Laboratorium 8

Wireshark cz. 5

W sprawozdaniu zamieść zrzuty ekranu z istotnych etapów oraz odpowiedzi na pytania.

Taki symbol oznacza, że trzeba w sprawozdaniu dodać zrzut ekranu (najczęściej 1) z wyniku działania polecenie.

Taki symbol oznacza, że należy dodać opis (najczęściej 1 zdanie) z wyniku działania polecenia.

Wstęp

Omówienie potencjału Wiresharka byłoby niepełne, gdyby zaprezentowana gama jego możliwości nie została poparta praktyką. Nadszedł więc czas, aby pokazać, dlaczego Wireshark jest tak popularnym i skutecznym narzędziem do analizy ruchu sieciowego. W dalszej części przedstawię sześć przykładowych scenariuszy wraz z najlepszymi praktykami, które od lat znajdują zastosowanie w codziennej pracy z Wiresharkiem.

Pierwsze dwa scenariusze będą dotyczyć wsparcia administracyjno-deweloperskiego. W kolejnych skupię się na aspektach cyberbezpieczeństwa, prezentując proaktywną analizę malware'u, stealera oraz anomalii w ruchu sieciowym charakterystycznych dla ataku typu Man-in-the-Middle.

Jakie wyzwania, poza cyberbezpieczeństwem, stoją przed administratorem na co dzień? Są to przede wszystkim problemy związane z połączeniami sieciowymi, takie jak retransmisje pakietów, analiza czasów odpowiedzi serwera, zrywanie połączeń, nadmierne opóźnienia w komunikacji, analiza ruchu DNS czy przeciążenia prowadzące do DoS – niekoniecznie wynikające z celowej próby naruszenia dostępności usług.

Przykładowe pliki PCAP wykorzystane w ćwiczeniu pochodzą z repozytorium:
Securitum, Wireshark – sample PCAP files, GitHub,
https://github.com/securitum-com/wireshark/tree/main/samples
(materiały użyte wyłącznie w celach dydaktycznych).

I. Wysycenie pasma

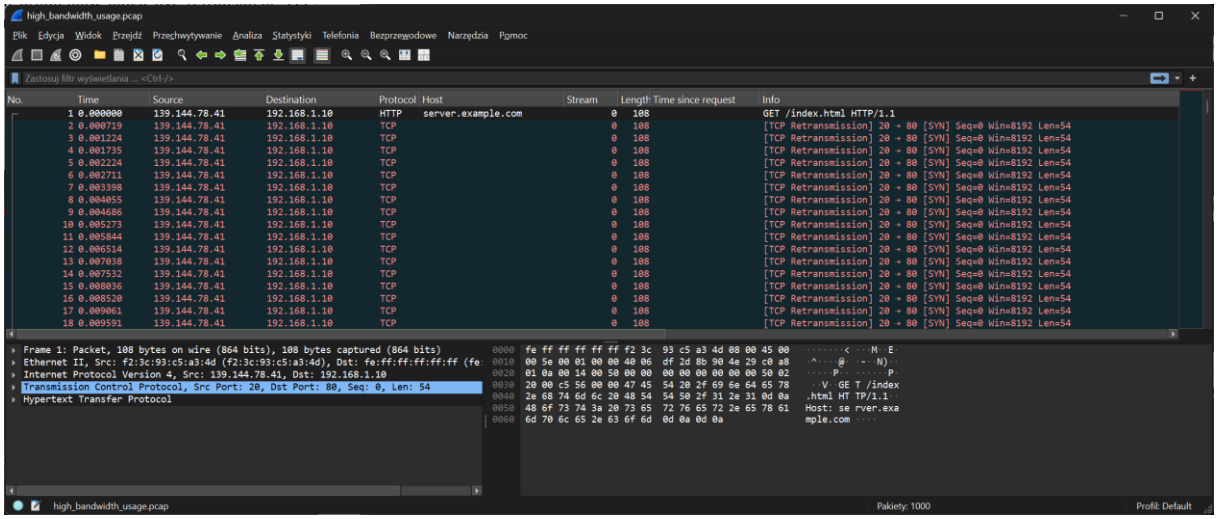
Problem: W infrastrukturze sieciowej stwierdzono, że jeden z hostów generuje ponadprzeciętne obciążenie łącza.

