Laboratorium 3

Wireshark cz. 1

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

Hosty (np. komputery) w sieci komputerowej komunikują się poprzez wymianę danych w postaci pakietów i ramek. **Pakiet** to podstawowa jednostka w sieciach IP: niesie treść użytkownika oraz informacje sterujące (np. typ protokołu, adresy logiczne). **Ramka** działa warstwę niżej — na łączu — i przenosi pakiet przez medium fizyczne, takie jak kabel miedziany, światłowód czy fale radiowe.

Wireshark to darmowy analizator ruchu sieciowego, który umożliwia przechwytywanie i interaktywną analizę pakietów. Dzięki wygodnemu interfejsowi i rozbudowanym filtrom jest jednym z podstawowych narzędzi administratorów, programistów i specjalistów bezpieczeństwa: pozwala szybko „wejść w głąb" komunikacji i skutecznie diagnozować problemy – w skrócie: pozwala wykrywać i analizować zagrożenia w sieciach komputerowych.

Wireshark jest narzędziem uniwersalnym, które może być wykorzystywane na różne sposoby. Przede wszystkim jednak jest używany w następujących scenariuszach:

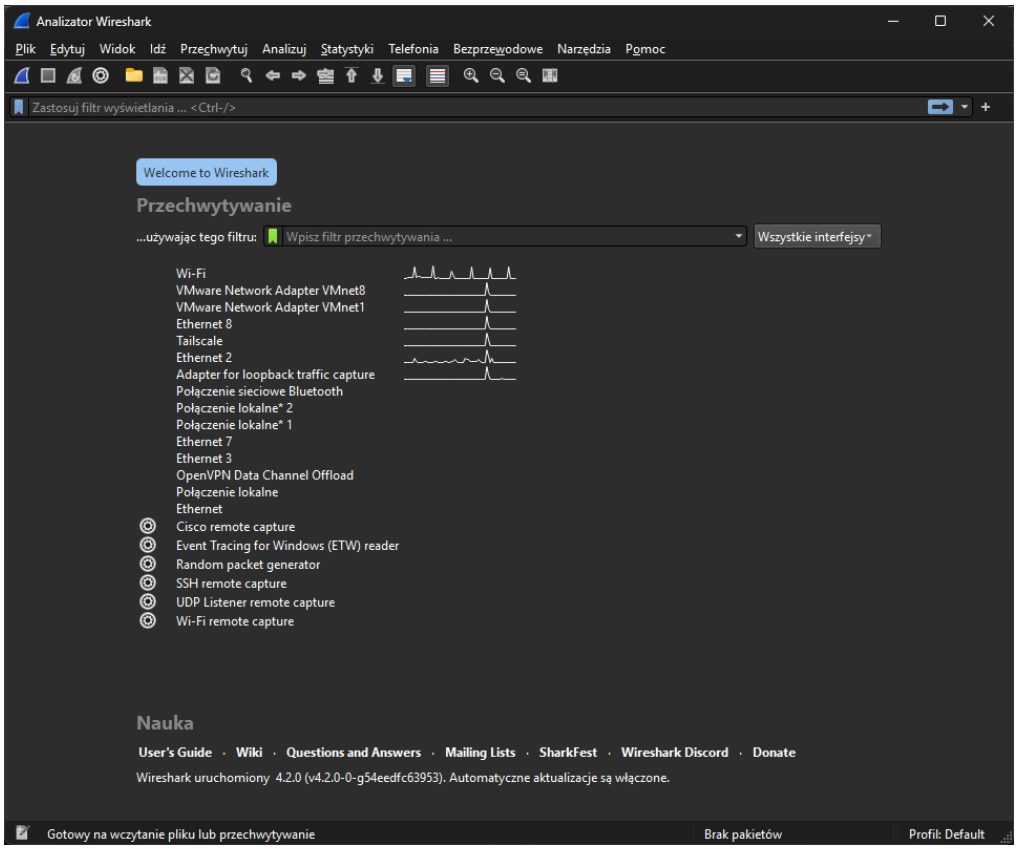
- **Diagnostyka sieci** – szybkie wykrywanie i rozwiązywanie problemów z łącznością i wydajnością.
- **Bezpieczeństwo** – monitorowanie ruchu pod kątem podejrzanych wzorców, analiza incydentów także po fakcie.
- **Rozwój i protokoły** – testowanie aplikacji oraz szczegółowa analiza działania protokołów.
- **Edukacja** – przystępne poznawanie złożonej komunikacji sieciowej.

