Lucrarea de laborator nr.1.

Lucrul cu analizorul de protocoale de reţea Wireshark

Un instrument util pentru observarea mesajelor schimbate între două entităţi ale unei reţele de calculatoare, în timpul executării unor protocoale, este analizorul de protocoale de reţea. Acest analizor, denumit şi "*packet sniffer*", reţine (prin copiere) mesajele transmise şi recepţionate de un computer, le arhivează şi afişează conţinutul diferitelor câmpuri ale protocoalelor.

Figura 1 arată structura unui astfel de analizor, care se prezintă ca un software alcătuit din două părţi:

- **Biblioteca pachetelor capturate**, care reţine o copie a fiecărui cadru de la nivelul legăturii de date, transmis sau recepţionat de computer. Reamintim că mesajele schimbate prin protocoalele de nivel înalt (HTTP, FTP, TCP, UDP, DNS, sau IP), sunt încapsulate în cadre la nivelul legăturii de date (link), care sunt transmise prin mediul fizic (eventual cablu Ethernet).
- **Analizorul de pachete**, care afişează conţinutul câmpurilor din mesajul protocolului. Pentru aceasta, analizorul trebuie "să înţeleagă" structura tuturor mesajelor schimbate prin protocoale.

De exemplu, dacă se afişează diferitele câmpuri ale mesajelor schimbate de protocolul HTTP, analizorul de pachete identifică în formatul cadrului Ethernet, datagrama IP. Analizează apoi formatul datagramei, astfel încât poate extrage segmentul TCP, din a cărui structură extrage mesajul HTTP. Din analiza acestuia, de exemplu, discerne că primii octeţi ai mesajului conţin anumite cuvinte ("POST", "HEAD").

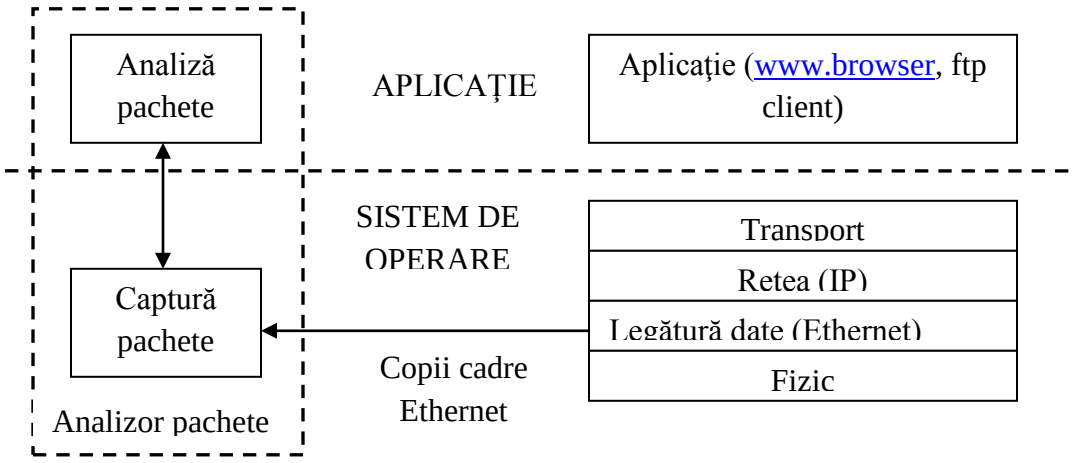

Figura 1 - Structura analizorului de pachete

În cursul laboratoarelor vom folosi analizorul de pachete Wireshark (http://www.wireshark.org/)

În scopul înţelegerii conţinutului mesajelor aparţinând protocoalelor transmise şi recepţionate la diferite nivele ale stivei de protocoale, Wireshark este disponibil sub Windows, Linux, Mac, iar ghidul de utilizator se poate descărca de la adresa http://www.wireshark.org/docs/wsug. El poate opera în calculatoare care folosesc Ethernet, Token-Ring, FDDI, LAN-uri wireless şi reţele ATM.

