LAB 3 - More on Wireshark and Introduction to Network Programming

NAME - DEV GOEL
ID - 2019A7PS0236G

Q 1. Generally, WireShark columns are arranged in following order (which you can observe on your machine): (0.75x6 = 4 marks)

No., Time, Source, Destination, Protocol, Length.

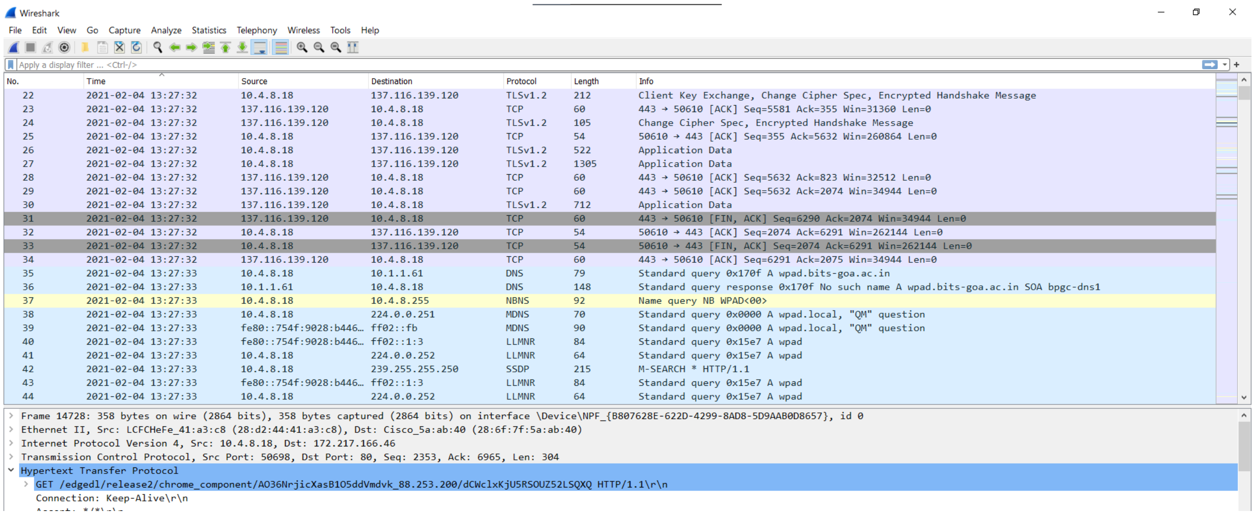
Being a security expert, and to have a better analysis, how do you arrange and add following columns in WireShark to display the information:

Date &amp;amp; time in UTC
Source IP and source port
Destination IP and destination port
HTTP host
HTTPS server
Info

Please include all relevant screenshots and also the final screenshot of your WireShark application.

Ans -

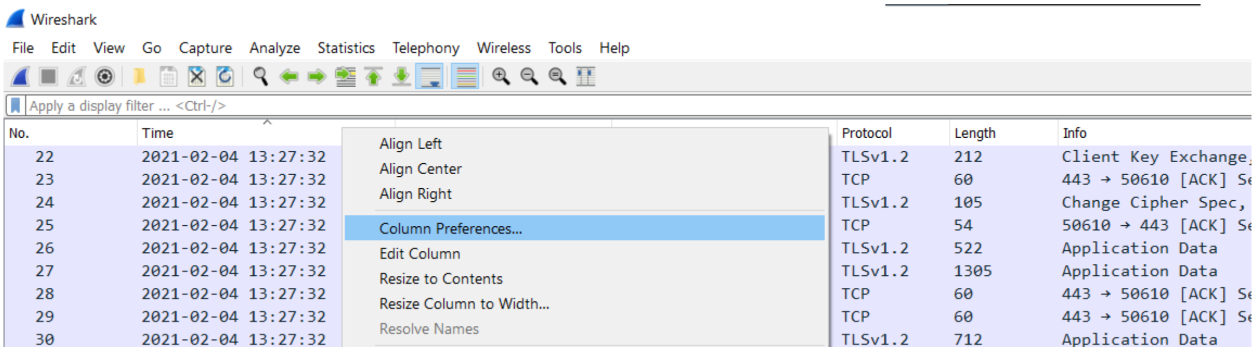
This is what the original window looks like.


