

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

Ву

#### **Eoghan Casey**

Presented At

The Digital Forensic Research Conference

**DFRWS 2003 USA** Cleveland, OH (Aug 6<sup>th</sup> - 8<sup>th</sup>)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

# 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

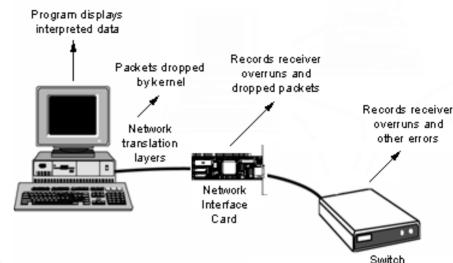
## • • Read Only

- 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

## • • 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</li>





























nd4 | logout 7/24/2003 17:51

Configuration
Recorder
<u>Interfaces</u>
Alarms
<u>Anomaly</u>
<u>Snort</u>
User Management
Local User Accounts
External Server
Management Interface
Network Paramerters
Firewall
Network Services
Logs & Jobs
2
Activities Log
Export Log
Job Queue

				Activities L	.og	
Timestamp	Origin IP Address	User Name			Activity Desc	cription
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	Dolated All events fr	om the Event Viewer dat	tabase.	
Mon Jul 14 23:12:13 EDT 2003	10,700 MTIP A	ddress	User Name	n.F. of	TCP-DATA/RECON_DATA filter	r: top and host 10.70.0.49 and port 1676 and host 207.46.108.42 a
Mon Jul 14 23:17:58 ED ≥ 003	10.70.0.2		admin	logged in		
Mon Jul 14 23:18 EDT 2003 Mon Jul 14 2	10.70.0.2		admin	Deleted ALL ev	vents from the Ev	
Tue Jul 12:13 EDT 2003	10.70.0.2		admin	Reconstructed of port 1863	data at 06/19/2003 ـ	
3:17:56 EDT 2003	10.70.0.2		admin	added/edited a	larm 1	p and host 207.48.108.42 and port 1863 and host 10.70.0.49 a
3:18:11 EDT 2003	10.70.0.2		admin	added/edited a	larm 2	host 10.0.0.249 and port 1481 and host 216.250.140.125 and po
19:02 EDT 2003	10.70.0.2		admin	added/edited a	larm 3	7
Tue Jul 15 5 EDT 2003	10.80.0.71		admin	logged in	ar	nd host 10.0.0.249 and port 1481 and host 216.250.140.125 and po
Tue Jul 15 08:22:			admin	logged III	ter: top ar	nd host 10.0.0.249 and port 1494 and host 64.208.42.41 and port 8
Tue Jul 15 08:22:31 ED 2003	10.70.0.2		admin	logged out	_waffic filter: top an	nd host 10.0.0.249 and port 1494 and host 64.208.42.41 and port 8
Tue Jul 15 08:22:39 EDT 2003	10.1/070.0.58		admin	logged in	ail/web_traffic filter: top ar	nd host 10.0.0.249 and port 1491 and host 216.250.140.125 and po
Tue Jul 15 09:08:56 EDT 2003	10.70.0.58	admin	timeout			
Tue Jul 15 09:08:58 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 a port 80	: 08/09/2001 17:46:45 of	CRA/code_red_attack filter: top	and host 63.237.137.50 and port 5648 and host 206.20.52.134 an
Tue Jul 15 09:53:52 EDT 2003	10.70.0.28	admin	Reconstructed data a port 80	: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 an
Tue Jul 15 09:54:05 EDT 2003	10.70.0.28	admin	Reconstructed data a port 80	: 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 an
Tue Jul 15 09:54:18 EDT 2003	10.70.0.28	admin	Reconstructed data a port 80	: 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 an
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 si	erra.mj.niksun.com in vo	ip001lpm-jfs-1.enc	
Tue Jul 15 16:10:21 EDT 2003	10.70.0.209	admin	Data Imported from si	erra.mj.niksun.com in vo	ip001lpm-jfs-1.enc.gz	
Tue Jul 15 16:15:40 EDT 2003	10.70.0.209	admin	Data Imported from si	erra.mj.niksun.com in vo	ip001lpm-jfs-1.enc.gz	
Tue Jul 15 16:25:39 EDT 2003	10.70.0.103	admin	logged in			

