T: Testy pasywne i aktywne sieci komputerowych.

Podział pomiarów i testów sieci komputerowych:
- testy parametrów fizycznych (okablowanie strukturalne),
- testy i pomiary pasywne (obserwacja funkcjonowania sieci),
- testy i pomiary aktywne (wykorzystanie dodatkowych danych testowych).

Wykonując testy pasywne administrator zbiera informacje dotyczące funkcjonowania sieci poprzez monitorowanie ruchu pakietów sieciowych między urządzeniami. Do testów pasywnych wykorzystywane są programy nazywane snifferami.

W testach pasywnych do analizy funkcjonowania sieci komputerowych można wykorzystać oprogramowanie typu sniffer. Sniffer to program komputerowy służący do przechwytywania i analizowania pakietów sieciowych.

Zadanie1:

Odszukaj w serwisie internetowym Wikipedii informacje na temat programów typu sniffery.

Sniffer – program komputerowy lub urządzenie, którego zadaniem jest przechwytywanie i ewentualnie analizowanie danych przepływających w sieci.

Wspólną cechą wielu takich analizatorów jest przełączenie karty sieciowej w tryb mieszany (ang. promiscuous), w którym urządzenie odbiera wszystkie ramki z sieci, także te nieadresowane bezpośrednio do niego; sniffery mogą być uruchamiane także na routerze lub na komputerze będącym jedną ze stron komunikacji sieciowej – i w tych przypadkach tryb promiscuous nie jest konieczny.

Sniffer stanowi nieodzowne narzędzie diagnostyczne większości administratorów sieci, zwłaszcza podczas diagnostyki problemów z niezawodnością lub wydajnością połączeń. Może być również stosowany do monitorowania aktywności sieciowej osób trzecich, co jest w większości przypadków niezgodne z prawem. W celu ochrony przed takimi atakami, niektóre protokoły komunikacyjne stosują mechanizmy kryptograficzne.

Najczęściej używanymi programami tego typu są: tcpdump, sniffit, ettercap, dsniff, wireshark (dawniej ethereal) oraz snort. Ten ostatni pełni także funkcję sieciowego systemu wykrywania intruzów. Istnieją także liczne bardziej specjalizowane narzędzia tego typu (np. komercyjne systemy przeznaczone na potrzeby organów ścigania i służb wywiadowczych).

Do najpopularniejszych programów do analizy ruchu sieciowego należą:
- tcpdump,
- wireshark (https://www.wireshark.org/),
- snort.

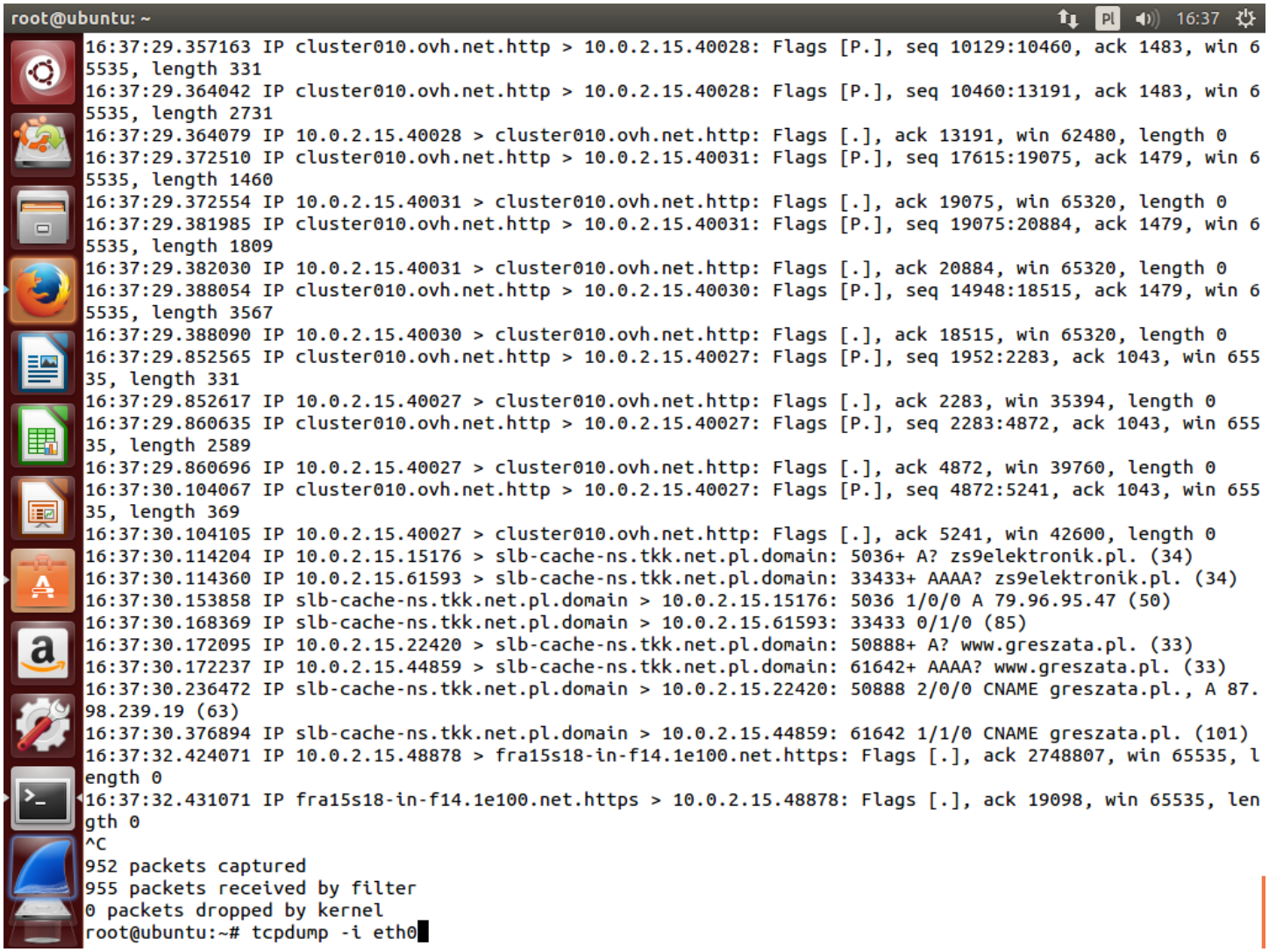
Zadanie2:

Przeprowadź diagnozę ruchu sieciowego w systemie Linux za pomocą programu `tcpdump`.

Jakie dane zostały przechwycone przez komputer stacjonarny?

```
ifconfig eth0 promisc
ifconfig eth0 -promisc
tcpdump -i enp0s3
tcpdump src or dst host 149.156.137.250
```

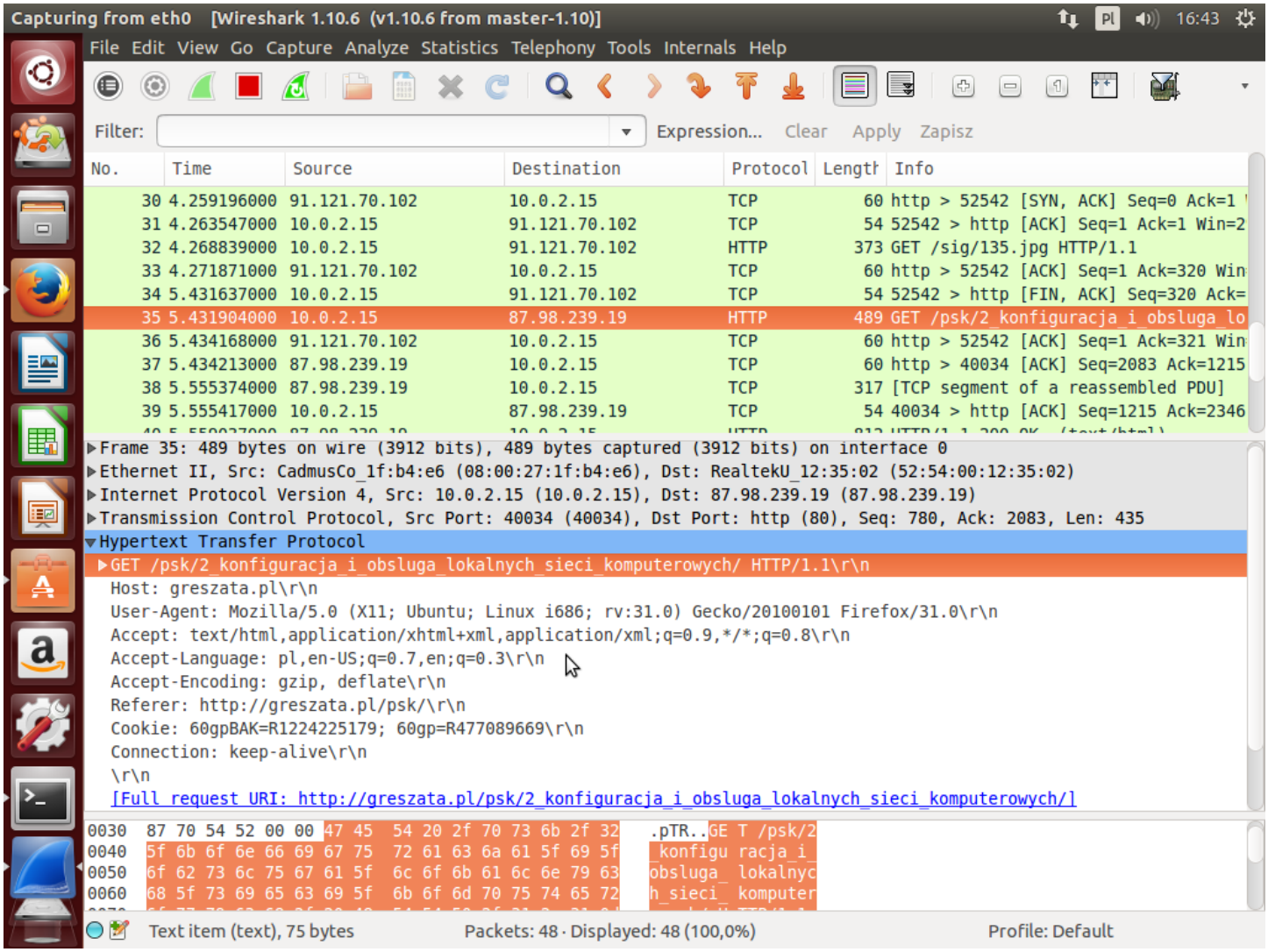
Zrzut ekranu prezentujący działanie programu `tcpdump`:



Zadanie3:

Odszukaj w serwisie internetowym dobreprogramy.pl informacje na temat programu Wireshark.

Wireshark jest jednym z popularniejszych programów wykorzystywanych do analizy ruchu sieciowego. W celu uniknięcia problemów z uprawnieniami do zarządzania kartami sieciowymi, program należy uruchomić z poziomu administratora systemu:



W celu wykorzystania programu Wireshark do analizy sieci wykonaj następujące czynności:

- uruchom program,
- wybierz polecenie Interfaces z menu Capture i wskaż kartę sieciową, z której będą przechwytywane dane,
- uruchom nasłuchiwanie ruchu sieciowego klikając przycisk Start,
- można wymusić ruch sieciowy poprzez połączenie z komputerem skanującym z innej stacji sieciowej dowolnym klientem sieciowym,
- po zarejestrowaniu danych sieciowych wyłączyć skanowanie klikając przycisk Stop z menu Capture.

Po zarejestrowaniu danych należy dokonać analizy przechwyconych pakietów. Do tego celu pomocne może być polecenie Follow TCP Stream dostępne w menu Analyze. Wcześniej należy zaznaczyć pakiet, dla którego chcemy przeprowadzić analizę.

Zadanie4:

Przeprowadź diagnozę ruchu sieciowego za pomocą programu `wireshark`. Ogranicz nasłuchiwanie programu do usługi ftp i przeprowadź nasłuch połączenia do serwera (TCP – ftp [SYN], Analyze/Follow TCP Stream).

```
/etc/init.d/vsftpd status
netstat -ant | grep :21
ftp admin3tib2@hostname
```

Do przeprowadzania monitoringu ruchu sieciowego w systemach Windows Serwer można wykorzystać oprogramowanie Microsoft Internet and Security Acceleration Server.

Wykonując testy aktywne administrator wprowadza do sieci dodatkowe dane, które ułatwiają monitorowanie ruchu pakietów sieciowych między urządzeniami. Pomiary aktywne przeprowadza się w celu sprawdzenia jakości usług sieciowych (QoS, ang. Quality of Service).

Testy aktywne pozwalają określić jakość usług sieciowych (Quality of Service, QoS).
Podczas testów aktywnych dokonuje się pomiarów następujących parametrów:
- dostępność usługi,
- opóźnienie w jednym kierunku (One Way Delay Minimum, OWD),
- zmienność opóźnienia przekazu pakietów (IP Packet Delay Variation, IPDV),
- opóźnienie pakietów w pętli (Round Trip Delay, RTD),
- straty pakietów (One Way Loss, OWL),
- poziom strat pakietów (IP Packet Loss Ratio, IPLR).

Parametry diagnozowane podczas pomiarów aktywnych:
- przepustowość sieci – możliwość przesyłania danych między źródłem a celem,
- opóźnienie przesyłanych danych – np. minimalne opóźnienie, średnie opóźnienie, sprawdzane w jednym kierunku lub w obu kierunkach,
- straty pakietów danych – np. ilość zagubionych danych przesyłanych w sieci.

