Universitatea Tehnică a Moldovei
Departamentul Ingineria Software şi Automatică

Raport

Lucrarea de laborator Nr.5

la disciplina
P.R.

A afectuat: st.gr.TI-142 Chirica Alexandru

A verificat lector asistent Ostapenco Stepan

Chişinău 2017

Tema: Inginerie inversă în rețea.

Obiectiv: Căpătarea unor deprinderi în lucrul cu aplicația Wireshark care ne permite să analizăm traficul de pachete din rețea.

Scopul lucrării: Obținerea capacităților de analiză a traficului internet și a cunoștințelor practice de utilizarea a analizatorului de pachete WireShark și a avantajelor sale.

Noțiuni teoretice

Ingineria inversă (în engleză reverse engineering) este procesul de descoperire a principiilor de funcționare a unui dispozitiv sau sistem prin analiza structurii, funcției și operațiilor acestuia. De obicei, ingineria inversă implică dezasamblarea sau descompunerea sistemului sau dispozitivului respectiv și analizarea în detaliu a funcționării sale, cu scopul de a realiza un nou dispozitiv sau sistem similar, care nu copiază nimic din cel original. In acelasi timp hackerii o folosesc pentru a sparge sistemele informattice.[1]

Un analizator de pachete (de asemenea , cunoscut ca un analizor de rețea , analizor de protocol sau de sniffer de pachete, pentru anumite tipuri de rețele , Ethernet sau Wifi) este un program de calculator sau o bucată de hardware care poate intercepta și jurnal de trafic care trece peste un convertor digital de rețea sau o parte a unei rețele. Sniffer -ul capturează fiecare pachet și, dacă este necesar, decodifică datele brute de pachete, arătând valorile diferitelor câmpuri din pachet, și analizează conținutul acestuia în conformitate cu corespunzătoare RFC sau alte specificații.[2]

Wireshark este aplicație de tip sursă deschisă care monitorizează pachete de date. Este utilizată pentru soluționarea problemelor în rețea, pentru analiza traficului, dezvoltarea produselor software și a protocoalelor de comunicare, în scopuri educaționale. Inițial, aplicația se numea Ethereal, dar în mai 2006 proiectul a fost redenumit în Wireshark din cauza problemelor legate de marca comercială.[3]

Efectuarea lucrării

Sarcina

Găsirea unui link pe care se află o imagine în orice format, studierea traficului în momentul accesării acestei pagini, extragerea octeților primiți de pe această resursă și salvarea acestora într-un fișier care corespunde tipului imaginii de pe resursă.

Realizarea

Primul pas în efectuarea acestui laborator a fost instalarea aplicației Wareshark, după aceasta la rulare se alege placa de rețea care trebui să fie urmărită în privința traficului de pachete. Interfața aplicației la prima rulare.(Fig. 1).