External MD	)5 Calc	ulations
NetDetector   Ne		
	<u>\$\$</u>	
		Export/Import
On-demand Export Sci		Pimport
	Export Parameters	
	Title of Export  Conversion Format	Test1  pcap (Topdump) ▼
	Transfer Mode	ftp
	IP Address	10.0.0.20
	Relative Path	/tmp/ Example: archive/hourly
	Login	guest
	Password	****
	Data Source	
	Interfaces	nd4.niksun.com/sf0
	Export Type	One time only
	Time Span	
	Start   ✓ Relative:	-1 hour hour
	End ☑ Relative:	now
	Begin Export At [Hour:Min]	00: ▼ 00 ▼
	Filter (Optional)	
	Exported File Slice Size	40MB ▼ (1MB - 40MB)
	Compress Data (gzip)	
Telnet test3		_
bash-2.04\$ cd /usr/local/mercury/tmp bash-2.04\$ ls		username@example.com
bash 2.047 is export_data_stream bash-2.04\$ md5 export_data_stream > export_da bash-2.04\$ scp export_data_stream* vcr@10.0.0	ta_stream.md5 .20:/tmn	SNMP Recipient (host or IP)
TOTAL		ncel

### • • Filtering During Collection

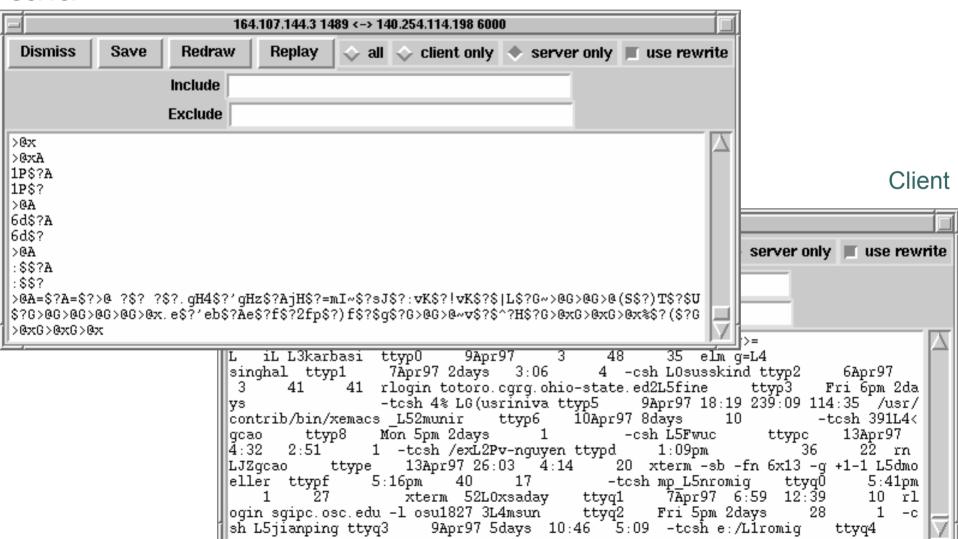
- BPF/Ethereal filtering syntax
  - IP address, port, etc.
- MAC address
- Custom NFR Security filters (using N-code)
- DCS1000
  - RADIUS
  - DHCP
- Filtering on protocol is risky
  - Pen register for e-mail (DCS1000)
  - If necessary, be very careful
  - Ideally use a specialized tool for this purpose

