Ministerul Educației a Republicii Moldova

Universitatea Tehnică din Moldova

Facultatea Calculatoare, Informatică și Microelectronică

Raport

La disciplina: Pogramarea în rețea

Lucrarea de laborator nr.6

Tema: “Inginerie inversă în rețea”

A efectuat:Chicu Roman.

Studentul grupei TI-142

A verificat: Ostapinco Stepan

Chișinău 2017

**Obiective**

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

**Link la repozitoriu:** https://github.com/logan11116/lab5

**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.

**Mersul Lucrării**

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

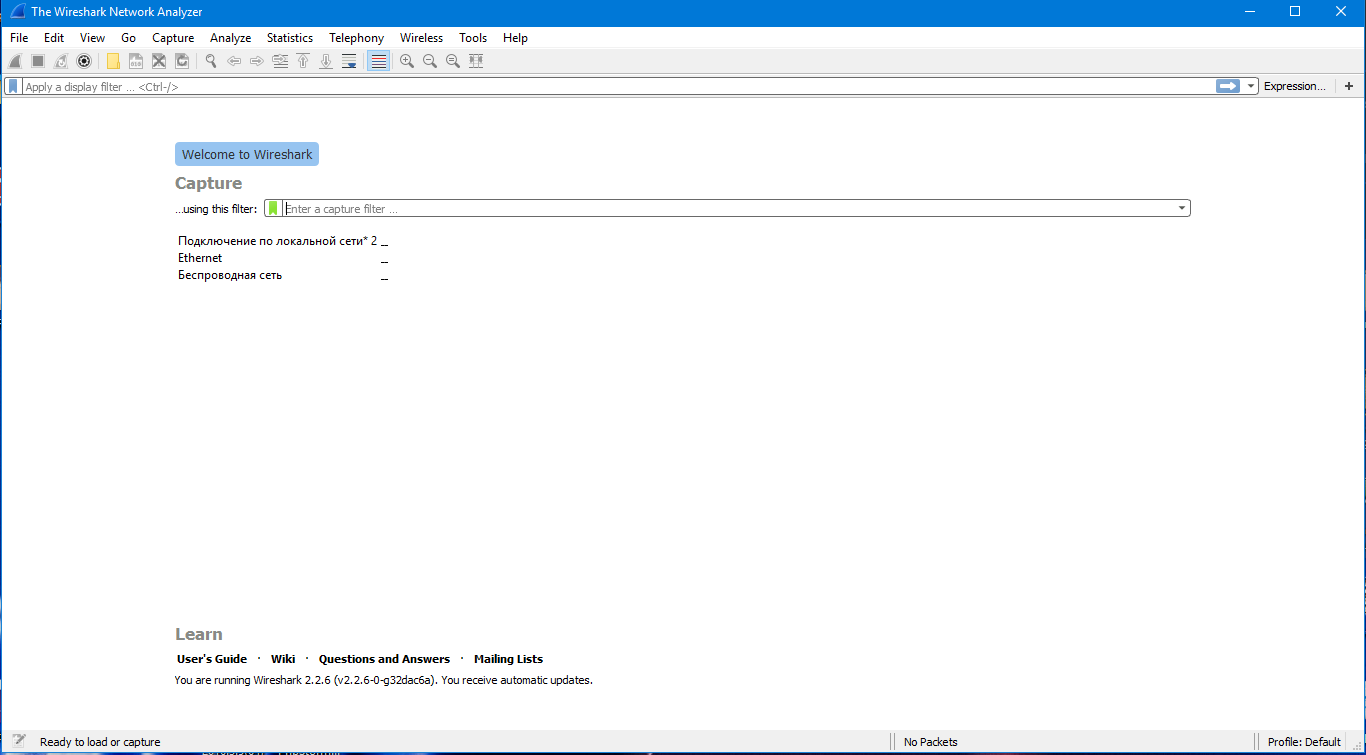


Figura 1 – Interfața de bază a Wireshark-ului

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.

