Lab 1

Objectives:

1. Install VM
2. Understand packet capture, filter them, inspect them using wireshark and pyshark
3. Understand CIA Triad

Task1. Install and run Wireshark on ubuntu machine.

(a) Update apt: sudo apt update

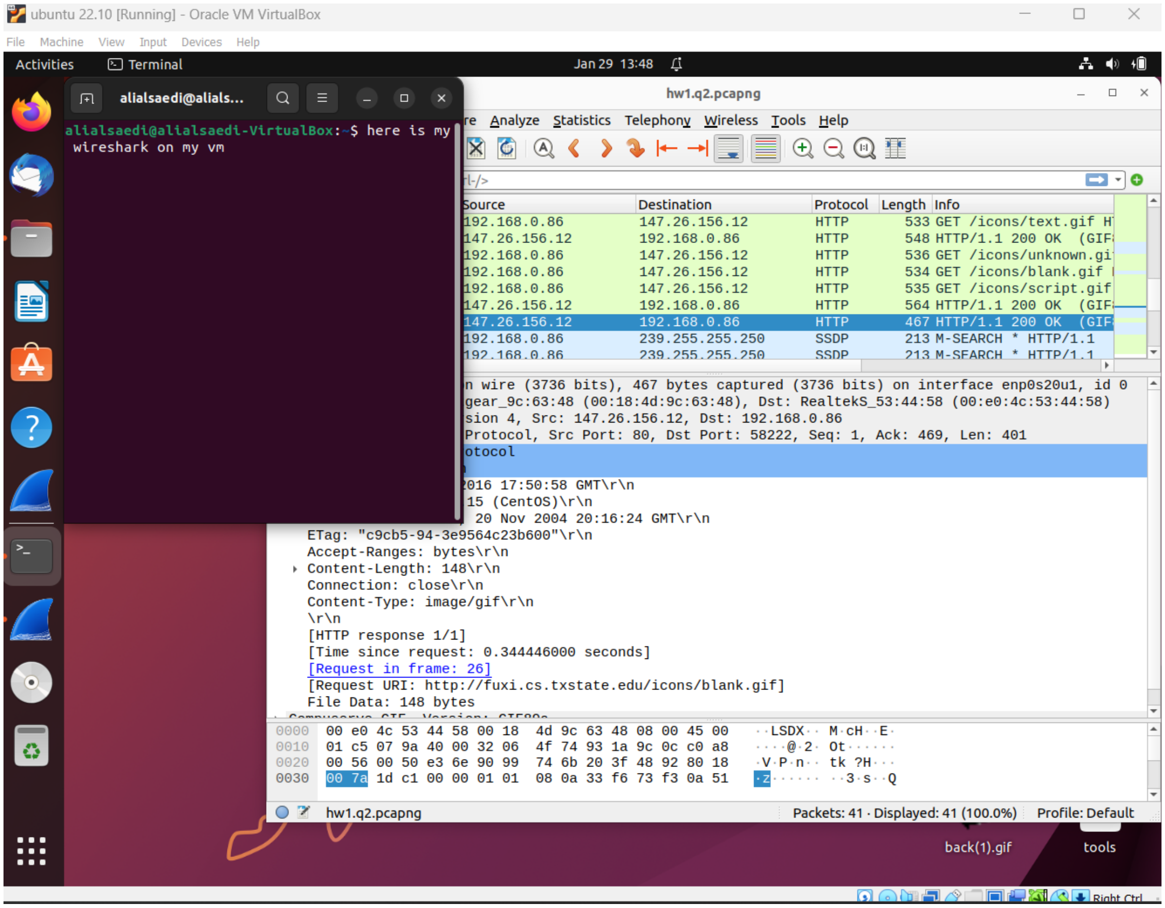
(b) Upgrade apt: sudo apt upgrade

(c) Install wireshark: sudo apt install wireshark

(d) Enable root privileges: When Wireshark installs on your system, you will be prompted by a window, as Wireshark requires superuser/root privileges to operate, this option asks to enable or disable permissions for all every user on the system. Press the “Yes” button to allow other users, or press the “No” button to restrict other users from using Wireshark.

