Forensic Network Analysis Tools: Strengths, Weaknesses, and Future Needs

By

Eoghan Casey

Presented At

The Digital Forensic Research Conference

DFRWS 2003 USA Cleveland, OH (Aug 6th - 8th)

Forensic Network Analysis Tools

Strengths, Weaknesses, and Future Needs

Eoghan Casey

- Author, *Digital Evidence and Computer Crime*
- Editor, *Handbook of Computer Crime Investigation*
- Technical Director, *Knowledge Solutions*
- *eco@corpus-delicti.com*

The Basics

- Hardware and configuration
- Read-only
- Security
- Integrity
  - Existing tools do not calculate MD5
  - ⇒ Do it yourself after collection
- Documenting losses
  - Existing tools to not log all losses
- Document system status & performance
- Logging examiner actions
  - Not currently => rely examiner's notes

Hardware

- CatOS Switched Port Analyzer (SPAN)
  - Only copies valid Ethernet packets
  - Not all error information duplicated
  - Low priority of SPAN may increase losses
- Physical tap
  - Copy signals without removing layers
  - May split Tx and Rx (reassembly required)
- Platform
  - Testing but no published data
  - < 200 Mb/sec => Linux
  - > 200 Mb/sec => FreeBSD
  - Kernel customization

HW (Vendor v Homemade)

- Commercial
  - More costly but uniform expertise
  - Vendor can testify about HW & OS config
  - Vendor responsible for problems
- Homemade
  - Less expensive but variable expertise
  - You can testify about HW & OS config
  - You are responsible for problems

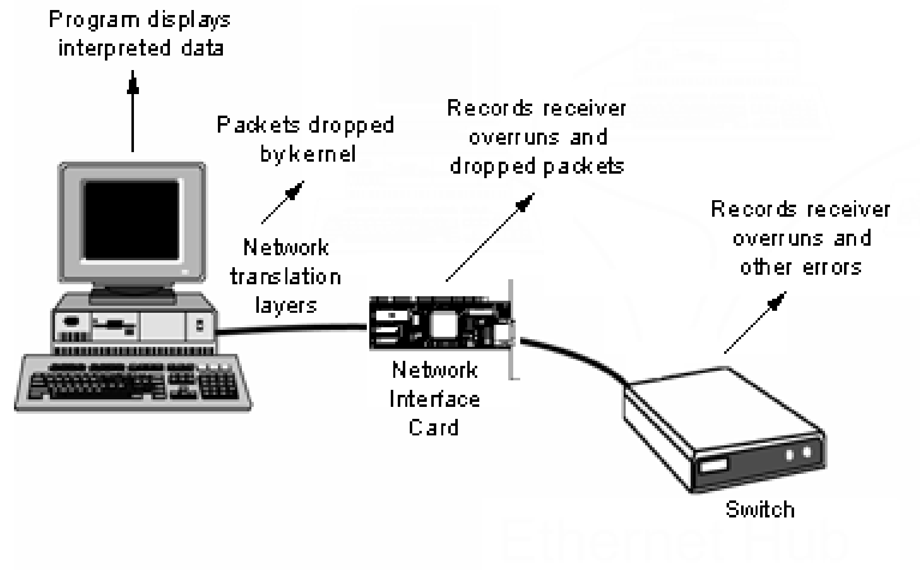
Read Only

- No network response
  - Including ARP replies
- No network queries
  - Use internal DNS resolution
- No downloads from Internet
  - Don’t insert content from the Web when reconstructing Web pages

Security

- Secure OS configuration
  - Patches
  - Do not overuse root/Administrator account
- Secure remote access
  - SSH
  - SSL
- Secure programming
  - Prevent buffer overflows
  - Prevent crashes (and resulting data loss)

Data Loss



NIC:

% /sbin/ifconfig
eth0 Link encap:Ethernet HWaddr 00:B0:D0:F3:CB:B5
inet addr:128.36.232.10 Bcast:128.36.232.255
Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:19877480 errors:0 dropped:0 **overruns:128** frame:0
TX packets:7327676 errors:0 dropped:0 overruns:0 carrier:1
collisions:442837 txqueuelen:100
Interrupt:23 Base address:0xec80

Kernel:

tcpdump -X host 192.168.12.5
tcpdump: listening on xl0
.....[data displayed on screen]…
^C
29451 packets received by filter
4227 packets dropped by kernel

- Losses at the switch
  - show inter
- Bug or misrepresentation in application

Figure from Eoghan Casey's "Error, Uncertainty, and Loss" article in International Journal of Digital Evidence (Vol. 1, Iss. 2)

Overview of Tools

- Tcpdump (www.tcpdump.org)
  - de facto standard file format (.dmp)
- Ethereal (www.ethereal.com)
- Review (www.net.ohio-state.edu/software/)
- IRIS (www.eye.com)
- InfiniStream (www.networkassociates.com)
- NetIntercept (www.sandstorm.net)
- NetDetector (www.niksun.com)
- NFR Security (www.nfrsecurity.com)
- NetWitness (www.forensicexplorers.com)
- SilentRunner (www.silentrunner.com)
- DCS1000 w/ CoolMiner/Packeteer (FBI)

Overview of Tool Features

- Tcpdump (multiple platforms, free)
  - Limited examination capabilities
- Ethereal (multiple platforms, free)
  - Basic examination capabilities
- IRIS (Windows, $)
  - Basic examination capabilities
- NetWitness (Windows, IIS, MSSQL, $)
  - Basic examination capabilities
  - Security concerns relating to ISS and MSSQL
- InfiniStream (Linux collector, Win console, $)
  - Tcpdump import but not export (.cap export)
  - Good examination capabilities (Sniffer-based)

Overview of Tool Features

- Review (Unix, free)
  - Good examination capabilities
- NetIntercept (FreeBSD, $)
  - Designed with evidentiary issues in mind
  - Excellent examination capabilities
    - Feature rich but still user-friendly
    - Decrypt SSH and SSL if key are available
  - Basic analysis capabilities
- NetDetector (FreeBSD, $)
  - Excellent examination capabilities
  - Graphic analysis features (Xpert)
  - Integrated IDS capabilities (Snort)

Overview of Tool Features

- NFR Security ($)
  - Custom analysis using N-code
  - OpenBSD collector, Windows admin console, Solaris/Linux mgmt server & Oracle database
- SilentRunner (Windows, $)
  - Powerful visual & analysis capabilities
- DCS1000 (Windows, available to LE)
  - Unique filtering with law enforcement in mind (e.g., RADIUS, e-mail pen register)
  - Not clear how robust (complexity of RADIUS and capturing content in e-mail header)

Examples

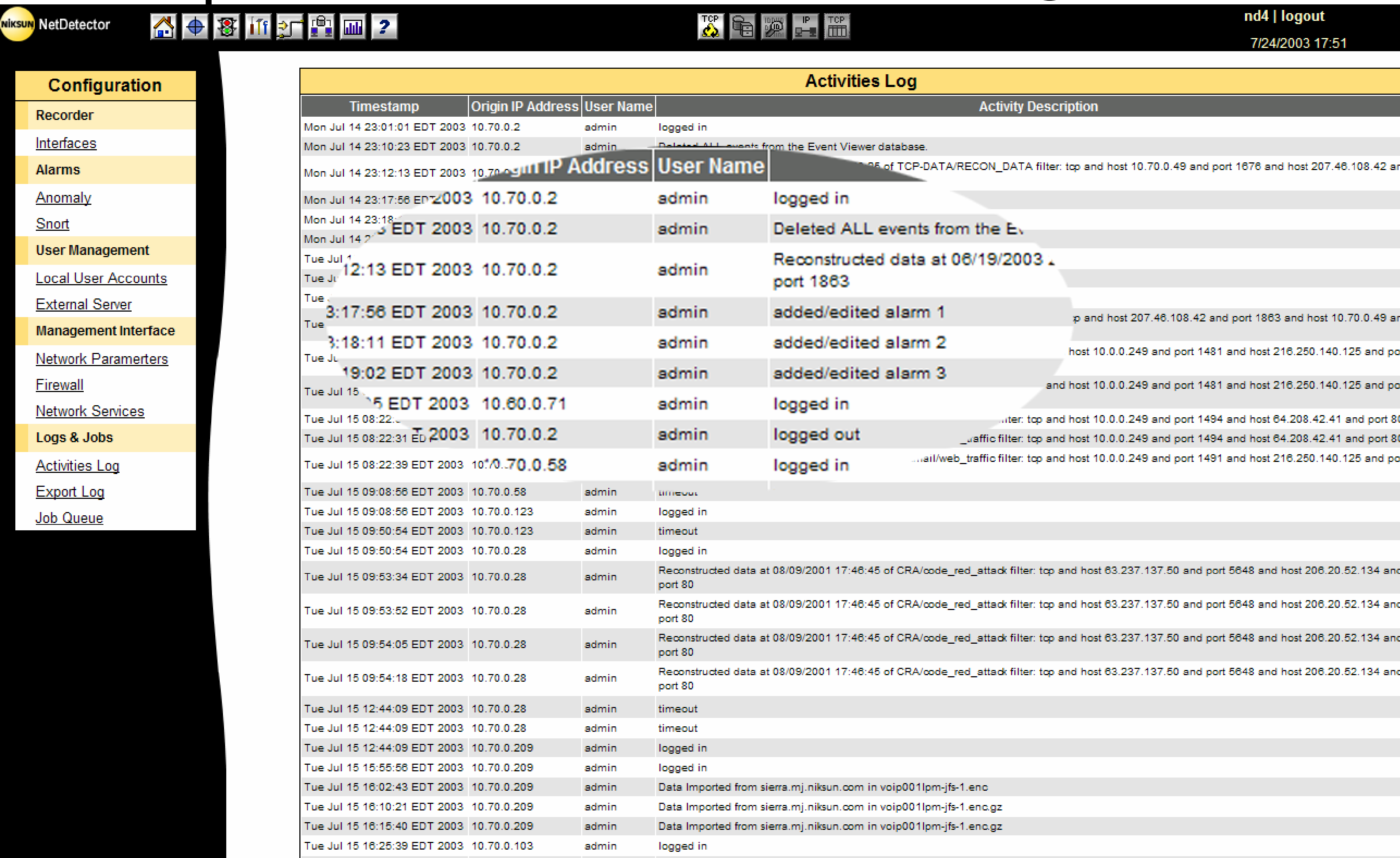
Key points

- Collection: capture all content versus filtering
- Documentation: poor across the board
- Examination: recover, classify, decode, reduce, search
- Analysis: individualize, evaluate source, advanced recovery, reconstruct, visualize, present

