

Homework #8 Forensics II

Honor Pledge: I pledge on my honor that I have not given or received any unauthorized assistance on this assignment/examination.

1. First, i downloaded the file from the URL provided. Next, I searched for http in wireshark. Then I searched for TCP in the Analyze tab in wireshark. Next I searched for a url and found

```
[Time since request: 0.01/95510/ seconds]
```

```
[Request in frame: 8]
```

```
[Request URI: http://supersecure.store:5454/MEMES/]
```

```
File Data: 162 bytes
```

```
e-based text data: text/html (7 lines)
```

This took me to a 404 page, but downloaded a file

← → ↻ ⚠ Not secure | supersecure.store:5454/MEMES/ 🔒

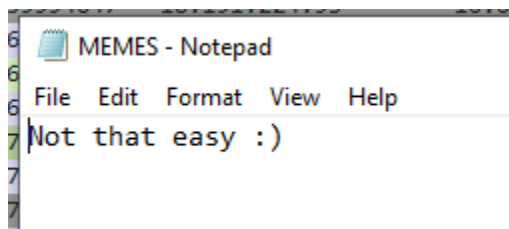
404 Not Found

nginx/1.18.0 (Ubuntu)

Activate Windows
Go to Settings to activate Windows

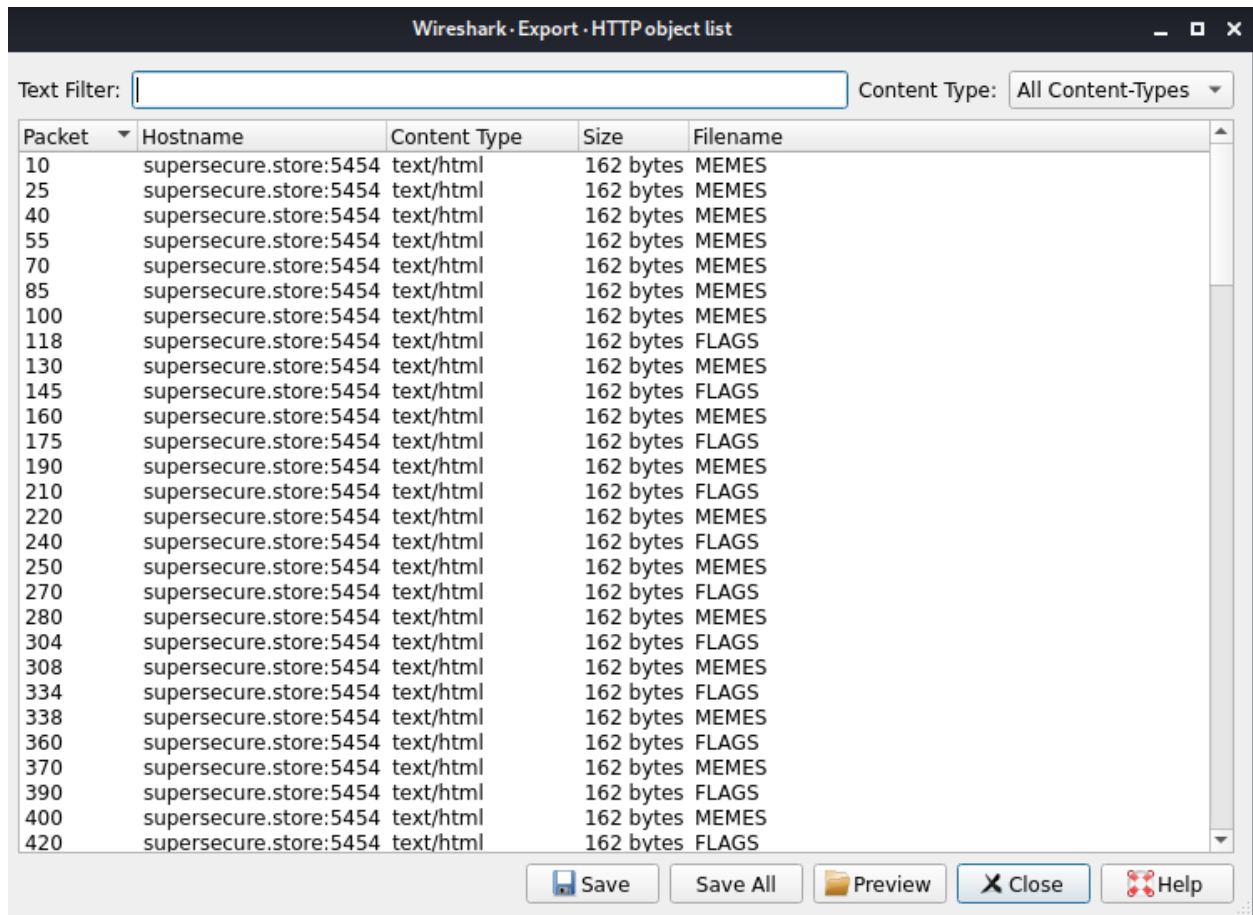
MEMES ^

Opening this file, I find



Which eliminates the idea that this will be a quick assignment.

Diving into more detail, I continue my search through the http data in wireshark. I next go to “file” and select “Export Objects”



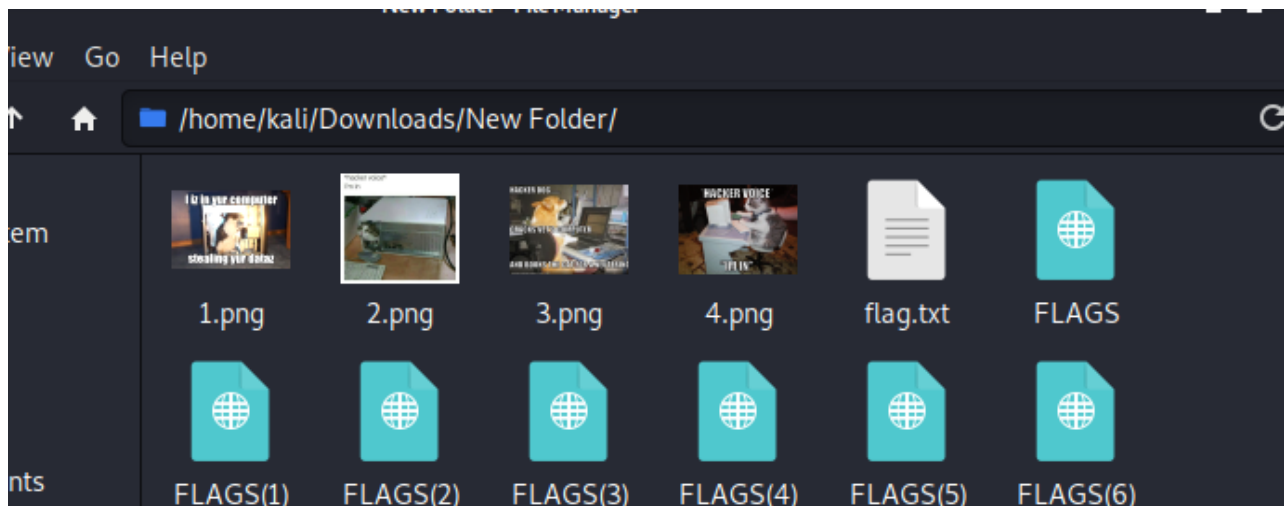
I search for ‘.png’ in the text filter and get 4 results.

