



МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ  
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ  
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»  
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ  
Кафедра Інформаційної Безпеки

### Практикум з Основ комп'ютерних мереж

Дослідження мережних протоколів HTTP, HTTPS, SSL/TLS та DNS

Перевірив:

\_\_\_\_\_

Виконав:

студент I курсу

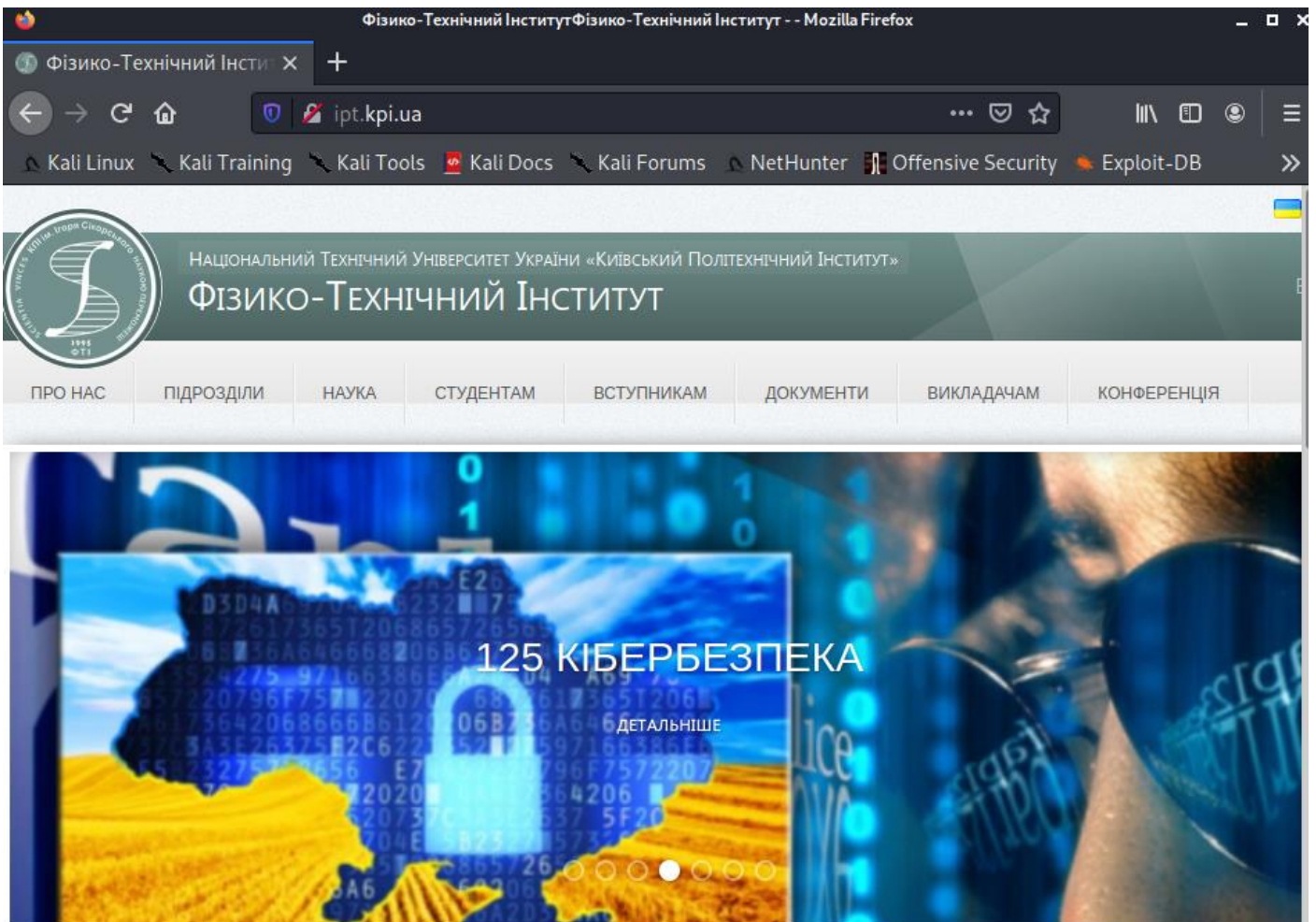
групи ФБ-01

Сахній Н.Р.

