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.

What Digital Evidence Can Be Found?

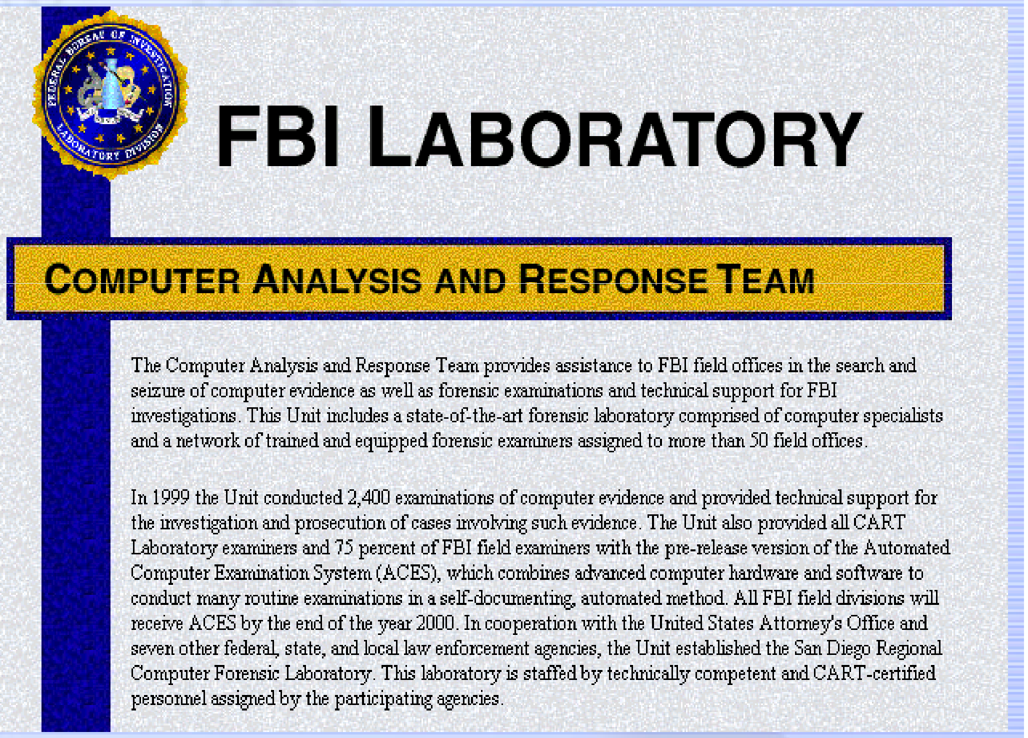
- Files listed in standard directory search
- Hidden files
- Deleted files
- Email
- Deleted email
- Certain Instant Messaging
- Passwords
- Who used the computer
- Who modified a document
- Was disk changed?
- Was a document edited?
- What devices were attached
- Encrypted files
- Web sites visited
- 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
- Smart phones
- Printers
- CD / DVDs
- Game boxes
- Networks
  - Logs
  - Intercepts/traces

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.

Digital Forensics Cases

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

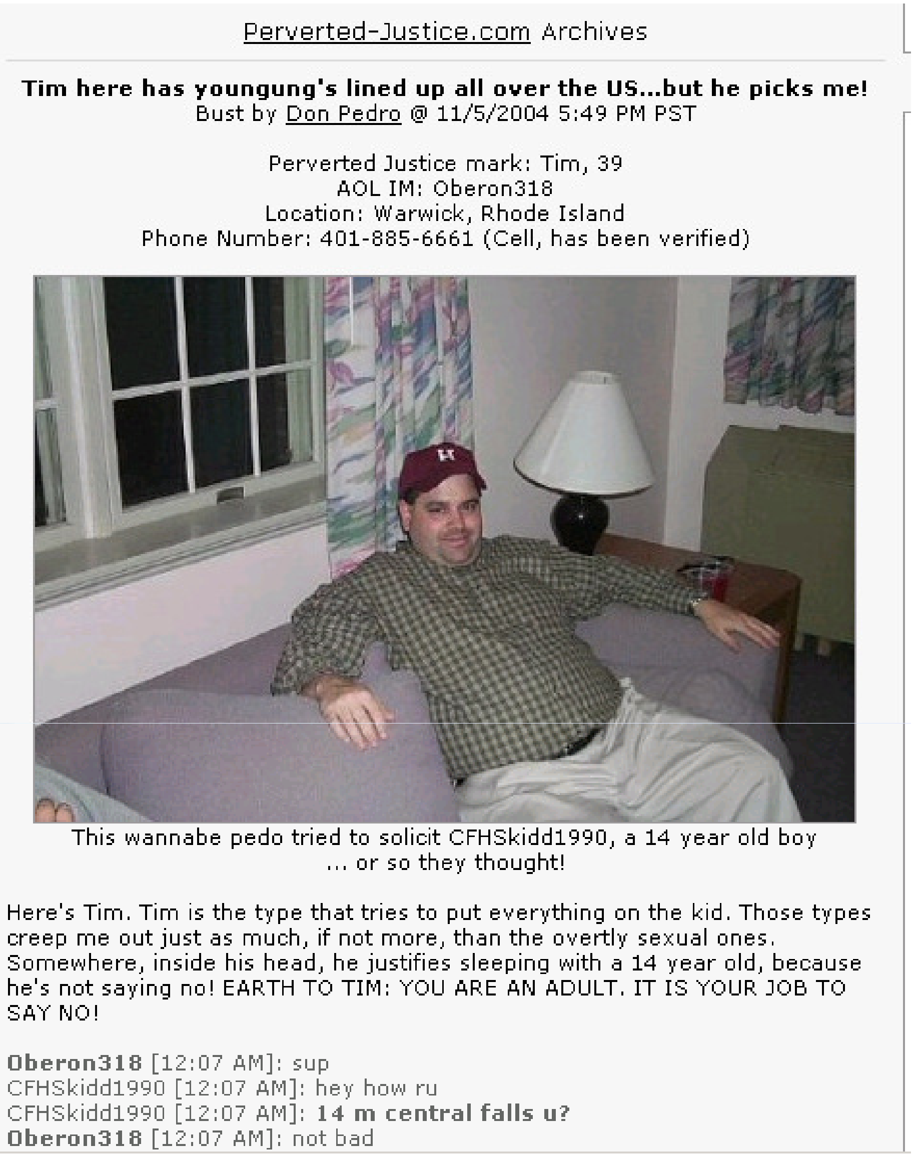
BY DANIEL BARBARISI
Journal Staff Writer

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

School administrators held an assembly yesterday morning to tell students that Tin 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 ni 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!

