SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

**Hrvoje Vujasinović**

ANALIZA I VIZUALIZACIJA DNEVNIČKIH ZAPISA U PYTHONU

ZAVRŠNI rad

Varaždin, 2020.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Hrvoje Vujasinović

Matični broj: 46252/17–R

Studij: Informacijski sustavi

ANALIZA I VIZUALIZACIJA DNEVNIČKIH ZAPISA U PYTHONU

ZAVRŠNI RAD

Mentor/Mentorica:

Dr. sc. Miran Zlatović

Varaždin, rujan 2020.

*Hrvoje Vujasinović*

Izjava o izvornosti

Izjavljujem da je moj završni/diplomski rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

*Autor/Autorica potvrdio/potvrdila prihvaćanjem odredbi u sustavu FOI-radovi*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Sažetak

Tema ovog završnog rada su dnevnički zapisi, njihova svrha i uloga na osobnim računalima i web poslužiteljima te analiza i vizualizacija podataka dobivenih iz dnevničkih zapisa. U radu ću najprije objasniti što su dnevnički zapisi i čemu služe, a zatim ću obraditi temu web poslužitelja. Nakon toga bit će opisana organizacija i struktura dnevničkih zapisa na osobnim računalima i to na Linux platformama za osobna računala, a za Windows platforme obradit ću Windows Event Viewer. Nakon toga obradit ću dnevničke zapise na web poslužiteljima i nekoliko formata dnevničkih zapisa koji se koriste na web poslužiteljima. U praktičnom dijelu rada izradit ću Python aplikaciju s grafičkim sučeljem pomoću modula Tkinter za parsiranje jednog od formata dnevničkih zapisa. Aplikacija će omogućavati parsiranje i pretraživanje podataka, ekstrakciju podskupa podataka i vizualizaciju ekstrahiranih podataka pomoću dostupnih Python biblioteka.

Ključne riječi: logs; event logs; server logs; Pyhon; web poslužitelji; parsiranje podataka; analiza podataka; vizualizacija podataka

Sadržaj

[Sadržaj iii](#_Toc49957730)

[1. Uvod 1](#_Toc49957731)

[2. Dnevnički zapisi i njihova svrha 2](#_Toc49957732)

[2.1. Dnevnički zapisi na osobnim računalima 3](#_Toc49957733)

[2.1.1. Windows Event Viewer 3](#_Toc49957734)

[2.1.2. Dnevnički zapisi na Linux platformama 6](#_Toc49957735)

[2.2. Dnevnički zapisi na web poslužiteljima 7](#_Toc49957736)

[2.2.1. Web poslužitelji 8](#_Toc49957737)

[*2.2.2.* *Common log format* 9](#_Toc49957738)

[*2.2.3.* *Extended common log format* 10](#_Toc49957739)

[*2.2.4.* *Microsoft IIS log format* 12](#_Toc49957740)

[3. Uvod u Pandas i Matplotlib 13](#_Toc49957741)

[4. Python aplikacija za analizu i vizualizaciju 21](#_Toc49957742)

[5. Zaključak 22](#_Toc49957743)

[Popis literature 23](#_Toc49957744)

[Popis slika 25](#_Toc49957745)

[Popis tablica 26](#_Toc49957746)

[Prilozi (1, 2, …) 27](#_Toc49957747)

1. Uvod

Osobna računala, web poslužitelji i informacijski sustavi generiraju dnevničke zapise (eng. *Logs*) koji dokumentiraju aktivnosti sustava. Takvi se zapisi sastoje od niza kronološki poredanih poruka koje sadrže informacije o aktivnostima i operacijama unutar operacijskog sustava, neke aplikacije, web poslužitelja ili nekog drugog uređaja. Analiza podataka dobivenih iz dnevničkih zapisa omogućuje praćenje ponašanja sustava i otkrivanje problema kao što su greške u radu ili napadi na sustav. Danas postoje i brojna programska rješenja za analizu dnevničkih zapisa koja omogućuju bolju ekstrakciju podataka iz dnevničkih zapisa i na taj način olakšavaju pronalaženje trendova i uzoraka u podacima pomoću kojih administratori sustava mogu donositi bolje poslovne odluke ili nadzirati sigurnost sustava. (E. Zhang, 2018)

U ovom radu bit će opisana organizacija dnevničkih zapisa na osobnim računalima i web poslužiteljima te izrađena vlastita Python aplikacija za analizu jednog formata dnevničkog zapisa.

1. Dnevnički zapisi i njihova svrha

Dnevnički zapisi su datoteke automatski generirane od strane računala koje sadrže popis događaja na tom računalu u obliku strukturiranih, kronološki poredanih poruka. Većina dnevničkih zapisa spremljeni su u formatu običnog teksta što omogućuje pregled u bilo kojem programu za uređivanje teksta i osigurava malu veličinu datoteke. (Christensson, 2010)

Postoji nekoliko standardiziranih formata dnevničkih zapisa, no uglavnom podaci, struktura, vrste i format poruka u dnevničkom zapisu nisu propisani pa tako ovise o odlukama i implementaciji razvojnih programera koji rade na razvoju određene aplikacije ili sustava. Iako se implementacije i formati poruka razlikuju sve su sastavljene od nekoliko zajedničkih komponenti. Svaka poruka ima datum i vrijeme kada je nastala, razinu zapisa, na primjer informativna poruka, poruka upozorenja, poruka greške ili neka druga definirana razina, i informacije o kontekstu koje nam pružaju dodatne informacije o stanju sustava ili aplikacije i okruženju u kojem je poruka nastala. (Lee, 2019)

Prema (Lee, 2019) dnevničke zapise možemo podijeliti na nekoliko osnovnih kategorija, a to su aplikacijski dnevnički zapisi (eng. *Application log*), sustavski dnevnički zapisi (eng. *System log*) i poslužiteljski dnevnički zapisi (eng. *Server log*). Aplikacijski dnevnički zapisi služe razvojnim programerima aplikacije kako bi lakše otkrili i otklonili probleme u radu aplikacije budući da se neki problemi ne mogu otkriti sve dok se aplikacija ne nađe u produkcijskoj okolini i bude dana na korištenje krajnjim korisnicima. Sustavski dnevnički zapisi sadrže informacije o radu sustava i sustavskim procesima dok poslužiteljski dnevnički zapisi bilježe informacije o korisnicima koji ga koriste.

Poslužiteljski dnevnički zapisi su od posebne važnosti za velike organizacije čije poslovanje ovisi o njihovoj mrežnoj infrastrukturi. Analiza i praćenje poslužiteljskih dnevničkih zapisa omogućuje im da povećaju pouzdanost svojih sustava ispravljanjem grešaka, sporih upita ili netočnih odgovora poslužitelja i na taj način poboljšaju iskustvo krajnjeg korisnika. Isto tako praćenjem dnevničkih zapisa osiguravaju sigurnost sustava i podataka od vanjskih napadača budući da ovi zapisi vode detalje o događajima vezanim za sigurnost kao što su uspiješne i neuspiješne prijave. Još jedan razlog za analizu poslužiteljskih dnevničkih zapisa je praćenje ponašanja korisnika na temelju kojega mogu optimizirati sustav da bolje odgovara njihovim potrebama ili donositi bolje poslovne odluke. Također organizacije mogu na vrijeme odgovoriti na povećanje opterećenja sustava zbog rasta broja korisnika uvođenjem dodatnih kapaciteta. (*What is a Log File? | Sumo Logic*, 2019)

Možemo reći da je glavna svrha svih dnevničkih zapisa dati korisnicima ili administratorima informacije o ponašanju sustava ili aplikacije kroz vrijeme kako bi pravovremeno mogli reagirati na probleme, greške i sigurnosne prijetnje u radu sustava ili mogli donositi bolje poslovne odluke. U narednim poglavljima ovog rada detaljnije će biti opisana organizacija dnevničkih zapisa na osobnim računalima i poslužiteljima.

