LAPORAN PRAKTIKUM JARINGAN KOMPUTER
PRAKTIKUM 5 (ANALISA PAKET ICMP & DNS DI JARINGAN KOMPUTER)

Nama : Ahmad Husin

NPM : 2340304028

Kelompok : 8

LABORATORIUM JARINGAN KOMPUTER

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS TEKNIK

UNIVERSITAS BORNEO TARAKAN

PRAKTIKUM 5

Analisa Paket ICMP & DNS Di Jaringan Komputer

Kemampuan akhir yang diharapkan

Mampu menganalisa paket ICMP & DNS di jaringan komputer.

Materi Pembelajaran

1. Menggunakan simulator Packet Tracer.
2. Analisa Packet Data Unit

Bahan & Peralatan

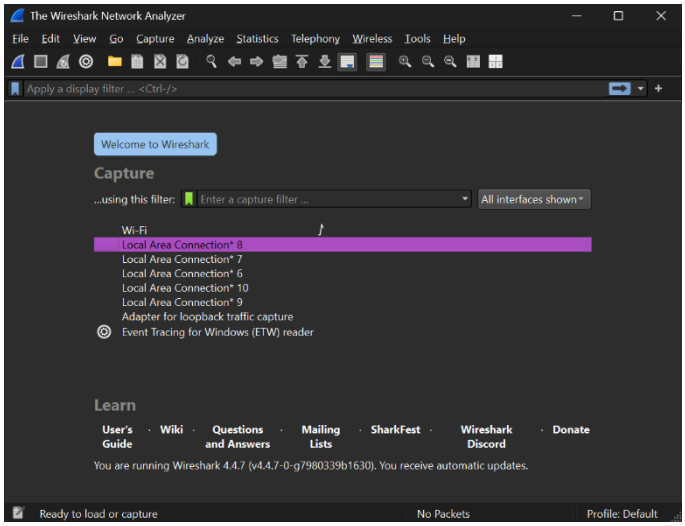
No.	Peralatan	Jumlah
1.	Komputer / Laptop	1 per mahasiswa
2.	Software Wireshark Versi 4	1 per mahasiswa

Indikator

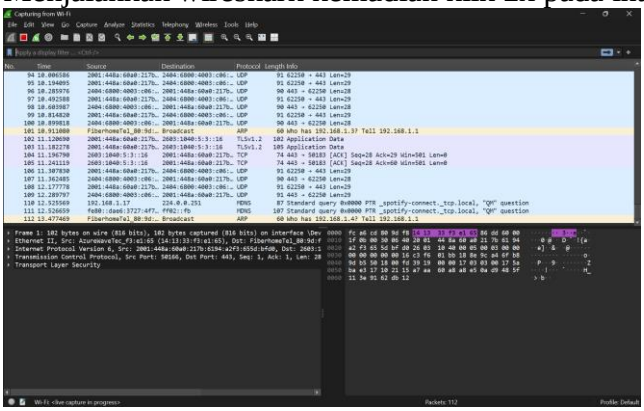
1. Mahasiswa mampu menganalisa paket ICMP pada jaringan komputer.
2. Mahasiswa mampu menganalisa paket DNS pada jaringan komputer.

Langkah – langkah praktikum :

1. Siaiapkan alat dan bahan praktikum sesuai pada tabel Peralatan.



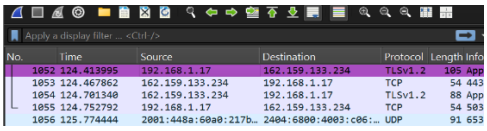
2. Mendownload & install software Wire Shark dari https://www.wireshark.org/ (jika belum terinstall di komputer).
3. Menjalankan wireshark kemudian klik 2x pada interface Ethernet.



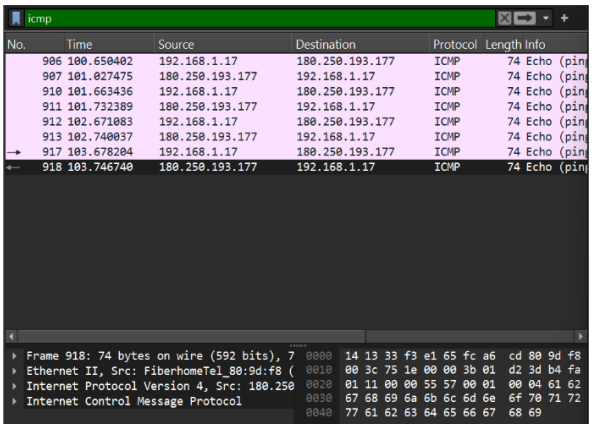
4. Membuka Command Prompt (cmd) kemudian ketikkan ping ke ubt.ac.id. pastikan Wireshark dalam posisi aktif / monitoring.

```
Microsoft Windows [Version 10.0.26100.4349]
(c) Microsoft Corporation. All rights reserved.

C:\Users\husen>ping ubt.ac.id

Pinging ubt.ac.id [180.250.193.177] with 32 bytes of da
ta:
Reply from 180.250.193.177: bytes=32 time=377ms TTL=59
Reply from 180.250.193.177: bytes=32 time=69ms TTL=59
Reply from 180.250.193.177: bytes=32 time=69ms TTL=59
Reply from 180.250.193.177: bytes=32 time=68ms TTL=59

Ping statistics for 180.250.193.177:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
,
Approximate round trip times in milli-seconds:
    Minimum = 68ms, Maximum = 377ms, Average = 145ms
```

