CA3 Report

Registration no.: 11910417

Name: Resham Chandak

Course: 301

Question no. :27

Topic: Use a Wireshark tool to analyse your network at the microscopic level and investigate at least 10 protocols, read the live data from Bluetooth and USB

1. Introduction

1.1. **Objective of this project:** This project is done to capture protocols for Wi-Fi, Bluetooth, and USB. I will analyse network at the microscopic level. I will also read the live data from Bluetooth and USB.

1.2. **Description of the project:** In this project, I have captured 10 protocols for network. List of ***Wi-Fi protocols*** which I have captured are:

a) Transfer Control Protocol (TCP)

b) Domain Name System (DNS): It is the most important protocol. With this protocol, you can see open websites on the browser. If you want to see DNS only, then you must type DNS on the search bar of the Wireshark.

c) Hypertext Transfer Protocol (HTTP): Through this protocol, you can see server details if it is possible to see otherwise most of the websites do not allow us to see server details. Http websites like give http server details.

d) TLS

e) User Data Protocol (UDP): UDP is generally used for online video streaming. It is connectionless and unreliable.

f) TLSv1.2: TLSv1.2 sends server hello message or shows 'Application details' after TCP. It gives messages for Client Key exchange, Client Cipher Spec and Encrypted Handshake. It knows about encrypted message. But not able to see that data. It needs great practice in Cryptanalysis.

g) Simple Service Discovery Protocol (SSDP): SSDP’s info details are like this: 'M-SEARCH * HTTP/1.1'.

h) Multicast Domain System (MDNS): MDNS shows message regarding connection of Spotify.

i) Internet Control Message Protocol version 6 (ICMP v6): ICMP v6 is generally used for multicasting. It gives Neighbour Solicitation and Neighbour Advertisement messages.

j) Address Resolution Protocol (ARP): ARP asks question like this: 'Who is 192.168.209.248? Tell 192.168.209.81’. After that question it tells us the position of ipv4 address at 70.66.55.f3.53.87.

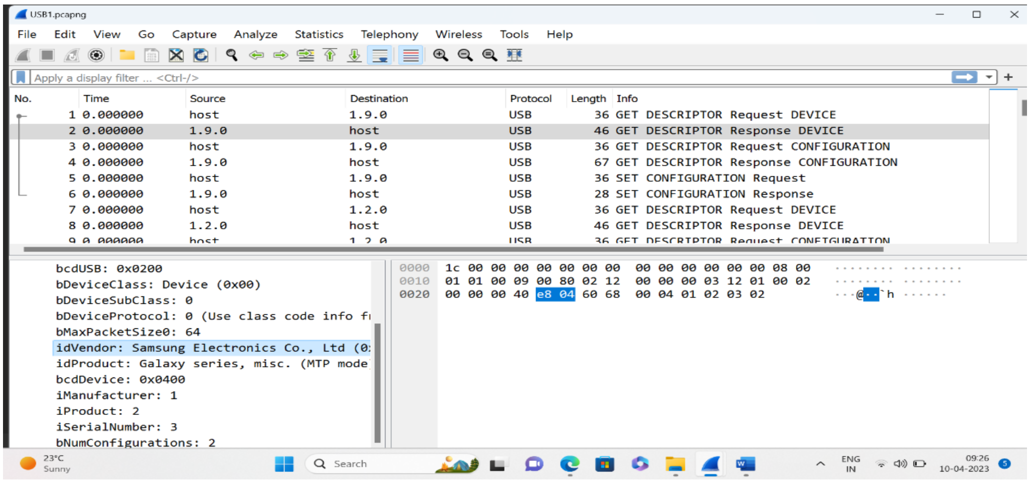
k) Online Certificate Status protocol (OCSP): OCSP generally gives message related to 'RESPONSE'. We can click on Follow TCP stream of it to know the server details.

l) NetBIOS Name Service (NBNS): NBNS gives information like ‘Registration NB WORKGROUP<00>’, ‘Name query NB WPAD<00>’, etc.

m) Dynamic Host Configuration Protocol (DHCP): DHCP gives information like ‘DHCP Request - Transaction ID 0xe4f49236’.

n) Internet Control Message Protocol v6 (ICMPv6): ICMPv6 is generally used for multicasting. It shows information like ‘Neighbor Advertisement fe80::7fb0:19e9:bdc4:60db (ovr) is at 20:68:9d:89:17:1d’.

After capturing Network protocols, I have captured USB protocols through USBPcap1. There were USB protocols only. In Second packet, we can see our mobile description as in Figure 1.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	host	1.9.0	USB	36	GET DESCRIPTOR Request DEVICE
2	0.000000	1.9.0	host	USB	46	GET DESCRIPTOR Response DEVICE
3	0.000000	host	1.9.0	USB	36	GET DESCRIPTOR Request CONFIGURATION
4	0.000000	1.9.0	host	USB	67	GET DESCRIPTOR Response CONFIGURATION
5	0.000000	host	1.9.0	USB	36	SET CONFIGURATION Request
6	0.000000	1.9.0	host	USB	28	SET CONFIGURATION Response
7	0.000000	host	1.2.0	USB	36	GET DESCRIPTOR Request DEVICE
8	0.000000	1.2.0	host	USB	46	GET DESCRIPTOR Response DEVICE
9	0.000000	host	1.2.0	USB	36	GET DESCRIPTOR Request CONFIGURATION

```
bcdUSB: 0x0200
bDeviceClass: Device (0x00)
bDeviceSubClass: 0
bDeviceProtocol: 0 (Use class code info fr
bMaxPacketSize0: 64
idVendor: Samsung Electronics Co., Ltd (0x
idProduct: Galaxy series, misc. (MTP mode
bcdDevice: 0x0400
iManufacturer: 1
iProduct: 2
iSerialNumber: 3
bNumConfigurations: 2
```

```
0000  1c 00 00 00 00 00 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  01 01 00 09 00 80 02 12  00 00 00 03 12 01 00 02   ········ ········
0020  00 00 00 40 e8 04 60 68  00 04 01 02 03 02         ···@··`h ······
```

Figure 1 Mobile Connection Success Image

USB protocols gives information regarding USB Request Block (URB). List of information (URB transfer type) in USB protocols with different packet nos.:

a. URB_BULK in: Receive data on a bulk pipe.
b. URB_INTERRUPT in: Receive data on an interrupt pipe.
c. URB_BULK out: Send data on a bulk pipe.
d. URB_INTERRUPT out: Send data on an interrupt pipe.
e. URB_ISOCHRONOUS in: Retrieve data from isochronous pipe.
f. URB_ISOCHRONOUS out: Send data to isochronous pipe.

After that I must capture Bluetooth protocols. I have done this with USBcap1. Here I have not connected any USB still USBPcap1 was working fine since I have connected my pc with mobile through Bluetooth. I have transferred one file to my mobile through Bluetooth. I was getting 5 protocols with my Bluetooth. List of Bluetooth Protocols:

a. Logical Link Control and Adaptation Protocol (L2CAP): L2CAP is a protocol used in the Bluetooth standard that operates just above the host-controller interface (HCI) passing data frames from the higher layers to either HCI or Link Manager.
b. HCI_EVT: HCI_EVT is a Bluetooth HCI Event. It
c. USB: It is shows device description and URB transfer type (E.g.: URB_BULK, URB_ISOCHRONOUS and URB_INTERRUPT) information.
d. HCI_CMD: HCI_CMD is a Bluetooth HCI Command.
e. HCI_USB: HCI_USB is a Bluetooth HCI USB Transport.
f. SDP:

1.3. Scope of the project: This project will help us in knowing protocols used in Wi-Fi, USB, and Bluetooth. We can configure the packets transfer processes in protocols. Some protocols will give us some information related to open websites in the browser.

