Digital Forensics

Dr. Vic Fay-Wolfe
Department of Computer Science
University of Rhode Island

Topics

- What is Digital Forensics?
- Cases
- Digital Forensics Practice
- Algorithms and Computer Sci
- Digital Forensics @ URI

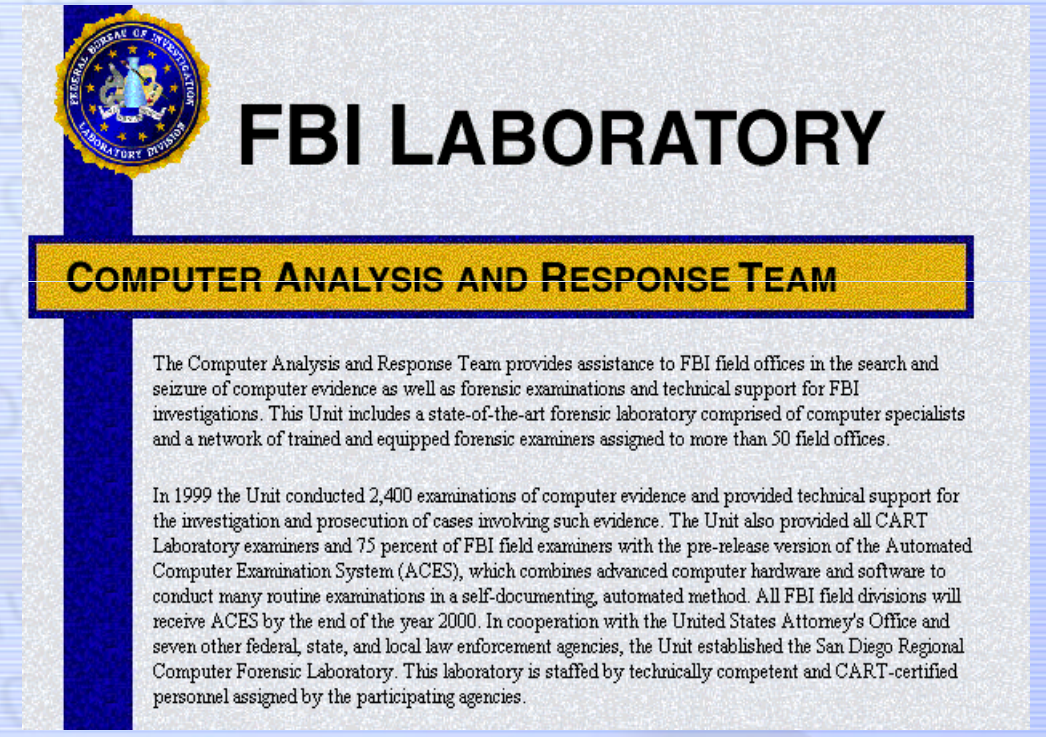
What is Digital Forensics?

The application of forensic science techniques to the discovery, collection and analysis of digital evidence.

5 Ws of Digital Evidence…

Who Uses Digital Evidence?

- Criminal law enforcement
- Criminal defense attorneys
- Civil attorneys
- Organization Information Technology (IT) personnel
- Homeland security
- IRS / SEC (financial enforcement)
- Military



FBI LABORATORY

COMPUTER ANALYSIS AND RESPONSE TEAM

The Computer Analysis and Response Team provides assistance to FBI field offices in the search and seizure of computer evidence as well as forensic examinations and technical support for FBI investigations. This Unit includes a state-of-the-art forensic laboratory comprised of computer specialists and a network of trained and equipped forensic examiners assigned to more than 50 field offices.

In 1999 the Unit conducted 2,400 examinations of computer evidence and provided technical support for the investigation and prosecution of cases involving such evidence. The Unit also provided all CART Laboratory examiners and 75 percent of FBI field examiners with the pre-release version of the Automated Computer Examination System (ACES), which combines advanced computer hardware and software to conduct many routine examinations in a self-documenting, automated method. All FBI field divisions will receive ACES by the end of the year 2000. In cooperation with the United States Attorney's Office and seven other federal, state, and local law enforcement agencies, the Unit established the San Diego Regional Computer Forensic Laboratory. This laboratory is staffed by technically competent and CART-certified personnel assigned by the participating agencies.

What Digital Evidence Can Be Found?

- Files listed in standard directory search
- Hidden files
- Deleted files
- Email
- Deleted email
- Certain Instant Messaging
- Passwords
- Who used the computer
- Who modified a document
- Was disk changed?
- Was a document edited?
- What devices were attached
- Encrypted files
- Web sites visited
- Searches performed
- Cookies
- Network traces
- Owners of servers
- **TIME**
  - When created
  - When changed
  - When modified
  - When sent/received
  - When login/out

Where Can Digital Evidence Be Found?

- Hard drives
- Digital cameras
- Memory sticks
- MP3 players
- Cell phones
- Printers
- CD / DVDs
- PDAs
- Game boxes
- Networks
  - Logs
  - Intercepts/traces






How Can Digital Evidence Be Used?

- Formerly not considered tangible evidence
- 4th Amendment - No "unreasonable" search and seizure
  - Computer data and network activity is private
  - Warrant (probable cause) required for government agents
  - "Plain View Doctrine" – can all files of computer be searched?
- Federal Rules of Evidence – Computer data is treated as document
- Frye & Daubert tests of scientific admissibility
  - Widely accepted, published, available, low error

When Can Digital Evidence Be Used?

