Experiential Learning Workshop on HTTP(S)

Jan 17, 2017

Dr. Ram P Rustagi
Dept of CSE
PES University
rprustagi@pes.edu

Network

Acronym

- **N**ovel
- **E**xperience of
- **T**heoretical,
- **W**orking,
- **O**perational, and
- **R**ealized
- **K**nowledge

Learning...

- Clarify your doubt
- Don't **ASSUME**
- If you do assume, following happens

ASS

U

ME

- **Stop not, allowed to go,** `or`
  Stop, not allowed to go
- Tying your shoes?

Expecations and Experience

- Define your expectations
- Make the learning fun with challenges
- Experience is the best tutor
  – Can only be acquired, can't be given
- Understand team working
- Exploit yourself to know your limits
  – and extend these
- Do your SWOT analysis

Exploration Topics

- Overview of Internet
- Overview of OSI Layers
- Overview of Tools
- Understanding Wireshark
- Wireshark filters
- Exercise - 1
- Overview of IP
- Exercise - 2
- Misc Content
- Summary

Recommended Readings

- Vint Cerf, Father of Internet, looks forward/back
  - http://www.washingtonpost.com/national/health-science/vint-cerf-father-of-the-internet-looks-forward--and-back/2014/07/28/3bc5c728-0876-11e4-8a6a-19355c7e870a_story.html
- Tim Berners Lee, As we celebrate 20 years…
  - http://blog.ted.com/2013/04/30/as-we-celebrate-20-years-of-the-world-wide-web-lessons-from-tim-berners-lee/
- Tim Berners Lee, A recap of "Where are we now?"
  - http://blog.ted.com/2014/03/19/power-poses-idea-technologies-and-the-internets-birthday-a-recap-of-where-are-we-now-all-stars-session-3-at-ted2014/

Vint Cerf Quotes

- We owe it to people who are not familiar with technology to make it as easy as possible to use.
- I am a little mystified with people who get carried away with some of the social networking activity. But I am not confounded by it.
- My wife is an avid user of the Internet, although it took me years to get her to use e-mail.
- I stay in touch with a very large group of friends around the world by means of e-mail. For me, it is an incredibly powerful tool.
- Writing software is a very intense, very personal thing. You have to have time to work your way through it, to understand it. Then debug it.

Lessons from Tim Berners Lee

- Harness your own frustration
  - annoyed that he couldn't collaborate easily and seamlessly with the many colleagues
- Involve others early
  - find your people and figure out how to harness their ideas and input. The web has enabled people from all sorts of locations and backgrounds to connect
- Don 't stop
  - conditions are ripe for new invention - "Linked Data"

The Web Today

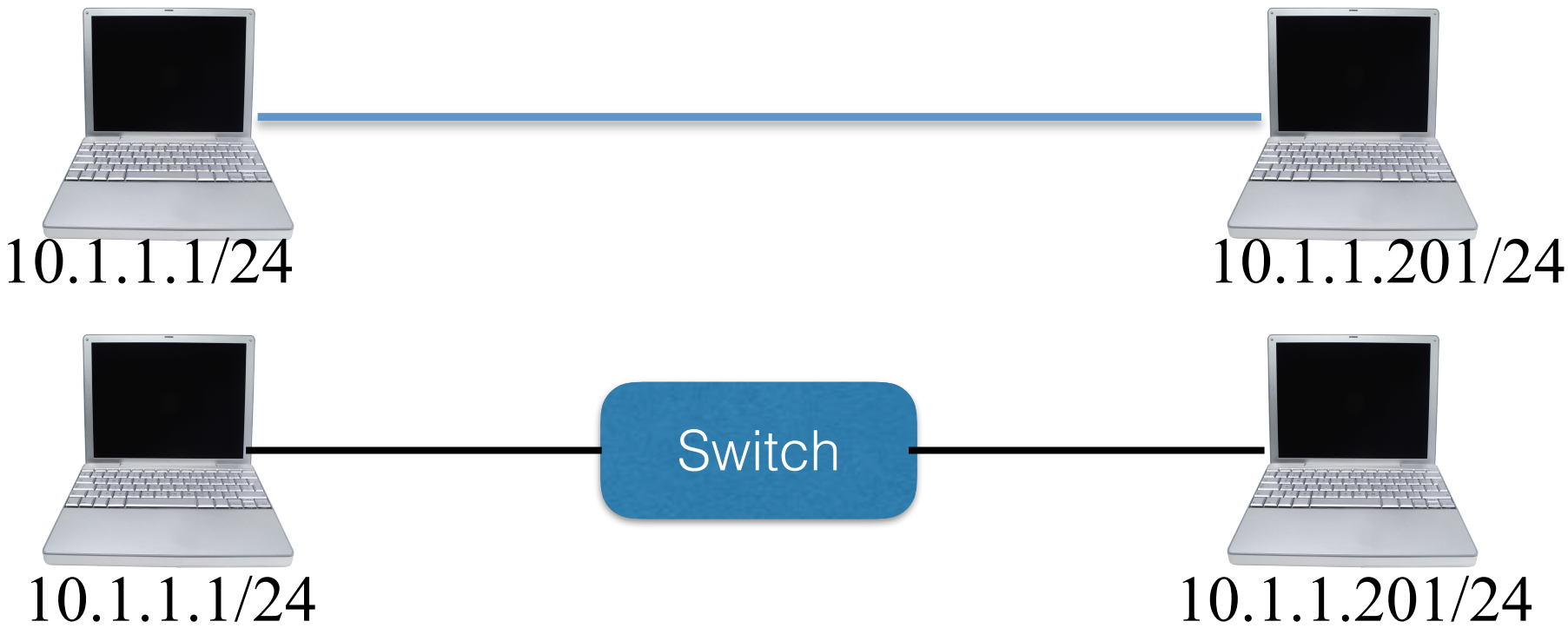
- Total num of hostnames and active sites (Feb 2017)
  - src: **http://news.netcraft.com/archives/category/web-server-survey/**
  - Number of sitenames and active sites
    - Sitenames: 1.7B, Active sites: 170+M
  - Web server vendors
    - Apache: 21% , Microsoft IIS : 43%, Nginx: 19%
  - Web Clients: GUI browsers, text browsers

- Analysis of www.dsce.in (webpagetest.org)
  - 40 URLs, total time : 17+s

Exploration Topics

- Overview of Internet
- Overview of Setup
- Overview of OSI Layers
- Overview of Tools
- Understanding Wireshark
- Wireshark filters
- Exercise - 1
- Overview of IP
- Exercise - 2
- Misc Content
- Summary

Setup Requirement



Exploration Topics

- Overview of Internet
- Overview of Setup
- Overview of OSI Layers
- Overview of Tools
- Understanding Wireshark
- Wireshark filters
- Exercise - 1
- Overview of IP
- Exercise - 2
- Misc Content
- Summary

Layers

Networks are complex, with many "pieces":

- hosts
- routers
- links of various media
- applications
- protocols
- hardware, software

Protocol "layers"

Networks are complex, with many "pieces":

- hosts
- routers
- links of various media
- applications
- protocols
- hardware, software

Question:

is there any hope of *organizing* structure of network?

…. or at least our discussion of networks?

