Lab# 02 Wireshark Lab: Installation and Basic Network Scan

🎯 Objective

Students will install Wireshark on their Windows computers, perform a basic network scan, and apply filters to analyze network traffic.

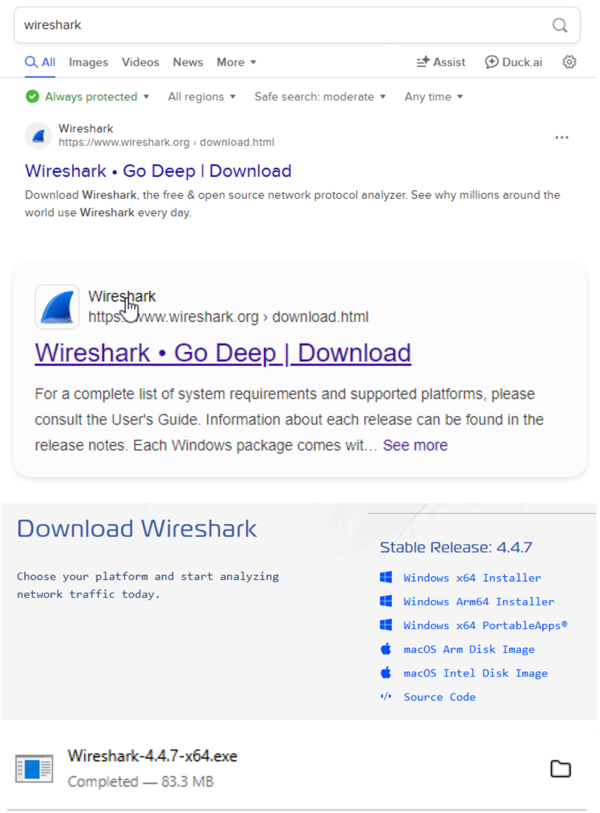
Step-by-Step Instructions / Summary

- Part 1: Install Wireshark on Windows
- Part 2: Perform a Basic Network Scan
- Part 3: Apply Filters in Wireshark
- Part 4: Advanced Filters
- Part 5: Capture and Export

Steps and screenshots for this lab:

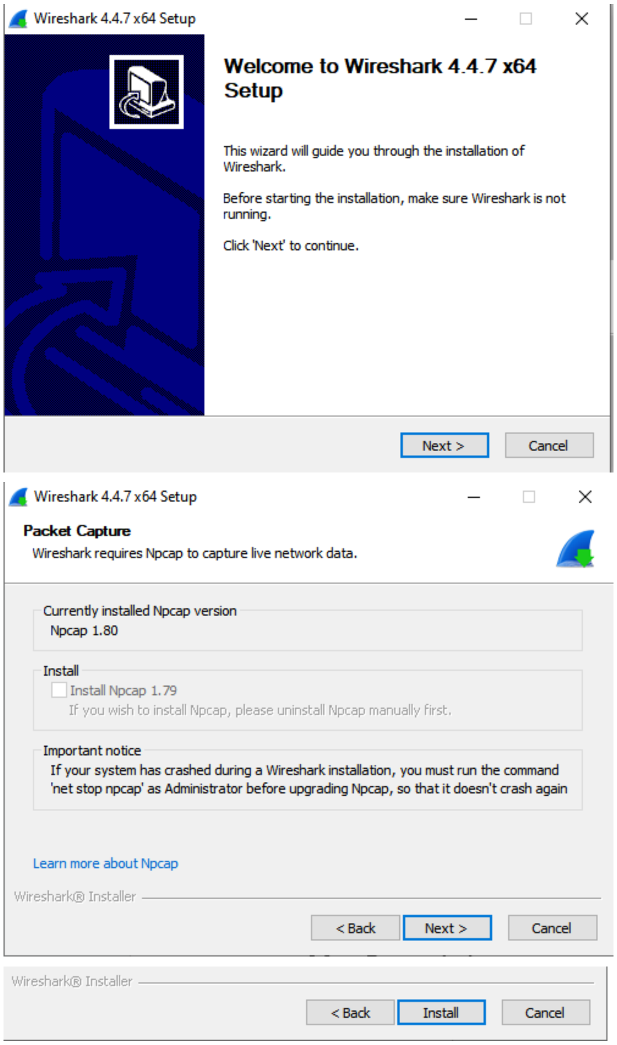
1. Install Wireshark on Windows

1.1. Download Wireshark

Going to the website to download Wireshark **Downloading the Windows Installer version**	 wireshark All Images Videos News More ▾ Assist Duck.ai Always protected ▾ All regions ▾ Safe search: moderate ▾ Any time ▾ Wireshark https://www.wireshark.org › download.html Wireshark • Go Deep | Download Download **Wireshark**, the free & open source network protocol analyzer. See why millions around the world use **Wireshark** every day. Wireshark https://www.wireshark.org › download.html Wireshark • Go Deep | Download For a complete list of system requirements and supported platforms, please consult the User's Guide. Information about each release can be found in the release notes. Each Windows package comes wit… See more Download Wireshark Choose your platform and start analyzing network traffic today. Stable Release: 4.4.7 Windows x64 Installer Windows Arm64 Installer Windows x64 PortableApps® macOS Arm Disk Image macOS Intel Disk Image Source Code Wireshark-4.4.7-x64.exe Completed — 83.3 MB

1.2. Install Wireshark

Running the installer
Accept all default components, includes WinPcap and NpCap


Wireshark 4.4.7 x64 Setup

Welcome to Wireshark 4.4.7 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.

Wireshark 4.4.7 x64 Setup

Packet Capture
Wireshark requires Npcap to capture live network data.

