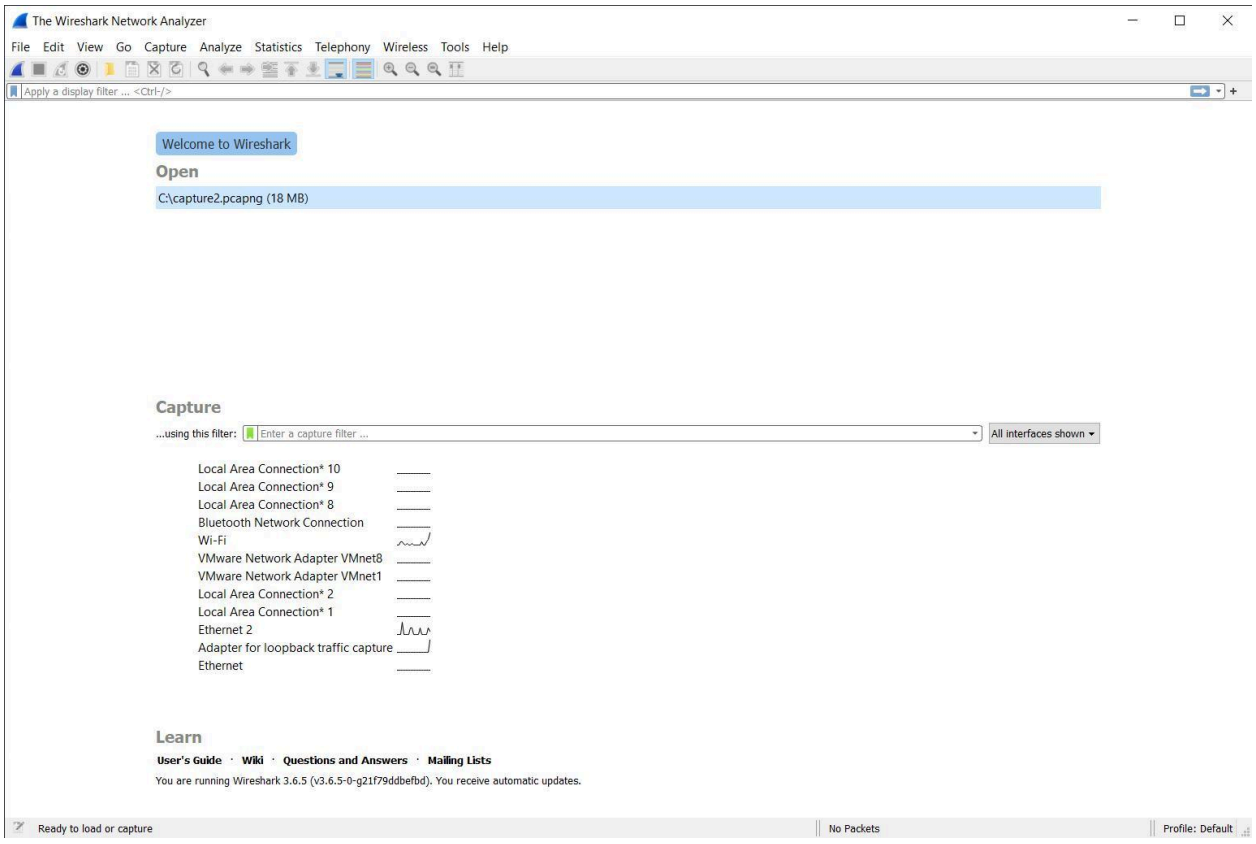
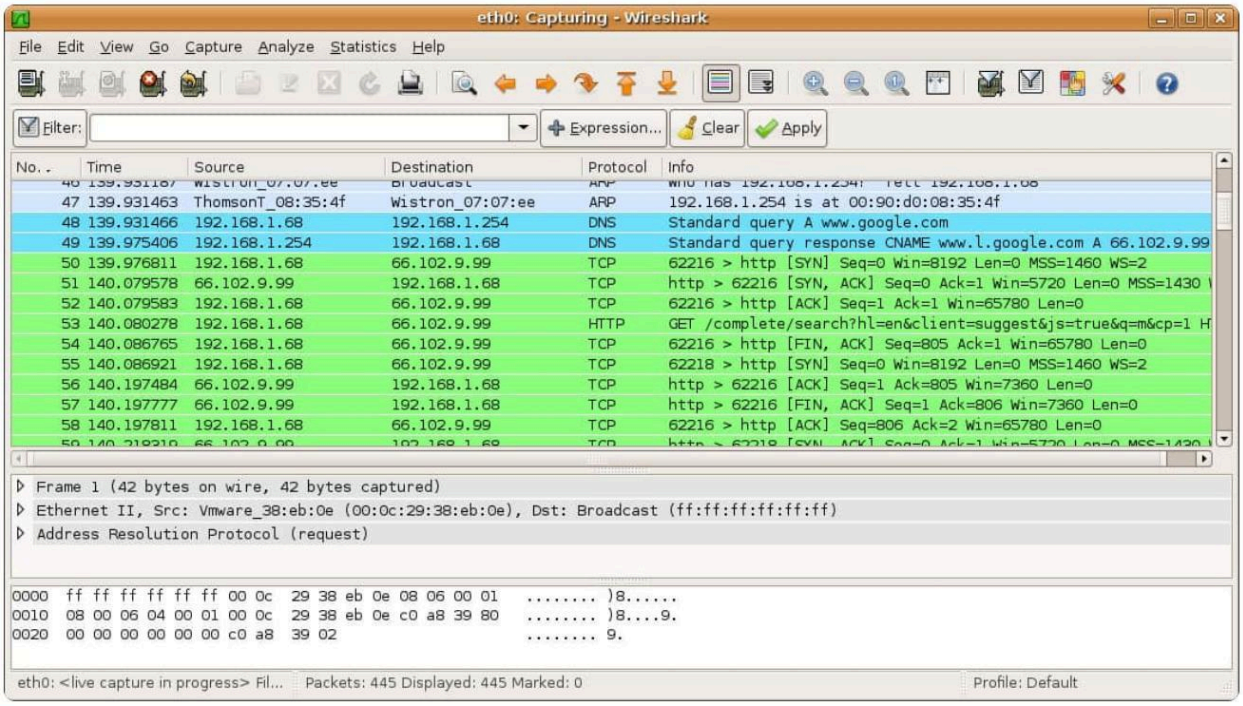
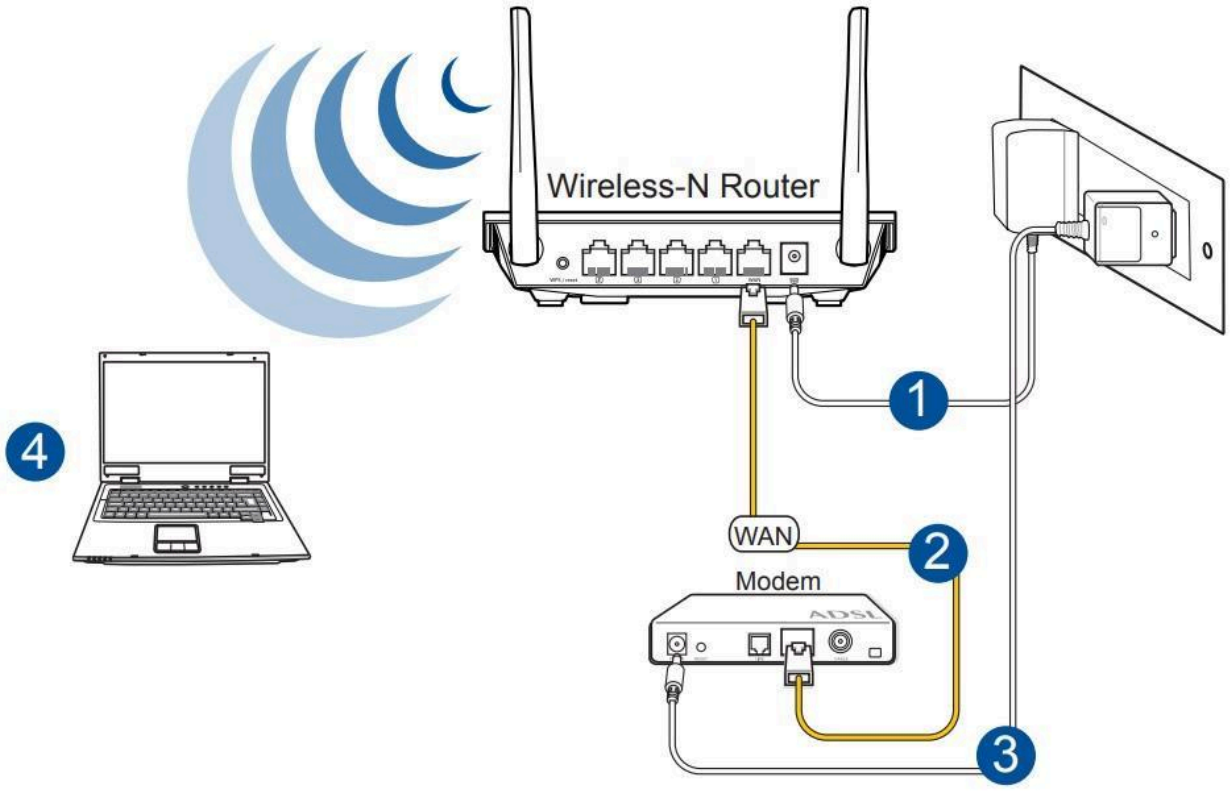
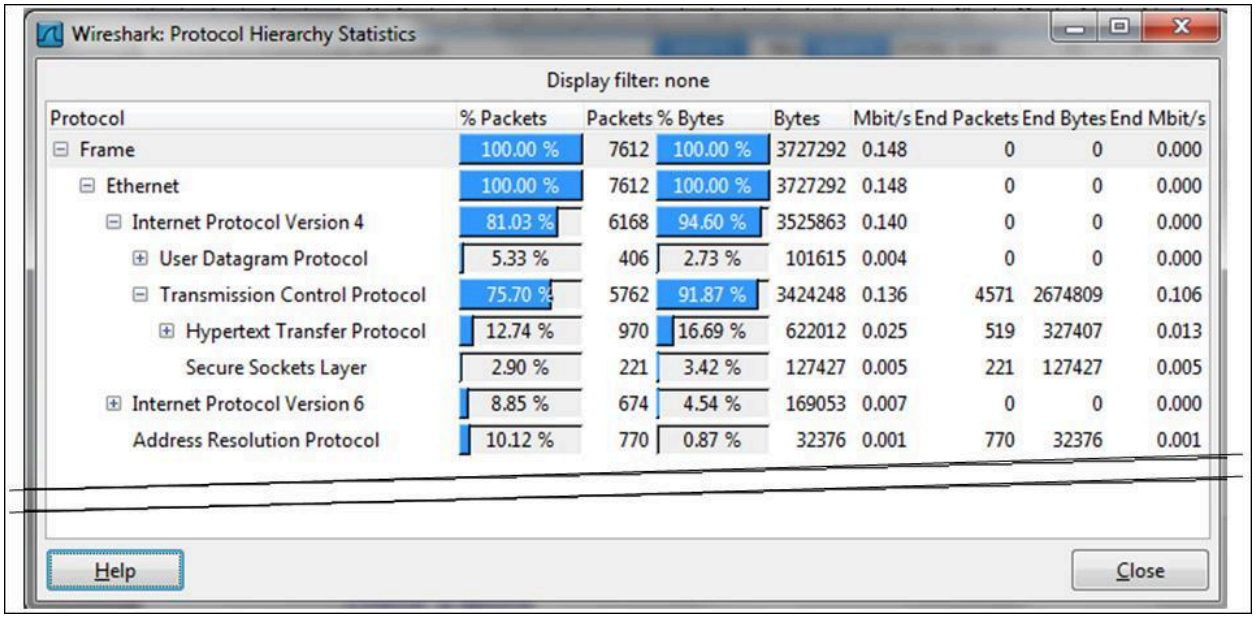
Wireshark Tutorial: Testing and Securing Network Traffic on a Home Network




eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. . Time Source Destination Protocol Info
47 139.931463 ThomsonT_08:35:4f Wistron_07:07:ee ARP 192.168.1.254 is at 00:90:d0:08:35:4f
48 139.931466 192.168.1.68 192.168.1.254 DNS Standard query A www.google.com
49 139.975406 192.168.1.254 192.168.1.68 DNS Standard query response CNAME www.l.google.com A 66.102.9.99
50 139.976811 192.168.1.68 66.102.9.99 TCP 62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
51 140.079578 66.102.9.99 192.168.1.68 TCP http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
52 140.079583 192.168.1.68 66.102.9.99 TCP 62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
53 140.080278 192.168.1.68 66.102.9.99 HTTP GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1
54 140.086765 192.168.1.68 66.102.9.99 TCP 62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
55 140.086921 192.168.1.68 66.102.9.99 TCP 62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
56 140.197484 66.102.9.99 192.168.1.68 TCP http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
57 140.197777 66.102.9.99 192.168.1.68 TCP http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
58 140.197811 192.168.1.68 66.102.9.99 TCP 62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
Frame 1 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 0c 29 38 eb 0e 08 06 00 01 ....)8......
0010 08 00 06 04 00 01 00 0c 29 38 eb 0e c0 a8 39 80 ....)8....9.
0020 00 00 00 00 00 00 c0 a8 39 02 .... 9.
eth0: <live capture in progress> Fil... Packets: 445 Displayed: 445 Marked: 0 Profile: Default


Wireless-N Router
WAN
Modem
ADSL
1
2
3
4



Introduction

Wireshark is a free, open-source network protocol analyzer used by network administrators, cybersecurity professionals, students, and home users to monitor, troubleshoot, and secure network communications. It allows you to capture network packets and inspect the data traveling between devices on your network.

This tutorial teaches you how to:

- Install Wireshark
- Capture network traffic safely
- Analyze common protocols
- Identify suspicious network activity
- Improve the security of your home network

Difficulty: Beginner to Intermediate

Estimated Time: 45–60 minutes

Learning Objectives

After completing this tutorial, you will be able to:

- Install Wireshark

- Capture packets on your home network
- Filter captured traffic
- Identify insecure protocols
- Detect unusual devices or communications
- Apply security improvements to your home network

