

# Wireshark

## Outlines:

- **What is Wireshark?**
- **A brief history of Wireshark**
- **Some intended purposes**
- **Features**
- **What Wireshark is not**

# What is Wireshark?

- Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.
- You could think of a network packet analyzer as a measuring device used to examine what's going on inside a network cable, just like a voltmeter is used by an electrician to examine what's going on inside an electric cable.

# A brief history of Wireshark

- In late 1997, Gerald Combs needed a tool for tracking down networking problems and wanted to learn more about networking, so he started writing Ethereal (the former name of the Wireshark project) as a way to solve both problems.
- Ethereal was initially released, after several pauses in development, in July 1998 as version 0.2.0. Within days, patches, bug reports, and words of encouragement started arriving, so Ethereal was on its way to success.
- Not long after that, Gilbert Ramirez saw its potential and contributed a low-level dissector to it.
- In October, 1998, Guy Harris of Network Appliance was looking for something better than tcpview, so he started applying patches and contributing dissectors to Ethereal.
- In late 1998, Richard Sharpe, who was giving TCP/IP courses, saw its potential on such courses, and started looking at it to see if it supported the protocols he needed. While it didn't at that point, new protocols could be easily added. So he started contributing dissectors and contributing patches.
- The list of people who have contributed to the project has become very long since then, and almost all of them started with a protocol that they needed that Wireshark or Ethereal did not already handle. So they copied an existing dissector and contributed the code back to the team.
- In 2006 the project moved house and re-emerged under a new name: Wireshark.
- In 2008, after ten years of development, Wireshark finally arrived at version 1.0. This release was the first deemed complete, with the minimum features implemented. Its release coincided with the first Wireshark Developer and User Conference, called SharkFest.

# Some intended purposes

- network administrators use it to **troubleshoot network problems**
- network security engineers use it to **examine security problems**
- developers use it to **debug protocol implementations**
- people use it to **learn network protocol internals**

# Features

- Available for **UNIX** and **Windows**.
- **Capture** live packet data from a network interface.
- Display packets with **very detailed protocol information**.
- **Open and Save** packet data captured.
- **Import and Export** packet data from and to a lot of other capture programs.
- **Filter packets** on many criteria.
- **Search** for packets on many criteria.
- **Colorize** packet display based on filters.
- Create various **statistics**.
- ... and **a lot more!**

# Wireshark captures packets

The screenshot shows the Wireshark interface with a packet capture of various protocols. The main pane displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Info. Packet 12 is selected, and the details pane shows the Transmission Control Protocol (TCP) fields, including Source port: 3196, Destination port: http (80), Sequence number: 0, and Flags: 0x0002 (SYN).

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.2	Broadcast	ARP	Who has 192.168.0.2? Gratuitous /
2	0.299139	192.168.0.1	192.168.0.2	NBNS	Name query NBSTAT *<00><00><00><00>
3	0.299214	192.168.0.2	192.168.0.1	ICMP	Destination unreachable (Port unreach)
4	1.025659	192.168.0.2	224.0.0.22	IGMP	V3 Membership Report
5	1.044366	192.168.0.2	192.168.0.1	DNS	Standard query SRV _ldap._tcp.nbgr
6	1.048652	192.168.0.2	239.255.255.250	UDP	Source port: 3193 Destination port: 1900
7	1.050784	192.168.0.2	192.168.0.1	DNS	Standard query SOA nb10061d.www004.
8	1.055053	192.168.0.1	192.168.0.2	UDP	Source port: 1900 Destination port: 3193
9	1.082038	192.168.0.2	192.168.0.255	NBNS	Registration NB NB10061D<00>
10	1.111945	192.168.0.2	192.168.0.1	DNS	Standard query A proxyconf.www004.
11	1.226156	192.168.0.2	192.168.0.1	TCP	3196 > http [SYN] Seq=0 Len=0 MSS=
12	1.227282	192.168.0.1	192.168.0.2	TCP	http > 3196 [SYN, ACK] Seq=0 Ack=

Frame 11 (62 bytes on wire, 62 bytes captured)  
Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear\_2d:75:9a (00:09:5b:2d:75:9a)  
Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)  
Transmission Control Protocol, Src Port: 3196 (3196), Dst Port: http (80), Seq: 0, Len: 0  
Source port: 3196 (3196)  
Destination port: http (80)  
Sequence number: 0 (relative sequence number)  
Header length: 28 bytes  
Flags: 0x0002 (SYN)  
Window size: 64240

```
0000  00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00  ..[-u... ] .....E.  
0010  00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8  .0.H@... a,.....  
0020  00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02  ...|.P<6 .....p.  
0030  fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02      ..'..... .....
```

File: "D:/test.pcap" 14 KB 00:00:02 | P: 120 D: 120 M: 0

# What Wireshark is not

- Wireshark isn't an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn't allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.
- Wireshark will not manipulate things on the network, it will only "measure" things from it. Wireshark doesn't send packets on the network or do other active things (except for name resolutions, but even that can be disabled).

# Questions



Install the Wireshark  
and monitor the packets