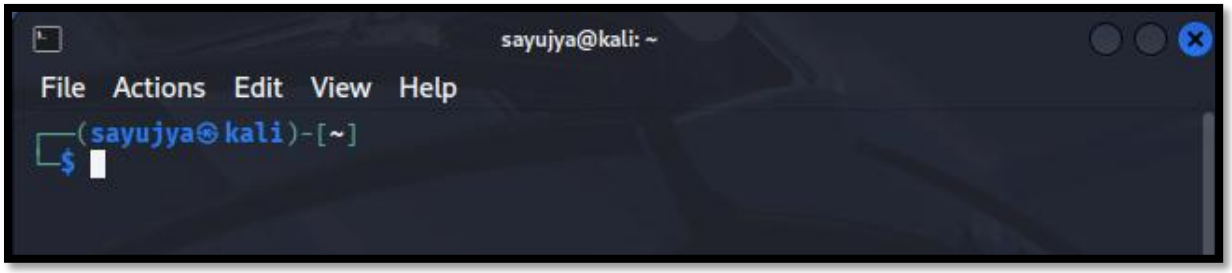
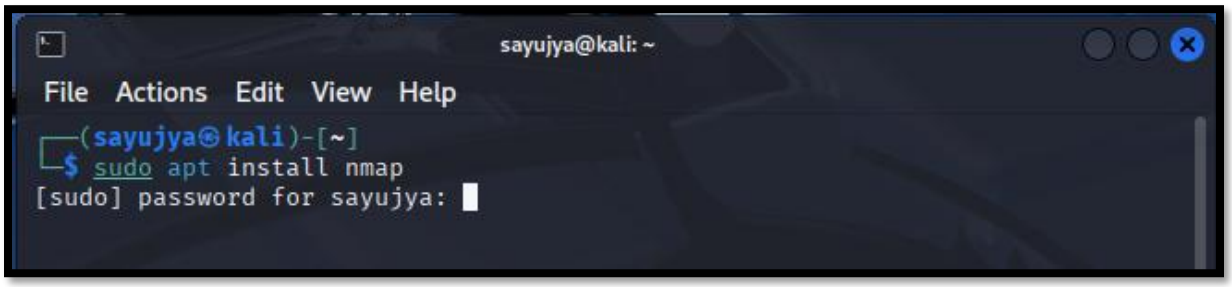
Lab 4: Use Nmap and Wireshark in Kali Linux

1. Setting up Nmap

Step 1: Open the terminal using Win + T



Step 2: Insert the command "sudo apt install nmap" and press enter



1.1. Purpose of Nmap:

Nmap is a powerful open-source tool used for network discovery and security auditing. It's widely used by network administrators and penetration testers.

1.1.1. Detailed Purposes:

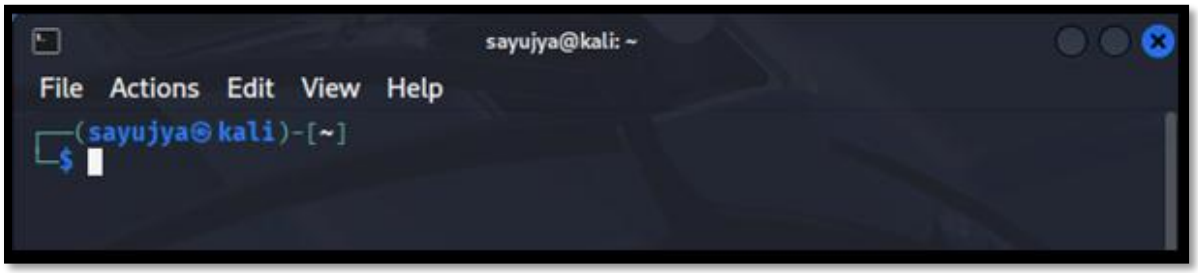
- **Host Discovery:** Detects which devices are currently online in a network.
- **Port Scanning:** Identifies which network ports are open and what services are running on them.
- **Service Version Detection:** Determines software versions running on open ports (e.g., Apache 2.4.54).
- **Operating System Detection:** Tries to identify the target's operating system.
- **Vulnerability Scanning (with NSE Scripts):** Detects known vulnerabilities using built-in or custom scripts via the Nmap Scripting Engine (NSE).
- **Network Mapping:** Helps visualize how hosts are connected and communicating on a network.
- **Stealth Scanning:** Useful in ethical hacking to scan without being easily detected by firewalls or IDS.

1.1.2. Use Case Example

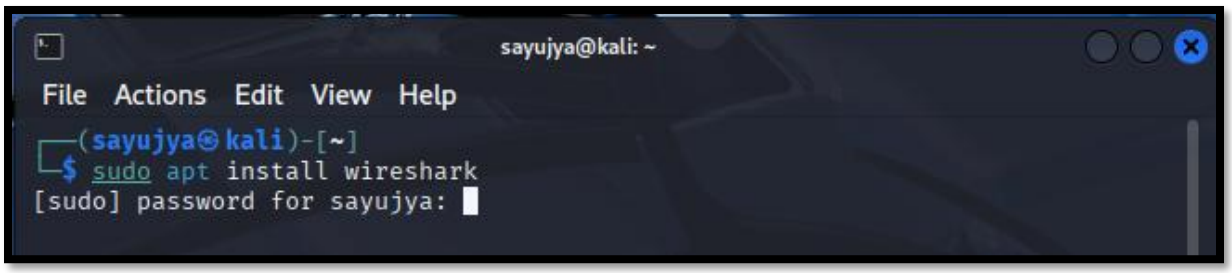
A network admin can use Nmap to scan the network and ensure no unauthorized devices are connected. Ethical hackers use it to find vulnerable points in a system.