Collection

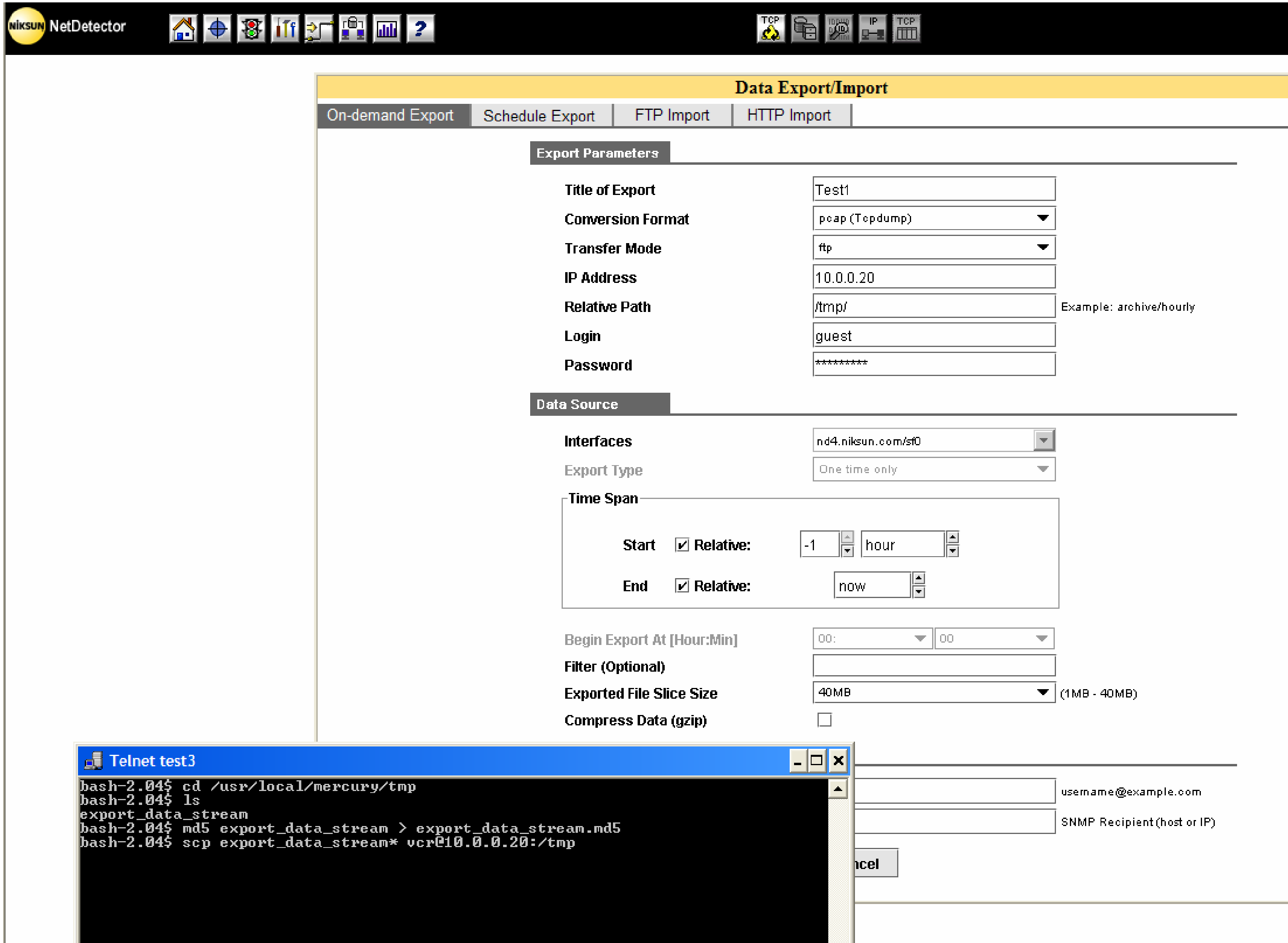
- Tcpdump
  - 68 byte default
- Ethereal
  - 65535 bytes default snap length
- Others
  - 68 < snap length < 65535 bytes

NetDetector: Audit Log



Timestamp	Origin IP Address	User Name	Activity Description
Mon Jul 14 23:01:01 EDT 2003	10.70.0.2	admin	logged in
Mon Jul 14 23:10:23 EDT 2003	10.70.0.2	admin	Deleted ALL events from the Event Viewer database.
Tue Jul 15 09:08:56 EDT 2003	10.70.0.58	admin	timeout
Tue Jul 15 09:08:56 EDT 2003	10.70.0.123	admin	logged in
Tue Jul 15 09:50:54 EDT 2003	10.70.0.123	admin	timeout
Tue Jul 15 09:50:54 EDT 2003	10.70.0.28	admin	logged in
Tue Jul 15 09:53:34 EDT 2003	10.70.0.28	admin	Reconstructed data at 08/09/2001 17:46:45 of CRA/code_red_attack filter: tcp and host 63.237.137.50 and port 5648 and host 206.20.52.134 and port 80
Tue Jul 15 09:53:52 EDT 2003	10.70.0.28	admin	Reconstructed data at 08/09/2001 17:46:45 of CRA/code_red_attack filter: tcp and host 63.237.137.50 and port 5648 and host 206.20.52.134 and port 80
Tue Jul 15 09:54:05 EDT 2003	10.70.0.28	admin	Reconstructed data at 08/09/2001 17:46:45 of CRA/code_red_attack filter: tcp and host 63.237.137.50 and port 5648 and host 206.20.52.134 and port 80
Tue Jul 15 09:54:18 EDT 2003	10.70.0.28	admin	Reconstructed data at 08/09/2001 17:46:45 of CRA/code_red_attack filter: tcp and host 63.237.137.50 and port 5648 and host 206.20.52.134 and port 80
Tue Jul 15 12:44:09 EDT 2003	10.70.0.28	admin	timeout
Tue Jul 15 12:44:09 EDT 2003	10.70.0.28	admin	timeout
Tue Jul 15 12:44:09 EDT 2003	10.70.0.209	admin	logged in
Tue Jul 15 15:55:56 EDT 2003	10.70.0.209	admin	logged in
Tue Jul 15 16:02:43 EDT 2003	10.70.0.209	admin	Data Imported from sierra.mj.niksun.com in voip001lpm-jfs-1.enc
Tue Jul 15 16:10:21 EDT 2003	10.70.0.209	admin	Data Imported from sierra.mj.niksun.com in voip001lpm-jfs-1.enc.gz
Tue Jul 15 16:15:40 EDT 2003	10.70.0.209	admin	Data Imported from sierra.mj.niksun.com in voip001lpm-jfs-1.enc.gz
Tue Jul 15 16:25:39 EDT 2003	10.70.0.103	admin	logged in

External MD5 Calculations



Filtering During Collection

- BPF/Ethereal filtering syntax
  - IP address, port, etc.
- MAC address
- Custom NFR Security filters (using N-code)
- DCS1000
  - RADIUS
  - DHCP
- Filtering on protocol is risky
  - Pen register for e-mail (DCS1000)
  - If necessary, be very careful
  - Ideally use a specialized tool for this purpose