2. System Description

2.1. **Target System Description:** Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible. You could think of a network packet analyzer as a measuring device for examining what’s happening inside a network cable, just like an electrician uses a voltmeter for examining what’s happening inside an electric cable. In the past, such tools were either very expensive, proprietary, or both. However, with the advent of

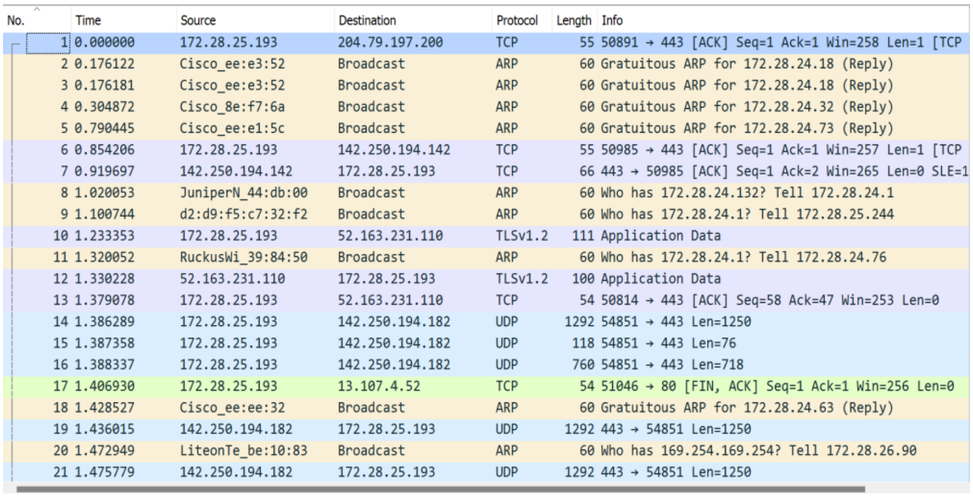
Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today. It is also used for capturing protocols for Bluetooth and USB using USBPcap.

3. Analysis Report

3.1. System snapshots and full analysis report:

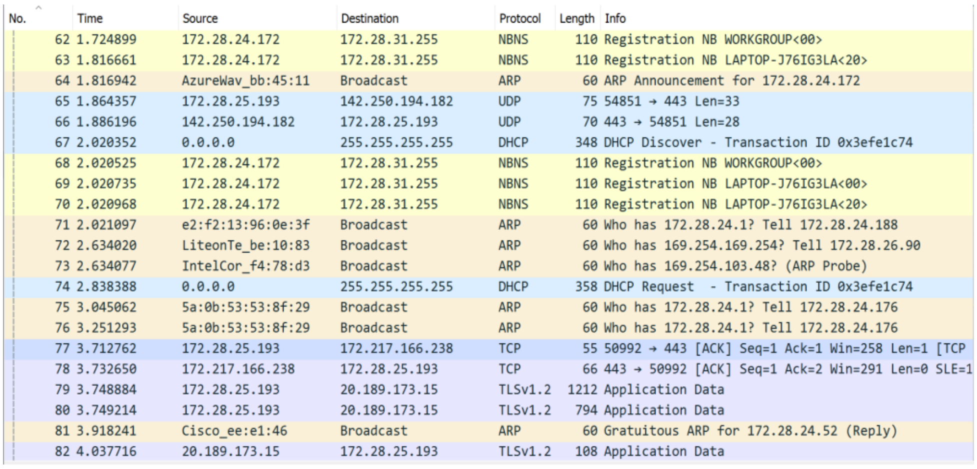
a) Wi-fi

Protocols Captured: TCP, ARP, TLSv1.2, UDP.



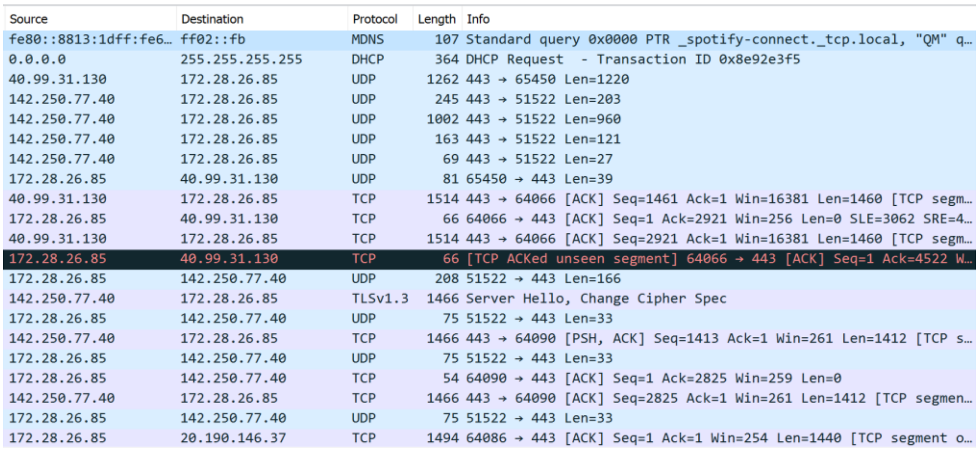
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.28.25.193	204.79.197.200	TCP	55	50891 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP
2	0.176122	Cisco_ee:e3:52	Broadcast	ARP	60	Gratuitous ARP for 172.28.24.18 (Reply)
3	0.176181	Cisco_ee:e3:52	Broadcast	ARP	60	Gratuitous ARP for 172.28.24.18 (Reply)
4	0.304872	Cisco_8e:f7:6a	Broadcast	ARP	60	Gratuitous ARP for 172.28.24.32 (Reply)
5	0.790445	Cisco_ee:e1:5c	Broadcast	ARP	60	Gratuitous ARP for 172.28.24.73 (Reply)
6	0.854206	172.28.25.193	142.250.194.142	TCP	55	50985 → 443 [ACK] Seq=1 Ack=1 Win=257 Len=1 [TCP
7	0.919697	142.250.194.142	172.28.25.193	TCP	66	443 → 50985 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1
8	1.020053	JuniperN_44:db:00	Broadcast	ARP	60	Who has 172.28.24.132? Tell 172.28.24.1
9	1.100744	d2:d9:f5:c7:32:f2	Broadcast	ARP	60	Who has 172.28.24.1? Tell 172.28.25.244
10	1.233353	172.28.25.193	52.163.231.110	TLSv1.2	111	Application Data
11	1.320052	RuckusWi_39:84:50	Broadcast	ARP	60	Who has 172.28.24.1? Tell 172.28.24.76
12	1.330228	52.163.231.110	172.28.25.193	TLSv1.2	100	Application Data
13	1.379078	172.28.25.193	52.163.231.110	TCP	54	50814 → 443 [ACK] Seq=58 Ack=47 Win=253 Len=0
14	1.386289	172.28.25.193	142.250.194.182	UDP	1292	54851 → 443 Len=1250
15	1.387358	172.28.25.193	142.250.194.182	UDP	118	54851 → 443 Len=76
16	1.388337	172.28.25.193	142.250.194.182	UDP	760	54851 → 443 Len=718
17	1.406930	172.28.25.193	13.107.4.52	TCP	54	51046 → 80 [FIN, ACK] Seq=1 Ack=1 Win=256 Len=0
18	1.428527	Cisco_ee:ee:32	Broadcast	ARP	60	Gratuitous ARP for 172.28.24.63 (Reply)
19	1.436015	142.250.194.182	172.28.25.193	UDP	1292	443 → 54851 Len=1250
20	1.472949	LiteonTe_be:10:83	Broadcast	ARP	60	Who has 169.254.169.254? Tell 172.28.26.90
21	1.475779	142.250.194.182	172.28.25.193	UDP	1292	443 → 54851 Len=1250

