

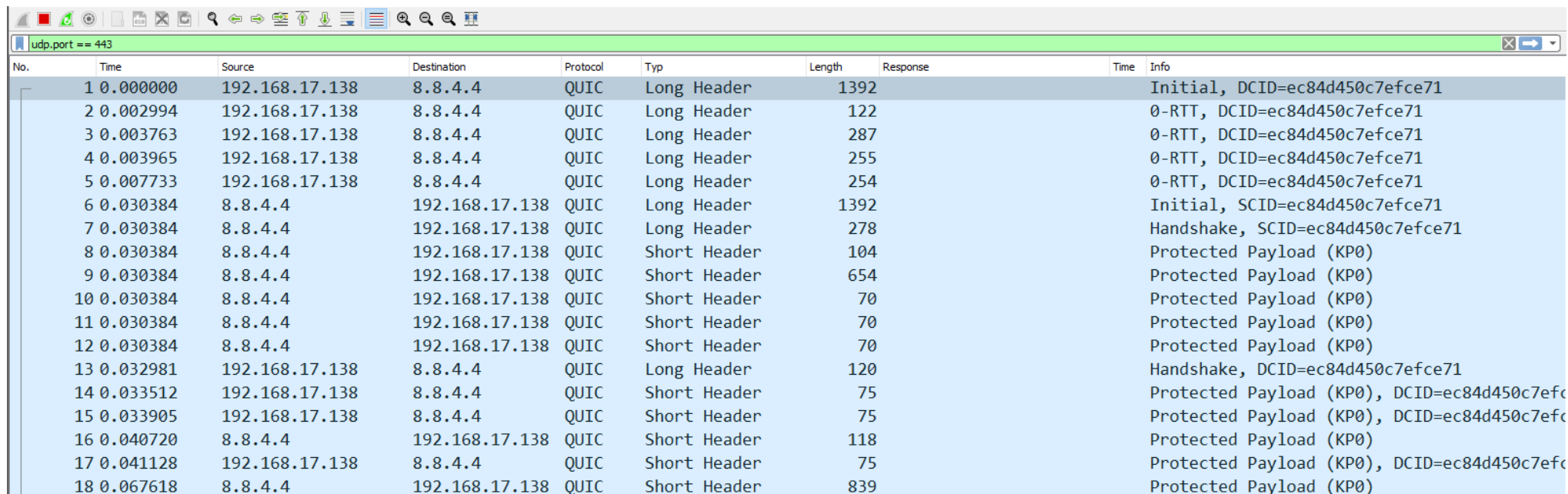
Šablona pro odevzdávání výstupů z distančních cvičení předmětu MPC-PKT určená k editaci a odevzdání po vytvoření PDF verze

Vaše jméno	Alex Sporní
VUT ID	204633
Vypracovaný lab (označení)	Lab8 (HTTPS, QUIC, TCP+TLS)

1. číslovaný úkol z návodu

Zadání úkolu: **Porovnejte pakety s Long Header a Short Header u protokolu QUIC. Spusťte Chrome pomocí příkazového řádku, tak aby jste spustili verzi draft-29. Načtěte zkušební webovou stránku a zachyťte toto načítání stránky pomocí programu Wireshark. Dále pak vytvořte nový sloupec v hlavním okně programu Wireshark, který vám u každého QUIC paketu vypíše použitý typ záhlaví. Využijte řetězec quic.header_form. Jako odpověď na tuto otázku se očekává printscreen obou typů paketů a jejich krátký slovní popis.**

Řešení:



No.	Time	Source	Destination	Protocol	Typ	Length	Response	Time	Info
1	0.000000	192.168.17.138	8.8.4.4	QUIC	Long Header	1392			Initial, DCID=ec84d450c7efce71
2	0.002994	192.168.17.138	8.8.4.4	QUIC	Long Header	122			0-RTT, DCID=ec84d450c7efce71
3	0.003763	192.168.17.138	8.8.4.4	QUIC	Long Header	287			0-RTT, DCID=ec84d450c7efce71
4	0.003965	192.168.17.138	8.8.4.4	QUIC	Long Header	255			0-RTT, DCID=ec84d450c7efce71
5	0.007733	192.168.17.138	8.8.4.4	QUIC	Long Header	254			0-RTT, DCID=ec84d450c7efce71
6	0.030384	8.8.4.4	192.168.17.138	QUIC	Long Header	1392			Initial, SCID=ec84d450c7efce71
7	0.030384	8.8.4.4	192.168.17.138	QUIC	Long Header	278			Handshake, SCID=ec84d450c7efce71
8	0.030384	8.8.4.4	192.168.17.138	QUIC	Short Header	104			Protected Payload (KP0)
9	0.030384	8.8.4.4	192.168.17.138	QUIC	Short Header	654			Protected Payload (KP0)
10	0.030384	8.8.4.4	192.168.17.138	QUIC	Short Header	70			Protected Payload (KP0)
11	0.030384	8.8.4.4	192.168.17.138	QUIC	Short Header	70			Protected Payload (KP0)
12	0.030384	8.8.4.4	192.168.17.138	QUIC	Short Header	70			Protected Payload (KP0)
13	0.032981	192.168.17.138	8.8.4.4	QUIC	Long Header	120			Handshake, DCID=ec84d450c7efce71
14	0.033512	192.168.17.138	8.8.4.4	QUIC	Short Header	75			Protected Payload (KP0), DCID=ec84d450c7efce71
15	0.033905	192.168.17.138	8.8.4.4	QUIC	Short Header	75			Protected Payload (KP0), DCID=ec84d450c7efce71
16	0.040720	8.8.4.4	192.168.17.138	QUIC	Short Header	118			Protected Payload (KP0)
17	0.041128	192.168.17.138	8.8.4.4	QUIC	Short Header	75			Protected Payload (KP0), DCID=ec84d450c7efce71
18	0.067618	8.8.4.4	192.168.17.138	QUIC	Short Header	839			Protected Payload (KP0)

Long Header:

- Pakety typu **Long Header** sa využívajú pri inicializácii spojenia, určeníu verzie a zostavenie 1-RTT kľúčov.
- Obsahujú informácie ako ID spojenia, číslo paketu, verziu, dĺžku rozšírenie headeru atď...

