

# Lab#3: Traffic Analysis

ผศ.ดร. อนันต์ พลเพิ่ม

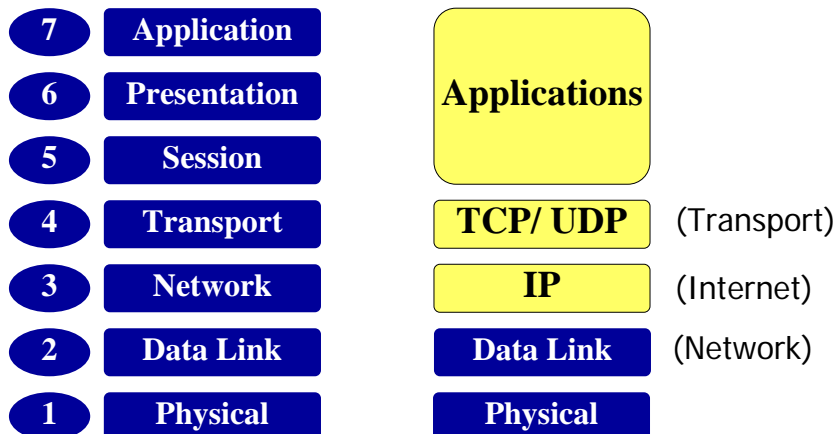
Asst.Prof.Anan Phonphoem, Ph.D.

[anan@cpe.ku.ac.th](mailto:anan@cpe.ku.ac.th)

<http://www.cpe.ku.ac.th/~anan>  
Computer Engineering Department  
Kasetsart University, Bangkok, Thailand

