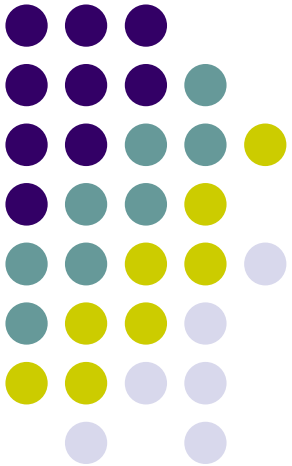
Windows Operativni sistem

Upoznavanje sa Registry Bazom podataka i ažuriranje iste



Šta je Registry i čemu služi?

Registri je hijerarhijska baza podataka svih podešavanja neophodnih za rad i instalaciju Windowsa i programa koji su pod njim instalirani (informacije i hardveru, konfiguraciji, o programima i datotekama, profilima i grupama korisnika, o podešavanju direktorijuma i datoteka).

Broj elemenata 50.000 – 1.000.000 (zavistan od broja korisnika i kolicine instaliranih programa)

Prvi put korišćen u Windows 95

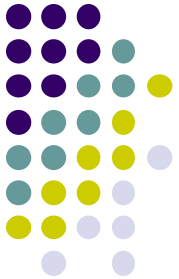
Centralizacija informacija u Registry ima dve prednosti:

- Sve informacije se nalaze na jednom mestu
- Lako se pravi rezervna kopija baze, te se može restaurirti.

Mana – oštećenje Registy-a znači oštećenje Windowsa

NAPOMENA: Ukoliko “petljate” po Registry, možete isključiti delove Windows-ove funkcionalnosti do te mere da se računar ne može ni podići. **Obavezno pravljenje rezervnih kopija pre bilo koje aktivnosti u Registry bazi!!!**

Zašto raditi sa Registry?



Zbog neophodnog predznanja i iskustva u radu sa Registry, Windows ne obezbeđuje direktni korisnički interfejs za prikaz i menjanje Registry sadržja (paradoks).

Ipak , neki parametri, čije se informacije čuvaju u Registry imaju svoje programe za rad i upravljanje njima, npr. Control Panel.

Razlika prikaza podataka u nekim od programa za podešavanje i održavanje sitema i Registy je u razumljivosti prikaza podataka.

Kad raditi sa Registry:

- menjate važne informacije za koje nema korisnički interfejs
- “pošlo je nešto naopako”
- pravite programe ili koristite makro jezik za pravljanje automatizovanih postupaka (VBA u Wordu, Excelu ili Outlooku)
- za zapisivanje “čudnih” informacija (imena, adresa,...) ali to je krajnje neefikasan i neprimeren posao za Registry, a
- najčešće, čuli ste za sjajnu izmenu, koju možete sprovesti unošenjem nove vrednosti ili promenom postojeće u Registry.

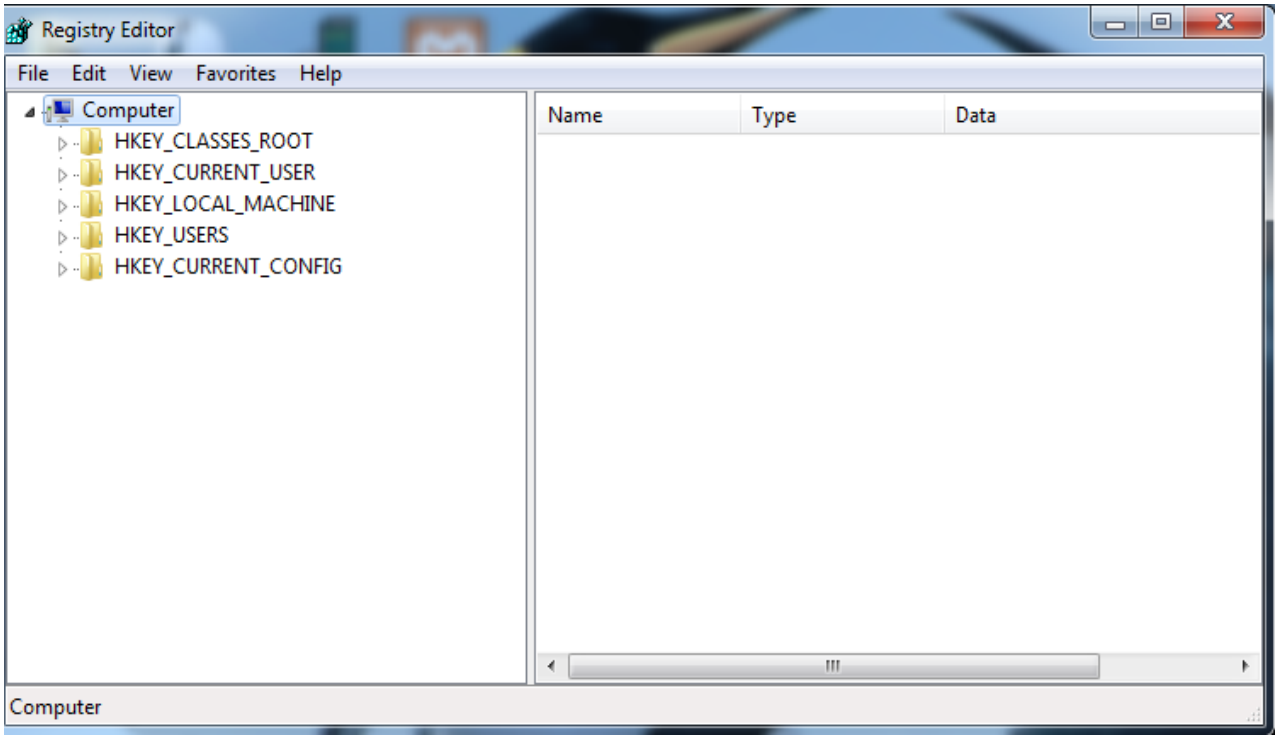
Registry Editor

U Windowsu ne postoji element menija za pokretanje Registry editora, ali možete napraviti prečicu koju će te smestiti u meni Start.

