S I E C I K O M P U T E R O W E I

LABORATORIUM NR 8
Monitorowanie funkcjonowania protokołu TCP

Celem ćwiczenia jest poznanie podstawowej funkcjonalności programów oraz metod monitorowania funkcjonowania protokołów TCP/IP.

Ćwiczenie jest wykonywane przez każdego studenta indywidualnie a wyniki, według poniższej instrukcji, mają zastać zebrane w postaci jednego sprawozdania na grupę.

CZĘŚĆ I - nmap : Przebieg ćwiczenia:

W trakcie tej części ćwiczenia wykorzystywany będzie pakiet nmap. Na wstępie należy sprawdzić czy w systemie Ubuntu zainstalowany jest pakiet Wireshark. W przypadku jego braku, proszę zainstalować go za pomocą polecenia:
sudo apt-get install nmap

Pakiet nmap udostępnia podstawowe metody pozyskiwania informacji o sieciach i pojedynczych hostach z punktu widzenia ich funkcjonowania na warstwie transportowej.

Najczęściej stosowane metody skanowania:

- **skanowanie połączenie TCP** (ang. TCP connect scan) – polega na połączeniu z wybranym portem i przeprowadzeniu pełnego trójstronnego powitania (SYN, SYN/ACK i ACK). Jeżeli port nasłuchuje połączenie powiedzie się, w przeciwnym razie port nie jest dostępny.

- **skanowanie TCP SYN** (ang. half-open scanning) - do wybranego portu przesyłany jest pakiet SYN tak jak w przypadku prawdziwego połączenia i następuje oczekiwanie na odpowiedź. Jeśli port odpowie sygnałem SYN/ACK to oznacza, że port nasłuchuje natomiast odpowiedź RST/ACK oznacza zazwyczaj, że port nie nasłuchuje.

- **skanowanie TCP FIN** – polega na przesłaniu do wybranego portu pakietu FIN. Cel powinien odpowiedzieć pakietem RST dla wszystkich zamkniętych portów.

- **skanowanie TCP Xmas Tree** – polega na przesłaniu do wybranego portu pakietów FIN, URG i PUSH. Cel powinien odpowiedzieć pakietem RST dla wszystkich zamkniętych portów.

- **skanowanie TCP Null** – w tej metodzie wyłączone są wszystkie flagi. Cel powinien odpowiedzieć pakietem RST dla wszystkich zamkniętych portów.

- **skanowanie TCP ACK** – metoda sprawdzająca czy zapora ogniowa celu to tylko prosty filtr pakietów, dopuszczający jedynie nawiązane połączenia (połączenia z ustawionym bitem ACK), czy też może jest to zaawansowana zapora przeprowadzająca rozbudowane filtrowanie pakietów.

- **skanowanie UDP** – polega na przesłaniu pakietu UDP do wybranego portu. Jeśli wybrany port odpowie komunikatem "ICMP port unrechable", to oznacza że jest on zamknięty; w przeciwnym razie można wnioskować, że port jest otwarty lub firewall zablokował komunikację.

Typowe zastosowanie pakietu nmap jest przedstawione poniżej (wykorzystane adresy są adresami przykładowymi). Warto jednak zapoznać się z podręcznikiem systemowym pakietu by poznać jego pełne możliwości.

- rozszerzony ping (ang. ping sweeping)

a. Icmp ping: **nmap -sP 10.0.0.0/24**

b. tcp ping: **nmap -sP -PT80 10.0.0.0/24** gdzie 80 oznacza „pingowany" port.

