CIS 700/002 : Special Topics :
Wireshark

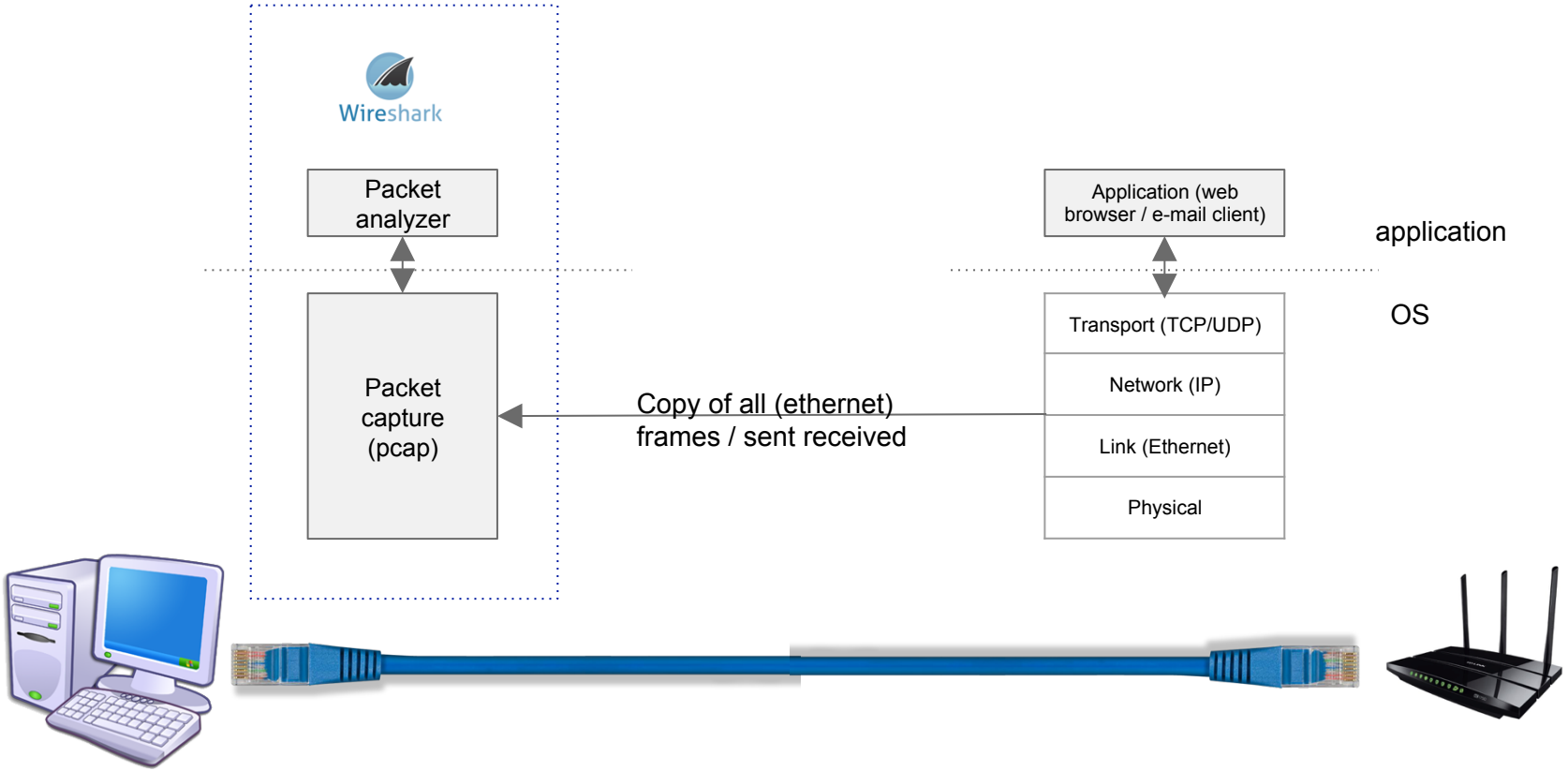
Bipeen Acharya and Omkar Nalawade
CIS 700/002: Security of EMBS/CPS/IoT
Department of Computer and Information Science
School of Engineering and Applied Science
University of Pennsylvania