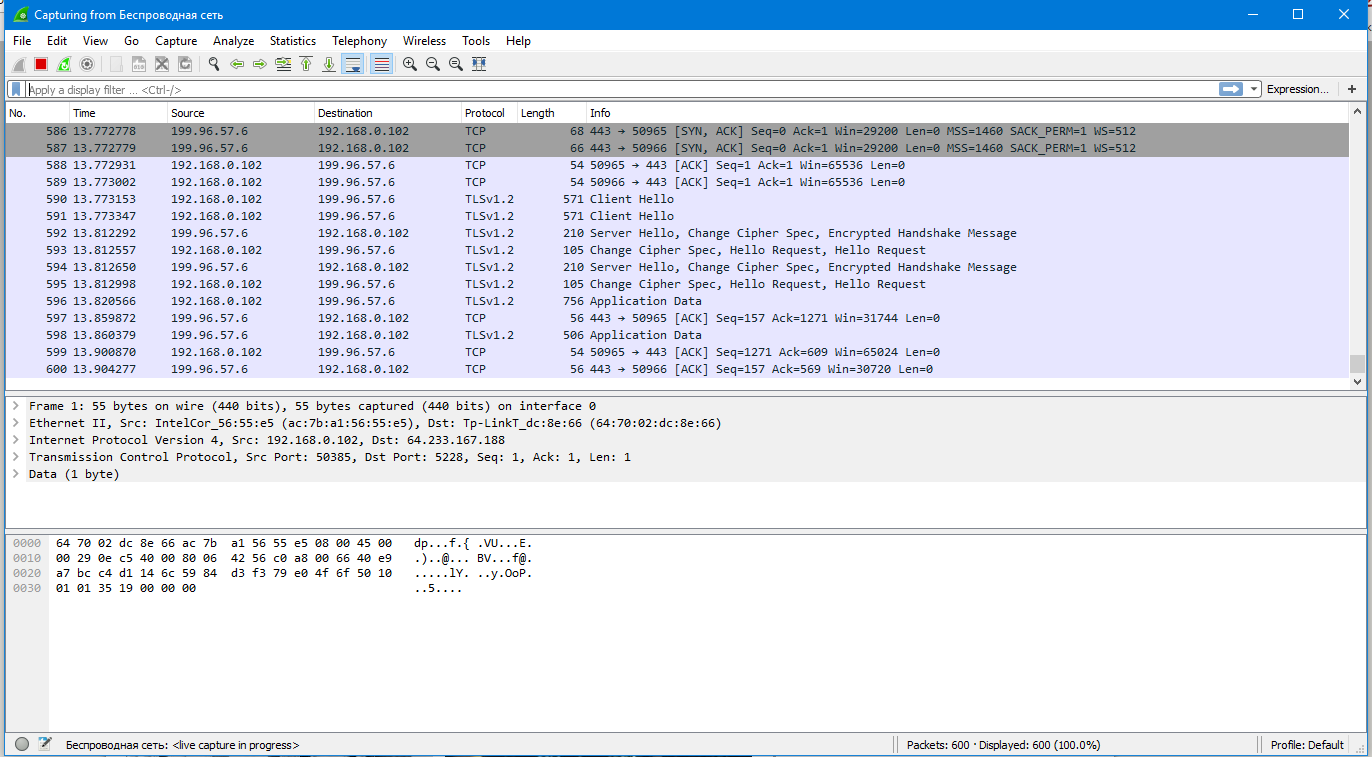


Figura 2 – Aplicația în momentul cînd este activ analizatorul de pachete

Pentru a salva o imagine pe local a fost accesat linkul <http://imdb.com/,> ceea ce este prezent pe această pagina web este reprezentat în Figura 3.

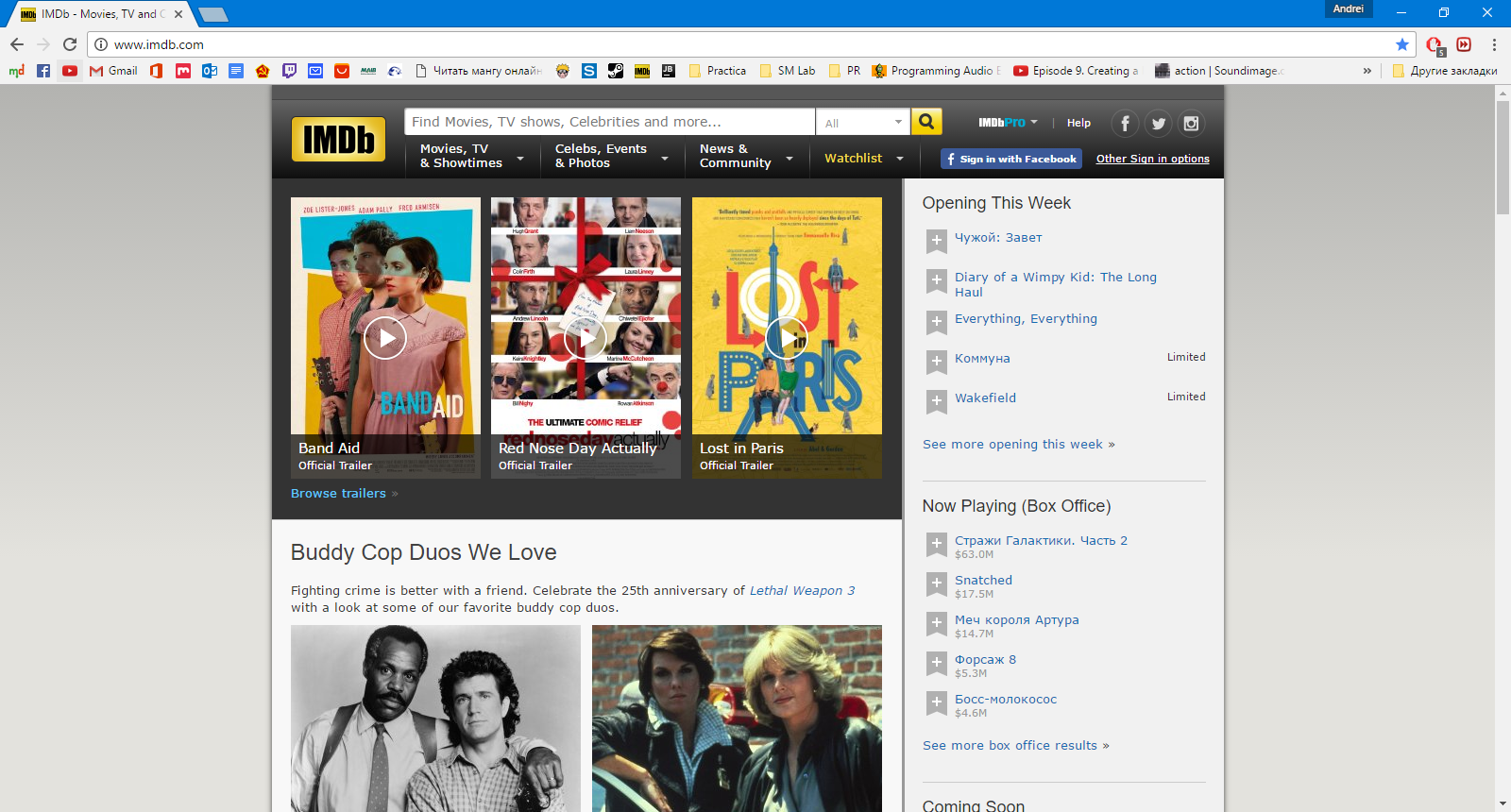


Figura 3 – Conținutul paginii de pe care urmează să fie salvată o imagine local

În *Wareshark* se indică filtrul *http* ceea ce înseamnă că se va afișa doar lista de pachete primite prin intermediul protocolului *http.*Pentru a obține cu ușurință resursa dorită folosim comanda *http.refer contains imdb.com* (Figura 4).

