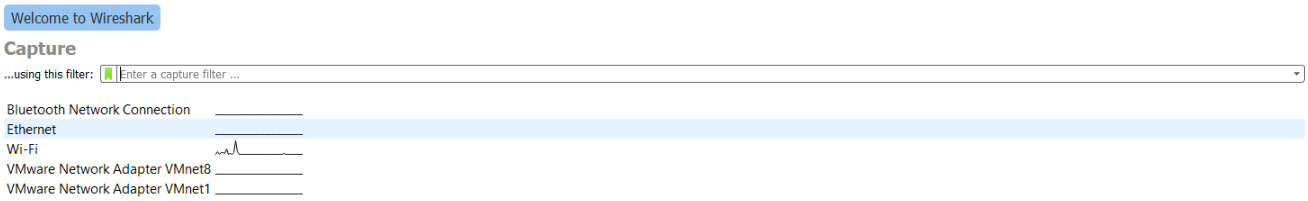
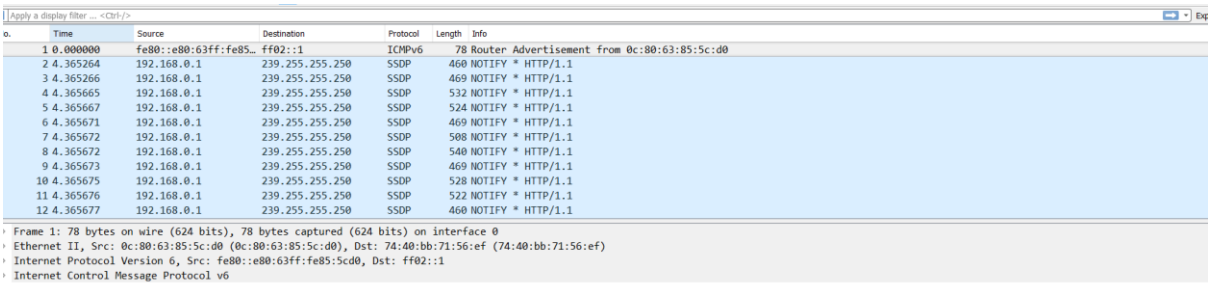
PROJECT -1 IP PACKET ANALYSIS USING WIRESHARK

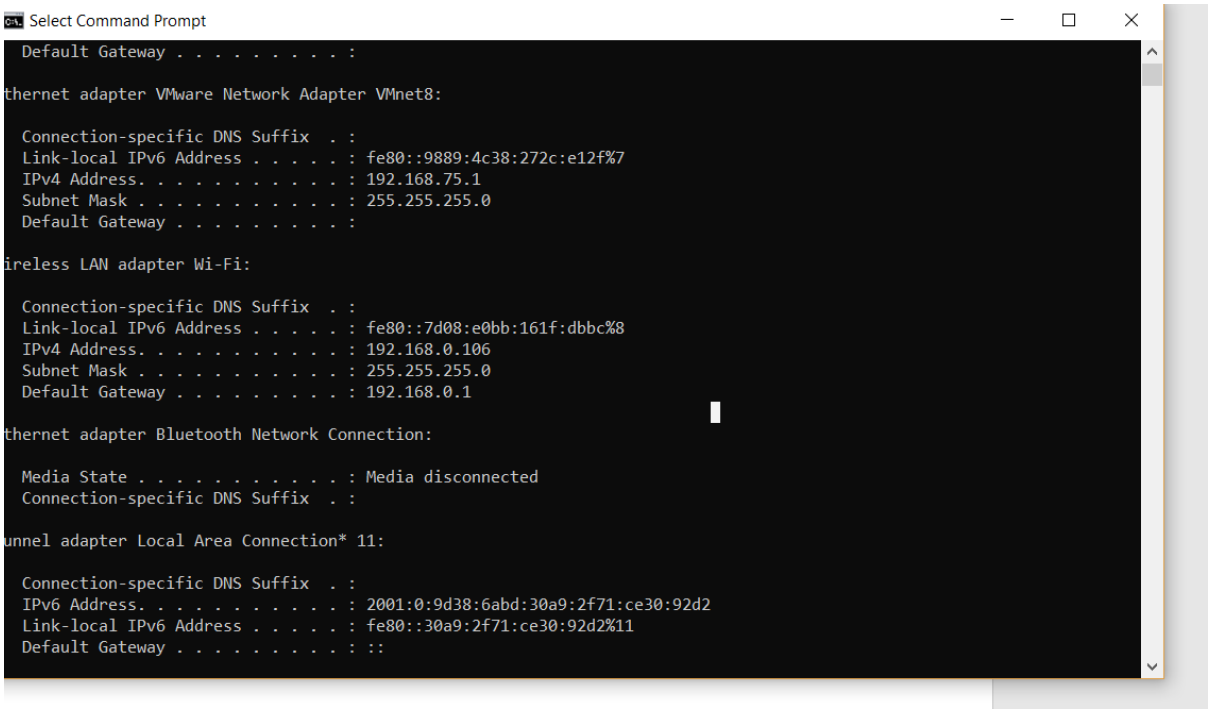
Step1-open wireshark (right click and run as administration)

