Registry Editor

Contents

1. About the Registry Editor . . . 2
2. How to start . . . 3
3. How to . . . 5
3.1. Open registry hive for editing . . . 5
3.2. Exit the Registry Editor . . . 10
3.3. Save hive to disk without exiting the Registry Editor . . . 11
3.4. Navigate the tree of registry keys . . . 12
3.5. Create registry key . . . 13
3.6. Rename registry key . . . 15
3.7. Delete registry key . . . 17
3.8. Create registry value . . . 19
3.9. Change registry value . . . 22
3.10. Delete registry value . . . 23
3.11. Copy or move registry value(s) between two keys via the clipboard . . . 24
3.12. Edit key class name and other properties in the raw mode . . . 25
3.13. Create or edit registry symbolic link . . . 28
3.14. Export registry key with subkeys and values . . . 30
3.15. Import registry key with subkeys and values . . . 35
3.16. Create difference report for a registry hive . . . 40
3.17. Search in a registry hive . . . 46

1. About the Registry Editor

Registry Editor is a component of Emergency Boot Kit which can be used to create, copy, rename, move, delete, export and import registry keys and values. Also it can create registry hive difference reports and perform full-text search in a registry hive.

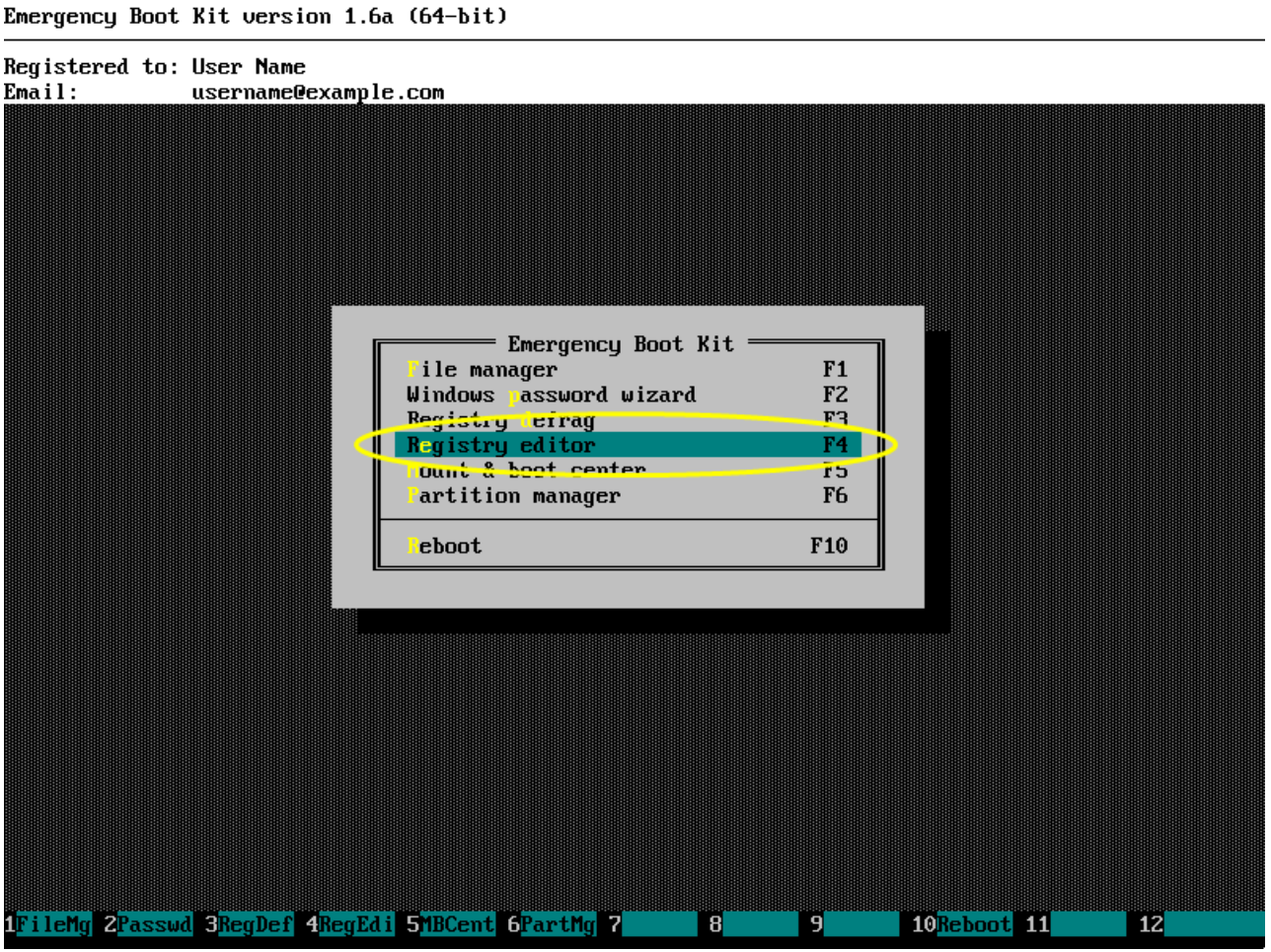
EmBootKit Registry Editor can handle registry hives created by all versions of Windows from Windows NT 4.0 to Windows 10. Original format of the registry hive is preserved after editing (not autoupgraded to the latest version as in Windows). It is able to replay (apply) registry log files to registry hives, and supports the new format of registry log files which was introduced in the Windows 8.1.

EmBootKit Registry Editor fully supports Unicode, class names, security descriptors, symbolic links, key flags and statistics and other rarely used features of Windows Registry. Export and import are supported in both formats: text (as in *regedit.exe*) and binary hive.

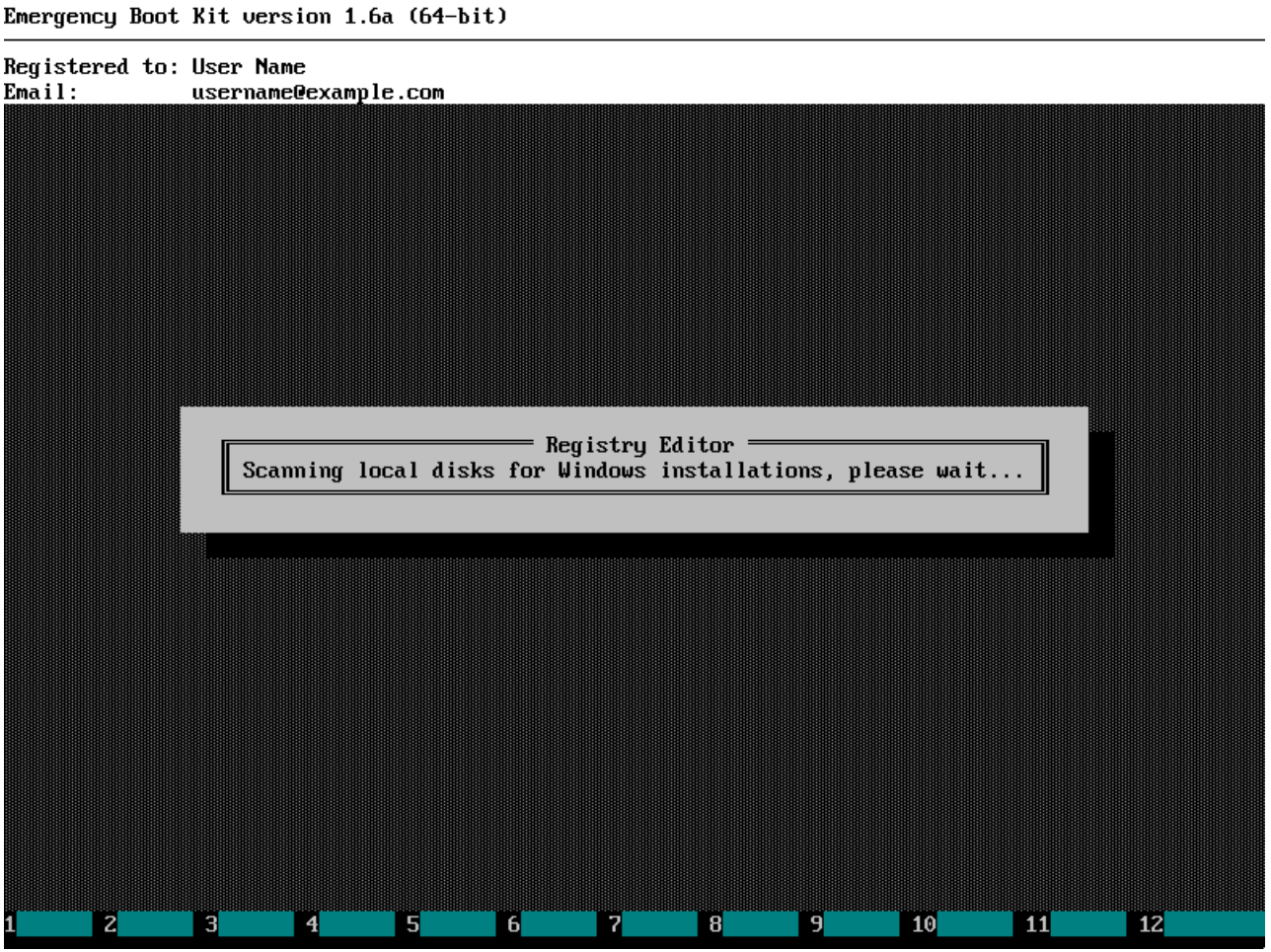
2. How to start

After booting, Emergency Boot Kit displays its main menu.

To start the Registry Editor, press the **F4** key or click mouse on *Registry editor* line.



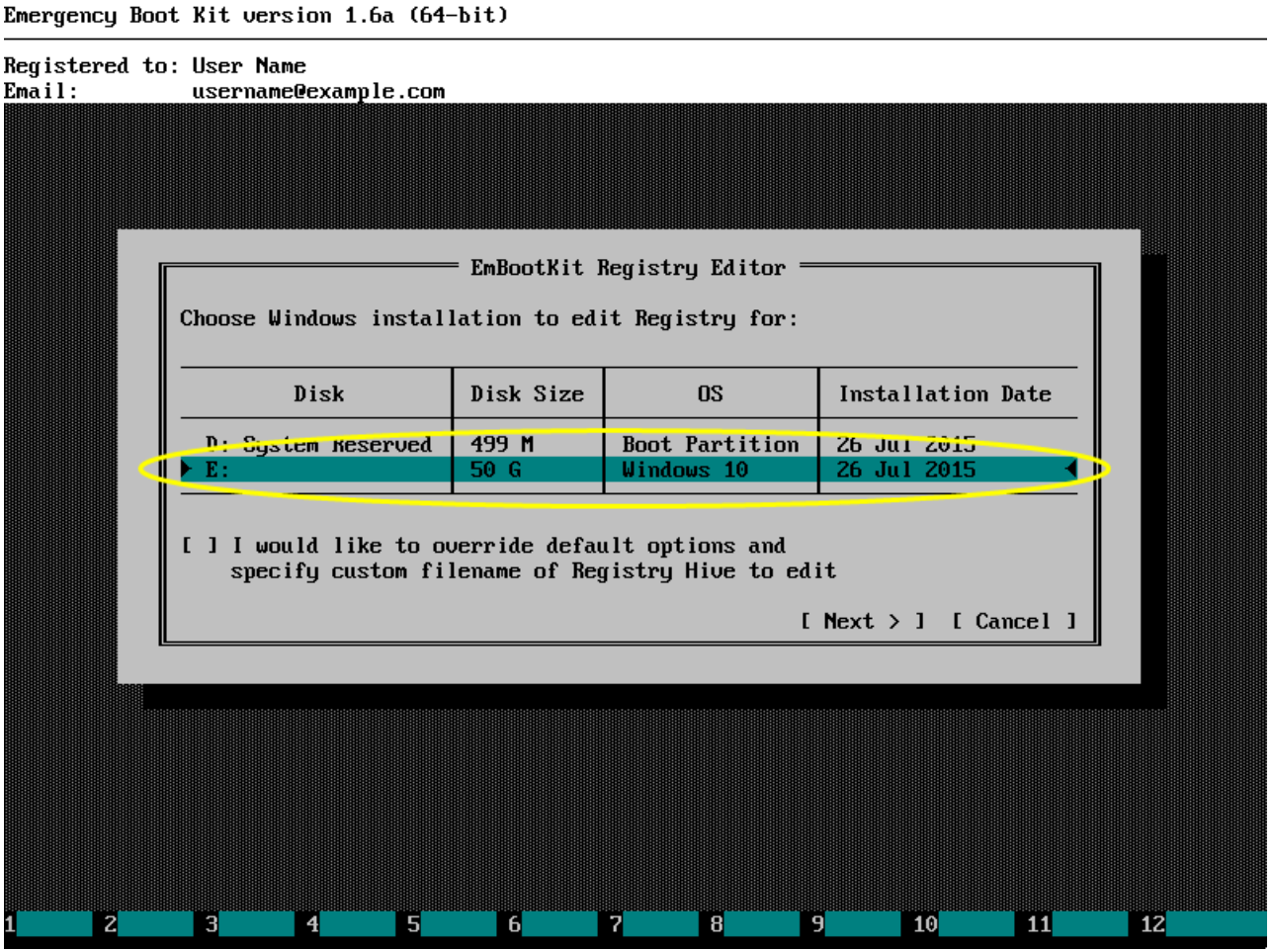
Wait while Registry Editor scans for Windows installations and registry hives. This window will automatically disappear when done.



