

Technologie sieciowe

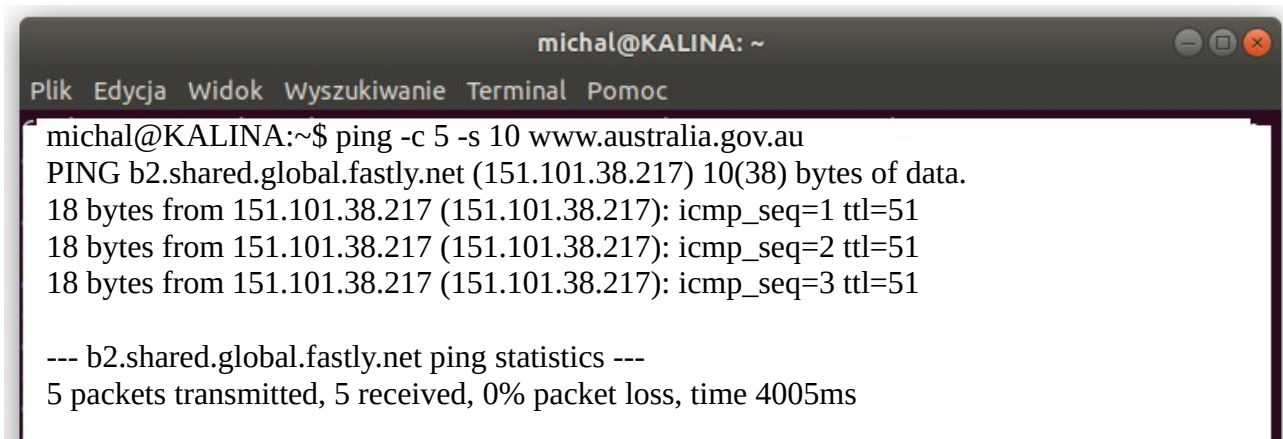
Lista 1

Michał Kalina
250088

Ping

Ping umożliwia wysyłanie i odbieranie danych sieciowych z innego komputera w sieci. Często jest używany do testowania na najbardziej podstawowym poziomie, czy inny system jest osiągalny przez sieć, a jeśli tak, to ile czasu zajmuje wymiana danych. Przykład:

```
ping -c 3 -s 10 www.australia.gov.au //wysyłanie 3 razy o rozmiarze 18 bytes
```

A terminal window titled 'michal@KALINA: ~' with a menu bar containing 'Plik', 'Edycja', 'Widok', 'Wyszukiwanie', 'Terminal', and 'Pomoc'. The terminal shows the command 'ping -c 5 -s 10 www.australia.gov.au' and its output: 'PING b2.shared.global.fastly.net (151.101.38.217) 10(38) bytes of data. 18 bytes from 151.101.38.217 (151.101.38.217): icmp_seq=1 ttl=51 18 bytes from 151.101.38.217 (151.101.38.217): icmp_seq=2 ttl=51 18 bytes from 151.101.38.217 (151.101.38.217): icmp_seq=3 ttl=51 --- b2.shared.global.fastly.net ping statistics --- 5 packets transmitted, 5 received, 0% packet loss, time 4005ms'.