What You'll Need

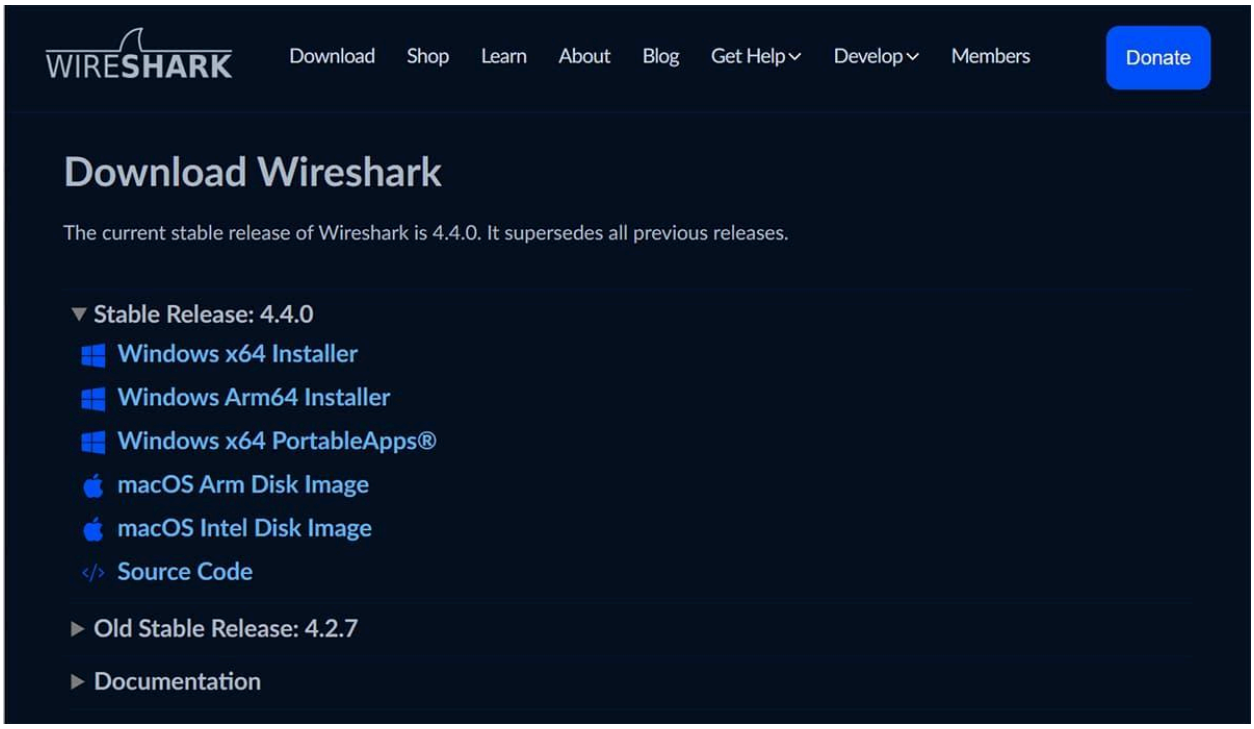
Hardware

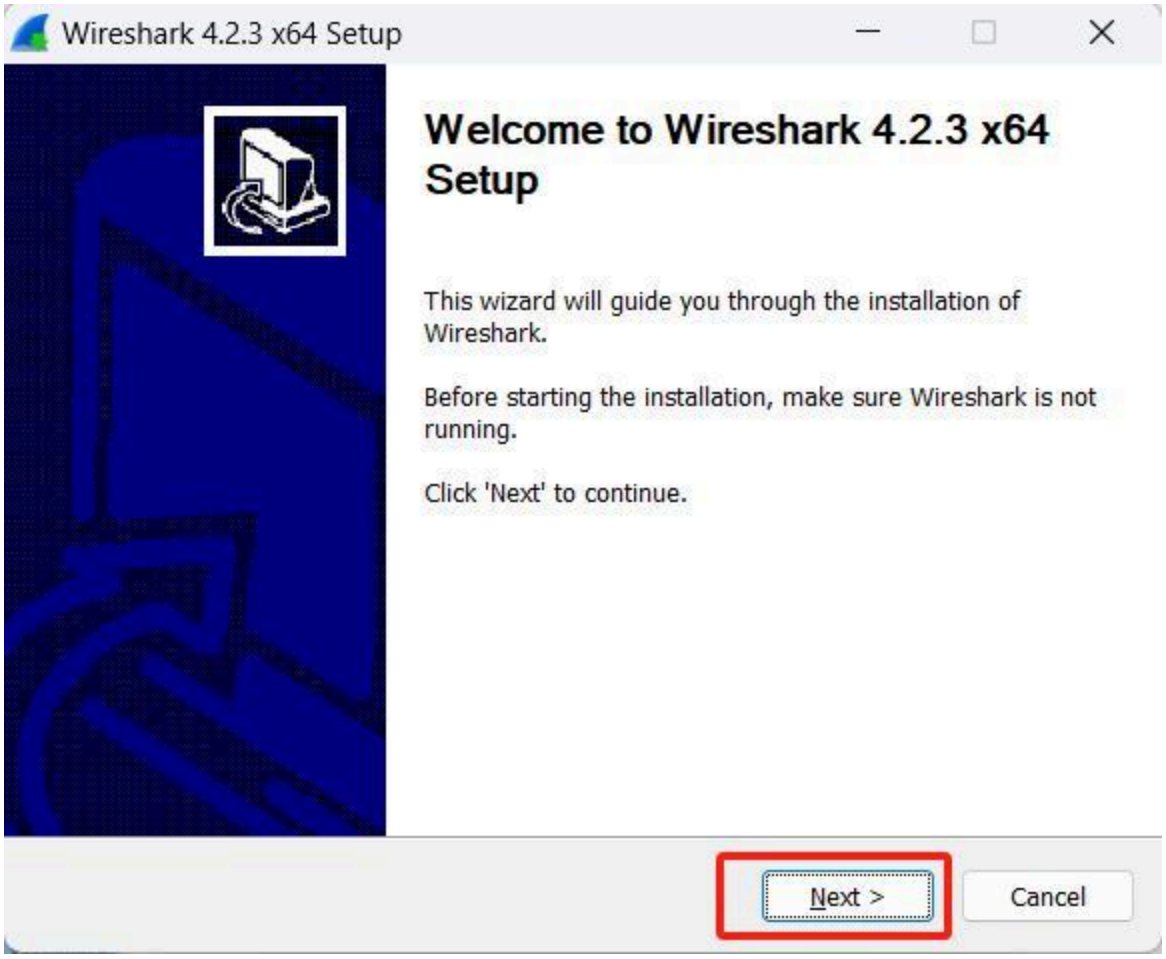
- Desktop or Laptop
- Home Wi-Fi Router
- Internet Connection

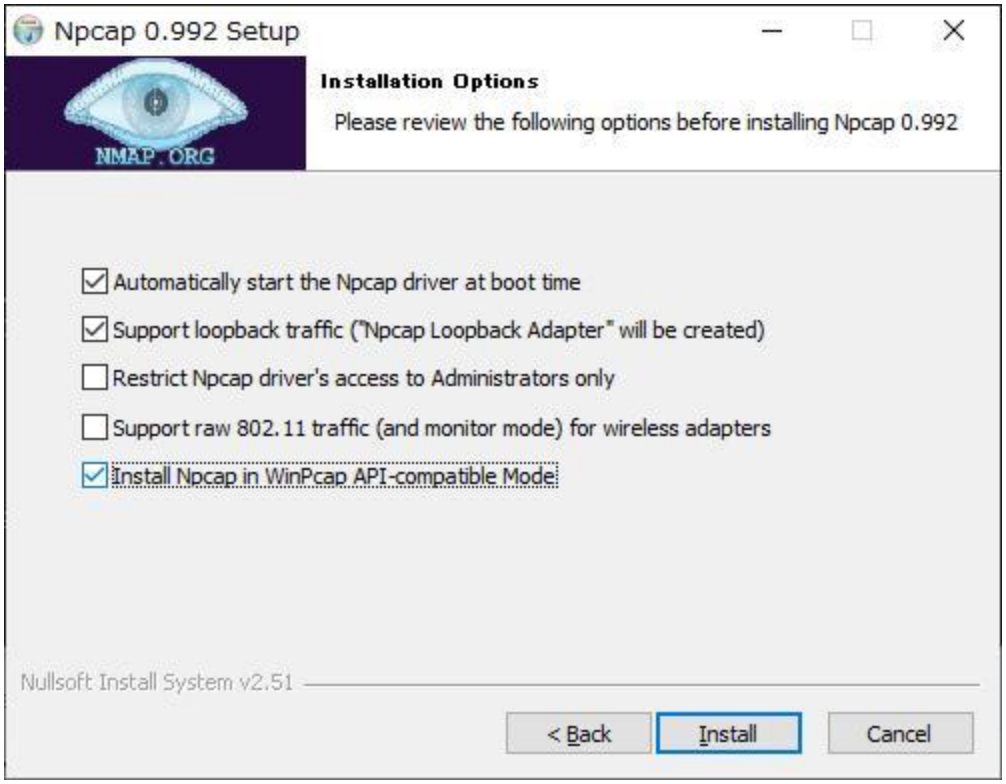
Software

- Wireshark (Latest Version)
- Windows, Linux, or macOS

Step 1: Download and Install Wireshark


WIRESHARK
Download
Shop
Learn
About
Blog
Get Help
Develop
Members
Donate
Download Wireshark
The current stable release of Wireshark is 4.4.0. It supersedes all previous releases.
Stable Release: 4.4.0
Windows x64 Installer
Windows Arm64 Installer
Windows x64 PortableApps®
macOS Arm Disk Image
macOS Intel Disk Image
Source Code
Old Stable Release: 4.2.7
Documentation


Wireshark 4.2.3 x64 Setup
Welcome to Wireshark 4.2.3 x64 Setup
This wizard will guide you through the installation of Wireshark.
Before starting the installation, make sure Wireshark is not running.
Click 'Next' to continue.
Next >
Cancel



1. Visit the official Wireshark website.
2. Download the version for your operating system.
3. Run the installer.
4. Install **Npcap** when prompted.
5. Restart your computer if requested.

