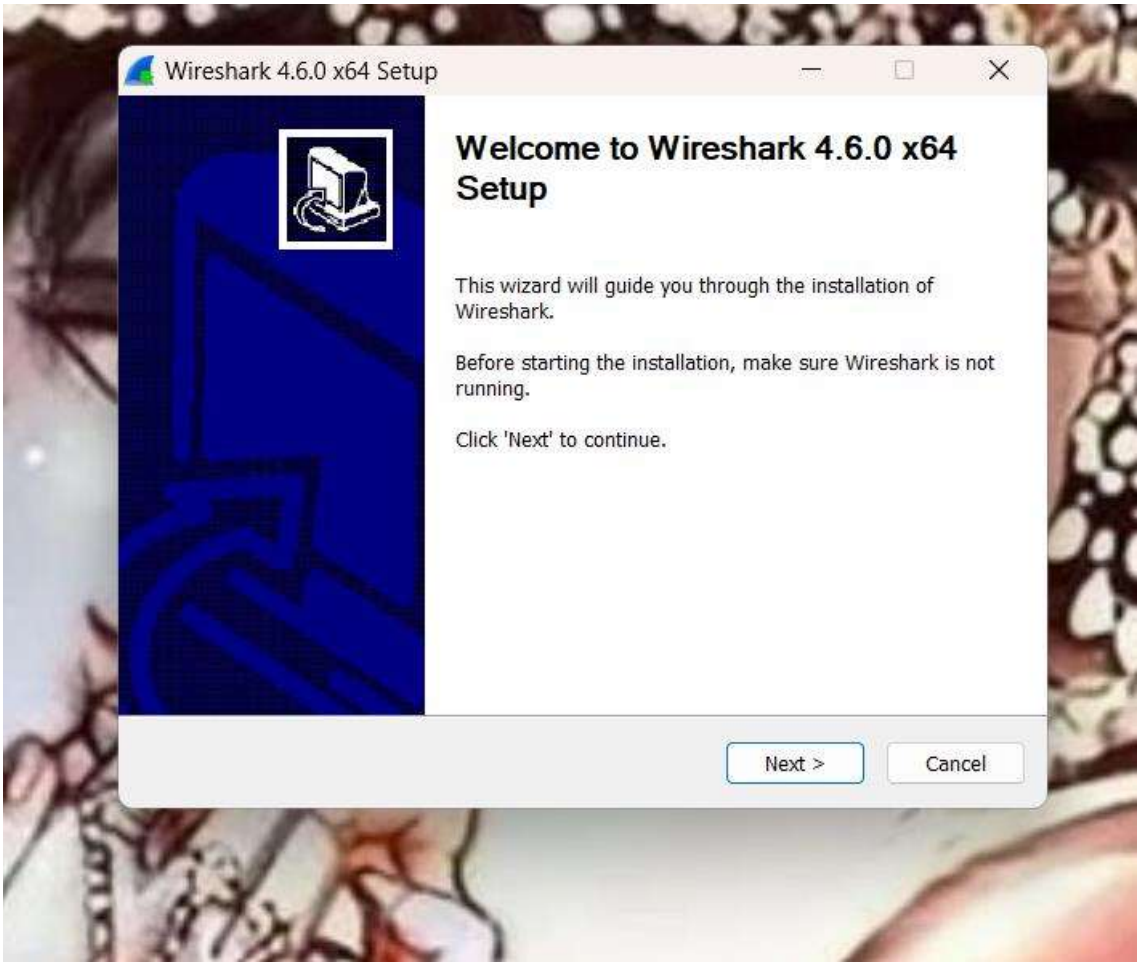
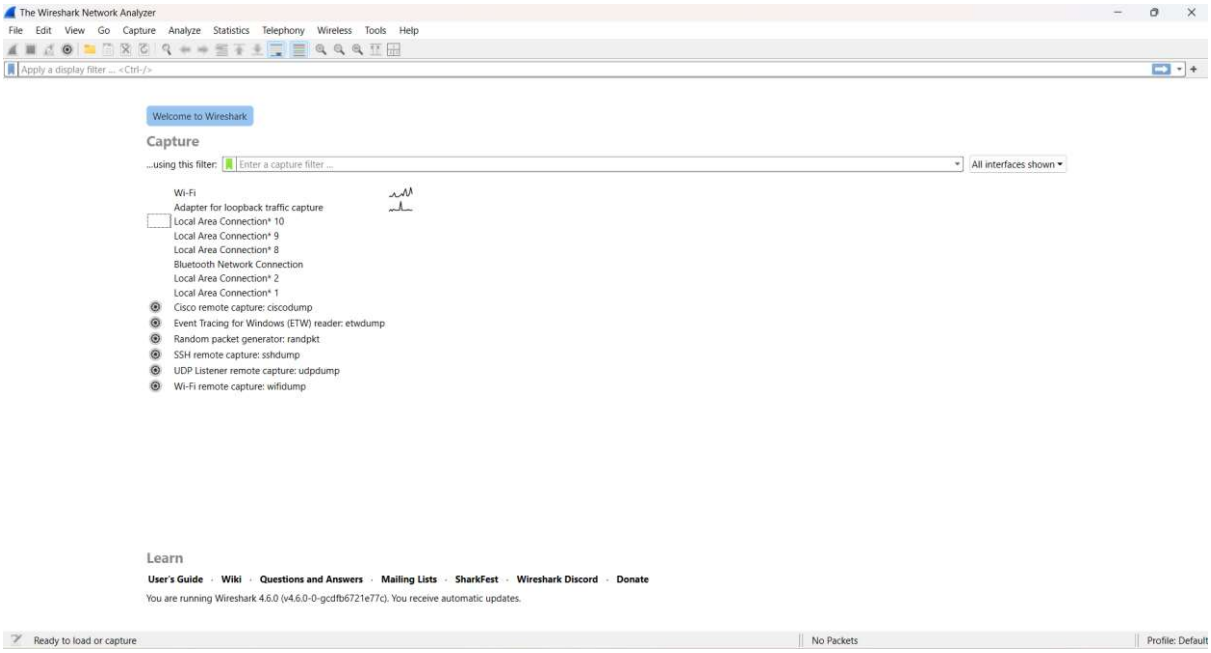
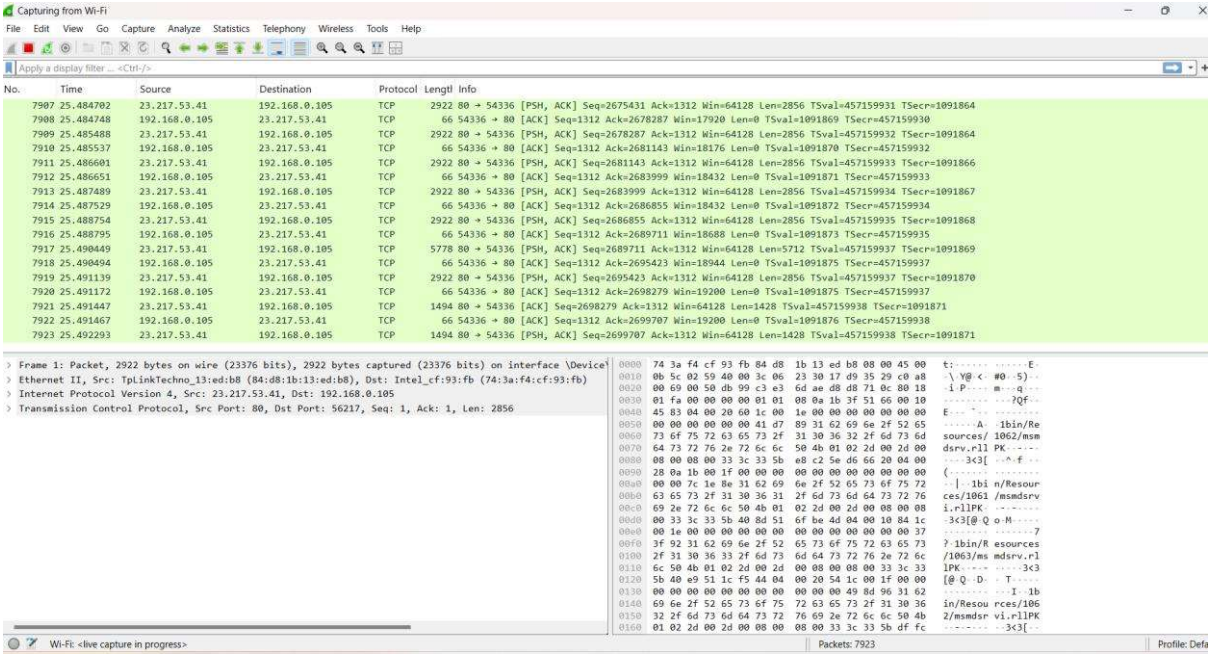