* 1. Dnevnički zapisi na osobnim računalima

Na modernim operacijskim sustavima za osobna računala ugrađeni su mehanizmi i protokoli za snimanje događaja i vođenje dnevničkih zapisa o događajima u sustavu. Takvi zapisi daju korisnicima uvid u rad sustava i prikupljaju informacije o radu sklopovlja i programa, problemima u sustavu i sigurnosnim događajima. U ovom poglavlju bit će obrađena organizacija sustavskih dnevničkih zapisa na Windows platformi i alat Windows Event Viewer te organizacija sustavskih dnevničkih zapisa na Linux platformi.

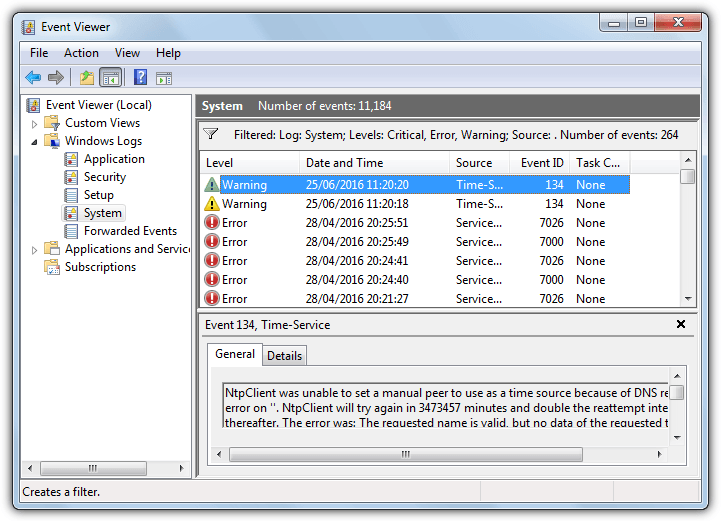
* + 1. Windows Event Viewer

Na Windows operacijskim sustavima dnevnički zapisi spremaju se u XML formatu na lokaciju *C:\WINDOWS\system32\config*. Svaki zapis sastoji se od (*Event Log Monitoring Tool - A Tutorial*, bez dat.):

1. Datum - datum na koji je događaj nastao
2. Vrijeme - vrijeme u koje je događaj nastao
3. Korisnik - prijavljeni korisnik u trenutku nastanka događaja
4. Računalo - naziv računala na kojem se događaj dogodio
5. ID događaja - identifikator događaja koji specificira tip događaja
6. Izvor - aplikacija ili komponenta koja je uzrokovala događaj
7. Tip ili razina - tip događaja prema važnosti

Na Windows platformi tip događaja ili razina zapisa može biti informacija (eng. *Information*), upozorenje (eng. *Warning*), greška (eng. *Error*), uspješna autorizacija (eng. *Success Audit*) ili neuspješna autorizacija (eng. *Failure Audit*). Informacija je događaj koji opisuje uspješnu operaciju neke radnje u aplikaciji, upravljačkom programu ili pokrenutom servisu. Upozorenje je događaj koji nije od prevelike važnosti, ali može ukazivati na neke buduće probleme koji bi mogli nastati. Greška je događaj koji ukazuje na problem koji je nastao u radu neke aplikacije ili komponente i pri tome uzrokovao gubitak podataka ili funkcionalnosti. Uspješna i neuspješna autorizacija su događaji koji opisuju uspješan ili neuspješan sigurnosni događaj, na primjer kada se korisnik uspješno ili neuspješno prijavi. (*Event Log Monitoring Tool - A Tutorial*, bez dat.)

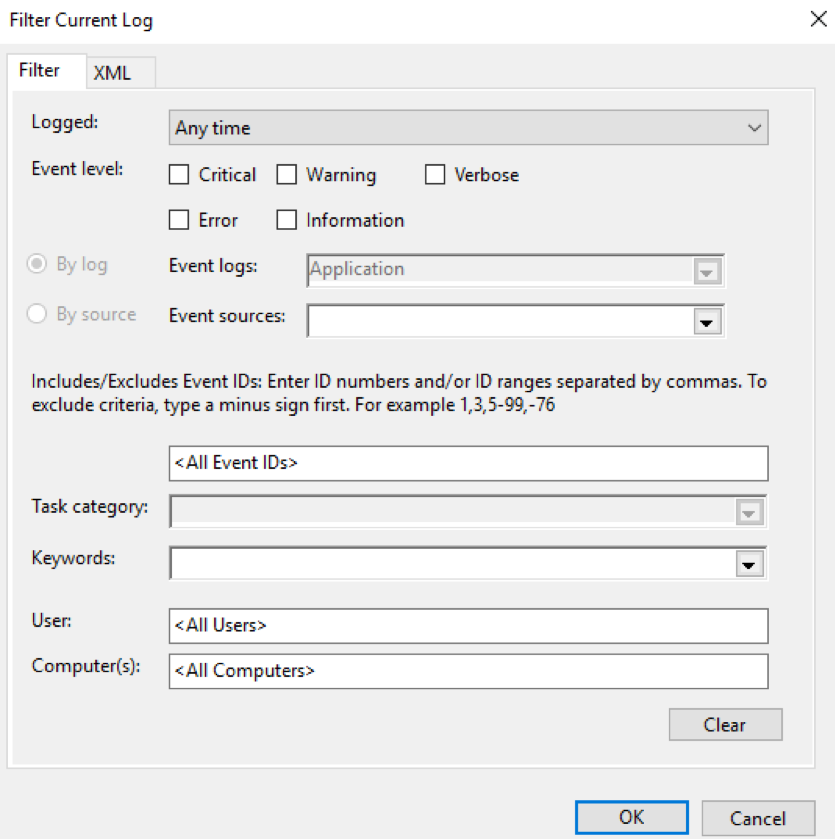
Event Viewer je sustavski alat koji dolazi u sklopu Windows operacijskog sustava i omogućuje pregled dnevničkih zapisa koje taj operacijski sustav generira. Alat omogućuje i dodatne opcije kao što su pretraživanje zapisa, filtriranje zapisa, izvoz zapisa u nekom drugom formatu pogodnom za daljnju analizu ili definiranje korisničkih vrsta događaja i dnevničkih zapisa.



