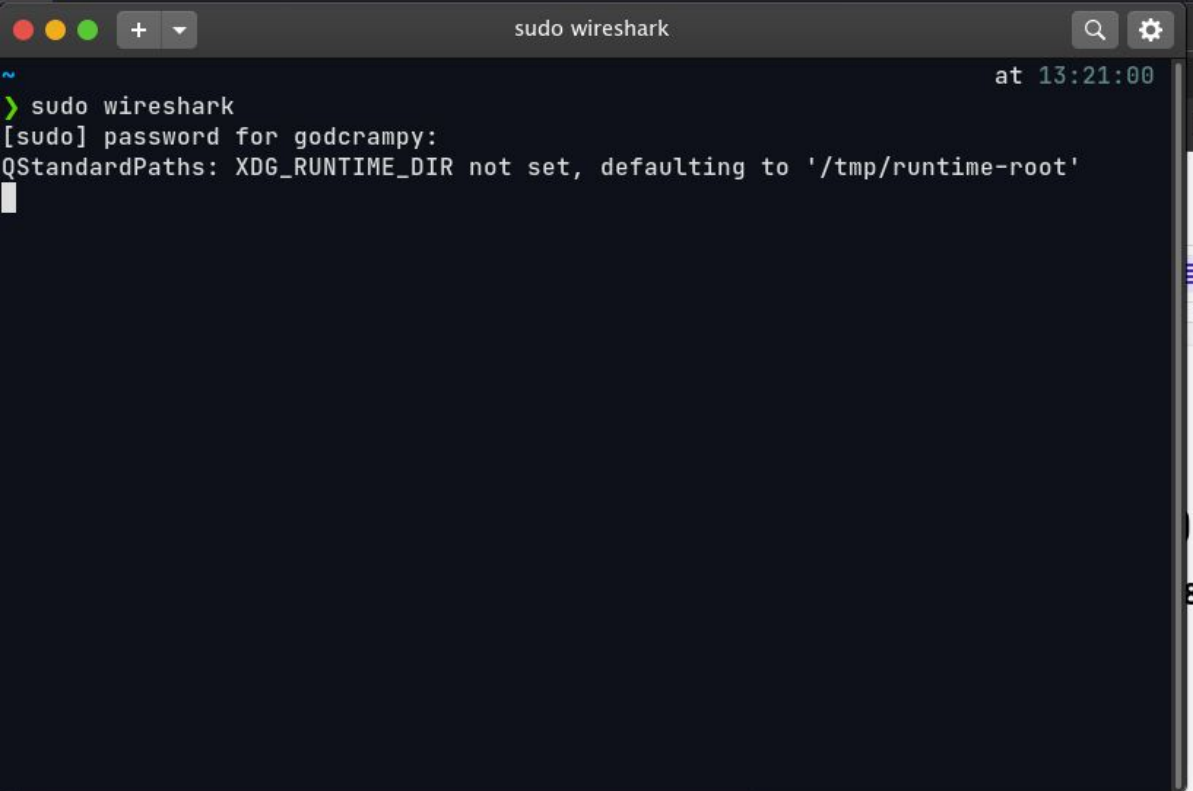


Computer Networks Lab 1

SAHIL BONDRE: U18CO021

1. Carefully read the lab instructions and finish all tasks above.

Starting Wireshark in Linux

A terminal window titled 'sudo wireshark' with standard Linux window controls (red, yellow, green buttons, a plus button, and a dropdown arrow). The terminal output shows the command 'sudo wireshark' being executed, followed by a password prompt '[sudo] password for godcrampy:' which has been entered. Below this, a message from QtStandardPaths states: 'XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root''. The terminal has a dark background with light-colored text. On the right side of the terminal window, there are search and settings icons. The text 'at 13:21:00' is visible in the top right corner of the terminal area. A vertical scrollbar is visible on the right edge of the terminal window.

```
at 13:21:00
> sudo wireshark
[sudo] password for godcrampy:
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

Welcome to Wireshark

Capture

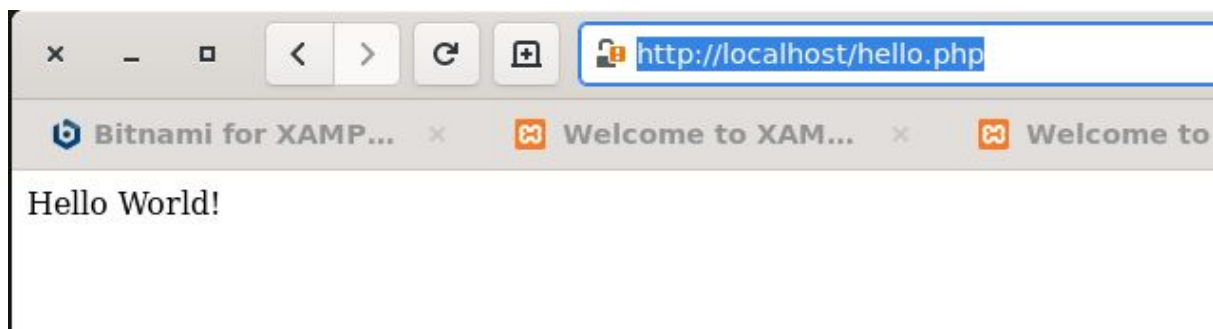
...using this filter:

wlo1	
Loopback: lo	
any	
virbr0	
eno1	
bluetooth-monitor	
nflog	
nfqueue	
bluetooth0	
usbmon0	
usbmon1	
usbmon2	
virbr0-nic	
⚙ Cisco remote capture: ciscodump	
⚙ DisplayPort AUX channel monitor capture: dpauxmon	
⚙ systemd Journal Export: sdjournal	
⚙ SSH remote capture: sshdump	
⚙ UDP Listener remote capture: udpdump	

Packet Analysis in Loopback

Sample Server running using PHP:

```
/opt/lampp/htdocs  
> cat hello.php  
<?php  
echo "Hello World!";  
?>
```



Captured Packet:

57	257.235807288	::1	::1	TCP
58	257.235936381	::1	::1	TCP
59	257.235977358	::1	::1	TCP
60	257.236720739	::1	::1	HTTP
61	257.236772268	::1	::1	TCP
62	257.241123896	::1	::1	HTTP
63	257.241266276	::1	::1	TCP

- Internet Protocol Version 6, Src: ::1, Dst: ::1
 - 0110 = Version: 6