Czego szukać: Zaleca się zawężenie analizy do ruchu HTTP oraz identyfikację źródeł wysyłających dużą liczbę pakietów lub zużywających znaczną część przepustowości. W tym celu warto skorzystać z mechanizmów statystycznych Wiresharka, takich jak `Statistics -> Conversations`.

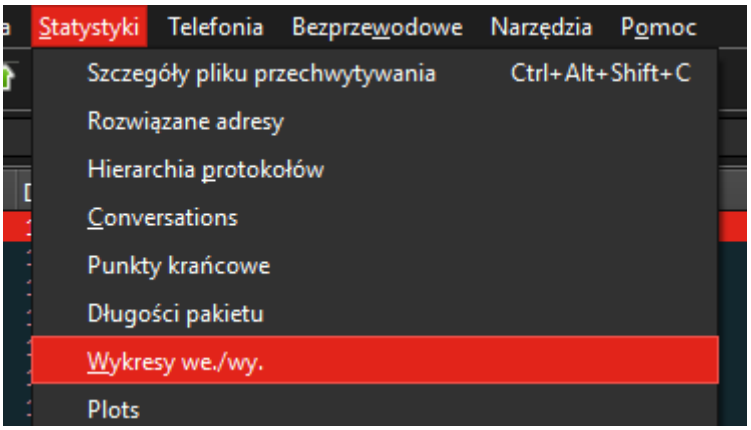
Na co zwrócić uwagę: Kluczowe jest sprawdzenie, czy nadmierne obciążenie łącza skutkuje powstawaniem kolejek lub stratą pakietów. Objawem takich problemów mogą być retransmisje TCP, które najwygodniej przeanalizować za pomocą wykresu I/O.

1. Przejdź do repozytorium i pobierz plik `high_bandwidth_usage.pcap`.

2. Otwórz plik w Wiresharku.



3. Przejdź do `Statystyki -> Wykresy we./wy`.



4. Jaki typ danych został przedstawiony na wykresie?

II. Analiza czasów odpowiedzi serwera

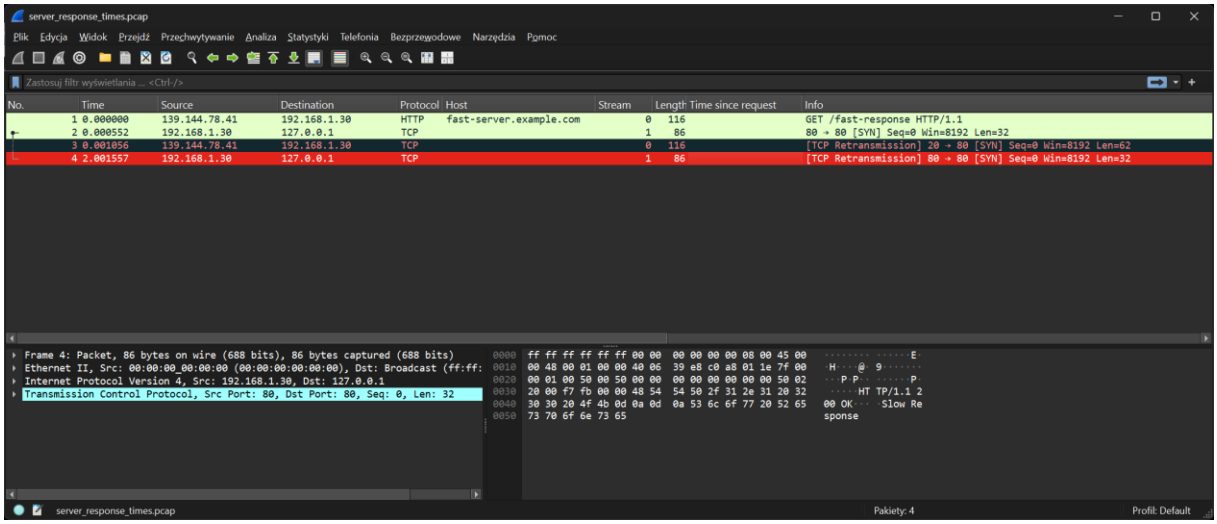
Problem: Działanie serwera WWW jest niestabilne mimo braku widocznych oznak ataku. Strony internetowe wczytują się naprzemiennie szybko i wolno, a zjawisko to ma charakter niedeterministyczny.