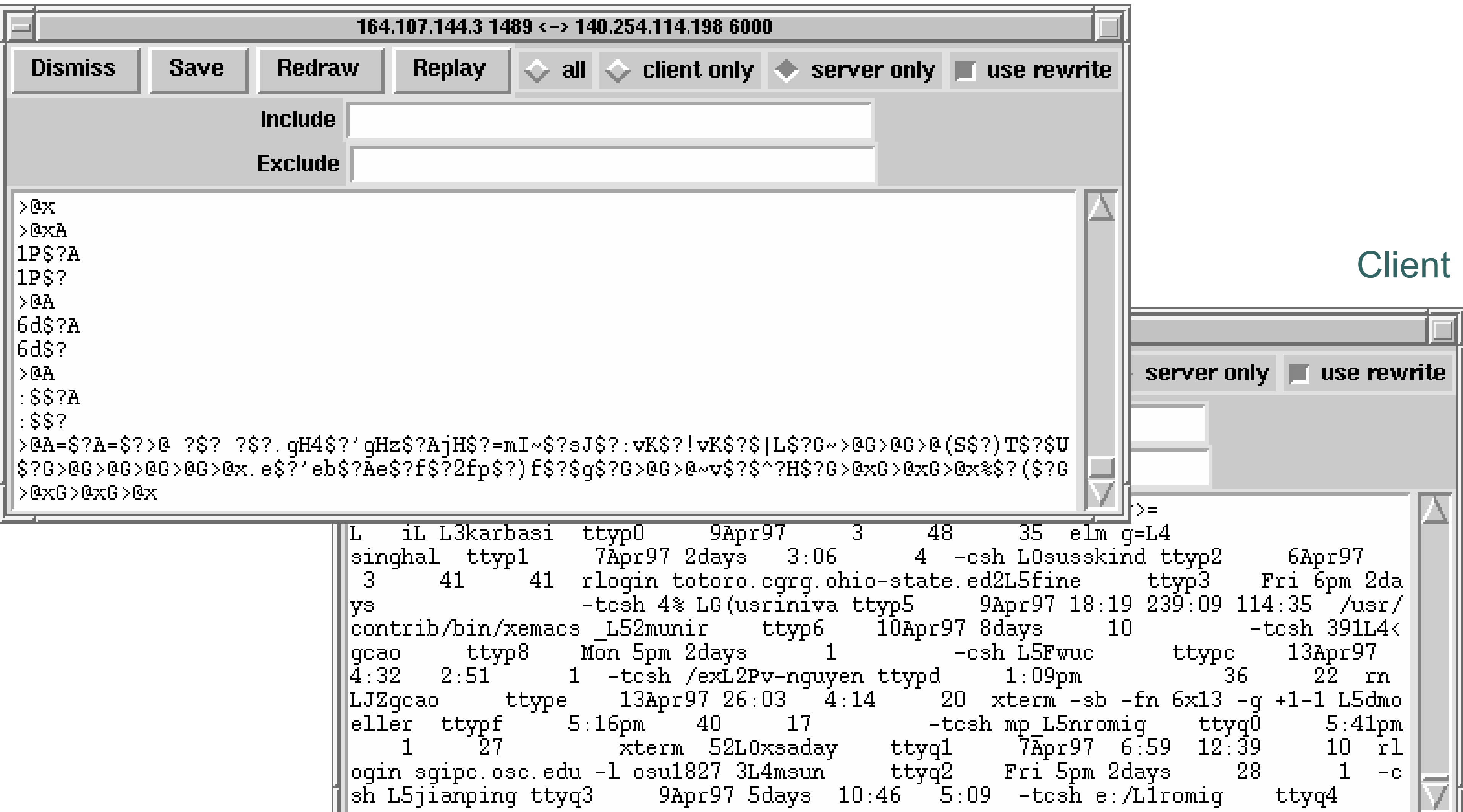
Examination: Protocol Decode

- Tcpdump has limited decode capabilities
- Ethereal
  - More decodes but assumes default behavior
  - “Decode As” feature
- InfiniStream/Sniffer
  - Several decodes including some VoIP
- NetDetector
  - Understands protocols including some VoIP
- NetIntercept
  - Understands protocols including some VoIP
  - More powerful stream reconstruction
  - Flags anomalies (like file sig mismatch)
  - Flags missing SEQ #’s in TCP session

Review: X Session Decode

Server

Client



Review: X Session Replay

- Step-by-step session replay
- Pauses before redrawing screen

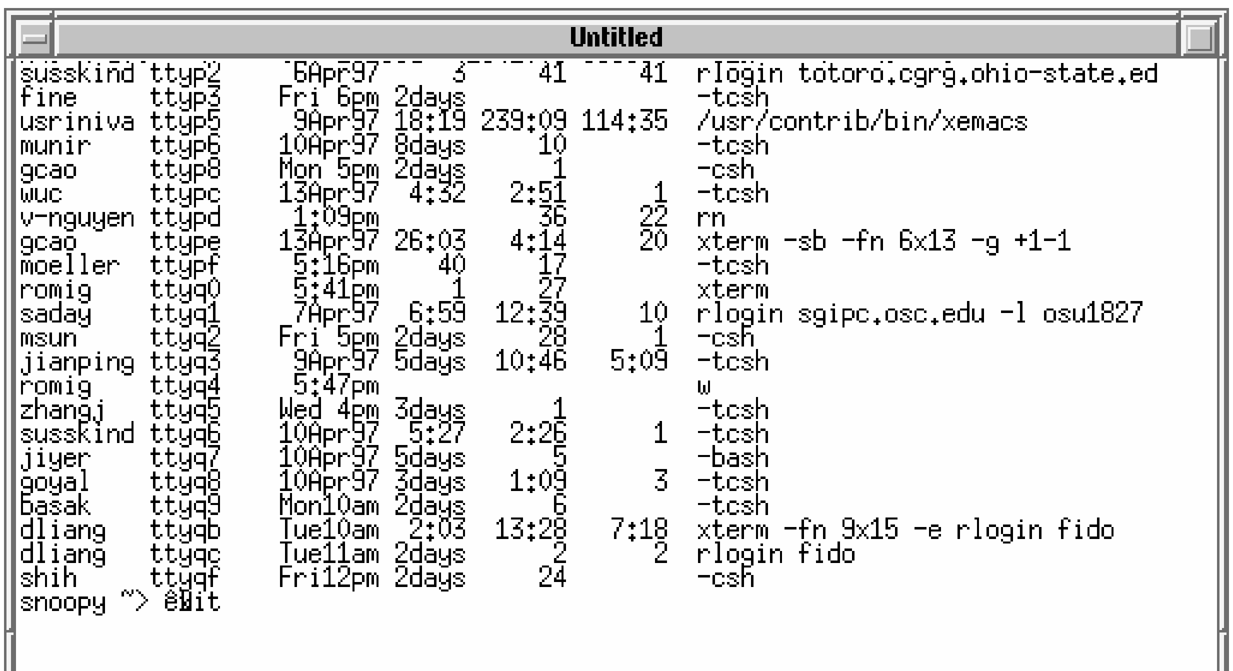
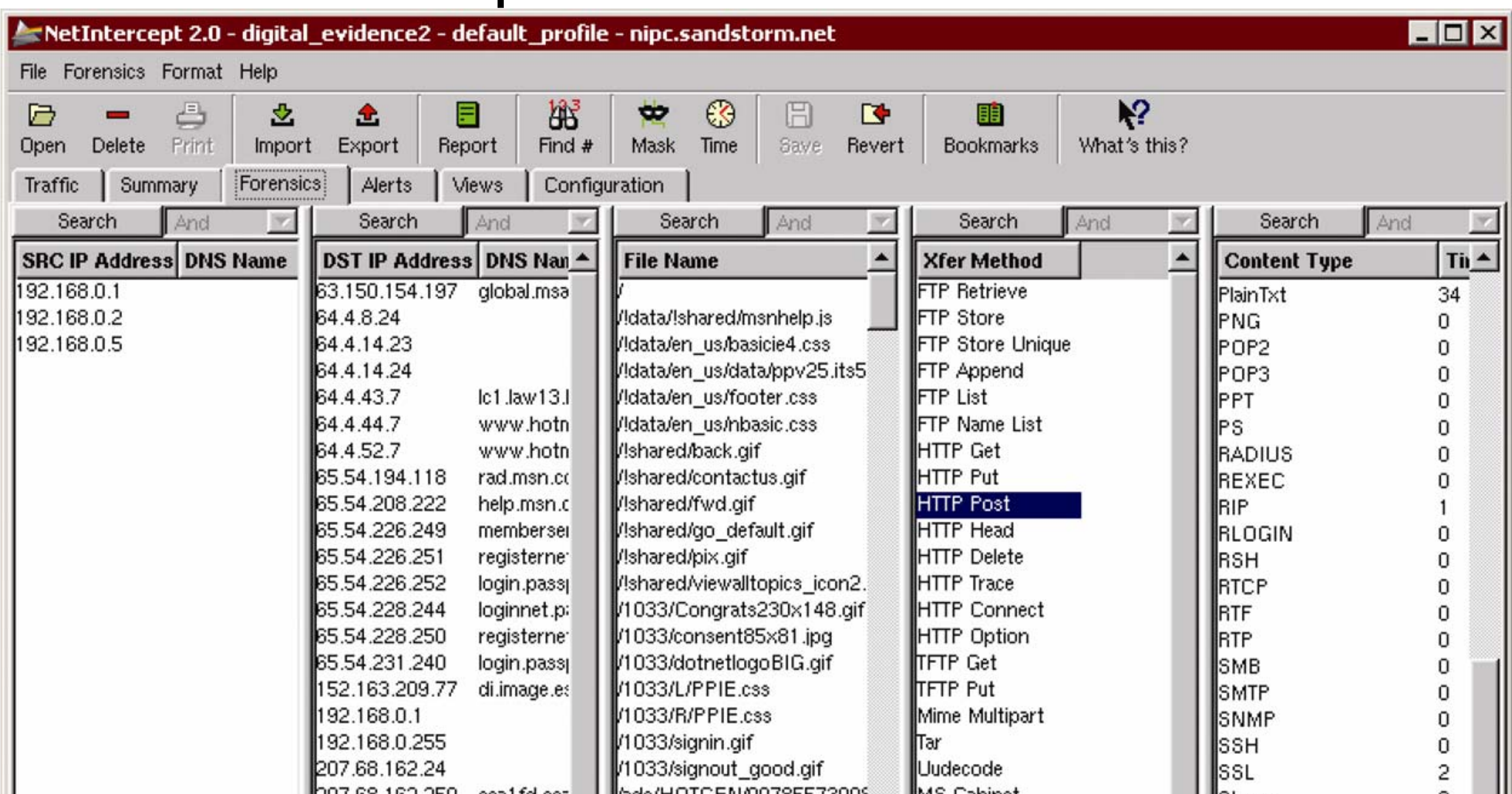


Figure from Steve Romig's "Incident Response Tools" chapter in Handbook of Computer Crime Investigation

