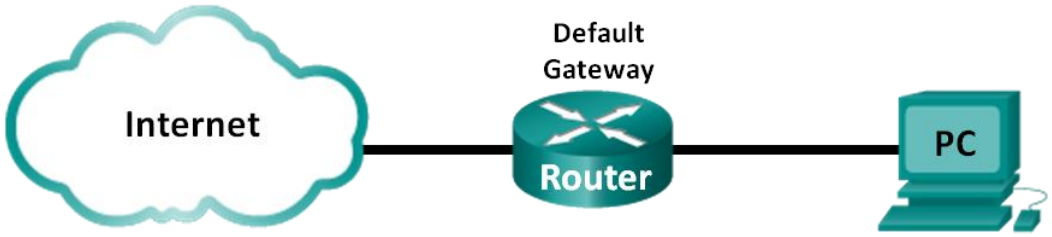
Folosirea Wireshark-ului pentru a Observa 3-Way Handshake-ul TCP-ului

Topologie



Obiective

Partea 1: Pregătiți Wireshark pentru a Captura Pachete

- Selectați o interfață corespunzătoare a plăcii de rețea pentru a captura pachete.

Partea 2: Capturați, Localizați și Examinați Pachete

- Capturați o sesiune web pe www.google.com.
- Localizați pachete corespunzătoare pentru o sesiune web.
- Examinați informația din cadrul pachetelor, inclusiv adresele IP, numerele porturilor TCP și flag-urile de control TCP.

Context/Scenariu

În acest laborator veți utiliza Wireshark pentru a captura și examina pachete generate între navigatorul calculatorului folosind HHTP și un server de wev, precum www.google.com.Atunci când o aplicație precum HTTP sau FTP pornește pentru prima dată pe un host, TCP folosește three-way handshake pentru a stabili o sesiune TCP fiabilă între două hosturi.De exemplu, atunci când un calculator folosește un navigator web pentru a naviga pe Internet, este inițiat un three-way handshake si este stabilită o sesiune între host și serverul de web.Un calculator poate avea mai multe sesiuni TCP active, simultan cu diferite site-uri web.

Notă: Acest laborator nu poate fi completat folosind Netlab.Acest laborator presupune că aveți acces la Internet.

Resurse necesare

1 calculator (cu Windows 7, Vista sau XP cu acces la ecranul de comandă și la Internet și care să aibă instalat Wireshark)

Partea 1: Pregătiți Wireshark pentru a Captura Pachete

În Partea 1 porniți programul Wireshark și selectați interfața corespunzătoare pentru a începe capturarea pachetelor.

Pasul 1: Obțineți adresele interfeței calculatorului.

Pentru acest laborator trebuie să obțineți adresa IP a calculatorului dumneavoastră și adresa fizică a plăcii de rețea, denumită și adresa MAC.

a. Deschideți un ecran de comandă, tastați **ipconfig /all** și apoi apăsați **Enter**.

```
Physical Address. . . . . : C8-0A-A9-FA-DE-0D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.1.130(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, December 01, 2012 1:43:35 PM
Lease Expires . . . . . : Sunday, December 02, 2012 1:43:35 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
```

b. Scrieți adresele IP și MAC asociate cu placa Ethernet selectată, deoarece aceasta este adresa sursei după care trebuie să vă uitați atunci când examinați pachetele capturate.