Slika 1: Izgled sučelja Windows Event Viewer-a (Izvor: raymond.cc, 2020)

S lijeve strane sučelja nalazi se okvir za navigaciju u kojem možemo izabrati dnevnički zapis koji želimo pregledati. Postoji pet zadanih kategorija Windows dnevničkih zapisa i to aplikacije (eng. *Application*), sigurnost (eng. *Security*), instalacija (eng. *Setup*), sustav (eng. *System*) i proslijeđeni događaji (eng. *Forwarded Events*). U dnevničkom zapisu aplikacije nalaze se informacije o događajima koje su generirale aplikacije instalirane na računalu. Dnevnički zapis sigurnost sadrži informacije o uspješnim i neuspješnim sigurnosnim događajima na računalu. Dnevnički zapis instalacija sadrži poruke o događajima vezanim uz instalaciju i nadogradnju operacijskog sustava. Dnevnički zapis sustav sadrži poruke koje je generirao operacijski sustav dok dnevnički zapis proslijeđeni događaji sadrži poruke o događajima s drugih računala na mreži u slučaju da je računalo konfigurirano da prikuplja te podatke. (*Windows Logging Basics - The Ultimate Guide To Logging*, 2015)

Na desnoj strani sučelja nalazi se popis poruka u odabranom dnevničkom zapisu s detaljima o vremenu i okruženju u kojem je poruka nastala. Poruke su poredane kronološki od najstarijih na dnu prema najnovijim na vrhu. Odabirom neke od poruka možemo vidjeti opis događaja u donjem desnom okviru pod kraticom *General* i dodatne detalje pod kraticom *Details*. Alat omogućuje i napredno filtriranje dnevničkih zapisa prema različitim kriterijima kao što su vrijeme nastanka poruke, razina ili tip poruke, ključnim riječima, izvoru događaja, ID događaja, računalu ili korisniku.

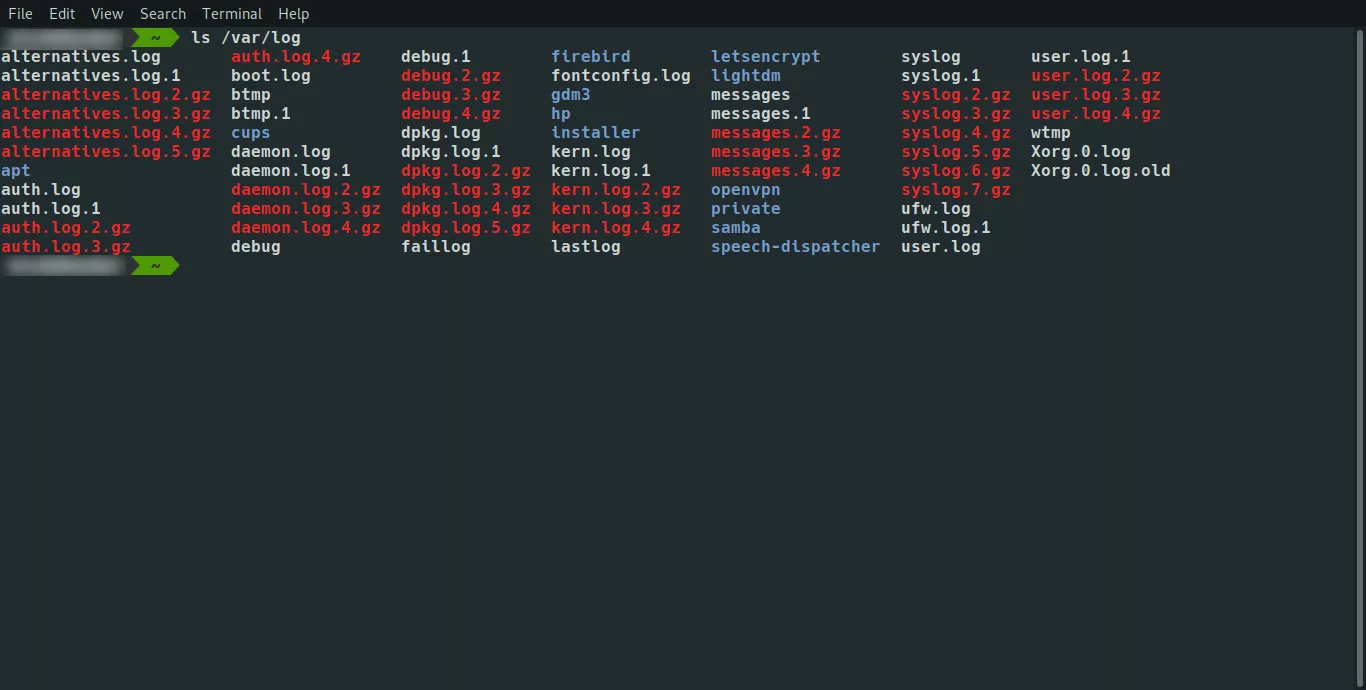


Slika 2: Opcije filtriranja u Event Viwer-u (Izvor: loggly.com, 2020)

* + 1. Dnevnički zapisi na Linux platformama

Program koji obavlja prikupljanje i sastavljanje dnevničkih zapisa na Linux platformama je *Sysklogd* i on se sastoji od dva alata, *syslogd* za prikupljanje sustavskih poruka i *klogd* za prikupljanje poruka jezgre sustava. (*sysklogd(8): system logging utilities - Linux man page*, bez dat.)

Na Linux operacijskim sustavima dnevnički zapisi spremljeni su u tekstualnom obliku na lokaciji */var/log* ili u nekom od poddirektorija vezanim uz pojedinu aplikaciju. Neki dnevnički zapisi komprimiraju se zbog svoje veličine pa imaju *.gz* nastavak. Svaki zapis definiran je *Syslog* formatom i sastoji se od standardiziranog zaglavlja. Zaglavlje sadrži datum i vrijeme nastanka događaja, naziv aplikacije koja je generirala događaj, mjesto na računalu koje je izvor poruke i prioritet poruke. Pri tome se prioritet poruke sastoji od dva broja od kojih prvi opisuje tip procesa koji je generirao događaj i može biti u rasponu od 0 do 23 gdje 0 označava poruku jezgre sustava, a 23 poruku aplikacije pokrenute na sustavu. Drugi broj odnosi se na važnost poruke i može biti između 0 i 7 gdje 0 znači da je poruka hitna i sustav se ne može koristiti, a poruka važnosti 7 opisuje pogrešku. Format poruke može se modificirati pomoću datoteke za konfiguraciju. (*Linux Logging Basics - The Ultimate Guide To Logging*, 2015)



Slika 3: Primjer sadržaja */var/log* direktorija (Izvor: lifewire.com, 2020)

Prema (*Linux Logging Basics - The Ultimate Guide To Logging*, 2015) neki od važnijih dnevničkih zapisa na Linux platformama su:

1. */var/log/syslog* ili */var/log/messages*
2. */var/log/auth.log* ili */var/log/secure*
3. */var/log/kern.log*
4. */var/log/cron*

Točan naziv datoteke ovisi o verziji operacijskog sustava, na primjer verzije bazirane na *Debian*-u koriste */var/log/syslog* i */var/log/auth.log* dok verzije bazirane na *Red Hat*-u koriste */var/log/messages* i */var/log/secure.* Dnevnički zapis *syslog* ili *messages* sadrži opće poruke sustava i informacije vezane uz rad sustava. Dnevnički zapis *auth.log* ili *secure* sadrži informacije o događajima vezanim za sigurnost kao što su prijava korisnika i slično. *Kern.log*  sadrži zapise o događajima, greškama i upozorenjima koje je generirala jezgra operacijskog sustava. *Cron* sadrži zapise o izvođenju korisnički zakazanih zadataka.