Protocol - Human Analogy

- Example : Classroom interaction
  - Teacher enters the class room
  - Students show respect (by standing up)
- Teacher droning about the protocols and class is confused. Stops to ask?
  - "Are you confused?"
  - Msg is transmitted & received by all (not sleeping)
- Some one raises a hand (msg to teacher)
- Teacher allows to ask a question
- Students ask the question,
- …
- What happens when you type a URL in browser

What's a protocol?

human protocols:

- "what's the time?"
- "I have a question"
- introductions

… specific msgs sent

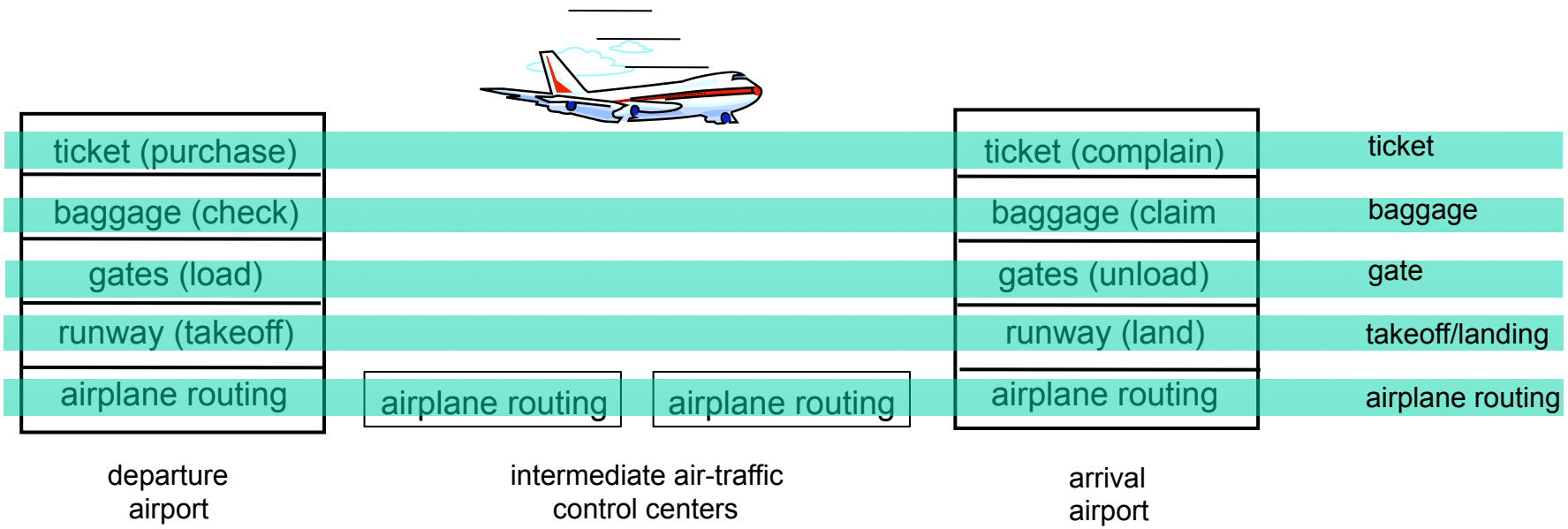
… specific actions taken when msgs received, or other events

Protocol View

- Network Protocols
  - machines rather than humans
  - all communication activity governed by protocols
  - Example: accessing a web server (HTTP protocol)

protocols define format, order of msgs sent and received among network entities, and actions taken on msg transmission, receipt

Layering of airline functionality



layers: each layer implements a service

- via its own internal-layer actions
- relying on services provided by layer below

Layering

- Another Example: Your education at college

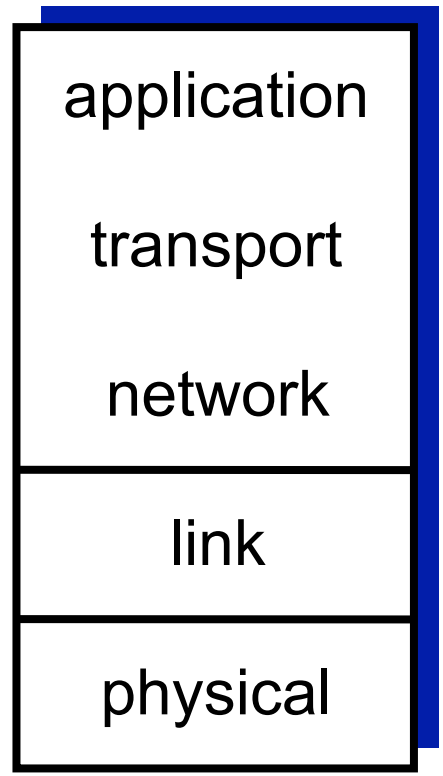
Why layering?

dealing with complex systems:

- explicit structure allows identification, relationship of complex system's pieces
  - layered *reference model* for discussion
- modularization eases maintenance, updating of system
  - change of implementation of layer's service transparent to rest of system
  - e.g., change in gate procedure doesn't affect rest of system
- layering considered harmful?

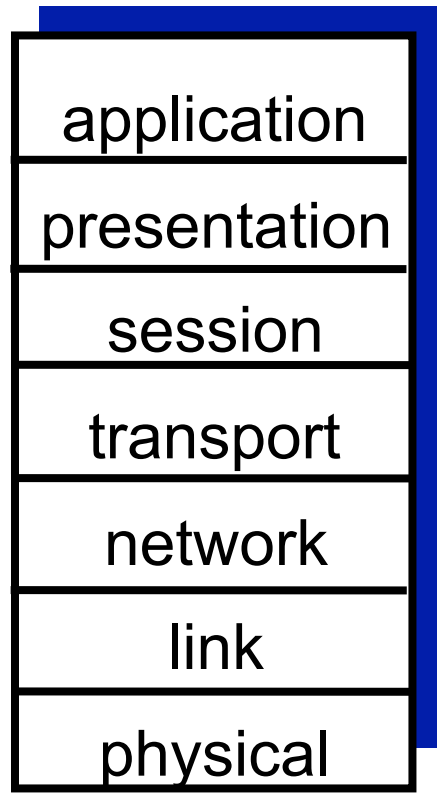
Internet protocol stack

- *application:* supporting network applications
  - FTP, SMTP, HTTP
- *transport:* process-process data transfer
  - TCP, UDP
- *network:* routing of datagrams from source to destination
  - IP, routing protocols
- *link:* data transfer between neighboring network elements
  - Ethernet, 802.111 (WiFi), PPP
- *physical:* bits "on the wire"

