21BDS0340

Abhinav Dinesh Srivatsa

Information Security Management

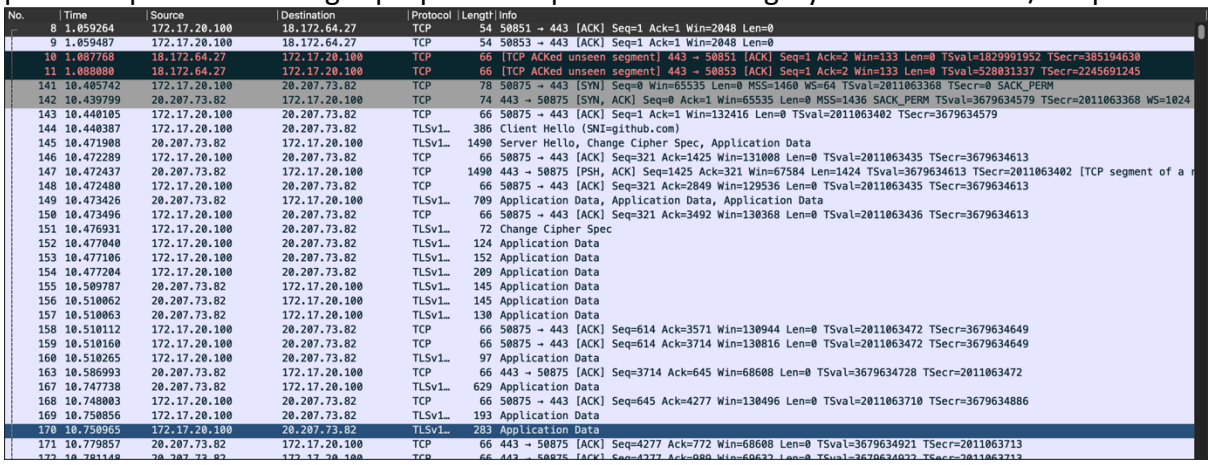
Assignment – III

Question 1

Aim
The monitor packets using the Wireshark software and understand the colour coding

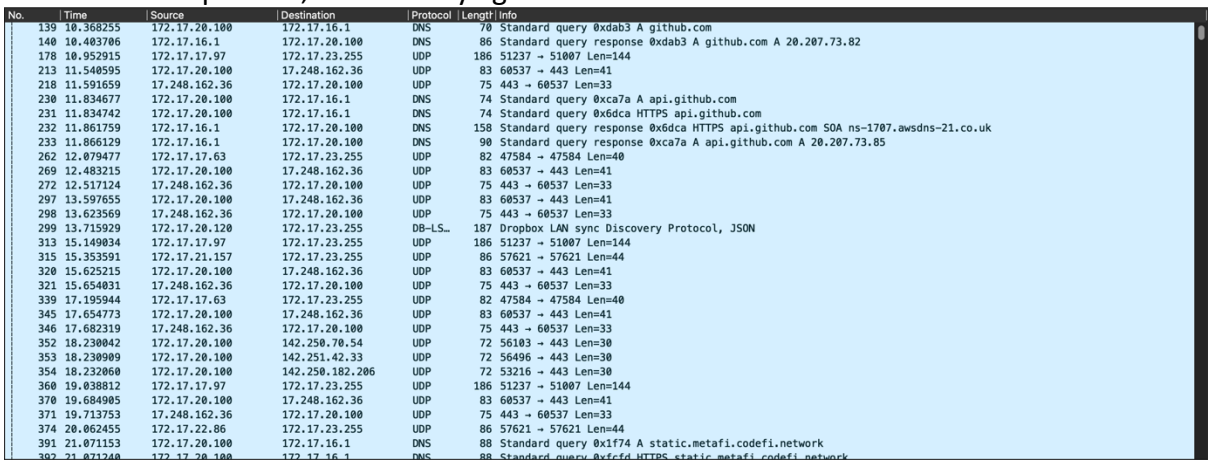
Procedure
1. Open the Wireshark software
2. Type various filters to analyse the packets

Screenshots and Results
TCP packet screen shots. The black background with red text means the packet has a potential problem. The light purple is TCP packets and the grey means TCP SYN/FIN packets.