2. Setting up Wireshark

Step 1: Open the terminal

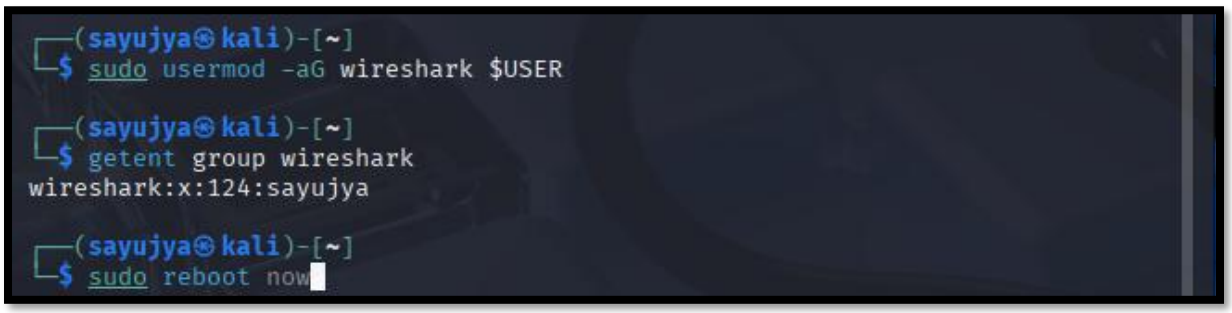


Step 2: Insert the command "sudo apt install wireshark" and press enter



Step 3: Adding current user to Wireshark group

- Run the command "sudo usermod -aG wireshark $USER"
- Then check for the users using "getent group wireshark"
- Finally, reboot to apply changes



2.1. Purpose of Wireshark

Wireshark is a network protocol analyzer that captures, filters, and analyzes live or saved packet data from a network interface.

2.1.1. Detailed Purposes

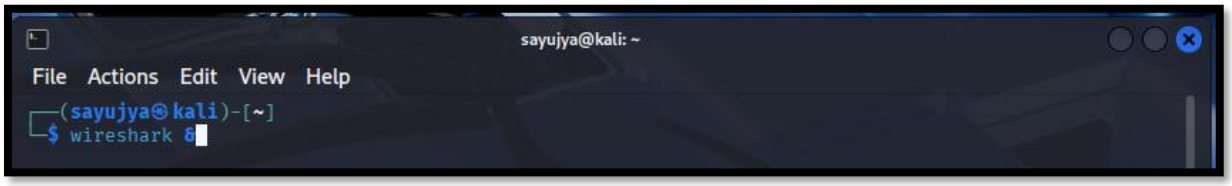
- **Packet Capture:** Captures all data packets passing through a selected network interface.
- **Protocol Analysis:** Understands and displays detailed information about thousands of network protocols like TCP, UDP, DNS, HTTP, ARP, etc.
- **Troubleshooting Network Issues:** Helps diagnose problems like slow network performance, failed connections, or incorrect configurations.
- **Security Monitoring:** Detects suspicious traffic like port scans, data leaks, or malware communication.
- **Educational Use:** Great for learning how protocols work (e.g., see how a DNS query or HTTP request looks at the packet level).
- **Filtering and Searching:** Offers advanced filters to isolate specific packet types or communication between devices.

2.1.2. Use Case Example

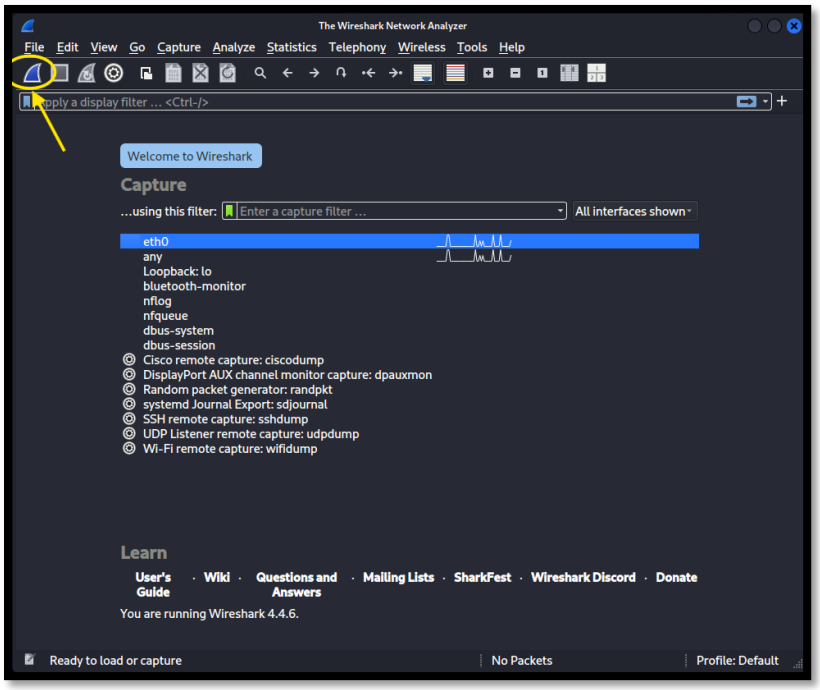
A cybersecurity student can use Wireshark to examine how a DNS request is structured, or a network engineer might use it to identify why certain packets are being dropped or delayed.