Step 2: Open Wireshark

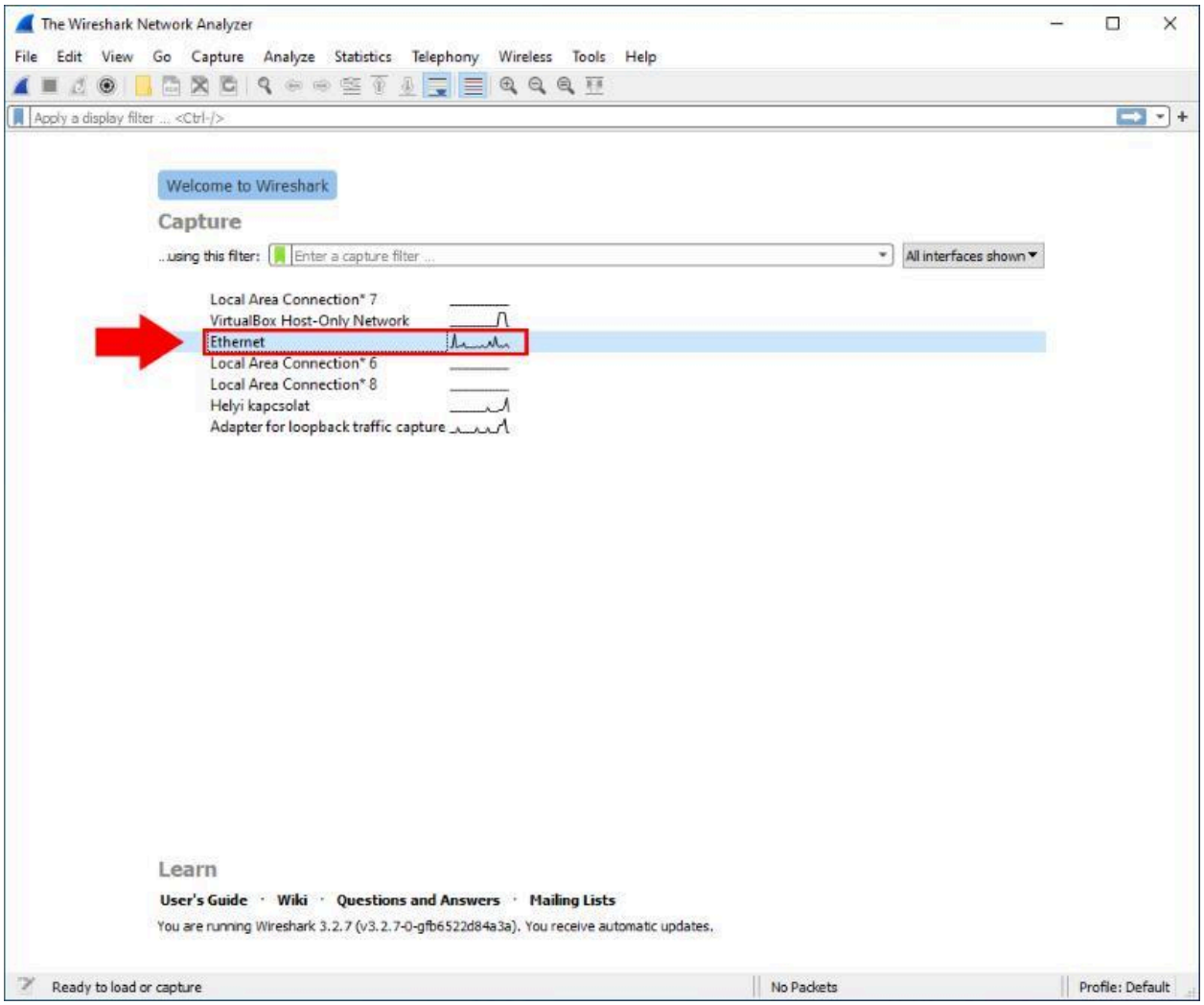
When Wireshark starts you'll see a list of available network interfaces.

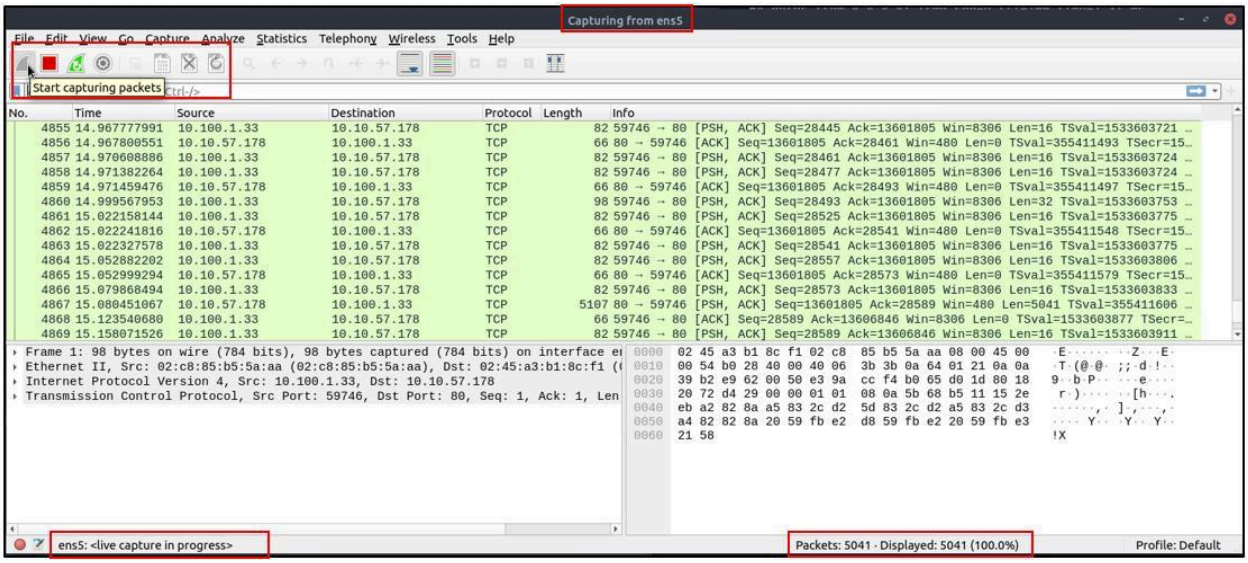
Examples include:

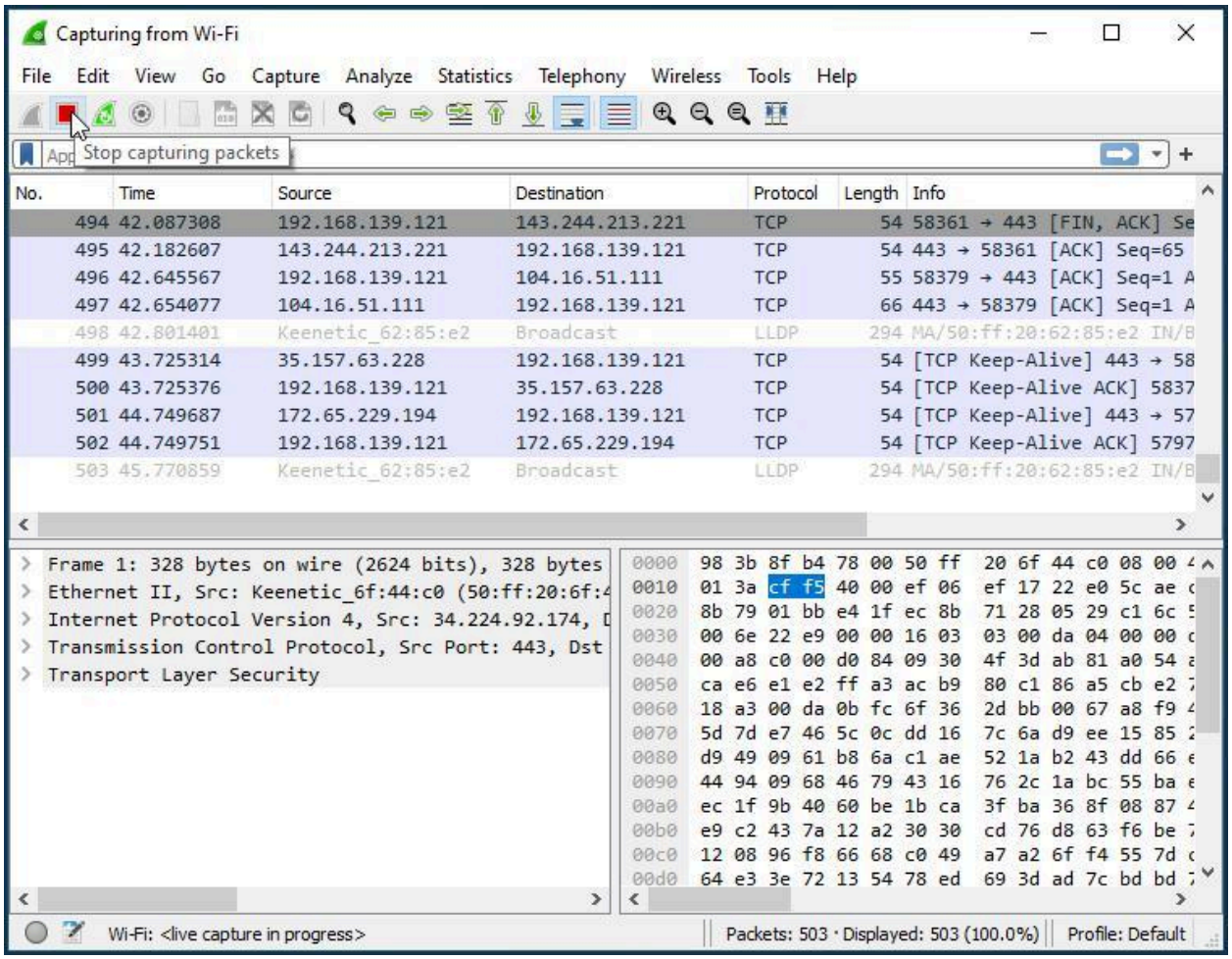
- Ethernet
- Wi-Fi
- VPN Adapter
- Loopback Interface

