Rejestr Systemu

Co to jest rejestr?

- Rejestr jest to centralna hierarchiczna baza danych systemu Windows zawierająca informacje na temat:
  - użytkowników,
  - aplikacji,
  - sprzętu.
- W skrócie: rejestr zawiera wszystkie informacje konfiguracyjne.

Hierarchiczna budowa rejestru

Gałęzie drzewa rejestru składają się z:

- Kluczy
- Podkluczy
- Wartości zawierających:
  - Nazwę
  - Typ
  - Dane

Główne klucze rejestru

- HKEY_LOCAL_MACHINE
  – konfiguracja systemu
- HKEY_CURRENT_CONFIG
  – aktualnie używany profil sprzętowy
- HKEY_CLASSES_ROOT
  = HKEY_LOCAL_MACHINE\SOFTWARE\Classes
  – powiązania dla typów plików
- HKEY_USERS
  – informacje konfiguracyjne dla wszystkich profili użytkowników
- HKEY_CURRENT_USER
  = podklucz HKEY_USERS
  – konfiguracja systemu dla bieżącego użytkownika
- HKEY_DYN_DATA
  – informacje przechowywane w pamięci RAM (???)

Typy danych

- REG_SZ – łańcuch (ciąg znaków) o stałej długości,
- REG_BINARY – dowolna wartość binarna, edycja w formacie szesnastkowym,
- REG_DWORD – liczba 32 bitowa, edycja w formacie binarnym, dziesiętnym lub szesnastkowym,
- REG_MULTI_SZ – łańcuch wielokrotny,
- REG_EXPAND_SZ – łańcuch o zmiennej długości,
- REG_FULL_RESOURCE_DESCRIPTOR - seria zagnieżdżonych macierzy zaprojektowanych do przechowywana listy zasobów składnika sprzętowego lub sterownika (tego nie edytujemy!!!).

Pliki rejestru (1/3)

Rejestr składa się z wielu plików, zawierających jedną lub więcej gałęzi.

Obsługiwane typy plików:

- .reg – pliki rejestru
- .txt – pliki tekstowe
- pliki binarne
- .reg – pliki rejestru w wersji 9x/NT4

Pliki rejestru (2/3)

Gałąź rejestru	Pliki pomocnicze
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav, Ntuser.dat, Ntuser.dat.log
HKEY_USERS\DEFAULT	Default, Default.log, Default.sav