 - 0000 0000 = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - 1111 1001 1010 1010 0101 = Flow Label: 0xf9aa5
 - Payload Length: 769
 - Next Header: TCP (6)
 - Hop Limit: 64
 - Source: ::1
 - Destination: ::1
- Transmission Control Protocol, Src Port: 32808, Dst Port: 80, Seq: 1, Ack: 1, Len: 737
 - Source Port: 32808
 - Destination Port: 80
 - [Stream index: 4]
 - [TCP Segment Len: 737]
 - Sequence number: 1 (relative sequence number)
 - Sequence number (raw): 2763860501
 - [Next sequence number: 738 (relative sequence number)]
 - Acknowledgment number: 1 (relative ack number)
 - Acknowledgment number (raw): 1578817614
 - 1000 = Header Length: 32 bytes (8)
 - Flags: 0x018 (PSH, ACK)
 - Window size value: 512
 - [Calculated window size: 65536]
 - [Window size scaling factor: 128]
 - Checksum: 0x0309 [unverified]
 - [Checksum Status: Unverified]
 - Urgent pointer: 0
 - Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
 - [SEQ/ACK analysis]
 - [Timestamps]
 - TCP payload (737 bytes)

- Frame 60: 823 bytes on wire (6584 bits), 823 bytes captured (6584 bits) on interface lo, id 0
 - Interface id: 0 (lo)
 - Encapsulation type: Ethernet (1)
 - Arrival Time: Aug 23, 2020 13:30:01.295662017 IST
 - [Time shift for this packet: 0.000000000 seconds]
 - Epoch Time: 1598169601.295662017 seconds
 - [Time delta from previous captured frame: 0.000743381 seconds]
 - [Time delta from previous displayed frame: 0.000743381 seconds]
 - [Time since reference or first frame: 257.236720739 seconds]
 - Frame Number: 60
 - Frame Length: 823 bytes (6584 bits)
 - Capture Length: 823 bytes (6584 bits)
 - [Frame is marked: False]
 - [Frame is ignored: False]
 - [Protocols in frame: eth:ethertype:ipv6:tcp:http]
 - [Coloring Rule Name: HTTP]
 - [Coloring Rule String: http || tcp.port == 80 || http2]
- Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
 - Destination: 00:00:00_00:00:00 (00:00:00:00:00:00)
 - Source: 00:00:00_00:00:00 (00:00:00:00:00:00)
 - Type: IPv6 (0x86dd)