Figure from Eoghan Casey's "Digital Evidence and Computer Crime", 2nd edition

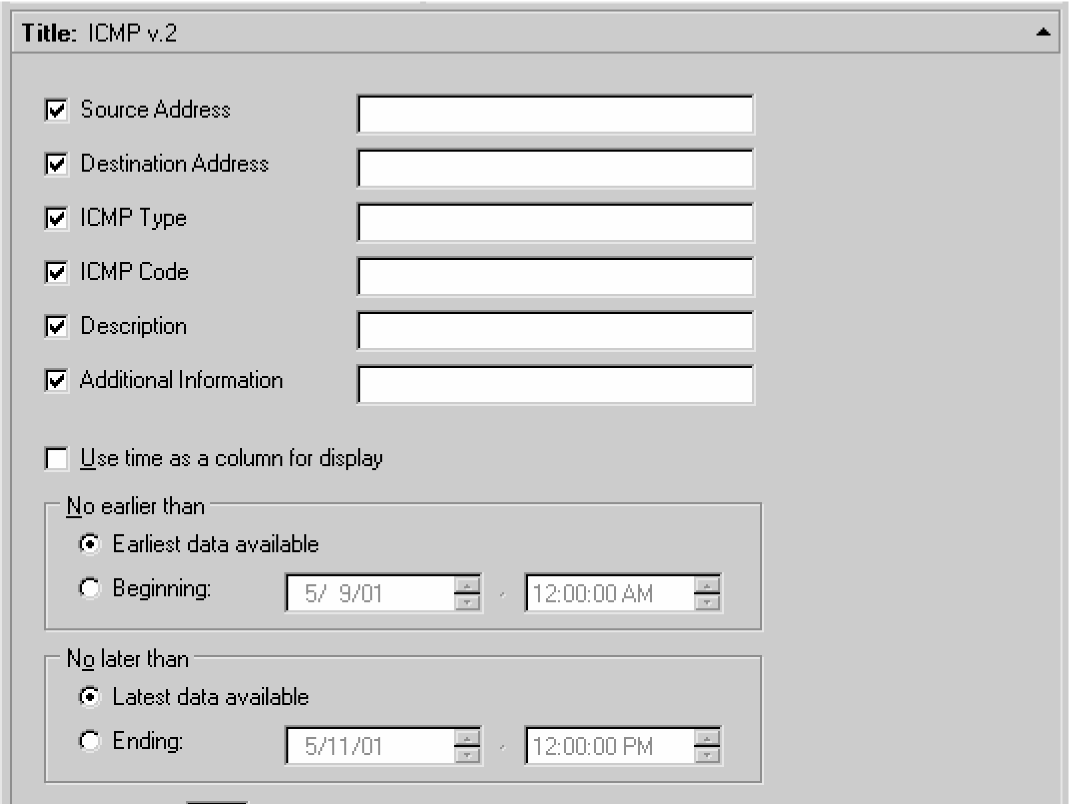
Examination: Data Reduction

- GUI versus command syntax
  - Review: session summary & browsing
  - NetIntercept: Forensics tab



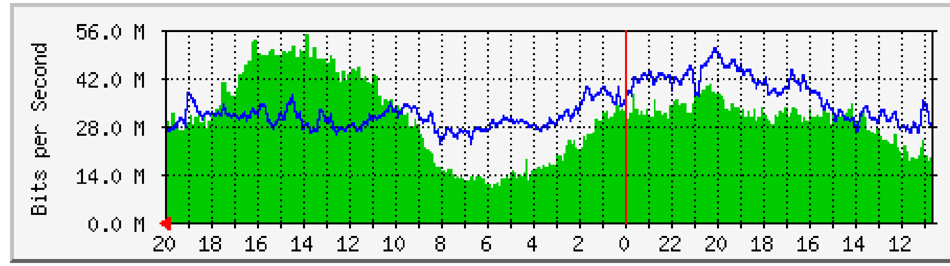
Examination: Data Reduction

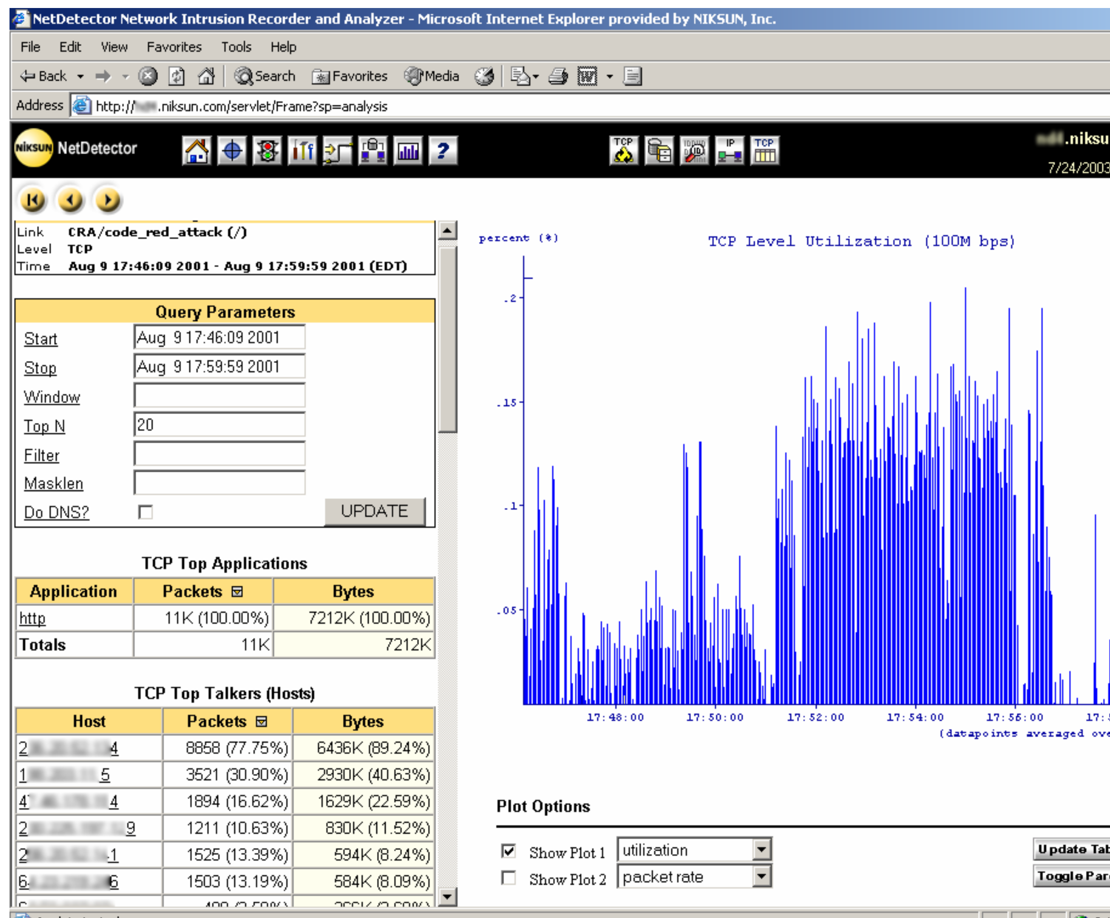
- SilentRunner: 3-D Visualization
- NFR Security: Query interface



Examination: Visualization

- Traffic charts
- Top Talkers
- Top Pairs





Examination: Visualization

- SilentRunner
  - 3-D display of traffic helps focus on interesting activities
- General purpose visualization tools
  - Clustering and other techniques for visually representing data to help examiners identify useful items in large datasets

Search and Recovery

- Ethereal
  - Miss keyword split between two packets
  - Export Web page & view in browser (bad)
  - File extraction requires expertise & tools
- NetIntercept
  - Performs search on reconstructed data
  - Sandbox for viewing Web pages
  - Does not execute code in Web pages
  - Automated file extraction
- NetDetector
  - GUI & regular expression on command line
  - Sandbox for viewing Web pages
- NFR Security database query customization
- SilentRunner N-gram Analysis