Protocols captured: NBNS, DHCP



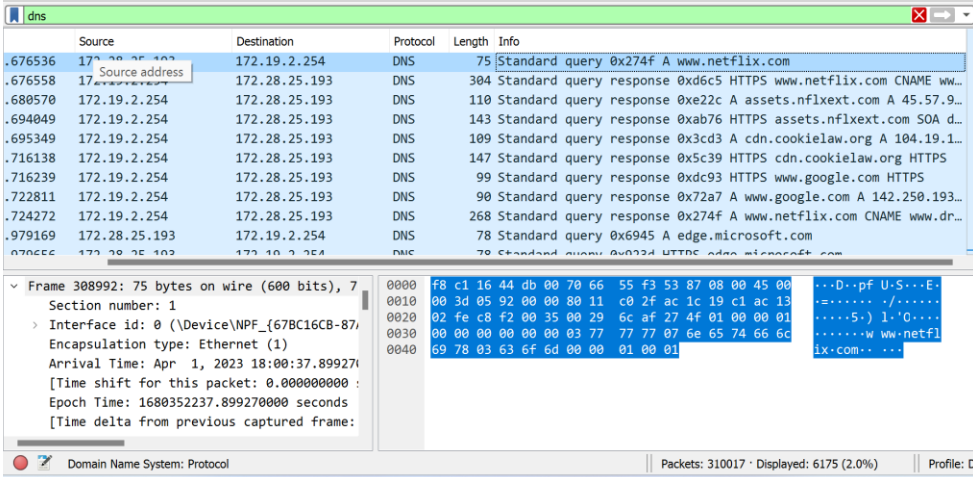
No.	Time	Source	Destination	Protocol	Length	Info
62	1.724899	172.28.24.172	172.28.31.255	NBNS	110	Registration NB WORKGROUP<00>
63	1.816661	172.28.24.172	172.28.31.255	NBNS	110	Registration NB LAPTOP-J76IG3LA<20>
64	1.816942	AzureWav_bb:45:11	Broadcast	ARP	60	ARP Announcement for 172.28.24.172
65	1.864357	172.28.25.193	142.250.194.182	UDP	75	54851 → 443 Len=33
66	1.886196	142.250.194.182	172.28.25.193	UDP	70	443 → 54851 Len=28
67	2.020352	0.0.0.0	255.255.255.255	DHCP	348	DHCP Discover - Transaction ID 0x3efe1c74
68	2.020525	172.28.24.172	172.28.31.255	NBNS	110	Registration NB WORKGROUP<00>
69	2.020735	172.28.24.172	172.28.31.255	NBNS	110	Registration NB LAPTOP-J76IG3LA<00>
70	2.020968	172.28.24.172	172.28.31.255	NBNS	110	Registration NB LAPTOP-J76IG3LA<20>
71	2.021097	e2:f2:13:96:0e:3f	Broadcast	ARP	60	Who has 172.28.24.1? Tell 172.28.24.188
72	2.634020	LiteonTe_be:10:83	Broadcast	ARP	60	Who has 169.254.169.254? Tell 172.28.26.90
73	2.634077	IntelCor_f4:78:d3	Broadcast	ARP	60	Who has 169.254.103.48? (ARP Probe)
74	2.838388	0.0.0.0	255.255.255.255	DHCP	358	DHCP Request - Transaction ID 0x3efe1c74
75	3.045062	5a:0b:53:53:8f:29	Broadcast	ARP	60	Who has 172.28.24.1? Tell 172.28.24.176
76	3.251293	5a:0b:53:53:8f:29	Broadcast	ARP	60	Who has 172.28.24.1? Tell 172.28.24.176
77	3.712762	172.28.25.193	172.217.166.238	TCP	55	50992 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP
78	3.732650	172.217.166.238	172.28.25.193	TCP	66	443 → 50992 [ACK] Seq=1 Ack=2 Win=291 Len=0 SLE=1
79	3.748884	172.28.25.193	20.189.173.15	TLSv1.2	1212	Application Data
80	3.749214	172.28.25.193	20.189.173.15	TLSv1.2	794	Application Data
81	3.918241	Cisco_ee:e1:46	Broadcast	ARP	60	Gratuitous ARP for 172.28.24.52 (Reply)
82	4.037716	20.189.173.15	172.28.25.193	TLSv1.2	108	Application Data

Protocols captured: MDNS.



Source	Destination	Protocol	Length	Info
fe80::8813:1dff:fe6…	ff02::fb	MDNS	107	Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" q…
0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x8e92e3f5
40.99.31.130	172.28.26.85	UDP	1262	443 → 65450 Len=1220
142.250.77.40	172.28.26.85	UDP	245	443 → 51522 Len=203
142.250.77.40	172.28.26.85	UDP	1002	443 → 51522 Len=960
142.250.77.40	172.28.26.85	UDP	163	443 → 51522 Len=121
142.250.77.40	172.28.26.85	UDP	69	443 → 51522 Len=27
172.28.26.85	40.99.31.130	UDP	81	65450 → 443 Len=39
40.99.31.130	172.28.26.85	TCP	1514	443 → 64066 [ACK] Seq=1461 Ack=1 Win=16381 Len=1460 [TCP segm…
172.28.26.85	40.99.31.130	TCP	66	64066 → 443 [ACK] Seq=1 Ack=2921 Win=256 Len=0 SLE=3062 SRE=4…
40.99.31.130	172.28.26.85	TCP	1514	443 → 64066 [ACK] Seq=2921 Ack=1 Win=16381 Len=1460 [TCP segm…
172.28.26.85	40.99.31.130	TCP	66	[TCP ACKed unseen segment] 64066 → 443 [ACK] Seq=1 Ack=4522 W…
172.28.26.85	142.250.77.40	UDP	208	51522 → 443 Len=166
142.250.77.40	172.28.26.85	TLSv1.3	1466	Server Hello, Change Cipher Spec
172.28.26.85	142.250.77.40	UDP	75	51522 → 443 Len=33
142.250.77.40	172.28.26.85	TCP	1466	443 → 64090 [PSH, ACK] Seq=1413 Ack=1 Win=261 Len=1412 [TCP s…
172.28.26.85	142.250.77.40	UDP	75	51522 → 443 Len=33
172.28.26.85	142.250.77.40	TCP	54	64090 → 443 [ACK] Seq=1 Ack=2825 Win=259 Len=0
142.250.77.40	172.28.26.85	TCP	1466	443 → 64090 [ACK] Seq=2825 Ack=1 Win=261 Len=1412 [TCP segmen…
172.28.26.85	142.250.77.40	UDP	75	51522 → 443 Len=33
172.28.26.85	20.190.146.37	TCP	1494	64086 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1440 [TCP segment o…

Protocols captured: DNS.



