TA: Xifan Zheng

Email: zhengxifan0403@gmail.com

Welcome to CPSC 441!

Today's Tutorial

- Introduction to wireshark
- Capture filter
- Display filter
- How to use wireshark for debugging

WIRESHARK

- **Wireshark** (Originally named Ethereal)is a free and open-source packet analyzer

- It is used for network troubleshooting, analysis, software and communication protocol development, and education.

- It has a graphical front-end, and many more information sorting and filtering options.

FEATURES AND FUNCTIONALITIES OF WIRESHARK

- Wireshark is software that "understands" the structure of different networking protocols. Thus, it is able to display the encapsulation and the fields along with their meanings of different packets specified by different networking protocols.

- Live data can be read from a number of types of network, including Ethernet, IEEE 802.11, PPP…

- Data display can be refined using a display filter.

INSTALLING WIRESHARK

- Download Wireshark from
  http://www.wireshark.org/download.html
- Choose appropriate version according to your operating system
- (For Windows), during installation agree to install **winpcap** as well.
- **pcap** (packet capture) consists of an application programming interface (API) for capturing network traffic. Unix-like systems implement pcap in the libpcap library. Windows uses a port of libpcap known as **WinPcap**.
- *http://wiki.wireshark.org/CaptureSetup* Provides a good tutorial on how to capture data using WireShark

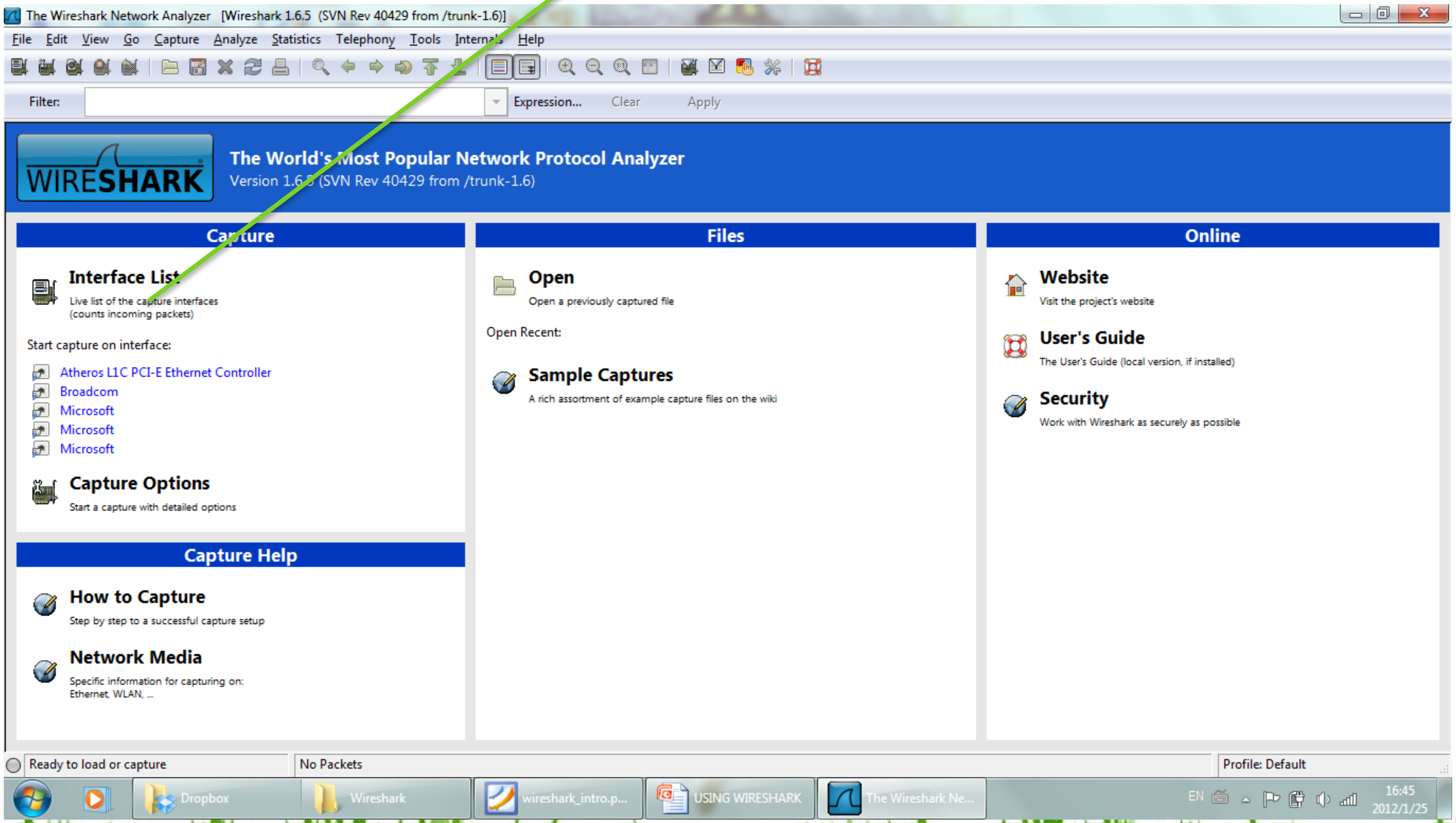
Before CAPTURING DATA

- **Are you allowed to do this?**
- Ensure that you have the permission to capture packets from the network you are connected with. (Corporate policies or applicable law might prohibit capturing data from the network)

- **General Setup**
- Operating system must support packet capturing, e.g. capture support is enabled
- You must have sufficient privileges to capture packets, e.g. root / Administrator privileges
- Your computer's time and time zone settings should be correct

CAPTURING DATA

- Check the interfaces are correctly listed



The Wireshark Network Analyzer [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

The World's Most Popular Network Protocol Analyzer
Version 1.6.5 (SVN Rev 40429 from /trunk-1.6)

Capture

Interface List
Live list of the capture interfaces (counts incoming packets)

Start capture on interface:
- Atheros L1C PCI-E Ethernet Controller
- Broadcom
- Microsoft
- Microsoft
- Microsoft

Capture Options
Start a capture with detailed options

Capture Help

How to Capture
Step by step to a successful capture setup

Network Media
Specific information for capturing on: Ethernet, WLAN, ...

Files

Open
Open a previously captured file

Open Recent:

Sample Captures
A rich assortment of example capture files on the wiki

Online

Website
Visit the project's website

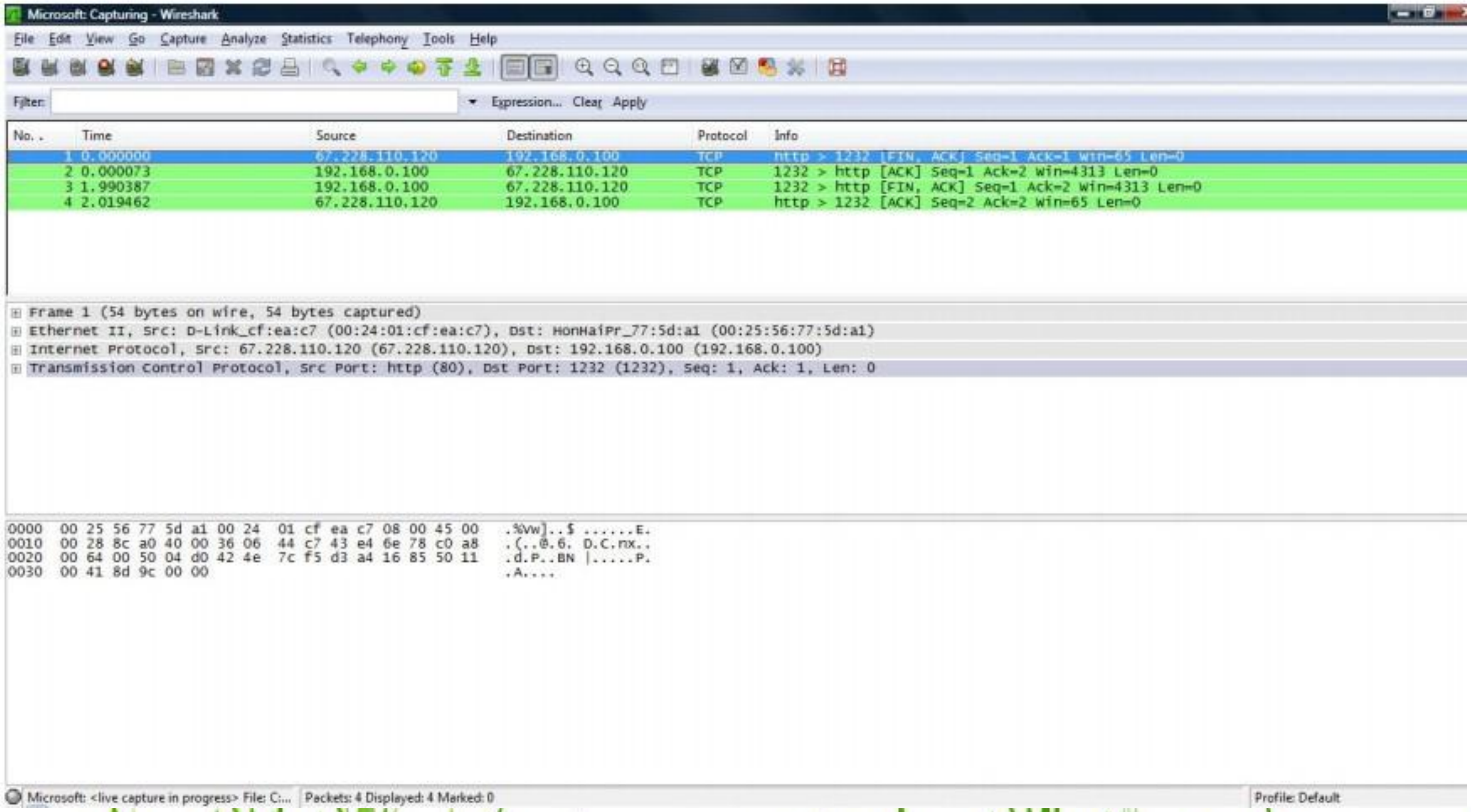
User's Guide
The User's Guide (local version, if installed)

Security
Work with Wireshark as securely as possible

Ready to load or capture | No Packets | Profile: Default

CAPTURING DATA

- **Click on the specific interface you want to capture traffic from.**


Microsoft: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply

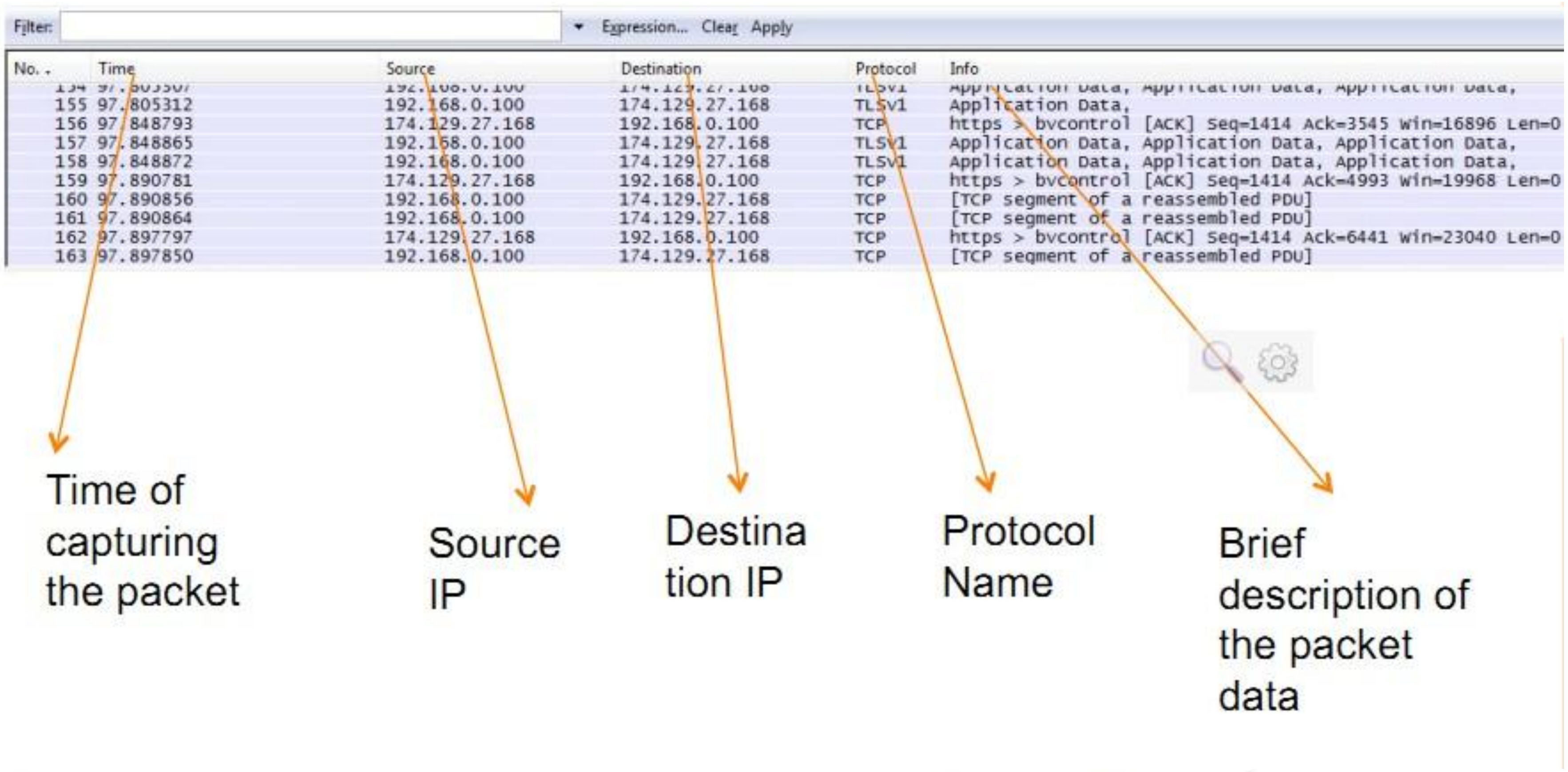
```
No. .  Time        Source            Destination       Protocol  Info
    1  0.000000    67.228.110.120    192.168.0.100     TCP       http > 1232 [FIN, ACK] Seq=1 Ack=1 Win=65 Len=0
    2  0.000073    192.168.0.100     67.228.110.120    TCP       1232 > http [ACK] Seq=1 Ack=2 Win=4313 Len=0
    3  1.990387    192.168.0.100     67.228.110.120    TCP       1232 > http [FIN, ACK] Seq=1 Ack=2 Win=4313 Len=0
    4  2.019462    67.228.110.120    192.168.0.100     TCP       http > 1232 [ACK] Seq=2 Ack=2 Win=65 Len=0
```

```
⊞ Frame 1 (54 bytes on wire, 54 bytes captured)
⊞ Ethernet II, Src: D-Link_cf:ea:c7 (00:24:01:cf:ea:c7), Dst: HonHaiPr_77:5d:a1 (00:25:56:77:5d:a1)
⊞ Internet Protocol, Src: 67.228.110.120 (67.228.110.120), Dst: 192.168.0.100 (192.168.0.100)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 1232 (1232), Seq: 1, Ack: 1, Len: 0
```

```
0000  00 25 56 77 5d a1 00 24  01 cf ea c7 08 00 45 00   .%Vw]..$ ......E.
0010  00 28 8c a0 40 00 36 06  44 c7 43 e4 6e 78 c0 a8   .(..@.6. D.C.nx..
0020  00 64 00 50 04 d0 42 4e  7c f5 d3 a4 16 85 50 11   .d.P..BN |.....P.
0030  00 41 8d 9c 00 00                                  .A....
```

