Лабораториска вежба бр. 3
TCP

Во оваа лабораториска вежба, детално ќе го испитаме однесувањето на познатиот TCP протокол. Анализата ќе биде спроведена преку анализа на трага (trace) од TCP сегментите испратени и примени при пренесување на датотека со големина 150KB (содржи текст на Алиса во Земјата на Чудата на Луис Карол) од вашиот компјутер на оддалечен сервер. Ќе ја проучиме употребата на TCP за секвенци и броеви за потврда со цел обезбедување на сигурен трансфер на податоци; ќе го разгледаме механизмот за контрола на застој (congestion control) на TCP - бавно започнување и избегнување на застој - во акција; и ќе го разгледаме механизмот за контрола на проток на рекламирани приемници на TCP. Исто така, накратко ќе ја разгледаме поставката за TCP конекција и ќе ги провериме перформансите (проток и време на патување) на TCP-врската помеѓу вашиот компјутер и серверот.

Пред да започнете со вежбата, прочитајте ги секциите 3.5 и 3.7 од текстот[1].

1. Трансфер на голем документ преку TCP од вашиот компјутер на оддалечен сервер

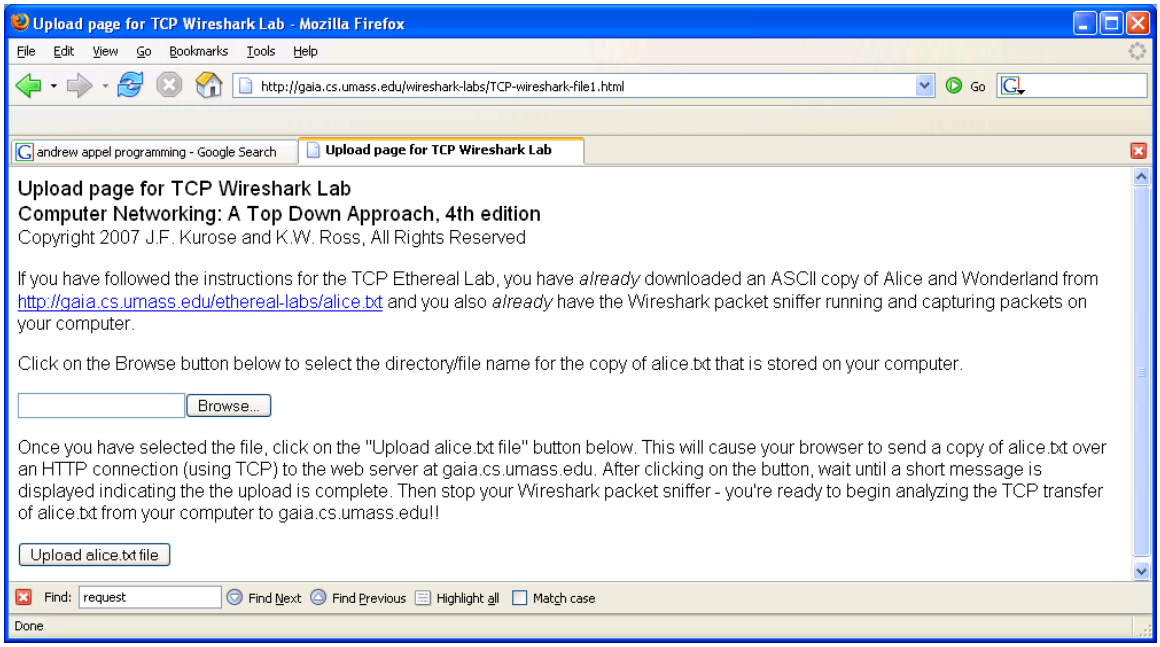
Пред да започнете со разгледување на можностите на TCP, потребно е да имате инсталирано Wireshark на компјутерот за да го следите пакетот кој се праќа од вашиот компјутер до далечниот сервер. Притоа, ќе користите пристапна веб страница на која ќе може да прикачите документ (ASCII текст од познатата книга Алиса во Земјата на Чудата) кој би сакале да го пратите со едноставна форма за прикачување. Праќањето е овозможено со користење на HTTP POST командата. Причината за користење на POST барање, наместо GET, е во тоа дека праќаме големо количество на податоци до далечниот сервер кое стандардно не може да се прати како GET барање. Во меѓувреме, на вашиот компјутер треба да биде стартуван Wireshark да работи во позадина за да се добие трага на TCP сегментите кои се праќаат и примаат од страна на вашиот компјутер.