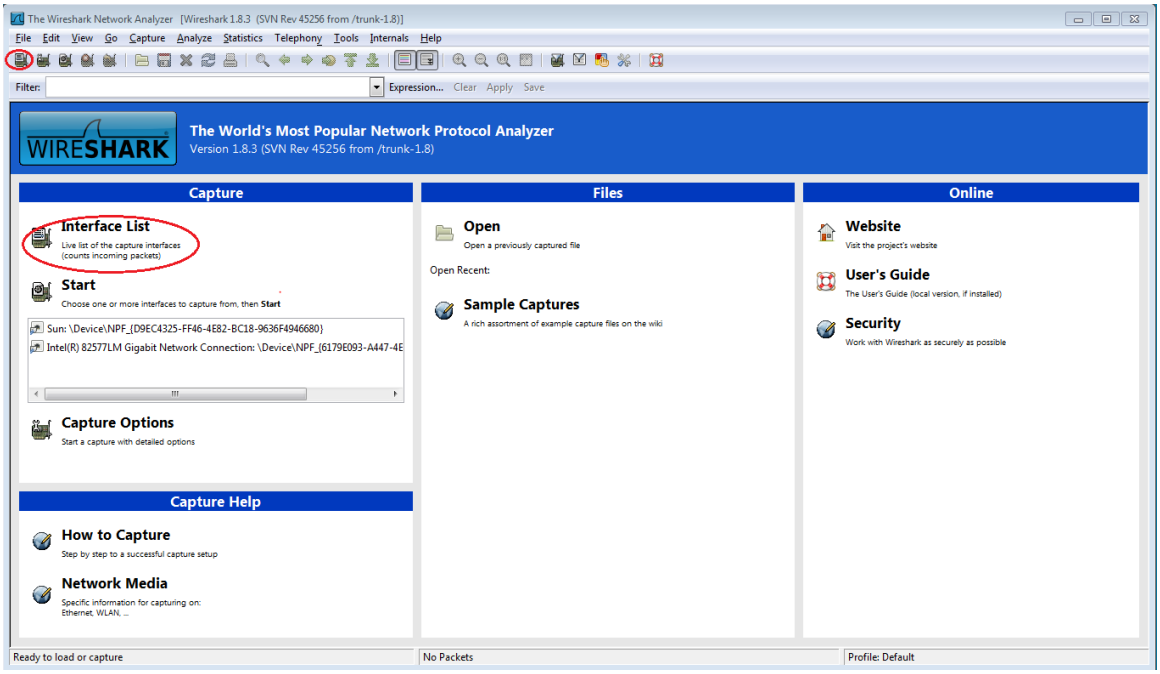
Adresa IP a hostului:_____

Adresa MAC a hostului: _____

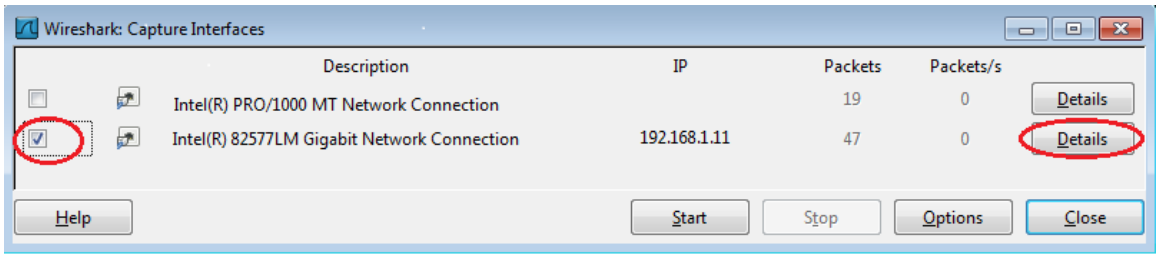
Pasul 2: Porniți Wireshark și selectați interfața corespunzătoare.

a. Dați clic pe butonul **Start** din Windows și dublu clic pe **Wireshark**.

b. După ce pornește Wireshark, dați clic pe **Interface List.**



c. În fereastra din Wireshark Capture Interfaces, bifați căsuța de lângă interfața conectată la rețeaua dumneavoastră LAN.



Notă: În cazul în care sunt afișate mai multe interfețe și nu sunteți sigur ce interfață să bifați, dați clic pe Details.Dați clic pe fila 802.3 (Ethernet) și verificați dacă adresa MAC se potrivește cu ce ați notat dumneavoastră la Pasul 1b.După verificare închideți fereastra Interface Details.