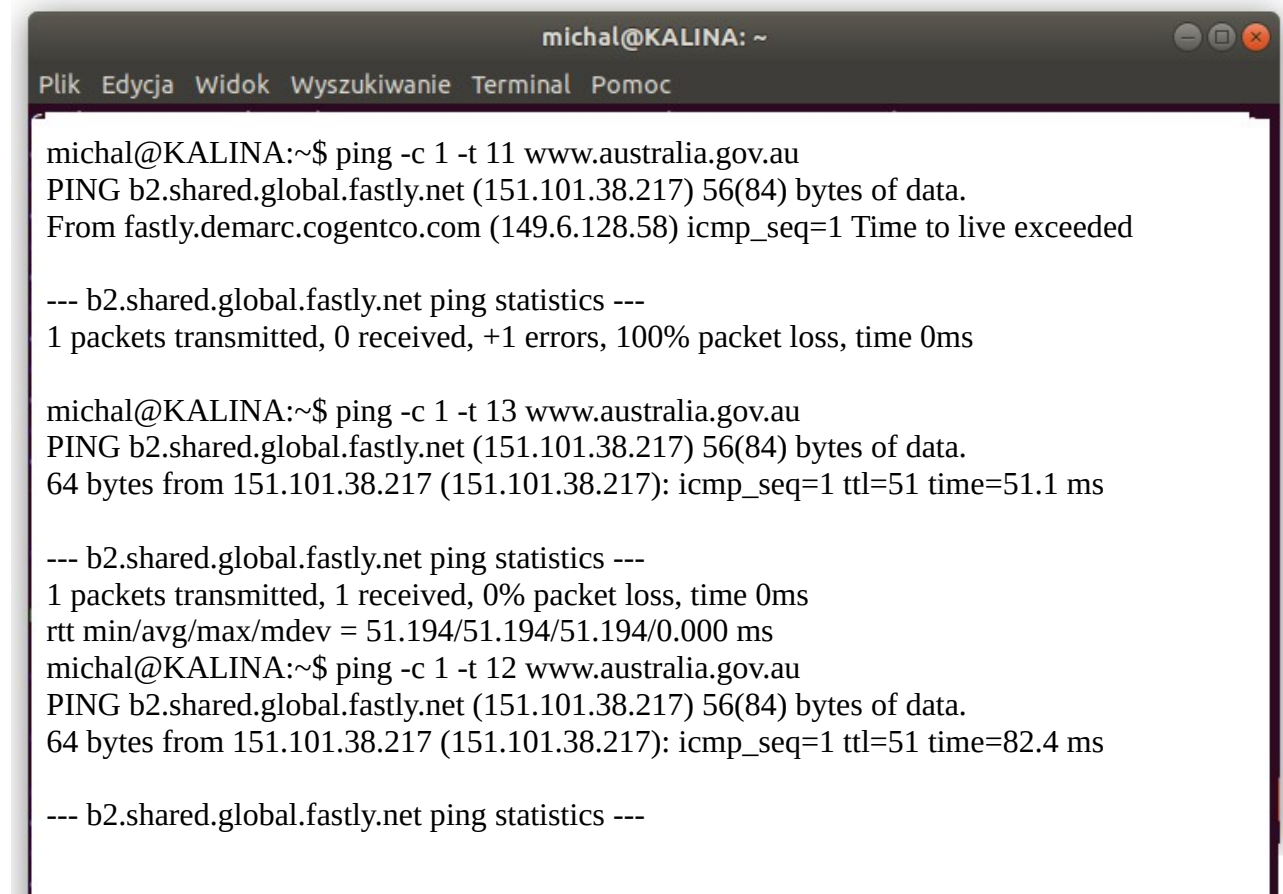
```
michal@KALINA:~$ ping -c 5 -s 10 www.australia.gov.au
PING b2.shared.global.fastly.net (151.101.38.217) 10(38) bytes of data.
18 bytes from 151.101.38.217 (151.101.38.217): icmp_seq=1 ttl=51
18 bytes from 151.101.38.217 (151.101.38.217): icmp_seq=2 ttl=51
18 bytes from 151.101.38.217 (151.101.38.217): icmp_seq=3 ttl=51

--- b2.shared.global.fastly.net ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
```

Ilość skoków można określić za pomocą ttl.
 $2^x = \text{ttl}$, czyli jeśli $\text{ttl}=51$, $64-51=13$, bo $2^6=64$

- i pozwala na wysyłanie w ramach jakiegoś czasu
- t pozwala określić ilość hops'ów
- w wait for response

Aby sprawdzić drogę powrotną to daję flagę *t* i jeśli dojdzie to zmniejszam, jak nie dojdzie to zwiększam i tak mogę oszacować ilość skoków w drodze powrotnej.

