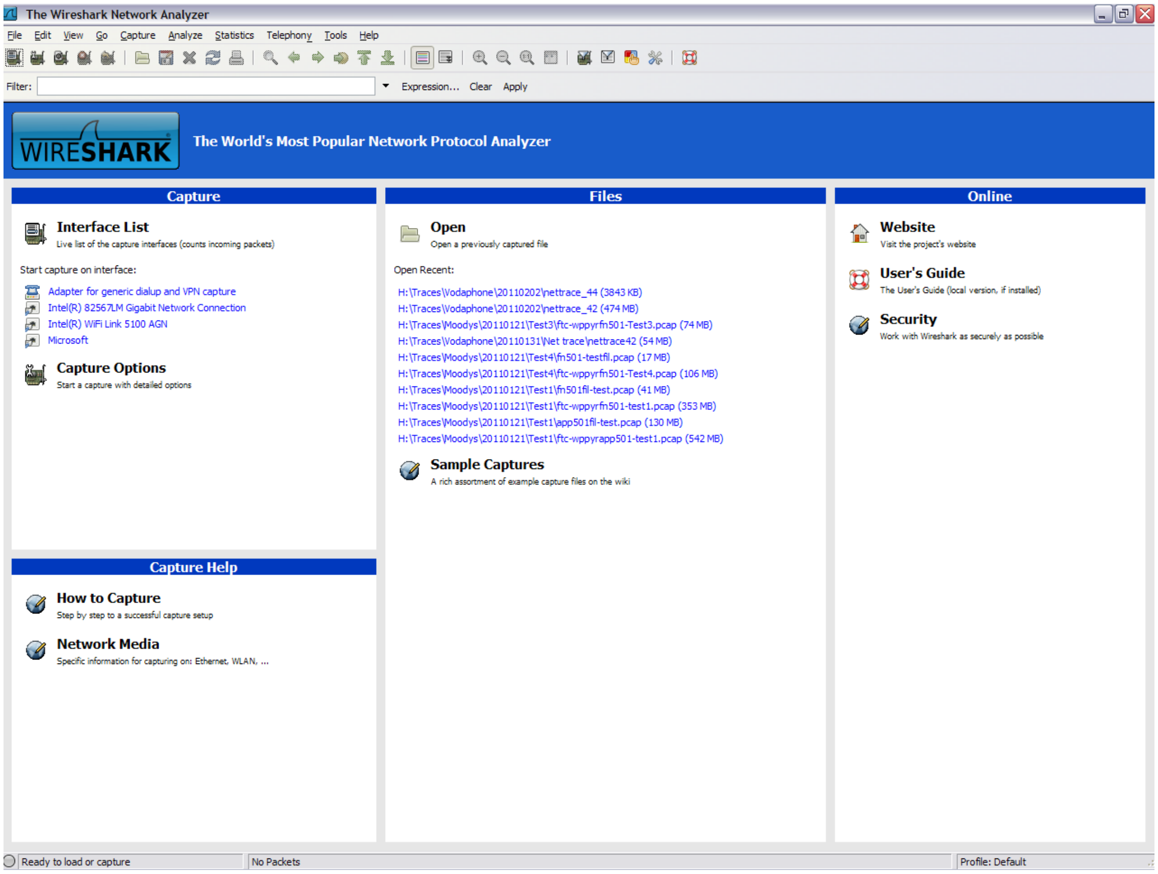
Packet Sniffers

The following are tools that are either built in to the software or freeware that can be obtained from the website indicated. They are used by the corresponding Operating Systems.

* Windows and Linux - Wireshark

AVAILABILITY:
http://www.wireshark.org/download.html
After installation of the Wireshark software,
USAGE:
[Start], Program files, Wireshark,Wireshark
(or if there is an icon present on the Desktop, double click it*)


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
WIRESHARK
Capture
Files
Online
Capture Help

The World's Most Popular Network Protocol Analyzer

Interface List
Live list of the capture interfaces (counts incoming packets)

Start capture on interface:

Adapter for generic dialup and VPN capture
Intel(R) 82567LM Gigabit Network Connection
Intel(R) WiFi Link 5100 AGN
Microsoft

Capture Options
Start a capture with detailed options

Open
Open a previously captured file

Open Recent:

H:\Traces\Vodaphone\20110202\nettrace_44 (3843 KB)
H:\Traces\Vodaphone\20110202\nettrace_42 (474 MB)
H:\Traces\Moodys\20110121\Test3\ftc-wppyrfn501-Test3.pcap (74 MB)
H:\Traces\Vodaphone\20110131\Net trace\nettrace42 (54 MB)
H:\Traces\Moodys\20110121\Test4\fn501-testfil.pcap (17 MB)
H:\Traces\Moodys\20110121\Test4\ftc-wppyrfn501-Test4.pcap (106 MB)
H:\Traces\Moodys\20110121\Test1\fn501fil-test.pcap (41 MB)
H:\Traces\Moodys\20110121\Test1\ftc-wppyrfn501-test1.pcap (353 MB)
H:\Traces\Moodys\20110121\Test1\app501fil-test.pcap (130 MB)
H:\Traces\Moodys\20110121\Test1\ftc-wppyrapp501-test1.pcap (542 MB)