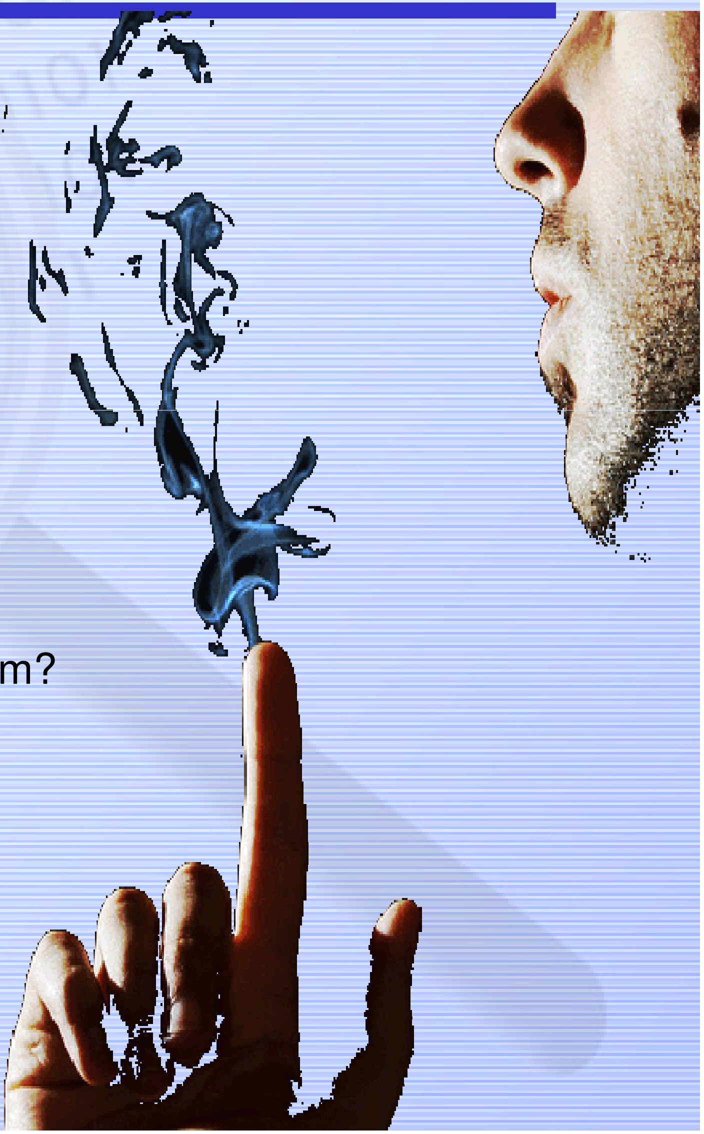
Oberon318 [12:07 AM]: sup
CFHSkidd1990 [12:07 AM]: hey how ru
CFHSkidd1990 [12:07 AM]: **14 m central falls u?**
Oberon318 [12:07 AM]: not bad

PERVERTED-JUSTICE.COM

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

URI Digital Forensics Center Cases

- **Political corruption**
  - Back door to town computer system
- **Suicide**
  - Suicide web sites, email from girlfriend
- **Murder**
  - Who did he know, who was he talking to?
- **School sexual assault**
  - IMs posted on Live Journal, edited?
- **School teacher inappropriate computer use**
  - Porn on the computer – who put it there? Simply spam?
- **Divorce**
  - Infidelity shown in emails
- **Corporate Espionage**
  - Company data to competitor – how did it get there?
- **Stalking**
  - Physical evidence of stalking, emails confirm?

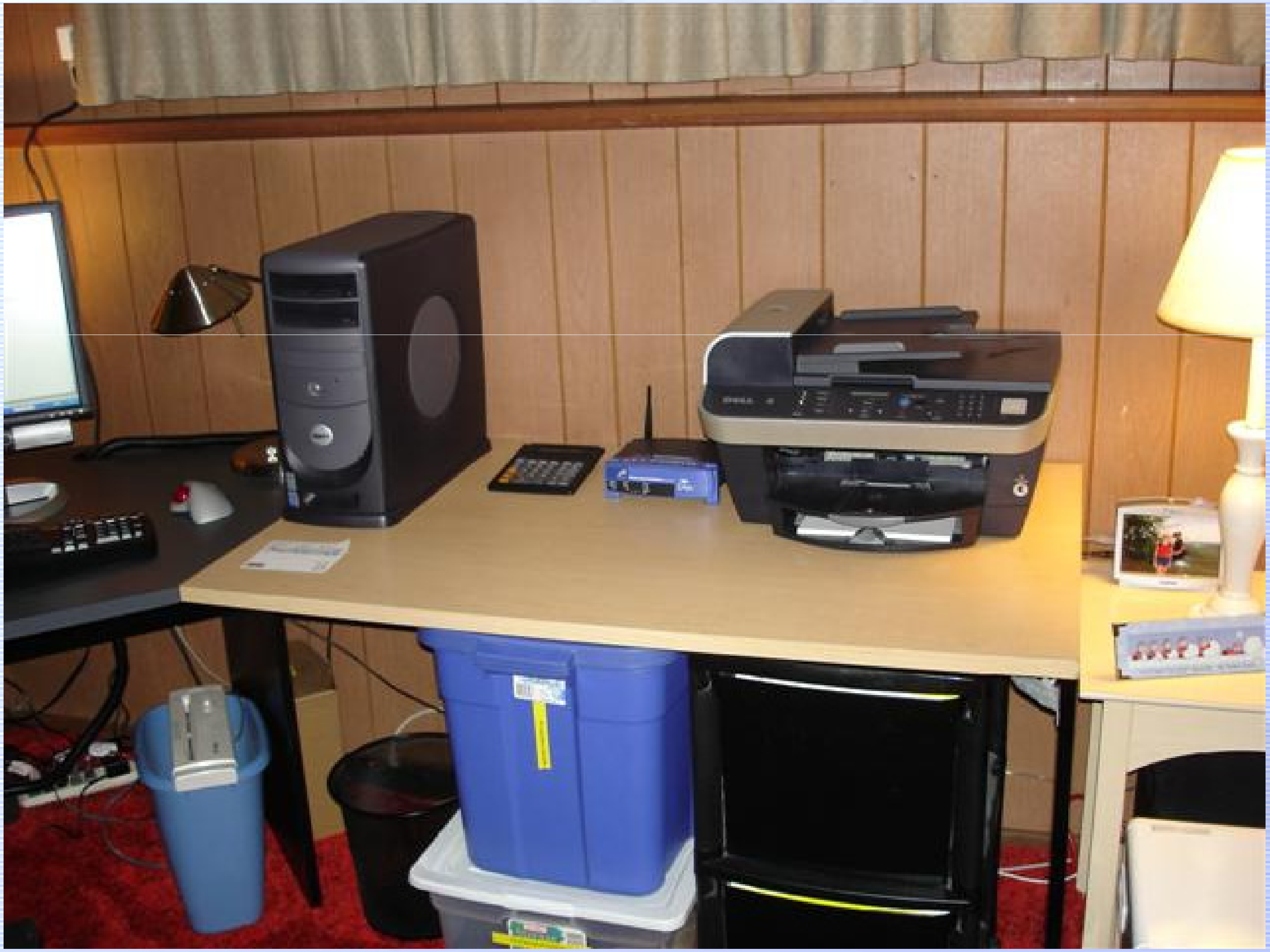


How Can Digital Evidence Be Used?

