Assignment 3:

I captured the three required video services: YouTube, DailyMotion, and Vimeo in the 3 cases.

The trace on smartphone is done by using the "PCAP Remote" App. The first step is to downloaded it from Google Play Store. It sets up a VPN and the network traffic will be recorded by the VPN server. It can select 1 specific App, trace its traffic and save the traced packets as "pcap" file. For YouTube, using the Youtube app for playing, while for the others, using the Chrome for playing.

Part A:

Case a: laptop+wifi

1. Youtube:

When using Chrome, Youtube is using QUIC connection; When using Safari, Youtube is using persistent TCP connection, and is running on multiple (two) connections. The figure for YouTube on safari is:

ip.addr==172.217.10.78

No.	Time	Source	Destination	Protocol	Length	Info
1497	5.256651	192.168.1.16	172.217.10.78	TCP	78	54583 → 443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=547806223 TSecr=0 SACK_PERM=1
1554	5.267395	172.217.10.78	192.168.1.16	TCP	74	443 → 54583 [SYN, ACK, ECN] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 TSval=275875481 TSecr=547806223 WS=256
1555	5.267504	192.168.1.16	172.217.10.78	TCP	66	54583 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0 TSval=547806233 TSecr=275875481
1556	5.268004	192.168.1.16	172.217.10.78	TLSv1…	583	Client Hello
1566	5.277822	172.217.10.78	192.168.1.16	TCP	66	443 → 54583 [ACK] Seq=1 Ack=518 Win=66816 Len=0 TSval=275875492 TSecr=547806233
1567	5.285102	172.217.10.78	192.168.1.16	TLSv1…	1484	Server Hello, Change Cipher Spec
1568	5.285106	172.217.10.78	192.168.1.16	TCP	1484	443 → 54583 [ACK] Seq=1419 Ack=518 Win=66816 Len=1418 TSval=275875500 TSecr=547806233 [TCP segment of a reassembled PDU]
1569	5.285194	192.168.1.16	172.217.10.78	TCP	66	54583 → 443 [ACK] Seq=518 Ack=2837 Win=129024 Len=0 TSval=547806249 TSecr=275875500
1570	5.285424	172.217.10.78	192.168.1.16	TLSv1…	1055	Application Data
1571	5.285473	192.168.1.16	172.217.10.78	TCP	66	54583 → 443 [ACK] Seq=518 Ack=3826 Win=130048 Len=0 TSval=547806249 TSecr=275875500
1573	5.349898	192.168.1.16	172.217.10.78	TLSv1…	130	Change Cipher Spec, Application Data
1574	5.350600	192.168.1.16	172.217.10.78	TLSv1…	112	Application Data
1575	5.350600	192.168.1.16	172.217.10.78	TLSv1…	109	Application Data
1576	5.350648	192.168.1.16	172.217.10.78	TLSv1…	101	Application Data
1577	5.350648	192.168.1.16	172.217.10.78	TLSv1…	262	Application Data
1578	5.361851	172.217.10.78	192.168.1.16	TCP	66	[TCP Previous segment not captured] 443 → 54583 [ACK] Seq=4406 Ack=902 Win=67840 Len=0 TSval=275875575 TSecr=547806312
1579	5.362261	172.217.10.78	192.168.1.16	TLSv1…	97	Application Data
1580	5.362298	192.168.1.16	172.217.10.78	TCP	78	[TCP Dup ACK 1571#1] 54583 → 443 [ACK] Seq=902 Ack=3826 Win=131072 Len=0 TSval=547806323 TSecr=275875500 SLE=4406 SRE=4437
1581	5.377433	172.217.10.78	192.168.1.16	TCP	646	[TCP Retransmission] 443 → 54583 [PSH, ACK] Seq=3826 Ack=902 Win=67840 Len=580 TSval=275875591 TSecr=547806323
1582	5.377497	192.168.1.16	172.217.10.78	TCP	66	54583 → 443 [ACK] Seq=902 Ack=4437 Win=130432 Len=0 TSval=547806338 TSecr=275875591
1583	5.377790	192.168.1.16	172.217.10.78	TLSv1…	97	Application Data
1584	5.393239	172.217.10.78	192.168.1.16	TCP	66	443 → 54583 [ACK] Seq=4437 Ack=933 Win=67840 Len=0 TSval=275875607 TSecr=547806338
1585	5.403997	172.217.10.78	192.168.1.16	TLSv1…	575	Application Data

1581	5.377433	172.217.10.78	192.168.1.16	TCP	646	[TCP Retransmission] 443 → 54583 [PSH, ACK] Seq=3826 Ack=902 Win=67840 Len=580 TSval=275875591 TSecr=547806323
1582	5.377497	192.168.1.16	172.217.10.78	TCP	66	54583 → 443 [ACK] Seq=902 Ack=4437 Win=130432 Len=0 TSval=547806338 TSecr=275875591
1583	5.377790	192.168.1.16	172.217.10.78	TLSv1…	97	Application Data
1584	5.393239	172.217.10.78	192.168.1.16	TCP	66	443 → 54583 [ACK] Seq=4437 Ack=933 Win=67840 Len=0 TSval=275875607 TSecr=547806338
1585	5.403997	172.217.10.78	192.168.1.16	TLSv1…	575	Application Data