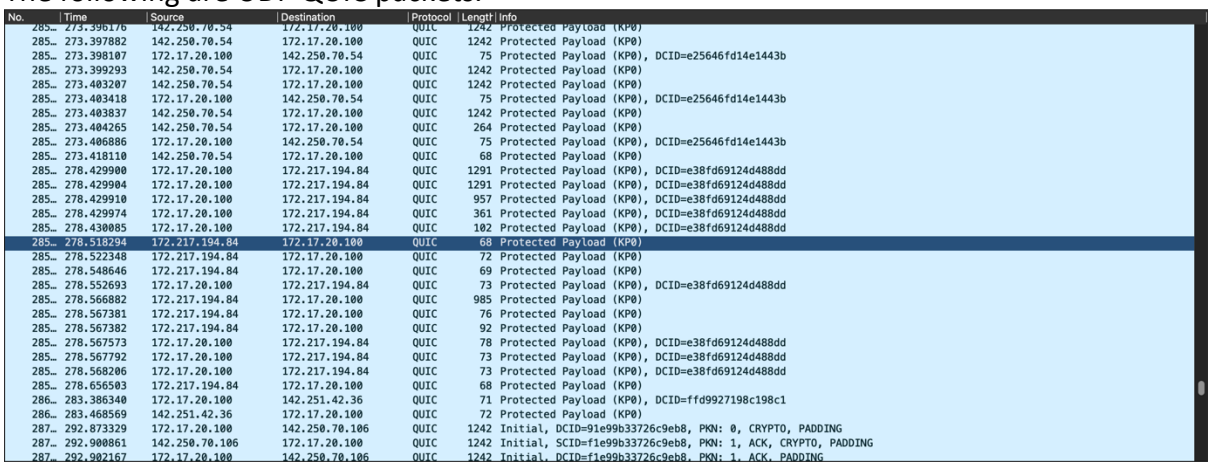
No.	Time	Source	Destination	Protocol	Length	Info
8	1.059264	172.17.20.100	18.172.64.27	TCP	54	50851 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
9	1.059487	172.17.20.100	18.172.64.27	TCP	54	50853 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
10	1.087768	18.172.64.27	172.17.20.100	TCP	66	[TCP ACKed unseen segment] 443 → 50851 [ACK] Seq=1 Ack=2 Win=133 Len=0 TSval=1829991952 TSecr=385194630
11	1.088080	18.172.64.27	172.17.20.100	TCP	66	[TCP ACKed unseen segment] 443 → 50853 [ACK] Seq=1 Ack=2 Win=133 Len=0 TSval=528031337 TSecr=2245691245
141	10.405742	172.17.20.100	20.207.73.82	TCP	78	50875 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2011063368 TSecr=0 SACK_PERM
142	10.439799	20.207.73.82	172.17.20.100	TCP	74	443 → 50875 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1436 SACK_PERM TSval=3679634579 TSecr=2011063368 WS=1024
143	10.440105	172.17.20.100	20.207.73.82	TCP	66	50875 → 443 [ACK] Seq=1 Ack=1 Win=132416 Len=0 TSval=2011063402 TSecr=3679634579
144	10.440387	172.17.20.100	20.207.73.82	TLSv1…	386	Client Hello (SNI=github.com)
145	10.471908	20.207.73.82	172.17.20.100	TLSv1…	1490	Server Hello, Change Cipher Spec, Application Data
146	10.472289	172.17.20.100	20.207.73.82	TCP	66	50875 → 443 [ACK] Seq=321 Ack=1425 Win=131008 Len=0 TSval=2011063435 TSecr=3679634613
147	10.472437	20.207.73.82	172.17.20.100	TCP	1490	443 → 50875 [PSH, ACK] Seq=1425 Ack=321 Win=67584 Len=1424 TSval=3679634613 TSecr=2011063402 [TCP segment of a r
148	10.472480	172.17.20.100	20.207.73.82	TCP	66	50875 → 443 [ACK] Seq=321 Ack=2849 Win=129536 Len=0 TSval=2011063435 TSecr=3679634613
149	10.473426	20.207.73.82	172.17.20.100	TLSv1…	709	Application Data, Application Data, Application Data
150	10.473496	172.17.20.100	20.207.73.82	TCP	66	50875 → 443 [ACK] Seq=321 Ack=3492 Win=130368 Len=0 TSval=2011063436 TSecr=3679634613
151	10.476931	172.17.20.100	20.207.73.82	TLSv1…	72	Change Cipher Spec
152	10.477040	172.17.20.100	20.207.73.82	TLSv1…	124	Application Data
153	10.477106	172.17.20.100	20.207.73.82	TLSv1…	152	Application Data
154	10.477204	172.17.20.100	20.207.73.82	TLSv1…	209	Application Data
155	10.509787	20.207.73.82	172.17.20.100	TLSv1…	145	Application Data
156	10.510062	20.207.73.82	172.17.20.100	TLSv1…	145	Application Data
157	10.510063	20.207.73.82	172.17.20.100	TLSv1…	130	Application Data
158	10.510112	172.17.20.100	20.207.73.82	TCP	66	50875 → 443 [ACK] Seq=614 Ack=3571 Win=130944 Len=0 TSval=2011063472 TSecr=3679634649
159	10.510160	172.17.20.100	20.207.73.82	TCP	66	50875 → 443 [ACK] Seq=614 Ack=3714 Win=130816 Len=0 TSval=2011063472 TSecr=3679634649
160	10.510265	172.17.20.100	20.207.73.82	TLSv1…	97	Application Data
163	10.586993	20.207.73.82	172.17.20.100	TCP	66	443 → 50875 [ACK] Seq=3714 Ack=645 Win=68608 Len=0 TSval=3679634728 TSecr=2011063472
167	10.747738	20.207.73.82	172.17.20.100	TLSv1…	629	Application Data
168	10.748003	172.17.20.100	20.207.73.82	TCP	66	50875 → 443 [ACK] Seq=645 Ack=4277 Win=130496 Len=0 TSval=2011063710 TSecr=3679634886
169	10.750856	172.17.20.100	20.207.73.82	TLSv1…	193	Application Data
170	10.750965	172.17.20.100	20.207.73.82	TLSv1…	283	Application Data
171	10.779857	20.207.73.82	172.17.20.100	TCP	66	443 → 50875 [ACK] Seq=4277 Ack=772 Win=68608 Len=0 TSval=3679634921 TSecr=2011063713

