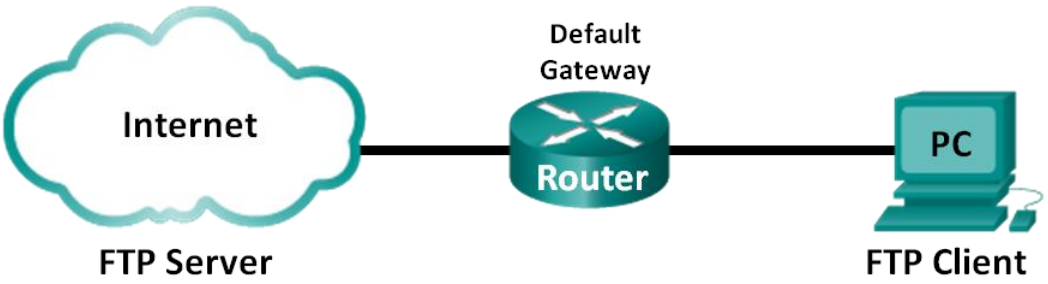
Laboratorium - Użycie z programu Wireshark do przechwytywania danych pochodzących z protokołu FTP i TFTP.

Topologia – Część 1 (FTP)

W części 1 omówimy przechwytywanie danych TCP w sesji FTP . Topologia składa się z komputera z dostępem do Internetu.



Topologia – Część 2 (TFTP)

W części 2 omówimy przechwytywanie danych UDP w sesji TFTP. Komputer musi być wyposażony w złącze Ethernet i połączenie konsolowe do przełącznika S1.

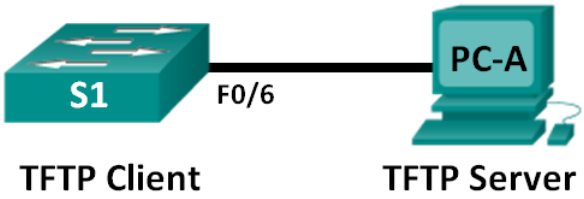


Tabela adresacji (Część 2)

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
S1	VLAN 1	192.168.1.1	255.255.255.0	Nie dotyczy
PC-A	Karta sieciowa	192.168.1.3	255.255.255.0	192.168.1.1

Cele

Część 1: Identyfikacja pól w nagłówku TCP oraz operacji przychwytywania przez Wireshark sesji FTP

Część 2: Identyfikacja pól w nagłówku datagramu UDP oraz operacji przechwytywania przez Wireshark w sesji TFTP

Scenariusz

Dwa protokoły w warstwie transportowej TCP/IP, to TCP zdefiniowane w RFC 761 oraz UDP zdefiniowane w RFC 768. Oba protokoły obsługują komunikację protokołów wyższych warstw. Na przykład, TCP jest używany do obsługi warstwy transportowej między innymi, dla protokołów Hypertext Transfer Protocol (HTTP) i FTP. Protokół UDP działa w warstwie transportowej i współpracuje między innymi z protokołami Domain Name System (DNS) oraz TFTP.

Uwaga: Zrozumienie zawartości nagłówków TCP i UDP oraz ich działania jest bardzo istotne dla inżynierów sieciowych.

W części 1 laboratorium będziesz używał programu typu Open Source Wireshark w celu przechwytywania i analizowania pól nagłówka protokołu TCP dla sesji FTP przesyłania plików pomiędzy komputerem hosta i anonimowym serwerem FTP. Aby połączyć się z anonimowym serwerem FTP i pobrać plik będzie używany Wiersz poleceń systemu Windows. W części 2 laboratorium będziesz używał programu Wireshark w celu przechwytywania i analizowania pól nagłówka protokołu UDP dla sesji przesyłania plików pomiędzy komputerem hosta i przełącznikiem S1 za pomocą TFTP.

Uwaga: Używany jest przełącznik Cisco Catalyst 2960s z systemem Cisco IOS w wersji 15.0 (2) (obraz lanbasek9). Można również używać innych przełączników i wersji systemu IOS. Zależnie od modelu urządzenia i wersji systemu IOS dostępne polecenia oraz wyniki ich działania mogą się różnić od prezentowanych w niniejszej instrukcji.

Uwaga: Upewnij się, czy przełącznik został wyczyszczony i nie ma konfiguracji początkowej. Jeśli nie jesteś pewien, poproś o pomoc instruktora.

Uwaga: Część 1 zakłada, że komputer ma dostęp do Internetu i część ta nie może być wykonywana przy użyciu Netlab. Część 2 jest kompatybilna z Netlab.

Wymagane zasoby - Część 1 (FTP)

1 PC (Windows 7, Vista, lub XP z dostępem do wiersza poleceń, dostępem do Internetu i zainstalowanym programem Wireshark)

Wymagane zasoby - Część 2 (TFTP)

- 1 przełącznik (Cisco 2960 z systemem Cisco IOS wersja15.0 (2) obraz lanbasek9 lub porównywalny)
- 1 PC (Windows 7, Vista lub XP z programem Wireshark oraz zainstalowanym serwerem TFTP, np. tftpd32)
- Do konfigurowania urządzeń Cisco podłącz kabel konsolowy poprzez port konsoli
- Kabel Ethernet pokazany jest na rysunku topologii

Część 1: Identyfikacja pól w nagłówku segmentu TCP oraz obserwacja działania w sesji FTP za pomocą programu Wireshark.

W części 1 należy użyć programu Wireshark do przechwytywania sesji FTP i sprawdzenia pól nagłówka TCP.

Krok 1: W programie Wireshark uruchom przechwytywanie.

a. Zamknij wszystkie zbędne komunikacje w sieci, takie jak na przykład przeglądarki WWW, aby ograniczyć ilość ruch podczas przechwytywania pakietów w programie Wireshark.

b. W programie Wireshark uruchom przechwytywanie.

