Lucrarea de laborator nr.4.
Protocolul TCP

În acest laborator vom investiga comportamentul protocolului TCP în detaliu.

Vom analiza o copie de segmente TCP trimise şi recepţionate transferând un fişier de 34kb (Fişierul *standard.txt* ce conţine descrierea standardului RFC1042) de la computerul dvs. la un server remote. Vom studia felul în care protocolul TCP foloseşte numerele secvenţiale şi de confirmare pentru a oferi un transfer stabil de date. Vom vedea algoritmul TCP de congestie – "slow start" şi "congestion avoidance" – în acţiune, şi vom observa mecanismul TCP de flow-control. Vom arunca o privire scurtă şi asupra setării conexiunii TCP şi asupra performanţelor (*throughput* şi *round-trip time*) a conexiunii TCP dintre computerul dvs şi server.

Volumul capturii unui transfer TCP de la calculatorul dvs la un server remote

Înainte de a începe, vom folosi Wireshark pentru a obţine un trace al unui transfer TCP a unui fişier de la computerul dvs la un server remote. Veţi accesa o pagină web unde veţi scrie numele unui fişier stocat pe computerul dvs (care conţine textul ASCII pentru standardul RFC1042), şi apoi veţi transfera fişierul către un server web folosind metoda HTTP POST. Preferăm metoda POST metodei GET, deoarece vrem să transferăm o cantitate mare de date de la computerul dvs. la alt computer. Wireshark va rula în tot acest timp pentru a obţine trace-ul segmentelor TCP trimise şi recepţionate de la computerul dvs.