Направете го следното:

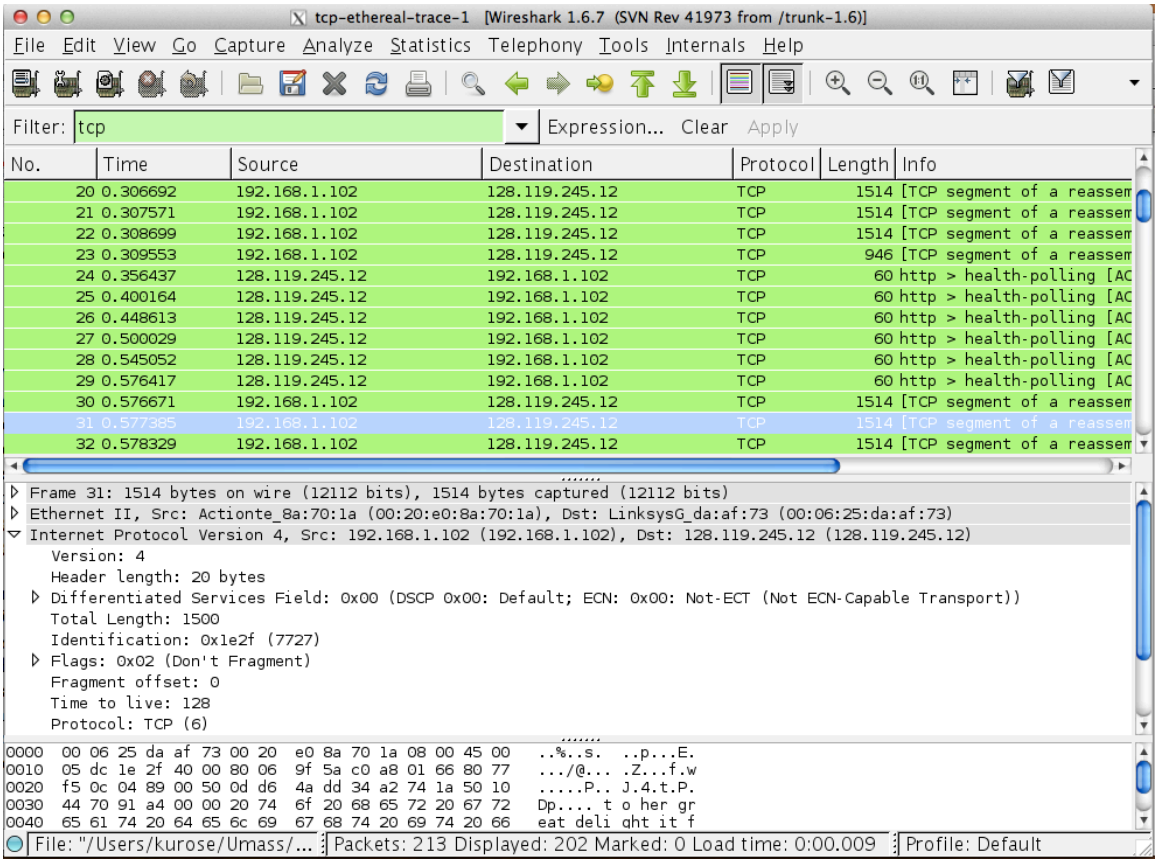
- Стартувајте веб прелистувач. Отворете ја следната страница http://gaia.cs.umass.edu/wireshark-labs/alice.txt и преземете копија од документот *Alice in Wonderland.* Зачувајте го фајлот на произволна локација во вашиот компјутер.

[1] References to figures and sections are for the 7th edition of our text, *Computer Networks, A Top-down Approach, 7th ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2016.*

- Следно, навигирајте кон http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html.
- Потребно е да ви се отвори следната страница:



- Користете го Browser копчето од формата за да ја внесете патеката на документот кој сакате да го прикачите. Во овој случај, користете го докуметот *Alice in Wonderland* кој претходно го преземавте. Не кликајте на копчето "*Upload alice.txt file*" сеуште.
- Потребно е да ја стартувате апликацијата Wireshark и да започнете со фаќање на пакетите со повик на командата *(Capture->Start)*. Кликнете на копчето OK на дијалогот кој ви се појавува (нема потреба од сетирање на кои опции овде).
- Вратете се назад на вашиот прелистувач, кликнете на копчето "*Upload alice.txt file*" за да започне процесот на праќање на фајлот кон серверот на локацијата gaia.cs.umass.edu. Штом документот е прикачен, кратка порака ќе ви биде прикажана на страницата дека прикачувањето е успешно.
- Стопирајте го фаќањето на пакети од страна на Wireshark. Изгледот на Wireshark, треба да постане сличен на прозорецот кој е прикажан на долната слика.