3. Using Wireshark: Packet Capture and Analysis

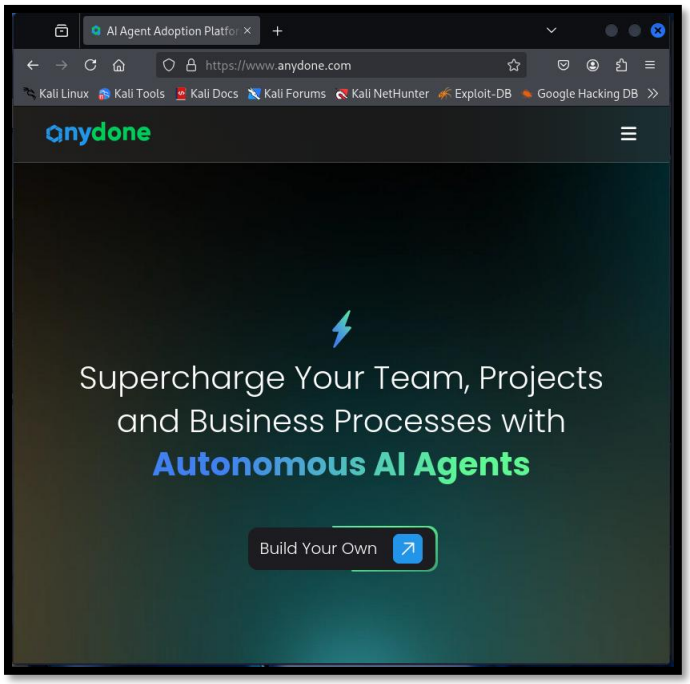
Step 1: Launch Wireshark



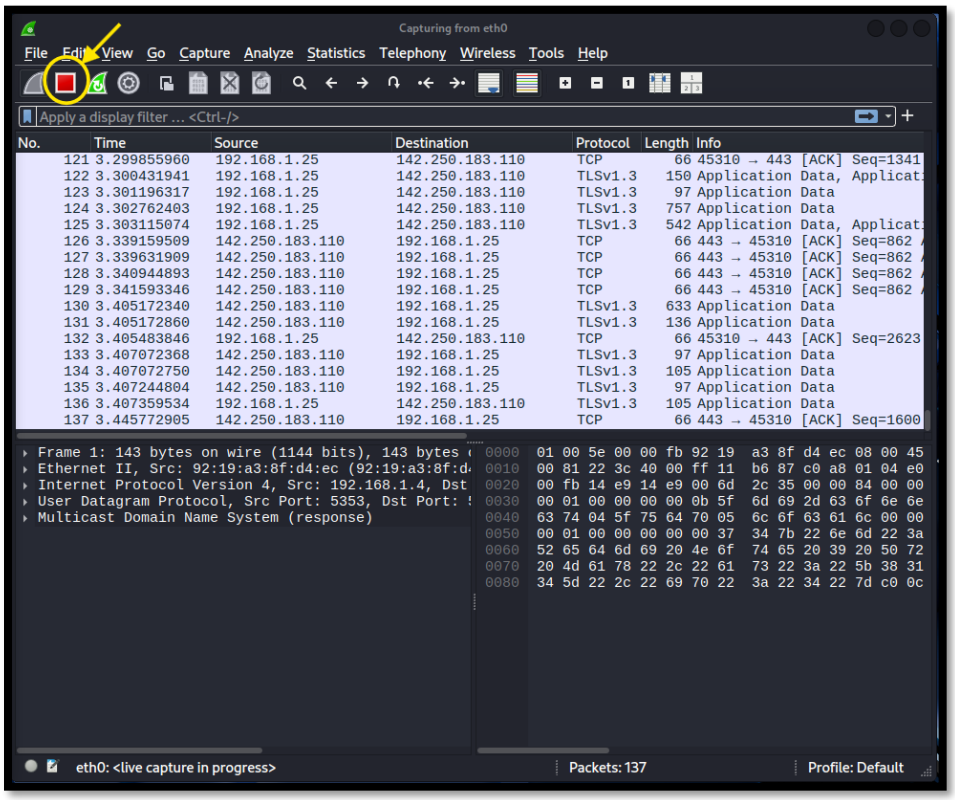
Step 2: Start Capturing by Clicking on the blue shark fin icon