Step2-click on the wifi option

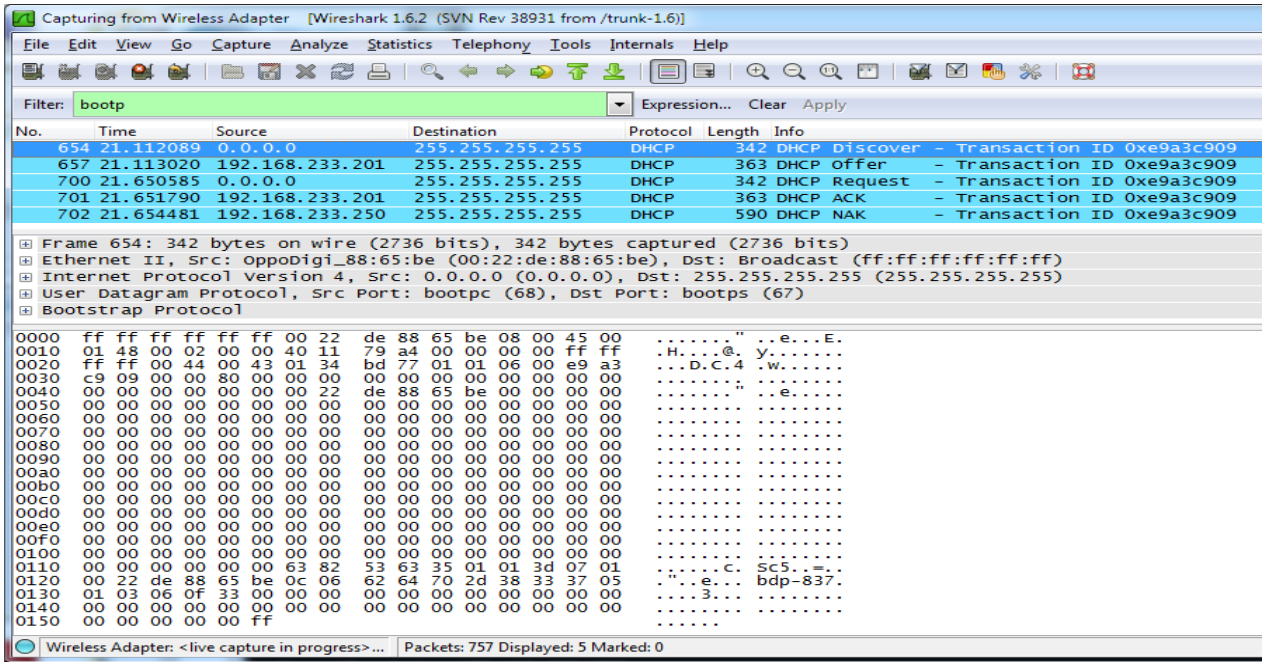




Step3- In the command prompt apply the ipconfig command



Step 4- In the filters tab apply the bootp filter (it captures only the DHCP traffic)



