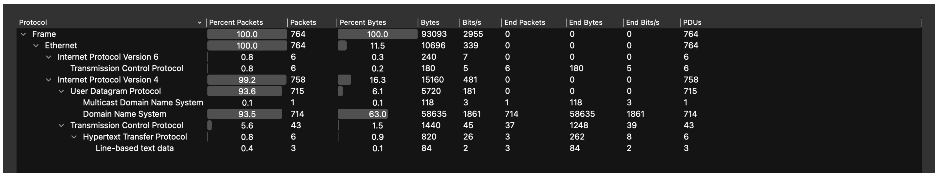
1. What types of traffic (HTTP, DNS, FTP, etc.) are present?

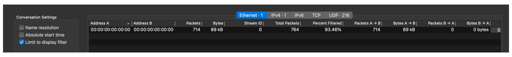
Ans: HTTP,DNS,TCP



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	764	100.0	93093	2955	0	0	0	764
Ethernet	100.0	764	11.5	10696	339	0	0	0	764
Internet Protocol Version 6	0.8	6	0.3	240	7	0	0	0	6
Transmission Control Protocol	0.8	6	0.2	180	5	6	180	5	6
Internet Protocol Version 4	99.2	758	16.3	15160	481	0	0	0	758
User Datagram Protocol	93.6	715	6.1	5720	181	0	0	0	715
Multicast Domain Name System	0.1	1	0.1	118	3	1	118	3	1
Domain Name System	93.5	714	63.0	58635	1861	714	58635	1861	714
Transmission Control Protocol	5.6	43	1.5	1440	45	37	1248	39	43
Hypertext Transfer Protocol	0.8	6	0.9	820	26	3	262	8	6
Line-based text data	0.4	3	0.1	84	2	3	84	2	3

2. How many DNS queries were made in total?

Ans:764



Conversation Settings

☐ Name resolution
☐ Absolute start time
☑ Limit to display filter

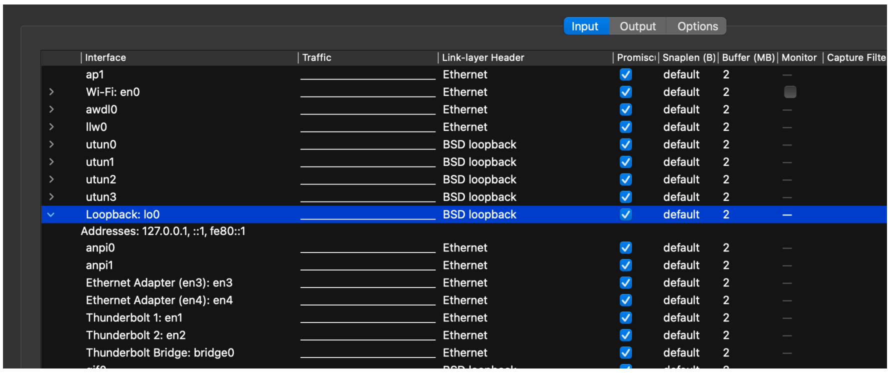
Address A	Address B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
00:00:00:00:00:00	00:00:00:00:00:00	714	89 kB	0	764	93.46%	714	89 kB	0	0 bytes

3. What types of DNS queries were made?

Ans:A,AAAA,HTTPS

4. What is a Loopback Interface?

Ans:A Loopback Interface is a virtual network interface used primarily for testing and internal communication within a device. It doesn't send data over a physical network but loops the data back to the same device.

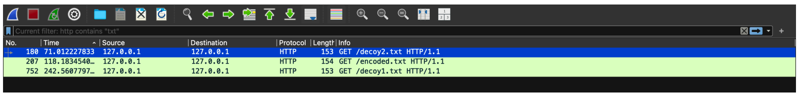


Interface	Traffic	Link-layer Header	Promisc	Snaplen (B)	Buffer (MB)	Monitor	Capture Filte
ap1		Ethernet	☑	default	2	—	
Wi-Fi: en0		Ethernet	☑	default	2	☐	
awdl0		Ethernet	☑	default	2	—	
llw0		Ethernet	☑	default	2	—	
utun0		BSD loopback	☑	default	2	—	
utun1		BSD loopback	☑	default	2	—	
utun2		BSD loopback	☑	default	2	—	
utun3		BSD loopback	☑	default	2	—	
Loopback: lo0		BSD loopback	☑	default	2	—	
Addresses: 127.0.0.1, ::1, fe80::1							
anpi0		Ethernet	☑	default	2	—	
anpi1		Ethernet	☑	default	2	—	
Ethernet Adapter (en3): en3		Ethernet	☑	default	2	—	
Ethernet Adapter (en4): en4		Ethernet	☑	default	2	—	
Thunderbolt 1: en1		Ethernet	☑	default	2	—	
Thunderbolt 2: en2		Ethernet	☑	default	2	—	
Thunderbolt Bridge: bridge0		Ethernet	☑	default	2	—	

