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

<u> Ćwiczenie dla Windows 10</u>

W tym ćwiczeniu zweryfikujesz budowę rejestru.

1. Ustaw opcje folderów jak poniżej

🀂 l 📝 🛄 🗸	Eksplorator plików	_	
Plik Narzę	ędzia główne Udostępnianie Widok		-=
Okienko nawigacji + Okienka	Image: Signal state is in the image	W Ukryj wybran elementy wanie	e <mark>Opcje</mark>
Opcje folderó	ýw -		
Ogólne Wide	ok Wyszukiwanie		
Widoki fol	Ideru Możesz zastosować ten widok (taki jak Szczegóły lub Ikony) do wszystkich folderów tego typu. Zastosuj do folderów Resetuj foldery		
Ustawienia Prz Uk Uk Uk Uk Uk Uk Uk Uk Uk Uk	zaawansowane: zywróć poprzednie okna folderów po zalogowaniu ryj chronione pliki systemu operacyjnego (zalecane) ryj konflikty scalania folderów ryj puste dyski ryj rozszerzenia znanych typów plików (ryte pliki i foldery) Nie pokazuj ukrytych plików, folderów ani dysków) Pokaż ukryte pliki, foldery i dyski uchom okna folderów w osobnych procesach tyj Kreatora udostępniania (zalecane) tyj pól wyboru do zaznaczania elementów		
<	Zastosuj		

- 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_USERS5. 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.

📑 Edytor rejestru – 🗆 🗙						×		
Plik Edycja Widok Ulubione Pomoc								
Komputer\HKEY_USERS\S-1-5-24-1309335599-181271987-4287773119-1001\Volatile Environment								
🗸 📙 S-1-5-19	, 1	^	Nazwa	Тур	Dane			
> 🔤 AppE	vents		ab (Domyślna)	REG_SZ	(wartość	f nie ustale	ona)	
> Cons	ole		ab APPDATA	REG SZ	C:\Users	;\PC\App[Data\F	Roamii
> Cont	rol Panel		ab HOMEDRIVE	REG SZ	C:			
Envir	onment		ab HOMEPATH	REG SZ	\Users\F	PC O		
				REG SZ	C:\Users	Appl PC\Appl	Data\I	ocal
> Keyb	oard Layout		ab LOGONSERVER	REG SZ	\\DESKT	OP-BKDB	25G	
> Softv	vare			REG SZ	DESKTO	P-BKDB2S	G	
> Syste	m			REG SZ	DESKTO	D_BKDB2S		
> \$-1-5-20				PEG S7	DESKTO	F-DRDD23	0	
× <u>S-1-5-2</u>	-1309335599-1812/198/-428///3119-10	-		REG_3Z	PC C\U	ADC.		
> Appl	vents		USERPROFILE	REG_SZ	C:\Users	(PC		
> Cons	ole							
> Cont	rol Panel							
- Envir	onment							
	2							
> 🔤 Keyb	oard Layout							
> Print	ers							
> Softv	vare							
> Syste	m							
> <mark>Volat</mark>	ile Environment							

Istnieje grupa kluczy, które tworzy system na każdym komputerze.

5. Sprawdź i zapisz w zeszycie co zawierają klucze:

AppEvents – klucz zawiera <mark>wpisy wartości zdarzeń aplikacji, takie jak dźwięki powiązane z</mark> 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 <mark>wpisy wartości reprezentujące ustawienia Panelu Sterowania systemu</mark> 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 – <mark>wpisy wartości tego klucza odpowiadają ustawieniom wszystkich aplikacji zdefiniowanych</mark> 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 – <mark>klucz zawiera informacje dotyczące sposobu uruchamiania systemu oraz lokalizacji plików systemowych</mark>.

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

G	Plik	Edycja	Widok	Ulubio	
	3	Importuj			
		Eksportu	j		
HKEY_USERS		Załaduj g	jałąź Reje	stru	
📑 Załaduj gałąź Rejestru					

← → · ↑ 📙 « Uż		
Organizuj 👻 🛛 Nowy fo	lder	
 Szybki dostęp Pulpit Pobrane Dokumenty Obrazy Muzyka 	Nazwa Ulubione Ustawienia lokalne Wideo Wyszukiwania Zapisane gry NTUSER.DAT	Otwórz
Ładowanie gałęzi Rejestru		
Nazwa klucza: <mark>Ad</mark> al <u>I</u>	ОК	

🔡 Edytor rejestru

Plik Edycja Widok Ulubione Pomoc

Komputer\HKEY_USERS\Ada\Control Panel\Desktop					
V Ada	^	Nazwa 🕏	Тур	Dane	
> AppEvents		👪 MaxMonitorDim	REG DWORD	0x00000400 (1024)	
> Console		100 MaxVirtualDeskt	REG DWORD	0x00000400 (1024)	
🗸 📙 Control Panel		ab MenuShowDelay	REG SZ	400	
> Accessibility		20 MoureWheelPo		0,0000002 (2)	
> Appearance			REG_DWORD	0.00000002 (2)	
> Bluetooth		PaintDesktopver	REG_DWORD	0x0000000 (0)	
Colors		100 Pattern	REG_DWORD	0x0000000 (0)	
- Cursors		RightOverlapCh	REG_SZ	3	
🗸 📙 Desktop		ScreenSaveActive	REG_SZ	1	
- Colors		ab SnapSizing	REG_SZ	1	
		ab TileWallpaper	REG_SZ	0	
	(👪 TranscodedIma	REG_BINARY	7a c3 01 00 0a 48 01 00 00 04 00 00 03 00 00 f5 dc	
> Infrared		🐯 TranscodedIma	REG_DWORD	0x00000001 (1)	
> 📙 Input Method		🕫 UserPreferences	REG_BINARY	9e 1e 07 80 12 00 00 00	
> 📙 International		ab WallPaper	REG_SZ	C:\Windows\web\wallpaper\Windows\img0.jpg	

W celu zwolnienia gałęzi użytkowania Ada:

	Plik	Edycja Widok Ulubic				
		Importui	Potwier	dź zwalnianie gałęzi		
	Eksportuj		Czy na pewno ch sz zwolnić bieżący klucz i wszystkie jego po			
🔺 🚺 Ada		Załaduj gałąź Rejestru <mark>Zwolnij gałąź Rejestru</mark>		Tak Nie		

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.