

1. Cài đặt công cụ:

a. tcpdump:

- Sử dụng câu lệnh: `sudo apt install tcpdump` trên kali linux

```
(chu@chu)-[~]  
$ sudo apt install tcpdump  
Reading package lists ... Done  
Building dependency tree ... Done  
Reading state information ... Done  
tcpdump is already the newest version (4.99.4-3).  
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

b. wireshark

- Sử dụng câu lệnh: `sudo apt install wireshark`

```
(chu@chu)-[~]  
$ sudo apt install wireshark  
Reading package lists ... Done  
Building dependency tree ... Done  
Reading state information ... Done  
wireshark is already the newest version (4.2.0-1).  
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

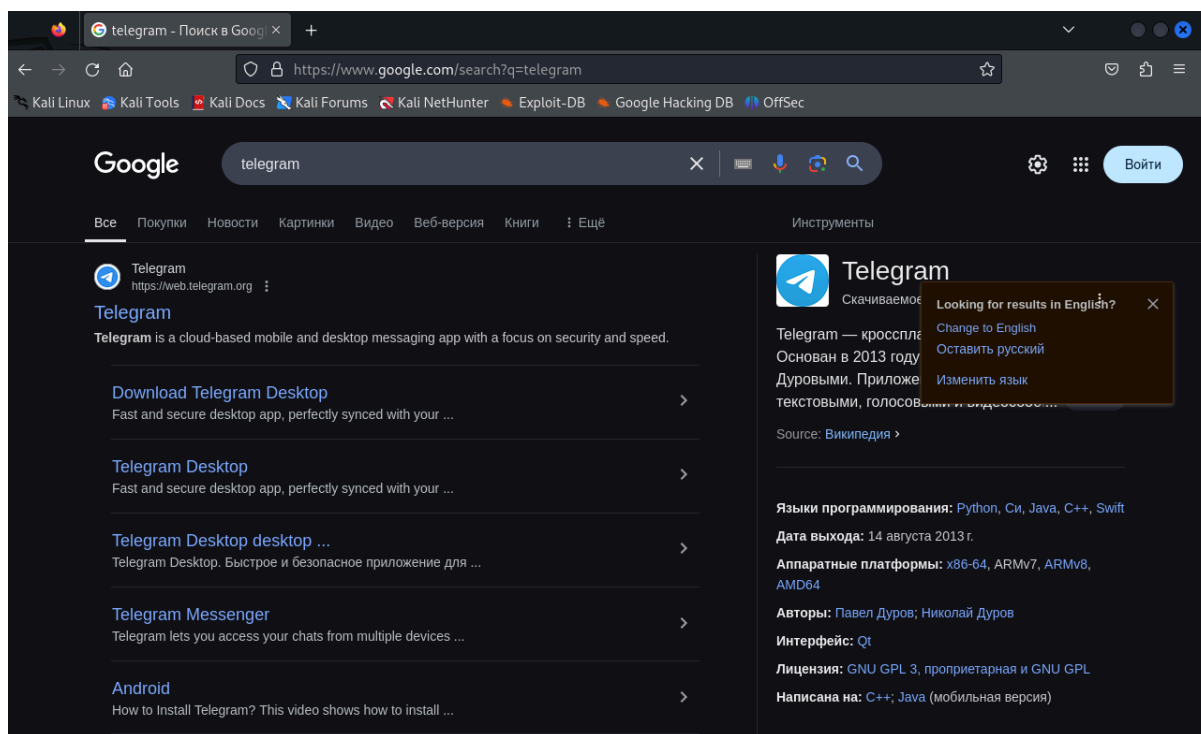
2. Phân tích lưu lượng mạng thông qua tcpdump

- Cú pháp để phân tích lưu lượng mạng và lưu kết quả vào file:

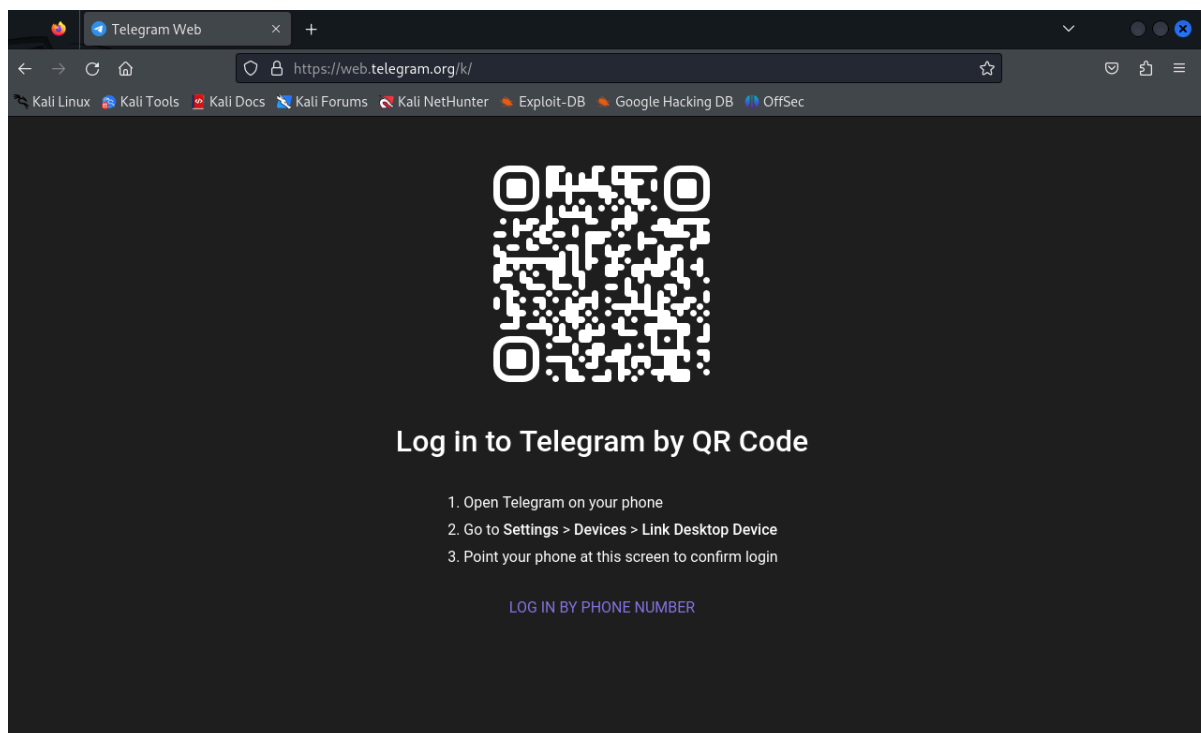
`sudo tcpdump -w telegram_tcpdump.pcap`

```
(chu@chu)-[~/Desktop]  
$ sudo tcpdump -w telegram_tcpdump.pcap  
[sudo] password for chu:  
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes  
█
```