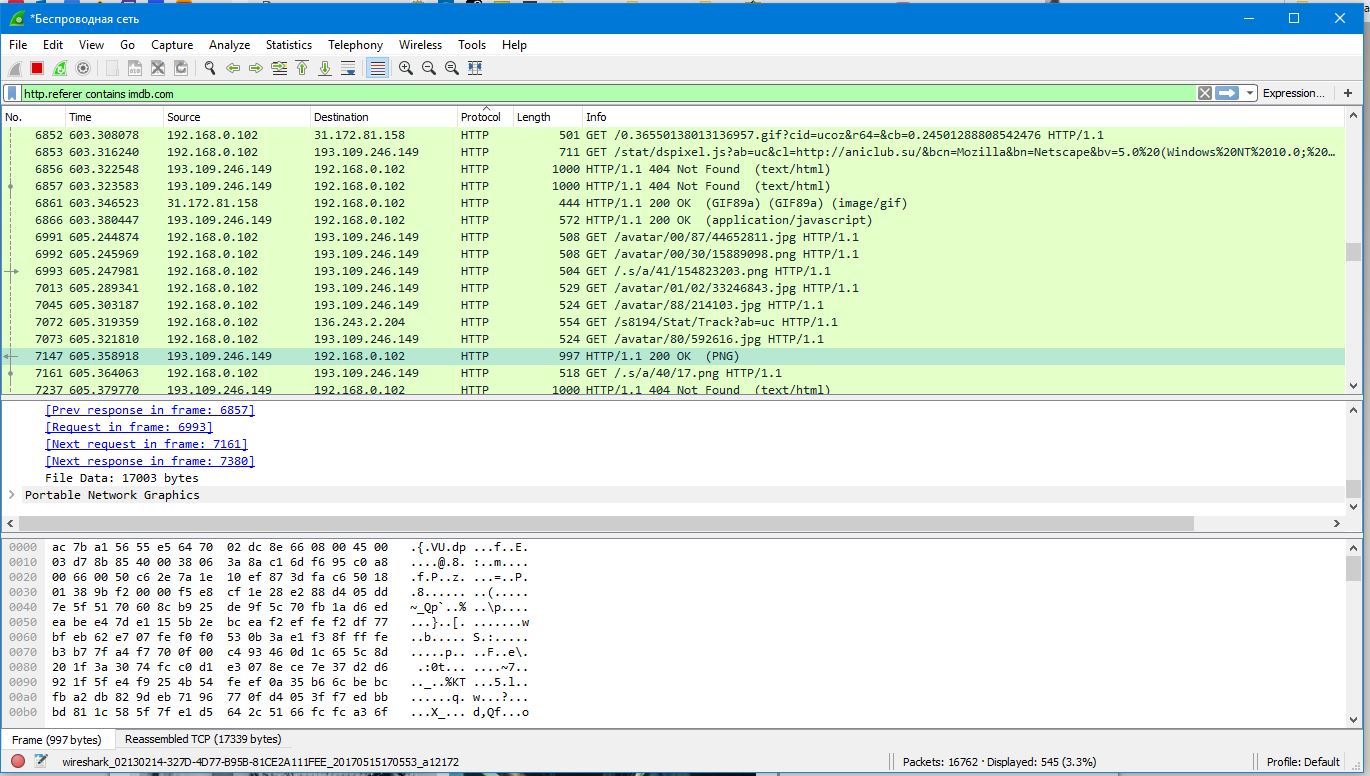


Figura 4 – Filtrarea după http.refer contains imdb.com

Următorul pas reprezintă salvare imaginei găsite. Pnetru asta se face click drept pe File Data și se allege opțiunea Export Packet Bytes ( Figura 5).