2. Прв поглед кон фатената трага на пакетите

Пред да го анализирате однесувањето на TCP конекцијата во детали, направете првичен преглед на трагата.

- Прво, филтрирајте ги пакетите кои се прикажани на Wireshark со внес на “tcp” (мали букви, без наводници, и без да заборавете да кликнете Enter по испишувањето!) командата во display филтерот најгоре на интерфејсот на Wireshark.

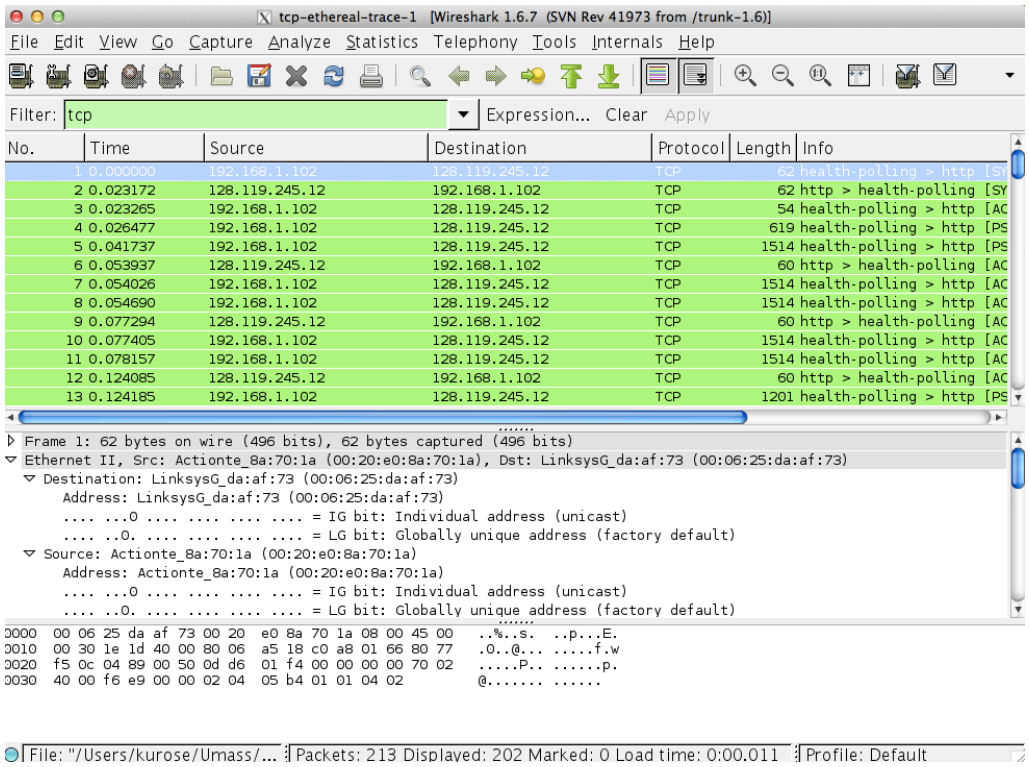
Ќе забележите серија од TCP и HTTP пораки меѓу вашиот компјутер и gaia.cs.umass.edu. Исто, ќе забележите иницијално 3-way ракување (handshake) коешто содржи SYN порака. Исто, ќе забележите HTTP POST порака. Во зависност од верзијата на Wireshark која ја користите, ќе забележите серија “HTTP Continuation” пораки кој се праќаат од вашиот компјутер до gaia.cs.umass.edu.

Во поновите верзии на Wireshark, ќе забележите „TCP segment of a reassembled PDU“ во колоната Info на приказот на Wireshark за да се укаже дека овој TCP сегмент содржи податоци што припаѓаат протокол од погорниот слој за пораки (во нашиот случај овде , HTTP). Исто така, треба да воочите дека TCP ACK сегментите се враќаат од gaia.cs.umass.edu на вашиот компјутер.

Одговорете на следните прашања со отворање на Wireshark фатениот пакет *tcp-ethereal-trace-1* кој се наоѓа на следната локација http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip (преземете ја трагата и отворете ја во Wireshark). Кога и да е можно, кога одговарате на прашање, треба да предадете отпечаток на пакетот (пакетите) во трагата што сте ја користеле за да одговорите на поставеното прашање. Анотирајте го печатењето за да го објасните вашиот одговор. За да отпечатите пакет, користете File-> Print, изберете *Selected packet only*, изберете *Packet summary line* и изберете ја минималната количина детали за пакетот што ви е потребна за да одговорите на прашањето.