Krok 2: Pobierz plik Readme.

a. W wierszu poleceń wpisz **ftp ftp.cdc.gov**.

b. Zaloguj się na stronę FTP Centers for Disease Control and Prevention (CDC) używając konta **anonymous** bez hasła.

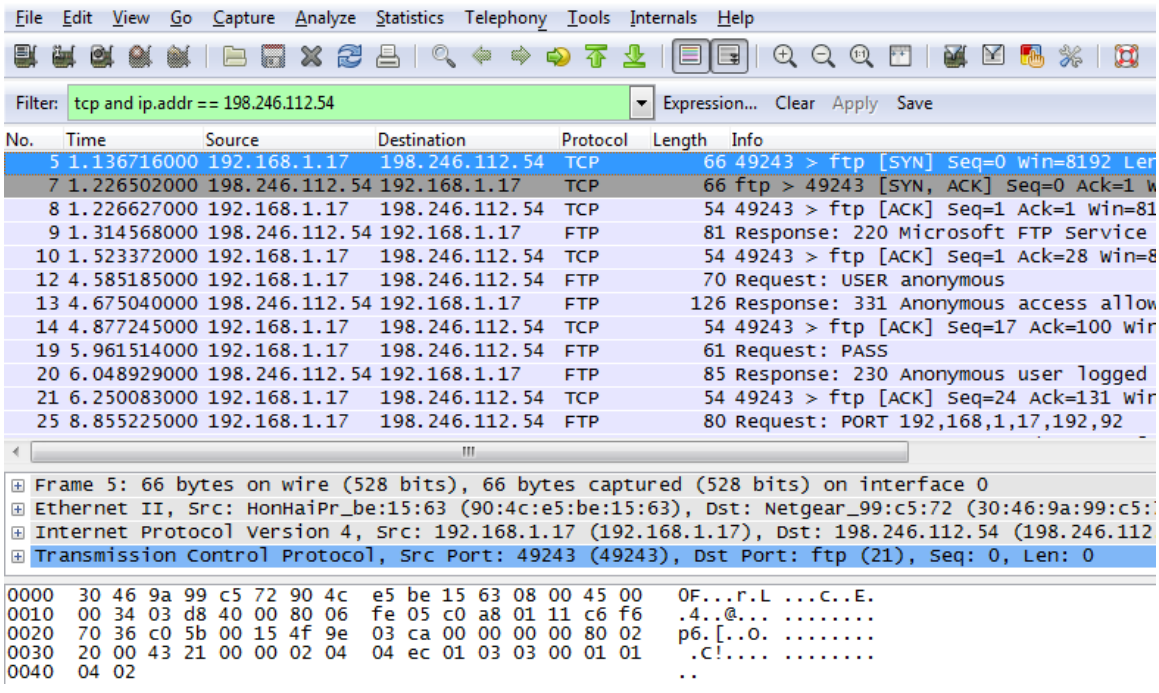
c. Znajdź i pobierz plik Readme.

```
C:\Users\user1>ftp ftp.cdc.gov
Connected to ftp.cdc.gov.
220 Microsoft FTP Service
User (ftp.cdc.gov:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
aspnet_client
pub
Readme
Siteinfo
up.htm
w3c
web.config
welcome.msg
226 Transfer complete.
ftp: 76 bytes received in 0.00Seconds 19.00Kbytes/sec.
ftp> get Readme
200 PORT command successful.
150 Opening ASCII mode data connection for Readme(1428 bytes).
226 Transfer complete.
ftp: 1428 bytes received in 0.01Seconds 204.00Kbytes/sec.
ftp> quit
221
```

Krok 3: Zatrzymaj przechwytywanie w programie Wireshark.

Krok 4: Przejdź do okna głównego programu Wireshark.

Wireshark przechwycił wiele pakietów w trakcie sesji FTP do strony ftp.cdc.gov. Aby ograniczyć ilość danych do analizy, w polu **Filter: entry** wpisz **tcp oraz ip.addr == 198.246.112.54** i kliknij **Apply**. Adres IP 198.246.112.54 jest adresem strony ftp.cdc.gov.



Krok 5: Przeanalizuj zawartości pól TCP.

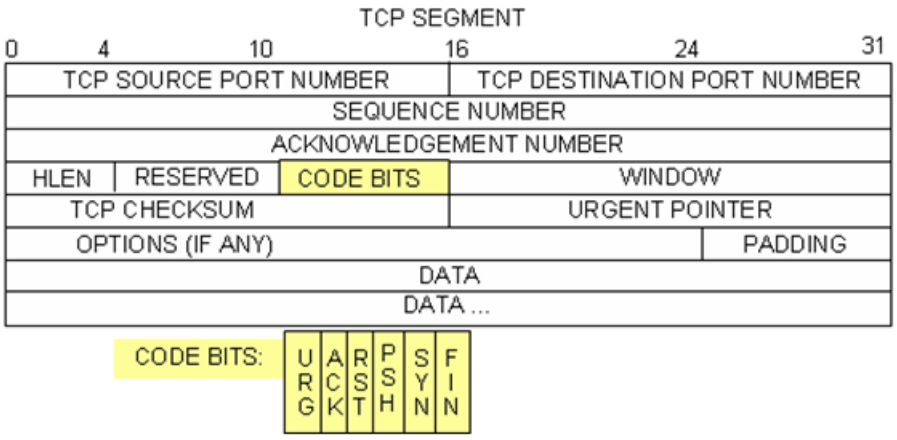
Po zastosowaniu filtru TCP pierwsze trzy ramki w okienku listy pakietów (górna sekcja) wyświetla w warstwie transportowej protokół TCP służący do tworzenia niezawodnej sesji. Sekwencja [SYN], [SYN, ACK], [ACK] ilustruje 3-etapowe uzgodnienie.

```
    5 1.136716000  192.168.1.17    198.246.112.54   TCP        66 49243 > ftp [SYN] Seq=0 Win=8192 Le
    7 1.226502000  198.246.112.54  192.168.1.17     TCP        66 ftp > 49243 [SYN, ACK] Seq=0 Ack=1
    8 1.226627000  192.168.1.17    198.246.112.54   TCP        54 49243 > ftp [ACK] Seq=1 Ack=1 Win=8
```

TCP jest rutynowo używany podczas sesji do kontroli dostarczenia datagramu, weryfikacji jego dotarcia i zarządzania rozmiarem okna. Dla każdej wymiany danych pomiędzy klientem a serwerem FTP jest uruchomiana nowa sesja TCP. Na zakończenie wymiany danych sesja TCP jest zamykana. Gdy sesja FTP jest zakończona, to TCP wykonuje procedurę zamknięcia i zakończenia połączenia.