A terminal window titled 'michal@KALINA: ~' with a menu bar containing 'Plik', 'Edycja', 'Widok', 'Wyszukiwanie', 'Terminal', and 'Pomoc'. The terminal shows two ping commands. The first is 'ping -c 1 -t 11 www.australia.gov.au' which results in '1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms'. The second is 'ping -c 1 -t 13 www.australia.gov.au' which results in '64 bytes from 151.101.38.217 (151.101.38.217): icmp_seq=1 ttl=51 time=51.1 ms'.

```
michal@KALINA:~$ ping -c 1 -t 11 www.australia.gov.au
PING b2.shared.global.fastly.net (151.101.38.217) 56(84) bytes of data.
From fastly.demarc.cogentco.com (149.6.128.58) icmp_seq=1 Time to live exceeded

--- b2.shared.global.fastly.net ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms

michal@KALINA:~$ ping -c 1 -t 13 www.australia.gov.au
PING b2.shared.global.fastly.net (151.101.38.217) 56(84) bytes of data.
64 bytes from 151.101.38.217 (151.101.38.217): icmp_seq=1 ttl=51 time=51.1 ms

--- b2.shared.global.fastly.net ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 51.194/51.194/51.194/0.000 ms
michal@KALINA:~$ ping -c 1 -t 12 www.australia.gov.au
PING b2.shared.global.fastly.net (151.101.38.217) 56(84) bytes of data.
64 bytes from 151.101.38.217 (151.101.38.217): icmp_seq=1 ttl=51 time=82.4 ms

--- b2.shared.global.fastly.net ping statistics ---
```

1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 82.453/82.453/82.453/0.000 ms

Przy wysłaniu pakietu o różnych wielkościach można uzyskać inną liczbę skoków. Ja jednak nie znalazłem takiego przypadku.



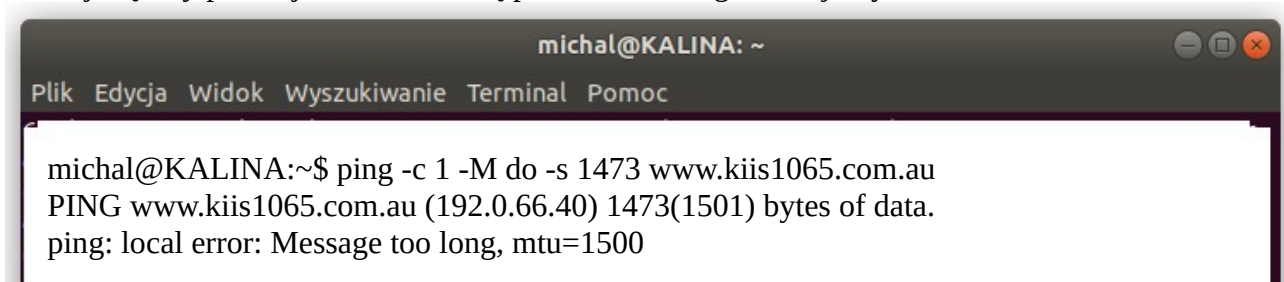
```
michal@KALINA: ~  
Plik Edycja Widok Wyszukiwanie Terminal Pomoc  
michal@KALINA:~$ ping -s 65600 www.australia.gov.au  
Error: packet size 65600 is too large. Maximum is 65507
```

Fragmentacja

Do fragmentacji korzystam z komendy *-M*

MTU (*Maximum Transmission Unit*) to maksymalna długość pakietu jaki może zostać przesłany przez sieć. Może ona wynosić do 64KiB

Największy pakiet jaki udało mi się przesłać bez fragmentacji wynosił 1472



```
michal@KALINA: ~  
Plik Edycja Widok Wyszukiwanie Terminal Pomoc  
michal@KALINA:~$ ping -c 1 -M do -s 1473 www.kiis1065.com.au  
PING www.kiis1065.com.au (192.0.66.40) 1473(1501) bytes of data.  
ping: local error: Message too long, mtu=1500
```