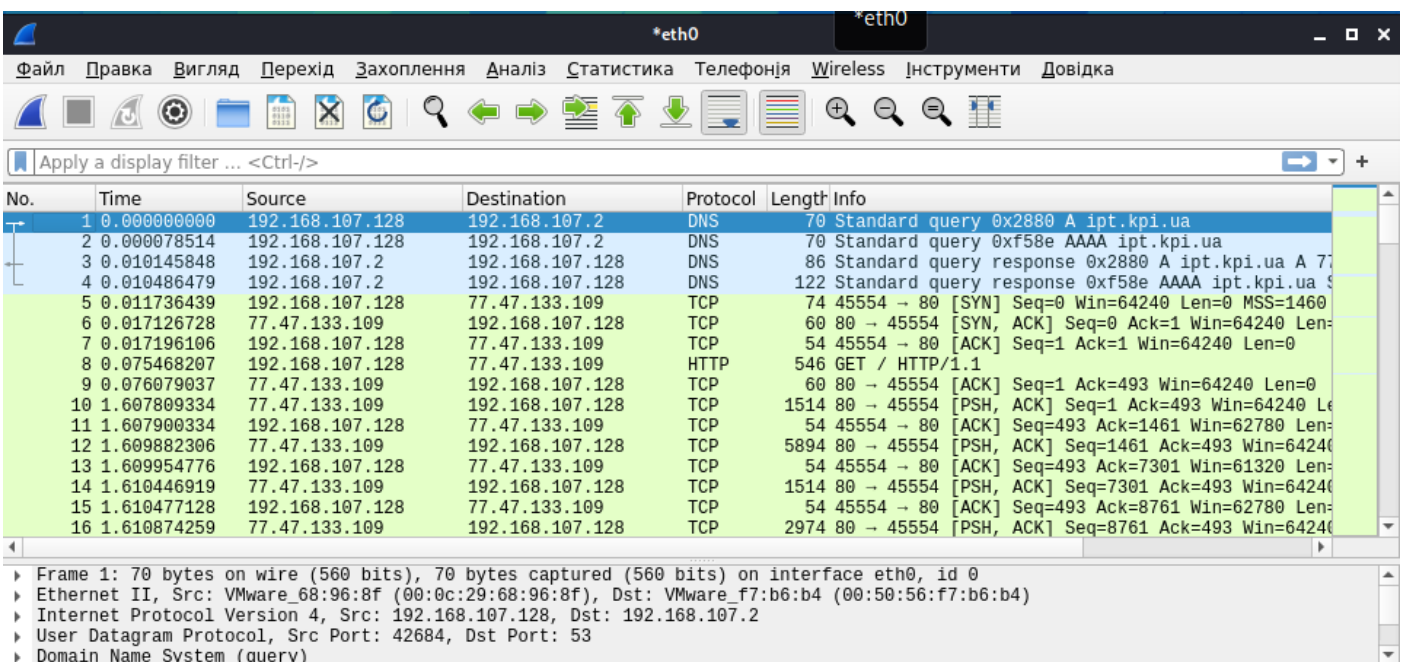
Київ 2021

## Протокол HTTP

2. Тепер, послуговуючись браузером, відкрийте за протоколом HTTP деяку Web-сторінку. Які вкладені об'єкти вона містить? Із даних записаних пакетів збережіть окремим файлом деякий графічний об'єкт (картинку у форматі jpg, gif, png, тощо). Скільки було встановлено з'єднань для завантаження Web сторінки повністю?



Відкривши Web-сторінку <http://ipt.kpi.ua>,  
перехопимо пакети у Wireshark



Wireshark · Export · HTTP object list

Text Filter:

Пакет	Hostname	Content Type	Size	Filename
18	ipt.kpi.ua	text/html	46kB	/
43	ipt.kpi.ua	image/png	446 bytes	uk.png
57	ipt.kpi.ua	image/png	609 bytes	en_US.png
93	ipt.kpi.ua	image/png	10kB	Logo-Samsung11.png
111	ipt.kpi.ua	image/jpeg	22kB	Bufer-obmena-1.jpg
168	ipt.kpi.ua	image/png	12kB	NAZYAVO.png
178	ipt.kpi.ua	image/jpeg	48kB	Rukopozhatye.jpg
255	ipt.kpi.ua	image/png	135kB	logo2.png
273	ipt.kpi.ua	image/png	229kB	opacity-logo1.png
279	ipt.kpi.ua	image/png	63kB	Novykov1.png
295	ipt.kpi.ua	image/jpeg	5 779 bytes	Partnerstvo.jpg
345	ipt.kpi.ua	image/png	78kB	SoftServ.png
346	ipt.kpi.ua	image/jpeg	12kB	Gomonaj.jpg
360	ipt.kpi.ua	image/png	66kB	logo.png
371	ipt.kpi.ua	image/png	58kB	Konf2.png
410	ipt.kpi.ua	image/png	62kB	Monastyrskiy.pr
433	ocsp.pki.goog	application/ocsp-request	84 bytes	gts101core
435	ocsp.pki.goog	application/ocsp-response	472 bytes	gts101core
474	ipt.kpi.ua	image/png	27kB	gbg2.png
475	ipt.kpi.ua	image/png	3 195 bytes	grad_1.png
478	ipt.kpi.ua	image/png	987 bytes	grad_3.png
480	ipt.kpi.ua	image/png	1 303 bytes	grad_2.png
538	ipt.kpi.ua	image/jpeg	133kB	Kiberbezpeka0.jpg
602	ipt.kpi.ua	image/jpeg	59kB	VFT.jpg
657	ipt.kpi.ua	image/png	17kB	sharpen_grad2.png
662	ipt.kpi.ua	image/jpeg	71kB	Prykladnaya-fyzyka.jpg
708	ipt.kpi.ua	image/jpeg	88kB	Prykladnaya-matematyka02.jpg
773	ipt.kpi.ua	image/gif	15kB	loadingAnimation.gif

Зберегти Зберегти все Preview Закрити Довідка

Wireshark · Save All Objects In...

Перегляд в: /hom...енти

Комп'ютер root

Тека:

Тип файлів: Теки

Обрати Скасувати

Дана сторінка містить графічні та html об'єкти, які можна завантажити на власний комп'ютер.

Wireshark · Conversations · eth0

TCP · 27

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
192.168.107.128	45554	77.47.133.109	80	108	235k	54	5 627	54	2
192.168.107.128	36846	69.16.175.10	80	7	416	4	236	3	
192.168.107.128	36848	69.16.175.10	80	7	416	4	236	3	
192.168.107.128	36850	69.16.175.10	80	7	416	4	236	3	
192.168.107.128	45562	77.47.133.109	80	97	218k	45	6 928	52	2
192.168.107.128	45564	77.47.133.109	80	182	491k	91	8 385	91	4
192.168.107.128	45566	77.47.133.109	80	114	207k	56	6 425	58	2
192.168.107.128	45568	77.47.133.109	80	70	125k	35	3 513	35	1
192.168.107.128	45570	77.47.133.109	80	394	995k	196	13k	198	9
192.168.107.128	33018	77.87.193.106	443	36	36k	18	1 986	18	
192.168.107.128	52446	142.250.180.202	443	27	7 383	14	2 010	13	5
192.168.107.128	57424	142.250.180.195	80	10	1 658	6	722	4	
192.168.107.128	56138	52.84.109.3					162	2	
192.168.107.128	39866	93.184.220.1					162	2	
192.168.107.128	36482	172.217.20.1					3 167	19	6

Щоб завантажити Web-сторінку повністю було встановлено 27 з'єднань

Визначення імен Limit to display filter Absolute start time Conversation Types

Скопіювати Follow Stream... Graph... Закрити Довідка

### 3. Знайдіть деяку Web-форму, що дозволяє передавати, файли та проаналізуйте, як завантажуються файли на сервер.

gaia.cs.umass.edu/wireshark-lab3-1-reply.htm

120%

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

Congratulations!

You've now transferred a copy of alice.txt from your computer to gaia.cs.umass.edu. You should now stop Wireshark packet capture. It's time to start analyzing the captured Wireshark packets!

tcp

No.	Time	Source	Destination	Protocol	Length	Info
16	4.048380	192.168.1.144	128.119.245.12	TCP	74	46170 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=14
17	4.163132	128.119.245.12	192.168.1.144	TCP	74	80 → 46170 [SYN, ACK] Seq=0 Ack=1 Win=28960 L
18	4.163334	192.168.1.144	128.119.245.12	TCP	66	46170 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0
19	4.164281	192.168.1.144	128.119.245.12	TCP	2962	46170 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 L
20	4.164769	192.168.1.144	128.119.245.12	TCP	2962	46170 → 80 [PSH, ACK] Seq=2897 Ack=1 Win=6425
21	4.165096	192.168.1.144	128.119.245.12	TCP	2962	46170 → 80 [PSH, ACK] Seq=5793 Ack=1 Win=6425
24	4.280917	192.168.1.144	128.119.245.12	TCP	2962	46170 → 80 [PSH, ACK] Seq=14481 Ack=1 Win=642
26	4.281943	128.119.245.12	192.168.1.144	TCP	66	80 → 46170 [ACK] Seq=1 Ack=2897 Win=34816 Len
27	4.281984	192.168.1.144	128.119.245.12	TCP	2962	46170 → 80 [PSH, ACK] Seq=17377 Ack=1 Win=642

3. Файл alice.txt завантажився на сервер завдяки протоколу транспортного рівня — TCP



## Протокол HTTPS

Відкрийте деяку Web-сторінку за протоколом HTTPS. Запишіть пакети цього з'єднання. По записаним пакетам ідентифікуйте версію протокол, що використовується, послідовність встановлення захищеного з'єднання та типи повідомлень, що передаються в процесі встановлення цього з'єднання.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.107.128	52.84.109.13	TCP	54	50258 → 443 [ACK] Seq=1 Ack=1 Win=63360 Len=0
2	0.276231472	192.168.107.128	192.168.107.2	DNS	75	Standard query 0x633d A www.youtube.com
3	0.276315374	192.168.107.128	192.168.107.2	DNS	75	Standard query response 0x1e33 AAAA www.youtube.com
4	0.281358321	192.168.107.2	192.168.107.128	DNS	240	Standard query response 0x633d A www.youtube.com CNAME youtube-ui
5	0.282524876	192.168.107.2	192.168.107.128	DNS	224	Standard query response 0x1e33 AAAA www.youtube.com CNAME youtube
6	0.282859861	192.168.107.128	172.217.16.110	TCP	74	43468 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSva
7	0.295544147	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.107.2? Tell 192.168.107.1
8	0.302468093	172.217.16.110	192.168.107.128	TCP	60	443 → 43468 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
9	0.302550419	192.168.107.128	172.217.16.110	TCP	54	43468 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	0.304627088	192.168.107.128	172.217.16.110	TLSv1.3	567	Client Hello
11	0.305821829	172.217.16.110	192.168.107.128	TCP	60	443 → 43468 [ACK] Seq=1 Ack=514 Win=64240 Len=0
12	0.343839395	172.217.16.110	192.168.107.128	TLSv1.3	1484	Server Hello, Change Cipher Spec
13	0.343866162	192.168.107.128	172.217.16.110	TCP	54	43468 → 443 [ACK] Seq=514 Ack=1431 Win=62920 Len=0
14	0.344204235	172.217.16.110	192.168.107.128	TCP	2914	443 → 43468 [PSH, ACK] Seq=1431 Ack=514 Win=64240 Len=2860 [TCP s
15	0.344211106	192.168.107.128	172.217.16.110	TCP	54	43468 → 443 [ACK] Seq=514 Ack=4291 Win=61320 Len=0
16	0.345033957	172.217.16.110	192.168.107.128	TCP	1484	443 → 43468 [PSH, ACK] Seq=4291 Ack=514 Win=64240 Len=1430 [TCP s
17	0.345040332	192.168.107.128	172.217.16.110	TCP	54	43468 → 443 [ACK] Seq=514 Ack=5721 Win=62780 Len=0
18	0.346428785	172.217.16.110	192.168.107.128	TLSv1.3	776	Application Data

Окрім протоколів TCP, DNS та ARP, бачимо також TLS версії 1.3, що виконує захищене рукоостискання, на відміну від TCP з'єднання.

↓ Далі вказано типи повідомлень, що передаються, а саме клієнт посилає “Client Hello” → сервер відповідає “Server Hello”, “Change Cipher Spec”, “Application Data” → клієнт посилає “Change Cipher Spec”, “Application Data” → далі починається обмін “Application Data”

No.	Time	Source	Destination	Protocol	Length	Info
10	0.304627088	192.168.107.128	172.217.16.110	TLSv1.3	567	Client Hello
12	0.343839395	172.217.16.110	192.168.107.128	TLSv1.3	1484	Server Hello, Change Cipher Spec
18	0.346428785	172.217.16.110	192.168.107.128	TLSv1.3	776	Application Data
31	0.433200122	192.168.107.128	172.217.16.110	TLSv1.3	118	Change Cipher Spec, Application Data
32	0.433489068	192.168.107.128	172.217.16.110	TLSv1.3	224	Application Data
33	0.433537248	192.168.107.128	172.217.16.110	TLSv1.3	346	Application Data
37	0.451644216	172.217.16.110	192.168.107.128	TLSv1.3	662	Application Data, Application Data
39	0.452020312	192.168.107.128	172.217.16.110	TLSv1.3	85	Application Data
41	0.469753639	172.217.16.110	192.168.107.128	TLSv1.3	85	Application Data

## Служба DNS

Для тестування роботи служби DNS використовується утиліта nslookup.