Szczegółowe informacje na temat TCP są dostępne w panelu szczegółów pakietów programu Wireshark (sekcja środkowa). Podświetl pierwszy datagram TCP z komputera hosta i rozwiń rekord TCP. Rozwinięty datagram TCP wydaje się być podobny do okienka szczegółów pakietu (packet detail) widocznego poniżej.

```
⊞ Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
⊞ Ethernet II, Src: HonHaiPr_be:15:63 (90:4c:e5:be:15:63), Dst: Netgear_99:c5:72 (30:46:9a:99:c5:72)
⊞ Internet Protocol Version 4, Src: 192.168.1.17 (192.168.1.17), Dst: 198.246.112.54 (198.246.112.54)
⊟ Transmission Control Protocol, Src Port: 49243 (49243), Dst Port: ftp (21), Seq: 0, Len: 0
    Source port: 49243 (49243)
    Destination port: ftp (21)
    [Stream index: 0]
    Sequence number: 0    (relative sequence number)
    Header length: 32 bytes
  ⊟ Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    ⊞ .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
    Window size value: 8192
    [Calculated window size: 8192]
  ⊞ Checksum: 0x4321 [validation disabled]
  ⊞ Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), Nc
```



Powyższy rysunek przedstawia schemat datagramu TCP. Opis każdego pola znajduje się w dokumencie:

- **Numer portu źródłowego TCP** przypisany jest do sesji TCP hosta, który otworzył połączenie. Liczba ta jest zwykle wartością losową powyżej 1023.
- **Numer portu docelowego** jest używany w celu określenia protokołu warstwy wyższej bądź aplikacji na komputerze docelowym (serwerze). Wartości z zakresu 0-1023 reprezentują "dobrze znane porty" i związane są z popularnymi usługami i aplikacjami (w sposób opisany w dokumencie RFC 1700, takimi jak Telnet, FTP, HTTP oraz innymi). Kombinacja czterech wartości (źródłowego adresu IP, źródłowego numeru portu, docelowego adresu IP, docelowego numeru portu) identyfikuje w sposób unikalny sesję dla obu hostów: klienta i serwera.

Uwaga: W programie Wireshark przechwycony poniżej port docelowy to 21, co oznacza że jest to FTP. Serwery FTP na porcie 21 nasłuchują połączenia od klienta FTP.

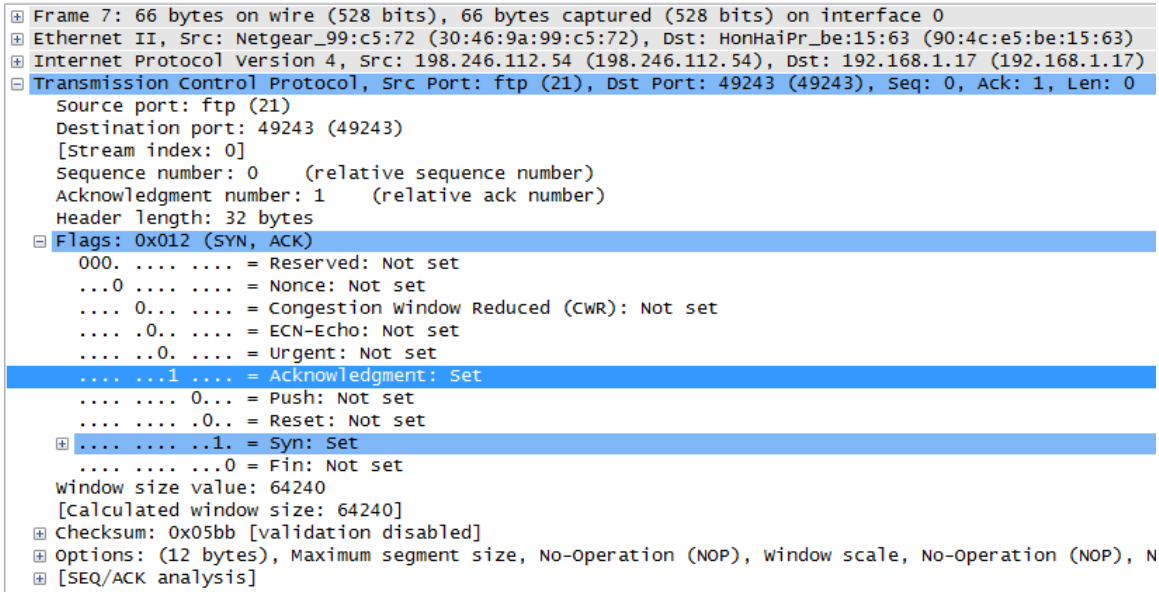
- **Numer sekwencyjny** określa numer ostatniego oktetu w segmencie.
- **Numer potwierdzenia** określa numer następnego oktetu oczekiwanego przez odbiorcę.
- **Bity kontrolne** (flagi) mają specjalne znaczenie w zarządzaniu sesją i w określaniu sposobu traktowania segmentów. Wśród nich wyróżniamy:
  - ACK — bit/flaga potwierdzenia otrzymania segmentu,
  - SYN — bit/flaga synchronizacji, ustawiona tylko wtedy, gdy nowa sesja jest negocjowana podczas trójetapowego uzgadniania,
  - FIN — bit/flaga zakończenia, która oznacza żądanie zamknięcia sesji.
- **Rozmiar okna** to wartość rozmiaru okna przesuwnego, oznaczająca ile oktetów może być przesłanych zanim nadawca będzie musiał czekać na potwierdzenie.
- **Wskaźnik Urgent** jest używany tylko z flagą Urgent (URG), gdy nadawca musi wysłać pilne dane do odbiornika.
- **Options** ma obecnie tylko jedną możliwość i jest określona jako maksymalna wielkość segmentu TCP (wartość opcjonalna).