Here

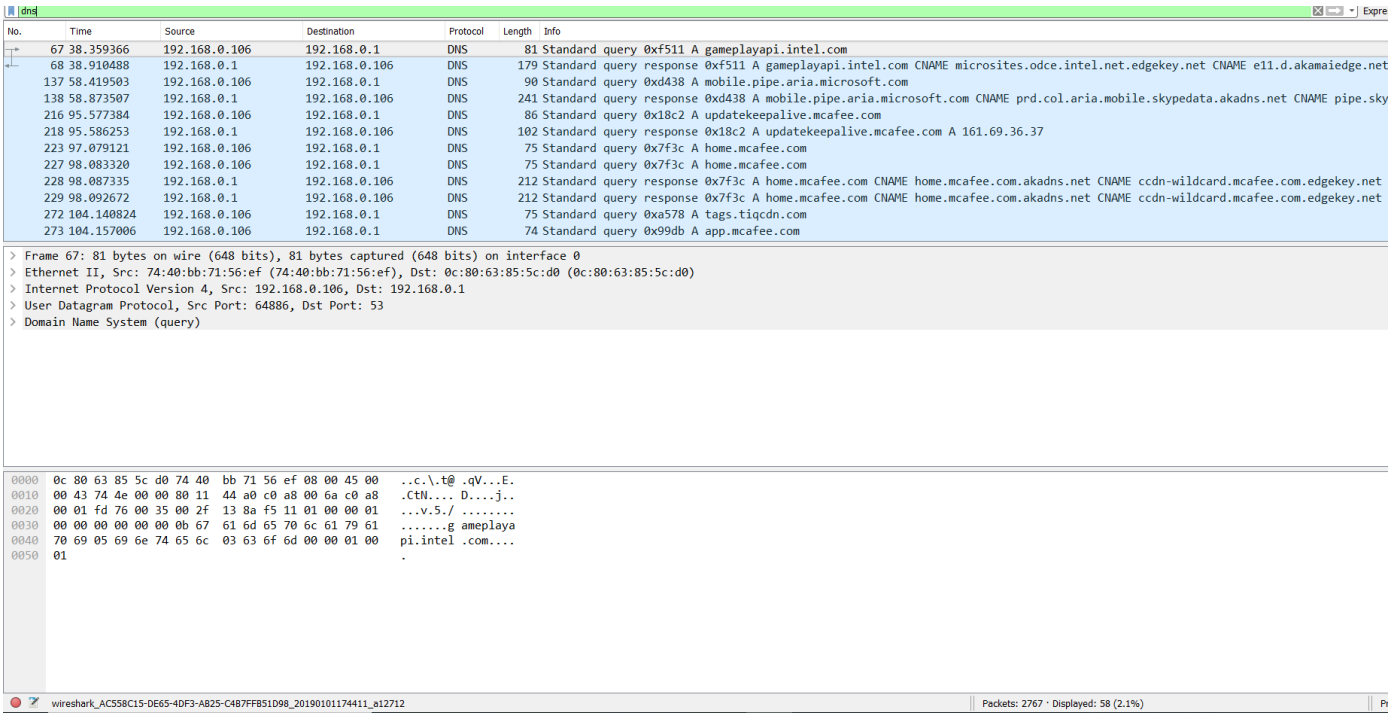
Discover is used to find the DHCP server

