

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА  
Факультет прикладної математики та інформатики

Комп'ютерні інформаційні мережі

ЛАБОРАТОРНА РОБОТА №8

Аналіз TCP-сегментів та UDP-датаграм засобами Wireshark

Виконав:

Студент групи ПМі-31

Яцуляк Андрій

2023

**Мета:** Здобути практичні навички з інтерпретації протокольних блоків даних транспортного рівня стеку TCP/IP.

## Хід роботи

1. Опрацював теоретичний матеріал.
2. Використовуючи Wireshark, почав захоплення пакетів. Здійснив активність в браузері, зокрема на сайтах, що працюють за протоколом http, завантажив файл.
3. Зупинив захоплення пакетів. Встановив фільтр tcp || udp:

No.	Time	Source	Destination	Protocol	Length	Info
2782	5.341468	192.168.0.104	176.103.62.204	TCP	54	51097 → 80 [ACK] Seq=966 Ack=63849 Win=132352 Len=0
2786	5.341652	192.168.0.104	176.103.62.204	TCP	54	51097 → 80 [ACK] Seq=966 Ack=68169 Win=132352 Len=0
2788	5.341780	192.168.0.104	176.103.62.204	TCP	54	51097 → 80 [ACK] Seq=966 Ack=69609 Win=132352 Len=0
3075	5.396652	192.168.0.104	176.103.62.204	TCP	54	51097 → 80 [ACK] Seq=966 Ack=86587 Win=132352 Len=0
6049	9.296237	192.168.0.104	176.103.62.204	TCP	54	51097 → 80 [FIN, ACK] Seq=4878 Ack=405175 Win=130816 Len=0
1396	4.940631	192.168.0.104	176.103.62.204	TCP	66	51097 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1413	4.978576	192.168.0.104	216.58.208.202	TCP	54	51098 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
1488	5.011639	192.168.0.104	216.58.208.202	TCP	54	51098 → 80 [ACK] Seq=397 Ack=14121 Win=131072 Len=0
1550	5.050016	192.168.0.104	216.58.208.202	TCP	54	51098 → 80 [ACK] Seq=397 Ack=16945 Win=131072 Len=0
1556	5.050380	192.168.0.104	216.58.208.202	TCP	54	51098 → 80 [ACK] Seq=397 Ack=22593 Win=131072 Len=0
1567	5.052657	192.168.0.104	216.58.208.202	TCP	54	51098 → 80 [ACK] Seq=397 Ack=25417 Win=131072 Len=0
1570	5.054451	192.168.0.104	216.58.208.202	TCP	54	51098 → 80 [ACK] Seq=397 Ack=28241 Win=131072 Len=0
1478	5.010304	192.168.0.104	216.58.208.202	TCP	54	51098 → 80 [ACK] Seq=397 Ack=2825 Win=131072 Len=0
1573	5.055571	192.168.0.104	216.58.208.202	TCP	54	51098 → 80 [ACK] Seq=397 Ack=30637 Win=131072 Len=0
1484	5.011396	192.168.0.104	216.58.208.202	TCP	54	51098 → 80 [ACK] Seq=397 Ack=9885 Win=131072 Len=0
6077	9.329667	192.168.0.104	216.58.208.202	TCP	54	51098 → 80 [ACK] Seq=398 Ack=30638 Win=131072 Len=0
6043	9.296089	192.168.0.104	216.58.208.202	TCP	54	51098 → 80 [FIN, ACK] Seq=397 Ack=30637 Win=131072 Len=0
1403	4.951928	192.168.0.104	216.58.208.202	TCP	66	51098 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1891	5.134961	192.168.0.104	172.217.16.35	TCP	54	51099 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
2023	5.211520	192.168.0.104	172.217.16.35	TCP	54	51099 → 443 [ACK] Seq=1282 Ack=11675 Win=131072 Len=0
2026	5.211870	192.168.0.104	172.217.16.35	TCP	54	51099 → 443 [ACK] Seq=1282 Ack=14499 Win=131072 Len=0
2028	5.212596	192.168.0.104	172.217.16.35	TCP	54	51099 → 443 [ACK] Seq=1282 Ack=15911 Win=131072 Len=0
2030	5.213002	192.168.0.104	172.217.16.35	TCP	54	51099 → 443 [ACK] Seq=1282 Ack=17323 Win=131072 Len=0

Фільтр tcp || udp фільтрує пакети на основі вказаних критеріїв, але не виключає пакети, що містять протоколи вищого рівня, інкапсульовані в TCP або UDP. Іншими словами, фільтр tcp || udp захоплює пакети TCP або UDP, але не відфільтровує пакети, які мають TCP або UDP як транспортні протоколи, а також містять протоколи вищого рівня, такі як DNS або HTTP.