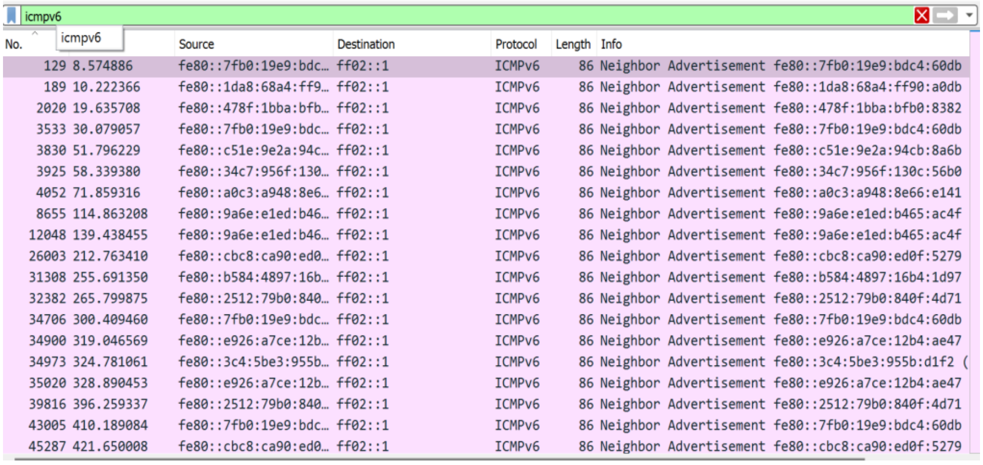
	Source	Destination	Protocol	Length	Info
.676536	172.28.25.193	172.19.2.254	DNS	75	Standard query 0x274f A www.netflix.com
.676558	172.19.2.254	172.28.25.193	DNS	304	Standard query response 0xd6c5 HTTPS www.netflix.com CNAME ww…
.680570	172.19.2.254	172.28.25.193	DNS	110	Standard query response 0xe22c A assets.nflxext.com A 45.57.9…
.694049	172.19.2.254	172.28.25.193	DNS	143	Standard query response 0xab76 HTTPS assets.nflxext.com SOA d…
.695349	172.19.2.254	172.28.25.193	DNS	109	Standard query response 0x3cd3 A cdn.cookielaw.org A 104.19.1…
.716138	172.19.2.254	172.28.25.193	DNS	147	Standard query response 0x5c39 HTTPS cdn.cookielaw.org HTTPS
.716239	172.19.2.254	172.28.25.193	DNS	99	Standard query response 0xdc93 HTTPS www.google.com HTTPS
.722811	172.19.2.254	172.28.25.193	DNS	90	Standard query response 0x72a7 A www.google.com A 142.250.193…
.724272	172.19.2.254	172.28.25.193	DNS	268	Standard query response 0x274f A www.netflix.com CNAME www.dr…
.979169	172.28.25.193	172.19.2.254	DNS	78	Standard query 0x6945 A edge.microsoft.com
.979656	172.28.25.193	172.19.2.254	DNS	78	Standard query 0x923d HTTPS edge.microsoft.com

```
⌄ Frame 308992: 75 bytes on wire (600 bits), 7
     Section number: 1
   › Interface id: 0 (\Device\NPF_{67BC16CB-87
     Encapsulation type: Ethernet (1)
     Arrival Time: Apr  1, 2023 18:00:37.89927
     [Time shift for this packet: 0.000000000
     Epoch Time: 1680352237.899270000 seconds
     [Time delta from previous captured frame:
```

```
0000  f8 c1 16 44 db 00 70 66  55 f3 53 87 08 00 45 00   ···D··pf U·S···E·
0010  00 3d 05 92 00 00 80 11  c0 2f ac 1c 19 c1 ac 13   ·=······ ·/······
0020  02 fe c8 f2 00 35 00 29  6c af 27 4f 01 00 00 01   ·····5·) l·'O····
0030  00 00 00 00 00 00 03 77  77 77 07 6e 65 74 66 6c   ·······w ww·netfl
0040  69 78 03 63 6f 6d 00 00  01 00 01                  ix·com·· ···
```

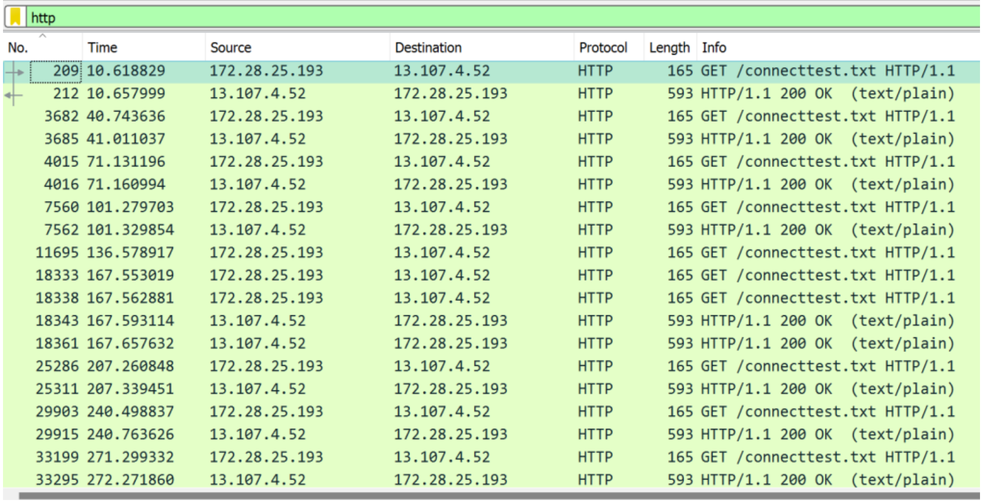
Domain Name System: Protocol   Packets: 310017 · Displayed: 6175 (2.0%)   Profile: D

Protocols captured: ICMPv6.



