Ethical Hacking and Countermeasures

Version 6

Module X

Sniffers

Scenario

Jamal, is an electrician who fixes electrical and network cables. He was called in for a regular inspection at the premises of XInsurance Inc. Jamal was surprised at his findings during a routine check of the AC ducts in the enterprise. The LAN wires were laid through the ducts.

He was tempted to find the information flowing through the LAN wires.

What can Jamal do to sabotage the network?

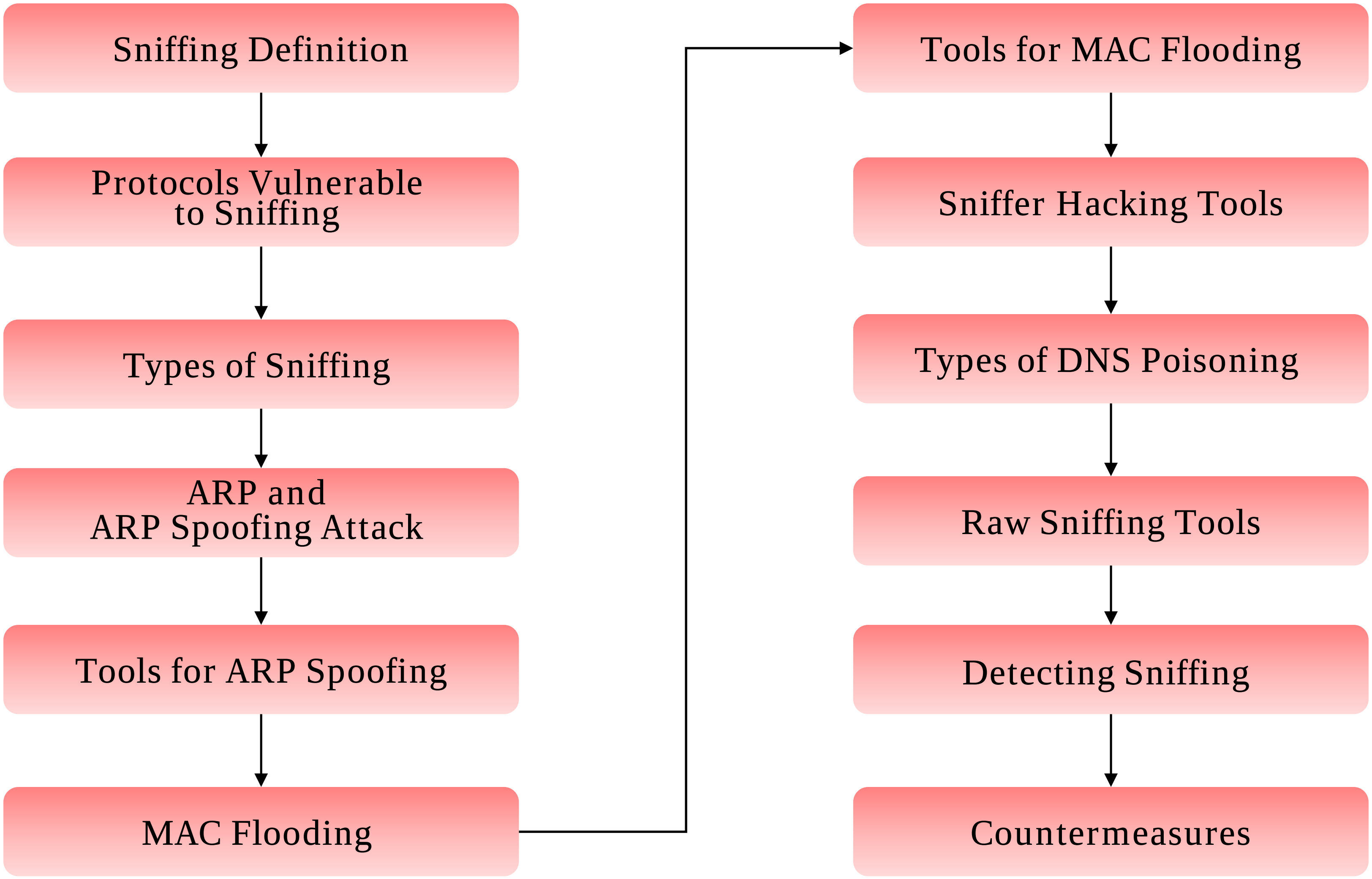
What information can he obtain and how sensitive is the information that he would obtain?

Module Objective

This module will familiarize you with:

- Sniffing
- Protocols vulnerable to sniffing
- Types of sniffing
- ARP and ARP spoofing attack
- Tools for ARP spoofing
- MAC flooding
- Tools for MAC flooding
- Sniffing tools
- Types of DNS poisoning
- Raw sniffing tools
- Detecting sniffing
- Countermeasures

Module Flow



Sniffing Definition

Protocols Vulnerable to Sniffing

Types of Sniffing

ARP and ARP Spoofing Attack

Tools for ARP Spoofing

MAC Flooding

Tools for MAC Flooding

Sniffer Hacking Tools

Types of DNS Poisoning

Raw Sniffing Tools

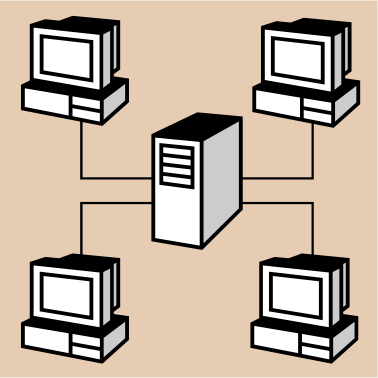
Detecting Sniffing

Countermeasures

Definition: Sniffing

Sniffing is a data interception technology

Sniffer is a program or device that captures the vital information from the network traffic specific to a particular network



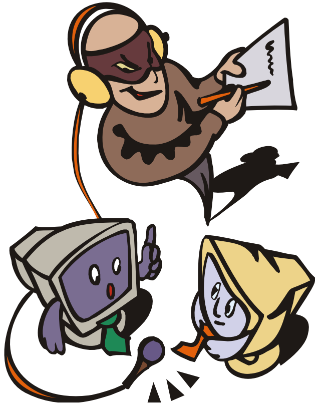
The objective of sniffing is to steal:

- Passwords (from email, the web, SMB, ftp, SQL, or telnet)
- Email text
- Files in transfer (email files, ftp files, or SMB)

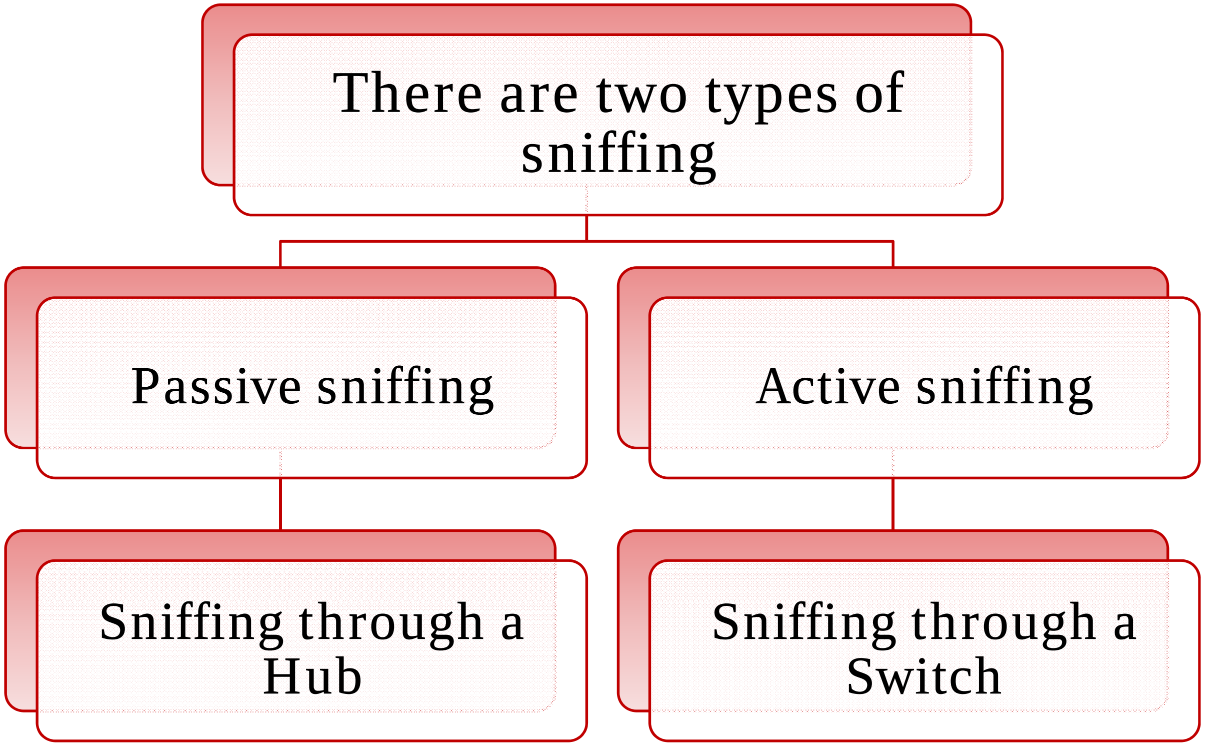
Protocols Vulnerable to Sniffing

Protocols that are susceptible to sniffers include:

- Telnet and Rlogin: Keystrokes including user names and passwords
- HTTP: Data sent in the clear text
- SMTP: Passwords and data sent in clear text
- NNTP: Passwords and data sent in clear text
- POP: Passwords and data sent in clear text
- FTP: Passwords and data sent in clear text
- IMAP: Passwords and data sent in clear text



Types of Sniffing



There are two types of sniffing

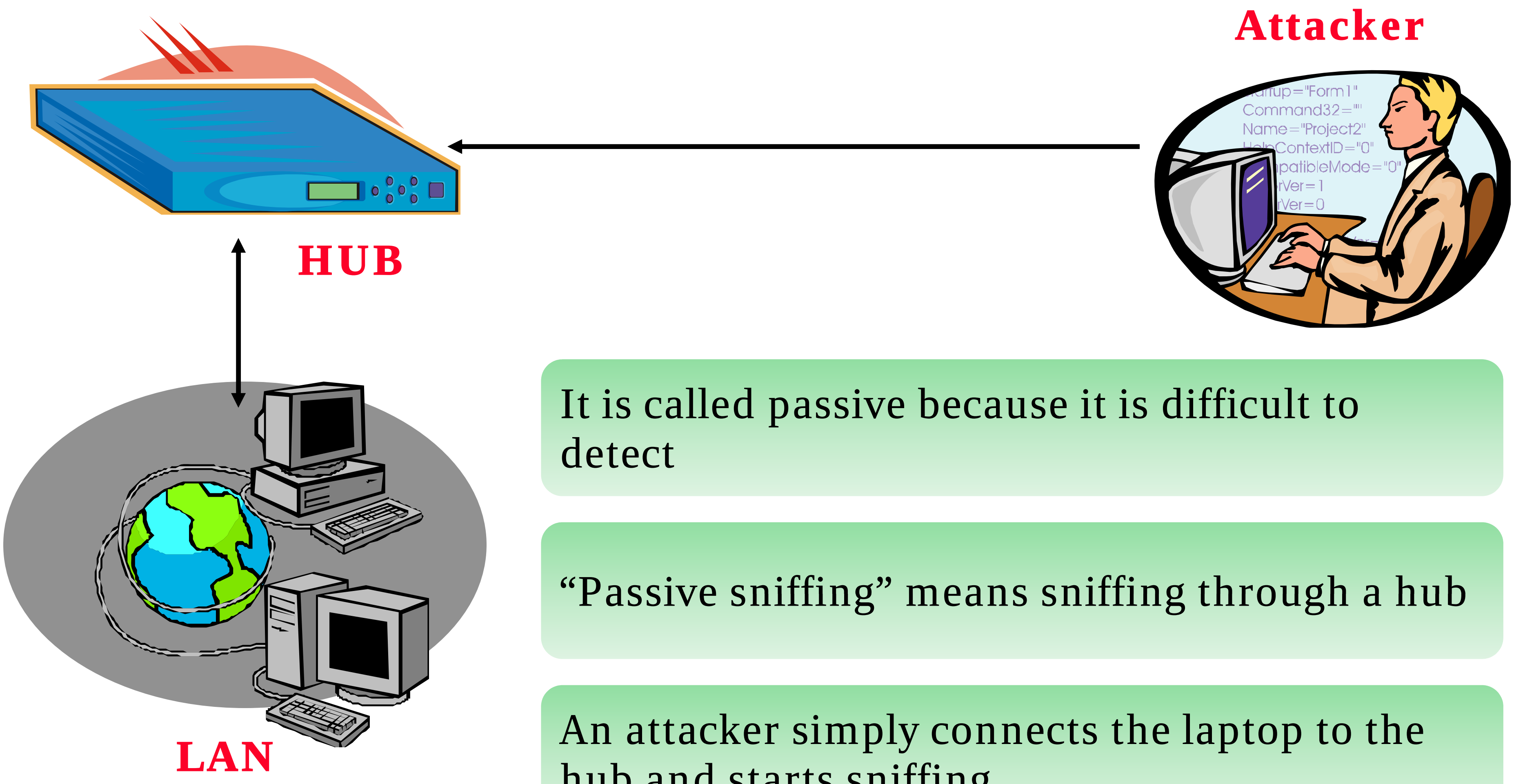
Passive sniffing

Active sniffing

Sniffing through a Hub

Sniffing through a Switch

Passive Sniffing



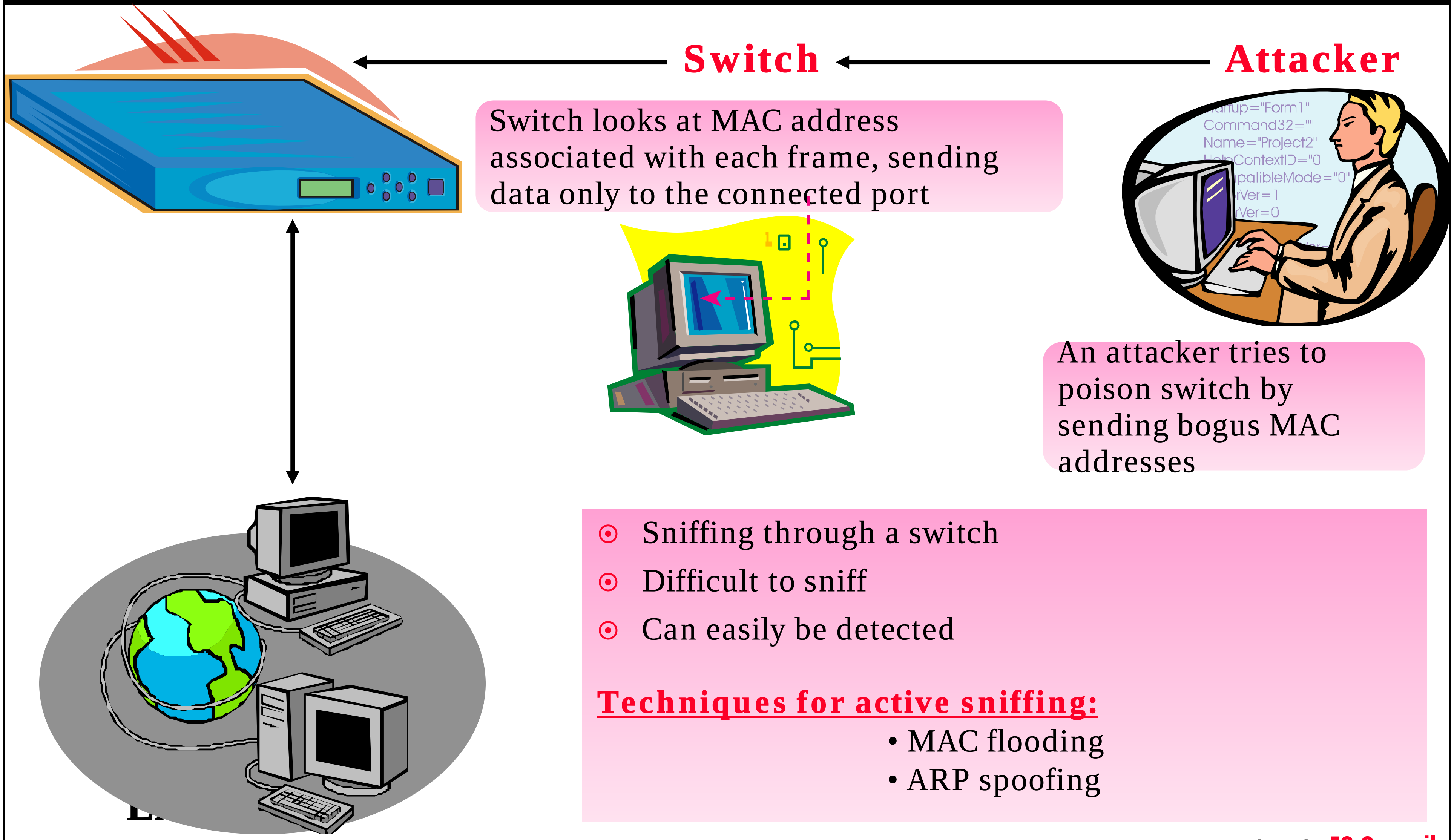
It is called passive because it is difficult to detect

“Passive sniffing” means sniffing through a hub

An attacker simply connects the laptop to the hub and starts sniffing

CEH™ Certified Ethical Hacker

Active Sniffing



Switch looks at MAC address associated with each frame, sending data only to the connected port

An attacker tries to poison switch by sending bogus MAC addresses

- Sniffing through a switch
- Difficult to sniff
- Can easily be detected

Techniques for active sniffing:

- MAC flooding
- ARP spoofing

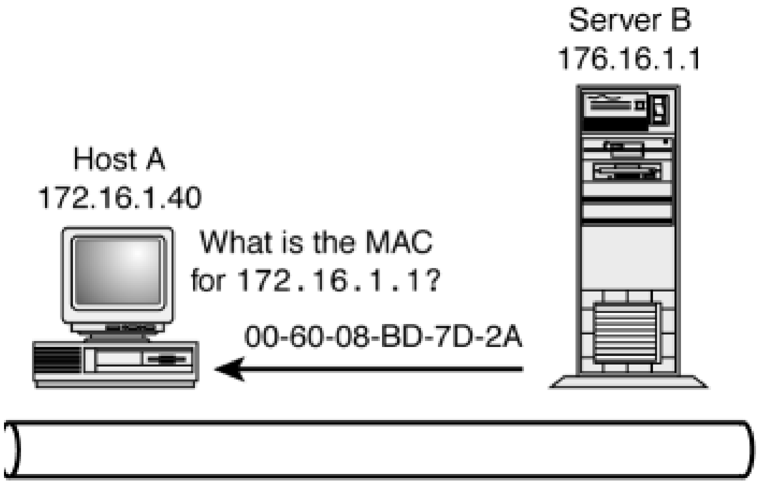
EC-Council

What is Address Resolution Protocol (ARP)

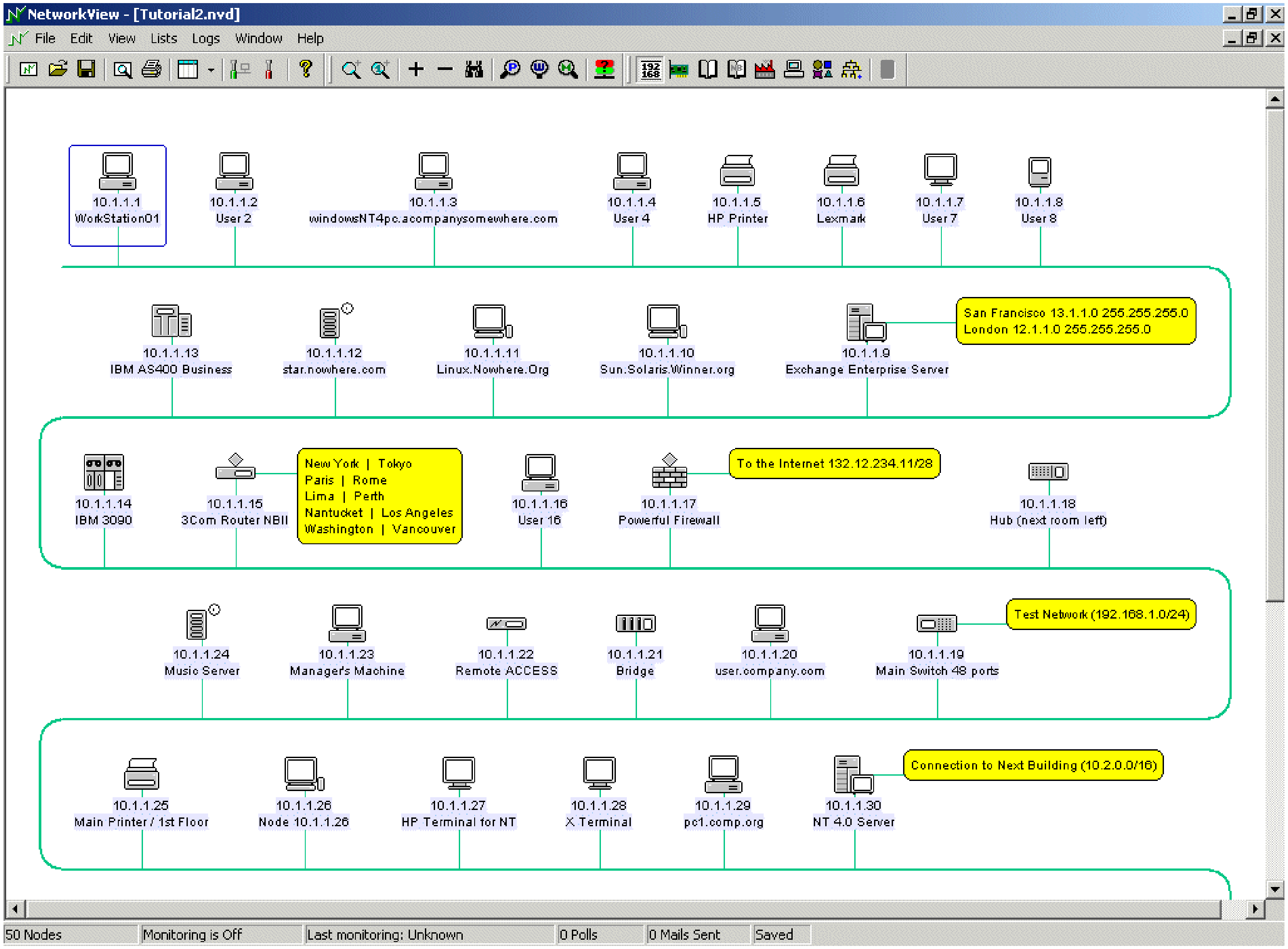
ARP is a network layer protocol used to convert an IP address to a physical address (called a MAC address), such as an Ethernet address

To obtain a physical address, host broadcasts an ARP request to the TCP/IP network

The host with the IP address in the request replies with its physical hardware address on the network



Tool: Network View – Scans the Network for Devices



The Dude Sniffer

Developed by Mikro Tik, the Dude network monitor is a new application which can improve the way you manage your network environment

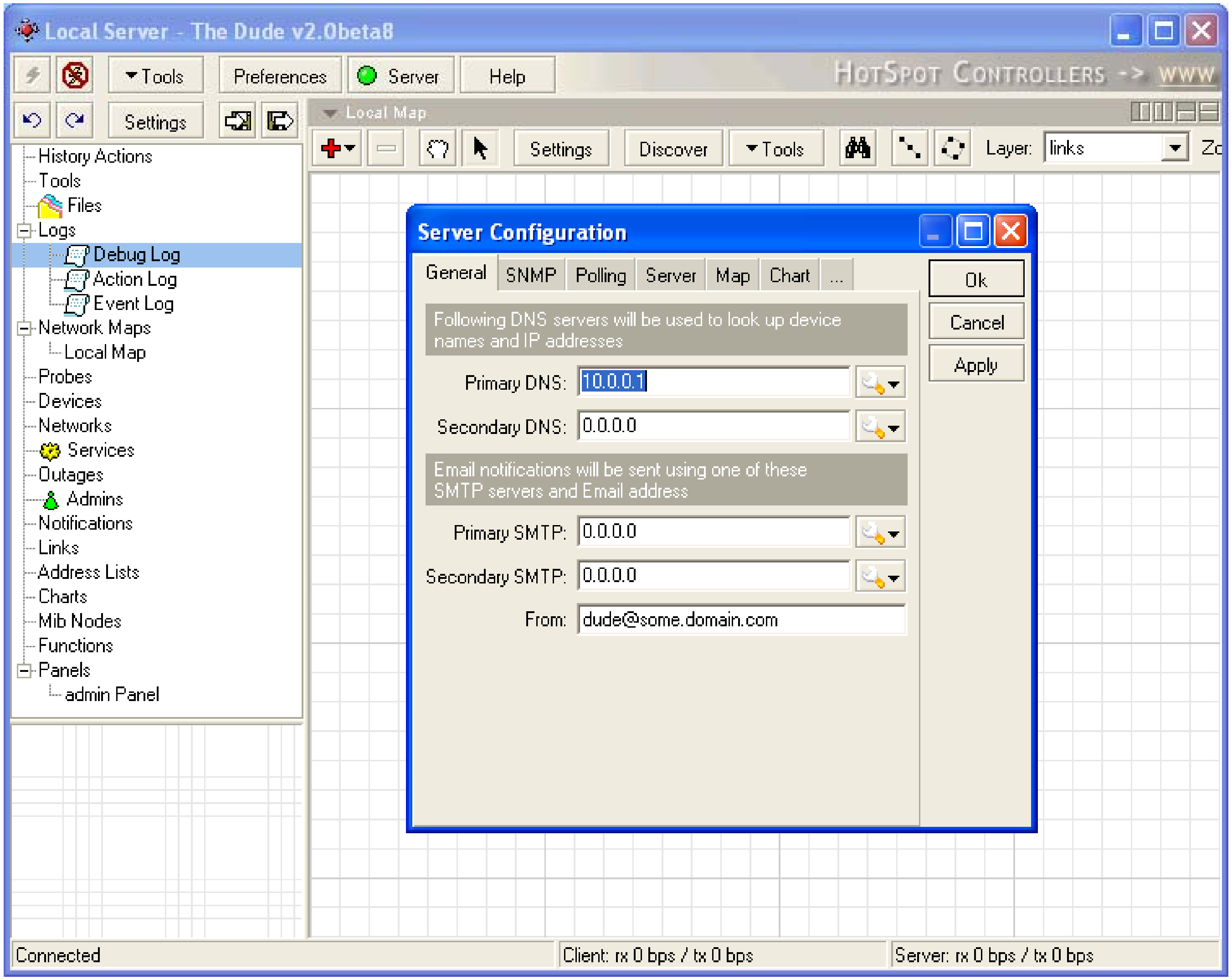
Functions:

- Automatically scans all devices within the specified subı
- Draws and lays out a map of your networks
- Monitors services of your devices
- Alerts you in case some service has problems

It is written in two parts:

- Dude Server, which runs in a background
- Dude Client, which may connect to local or remote dude server

The Dude Sniffer: Screenshot 1



Following DNS servers will be used to look up device names and IP addresses

Primary DNS: 10.0.0.1

Secondary DNS: 0.0.0.0

Email notifications will be sent using one of these SMTP servers and Email address

Primary SMTP: 0.0.0.0

Secondary SMTP: 0.0.0.0

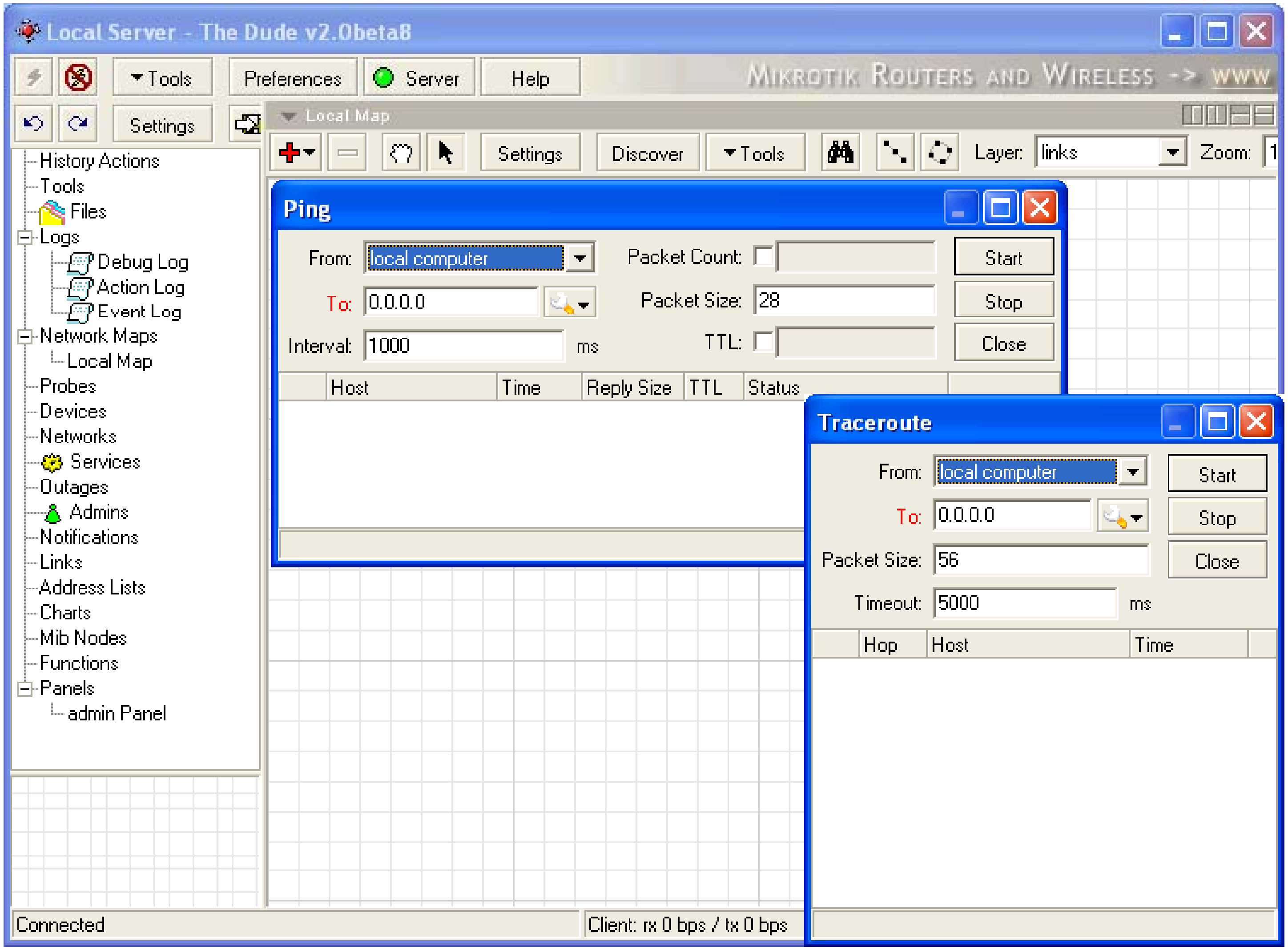
From: dude@some.domain.com

Connected

Client: rx 0 bps / tx 0 bps

Server: rx 0 bps / tx 0 bps

The Dude Sniffer: Screenshot 2



Local Server - The Dude v2.0beta8

Ping

From: local computer

To: 0.0.0.0

Interval: 1000 ms

Packet Count: □

Packet Size: 28

TTL: □

Host	Time	Reply Size	TTL	Status

Traceroute

From: local computer

To: 0.0.0.0

Packet Size: 56

Timeout: 5000 ms

Hop	Host	Time

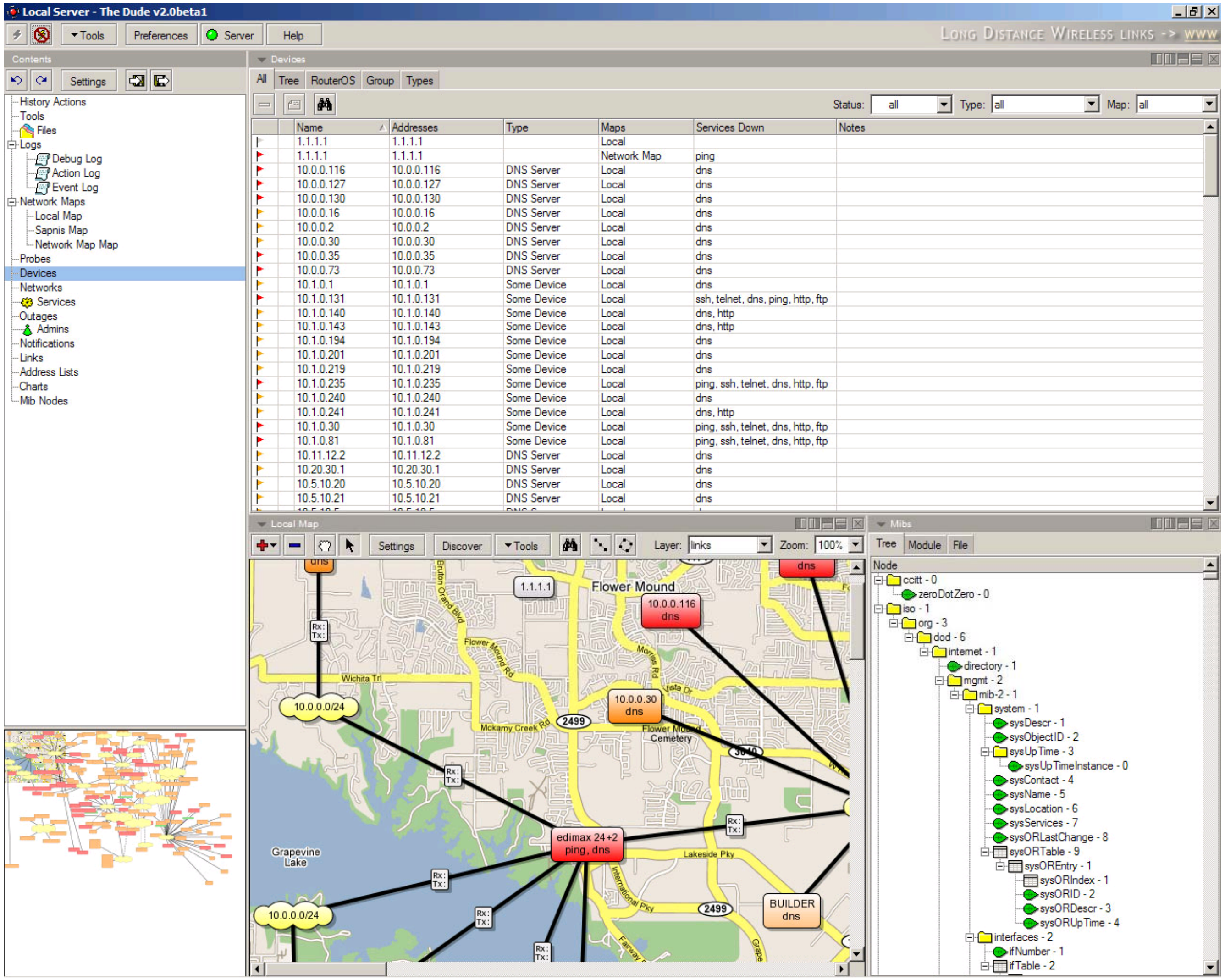
Layer: links

Zoom: 1

Connected

Client: rx 0 bps / tx 0 bps

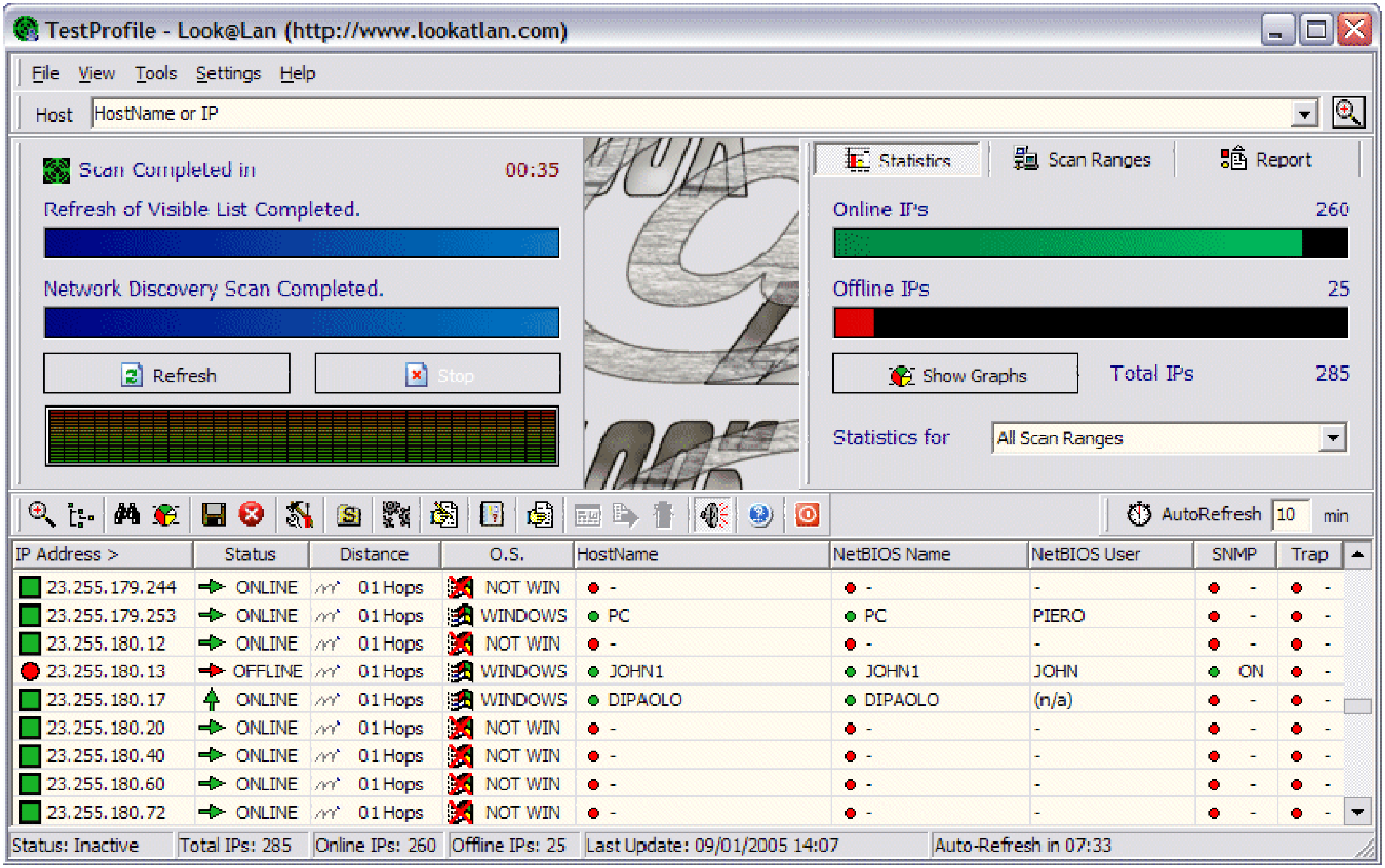
The Dude Sniffer: Screenshot 3



Name	Addresses	Type	Maps	Services Down	Notes
1.1.1.1	1.1.1.1		Local		
1.1.1.1	1.1.1.1		Network Map	ping	
10.0.0.116	10.0.0.116	DNS Server	Local	dns	
10.0.0.127	10.0.0.127	DNS Server	Local	dns	
10.0.0.130	10.0.0.130	DNS Server	Local	dns	
10.0.0.16	10.0.0.16	DNS Server	Local	dns	
10.0.0.2	10.0.0.2	DNS Server	Local	dns	
10.0.0.30	10.0.0.30	DNS Server	Local	dns	
10.0.0.35	10.0.0.35	DNS Server	Local	dns	
10.0.0.73	10.0.0.73	DNS Server	Local	dns	
10.1.0.1	10.1.0.1	Some Device	Local	dns	
10.1.0.131	10.1.0.131	Some Device	Local	ssh, telnet, dns, ping, http, ftp	
10.1.0.140	10.1.0.140	Some Device	Local	dns, http	
10.1.0.143	10.1.0.143	Some Device	Local	dns, http	
10.1.0.194	10.1.0.194	Some Device	Local	dns	
10.1.0.201	10.1.0.201	Some Device	Local	dns	
10.1.0.219	10.1.0.219	Some Device	Local	dns	
10.1.0.235	10.1.0.235	Some Device	Local	ping, ssh, telnet, dns, http, ftp	
10.1.0.240	10.1.0.240	Some Device	Local	dns	
10.1.0.241	10.1.0.241	Some Device	Local	dns, http	
10.1.0.30	10.1.0.30	Some Device	Local	ping, ssh, telnet, dns, http, ftp	
10.1.0.81	10.1.0.81	Some Device	Local	ping, ssh, telnet, dns, http, ftp	
10.11.12.2	10.11.12.2	DNS Server	Local	dns	
10.20.30.1	10.20.30.1	DNS Server	Local	dns	
10.5.10.20	10.5.10.20	DNS Server	Local	dns	
10.5.10.21	10.5.10.21	DNS Server	Local	dns	

EC-Council

Look@LAN



Scan Completed in 00:35

Refresh of Visible List Completed.

Network Discovery Scan Completed.

Online IP's 260

Offline IPs 25

Total IPs 285

Statistics for: All Scan Ranges

IP Address >	Status	Distance	O.S.	HostName	NetBIOS Name	NetBIOS User	SNMP	Trap
23.255.179.244	ONLINE	01 Hops	NOT WIN	● -	● -	-	● -	● -
23.255.179.253	ONLINE	01 Hops	WINDOWS	● PC	● PC	PIERO	● -	● -
23.255.180.12	ONLINE	01 Hops	NOT WIN	● -	● -	-	● -	● -
23.255.180.13	OFFLINE	01 Hops	WINDOWS	● JOHN1	● JOHN1	JOHN	● ON	● -
23.255.180.17	ONLINE	01 Hops	WINDOWS	● DIPAOLO	● DIPAOLO	(n/a)	● -	● -
23.255.180.20	ONLINE	01 Hops	NOT WIN	● -	● -	-	● -	● -
23.255.180.40	ONLINE	01 Hops	NOT WIN	● -	● -	-	● -	● -
23.255.180.60	ONLINE	01 Hops	NOT WIN	● -	● -	-	● -	● -
23.255.180.72	ONLINE	01 Hops	NOT WIN	● -	● -	-	● -	● -

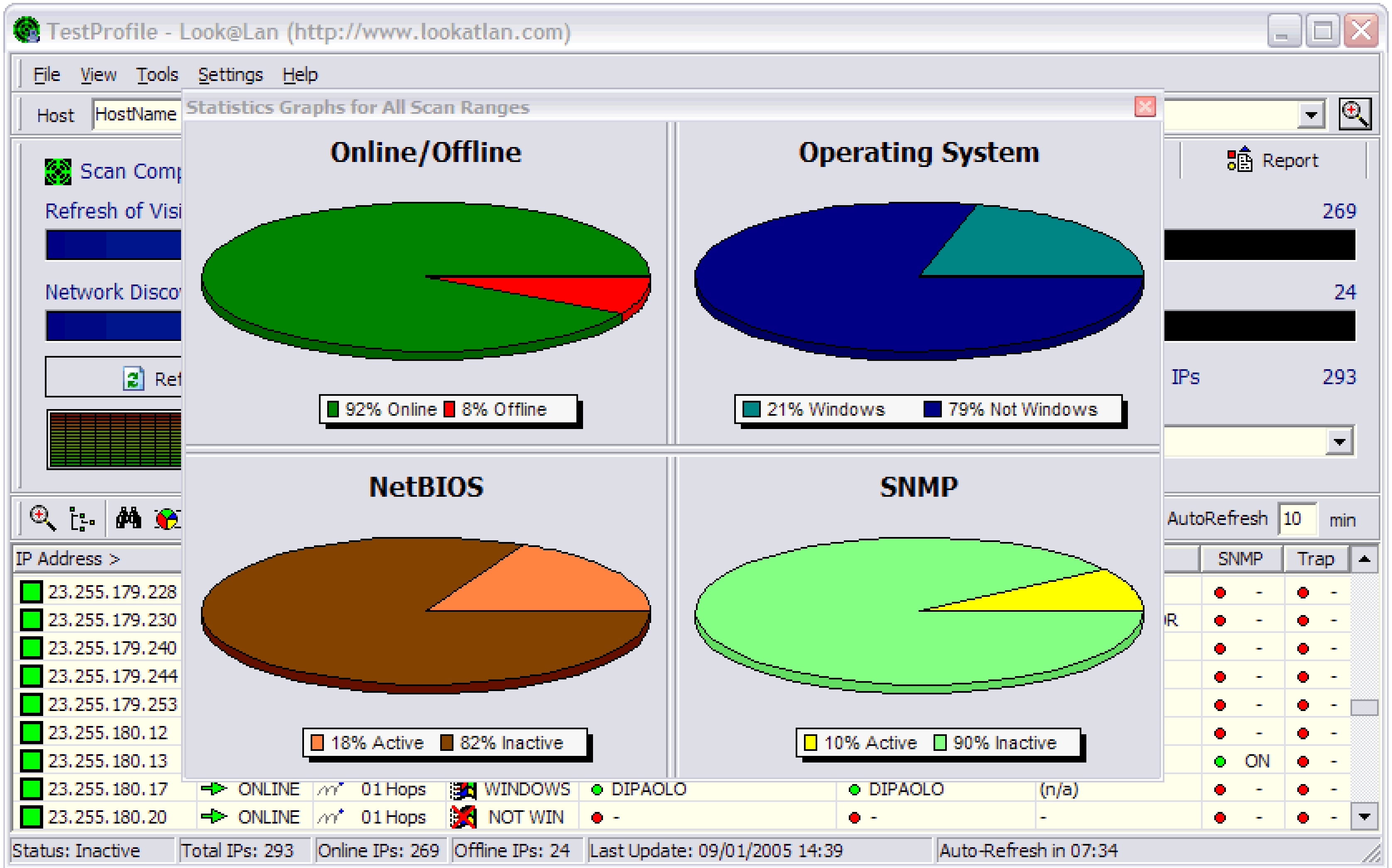
Status: Inactive | Total IPs: 285 | Online IPs: 260 | Offline IPs: 25 | Last Update: 09/01/2005 14:07 | Auto-Refresh in 07:33

EC-Council

Note: This slide is not in your courseware

Certified Ethical Hacker

Look@LAN



IP Address >								SNMP		Trap	
🟩 23.255.179.228								●	-	●	-
🟩 23.255.179.230							R	●	-	●	-
🟩 23.255.179.240								●	-	●	-
🟩 23.255.179.244								●	-	●	-
🟩 23.255.179.253								●	-	●	-
🟩 23.255.180.12								●	-	●	-
🟩 23.255.180.13								●	ON	●	-
🟩 23.255.180.17	ONLINE	01 Hops	WINDOWS	● DIPAOLO		● DIPAOLO	(n/a)	●	-	●	-
🟩 23.255.180.20	ONLINE	01 Hops	NOT WIN	● -		● -	-	●	-	●	-

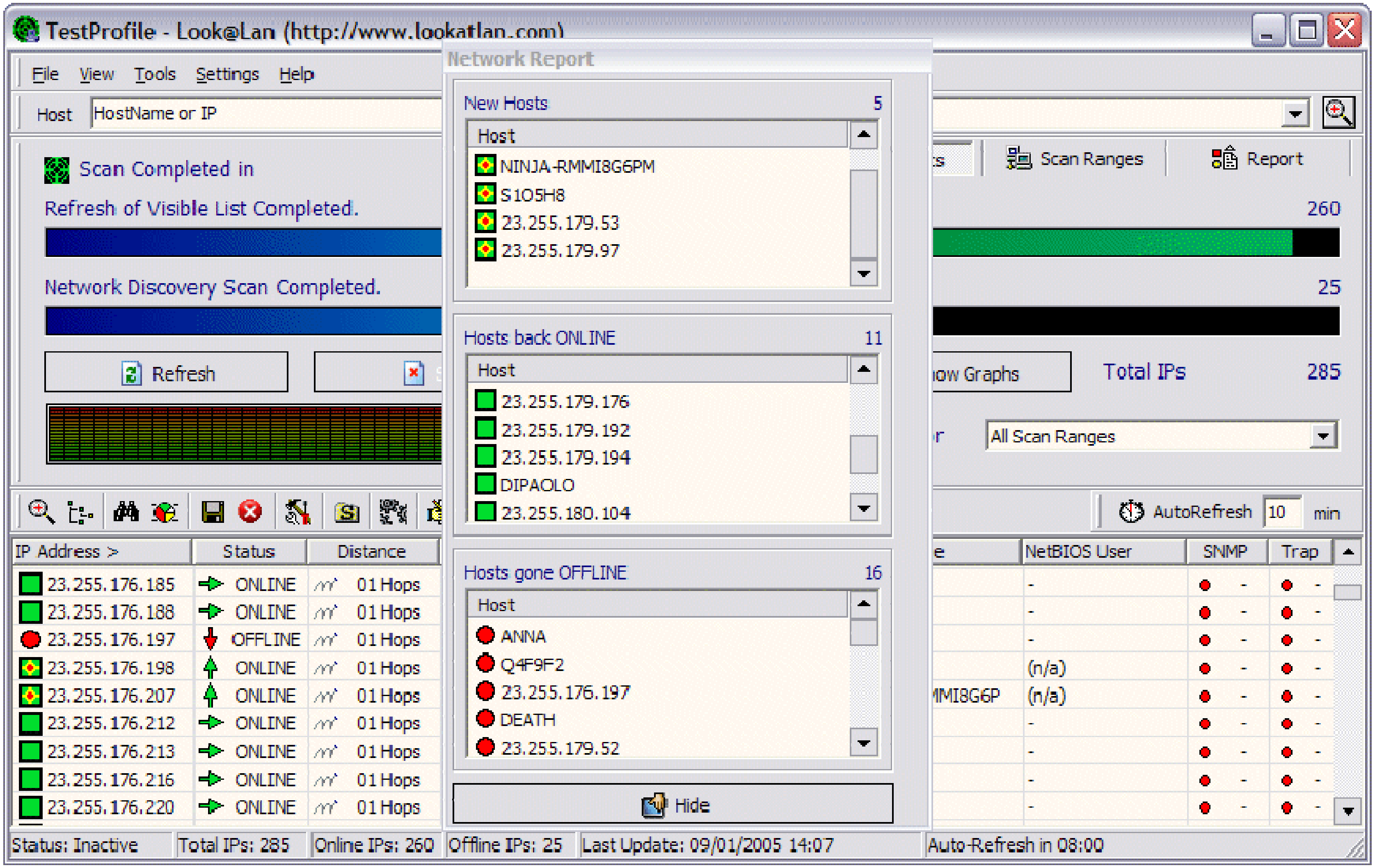
Status: Inactive | Total IPs: 293 | Online IPs: 269 | Offline IPs: 24 | Last Update: 09/01/2005 14:39 | Auto-Refresh in 07:34

EC-Council

Note: This slide is not in your courseware

CEH™ Certified Ethical Hacker

Look@LAN



TestProfile - Look@Lan (http://www.lookatlan.com)

Scan Completed in

Refresh of Visible List Completed. 260

Network Discovery Scan Completed. 25

Total IPs 285

All Scan Ranges

AutoRefresh 10 min

Network Report

New Hosts 5

Host
NINJA-RMMI8G6PM
S105H8
23.255.179.53
23.255.179.97

Hosts back ONLINE 11

Host
🟩 23.255.179.176
🟩 23.255.179.192
🟩 23.255.179.194
🟩 DIPAOLO
🟩 23.255.180.104

Hosts gone OFFLINE 16

Host
● ANNA
● Q4F9F2
● 23.255.176.197
● DEATH
● 23.255.179.52

IP Address >	Status	Distance	e	NetBIOS User	SNMP	Trap
🟩 23.255.176.185	ONLINE	01 Hops		-	● -	● -
🟩 23.255.176.188	ONLINE	01 Hops		-	● -	● -
● 23.255.176.197	OFFLINE	01 Hops		-	● -	● -
23.255.176.198	ONLINE	01 Hops		(n/a)	● -	● -
23.255.176.207	ONLINE	01 Hops	MMI8G6P	(n/a)	● -	● -
🟩 23.255.176.212	ONLINE	01 Hops		-	● -	● -
🟩 23.255.176.213	ONLINE	01 Hops		-	● -	● -
🟩 23.255.176.216	ONLINE	01 Hops		-	● -	● -
🟩 23.255.176.220	ONLINE	01 Hops		-	● -	● -

Status: Inactive | Total IPs: 285 | Online IPs: 260 | Offline IPs: 25 | Last Update: 09/01/2005 14:07 | Auto-Refresh in 08:00

EC-Council

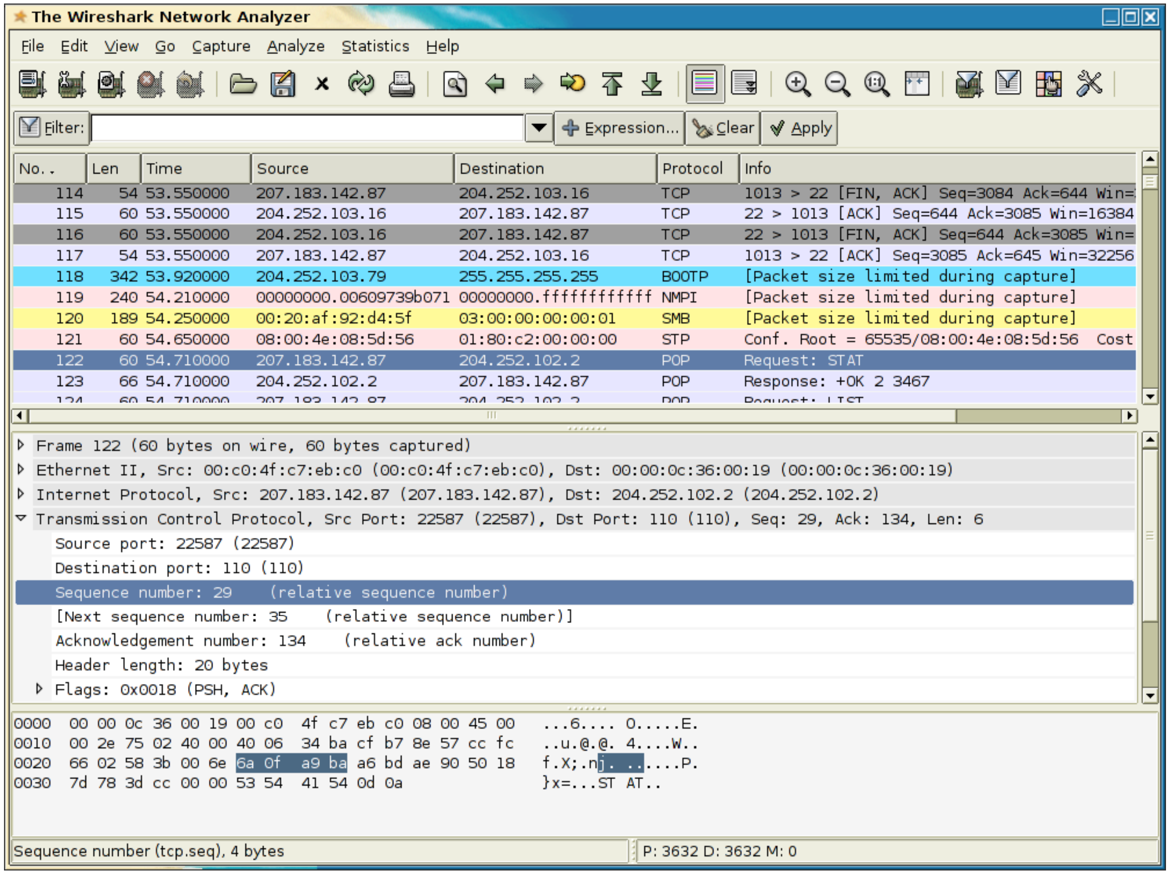
Note: This slide is not in your courseware

Wireshark

Wireshark is a network protocol analyzer for UNIX and Windows

It allows user to examine data from a live network or from a capture file on a disk

User can interactively browse captured data, viewing summary, and detailed information for each packet captured


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply

No. .	Len	Time	Source	Destination	Protocol	Info
114	54	53.550000	207.183.142.87	204.252.103.16	TCP	1013 > 22 [FIN, ACK] Seq=3084 Ack=644 Win=
115	60	53.550000	204.252.103.16	207.183.142.87	TCP	22 > 1013 [ACK] Seq=644 Ack=3085 Win=16384
116	60	53.550000	204.252.103.16	207.183.142.87	TCP	22 > 1013 [FIN, ACK] Seq=644 Ack=3085 Win=
117	54	53.550000	207.183.142.87	204.252.103.16	TCP	1013 > 22 [ACK] Seq=3085 Ack=645 Win=32256
118	342	53.920000	204.252.103.79	255.255.255.255	BOOTP	[Packet size limited during capture]
119	240	54.210000	00000000.00609739b071	00000000.ffffffffffff	NMPI	[Packet size limited during capture]
120	189	54.250000	00:20:af:92:d4:5f	03:00:00:00:00:01	SMB	[Packet size limited during capture]
121	60	54.650000	08:00:4e:08:5d:56	01:80:c2:00:00:00	STP	Conf. Root = 65535/08:00:4e:08:5d:56 Cost
122	60	54.710000	207.183.142.87	204.252.102.2	POP	Request: STAT
123	66	54.710000	204.252.102.2	207.183.142.87	POP	Response: +OK 2 3467
124	60	54.710000	207.183.142.87	204.252.102.2	POP	Request: LIST

```
▷ Frame 122 (60 bytes on wire, 60 bytes captured)
▷ Ethernet II, Src: 00:c0:4f:c7:eb:c0 (00:c0:4f:c7:eb:c0), Dst: 00:00:0c:36:00:19 (00:00:0c:36:00:19)
▷ Internet Protocol, Src: 207.183.142.87 (207.183.142.87), Dst: 204.252.102.2 (204.252.102.2)
▽ Transmission Control Protocol, Src Port: 22587 (22587), Dst Port: 110 (110), Seq: 29, Ack: 134, Len: 6
    Source port: 22587 (22587)
    Destination port: 110 (110)
    Sequence number: 29    (relative sequence number)
    [Next sequence number: 35    (relative sequence number)]
    Acknowledgement number: 134    (relative ack number)
    Header length: 20 bytes
  ▷ Flags: 0x0018 (PSH, ACK)
```

```
0000  00 00 0c 36 00 19 00 c0  4f c7 eb c0 08 00 45 00   ...6.... O.....E.
0010  00 2e 75 02 40 00 40 06  34 ba cf b7 8e 57 cc fc   ..u.@.@. 4....W..
0020  66 02 58 3b 00 6e 6a 0f  a9 ba a6 bd ae 90 50 18   f.X;.nj. ......P.
0030  7d 78 3d cc 00 00 53 54  41 54 0d 0a               }x=...ST AT..
```

Sequence number (tcp.seq), 4 bytes | P: 3632 D: 3632 M: 0

Display Filters in Wireshark

Display filters are used to change the view of packets in captured files

Display Filtering by Protocol

- Example: Type the protocol in the filter box
- arp, http, tcp, udp, dns

Filtering by IP Address

•ip.addr == 10.0.0.4

Filtering by multiple IP Addresses

•ip.addr == 10.0.0.4 or ip.addr == 10.0.0.5

Monitoring Specific Ports

•tcp.port==443

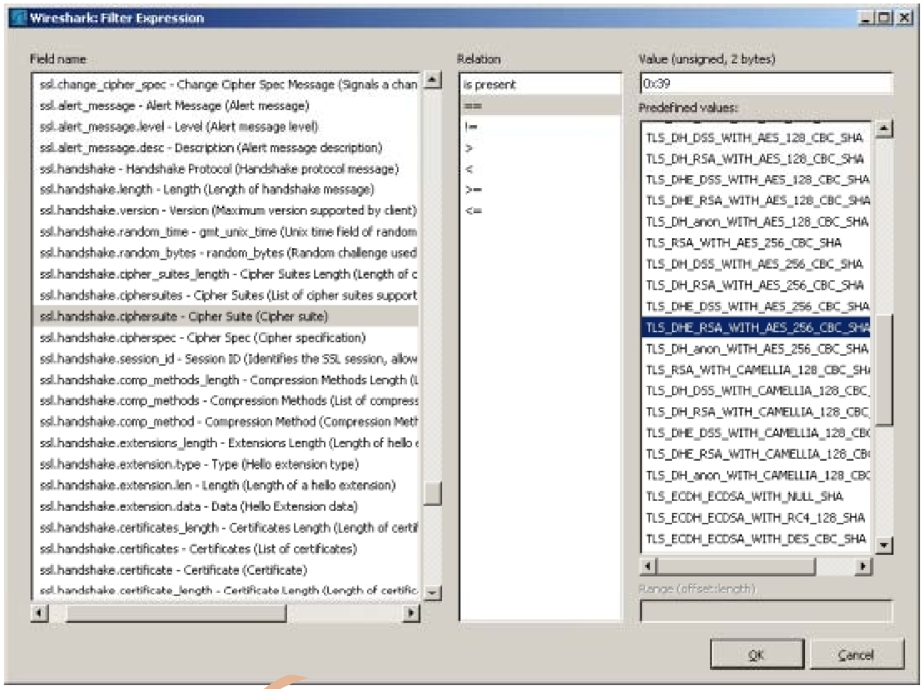
•ip.addr==192.168.1.100 machine
ip.addr==192.168.1.100 && tcp.port=443

Other Filters

•ip.dst == 10.0.1.50 && frame.pkt_len > 400

•ip.addr == 10.0.1.12 && icmp && frame.number > 15
&& frame.number < 30

•ip.src==205.153.63.30 or ip.dst==205.153.63.30



Field name

ssl.change_cipher_spec - Change Cipher Spec Message (Signals a chan
ssl.alert_message - Alert Message (Alert message)
ssl.alert_message.level - Level (Alert message level)
ssl.alert_message.desc - Description (Alert message description)
ssl.handshake - Handshake Protocol (Handshake protocol message)
ssl.handshake.length - Length (Length of handshake message)
ssl.handshake.version - Version (Maximum version supported by client)
ssl.handshake.random_time - gmt_unix_time (Unix time field of random
ssl.handshake.random_bytes - random_bytes (Random challenge used
ssl.handshake.cipher_suites_length - Cipher Suites Length (Length of c
ssl.handshake.ciphersuites - Cipher Suites (List of cipher suites support
ssl.handshake.ciphersuite - Cipher Suite (Cipher suite)
ssl.handshake.cipherspec - Cipher Spec (Cipher specification)
ssl.handshake.session_id - Session ID (Identifies the SSL session, allow
ssl.handshake.comp_methods_length - Compression Methods Length (L
ssl.handshake.comp_methods - Compression Methods (List of compress
ssl.handshake.comp_method - Compression Method (Compression Meth
ssl.handshake.extensions_length - Extensions Length (Length of hello e
ssl.handshake.extension.type - Type (Hello extension type)
ssl.handshake.extension.len - Length (Length of a hello extension)
ssl.handshake.extension.data - Data (Hello Extension data)
ssl.handshake.certificates_length - Certificates Length (Length of certi
ssl.handshake.certificates - Certificates (List of certificates)
ssl.handshake.certificate - Certificate (Certificate)
ssl.handshake.certificate_length - Certificate Length (Length of certific

Relation

is present
==
!=
>
<
>=
<=

Value (unsigned, 2 bytes)

0x39

Predefined values:

TLS_DH_DSS_WITH_AES_128_CBC_SHA
TLS_DH_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DH_DSS_WITH_AES_256_CBC_SHA
TLS_DH_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SH
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_
TLS_DHE_DSS_WITH_CAMELLIA_128_CB
TLS_DHE_RSA_WITH_CAMELLIA_128_CB
TLS_DH_anon_WITH_CAMELLIA_128_CBC
TLS_ECDH_ECDSA_WITH_NULL_SHA
TLS_ECDH_ECDSA_WITH_RC4_128_SHA
TLS_ECDH_ECDSA_WITH_DES_CBC_SHA

Range (offset:length)

Following the TCP Stream in Wireshark

Wireshark reassembles all packets in a TCP conversation and displays ASCII in an easy-to-read format

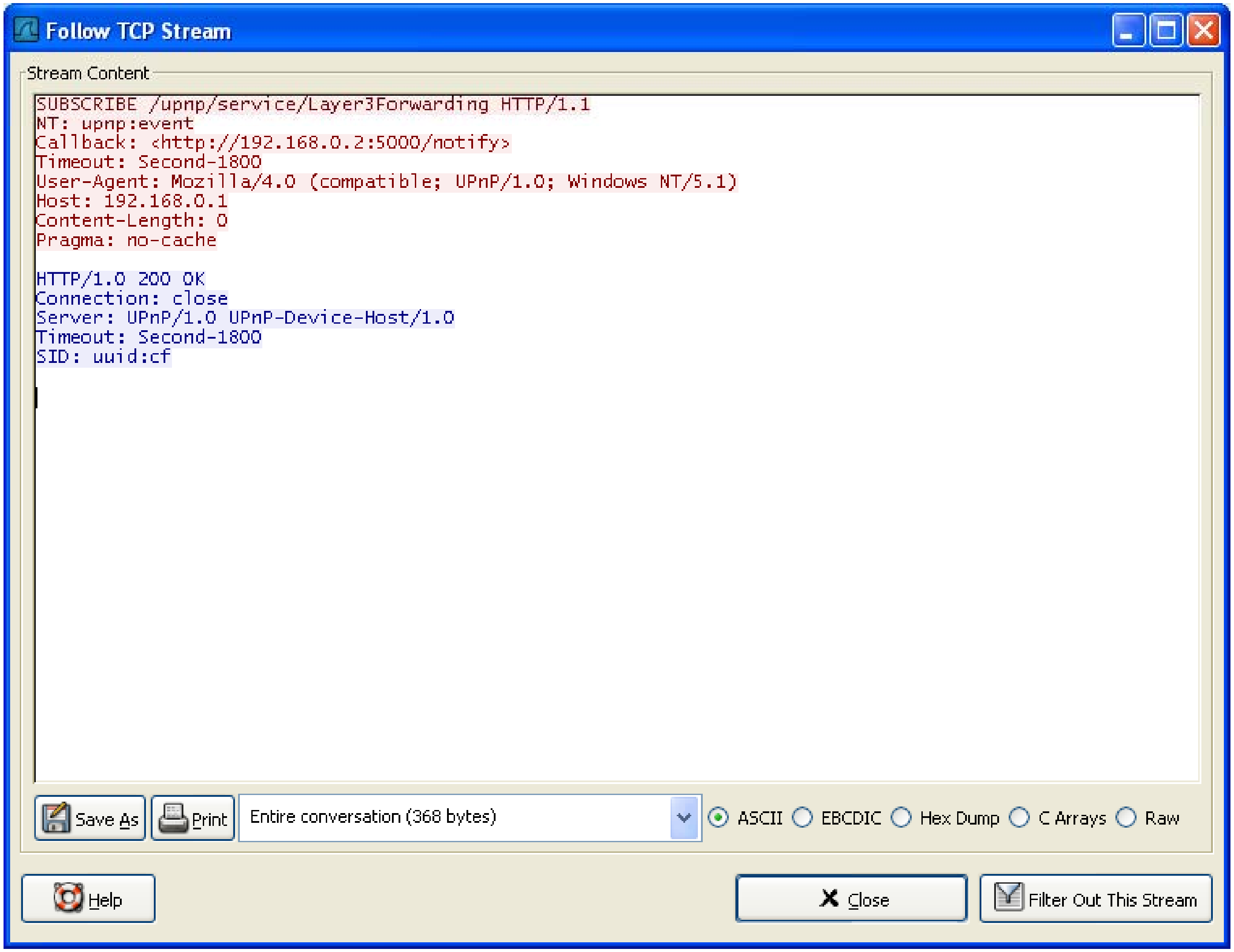
This makes it easy to pick out usernames and passwords from the insecure protocols such as Telnet and FTP

Example: Follow the stream of HTTP session and save the output to a file.