(e) Reconfigure permission settings:
sudo dpkg-reconfigure wireshark-common
Select Yes
sudo usermod -a -G wireshark
reboot

(f) Launch wireshark


ubuntu 22.10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Jan 29 13:48
alialsaedi@alials...
hw1.q2.pcapng
re Analyze Statistics Telephony Wireless Tools Help
back(1).gif
tools
Right Ctrl

```
alialsaedi@alialsaedi-VirtualBox:~$ here is my
 wireshark on my vm
```

```
Source          Destination      Protocol  Length Info
192.168.0.86    147.26.156.12    HTTP         533 GET /icons/text.gif H
147.26.156.12   192.168.0.86     HTTP         548 HTTP/1.1 200 OK  (GIF
192.168.0.86    147.26.156.12    HTTP         536 GET /icons/unknown.gi
192.168.0.86    147.26.156.12    HTTP         534 GET /icons/blank.gif
192.168.0.86    147.26.156.12    HTTP         535 GET /icons/script.gif
147.26.156.12   192.168.0.86     HTTP         564 HTTP/1.1 200 OK  (GIF
147.26.156.12   192.168.0.86     HTTP         467 HTTP/1.1 200 OK  (GIF
192.168.0.86    239.255.255.250  SSDP         213 M-SEARCH * HTTP/1.1
192.168.0.86    239.255.255.250  SSDP         213 M-SEARCH * HTTP/1.1
```

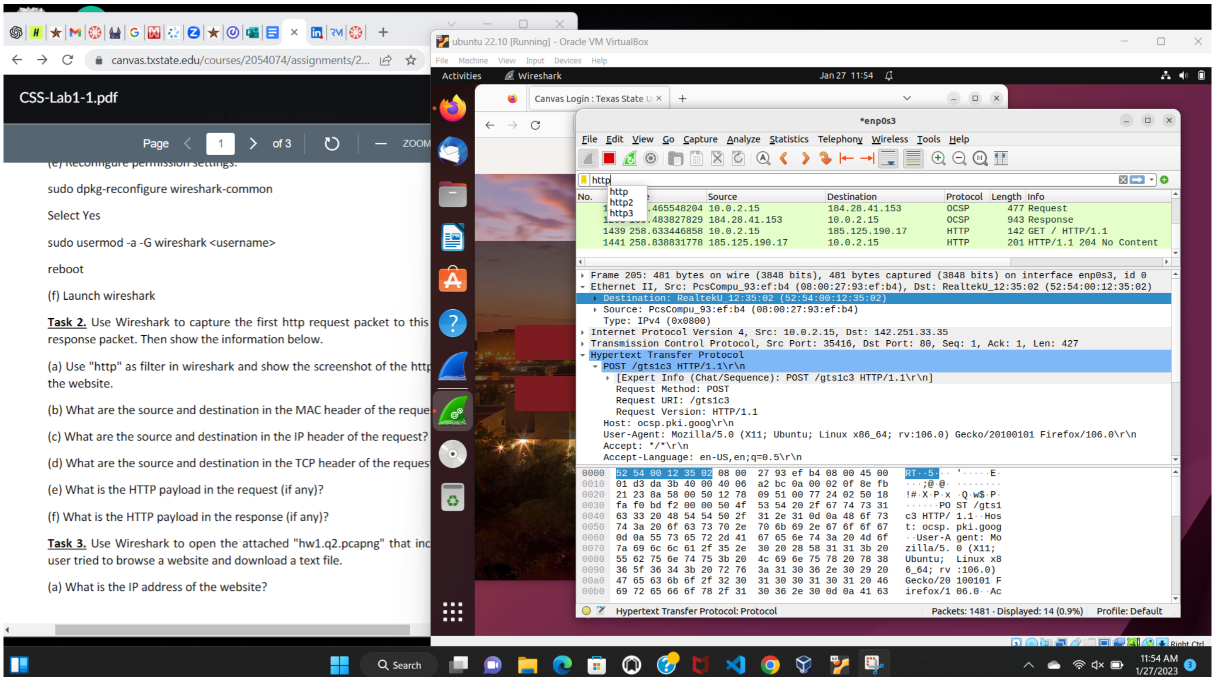
```
n wire (3736 bits), 467 bytes captured (3736 bits) on interface enp0s20u1, id 0
gear_9c:63:48 (00:18:4d:9c:63:48), Dst: RealtekS_53:44:58 (00:e0:4c:53:44:58)
sion 4, Src: 147.26.156.12, Dst: 192.168.0.86
Protocol, Src Port: 80, Dst Port: 58222, Seq: 1, Ack: 469, Len: 401
otocol
2016 17:50:58 GMT\r\n
15 (CentOS)\r\n
 20 Nov 2004 20:16:24 GMT\r\n
    ETag: "c9cb5-94-3e9564c23b600"\r\n
    Accept-Ranges: bytes\r\n
  ▸ Content-Length: 148\r\n
    Connection: close\r\n
    Content-Type: image/gif\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.344446000 seconds]
    [Request in frame: 26]
    [Request URI: http://fuxi.cs.txstate.edu/icons/blank.gif]
    File Data: 148 bytes
```

```
0000  00 e0 4c 53 44 58 00 18  4d 9c 63 48 08 00 45 00   ··LSDX·· M·cH··E·
0010  01 c5 07 9a 40 00 32 06  4f 74 93 1a 9c 0c c0 a8   ····@·2· Ot······
0020  00 56 00 50 e3 6e 90 99  74 6b 20 3f 48 92 80 18   ·V·P·n·· tk ?H···
0030  00 7a 1d c1 00 00 01 01  08 0a 33 f6 73 f3 0a 51   ·z······ ··3·s··Q
```

hw1.q2.pcapng   Packets: 41 · Displayed: 41 (100.0%)   Profile: Default

Task 2. Use Wireshark to capture the first http request packet to this website and the following http response packet. Then show the information below.

