Laboratorijska vježba broj 8

Teorijska osnova vježbe:

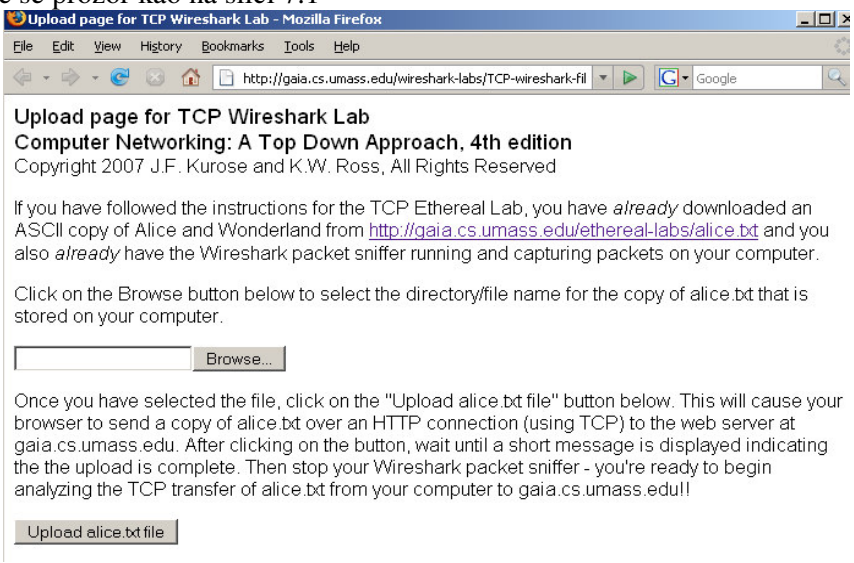
U ovoj laboratorijskoj vježbi detaljnije će biti proučen TCP protokol analiziranjem zapisa TCP segmenata poslatih i primljenih pri prenosu fajla veličine 150 KB (koji sadrži odlomak iz Luis Kerolove knjige ”Alisa u zemlji čuda“) od računara do udaljenog servera. Vidjeće se kako TCP koristi sekvencu i brojeve potvrde za obezbjeđivanje pouzdanog prenosa podataka. Takođe, ukratko će se razmotriti uspostavljanje TCP konekcije i performanse (propusnost i RTT) TCP konekcije između računara i servera.

Hvatanje najvećeg dijela TCP transfera od računara do udaljenog servera

Wireshark *packet sniffer* se koristi za dobijanje zapisa paketa iz TCP transfera fajlova od računara do udaljenog servera. Najprije će se *upload*-ovati fajl smješten na računaru (koji sadrži ASCII tekst ”Alisa u zemlji čuda“) do Web servera koristeći HTTP POST metod (koristeći pristup posebnom Web sajtu koji to dozvoljava). POST metod u redu zahtjeva HTTP poruke se upotrebljava kada se želi poslati velika količina podataka sa našeg na drugi računar.

Potrebno je pratiti sledeće korake:

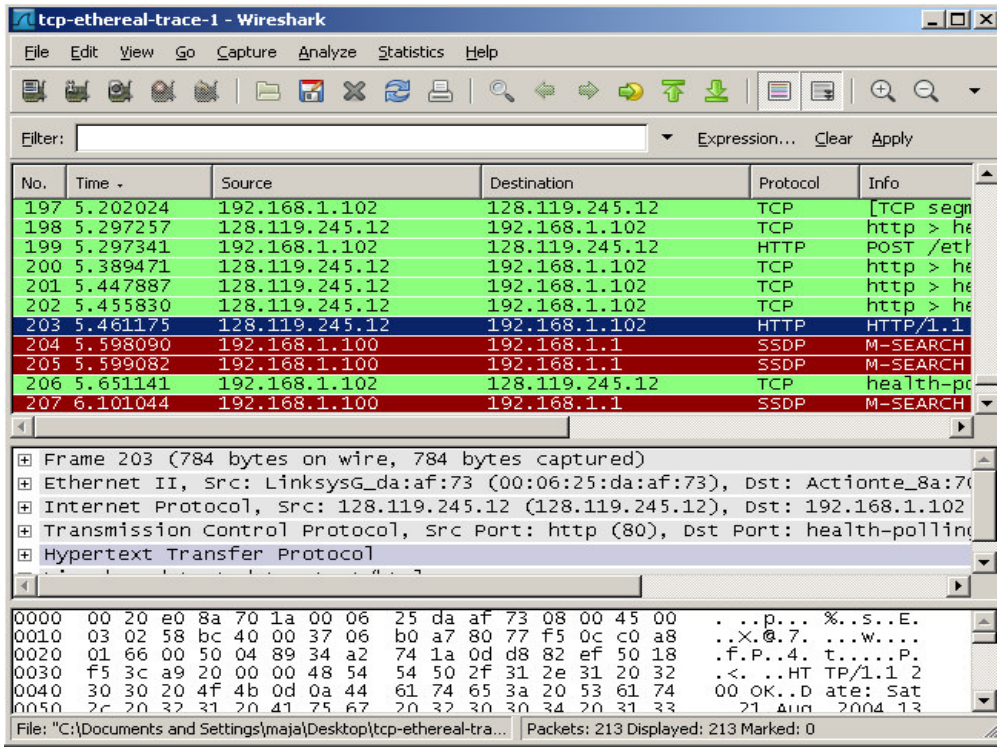
- Startovati Web browser i otvoriti stranu: http://gaia.cs.umass.edu/wireshark-labs/alice.txt, a zatim i sačuvati kopiju dokumenta ”Alisa u zemlji čuda“ na računaru na kojem radite (kliknuti na meni **File > Save As**).
- Zatim otvoriti stranu http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html
- Pojaviće se prozor kao na slici 7.1



Slika 7.1.

- Upotrijebiti Browse dugme za pronalaženje snimljenog fajla ”Alisa u zemlji čuda“. Još **ne treba pritiskati** *"Upload alice.txt file"* dugme.
- Startovati Wireshark i početi hvatanje paketa. Podesiti aktivni mrežni adapter i pritisnuti **OK**.
- Vratiti se u browser i pritisnuti “*Upload alice.txt file*” kako bi se upload-ovao fajl na gaia.cs.umass.edu server. Kada se ovaj proces završi ispisaće se kratka poruka u prozoru browser-a.
- Zaustaviti Wireshark hvatanje paketa.

Pojaviće se Wireshark prozor kao na slici 7.2.



Slika 7.2.

Ukoliko niste u mogućnosti da pokrenete Wireshark na aktivnoj Internet konekciji, možete downloadovati gotovi packet trace fajl sa adrese http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip i ekstraktovati fajl tcp-ethereal-trace-1.

Pogled na snimljeni zapis

Prije detaljnog analiziranja ponašanja TCP konekcije, potrebno je prvo:

- Filtrirati pakete prikazane u Wireshark prozoru unošenjem "tcp" u filter prozoru.

Prikazuje se niz TCP i HTTP poruka razmijenjenih između vašeg računara i gaia.cs.umass.edu servera. Uočava se inicijalni *three-way handshake* sa SYN porukom. Slijedi HTTP POST poruka i serija "reassembled PDU" poruka koje su poslate od računara do gaia.cs.umass.edu računara. Reassembled PDU poruka ustvari ne postoji – to je samo Wireshark-ov način da se pokaže da se za prenos jedne HTTP poruke koristi više TCP segmenata. Takođe, uočavaju se i TCP ACK segmenti koji su vraćeni od gaia.cs.umass.edu servera na vaš računar.

Pitanja:

1. Koja je IP adresa i broj TCP porta koje koristi računar (izvor) koji prenosi fajl do gaia.cs.umass.edu servera?
2. Koja je IP adresa i broj TCP porta koje koristi gaia.cs.umass.edu server?

S obzirom da se ova vježba odnosi na TCP, a ne na HTTP, promijeniti Wireshark-ov "listing of captured packets" prozor tako da on pokazuje informacije o TCP segmentima koji sadrže HTTP poruke. Izabrati ***Analyze->Enabled Protocols***. Zatim *uncheck* HTTP box i kliknuti OK.

TCP

Odgovoriti na sledeća pitanja u vezi TCP segmenata:

3. Koji je redni broj TCP SYN segmenta koji inicijalizuje TCP konekciju između klijenta i gaia.cs.umass.edu servera? Šta u segmentu nam govori da je to SYN segment?
4. Koji je redni broj SYN ACK segmenta koji šalje gaia.cs.umass.edu server klijentu u odgovoru na SYN? Koja je vrijednost ACKnowledgement polja u SYN ACK segmentu?
5. Koji je redni broj TCP segmenta koji sadrži HTTP PUSH (PSH) komandu? (Napomena: da bi pronašli POST komandu potrebno je analizirati polje sadržaja paketa na dnu Wireshark prozora dok se ne uoči sedment sa „PSH“ sadržajem u svom DATA polju)
6. Posmatrati TCP segment koji sadrži HTTP PSH **kao prvi segment u** TCP konekciji. Koji su brojevi portova prvih šest segmenata u TCP vezi (uključujući i segment koji sadrži HTTP PSH)?
7. Koji su brojevi sekvenci svakog od posmatranih segmenata?
8. S obzirom da je data vremenska razlika između trenutaka kada je svaki TCP segment poslat i kada je primljen ACK, koja je RTT vrijednost za prva tri od posmatranih 6 segmenata?
9. Kolika je dužina svakog od posmatranih šest TCP segmenta?

(*TCP segmenti u tcp-Wireshark-trace-1 trace fajlu su manji od 1460 bajta, zato što računar na kojem se ovo realizovalo ima Ethernet card koja ograničava dužinu IP paketa na maksimalnih 1500 bajta (40 bajta TCP/IP zaglavlja i 1460 bajta TCP korisnog sadržaja). Ovih 1500 bajta je standardna maksimalna dužina koju dozvoljava Ethernet. Ako dobijete TCP dužinu veću od 1500 bajta i vaš računar koristi Ethernet konekciju, onda Wireshark javlja pogrešnu dužinu TCP segmenta; vjerovatno će prikazati samo jedan veliki TCP segment, a ne više manjih segmenata. Vaš računar vjerovatno šalje više manjih segmenata, i za njih prima poruke potvrde-ACK. Ova nedosljednost u izvještaju o dužini segmenata nastaje zbog interakcije između Ethernet driver-a i Wireshark software-a*)

10. Da li se dogodila retransmisija ijednog segmenta u trace fajlu? Šta ste provjerili (u trace-u) da biste odgovorili na ovo pitanje?
11. Koliko podataka postoji u ACK prijemnika? Šta znači taj podatak?
12. Koliki je protok (broj prenešenih bita u jedinici vremena) za jedan TCP segment? Objasnite kako ste izračunali tu vrijednost.