

COMP4621 Wireshark Labs: Getting Started

TA: Waheed GHALI

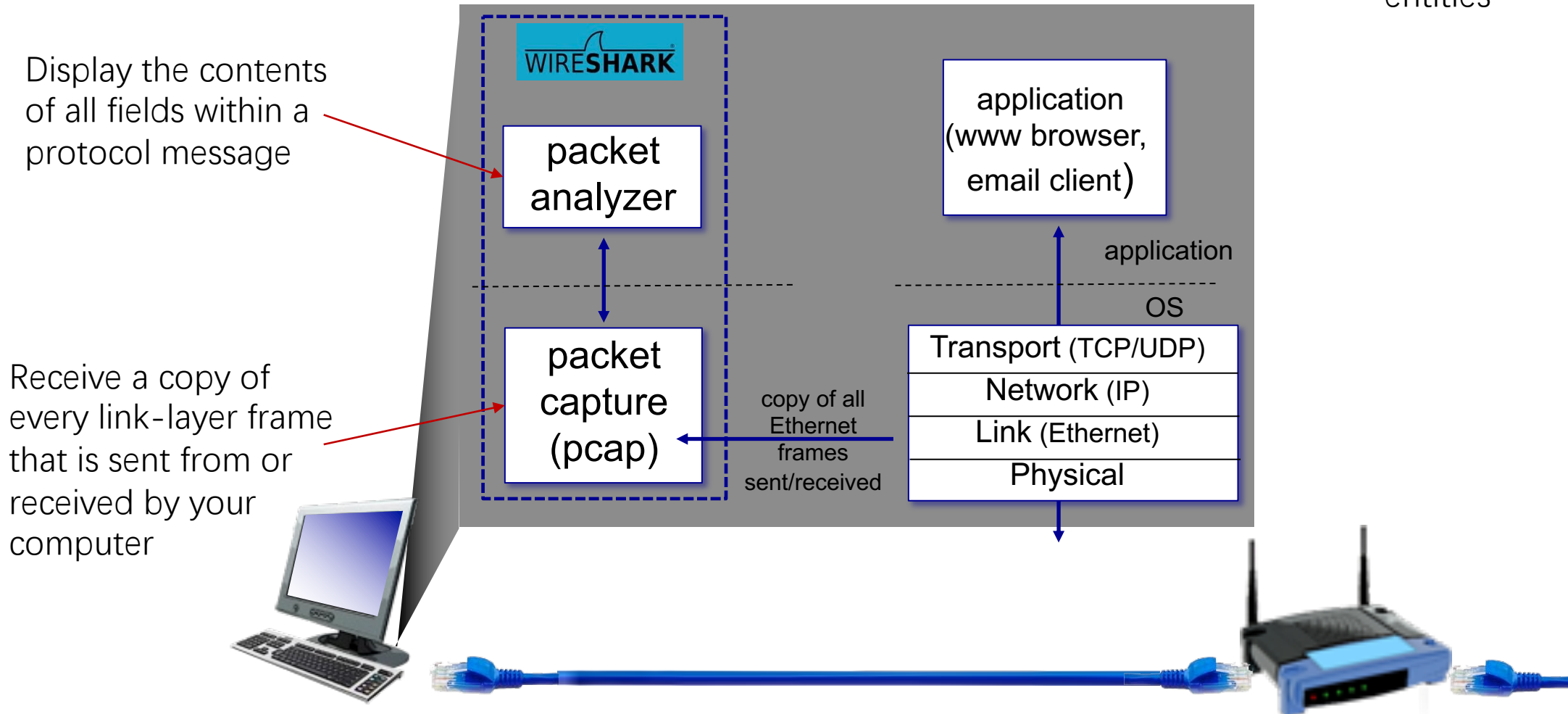
E-mail: wggghali@connect.ust.hk

Outline

- Packet sniffer and Wireshark
- Downloading Wireshark
- Running Wireshark
- Test Run: Basic HTTP GET / response interaction