Zadanie5:

> Odszukaj w serwisie internetowym Wikipedii informacje na temat protokołu ICMP oraz programów ping i traceroute. Zwróć uwagę na różnicę w działaniu programów tracert i mtr.

ICMP (ang. Internet Control Message Protocol, internetowy protokół komunikatów kontrolnych) – jest to protokół warstwy sieciowej modelu OSI, wykorzystywany w diagnostyce sieci oraz trasowaniu.

Programy przeznaczone do testów aktywnych:
- ping,
- tracert/traceroute.

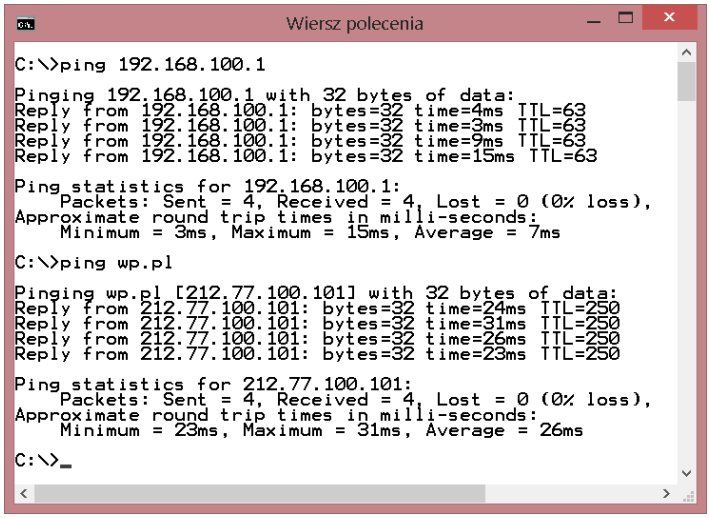
Ping – polecenie służące do diagnozowania połączeń sieciowych. Pozwala na sprawdzenie, czy istnieje połączenie pomiędzy hostami, zmierzenienie liczby zgubionych pakietów oraz opóźnień w ich transmisji, zwanych lagami. Opóźnienie to czas wymagany, aby wysłany pakiet danych dotarł do odbiorcy, a odpowiedź zwrotna trafiła z powrotem do nadawcy. Ping korzysta z protokołu ICMP, wysyła pakiety ICMP Echo Request i odbiera ICMP Echo Reply.

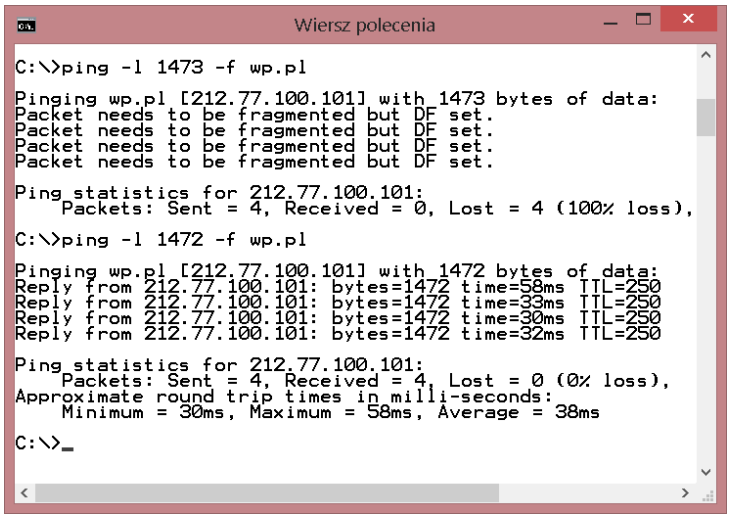
Zadanie6:

> Przeprowadź diagnozę ruchu sieciowego za pomocą programu `ping`.

```
ping localhost
ping -n 2 s27st01
ping -t wp.pl
ping -l 1500 -f wp.pl
```

Jakie dane zostały przekazane przez program ping?





Traceroute - program służący do badania trasy pakietów w sieci IP. Działanie traceroute opiera się na protokołach komunikacyjnych UDP oraz ICMP.

Zadanie7:

Przeprowadź diagnozę ruchu sieciowego za pomocą programu `traceroute`.

`tracert hostname`

`traceroute wp.pl`

`tracepath wp.pl`

`mtr wp.pl` (https://ubuntix.pl/jak-korzysta-z-komendy-linux-mtr-my-traceroute)

`gnome-nettool`