Sample Captures
A rich assortment of example capture files on the wiki

Website
Visit the project's website

User's Guide
The User's Guide (local version, if installed)

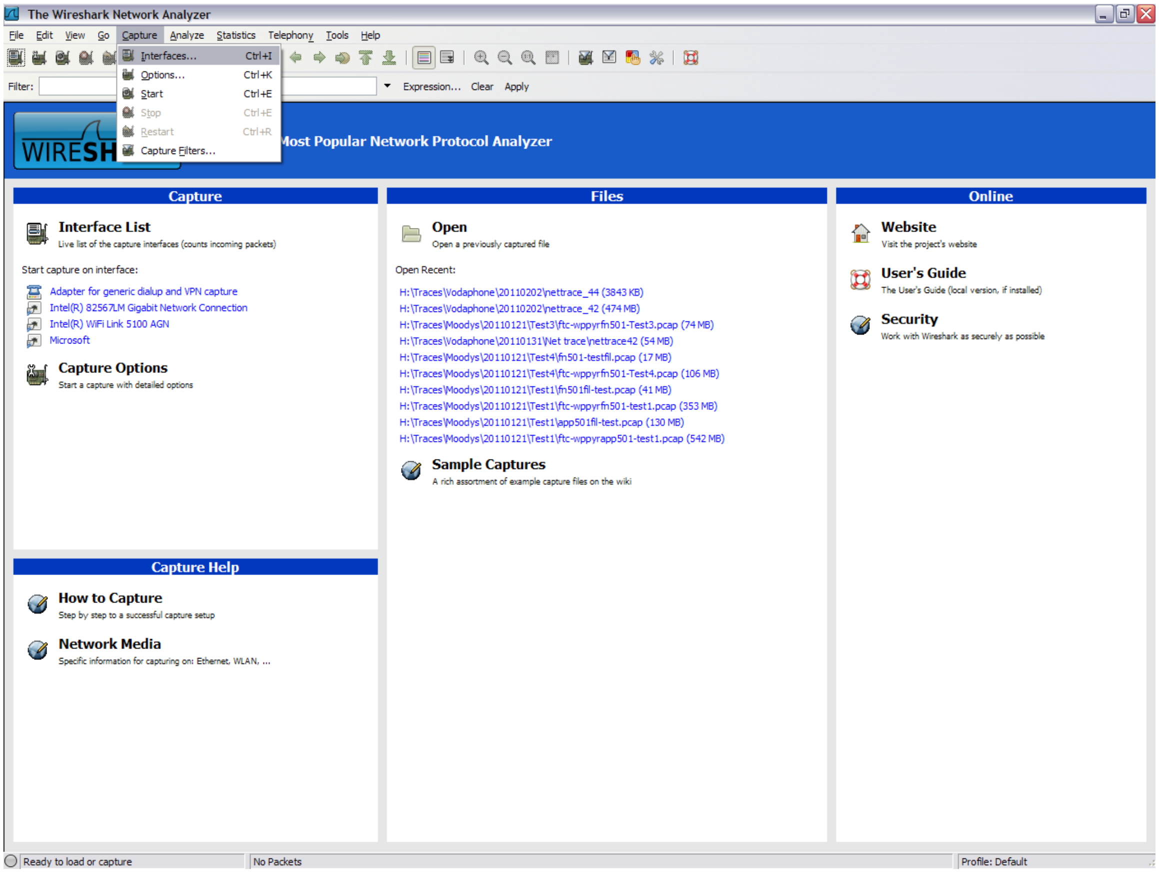
Security
Work with Wireshark as securely as possible

How to Capture
Step by step to a successful capture setup

Network Media
Specific information for capturing on: Ethernet, WLAN, ...

Ready to load or capture | No Packets | Profile: Default

- From the Tool bar, select Capture and then select “Interface”.



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Interfaces... Ctrl+I
Options... Ctrl+K
Start Ctrl+E
Stop Ctrl+E
Restart Ctrl+R
Capture Filters...
Filter:
Expression... Clear Apply
WIRESH
Most Popular Network Protocol Analyzer

Capture

Interface List
Live list of the capture interfaces (counts incoming packets)

Start capture on interface:

- Adapter for generic dialup and VPN capture
- Intel(R) 82567LM Gigabit Network Connection
- Intel(R) WiFi Link 5100 AGN
- Microsoft

Capture Options
Start a capture with detailed options

Files

Open
Open a previously captured file

Open Recent:

- H:\Traces\Vodaphone\20110202\nettrace_44 (3843 KB)
- H:\Traces\Vodaphone\20110202\nettrace_42 (474 MB)
- H:\Traces\Moodys\20110121\Test3\ftc-wppyrfn501-Test3.pcap (74 MB)
- H:\Traces\Vodaphone\20110131\Net trace\nettrace42 (54 MB)
- H:\Traces\Moodys\20110121\Test4\fn501-testfil.pcap (17 MB)
- H:\Traces\Moodys\20110121\Test4\ftc-wppyrfn501-Test4.pcap (106 MB)
- H:\Traces\Moodys\20110121\Test1\fn501fil-test.pcap (41 MB)
- H:\Traces\Moodys\20110121\Test1\ftc-wppyrfn501-test1.pcap (353 MB)
- H:\Traces\Moodys\20110121\Test1\app501fil-test.pcap (130 MB)
- H:\Traces\Moodys\20110121\Test1\ftc-wppyrapp501-test1.pcap (542 MB)

Sample Captures
A rich assortment of example capture files on the wiki

Online

Website
Visit the project's website

User's Guide
The User's Guide (local version, if installed)

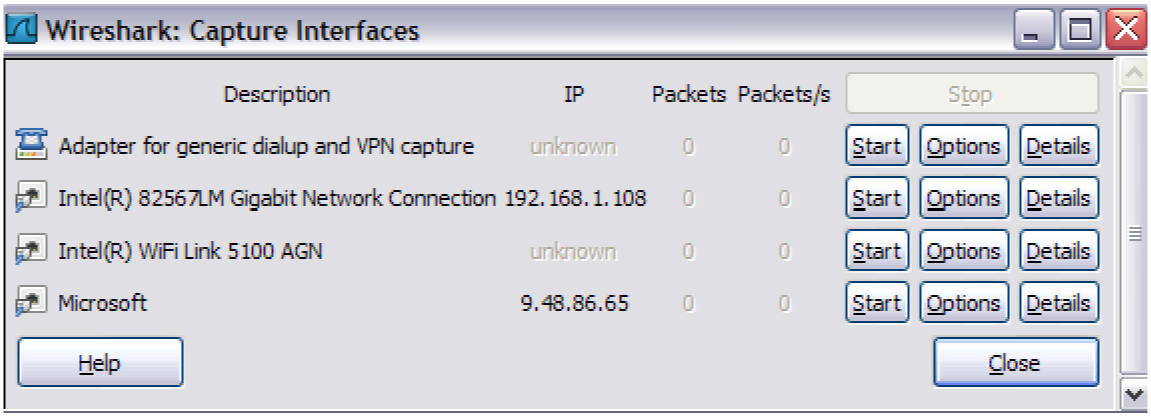
Security
Work with Wireshark as securely as possible

Capture Help

How to Capture
Step by step to a successful capture setup

Network Media
Specific information for capturing on: Ethernet, WLAN, ...

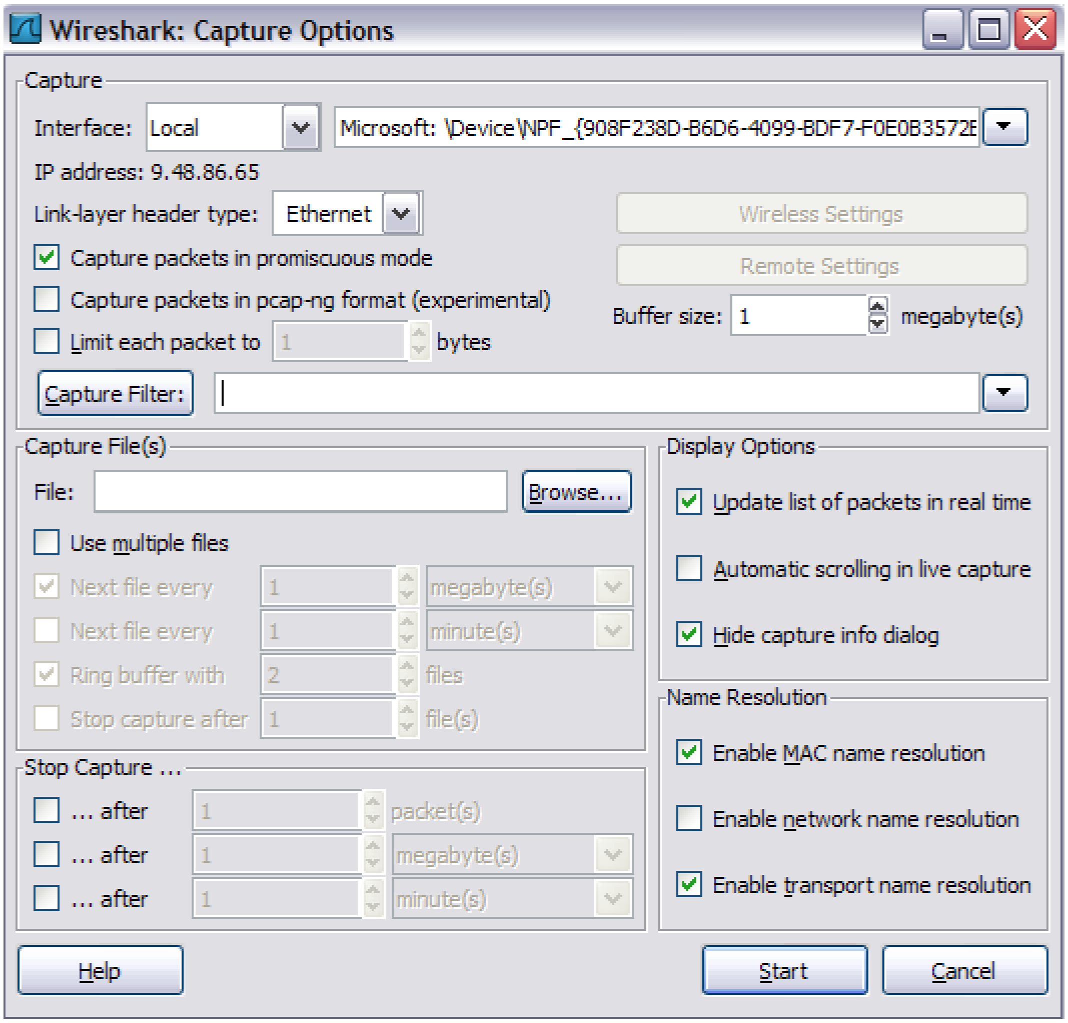
The next screen that will pop up will be the Capture Interface screen. From this screen you can start capturing data, view the "options" page or view the "detailed" information of that interface card.



