COMPUTER FORENSICS TEACHING RESOURCE WORKSHOP

CAE-CD Community Symposium

Westin Peachtree Plaza Hotel

Atlanta Georgia, June 8-10, 2022

Dr. Alfredo Cruz, Ph.D.

Politechnic University of
Puerto Rico San Juan

Jeffrey L. Duffany, Ph.D.

Ana G. Mendez University

Gurabo, Puerto Rico

WHAT IS COMPUTER FORENSICS AND DIGITAL EVIDENCE

Computer forensics is a branch of computer science that uses hardware and software to find and extract digital evidence found in computers and digital storage media.

Digital evidence or ***electronic evidence*** is any information stored or transmitted in digital form that can be used by law enforcement agencies or in a court of law.

COMPUTER FORENSICS AND CYBER DEFENSE

- To analyze a computer system after a break-in, for example, to determine how the attacker gained access and what the attacker did.
- To develop countermeasures to prevent or mitigate the the impact of cyberattacks.
- To determine who is originating the cyberattacks.
- To recover from the damages inflicted by cyberattacks.

COMPUTER FORENSIC AREAS

- Personal Computers
  - Hard Drive Forensics
  - Solid State Drive Forensics
- Network Forensics
- Mobile Device Forensics
  - cell phone
  - laptop
  - usb
  - ipad
  - tablet

PERSONAL COMPUTER FORENSICS

- Hard Drive Forensics
- Solid State Drive Forensics
- RAM Memory Forensics
- Recovering Deleted Files
- Hex Editors
- Hidden Files
- Hidden Information
- Internet Temporary Files
- Electronic Mail
- Drive Encryption and Password

NETWORK FORENSICS

Network Forensics is the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents.

Switch, Firewall, Router and Web Server Logs

Packet Capture Tools such as Wireshark

Intrusion Detection Systems

Honeypots

EXAMPLE CASES

Financial crimes

Drug crimes

Industrial Espionage

Denial of Service

Counterfeiting

Murder

Terrorism

Hacking

POLITECHNIC UNIVERSITY OF PUERTO RICO

Main Campus Located in San Juan, Puerto Rico

Undergraduate and Graduate Computer Science

NSA Center of Academic Excellence in Cyber Defense

NSF Scholarship for Service Program

Teaching Computer Forensics since 2008

CECS 7235 Computer Forensics (Fall)

CECS 7237 Advanced Computer Forensics (Spring)

GRADUATE CERTIFICATE IN DIGITAL FORENSICS (GCDF)

Provide a thorough and rigorous introduction to computer forensics and computer and network security.

Provide a quality educational experience that balances classroom theory with practical hands-on lab experience.

Create an infrastructure that supports faculty and student research.

POLITECHNIC UNIVERSITY OF PUERTO RICO

GRADUATE CERTIFICATE IN DIGITAL FORENSICS

TOTAL OF 18 CREDITS REQUIRED COURSEWORK:

CECS 6046 – Electronic Discovery & Digital Evidence

CECS 6130 – Data Communication Networks

CECS 7230 – Network Security

CECS 7235 – Computer Forensics

CECS 7237 – Advanced Computer Forensics

CECS 7570 – Computer Security

COMPUTER FORENSICS TEACHING RESOURCES

Nelson/Phillips Textbook

Andrew Blitz Lab Manual

Forensic Software Tools

- Autopsy
- FTK Imager
- Disk Editor

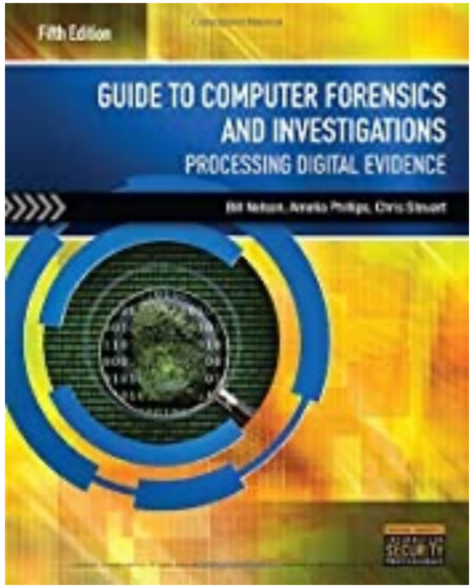
NIST CFTT Website

Digital Corpora Website

DFRWS Website

CECS 7235 TEXTBOOK

References: *Guide to Computer Forensics and Investigations*, Fifth Edition, 2015, Bill Nelson, Amelia Phillips, Christopher Steuart, Course Technology, Cengage Learning ISBN: 978-1285060033.