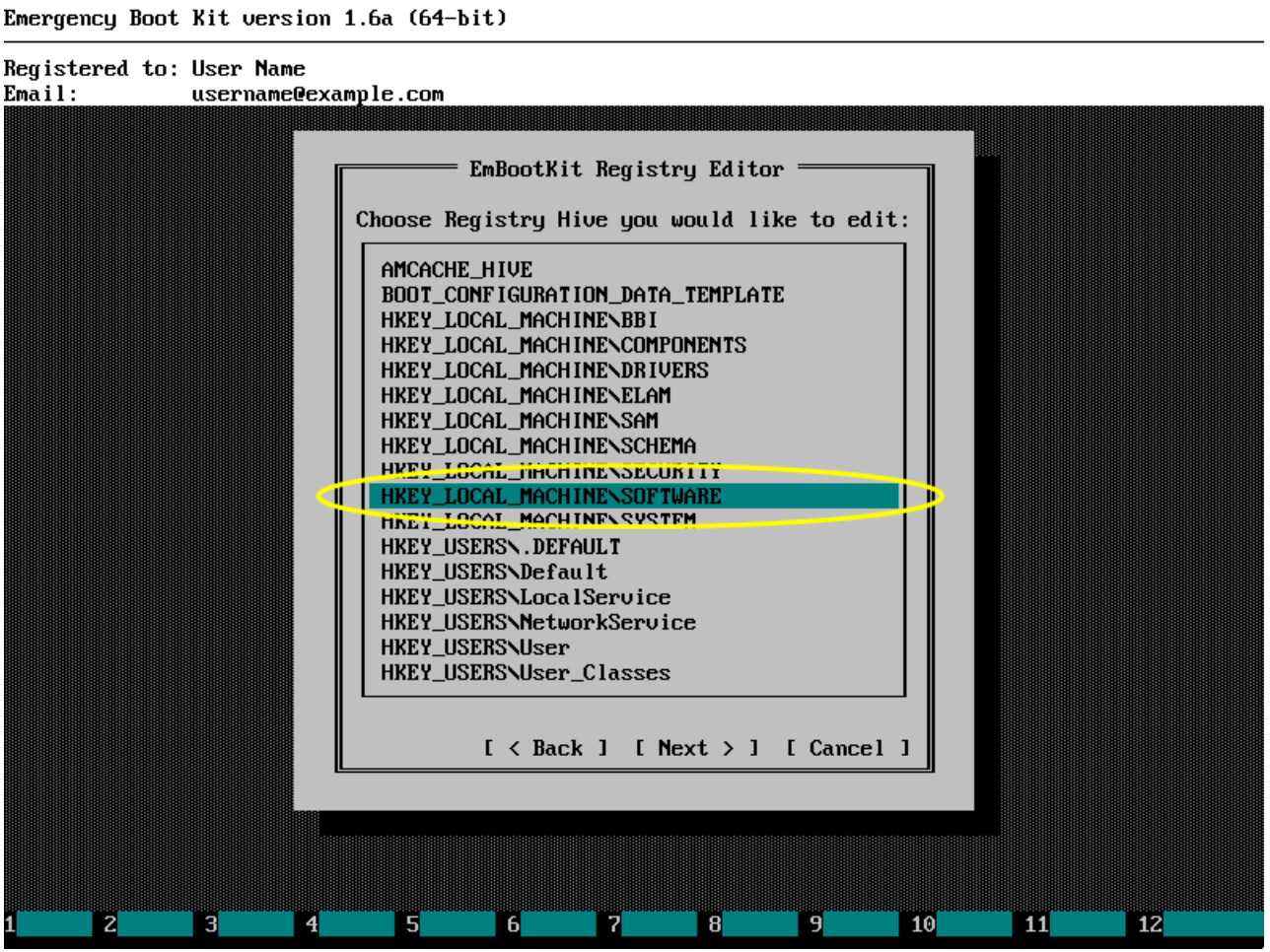
3. How to

3.1. Open registry hive for editing

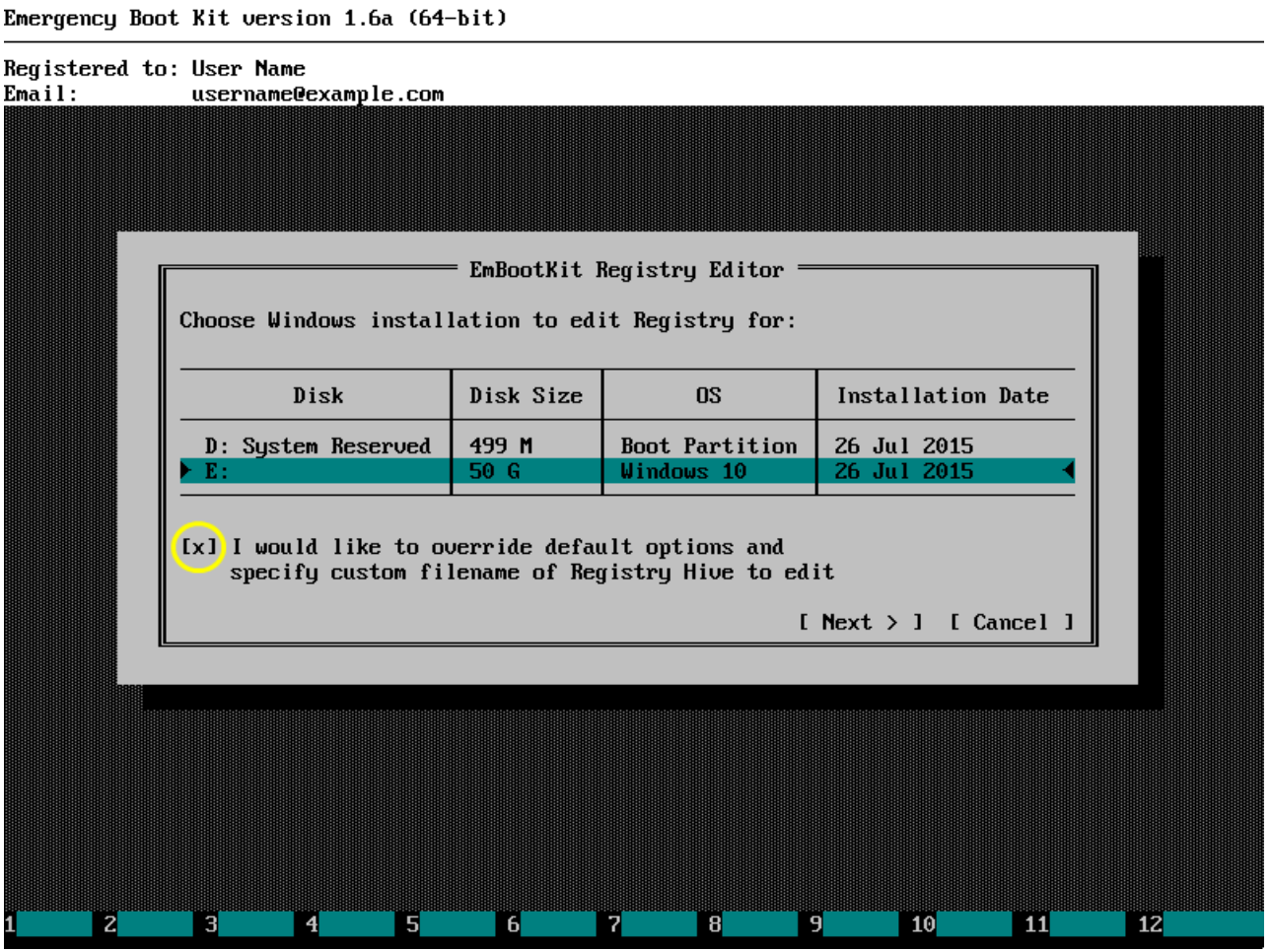
Choose OS you want to edit registry for. Boot partition has its own BCD hive which can be edited too.



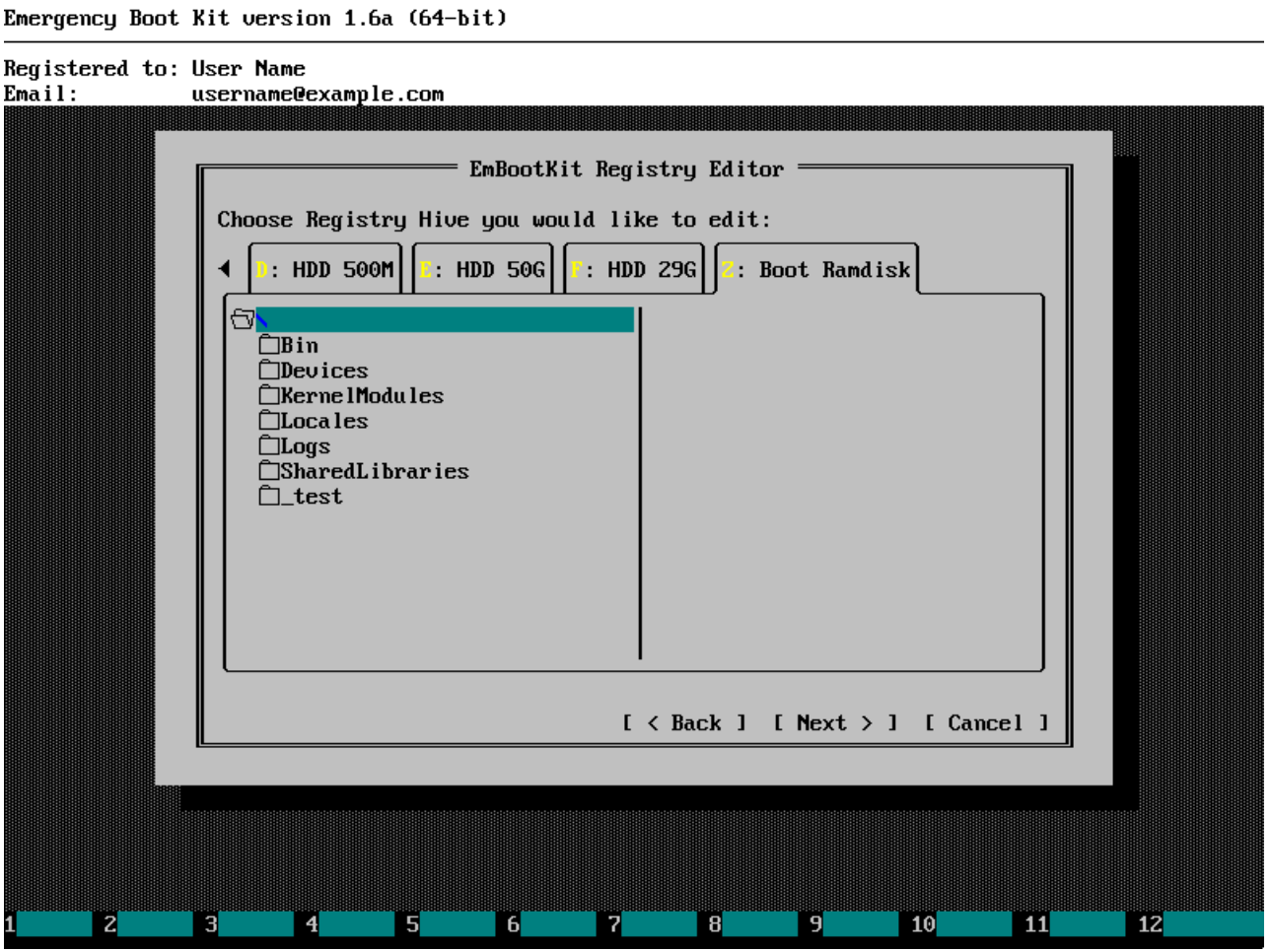
Choose registry hive you want to edit from the list. We are going to edit *HKEY_LOCAL_MACHINE\SOFTWARE* in this example.



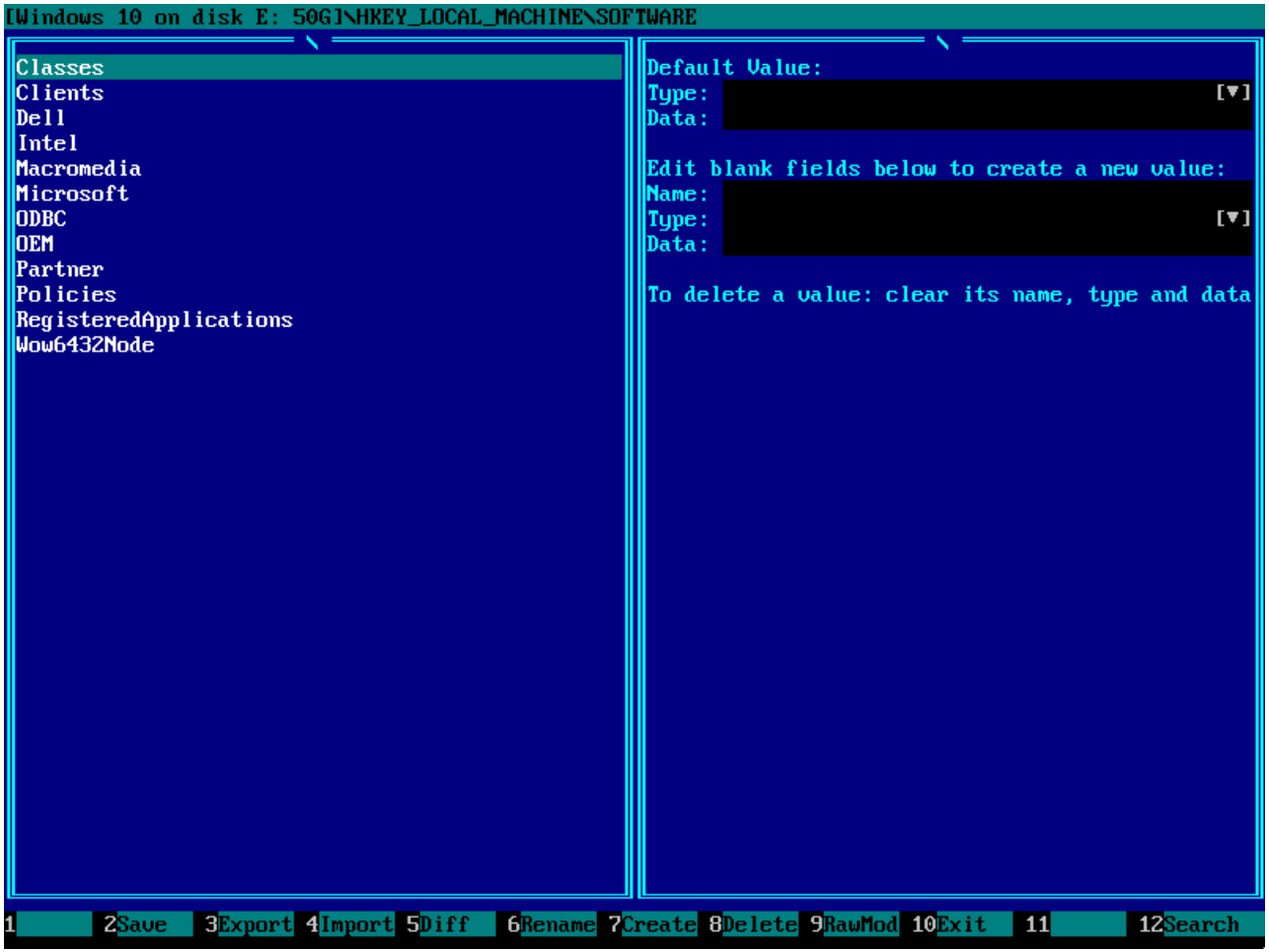
Alternatively, you can set the checkbox to override default options and specify custom filename of registry hive to edit.