Primer za Windows 10 OS:

*Desni-click na ikonu **Start** , izabrati opciju **Run**. Ukucajte komandu **regedit** u **Open:** box, izabrati **OK**.*

Za razliku od ranijih verzija Windows OS, ima samo jedan Registry Editor



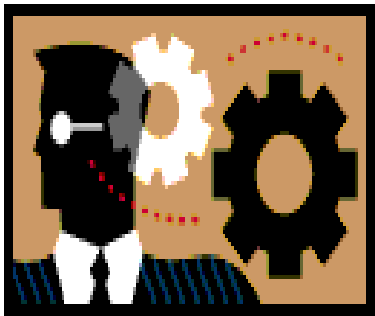
Rad u Registry

Registry podstabla:

- HKEY_CLASSES_ROOT – sadrži spisak vrsta datoteka koje OS prepoznaje i programa koji rade sa njima i dr.
- HKEY_CURRENT_USER – sadrži informacije o tekućem korisniku i njegovom podešavanju (npr. radna površina)
- HKEY_LOCAL_MACHINE – sadrži informacije o podešenju hardvera i softvera računara
- HKEY_USERS – sadrži informacije o korisnicima računara i DEFAULT informacije kada nijedan korisnik nije prijavljen
- HKEY_CURRENT_CONFIG – sadrži informacije o tekućoj konfiguraciji računara – hardver koji postoji kad se računar uključi

Otvaranje podstabla vrši se click na “+” pored imena ili 2xclick na ime podstabla.

Svako podstablo sadrži: **ključeve, podključeve i vrednosti**



Rad u Registry

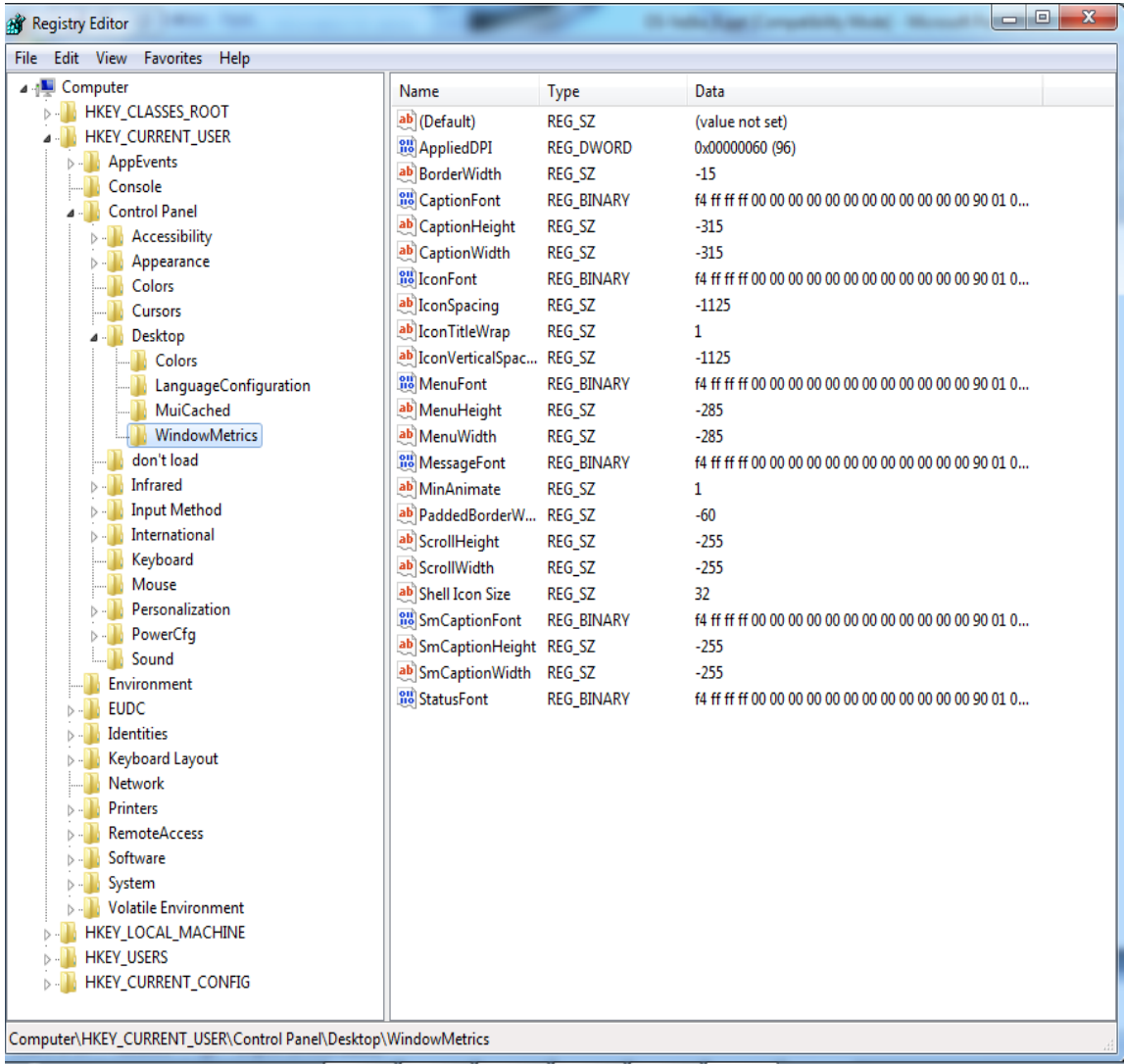
Ključ je jedan od direktorijuma podstabla. Podključ se nalazi unutar ključa, kao podirektorijum.

Svaki ključ ili podključ može sadržati pod-ključeve ili vrednosti.

Vrednost je tekuća definicija ključa i sastoji se od imena, tipa podataka i vrednosti koja je dodeljena ključu.