No.		Source	Destination	Protocol	Length	Info
129	8.574886	fe80::7fb0:19e9:bdc…	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::7fb0:19e9:bdc4:60db
189	10.222366	fe80::1da8:68a4:ff9…	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::1da8:68a4:ff90:a0db
2020	19.635708	fe80::478f:1bba:bfb…	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::478f:1bba:bfb0:8382
3533	30.079057	fe80::7fb0:19e9:bdc…	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::7fb0:19e9:bdc4:60db
3830	51.796229	fe80::c51e:9e2a:94c…	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::c51e:9e2a:94cb:8a6b
3925	58.339380	fe80::34c7:956f:130…	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::34c7:956f:130c:56b0
4052	71.859316	fe80::a0c3:a948:8e6…	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::a0c3:a948:8e66:e141
8655	114.863208	fe80::9a6e:e1ed:b46…	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::9a6e:e1ed:b465:ac4f
12048	139.438455	fe80::9a6e:e1ed:b46…	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::9a6e:e1ed:b465:ac4f
26003	212.763410	fe80::cbc8:ca90:ed0…	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::cbc8:ca90:ed0f:5279
31308	255.691350	fe80::b584:4897:16b…	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::b584:4897:16b4:1d97
32382	265.799875	fe80::2512:79b0:840…	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::2512:79b0:840f:4d71
34706	300.409460	fe80::7fb0:19e9:bdc…	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::7fb0:19e9:bdc4:60db
34900	319.046569	fe80::e926:a7ce:12b…	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::e926:a7ce:12b4:ae47
34973	324.781061	fe80::3c4:5be3:955b…	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::3c4:5be3:955b:d1f2 (
35020	328.890453	fe80::e926:a7ce:12b…	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::e926:a7ce:12b4:ae47
39816	396.259337	fe80::2512:79b0:840…	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::2512:79b0:840f:4d71
43005	410.189084	fe80::7fb0:19e9:bdc…	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::7fb0:19e9:bdc4:60db
45287	421.650008	fe80::cbc8:ca90:ed0…	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::cbc8:ca90:ed0f:5279

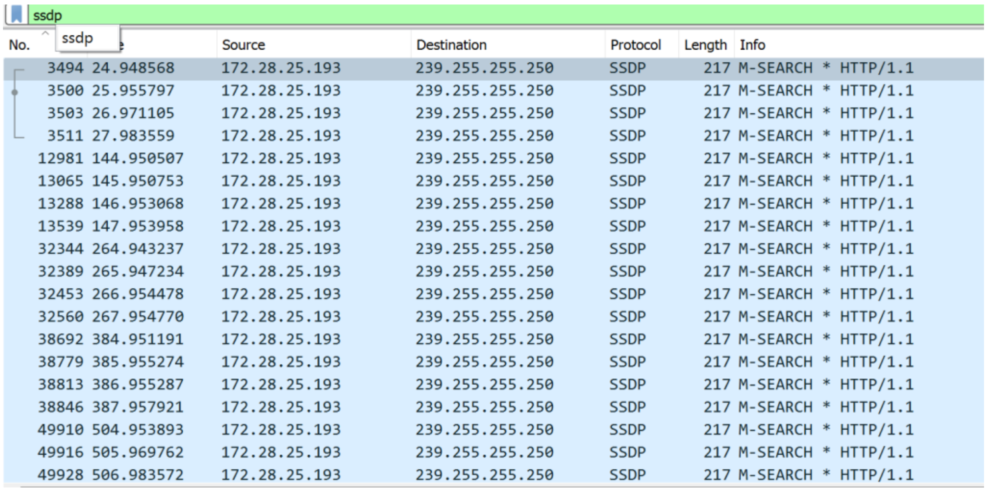
Protocols captured: HTTP



http

No.	Time	Source	Destination	Protocol	Length	Info
209	10.618829	172.28.25.193	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
212	10.657999	13.107.4.52	172.28.25.193	HTTP	593	HTTP/1.1 200 OK (text/plain)
3682	40.743636	172.28.25.193	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
3685	41.011037	13.107.4.52	172.28.25.193	HTTP	593	HTTP/1.1 200 OK (text/plain)
4015	71.131196	172.28.25.193	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
4016	71.160994	13.107.4.52	172.28.25.193	HTTP	593	HTTP/1.1 200 OK (text/plain)
7560	101.279703	172.28.25.193	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
7562	101.329854	13.107.4.52	172.28.25.193	HTTP	593	HTTP/1.1 200 OK (text/plain)
11695	136.578917	172.28.25.193	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
18333	167.553019	172.28.25.193	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
18338	167.562881	172.28.25.193	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
18343	167.593114	13.107.4.52	172.28.25.193	HTTP	593	HTTP/1.1 200 OK (text/plain)
18361	167.657632	13.107.4.52	172.28.25.193	HTTP	593	HTTP/1.1 200 OK (text/plain)
25286	207.260848	172.28.25.193	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
25311	207.339451	13.107.4.52	172.28.25.193	HTTP	593	HTTP/1.1 200 OK (text/plain)
29903	240.498837	172.28.25.193	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
29915	240.763626	13.107.4.52	172.28.25.193	HTTP	593	HTTP/1.1 200 OK (text/plain)
33199	271.299332	172.28.25.193	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
33295	272.271860	13.107.4.52	172.28.25.193	HTTP	593	HTTP/1.1 200 OK (text/plain)

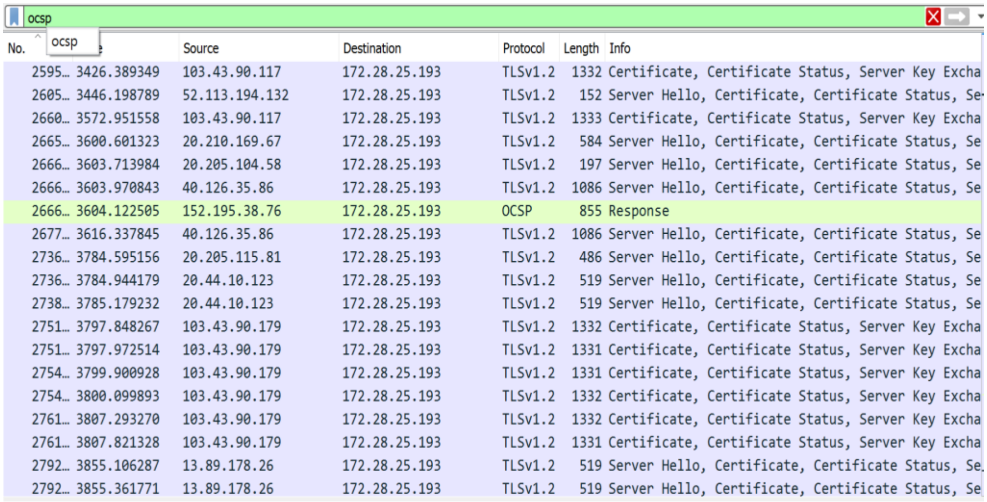
Protocols captured: SSDP



ssdp

No.	ssdp	Source	Destination	Protocol	Length	Info
3494	24.948568	172.28.25.193	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
3500	25.955797	172.28.25.193	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
3503	26.971105	172.28.25.193	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
3511	27.983559	172.28.25.193	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
12981	144.950507	172.28.25.193	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
13065	145.950753	172.28.25.193	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
13288	146.953068	172.28.25.193	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
13539	147.953958	172.28.25.193	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
32344	264.943237	172.28.25.193	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
32389	265.947234	172.28.25.193	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
32453	266.954478	172.28.25.193	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
32560	267.954770	172.28.25.193	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
38692	384.951191	172.28.25.193	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
38779	385.955274	172.28.25.193	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
38813	386.955287	172.28.25.193	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
38846	387.957921	172.28.25.193	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
49910	504.953893	172.28.25.193	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
49916	505.969762	172.28.25.193	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
49928	506.983572	172.28.25.193	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

Protocols captured: OCSP.