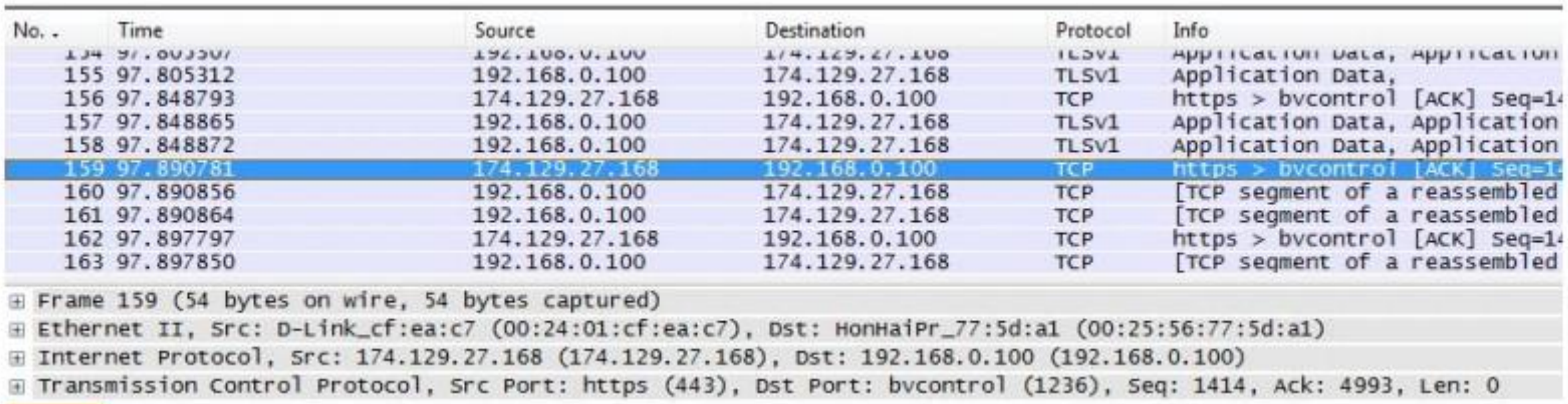
Microsoft: <live capture in progress> File: C:... Packets: 4 Displayed: 4 Marked: 0 Profile: Default

ANALYZING CAPTURED DATA



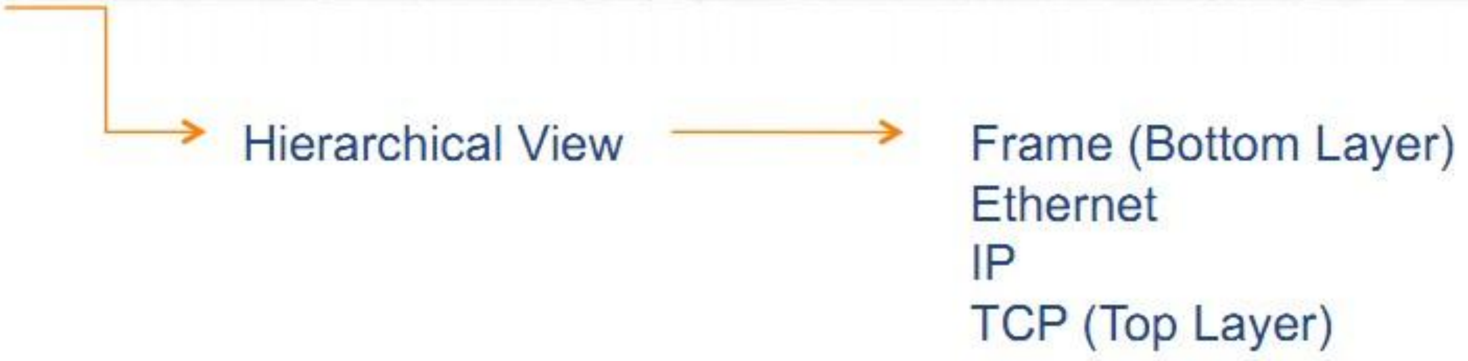
```
No. -  Time        Source          Destination     Protocol  Info
  154 97.805307   192.168.0.100   174.129.27.168  TLSv1     Application Data, Application Data, Application Data,
  155 97.805312   192.168.0.100   174.129.27.168  TLSv1     Application Data,
  156 97.848793   174.129.27.168  192.168.0.100   TCP       https > bvcontrol [ACK] Seq=1414 Ack=3545 Win=16896 Len=0
  157 97.848865   192.168.0.100   174.129.27.168  TLSv1     Application Data, Application Data, Application Data,
  158 97.848872   192.168.0.100   174.129.27.168  TLSv1     Application Data, Application Data, Application Data,
  159 97.890781   174.129.27.168  192.168.0.100   TCP       https > bvcontrol [ACK] Seq=1414 Ack=4993 Win=19968 Len=0
  160 97.890856   192.168.0.100   174.129.27.168  TCP       [TCP segment of a reassembled PDU]
  161 97.890864   192.168.0.100   174.129.27.168  TCP       [TCP segment of a reassembled PDU]
  162 97.897797   174.129.27.168  192.168.0.100   TCP       https > bvcontrol [ACK] Seq=1414 Ack=6441 Win=23040 Len=0
  163 97.897850   192.168.0.100   174.129.27.168  TCP       [TCP segment of a reassembled PDU]
```

