Politechnika Wrocławska

SPRAWOZDANIE Z ZAJĘĆ LABORATORYJNYCH
CYBERBEZPIECZEŃSTWO

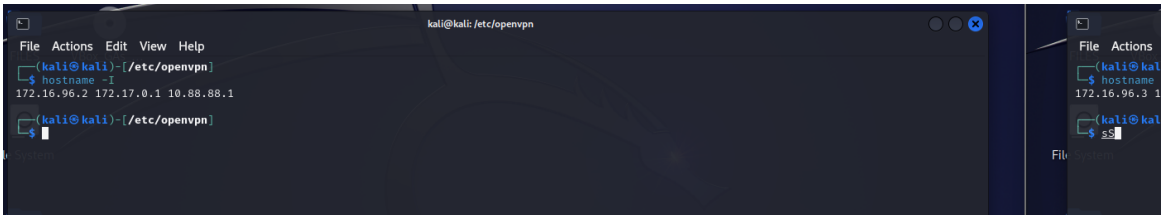
Lab 09
Ochrona komunikacji

Tomasz Mroczko, 266604

December 7, 2023

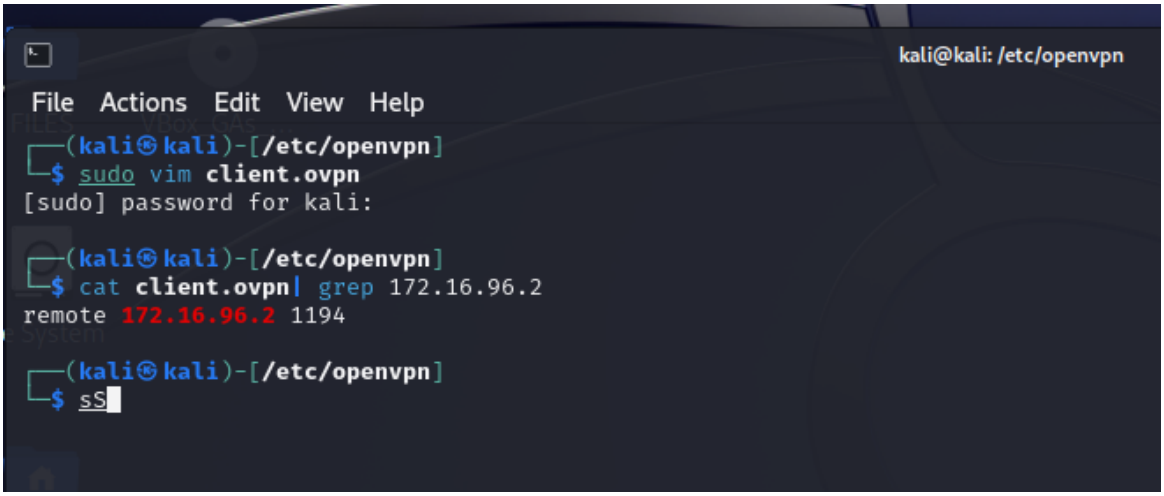
1 Konfiguracja środowiska

Adresy IP



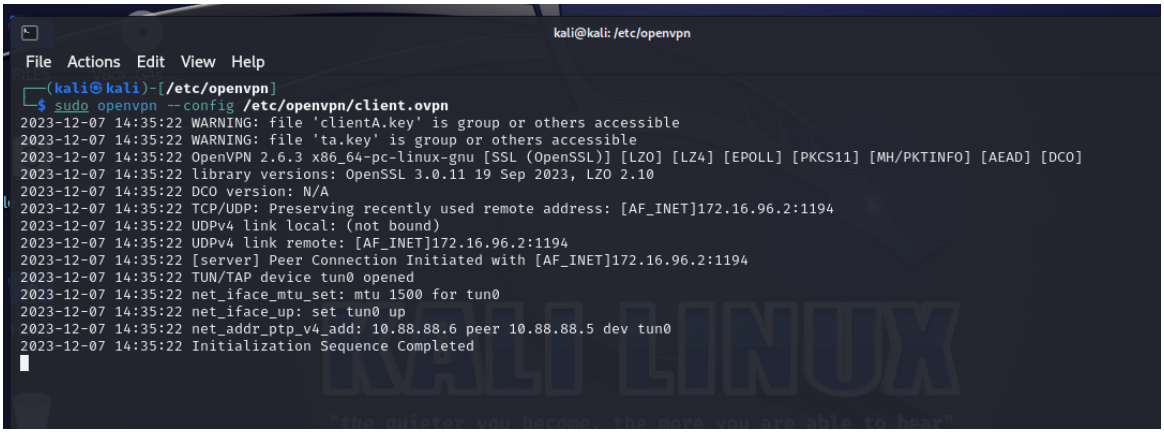
Maszyna używana jako server posiada IP 172.16.96.2.
Maszyna używana jako klient posiada IP 172.16.96.3.