Wireshark - Export - HTTP object list

Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
807	supersecure.store:5454	image/png	490kB	1.png
1142	supersecure.store:5454	image/png	1,337kB	2.png
1266	supersecure.store:5454	image/png	422kB	3.png
1686	supersecure.store:5454	image/png	1,403kB	4.png

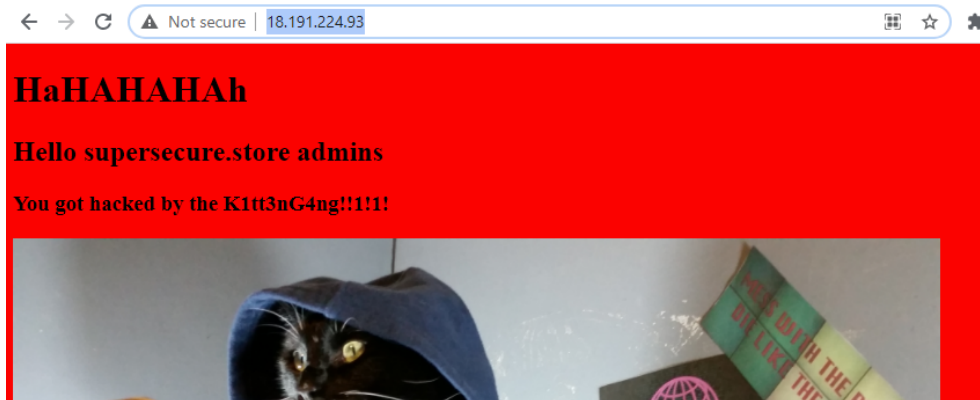
Saving all the data from here to a Folder and i can then see all of the memes.



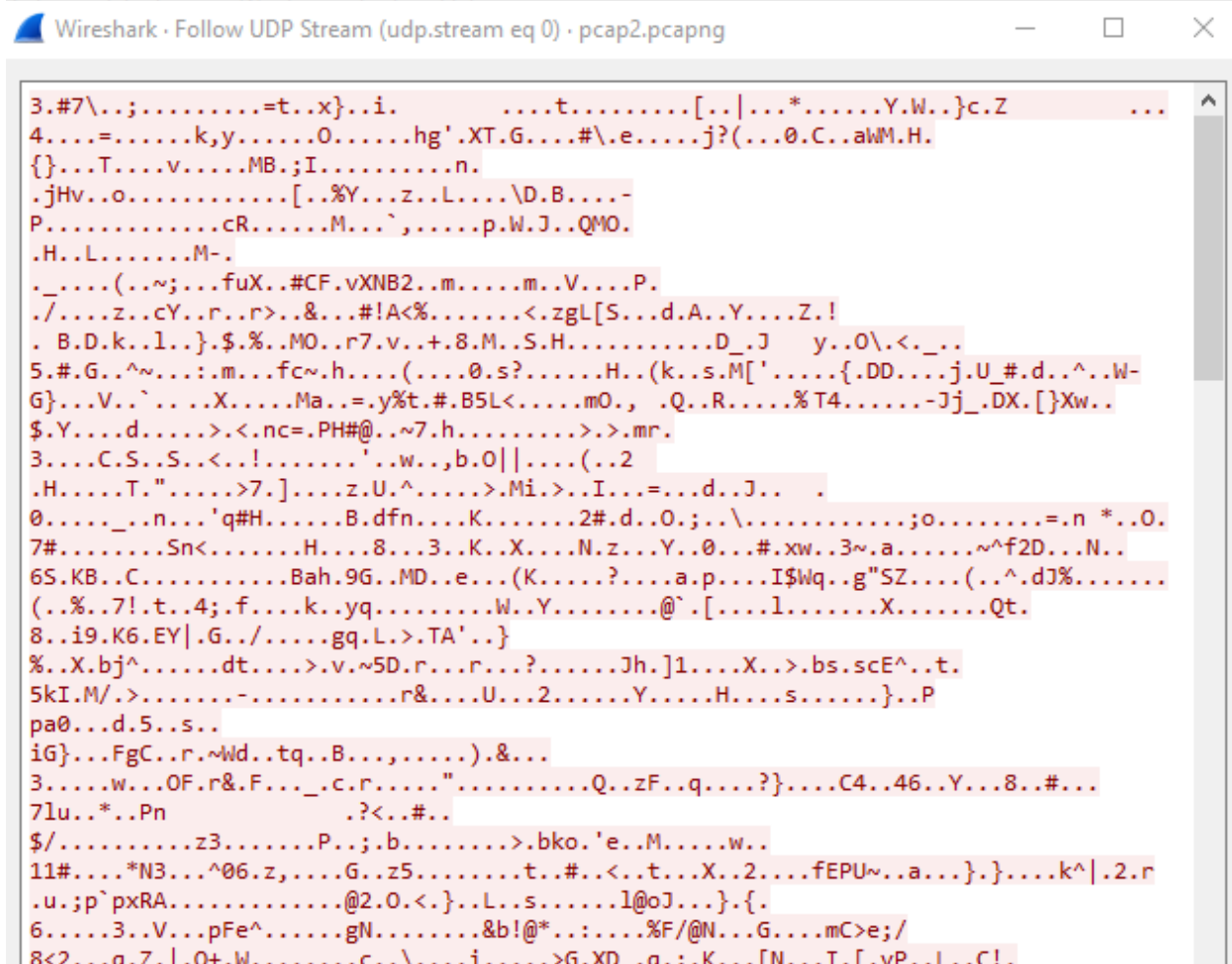
2. Having some trouble on this one but I see that all the packets are UDP with the exception of 4 that are ARP(Address resolution protocol) requests (via statistics tab and protocol hierarchy menu).