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

No.	Time	Source	Destination	Protocol	Length	Info
22	2021-02-04 13:27:32	10.4.8.18	137.116.139.120	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
23	2021-02-04 13:27:32	137.116.139.120	10.4.8.18	TCP	60	443 → 50610 [ACK] Seq=5581 Ack=355 Win=31360 Len=0
24	2021-02-04 13:27:32	137.116.139.120	10.4.8.18	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
25	2021-02-04 13:27:32	10.4.8.18	137.116.139.120	TCP	54	50610 → 443 [ACK] Seq=355 Ack=5632 Win=260864 Len=0
26	2021-02-04 13:27:32	10.4.8.18	137.116.139.120	TLSv1.2	522	Application Data
27	2021-02-04 13:27:32	10.4.8.18	137.116.139.120	TLSv1.2	1305	Application Data
28	2021-02-04 13:27:32	137.116.139.120	10.4.8.18	TCP	60	443 → 50610 [ACK] Seq=5632 Ack=823 Win=32512 Len=0
29	2021-02-04 13:27:32	137.116.139.120	10.4.8.18	TCP	60	443 → 50610 [ACK] Seq=5632 Ack=2074 Win=34944 Len=0
30	2021-02-04 13:27:32	137.116.139.120	10.4.8.18	TLSv1.2	712	Application Data
31	2021-02-04 13:27:32	137.116.139.120	10.4.8.18	TCP	60	443 → 50610 [FIN, ACK] Seq=6290 Ack=2074 Win=34944 Len=0
32	2021-02-04 13:27:32	10.4.8.18	137.116.139.120	TCP	54	50610 → 443 [ACK] Seq=2074 Ack=6291 Win=262144 Len=0
33	2021-02-04 13:27:32	10.4.8.18	137.116.139.120	TCP	54	50610 → 443 [FIN, ACK] Seq=2074 Ack=6291 Win=262144 Len=0
34	2021-02-04 13:27:32	137.116.139.120	10.4.8.18	TCP	60	443 → 50610 [ACK] Seq=6291 Ack=2075 Win=34944 Len=0
35	2021-02-04 13:27:33	10.4.8.18	10.1.1.61	DNS	79	Standard query 0x170f A wpad.bits-goa.ac.in
36	2021-02-04 13:27:33	10.1.1.61	10.4.8.18	DNS	148	Standard query response 0x170f No such name A wpad.bits-goa.ac.in SOA bpgc-dns1
37	2021-02-04 13:27:33	10.4.8.18	10.4.8.255	NBNS	92	Name query NB WPAD<00>
38	2021-02-04 13:27:33	10.4.8.18	224.0.0.251	MDNS	70	Standard query 0x0000 A wpad.local, "QM" question
39	2021-02-04 13:27:33	fe80::754f:9028:b446…	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
40	2021-02-04 13:27:33	fe80::754f:9028:b446…	ff02::1:3	LLMNR	84	Standard query 0x15e7 A wpad
41	2021-02-04 13:27:33	10.4.8.18	224.0.0.252	LLMNR	64	Standard query 0x15e7 A wpad
42	2021-02-04 13:27:33	10.4.8.18	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
43	2021-02-04 13:27:33	fe80::754f:9028:b446…	ff02::1:3	LLMNR	84	Standard query 0x15e7 A wpad
44	2021-02-04 13:27:33	10.4.8.18	224.0.0.252	LLMNR	64	Standard query 0x15e7 A wpad

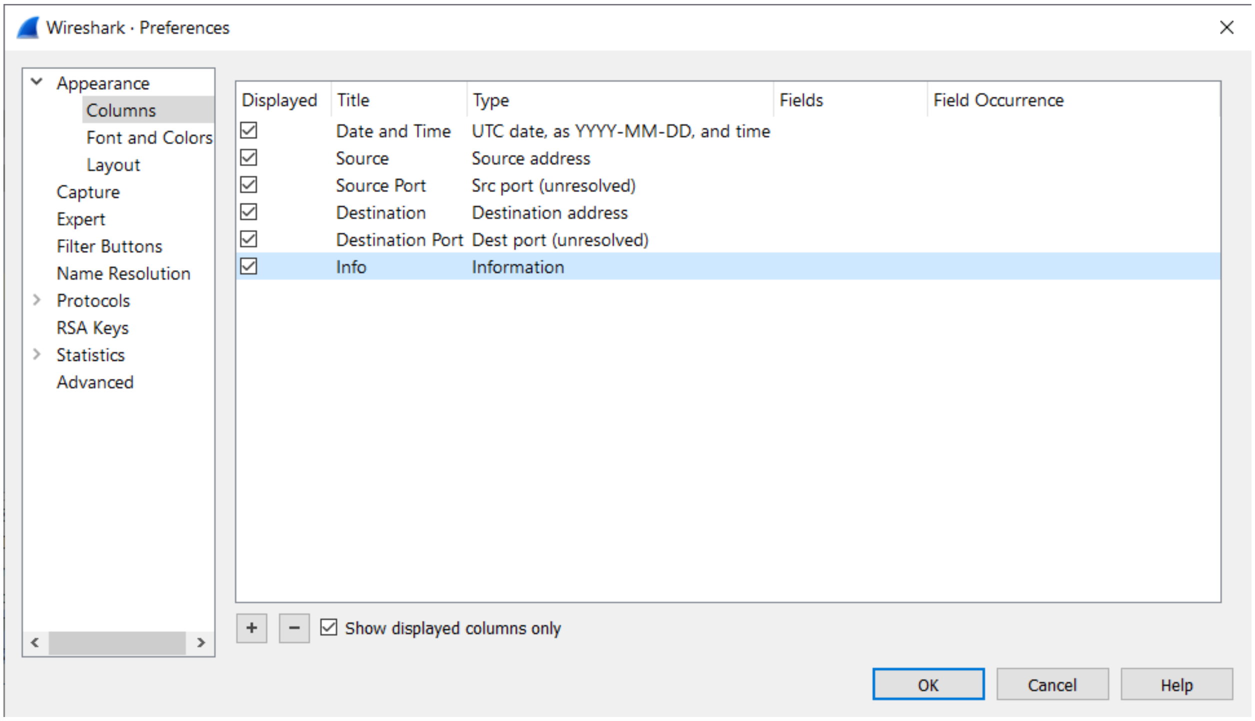
```
> Frame 14728: 358 bytes on wire (2864 bits), 358 bytes captured (2864 bits) on interface \Device\NPF_{B807628E-622D-4299-8AD8-5D9AAB0D8657}, id 0
> Ethernet II, Src: LCFCHeFe_41:a3:c8 (28:d2:44:41:a3:c8), Dst: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40)
> Internet Protocol Version 4, Src: 10.4.8.18, Dst: 172.217.166.46
> Transmission Control Protocol, Src Port: 50698, Dst Port: 80, Seq: 2353, Ack: 6965, Len: 304
v Hypertext Transfer Protocol
  > GET /edgedl/release2/chrome_component/AO36NrjicXasB1O5ddVmdvk_88.253.200/dCWclxKjU5RSOUZ52LSQXQ HTTP/1.1\r\n
    Connection: Keep-Alive\r\n
```