Dnevnički zapisi na Linux platformama također podržavaju rotiranje kako bi se izbjegla prevelika veličina datoteka. Alat *log rotate* obavlja ovu funkciju na način da briše dnevničke zapise starije od postavljenog vremenskog intervala i stvara nove umjesto njih. Namještanje vremeskog intervala vrši se u */etc/logrotate.conf* datoteci te se za svaku aplikaciju može postaviti vlastiti interval rotacije dnevničkog zapisa, hoće li se zapis komprimirati, slanje zapisa na e-mail prije brisanja i brojne druge opcije. (Haas, 2020)

* 1. Dnevnički zapisi na web poslužiteljima

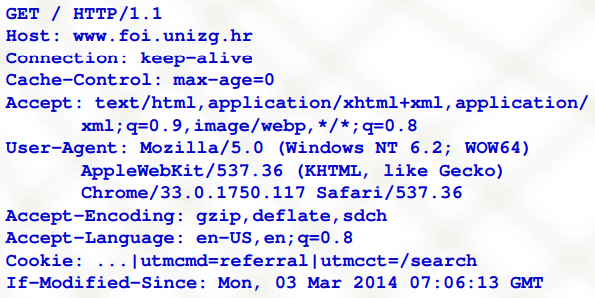
Na strani poslužitelja dnevničke zapise možemo podijeliti na nekoliko kategorija ovisno o vrsti informacija koje se u njih zapisuju, a to su dnevnički zapis pristupa (eng. *Access log*), dnevnički zapis agenata (eng. *Agent log*), dnevnički zapis grešaka (eng. *Error log*) i dnevnički zapis upućivanja (eng. *Referrer log*). I ovi dnevnički zapisi najčešće se u tekstualnom obliku i i njima se vode zapisi o aktivnosti poslužitelja. U dnevnički zapis pristupa spremaju se podaci o korisnicima od kojih su stigli zahtjevi za sadržajem i informacije o zahtjevima za sadržaj koje je web poslužitelj zaprimio kao što su metoda kojom je zahtjev poslan, statusni kod odgovora i vrijeme potrebno za odgovor na zahtjev. Dnevnički zapis agenata sadrži zapise o vrsti i verziji web preglednika sa kojeg je korisnik uputio zahtjev prema web poslužitelju. U dnevnički zapis grešaka generiraju se poruke o pogreškama odgovora web poslužitelja, na primjer u slučaju da je korisnik zatražio sadržaj koji se više ne nalazi na poslužitelju ili korisnik nema po pristup traženom sadržaju. U dnevničkom zapisu upućivanja vodi se popis stranica na kojima se korisnik nalazio neposredno prije nego što je poslao zahtjev prema poslužitelju tj. linkovi s kojih je korisnik upućen prema poslužitelju koji mogu poslužiti kako bi analizirali izvor korisničkog prometa prema poslužitelju. (Six, 2020a)

Česta praksa kod rukovanja s dnevničkim zapisima na strani poslužitelja je prikupljanje svih dnevničkih zapisa na jedno računalo radi lakše analize. Većina poslužiteljskih sustava ima mogućnost periodičkog slanja svojih dnevničkih zapisa na udaljenu lokaciju, a postoje i brojna druga programska rješenja za ovu namjenu. Problem koji se javlja kod centraliziranog prikupljanja dnevničkih zapisa je velika količina podataka koji se generiraju, već jedan korisnik može generirati tisuće zapisa pri jednom pristupu sadržaju poslužitelja, pa je najbolja praksa dnevničke zapise filtrirati i po potrebi pretvoriti u zajednički format pogodan za analizu prije slanja na centralno računalo ili poslužitelj za daljnju obradu. (A. Grimes, 2018)

U nastavku poglavlja bit će ukratko opisan princip rada web poslužitelja i nekoliko odabranih formata poslužiteljskih dnevničkih zapisa.

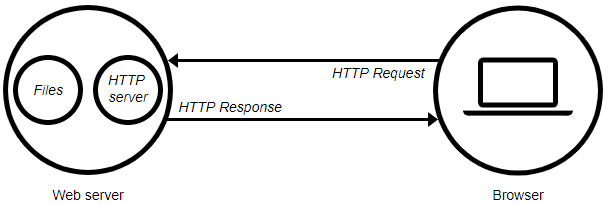
* + 1. Web poslužitelji

Web poslužitelji (eng. *Web server*)su računala s pripadnom programskom podrškom koja mogu zaprimati, obrađivati i odgovarati na zahtjeve klijenta pomoću HTTP ili drugih protokola. Klijent pomoću web preglednika (eng. *Browser*) šalje HTTP zahtjev koji sadrži informacije o klijentu, vrsti zahtjeva i traženom sadržaju prema web poslužitelju koji zatim prihvaća zahtjev i pronalazi traženi sadržaj te ga vraća klijentu u obliku HTTP odgovora. Ako traženi sadržaj nije pronađen ili je došlo do greške web poslužitelj vraća jedan od definiranih HTTP statusnih kodova. (*What is a web server? - Learn web development | MDN*, 2020)



Slika 4: Primjer HTTP zahtjeva (Izvor: Kermek D., 2020)

Sadržaj koji se vraća klijentu može biti statička web stranica ili dinamički generirana web stranica. Statička web stranica ima predefiniranu strukturu i sadržaj, najčešće pomoću HTML-a i CSS-a, pa je ista za svakog klijenta kojem se šalje. Svaka stranica spremljena je na web poslužitelju kao zaseban dokument i ukoliko ga je potrebno izmijeniti to može napraviti samo administrator. S druge strane, dinamički generirane web stranice generiraju se u stvarnom vremenu uzimajući u obzir klijenta koji je poslao zahtjev. Na web poslužitelju spremljeni su samo predlošci i dizajn za web stranicu dok se sadržaj popunjava iz baze podataka ili nekog drugog izvora pomoću nekog od programskih jezika za programiranje na strani poslužitelja kao što su PHP, ASP i drugi. (Robben, 2019)



Slika 5: Princip rada web poslužitelja (Izvor: MDN, 2020)

* + 1. *Common log format*

*Common log format,* poznat i pod nazivom *NCSA Common log format,* je standardizirani format dnevničkog zapisa koji se ne može uređivati ili prilagođavati. Ovaj format nije dostupan za FTP poslužitelje. Svaki zapis sastoji se od sljedećih elemenata (Six, 2020b):

1. IP adresa domaćina
2. identifikator korisnika - prema RFC 1413 protokolu (najčešće prazno)
3. korisničko ime
4. datum, vrijeme i vremenska zona
5. metoda i sadržaj koji se dohvaća
6. HTTP statusni kod
7. veličina dohvaćenog sadržaja - izražena u bajtovima

U ovom formatu uzima se lokalno vrijeme domaćina s vremenskom zonom, prazna polja označena su povlakom (-), a sama polja odvojena su razmakom. Primjer jednog ovakvog zapisa bio bi (Izvor: Izrada autora):

127.0.0.1 - lmodric [13/May/2020:16:36:46 +0200] "GET /projekt/css/style.css HTTP/1.1" 200 7701

U ovom primjeru IP adresa domaćina tj. računala s kojeg je zahtjev stigao je 127.0.0.1, identifikator korisnika je prazan, korisničko ime je lmodric, zahtjev je stigao 13. Svibnja 2020 godine u 16:36:46 sati po vremenskoj zoni GMT +2. Metoda kojom se sadržaj dohvaća je *GET*, sadržaj je datoteka pod nazivom *style.css* iz direktorija */projekt/css/* na poslužitelju. Na kraju zapisa vidimo da je poslužitelj odgovorio s HTTP statusnim kodom 200 za OK i veličinu tražene datoteke koja iznosi 7701 bajta.

