### Міністерство освіти та науки України Національний університет «Львівська політехніка»



Звіт до лабораторної роботи №3

# ВИВЧЕННЯ ЗАХОПЛЕНИХ ПАКЕТІВ DNS I UDP ЗА ДОПОМОГОЮ ПРОГРАМИ WIRESHARK

"Інтерфейси та протоколи передачі даних" Варіант 11

Виконав: Студент IP-42 Лис Ярослав

Прийняла: Влах-Вигриновська Г. I. **Мета роботи**: Ознайомлення з роботою системи доменних імен (DNS) та проведення аналізу трафіку локальної мережі на прикладі протоколів DNS і UDP.

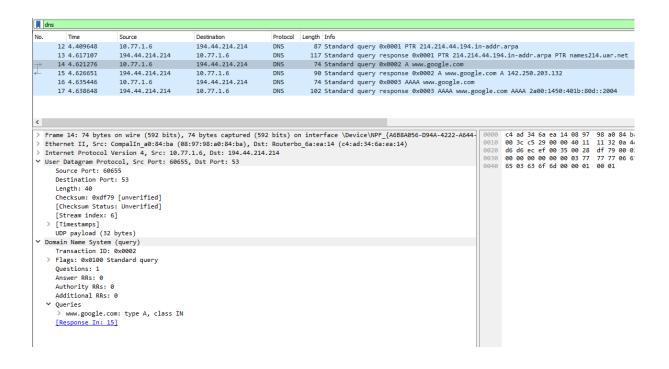
#### Запис даних ІР-конфігурації ПК

ІР-адреса	10.77.1.6
МАС-адреса	08-97-98-A0-84-BA
IP-адреса шлюзу замовчування	10.77.1.1
IP-адреса DNS-сервера	194.44.214.214

```
Ethernet adapter Ethernet:
  Connection-specific DNS Suffix .:
  Description . . . . . . . . . : Killer E2600 Gigabit Ethernet Controller
  Physical Address. . . . . . . : 08-97-98-A0-84-BA
  DHCP Enabled. . . . . . . . . : Yes
  Autoconfiguration Enabled . . . . : Yes
  Link-local IPv6 Address . . . . : fe80::60c:e324:6d10:8928%18(Preferred)
                                     10.77.1.6(Preferred)
  IPv4 Address. . . . . . . . . . . :
  Subnet Mask . . . . . . . . . . :
                                     255.255.255.0
  Lease Obtained. . . . . . . . : 11 жовтня 2023 р. 18:12:03
  Lease Expires . . . . . . . . : 11 жовтня 2023 р. 18:27:04
  Default Gateway . . . . . . . .
                                     10.77.1.1
  DHCP Server . . . . . . . . . . :
                                     10.77.1.1
  DHCPv6 IAID . . .
                                     134780824
  DHCPv6 Client DUID. . . . . . . : 00-01-00-01-26-E6-B8-D1-08-97-98-A0-84-BA
  DNS Servers . . . . . . . . . .
                                 .: 194.44.214.214
                                     194.44.214.40
  NetBIOS over Tcpip. . . . . . : Enabled
```

