EXPERIMENT-08

Aim: Study of packet sniffer tools like wireshark, ethereal, tcpdump etc

Roll No.	70
Name	MAYURI SHRIDATTA YERANDE
Class	D15-B
Subject	Internet Security Lab
LO Mapped	LO1: To apply the knowledge of symmetric cryptography to implement classical ciphers.

Aim: Study of packet sniffer tools like wireshark, ethereal, tcpdump etc

Objectives: To observe the performance in promiscuous & non-promiscuous mode & to find the packets based on different filters.

Outcomes: The leamer will be able to:

Identify different packets moving in/out of the network using packet sniffer for network analysis. Understand professional, ethical, legal, security and social issues and responsibilities. Also will be able to analyze the local and global impact of computing on individuals, organizations, and society. Match the industry requirements in the domains of Database management, Programming and Networking with the required management skills.

Hardware / Software Required: Wireshark, Ethereal and tcpdump.

Theory: Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and displays them in human-readable format. Wireshark includes filters, color-coding and other features that let you dig deep into network traffic and inspect individual packets.

Applications:

- 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 beside these examples can be
- helpful in many other situations too.

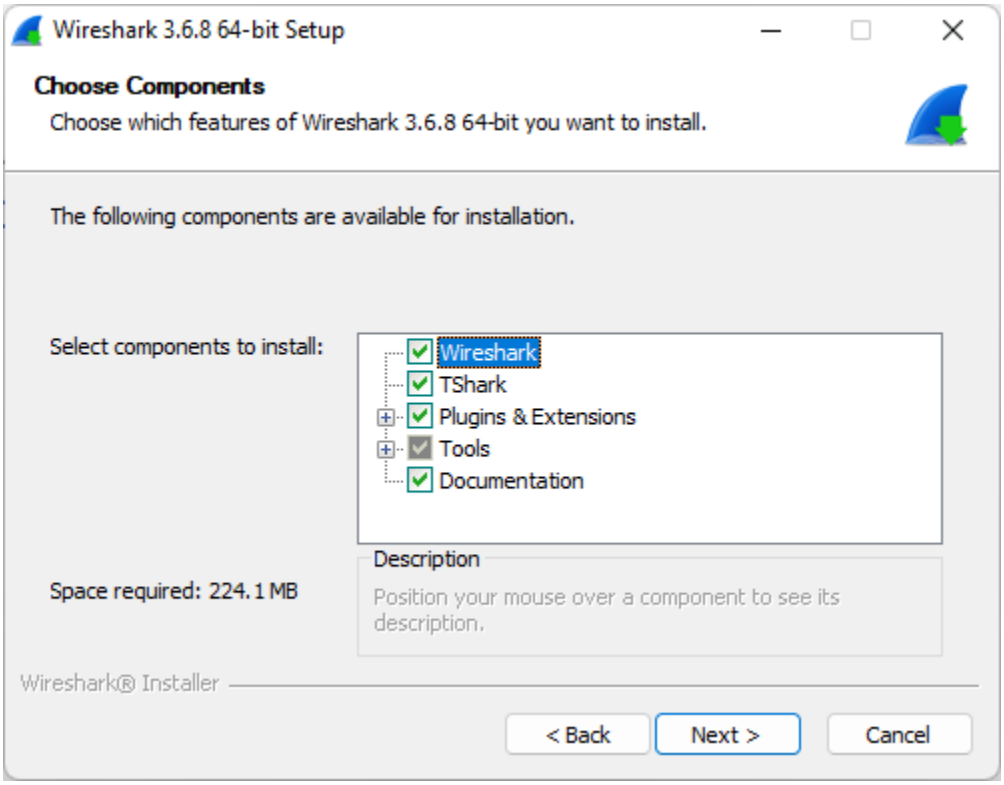
Features: The following are some of the many features Wireshark provides:

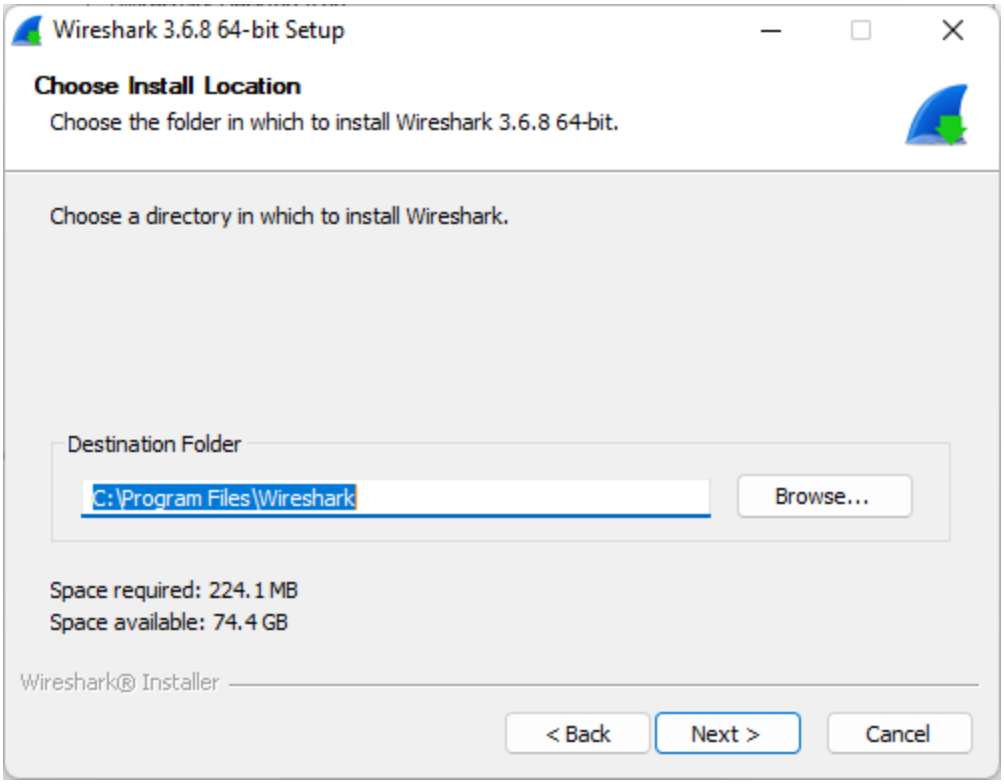
- Available for UNIX and Windows.
- Capture live packet data from a network interface.
- Open files containing packet data captured with tcpdump/WinDump, Wireshark and a number of other packet capture programs.
- Import packets from text files containing hex dumps of packet data.
- Display packets with very detailed protocol information.
- Export some or all packets in a number of capture file formats. Search for packets on many criteria.
- Colorize packet display based on filters.
- Create various statistics.

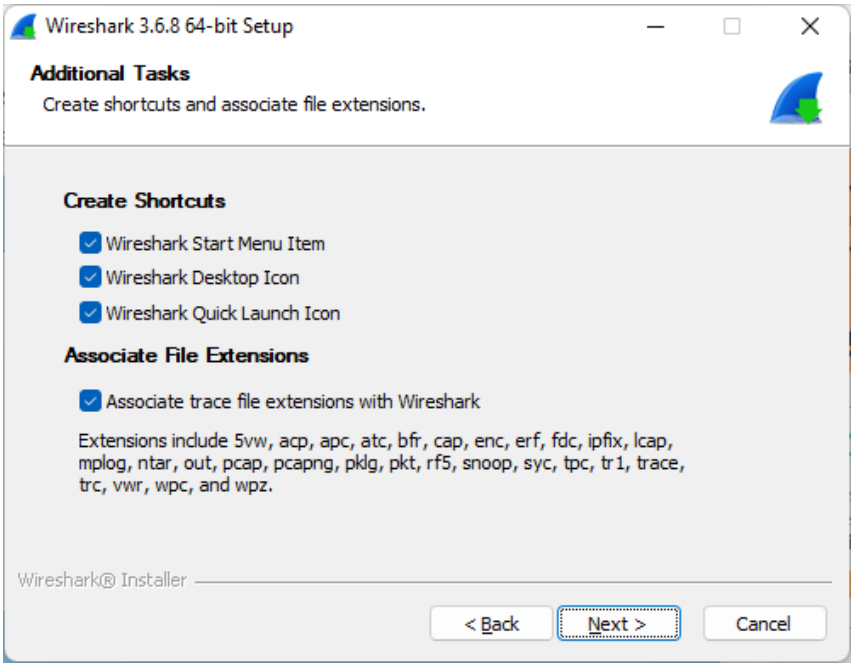
Installation:

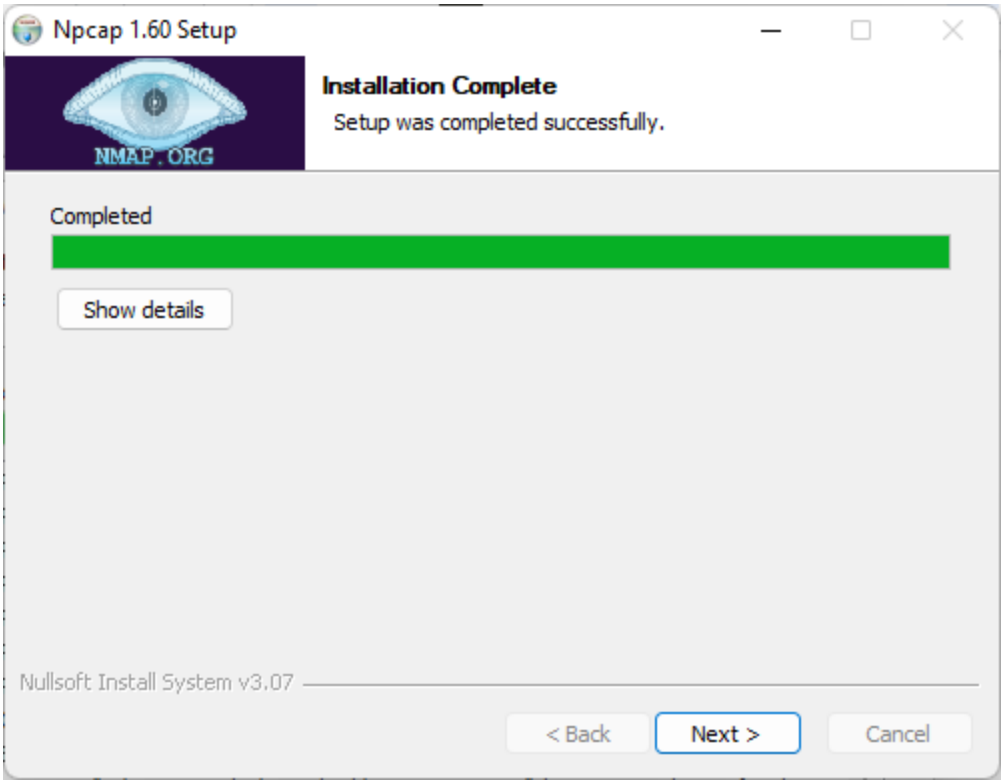
Download Wireshark for windows:

Link: https://www.wireshark.org/download.html

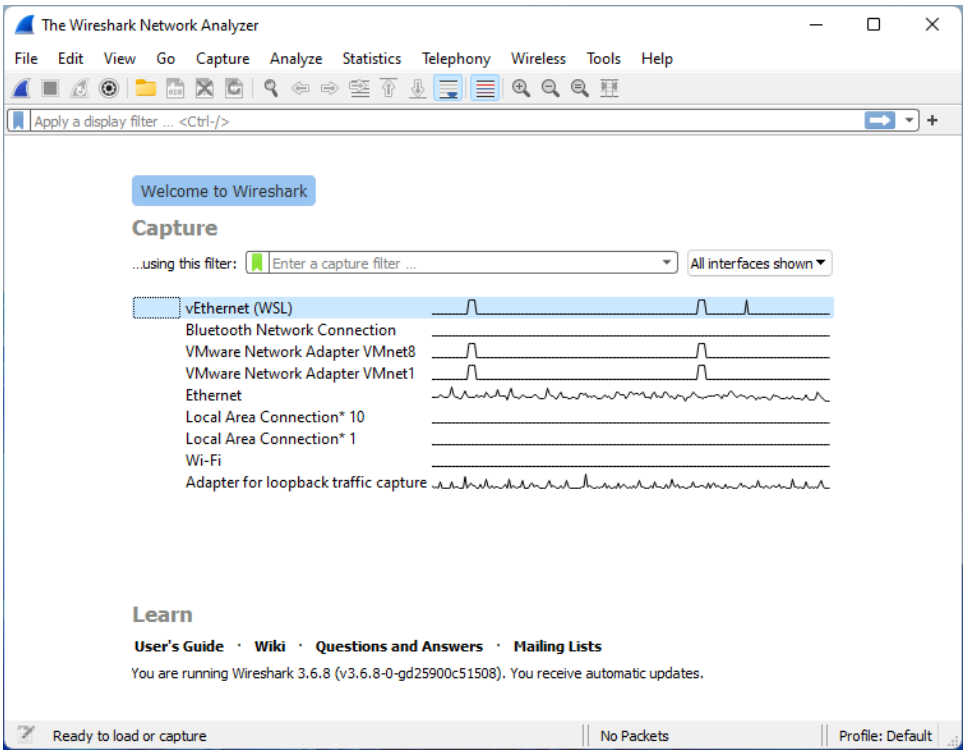



Wireshark 3.6.8 64-bit Setup
Choose Install Location
Choose the folder in which to install Wireshark 3.6.8 64-bit.
Choose a directory in which to install Wireshark.
Destination Folder
C:\Program Files\Wireshark
Browse...
Space required: 224.1 MB
Space available: 74.4 GB
Wireshark® Installer
< Back
Next >
Cancel