Plik client.ovpn



Modyfikacja pliku "client.ovpn".

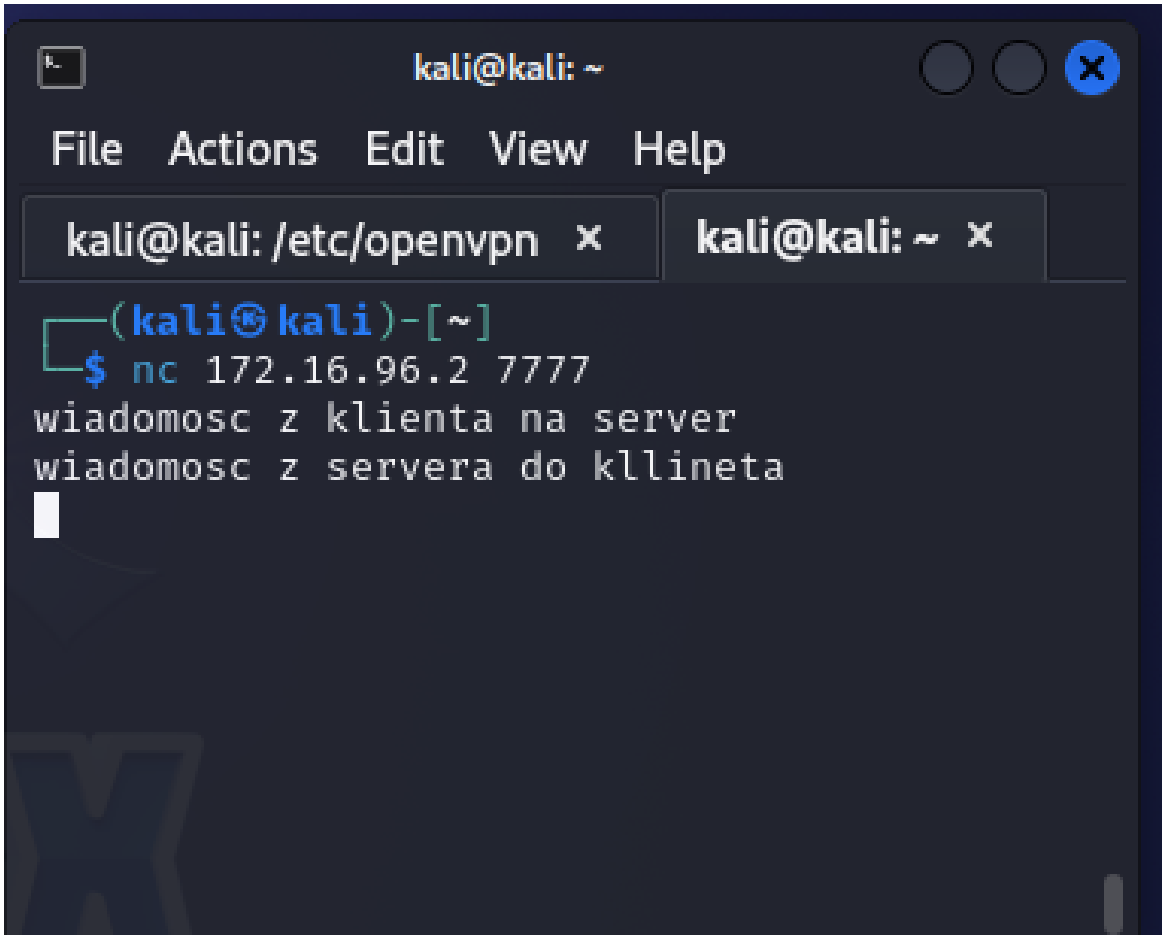
Nawiązanie połączenia z serverem VPN



2 Zadania

Zadanie 2.1

Wiadomości przesyłane przez netcat używając połączenia bez VPN (172.16.96.0/24)