Command: Selecting a TCP packet in Summary Window and then selecting **`Analyze -> Follow TCP Stream`** from menu bar will display “Follow TCP Stream window”

You can also right-click on a TCP packet in Summary Window and choose “Follow TCP Stream” to display window

Following the TCP Stream in Wireshark (cont'd)



Follow TCP Stream
Stream Content
Save As
Print
Entire conversation (368 bytes)
● ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ○ Raw
Help
Close
Filter Out This Stream

```
SUBSCRIBE /upnp/service/Layer3Forwarding HTTP/1.1
NT: upnp:event
Callback: <http://192.168.0.2:5000/notify>
Timeout: Second-1800
User-Agent: Mozilla/4.0 (compatible; UPnP/1.0; Windows NT/5.1)
Host: 192.168.0.1
Content-Length: 0
Pragma: no-cache

HTTP/1.0 200 OK
Connection: close
Server: UPnP/1.0 UPnP-Device-Host/1.0
Timeout: Second-1800
SID: uuid:cf
```

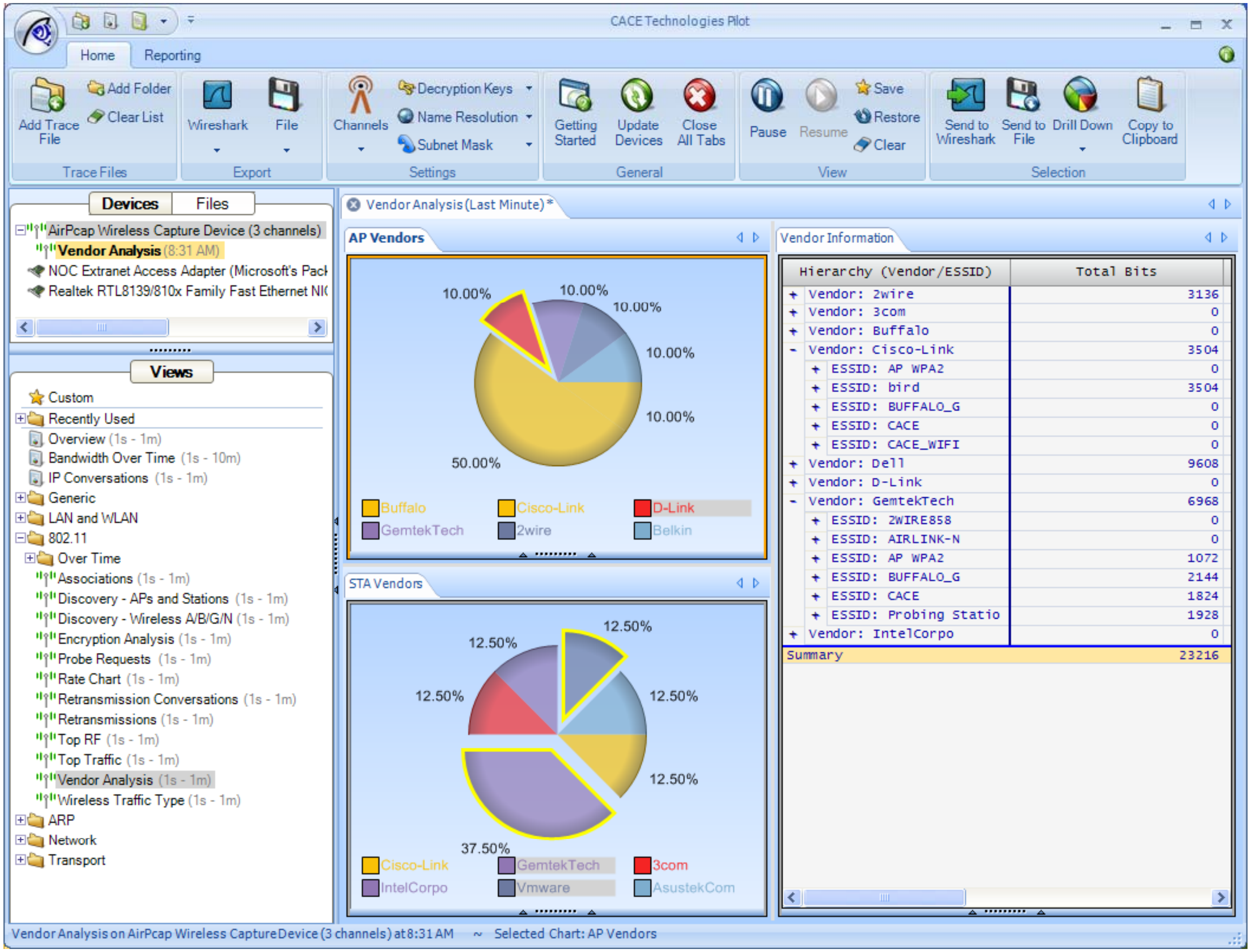
Pilot

Pilot is a powerful network analysis tool with an accessible and visually-oriented user interface designed to increase your troubleshooting effectiveness

Benefits:

- Integrated with Wireshark
- Powerful Network Analysis Engine
- Pilot Views: Flexible Analysis and Visualization Paradigm
- Pilot Charts: Innovative Visualization Components
- Drill-Down: An Innovative Analysis Paradigm
- Unparalleled Wireless Support with AirPcap
- Superior Reporting Capabilities

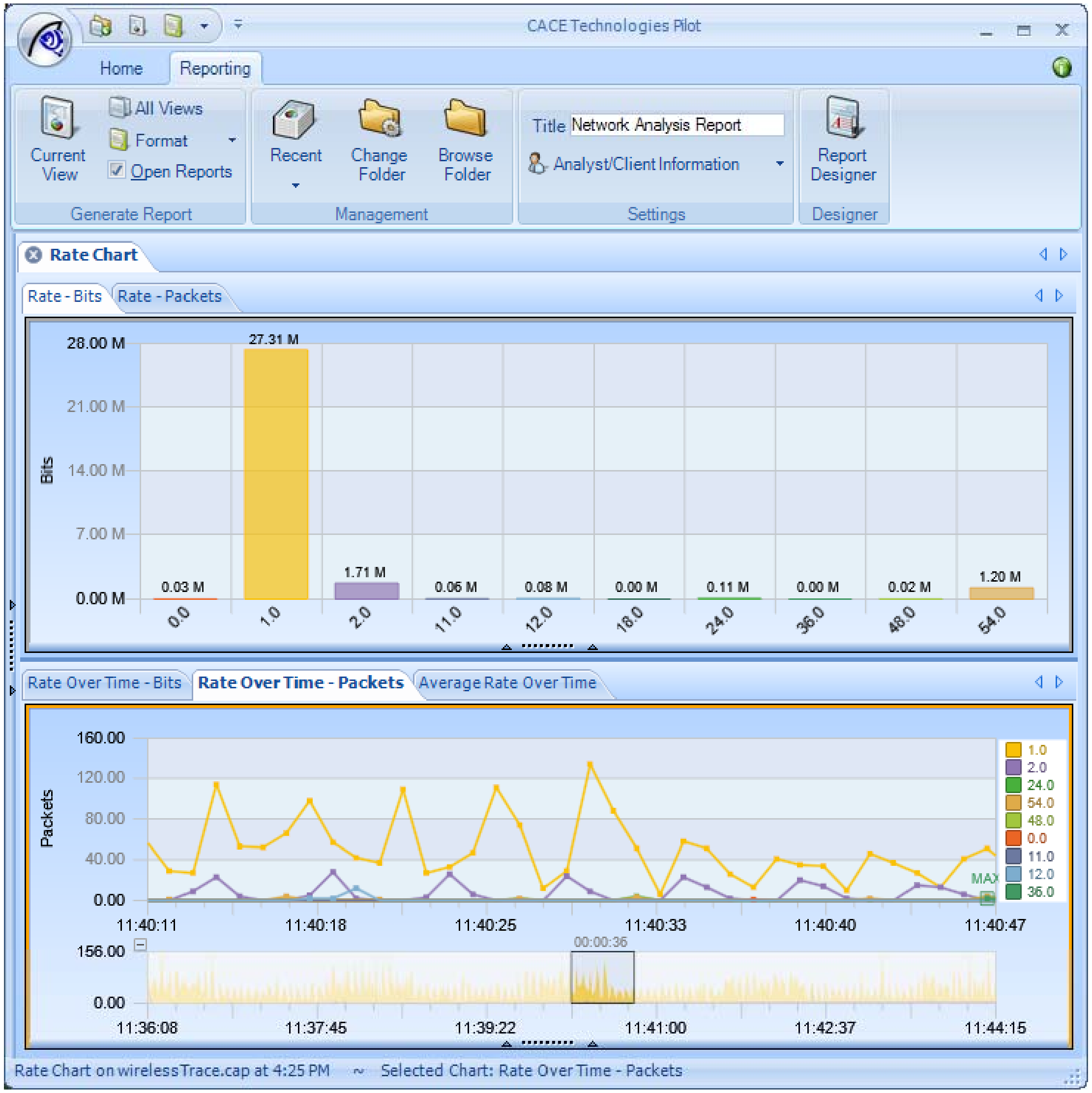
Pilot: Screenshot 1



Hierarchy (Vendor/ESSID)	Total Bits
+ Vendor: 2wire	3136
+ Vendor: 3com	0
+ Vendor: Buffalo	0
- Vendor: Cisco-Link	3504
+ ESSID: AP WPA2	0
+ ESSID: bird	3504
+ ESSID: BUFFALO_G	0
+ ESSID: CACE	0
+ ESSID: CACE_WIFI	0
+ Vendor: Dell	9608
+ Vendor: D-Link	0
- Vendor: GemtekTech	6968
+ ESSID: 2WIRE858	0
+ ESSID: AIRLINK-N	0
+ ESSID: AP WPA2	1072
+ ESSID: BUFFALO_G	2144
+ ESSID: CACE	1824
+ ESSID: Probing Statio	1928
+ Vendor: IntelCorpo	0
Summary	23216

Vendor Analysis on AirPcap Wireless Capture Device (3 channels) at 8:31 AM ~ Selected Chart: AP Vendors

Pilot: Screenshot 2

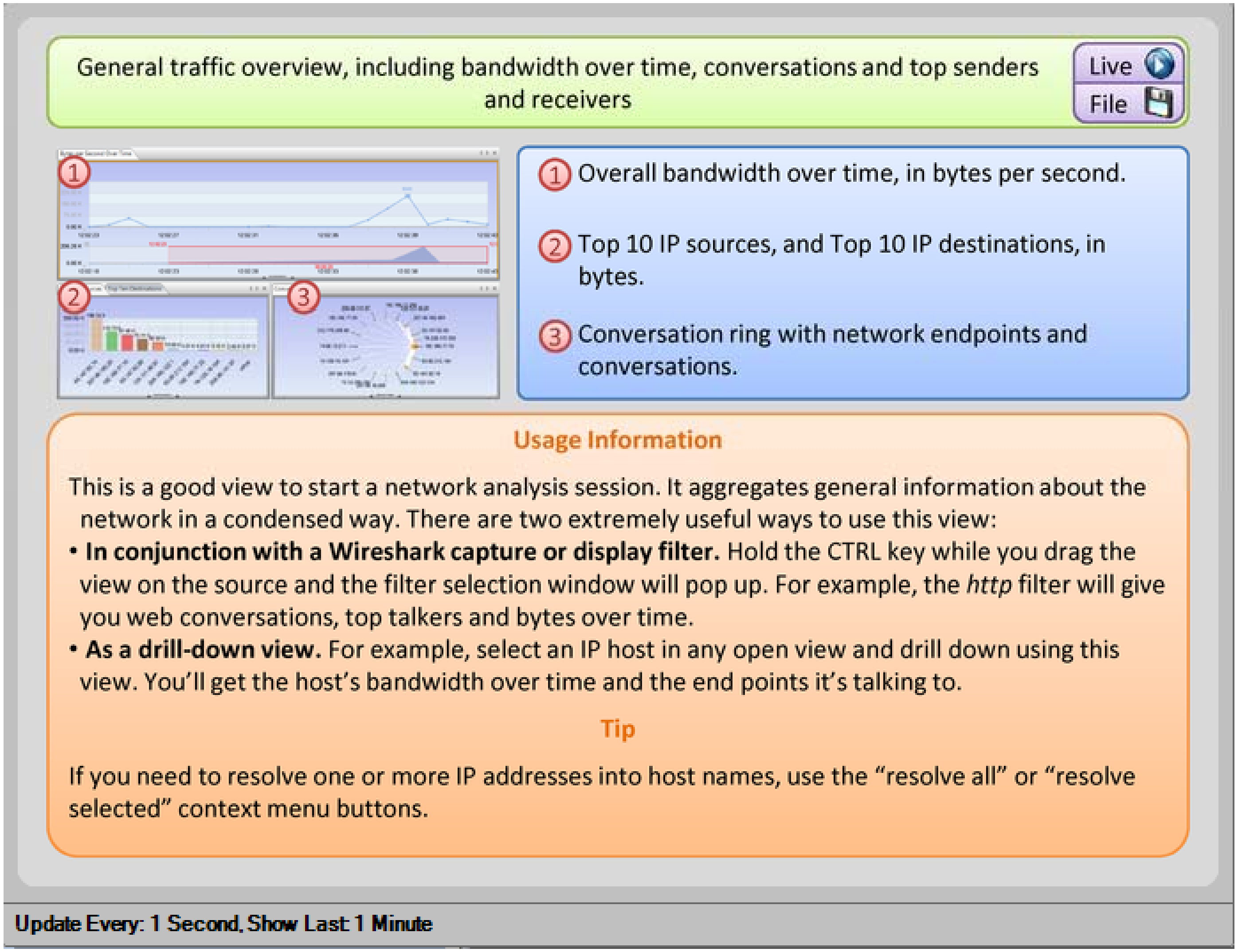


Title: Network Analysis Report

Rate Chart on wirelessTrace.cap at 4:25 PM ~ Selected Chart: Rate Over Time - Packets

EC-Council

Pilot: Screenshot 3



General traffic overview, including bandwidth over time, conversations and top senders and receivers

(1) Overall bandwidth over time, in bytes per second.

(2) Top 10 IP sources, and Top 10 IP destinations, in bytes.

(3) Conversation ring with network endpoints and conversations.

Usage Information

This is a good view to start a network analysis session. It aggregates general information about the network in a condensed way. There are two extremely useful ways to use this view:

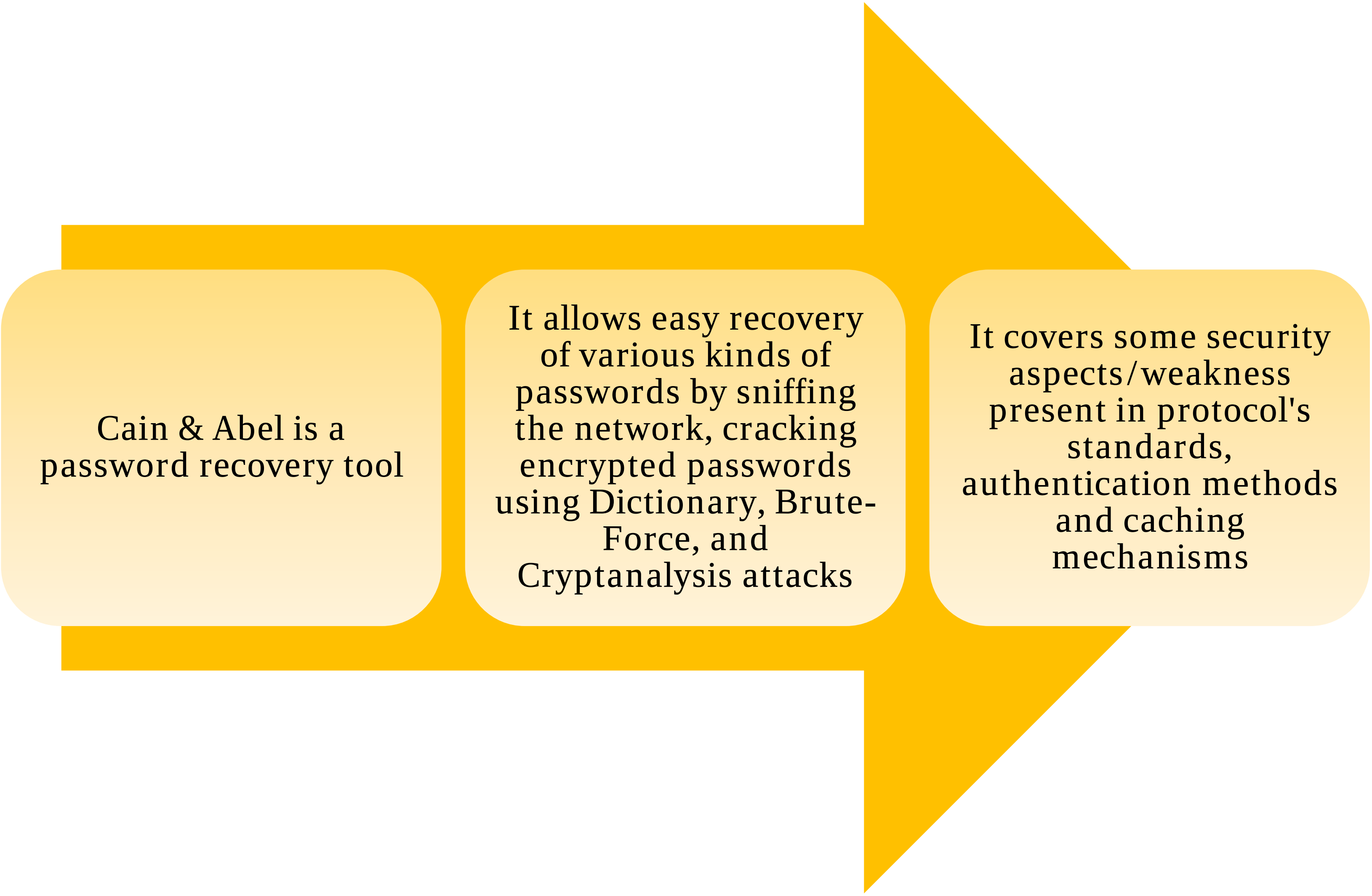
- **In conjunction with a Wireshark capture or display filter.** Hold the CTRL key while you drag the view on the source and the filter selection window will pop up. For example, the *http* filter will give you web conversations, top talkers and bytes over time.
- **As a drill-down view.** For example, select an IP host in any open view and drill down using this view. You'll get the host's bandwidth over time and the end points it's talking to.

Tip

If you need to resolve one or more IP addresses into host names, use the "resolve all" or "resolve selected" context menu buttons.

Update Every: 1 Second, Show Last: 1 Minute

Cain and Abel



Cain & Abel is a password recovery tool

It allows easy recovery of various kinds of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force, and Cryptanalysis attacks

It covers some security aspects/weakness present in protocol's standards, authentication methods and caching mechanisms

Cain and Abel (cont'd)

MSCACHE hashes Dumper

MSCACHE hashes dictionary and brute-force crackers

Sniffer filter for SIP-MD5 authentications

SIP-MD5 Hashes Dictionary and Brute-Force Crackers

Off-line capture file processing compatible with winpcap, tcpdump, and Wireshark format

Cain's sniffer can extract audio conversations based on SIP/RTP protocols and save them into WAV files

Cain and Abel: Features

Remote Registry Editor

SIREN codec support in VoIP sniffer

Supports new AES-128bit Keyfobs in RSA SecurID Token Calculator

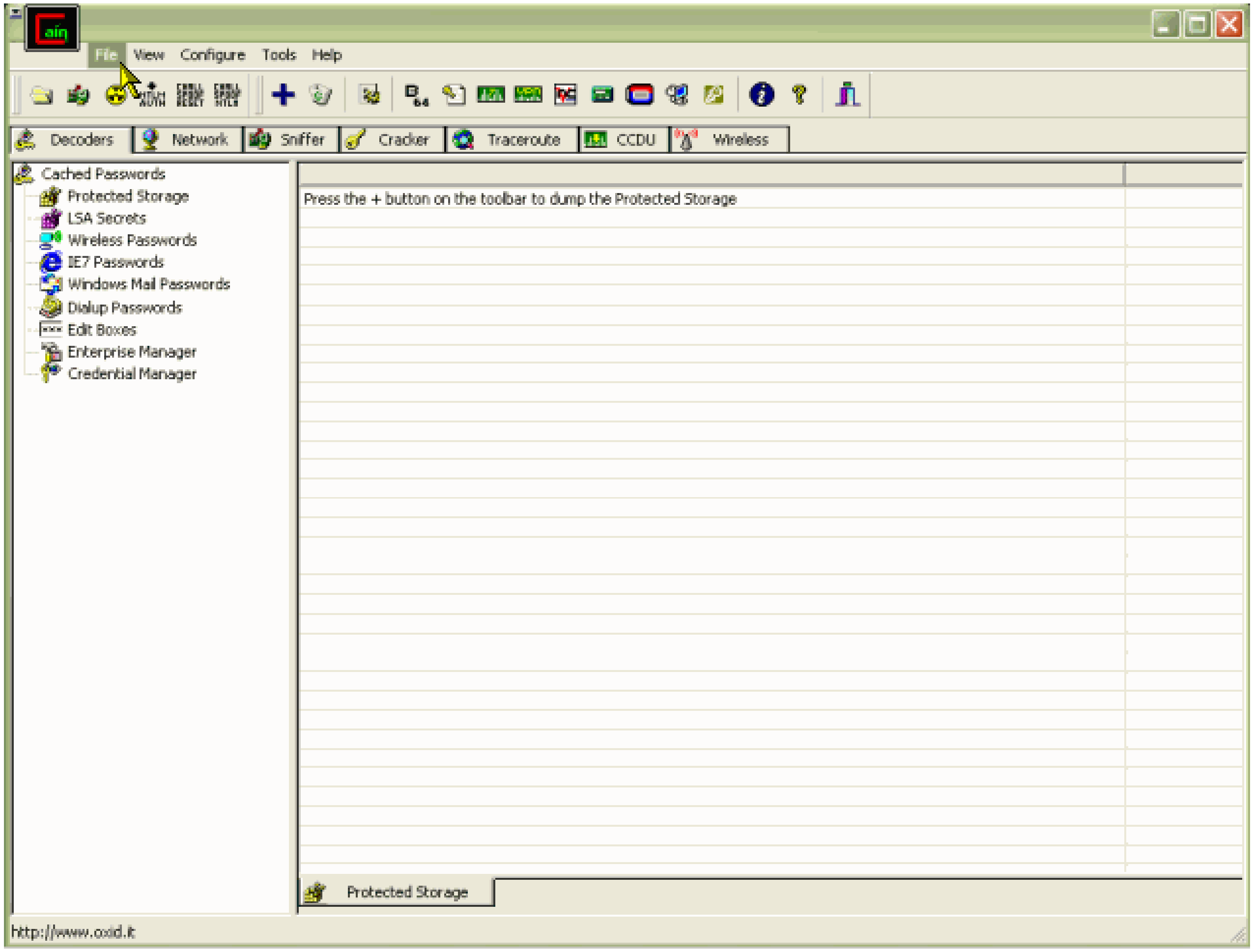
Microsoft SQL Server 2005 Password Extractor via ODBC

Fixed a bug in Internet Explorer 7 AutoComplete password decoder

Default HTTP users and passwords fields update

Automatic recognition of AirPcap TX capability based on channels

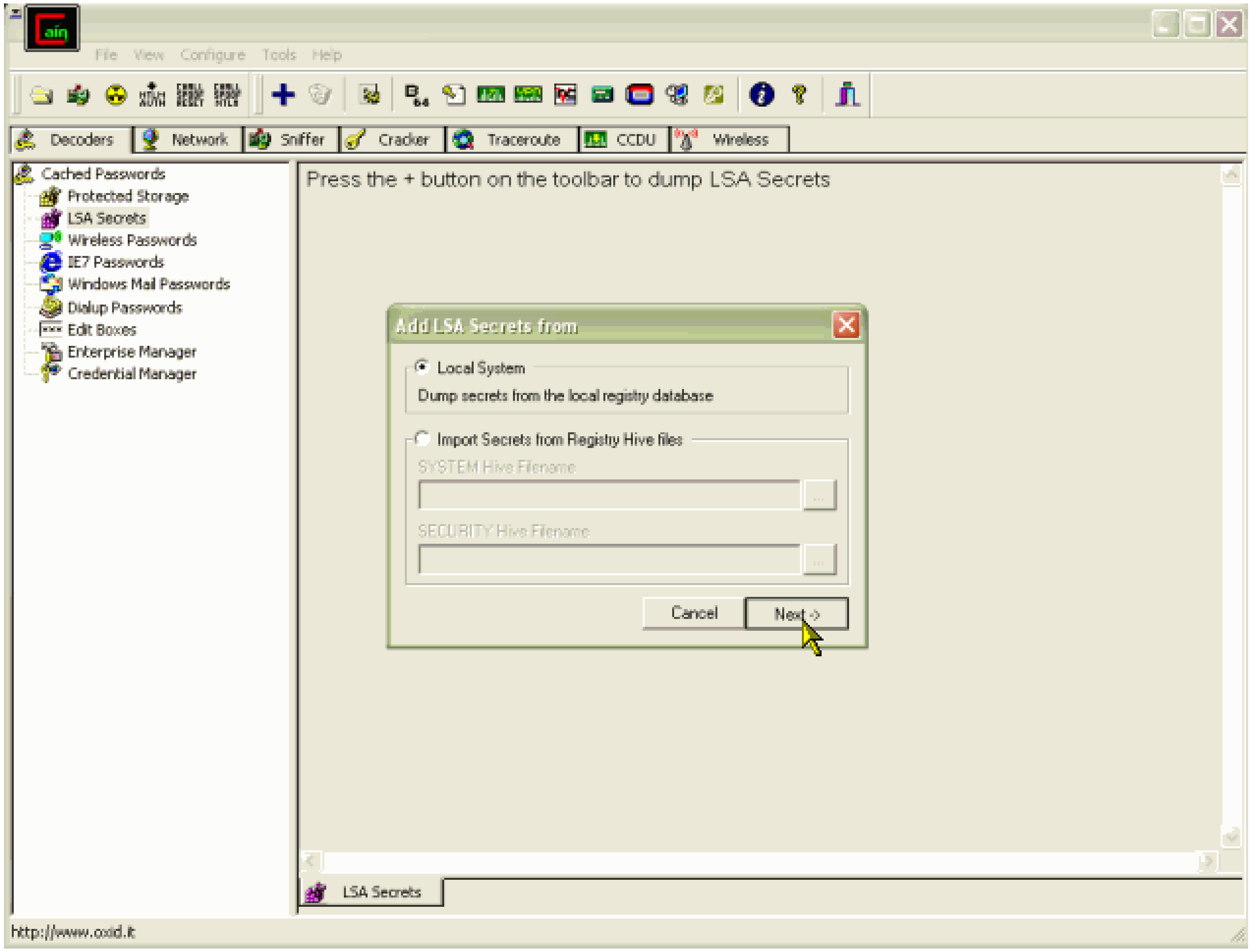
Cain and Abel: Screenshot 1



Press the + button on the toolbar to dump the Protected Storage

EC-Council

Cain and Abel: Screenshot 2



Press the + button on the toolbar to dump LSA Secrets

Add LSA Secrets from

● Local System

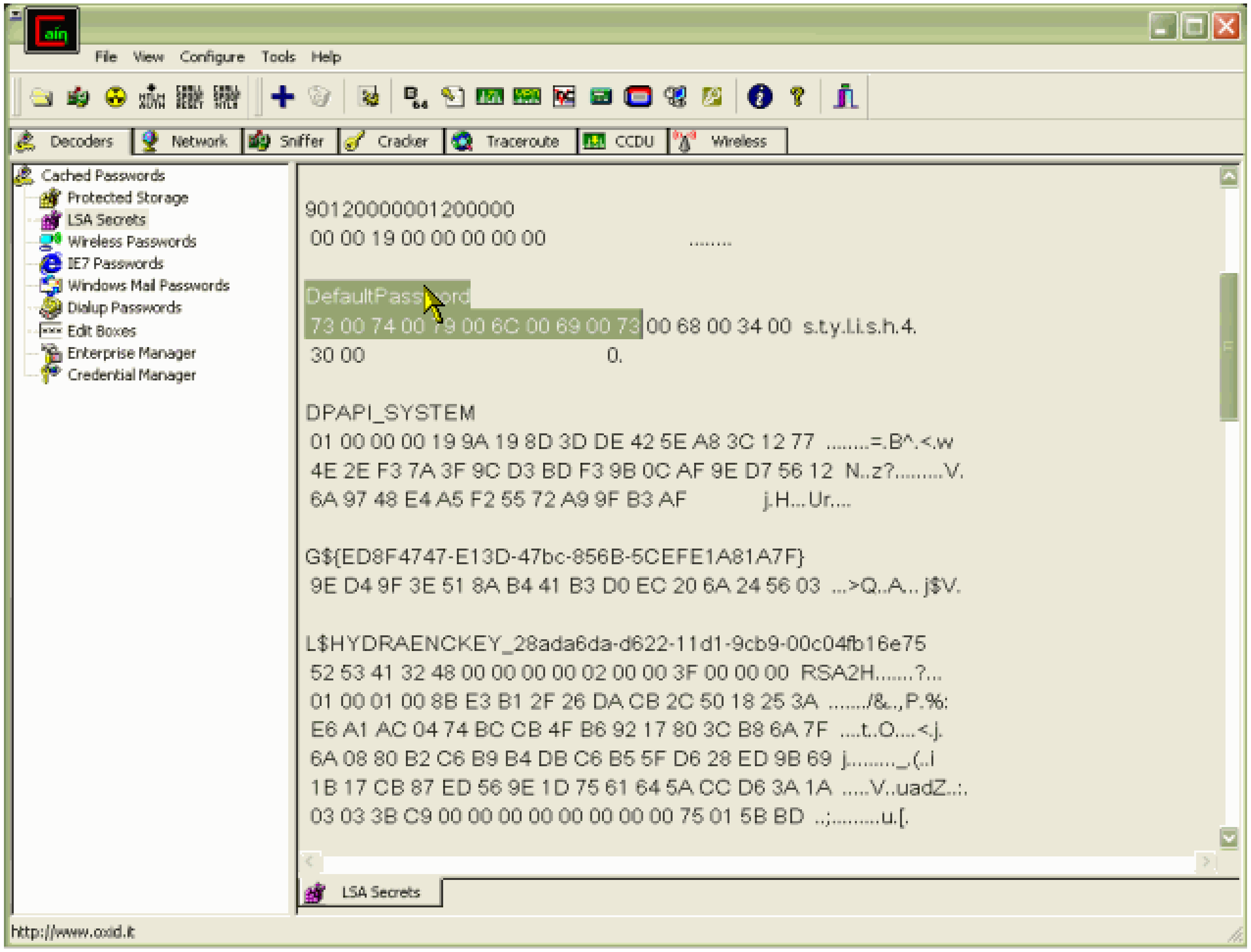
Dump secrets from the local registry database

○ Import Secrets from Registry Hive files

SYSTEM Hive Filename

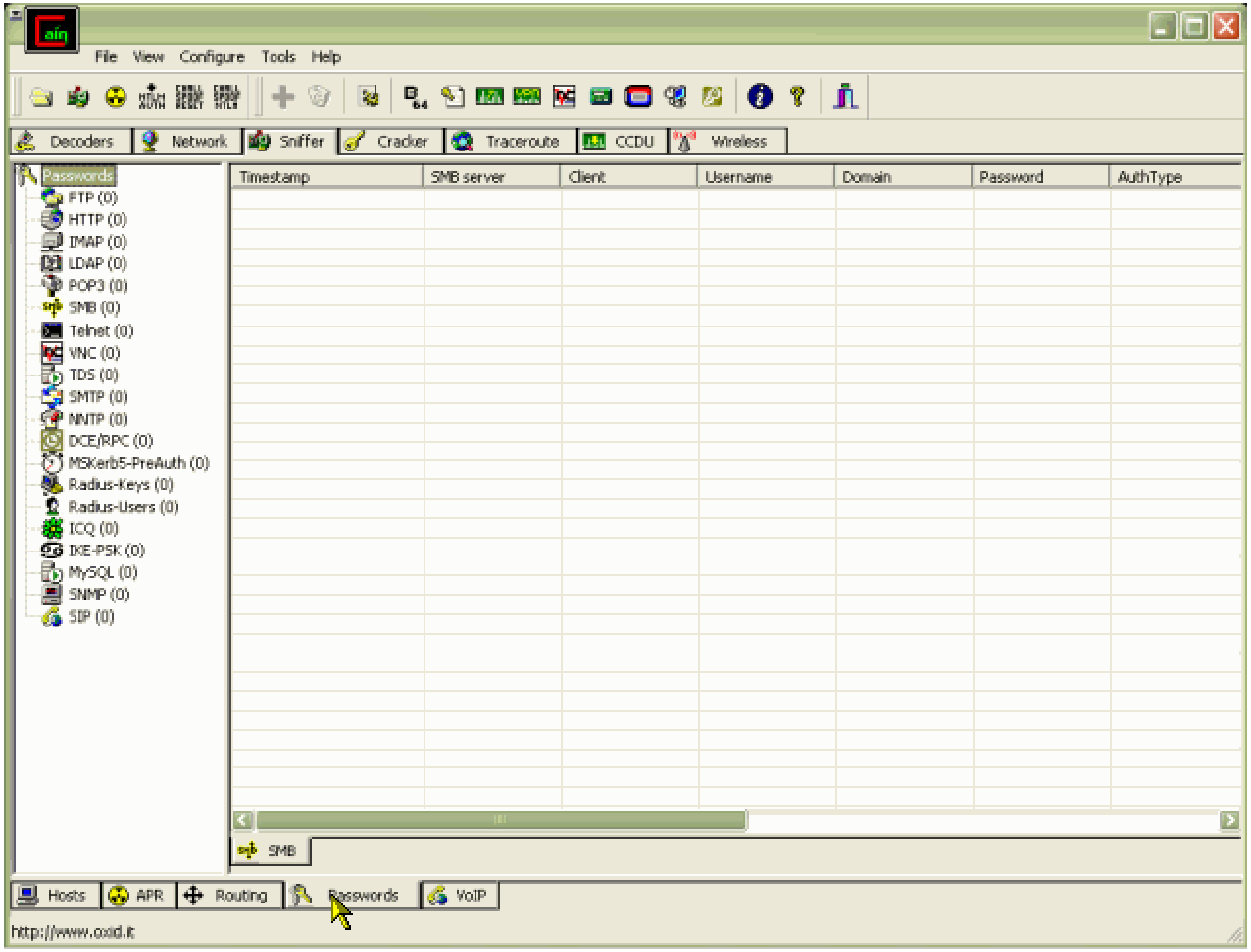
SECURITY Hive Filename

Cain and Abel: Screenshot 3



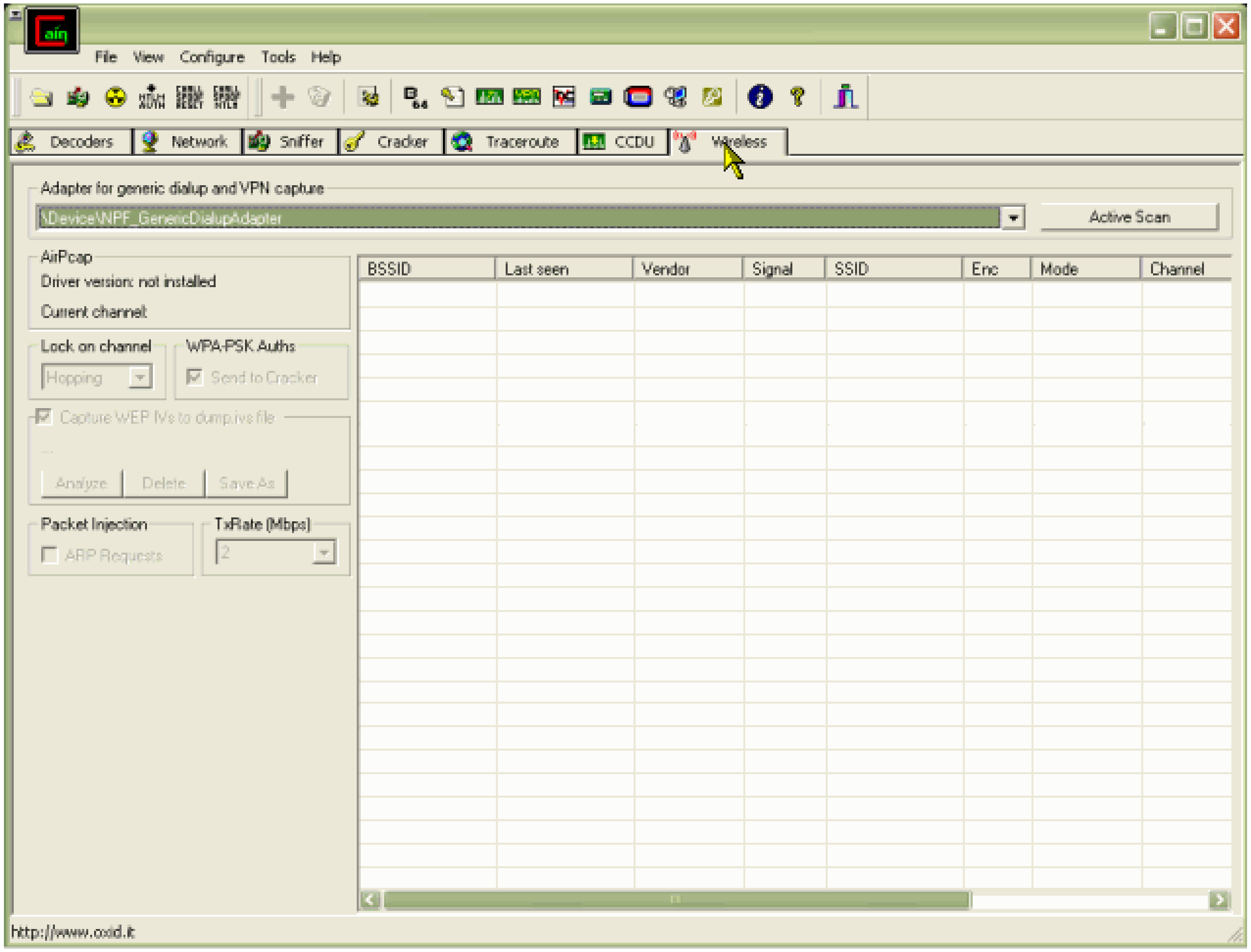
```
90120000001200000
 00 00 19 00 00 00 00 00                    ........

DefaultPassword
 73 00 74 00 79 00 6C 00 69 00 73 00 68 00 34 00  s.t.y.l.i.s.h.4.
 30 00                                            0.

DPAPI_SYSTEM
 01 00 00 00 19 9A 19 8D 3D DE 42 5E A8 3C 12 77  ........=.B^.<.w
 4E 2E F3 7A 3F 9C D3 BD F3 9B 0C AF 9E D7 56 12  N..z?.........V.
 6A 97 48 E4 A5 F2 55 72 A9 9F B3 AF              j.H...Ur....

G${ED8F4747-E13D-47bc-856B-5CEFE1A81A7F}
 9E D4 9F 3E 51 8A B4 41 B3 D0 EC 20 6A 24 56 03  ...>Q..A... j$V.

L$HYDRAENCKEY_28ada6da-d622-11d1-9cb9-00c04fb16e75
 52 53 41 32 48 00 00 00 00 02 00 00 3F 00 00 00  RSA2H.......?...
 01 00 01 00 8B E3 B1 2F 26 DA CB 2C 50 18 25 3A  ......./&..,P.%:
 E6 A1 AC 04 74 BC CB 4F B6 92 17 80 3C B8 6A 7F  ....t..O....<.j.
 6A 08 80 B2 C6 B9 B4 DB C6 B5 5F D6 28 ED 9B 69  j.........._.(..i
 1B 17 CB 87 ED 56 9E 1D 75 61 64 5A CC D6 3A 1A  .....V..uadZ..:.
 03 03 3B C9 00 00 00 00 00 00 00 00 75 01 5B BD  ..;.........u.[.
```

Cain and Abel: Screenshot 4



Timestamp	SMB server	Client	Username	Domain	Password	AuthType

Cain and Abel: Screenshot 5



Adapter for generic dialup and VPN capture: \Device\NPF_GenericDialupAdapter

AirPcap
Driver version: not installed
Current channel:

Lock on channel: Hopping

WPA-PSK Auths: ☑ Send to Cracker

☑ Capture WEP IVs to dump.ivs file

Packet Injection: □ ARP Requests

TxRate (Mbps): 2

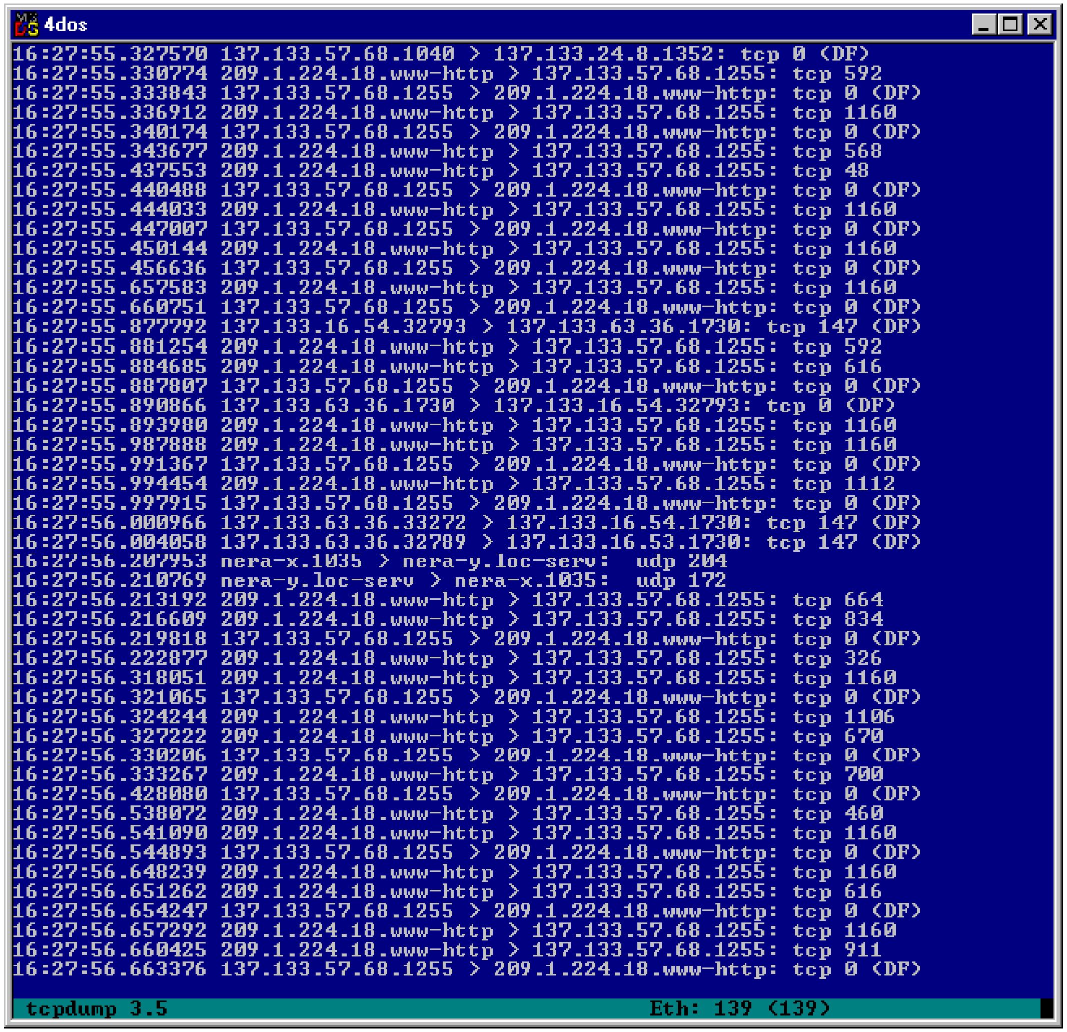
BSSID	Last seen	Vendor	Signal	SSID	Enc	Mode	Channel

http://www.oxid.it

Tcpdump

Tcpdump is a common computer network debugging tool that runs under command line

It allows user to intercept and display TCP/IP and other packets being transmitted or received over a network to which the computer is attached



```
16:27:55.327570 137.133.57.68.1040 > 137.133.24.8.1352: tcp 0 (DF)
16:27:55.330774 209.1.224.18.www-http > 137.133.57.68.1255: tcp 592
16:27:55.333843 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:55.336912 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1160
16:27:55.340174 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:55.343677 209.1.224.18.www-http > 137.133.57.68.1255: tcp 568
16:27:55.437553 209.1.224.18.www-http > 137.133.57.68.1255: tcp 48
16:27:55.440488 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:55.444033 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1160
16:27:55.447007 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:55.450144 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1160
16:27:55.456636 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:55.657583 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1160
16:27:55.660751 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:55.877792 137.133.16.54.32793 > 137.133.63.36.1730: tcp 147 (DF)
16:27:55.881254 209.1.224.18.www-http > 137.133.57.68.1255: tcp 592
16:27:55.884685 209.1.224.18.www-http > 137.133.57.68.1255: tcp 616
16:27:55.887807 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:55.890866 137.133.63.36.1730 > 137.133.16.54.32793: tcp 0 (DF)
16:27:55.893980 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1160
16:27:55.987888 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1160
16:27:55.991367 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:55.994454 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1112
16:27:55.997915 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:56.000966 137.133.63.36.33272 > 137.133.16.54.1730: tcp 147 (DF)
16:27:56.004058 137.133.63.36.32789 > 137.133.16.53.1730: tcp 147 (DF)
16:27:56.207953 nera-x.1035 > nera-y.loc-serv:  udp 204
16:27:56.210769 nera-y.loc-serv > nera-x.1035:  udp 172
16:27:56.213192 209.1.224.18.www-http > 137.133.57.68.1255: tcp 664
16:27:56.216609 209.1.224.18.www-http > 137.133.57.68.1255: tcp 834
16:27:56.219818 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:56.222877 209.1.224.18.www-http > 137.133.57.68.1255: tcp 326
16:27:56.318051 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1160
16:27:56.321065 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:56.324244 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1106
16:27:56.327222 209.1.224.18.www-http > 137.133.57.68.1255: tcp 670
16:27:56.330206 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:56.333267 209.1.224.18.www-http > 137.133.57.68.1255: tcp 700
16:27:56.428080 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:56.538072 209.1.224.18.www-http > 137.133.57.68.1255: tcp 460
16:27:56.541090 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1160
16:27:56.544893 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:56.648239 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1160
16:27:56.651262 209.1.224.18.www-http > 137.133.57.68.1255: tcp 616
16:27:56.654247 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:56.657292 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1160
16:27:56.660425 209.1.224.18.www-http > 137.133.57.68.1255: tcp 911
16:27:56.663376 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)

 tcpdump 3.5                                            Eth: 139 (139)
```

Tcpdump Commands

Exporting tcpdumps to a file

- `# tcpdump port 80 -l > webdump.txt & tail -f webdump.txt`
- `# tcpdump -w rawdump`
- `# tcpdump -r rawdump > rawdump.txt`
- `# tcpdump -c1000 -w rawdump`
- `# tcpdump -i eth1 -c1000 -w rawdump`

Captures traffic on a specific port

- `# tcpdump port 80`

You can select several hosts on your LAN and capture the traffic that passes between them

- `# tcpdump host workstation4 and workstation11 and workstation13`

Tcpdump Commands (cont'd)

Capture all the LAN traffic between workstation4 and the LAN, except for workstation11

- # tcpdump -e host workstation4 and workstation11 and workstation13

Capture all packets except those for certain ports

- # tcpdump not port 110 and not port 25 and not port 53 and not port 22

Filter by protocol

- # tcpdump udp
- # tcpdump ip proto OSPFIGP

Capture traffic on a specific host and restrict by protocol

- # tcpdump host server02 and ip
  # tcpdump host server03 and not udp
  # tcpdump host server03 and ip and igmp and not udp

Wiretap

Wiretapping is the monitoring of telephone and Internet conversations by a third party

The monitoring connection was applied to the wires of the telephone line being monitored and a small amount of the electrical signal carrying the conversation get tapped

RF Transmitter Wiretaps

In radio frequency (RF) transmitter tap technique, a small RF transmitter is attached to the telephone line or within the telephone instrument

In these wiretaps, audio fluctuations from the telephone conversation modulate the transmitter carrier that transmit the conversation into free air space

Infinity Transmitter

An infinity transmitter is the device used as a wiretap to monitor the communication

It operates independent of the telephone instrument and requires its own telephone line

It can be called from a remote telephone and activated with a tone signal

Slave Parallel Wiretaps

Slave Parallel Wiretaps device works in the same way as infinity transmitter and combines these features with a parallel wiretap

The slave is connected anywhere with the target telephone line

In these wiretaps, an attacker needs a working telephone line located in the same cable, cross-connect, or closet as the target line

Once lines are connected to the slave, the eavesdropper can call his leased telephone line and activate the slave

After activation, the slave automatically connects the eavesdroppers telephone line to the target telephone line

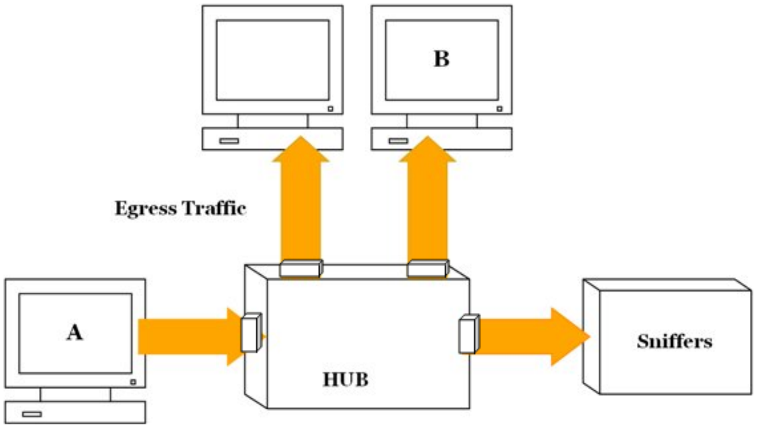
Switched Port Analyzer (SPAN)

The Switched Port Analyzer (SPAN) feature, also called port mirroring or port monitoring, selects network traffic for analysis by a network analyzer

The network analyzer can be a Cisco SwitchProbe device or other Remote Monitoring (RMON) probe

SPAN feature applies on switches because of a fundamental difference that switches have with hubs

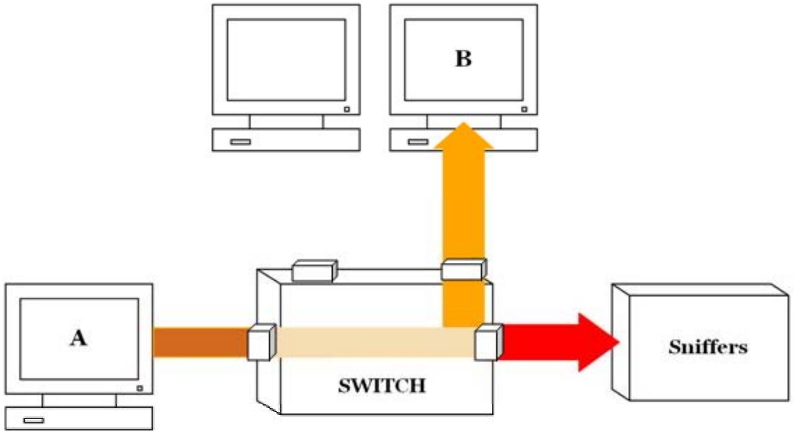
In a single local SPAN session, you can monitor source port traffic such as received (Rx), transmitted (Tx), or bidirectional (both) traffic

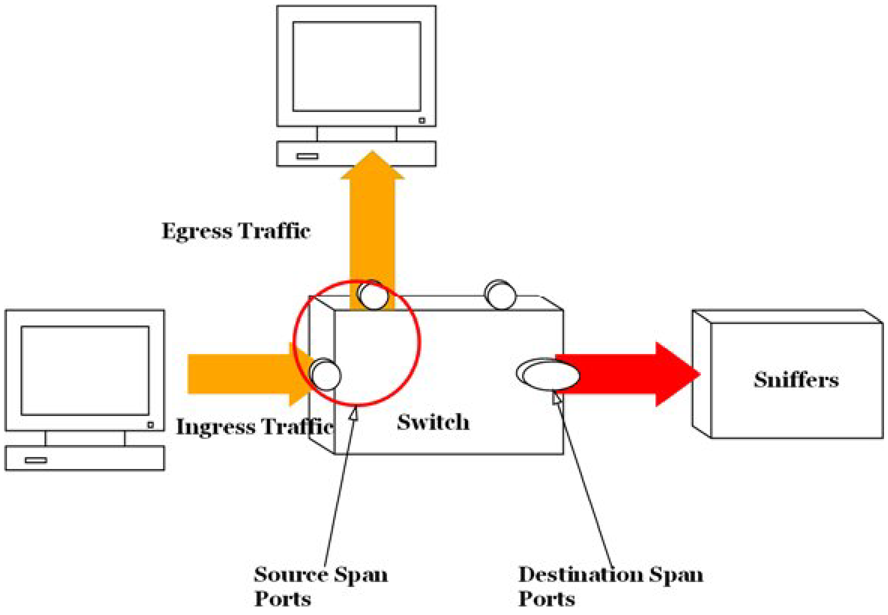


SPAN Port

SPAN port is the port to which sniffer is attached and configured to receive a copy of every packets sent from the source host to the destination host

- Source (SPAN) port: A port that is monitored with the use of the SPAN feature
- Destination (SPAN) port: A port that monitors source ports, usually where a network analyzer is connected





Lawful Intercept

Lawful intercept is a process that enables a Law Enforcement Agency (LEA) to perform electronic surveillance on an individual (a target) as authorized by a judicial or administrative order

The surveillance is performed through the use of wiretaps on traditional telecommunications and Internet services in voice, data, and multiservice networks

The LEA delivers a request for a wiretap to the target's service provider, who is responsible for intercepting data communication to and from the individual

The service provider uses the target's IP address or session to determine which of its edge routers handles the target's traffic (data communication)

The service provider then intercepts the target's traffic as it passes through the router and sends a copy of the intercepted traffic to the LEA without the target's knowledge.