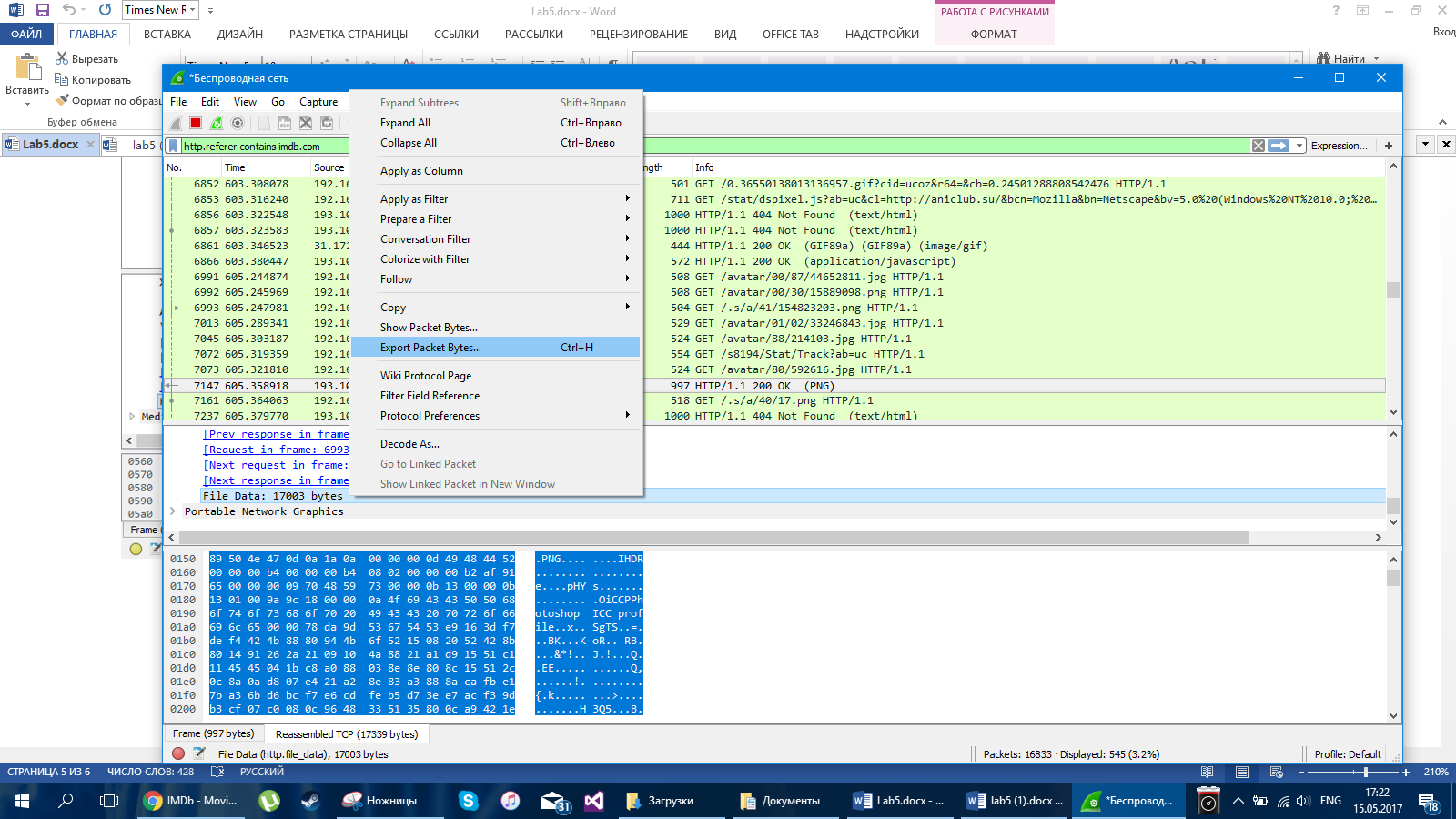


Figura 5 – Export Packet Bytes

Apoi se alege denumirea fișierul și se indică extensia acestuia (Figura 6).