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End
▼ Frame	100.0	251	100.0	73010	19k	0	0	0
▼ Ethernet	100.0	251	4.8	3514	949	0	0	0
▼ Internet Protocol Version 4	98.4	247	6.8	4940	1334	0	0	0
▼ User Datagram Protocol	98.4	247	2.7	1976	533	0	0	0
Data	98.4	247	85.5	62432	16k	247	62432	16k
Address Resolution Protocol	1.6	4	0.2	148	39	4	148	39

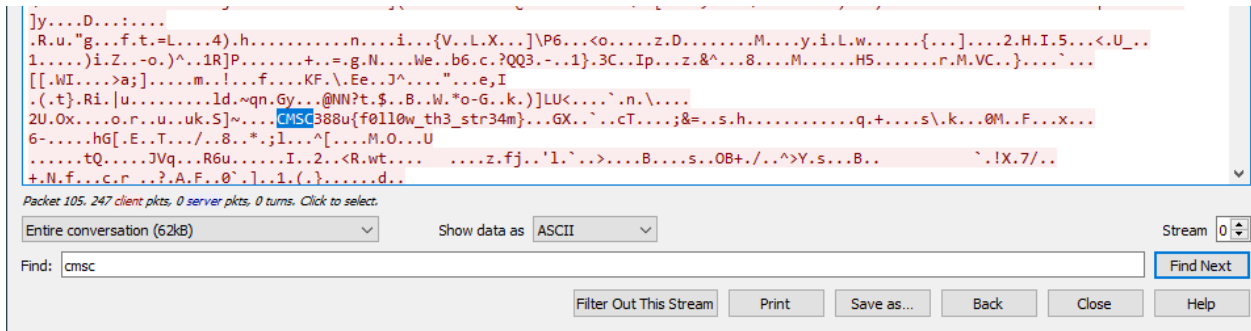
Additionally, all of the packets are originating from a host with an IP od 10.0.2.15 and reaching a destination of 18.191.224.93, which is



They are all going to port 5454 which is a simple page with a ‘:)’ on it.
Analysing the data and following the UDP stream, we get:



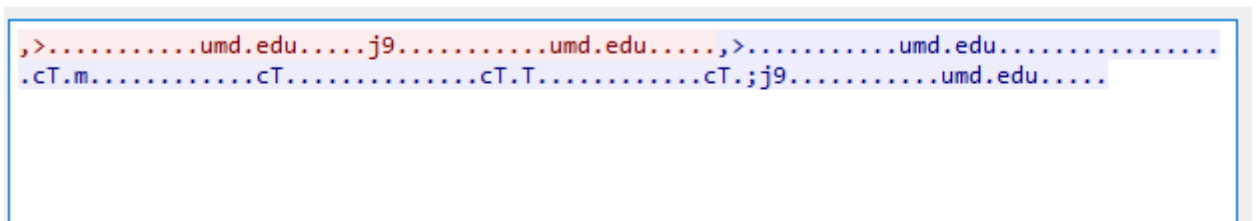
Using the search bar,



And there it is

Flag: CMSC388u{f0110w_th3_str34m}

3. Following the UDP stream we get



It looks like someone was trying to access the umd.edu website for some reason.

