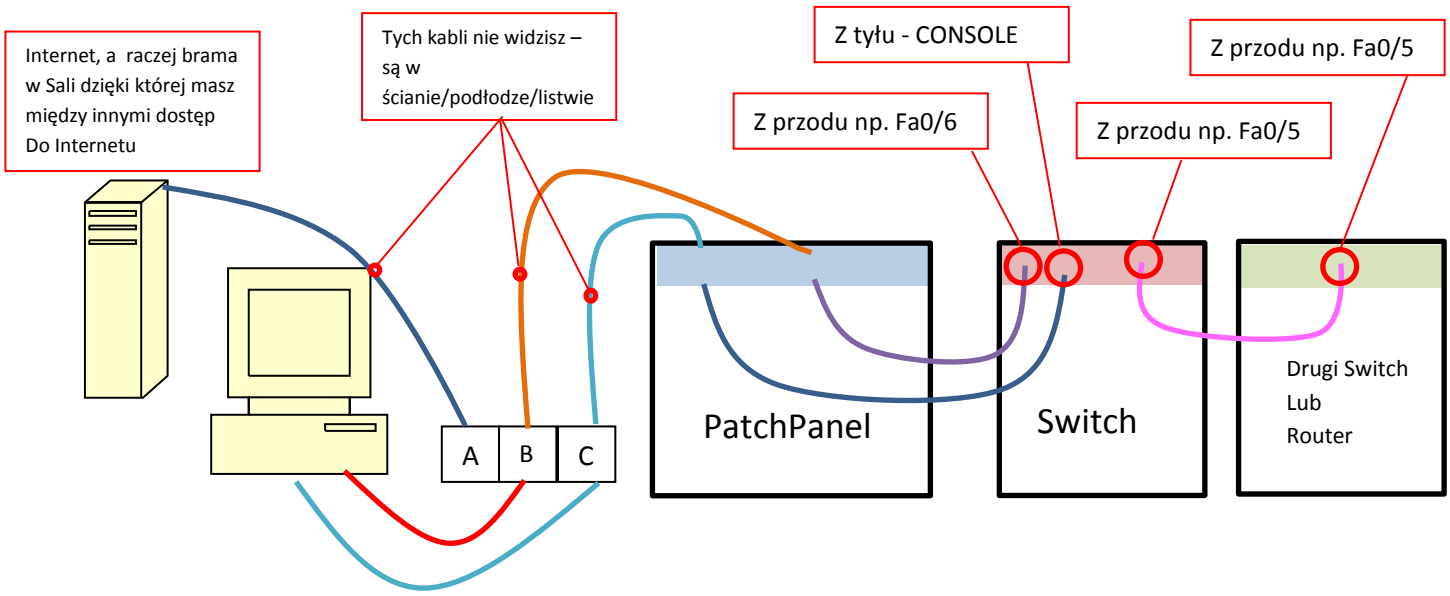
CISCO Skrypt Teleinformatyka WEKA v0.5 maj 2014 lukaszjok ☺ PWR ☺

Też się uczę – przed użyciem skonsultuj się z książką lub Internetami, jeśli zauważysz błąd zgłoś to.
Opracowywane na podstawie książek i strony CISCO oraz ogólnodostępnych materiałów w Internecie



Bezpośrednio z komputera wychodzą dwa kable (w rzeczywistości oczywiście mgą mieć inne kolory xD, tu opisuję zgodnie z moim rysunkiem) podłączamy je do tego gniazdka na biurku – to po prostu coś w rodzaju gniazdka natynkowego na wyjścia RJ-45 coś jakby gniazdko prądowe w mieszkaniu ☺ po prostu żeby było możliwe przedłużenie tego kabla.