Wireshark: Capture Interfaces

Description	IP	Packets	Packets/s	Stop		
Adapter for generic dialup and VPN capture	unknown	0	0	Start	Options	Details
Intel(R) 82567LM Gigabit Network Connection	192.168.1.108	0	0	Start	Options	Details
Intel(R) WiFi Link 5100 AGN	unknown	0	0	Start	Options	Details
Microsoft	9.48.86.65	0	0	Start	Options	Details

By identifying the correct Description and IP address of the interface you want to capture off of, select "options" for that interface. From the Capture Options screen you will be able to adjust the buffer size, capture packets in promiscuous mode, select capture filters (if needed*), and start the tracing tool.



Wireshark: Capture Options

Capture

Interface: Local ▾ Microsoft: \Device\NPF_{908F238D-B6D6-4099-BDF7-F0E0B3572E ▾

IP address: 9.48.86.65

Link-layer header type: Ethernet ▾

☑ Capture packets in promiscuous mode

□ Capture packets in pcap-ng format (experimental)

□ Limit each packet to 1 bytes

Buffer size: 1 megabyte(s)

Capture Filter:

Capture File(s)

File:

□ Use multiple files

☑ Next file every 1 megabyte(s)

□ Next file every 1 minute(s)

☑ Ring buffer with 2 files

□ Stop capture after 1 file(s)

Stop Capture ...

□ ... after 1 packet(s)

□ ... after 1 megabyte(s)

□ ... after 1 minute(s)