(a) Use "http" as a filter in wireshark and show the screenshot of the http request packet when browsing the website.



CSS-Lab1-1.pdf

(e) Reconfigure permission settings.

sudo dpkg-reconfigure wireshark-common

Select Yes

sudo usermod -a -G wireshark <username>

reboot

(f) Launch wireshark

Task 2. Use Wireshark to capture the first http request packet to this
response packet. Then show the information below.

(a) Use "http" as filter in wireshark and show the screenshot of the http
the website.

(b) What are the source and destination in the MAC header of the reque

(c) What are the source and destination in the IP header of the request?

(d) What are the source and destination in the TCP header of the reques

(e) What is the HTTP payload in the request (if any)?

(f) What is the HTTP payload in the response (if any)?

Task 3. Use Wireshark to open the attached "hw1.q2.pcapng" that inc
user tried to browse a website and download a text file.

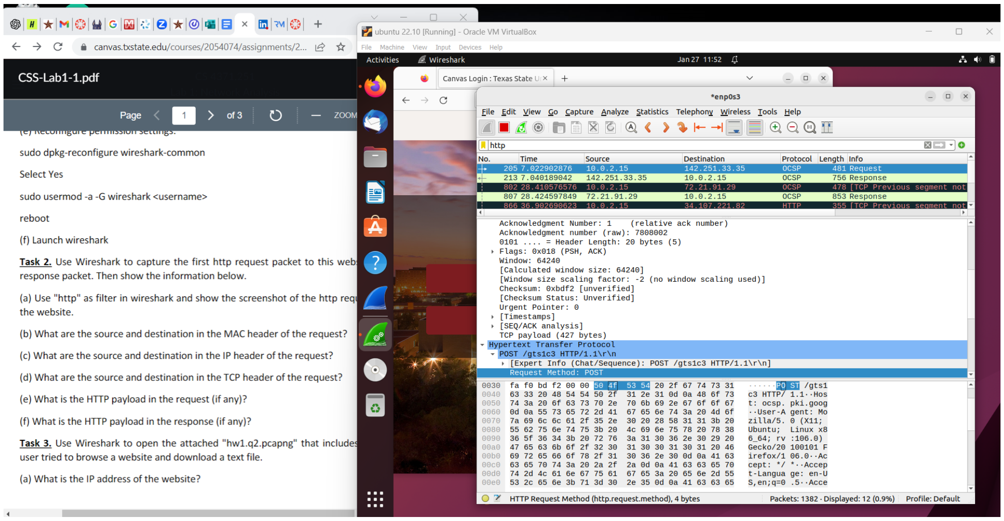
(a) What is the IP address of the website?

```
http

No.                   Source          Destination     Protocol Length Info
1   .465548204        10.0.2.15       184.28.41.153   OCSP     477 Request
1   .483827829        184.28.41.153   10.0.2.15       OCSP     943 Response
1439 258.633446858    10.0.2.15       185.125.190.17  HTTP     142 GET / HTTP/1.1
1441 258.838831778    185.125.190.17  10.0.2.15       HTTP     201 HTTP/1.1 204 No Content

Frame 205: 481 bytes on wire (3848 bits), 481 bytes captured (3848 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_93:ef:b4 (08:00:27:93:ef:b4), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
  Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
  Source: PcsCompu_93:ef:b4 (08:00:27:93:ef:b4)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.251.33.35
Transmission Control Protocol, Src Port: 35416, Dst Port: 80, Seq: 1, Ack: 1, Len: 427
Hypertext Transfer Protocol
  POST /gts1c3 HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): POST /gts1c3 HTTP/1.1\r\n]
    Request Method: POST
    Request URI: /gts1c3
    Request Version: HTTP/1.1
  Host: ocsp.pki.goog\r\n
  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:106.0) Gecko/20100101 Firefox/106.0\r\n
  Accept: */*\r\n
  Accept-Language: en-US,en;q=0.5\r\n

0000  52 54 00 12 35 02 08 00  27 93 ef b4 08 00 45 00   RT··5··· '·····E·
0010  01 d3 da 3b 40 00 40 06  a2 bc 0a 00 02 0f 8e fb   ···;@·@· ········
0020  21 23 8a 58 00 50 12 78  09 51 00 77 24 02 50 18   !#·X·P·x ·Q·w$·P·
0030  fa f0 bd f2 00 00 50 4f  53 54 20 2f 67 74 73 31   ······PO ST /gts1
0040  63 33 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73   c3 HTTP/ 1.1··Hos
0050  74 3a 20 6f 63 73 70 2e  70 6b 69 2e 67 6f 6f 67   t: ocsp. pki.goog
0060  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 4d 6f   ··User-A gent: Mo
0070  7a 69 6c 6c 61 2f 35 2e  30 20 28 58 31 31 3b 20   zilla/5. 0 (X11;
0080  55 62 75 6e 74 75 3b 20  4c 69 6e 75 78 20 78 38   Ubuntu;  Linux x8
0090  36 5f 36 34 3b 20 72 76  3a 31 30 36 2e 30 29 20   6_64; rv :106.0)
00a0  47 65 63 6b 6f 2f 32 30  31 30 30 31 30 31 20 46   Gecko/20 100101 F
00b0  69 72 65 66 6f 78 2f 31  30 36 2e 30 0d 0a 41 63   irefox/1 06.0··Ac

Hypertext Transfer Protocol: Protocol    Packets: 1481 · Displayed: 14 (0.9%)    Profile: Default
```