Czerwony - skrętka – jeżeli jest podłączona do portu A(najbardziej z lewej) to podłączamy się do Internetu, czyli to tak samo jakbyś się wpiął do rutera w swoim mieszkaniu/akademiku ☺

Pomarańczowy kabel który jest doprowadzony do portu B jest z kolei dalej pociągnięty do Patch Panelu - element pasywny – czyli nie mający zbędnej elektroniki – też jest stosowany jak to poprzednie gniazdko tyle, że większe. Równie dobrze zamiast stosowania dwóch kabli – pomarańczowego i fioletowego można by użyć jednego bezpośrednio z portu B do Switcha albo jeszcze lepiej ☺ - z jednostki komputera do switcha, jednak to bez sensu – ciągnąć 5 metrów kabla po całej Sali. Jak widać Patch Panel i to gniazdko na biurku porządkują jedynie okablowanie

Fioletowy kabel jak wspomniałem jest niejako przedłużeniem kabla pomarańczowego tudzież czerwonego, przy pomocy którego łączymy komputer ze switchem w sieć LAN dzięki temu będziemy mieli później także możliwość konfigurowania switcha przez sieć/Internet np. telnet jednak, żeby było to możliwe trzeba to sobie skonfigurować wcześniej przy użyciu kabla konsolowego.

Niebieski – podpinamy go do portu C(bo port B mamy zajęty, ale można by je stosować wymienię) i analogicznie z portu C wychodzi jego przedłużenie do Patch Panelu i z niego następnie znowu przedłużamy do wejścia konsolowego w switchu.
Tak samo jak poprzednio można by bezpośrednio podpiąć kabel z komputera(jednostki) do wejścia konsolowego w switchu ale ile to znowu byłoby metrów przewodu.

Różowym dołączasz do swojego switcha drugi switch lub router w zależności od polecenia – porty na przednich panelach urządzeń – luknij jakich przewodów kiedy się używa z przeplotem czy bez.

(Zielona czcionka wskazuje w jakim trybie działa polecenie)

Kiedy połączysz się z ze switchem lub routerem jesteś w trybie zwykłego użytkownika (User Exec Mode) zbyt wiele tu nie zrobisz, licha statystyka sieci, nic konkretnego. Musisz przejść do trybu uprzywilejowanego (Privileged Exec Mode) coś jak admin w Windowsie czy root w Linuksie

Przydatne skróty klawiszowe:
Tab - kończy jednoznaczne polecenie
Ctrl+R - ponownie wyświetla linię
Ctrl+Z - wychodzi z dowolnego trybu konfiguracji do trybu uprzywilejowanego
Ctrl+N lub strzałka w górę - poprzednie polecenie
Ctrl+P lub strzałka w dół - następne polecenie
Ctrl+Shift+6 - przerywa w trakcie wykonywania bieżące polecenie np. ping lub traceroute
Ctrl+C - przerywa polecenie i opuszcza tryb konfiguracyjny
Ctrl+A - przenosi na początek linii
Ctrl+E - przenosi na koniec linii
Ctrl+D - kasuje bieżący znak (zamiast przycisku Delete)

Podstawowa konfiguracja

No [jakaś komenda] – odwołuję wskazaną komendę, np. **Switch(config)#no hostname** – usuwa nazwę urządzenia

Router>? - wyświetleni dostępnych komend
Router> enable – przejście do trybu uprzywilejowanego (EXEC)
Router# show flash – wypisanie co jest na pamięci flash, można podejrzeć czy jest plik cvan.dat
Router# delete vlan.dat - kasuje plik vlan.dat
Router# reload - przeładowuje ustawienia, ponownie uruchamia przełącznik
Router# show version – informacje o nazwie/wersji system ; pamięciach: DRAM, NVRAM, FLASH

