

**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

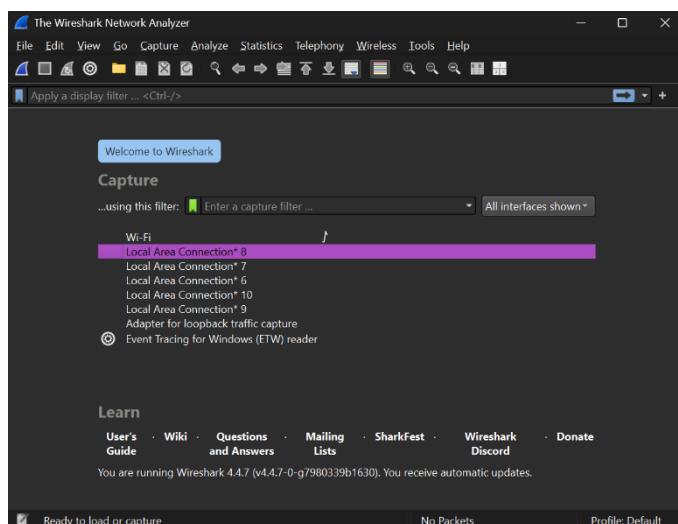
No.	Peralatan	Jumlah
1.	Komputer / Laptop	1 per mahasiswa
2.	Software Wireshark Versi 4	1 per mahasiswa

Indikator

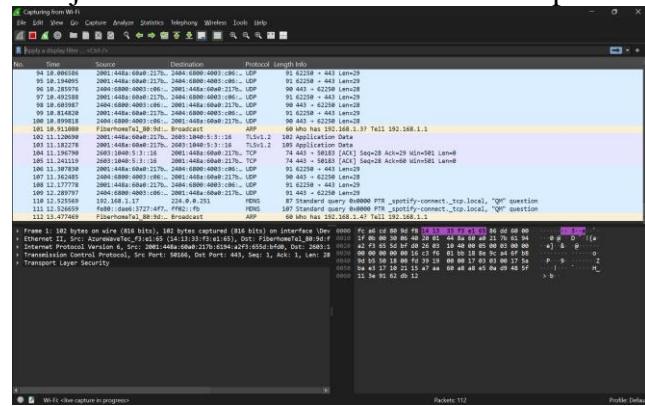
1. Mahasiswa mampu menganalisa paket ICMP pada jaringan komputer.
2. Mahasiswa mampu menganalisa paket DNS pada jaringan komputer.

Langkah – langkah praktikum :

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



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



- 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 data:
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
```

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

No.	Time	Source	Destination	Protocol	Length Info
1852	124.433959	192.168.1.17	162.159.133.234	TLSv1.2	195
1853	124.437652	162.159.133.234	192.168.1.17	TCP	54 443
1854	124.701540	162.159.133.234	192.168.1.17	TLSv1.2	60 443
1855	124.752792	192.168.1.17	162.159.133.234	TCP	54 593
1856	125.744444	2001:448a:60a0:217b::	2494:6880:4003:c06::	UDP	91 653

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

No.	Time	Source	Destination	Protocol	Length Info
906	100.650402	192.168.1.17	180.250.193.177	ICMP	74 Echo (ping)
907	101.027475	180.250.193.177	192.168.1.17	ICMP	74 Echo (ping)
910	101.663436	192.168.1.17	180.250.193.177	ICMP	74 Echo (ping)
911	101.732389	180.250.193.177	192.168.1.17	ICMP	74 Echo (ping)
912	102.671883	192.168.1.17	180.250.193.177	ICMP	74 Echo (ping)
913	102.740037	180.250.193.177	192.168.1.17	ICMP	74 Echo (ping)
917	103.678204	192.168.1.17	180.250.193.177	ICMP	74 Echo (ping)
918	103.746748	180.250.193.177	192.168.1.17	ICMP	74 Echo (ping)

Frame 918: 74 bytes on wire (592 bits), 7 0000 14 13 33 f3 e1 65 fc a6 cd 80 9d f8
> Ethernet II, Src: FiberhomeTel_80:9d:f8 (00:00:3c:75:1e:00) -> 00:00:3b:01:d2:3d bfa
> Internet Protocol Version 4, Src: 180.250.0.2020 01:11:00:00:55:57:00:01 00:04:61:62
> Internet Control Message Protocol 00:00:67:68:69:6a:6b:6c:6d:6e 6f:70:71:72
00:00:77:61:62:63:64:65:66:67 68:69

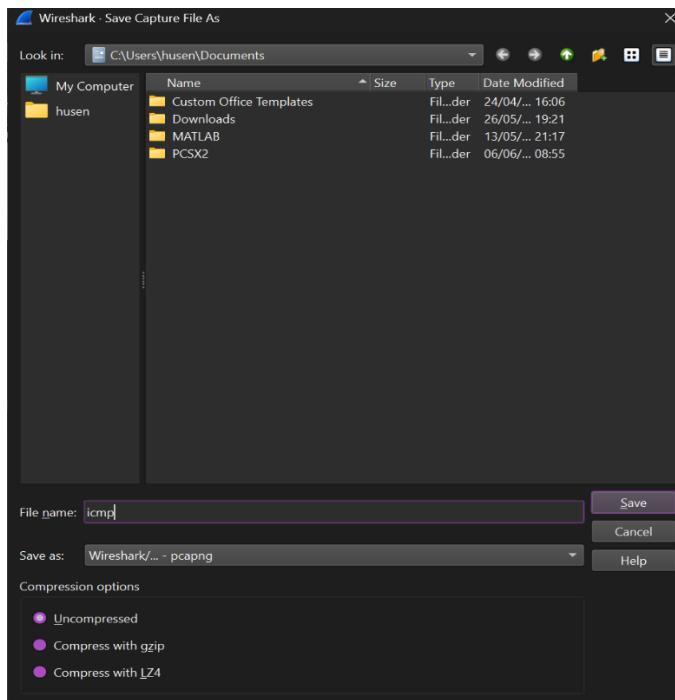
- Mengklik pada salah satu frame kemudian Analisa isi dari frame tersebut di bagian bawah Wireshark.