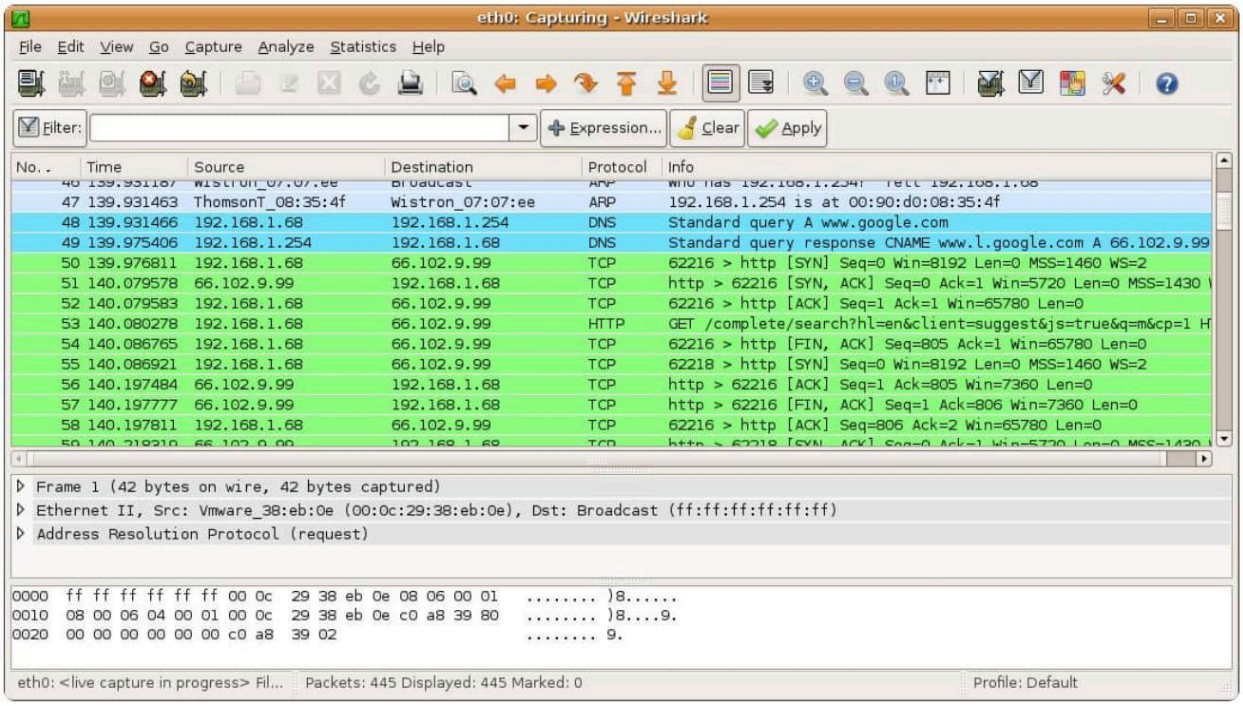
The interface with the moving graph is usually your active connection.

Step 3: Start Capturing Traffic




Capturing from ens5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Start capturing packets
No. Time Source Destination Protocol Length Info
4855 14.967777991 10.100.1.33 10.10.57.178 TCP 82 59746 → 80 [PSH, ACK] Seq=28445 Ack=13601805 Win=8306 Len=16 TSval=1533603721 …
4856 14.967800551 10.10.57.178 10.100.1.33 TCP 66 80 → 59746 [ACK] Seq=13601805 Ack=28461 Win=480 Len=0 TSval=355411493 TSecr=15…
4857 14.970608886 10.100.1.33 10.10.57.178 TCP 82 59746 → 80 [PSH, ACK] Seq=28461 Ack=13601805 Win=8306 Len=16 TSval=1533603724 …
4858 14.971382264 10.100.1.33 10.10.57.178 TCP 82 59746 → 80 [PSH, ACK] Seq=28477 Ack=13601805 Win=8306 Len=16 TSval=1533603724 …
4859 14.971459476 10.10.57.178 10.100.1.33 TCP 66 80 → 59746 [ACK] Seq=13601805 Ack=28493 Win=480 Len=0 TSval=355411497 TSecr=15…
4860 14.999567953 10.100.1.33 10.10.57.178 TCP 98 59746 → 80 [PSH, ACK] Seq=28493 Ack=13601805 Win=8306 Len=32 TSval=1533603753 …
4861 15.022158144 10.100.1.33 10.10.57.178 TCP 82 59746 → 80 [PSH, ACK] Seq=28525 Ack=13601805 Win=8306 Len=16 TSval=1533603775 …
4862 15.022241816 10.10.57.178 10.100.1.33 TCP 66 80 → 59746 [ACK] Seq=13601805 Ack=28541 Win=480 Len=0 TSval=355411548 TSecr=15…
4863 15.022327578 10.100.1.33 10.10.57.178 TCP 82 59746 → 80 [PSH, ACK] Seq=28541 Ack=13601805 Win=8306 Len=16 TSval=1533603775 …
4864 15.052882202 10.100.1.33 10.10.57.178 TCP 82 59746 → 80 [PSH, ACK] Seq=28557 Ack=13601805 Win=8306 Len=16 TSval=1533603806 …
4865 15.052999294 10.10.57.178 10.100.1.33 TCP 66 80 → 59746 [ACK] Seq=13601805 Ack=28573 Win=480 Len=0 TSval=355411579 TSecr=15…
4866 15.079868494 10.100.1.33 10.10.57.178 TCP 82 59746 → 80 [PSH, ACK] Seq=28573 Ack=13601805 Win=8306 Len=16 TSval=1533603833 …
4867 15.080451067 10.10.57.178 10.100.1.33 TCP 5107 80 → 59746 [PSH, ACK] Seq=13601805 Ack=28589 Win=480 Len=5041 TSval=355411606 …
4868 15.123540680 10.100.1.33 10.10.57.178 TCP 66 59746 → 80 [ACK] Seq=28589 Ack=13606846 Win=8306 Len=0 TSval=1533603877 TSecr=…
4869 15.158071526 10.100.1.33 10.10.57.178 TCP 82 59746 → 80 [PSH, ACK] Seq=28589 Ack=13606846 Win=8306 Len=16 TSval=1533603911 …
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface e
Ethernet II, Src: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa), Dst: 02:45:a3:b1:8c:f1 (
Internet Protocol Version 4, Src: 10.100.1.33, Dst: 10.10.57.178
Transmission Control Protocol, Src Port: 59746, Dst Port: 80, Seq: 1, Ack: 1, Len
0000 02 45 a3 b1 8c f1 02 c8 85 b5 5a aa 08 00 45 00
0010 00 54 b0 28 40 00 40 06 3b 3b 0a 64 01 21 0a 0a
0020 39 b2 e9 62 00 50 e3 9a cc f4 b0 65 d0 1d 80 18
0030 20 72 d4 29 00 00 01 01 08 0a 5b 68 b5 11 15 2e
0040 eb a2 82 8a a5 83 2c d2 5d 83 2c d2 a5 83 2c d3
0050 a4 82 82 8a 20 59 fb e2 d8 59 fb e2 20 59 fb e3
0060 21 58
ens5: <live capture in progress>
Packets: 5041 · Displayed: 5041 (100.0%)
Profile: Default