Figure from Eoghan Casey's "Digital Evidence and Computer Crime", 2nd edition

Ethereal: Search

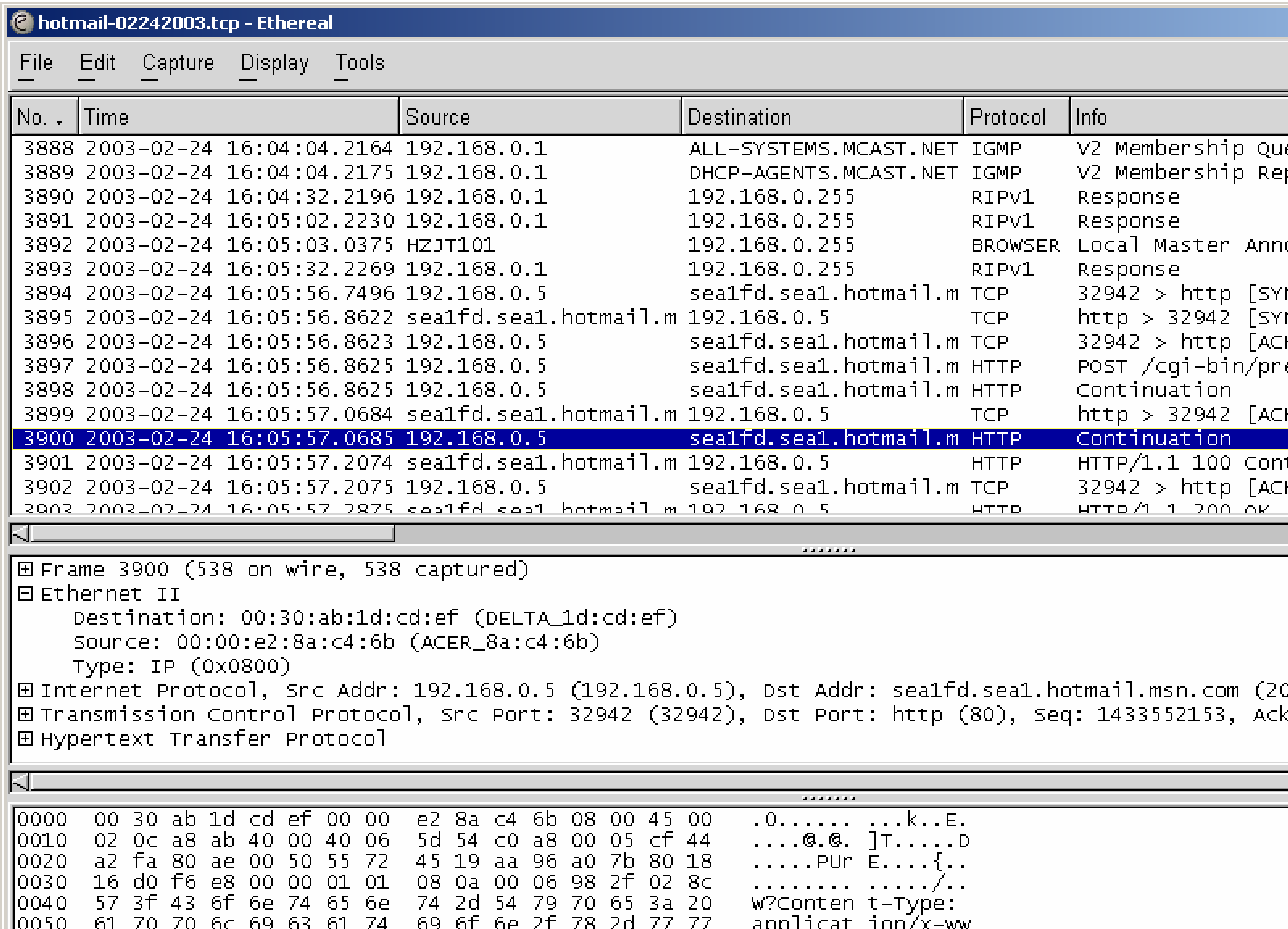
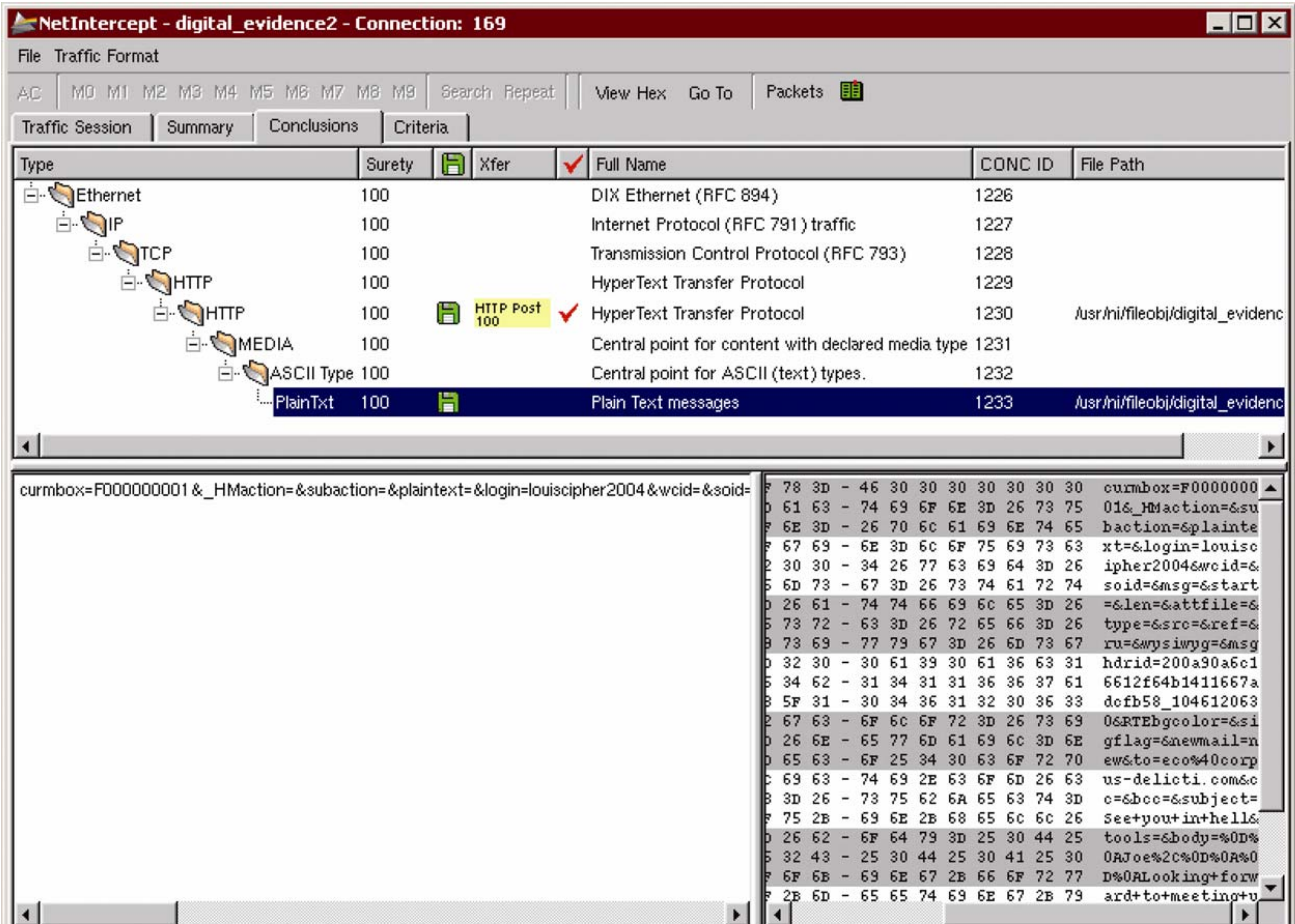
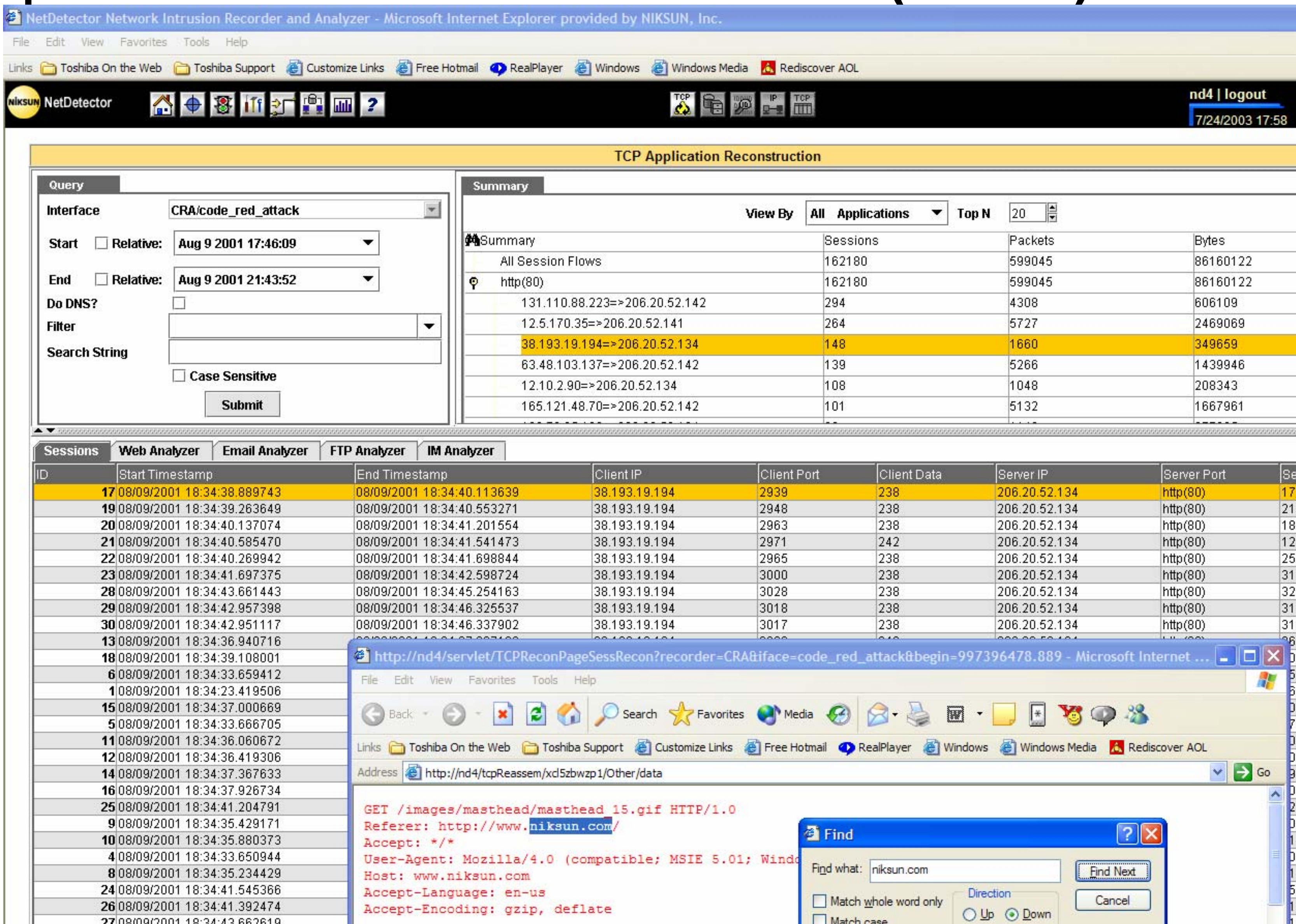


Figure from Eoghan Casey's "Digital Evidence and Computer Crime", 2nd edition

NetIntercept: Search



NetDetector: Search (GUI)