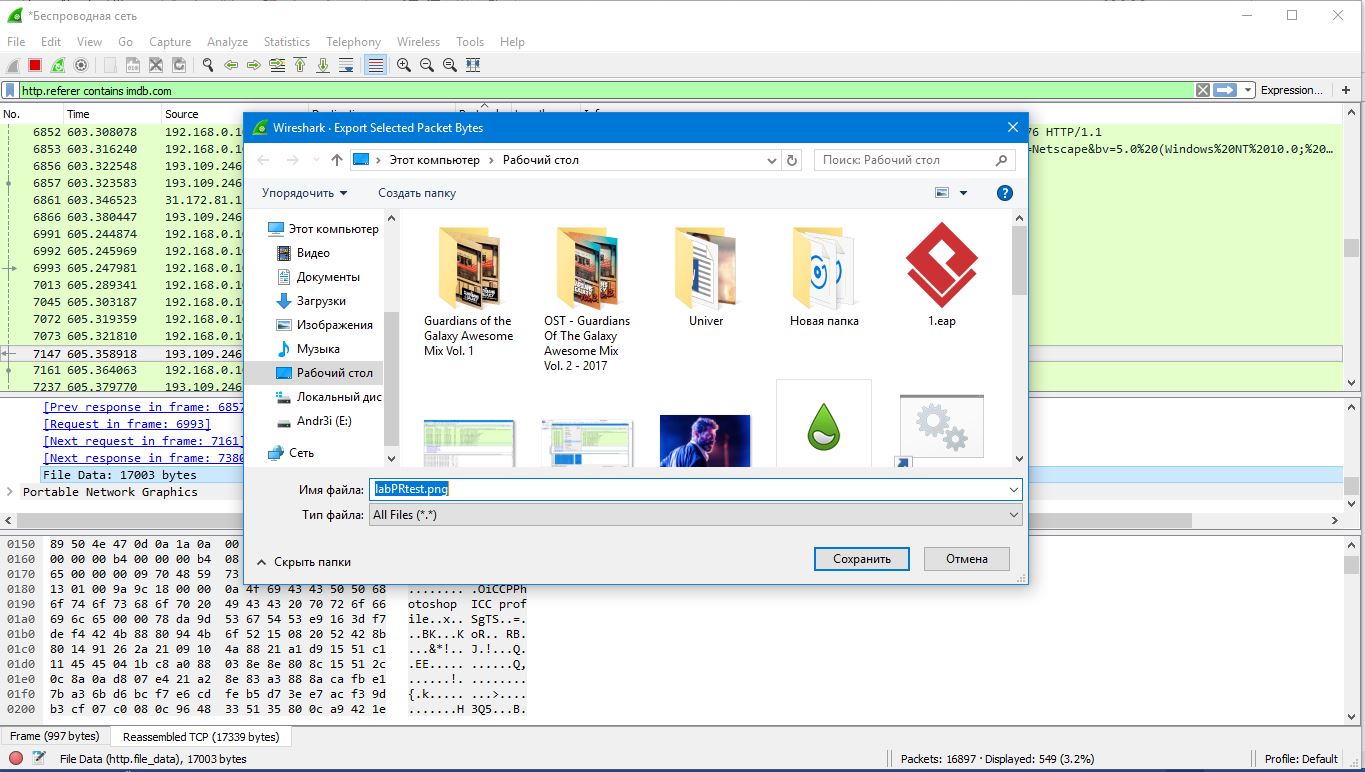


Figura 6 – Salvarea imaginei

# Rezultatul obținut este indicat în Figura 7.

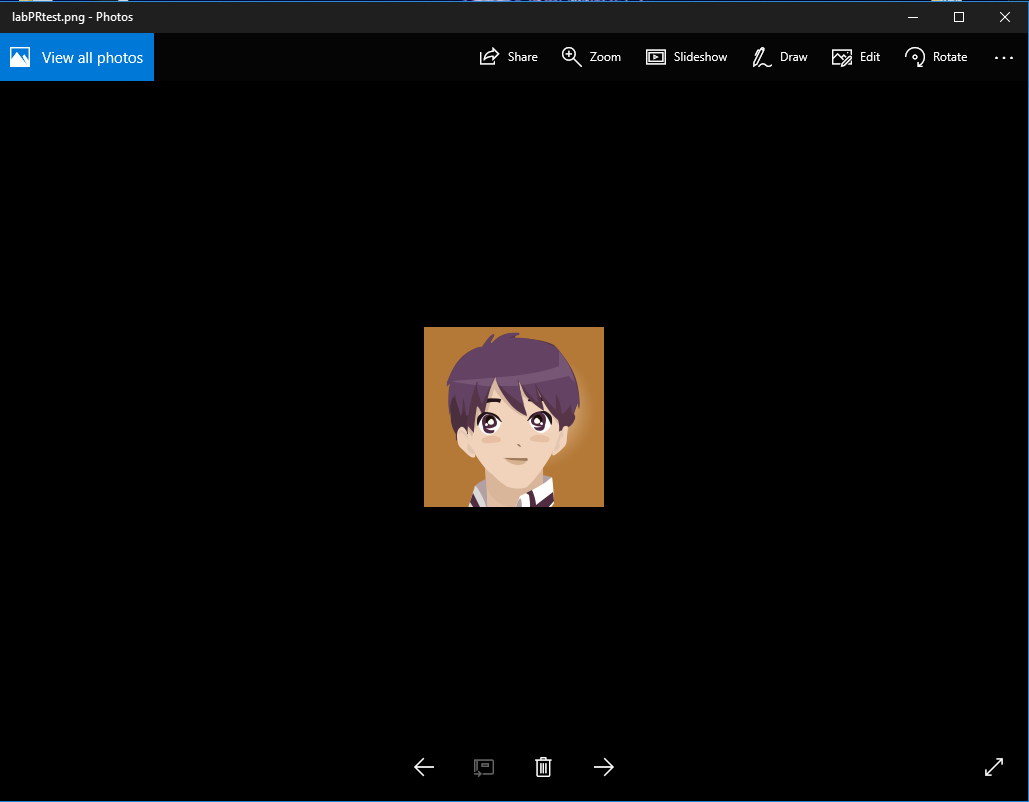


Figura 7– Imaginea obținută

Acum vom extrage o piesă pe care o ascultăm pe un sait de muzică online figura 8. Important de menționat că piesa se transmite subformă de fragmente/segmente de date.

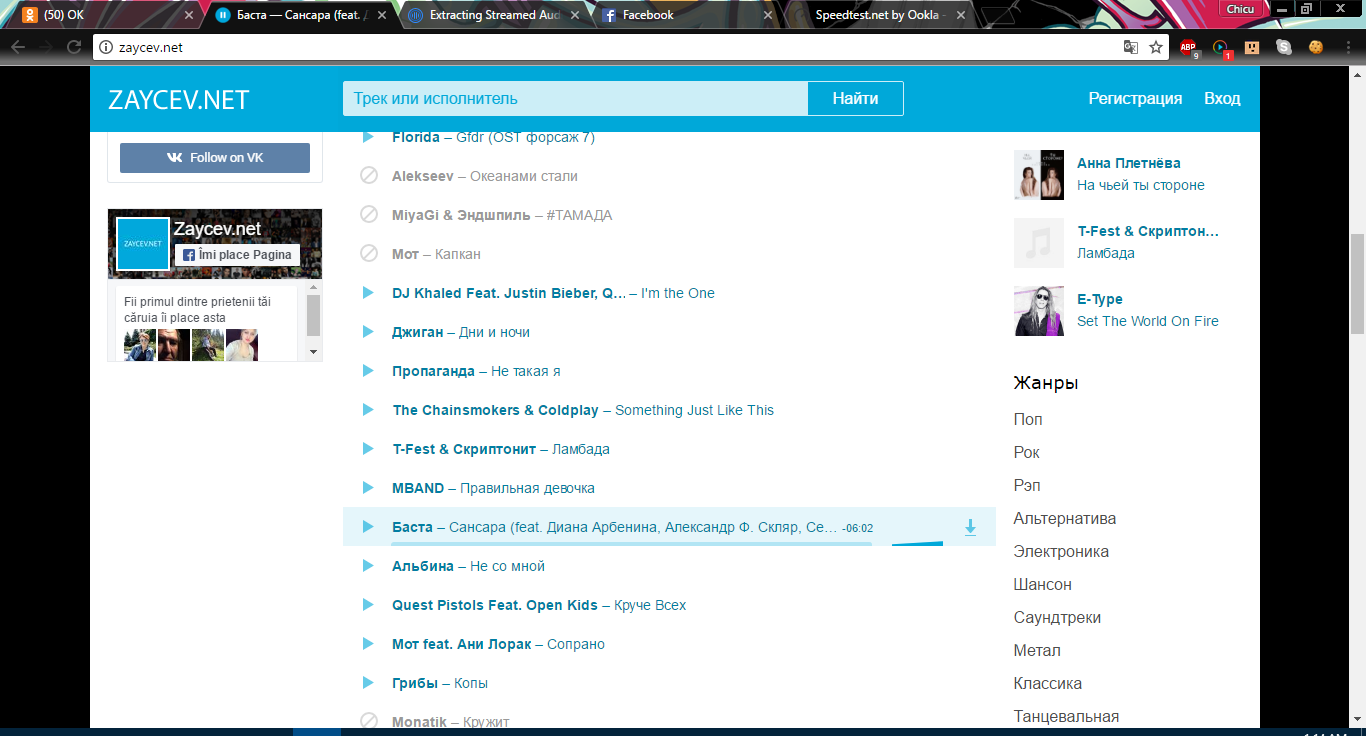


Figura 8. Site <http://zaycev.net/>

Primim pachetele de date prin intermediul protocolui TCP. Acest protocol folosește așa numita strîngere de mînă în 3 pași: syn,syn-ack,ack figura 9