Czego szukać: Należy zastosować filtr http.time i przeanalizować czasy odpowiedzi serwera, porównując odstęp czasu pomiędzy wysłaniem żądania a otrzymaniem odpowiedzi.

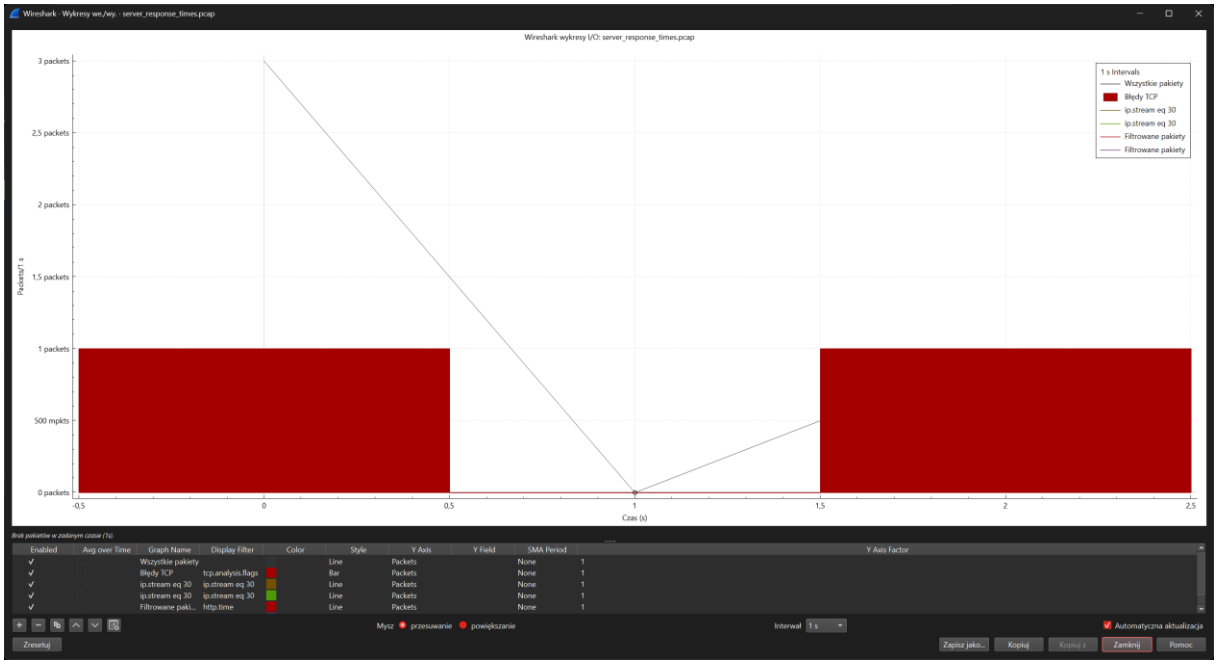
Na co zwrócić uwagę: Warto zidentyfikować serwery lub konkretne zasoby charakteryzujące się wydłużonym czasem odpowiedzi oraz rozważyć, czy przyczyną mogą być problemy po stronie serwera lub infrastruktury sieciowej.

1. Przejdź do repozytorium i pobierz plik `server_response_times.pcap`.

2. Otwórz plik w Wiresharku i zwróć uwagę na kolumnę Time. Jeden pakiet może wyróżniać się czasem – to odpowiedź serwera.



