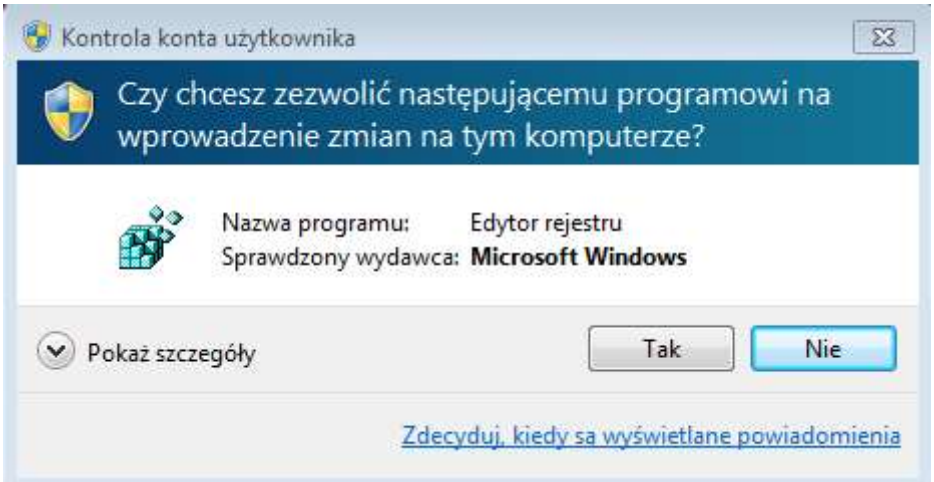
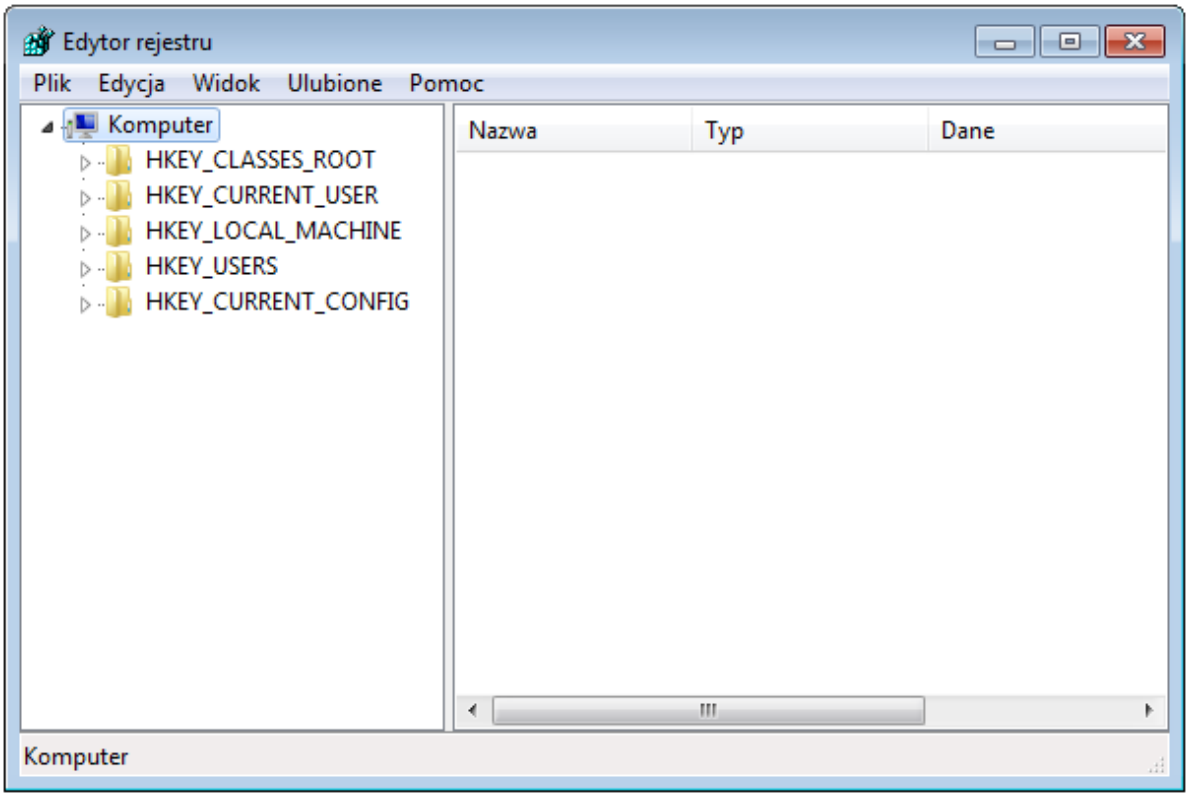
Paweł Pasternak 1Ib

Start>uruchom> regedit



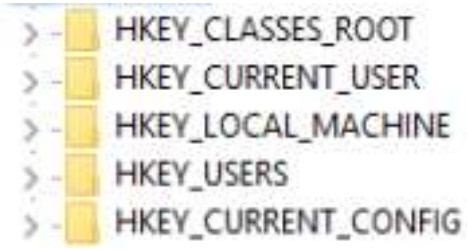

## 1. Czym jest rejestr?

Rejestr – hierarchiczna baza danych konfiguracyjnych w systemach operacyjnych Windows. Są w nim przechowywane informacje o konfiguracji i ustawieniach m.in. użytkowników, urządzeń podłączonych do komputera, a także zainstalowanych programów.

->Rejestr (Windows)

## 2. Jakie istnieją narzędzia do obsługi rejestru ?

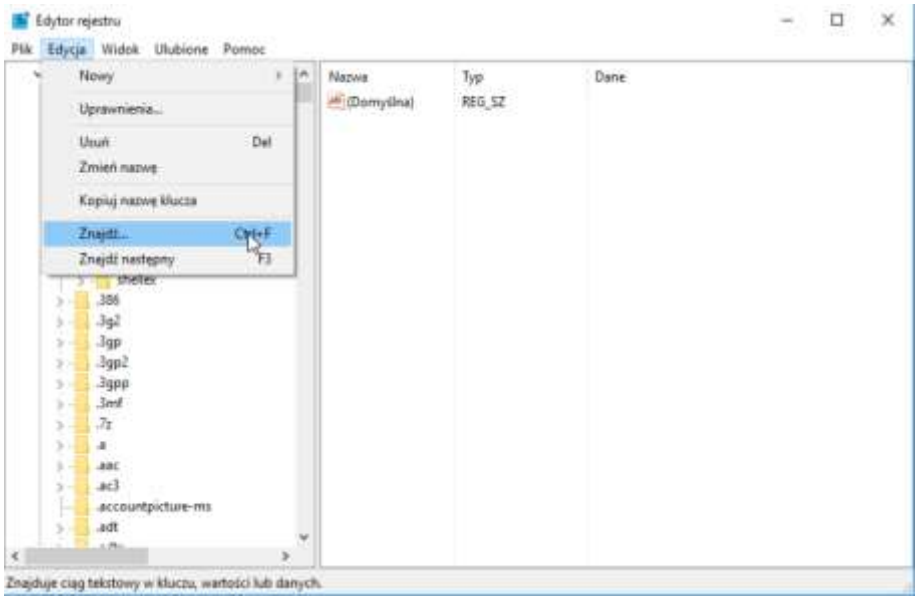
a. regedit




3. **Wymień 5 głównych kluczy rejestru**
4. **Wyjaśnić znaczenie poszczególnych kluczy (jaki jest ich sens jakie dane znajdują się w środku)**
    a. HKEY_CLASSES_ROOT – znajdują się tutaj powiązania z Eksploratorem Windows np. jaki program uruchomić dla danego rozszerzenie.
    b. HKEY_CURRENT_USER – informacje o zalogowanym obecnie użytkowniku, a więc między innymi ustawienia pulpitu, dostępne opcje w panelu sterowania, kolorystyka, czy ustawienia ekranu.
    c. HKEY_LOCAL_MACHINE – informacje dotyczące konfiguracji komputera (obejmuje wszystkich użytkowników).
    d. HKEY_USERS – miejsce w którym przechowywane są profile użytkowników systemu Windows.
    e. HKEY_CURRENT_CONFIG – informacje o sprzęcie.

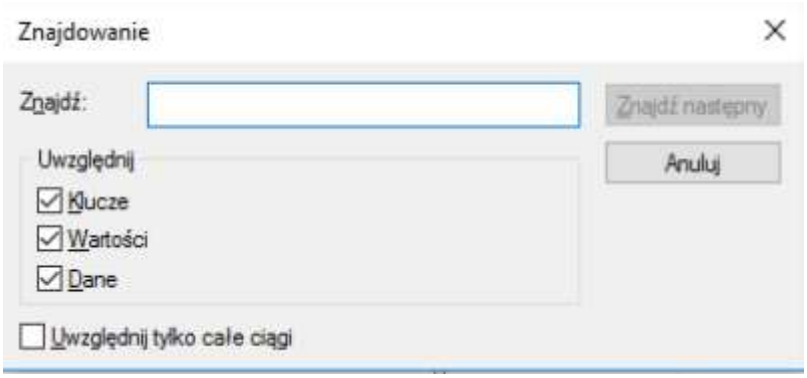
→ Opis kluczy rejestru Windows. Czym jest rejestr systemu Windows ?

5. **Jak można poruszać się w rejestrze i jak wyszukiwać określonych kluczy ?**



## 6. Jakiego skrótu klawiszowego można użyć by wyszukiwać określonych kluczy ?

Ctrl+F →




## 7. Dlaczego powinno pracować się na koncie z ograniczeniami i podnosić uprawnienia do wykonania tylko określonych zadań ?

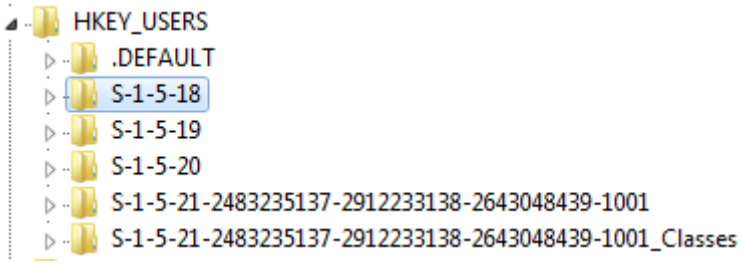
Powinno się pracować na kontach z ograniczeniami, ponieważ nieumiejętny użytkownik mógłby uszkodzić komputer, np. poprzez usunięcie gałęzi rejestru lub zmienienia ich wartości.

## 8. Czym jest SID i jakie znaczenie mają numery

Identyfikator zabezpieczeń (SID) to unikatowa wartość o zmiennej długości, która jest używana do identyfikowania podmiotu zabezpieczeń (na przykład grupy zabezpieczeń) w systemach operacyjnych Windows. Identyfikatory SID, które identyfikują użytkowników rodzajowy lub grupy rodzajowe jest szczególnie dobrze znane. Ich wartości pozostają stałe we wszystkich systemach operacyjnych.

Dobrze znane identyfikatory zabezpieczeń w systemach operacyjnych Windows

S-1-5-18 → Konto usługi, który jest używany przez system operacyjny.
S-1-5-19 → Usługi lokalne
S-1-5-20 → Usługi sieciowe
S-1-5-21-wygenerowany numer → Konta różnych użytkowników



a. Jak sprawdzić jaki numer jest przypisany do twojego profilu

**WMIC useraccount get name,sid**

```
Administrator          S-1-5-21-1272927352-3704931680-3968403175-500
Automat                S-1-5-21-1272927352-3704931680-3968403175-1009
defaultuser0           S-1-5-21-1272927352-3704931680-3968403175-1000
Gość                 S-1-5-21-1272927352-3704931680-3968403175-501
Konto domyślne        S-1-5-21-1272927352-3704931680-3968403175-503
Morty                  S-1-5-21-1272927352-3704931680-3968403175-1003
Ninja                  S-1-5-21-1272927352-3704931680-3968403175-1004
PPasternak             S-1-5-21-1272927352-3704931680-3968403175-1001
Rick                   S-1-5-21-1272927352-3704931680-3968403175-1002
Troll                  S-1-5-21-1272927352-3704931680-3968403175-1010
X                      S-1-5-21-1272927352-3704931680-3968403175-1011
```

**wmic useraccount where name='username' get sid**

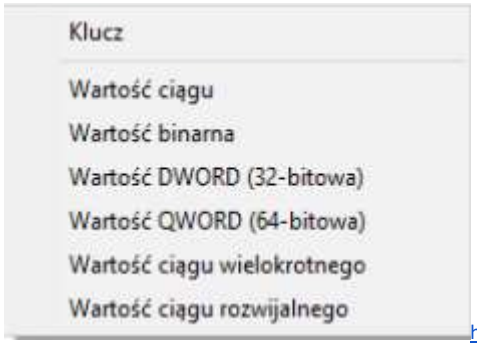
```
C:\Users\PPasternak>wmic useraccount where name="PPasternak" get sid
SID
S-1-5-21-1272927352-3704931680-3968403175-1001
```

b. Co oznaczają te numery

| S | 1 | 5 | 21-7623811015-3361044348-030300820 | 1013 |
|---|---|---|---|---|
| String jest SIDem | Wersja SIDa | Identyfikator uprawnienia | Identyfikator domeny lub lokalnego komputera | Relatywne ID (RID). Każda (z wyjątkami, patrz niżej) grupa lub użytkownik będzie mieć RID 1000 albo wyższy |

## 9. Jakie typy danych mogą znajdować się w rejestrze ?

a. **Klucz** – wybierając Nowy->Klucz dodamy, krótko mówiąc, folder, w którym możemy umieszczać dane w postaci wartości ciągów lub kolejne podklucze.
b. **Wartość ciągu** – jest to prosty ciąg tekstowy, o stałej wartości.
c. **Wartość binarna** – są to dane binarne. Jako ten typ danych, przechowywana jest większość informacji sprzętowych. Edytor rejestru wyświetla je, dla ułatwienia edycji, w formacie szesnastkowym.
d. **Wartość DWORD** – dane zapisane jak 32-bitowe liczby, mające więc długość 4 bajtów.
e. **Wartość QWORD** – rozszerzenie poprzedniej wartości, dane zapisywane są w postaci 64-bitowych liczb.
f. **Wartość ciągu wielokrotnego** – wartości zawierające wartości wielokrotne, zapisane w formie możliwej do odczytania przez użytkownika komputera. Wpisy te rozdzielane są znakami takimi jak spacja bądź przecinek.
g. **Wartość ciągu rozwijanego** – typ danych zawierający ciągi o zmiennej długości. Obejmuje on zmienne, są to dane, które zostaną zastąpione przez właściwe wartości, jeżeli program skorzysta z tych danych.



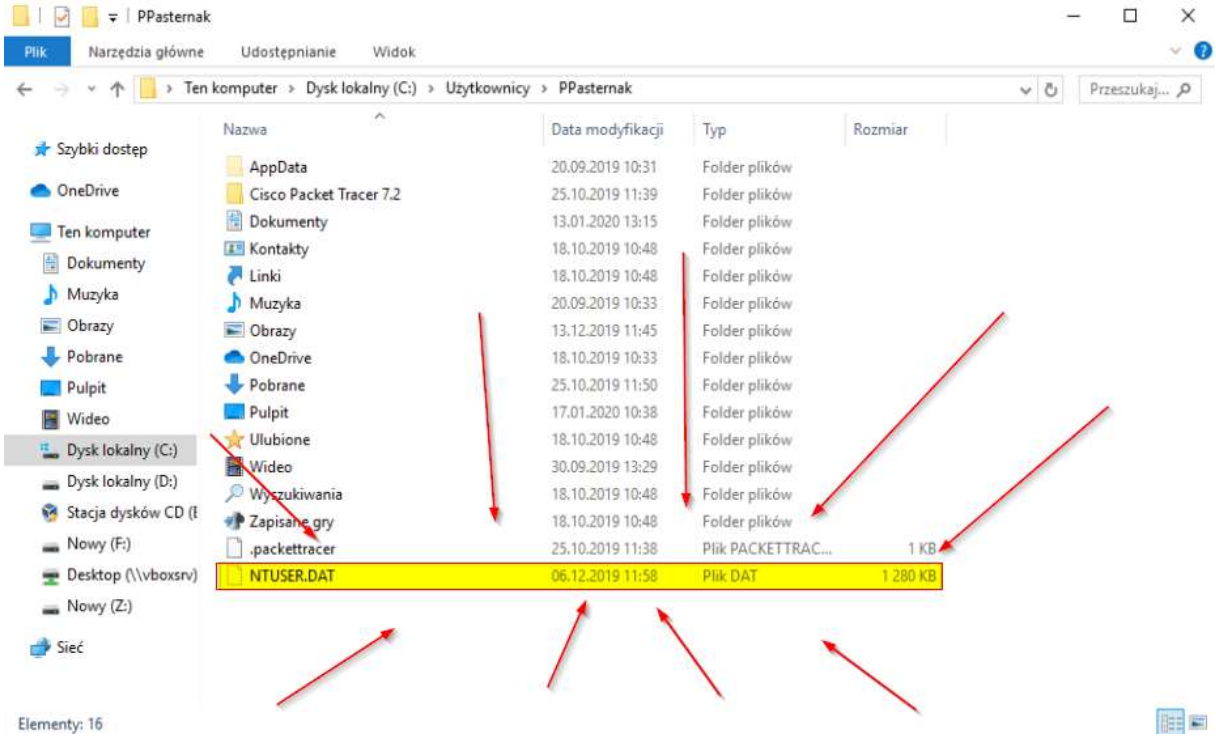
https://www.elektroda.pl/rtvforum/topic1975079.html

## 10.Czy rejestr jest jednym plikiem jeżeli nie to z jakich się składa?

Rejestr składa się z różnych plików o rozszerzeniu .dat .ini .bat .sys

Wiedza tajemna czyli coś niecoś o rejestrze Windows 7 cz.1

## 11.Gdzie zapisane są informacje (na dysku) odnośnie rejestru ?

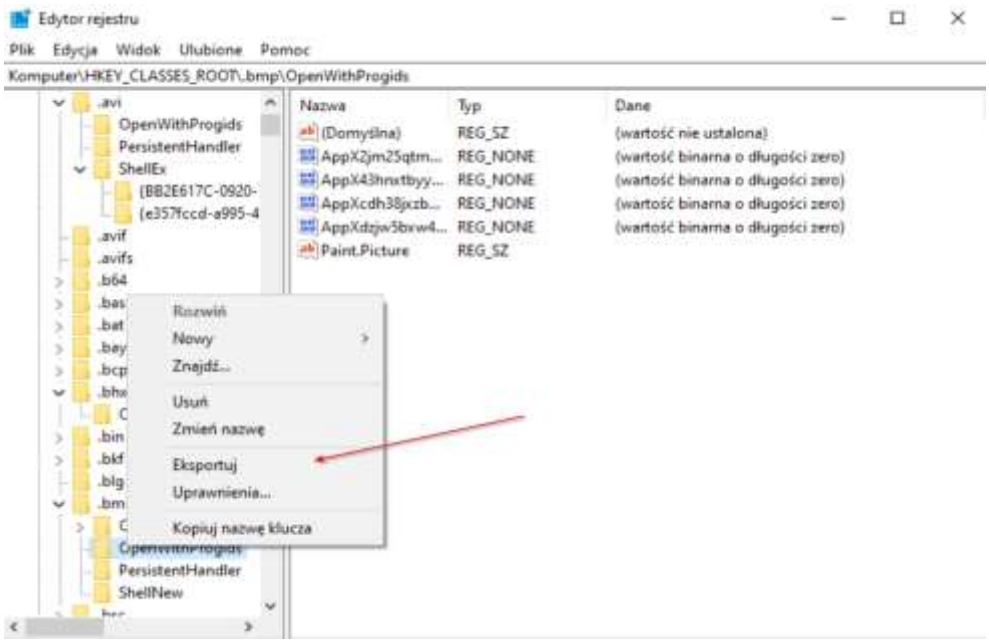


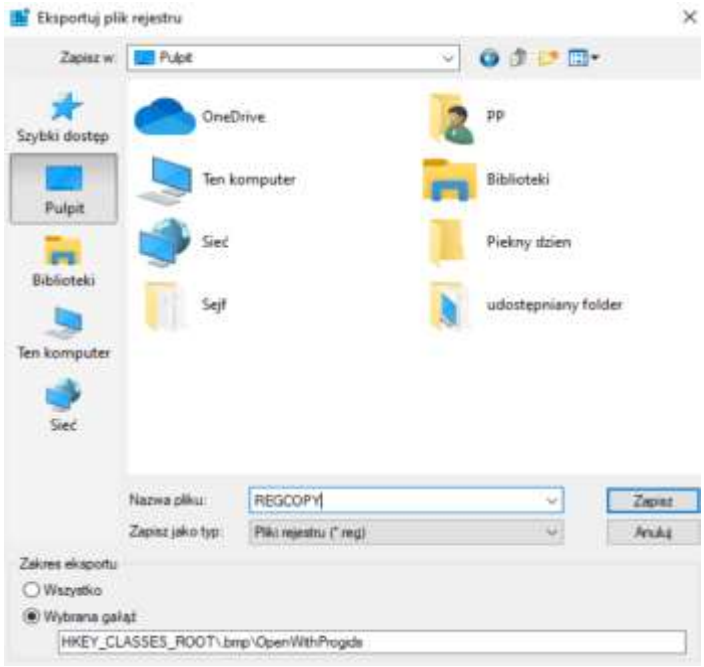

pliki znajdują się w folderze %SystemRoot%\System32\Config i w folderze \Users\nazwa użytkownika\ntuser.dat

Przeczytaj co to jest plik NTUSER.DAT

## 12.Jak wygląda procedura wykonania kopii bezpieczeństwa ?

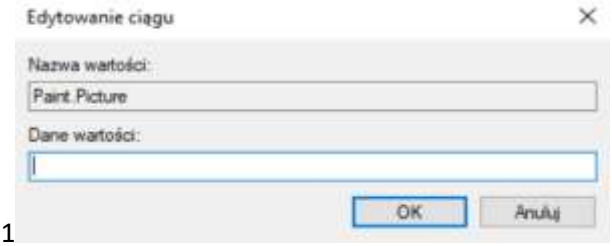
- jednego klucza

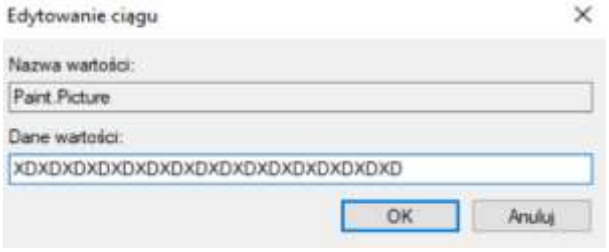


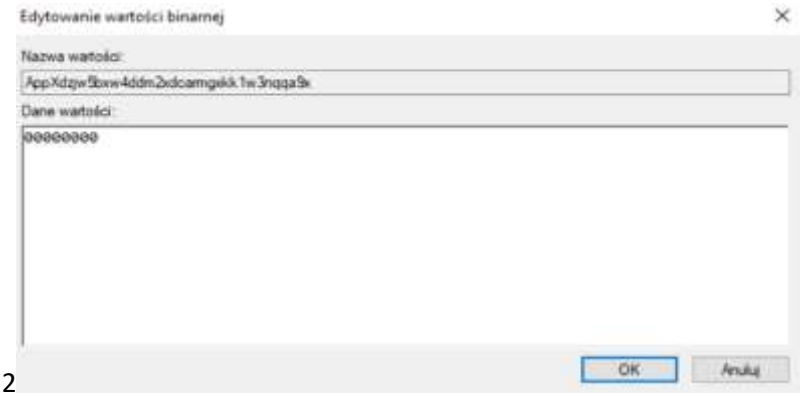

  - Dokonać 5 widocznych zmian w rejestrze i wykazać ich działanie na zasadzie (zad 1przed zad1po, zad2przed zad2po itp.)

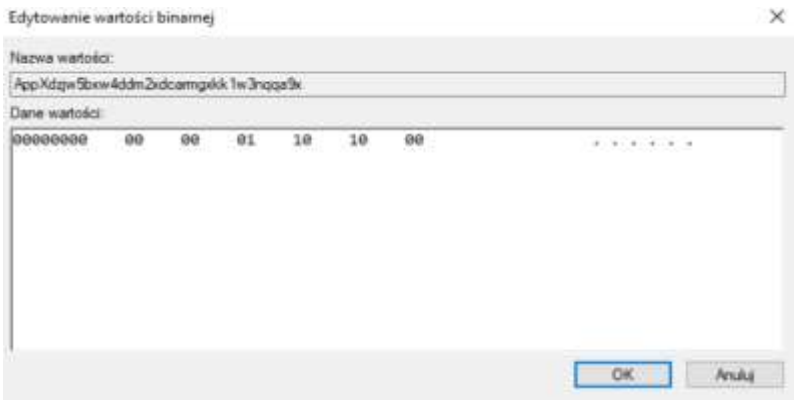
1

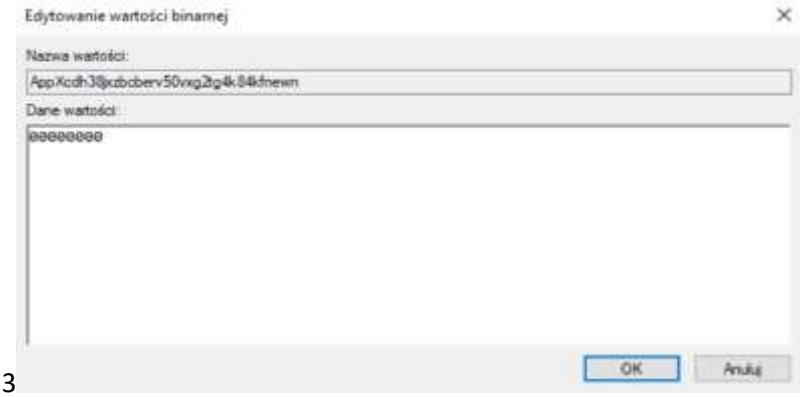

Edytowanie ciągu
Nazwa wartości:
Paint.Picture
Dane wartości:
OK
Anuluj


Edytowanie ciągu
Nazwa wartości:
Paint.Picture
Dane wartości:
xDXDXDXDXDXDXDXDXDXDXDXDXDXDXDXD
OK
Anuluj

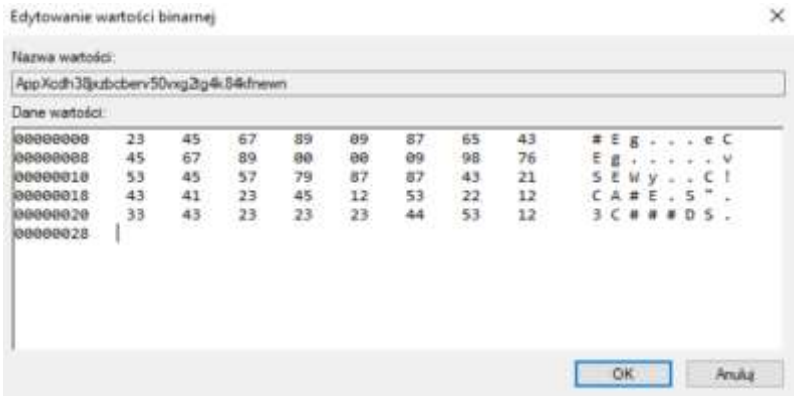
2

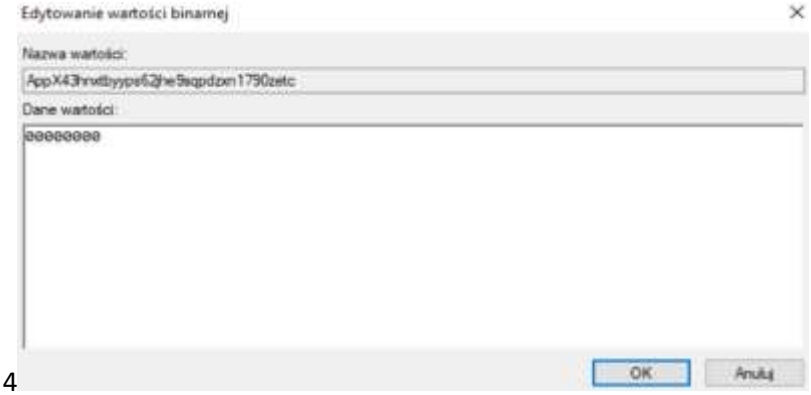

Edytowanie wartości binarnej
Nazwa wartości:
AppXdzjw5bxw4ddm2xdcamgxkk1w3nqqa9k
Dane wartości:
00000000
OK
Anuluj


Edytowanie wartości binarnej
Nazwa wartości:
AppXdzjw5bxw4ddm2xdcamgxkk1w3nqqa9k
Dane wartości:
00000000 00 00 01 10 10 00 . . . . . .
OK
Anuluj

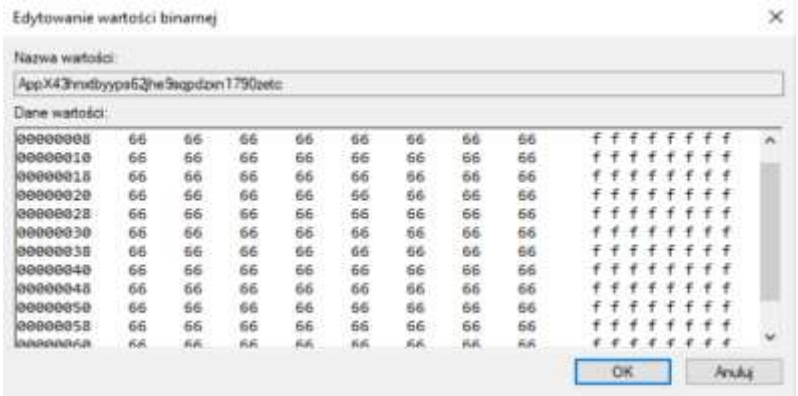

Edytowanie wartości binarnej
Nazwa wartości:
AppXcdh38jxzbcberv50vxg2g4k84kfnewn
Dane wartości:
00000000
OK
Anuluj

3

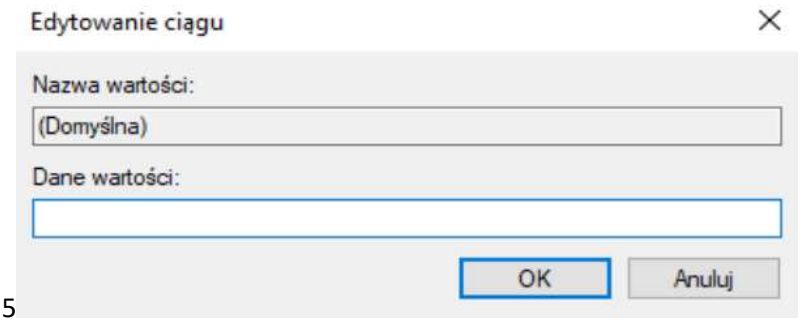

Edytowanie wartości binarnej
Nazwa wartości:
AppXcdh38jxzbcberv50vxg2g4k84kfnewn
Dane wartości:
00000000 23 45 67 89 89 87 65 43 # E g . . . e C
00000008 45 67 89 00 00 09 98 76 E g . . . . . v
00000010 53 45 57 79 87 87 43 21 S E W y . . C !
00000018 43 41 23 45 12 53 22 12 C A # E . S " .
00000020 33 43 23 23 23 44 53 12 3 C # # # D S .
00000028
OK
Anuluj

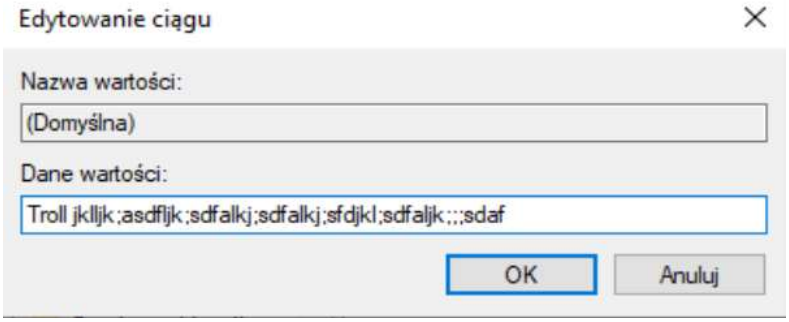

Edytowanie wartości binarnej
Nazwa wartości:
AppX43hrxtbyypx62jhe9sqpdzxn1790zetc
Dane wartości:
00000000
OK
Anuluj

4

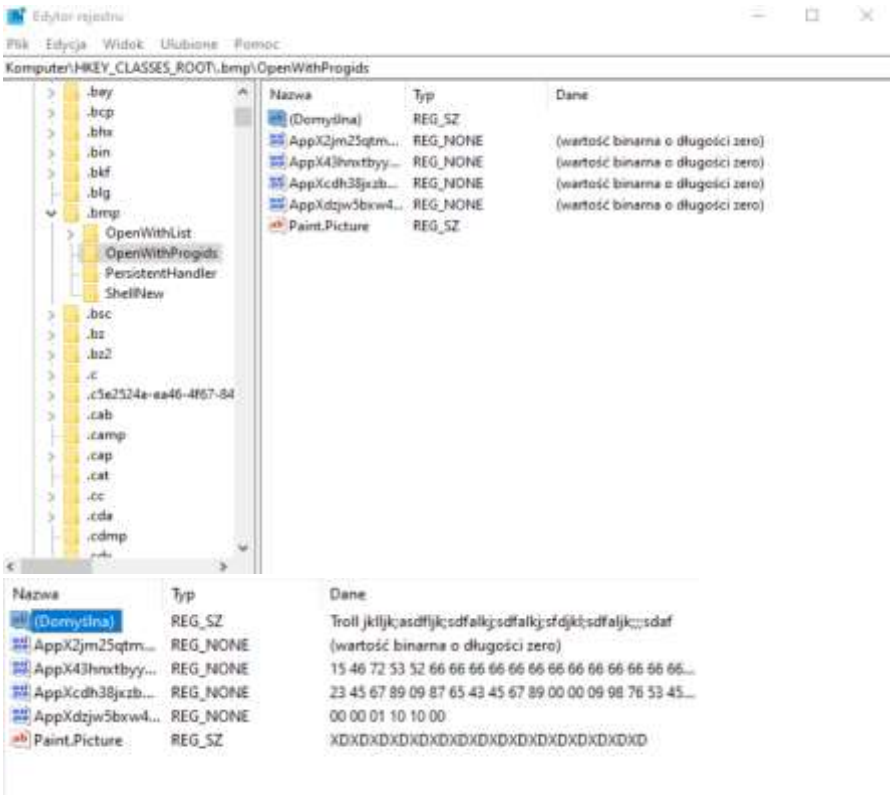

Edytowanie wartości binarnej
Nazwa wartości:
AppX43hrxtbyypx62jhe9sqpdzxn1790zetc
Dane wartości:
00000008 66 66 66 66 66 66 66 66 f f f f f f f f
00000010 66 66 66 66 66 66 66 66 f f f f f f f f
00000018 66 66 66 66 66 66 66 66 f f f f f f f f
00000020 66 66 66 66 66 66 66 66 f f f f f f f f
00000028 66 66 66 66 66 66 66 66 f f f f f f f f
00000030 66 66 66 66 66 66 66 66 f f f f f f f f
00000038 66 66 66 66 66 66 66 66 f f f f f f f f
00000040 66 66 66 66 66 66 66 66 f f f f f f f f
00000048 66 66 66 66 66 66 66 66 f f f f f f f f
00000050 66 66 66 66 66 66 66 66 f f f f f f f f
00000058 66 66 66 66 66 66 66 66 f f f f f f f f
OK
Anuluj

5

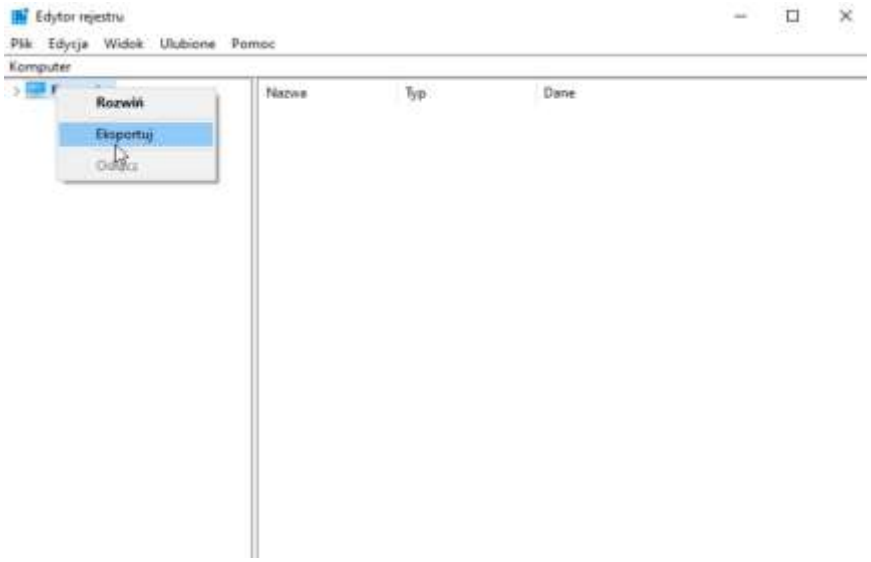

Edytowanie ciągu
Nazwa wartości:
(Domyślna)
Dane wartości:
OK
Anuluj

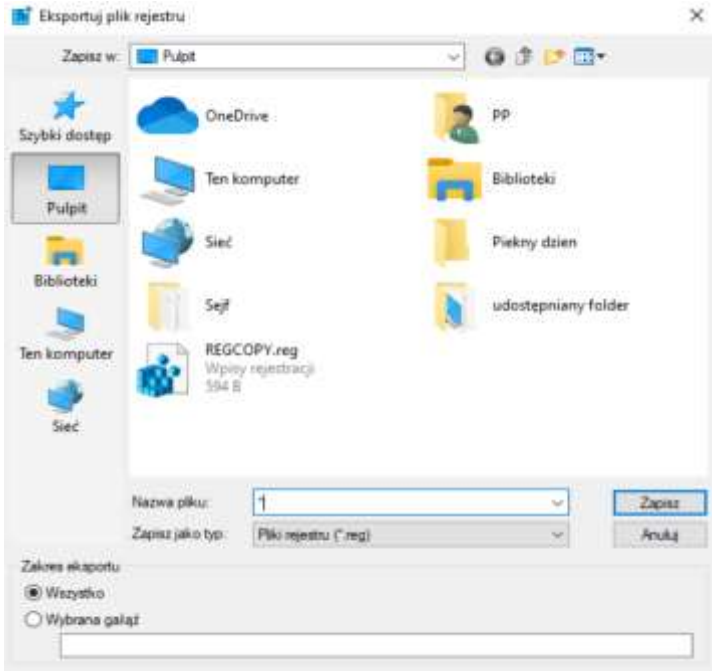

Edytowanie ciągu
Nazwa wartości:
(Domyślna)
Dane wartości:
Troll jkljk;asdfljk;sdfalkj;sdfalkj;sfdjkl;sdfaljk;;;sdaf
OK
Anuluj

Ogólnie


Komputer\HKEY_CLASSES_ROOT\.bmp\OpenWithProgids
OpenWithList
OpenWithProgids
PersistentHandler
ShellNew
Nazwa
Typ
Dane
(Domyślna)
REG_SZ
Troll jkljk;asdfljk;sdfalkj;sdfalkj;sfdjkl;sdfaljk;;;sdaf
AppX2jm25qtm...
REG_NONE
(wartość binarna o długości zero)
AppX43hnxtbyy...
15 46 72 53 52 66 66 66 66 66 66 66 66 66 66 66 66 66...
AppXcdh38jxzb...
23 45 67 89 09 87 65 43 45 67 89 00 00 09 98 76 53 45...
AppXdzjw5bxw4...
00 00 01 10 10 00
Paint.Picture
XDXDXDXDXDXDXDXDXDXDXDXDXDXD