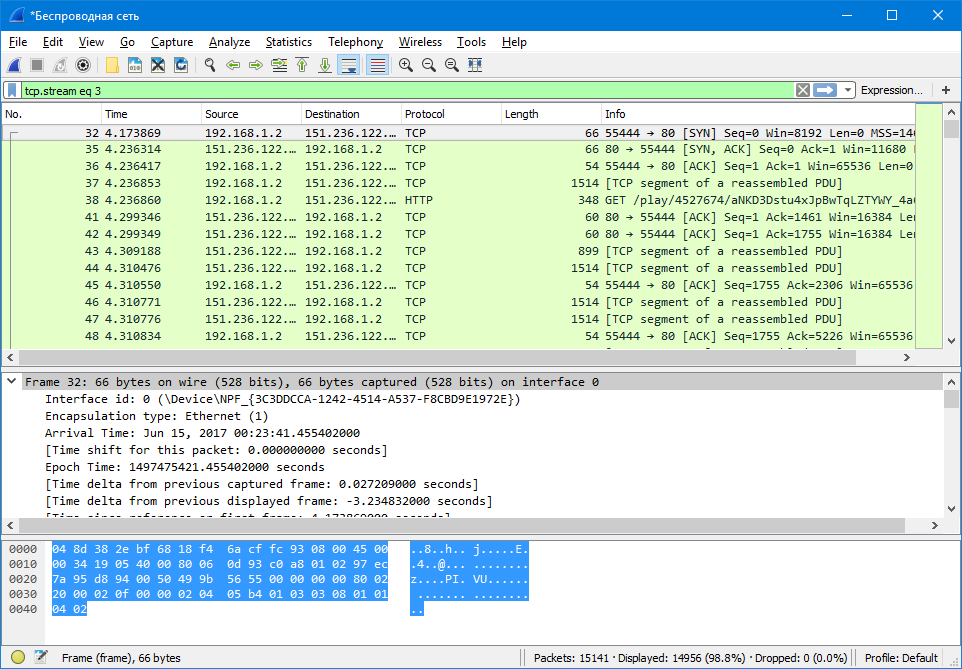


Figura 9. Primirea fișierului audio in TCP

Pentru a putea salva masivul de date primit este necesar să efectuăm o conversie a datelor figura 10.

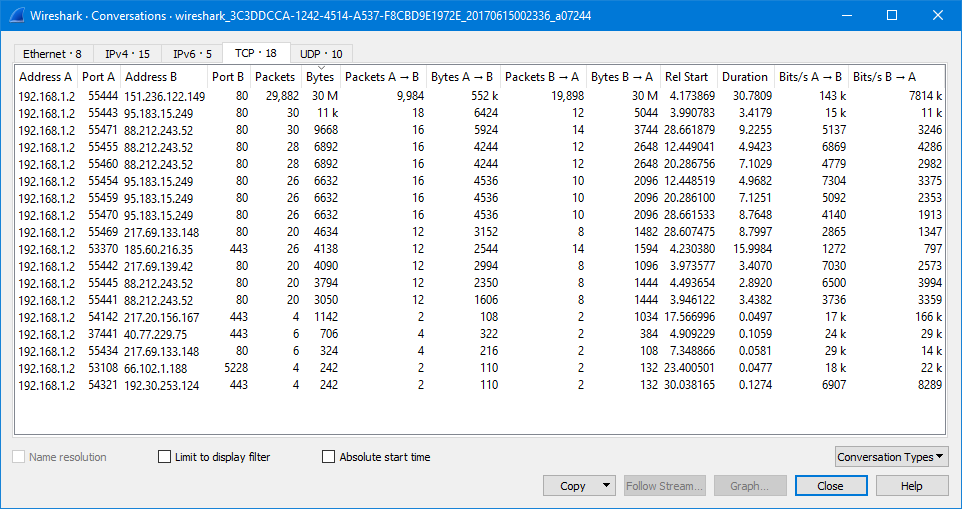


Figura 10. Conversia datelor

Salvăm datele convertite.Se obține un fișier de biți care necesită de a fi redenumit cu extensia .mp3. Ulterior el poate fi deschis cu ajutorul unui player figura 11.

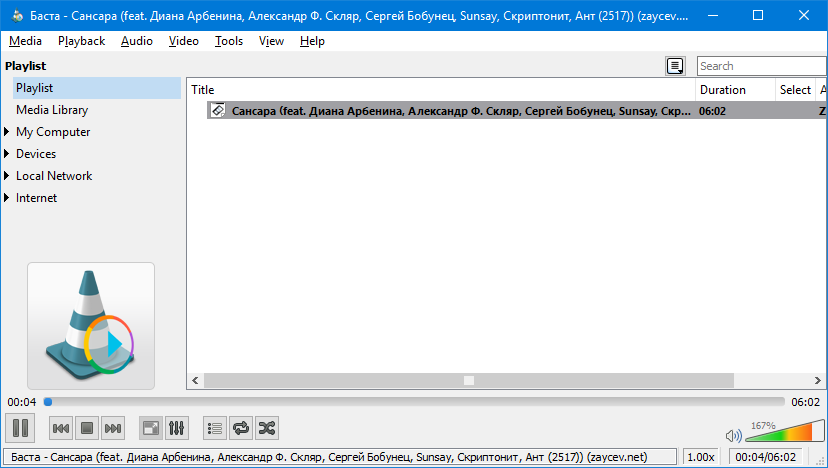


Figura 11. Redarea fișierului audio

Wireshark este o aplicație care monitorizează traficul în internet. În combinație cu alt program Cain and Abel este foarte ușor de folosit pentru furturile în rețea. Deci Wireshark analizează traficul in rețea , iar Cain and Abel (figura 12) face ca tot traficul al altor PC din aceiași rețea să treacă prin Wireshark. În calitate de victim voi folosi un dispozitiv mobil.