Najčešće korišćeni tipovi podataka u Registry:

- REG_SZ String
- REG_MULTI_SZ Multi-string
- REG_EXPAND_SZ Proširivi string
- REG_BINARY Binarni
- REG_DOWORD DOWORD



Čuvanje Registry

Veći deo Registy se čuva u nekoliko datoteka na HD – ***košnice*** (hives), to su binarne datoteke koje se mogu otvoriti u text editoru
košnice – Windows\sysWOW64\ – informacije o računaru
Košnice – Document & Settings\username – informacije o korisnicima

Osnovne datoteke "košnice":

SYSTEM – **hkey_local_machine\system** - sadrži osnovne informacije o hardveru i Windowsu

NTUSER.DAT – **hkey_kurent_user** – sadrži informacije o podešavanjima korisnika

SAM – **hkey_local_machine\sam –** sadrži bazu korisnika

SECURITY – **hkey_local_machine\security –** informacije o podešenju bezbednosti

SOFTWARE – **hkey_local_machine\software –** informacije o instaliranom softveru

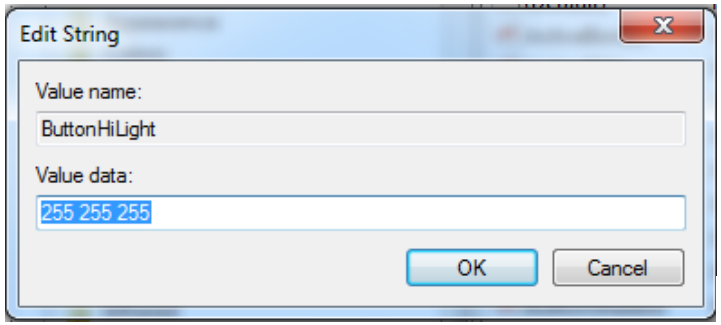
DEFAULT - **hkey_users\default –** informacije o početnom podešenju

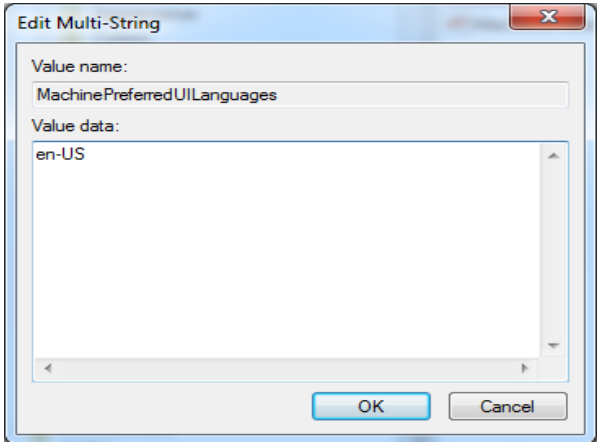
Datoteke koje beleže izmene u "košnicama": **default.log; software.log; netuser.dat.log; ...**

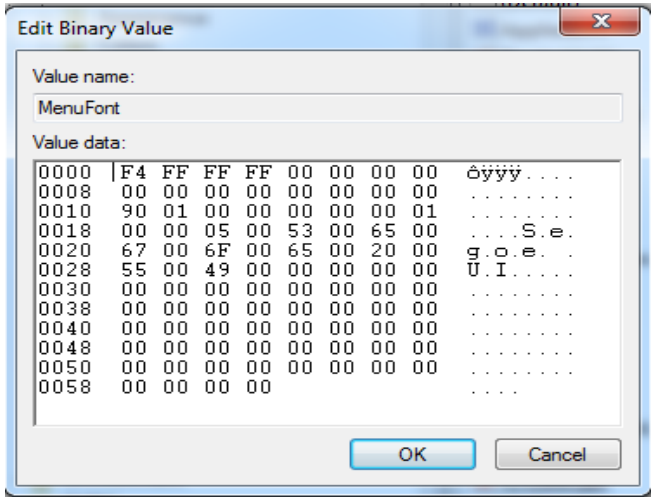
Rad u Registry

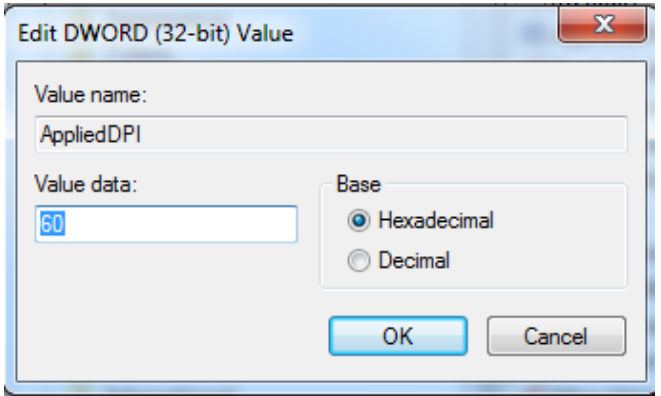
Pretraživanje - dvostruko: “ručno” i sa funkcijom **fin.** Obzirom na količinu informacija koju Windows čuva u Registry, prva stvar koja odgovara zahtevu ne mora biti ključ. Pretraživanje Registry nasličnije je pronalaženju datoteka u Exploreru.

Menjanje vrednosti – pronađite vrednost i 2xclick li označite vrednost odberite **edit→Modify**. Windows će otvoriti okvir za dijalog Edit koji odgovara tipu podataka.









Rad u Registry

Dodavanje ključa ili vrednosti – može se dodati automatski ili "ručno".

Atomatska dodela ključa koristi se kod registracije komercijalnih programa 2xclick na datoteku REG koju ste dobili i Windows će dodati neophodne ključeve i vrednosti.

Ručna dodela ključa:

1. Desnim tasterom miša click na ključ u koji želite da dodate ključ ili vrednost i odaberite New i iz podmenije birajte: key, String Value, Binary Value, DOWORD Value, Multi-String Value, ili Expandable String Value.
2. Unesite ime ključa ili vrednost
3. Enter, registry Editor će ključu, ili vrednosti dodeliti ime

Uklanjanje ključa ili vrednosti – desni click tastera miša otvara kontekst meni koji nudi opciju *Delete*, a zatim morate potvrditi *Confirme Value Delete* ili *Confirm Key Delete.* Uklanjanje ključeva je loša ideja ukoliko ih Vi niste napravili!!!