These are UDP packets, coloured by light blue.



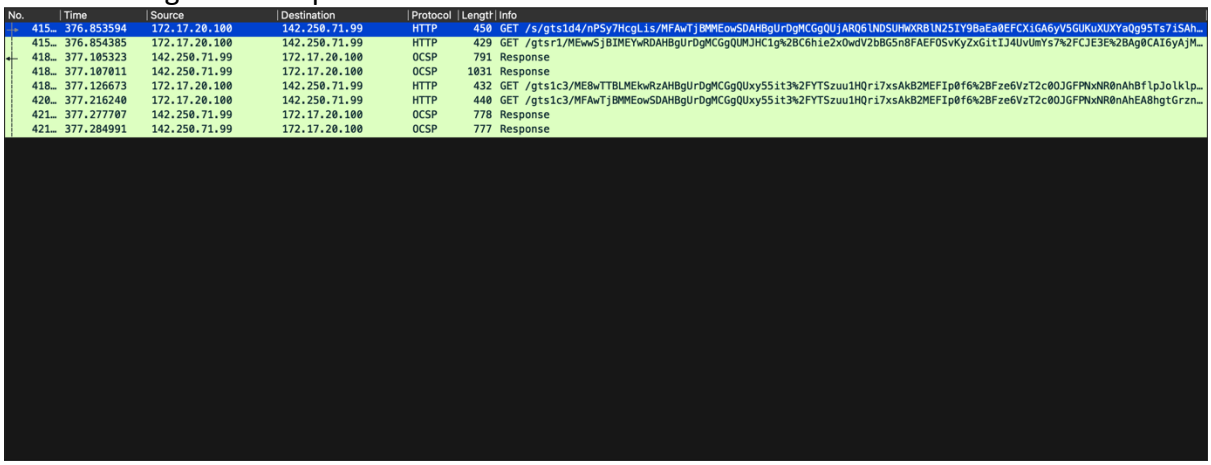
No.	Time	Source	Destination	Protocol	Length	Info
139	10.368255	172.17.20.100	172.17.16.1	DNS	70	Standard query 0xdab3 A github.com
140	10.403706	172.17.16.1	172.17.20.100	DNS	86	Standard query response 0xdab3 A github.com A 20.207.73.82
178	10.952915	172.17.17.97	172.17.23.255	UDP	186	51237 → 51007 Len=144
213	11.540595	172.17.20.100	17.248.162.36	UDP	83	60537 → 443 Len=41
218	11.591659	17.248.162.36	172.17.20.100	UDP	75	443 → 60537 Len=33
230	11.834677	172.17.20.100	172.17.16.1	DNS	74	Standard query 0xca7a A api.github.com
231	11.834742	172.17.20.100	172.17.16.1	DNS	74	Standard query 0x6dca HTTPS api.github.com
232	11.861759	172.17.16.1	172.17.20.100	DNS	158	Standard query response 0x6dca HTTPS api.github.com SOA ns-1707.awsdns-21.co.uk
233	11.866129	172.17.16.1	172.17.20.100	DNS	90	Standard query response 0xca7a A api.github.com A 20.207.73.85
262	12.079477	172.17.17.63	172.17.23.255	UDP	82	47584 → 47584 Len=40
269	12.483215	172.17.20.100	17.248.162.36	UDP	83	60537 → 443 Len=41
272	12.517124	17.248.162.36	172.17.20.100	UDP	75	443 → 60537 Len=33
297	13.597655	172.17.20.100	17.248.162.36	UDP	83	60537 → 443 Len=41
298	13.623569	17.248.162.36	172.17.20.100	UDP	75	443 → 60537 Len=33
299	13.715929	172.17.20.120	172.17.23.255	DB-LS…	187	Dropbox LAN sync Discovery Protocol, JSON
313	15.149034	172.17.17.97	172.17.23.255	UDP	186	51237 → 51007 Len=144
315	15.353591	172.17.21.157	172.17.23.255	UDP	86	57621 → 57621 Len=44
320	15.625215	172.17.20.100	17.248.162.36	UDP	83	60537 → 443 Len=41
321	15.654031	17.248.162.36	172.17.20.100	UDP	75	443 → 60537 Len=33
339	17.195944	172.17.17.63	172.17.23.255	UDP	82	47584 → 47584 Len=40
345	17.654773	172.17.20.100	17.248.162.36	UDP	83	60537 → 443 Len=41
346	17.682319	17.248.162.36	172.17.20.100	UDP	75	443 → 60537 Len=33
352	18.230042	172.17.20.100	142.250.70.54	UDP	72	56103 → 443 Len=30
353	18.230909	172.17.20.100	142.251.42.33	UDP	72	56496 → 443 Len=30
354	18.232060	172.17.20.100	142.250.182.206	UDP	72	53216 → 443 Len=30
360	19.038812	172.17.17.97	172.17.23.255	UDP	186	51237 → 51007 Len=144
370	19.684905	172.17.20.100	17.248.162.36	UDP	83	60537 → 443 Len=41
371	19.713753	17.248.162.36	172.17.20.100	UDP	75	443 → 60537 Len=33
374	20.062455	172.17.22.86	172.17.23.255	UDP	86	57621 → 57621 Len=44
391	21.071153	172.17.20.100	172.17.16.1	DNS	88	Standard query 0x1f74 A static.metafi.codefi.network