4. Вибрав пакет, що використовує протокол UDP:

243	0.745509	192.168.0.104	34.120.32.134	UDP	81	63177 → 443 Len=39
6480	10.684539	192.168.0.104	34.120.32.134	UDP	81	63177 → 443 Len=39

> Frame 243: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \Device\NPF\_{DA8BD773}

> Ethernet II, Src: CloudNet\_88:42:5f (90:0f:0c:88:42:5f), Dst: Tp-LinkT\_cd:e4:da (ec:08:6b:cd:e4:da)

> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 34.120.32.134

✓ User Datagram Protocol, Src Port: 63177, Dst Port: 443

Source Port: 63177

Destination Port: 443

Порт відправника 63177 динамічно або випадково призначається операційною системою або програмою, яка ініціює зв'язок.

Порт отримувача 443 є фіксованим і вибирається на основі протоколу чи служби, що використовується.

5. Вибрав пакет, що використовує протокол HTTP:

118 0.923190	192.168.0.135	2.21.173.139	HTTP	340 GET /msdownload/update/v3/static/trustedr/en/disallowedcertst1.cab?71ef43b5b087f688 HTTP/1.1	
119 0.948063	2.21.173.139	192.168.0.135	TCP	60 80 → 54569 [ACK] Seq=1 Ack=287 Win=63954 Len=0	
120 0.948044	2.21.173.139	192.168.0.135	HTTP	320 HTTP/1.1 304 Not Modified	
121 0.948896	52.223.194.183	192.168.0.135	TLSv1.2	254 Application Data	
122 0.948825	192.168.0.135	192.168.0.1	DNS	76 Standard query response query name: a.ocsn.entrust.net	
> Frame 118: 340 bytes on wire (2720 bits), 340 bytes captured (2720 bits) on interface \Device\NPF_{F356E22-4213-4C08-AC0B-000000000000} (00:00:00:00:00:00) on interface 0 > Ethernet II, Src: CompalIn_e6:85:3b (08:97:98:e6:85:3b), Dst: Tp-LinkT_81:94:0a (90:9a:4a:81:94:0a) > Internet Protocol Version 4, Src: 192.168.0.135, Dst: 2.21.173.139 > Transmission Control Protocol, Src Port: 54569, Dst Port: 80, Seq: 1, Ack: 1, Len: 286 Source Port: 54569 Destination Port: 80					0000 00 9a 4a 81 94 0a 08 97 98 e6 85 3b 08 00 45 00 ...J.....:E 0010 01 46 0b 1f 40 00 80 06 00 00 c0 a8 00 87 02 15 ...F@..... 0020 ad 8b d5 29 00 50 31 11 0e 65 66 bb 92 62 50 18 ......)P1...ef..bP 0030 fa f0 72 00 00 00 47 45 54 20 2f 6d 73 64 6f 77 ...r...GE T /msdown 0040 6e 6c 6f 61 64 2f 75 70 64 61 74 65 2f 76 33 2f nload/up date/v3/ 0050 73 74 61 74 69 63 2f 74 72 75 73 74 65 64 72 2f static/t rustedr/ 0060 65 6e 2f 6d 69 73 61 6c 6c 6f 77 65 64 63 65 72 en/dical lowdrer
3139 5.401687	192.168.0.104	176.103.62.204	HTTP	582 GET /userfiles/icons/tmb/e2553a12cc7e66e2d3f9e9dfe119322e.png HTTP/1.1	
3186 5.440182	192.168.0.104	176.103.62.204	HTTP	582 GET /userfiles/icons/tmb/e56722ch114d0167472c6894f4193fh7.png HTTP/1.1	
> Frame 3139: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits) on interface \Device\NPF_{DAB... > Ethernet II, Src: CloudNet_88:42:5f (90:0f:0c:88:42:5f), Dst: Tp-LinkT_cd:e4:da (ec:08:6b:cd:e4:da) > Internet Protocol Version 4, Src: 192.168.0.104, Dst: 176.103.62.204 > Transmission Control Protocol, Src Port: 51089, Dst Port: 80, Seq: 2962, Ack: 570292, Len: 528 Source Port: 51089 Destination Port: 80					0000 ec 08 6b cd e4 da 90 0f 0c 88 42 5f 0010 02 38 39 bb 40 00 80 06 0e c1 c0 a8 0020 3e cc c7 91 00 50 98 31 39 7c 0c 60 0030 0c e0 59 f4 00 00 47 45 54 20 2f 75 0040 69 6c 65 73 2f 69 63 6f 6e 73 2f 74 0050 32 35 35 33 61 31 32 63 63 37 65 36 0060 33 66 39 65 39 64 66 65 31 31 39 33