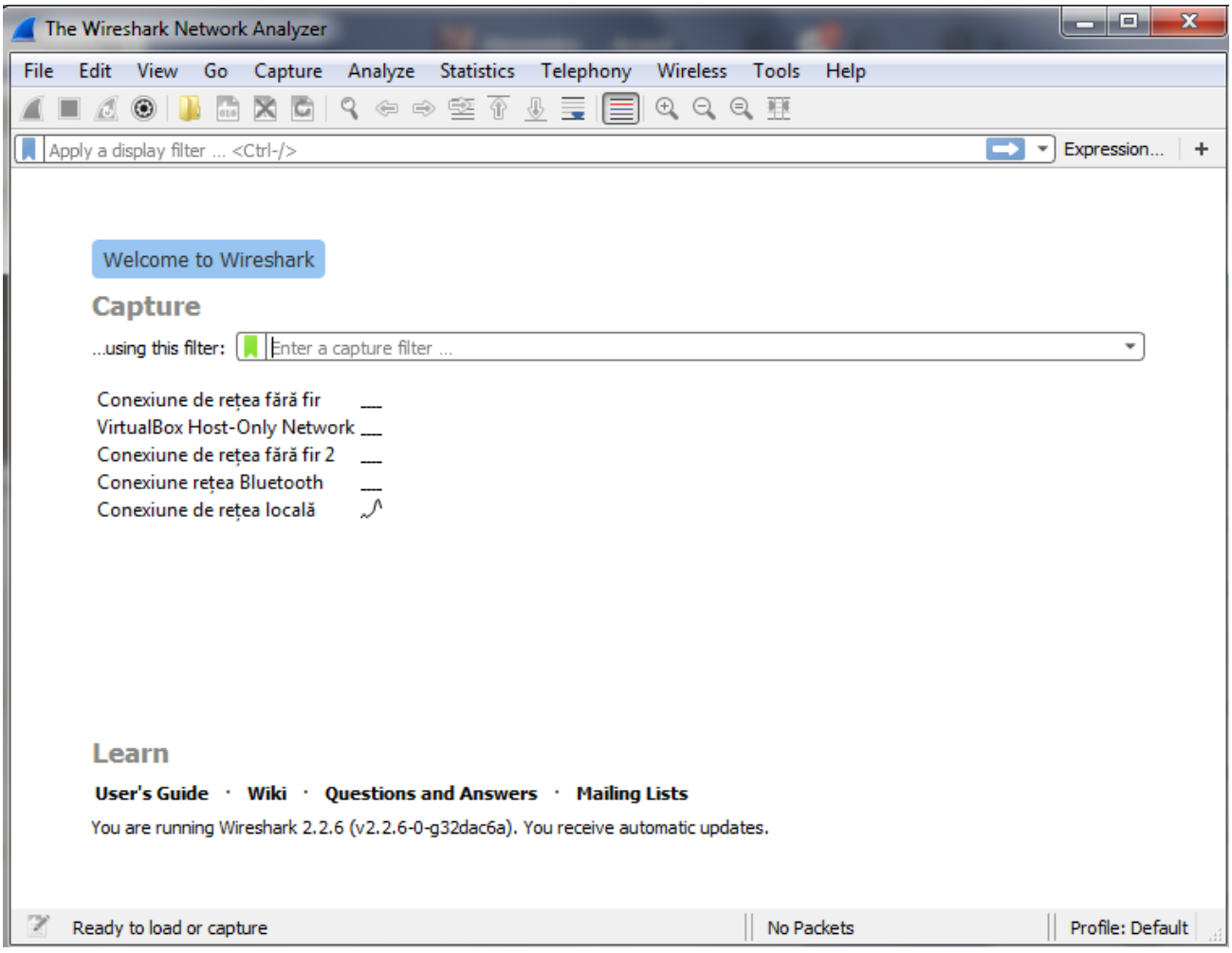

Figura 1. Fereastra alegerei interfeței ascultate

După ce a fost aleasă placa se rulează analizatorul de pachete. În figura 2 este reprezentată aplicația în momentul cînd este analizat tot traficul din rețea.