1586	5.404000	172.217.10.78	192.168.1.16	TLSv1…	368	Application Data
1587	5.404056	192.168.1.16	172.217.10.78	TCP	66	54583 → 443 [ACK] Seq=933 Ack=4946 Win=130560 Len=0 TSval=547806362 TSecr=275875617
1588	5.404056	192.168.1.16	172.217.10.78	TCP	66	54583 → 443 [ACK] Seq=933 Ack=5248 Win=130240 Len=0 TSval=547806362 TSecr=275875617
1589	5.405119	172.217.10.78	192.168.1.16	TLSv1…	97	Application Data
1590	5.405164	192.168.1.16	172.217.10.78	TCP	66	54583 → 443 [ACK] Seq=933 Ack=5279 Win=131008 Len=0 TSval=547806363 TSecr=275875619
1591	5.405350	172.217.10.78	192.168.1.16	TLSv1…	105	Application Data
1592	5.405392	192.168.1.16	172.217.10.78	TCP	66	54583 → 443 [ACK] Seq=933 Ack=5318 Win=131008 Len=0 TSval=547806363 TSecr=275875619
1593	5.405533	192.168.1.16	172.217.10.78	TLSv1…	105	Application Data
1595	5.421315	172.217.10.78	192.168.1.16	TCP	66	443 → 54583 [ACK] Seq=5318 Ack=972 Win=67840 Len=0 TSval=275875635 TSecr=547806363
1784	7.889905	192.168.1.16	172.217.10.78	TCP	78	54586 → 443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=547808820 TSecr=0 SACK_PERM=1
1788	7.899342	172.217.10.78	192.168.1.16	TCP	74	443 → 54586 [SYN, ACK, ECN] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 TSval=609453661 TSecr=547808820 WS
1789	7.899418	192.168.1.16	172.217.10.78	TCP	66	54586 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0 TSval=547808829 TSecr=609453661
1790	7.899921	192.168.1.16	172.217.10.78	TLSv1…	583	Client Hello
1793	7.909368	172.217.10.78	192.168.1.16	TCP	66	443 → 54586 [ACK] Seq=1 Ack=518 Win=66816 Len=0 TSval=609453671 TSecr=547808829
1794	7.920556	172.217.10.78	192.168.1.16	TLSv1…	1484	Server Hello, Change Cipher Spec
1795	7.920560	172.217.10.78	192.168.1.16	TCP	1484	443 → 54586 [ACK] Seq=1419 Ack=518 Win=66816 Len=1418 TSval=609453682 TSecr=547808829 [TCP segment of a reasser
1796	7.920561	172.217.10.78	192.168.1.16	TLSv1…	1055	Application Data
1797	7.920638	192.168.1.16	172.217.10.78	TCP	66	54586 → 443 [ACK] Seq=518 Ack=2837 Win=129024 Len=0 TSval=547808849 TSecr=609453682

As we can see here, there are two connections established, the server side (172.217.10.78) sends multiple packets over the two connections, and the client side (172.24.18.119) sends ACKs.

2.DailyMotion:

DailyMotion is using persistent TCP connection, and is running on multiple (two) = connections. Here's a snippet of part of the trace using Chrome:

Same as Youtube, there are two connections established and then multiple packets

ip.addr==195.8.215.138

No.	Time	Source	Destination	Protocol	Length	Info
31	3.354792	192.168. Source address	195.8.215.138	TCP	78	54218 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=547623294 TSecr=0 SACK_PERM=1
32	3.355252	192.168.1.16	195.8.215.138	TCP	78	54219 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=547623294 TSecr=0 SACK_PERM=1
53	3.479412	195.8.215.138	192.168.1.16	TCP	74	443 → 54219 [SYN, ACK] Seq=0 Ack=1 Win=43440 Len=0 MSS=1460 SACK_PERM=1 TSval=3969232709 TSecr=547623294 WS=2048
54	3.479533	192.168.1.16	195.8.215.138	TCP	66	54219 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=547623415 TSecr=3969232709
55	3.479885	192.168.1.16	195.8.215.138	TLSv1…	583	Client Hello
56	3.569276	192.168.1.16	195.8.215.138	TCP	78	54220 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=547623504 TSecr=0 SACK_PERM=1
57	3.586822	195.8.215.138	192.168.1.16	TCP	66	443 → 54219 [ACK] Seq=1 Ack=518 Win=45056 Len=0 TSval=3969232831 TSecr=547623415
58	3.589263	195.8.215.138	192.168.1.16	TLSv1…	1514	Server Hello
59	3.589268	195.8.215.138	192.168.1.16	TCP	1514	443 → 54219 [ACK] Seq=1449 Ack=518 Win=45056 Len=1448 TSval=3969232833 TSecr=547623415 [TCP segment of a reassembled PDU]
60	3.589270	195.8.215.138	192.168.1.16	TLSv1…	1066	Certificate, Certificate Status, Server Key Exchange, Server Hello Done
61	3.589352	192.168.1.16	195.8.215.138	TCP	66	54219 → 443 [ACK] Seq=518 Ack=2897 Win=128832 Len=0 TSval=547623523 TSecr=3969232833
62	3.589352	192.168.1.16	195.8.215.138	TCP	66	54219 → 443 [ACK] Seq=518 Ack=3897 Win=127872 Len=0 TSval=547623523 TSecr=3969232833
63	3.589410	192.168.1.16	195.8.215.138	TCP	66	[TCP Window Update] 54219 → 443 [ACK] Seq=518 Ack=3897 Win=131072 Len=0 TSval=547623523 TSecr=3969232833
64	3.619800	192.168.1.16	195.8.215.138	TLSv1…	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
65	3.660385	195.8.215.138	192.168.1.16	TCP	74	443 → 54220 [SYN, ACK] Seq=0 Ack=1 Win=43440 Len=0 MSS=1460 SACK_PERM=1 TSval=2005570587 TSecr=547623504 WS=2048
66	3.660490	192.168.1.16	195.8.215.138	TCP	66	54220 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=547623593 TSecr=2005570587
67	3.660852	192.168.1.16	195.8.215.138	TLSv1…	583	Client Hello
68	3.725454	195.8.215.138	192.168.1.16	TLSv1…	117	Change Cipher Spec, Encrypted Handshake Message
69	3.725555	192.168.1.16	195.8.215.138	TCP	66	54219 → 443 [ACK] Seq=644 Ack=3948 Win=131008 Len=0 TSval=547623657 TSecr=3969232970
70	3.726100	192.168.1.16	195.8.215.138	TLSv1…	700	Application Data
71	3.754789	195.8.215.138	192.168.1.16	TCP	66	443 → 54220 [ACK] Seq=1 Ack=518 Win=45056 Len=0 TSval=2005570680 TSecr=547623593
72	3.758324	195.8.215.138	192.168.1.16	TLSv1…	1514	Server Hello
73	3.758329	195.8.215.138	192.168.1.16	TCP	1514	443 → 54220 [ACK] Seq=1449 Ack=518 Win=45056 Len=1448 TSval=2005570682 TSecr=547623593 [TCP segment of a reassembled PDU]
74	3.758331	195.8.215.138	192.168.1.16	TLSv1…	1066	Certificate, Certificate Status, Server Key Exchange, Server Hello Done

sent between the two connections.

ip.addr==151.101.208.217

No.	Time	Source	Destination	Protocol	Length	Info
498	2.599747	192.168.1.16	151.101.208.217	TCP	78	54634 → 443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=548097675 TSecr=0 SACK_PERM=1
507	2.613904	151.101.208.217	192.168.1.16	TCP	74	443 → 54634 [SYN, ACK] Seq=0 Ack=1 Win=42904 Len=0 MSS=1396 SACK_PERM=1 TSval=1074594806 TSecr=548097675 WS=512
509	2.614013	192.168.1.16	151.101.208.217	TCP	66	54634 → 443 [ACK] Seq=1 Ack=1 Win=131456 Len=0 TSval=548097688 TSecr=1074594806
511	2.614243	192.168.1.16	151.101.208.217	TLSv1…	583	Client Hello
534	2.626211	151.101.208.217	192.168.1.16	TLSv1…	222	Server Hello, Change Cipher Spec, Encrypted Handshake Message
535	2.626212	151.101.208.217	192.168.1.16	TCP	66	443 → 54634 [ACK] Seq=1 Ack=518 Win=42496 Len=0 TSval=1074594820 TSecr=548097688
538	2.626323	192.168.1.16	151.101.208.217	TCP	66	54634 → 443 [ACK] Seq=518 Ack=157 Win=131264 Len=0 TSval=548097697 TSecr=1074594820
539	2.626323	192.168.1.16	151.101.208.217	TCP	66	[TCP Dup ACK 538#1] 54634 → 443 [ACK] Seq=518 Ack=157 Win=131264 Len=0 TSval=548097697 TSecr=1074594820
551	2.634280	192.168.1.16	151.101.208.217	TLSv1…	117	Change Cipher Spec, Encrypted Handshake Message
694	2.687188	151.101.208.217	192.168.1.16	TCP	66	443 → 54634 [ACK] Seq=157 Ack=569 Win=42496 Len=0 TSval=1074594882 TSecr=548097704
7436	8.705458	192.168.1.16	151.101.208.217	TLSv1…	1093	Application Data
7450	8.713405	151.101.208.217	192.168.1.16	TCP	66	443 → 54634 [ACK] Seq=157 Ack=1596 Win=41984 Len=0 TSval=1074600911 TSecr=548102985
7550	8.784315	151.101.208.217	192.168.1.16	TLSv1…	1450	Application Data
7551	8.784317	151.101.208.217	192.168.1.16	TLSv1…	1450	Application Data [TCP segment of a reassembled PDU]
7552	8.784318	151.101.208.217	192.168.1.16	TLSv1…	1400	Application Data, Application Data
7553	8.784460	192.168.1.16	151.101.208.217	TCP	66	54634 → 443 [ACK] Seq=1596 Ack=2925 Win=128512 Len=0 TSval=548103049 TSecr=1074600978
7554	8.784460	192.168.1.16	151.101.208.217	TCP	66	54634 → 443 [ACK] Seq=1596 Ack=4259 Win=127168 Len=0 TSval=548103049 TSecr=1074600978
7555	8.784461	192.168.1.16	151.101.208.217	TCP	66	[TCP Window Update] 54634 → 443 [ACK] Seq=1596 Ack=4259 Win=131072 Len=0 TSval=548103049 TSecr=1074600978
8556	9.861785	192.168.1.16	151.101.208.217	TLSv1…	1028	Application Data
8563	9.875566	151.101.208.217	192.168.1.16	TCP	66	443 → 54634 [ACK] Seq=4259 Ack=2558 Win=41984 Len=0 TSval=1074602067 TSecr=548104012
8565	9.877248	151.101.208.217	192.168.1.16	TLSv1…	1450	Application Data
8566	9.877252	151.101.208.217	192.168.1.16	TLSv1…	256	Application Data
8568	9.877323	192.168.1.16	151.101.208.217	TCP	66	54634 → 443 [ACK] Seq=2558 Ack=5833 Win=129472 Len=0 TSval=548104026 TSecr=1074602068

