WINDOWS REGISTRY
Priručnik

1. UVOD

1.1 Reč-dve o redžistriju

Registry je srce sistema i u okviru njega se nalaze informacije esencijalne za rad sistema. Preko njega mozemo vrsiti kompletnu administraciju sistema i zadavati operacije koje se ne mogu izvrsiti npr preko ini fajlova. Sve informacije u okviru registry baze su indexovane po hijerarhijskom redosledu i na taj nacin sintetizovane informacije se vrlo brzo izvrsavaju iako su iste veoma komplikovane. Ako vam neko kaze da je registry baza ostala nedirnuta nakon nekog poteza, operacije ili izvrsavanja zadatka, budite ubedjeni da je to laz. Sistem pristupa registry bazi pri svakom kliku i svakoj operaciji (ali bukvalno). Registry je zaseban za svakog ulogovanog korisnika, registry baza se menja iz dana u dan...A njene prednosti se stalno povecavaju. Evo na pr, ranije (u ranijim OS-evima), backup se vrsio u ini fajlovima i tu je bio princip "ono sto vidis u windowsu to se tu i nalazi". Medjutim, s pojavom reg baze i editovanjem iste su se mogle izvrsiti brojne customizacije sistema koje u okviru windowsa ne bismo nikako mogli podesiti (tipa uklanjanje shorcut arrow-a, uklanjanje shared dokumenata iz my computera itd.). A najvaznija komponenta koju registry baza omogucava je **Policy managment** a u okviru istog i sledece funkcije:

- Deplyment customisation
- Folder redirection
- Hardware profilies
- Offline files
- Performance monitoring
- Roaming user profiles
- Windows Managment instrumentation

1.2 Istorija redžistrija

Svaka stvar na svetu ima svoju proslost i nacin nastanka. Da bismo saznali kako je registry izgledao i funkcionisao u ranijim OS-evima, vraticemo se u proslost.

- **Kvazi registry u MS-DOS OS-u.** MS-DOS je prikupljao informacije iz dva bitna sistemska fajla: *Config.sys* i *Autoexec.bat*. Svrha *Config.sys* fajla je bila ucitavanje drajvera, a svrha *Autoexec.bat* fajla je bila pokretanje programa, postavljanje sistemskih varijabli (environment variables) kako bi se MS-DOS pripremio za upotrebu. Problem je naravno sto je svaka aplikacija tog tipa mogla da kontrolise iskljucivo sopstvene parametre, a nije postojalo univerzalno resenje koje ce vrsiti globalno nadgledanje izvrsavanja operacija.
- **Reg baza u Windows 3.0** Sa pojavom ovog OS-a javili su se i *ini* fajlovi koji su donekle prosirili mogucnosti Config.sys i Autoexec.bat fajlova. Posto sam vise puta pomenuo ini fajlove red je da nabrazaka i pojasnim sta su oni ustvari. To su tekstualni fajlovi izdeljeni na sekcije i u svakoj sekciji imaju po nekoliko informacija. Problem kod takvih fajlova je sto ne postoji hijerarhija i u njih je gotovo nemoguce smestiti binarne vrednosti. Posto ini fajl predstavlja spregu izmedju aplikacije i OS-a, svaka aplikacija ima svoj ini fajl sto takodje u brojnim situacijama stvara problem.
- **Reg baza u Windows 3.1** Kod ove verzije OS-a, registry baza je bila skladiste OLE (Object Linking and Embedding) informacija, a win 3.5 i win 95 sadrze registry kakav sada imamo na win xp. Medjutim i pored toga sto se umesto ini fajlova koriste mnogo bolji i laksi nacini skladistenja informacija, i dan danas postoje ini fajlovi koji su veoma korisni.