1. Која е IP адресата и TCP портата кои се користат од клиентскиот компјутер (изворот) при трансфер на документот до gaia.cs.umass.edu? За да одговорите на ова прашање, веројатно е најлесно да изберете HTTP-порака и да ги истражите деталите за TCP-пакетот што се користат за носење на оваа HTTP порака, користејќи ги „ details of the selected packet header window”.
2. Која е IP адресата на gaia.cs.umass.edu? Која порта ја користи за праќање и примање на TCP сегменти за оваа конекција?
3. Која е IP адресата и TCP портата која ја користи вашиот компјутер како клиент за праќање на податоци до серверот gaia.cs.umass.edu?

Поради тоа што оваа лабораториска вежба е за TCP наместо за HTTP, направете промена на “listing of captured packets” прозорецот на Wireshark, за да се прикажат информациите за TCP сегментите кои содржат HTTP пораки. За да се овозможи ова, изберете *Analyze->Enabled Protocols.* Потоа, деселектирајте ја HTTP опцијата и изберете OK. Wireshark прозорецот треба да изгледа како на сликата:



Тоа е она што го баравме- серија на TCP сегменти кои се разменуваат меѓу клиентот, вашиот компјутер, и серверот, во овој случај gaia.cs.umass.edu. Понатаму, за да го разгледаме однесувањето на TCP, ќе ја користиме трагата која ја фативте со Wireshark, или ако не успеавте, може да преземете пример трага на следниот линк http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip.

3. Основи на TCP

Одговорете ги следните прашања за TCP сегментите:

4. Кој е секвенционалниот број на TCP SYN сегментот кој се користи за иницирање на TCP конекција помеѓу клиентскиот компјутер и gaia.cs.umass.edu? Што е тоа во сегментот што го идентификува сегментот како SYN сегмент?
5. Кој е секвенционалниот број на SYNACK сегментот пратен од gaia.cs.umass.edu до клиентскиот компјутер како одговор на SYN? Која е вредноста на Acknowledgement полето во SYNACK сегментот? Како gaia.cs.umass.edu ја одредува таа вредност? Што е тоа во сегментот што го идентификува сегментот како SYNACK сегмент?
6. Кој е секвенционалниот број на TCP сегментот што ја содржи HTTP POST командата? За да ја идентификувате POST командата, мора да навлезете во полето што ја носи содржината на пакетот најдолу во прозорецот на Wireshark, за да го пронајдете сегментот кој го содржи "POST" во DATA полето.
7. Сметајте дека TCP сегментот кој го содржи барањето за HTTP POST е првиот сегмент во TCP врската. Кои се секвенционалните броеви на првите 6 сегменти во TCP врската (вклучувајќи го сегментот кој го содржи HTTP POST барањето)? Во кое време секој сегмент е пратен? Кога е примен ACK за секој сегмент? Земајќи ја во предвид разликата кога еден TCP сегмент е пратен и ACK за истиот е примен, која е вредноста на RTT за секој од овие 6 сегменти? Која е вредноста `EstimatedRTT` при приемот на секој ACK? Да претпоставиме дека вредноста на `EstimatedRTT` е еднаква на измерената RTT за првиот семгнет, и потоа се пресметува со користење на `EstimatedRTT` равенката за сите последователни сегменти.

