Politechnika Rzeszowska
Katedra Mechaniki Stosowanej i Robotyki

SIECI KOMPUTEROWE I BAZY DANYCH
Laboratorium

Temat 1:

Komendy i ustawienia sieciowe systemu Windows
Wireshark - wprowadzenie

Autor: dr inż. Paweł Penar

Rzeszów 2024

Instrukcja przygotowana z wykorzystaniem materiałów dodatkowych do książki Computer Networking: A Top-Down Approach, edycja 8 autorstwa J.F. Kurose and K.W. Ross dostępnych pod adresem: https://gaia.cs.umass.edu/kurose_ross/index.php

1. Cel laboratorium

Celem laboratorium jest:

- zapoznanie się z konsolowymi narzędziami sieciowymi systemu Windows*:*
  - *ipconfig**,***
  - *ping**,***
  - *tracert*
- przeprowadzenie konfiguracji kart sieciowych w systemie Windows
- zapoznanie się ze snifferem Wireshark.

2. Wprowadzenie

2.1. Komendy sieciowe Windows

Wszystkie współczesne systemy operacyjne posiadają podstawowe narzędzia do kontroli i analizy ruchu sieciowego. Przy ich pomocy można sprawdzić konfiguracje protokołu TCP/IP, interfejsów sieciowych czy przetestować usługę DNS. Co więcej, za pomocą wyżej wymienionych narzędzi można sprawdzić połączenie pomiędzy stacjami czy określić trasę przesyłanego zapytania.

Poniżej zamieszczono krótki spis możliwości wybranych narzędzi sieciowych dostępnych w systemie Windows:

ipconfig – narzędzie służy do wyświetlania konfiguracji sieci w protokole TCP/IP oraz odświeżenia informacji dot. DHCP i DNS. Wywołanie w konsoli systemu polecenie bez parametrów powoduje wyświetlenie: adresu IP, maski podsieci oraz bramy domyślnej dla wszystkich interfejsów sieciowych. Działanie programu może być modyfikowane przez dodanie parametrów np:

- parametr ***/all*** – wyświetla rozszerzone informacje dotyczące interfejsów sieciowych
- parametr ***/displaydns*** – wyświetla zawartość tablicy DNS która jest zapisana na lokalnej maszynie

***ping* –** narzędzie służące do testowania połączeń pomiędzy hostem testowanym i testującym poprzez wykorzystanie protokołu ICMP. Przykład polecenia konsolowego wykorzystującego program ping to komenda:

```
ping wp.pl lub ping 192.168.10.1
```

W pierwszym przypadku program **ping** korzysta z serwera DNS do określenia numeru IP hostu, z którym chce się połączyć. W drugim przypadku jest on podany jawnie.
Dodatkowo program *ping* może być użyty z szeregiem parametrów. Wybrane przykłady to:

- parametr **-t** – wysyłanie zapytania do czasu wybrania przez użytkownika **CTRL+C**. Wciskając **CTRL+BREAK** uzyskujemy podsumowania dotychczasowych zapytań.
- parametr **-n N** – żądanie wysłania dokładnie **N** zapytań. Domyślnie **N=4.**
- parametr **-l size** – żądanie wysłania pakietu o określonej długości **size**. Domyślnie **size=32** bajty, natomiast maksymalny rozmiar pakietu to 65527 bajtów.
- parametr **-a** – tłumaczy adresy na nazwy hostów

Program ping można wykonać także online na stronie: https://ping.eu/ping/

tracert – program służący do określania trasy pomiędzy hostem, na którym wykonano polecenie a hostem docelowym. Przykładem jego użycia jest polecenie

```
tracert wp.pl
```

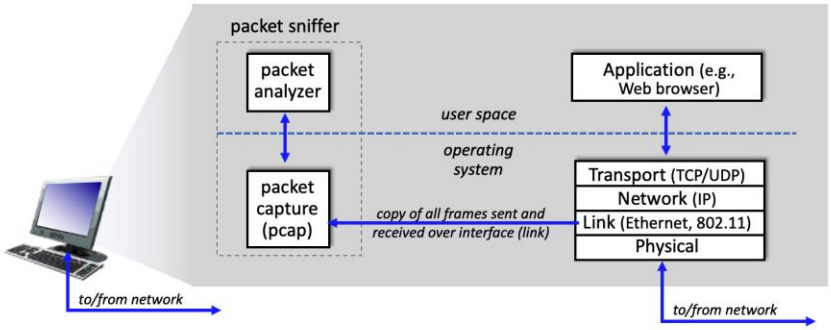
To polecenie sprawdzi trasę pakietów protokołu TCP/IP w przypadku połączenie z portalem Wirtualna Polska. Jednym z ciekawszych parametrów polecenia **tracert** jest parametr **-h N**, który określa maksymalną liczbę skoków na ścieżce pomiędzy nadawcą a odbiorcą. Domyślnie **h=30.**