3. Vimeo: is using is using persistent TCP connection, and is running on a single connection. (The above figure)

ip.addr==172.217.10.234

No.	Time	Source	Destination	Protocol	Length	Info
56	0.917784	10.1.10.1	172.217.10.234	UDP	1378	44184 → 443 Len=1350
57	0.918215	10.1.10.1	172.217.10.234	TCP	60	45790 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=9960 SACK_PERM=1 TSval=4284140048 TSecr=0 WS=512
58	0.936204	172.217.10.234	10.1.10.1	TCP	48	443 → 45790 [SYN, ACK] Seq=0 Ack=1 Win=16192 Len=0 MSS=59430 WS=1
59	0.936379	10.1.10.1	172.217.10.234	TCP	40	45790 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=0
60	0.936658	10.1.10.1	172.217.10.234	TLSv1…	629	Client Hello
61	0.936798	172.217.10.234	10.1.10.1	TCP	40	443 → 45790 [ACK] Seq=1 Ack=590 Win=16192 Len=0
62	0.959768	172.217.10.234	10.1.10.1	TLSv1…	252	Server Hello, Change Cipher Spec, Application Data
63	0.959914	10.1.10.1	172.217.10.234	TCP	40	45790 → 443 [ACK] Seq=590 Ack=213 Win=80896 Len=0
64	0.961020	10.1.10.1	172.217.10.234	TLSv1…	104	Change Cipher Spec, Application Data
65	0.961204	172.217.10.234	10.1.10.1	TCP	40	443 → 45790 [ACK] Seq=213 Ack=654 Win=16192 Len=0
66	0.961653	10.1.10.1	172.217.10.234	TLSv1…	132	Application Data
67	0.961727	172.217.10.234	10.1.10.1	TCP	40	443 → 45790 [ACK] Seq=213 Ack=746 Win=16192 Len=0
68	0.962163	10.1.10.1	172.217.10.234	TLSv1…	806	Application Data
69	0.962256	172.217.10.234	10.1.10.1	TCP	40	443 → 45790 [ACK] Seq=213 Ack=1512 Win=16192 Len=0
70	0.962674	10.1.10.1	172.217.10.234	TLSv1…	1403	Application Data
71	0.962845	172.217.10.234	10.1.10.1	TCP	40	443 → 45790 [ACK] Seq=213 Ack=2875 Win=16192 Len=0
72	0.975461	10.1.10.1	172.217.10.234	TLSv1…	315	Application Data
73	0.975570	172.217.10.234	10.1.10.1	TCP	40	443 → 45790 [ACK] Seq=213 Ack=3150 Win=16192 Len=0
74	0.975743	172.217.10.234	10.1.10.1	TLSv1…	620	Application Data, Application Data
75	0.975839	10.1.10.1	172.217.10.234	TLSv1…	1368	Application Data
76	0.975930	172.217.10.234	10.1.10.1	TCP	40	443 → 45790 [ACK] Seq=793 Ack=4478 Win=16192 Len=0
77	0.976042	10.1.10.1	172.217.10.234	TLSv1…	71	Application Data
78	0.976083	172.217.10.234	10.1.10.1	TCP	40	443 → 45790 [ACK] Seq=793 Ack=4509 Win=16192 Len=0

As shown in the figure, there is only one connection and many packets sent over this connection.