ubuntu 22.10 [Running] - Oracle VM VirtualBox
Activities
Wireshark
Jan 27 11:54
Canvas Login : Texas State U
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http2
http3
canvas.txstate.edu/courses/2054074/assignments/2...
Page 1 of 3
ZOOM
Search
11:54 AM
1/27/2023
Right Ctrl

(b) What are the source and destination in the MAC header of the request?
source: (08:00:27:93:ef:b4)   Destination: (52:54:00:12:35:02)

(c) What are the source and destination in the IP header of the request?
Source: 10.0.2.25   Destination: 35.223.170.84



CSS-Lab1-1.pdf

(e) Reconfigure permission settings.

sudo dpkg-reconfigure wireshark-common

Select Yes

sudo usermod -a -G wireshark <username>

reboot

(f) Launch wireshark

Task 2. Use Wireshark to capture the first http request packet to this web
response packet. Then show the information below.

(a) Use "http" as filter in wireshark and show the screenshot of the http requ
the website.

(b) What are the source and destination in the MAC header of the request?

(c) What are the source and destination in the IP header of the request?

(d) What are the source and destination in the TCP header of the request?

(e) What is the HTTP payload in the request (if any)?

(f) What is the HTTP payload in the response (if any)?

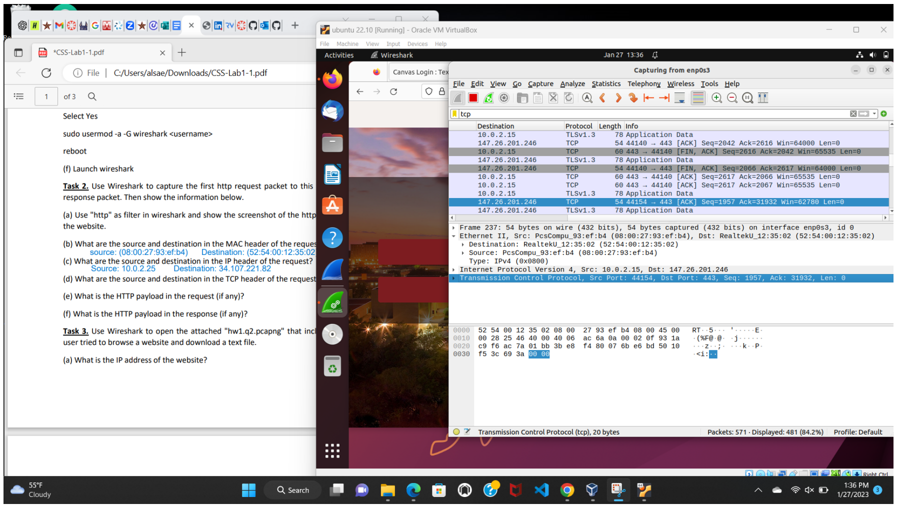
Task 3. Use Wireshark to open the attached "hw1.q2.pcapng" that include
user tried to browse a website and download a text file.