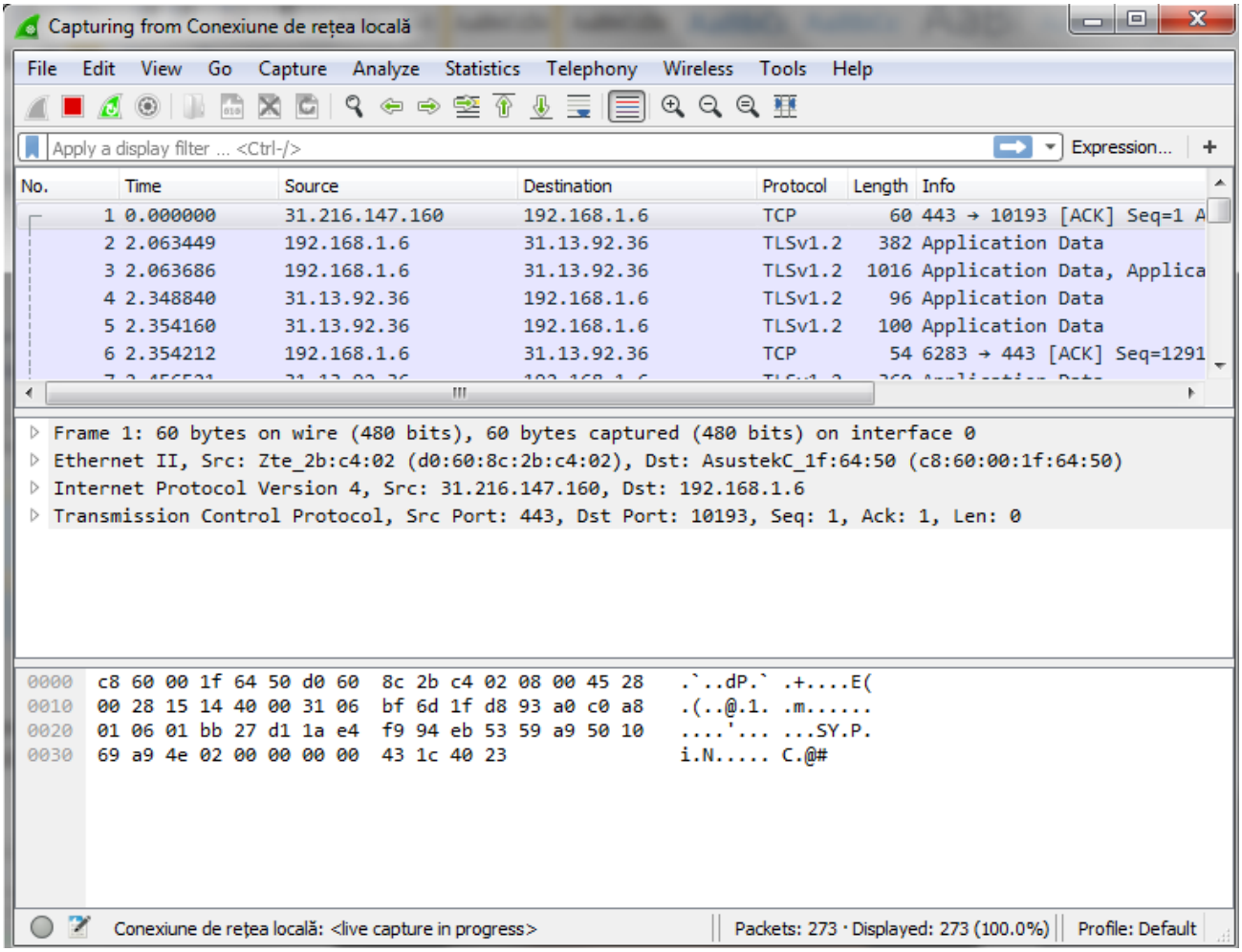

Figura 2. Modul de funcționare a aplicației

Primul pas în recepționarea imaginei este alegerea sursei și analiza request-ului din browser pentru filtrarea frame-ului necesar din tot fluxul existent(Fig. 3).