Using the statistics tab and protocol hierarchy menu, we get

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End B
▼ Frame	100.0	2053	100.0	350426	165k	0	0
▼ Ethernet	100.0	2053	8.2	28742	13k	0	0
▼ Internet Protocol Version 4	100.0	2053	11.7	41060	19k	0	0
▼ Transmission Control Protocol	100.0	2053	79.0	276930	130k	1683	52580
▼ Hypertext Transfer Protocol	18.0	370	66.0	231430	109k	92	6740
Line-based text data	9.0	185	41.5	145510	68k	185	14889
HTML Form URL Encoded	4.5	93	0.3	1197	564	93	1197

Which shows that there are TCP manu packets and HTTP requests.

Following the TCP steam

```
GET / HTTP/1.1
Host: umd.edu
User-Agent: curl/7.72.0
Accept: */*

HTTP/1.1 301 Moved Permanently
Server: CloudFront
Date: Tue, 06 Apr 2021 03:23:34 GMT
Content-Type: text/html
Content-Length: 183
Connection: keep-alive
Location: https://umd.edu/
X-Cache: Redirect from cloudfront
Via: 1.1 e06a155936c216d176543a7a25710ed0.cloudfront.net (CloudF
X-Amz-Cf-Pop: IAD89-C2
X-Amz-Cf-Id: gjczk1ItcB1lB5pipPlAEDSPCoJgzAezbx9se4LGctBut6ArmFl

<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<center><h1>301 Moved Permanently</h1></center>
<hr><center>CloudFront</center>
</body>
</html>
```

Which confirms the UDP stream that showed some sort of attempt to access umd.edu but the page has the text “301 Moved Permanently” and “CloudFront”

I think we should look at POST requests.

Using ‘http.request.method == POST’ in the search bar, we get only the HTTP requests that are POST requests.

Using this, I searched through all of the packets in the “HTML Form URL Encoded” and found this:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.method == POST && http.request.method != GET

Time	Source	Destination	Protocol	Length	Info
18	12.593222618	10.0.2.15	18.191.224.93	HTTP	239 POST / HTTP/1.1 (application/x-www-form-urlencoded)
54	12.721281748	10.0.2.15	99.84.176.109	HTTP	206 POST / HTTP/1.1 (application/x-www-form-urlencoded)

<

> Frame 2118: 239 bytes on wire (1912 bits), 239 bytes captured (1912 bits) on interface eth0, id 0
 > Ethernet II, Src: PcsCompu_ab:08:1c (08:00:27:ab:08:1c), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
 > Internet Protocol Version 4, Src: 10.0.2.15, Dst: 18.191.224.93
 > Transmission Control Protocol, Src Port: 41820, Dst Port: 5454, Seq: 1, Ack: 1, Len: 185

▼ Hypertext Transfer Protocol

> POST / HTTP/1.1\r\n
 Host: supersecure.store:5454\r\n
 User-Agent: curl/7.72.0\r\n
 Accept: */*\r\n
 > Content-Length: 29\r\n
 Content-Type: application/x-www-form-urlencoded\r\n
 \r\n
[\[Full request URI: http://supersecure.store:5454/\]](#)
[\[HTTP request 1/1\]](#)
[\[Response in frame: 2120\]](#)
 File Data: 29 bytes

▼ HTML Form URL Encoded: application/x-www-form-urlencoded

▼ Form item: "CMSC388u{filter_ing_is_sw33t}" = ""
 Key: CMSC388u{filter_ing_is_sw33t}
 Value:

Which appears to be the flag

Flag: CMSC388u{filter_ing_is_sw33t}