3. Uruchom `wykres we./wy`, analogicznie jak w poprzednim scenariuszu.

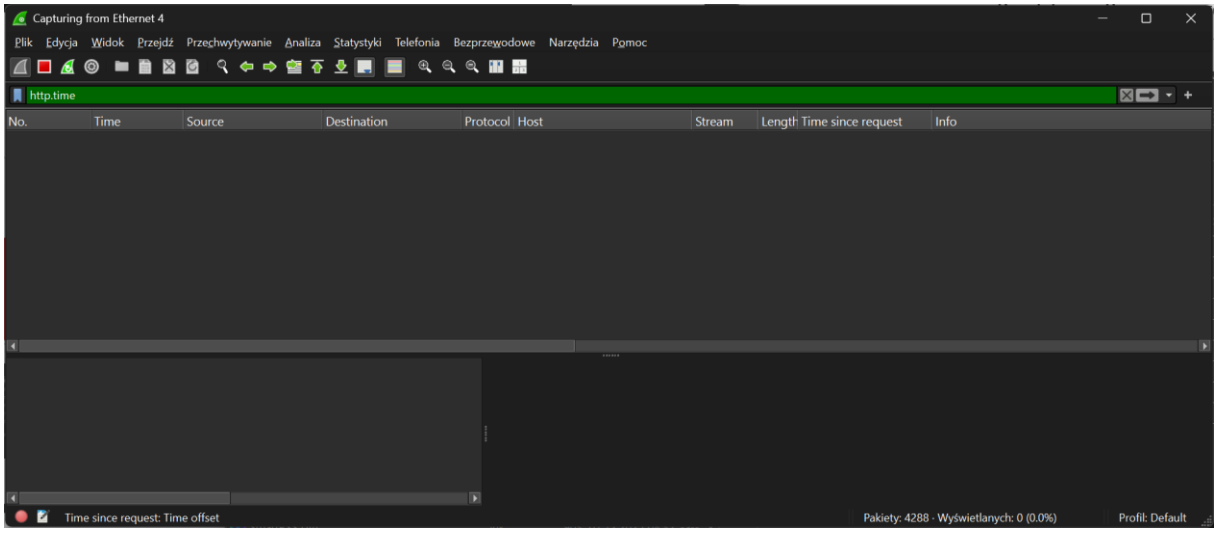


4. Zwróć uwagę na anomalie i nieregularności w czasie odpowiedzi serwera widoczne na wykresie.

5. Zamknij okna analizy.

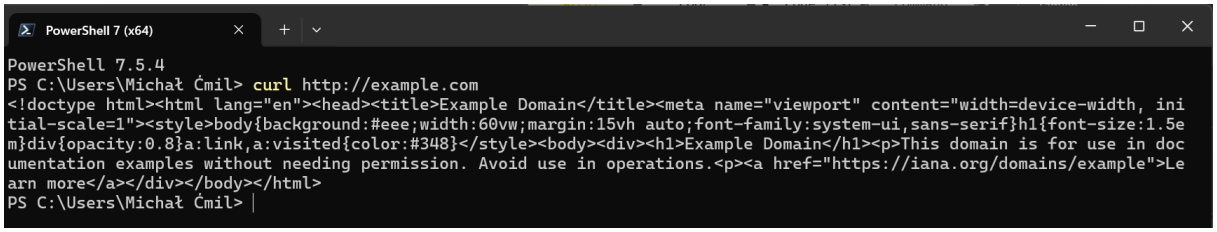
6. Uruchom Wireshark i rozpocznij nasłuch na swoim interfejsie sieciowym.

