

# Raport 8: Sieci komputerowe 2

## Wstęp

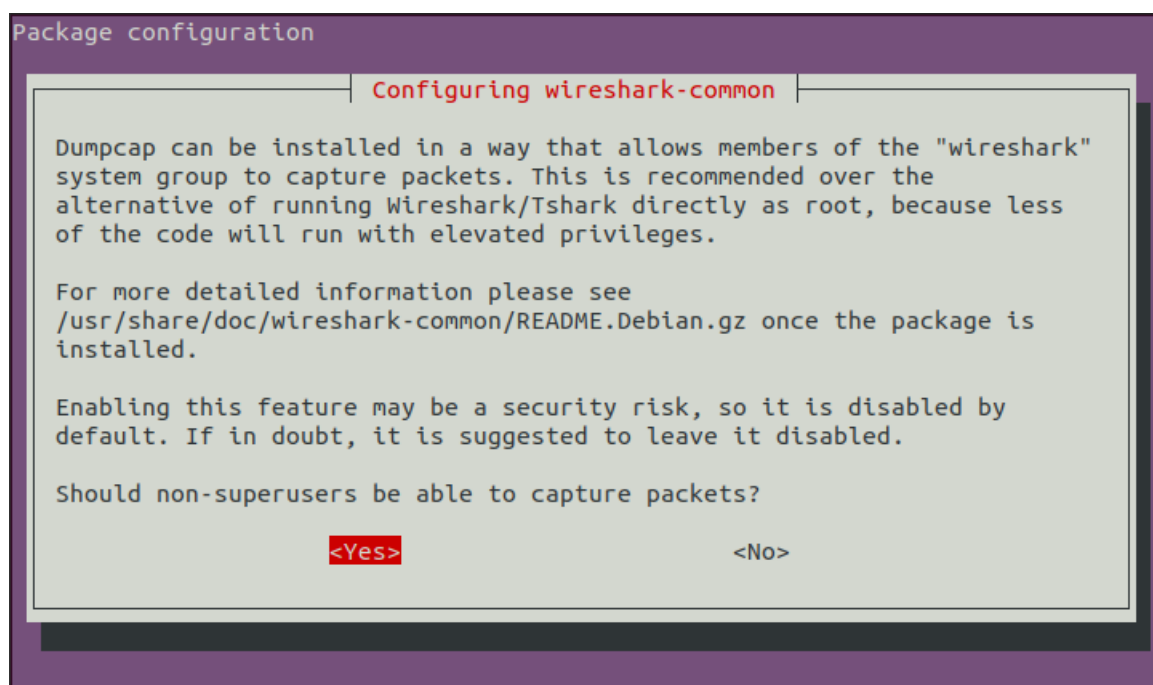
To laboratorium ma na celu zaznajomienie się z Wiresharkiem przy okazji weryfikując wiedzę z wykładu w temacie różnych protokołów sieciowych. W ramach trzech zadań zapoznamy się z podstawowym interfejsem Wiresharka.

### Konfiguracja Wiresharka

Na samym początku musisz wykonać dwie komendy, aby zezwolić swojemu użytkownikowi na nasłuchiwanie na ruch sieciowy:

```
$sudo dpkg-reconfigure wireshark-common
```

Pojawia się okno:



W oknie, które się wyświetli należy wybrać Yes.

Następnie należy wykonać:

```
$sudo usermod -a -G wireshark sansforensics
```

## 1 Obserwacja pakietów z wcześniejszego ćwiczenia

Uruchom Wireshark i rozpocznij nasłuchiwanie na interfejsie loopback.

### 1.1 TCP

Uruchom serwer i klienta TCP tak, jak w zadaniu 1b z poprzedniego ćwiczenia. Przejrzyj rezultaty działania w Wiresharku.