Display Options

☑ Update list of packets in real time

□ Automatic scrolling in live capture

☑ Hide capture info dialog

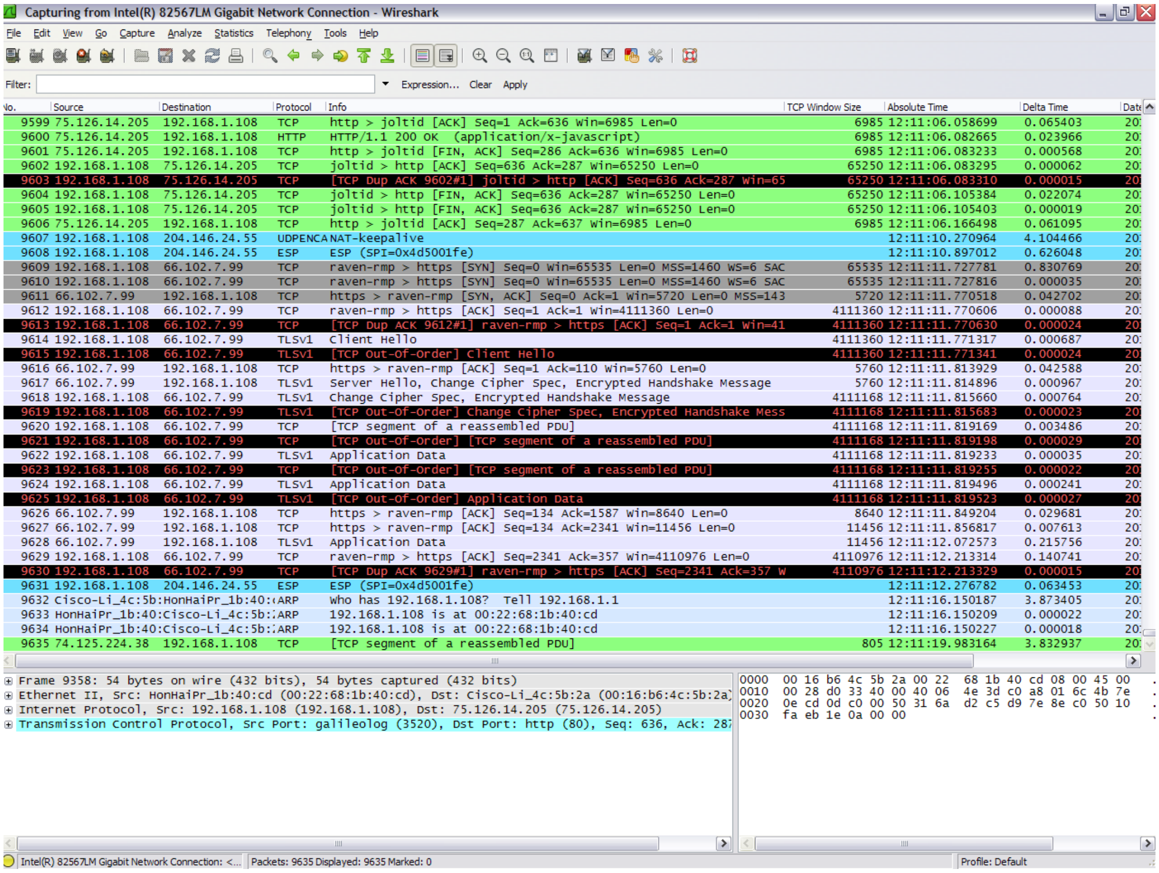
Name Resolution

☑ Enable MAC name resolution

□ Enable network name resolution

☑ Enable transport name resolution

Once the tool has started capturing data you will see data displayed in the three panels. To stop the trace, select the icon on the toolbar with the red and white circle over the interface card. You can also select Capture> Stop on the toolbar as well to stop the tracing.


Capturing from Intel(R) 82567LM Gigabit Network Connection - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