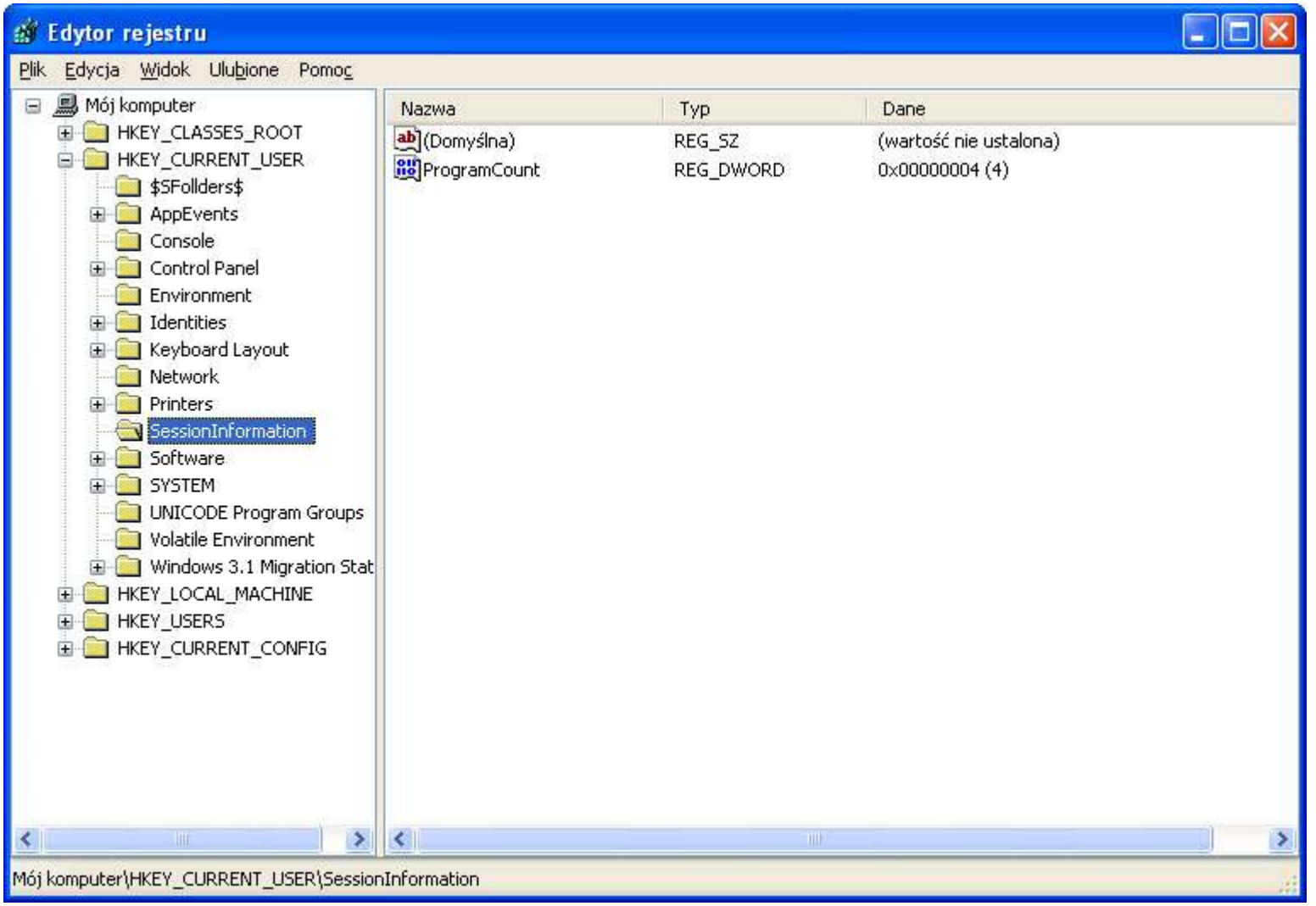
Pliki rejestru (3/3)

- w systemach Windows 95 i 98 są to ukryte pliki user.dat i system.dat znajdujące się w folderze systemowym (najczęściej C:\Windows)
- w Windows Me część rejestru zawiera dodatkowo plik classes.dat
- w systemach NT Rejestr znajduje się w folderach c:\Windows\System32\Config c:\Documents and Settings\%username%\ntuser.dat

Przeglądnie i modyfikacja rejestru (1/3)

- GUI : **regedit.exe, regedt32.exe**
- tryb tekstowy: **reg.exe**
  - odczyt REG QUERY
  - dodawanie klucza/wartości REG ADD
  - usuwanie klucza/wartości REG DELETE
  - kopiowanie kluczy/wartości REG COPY
  - zapisuje gałąź do pliku REG SAVE
  - przywraca gałąź z pliku REG RESTORE
  - tworzy nową gałąź z pliku REG LOAD
  - zwalnia gałąź REG UNLOAD
  - porównuje gałęzie rejestru REG COMPARE
  - eksport rejestru/gałęzi REG EXPORT
  - import rejestru/gałęzi REG IMPORT
- Zapis w pliku .reg i wybranie polecenia Scal z menu podręcznego.