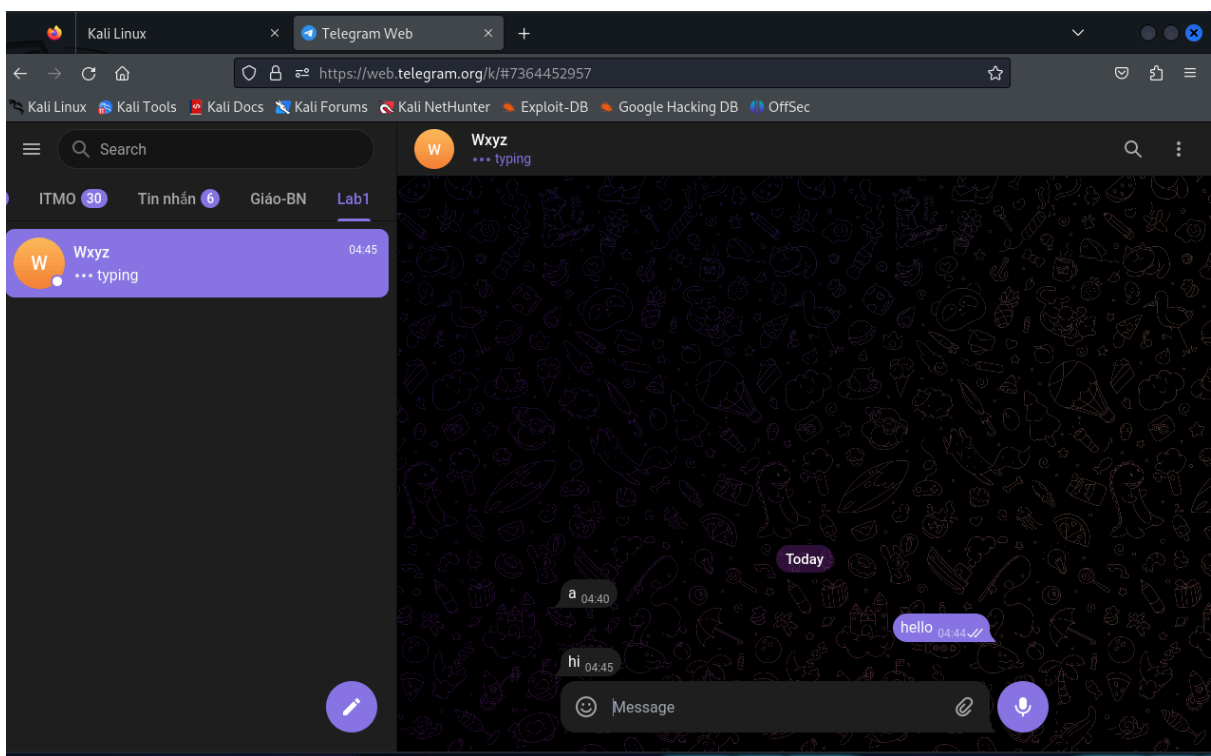
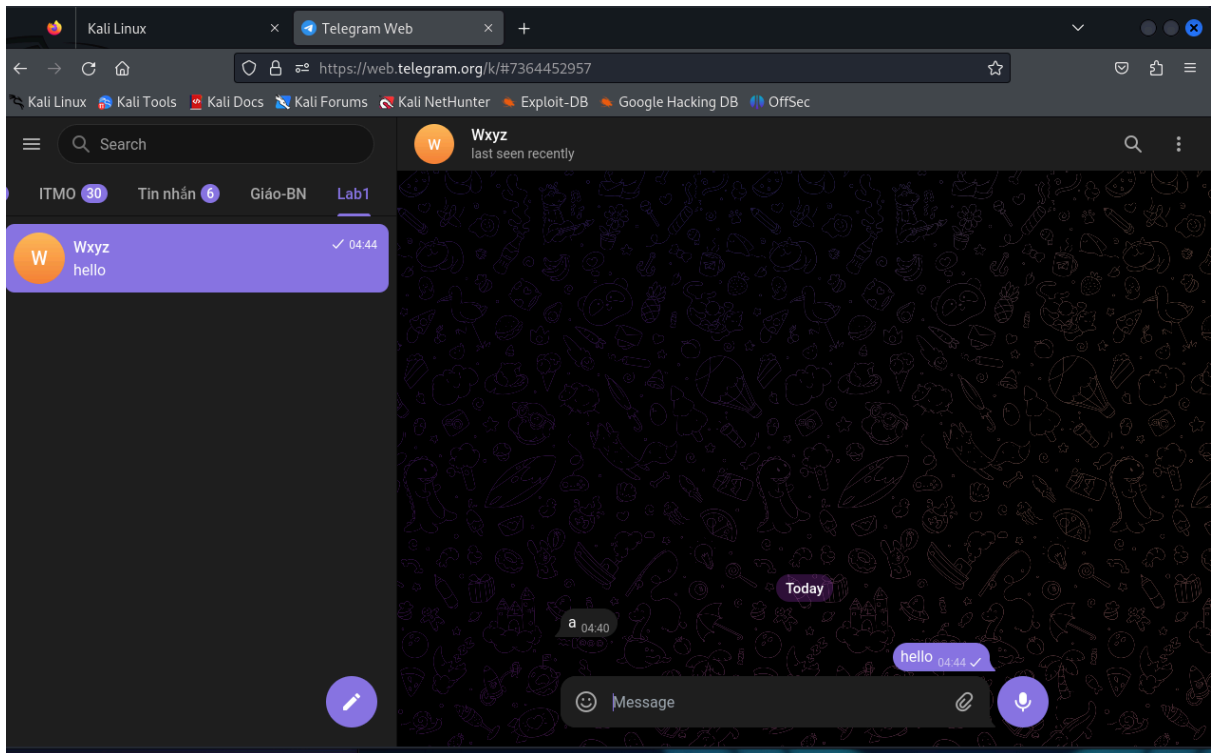
- Truy cập vào Firefox và tìm trang web telegram



