

**NAMA**

**NIM**

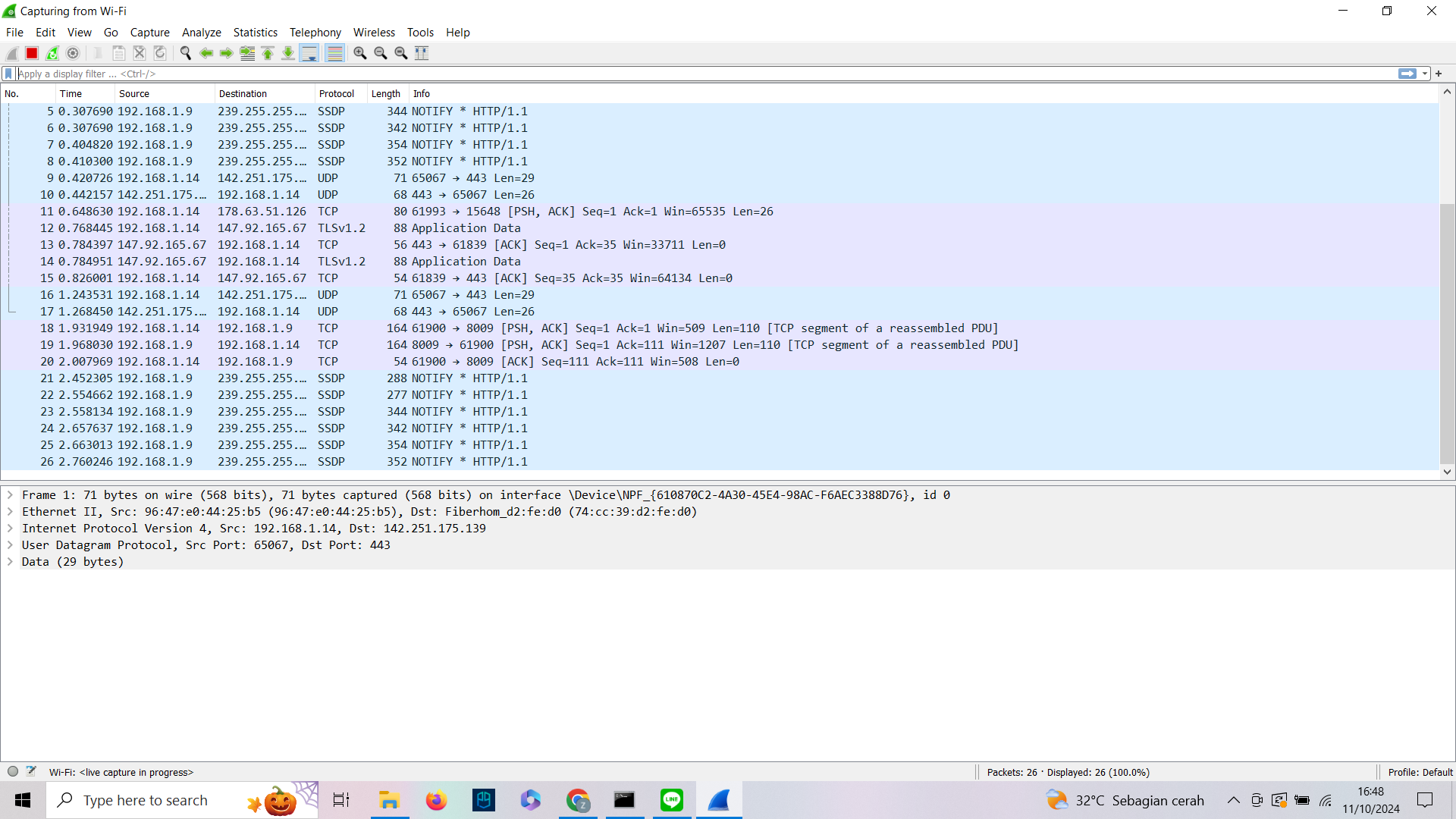
**UTS - SECURITY AND COMPUTER NETWORK LAB**

Wireshark merupakan perangkat lunak untuk analisis, checking, sniffing paket jaringan di dalam komputer. Dengan menggunakan Wireshark memungkinkan kita menganalisis setiap paket data yang melewati jaringan. Berikut merupakan implementasi wireshark dalam menangkap dan menganalisa paket jaringan.

# **PART 1 : CLO42-Sub-CLO4, CLO42-sub-CLO5**

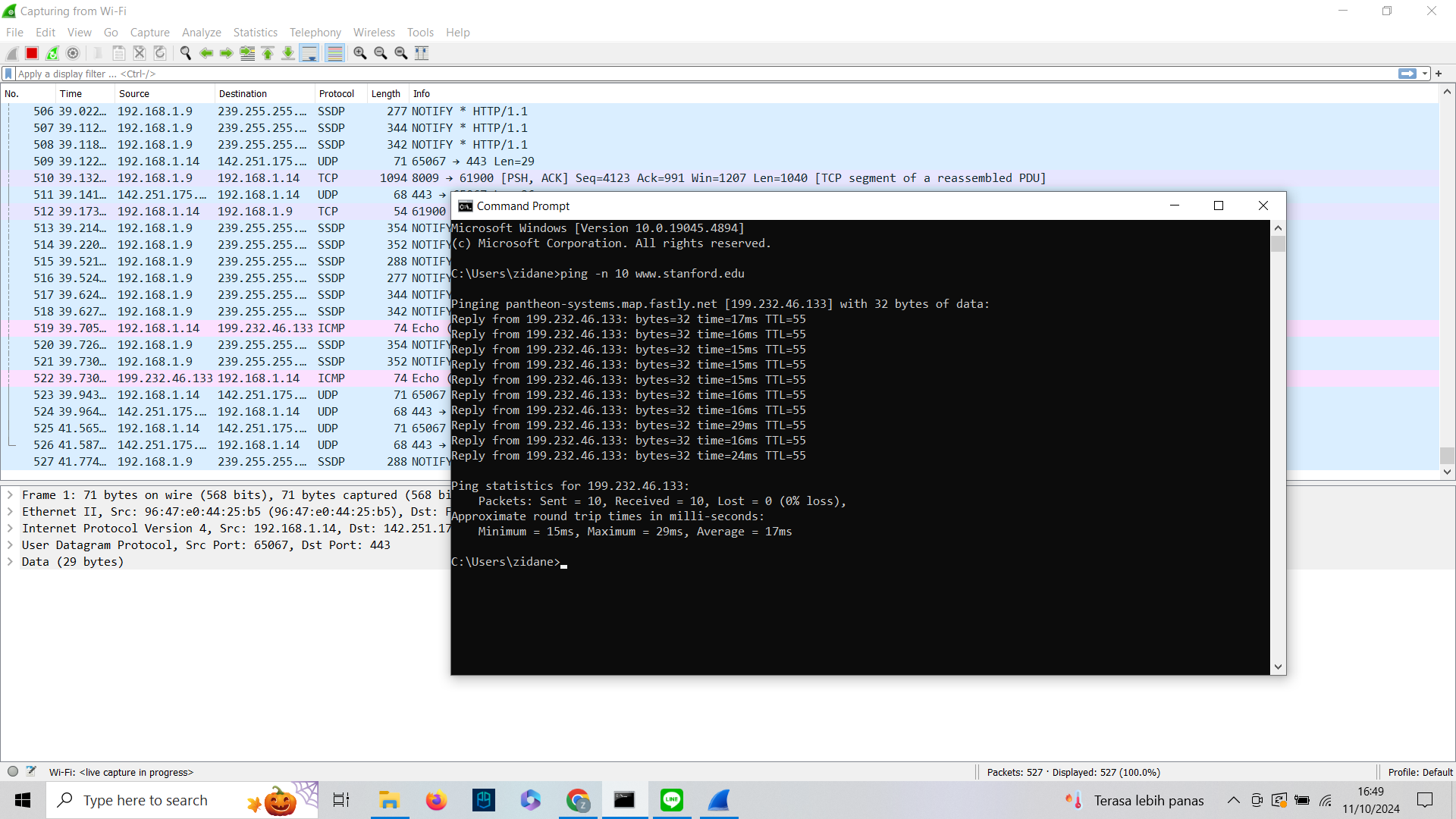
## Question A1

Pertama kita menyalakan wireshark terlebih dahulu untuk menangkap traffic dimana karena saya menggunakan wifi jadi saya memilih opsi wifi



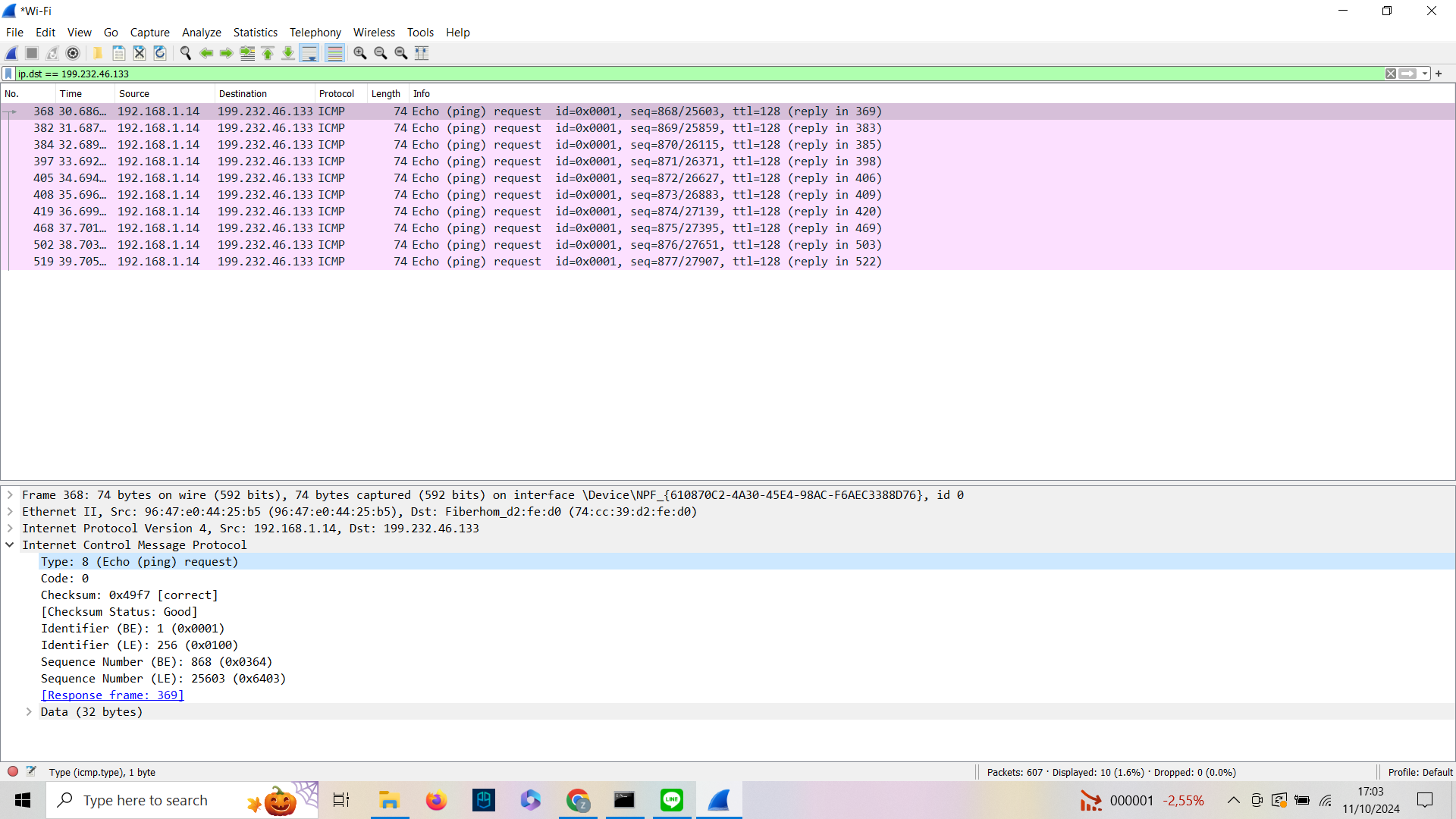
*Run wireshark*

biarkan paket wireshark berjalan terlebih dahulu kemudian membuka command prompt untuk melakukan ping terhadap server standford.edu. seperti gambar berikut :



*Ping Ip command*

Berdasarkan informasi diatas respon dalam alamat destinasi dari [www.standford.edu](http://www.standford.edu) yaitu dengan memiliki alamat 199.232.46.133 terdapat 10 paket yang dikirim dan 10 paket yang diterima dengan rata - rata waktu yang dibutuhkan semua paket ping untuk pergi dan kembali. Dalam hal ini, rata-ratanya adalah 17 milidetik. Dalam hal ini paket yang dikirim tidak ada yang hilang artinya semua paket berjalan dengan lancar. Selanjutnya saya akan melakukan filtering melalui wireshark untuk memastikan berapa total paket yang muncul dengan memasukan alamat dari standford.edu seperti berikut :



Melalui filtering alamat ip di wireshark menunjukan 10 paket yang tertangkap dari alamat standford.edu dimana protokol yang digunakan untuk melakukan request adalam ICMP protokol. Selain itu juga terdapat informasi sequence urutan setiap bits yang forward. Seperti yang di jelaskan sebelumnya terdapat 10 ping request dan 10 reply dari paket ICMP tersebut.