Case b: mobile+wifi

1.Youtube: (above figure in previous page)

As shown in the figure, when using Youtube app on mobile phone, Youtube is using persistent TCP connection, and is running on a single connection: many packets sent over the only connection.

2.DailyMotion:

Start capturing packets

No.	Time	Source	Destination	Protocol	Length	Info
1986	9.016568	10.1.10.1	195.8.215.138	TCP	60	47494 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=9960 SACK_PERM=1 TSval=751670715 TSecr=0 WS=512
1998	9.121568	195.8.215.138	10.1.10.1	TCP	48	443 → 47494 [SYN, ACK] Seq=0 Ack=1 Win=16192 Len=0 MSS=59430 WS=1
1999	9.121907	10.1.10.1	195.8.215.138	TCP	40	47494 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=0
2000	9.122213	10.1.10.1	195.8.215.138	TLSv1…	557	Client Hello
2001	9.122342	195.8.215.138	10.1.10.1	TCP	40	443 → 47494 [ACK] Seq=1 Ack=518 Win=16192 Len=0
2006	9.219165	195.8.215.138	10.1.10.1	TLSv1…	3936	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
2007	9.219680	10.1.10.1	195.8.215.138	TCP	40	47494 → 443 [ACK] Seq=518 Ack=3897 Win=87552 Len=0
2008	9.231092	10.1.10.1	195.8.215.138	TLSv1…	166	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2009	9.231350	195.8.215.138	10.1.10.1	TCP	40	443 → 47494 [ACK] Seq=3897 Ack=644 Win=16192 Len=0
2024	9.327676	195.8.215.138	10.1.10.1	TLSv1…	91	Change Cipher Spec, Encrypted Handshake Message
2025	9.328750	10.1.10.1	195.8.215.138	TLSv1…	3364	Application Data
2026	9.329025	195.8.215.138	10.1.10.1	TCP	40	443 → 47494 [ACK] Seq=3948 Ack=3968 Win=16192 Len=0
2132	9.559357	195.8.215.138	10.1.10.1	TCP	4384	443 → 47494 [ACK] Seq=3948 Ack=3968 Win=16192 Len=4344 [TCP segment of a reassembled PDU]
2133	9.559929	195.8.215.138	10.1.10.1	TLSv1…	3243	Application Data
2135	9.560265	10.1.10.1	195.8.215.138	TCP	40	47494 → 443 [ACK] Seq=3968 Ack=11495 Win=104960 Len=0
2311	9.838673	10.1.10.1	195.8.215.138	TLSv1…	3250	Application Data
2312	9.838984	195.8.215.138	10.1.10.1	TCP	40	443 → 47494 [ACK] Seq=11495 Ack=7178 Win=16192 Len=0
2328	9.952447	195.8.215.138	10.1.10.1	TLSv1…	2639	Application Data
2333	9.984383	10.1.10.1	195.8.215.138	TCP	40	47494 → 443 [ACK] Seq=7178 Ack=14094 Win=113664 Len=0
2607	10.653150	10.1.10.1	195.8.215.138	TCP	60	47546 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=9960 SACK_PERM=1 TSval=751672352 TSecr=0 WS=512
2627	10.756564	195.8.215.138	10.1.10.1	TCP	48	443 → 47546 [SYN, ACK] Seq=0 Ack=1 Win=16192 Len=0 MSS=59430 WS=1
2628	10.758995	10.1.10.1	195.8.215.138	TCP	40	47546 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=0
2629	10.759207	10.1.10.1	195.8.215.138	TLSv1…	557	Client Hello

When using google chrome to play dailymotion on phone with WIFI, we can see multiple persistent TCP connections running simultaneously.