NetIntercept: Image Extraction

Ethereal: Web Page

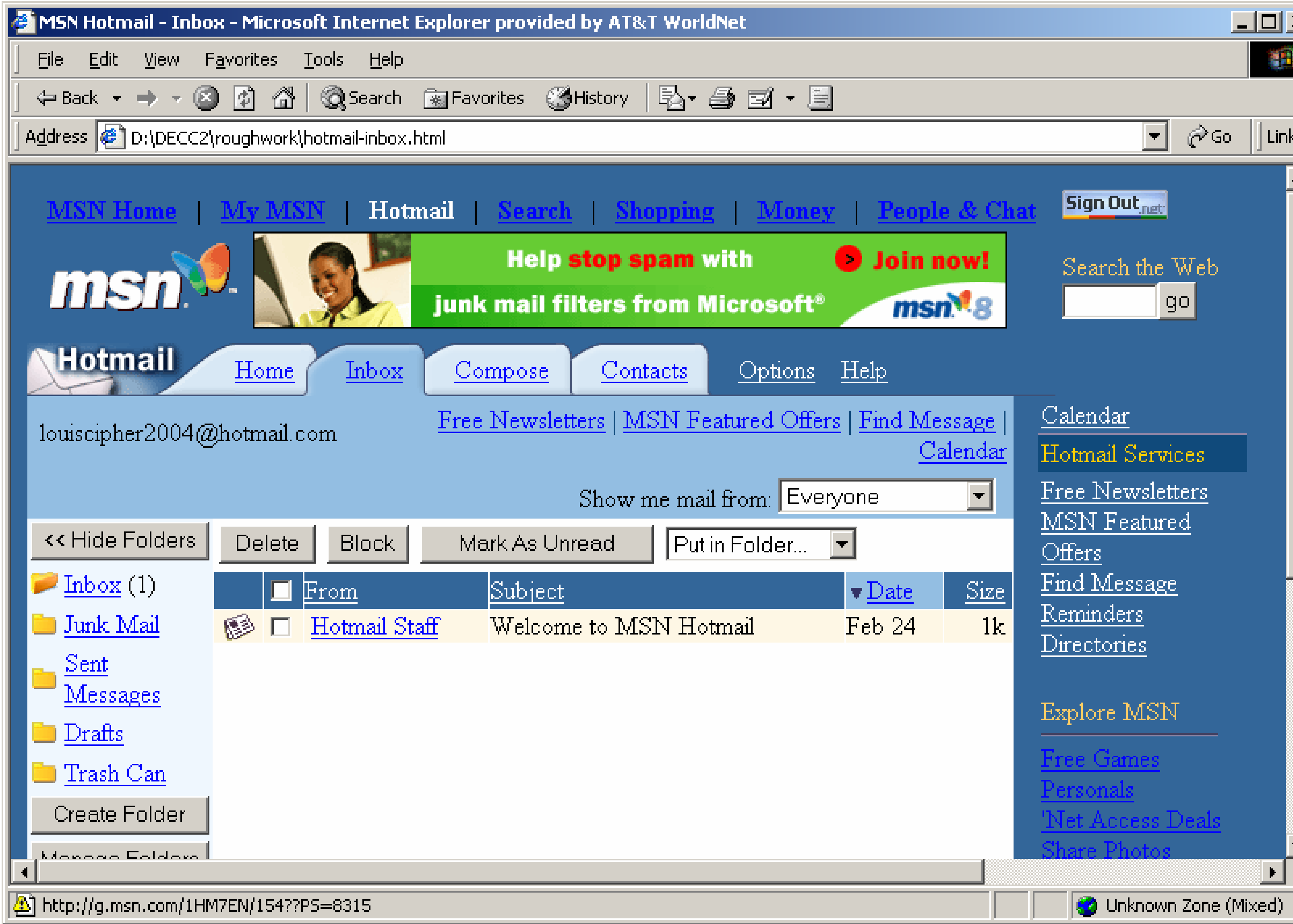


Figure from Eoghan Casey's "Digital Evidence and Computer Crime", 2nd edition

NetIntercept: Web Page

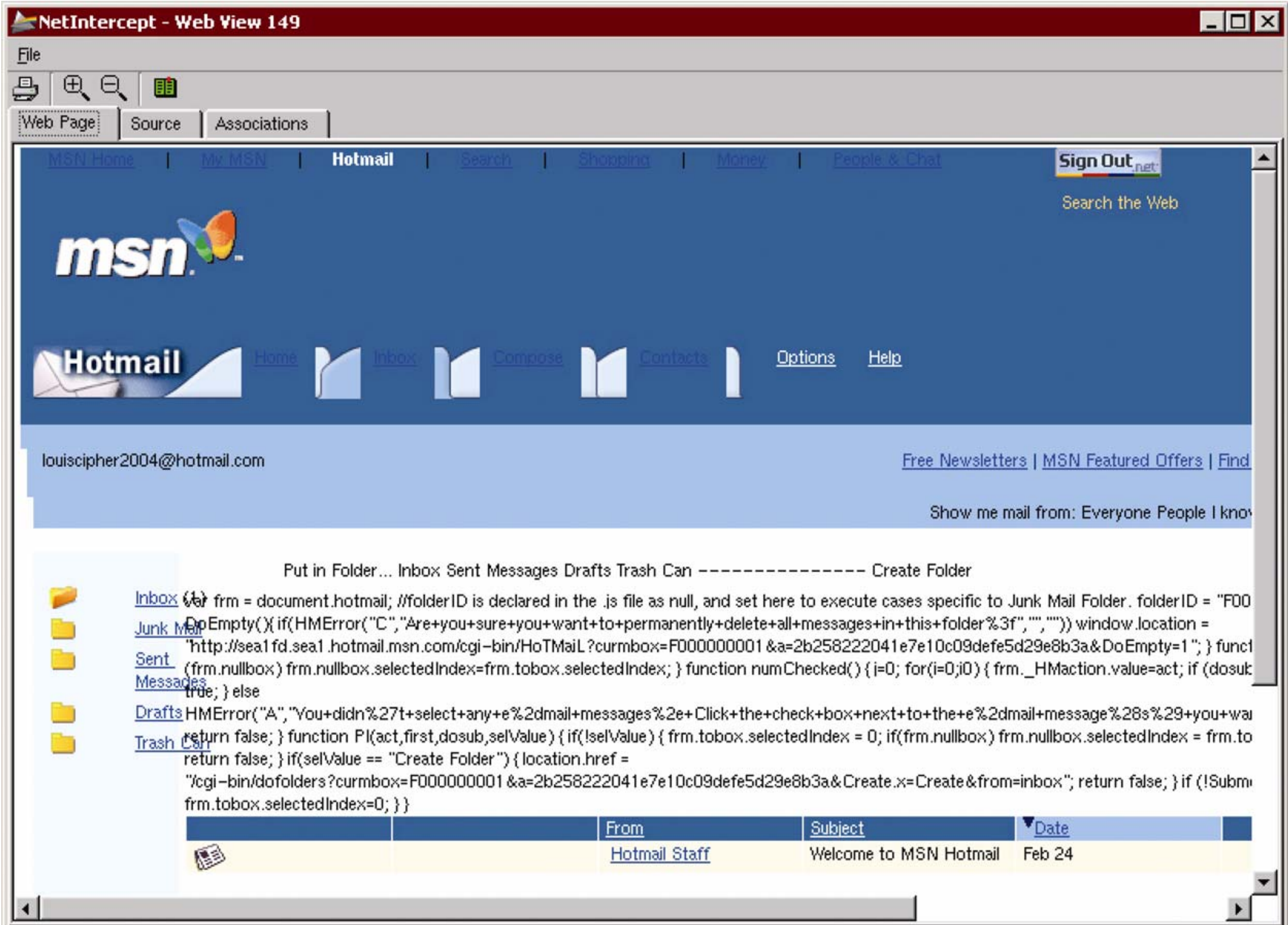
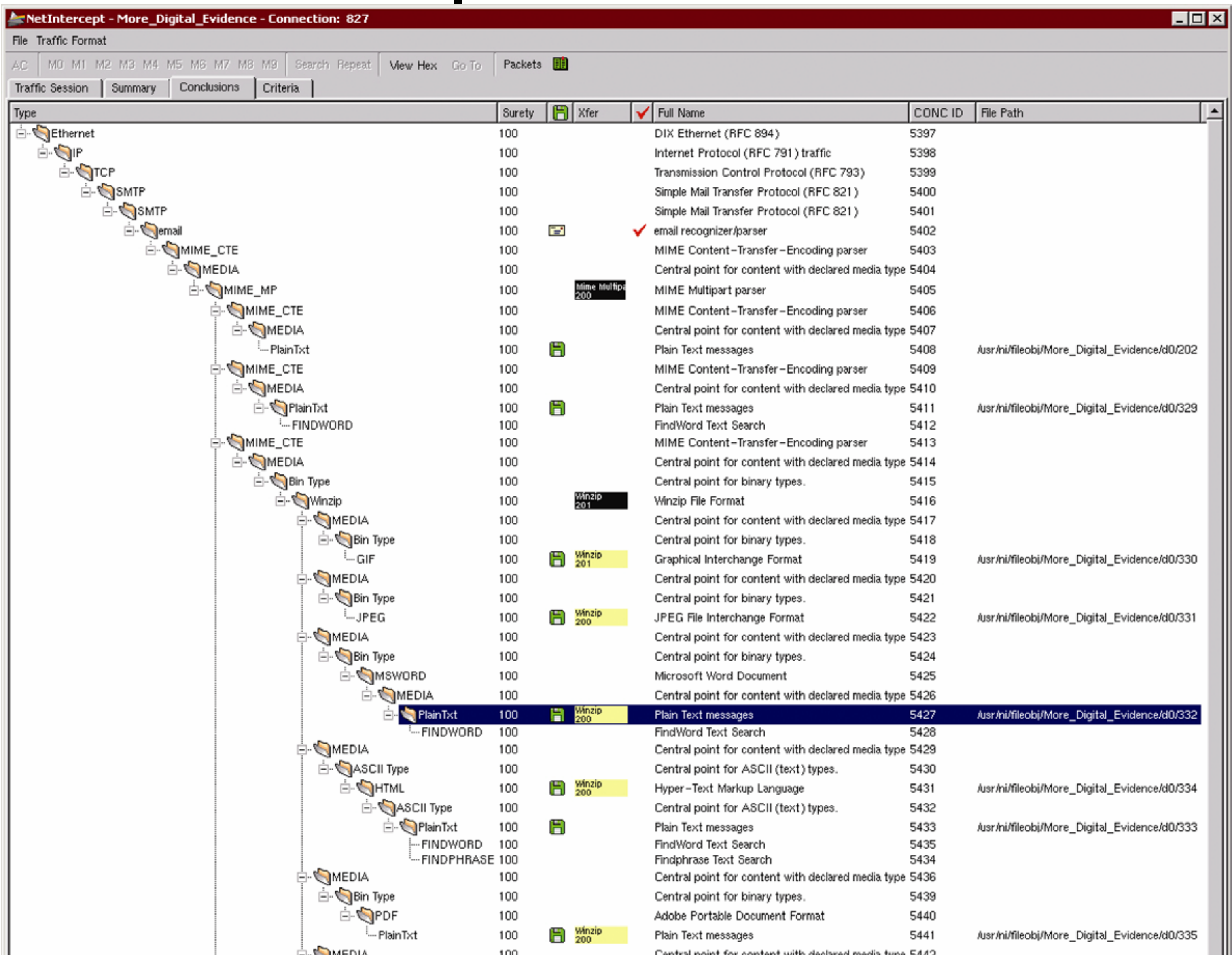