7. Użyj filtra `http.time`.

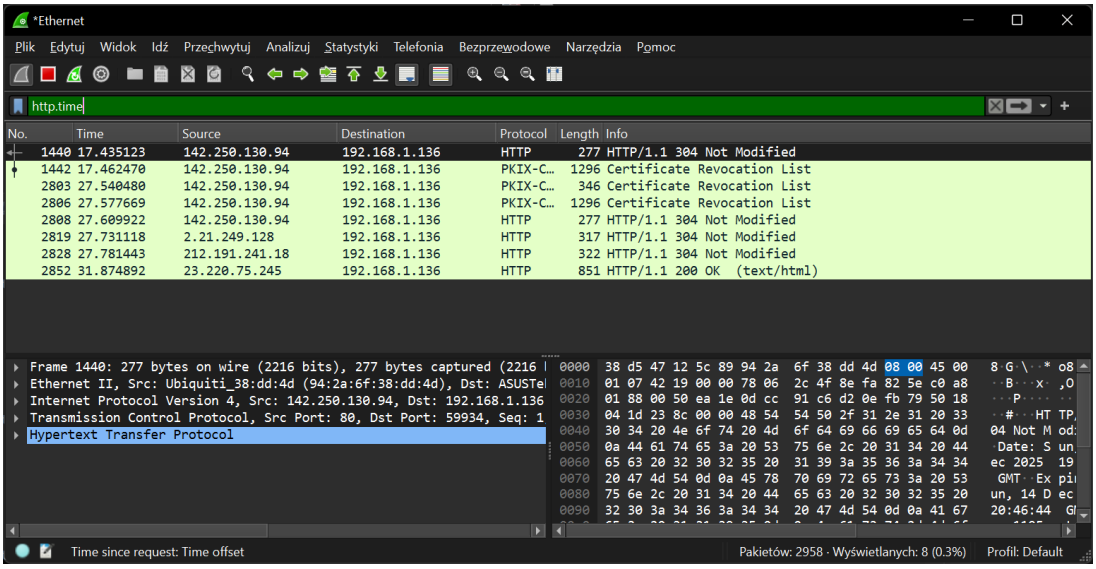


8. Otwórz konsolę PowerShell i wygeneruj ruch HTTP:

```
curl http://example.com
```



9. Wróć do Wiresharka – zobaczysz tylko pakiety HTTP z wyliczonym czasem transakcji.



10. Przetestuj jeszcze 2-3 inne strony i sprawdź ich czas odpowiedzi.

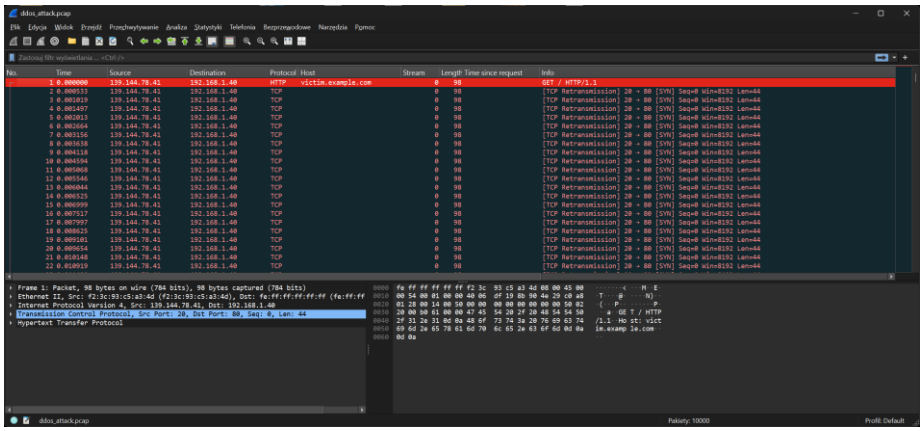
III. Atak DDoS

Problem: Po uruchomieniu serwer działa poprawnie, jednak po krótkim czasie zaczyna wolno odpowiadać, aż w końcu usługa całkowicie się zawiesza.