3. Vimeo:

ip.addr==151.101.64.217

No.	Time	Source	Destination	Protocol	Length	Info
276	4.095424	10.1.10.1	151.101.64.217	TCP	60	43454 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=9960 SACK_PERM=1 TSval=3505966654 TSecr=0 WS=512
277	4.099389	10.1.10.1	151.101.64.217	TCP	60	43456 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=9960 SACK_PERM=1 TSval=3505966656 TSecr=0 WS=512
279	4.114977	151.101.64.217	10.1.10.1	TCP	48	443 → 43454 [SYN, ACK] Seq=0 Ack=1 Win=16192 Len=0 MSS=59430 WS=1
281	4.115171	10.1.10.1	151.101.64.217	TCP	40	43454 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=0
282	4.115339	10.1.10.1	151.101.64.217	TLSv1…	557	Client Hello
283	4.115479	151.101.64.217	10.1.10.1	TCP	40	443 → 43454 [ACK] Seq=1 Ack=518 Win=16192 Len=0
284	4.122453	151.101.64.217	10.1.10.1	TCP	48	443 → 43456 [SYN, ACK] Seq=0 Ack=1 Win=16192 Len=0 MSS=59430 WS=1
285	4.122661	10.1.10.1	151.101.64.217	TCP	40	43456 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=0
286	4.123268	10.1.10.1	151.101.64.217	TLSv1…	557	Client Hello
287	4.123408	151.101.64.217	10.1.10.1	TCP	40	443 → 43456 [ACK] Seq=1 Ack=518 Win=16192 Len=0
288	4.131556	151.101.64.217	10.1.10.1	TLSv1…	196	Server Hello, Change Cipher Spec, Encrypted Handshake Message
289	4.131701	10.1.10.1	151.101.64.217	TCP	40	43454 → 443 [ACK] Seq=518 Ack=157 Win=80896 Len=0
290	4.132848	10.1.10.1	151.101.64.217	TLSv1…	91	Change Cipher Spec, Encrypted Handshake Message
291	4.133009	151.101.64.217	10.1.10.1	TCP	40	443 → 43454 [ACK] Seq=157 Ack=569 Win=16192 Len=0
292	4.133146	10.1.10.1	151.101.64.217	TLSv1…	1066	Application Data
293	4.133234	151.101.64.217	10.1.10.1	TCP	40	443 → 43454 [ACK] Seq=157 Ack=1595 Win=16192 Len=0
294	4.139768	151.101.64.217	10.1.10.1	TLSv1…	196	Server Hello, Change Cipher Spec, Encrypted Handshake Message
295	4.139901	10.1.10.1	151.101.64.217	TCP	40	43456 → 443 [ACK] Seq=518 Ack=157 Win=80896 Len=0
296	4.140440	10.1.10.1	151.101.64.217	TLSv1…	91	Change Cipher Spec, Encrypted Handshake Message
297	4.140581	151.101.64.217	10.1.10.1	TCP	40	443 → 43456 [ACK] Seq=157 Ack=569 Win=16192 Len=0
298	4.140744	10.1.10.1	151.101.64.217	TLSv1…	3460	Application Data
299	4.140902	151.101.64.217	10.1.10.1	TCP	40	443 → 43456 [ACK] Seq=157 Ack=3989 Win=16192 Len=0
300	4.192595	151.101.64.217	10.1.10.1	TLSv1…	1039	Application Data, Application Data

When using google chrome to play vimeo on phone with WIFI, we can see multiple persistent TCP connections running simultaneously.

Case c: mobile+4g

1. Youtube:

when using Youtube app on mobile phone, Youtube is using persistent TCP connection, and is running on a single connection: many packets sent over the only connection.

ip.addr==172.217.12.138

No.	Time	Source	Destination	Protocol	Length	Info
396	4.424070	10.1.10.1	172.217.12.138	TCP	60	39662 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=9960 SACK_PERM=1 TSval=2565227770 TSecr=0 WS=512
414	4.460198	172.217.12.138	10.1.10.1	TCP	48	443 → 39662 [SYN, ACK] Seq=0 Ack=1 Win=16192 Len=0 MSS=59430 WS=1
416	4.460481	10.1.10.1	172.217.12.138	TCP	40	39662 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=0
417	4.460805	10.1.10.1	172.217.12.138	TLSv1…	629	Client Hello
418	4.460935	172.217.12.138	10.1.10.1	TCP	40	443 → 39662 [ACK] Seq=1 Ack=590 Win=16192 Len=0
430	4.518323	172.217.12.138	10.1.10.1	TLSv1…	252	Server Hello, Change Cipher Spec, Application Data
431	4.518534	10.1.10.1	172.217.12.138	TCP	40	39662 → 443 [ACK] Seq=590 Ack=213 Win=80896 Len=0
432	4.519262	10.1.10.1	172.217.12.138	TLSv1…	104	Change Cipher Spec, Application Data
433	4.519394	172.217.12.138	10.1.10.1	TCP	40	443 → 39662 [ACK] Seq=213 Ack=654 Win=16192 Len=0
434	4.519527	10.1.10.1	172.217.12.138	TLSv1…	132	Application Data
435	4.519588	172.217.12.138	10.1.10.1	TCP	40	443 → 39662 [ACK] Seq=213 Ack=746 Win=16192 Len=0
436	4.519835	10.1.10.1	172.217.12.138	TLSv1…	831	Application Data
437	4.519931	172.217.12.138	10.1.10.1	TCP	40	443 → 39662 [ACK] Seq=213 Ack=1537 Win=16192 Len=0
438	4.520057	10.1.10.1	172.217.12.138	TLSv1…	315	Application Data
439	4.520115	172.217.12.138	10.1.10.1	TCP	40	443 → 39662 [ACK] Seq=213 Ack=1812 Win=16192 Len=0
440	4.520267	10.1.10.1	172.217.12.138	TLSv1…	1637	Application Data
441	4.520346	172.217.12.138	10.1.10.1	TCP	40	443 → 39662 [ACK] Seq=213 Ack=3409 Win=16192 Len=0
442	4.520577	10.1.10.1	172.217.12.138	TLSv1…	1553	Application Data
443	4.520657	172.217.12.138	10.1.10.1	TCP	40	443 → 39662 [ACK] Seq=213 Ack=4922 Win=16192 Len=0
458	4.559583	172.217.12.138	10.1.10.1	TLSv1…	620	Application Data, Application Data
459	4.559971	10.1.10.1	172.217.12.138	TLSv1…	71	Application Data
460	4.560078	172.217.12.138	10.1.10.1	TCP	40	443 → 39662 [ACK] Seq=793 Ack=4953 Win=16192 Len=0
462	4.572852	172.217.12.138	10.1.10.1	TLSv1…	71	Application Data

