Introduction to Wireshark

Shaoquan Jiang

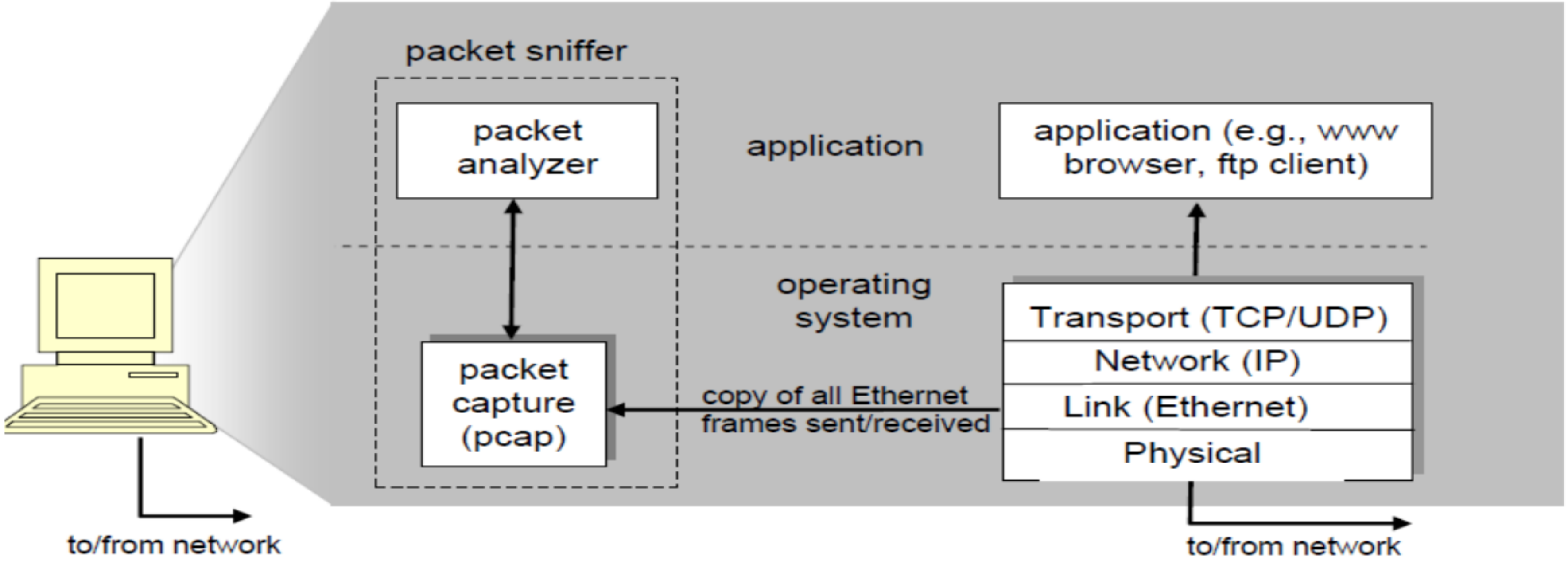
University of Windsor

Introduction

The basic tool for observing the messages exchanged between executing protocol entities is called a **packet sniffer.**

The packet sniffer consists of 2 parts:

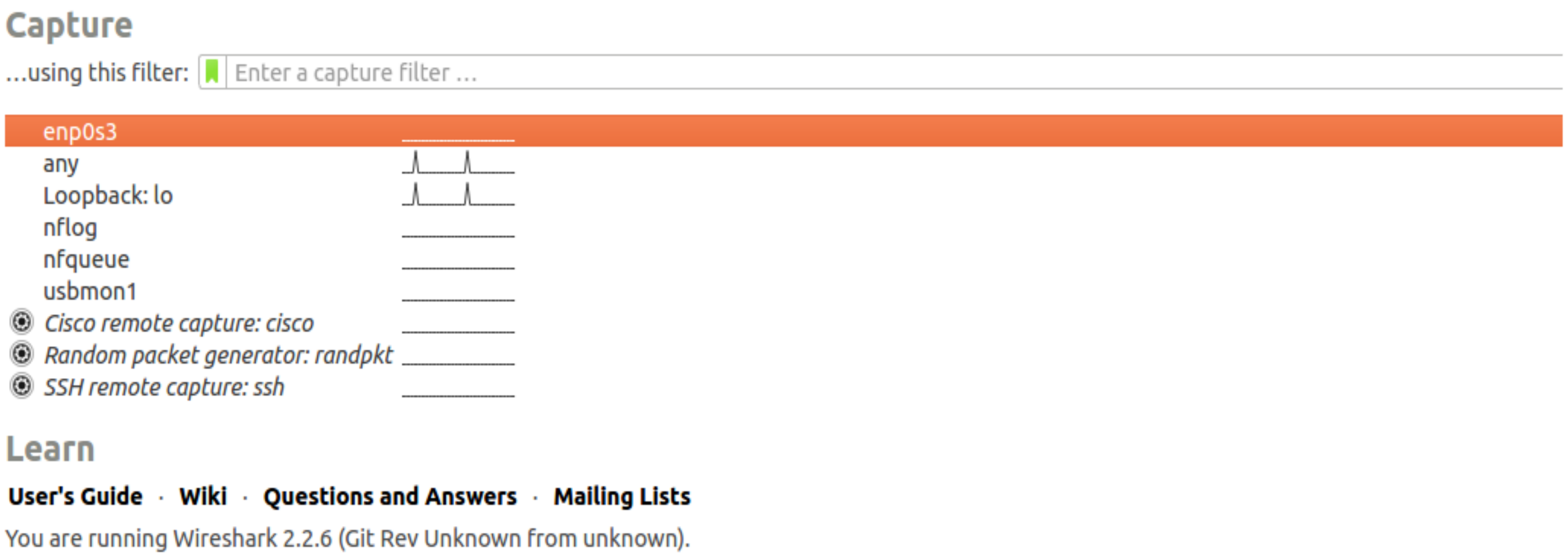
- The **packet capture** library receives a copy of every link layer frame that is sent from or received by your computer.
- The **packet analyzer** which displays the contents of all fields within a protocol message.



Start Wireshark

- After starting Wireshark, you will see the following figure.
- enp0s3 is the network interface of our VM connecting to the outside of VM. Double clicking on this interface will start the sniffer on traffic through this interface.

Double click this interface



Capture

...using this filter: Enter a capture filter ...

enp0s3
any
Loopback: lo
nflog
nfqueue
usbmon1
Cisco remote capture: cisco
Random packet generator: randpkt
SSH remote capture: ssh