Сформуйте запит стосовно деякої символічної адреси до вашого звичайного сервера DNS або до деякого публічного DNS-сервера (наприклад, DNS сервера Google з IP адресою 8.8.8.8) та запишіть пакети запитів до DNS та відповідей на них.

```
(snz24@cybernaz)-[~]
$ nslookup foxtrot.com.ua 8.8.8.8
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   foxtrot.com.ua
Address: 107.154.79.37
Name:   foxtrot.com.ua
Address: 45.60.100.37
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.107.128	8.8.8.8	DNS	74	Standard query 0x1925 A foxtrot.com.ua
2	0.019666570	8.8.8.8	192.168.107.128	DNS	106	Standard query response 0x1925 A foxtrot.com.ua A 107.154.79.37 A 45.60.100...
3	0.020162740	192.168.107.128	8.8.8.8	DNS	74	Standard query 0xae2c AAAA foxtrot.com.ua
4	0.039252949	8.8.8.8	192.168.107.128	DNS	132	Standard query response 0xae2c AAAA foxtrot.com.ua SOA ns5.n3.net.ua

На прикладі перехоплених пакетів дайте відповідь на наступні питання:

## HTTP:

1. Перехопіть з'єднання з Web-сервером і відновіть повідомлення, що містять запит і відповідь, а також інші об'єкти, що передаються в рамках даного з'єднання.
2. Знайдіть повідомлення HTTP GET. Скільки часу займає процес з моменту відправлення повідомлення HTTP GET до моменту отримання відповіді HTTP OK. Скільки запитів HTTP GET було відправлено браузером для отримання однієї Web - сторінки. На які Інтернет адреси були відправлені ці GET запити?

No.	Time	Source	Destination	Protocol	Length	Info
8	0.075468207	192.168.107.128	77.47.133.109	HTTP	546	GET / HTTP/1.1
18	1.612481964	77.47.133.109	192.168.107.128	HTTP	979	HTTP/1.1 200 OK (text/html)
33	2.067835155	192.168.107.128	77.47.133.109	HTTP	602	GET /wp-content/plugins/polylang/flags/uk.png HTTP/1.1
41	2.073149900	192.168.107.128	77.47.133.109	HTTP	605	GET /wp-content/plugins/polylang/flags/en_US.png HTTP/1.1
43	2.073503456	77.47.133.109	192.168.107.128	HTTP	768	HTTP/1.1 200 OK (PNG)
47	2.074656696	192.168.107.128	77.47.133.109	HTTP	614	GET /wp-content/themes/ipt_theme/images/opacity.png HTTP/1.1
49	2.075222714	192.168.107.128	77.47.133.109	HTTP	598	GET /wp-content/uploads/2020/01/logo2.png HTTP/1.1
53	2.076084290	192.168.107.128	77.47.133.109	HTTP	607	GET /wp-content/uploads/2020/11/Bufer-obmena-1.png HTTP/1.1
111	2.105398283	77.47.133.109	192.168.107.128	HTTP	1362	HTTP/1.1 200 OK (JPEG JFIF image)

З моменту відправлення HTTP GET до моменту HTTP OK пройшло 1.537013757. На даному скріншоті показано, що моїм браузером було відправлено 10 HTTP GET запитів на адресу 77.47.133.109

3. Як протокол HTTP завантажує малюнки. Продемонструйте пакети HTTP POST.

No.	Time	Source	Destination	Protocol	Length	Info
8	0.075468207	192.168.107.128	77.47.133.109	HTTP	546	GET / HTTP/1.1
18	1.612481964	77.47.133.109	192.168.107.128	HTTP	979	HTTP/1.1 200 OK (text/html)
33	2.067835155	192.168.107.128	77.47.133.109	HTTP	602	GET /wp-content/plugins/polylang/flags/uk.png HTTP/1.1
41	2.073149900	192.168.107.128	77.47.133.109	HTTP	605	GET /wp-content/plugins/polylang/flags/en_US.png HTTP/1.1
43	2.073503456	77.47.133.109	192.168.107.128	HTTP	768	HTTP/1.1 200 OK (PNG)
47	2.074656696	192.168.107.128	77.47.133.109	HTTP	614	GET /wp-content/themes/ipt_theme/images/opacity.png HTTP/1.1
49	2.075222714	192.168.107.128	77.47.133.109	HTTP	598	GET /wp-content/uploads/2020/01/logo2.png HTTP/1.1
53	2.076084290	192.168.107.128	77.47.133.109	HTTP	607	GET /wp-content/uploads/2020/11/Bufer-obmena-1.png HTTP/1.1
158	0.363180937	192.168.107.128	128.119.245.12	HTTP	2626	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1
159	0.363560072	128.119.245.12	192.168.107.128	TCP	60	80 → 39814 [ACK] Seq=1 Ack=151841 Win=10220 Len=0
160	0.363560072	128.119.245.12	192.168.107.128	TCP	60	80 → 39814 [ACK] Seq=1 Ack=152953 Win=9108 Len=0
161	0.363560072	128.119.245.12	192.168.107.128	TCP	60	80 → 39814 [ACK] Seq=1 Ack=152953 Win=9108 Len=0
162	0.608796134	128.119.245.12	192.168.107.128	HTTP	831	HTTP/1.1 200 OK (text/html)

Протокол HTTP завантажує малюнки, посилаючи відповідний запит HTTP GET на адресу сервера і потім отримує у відповідь HTTP OK

HTTP POST при завантаженні текстового документа на сервер

4. Як протокол HTTP захищає при автентифікації значення login і password, що передаються.

Найбільш серйозним недоліком базової автентифікації є те, що протокол HTTP не захищає значення login і password, тому це призводить до фактично відкритої передачі тексту пароля користувача фізичної мережі. Наприклад:

**`http://test_server.kiev.ua/program.php?user=guest&pass=rock`**

5. Ваш браузер використовує версію HTTP 1.0, 1.1 чи 2.0? Яку версію використовує сервер?

Мій браузер та сервер використовують версію HTTP 1.1

8	0.075468207	192.168.107.128	77.47.133.109	HTTP	546	GET / HTTP/1.1
18	1.612481964	77.47.133.109	192.168.107.128	HTTP	979	HTTP/1.1 200 OK (text/html)

6. В якому мовному кодуванні (якщо таке є) ваш браузер має можливість приймати інформацію від сервера?

```
▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    Host: ipt.kpi.ua\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
```

У мовному кодуванні en-US, en; q=0.5 мій браузер має можливість приймати інформацію від сервера

7. Яку відповідь дає сервер (код статусу та кодова фраза) на початкове повідомлення HTTP GET вашого браузера?

HTTP/1.1 200 OK - відповідь на перший HTTP GET

8. Який код статусу та кодова фраза міститься у HTTP відповіді? Які ще значення можуть зустрітися? Чи є якісь рядки статусу в HTTP, що пов'язані з розбивкою повідомлення на декілька TCP сегментів.