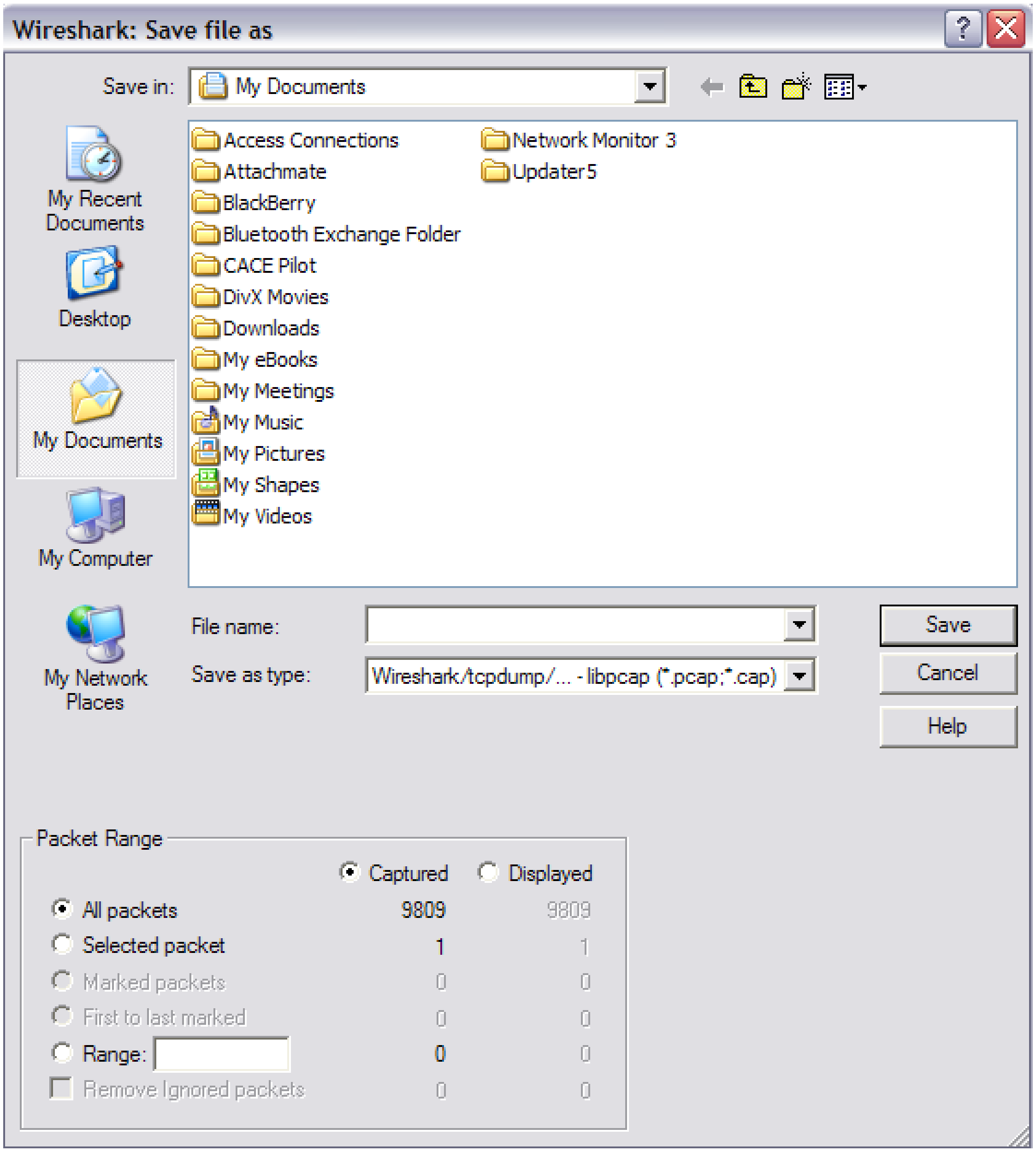
```
No.  Source         Destination     Protocol Info                                                               TCP Window Size Absolute Time      Delta Time Date
9599 75.126.14.205  192.168.1.108   TCP      http > joltid [ACK] Seq=1 Ack=636 Win=6985 Len=0                   6985 12:11:06.058699    0.065403  20:
9600 75.126.14.205  192.168.1.108   HTTP     HTTP/1.1 200 OK  (application/x-javascript)                        6985 12:11:06.082665    0.023966  20:
9601 75.126.14.205  192.168.1.108   TCP      http > joltid [FIN, ACK] Seq=286 Ack=636 Win=6985 Len=0            6985 12:11:06.083233    0.000568  20:
9602 192.168.1.108  75.126.14.205   TCP      joltid > http [ACK] Seq=636 Ack=287 Win=65250 Len=0               65250 12:11:06.083295    0.000062  20:
9603 192.168.1.108  75.126.14.205   TCP      [TCP Dup ACK 9602#1] joltid > http [ACK] Seq=636 Ack=287 Win=65   65250 12:11:06.083310    0.000015  20:
9604 192.168.1.108  75.126.14.205   TCP      joltid > http [FIN, ACK] Seq=636 Ack=287 Win=65250 Len=0          65250 12:11:06.105384    0.022074  20:
9605 192.168.1.108  75.126.14.205   TCP      joltid > http [FIN, ACK] Seq=636 Ack=287 Win=65250 Len=0          65250 12:11:06.105403    0.000019  20:
9606 75.126.14.205  192.168.1.108   TCP      http > joltid [ACK] Seq=287 Ack=637 Win=6985 Len=0                 6985 12:11:06.166498    0.061095  20:
9607 192.168.1.108  204.146.24.55   UDPENCA NAT-keepalive                                                            12:11:10.270964    4.104466  20:
9608 192.168.1.108  204.146.24.55   ESP      ESP (SPI=0x4d5001fe)                                                    12:11:10.897012    0.626048  20:
9609 192.168.1.108  66.102.7.99     TCP      raven-rmp > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=6 SAC   65535 12:11:11.727781    0.830769  20:
9610 192.168.1.108  66.102.7.99     TCP      raven-rmp > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=6 SAC   65535 12:11:11.727816    0.000035  20:
9611 66.102.7.99    192.168.1.108   TCP      https > raven-rmp [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=143    5720 12:11:11.770518    0.042702  20:
9612 192.168.1.108  66.102.7.99     TCP      raven-rmp > https [ACK] Seq=1 Ack=1 Win=4111360 Len=0           4111360 12:11:11.770606    0.000088  20:
9613 192.168.1.108  66.102.7.99     TCP      [TCP Dup ACK 9612#1] raven-rmp > https [ACK] Seq=1 Ack=1 Win=41 4111360 12:11:11.770630    0.000024  20:
9614 192.168.1.108  66.102.7.99     TLSv1    Client Hello                                                    4111360 12:11:11.771317    0.000687  20:
9615 192.168.1.108  66.102.7.99     TLSv1    [TCP Out-Of-Order] Client Hello                                 4111360 12:11:11.771341    0.000024  20:
9616 66.102.7.99    192.168.1.108   TCP      https > raven-rmp [ACK] Seq=1 Ack=110 Win=5760 Len=0               5760 12:11:11.813929    0.042588  20:
9617 66.102.7.99    192.168.1.108   TLSv1    Server Hello, Change Cipher Spec, Encrypted Handshake Message      5760 12:11:11.814896    0.000967  20:
9618 192.168.1.108  66.102.7.99     TLSv1    Change Cipher Spec, Encrypted Handshake Message                 4111168 12:11:11.815660    0.000764  20:
9619 192.168.1.108  66.102.7.99     TLSv1    [TCP Out-Of-Order] Change Cipher Spec, Encrypted Handshake Mess 4111168 12:11:11.815683    0.000023  20:
9620 192.168.1.108  66.102.7.99     TCP      [TCP segment of a reassembled PDU]                              4111168 12:11:11.819169    0.003486  20:
9621 192.168.1.108  66.102.7.99     TCP      [TCP Out-Of-Order] [TCP segment of a reassembled PDU]           4111168 12:11:11.819198    0.000029  20:
9622 192.168.1.108  66.102.7.99     TLSv1    Application Data                                                4111168 12:11:11.819233    0.000035  20:
9623 192.168.1.108  66.102.7.99     TCP      [TCP Out-Of-Order] [TCP segment of a reassembled PDU]           4111168 12:11:11.819255    0.000022  20:
9624 192.168.1.108  66.102.7.99     TLSv1    Application Data                                                4111168 12:11:11.819496    0.000241  20:
9625 192.168.1.108  66.102.7.99     TLSv1    [TCP Out-Of-Order] Application Data                             4111168 12:11:11.819523    0.000027  20:
9626 66.102.7.99    192.168.1.108   TCP      https > raven-rmp [ACK] Seq=134 Ack=1587 Win=8640 Len=0            8640 12:11:11.849204    0.029681  20:
9627 66.102.7.99    192.168.1.108   TCP      https > raven-rmp [ACK] Seq=134 Ack=2341 Win=11456 Len=0          11456 12:11:11.856817    0.007613  20:
9628 66.102.7.99    192.168.1.108   TLSv1    Application Data                                                  11456 12:11:12.072573    0.215756  20:
9629 192.168.1.108  66.102.7.99     TCP      raven-rmp > https [ACK] Seq=2341 Ack=357 Win=4110976 Len=0      4110976 12:11:12.213314    0.140741  20:
9630 192.168.1.108  66.102.7.99     TCP      [TCP Dup ACK 9629#1] raven-rmp > https [ACK] Seq=2341 Ack=357 W 4110976 12:11:12.213329    0.000015  20:
9631 192.168.1.108  204.146.24.55   ESP      ESP (SPI=0x4d5001fe)                                                    12:11:12.276782    0.063453  20:
9632 Cisco-Li_4c:5b:HonHaiPr_1b:40:(ARP      Who has 192.168.1.108?  Tell 192.168.1.1                                12:11:16.150187    3.873405  20:
9633 HonHaiPr_1b:40:Cisco-Li_4c:5b:ARP       192.168.1.108 is at 00:22:68:1b:40:cd                                   12:11:16.150209    0.000022  20:
9634 HonHaiPr_1b:40:Cisco-Li_4c:5b:ARP       192.168.1.108 is at 00:22:68:1b:40:cd                                   12:11:16.150227    0.000018  20:
9635 74.125.224.38  192.168.1.108   TCP      [TCP segment of a reassembled PDU]                                  805 12:11:19.983164    3.832937  20:
```

```
⊞ Frame 9358: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
⊞ Ethernet II, Src: HonHaiPr_1b:40:cd (00:22:68:1b:40:cd), Dst: Cisco-Li_4c:5b:2a (00:16:b6:4c:5b:2a)
⊞ Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 75.126.14.205 (75.126.14.205)
⊞ Transmission Control Protocol, Src Port: galileolog (3520), Dst Port: http (80), Seq: 636, Ack: 287
```

```
0000  00 16 b6 4c 5b 2a 00 22  68 1b 40 cd 08 00 45 00
0010  00 28 d0 33 40 00 40 06  4e 3d c0 a8 01 6c 4b 7e
0020  0e cd 0d c0 00 50 31 6a  d2 c5 d9 7e 8e c0 50 10
0030  fa eb 1e 0a 00 00
```