The following are UDP QUIC packets.



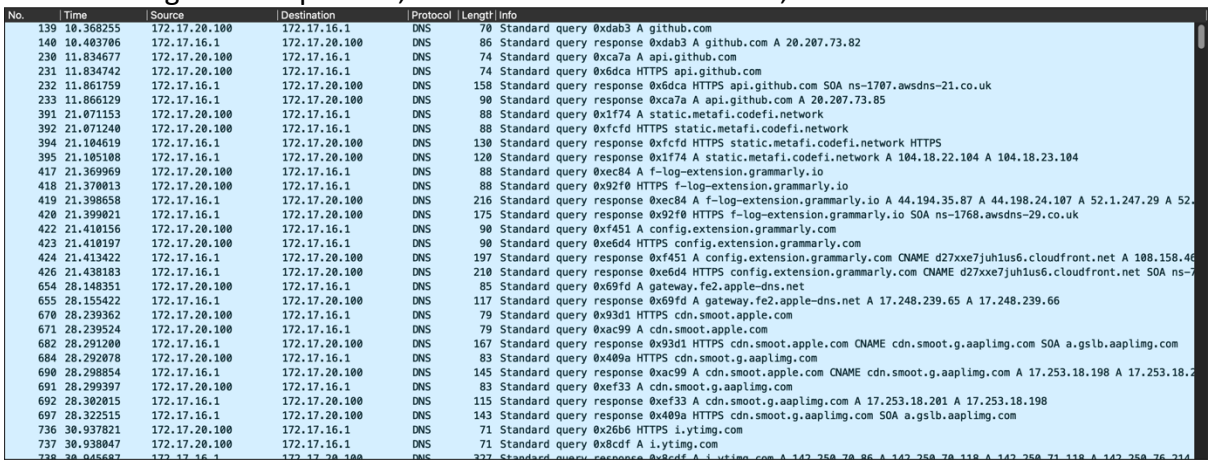
No.	Time	Source	Destination	Protocol	Length	Info
285…	273.396176	142.250.70.54	172.17.20.100	QUIC	1242	Protected Payload (KP0)
285…	273.397882	142.250.70.54	172.17.20.100	QUIC	1242	Protected Payload (KP0)
285…	273.398107	172.17.20.100	142.250.70.54	QUIC	75	Protected Payload (KP0), DCID=e25646fd14e1443b
285…	273.399293	142.250.70.54	172.17.20.100	QUIC	1242	Protected Payload (KP0)
285…	273.403207	142.250.70.54	172.17.20.100	QUIC	1242	Protected Payload (KP0)
285…	273.403418	172.17.20.100	142.250.70.54	QUIC	75	Protected Payload (KP0), DCID=e25646fd14e1443b
285…	273.403837	142.250.70.54	172.17.20.100	QUIC	1242	Protected Payload (KP0)
285…	273.404265	142.250.70.54	172.17.20.100	QUIC	264	Protected Payload (KP0)
285…	273.406886	172.17.20.100	142.250.70.54	QUIC	75	Protected Payload (KP0), DCID=e25646fd14e1443b
285…	273.418110	142.250.70.54	172.17.20.100	QUIC	68	Protected Payload (KP0)
285…	278.429900	172.17.20.100	172.217.194.84	QUIC	1291	Protected Payload (KP0), DCID=e38fd69124d488dd
285…	278.429904	172.17.20.100	172.217.194.84	QUIC	1291	Protected Payload (KP0), DCID=e38fd69124d488dd
285…	278.429910	172.17.20.100	172.217.194.84	QUIC	957	Protected Payload (KP0), DCID=e38fd69124d488dd
285…	278.429974	172.17.20.100	172.217.194.84	QUIC	361	Protected Payload (KP0), DCID=e38fd69124d488dd
285…	278.430085	172.17.20.100	172.217.194.84	QUIC	102	Protected Payload (KP0), DCID=e38fd69124d488dd
285…	278.518294	172.217.194.84	172.17.20.100	QUIC	68	Protected Payload (KP0)
285…	278.522348	172.217.194.84	172.17.20.100	QUIC	72	Protected Payload (KP0)
285…	278.548646	172.217.194.84	172.17.20.100	QUIC	69	Protected Payload (KP0)
285…	278.552693	172.17.20.100	172.217.194.84	QUIC	73	Protected Payload (KP0), DCID=e38fd69124d488dd
285…	278.566882	172.217.194.84	172.17.20.100	QUIC	985	Protected Payload (KP0)
285…	278.567381	172.217.194.84	172.17.20.100	QUIC	76	Protected Payload (KP0)