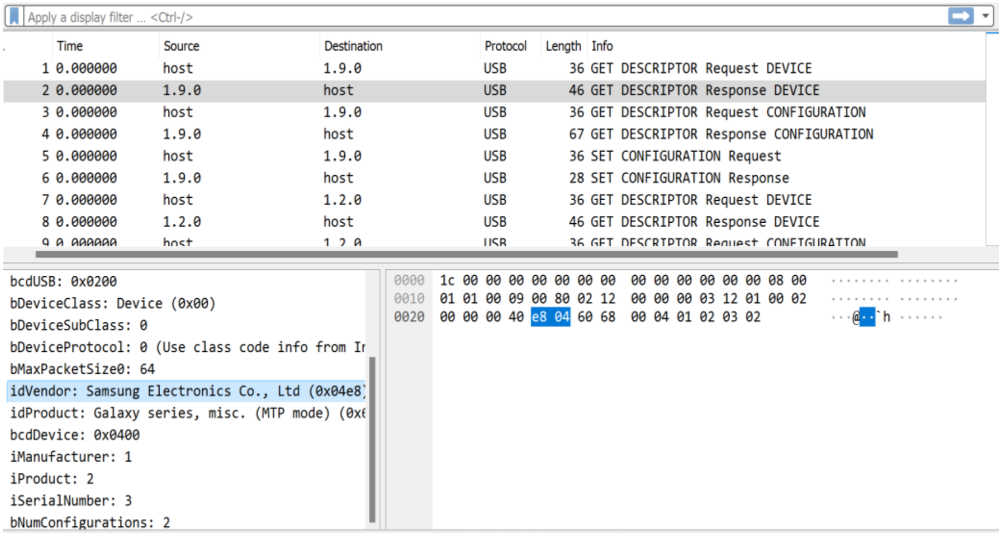


ocsp

No.	ocsp	Source	Destination	Protocol	Length	Info
2595…	3426.389349	103.43.90.117	172.28.25.193	TLSv1.2	1332	Certificate, Certificate Status, Server Key Excha
2605…	3446.198789	52.113.194.132	172.28.25.193	TLSv1.2	152	Server Hello, Certificate, Certificate Status, Se
2660…	3572.951558	103.43.90.117	172.28.25.193	TLSv1.2	1333	Certificate, Certificate Status, Server Key Excha
2665…	3600.601323	20.210.169.67	172.28.25.193	TLSv1.2	584	Server Hello, Certificate, Certificate Status, Se
2666…	3603.713984	20.205.104.58	172.28.25.193	TLSv1.2	197	Server Hello, Certificate, Certificate Status, Se
2666…	3603.970843	40.126.35.86	172.28.25.193	TLSv1.2	1086	Server Hello, Certificate, Certificate Status, Se
2666…	3604.122505	152.195.38.76	172.28.25.193	OCSP	855	Response
2677…	3616.337845	40.126.35.86	172.28.25.193	TLSv1.2	1086	Server Hello, Certificate, Certificate Status, Se
2736…	3784.595156	20.205.115.81	172.28.25.193	TLSv1.2	486	Server Hello, Certificate, Certificate Status, Se
2736…	3784.944179	20.44.10.123	172.28.25.193	TLSv1.2	519	Server Hello, Certificate, Certificate Status, Se
2738…	3785.179232	20.44.10.123	172.28.25.193	TLSv1.2	519	Server Hello, Certificate, Certificate Status, Se
2751…	3797.848267	103.43.90.179	172.28.25.193	TLSv1.2	1332	Certificate, Certificate Status, Server Key Excha
2751…	3797.972514	103.43.90.179	172.28.25.193	TLSv1.2	1331	Certificate, Certificate Status, Server Key Excha
2754…	3799.900928	103.43.90.179	172.28.25.193	TLSv1.2	1331	Certificate, Certificate Status, Server Key Excha
2754…	3800.099893	103.43.90.179	172.28.25.193	TLSv1.2	1332	Certificate, Certificate Status, Server Key Excha
2761…	3807.293270	103.43.90.179	172.28.25.193	TLSv1.2	1332	Certificate, Certificate Status, Server Key Excha
2761…	3807.821328	103.43.90.179	172.28.25.193	TLSv1.2	1331	Certificate, Certificate Status, Server Key Excha
2792…	3855.106287	13.89.178.26	172.28.25.193	TLSv1.2	519	Server Hello, Certificate, Certificate Status, Se
2792…	3855.361771	13.89.178.26	172.28.25.193	TLSv1.2	519	Server Hello, Certificate, Certificate Status, Se

b) USB

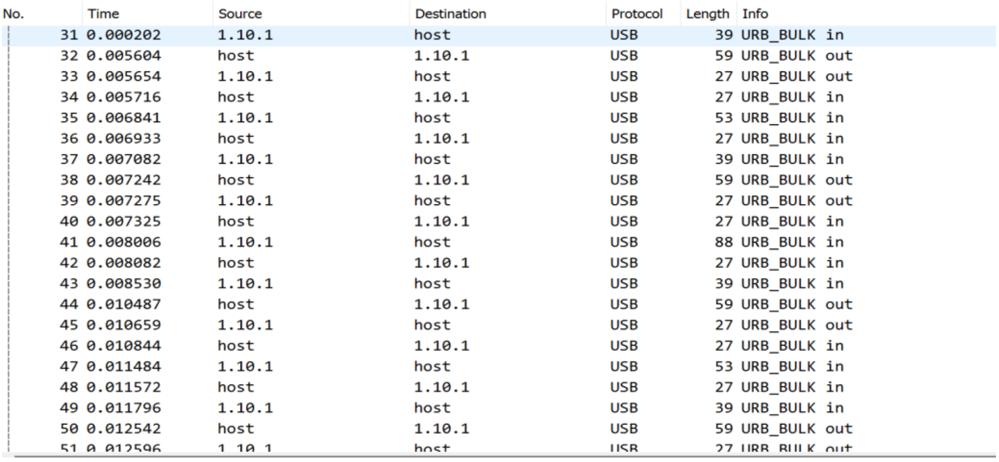
USB protocols can be captured through USBPcap.
Connection of mobile and pc through USB is successful.