* 10 Ping Request: Ini berarti Anda telah mengirimkan 10 paket data ping ke alamat IP tujuan. Setiap paket ini berisi informasi seperti alamat IP sumber, alamat IP tujuan, nomor urut, dan waktu pengiriman.
* 10 Ping Reply: Ini berarti semua 10 paket ping yang Anda kirimkan berhasil diterima oleh perangkat tujuan dan perangkat tersebut mengirimkan balasan. Balasan ini mengkonfirmasi bahwa perangkat tujuan masih aktif dan dapat dijangkau.

## Question A2

ICMP atau Internet Control Message Protocol merupakan sebuah protokol jaringan yang digunakan untuk mengirim pesan-pesan kontrol dan kesalahan antara perangkat dalam jaringan. Sederhananya, ICMP seperti seorang "posmen" di dunia jaringan yang bertugas menyampaikan kabar baik dan buruk tentang pengiriman data.

**Mengapa ICMP Dibutuhkan untuk Melakukan Ping?**

Saat Anda melakukan ping ke suatu alamat IP, sebenarnya Anda sedang mengirimkan sebuah pesan ICMP jenis echo request. Pesan ini meminta perangkat di alamat IP tersebut untuk mengirimkan balasan. Jika perangkat tersebut aktif dan terhubung ke jaringan, ia akan mengirimkan pesan ICMP jenis echo reply sebagai balasan. Berdasarkan informasi dari paket wireshark yang muncul protokol number ICMP pada paket tersebut yaitu 8 dapat dianalisis melalui layer bertuliskan Internet Control Message pada bagian tampilan di bawah pada wireshark seperti berikut :

**Frame 368: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{610870C2-4A30-45E4-98AC-F6AEC3388D76}, id 0**

**Ethernet II, Src: 96:47:e0:44:25:b5 (96:47:e0:44:25:b5), Dst: Fiberhom\_d2:fe:d0 (74:cc:39:d2:fe:d0)**

**Internet Protocol Version 4, Src: 192.168.1.14, Dst: 199.232.46.133**

**Internet Control Message Protocol**

**Type: 8 (Echo (ping) request)**

**Code: 0**

**Checksum: 0x49f7 [correct]**

**[Checksum Status: Good]**

**Identifier (BE): 1 (0x0001)**

**Identifier (LE): 256 (0x0100)**

**Sequence Number (BE): 868 (0x0364)**

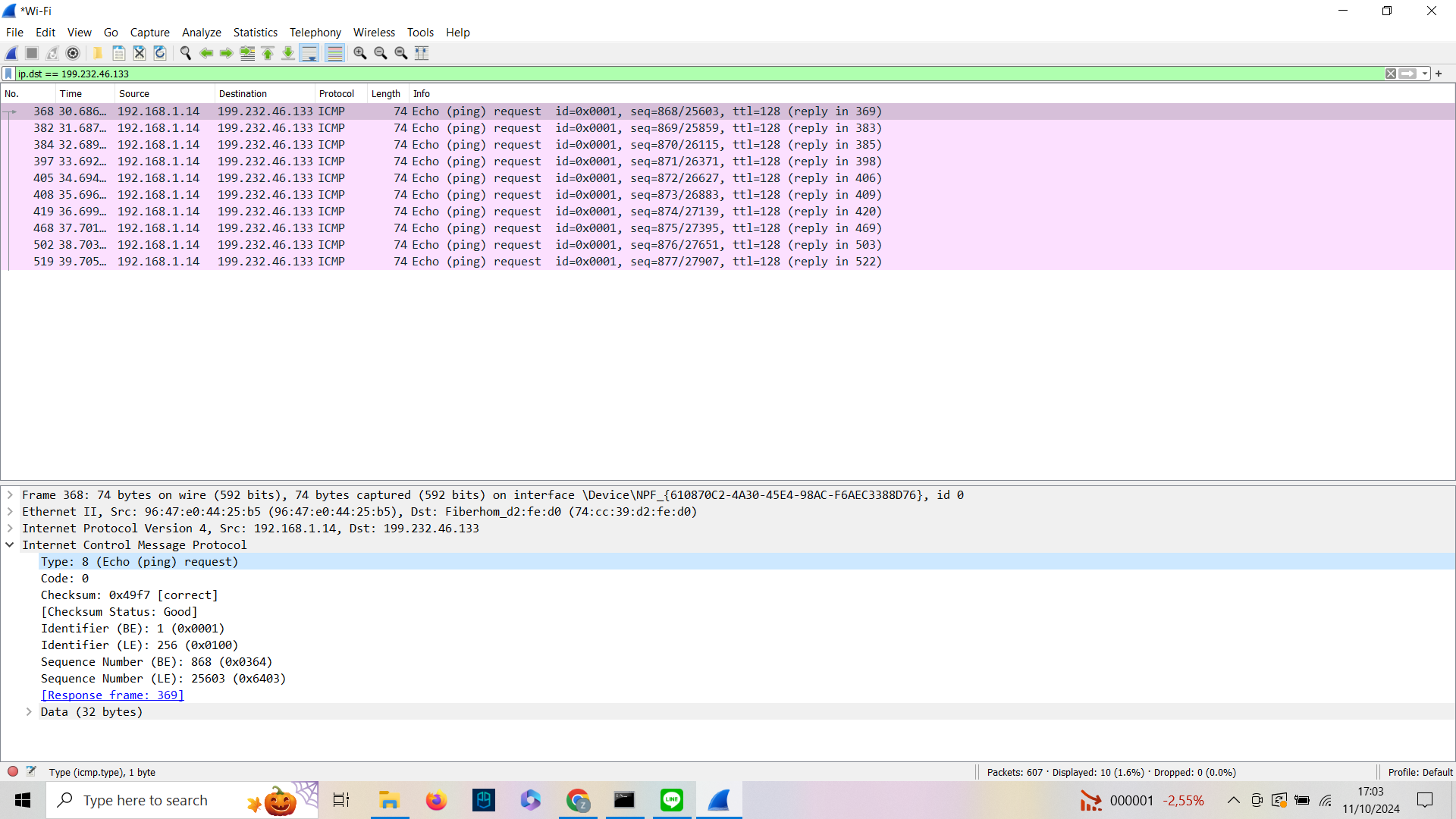
**Sequence Number (LE): 25603 (0x6403)**

**[Response frame: 369]**

**Data (32 bytes)**

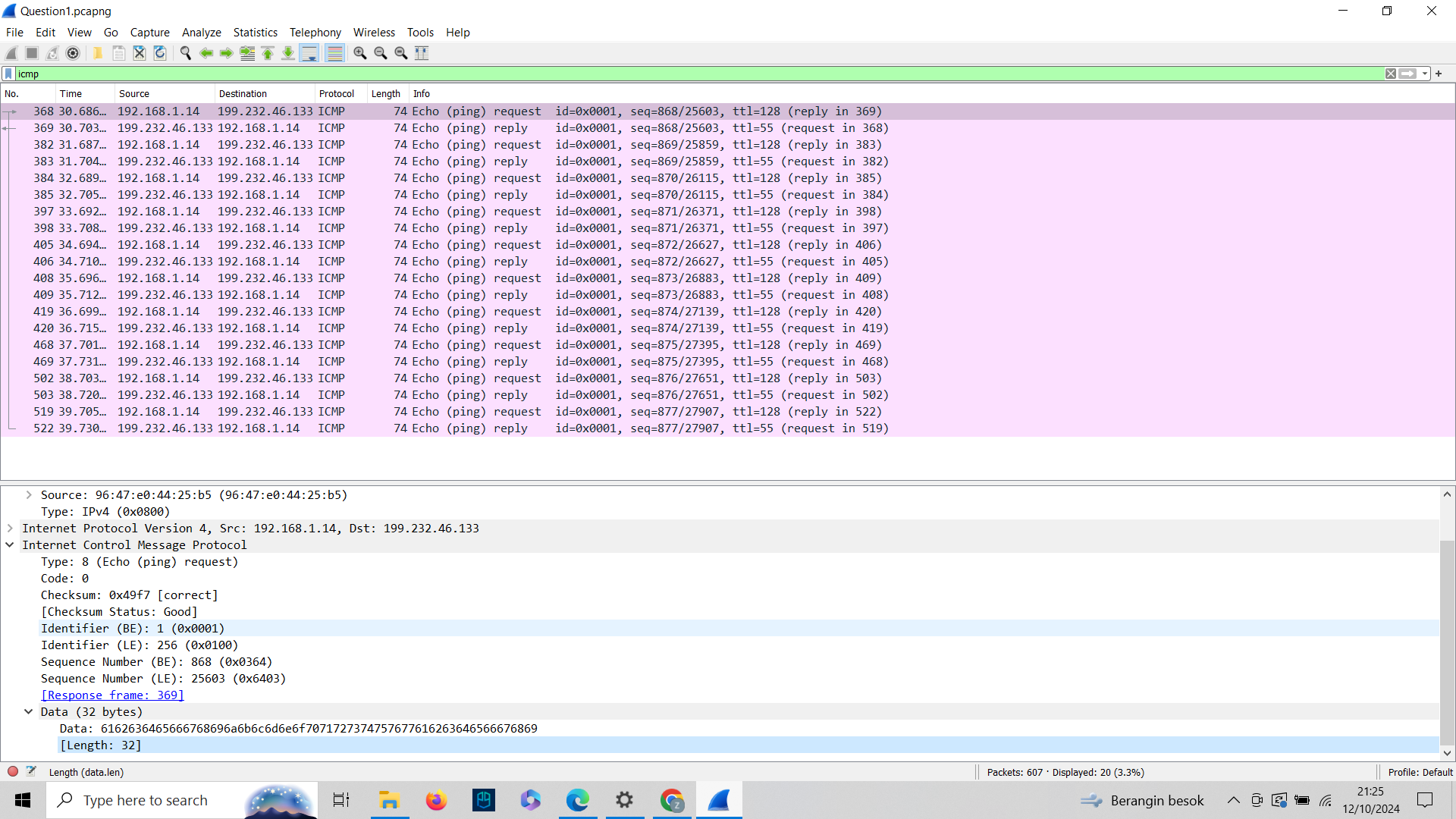
ICMP adalah protokol yang sangat penting dalam dunia jaringan. Ia memungkinkan kita untuk menguji keterhubungan, mengukur kinerja, dan mendiagnosis masalah pada jaringan. Tanpa ICMP, kita akan kesulitan untuk mengetahui apakah perangkat jaringan kita berfungsi dengan baik atau tidak.

## **SUB TOPIC 1 (ICMP AND PING)**

1. 

**Ip address Source :** 192.168.1.14

**Destination Address :** 199.232.46.133 / Domain name [www.standford.edu](http://www.standford.edu)

1. 

ICMP (Internet Control Message Protocol) adalah sebuah protokol tingkat jaringan yang digunakan untuk mengirim pesan kontrol antara perangkat jaringan. Pesan-pesan ini digunakan untuk melaporkan kesalahan, meminta informasi, atau memberikan umpan balik tentang status jaringan.

Alasan tidak adanya nomor port dalam paket ICMP adalah karena ICMP beroperasi pada tingkat jaringan. Protokol tingkat jaringan tidak menggunakan nomor port. Nomor port digunakan untuk mengidentifikasi layanan atau aplikasi tertentu dalam sebuah host. Karena ICMP tidak terkait dengan layanan atau aplikasi tertentu, ia tidak memerlukan nomor port.