To add the given columns, we right click on the columns bar, and select **'Column Preferences'**:


Wireshark
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Align Left
Align Center
Align Right
Column Preferences...
Edit Column
Resize to Contents
Resize Column to Width...
Resolve Names

No.	Time	Protocol	Length	Info
22	2021-02-04 13:27:32	TLSv1.2	212	Client Key Exchange,
23	2021-02-04 13:27:32	TCP	60	443 → 50610 [ACK] Se
24	2021-02-04 13:27:32	TLSv1.2	105	Change Cipher Spec,
25	2021-02-04 13:27:32	TCP	54	50610 → 443 [ACK] Se
26	2021-02-04 13:27:32	TLSv1.2	522	Application Data
27	2021-02-04 13:27:32	TLSv1.2	1305	Application Data
28	2021-02-04 13:27:32	TCP	60	443 → 50610 [ACK] Se
29	2021-02-04 13:27:32	TCP	60	443 → 50610 [ACK] Se
30	2021-02-04 13:27:32	TLSv1.2	712	Application Data

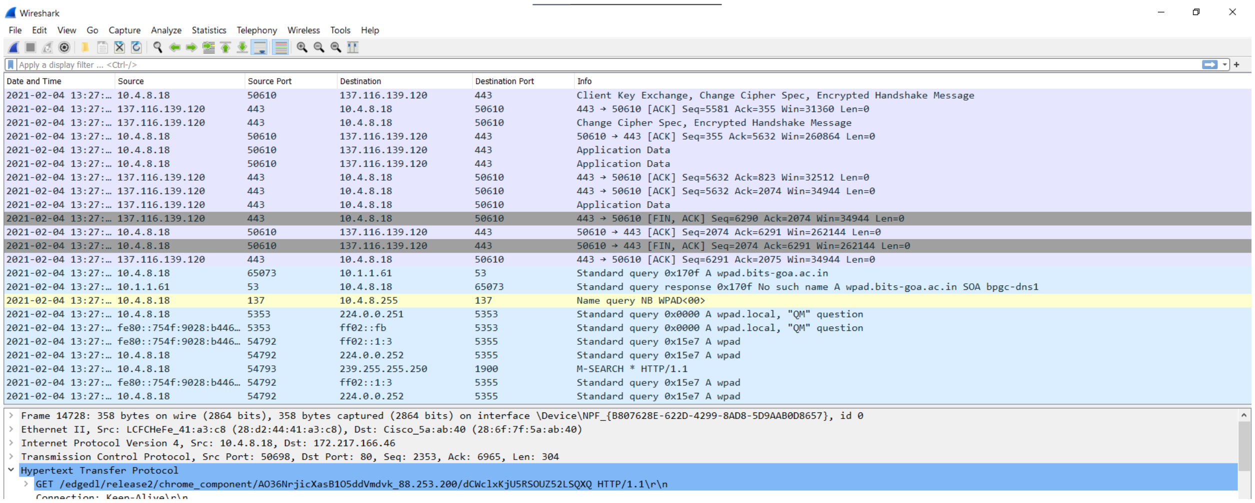
This opens the preferences window, where we add the required columns with their particular types using the **'+'** icons at the bottom of the window. The below screenshot shows the required columns after they have been added. We will add the **'HTTP Host'** and **'HTTPS Server'** columns later.



Displayed	Title	Type	Fields	Field Occurrence
☑	Date and Time	UTC date, as YYYY-MM-DD, and time		
☑	Source	Source address		
☑	Source Port	Src port (unresolved)		
☑	Destination	Destination address		
☑	Destination Port	Dest port (unresolved)		
☑	Info	Information		

☑ Show displayed columns only

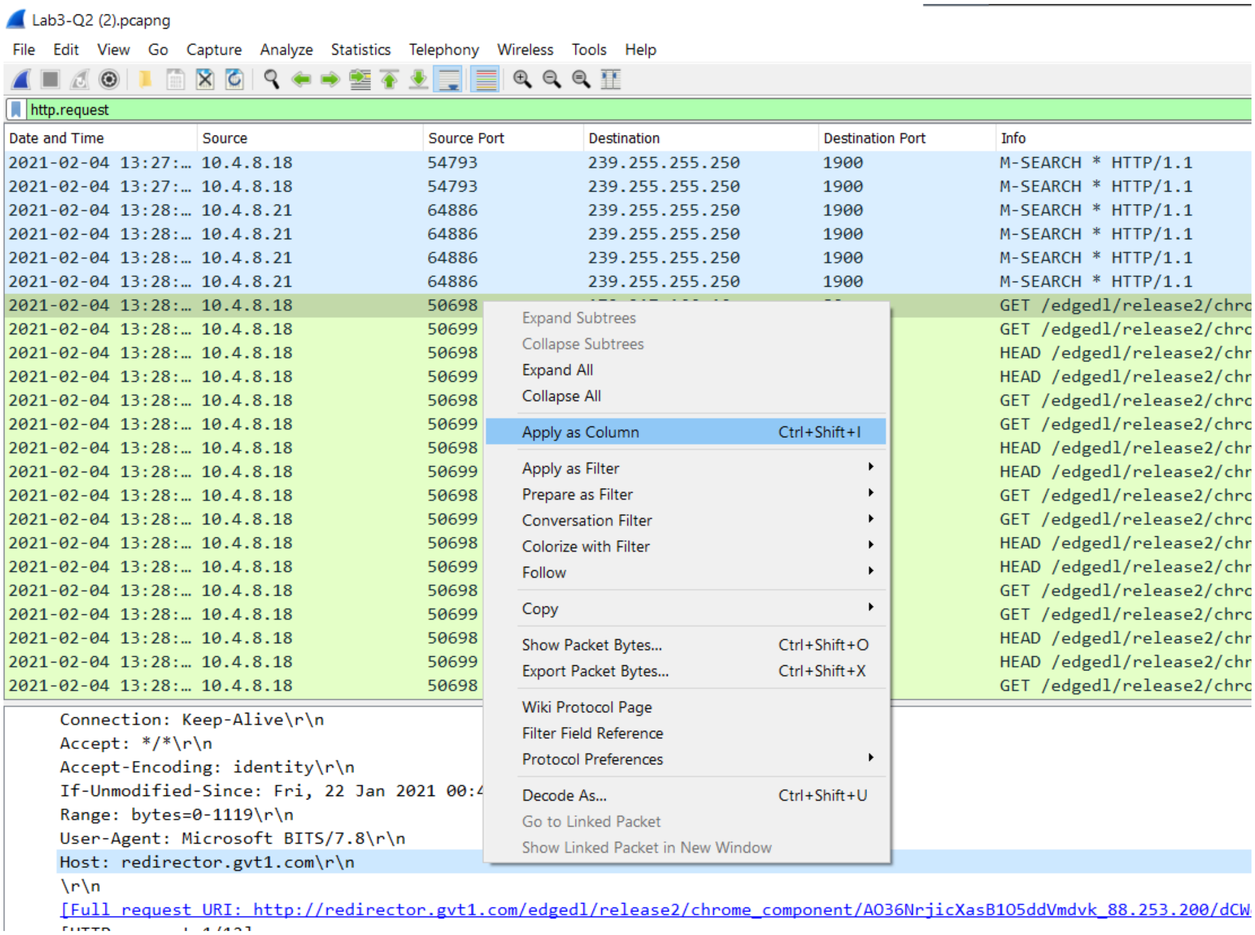
The window currently looks like this


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

```
Date and Time          Source                   Source Port  Destination      Destination Port  Info
2021-02-04 13:27:…  10.4.8.18                50610        137.116.139.120  443               Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2021-02-04 13:27:…  137.116.139.120          443          10.4.8.18        50610             443 → 50610 [ACK] Seq=5581 Ack=355 Win=31360 Len=0
2021-02-04 13:27:…  137.116.139.120          443          10.4.8.18        50610             Change Cipher Spec, Encrypted Handshake Message
2021-02-04 13:27:…  10.4.8.18                50610        137.116.139.120  443               50610 → 443 [ACK] Seq=355 Ack=5632 Win=260864 Len=0
2021-02-04 13:27:…  10.4.8.18                50610        137.116.139.120  443               Application Data
2021-02-04 13:27:…  10.4.8.18                50610        137.116.139.120  443               Application Data
2021-02-04 13:27:…  137.116.139.120          443          10.4.8.18        50610             443 → 50610 [ACK] Seq=5632 Ack=823 Win=32512 Len=0
2021-02-04 13:27:…  137.116.139.120          443          10.4.8.18        50610             443 → 50610 [ACK] Seq=5632 Ack=2074 Win=34944 Len=0
2021-02-04 13:27:…  137.116.139.120          443          10.4.8.18        50610             Application Data
2021-02-04 13:27:…  137.116.139.120          443          10.4.8.18        50610             443 → 50610 [FIN, ACK] Seq=6290 Ack=2074 Win=34944 Len=0
2021-02-04 13:27:…  10.4.8.18                50610        137.116.139.120  443               50610 → 443 [ACK] Seq=2074 Ack=6291 Win=262144 Len=0
2021-02-04 13:27:…  10.4.8.18                50610        137.116.139.120  443               50610 → 443 [FIN, ACK] Seq=2074 Ack=6291 Win=262144 Len=0