(a) What is the IP address of the website?

```
http

No.  Time          Source          Destination     Protocol Length Info
205  7.022902876   10.0.2.15       142.251.33.35   OCSP     481 Request
213  7.040189042   142.251.33.35   10.0.2.15       OCSP     756 Response
802  28.410576576  10.0.2.15       72.21.91.29     OCSP     478 [TCP Previous segment not
807  28.424597849  72.21.91.29     10.0.2.15       OCSP     853 Response
866  36.902690623  10.0.2.15       34.107.221.82   HTTP     355 [TCP Previous segment not

    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 7808002
    0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
    Window: 64240
    [Calculated window size: 64240]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0xbdf2 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  [Timestamps]
  [SEQ/ACK analysis]
    TCP payload (427 bytes)
Hypertext Transfer Protocol
  POST /gts1c3 HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): POST /gts1c3 HTTP/1.1\r\n]
    Request Method: POST

0030  fa f0 bd f2 00 00 50 4f  53 54 20 2f 67 74 73 31   ······PO ST /gts1
0040  63 33 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73   c3 HTTP/ 1.1··Hos
0050  74 3a 20 6f 63 73 70 2e  70 6b 69 2e 67 6f 6f 67   t: ocsp. pki.goog
0060  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 4d 6f   ··User-A gent: Mo
0070  7a 69 6c 6c 61 2f 35 2e  30 20 28 58 31 31 3b 20   zilla/5. 0 (X11;
0080  55 62 75 6e 74 75 3b 20  4c 69 6e 75 78 20 78 38   Ubuntu;  Linux x8
0090  36 5f 36 34 3b 20 72 76  3a 31 30 36 2e 30 29 20   6_64; rv :106.0)
00a0  47 65 63 6b 6f 2f 32 30  31 30 30 31 30 31 20 46   Gecko/20 100101 F
00b0  69 72 65 66 6f 78 2f 31  30 36 2e 30 0d 0a 41 63   irefox/1 06.0··Ac
00c0  63 65 70 74 3a 20 2a 2f  2a 0d 0a 41 63 63 65 70   cept: */ *··Accep
00d0  74 2d 4c 61 6e 67 75 61  67 65 3a 20 65 6e 2d 55   t-Langua ge: en-U
00e0  53 2c 65 6e 3b 71 3d 30  2e 35 0d 0a 41 63 63 65   S,en;q=0 .5··Acce

HTTP Request Method (http.request.method), 4 bytes    Packets: 1382 · Displayed: 12 (0.9%)    Profile: Default
```

ubuntu 22.10 [Running] - Oracle VM VirtualBox
Activities
Wireshark
Jan 27 11:52
Canvas Login : Texas State U
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
canvas.txstate.edu/courses/2054074/assignments/2...
Page 1 of 3
ZOOM

(d) What are the source and destination in the TCP header of the request?
source port: 56334   destination Port: 80



*CSS-Lab1-1.pdf

C:/Users/alsae/Downloads/CSS-Lab1-1.pdf

1 of 3

Select Yes

sudo usermod -a -G wireshark <username>

reboot

(f) Launch wireshark

Task 2. Use Wireshark to capture the first http request packet to this response packet. Then show the information below.

(a) Use "http" as filter in wireshark and show the screenshot of the http the website.

(b) What are the source and destination in the MAC header of the reques

source: (08:00:27:93:ef:b4) Destination: (52:54:00:12:35:02

(c) What are the source and destination in the IP header of the request?

Source: 10.0.2.25 Destination: 34.107.221.82

(d) What are the source and destination in the TCP header of the request

(e) What is the HTTP payload in the request (if any)?

(f) What is the HTTP payload in the response (if any)?

Task 3. Use Wireshark to open the attached "hw1.q2.pcapng" that incl user tried to browse a website and download a text file.

(a) What is the IP address of the website?

ubuntu 22.10 [Running] - Oracle VM VirtualBox

Jan 27 13:36

Capturing from enp0s3

Filter: tcp

```
Destination      Protocol  Length Info
10.0.2.15        TLSv1.3   78 Application Data
147.26.201.246   TCP       54 44140 → 443 [ACK] Seq=2042 Ack=2616 Win=64000 Len=0
10.0.2.15        TCP       60 443 → 44140 [FIN, ACK] Seq=2616 Ack=2042 Win=65535 Len=0
147.26.201.246   TLSv1.3   78 Application Data
147.26.201.246   TCP       54 44140 → 443 [FIN, ACK] Seq=2066 Ack=2617 Win=64000 Len=0
10.0.2.15        TCP       60 443 → 44140 [ACK] Seq=2617 Ack=2066 Win=65535 Len=0
10.0.2.15        TCP       60 443 → 44140 [ACK] Seq=2617 Ack=2067 Win=65535 Len=0
10.0.2.15        TLSv1.3   78 Application Data
147.26.201.246   TCP       54 44154 → 443 [ACK] Seq=1957 Ack=31932 Win=62780 Len=0
147.26.201.246   TLSv1.3   78 Application Data
```

```
▸ Frame 237: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface enp0s3, id 0
▾ Ethernet II, Src: PcsCompu_93:ef:b4 (08:00:27:93:ef:b4), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
  ▸ Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
  ▸ Source: PcsCompu_93:ef:b4 (08:00:27:93:ef:b4)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 147.26.201.246
▸ Transmission Control Protocol, Src Port: 44154, Dst Port: 443, Seq: 1957, Ack: 31932, Len: 0
```

```
0000  52 54 00 12 35 02 08 00  27 93 ef b4 08 00 45 00   RT··5···  '·····E·
0010  00 28 25 46 40 00 40 06  ac 6a 0a 00 02 0f 93 1a   ·(%F@·@·  ·j······
0020  c9 f6 ac 7a 01 bb 3b e8  f4 80 07 6b e6 bd 50 10   ···z··;·  ···k··P·
0030  f5 3c 69 3a 00 00                                  ·<i:··
```