```
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 200 OK\r\n
    ▶ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
```

Код статусу: 200

Кодова фраза: OK

Можуть зустрітися такі HTTP відповіді:

Інформаційні	Успішні операції	Перенаправлення	Помилки клієнта	Помилки сервера
100: Continue	200: OK	303: See Other	400: Bad Request	501: Not Implemented
101: Switching Protocol	202: Created	304: Not Modified	403: Forbidden	502: Bad Gateway
102: Processing	204: No Contest	305: Use Proxy	409: Conflict	503: Service Unavailable

9. Скільки знадобилося TCP сегментів, щоб передати звичайну HTTP відповідь?

```
▼ [5 Reassembled TCP Segments (12605 bytes): #10(1460), #12(5840), #14(1460), #16(2920), #18(925)]
  [Frame: 10, payload: 0-1459 (1460 bytes)]
  [Frame: 12, payload: 1460-7299 (5840 bytes)]
  [Frame: 14, payload: 7300-8759 (1460 bytes)]
  [Frame: 16, payload: 8760-11679 (2920 bytes)]
  [Frame: 18, payload: 11680-12604 (925 bytes)]
  [Segment count: 5]
  [Reassembled TCP length: 12605]
  [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a4461746553a205361742c203139204a756e2032...
```

Знадобилося 5 TCP-сегментів, щоб передати звичайну HTTP відповідь

10. Який був останній час модифікації HTML файлу, що ви отримали?

Last-Modified: Tue, 24 May 2016 16:43:04 GMT\r\n

11. Скільки байтів інформації було передано браузеру?

Content-Length: 11851\r\n

- передано разом із першою HTTP відповіддю

12. Чи були малюнки завантажені вашим браузером послідовно, чи вони завантажувалися з двох web сайтів паралельно? Поясніть.

No.	Time	Source	Destination	Protocol	Length Info
8	0.075468207	192.168.107.128	77.47.133.109	HTTP	546 GET / HTTP/1.1
18	1.612481964	77.47.133.109	192.168.107.128	HTTP	979 HTTP/1.1 200 OK (text/html)
33	2.067835155	192.168.107.128	77.47.133.109	HTTP	602 GET /wp-content/plugins/polylang/flags/uk.png HTTP/1.1
41	2.073149900	192.168.107.128	77.47.133.109	HTTP	605 GET /wp-content/plugins/polylang/flags/en-US.png HTTP/1.1
43					768 HTTP/1.1 200 OK (PNG)
47					614 GET /wp-content/themes/ipt_theme/images/opacity-logo1.png HTTP/1.1
49					598 GET /wp-content/uploads/2020/01/logo2.png HTTP/1.1
53					607 GET /wp-content/uploads/2020/11/Bufer-obmena-1.jpg HTTP/1.1
57					958 HTTP/1.1 200 OK (PNG)
59					605 GET /wp-content/uploads/2018/07/Rukopozhatye.jpg HTTP/1.1
61	2.079861221	192.168.107.128	77.47.133.109	HTTP	607 GET /wp-content/uploads/2021/06/Logo-Samsung11.png HTTP/1.1

Малюнки були завантажені моїм браузером паралельно, адже два різних HTTP GET пакети отримали дві різні HTTP OK відповіді

13. Коли ваш браузер відправив HTTP GET повідомлення вдруге, яке нове поле було додано?

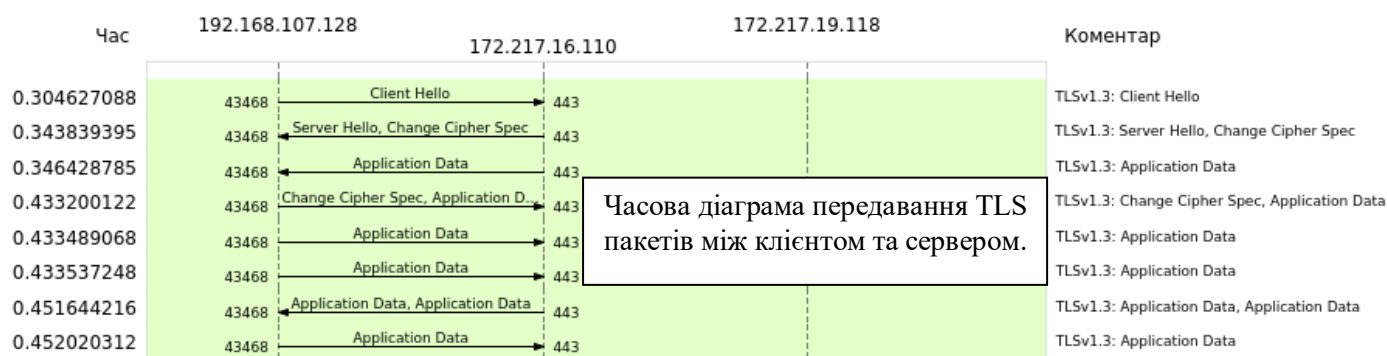
Referer: http://ipt.kpi.ua/\r\n

## SSL/TLS:

- Для кожного з перших восьми Ethernet фреймів визначте джерело повідомлення (сервер чи клієнт), визначте номер TLS запису, що вставлений у фрейм, і складіть список типів TLS повідомлень. Складіть часову діаграму передавання TLS пакетів між клієнтом та сервером.

Перші вісім Ethernet фреймів, що містять TLS повідомлення.				
No.	Time	Source	Destination	Details
10	0.304627088	192.168.107.128	172.217.16.110	TLSv1.3 567 Client Hello
12	0.343839395	172.217.16.110	192.168.107.128	TLSv1.3 1484 Server Hello, Change Cipher Spec
18	0.346428785	172.217.16.110	192.168.107.128	TLSv1.3 776 Application Data
31	0.433200122	192.168.107.128	172.217.16.110	TLSv1.3 118 Change Cipher Spec, Application Data
32	0.433489068	192.168.107.128	172.217.16.110	TLSv1.3 224 Application Data
33	0.433537248	192.168.107.128	172.217.16.110	TLSv1.3 346 Application Data
37	0.451644216	172.217.16.110	192.168.107.128	TLSv1.3 662 Application Data, Application Data
39	0.452020312	192.168.107.128	172.217.16.110	TLSv1.3 85 Application Data
41	0.469753639	172.217.16.110	192.168.107.128	TLSv1.3 85 Application Data

Номер фрейму	Сервер/клієнт	Номер TLS запису	TLS повідомлення
10	Клієнт	1	Client Hello
12	Сервер	2	Server Hello, Change Cipher Spec
18	Сервер	1	Application Data
31	Клієнт	2	Change Cipher Spec, Application Data
32	Клієнт	1	Application Data
33	Клієнт	1	Application Data
37	Сервер	2	Application Data, Application Data
39	Клієнт	1	Application Data



- Кожен TLS запис починається з однакових трьох полів (можливо, з різними значеннями). Одне з цих полів - це "content type", яке має розмір в один байт. Випишіть всі три поля та їхній розмір.