Offer is used to ask for the IPs

Request is used to assign IPs

Acknowledgment is used to give specific IPs

Step 5- Apply the dns filter in the filters tab



dns

No.	Time	Source	Destination	Protocol	Length	Info
67	38.359366	192.168.0.106	192.168.0.1	DNS	81	Standard query 0xf511 A gameplayapi.intel.com
68	38.910488	192.168.0.1	192.168.0.106	DNS	179	Standard query response 0xf511 A gameplayapi.intel.com CNAME microsites.odce.intel.net.ed
137	58.419503	192.168.0.106	192.168.0.1	DNS	90	Standard query 0xd438 A mobile.pipe.aria.microsoft.com
138	58.873507	192.168.0.1	192.168.0.106	DNS	241	Standard query response 0xd438 A mobile.pipe.aria.microsoft.com CNAME prd.col.aria.mobile
216	95.577384	192.168.0.106	192.168.0.1	DNS	86	Standard query 0x18c2 A updatekeepalive.mcafee.com
218	95.586253	192.168.0.1	192.168.0.106	DNS	102	Standard query response 0x18c2 A updatekeepalive.mcafee.com A 161.69.36.37
223	97.079121	192.168.0.106	192.168.0.1	DNS	75	Standard query 0x7f3c A home.mcafee.com
227	98.083320	192.168.0.106	192.168.0.1	DNS	75	Standard query 0x7f3c A home.mcafee.com
228	98.087335	192.168.0.1	192.168.0.106	DNS	212	Standard query response 0x7f3c A home.mcafee.com CNAME home.mcafee.com.akadns.net CNAME c
229	98.092672	192.168.0.1	192.168.0.106	DNS	212	Standard query response 0x7f3c A home.mcafee.com CNAME home.mcafee.com.akadns.net CNAME c
272	104.140824	192.168.0.106	192.168.0.1	DNS	75	Standard query 0xa578 A tags.tiqcdn.com
273	104.157006	192.168.0.106	192.168.0.1	DNS	74	Standard query 0x99db A app.mcafee.com

```
> Frame 67: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
> Ethernet II, Src: 74:40:bb:71:56:ef (74:40:bb:71:56:ef), Dst: 0c:80:63:85:5c:d0 (0c:80:63:85:5c:d0)
> Internet Protocol Version 4, Src: 192.168.0.106, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 64886, Dst Port: 53
v Domain Name System (query)
    [Response In: 68]
    Transaction ID: 0xf511
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
```

```
0000  0c 80 63 85 5c d0 74 40  bb 71 56 ef 08 00 45 00   ..c.\.t@ .qV...E.
0010  00 43 74 4e 00 00 80 11  44 a0 c0 a8 00 6a c0 a8   .CtN.... D....j..
0020  00 01 fd 76 00 35 00 2f  13 8a f5 11 01 00 00 01   ...v.5./ ........
0030  00 00 00 00 00 00 0b 67  61 6d 65 70 6c 61 79 61   .......g ameplaya
0040  70 69 05 69 6e 74 65 6c  03 63 6f 6d 00 00 01 00   pi.intel .com....
0050  01                                                .
```