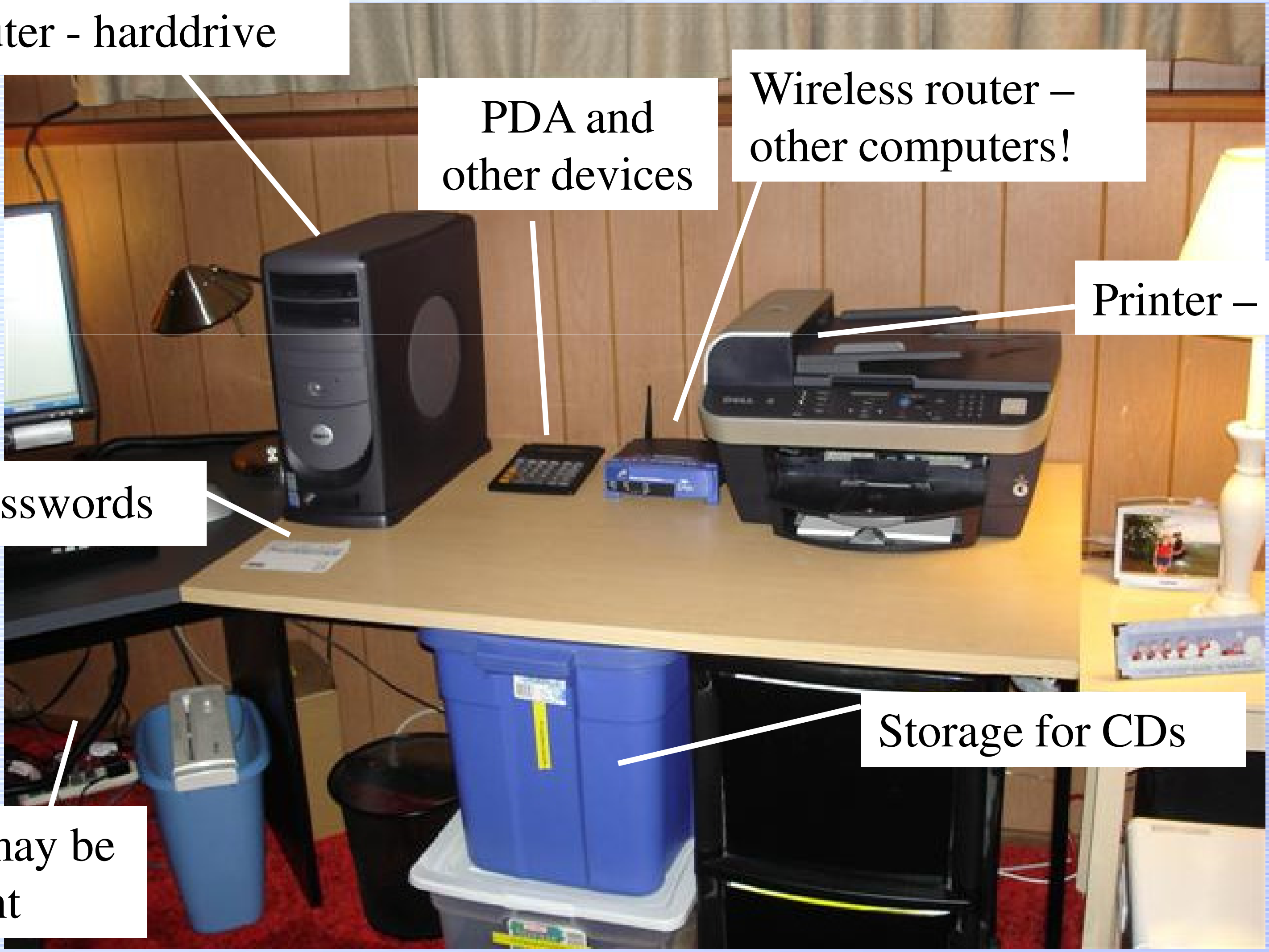
- 4th Amendment - No “unreasonable” search and seizure
  - Computer data and network activity is private
  - Warrant (probable cause) required for government agents
  - Exceptions to Warrant:
    - Permission (father, workplace)
    - Plain view
- Rules of Evidence – Computer data is treated as document
- Very strict expectations on digital evidence in courts
- Frye & Daubert tests of scientific admissibility
- New challenges
  - E.g. image originality

Digital Forensics Practice and Procedures

Crime Scene



Crime Scene



Computer - harddrive

PDA and other devices

Wireless router – other computers!

Printer – memory

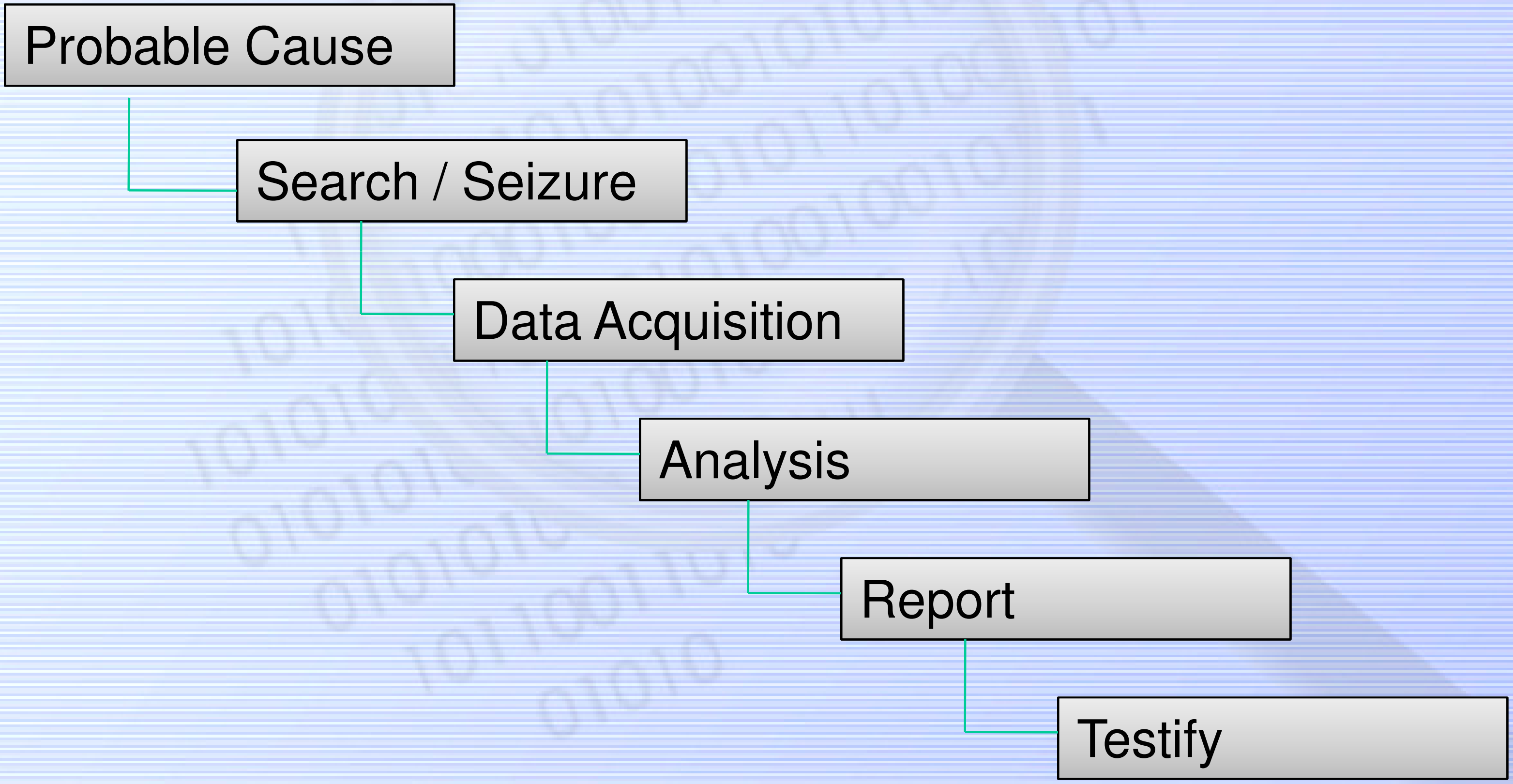
Paper - passwords

Storage for CDs

Cables may be important

Corporate Crime Scene

Digital Forensics Procedure



Probable Cause

Search / Seizure

Data Acquisition

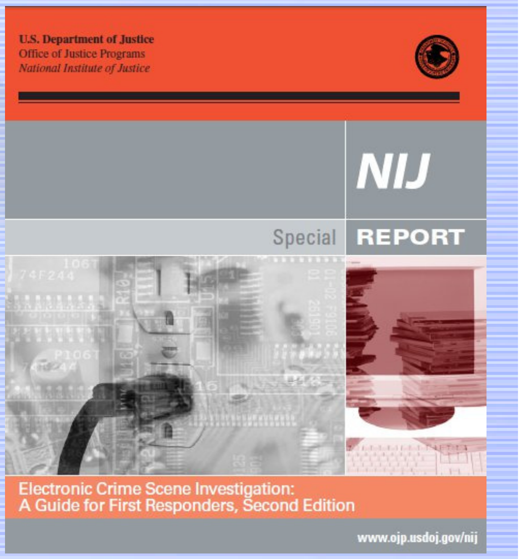
Analysis

Report

Testify

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


U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

NIJ

Special REPORT

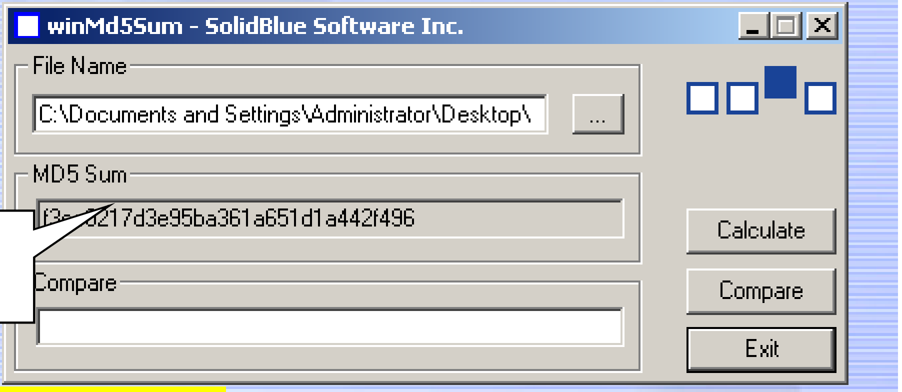
Electronic Crime Scene Investigation:
A Guide for First Responders, Second Edition

www.ojp.usdoj.gov/nij

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.



winMd5Sum - SolidBlue Software Inc.