Polecenie tracert może być również realizowane online na stronie: https://ping.eu/traceroute/

2.2. Wireshark

Zrozumienie protokołów sieciowych można lepiej zrozumieć poprzez „obserwacje protokołów w akcji" czy „bawiąc się protokołami" – tj. obserwując sekwencję komunikatów wymienianych między nadawcą i odbiorcą. Ma to na celu poznanie szczegółów działania protokołów i jest realizowane poprzez wykonanie określonej czynności, a następnie obserwowanie te czynności i ich konsekwencje. Można to zrobić w środowisku laboratoryjnym lub w „prawdziwym" środowisku sieciowym, takim jak Internet.

Podstawowym narzędziem do obserwacji komunikatów wymienianych pomiędzy nadawcą i odbiorcą w danym protokole jest sniffer pakietów. Jak sama nazwa wskazuje, sniffer pakietów przechwytuje wiadomości wysyłane/odbierane z/przez komputer; będzie również zwykle przechowywać i/lub wyświetlać zawartość różnych pól protokołów w tych przechwyconych wiadomościach. Sam sniffer pakietów jest pasywny. Obserwuje wiadomości wysyłane i odbierane przez aplikacje i protokoły uruchomione na komputerze, ale nigdy nie wysyła samodzielnie pakietów.



Rysunek 1: Struktura sniffer pakietów

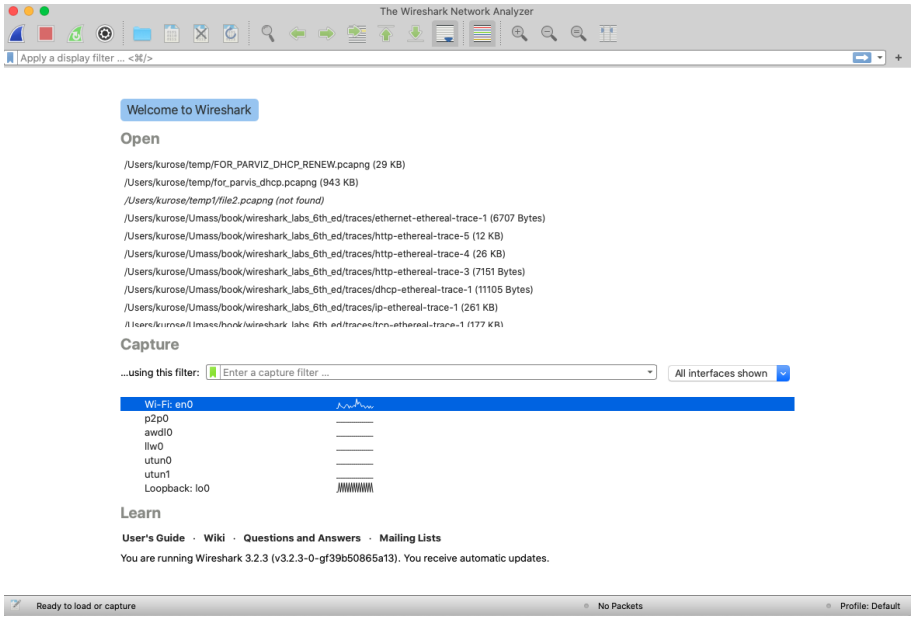
Rys. 1 przedstawia strukturę sniffera pakietów. Po prawej stronie rysunku 1 znajdują się protokoły (w tym przypadku protokoły internetowe) i aplikacje (takie jak przeglądarka internetowa lub klient poczty e-mail), które normalnie działają na komputerze. Sniffer pakietów, pokazany w przerywanym prostokącie na rysunku 1, jest dodatkiem do zwykłego oprogramowania w komputerze i składa się z dwóch części. Pierwsza z nich to biblioteka przechwytywania pakietów, która otrzymuje kopię każdej

ramki warstwy łącza danych. Ostatecznie to ona przesyła dane protokołów warstwy aplikacji, takich jak HTTP, FTP, TCP, UDP, DNS lub IP gdyż te są przesyłane przez nośniki fizyczne.
Drugim elementem sniffera pakietów jest analizator pakietów, który wyświetla zawartość wszystkich pól w komunikacie protokołu. W tym celu analizator pakietów musi „zrozumieć" strukturę wszystkich komunikatów wymienianych przez protokoły.

W tych laboratoriach będziemy używać sniffera pakietów Wireshark
http://www.wireshark.org/

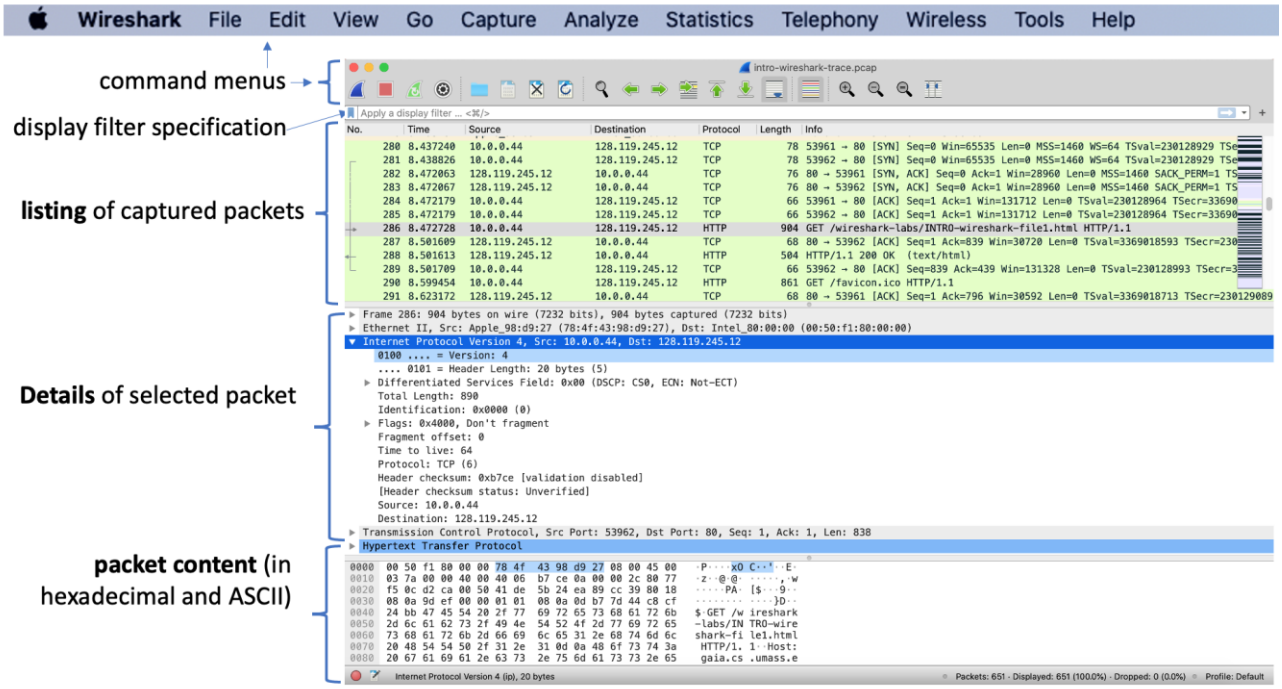
2.2.1. Uruchomienie Wireshark

Po uruchomieniu programu Wireshark widoczny jest ekran startowy, który wygląda podobnie do tego, który pokazano na rys. 2.



Rysunek 2: Ekran startowy Wireshark

Na ekranie startowym nie ma zbyt wiele interesujących rzeczy. Należy jednak pamiętać, że w sekcji *Capture* znajduje się lista interfejsów sieciowych przez które pakiety przechodzą do/z analizowanego komputera. W zależności od sposobu podłączenia do sieci będą to interfejsy WiFi lub Ethernet. Jeśli jeden z tych interfejsów zostanie wybrany, rozpocznie się przechwytywanie pakietów i zostanie wyświetlony ekran podobny do tego, który pokazano na rys. 3. Przechwytywania pakietów można zatrzymać, korzystając przycisku Stop.



Rysunek 3: Ekran Wiresharka podczas przechwytywania pakietów

Interfejs Wireshark składa się z pięciu głównych komponentów:

- **Menu poleceń** to standardowe rozwijane menu znajdujące się w górnej części okna programu Wireshark.