5. How many .txt files were requested? List their names

Ans:3

- decoy2.txt
- decoy1.txt
- encoded.txt



Current filter: http contains "txt"

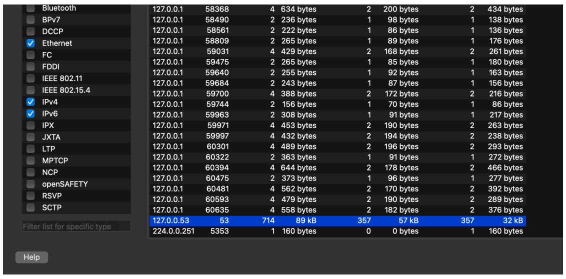
No.	Time	Source	Destination	Protocol	Length	Info
180	71.012227833	127.0.0.1	127.0.0.1	HTTP	153	GET /decoy2.txt HTTP/1.1
207	118.1834540…	127.0.0.1	127.0.0.1	HTTP	154	GET /encoded.txt HTTP/1.1
752	242.5607797…	127.0.0.1	127.0.0.1	HTTP	153	GET /decoy1.txt HTTP/1.1

6.One .txt file contains base64-encoded content. Identify and decode it.What does it contain?

Ans:FLAG{spid3r_network_master}

7. Was any attempt made to distract the analyst using decoy files? Explain.
Ans:
Yes, it looks like decoy files such as decoy1.txt were intentionally included to throw off the analyst. The file literally says "This is just a decoy," which makes it clear that it doesn't contain anything useful. It's likely there just to waste time or divert attention from the actual important data.

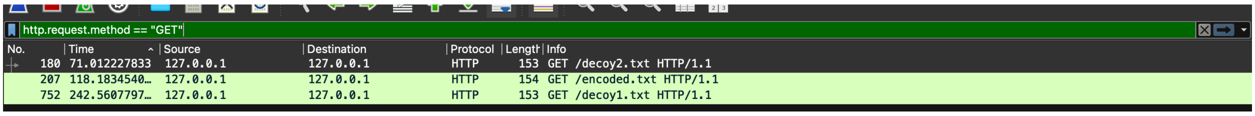
8. Are there any known ports being used for uncommon services?
Ans: There's clearly a lot of activity happening over port 53, which normally just handles quick DNS requests. But the amount of traffic here is too high for that. This could mean someone was using DNS not just to look up websites—but to send or receive data, possibly to avoid detection. It's like hiding in plain sight by disguising traffic as normal DNS.



☐ Bluetooth
☐ BPv7
☐ DCCP
☑ Ethernet
☐ FC
☐ FDDI
☐ IEEE 802.11
☐ IEEE 802.15.4
☑ IPv4
☑ IPv6
☐ IPX
☐ JXTA
☐ LTP
☐ MPTCP
☐ NCP
☐ openSAFETY
☐ RSVP
☐ SCTP