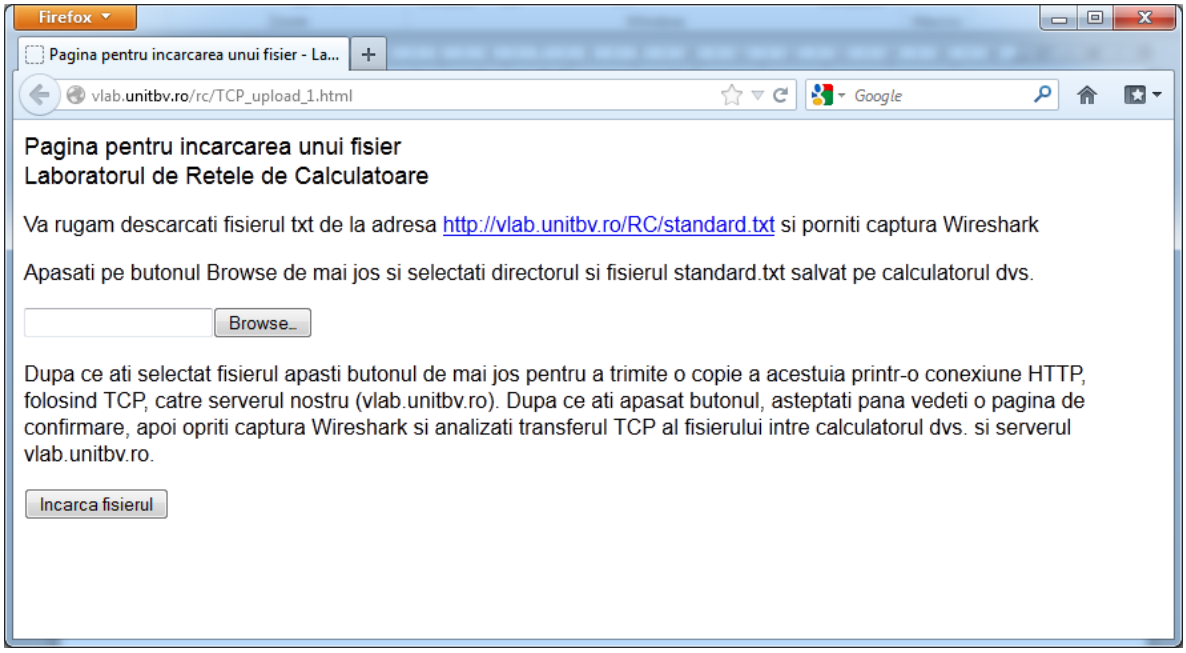

Figura 10 - Accesarea paginii web pentru transferul fişierului

- deschideţi browser-ul la http://vlab.unitbv.ro/rc/standard.txt şi descărcaţi o copie ASCII a descrierii standardului RFC1042. Salvaţi acest fişier pe computer;
- acum mergeţi la http://vlab.unitbv.ro/rc/TCP_upload_1.html - ar trebui să vedeţi un ecran asemănător cu cel din Figura 10;
- folosiţi butonul *Browse* pentru a introduce numele fişierului (full path) de pe computerul dvs care conţine *standard.txt* (sau faceţi acelaşi lucru manual). Nu apăsaţi încă butonul "*Încărcaţi fişierul*";
- porniţi captura Wireshark şi apăsaţi *OK* la Wireshark Packet Capture Options (nu selectaţi nici o opţiune);
- înapoi la browser, apăsaţi "*Încărcaţi fişierul*" pentru a încărca fişierul la serverul „vlab.unitbv.ro". După upload, va apărea un mesaj de felicitare în browser;
- opriţi Wireshark. Fereastra Wireshark ar trebui să arate ca în Figura 11:

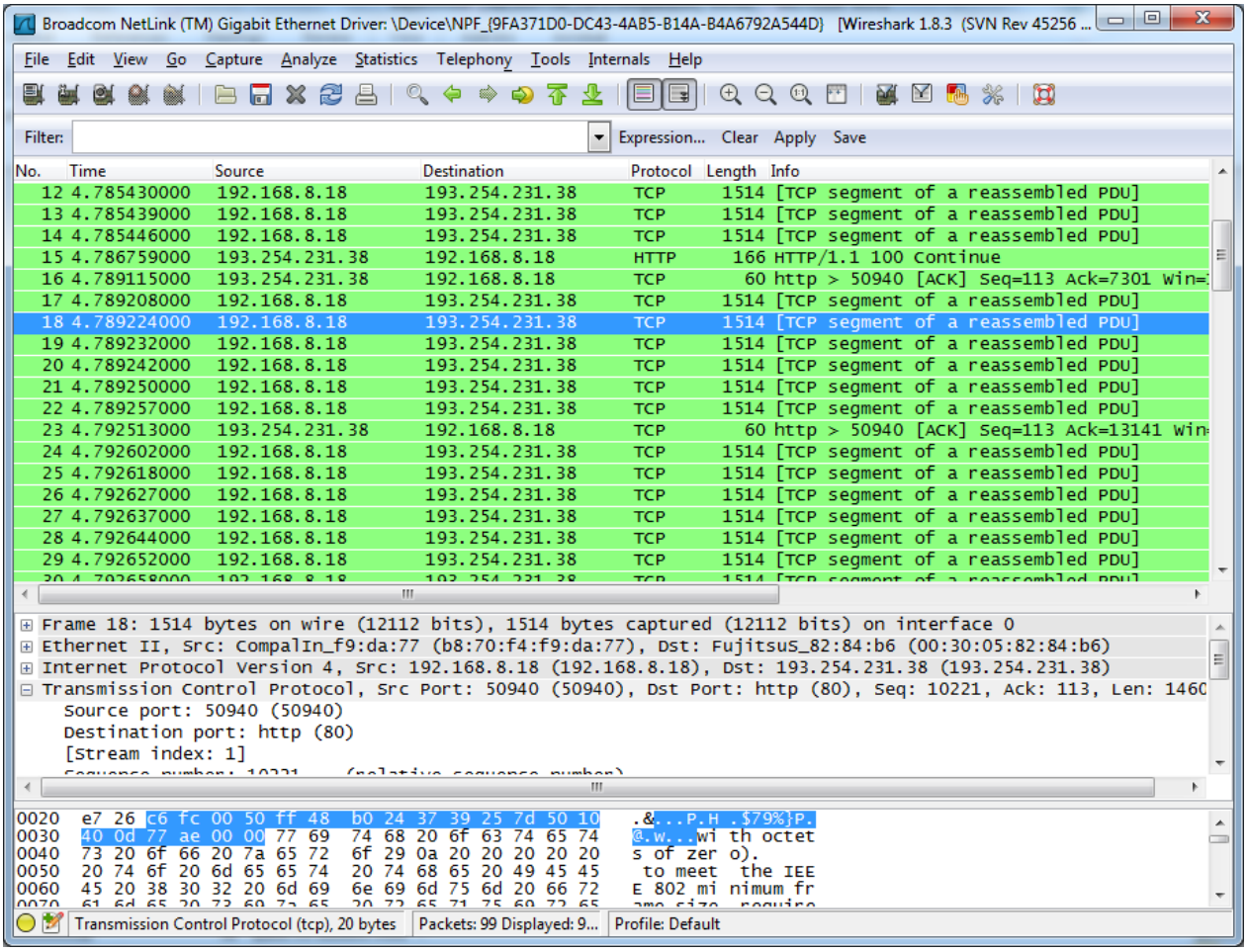

Figura 11 - Fereastra Wireshark după încărcarea fişierului

Dacă nu va merge Wireshark, extrageţi fişierul *tcp-ethereal-trace-1* din arhiva aflată pe CD.

O privire asupra capturii

Mai întâi, filtraţi pachetele afişate în Wireshark, scriind “tcp” în filtru. Ar trebui să vedeţi primul “three-way handshake” care conţine un mesaj SYN; apoi un mesaj HTTP POST şi o serie de mesaje “HTTP Continuation” care au fost trimise de la computerul dvs. la computerul cu adresa “vlab.unitbv.ro”. Aduceţi-vă aminte din laboratorul HTTP, că nu există vreun mesaj „HTTP Continuation” – acesta este modul Wireshark de a arăta că există segmente TCP multiple folosite pentru transportul unui singur mesaj HTTP. Ar trebui să mai vedeţi segmente TCP ACK trimise de la “vlab.unitbv.ro” către computerul dvs.

Deschideţi fişierul *tcp-ethereal-trace-1* de pe CD şi răspundeţi la întrebările de mai jos. Este recomandat să arătaţi un printout (*File → Print, Selected packet only, Packet summary line* şi selectaţi detaliul de pachete minim, de care aveţi nevoie pentru a răspunde la întrebări, a pachetelor din trace pe care le-aţi folosit.

1. Care este adresa IP şi portul TCP folosite de computerul care transferă fişierul către “vlab.unitbv.ro”? Puteţi selecta un mesaj HTTP şi explora detaliile pachetului TCP folosit pentru a transporta acest mesaj, folosind “details of the selected packet header window”?

2. Care este adresa IP a serverului “vlab.unitbv.ro”? Pe care port trimite şi pe care primeşte segmente TCP pentru această conexiune?

Dacă aţi putut să vă faceţi propriul trace, răspundeţi şi la întrebarea:

3. Care este adresa IP şi portul TCP folosite de computerul dvs. pentru a transfera fişierul la “vlab.unitbv.ro”?

Datorită faptului că acest laborator se referă la TCP, şi nu la HTTP, vom schimba fereastra cu lista pachetelor capturate astfel încât să arate informaţii despre segmentele TCP care conţin mesaje HTTP, şi nu vom mai vedea mesaje HTTP: *Analyze → Enabled Protocols*. Acum debifaţi HTTP şi apăsaţi *OK*. Fereastra Wireshark ar trebui să arate ca mai jos.