Digital Forensics Cases

Hacker: Kevin Mitnick

- Hacked into computers at Motorola, Nokia Mobile Phones, Fujitsu, Novell, NEC, Sun Microsystems, Colorado SuperNet and the University of Southern California. Damages were estimated to be as high as $80 million
- Jailed in 1995
- Made cell calls through intricate re-routing to modem, but there was a serial number log
- Dumped data at web site, but there was an IP address log
- Timeline of calls, data, linked to Mitnick behavior

DFC Case Example: Inappropriate Computer Use

Plaintiff showed:

- Defendant's account had extensive volume of porn
- Used shock value
- Used misleading terms
- Defendant was fired

On appeal we showed:

- Actual time on web sites very short – result of spam emails
- No intent to save
- Computer left on in public place
- Time of creation often did not match time person behind the computer
- Called into question forensics used to obtain plaintiff's evidence

- Extensive education of judge required
- We have done other cases where the inappropriate use was obvious

DFC Case Example: Corporate Espionage

Defendant:

- Left Company A to work for a competitor, Company B
- Showed signs of using Company A proprietary information: pricing, customer lists
- Denied taking information
- Company A had deleted files in question from his laptop before leaving

For plaintiff we showed:

- We wrote affidavit for subpoena to seize defendant's laptop
- We found evidence of emailing documents to Company B before leaving
- We found what USB devices had been inserted – fodder for further subpoena
- We found Company B names of recipients and servers – fodder for further subpoenas

DFC Case Example: Financial Fraud

- Suspected inappropriate use of federal funds
- Government issued: "*provide any and all relevant documents*"
- We copied 20+ computers and 3 servers (massive storage)
- Extensive documentation of process and chain of custody
- Took digital signature to authenticate snapshot of all disks
- Restored computers for business use within two days – copied evidence preserved in our evidence locker

DFC Other Case Examples

- Child porn
  - Result of sharing software?
  - Result of spam?
- Illegal music downloads
  - Extent?
  - Who did it?
- Suicide
  - Web sites showed means and motive
- Murder
  - Victim's computer showed suspects
- Sexual assault
  - Instant messages between adult and child authentic?
- Divorce
  - email infidelity, porn, financials

Case: Sept 11 "20th Terrorist"

- Zacarias Moussaoui – was to be on plane, but was detained
- Used Kinko's computers to communicate
- Computer records seized
- Hotmail account traced
- FBI testimony as to how digital evidence was obtained and verified

Hendricken HS Vice Principal

projo.com The Providence Journal

Providence Journal Tuesday Nov 9, 200

Hendricken official on leave over conduct

Bishop Hendricken's president says assistant principal Timothy administrative leave for alleged inappropriate actions on the In

01:00 AM EST on Tuesday, November 9, 2004

BY DANIEL BARBARISI
Journal Staff Writer

WARWICK -- The assistant principal of Bishop Hendricken High School has be because of allegations of a "breach of professional conduct," according to Brothe

School administrators held an assembly yesterday morning to tell students that Tir assistant principal for student life, had been placed on paid leave. They did not giv a letter home with students to inform parents of the action.

Brother Leto said that he was made aware Sunday night that Sheldon may have t the Internet. Sheldon was using his home computer a

Brother Leto said that he and the school principal w picture there, they decided to immediately place him from the school had spoken to Sheldon, or whether yesterday were unsuccessful.

Perverted-Justice.com Archives

Tim here has youngung's lined up all over the US...but he picks me!
Bust by Don Pedro @ 11/5/2004 5:49 PM PST

Perverted Justice mark: Tim, 39
AOL IM: Oberon318
Location: Warwick, Rhode Island
Phone Number: 401-885-6661 (Cell, has been verified)

This wannabe pedo tried to solicit CFHSkidd1990, a 14 year old boy ... or so they thought!

Here's Tim. Tim is the type that tries to put everything on the kid. Those types creep me out just as much, if not more, than the overtly sexual ones. Somewhere, inside his head, he justifies sleeping with a 14 year old, because he's not saying no! EARTH TO TIM: YOU ARE AN ADULT. IT IS YOUR JOB TO SAY NO!