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Stop capturing packets
No. Time Source Destination Protocol Length Info
494 42.087308 192.168.139.121 143.244.213.221 TCP 54 58361 → 443 [FIN, ACK] Se
495 42.182607 143.244.213.221 192.168.139.121 TCP 54 443 → 58361 [ACK] Seq=65
496 42.645567 192.168.139.121 104.16.51.111 TCP 55 58379 → 443 [ACK] Seq=1 A
497 42.654077 104.16.51.111 192.168.139.121 TCP 66 443 → 58379 [ACK] Seq=1 A
498 42.801401 Keenetic_62:85:e2 Broadcast LLDP 294 MA/50:ff:20:62:85:e2 IN/B
499 43.725314 35.157.63.228 192.168.139.121 TCP 54 [TCP Keep-Alive] 443 → 58
500 43.725376 192.168.139.121 35.157.63.228 TCP 54 [TCP Keep-Alive ACK] 5837
501 44.749687 172.65.229.194 192.168.139.121 TCP 54 [TCP Keep-Alive] 443 → 57
502 44.749751 192.168.139.121 172.65.229.194 TCP 54 [TCP Keep-Alive ACK] 5797
503 45.770859 Keenetic_62:85:e2 Broadcast LLDP 294 MA/50:ff:20:62:85:e2 IN/B
Frame 1: 328 bytes on wire (2624 bits), 328 bytes
Ethernet II, Src: Keenetic_6f:44:c0 (50:ff:20:6f:4
Internet Protocol Version 4, Src: 34.224.92.174, D
Transmission Control Protocol, Src Port: 443, Dst
Transport Layer Security
0000 98 3b 8f b4 78 00 50 ff 20 6f 44 c0 08 00
0010 01 3a cf f5 40 00 ef 06 ef 17 22 e0 5c ae
0020 8b 79 01 bb e4 1f ec 8b 71 28 05 29 c1 6c
0030 00 6e 22 e9 00 00 16 03 03 00 da 04 00 00
0040 00 a8 c0 00 d0 84 09 30 4f 3d ab 81 a0 54
0050 ca e6 e1 e2 ff a3 ac b9 80 c1 86 a5 cb e2
0060 18 a3 00 da 0b fc 6f 36 2d bb 00 67 a8 f9
0070 5d 7d e7 46 5c 0c dd 16 7c 6a d9 ee 15 85
0080 d9 49 09 61 b8 6a c1 ae 52 1a b2 43 dd 66
0090 44 94 09 68 46 79 43 16 76 2c 1a bc 55 ba
00a0 ec 1f 9b 40 60 be 1b ca 3f ba 36 8f 08 87
00b0 e9 c2 43 7a 12 a2 30 30 cd 76 d8 63 f6 be
00c0 12 08 96 f8 66 68 c0 49 a7 a2 6f f4 55 7d
00d0 64 e3 3e 72 13 54 78 ed 69 3d ad 7c bd bd
Wi-Fi: <live capture in progress>
Packets: 503 · Displayed: 503 (100.0%)
Profile: Default



1. Double-click your active network adapter.
2. Packet capture begins immediately.
3. Browse a few websites or stream a short video.
4. Watch packets appear in real time.

You'll quickly see thousands of packets.

Understanding the Packet Window

Each packet contains:

Column	Description
Number	Packet sequence
Time	Capture time
Source	Sending device
Destination	Receiving device

Protocol	Network protocol
Length	Packet size
Info	Packet summary

Step 4: Stop Capturing

Click the **red Stop button**.

You now have a snapshot of your network traffic for analysis.

Step 5: Save Your Capture

Select:

File → Save As

Save using the **.pcapng** format.

Example:

HomeNetworkTest.pcapng

Step 6: Use Display Filters

One of Wireshark's most useful features is filtering.

Examples:

Show only HTTP

http

Show only HTTPS

tls

Show only DNS

dns

Show only TCP

tcp

Show only UDP

udp

Show ICMP (Ping)

icmp

Show Traffic from One Device

ip.addr == 192.168.1.15

Replace the IP address with your own device.

Step 7: Identify Devices on Your Network

Look at:

- Source IP
- Destination IP

Common home addresses include:

192.168.x.x

10.x.x.x

172.16.x.x

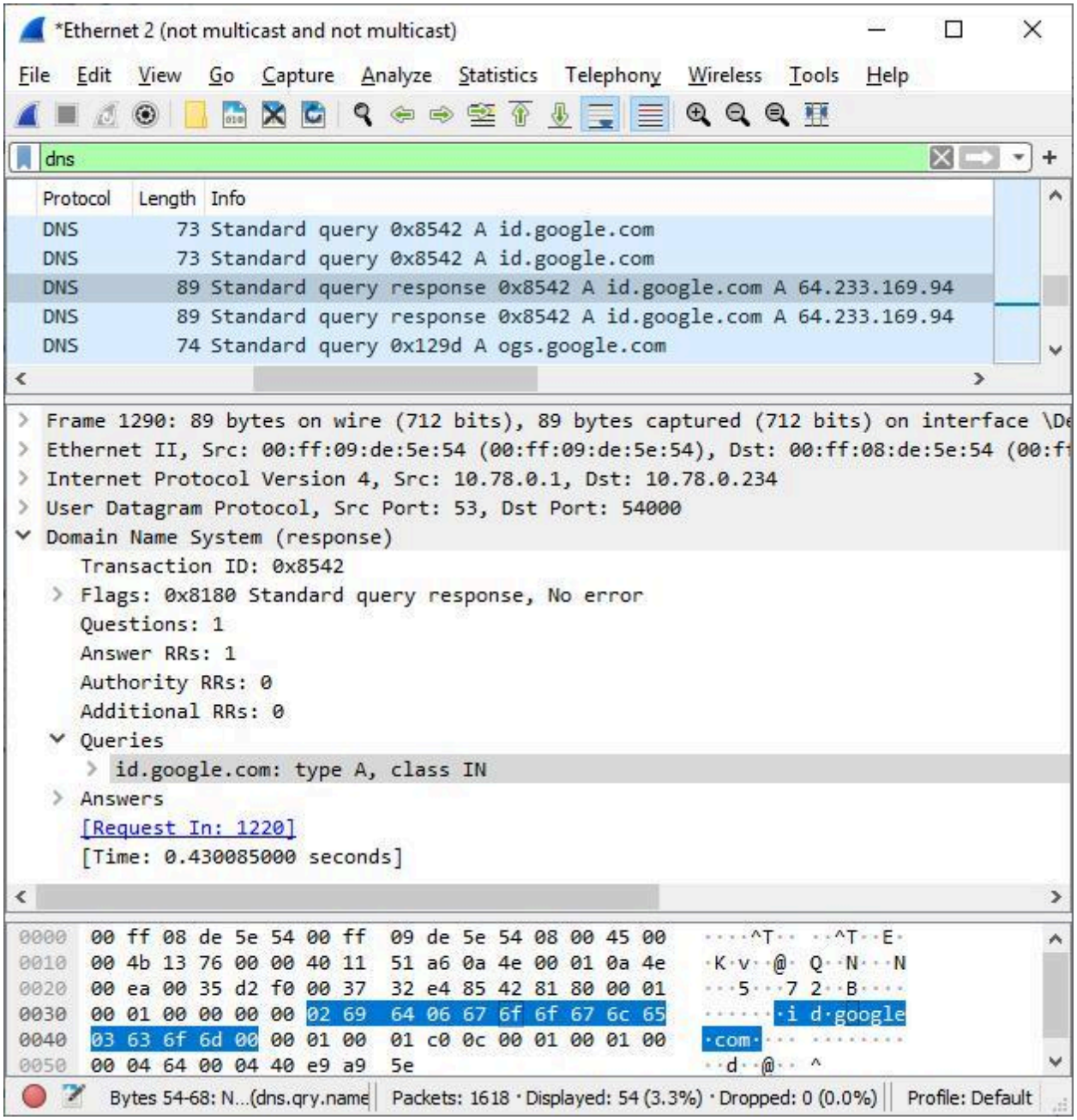
Unknown addresses may indicate:

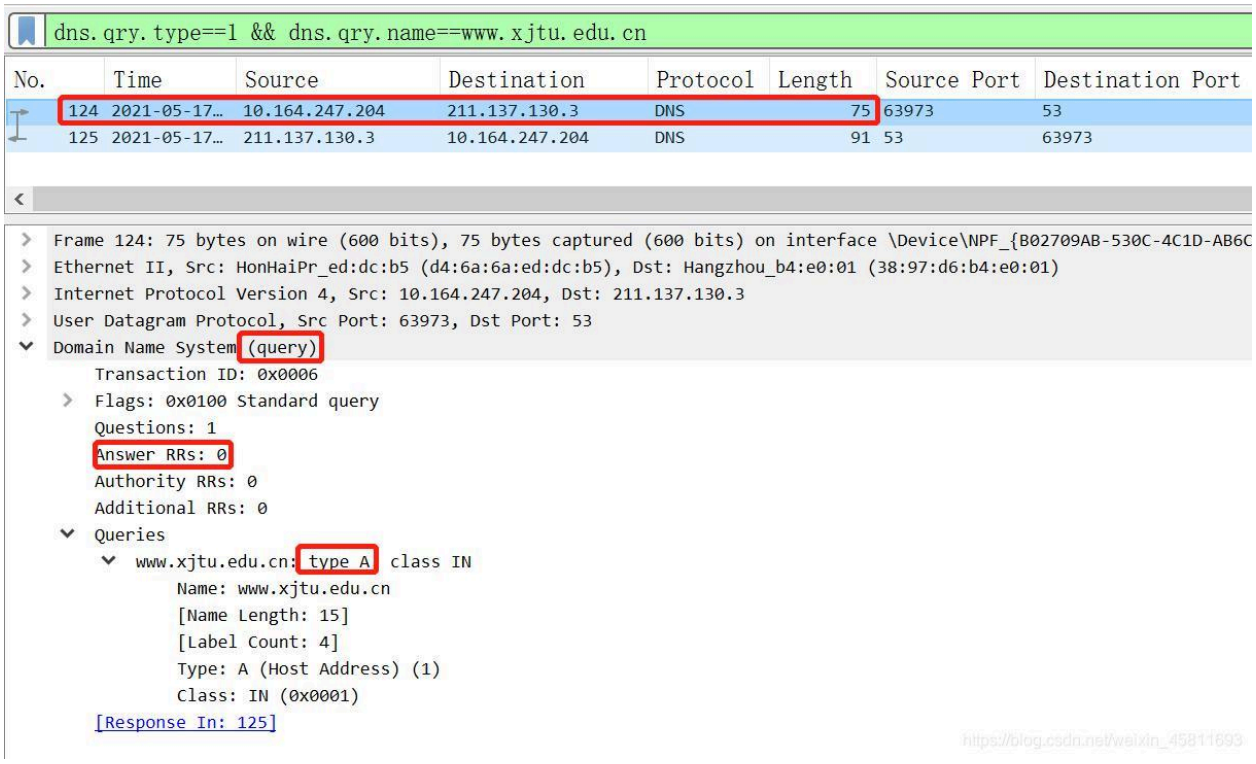
- Guest devices
- Smart TVs
- IoT devices
- Security cameras
- Printers