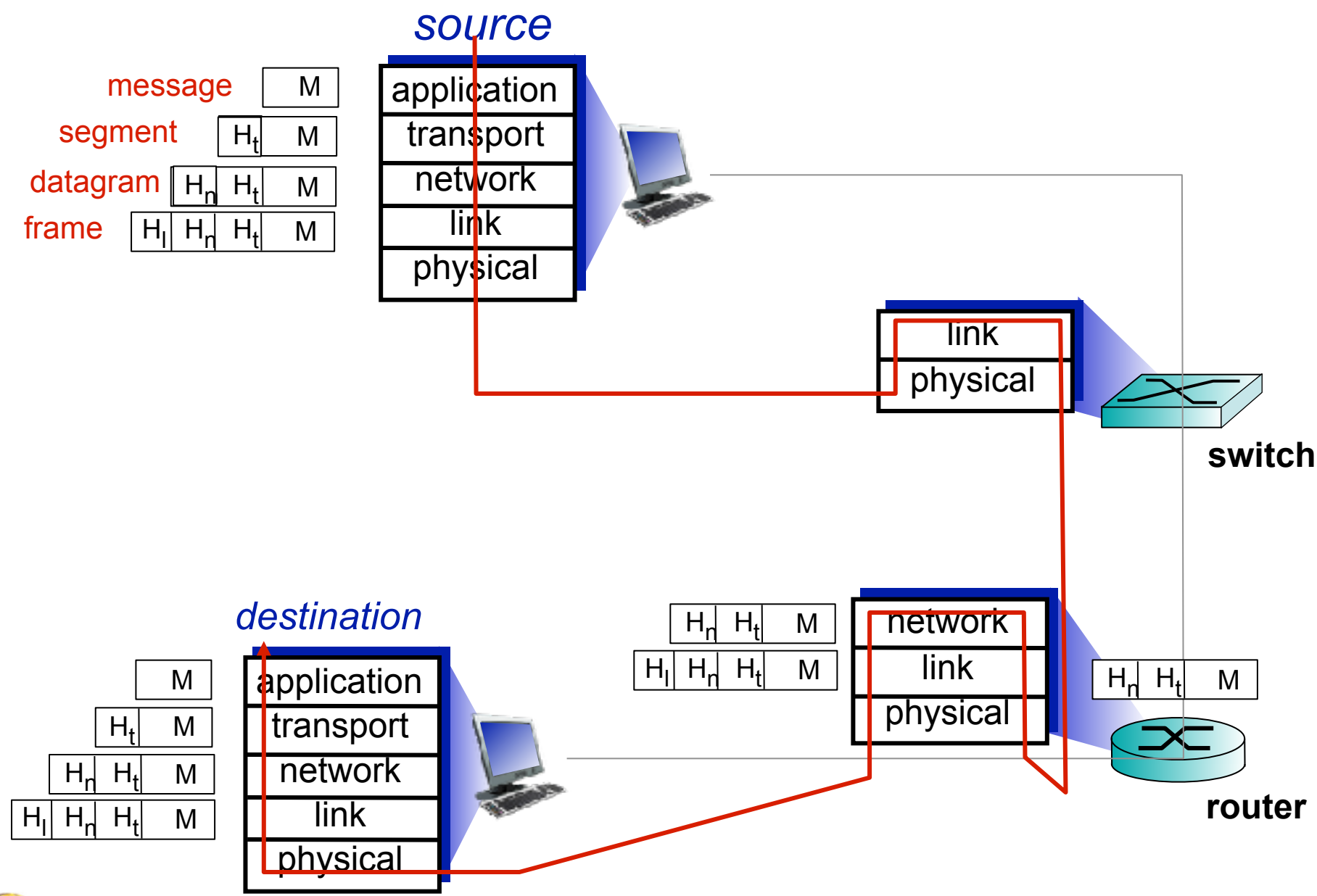


ISO/OSI reference model

- *presentation:* allow applications to interpret meaning of data, e.g., encryption, compression, machine-specific conventions
- *session:* synchronization, checkpointing, recovery of data exchange
- Internet stack "missing" these layers!
  - these services, *if needed,* must be implemented in application
  - needed?



Encapsulation



Payload Nomenclature

- Application layer
  - Message
- Transport layer
  - Segment
- Network layer
  - Datagram, packet
- Link layer
  - Frame
- Physical layer
  - bit

Exploration Topics

- Overview of Internet
- Overview of Setup
- Overview of OSI Layers
- Overview of Tools
- Understanding Wireshark
- Wireshark filters
- Exercise - 1
- Overview of IP
- Exercise - 2
- Misc Content
- Summary

Tools

- nc (netcat)
- telnet, ssh, scp
- ping, traceroute, netstat
- wget, curl, postman
- wireshark, tcpdump
- iproute2 package, iptables
- ttcp, iperf
- Web servers: Apache, nginx
- Simulators: GNS3, Cisco packet tracer, mininet
- VirtualBox, parallels

Tools

- nc (netcat)
  - Works as both transport layer client & server
  - Supports both TCP and UDP
  - Supports both IPv4 and IPv6
  - Common use
    - Simple TCP proxies
    - Shell script based HTTP clients and servers
    - Network daemon testing
    - SOCKS or HTTP ProxyCommand for ssh

Tools

- `nc` usage
  - `-l` acting as server
  - `-u` use UDP
  - `-6` to use IPv6
  - `-i` for interval based transmission (lines)
  - -k for keeping server up
- Examples
  - `nc` servername server port
  - `nc -l` port
  - to transfer files
    - Server: `nc -l` port >file.dat
    - Client: `cat` file.dat `|` `nc` servername port

Tools : `nc` usage

- Terminating connection after some idle time
  - `nc -w 10` server port # timeout after 10s
    - Don't use with server option
- Providing remote shell access on server to a client
  - Create a FIFO file
    - `rm -f /tmp/f; mkfifo /tmp/f`
  - run nc on server by executing the shell
    - `rm -f /tmp/f; mkfifo /tmp/f`
    - `cat /tmp/f | /bin/sh -i 2>&1 | nc -l 1234 > /tmp/f`

Tools: using ICMP

- ping
  - Checking reachability
    - ping hostname
  - -i changing packet interval
  - -c packet count
  - -f flooding the network
  - -a audible indication
  - -q quite mode
  - -s change packet size
  - -w response timeout
  - Ctrl + | (intermediate summary)

Tools: using traceroute

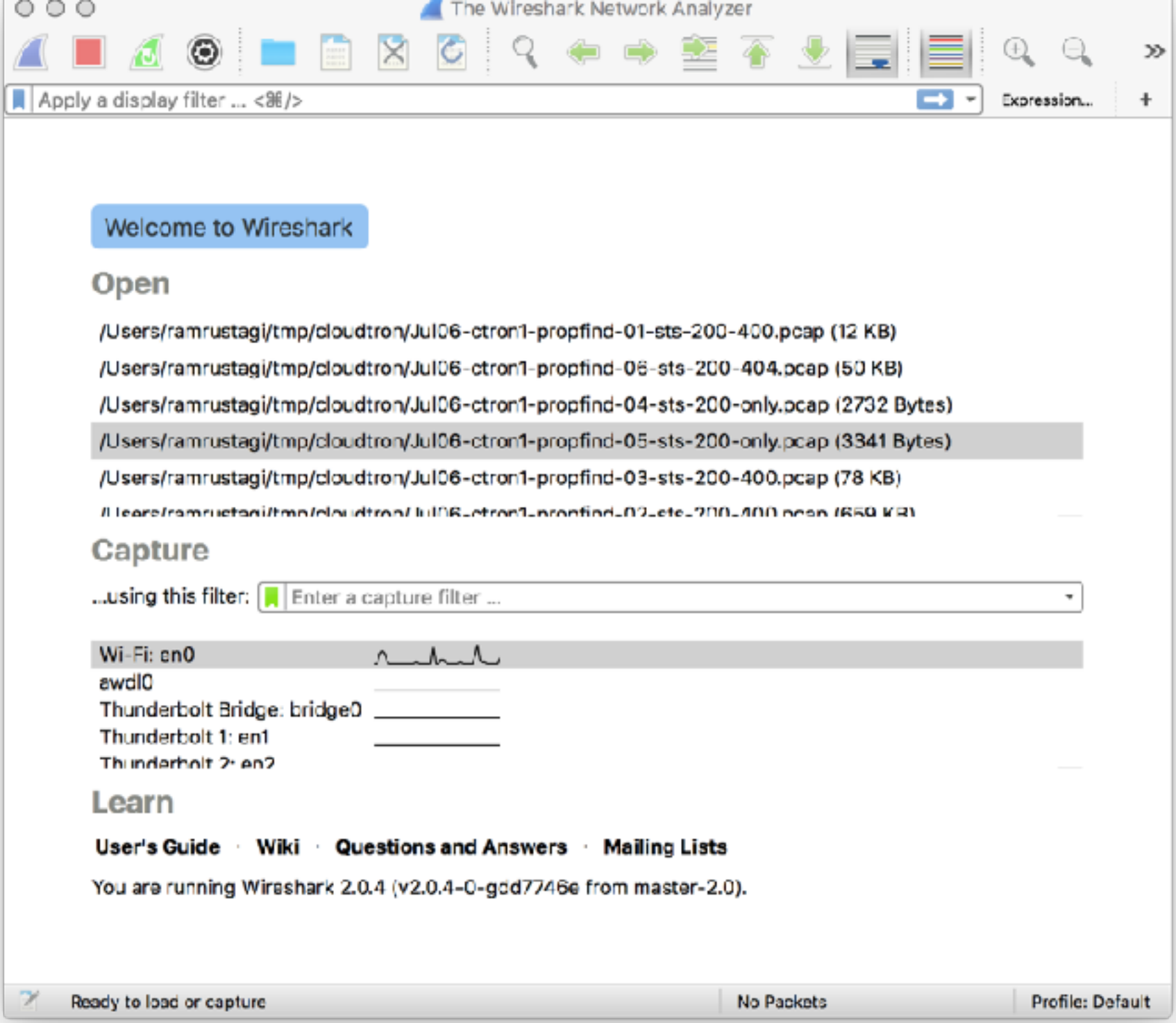
- Purpose
  - Finding intermediate routers
  - -n disabling IP to domain mapping
  - -w response wait time
  - -q Changing queries per hop (default 3)
  - -f initial TTL value