File Name: C:\Documents and Settings\Administrator\Desktop\

MD5 Sum: f3ec0217d3e95ba361a651d1a442f496

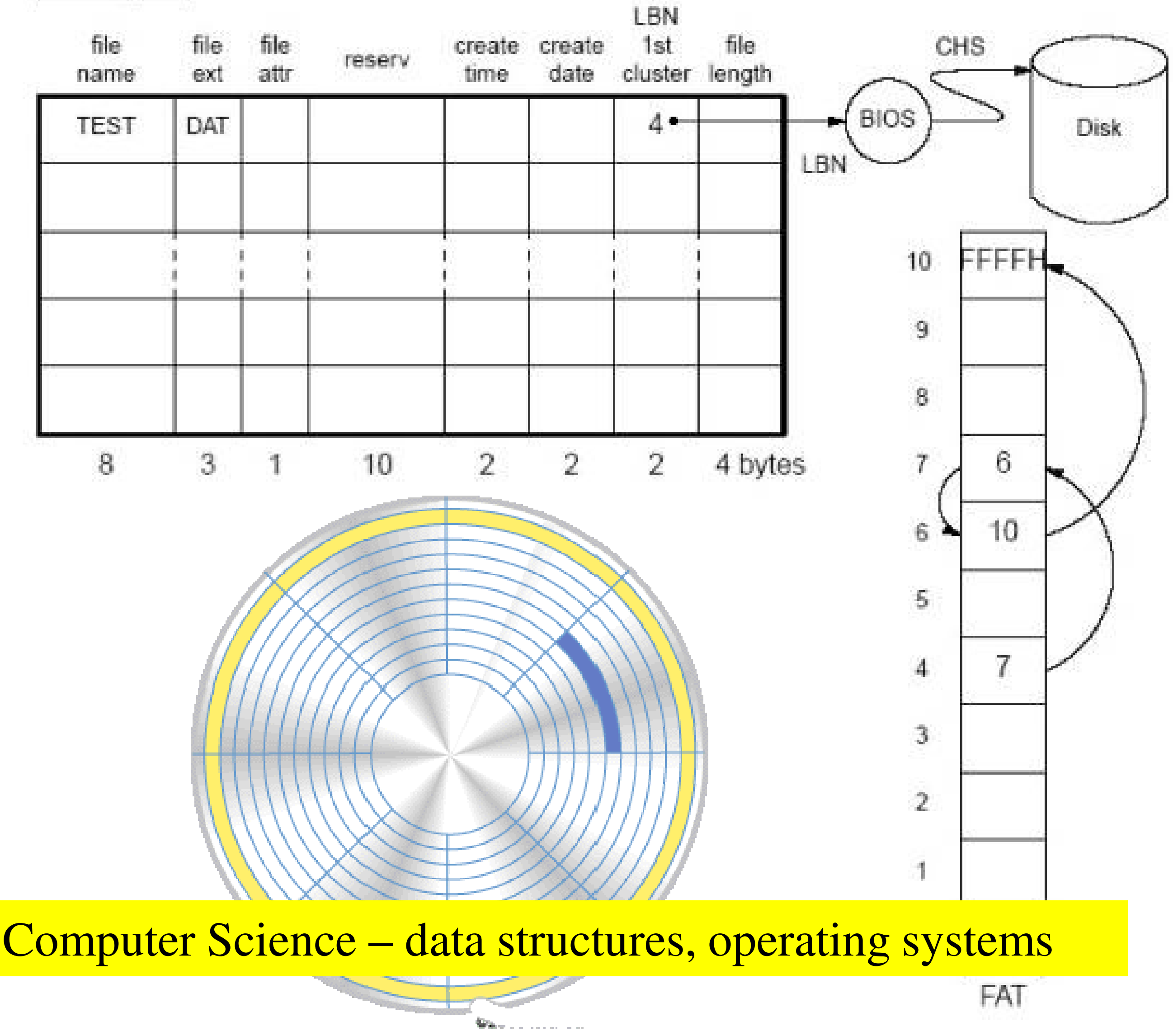
Compare:

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



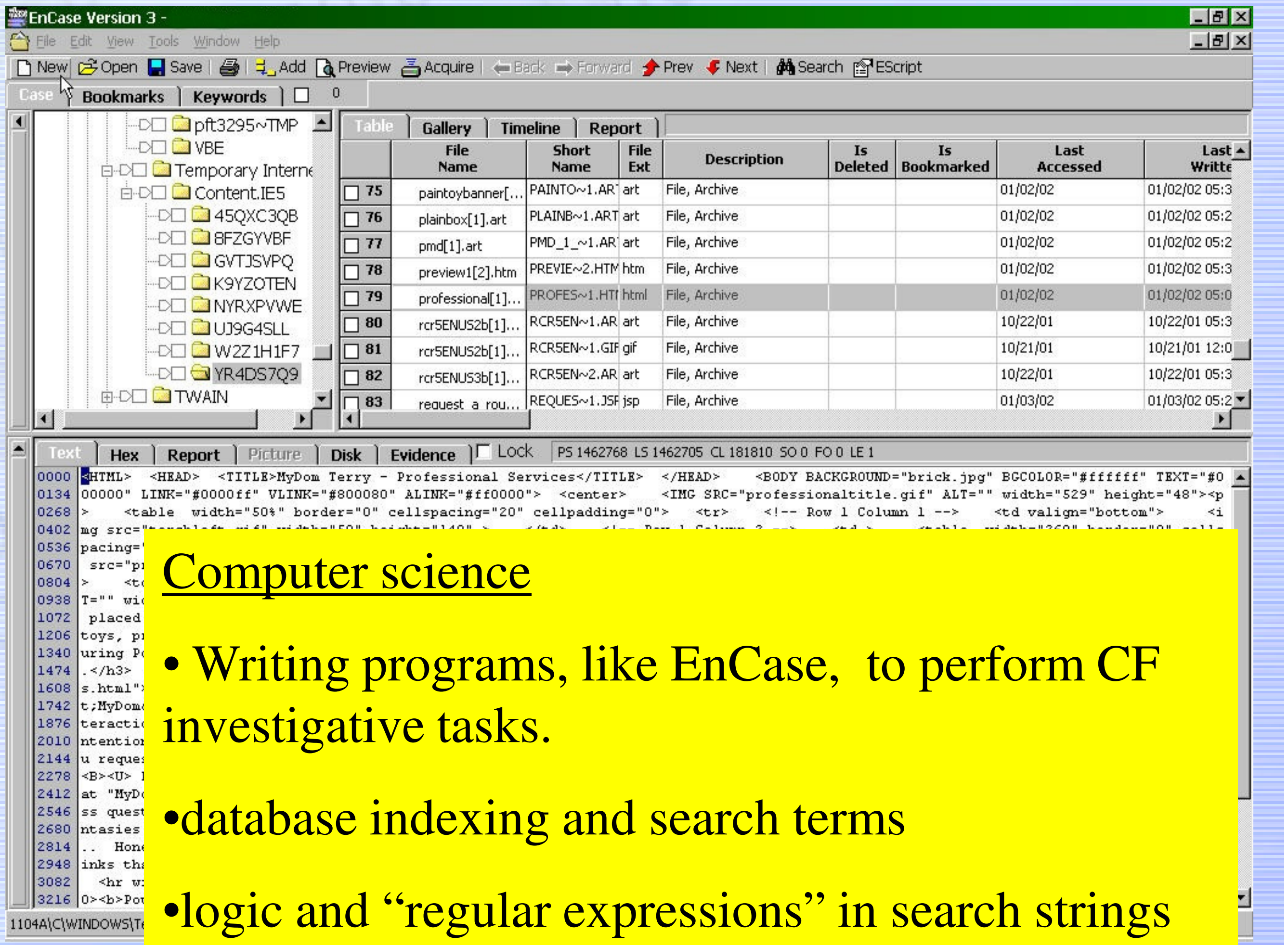
file name	file ext	file attr	reserv	create time	create date	LBN 1st cluster	file length
TEST	DAT					4	
8	3	1	10	2	2	2	4 bytes