Wireshark 3.6.8 64-bit Setup
Additional Tasks
Create shortcuts and associate file extensions.
Create Shortcuts
Wireshark Start Menu Item
Wireshark Desktop Icon
Wireshark Quick Launch Icon
Associate File Extensions
Associate trace file extensions with Wireshark
Extensions include 5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, ipfix, lcap, mplog, ntar, out, pcap, pcapng, pklg, pkt, rf5, snoop, syc, tpc, tr1, trace, trc, vwr, wpc, and wpz.
Wireshark® Installer
< Back
Next >
Cancel

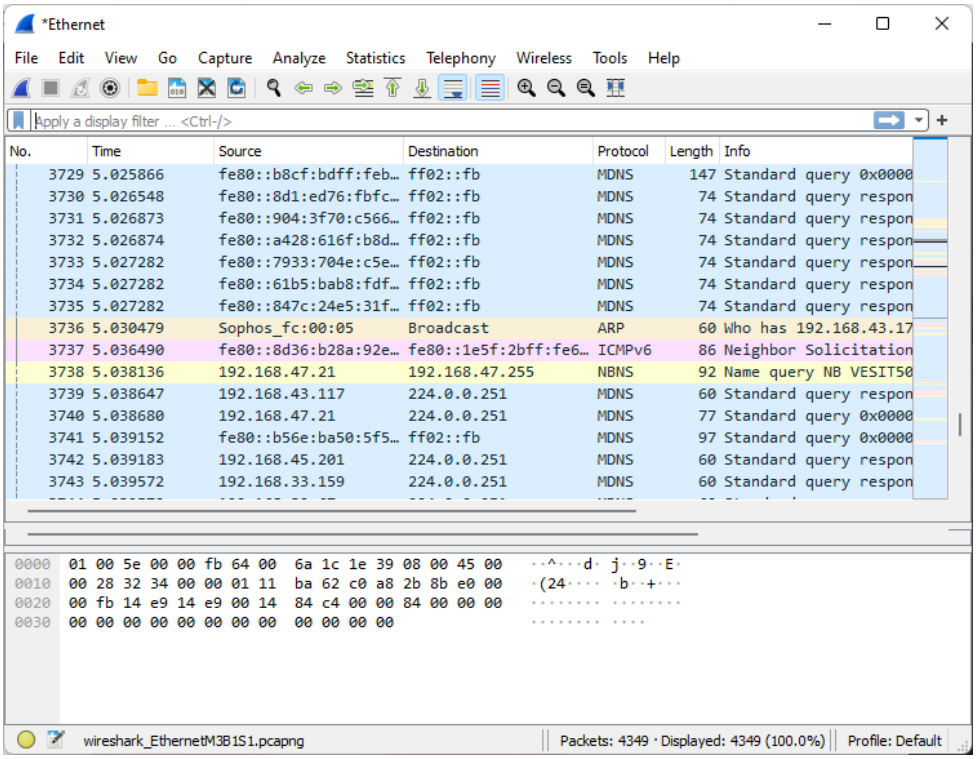


- **Wireshark is successfully installed.**



Capturing Packets

After downloading and installing wireshark, you can launch it and click the name of an interface under Interface List to start capturing packets on that interface. For example, if you want to capture traffic on the wireless network, click your wireless interface. You can configure advanced features by clicking Capture Options.