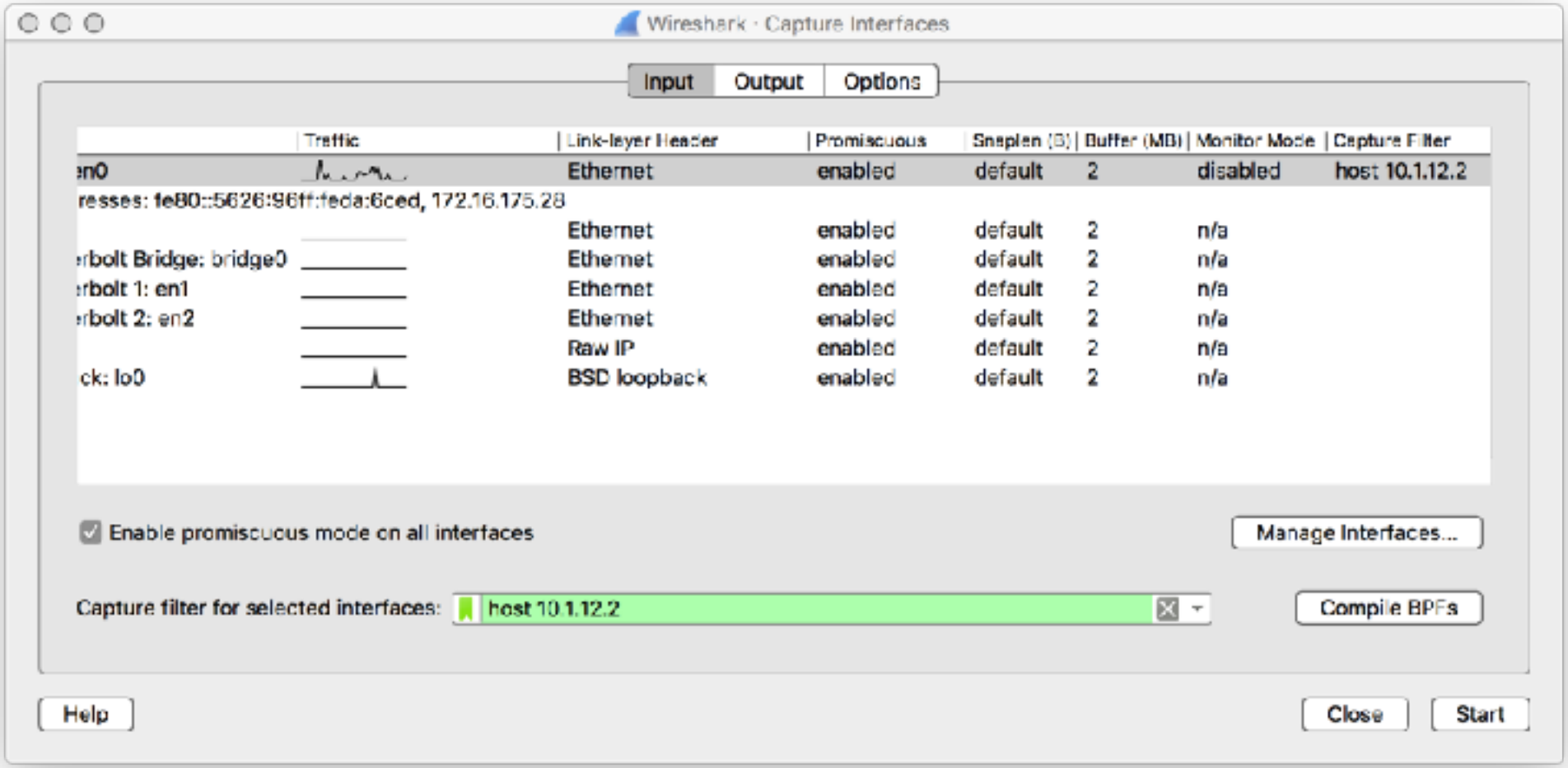
Exploration Topics

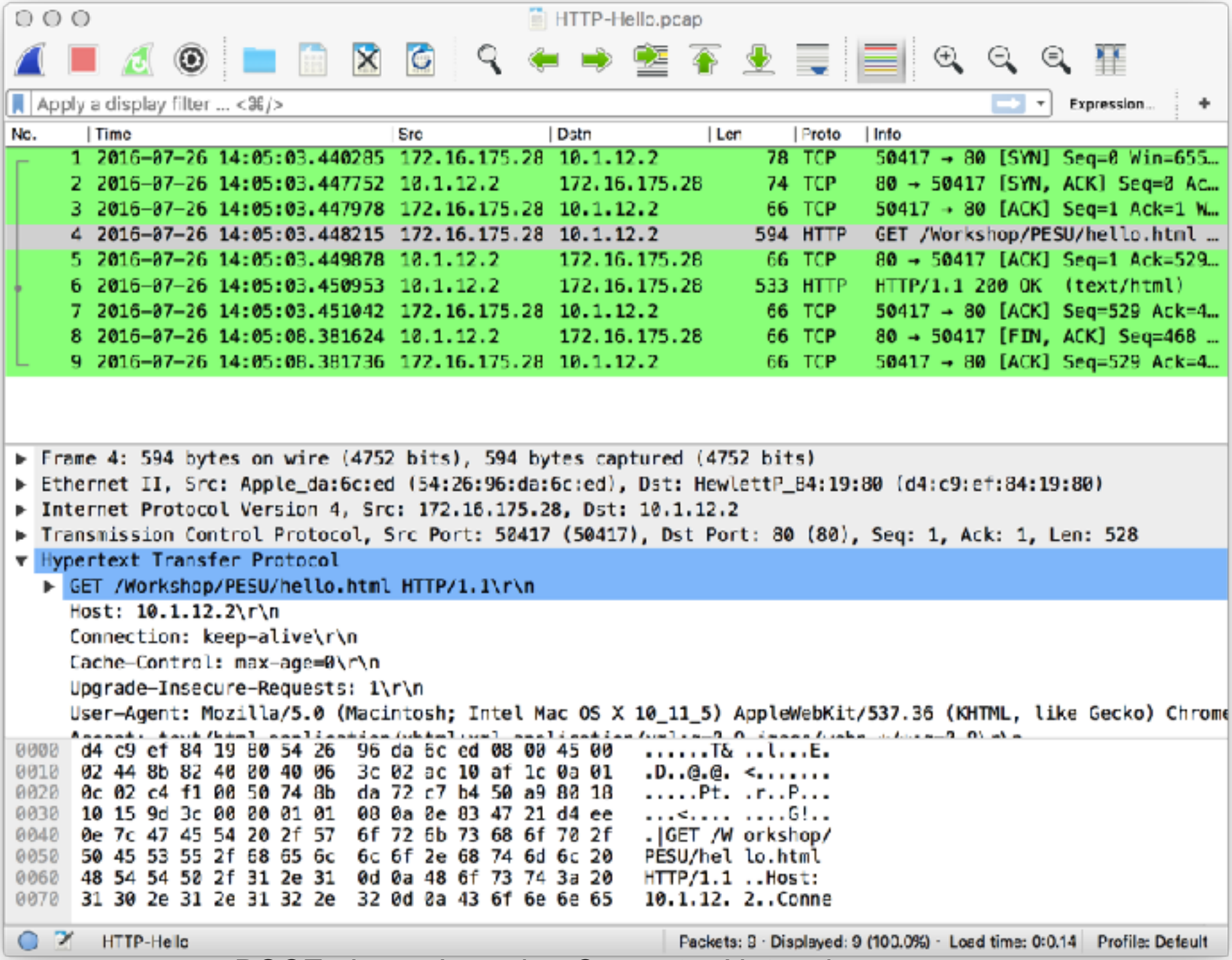
- Overview of Internet
- Overview of Setup
- Overview of OSI Layers
- Overview of Tools
- Understanding Wireshark
- Wireshark filters
- Exercise - 1
- Overview of IP
- Exercise - 2
- Misc Content
- Summary