Packet sniffer and Wireshark

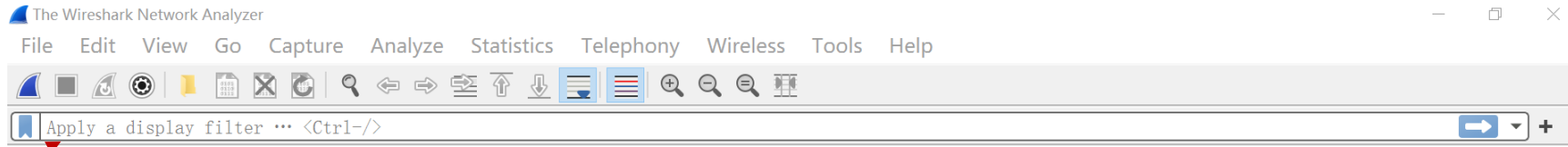
The basic tool for observing the messages exchanged between executing protocol entities



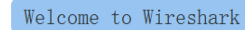
Downloading Wireshark

- <http://www.wireshark.org/download.html>
- Other useful pages
 - user-guide: http://www.wireshark.org/docs/wsug_html_chunked/
 - man pages: <http://www.wireshark.org/docs/man-pages/>
 - FAQ: <http://www.wireshark.org/faq.html>

Running Wireshark



Packet display filter



Open

E:\http-ethereal-trace-1 (4443 Bytes)

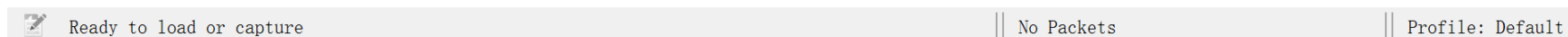


List of interfaces to capture packets from

Learn

[User's Guide](#) • [Wiki](#) • [Questions and Answers](#) • [Mailing Lists](#) • [SharkFest](#) • [Wireshark Discord](#) • [Donate](#)

You are running Wireshark 4.0.3 (v4.0.3-0-gc552f74cdc23). You receive automatic updates.



startup screen

Running Wireshark

Stop
capturing
packets

The image shows the Wireshark network protocol analyzer interface. At the top, the menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The main window is divided into three panes. The top pane, titled 'Current filter: tcp', displays a list of captured packets. The bottom pane shows the details of the selected packet (No. 61), including the Ethernet II header, Internet Protocol Version 4 header, Transmission Control Protocol header, Hypertext Transfer Protocol header, and Data (807 bytes). The status bar at the bottom indicates 'WLAN: <live capture in progress>' and 'Packets: 256 • Displayed: 236 (92.2%) | Profile: Default'.

No.	Time	Source	Destination	Protocol	Length	Info
55	21.8746...	10.79.27.165	43.155.124.118	TCP	1304	6256 → 80 [ACK] Seq=2501 Ack=1 Win=66048 Len=1250
56	21.8746...	10.79.27.165	43.155.124.118	HTTP	955	POST /mmtls/000076ac HTTP/1.1
57	21.8833...	58.20.136.6	10.79.27.165	TCP	66	[TCP Retransmission] 443 → 6223 [SYN, ACK] Seq=0
58	21.8862...	43.155.124.118	10.79.27.165	TCP	54	80 → 6256 [ACK] Seq=1 Ack=4652 Win=38528 Len=0
59	21.9940...	180.163.222.179	10.79.27.165	TCP	54	[TCP Dup ACK 14#1] 80 → 6227 [ACK] Seq=1 Ack=1 Wi
60	21.9941...	10.79.27.165	180.163.222.179	TCP	54	[TCP Dup ACK 15#1] 6227 → 80 [ACK] Seq=1 Ack=2 Wi
61	22.0469...	43.155.124.118	10.79.27.165	HTTP	960	HTTP/1.1 200 OK
62	22.0473...	10.79.27.165	43.155.124.118	TCP	54	6256 → 80 [FIN, ACK] Seq=4652 Ack=907 Win=65280 L
63	22.0498...	43.155.124.118	10.79.27.165	TCP	54	80 → 6256 [FIN, ACK] Seq=907 Ack=4652 Win=38528 L
64	22.0499...	10.79.27.165	43.155.124.118	TCP	54	6256 → 80 [ACK] Seq=4653 Ack=908 Win=65280 Len=0
65	22.0578...	43.155.124.118	10.79.27.165	TCP	54	80 → 6256 [ACK] Seq=908 Ack=4653 Win=38528 Len=0
66	22.9075...	58.20.136.6	10.79.27.165	TCP	66	[TCP Retransmission] 443 → 6223 [SYN, ACK] Seq=0
67	23.7943...	104.18.7.183	10.79.27.165	TLSv1.2	79	Application Data
68	23.7949...	10.79.27.165	104.18.7.183	TLSv1.2	83	Application Data