Benefits of Lawful Intercept

Allows multiple LEAs to run a lawful intercept on the same target without each other's knowledge

Does not affect subscriber services on the router

Supports wiretaps in both the input and output direction

Supports wiretaps of individual subscribers that share a single physical interface

Neither the network administrator nor the calling parties is aware that packets are being copied or that the call is being tapped

Hides information about lawful intercepts from all but the most privileged users

Provides two secure interfaces for performing an intercept: one for setting up the wiretap and one for sending the intercepted traffic to the LEA

Network Components Used for Lawful Intercept

Mediation Device:

- A mediation device (supplied by a third-party vendor) handles most of the processing for the lawful intercept

Intercept Access Point:

- An intercept access point (IAP) is a device that provides information for the lawful intercept

Collection Function:

- The collection function is a program that stores and processes traffic intercepted by the service provider

ARP Spoofing Attack

ARP resolves IP addresses to MAC (hardware) address of interface to send data

ARP packets can be forged to send data to the attacker’s machine

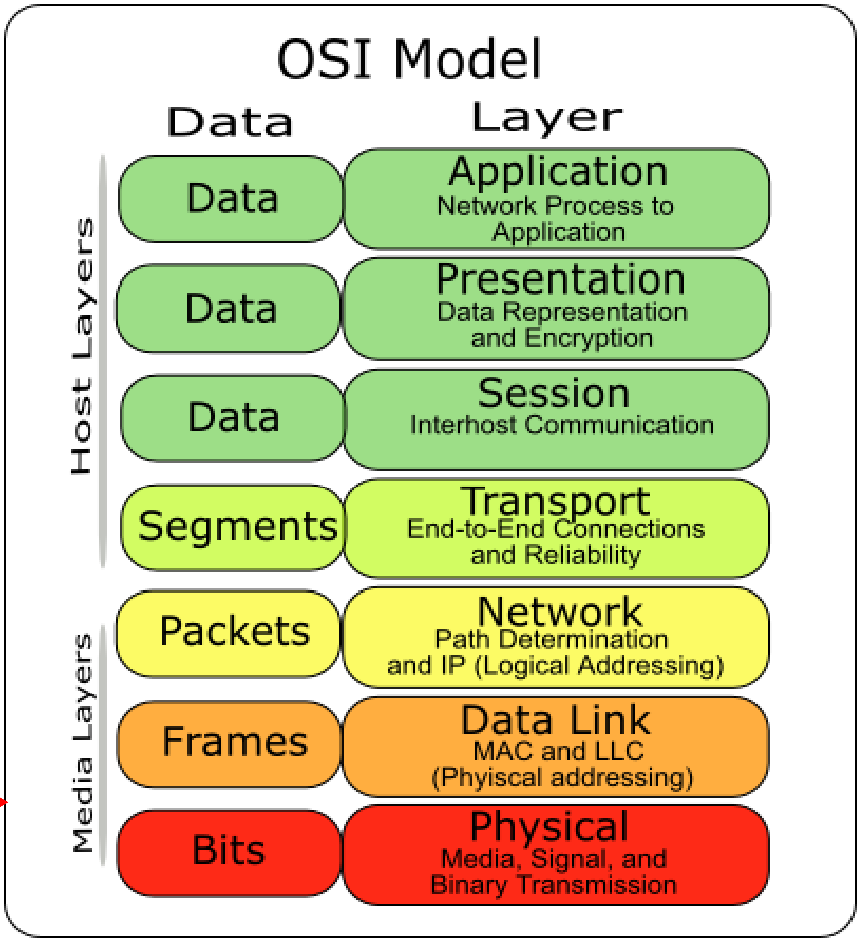
An attacker can exploit ARP poisoning to intercept the network traffic between two machines on the network

By MAC flooding a switch's ARP table with spoofed ARP replies, the attacker can overload switches and then packet sniff network while switch is in “forwarding mode”

How Does ARP Spoofing Work

When a legitimate user initiates a session with another user in the same Layer 2 broadcast domain, an ARP request is broadcasted using the recipient's IP address and the sender waits for the recipient to respond with a MAC address

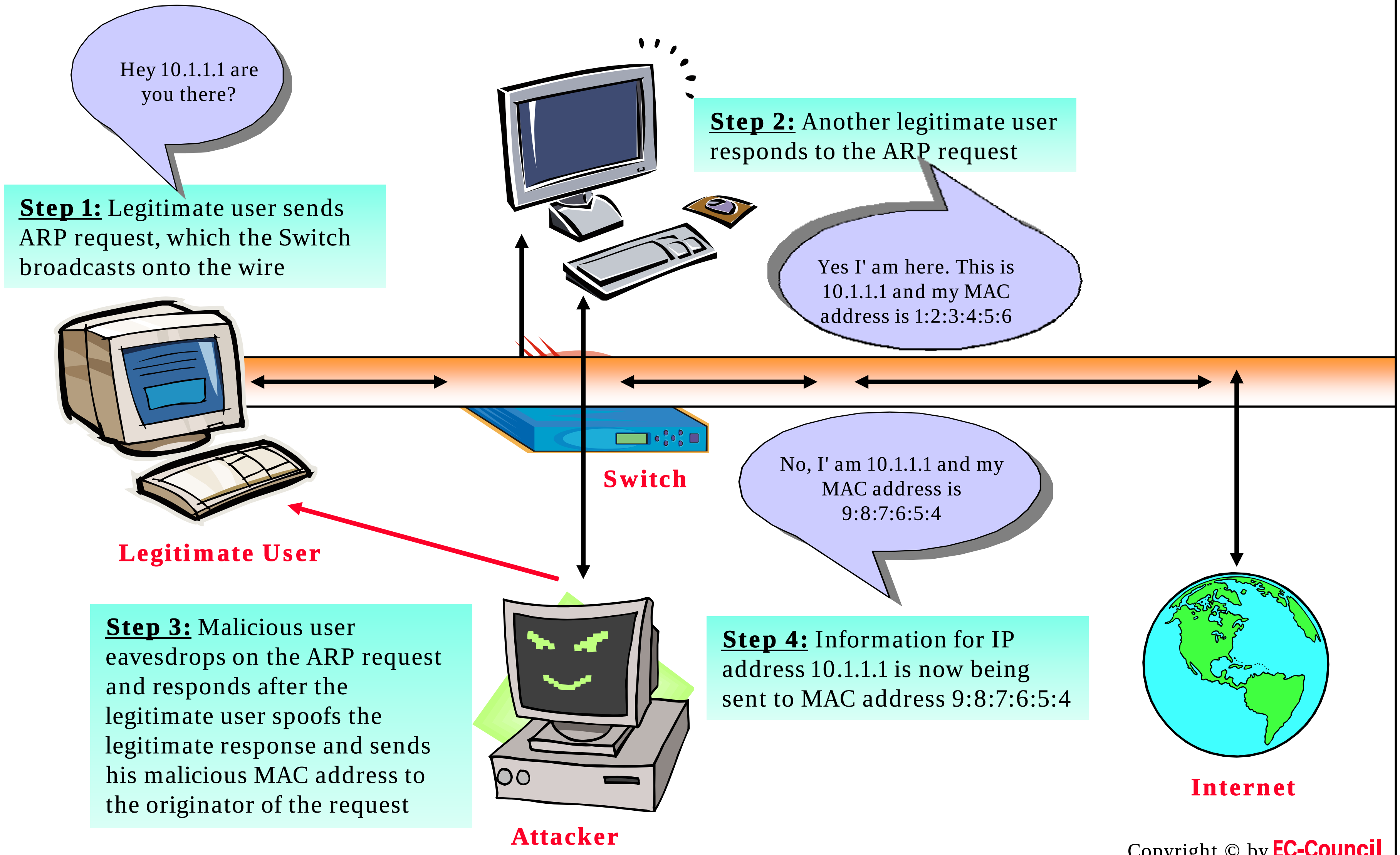
Malicious user eavesdrops on this unprotected Layer 2 broadcast domain and can respond to a broadcast ARP request and reply to the sender by spoofing the intended recipient's MAC address



OSI Model

	Data	Layer
Host Layers	Data	Application Network Process to Application
	Data	Presentation Data Representation and Encryption
	Data	Session Interhost Communication
	Segments	Transport End-to-End Connections and Reliability
Media Layers	Packets	Network Path Determination and IP (Logical Addressing)
	Frames	Data Link MAC and LLC (Phyiscal addressing)
	Bits	Physical Media, Signal, and Binary Transmission

ARP Poisoning


Hey 10.1.1.1 are you there?
Yes I' am here. This is 10.1.1.1 and my MAC address is 1:2:3:4:5:6
No, I' am 10.1.1.1 and my MAC address is 9:8:7:6:5:4
Legitimate User
Switch
Attacker
Internet

Step 1: Legitimate user sends ARP request, which the Switch broadcasts onto the wire

Step 2: Another legitimate user responds to the ARP request

Step 3: Malicious user eavesdrops on the ARP request and responds after the legitimate user spoofs the legitimate response and sends his malicious MAC address to the originator of the request

Step 4: Information for IP address 10.1.1.1 is now being sent to MAC address 9:8:7:6:5:4

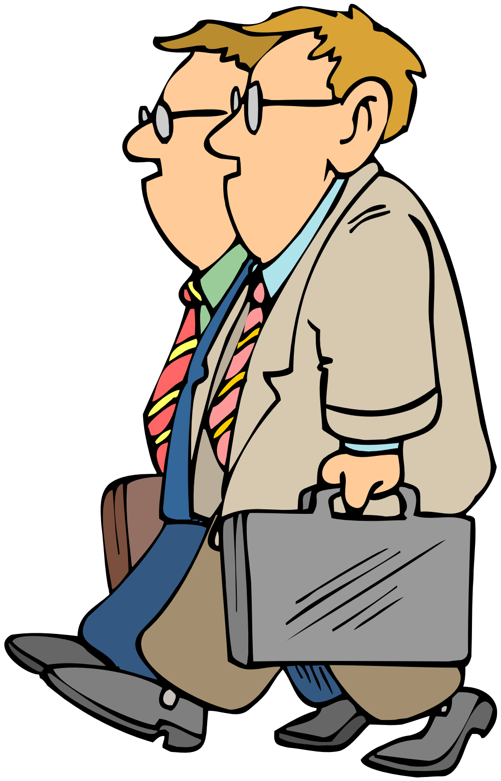
Mac Duplicating

MAC duplicating attack is launched by sniffing network for MAC addresses of clients who are actively associated with a switch port and re-use one of those addresses

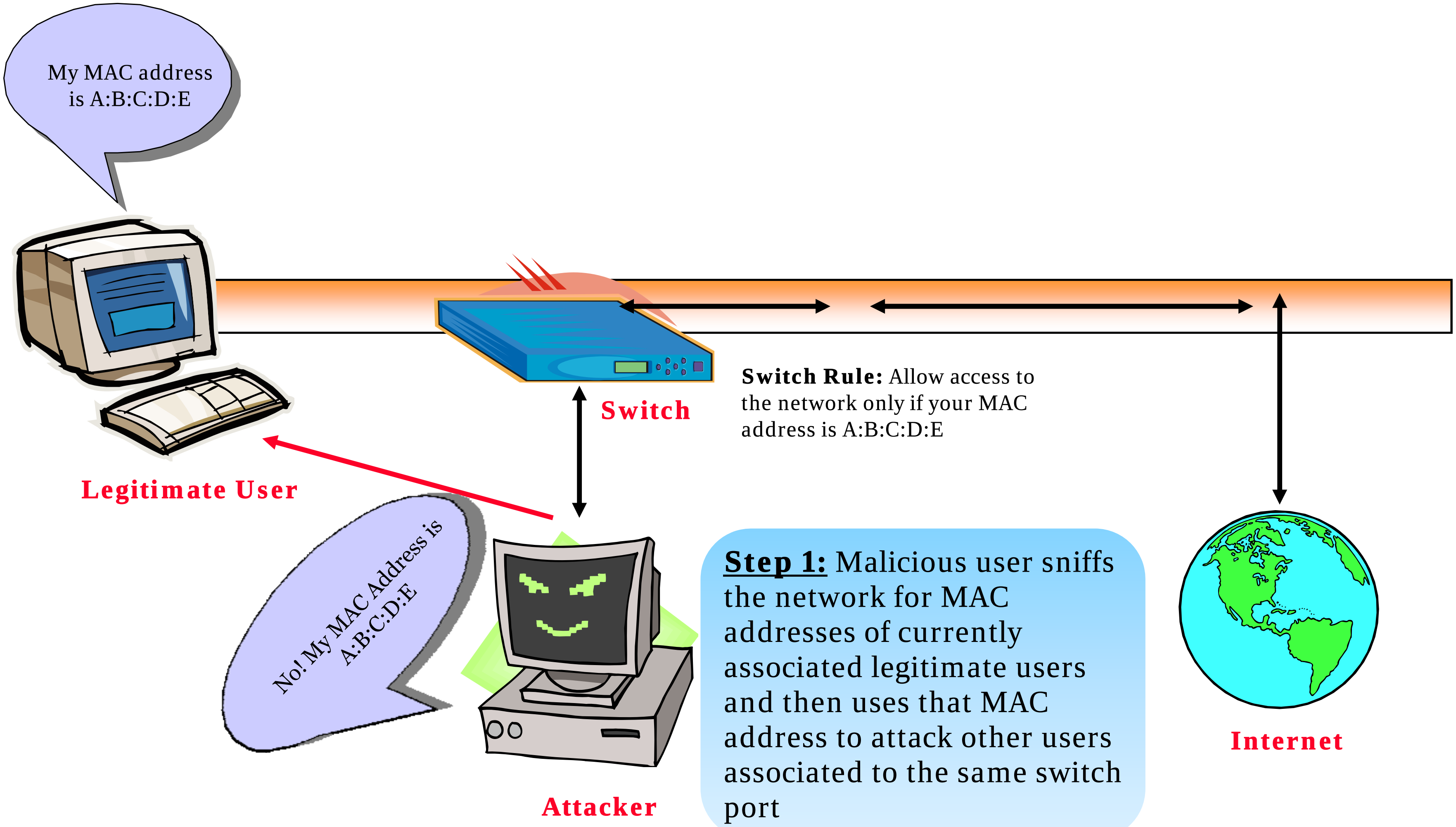
By listening to the traffic on the network, a malicious user can intercept and use a legitimate user's MAC address

An attacker will receive all the traffic destined for that the legitimate user

This technique works on Wireless Access Points with MAC filtering enabled



Mac Duplicating Attack



Switch Rule: Allow access to the network only if your MAC address is A:B:C:D:E

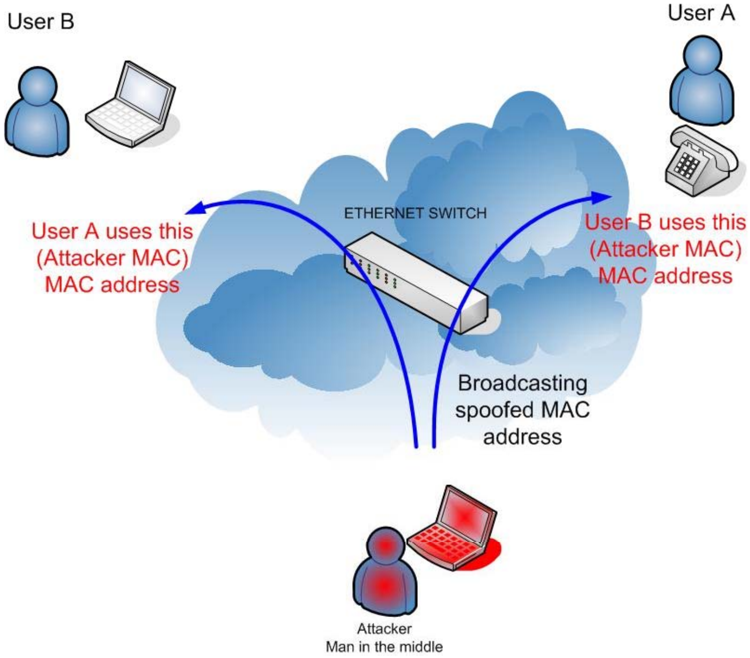
Step 1: Malicious user sniffs the network for MAC addresses of currently associated legitimate users and then uses that MAC address to attack other users associated to the same switch port

ARP Spoofing Tools

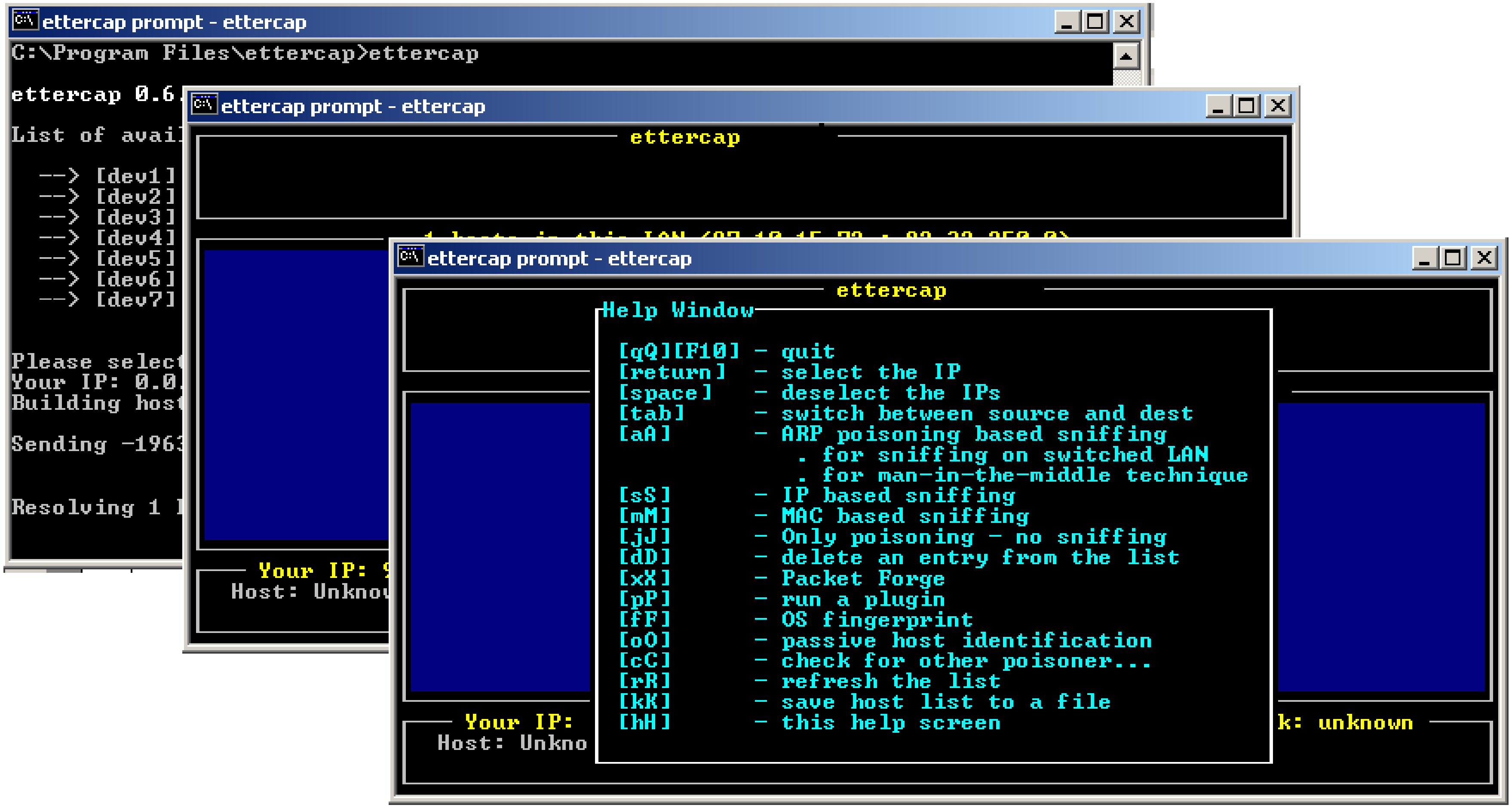
Tools for ARP Spoofing

Tools for ARP Spoofing

- Arpspoof (Linux-based tool)
- Ettercap (Linux and Windows)
Cain and Able
- ArpSpyX (Mac OS)


User B
User A
ETHERNET SWITCH
User A uses this (Attacker MAC) MAC address
User B uses this (Attacker MAC) MAC address
Broadcasting spoofed MAC address
Attacker
Man in the middle

Ettercap



```
ettercap prompt - ettercap
C:\Program Files\ettercap>ettercap

ettercap 0.6.

List of avai

  --> [dev1]
  --> [dev2]
  --> [dev3]
  --> [dev4]
  --> [dev5]
  --> [dev6]
  --> [dev7]


Please select
Your IP: 0.0.
Building host

Sending -1963


Resolving 1 
```

```
ettercap prompt - ettercap
                                  ettercap


 Your IP: 9
Host: Unknow
```

```
ettercap prompt - ettercap
                                  ettercap
            Help Window

             [qQ][F10] - quit
             [return]  - select the IP
             [space]   - deselect the IPs
             [tab]     - switch between source and dest
             [aA]      - ARP poisoning based sniffing
                            . for sniffing on switched LAN
                            . for man-in-the-middle technique
             [sS]      - IP based sniffing
             [mM]      - MAC based sniffing
             [jJ]      - Only poisoning - no sniffing
             [dD]      - delete an entry from the list
             [xX]      - Packet Forge
             [pP]      - run a plugin
             [fF]      - OS fingerprint
             [oO]      - passive host identification
             [cC]      - check for other poisoner...
             [rR]      - refresh the list
             [kK]      - save host list to a file
             [hH]      - this help screen

 Your IP:                                                   k: unknown
Host: Unkno
```

A tool for IP-based sniffing in a switched network, MAC-based sniffing, OS fingerprinting, ARP poisoning-based sniffing, and so on

ArpSpyX

ArpSpyX passively sniffs network ARP packets and displays IP and MAC address of the machine that generates packet

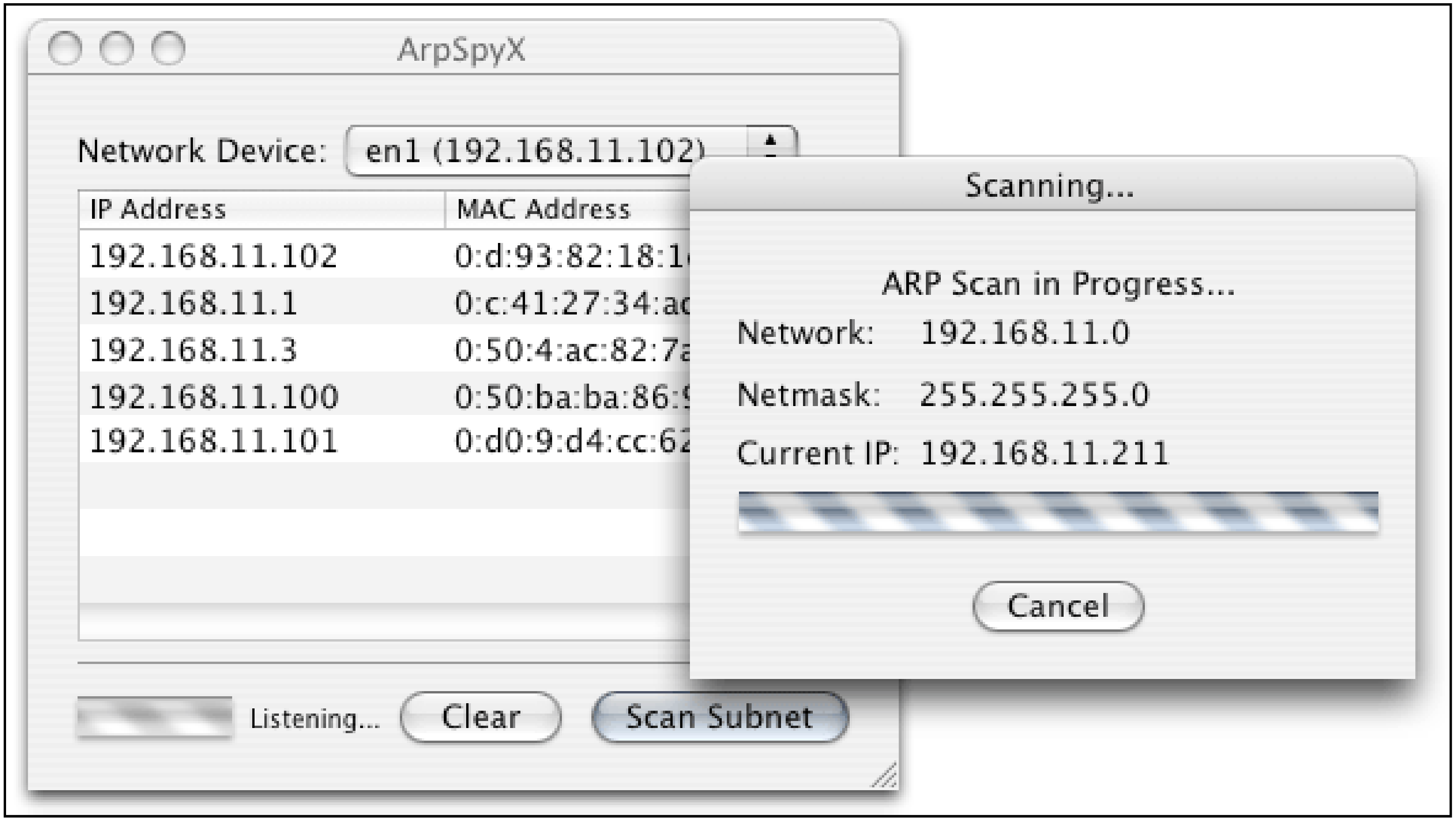
ArpSpyX supports two methods of scanning:

- The first method is a passive mode which only listens for traffic without sending any packets
- The second method is active and will send out arp who-has requests for every IP address on your subnet

Features of ArpSpyX include:

- Easily gathering MAC Addresses of the network machines remotely
- Quickly identifying new clients on your wireless network
- Identifying ARP Poisoning attacks by tracking multiple MAC Addresses for a single IP Address
- Creating a text file containing all IP addresses on your network

ArpSpyX: Screenshot



Network Device: en1 (192.168.11.102)

IP Address	MAC Address
192.168.11.102	0:d:93:82:18:1
192.168.11.1	0:c:41:27:34:ac
192.168.11.3	0:50:4:ac:82:7a
192.168.11.100	0:50:ba:ba:86:9
192.168.11.101	0:d0:9:d4:cc:62

ARP Scan in Progress...

Network: 192.168.11.0

Netmask: 255.255.255.0

Current IP: 192.168.11.211

C|EH™
Certified Ethical Hacker

MAC Flooding Tools

EC-Council

MAC Flooding

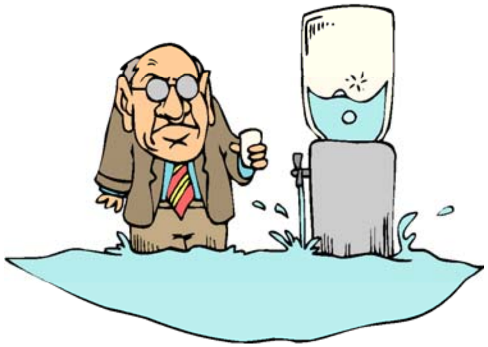
MAC flooding involves flooding switch with numerous requests

Switches have a limited memory for mapping various MAC addresses to the physical ports on switch

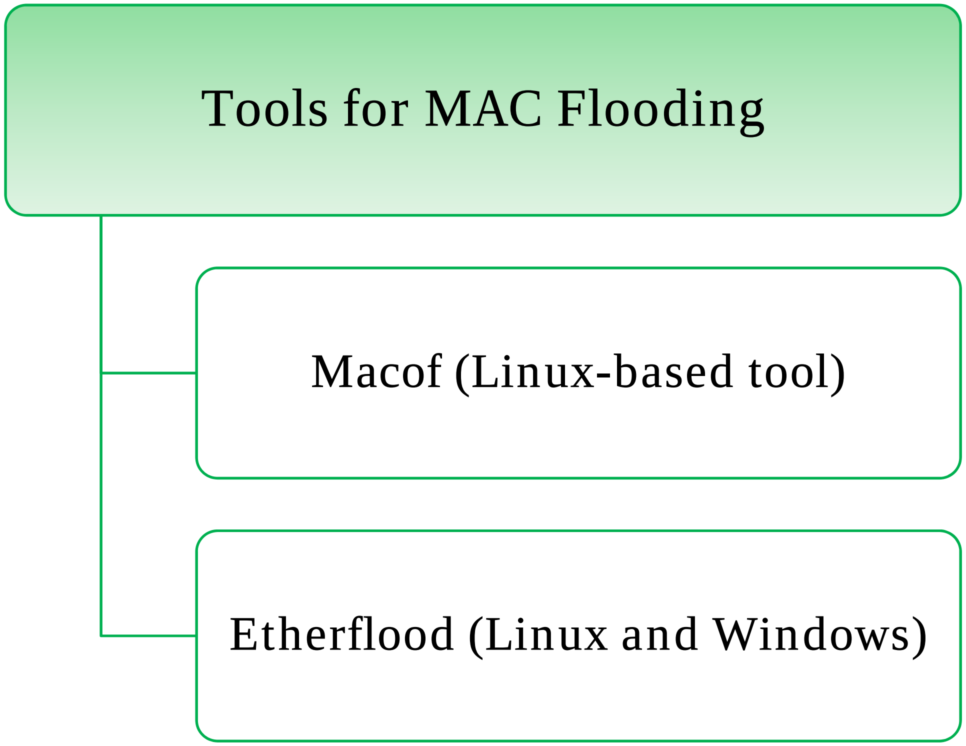
MAC flooding makes use of this limitation to bombard switch with fake MAC addresses until the switch cannot keep up

Switch then acts as a hub by broadcasting packets to all machines on the network

After this, sniffing can be easily performed



Tools for MAC Flooding



Tools for MAC Flooding

- Macof (Linux-based tool)
- Etherflood (Linux and Windows)

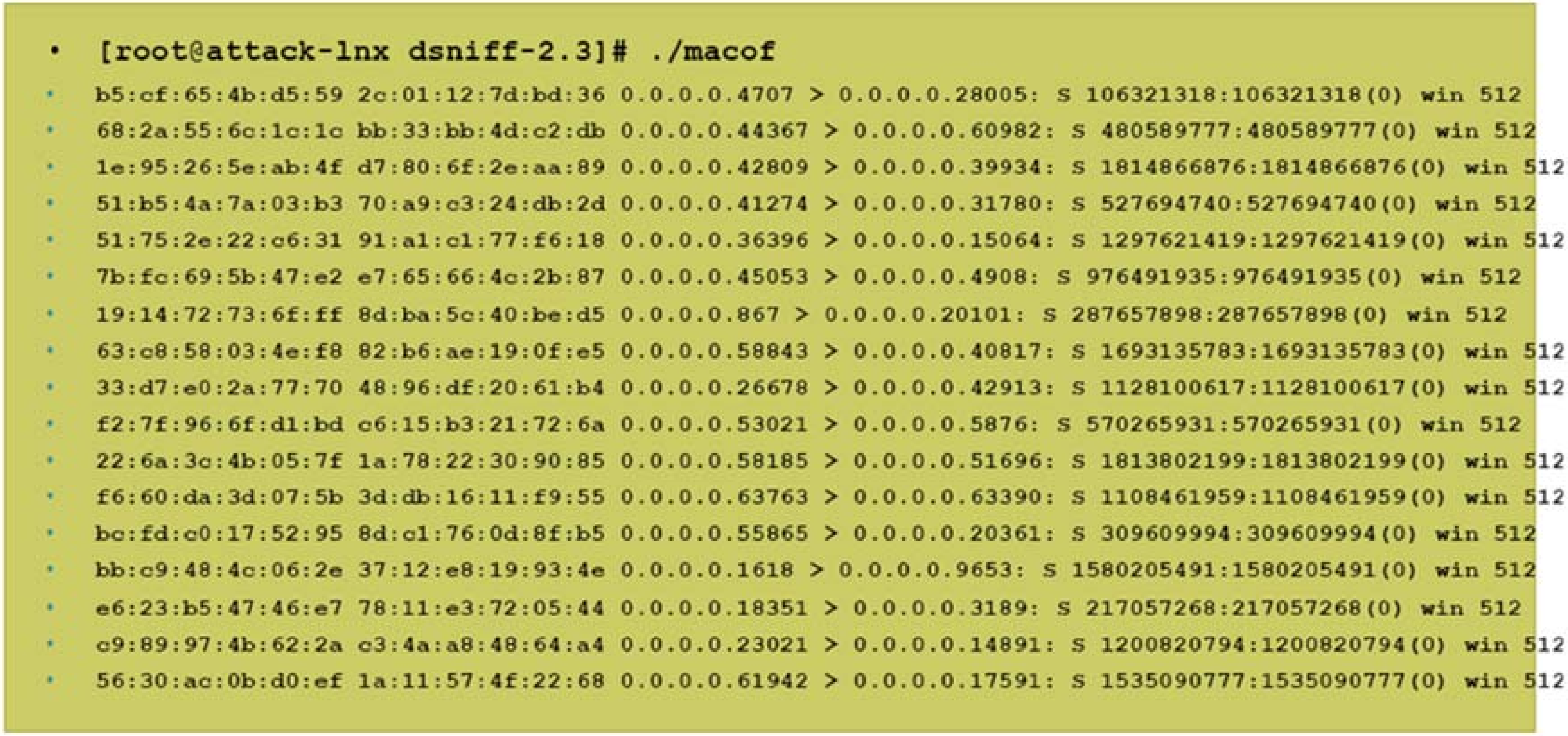
Linux Tool: Macof

Macof floods local network random MAC addresses, causing some switches to fail to open in the repeating mode, which facilitates sniffing

- `macof [-i interface] [-s src] [-d dst] [-e tha] [-x sport] [-y dport] [-n times]`

Macof: Screenshot

MAC Flooding Switches with Macof



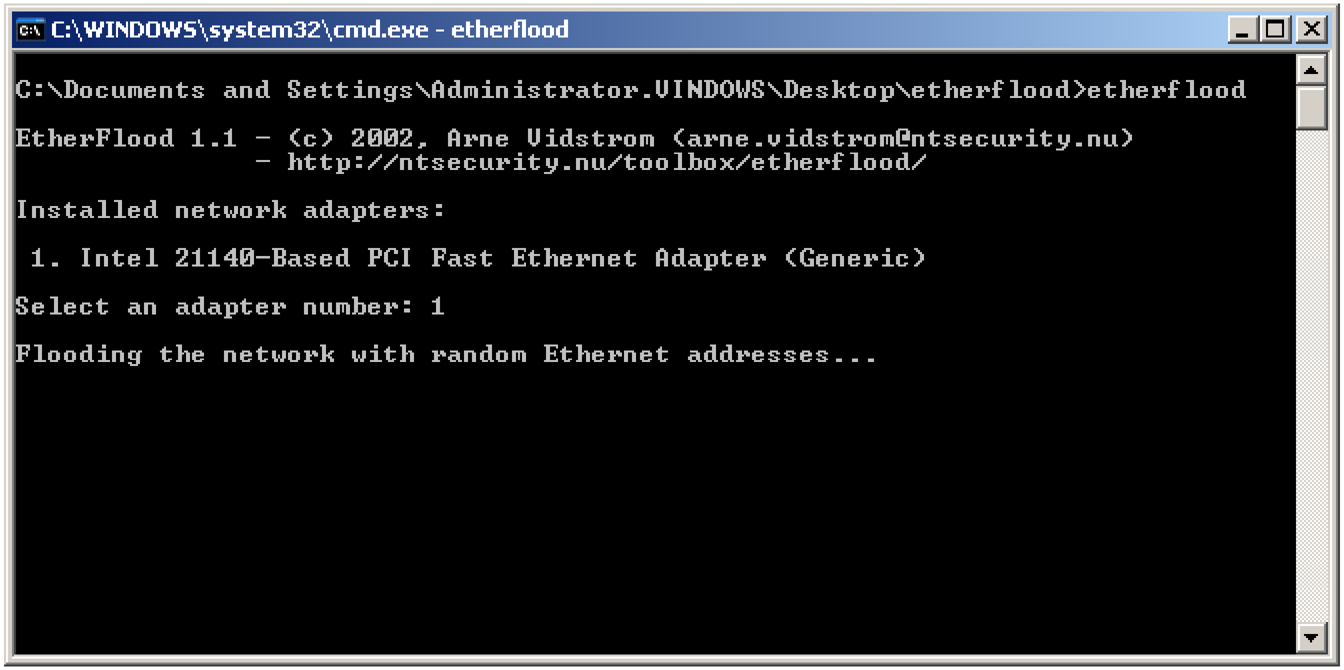
```
•  [root@attack-lnx dsniff-2.3]# ./macof
•  b5:cf:65:4b:d5:59 2c:01:12:7d:bd:36 0.0.0.0.4707 > 0.0.0.0.28005: S 106321318:106321318(0) win 512
•  68:2a:55:6c:1c:1c bb:33:bb:4d:c2:db 0.0.0.0.44367 > 0.0.0.0.60982: S 480589777:480589777(0) win 512
•  1e:95:26:5e:ab:4f d7:80:6f:2e:aa:89 0.0.0.0.42809 > 0.0.0.0.39934: S 1814866876:1814866876(0) win 512
•  51:b5:4a:7a:03:b3 70:a9:c3:24:db:2d 0.0.0.0.41274 > 0.0.0.0.31780: S 527694740:527694740(0) win 512
•  51:75:2e:22:c6:31 91:a1:c1:77:f6:18 0.0.0.0.36396 > 0.0.0.0.15064: S 1297621419:1297621419(0) win 512
•  7b:fc:69:5b:47:e2 e7:65:66:4c:2b:87 0.0.0.0.45053 > 0.0.0.0.4908: S 976491935:976491935(0) win 512
•  19:14:72:73:6f:ff 8d:ba:5c:40:be:d5 0.0.0.0.867 > 0.0.0.0.20101: S 287657898:287657898(0) win 512
•  63:c8:58:03:4e:f8 82:b6:ae:19:0f:e5 0.0.0.0.58843 > 0.0.0.0.40817: S 1693135783:1693135783(0) win 512
•  33:d7:e0:2a:77:70 48:96:df:20:61:b4 0.0.0.0.26678 > 0.0.0.0.42913: S 1128100617:1128100617(0) win 512
•  f2:7f:96:6f:d1:bd c6:15:b3:21:72:6a 0.0.0.0.53021 > 0.0.0.0.5876: S 570265931:570265931(0) win 512
•  22:6a:3c:4b:05:7f 1a:78:22:30:90:85 0.0.0.0.58185 > 0.0.0.0.51696: S 1813802199:1813802199(0) win 512
•  f6:60:da:3d:07:5b 3d:db:16:11:f9:55 0.0.0.0.63763 > 0.0.0.0.63390: S 1108461959:1108461959(0) win 512
•  bc:fd:c0:17:52:95 8d:c1:76:0d:8f:b5 0.0.0.0.55865 > 0.0.0.0.20361: S 309609994:309609994(0) win 512
•  bb:c9:48:4c:06:2e 37:12:e8:19:93:4e 0.0.0.0.1618 > 0.0.0.0.9653: S 1580205491:1580205491(0) win 512
•  e6:23:b5:47:46:e7 78:11:e3:72:05:44 0.0.0.0.18351 > 0.0.0.0.3189: S 217057268:217057268(0) win 512
•  c9:89:97:4b:62:2a c3:4a:a8:48:64:a4 0.0.0.0.23021 > 0.0.0.0.14891: S 1200820794:1200820794(0) win 512
•  56:30:ac:0b:d0:ef 1a:11:57:4f:22:68 0.0.0.0.61942 > 0.0.0.0.17591: S 1535090777:1535090777(0) win 512
```

Certified Ethical Hacker

Windows Tool: EtherFlood

EtherFlood floods a switched network with Ethernet frames with random hardware addresses

The effect on some switches is that they start sending all traffic out on all ports so that the attacker is able to sniff all traffic on sub-network



```
C:\Documents and Settings\Administrator.VINDOWS\Desktop\etherflood>etherflood

EtherFlood 1.1 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
                - http://ntsecurity.nu/toolbox/etherflood/

Installed network adapters:

 1. Intel 21140-Based PCI Fast Ethernet Adapter (Generic)

Select an adapter number: 1

Flooding the network with random Ethernet addresses...
```

Source: http://ntsecurity.nu/toolbox/etherflood/

Threats of ARP Poisoning

Internal network attacks are typically operated via ARP Poisoning attacks

Everyone can download on Internet Malicious software which is used to run ARP Spoofing attacks

Using fake ARP messages, an attacker can divert all communication between two machines so that all traffic is exchanged via his PC

By means, such as a man-in-the-middle attack, the attacker can, in particular:

- Run Denial of Service (DoS) attacks
- Intercept data
- Collect passwords
- Manipulate data
- Tap VoIP phone calls

IRS – ARP Attack Tool

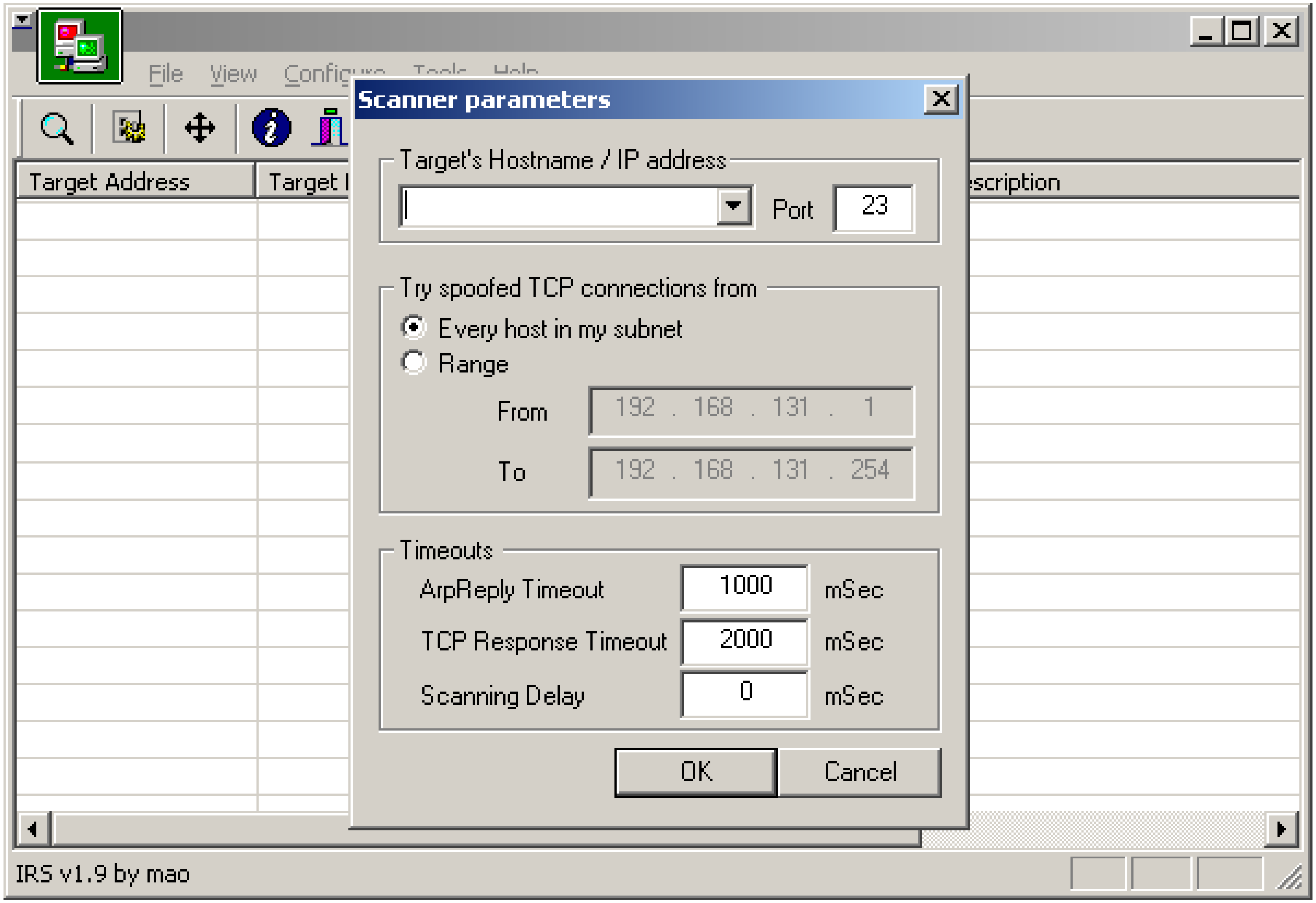
Many servers and network devices like routers and switches provide features like ACLs, IP Filters, Firewall rules, and so on, to give access to their services only to the particular network addresses (usually Administrators' workstations)

This tool scans for IP restrictions set for a particular service on a host

It combines "ARP Poisoning" and "Half-Scan" techniques and tries spoofed TCP connections to the selected port of the target

IRS is not a port scanner but a "valid source IP address" scanner for a given service

IRS – ARP Attack Tool: Screenshot



Scanner parameters

Target's Hostname / IP address

Port: 23

Try spoofed TCP connections from

● Every host in my subnet

○ Range

From: 192 . 168 . 131 . 1

To: 192 . 168 . 131 . 254

Timeouts

ArpReply Timeout: 1000 mSec

TCP Response Timeout: 2000 mSec

Scanning Delay: 0 mSec

IRS v1.9 by mao

EC-Council

ARPWorks Tool

ArpWorks is a utility for sending customized 'ARP announce' packets over the network

All ARP parameters, including Ethernet Source MAC address can be changed

Other features are: IP to MAC revolver, subnet MAC discovery, host isolation, packets redirection, and general IP conflict

CEH™ Certified Ethical Hacker

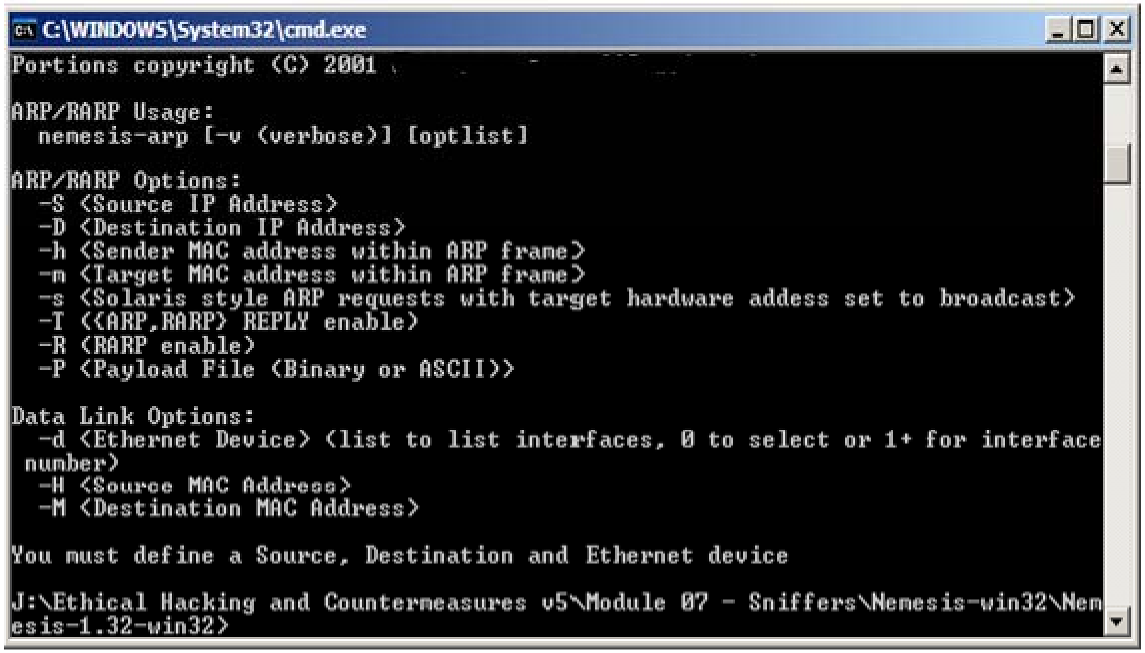
Tool: Nemesis

Nemesis provides an interface to craft and inject a variety of arbitrary packet types

It is also used for ARP Spoofing

Nemesis supports the following protocols:

- arp
- dns
- ethernet
- icmp
- igmp
- ip
- ospf
- rip
- tcp
- udp



```
Portions copyright (C) 2001

ARP/RARP Usage:
  nemesis-arp [-v (verbose)] [optlist]

ARP/RARP Options:
  -S <Source IP Address>
  -D <Destination IP Address>
  -h <Sender MAC address within ARP frame>
  -m <Target MAC address within ARP frame>
  -s <Solaris style ARP requests with target hardware addess set to broadcast>
  -I <<ARP,RARP> REPLY enable>
  -R <RARP enable>
  -P <Payload File <Binary or ASCII>>

Data Link Options:
  -d <Ethernet Device> <list to list interfaces, 0 to select or 1+ for interface
 number>
  -H <Source MAC Address>
  -M <Destination MAC Address>

You must define a Source, Destination and Ethernet device

J:\Ethical Hacking and Countermeasures v5\Module 07 - Sniffers\Nemesis-win32\Nemesis-1.32-win32>
```

IP-based Sniffing

IP-based Sniffing is the original way of packet sniffing

It works by putting network card into the promiscuous mode and sniffing all packets matching the IP address filter

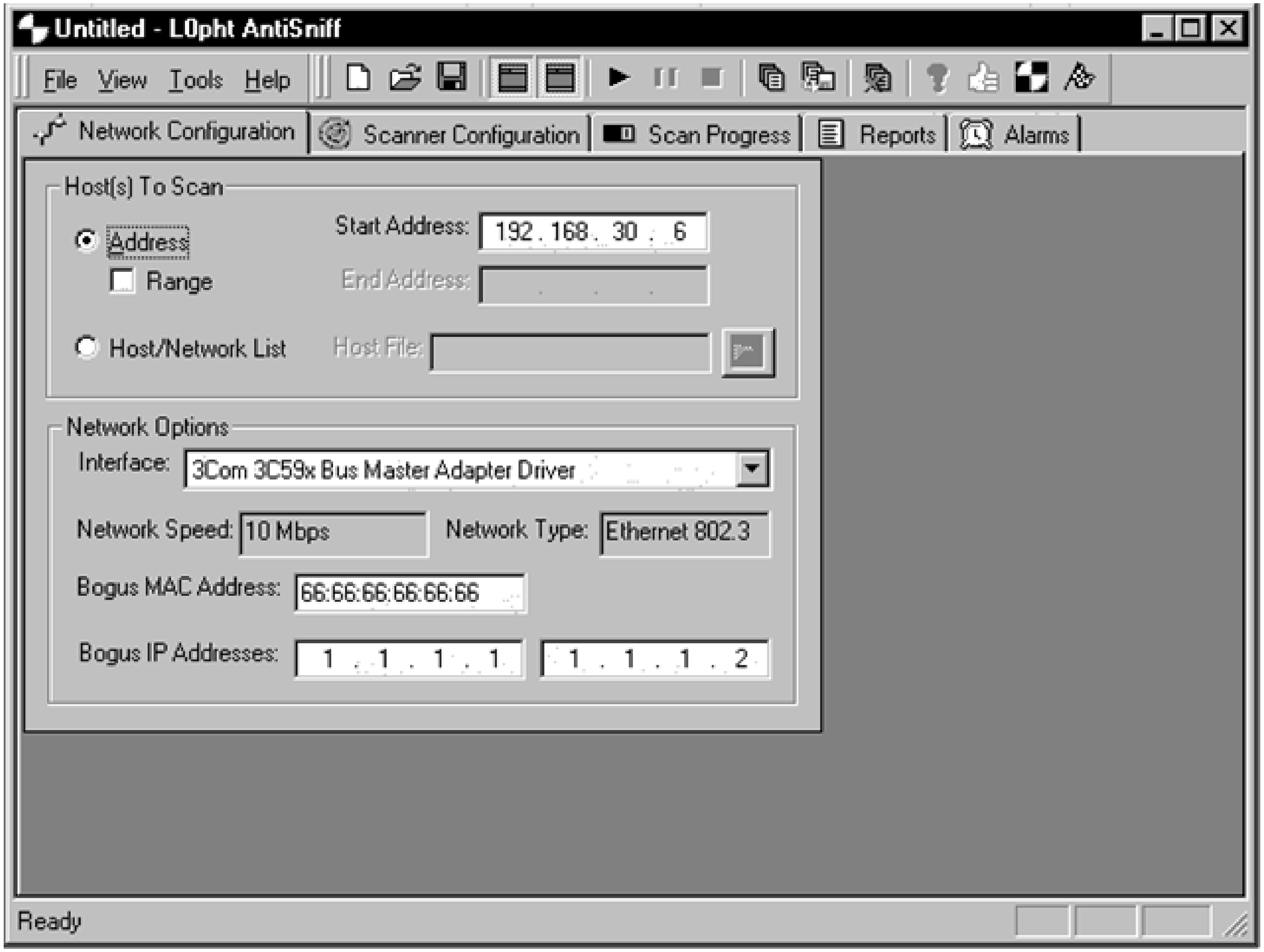
IP address filter can capture all packets even though it is not set

This method only works in non-switched networks

AntiSniff

- AntiSniff program determines if a device is listening to the traffic on the local network
- AntiSniff DNS test is vulnerable to a buffer overflow that would allow an attacker to execute an arbitrary code by sending a malformed DNS packet to the system running AntiSniff

IP-based Sniffing: Screenshot



Host(s) To Scan

● Address Start Address: 192 . 168 . 30 . 6

□ Range End Address:

○ Host/Network List Host File:

Network Options

Interface: 3Com 3C59x Bus Master Adapter Driver

Network Speed: 10 Mbps Network Type: Ethernet 802.3

Bogus MAC Address: 66:66:66:66:66:66

Bogus IP Addresses: 1 . 1 . 1 . 1 1 . 1 . 1 . 2

Ready

Linux Sniffing Tools

CEH™ Certified Ethical Hacker

Linux Sniffing Tools (dsniff package)

Sniffer hacking tools (These tools are available on the Linux CD-ROM)

arpspoof

- Intercepts packets on a switched LAN

dnsspoof

- Forges replies to DNS address and pointer queries

dsniff

- Password sniffer

filesnarf

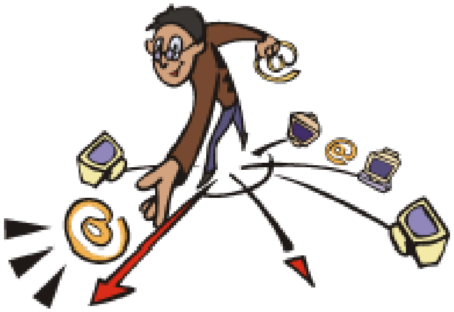
- Sniffs files from NFS traffic

mailsnarf

- Sniffs mail messages in Berkeley mbox format

msgsnarf

- Sniffs chat messages



Linux Sniffing Tools (cont'd)

sshmitm

- SSH monkey-in-the-middle

tcpkill

- Kills TCP connections on a LAN

tcpnice

- Slows down TCP connections on a LAN

urlsnarf

- Sniffs HTTP requests in Common Log Format

webspy

- Displays sniffed URLs in Netscape in real time

webmitm

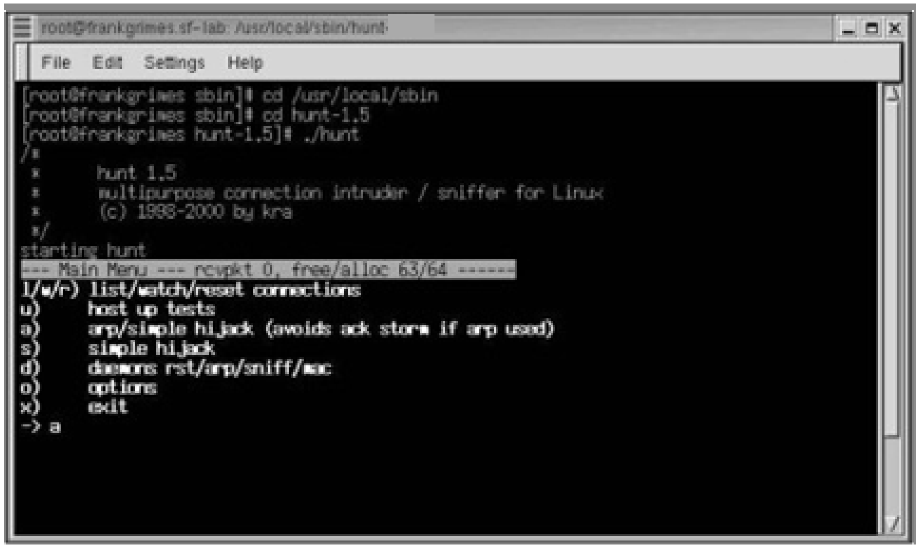
- HTTP/HTTPS monkey-in-the-middle

Linux Tool: Arpspoof

Arpspoof redirects packets from a target host intended for another host on the LAN by forging ARP replies

Arpspoof is the effective way of sniffing traffic on a switch

- `arpspoof [-i interface] [-t target] host`



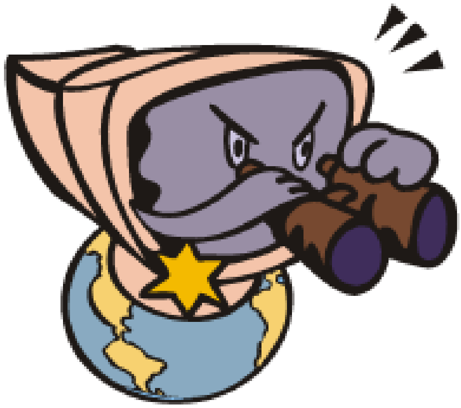
```
[root@frankgrimes sbin]# cd /usr/local/sbin
[root@frankgrimes sbin]# cd hunt-1.5
[root@frankgrimes hunt-1.5]# ./hunt
/*
 *      hunt 1.5
 *      multipurpose connection intruder / sniffer for Linux
 *      (c) 1998-2000 by kra
 */
starting hunt
--- Main Menu --- rcvpkt 0, free/alloc 63/64 ------
l/w/r) list/watch/reset connections
u)     host up tests
a)     arp/simple hijack (avoids ack storm if arp used)
s)     simple hijack
d)     daemons rst/arp/sniff/mac
o)     options
x)     exit
-> a
```

Linux Tool: Dnsspoof

Dnsspoof forges replies to arbitrary DNS address/pointer queries on the LAN

DNS spoofing is useful in bypassing hostname-based access controls, or in implementing a variety of man-in-the-middle attacks

- `dnsspoof [-i interface][-f hostsfile] [expression]`



Linux Tool: Dsniff

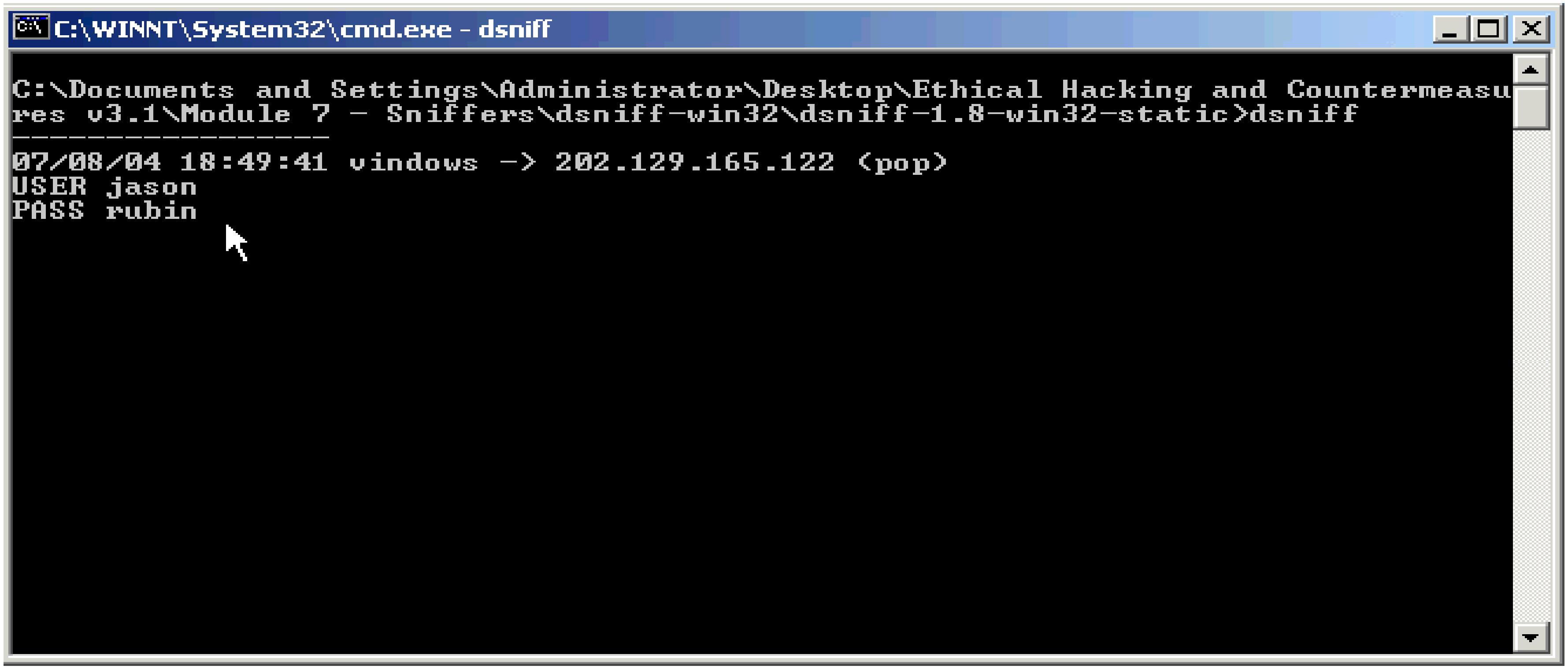
Dsniff is a password sniffer which handles FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP MS-CHAP, NFS, VRRP, and so on