Używając programu Wireshark przechwyć pierwszą fazę w sesji TCP (flaga SYN ustawiona na 1) i wypełnij informację o nagłówku datagramu TCP:

Z komputera PC do serwera CDC (tylko flaga SYN jest ustawiona na 1):

Adres IP nadawcy:	
Adres docelowy IP:	
Numer portu źródłowego:	
Numer portu docelowego	
Numer sekwencyjny:	
Numer potwierdzenia:	
Długość nagłówka:	
Rozmiar okna:	

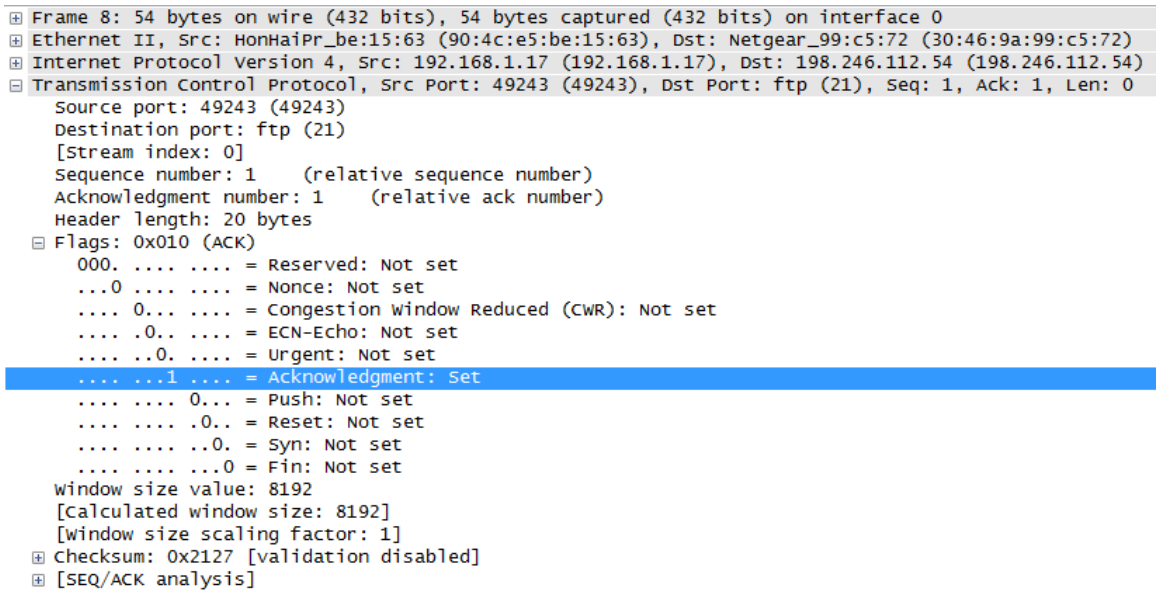
W drugim filtrowanym przechwytywaniu Wiresharka serwer CDC FTP potwierdza żądanie z komputera PC. Zanotuj wartości bitów SYN i ACK.



Wypełnij następujące informacje dotyczące wiadomości SYN-ACK.

Źródłowy adres IP:	
Adres docelowy IP:	
Numer portu źródłowego:	
Numer portu docelowego:	
Numer sekwencyjny:	
Numer potwierdzenia:	
Długość nagłówka:	
Rozmiar okna:	

W końcowej fazie negocjacji w celu nawiązania komunikacji, komputer wysyła do serwera komunikat potwierdzający. Zauważ, że tylko bit ACK jest ustawiony na 1, a numer sekwencyjny został zwiększony do 1.

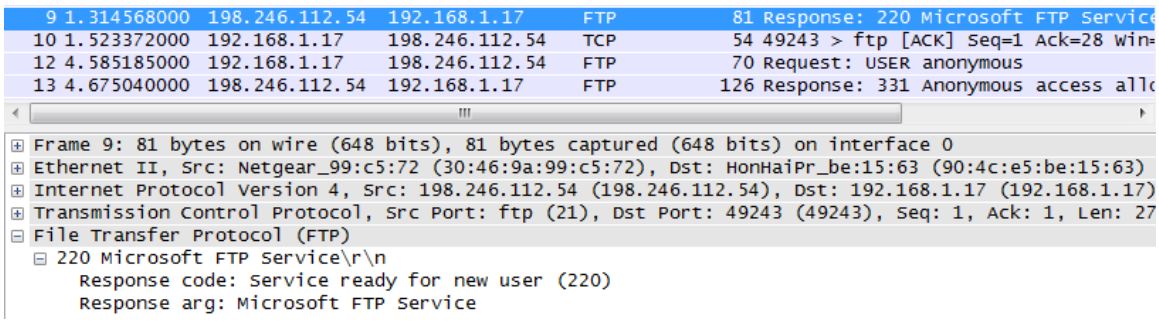


Wypełnij następujące informacje dotyczące wiadomości ACK.