Then a file open dialog will be displayed. Here, using a mouse, you can choose arbitrary location of registry hive and its log (e.g. on the USB thumbdrive).

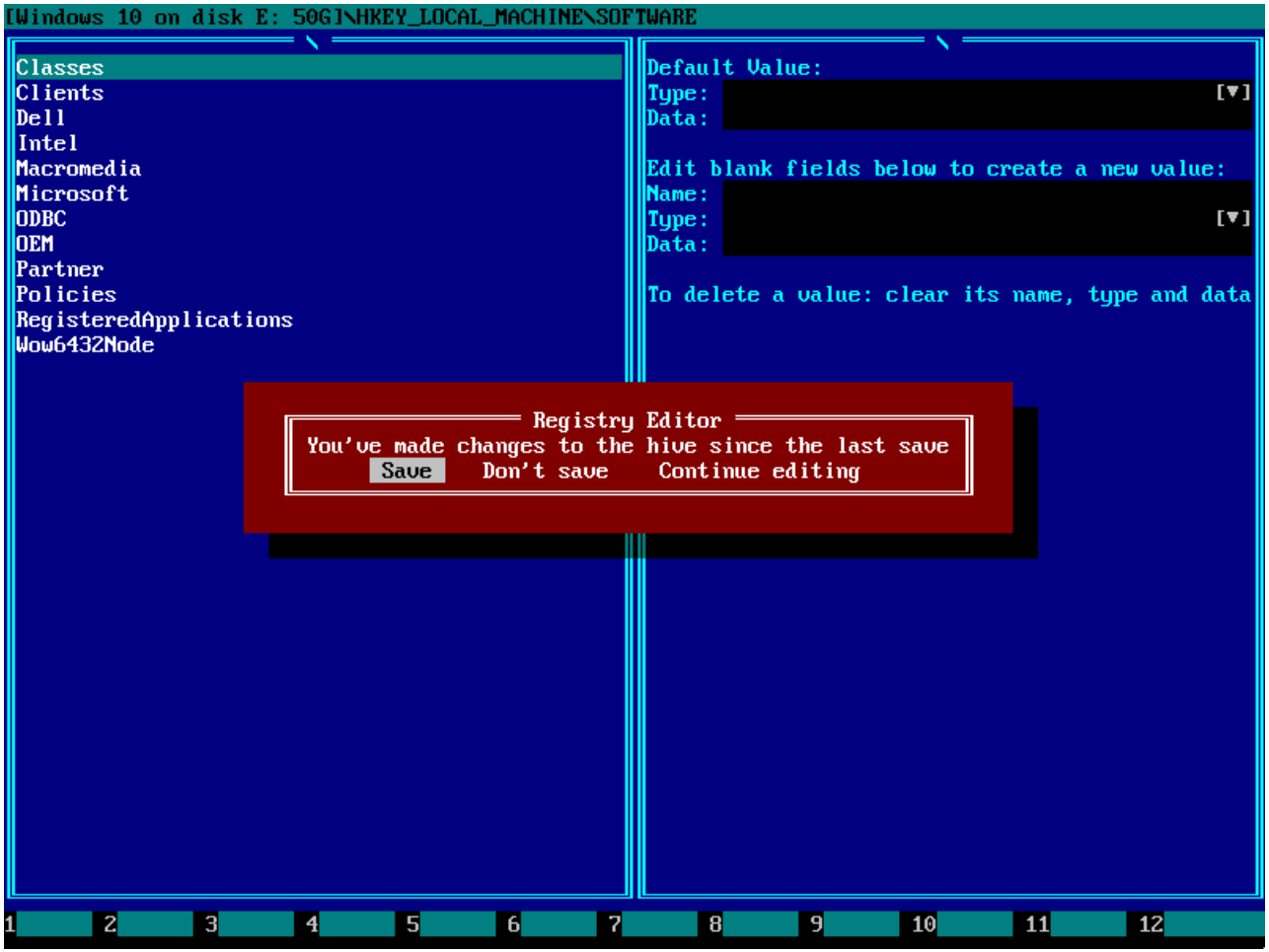


Regardless of the way registry hive was open, when Registry Editor loads it, you should see the screen like this.



3.2. Exit the Registry Editor

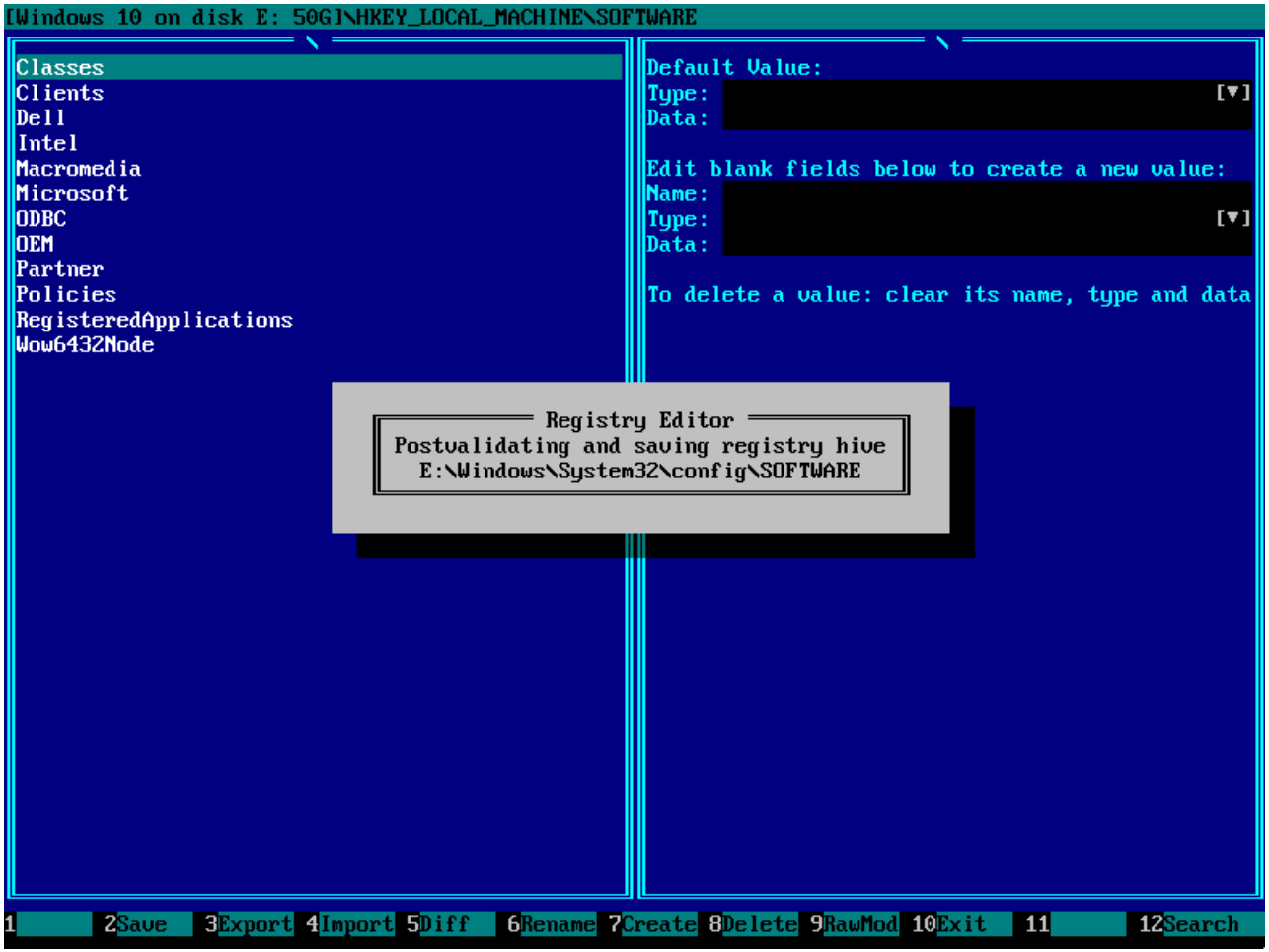
To exit the Registry Editor, press **F10** or **Esc**. If you have any unsaved changes in the registry hive, a window like this will be displayed.



3.3. Save hive to disk without exiting the Registry Editor

You may save current registry hive to disk at any moment without exiting the Registry Editor by pressing **F2**.

Postvalidation is necessary to make sure that modified registry is strictly valid. It happens in volatile memory, so if it fails, registry is not changed on disk.



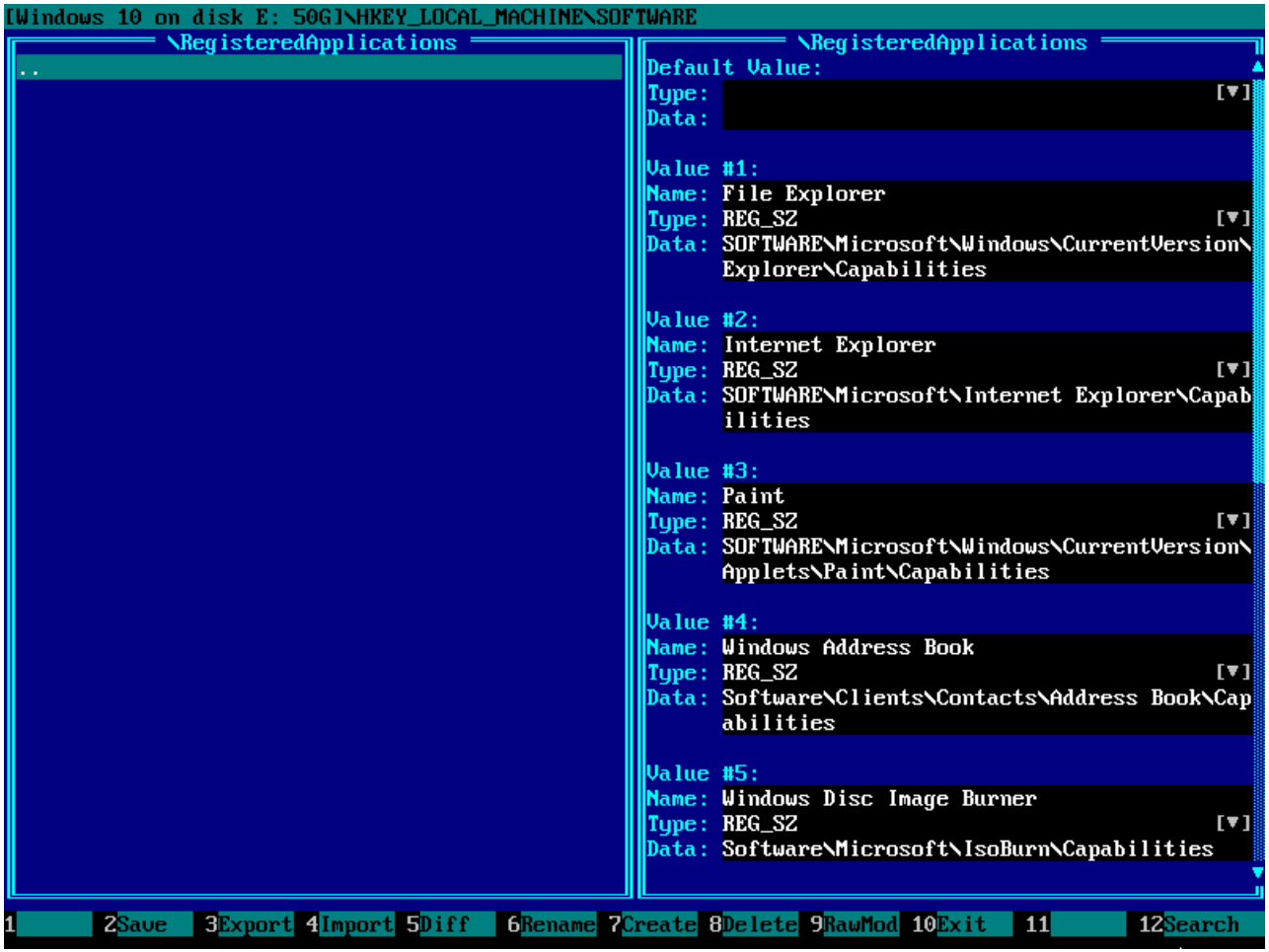
3.4. Navigate the tree of registry keys

Use ↑ and ↓ keys to move cursor between registry keys on the left panel. You may also left-click target registry key with a mouse.

Use **Enter** key or double-click the left mouse button to enter a registry key.

"**. .**" item is special: it's used to move up in the hierarchy of registry keys.