2017-2-24

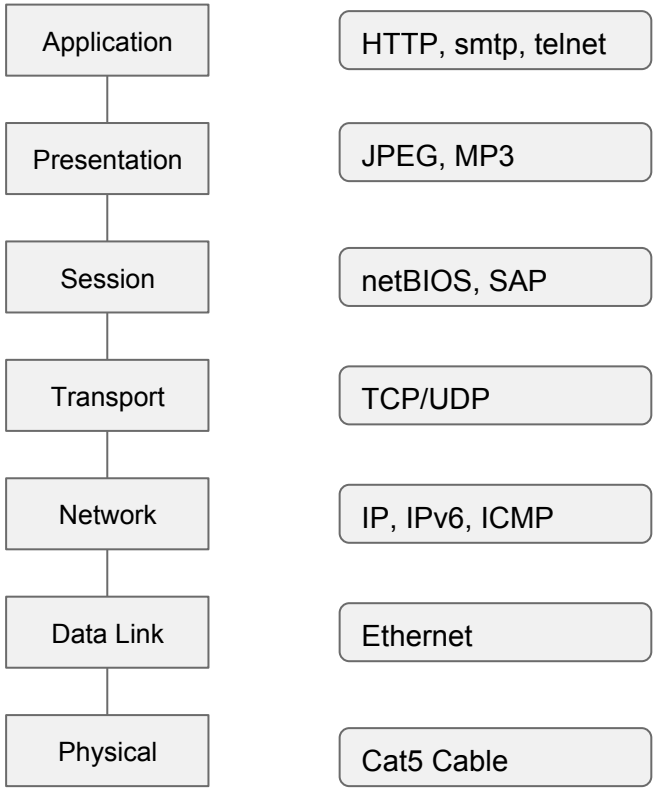
What is Wireshark?

- Network Packet Analyzer
  - –Capture packets and display detailed packet data
- Uses
  - –Troubleshoot network problems
  - –Examine security problems
  - –Debug protocol implementations

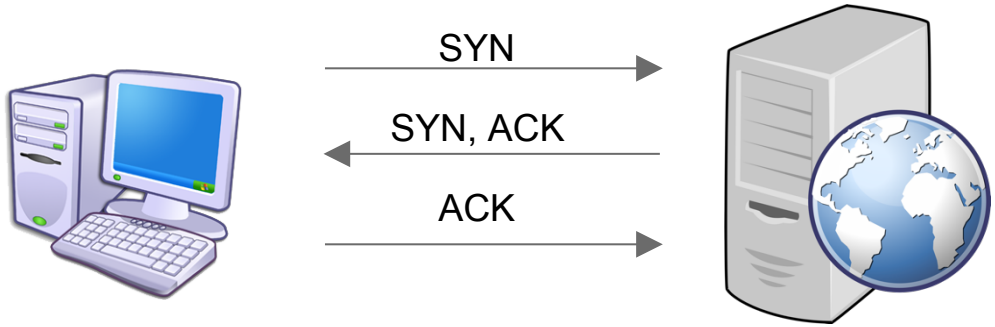
In the back


Wireshark
Packet analyzer
Packet capture (pcap)
Copy of all (ethernet) frames / sent received
Application (web browser / e-mail client)
Transport (TCP/UDP)
Network (IP)
Link (Ethernet)
Physical
application
OS

OSI layer


Application
HTTP, smtp, telnet
Presentation
JPEG, MP3
Session
netBIOS, SAP
Transport
TCP/UDP
Network
IP, IPv6, ICMP
Data Link
Ethernet
Physical
Cat5 Cable

TCP 3 way handshake



Using the GUI

- Capture Interfaces and options
- Start capture
- View capture (no, time, source, destination, protocol)
- Capture and Display Filters
- Follow TCP stream

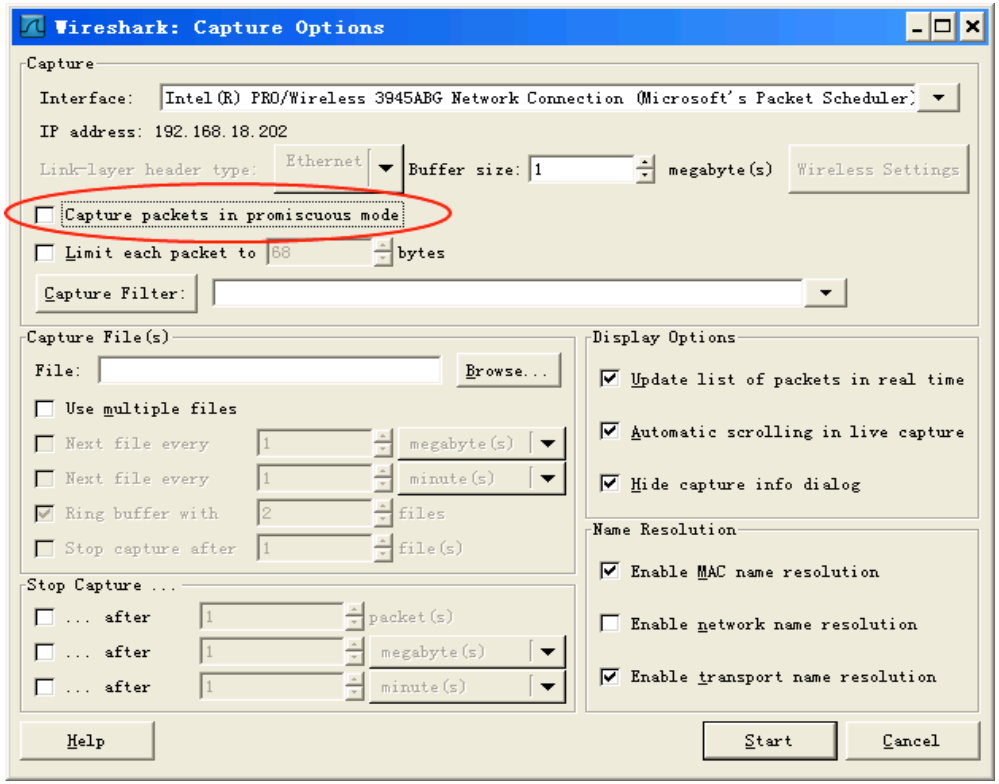
https://www.youtube.com/watch?v=6X5TwvGXHP0

Using the GUI

- Coloring rules / scheme

Promiscuous mode

- Listen on packets that do not pertain to you



Filters

- ip.addr (ip.src / ip.dst) == 10.0.0.145
- Http / tcp / DNS / arp → dns or http
- tcp.port == portno
- Tcp.analysis.flags (problems identified)
- !(arp or dns or icmp) → pruning
- Tcp/udp contains facebook
- Http.request → all gets, servers, clients
- Http.response.code == 200 (OK), 404, 500 (error)
- Tcp.flags.syn == 1

Wireshark - ARP & ICMP Packets

```
C:\Users\Omkar>ping 69.249.18.45

Pinging 69.249.18.45 with 32 bytes of data:
Reply from 69.249.18.45: bytes=32 time=114ms TTL=64
Reply from 69.249.18.45: bytes=32 time=5ms TTL=64
Reply from 69.249.18.45: bytes=32 time=9ms TTL=64
Reply from 69.249.18.45: bytes=32 time=22ms TTL=64

Ping statistics for 69.249.18.45:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 114ms, Average = 37ms
```

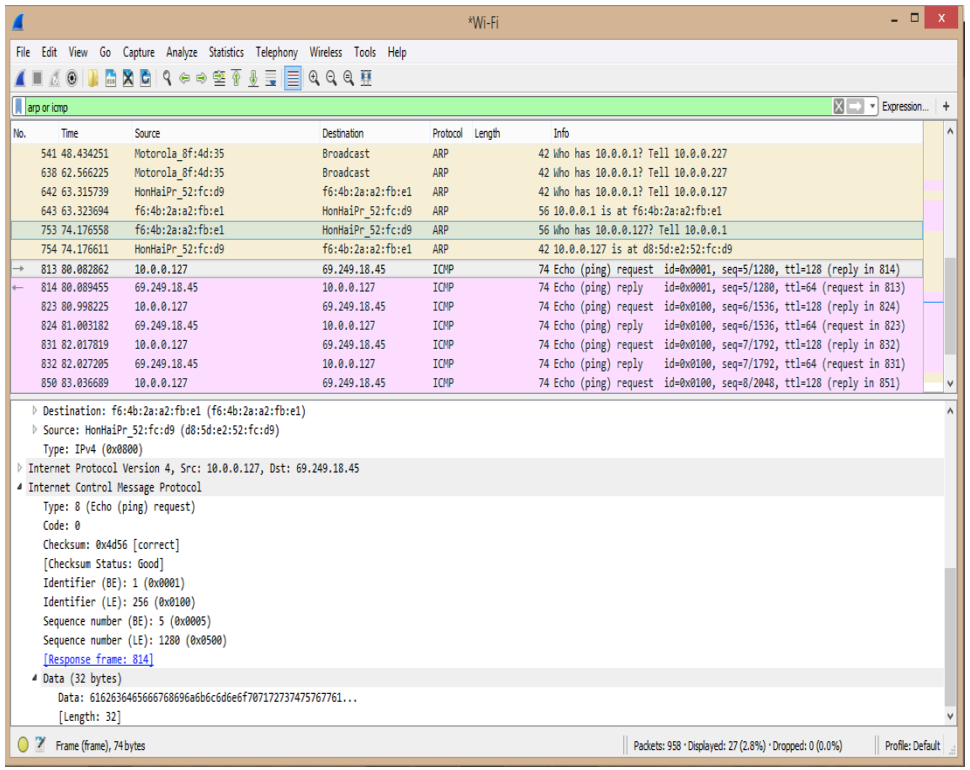
Generate ICMP traffic by using the Ping Command to check the connectivity of any neighbouring machine.

Simultaneously start Wireshark to capture the ARP and ICMP packets.

Wireshark -ARP & ICMP

1) ARP request broadcast
From PC determines the
Physical MAC address
Of the n/w IP address.

2)After ARP request, the
Pings echo request
And replies can be seen



Disadvantages

1) Wireshark is not intrusion detection system. No warnings if anyone does strange things on the network that is not allowed for that person.

2) No manipulations allowed on the network, it is just a network analyzer tool. Wireshark does not send packets on the network.

Concepts

1) Packet Sniffing.
2) GET vs POST
3) HTTP vs HTTPS
4) Monitor Mode in MacOS
5) Facebook Password Sniffing Using Cookie Injector and GreaseMonkey - Practice

THANK YOU

Questions

1. Capture http traffic, browse the web and find browsed images.
2. Capture home traffic and attempt to decrypt with Wireshark by providing Wireshark with the decryption keys.
3. What are some ways one can increase privacy on the web?
4. What is the difference between promiscuous mode and monitor mode?
5. How are packets sent and received on the OSI layer?
6. What is the difference between Capture filters and display filters?