Przeglądnie i modyfikacja rejestru (2/3)



Przeglądnie i modyfikacja rejestru (3/3)

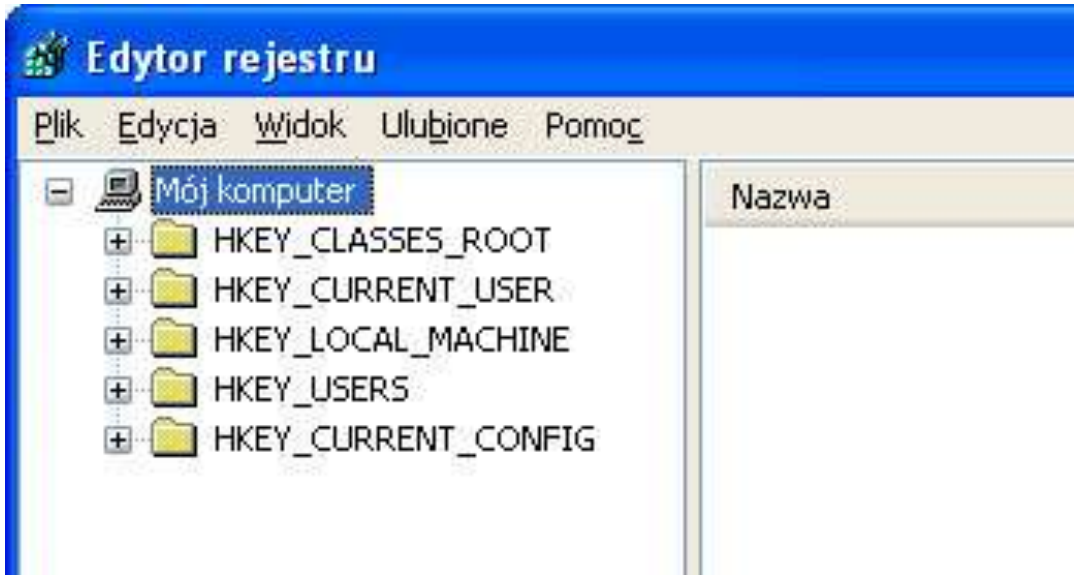
- **Ostrzeżenie**: Błędy popełnione podczas modyfikowania rejestru przy użyciu Edytora rejestru lub innej metody mogą być przyczyną poważnych problemów. W przypadku tych problemów może być wymagane ponowne zainstalowanie systemu operacyjnego. Użytkownik modyfikuje rejestr na własną odpowiedzialność.
  - Za pomocą Edytora rejestru można wykonać następujące czynności: Lokalizowanie poddrzewa, klucza, podklucza lub wartości
  - Dodawanie podklucza lub wartości
  - Zmienianie wartości
  - Usuwanie podklucza lub wartości
  - Zmienianie nazwy podklucza lub wartości
- W obszarze nawigacyjnym Edytora rejestru są wyświetlane foldery. Każdy folder reprezentuje wstępnie zdefiniowany klucz na komputerze lokalnym. W przypadku uzyskania dostępu do rejestru komputera zdalnego wyświetlane są tylko dwa wstępnie zdefiniowane klucze: HKEY_USERS i HKEY_LOCAL_MACHINE.

Kopia zapasowa rejestru (1/4)

- Zmieniając wartości rejestru możemy zmodyfikować wiele ustawień systemowych, poprawiając sobie tym samym komfort pracy z naszym komputerem. Należy jednak wiedzieć, że zapisane są tam również ważne informacje o naszym Windows, które czasami są kluczowe dla niektórych programów.
- Dlatego też nieprawidłowa praca z rejestrem systemu może wpakować nas w niezłe tarapaty. Na szczęście jest prosty sposób aby uchronić się przed załamaniem naszego środowiska. **Wystarczy, że przed każdą ingerencją w rejestr zrobimy jego kopię zapasową**.