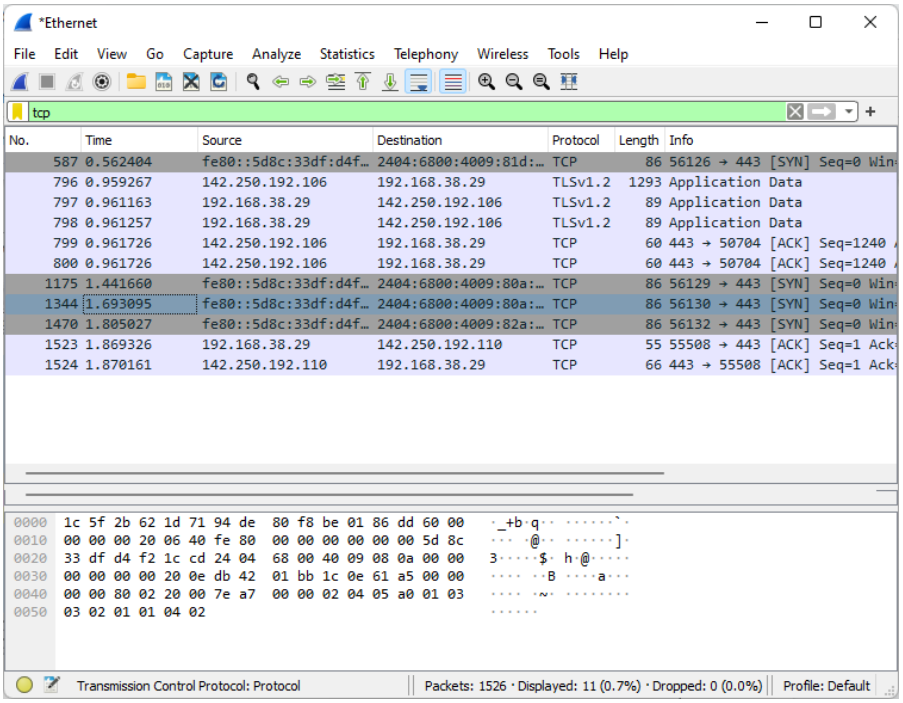


Filtering Packets

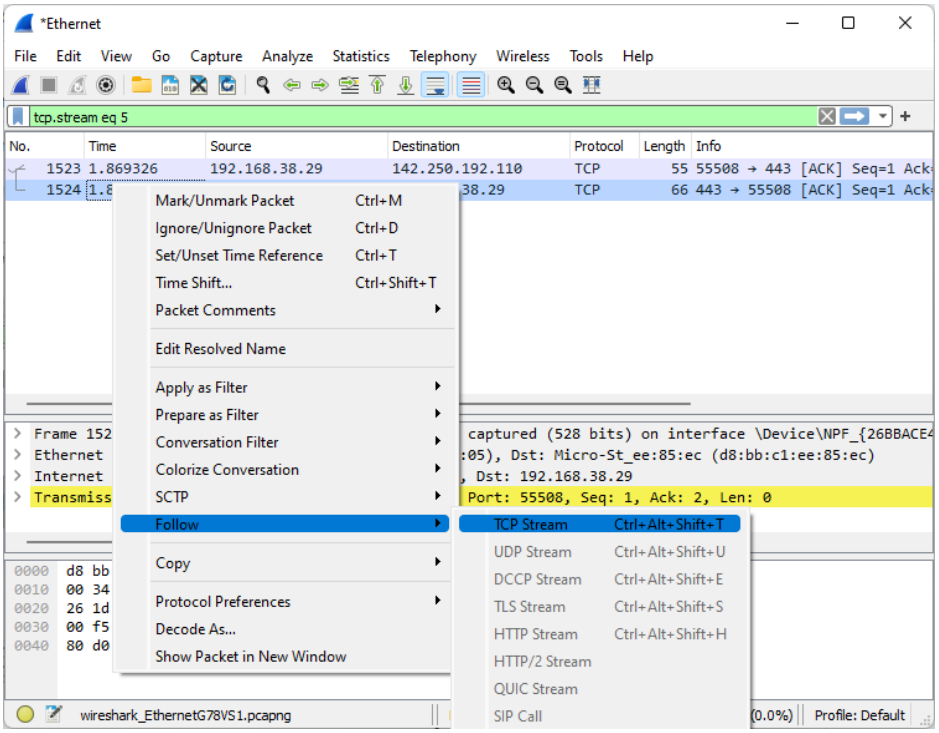
If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's whereWireshark's filters come in.

