



Israel Aladejebi
Computer Forensics
Century College
Information Technology Department



Being able to break security doesn't make you a hacker anymore than being able to hotwire cars makes you an automotive engineer.

- Eric S. Raymond



IT Department: Programs

- ◆ Computer Forensics & Investigative Sciences (Newly developed Program)
- ◆ Microcomputer Support Technology
- ◆ Information & Telecommunication Technology

Outline

- ◆ The Department in a Nutshell
- ◆ Computer Forensic Program
- ◆ Computer Forensics Courses
- ◆ Current Challenges
- ◆ Future Plan
- ◆ Q and A





Computer Forensics & Investigative Technology Awards

Program Awards are:

- ◆ Computer Forensics & Investigative Technology AAS Degree (64 credit)
- ◆ Computer Forensics & Investigative Technology Certificate (16 credit)
- ◆ Computer Security & Information Assurance (16 credit)



Computer Forensics Program focus

- ◆ “Try-it-by-hand” approach
 - 65% Labs, 35% Lecture
- ◆ Vendor-independent lab.
 - learn more than just how to use a tool

Computer Forensics Courses

- ◆ **CFIT2065 Introduction to Computer Forensics
3cr**
- ◆ **CFIT2080 Open Source Forensics Methodology
3cr**
- ◆ **CFIT 2070 Windows & NTFS File System
Forensics 3cr**
- ◆ **CFIT2075 Computer Investigative Law for
Forensic Analysts 3cr**





Computer Forensics Courses

- ◆ **CFIT2081 Computer & Network Hacker Security I 3cr**
- ◆ **CFIT2082 Computer & Network Hacker Security II 3cr**
- ◆ **CFIT2083 Secure Communication 3cr**
- ◆ **CFIT2084 Unix Network Admin, Security and Troubleshooting**
- ◆ **CFIT2083 Windows Security 3cr**



Computer Forensics Course

◆ CFIT2065 Introduction to Computer Forensics 3cr

- **This course consists of a comprehensive overview of computer forensics theories, methodologies, and practices.**
- **methods to properly conduct a computer forensics investigation including ethics, tools, procedures and analysis.**

CFIT2080 Open Source Forensics Methodology 3cr



- Students will use Linux tools to analyze multiple OS image to perform investigations.
- This course begins with file system fundamentals but moves rapidly to using advanced toolkits to perform a forensic audit of suspect systems.
- Forensic analysis is performed on gathered evidence contained in "disk images". Using a disk image of a computer involved in an actual forensic case,
- students will apply what they learn in class by investigating the incident in a hands-on setting

CFIT 2070 Windows & NTFS File System Forensics 3cr



- Recover a Rootkit From An SMB Attack Using A Hexeditor
- Perform Hardware and Network Identification on a live system
- Use dd for Windows to Obtain Images
- Perform Imaging of Memory on a live system
- Using Automated Toolkits To Collect Information From Windows Based Systems
- Image an NTFS/FAT file system over File Sharing Enabled Computers Using dd
- Using Autopsy, Foremost, and The Sleuth Kit to Examine NTFS/FAT Image



CFIT2081 Computer & Network Hacker Security I 3cr

◆ Reconnaissance

- What Does Your Network Reveal?
- Are You Leaking Too Much Information?
- Using Whois Lookups, ARIN, RIPE and APNIC
- Domain Name System Harvesting
- Data Gathering from Job Postings, Web Sites and Government Databases

◆ Scanning

- The Art of War Driving to Locate Insecure Wireless LANs
- War Dialing for Renegade Modems
- Port Scanning: Traditional, Stealth and Blind Scanning
- Active and Passive Operating System Fingerprinting
- Firewalking to Determine Firewall Filtering Rules
- Vulnerability Scanning Using Nessus and Other Tools
- CGI Scanning with Whisker

◆ Intrusion Detection System Evasion

- Foiling IDS at the Network Level: Fragmentation and Other Tricks
- Foiling IDS at the Application Level: Exploiting the Rich Syntax of Computer Languages
- Using Fragroute, Fragrouter and Whisker IDS Evasion Tactics

◆ Hands-on Exercises with the Following Tools:

- NetStumbler for Wireless LAN Discovery
- Nmap Port Scanner and Operating System Fingerprinting Tool
- Nessus Vulnerability Scanner
- Enum for Extracting Windows Data Through Null Sessions



CFIT2081 Computer & Network Hacker Security I 3cr

- ◆ Network-Level Attacks
 - Session Hijacking: From Telnet to SSL and SSH
 - Person-in-the-Middle Attacks
 - Passive Sniffing
- ◆ Gathering and Parsing Packets
 - Active Sniffing: ARP Cache Poisoning and DNS Injection
 - DNS Cache Poisoning: Redirecting Traffic on the Internet
 - Using and Abusing Netcat, Including Backdoors and Nasty Relays
 - IP Address Spoofing Variations
- ◆ Operating System and Application-Level Attacks
 - Buffer Overflows in Depth
 - The MetaSploit Exploitation Framework and Perl Exploit Library
 - Format String Attacks
- ◆ Netcat: The Attacker's Best Friend
 - Using Netcat to transfer files, create backdoors, and shovel shell
 - Netcat relays to obscure the source of an attack
 - Replay attacks using Netcat
- ◆ Hands-on Exercises with the Following Tools:
 - Sniffers, Including Tcpcat
 - Sniffer Detection Tools, Including ifconfig, ifstatus, and promiscdetect
 - Netcat for transferring files, creating backdoors, and setting up relays
 - Format String Vulnerabilities in Windows