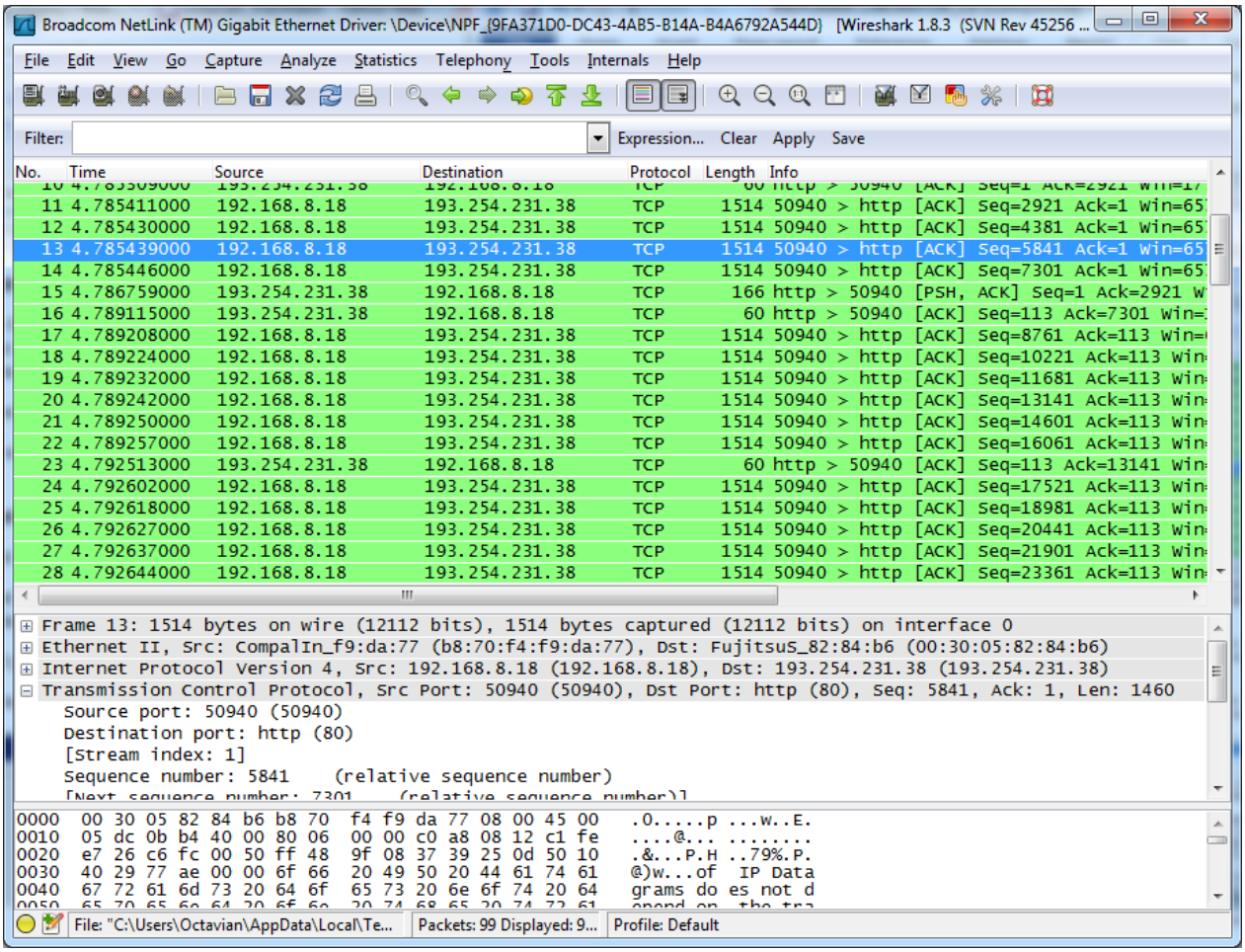

Figura 12 - Fereastra de captură Wireshark afişând segmentele TCP

Avem acum o serie de segmente TCP trimise între computerul dvs. şi serverul „vlab.unitbv.ro”. Vom folosi captura dvs. (sau *tcp-ethereal-trace-1* din arhiva menţionată mai sus) pentru a studia comportamentul TCP în restul laboratorului.

Fundamente TCP

Răspundeţi la următoarele întrebări despre segmentele TCP:

4. Care este numărul secvenţial al segmentului TCP SYN care este folosit pentru a iniţia conexiunea între computer şi “vlab.unitbv.ro”? Ce anume din segment îl identifică drept un segment SYN?
5. Care este numărul secvenţial al segmentului SYNACK trimis de “vlab.unitbv.ro” la computerul dvs., ca replică la SYN? Care este valoarea câmpului de confirmare în

segmentul SYNACK? Cum a determinat "vlab.unitbv.ro" valoarea? Ce anume din segment îl identifică drept un segment SYNACK?

6. Care este numărul secvenţial al segmentului TCP care conţine comanda HTTP POST? Pentru aceasta trebuie să căutaţi în "packet content field" şi să căutaţi un segment cu "POST" în câmpul DATA.
7. Priviţi segmentul TCP care conţine HTTP POST ca fiind primul segment în conexiunea TCP. Care sunt numerele secvenţiale în conexiunea TCP (inclusiv segmentul cu HTTP POST) ? La ce oră a fost trimis fiecare segment? Când a fost recepţionat ACK pentru fiecare segment? Dată fiind diferenţa dintre momentul în care a fost trimis fiecare segment TCP şi momentul în care i s-a răspuns cu o confirmare, care este valoarea RTT pentru fiecare dintre cele 6 segmente? Care este "*Estimated RTT Value*" după recepţia fiecărui ACK?

Nota: Wireshark va lasă să vizionaţi grafic RTT-ul pentru fiecare dintre segmentele TCP trimise. Selectaţi un segment TCP din lista pachetelor capturate care este trimisă de la client la serverul "vlab.unitbv.ro". Apoi selectaţi *Statistics → TCP Stream Graph → Round Trip Time Graph* .

8. Care este lungimea fiecăruia dintre cele 6 segmente TCP?

Segmentele TCP din fişierul tcp-ethereal-trace-1 sunt toate mai mici decât 1460 biţi, datorită plăcii de reţea a calculatorului de pe care s-a luat trace-ul, care limitează lungimea maximă a unui pachet IP la 1500 biţi (40biţi pentru header TCP/IP şi 1460biţi pentru payload-ul TCP). 1500biţi este lungimea maximă standard a pachetului permisă de către Ethernet. Dacă vedeţi o lungime TCP mai mare de 1500biţi şi folosiţi o conexiune TCP, atunci Wireshark indică o valoare greşită şi în cel mai probabil caz, va arăta doar un singur segment mare TCP decât mai multe segmente mici. Calculatorul dvs. este posibil într-adevăr să trimită mai multe segmente mici, după cum se vede şi din ACK-urile primite. Această inconsistenţă se datorează interacţiunilor dintre driver-ul Ethernet şi soft-ul Wireshark. Dacă vă loviţi de această inconsistenţă, recomandarea este să faceţi laboratorul cu trace-ul oferit mai sus.

9. Care este valoarea minimă de "buffer space" văzută la recepţie pentru întregul trace? Datorită faptului că spaţiul buffer-ului este prea mic, transmiţătorul este limitat?
10. Există vreun segment retransmis în trace? Justificaţi răspunsul.
11. Câtă informaţie confirmă receptorul în ACK? Puteţi identifica cazurile pentru care receptorul confirmă (ACK) la fiecare segment recepţionat?
12. Care este throughput-ul (numărul de biţi transferaţi în unitatea de timp) pentru conexiunea TCP? Justificaţi calculul.

4. Controlul congestiei TCP

Vom examina cantitatea de informaţie transmisă în unitatea de timp de la client la server. Decât sa facem un calcul obositor extrăgând informaţia din fereastra Wireshark, vom folosi un grafic TCP al Wireshark – *Time-Sequence_Graph (Stevens).*

Selectaţi un segment TCP din fereastra Wireshark. Apoi selectaţi *Statistics* → *TCP Stream Graph* → *time-Sequence-Graph(Stevens).* Ar trebui să vedeţi un grafic care arată asemănător graficului din Figura 13, care a fost creat din pachetele capturate din trace-ul *tcp-ethereal-trace-1* din arhiva *wireshark-traces.zip*.

Aici, fiecare punct reprezintă un segment TCP trimis, iar pe axe avem numărul secvenţial al segmentului pe timpul la care a fost trimis. Un set de puncte unul deasupra celuilalt reprezintă o serie de pachete care au fost trimise "back-to-back".