Official certification from the Wireshark Foundation is available! Learn about becoming a Wireshark Certified Analyst.
WIRESHARK
Download
Learn
Resources
Tools
Community
Develop
Members
Certifications
Donate
Download Wireshark: Your Network Analysis Tool
Choose your platform and start analyzing network traffic today.
Download Wireshark


Wireshark 4.6.0 x64 Setup
Welcome to Wireshark 4.6.0 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

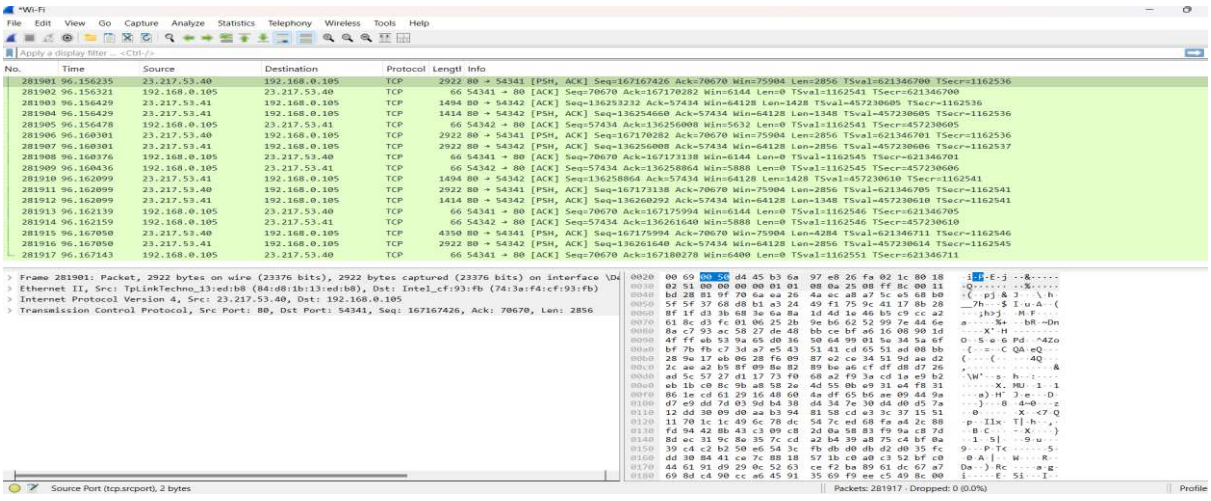

Wireshark

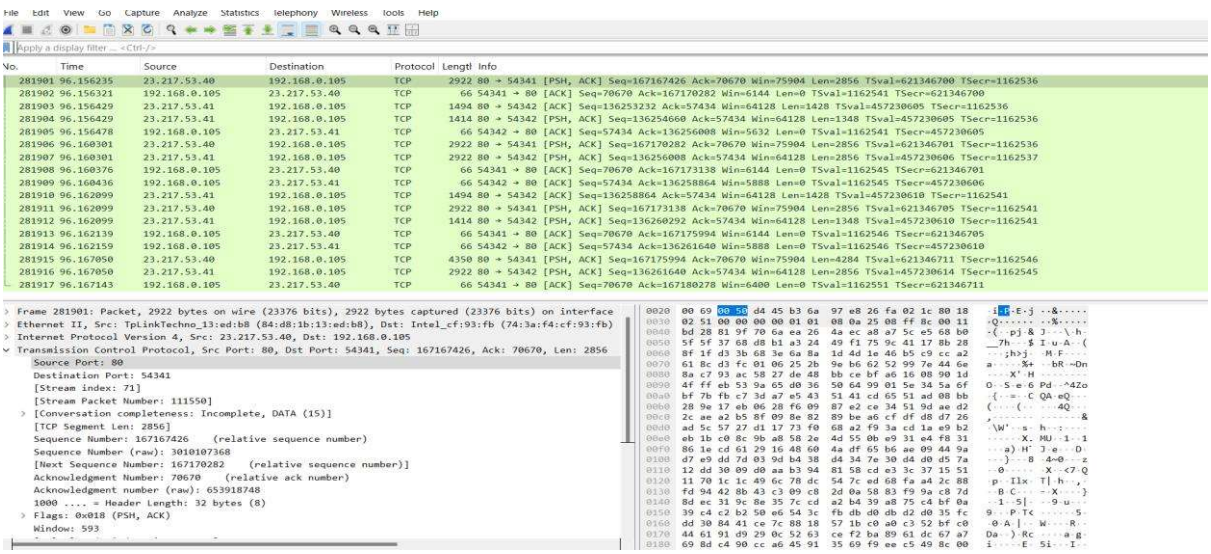


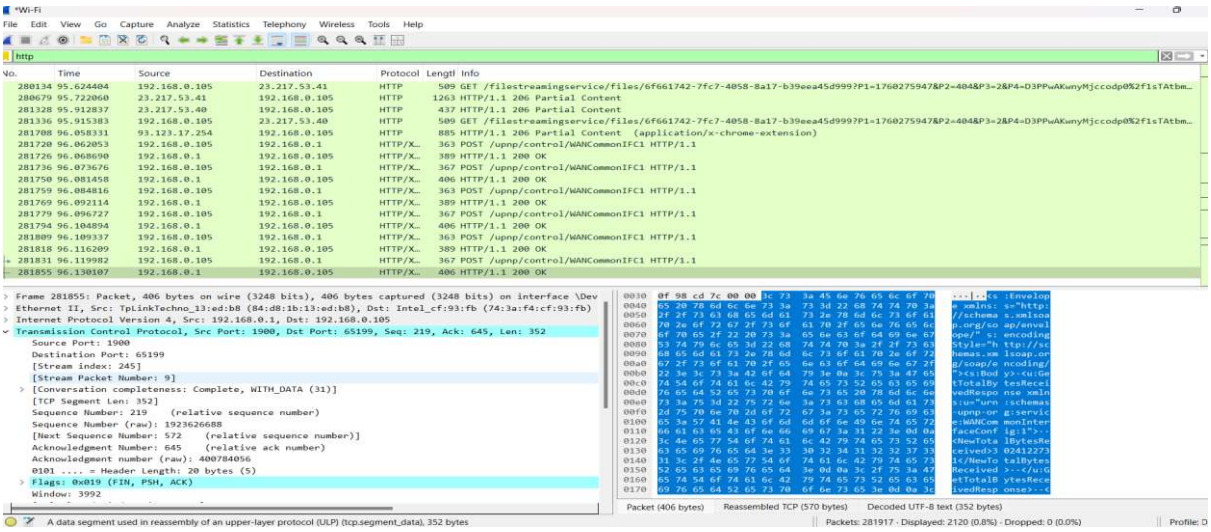
Capturing Traffic

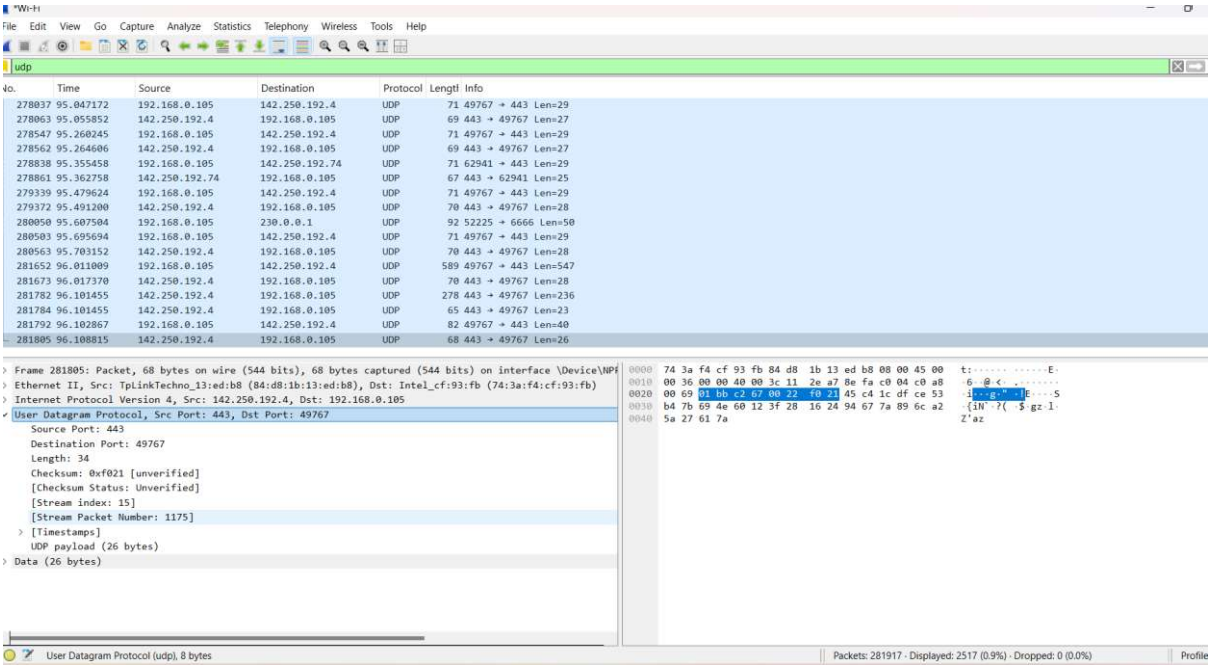


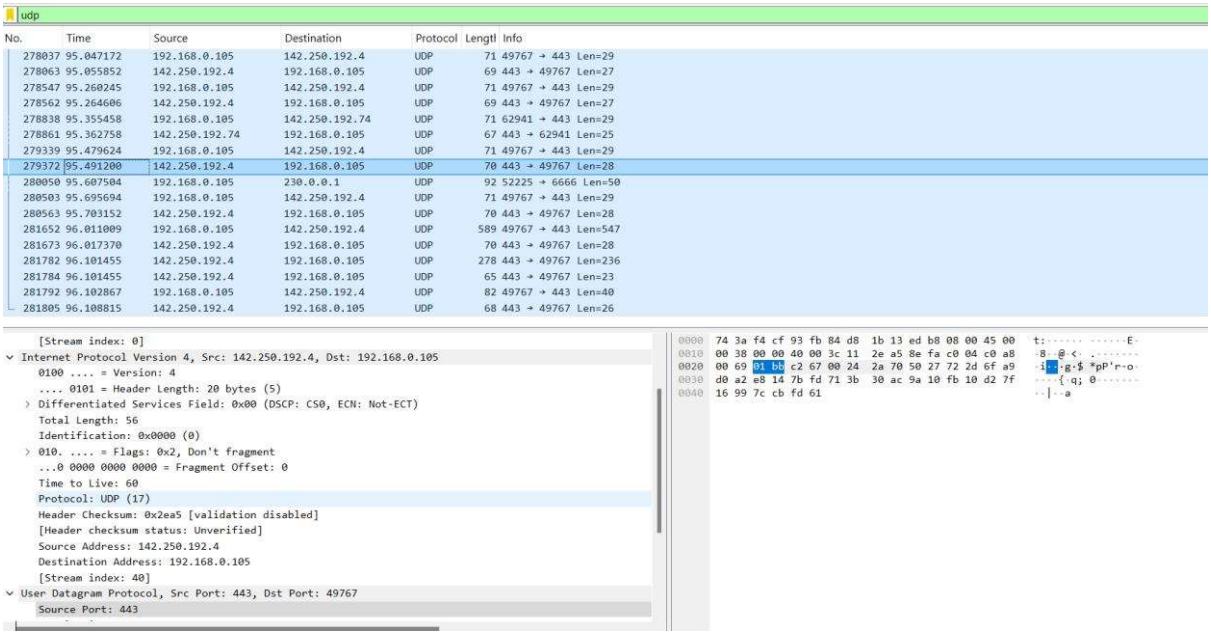
Analyzing and Filtering Packets

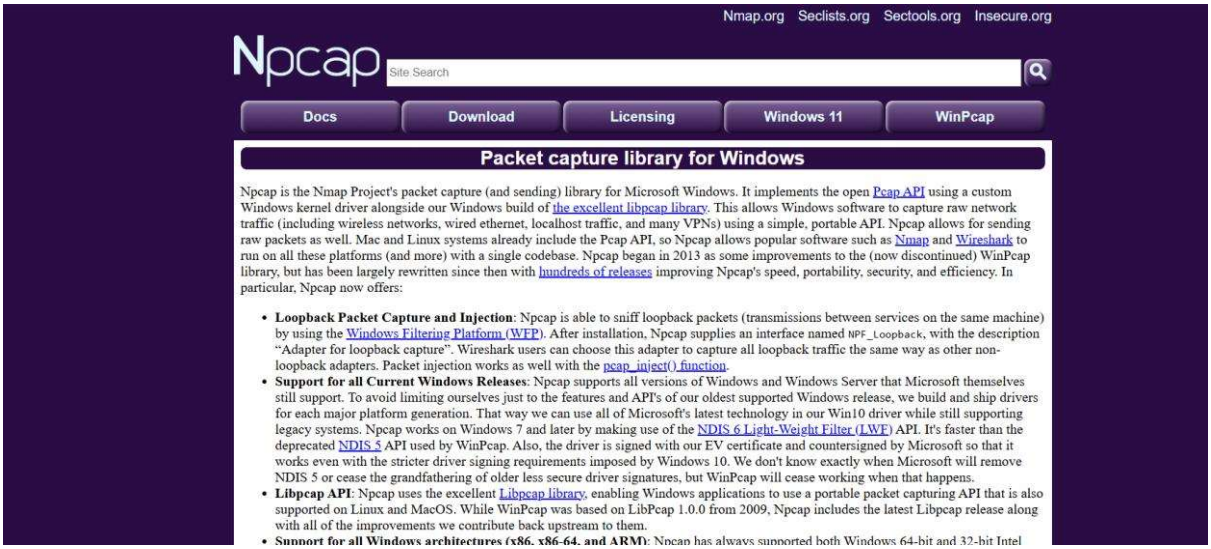

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
281901 96.156235 23.217.53.40 192.168.0.105 TCP 2922 80 → 54341 [PSH, ACK] Seq=167167426 Ack=70670 Win=75904 Len=2856 TSval=621346700 TSecr=1162536
281902 96.156321 192.168.0.105 23.217.53.40 TCP 66 54341 → 80 [ACK] Seq=70670 Ack=167170282 Win=6144 Len=0 TSval=1162541 TSecr=621346700
281903 96.156429 23.217.53.41 192.168.0.105 TCP 1494 80 → 54342 [ACK] Seq=136253232 Ack=57434 Win=64128 Len=1428 TSval=457230605 TSecr=1162536