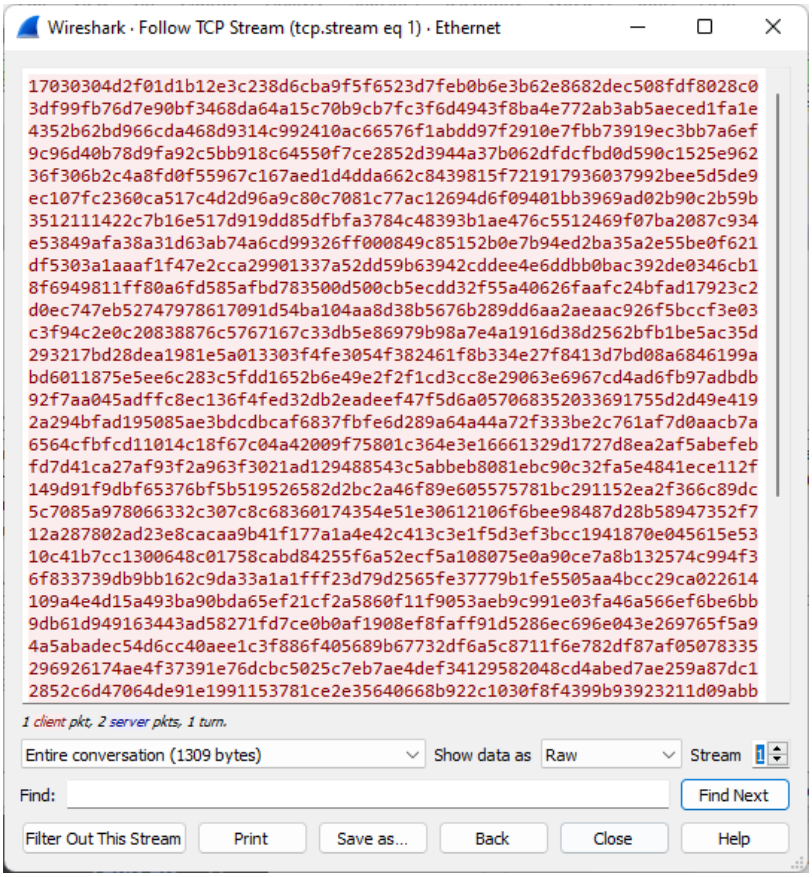
The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.

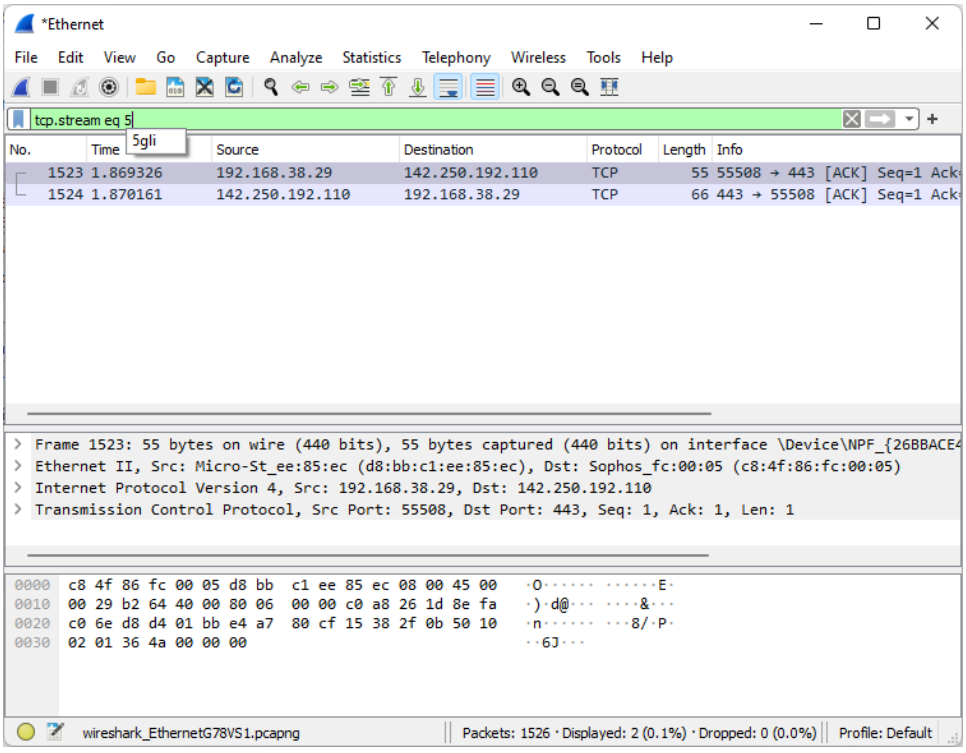
Filter the tcp packets by putting “tcp” in the filter box.