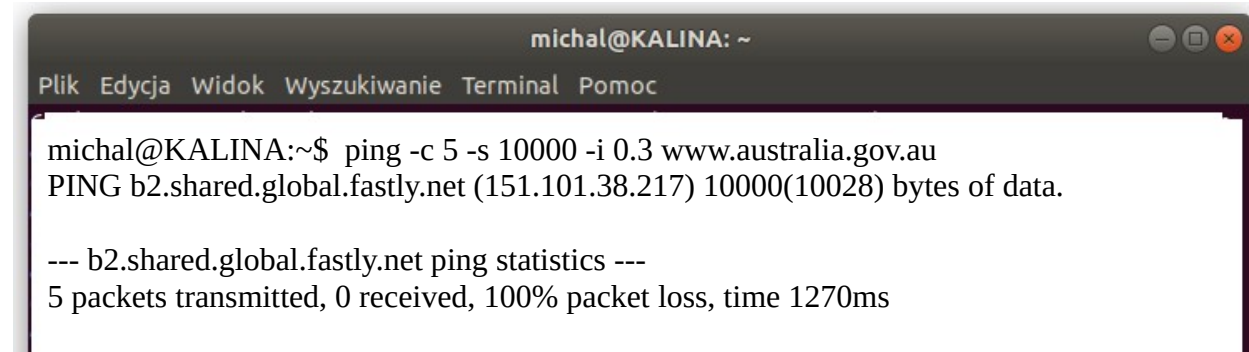
Do każdego pakietu musimy dodać 28 bajtów nagłówka, to oznacza że na moim sprzęcie limit ustawiony jest na 1500 bajtów.

Na przykładzie witryny www.kiis1065.com.au, średni czas:

- 80ms dla 100 bajtów z fragmentacją
- 40ms dla 100 bajtów bez fragmentacji
- 55ms dla 1000 bajtów z fragmentacją
- 80ms dla 1000 bajtów bez fragmentacji

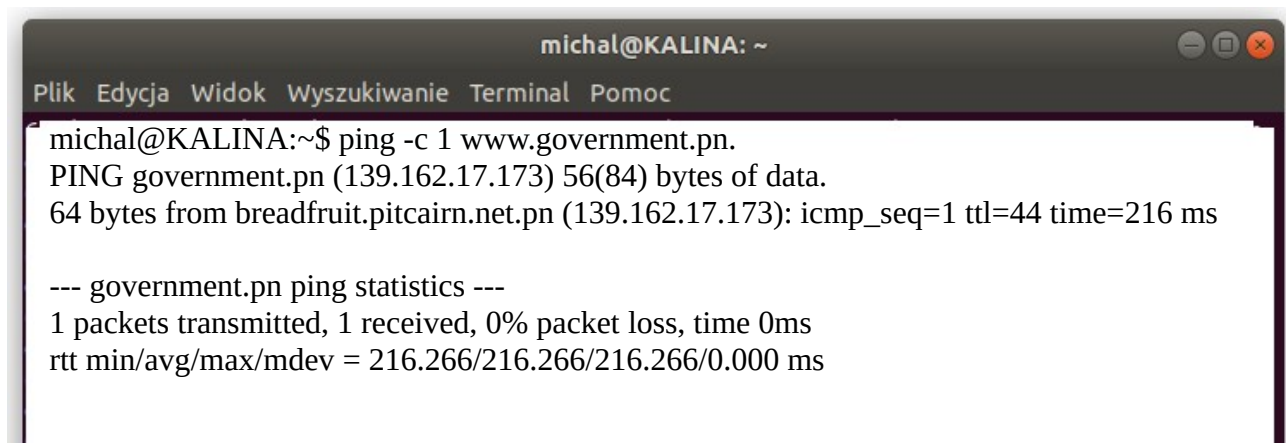
Ilość skoków do nas jest taka sama jak liczba skoków od nas.

Przy dużych pakietach mogą pojawić się problemy jak np.:



```
michal@KALINA: ~  
Plik Edycja Widok Wyszukiwanie Terminal Pomoc  
michal@KALINA:~$ ping -c 5 -s 10000 -i 0.3 www.australia.gov.au  
PING b2.shared.global.fastly.net (151.101.38.217) 10000(10028) bytes of data.  
  
--- b2.shared.global.fastly.net ping statistics ---  
5 packets transmitted, 0 received, 100% packet loss, time 1270ms
```

Najbardziej „oddalona” znaleziona witryna to www.government.pn. Posiada 20 węzłów.