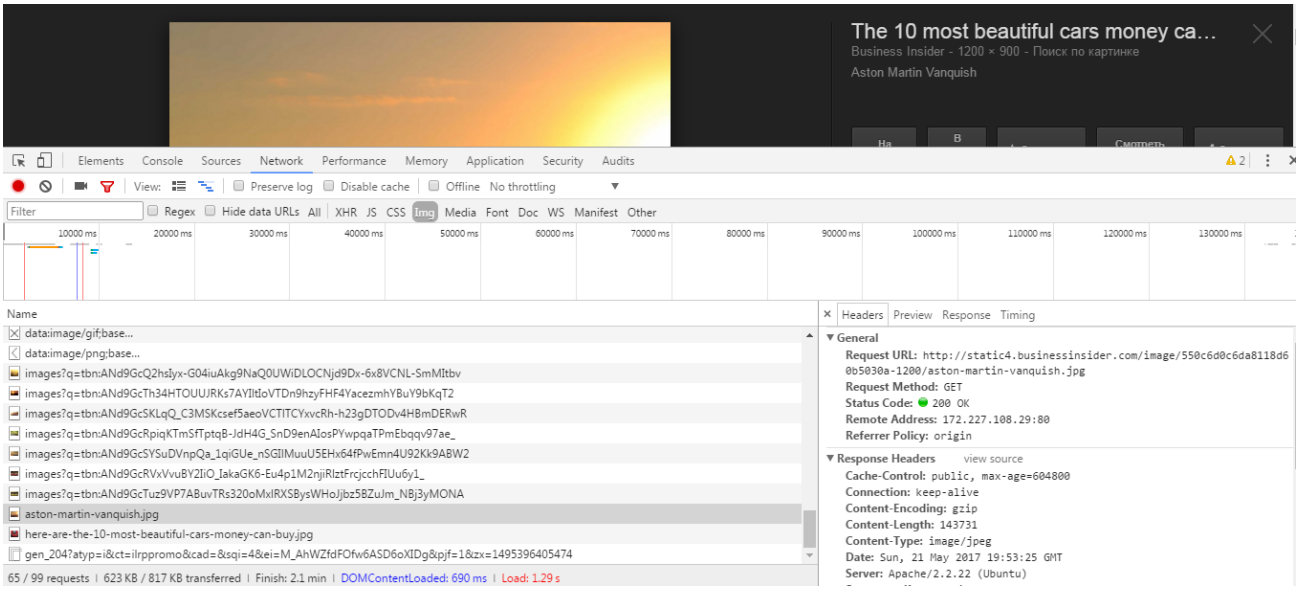

Figura 3. Analiza requestului către imagine

Pentru receptarea rapidă a imaginei folosim opțiunea de filtrare a aplicației Wireshark(Fig. 4) și găsim frame-ul imaginei necesare.