10	FFFFH
9	
8	
7	6
6	10
5	
4	7
3	
2	
1	

Computer Science – data structures, operating systems

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



	File Name	Short Name	File Ext	Description	Is Deleted	Is Bookmarked	Last Accessed	Last Writte
□ 75	paintoybanner[...	PAINTO~1.AR	art	File, Archive			01/02/02	01/02/02 05:3
□ 76	plainbox[1].art	PLAINB~1.ART	art	File, Archive			01/02/02	01/02/02 05:2
□ 77	pmd[1].art	PMD_1_~1.AR	art	File, Archive			01/02/02	01/02/02 05:2
□ 78	preview1[2].htm	PREVIE~2.HTM	htm	File, Archive			01/02/02	01/02/02 05:3
□ 79	professional[1]...	PROFES~1.HT	html	File, Archive			01/02/02	01/02/02 05:0
□ 80	rcr5ENUS2b[1]...	RCR5EN~1.AR	art	File, Archive			10/22/01	10/22/01 05:3
□ 81	rcr5ENUS2b[1]...	RCR5EN~1.GIF	gif	File, Archive			10/21/01	10/21/01 12:0
□ 82	rcr5ENUS3b[1]...	RCR5EN~2.AR	art	File, Archive			10/22/01	10/22/01 05:3
□ 83	request a rou...	REQUES~1.JSF	jsp	File, Archive			01/03/02	01/03/02 05:2

PS 1462768 LS 1462705 CL 181810 SO 0 FO 0 LE 1

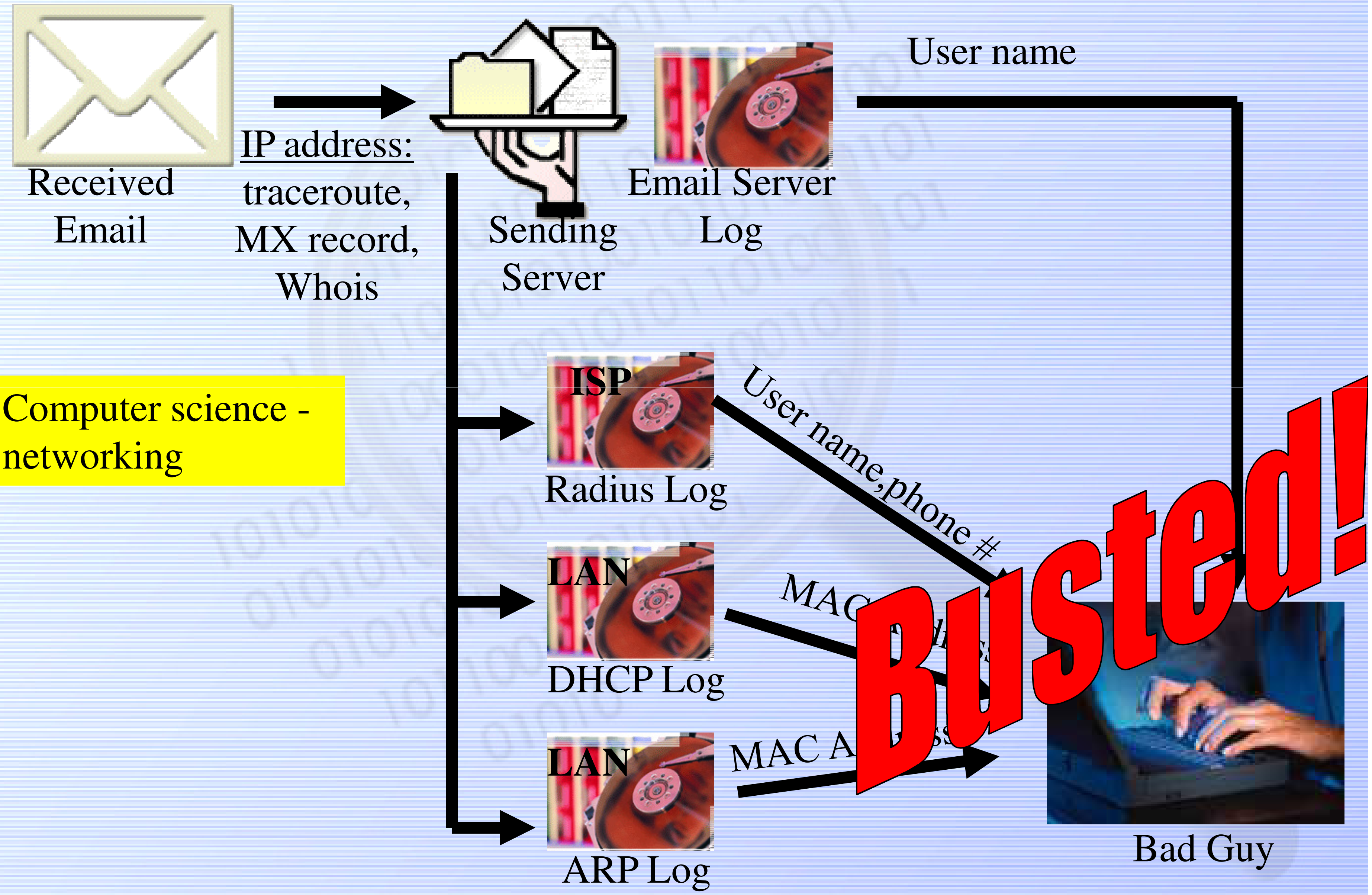
```
0000 <HTML>  <HEAD>  <TITLE>MyDom Terry - Professional Services</TITLE>  </HEAD>    <BODY BACKGROUND="brick.jpg" BGCOLOR="#ffffff" TEXT="#0
0134 00000" LINK="#0000ff" VLINK="#800080" ALINK="#ff0000">  <center>    <IMG SRC="professionaltitle.gif" ALT="" width="529" height="48"><p
0268 >    <table  width="50%" border="0" cellspacing="20" cellpadding="0">    <tr>    <!-- Row 1 Column 1 -->    <td valign="bottom">    <i
0402 mg src=
0536 pacing=
0670  src="pr
0804 >    <tc
0938 T="" wic
1072  placed
1206 toys, pr
1340 uring Pc
1474 .</h3>
1608 s.html"
1742 t;MyDomc
1876 teractic
2010 ntentior
2144 u reques
2278 <B><U> I
2412 at "MyDc
2546 ss quest
2680 ntasies
2814 ..  Hone
2948 inks tha
3082   <hr wi
3216 0><b>Pou
```