- **Okno listy pakietów** wyświetla jednowierszowe podsumowanie każdego przechwyconego pakietu, w tym numer pakietu, czas przechwycenia pakietu, adresy źródłowe i docelowe pakietu, typ protokołu i informacje specyficzne dla protokołu zawarte w pakiecie. Listę pakietów można sortować według dowolnej z tych kategorii, klikając nazwę kolumny. Pole typu protokołu zawiera protokół najwyższego poziomu, który wysłał lub odebrał ten pakiet.

- **Okno szczegółów nagłówka** pakietu zawiera szczegółowe informacje o pakiecie wybranym w oknie listy pakietów. Te szczegóły obejmują informacje o ramce Ethernet (zakładając, że pakiet został wysłany/odebrany przez interfejs Ethernet) oraz datagram IP, który zawiera ten pakiet. Ilość wyświetlanych szczegółów warstwy Ethernet i IP można rozszerzyć lub zminimalizować. Jeśli pakiet został przeniesiony przez protokoły TCP lub UDP, zostaną również wyświetlone szczegóły dotyczące protokołu TCP lub UDP, które w podobny sposób można rozszerzyć lub zminimalizować. Na koniec podano szczegółowe informacje na temat protokołu najwyższego poziomu, który wysłał lub odebrał ten pakiet.

- **Okno zawartości pakietu** wyświetla całą zawartość przechwyconej ramki, zarówno w formacie ASCII, jak i szesnastkowym.

- W górnej części graficznego interfejsu użytkownika programu Wireshark znajduje się **pole filtru** wyświetlania pakietów, w którym można wprowadzić nazwę protokołu lub inne informacje w celu przefiltrowania informacji wyświetlanych w oknie listy pakietów.

3. Zadania

3.1. Narzędzia sieciowe systemu Windows

1. Zapoznaj się z wynikiem działania programu **ipconfig** bez parametrów oraz z parametrami **/all** i **/displaydns.** Jakie informacje zostały zwrócone ? Opisz krótko, co oznacza: Adres IP, brama domyśla, maska podsieci, DNS, adres MAC.

2. Zapoznaj się z wynikiem działania programu ping w następujących sytuacjach:

a) wykonaj **ping** do strony **wp.pl**
b) wykonaj **ping** do serwera o numerze **IP 10.11.12.13**
c) wykonaj **ping** do serwera o numerze **IP 127.0.0.1** – dlaczego jest on tak niski ?
d) wykonaj **ping** do serwera **www.erzeszow.pl** o rozmiarze 2000 bajtów
e) wykonaj **ping** do serwera o numerze **IP 127.0.0.1** o rozmiarze 2000 bajtów
f) wykonaj ping do serwera wp.pl i www.erzeszow.pl za pomocą narzędzia online (https://ping.eu/ping/).

3. Korzystając z polecenia **tarcert** na stronie https://ping.eu/traceroute/ opisz jego wynik w następujących przypadkach:

a) połączenia z portalem **wp.pl**
b) połączenia z portalem **google.com**
c) połączenia z portalem **web.mit.edu**
d) połączenia z numerem **IP 127.0.0.1**
e) połączenia z numerem **IP 104.28.29.81**
f) połączenie z portalem **www.mofa.gov.mm**

Narzędzie WHOIS: https://who.is

3.2. Ustawienia kart sieciowych

4. Zapoznaj się ze sposobami konfiguracji karty sieciowej w Windows. Przedstaw je prowadzącemu.

3.3. Wireshark

5. Uruchom przeglądarkę internetową, która wyświetli stronę główną.

6. Uruchom oprogramowanie Wireshark. Początkowo wyświetli się okno podobne do pokazanego na rysunku 2. Wireshark nie zaczął jeszcze przechwytywać pakietów.

7. Aby rozpocząć przechwytywanie pakietów, z menu *Capture* i wybierz interfejs sieciowy. Spowoduje to rozpoczęcie przechwytywania.