Źródło: *https://levelup.gitconnected.com/wireshark-demystified-a-beginners-step-by-step-guide-ca55596facfb*

I. Pierwsze kroki z Wiresharkiem

1. Uruchom Wiresharka.

Po starcie zobaczysz listę interfejsów Po chwili pojawią się mikro-wykresy aktywności, które podpowiedzą, gdzie jest ruch.



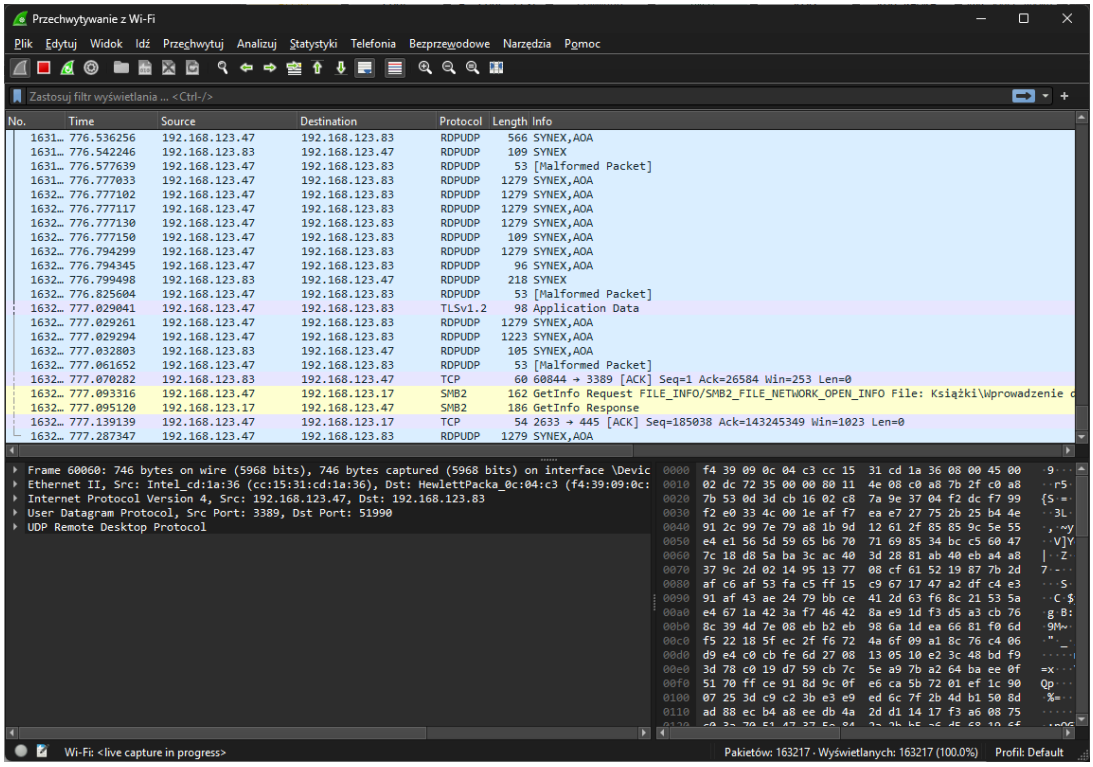
2. Wybierz interfejs do analizy (zwykle Ethernet lub Wi-Fi).

Jeżeli nie wiesz, który interfejs wybrać, uruchom konsolę `CMD` i wpisz polecenie `ipconfig`, aby odczytać nazwę interfejsu — będzie to ten z nadanym adresem IP widniejącym na naklejce na obudowie komputera.

3. Poznaj układ okien.

Domyślny widok ma trzy panele:

- Packet List (góra): na bieżąco rosnąca lista przechwyconych pakietów (możliwa kolorystyka według reguł).
- Packet Details (lewy dół): szczegóły wybranego pakietu w postaci drzewa protokołów i pól nagłówków.
- Packet Bytes (prawy dół): surowe bajty pakietu – rzeczywista postać transmisji na interfejsie.



Pierwsze uruchomienie Wiresharka może przytłoczyć ilością danych w przechwyconej komunikacji sieciowej. Dodatkowo może się okazać, że komputer także nie podoła temu zadaniu w przypadku przechwytywania pełnego ruchu sieciowego (Full Packet Capture). Użyj filtrów, by ograniczyć dane.

Wireshark ma dwa typy filtrów:

- Capture filters – stosowane przed przechwytywaniem; ograniczają to, co w ogóle zostanie zapisane (mniejsze obciążenie).
- Display filters – stosowane po przechwytywaniu; filtrują widok w GUI (nie zmieniają zebranych danych).