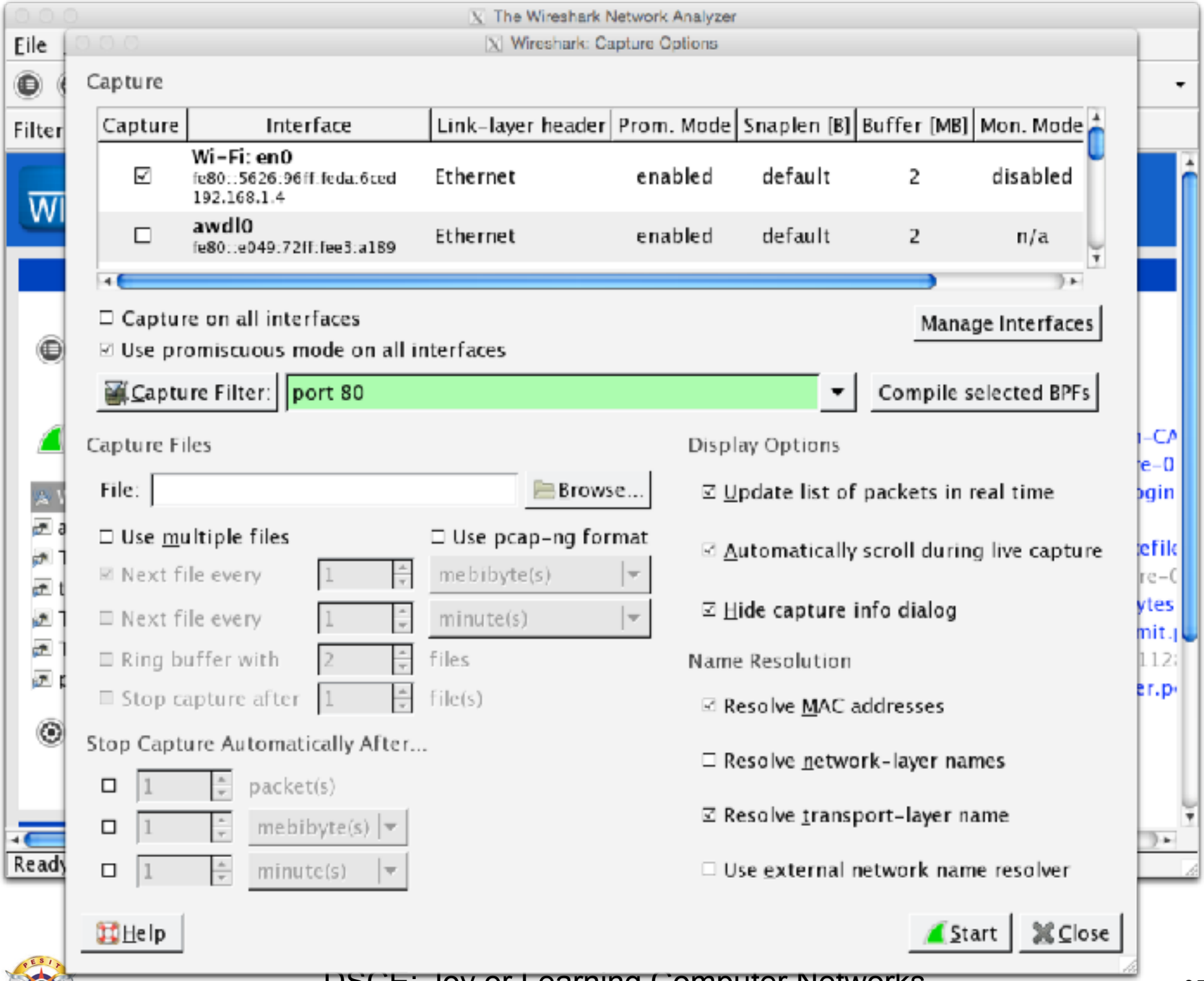
Tools

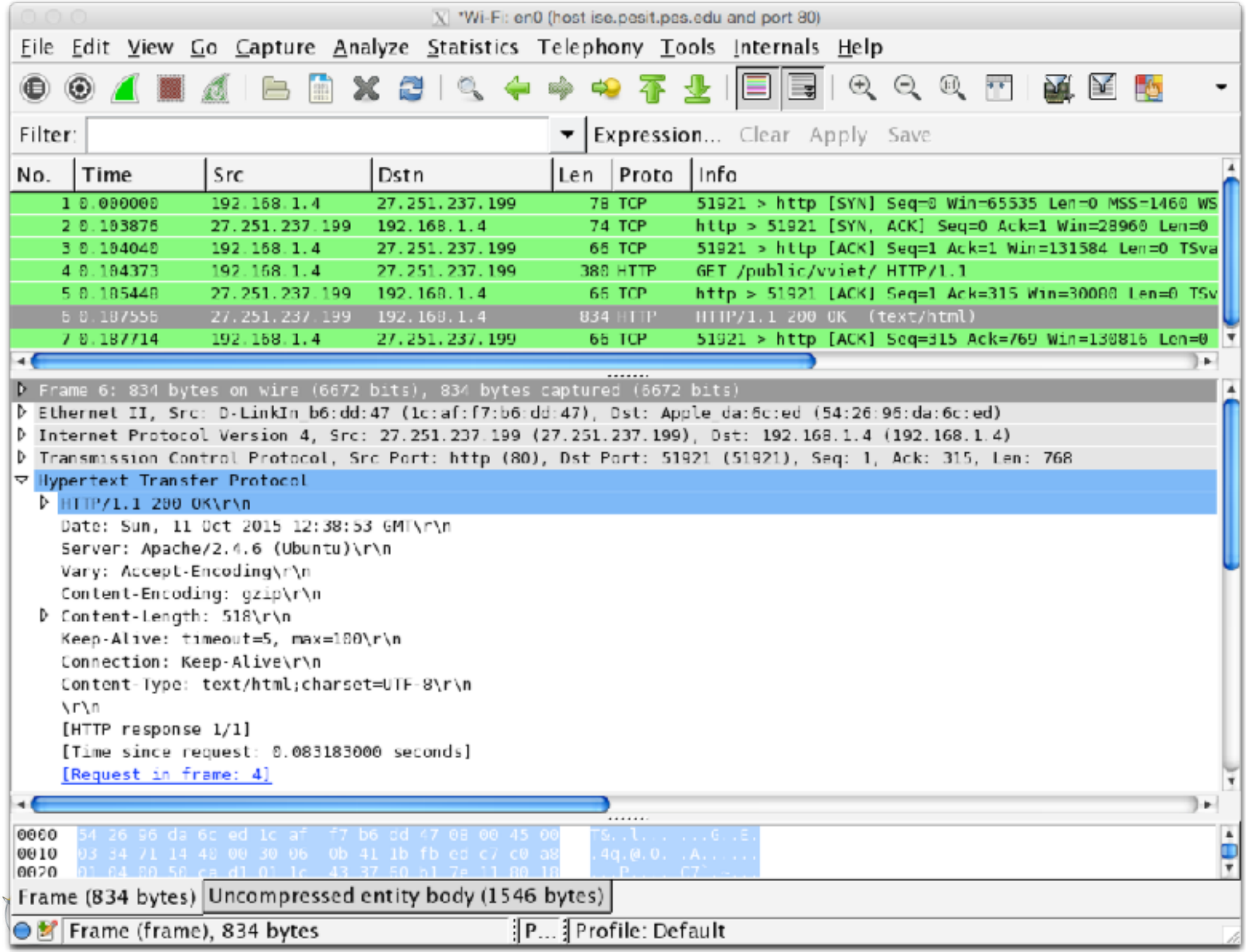
- `wireshark`
  - `https://www.wireshark.org/docs/wsug_html_chunked/`
  - Capture and Display filters
  - Graphical, built on tcpdump
  - TCP session display
  - Changing UI options
- `tcpdump`: command line capture tool
  - output file
  - packet count
  - interface names


The Wireshark Network Analyzer
Apply a display filter ... <⌘/>
Expression...
Welcome to Wireshark
Open
/Users/ramrustagi/tmp/cloudtron/Jul06-ctron1-propfind-01-sts-200-400.pcap (12 KB)
/Users/ramrustagi/tmp/cloudtron/Jul06-ctron1-propfind-06-sts-200-404.pcap (50 KB)
/Users/ramrustagi/tmp/cloudtron/Jul06-ctron1-propfind-04-sts-200-only.pcap (2732 Bytes)
/Users/ramrustagi/tmp/cloudtron/Jul06-ctron1-propfind-05-sts-200-only.pcap (3341 Bytes)
/Users/ramrustagi/tmp/cloudtron/Jul06-ctron1-propfind-03-sts-200-400.pcap (78 KB)
Capture
...using this filter:
Enter a capture filter ...
Wi-Fi: en0
awdl0
Thunderbolt Bridge: bridge0
Thunderbolt 1: en1
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.0.4 (v2.0.4-0-gdd7746e from master-2.0).
Ready to load or capture
No Packets
Profile: Default


Wireshark · Capture Interfaces
Input
Output
Options
Traffic
Link-layer Header
Promiscuous
Snaplen (B)
Buffer (MB)
Monitor Mode
Capture Filter
en0
Ethernet
enabled
default
2
disabled
host 10.1.12.2
resses: fe80::5626:96ff:feda:6ced, 172.16.175.28
Ethernet
enabled
default
2
n/a
rbolt Bridge: bridge0
Ethernet
enabled
default
2
n/a
rbolt 1: en1
Ethernet
enabled
default
2
n/a
rbolt 2: en2
Ethernet
enabled
default
2
n/a
Raw IP
enabled
default
2
n/a
ck: lo0
BSD loopback
enabled
default
2
n/a
Enable promiscuous mode on all interfaces
Manage Interfaces...
Capture filter for selected interfaces:
host 10.1.12.2
Compile BPFs
Help
Close
Start


HTTP-Hello.pcap
Apply a display filter ... <⌘/>
Expression...
No. | Time | Src | Dstn | Len | Proto | Info