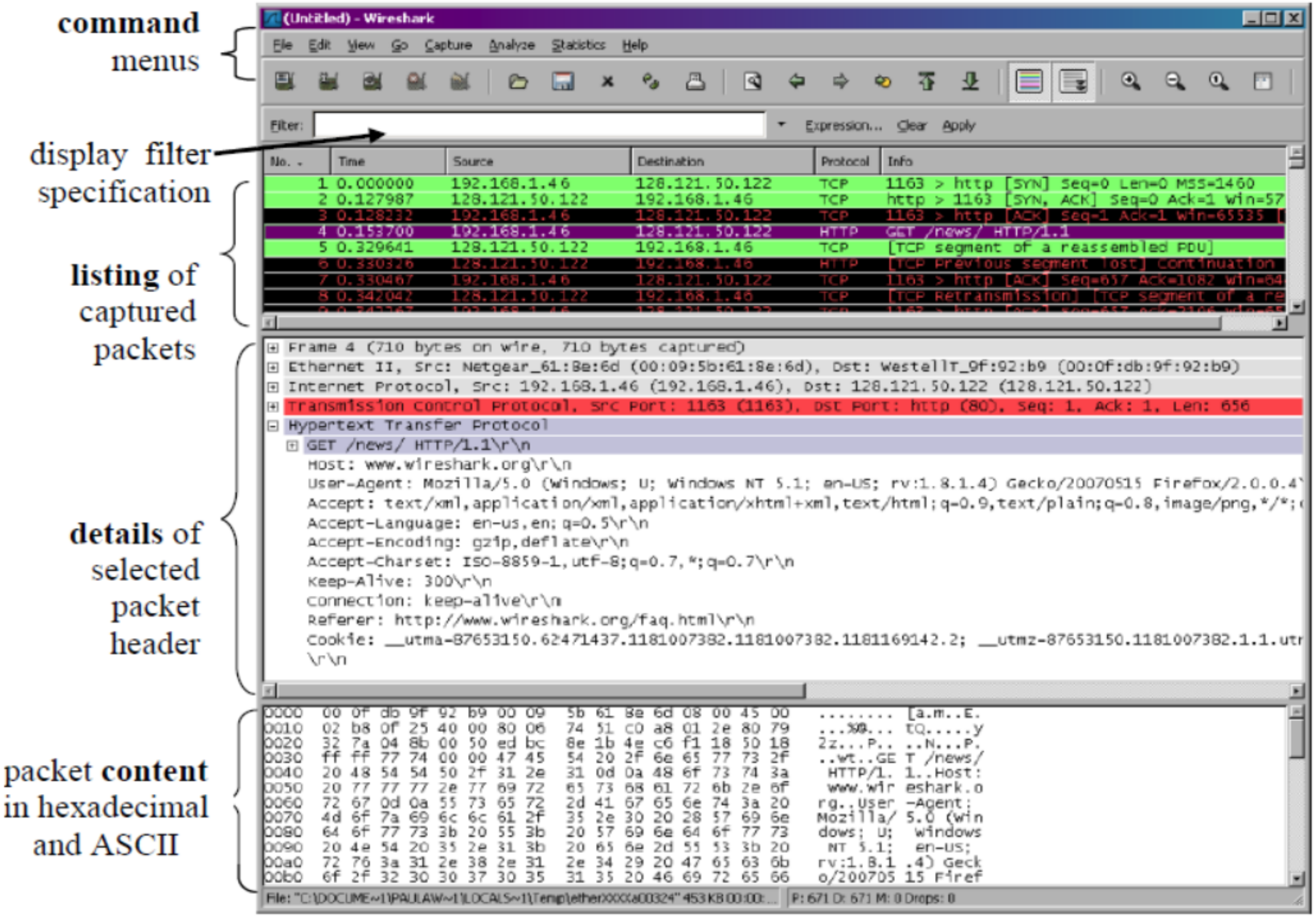
Learn

User's Guide · **Wiki** · **Questions and Answers** · **Mailing Lists**

You are running Wireshark 2.2.6 (Git Rev Unknown from unknown).

Wireshark Window

- Start firefox with a site (e.g., www.uwindsor.ca) and look wireshark window



command menus

display filter specification

listing of captured packets

details of selected packet header

packet content in hexadecimal and ASCII

```
No. .  Time       Source          Destination     Protocol  Info
     1 0.000000   192.168.1.46    128.121.50.122  TCP       1163 > http [SYN] Seq=0 Len=0 MSS=1460
     2 0.127987   128.121.50.122  192.168.1.46    TCP       http > 1163 [SYN, ACK] Seq=0 Ack=1 Win=57
     3 0.128232   192.168.1.46    128.121.50.122  TCP       1163 > http [ACK] Seq=1 Ack=1 Win=65535 [
     4 0.153700   192.168.1.46    128.121.50.122  HTTP      GET /news/ HTTP/1.1
     5 0.329641   128.121.50.122  192.168.1.46    TCP       [TCP segment of a reassembled PDU]
     6 0.330326   128.121.50.122  192.168.1.46    HTTP      [TCP Previous segment lost] Continuation
     7 0.330467   192.168.1.46    128.121.50.122  TCP       1163 > http [ACK] Seq=657 Ack=1082 Win=64
     8 0.342042   128.121.50.122  192.168.1.46    TCP       [TCP Retransmission] [TCP segment of a re
```