- Tiến hành đăng nhập bằng cách quét QR code



- Tiến hành gửi và nhận tin nhắn



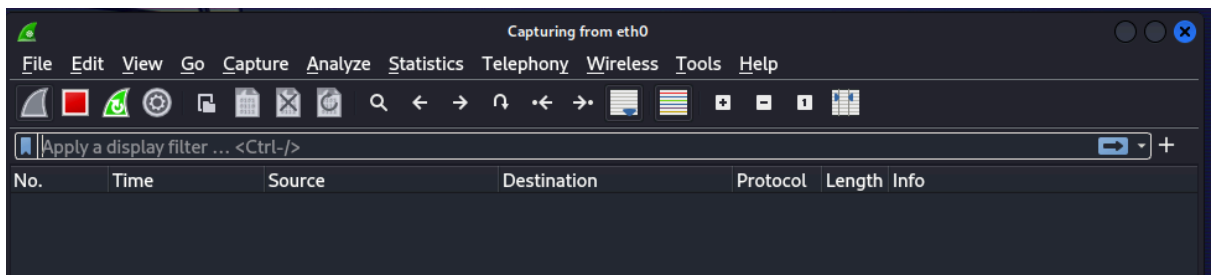
- sau đó nhấn tổ hợp phím Ctrl + C để kết thúc quá trình quét lưu lượng mạng

```
(chu@chu)-[~/Desktop]
$ sudo tcpdump -w telegram_tcpdump.pcap
[sudo] password for chu:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C3429 packets captured
3429 packets received by filter
0 packets dropped by kernel
```

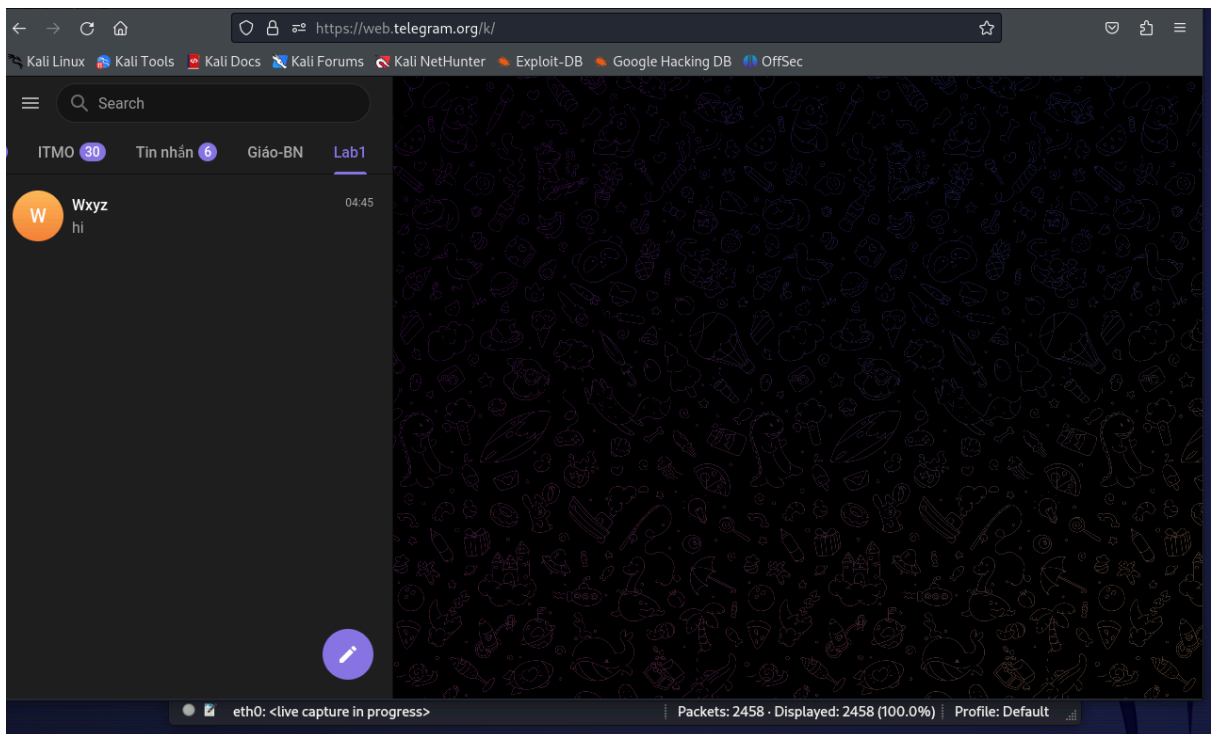
### 3. Phân tích lưu lượng mạng bằng công cụ Wireshark