Порт відправника 51089 динамічно або випадково призначається операційною системою або програмою, яка ініціює зв'язок. Порт отримувача 80 є добре відомим портом для HTTP. Це фіксований порт, призначений для протоколу HTTP.

## 6. Знаючи закріплений за HTTPS порт (443), знайшов пакети цього протоколу:

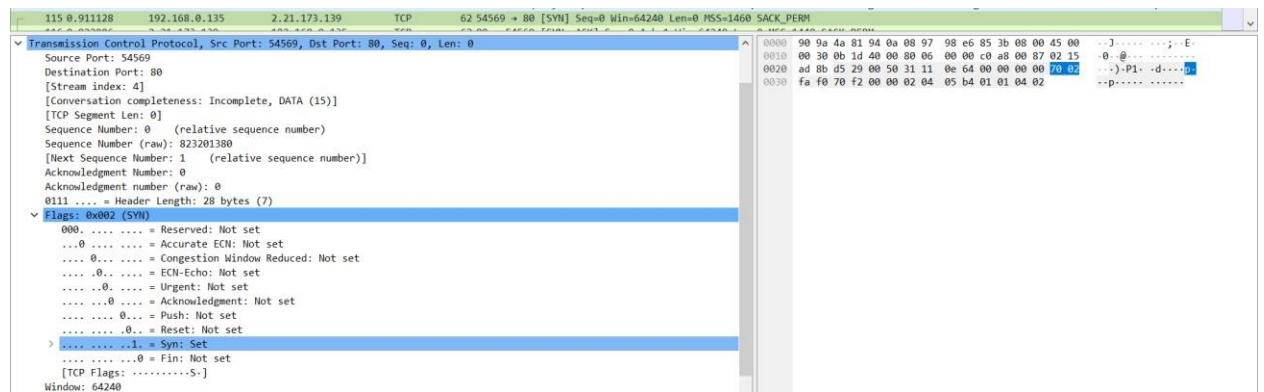
No.	Time	Source	Destination	Protocol	Length	Info
9126 19.314159	192.168.0.104	142.250.203.136	TCP	54	65529 → 443	[FIN, ACK] Seq=1271 Ack=90493 Win=130304 Len=0
7413 12.505559	192.168.0.104	142.250.203.136	TCP	66	65529 → 443	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
8180 15.311514	192.168.0.104	95.46.108.15	TCP	54	65532 → 443	[ACK] Seq=1 Ack=1 Win=132352 Len=0
8190 15.330382	192.168.0.104	95.46.108.15	TCP	54	65532 → 443	[ACK] Seq=597 Ack=2881 Win=132352 Len=0
8194 15.330837	192.168.0.104	95.46.108.15	TCP	54	65532 → 443	[ACK] Seq=597 Ack=4934 Win=132352 Len=0
8200 15.353845	192.168.0.104	95.46.108.15	TCP	54	65532 → 443	[ACK] Seq=605 Ack=4935 Win=132352 Len=0
8196 15.333904	192.168.0.104	95.46.108.15	TCP	54	65532 → 443	[FIN, ACK] Seq=604 Ack=4934 Win=132352 Len=0
8171 15.291246	192.168.0.104	95.46.108.15	TCP	66	65532 → 443	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
8652 17.185426	192.168.0.104	20.50.73.11	TCP	54	65533 → 443	[ACK] Seq=1 Ack=1 Win=132352 Len=0
8680 17.237185	192.168.0.104	20.50.73.11	TCP	1494	65533 → 443	[ACK] Seq=1794 Ack=6255 Win=132352 Len=1440 [TCP segment of a reassembled PDU]
8689 17.285762	192.168.0.104	20.50.73.11	TCP	54	65533 → 443	[ACK] Seq=4640 Ack=6375 Win=132352 Len=0
8700 17.335803	192.168.0.104	20.50.73.11	TCP	54	65533 → 443	[ACK] Seq=4678 Ack=6720 Win=131840 Len=0
12573 26.088406	192.168.0.104	20.50.73.11	TCP	54	65533 → 443	[ACK] Seq=4679 Ack=6721 Win=131840 Len=0
8673 17.234967	192.168.0.104	20.50.73.11	TCP	54	65533 → 443	[ACK] Seq=518 Ack=4321 Win=132352 Len=0
8676 17.235126	192.168.0.104	20.50.73.11	TCP	54	65533 → 443	[ACK] Seq=518 Ack=6255 Win=132352 Len=0
12544 26.039717	192.168.0.104	20.50.73.11	TCP	54	65533 → 443	[FIN, ACK] Seq=4678 Ack=6720 Win=131840 Len=0
8642 17.122210	192.168.0.104	20.50.73.11	TCP	66	65533 → 443	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
8195 15.333838	192.168.0.104	95.46.108.15	TLSv1.2	61	Alert (Level: Fatal, Description: Certificate Unknown)	
10051 21.280823	192.168.0.104	52.173.83.49	TLSv1.2	61	Alert (Level: Fatal, Description: Certificate Unknown)	
379 1.538120	104.18.39.102	192.168.0.104	TLSv1.2	80	Application Data	
380 1.539563	192.168.0.104	104.18.39.102	TLSv1.2	83	Application Data	
1098 4.203042	216.58.215.67	192.168.0.104	TLSv1.3	303	Application Data	
1266 4.716682	176.103.62.204	192.168.0.104	TLSv1.3	76	Application Data	
1286 4.758955	142.250.75.14	192.168.0.104	TLSv1.3	1347	Application Data	
1495 5.022785	142.250.186.202	192.168.0.104	TLSv1.3	667	Application Data	
1500 5.025634	192.168.0.104	142.250.186.202	TLSv1.3	146	Application Data	

