

10/11/25

Experiments on packet capture tool: Wireshark

Aim: Experiments on Packet Capture tool: Wireshark Exp No: 5

Packet Sniffer:

• Sniffs messages being sent / received from / by your computer.

• Store and display the contents of the various protocols / fields in the message.

• Passive program

- never sends packet itself
- no packets addressed to it
- receive a copy of all packets sent / received

Packet Sniffer Structure Diagnostic Tools:-

• Topdump

- Eg: topdump -enx host 10.129.41.2 -w ex2.out

• Wireshark

- wireshark -r ex3.out

Wireshark:-

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and displays them in human readable format.

What we can do with Wireshark:

- Capture network traffic
- Decode packet protocols using dissectors
- Watch packet statistics
- Analyse problems

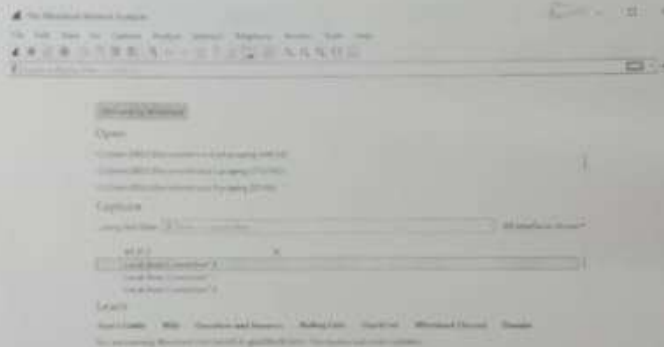
Wireshark used for:

- Network administrators: Troubleshoot network problem
- Developers: Debug protocol implementation
- People: Learn network protocol internals

Getting wireshark
or macs. Wireshark can be downloaded for windows from its official website.

Capturing packets:-

after downloading and installing wireshark launch it and double click the name of a network interface under capture to start capturing packets on that interface.



The "Packet Bytes" pane

The packet Bytes pane shows the data of the current packet (Selected in the 'Packet list' pane) in a hexdump style.

Sample Captures:-

If there's nothing interesting on your own network to inspect, Wireshark's Wiki has you covered.

Filtering packets:-

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using network so you can narrow down the traffic.

Still you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

The image shows the Wireshark interface with the packet list pane selected. It displays a list of captured packets with columns for No., Time, Source, Destination, and Protocol. The packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.1	192.168.1.100	HTTP	1024	GET / HTTP/1.1
2	0.000000	192.168.1.100	192.168.1.1	TCP	60	65535 → 80 [RST] Seq=1234567890 Win=0 Len=0
3	0.000000	192.168.1.1	192.168.1.100	TCP	60	80 → 65535 [RST] Seq=1234567890 Win=0 Len=0
4	0.000000	192.168.1.100	192.168.1.1	TCP	60	65535 → 80 [RST] Seq=1234567890 Win=0 Len=0
5	0.000000	192.168.1.1	192.168.1.100	TCP	60	80 → 65535 [RST] Seq=1234567890 Win=0 Len=0
6	0.000000	192.168.1.100	192.168.1.1	TCP	60	65535 → 80 [RST] Seq=1234567890 Win=0 Len=0
7	0.000000	192.168.1.1	192.168.1.100	TCP	60	80 → 65535 [RST] Seq=1234567890 Win=0 Len=0
8	0.000000	192.168.1.100	192.168.1.1	TCP	60	65535 → 80 [RST] Seq=1234567890 Win=0 Len=0
9	0.000000	192.168.1.1	192.168.1.100	TCP	60	80 → 65535 [RST] Seq=1234567890 Win=0 Len=0
10	0.000000	192.168.1.100	192.168.1.1	TCP	60	65535 → 80 [RST] Seq=1234567890 Win=0 Len=0

You can also click Analyze > Display Filters to choose a filter from among the default filters included in Wireshark. Close the window and you'll find a filter has been applied automatically. Wireshark is showing you the packet that make up the conversation.