1104A\C\WINDOWS\Te

Computer science

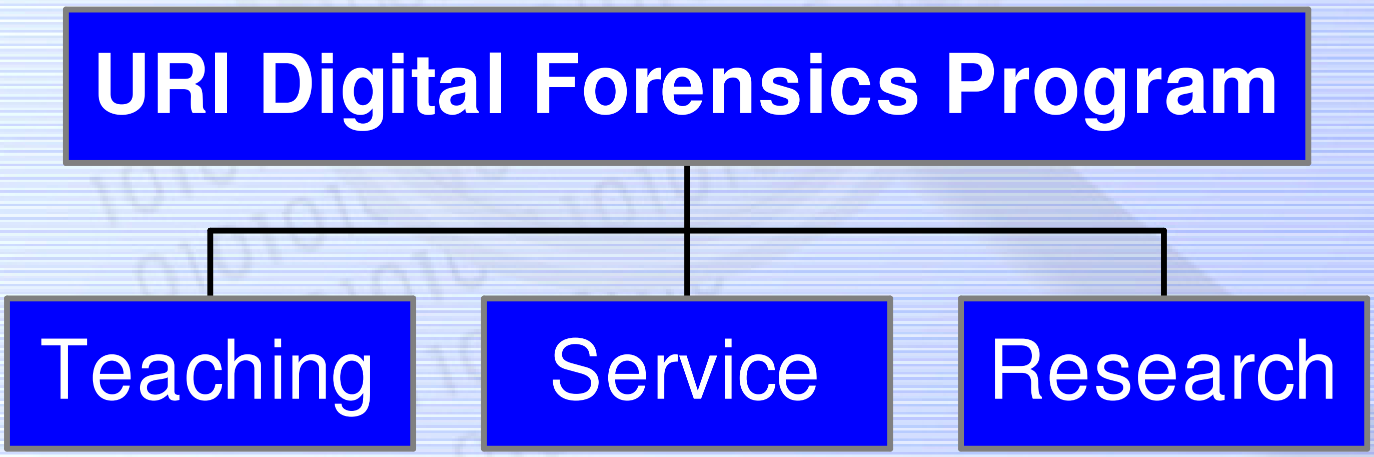
- Writing programs, like EnCase, to perform CF investigative tasks.
- database indexing and search terms
- logic and “regular expressions” in search strings

Email Trace



Computer science - networking

Digital Forensics @ URI

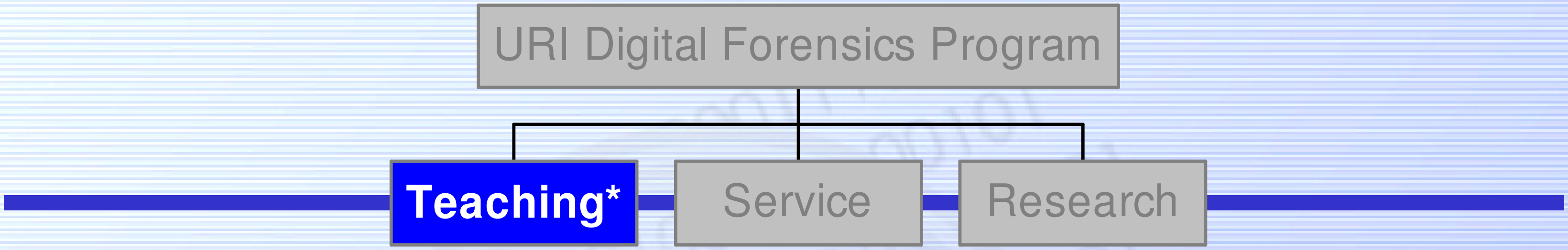


URI Digital Forensics Program

Teaching

Service

Research



URI Digital Forensics Program

Teaching*

Service

Research

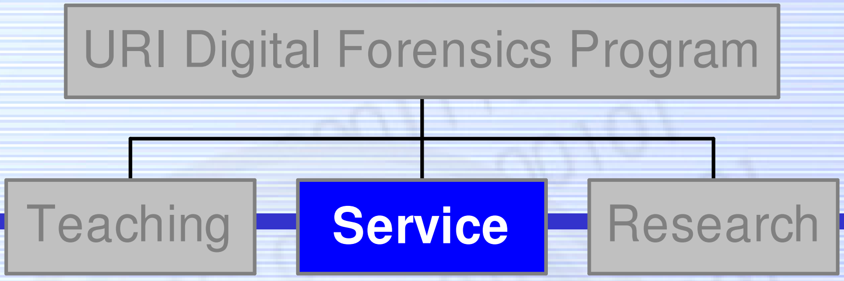
- **Courses:**
  - Taught By IRS Computer Crimes Special Agent Dan Dickerman and URI faculty and staff
  - Computer Forensics (2)
  - Network Forensics (2)
  - Basic Courses (2)
- **Digital Forensics Minor**
  - Can be done with any major
  - CS is the best to provide depth

- **Internships**
  - RI State Police
  - Naval Criminal Investigative Service
  - FBI, IRS, Secret Service
  - Local Police
  - Local companies
  - URI Digital Forensics Center
- Paid summer internships in the DFC
  - National Science Foundation REU program

http://forensics.cs.uri.edu

New URI Cyber Security Curriculum

- URI starting new program in Cyber Security
- Undergrad minor
- Courses:
  - Information Assurance
  - Incident Response
  - Intrustion Detection and Security
  - Ethical Hacking
  - Secure Programming
- First offering is *Information Assurance* this Spring
- Contact Dr. DiPippo or Dr. Fay-Wolfe for more information



URI Digital Forensics Program

Teaching

Service

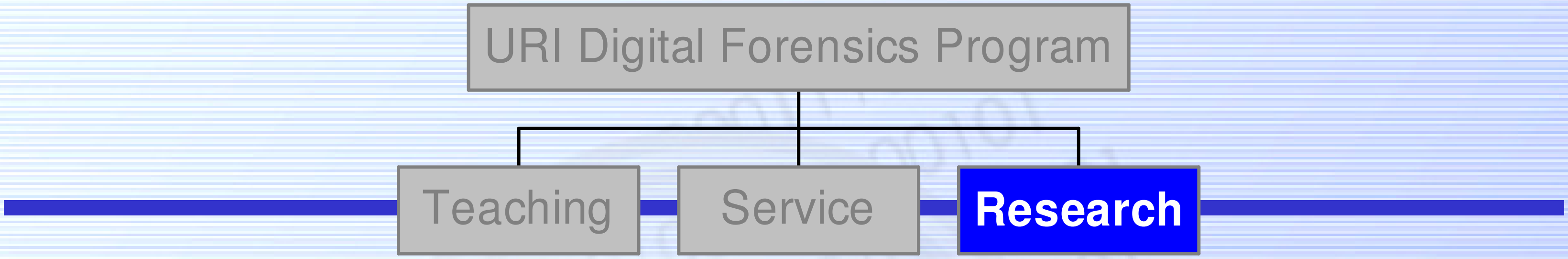
Research

University of Rhode Island
DIGITAL FORENSICS CENTER
An Independent Provider of Computer Investigation Services

- **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

- **Consulting**
  - URI DFC built the RI State Police Computer Crimes Lab



URI Digital Forensics Program

Teaching

Service

Research

THE UNIVERSITY OF RHODE ISLAND

Human Image Detection

Problem

- In a Child Pornography investigation, law enforcement investigators manually sort through 100s of thousands of images. The current practice is:
  - Error prone
  - Time-consuming
  - Creates backlogs
  - Wears on the investigator

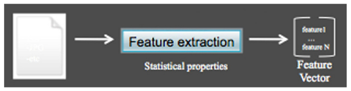
Current Practice

- Hash sets are *insufficient*:

  - Hash sets only capture known child pornography, not new images.
  - Hash sets are easily bypassed.
  - Hash sets don't work for video, which is an increasingly prominent form of distribution.