Dsniff automatically detects and minimally parses each application protocol, only saving interesting bits, and uses Berkeley DB as its output file format, only logging unique authentication attempts

Full TCP/IP reassembly is provided by libnids

- `dsniff [-c] [-d] [-m] [-n] [-i interface] [-s snaplen] [-f services] [-t trigger[,...]]] [-r|-w savefile] [expres- sion]`

Dsniff: Screenshot



```
C:\Documents and Settings\Administrator\Desktop\Ethical Hacking and Countermeasu
res v3.1\Module 7 - Sniffers\dsniff-win32\dsniff-1.8-win32-static>dsniff
-----------------
07/08/04 18:49:41 vindows -> 202.129.165.122 (pop)
USER jason
PASS rubin
```

Linux Tool: Filesnarf

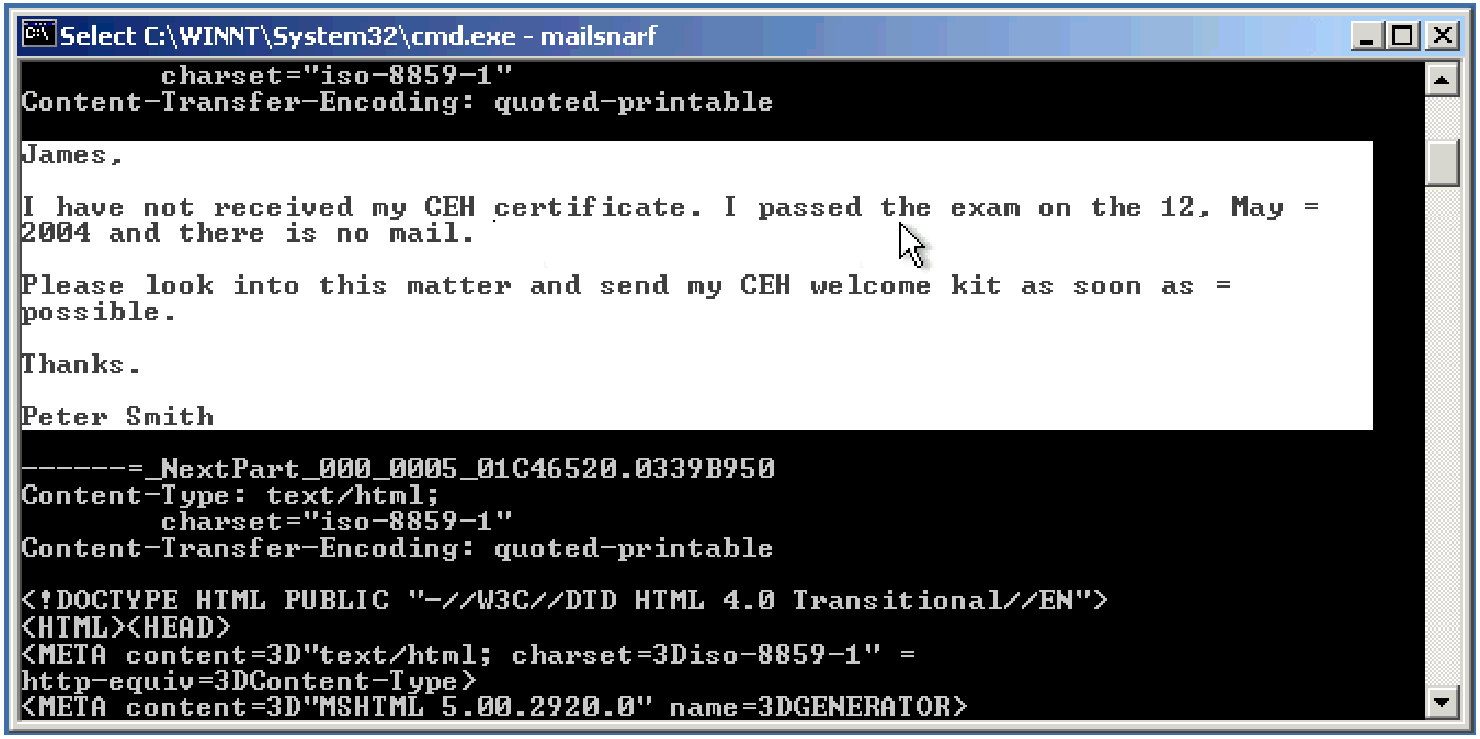
Filesnarf saves files sniffed from NFS traffic in the current working directory

- `filesnarf [-i interface] [[-v] pattern [expression]]`

Linux Tool: Mailsnarf

Mailsnarf outputs email messages sniffed from SMTP and POP traffic in Berkeley mbox format, suitable for offline browsing with your favorite mail reader

- `mailsnarf [-i interface] [[-v] pattern [expression]]`



```
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

James,

I have not received my CEH certificate. I passed the exam on the 12, May =
2004 and there is no mail.

Please look into this matter and send my CEH welcome kit as soon as =
possible.

Thanks.

Peter Smith

------=_NextPart_000_0005_01C46520.0339B950
Content-Type: text/html;
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META content=3D"text/html; charset=3Diso-8859-1" =
http-equiv=3DContent-Type>
<META content=3D"MSHTML 5.00.2920.0" name=3DGENERATOR>
```

Linux Tool: Msgsnarf

Msgsnarf records the selected messages from AOL Instant Messenger, ICQ 2000, IRC, MSN Messenger, or Yahoo Messenger chat sessions

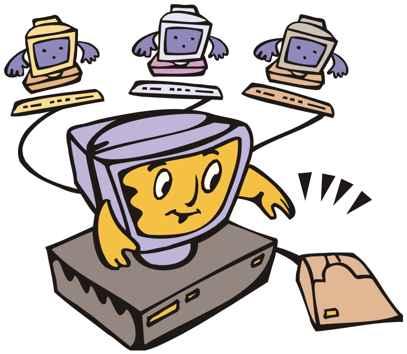
- `msgsnarf [-i interface] [[-v] pattern [expression]`

Linux Tool: Sshmitm

Sshmitm proxies and sniffs SSH traffic redirected by dnsspoof capturing SSH password logins, and optionally hijacking interactive sessions

Only SSH protocol version 1 is (or ever will be) supported

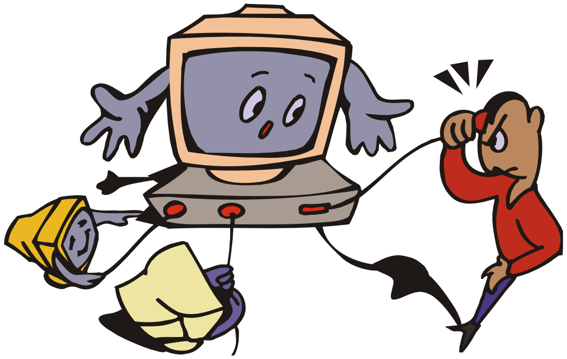
- `sshmitm [-d] [-I] [-p port] host [port]`



Linux Tool: Tcpkill

Tcpkill kills specified in-progress TCP connections (useful for libnids-based applications which require a full TCP 3-way handshake for TCB creation)

- `tcpkill [-i interface] [-1...9] expression`



Linux Tool: Tcpnice

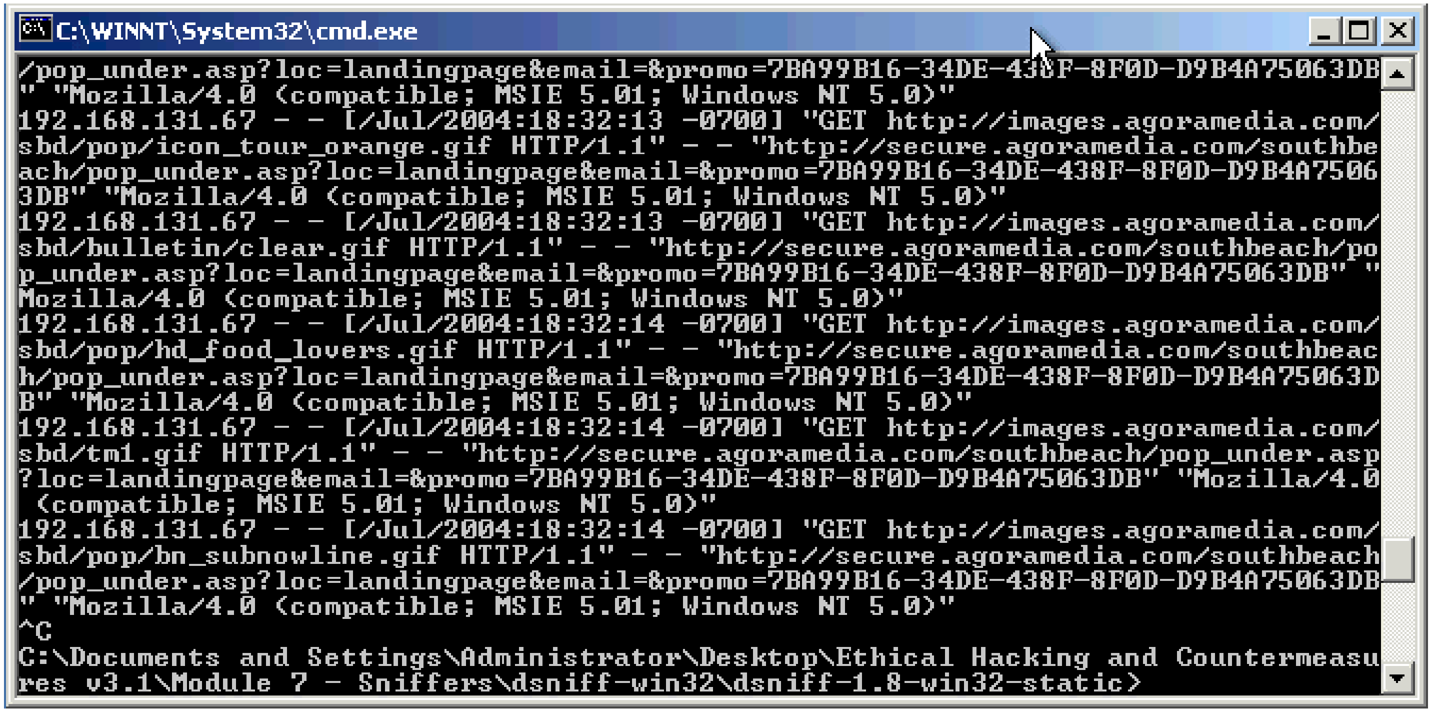
Tcpnice slows down the specified TCP connections on a LAN via active traffic shaping

- `tcpnice [-I] [-i interface] [-n increment] expression`

Linux Tool: Urlsnarf

Urlsnarf outputs all requested URLs sniffed from HTTP traffic in CLF (Common Log Format, used by almost all web servers), suitable for offline post-processing with your favorite web log analysis tool (analog, wwwstat, and so on)

- `urlsnarf [-n] [-i interface] [[-v] pattern [expression]]`



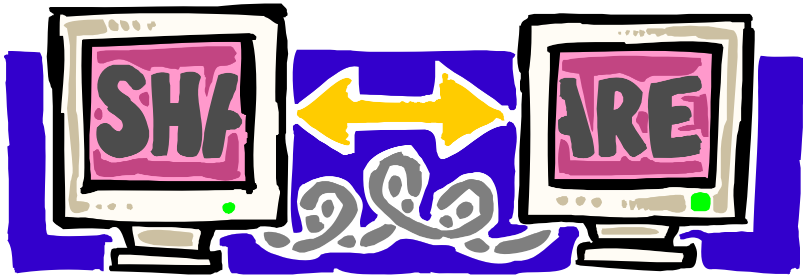
```
/pop_under.asp?loc=landingpage&email=&promo=7BA99B16-34DE-438F-8F0D-D9B4A75063DB
" "Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"
192.168.131.67 - - [/Jul/2004:18:32:13 -0700] "GET http://images.agoramedia.com/
sbd/pop/icon_tour_orange.gif HTTP/1.1" - - "http://secure.agoramedia.com/southbe
ach/pop_under.asp?loc=landingpage&email=&promo=7BA99B16-34DE-438F-8F0D-D9B4A7506
3DB" "Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"
192.168.131.67 - - [/Jul/2004:18:32:13 -0700] "GET http://images.agoramedia.com/
sbd/bulletin/clear.gif HTTP/1.1" - - "http://secure.agoramedia.com/southbeach/po
p_under.asp?loc=landingpage&email=&promo=7BA99B16-34DE-438F-8F0D-D9B4A75063DB" "
Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"
192.168.131.67 - - [/Jul/2004:18:32:14 -0700] "GET http://images.agoramedia.com/
sbd/pop/hd_food_lovers.gif HTTP/1.1" - - "http://secure.agoramedia.com/southbeac
h/pop_under.asp?loc=landingpage&email=&promo=7BA99B16-34DE-438F-8F0D-D9B4A75063D
B" "Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"
192.168.131.67 - - [/Jul/2004:18:32:14 -0700] "GET http://images.agoramedia.com/
sbd/tm1.gif HTTP/1.1" - - "http://secure.agoramedia.com/southbeach/pop_under.asp
?loc=landingpage&email=&promo=7BA99B16-34DE-438F-8F0D-D9B4A75063DB" "Mozilla/4.0
 (compatible; MSIE 5.01; Windows NT 5.0)"
192.168.131.67 - - [/Jul/2004:18:32:14 -0700] "GET http://images.agoramedia.com/
sbd/pop/bn_subnowline.gif HTTP/1.1" - - "http://secure.agoramedia.com/southbeach
/pop_under.asp?loc=landingpage&email=&promo=7BA99B16-34DE-438F-8F0D-D9B4A75063DB
" "Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"
^C
C:\Documents and Settings\Administrator\Desktop\Ethical Hacking and Countermeasu
res v3.1\Module 7 - Sniffers\dsniff-win32\dsniff-1.8-win32-static>
```

Linux Tool: Webspy

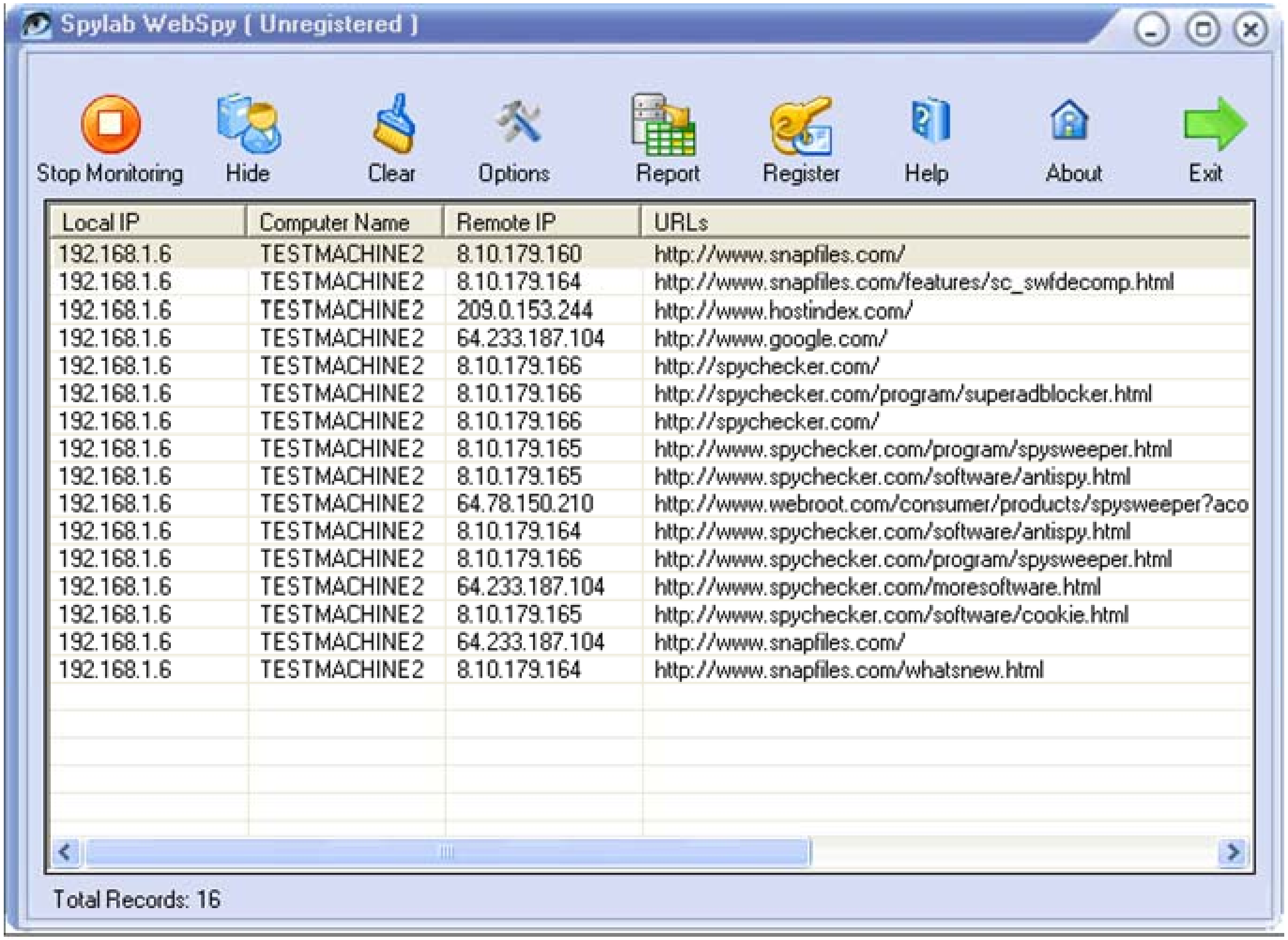
Webspy sends URLs sniffed from a client to local Netscape browser to display, updated in real time (as target surfs, browser surfs along with them, automatically)

Netscape must be running on your local X display ahead of time

- `webspy [-i interface] host`



Webspy: Screenshot



Local IP	Computer Name	Remote IP	URLs
192.168.1.6	TESTMACHINE2	8.10.179.160	http://www.snapfiles.com/
192.168.1.6	TESTMACHINE2	8.10.179.164	http://www.snapfiles.com/features/sc_swfdecomp.html
192.168.1.6	TESTMACHINE2	209.0.153.244	http://www.hostindex.com/
192.168.1.6	TESTMACHINE2	64.233.187.104	http://www.google.com/
192.168.1.6	TESTMACHINE2	8.10.179.166	http://spychecker.com/
192.168.1.6	TESTMACHINE2	8.10.179.166	http://spychecker.com/program/superadblocker.html
192.168.1.6	TESTMACHINE2	8.10.179.166	http://spychecker.com/
192.168.1.6	TESTMACHINE2	8.10.179.165	http://www.spychecker.com/program/spysweeper.html
192.168.1.6	TESTMACHINE2	8.10.179.165	http://www.spychecker.com/software/antispy.html
192.168.1.6	TESTMACHINE2	64.78.150.210	http://www.webroot.com/consumer/products/spysweeper?aco
192.168.1.6	TESTMACHINE2	8.10.179.164	http://www.spychecker.com/software/antispy.html
192.168.1.6	TESTMACHINE2	8.10.179.166	http://www.spychecker.com/program/spysweeper.html
192.168.1.6	TESTMACHINE2	64.233.187.104	http://www.spychecker.com/moresoftware.html
192.168.1.6	TESTMACHINE2	8.10.179.165	http://www.spychecker.com/software/cookie.html
192.168.1.6	TESTMACHINE2	64.233.187.104	http://www.snapfiles.com/
192.168.1.6	TESTMACHINE2	8.10.179.164	http://www.snapfiles.com/whatsnew.html

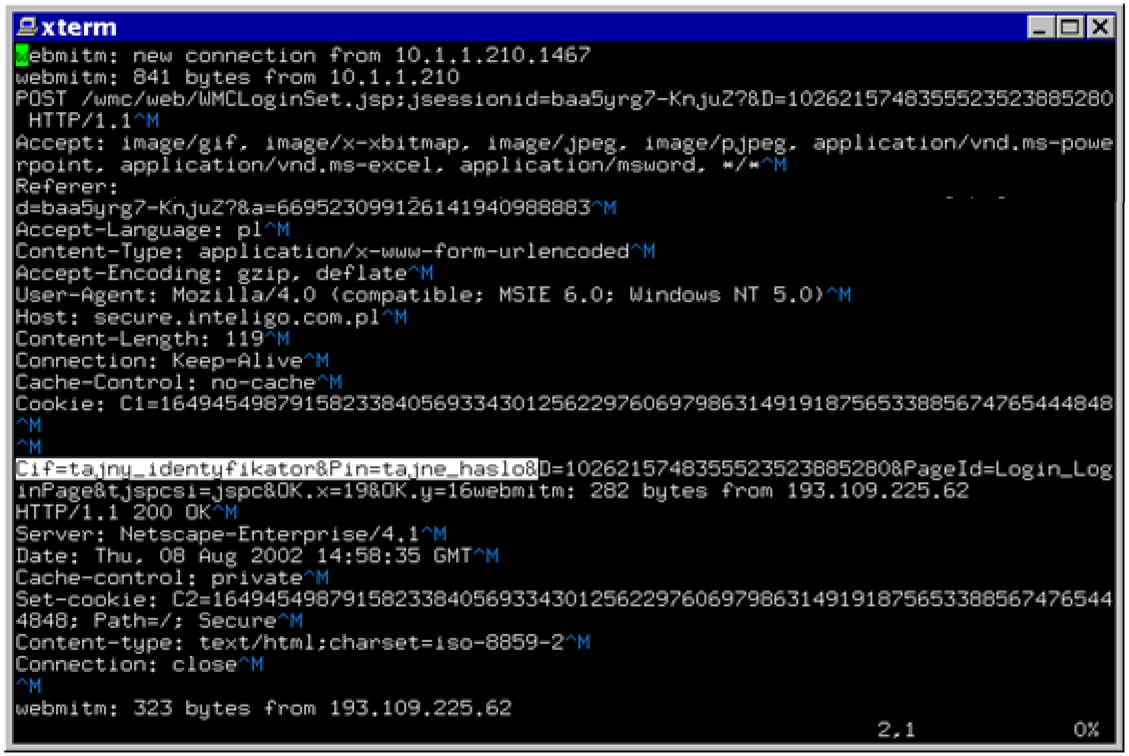
Total Records: 16

Certified Ethical Hacker

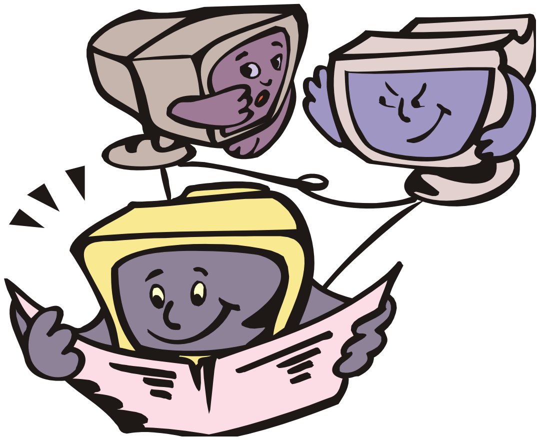
Linux Tool: Webmitm

Webmitm transparently proxies and sniffs HTTP/HTTPS traffic redirected by dnsspoof, capturing most secure SSL-encrypted webmail logins and form submissions

- **webmitm [-d]**



```
webmitm: new connection from 10.1.1.210.1467
webmitm: 841 bytes from 10.1.1.210
POST /wmc/web/WMCLoginSet.jsp;jsessionid=baa5yrg7-KnjuZ?&D=1026215748355523523885280
 HTTP/1.1^M
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-powe
rpoint, application/vnd.ms-excel, application/msword, */*^M
Referer:
d=baa5yrg7-KnjuZ?&a=669523099126141940988883^M
Accept-Language: pl^M
Content-Type: application/x-www-form-urlencoded^M
Accept-Encoding: gzip, deflate^M
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)^M
Host: secure.inteligo.com.pl^M
Content-Length: 119^M
Connection: Keep-Alive^M
Cache-Control: no-cache^M
Cookie: C1=1649454987915823384056933430125622976069798631491918756533885674765444848
^M
^M
Cif=tajny_identyfikator&Pin=tajne_haslo&D=1026215748355523523885280&PageId=Login_Log
inPage&tjspcsi=jspc&OK.x=19&OK.y=16webmitm: 282 bytes from 193.109.225.62
HTTP/1.1 200 OK^M
Server: Netscape-Enterprise/4.1^M
Date: Thu, 08 Aug 2002 14:58:35 GMT^M
Cache-control: private^M
Set-cookie: C2=164945498791582338405693343012562297606979863149191875653388567476544
4848; Path=/; Secure^M
Content-type: text/html;charset=iso-8859-2^M
Connection: close^M
^M
webmitm: 323 bytes from 193.109.225.62
                                                                     2,1          0%
```



DNS Poisoning Techniques

DNS Poisoning Techniques

The substitution of a false Internet provider address at the domain name service level (e.g., where web addresses are converted into numeric Internet provider addresses)

DNS poisoning is a technique that tricks a DNS server into believing that it has received authentic information when, in reality, it has not

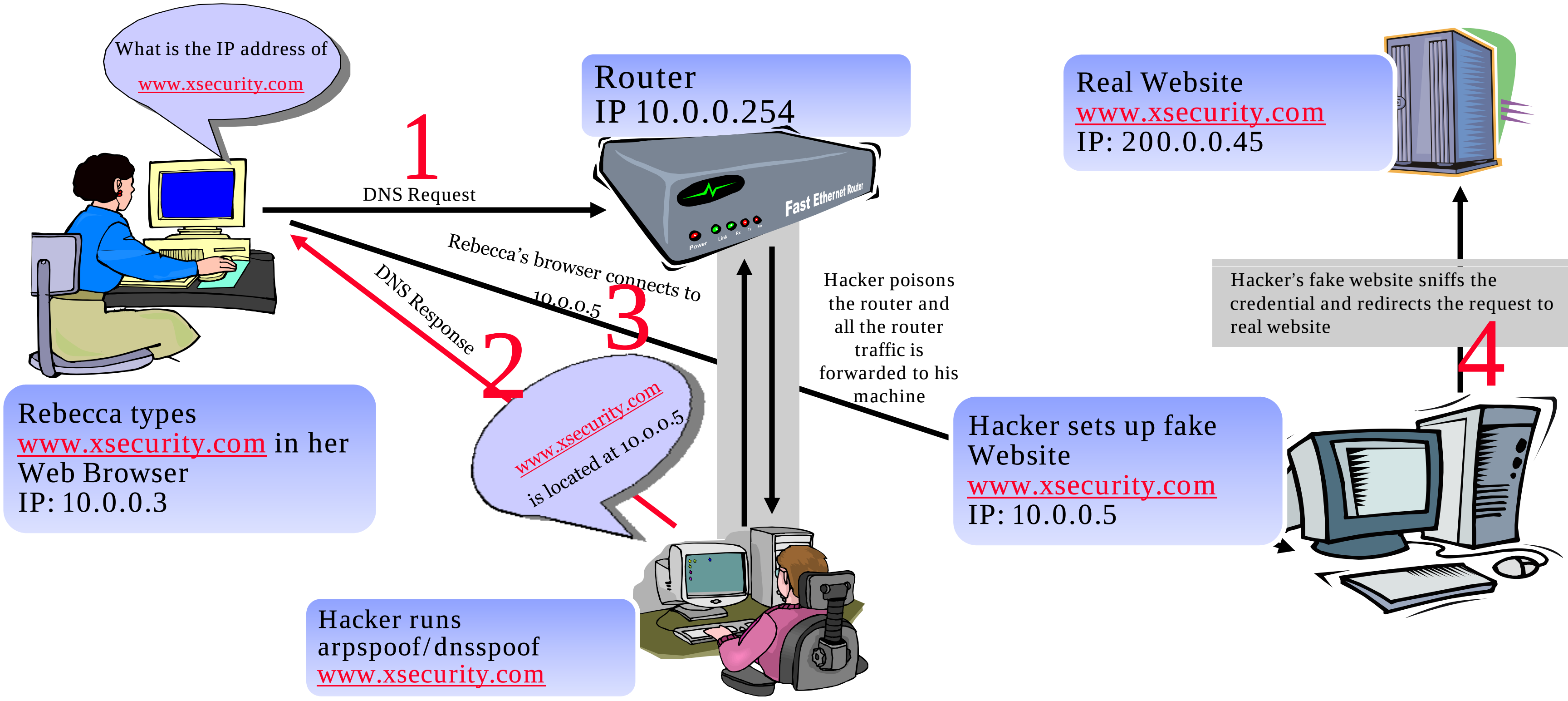
Types of DNS Poisoning:

- Intranet DNS Spoofing (Local network)
- Internet DNS Spoofing (Remote network)
- Proxy Server DNS Poisoning
- DNS Cache Poisoning

1. Intranet DNS Spoofing (Local Network)

For this technique, you must be connected to the local area network (LAN) and be able to sniff packets

It works well against switches with ARP poisoning the router



What is the IP address of www.xsecurity.com

Router
IP 10.0.0.254

Real Website
www.xsecurity.com
IP: 200.0.0.45

1
DNS Request

Rebecca's browser connects to 10.0.0.5

3

DNS Response

2

Hacker poisons the router and all the router traffic is forwarded to his machine

Hacker's fake website sniffs the credential and redirects the request to real website

4

Rebecca types www.xsecurity.com in her Web Browser
IP: 10.0.0.3

www.xsecurity.com is located at 10.0.0.5

Hacker sets up fake Website
www.xsecurity.com
IP: 10.0.0.5

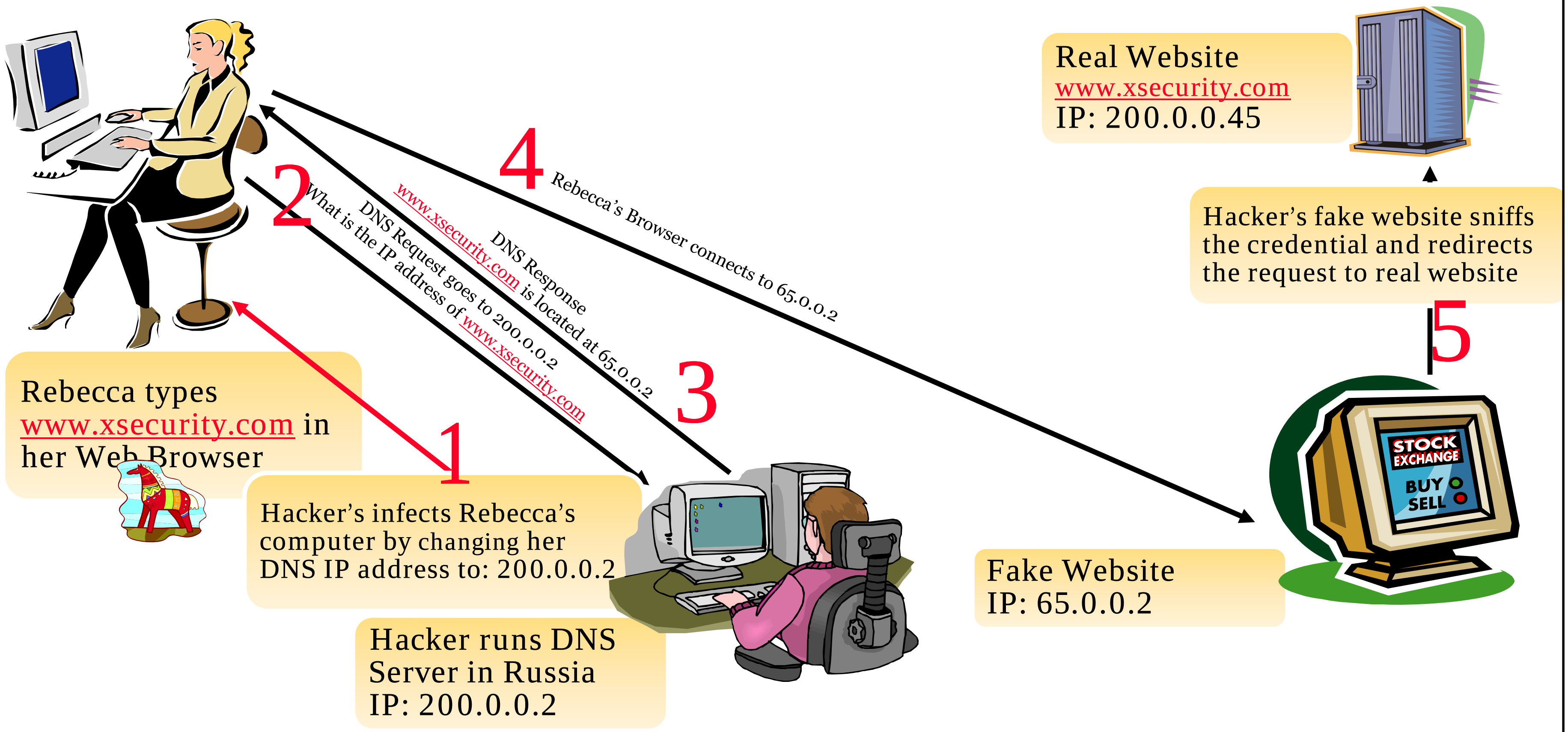
Hacker runs arpspoof/dnsspoof www.xsecurity.com

EC-Council

2. Internet DNS Spoofing (Remote Network)

Internet DNS Spoofing sends a Trojan to Rebecca's machine and changes her DNS IP address to that of the attacker's

It works across networks and is easy to set up and implement



Rebecca types www.xsecurity.com in her Web Browser

1

Hacker's infects Rebecca's computer by changing her DNS IP address to: 200.0.0.2

2

What is the IP address of www.xsecurity.com

DNS Request goes to 200.0.0.2

Hacker runs DNS Server in Russia
IP: 200.0.0.2

3

DNS Response www.xsecurity.com is located at 65.0.0.2

4

Rebecca's Browser connects to 65.0.0.2

Fake Website
IP: 65.0.0.2

5

Hacker's fake website sniffs the credential and redirects the request to real website

Real Website
www.xsecurity.com
IP: 200.0.0.45

Internet DNS Spoofing

To redirect all DNS request traffic going from the host machine to come to you

1. Set up a fake website on your computer

2. Install treewalk and modify the file mentioned in readme.txt to your IP address; Treewalk will make you the DNS server

3. Modify file dns-spoofing.bat and replace the IP address with your IP address

4. Trojanize the **`dns-spoofing.bat`** file and send it to Jessica (**`ex: chess.exe`**)

5. When host clicks trojaned file, it will replace Jessica's DNS entry in her TCP/IP properties with that of your machine's

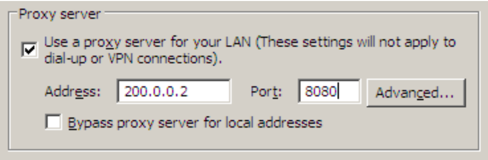
6. You will become the DNS server for Jessica and her DNS requests will go through you

7. When Jessica connects to XSECURITY.com, she resolves to fake XSECURITY website; you sniff the password and send her to the real website

3. Proxy Server DNS Poisoning

Send a Trojan to Rebecca's machine and change her proxy server settings in Internet Explorer to that of the attacker's

It works across networks and is easy to set up and implement



Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 200.0.0.2 Port: 8080 Advanced...

☐ Bypass proxy server for local addresses

Rebecca types www.xsecurity.com in her Web Browser

1

Hacker's infects Rebecca's computer by changing her IE Proxy address to: 200.0.0.2

2

All Rebecca's Web requests goes through Hacker's machine

Hacker runs Proxy Server in Russia
IP: 200.0.0.2

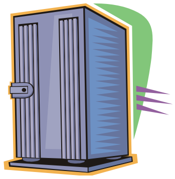
3

Hacker sends Rebecca's request to Fake website

Fake Website
IP: 65.0.0.2

4

Hacker's fake website sniffs the credential and redirects the request to the real website



Real Website
www.xsecurity.com
IP: 200.0.0.45

EC-Council

4. DNS Cache Poisoning

To perform a cache poisoning attack, the attacker exploits a flaw in the DNS server software that can make it accept incorrect information

If the server does not correctly validate DNS responses to ensure that they have come from an authoritative source, the server will end up caching the incorrect entries locally and serve them to users that make the same request

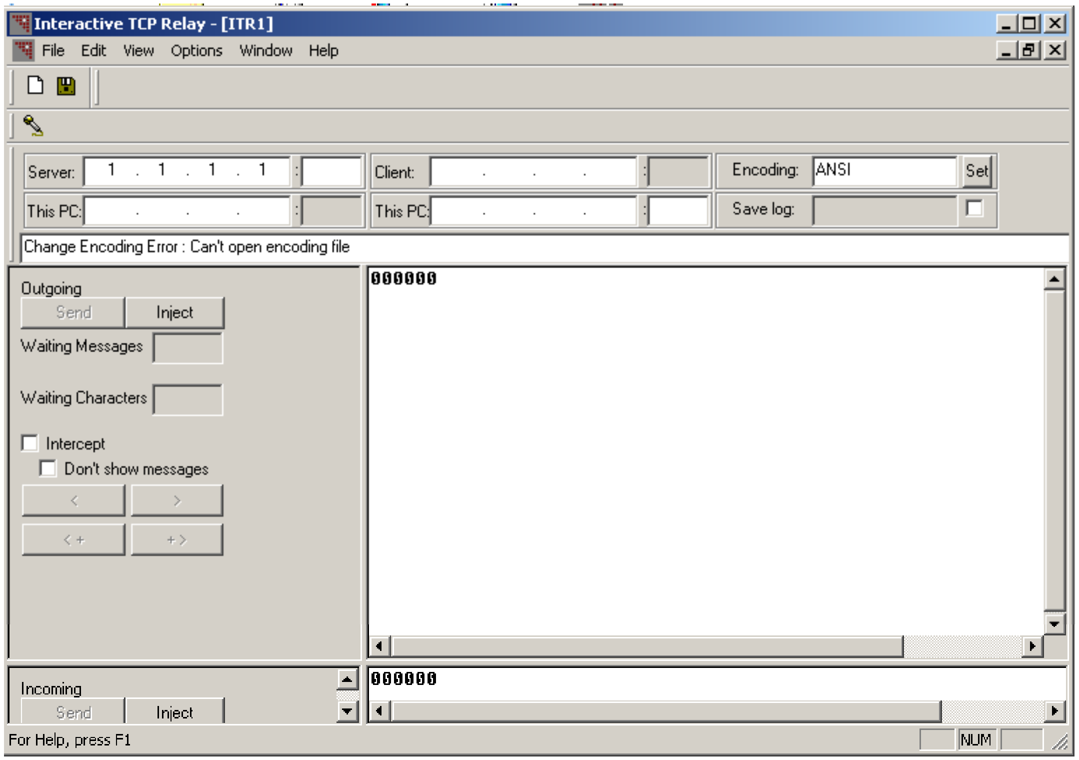
- For example, an attacker poisons the IP address DNS entries for a target website on a given DNS server, replacing them with the IP address of a server he/she controls
- He then creates fake entries for files on the server he/she controls with names matching those on the target server

Interactive TCP Relay

Interactive TCP Relay operates as a simple TCP tunnel listening on a specific port and forwarding all traffic to the remote host and port

The program can intercept and edit the traffic passing through it

The traffic can be edited with the built-in HEX editor



Server: 1 . 1 . 1 . 1

Encoding: ANSI

Change Encoding Error : Can't open encoding file

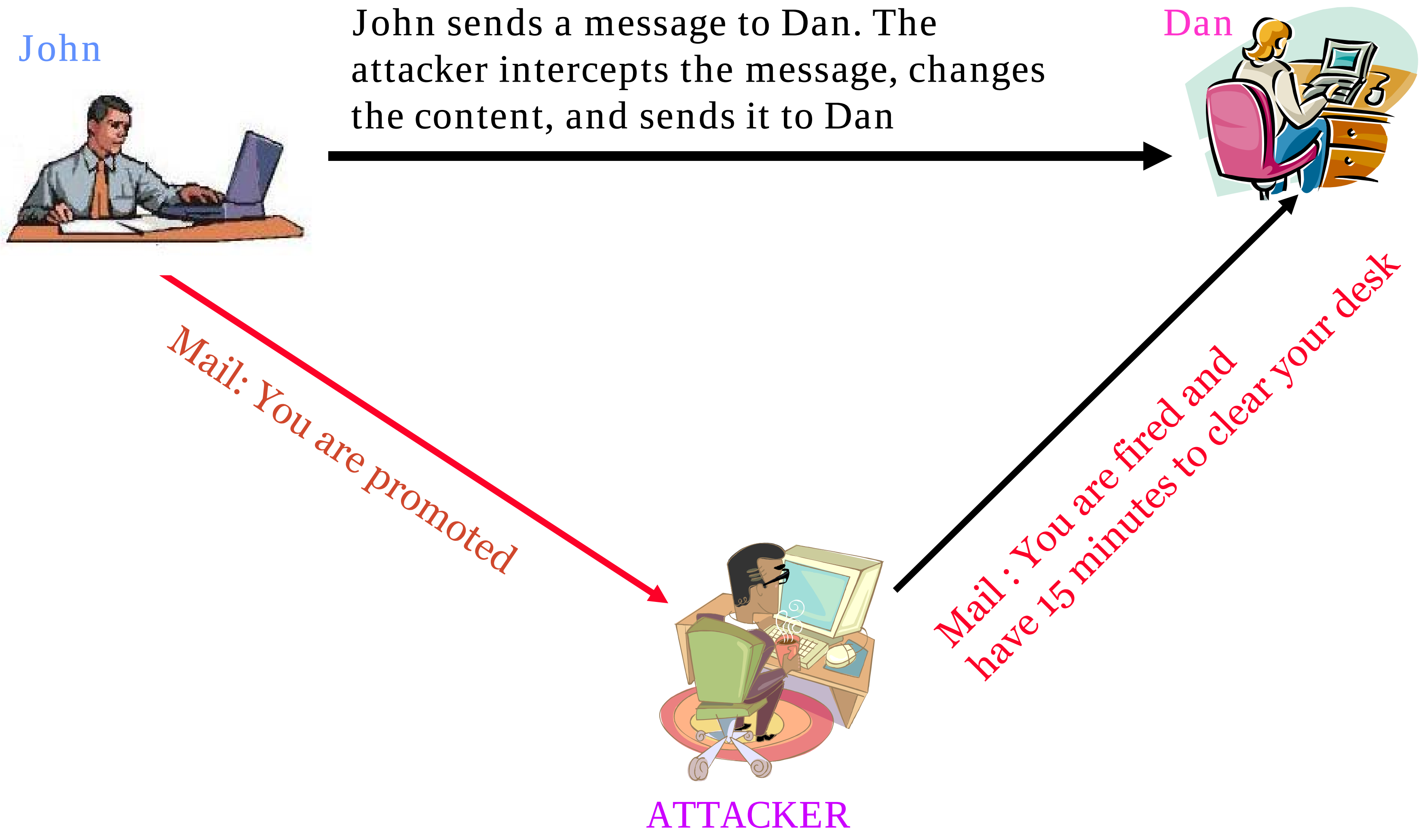
000000

000000

For Help, press F1

Interactive Replay Attacks

John sends a message to Dan. The attacker intercepts the message, changes the content, and sends it to Dan



Raw Sniffing Tools

Certified Ethical Hacker

Raw Sniffing Tools

- Sniffit
- Aldebaran
- Hunt
- NGSSniff
- Ntop
- pf
- IPTraf
- Etherape

- Snort
- Windump/tcpdump
- Etherpeek
- Mac Changer
- Iris
- NetIntercept
- WinDNSSpoof

CEH Certified Ethical Hacker™

Features of Raw Sniffing Tools

Data can be intercepted “off the wire” from a live network connection, or read from a captured file

It can read the captured files from tcpdump

Command line switches to the editcap program that enables the editing or conversion of the captured files

Display filter enables the refinement of the data

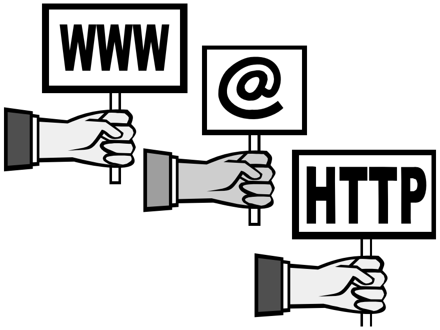
HTTP Sniffer: EffeTech

An HTTP protocol packet sniffer and network analyzer

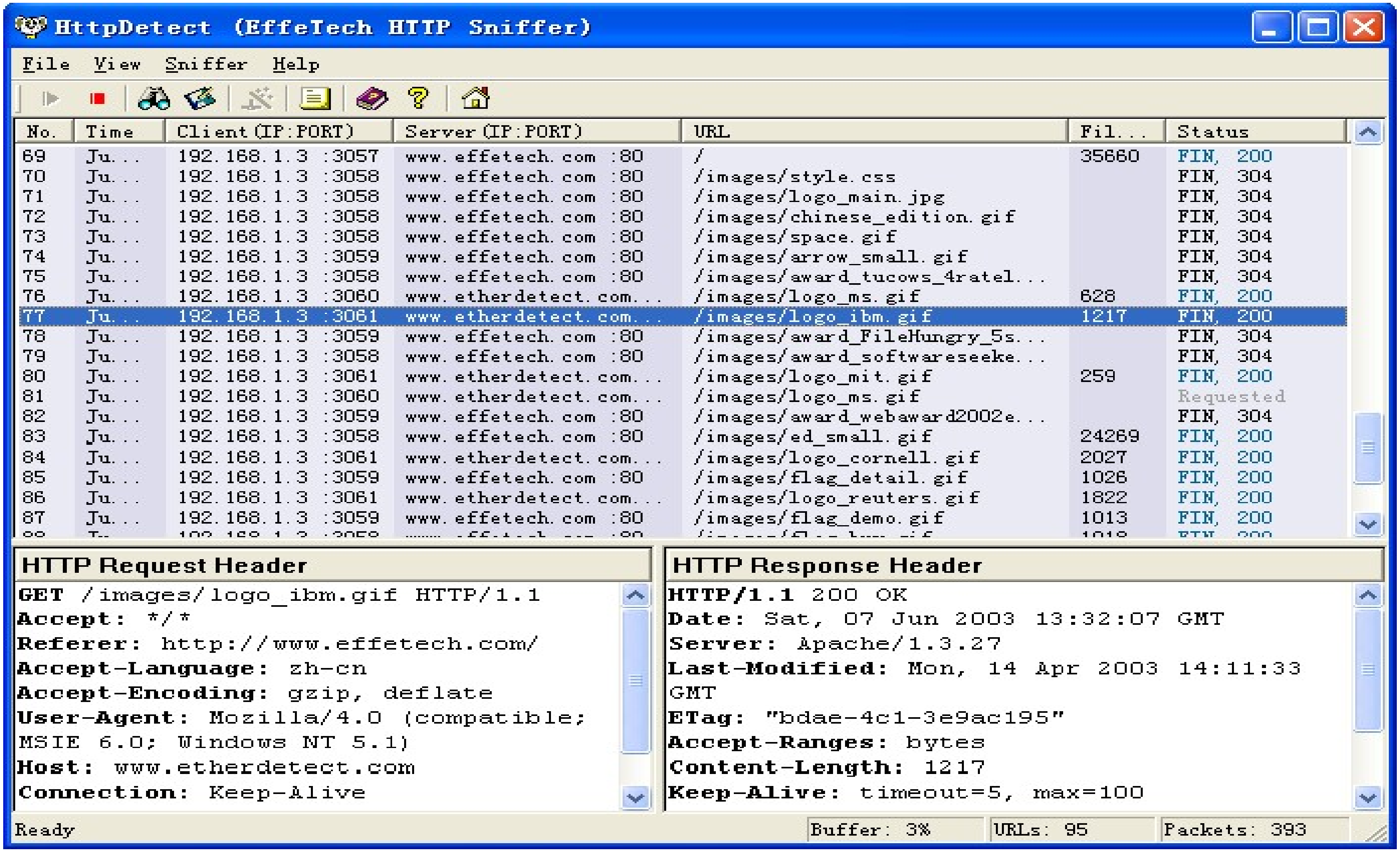
It captures IP packets containing HTTP protocol

It enables on-the-fly content viewing while monitoring and analyzing

It parses and decodes the HTTP protocol, and generates a web traffic report for reference



HTTP Sniffer: EffeTech



No.	Time	Client (IP:PORT)	Server (IP:PORT)	URL	Fil...	Status
69	Ju...	192.168.1.3 :3057	www.effetech.com :80	/	35660	FIN, 200
70	Ju...	192.168.1.3 :3058	www.effetech.com :80	/images/style.css		FIN, 304
71	Ju...	192.168.1.3 :3058	www.effetech.com :80	/images/logo_main.jpg		FIN, 304
72	Ju...	192.168.1.3 :3058	www.effetech.com :80	/images/chinese_edition.gif		FIN, 304
73	Ju...	192.168.1.3 :3058	www.effetech.com :80	/images/space.gif		FIN, 304
74	Ju...	192.168.1.3 :3059	www.effetech.com :80	/images/arrow_small.gif		FIN, 304
75	Ju...	192.168.1.3 :3058	www.effetech.com :80	/images/award_tucows_4ratel...		FIN, 304
76	Ju...	192.168.1.3 :3060	www.etherdetect.com...	/images/logo_ms.gif	628	FIN, 200
77	Ju...	192.168.1.3 :3061	www.etherdetect.com...	/images/logo_ibm.gif	1217	FIN, 200
78	Ju...	192.168.1.3 :3059	www.effetech.com :80	/images/award_FileHungry_5s...		FIN, 304
79	Ju...	192.168.1.3 :3058	www.effetech.com :80	/images/award_softwareseeke...		FIN, 304
80	Ju...	192.168.1.3 :3061	www.etherdetect.com...	/images/logo_mit.gif	259	FIN, 200
81	Ju...	192.168.1.3 :3060	www.etherdetect.com...	/images/logo_ms.gif		Requested
82	Ju...	192.168.1.3 :3059	www.effetech.com :80	/images/award_webaward2002e...		FIN, 304
83	Ju...	192.168.1.3 :3058	www.effetech.com :80	/images/ed_small.gif	24269	FIN, 200
84	Ju...	192.168.1.3 :3061	www.etherdetect.com...	/images/logo_cornell.gif	2027	FIN, 200
85	Ju...	192.168.1.3 :3059	www.effetech.com :80	/images/flag_detail.gif	1026	FIN, 200
86	Ju...	192.168.1.3 :3061	www.etherdetect.com...	/images/logo_reuters.gif	1822	FIN, 200
87	Ju...	192.168.1.3 :3059	www.effetech.com :80	/images/flag_demo.gif	1013	FIN, 200

HTTP Request Header

```
GET /images/logo_ibm.gif HTTP/1.1
Accept: */*
Referer: http://www.effetech.com/
Accept-Language: zh-cn
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible;
MSIE 6.0; Windows NT 5.1)
Host: www.etherdetect.com
Connection: Keep-Alive
```

HTTP Response Header

```
HTTP/1.1 200 OK
Date: Sat, 07 Jun 2003 13:32:07 GMT
Server: Apache/1.3.27
Last-Modified: Mon, 14 Apr 2003 14:11:33
GMT
ETag: "bdae-4c1-3e9ac195"
Accept-Ranges: bytes
Content-Length: 1217
Keep-Alive: timeout=5, max=100
```

Ready | Buffer: 3% | URLs: 95 | Packets: 393

EC-Council

Ace Password Sniffer

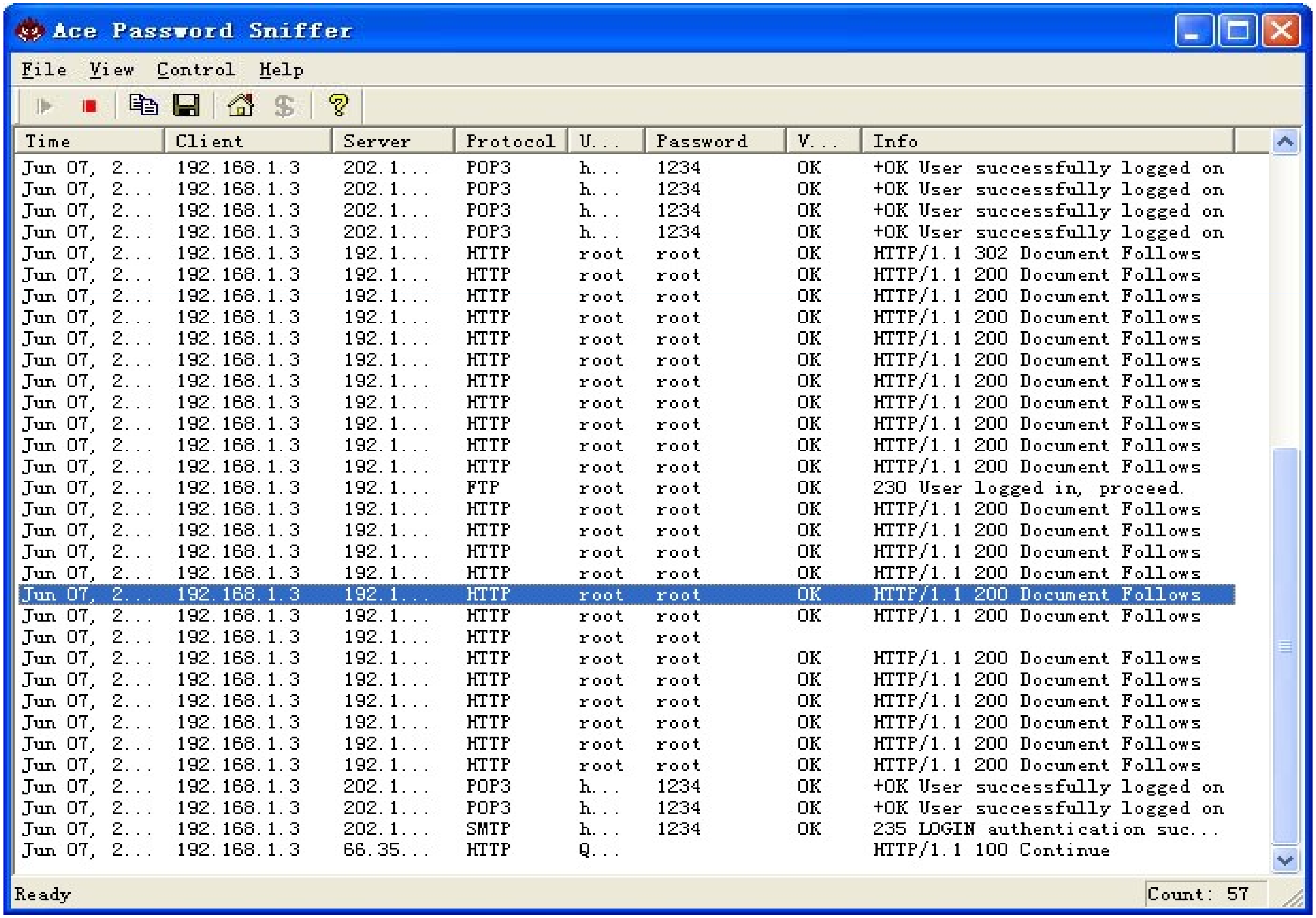
Ace Password Sniffer can monitor and capture passwords through FTP, POP3, HTTP, SMTP, Telnet, and some web mail passwords

It can listen on LAN and capture passwords of any network user

Ace Password Sniffer works passively and is hard to detect

If a network is connected through a switch, the sniffer can be run on the gateway or proxy server, which can get all the network traffic

Ace Password Sniffer: Screenshot



Time	Client	Server	Protocol	U...	Password	V...	Info
Jun 07, 2...	192.168.1.3	202.1...	POP3	h...	1234	OK	+OK User successfully logged on
Jun 07, 2...	192.168.1.3	202.1...	POP3	h...	1234	OK	+OK User successfully logged on
Jun 07, 2...	192.168.1.3	202.1...	POP3	h...	1234	OK	+OK User successfully logged on
Jun 07, 2...	192.168.1.3	202.1...	POP3	h...	1234	OK	+OK User successfully logged on
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 302 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	FTP	root	root	OK	230 User logged in, proceed.
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root		
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	202.1...	POP3	h...	1234	OK	+OK User successfully logged on
Jun 07, 2...	192.168.1.3	202.1...	POP3	h...	1234	OK	+OK User successfully logged on
Jun 07, 2...	192.168.1.3	202.1...	SMTP	h...	1234	OK	235 LOGIN authentication suc...
Jun 07, 2...	192.168.1.3	66.35...	HTTP	Q...			HTTP/1.1 100 Continue

Ready

Count: 57

Win Sniffer

Win Sniffer allows network administrators to capture passwords of any network user

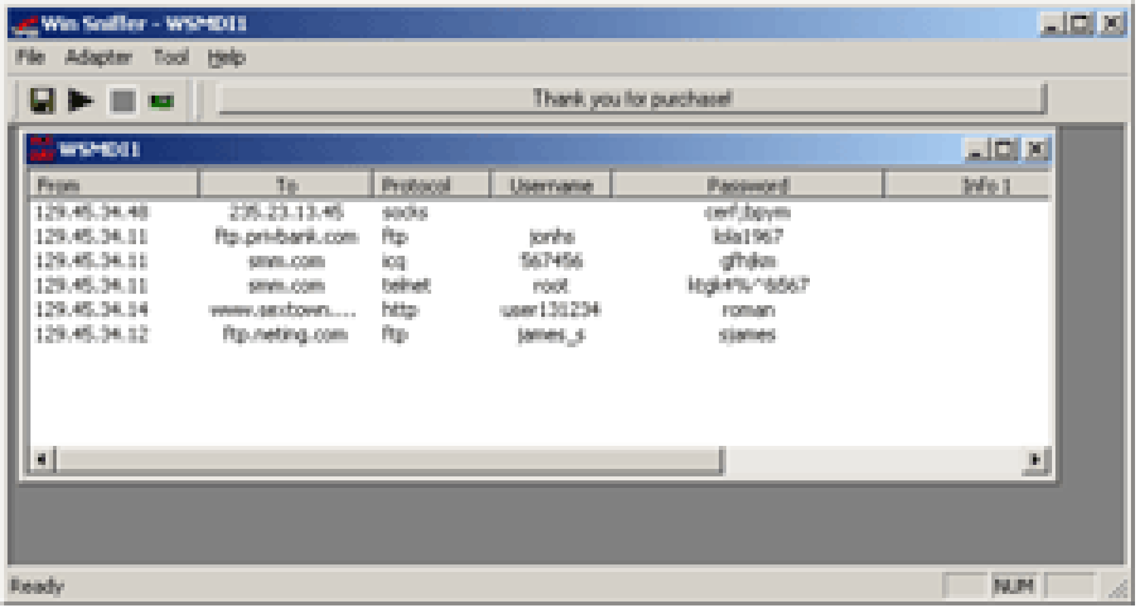
Win Sniffer monitors incoming and outgoing network traffic and decodes FTP, POP3, HTTP, ICQ, SMTP, Telnet, IMAP, and NNTP usernames and passwords

Administrators can assess the danger of clear text passwords in the network and develop ways to improve security using win sniffer

It has integrated technology that allows to reconstruct network traffic in a format that is simple to use and understand

It has one of the most intuitive packet filtering system, allowing you to look only at the desired packets

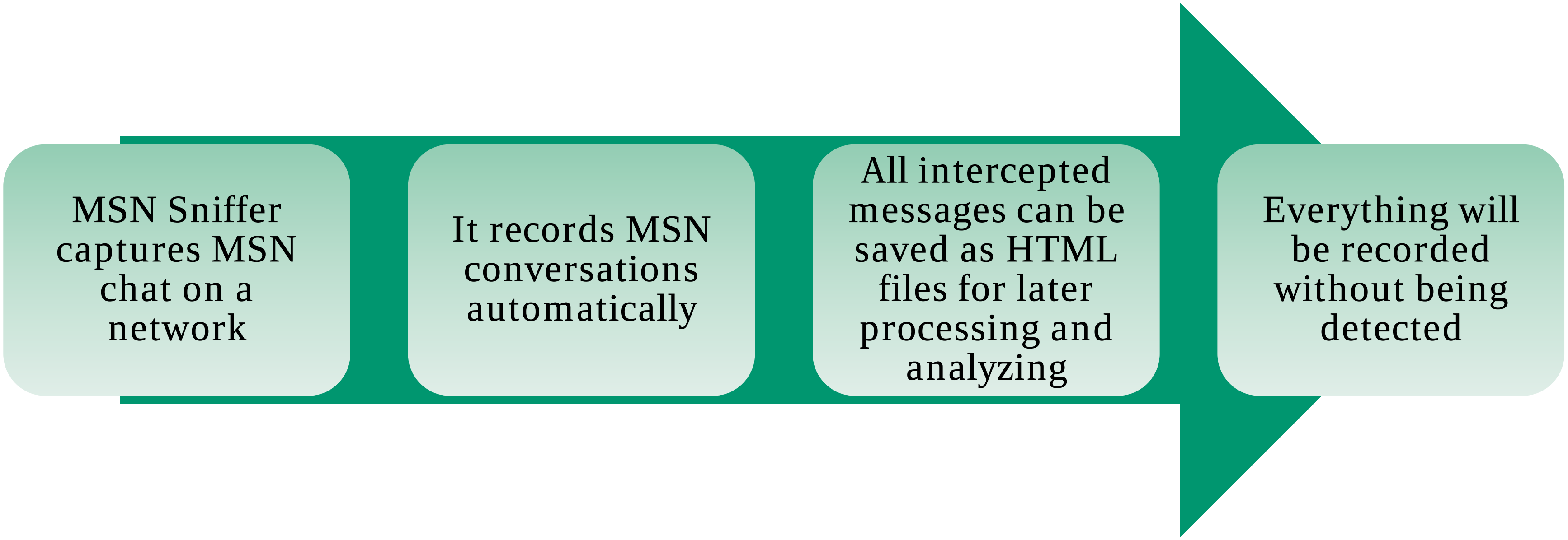
Win Sniffer: Screenshot



Thank you for purchase!