A screenshot of a terminal window titled "michal@KALINA: ~". The window has a menu bar with "Plik", "Edycja", "Widok", "Wyszukiwanie", "Terminal", and "Pomoc". The terminal output shows a ping command being executed: "michal@KALINA:~\$ ping -c 1 www.government.pn." followed by "PING government.pn (139.162.17.173) 56(84) bytes of data." and "64 bytes from breadfruit.pitcairn.net.pn (139.162.17.173): icmp_seq=1 ttl=44 time=216 ms". Below this, it shows "--- government.pn ping statistics ---", "1 packets transmitted, 1 received, 0% packet loss, time 0ms", and "rtt min/avg/max/mdev = 216.266/216.266/216.266/0.000 ms".

```
michal@KALINA: ~
Plik Edycja Widok Wyszukiwanie Terminal Pomoc
michal@KALINA:~$ ping -c 1 www.government.pn.
PING government.pn (139.162.17.173) 56(84) bytes of data.
64 bytes from breadfruit.pitcairn.net.pn (139.162.17.173): icmp_seq=1 ttl=44 time=216 ms

--- government.pn ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 216.266/216.266/216.266/0.000 ms
```

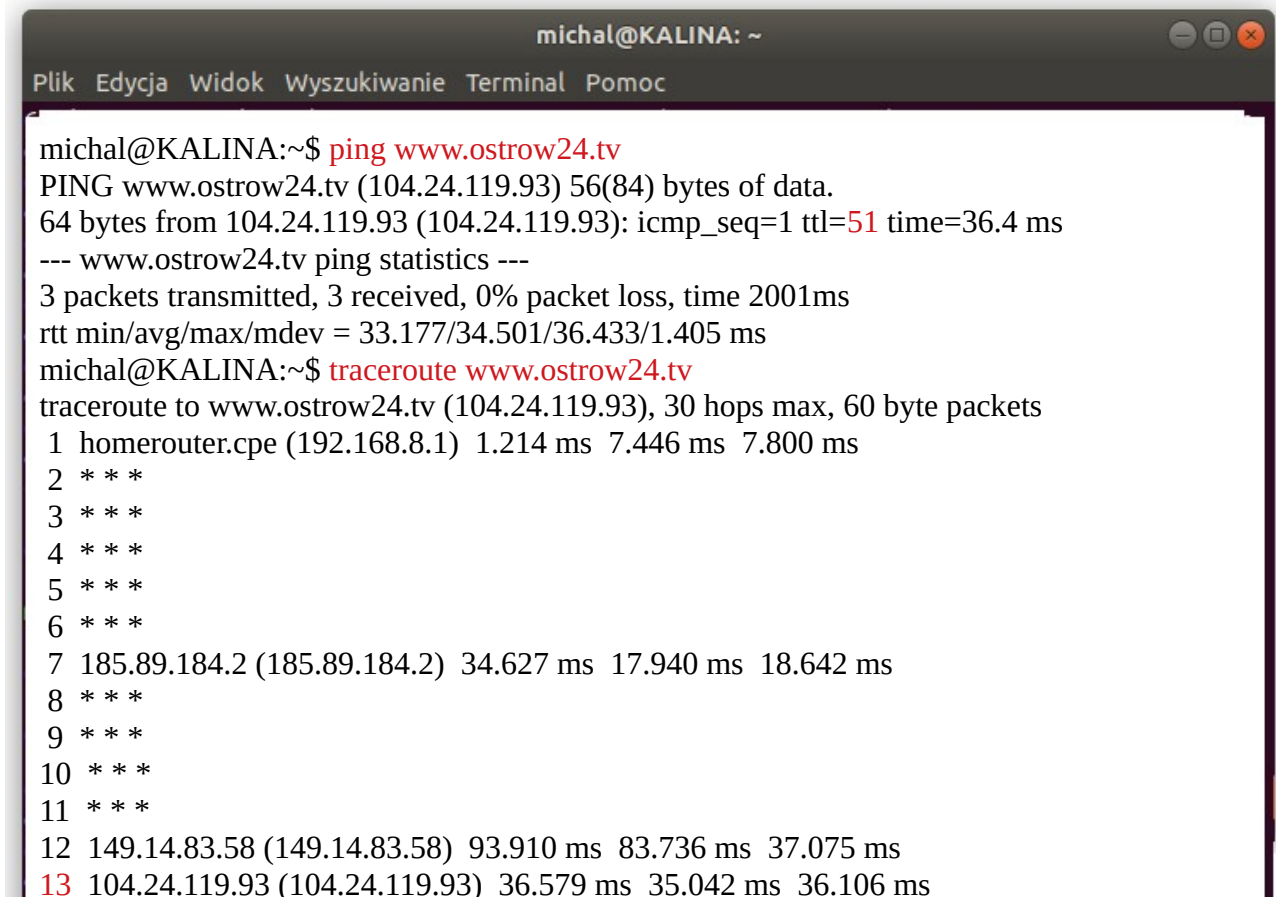
W „Cloud Computing” będzie więcej skoków. Jest to grupa użytkowników sieci działających w ramach jednego sprzętu. Jeśli pakiet wpadnie do takiej sieci to może w niej być wysyłany między sobą. Można podejrzewać że trafiliśmy na sieć wirtualną jeśli nasza liczba skoków jest nadzwyczaj duża, np. ttl=130