Partea 2: Capturați, Localizați și Examinați Pachete

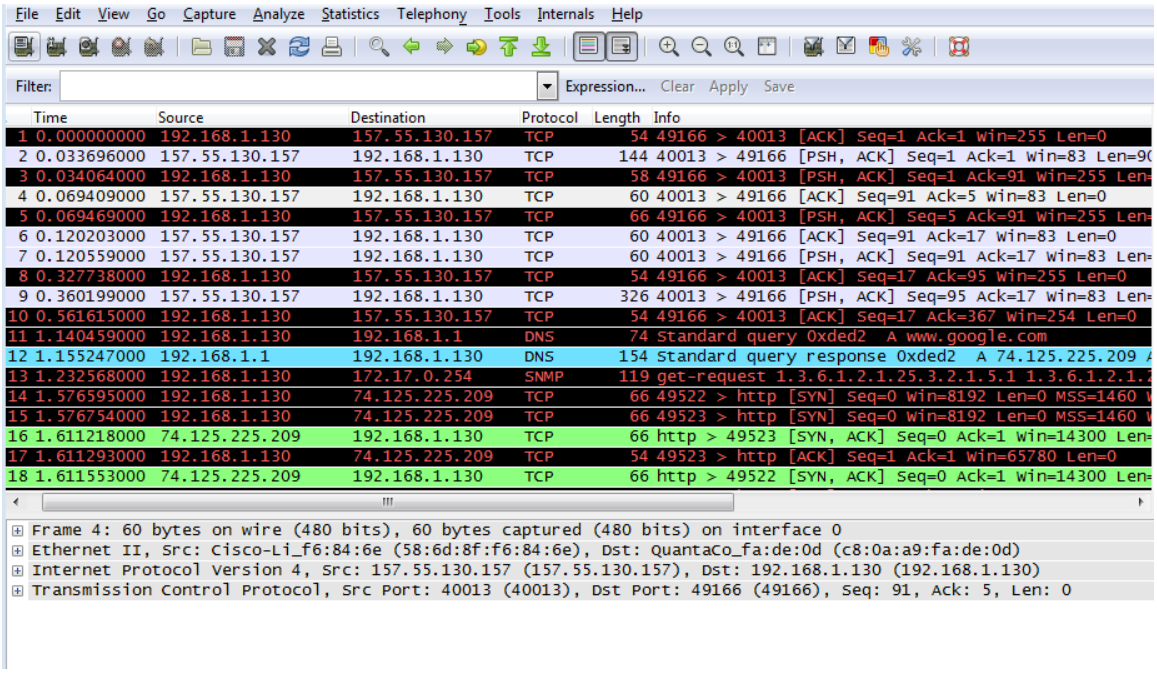
Pasul 1: Dați clic pe butonul Start pentru a începe capturarea datelor.

a. Mergeți la www.google.com.Minimizați fereastra Google și reveniți în Wireshark.Opriți capturarea datelor.Ar trebui să vedeți trafic capturat similat cu cel arătat la pasul b.

Notă: Este posibil ca instructorul să vă furnizeze un site web diferit.Dacă da, introduceți aici numele sau adresa site-ului web:

_____

b. Fereastra de captură este activată.Localizați coloanele **Sursă**, **Destinație** și **Protocol**.



Pasul 2: Localizați pachetele corespunzătoare pentru sesiunea web.

În cazul în care calculatorul a fost recent pornit și nu a existat activitate în accesarea Internetului, puteți vedea întregul proces în rezultatul obținut, inclusiv ARP, DNS și three-way handshake TCP.Ecranul de capturare din partea 2, Pasul 1 arată toate pachetele pe care calculatorul trebuie să le ducă la www.google.com.În acest caz, calculatorul deja are o intrare ARP pentru gateway-ul default; așadar, se începe cu interogarea DNS pentru a rezolva www.google.com.

a. Frame-ul 11 arată interogarea DNS de la calculator la serverul DNS, încercând să rezolve numele domeniului www.google.com în adresa IP a serverului de web.Calculatorul trebuie să aibă adresa IP înainte de putea trimite primul pachet la serverul web.

