# Network Monitoring Application

Rajadorai DS

## Description of implementation:

- Obtain the input specifications from the user using ‘flag’ package

  **Input Components:**

  - -i Interface name (Ex: en0 , lo0 etc.)
  - -r Trace filename (Ex: test.pcap)
  - -s String match pattern input (Ex: “HTTP”)
  - [expression] BPF Filter (Ex: “tcp and port 443”)

- **Determine mode of capture:**

  a) Read packets from trace file

  - If trace filename is given, the packets are captured from it (even if an interface name is provided for live capture).

  b) Live capture in promiscuous mode

  - If the trace file is not given, the packets are captured via live capture through the interface given in the user input. If the interface is also not provided, then a device name is picked up using packet.FindAllDevs() and an interface to capture the packets is chosen.

- Before packet capture, the **BPF Filter** (if provided) is applied to the handle.

- Each packet is checked to see if the payload of the packet contains the matching “**string -s**” provided by the user. If yes, the packet is checked for each Layer (from gopacket/layers) such as Ethernet, application layer, IP Layer etc. The required information is then captured and **printed** to the output.

## Sample Input Patterns:

(Note: Input flags (-i , -r, -s) can be in any order and the BPF Filter (if present) should be at the end of the input line as the final argument - as it does not have an identifier flag. All arguments are **optional**)

- go run mydump.go -i en0 -r “test.pcap” -s “HTTP” “tcp and port 80”

- go run mydump.go -r “test.pcap” -s “HTTP” “tcp and port 80”

- go run mydump.go -i en0 -s “HTTP” “tcp and port 80”

- go run mydump.go -s “HTTP” “tcp and port 80”

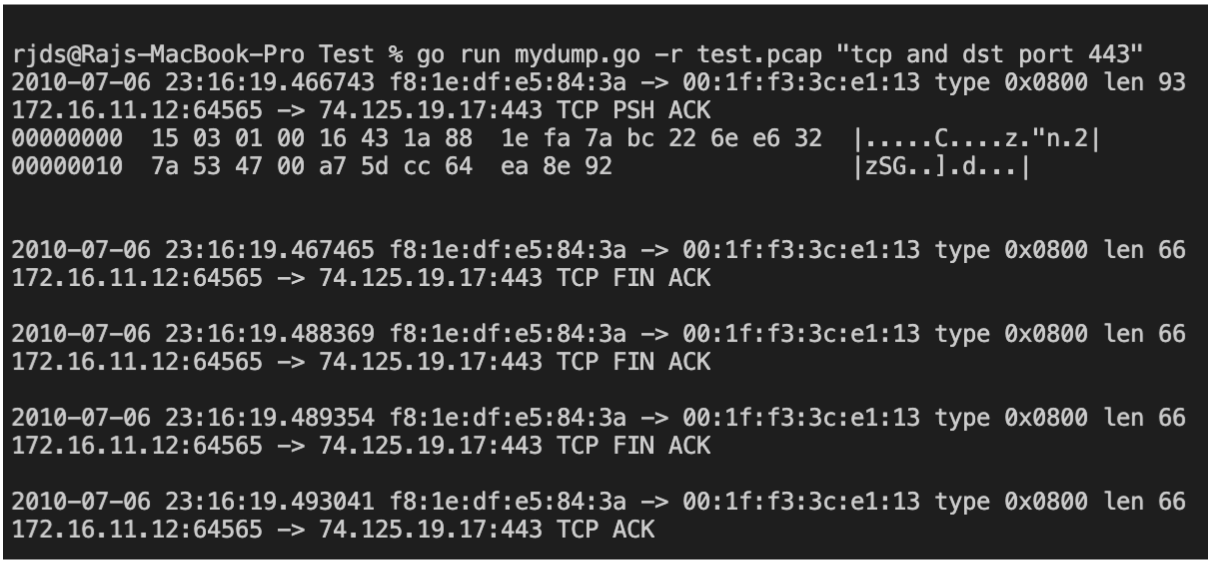
- go run mydump.go “tcp and port 80”

- go run mydump.go -s “HTTP”