285…	278.567382	172.217.194.84	172.17.20.100	QUIC	92	Protected Payload (KP0)
285…	278.567573	172.17.20.100	172.217.194.84	QUIC	78	Protected Payload (KP0), DCID=e38fd69124d488dd
285…	278.567792	172.17.20.100	172.217.194.84	QUIC	73	Protected Payload (KP0), DCID=e38fd69124d488dd
285…	278.568206	172.17.20.100	172.217.194.84	QUIC	73	Protected Payload (KP0), DCID=e38fd69124d488dd
285…	278.656503	172.217.194.84	172.17.20.100	QUIC	68	Protected Payload (KP0)
286…	283.386340	172.17.20.100	142.251.42.36	QUIC	71	Protected Payload (KP0), DCID=ffd9927198c198c1
286…	283.468569	142.251.42.36	172.17.20.100	QUIC	72	Protected Payload (KP0)
287…	292.873329	172.17.20.100	142.250.70.106	QUIC	1242	Initial, DCID=91e99b33726c9eb8, PKN: 0, CRYPTO, PADDING
287…	292.900861	142.250.70.106	172.17.20.100	QUIC	1242	Initial, SCID=f1e99b33726c9eb8, PKN: 1, ACK, CRYPTO, PADDING
287…	292.902167	172.17.20.100	142.250.70.106	QUIC	1242	Initial, DCID=f1e99b33726c9eb8, PKN: 1, ACK, PADDING

The following are HTTP packets:



No.	Time	Source	Destination	Protocol	Length	Info
415…	376.853594	172.17.20.100	142.250.71.99	HTTP	450	GET /s/gts1d4/nPSy7HcgLis/MFAwTjBMMEowSDAHBgUrDgMCGgQUjARQ6lNDSUHWXRBlN25IY9BaEa0EFCXiGA6yV5GUKuXUXYaQg95Ts7iSAh…
415…	376.854385	172.17.20.100	142.250.71.99	HTTP	429	GET /gtsr1/MEwwSjBIMEYwRDAHBgUrDgMCGgQUMJHC1g%2BC6hie2xOwdV2bBG5n8FAEFOSvKyZxGit1J4UvUmYs7%2FCJE3E%2BAg0CAI6yAjM…
418…	377.105323	142.250.71.99	172.17.20.100	OCSP	791	Response
418…	377.107011	142.250.71.99	172.17.20.100	OCSP	1031	Response
418…	377.126673	172.17.20.100	142.250.71.99	HTTP	432	GET /gts1c3/ME8wTTBLMEkwRzAHBgUrDgMCGgQUxy55it3%2FYTSzuu1HQri7xsAkB2MEFIp0f6%2BFze6VzT2c0OJGFPNxNR0nAhBflpJolklp…
420…	377.216240	172.17.20.100	142.250.71.99	HTTP	440	GET /gts1c3/MFAwTjBMMEowSDAHBgUrDgMCGgQUxy55it3%2FYTSzuu1HQri7xsAkB2MEFIp0f6%2BFze6VzT2c0OJGFPNxNR0nAhEA8hgtGrzn…
421…	377.277707	142.250.71.99	172.17.20.100	OCSP	778	Response
421…	377.284991	142.250.71.99	172.17.20.100	OCSP	777	Response