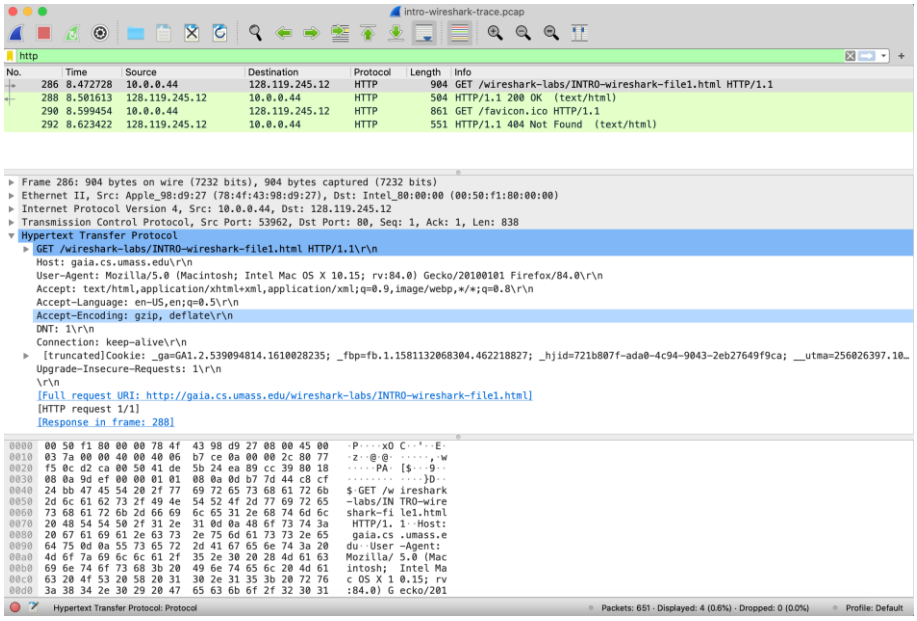
8. Gdy Wireshark jest uruchomiony, wprowadź adres URL:

<Podaje prowadzący>

W celu wyświetlenia strony przeglądarka połączy się z serwerem HTTP i wymieni dane protokołu HTTP w celu pobrania strony. Ramki Ethernet lub WiFi zawierające dane protokołu HTTP (jak również wszystkie inne ramki przechodzące przez interfejs Ethernet lub WiFi) zostaną przechwycone przez Wireshark.

9. Po wyświetleniu przez przeglądarkę strony, zatrzymaj przechwytywanie pakietów Wireshark wybierając *Stop* w oknie przechwytywania Wireshark. Główne okno programu Wireshark powinno teraz wyglądać podobnie jak na rysunku 3 i zawierać wszystkie pakiety wymieniane między komputerem a innymi urządzeniami sieciowymi. Dane protokołu HTTP wymieniane z serwerem *HTTP* są na tej liście. Niemniej, lista zawiera wiele innych typów pakietów, mimo że jedyną czynnością, która została wykonana, było pobranie strony internetowej. Najwyraźniej na komputerze działało wiele innych protokołów, których użytkownik nie widzi. Dlaczego tak jest?

10. Wpisz *http* (małymi literami – wszystkie nazwy protokołów w programie Wireshark są pisane małymi literami) w oknie specyfikacji filtra wyświetlania. Następnie naciśnij klawisz Enter. Spowoduje to wyświetlenie w oknie z listą pakietów tylko tych, które są związane z protokołem HTTP. Należy zauważyć, że w oknie pod listą pakietów można zobaczyć szczegółową zawartości komunikatu protokołu Hypertext Transfer Protocol, który należy do warstwy aplikacji. Te dane są przesyłane w segmencie TCP, który enkapsulowano w datagramie IPv4. Ostatecznie segment TCP jest transportowany w ramce protokołu Ethernet (rys. 4).



Rysunek 4: Szczegóły pakietu związanego z protokołem HTTP.

11. Ile czasu minęło od wysłania wiadomości HTTP GET do otrzymania odpowiedzi HTTP OK? (Domyślnie wartość kolumny czas w oknie z listą pakietów to czas w sekundach od rozpoczęcia śledzenia przez Wireshark).

12. Jaki jest adres IP serwera, który wysłał odpowiedz HTTP OK? Jaki jest adres IP komputera, który wysłał wiadomość HTTP GET?

13. Rozwiń informacje o wiadomości HTTP GET w oknie Wireshark. Jaki typ przeglądarki internetowej wysłał żądanie HTTP? Odpowiedź na to pytania, znajduje się w polu *User-Agent*.

14. Rozwiń informacje o protokole dla pakietu HTTP OK aby zobaczyć pola w segmencie TCP. Jaki jest numer portu docelowego? Odpowiedz na to pytanie to wartość pola Dest Port segmentu TCP.

4. Wymagania dotyczące sprawozdania

Sprawozdanie dokumentuje wykonanie zadań z punktu 3 (prócz zadania 4) za pomocą opisu, podpisanych screenów, odpowiedzi na pytania kontrolne i komentarzy.

Sprawozdanie należy oddać w e-learningu.