Short Header:

- Pakety typu **Short Header** sa používajú na rýchly prenos dát medzi užívateľmi. Nerieši sa stav linky ani iné parametre.
- Okrem dát, ktoré prenáša obsahuje aj short_header bit, key phase bit, ID spojenia a číslo paketu.

udp.port == 443

No.	Time	Source	Destination	Protocol	Type	Length	Response	Time	Info
1	0.000000	192.168.17.138	8.8.4.4	QUIC	Long Header	1392			Initial, DCID=ec84d450c7efce71

> Frame 1: 1392 bytes on wire (11136 bits), 1392 bytes captured (11136 bits) on interface \Device\NPF_{F54A6428-385F-4667-8D33-4C9ADC633F43}, id 0
> Ethernet II, Src: VMware_28:f7:4b (00:0c:29:28:f7:4b), Dst: VMware_fb:de:3c (00:50:56:fb:de:3c)
> Internet Protocol Version 4, Src: 192.168.17.138, Dst: 8.8.4.4
> User Datagram Protocol, Src Port: 61202, Dst Port: 443

QUIC IETF

> QUIC Connection information
[Packet Length: 1350]
1... = Header Form: Long Header (1)
.1.. = Fixed Bit: True
..00 = Packet Type: Initial (0)
.... 11.. = Reserved: 3
.... ..01 = Packet Number Length: 2 bytes (1)
Version: Unknown (0xff00001d)
Destination Connection ID Length: 8
Destination Connection ID: ec84d450c7efce71
Source Connection ID Length: 0
Token Length: 0
Length: 1332

> [Expert Info (Warning/Decryption): Failed to create decryption context: Decryption (checktag) failed: Checksum error]

8	0.030384	8.8.4.4	192.168.17.138	QUIC	Short Header	104			Protected Payload (KP0)
---	----------	---------	----------------	------	--------------	-----	--	--	-------------------------

> Frame 8: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface \Device\NPF_{F54A6428-385F-4667-8D33-4C9ADC633F43}, id 0
> Ethernet II, Src: VMware_fb:de:3c (00:50:56:fb:de:3c), Dst: VMware_28:f7:4b (00:0c:29:28:f7:4b)
> Internet Protocol Version 4, Src: 8.8.4.4, Dst: 192.168.17.138
> User Datagram Protocol, Src Port: 443, Dst Port: 61202

QUIC IETF

> QUIC Connection information
[Connection Number: 0]
[Packet Length: 62]

> QUIC Short Header
0... = Header Form: Short Header (0)
.1.. = Fixed Bit: True
..0. = Spin Bit: False
Remaining Payload: 53fbe4306c831467beed2405ee3e7f76eaf747401f7a8b22...

2. číslovaný úkol z návodu

Zadání úkolu: **Kolik bajtů dat je potřeba pro přenos informace o používané verzi protokolu QUIC u delší verze záhlaví?**

Řešení: Podľa wiresharku a [zdroja](#) má údaj o verzii veľkosť 32 bitov (4 B)

The image shows a Wireshark packet capture of a QUIC IETF packet. The packet list on the left shows a packet of length 1350. The packet details pane on the right shows the following fields:

- QUIC IETF
 - QUIC Connection information
 - [Connection Number: 0]
 - [Packet Length: 1350]
 - 1... = Header Form: Long Header (1)
 - .1.. = Fixed Bit: True
 - ..00 = Packet Type: Initial (0)
 - 11.. = Reserved: 3
 -01 = Packet Number Length: 2 bytes (1)
 - Version: Unknown (0xff00001d)
 - Destination Connection ID Length: 8
 - Destination Connection ID: ec84d450c7efce71
 - Source Connection ID Length: 0
 - Token Length: 0
 - Length: 1332
 - [Expert Info (Warning/Decryption): Failed to create decryption context: Decryption (checktag) failed: Remaining Payload: b7f013fdbcb5179a66de5c79a62889963aefc8d66ab6d3c6c...

The packet bytes pane at the bottom shows the hex dump of the packet. The first 4 bytes of the packet are 04 04 ef 12, which correspond to the version number 0xff00001d (0x0404ef12 ^ 0xffffffff). The packet bytes pane shows the following data:

Offset	Hex	ASCII
0020	04 04 ef 12 01 bb 05 4e e3 9d ce ff 00 00 1d 08NP...q ..E4....
0030	ec 84 d4 50 c7 ef ce 71 00 00 45 34 b7 f0 13 fdQy.m... b..c...f
0040	cb 51 79 a6 6d e5 c7 9a 62 88 99 63 ae fc 8d 66	..m<li... N...=8..
0050	ab 6d 3c 6c 69 c8 0c 9e 4e 86 a5 3d 94 38 1d 1e	...a...n . "=....
0060	0a e5 8f 61 a7 02 d0 6e cc 7c 22 3d bb 89 e9 e0	..;..... *hz`...
0070	c6 ae 3b 17 f3 a2 a9 ad c6 2a 68 7a ae 60 d2 b3	

The packet bytes pane also shows a legend for the version field: Version (quic.version), 4 bytes.

3. číslovaný úkol z návodu

Zadání úkolu: **Vytvořte si tabulku v hlavním operačním systému, viz Tab. 2.1 (je již v protokolu nachystána), do níž zaznamenejte počet paketů potřebných ke stažení webové stránky v obou dosud zmíněných scénářích.**

Řešení:

Wireshark · Protocol Hierarchy Statistics · Intel(R) 82574L Gigabit Network Connection: Ethernet0

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
▼ Frame	100.0	32799	100.0	35095464	1068 k	0	0	0
▼ Ethernet	100.0	32799	1.3	459186	13 k	0	0	0
▼ Internet Protocol Version 4	100.0	32799	1.9	655980	19 k	0	0	0
▼ User Datagram Protocol	50.3	16513	0.4	132104	4022	0	0	0
QUIC IETF	50.2	16468	48.4	16992343	517 k	16465	16989493	517 k
Data	0.1	48	0.1	21576	656	48	21576	656
▼ Transmission Control Protocol	49.7	16286	48.0	16829792	512 k	7622	5679126	172 k
Transport Layer Security	28.2	9263	48.4	16983334	517 k	8664	13875597	422 k

Display filter: (tcp.port == 443 or udp.port == 443) and !((ip.addr == 8.8.8.8 or ip.addr == 8.8.4.4))

CloseCopyHelp

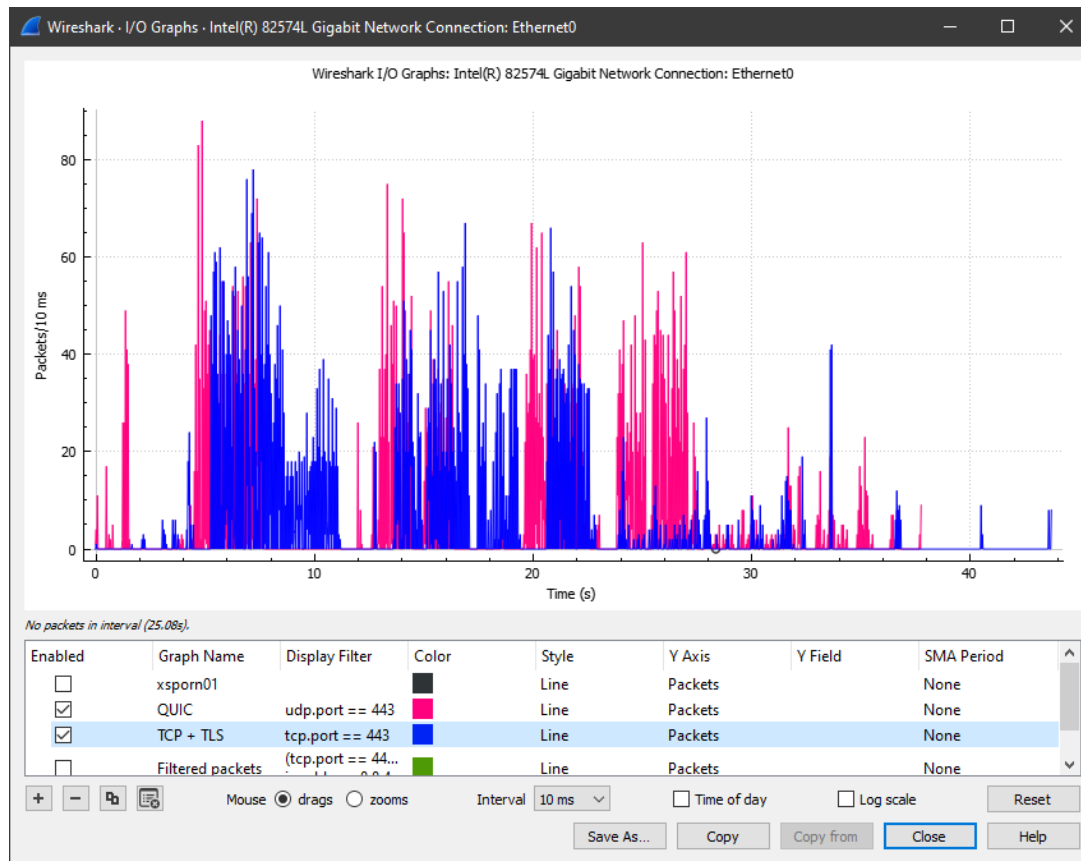
	Omezení hodnoty Bandwidth pro směr (in / out) [kbps]	Přidaný Packet loss pro směr (in/out) [%]	Přidaná latence pro směr (in/out) [ms]	Počet paketů (Packets) [-]	Čas přenosu stránky v Chrome (LOAD) [s]
TCP + TLS	- / -	0 / 0	0 / 0	25 549	16 s
QUIC	- / -	0 / 0	0 / 0	16 516	17,89 s
TCP + TLS	- / -	0 / 0	100 /100	50 104	25,37 s
QUIC	- / -	0 / 0	100 /100	15 060	25,36 s

4. číslovaný úkol z návodu

Zadání úkolu: **Do protokolu uložte vytvořený graf, ve kterém bude vidět váš VUT login, zobrazující počet celkově přenesených paketů protokolu UDP (QUIC) a TCP (TCP+TLS). Zobrazený graf krátce okomentujte.**

Řešení:

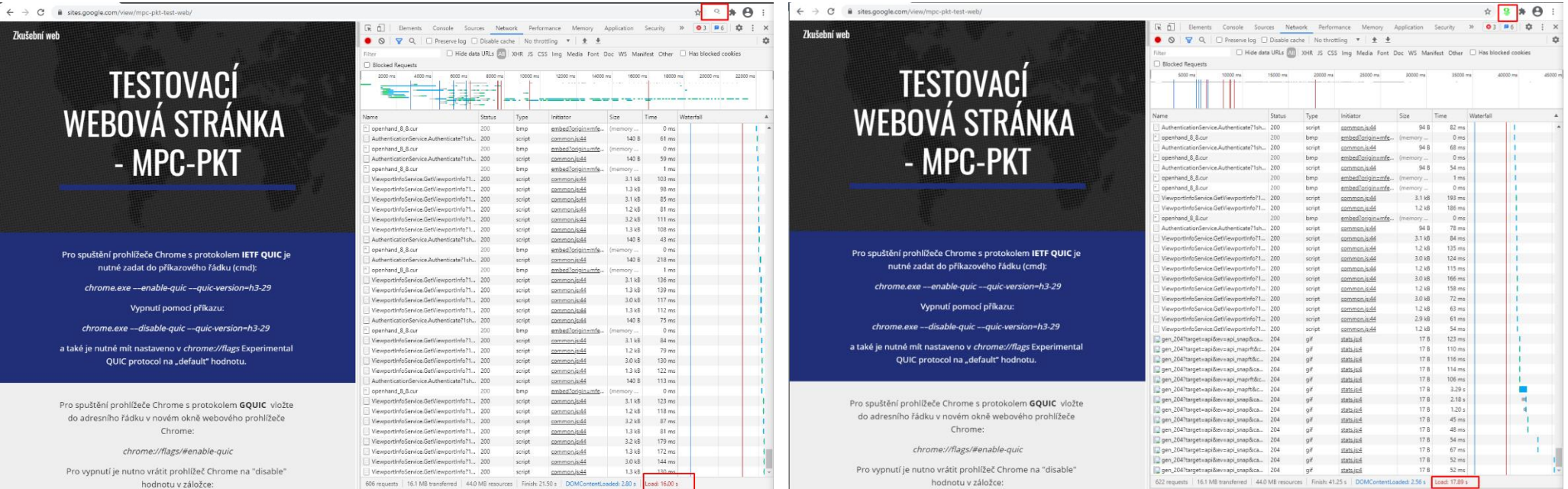
- Zo zadaného grafu môžeme vidieť, že v prípade UDP (QUIC) prenosu sú dosahované vyššie prenosové rýchlosti ako v prípade TCP (TCP + TLS)



5. číslovaný úkol z návodu

Zadání úkolu: Pomocí metody, která je popsána v následujícím odstavci, určete dobu přenosu u obou protokolů a doplňte zjištěné hodnoty do prvních dvou řádků tabulky (poslední sloupec).

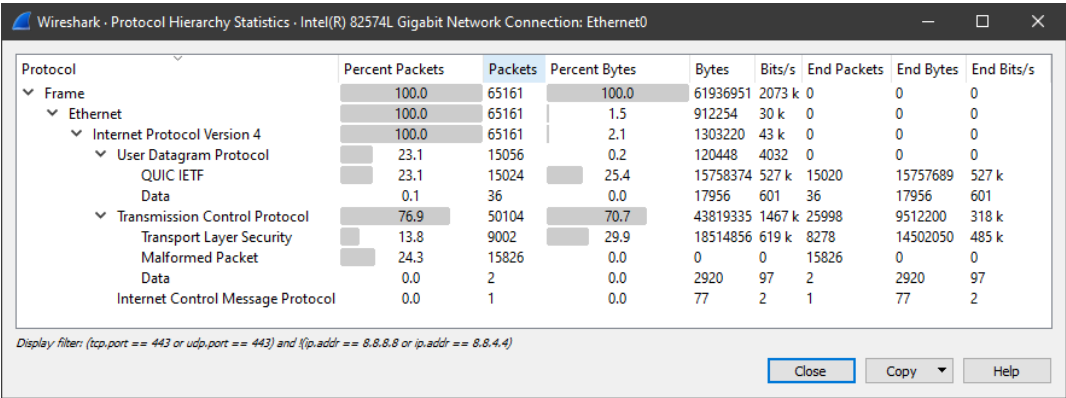
Řešení:



6. číslovaný úkol z návodu

Zadání úkolu: Uložte si printscreen z porovnání protokolů QUIC a TCP+TLS po změně nastavení VMwaru, který jste získali pomocí Statistics > Protocol Hierarchy.

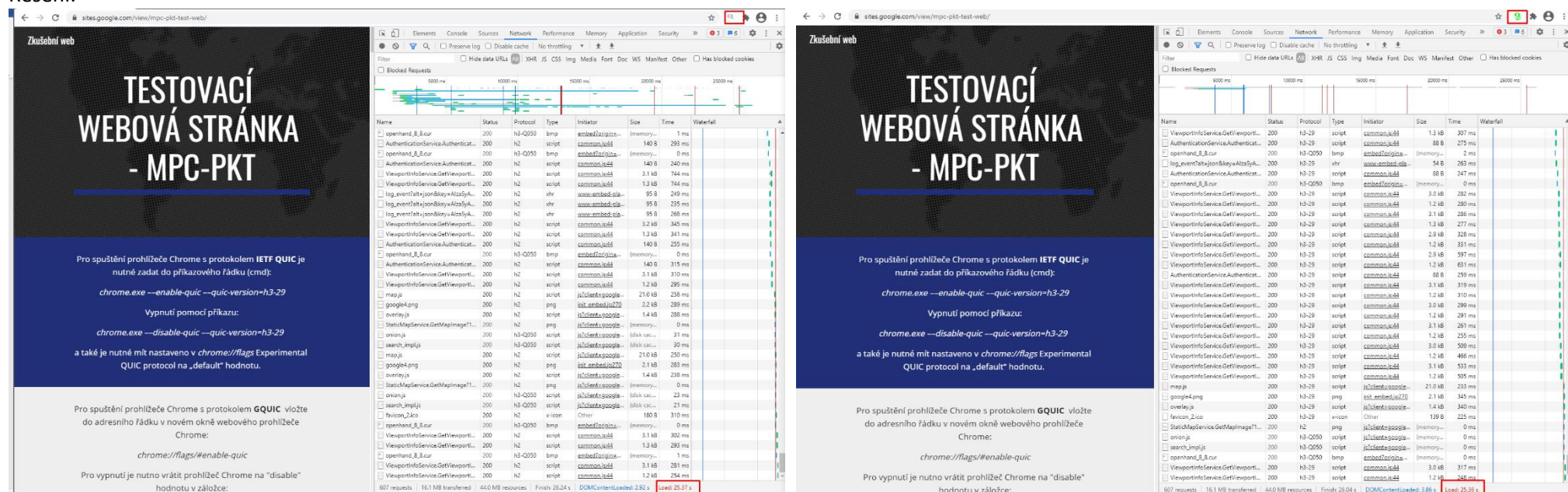
Řešení:



7. číslovaný úkol z návodu

Zadání úkolu: Jak se vložení umělého zpoždění projevilo na době přenosu u jednotlivých protokolů?