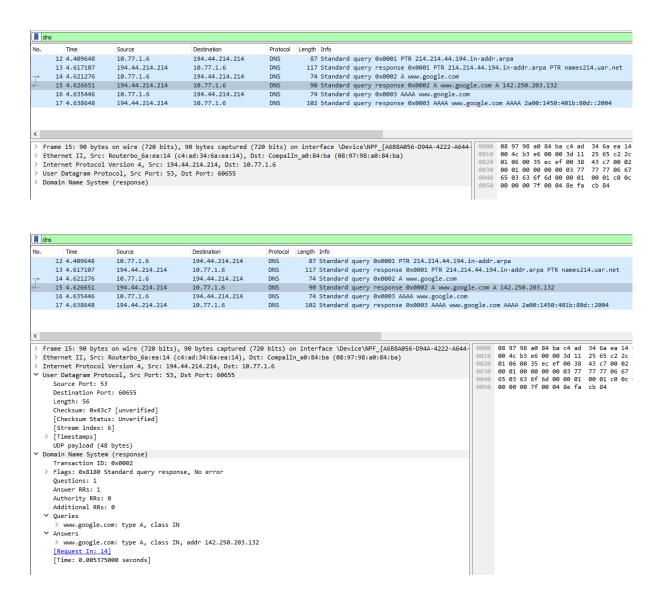
#### Захоплення запитів та відповідей DNS за допомогою програми Wireshark

```
dns
        Time
12 4.409648
                                                                 Destination
                                                                194.44.214.214
                                                                                                              87 Standard query 0x0001 PTR 214.214.44.194.in-addr.arpa
                                 10.77.1.6
                                                                                              DNS
                                                                                              DNS 87 Standard query 0x0001 PTR 214.214.44.194.in-addr.arpa
DNS 117 Standard query response 0x0001 PTR 214.214.44.194.in-addr.arpa PTR names214.uar.net
DNS 74 Standard query 0x0002 A www.google.com
                                                               10.77.1.6
194.44.214.214
         13 4.617107
                                  194.44.214.214
14 4.621276
                                10.77.1.6
                                                                                                        90 Standard query response 0x0002 A www.google.com A 142.250.203.132
74 Standard query 0x0003 AAAA www.google.com
102 Standard query response 0x0003 AAAA www.google.com AAAA 2a00:1450:401b:80d::2004
         15 4.626651
                                  194,44,214,214
                                                                 10.77.1.6
                                                                                               DNS
                                 10.77.1.6
         16 4.635446
                                                                194.44.214.214
         17 4.638648
                                                                10.77.1.6
                                                                                               DNS
                                                                                                                                                                                   0000 c4 ad 34 6a ea 14 08 97 98 a0 84 ba
0010 00 3c c5 29 00 00 40 11 11 32 0a 4d
0020 d6 d6 ec ef 00 35 00 28 df 79 00 02
0030 00 00 00 00 00 00 37 77 77 77 06 67
0040 65 03 63 6f 6d 00 00 01 00 01
 > Frame 14: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{AGB8A056-D94A-4222-A644}
    Ethernet II, Src: CompalIn a0:84:ba (08:97:98:a0:84:ba), Dst: Routerbo 6a:ea:14 (c4:ad:34:6a:ea:14)
   Internet Protocol Version 4, Src: 10.77.1.6, Dst: 194.44.214.214
User Datagram Protocol, Src Port: 60655, Dst Port: 53
 Domain Name System (query)
```



Розмір кадра	74 байти
МАС-адреса джерела	08-97-98-A0-84-BA
МАС-адреса призначення	C4:AD:34:6A:EA:14
IP-адреса джерела	10.77.1.6
IP-адреса призначення	10.77.1.1
Порт джерела	60655
Порт призначення	53

#### DNS пакет відповіді



МАС-адреса джерела: C4:AD:34:6A:EA:14 МАС-адреса призначення: 08-97-98-A0-84-BA

IP-адреса джерела: 10.77.1.1

IP-адреса призначення: 10.77.1.6

У DNS-пакеті відповіді ІР та МАС адреси помінялися місцями.

#### Розділ answers

```
> Frame 15: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{A6B8A056-D94A-4222-A644
> Ethernet II, Src: Routerbo_6a:ea:14 (c4:ad:34:6a:ea:14), Dst: CompalIn_a0:84:ba (08:97:98:a0:84:ba)
> Internet Protocol Version 4, Src: 194.44.214.214, Dst: 10.77.1.6
♥ User Datagram Protocol, Src Port: 53, Dst Port: 60655
     Source Port: 53
     Destination Port: 60655
     Length: 56
     Checksum: 0x43c7 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 6]
  > [Timestamps]
     UDP payload (48 bytes)

▼ Domain Name System (response)

     Transaction ID: 0x0002
   > Flags: 0x8180 Standard query response, No error
     Ouestions: 1
     Answer RRs: 1
     Authority RRs: 0
     Additional RRs: 0
   > Queries

✓ Answers

      www.google.com: type A, class IN, addr 142.250.203.132
           Name: www.google.com
           Type: A (Host Address) (1)
           Class: IN (0x0001)
          Time to live: 127 (2 minutes, 7 seconds)
          Data length: 4
          Address: 142.250.203.132
     [Request In: 14]
     [Time: 0.005375000 seconds]
```

## У чому переваги використання протоколу UDP замість протоколу TCP в якості транспортного протоколу для DNS?

Швидкість, відсутність потреби встановлення з'єднання, ідеально підходить для DNS оскільки запити та відповіді DNS мають надзвичайно малий обсяг і не вимагають використання службової інформації.

**Висновок**: на цій лабораторній роботі я ознайомився з роботою системи доменних імен (DNS) та провів аналізу трафіку локальної мережі на прикладі протоколів DNS і UDP.