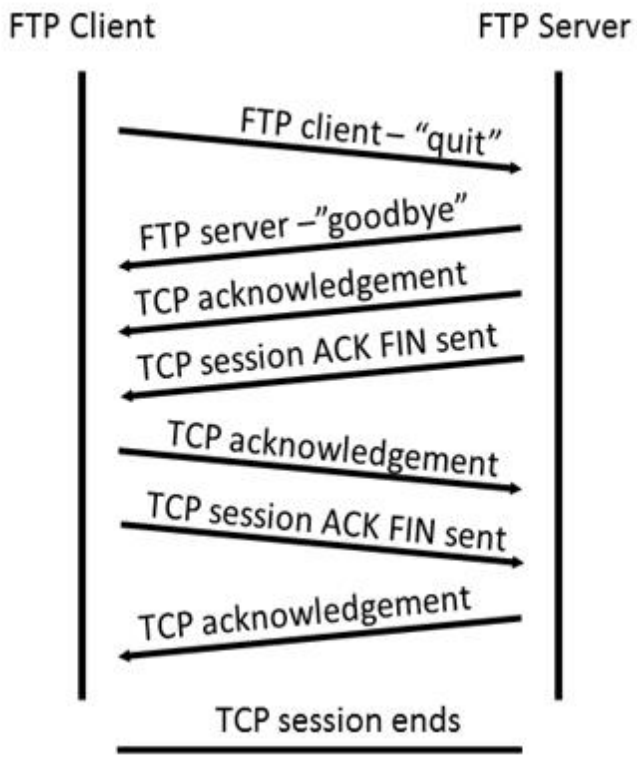
Źródłowy adres IP:	
Adres docelowy IP:	
Numer portu źródłowego:	
Numer portu docelowego:	
Numer sekwencyjny:	
Numer potwierdzenia:	
Długość nagłówka:	
Rozmiar okna:	

Ile innych datagramów TCP zawiera bit SYN?

Po ustanowieniu sesji TCP, może wystąpić ruch FTP pomiędzy komputerem PC i serwerem FTP. Klient i serwer FTP komunikują się ze sobą nie wiedząc, że TCP kontroluje i zarządza nawiązaną przez nich sesją. Gdy serwer FTP wysyła odpowiedź: 220 do klienta FTP, to sesja TCP w kliencie FTP wysyła potwierdzenie do sesji TCP na serwerze. Tą sekwencję można przechwycić i obejrzeć w programie Wireshark.



Gdy połączenie FTP jest zakończone, to klient FTP wysyła komendę "quit". Serwer FTP potwierdza zakończenie połączenia FTP za pomocą odpowiedzi: 221 Goodbye. W tym momencie sesja TCP w serwerze FTP wysyła datagram TCP do klienta FTP, ogłaszający zakończenie sesji TCP. Sesja TCP na kliencie FTP potwierdza otrzymanie datagramu kończącego sesję i wysyła własny datagram TCP kończący sesję. Gdy źródło zakończenia sesji TCP, serwer FTP otrzyma podwójne zakończenie, datagram z ustawionym bitem ACK jest wysyłany aby potwierdzić zakończenie sesji TCP i sesja TCP jest zamknięta. Tą sekwencję można przechwycić i obejrzeć na diagramie.



Dzięki zastosowaniu filtru **ftp**, cała sekwencja ruchu FTP może być badana w programie Wireshark. Zwróć uwagę na kolejność występowania zdarzeń podczas tej sesji FTP. Do pobrania pliku Readme użyto nazwy użytkownika anonymous. Po zakończeniu transferu plików użytkownik zakończył sesję FTP.

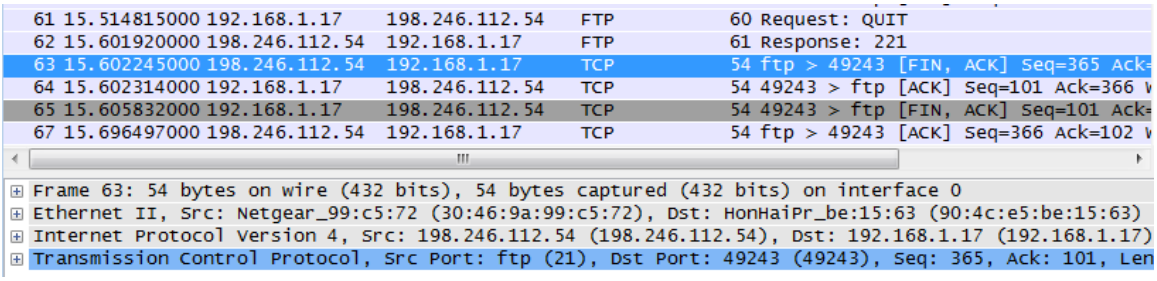
Filter: ftp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
9	1.314568000	198.246.112.54	192.168.1.17	FTP	81	Response: 220 Microsoft FTP Service
12	4.585185000	192.168.1.17	198.246.112.54	FTP	70	Request: USER anonymous
13	4.675040000	198.246.112.54	192.168.1.17	FTP	126	Response: 331 Anonymous access allowe
19	5.961514000	192.168.1.17	198.246.112.54	FTP	61	Request: PASS
20	6.048929000	198.246.112.54	192.168.1.17	FTP	85	Response: 230 Anonymous user logged i
25	8.855225000	192.168.1.17	198.246.112.54	FTP	80	Request: PORT 192,168,1,17,192,92
26	8.945530000	198.246.112.54	192.168.1.17	FTP	84	Response: 200 PORT command successful
27	8.955549000	192.168.1.17	198.246.112.54	FTP	60	Request: NLST
29	9.053034000	198.246.112.54	192.168.1.17	FTP	109	Response: 150 Opening ASCII mode data
39	9.347432000	198.246.112.54	192.168.1.17	FTP	78	Response: 226 Transfer complete.
42	12.621720000	192.168.1.17	198.246.112.54	FTP	80	Request: PORT 192,168,1,17,192,93
43	12.709658000	198.246.112.54	192.168.1.17	FTP	84	Response: 200 PORT command successful
44	12.722592000	192.168.1.17	198.246.112.54	FTP	67	Request: RETR Readme
45	12.811097000	198.246.112.54	192.168.1.17	FTP	118	Response: 150 Opening ASCII mode data
58	13.107294000	198.246.112.54	192.168.1.17	FTP	78	Response: 226 Transfer complete.
61	15.514815000	192.168.1.17	198.246.112.54	FTP	60	Request: QUIT
62	15.601920000	198.246.112.54	192.168.1.17	FTP	61	Response: 221

Zastosuj ponownie filtr TCP w Wireshark aby zbadać zakończenie sesji TCP. Cztery pakiety są transmitowane dla zakończenia sesji TCP. Ponieważ połączenie TCP jest typu full-duplex, to każda strona musi samodzielnie dokonać zakończenia. Sprawdź adresy źródłowe i docelowe.