Řešení:



- Z vyššie nameraných hodnôt vyplýva, že navýšenie hodnoty latencie spôsobilo dlhšiu dobu prenosu a to v prípade oboch protokolov. V prípade protokolu TCP/TLS došlo k nárastu približne o **9,37 s**. V prípade protokolu QUIC došlo k navýšeniu o **7,47 s**. Z nameraných hodnôt taktiež vyplýva, že protokol QUIC sa lepšie vysporiadal s 200 ms latenciou, čo je pochopiteľné, keďže sa jedná o protokol založený na transportnom protokole UDP, ktorý je menej náročný na réžii.

8. číslovaný úkol z návodu

Zadání úkolu: Okomentujte změnu počtu využitých paketů a také změnu počtu bajtů, které využily oba protokoly dle hodnot zapsaných v tabulce. Při komentování vezměte v potaz, že umělé zhoršení parametrů sítě by mělo mít negativní vliv na některý ze sledovaných parametrů komunikace při přenosu testovací webové stránky.

Řešení: V případě protokolu **QUIC** nedošlo k navýšeniu paketov, práve naopak, bolo poslaných o **1456** paketov menej, ako v prípade bez navýšenej latencie. V prípade protokolu **TCP+TLS** je možno badať dramatické navýšenie paketov. V prípade navýšenia latencie bolo poslaných celkovo o **24 555** paketov viac, čo predstavuje **96 %** nárast v poslaní paketov. Tento jav bol zapríčinený samotným protokolom TCP, ktorý je connection-oriented a obsahuje bezpečnostné mechanizmy na potvrdzovanie doručení jednotlivých paketov. Niektoré pakety museli byť v prípade navýšenia latencie poslané znovu, niektoré museli byť znovu usporiadané aby prišli v správnom poradí, to malo za následok navýšenie celkovej réžie.

48148	31.600769	192.168.17.138	216.58.201.78	TCP	54	[TCP ZeroWindow] 59151 → 443 [ACK] Seq=
48150	31.600776	192.168.17.138	172.217.23.202	TCP	54	[TCP ZeroWindow] 59094 → 443 [ACK] Seq=4
48151	31.600798	192.168.17.138	216.58.201.67	TCP	54	[TCP ZeroWindow] 59155 → 443 [ACK] Seq=1
48152	31.600820	192.168.17.138	172.217.23.227	TCP	54	[TCP ZeroWindow] 59152 → 443 [ACK] Seq=1
48153	31.600842	192.168.17.138	172.217.23.193	TCP	54	[TCP ZeroWindow] 59160 → 443 [ACK] Seq=1
48154	31.604703	172.217.23.238	192.168.17.138	TCP	60	[TCP Out-Of-Order] 443 → 59157 [FIN, PSH
48155	31.604720	192.168.17.138	172.217.23.238	TCP	54	[TCP ZeroWindow] 59157 → 443 [ACK] Seq=2
48156	31.702045	216.58.201.78	192.168.17.138	TCP	60	443 → 59151 [RST] Seq=1466 Win=32767 Len=0
48158	31.702045	172.217.23.202	192.168.17.138	TCP	60	443 → 59094 [RST] Seq=6090105 Win=32767 Len=0
48159	31.702045	216.58.201.67	192.168.17.138	TCP	60	443 → 59155 [RST] Seq=2571 Win=32767 Len=0
48160	31.702045	172.217.23.227	192.168.17.138	TCP	60	443 → 59152 [RST] Seq=16910 Win=32767 Len=0
48161	31.702045	172.217.23.193	192.168.17.138	TCP	60	443 → 59160 [RST] Seq=7350 Win=32767 Len=0
48162	31.706085	172.217.23.238	192.168.17.138	TCP	60	443 → 59157 [RST] Seq=5798 Win=32767 Len=0
48163	31.881815	216.58.201.78	192.168.17.138	TCP	60	443 → 59151 [RST] Seq=1466 Win=32767 Len=0
48182	34.190310	192.168.17.138	172.217.23.238	TCP	54	59165 → 443 [ACK] Seq=518 Ack=3825 Win=6
48183	34.196191	192.168.17.138	172.217.23.238	TLSv1.3	118	Change Cipher Spec, Application Data
48184	34.196458	192.168.17.138	172.217.23.238	TLSv1.3	146	Application Data
48185	34.196704	192.168.17.138	172.217.23.238	TLSv1.3	873	Application Data
48186	34.290326	172.217.23.238	192.168.17.138	TCP	1514	[TCP Out-Of-Order] 443 → 59165 [ACK] Seq=
48187	34.290326	172.217.23.238	192.168.17.138	TCP	1514	[TCP Out-Of-Order] 443 → 59165 [ACK] Seq=
48188	34.290326	172.217.23.238	192.168.17.138	TCP	958	[TCP Spurious Retransmission] 443 → 59165 [ACK] Seq=
48189	34.290362	192.168.17.138	172.217.23.238	TCP	54	[TCP Dup ACK 48182#1] 59165 → 443 [ACK] Seq=
48190	34.290396	192.168.17.138	172.217.23.238	TCP	54	[TCP Dup ACK 48182#2] 59165 → 443 [ACK] Seq=
48191	34.290418	192.168.17.138	172.217.23.238	TCP	54	[TCP Dup ACK 48182#3] 59165 → 443 [ACK] Seq=
48192	34.394554	172.217.23.238	192.168.17.138	TCP	1514	[TCP Out-Of-Order] 443 → 59165 [ACK] Seq=
48193	34.394554	172.217.23.238	192.168.17.138	TCP	1514	[TCP Out-Of-Order] 443 → 59165 [ACK] Seq=
48194	34.394554	172.217.23.238	192.168.17.138	TCP	958	[TCP Spurious Retransmission] 443 → 59165 [ACK] Seq=
48195	34.394652	192.168.17.138	172.217.23.238	TCP	54	[TCP Dup ACK 48182#4] 59165 → 443 [ACK] Seq=