Fifth Edition
GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS
PROCESSING DIGITAL EVIDENCE
Bill Nelson, Amelia Phillips, Chris Steuart

This is the required textbook for the introductory course (cecs 7235). Most of the lab exercises for CECS 7235 come from this book.

It is used mainly as a reference for the cecs 7237 advanced computer forensics course.

CECS 7235 COURSE SYLLABUS

Computer forensics is a survey course that covers all major topics in computer forensics.

Topics such as Locards Exchange Principle, 4th amendment, crime scene analysis, drive imaging, evidence searching, hash functions, recovering deleted files, data carving methods, photograph metadata, EXIF, email, cellphones, mobile device forensics, expert witnesses and courtroom procedures are discussed.

Students gain enhanced skills by performing hands-on lab exercises with computer forensic tools such as Autopsy, Prodiscover and FTK imager

CECS 7237 TEXTBOOK

Textbook: *Lab Manual for Guide to Computer Forensics and Investigations*, Fifth Edition, 2015,

Andrew Blitz, Course Technology, Cengage Learning ISBN-13:978-1285079080.

Fifth Edition
LAB MANUAL FOR GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS
PROCESSING DIGITAL EVIDENCE
Andrew Blitz

This book is mainly used for the lab exercises we do in the second half of the advanced computer forensics course.

It is the required textbook for cecs 7237.