127.0.0.1	58368	4	634 bytes	2	200 bytes	2	434 bytes
127.0.0.1	58490	2	236 bytes	1	98 bytes	1	138 bytes
127.0.0.1	58561	2	222 bytes	1	86 bytes	1	136 bytes
127.0.0.1	58809	2	265 bytes	1	89 bytes	1	176 bytes
127.0.0.1	59031	4	429 bytes	2	168 bytes	2	261 bytes
127.0.0.1	59475	2	265 bytes	1	85 bytes	1	180 bytes
127.0.0.1	59640	2	255 bytes	1	92 bytes	1	163 bytes
127.0.0.1	59684	2	243 bytes	1	87 bytes	1	156 bytes
127.0.0.1	59700	4	388 bytes	2	172 bytes	2	216 bytes
127.0.0.1	59744	2	156 bytes	1	70 bytes	1	86 bytes
127.0.0.1	59963	2	308 bytes	1	91 bytes	1	217 bytes
127.0.0.1	59971	4	453 bytes	2	190 bytes	2	263 bytes
127.0.0.1	59997	4	432 bytes	2	194 bytes	2	238 bytes
127.0.0.1	60301	4	489 bytes	2	196 bytes	2	293 bytes
127.0.0.1	60322	2	363 bytes	1	91 bytes	1	272 bytes
127.0.0.1	60394	4	644 bytes	2	178 bytes	2	466 bytes
127.0.0.1	60475	2	373 bytes	1	96 bytes	1	277 bytes
127.0.0.1	60481	4	562 bytes	2	170 bytes	2	392 bytes
127.0.0.1	60593	4	479 bytes	2	190 bytes	2	289 bytes
127.0.0.1	60635	4	558 bytes	2	182 bytes	2	376 bytes
127.0.0.53	53	714	89 kB	357	57 kB	357	32 kB
224.0.0.251	5353	1	160 bytes	0	0 bytes	1	160 bytes

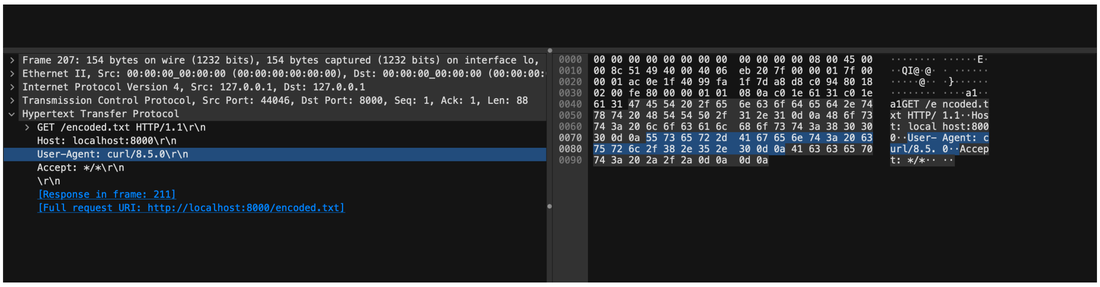
9. How many HTTP GET requests are visible in the capture?
Ans: There are three get requests visible.



```
http.request.method == "GET"
```

```
No.     | Time          | Source      | Destination | Protocol | Length | Info
    180  71.012227833   127.0.0.1     127.0.0.1     HTTP        153  GET /decoy2.txt HTTP/1.1
    207  118.1834540…   127.0.0.1     127.0.0.1     HTTP        154  GET /encoded.txt HTTP/1.1
    752  242.5607797…   127.0.0.1     127.0.0.1     HTTP        153  GET /decoy1.txt HTTP/1.1
```

10. What User-Agent was used to make the HTTP requests?
Ans: User-Agent: curl/8.5.0\r\n



```
> Frame 207: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface lo,
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 44046, Dst Port: 8000, Seq: 1, Ack: 1, Len: 88
v Hypertext Transfer Protocol
  > GET /encoded.txt HTTP/1.1\r\n
    Host: localhost:8000\r\n
    User-Agent: curl/8.5.0\r\n
    Accept: */*\r\n
    \r\n
    [Response in frame: 211]
    [Full request URI: http://localhost:8000/encoded.txt]
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ········ ······E·
0010  00 8c 51 49 40 00 40 06  eb 20 7f 00 00 01 7f 00   ··QI@·@· · ······
0020  00 01 ac 0e 1f 40 99 fa  1f 7d a8 d8 c0 94 80 18   ·····@·· ·}······
0030  02 00 fe 80 00 00 01 01  08 0a c0 1e 61 31 c0 1e   ········ ····a1··
0040  61 31 47 45 54 20 2f 65  6e 63 6f 64 65 64 2e 74   a1GET /e ncoded.t
0050  78 74 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73   xt HTTP/ 1.1··Hos
0060  74 3a 20 6c 6f 63 61 6c  68 6f 73 74 3a 38 30 30   t: local host:800
0070  30 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 63   0··User- Agent: c
0080  75 72 6c 2f 38 2e 35 2e  30 0d 0a 41 63 63 65 70   url/8.5. 0··Accep
0090  74 3a 20 2a 2f 2a 0d 0a  0d 0a                     t: */*·· ··
```