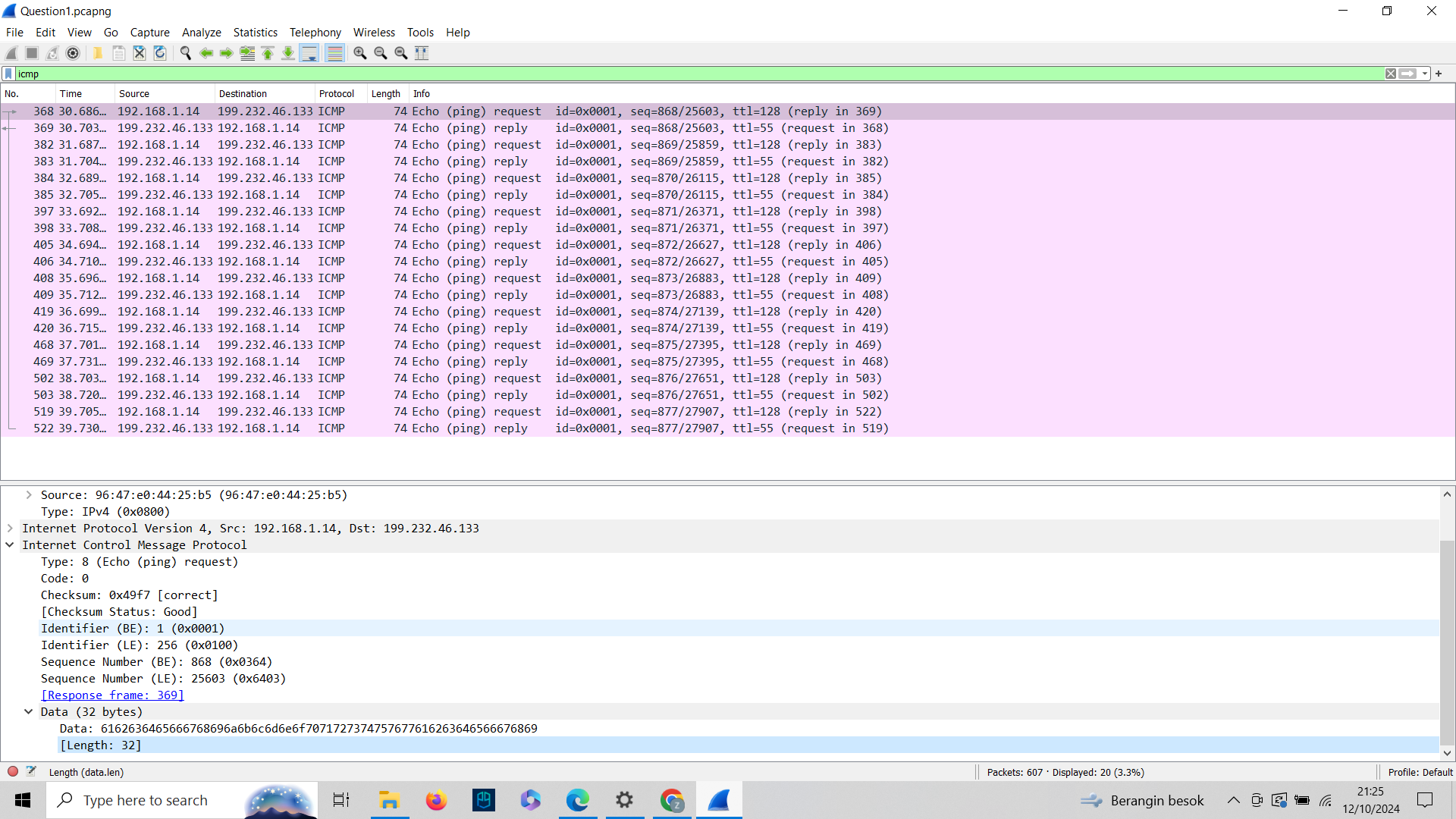
**Perbandingan dengan TCP dan UDP**

* **TCP (Transmission Control Protocol):** Menggunakan nomor port untuk mengidentifikasi aliran data antara dua aplikasi.
* **UDP (User Datagram Protocol):** Menggunakan nomor port untuk mengidentifikasi aplikasi tujuan tetapi tidak menjamin pengiriman paket.
* Fungsi ICMP

ICMP digunakan untuk berbagai fungsi seperti:

* **Ping:** Mengirim pesan echo untuk memeriksa ketersediaan host.
* **Traceroute:** Melacak jalur yang diambil oleh paket IP.
* **Fragmentation:** Mengirim pesan untuk menginformasikan tentang fragmentasi paket.
* **Error Reporting:** Mengirim pesan untuk melaporkan kesalahan jaringan.
* Kesimpulan

Karena ICMP adalah protokol tingkat jaringan dan tidak terkait dengan layanan atau aplikasi tertentu, ia tidak memerlukan nomor port. Nomor port digunakan untuk mengidentifikasi layanan atau aplikasi dalam sebuah host, yang tidak diperlukan oleh ICMP.

1. 

*ICMP REQUEST*

**Frame 368: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{610870C2-4A30-45E4-98AC-F6AEC3388D76}, id 0**

**Ethernet II, Src: 96:47:e0:44:25:b5 (96:47:e0:44:25:b5), Dst: Fiberhom\_d2:fe:d0 (74:cc:39:d2:fe:d0)**

**Internet Protocol Version 4, Src: 192.168.1.14, Dst: 199.232.46.133**

**Internet Control Message Protocol**

**Type: 8 (Echo (ping) request)**

**Code: 0**

**Checksum: 0x49f7 [correct]**

**[Checksum Status: Good]**

**Identifier (BE): 1 (0x0001)**

**Identifier (LE): 256 (0x0100)**

**Sequence Number (BE): 868 (0x0364)**

**Sequence Number (LE): 25603 (0x6403)**

**[Response frame: 369]**

**Data (32 bytes)**

**Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869**

**[Length: 32]**

**Type:** 8 Menunjukkan permintaan Echo (ping).

**Code:** 0 Menentukan jenis permintaan echo tertentu (dalam hal ini, permintaan echo standar).

**Checksum:** 0x49f7 - Sebuah checksum yang dihitung untuk memverifikasi integritas paket. Jika checksum yang dihitung cocok dengan checksum yang diterima, paket diasumsikan benar.

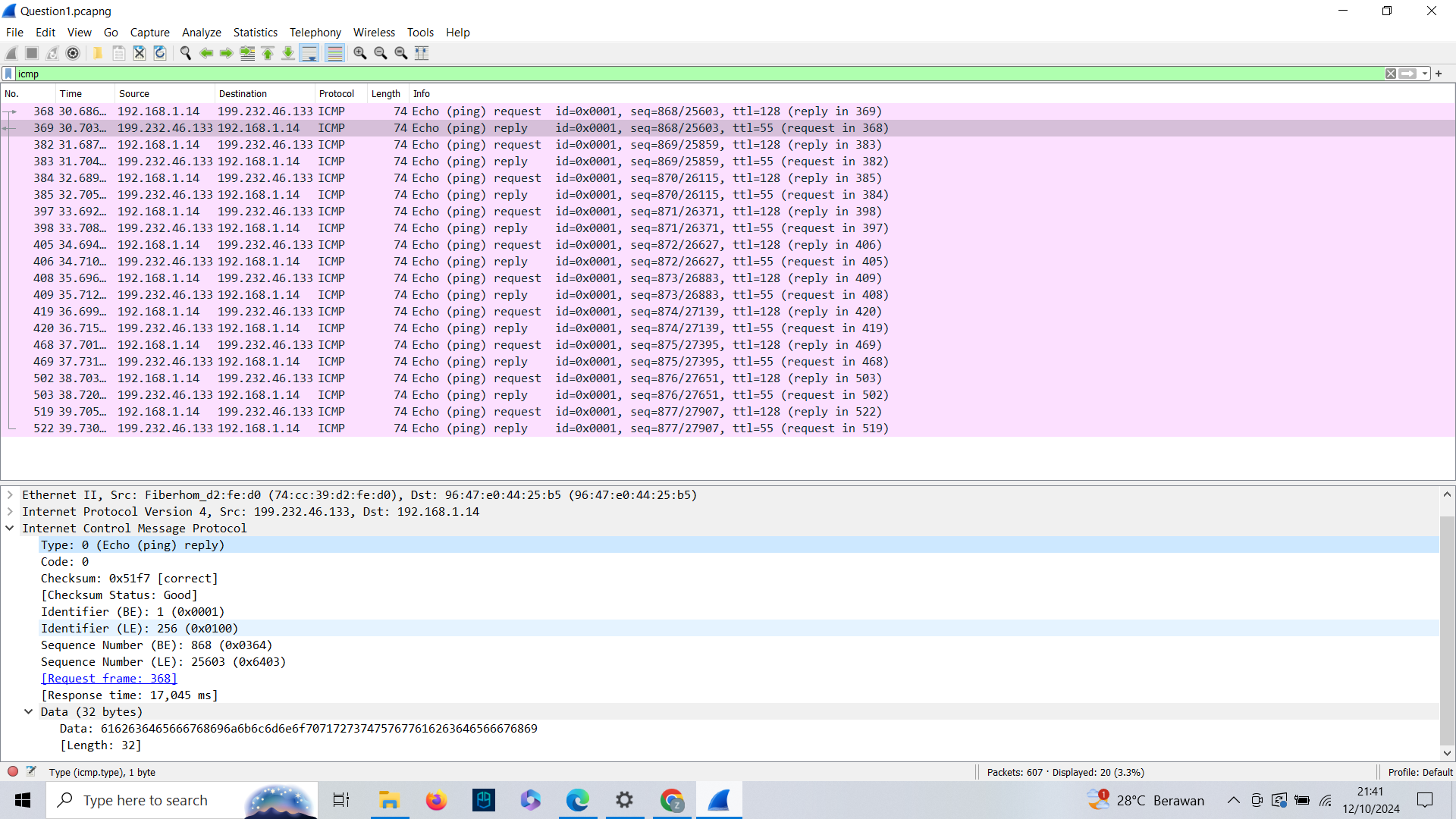
**Identifier:** 1 (0x0001) - Pengenal unik untuk permintaan ping spesifik ini. Digunakan untuk mencocokkan respons dengan permintaan.

Sequence Number: 868 (0x0364) - Nomor urutan yang digunakan untuk mengidentifikasi urutan permintaan ping dalam rangkaian.

**Data:** 32 bytes - Data ini dapat digunakan untuk informasi tambahan atau sebagai muatan untuk permintaan ping, tetapi seringkali dibiarkan kosong.

* Total Bytes: 74 bytes
* Checksum: 2 bytes (16 bits)
* Identifier: 2 bytes (16 bits)
* Sequence Number: 2 bytes (16 bits)
* Data: 32 bytes

Paket ICMP ini adalah permintaan ping yang dikirim dari 192.168.1.14 ke 199.232.46.133. Paket ini berisi pengenal unik dan nomor urutan untuk membantu mencocokkan respons. Bidang data kosong dalam kasus ini. Checksum digunakan untuk memverifikasi integritas paket.

1. 

*ICMP REPLYING*

**Frame 369: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{610870C2-4A30-45E4-98AC-F6AEC3388D76}, id 0**

**Ethernet II, Src: Fiberhom\_d2:fe:d0 (74:cc:39:d2:fe:d0), Dst: 96:47:e0:44:25:b5 (96:47:e0:44:25:b5)**

**Internet Protocol Version 4, Src: 199.232.46.133, Dst: 192.168.1.14**

**Internet Control Message Protocol**

**Type: 0 (Echo (ping) reply)**

**Code: 0**

**Checksum: 0x51f7 [correct]**

**[Checksum Status: Good]**

**Identifier (BE): 1 (0x0001)**

**Identifier (LE): 256 (0x0100)**

**Sequence Number (BE): 868 (0x0364)**

**Sequence Number (LE): 25603 (0x6403)**

**[Request frame: 368]**

**[Response time: 17,045 ms]**

**Data (32 bytes)**

**Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869**

**[Length: 32]**

**Type :** 0 - Menunjukkan respons Echo (ping).

**Code :** 0 - Menunjukkan jenis respons echo (dalam hal ini, respons echo standar).

**Checksum :** 0x51f7 - Sebuah checksum yang dihitung untuk memverifikasi integritas paket.

**Identifier :** 1 (0x0001) - Pengenal unik yang sama dengan permintaan ping, digunakan untuk mencocokkan respons dengan permintaan.

**Sequence Number:** 868 (0x0364) - Nomor urutan yang sama dengan permintaan ping, digunakan untuk mengidentifikasi urutan respons dalam rangkaian.

**Data :** 32 byte data - Data ini biasanya sama dengan data yang dikirim dalam permintaan ping, tetapi dapat diubah jika diperlukan.