Figure from Eoghan Casey’s “Digital Evidence and Computer Crime”, 2nd edition

NetIntercept: Search/Recover

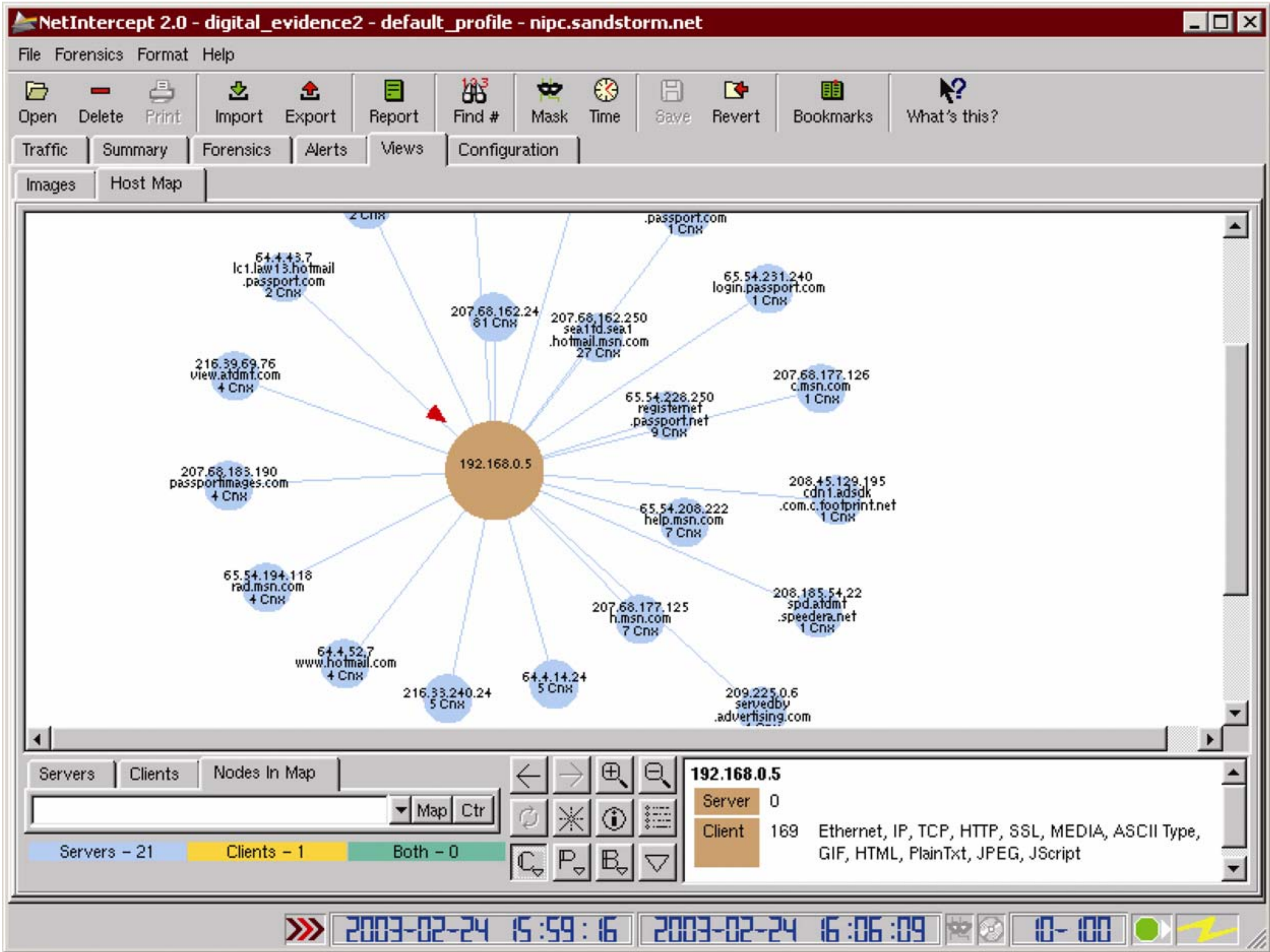


Analysis

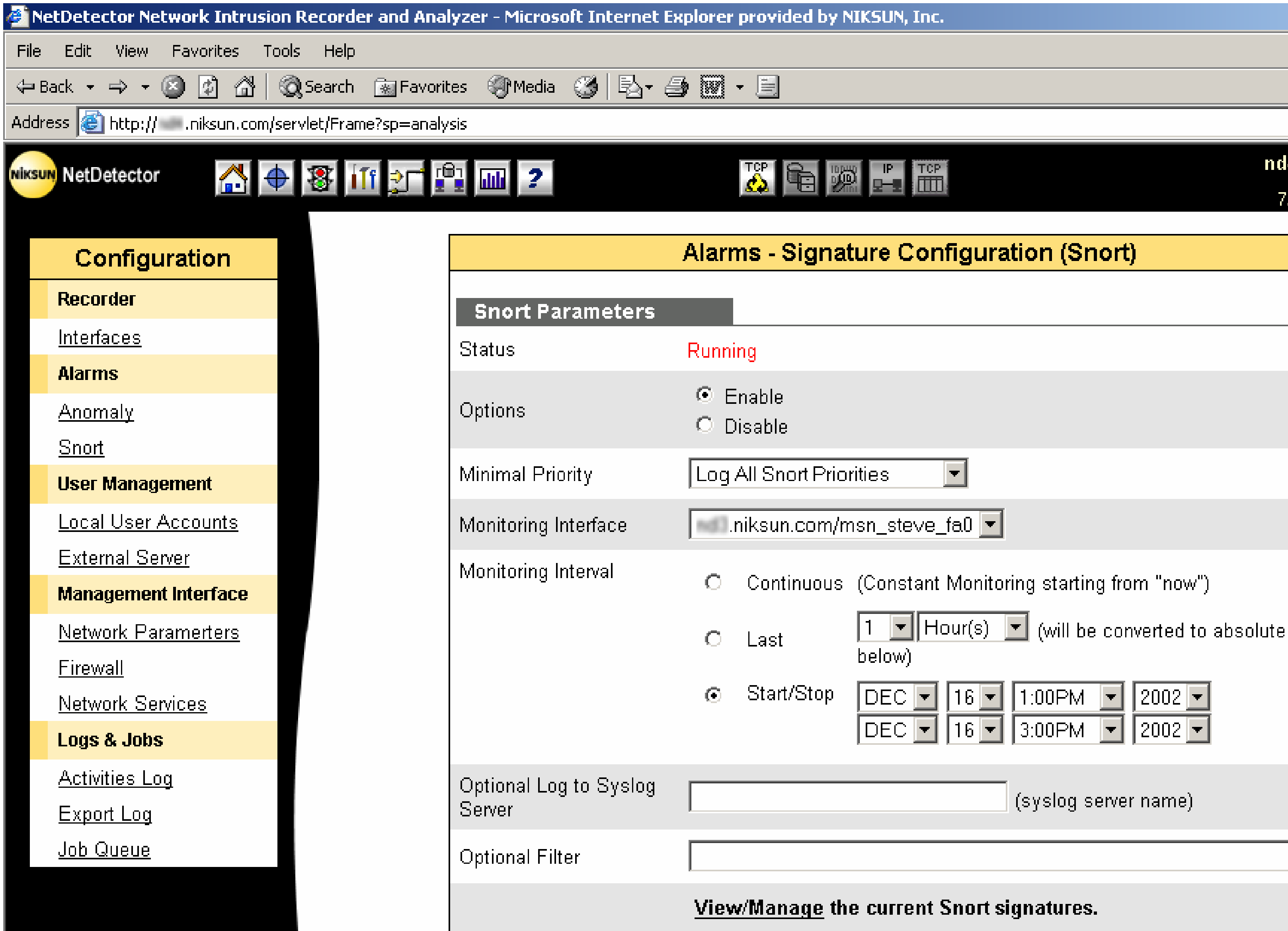
- Temporal views
  - Timelines
  - Histograms/charts
- Relational analysis
  - Thicker lines for higher traffic
  - N-gram analysis
- SilentRunner
  - 3-D visualization can be useful for analysis
  - Develop baseline of network activities for comparison
  - Visually represents anomalies and other noteworthy events