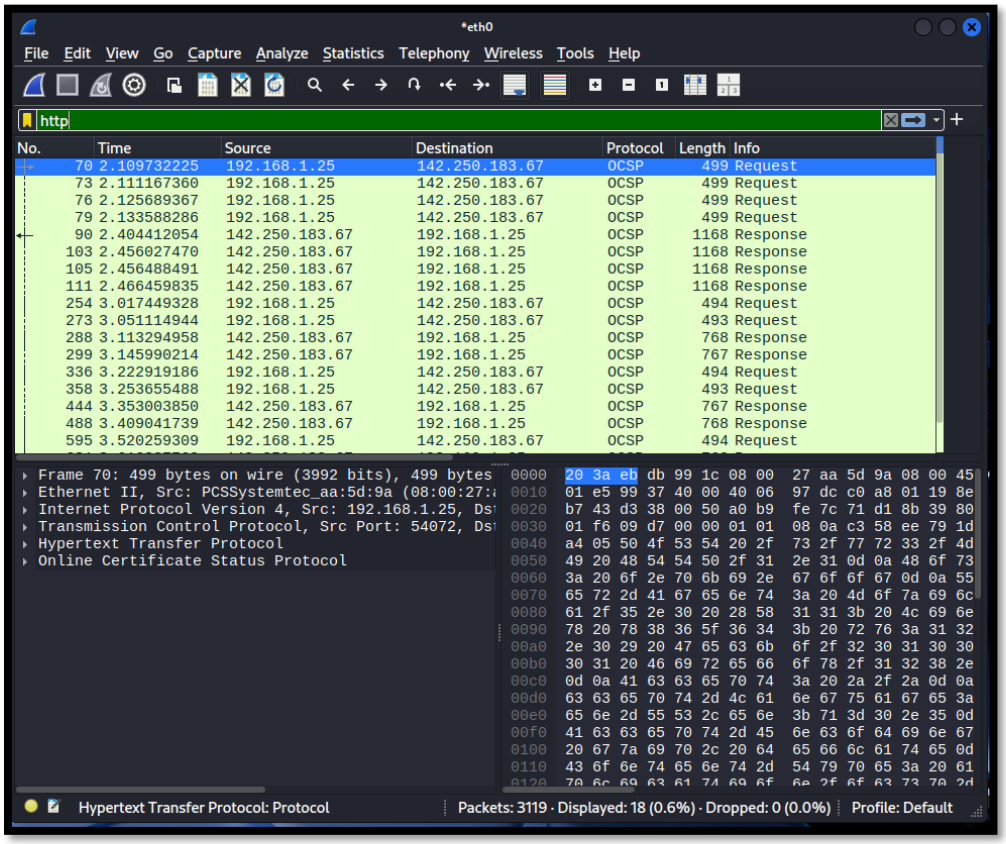
Step 3: Open browser and visit any website, in this case visiting www.anydone.com