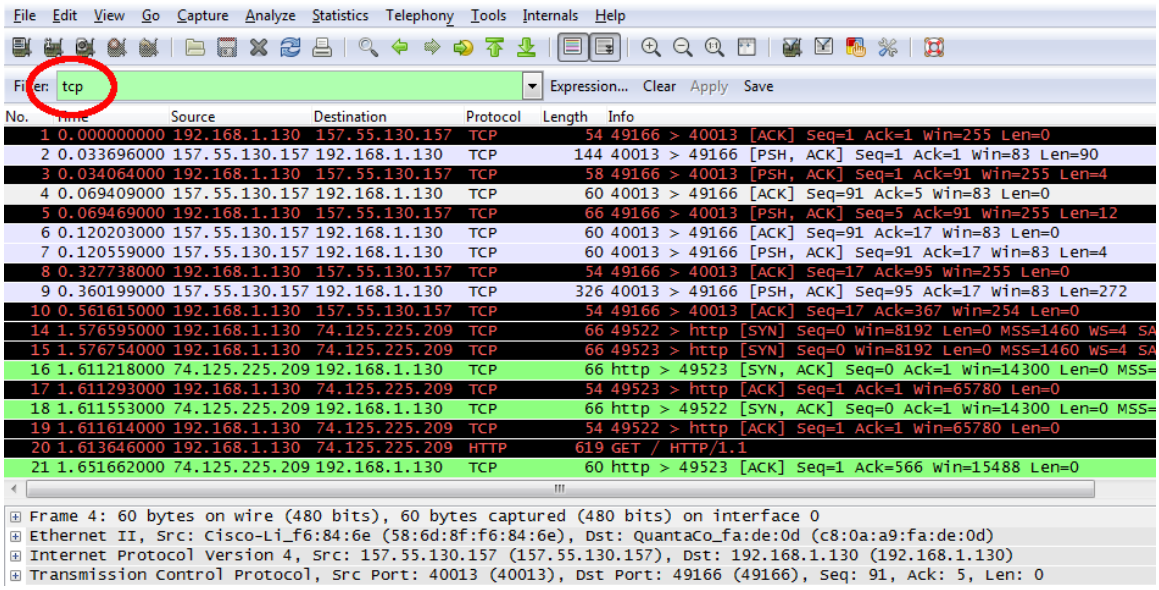
Care este adresa IP solicitată de calculator a serverului DSN ?_____

b.Frame-ul 12 este răspunsul de la serverul DNS cu adresa IP a lui www.google.com.

c. Găsiți pachetul corespunzător pentru începerea three-way handshake-ului.În acest exemplu, frame-ul 15 reprezintă începutul three-way handshake-ului TCP.

Care este adresa IP a serverului de web Google? _____

d. Dacă aveți mai multe pachete care nu au legătură cu conexiunea TCP, ar putea fi necesar să utilizați opțiunea de filtru din Wireshark.Tastați **tcp** în zona filtrului din Wireshark și apăsați pe **Enter**.



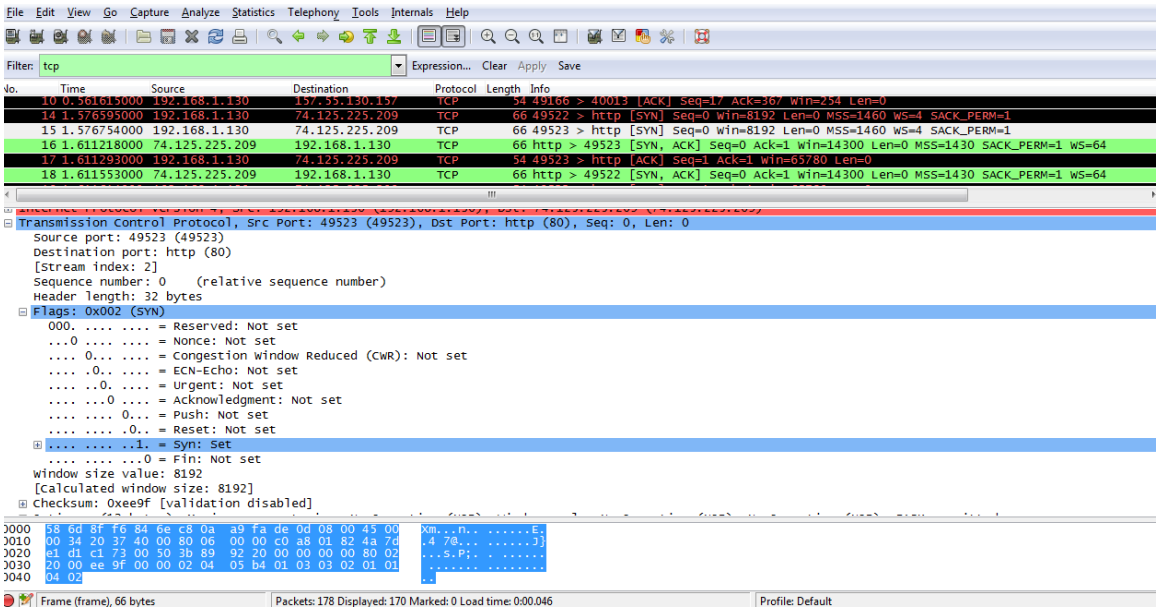
Pasul 3: Examinați informația din cadrul pachetelor, inclusiv adresele IP, numerele porturilor TCP și flag-urile de control TCP.