```

    for payload (in bytes)
  ▾ Hypertext Transfer Protocol
    ▸ GET /hello.php HTTP/1.1\r\n
      Host: localhost\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.89 Safari/537.36\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
      Sec-Fetch-Site: none\r\n
      Sec-Fetch-Mode: navigate\r\n
      Sec-Fetch-Dest: document\r\n
      Accept-Encoding: gzip, deflate, br\r\n
      Accept-Language: en-US,en-IN;q=0.9,en;q=0.8\r\n
      Cookie: _ga=GA1.1.587401620.1576861109; _ga_DBBY9ZZY6L=GS1.1.1576942641.7.1.1576942964.0; __utmz=111872281.1581787171.1.1.utmcsr=(direct)
    [Full request URI: http://localhost/hello.php]
    [HTTP request 1/1]
    [Response in frame: 62]

```

Hex Dump:

0030	00 00 00 00 00 01 80 28	00 50 a4 bd 2a 15 5e 1a(.P...*.A.
0040	d8 4e 80 18 02 00 03 09	00 00 01 01 08 0a f0 fb	.N.....
0050	df e9 f0 fb df e8 47 45	54 20 2f 68 65 6c 6c 6fGE T /hello
0060	2e 70 68 70 20 48 54 54	50 2f 31 2e 31 0d 0a 48	.php HTTP/1.1..H
0070	6f 73 74 3a 20 6c 6f 63	61 6c 68 6f 73 74 0d 0a	ost: loc alhost..
0080	43 6f 6e 6e 65 63 74 69	6f 6e 3a 20 6b 65 65 70	Connecti on: keep
0090	2d 61 6c 69 76 65 0d 0a	55 70 67 72 61 64 65 2d	-alive.. Upgrade-
00a0	49 6e 73 65 63 75 72 65	2d 52 65 71 75 65 73 74	Insecure -Request
00b0	73 3a 20 31 0d 0a 55 73	65 72 2d 41 67 65 6e 74	s: 1..Us er-Agent
00c0	3a 20 4d 6f 7a 69 6c 6c	61 2f 35 2e 30 20 28 58	: Mozill a/5.0 (X
00d0	31 31 3b 20 4c 69 6e 75	78 20 78 38 36 5f 36 34	11; Linu x x86_64
00e0	29 20 41 70 70 6c 65 57	65 62 4b 69 74 2f 35 33) AppleW ebKit/53
00f0	37 2e 33 36 20 28 4b 48	54 4d 4c 2c 20 6c 69 6b	7.36 (KH TML, lik
0100	65 20 47 65 63 6b 6f 29	20 43 68 72 6f 6d 65 2f	e Gecko) Chrome/
0110	38 34 2e 30 2e 34 31 34	37 2e 38 39 20 53 61 66	84.0.414 7.89 Saf

Packet Analysis over WLAN

1. Select WLAN interface in Wireshark
2. Start packet capture
3. Visit <http://wayne.edu>
4. Stop packet capture
5. Analyse the HTTP packet:

http.host==www.wayne.edu						
No.	Time	Source	Destination	Protocol	Length	Info
+	53.1310703255	192.168.0.104	141.217.1.160	HTTP	476	GET / HTTP/1.1

```

▶ Frame 53: 476 bytes on wire (3808 bits), 476 bytes captured (3808 bits) on interface wlo1, id 0
▶ Ethernet II, Src: IntelCor_81:0d:7b (40:a3:cc:81:0d:7b), Dst: TendaTec_c6:8f:40 (04:95:e6:c6:8f:40)
▶ Internet Protocol Version 4, Src: 192.168.0.104, Dst: 141.217.1.160
▶ Transmission Control Protocol, Src Port: 55462, Dst Port: 80, Seq: 1, Ack: 1, Len: 410
▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    Host: www.wayne.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.89 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://www.wayne.edu/]
    [HTTP request 1/1]
    [Response in frame: 57]

```