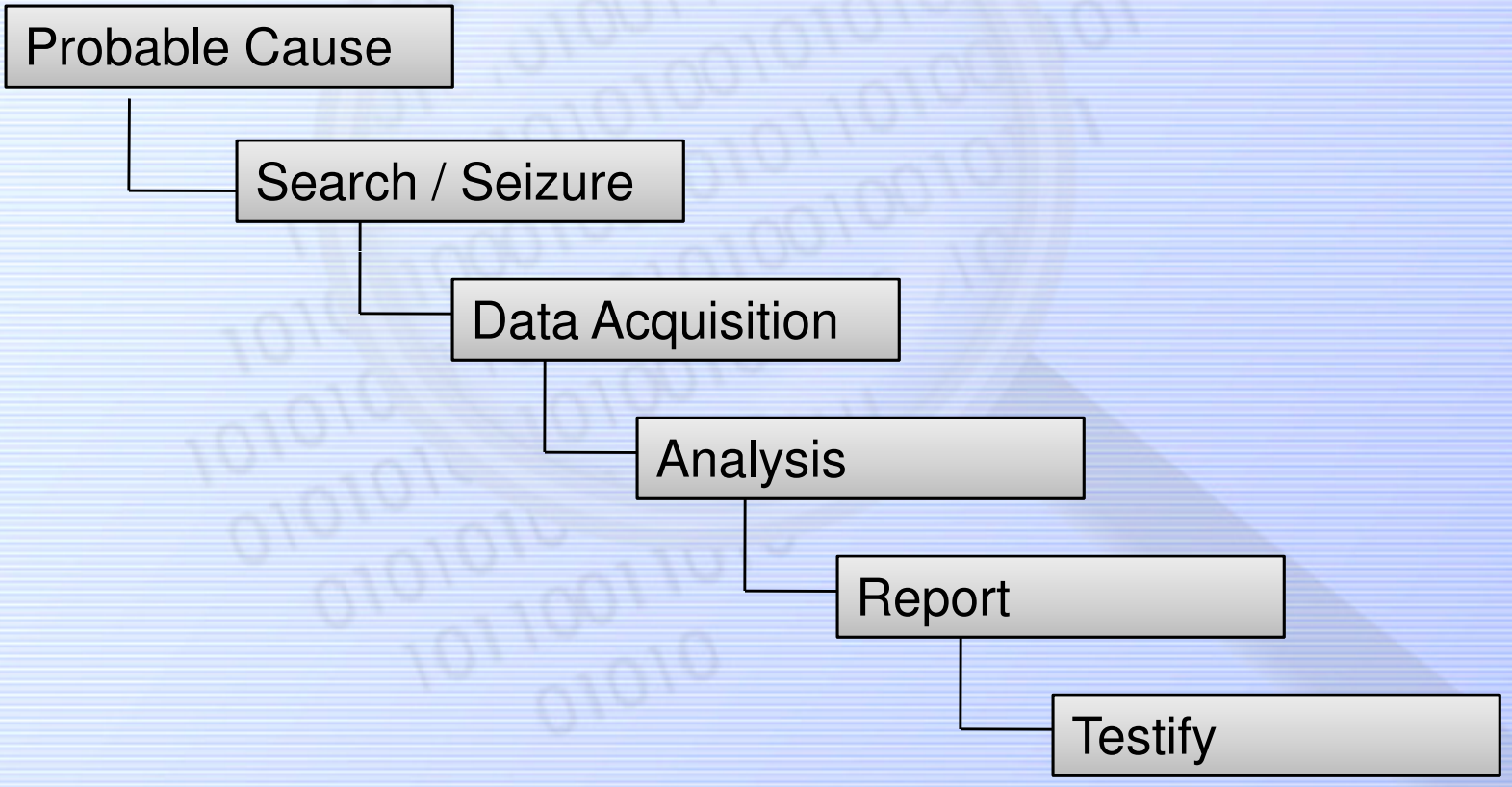
Oberon318 [12:07 AM]: sup
CFHSkidd1990 [12:07 AM]: hey how ru
CFHSkidd1990 [12:07 AM]: **14 m central falls u?**
Oberon318 [12:07 AM]: not bad

PERVERTED-JUSTICE.COM

As Long As Our Children Aren't Safe From Predators...
...Predators aren't safe from US.

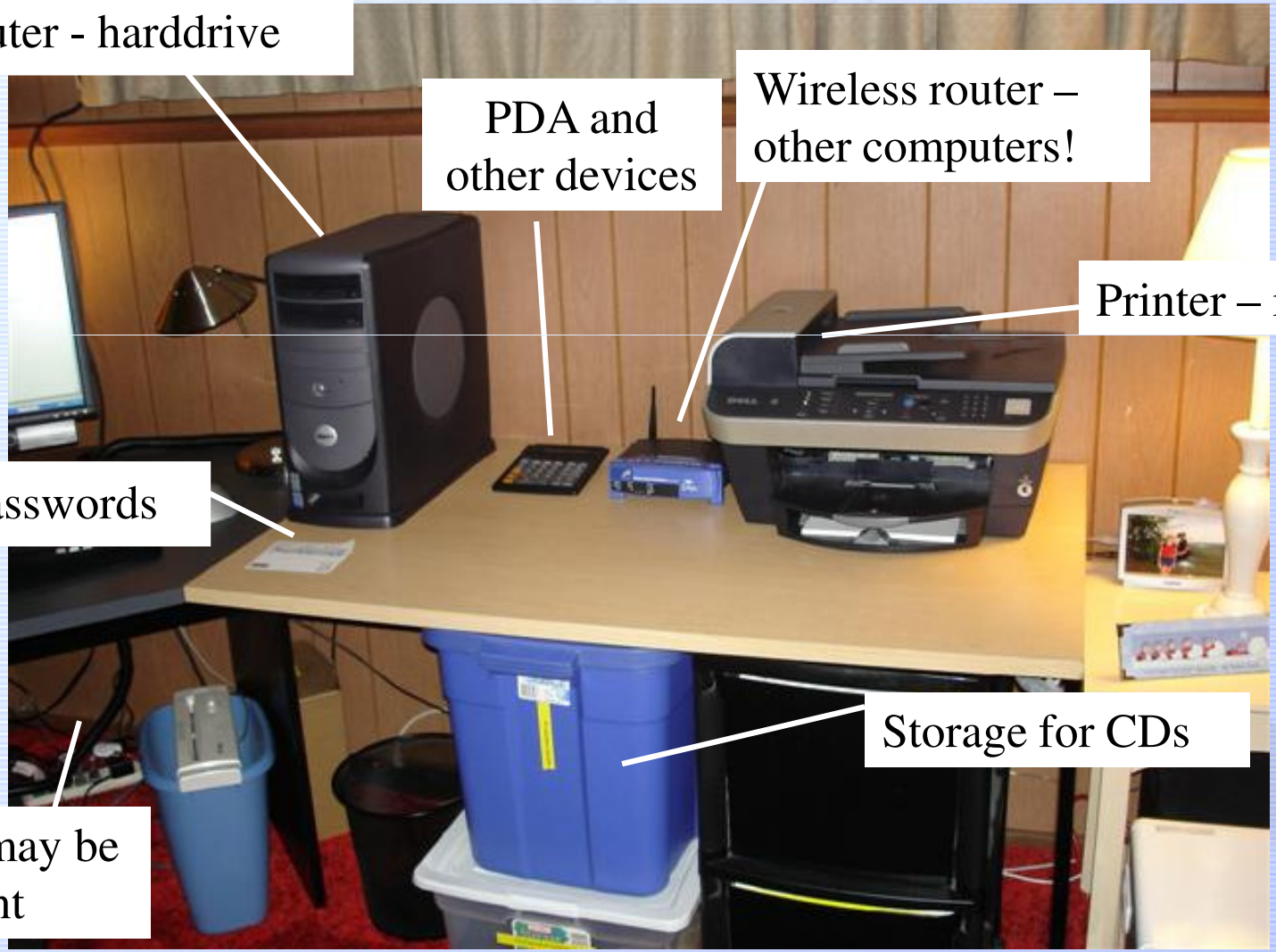
Digital Forensics Practice and Procedures