* + 1. *Extended common log format*

*Extended common log format* vrlo je sličan *Common log format*-u, ali uključuje neka dodatna polja i fleksibilan je pa tako pruža više informacija. U ovom formatu zapisa imamo mogućnost dodavanja polja koja su nam važna i uklanjanje polja s informacijama koje nam nisu bitne. Na ovaj način moguće je utjecati i na veličinu datoteke dnevničkog zapisa. Polja su kao i kod *Common log format*-a odvojena razmakom, prazna polja označena su povlakom (-), ali vrijeme i datum zapisuju se prema *UTC* vremenu. *Extended common log format* datoteka započinje popisom smjernica (eng. *Directives*) označenih ljestvama (#) za taj dnevnički zapis i to mogu biti (M. Hallam-Baker & Behlendorf, bez dat.):

1. Verzija - u obliku cijeli broj.cijeli broj
2. Polja - popis polja koja su uključena u zapis
3. Program - naziv programa koji je generirao zapis
4. Početni datum - datum i vrijeme nastanka dnevničkog zapisa
5. Završni datum - datum i vrijeme završetka dnevničkog zapisa
6. Datum - datum i vrijeme nastanka zapisa
7. Komentar - komentar s dodatnim informacijama o dnevničkom zapisu

Od ovih smjernica samo su verzija i polja obavezne. Smjernica polja opisuje od kojih elementata će se sastojati svaki zapis, a dostupna polja su redom:

1. datum - datum kada je zapis nastao
2. vrijeme - vrijeme u koje je zapis nastao
3. vrijeme obrade - vrijeme potrebno da se zahtjev obradi
4. bajtovi - veličina prenesenog sadržaja
5. priručna memorija - informacija je li se traženi sadržaj već nalazio u priručnoj memoriji
6. ip - ip adresa i port
7. dns - naziv DNS poslužitelja
8. status - HTTP statusni kod
9. komentar - komentar koji je vraćen uz statusni kod
10. metoda - metoda korištena za dohvaćanje sadržaja
11. uri - URI link
12. uri-stem - korijenski dio URI-a
13. uri-query - dio URI-a koji sadrži upit

U ovom formatu definirani su i prefiksi za polja. Za polja od a) do e) oni nisu obavezni dok su za ostala polja obavezni. Definirani prefiksi daju informaciju o tome između koga se zahtjev razmijenio i mogu biti:

1. c - prefiks koji označava klijenta
2. s - prefiks koji označava poslužitelja
3. r - prefiks koji označava udaljenog poslužitelja
4. cs - prefiks koji označava prijenos od klijenta do poslužitelja
5. sc - prefiks koji označava prijenos od poslužitelja do klijenta
6. sr - prefiks koji označava prijenos od poslužitelja do udaljenog poslužitelja
7. rs - prefiks koji označava prijenos od udaljenog poslužitelja do poslužitelja
8. x - prefiks koji identificira specifičnu aplikaciju

Primjer jednog dnevničkog zapisa ovog formata ima sljedeći oblik: (Izvor: w3.org, 2020):

#Version: 1.0

#Date: 12-Jan-1996 00:00:00

#Fields: time cs-method cs-uri

00:34:23 GET /foo/bar.html

12:21:16 GET /foo/bar.html

12:45:52 GET /foo/bar.html

12:57:34 GET /foo/bar.html

U ovom primjeru vidljivo je da je korištena verzija *Extended common log format*-a 1.0, zapis je dodan 12. Siječnja 1996 godine u 00:00:00 sati. Definirana polja u zapisu su vrijeme, metoda kojom je klijent poslao zahtjev i uri koji je klijent poslao prema poslužitelju, a smjer slanja opisan je prefiksom cs. Na kraju zapisa vidimo 4 linije koje pokazuju da je klijent poslao 4 *GET* zahtjeva za sadržajem */foo/bar.html* u različitim vremenima.

* + 1. *Microsoft IIS log format*

Ovaj format dnevničkog zapisa vrlo je sličan *Common log format*-u, također je fiksnog oblika i ne može se prilagođavati, ali pruža neka dodatna polja i samim time više informacija. Kod ovog formata vrijednosti polja u zapisu odvojena su zarezom (,), za polja kojima je vrijednost nepoznata koristi se povlaka (-), a u slučaju da polje sadrži znak koji se ne može printati (eng. *Nonprintable character*) koristi se plus (+) kako bi se zaštitio format zapisa. Ovo se može dogoditi u slučaju napada na sustav kod kojeg napdači šalju *CR* i *LF* znakove za kraj linije koji bi mogli uništiti strukturu zapisa i tako cijelu datoteku dnevničkog zapisa učiniti beskorisnom. Za vrijeme zapisa uzima se lokalno vrijeme računala, a vrijeme obrade mjeri se u milisekundama. (*IIS Logging | Microsoft Docs*, 2018)

Svaki zapis može se sastojati od sljedećih polja (*Brief introduction of log file formats*, bez dat.):

1. IP adresa klijenta
2. korisničko ime - korisničko ime ako je klijent autenticiran na poslužitelju
3. datum - datum na koji je zapis nastao
4. vrijeme - vrijeme u koje je zapis nastao
5. servis i instanca - servis i instanca koju je klijent koristio
6. naziv poslužitelja - naziv poslužitelja na kojem je generiran zapis
7. IP adresa poslužitelja
8. vrijeme obrade - vrijeme koje je bilo potrebno za obradu zahtjeva
9. bajtovi poslani od klijenta - količina bajtova koju je poslao klijent
10. bajtovi poslani od poslužitelja - količina bajtova koju je poslao poslužitelj
11. HTTP statusni kod
12. Windows statusni kod - Windows definirani kodovi, 0 označava uspjeh
13. metoda zahtjeva - metoda korištena za dohvaćanje sadržaja
14. ciljani sadržaj zahtjeva - naziv datoteke sadržaja koji se dohvaća

Prema (*Brief introduction of log file formats*, bez dat.) primjer jednog zapisa ovog formata ima sljedeći oblik:

192.168.114.201,-,03/20/98,7:55:20,W3SVC2,SALES1,192.168.114.201, 4502,163,3223,200,0,GET,DeptLogo.gif