ANALYZING CAPTURED DATA



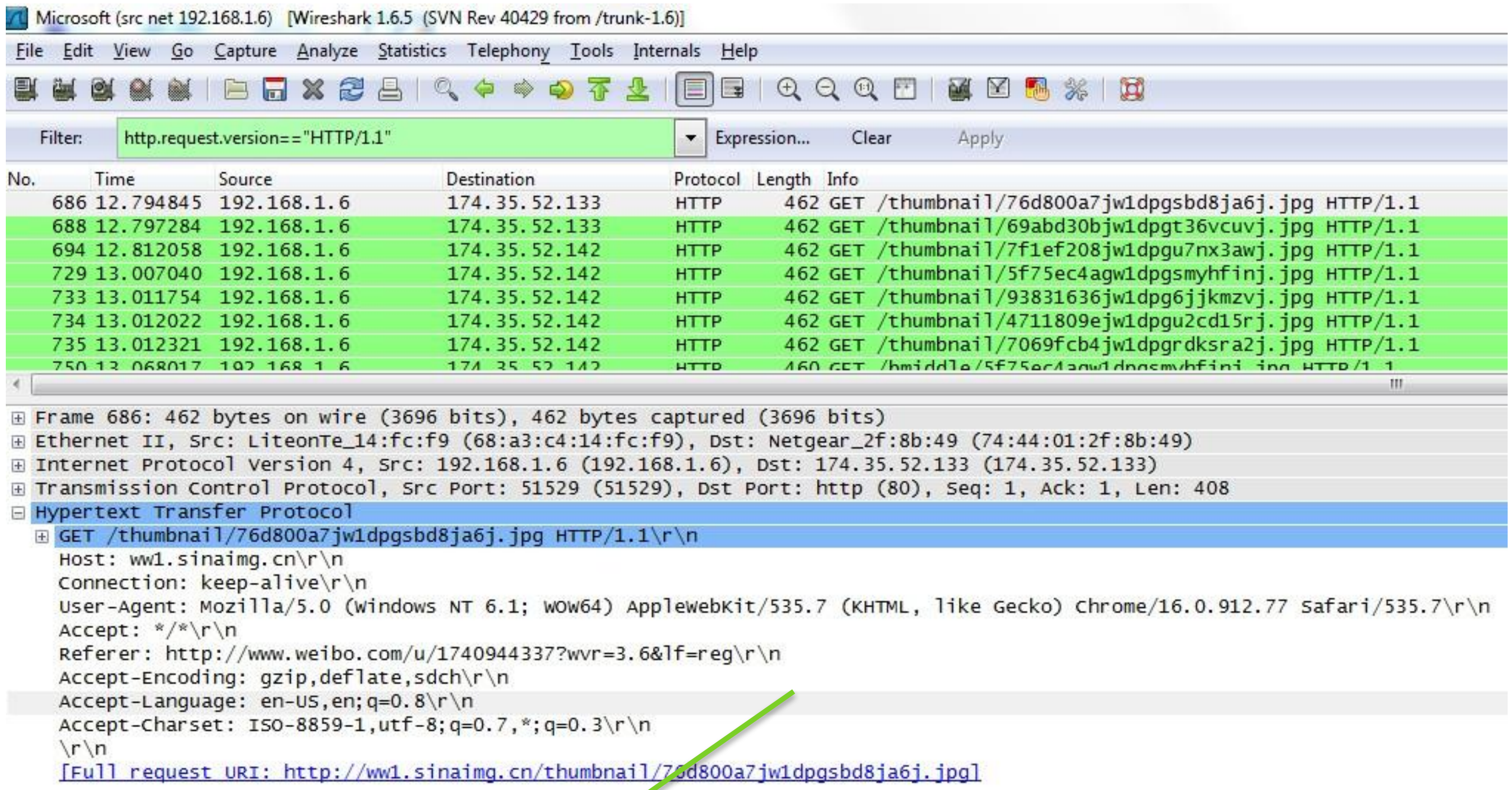
```
No. -  Time          Source          Destination     Protocol  Info
 154 97.805507      192.168.0.100   174.129.27.168  TLSv1     Application Data, Application
 155 97.805312      192.168.0.100   174.129.27.168  TLSv1     Application Data,
 156 97.848793      174.129.27.168  192.168.0.100   TCP       https > bvcontrol [ACK] Seq=1
 157 97.848865      192.168.0.100   174.129.27.168  TLSv1     Application Data, Application
 158 97.848872      192.168.0.100   174.129.27.168  TLSv1     Application Data, Application
 159 97.890781      174.129.27.168  192.168.0.100   TCP       https > bvcontrol [ACK] Seq=1
 160 97.890856      192.168.0.100   174.129.27.168  TCP       [TCP segment of a reassembled
 161 97.890864      192.168.0.100   174.129.27.168  TCP       [TCP segment of a reassembled
 162 97.897797      174.129.27.168  192.168.0.100   TCP       https > bvcontrol [ACK] Seq=1
 163 97.897850      192.168.0.100   174.129.27.168  TCP       [TCP segment of a reassembled

⊞ Frame 159 (54 bytes on wire, 54 bytes captured)
⊞ Ethernet II, Src: D-Link_cf:ea:c7 (00:24:01:cf:ea:c7), Dst: HonHaiPr_77:5d:a1 (00:25:56:77:5d:a1)
⊞ Internet Protocol, Src: 174.129.27.168 (174.129.27.168), Dst: 192.168.0.100 (192.168.0.100)
⊞ Transmission Control Protocol, Src Port: https (443), Dst Port: bvcontrol (1236), Seq: 1414, Ack: 4993, Len: 0
```



- Note: The hierarchical display here is upside down compared to the Internet protocol stack that you learn in the lecture.

ANALYZING CAPTURED DATA



Microsoft (src net 192.168.1.6) [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

Filter: http.request.version=="HTTP/1.1"

```
No.   Time      Source       Destination    Protocol Length Info
  686 12.794845 192.168.1.6  174.35.52.133  HTTP      462 GET /thumbnail/76d800a7jw1dpgsbd8ja6j.jpg HTTP/1.1
  688 12.797284 192.168.1.6  174.35.52.133  HTTP      462 GET /thumbnail/69abd30bjw1dpgt36vcuvj.jpg HTTP/1.1
  694 12.812058 192.168.1.6  174.35.52.142  HTTP      462 GET /thumbnail/7f1ef208jw1dpgu7nx3awj.jpg HTTP/1.1
  729 13.007040 192.168.1.6  174.35.52.142  HTTP      462 GET /thumbnail/5f75ec4agw1dpgsmyhfinj.jpg HTTP/1.1
  733 13.011754 192.168.1.6  174.35.52.142  HTTP      462 GET /thumbnail/93831636jw1dpg6jjkmzvj.jpg HTTP/1.1
  734 13.012022 192.168.1.6  174.35.52.142  HTTP      462 GET /thumbnail/4711809ejw1dpgu2cd15rj.jpg HTTP/1.1
  735 13.012321 192.168.1.6  174.35.52.142  HTTP      462 GET /thumbnail/7069fcb4jw1dpgrdksra2j.jpg HTTP/1.1
  750 13.068017 192.168.1.6  174.35.52.142  HTTP      460 GET /bmiddle/5f75ec4agw1dpgsmyhfinj.jpg HTTP/1.1
```

```
⊞ Frame 686: 462 bytes on wire (3696 bits), 462 bytes captured (3696 bits)
⊞ Ethernet II, Src: LiteonTe_14:fc:f9 (68:a3:c4:14:fc:f9), Dst: Netgear_2f:8b:49 (74:44:01:2f:8b:49)
⊞ Internet Protocol Version 4, Src: 192.168.1.6 (192.168.1.6), Dst: 174.35.52.133 (174.35.52.133)
⊞ Transmission Control Protocol, Src Port: 51529 (51529), Dst Port: http (80), Seq: 1, Ack: 1, Len: 408
⊟ Hypertext Transfer Protocol
  ⊞ GET /thumbnail/76d800a7jw1dpgsbd8ja6j.jpg HTTP/1.1\r\n
    Host: ww1.sinaimg.cn\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.7 (KHTML, like Gecko) Chrome/16.0.912.77 Safari/535.7\r\n
    Accept: */*\r\n
    Referer: http://www.weibo.com/u/1740944337?wvr=3.6&lf=reg\r\n
    Accept-Encoding: gzip,deflate,sdch\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3\r\n
    \r\n
    [Full request URI: http://ww1.sinaimg.cn/thumbnail/76d800a7jw1dpgsbd8ja6j.jpg]
```