a. În exemplul nostru, frame-ul 15 este începutului three-way handshake-ului între calculator și serverul de web Google.În panoul Packet List, selectați frame-ul.Acesta evidențiază linia și afișează informația decodificată din pachet în cele două panouri inferioare.Examinați informația TCP din panoul cu detalii despre pachete (secțiunea din mijloc a ferestrei principale).

b. Dați clic pe pictograma + din stânga TCP-ului în panoul cu detalii despre pachete pentru a extinde imaginea cu informații despre TCP.

c. Dați clic pe + situat în stânga lângă Flags.Priviți porturile sursă și de destinație și flag-urile care sunt setate.

Notă: Este posibil să fie nevoie să ajustați dimensiunile ferestrelor de sus și din mijloc din Wireshark pentru a afișa informațiile necesare.



Care este numărul portului sursă TCP? _____

Cum ați clasifica portul sursă? _____

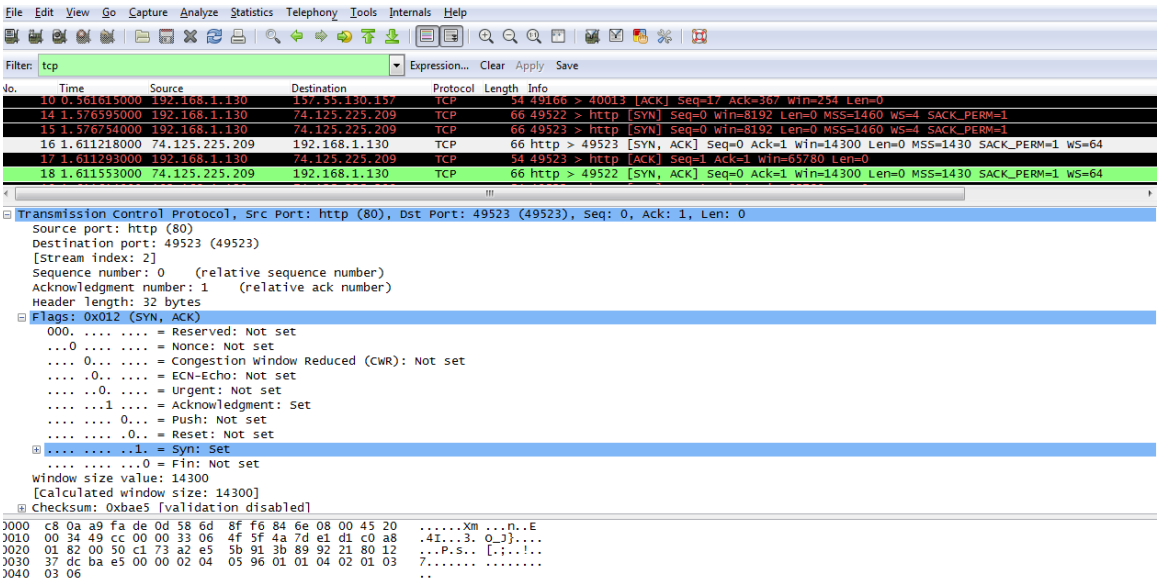
Care este numărul portului de destinație TCP? _____