- go run mydump.go

**Sample Outputs**

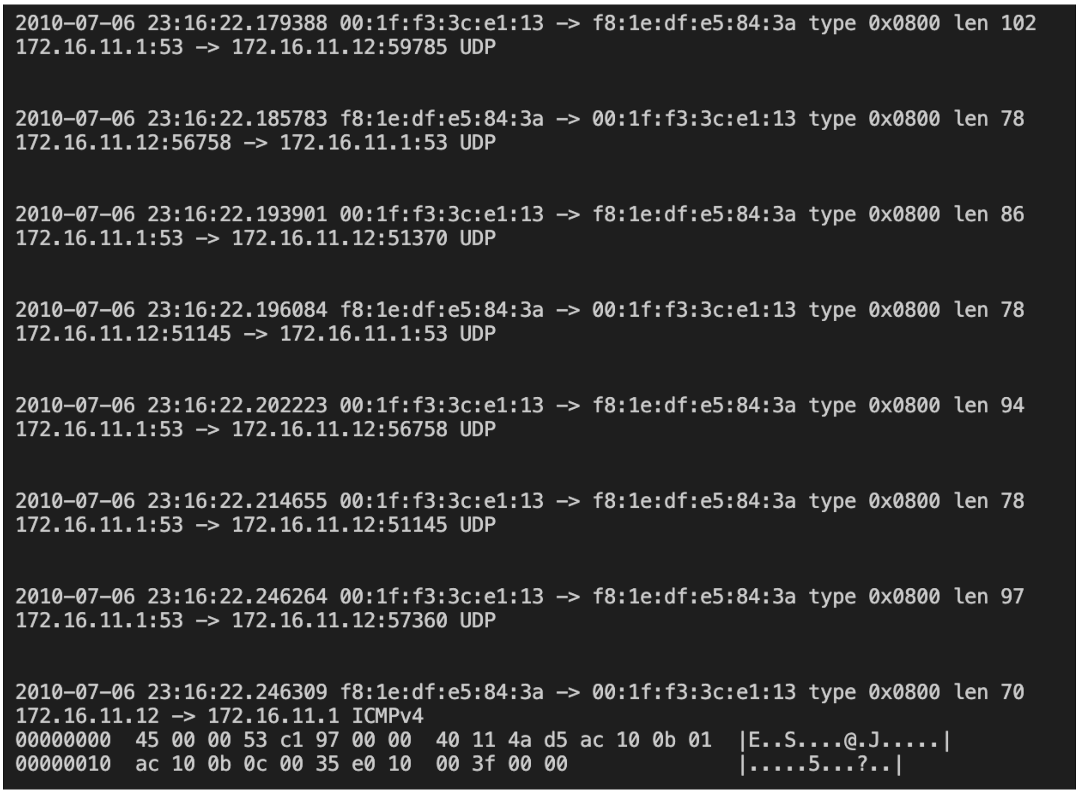
**1)**



```
rjds@Rajs-MacBook-Pro Test % go run mydump.go -r test.pcap "tcp and dst port 443"
2010-07-06 23:16:19.466743 f8:1e:df:e5:84:3a -> 00:1f:f3:3c:e1:13 type 0x0800 len 93
172.16.11.12:64565 -> 74.125.19.17:443 TCP PSH ACK
00000000  15 03 01 00 16 43 1a 88  1e fa 7a bc 22 6e e6 32  |.....C....z."n.2|
00000010  7a 53 47 00 a7 5d cc 64  ea 8e 92                 |zSG..].d...|


2010-07-06 23:16:19.467465 f8:1e:df:e5:84:3a -> 00:1f:f3:3c:e1:13 type 0x0800 len 66
172.16.11.12:64565 -> 74.125.19.17:443 TCP FIN ACK

2010-07-06 23:16:19.488369 f8:1e:df:e5:84:3a -> 00:1f:f3:3c:e1:13 type 0x0800 len 66
172.16.11.12:64565 -> 74.125.19.17:443 TCP FIN ACK

2010-07-06 23:16:19.489354 f8:1e:df:e5:84:3a -> 00:1f:f3:3c:e1:13 type 0x0800 len 66
172.16.11.12:64565 -> 74.125.19.17:443 TCP FIN ACK

2010-07-06 23:16:19.493041 f8:1e:df:e5:84:3a -> 00:1f:f3:3c:e1:13 type 0x0800 len 66
172.16.11.12:64565 -> 74.125.19.17:443 TCP ACK
```