- HTTP header

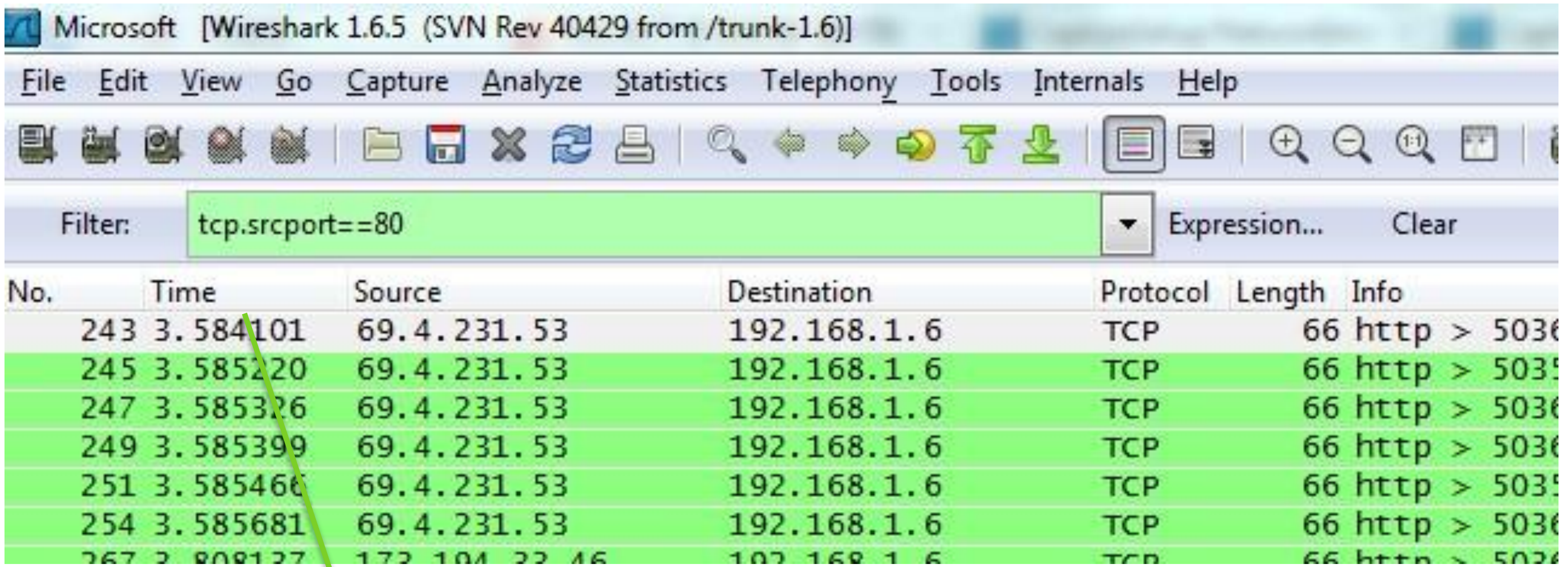
WIRESHARK FILTERS

- **Two types of filters:**
- **Capture Filters**
- **Display Filters**

- Wireshark contains a powerful **capture** filter engine that helps remove unwanted packets from a packet trace and only retrieves the packets of our interest.

- **Display** filters let you compare the fields within a protocol against a specific value, compare fields against fields, and check the existence of specified fields or protocols

EXAMPLE OF A DISPLAY FILTER


Microsoft [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear

Filter: tcp.srcport==80

```
No.      Time          Source            Destination      Protocol  Length  Info
     243 3.584101      69.4.231.53       192.168.1.6      TCP           66  http > 5036
     245 3.585220      69.4.231.53       192.168.1.6      TCP           66  http > 5035
     247 3.585326      69.4.231.53       192.168.1.6      TCP           66  http > 5036
     249 3.585399      69.4.231.53       192.168.1.6      TCP           66  http > 5036
     251 3.585466      69.4.231.53       192.168.1.6      TCP           66  http > 5035
     254 3.585681      69.4.231.53       192.168.1.6      TCP           66  http > 5036
     267 3.808137      173.194.33.46     192.168.1.6      TCP           66  http > 5036
```

- Display filter separates the packets to be displayed (In this case, only packets with source port 80 are displayed)

WIRESHARK FILTERS

- **Comparison operators**
- Fields can also be compared against values. The comparison operators can be expressed either through English-like abbreviations or through C-like symbols:
- eq, == Equal
- ne, != Not Equal
- gt, > Greater Than
- lt, < Less Than
- ge, >= Greater than or Equal to
- le, <= Less than or Equal to

WIRESHARK FILTERS

- **Logical Expressions**

  Tests can be combined using logical expressions. These too are expressible in C-like syntax or with English-like abbreviations:

and, &&	Logical AND
or, ||	Logical OR
not, !	Logical NOT

- Some Valid Filters
- tcp.port == 80 and ip.src == 192.168.2.1
- http and frame[100-199] contains "wireshark"

CAPTURE FILTERS

Syntax	Protocol	Direction	Host(s)	Logical Op.	Other Express.
Example	tcp	dst	136.159.5.20	and	host 136.159.5.6

- **Protocol:**
- *Values*: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp.
- If no protocol is specified, all the protocols are used.

- **Direction:**
- Values: src, dst, src and dst, src or dst
- If no source or destination is specified, the "src or dst" keywords are applied.
- For example, “host 136.159.5.20" is equivalent to "src or dst host 136.159.5.20".

CAPTURE FILTERS

- **Host(s):**
- Values: net, port, host, portrange.
- If no host(s) is specified, the "host" keyword is used.
- For example, "src 136.159.5.20" is equivalent to "src host 136.159.5.20".

- **Logical Operations:**
- Values: not, and, or.
- Negation ("not") has highest precedence. Alternation ("or") and concatenation ("and") have equal precedence and associate left to right.
- For example,

"not tcp port 3128 and tcp port 80" is equivalent to "(not tcp port 3128) and tcp port 80".

CAPTURE FILTERS(EXAMPLES)

- **tcp port 80**

  Displays packets with tcp protocol on port 80.

- **ip src host** 136.159.5.20

  Displays packets with source IP address equals to 136.159.5.20.

- **host** 136.159.5.1

  Displays packets with source or destination IP address equals to 136.159.5.1.

- **src portrange 2000-2500**

  Displays packets with source UDP or TCP ports in the 2000-2500 range.

CAPTURE FILTERS(EXAMPLES)

- **src host 136.159.5.20 and not dst host 136.159.5.1**

  Displays packets with source IP address equals to 136.159.5.20 and in the same time not with the destination IP address 136.159.5.1.