281904 96.156429 23.217.53.41 192.168.0.105 TCP 1414 80 → 54342 [PSH, ACK] Seq=136254660 Ack=57434 Win=64128 Len=1348 TSval=457230605 TSecr=1162536
281905 96.156478 192.168.0.105 23.217.53.41 TCP 66 54342 → 80 [ACK] Seq=57434 Ack=136256008 Win=5632 Len=0 TSval=1162541 TSecr=457230605
281906 96.160301 23.217.53.40 192.168.0.105 TCP 2922 80 → 54341 [PSH, ACK] Seq=167170282 Ack=70670 Win=75904 Len=2856 TSval=621346701 TSecr=1162536
281907 96.160301 23.217.53.41 192.168.0.105 TCP 2922 80 → 54342 [PSH, ACK] Seq=136256008 Ack=57434 Win=64128 Len=2856 TSval=457230606 TSecr=1162537
281908 96.160376 192.168.0.105 23.217.53.40 TCP 66 54341 → 80 [ACK] Seq=70670 Ack=167173138 Win=6144 Len=0 TSval=1162545 TSecr=621346701
281909 96.160436 192.168.0.105 23.217.53.41 TCP 66 54342 → 80 [ACK] Seq=57434 Ack=136258864 Win=5888 Len=0 TSval=1162545 TSecr=457230606
281910 96.162099 23.217.53.41 192.168.0.105 TCP 1494 80 → 54342 [ACK] Seq=136258864 Ack=57434 Win=64128 Len=1428 TSval=457230610 TSecr=1162541
281911 96.162099 23.217.53.40 192.168.0.105 TCP 2922 80 → 54341 [PSH, ACK] Seq=167173138 Ack=70670 Win=75904 Len=2856 TSval=621346705 TSecr=1162541
281912 96.162099 23.217.53.41 192.168.0.105 TCP 1414 80 → 54342 [PSH, ACK] Seq=136260292 Ack=57434 Win=64128 Len=1348 TSval=457230610 TSecr=1162541