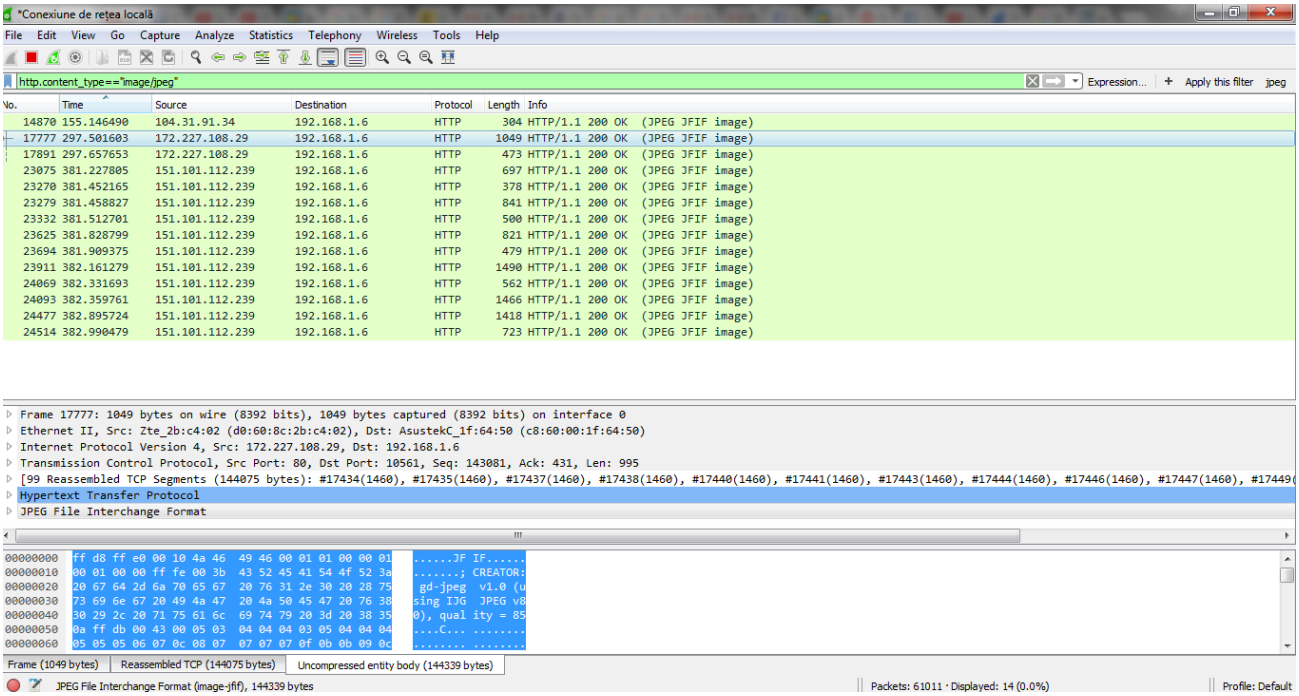

Figura 4. Filtrarare imaginilor jpeg

Alegem frame-ul necesar și vizionăm structura internă a frame-lui, acolo găsim imaginea transmisă(Fig. 5), și o exportam (Fig. 6).