- skanowanie portów (ang. port scanning)

a. TCP connect: **nmap -sT 10.0.0.1**

b. stealth scanning: **nmap -sS 10.0.0.1**

c. UDP scanning: **nmap -sU 10.0.0.1**

d. stealth FIN: **nmap -sF 10.0.0.1**

e. Xmas tree scanning: **nmap -sX 10.0.0.1**

f. Null scanning: **nmap -sN 10.0.0.1**

- wykrywanie systemu operacyjnego celu (ang. OS Fingerprinting)

nmap -sS -O 10.0.0.1

Zadanie 1. Monitorowanie hostów za pomocą nmap.

a. Należy określić jakie porty są otwarte na używanym komputerze i na komputerze sąsiada. W tym celu należy wykonać skanowanie tych dwóch hostów metodą *TCP connect* oraz *stealth*. W sprawozdaniu proszę umieścić otrzymane wyniki działania skanowania.

b. Czy wyniki z podpunktu a. różnią się między sobą dla własnego komputera i komputera sąsiada ? Na czym polega różnica pomiędzy skanowaniem *TCP connect* i *stealth* z punktu widzenia możliwości ich wykrycie przez cel ?

c. Spróbuj określić za pomocą nmap typ wykorzystywanego systemu operacyjnego na swoim komputerze i komputerze sąsiada. W sprawozdaniu proszę umieścić otrzymane wyniki działania odpowiedniego polecenia.

d. W jaki sposób (na podstawie jakich danych) nmap próbuje wykryć typ systemu operacyjnego celu ?

CZEŚĆ II – tcpdump : Przebieg ćwiczenia

Jest to jedno z najpopularniejszych i najbardziej natywnych, konsolowych narzędzi sieciowych w systemie Linux. Narzędzie to pozwala na przechwytywanie ruchu sieciowego według zadanych kryteriów. Program pozwala na „zrzucenie" ruchu sieciowego do pliku i

podgląd w zewnętrznej aplikacji.

Jedną z ważniejszych cech tego programu, są zaawansowane narzędzia do filtracji przechwytywanego ruchu sieciowego.

Składnia polecenia:

tcpdump [-deflnNOpqStvx] [-c count] [-F file][-i interface] [-r file] [-s snaplen][-T type] [-w file] [expression]

gdzie:

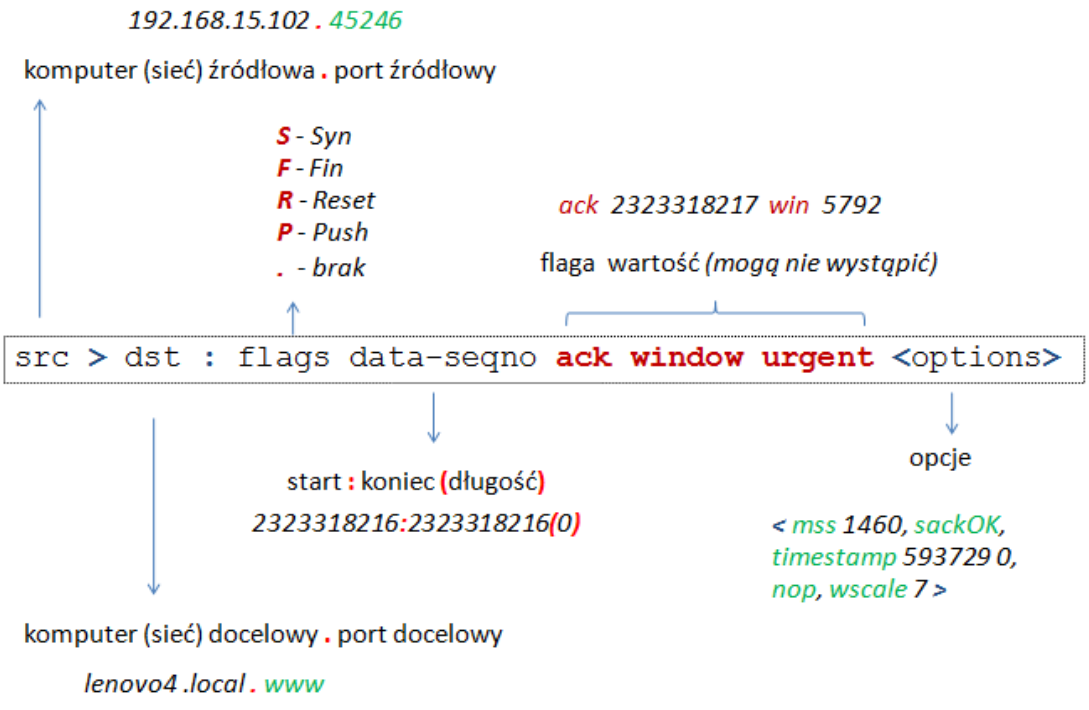
- i -interface Wymuszenie interfejsu, z którego program będzie zbierał pakiety
- l -wyłączenie buforowania pakietów (powodującego opóźnienia w stosunku do fizycznego odbioru pakietów)
- w file -wymuszenie zapisu wyników do określonego pliku (zamiast wysłania ich na standardowe wyjście)
- r file -pobranie wyników zapisanych w określonym pliku, proces odwrotny do flagi – w