Zadanie 2.2

Przchwycony ruch sieciowy podczas tej wymiany

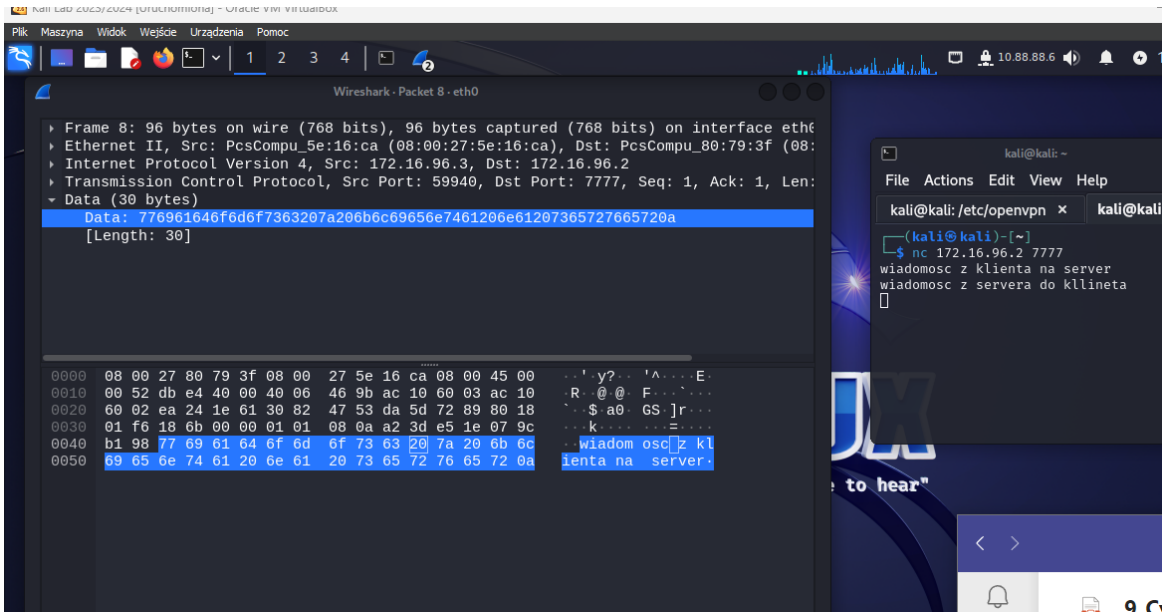


Figure 1: Przechwycona ramka z klienta na server.

Wiadomość przesłana z klienta na server została przechwycona. Widoczny jest adres IP źródła, adres IP celu oraz przede wszystkim treść wiadomości.