1 2016-07-26 14:05:03.440285 172.16.175.28 10.1.12.2 78 TCP 50417 → 80 [SYN] Seq=0 Win=655...
2 2016-07-26 14:05:03.447752 10.1.12.2 172.16.175.28 74 TCP 80 → 50417 [SYN, ACK] Seq=0 Ac...
3 2016-07-26 14:05:03.447978 172.16.175.28 10.1.12.2 66 TCP 50417 → 80 [ACK] Seq=1 Ack=1 W...
4 2016-07-26 14:05:03.448215 172.16.175.28 10.1.12.2 594 HTTP GET /Workshop/PESU/hello.html ...
5 2016-07-26 14:05:03.449878 10.1.12.2 172.16.175.28 66 TCP 80 → 50417 [ACK] Seq=1 Ack=529...
6 2016-07-26 14:05:03.450953 10.1.12.2 172.16.175.28 533 HTTP HTTP/1.1 200 OK (text/html)
7 2016-07-26 14:05:03.451042 172.16.175.28 10.1.12.2 66 TCP 50417 → 80 [ACK] Seq=529 Ack=4...
8 2016-07-26 14:05:08.381624 10.1.12.2 172.16.175.28 66 TCP 80 → 50417 [FIN, ACK] Seq=468 ...
9 2016-07-26 14:05:08.381736 172.16.175.28 10.1.12.2 66 TCP 50417 → 80 [ACK] Seq=529 Ack=4...
Frame 4: 594 bytes on wire (4752 bits), 594 bytes captured (4752 bits)
Ethernet II, Src: Apple_da:6c:ed (54:26:96:da:6c:ed), Dst: HewlettP_84:19:80 (d4:c9:ef:84:19:80)
Internet Protocol Version 4, Src: 172.16.175.28, Dst: 10.1.12.2
Transmission Control Protocol, Src Port: 50417 (50417), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 528
Hypertext Transfer Protocol
GET /Workshop/PESU/hello.html HTTP/1.1\r\n
Host: 10.1.12.2\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
0000 d4 c9 ef 84 19 80 54 26 96 da 6c ed 08 00 45 00 ......T& ..l...E.
0010 02 44 8b 82 40 00 40 06 3c 02 ac 10 af 1c 0a 01 .D..@.@. <.......
0020 0c 02 c4 f1 00 50 74 8b da 72 c7 b4 50 a9 80 18 .....Pt. .r..P...
0030 10 15 9d 3c 00 00 01 01 08 0a 8e 83 47 21 d4 ee ...<.... ....G!..
0040 0e 7c 47 45 54 20 2f 57 6f 72 6b 73 68 6f 70 2f .|GET /W orkshop/
0050 50 45 53 55 2f 68 65 6c 6c 6f 2e 68 74 6d 6c 20 PESU/hel lo.html
0060 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1 ..Host:
0070 31 30 2e 31 2e 31 32 2e 32 0d 0a 43 6f 6e 6e 65 10.1.12. 2..Conne
HTTP-Hello
Packets: 9 · Displayed: 9 (100.0%) · Load time: 0:0.14
Profile: Default