Co należy sprawdzić: Należy zwrócić uwagę na bardzo duży ruch sieciowy kierowany do jednego adresu IP. W tym celu można użyć filtra: `ip.dst == <adres_docelowy>`

Na co zwrócić uwagę: Warto sprawdzić, czy ruch pochodzi z wielu źródeł oraz czy zawiera wzorce typowe dla ataków DDoS, np. wielokrotne żądania HTTP w krótkim czasie.

1. Pobierz z repozytorium plik `ddos_attack.pcap` i otwórz go w Wiresharku.



2. Sprawdź `wykres we./wy`.

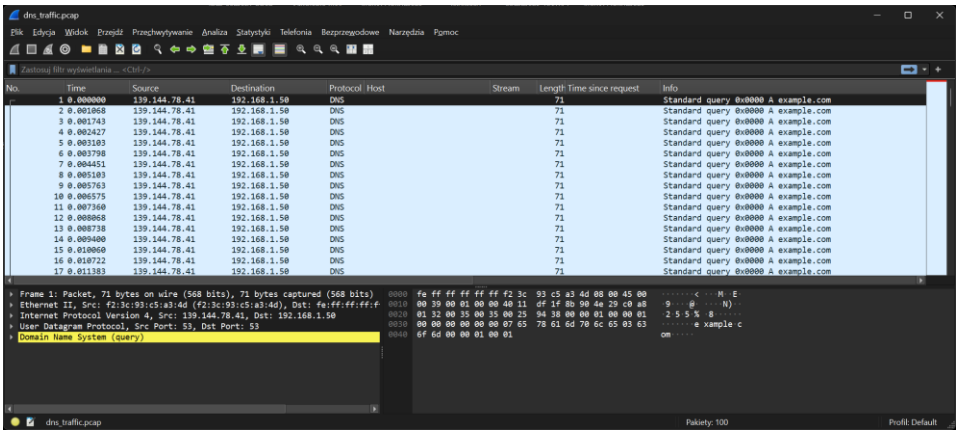
IV. DNS

Problem: Wiele rodzajów malware'u korzysta z usługi DNS do komunikacji z serwerami, aby pobierać dodatkowe złośliwe oprogramowanie lub instrukcje od atakującego. Analiza ruchu DNS pozwala wykryć nietypowe zapytania, które mogą wskazywać na obecność złośliwego oprogramowania w infrastrukturze.

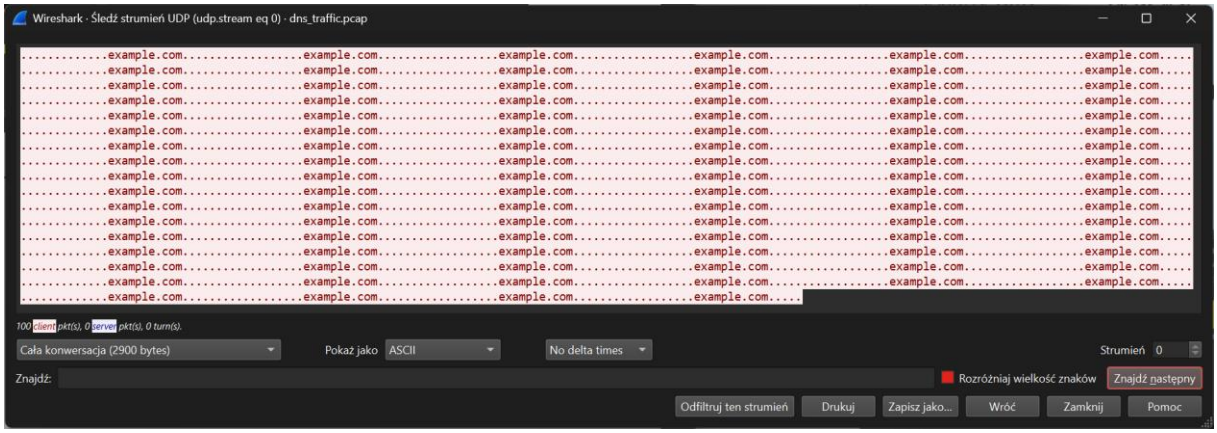
Co należy sprawdzić: Filtr dns pozwala wyizolować ruch DNS i skupić się na jego analizie.