2021-02-04 13:27:…  137.116.139.120          443          10.4.8.18        50610             443 → 50610 [ACK] Seq=6291 Ack=2075 Win=34944 Len=0
2021-02-04 13:27:…  10.4.8.18                65073        10.1.1.61        53                Standard query 0x170f A wpad.bits-goa.ac.in
2021-02-04 13:27:…  10.1.1.61                53           10.4.8.18        65073             Standard query response 0x170f No such name A wpad.bits-goa.ac.in SOA bpgc-dns1
2021-02-04 13:27:…  10.4.8.18                137          10.4.8.255       137               Name query NB WPAD<00>
2021-02-04 13:27:…  10.4.8.18                5353         224.0.0.251      5353              Standard query 0x0000 A wpad.local, "QM" question
2021-02-04 13:27:…  fe80::754f:9028:b446…    5353         ff02::fb         5353              Standard query 0x0000 A wpad.local, "QM" question
2021-02-04 13:27:…  fe80::754f:9028:b446…    54792        ff02::1:3        5355              Standard query 0x15e7 A wpad
2021-02-04 13:27:…  10.4.8.18                54792        224.0.0.252      5355              Standard query 0x15e7 A wpad
2021-02-04 13:27:…  10.4.8.18                54793        239.255.255.250  1900              M-SEARCH * HTTP/1.1
2021-02-04 13:27:…  fe80::754f:9028:b446…    54792        ff02::1:3        5355              Standard query 0x15e7 A wpad
2021-02-04 13:27:…  10.4.8.18                54792        224.0.0.252      5355              Standard query 0x15e7 A wpad
```

```
> Frame 14728: 358 bytes on wire (2864 bits), 358 bytes captured (2864 bits) on interface \Device\NPF_{B807628E-622D-4299-8AD8-5D9AAB0D8657}, id 0
> Ethernet II, Src: LCFCHeFe_41:a3:c8 (28:d2:44:41:a3:c8), Dst: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40)
> Internet Protocol Version 4, Src: 10.4.8.18, Dst: 172.217.166.46
> Transmission Control Protocol, Src Port: 50698, Dst Port: 80, Seq: 2353, Ack: 6965, Len: 304
v Hypertext Transfer Protocol
  > GET /edgedl/release2/chrome_component/AO36NrjicXasB105ddVmdvk_88.253.200/dCWclxKjU5RSOUZ52LSQXQ HTTP/1.1\r\n
    Connection: Keep-Alive\r\n
```

