Delo z registri

Pripravil:

Šolsko leto:

Direktoriji oz. poddrevesa (Subtree)

- **HKEY_CLASSES_ROOT** skrbi za povezavo med programi in tipi datotek.
- **HKEY_LOCAL_MACHINE** v nasprotju z prejšnjim poddrevesom vsebujejo vse nastavitve trenutnega računalnika.
- **HKEY_USERS** vsebuje vse aktivno naložene uporabniške profile.
- Večkrat boste kje zasledili naziv **hive**, s katerim bodo poimenovani nekatera poddrevesa. Sem spadajo vsa poddrevesa, ki svoje vsebine ne spreminjajo dinamično, kar pomeni, da so stalna.

Tipi registrov:

- **REG_BINARY** je čisto binaren tip in dovoljuje samo vrednosti 0 in 1. Večinoma takšen zapis uporabljajo programi za vrednosti, ki so kritičnega pomena in jih ni dobro spreminjati.

- **REG_DWORD** je zapis dolg 32 bitov oziroma 4 bajte. V tem formatu je zapisano veliko parametrov za gonilnike in druge sistemske servise.

- **REG_SZ** je pravzaprav navaden string oz. polje znakov, ki je človeku popolnoma razumljivo.

- **REG_MULTI_SZ** vključuje več polj, ki jih med sabo loči z NULL znakom.

- **REG_EXPANDED_SZ** je razširljiv niz znakov. V njem se nahaja neka spremenljivka npr. SystemRoot, ki jo program ob klicu zamenja z neko vrednostjo.

Registry Editor

- **Regedit.exe** ima podobo Windows NT Explorerja.

  Regedt.exe ima izboljšane opcije za iskanje po Registry.

  Omogoča nam iskanje po ključu, vrednosti ali podatkih. Z njim lahko ključe shranimo v datoteko in jih kasneje tudi odpremo. Ima pa še možnost odpiranja Registrya drugega računalnika. S tem pa se tudi njegove zmožnosti končajo.

- **regedt32.exe** je zmogljivejši, vendar ima star izgled.

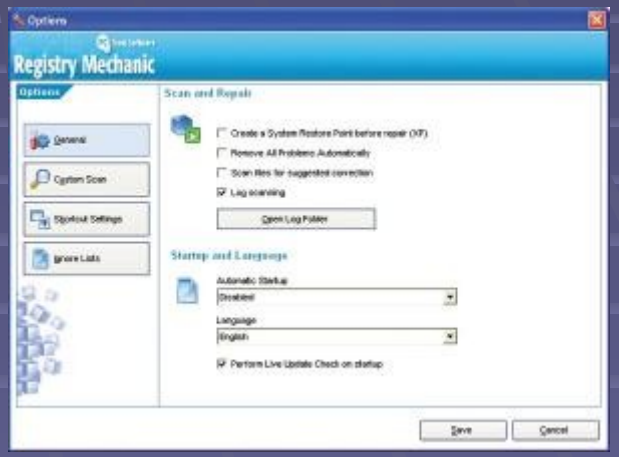
  Iskalne funkcije niso tako učinkovite, saj omogoča iskanje samo po ključih.

  Boljši je na področju varnost. Vsak ključ in poddrevo lahko določimo kdo ga lahko spreminja, bere itd.

  Določimo lahko tudi beleženja dogodkov. Regedt32.exe ima tudi samo bralni način (Read Only) in s tem preprečimo morebitno nezaželeno spreminjanje.

Čiščenje registrov

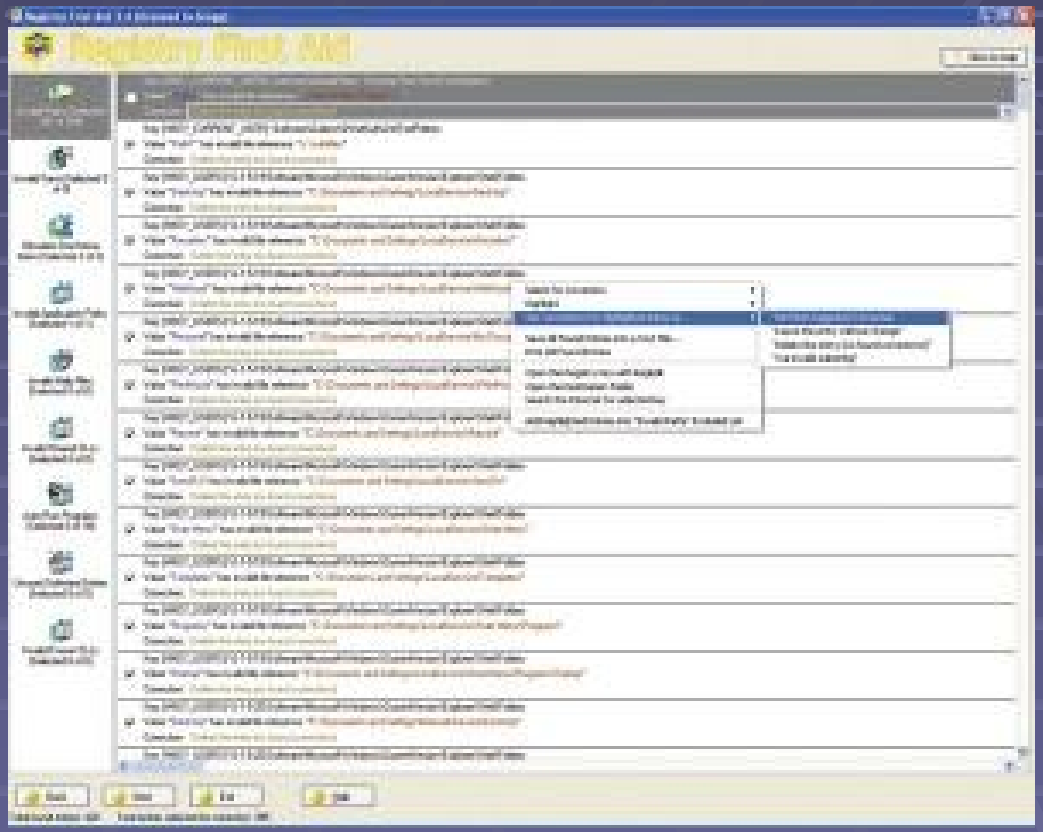
- Registry Mechanic se je v vseh pogledih izkazal dokaj povprečno. Uporabniški vmesnik je lepo oblikovan in preprost, a je naprednejših možnosti premalo za zahtevnega uporabnika.