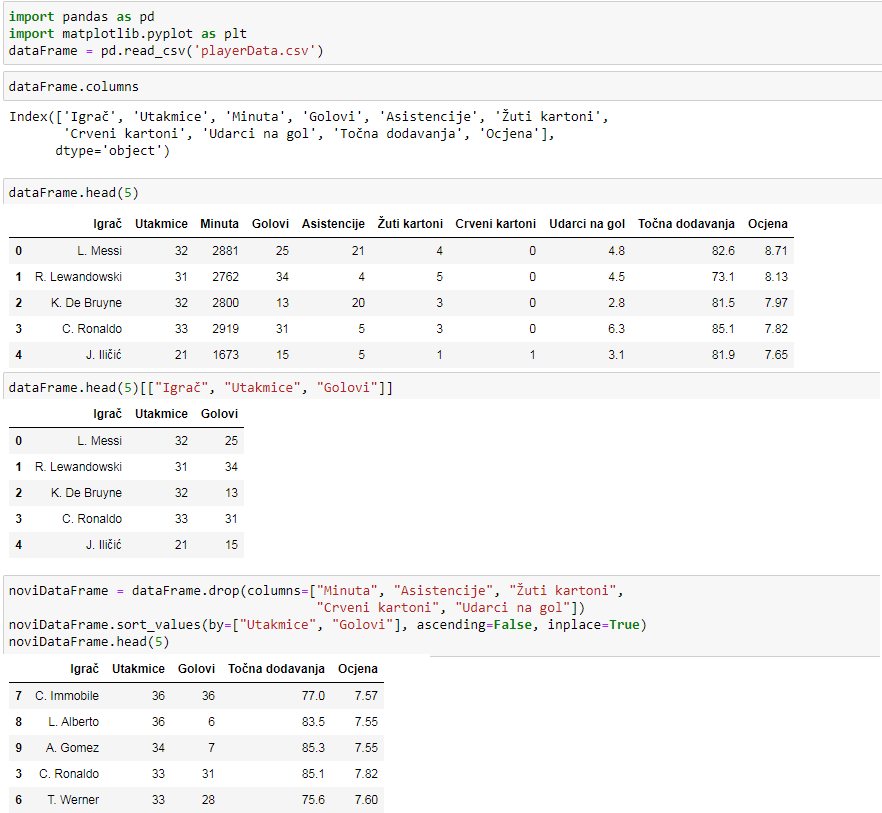
Iz ovog zapisa možemo redom pročitati vrijednosti polja. IP adresa klijenta je 192.168.114.201, korisničko ime je prazno što je označeno povlakom, zahtjev je zaprimljen 20. ožujka 1998. godine u 7:55:20 sati, servis i instanca je W3SVC2, naziv poslužitelja je SALES1, IP adresa poslužitelja je 192.168.114.201, vrijeme obrade iznosilo je 4502 milisekunde, klijent je poslao 163 bajta podataka dok je poslužitelj odgovorio s 3223 bajta podataka. HTTP statusni kod odgovora je 200 za OK, Windows statusni kod je 0 što označava uspješno obrađen zahtjev, metoda kojom je klijent poslao zahtjev je *GET*, a traženi sadržaj je datoteka naziva *DeptLogo.gif.*

1. Uvod u Pandas i Matplotlib

Pandas i Matplotlib su dobro poznate Python biblioteke za strukturiranje, obradu i vizualizaciju podataka. U ovom poglavlju bit će na kratkom primjeru pokazan rad s ovim bibliotekama i neke osnovne funkcionalnosti. Za rad i demonstraciju koristit ću Jupyter Notebook alat.

Pandas se uglavnom koristi za analizu podataka i omogućuje čitanje i manipuliranje različitim formatima podataka npr. JSON, CSV ili Excel tablice. Dva glavna objekta kojima se manipulira u radu s Pandas bibliotekom su *Series* i *Dataframe*. *Series* je struktura slična listi i sadrži jednu listu podataka uz koju može biti i lista s nazivom koja se naziva index. Na ovu strukturu možemo gledati kao jedan stupac u tablici. *Dataframe* predstavlja podatke organizirane u tablicu gdje je svaki stupac jedan *Series* objekt koji sadrži jednu vrstu podataka. *Dataframe* možemo stvoriti učitavanjem podataka iz neke vanjske datoteke, *Series* objekta, Python riječnika ili obične liste.

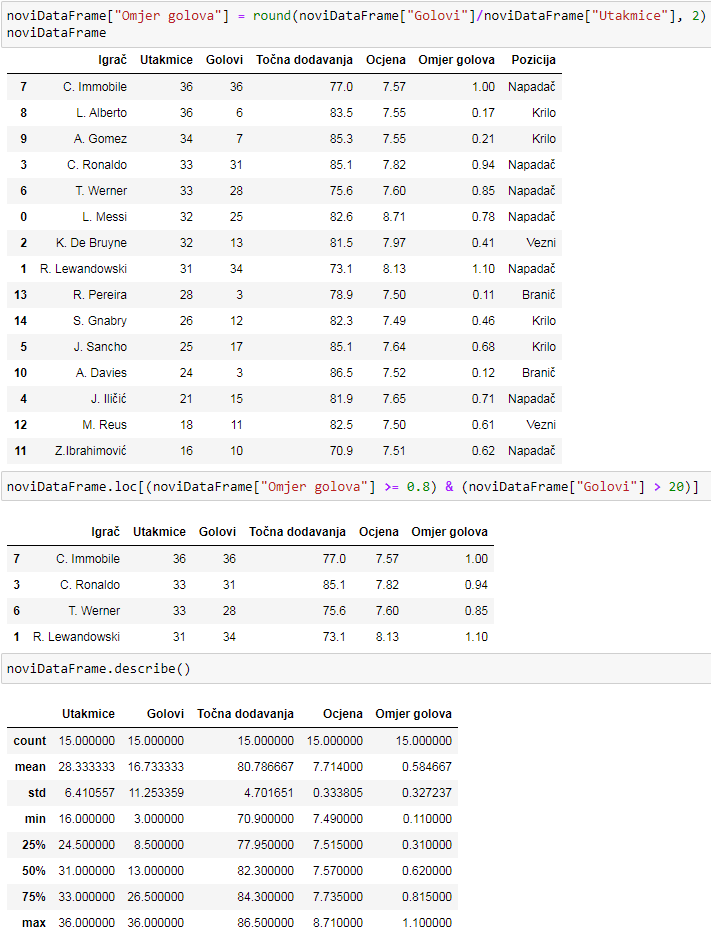
Kako bi započeli rad s ovim bibliotekama moramo ih prvo uključiti u program naredbom import. Set podataka koji ću koristiti u primjeru su statistike nogometnih igrača za prvih 15 igrača preuzete sa stranice *whoscored.com* (*whoscored.com/Statistics*)i prebačene u .csv format*.* Nakon što smo uključili biblioteku kreiramo *Dataframe* objekt pomoću *read\_csv­* funkcije kojoj kao argument predajemo naziv datoteke pod uvjetom da se ona nalazi u istom direktoriju kao i naš program. Možemo pogledati strukturu učitane datoteke tako da pomoću naredbe *print()* prikažemo *Dataframe* objekt, no ovo nije praktično za jako velike datoteke pa stoga koristimo naredbu *head()* koja kao argument može primiti koliko redova želimo pogledati i vraća prvih n redova u objektu.



Slika 6: Prvi primjer rada s *dataframe* objektom (Izvor: izrada autora)

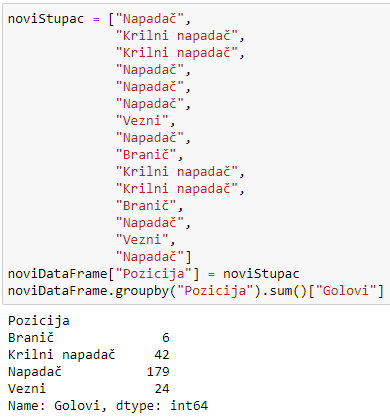
U ovom primjeru učitana je datoteka „playerData.csv“ u varijablu *dataFrame* i prikazani su nazivi stupaca u objektu pomoću atributa *columns*. Zatim je pomoću *head()* funkcije prikazano samo prvih 5 zapisa, a u drugom primjeru samo prvih 5 zapisa s odabranim stupcima koji su predani kao lista elemenata. Nakon toga stvorena je nova varijabla *noviDataFrame* u koju je spremljena kopija *dataFrame* objekta bez odabranih stupaca koji su uklonjeni pomoću naredbe *drop().* Elementi u novom objektu su zatim sortirani prvo prema stupcu „Utakmice“ i zatim prema stupcu „Golovi“ od najvećeg prema najmanjem.