Digital Forensics Procedure



Crime Scene

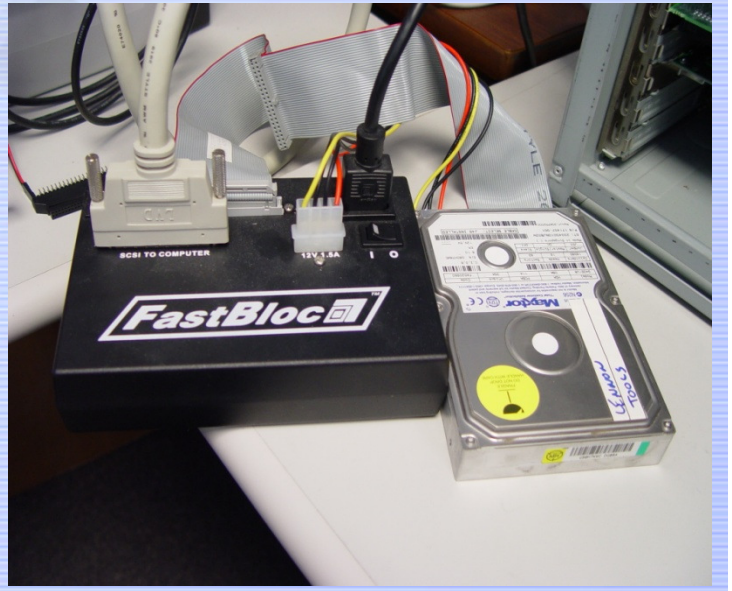
Crime Scene


Computer - harddrive
PDA and other devices
Wireless router – other computers!
Printer – memory
Paper - passwords
Storage for CDs
Cables may be important

Corporate Crime Scene

Acquisition And Verification

- Obtain a warrant/permission
- Take pictures (screen, wiring, devices etc)
- Take notes (BIOS time accuracy, labels on the machine for software product key, procedures, serial numbers (e.g. to call Dell),)
- If possible unobtrusively obtain RAM data
- Possibly unplug power plug from machine
  - This preserves swap file and does not allow wiping programs to run
  - Could corrupt (e.g. database, Linux file systems)
- From live machine: machine name, drives/file systems, network config
- Take digital signature of original storage media (e.g. harddrive)
- Seal original storage media
- Establish “Chain of Custody” for original storage media
- Get Drive:
  - Take whole computer to lab
  - Take drive to lab
  - Use hardware disk duplicator (hashes won’t match)
  - Boot target machine with second (wiped) drive to copy onto
    - Must write block original drive! Software or hardware write blocker
- Bit copy original storage media
  - Write block original
  - DD bit copy good, ghost bit copy bad
- Compare digital signature of copy and original
- Analyze copy of storage media

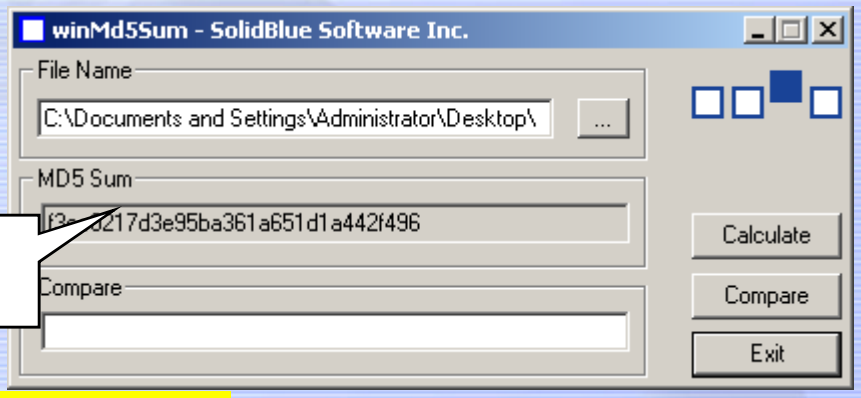


Algorithms and Computer Science

Digital Signatures

- *MD5 Hash* – 128 bit signature of entire drive generated by complex operations
- Used to authenticate evidence – has it been altered?
- Courts require digital signature before and after investigating the evidence.