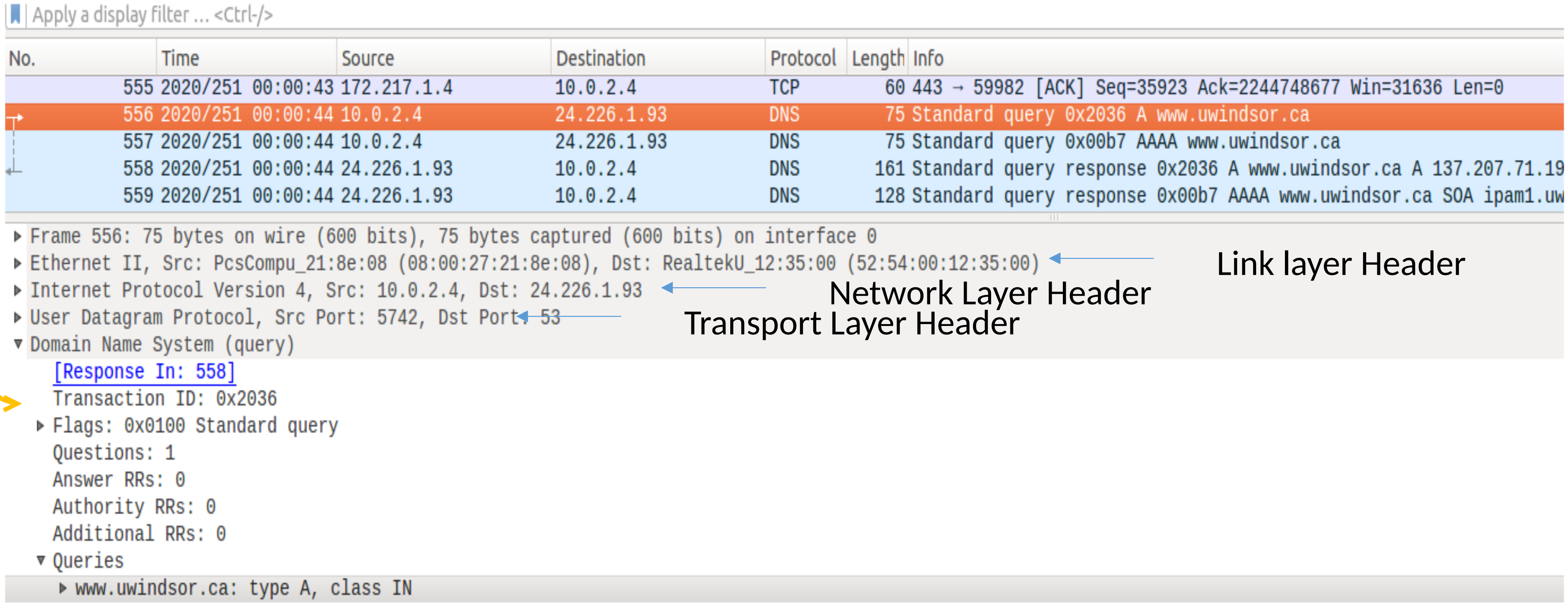
```
⊞ Frame 4 (710 bytes on wire, 710 bytes captured)
⊞ Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: WestellT_9f:92:b9 (00:0f:db:9f:92:b9)
⊞ Internet Protocol, Src: 192.168.1.46 (192.168.1.46), Dst: 128.121.50.122 (128.121.50.122)
⊞ Transmission Control Protocol, Src Port: 1163 (1163), Dst Port: http (80), Seq: 1, Ack: 1, Len: 656
⊟ Hypertext Transfer Protocol
  ⊞ GET /news/ HTTP/1.1\r\n
    Host: www.wireshark.org\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.4) Gecko/20070515 Firefox/2.0.0.4
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Referer: http://www.wireshark.org/faq.html\r\n
    Cookie: __utma-87653150.624714437.1181007382.1181007382.1181169142.2; __utmz-87653150.1181007382.1.1.utr
    \r\n
```

```
0000  00 0f db 9f 92 b9 00 09  5b 61 8e 6d 08 00 45 00   ........ [a.m..E.
0010  02 b8 0f 25 40 00 80 06  74 51 c0 a8 01 2e 80 79   ...%@... tQ.....y
0020  32 7a 04 8b 00 50 ed bc  8e 1b 4e c6 f1 18 50 18   2z...P.. ..N...P.
0030  ff ff 77 74 00 00 47 45  54 20 2f 6e 65 77 73 2f   ..wt..GE T /news/
0040  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1..Host:
0050  20 77 77 77 2e 77 69 72  65 73 68 61 72 6b 2e 6f    www.wir eshark.o
0060  72 67 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   rg..User -Agent: 
0070  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 57 69 6e   Mozilla/ 5.0 (Win
0080  64 6f 77 73 3b 20 55 3b  20 57 69 6e 64 6f 77 73   dows; U;  Windows
0090  20 4e 54 20 35 2e 31 3b  20 65 6e 2d 55 53 3b 20    NT 5.1;  en-US; 
00a0  72 76 3a 31 2e 38 2e 31  2e 34 29 20 47 65 63 6b   rv:1.8.1 .4) Geck
00b0  6f 2f 32 30 30 37 30 35  31 35 20 46 69 72 65 66   o/200705 15 Firef
```

```
File: "C:\DOCUME~1\PAULAW~1\LOCALS~1\Temp\etherXXXXa00324" 453 KB 00:00:...   P: 671 D: 671 M: 0 Drops: 0
```