–v | –vv | –vvv - wymuszenie trybów dokładności prezentacji pakietów
–t | –tt | –ttt | –tttt -wymuszenie trybów dokładności określenia czasu
–x | –X -wymuszenie prezentacji pakietów w postaci heksadecymalnej (–x) bądź ASCII (–X)
expression -określenie kryteriów filtracji pakietów

Przykładowo:
tcpdump –i eth0 src 192.168.1.1 and tcp dst port 22

Zarejestrowany ruch niesie w sobie informacje, których opis przedstawiony jest poniżej.

```
07:47:01.244771 IP 192.168.15.102.46913 > lenovo4.local.www :
S 600024415:600024415(0) win 5840
<mss 1460,sackOK,timestamp 183637 0,nop,wscale 7>
```



Zadanie 1. Przykład wykorzystania tcp do analizy metody skanowania.

a. Należy otworzyć dwa terminale. W pierwszym z nich będzie rejestrowana transmisja TCP generowana przez proces skanowania portów sąsiedniego komputera za pomocą programu nmap. Ruch sieciowy będzie zapisywany do pliku. Na drugim terminalu uruchomione ma być monitoring nmap. Należy zatem wydać następujące polecenia:

- Terminal 1:

```
sudo tcpdump -w ubuntu.txt -i eth0 -t host 192.168.1.1
```

gdzie:

- *ubuntu.txt* jest nazwą pliku, do którego zapisana będzie transmisja. Proszę dobrać dowolną nazwę. Plik zostanie domyślnie zapisany w katalogu domowym użytkownika.

- *eth0* to interfejs, na którym rejestrowany jest ruch. Proszę wstawić nazwę interfejsu podłączonego do Internetu.

- *192.168.1.1* jest adresem IP monitorowanego komputera. Proszę wstawić adres IP komputera sąsiada.

- Terminal 2:

```
nmap -sT -p 50-100 192.168.1.1
```

gdzie:

- *p* jest opcją ograniczającą skanowanie do zakresu portów od 50 do 100.

- *192.168.1.1* to jak poprzednio adres IP monitorowego komputera. Proszę wstawić adres IP komputera sąsiada.

b. Najpierw należy uruchomić polecenie na terminalu 1. Następnie uruchomić polecenie na terminalu 2. Gdzy zakończy się skanowanie portów, należy zakończyć rejestrację transmisji na terminalu 1 (za pomocą klawiszy Ctr-C).

c. Należy sprawdzić czy w katalogu domowym użytkownika został utworzony plik z zapisanym ruchem sieciowym.

