

Mondie Alhousainan

## Wireshark Lab 3 - TCP

IT 520-A – Enterprise Infrastructure & Networks Due Date: 09/24/18 (Handed in at the beginning of class)

## Instructions:

- Start up your web browser. Go the <a href="http://gaia.cs.umass.edu/wireshark-labs/alice.txt">http://gaia.cs.umass.edu/wireshark-labs/alice.txt</a> and retrieve an ASCII copy of *Alice in Wonderland*. Save this file somewhere on your computer.
- Next go to http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html.
- Use the *Browse* button in this form to enter the name of the file (full path name) on your computer containing *Alice in Wonderland* (or do so manually). Don't yet press the "*Upload alice.txt file*" button.
- Now start up Wireshark and begin packet capture (Capture->Start) and then press OK on the Wireshark Packet Capture Options screen (we'll not need to select any options here).
- Returning to your browser, press the "Upload alice.txt file" button to upload the file to the gaia.cs.umass.edu server. Once the file has been uploaded, a short congratulations message will be displayed in your browser window.
- Stop Wireshark packet capture and filter tcp packets.
- Pay attention to the SYN ACK packets.
- Include a terminal screenshot showing computer IP address on the front page before Question 1, and a full PRINT of the HTTP OK message as the last page. <u>Labs will NOT be graded if either of these two is missing.</u> (You can refer to Lab 1 for instructions on how to PRINT

## Ouestions:

(For each of these questions, take a screenshot of Wireshark, and attach it to your answer) - Questions without Full Screenshot will not be graded. Your screenshot should indicate the time and date on your computer.

- 1. What is the TCP port number used by your computer to communicate with gaia.cs.umass.edu?
- 2. What is the TCP port number used by gaia.cs.umass.edu to communicate with your computer?
- 3. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between your computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?
- What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu
  to the client computer in reply to the SYN? You must dig deep and find the
  ACK from gaia.cs.umass.edu.
- 5. What is the sequence number of the TCP segment containing the HTTP POST command? Note: that to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

Moude Alhou yinging

<

X

0 TN 9/23/2018 5 # 8 8 Media State . . . . . . . . . . . . Media disconnected Connection-specific DNS Suffix . : Media State . . . . . . . . . . . Media disconnected Connection-specific DNS Suffix . : Media State . . . . . . . . . . . Media disconnected Connection-specific DNS Suffix . : Media State . . . . . . . . . . . . Media disconnected Connection-specific DNS Suffix . : Wireless LAN adapter Local Area Connection\* 11: Ethernet adapter Bluetooth Network Connection: Ethernet adapter Ethernet 2: thernet adapter Ethernet 3: O Type here to search lireless LAN adapter Wi-Fi: ::\Users\moudi>\_

1514 58589 → 60696 [ACK] Seq=1 Ack=198 Win=15680 Len=1460 [TCP segment of a reassembled PDU] 66 58589 > 60696 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK PERM=1 WS=32 66 60696 → 58589 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1 66 60695 + 3911 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1 54 60696 → 58589 [FIN, ACK] Seq=198 Ack=2783 Win=65536 Len=0 60 58589 → 60696 [ACK] Seq=2783 Ack=199 Win=15680 Len=0 60 58589 → 60696 [FIN, ACK] Seq=2782 Ack=198 Win=15680 Len=0 54 60696 + 58589 [ACK] Seq=198 Ack=2783 Win=65536 Len=0 60 58589 → 60696 [ACK] Seq=1 Ack=198 Win=15680 Len=0 54 60696 → 58589 [ACK] Seq=1 Ack=1 Win=65536 Len=0 251 GET /rootDesc.xml HTTP/1.1 1375 HTTP/1.1 200 OK Length Info Help Tools HTTP/. HTTP TCP TCP TCP TCP 10 P TCP TCP . Capture Analyze Statistics Telephony Wireless 000 128.119.245.12 192.168.1.182 192.168.1.182 192.168.1.182 192.168.8.101 192.168.1.182 192.168.1.182 192.168.1.182 192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1 111 \*\*\*\* 30 22:51:25.026891 192.168.1.182 62 22:51:37.202140 192.168.1.182 2 22:51:16.648469 192.168.1.182 22:51:25.034494 192.168.1.182 33 22:51:25.034673 192.168.1.182 38 22:51:25.043816 192.168.1.182 39 22:51:25.043940 192.168.1.182 22:51:25.034382 192.168.1.1 22:51:25.042622 192.168.1.1 22:51:25.043547 192.168.1.1 36 22:51:25.043764 192.168.1.1 37 22:51:25.043764 192.168.1.1 40 22:51:25.049460 192.168.1.1 N X