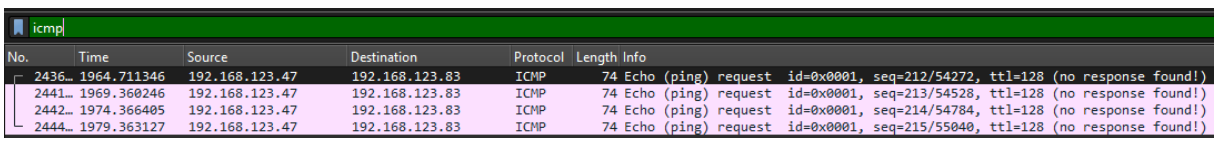
4. W polu `Zastosuj filtr wyświetlania` wpisz `icmp` i naciśnij `Enter`.

5. Zauważ efekt filtra – lista pokaże teraz tylko pakiety ICMP (pozostałe znikną z widoku).

6. Wygeneruj ruch ICMP – w CMD/PowerShell wykonaj:

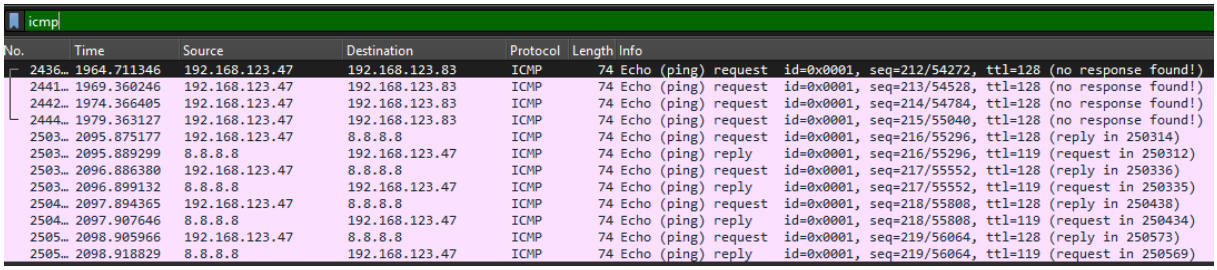
```
ping adres_IP_sąsiada
```

7. Komunikacja najprawdopodobniej się nie powiedzie. Spójrz ponownie w Wiresharku – powinieneś zobaczyć zarejestrowane pakiety podobne do tych na poniższym zrzucie.



8. Upewnij się, że sąsiad wyłączył zaporę systemu Windows (patrz poprzednie zajęcia).

9. Ponownie wykonaj polecenie `ping`.



10. Jak widzisz, tym razem komunikacja wygląda nieco inaczej. Wyjaśnij:

    - Dlaczego komunikacja się zmieniła po wyłączeniu zapory?
    - Czym różni się Echo Request od Echo Reply?
    - Co oznaczają parametry id, seq i ttl w pakietach ICMP?

11. Wpisz w polu filtra: `ip.addr == 8.8.8.8` i naciśnij `Enter`.

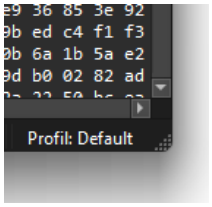
12. Wyślij ping do publicznego DNS Google.

13. Zweryfikuj przechwycenie ruchu – sprawdź, czy w Wiresharku widać odpowiednie request/reply do i z adresu 8.8.8.8

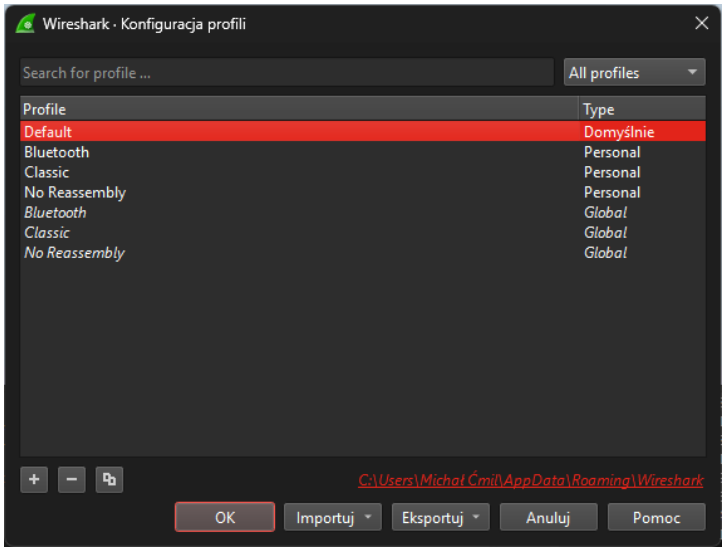
II. Dostosowanie wyglądu Wiresharka do własnych wymagań

Układ graficzny, kolory oraz rozkład okien w Wiresharku można zmienić i zapisać jako własny profil, a nawet stworzyć ich kilka!