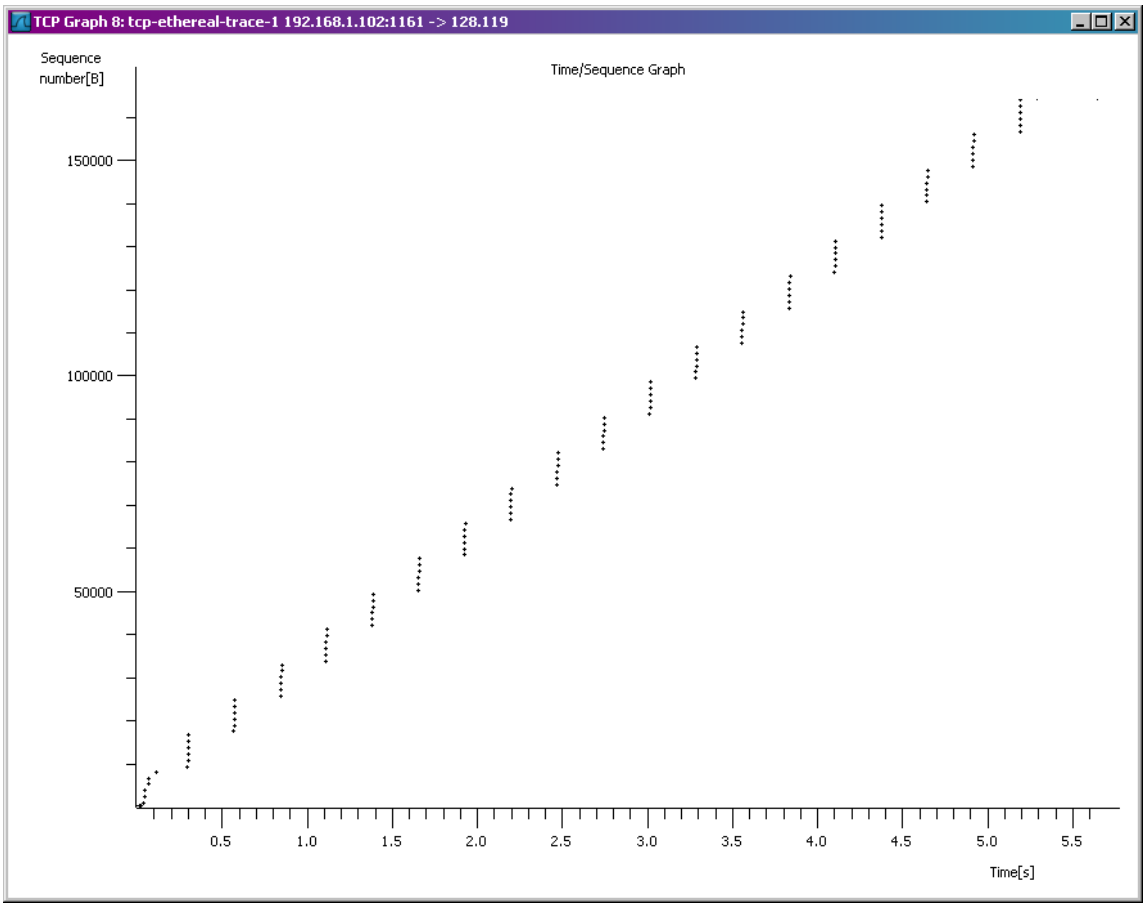
   Забелешка: Во Wireshark постои функционалност која ви овозможува да ја исцртате RTT вредноста за секој TCP сегмент кој е пратен. Избери TCP сегмент во прозорецот "listing of captured packets" кој е пратен од клиентот до gaia.cs.umass.edu серверот. Потоа избери: *Statistics->TCP Stream Graph->Round Trip Time Graph.*
8. Која е должината на секој од првите 6 сегменти?
9. Која е минималната количина на достапен бафер простор кај примачот за целата траса? Дали недостатокот на бафер простор кај примачот влијае врз праќачот? Објасни.
10. Дали постојат сегменти кои се препратени? Како може да откриете (во датотеката со трага) за да го одговорете ова прашање?

11. Колку податоци примачот најчесто потврдува со еден ACK?
12. Колкав е податочниот проток (бајти пренесени во единица време) (throughput) на TCP врската? Објасни како ја пресмета оваа вредност.

4. TCP контрола на застој

Во овој дел од вежбата, ваша задача е да го проверите количеството на податоци кој се праќа во единица време од клиентот до серверот. За оваа цел, користете ја алатката од Wireshark *Time-Sequence-Graph(Stevens)* - да ги исцрта податоците.

- Изберете TCP сегмент во прозорецот "listing of captured-packets". Потоа повикајте: *Statistics->TCP Stream Graph-> Time-Sequence-Graph(Stevens)*. Би требало да добиеш слично исцртување како на сликата, кое е добиено од фатените пакети во примерот: *tcp-ethereal-trace-1* кој се наоѓа на оваа локација http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip:



На сликата, секоја точка претставува испратен TCP сегмент, каде x-оската го означува времето кога е пратен, а y-оската го означува неговиот секвенцијален број. Забележете дека множеството точки поставени еден врз друг претставува серија на пакети што се пратени од праќачот.

Вчитајте ја пример-трагата која се наоѓа на следната локација http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip и одговорете ги следните прашања:

13. Користете ја алатката за цртање *Time-Sequence-Graph(Stevens*) за да ги прегледате секвенционалните броеви во однос на временското исцртување на сегментите кои се пратени од клиентот до серверот gaia.cs.umass.edu. Дали можете да го идентификувате почетокот и крајот на TCP slowstart фазата, и во кој момент почнува процесот на заштита од застој (congestion avoidance)?
14. Одговорете ги истите 2 прашања и за трагата која вие ја изгенерирвте со праќањето на големиот фајл до серверот gaia.cs.umass.edu.