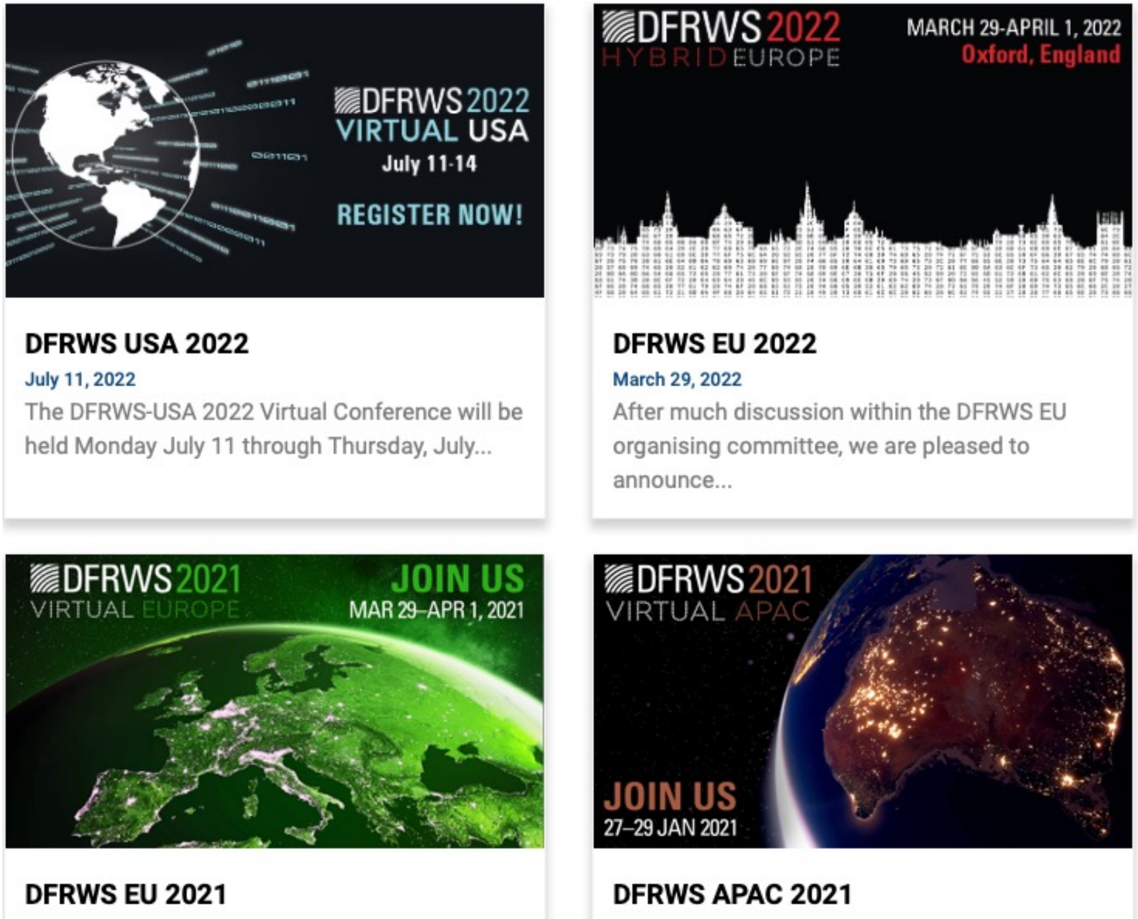
CECS 7237 COURSE SYLLABUS

Advanced computer forensics takes a more in-depth look at operating systems, filing systems and storage media such as Windows, DOS, MAC OSX, Linux, FAT32, FAT16, FAT12, NTFS, hard drives, floppy disks, usb drives, removable media, CD-ROMs, DVDs, and flash drives.

Advanced topics such as solid state drives, Windows registry, data carving methods, anti-forensics, network forensics and cloud forensics are discussed.

Students gain enhanced skills by performing hands-on lab exercises with computer forensic tools such as Autopsy, Prodiscover and FTK imager

Digital Forensics Research Workshop



DFRWS USA 2022

July 11, 2022

The DFRWS-USA 2022 Virtual Conference will be held Monday July 11 through Thursday, July...

DFRWS EU 2022

March 29, 2022

After much discussion within the DFRWS EU organising committee, we are pleased to announce...