* Total Bytes: 74 bytes
* Checksum: 2 bytes (16 bits)
* Identifier: 2 bytes (16 bits)
* Sequence Number: 2 bytes (16 bits)
* Data: 32 bytes

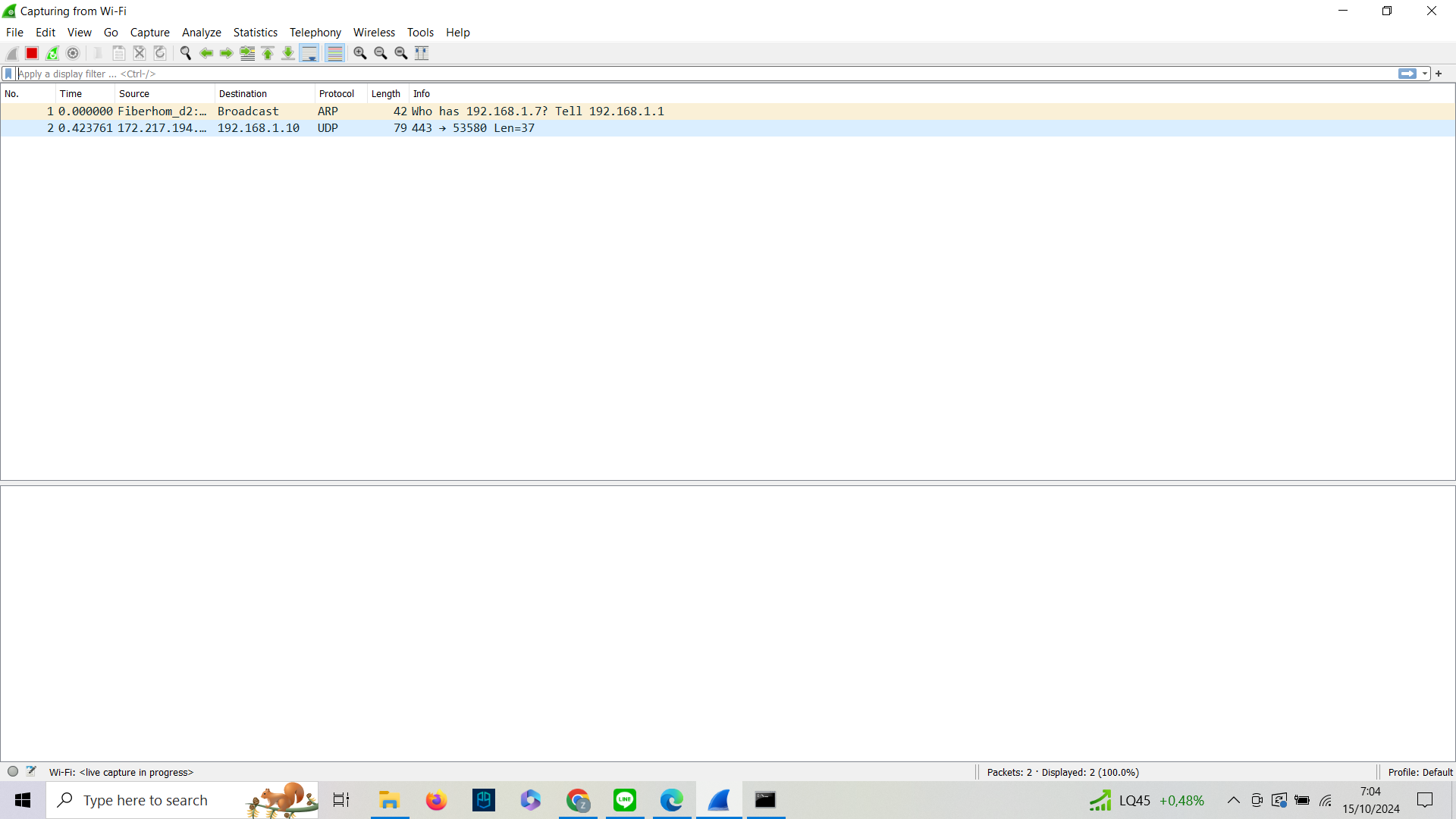
Paket ICMP ini adalah respons terhadap permintaan ping yang sebelumnya dikirim. Respons ini berisi pengenal unik dan nomor urutan yang sama dengan permintaan untuk mencocokkan keduanya. Data dalam respons biasanya sama dengan data dalam permintaan. Checksum digunakan untuk memverifikasi integritas paket.

## **SUB TOPIC 2 (ICMP AND TRACEROUTE)**

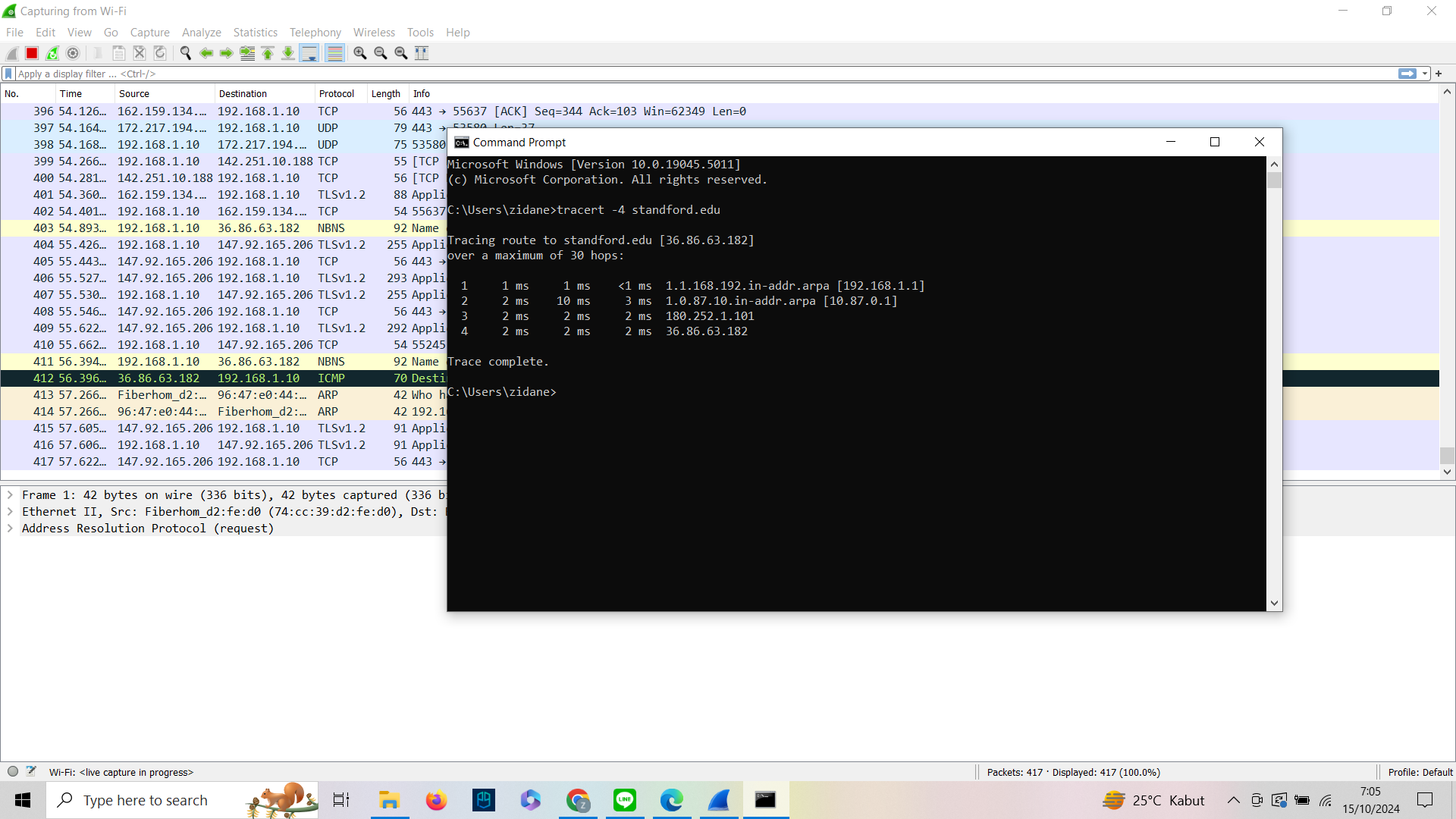
Traceroute, atau sering juga disebut tracert, adalah sebuah utilitas jaringan yang berfungsi untuk melacak jalur yang dilalui oleh sebuah paket data dari sumber (misalnya, komputer Anda) menuju tujuan (misalnya, sebuah server web). Bayangkan traceroute sebagai GPS untuk paket data di internet. Traceroute menunjukkan secara detail setiap "hop" atau lompatan yang dilalui paket data. Setiap hop mewakili sebuah router atau perangkat jaringan yang meneruskan paket data menuju tujuan akhir.Traceroute juga dapat digunakan untuk menganalisis kinerja jaringan secara keseluruhan. Dengan membandingkan waktu respon pada setiap hop, Kita dapat mengetahui bagian mana dari jaringan yang memiliki kinerja terbaik dan terburuk.

Traceroute bekerja dengan mengirimkan serangkaian paket ICMP (Internet Control Message Protocol) dengan nilai Time To Live (TTL) yang berbeda-beda. TTL adalah batas maksimum hop yang dapat dilalui oleh sebuah paket. Setiap kali sebuah paket mencapai batas TTL-nya, router akan membuang paket tersebut dan mengirimkan pesan ICMP Time Exceeded kembali ke sumber. Dengan cara ini, traceroute dapat melacak setiap hop yang dilalui oleh paket data. berikut bagaimana contohnya

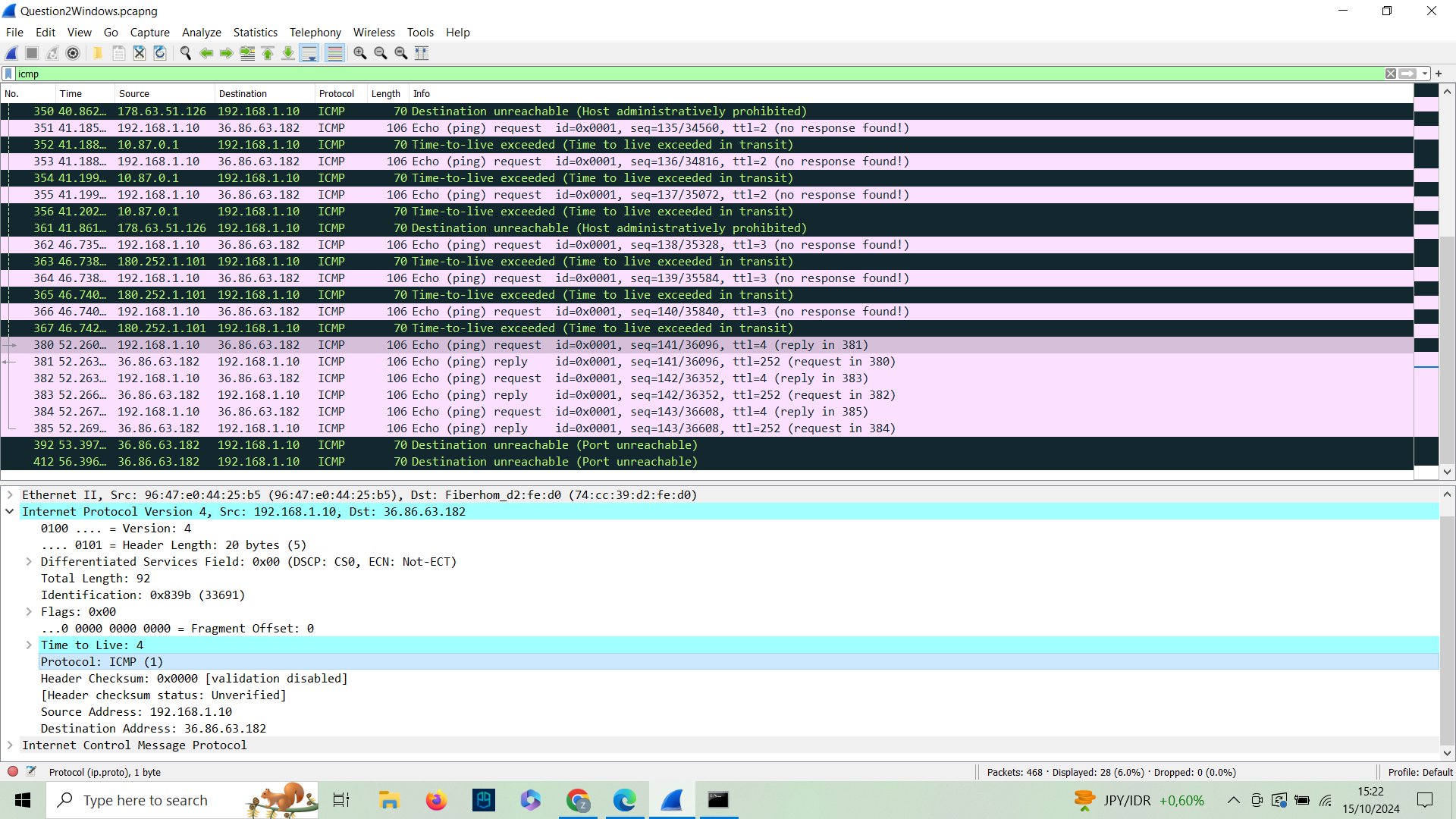
pertama membuka wireshark sebagai software untuk menangkap jaringan



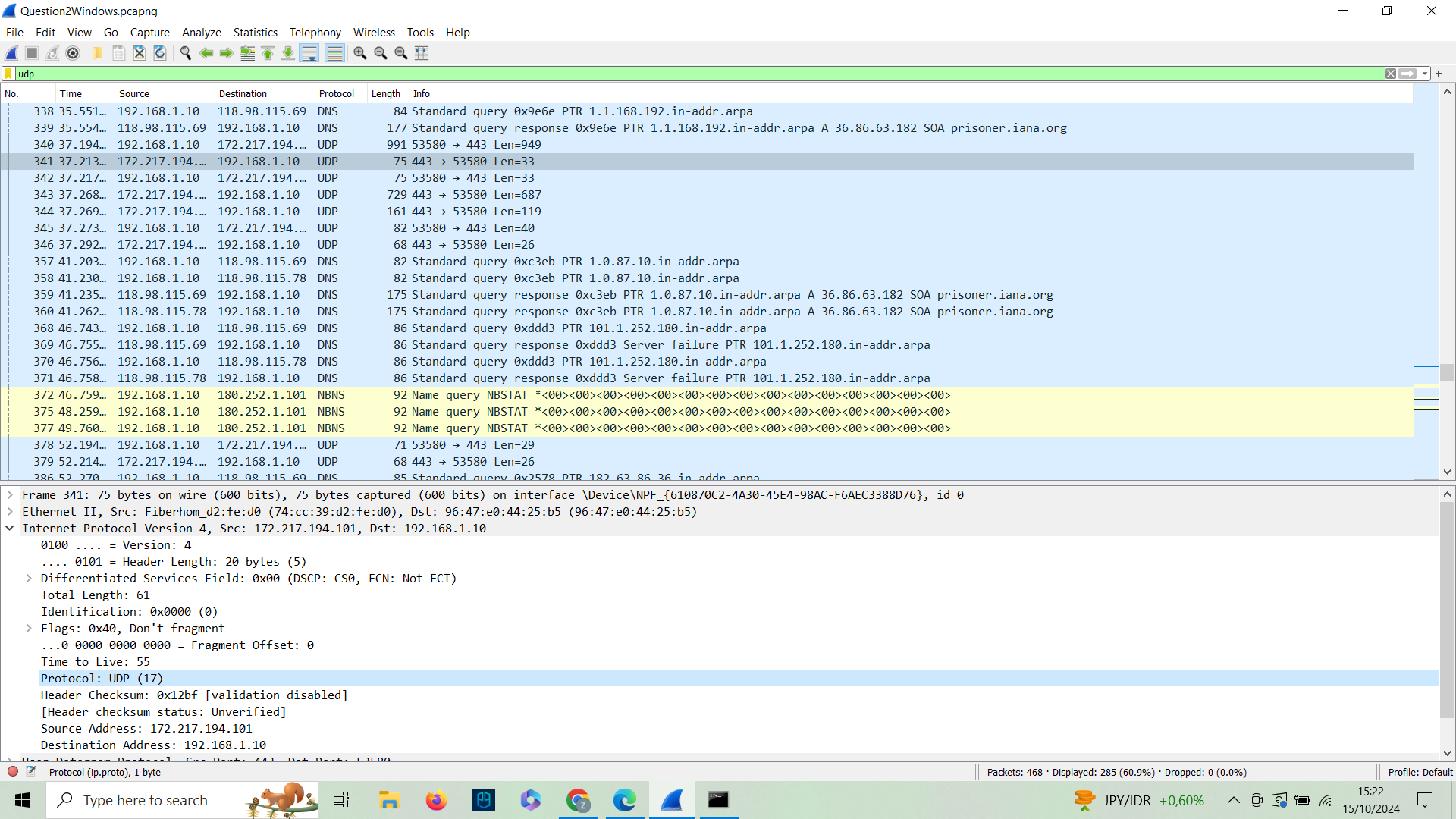
Kemudian membuka prompt sesuai sistem operasi yang digunakan dimana disini saya menggunakan windows.



Dengan menggunakan perintah tracert -4 standford.edu perintah yang digunakan untuk melacak rute yang diambil oleh paket data dari komputer Anda ke tujuan yang ditentukan. Dengan kata lain, tracert akan menunjukkan semua router yang dilalui oleh paket data dalam perjalanannya. Angka 4 setelah tracert menunjukkan bahwa kita ingin menggunakan protokol Internet versi 4 (IPv4) untuk melakukan pelacakan. IPv4 adalah protokol jaringan yang paling umum digunakan saat ini. stanford.edu adalah alamat domain dari Universitas Stanford. Ini adalah tujuan akhir yang ingin kita lacak rutenya.

1. 

*ICMP Protokol*

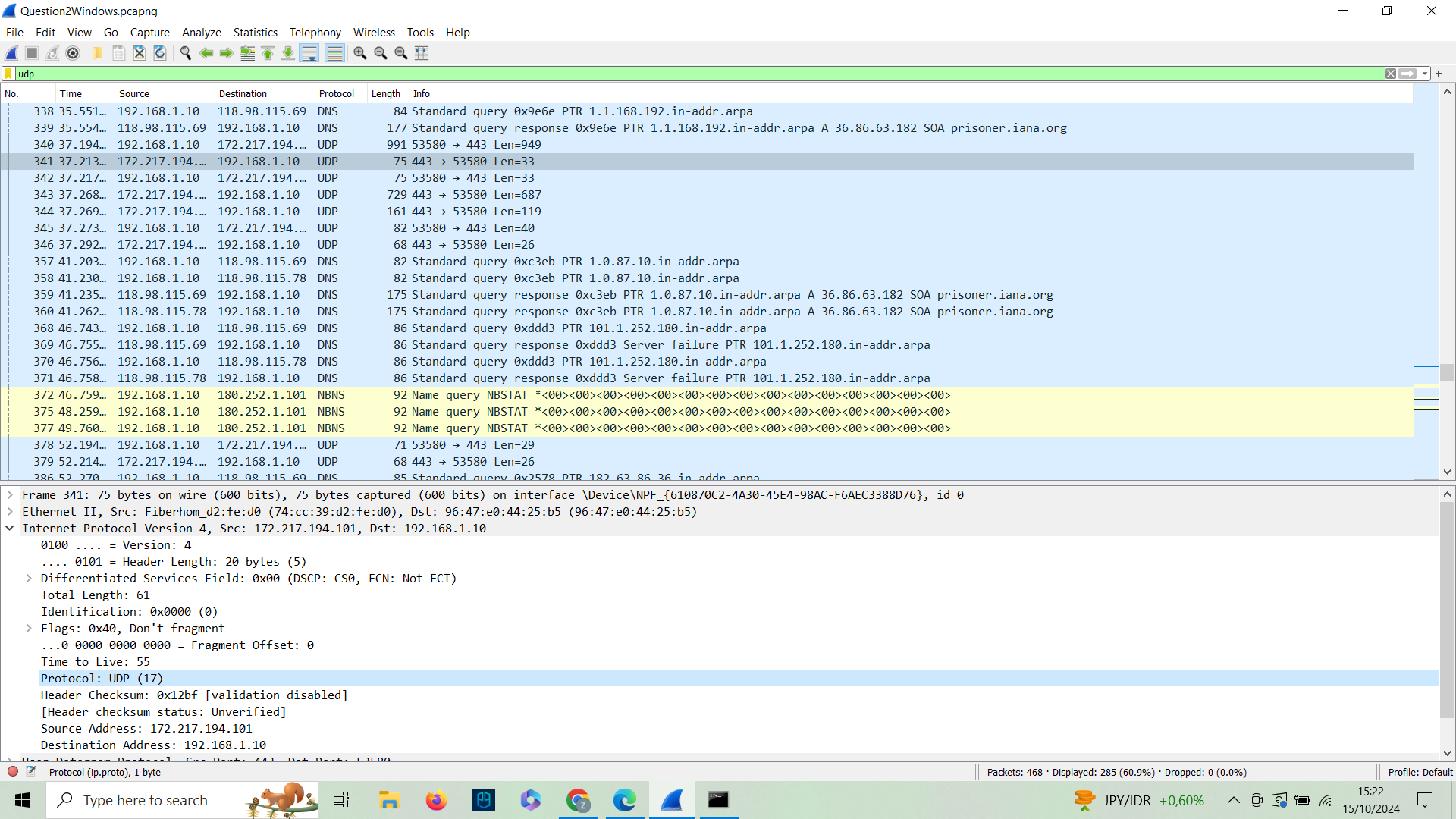


*UDP Protokol*

Berdasarkan hasil filtering paket ICMP dan UDP terdapat perubahan identitas pada paket protokol jaringan. Setiap protokol yang beroperasi di lapisan jaringan (IP) memiliki nomor protokol yang unik. Nomor ini berfungsi sebagai semacam **kartu identitas** yang memungkinkan router dan perangkat jaringan lainnya untuk mengenali dan memproses paket data dengan benar. Dimana **ICMP sendiri memiliki nomor identitas 1.** Penentuan nomor 1 untuk ICMP bersifat historis dan konvensional. Ketika protokol-protokol jaringan pertama kali dikembangkan, ICMP adalah salah satu protokol yang paling dasar dan sering digunakan. Oleh karena itu, diberi nomor yang kecil untuk memudahkan identifikasi. Sedangkan untuk paket UDP memiliki nomor identitas 17. Nomor 17 untuk UDP juga merupakan hasil dari penentuan nomor secara historis. UDP adalah protokol transport yang sederhana dan efisien, sering digunakan untuk aplikasi real-time seperti streaming audio dan video.

**Mengapa Nomor Protokol Penting?**

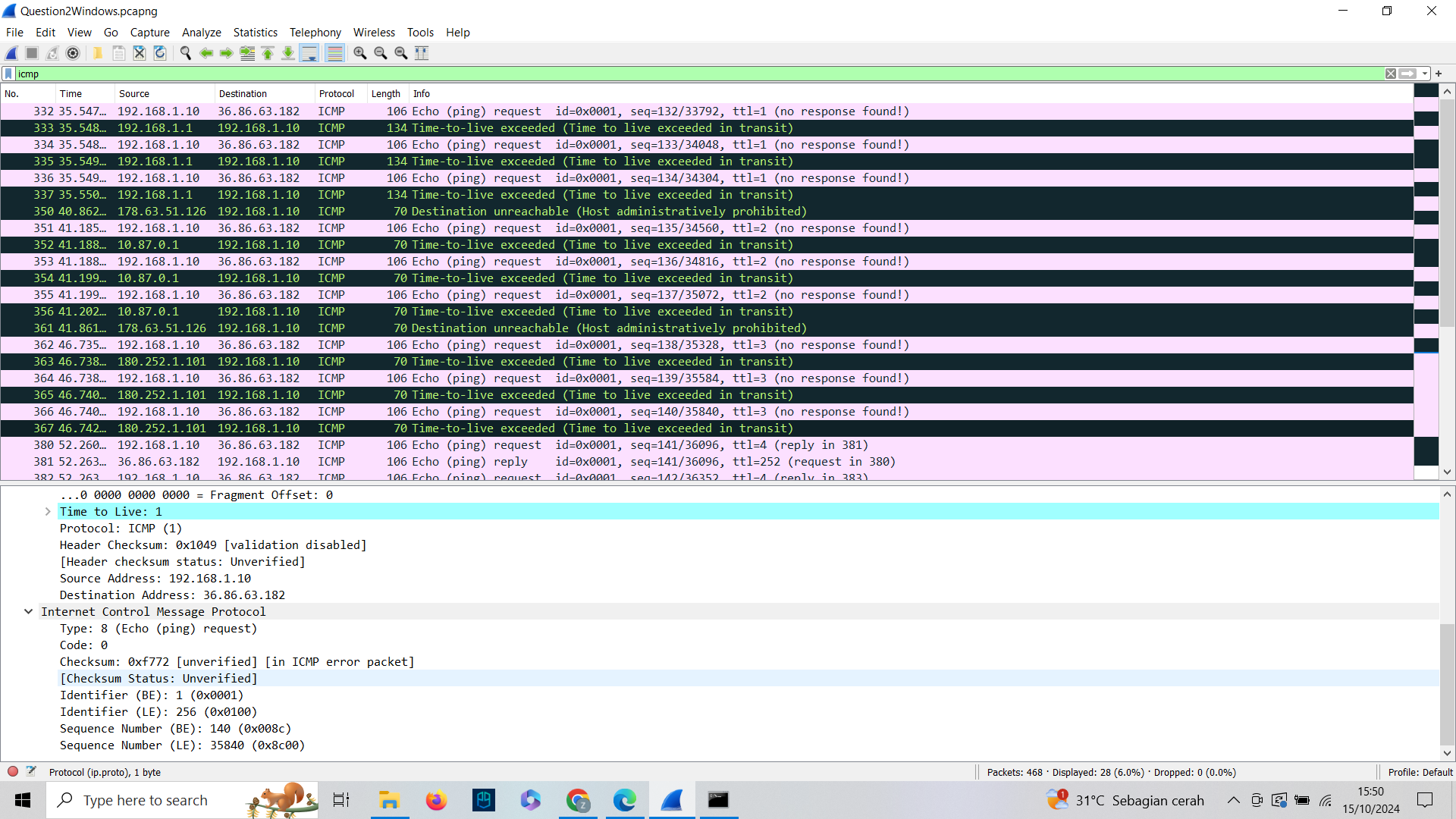
* **Routing:** Router menggunakan nomor protokol untuk menentukan jalur terbaik yang akan dilalui oleh paket data.
* **Pemrosesan Paket:** Setiap protokol memiliki cara pemrosesan yang berbeda. Nomor protokol membantu perangkat jaringan untuk memilih proses yang tepat.
* **Filter:** Firewall dan sistem keamanan jaringan menggunakan nomor protokol untuk memblokir atau mengizinkan lalu lintas tertentu.

