Objective	Secondary Objective	Environment
Law Enforcement	Prosecution		After the fact
Military IW Operations	Continuity of Operations	Prosecution	Real Time
Business & Industry	Availability of Service	Prosecution	Real Time

Cyber Forensics

- Includes:
  - Networks (Network Forensics)
  - Small Scale Digital Devices
  - Storage Media (Computer forensics)
  - Code Analysis

Cyber Forensics

- The scientific examination and analysis of digital evidence in such a way that the information can be used as evidence in a court of law.

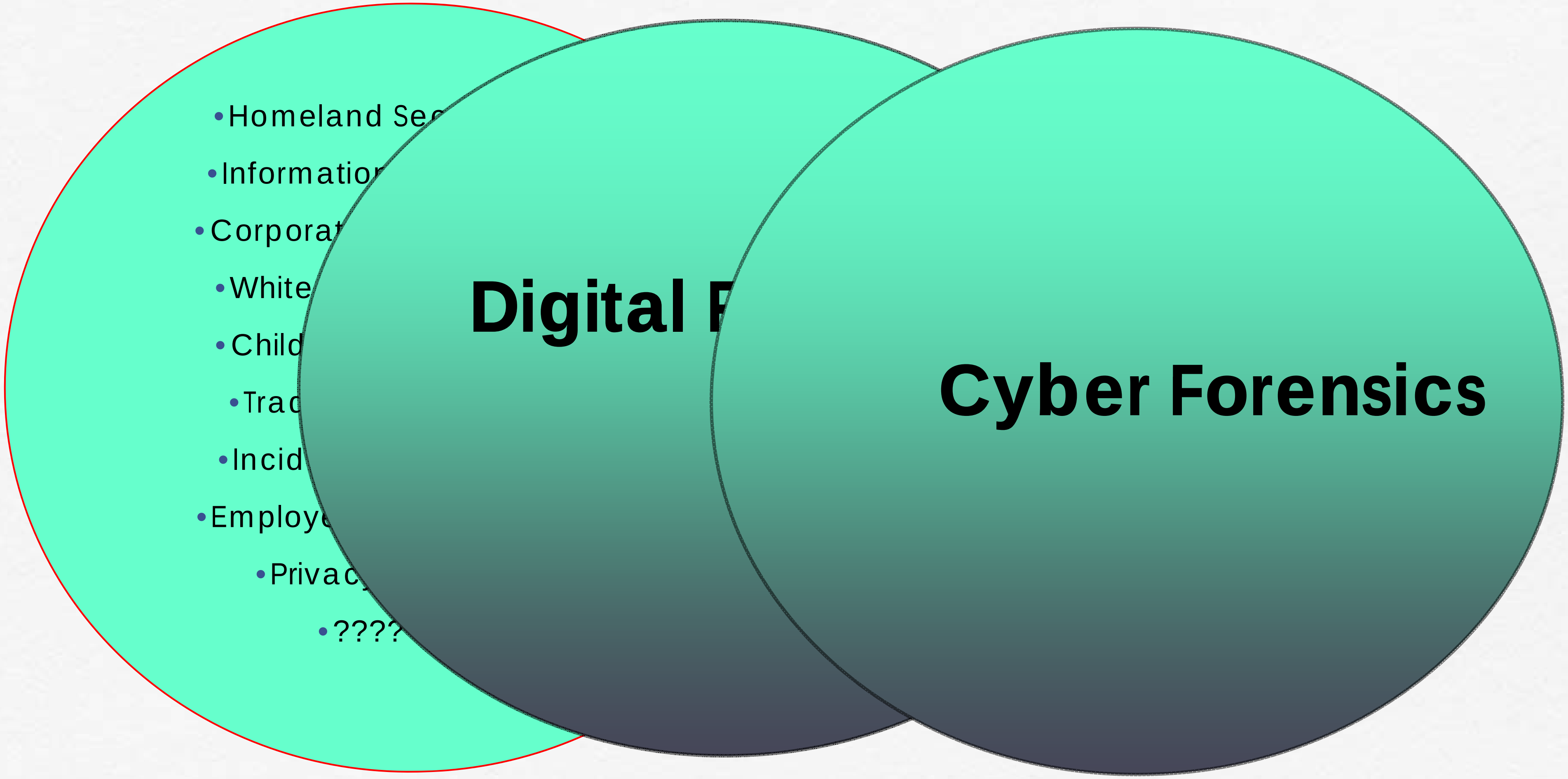
Cyber Forensic Activities

- Cyber forensics activities commonly include:
  - the secure collection of computer data
  - the identification of suspect data
  - the examination of suspect data to determine details such as origin and content
  - the presentation of computer-based information to courts of law
  - the application of a country's laws to computer practice.