```

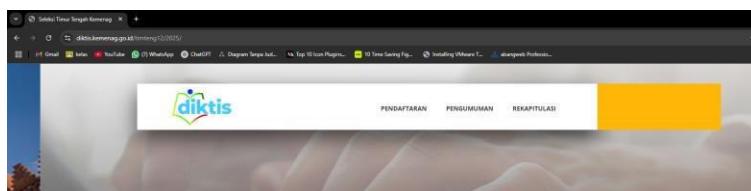
Frame 988: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{24450315-8799-487E-8857-004682FF66}
  Section number: 1
  > Interface id: 0 (Microsoft NPF_{24450315-8799-487E-8857-004682FF66})
  Encapsulation type: Ethernet (1)
  Arrival Time: Jun 17, 2025 03:15:58.047470000 Malay Peninsula Standard Time
  UTC Arrival Time: Jun 16, 2025 19:15:35.584747000 UTC
  Epoch Arrival Time: 179810495.584747000
  [Time shift for this packet: 0.000000 seconds]
  [Time since previous captured frame: 0.000000000 seconds]
  [Time since previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 100.656402000 seconds]
  Frame Number: 988
  Frame Length: 74 bytes (592 bits)
  Capture Length: 74 bytes (592 bits)
  [Frame is Marked: False]
  [Frame is Ignored: False]
  [Protocols in Frame: ethernet-type:ip:icmp-data]
  [Coloring Rule Name: ICMP]
  [Coloring Rule String: icmp || icmp6]
  Ethernet II, Src: AzurewaveTe_f3:e1:65 (14:13:33:f3:e1:65), Dst: FiberhomeTel_80:9d:f8 (fc:a6:cd:80:9d:f8)

```

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



- Membuka browser kemudian akses website <https://diktis.kemenag.go.id> dari browser anda.



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

No.	Time	Source	Destination	Protocol	Length	Info
876	188.706988	34.158.1.133	192.168.1.17	TCP	54	[TCP Win 1]
877	188.831882	34.158.1.133	192.168.1.17	TCP	54	[TCP Dup Win 1]
878	188.831885	34.158.1.133	192.168.1.17	TCP	54	[TCP Dup Win 1]
879	189.553160	FiberhomeTel_80:9d:f8	Broadcast	ARP	42	who has
880	189.554290	34.158.1.133	192.168.1.17	TCP	65	4978 x
881	189.595854	192.168.1.17	34.158.1.133	TCP	54	50374 x
882	189.740785	192.168.1.5	224.0.0.251	MDNS	87	Standard
883	189.741428	#880:a9ee:b41:542	#f02:1:fb	MDNS	107	Standard
884	189.941178	192.168.1.5	231.253.255.250	SSDP	167	N-SEARCH
885	189.941184	192.168.1.5	231.253.255.250	SSDP	167	N-SEARCH
886	110.126708	2409:1840:5:13::16	2801:48c:69a:217b::1	TCP	102	14:13:33.79.1.2
886	110.126708	2409:1840:5:13::16	2801:48c:69a:217b::1	TCP	74	443 x 56
887	110.161812	192.168.1.17	52.187.79.109	TCP	55	[TCP Keepalive]
888	110.259720	FiberhomeTel_80:9d:f8	AzurewaveTec_f3:e1:65	ARP	42	who has
889	110.317693	AzurewaveTec_f3:e1:65	FiberhomeTel_80:9d:f8	ARP	42	192.168.52.187.79.109
890	110.413363	2404:1880:1:69a:217b::1	2404:1880:1:69a:217b::1	UDP	140	14:13:33.79.1.2
891	110.413363	2404:1880:1:69a:217b::1	2404:1880:1:69a:217b::1	UDP	95	65321 x
892	110.413363	2404:1880:1:69a:217b::1	2404:1880:1:69a:217b::1	UDP	95	65321 x
893	110.559615	FiberhomeTel_80:9d:f8	Broadcast	ARP	42	who has

- Mengklik pada window bagian bawah untuk menganalisa frame tersebut.

```
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 77
  Identification: 0x0056 (10602)
  ...0 0000 0000 0000 = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (17)
  Header Checksum: 0x0000 [Validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.3.1.9
  Destination Address: 100.250.245.133
  [Source IP: 192.168.3.1]
  [Destination IP: 100.250.245.133]

- User Datagram Protocol, Src Port: 54530, Dst Port: 53
  Source Port: 54530
  Destination Port: 53
  Length: 49
  Data bytes: 0xe6c7c: [unverified]
  [Checksum Status: Unverified]
  [Stream Index: 3]
  [Stream Packet Number: 1]
  > [TTL: 128]
    UDP payload (49 bytes)

- Domain Name System (query)
  Transaction ID: 0xed24
  > Flags: 0x0000 Standard query
  Question: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  > Queries
    > [Query ID: 193]
```