1

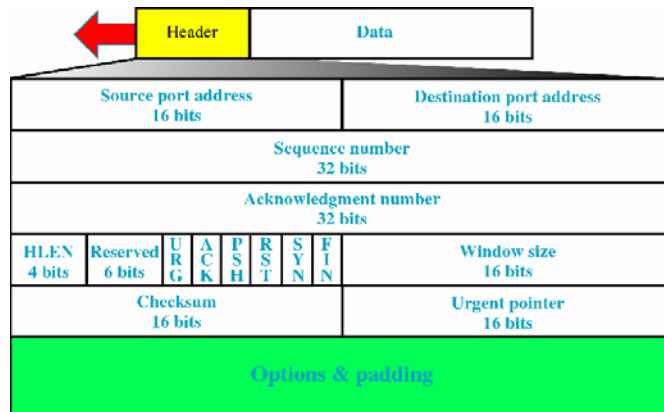
# OSI Model and TCP/IP



2

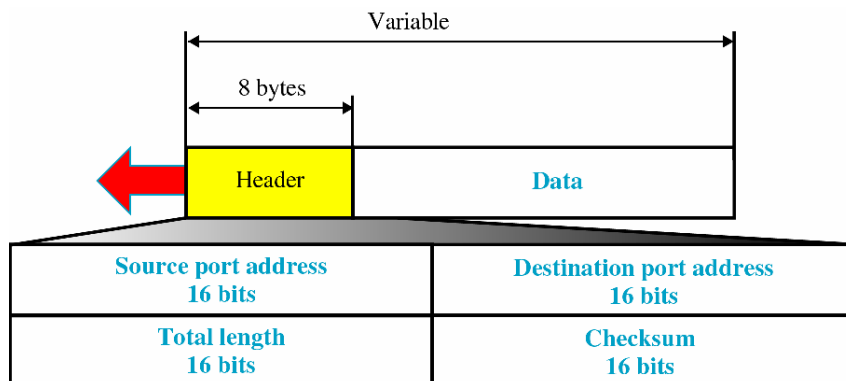


# TCP Segment Format



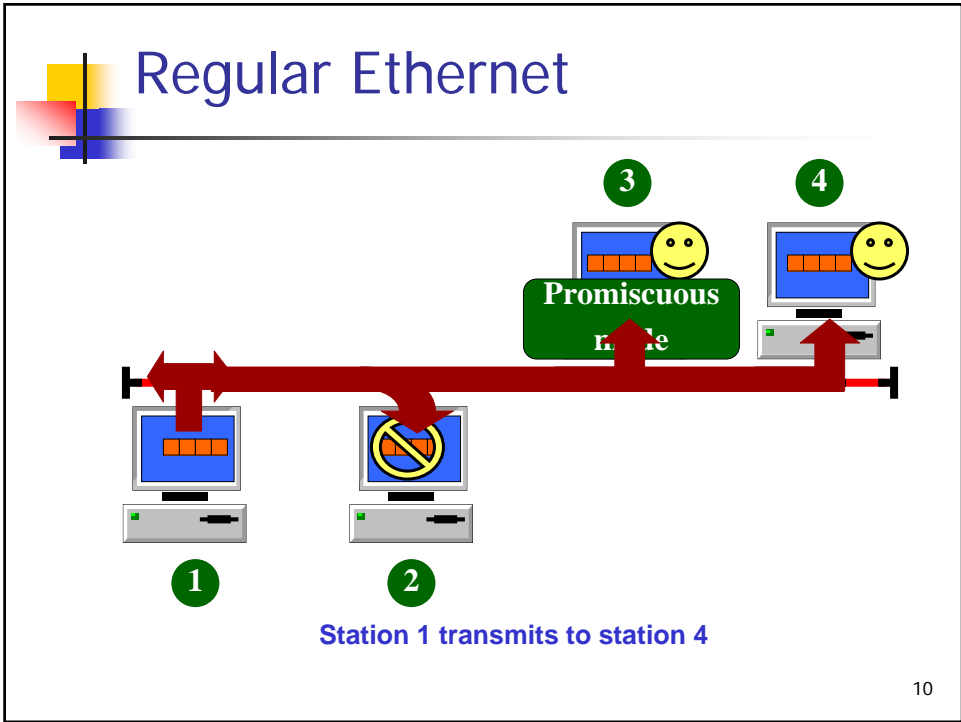
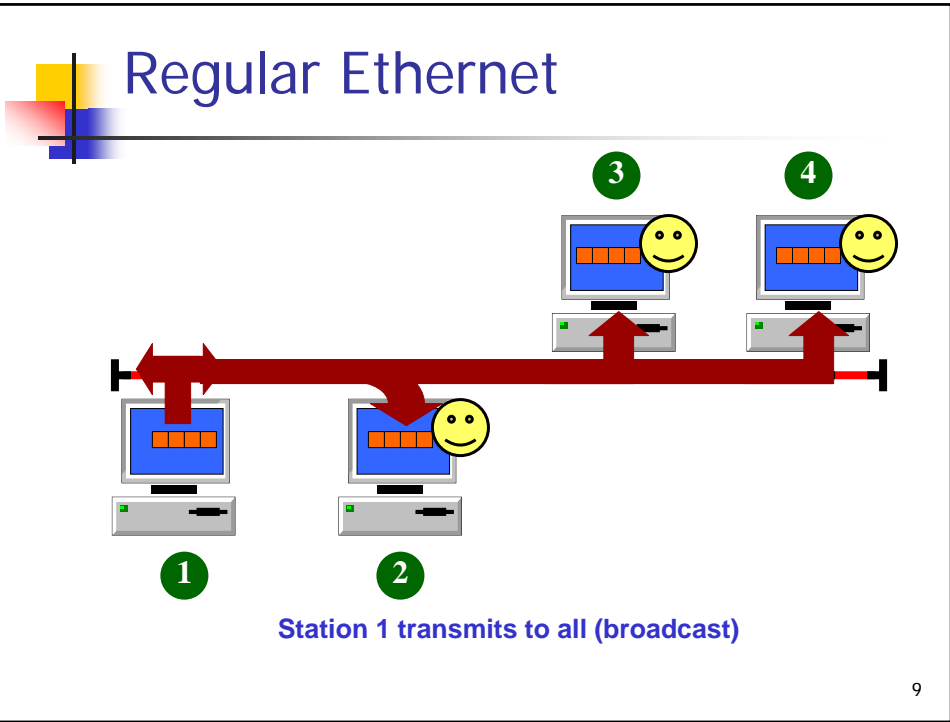
5

# UDP Datagram Format



6





# Sniffer

- Network and protocol analyzer
- For network maintenance and trouble shooting
- Capture, monitor, analyze, trouble shooting
- Example: Etherpeek, Ethereal

11

# Ethereal

The screenshot displays the Ethereal (Wireshark) interface. The main window shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Info. The selected packet (No. 357) is highlighted in blue. Below the list, the packet details pane shows the structure of the selected packet: Ethernet II, Internet Protocol, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Info
356	3.394264	158.108.2.69	158.108.135.137	HTTP	HTTP/1.1 304 Not Modified
357	3.394283	158.108.135.137	158.108.2.69	TCP	1617 > http [ACK] Seq=130
358	3.394302	158.108.135.137	158.108.2.69	TCP	1617 > http [ACK] Seq=130
359	3.394355	158.108.2.69	158.108.135.137	HTTP	HTTP/1.1 304 Not Modified
360	3.394360	158.108.2.69	158.108.135.137	TCP	http > 1618 [FIN, ACK] Seq=1618
361	3.394370	158.108.135.137	158.108.2.69	TCP	1618 > http [ACK] Seq=1618
362	3.395642	158.108.135.137	158.108.2.69	TCP	1617 > http [FIN, ACK] Seq=1617
363	3.395798	158.108.2.69	158.108.135.137	TCP	http > 1617 [ACK] Seq=1617
364	3.397766	158.108.135.137	158.108.2.69	TCP	1618 > http [FIN, ACK] Seq=1618
365	3.397946	158.108.2.69	158.108.135.137	TCP	http > 1618 [ACK] Seq=1618

Frame 357 (60 bytes on wire (60 bytes captured))

