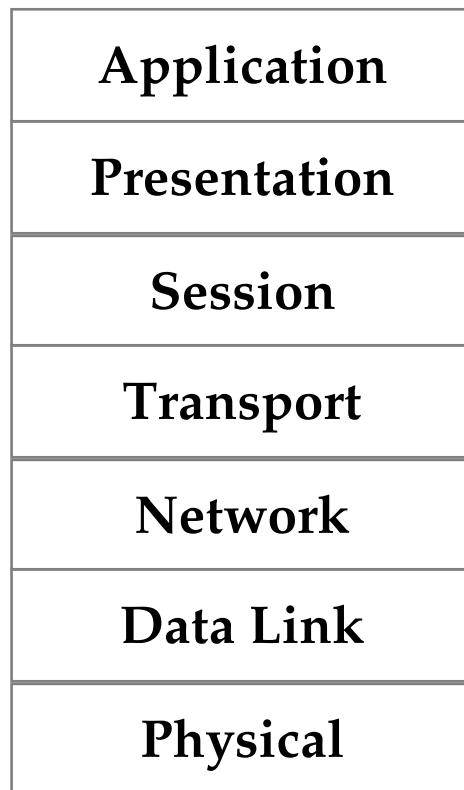


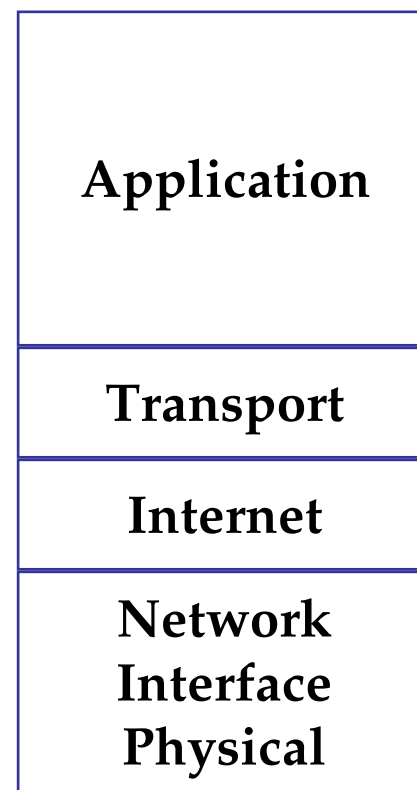
NETWORK FORENSIC

Pengantar
Budi Rahardjo
2004

Perbandingan OSI & TCP/IP

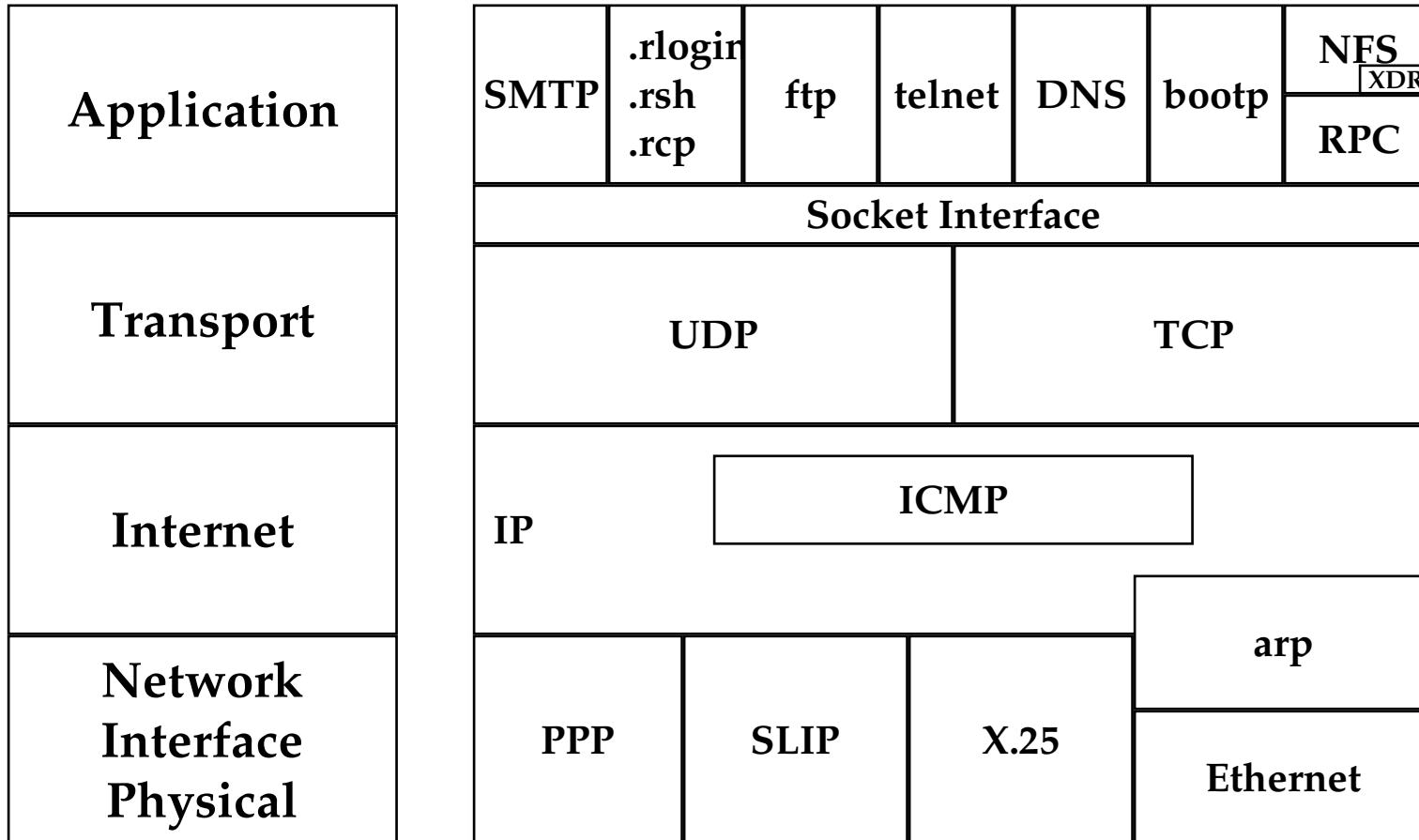


OSI



TCP/IP

Layer TCP/IP



Header & Data

- Header di sebuah layer menjadi data di layer berikutnya

TCP Header				Header	Data
IP Datagram			Header	Data	
Frame		Header	Data		
	Header	Data			

IP Header: 20 bytes

VER		TOS	Length in bytes
ID Field			Frag offset
TTL	Protocol		Header Checksum
Source IP Address			
Destination IP Address			

Sample TCP/IP Packet

Frame Header 14 bytes	IP Header 20 bytes	Protocol Header 20 bytes	Protocol Data 14 bytes
--------------------------	-----------------------	-----------------------------	---------------------------



Ethernet Frame



IP Datagram



Embedded Packet TCP, UDP, ICMP

TCPdump

- Tools untuk menganalisa packet
- Tersedia source code (untuk sistem UNIX)
- Ada WinDump untuk MS Windows

TCPdump Output

```
09:32:43:910000 nmap.edu.1173 > dns.net.21: S  
62697789:62697789(0) win 512
```

- **09:32:43:910000**: Time stamp
- **nmap.edu**: Source host name
- **1173**: Source port number
- **>**: tanda arah paket
- **dns.net**: Destination host name
- **21**: Destination port number
- **s**: TCP flag
- **62697789:62697789(0)**: TCP sequence number
begin:end (data bytes)
- **win 512**: Receiving TCP buffer size (in bytes) of
nmap.edu

TCP Flags

- SYN “S”
- ACK “ack”
- FIN “F”
- RESET “R”
- PUSH “P”
- URGENT “urg”
- Placeholder “.”

Tugas

- Tangkap “sesi” ICPM (via *ping*)
- Tangkap sesi *telnet* & *ftp*, khususnya perhatikan 3-way handshaking
- Tangkap sebuah sesi *nmap* yang melakukan port scanning
(boleh bebas atau menggunakan flag tertentu, misalnya untuk scanning dengan SYN saja)
- Beri komentar