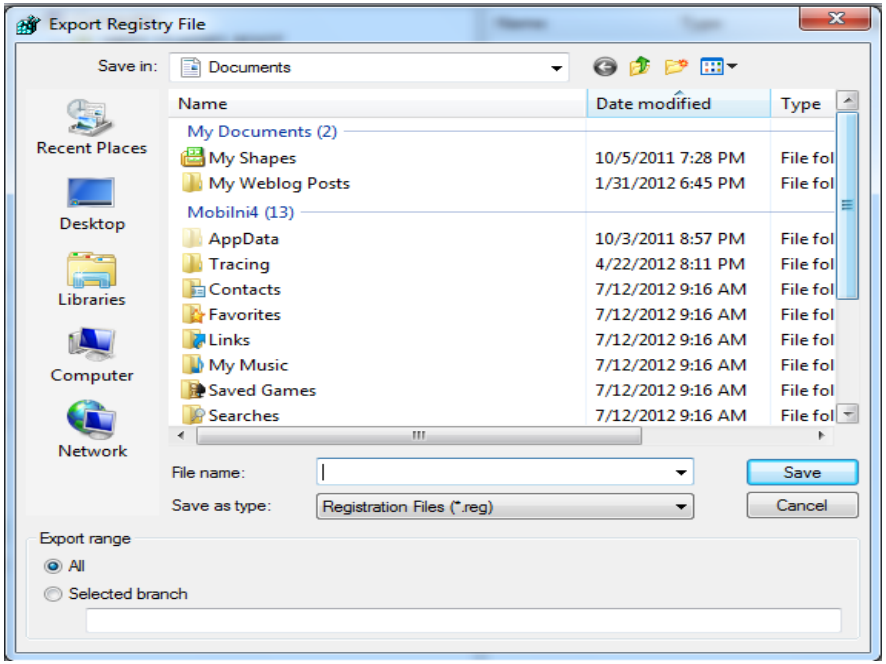
Kopiranje imena ključa – U levom panelu Registry Editora označi ključ i sa Edit→Copy Key Name, smestite ime u Cliboard

Pravljenje rezervne kopije Registry

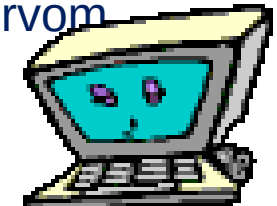
PRE NEGO BILO ŠTA URADITE SA REGISTRY-jem (čak i pregled postabala i ključeva) **NAPRAVITE REZERVNU KOPIJU!!!**

Rezervna kopija se pravi **eksportom,** a za to je neophodno da otvorite **Editor** kao Administrator:

1. Označite My Computer u Registry Editor-u
2. **File →Export**



3. U delu **Export Range** izaberite **All,** osim ako niste izabrali u prvom koraku, podstablo, tada vam se nudi **Selected Branch**
4. Zadajte ime datoteke i lokaciju



Restauriranje Registry-a

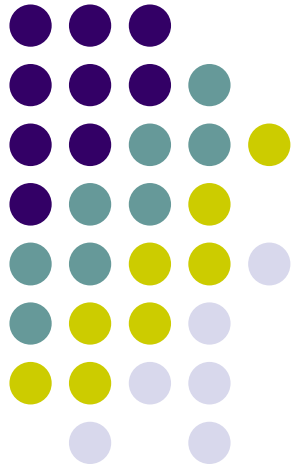
Može se restaurirati ceo Registry ili samo jedan njegov deo, pomoću datoteke koju ste predhodno eksportovali.

U Registry Editor-u odaberite:

1. **File →Import**, koji otvara dijalog **Open**
2. Iz liste **File** ili **Type**, odaberite **Registration Files** ili **Registry Hive File**
3. Odaberite Registry datoteku
4. Click **Open**, Registry Editor će importovati Registry datoteku i dodati je u registar.

Windows
Operativni sistem

Upoznavanje sa administrativnim programima i programima za zaštitu operativnog sistema

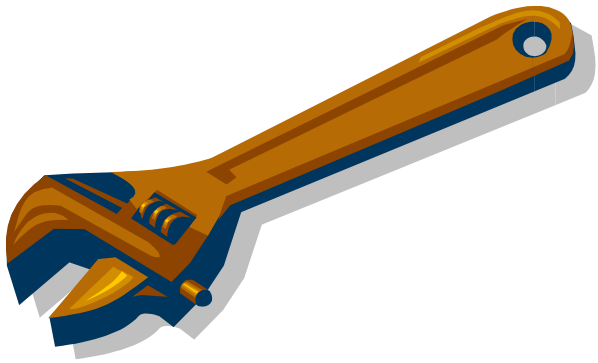


Administrativni programi

Administrativni programi ili alati, je zajedničko ime za nekoliko naprednih alatki-pomagala u Windows OS. Programi vidljivi među administrativnim alatima mogu se koristiti da se isplanira test memorije računara, upravljanje s aspekta korisnika i grupa, format hard diskova, konfiguriacije Windows usluga, promene načina na koji operativni sistem startuje, i još mnogo, mnogo više.

Aministrativnim alatima se pristupa sa Control Panela, neki od njih su:

- **Component Services**
- **Computer Management**
- **Defragment and Optimize Drives**
- **Data Sources (ODBC)**
- **Disk Cleanup**
- **Event Viewer**
- **iSCSI Initiator**
- **Local Security Policy**
- **Memory Diagnostics Tool**
- **. . .**



Microsoft Management Console (MMC)

U Windows OS objedinjena je familija adminstrativnih alata (User Manager, User Manager for Domains, server Manager, Event Viewer i Disc Administrator) u MMC. Većina je namenjena korišćenju na računaru, ali neki od njih su se mogli i koristiti na mreži.

Prednosti MMC:

- Jedan interfejs za sve alate
- Jedinstveno opredeljenje za korišćenje MMC-a
- Mogučnost samostalno pravljenja konzola
- Prilagodljivost konzola MMC-a podređenim administratorima u podeli poslova
- Help u MMC-u je kontekstna

Termini:

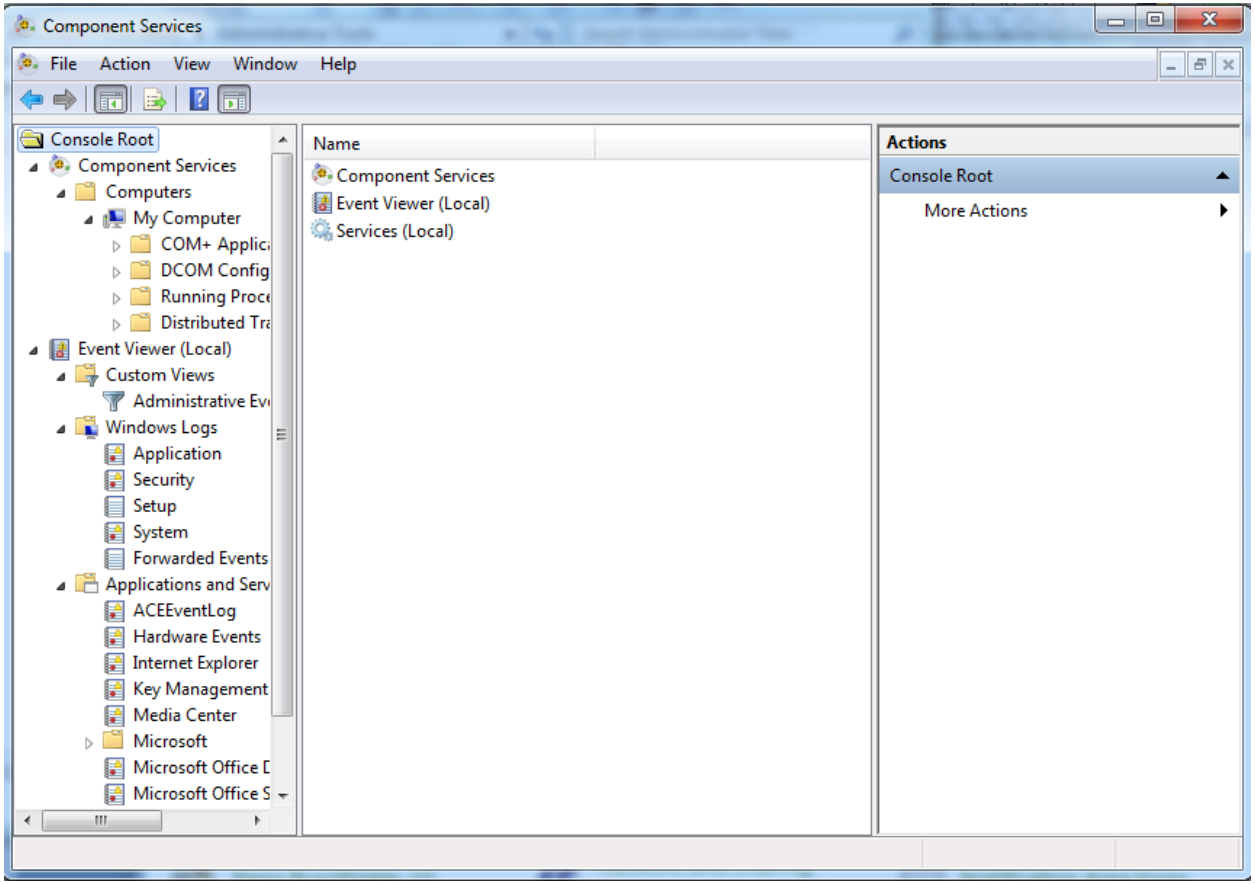
Konzola – jedan ili više alata za administriranje, deo MMC-a (konzole možete i samostalno)

Snap-inovi – alati za administraciju koji se mogu daodati konzoli.

Proširenje – je snap-in i ne radi samostalno u konzoli, zavisi od nekog samostalnog snap-ina (npr. Event Viewer i Computer Management)

Konzola Computer Management

Start→Control Panel→Performance & Maintenance→ Administrative Tools→Component Services.



Ovom opcijom administrator može aministrirati i upravljati procesima kroz grafički interfejs bez upotrebe programskih ili skript jezika.

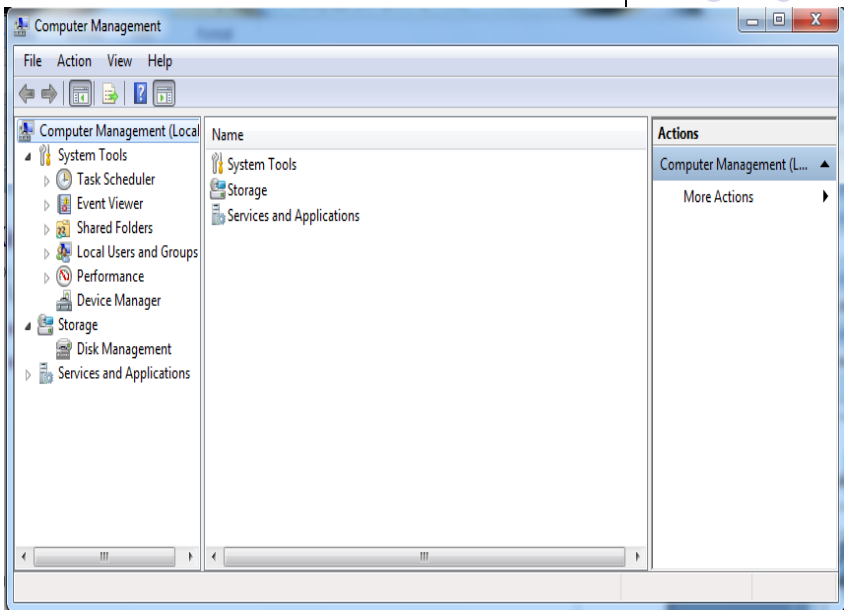
Component Service

U stablu postoje tri čvora:

- System Tools
- Storage
- Services and Applications

Starat→desni taster miša na

My Computer →Manage



Lokalni računar je u fokusu. Za konekciju sa drgim računarom odabrati connect to Another Computer.
Administrira lokalni PC, udaljeni PC i server.

Čvor System tools:

- Dnevnici događaja i upravljanje njima
- Sistemske informacije (hardver, sis. komponente i komponente servera
- Upravljanje deljenim direktorijumima, resursima, sesijama i datotekama
- Upravljanje uređajima
- Kreiranje korisnika, grupa korisnika i upravljanje s njima

Storage – opcije za upravljanje prenosnim diskovima

Services and Applications – opcije za podešavanje za telefoniju, indeksiranja IIS, konfiguracija usluga WMI.