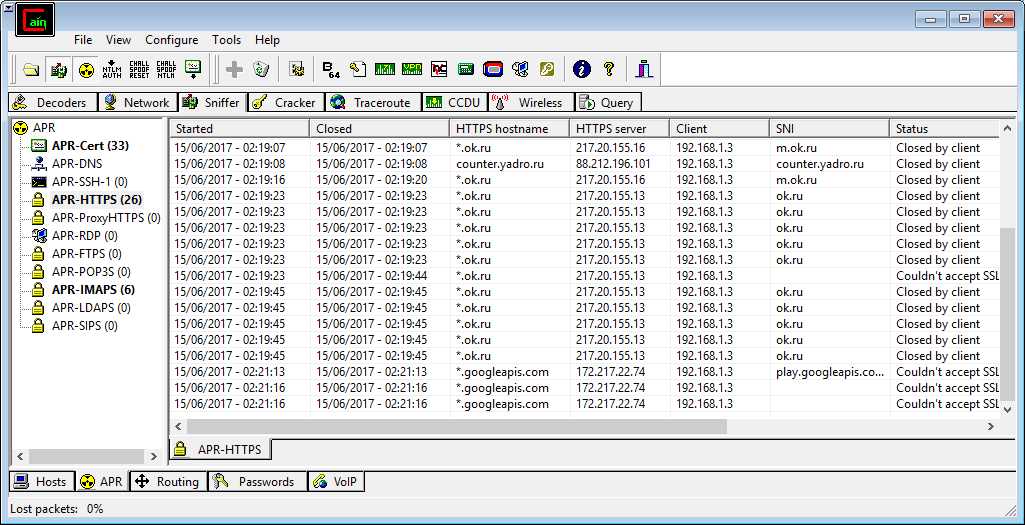


Figura 12. Reprezentarea datelor străine

Cu ajutorul wireshark au fost strinse datele de acces al dispozitivului mobil. Victima navigînd pe unul din saiturile de socializare ok.ru a pus la dispoziție unele id-uri de autentificare. Indetificăm cookie de accest strînse de wireshark figura 13.

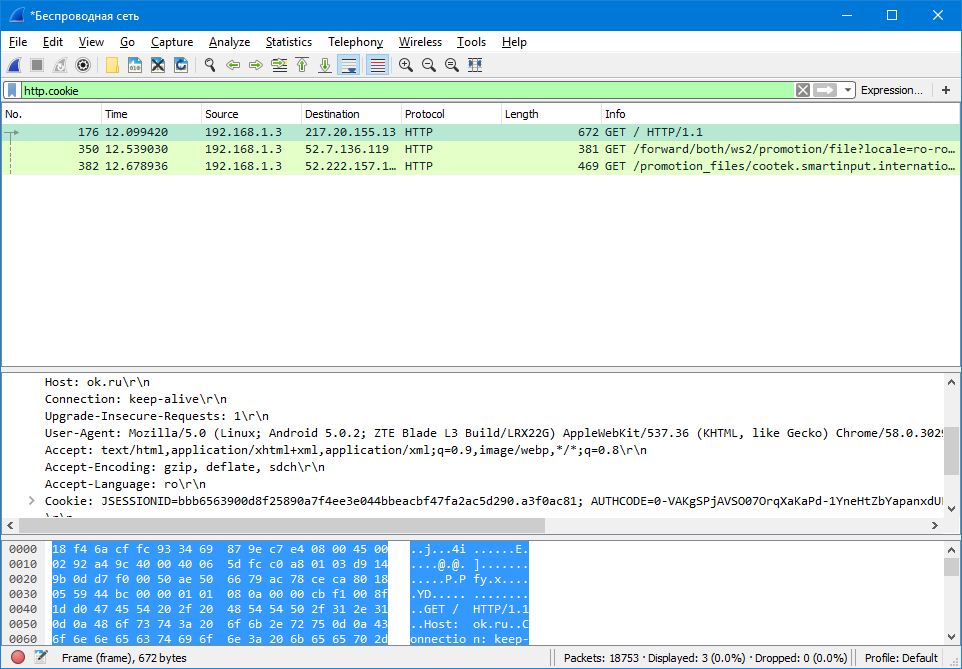


Figura 13. Reprezentare cookie acces

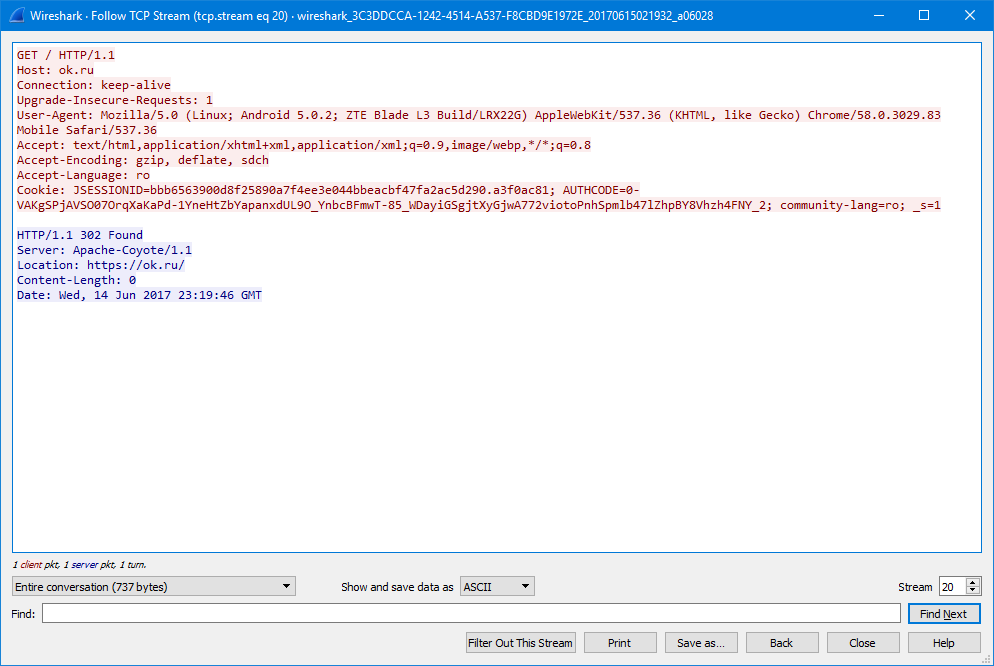


Figura 14. Repezentăm prin intermediul TCP stream datele

Instalăm o app pentru chrome EditThisCookie unde vom introduce cîteva cîmpuri de autentifiacare de pe ok.ru. Cîmpurile de acces care determină utelizatorul sunt următoarele JSESSIONID= și AUTHCODE=. Introducem în EditThisCookie acestea și reîncărcăm pagina figura 15,16.