From	To	Protocol	Username	Password	Info 1
129.45.34.48	235.23.13.45	socks		cerf,bpym	
129.45.34.11	ftp.pri-bank.com	ftp	jonhs	lola1967	
129.45.34.11	smm.com	icq	567456	gfhdks	
129.45.34.11	smm.com	telnet	root	ktgj4%^&567	
129.45.34.14	www.sextown....	http	user131234	roman	
129.45.34.12	ftp.neting.com	ftp	james_s	sjames	

MSN Sniffer

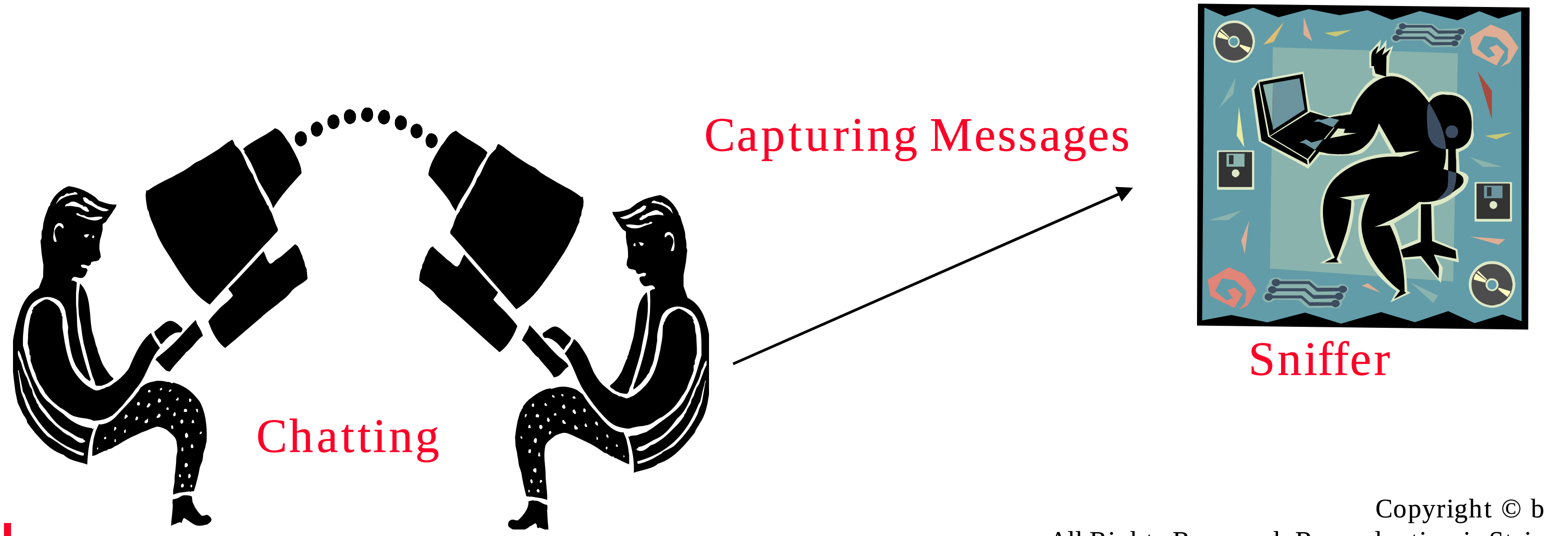


MSN Sniffer captures MSN chat on a network

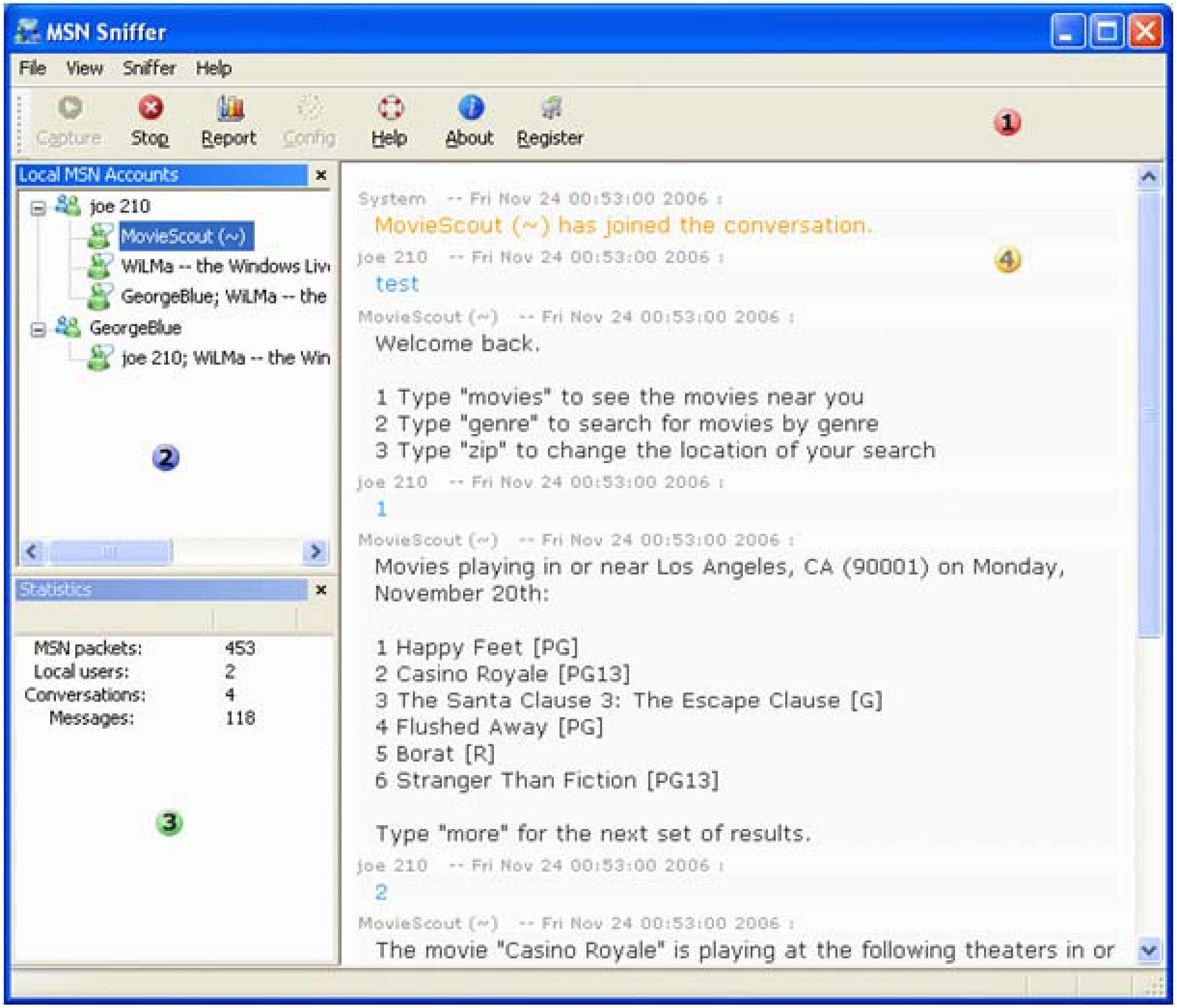
It records MSN conversations automatically

All intercepted messages can be saved as HTML files for later processing and analyzing

Everything will be recorded without being detected



MSN Sniffer: Screenshot



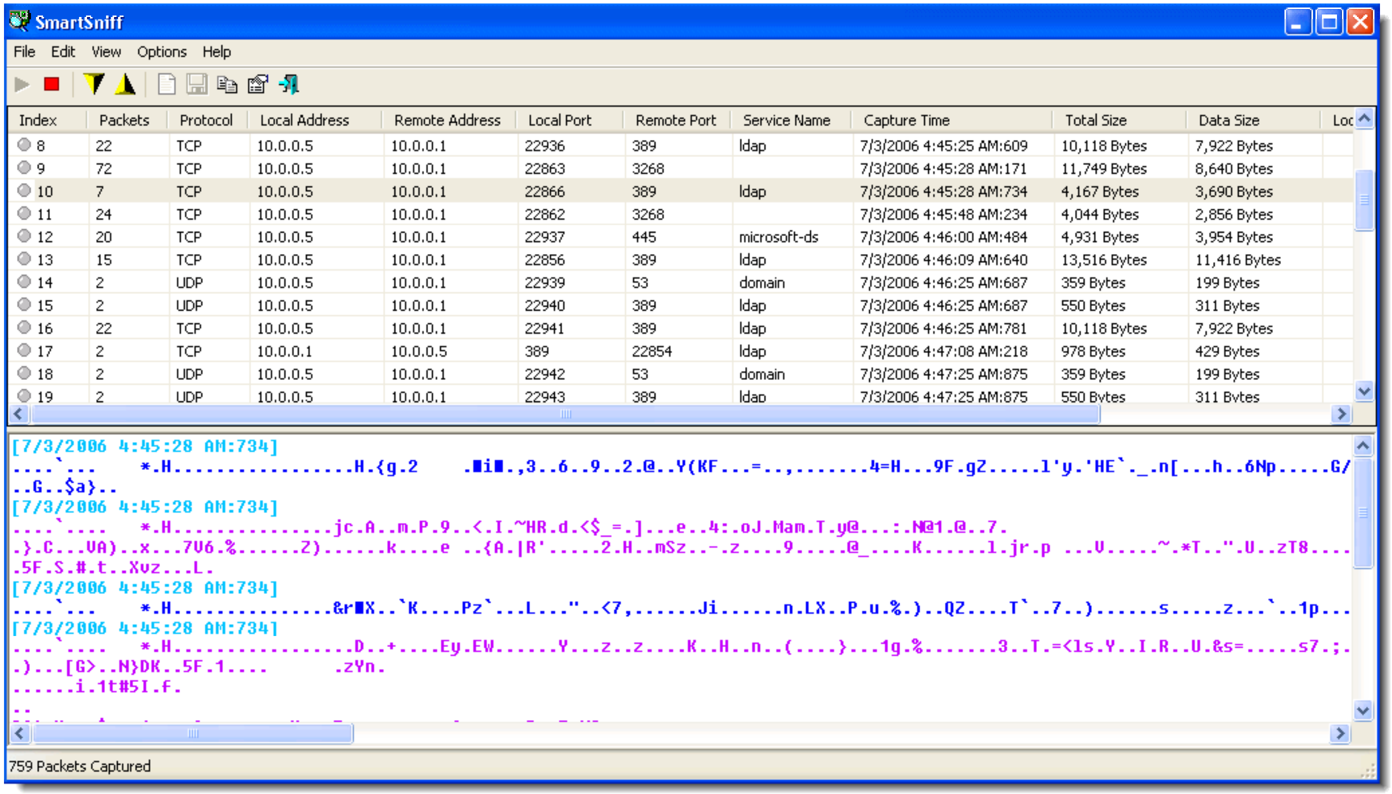
MSN packets:	453
Local users:	2
Conversations:	4
Messages:	118

```
System   -- Fri Nov 24 00:53:00 2006 :
 MovieScout (~) has joined the conversation.
joe 210   -- Fri Nov 24 00:53:00 2006 :
 test
MovieScout (~)   -- Fri Nov 24 00:53:00 2006 :
 Welcome back.

 1 Type "movies" to see the movies near you
 2 Type "genre" to search for movies by genre
 3 Type "zip" to change the location of your search
joe 210   -- Fri Nov 24 00:53:00 2006 :
 1
MovieScout (~)   -- Fri Nov 24 00:53:00 2006 :
 Movies playing in or near Los Angeles, CA (90001) on Monday,
 November 20th:

 1 Happy Feet [PG]
 2 Casino Royale [PG13]
 3 The Santa Clause 3: The Escape Clause [G]
 4 Flushed Away [PG]
 5 Borat [R]
 6 Stranger Than Fiction [PG13]

 Type "more" for the next set of results.
joe 210   -- Fri Nov 24 00:53:00 2006 :
 2
MovieScout (~)   -- Fri Nov 24 00:53:00 2006 :
 The movie "Casino Royale" is playing at the following theaters in or
```

SmartSniff

SmartSniff is a TCP/IP packet capture program that allows you to inspect the network traffic that passes through your network adapter

It is a valuable tool to check what packets your computer is sending to the outside world



Index	Packets	Protocol	Local Address	Remote Address	Local Port	Remote Port	Service Name	Capture Time	Total Size	Data Size	Loc
○ 8	22	TCP	10.0.0.5	10.0.0.1	22936	389	ldap	7/3/2006 4:45:25 AM:609	10,118 Bytes	7,922 Bytes	
○ 9	72	TCP	10.0.0.5	10.0.0.1	22863	3268		7/3/2006 4:45:28 AM:171	11,749 Bytes	8,640 Bytes	
○ 10	7	TCP	10.0.0.5	10.0.0.1	22866	389	ldap	7/3/2006 4:45:28 AM:734	4,167 Bytes	3,690 Bytes	
○ 11	24	TCP	10.0.0.5	10.0.0.1	22862	3268		7/3/2006 4:45:48 AM:234	4,044 Bytes	2,856 Bytes	
○ 12	20	TCP	10.0.0.5	10.0.0.1	22937	445	microsoft-ds	7/3/2006 4:46:00 AM:484	4,931 Bytes	3,954 Bytes	
○ 13	15	TCP	10.0.0.5	10.0.0.1	22856	389	ldap	7/3/2006 4:46:09 AM:640	13,516 Bytes	11,416 Bytes	
○ 14	2	UDP	10.0.0.5	10.0.0.1	22939	53	domain	7/3/2006 4:46:25 AM:687	359 Bytes	199 Bytes	
○ 15	2	UDP	10.0.0.5	10.0.0.1	22940	389	ldap	7/3/2006 4:46:25 AM:687	550 Bytes	311 Bytes	
○ 16	22	TCP	10.0.0.5	10.0.0.1	22941	389	ldap	7/3/2006 4:46:25 AM:781	10,118 Bytes	7,922 Bytes	
○ 17	2	TCP	10.0.0.1	10.0.0.5	389	22854	ldap	7/3/2006 4:47:08 AM:218	978 Bytes	429 Bytes	
○ 18	2	UDP	10.0.0.5	10.0.0.1	22942	53	domain	7/3/2006 4:47:25 AM:875	359 Bytes	199 Bytes	
○ 19	2	UDP	10.0.0.5	10.0.0.1	22943	389	ldap	7/3/2006 4:47:25 AM:875	550 Bytes	311 Bytes	

```
[7/3/2006 4:45:28 AM:734]
....`...     *.H..................H.{g.2     .■i■.,3..6..9..2.@..Y(KF...=..,........4=H...9F.gZ.....l'y.'HE`._.n[...h..6Np.....G/
..G..$a}..
[7/3/2006 4:45:28 AM:734]
....`....    *.H.................jc.A..m.P.9..<.I.~HR.d.<$_=.]...e..4:.oJ.Mam.T.y@...:.N@1.@..7.
.}.C...VA)..x...7V6.%......Z)......k....e ..{A.|R'.....2.H..mSz..-.z....9.....@_....K......l.jr.p ...V.....~.*T..".U..zT8....
.5F.S.#.t..Xvz...L.
[7/3/2006 4:45:28 AM:734]
....`...     *.H.................&r■X..`K....Pz`...L...."..<7,......Ji......n.LX..P.u.%.)..QZ....T`..7..)......s.....z...`..1p...
[7/3/2006 4:45:28 AM:734]
....`....    *.H..................D..+....Ey.EW......Y...z..z....K..H..n..(....}...1g.%.......3..T.=<1s.Y..I.R..U.&s=.....s7.;.
.)...[G>..N}DK..5F.1....       .zYn.
......i.1t#5I.f.
..
```

759 Packets Captured

Session Capture Sniffer: NetWitness

The patented technology recreates "sessions" and displays them on the screen

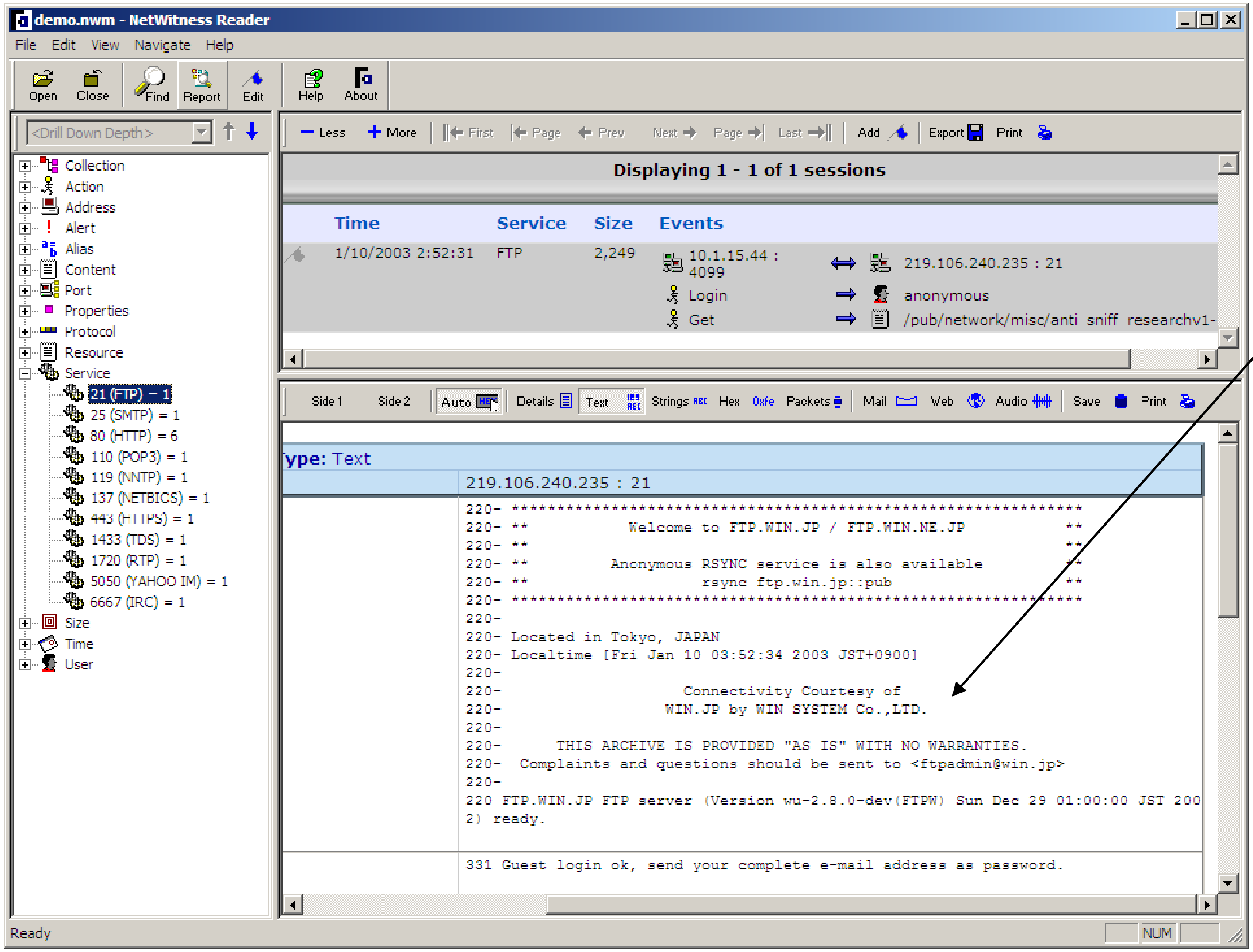
The Law enforcement agencies in the U.S. like FBI use this tool

NetWitness audits and monitors all traffic on the network

It evaluates activities into a format that like-minded network engineers and non-engineers can quickly understand

It records all activities, and transforms the "take" into a dense transactional model describing the network, application, and content levels of those activities

Session Capture Sniffer: NWreader



Displaying 1 - 1 of 1 sessions

Time	Service	Size	Events		
1/10/2003 2:52:31	FTP	2,249	10.1.15.44 : 4099	⇔	219.106.240.235 : 21
			Login	⇒	anonymous
			Get	⇒	/pub/network/misc/anti_sniff_researchv1-

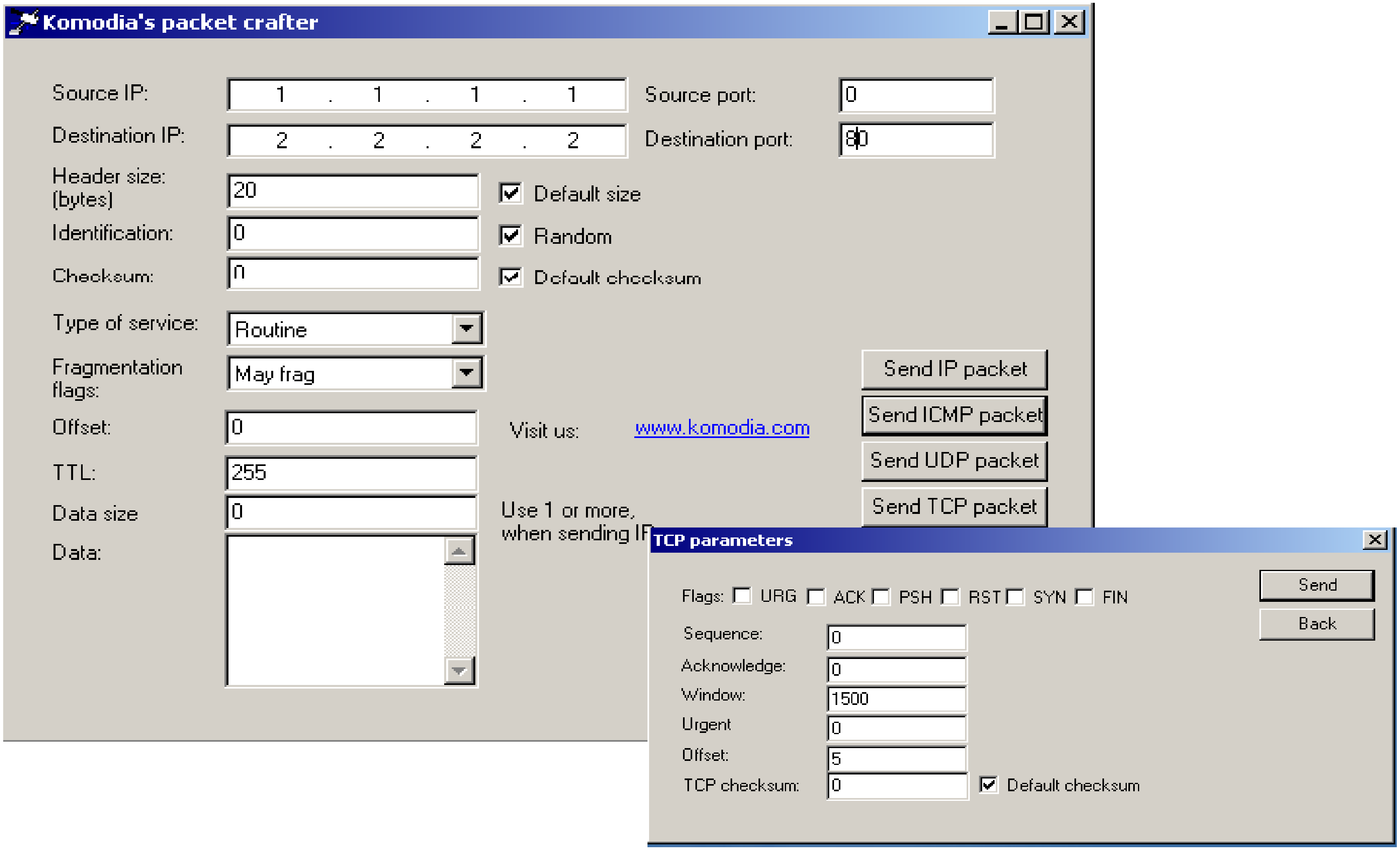
ype: Text

219.106.240.235 : 21

```
220- ********************************************************************
220- **          Welcome to FTP.WIN.JP / FTP.WIN.NE.JP                   **
220- **                                                                  **
220- **        Anonymous RSYNC service is also available                 **
220- **                    rsync ftp.win.jp::pub                         **
220- ********************************************************************
220-
220- Located in Tokyo, JAPAN
220- Localtime [Fri Jan 10 03:52:34 2003 JST+0900]
220-
220-                  Connectivity Courtesy of
220-                 WIN.JP by WIN SYSTEM Co.,LTD.
220-
220-     THIS ARCHIVE IS PROVIDED "AS IS" WITH NO WARRANTIES.
220-  Complaints and questions should be sent to <ftpadmin@win.jp>
220-
220 FTP.WIN.JP FTP server (Version wu-2.8.0-dev(FTPW) Sun Dec 29 01:00:00 JST 200
2) ready.

331 Guest login ok, send your complete e-mail address as password.
```

FTP Sessions captured

Packet Crafter Craft Custom TCP/IP Packets



Source IP: 1 . 1 . 1 . 1

Source port: 0

Destination IP: 2 . 2 . 2 . 2

Destination port: 80

Header size: (bytes) 20 ☑ Default size

Identification: 0 ☑ Random

Checksum: 0 ☑ Default checksum

Type of service: Routine

Fragmentation flags: May frag

Offset: 0

TTL: 255

Data size 0

Data:

Visit us: www.komodia.com

Use 1 or more, when sending IP

Flags: □ URG □ ACK □ PSH □ RST □ SYN □ FIN

Sequence: 0

Acknowledge: 0

Window: 1500

Urgent 0

Offset: 5

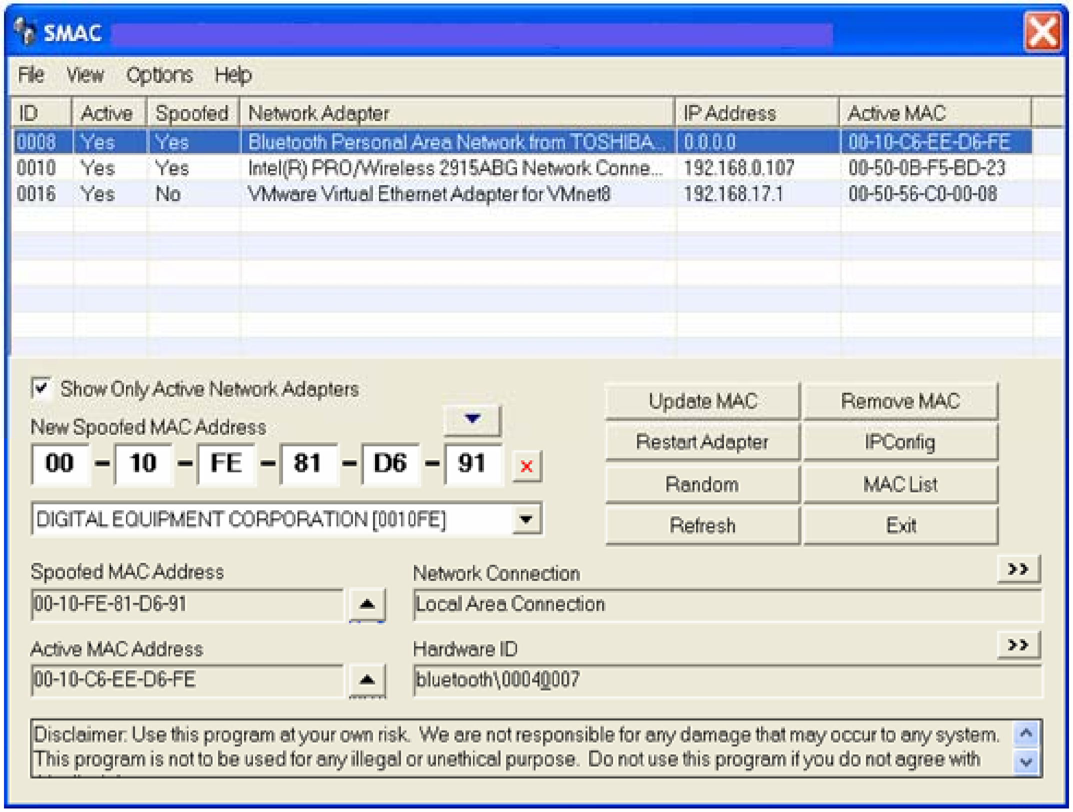
TCP checksum: 0 ☑ Default checksum

SMAC

SMAC is a MAC Address Modifying Utility (spoofer) for Windows 2000, XP, and Server 2003 systems

It displays the network information of available network adapters on one screen

The built-in logging capability allows it to track MAC address modification activities



ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0008	Yes	Yes	Bluetooth Personal Area Network from TOSHIBA...	0.0.0.0	00-10-C6-EE-D6-FE
0010	Yes	Yes	Intel(R) PRO/Wireless 2915ABG Network Conne...	192.168.0.107	00-50-0B-F5-BD-23
0016	Yes	No	VMware Virtual Ethernet Adapter for VMnet8	192.168.17.1	00-50-56-C0-00-08

☑ Show Only Active Network Adapters

New Spoofed MAC Address: 00 - 10 - FE - 81 - D6 - 91

DIGITAL EQUIPMENT CORPORATION [0010FE]

Spoofed MAC Address: 00-10-FE-81-D6-91

Network Connection: Local Area Connection

Active MAC Address: 00-10-C6-EE-D6-FE

Hardware ID: bluetooth\00040007

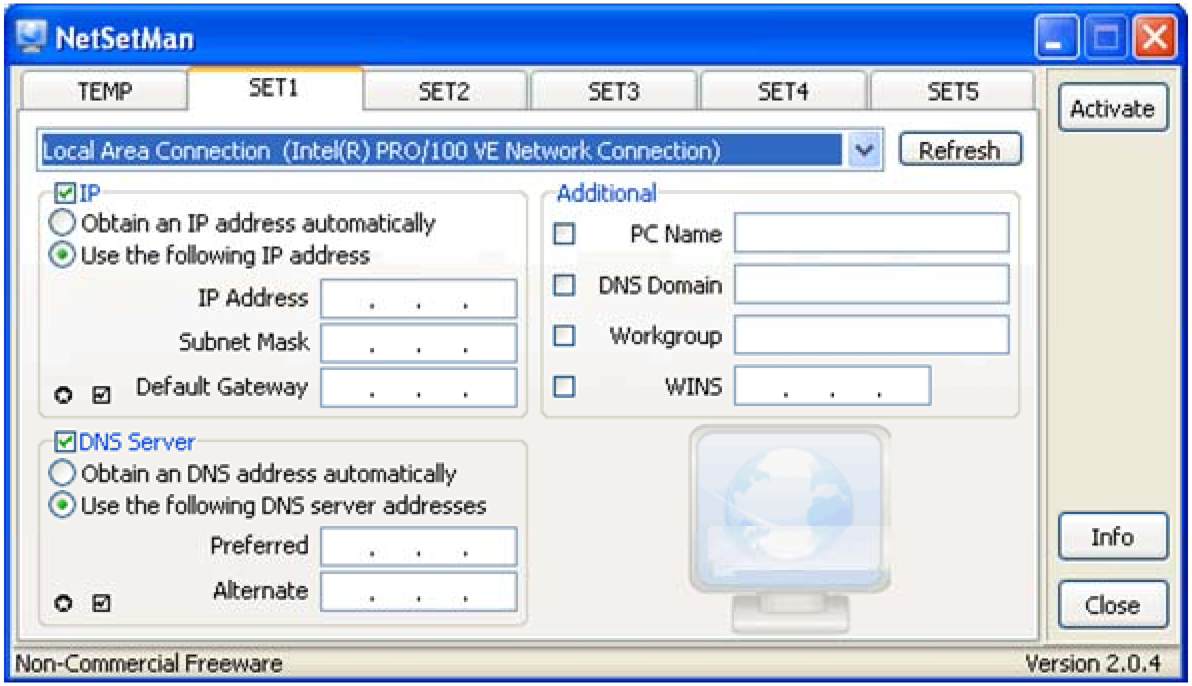
Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system.
This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

NetSetMan Tool

NetSetMan allows you to quickly switch between pre-configured network settings

It is ideal for ethical hackers who have to connect to different networks all the time and need to update their network settings each time

It allows you to create 6 profiles including IP address settings, Subnet Mask, Default Gateway, and DNS servers



Local Area Connection (Intel(R) PRO/100 VE Network Connection)

☑ IP

○ Obtain an IP address automatically

● Use the following IP address

IP Address . . .

Subnet Mask . . .

Default Gateway . . .

Additional

□ PC Name

□ DNS Domain

□ Workgroup

□ WINS . . .

☑ DNS Server

○ Obtain an DNS address automatically

● Use the following DNS server addresses

Preferred . . .

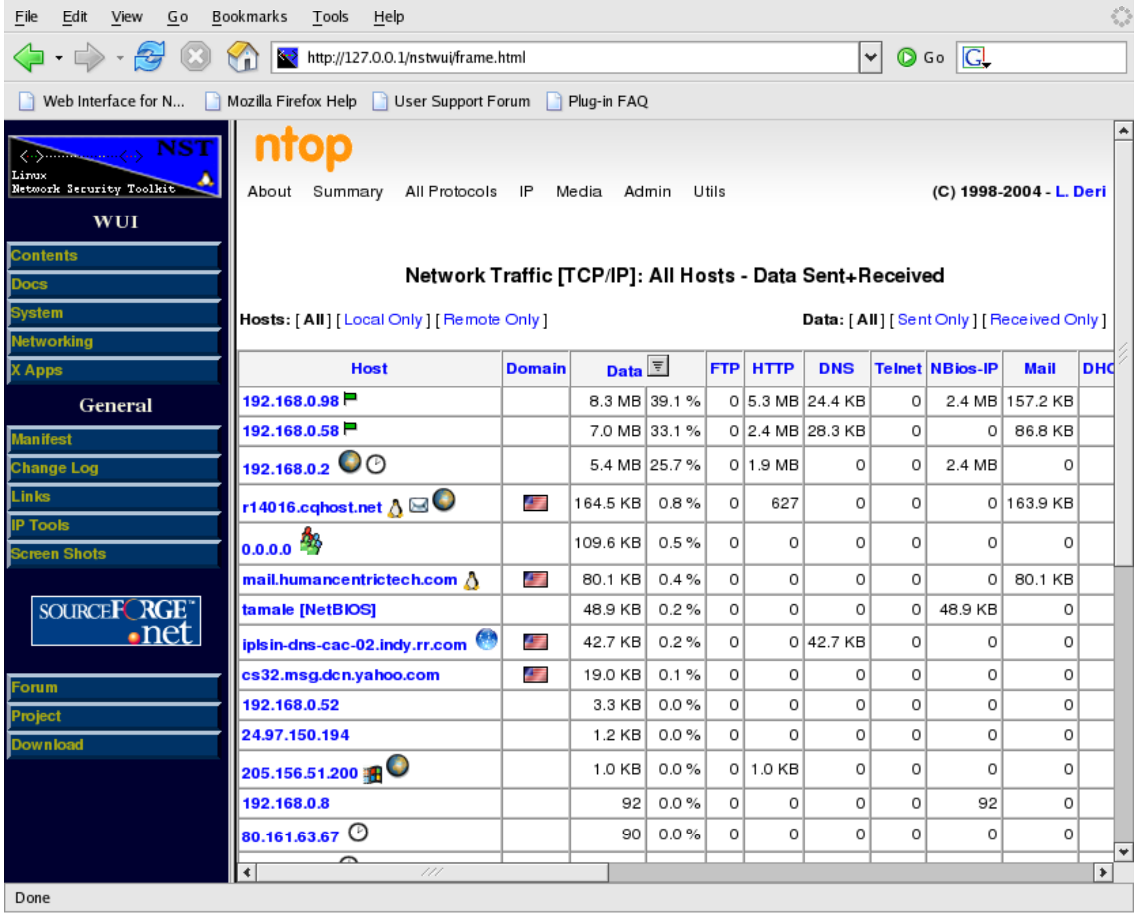
Alternate . . .

Non-Commercial Freeware

Version 2.0.4

Ntop

- Ntop is a network traffic probe that shows the network usage
- In interactive mode, it displays the network status on the user's terminal
- In web mode, it acts as a web server, creating an html dump of the network status



Network Traffic [TCP/IP]: All Hosts - Data Sent+Received

Hosts: [All] [Local Only] [Remote Only]

Data: [All] [Sent Only] [Received Only]

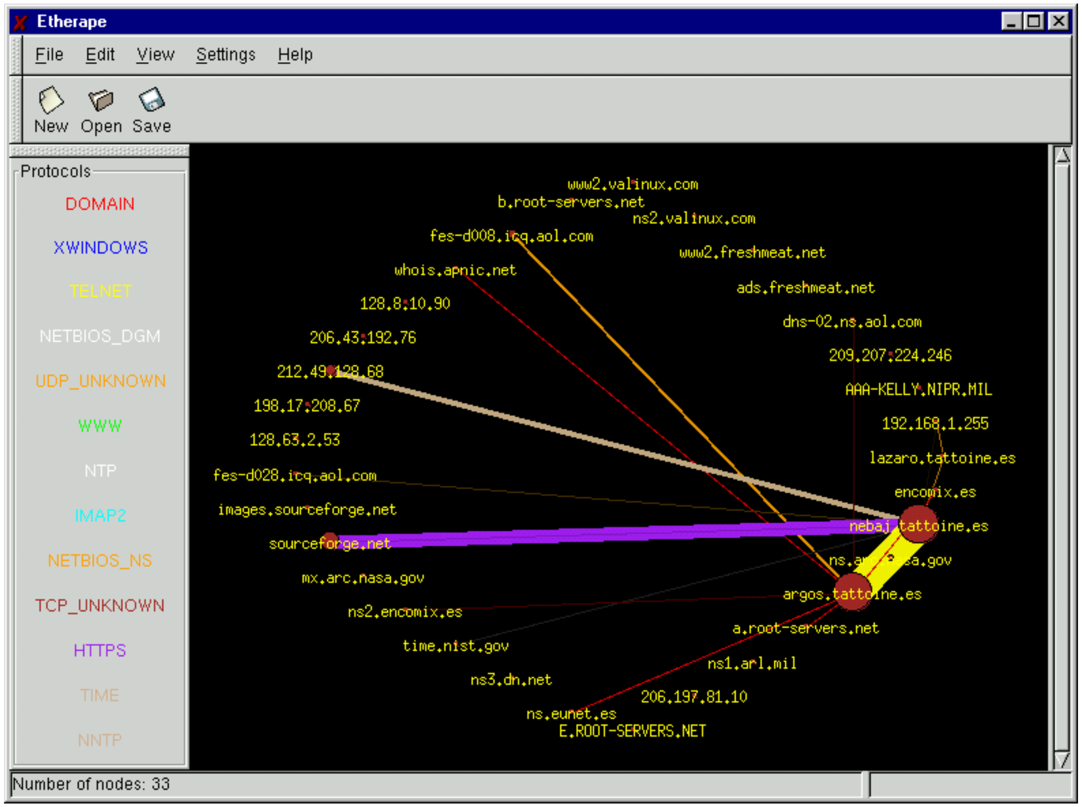
Host	Domain	Data		FTP	HTTP	DNS	Telnet	NBios-IP	Mail	DHC
192.168.0.98		8.3 MB	39.1 %	0	5.3 MB	24.4 KB	0	2.4 MB	157.2 KB	
192.168.0.58		7.0 MB	33.1 %	0	2.4 MB	28.3 KB	0	0	86.8 KB	
192.168.0.2		5.4 MB	25.7 %	0	1.9 MB	0	0	2.4 MB	0	
r14016.cqhost.net	🇺🇸	164.5 KB	0.8 %	0	627	0	0	0	163.9 KB	
0.0.0.0		109.6 KB	0.5 %	0	0	0	0	0	0	
mail.humancentrictech.com	🇺🇸	80.1 KB	0.4 %	0	0	0	0	0	80.1 KB	
tamale [NetBIOS]		48.9 KB	0.2 %	0	0	0	0	48.9 KB	0	
iplsin-dns-cac-02.indy.rr.com	🇺🇸	42.7 KB	0.2 %	0	0	42.7 KB	0	0	0	
cs32.msg.dcn.yahoo.com	🇺🇸	19.0 KB	0.1 %	0	0	0	0	0	0	
192.168.0.52		3.3 KB	0.0 %	0	0	0	0	0	0	
24.97.150.194		1.2 KB	0.0 %	0	0	0	0	0	0	
205.156.51.200		1.0 KB	0.0 %	0	1.0 KB	0	0	0	0	
192.168.0.8		92	0.0 %	0	0	0	0	92	0	
80.161.63.67		90	0.0 %	0	0	0	0	0	0	

EtherApe

EtherApe is a graphical network monitor for Unix

Featuring link layer, IP, and TCP modes, it displays the network activity graphically

It can filter traffic to be shown, and can read traffic from a file as well as live from the network



EtherApe Features

Network traffic is displayed graphically. The more talkative a node is, the bigger is its representation

A user may select what level of the protocol stack to concentrate on

A user may either look at the traffic within a network, end to end IP, or even port to port TCP

Data can be captured “off the wire” from a live network connection, or read from a tcpdump capture file

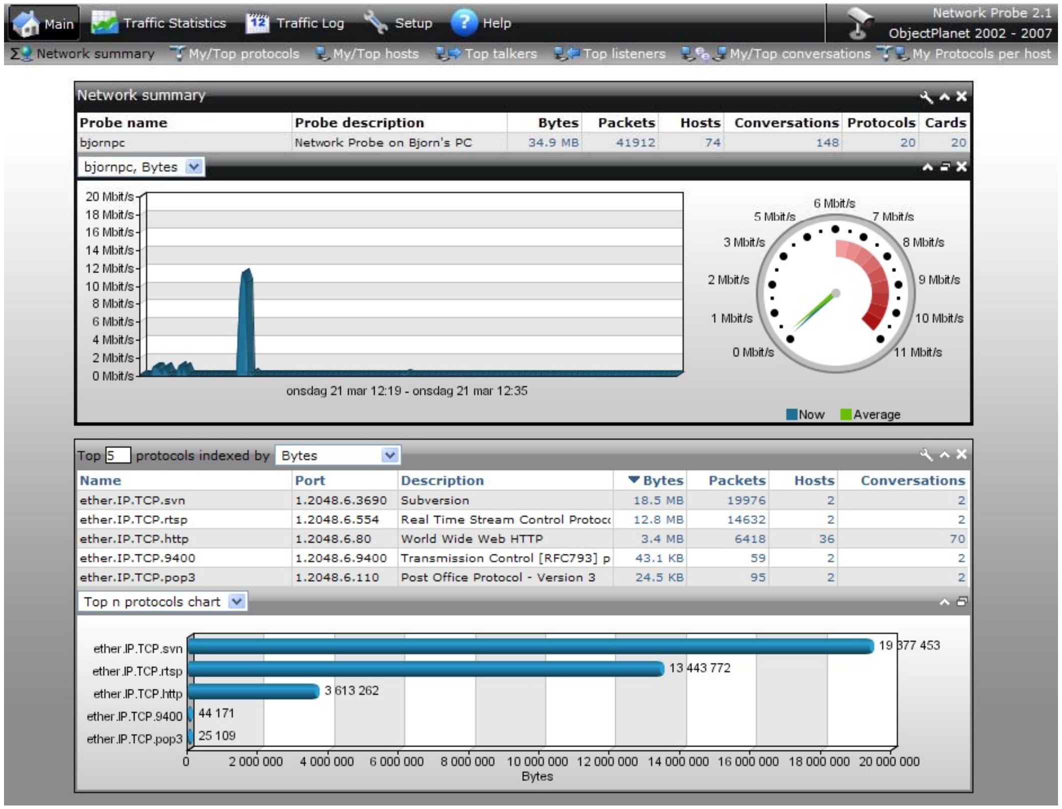
Data display can be refined using a network filter

Network Probe

Network Probe network monitor and protocol analyzer gives the user an instant picture of the traffic situation on the target network

All traffic is monitored in real time

All the information can be sorted, searched, and filtered by protocols, hosts, conversations, and network interfaces



Network summary

Probe name	Probe description	Bytes	Packets	Hosts	Conversations	Protocols	Cards
bjornpc	Network Probe on Bjorn's PC	34.9 MB	41912	74	148	20	20

Top 5 protocols indexed by Bytes

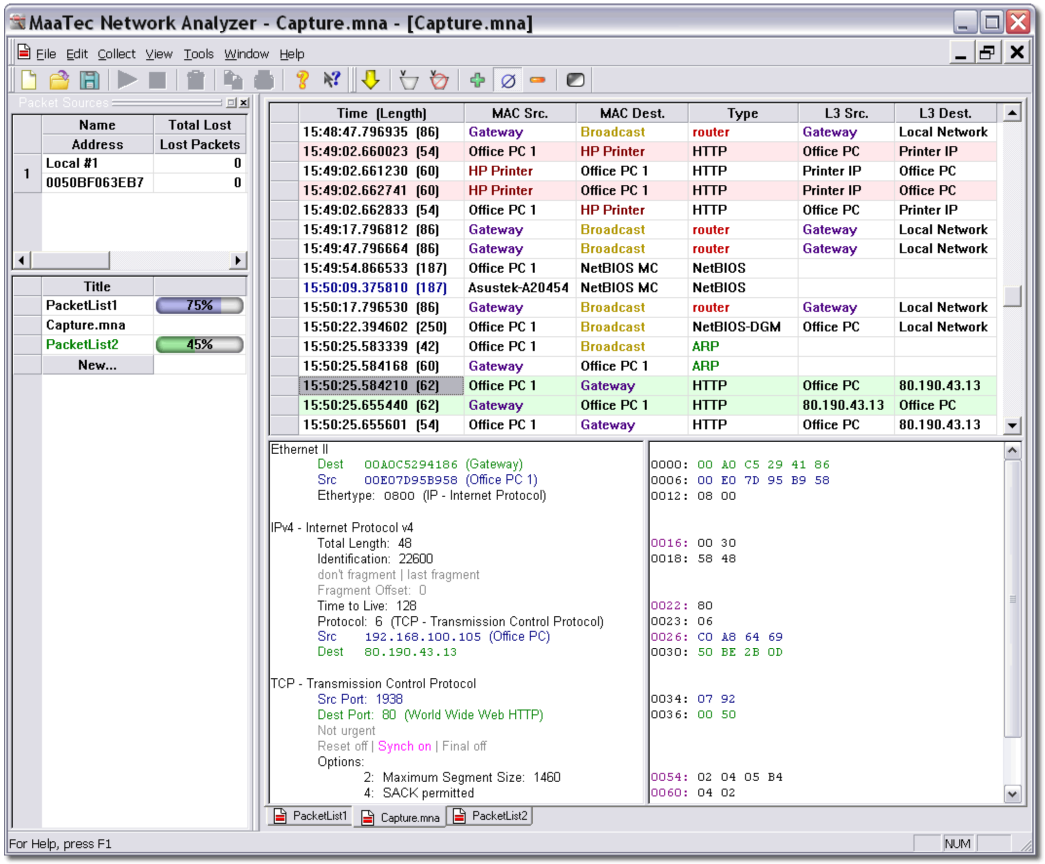
Name	Port	Description	▼Bytes	Packets	Hosts	Conversations
ether.IP.TCP.svn	1.2048.6.3690	Subversion	18.5 MB	19976	2	2
ether.IP.TCP.rtsp	1.2048.6.554	Real Time Stream Control Protoc	12.8 MB	14632	2	2
ether.IP.TCP.http	1.2048.6.80	World Wide Web HTTP	3.4 MB	6418	36	70
ether.IP.TCP.9400	1.2048.6.9400	Transmission Control [RFC793] p	43.1 KB	59	2	2
ether.IP.TCP.pop3	1.2048.6.110	Post Office Protocol - Version 3	24.5 KB	95	2	2

Maa Tec Network Analyzer

MaaTec Network Analyzer is a tool that is used for capturing, saving, and analyzing the network traffic

Features:

- Real-time network traffic statistics
- Scheduled network traffic reports
- Online view of incoming packets
- Multiple data color options


MaaTec Network Analyzer - Capture.mna - [Capture.mna]
File Edit Collect View Tools Window Help
Packet Sources
PacketList1
Capture.mna
PacketList2
NUM

	Name Address	Total Lost Lost Packets
1	Local #1 0050BF063EB7	0 0

Title	
PacketList1	75%
Capture.mna	
PacketList2	45%
New...	

Time (Length)	MAC Src.	MAC Dest.	Type	L3 Src.	L3 Dest.
15:48:47.796935 (86)	Gateway	Broadcast	router	Gateway	Local Network
15:49:02.660023 (54)	Office PC 1	HP Printer	HTTP	Office PC	Printer IP
15:49:02.661230 (60)	HP Printer	Office PC 1	HTTP	Printer IP	Office PC
15:49:02.662741 (60)	HP Printer	Office PC 1	HTTP	Printer IP	Office PC
15:49:02.662833 (54)	Office PC 1	HP Printer	HTTP	Office PC	Printer IP
15:49:17.796812 (86)	Gateway	Broadcast	router	Gateway	Local Network
15:49:47.796664 (86)	Gateway	Broadcast	router	Gateway	Local Network
15:49:54.866533 (187)	Office PC 1	NetBIOS MC	NetBIOS		
15:50:09.375810 (187)	Asustek-A20454	NetBIOS MC	NetBIOS		
15:50:17.796530 (86)	Gateway	Broadcast	router	Gateway	Local Network
15:50:22.394602 (250)	Office PC 1	Broadcast	NetBIOS-DGM	Office PC	Local Network
15:50:25.583339 (42)	Office PC 1	Broadcast	ARP		
15:50:25.584168 (60)	Gateway	Office PC 1	ARP		
15:50:25.584210 (62)	Office PC 1	Gateway	HTTP	Office PC	80.190.43.13
15:50:25.655440 (62)	Gateway	Office PC 1	HTTP	80.190.43.13	Office PC
15:50:25.655601 (54)	Office PC 1	Gateway	HTTP	Office PC	80.190.43.13

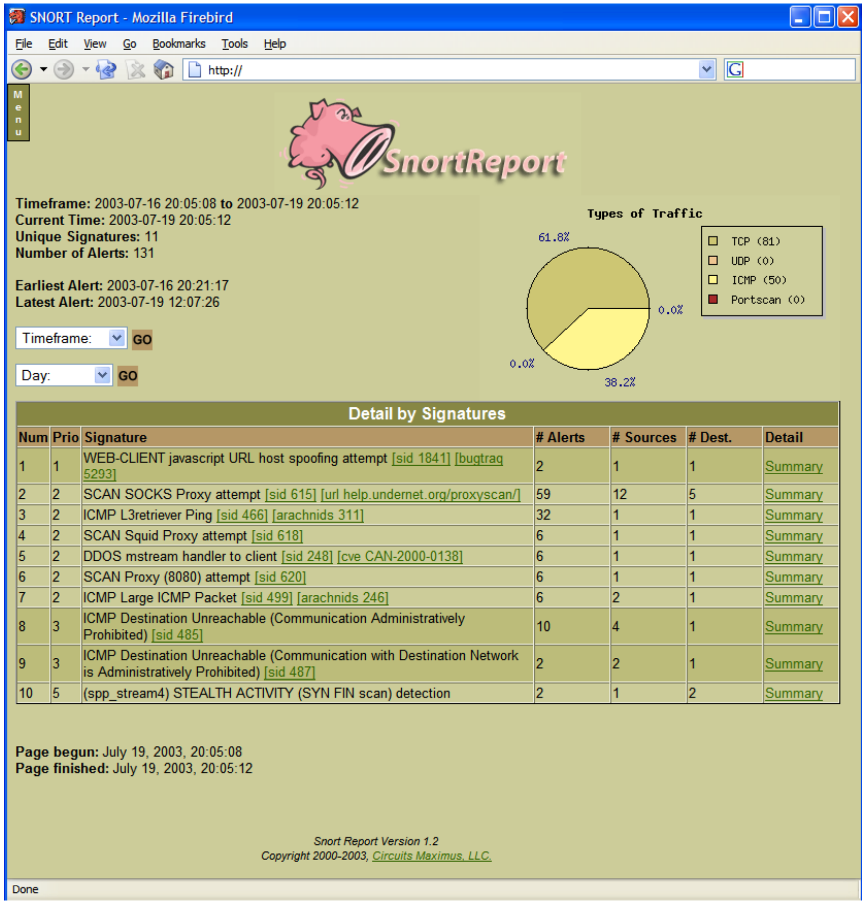
```
Ethernet II
        Dest     00A0C5294186  (Gateway)
        Src      00E07D95B958  (Office PC 1)
        Ethertype:  0800  (IP - Internet Protocol)

IPv4 - Internet Protocol v4
        Total Length:  48
        Identification:  22600
        don't fragment | last fragment
        Fragment Offset:  0
        Time to Live:  128
        Protocol:  6  (TCP - Transmission Control Protocol)
        Src      192.168.100.105  (Office PC)
        Dest     80.190.43.13

TCP - Transmission Control Protocol
        Src Port:  1938
        Dest Port:  80  (World Wide Web HTTP)
        Not urgent
        Reset off | Synch on | Final off
        Options:
                2:  Maximum Segment Size:  1460
                4:  SACK permitted
```

```
0000:  00  A0  C5  29  41  86
0006:  00  E0  7D  95  B9  58
0012:  08  00

0016:  00  30
0018:  58  48

0022:  80
0023:  06
0026:  C0  A8  64  69
0030:  50  BE  2B  0D

0034:  07  92
0036:  00  50

0054:  02  04  05  B4
0060:  04  02
```

For Help, press F1

EC-Council

Tool: Snort



Timeframe: 2003-07-16 20:05:08 **to** 2003-07-19 20:05:12
Current Time: 2003-07-19 20:05:12
Unique Signatures: 11
Number of Alerts: 131

Earliest Alert: 2003-07-16 20:21:17
Latest Alert: 2003-07-19 12:07:26

Timeframe: GO

Day: GO

Detail by Signatures

Num	Prio	Signature	# Alerts	# Sources	# Dest.	Detail
1	1	WEB-CLIENT javascript URL host spoofing attempt [sid 1841] [bugtraq 5293]	2	1	1	Summary
2	2	SCAN SOCKS Proxy attempt [sid 615] [url help.undernet.org/proxyscan/]	59	12	5	Summary
3	2	ICMP L3retriever Ping [sid 466] [arachnids 311]	32	1	1	Summary
4	2	SCAN Squid Proxy attempt [sid 618]	6	1	1	Summary
5	2	DDOS mstream handler to client [sid 248] [cve CAN-2000-0138]	6	1	1	Summary
6	2	SCAN Proxy (8080) attempt [sid 620]	6	1	1	Summary
7	2	ICMP Large ICMP Packet [sid 499] [arachnids 246]	6	2	1	Summary
8	3	ICMP Destination Unreachable (Communication Administratively Prohibited) [sid 485]	10	4	1	Summary
9	3	ICMP Destination Unreachable (Communication with Destination Network is Administratively Prohibited) [sid 487]	2	2	1	Summary
10	5	(spp_stream4) STEALTH ACTIVITY (SYN FIN scan) detection	2	1	2	Summary

Page begun: July 19, 2003, 20:05:08
Page finished: July 19, 2003, 20:05:12

Snort Report Version 1.2
Copyright 2000-2003, Circuits Maximus, LLC.