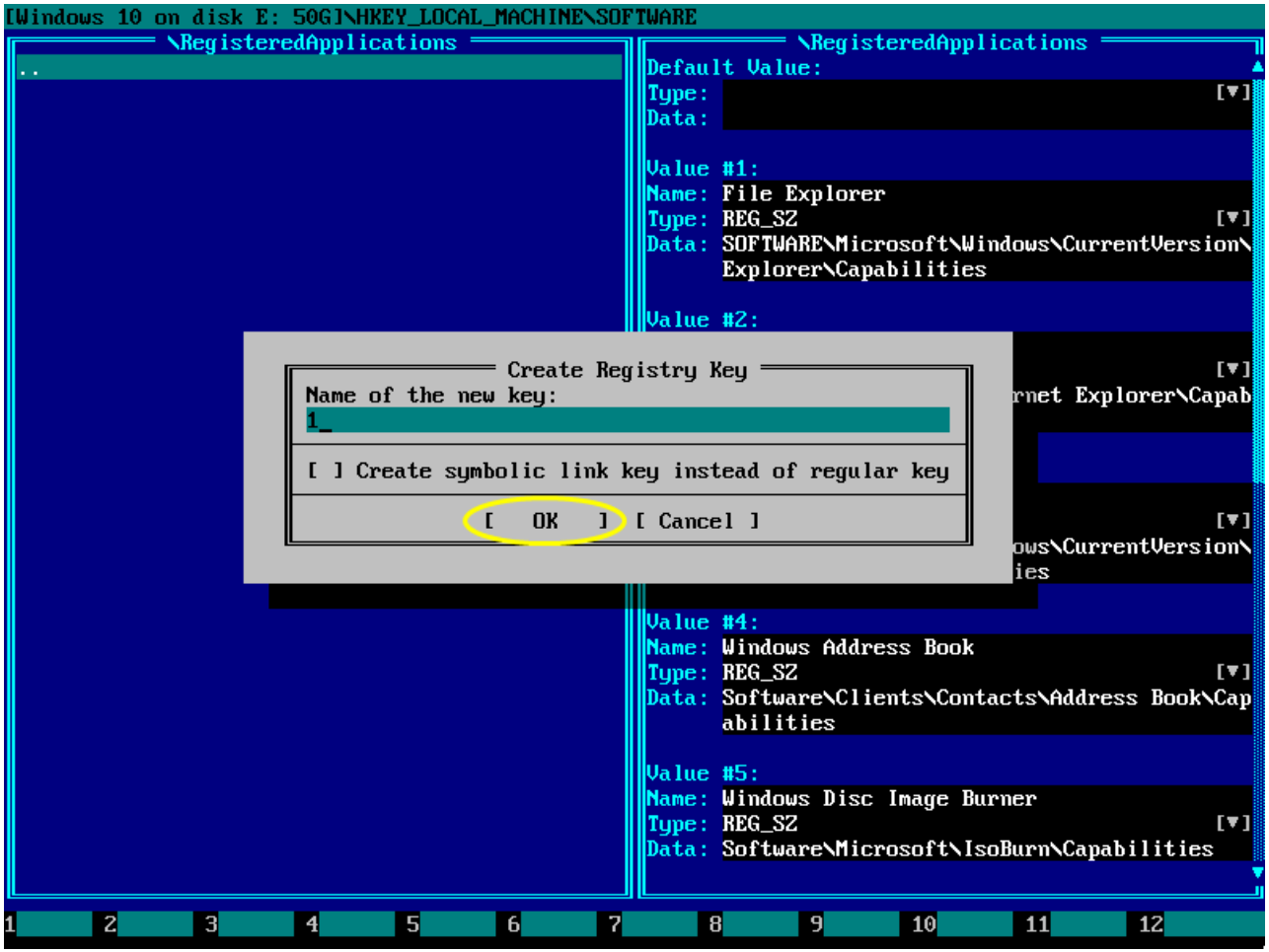
If there are too many items to fit the screen, left panel can be scrolled using **PageUp** and **PageDown** keys, or using a mouse wheel.



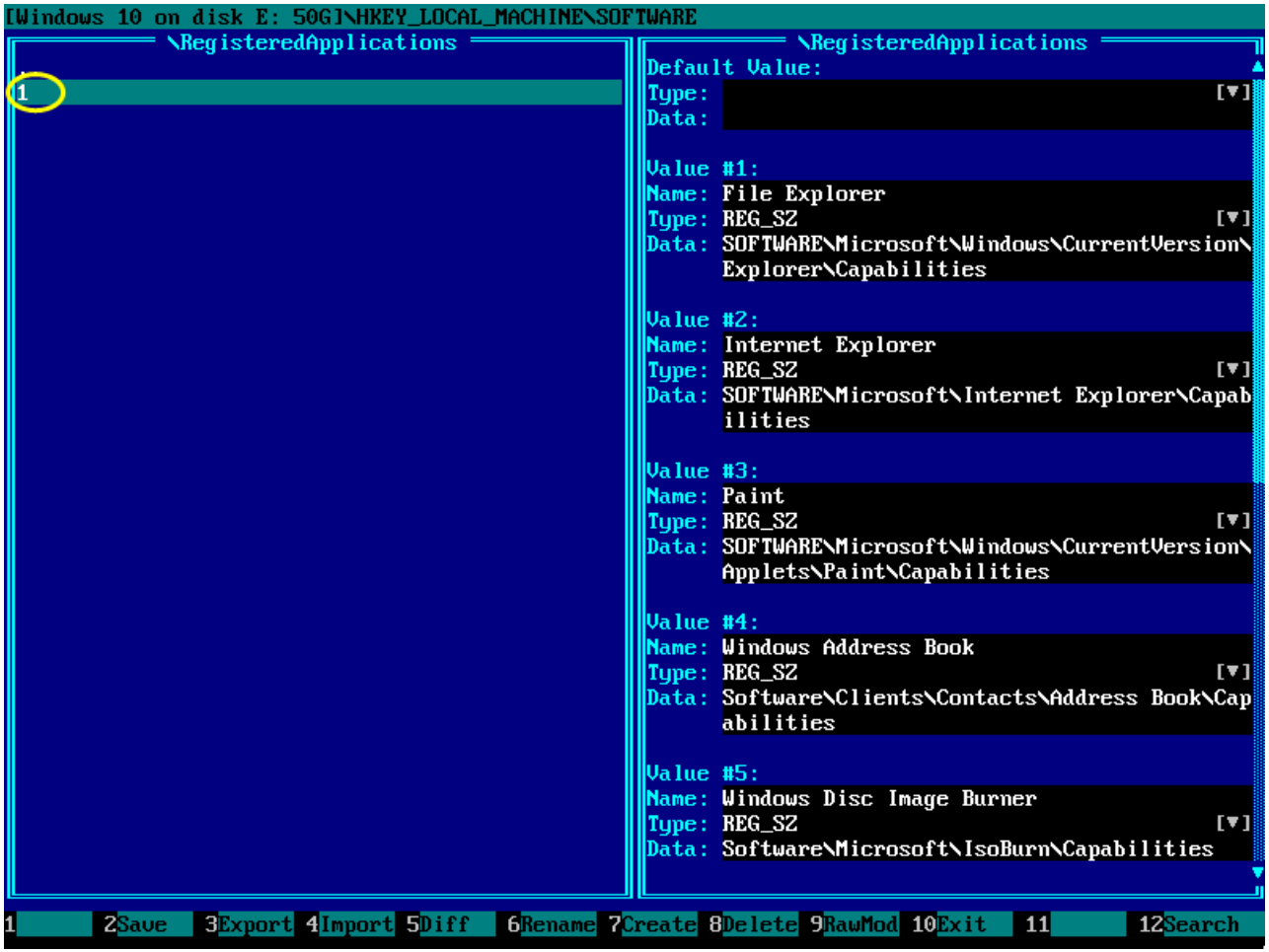
3.5. Create registry key

To create a new registry key, navigate to its parent key and press **F7**.

Then enter a name for new registry key and press **Enter** or click *OK*.



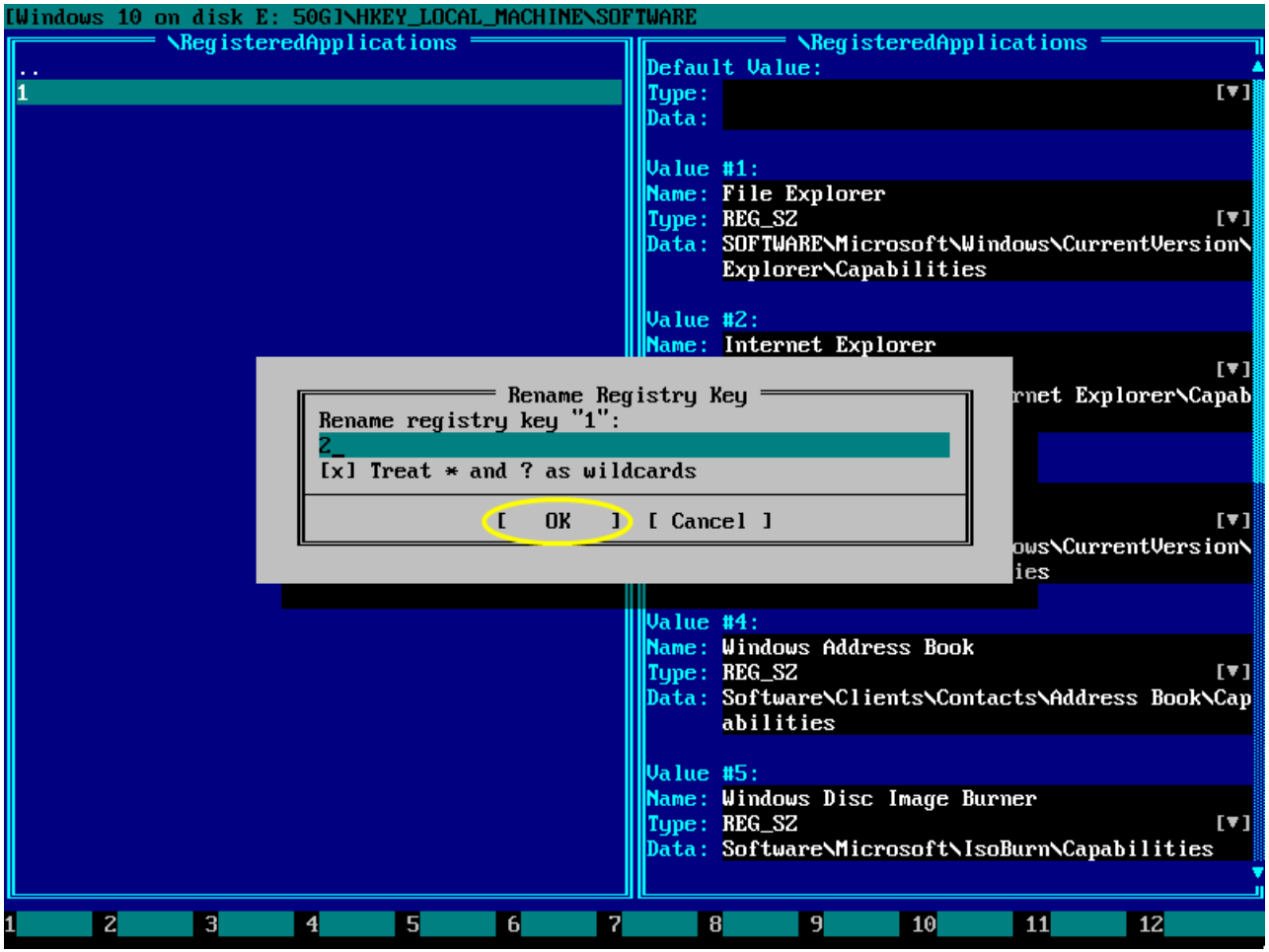
New key with specified name has been created.



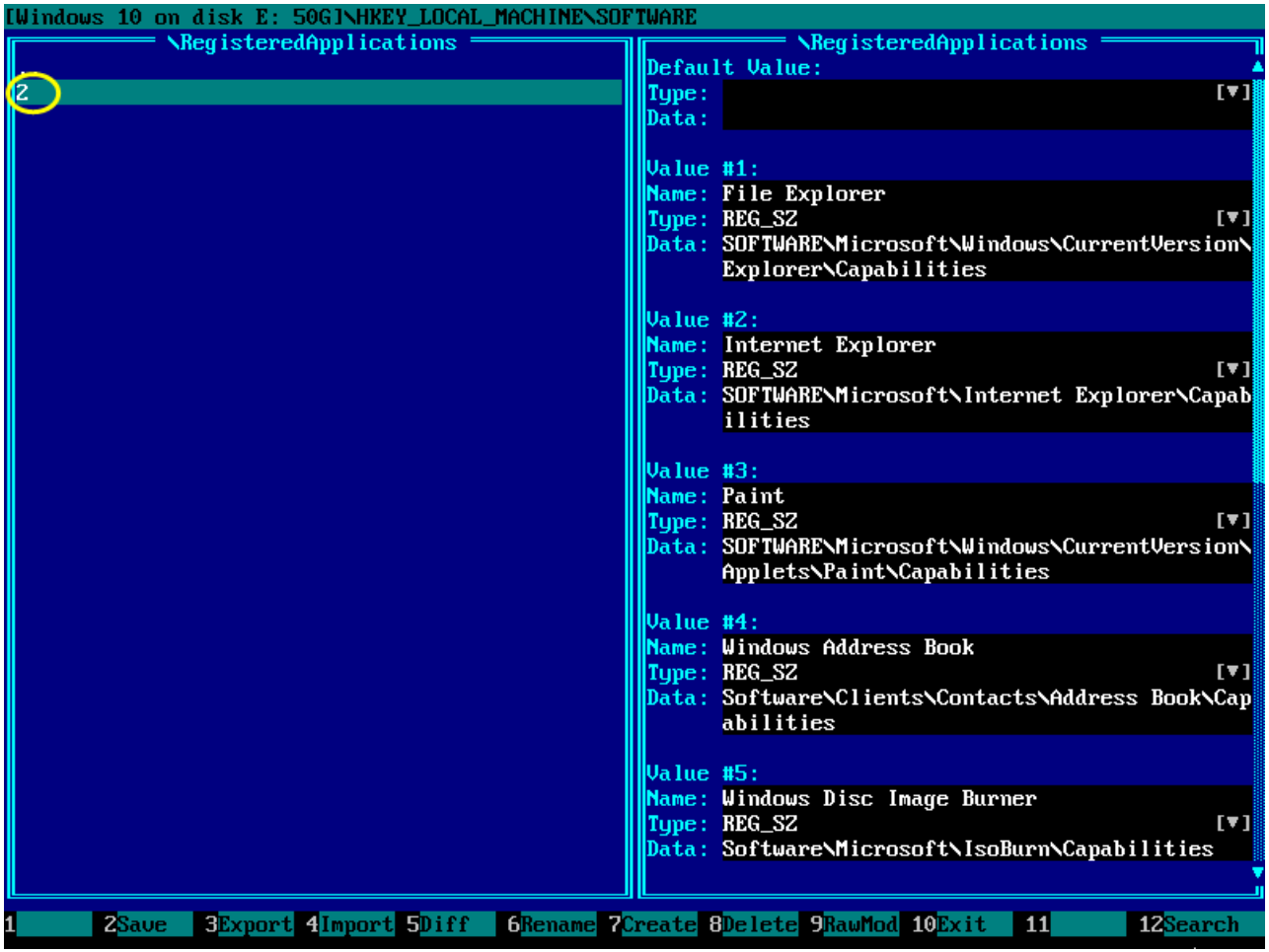
3.6. Rename registry key

To rename existing registry key, navigate to it and press **F6**.

Then enter a new name for existing registry key and press **Enter** or click *OK*.



A key has been renamed.