Task Manager

Task Manager je alat koji omogućuje nadgledanje Windows OS, da otkrijete i otklonite probleme, a naročito ako se tiču programa koji se izvršavaju. Pokretanje:

Desni click na **Tsakbar**→kontekst meni **Task Manager**

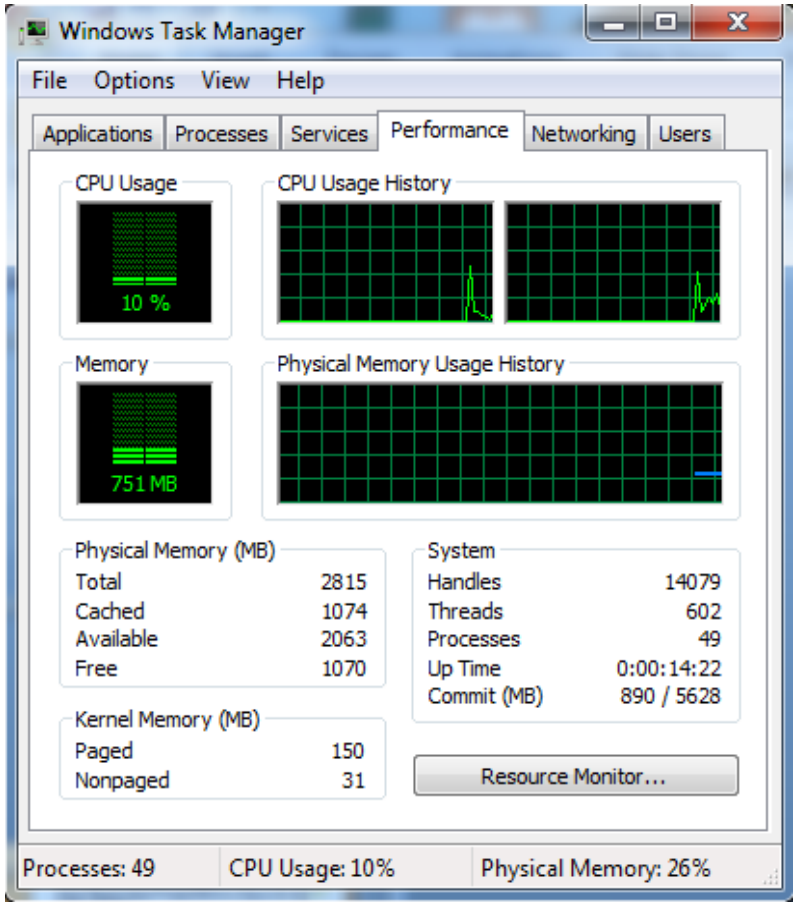
Ili

Start →**Run**→ukucajte **taskmgr**

Ili

Kombinacija tastera **Ctrl+Alt+Del**

Task manager ima više kartica, no bez obzira koja je od njih otvorena u dnu prozora je prikazan broj procesa koji rade, procenat iskorišćenosti procesora i količina memorije koja je upotrbljena, uključujući virtuelnu memoriju koja se koristi. Ovi podaci pomažu u razumevanju trenutnog stanja sistema.

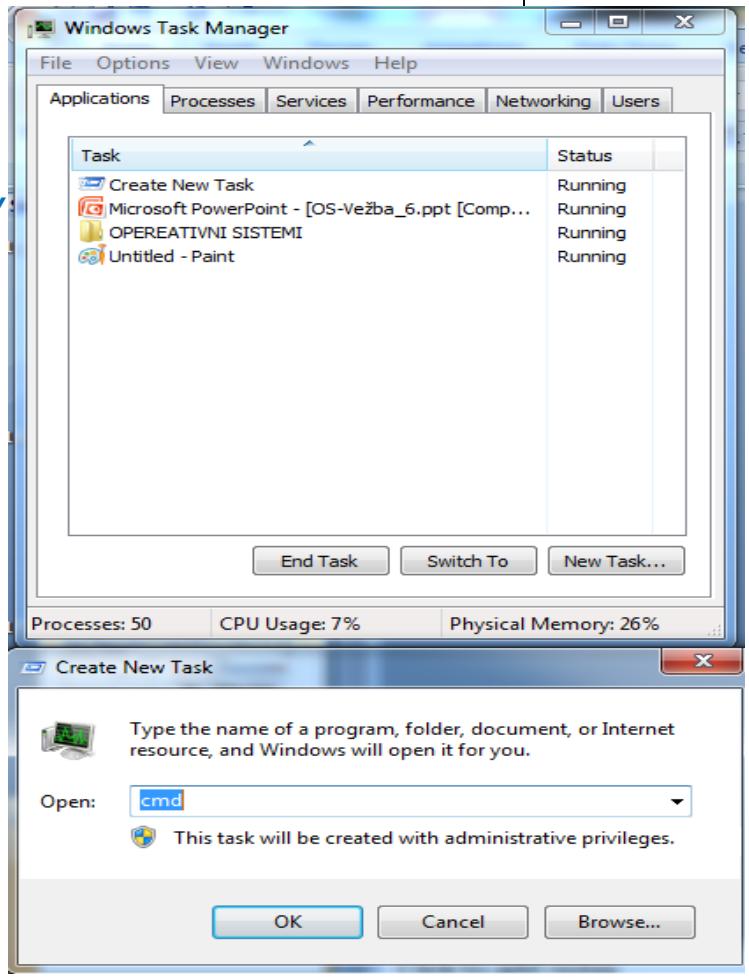


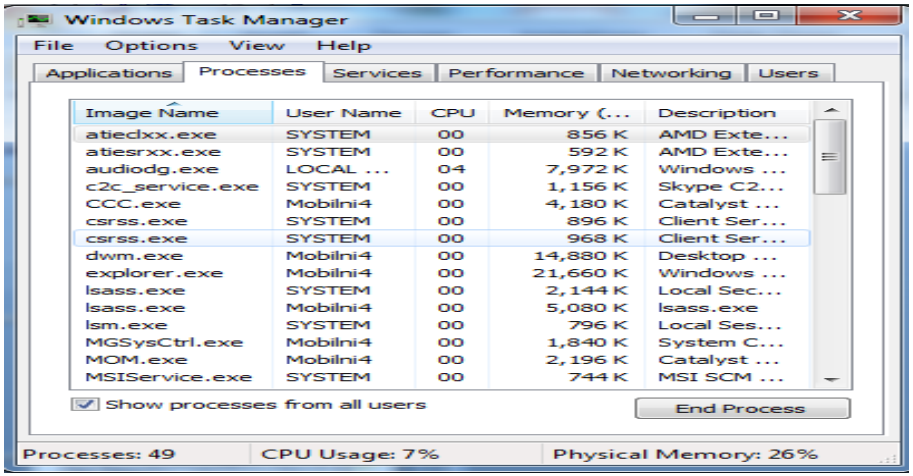
Task Manager

Kartica Aplication Task Manager – prikazuje spisak svih aplikacija koje se izvršavaju i njihov tekući status (Running ili Not Responding).