Registry First Aid 3.4

je našel daleč največ napak v registru in je skoraj vse tudi odpravil.

Očitno pa za večjo natančnost pri iskanju napak rabiš več časa, saj smo za preiskavo celotnega registra čakali nekajkrat dlje kakor pri drugih orodjih.



- **Registry Medic 3.0**

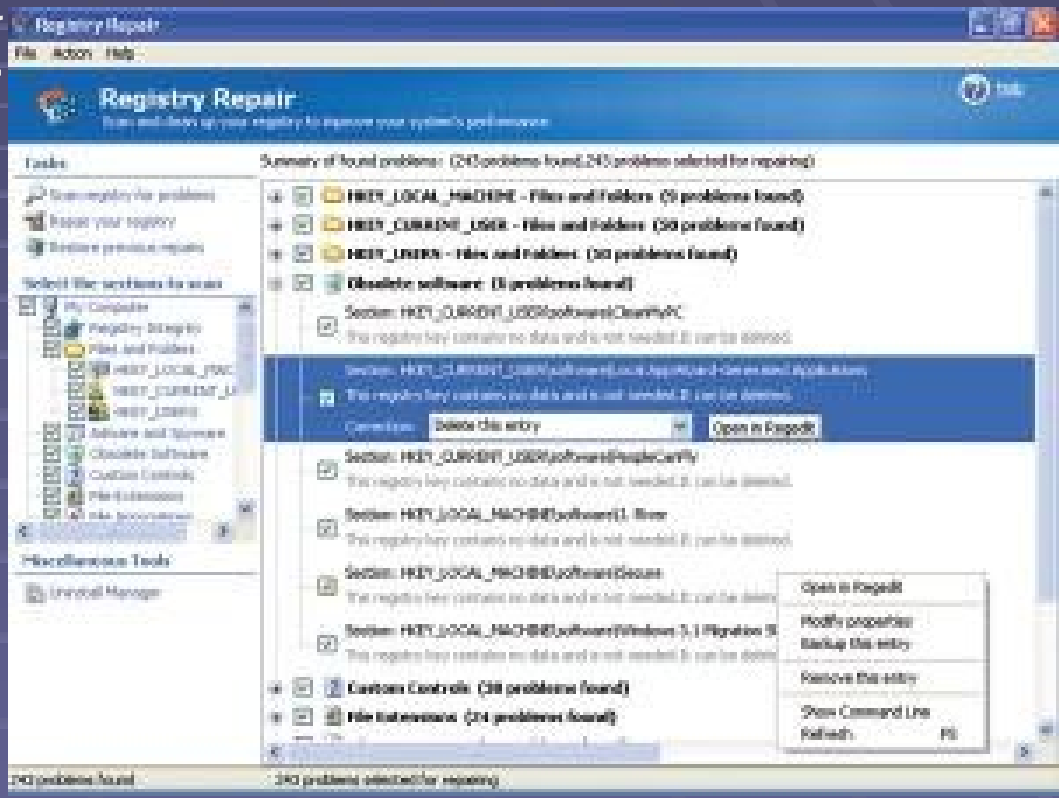
Najhitreje je delo opravil Registry Medic.

Po številu najdenih napak je bil sicer v zlati sredini, a je poleg napak v registru z njim mogoče odstraniti tudi trojanske konje, ki za svoje širjenje in izvajanje uporabljajo register.

- **Registry Repair 1.3**

Zaradi preveč preprostega vmesnika deluje Registry Repair na prvi pogled precej skromno.

a ima na področju varnosti veliko funkcij



END