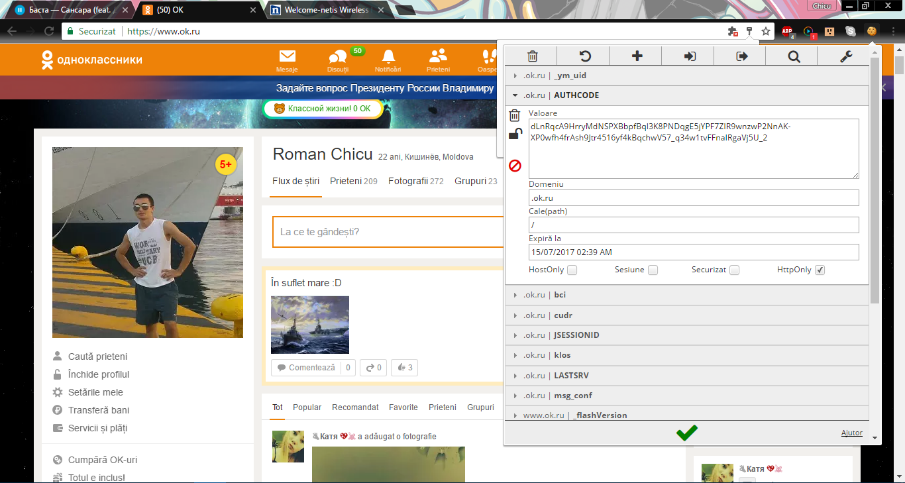


Figura 15. Introcudem cookie

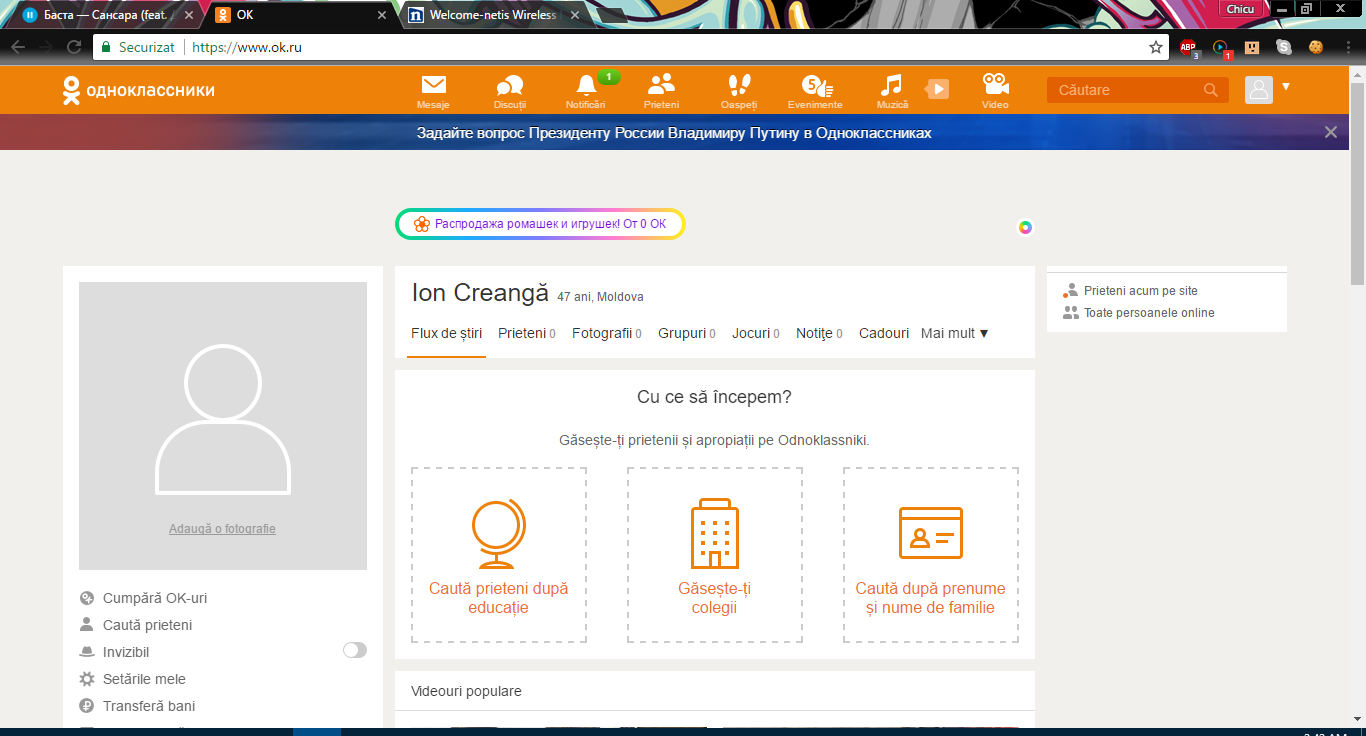


Figura 16. Accesul la profil străin

**Concluzie**

În această lucrare de laborator am căpătat primele deprinderi în lucrul cu aplicația **Wireshark**care servește analizator de pachete care circulă prin rețea în momentul interacțiunii calculatorului local cu serverele web.

Pentru a găsi mai ușor informația dorită am folosit filtrul http.refer contains imdb.com*.* Acest filtru ne permite din mulțimea de pachete care circulă să afișăm doar pe acelea de care avem nevoie și prin aceasta minimizăm cheltuielile de timp în momentul cînd căutăm ceva concret.