Бачу різні протоколи, зокрема TCP та TLSv1.2, TLSv1.3. Це пов'язано з тим, що мережевий трафік часто передбачає кілька рівнів інкапсуляції, а Wireshark відображає протоколи на основі доступних. Отже, сам вміст HTTPS може бути не відразу видимим, якщо трафік зашифровано, і для його розшифровки для аналізу потрібні додаткові кроки.

## 7. Відшукав послідовність пакетів процедури “потрійного рукошестикання”:

115 0.911128	192.168.0.135	2.21.173.139	TCP	62	54569 → 80	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
116 0.922906	2.21.173.139	192.168.0.135	TCP	62	80 → 54569	[SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1440 SACK_PERM
117 0.923058	192.168.0.135	2.21.173.139	TCP	54	54569 → 80	[ACK] Seq=1 Ack=1 Win=64240 Len=0

## 8. Аналіз пакетів з попереднього пункту: 1) Пакет №115:



Порт відправника – 54569, а порт отримувача – 80, який є портом за замовчуванням для HTTP.

Sequence Number (Relative): 0 - відноситься до початкового порядкового номера підключення.

Sequence Number (Raw): 823201380 - є фактичним 32-бітним порядковим номером.

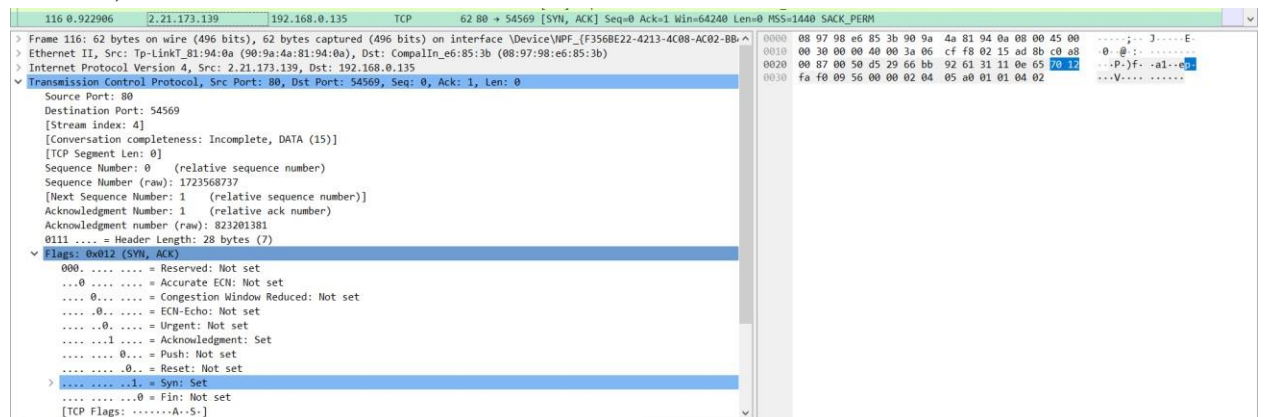
Next Sequence Number (Relative): 1 - вказує на те, що відправник очікує, що наступний пакет матиме порядковий номер 1.

Acknowledgment Number (Relative): 0 - відправник не отримав жодних даних від іншої сторони.

Acknowledgment Number (Raw): 0.

Прапорець 0x002 (SYN) вказує на початок нового TCP-з'єднання. Інші прапорці не встановлені (не використовуються в цьому пакеті).

## 2) Пакет №116:



Порт відправника – 80, який є портом за замовчуванням для HTTP, а порт отримувача – 54569.

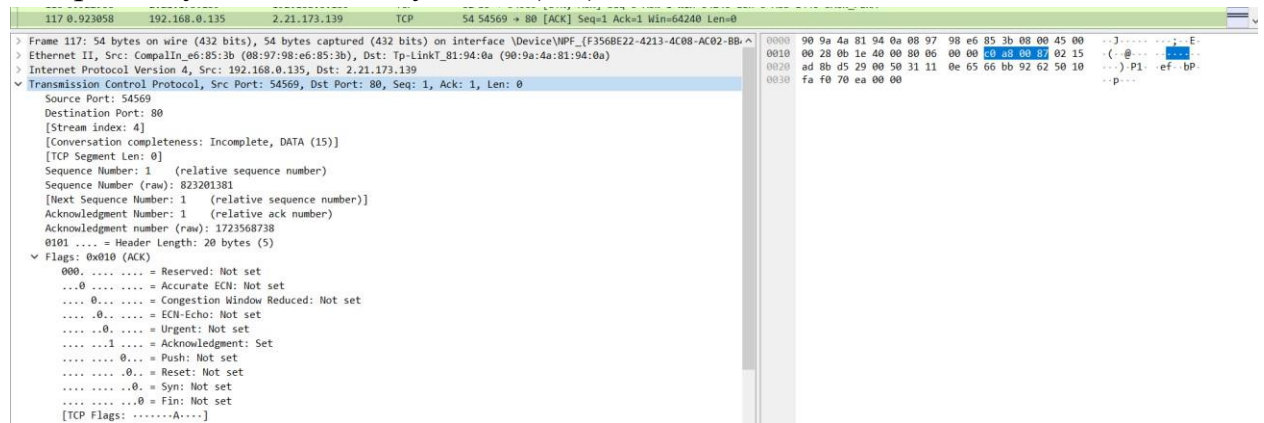
Sequence Number (Relative): 0 - відноситься до початкового порядкового номера підключення.

Sequence Number (Raw): 1723568737- є фактичним 32-бітним порядковим номером.

Next Sequence Number (Relative): 1 - вказує на те, що відправник очікує, що наступний пакет матиме порядковий номер 1.

Acknowledgment Number (Relative): 1 - вказує на те, що відправник отримав перший пакет (з порядковим номером 0). Acknowledgment Number (Raw): 823201381.

Прапорці 0x012 (SYN, ACK) вказують, що це пакет SYN-ACK, який підтверджує отриманий SYN. Інші прапорці не встановлені (не використовуються в цьому пакеті). 3) Пакет №117:



Порт відправника – 54569, а порт отримувача – 80, який є портом за замовчуванням для HTTP.

Sequence Number (Relative): 1 - відноситься до початкового порядкового номера підключення.

Sequence Number (Raw): 823201380 - є фактичним 32-бітним порядковим номером.

Next Sequence Number (Relative): 1 - вказує на те, що відправник очікує, що наступний пакет матиме порядковий номер 1.

Acknowledgment Number (Relative): 1 – вказує на те, що відправник отримав пакет SYN-ACK (з порядковим номером 0) і підтверджує його.

Acknowledgment Number (Raw): 1723568738.

Прапорець 0x010 (ACK) вказує на те, що це пакет ACK, який підтверджує отриманий SYN-ACK. Інші прапорці не встановлені (не використовуються в цьому пакеті).

9. Використовуючи фільтр `tls`, отримав пакети криптографічного протоколу TLS:



No.	Time	Source	Destination	Protocol	Length	Info
6	0.043712	52.223.194.183	192.168.0.135	TLSv1.2	980	Application Data, Application Data
8	0.144569	52.223.194.183	192.168.0.135	TLSv1.2	82	Application Data
14	0.145882	52.223.194.183	192.168.0.135	TLSv1.2	856	Application Data, Application Data
18	0.244564	52.223.194.183	192.168.0.135	TLSv1.2	82	Application Data
19	0.245071	52.223.194.183	192.168.0.135	TLSv1.2	1494	[TCP Previous segment not captured] . Ignored Unknown Record
22	0.245742	52.223.194.183	192.168.0.135	TLSv1.2	1356	Ignored Unknown Record
24	0.267953	172.217.19.99	192.168.0.135	TLSv1.2	127	Application Data
28	0.343060	52.223.194.183	192.168.0.135	TLSv1.2	82	Application Data
32	0.344159	52.223.194.183	192.168.0.135	TCP	1420	[TCP Previous segment not captured] 443 → 62447 [PSH, ACK] Seq=17542 Ack=1 Win=65535 Len=1366 [TCP segment of a reassembled PDU...]
41	0.444331	52.223.194.183	192.168.0.135	TLSv1.2	604	Application Data, Application Data
43	0.543408	52.223.194.183	192.168.0.135	TLSv1.2	82	Application Data
47	0.544580	52.223.194.183	192.168.0.135	TLSv1.2	1494	Application Data
52	0.545436	52.223.194.183	192.168.0.135	TLSv1.2	630	Application Data, Application Data
54	0.643826	52.223.194.183	192.168.0.135	TLSv1.2	82	Application Data
58	0.644934	52.223.194.183	192.168.0.135	TCP	668	[TCP Previous segment not captured] 443 → 62447 [PSH, ACK] Seq=34517 Ack=1 Win=65535 Len=614 [TCP segment of a reassembled PDU...]
61	0.743784	52.223.194.183	192.168.0.135	TLSv1.2	81	Application Data
65	0.744853	52.223.194.183	192.168.0.135	TLSv1.2	1168	Application Data, Application Data
67	0.833995	52.223.194.183	192.168.0.135	TLSv1.2	81	Application Data
71	0.834376	52.223.194.183	192.168.0.135	TLSv1.2	841	Application Data, Application Data, Application Data, Application Data
73	0.837230	192.168.0.135	52.223.194.183	TLSv1.2	1540	Application Data
75	0.863357	52.223.194.183	192.168.0.135	TLSv1.2	299	Application Data
109	0.873534	52.223.194.183	192.168.0.135	TLSv1.2	1185	Application Data
111	0.876194	192.168.0.135	52.223.194.183	TLSv1.2	1535	Application Data
121	0.948896	52.223.194.183	192.168.0.135	TLSv1.2	254	Application Data
123	0.949279	52.223.194.183	192.168.0.135	TLSv1.2	82	Application Data
143	0.953888	52.223.194.183	192.168.0.135	TLSv1.2	1494	Application Data
157	0.959738	52.223.194.183	192.168.0.135	TCP	1210	[TCP Previous segment not captured] 443 → 62447 [PSH, ACK] Seq=100610 Ack=2976 Win=65535 Len=1156 [TCP segment of a reassembled PDU...]
167	1.048737	52.223.194.183	192.168.0.135	TLSv1.2	81	Application Data
171	1.049704	52.223.194.183	192.168.0.135	TLSv1.2	228	Application Data, Application Data
176	1.149139	52.223.194.183	192.168.0.135	TLSv1.2	81	Application Data
180	1.150177	52.223.194.183	192.168.0.135	TLSv1.2	980	Application Data, Application Data
183	1.246102	192.168.0.135	52.223.194.183	TLSv1.2	1396	Application Data

## 10. Обрав пакети, що стосуються процедури TLS-рукоштовування:

7354	12.488112	172.217.16.35	192.168.0.104	TLSv1.3	1466	Application Data
7357	12.488822	192.168.0.104	172.217.16.35	TLSv1.3	93	Application Data
7358	12.489384	172.217.16.35	192.168.0.104	TLSv1.3	1466	Application Data

### Аналіз пакетів:

#### 1) Пакет № 7354:

7354	12.488112	172.217.16.35	192.168.0.104	TLSv1.3	1466	Application Data
7357	12.488822	192.168.0.104	172.217.16.35	TLSv1.3	93	Application Data

> Frame 7354: 1466 bytes on wire (11728 bits), 1466 bytes captured (11728 bits) on interface \Device\NPF...