CFIT2082 Computer & Network Hacker Security II 3cr



- ◆ Password Cracking
 - Password Cracking with John the Ripper
 - Analysis of Worm Trends From 1999-2005
 - Password Cracking With L0phtCrack and John the Ripper
- ◆ Web Application Attacks
 - Account Harvesting
 - SQL Injection: Manipulating Back-end Databases
 - Session Cloning: Grabbing Other Users' Web Sessions
 - Cross-Site Scripting
- ◆ Denial of Service Attacks
 - Distributed Denial of Service: Pulsing Zombies and Reflected Attacks
 - Local Denial of Service
 - SYN Floods and Smurf Attacks: DoS Building Blocks
- ◆ Hands-on Exercises with the Following Tools:
 - John the Ripper password cracker
 - Web application attack tools, including Achilles



CFIT2082 Computer & Network Hacker Security II 3cr

◆ Maintaining Access


- Backdoors: Using QAZ, Tini, and Other Popular Beasts
- Trojan Horse Backdoors: A Nasty Combo
- Application-level Trojan Horse Backdoor Suites (VNC, SubSeven, etc.)
- Rootkits: Substituting Binary Executables with Nasty Variations
- Kernel-level Rootkits: Attacking the Heart of the Operating System (Adore, the Super User Control Kit, and KIS)

◆ Covering the Tracks

- File and Directory Camouflage and Hiding
- Log File Editing on Windows and Unix
- Accounting Entry Editing: UTMP, WTMP, Shell Histories, etc.
- Covert Channels Over HTTP, ICMP, TCP and Other Protocols
- Sniffing Backdoors and How They Can Really Mess Up Your Investigations Unless You Are Aware of Them
- Steganography: Hiding Data in Images, Music, Binaries, or Any Other File Type

Uh Oh. You've
been
compromised!





Step 1: Collect the Evidence

Create an Investigative Log. Document EVERYTHING.

Make an image of the harddisks at that point in time.

Ghost/mirror entire drive, or
dd partition(s) to image(s)

```
dd if=/dev/hda1 of=/var/case01.dd
```

md5sum drive/image and document time, date and checksum (and possible digitally sign results)

```
date > case01.evidence.seal
```

```
md5sum case01.dd >> case01.evidence.seal
```

```
gpg --clearsign case01.evidence.seal
```

Sample Evidence Seal

cat case01.evidence.seal.asc

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Sun Dec 7 10:39:20 PST 2003

c20308685946b3d567f06d2c45e53904 case01.dd

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.2.1 (MingW32)

iD8DBQE/03Xj/VFbhJ3GXVMRAnf+AJ9hYhXkKUKT
jLZwJjj3bTRBzHyxgwCfSyyC
jLNK6kEXgfiwrBdo6x0G9Dc=
=gqEl

-----END PGP SIGNATURE-----



Step 2: Secure the Evidence

NEVER work on the original evidence. Work on the copy. Secure the original with checksum (or better yet an evidence seal) in a safe or evidence locker that only trusted people have access to.

To maintain evidence chain... you should document who has accessed the evidence, when they accessed it, and why... AT ALL TIMES. Physical security measures should ensure accountability. (ie CCTV to safe/locker) These procedures are not about paranoia, its about evidence integrity if needed in a criminal case





Step 3: Prep Analysis Machine

Boot into your favorite Linux OS with all the right tools, which we will list later)

Mount copy of evidence into filesystem
READ ONLY:

```
mount -o ro,loop,nodev,noexec case01.dd /mnt/evidence
```



Step 4: Create Timeline

Capture drive's forensic data

```
grave-robber -c /mnt/evidence -m \  
-d /var/investigations/case01 -o LINUX2
```

Extract deleted inode (mod/access/change) times

```
ils case01.dd | ils2mac > case01.ilsbody
```

Combine evidence for timeline conversion

```
cat case01.ilsbody body > case01.evidence
```

Generate Timeline

```
mactime -p /mnt/evidence/etc/passwd \  
-g /mnt/evidence/etc/group -b case01.evidence \  
11/28/2003 > case01.timeline
```



Step 5: Begin Analysis

At this point what happens is dependant on the investigation.

The timeline file will show modify, access, and changed actions at given times, and in sequence.

With patience, you should be able to trace exactly what went on



Tools to use during Analysis

istat – Display all known info about an inode

`istat case01.dd 12345`

dcat – Display chunks of a block of forensic data

`dcat -h case01.dd 65432`

icat – Access a block of forensic data by inode

`icat case01.dd 12345 > file`

unrm – Recover a block of forensic data

`unrm case01.dd startblock-endblock >`

`filedump`

hexdump – Dump data in hexadecimal

`hexdump -C file`

References / More Information

The Coroner's Toolkit

<http://www.porcupine.org/forensics/tct.html>

File System Analysis Techniques

http://www.sleuthkit.org/sleuthkit/docs/ref_fs.html

Autopsy

<http://www.sleuthkit.org/autopsy/download.php>

Good Forensic Analysis of HoneyNet Project Attack

<http://project.honeynet.org/challenge/results/dittrich/evidence.txt>

Good Practice Guide for Computer based Electronic Evidence

<http://www.nhtcu.org/ACPO%20Guide%20v3.0.pdf>

Knoppix-STD

<http://www.knoppix-std.org>





Kopp Technology Center Laboratory Initiative-\$10M

- ◆ 3-Advisory Committees
- ◆ December 12, 2004 Convergence Summit
- ◆ Presidents Technology Steering Committee
- ◆ Phased Implementation
- ◆ Orientation of Convergence-
 - Technology
 - Industry Support
 - Training Center
 - Partnerships



Current Challenges

- ◆ Textbook
- ◆ Faculty



Future Plans

- ◆ PDA/Mobil Forensics Course
- ◆ Partnerships with Business and Industry
- ◆ Internship Partnerships with Students



Q & A