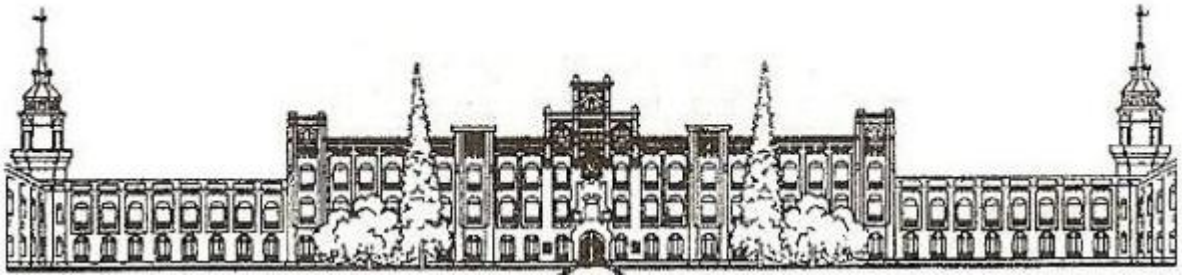


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»

КАФЕДРА ММСА

Лабораторна робота № 3

З дисципліни: Комп'ютерні мережі

Протоколи DNS

Виконала:

Студентка III курсу

Групи КА-72

Дунебабіна О.А

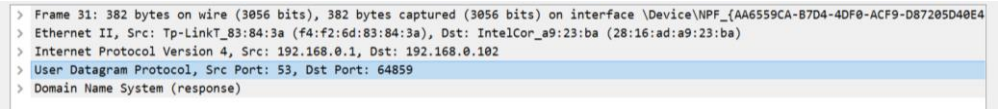
Перевірив: Кухарєв С. О.

Київ 2020

Мета роботи: аналіз деталей роботи протоколу DNS.

Контрольні запитання:

1. Знайдіть запит та відповідь DNS, який протокол вони використовують, UDP або TCP? Який номер цільового порта запиту DNS? Який номер вихідного порта відповіді DNS?



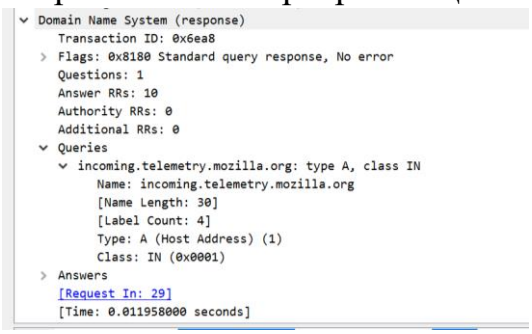
Цільовий порт: 53

Вихідний порт: 64859

2. На який адрес IP був відправлений запит DNS? Чи є цей адрес адресом локального сервера DNS?
   IP: 192.168.0.102. Так є.
3. Проаналізуйте повідомлення із запитом DNS. Якого «Типу» цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

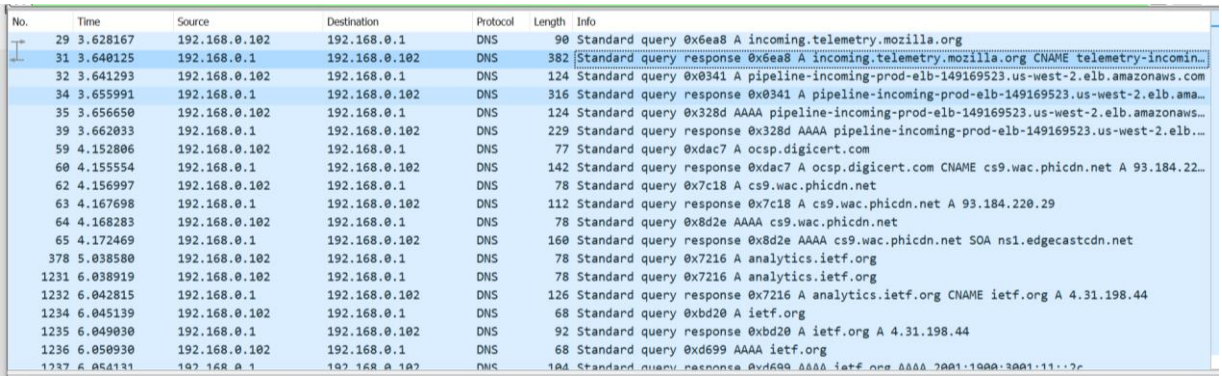
Цей запит – є запитом стандартного типу. Вміщує.