Transmission Control Protocol (tcp), 20 bytes | Packets: 571 · Displayed: 481 (84.2%) | Profile: Default

55°F Cloudy

1:36 PM 1/27/2023

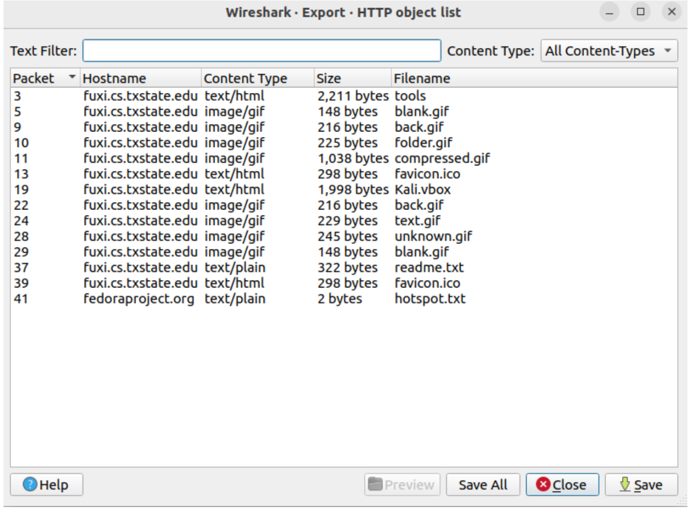
(e) What is the HTTP payload in the request (if any)?
88 bytes

(f) What is the HTTP payload in the response (if any)?
148 bytes

Task 3: Use Wireshark to open the attached "hw1.q2.pcapng" that includes the sniffed traffic when a user tried to browse a website and download a text file.

(a) What is the IP address of the website?
source: 192.168.0.86 destination: 147.26.156.12

(b) What are the web URLs the user successfully browsed in order?

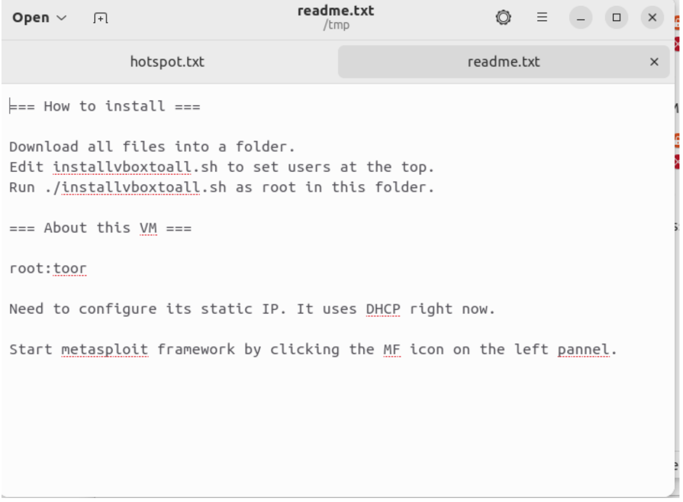


Wireshark · Export · HTTP object list

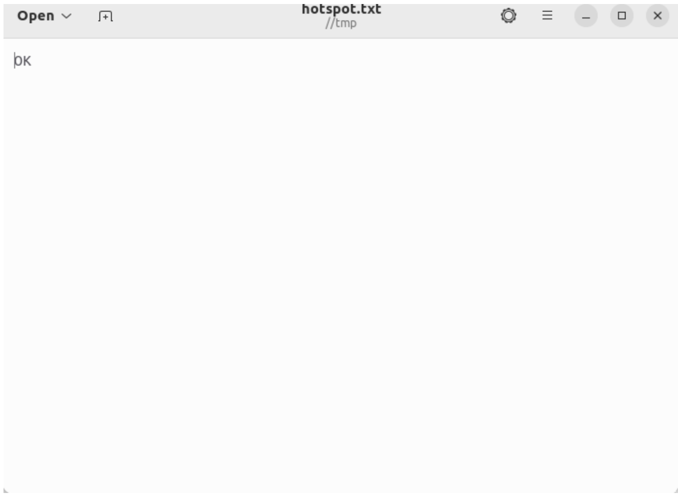
Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
3	fuxi.cs.txstate.edu	text/html	2,211 bytes	tools
5	fuxi.cs.txstate.edu	image/gif	148 bytes	blank.gif
9	fuxi.cs.txstate.edu	image/gif	216 bytes	back.gif
10	fuxi.cs.txstate.edu	image/gif	225 bytes	folder.gif
11	fuxi.cs.txstate.edu	image/gif	1,038 bytes	compressed.gif
13	fuxi.cs.txstate.edu	text/html	298 bytes	favicon.ico
19	fuxi.cs.txstate.edu	text/html	1,998 bytes	Kali.vbox
22	fuxi.cs.txstate.edu	image/gif	216 bytes	back.gif
24	fuxi.cs.txstate.edu	image/gif	229 bytes	text.gif
28	fuxi.cs.txstate.edu	image/gif	245 bytes	unknown.gif
29	fuxi.cs.txstate.edu	image/gif	148 bytes	blank.gif
37	fuxi.cs.txstate.edu	text/plain	322 bytes	readme.txt
39	fuxi.cs.txstate.edu	text/html	298 bytes	favicon.ico
41	fedoraproject.org	text/plain	2 bytes	hotspot.txt