Step6- Then apply the SSl filter

Ssl &&ip. address==

ssl && ip.addr==192.168.0.106

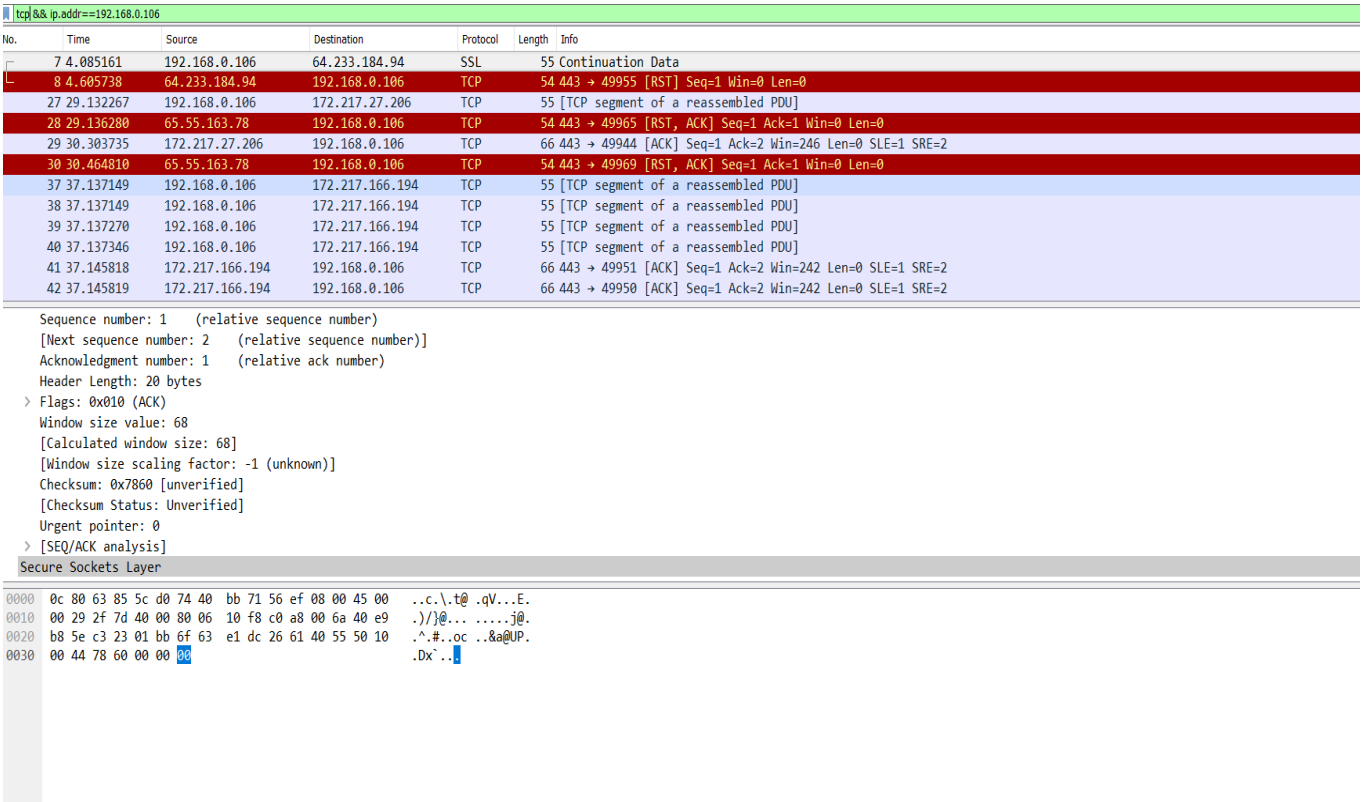
No.	Time	Source	Destination	Protocol	Length	Info
7	4.085161	192.168.0.106	64.233.184.94	SSL	55	Continuation Data
27	29.132267	192.168.0.106	172.217.27.206	TCP	55	[TCP segment of a reassembled PDU]
37	37.137149	192.168.0.106	172.217.166.194	TCP	55	[TCP segment of a reassembled PDU]
38	37.137149	192.168.0.106	172.217.166.194	TCP	55	[TCP segment of a reassembled PDU]
39	37.137270	192.168.0.106	172.217.166.194	TCP	55	[TCP segment of a reassembled PDU]
40	37.137346	192.168.0.106	172.217.166.194	TCP	55	[TCP segment of a reassembled PDU]
45	37.344814	192.168.0.106	172.217.166.194	TCP	55	[TCP segment of a reassembled PDU]
69	38.928151	192.168.0.106	161.69.226.21	TLSv1	443	Application Data
72	39.393112	161.69.226.21	192.168.0.106	TLSv1	155	Application Data
78	40.352754	192.168.0.106	23.56.24.24	TLSv1	179	Client Hello
80	40.753535	23.56.24.24	192.168.0.106	TLSv1	1494	Server Hello
81	40.753537	23.56.24.24	192.168.0.106	TLSv1	1494	Certificate[TCP segment of a reassembled PDU]

```
> Frame 7: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
> Ethernet II, Src: 74:40:bb:71:56:ef (74:40:bb:71:56:ef), Dst: 0c:80:63:85:5c:d0 (0c:80:63:85:5c:d0)
> Internet Protocol Version 4, Src: 192.168.0.106, Dst: 64.233.184.94
> Transmission Control Protocol, Src Port: 49955, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
  Secure Sockets Layer
```