## • • 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



### Review: X Session Replay

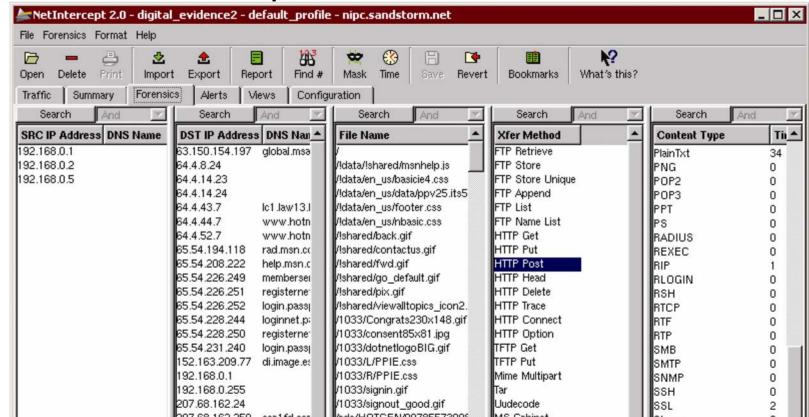
- Step-by-step session replay
- Pauses before redrawing screen

```
Untitled
susskind ttyp2
                                                            rlogin totoro.cgrg.ohio-state.ed
                       Fri 6pm 2days
9Apr97 18:19 239:09 114:35
10Apr97 @days 10
                                                            /usr/contrib/bin/xemacs
ļusriniva ttūp5
                                                             -csh
gcao
                                                            -tcsh
lūuc.
v-nguyen ttypd
gcao ttype
                                                           xterm -sb -fn 6x13 -g +1-1 -tcsh
lm̃oeller
romig
                                                       10 rlogin sgipc.osc.edu -l osu1827
Isadaŭ
                                                            -csh
                                                            -tcsh
jianping ttyc
romig
|zhanĝj
susskind
                       Mon10am
<u>Bašak</u>
                                                    7:18 xterm -fn 9x15 -e rlogin fido
2 rlogin fido
                        Tue10am
                       Tuellam 2days
Fril2pm 2days
snoopy ~>
```

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

### **Examination: Data Reduction**

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



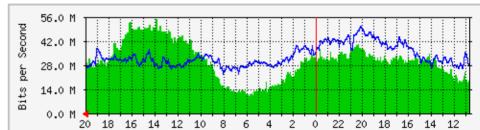
# • • Examination: Data Reduction

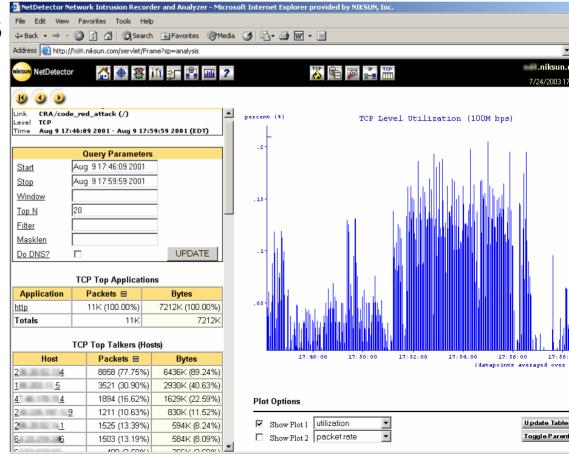
- SilentRunner: 3-D Visualization
- NFR Security: Query interface

	-
Title: ICMP v.2	
Source Address	
Destination Address	
▼ ICMP Type	
▼ ICMP Code	
✓ Description	
✓ Additional Information	
☐ <u>U</u> se time as a column for d ☐ <u>N</u> o earlier than ☐ Earliest data available	isplay
	9/01 × 12:00:00 AM ×
No later than <ul> <li>No Latest data available</li> </ul>	
C Ending: 5/1	11/01 = 12:00:00 PM =

