MS Windows

doc.dr. Samir Lemeš
slemes@mf.unze.ba

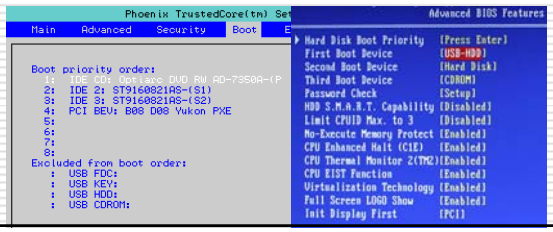
Univerzitet u Zenici - 2012

MS Windows

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

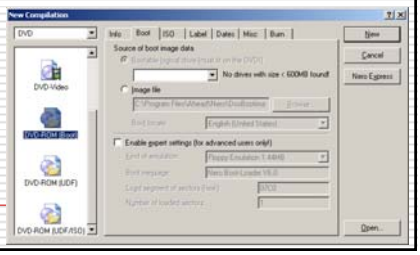
Boot disk

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

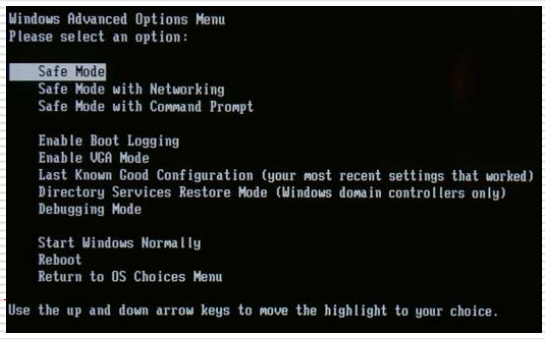


Boot disk

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



Safe Mode



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

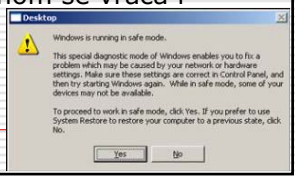
Drivers, DLL, DLL cache

- 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

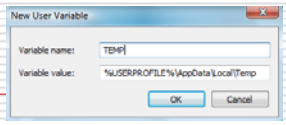


Default file locations

- 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

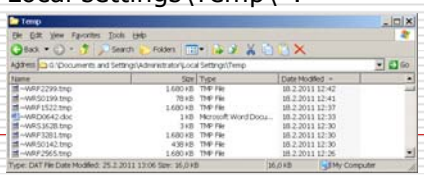


Page file

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

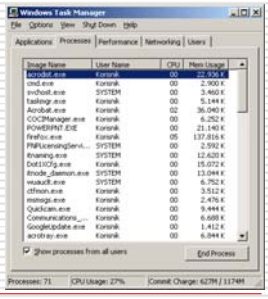
TMP

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



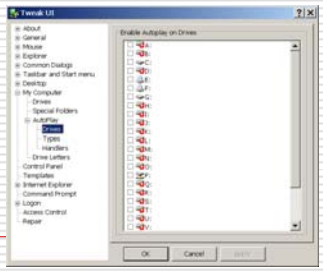
Task Manager

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



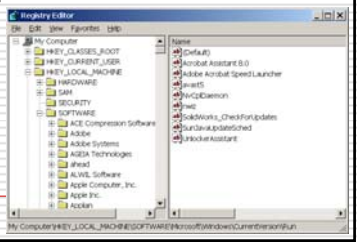
Windows Powertoys for XP

- `http://www.microsoft.com/windowsxp/downloads/powertoys/xppowertoys.mspx`
- 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