

# Investigating Network Intrusions

Eoghan Casey

[eoghan.casey@yale.edu](mailto:eoghan.casey@yale.edu)

Yale University

# Outline

- Overview of Forensic Science
- Basic Computer Intrusions
  - Password theft
  - Intellectual Property (IP) theft
- Large Scale Network Intrusions
  - Correlating logs
  - Network compromise
  - Internet tracking

# Forensic Science Overview

- Science exercised on behalf of the law
- Locard's exchange principle
- Recognition
  - not as easy as it sounds
- Collection, documentation & preservation
  - authenticity and reliability
- Crime reconstruction (forensic analysis)
  - when, where, how, what, who, why

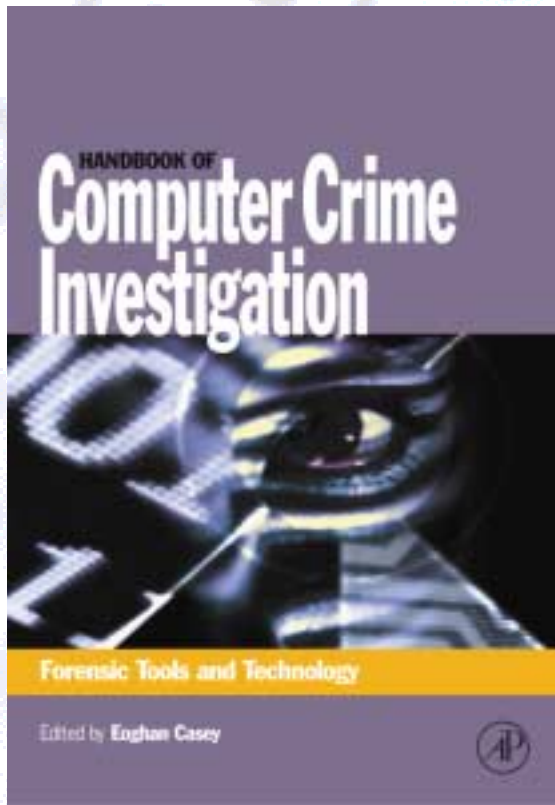
# Reconstruction & Analysis

- Low level analysis versus interpreted data
- Temporal reconstruction (timeline)
- Relational and functional reconstruction
- Risk assessment
- Motive and intent
- Corroborating data on network

# Interpreted data is necessary but confirm findings

```
MS-DOS DE
Auto
Disk editor (drive 1, sectors 0 - 2814335)
Window Edit View Search Help
0180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
01A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
01B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
01C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
01D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
01E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
01F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
Absolute sector 408 (cylinder 0, head 6, sector 31)
0000: 53 55 48 44 4C 4F 47 20 44 41 54 23 00 00 00 00 SUHDLOG DAT#....
0010: 00 00 00 00 00 00 30 73 4D 22 02 00 2E 14 00 00 .....0sM".....
0020: 42 4F 4F 54 4C 4F 47 20 50 52 56 22 00 00 00 00 BOOTLOG PRV"....
0030: 00 00 16 23 00 00 22 6A 16 23 03 00 D3 71 00 00 ...#.."j.#...q..
0040: 53 43 41 4E 44 49 53 4B 4C 4F 47 20 00 00 00 00 SCANDISKLOG ....
0050: 00 00 9A 29 00 00 F2 9B 9A 29 04 00 C1 01 00 00 ...).....).....
0060: 42 4F 4F 54 4C 4F 47 20 54 58 54 22 00 00 00 00 BOOTLOG TXT"....
0070: 00 00 16 23 00 00 44 6B 16 23 62 00 F0 73 00 00 ...#..Dk.#b..s..
0080: 43 4F 4D 4D 41 4E 44 20 43 4F 4D 20 00 00 00 00 COMMAND COM ....
0090: 00 00 8E 29 00 00 65 59 18 21 63 00 74 6E 01 00 ...)..eY.!c.tn..
00A0: 4D 53 44 4F 53 2D 2D 2D 53 59 53 27 00 4E E7 A1 MSDOS SYS'.M..
00B0: 9A 29 9A 29 00 00 E8 A1 9A 29 F6 1B 69 06 00 00 .).).....).i...
00C0: 41 55 54 4F 45 58 45 43 42 41 4B 00 00 29 D4 A6 AUTOEXECBAK...)
```