Kopia zapasowa rejestru (2/4)

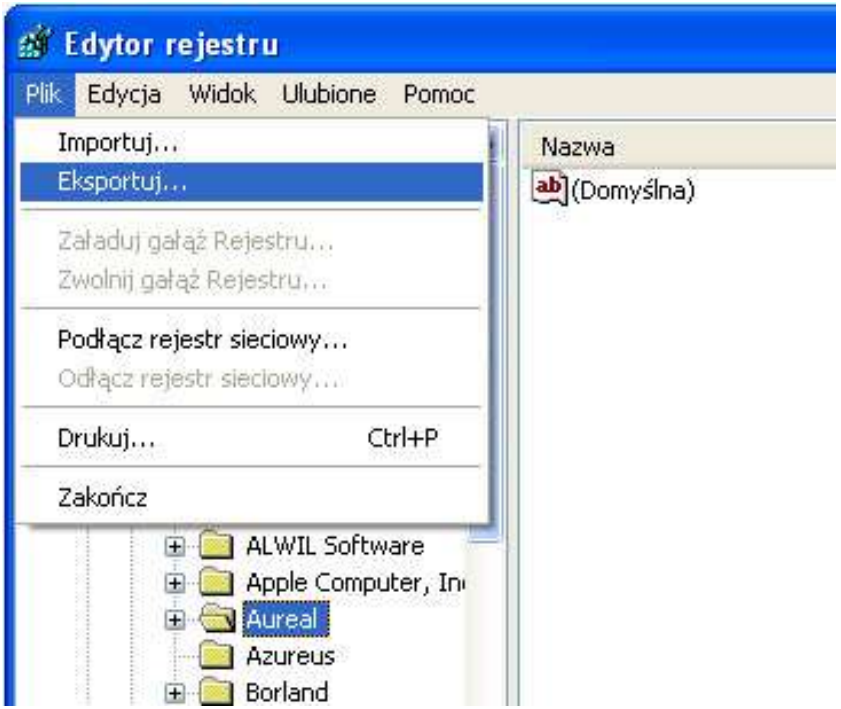
- Otwieramy **Rejestr systemu** wpisując w menu **Uruchom** komendę ***regedit***.
- Jeżeli chcemy zrobić kopię całego rejestru zaznaczamy ikonę **Mój komputer** a następnie z menu **Plik** wybieramy pozycję **Eksportuj...** .
- W następnym oknie podajemy miejsce, w którym zapiszemy naszą kopię i klikamy przycisk **Zapisz.**



Kopia zapasowa rejestru (3/4)

- Warto jednak wiedzieć, że robienie kopii całego rejestru trwa chwilkę i jest zazwyczaj mało opłacalne, ponieważ rzadko zmieniamy wszystkie klucze.
- Zazwyczaj ograniczamy się do edycji tylko niektórych wartości. Dlatego też wystarczy zrobić kopię tyko tych kluczy które zmieniamy.

W tym celu zaznaczamy wybrany klucz a następnie postępujemy tak samo: z menu Plik wybieramy pozycję Eksportuj...



Kopia zapasowa rejestru (4/4)

- Jeżeli po edycji rejestru, nie będziemy zadowoleni z naszych działań, korzystając z kopii zapasowej możemy przywrócić poprzedni wygląd kluczy i wartości. Wystarczy, że klikniemy dwukrotnie na ikonę **archiwum**.

