تمرین چهارم درس شبکه

سهیل محمودی

400130453

موضوع تمرین :

تحلیل ترافیک با Wireshark

Question1:

ابتدا از قسمت فیلتر پکت های TCP را فیلتر کردم و نیازی به Tcp.stream eq number نبود چون هر کدام از پکت ها مربوط به یک stream index بود و DHCP هم نداشتیم. با گذر از هر کدام از آن ها و مشاهده ی اطلاعات پکت ها هیچ flag وجود نداشت.
سپس با فیلتر کردن هر کدام از پروتکل های موجود از جمله IPV4, ICPM, UDP اطلاعات آن ها را مانند قبل بررسی شد. به همین ترتیب flag در پکت شماره ی ۱۵۱ پیدا شد. (از follow -> tcp stream هم استفاده شد که نتیجه ای نداشت)

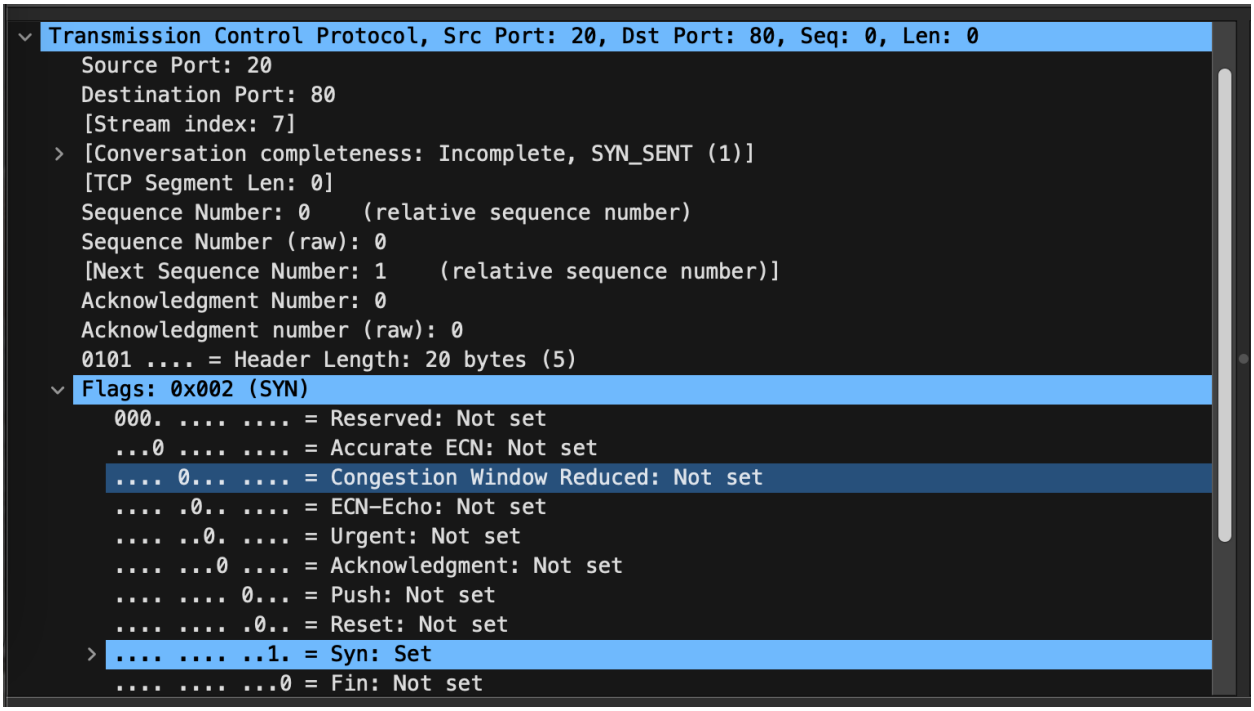
```
45 00 00 29 00 01 00 00  40 01 c9 dc 3e 66 85 6b   E··)···· @···>f·k
2f 1d be 08 08 00 74 23  00 00 00 00 46 6c 61 67   /·····t# ····Flag
7b 37 4b 4b 57 54 41 31  7d                        {7KKWTA1 }
```

Question2:

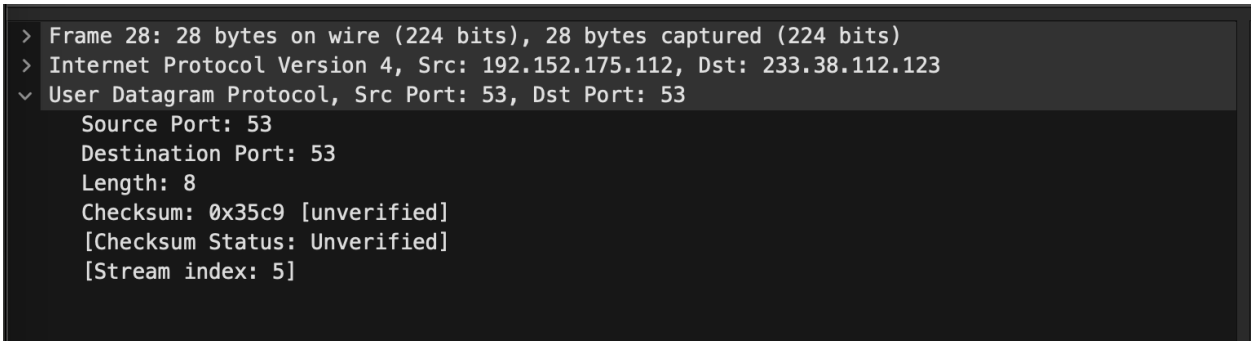
در این ترافیک ما پکت هایی داریم که از پروتکل های IPV4, ICPM, UDP, TCP است

```
> Frame 145: 53 bytes on wire (424 bits), 53 bytes captured (424 bits)
v Internet Protocol Version 4, Src: 119.117.35.129, Dst: 249.71.65.157
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 53
    Identification: 0x0001 (1)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: IPv6 Hop-by-Hop Option (0)
    Header Checksum: 0xa4ed [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 119.117.35.129
    Destination Address: 249.71.65.157
> IPv6 Hop-by-Hop Option
> IPv6 Hop-by-Hop Option
> [Malformed Packet: IPv6 Hop-by-Hop]
```

در این عکس اطلاعات یک malformed packet را داریم که از آیپی فرستنده و گیرنده را میتوان مشاهده کرد.

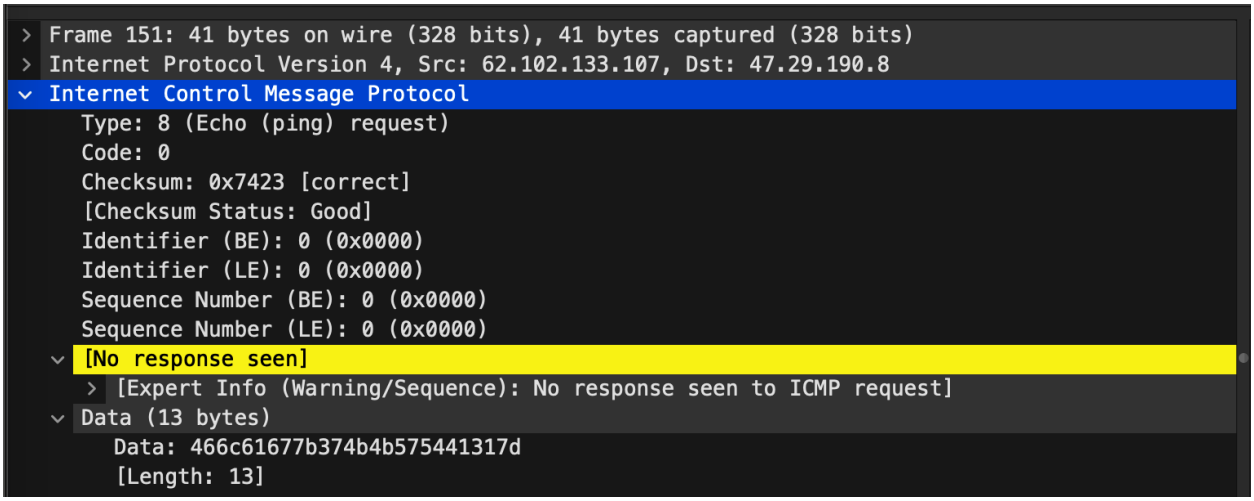


همانطور که دیده می شود stream index این پکت ۷ است و پروتکل آن TCP است. یک SYN flag مشاهده می کنیم که این فلگ ها در handshake اولیه ی پروتکل TCP استفاده می شوند و در اولین پکتی که از client برای سرور ارسال می شود قرار می گیرد تا اتصال برقرار شود.