Na co zwrócić uwagę: Należy dokładnie analizować zapytania i odpowiedzi DNS, aby wykryć: nietypową aktywność, błędne konfiguracje, powtarzalne lub podejrzane wartości w treści pakietów UDP.

1. Pobierz z repozytorium plik `dns_traffic.pcap` i otwórz go w Wiresharku.



2. Kliknij prawym przyciskiem myszy na dowolny pakiet i wybierz `Podążaj -> Strumień UDP`.



Zwróć uwagę, że w złożonym strumieniu UDP w treści pakietów występuje powtarzalna wartość z domeną `example.com`, co nie jest naturalnym zachowaniem protokołu DNS i może wskazywać na podejrzaną aktywność.

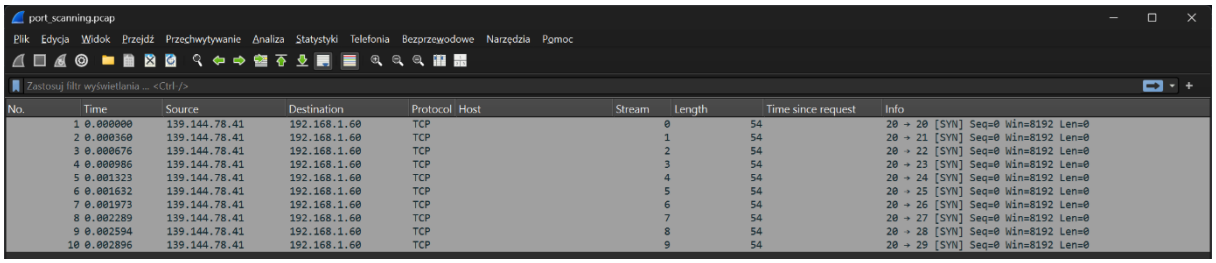
V. Skanowanie portów

Problem: Nieautoryzowane skanowanie portów jest często wstępem do bardziej złożonych ataków. Atakujący szukają słabych punktów, takich jak niezabezpieczone usługi, nieaktualne oprogramowanie lub porty dostępne z Internetu. Wykrycie skanowania pozwala na wczesne zidentyfikowanie zagrożenia i zwiększa czas na zabezpieczenie systemów.

Co sprawdzić: Szukać serii pakietów TCP lub UDP kierowanych na różne porty docelowe. Filtr w Wireshark: `tcp.flags.syn == 1 && !tcp.flags.ack`

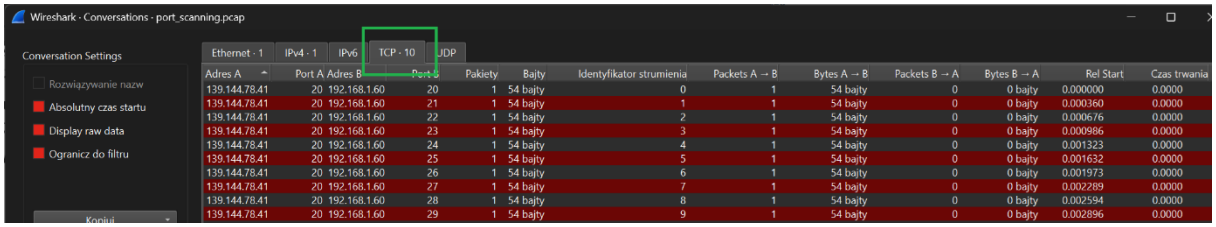
Na co zwrócić uwagę: Pakiety, które nie otrzymują odpowiedzi – mogą wskazywać na skanowanie portów.

1. Pobierz z repozytorium plik `port_scanning.pcap` i otwórz go w Wiresharku.



2. Przejdź do `Statystyki -> Conversations`.

3. Wybierz zakładkę `TCP`.



4. Analizując dane, określ, na jakiej podstawie można wnioskować, że użyto skanera portów.