> Ethernet II, Src: Tp-LinkT\_cd:e4:da (ec:08:6b:cd:e4:da), Dst: CloudNet\_88:42:5f (90:0f:0c:88:42:5f)

> Internet Protocol Version 4, Src: 172.217.16.35, Dst: 192.168.0.104

✓ Transmission Control Protocol, Src Port: 443, Dst Port: 65525, Seq: 133106, Ack: 1519, Len: 1412

Source Port: 443

Destination Port: 65525

[Stream index: 36]

[Conversation completeness: Complete, WITH\_DATA (31)]

[TCP Segment Len: 1412]

Sequence Number: 133106 (relative sequence number)

Sequence Number (raw): 2902651423

[Next Sequence Number: 134518 (relative sequence number)]

Acknowledgment Number: 1519 (relative ack number)

Acknowledgment number (raw): 4157094917

0101 .... = Header Length: 20 bytes (5)

✓ Flags: 0x010 (ACK)

000. .... = Reserved: Not set

...0 .... = Accurate ECN: Not set

.... 0... = Congestion Window Reduced: Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 = Acknowledgment: Set

.... .... 0... = Push: Not set

.... .... .0.. = Reset: Not set

.... .... ..0. = Syn: Not set

.... .... ...0 = Fin: Not set

[TCP Flags: .....A.....]

Порт відправника – 443, який є портом за замовчуванням для HTTPS, а порт отримувача – 65525.

Sequence Number (Relative): 133106 - відноситься до початкового порядкового номера підключення.

Sequence Number (Raw): 2902651423 - є фактичним 32-бітним порядковим номером.

Next Sequence Number (Relative): 134518 - вказує на те, що відправник очікує, що наступний пакет матиме порядковий номер 134518.

Acknowledgment Number (Relative): 1519 – вказує на те, що відправник отримав дані до порядкового номера 1519 і підтверджує це.

Acknowledgment Number (Raw): 4157094917.

Прапорці 0x010 (ACK) вказують на те, що дані надсилаються на прикладний рівень.

Інші прапорці не встановлені (не використовуються в цьому пакеті).

## 2) Пакет № 7357:

7357	12.488822	192.168.0.104	172.217.16.35	TLSv1.3	93	Application Data
7358	12.488824	172.217.16.35	192.168.0.104	TLSv1.3	1466	Application Data

> Frame 7357: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF\_{DA8B...} ^  
> Ethernet II, Src: CloudNet\_88:42:5f (90:0f:0c:88:42:5f), Dst: Tp-LinkT\_cd:e4:da (ec:08:6b:cd:e4:da)  
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 172.217.16.35  
✓ Transmission Control Protocol, Src Port: 65525, Dst Port: 443, Seq: 1519, Ack: 135930, Len: 39  
    Source Port: 65525  
    Destination Port: 443  
    [Stream index: 36]  
    [Conversation completeness: Complete, WITH\_DATA (31)]  
    [TCP Segment Len: 39]  
    Sequence Number: 1519      (relative sequence number)  
    Sequence Number (raw): 4157094917  
    [Next Sequence Number: 1558      (relative sequence number)]  
    Acknowledgment Number: 135930      (relative ack number)  
    Acknowledgment number (raw): 2902654247  
    0101 .... = Header Length: 20 bytes (5)  
    ✓ Flags: 0x018 (PSH, ACK)  
        000. .... = Reserved: Not set  
        ...0 .... = Accurate ECN: Not set  
        .... 0... = Congestion Window Reduced: Not set  
        .... .0.. = ECN-Echo: Not set  
        .... ..0. = Urgent: Not set  
        .... ...1 .... = Acknowledgment: Set  
        .... .... 1... = Push: Set  
        .... .... .0.. = Reset: Not set  
        .... .... ..0. = Syn: Not set  
        .... .... ...0 = Fin: Not set  
    [TCP Flags: .....AP...]

Порт відправника – 65525, а порт отримувача – 443, який є портом за замовчуванням для HTTPS.

Sequence Number (Relative): 1519 - відноситься до початкового порядкового номера підключення.

Sequence Number (Raw): 4157094917 - є фактичним 32-бітним порядковим номером.

Next Sequence Number (Relative): 1558 - вказує на те, що відправник очікує, що наступний пакет матиме порядковий номер 1558.

Acknowledgment Number (Relative): 135930 – вказує на те, що відправник отримав дані до порядкового номера 135930 і підтверджує це.

Acknowledgment Number (Raw): 2902654247.

Прапорці 0x018 (PSH, ACK) вказують на те, що це кадр підтвердження з функцією push, припускаючи, що дані надсилаються на прикладний рівень.

Інші прапорці не встановлені (не використовуються в цьому пакеті).