DFRWS EU 2021

DFRWS APAC 2021

DFRWS

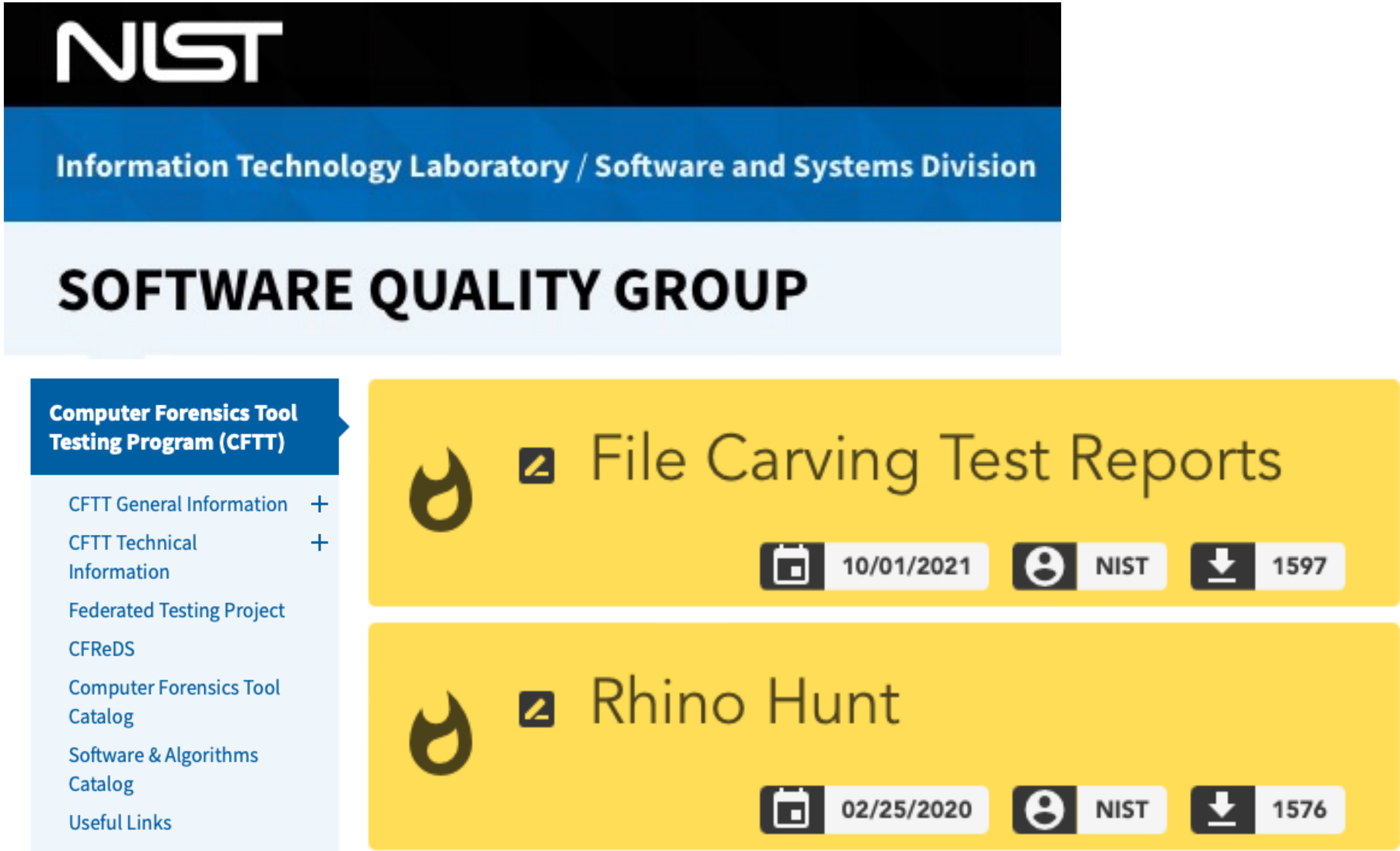
Papers & Presentations

Home › Papers & Presentations

DFRWS

Forensic Challenges

Home › Forensic Challenges



NIST

Information Technology Laboratory / Software and Systems Division

SOFTWARE QUALITY GROUP

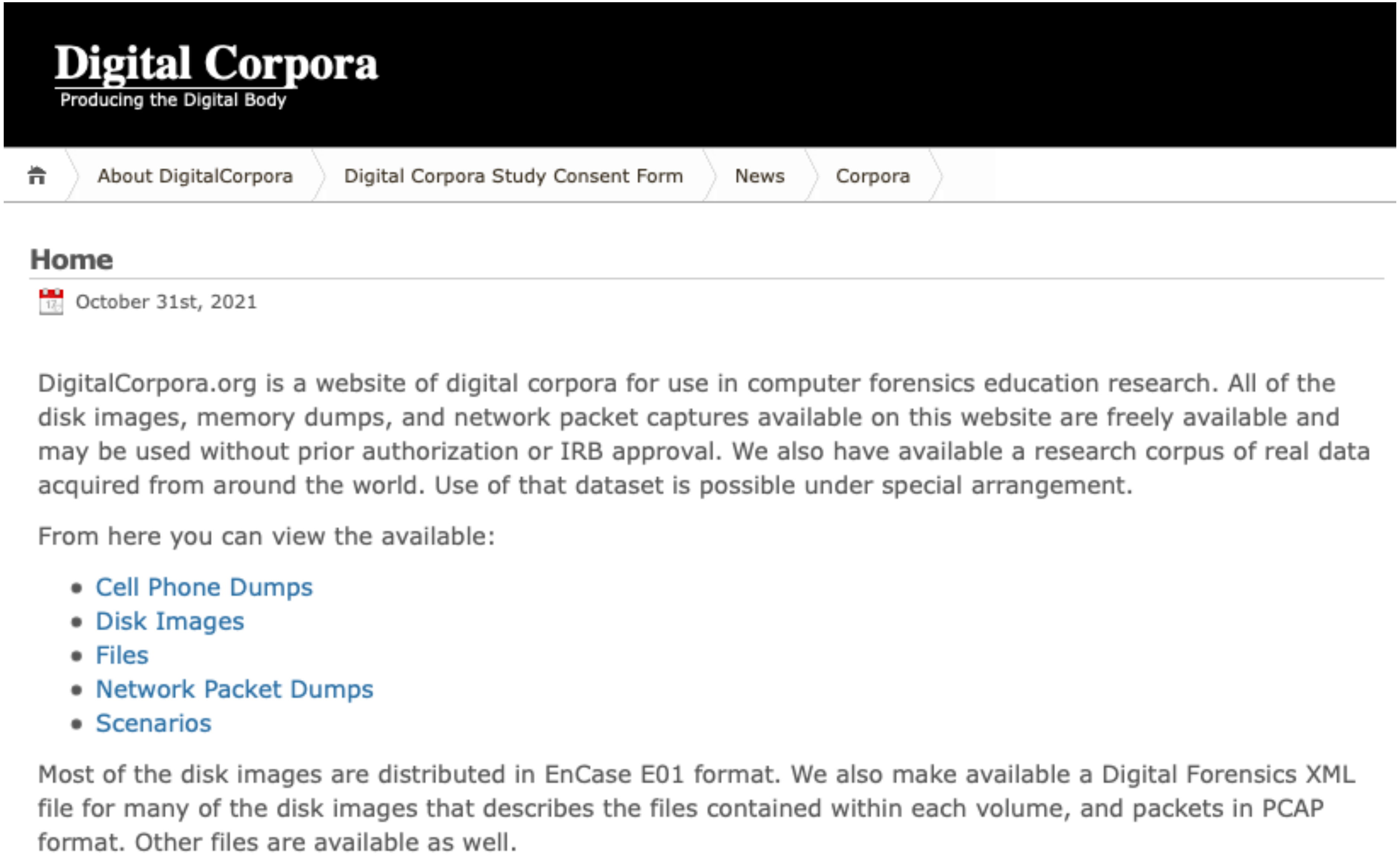
Computer Forensics Tool Testing Program (CFTT)
CFTT General Information +
CFTT Technical Information +
Federated Testing Project
CFReDS
Computer Forensics Tool Catalog
Software & Algorithms Catalog
Useful Links

File Carving Test Reports

10/01/2021 NIST 1597

Rhino Hunt

02/25/2020 NIST 1576


Digital Corpora
Producing the Digital Body
About DigitalCorpora
Digital Corpora Study Consent Form
News
Corpora

Home

October 31st, 2021

DigitalCorpora.org is a website of digital corpora for use in computer forensics education research. All of the disk images, memory dumps, and network packet captures available on this website are freely available and may be used without prior authorization or IRB approval. We also have available a research corpus of real data acquired from around the world. Use of that dataset is possible under special arrangement.

From here you can view the available:

- Cell Phone Dumps