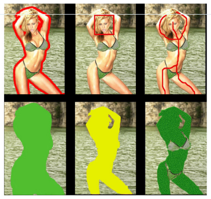
Research – Machine Learning

- Feature extraction and machine learning using Support Vector Machines (SVM) and Linear Discriminant Analysis (LDA):



Human Image Features

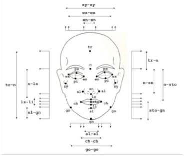
- Six Categories For Human Image Features:

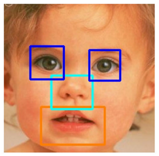


  - Edge detection
  - Face detection
  - Limb detection
  - Mass detection
  - Skin tone detection
  - Texture analysis

Child Detection

- Anthropometric models used to identify children in images based on facial feature extraction





RedLight Software

- Released free to law enforcement in 2010. The current tool is:
  - As accurate as commercial porn scanners.
  - Up to 10 times faster – this is important for law enforcement investigators.
  - Extensive search criteria.

THINK BIG WE DO

Digital Forensics Center

Funding support from the U.S. National Institute of Justice
Electronic Crimes Research Program

Research: Automated Human Image Detection For Law Enforcement

Problem – Child Porn Investigations

- Law Enforcement investigators currently manually sort through 100s of thousands of images when investigating a hard drive.
  - This is error prone
  - This is time-consuming, creating backlogs
  - This wears on the investigator
- Hash sets, which are used to identify child porn, are insufficient:
  - Hash sets only capture known child porn, not new
  - Hash sets are easily by-passed – changing one bit mitigates them
  - Hash sets don't work for video

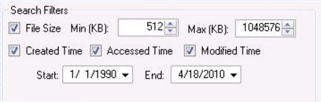
Solution - R&D Tool Development

- Create software tool that identifies human images/pornography based on criteria determined by law enforcement.

- Tool must integrate with law enforcement current tools and practice

- URI developed tool called *RedLight* – released free to law enforcement in 2010.

RedLight Results To Date



Search Filters

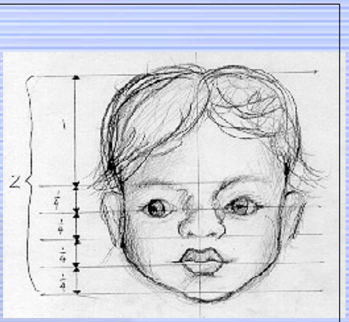
☑ File Size Min (KB): 512 Max (KB): 1048576

☑ Created Time ☑ Accessed Time ☑ Modified Time

Start: 1/ 1/1990 End: 4/18/2010

- RedLight is as accurate as commercial porn scanners
- Redlight is up to 10 times faster – this is important to law enforcement investigators
- RedLight has extensive search criteria
- Redlight is easily upgradeable to incorporate new research

RedLight Current Work



- Add automated detection of children
  - Use facial proportions extracted from images
  - RedLight will be 2 pass: porn, then child

- Add detection of porn/child porn in video

THE UNIVERSITY OF RHODE ISLAND

Cloud Forensics

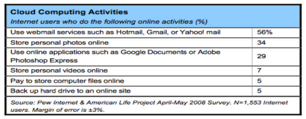
Cloud Computing

- Applications and data storage are provided as services to the user via the internet.
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS)
  - Infrastructure as a Service (IaaS)

amazon web services™ Microsoft® Office 365 Dropbox Google Docs

Future Development

- IDC Estimates
  - $16B in 2010
  - $56B by 2014



Cloud Computing Activities *Internet users who do the following online activities (%)*	
Use webmail services such as Hotmail, Gmail, or Yahoo! mail	56%
Store personal photos online	34
Use online applications such as Google Documents or Adobe Photoshop Express	29
Store personal videos online	7
Pay to store computer files online	5
Back up hard drive to an online site	5

Source: Pew Internet & American Life Project April-May 2008 Survey. N=1,553 Internet users. Margin of error is ±3%.

- By 2013 it is estimated that 60% of the server workloads will be performed by virtual servers

Problems

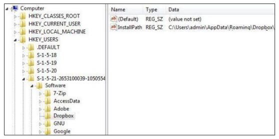
- Law Enforcement must know cloud was used
- Evidence is difficult for law enforcement to seize
  - Evidence is remote
  - Evidence is vast
  - Evidence has complex structure
  - Evidence can remotely changed by suspect

Solution

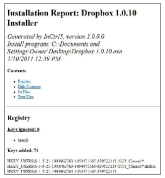
- Law Enforcement issues remote warrant to provider
- Valid warrant must have :
  - Which cloud app was used
  - Time of use
  - Associated username
- Create a tool to generate warrant information from seized devices (e.g. computers, phones, iPad)

Plan of Action

- Perform research on test machines to analyze where cloud applications store data remnants and what information resides in these remnants



Name	Type	Data
(Default)	REG_SZ	(value not set)
InstallPath	REG_SZ	C:\Users\admin\AppData\Roaming\Dropbox\



Installation Report: Dropbox 1.0.10 Installer

Generated by InCtrl5, version 1.0.0.0
Install program: C:\Documents and Settings\Owner\Desktop\Dropbox 1.0.10.exe
1/10/2011 12:39 PM

Contents

- Registry
- Disk Contents
- Ini Files
- Text Files

Registry

Keys ignored: 0

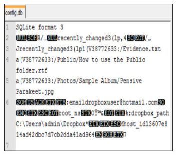
- (none)

Keys added: 71

HKEY_USERS\S-1-5-21-1993962763-1454471165-839522115-1003_Classes\*
HKEY_USERS\S-1-5-21-1993962763-1454471165-839522115-1003_Classes\*\shellex
HKEY_USERS\S-1-5-21-1993962763-1454471165-839522115

Examples of Remnants

- Google Docs Cached Web Sites
  - Start Page - https://docs.google.com
  - Create a Document - https://docs.google.com/documentary/create?hl=en
- Drop Box
  - Creates an SQLite file, config.db. This file contains various information such as the user's email address



config.db

```
SQLite format 3
NULSOHR/…NULrecently_changed3(lp,4SOEOT/„
Jrecently_changed3(lp1(V38772633:/Evidence.txt
a(V38772633:/Public/How to use the Public
folder.rtf
a(V38772633:/Photos/Sample Album/Pensive
Parakeet.jpg
SOHUSACKETXETB;emaildropboxuser@hotmail.comSO
ENQETXESCEOTroot_nsSTXOŸ™&EOTETX%;dropbox_path
C:\Users\admin\Dropbox*ETXETXESCMhost_id13607e8
14ad42dbc7d7cb2dda41ad964EMSOHETX7

```

Impact - Law Enforcement will be able to gather evidence from the cloud

THINK BIG WE DO

Digital Forensics Center

THE UNIVERSITY OF RHODE ISLAND

Cell Phone Forensics

Problem

- Different tools claim different amounts of support for each mobile device.
- There is currently no place to find which tool will get the best results for a given mobile device.

Solution

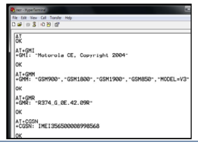
- Test tools in URI Lab
- Create online, searchable reference for Law Enforcement
  - Create a database of mobile devices and what each tool will retrieve from the device.
  - Create archive of URI test reports on tools and devices.