Click on follow stream and you will be able to see the entire conversation between client and server

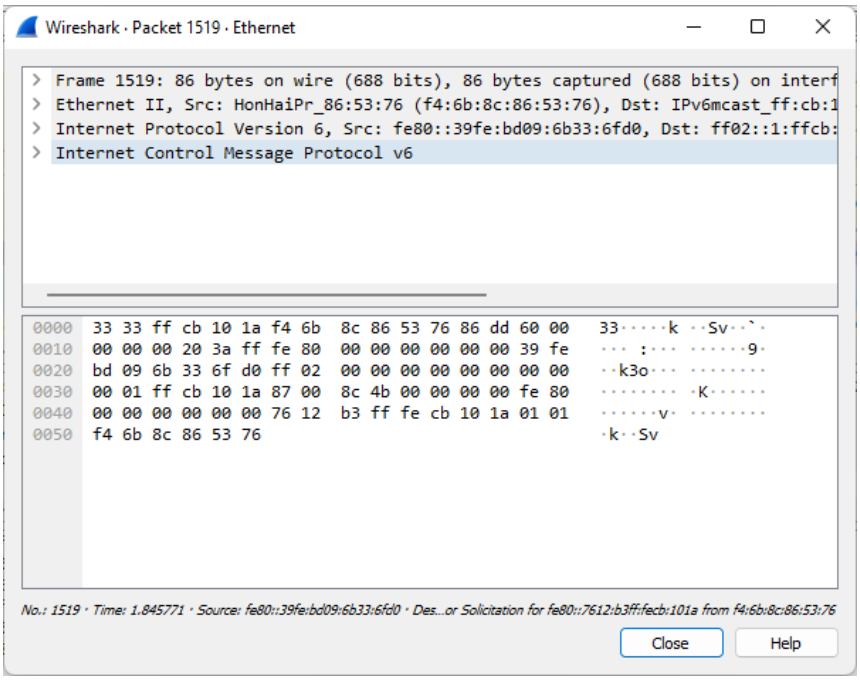



Wireshark · Follow TCP Stream (tcp.stream eq 1) · Ethernet
17030304d2f01d1b12e3c238d6cba9f5f6523d7feb0b6e3b62e8682dec508fdf8028c0
3df99fb76d7e90bf3468da64a15c70b9cb7fc3f6d4943f8ba4e772ab3ab5aeced1fa1e
4352b62bd966cda468d9314c992410ac66576f1abdd97f2910e7fbb73919ec3bb7a6ef
9c96d40b78d9fa92c5bb918c64550f7ce2852d3944a37b062dfdcfbd0d590c1525e962
36f306b2c4a8fd0f55967c167aed1d4dda662c8439815f721917936037992bee5d5de9
ec107fc2360ca517c4d2d96a9c80c7081c77ac12694d6f09401bb3969ad02b90c2b59b
3512111422c7b16e517d919dd85dfbfa3784c48393b1ae476c5512469f07ba2087c934
e53849afa38a31d63ab74a6cd99326ff000849c85152b0e7b94ed2ba35a2e55be0f621
df5303a1aaaf1f47e2cca29901337a52dd59b63942cddee4e6ddbb0bac392de0346cb1
8f6949811ff80a6fd585afbd783500d500cb5ecdd32f55a40626faafc24bfad17923c2
d0ec747eb52747978617091d54ba104aa8d38b5676b289dd6aa2aeaac926f5bccf3e03
c3f94c2e0c20838876c5767167c33db5e86979b98a7e4a1916d38d2562bfb1be5ac35d
293217bd28dea1981e5a013303f4fe3054f382461f8b334e27f8413d7bd08a6846199a
bd6011875e5ee6c283c5fdd1652b6e49e2f2f1cd3cc8e29063e6967cd4ad6fb97adbdb
92f7aa045adffc8ec136f4fed32db2eadeef47f5d6a057068352033691755d2d49e419
2a294bfad195085ae3bdcdbcaf6837fbfe6d289a64a44a72f333be2c761af7d0aacb7a
6564cfbfcd11014c18f67c04a42009f75801c364e3e16661329d1727d8ea2af5abefeb
fd7d41ca27af93f2a963f3021ad129488543c5abbeb8081ebc90c32fa5e4841ece112f
149d91f9dbf65376bf5b519526582d2bc2a46f89e605575781bc291152ea2f366c89dc
5c7085a978066332c307c8c68360174354e51e30612106f6bee98487d28b58947352f7
12a287802ad23e8cacaa9b41f177a1a4e42c413c3e1f5d3ef3bcc1941870e045615e53
10c41b7cc1300648c01758cabd84255f6a52ecf5a108075e0a90ce7a8b132574c994f3
6f833739db9bb162c9da33a1a1fff23d79d2565fe37779b1fe5505aa4bcc29ca022614
109a4e4d15a493ba90bda65ef21cf2a5860f11f9053aeb9c991e03fa46a566ef6be6bb
9db61d949163443ad58271fd7ce0b0af1908ef8faff91d5286ec696e043e269765f5a9
4a5abadec54d6cc40aee1c3f886f405689b67732df6a5c8711f6e782df87af05078335
296926174ae4f37391e76dcbc5025c7eb7ae4def34129582048cd4abed7ae259a87dc1
2852c6d47064de91e1991153781ce2e35640668b922c1030f8f4399b93923211d09abb
1 client pkt, 2 server pkts, 1 turn.
Entire conversation (1309 bytes)
Show data as
Raw
Stream
1
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