1. W prawym dolnym rogu znajdziesz rozwijaną listę `Profiles`. W zależności od zadania możesz przełączać się między profilami (np. administracyjny, analityczny, deweloperski). Sprawdź zdefiniowane wcześniej profile.



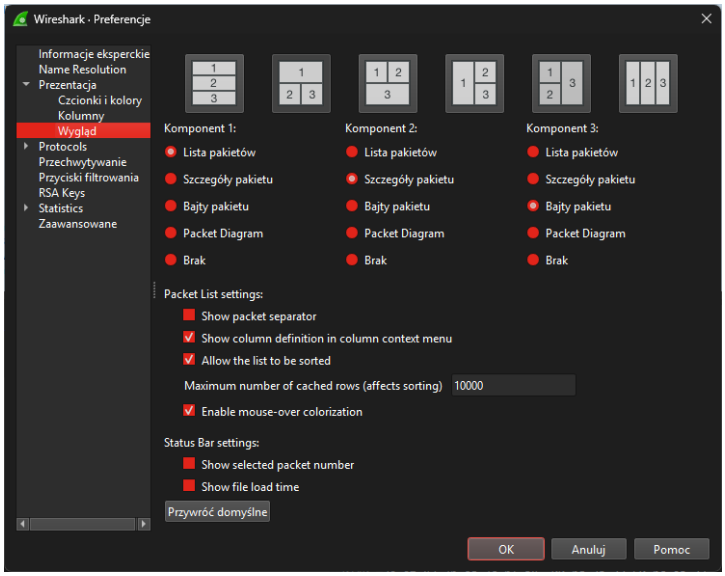
2. Kliknij prawym przyciskiem myszy i wybierz `Manage Profiles…`, aby zarządzać profilami.



3. Kliknij `+` (w lewym dolnym rogu) i nazwij nowy profil — jako nazwę podaj swój indeks.

4. Zatwierdź przyciskiem `OK`.

5. Nic nie stoi na przeszkodzie, aby zmienić tzw. układ (Layout) programu. Przejdź do: `Edycja -> Preferencje… -> Prezentacja -> Wygląd`.