```

TLSv1.3 Record Layer: Handshake Protocol: Client Hello
  Content Type: Handshake (22) 1 байт
  Version: TLS 1.0 (0x0301) 2 байти
  Length: 508 2 байти
  
```



3. Як шифруються дані прикладного рівня? Чи записи, які містять дані прикладного рівня, містять ще й значення хешу MAC (Message Authentication Code)? Чи Wireshark розмежовує дані прикладного рівня та хеш MAC?

Перед тим, як розпочати захищений обмін інформацією, клієнт та сервер мають узгодити алгоритм шифрування та відповідний ключ. Це відбувається під час процедури “рукоштовування” – відкриття сеансу зв’язку. Наступні алгоритми можуть бути використані для цього завдання: Криптографічна система RSA, Протокол Діффі-Геллмана, короточасні (ефемерні) ключі Діффі-Геллмана, Протокол Діффі-Геллмана на еліптичних кривих, короточасні ключі за протоколом Діффі-Геллмана на еліптичних кривих, анонімний протокол Діффі-Геллмана, попередньо узгоджений ключ та Secure Remote Password

TLS забезпечує відправку кожного повідомлення з кодом MAC (Message Authentication Code), алгоритм створення якого - одностороння криптографічна функція хешування (фактично - контрольна сума), ключі якої відомі обох учасникам зв’язку. Wireshark не відрізняє зашифровані дані прикладного рівня та хеш MAC

4. а) Які типи TLS повідомлень зустрічаються в перехопленні?

Handshake Type: Client Hello (1)
Handshake Type: Server Hello (2)
Opaque Type: Application Data (23)
Content Type: Change Cipher Spec (20)

б) Який ідентифікатор даної TLS сесії?

[Community ID: 1:qiaEIHdliFVqQdF8uYeGWiSPnxA=]

в) Які набори алгоритмів захисту підтримують клієнт і сервер?

Криптографічна система RSA, Протокол Діффі-Геллмана, короточасні (ефемерні) ключі Діффі-Геллмана, Протокол Діффі-Геллмана на еліптичних кривих, короточасні ключі за протоколом Діффі-Геллмана на еліптичних кривих, анонімний протокол Діффі-Геллмана, попередньо узгоджений ключ та Secure Remote Password

г) Де передається цифровий сертифікат?

Сервер стверджує версію використовуваного протоколу, вибирає спосіб шифрування з наданого списку, і відправляє відповідь клієнту, прикріпивши свій цифровий сертифікат разом із відповіддю “Server Hello”.

## DNS:

1. Ознайомтесь з форматом DNS запиту і відповіді.

Формат DNS запиту дуже простий, містить ім'я, тип і клас запису.

Ім'я
Тип запису
Клас запису



Формат *DNS відповіді* складніший, перші три поля точно такі ж ім'я, тип запису і клас запису. Потім вказується час життя, це час на який запис можна зберегти в кеші DNS resolver, потім вказується довжина даних і власне дані відповіді.

Ім'я
Тип запису
Клас запису
Час життя (TTL)
Довжина даних
Дані

- Відшукайте пакети запитів до DNS. Вони переслані за допомогою UDP чи TCP?
- Який номер порту призначення у відправленому пакеті DNS запиту? Який номер порту призначення у пакеті DNS відповіді?

No.	Time	Source	Destination	Protocol	No.	Time	Source	Destination	Protocol
1	0.000000000	192.168.107.128	8.8.8.8	DNS	1	0.000000000	192.168.107.128	8.8.8.8	DNS
2	0.019666570	8.8.8.8	192.168.107.128	DNS	2	0.019666570	8.8.8.8	192.168.107.128	DNS
3	0.020162740	192.168.107.128	8.8.8.8	DNS	3	0.020162740	192.168.107.128	8.8.8.8	DNS
4	0.039252949	8.8.8.8	192.168.107.128	DNS	4	0.039252949	8.8.8.8	192.168.107.128	DNS

<b>User Datagram Protocol</b> , Src Port: 37037, Dst Port: 53 Source Port: 37037 Destination Port: 53 Length: 40 Checksum: 0x3c72 [unverified] [Checksum Status: Unverified] [Stream index: 0] [Timestamps] UDP payload (32 bytes) Domain Name System (query) Transaction ID: 0x1925 Flags: 0x0100 Standard query Questions: 1 Answer RRs: 0	<b>User Datagram Protocol</b> , Src Port: 53, Dst Port: 37037 Source Port: 53 Destination Port: 37037 Length: 40 Checksum: 0x3c72 [unverified] [Checksum Status: Unverified] [Stream index: 0] [Timestamps] UDP payload (32 bytes) Domain Name System (response) Transaction ID: 0x1925 Flags: 0x8180 Standard query response, No error Questions: 1 Answer RRs: 2
---	---

- На яку IP адресу був відправлений DNS запит? Послугуючись утилітою *nslookup*, визначіть IP адреси вашого локального DNS серверу.

DNS запит був відправлений на публічний DNS-сервер Google з IP адресою 8.8.8.8