UWAGA: Utworzony plik jest w formacie niepozwalającym na podejrzenie go w zwykłym edytorze tekstu. W celu zapisu ruchu w formacie tekstowym można uzyskać przekierowując wynik działania tcpdump do pliku, np. poleceniem:

sudo tcpdump -i eth0 -t host 192.168.1.1 > tekstowy.txt

Zadanie 2. Analiza ruchu

```
student@cloudlab:~$ sudo tcpdump -r ubuntu.txt -t host 192.168.1.1 and port 80
reading from file ubuntu.txt, link-type EN10MB (Ethernet)
IP iphone.lan.36639 > blinksys.lan.http: Flags [S], seq 2125767395, win 29200, options [mss 1460,sackOK,TS val 15904868 ecr 0,nop,wscale 7], length 0
IP blinksys.lan.http > iphone.lan.36639: Flags [S.], seq 2469426555, ack 2125767396, win 5840, options [mss 1460,nop,nop,sackOK,nop,wscale 0], length 0
IP iphone.lan.36639 > blinksys.lan.http: Flags [.], ack 1, win 229, length 0
IP iphone.lan.36639 > blinksys.lan.http: Flags [R.], seq 1, ack 1, win 229, length 0
IP iphone.lan.36642 > blinksys.lan.http: Flags [S], seq 3155566267, win 29200, options [mss 1460,sackOK,TS val 15904869 ecr 0,nop,wscale 7], length 0
IP blinksys.lan.http > iphone.lan.36642: Flags [S.], seq 2467678301, ack 3155566268, win 5840, options [mss 1460,nop,nop,sackOK,nop,wscale 0], length 0
IP iphone.lan.36642 > blinksys.lan.http: Flags [.], ack 1, win 229, length 0
IP iphone.lan.36642 > blinksys.lan.http: Flags [R.], seq 1, ack 1, win 229, length 0
student@cloudlab:~$
```

a. Zapisany ruch można odczytać za pomocą programu tcpdump i poddać go dalszej analizie. Przykładowo, poniżej pokazano konwersację TCP podczas monitorowania portu 80 (otwartego) i 81 (zamkniętego). Proszę samodzielnie wykonać takie filtrowanie zapisanego w podpunkcie b ruchu. Jednocześnie proszę wybrać dwa porty o różnych stanach. W sprawozdaniu proszę umieścić wykorzystane polecenia i wynik ich działania.

```
student@cloudlab:~$ sudo tcpdump -r ubuntu.txt -t host 192.168.1.1 and port 81
reading from file ubuntu.txt, link-type EN10MB (Ethernet)
IP iphone.lan.36954 > blinksys.lan.81: Flags [S], seq 2551773004, win 29200, options [mss 1460,sackOK,TS val 15904871 ecr 0,nop,wscale 7], length 0
IP blinksys.lan.81 > iphone.lan.36954: Flags [R.], seq 0, ack 2551773005, win 0, length 0
student@cloudlab:~$
```

b. Na podstawie zadania 1 proszę samodzielnie dokonać rejestracji skanowania TCP Xmas tree. Otrzymany ruch przeanalizować w taki sposób by wyjaśnić na czym polega ten rodzaj skanowania. W sprawozdaniu proszę umieścić wykorzystane polecenia, wyniki ich działania oraz wyjaśnienie działania algorytmu skanowania w oparciu od odfiltrowane fragmenty ruchu.

CZĘŚĆ III – Wireshark : Przebieg ćwiczenia

W trakcie ćwiczenia wykorzystywany będzie pakiet Wireshark. Za jego pomocą rejestrowany będzie fragment transmisji danych (ang. packet trace). Każdy trace ruchu sieciowego zawiera znacznik czasu (ang. timestamp) dla każdego zarejestrowanego pakietu oraz wszystkie bity, które składają się na strukturę pakietu, na wszystkich warstwach (od nagłówków najniższych warstw po dane najwyższych warstw. Wireshark dostarcza szeregu narzędzi przeznaczonych do filtrowania ruchu sieciowego raz jego analizy. Podstawowe narzędzie tego typu zostaną użyte podczas realizacji ćwiczenia.

Na wstępie należy sprawdzić czy w systemie Ubuntu zainstalowany jest pakiet Wireshark. W przypadku jego braku, proszę zainstalować go za pomocą polecenia:

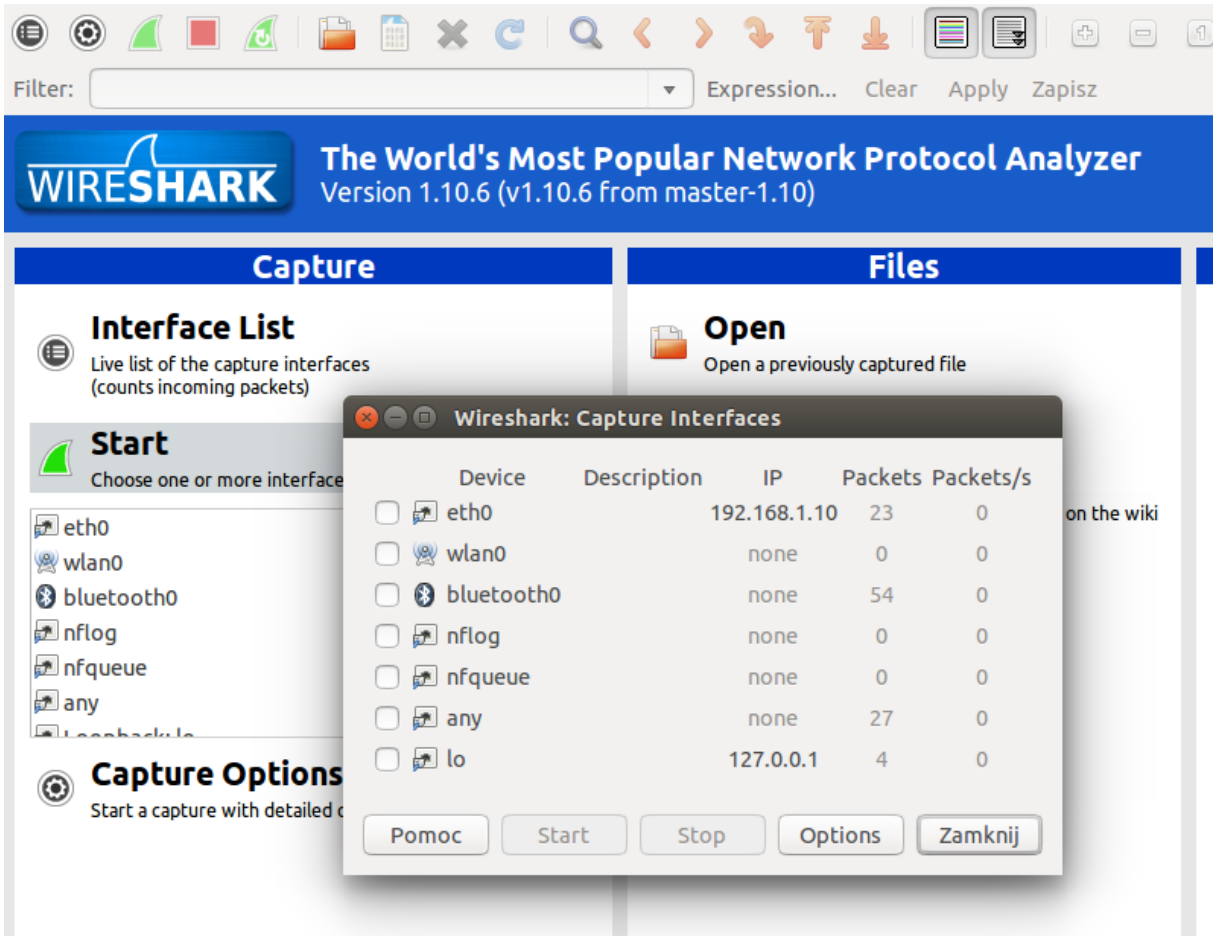
sudo apt-get install wireshark

Ponieważ Wireshark domyślnie dopuszcza rejestrację transmisji z uprawnieniami root-a a dalszą analizę zarejestrowanego ruchu sieciowego przez dowolnego użytkownika (szczegóły opcje i zasady konfiguracji można znaleźć pod adresem http://wiki.wireshark.org/CaptureSetup/CapturePrivileges lub w pliku dokumentacji file:///usr/share/doc/wireshark-common/README.Debian) to należy na wstępie zezwolić użytkownikowi *student* na dostęp do interfejsów i nagrywanie ruchu sieciowego (ang. traces).