9

File Edit View 0

to S. 34

| lab3.pcapng

Expression...

Ethernet II, Src: IntelCor\_c5:a0:c6 (00:e1:8c:c5:aq:c6); DSt: Verizon\_a8:f8:d6 (48:5d:36:a8:f8:d6) Frame 30: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

55 60688 + 80 [ACK] Seq=1 Ack=1 Win=253 Len=1

>

Internet Protocol Version 4, Src: 192.168.1.182, Dkt: 192.168.1.1

Transmission Control Protocol, Src Port: 60696, Dst Port: 58589, 5

Destination Port: 58589 Source Port: 60696

[Stream index: 1]

(relative sequence number) [TCP Segment Len: 0] Sequence number: 0

This destination as not gaineres ormass edu.

(relative sequence number)] [Next sequence number: 0

Acknowledgment number: 0

1000 .... = Header Length: 32 bytes (8)

Mindow cira valua. 64240 Flags: 0x002 (SYN)

H]6.... 8c c5 a0 c6 08 00 45 00 48 5d 36 a8 f8 d6 00 e1

O Type here to search Ready to load or capture

iiī



TN 9/23/2018 Packets: 1006 · Displayed: 443 (44.0%) · Dropped: 0 (0.0%) N N 1

Profile: Default

11:01 PM

< Expression... 1514 58589 → 60696 [ACK] Seq=1 Ack=198 Win=15680 Len=1460 [TCP segment of a reassembled PDU] O 66 58589 \$ 60696 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK\_PERM=1 MS=32 66 60696 + 58589 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1 66 60695 + 3911 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1 54 60696 → 58589 [FIN, ACK] Seq=198 Ack=2783 Win=65536 Len=0 60 58589 → 60696 [ACK] Seq=2783 Ack=199 Win=15680 Len=0 60 58589 + 60696 [FIN, ACK] Seq=2782 Ack=198 Win=15680 Len=6 54 60696 → 58589 [ACK] Seq=198 Ack=2783 Win=65536 Len=0 60 58589 → 60696 [ACK] Seq=1 Ack=198 Win=15680 Len=0 54 60696 → 58589 [ACK] Seq=1 Ack=1 Win=65536 Len=0 80 [ACK] Seq=1 Ack=1 Win=253 Len=1 251 GET /rootDesc.xml HTTP/1.1 1375 HTTP/1.1 200 OK 55 60688 → Length Info Help Go Capture Analyze Statistics Telephony Wireless Tools HTTP/. HTTP 70 TCP 77 P TCP TCP 45 TO 97 10 0 192.168.1.182 128.119.245.12 192.168.8.101 192.168.1.182 192.168.1.182 192.168.1.182 192.168.1.182 192.168.1.182 192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1 30 22:51:25.026891 192.168.1.182 22:51:25.034494 192.168.1.182 2 22:51:16.648469 192.168.1.182 33 22:51:25.034673 192.168.1.182 38 22:51:25.043816 192.168.1.182 39 22:51:25.043940 192.168.1.182 62 22:51:37.202140 192.168.1.182 22:51:25.034382 192.168.1.1 22:51:25.042622 192.168.1.1 22:51:25.043547 192.168.1.1 37 22:51:25.043764 192.168.1.1 36 22:51:25.043764 192.168.1.1 22:51:25.049460 192.168.1.1 Source File Edit View **⊙** □ ■ | lab3.pcapng 35 40 to No.

Frame 30: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

Internet Protocol Version 4, Src: 192.168.1.182, Dst: 192.168.1.1 v Transmission Control Protocol, Src Port: 60696, Dst Port: 58589, Seq: 0, Len: 0

It should be part 30 partier.

Destination Port: 58589 Source Port: 60696

[TCP Segment Len: 0] [Stream index: 1]

Sequence number: 0

[Next sequence number: 0 (relative sequence number)] (relative sequence number) Acknowledgment number: 0

1000 .... = Header Length: 32 bytes (8)

Flags: 0x002 (SYN)

8c c5 a0 c6 08 00 45 00

H]6....E.

Window cita walno. 64240

9899 48 5d 36 a8 f8 d6 90 e1

Ready to load or capture

O Type here to search



8 \*\*



Profile: Default

9/23/2018 ENG 11:01 PM TN 9/23/2018

万米 回

lab3.pcapng

Statistics Telephony Wireless Tools Help — © X		Times   Source   Source   Destination   Protect   Legib Info   10   10   10   10   10   10   10   1
Edit View Go Capture Analyze Statistics Telephony	\ \	No.   Time   Source   Destination   Protocol   Length

Profile: Default

Packets: 1006 · Displayed: 443 (44.0%) · Dropped: 0 (0.0%)

8 \*\*

iū

O Type here to search

Ready to load or capture

н]6....

48 5d 36 a8 f8 d6 00 e1 8c c5 a0 c6 08 00 45 00

ENG 11:01 PM TN 9/23/2018

× 7

し株の

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Iab3.pcapng

	+ < ,	· · · · · · · · · · · · · · · · · · ·
	Length Info  66 68695 + 3911 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1  66 68696 + 58589 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1  66 58589 + 68696 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1  54 68696 + 58589 [ACK] Seq=1 Ack=1 Win=15680 Len=0  251 GET /rootDesc.xml HTTP/1.1  60 58589 + 68696 [ACK] Seq=1 Ack=198 Win=15680 Len=0  1514 58589 + 68696 [ACK] Seq=1 Ack=198 Win=15680 Len=0  154 68696 + 58589 [ACK] Seq=2782 Ack=198 Win=15680 Len=0  54 68696 + 58589 [ACK] Seq=198 Ack=2783 Win=65536 Len=0  54 68696 + 58589 [FIN, ACK] Seq=199 Win=15680 Len=0  55 68688 + 80 [ACK] Seq=1 Ack=199 Win=15680 Len=0  55 68688 + 80 [ACK] Seq=1 Ack=1 Win=253 Len=1	interface 0 5: 30: c6 (00: e1: 8c: c5: a0: c6) Ack: 1, Len: 0  [Ack: 1, Len: 0  [Lus is not the coned well site.
	Protocol TCP	ts) on in selCor_c5:
6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	Destination 192.168.8.101 192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.182 192.168.1.182 192.168.1.182 192.168.1.182 192.168.1.182 192.168.1.182 192.168.1.182 192.168.1.182 192.168.1.182 192.168.1.182	8 bits), 66 bytes captured (528 bits) on 8:d6 (48:5d:36:a8:f8:d6), Dst: IntelCor Crc: 192.168.1.1, Dst: 192.168.1.182 Src Port: 58589, Dst Port: 60696, Seq: 8  ive sequence number) (relative sequence number) (relative ack number) 2 bytes (8)
	Time Source 2 22:51:16.648469 192.168.1.182 30 22:51:25.026891 192.168.1.182 31 22:51:25.034382 192.168.1.182 32 22:51:25.034464 192.168.1.182 33 22:51:25.034673 192.168.1.182 34 22:51:25.043673 192.168.1.1 35 22:51:25.043673 192.168.1.1 36 22:51:25.043764 192.168.1.1 37 22:51:25.043764 192.168.1.1 38 22:51:25.043764 192.168.1.182 39 22:51:25.043840 192.168.1.182 40 22:51:25.043460 192.168.1.182	Frame 31: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0  Ethernet II, Src: Verizon_a8:f8:d6 (48:5d:36:a8:f8:d6), Dst: IntelCor_c5:a0:c6 (00:e1:8c:c5:a0:c6)  Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.182  Vansmission Control Protocol, Src Port: 58589, Dst Port: 60696, Seq: 0, Ack: 1, Len: 0  Source Port: 58589  Destination Port: 60696  [Stream index: 1]  [TCP Segment Len: 0]  Sequence number: 0 (relative sequence number)  [Next sequence number: 0 (relative sequence number)]  Acknowledgment number: 1 (relative ack number)  1000 = Header Length: 32 bytes (8)  Flags: 0x012 (SYN, ACK)  Window, city willow, 14600
+-	. No.	> Fram

Profile: Default

Packets: 1006 · Displayed: 443 (44.0%) · Dropped: 0 (0.0%)

8 \*\*

jiit

O Type here to search

Ready to load or capture

(€ € €NG 11:05 PM TN 9/23/2018

0 354 GET /upnphost/udhisapi.dll?content=uuid:375c0d92-5f90-41f6-a23a-fd9f917d6d65 HTTP/1.1 1472 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain) Thats concel - That is the 18 of the webpergo. 831 HTTP/1.1 200 OK (text/html) 251 GET /rootDesc.xml HTTP/1.1 1114 HTTP/1.1 200 OK 1375 HTTP/1.1 200 OK Length Info HTTP/... HTTP/\_\_ Tools HTTP HTTP HTTP Capture Analyze Statistics Telephony Wireless **® © ©** 128.119.245.12 192.168.1.182 192.168.1.154 192.168.1.182 192.168.1.182 192.168.1.1 \* \* \* \* \* × × × 984 22:54:05.746653 128.119.245.12 715 22:53:53.090781 192.168.1.182 718 22:53:53.115085 192.168.1.154 934 22:54:05.717463 192.168.1.182 33 22:51:25.034673 192.168.1.182 36 22:51:25.043764 192.168.1.1 Source 9 File Edit View • | lab3.pcapng 77 http

> Ethernet II, Src: IntelCor\_c5:a0:c6 (00:e1:8c:c5:a0:c6), Dstí Verizon\_a8:f8:d6 (48:5d:36:a8:f8:d6) Frame 934: 1472 bytes on wire (11776 bits), 1472 bytes capturgd (11776 bits) on interface 0

 Transmission Control Protocol, Src Port: 60708, Dst Port: 80, Seq: 151555, Ack: 1, Len: 1418 Internet Protocol Version 4, Src: 192.168.1.182, Dst; 128.119.245.12

Source Port: 60708

Destination Port: 80

[TCP Segment Len: 1418] [Stream index: 24]

(relative sequence number) Sequence number: 151565

[Next sequence number: 152983 (relative sequence number)] (relative ack number) Acknowledgment number: 1

0101 .... = Header Length: 20 bytes (5) V Flage . AVAIR (DCH ACK)

Frame (1472 bytes) Reassembled TCP (152982 bytes)

Whertext Transfer Protocol: Protocol O Type here to search



Packets: 1006 · Displayed: 6 (0.6%) · Dropped: 0 (0.0%)

Profile: Default

11:12 PM

- wreet 1P.

```
No.
         Time
                            Source
                                                 Destination
                                                                      Protocol Length Info
      934 22:54:05.717463
                           192.168.1.182
                                                 128.119.245.12
                                                                      HTTP
                                                                              1472 POST /wireshark-labs/lab3-1-reply.htm HTTP,
  1.1 (text/plain)
  Frame 934: 1472 bytes on wire (11776 bits), 1472 bytes captured (11776 bits) on interface 0
  Ethernet II, Src: IntelCor_c5:a0:c6 (00:e1:8c:c5:a0:c6), Dst: Verizon_a8:f8:d6 (48:5d:36:a8:f8:d6)
 Internet Protocol Version 4, Src: 192.168.1.182, Dst: 128.119.245.12
 Transmission Control Protocol, Src Port: 60708, Dst Port: 80, Seq: 151565, Ack: 1, Len: 1418
     Source Port: 60708
     Destination Port: 80
     [Stream index: 24]
     [TCP Segment Len: 1418]
     Sequence number: 151565
                               (relative sequence number)
     [Next sequence number: 152983 (relative sequence number)]
     Acknowledgment number: 1
                               (relative ack number)
     0101 .... = Header Length: 20 bytes (5)
     Flags: 0x018 (PSH, ACK)
         000. .... = Reserved: Not set
         ...0 .... = Nonce: Not set
         .... \theta.... = Congestion Window Reduced (CWR): Not set
         .... .0.. .... = ECN-Echo: Not set
         .... ..0. .... = Urgent: Not set
         .... = Acknowledgment: Set
         .... 1... = Push: Set
         .... .0.. = Reset: Not set
         .... .... ..0. = Syn: Not set
         ···· Not set
         [TCP Flags: .....AP...]
     Window size value: 256
     [Calculated window size: 65536]
     [Window size scaling factor: 256]
     Checksum: 0xb4a1 [unverified]
     [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
        [iRTT: 0.022808000 seconds]
        [Bytes in flight: 75740]
        [Bytes sent since last PSH flag: 4338]
    [Timestamps]
    TCP payload (1418 bytes)
    TCP segment data (1418 bytes)
[107 Reassembled TCP Segments (152982 bytes): #772(661), #773(1460), #774(1460), #775(1460), #776(1460), #777(1460), #777(1460),
#779(1460), #780(1460), #781(1460), #785(1460), #787(1460), #788(1460), #790(1460), #791(1460), #793(1460), #79]
Hypertext Transfer Protocol
    POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Content-Length: 152321\r\n
    Cache-Control: max-age=0\r\n
    Origin: http://gaia.cs.umass.edu\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Content-Type: multipart/form-data; boundary=----WebKitFormBoundary14TsKLQ9uBqnBBkH\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/
537.36\r\n
    Referer: http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/lab3-1-reply.htm]
    [HTTP request 1/1]
    [Response in frame: 984]
    File Data: 152321 bytes
MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "----WebKitFormBoundary14TsKLQ9uBqnBBkH"
```

```
No.
          Time
                             Source
                                                   Destination
      984 22:54:05.746653
                                                                         Protocol Length Info
                            128.119.245.12
                                                   192.168.1.182
 Frame 984: 831 bytes on wire (6648 bits), 831 bytes captured (6648 bits) on interface 0
                                                                                        HTTP/1.1 200 OK (text/html)
 Ethernet II, Src: Verizon_a8:f8:d6 (48:5d:36:a8:f8:d6), Dst: IntelCor_c5:a0:c6 (00:e1:8c:c5:a0:c6)
 Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.182
 Transmission Control Protocol, Src Port: 80, Dst Port: 60708, Seq: 1, Ack: 152983, Len: 777
     Source Port: 80
     Destination Port: 60708
     [Stream index: 24]
     [TCP Segment Len: 777]
     Sequence number: 1 (relative sequence number)
     [Next sequence number: 778 (relative sequence number)]
Acknowledgment number: 152983 (relative ack number)
     0101 .... = Header Length: 20 bytes (5)
     Flags: 0x018 (PSH, ACK)
         000. .... = Reserved: Not set
         ...0 .... = Nonce: Not set
         .... 0... = Congestion Window Reduced (CWR): Not set
         .... .0.. .... = ECN-Echo: Not set
         .... ..0. .... = Urgent: Not set
         .... = Acknowledgment: Set
         .... 1... = Push: Set
         .... .0.. = Reset: Not set
         .... .... ..0. = Syn: Not set
         .... Not set
        [TCP Flags: ·····AP···]
    Window size value: 2093
     [Calculated window size: 267904]
     [Window size scaling factor: 128]
    Checksum: 0xccfd [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
        [iRTT: 0.022808000 seconds]
        [Bytes in flight: 777]
        [Bytes sent since last PSH flag: 777]
    [Timestamps]
    TCP payload (777 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Mon, 24 Sep 2018 02:54:06 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sat, 23 Oct 2010 11:38:58 GMT\r\n
    ETag: "1a2-4934734677880"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 418\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    [HTTP response 1/1]
    [Time since request: 0.029190000 seconds]
    [Request in frame: 934]
    File Data: 418 bytes
Line-based text data: text/html (11 lines)
```