- całego rejestru



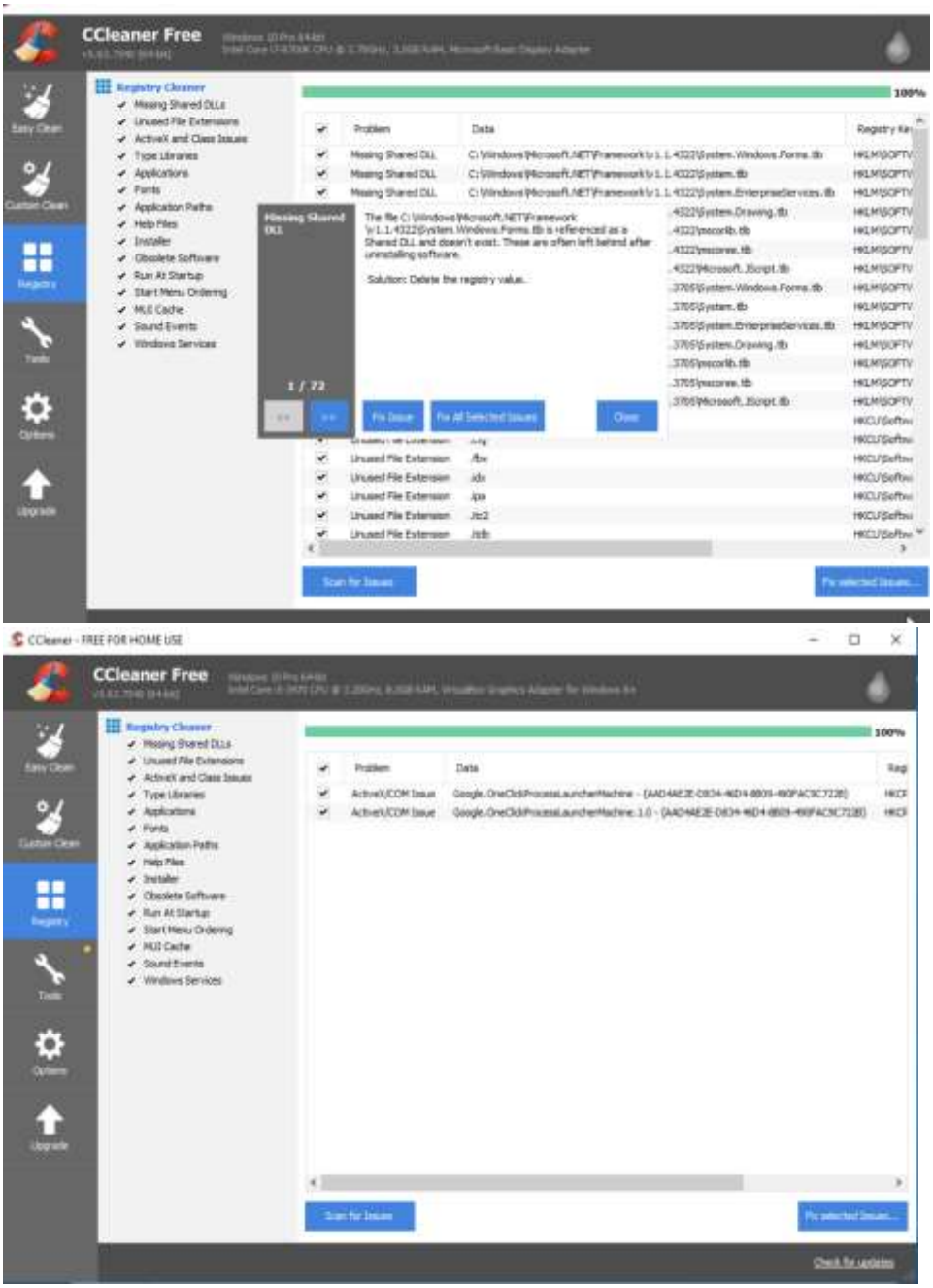



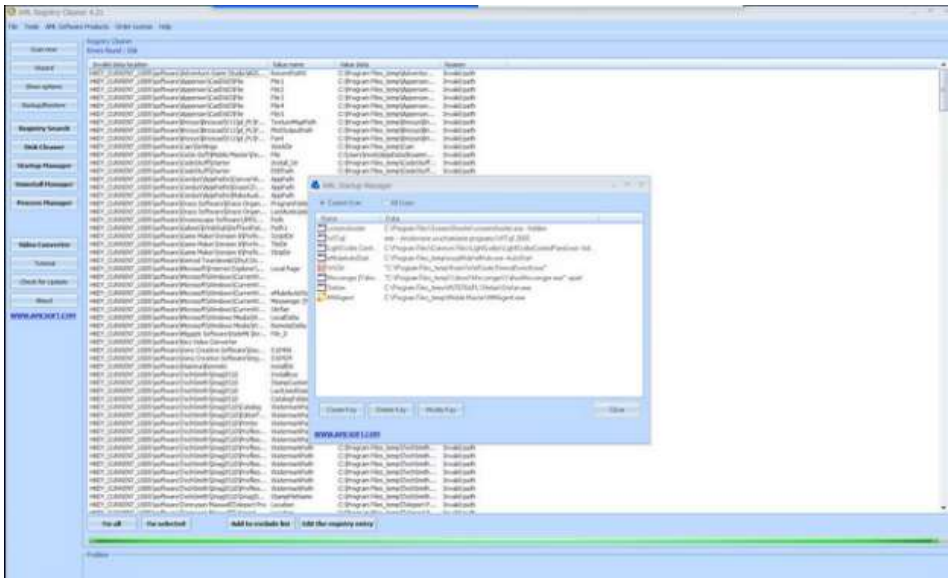

## 13.Do czego służy plik NTUSER.DAT

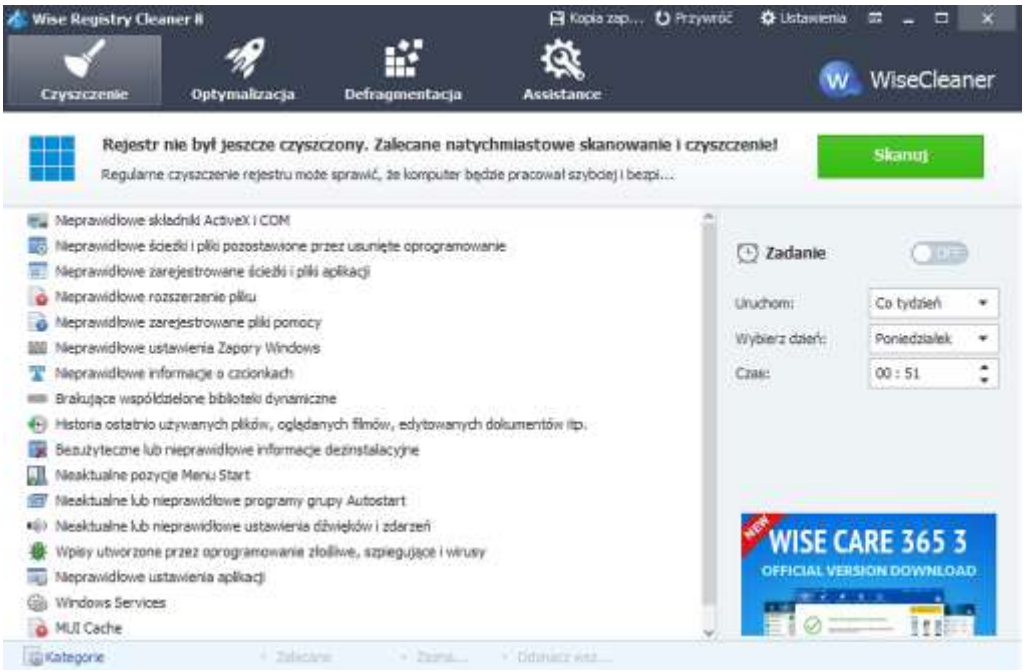
Podczas instalacji, Windows tworzy domyślny profil użytkownika w katalogu profilu Default User. Plik ten jest kopiowany do folderu z profilem każdego użytkownika logującego się po raz pierwszy na danym komputerze.

Fakt ten można wykorzystać aby wprowadzić do rejestru domyślne ustawienia rejestru, które będą aplikowane każdej nowej osobie. Szczegóły wykorzystania można przeczytać we wpisach traktujących o domyślnej tapecie i domyślnej stronie startowej IE. Na stronie Microsoft, jest też opisane jak ustawić jednorazowe uruchamianie skryptu logowania podczas logowania nowego użytkownika.

## 14.Pokaż działanie 3 programów do czyszczenia rejestru






Wise Registry Cleaner 8
Kopia zap...
Przywróć
Ustawienia
Czyszczenie
Optymalizacja
Defragmentacja
Assistance
WiseCleaner
Rejestr nie był jeszcze czyszczony. Zalecane natychmiastowe skanowanie i czyszczenie!
Regularne czyszczenie rejestru może sprawić, że komputer będzie pracował szybciej i bezpi...
Skanuj
Nieprawidłowe składniki ActiveX i COM
Nieprawidłowe ścieżki i pliki pozostawione przez usunięte oprogramowanie
Nieprawidłowe zarejestrowane ścieżki i pliki aplikacji
Nieprawidłowe rozszerzenie pliku
Nieprawidłowe zarejestrowane pliki pomocy
Nieprawidłowe ustawienia Zapory Windows
Nieprawidłowe informacje o czcionkach
Brakujące współdzielone biblioteki dynamiczne
Historia ostatnio używanych plików, oglądanych filmów, edytowanych dokumentów itp.
Bezużyteczne lub nieprawidłowe informacje dezinstalacyjne
Nieaktualne pozycje Menu Start
Nieaktualne lub nieprawidłowe programy grupy Autostart
Nieaktualne lub nieprawidłowe ustawienia dźwięków i zdarzeń
Wpisy utworzone przez oprogramowanie złośliwe, szpiegujące i wirusy
Nieprawidłowe ustawienia aplikacji
Windows Services
MUI Cache
Kategorie
Zadanie
Uruchom:
Co tydzień
Wybierz dzień:
Poniedziałek
Czas:
00 : 51
NEW
WISE CARE 365 3
OFFICIAL VERSION DOWNLOAD