9. číslovaný úkol z návodu

Zadání úkolu: **Ve Wiresharku vytvořte nový sloupec pro daný zachycený provoz zobrazující hodnoty „Destination Connection ID“ a „Source Connection ID“. Využijte řetězec quic.dcid a quic.scid.**

Řešení:

udp.port == 443 and !(ip.addr == 8.8.8.8 or ip.addr == 8.8.4.4)								
No.	Time	Source	Destination	Sour. Conn. ID	Dest. Conn. ID	Protocol	Type	Length
165	3.931274	192.168.17.138	172.217.23.234		94f1cadf5a89bb2c	QUIC	Long Header	139
166	3.931772	192.168.17.138	172.217.23.234		94f1cadf5a89bb2c	QUIC	Long Header	12
167	3.932958	192.168.17.138	216.58.201.67		7c88f29077dcee67	QUIC	Long Header	139
168	3.933439	192.168.17.138	216.58.201.67		7c88f29077dcee67	QUIC	Long Header	12
169	3.936510	192.168.17.138	172.217.23.202		abdfb3bc9db8fdb2	QUIC	Long Header	139
170	3.937125	192.168.17.138	172.217.23.202		abdfb3bc9db8fdb2	QUIC	Long Header	12
171	3.939295	192.168.17.138	172.217.23.206			UDP		29
176	3.948737	172.217.23.206	192.168.17.138			UDP		6
177	3.961801	216.58.201.67	192.168.17.138	7c88f29077dcee67		QUIC	Long Header	139
178	3.961801	216.58.201.67	192.168.17.138	7c88f29077dcee67		QUIC	Long Header	28
179	3.961801	216.58.201.67	192.168.17.138			QUIC	Short Header	10
180	3.962154	216.58.201.67	192.168.17.138			QUIC	Short Header	65
181	3.962558	192.168.17.138	172.217.23.234		94f1cadf5a89bb2c	QUIC	Long Header	139
182	3.963456	172.217.23.202	192.168.17.138	abdfb3bc9db8fdb2		QUIC	Long Header	139
183	3.963456	172.217.23.202	192.168.17.138	abdfb3bc9db8fdb2		QUIC	Long Header	28
184	3.963456	172.217.23.202	192.168.17.138			QUIC	Short Header	10
185	3.963705	172.217.23.202	192.168.17.138			QUIC	Short Header	65
186	3.963885	192.168.17.138	216.58.201.67		7c88f29077dcee67	QUIC	Long Header	12
187	3.964644	192.168.17.138	216.58.201.67		7c88f29077dcee67	QUIC	Short Header	7
194	3.965907	192.168.17.138	172.217.23.202		abdfb3bc9db8fdb2	QUIC	Long Header	12
195	3.966665	192.168.17.138	172.217.23.202		abdfb3bc9db8fdb2	QUIC	Short Header	7
197	3.967736	216.58.201.67	192.168.17.138			QUIC	Short Header	12
198	3.968205	172.217.23.234	192.168.17.138	94f1cadf5a89bb2c		QUIC	Long Header	139
199	3.968205	172.217.23.234	192.168.17.138	94f1cadf5a89bb2c		QUIC	Long Header	27
200	3.968205	172.217.23.234	192.168.17.138			QUIC	Short Header	10
202	3.968611	172.217.23.234	192.168.17.138			QUIC	Short Header	65
204	3.970009	192.168.17.138	172.217.23.234		94f1cadf5a89bb2c	QUIC	Long Header	12
205	3.970176	172.217.23.202	192.168.17.138			QUIC	Short Header	12
206	3.970474	192.168.17.138	172.217.23.234		94f1cadf5a89bb2c	QUIC	Short Header	7
208	3.975275	192.168.17.138	172.217.23.206			UDP		7
211	3.983262	172.217.23.234	192.168.17.138			QUIC	Short Header	12
214	3.997089	192.168.17.138	216.58.201.67		7c88f29077dcee67	QUIC	Short Header	7
215	3.997260	192.168.17.138	172.217.23.202		abdfb3bc9db8fdb2	QUIC	Short Header	7
220	4.009289	192.168.17.138	172.217.23.234		94f1cadf5a89bb2c	QUIC	Short Header	7
221	4.010534	192.168.17.138	216.58.201.78		b961df0cb6319501	QUIC	Long Header	139
222	4.015599	216.58.201.78	192.168.17.138	b961df0cb6319501		QUIC	Long Header	139
223	4.017913	192.168.17.138	216.58.201.78		b961df0cb6319501	QUIC	Long Header	139
224	4.029381	192.168.17.138	216.58.201.78		b961df0cb6319501	QUIC	Long Header	8
225	4.030587	216.58.201.78	192.168.17.138	b961df0cb6319501		QUIC	Long Header	139
226	4.030587	216.58.201.78	192.168.17.138	b961df0cb6319501		QUIC	Long Header	139
227	4.030587	216.58.201.78	192.168.17.138	b961df0cb6319501		QUIC	Long Header	127

10. číslovaný úkol z návodu

Zadání úkolu: Porovnejte Connection ID zachycená v prohlížeči s těmi ve Wiresharku. Shodují se? (Ve Wiresharku nemusí být tyto hodnoty viditelné u všech QUIC paketů.).