Currently installed Npcap version
Npcap 1.80

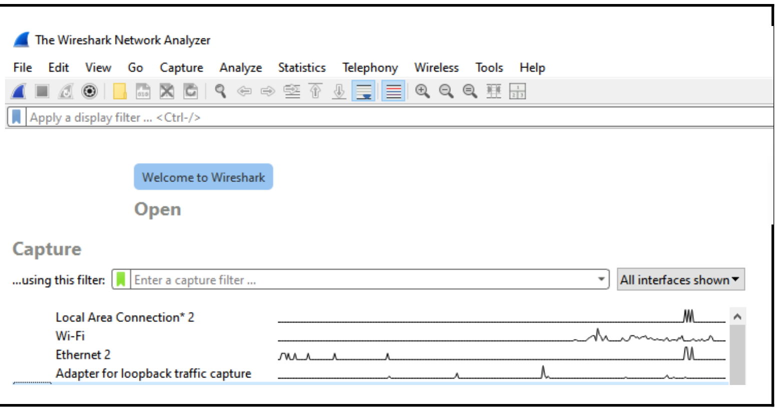
Install
□ Install Npcap 1.79
If you wish to install Npcap, please uninstall Npcap manually first.

Important notice
If your system has crashed during a Wireshark installation, you must run the command 'net stop npcap' as Administrator before upgrading Npcap, so that it doesn't crash again

Learn more about Npcap

1.3. Verify Installation

Open Wireshark
Ensure all that Wireshark lists available network interfaces (WiFi, Ethernet)

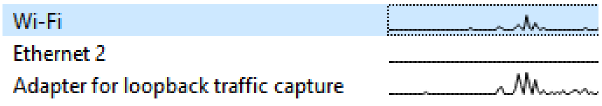

The Wireshark Network Analyzer

Local Area Connection* 2
Wi-Fi
Ethernet 2
Adapter for loopback traffic capture

2. Perform a Basic Network Scan

2.1. Select an interface

Selecting the Wi-FI interface



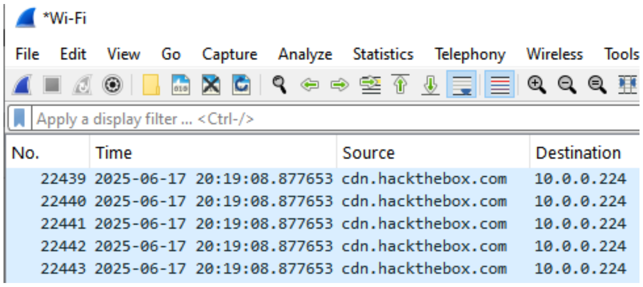
Wi-Fi

Ethernet 2

Adapter for loopback traffic capture

2.2. Browse the internet

Press the shark fin
Open a website and visit websites like hackthebox.com

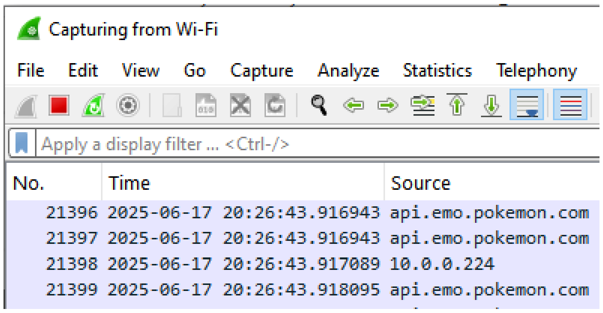


*Wi-Fi

No.	Time	Source	Destination
22439	2025-06-17 20:19:08.877653	cdn.hackthebox.com	10.0.0.224
22440	2025-06-17 20:19:08.877653	cdn.hackthebox.com	10.0.0.224
22441	2025-06-17 20:19:08.877653	cdn.hackthebox.com	10.0.0.224
22442	2025-06-17 20:19:08.877653	cdn.hackthebox.com	10.0.0.224
22443	2025-06-17 20:19:08.877653	cdn.hackthebox.com	10.0.0.224

2.3. Stop the Capture

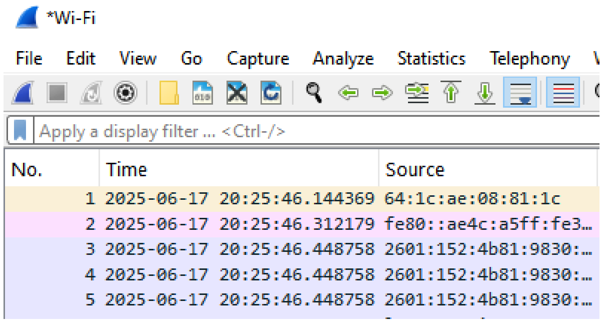
Press the red button to stop Wireshark from capture the packets



Capturing from Wi-Fi

No.	Time	Source
21396	2025-06-17 20:26:43.916943	api.emo.pokemon.com
21397	2025-06-17 20:26:43.916943	api.emo.pokemon.com
21398	2025-06-17 20:26:43.917089	10.0.0.224
21399	2025-06-17 20:26:43.918095	api.emo.pokemon.com

The screen once after the packets had stop capturing:



*Wi-Fi

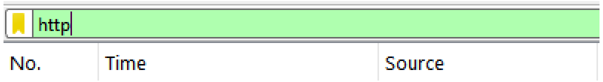
No.	Time	Source
1	2025-06-17 20:25:46.144369	64:1c:ae:08:81:1c
2	2025-06-17 20:25:46.312179	fe80::ae4c:a5ff:fe3…
3	2025-06-17 20:25:46.448758	2601:152:4b81:9830:…
4	2025-06-17 20:25:46.448758	2601:152:4b81:9830:…
5	2025-06-17 20:25:46.448758	2601:152:4b81:9830:…