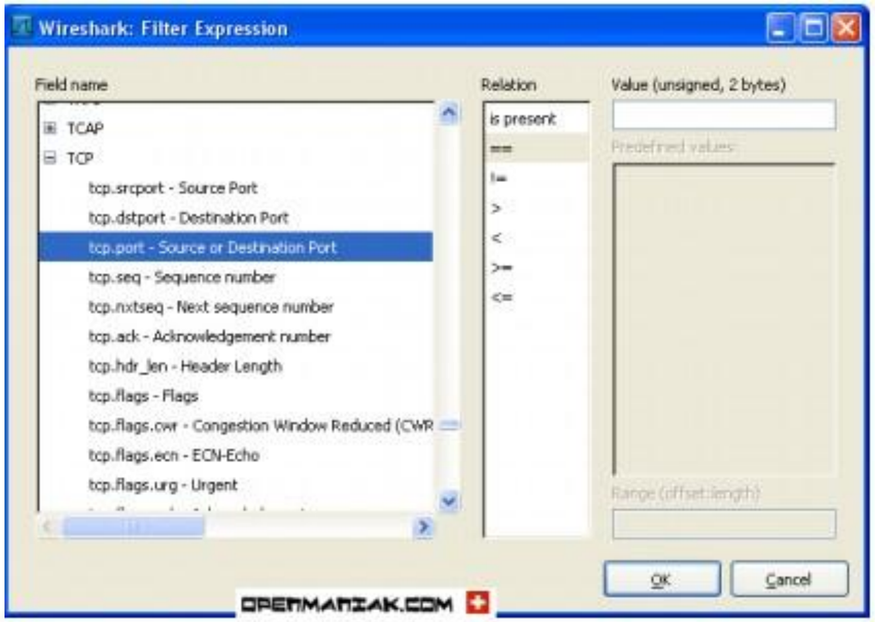
- **(src host 136.159.5.1 or src host 136.159.5.3) and tcp dst portrange 200-10000 and dst host 136.159.5.2**

  Displays packets with source IP address 136.159.5.1 or source address136.159.5.3, the result is then concatenated with packets having destination TCP portrange from 200 to 10000 and destination IP address136.159.5.2.

DISPLAY FILTERS

Syntax	Protocol	.	String 1	.	String 2	Comparison operators	Value	Logical Op.	Other Expr.
Example	http	.	request	.	method	==	get	or	tcp.port == 80

- String1, String2 (Optional settings): Sub protocol categories inside the protocol. To find them, look for a protocol and then click on the "+" character.


Wireshark: Filter Expression
Field name
TCAP
TCP
tcp.srcport - Source Port
tcp.dstport - Destination Port
tcp.port - Source or Destination Port
tcp.seq - Sequence number
tcp.nxtseq - Next sequence number
tcp.ack - Acknowledgement number
tcp.hdr_len - Header Length
tcp.flags - Flags
tcp.flags.cwr - Congestion Window Reduced (CWR
tcp.flags.ecn - ECN-Echo
tcp.flags.urg - Urgent
Relation
is present
==
!=
>
<
>=
<=
Value (unsigned, 2 bytes)
Predefined values:
Range (offset:length)
OK
Cancel
OPENMANIAK.COM

DISPLAY FILTERS(EXAMPLES)

- **ip.addr == 136.159.5.20**

  Displays the packets with source or destination IP address equals to 136.159.5.20 .