Řešení: Áno, jednotlivé Connection ID sa zhodujú, aspoň tie, ktoré bolo možné zachytiť v jednom screenshots

udp.port == 443 and (ip.addr == 8.8.8.8 or ip.addr == 8.8.4.4)

No.	Time	Source	Destination	Sour. Conn. ID	Dest. Conn. ID	Protocol	Type	Length
165	3.931274	192.168.17.138	172.217.23.234		94f1cadf5a89bb2c	QUIC	Long Header	139
166	3.931772	192.168.17.138	172.217.23.234		94f1cadf5a89bb2c	QUIC	Long Header	12
167	3.932958	192.168.17.138	216.58.201.67		7c88f29077dcee67	QUIC	Long Header	139
168	3.933439	192.168.17.138	216.58.201.67		7c88f29077dcee67	QUIC	Long Header	12
169	3.936510	192.168.17.138	172.217.23.202		abdfb3bc9db8fdb2	QUIC	Long Header	139
170	3.937125	192.168.17.138	172.217.23.202		abdfb3bc9db8fdb2	QUIC	Long Header	12
171	3.939295	192.168.17.138	172.217.23.206			UDP		29
176	3.948737	172.217.23.206	192.168.17.138			UDP		6
177	3.961801	216.58.201.67	192.168.17.138	7c88f29077dcee67		QUIC	Long Header	139
178	3.961801	216.58.201.67	192.168.17.138	7c88f29077dcee67		QUIC	Long Header	28
179	3.961801	216.58.201.67	192.168.17.138			QUIC	Short Header	10
180	3.962154	216.58.201.67	192.168.17.138			QUIC	Short Header	65
181	3.962558	192.168.17.138	172.217.23.234		94f1cadf5a89bb2c	QUIC	Long Header	139
182	3.963456	172.217.23.202	192.168.17.138	abdfb3bc9db8fdb2		QUIC	Long Header	139
183	3.963456	172.217.23.202	192.168.17.138	abdfb3bc9db8fdb2		QUIC	Long Header	28
184	3.963456	172.217.23.202	192.168.17.138			QUIC	Short Header	10
185	3.963705	172.217.23.202	192.168.17.138			QUIC	Short Header	65
186	3.963885	192.168.17.138	216.58.201.67		7c88f29077dcee67	QUIC	Long Header	12
187	3.964644	192.168.17.138	216.58.201.67		7c88f29077dcee67	QUIC	Short Header	7
194	3.965907	192.168.17.138	172.217.23.202		abdfb3bc9db8fdb2	QUIC	Long Header	12
195	3.966665	192.168.17.138	172.217.23.202		abdfb3bc9db8fdb2	QUIC	Short Header	7
197	3.967736	216.58.201.67	192.168.17.138			QUIC	Short Header	12
198	3.968205	172.217.23.234	192.168.17.138	94f1cadf5a89bb2c		QUIC	Long Header	139
199	3.968205	172.217.23.234	192.168.17.138	94f1cadf5a89bb2c		QUIC	Long Header	27
200	3.968205	172.217.23.234	192.168.17.138			QUIC	Short Header	10
202	3.968611	172.217.23.234	192.168.17.138			QUIC	Short Header	65
204	3.970009	192.168.17.138	172.217.23.234		94f1cadf5a89bb2c	QUIC	Long Header	12
205	3.970176	172.217.23.202	192.168.17.138			QUIC	Short Header	12
206	3.970474	192.168.17.138	172.217.23.234		94f1cadf5a89bb2c	QUIC	Short Header	7
208	3.975275	192.168.17.138	172.217.23.206			UDP		7
211	3.983262	172.217.23.234	192.168.17.138			QUIC	Short Header	12
214	3.997089	192.168.17.138	216.58.201.67		7c88f29077dcee67	QUIC	Short Header	7
215	3.997260	192.168.17.138	172.217.23.202		abdfb3bc9db8fdb2	QUIC	Short Header	7
220	4.009289	192.168.17.138	172.217.23.234		94f1cadf5a89bb2c	QUIC	Short Header	7
221	4.010534	192.168.17.138	216.58.201.78		b961df0cb6319501	QUIC	Long Header	139
222	4.015599	216.58.201.78	192.168.17.138	b961df0cb6319501		QUIC	Long Header	139
223	4.017913	192.168.17.138	216.58.201.78		b961df0cb6319501	QUIC	Long Header	139
224	4.029381	192.168.17.138	216.58.201.78		b961df0cb6319501	QUIC	Long Header	8
225	4.030587	216.58.201.78	192.168.17.138	b961df0cb6319501		QUIC	Long Header	139
226	4.030587	216.58.201.78	192.168.17.138	b961df0cb6319501		QUIC	Long Header	139
227	4.030587	216.58.201.78	192.168.17.138	b961df0cb6319501		QUIC	Long Header	127

chrome-net-export-log.json

Connection ID 1/1

Code

Import

Proxy

Events

Timeline

DNS

Sockets

Alt-Svc

HTTP/2

QUIC

Reporting

Cache

Modules

Prerender

QUIC Option	Value
Supported Versions	draft29
Connection options	
Max Packet Length	1350
Idle Connection Timeout In Seconds	30
Reduced Ping Timeout In Seconds	15
Packet Reader Yield After Duration in Milliseconds	
Mark QUIC Broken When Network Blackholes	false
Do Not Mark QUIC Broken on Network Changes	false
Retry without Alt-Svc on QUIC Errors	true
Do Not Fragment	false
Allow Server Migrations	false
Migrate Sessions Early V2	false
Migrate Sessions on Network Change V2	false
Retransmittable on Wire Timeout in Milliseconds	false
Disable Bidirectional Streams	false
Race Cert Verification	false
Race Stale DNS On Connection	false
Estimate Initial RTT	false
Force Head of Line Blocking	false
Max Server Configs Stored in Properties	0
Origins To Force QUIC On	
Server Push Cancellation	false

QUIC sessions

[View live QUIC sessions](#)