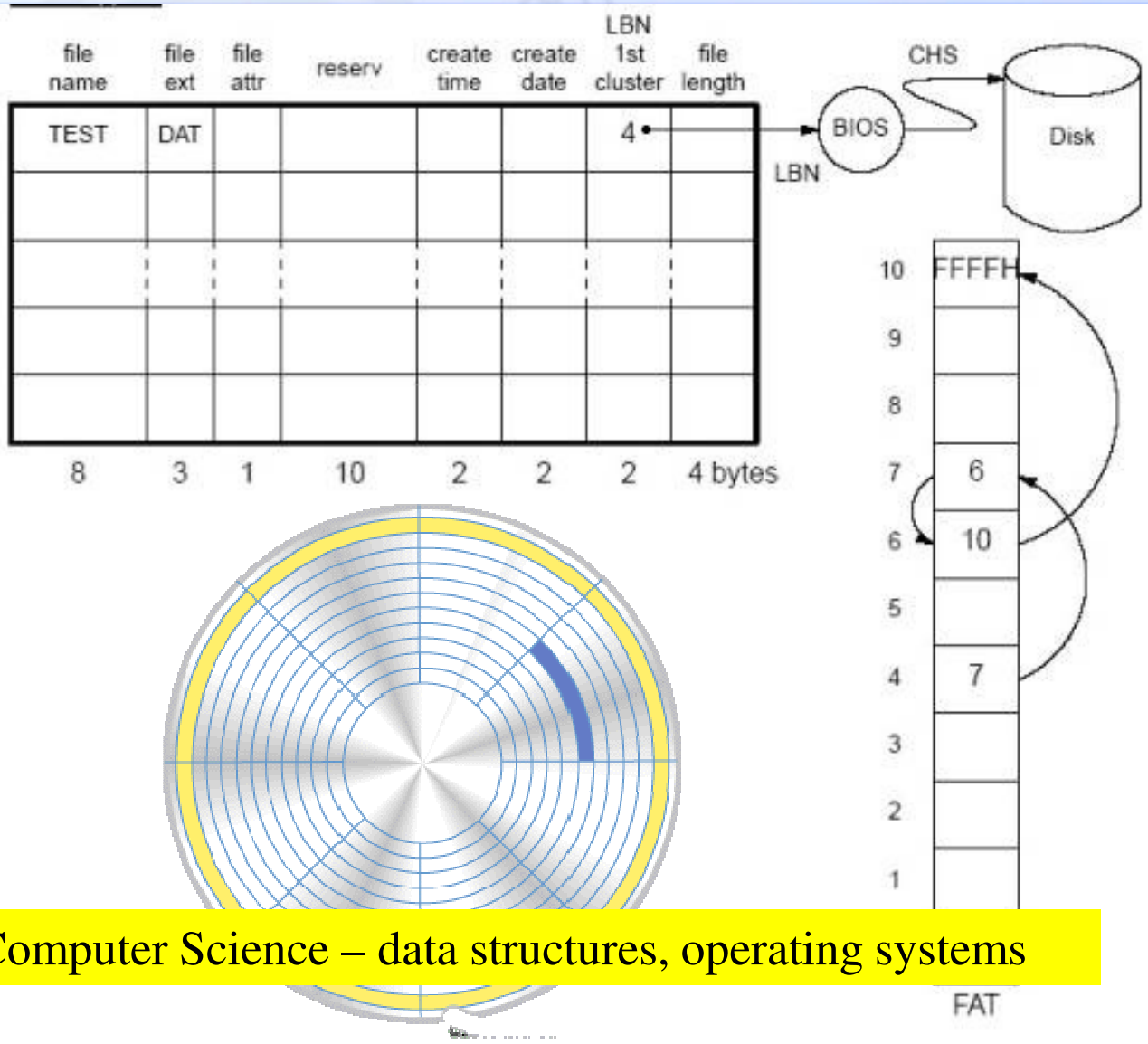
f3ec0217d3e95ba361a651d1a442f496



Computer science algorithms for digital signatures

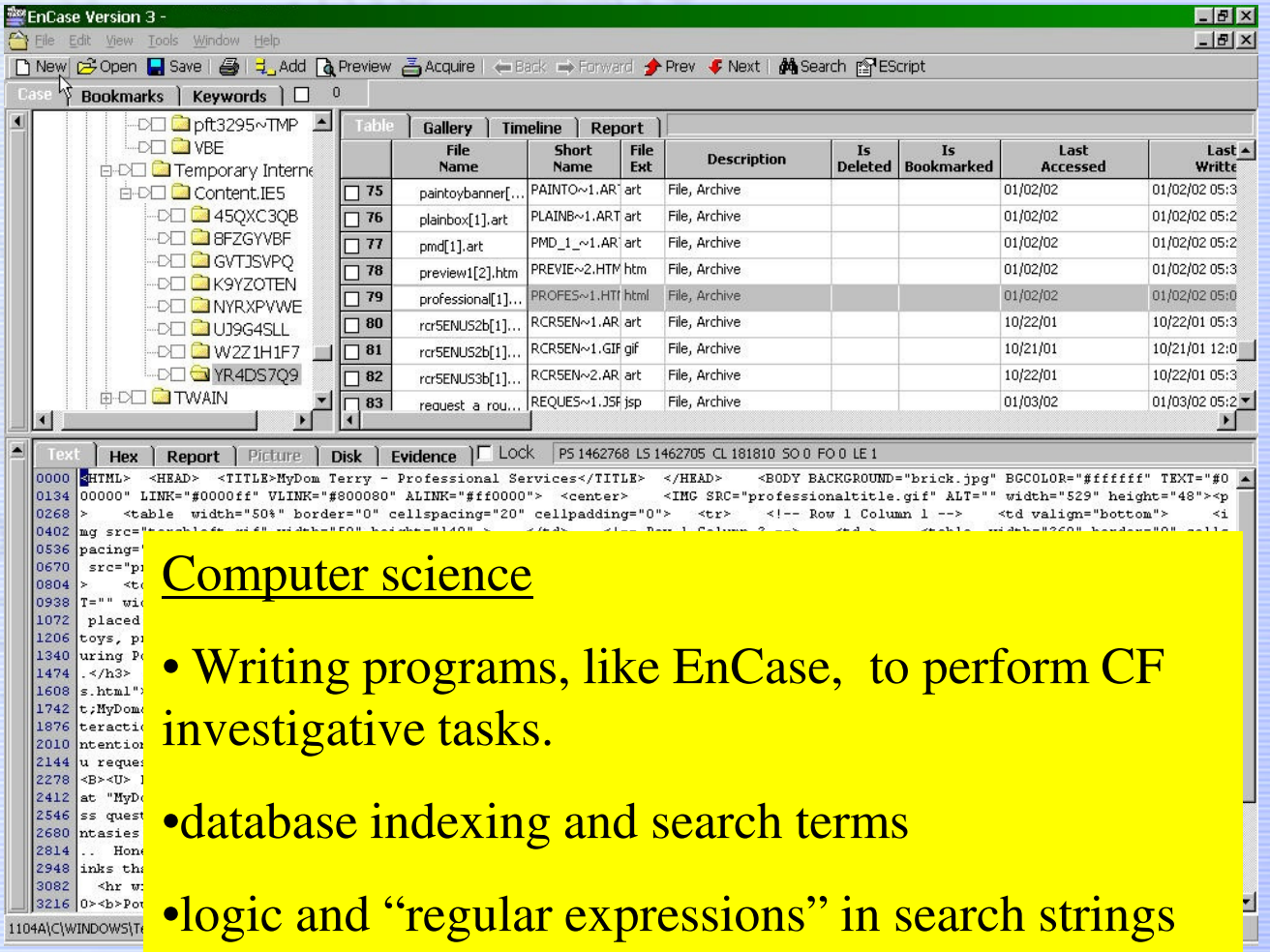
Deleted Files

- Recycle Bin
- ***Unallocated*** – previously written, but not pointed to in file system
- ***Slack*** – unused at end of cluster



Professional CF Software: EnCase

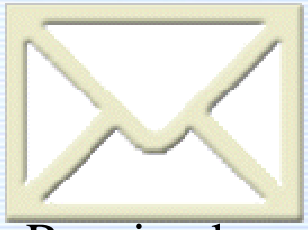
- Used by State Police, FBI, State Crime Lab
- Enter keywords or times
- It searches all digital data including deleted files and “slack space”
- It generates CF-friendly reports
- URI has professional version in DFC



Computer science

- Writing programs, like EnCase, to perform CF investigative tasks.
- database indexing and search terms
- logic and “regular expressions” in search strings