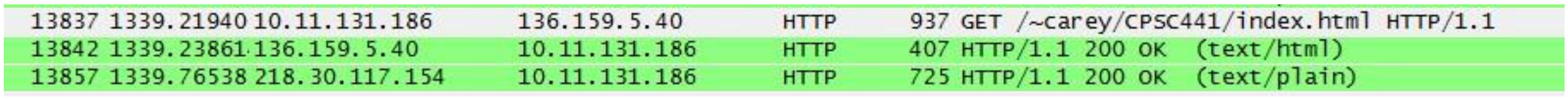
- **http.request.version=="HTTP/1.1“**

  Display http Version

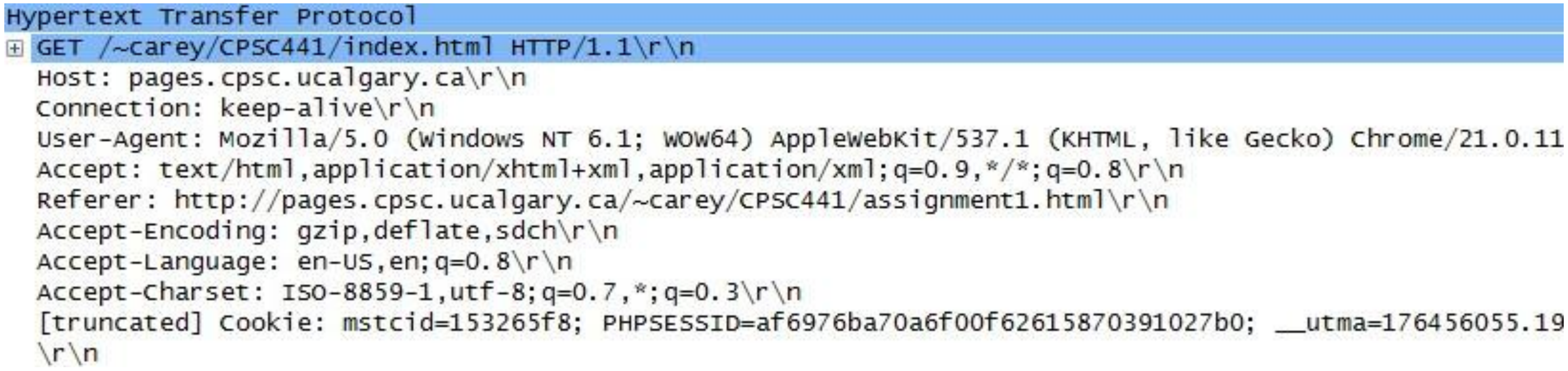
- **tcp.dstport == 25**
- **tcp.flags**

  Display packets having a TCP flags

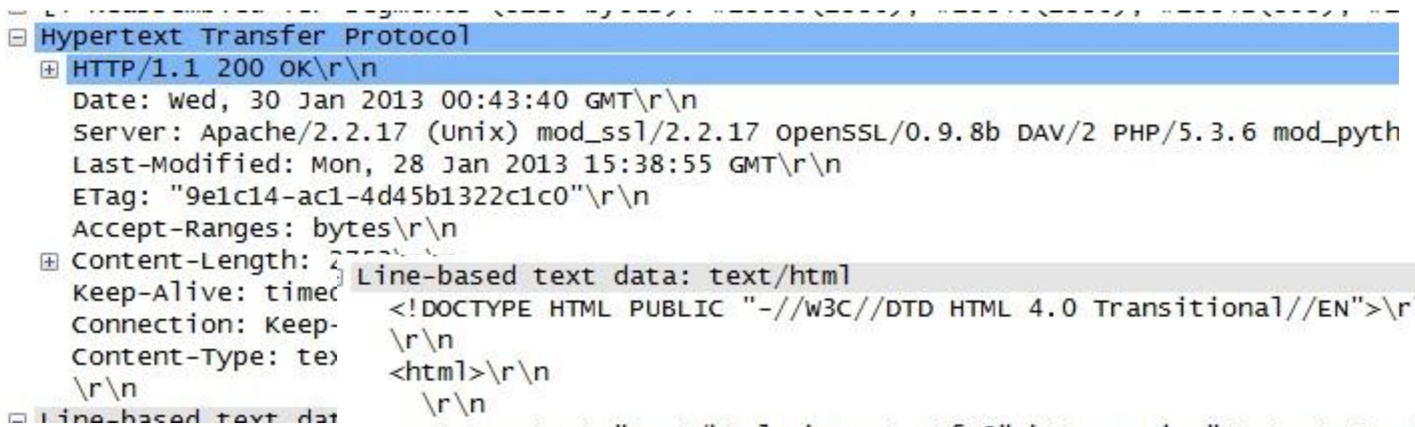
Example



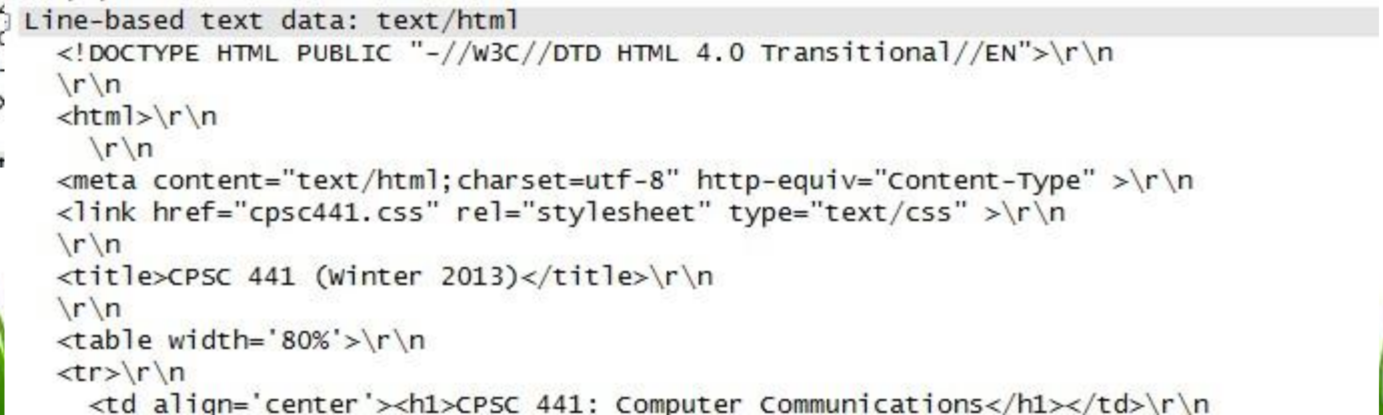
```
13837 1339.21940 10.11.131.186    136.159.5.40     HTTP    937 GET /~carey/CPSC441/index.html HTTP/1.1
13842 1339.23861 136.159.5.40     10.11.131.186    HTTP    407 HTTP/1.1 200 OK  (text/html)
13857 1339.76538 218.30.117.154   10.11.131.186    HTTP    725 HTTP/1.1 200 OK  (text/plain)
```



```
Hypertext Transfer Protocol
⊞ GET /~carey/CPSC441/index.html HTTP/1.1\r\n
   Host: pages.cpsc.ucalgary.ca\r\n
   Connection: keep-alive\r\n
   User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.1 (KHTML, like Gecko) Chrome/21.0.11
   Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
   Referer: http://pages.cpsc.ucalgary.ca/~carey/CPSC441/assignment1.html\r\n
   Accept-Encoding: gzip,deflate,sdch\r\n
   Accept-Language: en-US,en;q=0.8\r\n
   Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3\r\n
   [truncated] Cookie: mstcid=153265f8; PHPSESSID=af6976ba70a6f00f62615870391027b0; __utma=176456055.19
   \r\n
```

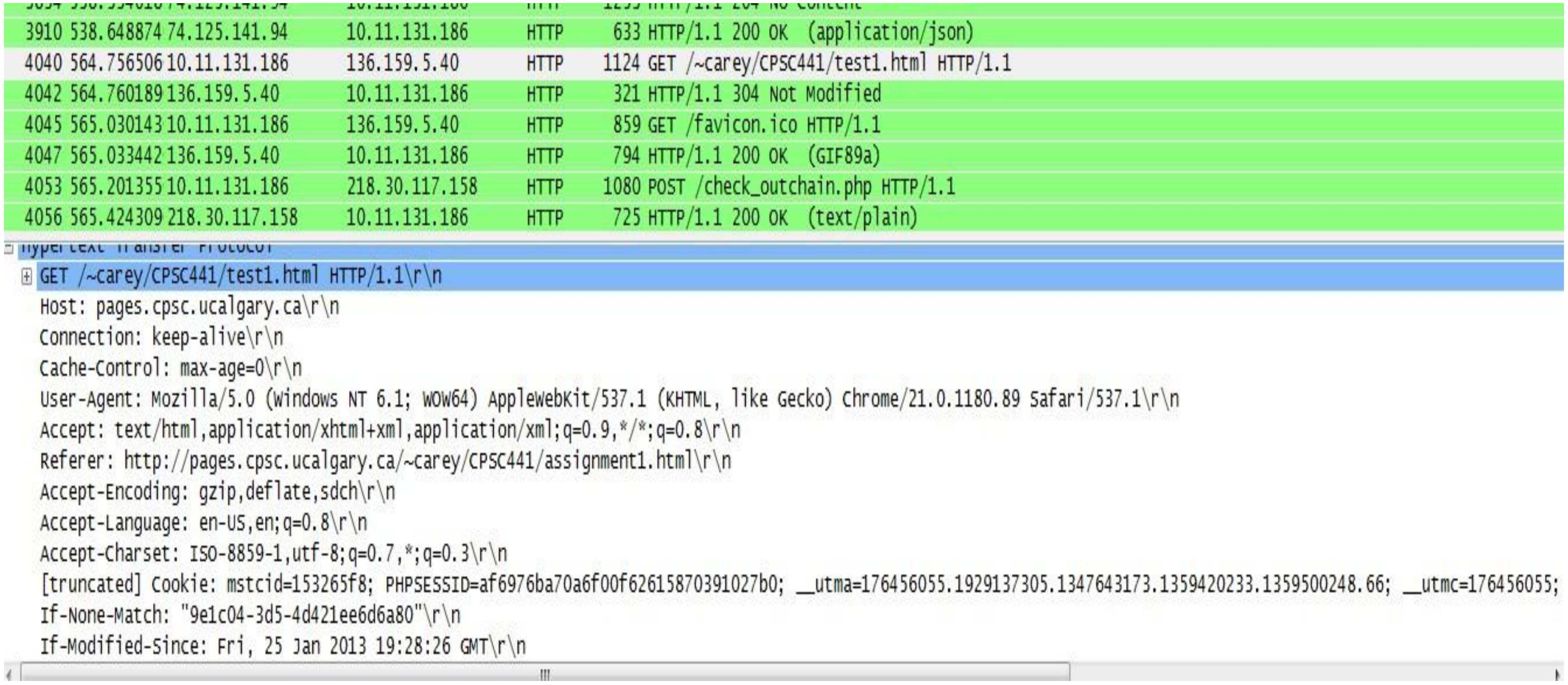


```
⊟ Hypertext Transfer Protocol
   ⊞ HTTP/1.1 200 OK\r\n
      Date: Wed, 30 Jan 2013 00:43:40 GMT\r\n
      Server: Apache/2.2.17 (Unix) mod_ssl/2.2.17 OpenSSL/0.9.8b DAV/2 PHP/5.3.6 mod_pyth
      Last-Modified: Mon, 28 Jan 2013 15:38:55 GMT\r\n
      ETag: "9e1c14-ac1-4d45b1322c1c0"\r\n
      Accept-Ranges: bytes\r\n
   ⊞ Content-Length: 2
      Keep-Alive: timed
      Connection: Keep-
      Content-Type: tex
      \r\n
⊟ Line-based text dat
```