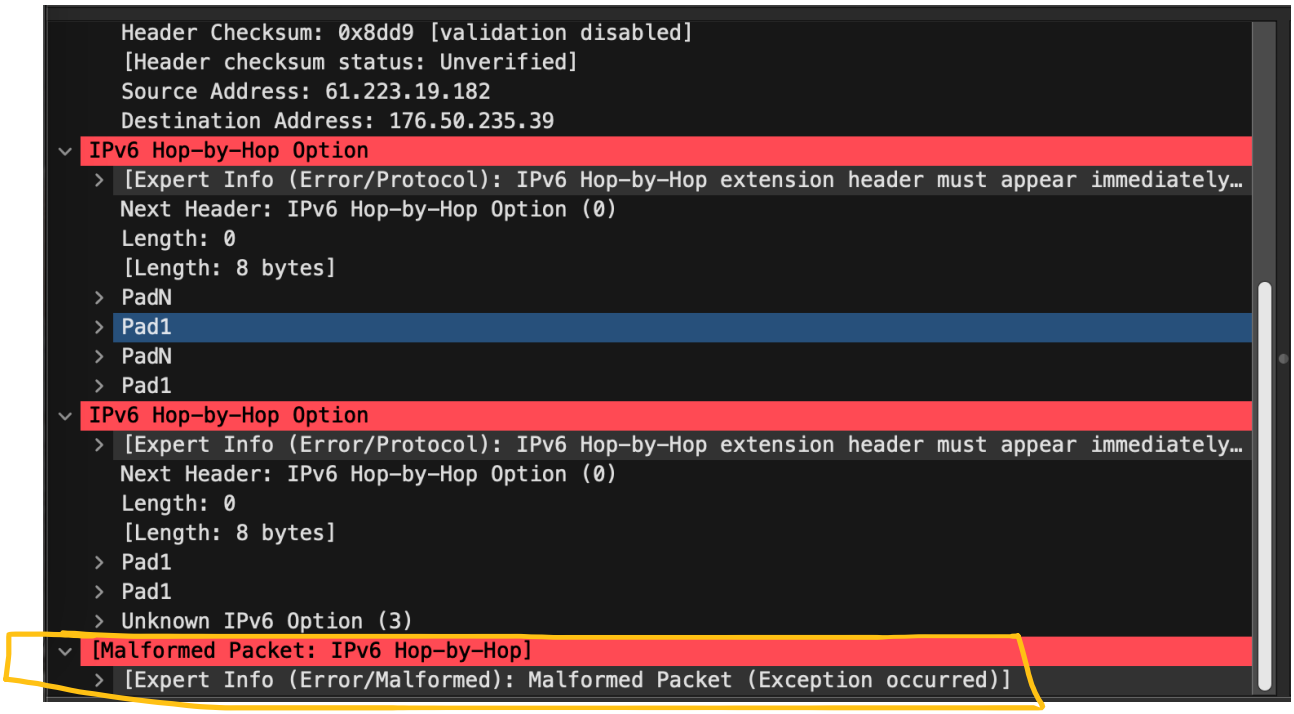
در پکت شماره ۲۸ که در پروتکل UDP است هم میتوانیم پورت مبدا و مقصد همچنین مقدار checksum را مشاهده کنیم.

(چک‌سام یک مقدار است که برای تأیید یکپارچگی داده‌ها و تشخیص خطاها در انتقال داده‌ها استفاده می‌شود. این یک محاسبه ریاضی است که روی داده‌ها انجام می‌شود، معمولاً یک بلوک داده یا یک بسته، تا یک مقدار ایجاد کند که محتویات داده‌ها را نشان دهد.)



اینجا یک Internet Control Message Protocol را مشاهده می کنیم که یک درخواست ping به هدف ارسال شده تا در دسترس بودن و اتصال شبکه را بررسی کند اما هیچ جوابی پاسخی در یک دوره ی زمانی مشخص دریافت نکرده است که می تواند دلایل مختلفی داشته باشد مانند:

1. هدف غیرقابل دسترسی باشد: مقصد ممکن است آفلاین باشد، خاموش باشد، یا به دلیل مسائل شبکه قابل دسترسی نباشد.
2. مسدود شدن توسط فایروال: ممکن است یک فایروال یا تنظیمات امنیتی شبکه روی مقصد یا در مسیر شبکه باشد که بسته‌های ICMP را مسدود می‌کند.
3. ازدحام یا خرابی شبکه: ممکن است ازدحام شبکه یا مسائل دیگری وجود داشته باشد که مانع از رسیدن بسته ICMP به هدف یا برگشت پاسخ شود.
4. مهلت زمانی: گاهی اوقات هدف در پاسخ‌دهی کند است یا اتصال شبکه تأخیر دارد، که باعث می‌شود درخواست قبل از دریافت پاسخ منقضی شود.



در این قسمت هم متوجه می شویم که یک خطا رخ داده است و فرآیند تحلیل را مختل کرده است. این بسته مطابق با ساختار مورد نظر پروتکل خود (IPV4) نیست که ممکن است به دلیل این باشد که داده های خراب دارد و یا بسته ناقص و کوتاه است. به این ترتیب wireshark در تلاش برای پردازش پکت با یک استثنا یا خطا مواجه شده است.