### **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

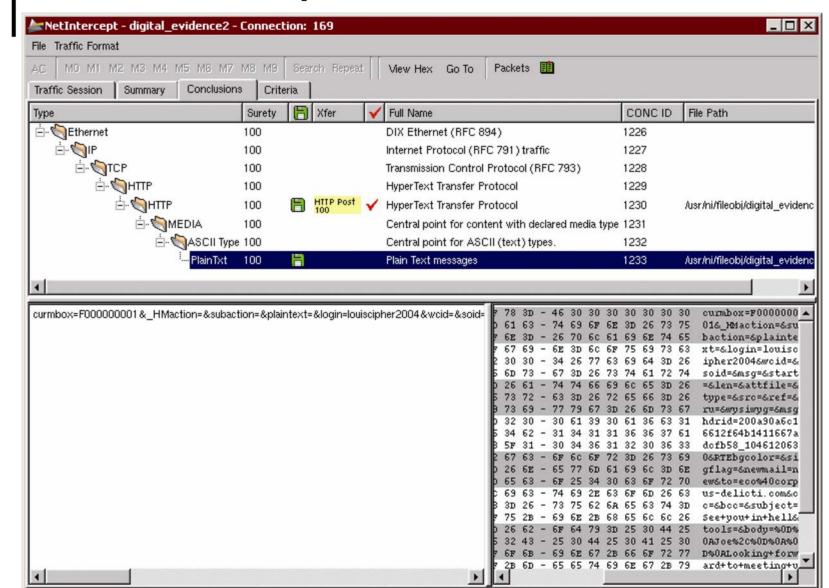
### • Search and Recovery

- 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

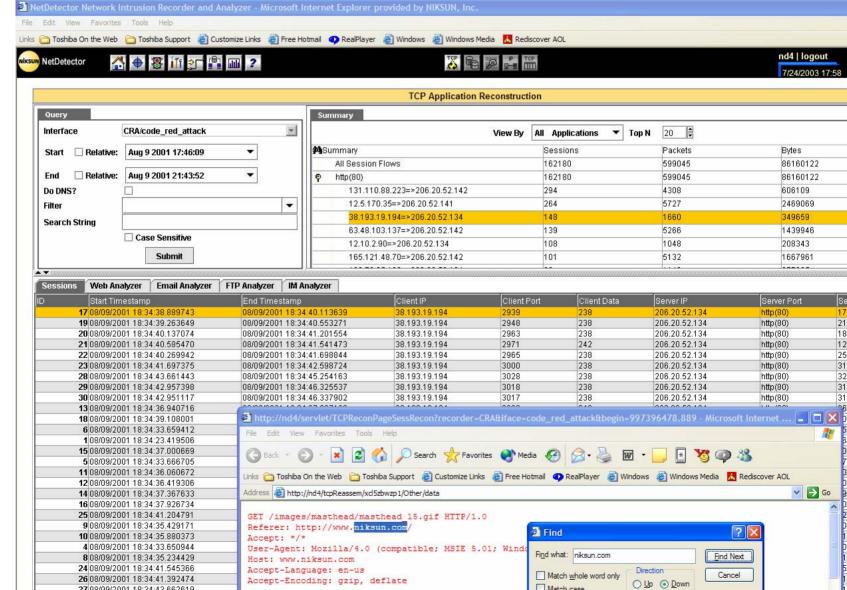
# Ethereal: Search hotmail-02242003.tcp - Ethereal

