

MSSV: 21520417

HỌ TÊN: HUỖNH NGỌC QUÍ

- **PHẦN 1: Bắt gói và phân tích UDP**

1. Các trường (field) trong UDP header là:

- Source Port
- Destination Port
- Length
- Checksum

udp						
No.	Time	Source	Destination	Protocol	Length	Info
43	0.037856	fe80::84b:6183:c068...	ff02::fb	MDNS	195	Standard query 0x0000 PTR _companion-link._tcp.local, "QU" question PTR _sleep-proxy._udp.l
44	0.038073	172.30.113.152	224.0.0.251	MDNS	175	Standard query 0x0000 PTR _companion-link._tcp.local, "QU" question PTR _sleep-proxy._udp.l
45	0.039416	172.30.138.73	172.30.255.255	UDP	305	54915 → 54915 Len=263
46	0.039648	172.30.179.46	224.0.0.251	MDNS	364	Standard query response 0x0000 TXT PTR shenkha._companion-link._tcp.local AAAA, cache flush
47	0.040574	fe80::1062:4018:916...	ff02::fb	MDNS	384	Standard query response 0x0000 TXT PTR shenkha._companion-link._tcp.local AAAA, cache flush

> Frame 45: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on interface \Device\NPF_{A827C446-05D2-4D95-B2D2-3888749E8386}, id 0

> Ethernet II, Src: Chongqin_08:2b:a7 (40:23:43:08:2b:a7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Internet Protocol Version 4, Src: 172.30.138.73, Dst: 172.30.255.255

▼ User Datagram Protocol, Src Port: 54915, Dst Port: 54915

Source Port: 54915

Destination Port: 54915

Length: 271

Checksum: 0x3a91 [unverified]

[Checksum Status: Unverified]

[Stream index: 34]

> [Timestamps]

UDP payload (263 bytes)

> Data (263 bytes)

2. Độ dài của mỗi trường trong UDP header là:

- Sourt Port: 2 bytes
- Destination Port: 2 bytes
- Length: 2 bytes
- Checksum: 2 bytes

> Frame 45: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits)
> Ethernet II, Src: Chongqin_08:2b:a7 (40:23:43:08:2b:a7), Dst: Broadcast
> Internet Protocol Version 4, Src: 172.30.138.73, Dst: 172.30.255.255
▼ User Datagram Protocol, Src Port: 54915, Dst Port: 54915
Source Port: 54915
Destination Port: 54915
Length: 271
Checksum: 0x3a91 [unverified]
[Checksum Status: Unverified]
[Stream index: 34]
> [Timestamps]
UDP payload (263 bytes)
> Data (263 bytes)

Source Port (udp.srcport), 2 bytes

> Frame 45: 305 bytes on wire (2440 bits), 305 bytes captured (2440 b
> Ethernet II, Src: Chongqin_08:2b:a7 (40:23:43:08:2b:a7), Dst: Broad
> Internet Protocol Version 4, Src: 172.30.138.73, Dst: 172.30.255.25
▼ User Datagram Protocol, Src Port: 54915, Dst Port: 54915
Source Port: 54915
Destination Port: 54915
Length: 271
Checksum: 0x3a91 [unverified]
[Checksum Status: Unverified]
[Stream index: 34]
> [Timestamps]
UDP payload (263 bytes)
> Data (263 bytes)

Destination Port (udp.dstport), 2 bytes

```
> Frame 45: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on i
> Ethernet II, Src: Chongqin_08:2b:a7 (40:23:43:08:2b:a7), Dst: Broadcast (ff:
> Internet Protocol Version 4, Src: 172.30.138.73, Dst: 172.30.255.255
▼ User Datagram Protocol, Src Port: 54915, Dst Port: 54915
  Source Port: 54915
  Destination Port: 54915
  Length: 271
  Checksum: 0x3a91 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 34]
  > [Timestamps]
  UDP payload (263 bytes)
> Data (263 bytes)
```