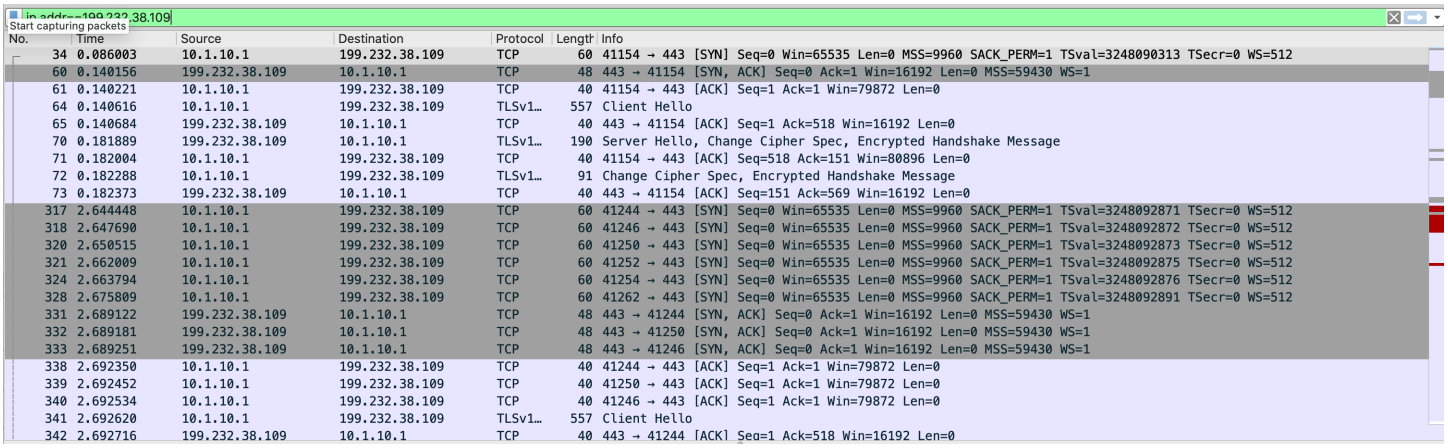
2.DailyMotion: When using google chrome to play dailymotion on phone with 4g, we

Start capturing packets

No.	Time	Source	Destination	Protocol	Length	Info
141	1.602466	10.1.10.1	195.8.215.138	TCP	60	38768 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=9960 SACK_PERM=1 TSval=718786545 TSecr=0 WS=512
142	1.605024	10.1.10.1	195.8.215.138	TCP	60	38770 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=9960 SACK_PERM=1 TSval=718786547 TSecr=0 WS=512
155	1.716725	195.8.215.138	10.1.10.1	TCP	48	443 → 38768 [SYN, ACK] Seq=0 Ack=1 Win=16192 Len=0 MSS=59430 WS=1
156	1.716821	195.8.215.138	10.1.10.1	TCP	48	443 → 38770 [SYN, ACK] Seq=0 Ack=1 Win=16192 Len=0 MSS=59430 WS=1
157	1.716939	10.1.10.1	195.8.215.138	TCP	40	38768 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=0
158	1.717012	10.1.10.1	195.8.215.138	TCP	40	38770 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=0
159	1.717162	10.1.10.1	195.8.215.138	TLSv1…	557	Client Hello
160	1.717244	195.8.215.138	10.1.10.1	TCP	40	443 → 38768 [ACK] Seq=1 Ack=518 Win=16192 Len=0
161	1.717543	10.1.10.1	195.8.215.138	TLSv1…	557	Client Hello
162	1.717638	195.8.215.138	10.1.10.1	TCP	40	443 → 38770 [ACK] Seq=1 Ack=518 Win=16192 Len=0
169	1.878086	195.8.215.138	10.1.10.1	TLSv1…	183	Server Hello, Change Cipher Spec, Encrypted Handshake Message
172	1.878468	10.1.10.1	195.8.215.138	TCP	40	38770 → 443 [ACK] Seq=518 Ack=144 Win=80896 Len=0
175	1.879146	10.1.10.1	195.8.215.138	TLSv1…	91	Change Cipher Spec, Encrypted Handshake Message
176	1.879273	195.8.215.138	10.1.10.1	TCP	40	443 → 38770 [ACK] Seq=144 Ack=569 Win=16192 Len=0
180	1.883976	195.8.215.138	10.1.10.1	TLSv1…	3936	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
181	1.884312	10.1.10.1	195.8.215.138	TCP	40	38768 → 443 [ACK] Seq=518 Ack=3897 Win=87552 Len=0
195	1.898067	10.1.10.1	195.8.215.138	TLSv1…	166	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
196	1.898182	195.8.215.138	10.1.10.1	TCP	40	443 → 38768 [ACK] Seq=3897 Ack=644 Win=16192 Len=0
266	2.006757	195.8.215.138	10.1.10.1	TLSv1…	91	Change Cipher Spec, Encrypted Handshake Message
273	2.042265	10.1.10.1	195.8.215.138	TCP	40	38768 → 443 [ACK] Seq=644 Ack=3948 Win=87552 Len=0
274	2.049220	10.1.10.1	195.8.215.138	TLSv1…	3419	Application Data
275	2.049498	195.8.215.138	10.1.10.1	TCP	40	443 → 38770 [ACK] Seq=144 Ack=3948 Win=16192 Len=0
299	2.203792	195.8.215.138	10.1.10.1	TCP	2776	443 → 38770 [ACK] Seq=144 Ack=3948 Win=16192 Len=2736 [TCP segment of a reassembled PDU]