Email Trace



Received Email

IP address:
traceroute,
MX record,
Whois

Sending Server

Email Server Log

User name

Computer science - networking

Radius Log

User name,phone #

DHCP Log

MAC

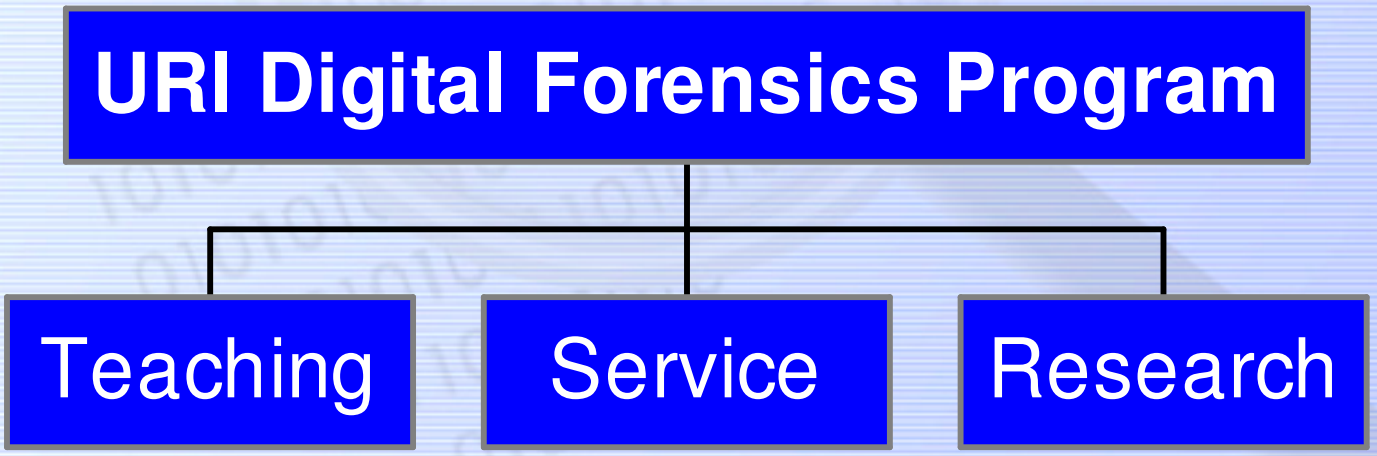
ARP Log

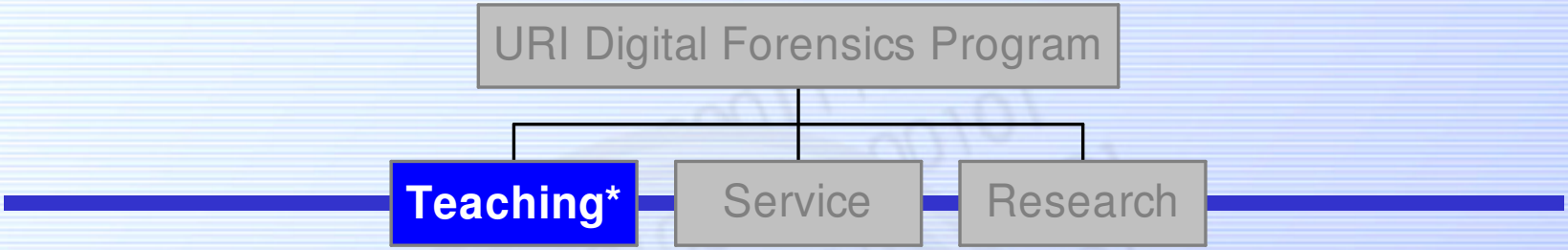
MAC A

Busted!

Bad Guy

Digital Forensics @ URI

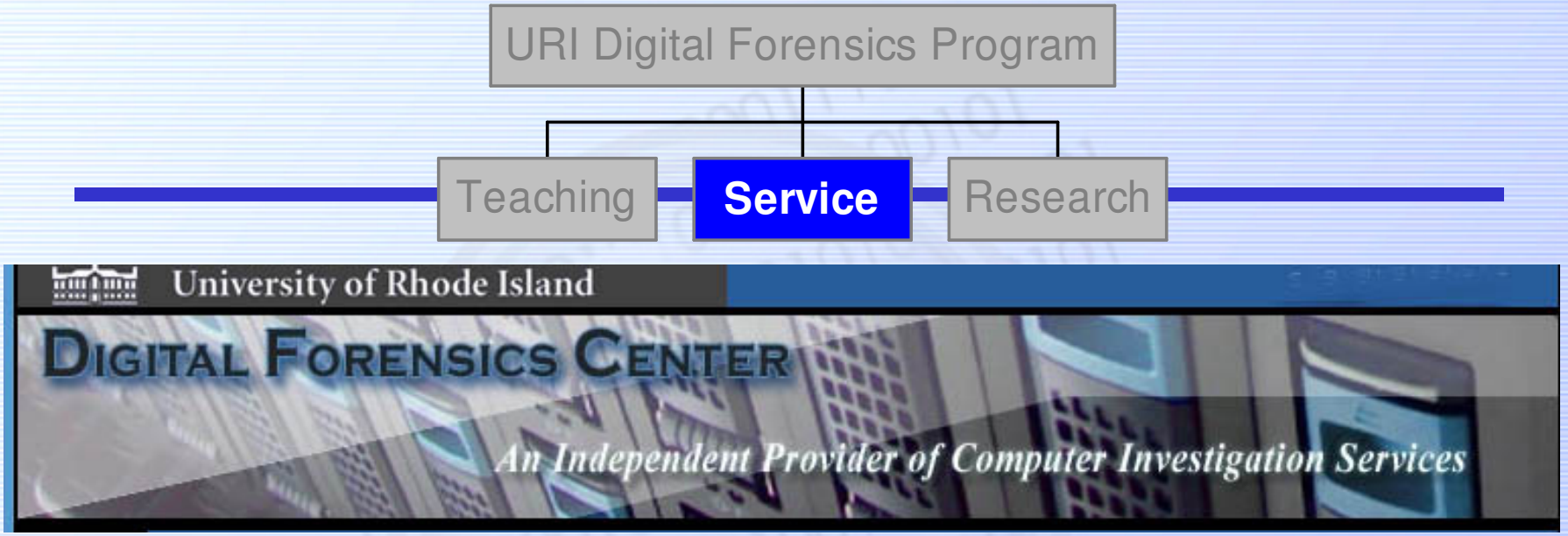




- **Courses:**
  - Taught By IRS Computer Crimes Special Agent Dan Dickerman and URI faculty and staff
  - Computer Forensics (2)
  - Network Forensics (2)
  - Basic Courses (2)