W raporcie odpowiedz na pytania:

1. Ile pakietów zawierających strumień TCP zostało wymienionych? **24**

2. Ile z nich pochodziło od klienta a ile od serwera?

**Serwer: 13**

**Klient: 11**

3. Z jakiego portu korzystał klient a z jakiego serwer?

**Serwer: 7777**

**Klient: 40942**

4. Jakie były czasy TTL pakietów IP klienta i serwera?

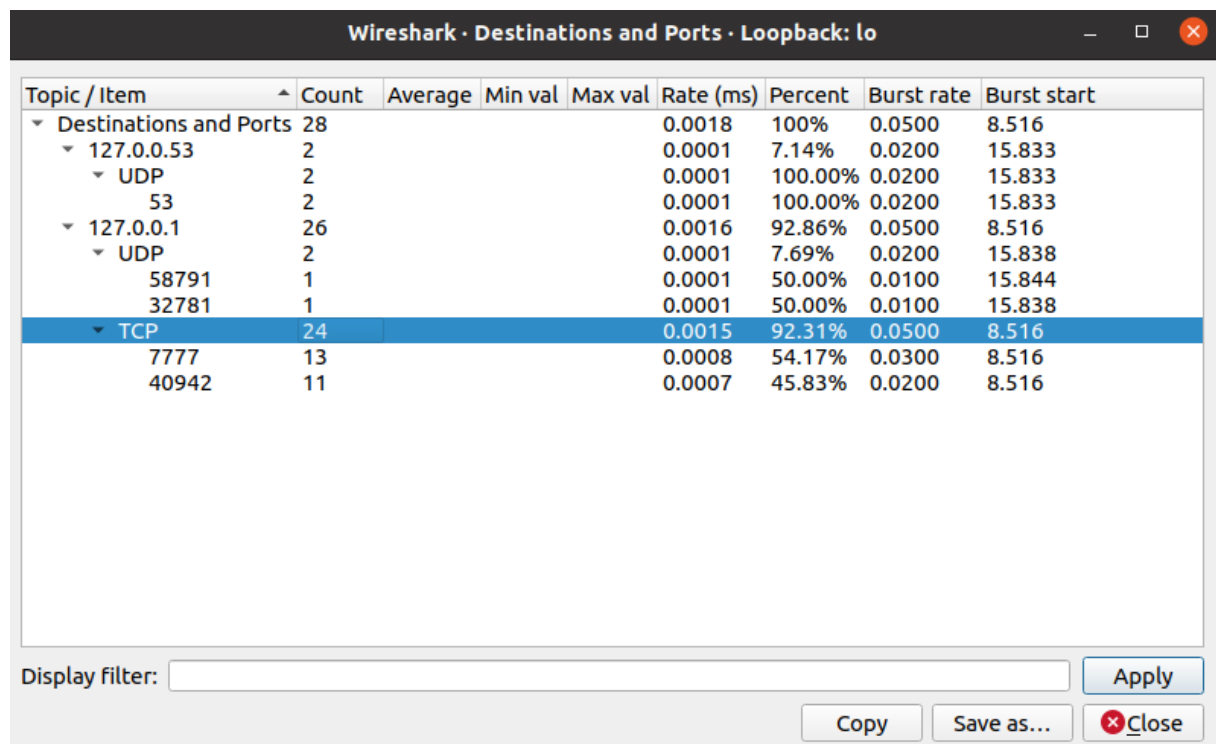
**Klient: 64**

**Serwer: 64**

5. Jakie flagi TCP miał ustawione pierwszy pakiet po ustanowieniu połączenia (po three-way handshake)? **PSH, ASK**

6. Jaki kod ma protokół TCP w pakiecie IP? **0x05**

Do raportu dołącz zrzut ekranu z okna wywołanego przez menu Statistics IPv4 Statistics Destination and Ports



Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
▼ Destinations and Ports	28				0.0018	100%	0.0500	8.516
▼ 127.0.0.53	2				0.0001	7.14%	0.0200	15.833
▼ UDP	2				0.0001	100.00%	0.0200	15.833
53	2				0.0001	100.00%	0.0200	15.833
▼ 127.0.0.1	26				0.0016	92.86%	0.0500	8.516
▼ UDP	2				0.0001	7.69%	0.0200	15.838
58791	1				0.0001	50.00%	0.0100	15.844
32781	1				0.0001	50.00%	0.0100	15.838
▼ TCP	24				0.0015	92.31%	0.0500	8.516
7777	13				0.0008	54.17%	0.0300	8.516
40942	11				0.0007	45.83%	0.0200	8.516