281913 96.162139 192.168.0.105 23.217.53.40 TCP 66 54341 → 80 [ACK] Seq=70670 Ack=167175994 Win=6144 Len=0 TSval=1162546 TSecr=621346705
281914 96.162159 192.168.0.105 23.217.53.41 TCP 66 54342 → 80 [ACK] Seq=57434 Ack=136261640 Win=5888 Len=0 TSval=1162546 TSecr=457230610
281915 96.167050 23.217.53.40 192.168.0.105 TCP 4350 80 → 54341 [PSH, ACK] Seq=167175994 Ack=70670 Win=75904 Len=4284 TSval=621346711 TSecr=1162546
281916 96.167050 23.217.53.41 192.168.0.105 TCP 2922 80 → 54342 [PSH, ACK] Seq=136261640 Ack=57434 Win=64128 Len=2856 TSval=457230614 TSecr=1162545
281917 96.167143 192.168.0.105 23.217.53.40 TCP 66 54341 → 80 [ACK] Seq=70670 Ack=167180278 Win=6400 Len=0 TSval=1162551 TSecr=621346711
Frame 281901: Packet, 2922 bytes on wire (23376 bits), 2922 bytes captured (23376 bits) on interface \D
Ethernet II, Src: TpLinkTechno_13:ed:b8 (84:d8:1b:13:ed:b8), Dst: Intel_cf:93:fb (74:3a:f4:cf:93:fb)
Internet Protocol Version 4, Src: 23.217.53.40, Dst: 192.168.0.105
Transmission Control Protocol, Src Port: 80, Dst Port: 54341, Seq: 167167426, Ack: 70670, Len: 2856
Source Port (tcp.srcport), 2 bytes
Packets: 281917 · Dropped: 0 (0.0%)
Profile