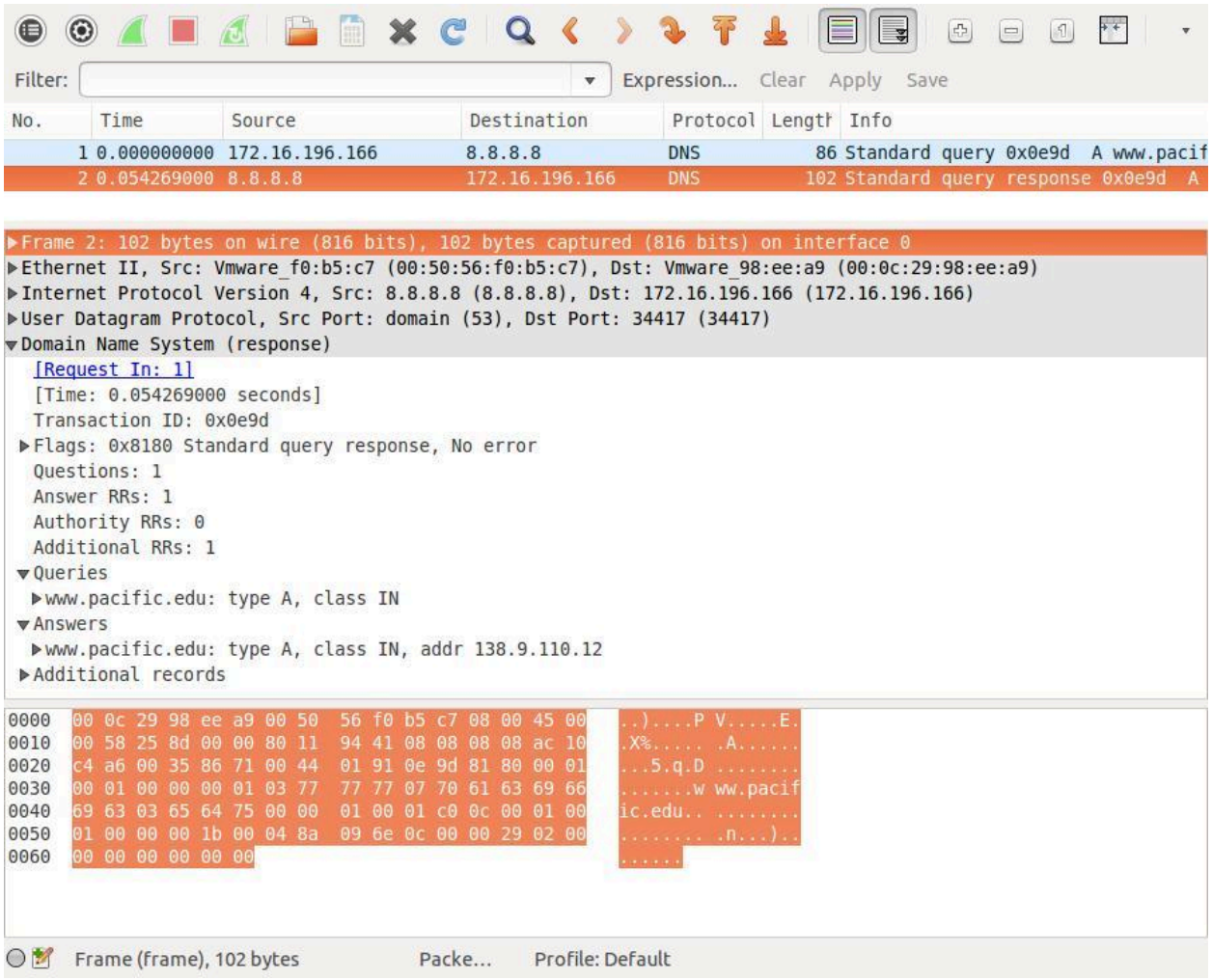
If you find an unknown device:

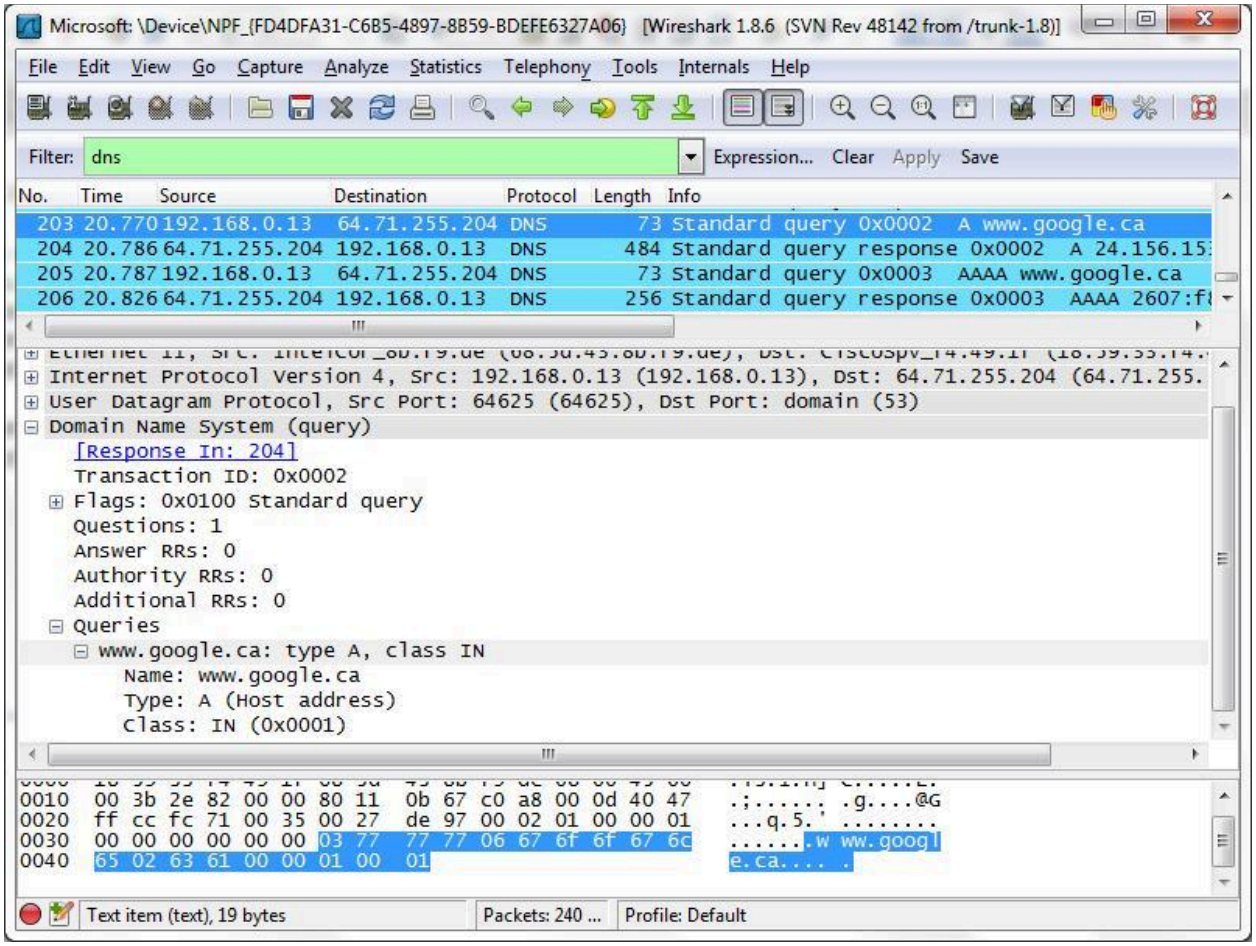
- Check your router's device list
- Change your Wi-Fi password if needed
- Disable WPS
- Update router firmware