W tym celu należy wydać kolejno polecenia jak na rysunku poniżej.

```
student@cloudlab:~$ sudo addgroup -system wireshark
Dodawanie grupy "wireshark" (GID 126)...
Gotowe.
student@cloudlab:~$ sudo chown root:wireshark /usr/bin/dumpcap
student@cloudlab:~$ sudo setcap cap_net_raw,cap_net_admin=eip /usr/bin/dumpcap
student@cloudlab:~$ sudo usermod -a -G wireshark student
student@cloudlab:~$
```

Po wykonaniu powyższych poleceń dostępne powinny być wszystkie aktywne interfejsy sieciowe. Aby to sprawdzić, należy uruchomić Wireshark i na stronie startowej sprawdzić czy wyświetlone są interfejsy ethx (tj. eth0, eth1 … - pola „Start” oraz po kliknięciu - „Interfejs list”). Przykład oczekiwanego wyniku ilustruje rysunek poniżej.

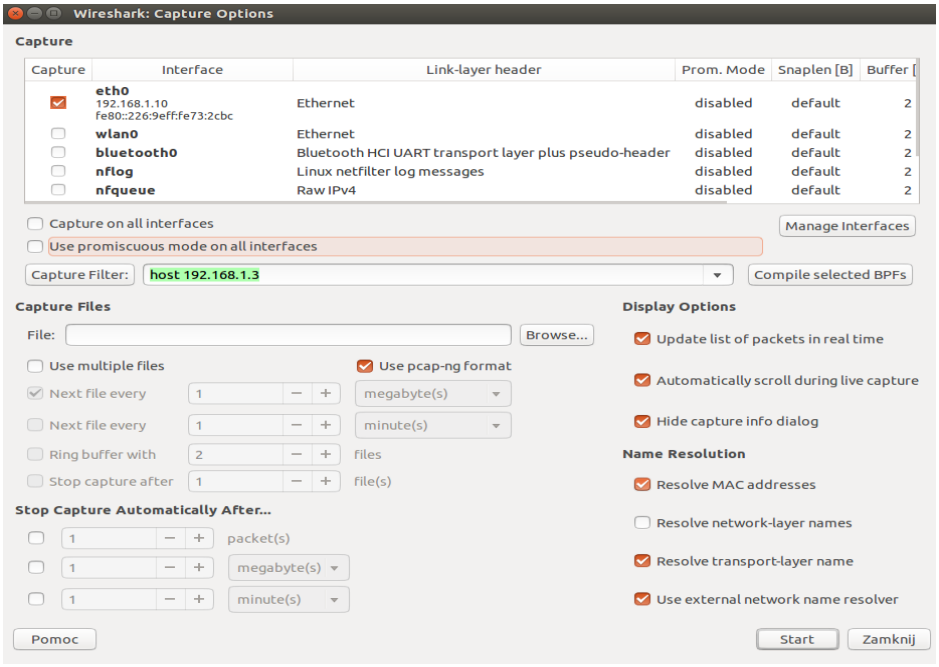


W zajęć wykorzystywana będzie karta przyłączona do Internetu.

Zadanie 1. Rejestracja transmisji danych za pomocą Wireshark

a. W Należy wybrać z meny programu Wireshark : *Capture* > *Interfaces* a następnie, w nowo otwartym oknie zaznaczyć używaną kartę sieciową. Następnie należy wybrać „Options”.

Otworzy się nowe okno, którego przykładowy wygląd przedstawiony na rysunku powyżej.