1. 

*ICMP Paket*

Terdapat perbedaan pada echo packet di proses yang pertama yaitu ping pada sub topic 1 dimana destinasti yang dituju adalah standford.edu. Perbedaanya dapat dilihat pada bagian menu/layer ICMPnya dimana untuk paket echo ini terdapat informasi time to livenya yaitu sebesar 4 seperti yang terlihat pada gambar diatas. Alasannya adalah Perintah ping dirancang secara khusus untuk memeriksa ketercapaian (reachability) sebuah host. Ia mengirim paket ICMP echo request dan menunggu balasan echo reply. Informasi utama yang dicari adalah apakah host tujuan dapat dijangkau atau tidak, serta waktu responnya. Sedangkan Traceroute memiliki tujuan yang lebih kompleks, yaitu melacak rute yang dilalui paket data dari sumber ke tujuan. Untuk mencapai tujuan ini, traceroute secara bertahap mengurangi nilai TTL pada setiap hop (router) yang dilalui paket.

Meskipun keduanya menggunakan paket ICMP echo, ping dan traceroute memiliki tujuan yang berbeda dan oleh karena itu menampilkan informasi yang berbeda. Traceroute secara eksplisit memanfaatkan TTL untuk mencapai tujuannya dalam melacak rute, sementara ping lebih fokus pada ketercapaian host.

1. 

*ICMP ERROR Paket*

Terlihat jelas adanya sejumlah besar paket ICMP dengan error "Time to Live exceeded". Ini mengindikasikan adanya **masalah dalam perjalanan paket dari sumber ke tujuan.** Setiap paket IP memiliki header TTL yang berfungsi sebagai penghitung mundur. Setiap kali paket melewati sebuah router, nilai TTL akan dikurangi satu. Jika nilai TTL mencapai nol sebelum paket mencapai tujuan, router akan membuang paket dan mengirimkan pesan ICMP "Time to Live exceeded" kembali ke pengirim. Nilai TTL awal yang terlalu rendah atau konfigurasi router yang tidak sesuai dapat menyebabkan masalah ini.

**Paket data terjebak dalam loop routing,** terus menerus berputar di antara beberapa router tanpa mencapai tujuan. Hal ini menyebabkan nilai TTL terus berkurang hingga akhirnya mencapai nol. Konfigurasi routing yang salah atau masalah pada protokol routing. Jaringan mengalami beban yang sangat tinggi sehingga paket data mengalami penundaan yang signifikan. Akibatnya, nilai TTL habis sebelum paket mencapai tujuan. Dikarenakan banyaknya pengguna yang mengakses jaringan, bandwidth yang terbatas, atau adanya bottleneck dalam jaringan.

Kerusakan pada perangkat jaringan seperti router atau switch dapat menyebabkan paket data dibuang atau dialihkan secara tidak benar. Hardware atau software yang bermasalah pada perangkat jaringan. Efek dari Paket Error ICMP "Time to Live Exceeded" :

* **Kegagalan Pengiriman Paket:** Paket data tidak dapat mencapai tujuan karena dibuang oleh router.
* **Peningkatan Latensi:** Jika paket berhasil mencapai tujuan, tetapi melewati rute yang lebih panjang karena masalah routing, maka akan terjadi peningkatan latensi.
* **Penurunan Kualitas Layanan:** Aplikasi yang sensitif terhadap latensi, seperti VoIP atau video streaming, akan mengalami gangguan.
* **Kesulitan dalam Diagnostik:** Banyaknya paket error dapat menyulitkan dalam mengidentifikasi akar masalah jaringan.

Paket error ICMP "Time to Live exceeded" mengindikasikan adanya masalah dalam pengiriman paket data. Untuk mengatasi masalah ini, diperlukan analisis yang lebih mendalam terhadap jaringan dan identifikasi akar penyebab masalah. Dengan memperbaiki masalah yang mendasar, kinerja jaringan dapat ditingkatkan dan kualitas layanan dapat dijamin.

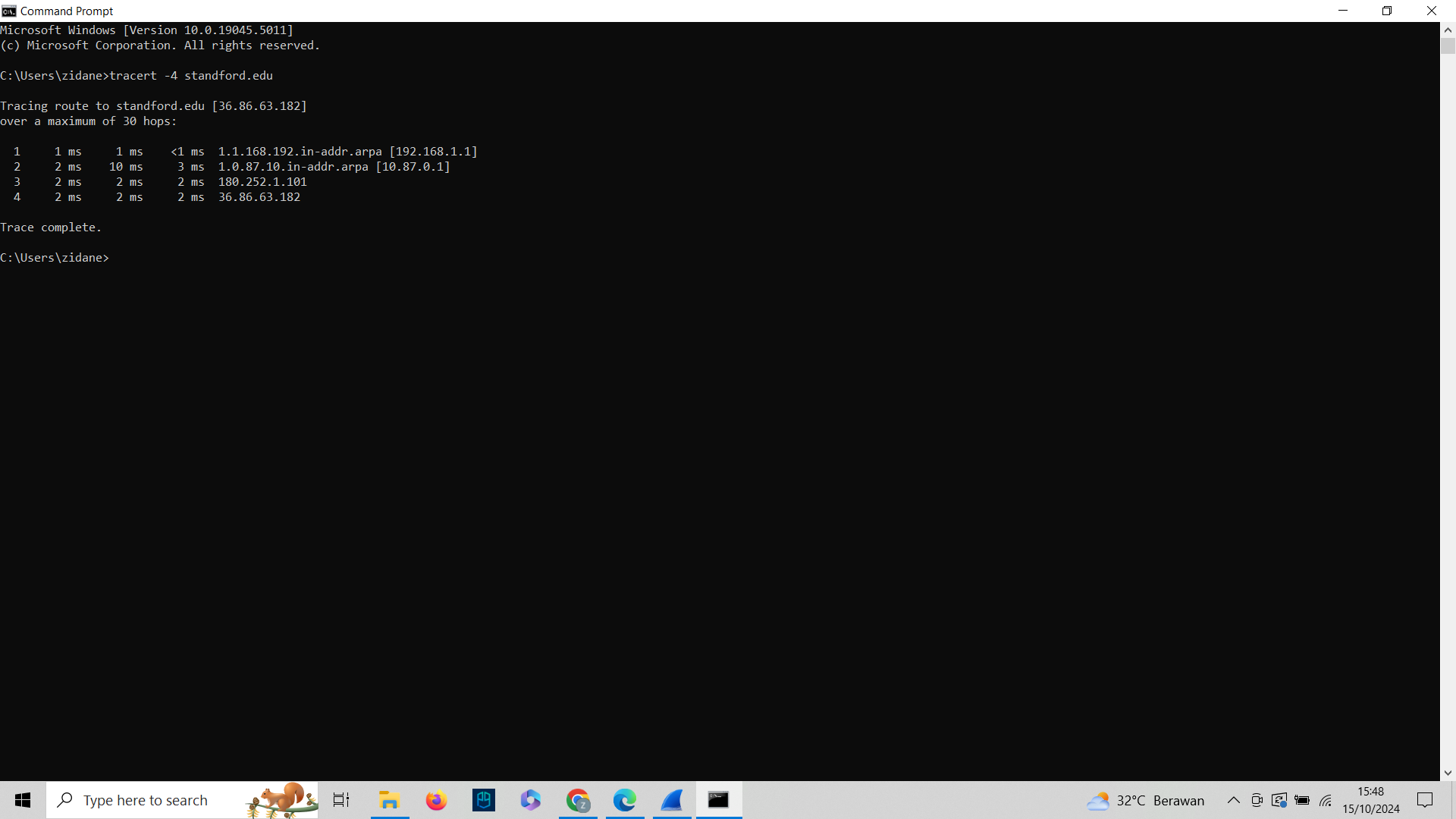
1. Dari informasi pada pertanyaan sebelumnya ada beberapa faktor yang memungkinkan bahwa terdapat paket ICMP yang diterima. yaitu :

* **TTL:** Nilai TTL masih cukup besar ketika paket mencapai tujuan, sehingga paket tidak dibuang oleh router.
* **Waktu Respon:** Waktu tempuh paket dari sumber ke tujuan relatif singkat dan stabil.
* **Ukuran Paket:** Ukuran paket sesuai dengan yang diharapkan.
* **Flag:** Flag pada header IP umumnya tidak memiliki nilai yang signifikan dalam hal error "Time to Live Exceeded".
* **Checksum:** Nilai checksum valid, menunjukkan bahwa data paket tidak rusak selama transmisi.

**Perbandingan dan Implikasi:**

| **Karakteristik** | **Paket Berhasil** | **Paket Error** | **Implikasi** |
| --- | --- | --- | --- |
| **TTL** | Cukup besar | 0 atau sangat kecil | Paket dibuang karena melewati terlalu banyak hop |
| **Waktu Respon** | Singkat dan stabil | Tidak terukur atau sangat lama | Paket tidak mencapai tujuan |
| **ICMP Error Message** | Tidak ada | Time to Live Exceeded | Menunjukkan penyebab error |

Dengan membandingkan paket yang berhasil dengan paket yang mengalami error, kita dapat mengidentifikasi penyebab utama masalah dan mengambil tindakan perbaikan yang tepat. Pemahaman yang mendalam tentang karakteristik paket dan penggunaan alat analisis jaringan seperti Wireshark akan sangat membantu dalam proses troubleshooting.

1. 

Berdasarkan hasil traceroute yang dilakukan menunjukkan rute yang diambil oleh paket data dari perangkat Anda menuju ke Stanford University (dengan alamat IP 36.86.63.182). Setiap baris mewakili satu hop atau lompatan yang dilakukan paket data, mulai dari perangkat Anda hingga mencapai tujuan akhir.

* **Nomor Hop:** Menunjukkan urutan hop atau lompatan yang dilalui paket.
* **Waktu (ms):** Menunjukkan waktu yang dibutuhkan paket untuk mencapai router pada hop tersebut dalam satuan milidetik. Tiga nilai waktu yang ditampilkan biasanya adalah rata-rata, minimum, dan maksimum dari beberapa pengukuran.

Untuk mengidentifikasi link dengan latensi tinggi, kita perlu membandingkan waktu yang dibutuhkan paket untuk melewati setiap hop. Dalam contoh Anda, terlihat bahwa:

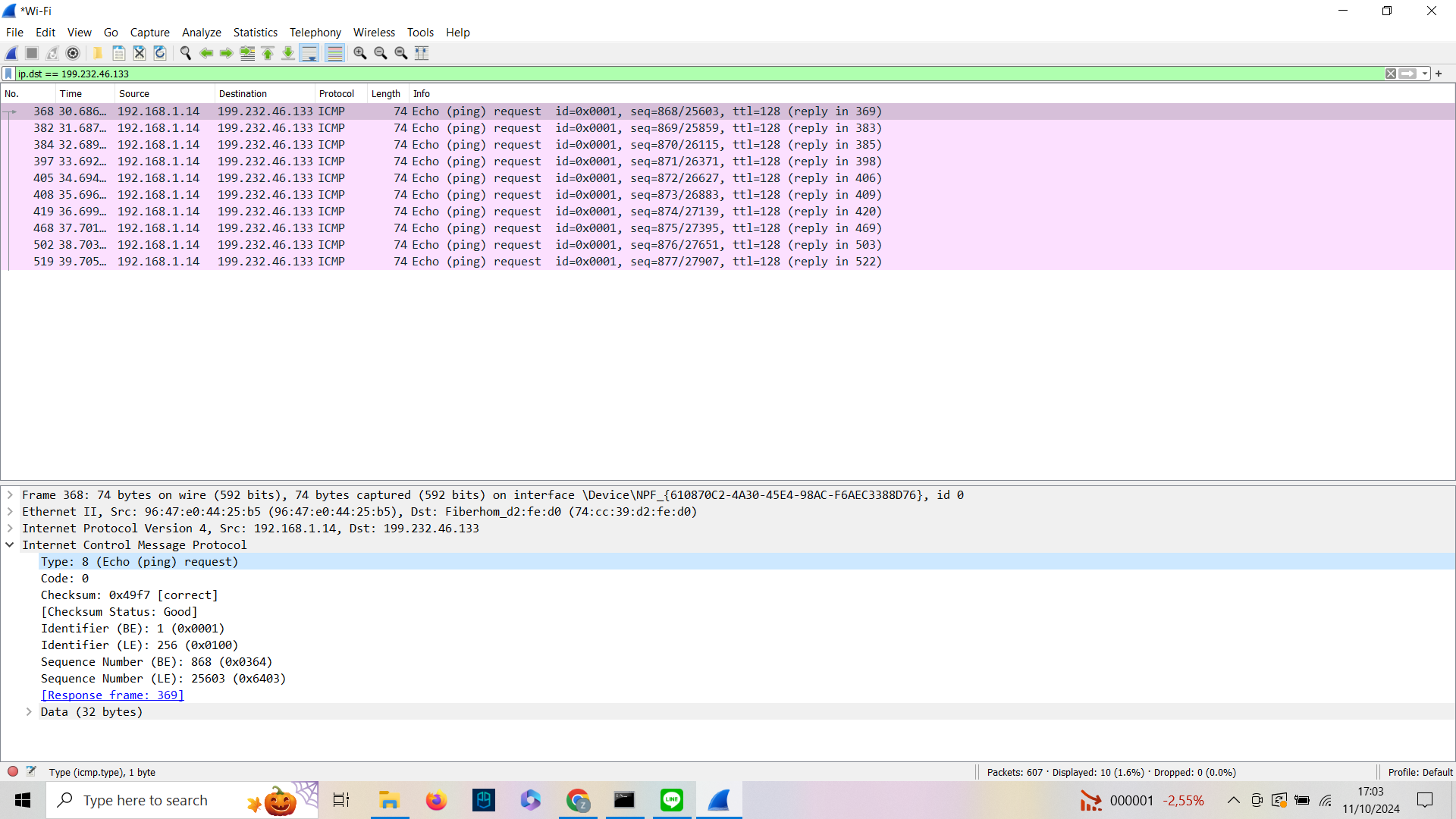
* **Hop 1 dan 3:** Memiliki latensi yang sangat rendah (kurang dari 3 ms), menunjukkan koneksi yang sangat baik antara perangkat Anda dengan router pertama dan antara router di hop 3 dengan tujuan akhir.
* **Hop 2:** Memiliki latensi yang sedikit lebih tinggi dibandingkan hop 1 dan 3, dengan waktu rata-rata sekitar 5 ms.

Berdasarkan hasil traceroute ini, link yang paling mungkin memiliki latensi lebih tinggi adalah antara hop 1 dan hop 2. Namun, perbedaannya tidak terlalu signifikan dan masih dapat dianggap normal dalam jaringan yang kompleks.

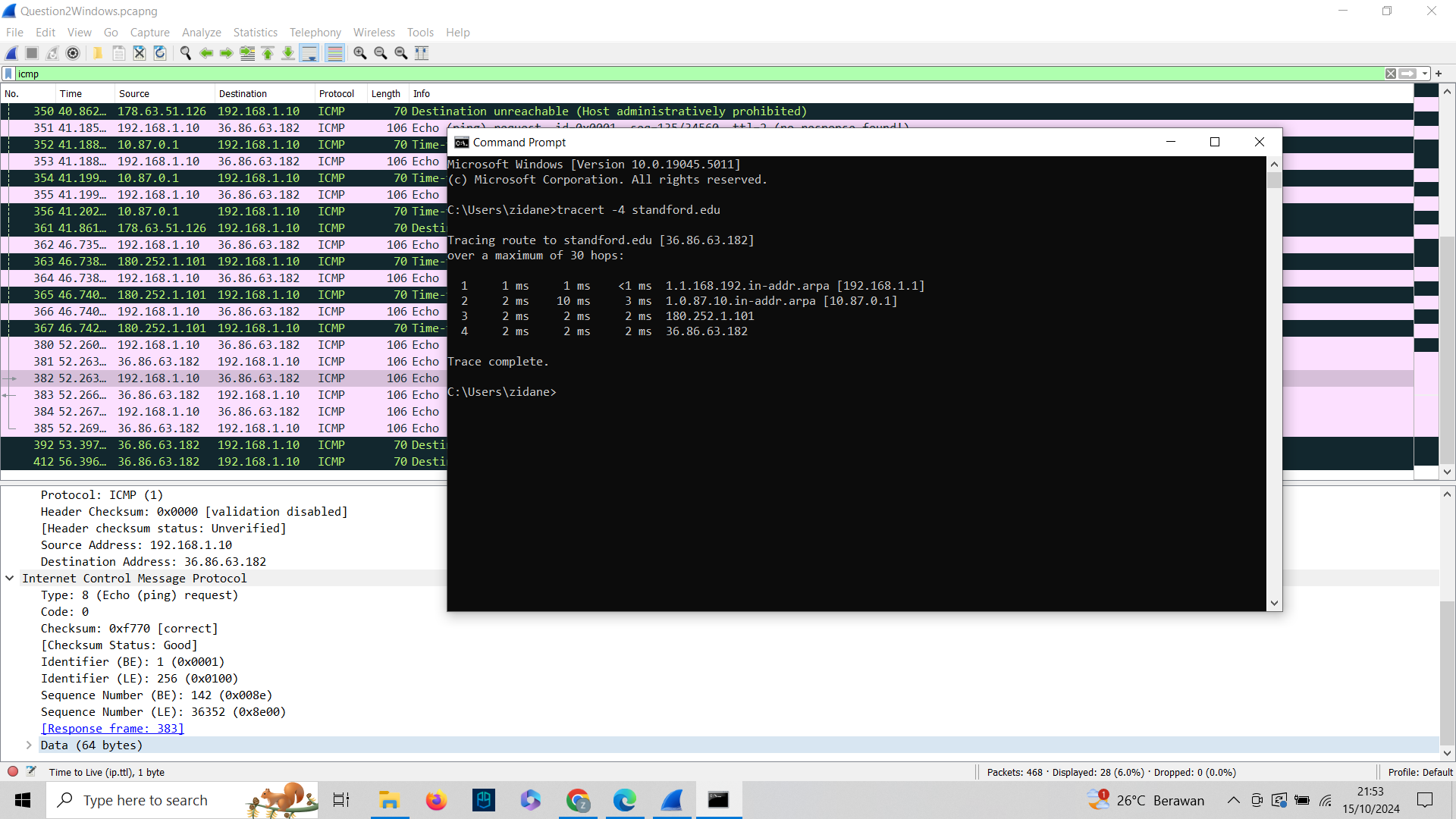
1. Berdasarkan hasil screenshot pada command promt untuk melakukan traceroute pada domain standford.edu, **tidak terlihat adanya perbedaan latensi yang signifikan antara setiap hop (link) yang dilalui paket data menuju Stanford University.** Waktu tempuh paket relatif stabil di sekitar 2-3 milidetik. Ini mengindikasikan koneksi yang cukup baik dan stabil. Kemudian berdasarkan nama - nama routernya dapat diidentifikasikan :

* **1.1.168.192.in-addr.arpa [192.168.1.1]:** Nama ini merupakan alamat IP dalam format reverse DNS. Angka "192.168.1.1" adalah alamat IP yang umum digunakan untuk gateway default pada jaringan home atau small office. Jadi, router ini kemungkinan besar adalah router Anda sendiri atau router di dalam jaringan lokal Anda.
* **1.0.87.10.in-addr.arpa [10.87.0.1]:** Alamat IP ini menggunakan rentang alamat private (10.0.0.0/8). Ini adalah alamat yang sering digunakan di dalam jaringan internal suatu organisasi. Router ini kemungkinan adalah router milik ISP Anda atau router di jaringan backbone ISP.
* **180.252.1.101** : Kemungkinan alamat ini merupakan jaringan backbone ISP dan berfungsi sebagai titik transit untuk lalu lintas internet atau router yang menghubungkan jaringan internal ISP Anda ke jaringan internet yang lebih luas(NAT).
* **36.86.63.182** : Merupalan alamat server address dari standford.edu