End Task – prekid izvršavanja programa
Switch To – prelazak na aplikaciju koja se izvrš
File →New Task(Run)→Open→*ukucajte naziv aplikacije* ***(npr. cmd)***

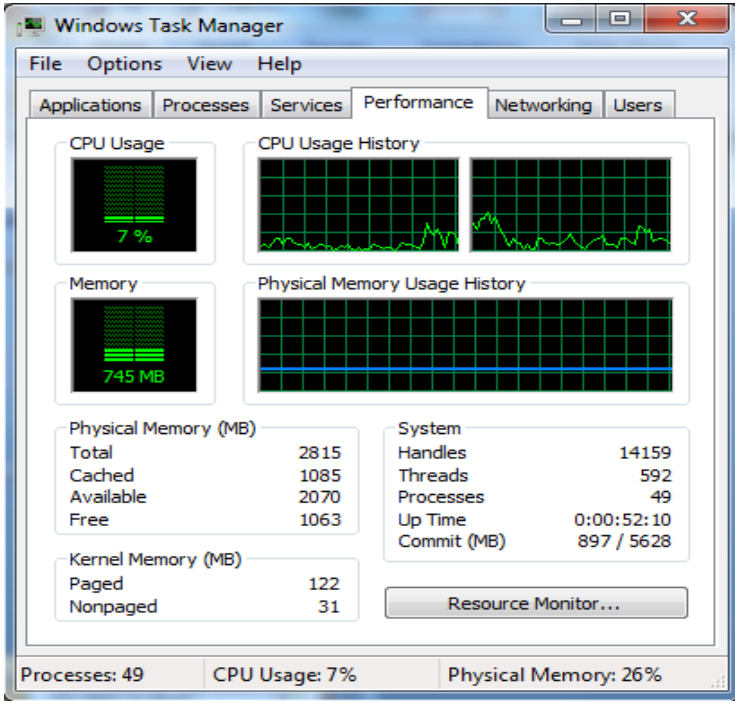
Kartica Processes Task Manager – prikazuje spisak procesa da bi ste nadgledali i zaustavili iste. Procesi su sve izvršne datoteke koje OS konkurentno izvršava.
End proces*s* – prekid izvršavanja procesa

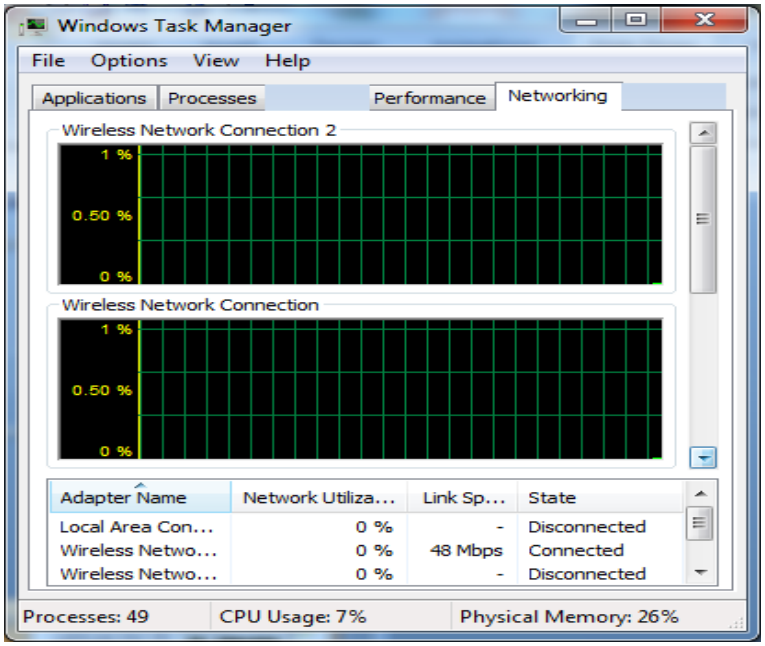




Task Manager

Kartica PerformanceTask Manager – prikazuje kako računar koristi memoriju, procesorsko vreme i druge resurse. Ovaj alat podržava praćenje rada više procesora, biloo na jednom ili više grafikona (kako se odabere). Ova kartica može prikazati informacije o korišćenju fizičke memorije i koliko memorije koristi OS kernel.





Kartica Networking Task Manager – koristi se za nadgledanje Inerneta i lokalne mreže. U dnu prozora prikazuju se informacije o brzini prenosa i broju bajtova koju je emitovala svaka mrežna kartica.