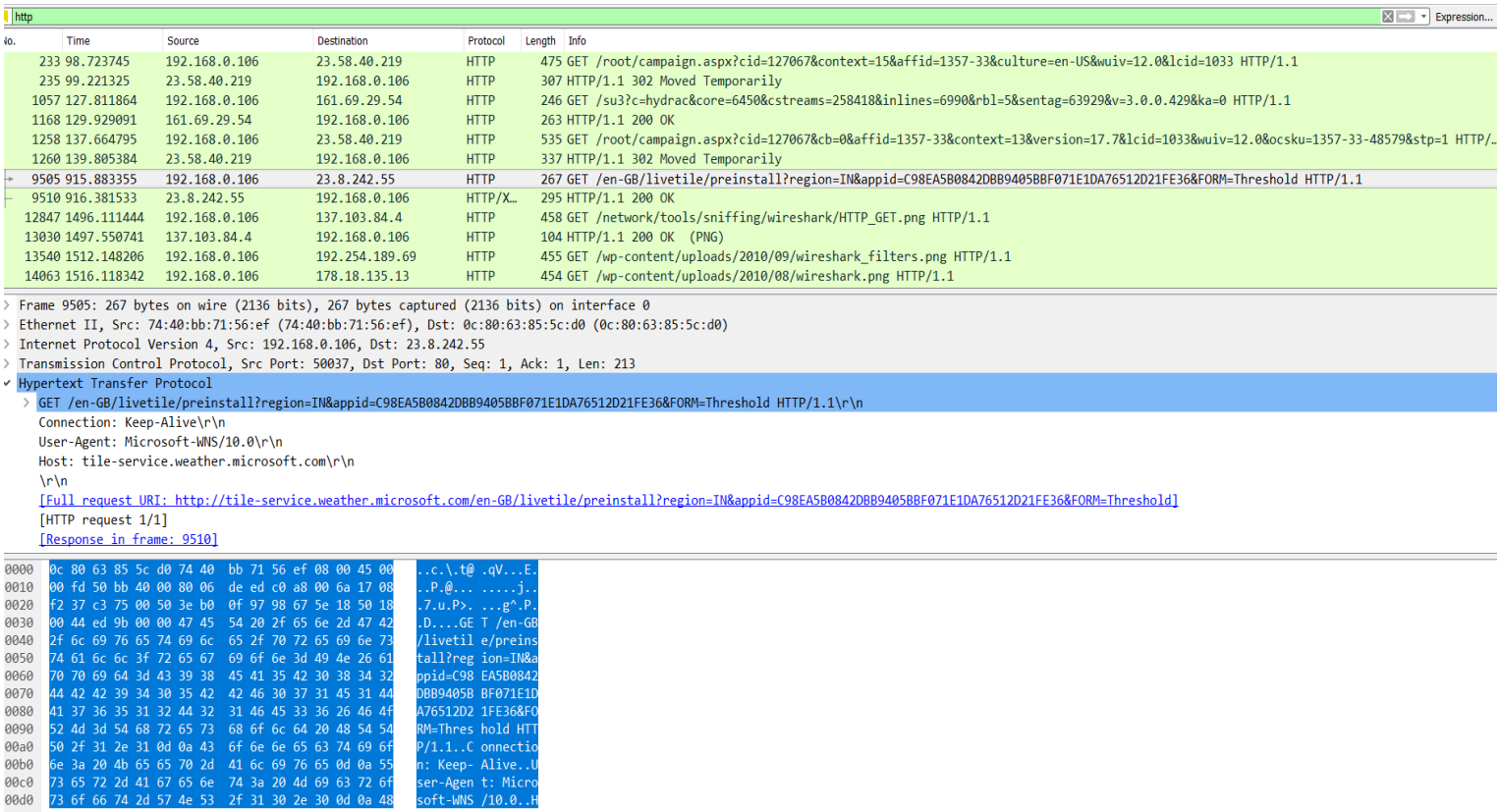
```
0000  0c 80 63 85 5c d0 74 40  bb 71 56 ef 08 00 45 00   ..c.\.t@ .qV...E.
0010  00 29 2f 7d 40 00 80 06  10 f8 c0 a8 00 6a 40 e9   .)/}@... .....j@.
0020  b8 5e c3 23 01 bb 6f 63  e1 dc 26 61 40 55 50 10   .^.#..oc ..&a@UP.
0030  00 44 78 60 00 00 00                              .Dx`...
```