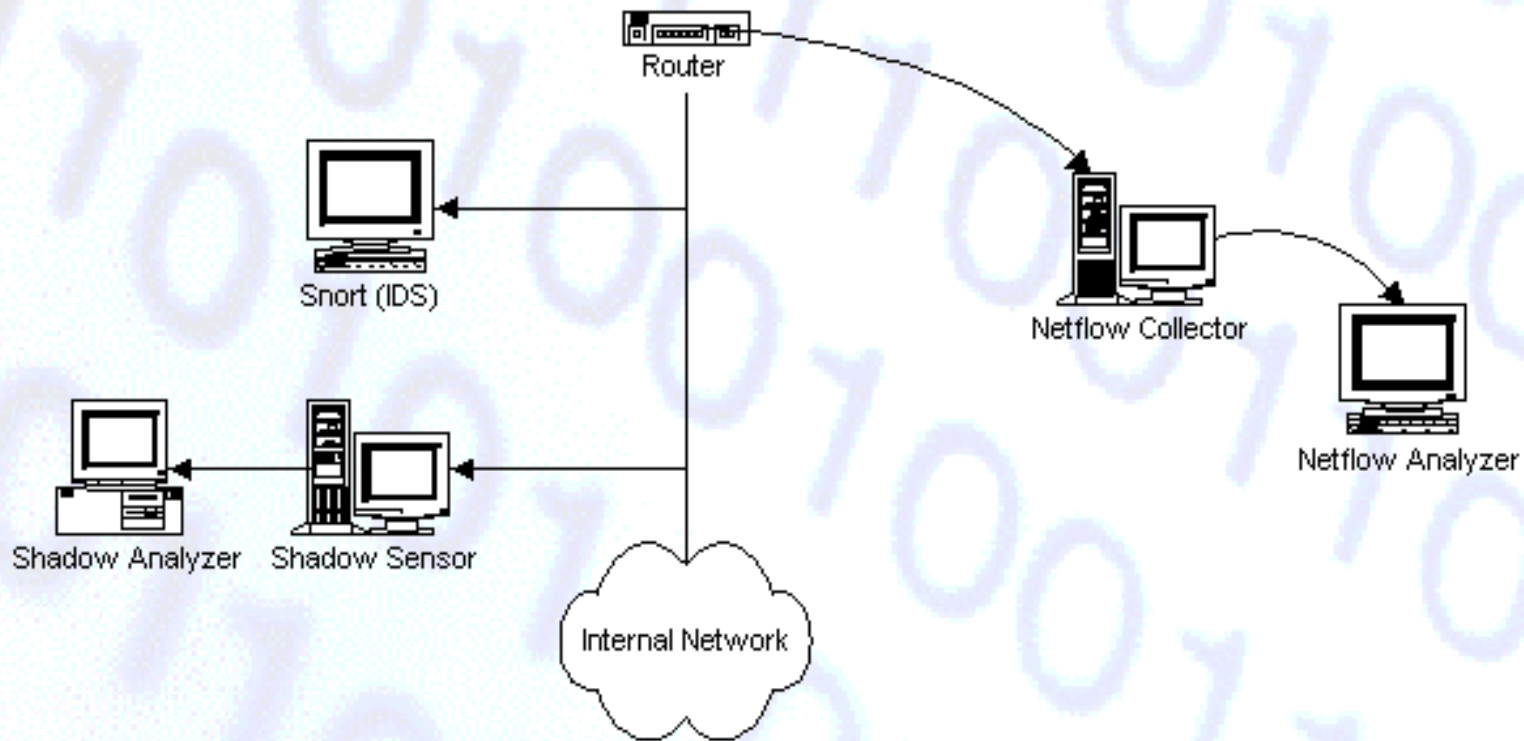
# Advanced Forensic Analysis



- Networked PCs
- Servers
- Network devices
- Network traffic
- Wireless systems
- Embedded systems