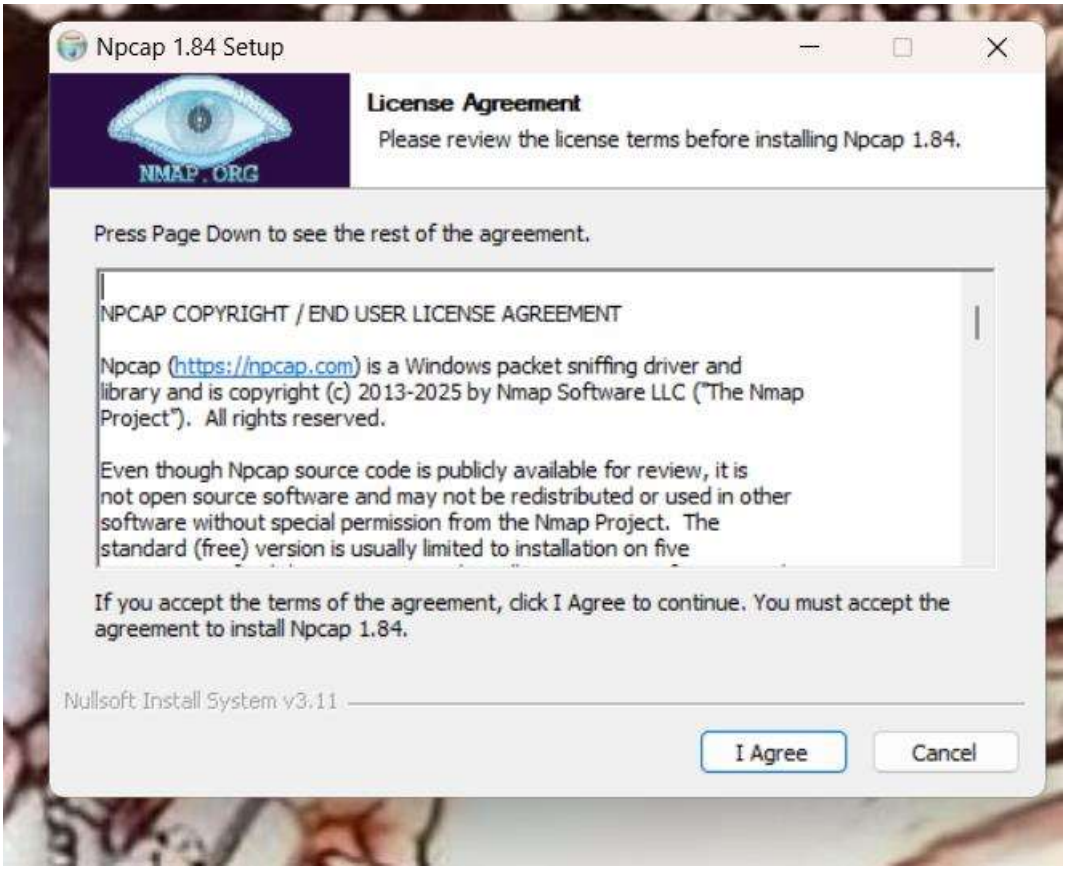

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
281901 96.156235 23.217.53.40 192.168.0.105 TCP 2922 80 → 54341 [PSH, ACK] Seq=167167426 Ack=70670 Win=75904 Len=2856 TSval=621346700 TSecr=1162536
281902 96.156321 192.168.0.105 23.217.53.40 TCP 66 54341 → 80 [ACK] Seq=70670 Ack=167170282 Win=6144 Len=0 TSval=1162541 TSecr=621346700
281903 96.156429 23.217.53.41 192.168.0.105 TCP 1494 80 → 54342 [ACK] Seq=136253232 Ack=57434 Win=64128 Len=1428 TSval=457230605 TSecr=1162536
281904 96.156429 23.217.53.41 192.168.0.105 TCP 1414 80 → 54342 [PSH, ACK] Seq=136254660 Ack=57434 Win=64128 Len=1348 TSval=457230605 TSecr=1162536
281905 96.156478 192.168.0.105 23.217.53.41 TCP 66 54342 → 80 [ACK] Seq=57434 Ack=136256008 Win=5632 Len=0 TSval=1162541 TSecr=457230605
281906 96.160301 23.217.53.40 192.168.0.105 TCP 2922 80 → 54341 [PSH, ACK] Seq=167170282 Ack=70670 Win=75904 Len=2856 TSval=621346701 TSecr=1162536
281907 96.160301 23.217.53.41 192.168.0.105 TCP 2922 80 → 54342 [PSH, ACK] Seq=136256008 Ack=57434 Win=64128 Len=2856 TSval=457230606 TSecr=1162537
281908 96.160376 192.168.0.105 23.217.53.40 TCP 66 54341 → 80 [ACK] Seq=70670 Ack=167173138 Win=6144 Len=0 TSval=1162545 TSecr=621346701
281909 96.160436 192.168.0.105 23.217.53.41 TCP 66 54342 → 80 [ACK] Seq=57434 Ack=136258864 Win=5888 Len=0 TSval=1162545 TSecr=457230606
281910 96.162099 23.217.53.41 192.168.0.105 TCP 1494 80 → 54342 [ACK] Seq=136258864 Ack=57434 Win=64128 Len=1428 TSval=457230610 TSecr=1162541
281911 96.162099 23.217.53.40 192.168.0.105 TCP 2922 80 → 54341 [PSH, ACK] Seq=167173138 Ack=70670 Win=75904 Len=2856 TSval=621346705 TSecr=1162541
281912 96.162099 23.217.53.41 192.168.0.105 TCP 1414 80 → 54342 [PSH, ACK] Seq=136260292 Ack=57434 Win=64128 Len=1348 TSval=457230610 TSecr=1162541
281913 96.162139 192.168.0.105 23.217.53.40 TCP 66 54341 → 80 [ACK] Seq=70670 Ack=167175994 Win=6144 Len=0 TSval=1162546 TSecr=621346705
281914 96.162159 192.168.0.105 23.217.53.41 TCP 66 54342 → 80 [ACK] Seq=57434 Ack=136261640 Win=5888 Len=0 TSval=1162546 TSecr=457230610
281915 96.167050 23.217.53.40 192.168.0.105 TCP 4350 80 → 54341 [PSH, ACK] Seq=167175994 Ack=70670 Win=75904 Len=4284 TSval=621346711 TSecr=1162546
281916 96.167050 23.217.53.41 192.168.0.105 TCP 2922 80 → 54342 [PSH, ACK] Seq=136261640 Ack=57434 Win=64128 Len=2856 TSval=457230614 TSecr=1162545
281917 96.167143 192.168.0.105 23.217.53.40 TCP 66 54341 → 80 [ACK] Seq=70670 Ack=167180278 Win=6400 Len=0 TSval=1162551 TSecr=621346711
Frame 281901: Packet, 2922 bytes on wire (23376 bits), 2922 bytes captured (23376 bits) on interface
Ethernet II, Src: TpLinkTechno_13:ed:b8 (84:d8:1b:13:ed:b8), Dst: Intel_cf:93:fb (74:3a:f4:cf:93:fb)
Internet Protocol Version 4, Src: 23.217.53.40, Dst: 192.168.0.105
Transmission Control Protocol, Src Port: 80, Dst Port: 54341, Seq: 167167426, Ack: 70670, Len: 2856
Source Port: 80
Destination Port: 54341
[Stream index: 71]
[Stream Packet Number: 111550]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 2856]
Sequence Number: 167167426 (relative sequence number)
Sequence Number (raw): 3010107368
[Next Sequence Number: 167170282 (relative sequence number)]
Acknowledgment Number: 70670 (relative ack number)
Acknowledgment number (raw): 653918748
1000 .... = Header Length: 32 bytes (8)
Flags: 0x018 (PSH, ACK)
Window: 593