The image shows the Wireshark interface with the packet list pane selected. A filter has been applied, and the packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.1	192.168.1.100	HTTP	1024	GET / HTTP/1.1
2	0.000000	192.168.1.100	192.168.1.1	TCP	60	65535 → 80 [RST] Seq=1234567890 Win=0 Len=0
3	0.000000	192.168.1.1	192.168.1.100	TCP	60	80 → 65535 [RST] Seq=1234567890 Win=0 Len=0
4	0.000000	192.168.1.100	192.168.1.1	TCP	60	65535 → 80 [RST] Seq=1234567890 Win=0 Len=0
5	0.000000	192.168.1.1	192.168.1.100	TCP	60	80 → 65535 [RST] Seq=1234567890 Win=0 Len=0
6	0.000000	192.168.1.100	192.168.1.1	TCP	60	65535 → 80 [RST] Seq=1234567890 Win=0 Len=0
7	0.000000	192.168.1.1	192.168.1.100	TCP	60	80 → 65535 [RST] Seq=1234567890 Win=0 Len=0
8	0.000000	192.168.1.100	192.168.1.1	TCP	60	65535 → 80 [RST] Seq=1234567890 Win=0 Len=0
9	0.000000	192.168.1.1	192.168.1.100	TCP	60	80 → 65535 [RST] Seq=1234567890 Win=0 Len=0
10	0.000000	192.168.1.100	192.168.1.1	TCP	60	65535 → 80 [RST] Seq=1234567890 Win=0 Len=0

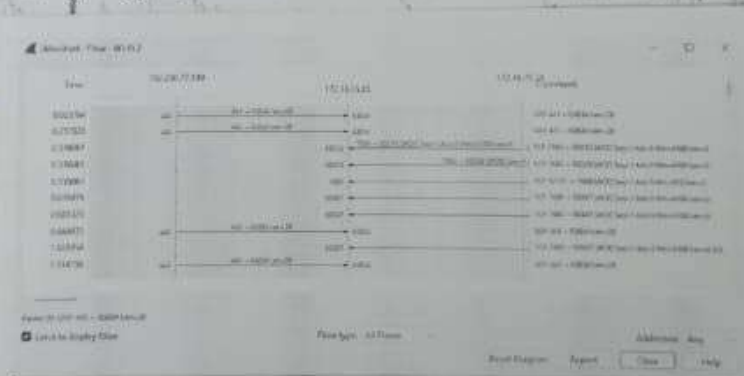
Inspecting packets - click a packet to select it and you can dig down to view its details.

The 100 Most Common Network Protocols

No.	Name	Category	Port Number	Protocol	Protocol	Protocol
1	TCP	Transport	65535	TCP	TCP	TCP
2	UDP	Transport	65535	UDP	UDP	UDP
3	HTTP	Application	80	HTTP	HTTP	HTTP
4	FTP	Application	21	FTP	FTP	FTP
5	SMTP	Application	25	SMTP	SMTP	SMTP
6	POP3	Application	110	POP3	POP3	POP3
7	IMAP4	Application	143	IMAP4	IMAP4	IMAP4
8	SSH	Application	22	SSH	SSH	SSH
9	TELNET	Application	23	TELNET	TELNET	TELNET
10	SNMP	Application	161	SNMP	SNMP	SNMP
11	NTP	Application	123	NTP	NTP	NTP
12	LDAP	Application	389	LDAP	LDAP	LDAP
13	XMPP	Application	5222	XMPP	XMPP	XMPP
14	RTSP	Application	554	RTSP	RTSP	RTSP
15	RTMP	Application	1935	RTMP	RTMP	RTMP
16	RTMPS	Application	1935	RTMPS	RTMPS	RTMPS
17	RTMPFLV	Application	1935	RTMPFLV	RTMPFLV	RTMPFLV
18	RTMPE	Application	1935	RTMPE	RTMPE	RTMPE
19	RTMPSH	Application	1935	RTMPSH	RTMPSH	RTMPSH
20	RTMPSA	Application	1935	RTMPSA	RTMPSA	RTMPSA
21	RTMPSB	Application	1935	RTMPSB	RTMPSB	RTMPSB
22	RTMPSD	Application	1935	RTMPSD	RTMPSD	RTMPSD
23	RTMPSF	Application	1935	RTMPSF	RTMPSF	RTMPSF
24	RTMPSG	Application	1935	RTMPSG	RTMPSG	RTMPSG
25	RTMPSH	Application	1935	RTMPSH	RTMPSH	RTMPSH
26	RTMPSA	Application	1935	RTMPSA	RTMPSA	RTMPSA
27	RTMPSB	Application	1935	RTMPSB	RTMPSB	RTMPSB
28	RTMPSD	Application	1935	RTMPSD	RTMPSD	RTMPSD
29	RTMPSF	Application	1935	RTMPSF	RTMPSF	RTMPSF
30	RTMPSG	Application	1935	RTMPSG	RTMPSG	RTMPSG

You can also create filters from here - just right-click one of the details and use the Apply as filters sub-menu to create a filter based on it.