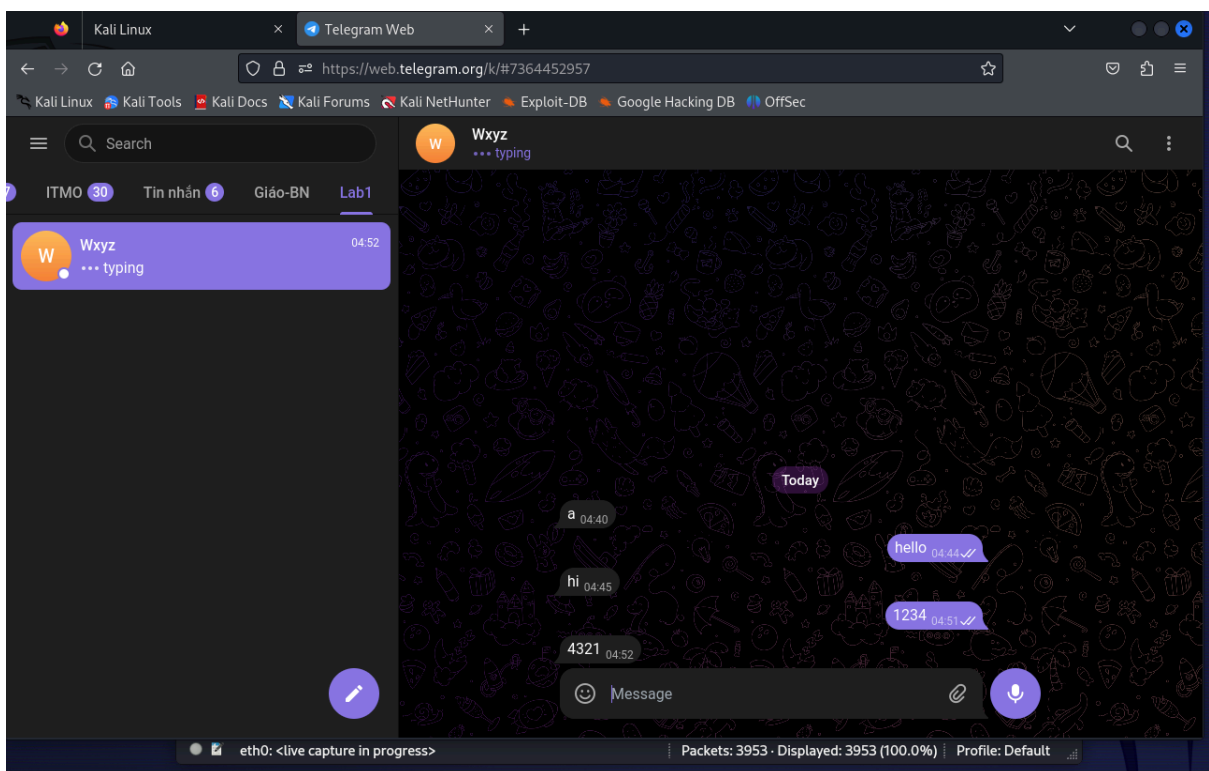
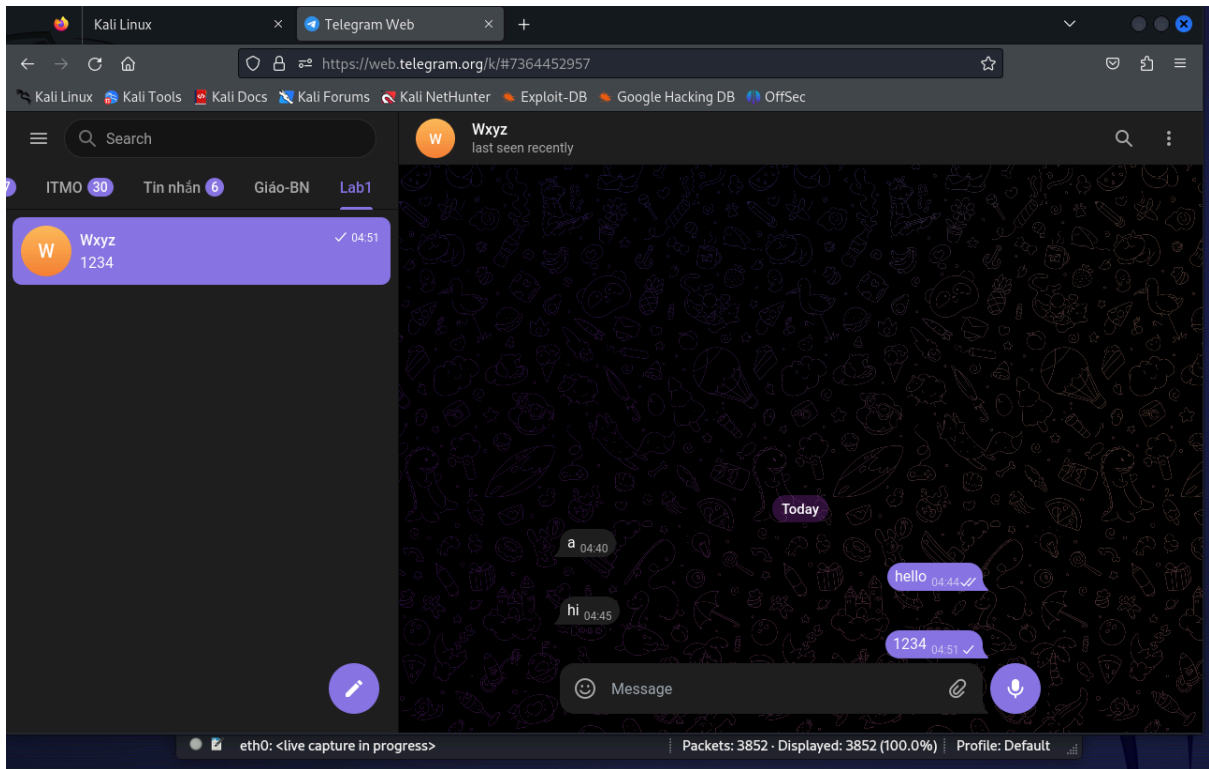
- Mở ứng dụng Wireshark và thực hiện như sau để quét lưu lượng mạng:

Chọn Capture -> Start hoặc nhấn tổ hợp phím Ctrl + E



- Sau đó mở trình duyệt và đăng nhập tương tự như thực hiện bằng tcpdump ở trên





- Sau đó tắt trình duyệt và dừng quét



telegram\_wireshark.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
4043	128.420720496	10.0.2.15	149.154.167.99	TCP	54	47970 → 443 [RST] Seq=
4044	128.491288683	34.117.188.166	10.0.2.15	TCP	60	443 → 47370 [FIN, ACK]
4045	128.491290639	34.107.243.93	10.0.2.15	TCP	60	443 → 51098 [FIN, ACK]
4046	128.491313267	10.0.2.15	34.117.188.166	TCP	54	47370 → 443 [ACK] Seq=
4047	128.491333102	10.0.2.15	34.107.243.93	TCP	54	51098 → 443 [ACK] Seq=
4048	128.496864252	34.107.243.93	10.0.2.15	TCP	60	443 → 51100 [FIN, ACK]
4049	128.496879058	10.0.2.15	34.107.243.93	TCP	54	51100 → 443 [ACK] Seq=
4050	128.510215390	142.251.141.35	10.0.2.15	TCP	60	80 → 52302 [FIN, ACK]
4051	128.510247238	10.0.2.15	142.251.141.35	TCP	54	52302 → 80 [ACK] Seq=8
4052	128.522867836	149.154.167.99	10.0.2.15	TCP	60	443 → 47956 [FIN, ACK]
4053	128.522899963	10.0.2.15	149.154.167.99	TCP	54	47956 → 443 [ACK] Seq=
4054	128.528230250	149.154.167.99	10.0.2.15	TCP	60	443 → 47946 [FIN, ACK]
4055	128.528232764	149.154.167.99	10.0.2.15	TCP	60	443 → 47966 [FIN, ACK]
4056	128.528234999	149.154.167.99	10.0.2.15	TCP	60	443 → 47962 [FIN, ACK]
4057	128.528264612	10.0.2.15	149.154.167.99	TCP	54	47946 → 443 [ACK] Seq=
4058	128.528287519	10.0.2.15	149.154.167.99	TCP	54	47966 → 443 [ACK] Seq=
4059	128.528304561	10.0.2.15	149.154.167.99	TCP	54	47962 → 443 [ACK] Seq=

▶ Frame 1: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface eth0, id 0  
 ▶ Ethernet II, Src: PCSSystemtec\_5a:5f:f0 (08:00:27:5a:5f:f0), Dst: 52:55:0a:00:02:03 (52:55:0a:00:02:03)  
 ▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3  
 ▶ User Datagram Protocol, Src Port: 57260, Dst Port: 53  
 ▶ Domain Name System (query)

4. Tìm địa chỉ IP
  - a. Tìm địa chỉ IP của máy
  - Sử dụng lệnh ifconfig

```

chu@chu: ~/Desktop
File Actions Edit View Help
-rw-r--r-- 1 tcpdump tcpdump 15010446 Feb 16 04:45 teleram_tcpdump.pcap

(chu@chu)-[~/Desktop]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fd00::a00:27ff:fe5a:5ff0 prefixlen 64 scopeid 0<global>
    inet6 fe80::a00:27ff:fe5a:5ff0 prefixlen 64 scopeid 0<20<link>
    inet6 fd00::f3f6:dfc0:d362:d321 prefixlen 64 scopeid 0<0<global>
    ether 08:00:27:5a:5f:f0 txqueuelen 1000 (Ethernet)
    RX packets 27924 bytes 25775361 (24.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 14668 bytes 1953715 (1.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 24 bytes 1240 (1.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24 bytes 1240 (1.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
  
```

Ta nhận ra rằng máy chúng ta đang sử dụng giao diện mạng eth0 với địa chỉ IPv4 là 10.0.2.15

- b. Tìm địa chỉ của trang web Telegram

- Ta sử dụng công cụ nslookup

```
(chu@chu)-[~/Desktop]
$ nslookup telegram.org

Server:          10.0.2.3
Address:         10.0.2.3#53

Non-authoritative answer:
Name:   telegram.org
Address: 149.154.167.99
Name:   telegram.org
Address: 2001:67c:4e8:f004::9
```

- Chúng ta thấy rằng trang web Telegram có địa chỉ là 159.154.167.99

## 5. Phân tích lưu lượng mạng bằng công cụ tcpdump.

Xem rõ hơn ở đây:

[https://github.com/CHu292/SOC/blob/main/M%E1%BA%A1ng%20m%C3%A1y%20t%C3%ADnh%20v%C3%A0%20ki%E1%BB%83m%20so%C3%A1t%20an%20ninh%20trong%20m%E1%BA%A1ng%20m%C3%A1y%20t%C3%ADnh/Lab1/tcpdump\\_and\\_wireshark.md#2-m%E1%BB%9F-wireshark-v%C3%A0-b%E1%BA%Aft-g%C3%B3i-tin](https://github.com/CHu292/SOC/blob/main/M%E1%BA%A1ng%20m%C3%A1y%20t%C3%ADnh%20v%C3%A0%20ki%E1%BB%83m%20so%C3%A1t%20an%20ninh%20trong%20m%E1%BA%A1ng%20m%C3%A1y%20t%C3%ADnh/Lab1/tcpdump_and_wireshark.md#2-m%E1%BB%9F-wireshark-v%C3%A0-b%E1%BA%Aft-g%C3%B3i-tin)