### 3) Пакет № 7358:

7358	12.489384	172.217.16.35	192.168.0.104	TLSv1.3	1466 Application Data
7358	12.489384	172.217.16.35	192.168.0.104	TLSv1.3	1466 Application Data
> Frame 7358: 1466 bytes on wire (11728 bits), 1466 bytes captured (11728 bits) on interface \Device\NPF{...}					
> Ethernet II, Src: Tp-LinkT_cd:e4:da (ec:08:6b:cd:e4:da), Dst: CloudNet_88:42:5f (90:0f:0c:88:42:5f)					
> Internet Protocol Version 4, Src: 172.217.16.35, Dst: 192.168.0.104					
✓ Transmission Control Protocol, Src Port: 443, Dst Port: 65525, Seq: 135930, Ack: 1519, Len: 1412					
Source Port: 443					
Destination Port: 65525					
[Stream index: 36]					
[Conversation completeness: Complete, WITH_DATA (31)]					
[TCP Segment Len: 1412]					
Sequence Number: 135930 (relative sequence number)					
Sequence Number (raw): 2902654247					
[Next Sequence Number: 137342 (relative sequence number)]					
Acknowledgment Number: 1519 (relative ack number)					
Acknowledgment number (raw): 4157094917					
0101 .... = Header Length: 20 bytes (5)					
✓ Flags: 0x010 (ACK)					
000. .... = Reserved: Not set					
...0 .... = Accurate ECN: Not set					
.... 0... = Congestion Window Reduced: Not set					
.... .0.. = ECN-Echo: Not set					
.... ..0. = Urgent: Not set					
.... ...1 = Acknowledgment: Set					
.... .... 0... = Push: Not set					
.... .... .0.. = Reset: Not set					
.... .... ..0. = Syn: Not set					
.... .... ...0 = Fin: Not set					
[TCP Flags: .....A....]					

Порт відправника – 443, який є портом за замовчуванням для HTTPS, а порт отримувача – 65525.

Sequence Number (Relative): 135930 - відноситься до початкового порядкового номера підключення.

Sequence Number (Raw): 2902654247 - є фактичним 32-бітним порядковим номером.

Next Sequence Number (Relative): 137342 - вказує на те, що відправник очікує, що наступний пакет матиме порядковий номер 137342.

Acknowledgment Number (Relative): 1519 – вказує на те, що відправник отримав дані до порядкового номера 1519 і підтверджує це.

Acknowledgment Number (Raw): 4157094917.

Прапорці 0x010 (ACK) вказують на те, що дані надсилаються на прикладний рівень.

Інші прапорці не встановлені (не використовуються в цьому пакеті).

### 11. Вибравши пакет з даними, переконався, що вони зашифровані:

379	1.538120	104.18.39.102	192.168.0.104	TLSv1.2	80 Application Data
380	1.539563	192.168.0.104	104.18.39.102	TLSv1.2	83 Application Data
> Frame 379: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF_{DABBD773...}					
> Ethernet II, Src: Tp-LinkT_cd:e4:da (ec:08:6b:cd:e4:da), Dst: CloudNet_88:42:5f (90:0f:0c:88:42:5f)					
> Internet Protocol Version 4, Src: 104.18.39.102, Dst: 192.168.0.104					
> Transmission Control Protocol, Src Port: 443, Dst Port: 50770, Seq: 1, Ack: 1, Len: 25					
✓ Transport Layer Security					
✓ TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol					
Content Type: Application Data (23)					
Version: TLS 1.2 (0x0303)					
Length: 20					
Encrypted Application Data: dd62bc241529525d4a49b368da2112377b914722					
[Application Data Protocol: Hypertext Transfer Protocol]					

0000	90 0f 0c 88 42 5f ec 08 6b cd e4 da 08 00 45 00	...B...k....E
0010	00 41 77 a1 40 00 3b 06 77 8d 68 12 27 66 c0 a8	...Aw@...w.h'f..
0020	00 68 01 bb c6 52 10 b1 9f be b8 42 0a 2f 50 18	...h...R...B./P
0030	00 08 2a 13 00 00 17 03 03 00 14 dd 62 bc 24 15	...*.....b-\$
0040	29 52 5d 4a 49 b3 68 4a 21 12 37 7b 91 47 22 6b	[R]]I-hj l-7(-Gk



**Висново:** Під час виконання лабораторної роботи я здобув практичні навички з інтерпретації протокольних блоків даних транспортного рівня стеку TCP/IP.