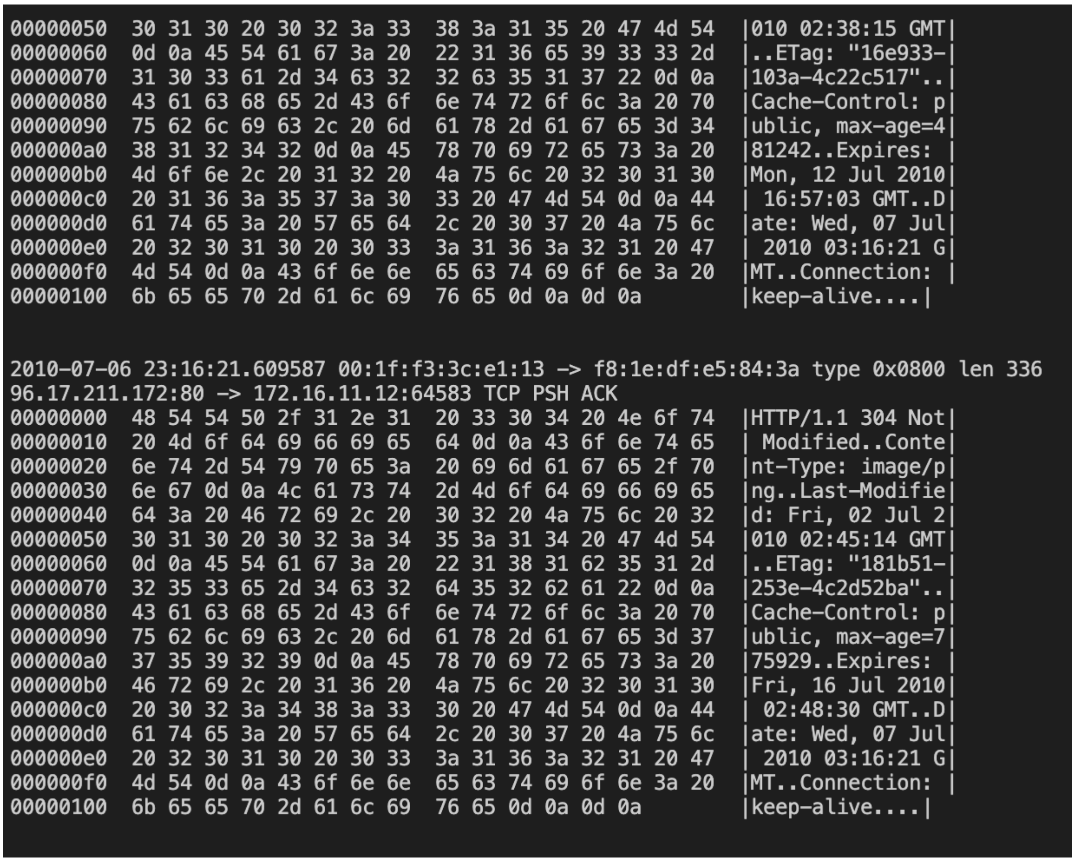
(Contd. below)

**2)**



```
2010-07-06 23:16:22.179388 00:1f:f3:3c:e1:13 -> f8:1e:df:e5:84:3a type 0x0800 len 102
172.16.11.1:53 -> 172.16.11.12:59785 UDP


2010-07-06 23:16:22.185783 f8:1e:df:e5:84:3a -> 00:1f:f3:3c:e1:13 type 0x0800 len 78
172.16.11.12:56758 -> 172.16.11.1:53 UDP


2010-07-06 23:16:22.193901 00:1f:f3:3c:e1:13 -> f8:1e:df:e5:84:3a type 0x0800 len 86
172.16.11.1:53 -> 172.16.11.12:51370 UDP


2010-07-06 23:16:22.196084 f8:1e:df:e5:84:3a -> 00:1f:f3:3c:e1:13 type 0x0800 len 78
172.16.11.12:51145 -> 172.16.11.1:53 UDP


2010-07-06 23:16:22.202223 00:1f:f3:3c:e1:13 -> f8:1e:df:e5:84:3a type 0x0800 len 94
172.16.11.1:53 -> 172.16.11.12:56758 UDP


2010-07-06 23:16:22.214655 00:1f:f3:3c:e1:13 -> f8:1e:df:e5:84:3a type 0x0800 len 78
172.16.11.1:53 -> 172.16.11.12:51145 UDP


2010-07-06 23:16:22.246264 00:1f:f3:3c:e1:13 -> f8:1e:df:e5:84:3a type 0x0800 len 97
172.16.11.1:53 -> 172.16.11.12:57360 UDP


2010-07-06 23:16:22.246309 f8:1e:df:e5:84:3a -> 00:1f:f3:3c:e1:13 type 0x0800 len 70
172.16.11.12 -> 172.16.11.1 ICMPv4
00000000  45 00 00 53 c1 97 00 00  40 11 4a d5 ac 10 0b 01  |E..S....@.J.....|
00000010  ac 10 0b 0c 00 35 e0 10  00 3f 00 00              |.....5...?..|
```