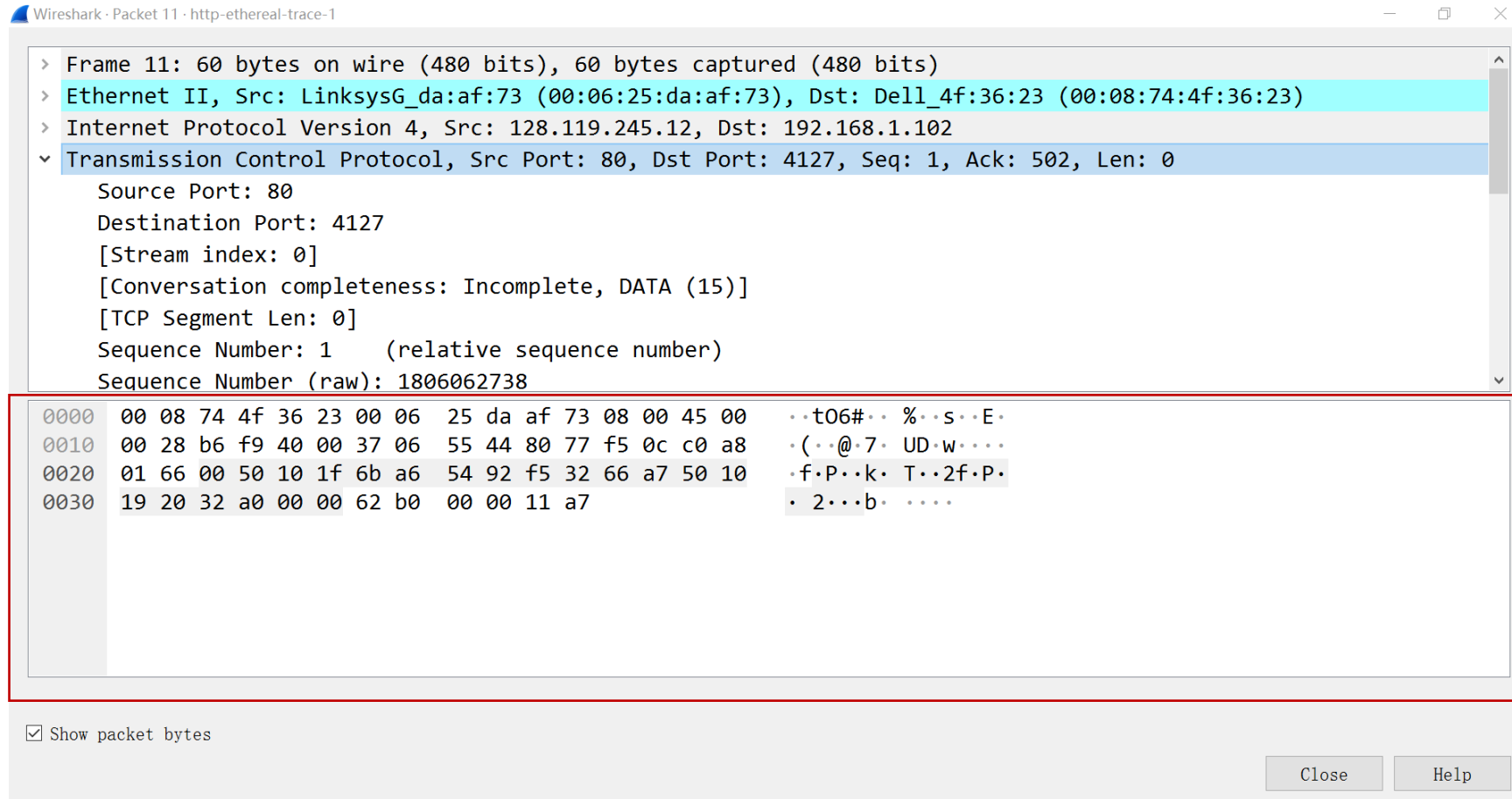
Details of selected packet (No. 61):