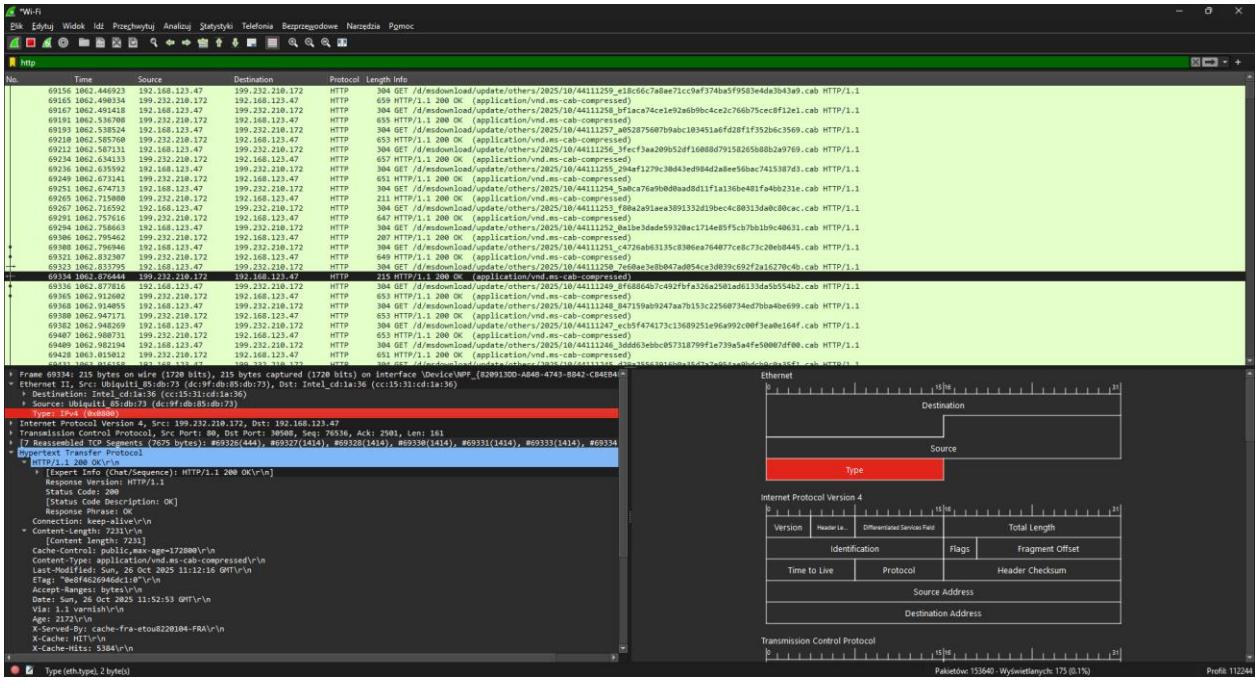


Domyślnie wyświetlane są: Lista pakietów, Szczegóły pakietu i Bajty pakietu, ale widoki można modyfikować.

6. Zmień komponent nr 3 na `Packet Diagram`.

7. Wcześniej przechwytywałeś ICMP; tym razem przechwyć ruch HTTP.

8. Wybierz dowolny pakiet z listy.



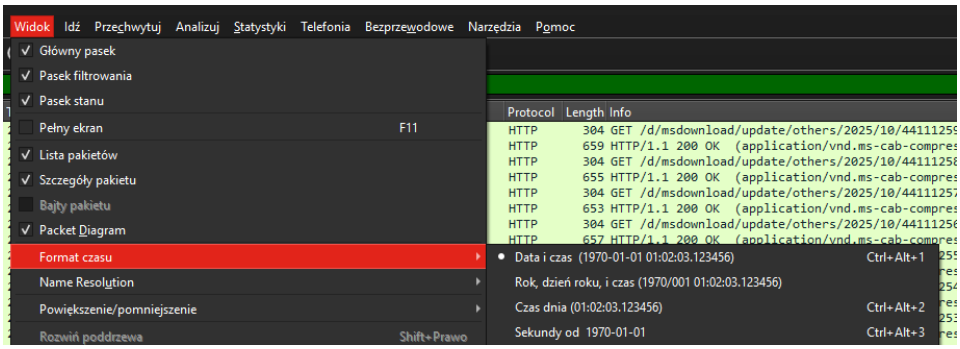
Packet Diagram pokazuje pakiet „na płasko” — warstwa po warstwie, bit po bicie. Gdy klikniesz dowolne pole w lewym oknie, odpowiadający mu fragment nagłówka podświetli się po prawej (i odwrotnie). Wybór pakietu w górnej liście steruje tym, co oba okna pokazują.

9. Znajdź i odczytaj TTL w nagłówku IPv4.

Kolejną istotną kwestią podczas analizy jest właściwe oznaczenie czasu zdarzeń — szczególnie w środowiskach międzynarodowych, gdzie pliki mogą mieć różne strefy czasowe.

10. Spójrz na kolumnę Time – domyślny format bywa mało czytelny.

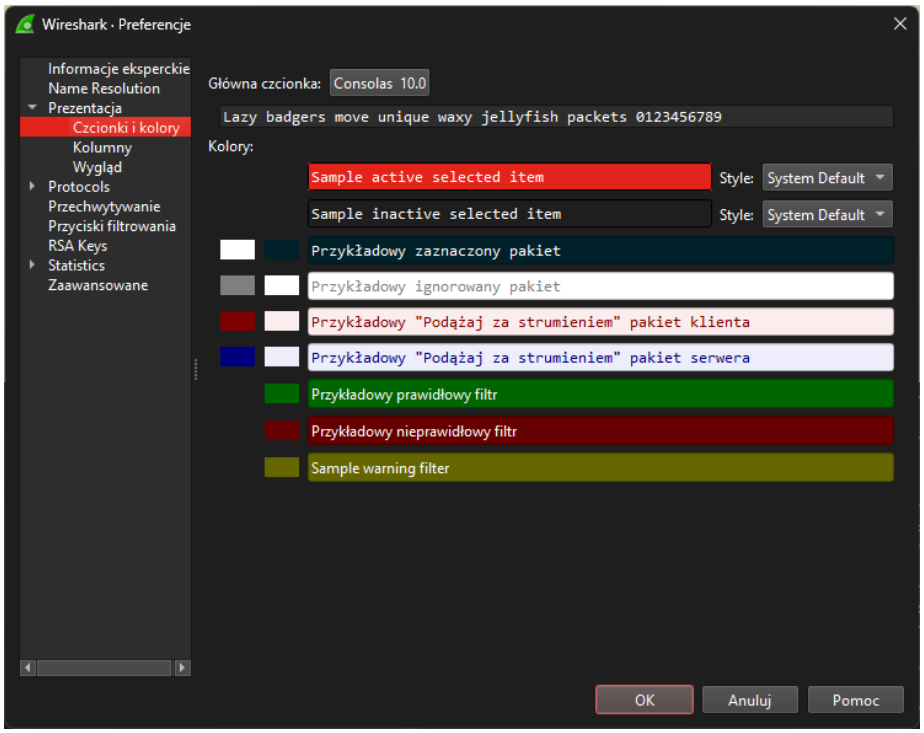
11. Przejdź do: `Widok -> Format czasu`, a następnie wybierz odpowiedni format, np. `Data i czas`.