4. Дослідіть повідомлення із відповіддю DNS. Яка кількість відповідей запропонована сервером? Що вміщує кожна з цих відповідей?



5. Проаналізуйте повідомлення TCP SYN, яке відправила ваша робоча станція після отримання відповіді сервера DNS. Чи співпадає цільова IP адреса цього повідомлення з одною із відповідей сервера DNS?

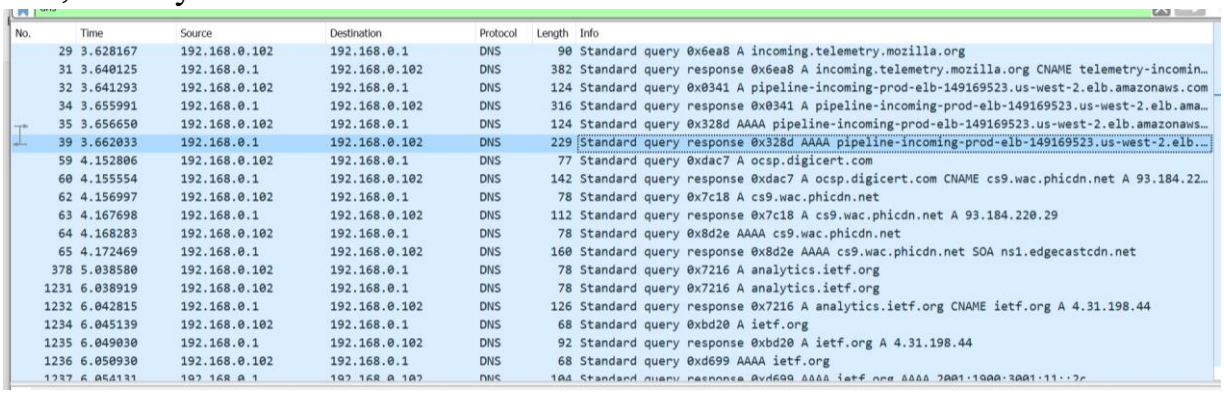
Так, збігається.



No.	Time	Source	Destination	Protocol	Length	Info
29	3.628167	192.168.0.102	192.168.0.1	DNS	90	Standard query 0x6ea8 A incoming.telemetry.mozilla.org
31	3.640125	192.168.0.1	192.168.0.102	DNS	382	Standard query response 0x6ea8 A incoming.telemetry.mozilla.org CNAME telemetry-incomin…
32	3.641293	192.168.0.102	192.168.0.1	DNS	124	Standard query 0x0341 A pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com
34	3.655991	192.168.0.1	192.168.0.102	DNS	316	Standard query response 0x0341 A pipeline-incoming-prod-elb-149169523.us-west-2.elb.ama…
35	3.656650	192.168.0.102	192.168.0.1	DNS	124	Standard query 0x328d AAAA pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws…
39	3.662033	192.168.0.1	192.168.0.102	DNS	229	Standard query response 0x328d AAAA pipeline-incoming-prod-elb-149169523.us-west-2.elb.…
59	4.152806	192.168.0.102	192.168.0.1	DNS	77	Standard query 0xdac7 A ocsp.digicert.com
60	4.155554	192.168.0.1	192.168.0.102	DNS	142	Standard query response 0xdac7 A ocsp.digicert.com CNAME cs9.wac.phicdn.net A 93.184.22…
62	4.156997	192.168.0.102	192.168.0.1	DNS	78	Standard query 0x7c18 A cs9.wac.phicdn.net
63	4.167698	192.168.0.1	192.168.0.102	DNS	112	Standard query response 0x7c18 A cs9.wac.phicdn.net A 93.184.220.29
64	4.168283	192.168.0.102	192.168.0.1	DNS	78	Standard query 0x8d2e AAAA cs9.wac.phicdn.net
65	4.172469	192.168.0.1	192.168.0.102	DNS	160	Standard query response 0x8d2e AAAA cs9.wac.phicdn.net SOA ns1.edgecastcdn.net
378	5.038580	192.168.0.102	192.168.0.1	DNS	78	Standard query 0x7216 A analytics.ietf.org
1231	6.038919	192.168.0.102	192.168.0.1	DNS	78	Standard query 0x7216 A analytics.ietf.org
1232	6.042815	192.168.0.1	192.168.0.102	DNS	126	Standard query response 0x7216 A analytics.ietf.org CNAME ietf.org A 4.31.198.44
1234	6.045139	192.168.0.102	192.168.0.1	DNS	68	Standard query 0xbd20 A ietf.org
1235	6.049030	192.168.0.1	192.168.0.102	DNS	92	Standard query response 0xbd20 A ietf.org A 4.31.198.44
1236	6.050930	192.168.0.102	192.168.0.1	DNS	68	Standard query 0xd699 AAAA ietf.org
1237	6.054131	192.168.0.1	192.168.0.102	DNS	104	Standard query response 0xd699 AAAA ietf.org AAAA 2001:1900:3001:11::2c