<b>O</b> noth	nail-02242003.t	cp - Ethereai								
File .	Edit <u>C</u> apture	Display :	Tools							
	Time			Source		Destination		Protocol	Info	
3888	2003-02-24	16:04:04.	2164	192.168.0.1		ALL-SYSTEMS.	MCAST.NET	IGMP	V2 Membershi	ip Q
3889	2003-02-24	16:04:04.	2175	192.168.0.1		DHCP-AGENTS.	MCAST.NET	IGMP	V2 Membershi	ip R
3890	2003-02-24	16:04:32.	2196	192.168.0.1		192.168.0.25	5	RIPV1	Response	
3891	2003-02-24	16:05:02.	2230	192.168.0.1		192.168.0.25	5	RIPV1	Response	
3892	2003-02-24	16:05:03.	0375	HZJT101		192.168.0.25	5	BROWSER	Local Master	· Ani
3893	2003-02-24	16:05:32.	2269	192.168.0.1		192.168.0.25	5	RIPV1	Response	
3894	2003-02-24	16:05:56.	7496	192.168.0.5		sea1fd.sea1.	hotmail.m	TCP	32942 > http	) [S
				sealfd.seal.	hotmail.m			TCP	http > 32942	
				192.168.0.5		sealfd.seal.	hotmail.m	TCP	32942 > http	
				192.168.0.5		sealfd.seal.			POST /cgi-bi	
				192.168.0.5		sealfd.seal.			Continuation	
				sealfd.seal.	hotmail.m	192.168.0.5		TCP	http > 32942	: Гас
				192.168.0.5		sea1fd.sea1.	hotmail.m	HTTP	Continuation	
3901	2003-02-24	16:05:57.	2074	sea1fd.sea1.	hotmail.m	192.168.0.5		HTTP	HTTP/1.1 100	) Cor
				192.168.0.5			hotmail.m	TCP	32942 > http	[A0
Saus	2003-02-24	16.05.57	7875	1دمه 1fdدمه	hotmail m	107 168 0 5		нттр	HTTD/1 1 700	
<u> </u>						****				
⊞ Fra	me 3900 (53	8 on wire	, 538	captured)						
	ernet II									
[	estination	: 00:30:ak	o:1d:d	d:ef (DELTA	_ld:cd:ef)					
Destination: 00:30:ab:1d:cd:ef (DELTA_1d:cd:ef) Source: 00:00:e2:8a:c4:6b (ACER_8a:c4:6b)										
	ype: IP (0:				-					
									otmail.msn.co	
									q: 1433552153	
	ertext Tran			-	•	• •		- • •		-
<u> </u>						****				
0000	00 30 ab 1	d cd af O	0.00	e2 8a c4 6b	08 00 45		kE			
0010	02 Oc a8 a	b 40 00 4	0 06	5d 54 c0 a8	00 05 cf	44@.@	. ]T			
0020	a2 fa 80 a	e 00 50 5	5 72	5d 54 c0 a8 45 19 aa 96	a0 7b 80	18PU				
0030	16 d0 f6 e	.8 00 00 0	1 01	-08 0a 00 06	6 98 2f 02	8c	/.			
0040	57 3f 43 6	if 6e 74 6	5 6e	74 2d 54 79	70 65 3a	20 W?Conte	n ţ-Type:			
<u> 10050                                  </u>	61 70 70 6	ic 69 63 6	1 74	69 6f 6e 2f	78 2d 77	77 annlica	t ion∕x-w	W		