Task Manager

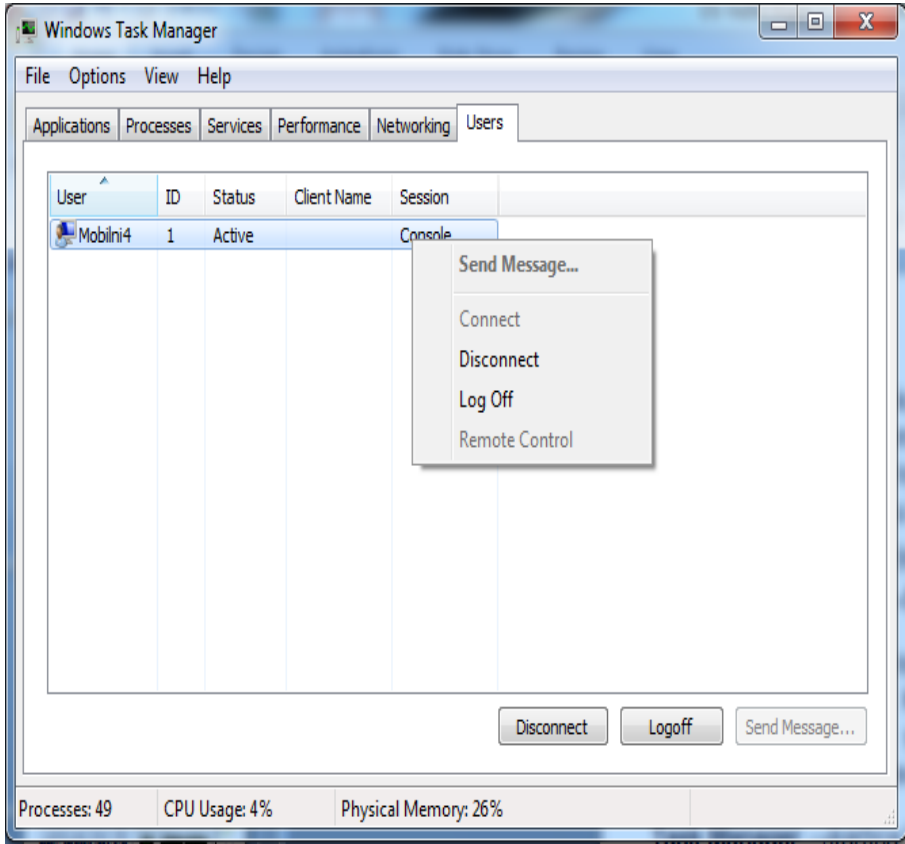
Kartica User – provera korisnika na računaru prikazuje spisak korisnika i njihove statuse. Potvrdom opcije Show Processes from All Users dobijaju se procesi koji drugi korisnici koriste. Opcijom sortiranja kolona po User Name, grupišu se procesi za pojedine korisnike.

Pregled virtualne memorije koliko koji proces koristi:

Task Manager→View →Select Columns →Virtual Memory Size →OK

Odjavljivanja drugog korisnika - bilo koji kopjuter administrator može da odjavi drugog korisnika. Kod odjavljivanja mora se voditi računa da li su drugi korisnici sačuvali svoje podatke. U tu svrhu se šalju poruke o "ubijanju" procesa ili odjavljivanju korisnika:

Task Manager→kartica **User**→desni taster miša→**k**ontekst meni **Send Message**→naslov poruke **Message Title**→poruka **Message**→**Ctrl+Enetr** započinjanje novog teksta→**Enter** ili **OK** šalje poruku



Programi za zaštitu operativnog sistema

Antivirusni softver ili antivirus je onaj koji se koristi za zaštitu, identifikaciju i uklanjanje računarskih virusa, kao i svakog drugog softvera koji može da ošteti ili nanese štetu računarskom softveru, a jednim imenom se naziva malver.

Prvobitni antivirusi su tertirali samo viruse u sistemu, moderni dizajn ovih softvera štiti od crva, fišing napada, bekdor, rutkit, trojanaca,...

Identifikacija malvera:

- Detekcija bazirana na signatirama
- Detekcija štetnih aktivnosti
- Heuristička metoda

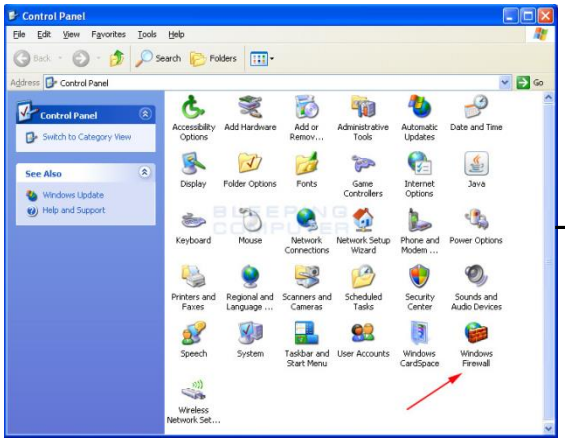
Još ne postoji ni jedan dokaz da je rašunarski virus oštetio ijedan računarski hardver. Do sada se šteta odnosila isključivo na podatke i softver, ali nije isključeno da jednog dana i sam harver bude ugrožen ovim pretnjama.

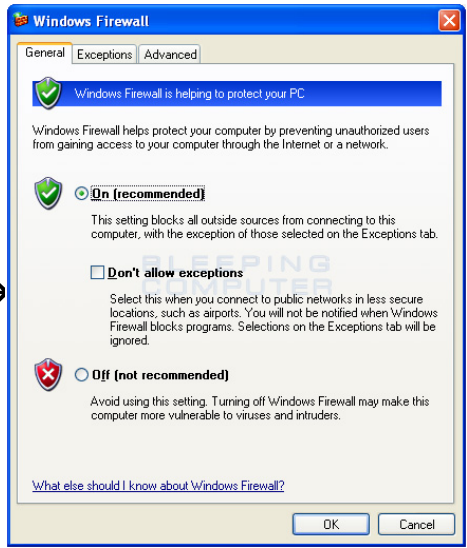
Programi za zaštitu operativnog sistema

Osim korišćenja antivirusnog softvera, zaštita od virusa se može pojačati i realizacijom **mrežnog fajervola (Firewall)** ili korišćenjem sistema **virtuelizacije**. Ove metode zaštite, u svakom slučaju, ne mogu zameniti antivirusni softver, već samo dopuniti sistem zaštite, pre svega u domenu novih i neotkrivenih malvera.

Firewall – sprečava da neidentifikovani programi i internet procesi pristupaju sistemu ili njegovom delu koji se štiti. **On nije antivirusni sistem, ne detektuje niti uklanja viruse, stoga i nije alternativa, već dopuna antivirusnoj zaštiti.** Ipak pomaže zaštiti sistema od spoljnih napada, zatvarajući računarski sistem ili računarsku mrežu, ograničavajući ili blokirajući sve sumnjive aktivnosti, koje su inicirane izvan zaštičenog dela sistema. To se čini tako što blokira sve ulazne i izlazne zahteve na kontrolisanim TCP/IP portovima.

Internet Connection Firewall je deo Windows OS**:**
Start→Connect To →Show All Conections →desni taster miša kontekst meni **Propretis** →kartica **Advanced** →čekirati polje **Connection Firewall** →**OK**





Krajjjjjj…