3. Apply Filters in Wireshark

3.1. Basic Filters

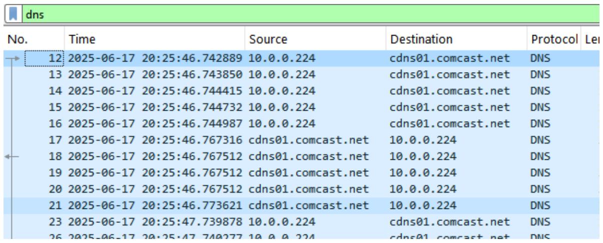
Filter http traffic
Filter dns traffic
Filter tcp traffic
Filter icmp traffic

There were no http traffic:



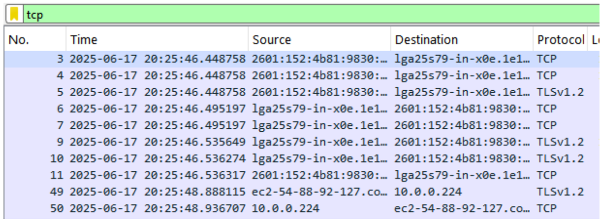
No.	Time	Source

There appears to be dns traffic:



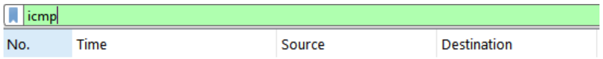
No.	Time	Source	Destination	Protocol	Le
12	2025-06-17 20:25:46.742889	10.0.0.224	cdns01.comcast.net	DNS	
13	2025-06-17 20:25:46.743850	10.0.0.224	cdns01.comcast.net	DNS	
14	2025-06-17 20:25:46.744415	10.0.0.224	cdns01.comcast.net	DNS	
15	2025-06-17 20:25:46.744732	10.0.0.224	cdns01.comcast.net	DNS	
16	2025-06-17 20:25:46.744987	10.0.0.224	cdns01.comcast.net	DNS	
17	2025-06-17 20:25:46.767316	cdns01.comcast.net	10.0.0.224	DNS	
18	2025-06-17 20:25:46.767512	cdns01.comcast.net	10.0.0.224	DNS	
19	2025-06-17 20:25:46.767512	cdns01.comcast.net	10.0.0.224	DNS	
20	2025-06-17 20:25:46.767512	cdns01.comcast.net	10.0.0.224	DNS	
21	2025-06-17 20:25:46.773621	cdns01.comcast.net	10.0.0.224	DNS	
23	2025-06-17 20:25:47.739878	10.0.0.224	cdns01.comcast.net	DNS	
26	2025-06-17 20:25:47.740277	10.0.0.224	cdns01.comcast.net	DNS	

There appears to be tcp traffic:



No.	Time	Source	Destination	Protocol	L
3	2025-06-17 20:25:46.448758	2601:152:4b81:9830:…	lga25s79-in-x0e.1e1…	TCP	
4	2025-06-17 20:25:46.448758	2601:152:4b81:9830:…	lga25s79-in-x0e.1e1…	TCP	
5	2025-06-17 20:25:46.448758	2601:152:4b81:9830:…	lga25s79-in-x0e.1e1…	TLSv1.2	
6	2025-06-17 20:25:46.495197	lga25s79-in-x0e.1e1…	2601:152:4b81:9830:…	TCP	
7	2025-06-17 20:25:46.495197	lga25s79-in-x0e.1e1…	2601:152:4b81:9830:…	TCP	
9	2025-06-17 20:25:46.535649	lga25s79-in-x0e.1e1…	2601:152:4b81:9830:…	TLSv1.2	
10	2025-06-17 20:25:46.536274	lga25s79-in-x0e.1e1…	2601:152:4b81:9830:…	TLSv1.2	
11	2025-06-17 20:25:46.536317	2601:152:4b81:9830:…	lga25s79-in-x0e.1e1…	TCP	
49	2025-06-17 20:25:48.888115	ec2-54-88-92-127.co…	10.0.0.224	TLSv1.2	
50	2025-06-17 20:25:48.936707	10.0.0.224	ec2-54-88-92-127.co…	TCP	

