MINISTERUL EDUCATIEI REPUBLICII MOLDOVA

UNIVERSITATEA TEHNICA A MOLDOVEI

Facultatea „Calculatoare, Informatică și Microelectronică”

Departamentul Automatica și Tehnologii Informaționale

RAPORT

Programarea în rețea

Lucrare de laborator Nr. 5

Tema: Ingineria inversă în Rețea

A elaborat: st. gr. TI-142 Țurcan Tudor

A verificat: asist. univ. Donos Eugenia

Chișinău 2017

Cuprins

Scopul lucrării

Analizatorul de pachete Wireshark.

Sarcina lucrării

De identificat fluxul de octeți prin care are loc transmiterea imaginilor unui site. De salvat stream-ul în fișier corespunzător formatului.

Analizator de trafic de rețea(Wireshark)

Analizoarele de trafic de rețea sunt în general instrumente software care sunt capabile să capteze și să analizeze traficul transmis sau recepționat de către un calculator care este conectat într-o rețea. Aceste instrumente pot fi utilizate atât în scop de studiu al funcționării protocoalelor de rețea (mecanisme, structura cadrelor etc), cât și pentru îmbunătățirea funcționalității și a securității rețelei. Cele mai multe dintre aceste instrumente se descarcă gratuit de pe Internet, unele dintre ele fiind chiar părți integrante ale unor sisteme de operare. Câteva analizoare de rețea (uneori denumite în limba engleză "packet sniffer") des folosite sunt: Ethereal, Wireshark (versiunea nouă a lui Ethereal), tcpdump (asemănător cu cele două programe anterioare, dar apelabil doar în linia de comandă), Microsoft Network Monitor (pachet suplimentar al sistemelor de operare Windows), ettercap (program ce poate fi folosit pentru capturarea parolelor transmise într-o reţea de către unele protocoale de nivel aplicaţie) etc.

Wireshark (al cărui versiune mai veche se numește Ethereal) este un pachet software gratuit care poate fi utilizat în mod interactiv pentru capturarea și analiza traficului de rețea. Acest instrument software beneficiază de o interfață grafică utilizator, care îl face simplu de utilizat. La fel ca și alte analizoare de pachete, fereastra principală din Wireshark prezintă trei imagini graduale asupra unui pachet (1).

În primul rând, o descriere sumară a pachetului, în care se dau informații de bază despre pachetul respectiv. Aceasta este completată de o fereastră de detaliu în care se dau detalii asupra protocoalelor care compun pachetul (tipul protocolului, dimensiunea headerului etc). În cele din urmă, avem imaginea exactă a șirului de octeți (codați în hexazecimal) care compun pachetul. În figura 1 se poate vedea o imagine a interfeței grafice utilizator a programului Wireshark.

Cadrele de informație sunt capturate cu ajutorul unei colecții cuprinzătoare de filtre. Aceste filtre pot fi preinstalate sau definite de către utilizator, care poate preciza ce fel de pachete să fie capturate, cât să dureze captura, dimensiunea maximă a pachetelor şi alte detalii. Mai mult decât atât, pachetele capturate pe durata unei conversaţii "TCP/IP" pot fi afişate într-un format ASCII ușor de utilizat.

Desfășurarea lucrării

Pentru a analiza pachetele ce survolează rețeaua trebuie să deschidem un browser și să accesăm o pagină web. Pagina dată va fi http://net-informations.com/about.htm unde există doar cîteva imagini. În figura 1 este reprezentată imaginea noastră, care trebuie căutată de Wireshark (2).

Fig.1 Imaginea ce necesită identificare

Aplicația Wireshark prin intermediul metodei Get va trebui să preia resursele. În momentul monitorizării rețelei de către aplicația dată sunt preluate toate datele din rețea. Pentru a utiliza doar datele ce ne interesează trebuie să le filtrăm. Pentru această în câmpul *Filter* al aplicației aplică, filtrul necesar. Expresia ce este introdusă o putem vizualiza în figura de mai jos (figura 2). Astfel noi indicăm să ne fie afișate rezultatele protocolului http din rețea, serverul fiind *URL* indicat de noi.

Fig. 2 Rezultatele filtrării

După ce am identificat pachetele ce au fost captate de aplicație facem click pe imaginea care ne interesează. Astfel accesăm fluxul de biți ce a fost transportat prin protocolul TCP.

