ENSF 462 Networked Systems

Lab 01 – Wireshark Lab and Socket Programming

Macayla Konig
30122680

Part I – Wireshark Lab

1. The protocols TCP and HTTP are shown as appearing in the trace file.

2. The time it took from when the HTTP GET message was sent until the HTTP OK reply was received was 0.070486 seconds.

   Frame 30 time: 8.340199s
   Frame 32 time: 8.410685s

   8.410685s – 8.340199s = 0.070486s

3. The Internet address of the gaia.cs.umass.edu is 128.119.245.12. The Internet address of the computer that sent the HTTP GET message is 10.13.99.93.

4. The Web browser type, Safari, issued the HTTP request.

5. The destination port number to which this HTTP request is being sent is 80.

6. If you enter the URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html multiple times during Wireshark packet capture, there are no differences in the sent HTTP message and the received HTTP reply.

/var/folders/1l/7bty1qvd44gdjyllffd6yg180000gn/T/wireshark_Wi-FiHZ25A2.pcapng 97 total packets, 4 shown

```
No.     Time           Source                Destination           Protocol
Length Info
     30 8.340199       10.13.99.93           128.119.245.12        HTTP
473    GET /wireshark-
labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 30: 473 bytes on wire (3784 bits), 473 bytes captured (3784 bits) on
interface en0, id 0
    Section number: 1
    Interface id: 0 (en0)
        Interface name: en0
        Interface description: Wi-Fi
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 20, 2023 17:58:25.412454000 MDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1695254305.412454000 seconds
    [Time delta from previous captured frame: 0.000175000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 8.340199000 seconds]
    Frame Number: 30
    Frame Length: 473 bytes (3784 bits)
    Capture Length: 473 bytes (3784 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Apple_7a:83:4e (1c:57:dc:7a:83:4e), Dst: Cisco_94:75:1f
(6c:8b:d3:94:75:1f)
    Destination: Cisco_94:75:1f (6c:8b:d3:94:75:1f)
        Address: Cisco_94:75:1f (6c:8b:d3:94:75:1f)
        .... ..0. .... .... .... .... = LG bit: Globally unique address
(factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Apple_7a:83:4e (1c:57:dc:7a:83:4e)
        Address: Apple_7a:83:4e (1c:57:dc:7a:83:4e)
        .... ..0. .... .... .... .... = LG bit: Globally unique address
(factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.13.99.93, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x02 (DSCP: CS0, ECN: ECT(0))
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..10 = Explicit Congestion Notification: ECN-Capable Transport
codepoint '10' (2)
    Total Length: 459
    Identification: 0x0000 (0)
    010. .... = Flags: 0x2, Don't fragment
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
```

```
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x563d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.13.99.93
    Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 53082, Dst Port: 80, Seq: 1, Ack: 1,
Len: 419
    Source Port: 53082
    Destination Port: 80
    [Stream index: 2]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 419]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 841450121
    [Next Sequence Number: 420    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
```

/var/folders/1l/7bty1qvd44gdjyllffd6yg180000gn/T/wireshark_Wi-FiHZ25A2.pcapng 97 total packets, 4 shown

```
    Acknowledgment number (raw): 2314854984
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Accurate ECN: Not set
        .... 0... .... = Congestion Window Reduced: Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·······AP···]
    Window: 4096
    [Calculated window size: 262144]
    [Window size scaling factor: 64]
    Checksum: 0xf818 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
        [Time since first frame in this TCP stream: 0.068074000 seconds]
        [Time since previous frame in this TCP stream: 0.000175000 seconds]
    [SEQ/ACK analysis]
        [iRTT: 0.067899000 seconds]
        [Bytes in flight: 419]
        [Bytes sent since last PSH flag: 419]
    TCP payload (419 bytes)
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1\r\n]
            [GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
```

```
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /wireshark-labs/INTRO-wireshark-file1.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/605.1.15 (KHTML, like
Gecko) Version/16.3 Safari/605.1.15\r\n
    Accept-Language: en-CA,en-US;q=0.9,en;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-
wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 32]

No.

   Time           Source                Destination           Protocol Length
Info
32 8.410685       128.119.245.12        10.13.99.93           HTTP     492
HTTP/1.1 200 OK
(text/html)
Frame 32: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on
interface en0, id 0
    Section number: 1
    Interface id: 0 (en0)
        Interface name: en0
        Interface description: Wi-Fi
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 20, 2023 17:58:25.482940000 MDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1695254305.482940000 seconds
    [Time delta from previous captured frame: 0.000569000 seconds]
```