## 1.2 UDP

Uruchom serwer i klienta UDP tak, jak w zadaniu 2a z poprzedniego ćwiczenia. Przejrzyj rezultaty działania w Wiresharku

W raporcie odpowiedz na pytania:

1. Ile pakietów zawierających datagramy UDP zostało wymienionych? **12**

2. Ile z nich pochodziło od klienta a ile od serwera?

**Serwer: 0**

**Klient: 12**

3. Z jakiego portu korzystał klient a z jakiego serwer?

**Serwer: 7741**

**Klient: ??**

4. Jakie były czasy TTL pakietów IP klienta i serwera?

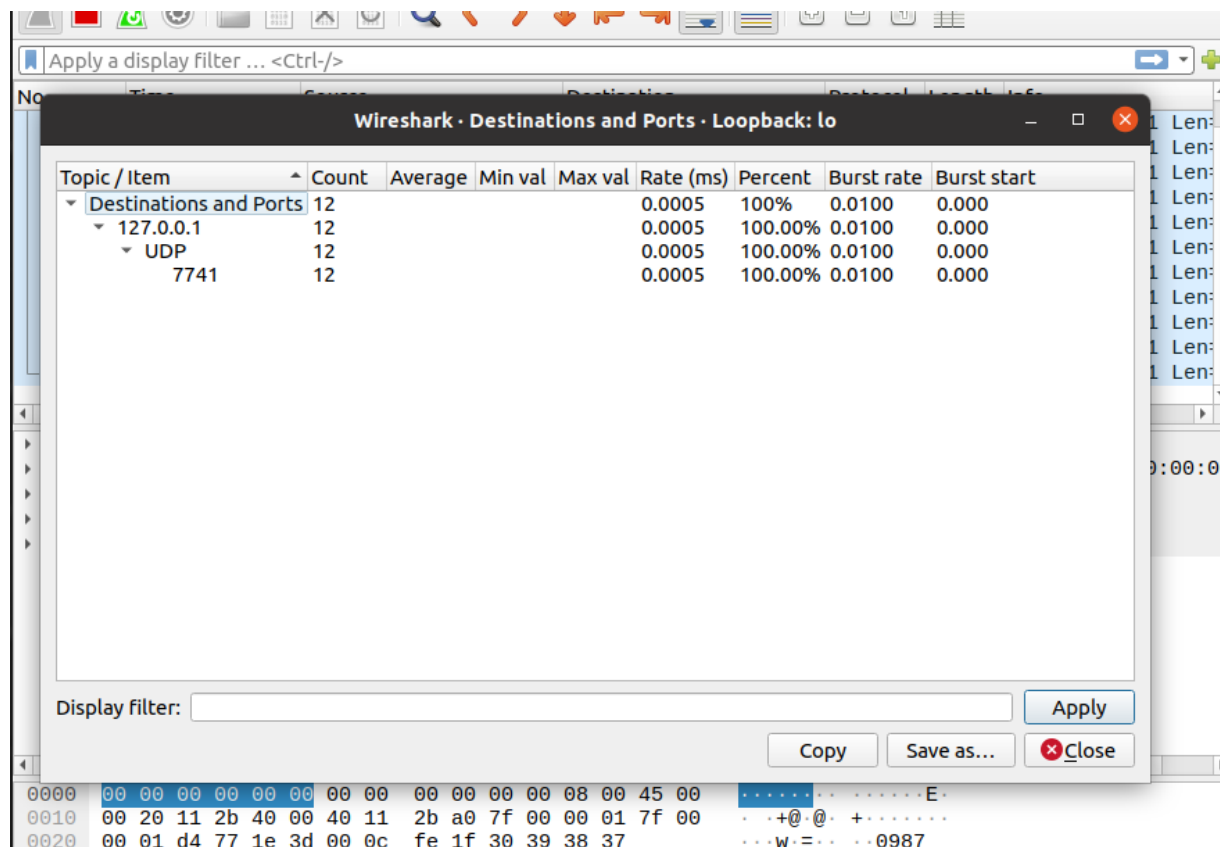
**Klient: 64**

**Serwer: brak**

5. Jaki kod ma protokół UDP w pakiecie IP?

**17 (0x11)**

Do raportu dołącz zrzut ekranu z okna wywołanego przez menu Statistics IPv4 Statistics Destination and Ports



## 2 Obserwujemy różne pakiety

Uruchom Wiresharka w maszynie wirtualnej, rozpocznij nasłuchiwanie na interfejsie publicznym maszyny wirtualnej i zostaw na pewien czas. Po pewnym czasie odnajdź przynajmniej po jednym pakiecie:

- protokołu DNS

- protokołu ICMP
- protokołu ARP
- broadcast warstwy 2
- multicast warstwy 3.