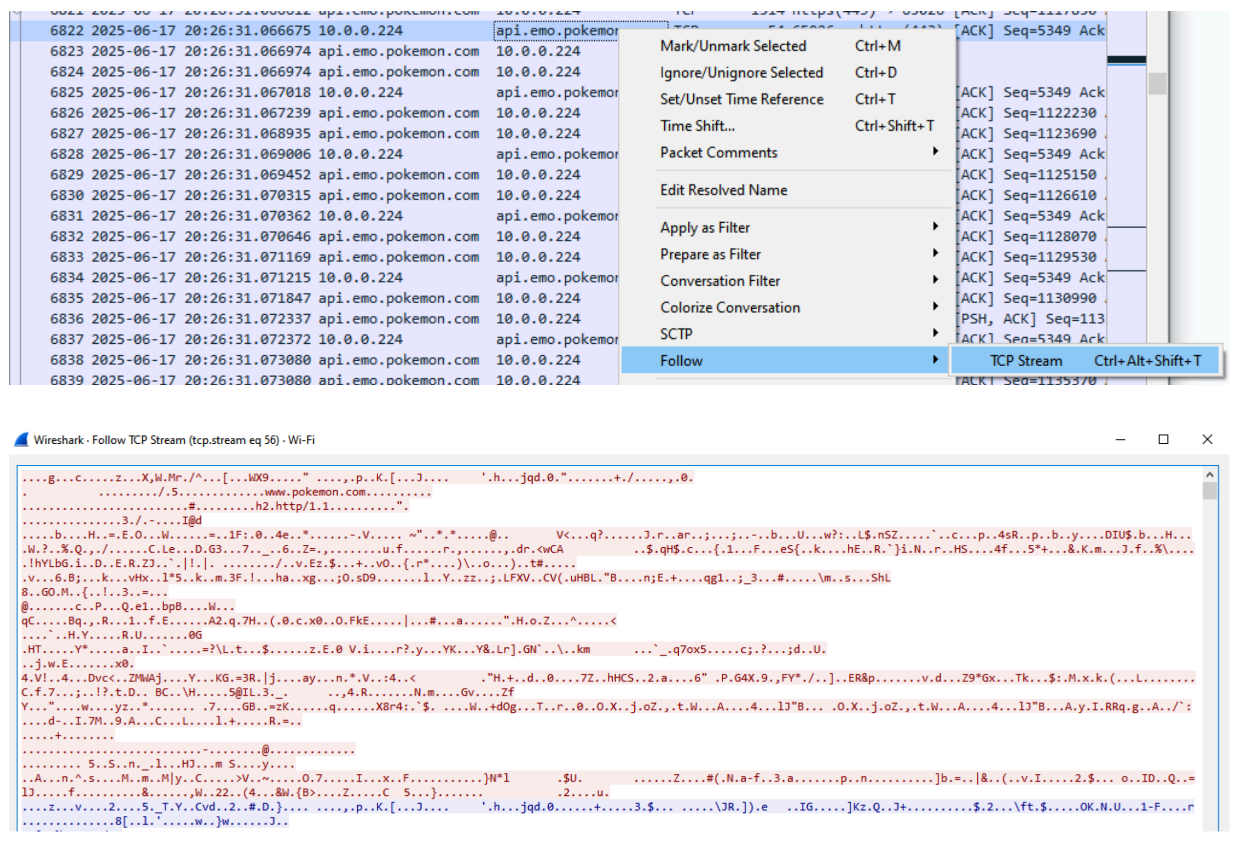
There appears to be no icmp traffic:



No.	Time	Source	Destination

3.2. Conservation Filters

Pressing right click and following the TCP stream


Mark/Unmark Selected Ctrl+M
Ignore/Unignore Selected Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
TCP Stream Ctrl+Alt+Shift+T

```
6822 2025-06-17 20:26:31.066675 10.0.0.224          api.emo.pokemon                                   [ACK] Seq=5349 Ack
6823 2025-06-17 20:26:31.066974 api.emo.pokemon.com 10.0.0.224
6824 2025-06-17 20:26:31.066974 api.emo.pokemon.com 10.0.0.224
6825 2025-06-17 20:26:31.067018 10.0.0.224          api.emo.pokemon                                   [ACK] Seq=5349 Ack
6826 2025-06-17 20:26:31.067239 api.emo.pokemon.com 10.0.0.224                                        [ACK] Seq=1122230
6827 2025-06-17 20:26:31.068935 api.emo.pokemon.com 10.0.0.224                                        [ACK] Seq=1123690
6828 2025-06-17 20:26:31.069006 10.0.0.224          api.emo.pokemon                                   [ACK] Seq=5349 Ack
6829 2025-06-17 20:26:31.069452 api.emo.pokemon.com 10.0.0.224                                        [ACK] Seq=1125150
6830 2025-06-17 20:26:31.070315 api.emo.pokemon.com 10.0.0.224                                        [ACK] Seq=1126610
6831 2025-06-17 20:26:31.070362 10.0.0.224          api.emo.pokemon                                   [ACK] Seq=5349 Ack
6832 2025-06-17 20:26:31.070646 api.emo.pokemon.com 10.0.0.224                                        [ACK] Seq=1128070
6833 2025-06-17 20:26:31.071169 api.emo.pokemon.com 10.0.0.224                                        [ACK] Seq=1129530
6834 2025-06-17 20:26:31.071215 10.0.0.224          api.emo.pokemon                                   [ACK] Seq=5349 Ack
6835 2025-06-17 20:26:31.071847 api.emo.pokemon.com 10.0.0.224                                        [ACK] Seq=1130990
6836 2025-06-17 20:26:31.072337 api.emo.pokemon.com 10.0.0.224                                        [PSH, ACK] Seq=113
6837 2025-06-17 20:26:31.072372 10.0.0.224          api.emo.pokemon                                   [ACK] Seq=5349 Ack
6838 2025-06-17 20:26:31.073080 api.emo.pokemon.com 10.0.0.224
6839 2025-06-17 20:26:31.073080 api.emo.pokemon.com 10.0.0.224                                        [ACK] Seq=1135370
```