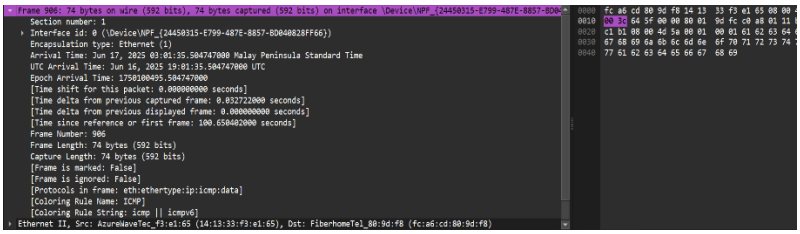
5. Mengklik pada tombol Stop Capturing Packet untuk menghentikan Wireshark dalam mengambil data dari jaringan komputer.



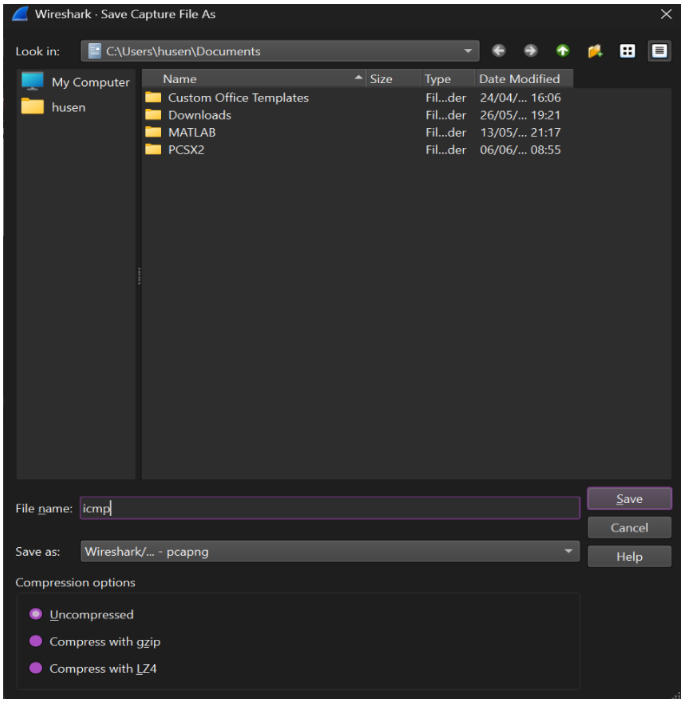
6. Mengetikan icmp pada kolom filter untuk menampilkan hanya paket ICMP.



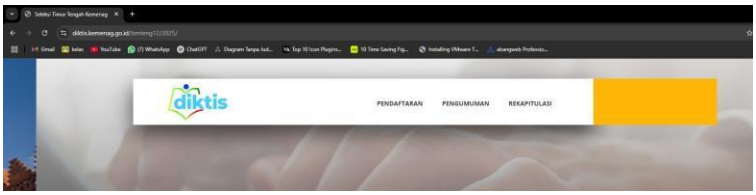
7. Mengklik pada salah satu frame kemudian Analisa isi dari frame tersebut di bagian bawah Wireshark.



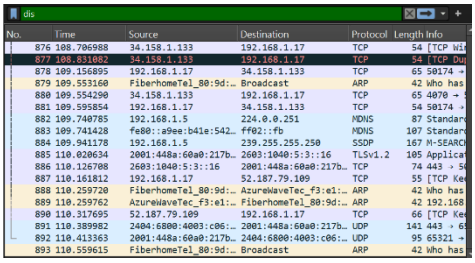
8. Mengaktifkan kembali Wireshark dengan klik icon segitiga biru. Klik save dan simpan dengan nama icmp.



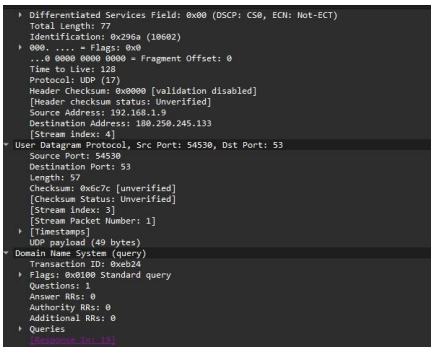
9. Membuka browser kemudian akses website https://diktis.kemenag.go.id dari browser anda.



10. Menstop kembali wireshark kemudian ketikkan dns pada kolom filter di wireshark. Kemudian cari frame diktis.kemenag.go.id pada kolom info



11. Mengklik pada window bagian bawah untuk menganalisa frame tersebut.


▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 77
Identification: 0x296a (10602)
▸ 000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.9
Destination Address: 180.250.245.133
[Stream index: 4]
▾ User Datagram Protocol, Src Port: 54530, Dst Port: 53
Source Port: 54530
Destination Port: 53
Length: 57
Checksum: 0x6c7c [unverified]
[Checksum Status: Unverified]
[Stream index: 3]
[Stream Packet Number: 1]
▸ [Timestamps]
UDP payload (49 bytes)
▾ Domain Name System (query)
Transaction ID: 0xeb24
▸ Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▸ Queries
[Response In: 191]