

RegPod V2.0 – Remote Data Access in Registry Base

Miloš M. Marinović¹, Nenad V. Micaković¹

Abstract - From time to time, there is a need to collect some information from a number of computers, like version of program packages or some information from registry database. This information is needed for some required system change or reports collecting. Modified solution of RegPod application, on very simple way shows required information, and based on that, user can plan further actions and solutions of given tasks. Comparing to Microsoft Regedit application, RegPod can collect data from multiple computers more then 20 times faster. Also, there are a few new options - program can be run with differential credentials and added HKDD registry hive.

Keywords - Registry, data collection, RegPod v2.0

I. INTRODUCTION

Registry database can be defined as central hierarchical database used in Microsoft Windows 98, Windows CE, Windows NT, and Windows 2000 used to store information that is necessary to configure the system for one or more users, applications and hardware devices [3].

The Registry contains information that Windows continually references during operation, such as profiles for each user, the applications installed on the computer and the types of documents that each can create, property sheet settings for folders and application icons, what hardware exists on the system, and the ports that are being used. The Registry replaces most of the text-based .ini files that are used in Windows 3.x and MS-DOS configuration files, such as the Autoexec.bat and Config.sys. Although the Registry is common to several Windows operating systems, there are some differences among them.

A registry hive is a group of keys, sub keys, and values in the registry that has a set of supporting files that contain backups of its data. The supporting files for all hives except HKEY_CURRENT_USER are in the %SystemRoot%\System32\Config folder on Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, and Windows Vista. The supporting files for HKEY_CURRENT_USER are in the %SystemRoot%\Profiles\Username folder. The file name extensions of the files in these folders indicate the type of data that they contain. Also, the lack of an extension may sometimes indicate the type of data that they contain.

Predefined keys that operating system uses are [1,2]:

HKEY_CURRENT_USER

Contains the root of the configuration information for the user who is currently logged on. The user's folders, screen colors, and Control Panel settings are stored here. This information is associated with the user's profile. This key is sometimes abbreviated as "HKCU".

HKEY_LOCAL_MACHINE

Contains configuration information particular to the computer (any user). This key is sometimes abbreviated as "HKLM".

HKEY_CLASSES_ROOT

The information that is stored here makes sure that the correct program opens when you open a file by using Windows Explorer. This key is sometimes abbreviated as "HKCR".

HKEY_CURRENT_CONFIG

Contains information about the hardware profile that is used by the local computer at system startup.

HKEY_DYN_DATA

Can be found on Windows 95/98/ME operating systems and contains information about Plug i Play hardware components.

II. PROGRAM USAGE

Figure 1 shows main form of program package RegPod version 2.0. In addition to version 1.0, this version brings redesigned user interface with a new look and feel and makes it more intuitive, and simpler for use. Below menu line, are few fields for required data and start button.



Fig. 1. Main form

¹ ProCredit Bank A.D., Svetozara Markovića 10, 18000 Niš, Serbia

Also, in this version of program package, menu line contains another item - 'Logon as...'. There can be chosen username and password, to impersonate a user under which credentials the registry database is to be accessed. Options are 'Current user' and 'Different user'. Dialog is shown on figure 2.

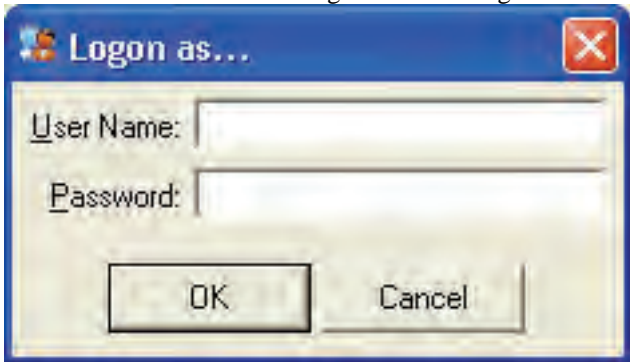


Fig. 2. Username and password input form

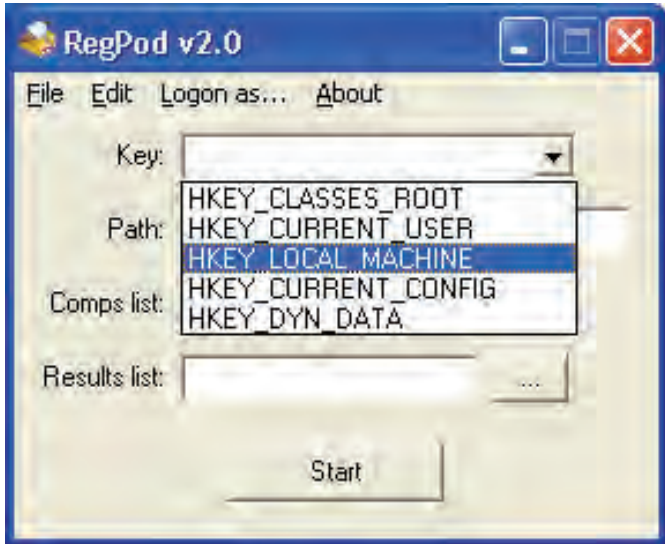


Fig. 3. Top level registry hives



Fig. 4. Path to key value

Figure 3 shows four fields for data input, that must be entered before required data collection. First field is combo box, which consists one of five top level registry. After top level registry key is choused, in 'Path' field, user has to enter rest of path to key which value has to be checked. This is shown on figure 4. After key path is entered, path to computers list is needed. That can be achieved on two ways. In 'Comps list' field, user can type location to list or by pressing button, choose file with list of computers. File is regular text file that can be opened and changed with any textual editor, like Notepad.exe. This list is shown on figure 5.

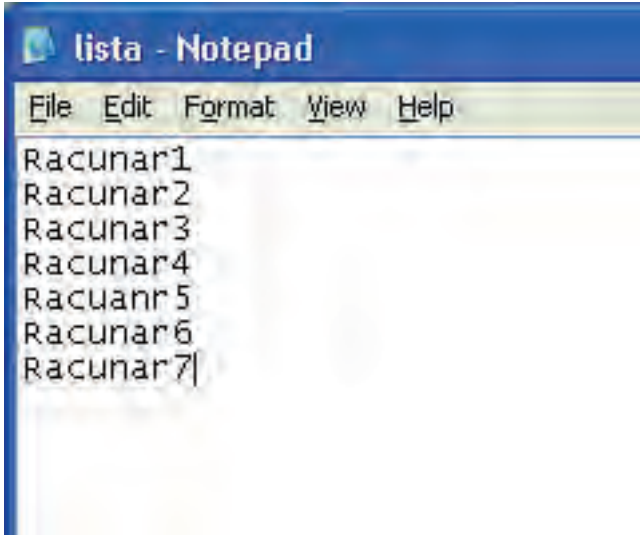


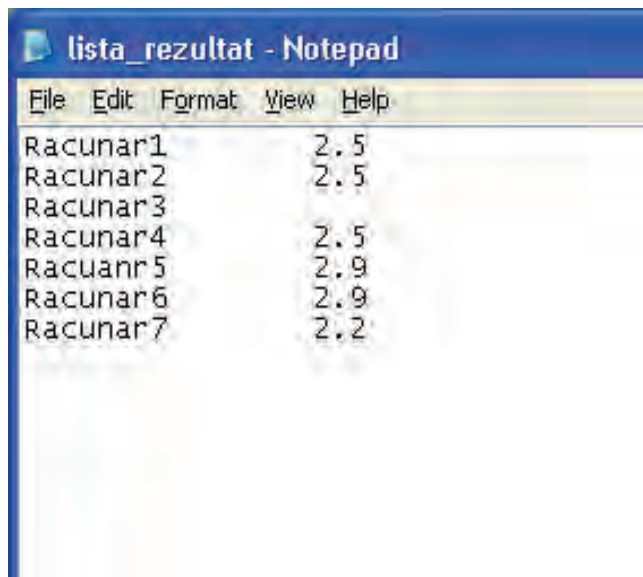
Fig. 5. List of computers

After list of computers is finished, in the field 'Results list' automatically will be created path to the list with results. Word '_rezultat' will be added to the filename of result list and then the extension which has had original file. User can change that default name of file. This is shown on figure 6. By pressing on the button 'Start', program starts with collecting data.



Fig. 6. Setting registry querying parameters: input file name which contains a list of computers to be queried and output file name which contains search results

Following is a sample of an output file created by application. It contains a list of queried computers, and registry key value searched for, in this example an application version installed on them. Now, we can easily conclude that only two computers are up-to-date, one doesn't have requested application and that all other computers have old application version installed on them. This example demonstrates that we can on a very easy and reliable way check huge number of computers in our local area network for some particular information stored in the registry database.



File	Edit	Format	View	Help
Racunar1		2.5		
Racunar2		2.5		
Racunar3				
Racunar4		2.5		
Racunar5		2.9		
Racunar6		2.9		
Racunar7		2.2		

Fig. 7. Output file: Computers list with collected data

This software package has been developed as a standard win32 application and it can be used on any Windows platform. However, regarding windows security issues there are few prerequisites to be fulfilled in order to install and use application properly. Except Regedit application, which comes with Microsoft operating systems, authors did not find similar application, which does some data collection as RegPod v2.0. Of course, that does not mean, that similar application does not exist.

User account under which credentials application is to be executed must have enough privileges to access registry database on local computer as well as on a remote computers listed in the configuration file. If this is not fulfilled when application attempts to access a registry database an error will be raised. Furthermore, if application is to be used for querying remote computers then Remote Registry service have to be started on every computer listed in a configuration file in order to provide access to registry database on a remote computer. In order to simplify application usage it's possible to query registry database on a selected computers under different user account credentials then one used for starting the application.

III. CONCLUSION

Software package RegPod v2.0 is the tool which can reduce time of data acquisitions from the Microsoft Windows registry base. This is very essentially, when it is about large systems, where is time necessary for obtaining such information and treating according to given results is very short. Comparing to Microsoft Regedit application, RegPod can collect data from multiple computers more then 20 times faster. This paper presents basic characteristic, as well as the basic form of program. Also, there are few requirements that need to be fulfilled, like started 'Remote Registry' service. Program has been developed in Visual Basic programming language and is very intuitive and simple for usage. With Microsoft Windows Regedit tools it's possible to explore registry database of one computer at the time. RegPod advantages come out with large computer networks, since unlike Regedit approach RegPod uses configuration files to setup a set of computers which registry is to be explored at once.

REFERENCES

- [1] Windows registry information for advanced users, <http://support.microsoft.com/kb/256986>
- [2] Jerry Honeycutt, *Microsoft Windows Registry Guide, Second Edition*, 08/17/2005, ISBN 9780735622180
- [3] Microsoft Press, *Microsoft Computer Dictionary, Fifth Edition*, ISBN: 0735614954
- [4] Peter Norton, *Guide to Visual Basic 6*, Sams, September 9, 1998, ISBN-10: 0672310546, ISBN-13: 978-0672310546