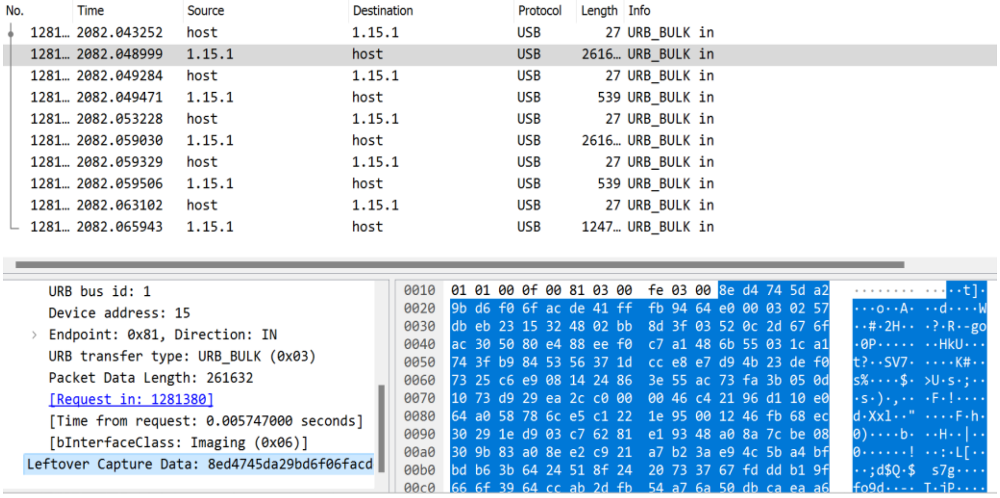
```
Apply a display filter ... <Ctrl-/>

   Time       Source    Destination   Protocol  Length Info
 1 0.000000   host      1.9.0         USB       36 GET DESCRIPTOR Request DEVICE
 2 0.000000   1.9.0     host          USB       46 GET DESCRIPTOR Response DEVICE
 3 0.000000   host      1.9.0         USB       36 GET DESCRIPTOR Request CONFIGURATION
 4 0.000000   1.9.0     host          USB       67 GET DESCRIPTOR Response CONFIGURATION
 5 0.000000   host      1.9.0         USB       36 SET CONFIGURATION Request
 6 0.000000   1.9.0     host          USB       28 SET CONFIGURATION Response
 7 0.000000   host      1.2.0         USB       36 GET DESCRIPTOR Request DEVICE
 8 0.000000   1.2.0     host          USB       46 GET DESCRIPTOR Response DEVICE
 9 0.000000   host      1.2.0         USB       36 GET DESCRIPTOR Request CONFIGURATION
```

```
bcdUSB: 0x0200                                    0000  1c 00 00 00 00 00 00 00  00 00 00 00 00 00 08 00   ········ ········
bDeviceClass: Device (0x00)                       0010  01 01 00 09 00 80 02 12  00 00 00 03 12 01 00 02   ········ ········
bDeviceSubClass: 0                                0020  00 00 00 40 e8 04 60 68  00 04 01 02 03 02         ···@··`h ······
bDeviceProtocol: 0 (Use class code info from Ir
bMaxPacketSize0: 64
idVendor: Samsung Electronics Co., Ltd (0x04e8)
idProduct: Galaxy series, misc. (MTP mode) (0x6
bcdDevice: 0x0400
iManufacturer: 1
iProduct: 2
iSerialNumber: 3
bNumConfigurations: 2
```



```
No.  Time      Source   Destination  Protocol  Length Info
  31 0.000202  1.10.1   host         USB       39 URB_BULK in
  32 0.005604  host     1.10.1       USB       59 URB_BULK out
  33 0.005654  1.10.1   host         USB       27 URB_BULK out
  34 0.005716  host     1.10.1       USB       27 URB_BULK in
  35 0.006841  1.10.1   host         USB       53 URB_BULK in
  36 0.006933  host     1.10.1       USB       27 URB_BULK in
  37 0.007082  1.10.1   host         USB       39 URB_BULK in
  38 0.007242  host     1.10.1       USB       59 URB_BULK out
  39 0.007275  1.10.1   host         USB       27 URB_BULK out
  40 0.007325  host     1.10.1       USB       27 URB_BULK in
  41 0.008006  1.10.1   host         USB       88 URB_BULK in
  42 0.008082  host     1.10.1       USB       27 URB_BULK in
  43 0.008530  1.10.1   host         USB       39 URB_BULK in
  44 0.010487  host     1.10.1       USB       59 URB_BULK out
  45 0.010659  1.10.1   host         USB       27 URB_BULK out
  46 0.010844  host     1.10.1       USB       27 URB_BULK in
  47 0.011484  1.10.1   host         USB       53 URB_BULK in
  48 0.011572  host     1.10.1       USB       27 URB_BULK in
  49 0.011796  1.10.1   host         USB       39 URB_BULK in
  50 0.012542  host     1.10.1       USB       59 URB_BULK out
  51 0.012596  1.10.1   host         USB       27 URB_BULK out
```

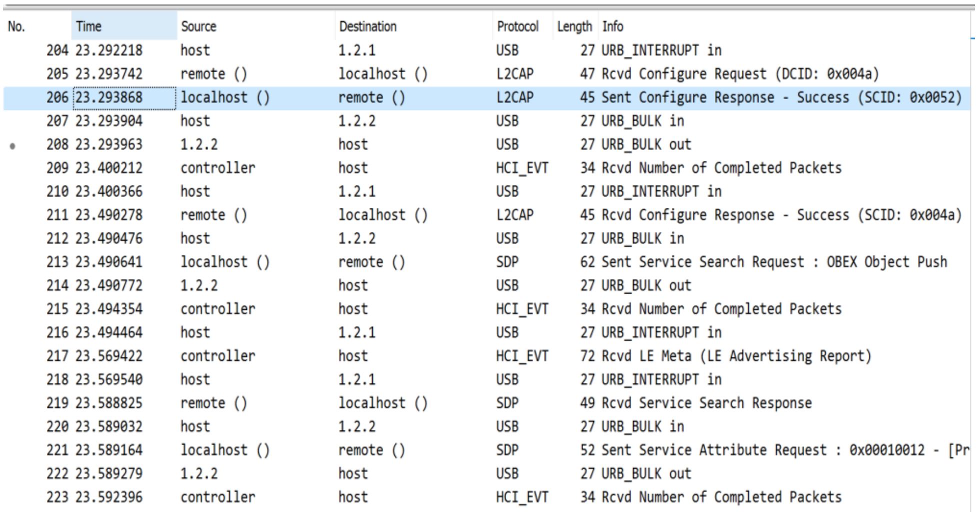


```
No.    Time         Source   Destination  Protocol  Length Info
1281… 2082.043252   host     1.15.1       USB         27 URB_BULK in
1281… 2082.048999   1.15.1   host         USB       2616… URB_BULK in
1281… 2082.049284   host     1.15.1       USB         27 URB_BULK in
1281… 2082.049471   1.15.1   host         USB        539 URB_BULK in
1281… 2082.053228   host     1.15.1       USB         27 URB_BULK in
1281… 2082.059030   1.15.1   host         USB       2616… URB_BULK in
1281… 2082.059329   host     1.15.1       USB         27 URB_BULK in
1281… 2082.059506   1.15.1   host         USB        539 URB_BULK in
1281… 2082.063102   host     1.15.1       USB         27 URB_BULK in
1281… 2082.065943   1.15.1   host         USB       1247… URB_BULK in
```

```
  URB bus id: 1                                        0010  01 01 00 0f 00 81 03 00  fe 03 00 8e d4 74 5d a2   ········ ···t]·
  Device address: 15                                   0020  9b d6 f0 6f ac de 41 ff  fb 94 64 e0 00 03 02 57   ···o··A· ··d····W
> Endpoint: 0x81, Direction: IN                        0030  db eb 23 15 32 48 02 bb  8d 3f 03 52 0c 2d 67 6f   ··#·2H·· ·?·R·-go
  URB transfer type: URB_BULK (0x03)                   0040  ac 30 50 80 e4 88 ee f0  c7 a1 48 6b 55 03 1c a1   ·0P····· ··HkU···
  Packet Data Length: 261632                           0050  74 3f b9 84 53 56 37 1d  cc e8 e7 d9 4b 23 de f0   t?··SV7· ····K#··
  [Request in: 1281380]                                0060  73 25 c6 e9 08 14 24 86  3e 55 ac 73 fa 3b 05 0d   s%····$· >U·s·;··
  [Time from request: 0.005747000 seconds]             0070  10 73 d9 29 ea 2c c0 00  00 46 c4 21 96 d1 10 e0   ·s·)·,·· ·F·!····
  [bInterfaceClass: Imaging (0x06)]                    0080  64 a0 58 78 6c e5 c1 22  1e 95 00 12 46 fb 68 ec   d·Xxl··" ····F·h·
Leftover Capture Data: 8ed4745da29bd6f06facd           0090  30 29 1e d9 03 c7 62 81  e1 93 48 a0 8a 7c be 08   0)····b· ··H··|··
                                                       00a0  30 9b 83 a0 8e e2 c9 21  a7 b2 3a e9 4c 5b a4 bf   0······! ··:·L[··
                                                       00b0  bd b6 3b 64 24 51 8f 24  20 73 37 67 fd dd b1 9f   ··;d$Q·$  s7g····
                                                       00c0  66 6f 39 64 cc ab 2d fb  54 a7 6a 50 db ca ea a6   fo9d··-· T·jP····
```