Răspundeţi la următoarele întrebări pentru trace-ul *tcp-ethereal-trace-1* din arhiva *wireshark-traces.zip*.

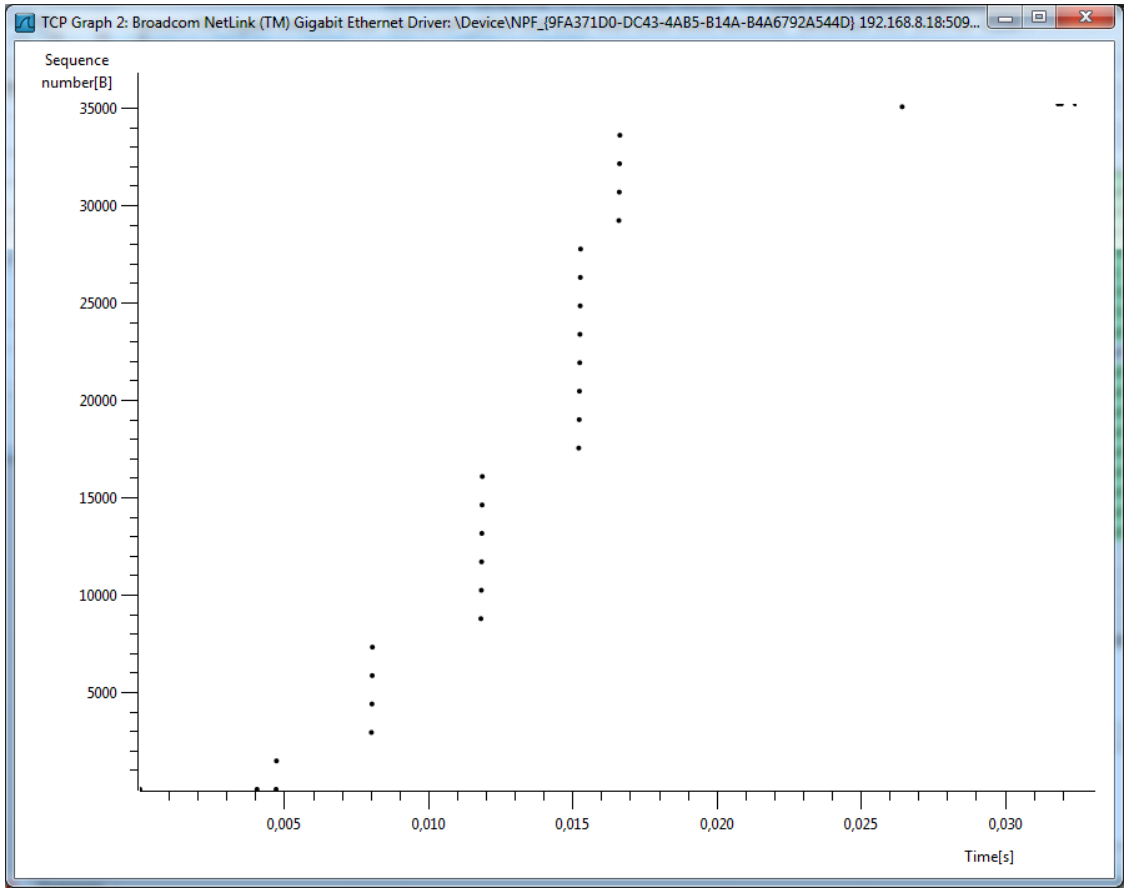

Figura 13 - Graficul secvenţe-timp

13. Folosiţi *Time-Sequence-Graph(Stevens)* pentru a vedea graficul segmentelor trimise de la client la serverul "vlab.unitbv.ro". Puteţi spune unde începe şi unde se termină faza TCP "slowstart" şi unde apare "congestion avoidance" ? Discutaţi modurile în care măsurătoarea voastră diferă de comportamentul ideal TCP pe care l-am studiat în text.

Cuprins