Ethernet II, Src: 00:04:dd:49:22:02, Dst: 00:0b:5d:51:ac:5b

Internet Protocol, Src Addr: 158.108.2.69 (158.108.2.69), Dst Addr: 158.108.135.137 (158.108.135.137)

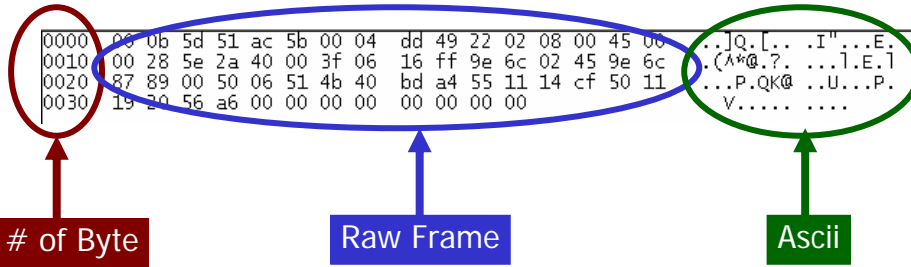
Transmission Control Protocol, Src Port: http (80), Dst Port: 1617 (1617), Seq: 130, Ack: 1617

0000 00 0b 5d 51 ac 00 04 dd 49 22 02 08 00 45 00 ..]Q.L..I" .E.  
0010 00 28 5e 2a 40 00 3f 06 16 ff 9e 6c 02 45 9e 6c (<A>?7. ..1.E.1  
0020 87 89 00 50 06 51 4b 40 bd a4 55 11 14 cf 50 11 ..P.Qk@ ..U..P.  
0030 19 20 56 a6 00 00 00 00 00 00 00 00 ..V.....

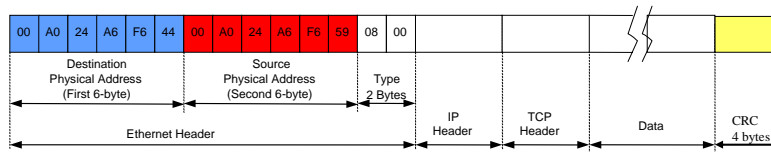
Frame (frame), 60 bytes: P: 703 D: 703 M: 0

12

# Raw Frame



# Ethernet Header/Trailer



Ethernet Header

Ethernet Trailer

```

Ethernet II, Src: 00:04:dd:49:22:02, Dst: 00:0b:5d:51:ac:5b
  Destination: 00:0b:5d:51:ac:5b (128.199.0.2)
  Source: 00:04:dd:49:22:02 (158.108.128.1)
  Type: IP (0x0800)
  Trailer: 000000000000
  Internet Protocol, Src Addr: 158.108.2.69 (158.108.2.69), Dst Addr: 158.108.135.137 (158
  Transmission Control Protocol, Src Port: http (80), Dst Port: 1617 (1617), Seq: 130, Ack
  0000 00 0b 5d 51 ac 5b 00 04 dd 49 22 02 08 00 45 00 ..]Q.[...I"...E.
  0010 00 28 5e 2a 40 00 3f 06 16 ff 9e 6c 02 45 9e 6c (.A*Q.?...].E.]
  0020 87 89 00 50 06 51 4b 40 bd a4 55 11 14 cf 50 11 ...P.QK@ ..U...P.
  0030 19 20 56 a6 00 00 00 00 00 00 00 00 00 00 00 V.....
  
```

# IP Header

**Destination IP Address**  
158.108.135.137

**Source IP Address**  
9e 6c 02 45  
158.108.2.69

```

> Internet Protocol, Src Addr: 158.108.2.69 (158.108.2.69), Dst Addr: 158.108.135.137 (158.108.135.137)
> Transmission Control Protocol, Src Port: http (80), Dst Port: 1617 (1617), Seq: 130, Ack: 1617, Win: 65536, Len: 100

```

0000	00 0b 5d 51 ac 5b 00 04 dd 49 22 02 08 00 45 00	..]Q.[...I"...E.
0010	00 28 5e 2a 40 00 3f 06 16 ff 9e 6c 02 45 9e 6c	.(A*Q.?....].E.]
0020	87 89 00 50 06 51 4b 40 bd a4 55 11 14 cf 50 11	..P.QK@...U...P.
0030	19 20 56 a6 00 00 00 00 00 00 00 00	.V....

# TCP Header

**TCP Header**

```

> Transmission Control Protocol, Src Port: http (80), Dst Port: 1617 (1617), Seq: 130, Ack: 1617, Win: 65536, Len: 100

```

0000	00 0b 5d 51 ac 5b 00 04 dd 49 22 02 08 00 45 00	..]Q.[...I"...E.
0010	00 28 5e 2a 40 00 3f 06 16 ff 9e 6c 02 45 9e 6c	.(A*Q.?....].E.]
0020	87 89 00 50 06 51 4b 40 bd a4 55 11 14 cf 50 11	..P.QK@...U...P.
0030	19 20 56 a6 00 00 00 00 00 00 00 00	.V....



# Live Capture

---

- Demo