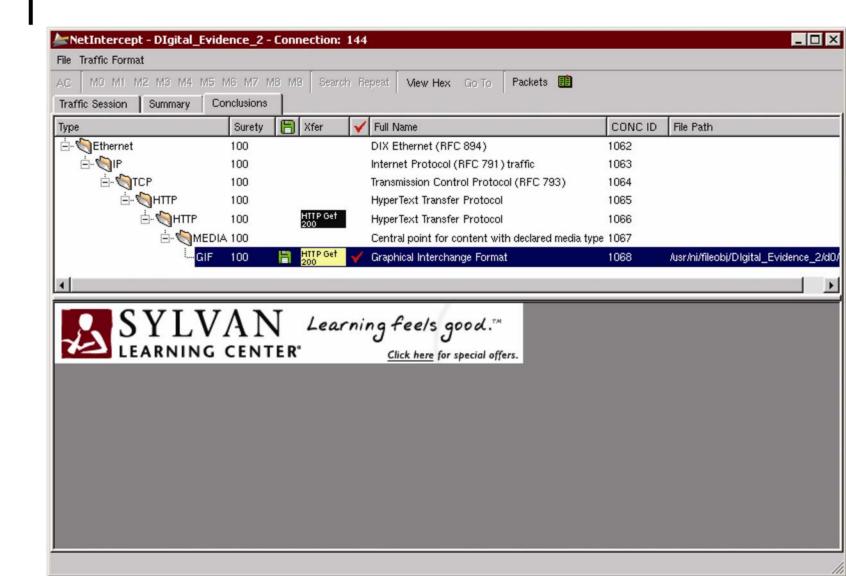
### NetIntercept: Search



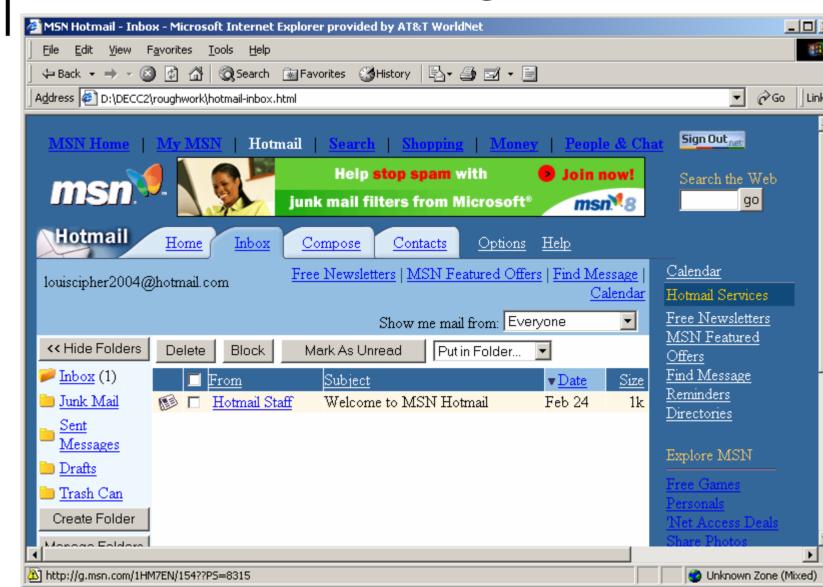
### NetDetector: Search (GUI)