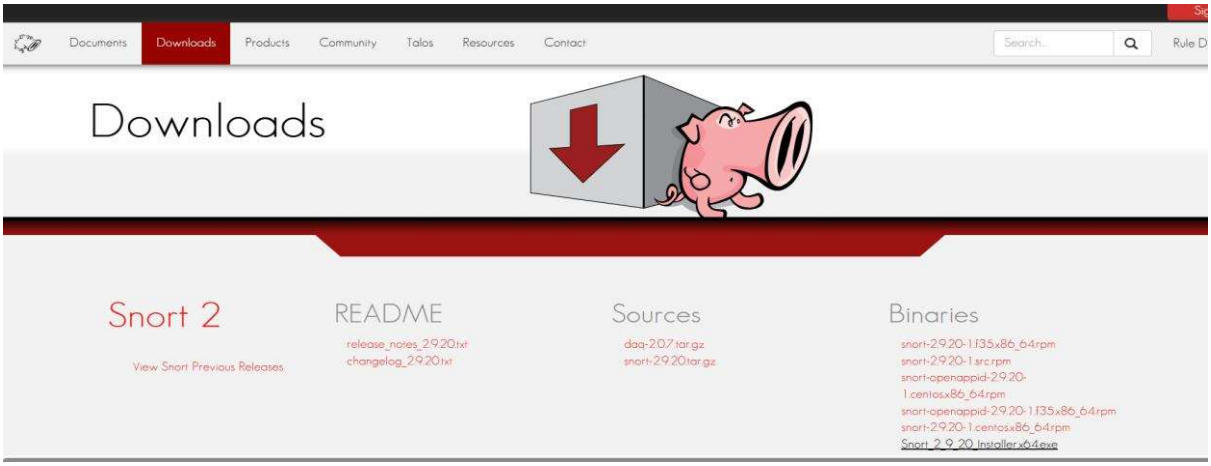

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
280134 95.624404 192.168.0.105 23.217.53.41 HTTP 509 GET /filestreamingservice/files/6f661742-7fc7-4058-8a17-b39eea45d999?P1=1760275947&P2=404&P3=2&P4=D3PPwAKwnyMjccodp0%2f1sTAtbm...
280679 95.722060 23.217.53.41 192.168.0.105 HTTP 1263 HTTP/1.1 206 Partial Content
281328 95.912837 23.217.53.40 192.168.0.105 HTTP 437 HTTP/1.1 206 Partial Content
281336 95.915383 192.168.0.105 23.217.53.40 HTTP 509 GET /filestreamingservice/files/6f661742-7fc7-4058-8a17-b39eea45d999?P1=1760275947&P2=404&P3=2&P4=D3PPwAKwnyMjccodp0%2f1sTAtbm...
281708 96.058331 93.123.17.254 192.168.0.105 HTTP 885 HTTP/1.1 206 Partial Content (application/x-chrome-extension)
281720 96.062053 192.168.0.105 192.168.0.1 HTTP/X... 363 POST /upnp/control/WANCommonIFC1 HTTP/1.1
281726 96.068690 192.168.0.1 192.168.0.105 HTTP/X... 389 HTTP/1.1 200 OK
281736 96.073676 192.168.0.105 192.168.0.1 HTTP/X... 367 POST /upnp/control/WANCommonIFC1 HTTP/1.1
281750 96.081458 192.168.0.1 192.168.0.105 HTTP/X... 406 HTTP/1.1 200 OK
281759 96.084816 192.168.0.105 192.168.0.1 HTTP/X... 363 POST /upnp/control/WANCommonIFC1 HTTP/1.1
281769 96.092114 192.168.0.1 192.168.0.105 HTTP/X... 389 HTTP/1.1 200 OK
281779 96.096727 192.168.0.105 192.168.0.1 HTTP/X... 367 POST /upnp/control/WANCommonIFC1 HTTP/1.1
281794 96.104894 192.168.0.1 192.168.0.105 HTTP/X... 406 HTTP/1.1 200 OK
281809 96.109337 192.168.0.105 192.168.0.1 HTTP/X... 363 POST /upnp/control/WANCommonIFC1 HTTP/1.1
281818 96.116209 192.168.0.1 192.168.0.105 HTTP/X... 389 HTTP/1.1 200 OK
281831 96.119982 192.168.0.105 192.168.0.1 HTTP/X... 367 POST /upnp/control/WANCommonIFC1 HTTP/1.1
281855 96.130107 192.168.0.1 192.168.0.105 HTTP/X... 406 HTTP/1.1 200 OK
Frame 281855: Packet, 406 bytes on wire (3248 bits), 406 bytes captured (3248 bits) on interface \Dev
Ethernet II, Src: TpLinkTechno_13:ed:b8 (84:d8:1b:13:ed:b8), Dst: Intel_cf:93:fb (74:3a:f4:cf:93:fb)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.105
Transmission Control Protocol, Src Port: 1900, Dst Port: 65199, Seq: 219, Ack: 645, Len: 352
Source Port: 1900
Destination Port: 65199
[Stream index: 245]
[Stream Packet Number: 9]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 352]
Sequence Number: 219 (relative sequence number)
Sequence Number (raw): 1923626688
[Next Sequence Number: 572 (relative sequence number)]
Acknowledgment Number: 645 (relative ack number)
Acknowledgment number (raw): 400784056
0101 .... = Header Length: 20 bytes (5)
Flags: 0x019 (FIN, PSH, ACK)
Window: 3992
A data segment used in reassembly of an upper-layer protocol (ULP) (tcp.segment_data), 352 bytes
Packet (406 bytes)
Reassembled TCP (570 bytes)
Decoded UTF-8 text (352 bytes)
Packets: 281917 · Displayed: 2120 (0.8%) · Dropped: 0 (0.0%)
Profile: D