12. Sprawdź ponownie kolumnę Time — powinna być teraz czytelniejsza.

Choć może to zaskakiwać, bardzo pomocne bywa zdefiniowanie własnych kolorów interfejsu oraz reguł kolorowania danych na podstawie zadanych kryteriów.

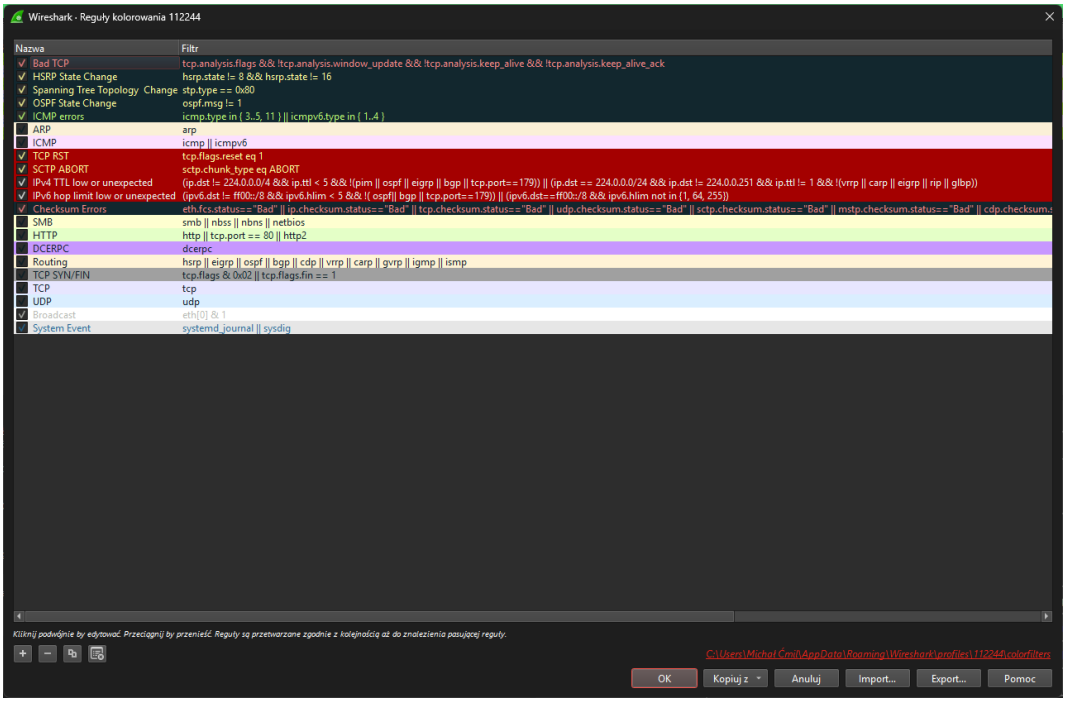
13. Aby zmienić kolory interfejsu, przejdź do: `Edycja -> Preferencje… -> Prezentacja -> Czcionki i kolory`.