Flow Graph gives a better understanding of what is going on.



1. Create a filter to display only TCP/UDP packets, inspect the packets and provide the flow graph.
2. Create a filter to display only ARP packets and inspect the packets.
3. Create a filter to display only DNS packets & provide the flow graph:
 - Go to capture → option
 - Select stop capture automatically after 100 packets
 - Then click start capture.
 - Search DNS packets in search bar.
 - To see flow graph click statistics → flow graph.
 - save the packets.

4. Create a filter to display only HTTP packets and inspect the packets.

Procedure:

- * Select Local Area Connection in WinPcap
- * Go to Capture → option
- * Select Stop capture automatically after 1
- * Then click Start capture
- * Search HTTP packets and save packets.

Wireshark 2.8.2

File Edit View Go Capture Analyze Statistics Display Windows Help

Filter: *
 Show packet bytes > 1000
 Show packet details > 1000
 Show packet raw data > 1000

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
2	0.000000	192.168.1.1	192.168.1.100	HTTP	1024	200 OK
3	0.000000	192.168.1.100	192.168.1.1	HTTP	1024	GET / HTTP/1.1
4	0.000000	192.168.1.1	192.168.1.100	HTTP	1024	200 OK

Packet 1: 1024 bytes on wire (8192 bits), 784 bytes captured (6272 bits) on interface 0
 Ethernet II, Src: Realtek-802.27.00, Dst: 08:00:27:00:00:00
 Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.1
 Transmission Control Protocol, Src Port: 54321, Dst Port: 80
 Hypertext Transfer Protocol
 GET / HTTP/1.1

Packet 2: 1024 bytes on wire (8192 bits), 784 bytes captured (6272 bits) on interface 0
 Ethernet II, Src: Realtek-802.27.00, Dst: 08:00:27:00:00:00
 Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.100
 Transmission Control Protocol, Src Port: 80, Dst Port: 54321
 Hypertext Transfer Protocol
 200 OK

5. Create a Filter to display only IP/ICMP packets & inspect the packets:-
- Select Local Area connection in Wireshark.
 - Go to Capture → option.
 - Select Stop capture automatically after 100 packets.
 - Then click Start capture.
 - Search ICMP/IP packets in Search bar.
 - Save the packets.

Wireshark 2.8.2

File Edit View Go Capture Analyze Statistics Display Windows Help

Filter: *
 Show packet bytes > 1000
 Show packet details > 1000
 Show packet raw data > 1000

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) request
2	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Echo (ping) reply
3	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) request
4	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Echo (ping) reply

Packet 1: 60 bytes on wire (480 bits), 48 bytes captured (384 bits) on interface 0
 Ethernet II, Src: Realtek-802.27.00, Dst: 08:00:27:00:00:00
 Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.1
 ICMP, Src Port: 54321, Dst Port: 80
 Echo (ping) request

Packet 2: 60 bytes on wire (480 bits), 48 bytes captured (384 bits) on interface 0
 Ethernet II, Src: Realtek-802.27.00, Dst: 08:00:27:00:00:00
 Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.100
 ICMP, Src Port: 80, Dst Port: 54321
 Echo (ping) reply

6. Create a filter to display only DHCP packets and inspect the packets.

Student Observation :-

(1) What is promiscuous mode?

Promiscuous mode is setting for a network interface card (NIC) where it captures all network packet that pass through it, not just the ones addressed to it. It is used in packet sniffing and network monitoring.

(2) Do ARP packets have transport layer header? Explain.
No, ARP (Address Resolution Protocol) packets do not have a transport layer header. ARP works at Data link layer to map an IP address to a MAC address.

(3) Which Transport layer protocol is used by DNS?

DNS can use: UDP on port 53 for most queries (faster). TCP on port 53 for tasks like zone transfers or responses exceeding 512 bytes.

(4) What is the port number used by HTTP protocol?
HTTP uses port 80 (TCP). for secure HTTP (HTTPS), the port is 443 (TCP).

(5) What is broadcast IP address?
A broadcast IP address is an address used to send data to all hosts in a network simultaneously.
In IPv4, it's highest address in a subnet.
Ex: For network 192.168.1.0/24, the broadcast address is 192.168.1.255.

Result :-

Experiments on packet capture tool, Wireshark was successfully completed.
14/8/20