(c) What is the content of the text file (not just text, but a text file, and only one text file) from the website?
One file had the downloading instructions the other had the word OK



```
=== How to install ===

Download all files into a folder.
Edit installvboxtoall.sh to set users at the top.
Run ./installvboxtoall.sh as root in this folder.

=== About this VM ===

root:toor

Need to configure its static IP. It uses DHCP right now.

Start metasploit framework by clicking the MF icon on the left pannel.
```



```
OK
```

Task 4: : Install pyshark and related dependencies

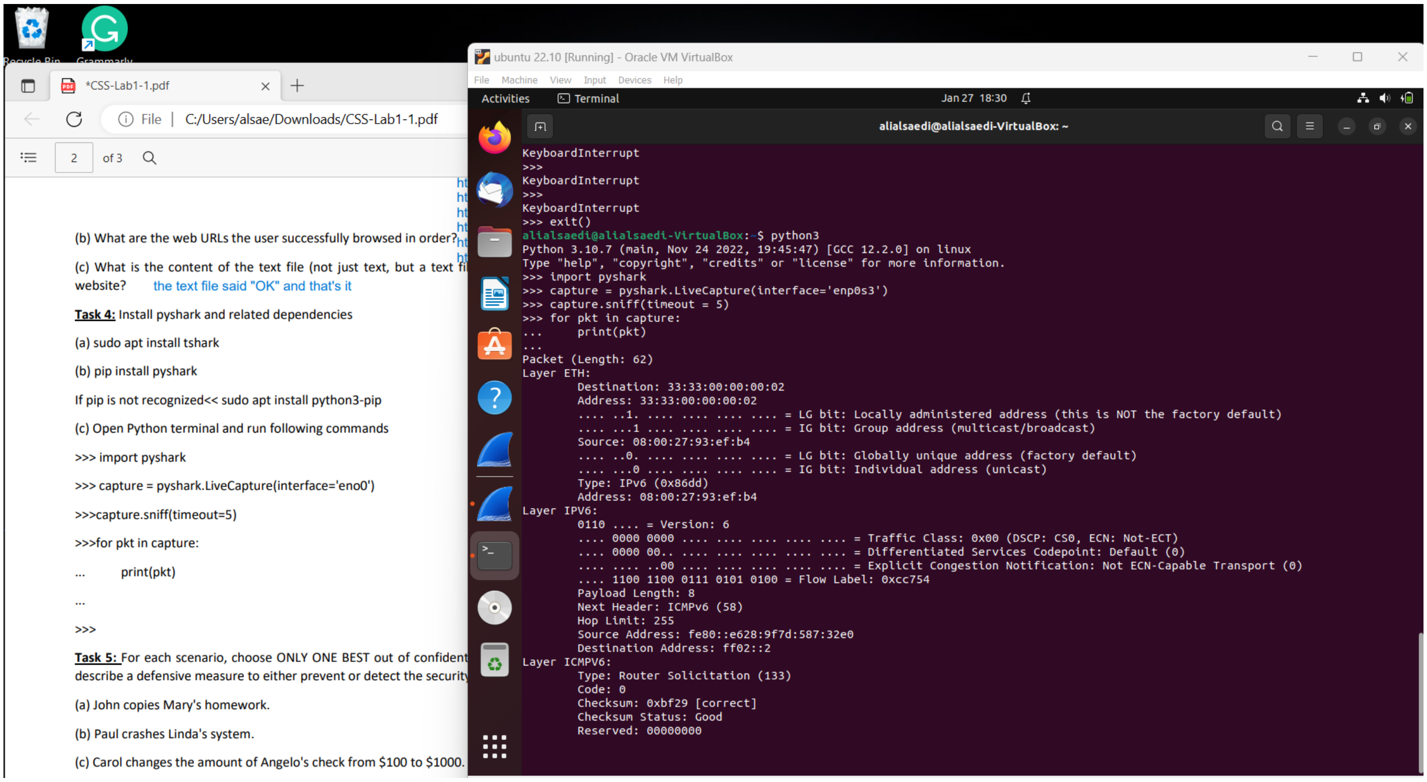
(a) sudo apt install tshark

(b) pip install pyshark

If pip is not recognized<< sudo apt install python3-pip

(c) Open Python terminal and run following commands

```
>>> import pyshark
>>> capture = pyshark.LiveCapture(interface='eno0')
>>>capture.sniff(timeout=5)
>>>for pkt in capture:
…          print(pkt)
...
>>>
```


Recycle Bin
Grammarly
*CSS-Lab1-1.pdf
File | C:/Users/alsae/Downloads/CSS-Lab1-1.pdf
2
of 3
ubuntu 22.10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Jan 27 18:30
alialsaedi@alialsaedi-VirtualBox: ~

(b) What are the web URLs the user successfully browsed in order?

(c) What is the content of the text file (not just text, but a text fi
website? the text file said "OK" and that's it

Task 4: Install pyshark and related dependencies

(a) sudo apt install tshark

(b) pip install pyshark

If pip is not recognized<< sudo apt install python3-pip

(c) Open Python terminal and run following commands

```
>>> import pyshark

>>> capture = pyshark.LiveCapture(interface='eno0')

>>>capture.sniff(timeout=5)

>>>for pkt in capture:

...        print(pkt)

...

>>>
```

Task 5: For each scenario, choose ONLY ONE BEST out of confident
describe a defensive measure to either prevent or detect the security

(a) John copies Mary's homework.

(b) Paul crashes Linda's system.

(c) Carol changes the amount of Angelo's check from $100 to $1000.

```
KeyboardInterrupt
>>>
KeyboardInterrupt
>>>
KeyboardInterrupt
>>> exit()
alialsaedi@alialsaedi-VirtualBox:~$ python3
Python 3.10.7 (main, Nov 24 2022, 19:45:47) [GCC 12.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import pyshark
>>> capture = pyshark.LiveCapture(interface='enp0s3')
>>> capture.sniff(timeout = 5)
>>> for pkt in capture:
...     print(pkt)
...
Packet (Length: 62)
Layer ETH:
        Destination: 33:33:00:00:00:02
        Address: 33:33:00:00:00:02
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
        .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
        Source: 08:00:27:93:ef:b4