Wireshark · Follow TCP Stream (tcp.stream eq 56) · Wi-Fi

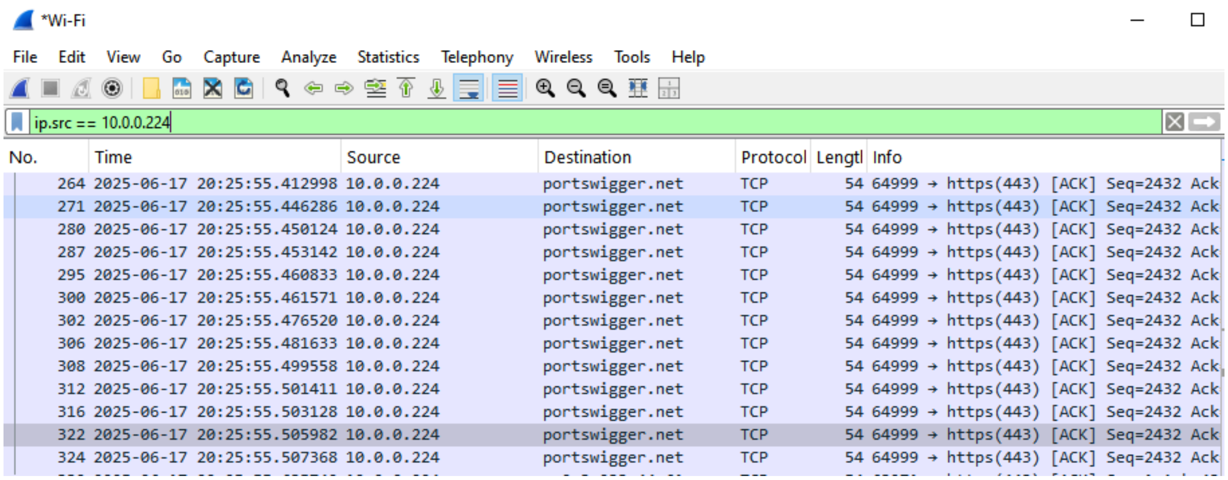
```
....g...c.....z...X,W.Mr./^...[...WX9....." ....,.p..K.[...J....    '.h...jqd.0.".......+./.....,.0.
.          ........./.5............www.pokemon.com.........
........................#.........h2.http/1.1.........".
...............3./.-....I@d
.....b....H..=.E.O...W......=..1F:.0..4e..*......-.V..... ~"..*.*.....@..       V<...q?......J.r..ar..;...;..-..b...U...w?:..L$.nSZ.....`..c...p..4sR..p..b..y....DIU$.b...H...
.W.?..%.Q.,./......C.Le...D.G3...7.._..6..Z=.,........u.f......r.,.......,.dr.<wCA          ..$.qH$.c...{.1...F...eS{..k....hE..R.`}i.N..r..HS....4f...5*+...&.K.m...J.f..%\....
.!hYLbG.i..D..E.R.ZJ..`.|!.|. ......../..v.Ez.$...+..vO..{.r*....)\..o...)..t#.....
.v...6.B;...k...vHx..1*5..k..m.3F.!...ha..xg...;O.sD9.......l..Y..zz..;.LFXV..CV(.uHBL."B....n;E.+....qg1..;_3...#.....\m..s...ShL
8..GO.M..{..!..3..=...
@.......c..P...Q.e1..bpB....W...
qC.....Bq.,.R...1..f.E......A2.q.7H..(.0.c.x0..O.FkE.....|...#...a......".H.o.Z...^.....<
....`..H.Y.....R.U.......0G
.HT.....Y*.....a..I..`.....=?\L.t...$......z.E.0 V.i....r?.y...YK...Y&.Lr].GN`..\..km       ...`_.q7ox5.....c;.?...;d..U.
..j.w.E.......x0.
4.V!..4...Dvc<..ZMWAj....Y...KG.=3R.|j....ay...n.*.V..:4..<         ."H.+..d..0....7Z..hHCS..2.a....6" .P.G4X.9.,FY*./..]..ER&p.......v.d...Z9*Gx...Tk...$:.M.x.k.(...L........
C.f.7...;..!?.t.D.. BC..\H.....5@IL.3._.      ..,4.R.......N.m....Gv....Zf
Y..."....w....yz..*....... .7....GB..=zK......q......X8r4:.`$. ....W..+dOg...T..r..0..O.X..j.oZ.,.t.W...A....4...1J"B... .O.X..j.oZ.,.t.W...A....4...1J"B...A.y.I.RRq.g..A../`:
....d-..I.7M..9.A...C...L....l.+.....R.=..
.....+........
..........................-........@............
......... 5..S..n._.l...HJ...m S....y....
..A...n.^.s....M..m..M|y..C.....>V..~.....O.7.....I...x..F...........}N*l       .$U.        ......Z....#(.N.a-f..3.a.......p..n..........]b.=..|&..(..v.I.....2.$... o..ID..Q..=
lJ.....f..........&......,W..22..(4...&W.{B>....Z.....C  5...}.......          .2....u.
....z...v....2....5._T.Y..Cvd..2..#.D.}.... ....,.p..K.[...J....    '.h...jqd.0......+.....3.$... .....\JR.]).e   ..IG.....]Kz.Q..J+..........$.2...\ft.$.....OK.N.U...1-F....r
..............8[..l.'.....w..}w......J..
```

4. Advanced Filters

4.1. Filter A <-> Any

Apply a filter to show packets sent from your IP address to any destination.