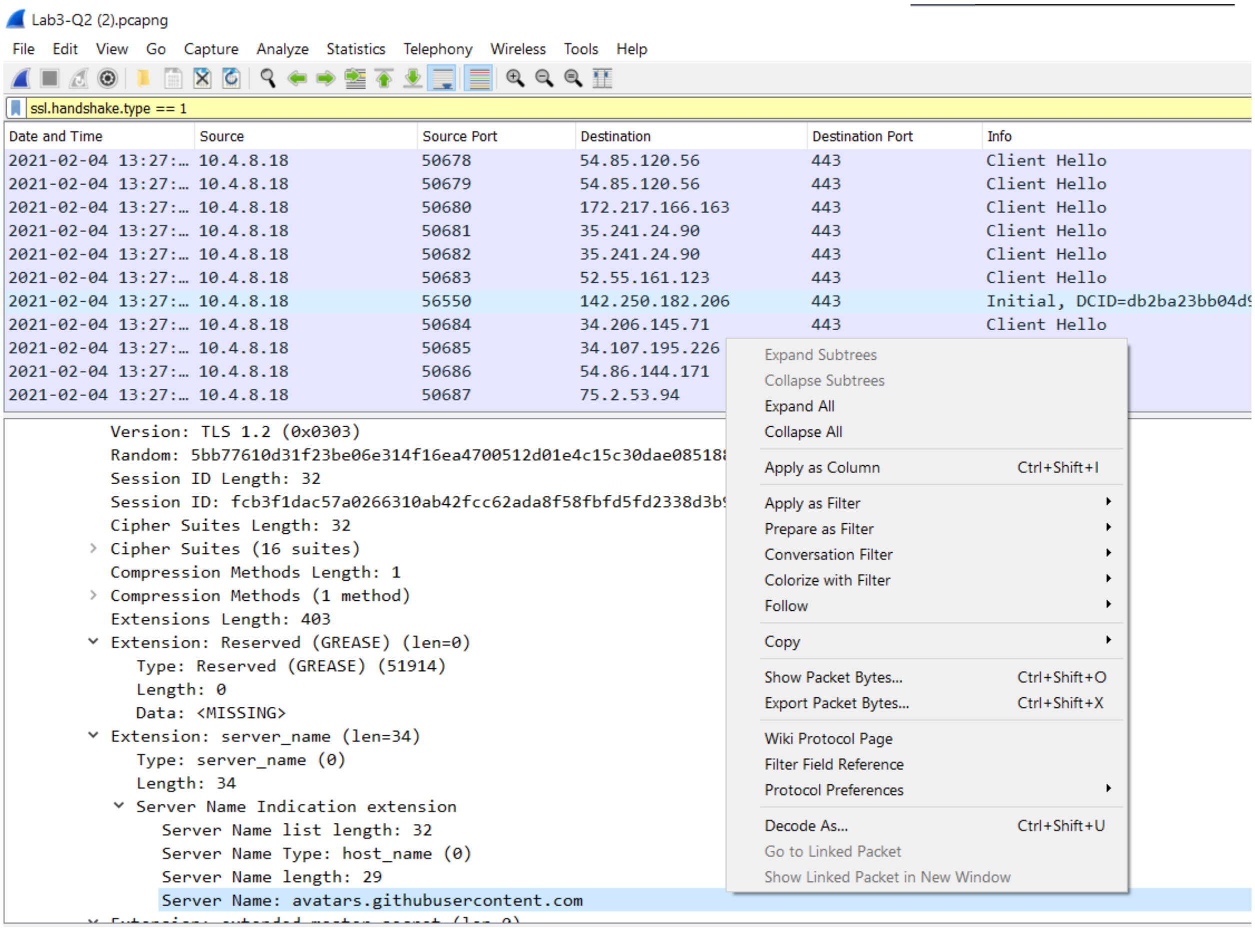
We now add the filter **‘http.request’** in the Wireshark filter window. Now, we select any packet and add the host as a column by right clicking **Host** in the frame details window, and selecting **‘Apply as Column’.**



```
Date and Time         Source      Source Port  Destination      Destination Port  Info
2021-02-04 13:27:…  10.4.8.18   54793        239.255.255.250  1900              M-SEARCH * HTTP/1.1
2021-02-04 13:27:…  10.4.8.18   54793        239.255.255.250  1900              M-SEARCH * HTTP/1.1
2021-02-04 13:28:…  10.4.8.21   64886        239.255.255.250  1900              M-SEARCH * HTTP/1.1
2021-02-04 13:28:…  10.4.8.21   64886        239.255.255.250  1900              M-SEARCH * HTTP/1.1
2021-02-04 13:28:…  10.4.8.21   64886        239.255.255.250  1900              M-SEARCH * HTTP/1.1
2021-02-04 13:28:…  10.4.8.21   64886        239.255.255.250  1900              M-SEARCH * HTTP/1.1
2021-02-04 13:28:…  10.4.8.18   50698                                            GET /edgedl/release2/chro
2021-02-04 13:28:…  10.4.8.18   50699                                            GET /edgedl/release2/chro
2021-02-04 13:28:…  10.4.8.18   50698                                            HEAD /edgedl/release2/chr
2021-02-04 13:28:…  10.4.8.18   50699                                            HEAD /edgedl/release2/chr
2021-02-04 13:28:…  10.4.8.18   50698                                            GET /edgedl/release2/chro
2021-02-04 13:28:…  10.4.8.18   50699                                            GET /edgedl/release2/chro
2021-02-04 13:28:…  10.4.8.18   50698                                            HEAD /edgedl/release2/chr
2021-02-04 13:28:…  10.4.8.18   50699                                            HEAD /edgedl/release2/chr
2021-02-04 13:28:…  10.4.8.18   50698                                            GET /edgedl/release2/chro
2021-02-04 13:28:…  10.4.8.18   50699                                            GET /edgedl/release2/chro
2021-02-04 13:28:…  10.4.8.18   50698                                            HEAD /edgedl/release2/chr
2021-02-04 13:28:…  10.4.8.18   50699                                            HEAD /edgedl/release2/chr
2021-02-04 13:28:…  10.4.8.18   50698                                            GET /edgedl/release2/chro
2021-02-04 13:28:…  10.4.8.18   50699                                            GET /edgedl/release2/chro
2021-02-04 13:28:…  10.4.8.18   50698                                            HEAD /edgedl/release2/chr
2021-02-04 13:28:…  10.4.8.18   50699                                            HEAD /edgedl/release2/chr
2021-02-04 13:28:…  10.4.8.18   50698                                            GET /edgedl/release2/chro
```

```
    Connection: Keep-Alive\r\n
    Accept: */*\r\n
    Accept-Encoding: identity\r\n
    If-Unmodified-Since: Fri, 22 Jan 2021 00:4
    Range: bytes=0-1119\r\n
    User-Agent: Microsoft BITS/7.8\r\n
    Host: redirector.gvt1.com\r\n
    \r\n
    [Full request URI: http://redirector.gvt1.com/edgedl/release2/chrome_component/AO36NrjicXasB105ddVmdvk_88.253.200/dCW
```