Interfaţa grafică

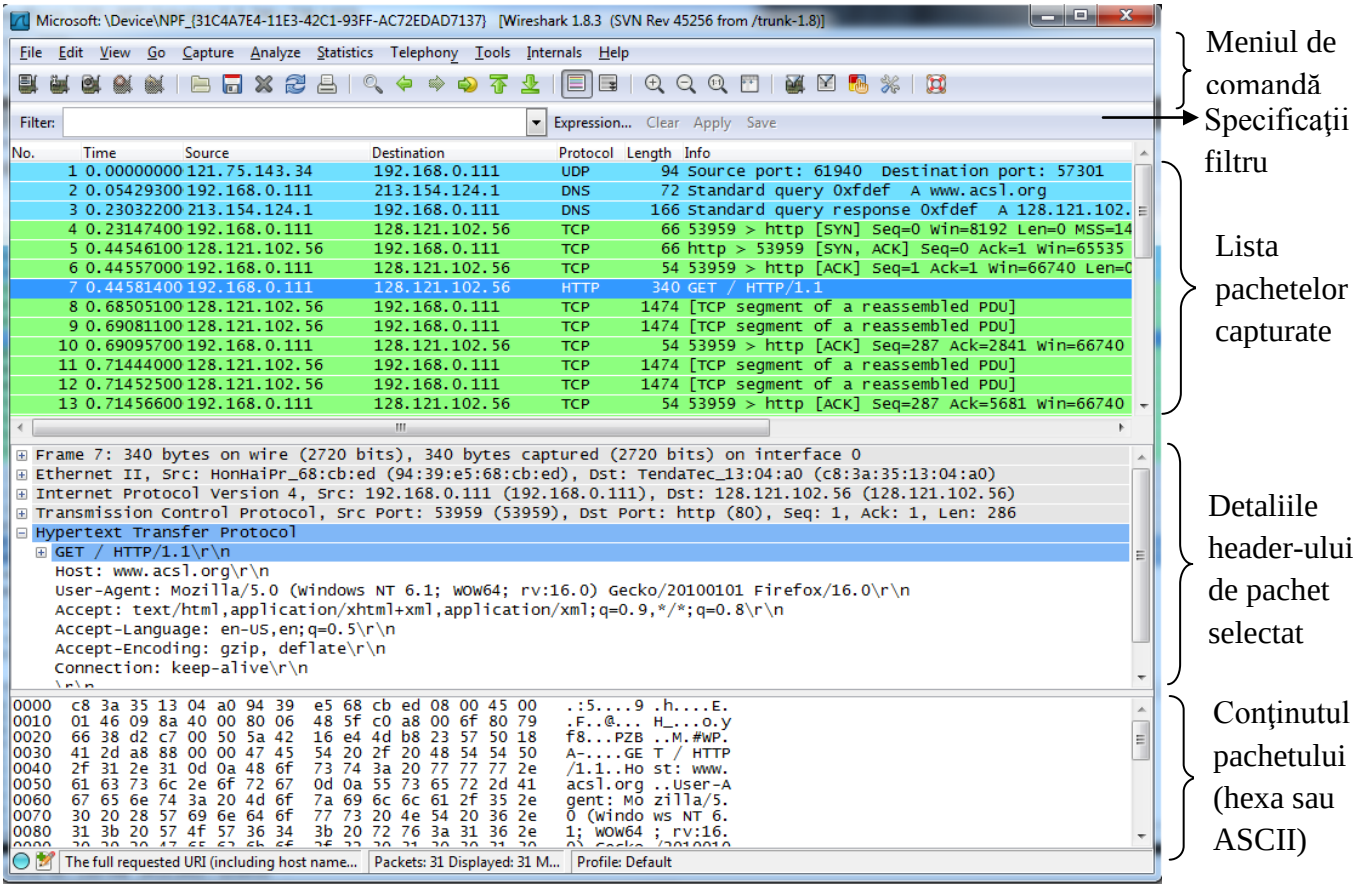

Figura 2 - Model de interfaţă grafică Wireshark

Meniul de comandă conţine, pentru prima lucrare, submeniurile „File” şi „Capture”. „File” permite salvarea datelor pachetelor capturate, sau accesarea datelor referitoare la capturile precedente şi părăsirea aplicaţiei Wireshark. “Capture” permite începerea capturării pachetelor.

Specificaţiile filtrului reprezintă câmpul în care se introduc numele protocolului şi alte informaţii referitore la datele din lista pachetelor capturate cu privire la heder-ul şi conţinutul pachetului.

Lista pachetelor capturate, se referă la fiecare pachet capturat, prin numărul de ordine asignat de Wireshark, momentul la care a fost capturat, adresele sursei şi destinaţiei, tipul de protocol şi informaţia specifică a protocolului conţinută în pachet. Lista pachetelor poate fi sortată după oricare din aceste categorii, printr-un click pe numele coloanei. În coloana tipului de protocol sunt listate protocoalele de cel mai înalt nivel cu care sunt transmise sau recepţionate pachetele.