1.3 Registry danas

Prebacujemo se iz proslosti u sadasnjost i sagledavamo kakav je registry danas:

REGEDIT se aktivira preko RUN-a: start -> run-> regedit. Regedit sa leve strane ima pet foldera, koji predstavljaju root kljuceve.:

- **HKEY_CLASSES_ROOT (HKCR)** - Iako je u redzistiju predstavljen kao root kljuc, on ustvari predstavlja podkljuc kljuca HKEY_LOCAL_MACHINE\Software i u njemu se smestaju informacije o OLE klasama i o registrovanim COM objektima. Ovaj kljuc omogucava asociranje ekstenzija sa tipovima fajlova i odgovarajucim programima. Uzmimo za primer pdf ekstenziju. Uz pomoc informacija pothranjenih u HKCR kljucu, doticnu ekstenziju otvarace na pr Adobe Reader. Naravno, to je sve relativno i koji program ce otvarati koji tip fajla, zavisi od informacija upravo u okviru HKCR kljuca i varira od korisnika do korisnika. Takodje, ovaj kljuc objedinjuje informacije koje se nalaze u okviru

podkljuceva HKEY_LOCAL_MACHINE\Software\Classes i HKEY_CURRENT_USER\Software\Classes

- **HKEY_CURRENT_USER** - predstavlja link ka HKEY_USERS i sadrzi informacije o konfiguraciji trenutno logovanog korisnika. Te informacije su: izgled destkopa, izgled i postavka fajlova i foldera, postavke u Cpanelu, itd.
- **HKEY_LOCAL_MACHINE** - sve informacije o systemu (podatke o hardveru, softveru..)
- **HKEY_USERS** - sadrzi pojedinacne podatke za svakog korisnika posebno i svaki korisnik je predstavljen u vidu zasebnog SID pod-kljuca.
- **HKEY_CURRENT_CONFIG** - predstavlja link ka HKEY_LOCAL_MACHINE i odgovara podacima za trenutna hardverska podesavanja.

Svaki folder je ustvari jedan key. U svakom folderu se nalaze ili jos podfoldera ili neke vrednosti (value) koje se prikazuju u desnom prozoru i mogu biti:

- **STRING VALUE** - textualna vrednost
- **DWORD VALUE** - binarna vrednost (0 ili 1) -> 0 - disable, 1 - enable
- **BINARY VALUE** - hexadecimalna vrednost

Da biste napravili novi key ili value, kliknite desni klik (za key na neki folder sa leve strane. a za value sa leve strane), i izaberite. Kada klknete desnim klikom na neku vrednost ili key imacete sledece opcije:

- **MODIFY** - prepravljanje i
- **DELETE** - brisanje.

2. REGISTRY IDENTIFIERS

2.1 Security Identifiers (SIDs) - bezbednosni identifikatori

Korisnicki nalozi se identifikuju putem bezbednosnih identifikatora - Security identifiers-a (SIDs). SID je jedinstvena sifra koja sluzi za identifikaciju bezbednosnih subjekata, kao sto su: racunarski i korisnicki nalozi i grupe.

Sada cemo lepo uhvatiti i rasclaniti SID i objasniti svaki njegov delic:

Evo na pr (verovatno i ne postoji ovaj SID, ali bitan je shablon)

S-1-5-23-547-0123456789-0123456789-0123456789-123

SID uvek zapocinje sa **S-** . Sledeci broj predstavlja verziju SID-a (u nasem slucaju to je verzija 1); sledeci broj pokazuje bod cijim je ovlascenjem SID (u nasem

slucaju to je 5, a to je ustvari SID pod NT nalogom). Ove ostale brojke sto vidimo, u tri dela po 10 komada su domain identifieri i na kraju ovaj zadnji broj je relativni identifier. E sad, nisu svi SID-ovi ovako dugaciki, tj ima i onih koji su na pr u formi

S-1-5-18

i kao takvi spadaju u najpoznatije SID-ove.

Najpoznatiji univerzali SID-ovi

Univerzalni well-known SID	Prepoznaje
Null SID Value: (S-1-0-0)	Grupu bez predstavnika. Upotrebljava se najcesce kada je SID nepoznat
World Value: (S-1-1-0)	Grupu koja ukljucuje sve korisnike.
Local Value: (S-1-2-0)	Korisnike koji su logovani na terminale fizicki konektovane na sistem.
Creator Owner ID Value: (S-1-3-0)	SID zamenjen SID-om korisnika koji je kreirao novi objekat.
Creator Group ID Value: (S-1-3-1)	SID zamenjen primary-group SID-om korisnika, koji je kreirao novi objekat

RID vrednosti koriscene od strane najpoznatijih SID-ova

Nalog identifikatora	Value	Nalog identifikatora
SECURITY_NULL_RID	0	S-1-0
SECURITY_WORLD_RID	0	S-1-1
SECURITY_LOCAL_RID	0	S-1-2
SECURITY_CREATOR_OWNER_RID	0	S-1-3
SECURITY_CREATOR_GROUP_RID	1	S-1-3

2.2 Globaly Unique Identifiers (GUIDs)

Pored security identifiers-a, postoje i Globaly Unique identifiers (GUIDs). Oni obelezavaju objekte u vidu specijalnih brojeva. Ti objekti uglavnom vec imaju svoja imena ali iako se desi da se nazivi tih objekata podudaraju, njihovi GUIDs-i ce ostati jedinstveni i po njima ih mozemo ralzikovati. GUIDs-i imaju svoju strukturu i svi su strukturisani po istom sablonu: 16-o biti hexadecimalni brojevi, rasporedjeni u grupama i to sledecim redosledom od po: 8,4,4,4 i 12 znakova (od slova se koriste sva od A do F, a od cifara sva od 0 do 9). Evo na pr GUID-a od my computer-a:

{20D04FE0-3AEA-1069-A2D8-08002B30309D}

3. REGISTRY DATABASE

3.1 (Heksa)decimalni zapisi i bit maske

Najveci broj podataka redzistrija je u vidu hexadecimalnih zapisa, a pored hexadecimalnih postoje i binarni i decimalni zapisi. Ajde da se podsetimo sta su sve te stvari.

- **Decimalni zapis** broja `856` bice: `8*10^2 + 6*10^1 + 6*10^0` i oznaka "^" je u nasam narodu nazvana *na* . Tj. 10^3 je *10 na treci* i istice koliko decimala (ili seljacki receno: koliko nula) sadrzi taj broj, i cifre su 0 - 9. Broj 10 stalno ostaje isti i on se zove baza 6 (base 6), a brojevi, na koliko se ta desetka *stepenuje*, se menjaju.
- **Binarni zapis** broja `1011` bice: `1x2^3 + 0*2^2 + 1*2^1 + 1*2^0` ili jednostavno `11`. Cifre su 0 i 1. Broj 2 stalno ostaje isti i on se zove baza 2 (base 2), a brojevi, na koliko se ta dvojka *stepenuje*, se menjaju.
- **Hexadecimalni zapis** decimalnog broja `01101111` iznosi `6f` (jer je 0110 hexadecimal 6, a 1111 hexadecimal f). A postoji i obrnut nacin, znaci da iz hexadecimalnog broja dobijemo decimalni broj. Evo na pr `B02F` bice: `11*16^3 + 0*16^2 + 2*16^1 + 15*16^0`

Sad se pitate, pa pobogu po kom je ovo sablonu ? Evo, postoji tabela, malo je proucite i sve ce vam biti jasno ko dan:

Binarno	Hexadecimalno	Decimalno
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	A	10
1011	B	11
1100	C	12
1101	D	13
1110	E	14
1111	F	15

Sledeci pojam koji je bitan za nas su **bit maske** (bit masks). Ponekad se u redzistriju vise podesavanja pakuje u jedan broj i svaki bit u tom broju predstavlja razlicito

podesavanje. Znaci u bajtu se moze smestiti 8 podesavanja, 16 podesavanja u okviru jedne reci, itd. Bit mask je prestavljen u formi na pr `0x21`.

3.2 Regedit

Regedit je tool koji omogucava administraciju reg baze i ekvivalentan je win exploreru. Sa leve strane regedit-a se nalaze folderi, a sa desne se nalazi sadrzaj selektovanog foldera. Znaci kljucevi su ekvivalent folderima u win exploreru i mogu sadrzati vise podkljuceva, a naziv samog kljuca je limitiran na 512 ANSI ili 256 UNICODE karaktera a mogu sadrzati i sve ASCII znakove sem ***/ **** i **?** . Reg baza je usko povezana sa win folderima/fajlovima i evo i primera. Koncentrisemo se na putanju `C:\WINDOWS\system32\cmd.exe` . Ova putanja se odnosi na cmd fajl koji se nalazi u system32 podfolderu foldera windows. Paralelno sa ovim na pr gledamo `KEY_LOCAL_MACHINE\SOFTWARE\blabla soft\` i odatle zakljucujem da vrednost *blabla soft* pripada podkljucu *SOFTWARE* gavnog kljuca *HLM*. Znaci tu smo zaokruzili ovau malu pricicu o kljucevima (keys)

4. REGISTRY VALUES

Sledece sto zapazimo u redzistriju su vrednosti (values). Svaki kljuc ima svoje values-e. Setite se kad sam pricao da je regedit ekvivalentan win exploreru...e pa i valuesi su ekvivalentni fajlovima i to po sledecoj analogiji:

- **NAME** valuesa odgovara nazivu fajla.
- **TYPE** valuesa odgovara extenziji fajla sto ustvari odredjuje tip tog fajla
- **DATA** valuesa ogovara trenutnom sadrzaju fajla.

Odavde zakljucujemo da postoji tri dela valuesa, a to su: Name, Type i Data (to sve vidimo kada kliknemo na neki kljuc i to se prikaze na desnoj strani regdzistrija)

4.1 Value's Name

NAME: svaki value ima svoj naziv i kod njega vlada pravilo kao i kod imena kjuceva: naziv valuesa je limitiran na 512 ANSI ili 256 UNICODE karaktera a mogu sadrzati i sve ASCII znakove sem ***/ **** i **?**

4.2 Value's Type

TYPE: Kao sto rekoh, svaki tip values opisuje tip podataka koje sadrzi

GLAVNI TIPOVI VALUESA		
Tip value-a	**Opis**	**Primer**
String (REG_SZ)	Tekst stalne duzine. Pored dword-a, ovo je najprisutniji tip valuesa. Javlja se u dva oblika :	
	kao naziv nekog podatka	7-Zip
	kao putanja values ovog tipa se zavrsava sa nultim karakterom i ne sme sadrzati enirоment variables.	C:\Program Files\7-Zip\7z
Binary (REG_BINARY)	Binarni podaci (Binary data). Redzistri ispisuje binarne podatke u hexadecimalnom zapisu, a i mi sami kada unosimo te binarne podatke u hexadecimalnom obliku.	0x02 0xFE 0xA9 0x38 0x92 0x38 0xAB
Dword (REG_DWORD)	Double-word values (32 bita). Valuesi ovog tipa se prikazuju u obliku nule ili jedinice i one se zovu Bulenove oznake (Boolean flags).	0 - false/disable/no 1 - true/enable/yes
	U dwordu se moze smestiti i vreme u milisekundama.	1000 je 1 sekund
	Dword se moze pregledati i editovati u decimalnom ili heksadecimanom zapisu	0xFE020001 0x10010001
(REG_MULTI_SZ)	Sadrze liste znakova (strings)i svaki upis je podeljen "null" karakterom (0x00), a dva null karaktera zavrsavaju listu.	
Expandable string (REG_EXPAND_SZ)	Tekst varirajuce duzine. Values ovog tipa sadrzi environment variables i pre nego sto iskoristi te enironment variables, program mora da ih produzi u odgovarajuci oblik tj. putanju.	%userprofile%\Favorite

OSTALI TIPOVI VALUESA		
Tip value-a	**Opis**	**Primer**
REG_DWORD_BIG_ENDIAN	/	0X010203 smesten kao 0x01 0x02 0x03
REG_DWORD_LITTLE_ENDIAN	/	0X010203 smesten kao 0x03 0x02 0x01
REG_FULL_RESOURCE_DESCRIPTOR	/	Za primer pogledati u HKLM\HARDWARE\DESCRIPTION\Description
REG_LINK	Predstavljaju link. Korisnik ga ne moze kreirati.	/
REG_QWORD	Isti kao i dword samo sto za razliku od njega ne sadrzi 32 bita vec 64.	0xFE02000110010001
REG_QWORD_BIG_ENDIAN	/	Za primer pogledati u REG_QWORD_BIG_ENDIAN
REG_QWORD_LITTLE_ENDIAN	/	Za primer pogledati u REG_QWORD_LITTLE_ENDIAN
REG_RESOURCE_LIST	Lista REG_FULL_RESOURCE_DESCRIPTOR valuesa. Korisnik moze videti ovaj tip valuesa, ali ga ne moze menjati.	/
REG_NONE	Values nedefinisanog tipa	/

5. REGISTRY KEYS

Kao sto sam ranije napomenuo u redzistriju se nalazi **5 root kljuceva**:

- HKEY_CLASSES_ROOT (HKCR)
- HKEY_CURRENT_USER (HKCU)
- HKEY_LOCAL_MACHINE (HKLM)
- HKEY_USERS (HKU)
- HKEY_CURRENT_CONFIG (HKCC)

Od gore nabrojanih, HKLM i HKU su najvazniji i to su jedini root kljucevi koje win smesta na disk, dok ostali root kljucevi predstavljaju linkove do potkljuceva u HKLM.

- **HKCR** je link podkljuca Classes koji se nalazi u HKLM\SOFTWARE\Classes
- **HKCU** je link podkljuca na pr: HKEY_USERS\S-1-5-19
- **HKCC** je link podkljuca Current koji se nalazi u HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current

Negde na pocetku tutora sam na blic objasnio o root kljucevima, a sada cu malo potpunije objasniti svaki ponaosob.

5.1 HKEY_CLASSES_ROOT

HKEY_CLASSES_ROOT - Ovaj root key sadrzi dve komponente. Prvu predstavlja sinteza fajlova koju cine tipovi fajlova zajedno sa programima koji iste te fajlove mogu otvoriti/editovati/stampati. A druga komponenta su registracije COM fajlova. I jos da napomenem da je ovaj root kljuc otvara najvise mogucnosti za kustomizaciju i najveci je root kljuc u registry bazi. HKCR je nastao spajanjem HKLM\SOFTWARE\Classes i HKCU\SOFTWARE\Classes , a ukoliko se isti values javi u i u jednom i u drugom path-u, path HKCU\SOFTWARE\Classes ima vecu prednost.

Sinteza ova dva patha ima brojne prednosti:

- Programi mogu registrovati per-computer i per-user asocijacije fajlova i programskih klasa, sto znaci da jedan korisnik moze posedovati asocijaciju fajlova koju, drugi korisnici koji sheruju komp nemaju.
- Korisnik koji sheruje jedan komp moze koristiti dva razlicita programa za editovanje istog tipa fajla, bez medjusobnog uticaja.
- Posto su per-user asocijacije i class registracije u user profilima, oni prate korisnike od kompa do kompa kada koriste roaming user profile.

- Pristup HKLM\SOFTWARE\Classes se moze limitirati bez cackanja po HKCU\SOFTWARE\Classes .

5.2 KEY_CURRENT_USER

HKEY_CURRENT_USER - Sadrzi podesavanja samog korisnika (per-user) i predstavlja link ka HKU\SID , a SID smo vec naucili sta je (pricao sam u gornjem delu tuta).

U okviru ovog root kljuca se nalaze sledeci podkljucevi:

- **AppEvents** - Omogucava da se cuje odredjen zvuk pri odredjenoj radnji (zvuk pri otvaranju foldera, zvuk pri logovanju...)
- **Console** - Smesta podatke za konzolni podsistem (command prompt...)
- **Control panel** - Sadrzi brojna podesavanja za jezik, izgled GUI-a...
- **Environment** - Sadrzi envionment varijable postavljene od strane korisnika.
- **Identifies** - Sadrzi podkljuceve za identitete u M$ Outlook-u. Ti identiteti u OE omogucavaju da vise usera deli jedan mail klijent
- **Keyboard Layout** - Podaci o tastaturi
- **Network** - Informacije o "mapiranim" mreznim drajvovima
- **Printers** - Korisnicki podaci za stampace
- **Software** - Sadrzi podatke i podesavanja korisnickih aplikacija. U ovom podkljucu se takodje nalaze i winove konfiguracije.
- **Volatile Environment** - Sadrzi envionment varijable koje su postavljene pri logovanju korisnika.

5.3 HKEY_LOCAL_MACHINE

HKEY_LOCAL_MACHINE - Sadrzi podesavanja samog sistema (per-computer), sto znaci da ce ista uticati na bilo kog korisnika koji se loguje na racunar. Tu spada podesavanja drajvera, menadzment win podataka...

U okviru ovog root kljuca se nalaze sledeci podkljucevi:

- **Hardware** - Opis hardwera koje je win detektovao. Ovaj podkljuc se kreira pri svakom dizanju sistema i sadrzi podatke o uredjajima i njihovim drajverima.
- **SAM** - Sadrzi sigurnosu bazu win podataka, Security Accounts Manager (SAM). Seljacki receno: tu su smestene sve sifre u windowsu i iste su nedostupne i samom administratoru. To je u normalnim okolnostima, medjutim...Postoje

programi kojima se moze crackovati SAM i time doci do potrebnih sifri. SAM je lik ka kljucu HKLM\SECURITY\SAM

- **Security** - Sadrzi sve podatke iz podkljuca SAM, kao i ostale security podatke.
- **Software** - Da se ne ponavljam, procitajte obavestenje za ovaj podljuc koje sam dao kod HKCU root kljuca
- **System** - sadrzi podesavanja kontrola. Podkljuc se nalazi u sledecem pathu: `HKLM\SYSTEM\CurrentControlSet`

5.4 HKEY_USERS

HKEY_USERS - sadrzi pojedinacne podatke za svakog korisnika posebno i svaki korisnik je predstavljen u vidu SID pod-kljuca.

U okviru ovog root kljuca se nalaze sledeci podkljucevi:

- **Default** - Sadrze podatke koje win koristi da bi prikazao desktop pre nego sto se bilo koji korisnik loguje na komp.
- **SID** - Kod ovog podkljuca SID predstavlja security identifier za console user i sadrzi per-user podesavanja i to podesavanja desktopa, podesavanja u control panelu...
- **SID_Classes** - Kod ovog podkljuca SID predstavlja security identifier za console user i sadrzi per-user klase registracija i asocijacije fajlova. Win spaja sadrzaje HKLM\software\Classes i HKU\SID_Classes kljuceva u HKCR.

Pored ovih podkljuceva, postoje jos tri u okviru HKU, a to su:

- S-1-5-18
- S-1-5-19
- S-1-5-20

5.5 HKEY_CURRENT_CONFIG

HKEY_CURRENT_CONFIG - Predstavlja link ka podacima o konfiguraciji za aktuelni hardver profil, `HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Curent` a obrnuto gledano, *Current* je link ka kljucu `HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\xxxx`, gde je *xxxx* specijalni broj pocevsi od 0000.