Router# clock set [czas] [data] – ustawienie zegaru np. **Router# clock set 11:23:00 20 March 2014**
Router# Configure terminal lub **config t** – przejście do trybu konfiguracji
Router(config)# Hostname [nazwa urządzenie] – nadaje urządzeniu nazwę
Router(config)# no ip domain-lookup zabezpieczenie przed niepożądanymi zapytaniami DNS
Router(config)# banner motd # -ustawienie wiadomości powitalnej. Pamiętaj zakończyć ją znakiem #
Router# configure terminal - przejście do trybu konfiguracji
Router(config)# enable password noweHaslo1 – ustawienie hasła do trybu EXEC, czyli zapyta Cię o nie po wydaniu polecenia **enable** jednak nie jest ono w żaden sposób szyfrowane i można je łatwo odczytać z pliku
Router(config)# enable secret noweHaslo2 - ustawienie hasła do trybu EXEC, tym razem już szyfrowane
Router(config)# security password min-length 10 – minimalne długość hasła 10 znaków
Router(config)# username admin privilege 15 secret noweHasło – tworzy bazę danych użytkowników lokalnych (tu: tworzy admina o przywilejach 15(najwiekszych) z szyfrowanym haslem)
Router(config)# service password-encryption – powoduje zaszyfrowanie haseł zapisanych tekstem jawnym
Router(config)# ip domain-name ccna-lab.com –stworzenie domeny routera
Router(config)# ip default-gateway xxx.xxx.xxx.xxx - ustawia bramę domyślna

---

Konfiguracja interfejsu konsoli

Router(config)# line con 0 (lub inaczej **Router(config)# line console 0**)– uruchamia tryb (Line-Configuration) umożliwiający konfigurację interfejsu konsolowego, w tym przykładzie o numerze 0
Router(config-line)# password noweHaslo ustala hasło dla trybu konsolowego
Router(config)# exec-timeout 5 0 - wyrzuca użytkownika z trybu EXEC po pięciu minutach bezczynności
Router(config-line)# login ta opcja powoduje, że łącząc się przez konsolę woła o podanie hasła, jak nie podasz tego polecenia nie połączysz się w przyszłości nią
Router(config-line)# end - powrót trybu uprzywilejowanego (to samo zrobisz dając CTRL+Z)
Router(config)#

Konfiguracja połączenia telnet i ssh – zdalny dostęp

Aby móc zalogować się na router lub przełącznik korzystając telnet, należy konfigurować hasło dla wirtualnych terminali urządzenia. Bez nadania hasła usługa telnet nie będzie osiągalna

Router(config)# line vty 0 4 – uruchamia tryb (Line-Configuration) umożliwiający konfigurację interfejsów wirtualnych, w tym przykładzie o numerach od 0 do 4
Router(config-line)# password noweHaslo ustala hasło dla tych interfejsów
Router(config-line)# login ta opcja powoduje, że łącząc się przez telnet woła o podanie hasła, jak nie podasz tego polecenia nie połączysz się w przyszłości przez telnet
Router(config)# exec-timeout 5 0 - wyrzuca użytkownika z trybu EXEC po pięciu minutach bezczynności
Router(config-line)# transport input ssh – akceptacja połączeń ssh blokuje TELNET
Router(config-line)# transport input telnet ssh – akceptacja połączeń TELNET i SSH
Router(config-line)# login local - umożliwia linii VTY korzystanie z lokalnej bazy użytkowników
Router(config-line)# exit - powrót do poprzedniego menu
Router(config)# crypto key generate rsa modulus 1024– (UWAGA!!! Na switchu inaczej, patrz niżej)generuje klucz RSA o długości 1024 bitów
Switch(config)# crypto key generate rsa [ENTER] wpisujesz teraz → 1024 [ENTER]
Router(config)# login block-for 30 attempts 2 within 120 - blokada logowania przez 30 sekund jeśli nastąpiły 2 nieudane próby w czasie 120s

---

Konfiguracja dowolnego interfejsu sieciowego

Router# configure terminal – przejście do trybu konfiguracji
Router(config)# **interface [nazwa interfejsu]** , np**. interface F0/5 –** wskazuje którym interfejsem się zajmujesz
Router(config)# **interface vlan1 –** konfiguracja interfejsu vlan1 albo inna nazwa SVI
Router(config-if)# **ip address 192.168.0.1 255.255.255.0** - nadanie adresu ip maski
Router(config-if)# **io shutdown** lub **no shut** – włącza ten interfejs
Router(config-if)# **description** [jakiś tekst] – opisuje słownie interfejs/komentarz
Router(config-if)# clock rate 128000 - ustawia taktowanie zegara na wszystkich interfejsach DCE
Router(config-if)# **Exit** – wyjście z danego trybu do poprzedniego