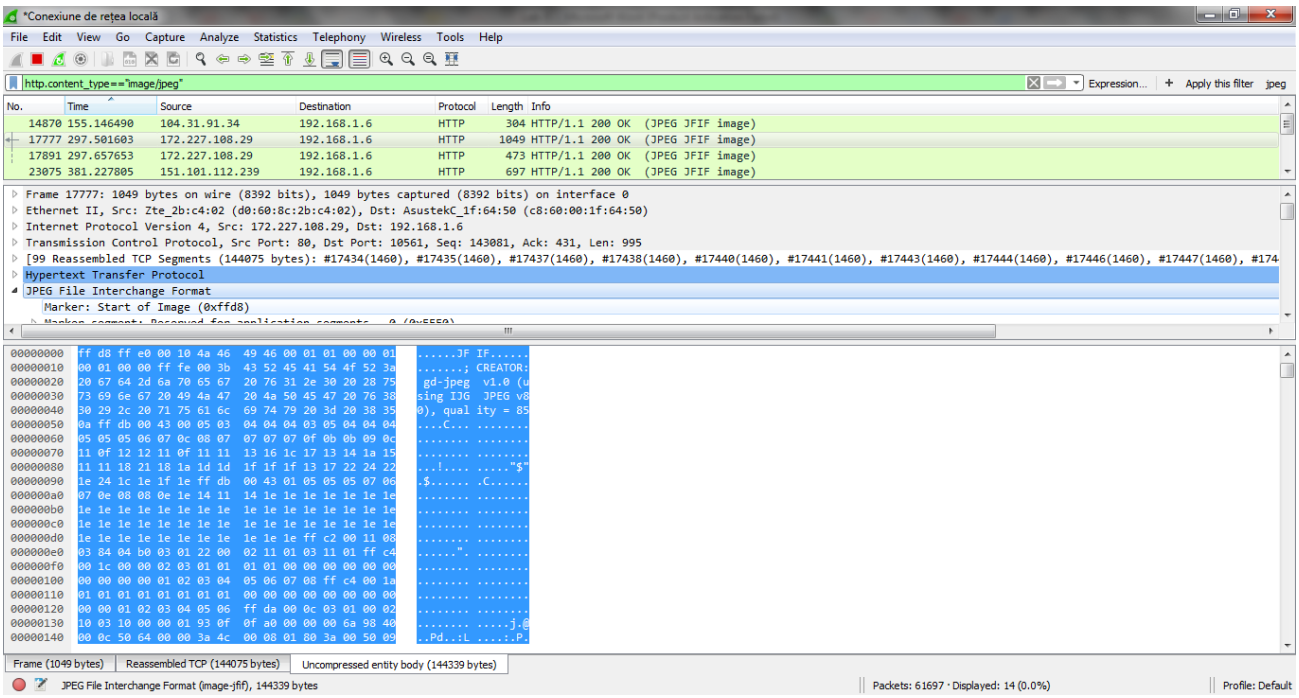

Figura 5. Fișierul jpeg

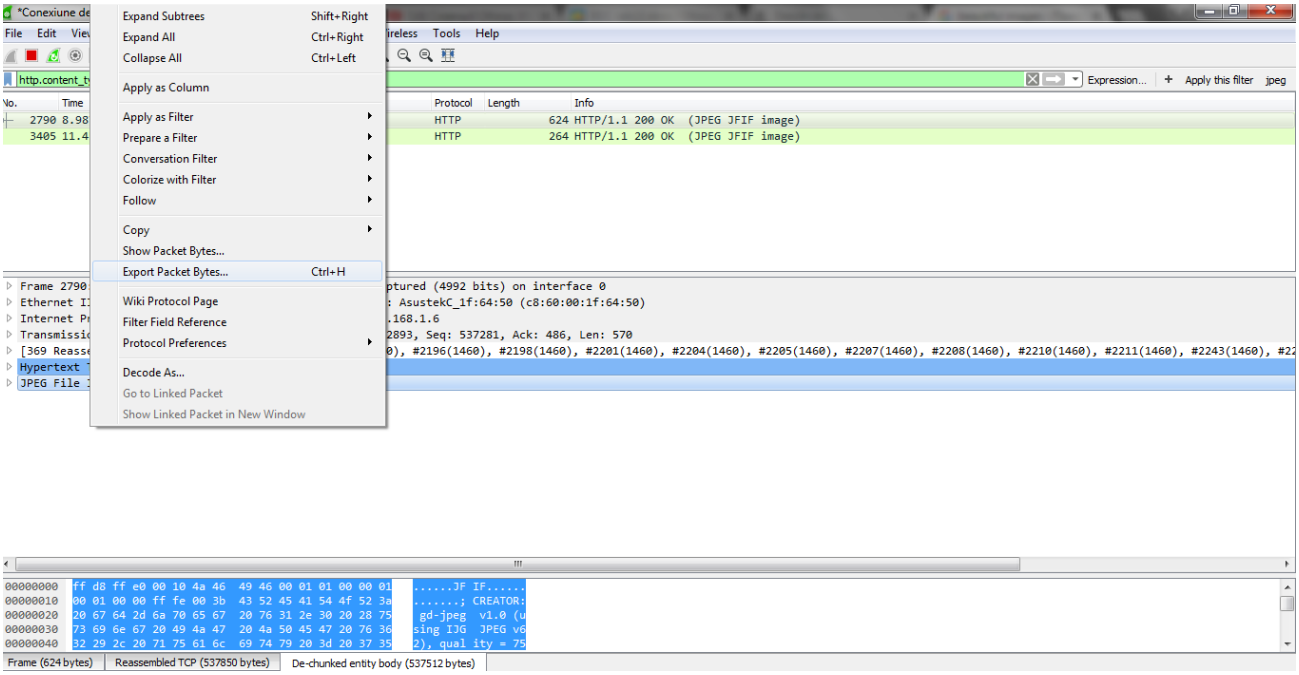

Figura 6. Exportarea bitilor

Pasul următor constă în vizualizarea bitilor ASCII(Fig. 7), și salvarea în formatul JPEG. În rezultat obținem imaginea dorită (Fig. 8) .

Figura 7. Rezultatul coneversiei în ASCII

Figura 8. Imaginea obținută

Concluzie

În urma efectuării lucrării de laborator Nr.5 la PR am obținut cunoștințe despre analiza și ascultarea traficului de rețea cu ajutorul aplicației Wireshark care reprezintă una din cele mai avansate aplicații de analiză a pachetelor(sau sniffer eng.).

Cu ajutorul analizatorului de pachete acum am înțeles mai bine structura frame-ului și a protocoalelor, și putem cerceta traficul în studierea procesului de comunicare a aplicațiilor instalate și depistarea transmiterilor malițioase.

Referințe

[1] Wikipedia https://ro.wikipedia.org/wiki/Inginerie_invers%C4%83 10.05.2017 10:00
[2] Wikipedia https://en.wikipedia.org/wiki/Packet analyzer 10.05.2017 10:05
[3] Wikipedia https://ro.wikipedia.org/wiki/Wireshark 10.05.2017 10:10