Specific packet

- Detailed packet example: DNS query packet.
- The structured as <u>LinkLayerHeader</u>||<u>NetworkLayer Header</u>||<u>TransportLayer Header</u>||<u>DNS query</u>



Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
555	2020/251 00:00:43	172.217.1.4	10.0.2.4	TCP	60	443 → 59982 [ACK] Seq=35923 Ack=2244748677 Win=31636 Len=0
556	2020/251 00:00:44	10.0.2.4	24.226.1.93	DNS	75	Standard query 0x2036 A www.uwindsor.ca
557	2020/251 00:00:44	10.0.2.4	24.226.1.93	DNS	75	Standard query 0x00b7 AAAA www.uwindsor.ca
558	2020/251 00:00:44	24.226.1.93	10.0.2.4	DNS	161	Standard query response 0x2036 A www.uwindsor.ca A 137.207.71.19
559	2020/251 00:00:44	24.226.1.93	10.0.2.4	DNS	128	Standard query response 0x00b7 AAAA www.uwindsor.ca SOA ipam1.uw

```
▸ Frame 556: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_21:8e:08 (08:00:27:21:8e:08), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
▸ Internet Protocol Version 4, Src: 10.0.2.4, Dst: 24.226.1.93
▸ User Datagram Protocol, Src Port: 5742, Dst Port: 53
▾ Domain Name System (query)
    [Response In: 558]
    Transaction ID: 0x2036
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ www.uwindsor.ca: type A, class IN
```