Host	Version	Peer address	Connection ID	Active stream count	Active streams	Total stream count	Packets Sent	Packets Lost	Packets Received	Connected
41641275-atari-embeds.googleusercontent.com:443										
lh3.googleusercontent.com:443										
lh4.googleusercontent.com:443	draft29	172.217.23.193.443	1914e4cb2a451467	0	None	9	157	0	722	true
lh5.googleusercontent.com:443										
lh6.googleusercontent.com:443										
yt3.ggpht.com:443										
apis.google.com:443	draft29	216.58.201.78.443	b961df0cb6319501	0	None	62	451	0	1916	true
ssl.google.com:443										
www.youtube.com:443										
dns.google:443	draft29	8.8.8.443	bed98e4c971f5d9a	0	None	5	21	0	27	true
fonts.gstatic.com:443	draft29	216.58.201.67.443	7c88f29077dcee67	0	None	12	138	0	531	true
www.gstatic.com:443	draft29	216.58.201.67.443	b2c549f5b0fac4a5	0	None	13	82	0	179	true
fontsource.gstatic.com:443	draft29	216.58.201.66.443	9ad1a465f1e78604	0	None	3	16	0	17	true
googleads.g.doubleclick.net:443	draft29	172.217.23.214.443	6ac17a5de823ddb9	0	None	3	46	0	80	true
ytimg.com:443	draft29	172.217.23.202.443	abdfb3bc9db8fdb2	0	None	256	1326	0	5190	true
maps.googleapis.com:443	draft29	172.217.23.227.443	5b26b6353284559d	0	None	64	437	0	1825	true
www.gstatic.com:443	draft29	172.217.23.195.443	ada9824fc33eaa52	0	None	2	287	0	2100	true
static.doubleclick.net:443	draft29	172.217.23.198.443	a3dac221441aa683	0	None	3	15	0	16	true
www.google.com:443	draft29	172.217.23.196.443	62243ade65c9d404	0	None	35	102	0	152	true

11. číslovaný úkol z návodu

Zadání úkolu: Zobrazte si QUIC pakety zachycené ve Wiresharku. Můžeme zde také zobrazit HTML kód?

Řešení: V programe Wireshark nie je možné si zobrazit HTML kód, pretože Wireshark zachytáva zašifrované pakety. Samotný Wireshark nemá možnosť zistiť aký obsah je posielaný medzi serverom a klientom...

179	3.961801	216.58.201.67	192.168.17.138		QUIC	Short Header	103	Protected Payload (KP0)
180	3.962154	216.58.201.67	192.168.17.138		QUIC	Short Header	654	Protected Payload (KP0)
181	3.962558	192.168.17.138	172.217.23.234	94f1cadf5a89bb2c	QUIC	Long Header	1392	Initial, DCID=94f1cadf5
182	3.963456	172.217.23.202	192.168.17.138	abdfb3bc9db8fdb2	QUIC	Long Header	1392	Initial, SCID=abdfb3bc9
183	3.963456	172.217.23.202	192.168.17.138	abdfb3bc9db8fdb2	QUIC	Long Header	281	Handshake, SCID=abdfb3b
184	3.963456	172.217.23.202	192.168.17.138		QUIC	Short Header	106	Protected Payload (KP0)
185	3.963705	172.217.23.202	192.168.17.138		QUIC	Short Header	654	Protected Payload (KP0)
186	3.963885	192.168.17.138	216.58.201.67	7c88f29077dcee67	QUIC	Long Header	120	Handshake, DCID=7c88f29
187	3.964644	192.168.17.138	216.58.201.67	7c88f29077dcee67	QUIC	Short Header	75	Protected Payload (KP0)
194	3.965907	192.168.17.138	172.217.23.202	abdfb3bc9db8fdb2	QUIC	Long Header	120	Handshake, DCID=abdfb3b

< >

> Frame 179: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface \Device\NPF_{F54A6428-385F-4667-8D33-4C9ADC633F43}, id 0

> Ethernet II, Src: VMware_fb:de:3c (00:50:56:fb:de:3c), Dst: VMware_28:f7:4b (00:0c:29:28:f7:4b)

> Internet Protocol Version 4, Src: 216.58.201.67, Dst: 192.168.17.138

> User Datagram Protocol, Src Port: 443, Dst Port: 52719

▼ QUIC IETF

▼ QUIC Connection information

[Connection Number: 3]

[Packet Length: 61]

▼ QUIC Short Header

0... = Header Form: Short Header (0)

.1.. = Fixed Bit: True

..0. = Spin Bit: False

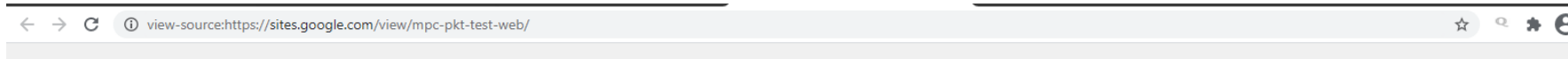
Remaining Payload: 8287f8bf2341343cd5d0aa7f0bb9db6479998dab13d8f4f5...

0000	00 0c 29 28 f7 4b 00 50 56 fb de 3c 08 00 45 00	..)(.K.P V..<..E.
0010	00 59 7c 0f 00 00 80 11 4a d4 d8 3a c9 43 c0 a8	.YJ...:C..
0020	11 8a 01 bb cd ef 00 45 69 0e 4c 82 87 f8 bf 23E i.L....#
0030	41 34 3c d5 d0 aa 7f 0b b9 db 64 79 99 8d ab 13	A4<.....dy....
0040	d8 f4 f5 b9 08 45 7c 89 f6 d5 20 47 3f 69 8b 9fE ... G?i..
0050	df a2 16 f3 11 08 54 fd 8f 40 cb 49 ba 3b 8c c3T. @.I.;..
0060	68 cb 6b e2 cb 2e bb	h.k....

12. číslovaný úkol z návodu

Zadání úkolu: **Posledním úkolem bude nalézt tajný vzkaz schovaný na testovací webové stránce. Kde přesně jste ji hledali v případě utility Netlog viewer? Nápověda: použijte CTRL+F VZKAZ.**

Řešení: Cez filter „mpc“, následne vybrať URL request v programe Netlog viewer... Mne osobne to nenašlo žiadny kód ani po opakovaných logovaniach. Avšak tajný odkaz sa mi podarilo zobrazit' cez zdrojový kód stránky. Vid' screenshot



:f3a9d4d223a0a3fd8b0eec5d/inner-frame-minified.html" data-code="=====TAJNY VZKAZ: KONEC LABORATORNI ULOHY=====" jsaction="rcuQ6b:WYd;"><div class="EmVfjc