- Chúng ta xem nội dung file với 20 dòng cuối cùng:

```
(chu@chu)-[~/Desktop]
$ tcpdump -r telegram_tcpdump.pcap | tail -n 20
reading from file telegram_tcpdump.pcap, link-type EN10MB (Ethernet), snapshot length 262144
06:09:59.010199 IP 149.154.167.99.https > 10.0.2.15.52176: Flags [F.], seq 7026, ack 1254, win 65535, length 0
06:09:59.010199 IP 149.154.167.99.https > 10.0.2.15.45040: Flags [F.], seq 8060, ack 1475, win 65535, length 0
06:09:59.010200 IP 149.154.167.99.https > 10.0.2.15.45024: Flags [F.], seq 218003, ack 1849, win 65535, length 0
06:09:59.010215 IP 10.0.2.15.52176 > 149.154.167.99.https: Flags [.], ack 7027, win 63360, length 0
06:09:59.010228 IP 10.0.2.15.45040 > 149.154.167.99.https: Flags [.], ack 8061, win 63360, length 0
06:09:59.010232 IP 10.0.2.15.45024 > 149.154.167.99.https: Flags [.], ack 218004, win 36640, length 0
06:09:59.025994 IP 149.154.174.100.https > 10.0.2.15.48886: Flags [P.], seq 5704:6552, ack 1410, win 65535, length 848
06:09:59.025995 IP 149.154.167.99.https > 10.0.2.15.52184: Flags [F.], seq 6995, ack 1249, win 65535, length 0
06:09:59.026015 IP 10.0.2.15.48886 > 149.154.174.100.https: Flags [R], seq 2078181254, win 0, length 0
06:09:59.026037 IP 10.0.2.15.52184 > 149.154.167.99.https: Flags [.], ack 6996, win 63360, length 0
06:09:59.148877 IP 149.154.174.100.https > 10.0.2.15.44660: Flags [P.], seq 93234:93296, ack 5343, win 65535, length 62
06:09:59.148877 IP 149.154.174.100.https > 10.0.2.15.44660: Flags [F.], seq 93296, ack 5343, win 65535, length 0
06:09:59.148896 IP 10.0.2.15.44660 > 149.154.174.100.https: Flags [R], seq 605923747, win 0, length 0
06:09:59.148916 IP 10.0.2.15.44660 > 149.154.174.100.https: Flags [R], seq 605923747, win 0, length 0
06:09:59.149028 IP 149.154.174.100.https > 10.0.2.15.44660: Flags [R.], seq 4208439295, ack 5343, win 0, length 0
06:09:59.156335 IP 149.154.174.100.https > 10.0.2.15.48864: Flags [P.], seq 124218:124280, ack 5522, win 65535, length 62
06:09:59.156335 IP 149.154.174.100.https > 10.0.2.15.48864: Flags [F.], seq 124280, ack 5522, win 65535, length 0
06:09:59.156349 IP 10.0.2.15.48864 > 149.154.174.100.https: Flags [R], seq 112037241, win 0, length 0
06:09:59.156365 IP 10.0.2.15.48864 > 149.154.174.100.https: Flags [R], seq 112037241, win 0, length 0
06:09:59.156494 IP 149.154.174.100.https > 10.0.2.15.48864: Flags [R.], seq 4207479295, ack 5522, win 0, length 0
```

- Tìm các gói tin thực hiện quy tắc 3 bước ( three-way handshake)

```
(chu@chu) [~/Desktop]
$ tcpdump -i telegram_tcpdump.pcap 'tcp[tcpflags] & (tcp-syn|tcp-ack) != 0' and host 10.0.2.15 and host 149.154.167.99 | head -n 20
reading from file telegram_tcpdump.pcap, link-type EN10MB (Ethernet), snapshot length 262144
06:09:06.910684 IP 10.0.2.15.45018 > 149.154.167.99.https: Flags [S], seq 640055681, win 64240, options [mss 1460,sackOK,TS val 3749582594 ecr 0,nop,wscale 7], length 0
06:09:06.910779 IP 10.0.2.15.45024 > 149.154.167.99.https: Flags [S], seq 2799946822, win 64240, options [mss 1460,sackOK,TS val 3749582594 ecr 0,nop,wscale 7], length 0
06:09:06.929934 IP 10.0.2.15.45038 > 149.154.167.99.https: Flags [S], seq 1681089595, win 64240, options [mss 1460,sackOK,TS val 3749582614 ecr 0,nop,wscale 7], length 0
06:09:07.025976 IP 149.154.167.99.https > 10.0.2.15.45024: Flags [S.], seq 79552801, ack 2799946823, win 65535, options [mss 1460], length 0
06:09:07.026011 IP 10.0.2.15.45024 > 149.154.167.99.https: Flags [S.], ack 1, win 64240, length 0
06:09:07.028124 IP 10.0.2.15.45024 > 149.154.167.99.https: Flags [P.], seq 1:518, ack 1, win 64240, length 517
06:09:07.028312 IP 149.154.167.99.https > 10.0.2.15.45024: Flags [S.], ack 518, win 65535, length 0
06:09:07.028565 IP 149.154.167.99.https > 10.0.2.15.45018: Flags [S.], seq 79616001, ack 640055682, win 65535, options [mss 1460], length 0
06:09:07.028582 IP 10.0.2.15.45018 > 149.154.167.99.https: Flags [S.], ack 1, win 64240, length 0
06:09:07.029963 IP 10.0.2.15.45018 > 149.154.167.99.https: Flags [P.], seq 1:518, ack 1, win 64240, length 517
06:09:07.029910 IP 149.154.167.99.https > 10.0.2.15.45018: Flags [S.], ack 518, win 65535, length 0
06:09:07.038079 IP 149.154.167.99.https > 10.0.2.15.45038: Flags [S.], seq 79680001, ack 1681089596, win 65535, options [mss 1460], length 0
06:09:07.038111 IP 10.0.2.15.45038 > 149.154.167.99.https: Flags [S.], ack 1, win 64240, length 0
06:09:07.041155 IP 10.0.2.15.45038 > 149.154.167.99.https: Flags [P.], seq 1:518, ack 1, win 64240, length 517
06:09:07.041384 IP 149.154.167.99.https > 10.0.2.15.45038: Flags [S.], ack 518, win 65535, length 0
06:09:07.141572 IP 149.154.167.99.https > 10.0.2.15.45024: Flags [P.], seq 1:2457, ack 518, win 65535, length 2456
06:09:07.141806 IP 10.0.2.15.45024 > 149.154.167.99.https: Flags [S.], ack 2457, win 63360, length 0
06:09:07.143637 IP 149.154.167.99.https > 10.0.2.15.45024: Flags [P.], seq 2457:4097, ack 518, win 65535, length 1640
06:09:07.143451 IP 10.0.2.15.45024 > 149.154.167.99.https: Flags [S.], ack 4097, win 63360, length 0
06:09:07.145148 IP 149.154.167.99.https > 10.0.2.15.45024: Flags [P.], seq 4097:5698, ack 518, win 65535, length 1601
tcpdump: Unable to write output: Broken pipe
```