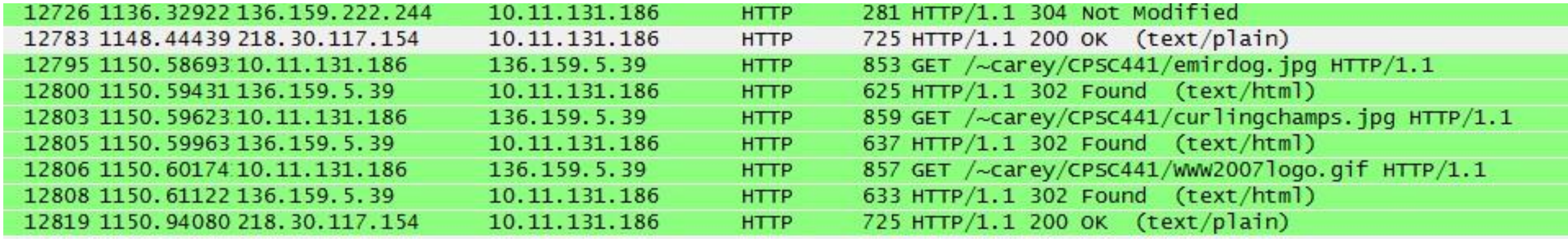
```
Line-based text data: text/html
   <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">\r\n
   \r\n
   <html>\r\n
     \r\n
   <meta content="text/html;charset=utf-8" http-equiv="Content-Type" >\r\n
   <link href="cpsc441.css" rel="stylesheet" type="text/css" >\r\n
   \r\n
   <title>CPSC 441 (Winter 2013)</title>\r\n
   \r\n
   <table width='80%'>\r\n
   <tr>\r\n
     <td align='center'><h1>CPSC 441: Computer Communications</h1></td>\r\n
```

Example

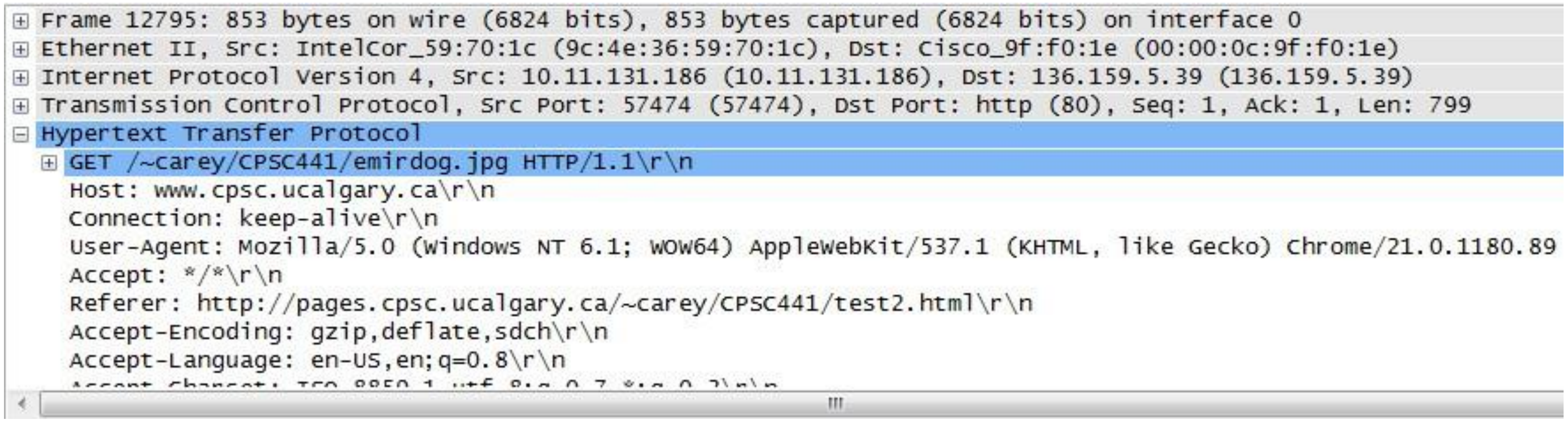


```
3910 538.648874 74.125.141.94    10.11.131.186   HTTP    633 HTTP/1.1 200 OK  (application/json)
4040 564.756506 10.11.131.186    136.159.5.40    HTTP   1124 GET /~carey/CPSC441/test1.html HTTP/1.1
4042 564.760189 136.159.5.40     10.11.131.186   HTTP    321 HTTP/1.1 304 Not Modified
4045 565.030143 10.11.131.186    136.159.5.40    HTTP    859 GET /favicon.ico HTTP/1.1
4047 565.033442 136.159.5.40     10.11.131.186   HTTP    794 HTTP/1.1 200 OK  (GIF89a)
4053 565.201355 10.11.131.186    218.30.117.158  HTTP   1080 POST /check_outchain.php HTTP/1.1
4056 565.424309 218.30.117.158   10.11.131.186   HTTP    725 HTTP/1.1 200 OK  (text/plain)
Hypertext Transfer Protocol
  GET /~carey/CPSC441/test1.html HTTP/1.1\r\n
  Host: pages.cpsc.ucalgary.ca\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.1 (KHTML, like Gecko) Chrome/21.0.1180.89 Safari/537.1\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Referer: http://pages.cpsc.ucalgary.ca/~carey/CPSC441/assignment1.html\r\n
  Accept-Encoding: gzip,deflate,sdch\r\n
  Accept-Language: en-US,en;q=0.8\r\n
  Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3\r\n
  [truncated] Cookie: mstcid=153265f8; PHPSESSID=af6976ba70a6f00f62615870391027b0; __utma=176456055.1929137305.1347643173.1359420233.1359500248.66; __utmc=176456055;
  If-None-Match: "9e1c04-3d5-4d421ee6d6a80"\r\n
  If-Modified-Since: Fri, 25 Jan 2013 19:28:26 GMT\r\n
```

Example



```
12726 1136.32922 136.159.222.244   10.11.131.186   HTTP   281 HTTP/1.1 304 Not Modified
12783 1148.44439 218.30.117.154    10.11.131.186   HTTP   725 HTTP/1.1 200 OK  (text/plain)
12795 1150.58693 10.11.131.186     136.159.5.39    HTTP   853 GET /~carey/CPSC441/emirdog.jpg HTTP/1.1
12800 1150.59431 136.159.5.39      10.11.131.186   HTTP   625 HTTP/1.1 302 Found  (text/html)
12803 1150.59623 10.11.131.186     136.159.5.39    HTTP   859 GET /~carey/CPSC441/curlingchamps.jpg HTTP/1.1
12805 1150.59963 136.159.5.39      10.11.131.186   HTTP   637 HTTP/1.1 302 Found  (text/html)
12806 1150.60174 10.11.131.186     136.159.5.39    HTTP   857 GET /~carey/CPSC441/www2007logo.gif HTTP/1.1
12808 1150.61122 136.159.5.39      10.11.131.186   HTTP   633 HTTP/1.1 302 Found  (text/html)
12819 1150.94080 218.30.117.154    10.11.131.186   HTTP   725 HTTP/1.1 200 OK  (text/plain)
```



```
⊞ Frame 12795: 853 bytes on wire (6824 bits), 853 bytes captured (6824 bits) on interface 0
⊞ Ethernet II, Src: IntelCor_59:70:1c (9c:4e:36:59:70:1c), Dst: Cisco_9f:f0:1e (00:00:0c:9f:f0:1e)
⊞ Internet Protocol Version 4, Src: 10.11.131.186 (10.11.131.186), Dst: 136.159.5.39 (136.159.5.39)
⊞ Transmission Control Protocol, Src Port: 57474 (57474), Dst Port: http (80), Seq: 1, Ack: 1, Len: 799
⊟ Hypertext Transfer Protocol
  ⊞ GET /~carey/CPSC441/emirdog.jpg HTTP/1.1\r\n
    Host: www.cpsc.ucalgary.ca\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.1 (KHTML, like Gecko) Chrome/21.0.1180.89
    Accept: */*\r\n
    Referer: http://pages.cpsc.ucalgary.ca/~carey/CPSC441/test2.html\r\n
    Accept-Encoding: gzip,deflate,sdch\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3\r\n
```

Thanks for attending!