W tym przykładzie serwer FTP nie ma już danych do wysłania w strumieniu; serwer wysyła segment z ustawioną flagą FIN w ramce 63. PC wysyła ACK, aby potwierdzić otrzymanie FIN w celu zakończenia sesji z serwera do klienta w ramce 64.

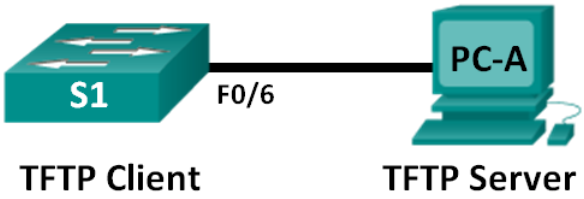
W ramce 65 komputer PC wysyła FIN do serwera FTP, aby zakończyć sesję TCP. Serwer FTP odpowiada za pomocą ACK, aby potwierdzić FIN przychodzący z komputera PC w ramce 67. Teraz sesja TCP między serwerem FTP i PC jest zakończona.



Część 2: Identyfikacja pól w nagłówku datagramu UDP oraz obserwacja operacji w przechwyconej sesji TFTP za pomocą programu Wireshark

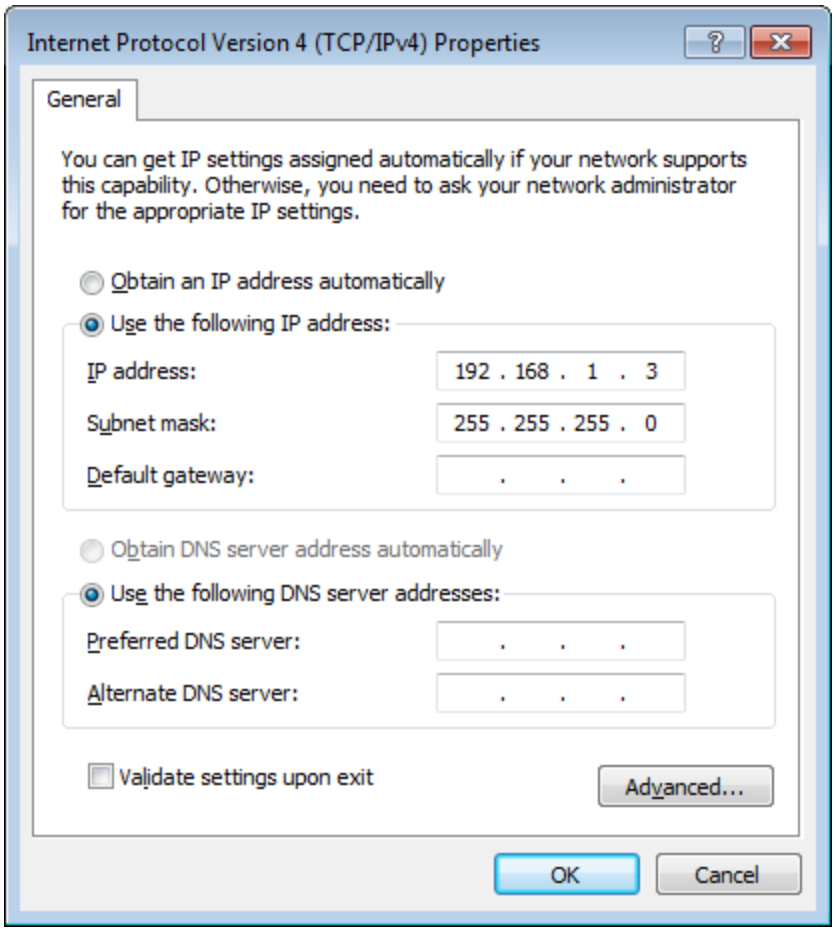
W części 2 należy użyć programu Wireshark do przechwytywania sesji TFTP i sprawdzania pól w nagłówku UDP.

Krok 1: Ustaw fizyczną topologię i przygotuj się do przechwytywania TFTP.



d. Utwórz połączenie konsolowe i Ethernet między PC-A i przełącznikiem S1.

e. Jeśli jeszcze tego nie zrobiłeś, to ustaw ręcznie adres IP na komputerze na 192.168.1.3. Ustawienie domyślnej bramy nie jest konieczne.



f. Skonfiguruj przełącznik. Przypisz adres IP 192.168.1.1 do interfejsu VLAN 1. Sprawdź połączenie z komputerem za pomocą **ping 192.168.1.3**. W przypadku wystąpienia problemów spróbuj je rozwiązać.

```
Switch> enable
Switch# conf t
Wprowadź polecenia konfiguracyjne, podając w każdym wierszu tylko jedno polecenie.  Zakończ za pomocą CNTL/Z.
Switch(config)# host S1
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.1 255.255.255.0
S1(config-if)# no shut
*Mar  1 00:37:50.166: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*Mar  1 00:37:50.175: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
S1(config-if)# end
S1# ping 192.168.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/203/1007 ms
```