There are three main modes in which Snort can be configured: sniffer, packet logger, and network intrusion detection system

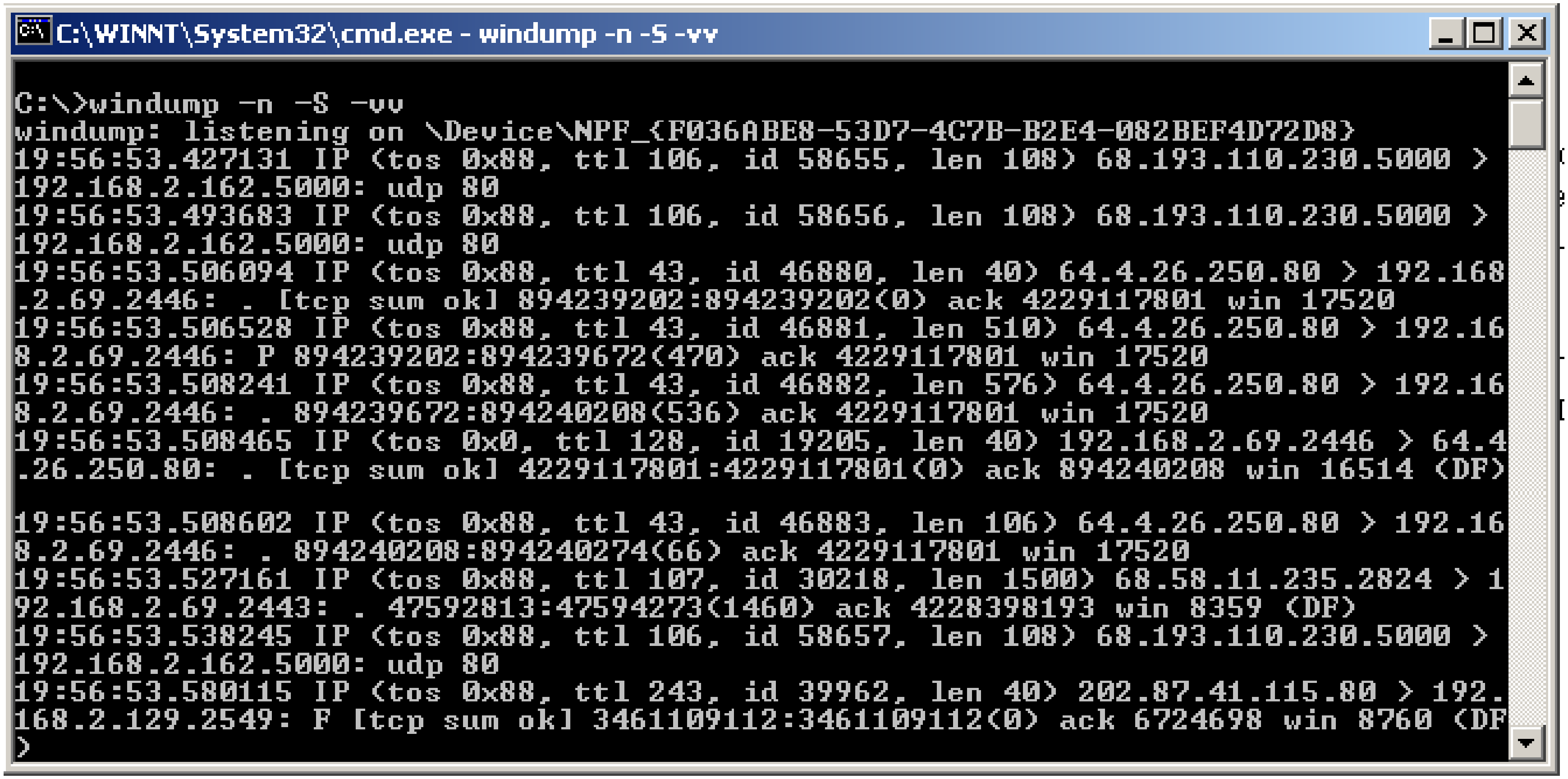
Sniffer mode reads the packets off of the network and displays them for you in a continuous stream on the console

Packet logger mode logs the packets to the disk

Network intrusion detection mode is the most complex and configurable configuration, allowing Snort to analyze the network traffic for matches against a user-defined rule set

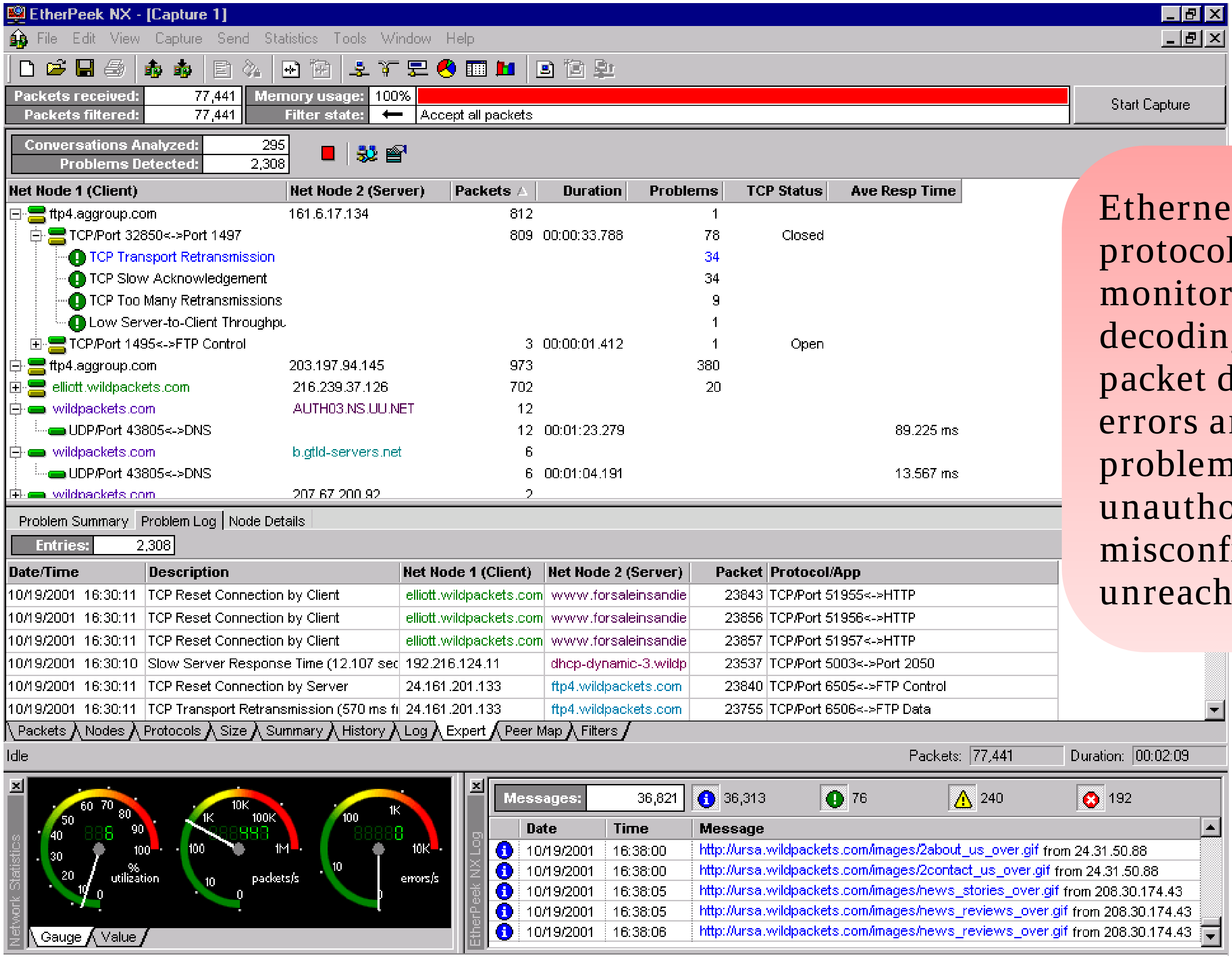
Tool: Windump

WinDump is the porting to the Windows platform of tcpdump, the most used network sniffer/analyzer for UNIX



```
C:\>windump -n -S -vv
windump: listening on \Device\NPF_{F036ABE8-53D7-4C7B-B2E4-082BEF4D72D8}
19:56:53.427131 IP (tos 0x88, ttl 106, id 58655, len 108) 68.193.110.230.5000 >
192.168.2.162.5000: udp 80
19:56:53.493683 IP (tos 0x88, ttl 106, id 58656, len 108) 68.193.110.230.5000 >
192.168.2.162.5000: udp 80
19:56:53.506094 IP (tos 0x88, ttl 43, id 46880, len 40) 64.4.26.250.80 > 192.168
.2.69.2446: . [tcp sum ok] 894239202:894239202(0) ack 4229117801 win 17520
19:56:53.506528 IP (tos 0x88, ttl 43, id 46881, len 510) 64.4.26.250.80 > 192.16
8.2.69.2446: P 894239202:894239672(470) ack 4229117801 win 17520
19:56:53.508241 IP (tos 0x88, ttl 43, id 46882, len 576) 64.4.26.250.80 > 192.16
8.2.69.2446: . 894239672:894240208(536) ack 4229117801 win 17520
19:56:53.508465 IP (tos 0x0, ttl 128, id 19205, len 40) 192.168.2.69.2446 > 64.4
.26.250.80: . [tcp sum ok] 4229117801:4229117801(0) ack 894240208 win 16514 (DF)

19:56:53.508602 IP (tos 0x88, ttl 43, id 46883, len 106) 64.4.26.250.80 > 192.16
8.2.69.2446: . 894240208:894240274(66) ack 4229117801 win 17520
19:56:53.527161 IP (tos 0x88, ttl 107, id 30218, len 1500) 68.58.11.235.2824 > 1
92.168.2.69.2443: . 47592813:47594273(1460) ack 4228398193 win 8359 (DF)
19:56:53.538245 IP (tos 0x88, ttl 106, id 58657, len 108) 68.193.110.230.5000 >
192.168.2.162.5000: udp 80
19:56:53.580115 IP (tos 0x88, ttl 243, id 39962, len 40) 202.87.41.115.80 > 192.
168.2.129.2549: F [tcp sum ok] 3461109112:3461109112(0) ack 6724698 win 8760 (DF
)
```

Tool: Etherpeek



EtherPeek NX - [Capture 1]
File Edit View Capture Send Statistics Tools Window Help
Start Capture
Problem Summary | Problem Log | Node Details
Packets | Nodes | Protocols | Size | Summary | History | Log | Expert | Peer Map | Filters
Gauge | Value
Network Statistics
EtherPeek NX Log
60 70 80 90 100 50 40 30 20 10 0 % utilization
1K 10K 100K 1M 100 10 0 packets/s
100 1K 10K 10 errors/s

Packets received: 77,441
Packets filtered: 77,441
Memory usage: 100%
Filter state: Accept all packets

Conversations Analyzed: 295
Problems Detected: 2,308

Net Node 1 (Client)	Net Node 2 (Server)	Packets	Duration	Problems	TCP Status	Ave Resp Time
ftp4.aggroup.com	161.6.17.134	812		1		
TCP/Port 32850<->Port 1497		809	00:00:33.788	78	Closed	
TCP Transport Retransmission				34		
TCP Slow Acknowledgement				34		
TCP Too Many Retransmissions				9		
Low Server-to-Client Throughpu				1		
TCP/Port 1495<->FTP Control		3	00:00:01.412	1	Open	
ftp4.aggroup.com	203.197.94.145	973		380		
elliott.wildpackets.com	216.239.37.126	702		20		
wildpackets.com	AUTH03.NS.UU.NET	12				
UDP/Port 43805<->DNS		12	00:01:23.279			89.225 ms
wildpackets.com	b.gtld-servers.net	6				
UDP/Port 43805<->DNS		6	00:01:04.191			13.567 ms
wildpackets.com	207.67.200.92	2				

Entries: 2,308

Date/Time	Description	Net Node 1 (Client)	Net Node 2 (Server)	Packet	Protocol/App
10/19/2001 16:30:11	TCP Reset Connection by Client	elliott.wildpackets.com	www.forsaleinsandie	23843	TCP/Port 51955<->HTTP
10/19/2001 16:30:11	TCP Reset Connection by Client	elliott.wildpackets.com	www.forsaleinsandie	23856	TCP/Port 51956<->HTTP
10/19/2001 16:30:11	TCP Reset Connection by Client	elliott.wildpackets.com	www.forsaleinsandie	23857	TCP/Port 51957<->HTTP
10/19/2001 16:30:10	Slow Server Response Time (12.107 sec	192.216.124.11	dhcp-dynamic-3.wildp	23537	TCP/Port 5003<->Port 2050
10/19/2001 16:30:11	TCP Reset Connection by Server	24.161.201.133	ftp4.wildpackets.com	23840	TCP/Port 6505<->FTP Control
10/19/2001 16:30:11	TCP Transport Retransmission (570 ms fi	24.161.201.133	ftp4.wildpackets.com	23755	TCP/Port 6506<->FTP Data

Idle Packets: 77,441 Duration: 00:02:09

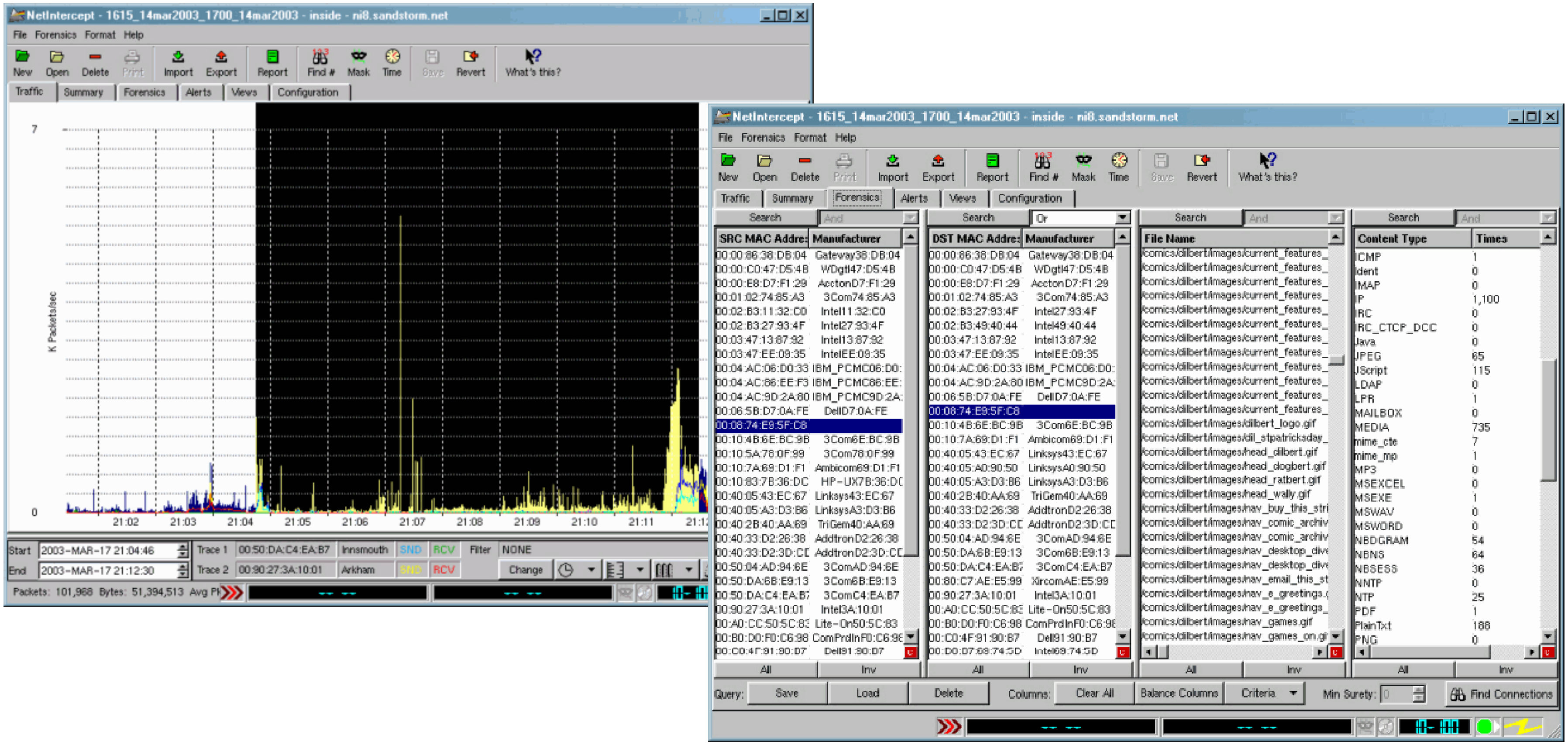
Messages: 36,821 | 36,313 | 76 | 240 | 192

Date	Time	Message
10/19/2001	16:38:00	http://ursa.wildpackets.com/images/2about_us_over.gif from 24.31.50.88
10/19/2001	16:38:00	http://ursa.wildpackets.com/images/2contact_us_over.gif from 24.31.50.88
10/19/2001	16:38:05	http://ursa.wildpackets.com/images/news_stories_over.gif from 208.30.174.43
10/19/2001	16:38:05	http://ursa.wildpackets.com/images/news_reviews_over.gif from 208.30.174.43
10/19/2001	16:38:06	http://ursa.wildpackets.com/images/news_reviews_over.gif from 208.30.174.43

Ethernet network traffic and protocol analyzer. By monitoring, filtering, decoding, and displaying packet data, it finds protocol errors and detects network problems such as unauthorized nodes, misconfigured routers, and unreachable devices

NetIntercept

A sniffing tool that studies external break-in attempts, watches for the misuse of confidential data, displays the contents of an unencrypted remote login or web session, categorizes or sorts traffic by dozens of attributes, and searches traffic by criteria such as email headers, websites, and file names


NetIntercept - 1615_14mar2003_1700_14mar2003 - inside - ni8.sandstorm.net
File Forensics Format Help
New Open Delete Print Import Export Report Find # Mask Time Save Revert What's this?
Traffic Summary Forensics Alerts Views Configuration
7
0
K Packets/sec
21:02
21:03
21:04
21:05
21:06
21:07
21:08
21:09
21:10
21:11
21:12
Change
NetIntercept - 1615_14mar2003_1700_14mar2003 - inside - ni8.sandstorm.net
File Forensics Format Help
New Open Delete Print Import Export Report Find # Mask Time Save Revert What's this?
Traffic Summary Forensics Alerts Views Configuration
Search
All
Inv
Query: Save Load Delete
Columns: Clear All Balance Columns Criteria
Min Surety: 0
Find Connections

Start 2003-MAR-17 21:04:46
End 2003-MAR-17 21:12:30
Trace 1 00:50:DA:C4:EA:B7 Innsmouth SND RCV
Trace 2 00:90:27:3A:10:01 Arkham SND RCV
Filter NONE
Packets: 101,968 Bytes: 51,394,513 Avg Pk

Search And

SRC MAC Addre:	Manufacturer
00:00:86:38:DB:04	Gateway38:DB:04
00:00:C0:47:D5:4B	WDgtl47:D5:4B
00:00:E8:D7:F1:29	AcctonD7:F1:29
00:01:02:74:85:A3	3Com74:85:A3
00:02:B3:11:32:C0	Intel11:32:C0
00:02:B3:27:93:4F	Intel27:93:4F
00:03:47:13:87:92	Intel13:87:92
00:03:47:EE:09:35	IntelEE:09:35
00:04:AC:06:D0:33	IBM_PCMC06:D0:
00:04:AC:86:EE:F3	IBM_PCMC86:EE:
00:04:AC:9D:2A:80	IBM_PCMC9D:2A:
00:06:5B:D7:0A:FE	DellD7:0A:FE
00:08:74:E9:5F:C8	
00:10:4B:6E:BC:9B	3Com6E:BC:9B
00:10:5A:78:0F:99	3Com78:0F:99
00:10:7A:69:D1:F1	Ambicom69:D1:F1
00:10:83:7B:36:DC	HP-UX7B:36:DC
00:40:05:43:EC:67	Linksys43:EC:67
00:40:05:A3:D3:B6	LinksysA3:D3:B6
00:40:2B:40:AA:69	TriGem40:AA:69
00:40:33:D2:26:38	AddtronD2:26:38
00:40:33:D2:3D:CD	AddtronD2:3D:CD
00:50:04:AD:94:6E	3ComAD:94:6E
00:50:DA:6B:E9:13	3Com6B:E9:13
00:50:DA:C4:EA:B7	3ComC4:EA:B7
00:90:27:3A:10:01	Intel3A:10:01
00:A0:CC:50:5C:83	Lite-On50:5C:83
00:B0:D0:F0:C6:98	ComPrdInF0:C6:98
00:C0:4F:91:90:D7	Dell91:90:D7

Search Or

DST MAC Addre:	Manufacturer
00:00:86:38:DB:04	Gateway38:DB:04
00:00:C0:47:D5:4B	WDgtl47:D5:4B
00:00:E8:D7:F1:29	AcctonD7:F1:29
00:01:02:74:85:A3	3Com74:85:A3
00:02:B3:27:93:4F	Intel27:93:4F
00:02:B3:49:40:44	Intel49:40:44
00:03:47:13:87:92	Intel13:87:92
00:03:47:EE:09:35	IntelEE:09:35
00:04:AC:06:D0:33	IBM_PCMC06:D0:
00:04:AC:9D:2A:80	IBM_PCMC9D:2A:
00:06:5B:D7:0A:FE	DellD7:0A:FE
00:08:74:E9:5F:C8	
00:10:4B:6E:BC:9B	3Com6E:BC:9B
00:10:7A:69:D1:F1	Ambicom69:D1:F1
00:40:05:43:EC:67	Linksys43:EC:67
00:40:05:A0:90:50	LinksysA0:90:50
00:40:05:A3:D3:B6	LinksysA3:D3:B6
00:40:2B:40:AA:69	TriGem40:AA:69
00:40:33:D2:26:38	AddtronD2:26:38
00:40:33:D2:3D:CD	AddtronD2:3D:CD
00:50:04:AD:94:6E	3ComAD:94:6E
00:50:DA:6B:E9:13	3Com6B:E9:13
00:50:DA:C4:EA:B7	3ComC4:EA:B7
00:80:C7:AE:E5:99	XircomAE:E5:99
00:90:27:3A:10:01	Intel3A:10:01
00:A0:CC:50:5C:83	Lite-On50:5C:83
00:B0:D0:F0:C6:98	ComPrdInF0:C6:98
00:C0:4F:91:90:B7	Dell91:90:B7
00:D0:07:69:74:5D	Intel69:74:5D

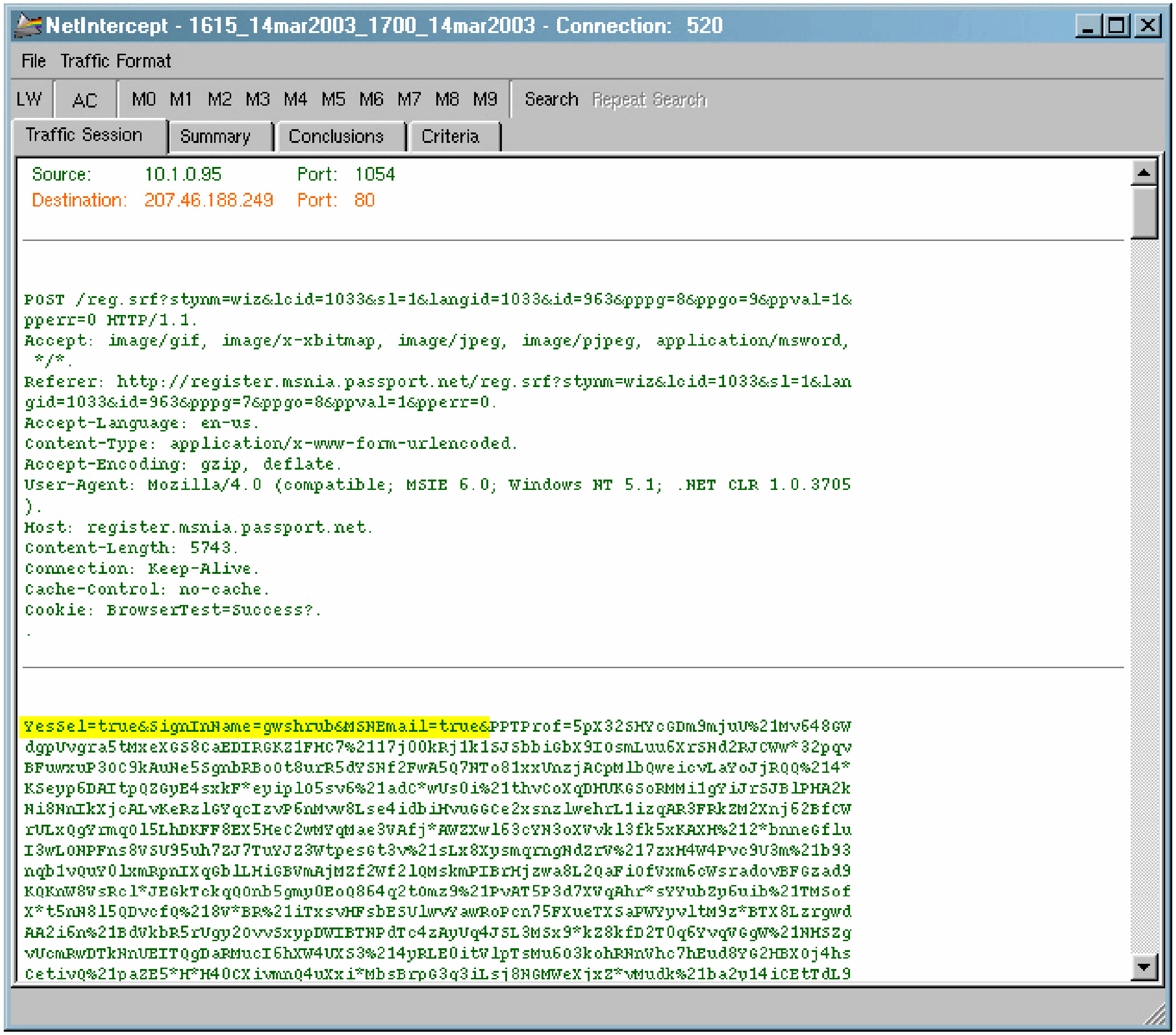
Search And

File Name
/comics/dilbert/images/current_features_
/comics/dilbert/images/current_features_
/comics/dilbert/images/current_features_
/comics/dilbert/images/current_features_
/comics/dilbert/images/current_features_
/comics/dilbert/images/current_features_
/comics/dilbert/images/current_features_
/comics/dilbert/images/current_features_
/comics/dilbert/images/current_features_
/comics/dilbert/images/current_features_
/comics/dilbert/images/current_features_
/comics/dilbert/images/current_features_
/comics/dilbert/images/dilbert_logo.gif
/comics/dilbert/images/dil_stpatricksday_
/comics/dilbert/images/head_dilbert.gif
/comics/dilbert/images/head_dogbert.gif
/comics/dilbert/images/head_ratbert.gif
/comics/dilbert/images/head_wally.gif
/comics/dilbert/images/nav_buy_this_stri
/comics/dilbert/images/nav_comic_archiv
/comics/dilbert/images/nav_comic_archiv
/comics/dilbert/images/nav_desktop_dive
/comics/dilbert/images/nav_desktop_dive
/comics/dilbert/images/nav_email_this_st
/comics/dilbert/images/nav_e_greetings.(
/comics/dilbert/images/nav_e_greetings_
/comics/dilbert/images/nav_games.gif
/comics/dilbert/images/nav_games_on.gi

Search And

Content Type	Times
ICMP	1
Ident	0
IMAP	0
IP	1,100
IRC	0
IRC_CTCP_DCC	0
Java	0
JPEG	65
JScript	115
LDAP	0
LPR	1
MAILBOX	0
MEDIA	735
mime_cte	7
mime_mp	1
MP3	0
MSEXCEL	0
MSEXE	1
MSWAV	0
MSWORD	0
NBDGRAM	54
NBNS	64
NBSESS	36
NNTP	0
NTP	25
PDF	1
PlainTxt	188
PNG	0

NetIntercept: Screenshot 1

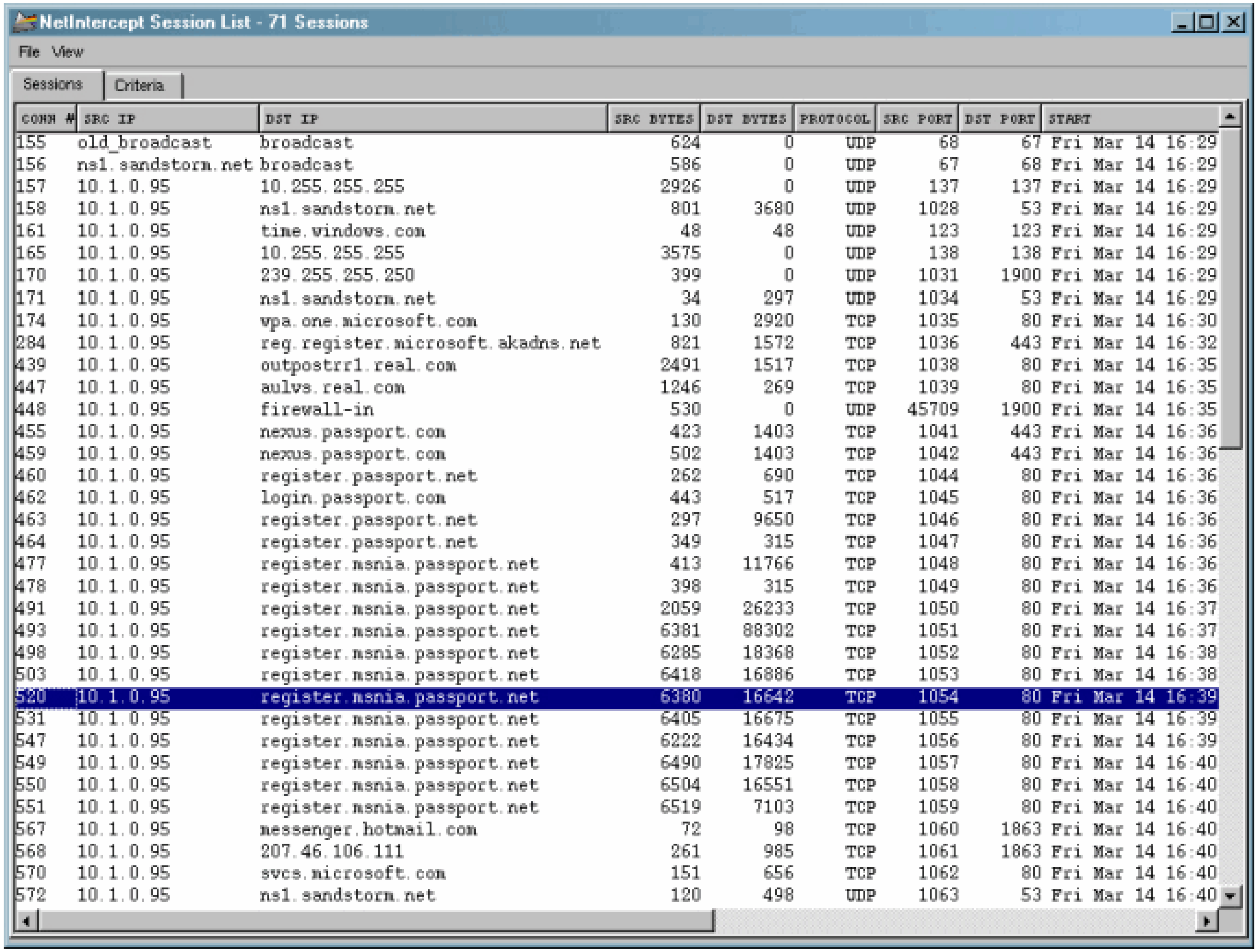

NetIntercept - 1615_14mar2003_1700_14mar2003 - Connection: 520
File Traffic Format
LW AC M0 M1 M2 M3 M4 M5 M6 M7 M8 M9 Search Repeat Search
Traffic Session Summary Conclusions Criteria

Source: 10.1.0.95 Port: 1054
Destination: 207.46.188.249 Port: 80

```
POST /reg.srf?stynm=wiz&lcid=1033&sl=1&langid=1033&id=963&pppg=8&ppgo=9&ppval=1&
pperr=0 HTTP/1.1.
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/msword,
 */*.
Referer: http://register.msnia.passport.net/reg.srf?stynm=wiz&lcid=1033&sl=1&lan
gid=1033&id=963&pppg=7&ppgo=8&ppval=1&pperr=0.
Accept-Language: en-us.
Content-Type: application/x-www-form-urlencoded.
Accept-Encoding: gzip, deflate.
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.0.3705
).
Host: register.msnia.passport.net.
Content-Length: 5743.
Connection: Keep-Alive.
Cache-Control: no-cache.
Cookie: BrowserTest=Success?.
.
```

```
YesSel=true&SignInName=gwshrub&MSNEmail=true&PPTProf=5pX32SHYcGDm9mjuU%21Mv648GW
dgpUvgra5tMxeXGS8CaEDIRGKZ1FHC7%2117j00kRj1k1SJSbbiGbX9I0smLuu6XrSNd2RJCWw*32pqv
BFuwxuP30C9kAuNe5SgnbRBo0t8urR5dYSNf2FwA5Q7NTo81xxUnzjACpM1bQweicvLaYoJjRQQ%214*
KSeyp6DAItpQZGyE4sxkF*eyipl05sv6%21adC*wUs0i%21thvCoXqDHUKGSoRMMi1gYiJrSJBlPHA2k
Ni8NnIkXjcALvKeRzlGYqcIzvP6nMvw8Lse4idbiHvuGGCe2xsnzlwehrL1izqAR3FRkZM2Xnj62BfCW
rULxQgYrmq0l5LhDKFF8EX5HeC2wMYqMae3VAfj*AWZXwl63cYN3oXVvkl3fk5xKAXH%212*bnneGflu
I3wLONPFns8VSU95uh7ZJ7TuYJZ3WtpesGt3v%21sLx8XysmqrngNdZrV%217zxH4W4Pvc9U3m%21b93
nqb1vQuY0lxmRpnIXqGblLHiGBVmAjMZf2Wf2lQMskmPIBrHjzwa8L2QaFi0fVxm6cWsradovBFGzad9
KQKnW8VsRcl*JEGkTckqQ0nb5gmy0EoQ864q2t0mz9%21PvAT5P3d7XVqAhr*sYYubZy6uib%21TMSof
X*t5nN8l5QDvcfQ%218V*BR%21iTxsVHFsbESUlwvYawRoPcn75FXueTXSaPWYyvltM9z*BTX8Lzrgwd
AA2i6n%21BdVkbR5rUgy2OvvSxypDWIBTNPdTc4zAyUq4JSL3MSx9*kZ8kfD2T0q6YvqVGgW%21NHSZg
vUcmRwDTkNnUEITQgDaRMucI6hXW4UXS3%214yRLE0itVlpTsMu603kohRNnVhc7hEud8YG2HBX0j4hs
CetivQ%21paZE5*H*H40CXivmnQ4uXxi*MbsBrpG3q3iLsj8NGMWeXjxZ*vMudk%21ba2y14iCEtTdL9
```

NetIntercept: Screenshot 2



CONN #	SRC IP	DST IP	SRC BYTES	DST BYTES	PROTOCOL	SRC PORT	DST PORT	START
155	old_broadcast	broadcast	624	0	UDP	68	67	Fri Mar 14 16:29
156	ns1.sandstorm.net	broadcast	586	0	UDP	67	68	Fri Mar 14 16:29
157	10.1.0.95	10.255.255.255	2926	0	UDP	137	137	Fri Mar 14 16:29
158	10.1.0.95	ns1.sandstorm.net	801	3680	UDP	1028	53	Fri Mar 14 16:29
161	10.1.0.95	time.windows.com	48	48	UDP	123	123	Fri Mar 14 16:29
165	10.1.0.95	10.255.255.255	3575	0	UDP	138	138	Fri Mar 14 16:29
170	10.1.0.95	239.255.255.250	399	0	UDP	1031	1900	Fri Mar 14 16:29
171	10.1.0.95	ns1.sandstorm.net	34	297	UDP	1034	53	Fri Mar 14 16:29
174	10.1.0.95	wpa.one.microsoft.com	130	2920	TCP	1035	80	Fri Mar 14 16:30
284	10.1.0.95	reg.register.microsoft.akadns.net	821	1572	TCP	1036	443	Fri Mar 14 16:32
439	10.1.0.95	outpostrr1.real.com	2491	1517	TCP	1038	80	Fri Mar 14 16:35
447	10.1.0.95	aulvs.real.com	1246	269	TCP	1039	80	Fri Mar 14 16:35
448	10.1.0.95	firewall-in	530	0	UDP	45709	1900	Fri Mar 14 16:35
455	10.1.0.95	nexus.passport.com	423	1403	TCP	1041	443	Fri Mar 14 16:36
459	10.1.0.95	nexus.passport.com	502	1403	TCP	1042	443	Fri Mar 14 16:36
460	10.1.0.95	register.passport.net	262	690	TCP	1044	80	Fri Mar 14 16:36
462	10.1.0.95	login.passport.com	443	517	TCP	1045	80	Fri Mar 14 16:36
463	10.1.0.95	register.passport.net	297	9650	TCP	1046	80	Fri Mar 14 16:36
464	10.1.0.95	register.passport.net	349	315	TCP	1047	80	Fri Mar 14 16:36
477	10.1.0.95	register.msnia.passport.net	413	11766	TCP	1048	80	Fri Mar 14 16:36
478	10.1.0.95	register.msnia.passport.net	398	315	TCP	1049	80	Fri Mar 14 16:36
491	10.1.0.95	register.msnia.passport.net	2059	26233	TCP	1050	80	Fri Mar 14 16:37
493	10.1.0.95	register.msnia.passport.net	6381	88302	TCP	1051	80	Fri Mar 14 16:37
498	10.1.0.95	register.msnia.passport.net	6285	18368	TCP	1052	80	Fri Mar 14 16:38
503	10.1.0.95	register.msnia.passport.net	6418	16886	TCP	1053	80	Fri Mar 14 16:38
520	10.1.0.95	register.msnia.passport.net	6380	16642	TCP	1054	80	Fri Mar 14 16:39
531	10.1.0.95	register.msnia.passport.net	6405	16675	TCP	1055	80	Fri Mar 14 16:39
547	10.1.0.95	register.msnia.passport.net	6222	16434	TCP	1056	80	Fri Mar 14 16:39
549	10.1.0.95	register.msnia.passport.net	6490	17825	TCP	1057	80	Fri Mar 14 16:40
550	10.1.0.95	register.msnia.passport.net	6504	16551	TCP	1058	80	Fri Mar 14 16:40
551	10.1.0.95	register.msnia.passport.net	6519	7103	TCP	1059	80	Fri Mar 14 16:40
567	10.1.0.95	messenger.hotmail.com	72	98	TCP	1060	1863	Fri Mar 14 16:40
568	10.1.0.95	207.46.106.111	261	985	TCP	1061	1863	Fri Mar 14 16:40
570	10.1.0.95	svcs.microsoft.com	151	656	TCP	1062	80	Fri Mar 14 16:40
572	10.1.0.95	ns1.sandstorm.net	120	498	UDP	1063	53	Fri Mar 14 16:40

Colasoft EtherLook

Colasoft EtherLook is a TCP/IP network monitoring tool for Windows-based platforms

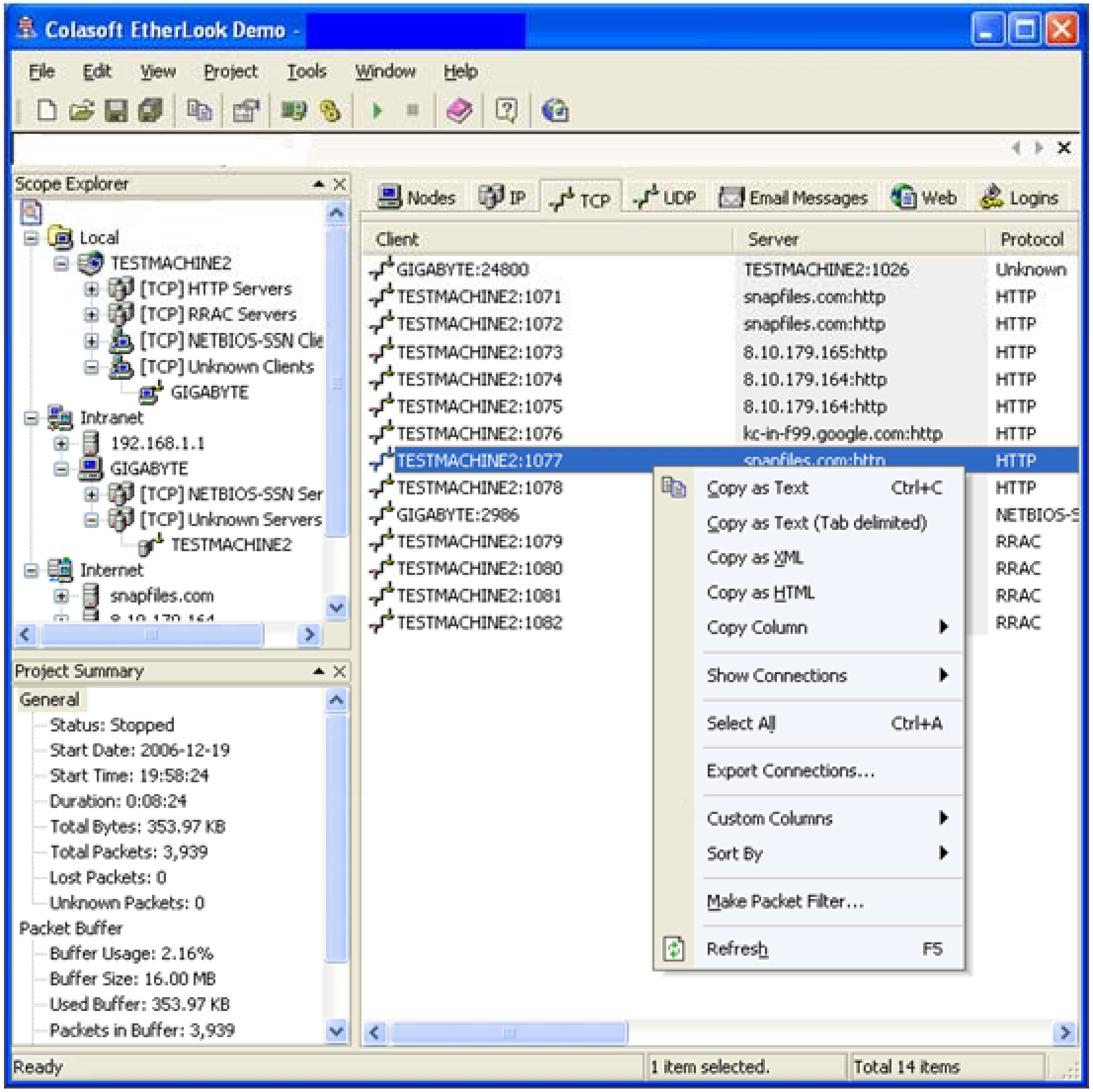
It monitors the real time traffic flowing around the local network and to/from the Internet efficiently

Traffic Analysis module enables to capture the network traffic in real time, displays data received and sent by every host in LAN in different views

Colasoft EtherLook has 3 advanced analysis modules:

- Email Analysis Module: Captures email messages and restores its contents including sender, recipient, subject, protocol, etc
- Web Analysis Module: Allows detailed tracking of web accesses from the network
- Login Analysis Module: Analyzes all data logins within the network and records all the related data

Colasoft EtherLook: Screenshot 1



Project Summary

General
- Status: Stopped
- Start Date: 2006-12-19
- Start Time: 19:58:24
- Duration: 0:08:24
- Total Bytes: 353.97 KB
- Total Packets: 3,939
- Lost Packets: 0
- Unknown Packets: 0

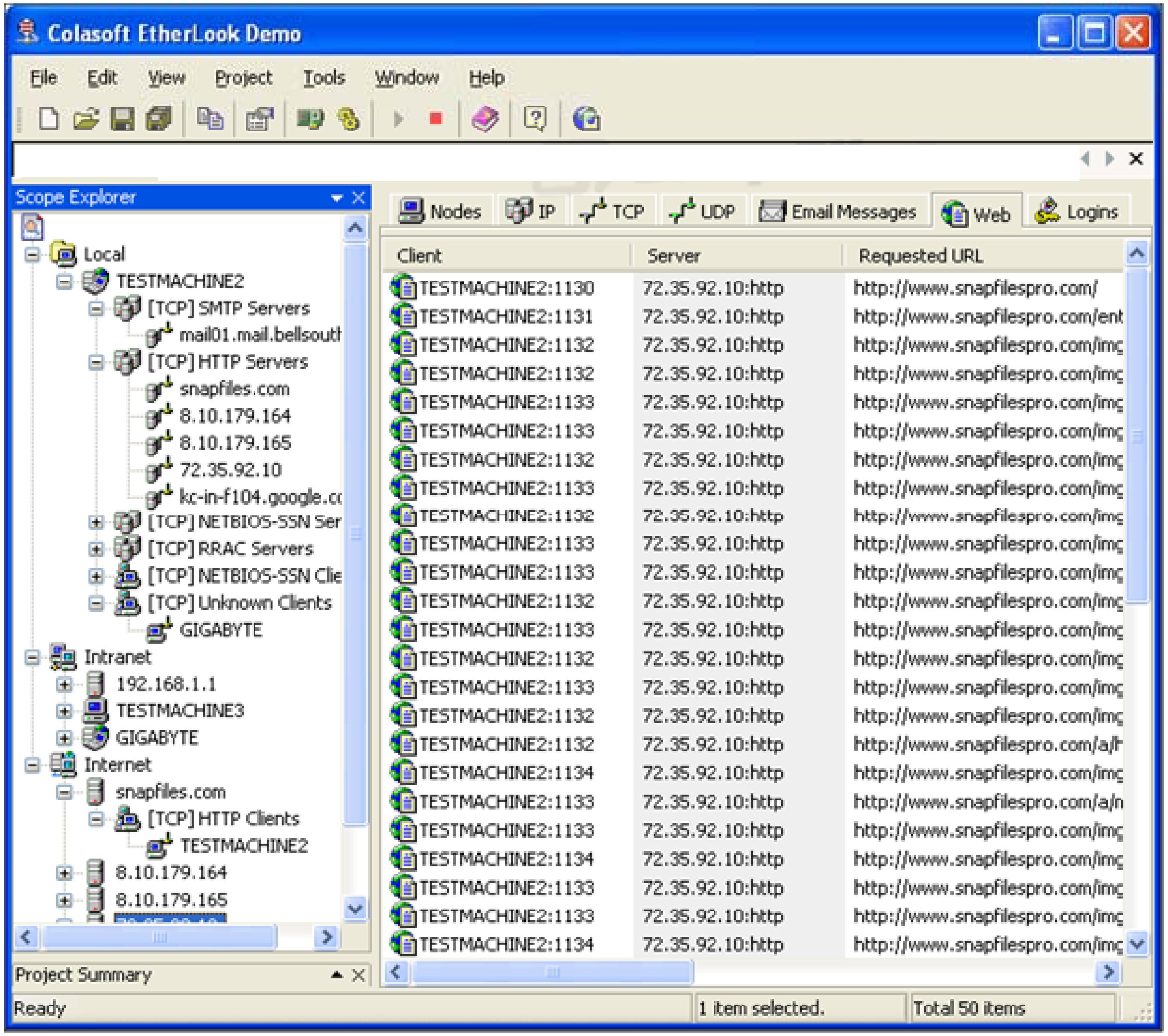
Packet Buffer
- Buffer Usage: 2.16%
- Buffer Size: 16.00 MB
- Used Buffer: 353.97 KB
- Packets in Buffer: 3,939

Client	Server	Protocol
GIGABYTE:24800	TESTMACHINE2:1026	Unknown
TESTMACHINE2:1071	snapfiles.com:http	HTTP
TESTMACHINE2:1072	snapfiles.com:http	HTTP
TESTMACHINE2:1073	8.10.179.165:http	HTTP
TESTMACHINE2:1074	8.10.179.164:http	HTTP
TESTMACHINE2:1075	8.10.179.164:http	HTTP
TESTMACHINE2:1076	kc-in-f99.google.com:http	HTTP
TESTMACHINE2:1077	snapfiles.com:http	HTTP
TESTMACHINE2:1078		HTTP
GIGABYTE:2986		NETBIOS-S
TESTMACHINE2:1079		RRAC
TESTMACHINE2:1080		RRAC
TESTMACHINE2:1081		RRAC
TESTMACHINE2:1082		RRAC

Ready | 1 item selected. | Total 14 items

EC-Council

Colasoft EtherLook: Screenshot 2



Client	Server	Requested URL
TESTMACHINE2:1130	72.35.92.10:http	http://www.snapfilespro.com/
TESTMACHINE2:1131	72.35.92.10:http	http://www.snapfilespro.com/ent
TESTMACHINE2:1132	72.35.92.10:http	http://www.snapfilespro.com/imc
TESTMACHINE2:1132	72.35.92.10:http	http://www.snapfilespro.com/imc
TESTMACHINE2:1133	72.35.92.10:http	http://www.snapfilespro.com/imc
TESTMACHINE2:1133	72.35.92.10:http	http://www.snapfilespro.com/imc
TESTMACHINE2:1132	72.35.92.10:http	http://www.snapfilespro.com/imc
TESTMACHINE2:1133	72.35.92.10:http	http://www.snapfilespro.com/imc
TESTMACHINE2:1132	72.35.92.10:http	http://www.snapfilespro.com/imc
TESTMACHINE2:1133	72.35.92.10:http	http://www.snapfilespro.com/imc
TESTMACHINE2:1133	72.35.92.10:http	http://www.snapfilespro.com/imc
TESTMACHINE2:1132	72.35.92.10:http	http://www.snapfilespro.com/imc
TESTMACHINE2:1133	72.35.92.10:http	http://www.snapfilespro.com/imc
TESTMACHINE2:1132	72.35.92.10:http	http://www.snapfilespro.com/imc
TESTMACHINE2:1133	72.35.92.10:http	http://www.snapfilespro.com/imc
TESTMACHINE2:1132	72.35.92.10:http	http://www.snapfilespro.com/imc
TESTMACHINE2:1132	72.35.92.10:http	http://www.snapfilespro.com/a/h
TESTMACHINE2:1134	72.35.92.10:http	http://www.snapfilespro.com/imc
TESTMACHINE2:1133	72.35.92.10:http	http://www.snapfilespro.com/a/n
TESTMACHINE2:1133	72.35.92.10:http	http://www.snapfilespro.com/imc
TESTMACHINE2:1134	72.35.92.10:http	http://www.snapfilespro.com/imc
TESTMACHINE2:1133	72.35.92.10:http	http://www.snapfilespro.com/imc
TESTMACHINE2:1133	72.35.92.10:http	http://www.snapfilespro.com/imc
TESTMACHINE2:1134	72.35.92.10:http	http://www.snapfilespro.com/imc

Ready | 1 item selected. | Total 50 items

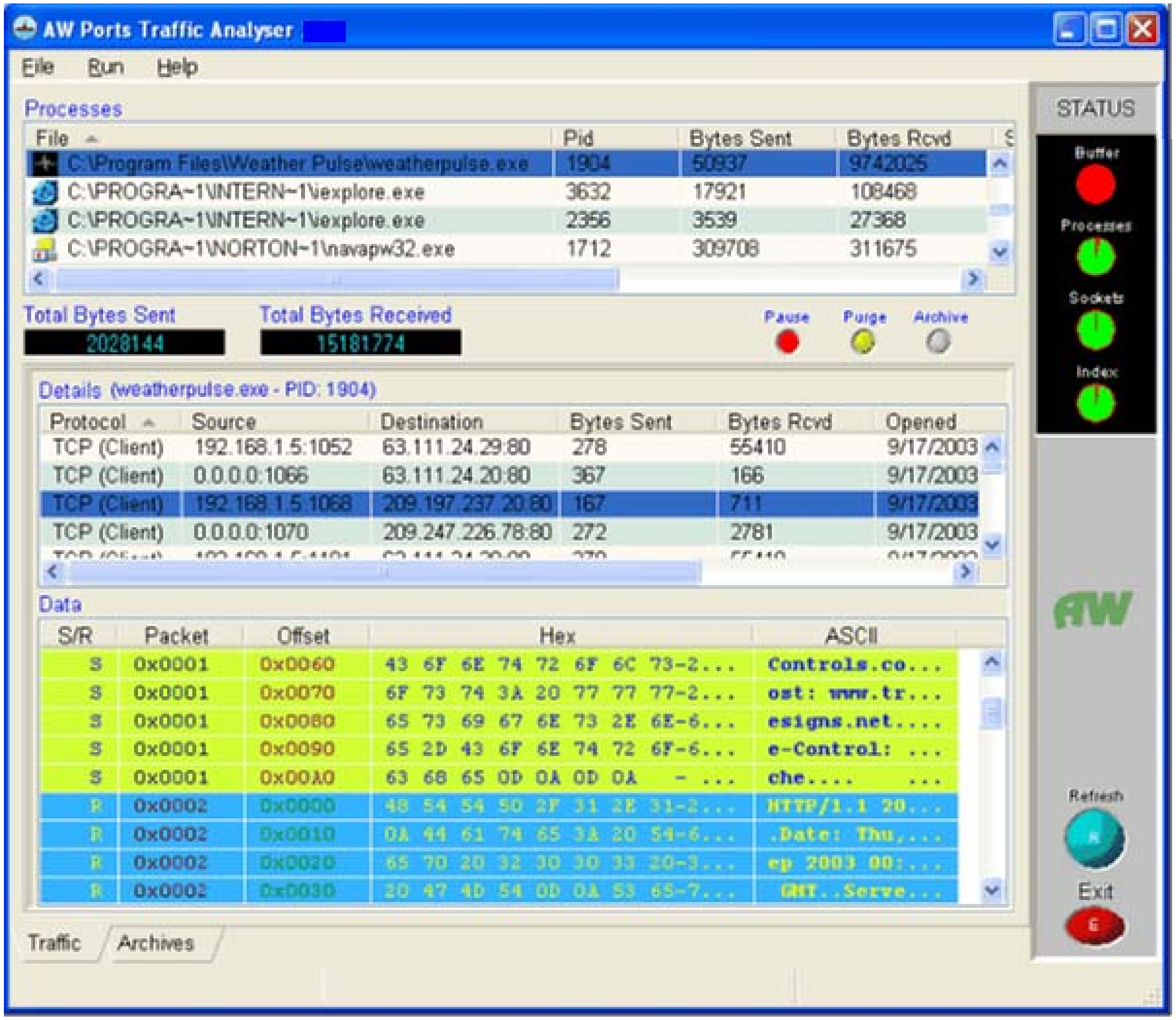
AW Ports Traffic Analyzer

Atelier Web Ports Traffic Analyzer is a network traffic sniffer and logger that allows you to monitor all Internet and network traffic on your PC and view the actual content of the packets

This includes all traffic initiated by software products, web sites etc. The capability to audit what flows in and out of every piece of software is critical for security aware users

Atelier Web Ports Traffic Analyzer provides Real-time mapping of ports to processes (applications and services) and shows the history since boot time of every TCP, UDP, or RAW port opened through Winsock

AW Ports Traffic Analyzer: Screenshot



Processes

File	Pid	Bytes Sent	Bytes Rcvd
C:\Program Files\Weather Pulse\weatherpulse.exe	1904	50937	9742025
C:\PROGRA~1\INTERN~1\iexplore.exe	3632	17921	108468
C:\PROGRA~1\INTERN~1\iexplore.exe	2356	3539	27368
C:\PROGRA~1\NORTON~1\navapw32.exe	1712	309708	311675

Total Bytes Sent: 2028144

Total Bytes Received: 15181774

Details (weatherpulse.exe - PID: 1904)

Protocol	Source	Destination	Bytes Sent	Bytes Rcvd	Opened
TCP (Client)	192.168.1.5:1052	63.111.24.29:80	278	55410	9/17/2003
TCP (Client)	0.0.0.0:1066	63.111.24.20:80	367	166	9/17/2003
TCP (Client)	192.168.1.5:1068	209.197.237.20:80	167	711	9/17/2003
TCP (Client)	0.0.0.0:1070	209.247.226.78:80	272	2781	9/17/2003

Data

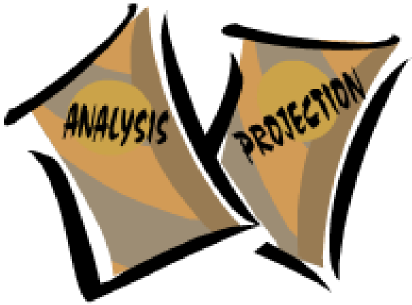
S/R	Packet	Offset	Hex	ASCII
S	0x0001	0x0060	43 6F 6E 74 72 6F 6C 73-2...	Controls.co...
S	0x0001	0x0070	6F 73 74 3A 20 77 77 77-2...	ost: www.tr...
S	0x0001	0x0080	65 73 69 67 6E 73 2E 6E-6...	esigns.net....
S	0x0001	0x0090	65 2D 43 6F 6E 74 72 6F-6...	e-Control: ...
S	0x0001	0x00A0	63 68 65 0D 0A 0D 0A - ...	che.... ...
R	0x0002	0x0000	48 54 54 50 2F 31 2E 31-2...	HTTP/1.1 20...
R	0x0002	0x0010	0A 44 61 74 65 3A 20 54-6...	.Date: Thu,...
R	0x0002	0x0020	65 70 20 32 30 30 33 20-3...	ep 2003 00:...
R	0x0002	0x0030	20 47 4D 54 0D 0A 53 65-7...	GMT..Serve...