## Xác định các gói tin bắt tay TCP (3-Way Handshake)

Quá trình bắt tay TCP gồm:

1. **Gói SYN** – Máy khách gửi yêu cầu kết nối.
2. **Gói SYN-ACK** – Máy chủ phản hồi yêu cầu.
3. **Gói ACK** – Máy khách xác nhận, kết nối hoàn tất.

### a. Gói SYN (Máy khách gửi yêu cầu kết nối):

06:09:06.910684 IP 10.0.2.15.45018 > 149.154.167.99.https: Flags [S], seq 640055681, win 64240, options [mss 1460,sackOK,TS val 3749582594 ecr 0,nop,wscale 7], length 0

06:09:06.910779 IP 10.0.2.15.45024 > 149.154.167.99.https: Flags [S], seq 2799946822, win 64240, options [mss 1460,sackOK,TS val 3749582594 ecr 0,nop,wscale 7], length 0

06:09:06.929394 IP 10.0.2.15.45038 > 149.154.167.99.https: Flags [S], seq 1681089596, win 64240, options [mss 1460,sackOK,TS val 3749582614 ecr 0,nop,wscale 7], length 0

**Ý nghĩa:**

- Máy khách (**10.0.2.15**) gửi yêu cầu kết nối đến máy chủ Telegram (**149.154.167.99**).
- **Cổng nguồn:** **45018**, **45024**, **45038** (cổng ngẫu nhiên do hệ thống chọn).
- **Cổng đích:** **443** (HTTPS).
- **Cờ TCP:** **[S]** (SYN) → Bắt đầu kết nối.



### b. Gói SYN-ACK (Máy chủ phản hồi)

06:09:07.025916 IP 149.154.167.99.https > 10.0.2.15.45024: Flags [S.], seq 79552001, ack 2799946823, win 65535, options [mss 1460], length 0

Ý nghĩa:

- Máy chủ Telegram (**149.154.167.99**) phản hồi gói SYN từ máy khách (**10.0.2.15**).
- **Cổng nguồn: 443** (HTTPS).
- **Cổng đích: 45024** (khớp với gói SYN trước đó).
- **Cờ TCP: [S.]** (SYN-ACK) → Máy chủ xác nhận yêu cầu.
- **Số thứ tự (Seq): 79552001**
- **Số xác nhận (Ack): 2799946823** → Xác nhận đã nhận gói **SYN** từ máy khách.

### c. Gói ACK (Máy khách xác nhận kết nối)

06:09:07.026011 IP 10.0.2.15.45024 > 149.154.167.99.https: Flags [.], ack 1, win 64240, length 0

Ý nghĩa:

- Máy khách (**10.0.2.15**) xác nhận rằng nó đã nhận được gói SYN-ACK từ máy chủ (**149.154.167.99**).
- **Cổng nguồn: 45024**.
- **Cổng đích: 443**.
- **Cờ TCP: [.]** (ACK) → Máy khách xác nhận kết nối thành công.
- **Ack=1** → Xác nhận thành công với máy chủ.

### Kết luận

✅ Quá trình bắt tay TCP 3 bước đã hoàn tất!

- **Gói SYN:** Máy khách gửi yêu cầu kết nối.
- **Gói SYN-ACK:** Máy chủ phản hồi xác nhận.
- **Gói ACK:** Máy khách xác nhận lại.

 Sau bước này, kết nối TCP đã thiết lập, dữ liệu HTTPS có thể được truyền tải giữa máy khách và Telegram.

## 6. Phân tích lưu lượng mạng bằng Wireshark

ip.addr==149.154.167.99						
No.	Time	Source	Destination	Protocol	Length	Info
159	9.452334863	10.0.2.15	149.154.167.99	TCP	54	47946 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
160	9.453744260	10.0.2.15	149.154.167.99	TLSv1.3	571	Client Hello (SNI=web.telegram.org)
161	9.453981162	149.154.167.99	10.0.2.15	TCP	60	443 → 47946 [ACK] Seq=1 Ack=518 Win=65535 Len=0
162	9.456357162	149.154.167.99	10.0.2.15	TCP	60	443 → 47930 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
163	9.456398229	10.0.2.15	149.154.167.99	TCP	54	47930 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
164	9.457952337	10.0.2.15	149.154.167.99	TLSv1.3	571	Client Hello (SNI=web.telegram.org)
165	9.458164096	149.154.167.99	10.0.2.15	TCP	60	443 → 47930 [ACK] Seq=1 Ack=518 Win=65535 Len=0
166	9.555701973	10.0.2.15	149.154.167.99	TCP	74	47954 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2651983202 TSecr=0 WS=128
167	9.567842062	149.154.167.99	10.0.2.15	TLSv1.3	1282	Server Hello, Change Cipher Spec, Application Data
168	9.567866865	10.0.2.15	149.154.167.99	TCP	54	47946 → 443 [ACK] Seq=518 Ack=1229 Win=63856 Len=0
169	9.568610814	149.154.167.99	10.0.2.15	TCP	4150	443 → 47946 [PSH, ACK] Seq=1229 Ack=518 Win=65535 Len=4096 [TCP segment of a reassembled PDU]
170	9.568625341	10.0.2.15	149.154.167.99	TCP	54	47946 → 443 [ACK] Seq=518 Ack=5325 Win=61920 Len=0
171	9.568763966	149.154.167.99	10.0.2.15	TLSv1.3	427	Application Data, Application Data, Application Data
172	9.568772567	10.0.2.15	149.154.167.99	TCP	54	47946 → 443 [ACK] Seq=518 Ack=5698 Win=63360 Len=0
173	9.579266359	149.154.167.99	10.0.2.15	TLSv1.3	1282	Server Hello, Change Cipher Spec, Application Data
174	9.579289546	10.0.2.15	149.154.167.99	TCP	54	47930 → 443 [ACK] Seq=518 Ack=1229 Win=63856 Len=0
175	9.579907562	149.154.167.99	10.0.2.15	TCP	2922	443 → 47930 [PSH, ACK] Seq=1229 Ack=518 Win=65535 Len=2868 [TCP segment of a reassembled PDU]
176	9.579921190	10.0.2.15	149.154.167.99	TCP	54	47930 → 443 [ACK] Seq=518 Ack=4097 Win=63360 Len=0
177	9.580809813	149.154.167.99	10.0.2.15	TLSv1.3	1655	Application Data, Application Data, Application Data
178	9.580824378	10.0.2.15	149.154.167.99	TCP	54	47930 → 443 [ACK] Seq=518 Ack=5698 Win=63360 Len=0
179	9.609241303	149.154.167.99	10.0.2.15	TCP	60	443 → 47930 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
182	9.609283665	10.0.2.15	149.154.167.99	TCP	54	47954 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
183	9.670533545	10.0.2.15	149.154.167.99	TLSv1.3	571	Client Hello (SNI=web.telegram.org)