6. Чи виконує ваша робоча станція нові запити DNS для отримання ресурсів, які використовує документ, що отримав браузер?

Так, виконує.



No.	Time	Source	Destination	Protocol	Length	Info
29	3.628167	192.168.0.102	192.168.0.1	DNS	90	Standard query 0x6ea8 A incoming.telemetry.mozilla.org
31	3.640125	192.168.0.1	192.168.0.102	DNS	382	Standard query response 0x6ea8 A incoming.telemetry.mozilla.org CNAME telemetry-incomin…
32	3.641293	192.168.0.102	192.168.0.1	DNS	124	Standard query 0x0341 A pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com
34	3.655991	192.168.0.1	192.168.0.102	DNS	316	Standard query response 0x0341 A pipeline-incoming-prod-elb-149169523.us-west-2.elb.ama…
35	3.656650	192.168.0.102	192.168.0.1	DNS	124	Standard query 0x328d AAAA pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws…
39	3.662033	192.168.0.1	192.168.0.102	DNS	229	Standard query response 0x328d AAAA pipeline-incoming-prod-elb-149169523.us-west-2.elb.…
59	4.152806	192.168.0.102	192.168.0.1	DNS	77	Standard query 0xdac7 A ocsp.digicert.com
60	4.155554	192.168.0.1	192.168.0.102	DNS	142	Standard query response 0xdac7 A ocsp.digicert.com CNAME cs9.wac.phicdn.net A 93.184.22…
62	4.156997	192.168.0.102	192.168.0.1	DNS	78	Standard query 0x7c18 A cs9.wac.phicdn.net
63	4.167698	192.168.0.1	192.168.0.102	DNS	112	Standard query response 0x7c18 A cs9.wac.phicdn.net A 93.184.220.29
64	4.168283	192.168.0.102	192.168.0.1	DNS	78	Standard query 0x8d2e AAAA cs9.wac.phicdn.net
65	4.172469	192.168.0.1	192.168.0.102	DNS	160	Standard query response 0x8d2e AAAA cs9.wac.phicdn.net SOA ns1.edgecastcdn.net
378	5.038580	192.168.0.102	192.168.0.1	DNS	78	Standard query 0x7216 A analytics.ietf.org
1231	6.038919	192.168.0.102	192.168.0.1	DNS	78	Standard query 0x7216 A analytics.ietf.org
1232	6.042815	192.168.0.1	192.168.0.102	DNS	126	Standard query response 0x7216 A analytics.ietf.org CNAME ietf.org A 4.31.198.44
1234	6.045139	192.168.0.102	192.168.0.1	DNS	68	Standard query 0xbd20 A ietf.org
1235	6.049030	192.168.0.1	192.168.0.102	DNS	92	Standard query response 0xbd20 A ietf.org A 4.31.198.44
1236	6.050930	192.168.0.102	192.168.0.1	DNS	68	Standard query 0xd699 AAAA ietf.org
1237	6.054131	192.168.0.1	192.168.0.102	DNS	104	Standard query response 0xd699 AAAA ietf.org AAAA 2001:1900:3001:11::2c

7. Яким був цільовий порт повідомлення із запитом DNS? Яким був вихідний порт повідомлення із відповіддю DNS?

   Цільовий: 192.168.0.1

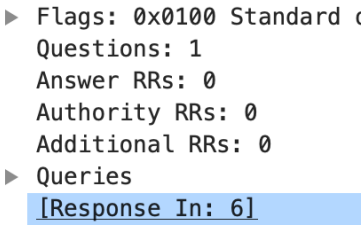
   Вихідний: 192.168.0.102

8. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?

   192.168.0.1. Так, є адресою локального сервера.