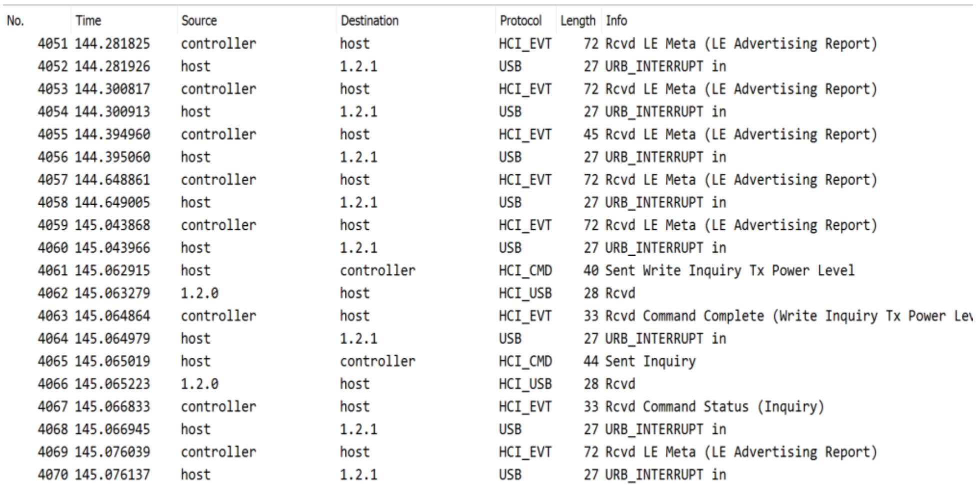
c) Bluetooth

Bluetooth protocols can also be captured through USBPcap.
Protocols captured: L2CAP, SDP, USB, HCI_EVT



No.	Time	Source	Destination	Protocol	Length	Info
204	23.292218	host	1.2.1	USB	27	URB_INTERRUPT in
205	23.293742	remote ()	localhost ()	L2CAP	47	Rcvd Configure Request (DCID: 0x004a)
206	23.293868	localhost ()	remote ()	L2CAP	45	Sent Configure Response - Success (SCID: 0x0052)
207	23.293904	host	1.2.2	USB	27	URB_BULK in
208	23.293963	1.2.2	host	USB	27	URB_BULK out
209	23.400212	controller	host	HCI_EVT	34	Rcvd Number of Completed Packets
210	23.400366	host	1.2.1	USB	27	URB_INTERRUPT in
211	23.490278	remote ()	localhost ()	L2CAP	45	Rcvd Configure Response - Success (SCID: 0x004a)
212	23.490476	host	1.2.2	USB	27	URB_BULK in
213	23.490641	localhost ()	remote ()	SDP	62	Sent Service Search Request : OBEX Object Push
214	23.490772	1.2.2	host	USB	27	URB_BULK out
215	23.494354	controller	host	HCI_EVT	34	Rcvd Number of Completed Packets
216	23.494464	host	1.2.1	USB	27	URB_INTERRUPT in
217	23.569422	controller	host	HCI_EVT	72	Rcvd LE Meta (LE Advertising Report)
218	23.569540	host	1.2.1	USB	27	URB_INTERRUPT in
219	23.588825	remote ()	localhost ()	SDP	49	Rcvd Service Search Response
220	23.589032	host	1.2.2	USB	27	URB_BULK in
221	23.589164	localhost ()	remote ()	SDP	52	Sent Service Attribute Request : 0x00010012 - [Pr
222	23.589279	1.2.2	host	USB	27	URB_BULK out
223	23.592396	controller	host	HCI_EVT	34	Rcvd Number of Completed Packets

Protocols captured: HCI_CMD, HCI_USB



No.	Time	Source	Destination	Protocol	Length	Info
4051	144.281825	controller	host	HCI_EVT	72	Rcvd LE Meta (LE Advertising Report)
4052	144.281926	host	1.2.1	USB	27	URB_INTERRUPT in
4053	144.300817	controller	host	HCI_EVT	72	Rcvd LE Meta (LE Advertising Report)
4054	144.300913	host	1.2.1	USB	27	URB_INTERRUPT in
4055	144.394960	controller	host	HCI_EVT	45	Rcvd LE Meta (LE Advertising Report)
4056	144.395060	host	1.2.1	USB	27	URB_INTERRUPT in
4057	144.648861	controller	host	HCI_EVT	72	Rcvd LE Meta (LE Advertising Report)
4058	144.649005	host	1.2.1	USB	27	URB_INTERRUPT in
4059	145.043868	controller	host	HCI_EVT	72	Rcvd LE Meta (LE Advertising Report)
4060	145.043966	host	1.2.1	USB	27	URB_INTERRUPT in
4061	145.062915	host	controller	HCI_CMD	40	Sent Write Inquiry Tx Power Level
4062	145.063279	1.2.0	host	HCI_USB	28	Rcvd
4063	145.064864	controller	host	HCI_EVT	33	Rcvd Command Complete (Write Inquiry Tx Power Lev
4064	145.064979	host	1.2.1	USB	27	URB_INTERRUPT in
4065	145.065019	host	controller	HCI_CMD	44	Sent Inquiry
4066	145.065223	1.2.0	host	HCI_USB	28	Rcvd
4067	145.066833	controller	host	HCI_EVT	33	Rcvd Command Status (Inquiry)
4068	145.066945	host	1.2.1	USB	27	URB_INTERRUPT in
4069	145.076039	controller	host	HCI_EVT	72	Rcvd LE Meta (LE Advertising Report)
4070	145.076137	host	1.2.1	USB	27	URB_INTERRUPT in

4. References

- https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs
- Microsoft-defined Bluetooth HCI commands and events - Windows drivers | Microsoft Learn
- CAPTURE USB TRAFFIC WITH WIRESHARK – YouTube

5. GitHub Link

https://github.com/11910417/Capturing-protocols-for-Wifi-USB-and-Bluetooth-through-Wireshark.git