The following are DNS packets, which uses UDP underneath, hence the same colour:



No.	Time	Source	Destination	Protocol	Length	Info
139	10.368255	172.17.20.100	172.17.16.1	DNS	70	Standard query 0xdab3 A github.com
140	10.403706	172.17.16.1	172.17.20.100	DNS	86	Standard query response 0xdab3 A github.com A 20.207.73.82
230	11.834677	172.17.20.100	172.17.16.1	DNS	74	Standard query 0xca7a A api.github.com
231	11.834742	172.17.20.100	172.17.16.1	DNS	74	Standard query 0x6dca HTTPS api.github.com
232	11.861759	172.17.16.1	172.17.20.100	DNS	158	Standard query response 0x6dca HTTPS api.github.com SOA ns-1707.awsdns-21.co.uk
233	11.866129	172.17.16.1	172.17.20.100	DNS	90	Standard query response 0xca7a A api.github.com A 20.207.73.85
391	21.071153	172.17.20.100	172.17.16.1	DNS	88	Standard query 0x1f74 A static.metafi.codefi.network
392	21.071240	172.17.20.100	172.17.16.1	DNS	88	Standard query 0xfcfd HTTPS static.metafi.codefi.network
394	21.104619	172.17.16.1	172.17.20.100	DNS	130	Standard query response 0xfcfd HTTPS static.metafi.codefi.network HTTPS
395	21.105108	172.17.16.1	172.17.20.100	DNS	120	Standard query response 0x1f74 A static.metafi.codefi.network A 104.18.22.104 A 104.18.23.104
417	21.369969	172.17.20.100	172.17.16.1	DNS	88	Standard query 0xec84 A f-log-extension.grammarly.io
418	21.370013	172.17.20.100	172.17.16.1	DNS	88	Standard query 0x92f0 HTTPS f-log-extension.grammarly.io
419	21.398658	172.17.16.1	172.17.20.100	DNS	216	Standard query response 0xec84 A f-log-extension.grammarly.io A 44.194.35.87 A 44.198.24.107 A 52.1.247.29 A 52.
420	21.399021	172.17.16.1	172.17.20.100	DNS	175	Standard query response 0x92f0 HTTPS f-log-extension.grammarly.io SOA ns-1768.awsdns-29.co.uk
422	21.410156	172.17.20.100	172.17.16.1	DNS	90	Standard query 0xf451 A config.extension.grammarly.com
423	21.410197	172.17.20.100	172.17.16.1	DNS	90	Standard query 0xe6d4 HTTPS config.extension.grammarly.com
424	21.413422	172.17.16.1	172.17.20.100	DNS	197	Standard query response 0xf451 A config.extension.grammarly.com CNAME d27xxe7juh1us6.cloudfront.net A 108.158.46
426	21.438183	172.17.16.1	172.17.20.100	DNS	210	Standard query response 0xe6d4 HTTPS config.extension.grammarly.com CNAME d27xxe7juh1us6.cloudfront.net SOA ns-7
654	28.148351	172.17.20.100	172.17.16.1	DNS	85	Standard query 0x69fd A gateway.fe2.apple-dns.net
655	28.155422	172.17.16.1	172.17.20.100	DNS	117	Standard query response 0x69fd A gateway.fe2.apple-dns.net A 17.248.239.65 A 17.248.239.66
670	28.239362	172.17.20.100	172.17.16.1	DNS	79	Standard query 0x93d1 HTTPS cdn.smoot.apple.com
671	28.239524	172.17.20.100	172.17.16.1	DNS	79	Standard query 0xac99 A cdn.smoot.apple.com
682	28.291200	172.17.16.1	172.17.20.100	DNS	167	Standard query response 0x93d1 HTTPS cdn.smoot.apple.com CNAME cdn.smoot.g.aaplimg.com SOA a.gslb.aaplimg.com
684	28.292078	172.17.20.100	172.17.16.1	DNS	83	Standard query 0x409a HTTPS cdn.smoot.g.aaplimg.com
690	28.298854	172.17.16.1	172.17.20.100	DNS	145	Standard query response 0xac99 A cdn.smoot.apple.com CNAME cdn.smoot.g.aaplimg.com A 17.253.18.198 A 17.253.18.2
691	28.299397	172.17.20.100	172.17.16.1	DNS	83	Standard query 0xef33 A cdn.smoot.g.aaplimg.com
692	28.302015	172.17.16.1	172.17.20.100	DNS	115	Standard query response 0xef33 A cdn.smoot.g.aaplimg.com A 17.253.18.201 A 17.253.18.198
697	28.322515	172.17.16.1	172.17.20.100	DNS	143	Standard query response 0x409a HTTPS cdn.smoot.g.aaplimg.com SOA a.gslb.aaplimg.com
736	30.937821	172.17.20.100	172.17.16.1	DNS	71	Standard query 0x26b6 HTTPS i.ytimg.com
737	30.938047	172.17.20.100	172.17.16.1	DNS	71	Standard query 0x8cdf A i.ytimg.com
738	30.945687	172.17.16.1	172.17.20.100	DNS	327	Standard query response 0x8cdf A i.ytimg.com A 142.250.70.86 A 142.250.70.118 A 142.250.71.118 A 142.250.76.214