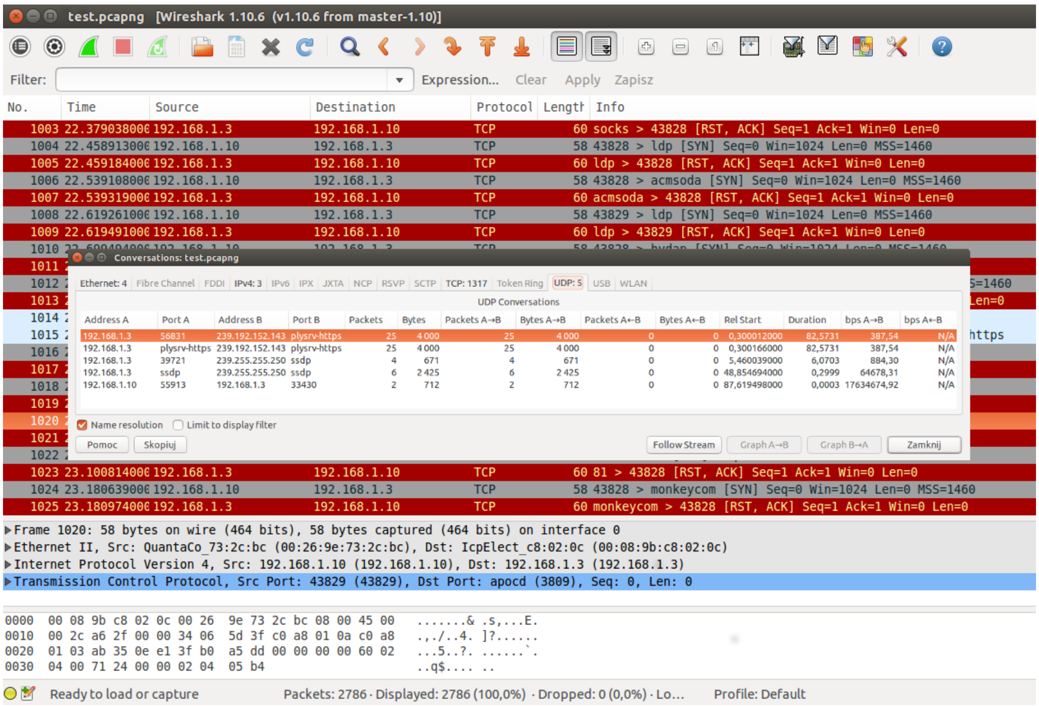


Wszystkie ustawienia powinny być jak na rysunku z wyjątkiem pola „Capture Filter”, w którym należy adres IP zamienić na adres IP komputera sąsiada.

b. Należy otworzyć terminal a w nim uruchomić program nmap z opcją wykrywania systemu operacyjnego.

c. Należy uruchomić rejestrację ruchu w programie Wireshark a następnie nmap w terminalu. Po zakończeniu działania programu nmap należy zatrzymać rejestrację transmisji w Wireshark. Następnie należy zapisać wynik działania Wireshark do pliku w katalogu domowym użytkownika dzięki temu będzie można go otworzyć w dowolnej chwili i poddać analizie.

d. Przykład zarejestrowanego ruchu i okna *Statistics>Conversations* przedstawione są poniżej. Biorąc pod uwagę typy i parametry wykorzystanych protokołów, analizując każdą z konwersacji z pomocą narzędzi filtrowania ruchu, należy w sprawozdaniu wyjaśnić w jaki sposób nmap rozpoznaje system operacyjny. Proszę w sprawozdaniu wyjaśnienie to zilustrować właściwymi zrzutami ekranu z Wiresharka.



!!

1. Sprawozdanie należy nazwać "Cw9-nazwisko" gdzie nazwisko, oznacza nazwisko wykonującego sprawozdanie i wgrać do katalogu na Dropbox (katalog Sprawozdania, podkatalog odpowiadający terminowi zajęć).

2. Na wstępie sprawozdania proszę podać imiona i nazwiska wszystkich członków grupy ćwiczeniowej, która uczestniczyła w wykonaniu ćwiczenia.

3. Format sprawozdania: PDF. !

!!