Uwagi:

- Sieć zmienia się dynamicznie, przez co pomiary robione jednego dnia mogą się znacząco różnić dnia następnego.
- Położenie geograficzne, nie ma większego wpływu na ilość skoków. Przykładami są chociażby domeny: ostrow24.tv (strona lokalnej gazety mojego miasta) oraz australia.gov.au (rządowa strona FA), obydwie wymagają 13 skoków.
- Część stron jak: australia.gov.au, nie odpowiada gdy podamy dużą ilość danych
- Fragmentacja nie ma wpływu na liczbę skoków ale ma wpływ na czas

Traceroute

Traceroute służy do sprawdzania przez jakie rozgłośnie przechodzi moje zapytanie do podanego adresu. np. (próba połączenia do rządowej strony FA przez laptop połączony z telefonem). N(reduce the number of requests) i w(increase the timeout)

A screenshot of a terminal window titled 'michal@KALINA: ~'. The window has a menu bar with 'Plik', 'Edycja', 'Widok', 'Wyszukiwanie', 'Terminal', and 'Pomoc'. The terminal shows the following commands and output:

```
michal@KALINA:~$ ping www.ostrow24.tv
PING www.ostrow24.tv (104.24.119.93) 56(84) bytes of data.
64 bytes from 104.24.119.93 (104.24.119.93): icmp_seq=1 ttl=51 time=36.4 ms
--- www.ostrow24.tv ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 33.177/34.501/36.433/1.405 ms
michal@KALINA:~$ traceroute www.ostrow24.tv
traceroute to www.ostrow24.tv (104.24.119.93), 30 hops max, 60 byte packets
 1  homerouter.cpe (192.168.8.1)  1.214 ms  7.446 ms  7.800 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  185.89.184.2 (185.89.184.2)  34.627 ms  17.940 ms  18.642 ms
 8  * * *
 9  * * *
10  * * *
11  * * *
12  149.14.83.58 (149.14.83.58)  93.910 ms  83.736 ms  37.075 ms
13  104.24.119.93 (104.24.119.93)  36.579 ms  35.042 ms  36.106 ms
```

Na powyższym przykładzie widać że dane z programu ping pokrywają się z traceroute.
* to brak odpowiedzi, traceroute domyślnie wysyła trzy pakiety do każdego urządzenia na trasie.

traceroute pl.wikipedia.org 11 //wielkość pakietu = 11

Tagi:

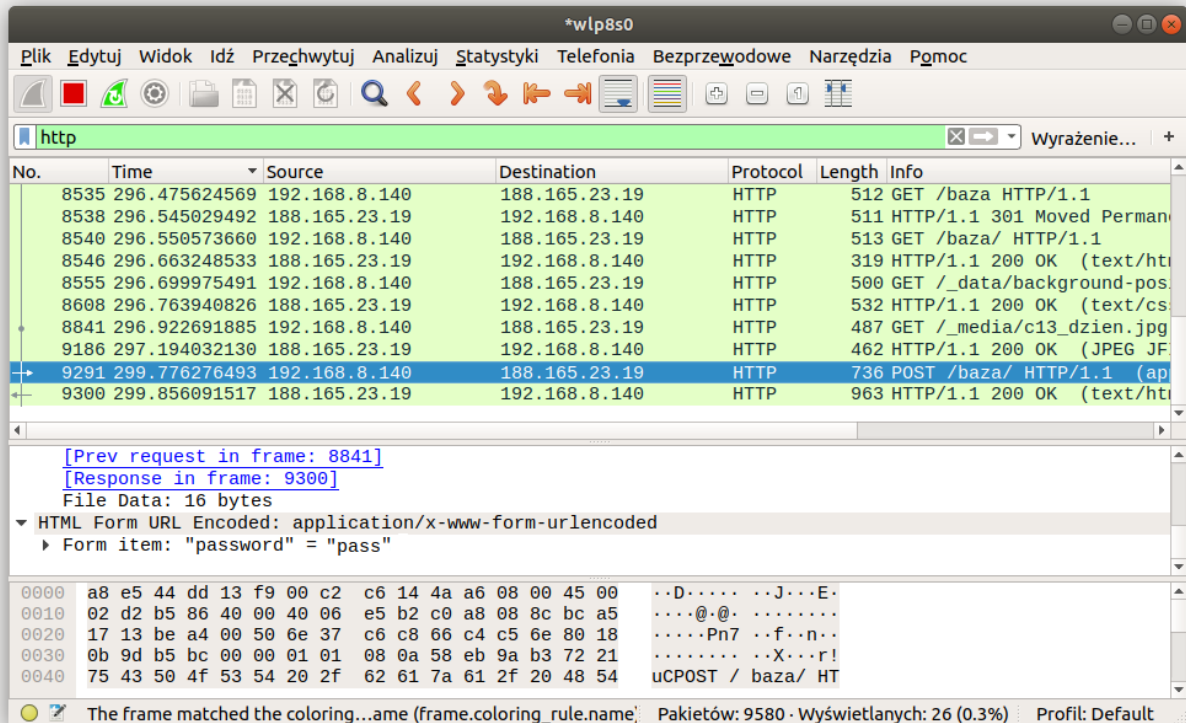
- -n zakrywa nazwy
- -m maksymalna liczba skoków
- -F zapobiega fragmentacji pakietu

Program może pomóc gdy sieć nie działa poprawnie tzn. jeśli nie możemy się połączyć to możemy sprawdzić „drogę” sygnału i określić w którym miejscu następuje przerwanie. Jeśli podczas przesyłania danych wystąpi jakakolwiek czkawka lub przerwa, trasa automatycznie pokaże, gdzie wzdłuż łańcucha naprawdę wystąpił problem.

WireShark

Analiza ruchów w realnej sieci i ocena jej prawidłowego funkcjonowania. Wszystkie ruchy można zapisać do pliku. Na przykład jeśli komuś internet nie działa wystarczająco szybko, to instalujemy Whiles shark'a, włączmy nasłuchiwanie, całość zapisujemy do pliku a następnie możemy wyniki przeanalizować w domu.

W przypadku poniżej za pomocą filtra wpisałem http, przez co widzę tylko elementy wykorzystujące protokół http. Przy witrynach nieodpowiednio zabezpieczonych mogą także zobaczyć dane logowania. Jak w przypadku poniżej(hasło: pass):



W celu wykrycia potencjalnie niebezpiecznego zdarzenia w sieci, należy odnaleźć pakiet należący do podejrzanej sesji. Jeśli liczba analizowanych pakietów jest duża, może sprawić to problem. Istnieje także funkcja *Podążaj za adresem TCP*, umożliwiającą rekonstrukcję całej sesji TCP i wyświetlenie wszystkich danych przesyłanych w aplikacji między hostem źródłowym (czerwony) a docelowym (niebieski):