ip.src == 10.0.0.224


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

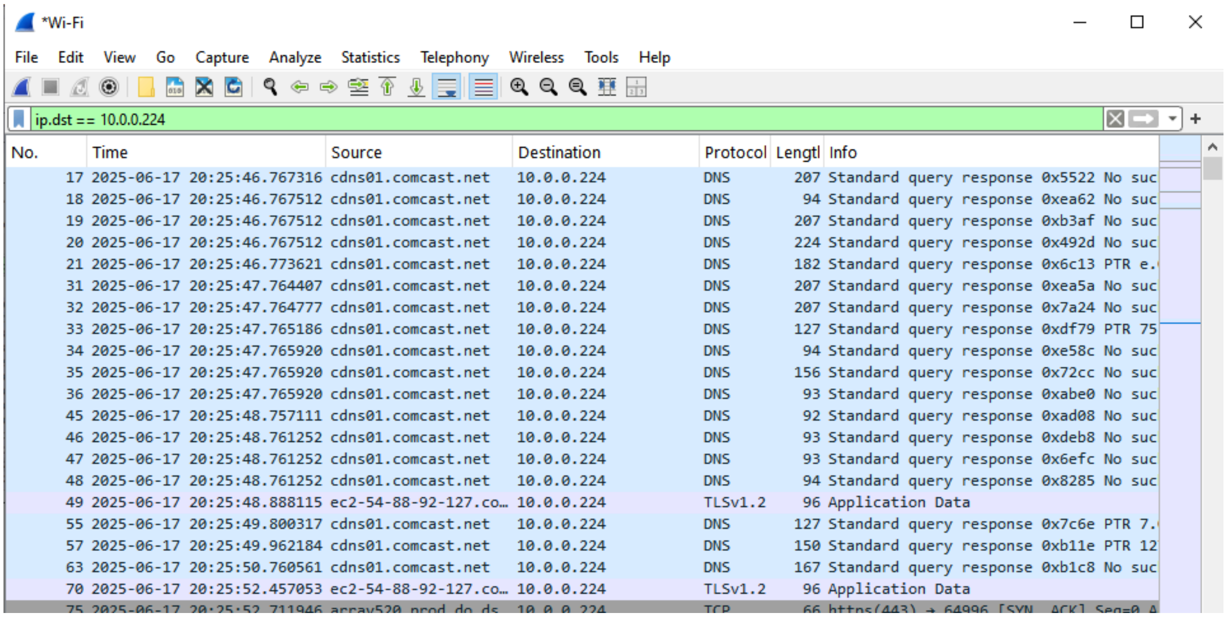
ip.src == 10.0.0.224

```
No.  Time                       Source      Destination      Protocol Lengtl Info
 264 2025-06-17 20:25:55.412998 10.0.0.224  portswigger.net  TCP       54 64999 → https(443) [ACK] Seq=2432 Ack
 271 2025-06-17 20:25:55.446286 10.0.0.224  portswigger.net  TCP       54 64999 → https(443) [ACK] Seq=2432 Ack
 280 2025-06-17 20:25:55.450124 10.0.0.224  portswigger.net  TCP       54 64999 → https(443) [ACK] Seq=2432 Ack
 287 2025-06-17 20:25:55.453142 10.0.0.224  portswigger.net  TCP       54 64999 → https(443) [ACK] Seq=2432 Ack
 295 2025-06-17 20:25:55.460833 10.0.0.224  portswigger.net  TCP       54 64999 → https(443) [ACK] Seq=2432 Ack
 300 2025-06-17 20:25:55.461571 10.0.0.224  portswigger.net  TCP       54 64999 → https(443) [ACK] Seq=2432 Ack
 302 2025-06-17 20:25:55.476520 10.0.0.224  portswigger.net  TCP       54 64999 → https(443) [ACK] Seq=2432 Ack
 306 2025-06-17 20:25:55.481633 10.0.0.224  portswigger.net  TCP       54 64999 → https(443) [ACK] Seq=2432 Ack
 308 2025-06-17 20:25:55.499558 10.0.0.224  portswigger.net  TCP       54 64999 → https(443) [ACK] Seq=2432 Ack
 312 2025-06-17 20:25:55.501411 10.0.0.224  portswigger.net  TCP       54 64999 → https(443) [ACK] Seq=2432 Ack
 316 2025-06-17 20:25:55.503128 10.0.0.224  portswigger.net  TCP       54 64999 → https(443) [ACK] Seq=2432 Ack
 322 2025-06-17 20:25:55.505982 10.0.0.224  portswigger.net  TCP       54 64999 → https(443) [ACK] Seq=2432 Ack
 324 2025-06-17 20:25:55.507368 10.0.0.224  portswigger.net  TCP       54 64999 → https(443) [ACK] Seq=2432 Ack
```

4.2. Filter Any <-> A

Apply a filter to show packets sent to your IP address from any source.