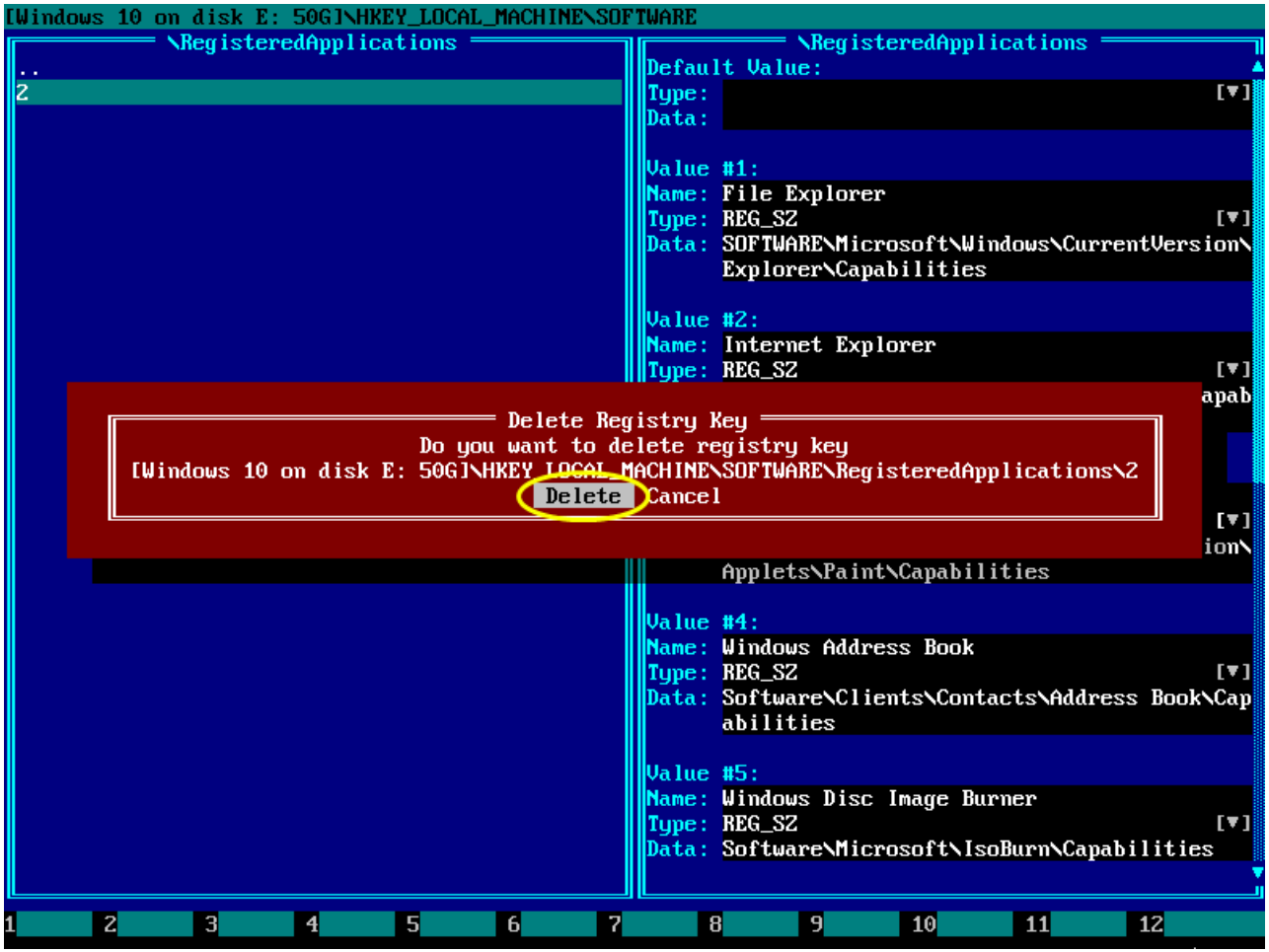


3.7. Delete registry key

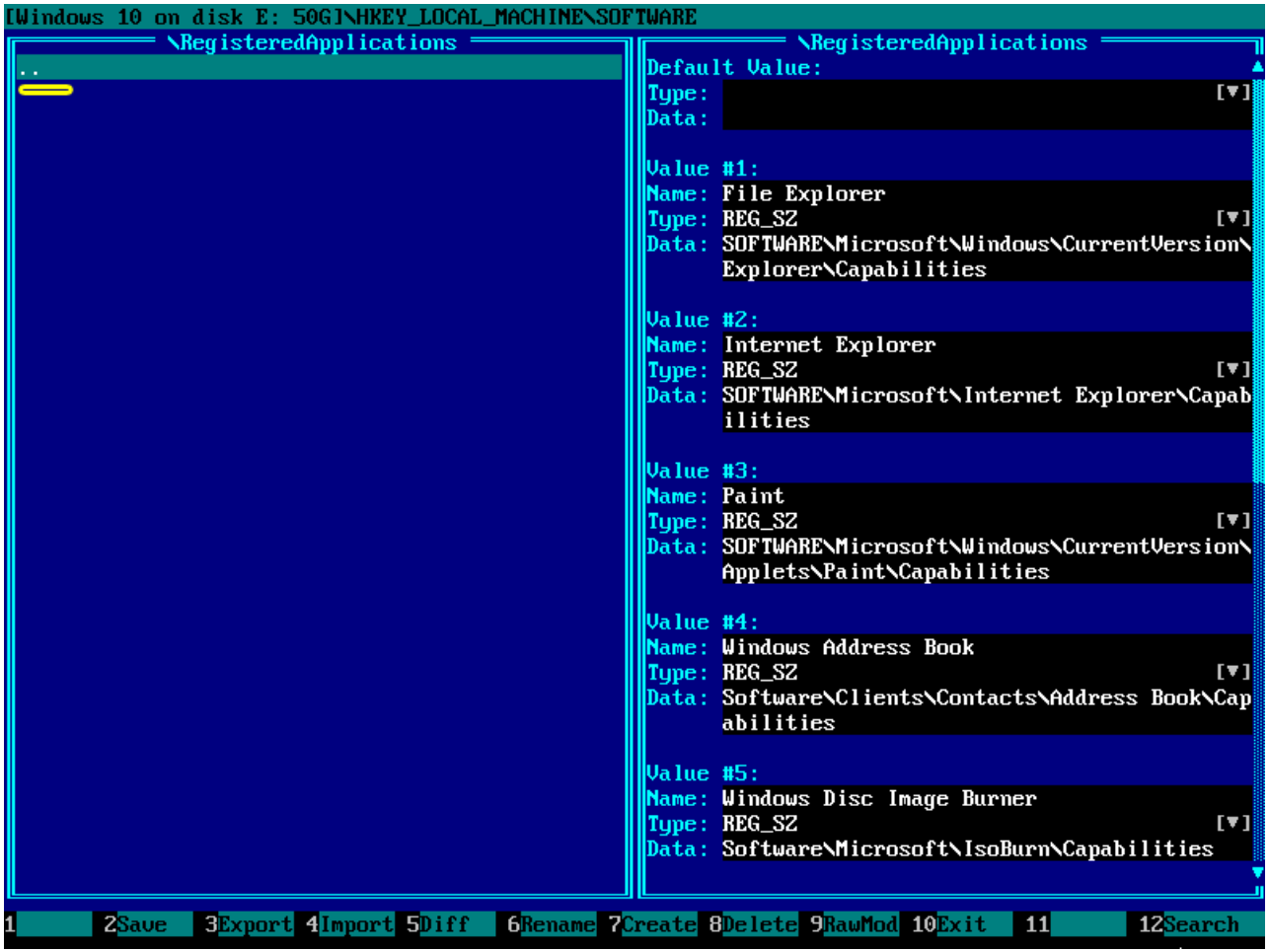
To rename existing registry key, navigate to it and press **F8**.

Confirm deletion by pressing **Enter** or clicking *OK*.

If you decided not to delete a registry key, then press **Esc** or click *Cancel*.



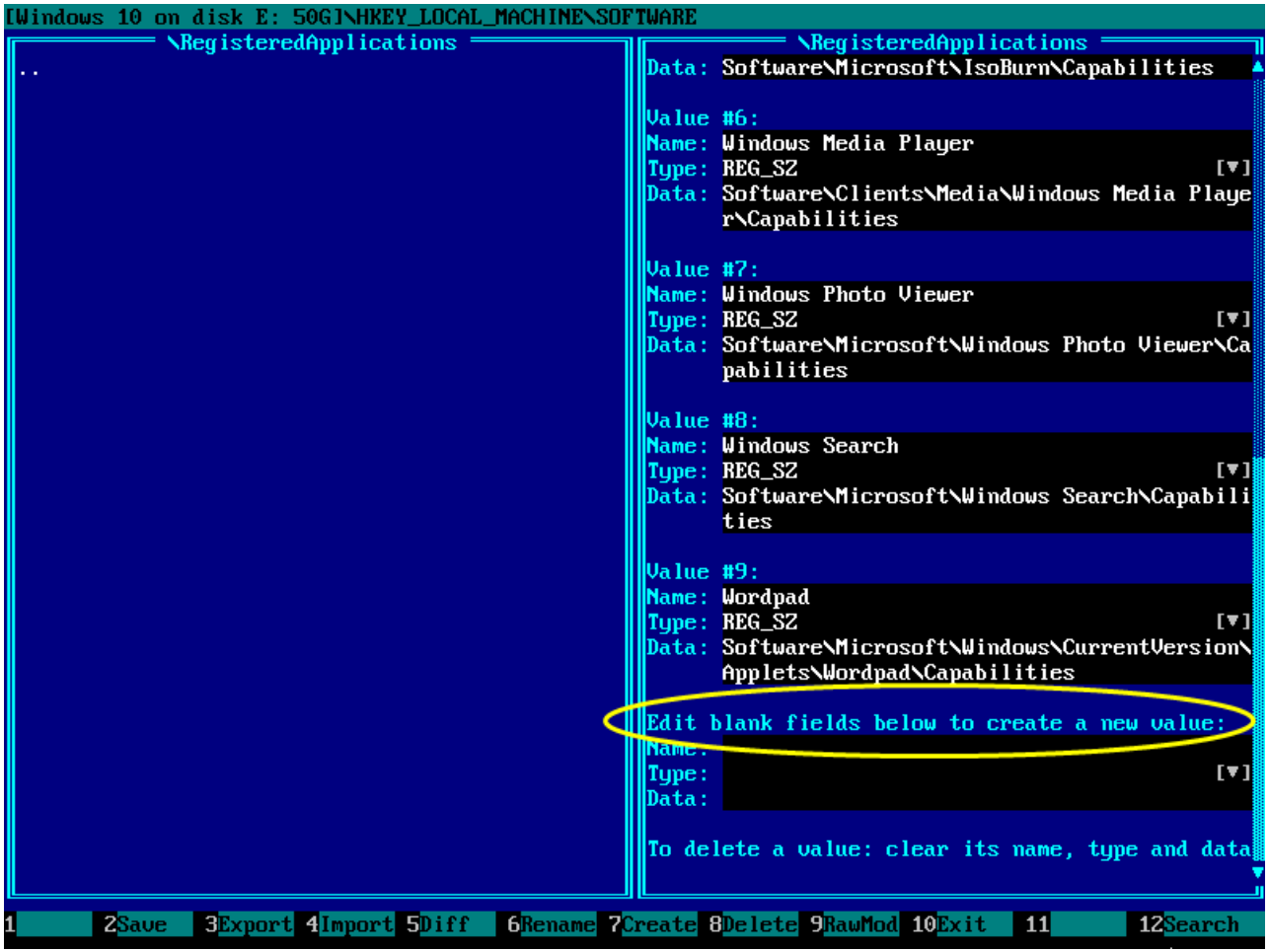
A key has been deleted.



3.8. Create registry value

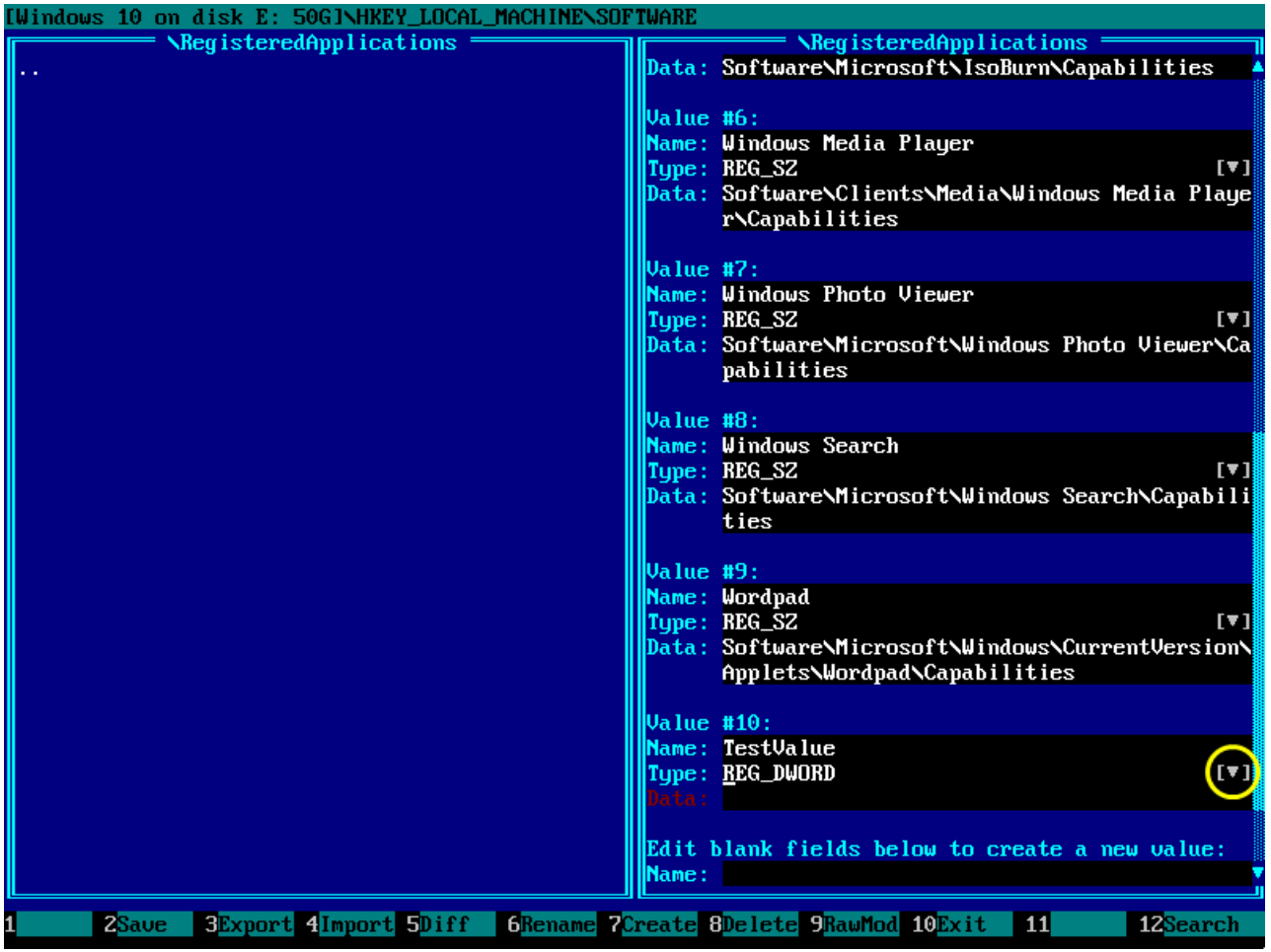
Navigate to a registry key where you want to create a new registry value.