Acum trebuie să identificăm in ce cadru a fost transmisă imaginea preluată de WireShark. Pentru asta deschidem *Hypertext Tranfer Protocol*, unde putem vizualiza că răspunsul a fost preluat in cadru 238 (figura 3). Aplicăm al filtru pentru a vedea codul de statut al cererii noastre către serverul dat. Astfel identificăm că răspunsul a fost unul pozitiv din partea serverului (figura 4).

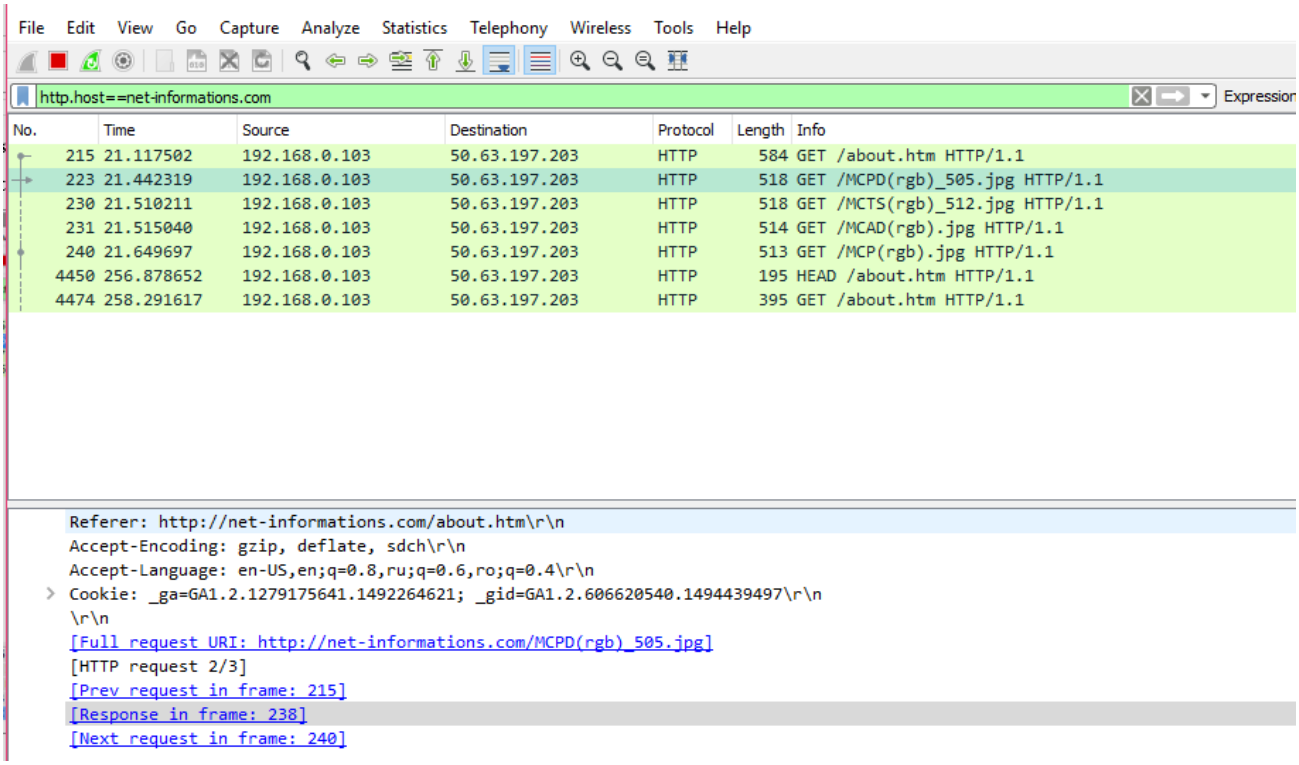


Fig. 3 Vizualizarea frame-ului unde se regăsește răspunsul

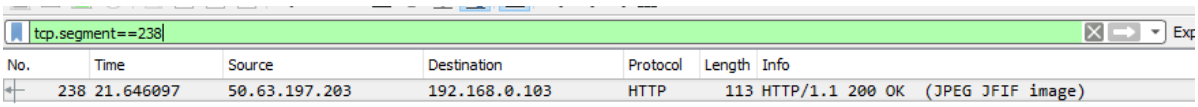
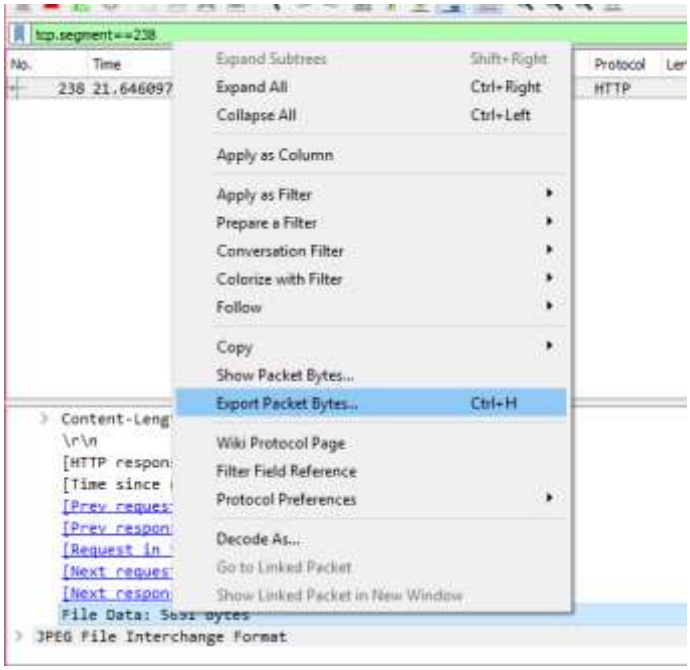


Fig 4.Rezultatul filtrării

Pentru a putea obține imaginea căutată trebuie doar să apasăm click dreapta pe segmenul cu denumirea Data File ce se află în Content-length după care accesăm Transport Packet Bytes...(Fig.5) , după care se va putea salva imaginea in format png în directoriul dorit.



Mai apoi dăm denumire fișierului nostru cu extensia .png și-l salvam pe Desktop .

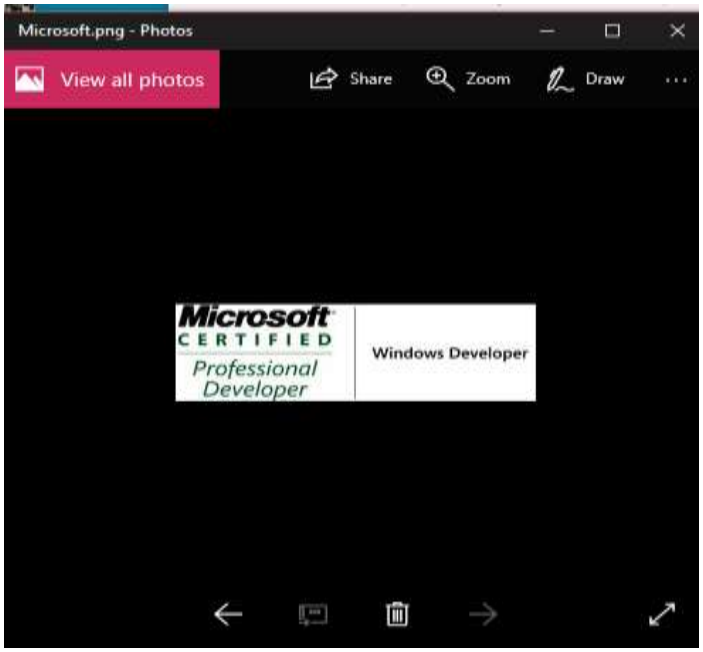


Fig. 9 Imaginea salvată datorită pachetelor preluate prin Wireshark

Concluzie