Step 7- Apply the Tcp filter

TCP && ip.adder==



Step 8- Apply the Http filter


http
Expression...
No. Time Source Destination Protocol Length Info
233 98.723745 192.168.0.106 23.58.40.219 HTTP 475 GET /root/campaign.aspx?cid=127067&context=15&affid=1357-33&culture=en-US&wuiv=12.0&lcid=1033 HTTP/1.1
235 99.221325 23.58.40.219 192.168.0.106 HTTP 307 HTTP/1.1 302 Moved Temporarily
1057 127.811864 192.168.0.106 161.69.29.54 HTTP 246 GET /su3?c=hydrac&core=6450&cstreams=258418&inlines=6990&rbl=5&sentag=63929&v=3.0.0.429&ka=0 HTTP/1.1
1168 129.929091 161.69.29.54 192.168.0.106 HTTP 263 HTTP/1.1 200 OK
1258 137.664795 192.168.0.106 23.58.40.219 HTTP 535 GET /root/campaign.aspx?cid=127067&cb=0&affid=1357-33&context=13&version=17.7&lcid=1033&wuiv=12.0&ocsku=1357-33-48579&stp=1 HTTP/…
1260 139.805384 23.58.40.219 192.168.0.106 HTTP 337 HTTP/1.1 302 Moved Temporarily
9505 915.883355 192.168.0.106 23.8.242.55 HTTP 267 GET /en-GB/livetile/preinstall?region=IN&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold HTTP/1.1
9510 916.381533 23.8.242.55 192.168.0.106 HTTP/X… 295 HTTP/1.1 200 OK
12847 1496.111444 192.168.0.106 137.103.84.4 HTTP 458 GET /network/tools/sniffing/wireshark/HTTP_GET.png HTTP/1.1
13030 1497.550741 137.103.84.4 192.168.0.106 HTTP 104 HTTP/1.1 200 OK (PNG)
13540 1512.148206 192.168.0.106 192.254.189.69 HTTP 455 GET /wp-content/uploads/2010/09/wireshark_filters.png HTTP/1.1
14063 1516.118342 192.168.0.106 178.18.135.13 HTTP 454 GET /wp-content/uploads/2010/08/wireshark.png HTTP/1.1
Frame 9505: 267 bytes on wire (2136 bits), 267 bytes captured (2136 bits) on interface 0
Ethernet II, Src: 74:40:bb:71:56:ef (74:40:bb:71:56:ef), Dst: 0c:80:63:85:5c:d0 (0c:80:63:85:5c:d0)
Internet Protocol Version 4, Src: 192.168.0.106, Dst: 23.8.242.55
Transmission Control Protocol, Src Port: 50037, Dst Port: 80, Seq: 1, Ack: 1, Len: 213
Hypertext Transfer Protocol
GET /en-GB/livetile/preinstall?region=IN&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold HTTP/1.1\r\n
Connection: Keep-Alive\r\n
User-Agent: Microsoft-WNS/10.0\r\n
Host: tile-service.weather.microsoft.com\r\n
\r\n
[Full request URI: http://tile-service.weather.microsoft.com/en-GB/livetile/preinstall?region=IN&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold]
[HTTP request 1/1]
[Response in frame: 9510]
0000 0c 80 63 85 5c d0 74 40 bb 71 56 ef 08 00 45 00 ..c.\.t@ .qV...E.
0010 00 fd 50 bb 40 00 80 06 de ed c0 a8 00 6a 17 08 ..P.@... .....j..
0020 f2 37 c3 75 00 50 3e b0 0f 97 98 67 5e 18 50 18 .7.u.P>. ...g^.P.
0030 00 44 ed 9b 00 00 47 45 54 20 2f 65 6e 2d 47 42 .D....GE T /en-GB
0040 2f 6c 69 76 65 74 69 6c 65 2f 70 72 65 69 6e 73 /livetil e/preins
0050 74 61 6c 6c 3f 72 65 67 69 6f 6e 3d 49 4e 26 61 tall?reg ion=IN&a
0060 70 70 69 64 3d 43 39 38 45 41 35 42 30 38 34 32 ppid=C98 EA5B0842
0070 44 42 42 39 34 30 35 42 42 46 30 37 31 45 31 44 DBB9405B BF071E1D
0080 41 37 36 35 31 32 44 32 31 46 45 33 36 26 46 4f A76512D2 1FE36&FO
0090 52 4d 3d 54 68 72 65 73 68 6f 6c 64 20 48 54 54 RM=Thres hold HTT
00a0 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f P/1.1..C onnectio
00b0 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 55 n: Keep- Alive..U
00c0 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f ser-Agen t: Micro
00d0 73 6f 66 74 2d 57 4e 53 2f 31 30 2e 30 0d 0a 48 soft-WNS /10.0..H