ip.dst == 10.0.0.224



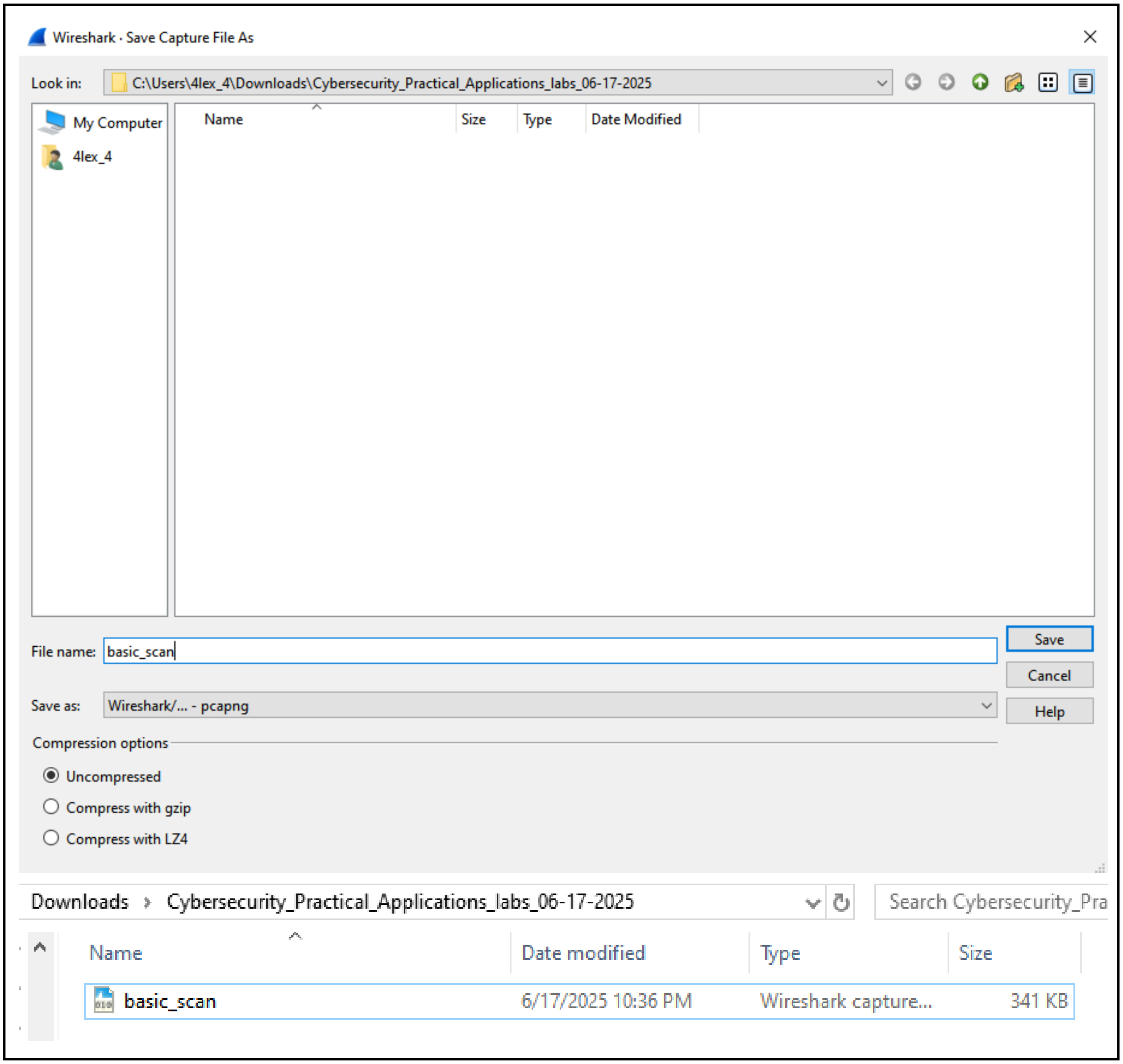
ip.dst == 10.0.0.224

```
No.   Time                       Source                 Destination  Protocol Lengtl Info
   17 2025-06-17 20:25:46.767316 cdns01.comcast.net     10.0.0.224   DNS       207 Standard query response 0x5522 No suc
   18 2025-06-17 20:25:46.767512 cdns01.comcast.net     10.0.0.224   DNS        94 Standard query response 0xea62 No suc
   19 2025-06-17 20:25:46.767512 cdns01.comcast.net     10.0.0.224   DNS       207 Standard query response 0xb3af No suc
   20 2025-06-17 20:25:46.767512 cdns01.comcast.net     10.0.0.224   DNS       224 Standard query response 0x492d No suc
   21 2025-06-17 20:25:46.773621 cdns01.comcast.net     10.0.0.224   DNS       182 Standard query response 0x6c13 PTR e.
   31 2025-06-17 20:25:47.764407 cdns01.comcast.net     10.0.0.224   DNS       207 Standard query response 0xea5a No suc
   32 2025-06-17 20:25:47.764777 cdns01.comcast.net     10.0.0.224   DNS       207 Standard query response 0x7a24 No suc
   33 2025-06-17 20:25:47.765186 cdns01.comcast.net     10.0.0.224   DNS       127 Standard query response 0xdf79 PTR 75
   34 2025-06-17 20:25:47.765920 cdns01.comcast.net     10.0.0.224   DNS        94 Standard query response 0xe58c No suc
   35 2025-06-17 20:25:47.765920 cdns01.comcast.net     10.0.0.224   DNS       156 Standard query response 0x72cc No suc
   36 2025-06-17 20:25:47.765920 cdns01.comcast.net     10.0.0.224   DNS        93 Standard query response 0xabe0 No suc
   45 2025-06-17 20:25:48.757111 cdns01.comcast.net     10.0.0.224   DNS        92 Standard query response 0xad08 No suc
   46 2025-06-17 20:25:48.761252 cdns01.comcast.net     10.0.0.224   DNS        93 Standard query response 0xdeb8 No suc
   47 2025-06-17 20:25:48.761252 cdns01.comcast.net     10.0.0.224   DNS        93 Standard query response 0x6efc No suc
   48 2025-06-17 20:25:48.761252 cdns01.comcast.net     10.0.0.224   DNS        94 Standard query response 0x8285 No suc
   49 2025-06-17 20:25:48.888115 ec2-54-88-92-127.co…   10.0.0.224   TLSv1.2    96 Application Data
   55 2025-06-17 20:25:49.800317 cdns01.comcast.net     10.0.0.224   DNS       127 Standard query response 0x7c6e PTR 7.
   57 2025-06-17 20:25:49.962184 cdns01.comcast.net     10.0.0.224   DNS       150 Standard query response 0xb11e PTR 12
   63 2025-06-17 20:25:50.760561 cdns01.comcast.net     10.0.0.224   DNS       167 Standard query response 0xb1c8 No suc
   70 2025-06-17 20:25:52.457053 ec2-54-88-92-127.co…   10.0.0.224   TLSv1.2    96 Application Data
   75 2025-06-17 20:25:52.711946 array520.prod.do.ds…   10.0.0.224   TCP        66 https(443) → 64996 [SYN, ACK] Seq=0 A
```

5. Capture and Export

5.1. Export the capture

Export file and save as “basic_scan.pcapng”



Wireshark · Save Capture File As

Look in: C:\Users\4lex_4\Downloads\Cybersecurity_Practical_Applications_labs_06-17-2025