---

Podgląd/kasowanie ustawień

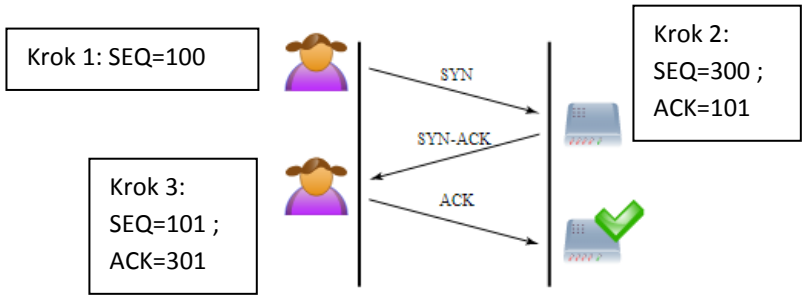
Router# show login – informacje o logowaniach
Router# show running-config – pokazuje aktualną konfigurację urządzenia
Router# show startup-config - pokazuje startową konfigurację urządzenia
Router# show ip interface brief – wyświetla krótkie podsumowanie informacji o adresie IP i jego stanie – up/down
Router# show interfaces – szczegółowe informacje o wszystkich interfejsów
Router# show interface g0/1 - - pokazuje informacje o danym interfejsie
Router# show mac address-table - wyświetla tablicę adresów MAC
Router# clear mac address-table dynamic – czyści tablicę adresów MAC
Router# show ip arp – wyświetla wpisy ARP
Router# show ip route – wyświetla tablice routingu
Router# show cdp neighbors detail - pokazuje device ID i inne info o sąsiednich urządzeniach
Router# copy running-config startup-config – zapisanie bieżącej konfiguracji jako konfigurację startową do pamięci NVRAM– dostępna po restarcie
Router# copy start tftp – kopiowanie konfiguracji startup-config na tftp
Router# copy tftp: startup-config – kopiowanie konfiguracji startup-config z tftp
Router# erase startup-config – wykasowanie konfiguracji startowej

Three-way-Handshake

Three Way Handshake polega na tym, że protokół TCP inicjuje połączenie, wysyła pakiet synchronizujący, serwer odsyła potwierdzenie, host wysyła potwierdzenie, że otrzymał portwierdzenie.

Wygląda to mniej więcej tak:

- *cześć tu Łukasz chcę nawiązać połączenie (TCP SYN)*
- serwer odpowiada: *spoko, pogadajmy (TCP SYN ACK)*
- host odsyła potwierdzenie: *dzięki, że się zgodziłeś (ACK)*



W pierwszym kroku host chce nawiązać połączenie wysyła do serwera numer sekwencyjny **SEQ** o wartości początkowej **100.**

W kroku drugim kroku serwer go odbiera i wysyła potwierdzenie w postaci flagi **ACK**, której wartość to powiększona o **+1** wartość SEQ hosta. W tym samym w tym samym kroku serwer wysyła swój **SEQ=300**.