- > Frame 61: 960 bytes on wire (7680 bits), 960 bytes captured (7680 bits) on interface \Device\NPF_{714D37A8-0CF5-40EE-9574-E8DC5F06AE0A}, id
- > Ethernet II, Src: Cisco_93:c2:1f (34:73:2d:93:c2:1f), Dst: IntelCor_d0:8d:0b (90:78:41:d0:8d:0b)
- > Internet Protocol Version 4, Src: 43.155.124.118, Dst: 10.79.27.165
- > Transmission Control Protocol, Src Port: 80, Dst Port: 6256, Seq: 1, Ack: 4652, Len: 906
- > Hypertext Transfer Protocol
- > Data (807 bytes)

List of
captured
packets

details of
selected
packet
header

Running Wireshark



Packet-contents
window

Running Wireshark

http-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst == 128.119.245.12

No.	Time	Source	Destination	Protocol	Length	Info
7	4.675312	192.168.1.102	128.119.245.12	TCP	62	4127 → 80 [SYN] Seq=0 Win=64240 Len=0 M
9	4.694458	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=1 Ack=1 Win=64240 L
10	4.694850	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-1.html HTTP/1.1
13	4.724332	192.168.1.102	128.119.245.12	HTTP	541	GET /favicon.ico HTTP/1.1
15	4.859777	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=989 Ack=1727 Win=64

http-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
9	4.694458	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=1 Ack=1 Win=64240 L
15	4.859777	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=989 Ack=1727 Win=64
11	4.717289	128.119.245.12	192.168.1.102	TCP	60	80 → 4127 [ACK] Seq=1 Ack=502 Win=6432
7	4.675312	192.168.1.102	128.119.245.12	TCP	62	4127 → 80 [SYN] Seq=0 Win=64240 Len=0 M
8	4.694429	128.119.245.12	192.168.1.102	TCP	62	80 → 4127 [SYN, ACK] Seq=0 Ack=1 Win=58
12	4.718993	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
13	4.724332	192.168.1.102	128.119.245.12	HTTP	541	GET /favicon.ico HTTP/1.1
10	4.694850	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-1.html HTTP/1.1
14	4.750366	128.119.245.12	192.168.1.102	HTTP	1395	HTTP/1.1 404 Not Found (text/html)

Test Run: Basic HTTP GET / response interaction

1. Start up your web browser
2. Open the Wireshark packet sniffer
3. Select your interface and begin Wireshark packet capture
4. Enter the following in your web browser:
`http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html`
5. After your browser has displayed the INTRO-wireshark-file1.html page, stop the Wireshark packet capture
6. Type 'http' in the display filter window

Test Run: Basic HTTP GET / response interaction

The image shows a Wireshark packet capture of an HTTP GET request and response. The packet list shows four packets: a GET request (frame 282), a 200 OK response (frame 286), a GET request for a favicon (frame 327), and a 404 Not Found response (frame 368). The details pane for the first packet (frame 282) is expanded, showing the Hypertext Transfer Protocol section. The request is a GET for /wireshark-labs/INTRO-wireshark-file1.html. The response (frame 286) is a 200 OK with content type text/html.