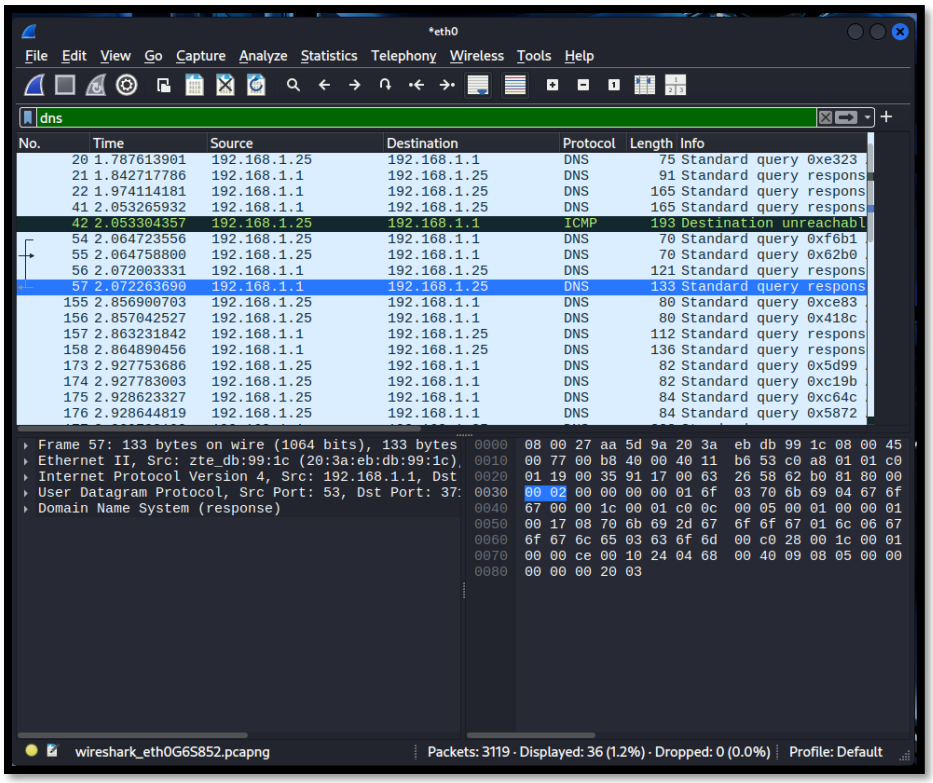


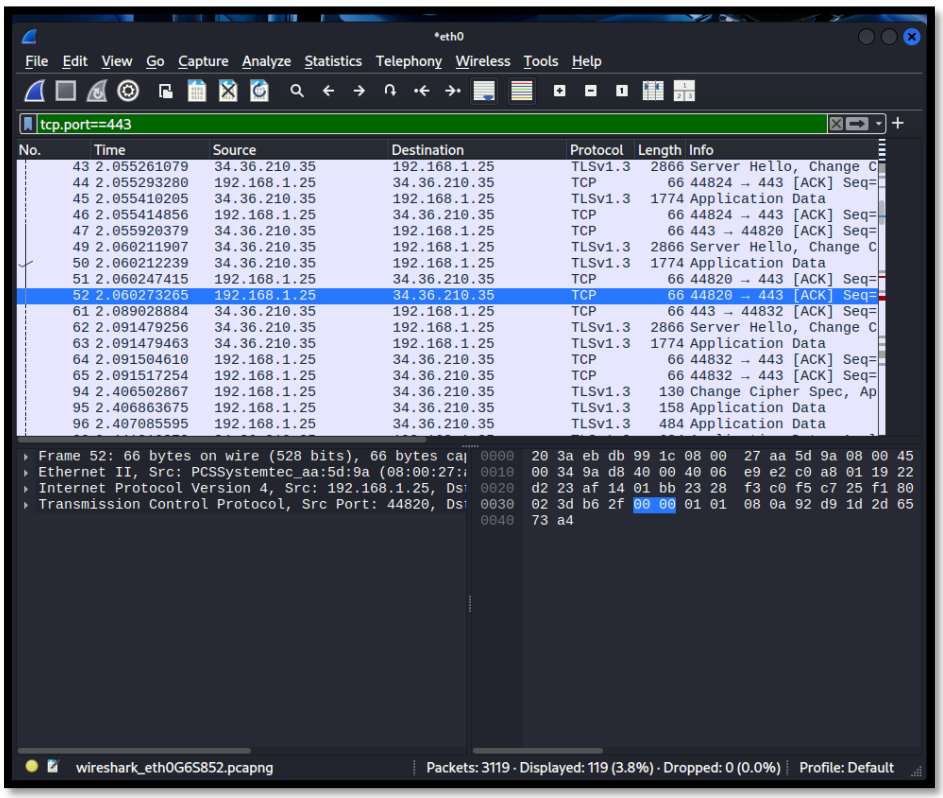
Step 5: After successfully opening, stop the recording by clicking on the red stop icon



Step 6: Filter the results between http, dns, and tcp.port==443




*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
20 1.787613901 192.168.1.25 192.168.1.1 DNS 75 Standard query 0xe323
21 1.842717786 192.168.1.1 192.168.1.25 DNS 91 Standard query respons
22 1.974114181 192.168.1.1 192.168.1.25 DNS 165 Standard query respons
41 2.053265932 192.168.1.1 192.168.1.25 DNS 165 Standard query respons
42 2.053304357 192.168.1.25 192.168.1.1 ICMP 193 Destination unreachabl
54 2.064723556 192.168.1.25 192.168.1.1 DNS 70 Standard query 0xf6b1
55 2.064758800 192.168.1.25 192.168.1.1 DNS 70 Standard query 0x62b0
56 2.072003331 192.168.1.1 192.168.1.25 DNS 121 Standard query respons
57 2.072263690 192.168.1.1 192.168.1.25 DNS 133 Standard query respons
155 2.856900703 192.168.1.25 192.168.1.1 DNS 80 Standard query 0xce83
156 2.857042527 192.168.1.25 192.168.1.1 DNS 80 Standard query 0x418c
157 2.863231842 192.168.1.1 192.168.1.25 DNS 112 Standard query respons
158 2.864890456 192.168.1.1 192.168.1.25 DNS 136 Standard query respons
173 2.927753686 192.168.1.25 192.168.1.1 DNS 82 Standard query 0x5d99
174 2.927783003 192.168.1.25 192.168.1.1 DNS 82 Standard query 0xc19b
175 2.928623327 192.168.1.25 192.168.1.1 DNS 84 Standard query 0xc64c
176 2.928644819 192.168.1.25 192.168.1.1 DNS 84 Standard query 0x5872
Frame 57: 133 bytes on wire (1064 bits), 133 bytes
Ethernet II, Src: zte_db:99:1c (20:3a:eb:db:99:1c),
Internet Protocol Version 4, Src: 192.168.1.1, Dst
User Datagram Protocol, Src Port: 53, Dst Port: 37:
Domain Name System (response)
0000 08 00 27 aa 5d 9a 20 3a eb db 99 1c 08 00 45
0010 00 77 00 b8 40 00 40 11 b6 53 c0 a8 01 01 c0
0020 01 19 00 35 91 17 00 63 26 58 62 b0 81 80 00
0030 00 02 00 00 00 00 01 6f 03 70 6b 69 04 67 6f
0040 67 00 00 1c 00 01 c0 0c 00 05 00 01 00 00 01
0050 00 17 08 70 6b 69 2d 67 6f 6f 67 01 6c 06 67
0060 6f 67 6c 65 03 63 6f 6d 00 c0 28 00 1c 00 01
0070 00 00 ce 00 10 24 04 68 00 40 09 08 05 00 00
0080 00 00 00 20 03
wireshark_eth0G6S852.pcapng
Packets: 3119 · Displayed: 36 (1.2%) · Dropped: 0 (0.0%)
Profile: Default