```

GET / HTTP/1.1
Host: www.wayne.edu
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.89 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 307 Temporary Redirect
Server: nginx/1.10.3
Date: Sun, 23 Aug 2020 08:59:01 GMT
Content-Type: text/html; charset=iso-8859-1
Content-Length: 228
Connection: keep-alive
Location: https://wayne.edu/
Cache-Control: max-age=0
Expires: Sun, 23 Aug 2020 08:59:01 GMT

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>307 Temporary Redirect</title>
</head><body>
<h1>Temporary Redirect</h1>
<p>The document has moved <a href="https://wayne.edu/">here</a>.</p>
</body></html>

```

2. If a packet is highlighted by black, what does it mean for the packet?

It means that the checksum was not matched.

View > Coloring Rules



The image shows a snippet of the Wireshark packet list. A packet is highlighted with a black background, which is a visual indicator for a 'Checksum Error'. The text 'Checksum Errors' is visible in the left column, and the packet details on the right show 'eth.fcs.status=="Bad"'.

3. What is the filter command for listing all outgoing http traffic?

Type http in the filter box.

http				
No.	Time	Source	Destination	Protocol
5	88.782738051	::1	::1	HTTP
7	88.959059067	::1	::1	HTTP
9	88.968653747	::1	::1	HTTP
11	89.160324491	::1	::1	HTTP
21	141.871617666	::1	::1	HTTP
23	142.761932833	::1	::1	HTTP
25	142.981581127	::1	::1	HTTP
27	143.240095803	::1	::1	HTTP
36	157.915332988	::1	::1	HTTP
38	157.916765665	::1	::1	HTTP
40	161.665778023	::1	::1	HTTP
42	161.666280809	::1	::1	HTTP
51	172.474522787	::1	::1	HTTP
53	172.476791329	::1	::1	HTTP
60	257.236720739	::1	::1	HTTP
62	257.241123896	::1	::1	HTTP

4. Why does DNS use Follow UDP Stream while HTTP use Follow TCP Stream?

UDP is unstable but quicker than TCP. DNS requests are tiny, so they have no difficulties fitting into the UDP segments. It doesn't utilise a time-consuming three-way hand-shake scheme to start the data transfer as TCP does. The UDP sends the data and saves lots of time.

HTTP uses TCP instead of UDP because it supports delivery via a three-way handshake and re-transmission of dropped packets. UDP is mainly used for voice and video streaming to avoid out of order packet assembly that can create jitter and doesn't require the use of a three-way handshake.

5. Using Wireshark to capture the FTP password

Connecting to another system using FTP

Username: android

Password: admin123

Credentials Captured in a packet:

2c fd ab 26 ee a2 40 a3 cc 81 0d 7b 08 00 45 00	, . & . @ . . . { . . E .
00 42 5d 39 40 00 40 06 5b 5f c0 a8 00 68 c0 a8	. B]9@ . @ . [_ . . h . .
00 65 ed dc 08 ad 25 c2 53 24 ad 7b 5f 9e 80 18	. e . . . % . S\$. { _ . . .
01 f6 4c 38 00 00 01 01 08 0a ac 70 28 e5 02 00	. . L8 p (. . .
40 32 55 53 45 52 20 61 6e 64 72 6f 69 64 0d 0a	@2USER a ndroid . . .

```

40 a3 cc 81 0d 7b 2c fd ab 26 ee a2 08 00 45 00 @...{, . &...E.
00 64 1f 47 40 00 40 06 99 2f c0 a8 00 65 c0 a8 .d.G@.@ /...e.
00 68 08 ad ed dc ad 7b 5f 9e 25 c2 53 32 80 18 .h...{ _%S2..
01 54 39 f3 00 00 01 01 08 0a 02 00 46 2e ac 70 .T9....F..p
28 e5 33 33 31 20 55 73 65 72 20 6e 61 6d 65 20 (.331 Us er name
6f 6b 61 79 2c 20 6e 65 65 64 20 70 61 73 73 77 okay, ne ed passw
6f 72 64 20 66 6f 72 20 61 6e 64 72 6f 69 64 2e ord for android.
0d 0a

```