```
C:\Users\user>nslookup
Default Server:  router.asus.com
Address:  192.168.1.1
```

- Дослідіть пакети DNS запитів. Що означає поле "Type" в ньому? Чи повідомлення містить якесь поле "Answers"?

TYPE (Тип) — визначає формат і призначення цього ресурсного запису

```
Queries
  foxtro.com.ua: type A, class IN
    Name: foxtro.com.ua
    [Name Length: 14]
    [Label Count: 3]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
```

Запис A (address record) — запис адреси — пов'язує ім'я хосту з адресою протоколу IPv4

6. Дослідіть повідомлення DNS відповіді. Скільки “відповідей” було отримано?

7. Що кожна з цих відповідей містить?

1	0.000000000	192.168.107.128	8.8.8.8	DNS	74 Standard query 0x1925 A foxtrot.com.ua
2	0.019666570	8.8.8.8	192.168.107.128	DNS	106 Standard query response 0x1925 A foxtrot.com.ua A 107
3	0.020162740	192.168.107.128	8.8.8.8	DNS	74 Standard query 0xae2c AAAA foxtrot.com.ua
4	0.039252949	8.8.8.8	192.168.107.128	DNS	132 Standard query response 0xae2c AAAA foxtrot.com.ua SC

Answers

foxtrot.com.ua: type A, class IN, addr 107.154.79.37

Name: foxtrot.com.ua  
Type: A (Host Address) (1)  
Class: IN (0x0001)  
Time to live: 674 (11 minutes, 14 seconds)  
Data length: 4  
Address: 107.154.79.37

foxtrot.com.ua: type A, class IN, addr 45.60.100.37

Name: foxtrot.com.ua  
Type: A (Host Address) (1)  
Class: IN (0x0001)  
Time to live: 674 (11 minutes, 14 seconds)  
Data length: 4  
Address: 45.60.100.37

6. Було отримано дві “відповіді” на DNS-запит.

7. Вони містять ім'я хоста, тип і клас запису, час життя (TTL), довжину даних, дані (IP-адреса)

8. Якщо на Web сторінці містяться малюнки, то чи надсилає ваш хост нові DNS запити перед завантаженням кожного з цих малюнків?

Ні, не надсилає.

9. На прикладах перехоплених пакетів опишіть роботу системи DNS. Який з протоколів (TCP або UDP) використовує DNS. Які номери портів мають повідомлення DNS.

Протокол DNS (порт 53) може використовувати для роботи TCP або UDP, проте традиційно запити та відповіді відправляються у вигляді однієї UDP дейтаграми, а TCP використовується для AXFR-запитів.

DNS-запит

User Datagram Protocol,  
Source Port: 37037  
Destination Port: 53

DNS-відповідь

User Datagram Protocol, Sr  
Source Port: 53  
Destination Port: 37037