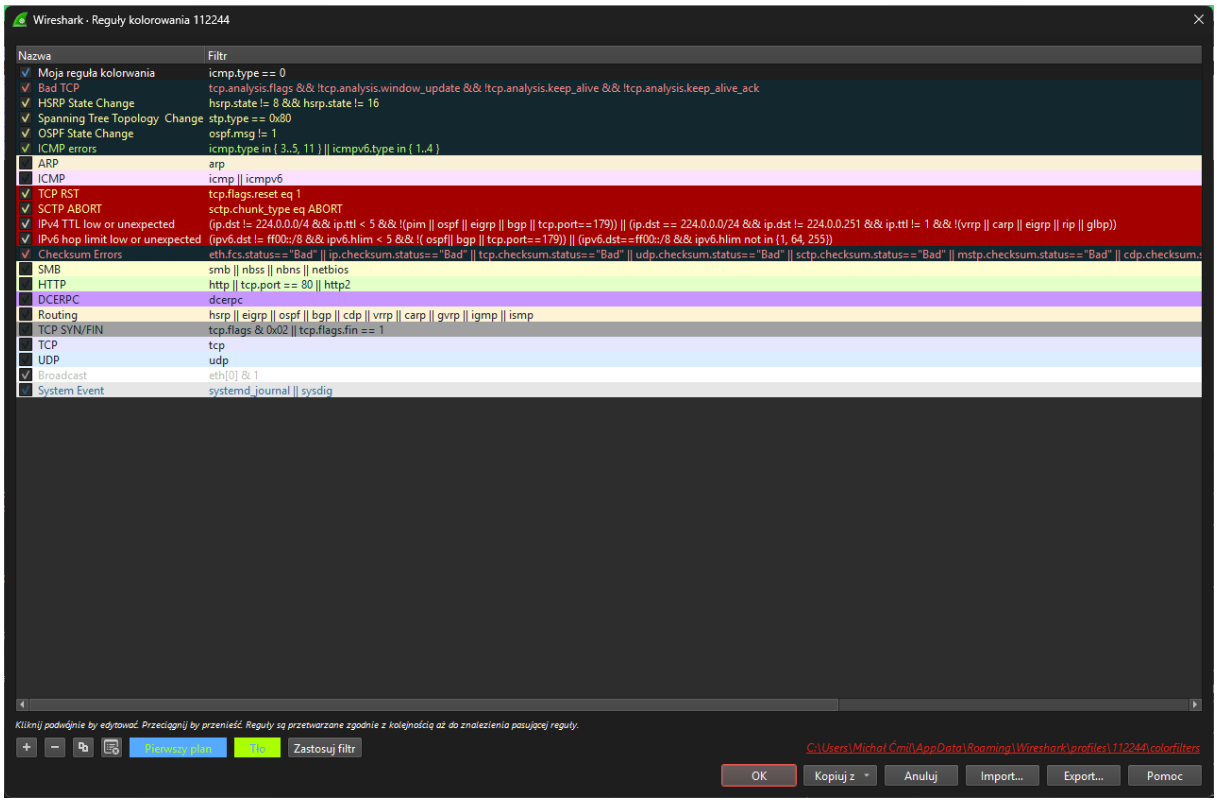
14. Dostosuj kolory do swoich preferencji i zatwierdź `OK`.

Jednak sam wygląd danych to nie koniec możliwości konfiguracyjnych Wiresharka podczas pracy. Reguły kolorowania mogą pomóc w namierzeniu istotnych danych.

15. Zdefiniujmy własną regułę kolorowania. Przejdź do: `Widok -> Reguły kolorowania…`.

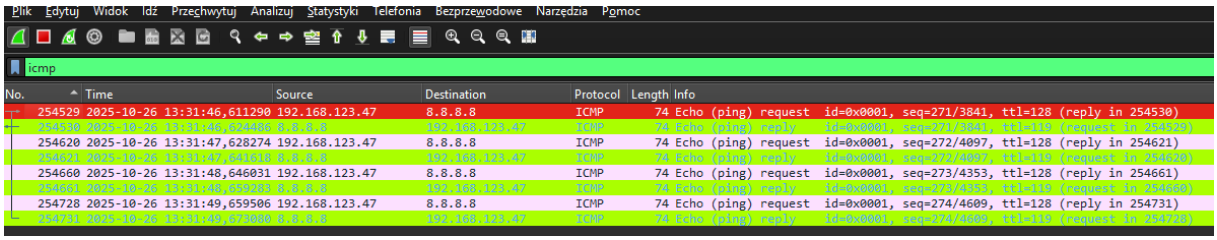


16. Dodaj nową regułę (`+`), nadaj nazwę i ustaw filtr `icmp.type == 0`. Ustaw kolory pierwszego planu i tła tak, aby były wyraźne i czytelne. Zatwierdź `OK`.



Otworzona reguła będzie kolorować pakiety ICMP Echo Reply. Sprawdźmy to.