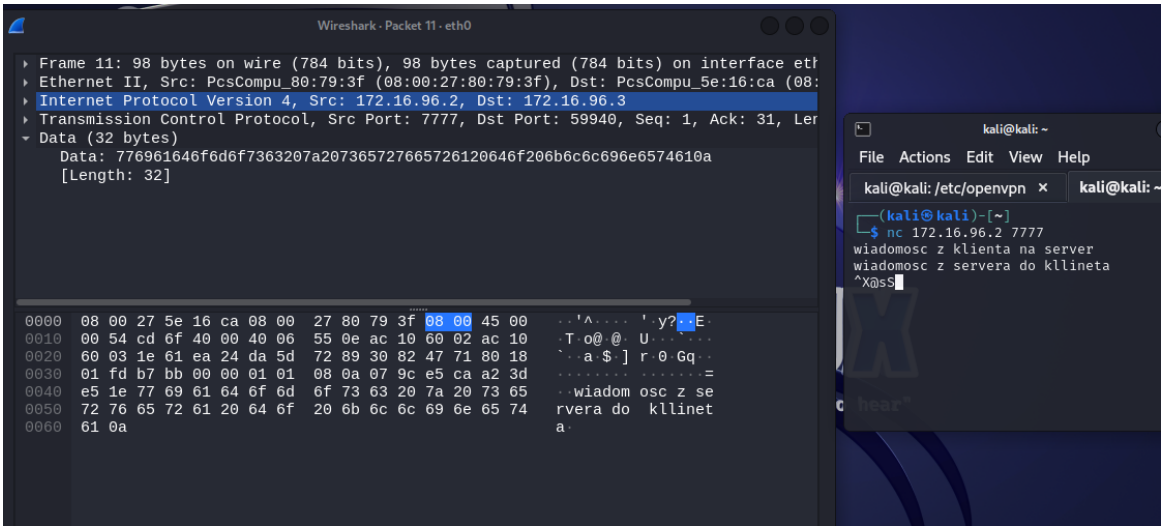
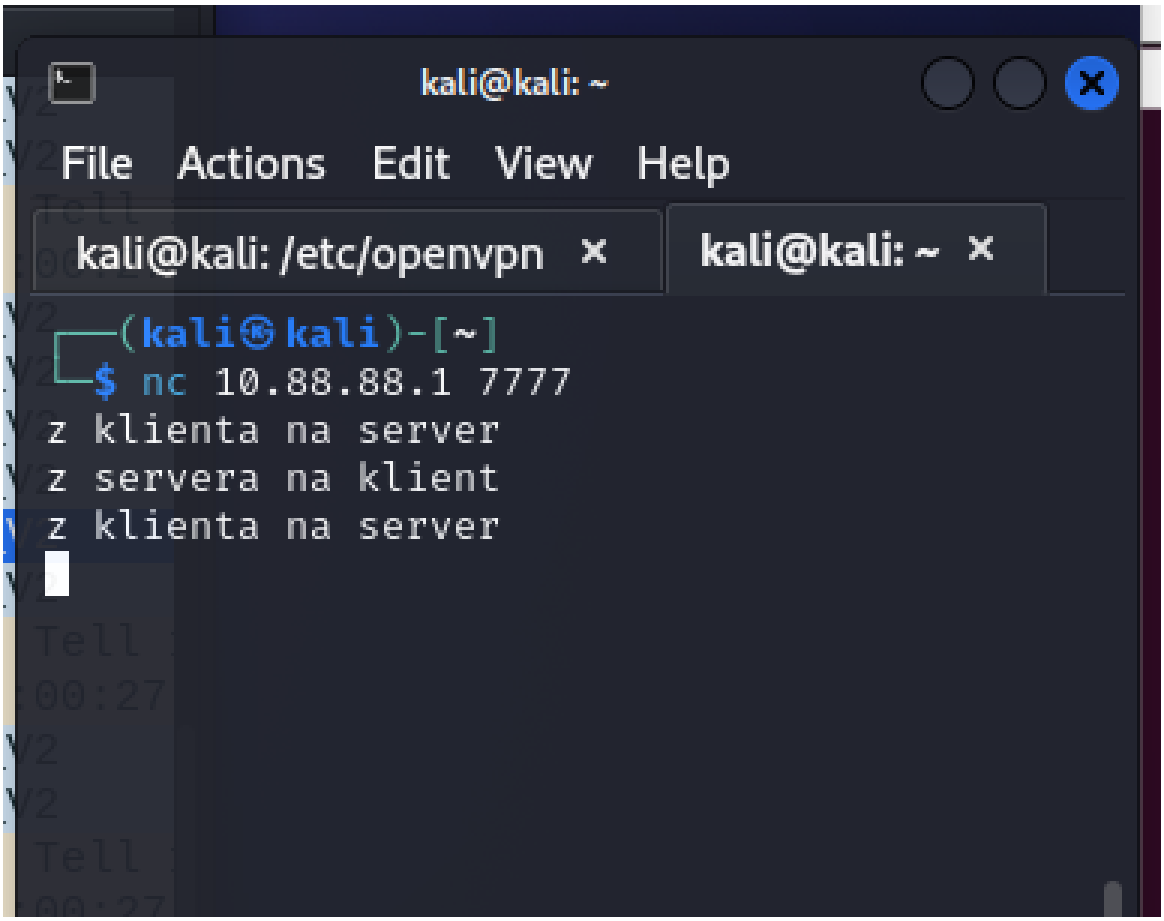


Figure 2: Przechwycona ramka z servera do klienta.

Wiadomość z servera do klienta również została przechwycona i ukazuje nam treść wiadomośći.