# Basic Computer Intrusions

- Confirm report & assess damage
- Collect/preserve most volatile evidence first
- Document everything
  - pay special attention to system clock offsets
- Analyze/reconstruct events
  - assess target risk
  - determine intruder motive, intent, and skill
  - locate collateral victims
  - perform research when necessary



# Network Overview

# Case #1: Password Theft

- Individual's password was repeatedly stolen
  - Every day he would change his password
  - Every day the intruder had the new password
  - Was our primary server compromised?
  - No, our server appeared to be intact
- Reconstruction of victim's activities
  - Victim only used his work system
  - Monitored traffic to and from this system
  - Nothing unusual

# Password Theft (part 2)

- Individual's password was still being stolen
  - Second interview: victim also used home PC
  - “But nobody else uses my home PC”
- Monitor traffic when victim dials in
  - Capture traffic for one dial-up account (not all)
  - tacacs-action and tcpdump
  - Carnivore with RADIUS trigger

# Password Theft (haha!)

- Network traffic showed connection from UK dial-up to home PC

09:24 userbf38.aol.uk.uudial.com.1391 > dialup03.its.yale.edu.1982

0000: 4500 002f 9fd9 4000 7406 a606 3e7d 0c2f E../..@.t...>}/

0010: 8284 f3b8 056f 07be 0340 c236 0003 ef1b .....o...@.6....

0020: 5018 2395 b25c 0000 5057 4468 6168 61 P.#..\..**PWDhaha**

09:24 dialup03.its.yale.edu.1982 > userbf38.aol.uk.uudial.com.1391

0000: 4500 006d d800 4000 7e06 63a1 8284 f3b8 E..m..@.~.c.....

0010: 3e7d 0c2f 07be 056f 0003 ef1b 0340 c23d >}/...o.....@.=

0020: 5018 2179 6089 0000 636f 6e6e 6563 7465 P.!y`...connecte

0030: 642e 2030 393a

d. 09:

# Password Theft (server side)

- Network traffic showed connection from UK to our main server

```
09:25 server.yale.edu.telnet > userbf38.aol.uk.uudial.com.2231
0000: 4510 0034 f6e2 4000 fe06 28a8 8284 8ff8 E..4..@...(.....
0010: 3e7d 0c2f 0017 08b7 3d2d f4d9 06bf f9fb >}/.....=-.....
0020: 5018 faf0 2744 0000 0d0a 5061 7373 776f P...'D....Passwo
0030: 7264 3a20                                rd:
```

- Corresponding login on server:

```
user pts/41 userbf38.aol.uk. Wed Jun 14 09:21 - 09:21 (00:00)
```

- Note: server was approximately 5 minutes behind sniffer

# Password Theft (lessons)

- Rely on evidence not interviews
- tcpdump
  - only captures first 68 bytes of packet by default
  - output is difficult to read (review)
- Use focused capture
  - limits risk of privacy invasion
  - reduces chance of packet loss
  - less irrelevant data to sort through
- Beware of temporal discrepancies

# Case #2: Intellectual Property

- IDS logs show intrusion

[\*\*] FTP-site-exec [\*\*]

09/14-12:27: 208.181.151.231 -> 130.132.x.y

09/14-12:28: 24.11.120.215 -> 130.132.x.y

09/14-12:33: 64.28.102.2 -> 130.132.x.y

- Concern: system contains sensitive data

# IP theft (confirm/assess damage)

- Initial examination of compromised host showed no signs of compromise
  - no wtmp entries from site exec exploit
  - no syslog entries
  - no unusual processes using ps or files using ls
- System clock was 5 hours fast ( $\Delta t = 5\text{hrs}$ )
- Oddities on system suggested compromise
  - difference between ps & lsof; /tmp/.tmp/

# IP theft (preservation & analysis)

- Used EnCase to preserve/analyze evidence
- Recovered deleted syslogs (noting  $\Delta t$ )