Każdy z tych pakietów dokładnie obejrzyj i wykonaj zrzuty ekranu ich struktur.

	Adres MAC źródłowy	Adres IP źródłowy	Adres MAC docelowy	Adres IP docelowy	Protokół
<b>protokół ARP</b>	52:54:00:12: 35:02	10.0.2.2	80:00:27:f3:d9 :f3	10.0.2.15	ARP
<b>broadcast warstwy 2</b>					
<b>protokół DNS</b>	52:54:00: :12:35:02	10.0.2.15	08:00:27: :f3:d9:f3	10.204.0. 1	IP/UDP/ DNS
<b>protokół ICMP</b>	08:00:27: :f3:d9:f3	10.0.2.15	52:54:00:12:3 5:02	192.168. 1.1	IP/ICMP
<b>multicast warstwy 3</b>					

- DNS

```

Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.204.0.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 81
    Identification: 0x02c1 (705)
  ▶ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0x2100 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.15
    Destination: 10.204.0.1
- User Datagram Protocol, Src Port: 48276, Dst Port: 53
  Source Port: 48276
  Destination Port: 53
  Length: 61
  Checksum: 0x172a [unverified]
  [Checksum Status: Unverified]
  [Stream index: 1]
  ▶ [Timestamps]
- Domain Name System (query)

```

- ICMP

```

▼ Ethernet II, Src: PcsCompu_f3:d9:f3 (08:00:27:f3:d9:f3), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
  ▼ Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
    Address: RealtekU_12:35:02 (52:54:00:12:35:02)
    .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  ▼ Source: PcsCompu_f3:d9:f3 (08:00:27:f3:d9:f3)
    Address: PcsCompu_f3:d9:f3 (08:00:27:f3:d9:f3)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.1.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xdaf2 (56050)
  ▶ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x91fe [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.15
    Destination: 192.168.1.1

```

```

Frame 7: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_f3:d9:f3 (08:00:27:f3:d9:f3)
  Destination: PcsCompu_f3:d9:f3 (08:00:27:f3:d9:f3)
    Address: PcsCompu_f3:d9:f3 (08:00:27:f3:d9:f3)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Source: RealtekU_12:35:02 (52:54:00:12:35:02)
    Address: RealtekU_12:35:02 (52:54:00:12:35:02)
      ....1. .... = LG bit: Locally administered address (this is NOT the factory default)
      ....0. .... = IG bit: Individual address (unicast)
Type: ARP (0x0806)
Padding: 0000000000000000000000000000000000000000000000000000000000000000
Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: RealtekU_12:35:02 (52:54:00:12:35:02)
  Sender IP address: 10.0.2.2
  Target MAC address: PcsCompu_f3:d9:f3 (08:00:27:f3:d9:f3)
  Target IP address: 10.0.2.15

```

```

▼ Frame 2871: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface eth0, id 0
  ► Interface id: 0 (eth0)
    Encapsulation type: Ethernet (1)
    Arrival Time: May 16, 2022 11:06:35.275549948 UTC
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1652699195.275549948 seconds
    [Time delta from previous captured frame: 0.000200414 seconds]
    [Time delta from previous displayed frame: 0.000200414 seconds]
    [Time since reference or first frame: 125675.813988808 seconds]
    Frame Number: 2871
    Frame Length: 85 bytes (680 bits)
    Capture Length: 85 bytes (680 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:tls]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
  ▼ Ethernet II, Src: PcsCompu_f3:d9:f3 (08:00:27:f3:d9:f3), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
    ► Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
    ► Source: PcsCompu_f3:d9:f3 (08:00:27:f3:d9:f3)
    Type: IPv4 (0x0800)
  ▼ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 35.82.222.81
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)