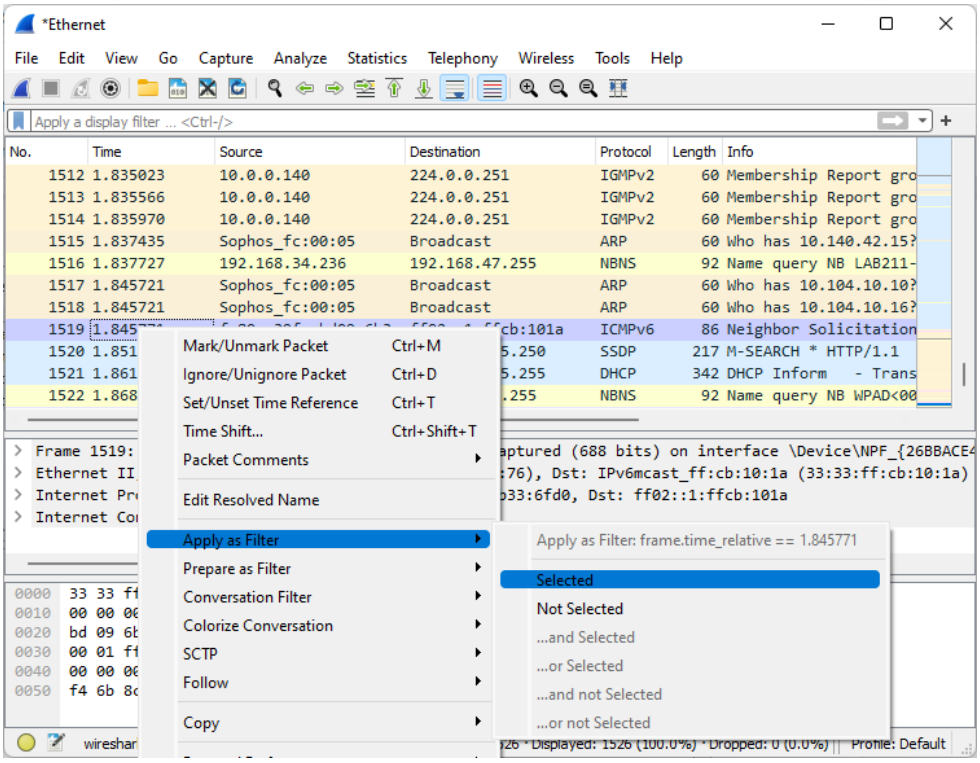

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 5
5gli
No. Time Source Destination Protocol Length Info
1523 1.869326 192.168.38.29 142.250.192.110 TCP 55 55508 → 443 [ACK] Seq=1 Ack
1524 1.870161 142.250.192.110 192.168.38.29 TCP 66 443 → 55508 [ACK] Seq=1 Ack
Frame 1523: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{26BBACE4
Ethernet II, Src: Micro-St_ee:85:ec (d8:bb:c1:ee:85:ec), Dst: Sophos_fc:00:05 (c8:4f:86:fc:00:05)
Internet Protocol Version 4, Src: 192.168.38.29, Dst: 142.250.192.110
Transmission Control Protocol, Src Port: 55508, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
0000 c8 4f 86 fc 00 05 d8 bb c1 ee 85 ec 08 00 45 00 ·O···· ····· ·····E·
0010 00 29 b2 64 40 00 80 06 00 00 c0 a8 26 1d 8e fa ·)·d@··· ····&···
0020 c0 6e d8 d4 01 bb e4 a7 80 cf 15 38 2f 0b 50 10 ·n····· ···8/·P·
0030 02 01 36 4a 00 00 00 ··6J···
wireshark_EthernetG78VS1.pcapng
Packets: 1526 · Displayed: 2 (0.1%) · Dropped: 0 (0.0%)
Profile: Default

Inspecting Packets

Click a packet to select it and you can dig down to view its details.



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



Conclusion: In this experiment we analyzed various packet sniffing tools that monitor network traffic transmitted between legitimate users or in the network. It is opted for network monitoring, traffic analysis, troubleshooting, Packet grabbing, message, protocol analysis, penetration testing and many other purposes.