Sep 14 17:07:22 host ftpd[617]: FTP session closed

Sep 15 00:21:54 host ftpd[622]: ANONYMOUS FTP LOGIN FROM  
231.efinityonline.com [208.181.151.231],

```
1À1Û1É°FÍ 1À1ÛC
%_ÙA°?Í ëk^1À1É ^A^F^Df1ÿ^A°Í 1À ^A°=Í 1À1Û ^H%_C^B
1ÉpÉ1À ^H°^LÍ pÉuó1À^F^I ^H°=Í p^N°0pÈ^F^D1À^F^G%_v^H
%_F^L%_ó N^H V^L°^KÍ 1À1Û°^AÍ è ÿÿÿ0bin0sh1..11
```

Sep 14 17:22:54 host inetd[448]: pid 622: exit status 1

# EnCase (preservation & analyze)

The screenshot displays the EnCase (Professional Edition) interface for a case named [Case2.cas]. The main window is divided into several sections:

- Menu Bar:** File, Edit, View, Tools, Window, Help.
- Toolbar:** New, Open, Save, Add, Acquire, Preview, Case, Prev, Next, Search, Sigs.
- Navigation Tabs:** Case, All Files, Found, File, Gallery, Disk, Report, Script.
- File List:** A table listing files found in the case. The selected file is 'Volume Boot Sect'.
- Hex Editor:** A view showing the raw data of the selected file, with columns for Hex, Text, Report, Picture, and Bookmarks.

File Name	Bookmarks	Short Name	File Ext	Description
1 NCX99.EXE		NCX99.EXE	EXE	File, Archive
2 NCX.EXE		NCX.EXE	EXE	File, Archive
3 WEBSCAN.TXT		WEBSCAN.TXT	TXT	File, Archive
4 ZIGNZAG.HTM		ZIGNZAG.HTM	HTM	File, Archive
5 <input checked="" type="checkbox"/> Volume Boot Sect				File, Sector Range
6 <input checked="" type="checkbox"/> Primary FAT 1-9				File, Sector Range
7 <input checked="" type="checkbox"/> Secondary FAT 10				File, Sector Range
8 <input type="checkbox"/> Unallocated Cluste				Folder, Unallocated

Hex	Text	Report	Picture	Bookmarks
000 EB 3C 90 29 78 3E 32 6F 49 48 43 00 02 01 01 00 02 E0				e<□>x>2oIHC.....à
018 00 40 0B F0 09 00 12 00 02 00 00 00 00 00 00 00				.@.ð.....
036 00 00 29 89 C2 E5 5C 4E 4F 20 4E 41 4D 45 20 20 20				..):ÅÅ\NO NAME
054 46 41 54 31 32 20 20 20 33 C9 8E D1 BC F0 7B 8E D9 B8				FAT12 3ÉŽÑ*8(ŽÜ,
072 00 20 8E C0 FC BD 00 7C 38 4E 24 7D 24 8B C1 99 E8 3C				. ŽÄü*.18N\$)§<Áªè<
090 01 72 1C 83 EB 3A 66 A1 1C 7C 26 66 3B 07 26 8A 57 FC				.r.fë:f;. &f;.&šWü
108 75 06 80 CA 02 88 56 02 80 C3 10 73 EB 33 C9 8A 46 10				u.eĚ.ˆV.eĀ.së3ĚšF.
126 98 F7 66 16 03 46 1C 13 56 1E 03 46 0E 13 D1 8B 76 11				"~+f..F.V..F.Ň<v.
144 60 89 46 FC 89 56 FE B8 20 00 F7 E6 8B 5E 0B 03 C3 48				`%FüKvP. .+æ<ˆ..ĀH
162 F7 F3 01 46 FC 11 4E FE 61 BF 00 00 E8 E6 00 72 39 26				+ó.Fü.Npaç...èæ.r9&
180 38 2D 74 17 60 B1 0B BE A1 7D F3 A6 61 74 32 4E 74 09				8-t.ˆ±.Ź;)}ó!;at2Nt.
198 83 C7 20 3B FB 72 E6 EB DC A0 FB 7D B4 7D 8B F0 AC 98				fç ;ûraëÜ ú)'<ð~"
216 40 74 0C 48 74 13 B4 0E BB 07 00 CD 10 EB EF A0 FD 7D				@t.Ht.ˆ.»...Í.ëi ý)