Press **Tab** to make right panel active, or left-click it with a mouse. Then use **PageDown** key to scroll to the bottom of the screen or use a mouse wheel for the same purpose.



Enter a name of new value in the *Name:* field using normal keys like letters and numbers. Use **Backspace**, **Del**, ← and → keys if necessary.

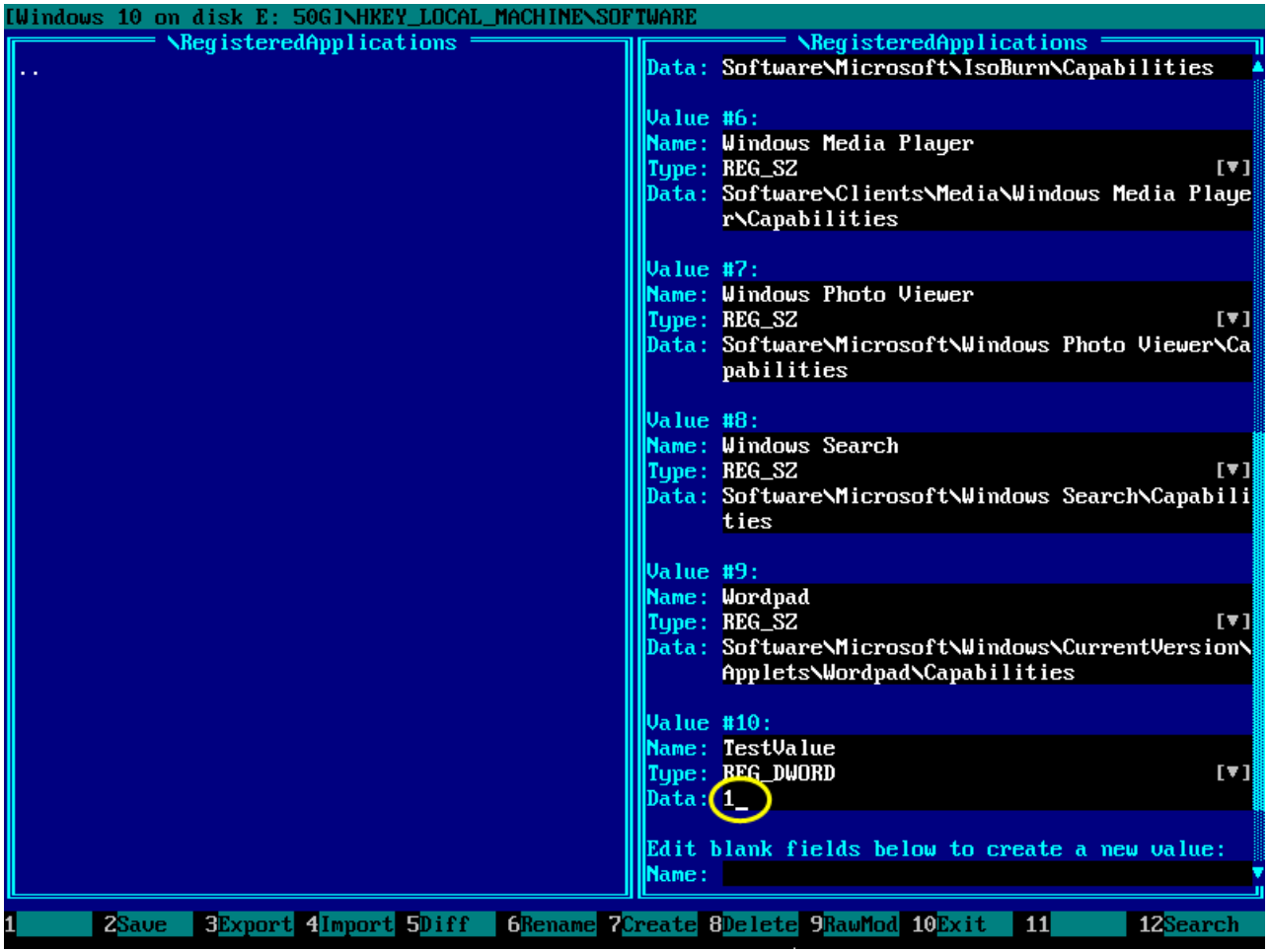
Then press ↓ key to navigate to the *Type:* field and enter a type of new registry value (*REG_DWORD* in this example) or choose it from drop-down list using a mouse.



Press ↓ key to navigate to the *Data:* field and enter the data for a new registry value (*1* in this example).

If entered data is correct, then red color for the *Data:* field label will be changed to normal cyan color. This means new value is accepted and will be saved to the registry next time you press **F2**.

If you need to switch back to the left panel with registry keys, press **Tab** or left-click it with a mouse.



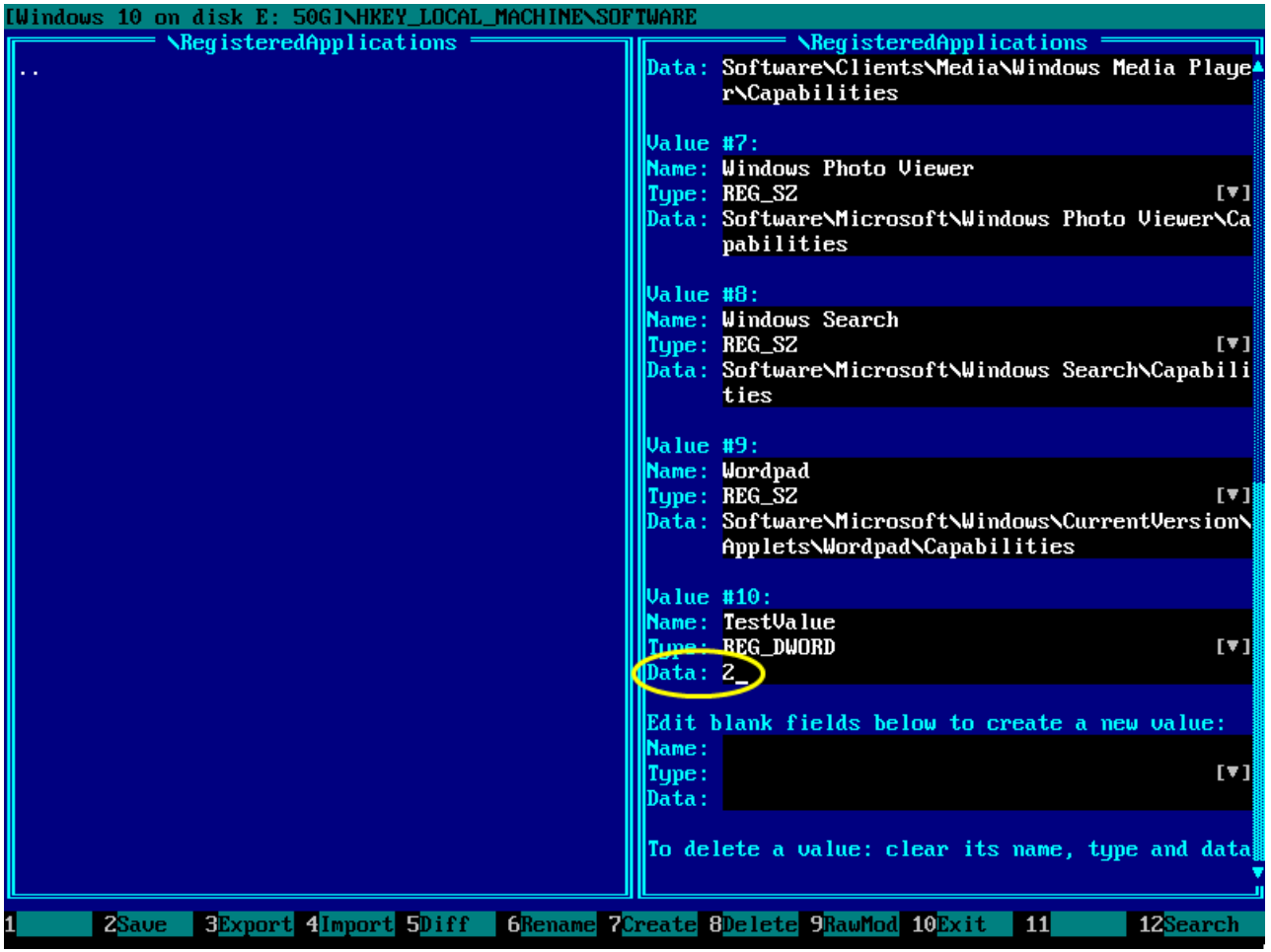
3.9. Change registry value

Make left panel active using a **Tab** key or using a mouse left-click.

Navigate to a registry key where you want to change existing registry value (using ↑, ↓, **PageUp**, **PageDown** and **Enter** keys).

Press **Tab** to make right panel active, or left-click it with a mouse. Then use ↑, ↓, **PageUp** and **PageDown** keys to scroll the view. Values are sorted alphabetically, with default (nameless) value at the top.

Navigate to the *Data:* field of desired value and edit the data using normal keys like letters and numbers. Use **Backspace**, **Del**, ← and → keys if necessary.



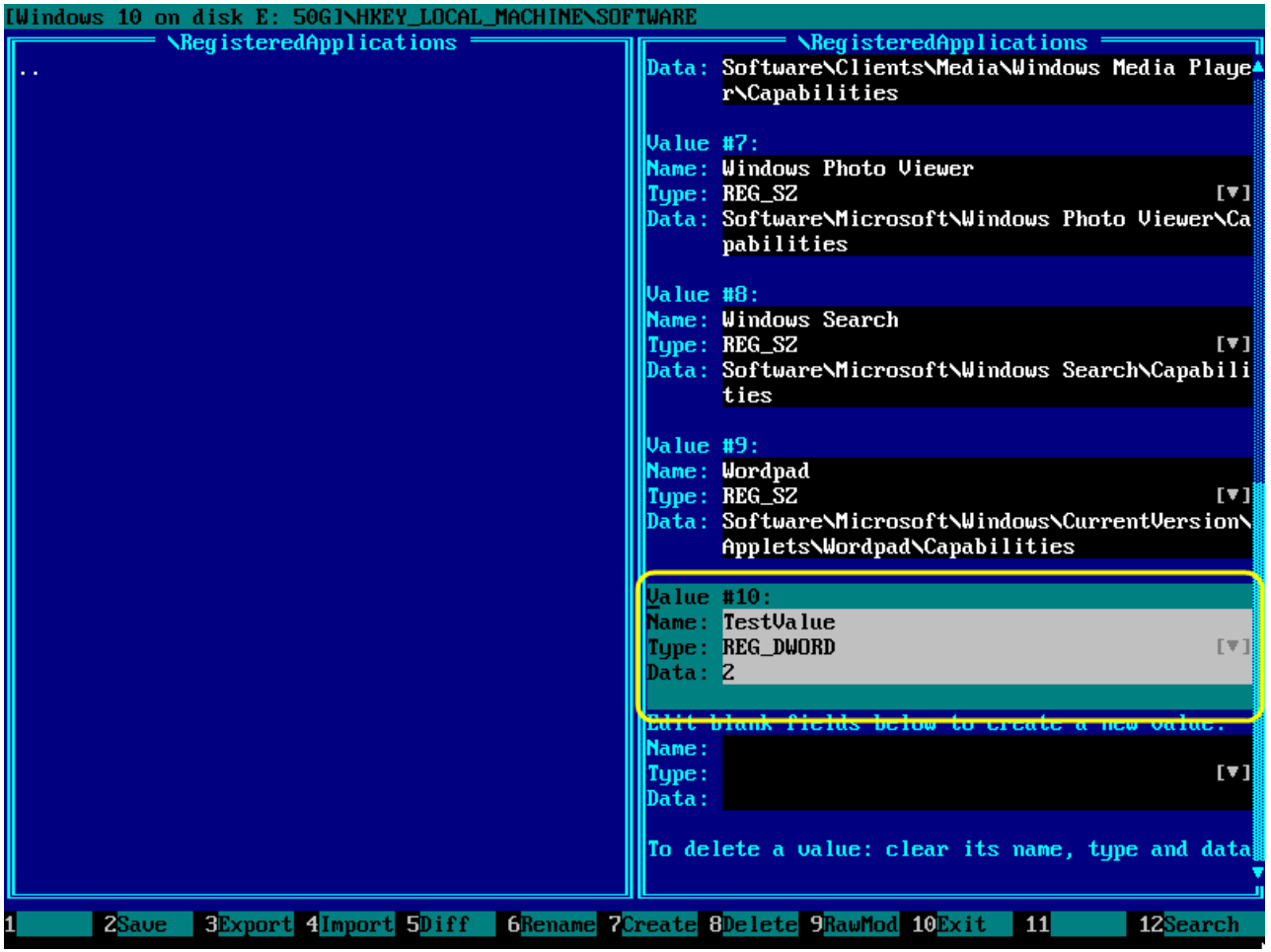
3.10. Delete registry value

Make left panel active using a **Tab** key or using a mouse left-click.

Navigate to a registry key where a value to be deleted resides (using ↑, ↓, **PageUp**, **PageDown** and **Enter** keys).

Press **Tab** to make right panel active, or left-click it with a mouse. Then use ↑, ↓, **PageUp** and **PageDown** keys to scroll the view.

