

MS Windows

doc.dr. Samir Lemeš
slemes@mf.unze.ba

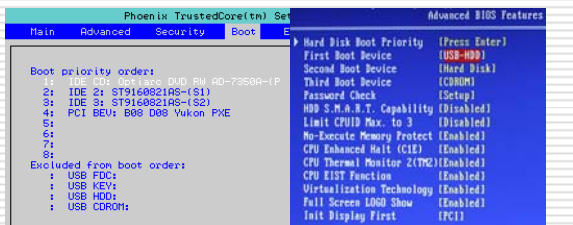
Univerzitet u Zenici - 2012

MS Windows

- Boot disk
- Safe mode
- Drivers, DLL, DLL cache
- System restore
- Default file locations
- Environment variables
- Page file, TMP
- Task Manager, Registry

Boot disk

- Win98 Startup floppy (FORMAT /S)
- Boot CD, Boot DVD
- BIOS boot sequence



Boot disk

- F6 – floppy SCSI/SATA driver
- nLite: <http://www.nliteos.com>
- ISO image



Safe Mode

```
Windows Advanced Options Menu
Please select an option:

Safe Mode
Safe Mode with Networking
Safe Mode with Command Prompt

Enable Boot Logging
Enable UCA Mode
Last Known Good Configuration (your most recent settings that worked)
Directory Services Restore Mode (Windows domain controllers only)
Debugging Mode

Start Windows Normally
Reboot
Return to OS Choices Menu

Use the up and down arrow keys to move the highlight to your choice.
```

Safe Mode

- Shift-F5, F8
- **Safe Mode**
grafičko okruženje bez drivera
- **Safe Mode with Networking**
samo driver za mrežnu karticu
- **Safe Mode with Command Prompt**
bez grafičkog okruženja i bez autoexec.bat
- **Start Windows Normally**
normalan operativni sistem

Drivers, DLL, DLL cache

- ❑ Generički driveri (VGA 640x480)
- ❑ Driveri proizvođača hardvera
- ❑ Digitally signed driver
- ❑ www.driverguide.com

- ❑ DLL – Dynamic Link Library
- ❑ `c:\windows\system32\dllcache`

System Restore

- ❑ Postoji u Windows ME, XP, Vista, 7
- ❑ Može se isključiti
- ❑ My Computer / Properties
- ❑ U slučaju zaraze virusom mora se isključiti – u protivnom se vraća i zaraženi kod
- ❑ F8 ili Install Boot CD

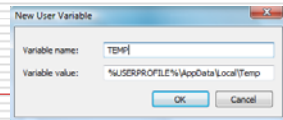


Default file locations

- ❑ C:\Windows
- ❑ C:\Program Files (C:\PROGRA~1)
- ❑ C:\Documents And Settings\
 user\Desktop
- user\My Documents
- user\Local Settings\Temp
- user\Temporary Internet Files
- ❑ Vista, 7: C:\Users\user\...

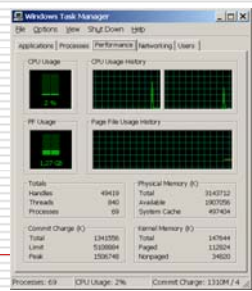
Environment variables

- ❑ U Win 9x – u autoexec.bat
 SET TMP=c:\windows\temp
 SET PATH=c:\qbasic
- ❑ U Win 2K/XP/Vista/7
 My Computer / Properties / Advanced
 Environment Variables
- ❑ System variables
- ❑ User variables



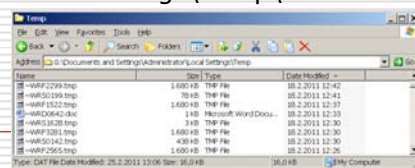
Page file

- ❑ Virtual memory, swap file, page file
- ❑ Koristi se da nadoknadi nedostatak RAM-a
- ❑ My Computer / Properties / Advanced
- ❑ Manual / Let Windows Manage... (1:1,5)



TMP

- ❑ OS i aplikacije kreiraju veliki broj privremenih datoteka
- ❑ DEL C:\Windows\Temp*.*
- ❑ DEL C:\Documents and settings\user\Local settings\Temp*.*



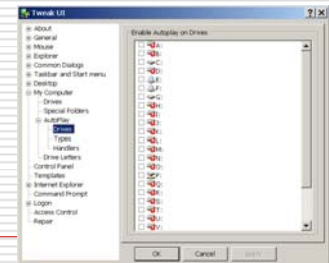
Task Manager

- ❑ Ctrl-Alt-Del
- ❑ Ctrl-Shift-Esc
- ❑ End Task
- ❑ Processes
- ❑ svchost
- ❑ Virusi (svchosts)
- ❑ Explorer
- ❑ cmd/TASKLIST

Image Name	User Name	CPU	Mem Usage
cmd.exe	Korana	00	2.900 K
svchost.exe	SYSTEM	00	3.860 K
taskmgr.exe	Korana	00	5.144 K
Acrobat.exe	Korana	02	36.240 K
CCManager.exe	Korana	00	6.252 K
Power2Go.exe	Korana	00	21.140 K
RealPlayer.exe	Korana	00	137.816 K
PoweringDem...	SYSTEM	00	2.592 K
PoweringDem...	SYSTEM	00	12.620 K
DatSI05.exe	Korana	00	15.072 K
tride_demon.exe	SYSTEM	00	13.044 K
wuauclt.exe	SYSTEM	00	4.752 K
ctfmon.exe	Korana	00	3.512 K
msnappoint.exe	Korana	00	2.476 K
QuickScan.exe	Korana	00	9.444 K
Communicatio...	Korana	00	6.688 K
GoogleUpdate.exe	Korana	00	1.412 K
svchost.exe	Korana	00	6.844 K

Windows Powertoy for XP

- ❑ <http://www.microsoft.com/windowsxp/downloads/powertoys/xppowertoys.msp>
- ❑ Autorun.inf
- ❑ TweakUI



Registry editor

- ❑ Start / Run / regedit
- ❑ Hijerarhijska baza podataka koja čuva informacije o postavkama konfiguracije i podesivim opcijama OS
- ❑ .REG datoteke



Registry editor

- ❑ \Windows\System32\Config\Software
 - System (hardware)
 - SAM (Security Accounts Manager service)
 - Security (sigurnosne postavke)
 - Default (default postavke za korisnike)
 - UserDiff (HKEY_USERS za svakog korisnika)
- ❑ \Documents and Settings\User\NTuser.dat