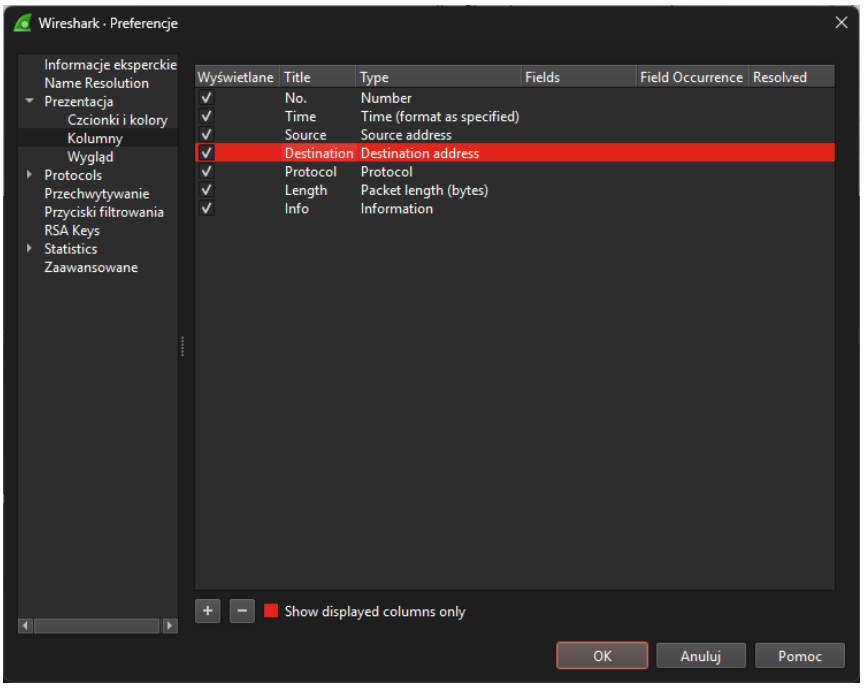
17. Przechwyć pakiety icmp i sprawdź kolorwanie. (jeśli ich nie ma, wykonaj ponownie `ping` do hosta w sieci).



Dzięki kolorowaniu łatwiej skupić się na ważnych zdarzeniach (błędy, retransmisje, anomalie) i szybciej je wychwycić.

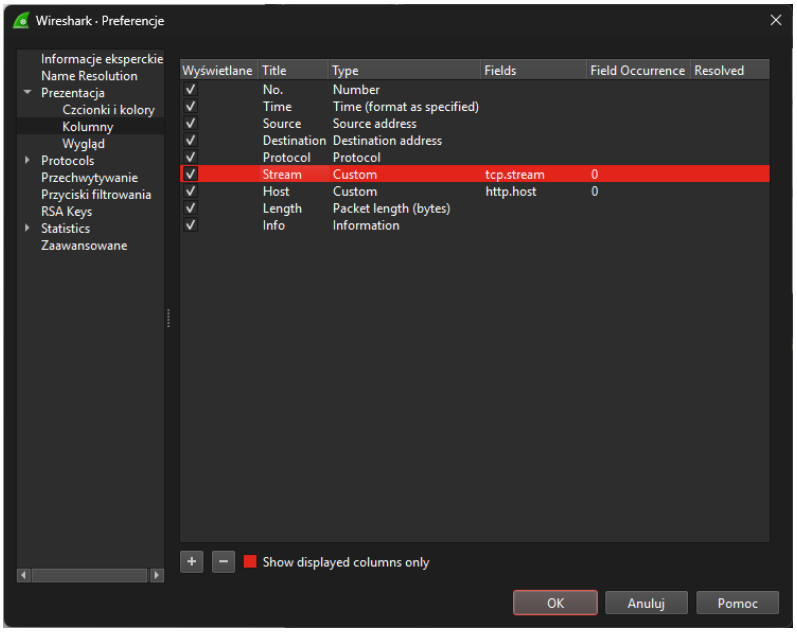
W pracy analityka i administratora przydatną wartością przyspieszającą analizę ruchu sieciowego jest dołączenie kolumn z filtrami http.host oraz tcp.stream. Ułatwia to przegląd zrzutu przechwytywania nawet bez konkretnego filtra.

18. Dodaj nową kolumnę: `Edycja -> Preferencje… -> Prezentacja -> Kolumny`.



19. Dodaj dwie kolumny (przycisk `+`), nazywając je `Stream` i `Host`, z wartościami odpowiednio `tcp.stream` oraz `http.host`.

Uwaga: nowe kolumny domyślnie pojawią się na końcu – przeciągnij je w górę listy, aby były widoczne bez przewijania.



20. Zatwierdź przyciskiem `OK` i sprawdź dwie nowe kolumny na liście przechwyconych pakietów.