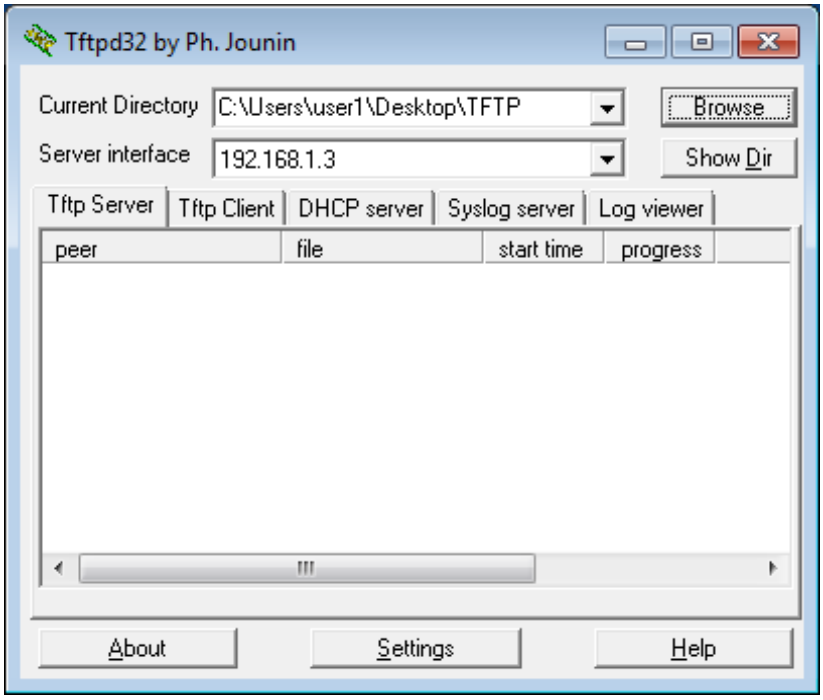
Krok 2: Przygotuj serwer TFTP na komputerze PC.

a. Utwórz folder o nazwie **TFTP** na pulpicie komputera PC, jeżeli ten folder nie istnieje. Pliki z przełącznika zostaną skopiowane do tego miejsca.

b. Na PC uruchom **tftpd32**.

c. Kliknij **Browse** i zmień aktualny katalog na **C:\Users\user1\Desktop\TFTP** poprzez zmianę user1 na twoją nazwę użytkownika.

Serwer TFTP powinien wyglądać tak:



Zauważ, że w bieżącym katalogu można znaleźć użytkownika i interfejs serwera (PC-A) z adresem IP **192.168.1.3**.

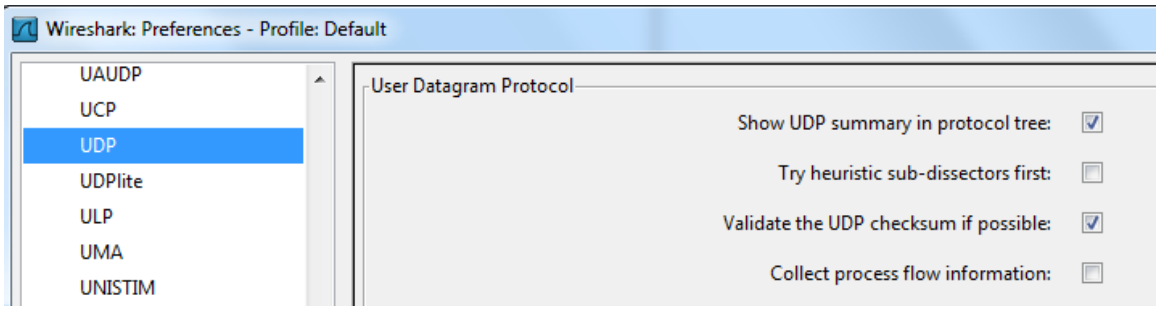
d. Przetestuj możliwość kopiowania plików z przełącznika do komputera przy użyciu protokołu TFTP. W przypadku wystąpienia problemów spróbuj je rozwiązać.

```
S1# copy start tftp
Address or name of remote host []? 192.168.1.3
Destination filename [s1-confg]?
!!
1638 bytes copied in 0.026 secs (63000 bytes/sec)
```

Jeżeli widzisz, że plik został skopiowany (jak w powyższym przykładzie), to jesteś gotowy, aby przejść do następnego kroku. Jeśli nie, to rozwiąż problemy. Jeżeli otrzymasz błąd `%Error opening tftp (Permission denied)`, to najpierw upewnij się czy twoja zapora sieciowa nie blokuje TFTP, a także czy kopiujesz do miejsca w którym dla twojej nazwy użytkownika są nadane odpowiednie prawa, np do pulpitu.

Krok 3. Przechwytywanie sesji TFTP w Wireshark

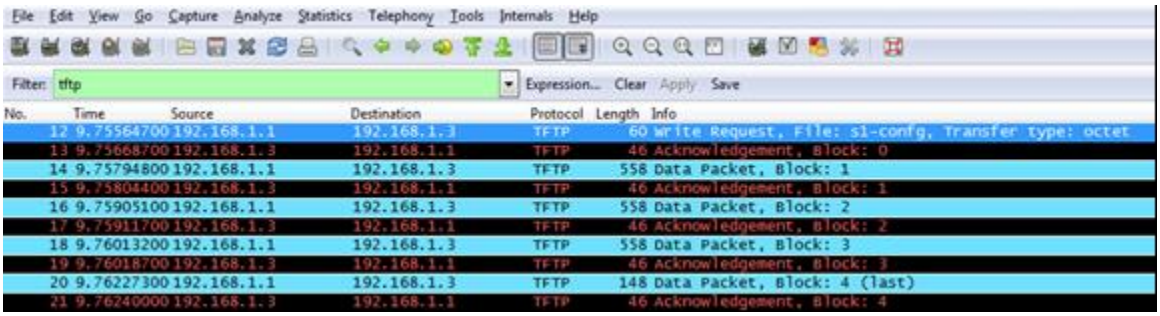
a. Uruchom program Wireshark. W menu **Edit** wybierz **Preferences** i kliknij znak (+) aby rozwinąć **Protocols**. Przewiń w dół i wybierz opcję **UDP**. Kliknij opcję **Validate the UDP checksum if possible** i kliknij **Apply**. Następnie kliknij **OK**.



b. Uruchom przechwytywanie.

