

LABORATORIUM SIECI KOMPUTEROWYCH

**Data wykonania
ćwiczenia:**

20.04.2023

Rok studiów:

2

Semestr:

4

Grupa studencka:

2

Grupa laboratoryjna:

2B

Ćwiczenie nr.

8

Temat: Wykorzystanie programu Wireshark do badania ruchu sieciowego

Osoby wykonujące ćwiczenia:

1. Igor Gawłowicz

Katedra Informatyki i Automatyki

1. Użycie programu Wireshark do przechwycenia i analizy lokalnych danych ICMP

Po sprawdzeniu adresów komputera i laptopa w tej samej sieci oraz uruchomienia filtru w programie za pomocą polecenia ping wysyłamy sygnały do drugiego urządzenia.

```
C:\Users\igorg>ping 192.168.88.19

Pinging 192.168.88.19 with 32 bytes of data:
Reply from 192.168.88.19: bytes=32 time<1ms TTL=128
Reply from 192.168.88.19: bytes=32 time<1ms TTL=128
Reply from 192.168.88.19: bytes=32 time<1ms TTL=128
Reply from 192.168.88.19: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.88.19:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

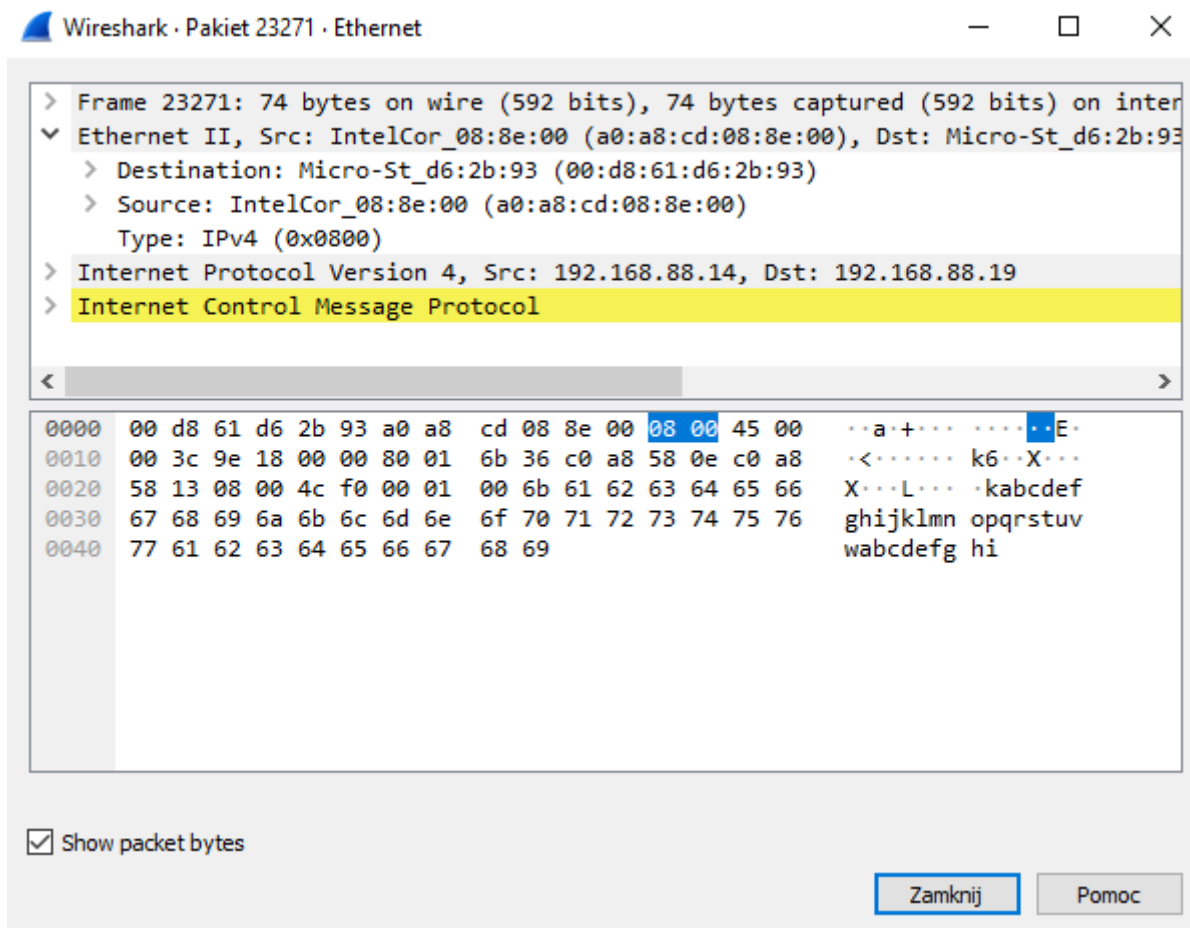
Odbieramy te sygnały w programie Wireshark

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes options like 'Plik', 'Edytuj', 'Widok', 'Idź', 'Przechwytyj', 'Analizuj', 'Statystyki', 'Telefonia', 'Bezprzewodowe', 'Narzędzia', and 'Pomoc'. The toolbar contains various icons for file operations, packet capture, and analysis. The main window shows a capture on the 'Ethernet' interface, filtered for 'icmp'. The packet list pane displays four ICMP Echo (ping) requests, all from source 192.168.88.14 to destination 192.168.88.19. The first packet (No. 23271) is selected and expanded in the packet details pane, showing the following structure:

- Frame 23271: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
- Ethernet II, Src: IntelCor_08:8e:00 (a0:a8:cd:08:8e:00), Dst: 192.168.88.19 (08:00:27:1c:1c:1c)
- Internet Protocol Version 4, Src: 192.168.88.14, Dst: 192.168.88.19
- Internet Control Message Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII format. The status bar at the bottom indicates 'Pakietów: 66962 · Wyświetlanych: 4 (0.0%)' and 'Profil: Default'.

Na podstawie tych sygnałów możemy zobaczyć dane na temat źródła oraz celu sygnału włącznie z adresami MAC obu urządzeń.



2. Użycie programu Wireshark do przechwycenia i analizy zdalnych danych ICMP

Następnym krokiem jest wysłanie sygnału ping do 3 domen internetowych i spisanie wyników.

- www.yahoo.com - 87.248.100.215
Address: Micro-St_d6:2b:93 (00:d8:61:d6:2b:93)
- www.cisco.com - 104.81.209.77 Address: Micro-St_d6:2b:93 (00:d8:61:d6:2b:93)
- www.google.com - 216.58.209.4 Address: Micro-St_d6:2b:93 (00:d8:61:d6:2b:93)

Możemy zaobserwować że adres MAC dla wszystkich trzech został zwrócony dokładnie taki sam znaczy to że nie uzyskujemy dokładnego adresu MAC więc jest to trochę zbytczne by sprawdzać go dla adresów zdalnych. Może to być powiązane z tym że w ramach zabezpieczenia adres MAC jest chroniony przez system i nie wysyłany do adresata taka długo jak nie jest się z nim w jednej sieci lokalnej.

3. Wnioski

Urządzenie WireShark jest bardzo przydatnym narzędziem przy śledzeniu aktywności dużych sieci lokalnych takich jak biura czy firmy. Pozwala nam on bardzo łatwo wychwycić wszelki ruch wypływający i przyływający do naszej sieci.