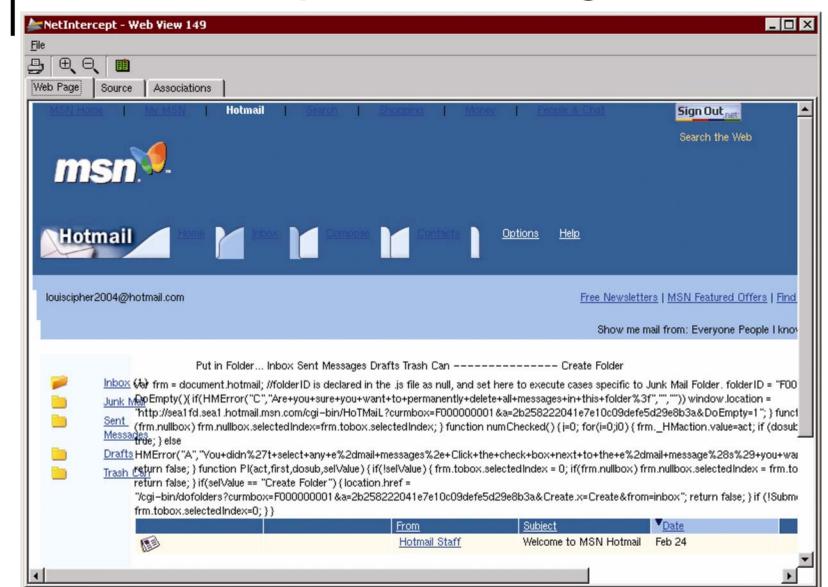
### NetIntercept: Image Extraction



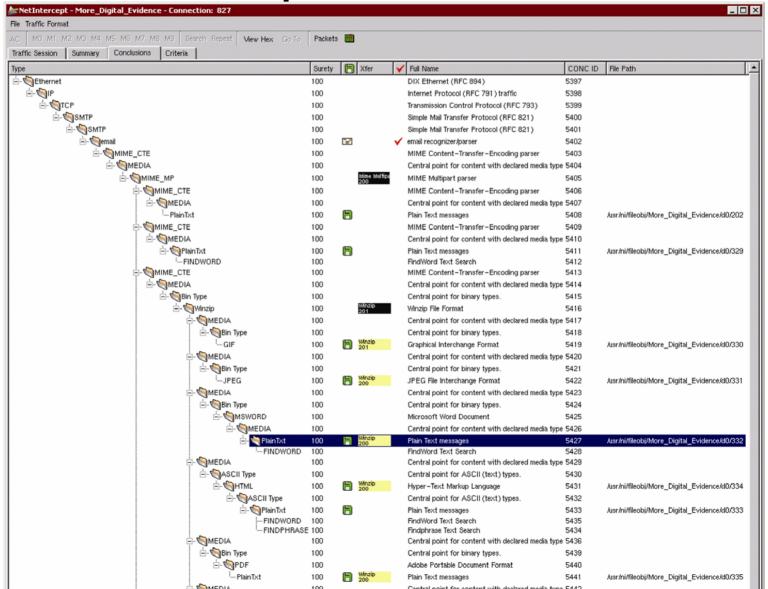
### Ethereal: Web Page



### NetIntercept: Web Page



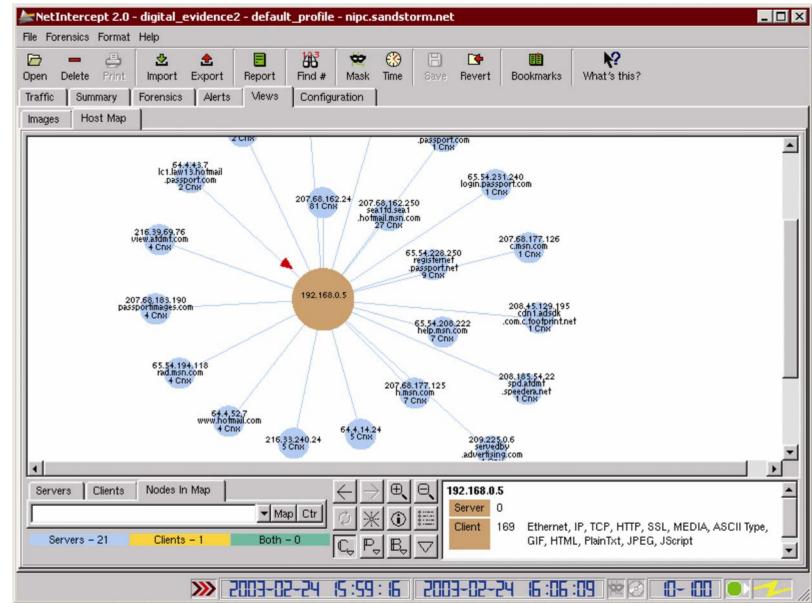
### NetIntercept: Search/Recover



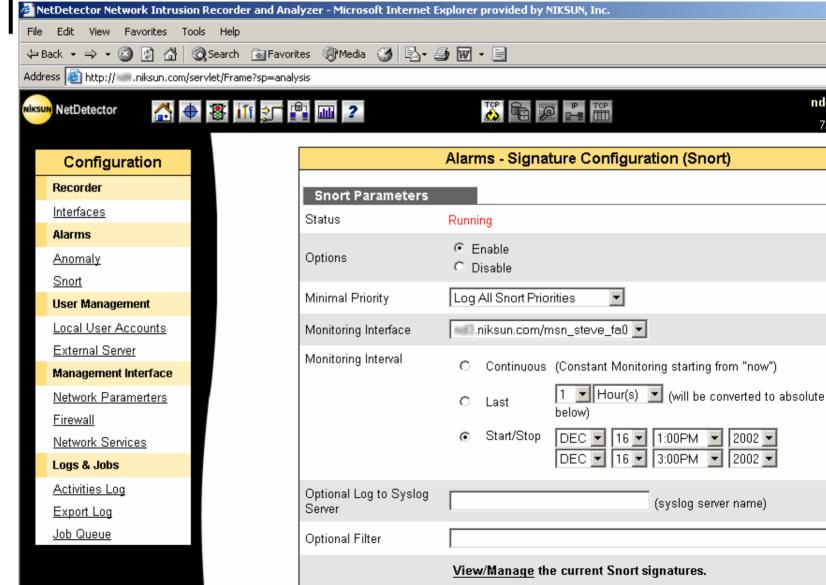
# • • Analysis

- 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

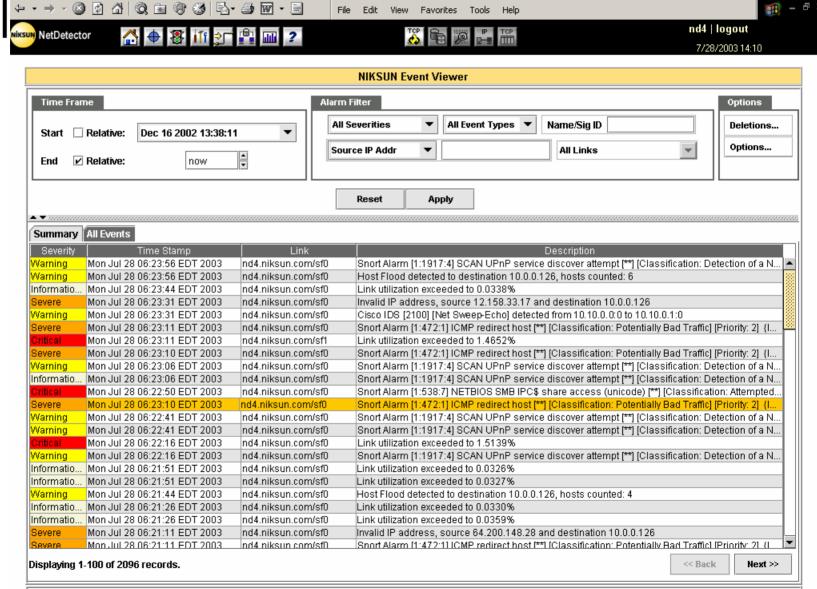
### Analysis: NetIntercept



### 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

```
sports For logs/1989-06-12_18;/1;39,tcp
            Redraw
logs/1999-06-12 18:41:39 tcp
 ŰNTZ P⊣ssvord[Files
   Eco 127, 0, 0, 1 10524 127, 0, 0, 1 1070
 whifter Logo
   tep 127, 0.0, 1 13524 127, 0.0, 1 1073
 TTP Summary
   tsD1-9 homenet obio-state.edu
                                            access.mountain.net
                                                                                   CWD nes
                                                                                   RETR 100inl sip
    to31 9 homenet ohio otate.ccu
                                            accepe, mountain, not
   ts31-9 homenet ohio-state.edu
                                                                                   RETH 10yard sip
                                            access.mountain.nst
   ts31-9 homenet ohio-state.edu
                                            access.mountain.nst
                                                                                   RITE 13th zip
   tall-9 homenet objo-state edu.
                                                                                   BVTB Ostooges zije
                                           laccese mountain net
   to31 9 homenet ohio otate.ccu
                                                                                   RETR 720, sip
                                           access.mountain.nst
   ts31-9 homenet ohio-state.edu