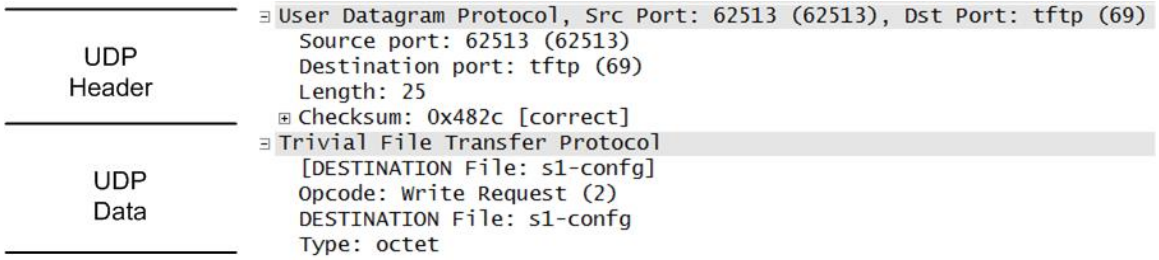
c. Na przełączniku uruchom polecenie **`copy start tftp`**.

d. Zatrzymaj przechwytywanie w programie Wireshark.

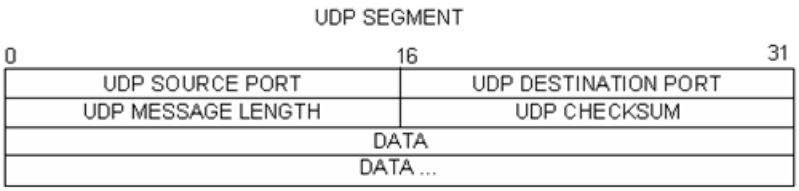


e. Ustaw filtr na **tftp**. Wynik komendy powinien być podobny do przykładu przedstawionego poniżej. Transfer TFTP został użyty do analizy operacji zachodzących w warstwie transportowej dla protokołu UDP.

W programie Wireshark szczegółowe informacje o UDP są dostępne okienku szczegółów pakietu. Zaznacz (podświetl) pierwszy datagram UDP pochodzący z komputera lokalnego i przesuń kursor myszy nad okna zawierającego szczegóły pakietu. Może być konieczne dostosowanie rozmiaru okna i rozwinięcie przechwyconych informacji o UDP przez kliknięcie odpowiedniego przycisku rozwinięcia (+). Rozwinięty datagram UDP powinien być podobny do poniższego diagramu.



Rysunek poniżej przedstawia schemat datagramu UDP. Informacji zawartych w nagłówku datagramu UDP jest niewiele w porównaniu z nagłówkiem datagramu TCP. Podobnie jak w przypadku TCP, każdy datagram UDP jest identyfikowany przez port źródłowy UDP i port docelowy UDP.



Używając przechwyconych informacji przez program Wireshark wypełnij poniższe informacje dotyczące nagłówka segmentu UDP. Suma kontrolna to liczba szesnastkowa oznaczona przedrostkiem 0x:

Adres IP źródłowy:	
Adres docelowy IP:	
Numer portu źródłowego:	
Numer portu docelowego:	
Długość wiadomości UDP:	
Suma kontrolna UDP:	

Jak UDP weryfikuje poprawność datagramu?

_____

_____

Przeanalizuj pierwszą ramkę zwróconą przez serwer tftpd. Wypełnij informacje dotyczące nagłówka UDP:

Adres IP nadawcy:	
Adres docelowy IP:	
Numer portu źródłowego:	
Numer portu docelowego:	
Długość wiadomości UDP:	
Suma kontrolna UDP:	

```
⊟ User Datagram Protocol, Src Port: 58565 (58565), Dst Port: 62513 (62513)
    Source port: 58565 (58565)
    Destination port: 62513 (62513)
    Length: 12
  ⊞ Checksum: 0x8372 [incorrect, should be 0xa385 (maybe caused by "UDP checksum offload"?)]
⊟ Trivial File Transfer Protocol
    [DESTINATION File: s1-confg]
    Opcode: Acknowledgement (4)
    Block: 0
```

Zauważ, że zwrócony datagram UDP ma inny źródłowy port, ale ten źródłowy port jest użyty w dalszym transferze TFTP. Ponieważ w tym przypadku nie jest to połączenie niezawodne, tylko oryginalny port źródłowy używany do rozpoczęcia sesji TFTP, jest używany do utrzymywania transferu TFTP.

Zauważ również, że suma kontrolna UDP jest niepoprawna. Jest to najprawdopodobniej spowodowane przez tzw. "UDP checksum offload". Możesz dowiedzieć się więcej o tym, dlaczego tak się dzieje, wyszukując frazę "UDP checksum offload".

Do przemyślenia

To laboratorium przedstawia studentom możliwości analizy operacji występujących w protokołach TCP oraz UDP, z przechwyconych sesji FTP i TFTP. W jaki sposób zarządzanie komunikacją w TCP różni się od UDP?

_____

_____

Wyzwanie

Ponieważ ani FTP i ani TFTP nie są bezpiecznymi protokołami, to wszystkie dane przesyłane za ich pomocą wysyłane są otwartym tekstem. Dotyczy to także ID użytkowników, haseł i zawartości plików tekstowych nieszyfrowanych. Analizując sesję FTP szybko odnajdziemy ID użytkownika, hasło a także hasła w plikach konfiguracyjnych. Analiza danych przesyłanych za pomocą TFTP jest trochę bardziej skomplikowana, ale i tu da się odnaleźć ID użytkowników i hasła.

Oczyszczanie komputera

O ile instruktor nie wskazał inaczej, to:

- usuń pliki, które zostały skopiowane do twojego komputera,
- usuń konfigurację na przełączniku **S1**,
- usuń ręcznie skonfigurowany adres IP z komputera i przywróć łączność z Internetem.