Intel(R) 82567LM Gigabit Network Connection: <...
Packets: 9635 Displayed: 9635 Marked: 0
Profile: Default

Once the tool has stopped, from the toolbar elect File> Save As. This will allow you to save the captured data in a number of different formats. You can take the default format which is tcpdump or *.cap.



Save in: My Documents

File name:

Save as type: Wireshark/tcpdump/... - libpcap (*.pcap;*.cap)

Packet Range

	● Captured	○ Displayed
● All packets	9809	9809
○ Selected packet	1	1
○ Marked packets	0	0
○ First to last marked	0	0
○ Range:	0	0
□ Remove Ignored packets	0	0

Once the file has been saved, you can compress it and have it delivered to the IBM FileNet Network Analyst.

* Solaris: snoop

AVAILABILITY: Built in to Solaris

You must be root to run this tool.

- netstat -in => IDENTIFY AVAILABLE INTERFACES, LOCAL IP ADDR
- snoop -d hme0 -o snoop.cap
- flat snoop.cap

snoop - capture and inspect network packets

SYNOPSIS

snoop [-aCDNPSvV] [-t [r | a | d]] [-c maxcount] [-d device] [-i filename] [-n filename] [-o filename] [-p first [, last]] [-s snaplen] [-x offset [, length]] [expression]

DESCRIPTION

snoop captures packets from the network and displays their contents. snoop uses both the network packet filter and streams buffer modules to provide efficient capture of packets from the network. Captured packets can be displayed as they are received, or saved to a file for later inspection.

snoop can display packets in a single-line summary form or in verbose multi-line forms. In summary form, only the data pertaining to the highest level protocol is displayed. For example, an NFS packet will have only NFS information displayed. The underlying RPC, UDP, IP, and ethernet frame information is suppressed but can be displayed if either of the verbose options are chosen.

snoop requires an interactive interface.