# **PART 2 : CLO42-Sub-CLO6**

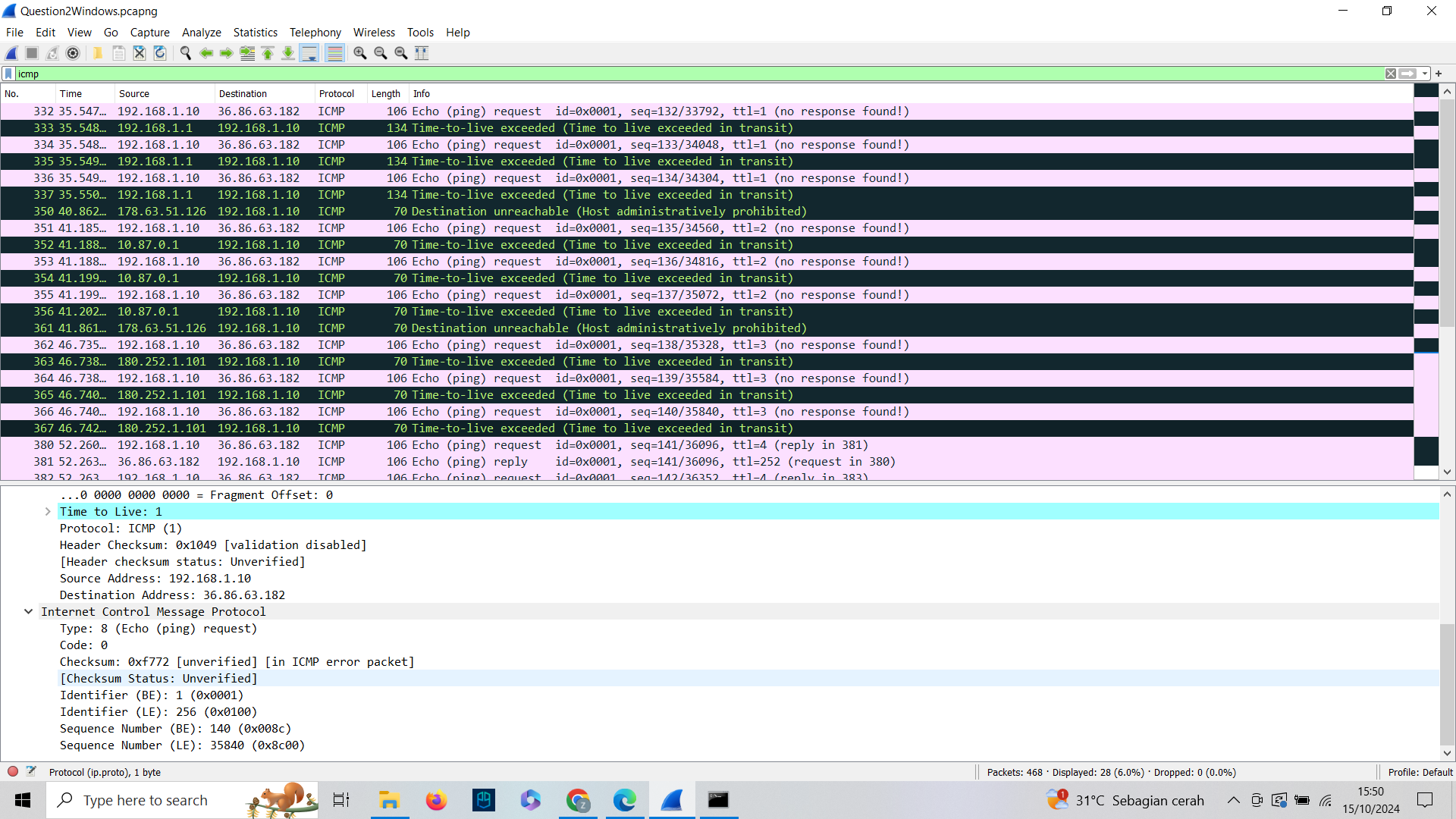


TASK 1



TASK 2

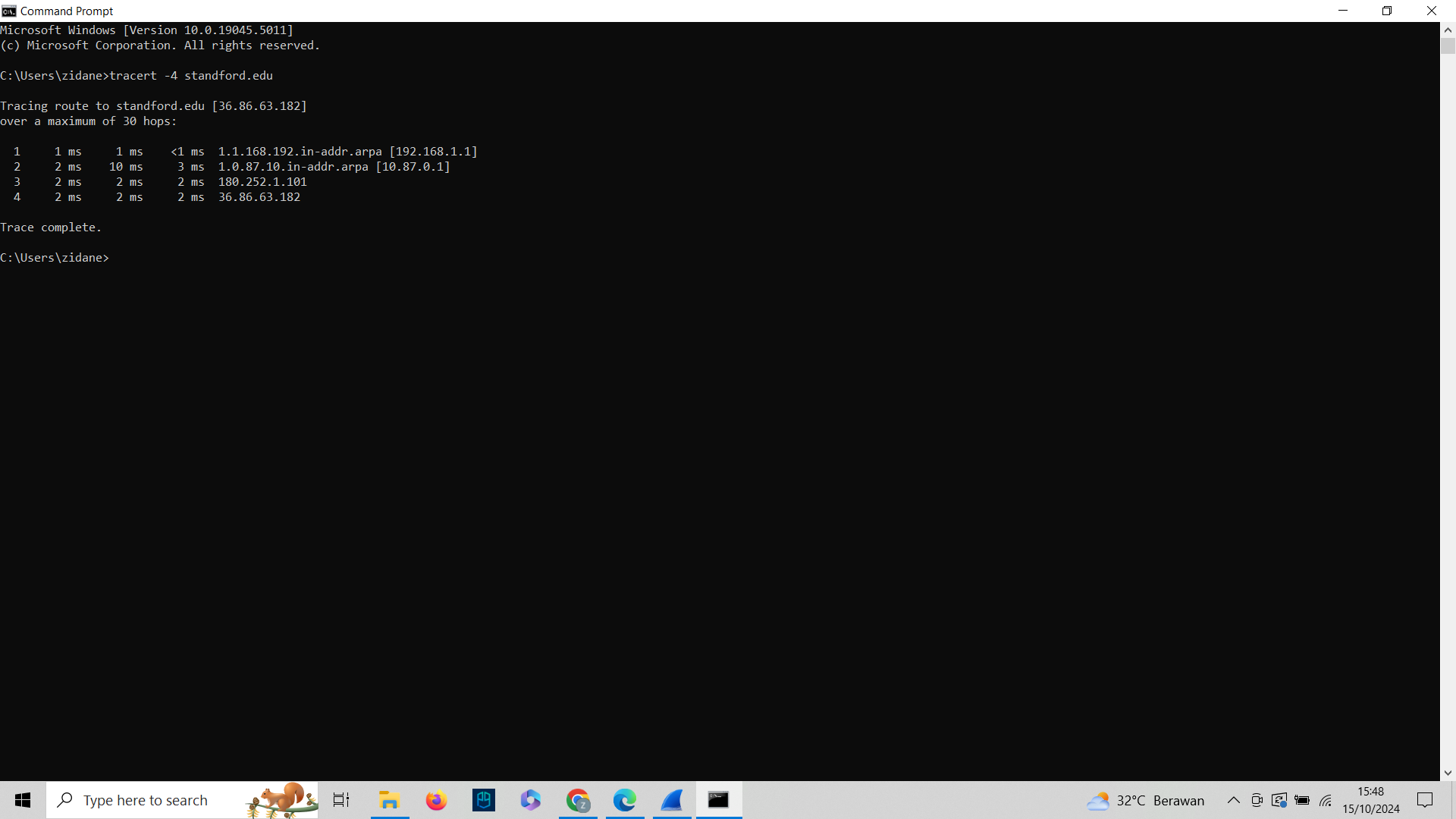
* Data per bytes : 64
* TTL : 4 dan 252
* Nilai yang tertera: 2 ms, 10 ms, 3 ms
* Nilai minimum: 2 ms
* Nilai maksimum: 10 ms
* Nilai rata-rata: (2+10+3) / 3 = 5 ms



TASK 3

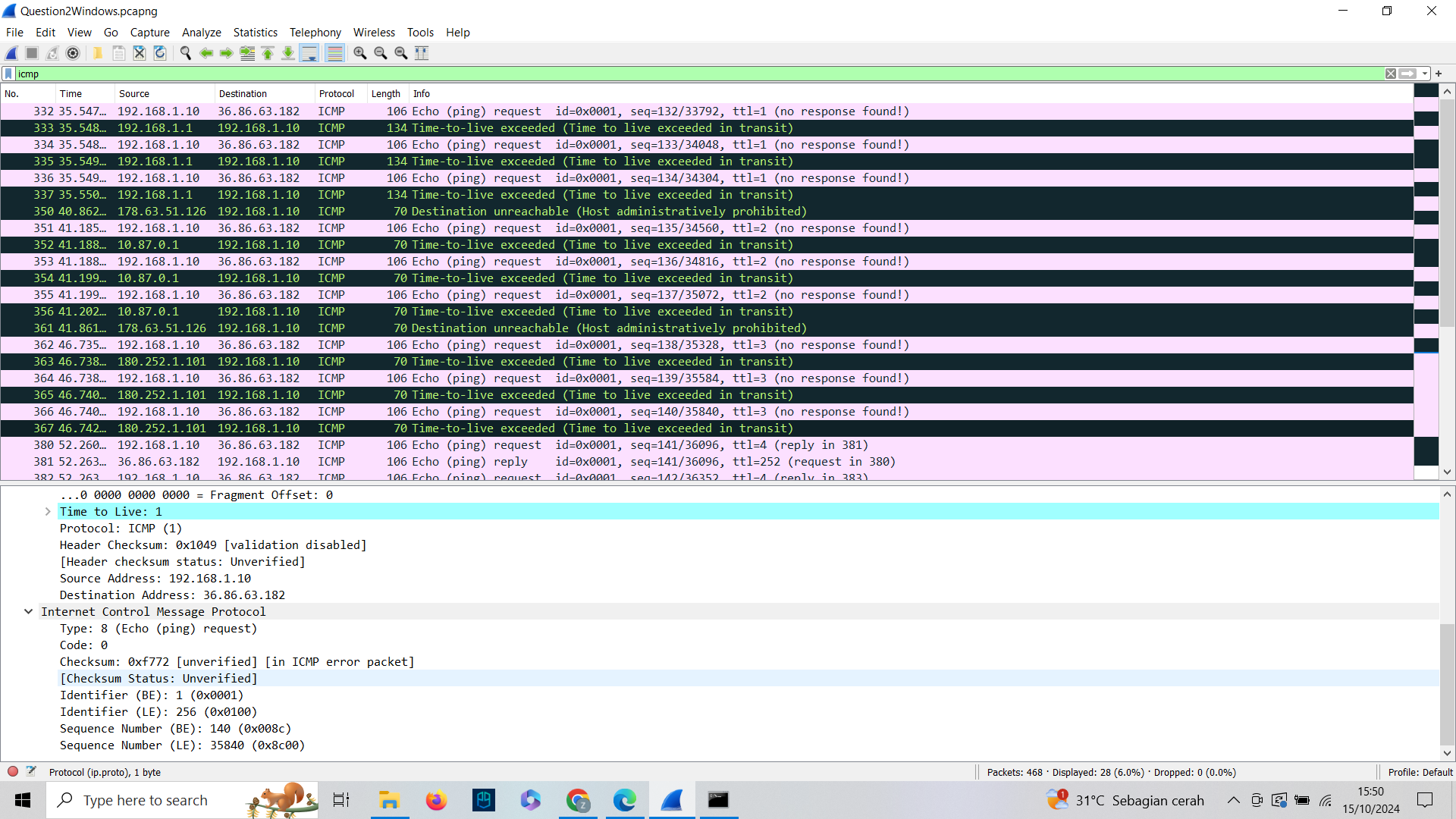
**Header IPv4**

* **Versi (Version):** Menunjukkan bahwa paket ini menggunakan protokol IPv4, versi yang paling umum digunakan di internet.
* **Panjang Header (Header Length):** Menunjukkan panjang header IPv4 dalam satuan byte. Nilai 20 byte adalah panjang minimum untuk header IPv4.
* **Bidang Layanan Terbedakan (Differentiated Services Field):** Digunakan untuk memberikan informasi kualitas layanan (QoS) yang diinginkan. Nilai 0x00 menunjukkan layanan "best effort" yang umum digunakan.
* **Panjang Total (Total Length):** Menunjukkan total panjang paket, termasuk header dan data. Dalam kasus ini, panjang paket adalah 92 byte.
* **Identifikasi (Identification):** Sebuah nomor unik yang diberikan pada setiap paket untuk m**Offset Fragmen (Fragment Offset):**melacak fragmen paket jika paket tersebut perlu dipecah menjadi bagian-bagian yang lebih kecil.
* **Flag:** Digunakan untuk mengontrol fragmentasi paket. Nilai 0x00 menunjukkan bahwa paket tidak dipecah. Menunjukkan posisi offset dari fragmen dalam paket asli jika paket tersebut dipecah.
* **Waktu Hidup (Time to Live):** Menunjukkan jumlah maksimum hop yang dapat dilalui paket sebelum dibuang. Nilai 4 menunjukkan bahwa paket hanya boleh melalu 4 router.
* **Protokol (Protocol):** Menunjukkan protokol yang digunakan dalam data paket. Dalam hal ini, protokolnya adalah ICMP (Internet Control Message Protocol).
* **Checksum Header:** Digunakan untuk mendeteksi kesalahan pada header IPv4.
* **Type**: Menunjukkan tipe pesan ICMP. Nilai 8 menunjukkan pesan echo request, yang biasa digunakan untuk melakukan ping.
* **Code:** Memberikan informasi tambahan tentang tipe pesan. Nilai 0 menunjukkan echo request biasa.
* **Checksum:** Digunakan untuk mendeteksi kesalahan pada pesan ICMP.
* **Identifier:** Digunakan untuk mengidentifikasi permintaan echo.
* **Nomor Urut (Sequence Number):** Digunakan untuk membedakan permintaan echo yang berbeda.
* **Data:** Data yang dikirimkan bersama dengan permintaan echo. Biasanya berisi data acak atau nol.



TASK 4

* Baris pertama menunjukkan proses pelacakan dimulai. Targetnya adalah stanford.edu yang memiliki alamat IP 36.86.63.182. Penelusuran dilakukan maksimal 30 lompatan (hop).
* Baris selanjutnya menunjukkan detail setiap lompatan:
* **Hop:** menunjukkan urutan lompatan. Maksimal 30 lompatan.
* **Time (ms):** menunjukkan waktu yang dibutuhkan untuk mencapai router tersebut dalam 3 percobaan (biasanya milidetik). Semakin kecil angkanya, semakin cepat koneksi.
* **Hostname (IP address):** menunjukkan nama domain (jika tersedia) dan alamat IP dari router yang dilewati.
* **1.1.168.192.in-addr.arpa [192.168.1.1]:** Nama ini merupakan alamat IP dalam format reverse DNS. Angka "192.168.1.1" adalah alamat IP yang umum digunakan untuk gateway default pada jaringan home atau small office. Jadi, router ini kemungkinan besar adalah router Anda sendiri atau router di dalam jaringan lokal Anda.
* **1.0.87.10.in-addr.arpa [10.87.0.1]:** Alamat IP ini menggunakan rentang alamat private (10.0.0.0/8). Ini adalah alamat yang sering digunakan di dalam jaringan internal suatu organisasi. Router ini kemungkinan adalah router milik ISP Anda atau router di jaringan backbone ISP.
* **180.252.1.101** : Kemungkinan alamat ini merupakan jaringan backbone ISP dan berfungsi sebagai titik transit untuk lalu lintas internet atau router yang menghubungkan jaringan internal ISP Anda ke jaringan internet yang lebih luas(NAT).
* **36.86.63.182** : Merupalan alamat server address dari standford.edu



TASK 5

**Type: 8 (Echo (ping) request):**

Ini artinya pesan ICMP ini adalah sebuah permintaan ping. Ping adalah sebuah perintah yang digunakan untuk memeriksa apakah sebuah perangkat di jaringan dapat dijangkau. Jadi, komputer pengirim sedang "mengetuk pintu" komputer tujuan untuk melihat apakah ada jawaban.

Kode: 0

Kode ini biasanya digunakan untuk memberikan informasi tambahan tentang tipe pesan. Dalam kasus ini, kode 0 menunjukkan bahwa ini adalah permintaan ping standar, tanpa ada informasi khusus lainnya.

**Checksum: 0xf771:**

Checksum ini seperti sidik jari dari header ICMP. Nilai ini dihitung berdasarkan data yang ada di header, dan digunakan untuk memastikan bahwa data tidak rusak selama perjalanan di jaringan. Jika nilai checksum yang diterima tidak sama dengan nilai yang dihitung, maka paket tersebut akan dibuang.

**Identifier: 1 (0x0001)**

Identifier ini seperti nomor seri untuk setiap permintaan ping. Jika sebuah komputer mengirim banyak permintaan ping, setiap permintaan akan memiliki identifier yang berbeda. Hal ini berguna untuk membedakan respon dari setiap permintaan.

**Sequence Number: 141 (0x008d)**

Sequence number ini digunakan untuk mengurutkan permintaan ping. Jika sebuah komputer mengirim beberapa permintaan ping secara berurutan, setiap permintaan akan memiliki nomor urut yang berbeda.

**Data (64 bytes)**

Bagian ini berisi data tambahan yang mungkin disertakan dalam pesan ICMP. Dalam kasus ping, data ini biasanya kosong atau berisi pola data tertentu.