can see multiple persistent TCP connections running simultaneously.

3. Vimeo:



No.	Time	Source	Destination	Protocol	Length	Info
34	0.086003	10.1.10.1	199.232.38.109	TCP	60	41154 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=9960 SACK_PERM=1 TSval=3248090313 TSecr=0 WS=512
60	0.140156	199.232.38.109	10.1.10.1	TCP	48	443 → 41154 [SYN, ACK] Seq=0 Ack=1 Win=16192 Len=0 MSS=59430 WS=1
61	0.140221	10.1.10.1	199.232.38.109	TCP	40	41154 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=0
64	0.140616	10.1.10.1	199.232.38.109	TLSv1…	557	Client Hello
65	0.140684	199.232.38.109	10.1.10.1	TCP	40	443 → 41154 [ACK] Seq=1 Ack=518 Win=16192 Len=0
70	0.181889	199.232.38.109	10.1.10.1	TLSv1…	190	Server Hello, Change Cipher Spec, Encrypted Handshake Message
71	0.182004	10.1.10.1	199.232.38.109	TCP	40	41154 → 443 [ACK] Seq=518 Ack=151 Win=80896 Len=0
72	0.182288	10.1.10.1	199.232.38.109	TLSv1…	91	Change Cipher Spec, Encrypted Handshake Message
73	0.182373	199.232.38.109	10.1.10.1	TCP	40	443 → 41154 [ACK] Seq=151 Ack=569 Win=16192 Len=0
317	2.644448	10.1.10.1	199.232.38.109	TCP	60	41244 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=9960 SACK_PERM=1 TSval=3248092871 TSecr=0 WS=512
318	2.647690	10.1.10.1	199.232.38.109	TCP	60	41246 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=9960 SACK_PERM=1 TSval=3248092872 TSecr=0 WS=512
320	2.650515	10.1.10.1	199.232.38.109	TCP	60	41250 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=9960 SACK_PERM=1 TSval=3248092873 TSecr=0 WS=512
321	2.662009	10.1.10.1	199.232.38.109	TCP	60	41252 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=9960 SACK_PERM=1 TSval=3248092875 TSecr=0 WS=512
324	2.663794	10.1.10.1	199.232.38.109	TCP	60	41254 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=9960 SACK_PERM=1 TSval=3248092876 TSecr=0 WS=512
328	2.675809	10.1.10.1	199.232.38.109	TCP	60	41262 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=9960 SACK_PERM=1 TSval=3248092891 TSecr=0 WS=512
331	2.689122	199.232.38.109	10.1.10.1	TCP	48	443 → 41244 [SYN, ACK] Seq=0 Ack=1 Win=16192 Len=0 MSS=59430 WS=1
332	2.689181	199.232.38.109	10.1.10.1	TCP	48	443 → 41250 [SYN, ACK] Seq=0 Ack=1 Win=16192 Len=0 MSS=59430 WS=1
333	2.689251	199.232.38.109	10.1.10.1	TCP	48	443 → 41246 [SYN, ACK] Seq=0 Ack=1 Win=16192 Len=0 MSS=59430 WS=1
338	2.692350	10.1.10.1	199.232.38.109	TCP	40	41244 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=0
339	2.692452	10.1.10.1	199.232.38.109	TCP	40	41250 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=0
340	2.692534	10.1.10.1	199.232.38.109	TCP	40	41246 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=0
341	2.692620	10.1.10.1	199.232.38.109	TLSv1…	557	Client Hello
342	2.692716	199.232.38.109	10.1.10.1	TCP	40	443 → 41244 [ACK] Seq=1 Ack=518 Win=16192 Len=0

When using google chrome to play Vimeo on phone with 4g, we can see multiple persistent TCP connections running simultaneously.