Select one or more registry values by holding a **Shift** when using navigation keys, then press **Del** to delete it or **Ctrl+X** to cut it into the clipboard.

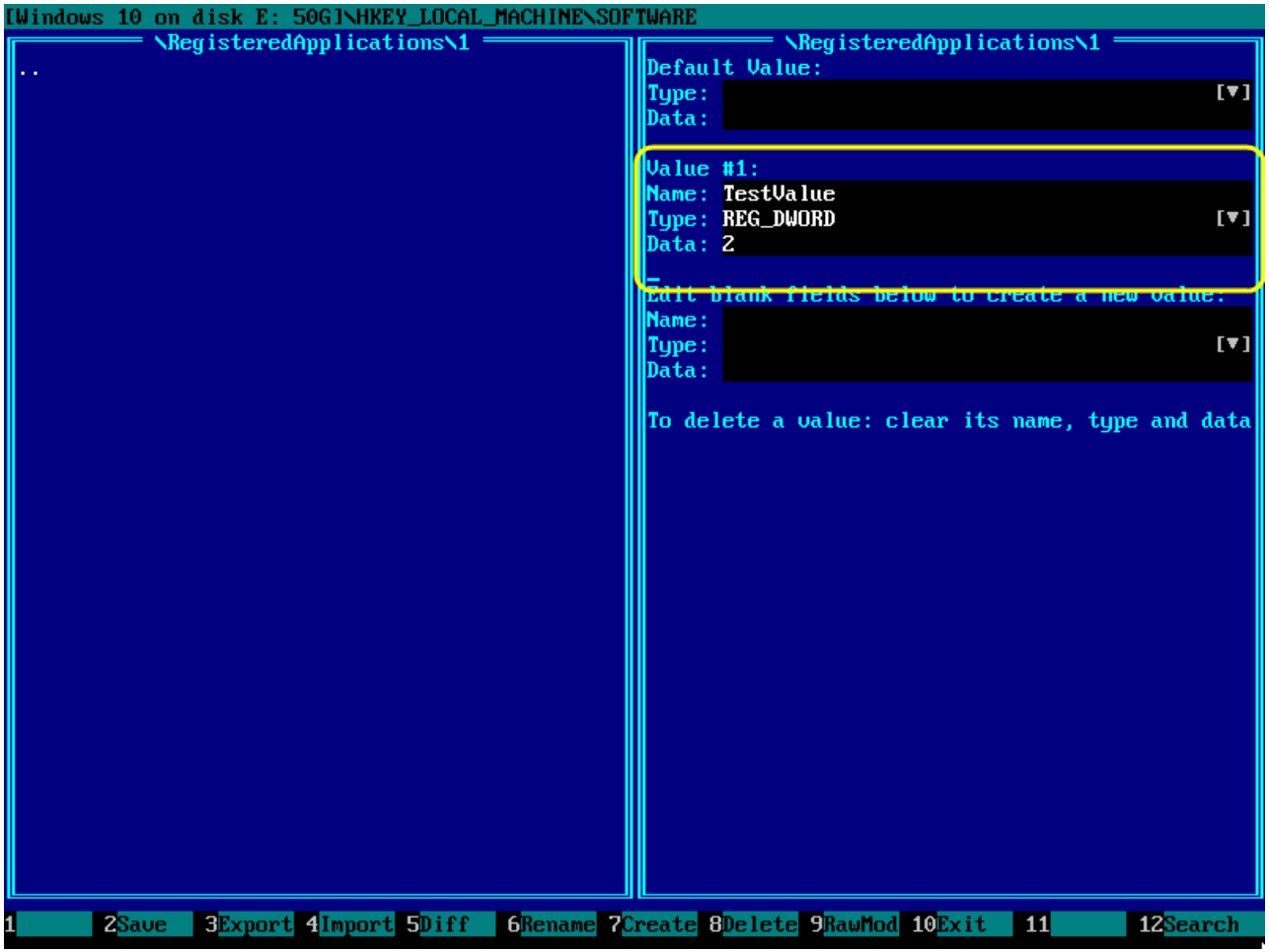


3.11. Copy or move registry value(s) between two keys via the clipboard

Registry values can be copied and moved between registry keys via the clipboard.

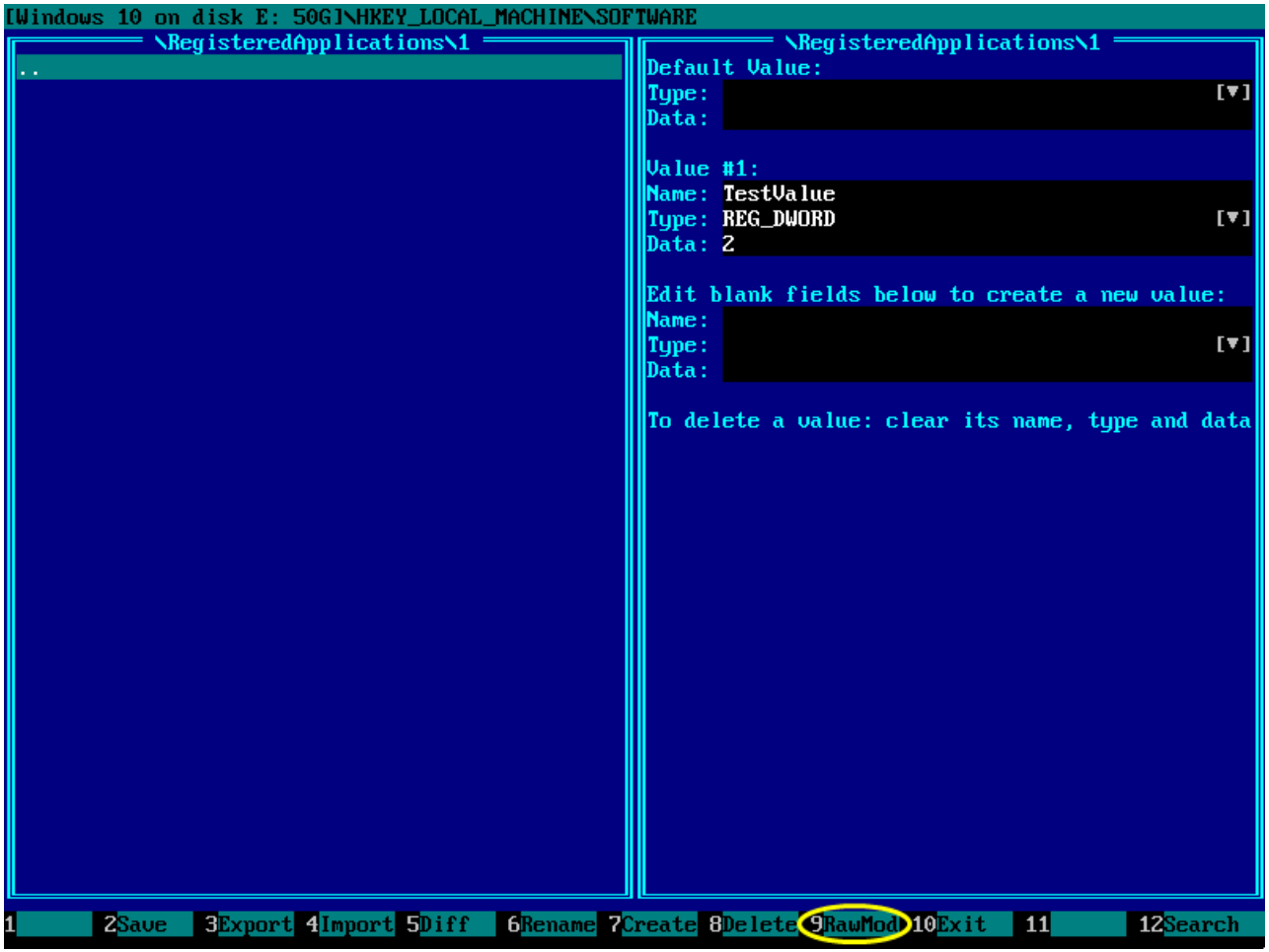
Operation	Key
Cut to clipboard	**Ctrl+X**
Copy to clipboard	**Ctrl+C**
Paste from clipboard	**Ctrl+V**
Select up	**Shift+↑**
Select down	**Shift+↓**
Select left	**Shift+←**
Select right	**Shift+→**

Screenshot shows how recently cut value was pasted into new empty key named *1*.



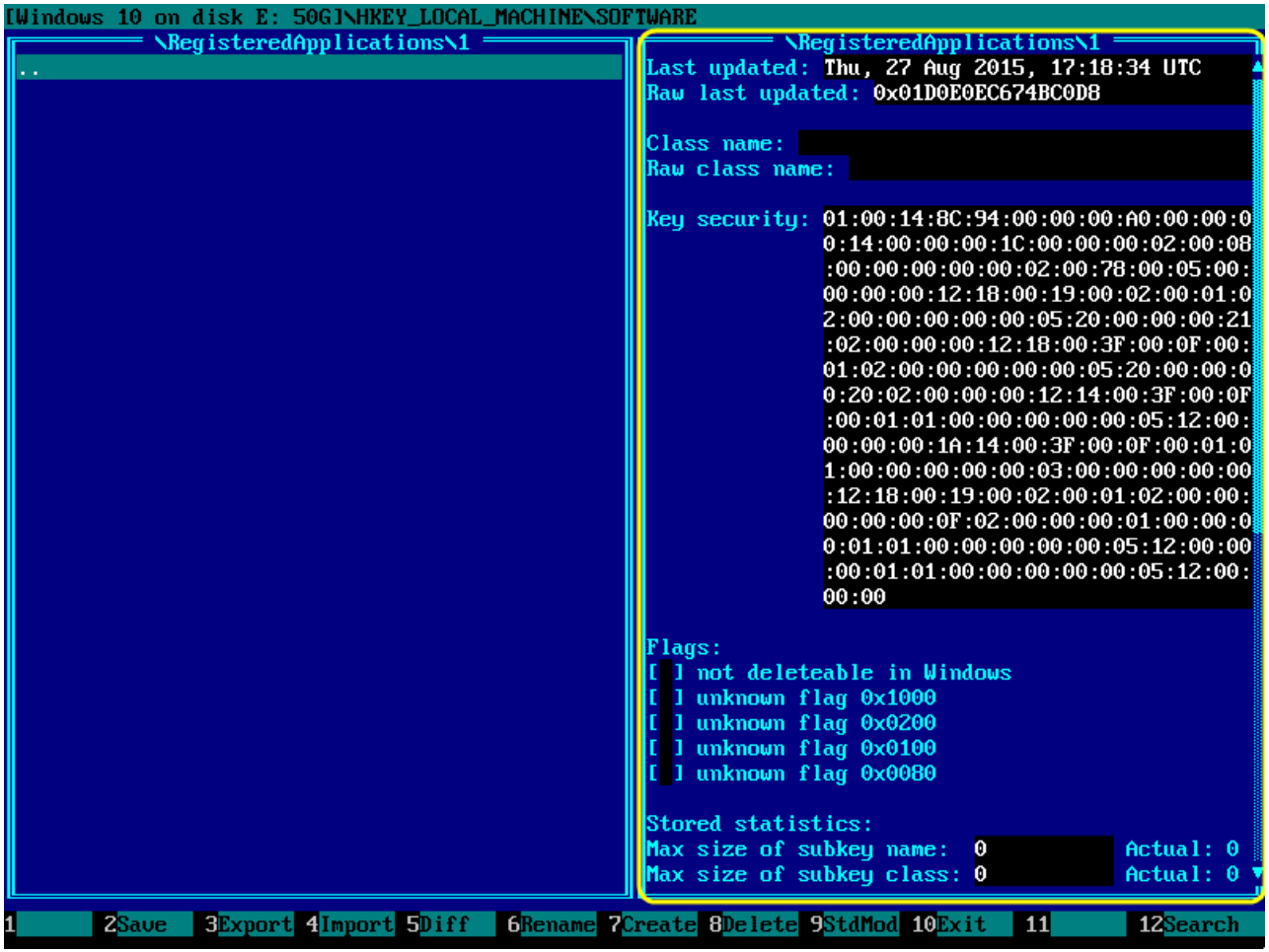
3.12. Edit key class name and other properties in the raw mode

Navigate to the key you want to edit class name for. Then press **F9** to enter the raw mode:



Right panel will switch into the raw mode (much more detailed than standard mode).

You can use **F9** at any moment to switch back to standard mode.

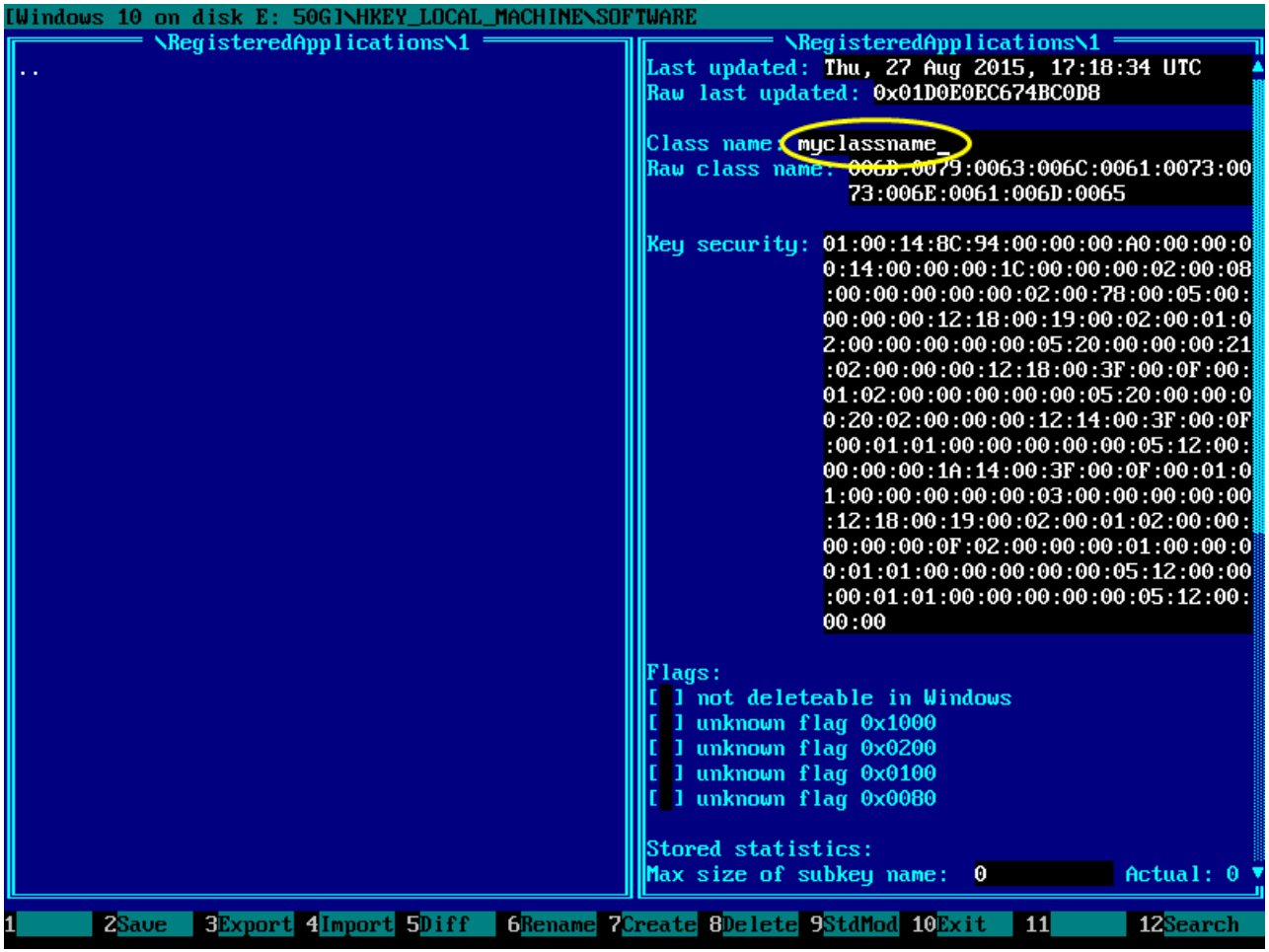


Press **Tab** to make right panel active.