Cum ați clasifica portul de destinație? _____

Ce flag (sau flag-uri) este setat? _____

La cât este setat numărul de secvență relativ? _____

d. Pentru a selecta următorul frame și three-way handshake, selectați **Go** din meniul Wireshark și apoi **Next Packet In Conversation**.În acest exemplu, acest frame este 16.Acesta este răspunsul serverului de web Google la solicitarea inițială de pornire a sesiunii.



Care sunt valorile porturilor de destinație și sursă? _____

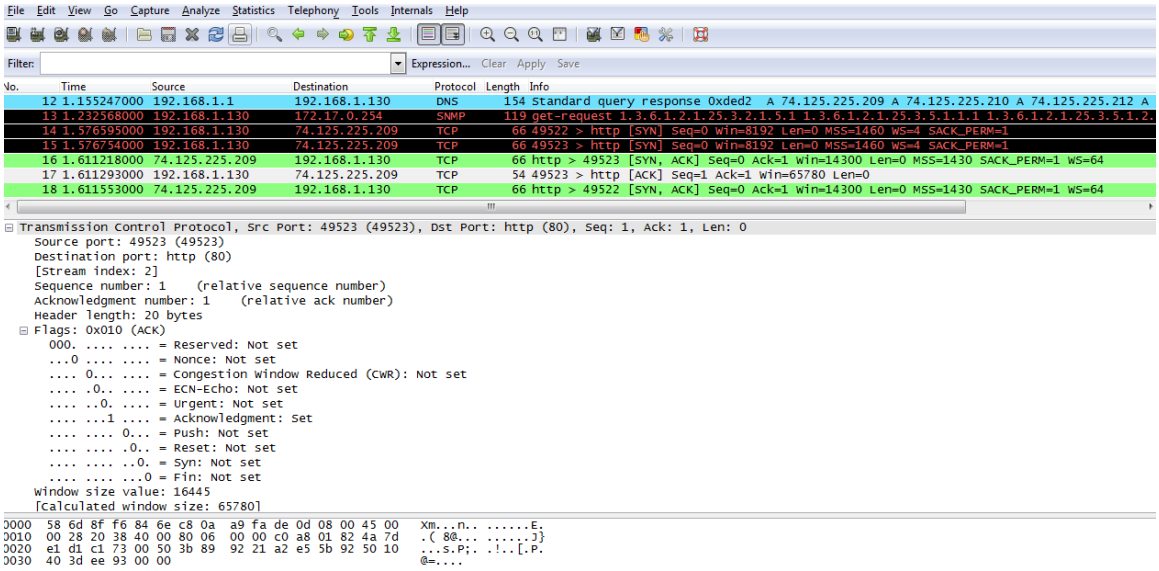
Ce flag-uri sunt setate?

_____

Ce valori au numerele de confirmare și cel de secvență?

_____

e. În final, examinați al treilea pachet al three-way handshake-ului din exemplu.Dând clic pe frame-ul 17 din fereastra de sus, se afișează următoarea informație în acest exemplu:



Examinați al treilea și ultimul pachet al handshake-ului.

Ce flag (sau flag-uri) este setat? _____

Numerele relative de secvență și de confirmare sunt setate la 1 ca punct de pornire.Conexiunea TCP este acum stabilită, iar comunicația între calculatorul sursă și serverul de web poate începe.

f. Închideți programul Wireshark.

Reflecție

1. Există sute de filtre disponibile în Wireshark.O rețea mare ar putea avea numeroase filtre și mai multe tipuri diferite de trafic.Care trei filtre din listă pot fi utile unui administrator de rețea?

_____

.

2. În ce alte feluri ar putea fi utilizat Wireshark într-o rețea de producție?

_____