packet details

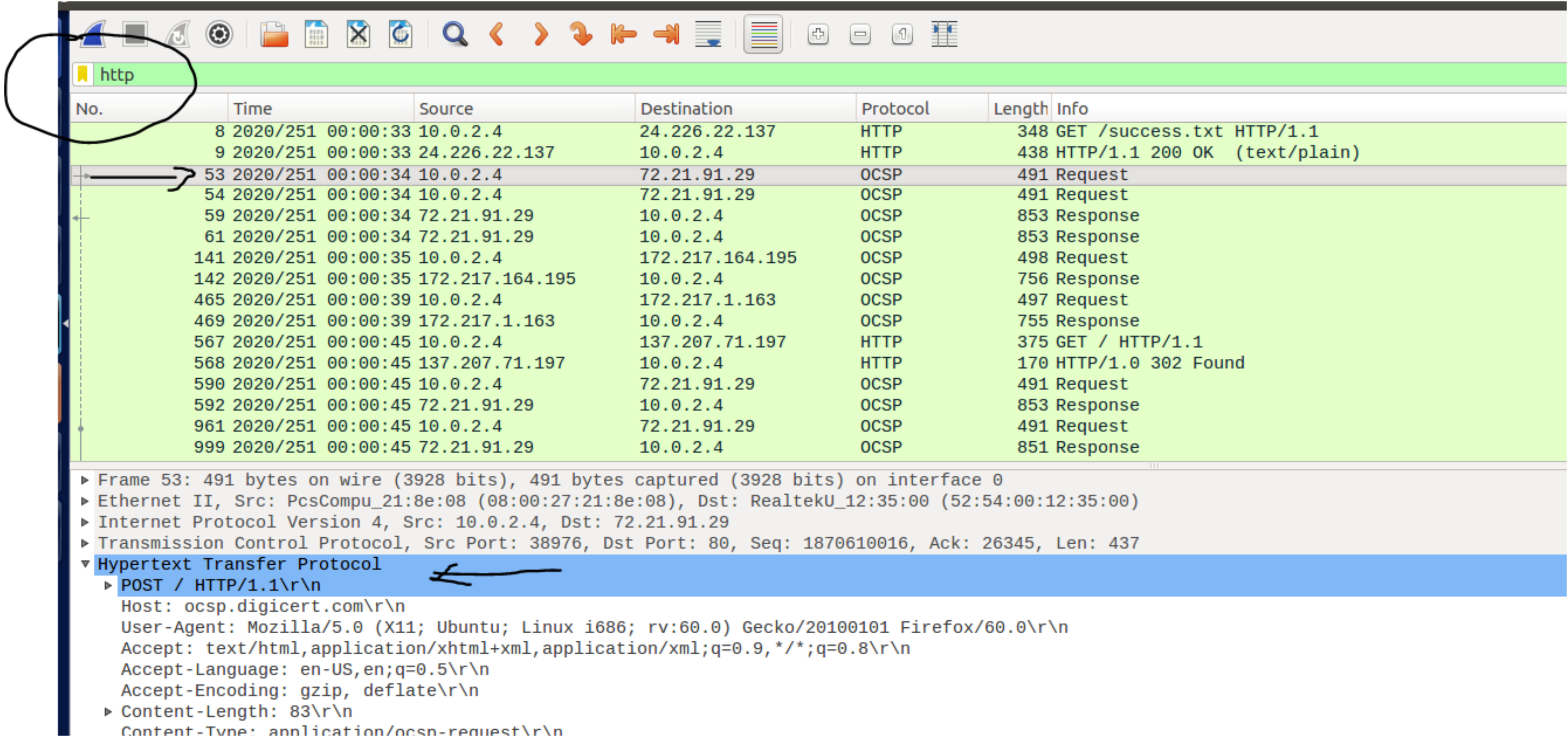
Link layer Header

Network Layer Header

Transport Layer Header

Packet Filter

- We can apply a display filter to show restricted packets.
- Example: using **http** filter will only show the packets containing http protocol



```
http
```

```
No.    Time                Source            Destination       Protocol  Length Info
     8 2020/251 00:00:33 10.0.2.4          24.226.22.137     HTTP         348 GET /success.txt HTTP/1.1
     9 2020/251 00:00:33 24.226.22.137     10.0.2.4          HTTP         438 HTTP/1.1 200 OK  (text/plain)
    53 2020/251 00:00:34 10.0.2.4          72.21.91.29       OCSP         491 Request
    54 2020/251 00:00:34 10.0.2.4          72.21.91.29       OCSP         491 Request
    59 2020/251 00:00:34 72.21.91.29       10.0.2.4          OCSP         853 Response
    61 2020/251 00:00:34 72.21.91.29       10.0.2.4          OCSP         853 Response
   141 2020/251 00:00:35 10.0.2.4          172.217.164.195   OCSP         498 Request
   142 2020/251 00:00:35 172.217.164.195   10.0.2.4          OCSP         756 Response
   465 2020/251 00:00:39 10.0.2.4          172.217.1.163     OCSP         497 Request
   469 2020/251 00:00:39 172.217.1.163     10.0.2.4          OCSP         755 Response
   567 2020/251 00:00:45 10.0.2.4          137.207.71.197    HTTP         375 GET / HTTP/1.1
   568 2020/251 00:00:45 137.207.71.197    10.0.2.4          HTTP         170 HTTP/1.0 302 Found
   590 2020/251 00:00:45 10.0.2.4          72.21.91.29       OCSP         491 Request
   592 2020/251 00:00:45 72.21.91.29       10.0.2.4          OCSP         853 Response
   961 2020/251 00:00:45 10.0.2.4          72.21.91.29       OCSP         491 Request
   999 2020/251 00:00:45 72.21.91.29       10.0.2.4          OCSP         851 Response
```

```
▶ Frame 53: 491 bytes on wire (3928 bits), 491 bytes captured (3928 bits) on interface 0
▶ Ethernet II, Src: PcsCompu_21:8e:08 (08:00:27:21:8e:08), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
▶ Internet Protocol Version 4, Src: 10.0.2.4, Dst: 72.21.91.29
▶ Transmission Control Protocol, Src Port: 38976, Dst Port: 80, Seq: 1870610016, Ack: 26345, Len: 437
▼ Hypertext Transfer Protocol
  ▶ POST / HTTP/1.1\r\n
    Host: ocsp.digicert.com\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
  ▶ Content-Length: 83\r\n
    Content-Type: application/ocsp-request\r\n
```