The Wireshark Network Analyzer
Wireshark: Capture Options
Capture
Capture
Interface
Link-layer header
Prom. Mode
Snaplen [B]
Buffer [MB]
Mon. Mode
Wi-Fi: en0
fe80::5626:96ff:feda:6ced
192.168.1.4
Ethernet
enabled
default
2
disabled
awdl0
fe80::e049:72ff:fee3:a189
Ethernet
enabled
default
2
n/a
Capture on all interfaces
Use promiscuous mode on all interfaces
Manage Interfaces
Capture Filter:
port 80
Compile selected BPFs
Capture Files
File:
Browse...
Use multiple files
Use pcap-ng format
Next file every
1
megibyte(s)
Next file every
1
minute(s)
Ring buffer with
2
files
Stop capture after
1
file(s)
Stop Capture Automatically After...
1
packet(s)
1
megibyte(s)
1
minute(s)
Display Options
Update list of packets in real time
Automatically scroll during live capture
Hide capture info dialog
Name Resolution
Resolve MAC addresses
Resolve network-layer names
Resolve transport-layer name
Use external network name resolver
Help
Start
Close


*Wi-Fi: en0 (host ise.posit.pos.edu and port 80)
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Src Dstn Len Proto Info
1 0.000000 192.168.1.4 27.251.237.199 78 TCP 51921 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS
2 0.193876 27.251.237.199 192.168.1.4 74 TCP http > 51921 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0
3 0.194048 192.168.1.4 27.251.237.199 66 TCP 51921 > http [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSva
4 0.194373 192.168.1.4 27.251.237.199 380 HTTP GET /public/vviet/ HTTP/1.1
5 0.385448 27.251.237.199 192.168.1.4 66 TCP http > 51921 [ACK] Seq=1 Ack=315 Win=30080 Len=0 TSv
6 0.387556 27.251.237.199 192.168.1.4 834 HTTP HTTP/1.1 200 OK (text/html)
7 0.387714 192.168.1.4 27.251.237.199 66 TCP 51921 > http [ACK] Seq=315 Ack=769 Win=130816 Len=0
Frame 6: 834 bytes on wire (6672 bits), 834 bytes captured (6672 bits)
Ethernet II, Src: D-LinkIn_b6:dd:47 (1c:af:f7:b6:dd:47), Dst: Apple_da:6c:ed (54:26:96:da:6c:ed)
Internet Protocol Version 4, Src: 27.251.237.199 (27.251.237.199), Dst: 192.168.1.4 (192.168.1.4)
Transmission Control Protocol, Src Port: http (80), Dst Port: 51921 (51921), Seq: 1, Ack: 315, Len: 768
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Sun, 11 Oct 2015 12:38:53 GMT\r\n
Server: Apache/2.4.6 (Ubuntu)\r\n
Vary: Accept-Encoding\r\n
Content-Encoding: gzip\r\n
Content-Length: 518\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html;charset=UTF-8\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.083183000 seconds]
[Request in frame: 4]
0000 54 26 96 da 6c ed 1c af f7 b6 dd 47 08 00 45 00
0010 03 34 71 14 40 00 30 06 0b 41 1b fb ed c7 c0 a8
Frame (834 bytes)
Uncompressed entity body (1546 bytes)
Frame (frame), 834 bytes
P...
Profile: Default

Wireshark: UI options

- Color coding
- Time format
- Packet reordering (in display)
- Defining protocol
- Using display filter
- Following TCP Stream
- Inspecting packets
  – needed for analyzing packet layers

Wireshark Capture Filters

- Traffic between A and either B or C

```
host A and \( B or C\)
```

- Traffic between A any host except B

```
host A and not B
```

- Capture just SYN or FIN pkts

```
tcp[tcpflags] & (tcp-syn|tcp-fin) != 0
```

- Web traffic containing data i.e. avoid TCP acks

```
tcp port 80 and (((ip[2:2] -
((ip[0]&0xf)<<2)) -
((tcp[12]&0xf0)>>2)) != 0)
```

Wireshark Display Filters

- Source IP filter
  - `ip.src == 192.168.1.1`
- Destination IP filter
  - `ip.dst == 192.168.1.1`
  - `ip.dst != 192.168.1.1`
- Protocol filter
  - `http || icmp`
- port number
  - `tcp.port eq 80`
- TCP Seq
  - `tcp.stream eq 1`

Wireshark Others

- Saving file
  – saving selected packets
- Reading from file
- Time display format
- Statistics
- Other options

Tools: tcpdump

- command line interface
  - ASCII content
  - Capture full packet
  - capture filters
  - output file
  - ethernet frame display

Tools

- Apache Web Server (www.apache.org)
  - Configurations (/etc/apache2/apache2.config)
    - /etc/apache2/sites-available/000-default.conf
      - Directives
      - Logging
      - DocumentRoot
      - Loadable Modules
      - Virtual Host
- Firefox browser
  - Options for configurations
    - `about:config`

Tools : wget

- **wget**
  - `wget -d http://<hostname>/uri`
  - `wget -d --header=`**“hdr: value”**
  - `wget -O` **<outfile> <URL>**

Exploration Topics

- Overview of Internet
- Overview of Setup
- Overview of OSI Layers
- Overview of Tools
- Understanding Wireshark
- Exercise - 1
- Overview of IP
- Exercise - 2
- Misc Content
- Summary

Exercise 1 : nc

- Using nc
  - simple TCP communication
  - simple udp communication
  - idle timeout communication (option -w)
  - interval based communication (option -i)
  - file transfer
  - IPv6 communication (option -6)
  - Running server for ever (option -k)
  - Giving remote access to client from server

Exercise `1: ping`

- Quite mode
- packet count
- changing default interval
- Flooding the network
- Audible indication
- Using timeout
- changing packet size
- changing pattern
- Intermediate summary

Exercise 1: traceroute

- Changing number of hops
- changing response time
- changing initial TTL value
- Disabling domain name display

Exercise 1: wireshark/tcpdump

- Wireshark
  - Capture only or www.dsce.in
  - Capture only ping packets
    - run traceroute and capture packets
  - Analyze tcp stream for DSCE
  - Others
- tcpdump
  - capture 10 packets
  - Display in ASCII
  - Save in file

Exercise 1: TCP/IP Layers

- Layer 7: HTTP protocol
  - Specify proper capture filter for following
    - www.dsce.in
    - http://dayanandasagar.edu
    - google.co.in
  - Taks: Identify the following
    - HTTP protocol version
    - Various HTTP headers
    - User-Agent
    - Language
    - Others

Exercise 1: TCP/IP Layers

- Layer 7: DNS protocol
  - Specify proper capture filter (port 53)
  - Resolve domain names using nslookup, dig, host
  - Taks: Identify the following
    - Request in the name
    - Resolved IP address
    - Other information e.g. MX Records

Exercise 1: TCP/IP layers

- Layer 7 Application: ssh, HTTPS
  - Specify proper capture filter (port 22, 443)
  - Access other m/c using ssh
  - Taks: Identify the following
    - ssh protocol
    - key exchange, cipher suite
    - packet lengths

Exercise 1: TCP/IP layers

- Layer 4: UDP
  - Specify proper capture filter
  - Run UDP server
  - Connect with UDP Client
  - Identify
    - src port
    - dst port
    - data
    - checksum
    - length

Exercise 1: TCP/IP layers

- Layer 4: TCP
  - Specify proper capture filter
  - Run TCP server
  - Connect with TCP Client
  - Identify
    - protocol handshake
    - src port, dst port
    - Seq nums, Acks
    - Other protocol headers
    - data