Length in octets including this header and the data (udp.length), 2 bytes

```
> Frame 45: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on interfac
> Ethernet II, Src: Chongqin_08:2b:a7 (40:23:43:08:2b:a7), Dst: Broadcast (ff:ff:ff:f
> Internet Protocol Version 4, Src: 172.30.138.73, Dst: 172.30.255.255
▼ User Datagram Protocol, Src Port: 54915, Dst Port: 54915
  Source Port: 54915
  Destination Port: 54915
  Length: 271
  Checksum: 0x3a91 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 34]
  > [Timestamps]
  UDP payload (263 bytes)
> Data (263 bytes)
```

Details at: https://www.wireshark.org/docs/wsug_html_chunked/ChAdvChecksums.html (udp.checksum), 2 bytes

3. Giá trị của trường Length trong UDP header là độ dài toàn bộ gói tin UDP, bao gồm 8 bytes UDP header và 263 bytes của data.

Chứng minh:

$$\text{Length} = 8 + 263 = 271 \text{ (bytes)}$$

```
> Frame 59: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) o
> Ethernet II, Src: Chongqin_a9:ab:55 (c8:94:02:a9:ab:55), Dst: Broadcast (
> Internet Protocol Version 4, Src: 172.30.170.43, Dst: 172.30.255.255
▼ User Datagram Protocol, Src Port: 54915, Dst Port: 54915
  Source Port: 54915
  Destination Port: 54915
  Length: 271
  Checksum: 0x85d5 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 46]
  > [Timestamps]
  UDP payload (263 bytes)
> Data (263 bytes)
```

4. Số bytes lớn nhất mà payload của UDP có thể chứa:

$$\text{Max length payload} = \text{Max length} - 8 \text{ bytes header} = 2^{16} - 1 - 8 = 65527 \text{ bytes}$$

5. Giá trị lớn nhất có thể có của Port nguồn (Source Port): $2^{16} - 1 = 65535$

6. Xác định protocol number của UDP:

Hệ 10: 17

Hệ 16: 0x11

```
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0xa6cf [validation disabled]
[Header checksum status: Unverified]
Source Address: 172.30.170.43
Destination Address: 172.30.255.255
```

• PHẦN 2: Phân tích hành vi TCP

7. Địa chỉ IP của máy khách là 172.30.182.96 và TCP port là 62566

175	0.839837	172.30.182.96	128.119.245.12	TCP	66 62566 → 80 [SYN] Seq=0 Win=6424
176	0.866690	151.101.1.44	172.30.182.96	TCP	129 [TCP Retransmission] 443 → 6348
223	1.076639	128.119.245.12	172.30.182.96	TCP	66 80 → 62566 [SYN, ACK] Seq=0 Ack
224	1.076691	172.30.182.96	128.119.245.12	TCP	54 62566 → 80 [ACK] Seq=1 Ack=1 Wi
226	1.091307	172.30.182.96	142.251.220.14	TLSv1.2	133 Application Data

> Frame 175: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A827C446-05D2-4000-8000-000000000000}

> Ethernet II, Src: IntelCor_a2:48:06 (f0:9e:4a:a2:48:06), Dst: JuniperN_8c:35:b0 (44:f4:77:8c:35:b0)

> Internet Protocol Version 4, Src: 172.30.182.96, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 62566, Dst Port: 80, Seq: 0, Len: 0

8. Địa chỉ IP của gaia.cs.umass.edu là 128.119.245.12 và TCP port là 80

175	0.839837	172.30.182.96	128.119.245.12	TCP	66 62566 → 80 [SYN] Seq=0 Win=6424
176	0.866690	151.101.1.44	172.30.182.96	TCP	129 [TCP Retransmission] 443 → 6348
223	1.076639	128.119.245.12	172.30.182.96	TCP	66 80 → 62566 [SYN, ACK] Seq=0 Ac
224	1.076691	172.30.182.96	128.119.245.12	TCP	54 62566 → 80 [ACK] Seq=1 Ack=1 v
226	1.091307	172.30.182.96	142.251.220.14	TLSv1.2	133 Application Data

> Frame 175: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A827C446-05D2-4000-8000-000000000000}

> Ethernet II, Src: IntelCor_a2:48:06 (f0:9e:4a:a2:48:06), Dst: JuniperN_8c:35:b0 (44:f4:77:8c:35:b0)

> Internet Protocol Version 4, Src: 172.30.182.96, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 62566, Dst Port: 80, Seq: 0, Len: 0

9. TCP SYN segment sử dụng sequence number là 0 để tạo kết nối TCP giữa máy khách và gaia.cs.umass.edu. Trong trường Flats, SYN flag được đặt thành 1 cho biết rằng segment này là một TCP SYN segment

175	0.839837	172.30.182.96	128.119.245.12	TCP	66 62566 → 80 [SYN] Seq=0 Win=6424
176	0.866690	151.101.1.44	172.30.182.96	TCP	129 [TCP Retransmission] 443 → 6348
223	1.076639	128.119.245.12	172.30.182.96	TCP	66 80 → 62566 [SYN, ACK] Seq=0 Ack
224	1.076691	172.30.182.96	128.119.245.12	TCP	54 62566 → 80 [ACK] Seq=1 Ack=1 Wi

Transmission Control Protocol, Src Port: 62566, Dst Port: 80, Seq: 0, Len: 0

Source Port: 62566
Destination Port: 80
[Stream index: 3]
[Conversation completeness: Incomplete, ESTABLISHED (7)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 4157203874
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 = Header Length: 32 bytes (8)

Flags: 0x002 (SYN)

000. = Reserved: Not set
...0 = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...0 = Acknowledgment: Not set
....0... = Push: Not set
....0... = Reset: Not set
....1. = Syn: Set
....0 = Fin: Not set
[TCP Flags:S.]

10. Sequence number của SYNACK segment được gửi bởi gaia.cs.umass.edu đến máy khách là 0. Giá trị của Acknowledgement trong SYNACK segment là 1. Một segment sẽ được xác định là SYNACK segment nếu cả giá trị SYN flag và Acknowledgement flag trong segment được đặt thành 1.

175	0.839837	172.30.182.96	128.119.245.12	TCP	66 62566 → 80 [SYN] Seq=0 Win=64240 Len=0
176	0.866690	151.101.1.44	172.30.182.96	TCP	129 [TCP Retransmission] 443 → 63481 [FIN] Seq=443 Win=0 Len=0
223	1.076639	128.119.245.12	172.30.182.96	TCP	66 80 → 62566 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
224	1.076691	172.30.182.96	128.119.245.12	TCP	54 62566 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0

Transmission Control Protocol, Src Port: 80, Dst Port: 62566, Seq: 0, Ack: 1, Len: 0

Source Port: 80

Destination Port: 62566

[Stream index: 3]

[Conversation completeness: Incomplete, ESTABLISHED (7)]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 3269992850

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 4157203875

1000 = Header Length: 32 bytes (8)

Flags: 0x012 (SYN, ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion Window Reduced (CWR): Not set

.... .0.. = ECN-Echo: Not set

.....0 = Urgent: Not set

.... ..1 = Acknowledgment: Set

.... 0... = Push: Not set

.....0 = Reset: Not set

....1. = Syn: Set

....0 = Fin: Not set

[TCP Flags:A..S.]

11. Sequence number của TCP segment có chứa lệnh HTTP POST là: 1

No.	Time	Source	Destination	Protocol	Length	Info
921	3.194529	172.30.182.96	128.119.245.12	HTTP	56543	POST /wireshark-l
1081	3.795236	128.119.245.12	172.30.182.96	HTTP	831	HTTP/1.1 200 OK

> Frame 921: 56543 bytes on wire (452344 bits), 56543 bytes captured (452344 bits) on interface
> Ethernet II, Src: IntelCor_a2:48:06 (f0:9e:4a:a2:48:06), Dst: JuniperN_8c:35:b0 (44:f4:77:8c:35:b0)
> Internet Protocol Version 4, Src: 172.30.182.96, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 62556, Dst Port: 80, Seq: 96582, Ack: 1, Len: 56489
v [7 Reassembled TCP Segments (153070 bytes): #229(749), #230(13068), #371(27588), #613(31944),
[Frame: 229, payload: 0-748 (749 bytes)]
[Frame: 230, payload: 749-13816 (13068 bytes)]
[Frame: 371, payload: 13817-41404 (27588 bytes)]
[Frame: 613, payload: 41405-73348 (31944 bytes)]
[Frame: 616, payload: 73349-87868 (14520 bytes)]
[Frame: 618, payload: 87869-96580 (8712 bytes)]
[Frame: 921, payload: 96581-153069 (56489 bytes)]
[Segment count: 7]
[Reassembled TCP length: 153070]

Offset	Hex	ASCII
00000000	50 4f 53 54 20 2f 77 69 72 65 73 68 61 72 6b 2d	POST /wireshark-
00000010	6c 61 62 73 2f 6c 61 62 33 2d 31 2d 72 65 70 6c	labs/lab3-1-repl
00000020	79 2e 68 74 6d 20 48 54 54 50 2f 31 2e 31 0d 0a	y.htm HTTP/1.1..
00000030	48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d	Host: gaia.cs.um
00000040	61 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74	ass.edu. Connect
00000050	69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d	ion: keep-alive.
00000060	0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a	.Content-Length:
00000070	20 31 35 32 33 32 31 0d 0a 43 61 63 68 65 2d 43	152321. Cache-C
00000080	6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 3d	ontrol: max-age=
00000090	30 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63	0. Upgrade-Insec
000000a0	75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d	ure-Requests: 1.
000000b0	0a 4f 72 69 67 69 6e 3a 20 68 74 74 70 3a 2f 2f	.Origin: http://

No.	Time	Source	Destination	Protocol	Length	Info
228	1.091352	172.30.182.96	142.251.220.14	TLSv1.2	516	Application Data
229	1.092331	172.30.182.96	128.119.245.12	TCP	803	62556 → 80 [PSH, ACK] Seq=1 A
230	1.092430	172.30.182.96	128.119.245.12	TCP	13122	62556 → 80 [ACK] Seq=750 Ack=
263	1.303412	151.101.1.44	172.30.182.96	TCP	129	[TCP Retransmission] 443 → 63

> Frame 229: 803 bytes on wire (6424 bits), 803 bytes captured (6424 bits) on interface \Device\NPF_{A827C44
> Ethernet II, Src: IntelCor_a2:48:06 (f0:9e:4a:a2:48:06), Dst: JuniperN_8c:35:b0 (44:f4:77:8c:35:b0)
> Internet Protocol Version 4, Src: 172.30.182.96, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 62556, Dst Port: 80, Seq: 1, Ack: 1, Len: 749
Source Port: 62556
Destination Port: 80
[Stream index: 5]
[Conversation completeness: Incomplete (12)]
[TCP Segment Len: 749]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 686392096
[Next Sequence Number: 750 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 110485145

Offset	Hex	ASCII
0020	f5 0c f4 5c 00 50 28 e9 83 20 06 95 de 99 50 18	...P(.P.
0030	02 04 db 0a 00 00 50 4f 53 54 20 2f 77 69 72 65POST /wire
0040	73 68 61 72 6b 2d 6c 61 62 73 2f 6c 61 62 33 2d	shark-labs/lab3-
0050	31 2d 72 65 70 6c 79 2e 68 74 6d 20 48 54 50	1-reply.htm HTTP
0060	2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 67 61 69 61	/1.1..Host: gaia
0070	2e 63 73 2e 75 6d 61 73 73 2e 65 64 75 0d 0a 43	.cs.umass.edu..C