

Package Analyses

- set2.pcap (391KB) - For second exercise, extrating pictures and files
- set3.pcap (39MB) - For third exercise, reconstructing a media file
- set4.pcap (17KB) - For fourth exercise, finding and verifying plaintext credentials
- set5.pcap (61MB) - For fifth exercise, finding and verifying plaintext credentials in a larger PCAP file

set2.pcap

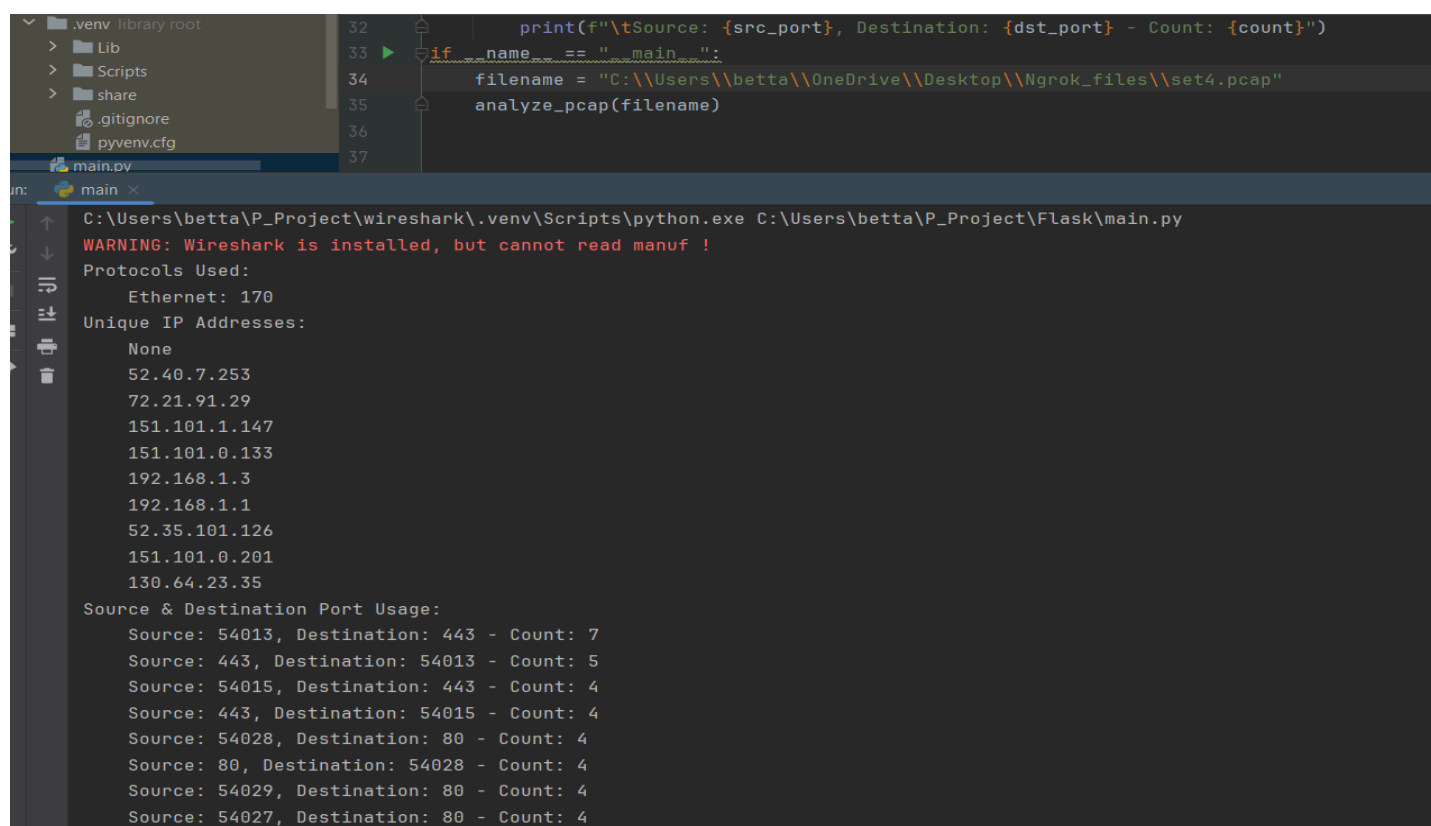
```
main.py x
1 from scapy.all import rdpcap
2 from collections import defaultdict
3
4 def analyze_pcap(filename):
5     protocol_counts = defaultdict(int)
6     ip_addresses = set()
7     port_usage = defaultdict(int)
8     packets = rdpcap(filename)
9     for packet in packets:
10         protocol = packet.name
11         ip_src, ip_dst = None, None
12         src_port, dst_port = None, None
13         if packet.haslayer('IP'):
14             ip_src = packet['IP'].src
15             ip_dst = packet['IP'].dst
16         transport_layer = packet.getlayer('TCP') or packet.getlayer('UDP')
17         if transport_layer:
18             src_port = transport_layer.sport
19             dst_port = transport_layer.dport
20         protocol_counts[protocol] += 1
21         ip_addresses.update({ip_src, ip_dst})
22         if src_port and dst_port:
23             port_usage[(src_port, dst_port)] += 1
24     print("Protocols Used:")