No.	Time	Source	Destination	Protocol	Length	Info
282	11.380803	10.79.27.165	128.119.245.12	HTTP	527	GET /wireshark-labs/INTRO-wireshark-file1.html
286	11.685040	128.119.245.12	10.79.27.165	HTTP	492	HTTP/1.1 200 OK (text/html)
327	11.787250	10.79.27.165	128.119.245.12	HTTP	473	GET /favicon.ico HTTP/1.1
368	12.090380	128.119.245.12	10.79.27.165	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 282: 527 bytes on wire (4216 bits), 527 bytes captured (4216 bits) on interface \Device\NPF_{714D37A8-0CF5-40EE-9574-E8DC5F06AE0A}, id 0
Ethernet II, Src: IntelCor_d0:8d:0b (90:78:41:d0:8d:0b), Dst: All-HSRP-routers_f1 (00:00:0c:07:ac:f1)
Internet Protocol Version 4, Src: 10.79.27.165, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 7036, Dst Port: 80, Seq: 1, Ack: 1, Len: 473
Hypertext Transfer Protocol
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: zh-CN,zh;q=0.9\r\n\r\n[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
[HTTP request 1/2]
[Response in frame: 286]
[Next request in frame: 327]

Test Run: Basic HTTP GET / response interaction

lab1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
282	11.380803	10.79.27.165	128.119.245.12	HTTP	527	GET /wireshark-labs/INTRO-wireshark-file1.html
286	11.685040	128.119.245.12	10.79.27.165	HTTP	492	HTTP/1.1 200 OK (text/html)
327	11.787250	10.79.27.165	128.119.245.12	HTTP	473	GET /favicon.ico HTTP/1.1
368	12.090380	128.119.245.12	10.79.27.165	HTTP	538	HTTP/1.1 404 Not Found (text/html)

> Frame 286: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{714D37A8-0CF5-40EE-9574-E8DC5F06AE0A}, id 0

> Ethernet II, Src: Cisco_93:c2:1f (34:73:2d:93:c2:1f), Dst: IntelCor_d0:8d:0b (90:78:41:d0:8d:0b)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.79.27.165

> Transmission Control Protocol, Src Port: 80, Dst Port: 7036, Seq: 1, Ack: 474, Len: 438

▼ Hypertext Transfer Protocol

▼ HTTP/1.1 200 OK\r\n

> [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Date: Thu, 16 Feb 2023 07:21:04 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Thu, 16 Feb 2023 06:59:02 GMT\r\n

Etag: "51-5f4cbbb55e59f"\r\n

Accept-Ranges: bytes\r\n

> Content-Length: 81\r\n

Keep-Alive: timeout=5, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=UTF-8\r\n

Hypertext Transfer Protocol (http), 357 bytes | Packets: 401 • Displayed: 7 (1.7%) | Profile: Default

▼ Line-based text data: text/html (3 lines)

```
<html>\n
Congratulations. You've downloaded the file lab2-1.html!\n
</html>\n
```

HTTP response message

Conclusion

- Packet sniffer and Wireshark
 - packet capture library
 - packet analyzer
- Downloading Wireshark
- Running Wireshark
 - Start the Wireshark
 - Select the interface and begin Wireshark packet capture
 - Stop the Wireshark packet capture
 - Use the display filter to filter the packets displayed

Lab Exercise

- What is the **IP address** of the gaia.cs.umass.edu? What is the **IP address** of your computer?
- Use the display filter to find the **HTTP** packets where the **destination IP address** is the IP address of the gaia.cs.umass.edu.
- Use the display filter to find the **TCP** packets where the **source IP address** is the IP address of the gaia.cs.umass.edu and the **destination IP address** is the IP address of your computer.
- Hint
 - https://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html