Detaliile header-ului de pachet selectat, furnizează amănuntele referitoare fiecărui pachet selectat din lista de pachete capturate (pentru selecţia unui pachet din listă, pe linia pachetului respectiv, daţi click pe butonul stâng al mouse-lui). Detaliile includ informaţii despre cadrul Ethernet şi despre datagrama IP conţinută în pachet. Cantitatea de informaţii de la nivelele Ethernet şi IP poate fi majorată sau minimizată printr-un click în pătratele cu plus şi minus din stânga liniilor cu cadre Ethernet sau datagrame IP. Dacă pachetul a fost transportat prin TCP sau UDP, vor fi afişate detaliile TCP sau UDP, care pot fi la fel majorate sau minimizate. În final sunt furnizate detaliile aferente protocolului de cel mai înalt nivel, cu care a fost transmis sau recepţionat pachetul.

Conţinutul pachetului se referă la întregul conţinut al cadrului capturat în format hexazecimal sau ASCII.

Lucrul cu analizorul de protocoale de reţea WIRESHARK

Computerul cu care se lucrează va fi conectat la Internet prin interfaţa cablată Ethernet. Se parcurg următorii paşi:

1. Se accesează un browser web.

2. După instalarea soft-ului Wireshark, la deschiderea acestuia se va vedea o fereastră asemănătoare cu cea din Figura 2, fără a fi prezente informaţiile referitoare la lista de pachete, header-ele sau conţinutul pachetelor, deoarece Wireshark nu a capturat încă nimic.

3. Din bara de comenzi superioară, se selectează submeniul *Capture* şi de aici se alege *Options*. Această comandă va determina apariţia ferestrei din Figura 3.

4. Se pot utiliza valorile setate din această fereastră cu excepţia “Hide capture info dialog” care se va dezactiva. Interfeţele de reţea (conexiunile de la nivelul fizic) ale computerului, vor fi prezentate în căsuţa de dialog “Interface”, unde trebuie făcută o alegere prin selectarea interfeţei prin care se vor transmite şi recepţiona pachetele. După selectarea interfeţei de reţea se dă click pe butonul “Start”. Din acest moment începe capturarea pachetelor transmise şi recepţionate de computerul la care se lucrează.

5. Odată începută capturarea pachetelor, va apare o fereastră (Figura 4) în care se sintetizează numărul de pachete capturate de diferite tipuri şi în care există şi butonul “Stop” pentru oprirea operaţiei de capturare. Nu opriţi deocamdată capturarea!

6. În timp ce Wireshark lucrează accesaţi următorul URL:
   1. http://standards.ieee.org/about/get/802/802.3.html

Pentru a afişa această pagină browser-ul ales de dumneavoastră va contacta serverul HTTP la *standards.ieee.org* şi va schimba mesaje HTTP cu serverul pentru a descărca această pagină. Cadrele Ethernet care conţin aceste mesaje HTTP vor fi capturate de Wireshark.

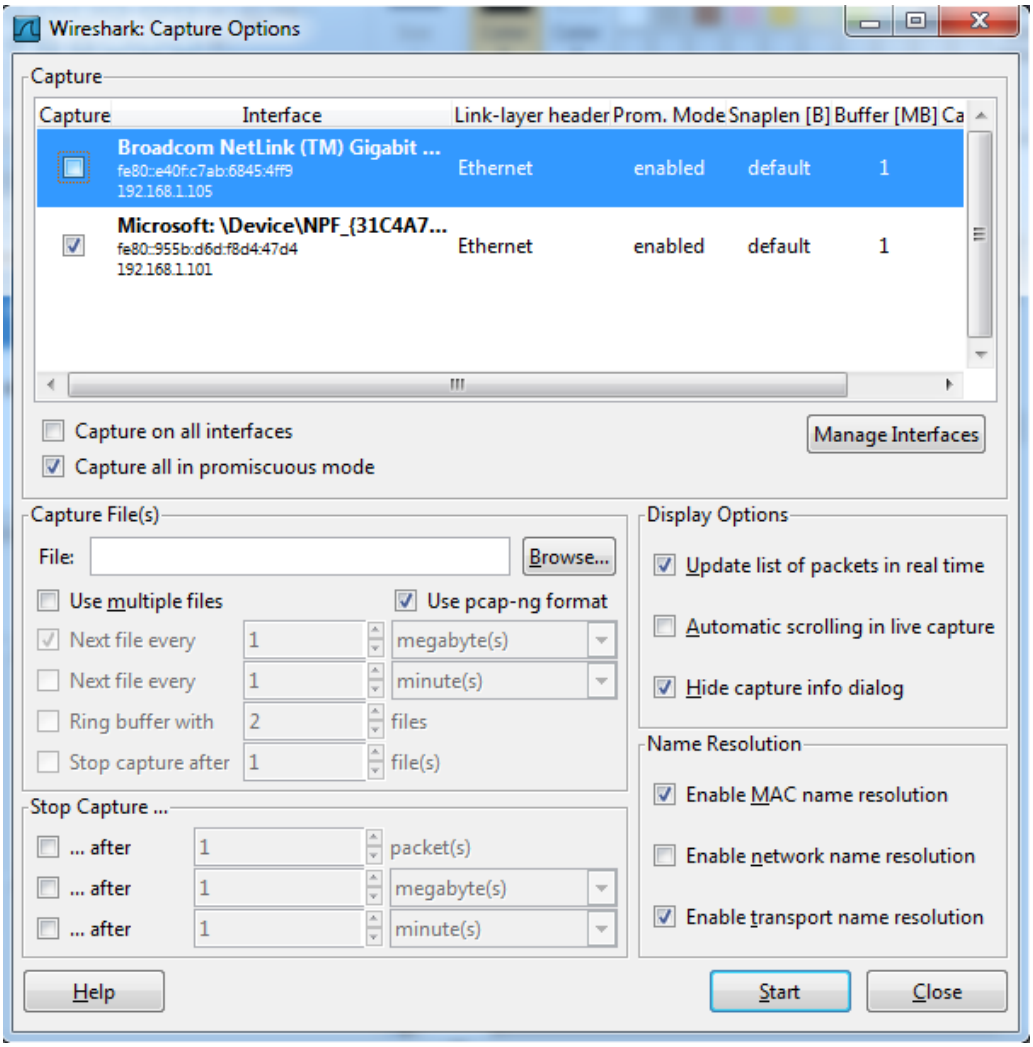

Figura 3 - Fereastra opţiunilor de captură Wireshark

7. După ce browser-ul a afişat pagina *802.3.html*, se opreşte capturarea pachetelor prin selectarea butonului "Stop" din fereastra de captură Wireshark.

Această fereastră va dispărea şi va apare fereastra principală (asemănătoare cu cea din Figura 2) în care se vor vedea toate pachetele capturate. Aici se vor afla toate pachetele care conţin mesajele protocoalelor schimbate între computerul dumneavoastră şi alte entităţi din reţea. Mesajele HTTP schimbate cu serverul web *standards.ieee.org* vor apare undeva în lista de pachete capturate. În acelaşi timp vor exista multe alte tipuri de pachete, corespunzătoare diferitelor tipuri de protocoale afişate în coloana "Protocoale".

Chiar dacă singura acţiune a fost descărcarea unei pagini web, există multe alte protocoale care rulează pe computer, fără să fie văzute de utilizator. Vom învăţa mai târziu despre ele.

8. Scrieţi http (fără ghilimele) în câmpul de specificaţii de filtru, din partea de sus a ferestrei principale Wireshark. Apoi selectaţi "Apply", în partea dreaptă . Această comandă va afişa doar mesajele HTTP în lista de pachete.

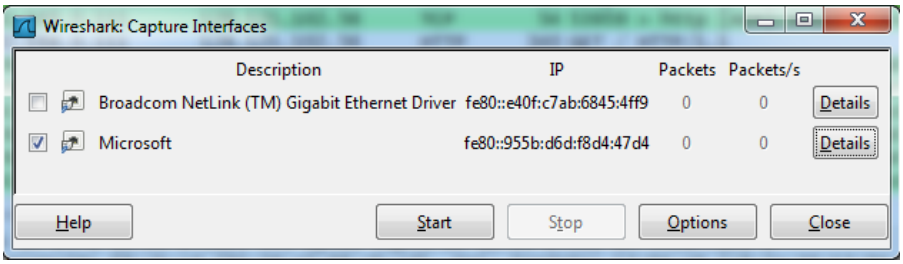

Figura 4 - Interfeţele de captură Wireshark

9. Selectaţi primul mesaj http din lista pachetelor capturate. Acesta poate fi mesajul HTTP GET care a fost transmis de serverul *standards.ieee.org*.