**3)**



```
00000050  30 31 30 20 30 32 3a 33  38 3a 31 35 20 47 4d 54  |010 02:38:15 GMT|
00000060  0d 0a 45 54 61 67 3a 20  22 31 36 65 39 33 33 2d  |..ETag: "16e933-|
00000070  31 30 33 61 2d 34 63 32  32 63 35 31 37 22 0d 0a  |103a-4c22c517"..|
00000080  43 61 63 68 65 2d 43 6f  6e 74 72 6f 6c 3a 20 70  |Cache-Control: p|
00000090  75 62 6c 69 63 2c 20 6d  61 78 2d 61 67 65 3d 34  |ublic, max-age=4|
000000a0  38 31 32 34 32 0d 0a 45  78 70 69 72 65 73 3a 20  |81242..Expires: |
000000b0  4d 6f 6e 2c 20 31 32 20  4a 75 6c 20 32 30 31 30  |Mon, 12 Jul 2010|
000000c0  20 31 36 3a 35 37 3a 30  33 20 47 4d 54 0d 0a 44  | 16:57:03 GMT..D|
000000d0  61 74 65 3a 20 57 65 64  2c 20 30 37 20 4a 75 6c  |ate: Wed, 07 Jul|
000000e0  20 32 30 31 30 20 30 33  3a 31 36 3a 32 31 20 47  | 2010 03:16:21 G|
000000f0  4d 54 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20  |MT..Connection: |
00000100  6b 65 65 70 2d 61 6c 69  76 65 0d 0a 0d 0a        |keep-alive....|


2010-07-06 23:16:21.609587 00:1f:f3:3c:e1:13 -> f8:1e:df:e5:84:3a type 0x0800 len 336
96.17.211.172:80 -> 172.16.11.12:64583 TCP PSH ACK
00000000  48 54 54 50 2f 31 2e 31  20 33 30 34 20 4e 6f 74  |HTTP/1.1 304 Not|
00000010  20 4d 6f 64 69 66 69 65  64 0d 0a 43 6f 6e 74 65  | Modified..Conte|
00000020  6e 74 2d 54 79 70 65 3a  20 69 6d 61 67 65 2f 70  |nt-Type: image/p|
00000030  6e 67 0d 0a 4c 61 73 74  2d 4d 6f 64 69 66 69 65  |ng..Last-Modifie|
00000040  64 3a 20 46 72 69 2c 20  30 32 20 4a 75 6c 20 32  |d: Fri, 02 Jul 2|
00000050  30 31 30 20 30 32 3a 34  35 3a 31 34 20 47 4d 54  |010 02:45:14 GMT|
00000060  0d 0a 45 54 61 67 3a 20  22 31 38 31 62 35 31 2d  |..ETag: "181b51-|
00000070  32 35 33 65 2d 34 63 32  64 35 32 62 61 22 0d 0a  |253e-4c2d52ba"..|
00000080  43 61 63 68 65 2d 43 6f  6e 74 72 6f 6c 3a 20 70  |Cache-Control: p|
00000090  75 62 6c 69 63 2c 20 6d  61 78 2d 61 67 65 3d 37  |ublic, max-age=7|
000000a0  37 35 39 32 39 0d 0a 45  78 70 69 72 65 73 3a 20  |75929..Expires: |
000000b0  46 72 69 2c 20 31 36 20  4a 75 6c 20 32 30 31 30  |Fri, 16 Jul 2010|
000000c0  20 30 32 3a 34 38 3a 33  30 20 47 4d 54 0d 0a 44  | 02:48:30 GMT..D|
000000d0  61 74 65 3a 20 57 65 64  2c 20 30 37 20 4a 75 6c  |ate: Wed, 07 Jul|
000000e0  20 32 30 31 30 20 30 33  3a 31 36 3a 32 31 20 47  | 2010 03:16:21 G|
000000f0  4d 54 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20  |MT..Connection: |
00000100  6b 65 65 70 2d 61 6c 69  76 65 0d 0a 0d 0a        |keep-alive....|
```