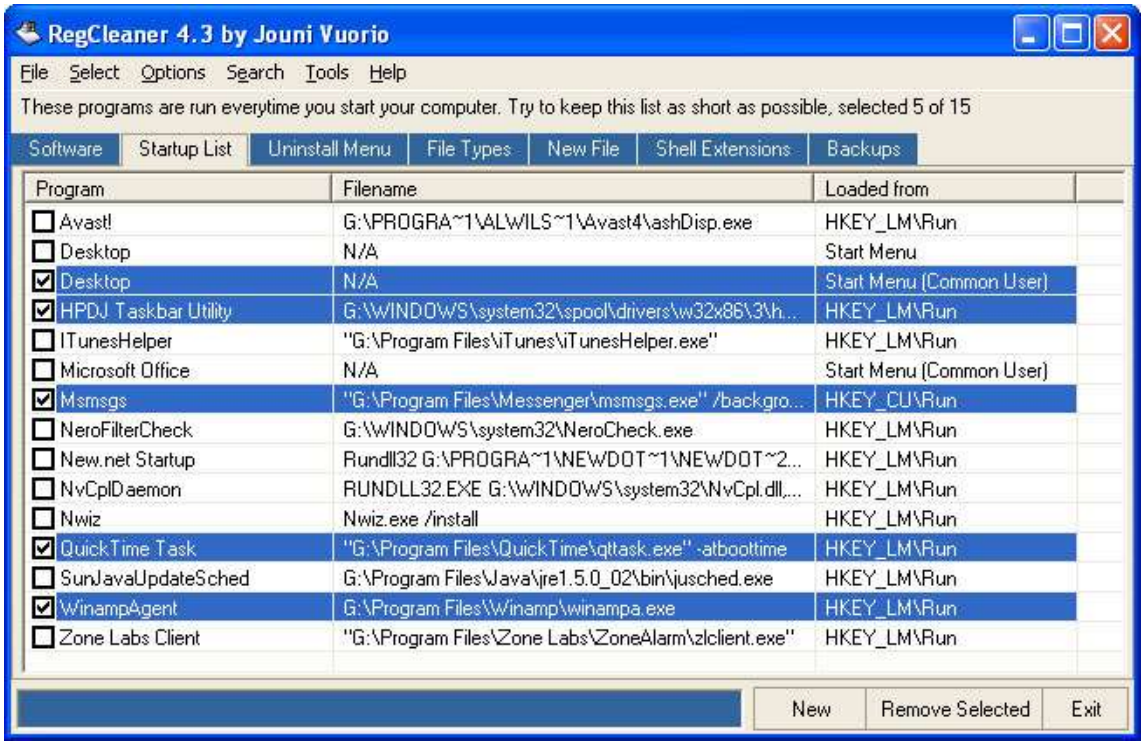
Czyszczenie rejestru (1/4)

- Każdy program wprowadza swoje dane do **Rejestru systemu**. W trakcie deinstalacji powinien swoje wpisy usunąć. Zdarza się jednak dość często, że programy pozostawiają w rejestrze klucze, które nie służą do niczego.
- Pozycje te spowalniają nasz system ponieważ Windows musi analizować wiele kluczy, które nie oznaczają nic.
- Dlatego też powstały programy, które czyszczą rejestr ze "*śmieci*" Jednym z nich jest RegCleaner**.** Jest to aplikacja darmowa.
- Jest również wiele innych aplikacji – proszę poszukać…

Czyszczenie rejestru (2/4)

RegCleaner – sposób użycia.

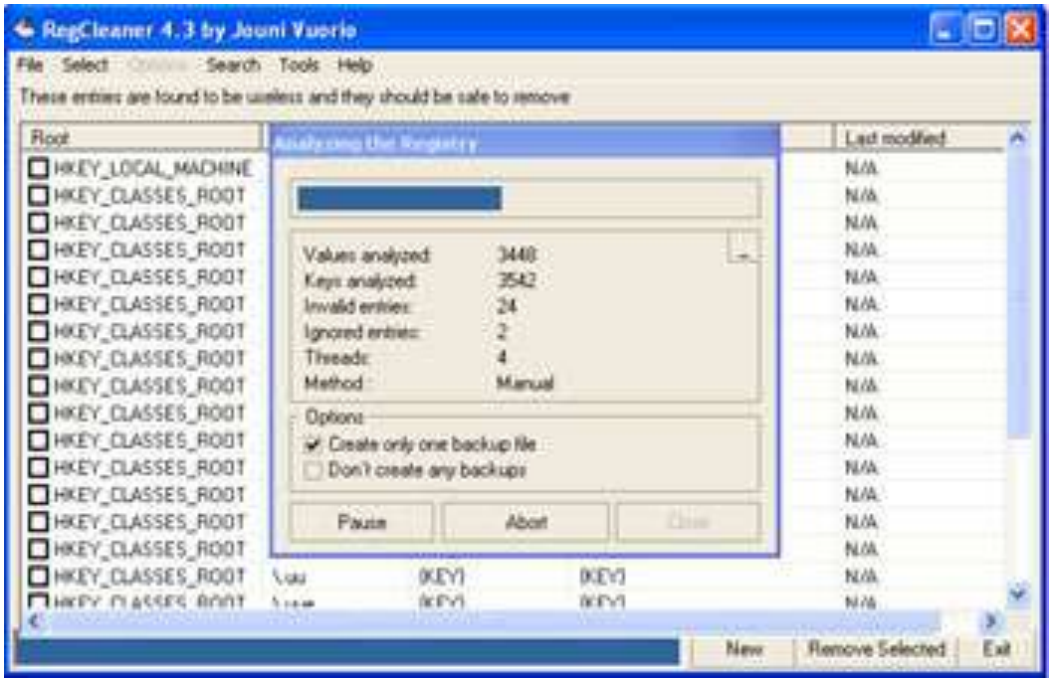
- Główne okno programu podzielone jest na osiem kategorii, którymi możemy w prosty sposób zarządzać. Bez problemu np. wybieramy kategorię **Startup List** a następnie zaznaczamy elementy i kasujemy te pozycje, których nie chcemy uruchamiać wraz ze startem systemu.