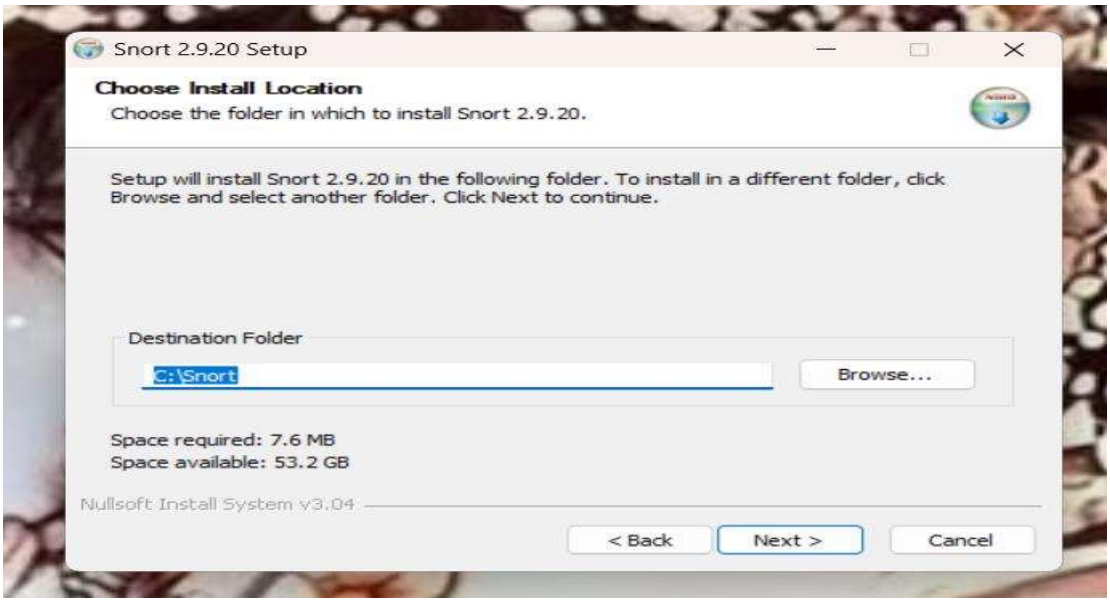

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
No. Time Source Destination Protocol Length Info
278037 95.047172 192.168.0.105 142.250.192.4 UDP 71 49767 → 443 Len=29
278063 95.055852 142.250.192.4 192.168.0.105 UDP 69 443 → 49767 Len=27
278547 95.260245 192.168.0.105 142.250.192.4 UDP 71 49767 → 443 Len=29
278562 95.264606 142.250.192.4 192.168.0.105 UDP 69 443 → 49767 Len=27
278838 95.355458 192.168.0.105 142.250.192.74 UDP 71 62941 → 443 Len=29
278861 95.362758 142.250.192.74 192.168.0.105 UDP 67 443 → 62941 Len=25
279339 95.479624 192.168.0.105 142.250.192.4 UDP 71 49767 → 443 Len=29
279372 95.491200 142.250.192.4 192.168.0.105 UDP 70 443 → 49767 Len=28
280050 95.607504 192.168.0.105 230.0.0.1 UDP 92 52225 → 6666 Len=50
280503 95.695694 192.168.0.105 142.250.192.4 UDP 71 49767 → 443 Len=29
280563 95.703152 142.250.192.4 192.168.0.105 UDP 70 443 → 49767 Len=28
281652 96.011009 192.168.0.105 142.250.192.4 UDP 589 49767 → 443 Len=547
281673 96.017370 142.250.192.4 192.168.0.105 UDP 70 443 → 49767 Len=28
281782 96.101455 142.250.192.4 192.168.0.105 UDP 278 443 → 49767 Len=236
281784 96.101455 142.250.192.4 192.168.0.105 UDP 65 443 → 49767 Len=23
281792 96.102867 192.168.0.105 142.250.192.4 UDP 82 49767 → 443 Len=40
281805 96.108815 142.250.192.4 192.168.0.105 UDP 68 443 → 49767 Len=26
Frame 281805: Packet, 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface \Device\NPF
Ethernet II, Src: TpLinkTechno_13:ed:b8 (84:d8:1b:13:ed:b8), Dst: Intel_cf:93:fb (74:3a:f4:cf:93:fb)
Internet Protocol Version 4, Src: 142.250.192.4, Dst: 192.168.0.105
User Datagram Protocol, Src Port: 443, Dst Port: 49767
Source Port: 443
Destination Port: 49767
Length: 34
Checksum: 0xf021 [unverified]
[Checksum Status: Unverified]
[Stream index: 15]
[Stream Packet Number: 1175]
[Timestamps]
UDP payload (26 bytes)
Data (26 bytes)
0000 74 3a f4 cf 93 fb 84 d8 1b 13 ed b8 08 00 45 00
0010 00 36 00 00 40 00 3c 11 2e a7 8e fa c0 04 c0 a8
0020 00 69 01 bb c2 67 00 22 f0 21 45 c4 1c df ce 53
0030 b4 7b 69 4e 60 12 3f 28 16 24 94 67 7a 89 6c a2
0040 5a 27 61 7a
User Datagram Protocol (udp), 8 bytes
Packets: 281917 · Displayed: 2517 (0.9%) · Dropped: 0 (0.0%)
Profile

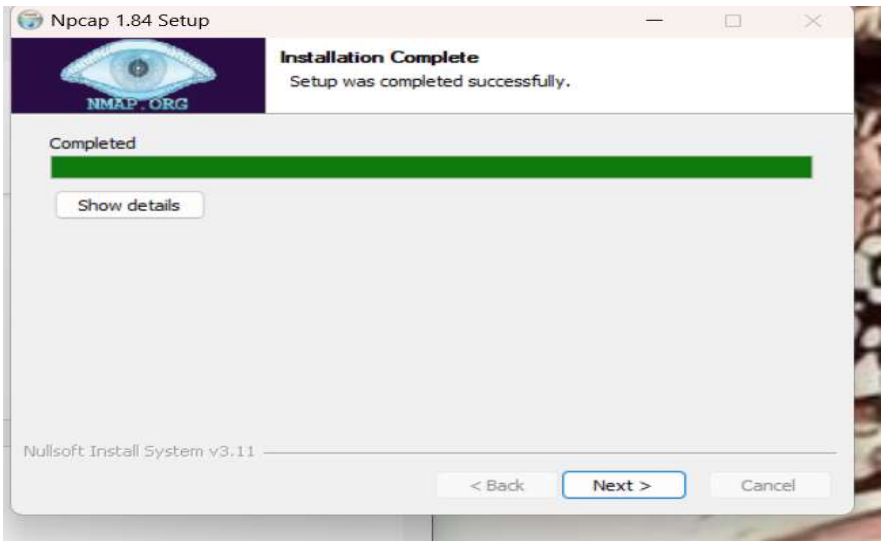

udp
No. Time Source Destination Protocol Length Info
278037 95.047172 192.168.0.105 142.250.192.4 UDP 71 49767 → 443 Len=29
278063 95.055852 142.250.192.4 192.168.0.105 UDP 69 443 → 49767 Len=27
278547 95.260245 192.168.0.105 142.250.192.4 UDP 71 49767 → 443 Len=29
278562 95.264606 142.250.192.4 192.168.0.105 UDP 69 443 → 49767 Len=27
278838 95.355458 192.168.0.105 142.250.192.74 UDP 71 62941 → 443 Len=29
278861 95.362758 142.250.192.74 192.168.0.105 UDP 67 443 → 62941 Len=25
279339 95.479624 192.168.0.105 142.250.192.4 UDP 71 49767 → 443 Len=29
279372 95.491200 142.250.192.4 192.168.0.105 UDP 70 443 → 49767 Len=28
280050 95.607504 192.168.0.105 230.0.0.1 UDP 92 52225 → 6666 Len=50
280503 95.695694 192.168.0.105 142.250.192.4 UDP 71 49767 → 443 Len=29
280563 95.703152 142.250.192.4 192.168.0.105 UDP 70 443 → 49767 Len=28
281652 96.011009 192.168.0.105 142.250.192.4 UDP 589 49767 → 443 Len=547
281673 96.017370 142.250.192.4 192.168.0.105 UDP 70 443 → 49767 Len=28
281782 96.101455 142.250.192.4 192.168.0.105 UDP 278 443 → 49767 Len=236
281784 96.101455 142.250.192.4 192.168.0.105 UDP 65 443 → 49767 Len=23
281792 96.102867 192.168.0.105 142.250.192.4 UDP 82 49767 → 443 Len=40
281805 96.108815 142.250.192.4 192.168.0.105 UDP 68 443 → 49767 Len=26
[Stream index: 0]
Internet Protocol Version 4, Src: 142.250.192.4, Dst: 192.168.0.105
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 56
Identification: 0x0000 (0)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 60
Protocol: UDP (17)
Header Checksum: 0x2ea5 [validation disabled]
[Header checksum status: Unverified]
Source Address: 142.250.192.4
Destination Address: 192.168.0.105
[Stream index: 40]
User Datagram Protocol, Src Port: 443, Dst Port: 49767
Source Port: 443
0000 74 3a f4 cf 93 fb 84 d8 1b 13 ed b8 08 00 45 00
0010 00 38 00 00 40 00 3c 11 2e a5 8e fa c0 04 c0 a8
0020 00 69 01 bb c2 67 00 24 2a 70 50 27 72 2d 6f a9
0030 d0 a2 e8 14 7b fd 71 3b 30 ac 9a 10 fb 10 d2 7f
0040 16 99 7c cb fd 61