Cu ajutorul lucrării de laborator Nr. 5 s-a studiat ingineria inversă în rețea prin intermediul softului Whireshark. Astfel această tehnologie este potrivită pentru captarea pachetelor în timp real și afișarea acestora într-un format ce poate fi perceput de om. Wireshark oferă filtre, color-coding și alte instrumente care permit căutarea în adâncime în interiorul traficului de internet și inspecția pachetelor individuale. Acest instrument colorează fiecare tip de trafic într-o anumită culoare pentru identificarea mai rapidă, pentru protocolul TCP este prestabilit culoarea verde, UDP- albastru deschis, pachete TCP cu probleme- negru. Alt lucru deosebit de interesant este posibilitatea de urmărire a conversației întregi între client și server, urmărind TCP stream-ul.

Bibliography

1. Capturarea și analizarea traficului de rețea. *www.tc.etc.upt.ro.* [Online] [Cited: Aprilie 29, 2016.] http://www.tc.etc.upt.ro/teaching/arc/Lab6.pdf.

2. How-To-Geek, LLC. How to Use Wireshark to Capture, Filter and Inspect Packets. *www.howtogeek.com.* [Online] [Cited: Aprilie 27, 2016.] http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/.

3. Wireshark. Inc. Chapter 1. Introduction. *www.wireshark.org.* [Online] [Cited: Martie 29, 2016.] https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroFeatures.