Slojnost omrežja in Wireshark

Komunikacije v avtomatiki – Laboratorijske vaje

15. oktober 2013

Povzetek

Namen prve laboratorijske vaje je spoznati se programom Wireshark. V vaji boste analizirali pretok podatkov med strežnikom in klientom pri prenosu spletne strani. Vaja je razdeljena v dva sklopa, na koncu vsakega sklopa pa so vprašanja. Na ta vprašanja odgovorite, in jih zapišite v dokument (npr., uporabite LibreOffice in njegov urejevalnik Writer). Da boste lažje argumentirali svoje odgovore, naredite slike Wiresharka, (npr. s programom "ksnapshot", ki ga prikliče pritisk na tipko PrintScreen) iz katerih so razvidni podatki, ki ste ji uporabili za odgovor, in jih priložite v dokument.

1 Prvi koraki z Wiresharkom

Delali boste pod operacijskim sistemom Linux, z namizjem KDE. Programi, ki jih boste uporabljali, obstajajo tudi v različici za Microsoft Windows, in imajo zelo podobno funkcionalnost. Za začetek si bomo pogledali osnovne korake, ki so potrebni za analizo mrežnega prometa z Wiresharkom. Zaženite omrežni brskalnik Firefox in sledite naslednjim korakom.

- V orodni vrstici programa Wireshark izberite zavihek "Capture→Interfaces".
- Na voljo je več mrežnih vmesnikov. Izberite tistega, ki je aktiven in kliknite na "Options".
- Izbrišite kljukico na "Capture packets in promiscuous mode".
- Prestrezanje paketov zaženete s klikom na "Start". Sedaj lahko v glavnem oknu opazujete pakete, ki prihajajo in odhajajo z vašega računalnika preko izbranega mrežnega vmesnika.
- V brskalnik Firefox vpišite naslov `http://vision.fe.uni-lj.si/classes/KA-vaje/index.html`. Brskalnik s tem kontaktira HTTP strežnik `http://vision.fe.uni-lj.si`, si izmenja z njim sporočila po protokolu HTTP, in pretoči k sebi glavno stran predmeta "Komunikacije v avtomatiki". Pakete tipa HTTP z vsebino spletne strani prestreže Wireshark in jih prikaže v svojem vmesniku, ki je razdeljen po vertikali v tri dele. Prvi, zgornji, del prikazuje posamezne pakete v časovnem zaporedju. Drugi, srednji, del prikazuje vsebino izbranega paketa, interpretirano po slojih TCP/IP slojnega modela. Tretji, spodnji, del prikazuje surovo vsebino izbranega paketa v heksadecimalnem zapisu in zapisu ASCII.
- Ko se spletna stran predmeta v celoti prikaže v Firefoxu, ustavite sledenje paketov v Wiresharku tako, da izberete v Wiresharkovi najvišji orodni vrstici "Capture→Stop". Enako lahko storite s klikom na četrto ikono z leve strani v orodni vrstici.
- Glavno okno v Wiresharku vsebuje vse pakete, z različnimi protokoli. Med njimi so tudi tisti HTTP paketi, preko katerih je naš računalnik kontaktiral strežnik in pretočil vsebino spletne strani. Protokol posameznega paketa je viden v stolpcu "Protocol". Zaradi množice paketov, ki neprestano prehajajo skozi mrežni vmesnik,

je prikaz paketov zelo nepregleden. Preglednost lahko izboljšate z uporabo "Filter" v Orodni vrstici. Kliknite na gumb "Expression", poiščite pod "Field name" besedo "HTTP" in pritisnite "Ok". Wireshark zdaj prikaže samo tiste pakete, ki se podrejajo protokolu "HTTP". Hitreje lahko filter nastavite tudi tako, da direktno v okence pri "Filter" vpišete "http" in pritisnete "apply". Ee želite resetirati filter, pritisnite na "Clear".

- Postavite se na enega od HTTP paketkov. Vsebino paketa, ki pripada različnim slojem TPC/IP modela lahko opazujete v srednjem delu grafičnega vmesnika. Ker protokol HTTP teče na aplikacijskem sloju (4 sloj) lahko opazujemo za vsak sloj posebej informacijo, ki se nahaja v glavi paketa. Opazimo, da v prikazu zares vidimo 5 zavihkov, kjer je najvišji zavihek kar "Okvir", ki je tekel po prenosnem sredstvu od enega mrežnega vmesnika do drugega. Ker je HTTP na najvišjem sloju, se ukazi posredovani po tem protokolu (npr., GET) ovijejo v TCP segment (sloj 3), ki se ovije v IP datagram (sloj 2), ki se vsadi v Ethernet okvir (sloj 1) in pošlje po prenosnem sredstvu.
- Ee želite ponovno zagnati prestrezanje paketkov, to storite kot v koraku 4 zgoraj. Wireshark vas bo pred ponovnim zagonom vprašal če shrani vaš trenutni izpis paketkov. Ee ne želite shraniti izpisa pritisnite "Cancel".

Odgovorite na vprašanja

1. Naštejte do največ pet različnih protokolov, ki ste jih zaznali v stolpcu "Protocol" v nefiltriranem oknu s paketi.
2. Koliko časa je preteklo med HTTP ukazom `GET / HTTP/1.1`, ki ga je posredoval Firefox in ukazom HTTP OK, ki ga je posredoval strežnik? Eas v sekundah lahko odčitate tudi v stolpcu "Time", ki kaže pretekel čas od zagona prestrezanja paketov z Wiresharkom.
3. Preverite IP naslov vašega računalnika. To storite tako, da odprete terminal ("Konsole"). Ko se vam odpre okno z ukazno vrstico, vtipkate "ifconfig" in pritisnete Enter. Izpisali se bodo naslovi (in še nekaj dodatnih podatkov) o vseh omrežnih vmesnikih, ki so v računalniku. Najdite pravega in razberite IP naslov. Ali lahko v Wiresharku na HTTP paketku, ki vsebuje ukaz `GET /HTTP/1.1` najdete vaš IP? Kakšen je IP naslov strežnika in kje ga lahko najdete? V katerem sloju TCP/IP modela lahko v Wiresharku odčitamo tako izvorni kot ponorni naslov?

2 Opazovanje protokola z Wiresharkom: primer HTTP

V prejšnji nalogi smo se spoznali z osnovnimi funkcijami Wiresharka. V tej nalogi si bomo pogledali analizo komunikacije na primeru protokola HTTP.

2.1 Preprost klic HTTP

- Zaženite brskalnik Firefox. Poskrbite, da je spomin v brskalniku prazen in da ne vsebuje predpomnjenih internetnih strani. To dosežete tako, da v brskalniku izberete "History→Clear recent history", izberete vse kljukice, ki jih je možno izbrati in pritisnete "Clear Now".
- Zaženite Wireshark in izberite primerni mrežni vmesnik (na večini računalnikov je to `em1`)
- V brskalnik vpišite naslov `http://vision.fe.uni-lj.si/classes/KA-vaje/simple.html`. Ko se stran naloži, ustavite zajem paketov v Wiresharku.

- Z uporabo Filtra prikažite samo pakete, ki ustrezajo protokolu "HTTP".
- Postavite se na prvi HTTP paket z ukazom "GET /classes/KA-...". V srednjem oknu, kjer je vidna vsebina paketov po slojih, poiščite z odpiranjem vsebine slojev ukaz "GET /classes/KA-...". Poiščite značko "Request Method:" in se postavite nanjo. Vsebina te značke je ukaz "GET". Ta ukaz vidite tudi v najnižjem oknu, kjer je izpisan celotni paket v dveh stolpcih. Prvi stolpec prikazuje paket v heksadecimalni obliki, drugi pa v obliki ASCII. S pomočjo teh stolpcev odgovorite na vprašanje 2 spodaj.
- Za ilustrativen pogled pogovora med brskalnikom in strežnikom izberite "Statistics→Flow Graph", izberite "General Flow" in pritisnite "Ok". S pomočjo dobljene slike odgovorite na vprašanje 3 spodaj.
- Zaprite vmesnik za prikaz pretoka "Flow Graph".
- V glavnem oknu Wiresharka, kjer so izpisani paketi, se postavite na prvi paket z vsebino "GET /classes/KA-vaje...", pritisnite na miški na desni gumb in izberite "Follow TCP Stream". Prikaže se vam celotni pogovor med brskalnikom in strežnikom, v katerem se razločno vidi vsebina glave HTTP paketov. Vsebina paketov, ki jih pošilja brskalnik, je obarvana rdeče, vsebina paketov, ki jih pošilja strežnik, pa modro. Odgovorite na vprašanja 4,5,6 spodaj.
- Zaprite "Follow TCP Stream". Opazimo, da se je s klicem "Follow TCP Stream" spremenila vsebina okenca v "Filter". Zdaj filtriramo vse paketke (ne glede na protokol), ki so bili poslani med brskalnikom in strežnikom ter so del pogovora. Lahko opazimo, da se dejansko pred paketom z ukazom "GET /classes/KA-..." nahajajo še trije TCP paketi in nato po en TCP paket za vsakim HTTP ukazom. Prvi trije paketi pripadajo tako imenovanem procesu "three-way handshake" (glej recimo `http://en.wikipedia.org/wiki/TCP_handshake#Connection_establishment`). S temi paketi se brskalnik in strežnik sinhronizirata in vzpostavita TCP povezavo. S preostalimi TCP paketi, ki so tudi vidni, si med pogovorom strežnik in brskalnik sporočata uspešno prejeta sporočila.

Odgovorite na vprašanja

1. Katero verzijo protokola HTTP uporablja vaš Firefox: 1.0 ali 1.1 ? Katera verzija teče na strežniku?
2. Zapišite v heksadecimalni obliki ukaz "GET".
3. Koliko ukazov HTTP tipa "GET" posreduje brskalnik strežniku?
4. Kdaj je bil dokument "simple.html" nazadnje spremenjen?
5. Koliko bajtov podatkov posreduje strežnik brskalniku? Bodite pozorni, na število odgovorov, ki jih strežnik pošlje brskalniku.
6. Koliko bajtov je dolg celotni pogovor?