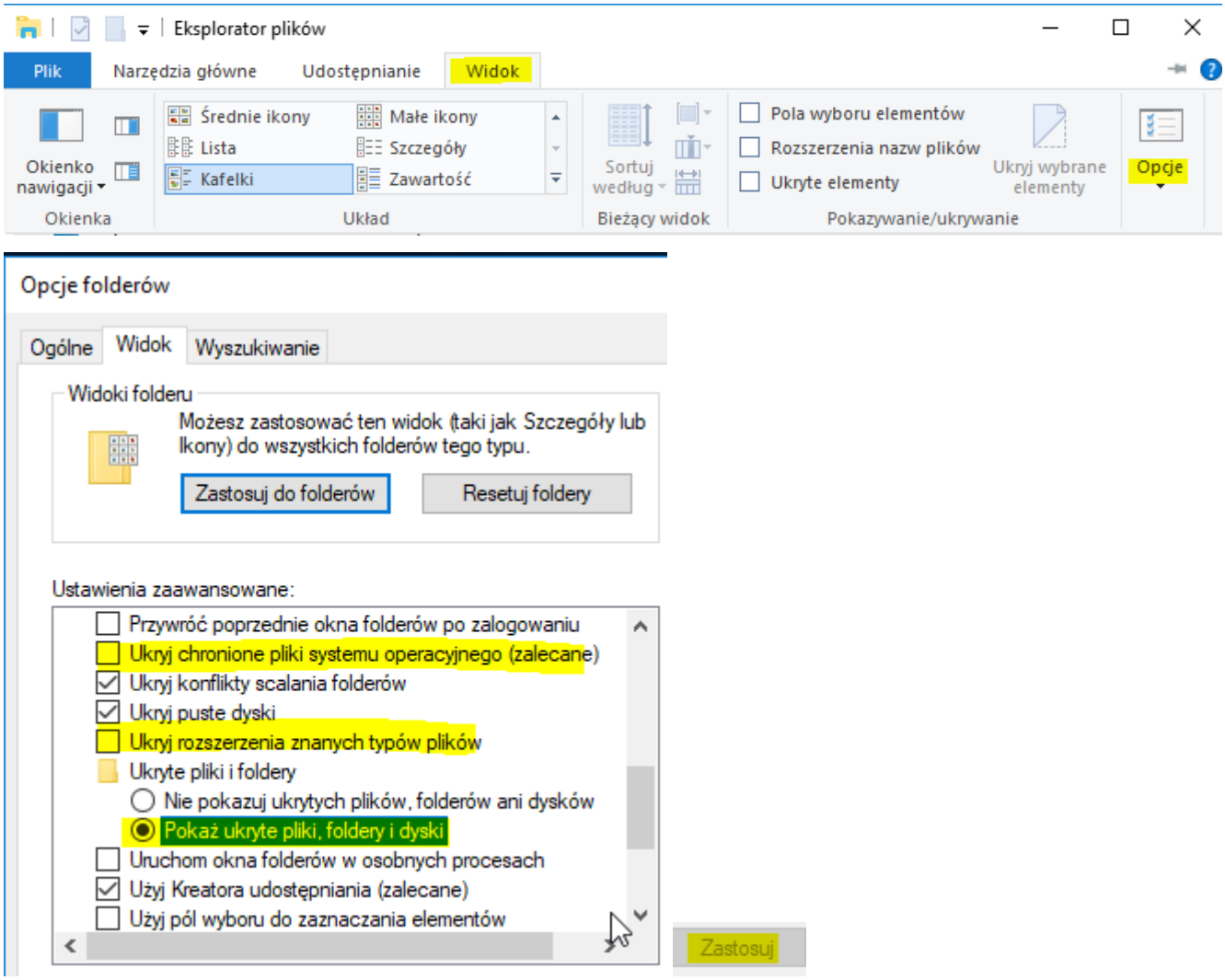
T: Edytor rejestru: dane, klucze i ich zawartość.

Ćwiczenie dla Windows 10

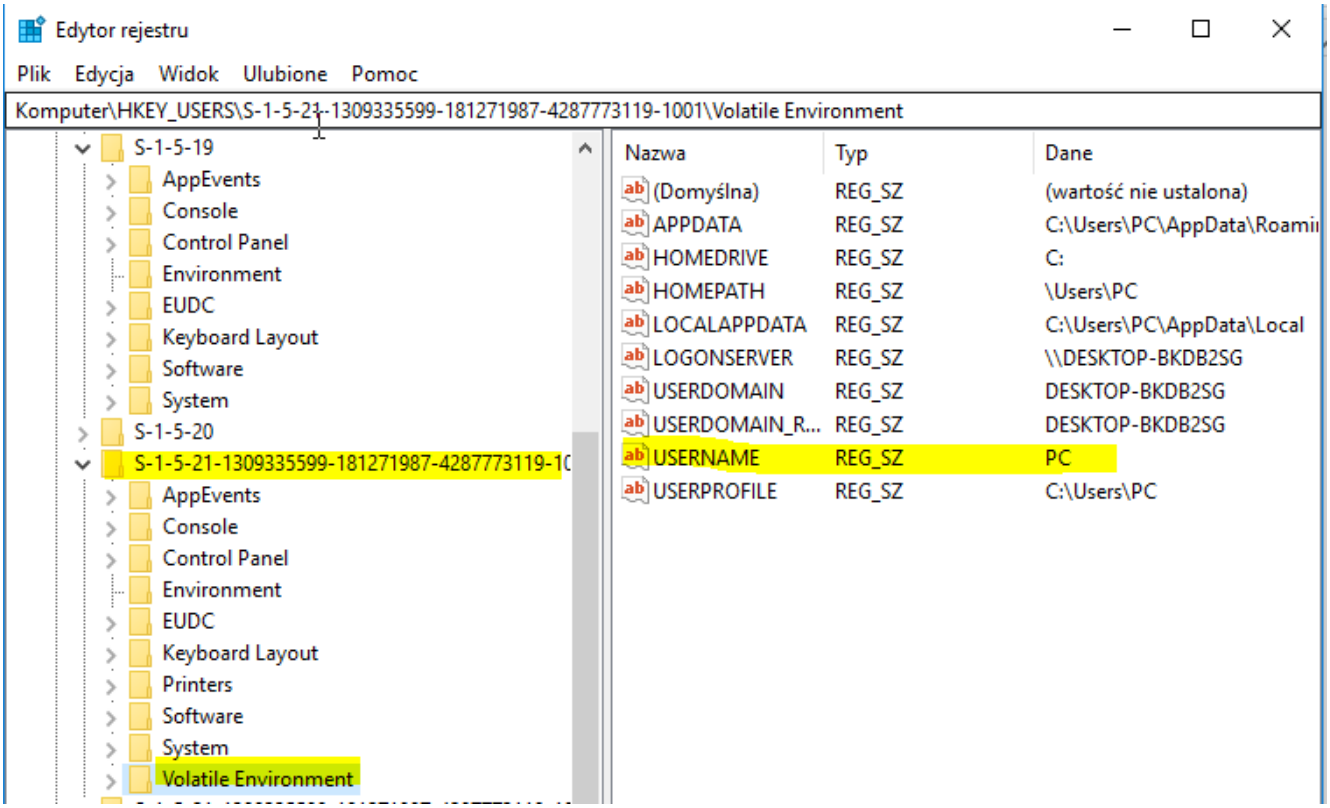
W tym ćwiczeniu zweryfikujesz budowę rejestru.

1. Ustaw opcje folderów jak poniżej



2. Odszukaj na komputerze pliki rejestru (pliki, w których przechowywany jest Rejestr systemu Windows). Zapisz w zeszycie nazwy tych plików i wyjaśnij ich funkcje (zgłoś wykonanie tego punktu). Pliki te nazywane hives (ule) umieszczone są w folderach
   - \Windows\System32\config,
   - \Users\nazwa_użytkownika.
3. Z **menu wyszukiwania** w polu wyszukiwania wpisz **regedit.exe**, wybierz prawoklik „Uruchom jako administrator” a następnie naciśnij klawisz Enter. Jeśli zostanie wyświetlony monit o hasło administratora lub potwierdzenie, wpisz hasło lub potwierdź.

4. W Edytorze rejestru zlokalizuj i kliknij klucz rejestru, podklucz, i ich zawartość. Sprawdź czy
   a) w rejestrze znajduje się pięć poddrzew: 1. HKEY_CLASSES_ROOT 2. HKEY_CURRENT_USER 3. HKEY_LOCAL_MACHINE 4. HKEY_USERS 5. HKEY_CURRENT_CONFIG
   b) poddrzewo HKEY_CLASSES_ROOT (HKCR) zawiera informacje na temat powiązań, czyli jakie typy plików są uruchamiane za pomocą jakich aplikacji.
   c) poddrzewo HKCR zawiera definicje każdego obiektu istniejącego w Windows.
   d) poddrzewo HKCR zawiera klucze rozszerzeń plików, których nazwy są takie same jak rozszerzenia plików, których dotyczą (.doc, .txt)
   e) poddrzewo HKCR zawiera klucze definicji klasy zawierające informacje o obiektach COM (ang. Component Object Model);
   f) poddrzewo Poddrzewo HKEY_CURRENT_USER (HKCU) zawiera ustawienia profilu użytkownika, który aktualnie jest zalogowany w systemie.
   g) każdy z użytkowników komputera ma własną kopię pliku USER.DAT umieszczoną w folderze użytkownika wewnątrz folderu Users.
   h) HKCU jest jedynie wskaźnikiem do odpowiedniego klucza w poddrzewie HKEY_USERS.



Istnieje grupa kluczy, które tworzy system na każdym komputerze.

5. Sprawdź i zapisz w zeszycie co zawierają klucze:

AppEvents – klucz zawiera wpisy wartości zdarzeń aplikacji, takie jak dźwięki powiązane z określonymi wydarzeniami w systemie (np. pojawiającego się błędu), jak również zapisane schematy dźwiękowe.

Console – zawiera wpisy wartości odpowiedzialne za wygląd wiersza poleceń systemu Windows

Control Panel - klucz zawiera wpisy wartości reprezentujące ustawienia Panelu Sterowania systemu Windows. Klucz ten opowiada plikom WIN.INI i CONTROL.INI wykorzystywanym w poprzednich wersjach

Environment – klucz przechowujący zmienne środowiskowe ustawione za pomocą apletu System w Panelu sterowania

Volatile Environment - klucz zawiera wpisy wartości, które opisują identyfikatory (ID) domyślnego użytkownika i ostatniego użytkownika, który pomyślnie zalogował się do systemu

Keyboard Layout – wpisy wartości tego klucza odpowiadają językowi bieżącego ustawienia klawiatury

Printers – klucz zawiera wpisy wartości opisujące drukarki dostępne dla bieżącego użytkownika

Software – wpisy wartości tego klucza odpowiadają ustawieniom wszystkich aplikacji zdefiniowanych dla bieżącego użytkownika i mają analogiczną strukturę co HKLM Software

6. W poddrzewie HKLM sprawdź i zapisz w zeszycie co zawierają podklucze:

Hardware – urządzenia sprzętowe, które zostaną wykryte podczas uruchamiania systemu.

SAM – klucz przechowuje bazę SAM (ang. Security Manager Accounts), która zawiera informacje dotyczące użytkowników i grup skonfigurowanych na tym komputerze.

Security – klucz zawiera aktualne ustawienia zabezpieczeń odnoszące się do zasad uprawnień użytkownika.

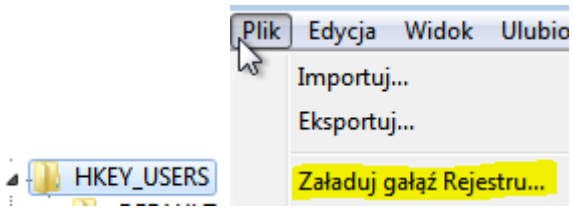
Software – klucz zawiera ustawienia większości aplikacji i systemu.

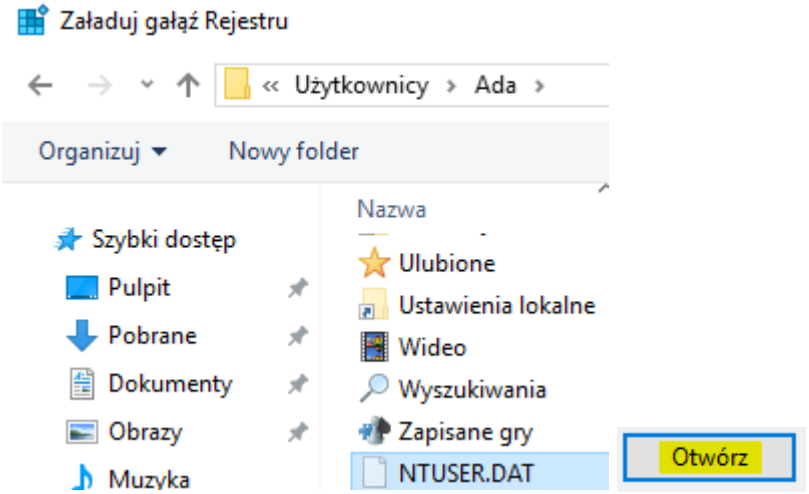
System – klucz zawiera informacje dotyczące sposobu uruchamiania systemu oraz lokalizacji plików systemowych.

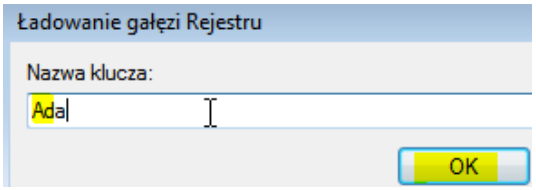
7. W poddrzewie HKU sprawdź i zapisz w zeszycie co zawiera podklucz