Volume A\Volume Boot Sectors 0-0 Sel 0 PS 0 LS 0 SO 0 FO 0 LE1

# IP theft (crime reconstruction)

- Confirmed source of initial intrusion
- Determined that target was high risk
- Determined motive and intent
  - not aware of sensitive information on host
  - used host for DoS, scanning, and IRC
- Determined that a sniffer had been used
- Located other compromised systems
  - notified system owners on outside networks

# Intrusion (research - t0rnkit)

- Intruder used a rootkit called t0rn
  - replaces system binaries to conceal presence
  - creates backdoors to allow future access
  - patches the FTP site exec vulnerability
  - replaces SSH daemon (/usr/info/.t0rn)
- /usr/src/.puta/t0rnsniff
- See CERT Incident Note 2000-10

# Intrusion (lessons)

- IDS is necessary but not sufficient
- Rootkits are becoming more sophisticated
- Cannot trust a compromised system
- EnCase is necessary but not sufficient
- Need to restore system to fully analyze it
- Research can lead to useful resources
- Understand the intruders (skill, motive, etc.)
- Beware of temporal discrepancies

# Large Scale Network Compromise

- Recognition
  - many potential sources of digital evidence
- Collection, preservation & documentation
  - varies widely depending on circumstances
  - remote collection
  - observe intruder(s)
- Analysis & reconstruction
  - correlating multiple independent sources

# Finding Evidence on Networks

- Internet
  - Web, newsgroups, chat
- Log files
  - server (e.g. e-mail, Web, dial-up server)
  - correlate with logs on clients
- User information (e.g. finger, nbtstat, who)
- State tables (e.g. netstat, arp, show conn)
  - network devices are a challenge
- Network traffic (e.g. NetFlow & tcpdump)

# Collect, Preserve, Document

- Proactive evidence gathering
  - NFR, Shadow, Dragon, NetFlow
- Remote/dynamic collection
  - print screens, video, log keystrokes
- Document evidence
  - MD5, digital signatures, encryption
- Are the system times & logs reliable?
  - know and test systems
  - [www.counterpane.com](http://www.counterpane.com)

# Tracking Offenders

- Locate source
  - logs, state tables, finger, nbtstat, etc.
- Contact source ISP (e.g. logs, ANI)
- Search Internet for rough edges
- Observe offender on Internet (e.g. IRC)

# The Coroner's Toolkit

- Lazarus
  - Bitstream copy like dd
  - Attempts to categorize data
- Grave Robber
  - MACtime database
  - Gather host info, processes, and select files
  - Calculate MD5 of important system files
  - Save open files using icat

# Case #3: Correlating Logs

- Logs show only one suspicious connection at 22:50 from 62-30-247-138-do.blueyonder.co.uk

/var/log/secure:

Apr 24 **22:50:34** target in.ftpd[2103]: connect from 62.30.247.138

/var/log/messages:

Apr 24 22:48:15 target inetd[25739]: login/tcp: bind: Address already in use

Apr 25 **02:50:40** target ftpd[2103]: ANONYMOUS FTP LOGIN FROM pc-62-30-247-138-do.blueyonder.co.uk [62.30.247.138], guest@here.com

Apr 25 **02:50:40** target ftpd[2103]: FTP session closed

Apr 24 22:58:15 target inetd[25739]: login/tcp: bind: Address already in use

/var/log/wtmp:

ftp ftp pc-62-30-247-138-do.blueyonder.co.uk [62.30.247.138] Tue Apr 24  
**22:50 - 22:50** (00:00)

# Correlating Logs (IDS)

- IDS logs do not show intrusion at 22:50
- IDS logs show intrusion from Italy (62-122-10-221.flat.galactica.it) hours later

[\*\*] FTP-site-exec [\*\*]

04/25-02:48:45.012306 **62.122.10.221**:4158 -> 192.168.1.34:21

TCP TTL:46 TOS:0x0 ID:20194 IpLen:20 DgmLen:468 DF

\*\*\*AP\*\*\* Seq: 0x11A6920B Ack: 0xD567116C Win: 0x3EBC

TCP Options (3) => NOP NOP TS: 98258650 1405239787

# Correlating Logs (NetFlow)

- FTP scans from UK and Taiwan
- Intrusion on April 25 at 02:47:12 (Italy)
- NetFlow shows two connections from target
  - Downloaded RPM to fix vulnerability
  - Connected to [www.xoom.it](http://www.xoom.it)

```
srcaddr|dstaddr|src_as|dst_as|input|output|srcport|dstport|protocol|pkts|octets|flows  
192.168.1.34|18.29.1.70|0|0|4|17|2382|20|TCP-FTP|61|3180|1  
192.168.1.34|18.29.1.70|0|0|4|17|2381|21|TCP-FTP|14|855|1  
192.168.1.34|206.132.163.187|0|0|4|17|2383|80|TCP-WWW|94|1204|1
```