The 3 As

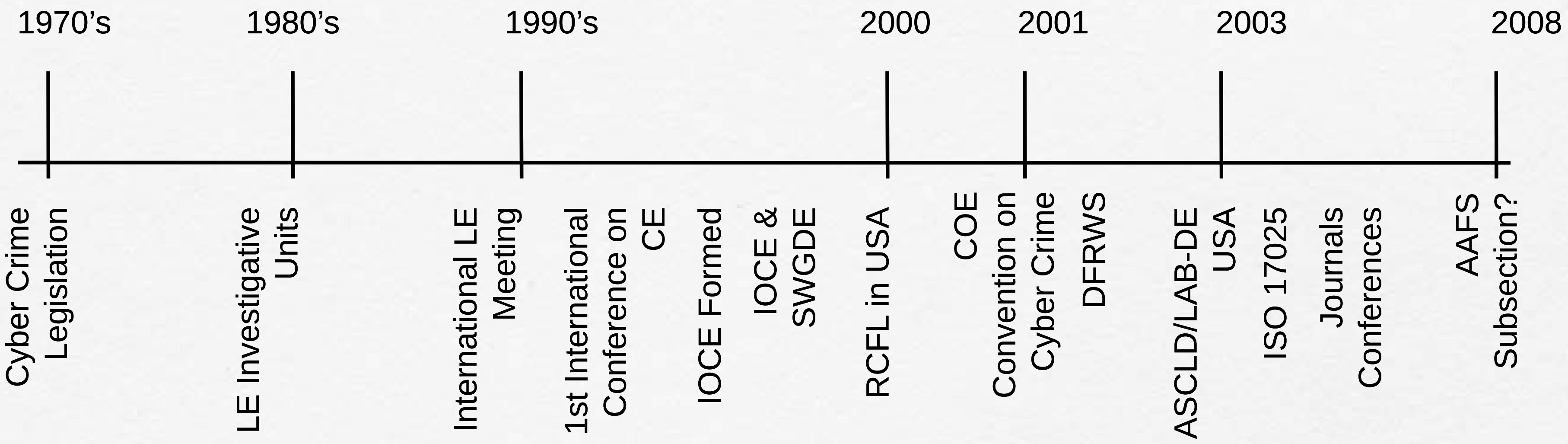
- The basic methodology consists of the 3 As:
  - *Acquire* the evidence without altering or damaging the original
  - *Authenticate* the image
  - *Analyze* the data without modifying it

Context of Cyber Forensics



- Homeland Sec
- Information
- Corporat
- White
- Child
- Trad
- Incid
- Employe
- Privac
- ????

A Brief Timeline



1970’s

Cyber Crime Legislation

1980’s

LE Investigative Units

1990’s

International LE Meeting

1st International Conference on CE

IOCE Formed

IOCE & SWGDE

2000

RCFL in USA

COE Convention on Cyber Crime

2001

DFRWS

ASCLD/LAB-DE USA

2003

ISO 17025

Journals Conferences

2008

AAFS Subsection?

Crime Scenes

- Physical Crime Scenes vs. Cyber/Digital Crime Scenes
- Overlapping principals
- The basics of criminalistics are constant across both physical and cyber/digital
- Locard’s Principle applies
  - “When a person commits a crime something is always left at the scene of the crime that was not present when the person arrived”

Digital Crime Scene

- Digital Evidence
  - Digital data that establish that a crime has been committed, can provide a link between a crime and its victim, or can provide a link between a crime and the perpetrator (Carrier & Spafford, 2003)
- Digital Crime Scene
  - The electronic environment where digital evidence can potentially exist (Rogers, 2005)
  - Primary & Secondary Digital Scene(s) as well