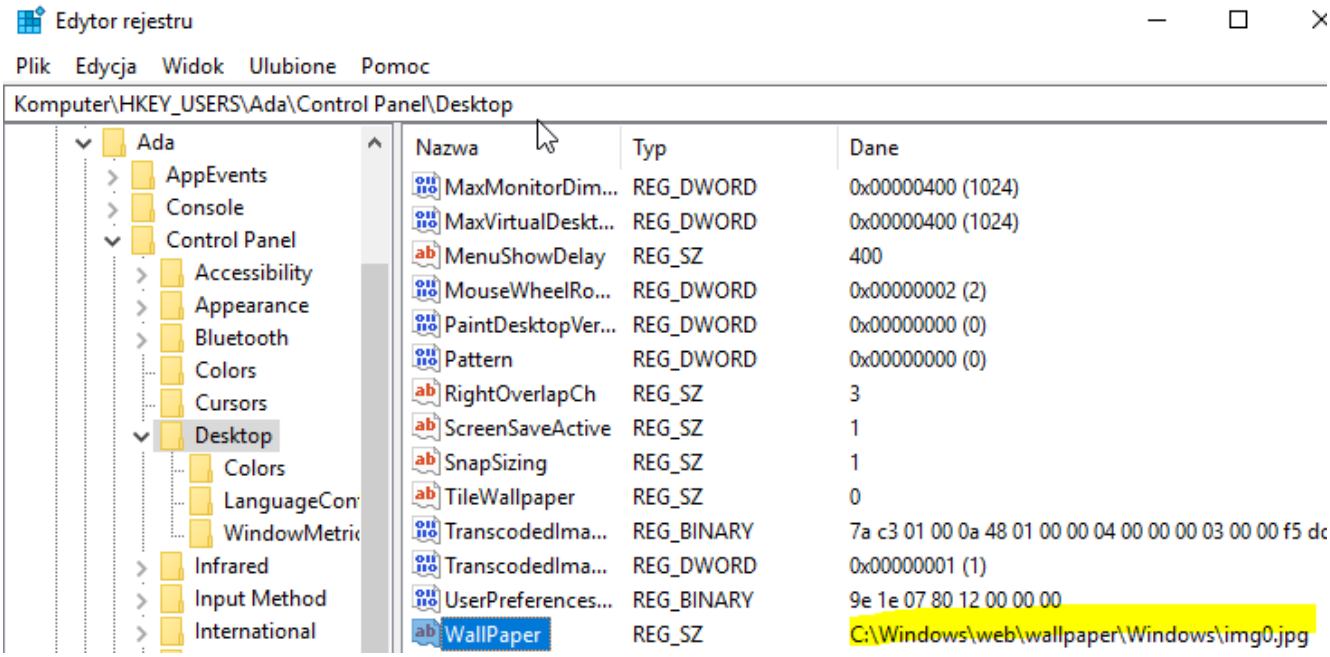
- .Default, zawiera zestaw domyślnych ustawień, które są wykorzystywane, jeśli użytkownik nie ma jeszcze skonfigurowanego profilu.
- konta Administrator.

8. Utwórz nowego użytkownika Ada, zaloguj się do niego i wyloguj, wróć do konta administratora (PC).
9. Sprawdź, czy został utworzony nowy klucz. W celu sprawdzenia czy został utworzony nowy klucz załaduj gałęzi użytkowania Ada: Zaznacz klucz jak poniżej HKEY_USERS

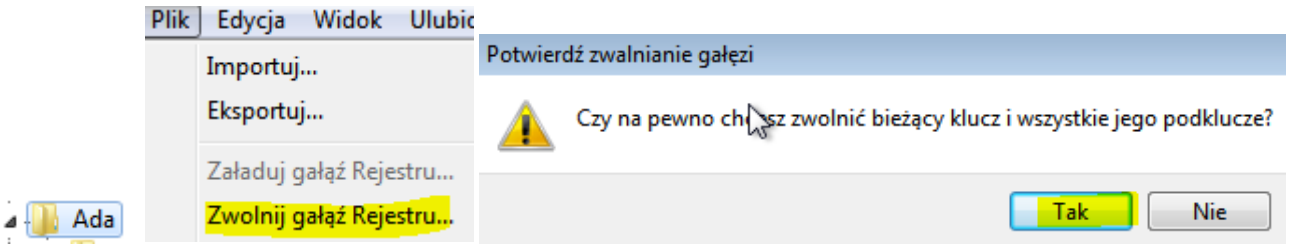








W celu zwolnienia gałęzi użytkowania Ada:



Powód – łatwiej jest wprowadzić zmiany w Podkluczu HKCU niż próbować odnaleźć identyfikator bezpieczeństwa aktualnie zalogowanego użytkownika.

10. Sprawdź i zapisz w zeszycie co zawiera Poddrzewo HKEY_CURRENT_CONFIG (HKCC) zawiera informacje o aktualnie używanym profilu sprzętowym oraz o urządzeniach sprzętowych generowane podczas uruchamiania systemu Windows. To poddrzewo jest jedynie wskazaniem do klucza w drzewie HKLM: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Hardware Profiles\Current.