Exercise 1: TCP/IP layers

- Layer 3: IP, ICMP
  - Specify proper capture filter (icmp)
  - ping some server e.g. google.com
    - Invoke multiple instances
  - Identify
    - request and response packets
    - data
    - id and seq number
    - Src and Destination IP
  - Run traceroute

Exercise 1: TCP/IP layers

- Layer 3: IP, ICMP
  - Specify proper capture filter (icmp)
  - `traceroute` some server e.g. google.com
  - Identify
    - request and response packets
    - TTL value
    - Src and Destination IP
- Layer 3: ARP
  - identify ARP Request and response
  - Look at IP headers

Exercise 1: TCP/IP layers

- Layer 2: Ethernet
  - Specify proper capture filter (icmp)
  - Access www.dsce.in
  - Identify
    - Source MAC and destination MAC
    - Ethtype

Exercise : Wireshakr

- Analyze give capture files.
  – captures.zip

Exploration Topics

- Overview of Internet
- Overview of Setup
- Overview of OSI Layers
- Overview of Tools
- Understanding Wireshark
- Exercise - 1
- Overview of IP
- Exercise - 2
- Misc Content
- Summary

IP Overview

- IPv4 addresses are unique and universal
  - exceptions ?
- IPv4 address is 32 bit long
  - total available addresses: **4,294,967,296**
- Uses Dotted Decimal Notation (DDN)
  - example: 119.82.126.182
- Exercise:
  - Find the error in following addresses
    - 119.082.126.182
    - 119.82.126.182.80
    - 119.82.126.282
    - 119.01010010.126.82

IP Addressing

- Address types
  - Unicast
  - Multicast
  - Broadcast
  - Anycast
- Classful addressing:
  - first byte value determines the class
  - Class A, B, C, D, & E
- Large part of address space is wasted

IP subnets

- Identified by subnet masks : a.b.c.d/n
- A router is needed to connect two networks
- Masks for classful addresses
  - Class A: 255.0.0.0 or /8
  - Class B: 255.255.0.0 or /16
  - Class C: 255.255.255.0 or /24
- Classful addressing obsolete now
  - replaced with classless addressing (CIDR)
- RFCs
  - RFC 1518: Architecture for IP addr allocation with CIDR
  - RFC 1466: Guidelines for IP addr space management
  - RFC 917: Internet subnets

Subnets

- Few terms to understand
  - network portion and host portion
  - network number
    - apply subnet mask to IP address (bitwise AND)
  - Broadcast address
    - set all bits to 1 in host portion
  - network mask
    - set all bits to 0 in host portion
  - first available address in the block
    - value of host portion = 1
  - last available address in the block
    - value of host portion = $2^n - 2$

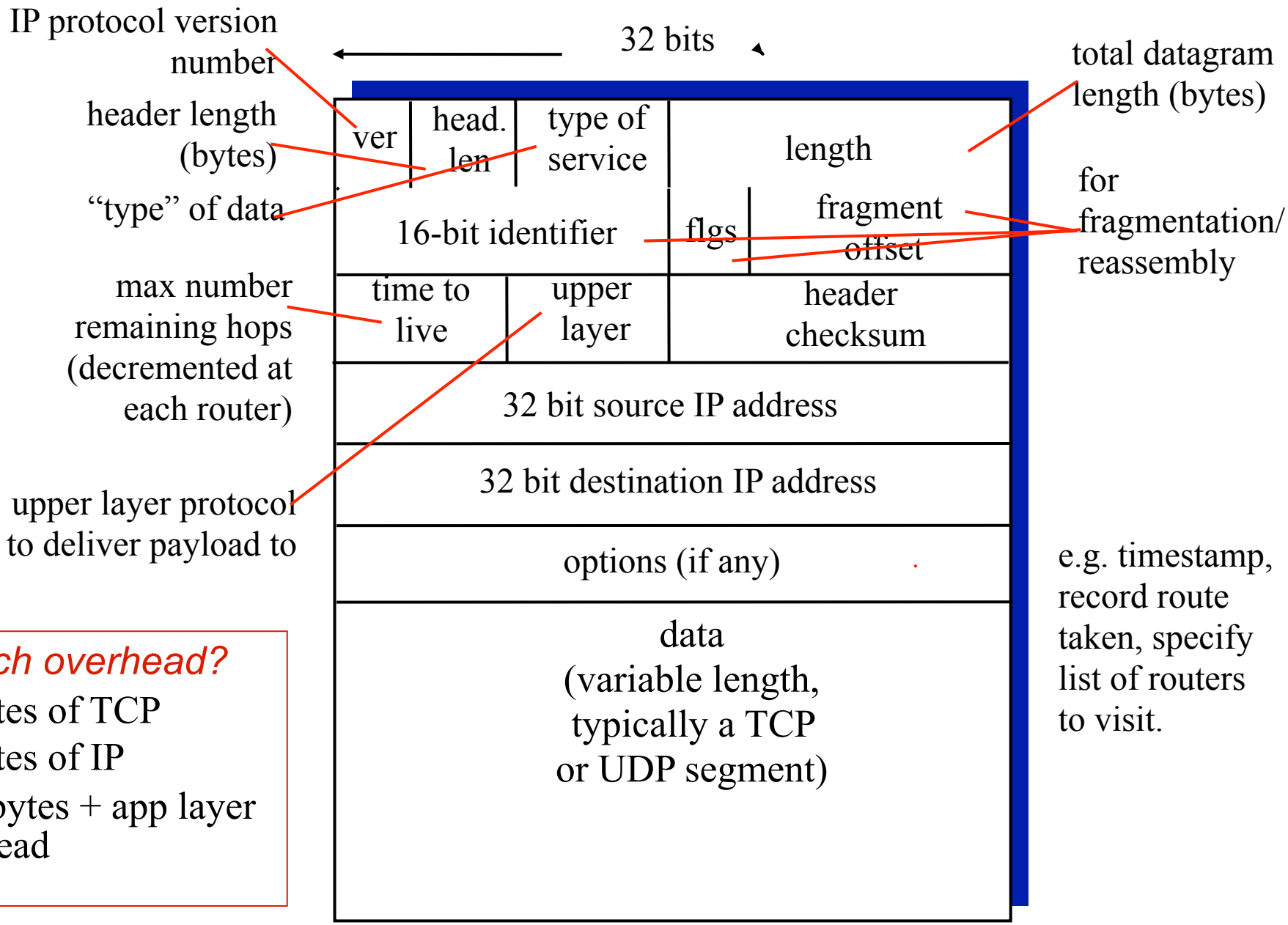
IP Subnets

- Exercise 1
  - a block of addresses is granted to a small organization. one of the address is 119.82.126.182/27. Find out the following:
    - the network number
    - subnet mask
    - broadcast address
    - first & last available address
- Exercise 2:
  - repeat the above exercise for address
    - 192.168.100.200/18

IP Packet Format

- Header + Data
- Header
  - fixed header - 20 bytes
    - src IP, dst IP, TTL, Hlen, Pkt Len
  - options
    - generally not used
    - record route, source route, timestamp
- data

IP Packet Format



how much overhead?

- 20 bytes of TCP
- 20 bytes of IP
- = 40 bytes + app layer overhead

Exploration Topics

- Overview of Internet
- Overview of Setup
- Overview of OSI Layers
- Overview of Tools
- Understanding Wireshark
- Exercise - 1
- Overview of IP
- Exercise - 2
- Misc Content
- Summary

IP Addressing

- Assign IP Address to your machine
- Ping your neighbours
- Change your subnet
- See reachability
- Analyze IP packet header
- Change TTL
- Change default route.
- Access internet
- Assign ARP mapping
- access other hosts

Thank You