The following are ARP packets:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Intel_f2:db:81	Broadcast	ARP	60	Who has 172.17.19.55? Tell 172.17.20.25
2	0.000183	CenturyXinya_d7:76…	Broadcast	ARP	60	Who has 172.17.21.60? Tell 172.17.17.105
3	0.409445	HewlettPacka_ce:84…	Broadcast	ARP	60	Who has 172.17.21.41? Tell 172.16.1.1
4	0.409493	Intel_6c:42:e2	Broadcast	ARP	60	Who has 172.17.16.1? Tell 172.17.22.15
5	0.614247	HewlettPacka_ce:84…	Broadcast	ARP	60	Who has 172.17.19.8? Tell 172.17.16.1
6	0.818852	CenturyXinya_d7:76…	Broadcast	ARP	60	Who has 172.17.21.60? Tell 172.17.17.105
7	0.818910	HewlettPacka_ce:84…	Broadcast	ARP	60	Who has 172.17.20.48? Tell 172.17.16.1
13	1.228287	HewlettPacka_ce:84…	Broadcast	ARP	60	Who has 172.17.17.240? Tell 172.17.16.1
16	1.432645	HewlettPacka_ce:84…	Broadcast	ARP	60	Who has 172.17.21.41? Tell 172.16.1.1
17	1.637621	HewlettPacka_ce:84…	Broadcast	ARP	60	Who has 172.17.19.8? Tell 172.17.16.1
18	1.842260	CenturyXinya_d7:76…	Broadcast	ARP	60	Who has 172.17.21.60? Tell 172.17.17.105
19	1.842318	HewlettPacka_ce:84…	Broadcast	ARP	60	Who has 172.17.20.48? Tell 172.17.16.1
20	2.251739	HewlettPacka_ce:84…	Broadcast	ARP	60	Who has 172.17.17.240? Tell 172.17.16.1
21	2.251829	HewlettPacka_ce:84…	Broadcast	ARP	60	Who has 172.17.18.205? Tell 172.17.16.1
23	2.456340	4a:91:21:b9:d1:28	Broadcast	ARP	60	Who has 172.17.16.1? Tell 172.17.20.42
24	2.456407	HewlettPacka_ce:84…	Broadcast	ARP	60	Who has 172.17.21.41? Tell 172.16.1.1
25	2.456973	ChongqingFug_f3:26…	Broadcast	ARP	60	Who has 169.254.169.254? Tell 172.17.21.38
26	2.865834	HewlettPacka_ce:84…	Broadcast	ARP	60	Who has 172.17.20.48? Tell 172.17.16.1
28	3.070555	ChongqingFug_f3:26…	Broadcast	ARP	60	Who has 169.254.169.254? Tell 172.17.21.38
29	3.275222	HewlettPacka_ce:84…	Broadcast	ARP	60	Who has 172.17.17.240? Tell 172.17.16.1
30	3.275224	HewlettPacka_ce:84…	Broadcast	ARP	60	Who has 172.17.18.205? Tell 172.17.16.1
39	3.479634	HewlettPacka_ce:84…	Broadcast	ARP	60	Who has 172.17.21.41? Tell 172.16.1.1
46	3.889135	HewlettPacka_ce:84…	Broadcast	ARP	60	Who has 172.17.20.48? Tell 172.17.16.1
47	4.093788	CenturyXinya_d7:76…	Broadcast	ARP	60	Who has 172.17.21.60? Tell 172.17.17.105
48	4.093839	ChongqingFug_f3:26…	Broadcast	ARP	60	Who has 169.254.169.254? Tell 172.17.21.38
49	4.298561	HewlettPacka_ce:84…	Broadcast	ARP	60	Who has 172.17.18.205? Tell 172.17.16.1
50	4.298621	HewlettPacka_ce:84…	Broadcast	ARP	60	Who has 172.17.21.41? Tell 172.16.1.1
51	4.503291	Intel_6c:42:e2	Broadcast	ARP	60	Who has 172.17.16.1? Tell 172.17.22.15
52	4.707917	CenturyXinya_d7:76…	Broadcast	ARP	60	Who has 172.17.21.60? Tell 172.17.17.105
53	5.017877	HewlettPacka_ce:84…	Broadcast	ARP	60	Who has 172.17.20.48? Tell 172.17.16.1