Osim sortiranja i brisanja postojećih stupaca možemo dodavati vlastite stupce ili filtrirati stupce po nekom uvjetu. U sljedećem primjeru dodan je stupac „Omjer golova“ kao omjer vrijednosti u stupcima „Golovi“ i „Utakmice“ zaokruženo na dva decimalna mjesta, a zatim su pomoću *loc* metode prikazani samo oni igrači za koje je vrijednost u stupcu „Omjer golova“ veća ili jednaka od 0.8 i vrijednost u stupcu „Golovi“ veća od 20. Možemo primjetiti da su podaci u objektu ostali sortirani iz prijašnjeg primjera zbog argumenta *inplace=True* zbog kojeg je sortiran postojeći objekt.Pomoću metode *describe()* možemo vidjeti neke osnovne statističke informacije o odabranom *dataframe* objektu kao što su minimalna i maksimalna vrijednost, broj zapisa, prosjek i slično za svaki stupac.



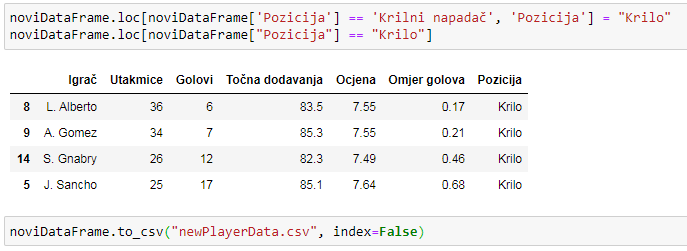
Slika 7: Drugi primjer rada s *dataframe* objektom (Izvor: izrada autora)

Još jedna zanimljiva metoda za obradu podataka je *groupby()*  koja nam omogućuje da podatke grupiramo prema jednom ili više stupaca pa onda na grupirane podatke primijenimo neke druge funkcije npr. *mean(), sum(), max(), min()* i ostale. U sljedećem primjeru prvo je stvorena nova lista s popisom nogometnih pozicija koje odgovaraju igračima u objektu te je zatim ta lista dodana u *dataframe* kao novi stupac. Na novi objekt zatim je primijenjena metoda *groupby()* s parametrom „Pozicija“ te je na tako grupirane igrače primijenjena metoda *sum()* s parametrom „Golovi“. Rezultat ovih operacija je prikaz ukupnog broja golova prema pozicijama igrača.



Slika 8: Treći primjer rada s *dataframe* objektom (Izvor: izrada autora)

Ako želimo izmijeniti neku vrijednost u cijelom objektu to možemo učiniti kombinacijom *loc()* metode i uvjeta po kojem mijenjamo vrijednost. U sljedećem primjeru sve pojave vrijednosti „Krilni napadač“ zamijenjene su vrijednošću „Krilo“. Na kraju kada smo zadovoljni s modificiranim podacima možemo cijeli *dataframe* objekt spremiti u nekom obliku po izboru. Ja sam u ovom slučaju koristio metodu *to\_csv()* kako bi *noviDataFrame* objekt spremio u .*csv* obliku.

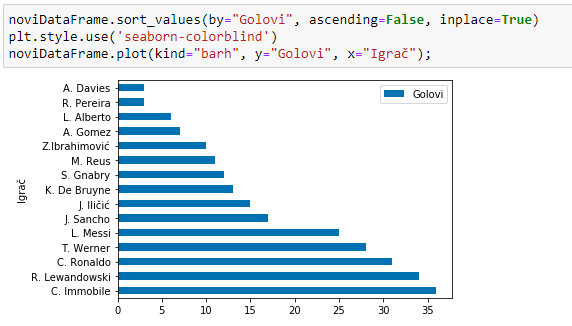


Slika 9: Četvrti primjer rada s *dataframe* objektom (Izvor: izrada autora)

U sljedećem dijelu ovog poglavlja ukratko ću opisati vizualizaciju podataka pomoću Matplotlib biblioteke. Koristit ću isti set podataka kao i ranije tj. isti *dataframe* objekt.

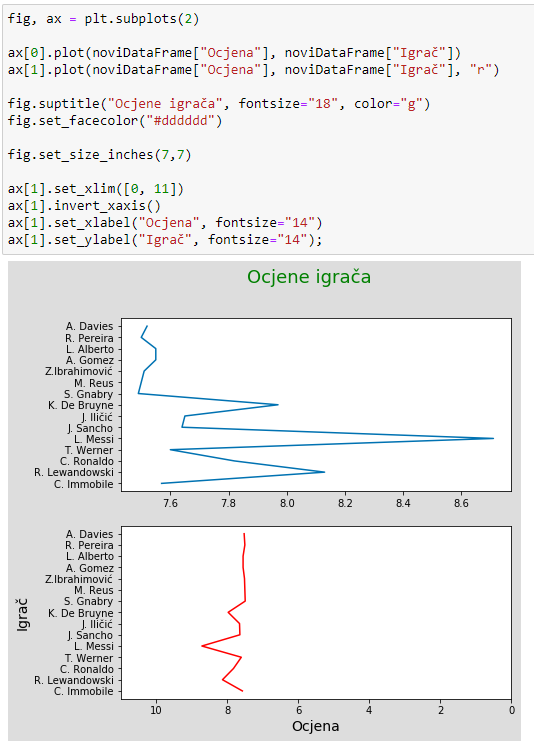
Kod Matplotlib biblioteke rad se svodi na manipulaciju objektima *Figure* i *Axes*. *Figure* je konačna slika i sadrži cijeli graf. Može se sastojati od ostalih elemenata kao što su podgrafovi, naslovi, podnaslovi, legende i drugi elementi. *Axes* definira podgraf koji je dio *Figure* objekta i može imati vlastito definirane elemente poput raspona x-osi, raspona y-osi, labela na osima, tip grafa, boje i ostalih elemenata.

U prvom primjeru prije crtanja grafa sortiran je *dataframe* i pozvana je funkcija *style.use* kojom je stil grafova postavljen na *„seaborn-colorblind“*, jedan od predefiniranih stilova u biblioteci. Jednostavnim pozivom funkcije *plot()* nad Pandas objektom i proslijeđivanjem parametara koji opisuju vrstu grafa i elemente na osima na brz način možemo dobiti vizualizaciju podataka. U ovom slučaju za vrstu grafa odabrao sam horizontalni stupčasti graf (*hbar)* te kao vrijednosti na x-osi broj golova igrača, a na y-osi ime igrača. No ovakav način rada ne dopušta nam uređivanje pojedinih detalja na grafu pa je stoga u sljedećim primjerima pokazan rad u kojem se direktno manipulira Matplotlib objektima.