Czyszczenie rejestru (3/4)

RegCleaner – sposób użycia.

- Aby dokonać czyszczenia rejestru wybieramy kolejno **Tools, Registry cleanup** a następnie wybraną przez nas opcję z podmenu. Najlepiej wybrać **Do them all**, która spowoduje najgłębsze przejrzenie naszego rejestru. W wyniku tych operacji program zacznie przeglądać klucze i wartości.



Czyszczenie rejestru (4/4)

RegCleaner – sposób użycia.

- Następnie program wyświetli wynik swojej pracy.
- Teraz powinniśmy usunąć znalezione klucze. Wybieramy z menu **Select** pozycję **All,** a następnie klikamy w przycisk **Remove Selected** umieszczony w prawym dolnym rogu ekranu.
- **Pamiętajmy jednak, że program może pomylić się w pracy i wybrać zły klucz. Dlatego też warto zrobić kopię zapasową całego rejestru przed uruchomieniem aplikacji.**

Stosowane skróty nazw kluczy

Dostępne na komputerze lokalnym/zdalnym

- HKLM – HKEY_LOCAL_MACHINE
- HKU – HKEY_USERS

Dostępne tylko na komputerze lokalnym

- HKCU – HKEY_CURRENT_USER
- HKCR – HKEY_CLASSES_ROOT
- HKCC – HKEY_CURRENT_CONFIG

Uwaga!!!

Dostęp do większości informacji dostępnych w rejestrze możliwa jest za pomocą innych narzędzi – należy z nich korzystać.

Zawartość rejestru może się zmieniać.

Istnieją różnice w budowie rejestru dla różnych wersji systemu Windows.

Rejestr nie zawsze jest spójny dla różnych maszyn w sieci.

Przydatne klucze rejestru

- HKLM\System\
- HKLM\Hardware\
- HKLM\Software\Microsoft\Windows\CurrentVersion
- HKCU\Software\Microsoft\Windows\CurrentVersion \Explorer
- HKCU\Software\Microsoft\Windows\CurrentVersion \System
- HKCU\Software\Microsoft\Windows\CurrentVersion \Policies
- HKCU\Volatile Environment

Informacje o systemie

- winmsd.exe
- Tylko do odczytu
- Możliwość podłączenia do komputera zdalnego
  - wykorzystanie pamięci
  - usługi
  - urządzenia
  - przerwania IRQ
  - porty
  - zmienne środowiskowe
  - informacje o sieci
  - informacje o sprzęcie

Adres strony z podpowiedziami co można zmodyfikować w rejestrach

- http://www.agavk.p9.pl/strony/xp_skorowidz_rejestrowy.php

Koniec

- Źródła:
  - http://support.microsoft.com
  - http://www.centrumxp.pl