Când selectaţi mesajul HTTP GET , în fereastra cu detaliile header-ului de pachete vor fi afişate informaţiile legate de cadrul Ethernet, datagrama IP, segmentul TCP şi header-ul mesajului HTTP. Remarcaţi că în cadrul Ethernet este conţinută (încapsulată) datagrama IP, care conţine la rândul ei segmentul TCP şi care segment conţine mesajul de la serverul web "standards.ieee.org".

Prin click pe săgeţile dreapta şi jos din partea stângă a ferestrei cu detaliile pachetelor, se minimizează informaţiile referitoare la cadrul Ethernet, IP şi TCP. Maximizaţi informaţiile legate de protocolul HTTP şi minimizaţi informaţiile legate de toate celelalte protocoale. Acum, fereastra afişată va arăta ca în Figura 5.

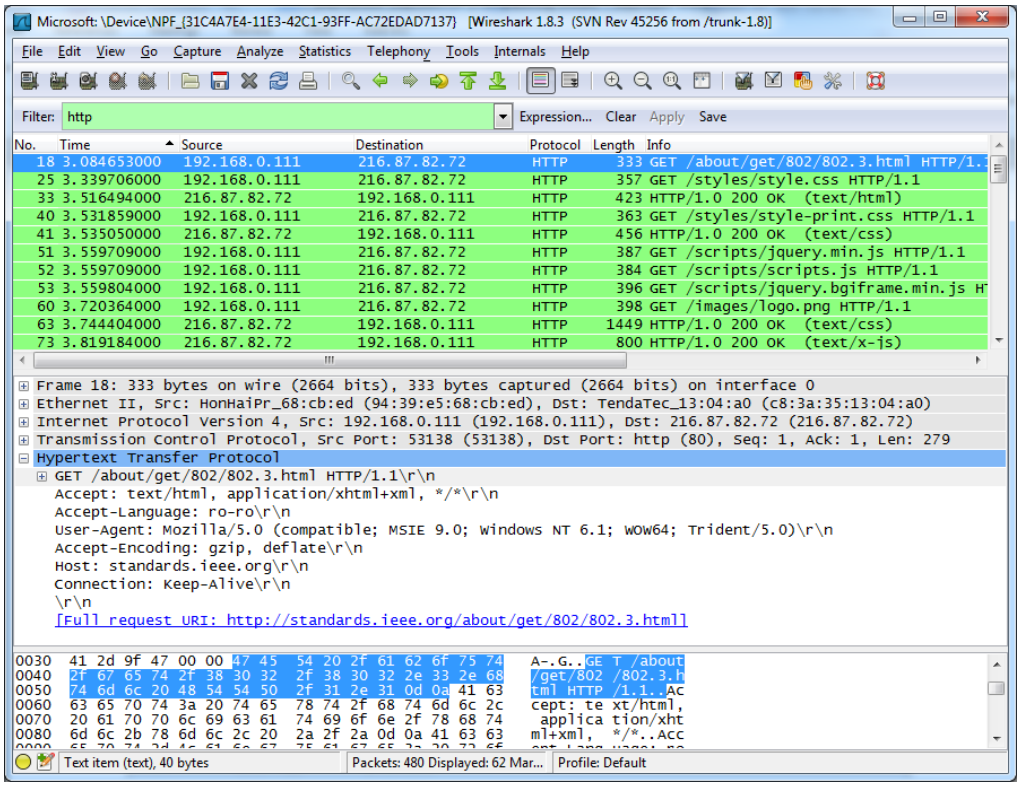

Figura 5 - Fereastra Wireshark după pasul 9

Scopul laboratorului

Desfăşurarea acestui laborator are ca scop introducerea în procedura de lucru cu analizorul de protocoale de reţea, Wireshark.

Răspundeţi la următoarele întrebări pentru confirmarea înţelegerii capabilităţilor soft-ului Wireshark.

1. Enumeraţi o serie de protocoale care apar în coloana de protocoale nefiltrate de la pasul 7.

2. Care este durata între transmiterea mesajului HTTP GET şi recepţionarea răspunsului HTTP GET? (În coloana “Time” din lista de pachete se măsoară timpul în secunde din momentul începerii capturării. Pentru a se afişa timpul current se selectează submeniul “View/Display Format/Time of day”).

3. Care este adresa de Internet pentru *standards.ieee.org*? Care este adresa de Internet a computerului dumneavoastră?

4. Tipăriţi la imprimantă două mesaje „http” din pasul 9. Pentru aceasta selectaţi “Print” din meniul „File”, selectaţi „Selected Packet Only” şi „Print as displayed”, după care daţi comanda OK.