                                                                                   RATE ARGUS, zip
                                           access.mountain.nst
   ts31-9 homenet ohio-state.edu
                                           access.mountain.nst
                                                                                   RITE ARKANOID ZIO
 TRO NICKS Used
   NICK doorus
   NIUM doofub
   NICK king-doofus
 Web Visits
    Sthp //205 210 156 56/
   http://ocarch.tucovo.com/
   http://207-136-64.46/ogi-bir/barner.col/act-image&li-idl
   http://206 230 157 235/
    htt¦r://206-230-157-254/ogi-bir/evalexe/condectsT5ST°5
   http://206-200-157-205/tucows/index.html
   http://206_230_157_235/tucows/vindow95.html
http://206_230_157_235/tucows/vindow95.html
http://206_230_157_235/tucows/vindow95.html
   http://206-200-157-205/tucows/files/02cftp10.exe
```

# • • Report Examples

Connection	Size	File Name	Г
Host: 64.4.1	4.23		
12	311	/cgi-bin/linkdirector/signup?_lang=EN	(
Host: help.1	nsn.com	ı	N
31	5405	/en_us/frameset.asp?Topic=REGTyp 20Passport BrandID= Filter= H_VEI	2
31	1152	/en_us/helpwindow.asp?Topic=REG 20Passport BrandID= Filter= H_VEI	2
31	3822	/en_us/h_tbar.asp?INI=PPv25.ini H_ ITSFile=ppv25.its51 H_VER=1.5 bI	1 2
32	2338	/!data/en_us/data/ppv25.its51/\$conte H_APP=Microsoft+%2ENET+Pass; xmltoc=	1
Host: lcl.la	w5.hotn	nail.passport.com	N
4	10471	/cgi-bin/login	1
Host: login	netpass	portcom	l
184	672	/logout.srf?_lang=EN lc=1033 id=2 n	1
			N

Web Pages

/\lartc	
AIPH	2

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' reque	sted by GIF, l	but it didn't match an	d 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	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: Windo	w 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				

### • • 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
- o 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