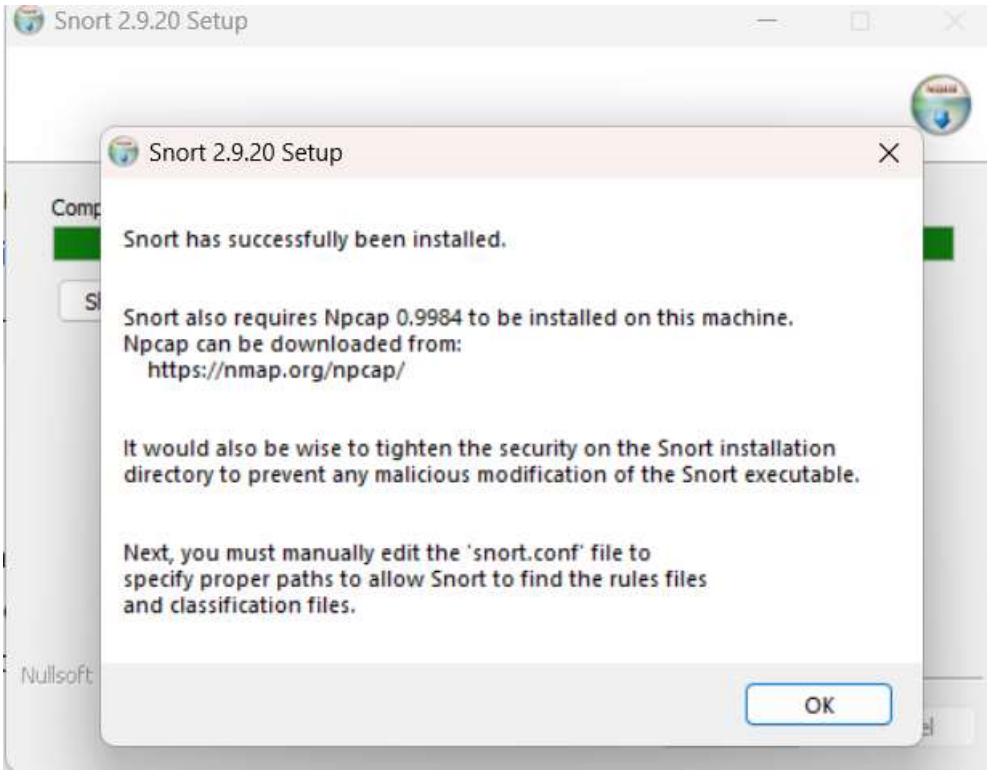

Nmap.org Seclists.org Sectools.org Insecure.org
Npcap
Site Search
Docs
Download
Licensing
Windows 11
WinPcap
Packet capture library for Windows
Npcap is the Nmap Project's packet capture (and sending) library for Microsoft Windows. It implements the open Pcap API using a custom Windows kernel driver alongside our Windows build of the excellent libpcap library. This allows Windows software to capture raw network traffic (including wireless networks, wired ethernet, localhost traffic, and many VPNs) using a simple, portable API. Npcap allows for sending raw packets as well. Mac and Linux systems already include the Pcap API, so Npcap allows popular software such as Nmap and Wireshark to run on all these platforms (and more) with a single codebase. Npcap began in 2013 as some improvements to the (now discontinued) WinPcap library, but has been largely rewritten since then with hundreds of releases improving Npcap's speed, portability, security, and efficiency. In particular, Npcap now offers:
Loopback Packet Capture and Injection: Npcap is able to sniff loopback packets (transmissions between services on the same machine) by using the Windows Filtering Platform (WFP). After installation, Npcap supplies an interface named NPF_Loopback, with the description "Adapter for loopback capture". Wireshark users can choose this adapter to capture all loopback traffic the same way as other non-loopback adapters. Packet injection works as well with the pcap_inject() function.
Support for all Current Windows Releases: Npcap supports all versions of Windows and Windows Server that Microsoft themselves still support. To avoid limiting ourselves just to the features and API's of our oldest supported Windows release, we build and ship drivers for each major platform generation. That way we can use all of Microsoft's latest technology in our Win10 driver while still supporting legacy systems. Npcap works on Windows 7 and later by making use of the NDIS 6 Light-Weight Filter (LWF) API. It's faster than the deprecated NDIS 5 API used by WinPcap. Also, the driver is signed with our EV certificate and countersigned by Microsoft so that it works even with the stricter driver signing requirements imposed by Windows 10. We don't know exactly when Microsoft will remove NDIS 5 or cease the grandfathering of older less secure driver signatures, but WinPcap will cease working when that happens.
Libpcap API: Npcap uses the excellent Libpcap library, enabling Windows applications to use a portable packet capturing API that is also supported on Linux and MacOS. While WinPcap was based on LibPcap 1.0.0 from 2009, Npcap includes the latest Libpcap release along with all of the improvements we contribute back upstream to them.
Support for all Windows architectures (x86, x86-64, and ARM): Npcap has always supported both Windows 64-bit and 32-bit Intel


Npcap 1.84 Setup
NMAP.ORG
License Agreement
Please review the license terms before installing Npcap 1.84.
Press Page Down to see the rest of the agreement.
NPCAP COPYRIGHT / END USER LICENSE AGREEMENT
Npcap (https://npcap.com) is a Windows packet sniffing driver and library and is copyright (c) 2013-2025 by Nmap Software LLC ("The Nmap Project"). All rights reserved.
Even though Npcap source code is publicly available for review, it is not open source software and may not be redistributed or used in other software without special permission from the Nmap Project. The standard (free) version is usually limited to installation on five
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Npcap 1.84.
Nullsoft Install System v3.11
I Agree
Cancel


Documents
Downloads
Products
Community
Talos
Resources
Contact
Search...
Rule D
Downloads
Snort 2
View Snort Previous Releases
README
release_notes_2.9.20.txt
changelog_2.9.20.txt
Sources
daq-2.0.7.tar.gz
snort-2.9.20.tar.gz
Binaries
snort-2.9.20-1.fc35.x86_64.rpm
snort-2.9.20-1.src.rpm
snort-openappid-2.9.20-1.centos.x86_64.rpm
snort-openappid-2.9.20-1.fc35.x86_64.rpm
snort-2.9.20-1.centos.x86_64.rpm
Snort_2_9_20_Installer.x64.exe


Snort 2.9.20 Setup
Choose Install Location
Choose the folder in which to install Snort 2.9.20.
Setup will install Snort 2.9.20 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.
Destination Folder
C:\Snort
Browse...
Space required: 7.6 MB
Space available: 53.2 GB
Nullsoft Install System v3.04
< Back
Next >
Cancel


Npcap 1.84 Setup
NMAP.ORG
Installation Complete
Setup was completed successfully.
Completed
Show details
Nullsoft Install System v3.11
< Back
Next >
Cancel


Snort 2.9.20 Setup
Snort 2.9.20 Setup
Snort has successfully been installed.
Snort also requires Npcap 0.9984 to be installed on this machine.
Npcap can be downloaded from:
https://nmap.org/npcap/
It would also be wise to tighten the security on the Snort installation directory to prevent any malicious modification of the Snort executable.
Next, you must manually edit the 'snort.conf' file to specify proper paths to allow Snort to find the rules files and classification files.
OK
Nullsoft