Zadanie 3.1

Wiadomości przesyłane przez netcat używając połączenia VPN (10.88.88.0/24)



Zadanie 3.2

Przchwycony ruch sieciowy podczas tej wymiany

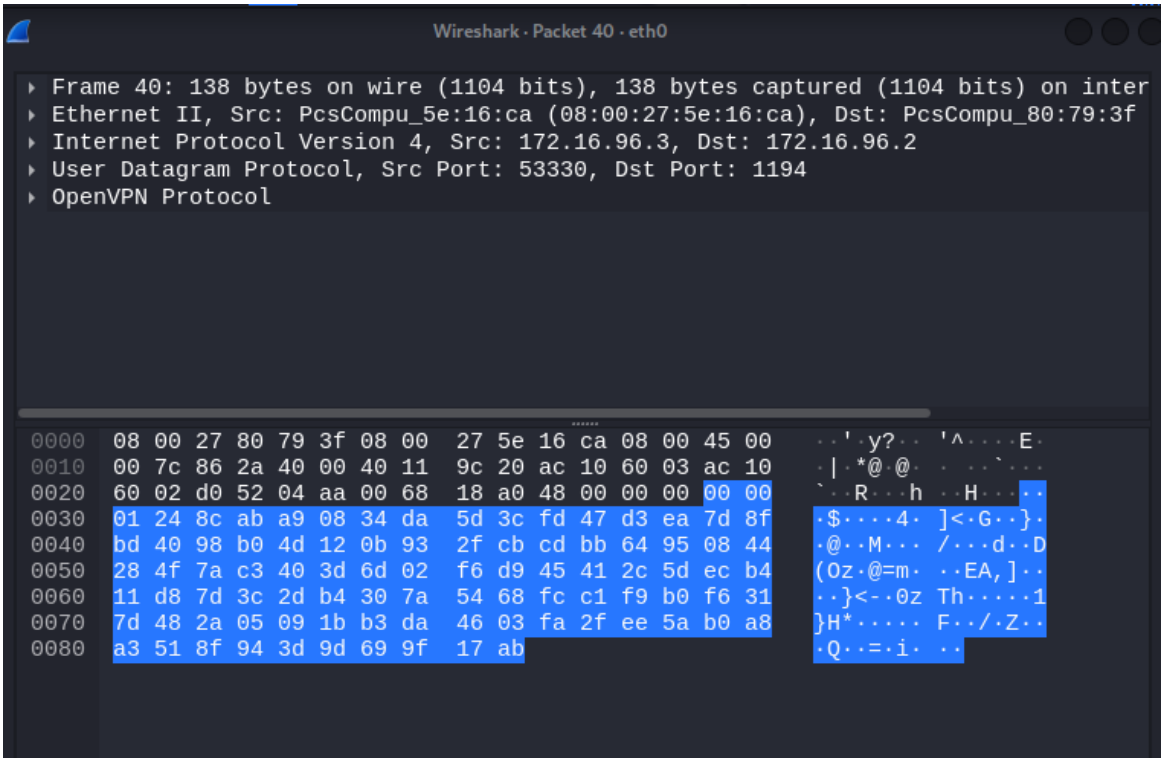


Figure 3: Ramka z klienta na server przy połączeniu VPN

Treść wiadomości nie jest czytelna z przechwyconej ramki.