We now add the filter **‘ssl.handshake.type == 1’** in the Wireshark filter window. In the frame details window we expand the line **"Transport Layer Security".** Then expand the line for the ‘**TLS Record Layer’** and after that expand another line titled **‘Handshake Protocol: Client Hello’.** We select the **‘Server Name’** entry in the **‘Extension: server_name**’ by right clicking and selecting **‘Apply as Column’** option. This shows us the server entry for each packet.



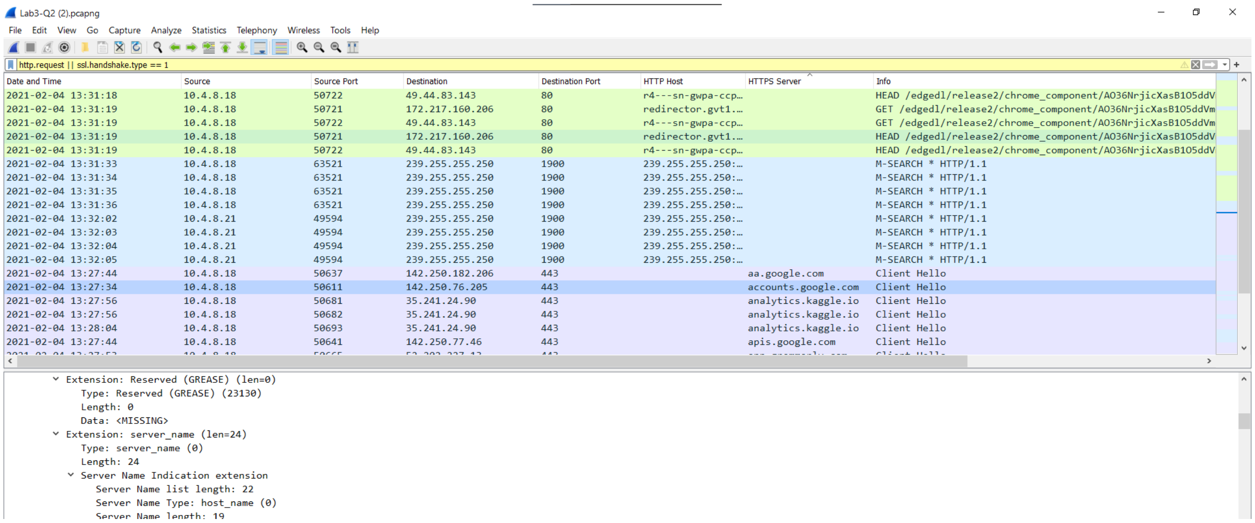
Lab3-Q2 (2).pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ssl.handshake.type == 1
```

```
Date and Time      Source        Source Port  Destination      Destination Port  Info
2021-02-04 13:27:… 10.4.8.18     50678        54.85.120.56     443               Client Hello
2021-02-04 13:27:… 10.4.8.18     50679        54.85.120.56     443               Client Hello
2021-02-04 13:27:… 10.4.8.18     50680        172.217.166.163  443               Client Hello
2021-02-04 13:27:… 10.4.8.18     50681        35.241.24.90     443               Client Hello
2021-02-04 13:27:… 10.4.8.18     50682        35.241.24.90     443               Client Hello
2021-02-04 13:27:… 10.4.8.18     50683        52.55.161.123    443               Client Hello
2021-02-04 13:27:… 10.4.8.18     56550        142.250.182.206  443               Initial, DCID=db2ba23bb04d
2021-02-04 13:27:… 10.4.8.18     50684        34.206.145.71    443               Client Hello
2021-02-04 13:27:… 10.4.8.18     50685        34.107.195.226
2021-02-04 13:27:… 10.4.8.18     50686        54.86.144.171
2021-02-04 13:27:… 10.4.8.18     50687        75.2.53.94
```