Step 8: Analyze DNS Requests


*Ethernet 2 (not multicast and not multicast)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Protocol Length Info
DNS 73 Standard query 0x8542 A id.google.com
DNS 73 Standard query 0x8542 A id.google.com
DNS 89 Standard query response 0x8542 A id.google.com A 64.233.169.94
DNS 89 Standard query response 0x8542 A id.google.com A 64.233.169.94
DNS 74 Standard query 0x129d A ogs.google.com
Frame 1290: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \De
Ethernet II, Src: 00:ff:09:de:5e:54 (00:ff:09:de:5e:54), Dst: 00:ff:08:de:5e:54 (00:ff
Internet Protocol Version 4, Src: 10.78.0.1, Dst: 10.78.0.234
User Datagram Protocol, Src Port: 53, Dst Port: 54000
Domain Name System (response)
Transaction ID: 0x8542
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
id.google.com: type A, class IN
Answers
[Request In: 1220]
[Time: 0.430085000 seconds]
0000 00 ff 08 de 5e 54 00 ff 09 de 5e 54 08 00 45 00
0010 00 4b 13 76 00 00 40 11 51 a6 0a 4e 00 01 0a 4e
0020 00 ea 00 35 d2 f0 00 37 32 e4 85 42 81 80 00 01
0030 00 01 00 00 00 00 02 69 64 06 67 6f 6f 67 6c 65
0040 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00 01 00
0050 00 04 64 00 04 40 e9 a9 5e
Bytes 54-68: N...(dns.qry.name
Packets: 1618 · Displayed: 54 (3.3%) · Dropped: 0 (0.0%)
Profile: Default


dns.qry.type==1 && dns.qry.name==www.xjtu.edu.cn
No. Time Source Destination Protocol Length Source Port Destination Port
124 2021-05-17… 10.164.247.204 211.137.130.3 DNS 75 63973 53
125 2021-05-17… 211.137.130.3 10.164.247.204 DNS 91 53 63973
Frame 124: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{B02709AB-530C-4C1D-AB6C
Ethernet II, Src: HonHaiPr_ed:dc:b5 (d4:6a:6a:ed:dc:b5), Dst: Hangzhou_b4:e0:01 (38:97:d6:b4:e0:01)
Internet Protocol Version 4, Src: 10.164.247.204, Dst: 211.137.130.3
User Datagram Protocol, Src Port: 63973, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x0006
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.xjtu.edu.cn: type A class IN
Name: www.xjtu.edu.cn
[Name Length: 15]
[Label Count: 4]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 125]


Filter:
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1 0.000000000 172.16.196.166 8.8.8.8 DNS 86 Standard query 0x0e9d A www.pacif
2 0.054269000 8.8.8.8 172.16.196.166 DNS 102 Standard query response 0x0e9d A
Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
Ethernet II, Src: Vmware_f0:b5:c7 (00:50:56:f0:b5:c7), Dst: Vmware_98:ee:a9 (00:0c:29:98:ee:a9)
Internet Protocol Version 4, Src: 8.8.8.8 (8.8.8.8), Dst: 172.16.196.166 (172.16.196.166)
User Datagram Protocol, Src Port: domain (53), Dst Port: 34417 (34417)
Domain Name System (response)
[Request In: 1]
[Time: 0.054269000 seconds]
Transaction ID: 0x0e9d
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 1
Queries
www.pacific.edu: type A, class IN
Answers
www.pacific.edu: type A, class IN, addr 138.9.110.12
Additional records
0000 00 0c 29 98 ee a9 00 50 56 f0 b5 c7 08 00 45 00 ..)....P V.....E.
0010 00 58 25 8d 00 00 80 11 94 41 08 08 08 08 ac 10 .X%..... .A......
0020 c4 a6 00 35 86 71 00 44 01 91 0e 9d 81 80 00 01 ...5.q.D ....
0030 00 01 00 00 00 01 03 77 77 77 07 70 61 63 69 66 ....w ww.pacif
0040 69 63 03 65 64 75 00 00 01 00 01 c0 0c 00 01 00 ic.edu.. ....
0050 01 00 00 00 1b 00 04 8a 09 6e 0c 00 00 29 02 00 .... .n...)..
0060 00 00 00 00 00 00 ......
Frame (frame), 102 bytes
Packe...
Profile: Default



Filter:

dns

You can see:

- Websites visited
- Domain lookups
- DNS servers

Watch for:

- Unknown domains
- Excessive DNS requests
- Suspicious country domains

Step 9: Look for Unencrypted Traffic

Filter:

http

If you see usernames or passwords sent in plain text, those services are insecure.

Prefer websites using **HTTPS** (encrypted with TLS).

Step 10: Check for Malware Indicators

Signs include:

- Thousands of repeated connections
- Continuous DNS requests
- Connections to unfamiliar countries
- Large outbound uploads
- Strange port numbers

Useful filters:

tcp.flags.syn==1

tcp.analysis.retransmission

dns

Step 11: View Protocol Statistics

Go to:

Statistics
→
Protocol Hierarchy

This report shows:

- HTTP
- HTTPS
- DNS
- TCP
- UDP
- IPv4
- IPv6

A high percentage of encrypted (TLS/HTTPS) traffic is generally a good sign.

Step 12: Find the Most Active Devices

Go to:

Statistics

→

Endpoints

This window shows:

- IP addresses
- MAC addresses
- Packets sent
- Bytes transferred

Look for devices transferring unusually large amounts of data.

Step 13: View Conversations

Select:

Statistics

→

Conversations

You'll see:

- Which devices are communicating
- Data transferred
- Ports used
- Protocols

This helps identify devices making unexpected external connections.

Step 14: Secure Your Home Network

After analyzing your traffic:

Enable WPA3 (or WPA2 if WPA3 is unavailable)

Use strong Wi-Fi encryption.

Disable WPS

WPS can be vulnerable to brute-force attacks.

Update Router Firmware

Install security updates regularly.

Use Strong Passwords

Choose long, unique passwords for:

- Router administration
- Wi-Fi network
- Connected devices

Enable Automatic Updates

Keep operating systems and applications current.

Remove Unknown Devices

Disconnect and investigate unfamiliar devices connected to your network.

Use a Firewall

Ensure your router's firewall is enabled.

Enable DNS Filtering (Optional)

Consider family-safe or security-focused DNS providers to block known malicious domains.

Practice Exercise

1. Start a packet capture.
2. Visit five websites.
3. Stop the capture.
4. Filter for:

dns

5. Identify each website lookup.
6. Filter:

tls

7. Confirm that most browsing traffic is encrypted.
8. Open **Statistics** → **Endpoints** and identify your devices.

9. Save the capture.

Common Wireshark Filters

Purpose	Filter
HTTP	`http`
HTTPS/TLS	`tls`
DNS	`dns`
TCP	`tcp`
UDP	`udp`
ICMP	`icmp`
ARP	`arp`
DHCP	`bootp`
IPv4	`ip`
IPv6	`ipv6`
One IP Address	`ip.addr == 192.168.1.10`
One TCP Port	`tcp.port == 443`
One UDP Port	`udp.port == 53`

Troubleshooting

Problem	Solution
No packets captured	Verify you selected the correct interface.

No web traffic visible	Ensure you're capturing on the active network adapter.
Interface missing	Reinstall or repair Npcap.
Capture too large	Stop the capture sooner or apply capture filters.
Only encrypted traffic appears	This is normal on modern websites using HTTPS.

Best Practices

- Capture only traffic from networks you own or are authorized to analyze.
- Avoid capturing sensitive information longer than necessary.
- Save capture files securely and delete them when no longer needed.
- Keep Wireshark updated to benefit from the latest protocol support and security fixes.

Summary

Wireshark is a powerful tool for understanding and improving the security of your home network. By learning to capture packets, apply filters, inspect protocols, and review endpoint and conversation statistics, you can identify misconfigurations, spot unusual activity, and verify that most of your network traffic is encrypted.

With regular monitoring and good security practices—such as using WPA3, disabling WPS, updating router firmware, and keeping your devices patched—you can significantly reduce the risk of unauthorized access and network-based attacks.