```

- multicast warstwy 3

### 3. Obserwujemy sieć lokalną

Uruchom Wireshark na swoim komputerze (nie w maszynie wirtualnej) i zostaw na pewien czas. Po tym czasie zatrzymaj nasłuchiwanie i wygeneruj statystyki (menu Statistics):

- Protocol Hierarchy

Protokół	Pakiety [%]	Pakiety	Bajty [%]
▼ Frame	100.0	140071	100.0
▼ Ethernet	100.0	140071	1.3
▼ Internet Protocol Version 6	0.0	52	0.0
▼ User Datagram Protocol	0.0	47	0.0
Multicast Domain Name System	0.0	4	0.0
Link-local Multicast Name Resolution	0.0	1	0.0
Data	0.0	42	0.0
Internet Control Message Protocol v6	0.0	5	0.0
▼ Internet Protocol Version 4	99.8	139833	1.9
▼ User Datagram Protocol	85.2	119406	0.7
Simple Service Discovery Protocol	0.1	96	0.0
▼ QUIC IETF	85.0	118993	87.0
Malformed Packet	0.0	4	0.0
Multicast Domain Name System	0.0	4	0.0

- Conversations - tab Ethernet (jeżeli chcesz, to zasłoń prawą połowę adresów MAC czarnym prostokątem w dowolnym programie graficznym)

Ethernet · 12		IPv4 · 127	IPv6 · 4	TCP · 157	UDP · 214		
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes
4c:d5:77:7c:f7:31	ac:1f:6b:24:b0:3c	137 465	143 M	23 541	4059 k	113 924	
4c:d5:77:7c:f7:31	33:33:00:00:00:0c	42	30 k	42	30 k	0	
4c:d5:77:7c:f7:31	01:00:5e:7f:ff:fa	136	49 k	136	49 k	0	
4c:d5:77:7c:f7:31	ff:ff:ff:ff:ff:ff	1	342	1	342	0	
4c:d5:77:7c:f7:31	33:33:00:00:00:16	5	450	5	450	0	
4c:d5:77:7c:f7:31	01:00:5e:00:00:16	5	270	5	270	0	
4c:d5:77:7c:f7:31	01:00:5e:00:00:fb	4	372	4	372	0	
4c:d5:77:7c:f7:31	33:33:00:00:00:fb	4	452	4	452	0	
4c:d5:77:7c:f7:31	33:33:00:01:00:03	1	88	1	88	0	
4c:d5:77:7c:f7:31	01:00:5e:00:00:fc	1	68	1	68	0	
e0:63:da:b6:f1:95	ff:ff:ff:ff:ff:ff	75	3150	75	3150	0	


- HTTP – Packet Counter

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
✓ Total HTTP Packets	100				0,0001	100%	0,0400	647,550
Other HTTP Packets	0				0,0000	0,00%	-	-
✓ HTTP Response Packets	4				0,0000	4,00%	0,0200	647,571
??? : broken	0				0,0000	0,00%	-	-
5xx: Server Error	0				0,0000	0,00%	-	-
4xx: Client Error	0				0,0000	0,00%	-	-
✓ 3xx: Redirection	2				0,0000	50,00%	0,0200	647,571
304 Not Modified	2				0,0000	100,00%	0,0200	647,571
✓ 2xx: Success	2				0,0000	50,00%	0,0100	577,425
200 OK	2				0,0000	100,00%	0,0100	577,425
1xx: Informational	0				0,0000	0,00%	-	-
✓ HTTP Request Packets	96				0,0001	96,00%	0,0200	647,550
SEARCH	92				0,0001	95,83%	0,0100	62,443
GET	4				0,0000	4,17%	0,0200	647,550

- IPv4 Statistics – IP Protocol Types

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
✓ IP Protocol Types	133273				0,0966	100%	10,1500	349,958
UDP	113506				0,0823	85,17%	10,1500	349,958
TCP	19722				0,0143	14,80%	6,2900	45,141
NONE	45				0,0000	0,03%	0,0400	558,011

- IPv6 Statistics – IP Protocol Types


Wireshark · IP Protocol Types · Wi-Fi

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
✓ IP Protocol Types	45				0,0000	100%	0,0900	558,011
UDP	40				0,0000	88,89%	0,0500	558,026
NONE	5				0,0000	11,11%	0,0400	558,011