OPTIONS

-P Capture packets in non-promiscuous mode. Only broadcast, multicast, or packets addressed to the host machine will be seen.

-v Verbose mode. Print packet headers in lots of detail. This display consumes many lines per packet and should be used only on selected packets.

-V Verbose summary mode. This is halfway between summary mode and verbose mode in degree of verbosity. Instead of displaying just the summary line for the highest level protocol in a packet, it displays a summary line for each protocol layer in the packet. For instance, for an NFS packet it will display a line each for the ETHER, IP, UDP, RPC and NFS layers. Verbose summary mode output may be easily piped through grep to extract packets of interest. For example to view only RPC summary lines:

```
example# snoop -i rpc.cap -V | grep RPC
```

-d device Receive packets from the network using the interface specified by device. Usually le0 or ie0. The program netstat(1M), when invoked with the -i flag, lists all the interfaces that a machine has. Normally, snoop will automatically choose the first non-loopback interface it finds.

-o filename

Save captured packets in filename as they are captured. During packet capture, a count of the number of packets saved in the file is displayed. If you wish just to count packets without saving to a file, name the file /dev/null.

More options for the snoop tool ******>>>>>

```
    [ -a ]                 # Listen to packets on audio
    [ -d device ]          # Network interface to snoop (le?, ie?, bf?, tr?)
    [ -s snaplen ]         # Truncate packets
    [ -c count ]           # Quit after count packets
    [ -P ]                 # Turn OFF promiscuous mode
    [ -D ]                 # Report dropped packets
    [ -S ]                 # Report packet size
    [ -i file ]            # Read previously captured packets
    [ -o file ]            # Capture packets in file
    [ -n file ]            # Load addr-to-name table from file
    [ -N ]                 # Create addr-to-name table
    [ -t  r|a|d ]          # Time: Relative, Absolute or Delta
    [ -v ]                 # Verbose packet display
    [ -V ]                 # Show all summary lines
    [ -p first[,last] ]    # Select packet(s) to display
    [ -x offset[,length] ] # Hex dump from offset for length
    [ -C ]                 # Print packet filter code
    [ -q ]                 # Suppress printing packet count
    [ -r ]                 # Do not resolve address to name
```

****

*AIX: iptrace

AVAILABILITY: Built in to AIX
USAGE:

- **su to “root” first and formost******
- netstat -in => IDENTIFY AVAILABLE INTERFACES, LOCAL IP ADDR
- cd /fnsw/local/tmp
- iptrace -a -b -d 10.70.11.233 [-p cor] logtest.out
- ps -eaf|grep iptrace => PID 27581; kill -9 27581 => STOP IPTRACE
- ls –l logtest.out
- flat logtest.out

Reference :

http://publib.boulder.ibm.com/infocenter/aix/v6r1/index.jsp?topic=/com.ibm.aix.cmds/doc/aixcmds3/iptrace.htm

*HPUX: nettl

USAGE: ROOT user only.

```
nettl -start
Initializing Network Tracing and Logging...
nettl   :       Failed to start console logging due to invalid configuration
                file.  Console logging will be disabled.  To correct the
                problem, enter the command netfmt -pc /var/adm/conslog.opts
                and check the output.
```

```
 SYNOPSIS
     /usr/sbin/nettl -start

     /usr/sbin/nettl -stop

     /usr/sbin/nettl -firmlog 0|1|2 -card dev_name ...

     /usr/sbin/nettl -log class ... -entity subsystem ...

     /usr/sbin/nettl -status [log |trace |all]

     /usr/sbin/nettl -traceon kind ... -entity subsystem ...
```

```
          [-card dev_name ...] [-file tracename] [-m bytes] [-size portsize]
          [-tracemax maxsize]

      /usr/sbin/nettl -traceoff -entity subsystem ...
```

-start (Abbr.: -st)
Used alone without other options.

Initialize the tracing and logging facility, start up default logging, and optionally start up console logging. Logging is enabled for all subsystems as determined by the /etc/nettlgen.conf file.

-stop (Abbr.: -sp)
Used alone without other options.

Terminate the trace/log facility. Once this command is issued, the trace/log facility is no longer able to accept the corresponding trace/log calls from the network subsystems.

Log messages are sent to a log file whose name is determined by adding the suffix .LOG00 to the log file name specified in the /etc/nettlgen.conf configuration file. Console logging is started if console logging has been configured in the /etc/nettlgen.conf file.

nettl(1M) Reference nettlconf(1M) and nettlgen.conf(4) for an explanation of the configuration file. If the log file (with suffix) already exists, it is opened in append mode; that is, new data is added to the file. The default name is /var/adm/nettl (logging starts to file /var/adm/nettl.LOG00).

This tool should be used by experienced Engineers. There are many options to use with this tool, so be aware.