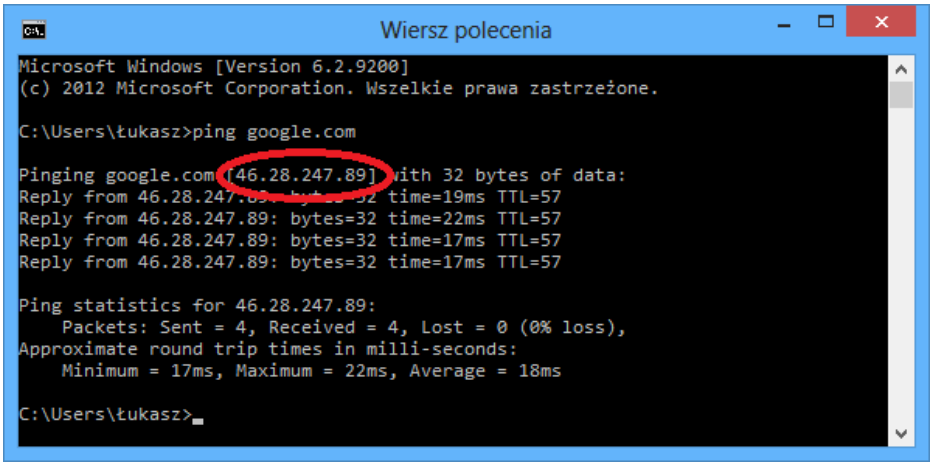
W kroku trzecim teraz host potwierdza numer sekwencyjny serwera wysyłając mu potwierdzenie – flaga **ACK,** której wartość to powiększona o **+1** czyli **301.**

Połączenie nawiązane!

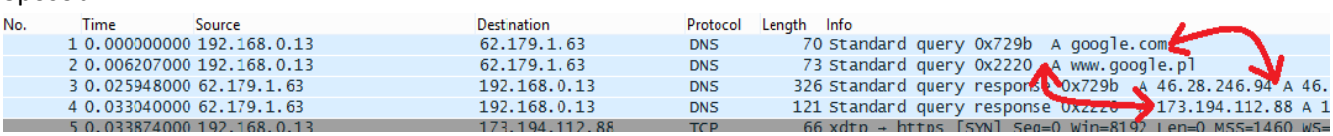
Proces ten możesz zaobserwować w programie Wireshark:

1. Uruchom przechwytywanie pakietów na odpowiednim interfejsie
2. W przeglądarce wejdź na dowolną stronę internetową, np. google.com
3. Zakończ przechwytywanie pakietów w Wireskark
4. Ustal adres IP strony na którą wszedłeś w poprzednim kroku:

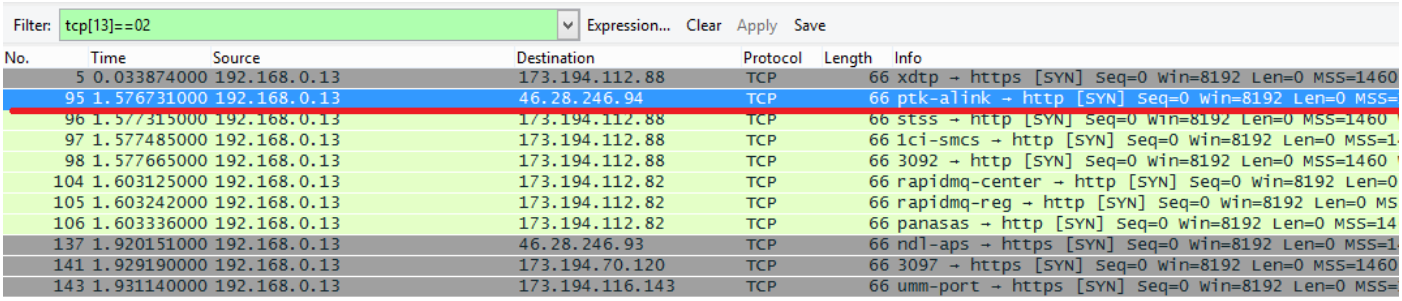
Sposób1:



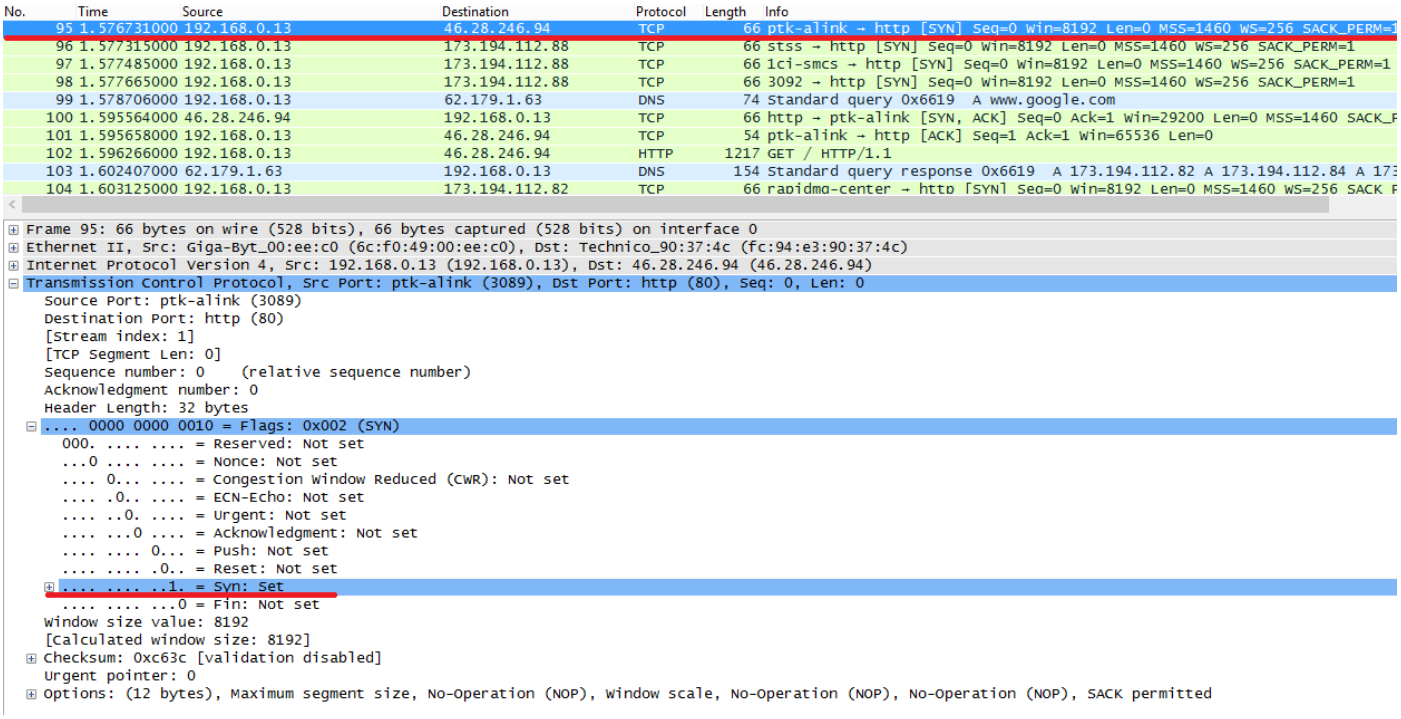
Sposób2:



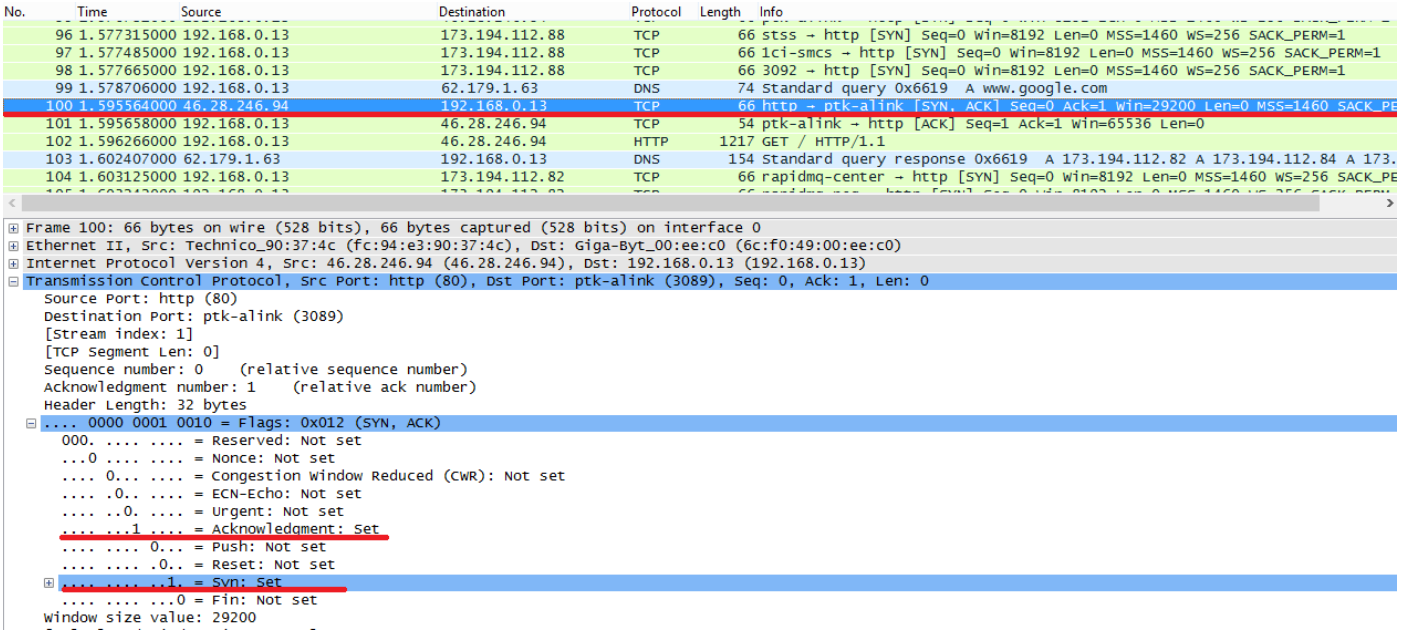
5. W Wireshark odszukaj pierwszą z trzech ramek Handshake. Możesz to zrobić na „czuja” – w wierszu ten ramki w kolumnie „Info” będzie widniała flaga **[SYN].** Możesz zastosować odpowiedni filtr **tcp[13]==02** wpisujesz go w pole „filter”. Wybierasz wiersz z adresem IP strony na którą wcześniej wchodziłeś(będzie on w kolumnie destination):



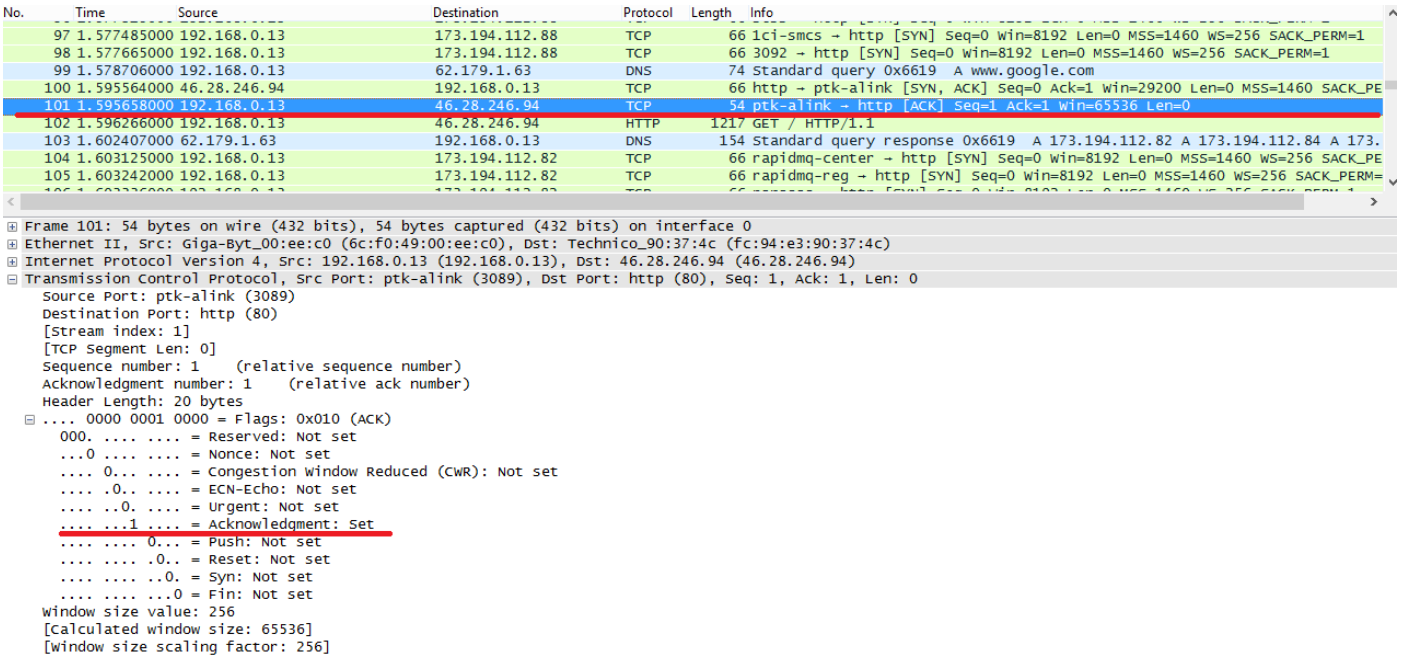
Aby przejść do kolejnej ramki tego samego handhake, kliknij na interesującą nas ramkę lub zapamiętaj jej numer porządkowy (tu: 95), następnie wykasuj filtr i wciśnij **[ENTER]**.