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port==443
No. Time Source Destination Protocol Length Info
43 2.055261079 34.36.210.35 192.168.1.25 TLSv1.3 2866 Server Hello, Change C
44 2.055293280 192.168.1.25 34.36.210.35 TCP 66 44824 → 443 [ACK] Seq=
45 2.055410205 34.36.210.35 192.168.1.25 TLSv1.3 1774 Application Data
46 2.055414856 192.168.1.25 34.36.210.35 TCP 66 44824 → 443 [ACK] Seq=
47 2.055920379 34.36.210.35 192.168.1.25 TCP 66 443 → 44820 [ACK] Seq=
49 2.060211907 34.36.210.35 192.168.1.25 TLSv1.3 2866 Server Hello, Change C
50 2.060212239 34.36.210.35 192.168.1.25 TLSv1.3 1774 Application Data
51 2.060247415 192.168.1.25 34.36.210.35 TCP 66 44820 → 443 [ACK] Seq=
52 2.060273265 192.168.1.25 34.36.210.35 TCP 66 44820 → 443 [ACK] Seq=
61 2.089028884 34.36.210.35 192.168.1.25 TCP 66 443 → 44832 [ACK] Seq=
62 2.091479256 34.36.210.35 192.168.1.25 TLSv1.3 2866 Server Hello, Change C
63 2.091479463 34.36.210.35 192.168.1.25 TLSv1.3 1774 Application Data
64 2.091504610 192.168.1.25 34.36.210.35 TCP 66 44832 → 443 [ACK] Seq=
65 2.091517254 192.168.1.25 34.36.210.35 TCP 66 44832 → 443 [ACK] Seq=
94 2.406502867 192.168.1.25 34.36.210.35 TLSv1.3 130 Change Cipher Spec, Ap
95 2.406863675 192.168.1.25 34.36.210.35 TLSv1.3 158 Application Data
96 2.407085595 192.168.1.25 34.36.210.35 TLSv1.3 484 Application Data
Frame 52: 66 bytes on wire (528 bits), 66 bytes ca
Ethernet II, Src: PCSSystemtec_aa:5d:9a (08:00:27:
Internet Protocol Version 4, Src: 192.168.1.25, Ds
Transmission Control Protocol, Src Port: 44820, Ds
0000 20 3a eb db 99 1c 08 00 27 aa 5d 9a 08 00 45
0010 00 34 9a d8 40 00 40 06 e9 e2 c0 a8 01 19 22
0020 d2 23 af 14 01 bb 23 28 f3 c0 f5 c7 25 f1 80
0030 02 3d b6 2f 00 00 01 01 08 0a 92 d9 1d 2d 65
0040 73 a4
wireshark_eth0G6S852.pcapng
Packets: 3119 · Displayed: 119 (3.8%) · Dropped: 0 (0.0%)
Profile: Default

4. Using Nmap for Network Scanning

Simulate an Attacker's First Move:

4.1. Nmap the domain

Syntax: nmap -sV -O www.anydone.com

```
sayujya@kali: ~
File  Actions  Edit  View  Help
┌──(sayujya㉿kali)-[~]
└─$ nmap -sV -O www.anydone.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 12:59 EDT
Nmap scan report for www.anydone.com (34.36.210.35)
Host is up (0.041s latency).
rDNS record for 34.36.210.35: 35.210.36.34.bc.googleusercontent.com
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE   VERSION
80/tcp  open  http
443/tcp open  ssl/https Google Frontend
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at
 https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.95%I=7%D=5/10%Time=681F85F6%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,BF,"HTTP/1\.0\x20301\x20Moved\x20Permanently\r\nCache-Control:\x
SF:20private\r\nLocation:\x20https://34\.36\.210\.35:443/\r\nContent-Lengt
SF:h:\x200\r\nDate:\x20Sat,\x2010\x20May\x202025\x2016:58:44\x20GMT\r\nCon
SF:tent-Type:\x20text/html;\x20charset=UTF-8\r\n\r\n")%r(HTTPOptions,BF,"H
SF:TTP/1\.0\x20301\x20Moved\x20Permanently\r\nCache-Control:\x20private\r\
SF:nLocation:\x20https://34\.36\.210\.35:443/\r\nContent-Length:\x200\r\nD
SF:ate:\x20Sat,\x2010\x20May\x202025\x2016:58:44\x20GMT\r\nContent-Type:\x
SF:20text/html;\x20charset=UTF-8\r\n\r\n")%r(RTSPRequest,1AD,"HTTP/1\.0\x2
SF:0400\x20Bad\x20Request\r\nContent-Type:\x20text/html;\x20charset=UTF-8\
SF:r\nReferrer-Policy:\x20no-referrer\r\nContent-Length:\x20273\r\nDate:\x
SF:20Sat,\x2010\x20May\x202025\x2016:58:44\x20GMT\r\n\r\n\n<html><head>\n<
SF:meta\x20http-equiv=\"content-type\"\x20content=\"text/html;charset=utf-
SF:8\">\n<title>400\x20Bad\x20Request</title>\n</head>\n<body\x20text=#000
SF:000\x20bgcolor=#ffffff>\n<h1>Error:\x20Bad\x20Request</h1>\n<h2>Your\x2
SF:0client\x20has\x20issued\x20a\x20malformed\x20or\x20illegal\x20request\
SF:.</h2>\n<h2></h2>\n</body></html>\n")%r(FourOhFourRequest,DE,"HTTP/1\.0
SF:\x20301\x20Moved\x20Permanently\r\nCache-Control:\x20private\r\nLocatio
SF:n:\x20https://34\.36\.210\.35:443/nice%20ports%2C/Trinity\.txt\.bak\r\n
SF:Content-Length:\x200\r\nDate:\x20Sat,\x2010\x20May\x202025\x2016:58:50\
SF:x20GMT\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\n\r\n")%r(DNSV
SF:ersionBindReqTCP,B3,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Leng
SF:th:\x2054\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\nDate:\x20S
SF:at,\x2010\x20May\x202025\x2016:59:00\x20GMT\r\n\r\n<html><title>Error\x
SF:20400\x20\(Bad\x20Request\)!!1</title></html>")%r(DNSStatusRequestTCP,B
SF:3,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Length:\x2054\r\nConte
```

```
sayujya@kali: ~
File  Actions  Edit  View  Help
SF:v=\"refresh\"\x20content=\"no-cache\"/><meta\x20name=\"viewport\"\x20co
SF:ntent=\"width=device-width,initial-scale=1\"/><meta\x20property=\"og:im
SF:age\"\x20content=\"http")%r(tor-versions,B3,"HTTP/1\.0\x20400\x20Bad\x2
SF:0Request\r\nContent-Length:\x2054\r\nContent-Type:\x20text/html;\x20cha
SF:rset=UTF-8\r\nDate:\x20Sat,\x2010\x20May\x202025\x2016:58:52\x20GMT\r\n
SF:\r\n<html><title>Error\x20400\x20\(Bad\x20Request\)!!1</title></html>")
SF:%r(RTSPRequest,1AD,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Type:
SF:\x20text/html;\x20charset=UTF-8\r\nReferrer-Policy:\x20no-referrer\r\nC
SF:ontent-Length:\x20273\r\nDate:\x20Sat,\x2010\x20May\x202025\x2016:58:58
SF:\x20GMT\r\n\r\n\n<html><head>\n<meta\x20http-equiv=\"content-type\"\x20
SF:content=\"text/html;charset=utf-8\">\n<title>400\x20Bad\x20Request</tit
SF:le>\n</head>\n<body\x20text=#000000\x20bgcolor=#ffffff>\n<h1>Error:\x20
SF:Bad\x20Request</h1>\n<h2>Your\x20client\x20has\x20issued\x20a\x20malfor
SF:med\x20or\x20illegal\x20request\.</h2>\n<h2></h2>\n</body></html>\n")%r
SF:(DNSVersionBindReqTCP,B3,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent
SF:-Length:\x2054\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\nDate:
SF:\x20Sat,\x2010\x20May\x202025\x2016:59:03\x20GMT\r\n\r\n<html><title>Er
SF:ror\x20400\x20\(Bad\x20Request\)!!1</title></html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Apple macOS 11.X|12.X (86%), FreeBSD 8.X (86%)
OS CPE: cpe:/o:apple:mac_os_x:11 cpe:/o:apple:mac_os_x:12 cpe:/o:freebsd:freebsd:8.2
Aggressive OS guesses: Apple macOS 11 (Big Sur) - 12 (Monterey) (Darwin 20.6.0 - 21.3.0) (86%), FreeBSD 8.2-RELEASE (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 12 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 84.97 seconds
```