# Case #4: Network Compromise

- External complaint about compromised host
- Internal report of another compromised host
- CERT team members examined machines
  - confirmed reports & assessed damage
  - determined source and method of attack
- CMSD vulnerability exploited
- Stolen dial-up account used to launch attack
- Backdoors and sniffers installed on all hosts

# Network Compromise (cont.)

- Located other compromised systems
  - scanned network for known backdoors
  - received additional reports from sys admins
- Collected evidence remotely (40+ systems)
- Documented collection process and results
  - script to monitor keystrokes
  - digitally signed each evidence file
- Performed basic analysis and reconstruction

# Network Compromise (live)

- Observed intruder returning to crime scenes
- Recorded unauthorized access (sniffer log)
- Telneted to one machine with intruder
  - gathered corroborating evidence (telnet log)
  - shutdown and seized the machine
- Documented collection process and results
- Called source ISP to gather evidence (ANI)

# Network Compromise (analysis)

- Analyzed evidence in more detail
  - remembered similar M.O. to past intrusion
  - compared cases and found many similarities
- Performed basic reconstruction of events
- Compiled reports for law enforcement
- Monitored IRC for intruder
- Seized suspect's computer

# Network Compromise (lessons)

- Be swift, thorough, and lucky
- Multiple independent sources of evidence
- Dial-up account used versus ANI
- Reports for law enforcement and attorneys
  - misread IP address
  - incident summary
  - reconstruction summary
  - full documentation and evidence inventory
  - provide search tips for forensic examiners (hash files)

# Case #4: Internet Tracking

- Compromised Windows 98 machines
  - Back Orifice and IRC bot
  - Intruders left voluminous chat logs
  - Subsequent credit card fraud
- Monitoring IRC led to group of intruders
- Focused on primary intruder
  - Many personal details in logs, including name
  - Net search & finger linked her with intrusions

# Internet Tracking (particulars)

- `finger username@primenet.com host`
  - leads to dial-up connection

```
% finger username@usr07.primenet.com (206.165.6.207) ...
```

```
Login: username Name: First Last
```

```
Directory: /user/u/username Shell: /bin/bash
```

```
Mailbox last read: Tue Oct 24 12:31:24 2000
```

```
Currently logged in via 208-50-51 49.nas2.fhu.primenet.com
```

```
% finger @208-50-51-49.nas2.fhu.primenet.com (208.50.51.49) ...
```

if your name is xxxxxx xxxxxxxx, you're a *explicatives removed*.

also: [www.domainname.net](http://www.domainname.net)

# Internet Tracking (particulars)

- Web site registered to intruder
  - Whois gives home address and phone number
- IRC chat encounter reveals personal info
  - use online undercover identity
- Collect evidence while you can
  - chat logs, finger results, and even Web sites
- Temporal discrepancies
  - Sam spade time stamp earlier than finger results

# Digital Evidence Challenges

- Getting the evidence
  - distribution of crime scenes
  - volume of data (needle in haystack)
  - investigators require technical expertise
  - legal barriers (jurisdiction, admissibility)
  - evidence dynamics
- Connecting computer activity to individual
- Preserving probity of digital evidence
  - case database
  - evidence locker

# Best Practices

- Be prepared with procedures and tools
  - proactive evidence gathering
  - do not rely entirely on one tool
  - document everything & maintain chain
  - always perform a full analysis (do not skip steps)
  - seek multiple independent sources of evidence
  - rely on evidence when making conclusions
- Computer clocks are critically important
- Forensic analysis includes human behavior
  - build understanding of intruders (motives, skill)
  - know your audience when writing reports