File name: basic_scan

Save as: Wireshark/... - pcapng

Compression options

- ● Uncompressed
- ○ Compress with gzip
- ○ Compress with LZ4

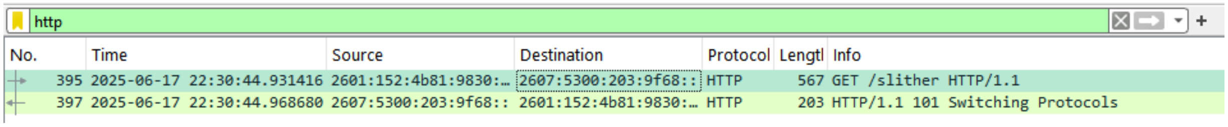
Downloads › Cybersecurity_Practical_Applications_labs_06-17-2025

Search Cybersecurity_Pra

Name	Date modified	Type	Size
basic_scan	6/17/2025 10:36 PM	Wireshark capture...	341 KB

5.2. Take screenshots

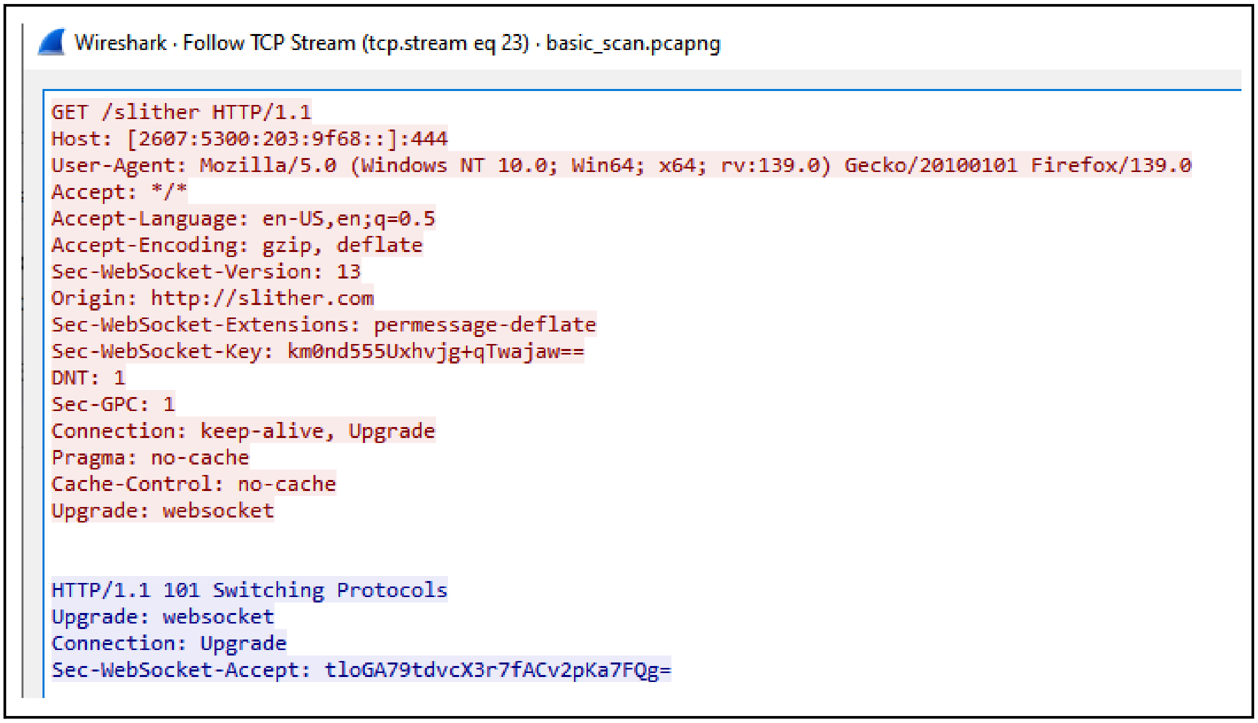
http filter



http

```
No.   Time                        Source                Destination           Protocol Lengtl Info
  395 2025-06-17 22:30:44.931416 2601:152:4b81:9830:… 2607:5300:203:9f68:: HTTP      567 GET /slither HTTP/1.1
  397 2025-06-17 22:30:44.968680 2607:5300:203:9f68:: 2601:152:4b81:9830:… HTTP      203 HTTP/1.1 101 Switching Protocols
```

Following the tcp



Wireshark · Follow TCP Stream (tcp.stream eq 23) · basic_scan.pcapng

```
GET /slither HTTP/1.1
Host: [2607:5300:203:9f68::]:444
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:139.0) Gecko/20100101 Firefox/139.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Sec-WebSocket-Version: 13
Origin: http://slither.com
Sec-WebSocket-Extensions: permessage-deflate
Sec-WebSocket-Key: km0nd555Uxhvjg+qTwajaw==
DNT: 1
Sec-GPC: 1
Connection: keep-alive, Upgrade
Pragma: no-cache
Cache-Control: no-cache
Upgrade: websocket


HTTP/1.1 101 Switching Protocols
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Accept: tloGA79tdvcX3r7fACv2pKa7FQg=
```

🧰 Tools & Skills Used

- **Wireshark**
- **Windows 10**
- **Packet Filtering**
- **Network Protocol Analysis**

🧠 Reflection & Takeaways

This lab helped me reinforce my prior knowledge with Wireshark. While I was familiar with Wireshark before with ctf competitions and other tasks. Revisiting this tool helps me identify small knowledge gaps with filtering syntax and capturing exports.
Due to performance issues with the vm, I opted to use my personal Windows 10 computer which gives me an optimal experience.