Colasoft Capsa Network Analyzer

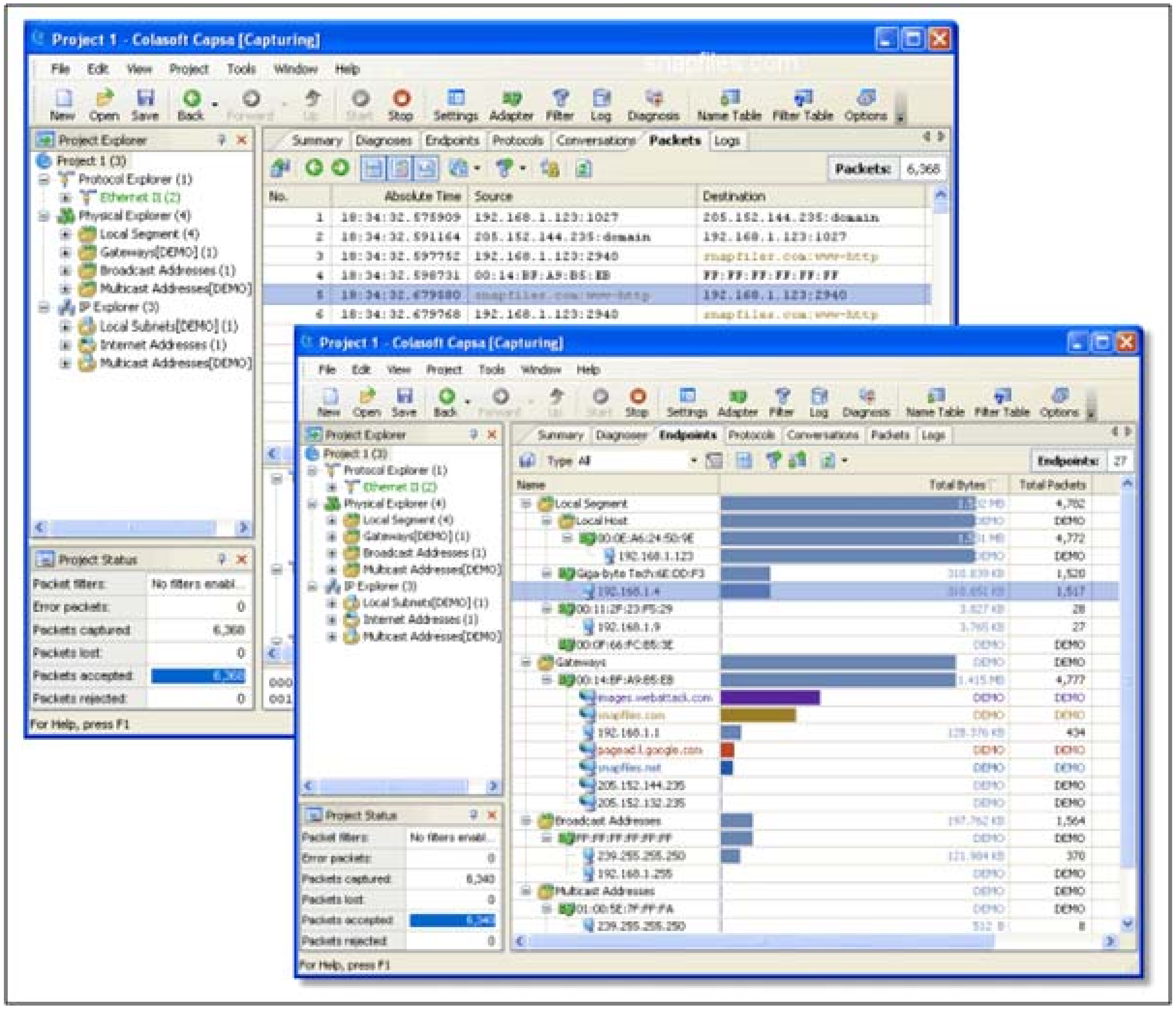
Colasoft Capsa Network Analyzer is a TCP/IP Network Sniffer and Analyzer that offers real time monitoring and data analyzing of the network traffic

It also offers Email Analysis, Web Analysis, and Transaction Analysis modules, which allow you to quickly view the email traffic

It also offers custom filtering options, data export, customizable interface, and more



Colasoft Capsa Network Analyzer : Screenshot


Project 1 - Colasoft Capsa [Capturing]
File Edit View Project Tools Window Help
New Open Save Back Forward Up Start Stop Settings Adapter Filter Log Diagnosis Name Table Filter Table Options
Project Explorer
Project 1 (3)
Protocol Explorer (1)
Ethernet II (2)
Physical Explorer (4)
Local Segment (4)
Gateways[DEMO] (1)
Broadcast Addresses (1)
Multicast Addresses[DEMO]
IP Explorer (3)
Local Subnets[DEMO] (1)
Internet Addresses (1)
Multicast Addresses[DEMO]
Summary Diagnoses Endpoints Protocols Conversations Packets Logs
Type All
For Help, press F1

Packets: 6,368

No.	Absolute Time	Source	Destination
1	18:34:32.575909	192.168.1.123:1027	205.152.144.235:domain
2	18:34:32.591164	205.152.144.235:domain	192.168.1.123:1027
3	18:34:32.597752	192.168.1.123:2940	snapfiles.com:www-http
4	18:34:32.598731	00:14:BF:A9:B5:EB	FF:FF:FF:FF:FF:FF
5	18:34:32.679580	snapfiles.com:www-http	192.168.1.123:2940
6	18:34:32.679768	192.168.1.123:2940	snapfiles.com:www-http

Project Status

Packet filters:	No filters enabl...
Error packets:	0
Packets captured:	6,368
Packets lost:	0
Packets accepted:	6,368
Packets rejected:	0

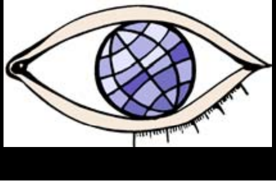
Endpoints: 27

Name	Total Bytes	Total Packets
Local Segment	[illegible] MB	4,782
Local Host	DEMO	DEMO
00:0E:A6:24:50:9E	[illegible] MB	4,772
192.168.1.123	DEMO	DEMO
Giga-byte Tech:6E:DD:F3	310.839 KB	1,520
192.168.1.4	310.651 KB	1,517
00:11:2F:23:F5:29	3.827 KB	28
192.168.1.9	3.765 KB	27
00:0F:66:FC:B5:3E	DEMO	DEMO
Gateways	DEMO	DEMO
00:14:BF:A9:B5:EB	1.415 MB	4,777
images.webattack.com	DEMO	DEMO
snapfiles.com	DEMO	DEMO
192.168.1.1	128.376 KB	434
pagead.l.google.com	DEMO	DEMO
snapfiles.net	DEMO	DEMO
205.152.144.235	DEMO	DEMO
205.152.132.235	DEMO	DEMO
Broadcast Addresses	197.762 KB	1,564
FF:FF:FF:FF:FF:FF	DEMO	DEMO
239.255.255.250	121.904 KB	370
192.168.1.255	DEMO	DEMO
Multicast Addresses	DEMO	DEMO
01:00:5E:7F:FF:FA	DEMO	DEMO
239.255.255.250	512 B	8

Project Status

Packet filters:	No filters enabl...
Error packets:	0
Packets captured:	6,340
Packets lost:	0
Packets accepted:	6,340
Packets rejected:	0

CommView



CommView is a program for monitoring the network activity capable of capturing and analyzing packets on any Ethernet network

It gathers information about data flowing on a LAN and decodes the analyzed data

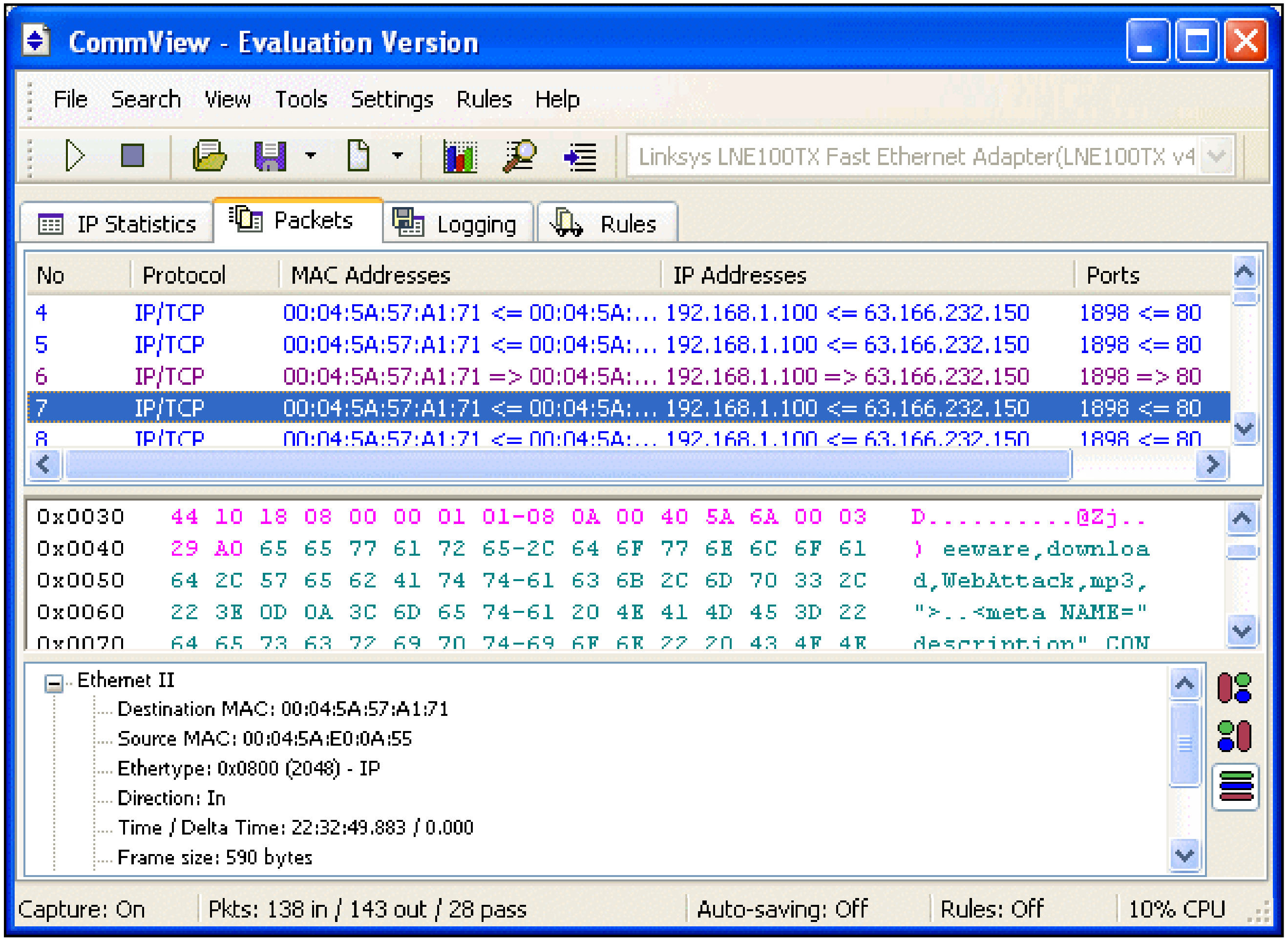
With CommView, you can view the list of network connections and vital IP statistics and examine individual packets

It decodes the IP packets down to the lowest layer with full analysis of the main IP protocols: TCP, UDP, and ICMP

It also provides full access to the raw data

It saves the captured packets to log files for future analysis

CommView: Screenshot


CommView - Evaluation Version
File
Search
View
Tools
Settings
Rules
Help
Linksys LNE100TX Fast Ethernet Adapter(LNE100TX v4
IP Statistics
Packets
Logging
Rules

No	Protocol	MAC Addresses	IP Addresses	Ports
4	IP/TCP	00:04:5A:57:A1:71 <= 00:04:5A:...	192.168.1.100 <= 63.166.232.150	1898 <= 80
5	IP/TCP	00:04:5A:57:A1:71 <= 00:04:5A:...	192.168.1.100 <= 63.166.232.150	1898 <= 80
6	IP/TCP	00:04:5A:57:A1:71 => 00:04:5A:...	192.168.1.100 => 63.166.232.150	1898 => 80
7	IP/TCP	00:04:5A:57:A1:71 <= 00:04:5A:...	192.168.1.100 <= 63.166.232.150	1898 <= 80
8	IP/TCP	00:04:5A:57:A1:71 <= 00:04:5A:...	192.168.1.100 <= 63.166.232.150	1898 <= 80

```
0x0030   44 10 18 08 00 00 01 01-08 0A 00 40 5A 6A 00 03   D..........@Zj..
0x0040   29 A0 65 65 77 61 72 65-2C 64 6F 77 6E 6C 6F 61   ) eeware,downloa
0x0050   64 2C 57 65 62 41 74 74-61 63 6B 2C 6D 70 33 2C   d,WebAttack,mp3,
0x0060   22 3E 0D 0A 3C 6D 65 74-61 20 4E 41 4D 45 3D 22   ">..<meta NAME="
0x0070   64 65 73 63 72 69 70 74-69 6F 6E 22 20 43 4F 4E   description" CON
```

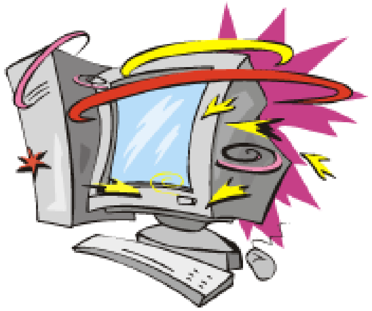
```
⊟ Ethernet II
    Destination MAC: 00:04:5A:57:A1:71
    Source MAC: 00:04:5A:E0:0A:55
    Ethertype: 0x0800 (2048) - IP
    Direction: In
    Time / Delta Time: 22:32:49.883 / 0.000
    Frame size: 590 bytes
```

Capture: On | Pkts: 138 in / 143 out / 28 pass | Auto-saving: Off | Rules: Off | 10% CPU

Sniffem

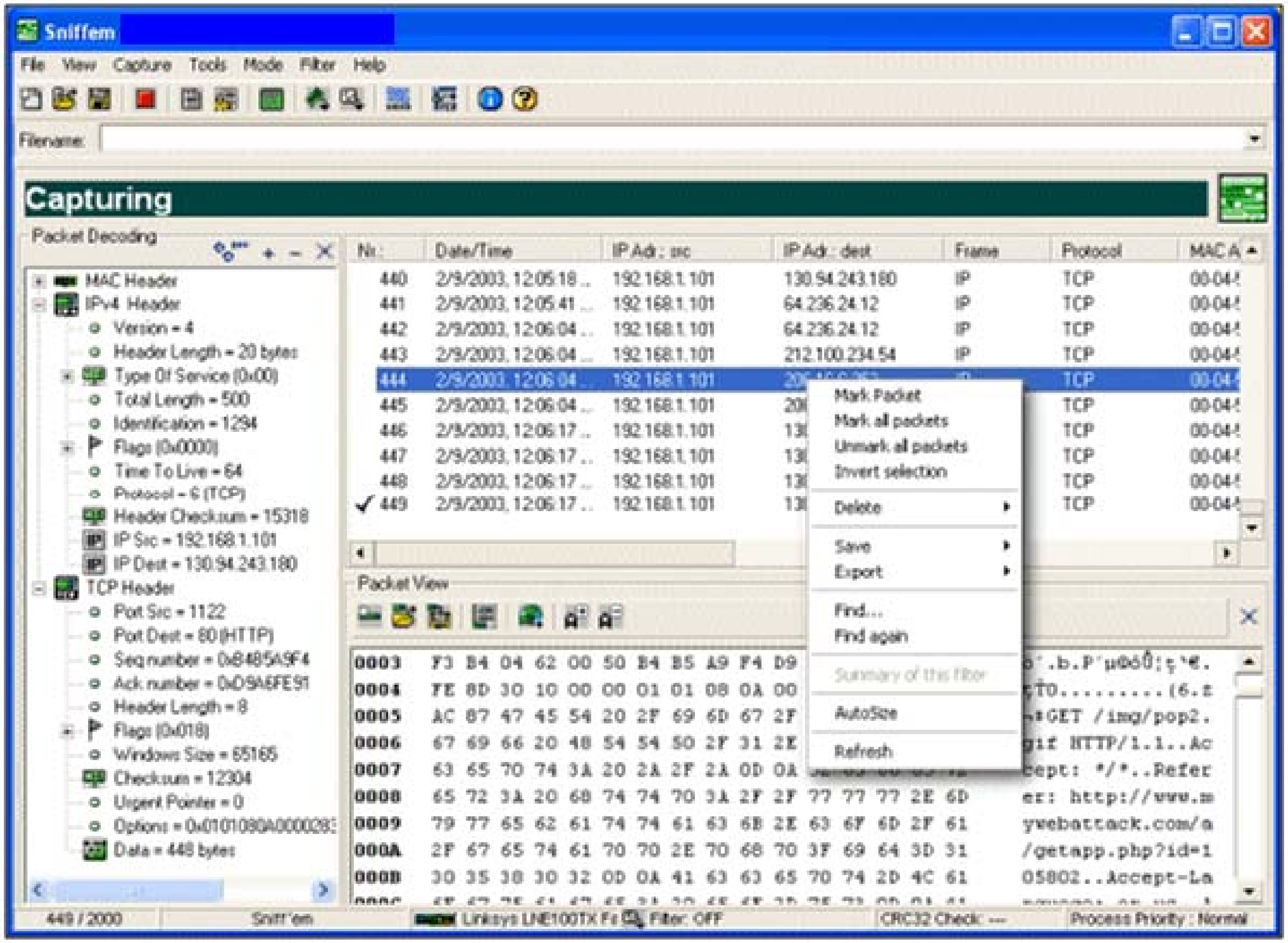
Sniffem is a Windows packet sniffer and network analyzer that captures, monitors, and decodes data traveling through the network including Dialup or DSL uplink

It features advanced hardware and software filtering options, TCP/IP traffic monitoring, as well as an IP address book that assigns aliases for frequently encountered IP addresses



Sniffem also comes with a built-in scheduler to enable capturing at the user defined intervals

Sniffem: Screenshot



- MAC Header
- IPv4 Header
  - Version = 4
  - Header Length = 20 bytes
  - Type Of Service (0x00)
  - Total Length = 500
  - Identification = 1294
  - Flags (0x0000)
  - Time To Live = 64
  - Protocol = 6 (TCP)
  - Header Checksum = 15318
  - IP Src = 192.168.1.101
  - IP Dest = 130.94.243.180
- TCP Header
  - Port Src = 1122
  - Port Dest = 80 (HTTP)
  - Seq number = 0xB485A9F4
  - Ack number = 0xD9A6FE91
  - Header Length = 8
  - Flags (0x018)
  - Windows Size = 65165
  - Checksum = 12304
  - Urgent Pointer = 0
  - Options = 0x0101080A000028
  - Data = 448 bytes

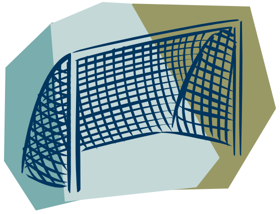
Nr.	Date/Time	IP Adr. src	IP Adr. dest	Frame	Protocol	MAC A
440	2/9/2003, 12:05:18 ...	192.168.1.101	130.94.243.180	IP	TCP	00-04-
441	2/9/2003, 12:05:41 ...	192.168.1.101	64.236.24.12	IP	TCP	00-04-
442	2/9/2003, 12:06:04 ...	192.168.1.101	64.236.24.12	IP	TCP	00-04-
443	2/9/2003, 12:06:04 ...	192.168.1.101	212.100.234.54	IP	TCP	00-04-
444	2/9/2003, 12:06:04 ...	192.168.1.101	20	IP	TCP	00-04-
445	2/9/2003, 12:06:04 ...	192.168.1.101	20		TCP	00-04-
446	2/9/2003, 12:06:17 ...	192.168.1.101	13		TCP	00-04-
447	2/9/2003, 12:06:17 ...	192.168.1.101	13		TCP	00-04-
448	2/9/2003, 12:06:17 ...	192.168.1.101	13		TCP	00-04-
✓ 449	2/9/2003, 12:06:17 ...	192.168.1.101	13		TCP	00-04-

```
0003   F3 B4 04 62 00 50 B4 B5 A9 F4 D9                      ó´.b.P´µ©ô
0004   FE 8D 30 10 00 00 01 01 08 0A 00                      ;T0.........(6.£
0005   AC 87 47 45 54 20 2F 69 6D 67 2F                      ¬‡GET /img/pop2.
0006   67 69 66 20 48 54 54 50 2F 31 2E                      gif HTTP/1.1..Ac
0007   63 65 70 74 3A 20 2A 2F 2A 0D 0A                      cept: */*..Refer
0008   65 72 3A 20 68 74 74 70 3A 2F 2F 77 77 77 2E 6D       er: http://www.m
0009   79 77 65 62 61 74 74 61 63 6B 2E 63 6F 6D 2F 61       ywebattack.com/a
000A   2F 67 65 74 61 70 70 2E 70 68 70 3F 69 64 3D 31       /getapp.php?id=1
000B   30 35 38 30 32 0D 0A 41 63 63 65 70 74 2D 4C 61       05802..Accept-La
```

449 / 2000 | Sniff'em | Linksys LNE100TX Fa | Filter: OFF | CRC32 Check: --- | Process Priority : Normal

NetResident

NetResident is a network traffic monitor that captures, stores, and analyzes all the packet traffic from selected protocols

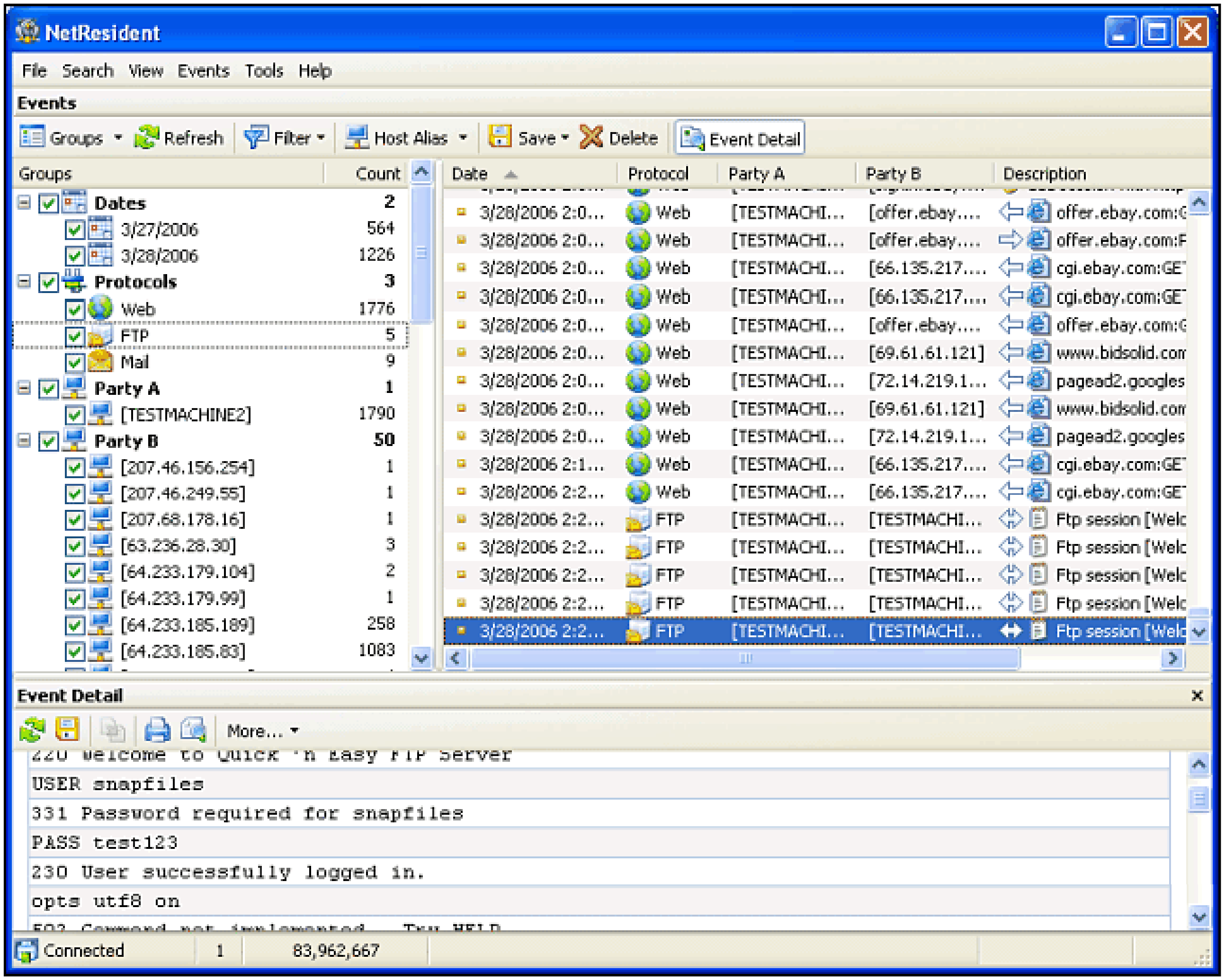


It reconstructs each event and displays a preview of the web page, email message, or other communication that takes place, including transmitted (unencrypted) passwords

NetResident supports standard HTTP, FTP, and Mail protocols, as well as special protocols via plug-ins (ICQ, MSN, News)

NetResident runs as a local service

NetResident: Screenshot


NetResident
File Search View Events Tools Help
Events
Groups Refresh Filter Host Alias Save Delete Event Detail
Event Detail
More...

Groups	Count
☑ **Dates**	**2**
☑ 3/27/2006	564
☑ 3/28/2006	1226
☑ **Protocols**	**3**
☑ Web	1776
☑ FTP	5
☑ Mail	9
☑ **Party A**	**1**
☑ [TESTMACHINE2]	1790
☑ **Party B**	**50**
☑ [207.46.156.254]	1
☑ [207.46.249.55]	1
☑ [207.68.178.16]	1
☑ [63.236.28.30]	3
☑ [64.233.179.104]	2
☑ [64.233.179.99]	1
☑ [64.233.185.189]	258
☑ [64.233.185.83]	1083

Date	Protocol	Party A	Party B	Description
3/28/2006 2:0...	Web	[TESTMACHI...	[offer.ebay....	⇦ offer.ebay.com:(
3/28/2006 2:0...	Web	[TESTMACHI...	[offer.ebay....	⇨ offer.ebay.com:F
3/28/2006 2:0...	Web	[TESTMACHI...	[66.135.217....	⇦ cgi.ebay.com:GE
3/28/2006 2:0...	Web	[TESTMACHI...	[66.135.217....	⇦ cgi.ebay.com:GE
3/28/2006 2:0...	Web	[TESTMACHI...	[offer.ebay....	⇦ offer.ebay.com:(
3/28/2006 2:0...	Web	[TESTMACHI...	[69.61.61.121]	⇦ www.bidsolid.com
3/28/2006 2:0...	Web	[TESTMACHI...	[72.14.219.1...	⇦ pagead2.googles
3/28/2006 2:0...	Web	[TESTMACHI...	[69.61.61.121]	⇦ www.bidsolid.com
3/28/2006 2:0...	Web	[TESTMACHI...	[72.14.219.1...	⇦ pagead2.googles
3/28/2006 2:1...	Web	[TESTMACHI...	[66.135.217....	⇦ cgi.ebay.com:GE
3/28/2006 2:2...	Web	[TESTMACHI...	[66.135.217....	⇦ cgi.ebay.com:GE
3/28/2006 2:2...	FTP	[TESTMACHI...	[TESTMACHI...	⇔ Ftp session [Welc
3/28/2006 2:2...	FTP	[TESTMACHI...	[TESTMACHI...	⇔ Ftp session [Welc
3/28/2006 2:2...	FTP	[TESTMACHI...	[TESTMACHI...	⇔ Ftp session [Welc
3/28/2006 2:2...	FTP	[TESTMACHI...	[TESTMACHI...	⇔ Ftp session [Welc
3/28/2006 2:2...	FTP	[TESTMACHI...	[TESTMACHI...	⇔ Ftp session [Welc

```
220 Welcome to Quick 'n Easy FTP Server
USER snapfiles
331 Password required for snapfiles
PASS test123
230 User successfully logged in.
opts utf8 on
502 Command not implemented - Try HELP
```

Connected 1 83,962,667

IP Sniffer

IP sniffer is a protocol analyzer that uses XP/2K Raw Socket features

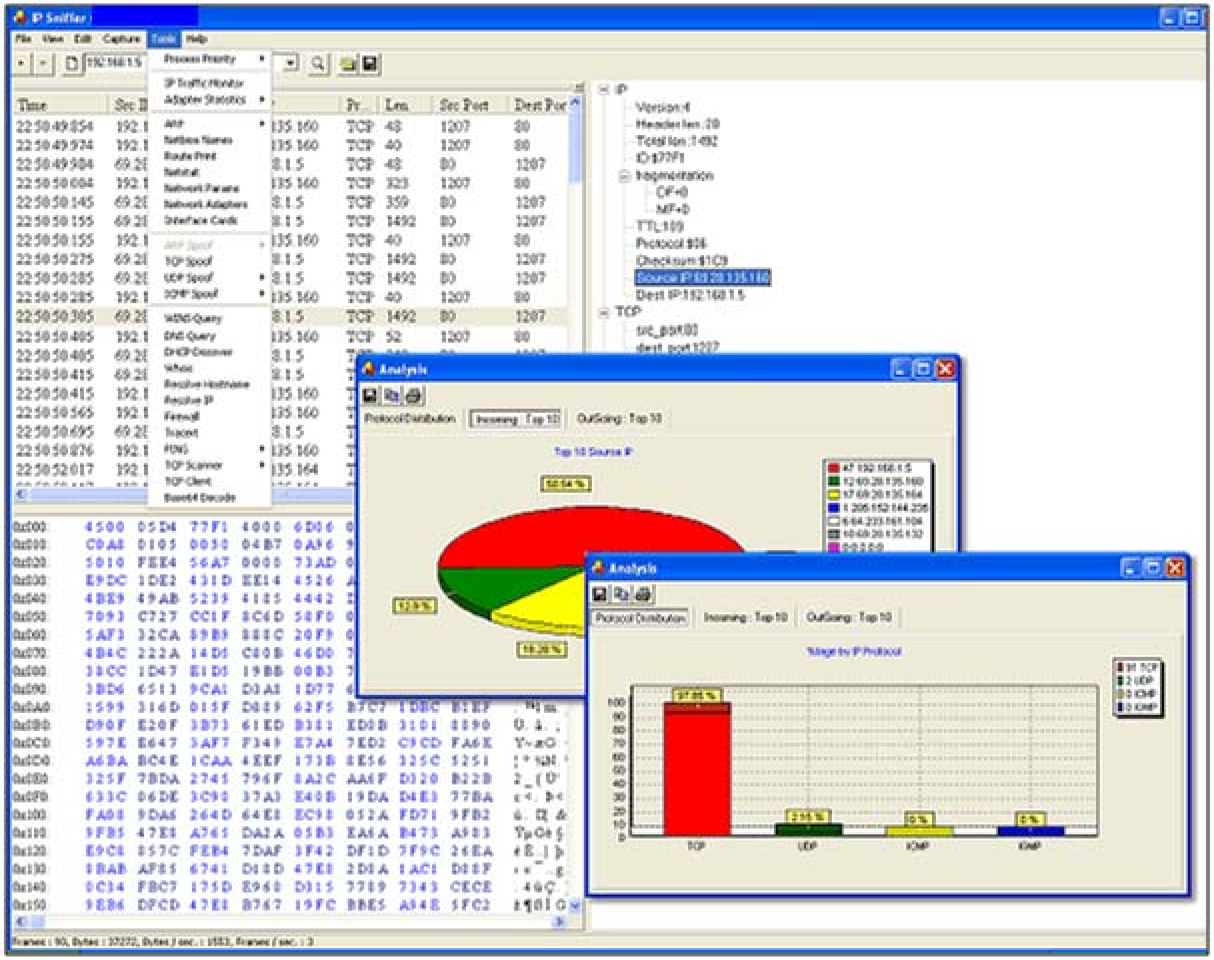
It supports filtering rules, adapter selection, packet decoding, advanced protocol description, and more

Detailed information about each packet is provided in a tree-style view, and the right-click menu allows to resolve or scan the selected source IP address

Additional features include:

- Adapter statistics
- IP traffic monitoring
- Traceroute
- Ping
- Port scanning
- TCP/UDP/ICMP spoofing options
- Open tcp/udp ports attached to process
- Mac address changing
- DNS/WINS/SNMP/WHOIS/DHCP queries

IP Sniffer: Screenshot



```
Time          Src I   Pr.  Len   Src Port  Dest Por
22:50:49.854  192.1   135.160  TCP  48    1207  80
22:50:49.934  192.1   135.160  TCP  40    1207  80
22:50:49.984  69.2    8.1.5    TCP  48    80    1207
22:50:50.004  192.1   135.160  TCP  323   1207  80
22:50:50.145  69.2    8.1.5    TCP  359   80    1207
22:50:50.155  69.2    8.1.5    TCP  1492  80    1207
22:50:50.155  192.1   135.160  TCP  40    1207  80
22:50:50.275  69.2    8.1.5    TCP  1492  80    1207
22:50:50.285  69.2    8.1.5    TCP  1492  80    1207
22:50:50.285  192.1   135.160  TCP  40    1207  80
22:50:50.305  69.2    8.1.5    TCP  1492  80    1207
22:50:50.405  192.1   135.160  TCP  52    1207  80
22:50:50.405  69.2    8.1.5
22:50:50.415  69.2    8.1.5
22:50:50.415  192.1   135.160
22:50:50.565  192.1   135.160
22:50:50.695  69.2    8.1.5
22:50:50.876  192.1   135.160
22:50:52.017  192.1   135.164
```

```
IP
  Version:4
  Header len :20
  Total len :1492
  ID:$77F1
  fragmentation
    DF=0
    MF=0
  TTL:109
  Protocol:$06
  Checksum:$1C9
  Source IP:69.20.135.160
  Dest IP:192.168.1.5
TCP
  src_port:80
  dest_port:1207
```

```
0x000   4500 05D4 77F1 4000 6D06
0x010   C0A8 0105 0050 04B7 0AF6
0x020   5010 FEE4 56A7 0000 73AD
0x030   E9DC 1DE2 431D EE14 4526
0x040   4BE9 49AB 5239 4185 4442
0x050   7093 C727 CC1F 8C4D 58F0
0x060   5AF3 32CA 89B9 888C 20F9
0x070   4B4C 222A 14D5 C80B 44D0
0x080   38CC 1D47 E1D5 19BB 00B3
0x090   3BD6 6513 9CA1 D3A1 1D77
0x0A0   1599 314D 015F D889 62F5 B7C7 1DBC B1EF
0x0B0   D90F E20F 3B73 61ED B111 ED0B 3101 8890   Ù. ↓ .
0x0C0   597E E647 3AF7 F349 E7A4 7ED2 C9CD FA6E   Y~.æO
0x0D0   A6BA BC4E 1CAA 4EEF 173B 8E56 325C 5251   ¦ º %M
0x0E0   325F 7BDA 2745 796F 8A2C AA6F D120 B22B   2_{Ú'
0x0F0   633C 06DE 3C90 37A3 E40B 19DA D4E3 77BA   c<. Þ<
0x100   FA08 9DA6 264D 64E8 EC98 052A FD71 9FB2   ú. Ħ &
0x110   9FB5 47E8 A765 DA2A 05B3 EA6A B473 A983   Ÿµ G è §
0x120   E9C8 857C FEB4 7DAF 3F42 DF1D 7F9C 26EA   éÈ_|}
0x130   8BAB AF85 6741 D88D 47E8 2D8A 8AC8 D88F   « «   g
0x140   0C34 FBC7 175D E960 D315 7789 7343 CECE    4ûÇ
0x150   9E86 DFCD 47E8 B767 19FC BBE5 A54E 5FC2   ž¶ßÍ G
```

Frames : 90, Bytes : 37272, Bytes / sec. : 1553, Frames / sec. : 3

Sniphere

Sniphere is a WinPCAP network sniffer that supports most of common protocols

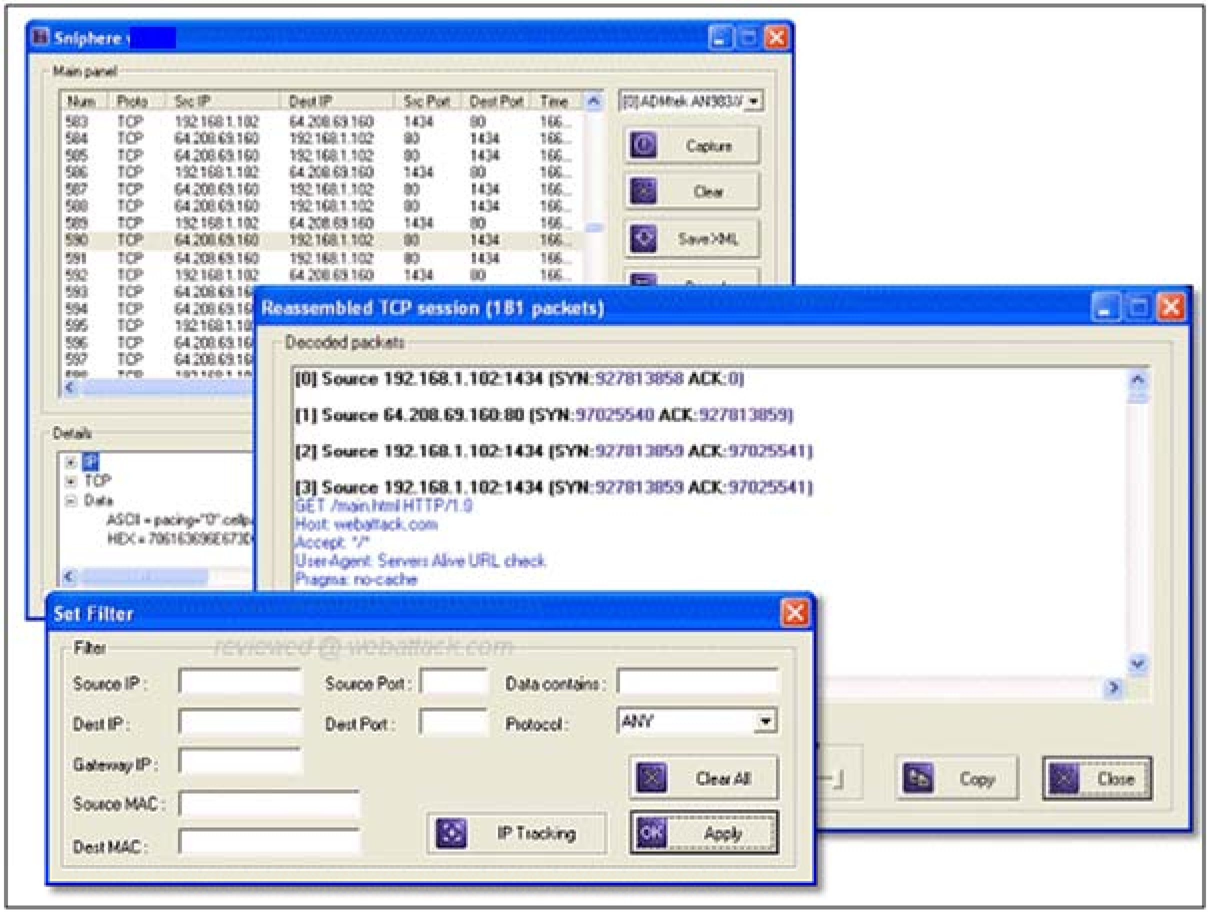
It can be used on ethernet devices and supports PPPoE modems

Sniphere allows to set filters based on IP, Mac Address, ports, protocol etc. and also decodes packages into an easy to understand format

In addition, session logs can be saved in XML format and selected packets copied to clipboard

Sniphere supports most common protocols, including IP, TCP, UDP, and ICMP

Sniphere: Screenshot



Sniphere [redacted]

Main panel

```
Num  Proto  Src IP         Dest IP        Src Port  Dest Port  Time
583  TCP    192.168.1.102  64.208.69.160  1434      80         166...
584  TCP    64.208.69.160  192.168.1.102  80        1434       166...
585  TCP    64.208.69.160  192.168.1.102  80        1434       166...
586  TCP    192.168.1.102  64.208.69.160  1434      80         166...
587  TCP    64.208.69.160  192.168.1.102  80        1434       166...
588  TCP    64.208.69.160  192.168.1.102  80        1434       166...
589  TCP    192.168.1.102  64.208.69.160  1434      80         166...
590  TCP    64.208.69.160  192.168.1.102  80        1434       166...
591  TCP    64.208.69.160  192.168.1.102  80        1434       166...
592  TCP    192.168.1.102  64.208.69.160  1434      80         166...
593  TCP    64.208.69.16
594  TCP    64.208.69.16
595  TCP    192.168.1.10
596  TCP    64.208.69.16
597  TCP    64.208.69.16
```

[0] ADMtek AN983/

Details

```
+ IP
+ TCP
- Data
    ASCII = pacing="0" cellp
    HEX = 706163696E6730
```

Reassembled TCP session (181 packets)

Decoded packets

```
[0] Source 192.168.1.102:1434 (SYN:927813858 ACK:0)

[1] Source 64.208.69.160:80 (SYN:97025540 ACK:927813859)

[2] Source 192.168.1.102:1434 (SYN:927813859 ACK:97025541)

[3] Source 192.168.1.102:1434 (SYN:927813859 ACK:97025541)
GET /main.html HTTP/1.0
Host: webattack.com
Accept: */*
User-Agent: Servers Alive URL check
Pragma: no-cache
```

Set Filter

Filter

Source IP:

Dest IP:

Gateway IP:

Source MAC:

Dest MAC:

Source Port:

Dest Port:

Data contains:

Protocol: ANY

IE HTTP Analyzer

IE HTTP Analyzer is an add-in for Internet Explorer, that allows to capture HTTP/HTTPS traffic in real-time

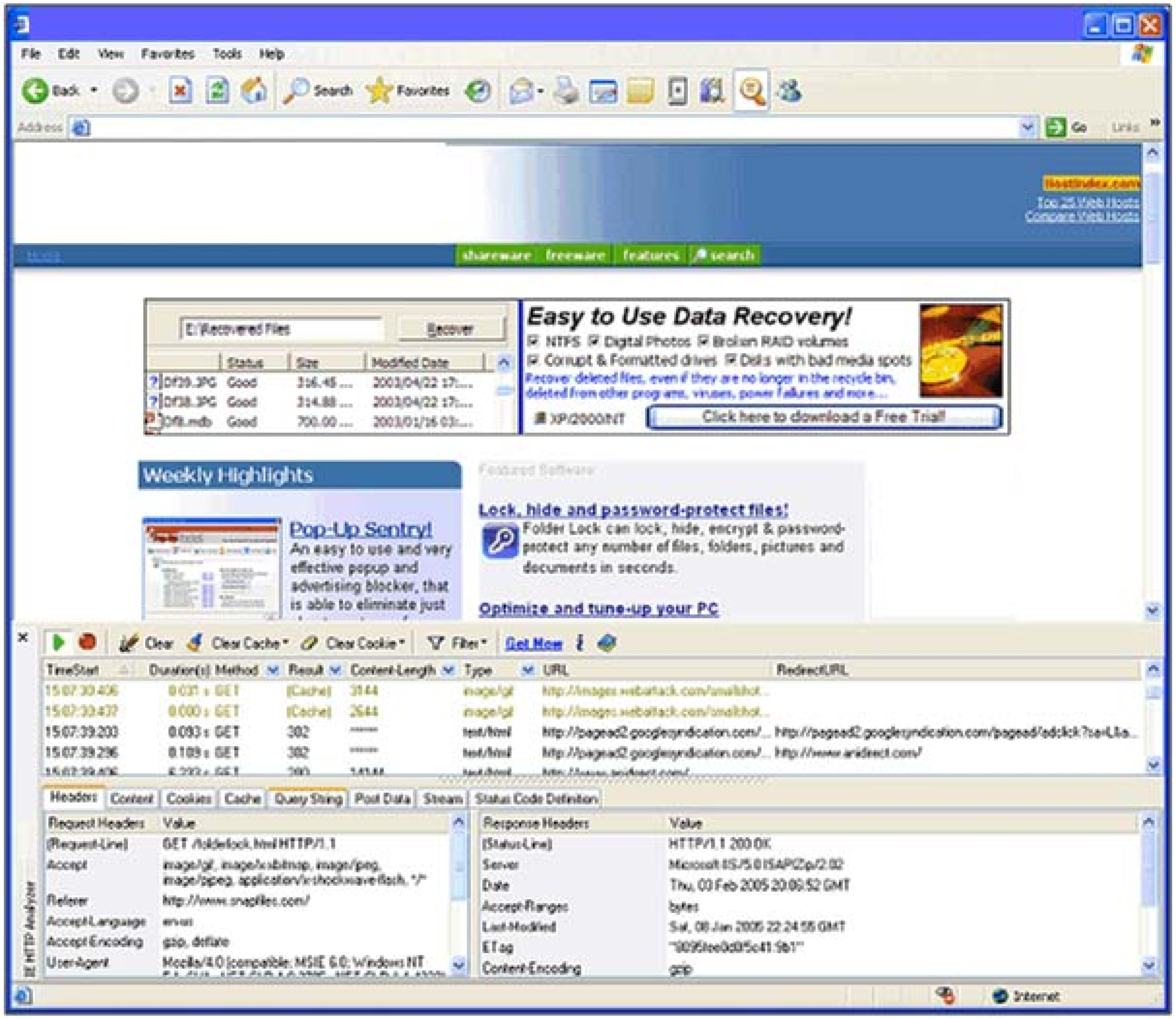
It displays a wide range of information, including Header, Content, Cookies, Query Strings, Post data, and redirection URLs

It also provides cache information and session clearing, as well as HTTP status code information and several filtering options

A useful developer tool for performance analysis, debugging, and diagnostics

IE HTTP Analyzer integrates into lower part of IE browser window and can be opened/closed from IE toolbar

IE HTTP Analyzer: Screenshot



File Edit View Favorites Tools Help
Back Search Favorites
Address Go Links
shareware freeware features search
Recover
Status Size Modified Date
Weekly Highlights
Featured Software
Clear Clear Cache Clear Cookie Filter Get Now
Headers Content Cookies Cache Query String Post Data Stream Status Code Definition
IE HTTP Analyzer
Internet

Easy to Use Data Recovery!

☑ NTFS ☑ Digital Photos ☑ Broken RAID volumes
☑ Corrupt & Formatted drives ☑ Disks with bad media spots

Recover deleted files, even if they are no longer in the recycle bin, deleted from other programs, viruses, power failures and more...

XP/2000/NT — Click here to download a Free Trial!

Pop-Up Sentry! An easy to use and very effective popup and advertising blocker, that is able to eliminate just

Lock, hide and password-protect files! Folder Lock can lock, hide, encrypt & password-protect any number of files, folders, pictures and documents in seconds.

Optimize and tune-up your PC

TimeStart	Duration(s)	Method	Result	Content-Length	Type	URL	RedirectURL
15:07:30.406	0.031 s	GET	(Cache)	3144	image/gif	http://images.webattack.com/smallshot...	
15:07:30.437	0.000 s	GET	(Cache)	2644	image/gif	http://images.webattack.com/smallshot...	
15:07:39.203	0.093 s	GET	302	******	text/html	http://pagead2.googlesyndication.com/...	http://pagead2.googlesyndication.com/pagead/adclick?sa=L&a...
15:07:39.296	0.109 s	GET	302	******	text/html	http://pagead2.googlesyndication.com/...	http://www.aridirect.com/

Request Headers	Value
(Request-Line)	GET /folderlock.html HTTP/1.1
Accept	image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer	http://www.snapfiles.com/
Accept-Language	en-us
Accept-Encoding	gzip, deflate
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT

Response Headers	Value
(Status-Line)	HTTP/1.1 200 OK
Server	Microsoft-IIS/5.0 ISAPIZip/2.02
Date	Thu, 03 Feb 2005 20:00:52 GMT
Accept-Ranges	bytes
Last-Modified	Sat, 08 Jan 2005 22:24:55 GMT
ETag	"0095fee0d05c41:9b1"
Content-Encoding	gzip

CEH™ Certified Ethical Hacker

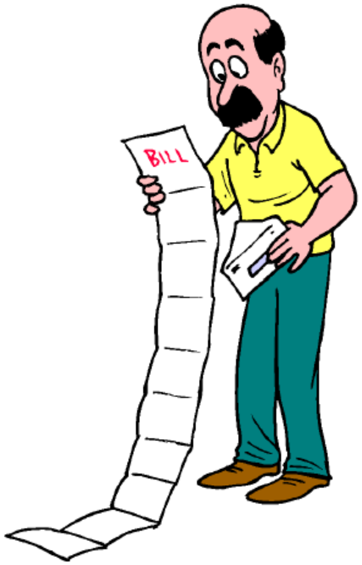
BillSniff

BillSniff is a network protocol analyzer (sniffer) that provides detailed information about current traffic, as well as overall protocol statistics

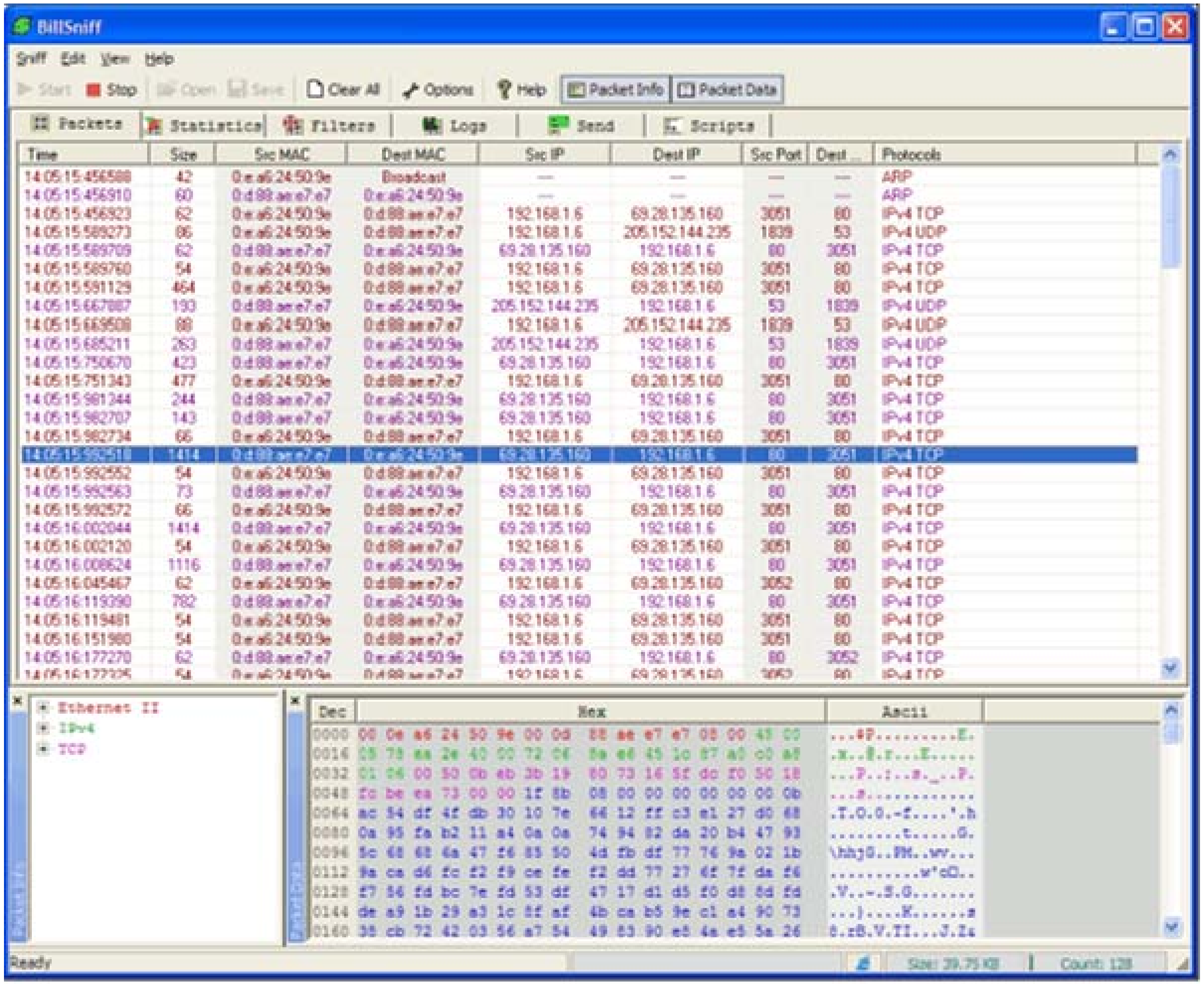
It supports various protocols including ip4, TCP, UDP, IEEE 802.2 frame, Ethernet II frame, NetBios, and IPX

In addition to real-time monitoring, it includes an extensive array of filter options that allows to limit capture based on IP, Port, Protocol, MAC address, packet size and other criteria, as well as graphical statistics for network layers

BillSniff can also be used to send packets and script custom protocols



BillSniff: Screenshot


BillSniff
Sniff Edit View Help
Start Stop Open Save Clear All Options Help Packet Info Packet Data
Packets Statistics Filters Logs Send Scripts
Ethernet II
IPv4
TCP
Packet Info
Packet Data

Time	Size	Src MAC	Dest MAC	Src IP	Dest IP	Src Port	Dest ...	Protocols
14:05:15.456588	42	0:e:a6:24:50:9e	Broadcast	---	---	---	---	ARP
14:05:15.456910	60	0:d:88:ae:e7:e7	0:e:a6:24:50:9e	---	---	---	---	ARP
14:05:15.456923	62	0:e:a6:24:50:9e	0:d:88:ae:e7:e7	192.168.1.6	69.28.135.160	3051	80	IPv4 TCP
14:05:15.589273	86	0:e:a6:24:50:9e	0:d:88:ae:e7:e7	192.168.1.6	205.152.144.235	1839	53	IPv4 UDP
14:05:15.589709	62	0:d:88:ae:e7:e7	0:e:a6:24:50:9e	69.28.135.160	192.168.1.6	80	3051	IPv4 TCP
14:05:15.589760	54	0:e:a6:24:50:9e	0:d:88:ae:e7:e7	192.168.1.6	69.28.135.160	3051	80	IPv4 TCP
14:05:15.591129	464	0:e:a6:24:50:9e	0:d:88:ae:e7:e7	192.168.1.6	69.28.135.160	3051	80	IPv4 TCP
14:05:15.667887	190	0:d:88:ae:e7:e7	0:e:a6:24:50:9e	205.152.144.235	192.168.1.6	53	1839	IPv4 UDP
14:05:15.669508	88	0:e:a6:24:50:9e	0:d:88:ae:e7:e7	192.168.1.6	205.152.144.235	1839	53	IPv4 UDP
14:05:15.685211	263	0:d:88:ae:e7:e7	0:e:a6:24:50:9e	205.152.144.235	192.168.1.6	53	1839	IPv4 UDP
14:05:15.750670	423	0:d:88:ae:e7:e7	0:e:a6:24:50:9e	69.28.135.160	192.168.1.6	80	3051	IPv4 TCP
14:05:15.751343	477	0:e:a6:24:50:9e	0:d:88:ae:e7:e7	192.168.1.6	69.28.135.160	3051	80	IPv4 TCP
14:05:15.981344	244	0:d:88:ae:e7:e7	0:e:a6:24:50:9e	69.28.135.160	192.168.1.6	80	3051	IPv4 TCP
14:05:15.982707	143	0:d:88:ae:e7:e7	0:e:a6:24:50:9e	69.28.135.160	192.168.1.6	80	3051	IPv4 TCP
14:05:15.982734	66	0:e:a6:24:50:9e	0:d:88:ae:e7:e7	192.168.1.6	69.28.135.160	3051	80	IPv4 TCP
14:05:15.992518	1414	0:d:88:ae:e7:e7	0:e:a6:24:50:9e	69.28.135.160	192.168.1.6	80	3051	IPv4 TCP
14:05:15.992552	54	0:e:a6:24:50:9e	0:d:88:ae:e7:e7	192.168.1.6	69.28.135.160	3051	80	IPv4 TCP
14:05:15.992563	73	0:d:88:ae:e7:e7	0:e:a6:24:50:9e	69.28.135.160	192.168.1.6	80	3051	IPv4 TCP
14:05:15.992572	66	0:e:a6:24:50:9e	0:d:88:ae:e7:e7	192.168.1.6	69.28.135.160	3051	80	IPv4 TCP
14:05:16.002044	1414	0:d:88:ae:e7:e7	0:e:a6:24:50:9e	69.28.135.160	192.168.1.6	80	3051	IPv4 TCP
14:05:16.002120	54	0:e:a6:24:50:9e	0:d:88:ae:e7:e7	192.168.1.6	69.28.135.160	3051	80	IPv4 TCP
14:05:16.008624	1116	0:d:88:ae:e7:e7	0:e:a6:24:50:9e	69.28.135.160	192.168.1.6	80	3051	IPv4 TCP
14:05:16.045467	62	0:e:a6:24:50:9e	0:d:88:ae:e7:e7	192.168.1.6	69.28.135.160	3052	80	IPv4 TCP
14:05:16.119390	782	0:d:88:ae:e7:e7	0:e:a6:24:50:9e	69.28.135.160	192.168.1.6	80	3051	IPv4 TCP
14:05:16.119481	54	0:e:a6:24:50:9e	0:d:88:ae:e7:e7	192.168.1.6	69.28.135.160	3051	80	IPv4 TCP
14:05:16.151980	54	0:e:a6:24:50:9e	0:d:88:ae:e7:e7	192.168.1.6	69.28.135.160	3051	80	IPv4 TCP
14:05:16.177270	62	0:d:88:ae:e7:e7	0:e:a6:24:50:9e	69.28.135.160	192.168.1.6	80	3052	IPv4 TCP
14:05:16.177325	54	0:e:a6:24:50:9e	0:d:88:ae:e7:e7	192.168.1.6	69.28.135.160	3052	80	IPv4 TCP

```
Dec   Hex                                              Ascii
0000  00 0e a6 24 50 9e 00 0d  88 ae e7 e7 08 00 45 00  ...$P.........E.
0016  05 78 ea 2e 40 00 72 06  8a e6 45 1c 87 a0 c0 a8  .x...@.r...E.....
0032  01 06 00 50 0b eb 3b 19  80 73 16 5f dc f0 50 18  ...P..;..s._..P.
0048  fc be ea 73 00 00 1f 8b  08 00 00 00 00 00 00 0b  ...s............
0064  ac 54 df 4f db 30 10 7e  66 12 ff c3 e1 27 d0 68  .T.O.0.~f....'.h
0080  0a 95 fa b2 11 a4 0a 0a  74 94 82 da 20 b4 47 93  ........t.....G.
0096  5c 68 68 6a 47 f6 85 50  4d fb df 77 76 9a 02 1b  \hhjG..PM..wv...
0112  9a ca d6 fc f2 f9 ce fe  f2 dd 77 27 6f 7f da f6  ..........w'oD..
0128  f7 56 fd bc 7e fd 53 df  47 17 d1 d5 f0 d8 8d fd  .V..~.S.G.......
0144  de a9 1b 29 a3 1c 8f af  4b ca b5 9e c1 a4 90 73  ...)....K......s
0160  38 cb 72 42 03 56 a7 54  49 83 90 e5 4a e5 5a 26  8.rB.V.TI...J.Z&
```

Ready   Size: 39.75 KB   Count: 128

EC-Council

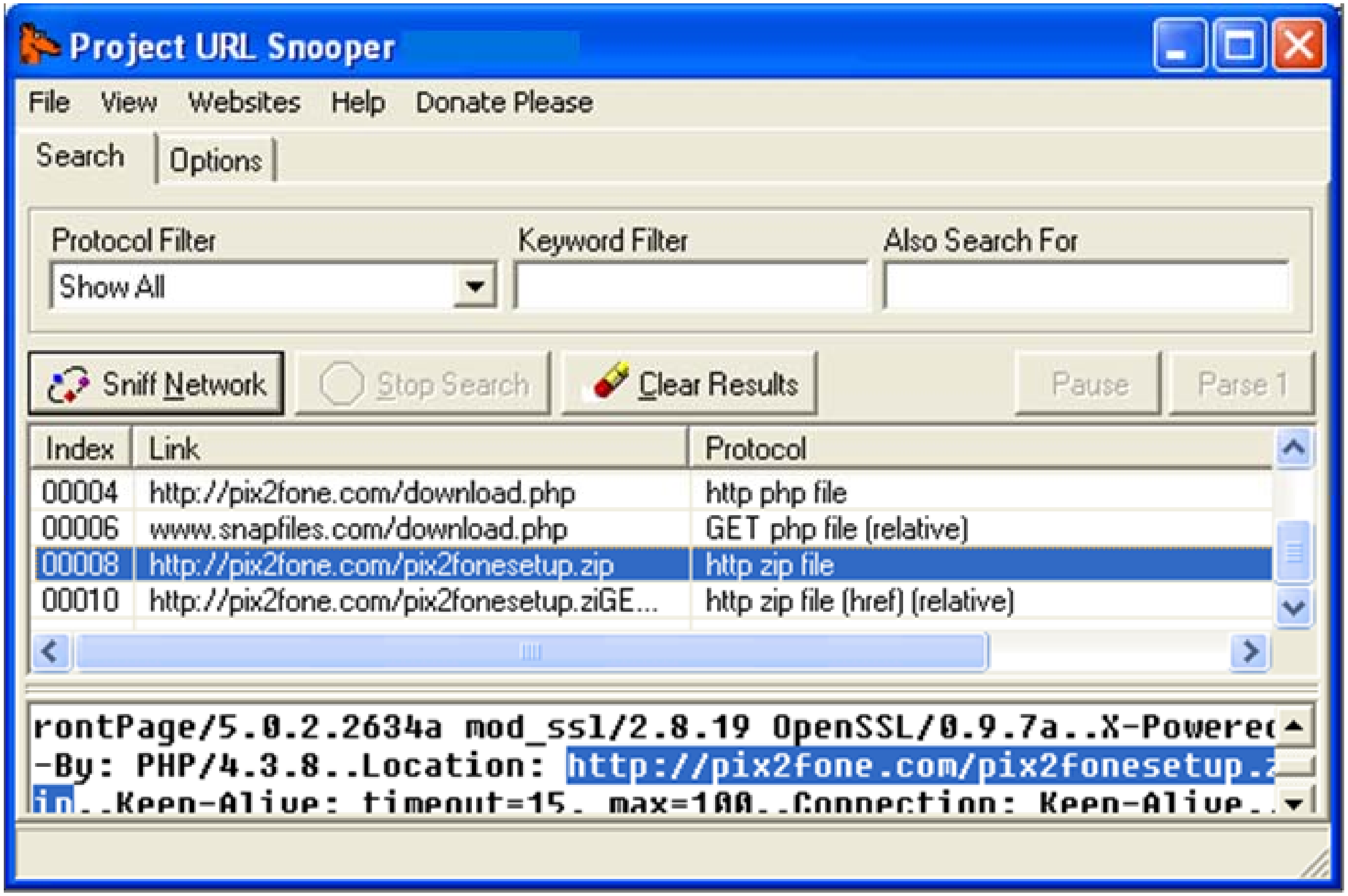
URL Snooper

URL Snooper enables to extract links that are masked or hidden behind scripts and/or server redirections

It uses WinPcap and acts as a small network sniffer, that automatically filters all URL requests that it encounters

You can further filter the list to only show multimedia links

URL Snooper: Screenshot



Protocol Filter: Show All
Keyword Filter:
Also Search For:

Index	Link	Protocol
00004	http://pix2fone.com/download.php	http php file
00006	www.snapfiles.com/download.php	GET php file (relative)
00008	http://pix2fone.com/pix2fonesetup.zip	http zip file
00010	http://pix2fone.com/pix2fonesetup.ziGE...	http zip file (href) (relative)

```
rontPage/5.0.2.2634a mod_ssl/2.8.19 OpenSSL/0.9.7a..X-Powere
-By: PHP/4.3.8..Location: http://pix2fone.com/pix2fonesetup.z
ip..Keep-Alive: timeout=15, max=100..Connection: Keep-Alive..
```

EtherDetect Packet Sniffer

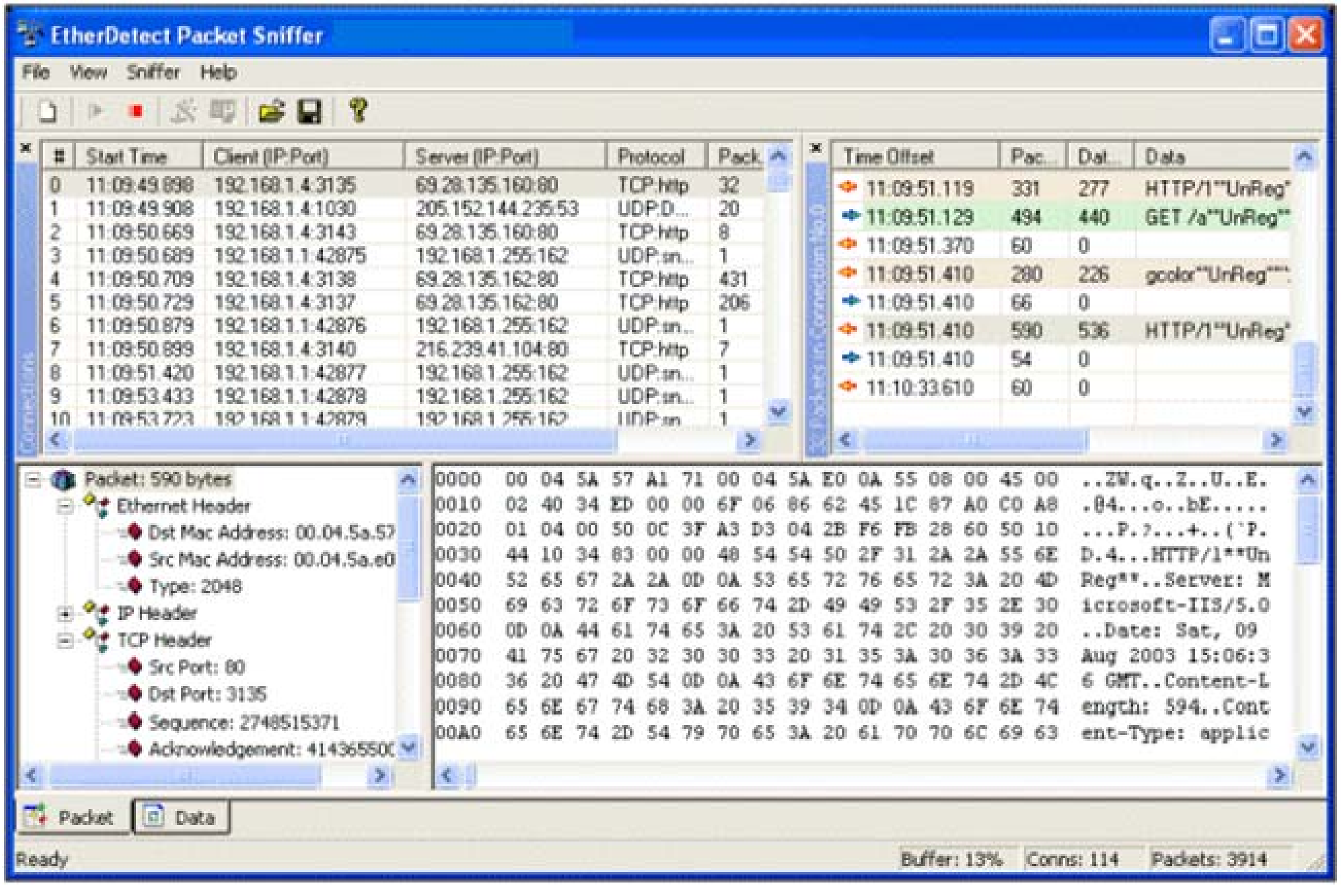
EtherDetect Packet Sniffer is an easy to use packet sniffer and network protocol analyzer

It captures and groups all the network traffic and allows you to view real-time details for each packet as well as the content

It can also set up filters based on the IP address and port and saves the captured traffic to file for later review

The built-in viewer supports syntax highlighting for HTML, ASP, and XML

EtherDetect Packet Sniffer: Screenshot



#	Start Time	Client (IP:Port)	Server (IP:Port)	Protocol	Pack
0	11:09:49.898	192.168.1.4:3135	69.28.135.160:80	TCP:http	32
1	11:09:49.908	192.168.1.4:1030	205.152.144.235:53	UDP:D...	20
2	11:09:50.669	192.168.1.4:3143	69.28.135.160:80	TCP:http	8
3	11:09:50.689	192.168.1.1:42875	192.168.1.255:162	UDP:sn...	1
4	11:09:50.709	192.168.1.4:3138	69.28.135.162:80	TCP:http	431
5	11:09:50.729	192.168.1.4:3137	69.28.135.162:80	TCP:http	206
6	11:09:50.879	192.168.1.1:42876	192.168.1.255:162	UDP:sn...	1
7	11:09:50.899	192.168.1.4:3140	216.239.41.104:80	TCP:http	7
8	11:09:51.420	192.168.1.1:42877	192.168.1.255:162	UDP:sn...	1
9	11:09:53.433	192.168.1.1:42878	192.168.1.255:162	UDP:sn...	1
10	11:09:53.723	192.168.1.1:42879	192.168.1.255:162	UDP:sn	1