```
        Version: TLS 1.2 (0x0303)
        Random: 5bb77610d31f23be06e314f16ea4700512d01e4c15c30dae085188
        Session ID Length: 32
        Session ID: fcb3f1dac57a0266310ab42fcc62ada8f58fbfd5fd2338d3b
        Cipher Suites Length: 32
      > Cipher Suites (16 suites)
        Compression Methods Length: 1
      > Compression Methods (1 method)
        Extensions Length: 403
      ˅ Extension: Reserved (GREASE) (len=0)
          Type: Reserved (GREASE) (51914)
          Length: 0
          Data: <MISSING>
      ˅ Extension: server_name (len=34)
          Type: server_name (0)
          Length: 34
        ˅ Server Name Indication extension
            Server Name list length: 32
            Server Name Type: host_name (0)
            Server Name length: 29
            Server Name: avatars.githubusercontent.com
```

The final window looks like this



http.request || ssl.handshake.type == 1

Date and Time	Source	Source Port	Destination	Destination Port	HTTP Host	HTTPS Server	Info
2021-02-04 13:31:18	10.4.8.18	50722	49.44.83.143	80	r4---sn-gwpa-ccp…		HEAD /edgedl/release2/chrome_component/AO36NrjicXasB1O5ddV
2021-02-04 13:31:19	10.4.8.18	50721	172.217.160.206	80	redirector.gvt1.…		GET /edgedl/release2/chrome_component/AO36NrjicXasB1O5ddVm
2021-02-04 13:31:19	10.4.8.18	50722	49.44.83.143	80	r4---sn-gwpa-ccp…		GET /edgedl/release2/chrome_component/AO36NrjicXasB1O5ddVm
2021-02-04 13:31:19	10.4.8.18	50721	172.217.160.206	80	redirector.gvt1.…		HEAD /edgedl/release2/chrome_component/AO36NrjicXasB1O5ddV
2021-02-04 13:31:19	10.4.8.18	50722	49.44.83.143	80	r4---sn-gwpa-ccp…		HEAD /edgedl/release2/chrome_component/AO36NrjicXasB1O5ddV
2021-02-04 13:31:33	10.4.8.18	63521	239.255.255.250	1900	239.255.255.250:…		M-SEARCH * HTTP/1.1
2021-02-04 13:31:34	10.4.8.18	63521	239.255.255.250	1900	239.255.255.250:…		M-SEARCH * HTTP/1.1
2021-02-04 13:31:35	10.4.8.18	63521	239.255.255.250	1900	239.255.255.250:…		M-SEARCH * HTTP/1.1
2021-02-04 13:31:36	10.4.8.18	63521	239.255.255.250	1900	239.255.255.250:…		M-SEARCH * HTTP/1.1
2021-02-04 13:32:02	10.4.8.21	49594	239.255.255.250	1900	239.255.255.250:…		M-SEARCH * HTTP/1.1
2021-02-04 13:32:03	10.4.8.21	49594	239.255.255.250	1900	239.255.255.250:…		M-SEARCH * HTTP/1.1
2021-02-04 13:32:04	10.4.8.21	49594	239.255.255.250	1900	239.255.255.250:…		M-SEARCH * HTTP/1.1
2021-02-04 13:32:05	10.4.8.21	49594	239.255.255.250	1900	239.255.255.250:…		M-SEARCH * HTTP/1.1
2021-02-04 13:27:44	10.4.8.18	50637	142.250.182.206	443		aa.google.com	Client Hello
2021-02-04 13:27:34	10.4.8.18	50611	142.250.76.205	443		accounts.google.com	Client Hello
2021-02-04 13:27:56	10.4.8.18	50681	35.241.24.90	443		analytics.kaggle.io	Client Hello
2021-02-04 13:27:56	10.4.8.18	50682	35.241.24.90	443		analytics.kaggle.io	Client Hello
2021-02-04 13:28:04	10.4.8.18	50693	35.241.24.90	443		analytics.kaggle.io	Client Hello
2021-02-04 13:27:44	10.4.8.18	50641	142.250.77.46	443		apis.google.com	Client Hello

```
    ˅ Extension: Reserved (GREASE) (len=0)
        Type: Reserved (GREASE) (23130)
        Length: 0
        Data: <MISSING>
    ˅ Extension: server_name (len=24)
        Type: server_name (0)
        Length: 24
      ˅ Server Name Indication extension
          Server Name list length: 22
          Server Name Type: host_name (0)
          Server Name length: 19
```