Do kolejnej ramki w, gąszczu pozostałych, program „przeskoczy” automatycznie jeżeli wciśniesz skrót: **Ctrl+.**
(kontrol plus kropka xD)



OK, jeszcze raz i mamy 3 etap handshake:



```
No.  Time          Source          Destination     Protocol Length Info
  97 1.577485000 192.168.0.13    173.194.112.88  TCP        66 1ci-smcs → http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  98 1.577665000 192.168.0.13    173.194.112.88  TCP        66 3092 → http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  99 1.578706000 192.168.0.13    62.179.1.63     DNS        74 Standard query 0x6619  A www.google.com
 100 1.595564000 46.28.246.94    192.168.0.13    TCP        66 http → ptk-alink [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PE
 101 1.595658000 192.168.0.13    46.28.246.94    TCP        54 ptk-alink → http [ACK] Seq=1 Ack=1 Win=65536 Len=0
 102 1.596266000 192.168.0.13    46.28.246.94    HTTP     1217 GET / HTTP/1.1
 103 1.602407000 62.179.1.63     192.168.0.13    DNS       154 Standard query response 0x6619  A 173.194.112.82 A 173.194.112.84 A 173.
 104 1.603125000 192.168.0.13    173.194.112.82  TCP        66 rapidmq-center → http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PE
 105 1.603242000 192.168.0.13    173.194.112.82  TCP        66 rapidmq-reg → http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=
```

```
⊞ Frame 101: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
⊞ Ethernet II, Src: Giga-Byt_00:ee:c0 (6c:f0:49:00:ee:c0), Dst: Technico_90:37:4c (fc:94:e3:90:37:4c)
⊞ Internet Protocol Version 4, Src: 192.168.0.13 (192.168.0.13), Dst: 46.28.246.94 (46.28.246.94)
⊟ Transmission Control Protocol, Src Port: ptk-alink (3089), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0
    Source Port: ptk-alink (3089)
    Destination Port: http (80)
    [Stream index: 1]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    Header Length: 20 bytes
  ⊟ .... 0000 0001 0000 = Flags: 0x010 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
    Window size value: 256
    [Calculated window size: 65536]
    [Window size scaling factor: 256]
```

Inne filtry:

- SYN packet from Clients: **tcp[13]==02**
- SYN_ACK packets from Server: **tcp[13]==12**
- ACK 3-way handshake: **tcp.seq==1 && tcp.ack==1 && tcp.len==0 && tcp.window_size_scalefactor ge 0**