4.2. Analyze Web Info

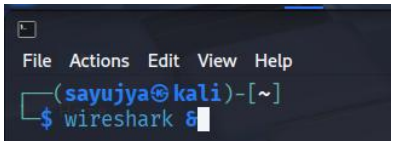
Syntax: whatweb www.anydone.com

```
┌──(sayujya㉿kali)-[~]
└─$ whatweb www.anydone.com
http://www.anydone.com [301 Moved Permanently] Country[UNITED STATES][US], IP[34.36.210.35], RedirectLocation[https://www.anydone.com:443/]
https://www.anydone.com/ [200 OK] Country[UNITED STATES][US], Email[ai_csr@anydone.com], HTML5, HTTPServer[Google Frontend], IP[34.36.210.35], Script, Title[AI Agent Adoption Platform | any
done], UncommonHeaders[x-anydone-cache,x-content-type-options,alt-svc], Via-Proxy[1.1 google], X-XSS-Protection[1; mode=block]
```

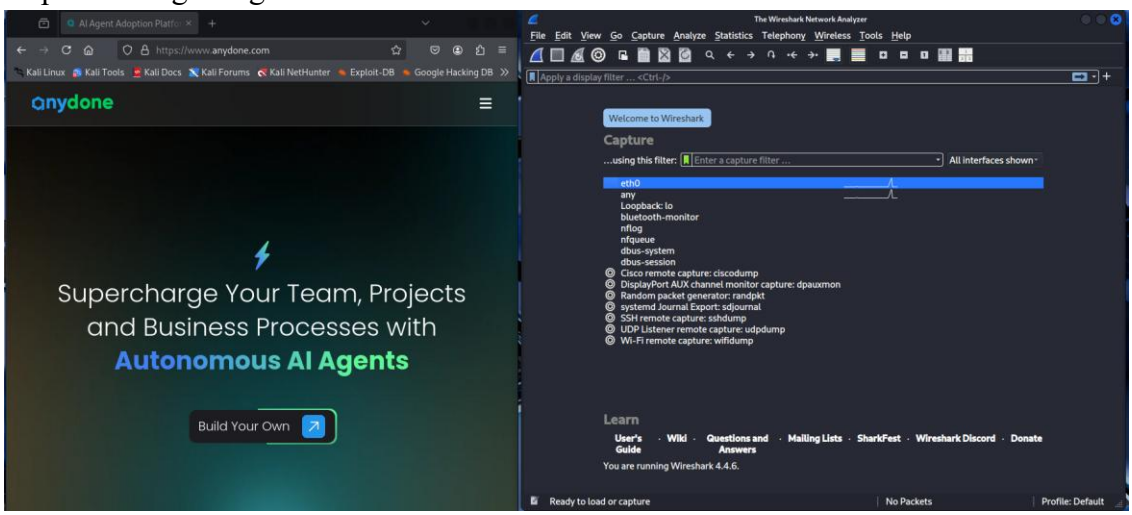
4.3. Sniff DNS with Wireshark

Filter with [tcp && ip.addr==34.36.210.35]