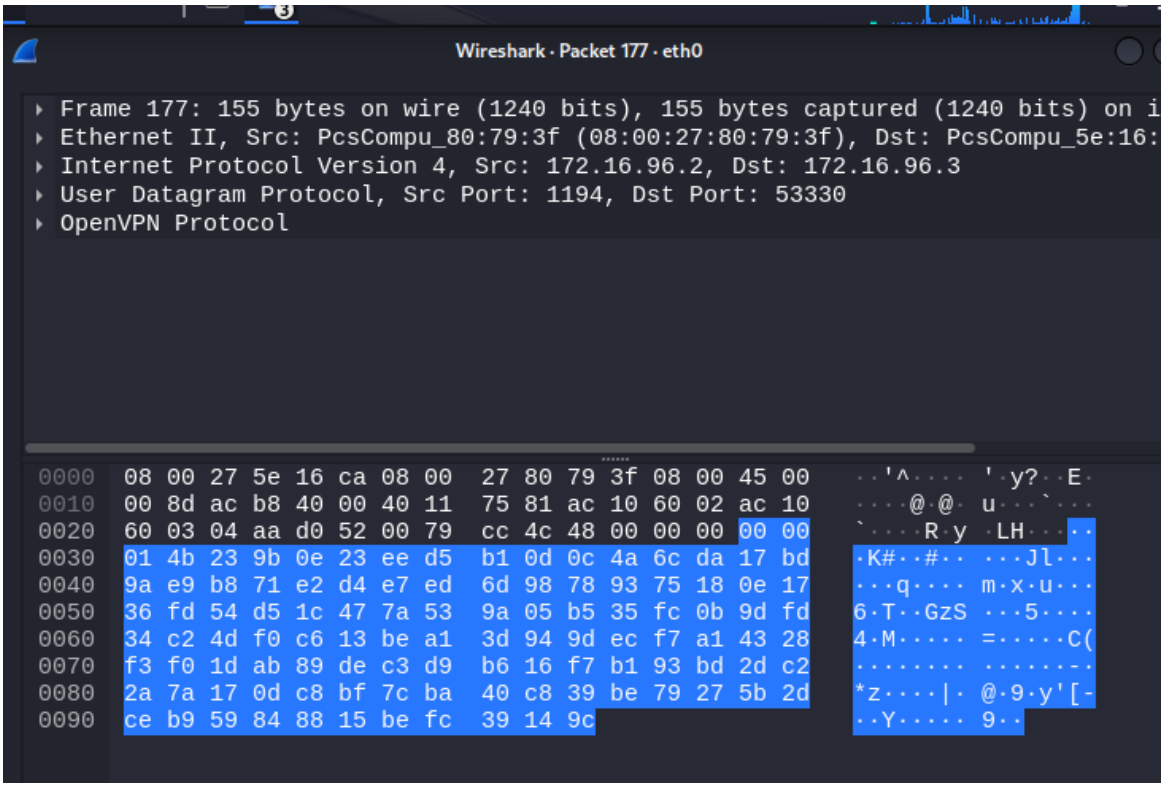


Figure 4: Ramka z servera do klienta przy połączeniu VPN

Ponownie treść wiadomości nie jest czytelna z przechwyconej ramki.

Pytanie 3.5

Czy można odczytać wiadomość wysłaną przez netcat?

- **Interfejs fizyczny**
  W przypadku użycia kanału komunikacji bez zabezpieczeń łatwe jest przechwycenie ramek, zawierających nadawcę, odbiorcę oraz treść wiadomości w niezaszyfrowanej postaci. Przechwycenie i odczytanie wiadomości nie było problematyczne. Przechwycone były ramki TCP, a ich zawartość łatwa do odczytania.
  W przypadku korzystania z VPN, przechwytone zostały tylko ramki OpenVPN. Treść wiadomości była zaszyfrowana.
- **Interfejs VPN (tun0)**
  Podczas połączenia za pomocą netcat, na adres VPN (10.88.88.0/24), przechwycone były ramki TCP, podobnie jak dla komunikacji bez szyfrowania VPN. Można było odczytać treść ramek oraz nadawców i odbiorców (10.88.88.0/24).

Pytanie 3.6

Jaka jest charakterystyka przechwyconego ruchu na interfejsie sieci VPN i interfejsie hosta?

- **Podczas połączenia VPN**
  W przypadku połączenia VPN, ruch na interfejsie VPN był minimalistyczny. Jedyne ramki

nadawane tym interfejsem to komunikaty TCP nadane przez netcat. Posiadały one prywatne adresy IP (z puli 10.88.88.0/24). Ich treść nie była szyfrowana wewnątrz kanału.

Ruch na interfejcie fizycznym (hosta) był dużo większy. Zamiast komunikatów TCP z treścią wiadomości netcat, nadawane były komunikaty OpenVPN, z zaszyfrowaną treścią wiadomości. Występował duży ruch protokołów takich jak ARP. Treść wiadomości nie była możliwa do odczytania.

- **Bez połączenia VPN**
  W przypadku braku połączenia VPN, ruch na interfejsie VPN(tun0), zgodnie z oczekiwaniami, nie występował wcale.
  Jeśli chodzi o ruch na interfejsie fizycznym, to możliwe było przechwycenie wszystkich wiadomości netcat,

Pytanie 3.7

Jakie istotne informacje można zobaczyć analizując ruch w obu przypadkach?

- **Podczas połączenia VPN**
  Podczas połączenia VPN, na interfejsie VPN, przechwycić można było zarówno adresy nadawcy oraz odbiorcy (wewnątrz sieci VPN), jak i treść wiadomości.
  Interfejs fizyczny jednak wysyłał zaszyforwane ramki OpenVPN, które nie pozwalały na przechwycenie treści komunikatów.
- **Bez połączenia VPN**
  Jeśli chodzi o interfejs VPN, to oczywiście nie przepływały przez niego informacje.
  Interfejs fizyczny dawał możliwość przechwycenia wielu przydatnych infromacji, takich jak adres nadawcy, odbiorcy oraz treść wiadomości.