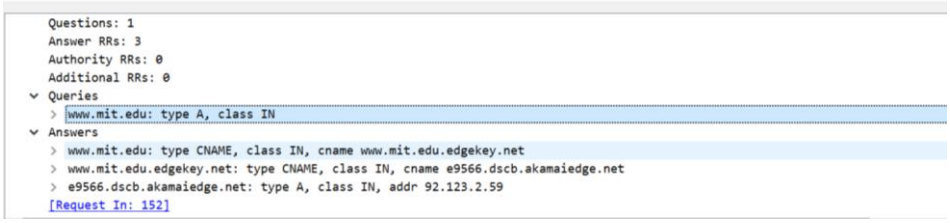
9. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

Цей запит – є запитом стандартного типу. Вміщує.



```
▶ Flags: 0x0100 Standard q
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
▶ Queries
  [Response In: 6]
```

10. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна із цих відповідей?



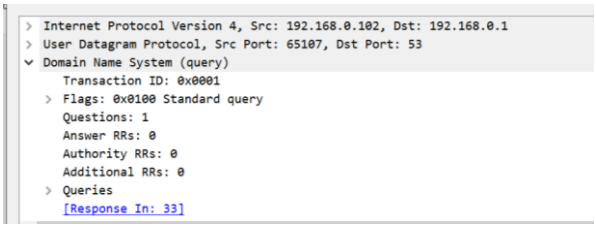
```
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 0
▼ Queries
  > www.mit.edu: type A, class IN
▼ Answers
  > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
  > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
  > e9566.dscb.akamaiedge.net: type A, class IN, addr 92.123.2.59
  [Request In: 152]
```

11. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?

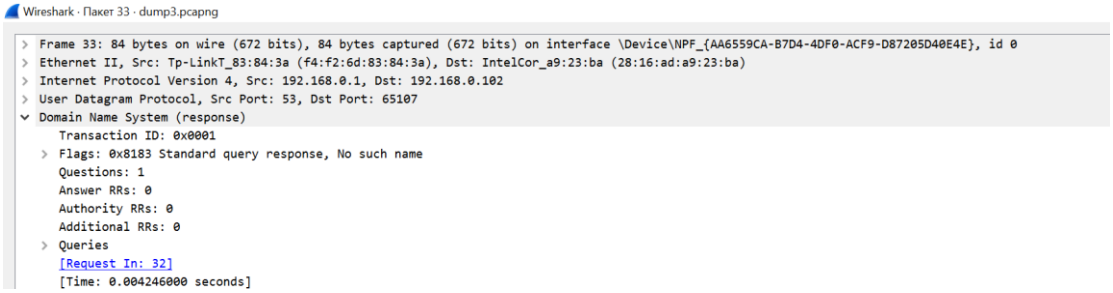
IP: 192.168.0.1. Так є.

12. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

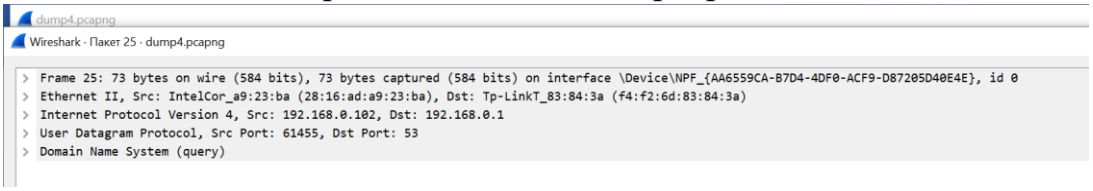
Стандартний тип запиту. Так вміщує.



13. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? Які сервери DNS були запропоновані у відповіді? Сервери були запропоновані за допомогою доменного імені, адреси IP або й того й іншого?

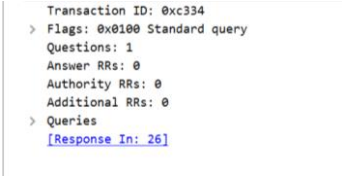


14. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням? Якщо ні, то якому доменному імені відповідає ця IP-адреса?
IP: 192.168.0.1. є адресою локального сервера.

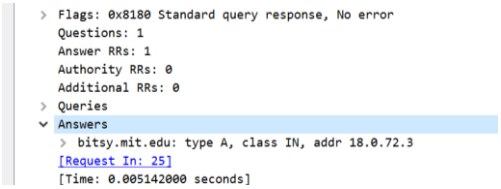


15. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

Стандартний тип запиту. вміщує.



16. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна з цих відповідей?



Висновок

В ході виконання даної лабораторної роботи, були покращено навички використання програми Wireshark для захоплення пакетів. Було проаналізовано протоколи DNS та було проведено аналіз деталей роботи даних протоколів.