- **Digital Forensics Minor**
  - Can be done with any major
  - CS is the best to provide depth
- **Internships**
  - RI State Police
  - Naval Criminal Investigative Service
  - FBI, IRS, Secret Service
  - Local Police
  - Local companies
  - URI Digital Forensics Center

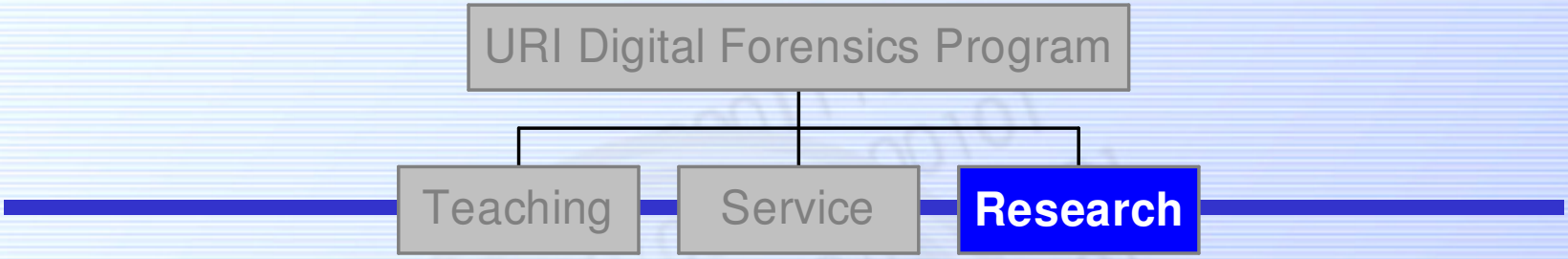
http://forensics.cs.uri.edu



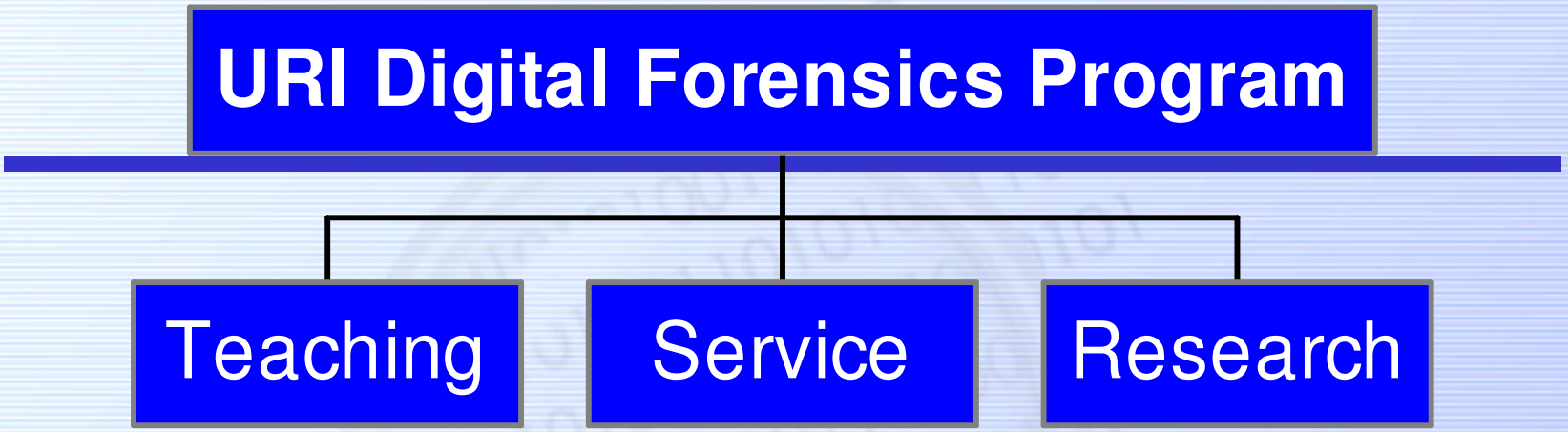
- **Facilities**
  - On-campus lab
  - Forensic acquisition hardware and software
  - Forensic workstation(s)
  - EnCase Forensic and FTK for acquisition and analysis
  - VMWare, other software tools
  - Evidence and storage data center
  - Law enforcement quality procedures
  - Staff, faculty, student interns

- **Services**
  - Forensic acquisition
  - Digital evidence analysis
  - Targeted research and analysis of technologies
  - Data recovery

- **Online Information**
  - Our web site provides
    - Whitepapers
    - Research results



- **Original DF Research**
  - ***Human image detection and authentication****
  - ***Steg detection and breaking****
  - Password cracking
  - Uses of virtual machines
  - Alternative digital signatures
  - ***GREP generation and repository****
- **DF Whitepapers**
  - Useful registry entries
  - P2P sharing behavior
- **DF Software Evaluation**
  - Does a piece of software claim to do what it states it does?
  - University independent opinion
- **DF Software Development**
  - Forensic Boot Disk
  - ***Software write blockers****
  - Grep expression generators



Dr. Victor Fay-Wolfe
University of Rhode Island
Director, Digital Forensics Program
wolfe@cs.uri.edu

http://forensics.cs.uri.edu