25     for protocol, count in protocol_counts.items():
26         print(f"\t{protocol}: {count}")
27     print("Unique IP Addresses:")
28     for ip in ip_addresses:
29         print(f"\t{ip}")
30     print("Source & Destination Port Usage:")
31     for (src_port, dst_port), count in port_usage.items():
32         print(f"\tSource: {src_port}, Destination: {dst_port} - Count: {count}")
33 if __name__ == "__main__":
34     filename = "C:\\Users\\betta\\OneDrive\\Desktop\\Ngrok_files\\set2.pcap"
35     analyze_pcap(filename)
```

```

C:\Users\betta\P_Project\wireshark\.venv\Scripts\python.exe C:\Users\betta\P_Project\Flask\main.py
WARNING: Wireshark is installed, but cannot read manuaf !
Protocols Used:
    Ethernet: 482
Unique IP Addresses:
    192.168.1.8
    192.168.1.228
Source & Destination Port Usage:
    Source: 49979, Destination: 21 - Count: 40
    Source: 21, Destination: 49979 - Count: 25
    Source: 20, Destination: 49980 - Count: 13
    Source: 49980, Destination: 20 - Count: 13
    Source: 20, Destination: 49981 - Count: 46
    Source: 49981, Destination: 20 - Count: 52
    Source: 20, Destination: 49982 - Count: 47
    Source: 49982, Destination: 20 - Count: 47
    Source: 20, Destination: 49983 - Count: 66
    Source: 49983, Destination: 20 - Count: 103
    Source: 20, Destination: 49984 - Count: 15
    Source: 49984, Destination: 20 - Count: 15

```

Set3.pcap



```

32     print(f"\tSource: {src_port}, Destination: {dst_port} - Count: {count}")
33     if name == "main":
34         filename = "C:\\Users\\betta\\OneDrive\\Desktop\\Ngrok_files\\set4.pcap"
35         analyze_pcap(filename)
36
37

```

```

C:\Users\betta\P_Project\wireshark\.venv\Scripts\python.exe C:\Users\betta\P_Project\Flask\main.py
WARNING: Wireshark is installed, but cannot read manuaf !
Protocols Used:
    Ethernet: 170
Unique IP Addresses:
    None
    52.40.7.253
    72.21.91.29
    151.101.1.147
    151.101.0.133
    192.168.1.3
    192.168.1.1
    52.35.101.126
    151.101.0.201
    130.64.23.35
Source & Destination Port Usage:
    Source: 54013, Destination: 443 - Count: 7
    Source: 443, Destination: 54013 - Count: 5
    Source: 54015, Destination: 443 - Count: 4
    Source: 443, Destination: 54015 - Count: 4
    Source: 54028, Destination: 80 - Count: 4
    Source: 80, Destination: 54028 - Count: 4
    Source: 54029, Destination: 80 - Count: 4
    Source: 54027, Destination: 80 - Count: 4

```

Set4.pcap

eth matches "plain"						
No.	Time	Source	Destination	Protocol	Length	Info
65592	19:48:51	205.178.146.249	10.139.31.212	SMTP	181	S: 250-mailpod.hostingplatform.com STARTTLS PIPELINING 8BITIME SIZE 6500000 AUTH LOGIN PLAIN CRAM-MD5
65593	19:48:51	205.178.146.249	10.139.31.212	TCP	181	[TCP Retransmission] 587 → 52682 [PSH, ACK] Seq=40 Ack=23 Win=14600 Len=127
25767	19:48:48	172.20.63.254	208.85.40.35	TCP	495	51761 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=429 TSval=170418760 TSecr=1540511418 [TCP segment of a reassembled PDU]
25768	19:48:48	172.20.63.254	208.85.40.35	TCP	495	[TCP Retransmission] 51761 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=429 TSval=170418760 TSecr=1540511418
41039	19:48:49	50.19.80.43	10.111.30.146	HTTP	1422	HTTP/1.1 200 OK (text/plain)
41040	19:48:49	50.19.80.43	10.111.30.146	TCP	1422	[TCP Retransmission] 6969 → 63562 [PSH, ACK] Seq=1 Ack=369 Win=30336 Len=1368
74964	19:48:52	10.139.31.212	205.178.146.249	SMTP	1440	C: DATA fragment, 1386 bytes
74965	19:48:52	10.139.31.212	205.178.146.249	TCP	1440	[TCP Retransmission] 52682 → 587 [ACK] Seq=151 Ack=224 Win=65535 Len=1386

Set5.pcap

eth contains 'text'

No.	Time	Source	Destination	Protocol	Length	Info
+	60	05:29:37	192.168.1.3	130.64.23.35	HTTP	496 GET /~cgregg/grades/ HTTP/1.1
+	62	05:29:37	130.64.23.35	192.168.1.3	HTTP	793 HTTP/1.1 401 Authorization Required (text/html)
	138	05:29:49	192.168.1.3	130.64.23.35	HTTP	480 GET /~cgregg/grades/ HTTP/1.1
	140	05:29:49	130.64.23.35	192.168.1.3	HTTP	793 HTTP/1.1 401 Authorization Required (text/html)
	163	05:29:59	192.168.1.3	130.64.23.35	HTTP	472 GET /~cgregg/grades/ HTTP/1.1
	165	05:29:59	130.64.23.35	192.168.1.3	HTTP	793 HTTP/1.1 401 Authorization Required (text/html)

> Frame 62: 793 bytes on wire (6344 bits), 793 bytes captured (6344 bits)

> Ethernet II, Src: ActiontecEle6d:c7:27 (f8:e4:fb:6d:c7:27), Dst: Apple_cf:53:89 (aa:00:00:00:00:00)

> Internet Protocol Version 4, Src: 130.64.23.35, Dst: 192.168.1.3

> Transmission Control Protocol, Src Port: 80, Dst Port: 54042, Seq: 1, Ack: 431, Len: 0

> Hypertext Transfer Protocol

> Line-based text data: text/html (14 lines)

```

0000  a4 5e 60 cf 53 89 f8 e4 fb 6d c7 27 08 00 45 4a  .^ S...m...EJ
0010  03 0b dd c5 40 00 32 06 0c cf 82 40 17 23 0c a8  ...@.2...@.#...
0020  01 03 00 50 13 1a e3 5b 96 df 8b 01 e0 da 80 18  ...P...
0030  00 7a cd 5f 00 00 01 01 08 04 45 91 4b 21 02 50  -z...E...
0040  c0 81 48 54 54 50 2f 31 2e 31 20 3a 30 20 41 01  -HTTP/1.1 401 A
0050  75 74 68 6f 72 69 7a 61 74 69 6f 6e 52 65 71  authorization Req
0060  75 69 72 65 64 0d 0a 44 61 74 65 3a 20 54 68 75  uired-D ate: Thu
0070  2c 20 32 35 20 4a 61 6e 20 32 30 31 38 20 30 34  , 25 Jan 2018 04
0080  3a 32 39 3a 33 37 20 47 4d 54 0d 0a 53 65 72 76  :29:37 G MT- Serv
0090  65 72 3a 20 41 70 61 63 68 65 2f 32 2e 32 3e 31  er: Apac he/2.2.1
00a0  35 20 28 52 65 64 20 48 61 74 29 0d 0a 57 57 57  5 (Red H at)-WWW
00b0  2d 41 75 74 68 65 64 7a 69 63 61 74 65 3a 20 42  -Authn icate: B
00c0  61 73 69 63 20 72 65 61 6c 6d 3d 22 66 69 7a 7d  asic rae lm="Virt
00d0  75 61 6c 20 47 72 61 64 65 22 0d 0a 43 6f 6e 74  ual Grad e". Cont
00e0  65 74 2d 4c 65 6e 67 74 68 3a 20 39 38 76 0d  ent-Leng th: 486
00f0  0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74  -Content -Type: t
0100  65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65  ext/html ; charse
0110  74 3d 69 73 6f 2d 38 35 39 2d 31 0d 0a 43 6f  t-iso-88 59-1 .Co
0120  6e 65 63 6f 69 6f 6e 6c 3a 20 63 6f 6f 73 65 0d  nnection : close

```

```

0000  a4 5e 60 cf 53 89 f8 e4 fb 6d c7 27 08 00 45 4a  .^ S...m...EJ
0010  03 0b dd c5 40 00 32 06 0c cf 82 40 17 23 0c a8  ...@.2...@.#...
0020  01 03 00 50 13 1a e3 5b 96 df 8b 01 e0 da 80 18  ...P...
0030  00 7a cd 5f 00 00 01 01 08 04 45 91 4b 21 02 50  -z...E...
0040  c0 81 48 54 54 50 2f 31 2e 31 20 3a 30 20 41 01  -HTTP/1.1 401 A
0050  75 74 68 6f 72 69 7a 61 74 69 6f 6e 52 65 71  authorization Req
0060  75 69 72 65 64 0d 0a 44 61 74 65 3a 20 54 68 75  uired-D ate: Thu
0070  2c 20 32 35 20 4a 61 6e 20 32 30 31 38 20 30 34  , 25 Jan 2018 04
0080  3a 32 39 3a 33 37 20 47 4d 54 0d 0a 53 65 72 76  :29:37 G MT- Serv
0090  65 72 3a 20 41 70 61 63 68 65 2f 32 2e 32 3e 31  er: Apac he/2.2.1
00a0  35 20 28 52 65 64 20 48 61 74 29 0d 0a 57 57 57  5 (Red H at)-WWW
00b0  2d 41 75 74 68 65 64 7a 69 63 61 74 65 3a 20 42  -Authn icate: B
00c0  61 73 69 63 20 72 65 61 6c 6d 3d 22 66 69 7a 7d  asic rae lm="Virt
00d0  75 61 6c 20 47 72 61 64 65 22 0d 0a 43 6f 6e 74  ual Grad e". Cont
00e0  65 74 2d 4c 65 6e 67 74 68 3a 20 39 38 76 0d  ent-Leng th: 486
00f0  0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74  -Content -Type: t
0100  65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65  ext/html ; charse
0110  74 3d 69 73 6f 2d 38 35 39 2d 31 0d 0a 43 6f  t-iso-88 59-1 .Co
0120  6e 65 63 6f 69 6f 6e 6c 3a 20 63 6f 6f 73 65 0d  nnection : close

```

> Frame 41039: 1422 bytes on wire (11376 bits), 1422 bytes captured (11376 bits)

> Ethernet II, Src: Intel_31:f8:14 (a0:36:9f:31:f8:14), Dst: Apple_a1:e0:e1 (f4:5c:89:a:00:00:00:00:00)

> Internet Protocol Version 4, Src: 50.19.80.43, Dst: 10.111.30.146

> Transmission Control Protocol, Src Port: 6969, Dst Port: 63562, Seq: 1, Ack: 369, Len 0

> Hypertext Transfer Protocol

> Line-based text data: text/plain (5 lines)

```

0040  30 30 20 4f 4b 0d 0a 43 6f 6e 74 65 6e 74 2d
```