/var/folders/1l/7bty1qvd44gdjyllffd6yg180000gn/T/wireshark_Wi-FiHZ25A2.pcapng 97 total packets, 4 shown

```
    [Time delta from previous displayed frame: 0.070486000 seconds]
    [Time since reference or first frame: 8.410685000 seconds]
    Frame Number: 32
    Frame Length: 492 bytes (3936 bits)
    Capture Length: 492 bytes (3936 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
```

```
Ethernet II, Src: Cisco_94:75:1f (6c:8b:d3:94:75:1f), Dst: Apple_7a:83:4e
(1c:57:dc:7a:83:4e)
    Destination: Apple_7a:83:4e (1c:57:dc:7a:83:4e)
        Address: Apple_7a:83:4e (1c:57:dc:7a:83:4e)
        .... ..0. .... .... .... .... = LG bit: Globally unique address
(factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Cisco_94:75:1f (6c:8b:d3:94:75:1f)
        Address: Cisco_94:75:1f (6c:8b:d3:94:75:1f)
        .... ..0. .... .... .... .... = LG bit: Globally unique address
(factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.13.99.93
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x02 (DSCP: CS0, ECN: ECT(0))
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..10 = Explicit Congestion Notification: ECN-Capable Transport
codepoint '10' (2)
    Total Length: 478
    Identification: 0x8bee (35822)
    010. .... = Flags: 0x2, Don't fragment
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 32
    Protocol: TCP (6)
    Header Checksum: 0xea3b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.119.245.12
    Destination Address: 10.13.99.93
Transmission Control Protocol, Src Port: 80, Dst Port: 53082, Seq: 1, Ack:
420, Len: 438
    Source Port: 80
    Destination Port: 53082
    [Stream index: 2]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 438]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2314854984
    [Next Sequence Number: 439    (relative sequence number)]
    Acknowledgment Number: 420    (relative ack number)
    Acknowledgment number (raw): 841450540
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Accurate ECN: Not set
        .... 0... .... = Congestion Window Reduced: Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
```

```
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
```

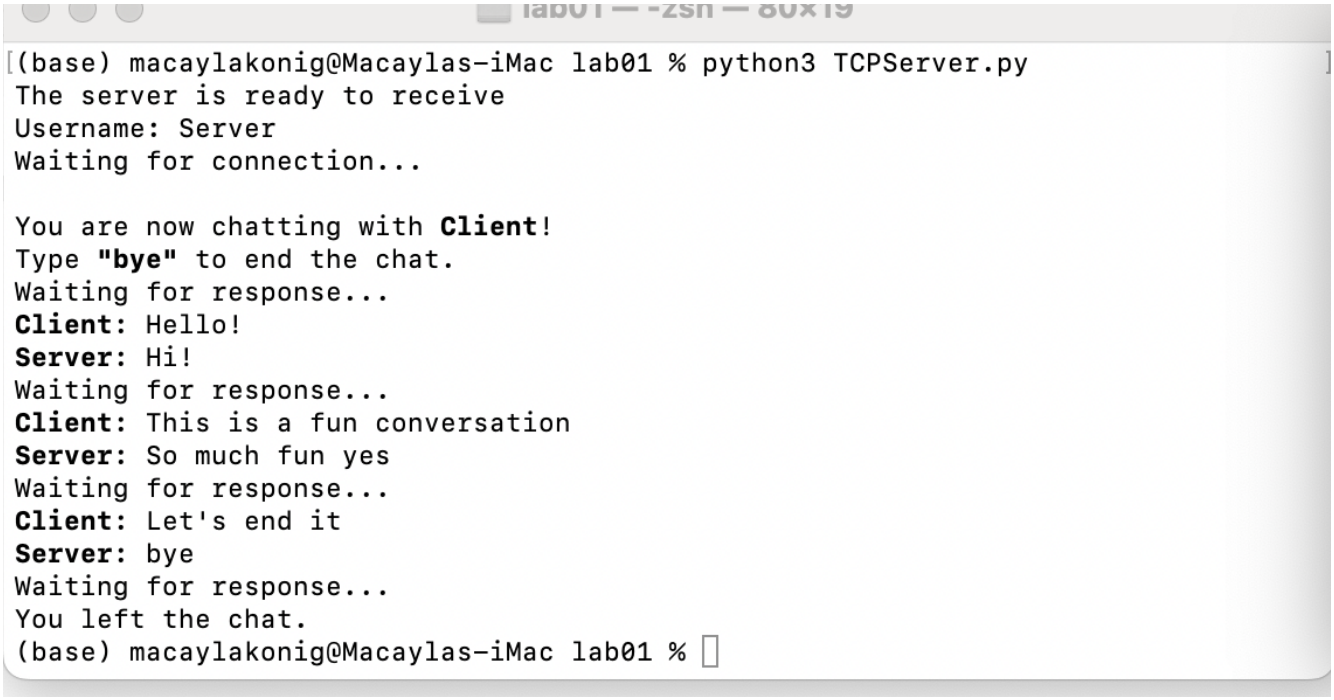
/var/folders/1l/7bty1qvd44gdjyllffd6yg180000gn/T/wireshark_Wi-FiHZ25A2.pcapng 97 total packets, 4 shown

```
        [TCP Flags: ·······AP···]
    Window: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0x351c [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
        [Time since first frame in this TCP stream: 0.138560000 seconds]
        [Time since previous frame in this TCP stream: 0.000569000 seconds]
    [SEQ/ACK analysis]
        [iRTT: 0.067899000 seconds]
        [Bytes in flight: 438]
        [Bytes sent since last PSH flag: 438]
    TCP payload (438 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Wed, 20 Sep 2023 23:58:25 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: Wed, 20 Sep 2023 05:59:02 GMT\r\n
    ETag: "51-605c4127aa6f9"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\r\n
        [Content length: 81]
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.070486000 seconds]
    [Request in frame: 30]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-
file1.html]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
    <html>\n
    Congratulations!  You've downloaded the first Wireshark lab file!\n
    </html>\n
```