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        Type: IPv6 (0x86dd)
        Address: 08:00:27:93:ef:b4
Layer IPV6:
        0110 .... = Version: 6
        .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
        .... 0000 00.. .... .... .... .... .... = Differentiated Services Codepoint: Default (0)
        .... .... ..00 .... .... .... .... .... = Explicit Congestion Notification: Not ECN-Capable Transport (0)
        .... 1100 1100 0111 0101 0100 = Flow Label: 0xcc754
        Payload Length: 8
        Next Header: ICMPv6 (58)
        Hop Limit: 255
        Source Address: fe80::e628:9f7d:587:32e0
        Destination Address: ff02::2
Layer ICMPV6:
        Type: Router Solicitation (133)
        Code: 0
        Checksum: 0xbf29 [correct]
        Checksum Status: Good
        Reserved: 00000000
```

Task 5: For each scenario, choose ONLY ONE BEST out of confidentiality, integrity and availability, and describe a defensive measure to either prevent or detect the security violation.
(a) John copies Mary's homework.

Confidentiality, a way mary can prevent john from copying her homework is by putting some better protections in place for example only people with a password can access marys homework 2 factor authentication would be the best choice for a situation like this

(b) Paul crashes Linda's system.

Avalibility, one saftey measure could be to insert a firewall or even to some kind of intrusion detection so they arent able to access the system in the first place another one would be for linda to back her system up elsewhere just in case something like this happens her system isnt completely gone

(c) Carol changes the amount of Angelo's check from $100 to $1000.

Integrity, one way to prevent or detect this change would be to enable a notification whenever the amount of you check is changed, as well as having a passkey to access the check so no one can manipulate it unless the have that access key

(d) Gina forges Roger's signature on a deed.

Integrity, 2 factor authentication would be the best way to make sure something like this doesnt occur, so the person not only needs the signature but also something else like a thumb print

(e) Rhonda deletes all web services from the university’s web servers.

Availability, changing the criteria to has access to the universities web servers would prevent someone like from rhonda to come in and delete all the files

(f) Henry spoofs Julie's IP address to gain access to her computer

Confidentiality, the best way julie can stop this is to have some firewalls in place or to use a vpn to make sure her info isn't getting viewed by others