Chúng ta sử dụng bộ lọc và tìm ra đc các gói

các gói tin cho quá trình **bắt tay 3 bước TCP hoàn chỉnh (TCP 3-Way Handshake)** giữa máy tính của bạn (**10.0.2.15**) và máy chủ Telegram (**149.154.167.99**).

## Xác định các gói tin trong quá trình bắt tay TCP

Quá trình bắt tay TCP bao gồm **3 bước**:

1. **SYN:** Máy khách (**10.0.2.15**) gửi gói tin **SYN** để bắt đầu kết nối.
2. **SYN, ACK:** Máy chủ (**149.154.167.99**) phản hồi bằng **SYN**, **ACK** để xác nhận yêu cầu.
3. **ACK:** Máy khách gửi **ACK** để hoàn tất quá trình bắt tay.

## Danh sách các gói tin liên quan đến quá trình bắt tay TCP

No.	Time	Source	Destination	Protocol	Info
166	9.555701073	10.0.2.15	149.154.167.9	TCP	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
181	9.669249303	149.154.167.9	10.0.2.15	TCP	[SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
182	9.669283665	10.0.2.15	149.154.167.9	TCP	[ACK] Seq=1 Ack=1 Win=64240 Len=0

## Phân tích chi tiết từng bước

### Bước 1: Máy khách gửi **SYN**

166 9.555701073 10.0.2.15 → 149.154.167.99 TCP 74 47954 → 443 [SYN] Seq=0  
Win=64240 Len=0 MSS=1460 SACK\_PERM TSval=2651903202 TSecr=0 WS=128

- **Máy nguồn:** 10.0.2.15 (máy của bạn)
- **Máy đích:** 149.154.167.99 (máy chủ Telegram)
- **Cổng nguồn:** 47954 (một cổng tạm thời được chọn ngẫu nhiên)
- **Cổng đích:** 443 (HTTPS)
- **Cờ TCP:** SYN (yêu cầu bắt đầu kết nối)
- **MSS=1460:** Maximum Segment Size (giới hạn kích thước gói tin)
- **SACK\_PERM:** Hỗ trợ Selective Acknowledgment (tăng hiệu suất)
- **WS=128:** Window Scaling Factor (tăng cửa sổ TCP)

### Bước 2: Máy chủ phản hồi **SYN, ACK**

181 9.669249303 149.154.167.99 → 10.0.2.15 TCP 60 443 → 47954 [SYN, ACK]  
Seq=0 Ack=1 Win=65535 Len=0 MSS=1460

- **Máy nguồn:** 149.154.167.99 (máy chủ Telegram)
- **Máy đích:** 10.0.2.15 (máy của bạn)

- Cổng nguồn: 443 (HTTPS)
  - Cổng đích: 47954
  - Cờ TCP: SYN, ACK (máy chủ xác nhận yêu cầu)
  - Ack=1: Xác nhận nhận gói SYN từ máy khách
  - MSS=1460: Giới hạn kích thước gói tin
- 

### Bước 3: Máy khách gửi ACK


182 9.669283665 10.0.2.15 → 149.154.167.99 TCP 54 47954 → 443 [ACK] Seq=1  
Ack=1 Win=64240 Len=0

- Máy nguồn: 10.0.2.15 (máy của bạn)
  - Máy đích: 149.154.167.99 (máy chủ Telegram)
  - Cổng nguồn: 47954
  - Cổng đích: 443 (HTTPS)
  - Cờ TCP: ACK (máy khách xác nhận kết nối)
  - Seq=1, Ack=1: Xác nhận hoàn tất quá trình bắt tay TCP
- 

### Kết luận

#### Quá trình bắt tay TCP 3 bước đã hoàn tất thành công!

- Gói SYN (#166): Máy khách gửi yêu cầu kết nối.
- Gói SYN, ACK (#181): Máy chủ phản hồi xác nhận.
- Gói ACK (#182): Máy khách xác nhận lại -> kết nối TCP được thiết lập.

 Sau bước này, dữ liệu sẽ được truyền qua HTTPS bằng TLS v1.3, như bạn thấy trong các gói tin Client Hello và Server Hello ngay sau đó.

### Kiểm tra thêm

Nếu bạn muốn kiểm tra thêm, bạn có thể lọc trong **Wireshark** bằng cách nhập:

```
tcp.flags.syn==1 || tcp.flags.ack==1
```

hoặc trên terminal bằng:

```
sudo tcpdump -i any host 149.154.167.99 and port 443
```