Part II – Socket Programming

```python
# TCPServer.py

from socket import *
serverPort = 12000
serverSocket = socket(AF_INET, SOCK_STREAM)

serverSocket.bind(('',serverPort))
serverSocket.listen(1)
print('The server is ready to receive')

user2 = input('Username: ')

while True:
    print("Waiting for connection...")
    connectionSocket, addr = serverSocket.accept()

    user1 = connectionSocket.recv(1024).decode()
    connectionSocket.send(user2.encode())

    print('You are now chatting with', '\033[1m' + user1 + '\033[0m' + '!')
    print('Type \033[1mbye\033[0m to end the chat.')

    while True:
        message = connectionSocket.recv(1024).decode()
        print('\033[1m' + user1 + '\033[0m: ' + message)

        if message == 'bye':
            print(user1 + ' left the chat.')
            break

        reply_message = input('\033[1m' + user2 + '\033[0m: ')
        connectionSocket.send(reply_message.encode())

        if reply_message == 'bye':
            print('You left the chat.')
            break

    connectionSocket.close()
    break

serverSocket.close()
```

```python
# TCPClient.py

from socket import *
serverName = "localhost"
serverPort = 12000
clientSocket = socket(AF_INET, SOCK_STREAM)

print("Connecting to server...")
clientSocket.connect((serverName,serverPort))
print("Connected to server!")

user1 = input('Username: ')
clientSocket.send(user1.encode())

user2 = clientSocket.recv(1024).decode()
print('You are now chatting with', '\033[1m' + user2 + '!\033[0m')
print('Type \033[1mbye\033[0m to end the chat.')

while True:
    message = input('\033[1m' + user1 + '\033[0m: ')
    clientSocket.send(message.encode())

    if message == 'bye':
        print('You ended the chat')
        break

    print("Waiting for response...")
    recieved_message = clientSocket.recv(1024).decode()
    print('\033[1m' + user2 + '\033[0m: ' + recieved_message)

    if message == 'bye':
        print(user2 + ' left the chat')
        break

clientSocket.close()
```


(base) macaylakonig@Macaylas-iMac lab01 % python3 TCPServer.py
The server is ready to receive
Username: Server
Waiting for connection...
You are now chatting with Client!
Type "bye" to end the chat.
Waiting for response...
Client: Hello!
Server: Hi!
Waiting for response...
Client: This is a fun conversation
Server: So much fun yes
Waiting for response...
Client: Let's end it
Server: bye
Waiting for response...
You left the chat.
(base) macaylakonig@Macaylas-iMac lab01 %


lab01 — -zsh — 80×18
(base) macaylakonig@Macaylas-iMac lab01 % python3 TCPClient.py
Connecting to server...
Connected to server!
Username: Client
You are now chatting with Server!
Type "bye" to end the chat.
Client: Hello!
Waiting for response...
Server: Hi!
Client: This is a fun conversation
Waiting for response...
Server: So much fun yes
Client: Let's end it
Waiting for response...
Server: bye
Server left the chat
(base) macaylakonig@Macaylas-iMac lab01 %