Time Offset	Pac...	Dat...	Data
11:09:51.119	331	277	HTTP/1"UnReg"
11:09:51.129	494	440	GET /a"UnReg"
11:09:51.370	60	0	
11:09:51.410	280	226	gcolor"UnReg"":
11:09:51.410	66	0	
11:09:51.410	590	536	HTTP/1"UnReg"
11:09:51.410	54	0	
11:10:33.610	60	0	

- Packet: 590 bytes
  - Ethernet Header
    - Dst Mac Address: 00.04.5a.57
    - Src Mac Address: 00.04.5a.e0
    - Type: 2048
  - IP Header
  - TCP Header
    - Src Port: 80
    - Dst Port: 3135
    - Sequence: 2748515371
    - Acknowledgement: 41436550C

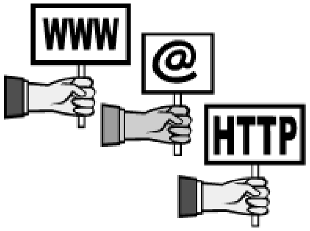
```
0000   00 04 5A 57 A1 71 00 04 5A E0 0A 55 08 00 45 00   ..ZW.q..Z..U..E.
0010   02 40 34 ED 00 00 6F 06 86 62 45 1C 87 A0 C0 A8   .@4...o..bE.....
0020   01 04 00 50 0C 3F A3 D3 04 2B F6 FB 28 60 50 10   ...P.?...+..(`P.
0030   44 10 34 83 00 00 48 54 54 50 2F 31 2A 2A 55 6E   D.4...HTTP/1**Un
0040   52 65 67 2A 2A 0D 0A 53 65 72 76 65 72 3A 20 4D   Reg**..Server: M
0050   69 63 72 6F 73 6F 66 74 2D 49 49 53 2F 35 2E 30   icrosoft-IIS/5.0
0060   0D 0A 44 61 74 65 3A 20 53 61 74 2C 20 30 39 20   ..Date: Sat, 09
0070   41 75 67 20 32 30 30 33 20 31 35 3A 30 36 3A 33   Aug 2003 15:06:3
0080   36 20 47 4D 54 0D 0A 43 6F 6E 74 65 6E 74 2D 4C   6 GMT..Content-L
0090   65 6E 67 74 68 3A 20 35 39 34 0D 0A 43 6F 6E 74   ength: 594..Cont
00A0   65 6E 74 2D 54 79 70 65 3A 20 61 70 70 6C 69 63   ent-Type: applic
```

Ready   Buffer: 13%   Conns: 114   Packets: 3914

EffeTech HTTP Sniffer

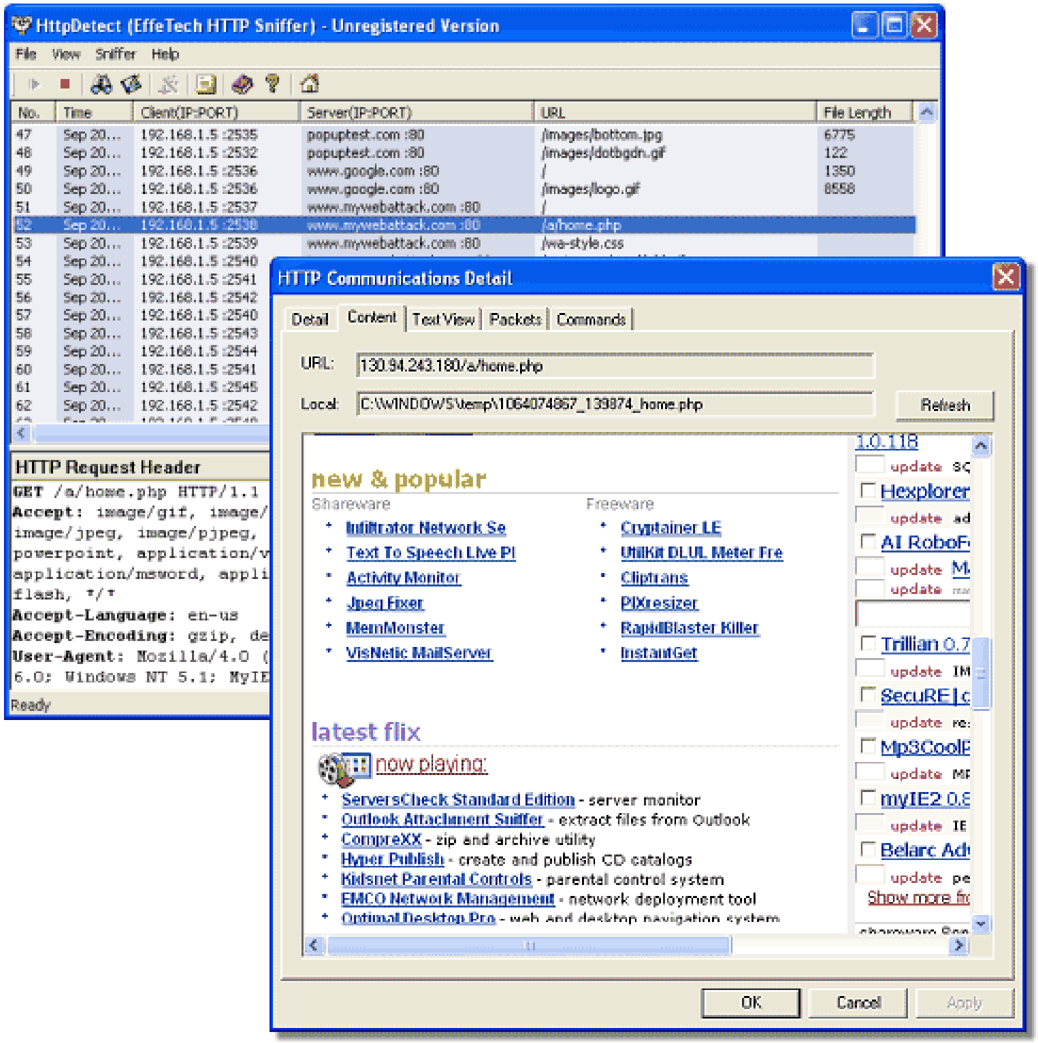
EffeTech HTTP Sniffer is a HTTP packet sniffer and protocol analyzer that is specialized for the web traffic

It can rebuild the HTTP sessions and reassemble files sent through the HTTP protocol



Main window displays a list of all logged connections, as well as the detailed information for the request and response headers; this allows for a quick overview without much details

EffeTech HTTP Sniffer: Screenshot


HttpDetect (EffeTech HTTP Sniffer) - Unregistered Version
File View Sniffer Help
HTTP Communications Detail
Detail Content Text View Packets Commands
Refresh
OK Cancel Apply
Ready

No.	Time	Client(IP:PORT)	Server(IP:PORT)	URL	File Length
47	Sep 20...	192.168.1.5 :2535	popuptest.com :80	/images/bottom.jpg	6775
48	Sep 20...	192.168.1.5 :2532	popuptest.com :80	/images/dotbgdn.gif	122
49	Sep 20...	192.168.1.5 :2536	www.google.com :80	/	1350
50	Sep 20...	192.168.1.5 :2536	www.google.com :80	/images/logo.gif	8558
51	Sep 20...	192.168.1.5 :2537	www.mywebattack.com :80	/	
52	Sep 20...	192.168.1.5 :2538	www.mywebattack.com :80	/a/home.php	
53	Sep 20...	192.168.1.5 :2539	www.mywebattack.com :80	/wa-style.css	
54	Sep 20...	192.168.1.5 :2540			
55	Sep 20...	192.168.1.5 :2541			
56	Sep 20...	192.168.1.5 :2542			
57	Sep 20...	192.168.1.5 :2540			
58	Sep 20...	192.168.1.5 :2543			
59	Sep 20...	192.168.1.5 :2544			
60	Sep 20...	192.168.1.5 :2541			
61	Sep 20...	192.168.1.5 :2545			
62	Sep 20...	192.168.1.5 :2542			

HTTP Request Header

```
GET /a/home.php HTTP/1.1
Accept: image/gif, image/
image/jpeg, image/pjpeg,
powerpoint, application/v
application/msword, appli
flash, */*
Accept-Language: en-us
Accept-Encoding: gzip, de
User-Agent: Mozilla/4.0 (
6.0; Windows NT 5.1; MyIE
```

URL: 130.94.243.180/a/home.php

Local: C:\WINDOWS\temp\1064074867_139874_home.php

new & popular

Shareware

- Infiltrator Network Se
- Text To Speech Live Pl
- Activity Monitor
- Jpeg Fixer
- MemMonster
- VisNetic MailServer

Freeware

- Cryptainer LE
- UtilKit DLUL Meter Fre
- Cliptrans
- PIXresizer
- RapidBlaster Killer
- InstantGet

latest flix

now playing:

- ServersCheck Standard Edition - server monitor
- Outlook Attachment Sniffer - extract files from Outlook
- CompreXX - zip and archive utility
- Hyper Publish - create and publish CD catalogs
- Kidsnet Parental Controls - parental control system
- EMCO Network Management - network deployment tool
- Optimal Desktop Pro - web and desktop navigation system

1.0.118
update sq
□ Hexplorer
update ad
□ AI RoboF
update M
update
□ Trillian 0.7
update IM
□ SecuRE|c
update re
□ Mp3CoolP
update MP
□ myIE2 0.8
update IE
□ Belarc Adv
update pe
Show more fr

AnalogX Packetmon

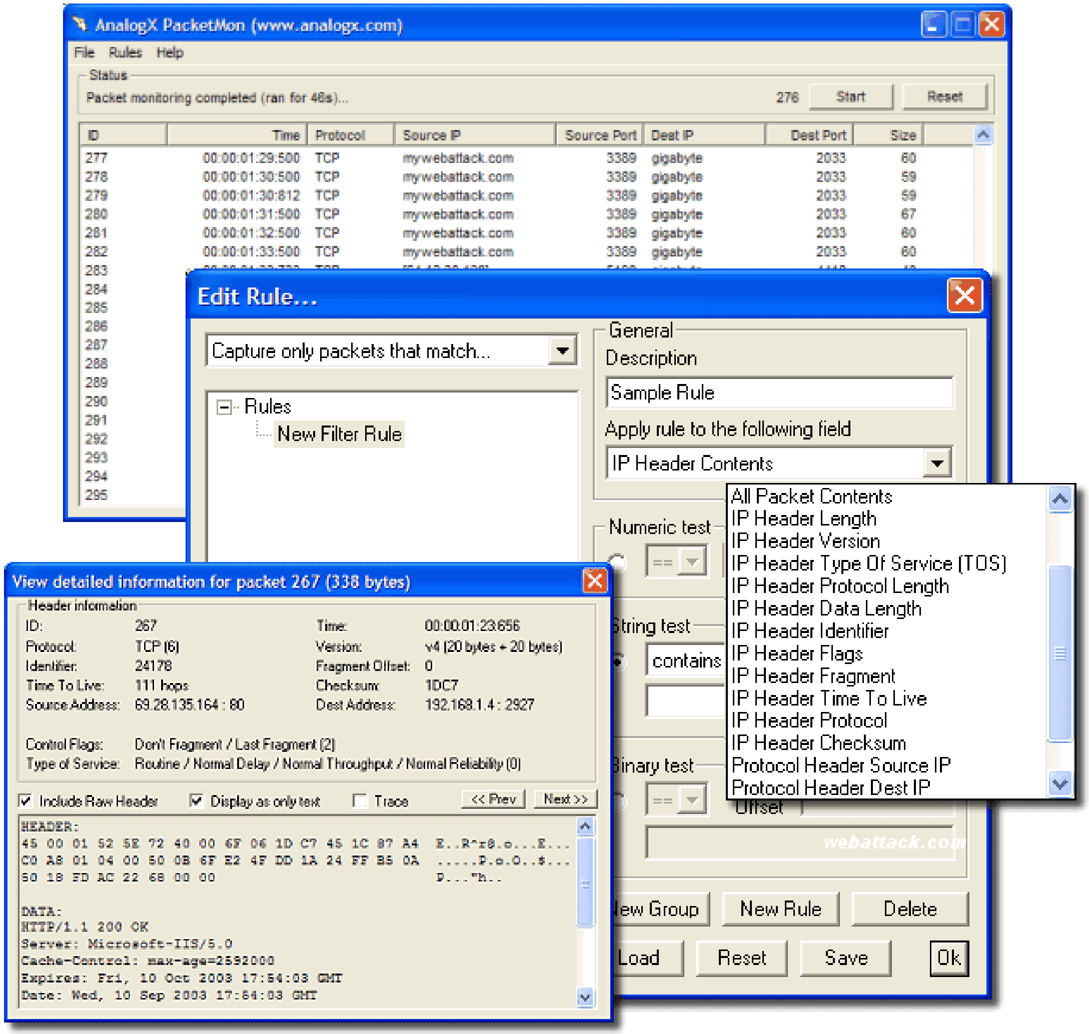
AnalogX Packetmon allows to capture IP packets that pass through the network's interface - whether they originated from the machine on which PacketMon is installed or a completely different machine on the network

Once the packet is received, it can use built in viewer to examine header as well as contents, and it can also export results into a standard comma-delimited file for further processing

PacketMon includes a powerful rule system that allows advanced users to narrow down packets

It captures to ensure you get exactly what you want, without having to dig through tons of unrelated information

AnalogX Packetmon: Screenshot



Status
Packet monitoring completed (ran for 46s)... 276

ID	Time	Protocol	Source IP	Source Port	Dest IP	Dest Port	Size
277	00:00:01:29:500	TCP	mywebattack.com	3389	gigabyte	2033	60
278	00:00:01:30:500	TCP	mywebattack.com	3389	gigabyte	2033	59
279	00:00:01:30:812	TCP	mywebattack.com	3389	gigabyte	2033	59
280	00:00:01:31:500	TCP	mywebattack.com	3389	gigabyte	2033	67
281	00:00:01:32:500	TCP	mywebattack.com	3389	gigabyte	2033	60
282	00:00:01:33:500	TCP	mywebattack.com	3389	gigabyte	2033	60
283							
284							
285							
286							
287							
288							
289							
290							
291							
292							
293							
294							
295							

Capture only packets that match...

Description: Sample Rule

Apply rule to the following field: IP Header Contents

- All Packet Contents
- IP Header Length
- IP Header Version
- IP Header Type Of Service (TOS)
- IP Header Protocol Length
- IP Header Data Length
- IP Header Identifier
- IP Header Flags
- IP Header Fragment
- IP Header Time To Live
- IP Header Protocol
- IP Header Checksum
- Protocol Header Source IP
- Protocol Header Dest IP

== contains

View detailed information for packet 267 (338 bytes)

Header information

ID:	267	Time:	00:00:01:23:656
Protocol:	TCP (6)	Version:	v4 (20 bytes + 20 bytes)
Identifier:	24178	Fragment Offset:	0
Time To Live:	111 hops	Checksum:	1DC7
Source Address:	69.28.135.164 : 80	Dest Address:	192.168.1.4 : 2927

Control Flags: Don't Fragment / Last Fragment (2)
Type of Service: Routine / Normal Delay / Normal Throughput / Normal Reliability (0)

☑ Include Raw Header ☑ Display as only text □ Trace

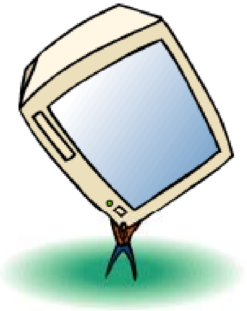
```
HEADER:
45 00 01 52 5E 72 40 00 6F 06 1D C7 45 1C 87 A4   E..R^r@.o...E...
C0 A8 01 04 00 50 0B 6F E2 4F DD 1A 24 FF B5 0A   .....P.o.O..$...
50 18 FD AC 22 68 00 00                           P..."h..

DATA:
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Cache-Control: max-age=2592000
Expires: Fri, 10 Oct 2003 17:54:03 GMT
Date: Wed, 10 Sep 2003 17:54:03 GMT
```

Colasoft MSN Monitor

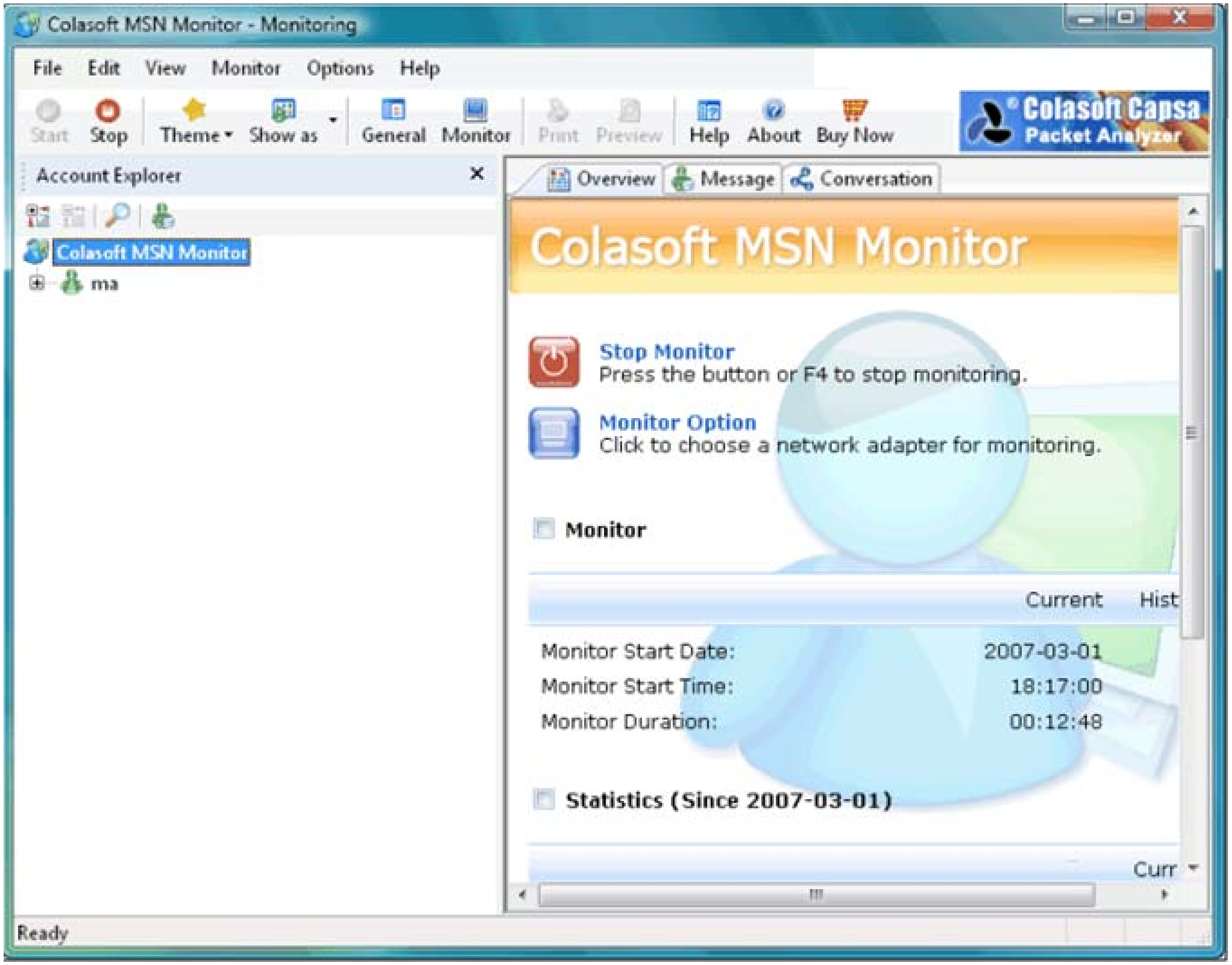
Colasoft MSN Monitor enables network administrators to capture MSN Messenger conversations along with all related details, including usernames, usage statistics, and more

Program displays information in a nicely organized overview, sorted by the user and contact address

It also displays current online status, client IP addresses, software version and account names, as well as a unique conversation matrix that enables to view all users and conversations at once



Colasoft MSN Monitor: Screenshot 1



Stop Monitor
Press the button or F4 to stop monitoring.

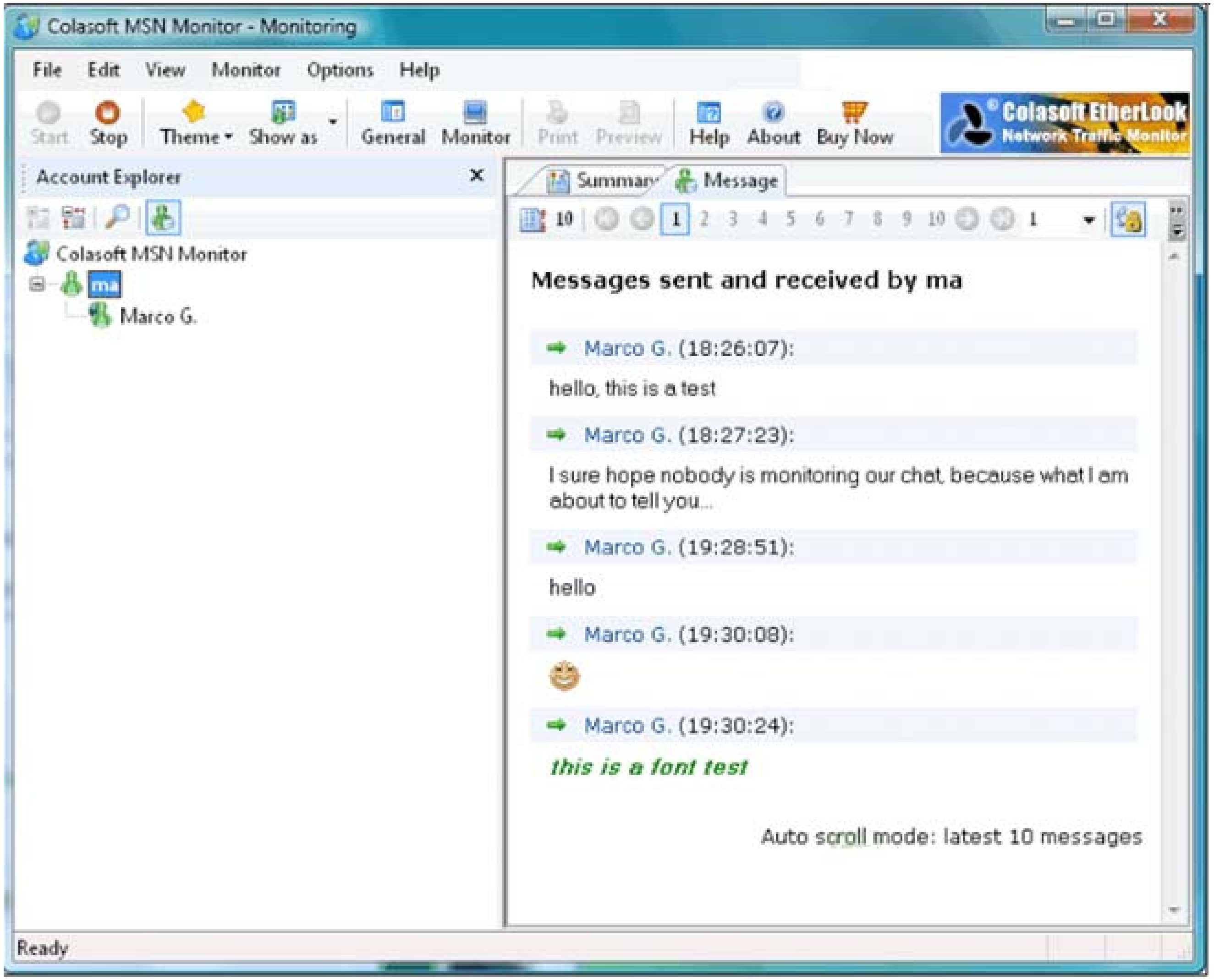
Monitor Option
Click to choose a network adapter for monitoring.

□ Monitor

	Current	Hist
Monitor Start Date:	2007-03-01	
Monitor Start Time:	18:17:00	
Monitor Duration:	00:12:48	

□ Statistics (Since 2007-03-01)

Colasoft MSN Monitor: Screenshot 2


Colasoft MSN Monitor - Monitoring
File Edit View Monitor Options Help
Start Stop Theme Show as General Monitor Print Preview Help About Buy Now
Colasoft EtherLook Network Traffic Monitor
Account Explorer
Colasoft MSN Monitor
ma
Marco G.
Summary Message
Ready

Messages sent and received by ma

Marco G. (18:26:07):

hello, this is a test

Marco G. (18:27:23):

I sure hope nobody is monitoring our chat, because what I am about to tell you...

Marco G. (19:28:51):

hello

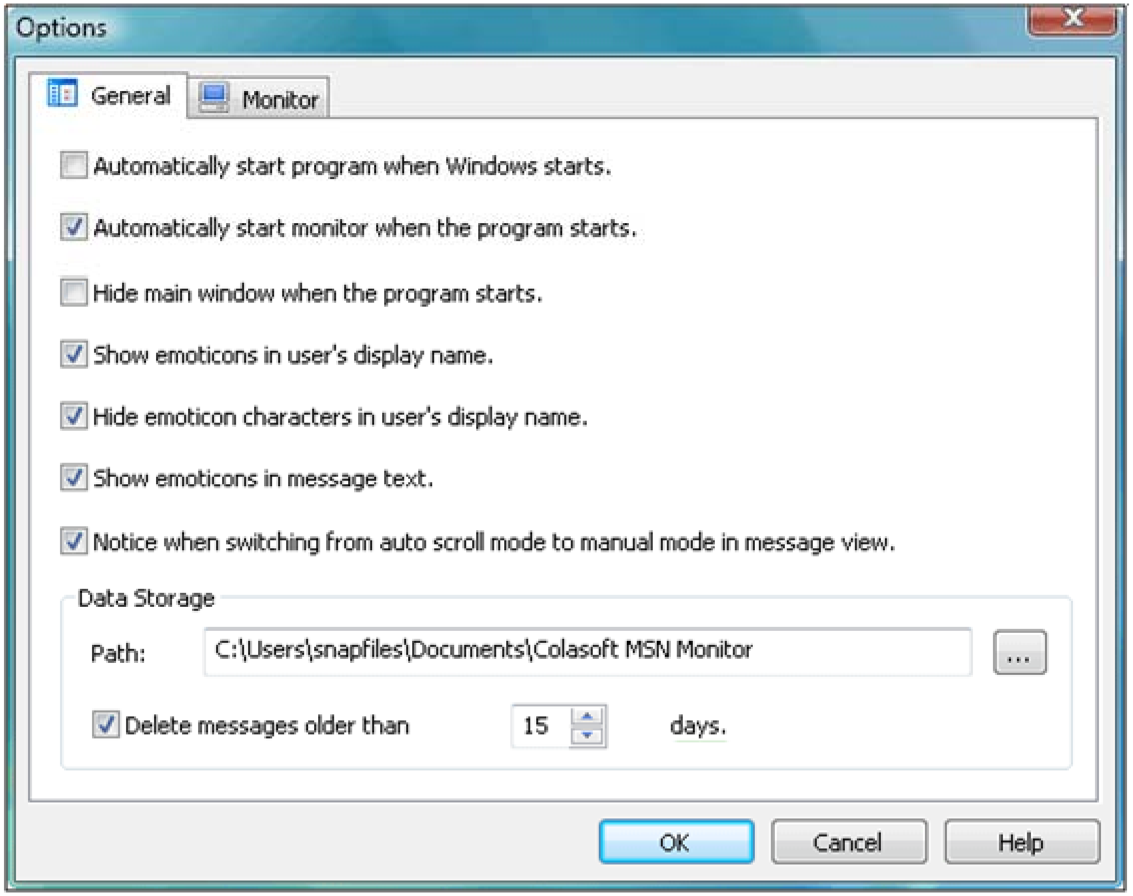
Marco G. (19:30:08):

Marco G. (19:30:24):

this is a font test

Auto scroll mode: latest 10 messages

Colasoft MSN Monitor: Screenshot 3



☐ Automatically start program when Windows starts.

☑ Automatically start monitor when the program starts.

☐ Hide main window when the program starts.

☑ Show emoticons in user's display name.

☑ Hide emoticon characters in user's display name.

☑ Show emoticons in message text.

☑ Notice when switching from auto scroll mode to manual mode in message view.

Data Storage

Path: C:\Users\snapfiles\Documents\Colasoft MSN Monitor

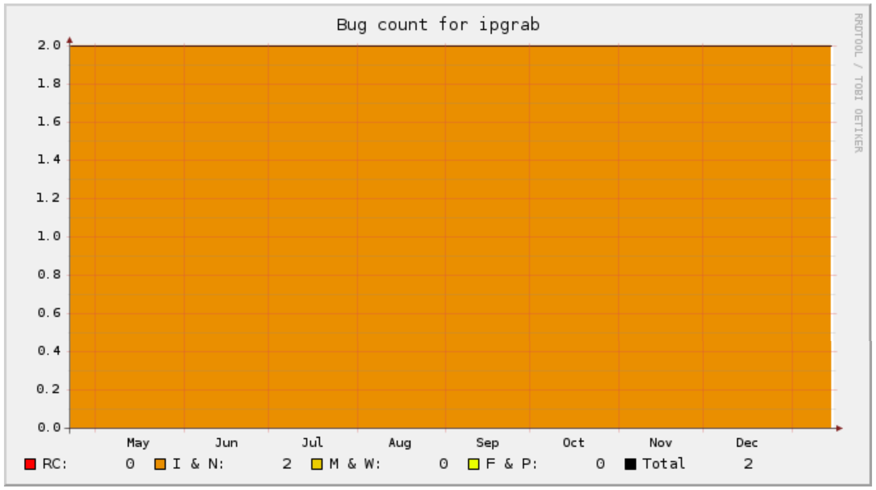
☑ Delete messages older than 15 days.

IPgrab

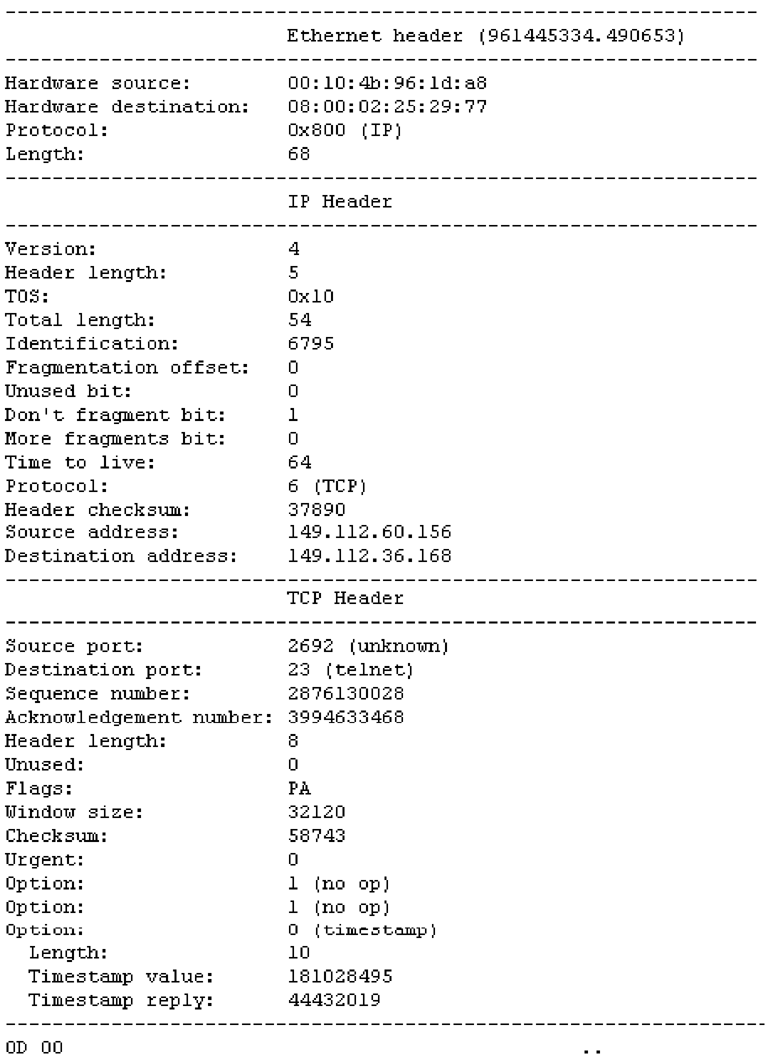
IPgrab can do whatever it likes with the resulting image of a packet

Packet sniffers have been used for many years to detect network problems, troubleshoot protocols, and detect intruders

IPgrab also supports a minimal mode in which all information about all parts of a packet are displayed in a single line of text



Ipgrab: Screenshot



```
----------------------------------------------------------------
                        Ethernet header (961445334.490653)
----------------------------------------------------------------
Hardware source:        00:10:4b:96:1d:a8
Hardware destination:   08:00:02:25:29:77
Protocol:               0x800 (IP)
Length:                 68
----------------------------------------------------------------
                        IP Header
----------------------------------------------------------------
Version:                4
Header length:          5
TOS:                    0x10
Total length:           54
Identification:         6795
Fragmentation offset:   0
Unused bit:             0
Don't fragment bit:     1
More fragments bit:     0
Time to live:           64
Protocol:               6 (TCP)
Header checksum:        37890
Source address:         149.112.60.156
Destination address:    149.112.36.168
----------------------------------------------------------------
                        TCP Header
----------------------------------------------------------------
Source port:            2692 (unknown)
Destination port:       23 (telnet)
Sequence number:        2876130028
Acknowledgement number: 3994633468
Header length:          8
Unused:                 0
Flags:                  PA
Window size:            32120
Checksum:               58743
Urgent:                 0
Option:                 1 (no op)
Option:                 1 (no op)
Option:                 0 (timestamp)
  Length:               10
  Timestamp value:      181028495
  Timestamp reply:      44432019
-----------------------------------------------------------------
0D 00                                            ..
```

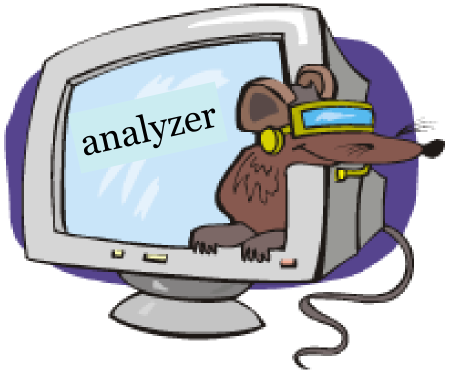
Example telnet output

EtherScan Analyzer

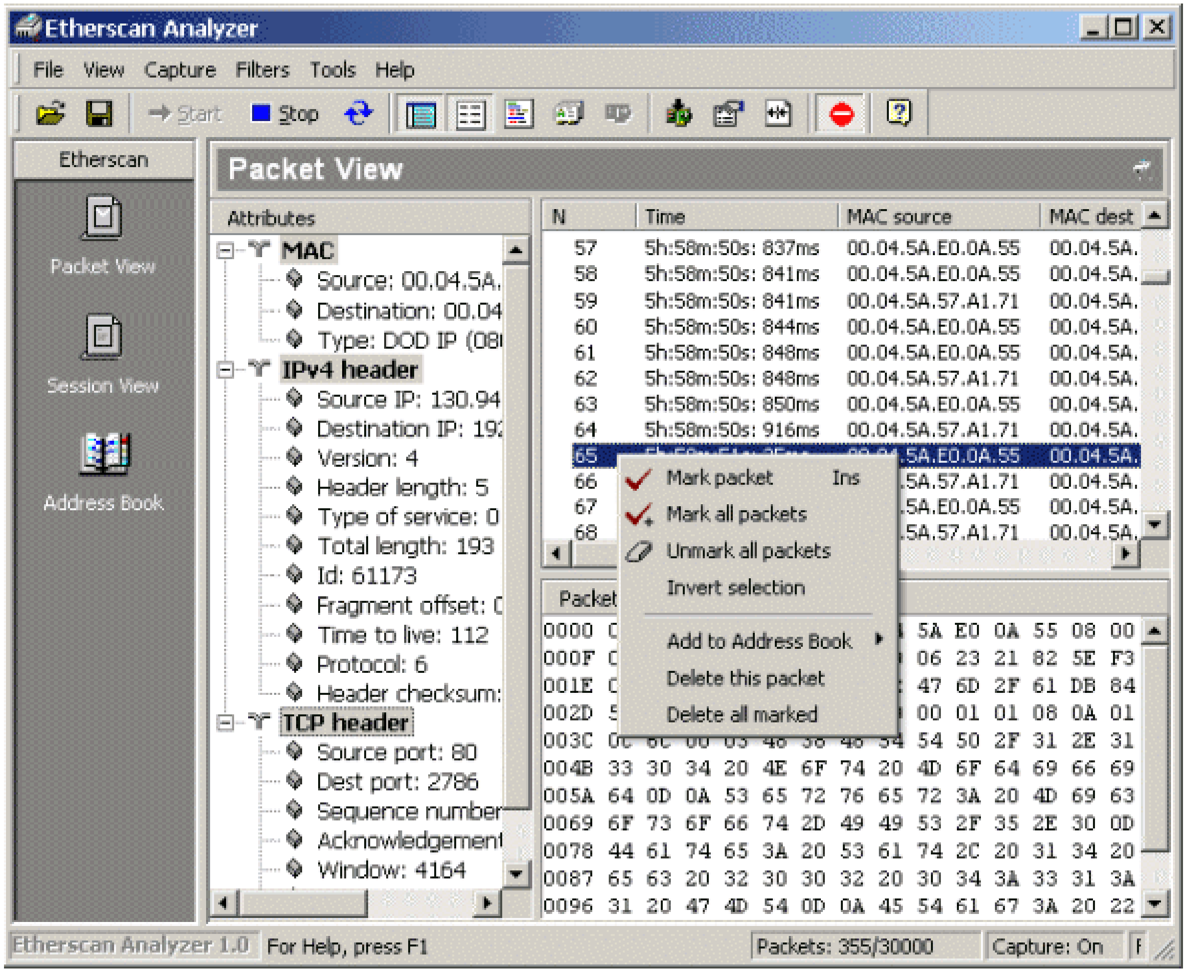
EtherScan Analyzer is a network traffic and protocol analyzer

It captures and analyses the packets over the local network

It decodes the major protocols and is capable of reconstructing TCP/IP sessions



EtherScan Analyzer: Screenshot



Attributes

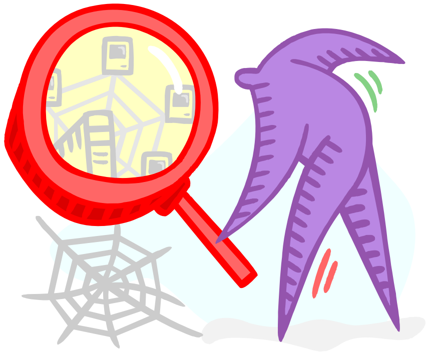
- MAC
  - Source: 00.04.5A.
  - Destination: 00.04
  - Type: DOD IP (08
- IPv4 header
  - Source IP: 130.94
  - Destination IP: 19
  - Version: 4
  - Header length: 5
  - Type of service: 0
  - Total length: 193
  - Id: 61173
  - Fragment offset: 0
  - Time to live: 112
  - Protocol: 6
  - Header checksum:
- TCP header
  - Source port: 80
  - Dest port: 2786
  - Sequence number
  - Acknowledgement
  - Window: 4164

N	Time	MAC source	MAC dest
57	5h:58m:50s: 837ms	00.04.5A.E0.0A.55	00.04.5A.
58	5h:58m:50s: 841ms	00.04.5A.E0.0A.55	00.04.5A.
59	5h:58m:50s: 841ms	00.04.5A.57.A1.71	00.04.5A.
60	5h:58m:50s: 844ms	00.04.5A.E0.0A.55	00.04.5A.
61	5h:58m:50s: 848ms	00.04.5A.E0.0A.55	00.04.5A.
62	5h:58m:50s: 848ms	00.04.5A.57.A1.71	00.04.5A.
63	5h:58m:50s: 850ms	00.04.5A.E0.0A.55	00.04.5A.
64	5h:58m:50s: 916ms	00.04.5A.57.A1.71	00.04.5A.
65	[illegible]	.5A.E0.0A.55	00.04.5A.
66		.5A.57.A1.71	00.04.5A.
67		.5A.E0.0A.55	00.04.5A.
68		.5A.57.A1.71	00.04.5A.

Packet

```
0000 0                            5A E0 0A 55 08 00
000F 0                            06 23 21 82 5E F3
001E 0                            47 6D 2F 61 DB 84
002D 5                            00 01 01 08 0A 01
003C 0C                           54 50 2F 31 2E 31
004B 33 30 34 20 4E 6F 74 20 4D 6F 64 69 66 69
005A 64 0D 0A 53 65 72 76 65 72 3A 20 4D 69 63
0069 6F 73 6F 66 74 2D 49 49 53 2F 35 2E 30 0D
0078 44 61 74 65 3A 20 53 61 74 2C 20 31 34 20
0087 65 63 20 32 30 30 32 20 30 34 3A 33 31 3A
0096 31 20 47 4D 54 0D 0A 45 54 61 67 3A 20 22
```

Etherscan Analyzer 1.0 | For Help, press F1 | Packets: 355/30000 | Capture: On



Detecting Sniffing

How to Detect Sniffing

You will need to check which machines are running in promiscuous mode

Run ARPWATCH and notice if the MAC address of certain machines has changed (Example: router's MAC address)

Run network tools like HP OpenView and IBM Tivoli network health check tools to monitor the network for strange packets

Countermeasures

Restriction of physical access to network media ensures that a packet sniffer cannot be installed

The best way to be secured against sniffing is to use encryption. It would not prevent a sniffer from functioning but will ensure that what a sniffer reads is not important

ARP Spoofing is used to sniff a switched network, so an attacker will try to ARP spoof the gateway. This can be prevented by permanently adding the MAC address of the gateway to the ARP cache

Countermeasures (cont'd)

Another way to prevent the network from being sniffed is to change the network to SSH

There are various methods to detect a sniffer in a network:

- Ping method
- ARP method
- Latency method
- Using IDS

Countermeasures (cont'd)

Small Network

- Use of static IP addresses and static ARP tables prevent hackers from adding spoofed ARP entries for machines in the network

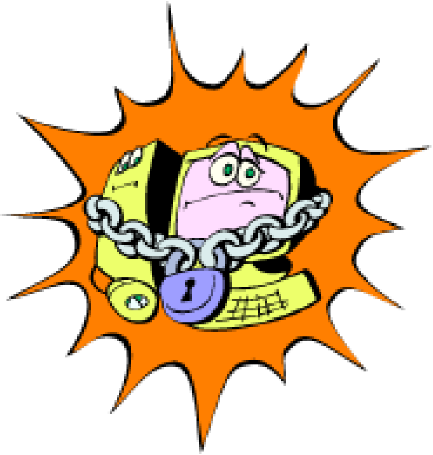
Large Networks

- Enable network switch port security features
- Use ArpWatch to monitor Ethernet activity

Countermeasures (cont'd)

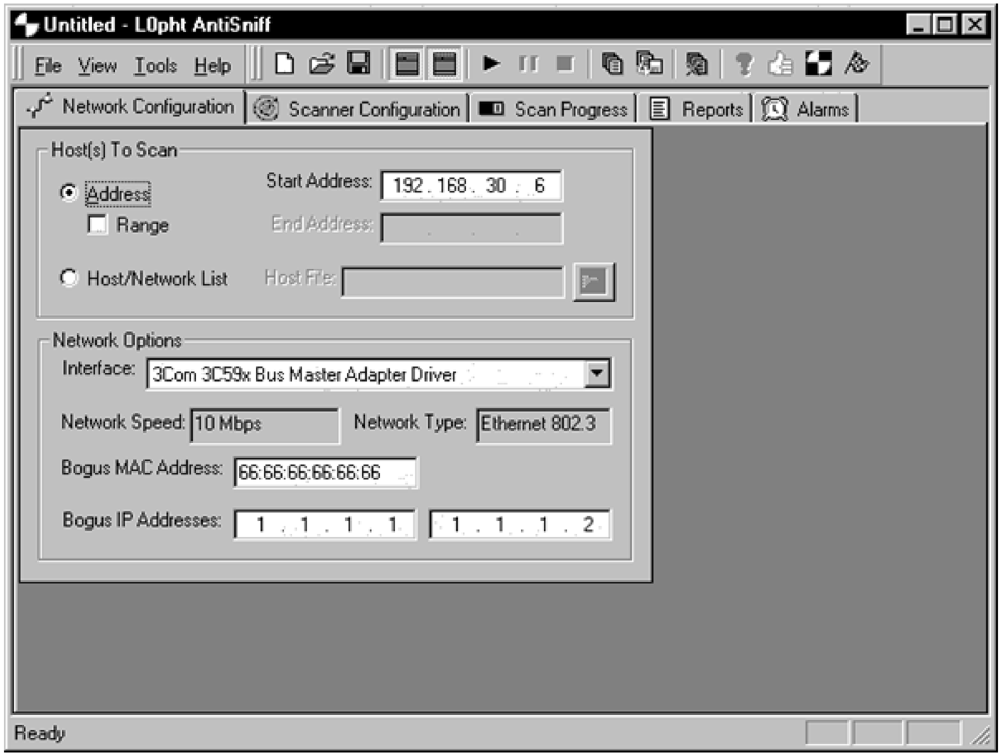
There are various tools to detect a sniffer in a network:

- ARP Watch
- Promiscan
- Antisniff
- Prodetect



AntiSniff Tool

AntiSniff tool can detect machines on the network that are running in the promiscuous mode



Untitled - L0pht AntiSniff

Host(s) To Scan

● Address

□ Range

○ Host/Network List

Start Address: 192 . 168 . 30 . 6

End Address:

Host File:

Network Options

Interface: 3Com 3C59x Bus Master Adapter Driver

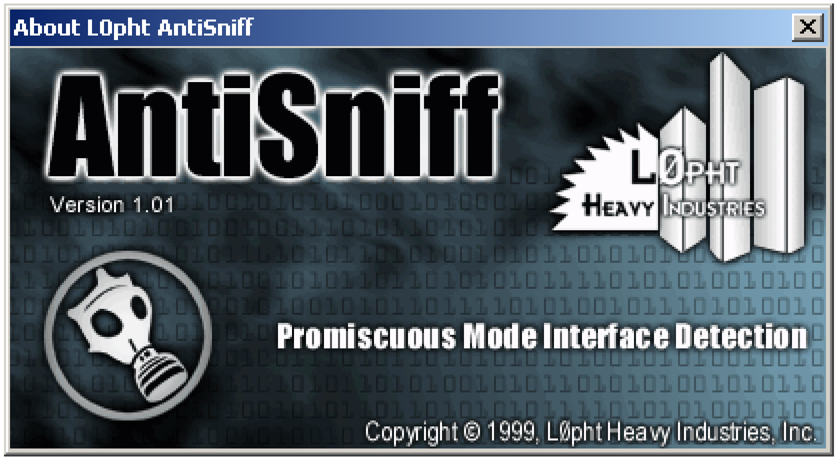
Network Speed: 10 Mbps

Network Type: Ethernet 802.3

Bogus MAC Address: 66:66:66:66:66:66

Bogus IP Addresses: 1 . 1 . 1 . 1   1 . 1 . 1 . 2

Ready



About L0pht AntiSniff

AntiSniff

Version 1.01

Promiscuous Mode Interface Detection

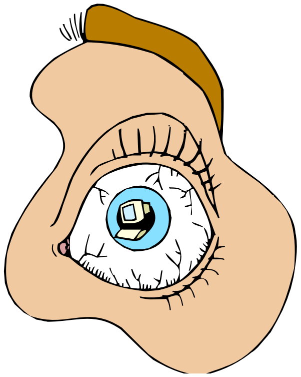
Copyright © 1999, L0pht Heavy Industries, Inc.

ArpWatch Tool

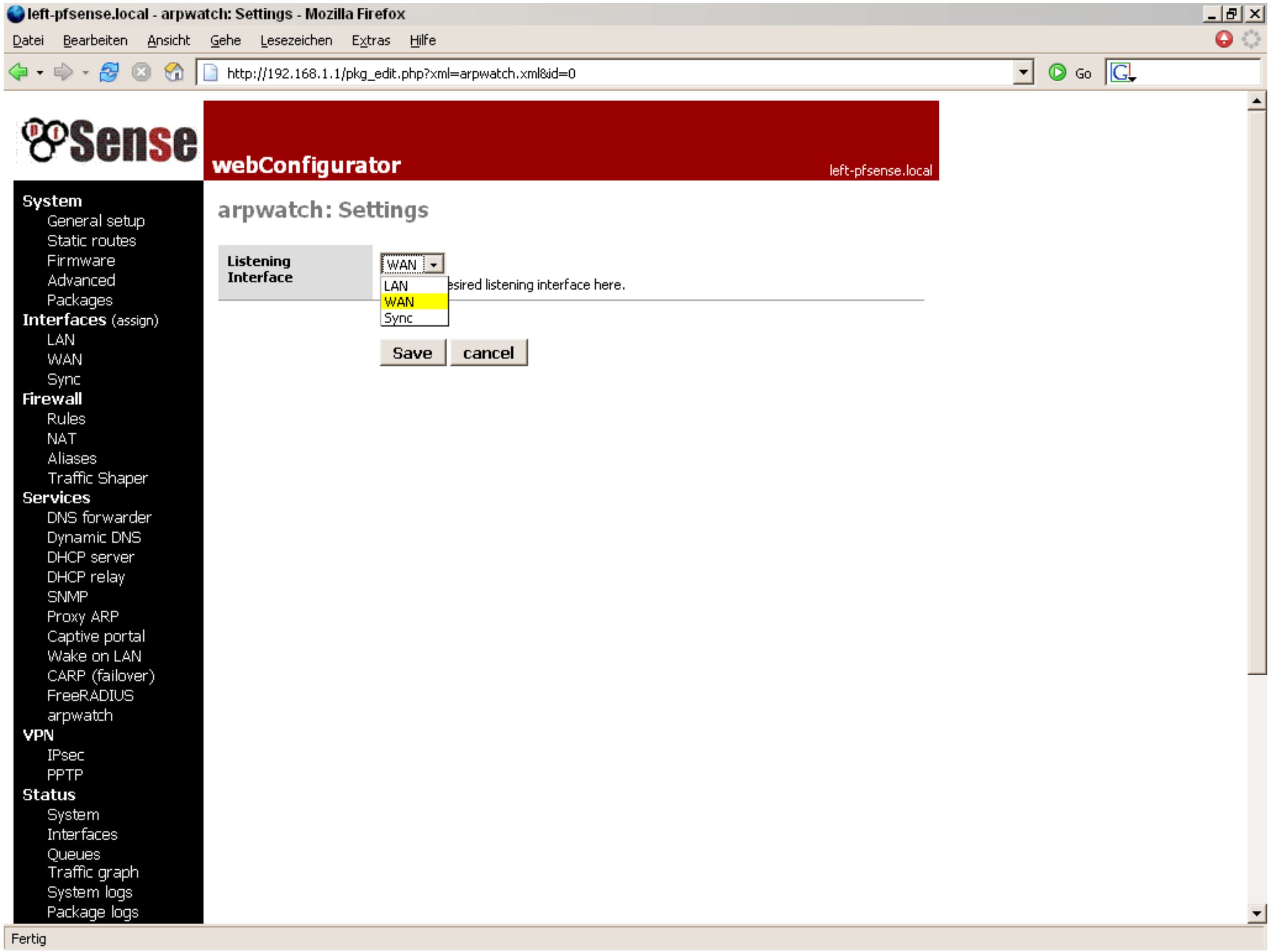
ArpWatch is a tool that monitors the Ethernet activity and keeps a database of Ethernet/IP address pairings

It also reports certain changes via email

Place triggers when your router's MAC address changes on your network



ArpWatch Tool: Screenshot



left-pfsense.local - arpwatch: Settings - Mozilla Firefox

http://192.168.1.1/pkg_edit.php?xml=arpwatch.xml&id=0

webConfigurator

left-pfsense.local

arpwatch: Settings

Listening Interface	WAN …sired listening interface here.

PromiScan

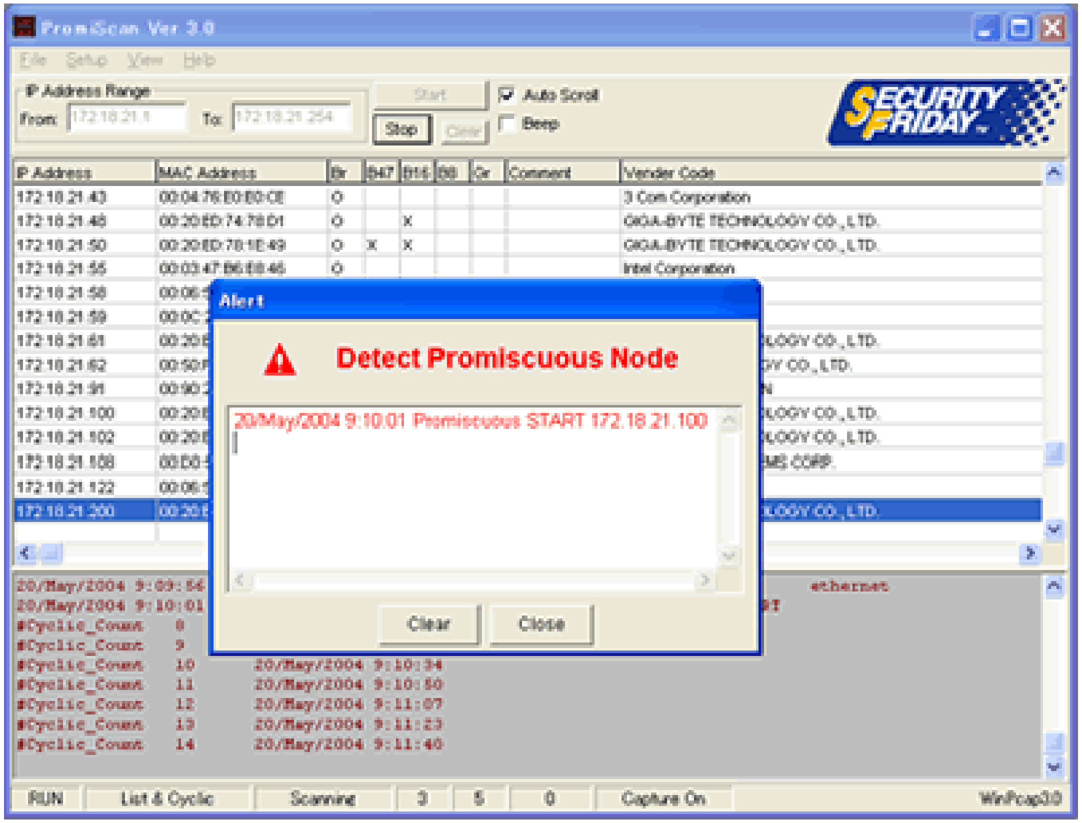
PromiScan is a renowned sniffing node detection tool

It provides continuous monitoring to detect starting and ending promiscuous applications, without increasing the network load

Features:

- Cyclic scanning
- Slow scanning supported
- Logging
- Node Viewer
- Warning Window
- Logging with SYSLOG

PromiScan: Screenshot



IP Address Range
From: 172.18.21.1 To: 172.18.21.254

☑ Auto Scroll
□ Beep

IP Address	MAC Address	Br	B47	B16	B8	Gr	Comment	Vender Code
172.18.21.43	00:04:76:E0:E0:CE	O						3 Com Corporation
172.18.21.48	00:20:ED:74:78:D1	O		X				GIGA-BYTE TECHNOLOGY CO., LTD.
172.18.21.50	00:20:ED:78:1E:49	O	X	X				GIGA-BYTE TECHNOLOGY CO., LTD.
172.18.21.55	00:03:47:B6:E8:46	O						Intel Corporation
172.18.21.58	00:06:5							
172.18.21.59	00:0C:							
172.18.21.61	00:20:E							LOGY CO., LTD.
172.18.21.62	00:50:F							GY CO., LTD.
172.18.21.91	00:90:2							N
172.18.21.100	00:20:E							LOGY CO., LTD.
172.18.21.102	00:20:E							LOGY CO., LTD.
172.18.21.108	00:D0:5							MS CORP.
172.18.21.122	00:06:5							
172.18.21.200	00:20:E							LOGY CO., LTD.

Detect Promiscuous Node

```
20/May/2004 9:10:01 Promiscuous START 172.18.21.100
```

```
20/May/2004 9:09:56                                      ethernet
20/May/2004 9:10:01                                  ST
#Cyclic_Count   8
#Cyclic_Count   9
#Cyclic_Count   10      20/May/2004 9:10:34
#Cyclic_Count   11      20/May/2004 9:10:50
#Cyclic_Count   12      20/May/2004 9:11:07
#Cyclic_Count   13      20/May/2004 9:11:23
#Cyclic_Count   14      20/May/2004 9:11:40
```

RUN	List & Cyclic	Scanning	3	5	0	Capture On	WinPcap3.0

proDETECT

proDETECT is an open source promiscious mode scanner with a GUI

It uses the ARP packet analyzing technique to detect adapters in promiscious mode

This tool can be used by security administrators to detect sniffers in a LAN

Network Packet Analyzer CAPSA

Network Packet Analyzer CAPSA is an advanced network traffic monitoring, analysis, and reporting tool

It captures and analyzes all traffic transport over both Ethernet and WLAN networks and decodes all major TCP/IP and application protocols

Its advanced application analysis modules allows you to view and log key communication applications such as emails, http traffic, instant messages, and DNS queries

Network Packet Analyzer CAPSA (cont'd)

Network Packet Analyzer CASPA is a comprehensive and affordable solution to the following problems:

- Troubleshooting network problems
- Testing network performance and debugging new applications with network communication involved
- Monitoring network traffic for performance, bandwidth usage, and security reasons
- Analyzing network traffic to trace specific transactions or find security breaches
- Monitoring user Internet access, email communications, instant messages, ftp downloads, and other transactions to enforce company policies
- Generating and viewing reports in tables and charts on network usage and statistics for network performance review

What Happened Next

Jamal returns to his office and snoops a protocol analyzer into the premise of XInsurance Inc. He goes to the same room where he had found the wires lying in the AC duct.

Jamal cuts one of the LAN wires and attaches the protocol analyzer to the partially-cut wire to sniff the traffic.

He could get the following information:

- Various protocols used
- Some raw data that was not encrypted

Summary

Sniffing allows to capture vital information from network traffic. It can be done over the hub or the switch (passive or active)

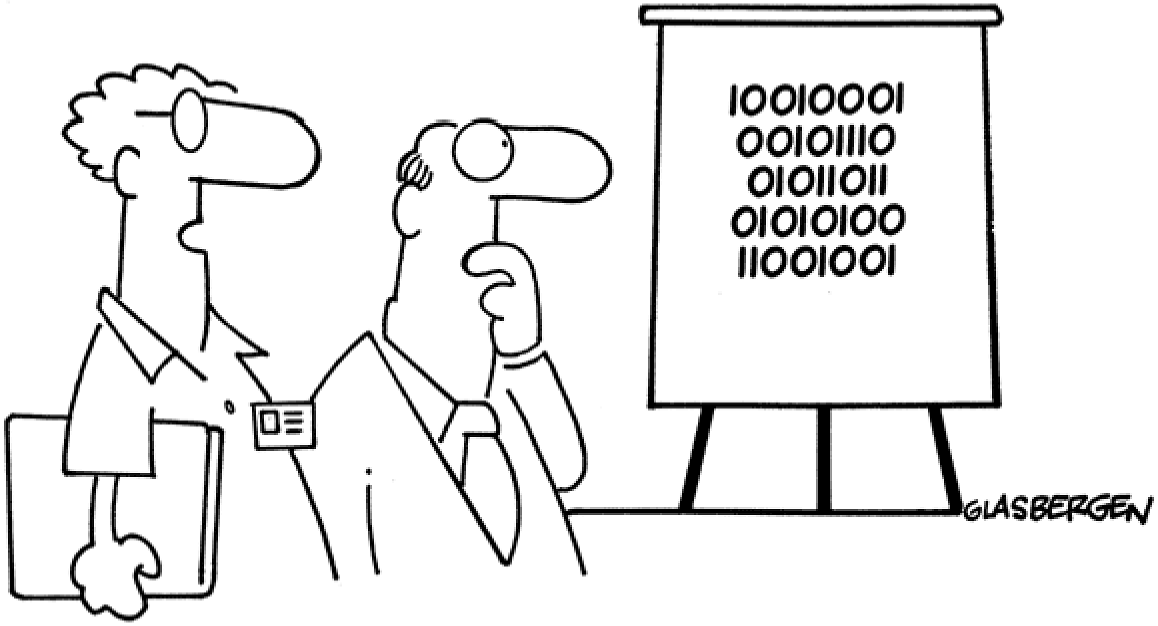
Passwords, emails, and files can be grabbed by means of sniffing

ARP poisoning can be used to change the switch mode of the network to the Hub mode and subsequently carry out packet sniffing

Wireshark, Dsniff, Sniffit, Aldebaran, Hunt, and NGSSniff are some of the most popular sniffing tools

The best way to be secured against sniffing is to use encryption, and apply the latest patches or other lockdown techniques to the system

"We don't need to worry about information security or message encryption. Most of our communications are impossible to understand in the first place."



"We've devised a new security encryption code.
Each digit is printed upside down."