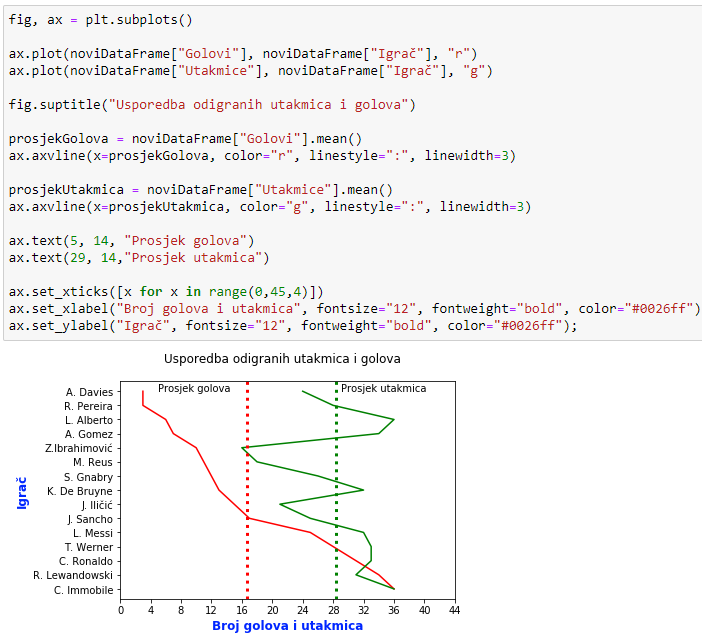
Slika 10: Primjer rada s *plot()* funkcijom (Izvor: Izrada autora)

U sljedećem primjeru na jedan *Figure* element dodana su dva *Axes* objekta koji prikazuju iste podatke, ali su na drugom podgrafu uređeni neki detalji poput raspona x-osi, boje linije i smjera x-osi. Na podgrafu za koji nisu definirani nikakvi detalji prikazan je stilom koji je odabran na početku, a raspon x-osi je određen automatski. Na *Figure* element također je dodan podnaslov i uređena je pozadinska boja. Svaki od dodanih grafova moguće je posebno uređivati prema želji te postoje brojne druge opcije koje je moguće prilagođavati.



Slika 11: Primjer s dva *Axes* objekta na istom *Figure* objektu (Izvor: Izrada autora)

U zadnjem primjeru na istom grafu prikazana su dva seta podataka. Crvenom linijom prikazan je broj golova po igraču dok je zelenom linijom prikazan broj odigranih utakmica po igraču. Zatim je za svaki set podataka izračunat prosjek te su na graf dodane vertikalne linije koje ga prikazuju pomoću funkcije *axvline()* i pripadajuće labele za te linije koje su dodane pomoću funkcije *text()*. Na kraju je za graf modificirana podjela x-osi i postavljene su labele za svaku od osi s definiranom veličinom i bojom slova.



Slika 12: Složeniji primjer uređivanja grafa (Izvor: Izrada autora)

Biblioteka Matplotlib nudi brojne druge opcije prilagođavanja *Figure* i *Axes* objekata i kombiniranja različitih vrsti i detalja grafova. Dodatne informacije mogu se pronaći u dokumentaciji koja je opsežna i detaljno opisuje svaku opciju.

1. Python aplikacija za analizu i vizualizaciju

log izvor : <https://github.com/elastic/examples/blob/master/Common%20Data%20Formats/apache_logs/apache_logs>

1. Zaključak

Ovdje treba sažeto rezimirati najvažnije rezultate razrade teme rada. Potrebno je sažeto opisati što je predmet rada, koje su metode, tehnike, programski alati ili aplikacije korištene u razradi rada te koje su pretpostavke dokazane, a koje opovrgnute. Sadržajno, ono što se u uvodu rada najavljuje i kasnije je obuhvaćeno u samom radu, moralo bi biti opisano u zaključnom dijelu kroz rezultate rada.

Popis literature

A. Grimes, R. (2018). *Why you need centralized logging and event log management | CSO Online*. https://www.csoonline.com/article/3280123/why-you-need-centralized-logging-and-event-log-management.html

*Brief introduction of log file formats*. (bez dat.). Preuzeto 29. kolovoz 2020., od https://www.loganalyzer.net/log-analysis/log-file-format.html#W3CExtendedLogFileFormat

Christensson, P. (2010, travanj 14). *Log File Definition*. https://techterms.com/definition/logfile

E. Zhang. (2018). *What is Log Analysis? Use Cases, Best Practices, and More | Digital Guardian*. https://digitalguardian.com/blog/what-log-analysis-use-cases-best-practices-and-more

*Event Log Monitoring Tool - A Tutorial*. (bez dat.). Preuzeto 24. kolovoz 2020., od https://www.manageengine.com/network-monitoring/Eventlog\_Tutorial\_Part\_I.html

Haas, J. (2020, veljača 14). *What Are Linux Log Files and How Can You Read Them?* https://www.lifewire.com/introduction-to-linux-log-files-2192233

*IIS Logging | Microsoft Docs*. (2018, svibanj 31). https://docs.microsoft.com/en-us/windows/win32/http/iis-logging

Lee, D. (2019). *Application Logs: What They Are and How to Use Them - XpoLog*. https://www.xplg.com/application-logs-what-how/

*Linux Logging Basics - The Ultimate Guide To Logging*. (2015, rujan 15). https://www.loggly.com/ultimate-guide/linux-logging-basics/

M. Hallam-Baker, P., & Behlendorf, B. (bez dat.). *Extended Log File Format*. Preuzeto 28. kolovoz 2020., od https://www.w3.org/TR/WD-logfile.html

Robben. (2019, studeni). *How do servers work? A Detailed Guide into Web Servers*. https://host4geeks.com/blog/how-do-servers-work/?

Six, B. (2020a). *Server Log Files in a Nutshell | Graylog*. https://www.graylog.org/post/server-log-files-in-a-nutshell

Six, B. (2020b, siječanj 15). *Log Formats – a (Mostly) Complete Guide | Graylog*. https://www.graylog.org/post/log-formats-a-complete-guide

*sysklogd(8): system logging utilities - Linux man page*. (bez dat.). Preuzeto 26. kolovoz 2020., od https://linux.die.net/man/8/sysklogd

*What is a Log File? | Sumo Logic*. (2019). https://www.sumologic.com/glossary/log-file/

*What is a web server? - Learn web development | MDN*. (2020). https://developer.mozilla.org/en-US/docs/Learn/Common\_questions/What\_is\_a\_web\_server

*Windows Logging Basics - The Ultimate Guide To Logging*. (2015, rujan 15). https://www.loggly.com/ultimate-guide/windows-logging-basics/

Popis slika

[Slika 1: Izgled sučelja Windows Event Viewer-a 4](#_Toc49957718)

[Slika 2: Opcije filtriranja u Event Viwer-u 5](#_Toc49957719)

[Slika 3: Primjer sadržaja */var/log* direktorija 6](#_Toc49957720)

[Slika 4: Primjer HTTP zahtjeva 8](#_Toc49957721)

[Slika 5: Princip rada web poslužitelja 9](#_Toc49957722)

[Slika 6: Prvi primjer rada s *dataframe* objektom 14](#_Toc49957723)

[Slika 7: Drugi primjer rada s *dataframe* objektom 15](#_Toc49957724)

[Slika 8: Treći primjer rada s *dataframe* objektom 16](#_Toc49957725)

[Slika 9: Četvrti primjer rada s *dataframe* objektom 17](#_Toc49957726)

[Slika 10: Primjer rada s *plot()* funkcijom 18](#_Toc49957727)

[Slika 11: Primjer s dva *Axes* objekta na istom *Figure* objektu 19](#_Toc49957728)

[Slika 12: Složeniji primjer uređivanja grafa 20](#_Toc49957729)

Popis tablica

Popis tablica treba biti izrađen po uzoru na indeksirani sadržaj, te upućivati na broj stranice na kojoj se tablica može pronaći.

[Tablica 1: Prikaz podataka o učestalosti pojavljivanja objekta 7](#_Toc496692416)

Prilozi (1, 2, …)