Forensic Principles

- Digital/ Electronic evidence is extremely volatile!
- Once the evidence is contaminated it cannot be de-contaminated!
- The courts acceptance is based on the best evidence principle
  - With computer data, printouts or other output readable by sight, and bit stream copies adhere to this principle.
- Chain of Custody is crucial

Cyber Forensic Principles

- **The 6 Principles are:**

1. When dealing with digital evidence, all of the general forensic and procedural principles must be applied.

2. Upon seizing digital evidence, actions taken should not change that evidence.

3. When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.

4. All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.

5. An Individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.

6. Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

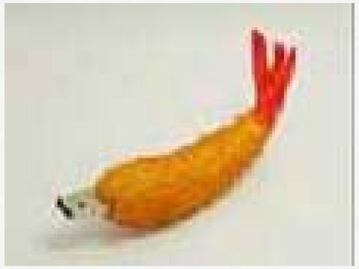
Process/Phases

- Identification
- Collection
  - Bag & Tag
- Preservation
- Examination
- Analysis
- Presentation/Report

Identification

- The first step is identifying evidence and potential containers of evidence
- More difficult than it sounds
  - Small scale devices
  - Non-traditional storage media
  - Multiple possible crime scenes

Devices Identification



Identification

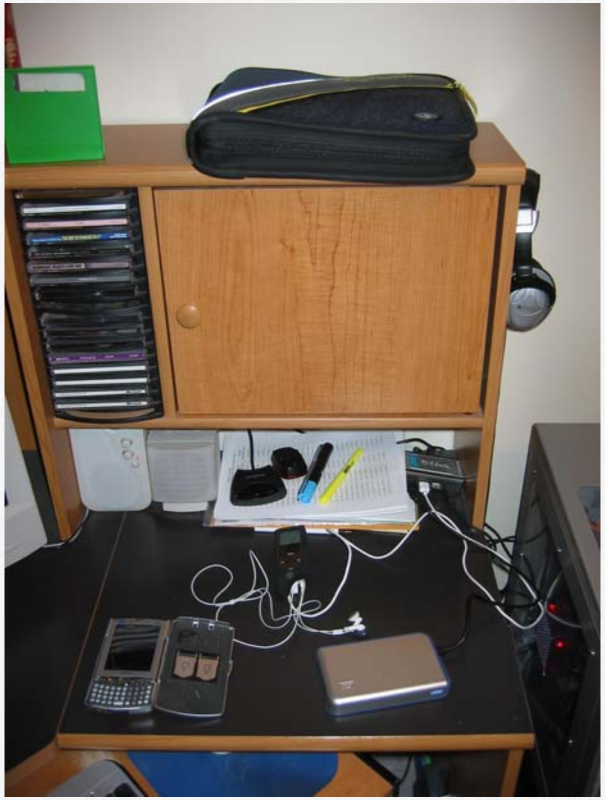
- Context of the investigation is very important
- Do not operate in a vacuum!
- Do not overlook non-electronic sources of evidence
  - Manuals, papers, printouts, etc.

Collection

Care must be taken to minimize contamination

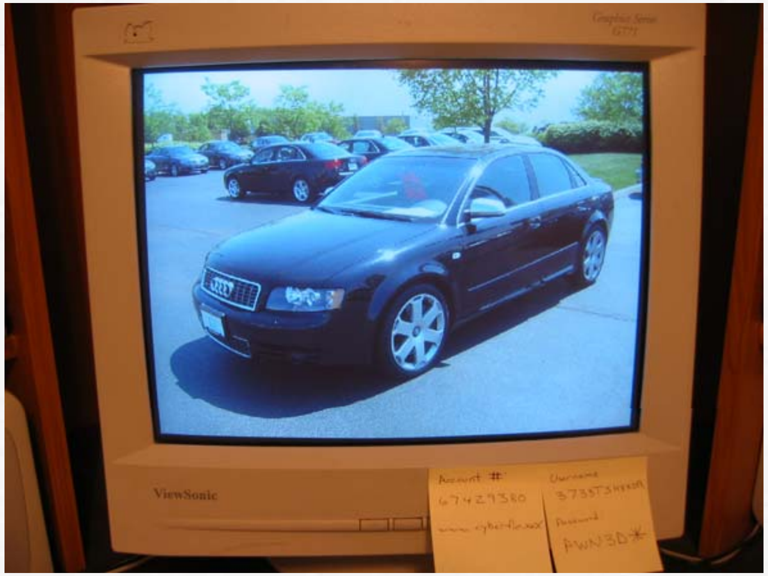
- Collect or seize the system(s)
- Create forensic image
  - Live or Static?
  - Do you own the system
  - What does your policy say?

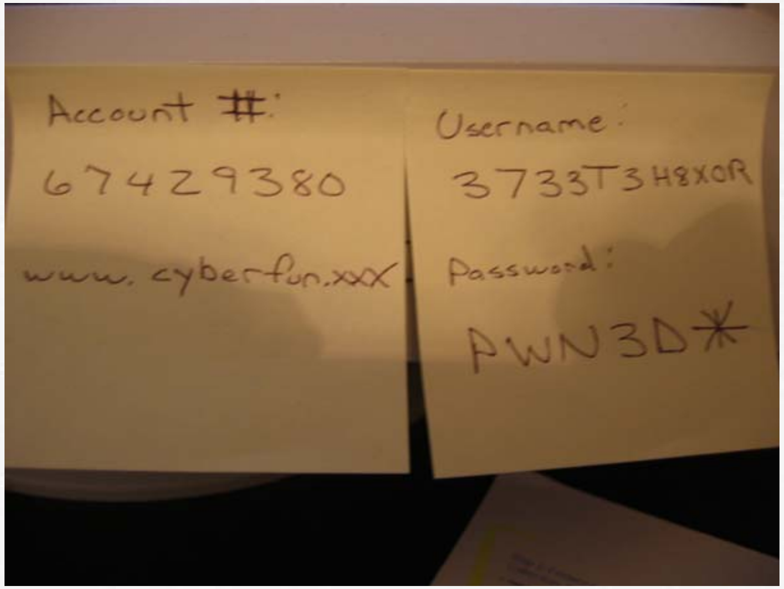
Collection: Documentation



Collection: Documentation

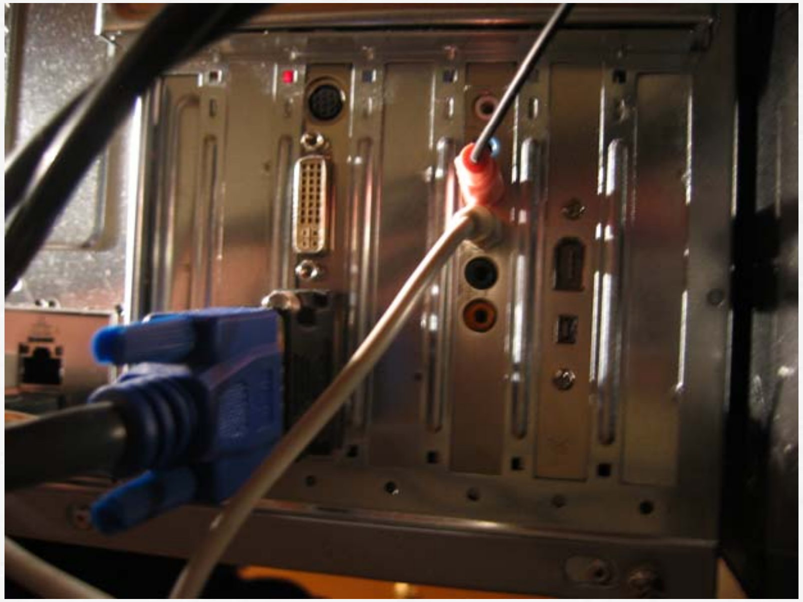
- Take detailed photos and notes of the computer / monitor
  - If the computer is “on”, take photos of what is displayed on the monitor – DO NOT ALTER THE SCENE





Collection: Documentation

- Make sure to take photos and notes of all connections to the computer/other devices



Collection: Imaging

- Rule of Thumb: make 2 copies and don’t work from the original (if possible)
- A file copy does not recover all data areas of the device for examination
- Working from a duplicate image
    - Preserves the original evidence
    - Prevents inadvertent alteration of original evidence during examination
    - Allows recreation of the duplicate image if necessary

Collection: Imaging

- Digital evidence can be duplicated with no degradation from copy to copy
  - This is not the case with most other forms of evidence

Collection: Imaging

- Write blockers
  - Software
  - Hardware
- Hardware write blockers are becoming the industry standard
  - USB, SATA, IDE, SCSI, SIM, Memory Cards
  - Not BIOS dependent
  - But still verify prior to usage!

Collection: Imaging

- Forensic Copies (Bitstream)
  - Bit for Bit copying captures all the data on the copied media including hidden and residual data (e.g., slack space, swap, residue, unused space, deleted files etc.)
- Often the “smoking gun” is found in the residual data.
- Imaging from a disk (drive) to a file is becoming the norm
  - Multiple cases stored on same media
  - No risk of data leakage from underlying media
- Remember avoid working for original
- Use a write blocker even when examining a copy!

Imaging: Authenticity & Integrity

- How do we demonstrate that the image is a true unaltered copy of the original?

  -Hashing (MD5, SHA 256)

- A mathematical algorithm that produces a unique value (128 Bit, 512 Bit)
  - Can be performed on various types of data (files, partitions, physical drive)
- The value can be used to demonstrate the integrity of your data
  - Changes made to data will result in a different value
- The same process can be used to demonstrate the image has not changed from time-1 to time-n

Examination

- Higher level look at the file system representation of the data on the media
- Verify integrity of image
  - MD5, SHA1 etc.
- Recover deleted files & folders
- Determine keyword list
  - What are you searching for
- Determine time lines
  - What is the timezone setting of the suspect system
  - What time frame is of importance
  - Graphical representation is very useful

Examination

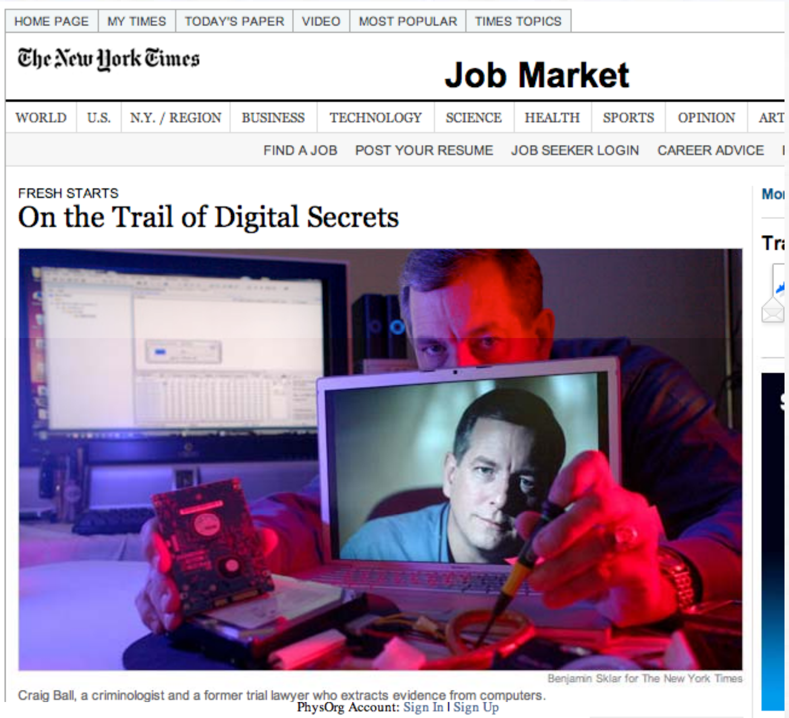
- Examine directory tree
  - What looks out of place
  - Stego tools installed
  - Evidence Scrubbers
- Perform keyword searches
  - Indexed
  - Slack & unallocated space
- Search for relevant evidence types
  - Hash sets can be useful
  - Graphics
  - Spreadsheets
  - Hacking tools
  - Etc.
- Look for the obvious first
- When is enough enough??

Issues

- lack of certification for tools
- Lack of standards
- lack of certification for professionals
- lack of understanding by Judiciary
- lack of curriculum accreditation
- Rapid changes in technology!
- Immature Scientific Discipline

Careers

- One of the fastest growing job markets!



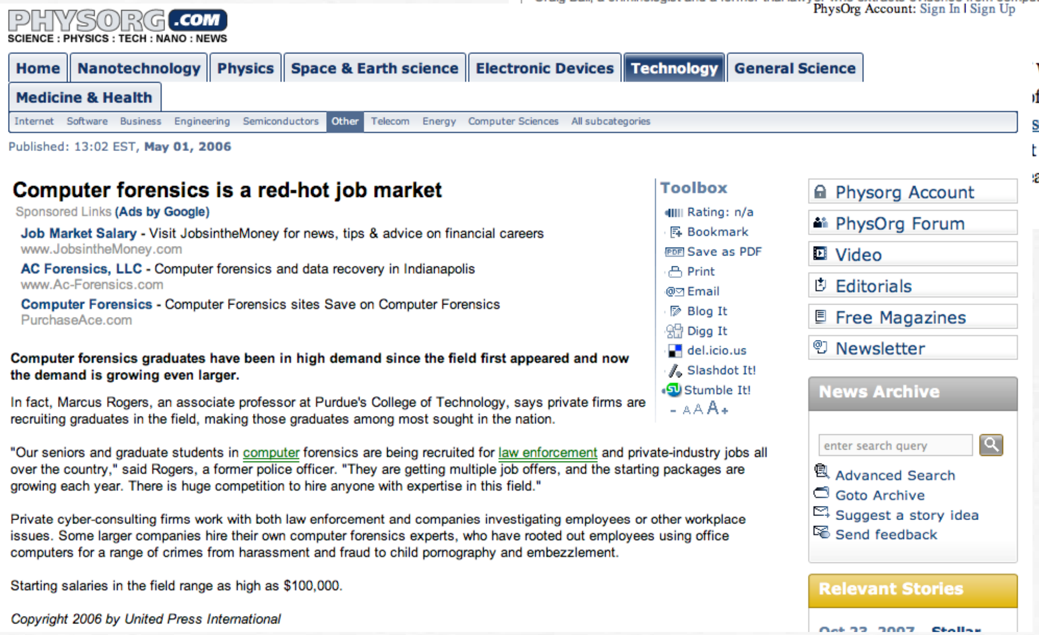
FRESH STARTS

On the Trail of Digital Secrets

Benjamin Sklar for The New York Times

Craig Ball, a criminologist and a former trial lawyer who extracts evidence from computers.

Wichita,
f
son's
t on his
a where



Published: 13:02 EST, **May 01, 2006**

Computer forensics is a red-hot job market

Sponsored Links **(Ads by Google)**

Job Market Salary - Visit JobsintheMoney for news, tips & advice on financial careers
www.JobsintheMoney.com

AC Forensics, LLC - Computer forensics and data recovery in Indianapolis
www.Ac-Forensics.com

Computer Forensics - Computer Forensics sites Save on Computer Forensics
PurchaseAce.com

Computer forensics graduates have been in high demand since the field first appeared and now the demand is growing even larger.

In fact, Marcus Rogers, an associate professor at Purdue's College of Technology, says private firms are recruiting graduates in the field, making those graduates among most sought in the nation.

"Our seniors and graduate students in computer forensics are being recruited for law enforcement and private-industry jobs all over the country," said Rogers, a former police officer. "They are getting multiple job offers, and the starting packages are growing each year. There is huge competition to hire anyone with expertise in this field."

Private cyber-consulting firms work with both law enforcement and companies investigating employees or other workplace issues. Some larger companies hire their own computer forensics experts, who have rooted out employees using office computers for a range of crimes from harassment and fraud to child pornography and embezzlement.

Starting salaries in the field range as high as $100,000.

Copyright 2006 by United Press International

Paths to Careers in CF

- Certifications
- Associate Degree
- Bachelor Degree
- Post Grad Certificate
- Masters
- Doctorate

Job Functions

- CF Technician
- CF Investigator
- CF Analyst/Examiner (lab)
- CF Lab Director
- CF Scientist

Professional Opportunities

- Law Enforcement
- Private Sector
- Intelligence Community
- Military
- Academia

Summary

- Cyber Forensics is a maturing forensic Science
- AAFS new section Feb 2008
- Excellent career opportunities
- Proper education & training is paramount!

QUestions???

Contact Information

Marcus Rogers, PhD, CISSP, CCCI

cyberforensics@mac.com

http://www.cyberforensics.purdue.edu

765-494-2561