- Disk Images
- Files
- Network Packet Dumps
- Scenarios

Most of the disk images are distributed in EnCase E01 format. We also make available a Digital Forensics XML file for many of the disk images that describes the files contained within each volume, and packets in PCAP format. Other files are available as well.

COMPUTER FORENSIC TOOLS

HARDWARE & SOFTWARE

Hardware

Forensic Machine

Write Blocker

Media Reader

External Image Device

Software

Forensic Examination (GUI)

Forensic Examination (DOS Based)

Disk Editor

Password Cracking

Imaging

Wiping

Hash Routines

Internet History

COMPUTER FORENSIC SOFTWARE

- AccessData (Forensic Tool Kit)
- Guidance Software (Encase)
- Technology Pathways (Prodiscover)
- Paraben (Paradigm P2 Suite)
- Digital Intelligence (FRED)
- Autopsy

PRODISCOVER® Forensics

Guidance SOFTWARE | EnCase

LEARNING RESOURCE CHALLENGES

- Coordinating topics between CECS 7235 and CECS 7237
- Should CECS 7235 be a prerequisite for CECS 7237
- Coordination of Software with IT Department
- Depth vs. breadth of material coverage
- Windows/MACOSX/Linux Compatibility
- Adapt Learning Resources to Teaching Environment
- How to incorporate Forensic Challenges (DFRWS)

questions

?preguntitas?