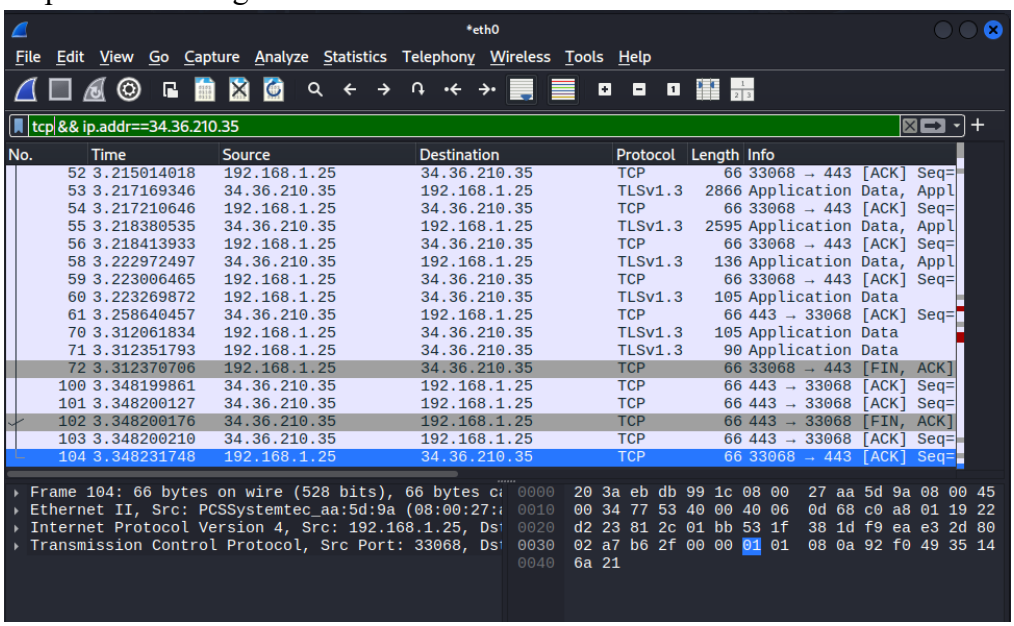
Step 1: Open terminal and enter “wireshark &”



Step 2: Start the recording, open the browser and visit www.anydone.com and after loading stop recording using Wireshark



Step 3: Filter using the command



4.4. Try basic Nikto scan

Syntax: nikto -h https://www.anydone.com

```
sayujya@kali: ~
File  Actions  Edit  View  Help
┌──(sayujya㉿kali)-[~]
└─$ nikto -h https://www.anydone.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          34.36.210.35
+ Target Hostname:    www.anydone.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=anydone.com
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Google Trust Services/CN=WR3
+ Start Time:         2025-05-10 13:19:11 (GMT-4)
---------------------------------------------------------------------------
+ Server: Google Frontend
+ /: Retrieved via header: 1.1 google.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Hea
ders/X-Frame-Options
+ /: Uncommon header 'x-cloud-trace-context' found, with contents: 7a89bb08ae9f4b1eadd292cfc8607bba.
+ /: Uncommon header 'x-anydone-cache' found, with contents: no.
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-U
S/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. S
ee: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /fhxEp0HT.php#: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the
 site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mis
sing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See:
 http://breachattack.com/
+ Hostname 'www.anydone.com' does not match certificate's names: anydone.com. See: https://cwe.mitre.org/data/definitions/297.html
+ /www_anydone_com.zip: Potentially interesting backup/cert file found. (NOTE: requested by IP address). See: https://cwe.mitre.org/data/definitions/530.html
+ /www.tar.bz2: Potentially interesting backup/cert file found. (NOTE: requested by IP address). See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.sql: Potentially interesting backup/cert file found. (NOTE: requested by IP address). See: https://cwe.mitre.org/data/definitions/530.html
+ /www.anydone.tar.bz2: Potentially interesting backup/cert file found. (NOTE: requested by IP address). See: https://cwe.mitre.org/data/definitions/530.html
+ /www.alz: Potentially interesting backup/cert file found. (NOTE: requested by IP address). See: https://cwe.mitre.org/data/definitions/530.html
+ /site.war: Potentially interesting backup/cert file found. (NOTE: requested by IP address). See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.pem: Potentially interesting backup/cert file found. (NOTE: requested by IP address). See: https://cwe.mitre.org/data/definitions/530.html
+ /anydone.alz: Potentially interesting backup/cert file found. (NOTE: requested by IP address). See: https://cwe.mitre.org/data/definitions/530.html
+ /34.36.210.35.tar.bz2: Potentially interesting backup/cert file found. (NOTE: requested by IP address). See: https://cwe.mitre.org/data/definitions/530.html
```