Figure from Eoghan Casey's "Digital Evidence and Computer Crime", 2nd edition

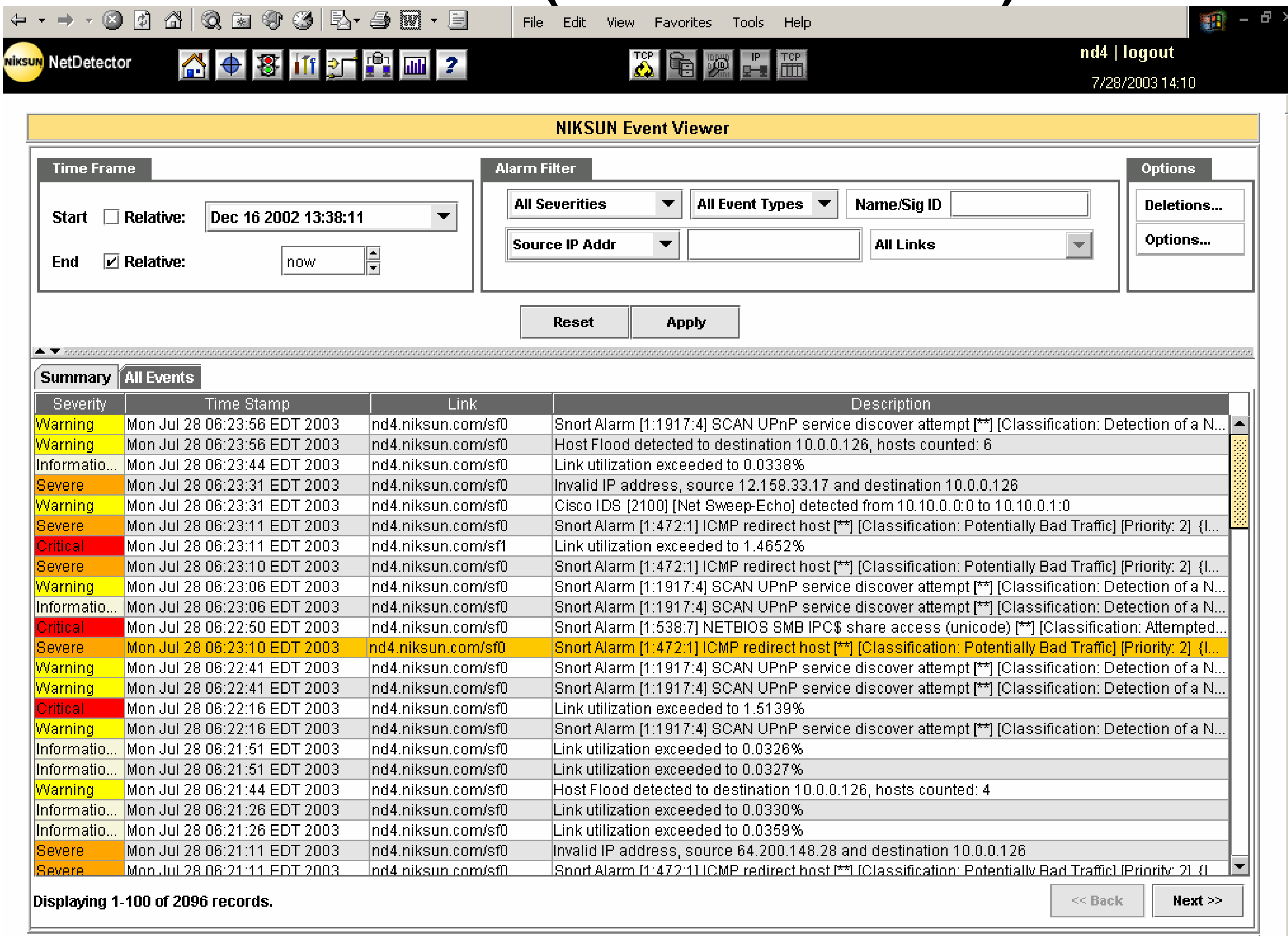
Analysis: NetIntercept



Analysis: NetDetector (Snort)



NetDetector (Snort cont.)



Visualization & Data mining

- Visualization techniques
  - Clustering and other techniques for visually representing data to help examiners identify noteworthy patterns and items in large datasets
- Data mining
  - Finding patterns, associations, links
  - Recognizing patterns of behavior

Reporting

- Bookmarks
- Default reports
  - Inventory hosts, accounts, nicknames files, etc.
  - Top talkers
  - Alerts

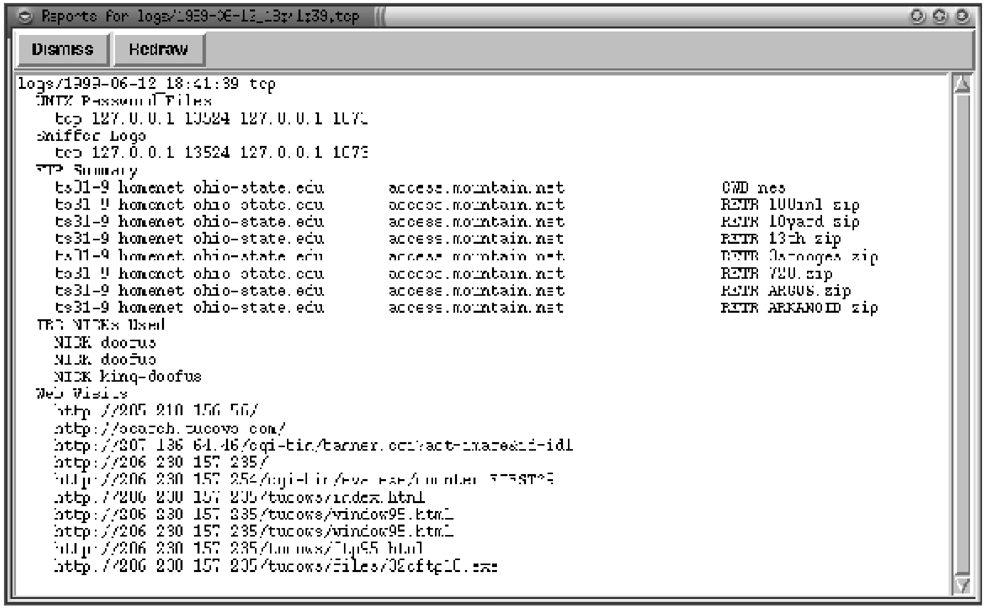


Figure from Steve Romig's "Incident Response Tools" chapter in Handbook of Computer Crime Investigation

Report Examples

Web Pages

Connection	Size	File Name
Host: 64.4.14.23		
12	311	/cgi-bin/linkdirector/signup?_lang=EN
Host: help.msn.com		
31	5405	/en_us/frameset.asp?Topic=REGTyp 20Passport BrandID= Filter= H_VEI
31	1152	/en_us/helpwindow.asp?Topic=REG 20Passport BrandID= Filter= H_VEI
31	3822	/en_us/h_tbar.asp?INI=PPv25.ini H_ ITSFile=ppv25.its51 H_VER=1.5 bI
32	2338	/!data/en_us/data/ppv25.its51/$conte H_APP=Microsoft+%2ENET+Pass xmltoc=
Host: lc1.law5.hotmail.passport.com		
4	10471	/cgi-bin/login
Host: loginnet.passport.com		
184	672	/logout.srf?_lang=EN lc=1033 id=2 n

Alerts

Connection ID	Time	Src IP	Src MAC	Dst IP	Dst MAC
Message: Connection close not captured					
199	2003-02-24 16:06:38	192.168.0.5	00:00:E2:8A:C4:6B	207.68.172.245	00:30:AB:1D:CD:EF
202	2003-02-24 16:06:38	192.168.0.5	00:00:E2:8A:C4:6B	63.150.154.197	00:30:AB:1D:CD:EF
203	2003-02-24 16:06:38	192.168.0.5	00:00:E2:8A:C4:6B	63.150.154.197	00:30:AB:1D:CD:EF
204	2003-02-24 16:06:38	192.168.0.5	00:00:E2:8A:C4:6B	152.163.209.77	00:30:AB:1D:CD:EF
116	2003-02-24 16:06:40	192.168.0.5	00:00:E2:8A:C4:6B	207.68.172.245	00:30:AB:1D:CD:EF
201	2003-02-24 16:06:40	192.168.0.5	00:00:E2:8A:C4:6B	207.68.172.245	00:30:AB:1D:CD:EF
Message: Media type 'image/gif' requested by GIF, but it didn't match and PlainTxt did					
141	2003-02-24 16:03:31	192.168.0.5	00:00:E2:8A:C4:6B	209.225.0.6	00:30:AB:1D:CD:EF
Message: Media type 'text/html' requested by HTML, but it didn't match and ASCII Type did					
187	2003-02-24 16:06:34	192.168.0.5	00:00:E2:8A:C4:6B	65.54.231.240	00:30:AB:1D:CD:EF
Message: Media type 'text/html' requested by HTML, but it didn't match and PlainTxt did					
190	2003-02-24 16:06:35	192.168.0.5	00:00:E2:8A:C4:6B	65.54.226.252	00:30:AB:1D:CD:EF
Message: Reset out of window					
14	2003-02-24 15:59:48	192.168.0.5	00:00:E2:8A:C4:6B	65.54.226.251	00:30:AB:1D:CD:EF
35	2003-02-24 16:02:01	192.168.0.5	00:00:E2:8A:C4:6B	65.54.208.222	00:30:AB:1D:CD:EF
193	2003-02-24 16:06:36	192.168.0.5	00:00:E2:8A:C4:6B	207.68.183.190	00:30:AB:1D:CD:EF
195	2003-02-24 16:06:36	192.168.0.5	00:00:E2:8A:C4:6B	207.68.183.190	00:30:AB:1D:CD:EF
Message: Window ignored					
14	2003-02-24 15:59:48	192.168.0.5	00:00:E2:8A:C4:6B	65.54.226.251	00:30:AB:1D:CD:EF
35	2003-02-24 16:02:01	192.168.0.5	00:00:E2:8A:C4:6B	65.54.208.222	00:30:AB:1D:CD:EF

This report was generated by NetIntercept® 2.0.

Comparison Summary

- NetIntercept & NetDetector
  - Best starting point for examination
  - Useful for most common analysis needs
- NFR Security
  - Advanced evidence processing using N-Code, GUI Queries & Perl Query Add-on
- SilentRunner
  - 3-D visualization useful in some cases
- DCS1000
  - Good effort to filter during collection (e.g., pen register, RADIUS, DHCP)

Summary of Future Needs

- Platform standards to minimize losses
  - Published performance testing
  - Consider security and stability
- Read-only
  - No network responses or queries during collection or examination
- Integrity
  - Not necessarily during collection (after)
- Validate security and data interpretation of tools
- Documentation
  - System status & performance (proper operation)
  - Record primary sources of losses
  - Audit trail of examiner actions

Future Needs (cont.)

- Support tcpdump format import and export
  - Collect using one tool, examine w/ other
- Filtering capabilities during collection
  - DHCP & RADIUS
  - May be safer to use specialize tool for protocol filtering & pen register needs
- Filtering during examination
  - Exclude known files (e.g., logo, safe content)
  - Flag suspicious files (e.g., encrypted files or intellectual property/hacker tools using MD5)
  - Drill down on top host/protocols (e.g., ntop.org)
  - More visualization of data to help filtering

Future Needs (cont.)

- Protocol identification and decode
  - Based on protocol v. variables chars
  - Flag protocol violations, missing SEQ #s
  - More decodes and step-by-step replay
- Text search capabilities
  - Keywords split between multiple packets
  - Grep syntax
- More file extraction capabilities
  - KaZaA fragments from multiple sources
- More analysis capabilities
  - Behavior pattern recognition
  - System profile violations