A Ilica 242, HR-10000 Zagreb
T (01) 2222 182
E student@algebra.hr
www.algebra.hr

ALGEBRA

KATEDRA ZA SISTEMSKO INŽENJERSTVI I KIBERNETIČKU SIGURNOST

OPERACIJSKI SUSTAVI

Lab: MS Registry i upravljački programi

REV 3.0

A Ilica 242, HR-10000 Zagreb
T (01) 2222 182
E student@algebra.hr
www.algebra.hr

ALGEBRA

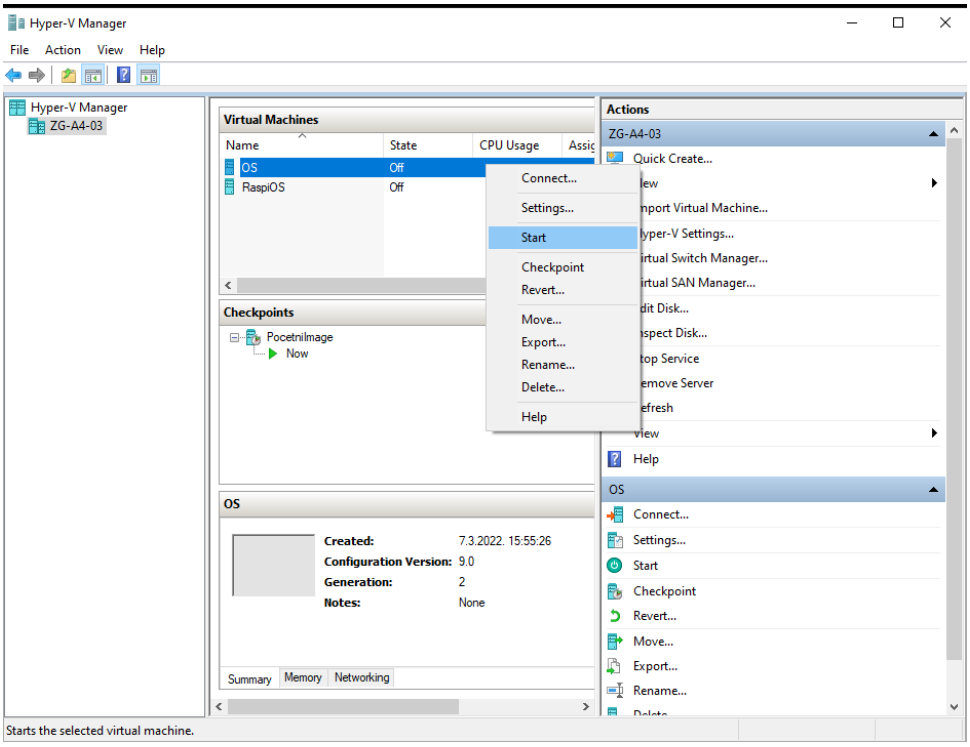
Sadržaj

A Ilica 242, HR-10000 Zagreb
T (01) 2222 182
E student@algebra.hr
www.algebra.hr

1 Pokretanje virtualnog računala

Za pokretanje virtualnog računala potrebno je:

1. Ulogirati se na studentsko računalo sa podacima:
    a. Korisničko ime: **hyperv**
    b. Korisnička zaporka/password: **hyperv**
2. Pokrenuti virtualno računalo putem Hyper-V managera i pokrenuti virtualno „**OS**“ računalo
3. Ulogirati se na virtualno računalo sa podacima:
    a. Korisničko ime/username: **korisnik**
    b. Korisnička zaporka/password: **Pa$$w0rd**



U ovoj vježbi koristiti ćemo alate iz prethodne vježbe, pa provjerite da li isti postoje na računalu:

- Process explored
- Livekd

A Ilica 242, HR-10000 Zagreb
T (01) 2222 182
E student@algebra.hr
www.algebra.hr

ALGEBRA

2 Registry

Windows Registry ima važnu ulogu u konfiguraciji i kontroli sustava. Registry je repozitorij cjelokupnih računalnih i korisničkih postavki. Pomoću Registry-ja možemo promijeniti praktički sve postavke Windowsa. Zapravo, brojni poznati alati za konfiguraciju Windowsa (npr. moduli Control Panela, gpedit.msc, secpol.msc konzole i sl.) su samo sučelja prema lokacijama u Registry-ju koja koristimo radi jednostavnosti.

Registry možete modificirati putem **regedit** alata (pokreće se iz Command Prompta ili Run dijaloga). Slijede tablice koje prikazuju značenja ključeva i vrijednosti Registry-ja.

Registry type name/value	Description
REG_NONE	No value type is defined.
REG_SZ	A string.
REG_EXPAND_SZ	A string that can contain unexpanded references to environment variables, for example, "%PATH%".
REG_BINARY	Binary data in any form.
REG_DWORD	A 32-bit number.
REG_DWORD_LITTLE_ENDIAN	A 32-bit number in little-endian format; equivalent to REG_DWORD.
REG_DWORD_BIG_ENDIAN	A 32-bit number in big-endian format.
REG_LINK	Symbolic link to a registry key.
REG_MULTI_SZ	A REG_MULTI_SZ structure as specified in [MS-RRP] section 2.2.5.
REG_RESOURCE_LIST	A device driver resource list.
REG_QWORD	A 64-bit number.
REG_QWORD_LITTLE_ENDIAN	A 64-bit number in little-endian f

Table 1:Tipovi podataka Registry-ja (source: https://docs.microsoft.com/)

Folder/predefined key	Description
HKEY_CURRENT_USER	Contains the root of the configuration information for the user who is currently logged on (current user).
HKEY_USERS	Contains all the actively loaded user profiles on the computer.
HKEY_LOCAL_MACHINE	Contains configuration information (settings) particular to the computer (for any user).
HKEY_CLASSES_ROOT	Is a subkey of HKEY_LOCAL_MACHINE\Software. The information that is stored here makes sure that the correct program opens when you open a file by using Windows Explorer.
HKEY_CURRENT_CONFIG	Contains information about the current hardware profile that is used by the local computer at system startup.

Table 2: Šest vršnih ključeva Registry-ja (source: https://docs.microsoft.com/)

2.1 Postavke unutar Registry-ja

U određenim slučajevima morat ćete pronaći lokaciju u Registry-ju na koju je neka aplikacija pohranila svoje konfiguracijske podatke. Za demonstraciju postupka koristit ćemo Notepad. Notepad je jednostavna aplikacija, ali, kao i ostale aplikacije pod Windows sustavima postavke (npr. font, veličina fonta, veličina ili položaj prozora) sprema u Registry. Alat koji ćemo koristiti je Process Monitor iz Sysinternals grupe alata. Pomoću njega se može pratiti kako Notepad čita ili zapisuje postavke.

Demonstrirajmo:

1. Pokrenite virtualno računalo **OS**.
2. Otvorite Notepad i promijenite mu postavke. Npr. promijenite font u Times New Roman i potom isključite Notepad.
3. Pokrenite Process Monitor. Ukoliko se odmah ne prikaže dijalog za konfiguraciju filtra kliknite na izbornik **Filter->Filter**. Zatim iz filtarskog dijaloga postavite sljedeće parametre:
    a. Prvi padajući izbornik: **Proces Name**
    b. Drugi padajući izbornik: **Is**
    c. Okvir za unos teksta: **notepad.exe**
    d. Treći padajući izbornik: **Include**
    e. Kliknite na gumb **Add** i zatim na **OK**.
4. Pokrenite Notepad. Nakon što se pokrene, iz Proces Monitora odaberite naredbu **File-> Capture Events**.

5. Ovime ste isključili nadgledanje Notepada. Notepad sad možete isključiti i koncentrirati se na log prikazan u Process Monitoru.
6. Označite prvi unos u log i kliknite na izbornik **Edit->Find**. Upišite tekst za pretragu **times new** i kliknite na gumb **Find Next**.
7. Pretraga će označiti jedan redak u logu. U tom retku je zabilježena aktivnost procesa notepad.exe koja je iz Registry-ja pročitala parametar koji odgovara rezultatu pretrage.
8. Uočite lokaciju u Registry-ju iz koje je pročitan predefinirani font. Susjedne lokacije upućuju na ostale konfiguracijske postavke Notepada.
9. Desnom tipkom miša kliknite na označeni redak i odaberite opciju **Jump To**. Otvorit će se program *Regedit* na poziciji koju smo pronašli Process Monitorom.
10. Ručno promijenite vrijednost u ključu **lfFaceName** u **Arial**. Zatvorite Regedit i pokrenite Notepad. Provjerite koji je postavljeni font.
11. Na isti način probajte uključiti opciju **Word Wrap.**

A Ilica 242, HR-10000 Zagreb
T (01) 2222 182
E student@algebra.hr
www.algebra.hr

ALGEBRA

3 Upravljački program (Drivers)

Upravljački programi su moduli koji se učitavaju i izvršavaju u kernel modu. Realizirani su putem datoteka (najčešće sa .**sys** ekstenzijom) i predstavljaju sučelje između **U/I upravitelja** i hardverskih komponenti. Njihovo izvršavanje dijelimo prema tri konteksta:

- korisničke dretve koja je inicijalizirala U/I funkciju
- sistemska dretva kernel moda
- posljedica prekida (stoga je izvan konteksta bilo kojeg procesa ili dretve)

Otprije znamo da upravljački programi ne pristupaju direktno hardveru nego pozivaju odgovarajuće funkcije iz HAL-a. Sami programi su pisani u programskom jeziku C (ponekad i u C++).

Ponovimo i njihove kategorije:

- **hardverski upravljački programi**: upravljaju hardverom (putem HAL-a) kako bi izvršavali operacije čitanja ili pisanja s ili na fizički uređaj ili mrežu. Postoje brojne kategorije ovakvih upravljačkih programa, kao što su upravljački programi za sabirnice, uređaje za interakciju, uređaje za pohranu podataka itd.
- **upravljački programi datotečnog sustava**: zaprimaju U/I zahtjeve u obliku datoteka te ih prevode u U/I zahtjeve specifične pojedinim uređajima (npr. IDE diskovima)
- **filtarski upravljački programi** datotečnog sustava: omogućuju podršku za diskove konfigurirane u mirror polje, ili za enkriptirane diskove.
- **mrežni usmjerivači**: upravljački programi datotečnih sustava koji omogućuju U/I operacije lokalnog i udaljenog datotečnog sustava
- **upravljački programi protokola**: implementiraju mrežne protokole, kao što su TCP/IP, NetBEUI i IPX/SPX.
- **kernel filtarski upravljački programi**: omogućuju upravljanje signalima unutar streamova, što je nužno potrebno za prikaz ili snimanje audia i videa.

Instalacija upravljačkog programa je jedini način za dodavanje vlastitog koda u kernel mod rada. Brojni alati iz Sysinternals grupe alata rade upravo to: implementiraju upravljački program povezan s GUI aplikacijom kako bi pristupili internim komponentama operacijskog sustava koje nisu dobavljive iz korisničkog moda.

A Ilica 242, HR-10000 Zagreb
T (01) 2222 182
E student@algebra.hr
www.algebra.hr

ALGEBRA

3.1 Pregled instaliranih upravljačkih programa

Instalirane upravljačke programe možete vidjeti putem **Msinfo32** aplikacije:

1. Otvorite **Command Prompt** (cmd)
2. Upišite naredbu **msinfo32**
3. Iz lijevog okna prozora proširite čvor **Software Environment** i otvorite **System Drivers**.
4. Prozor prikazuje popis upravljačkih programa kako su definiranu u Registry-ju, njihovu vrstu i status (pokrenut ili zaustavljen).

Upravljački programi i servisi su definirani u Registry-ju na lokaciji **HKLM\System\Current Control Set\Services**. Separiraju se prema ključu Type, kao što prikazuje donja tablica.

Type vrijednost	Opis
SERVICE_KERNEL_DRIVER (1)	Upravljacki program.
SERVICE_FILE_SYSTEM_DRIVER (2)	Upravljacki program datotecnog sustava.
SERVICE_ADAPTER (4)	Zastarjelo, ne koristi se.
SERVICE_RECOGNIZER_DRIVER (8)	Prepoznaje datotecni sustav i ucitava odgovarajuci upravljacki program.
SERVICE_WIN32_OWN_PROCESS (16)	Servis se izvršava unutar procesa koji opslužuje samo taj servis
SERVICE_WIN32_SHARE_PROCESS (32)	Servis se izvršava unutar procesa koji opslužuje više servisa
SERVICE_INTERACTIVE_PROCESS (256)	Servis smije prikazivati prozore i obradivati zahtjeve korisnika ali samo unutar jedne sesije, kako ne bi došlo do konflikata u slucaju više korisnika prijavljenih na sustav (interaktivno ili lokalno).

Table 3: Informacija o svakom sistemu u Registry-ju

Pregledajte definirane upravljačke programe i servise:

1. Unutar Command Prompta upišite naredbu **regedit**
2. Otvorite lokaciju **HKLM\System\Current Control Set\Services**
3. Usporedite informacije iz msinfo32 aplikacije i iz regedita za **cdfs** i **cdrom** upravljačke programe. Sravnite ih s gornjom tablicom provjerite da li se slažu.
4. Zatvorite regedit i msinfo32.

Učitane upravljačke programe je moguće vidjeti i pomoću Sysinternals alata:

- unutar Process Explorera tako da označite proces **System** i pregledajte njegove DLL module
- pokrenite **livekd.exe** alat (alat za debugiranje kernela koji smo koristili u prošloj vježbi) i upišite naredbu **lm kv**

A Ilica 242, HR-10000 Zagreb
T (01) 2222 182
E student@algebra.hr
www.algebra.hr

ALGEBRA

3.2 Mapiranje sistemskih dretvi na upravljačke programe

Proces **System** (PID 4) sadrži specijalne dretve koje se izvršavaju isključivo unutar kernel moda. One se, grupno, zovu **sistemske dretve**. Iako imaju sve atribute korisničkih dretvi (npr. kontekst, prioritet itd.) izvršavaju kod unutar kernel moda. Dotični kod može bit sadržan unutar ntoskrnl.exe datoteke ili nekog upravljačkog programa. Windowsi i razni upravljački programi kreiraju sistemske dretve prilikom inicijalizacije sustava kako bi ih koristile za U/I naredbe, straničenja memorije i sl.

----------NAPOMENA----------
Predefinirano, sistemske dretve su vlasništvo System procesa ali ih upravljački programi mogu kreirati unutar bilo kojeg procesa.

Pokušajmo pomoću Process Explorer alata pronaći upravljački program koji uzrokuje opterećenje na procesor:

1. Pokrenite **Process Explorer**.
2. Pokrenite **Command Prompt.**
3. Upišite naredbu **dir \\ime_računala\c$ /s**
   Napomena: Ime računala možete pogledati u komandnoj liniji s naredbom **hostname**.
4. Unutar Process Explorera, **dvostrukim klikom** otvorite svojstva **System** procesa
5. Kliknite na karticu **Threads**
6. Sortirajte dretve prema stupcu **CSwitch Delta**. Primijetite da jedna ili više dretvi koristi datoteku **Srv2.sys**.
7. Označite dretvu i kliknite na **Module** gumb. Time ćete otvoriti svojstva datoteke. Čemu služi Srv2.sys datoteka (što ona implementira)?

----------NAPOMENA----------

U gornjem primjeru smo koristili termin **Cswitch Delta**. Puno ime ovog termina je Context Switch Delta. On označava broj promjena konteksta dretve unutar intervala osvježavanja prikaza. Predefinirano, radi se o 1 sekundi. Dretve čija vrijednost CSwitch Delta nije prikazana se izvršavaju unutar intervala od 10 ms i ne prikazuju se (nema smisla pratiti njihovu aktivnost).

Naredba **dir \\ime_računala\c$ /s** ispisuje sadržaj svih poddirektorija diska C koristeći mrežnu putanju. Ovim načinom generiramo aktivnost serverskog podsustava za dijeljenje datoteka pod Windows OS-om. Navedeni podsustav je baziran na **SMB** (eng. Server Message Block) protokolu.

A Ilica 242, HR-10000 Zagreb
T (01) 2222 182
E student@algebra.hr
www.algebra.hr

4 Što treba znati nakon ove vježbe?

1. Opisati vrste upravljačkih programa
2. Prikazati instalirane upravljačke programe
3. Pomoću Process Monitora pronaći postavke aplikacije
4. Objasniti na primjeru koje informacije aplikacija sprema u Registry