Recoverable Items

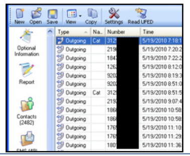
- Items that can be retrieved from a cell phone:
  - Contacts
  - Call logs
  - Calendar
  - SMS
  - Pictures
  - Videos
  - Audio Files
  - ESN/IMEI
  - Full File System
  - Physical dump

Analysis Tool Growth

- Tools have grown more user friendly and less technical
  - More graphical interfaces
  - Point and click rather than technical knowledge



```
AT
OK

AT+GMI
+GMI: "Motorola CE, Copyright 2004"

OK

AT+GMM
+GMM: "GSM900","GSM1800","GSM1900","GSM850","MODEL=V3"

OK

AT+GMR
+GMR: "R374_G_0E.42.09R"

OK

AT+CGSN
+CGSN: IMEI356500008998568

OK
```



Type	Na..	Number	Time
Outgoing	Cat	312[redacted]	5/19/2010 7:18:1
Outgoing		219[redacted]	5/19/2010 7:20:2
Outgoing		184[redacted]	5/19/2010 7:22:2
Outgoing		126[redacted]	5/19/2010 8:12:0
Outgoing		920[redacted]	5/19/2010 8:19:3
Outgoing		920[redacted]	5/19/2010 8:51:0
Outgoing	Cat	312[redacted]	5/19/2010 8:51:5
Outgoing		219[redacted]	5/19/2010 9:07:4
Outgoing		186[redacted]	5/19/2010 10:58
Outgoing		186[redacted]	5/19/2010 10:58
Outgoing		176[redacted]	5/19/2010 11:10
Outgoing		176[redacted]	5/19/2010 11:29
Outgoing		180[redacted]	5/19/2010 11:36

Research

- Test tools with popular mobile devices
  - Work with leading refurbishing company to determine which phones are most popular and get some test phones
  - Test tools to determine the validity of the manufacturers' claims for support.

Impact

- Release on the ECTCoE website
- This reference will be the place to go for investigators to determine which tool to try before wasting time with other tools.

NIJ ECTCOE Electronic Crime Technology Center of Excellence

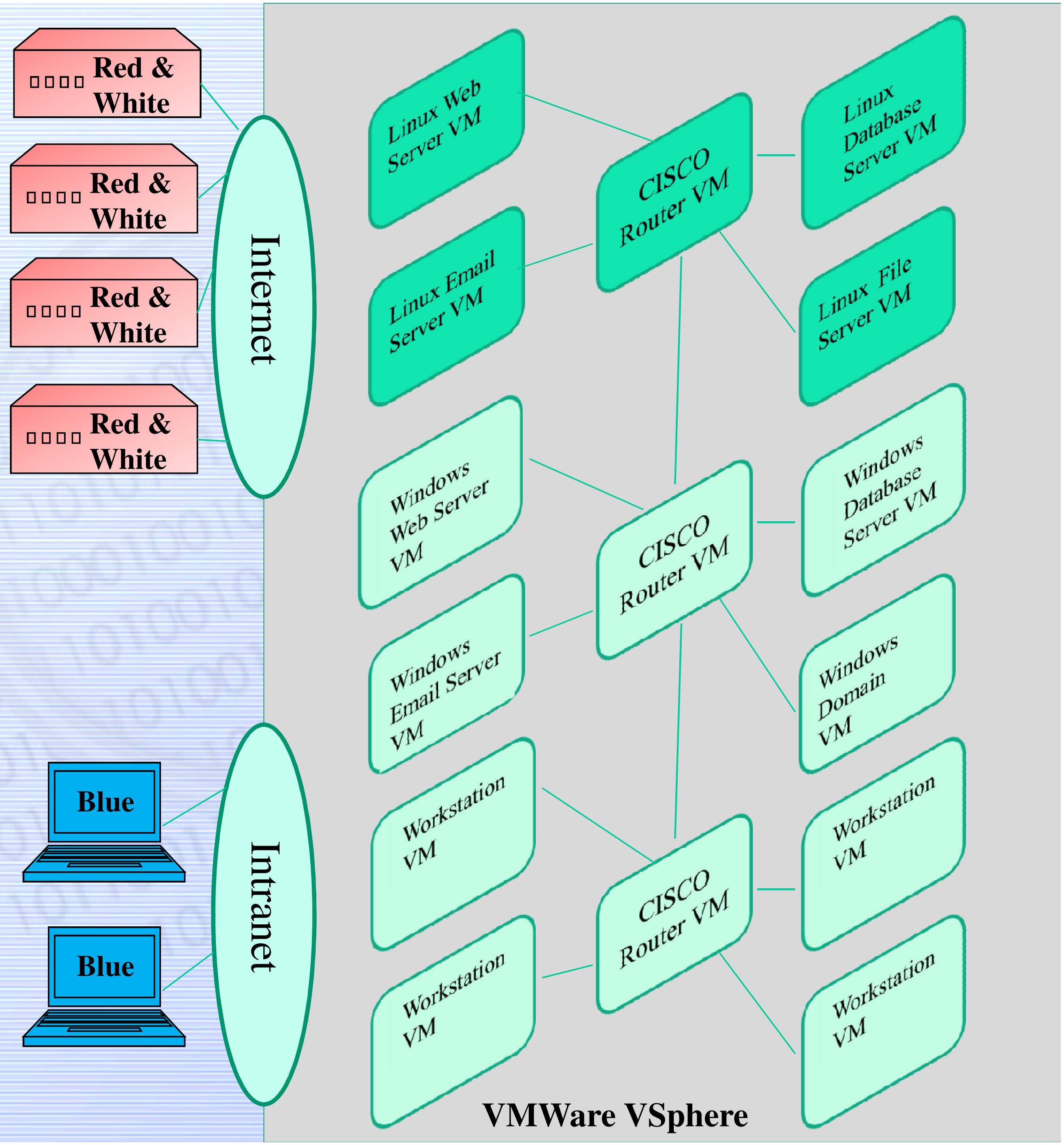
THINK BIG WE DO

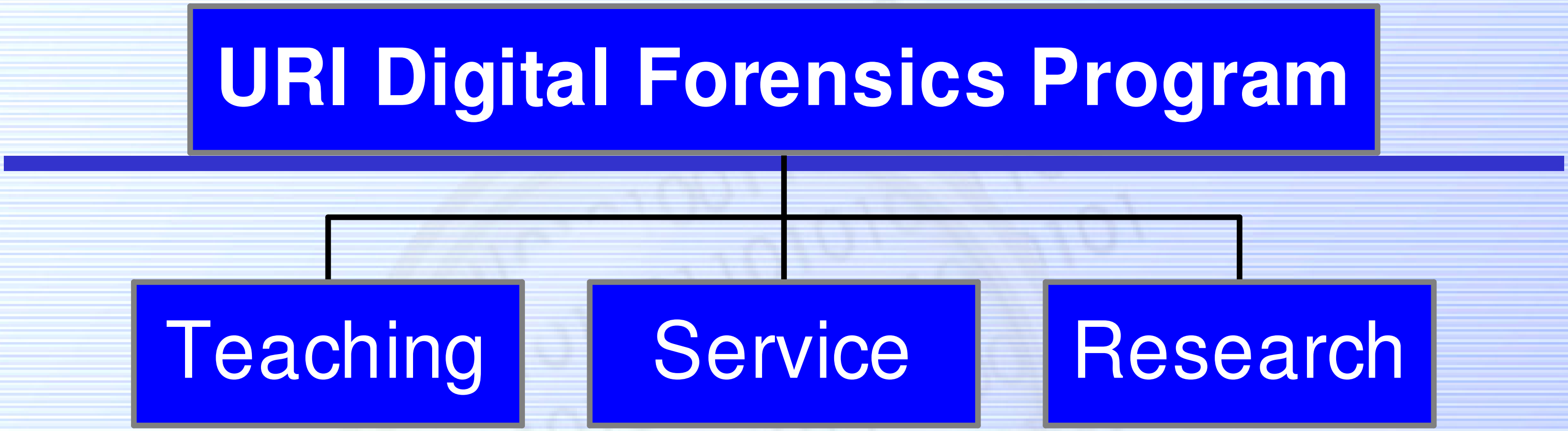
Digital Forensics Center

In partnership with the ECTCoE
With support from University of Rhode Island Division of Research

Open Cyber Challenge Platform

- Blue team defends network and data
- White team is normal use
- Red team is attackers





URI Digital Forensics Program

Teaching

Service

Research

Dr. Victor Fay-Wolfe

University of Rhode Island

Director, Digital Forensics Program

wolfe@cs.uri.edu

http://forensics.cs.uri.edu