Conclusion

The colour coding and packet sniffing has been better understood using the Wireshark software.

Question 2

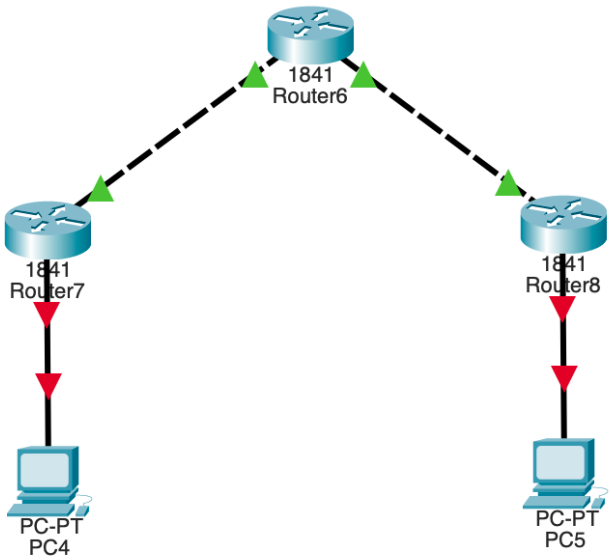
Aim

To configure a VPN tunnelling connection between two routers

Procedure

1. Select 3 1841 routers
2. Connect the routers, the middle one will act as a discovery router between router 1 and 3
3. Connect 2 PCs to the routers 1 and 3
4. Configure IP addresses on all routers and default routing
5. Configure VPN tunnelling between the routers
6. Test the connection

Screenshots



Ping Router 3 from Router 1

```
r1#ping 2.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Ping Router 1 from Router 3

```
r3#ping 1.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Router 1 Tunnel Configuration

```
r1(config)#interface tunnel 10

r1(config-if)#
%LINK-5-CHANGED: Interface Tunnel10, changed state to up

r1(config-if)#ip address 172.16.1.2 255.255.0.0
r1(config-if)#tunnel source fa0/0
r1(config-if)#tunnel destination 2.0.0.2
r1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel10, changed state to up

r1(config-if)#no shut
```

Router 3 Tunnel Configuration

```
r3(config)#interface tunnel 10

r3(config-if)#
%LINK-5-CHANGED: Interface Tunnel10, changed state to up

r3(config-if)#ip address 172.16.1.1 255.255.0.0
r3(config-if)#tunnel source fa0/1
r3(config-if)#tunnel destination 2.0.0.2
r3(config-if)#no shut
r3(config-if)#exit
r3(config)#interface tunnel 10
r3(config-if)#ip address 172.16.1.1 255.255.0.0
r3(config-if)#tunnel source fa0/0
r3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel10, changed state to up

r3(config-if)#tunnel destination 1.0.0.1
r3(config-if)#no shut
```

Ping Router 3 from Router 1

```
r1#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/9 ms
```

Ping Router 1 from Router 3

```
r3#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Setting up VPN Tunnel:

```
r1(config)#ip route 192.168.2.0 255.255.255.0 172.16.1.1
```

```
r3(config)#ip route 192.168.1.0 255.255.255.0 172.16.1.2
```

Results

Viewing Router 1 Tunnel

```
r1#show interfaces tunnel 10
Tunnel10 is up, line protocol is up (connected)
  Hardware is Tunnel
  Internet address is 172.16.1.2/16
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 1.0.0.1 (FastEthernet0/0), destination 2.0.0.2
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 14 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     13 packets input, 1664 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
      0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

Viewing Router 3 Tunnel

```
r3#show interfaces tunnel 10
Tunnel10 is up, line protocol is up (connected)
  Hardware is Tunnel
  Internet address is 172.16.1.1/16
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 2.0.0.2 (FastEthernet0/0), destination 1.0.0.1
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 26 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     14 packets input, 1792 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
      0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

Conclusion

This packet tracer demo has been constructed to successfully demonstrate the connection of two networks (routers) using a VPN tunnelling mechanism.