Navigate to the *Class name:* field using arrow keys and type the class name (*myclassname* in this example). *Raw class name:* field will change its data as you type.

The same way you can change the security descriptor (or copy-paste it from another key), last update time of the key, its flags and stored statistics.

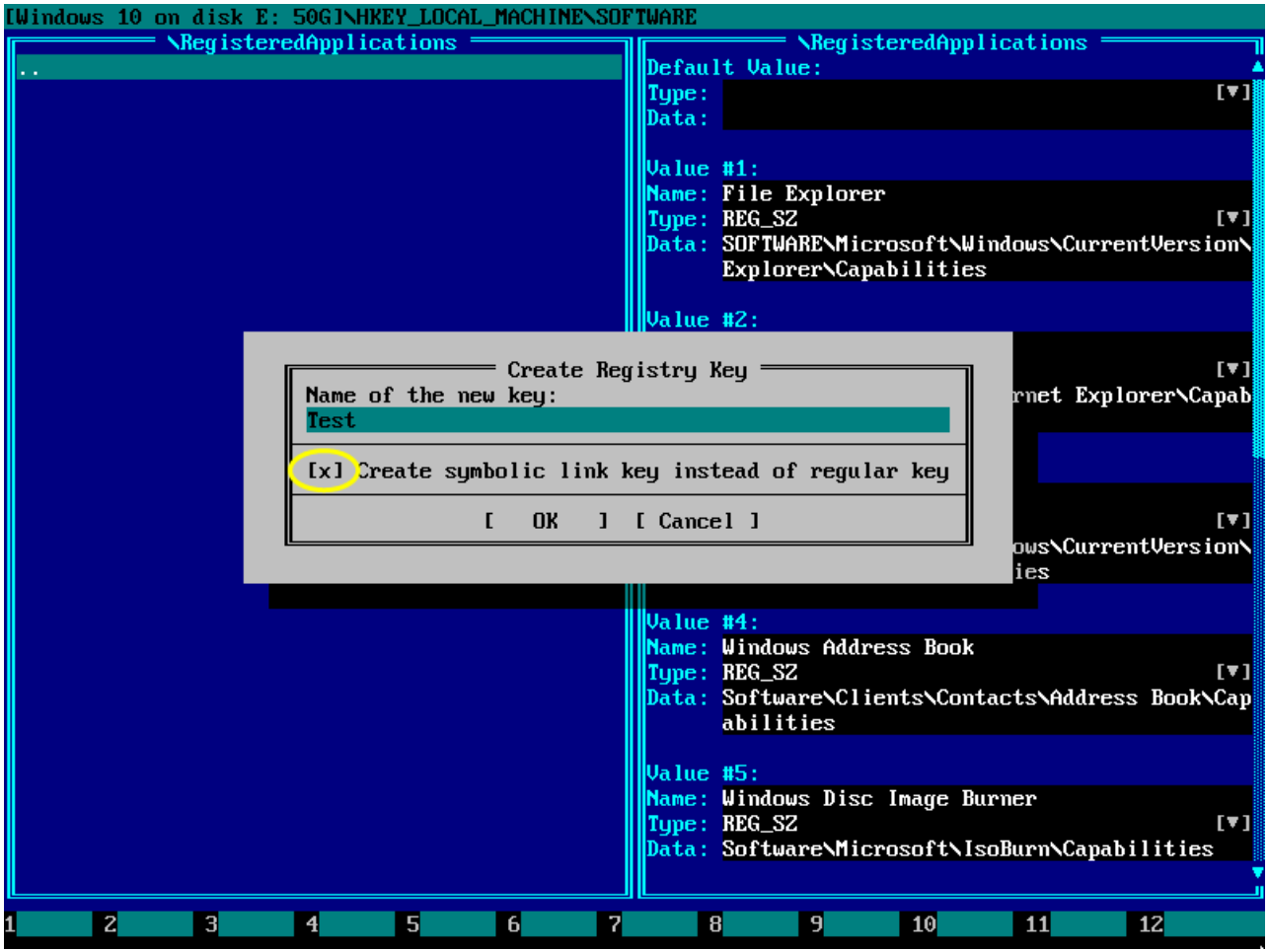
When done, you may press **F9** to exit raw mode and get back to standard mode.



3.13. Create or edit registry symbolic link

To create new symbolic link in registry, press **F7** and enable the checkbox "*Create symbolic link key instead of regular key*"

Then press **Enter** or click *OK* to confirm and close dialog box.



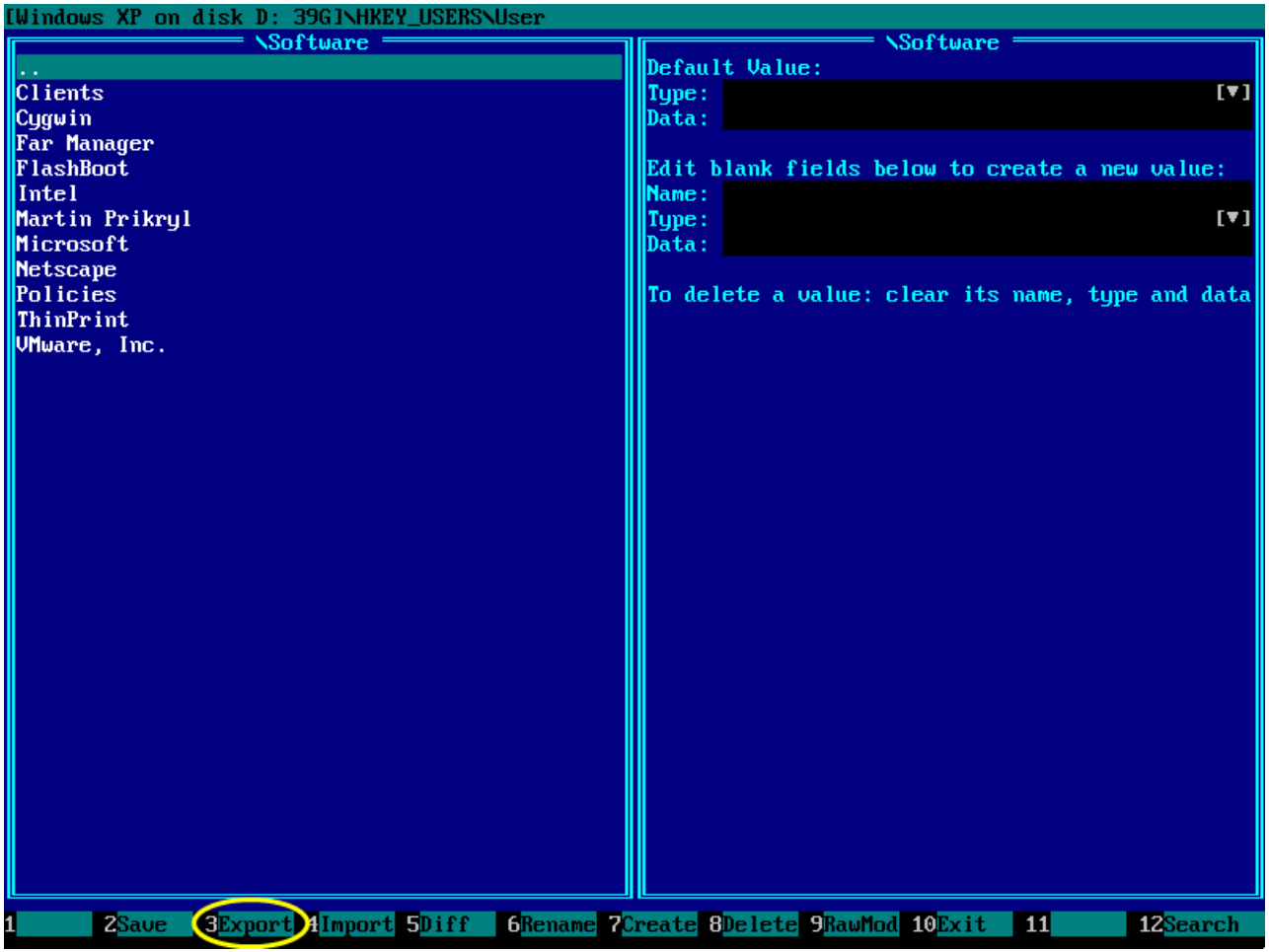
After a special symlink key has been created, press **Enter** to enter it, then press **Tab** to make right panel active.

You may edit symlink target now. Please note that symlink targets are specified in NT Native format, e.g. *\REGISTRY\MACHINE\SOFTWARE\...*, *\REGISTRY\MACHINE\SYSTEM\...*.

Symlink also has a security descriptor which can be edited in the raw mode (**F9**).

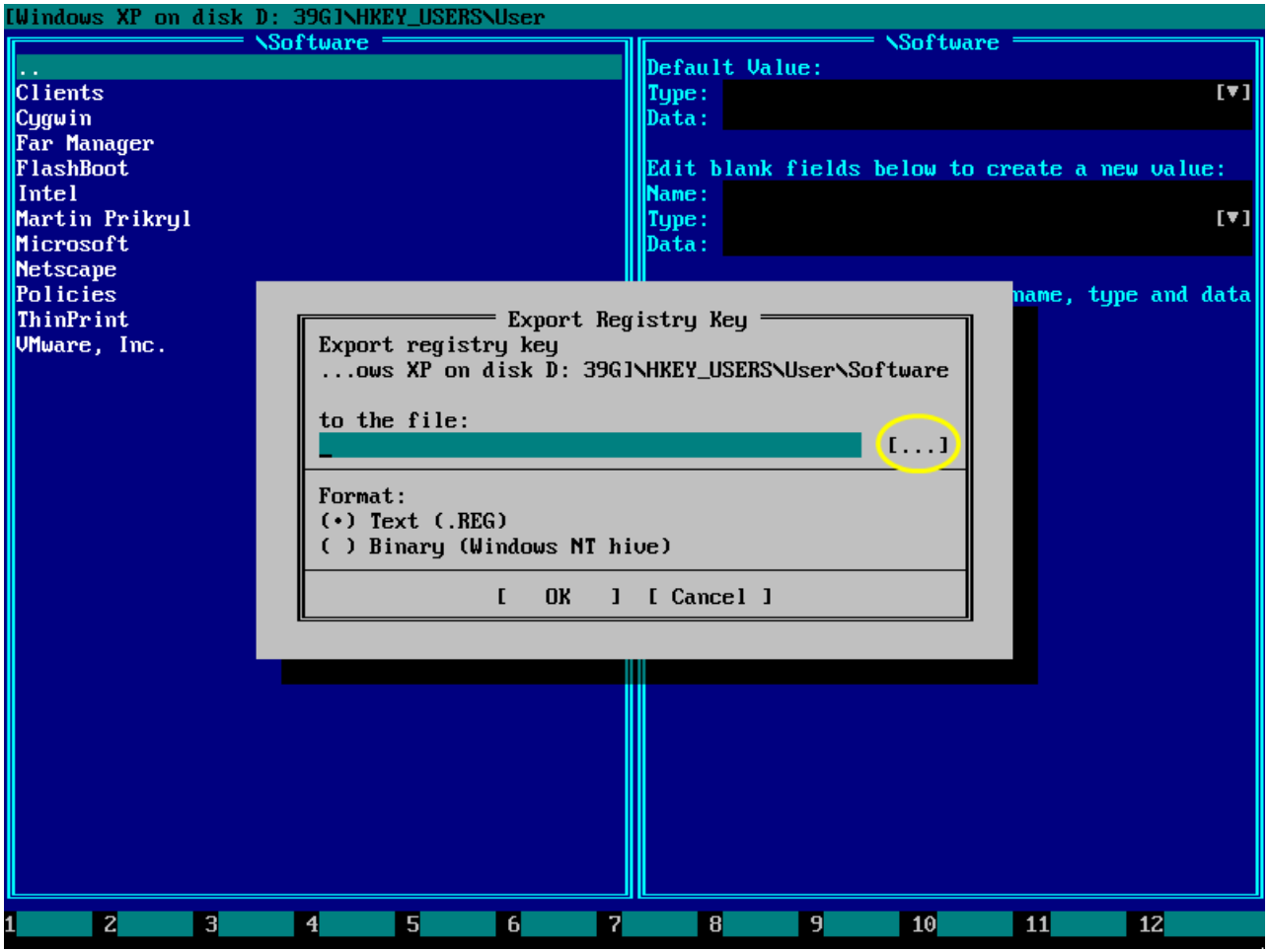
3.14. Export registry key with subkeys and values

Navigate to the registry key you want to export and press **F3** to begin export of the current key to external file.

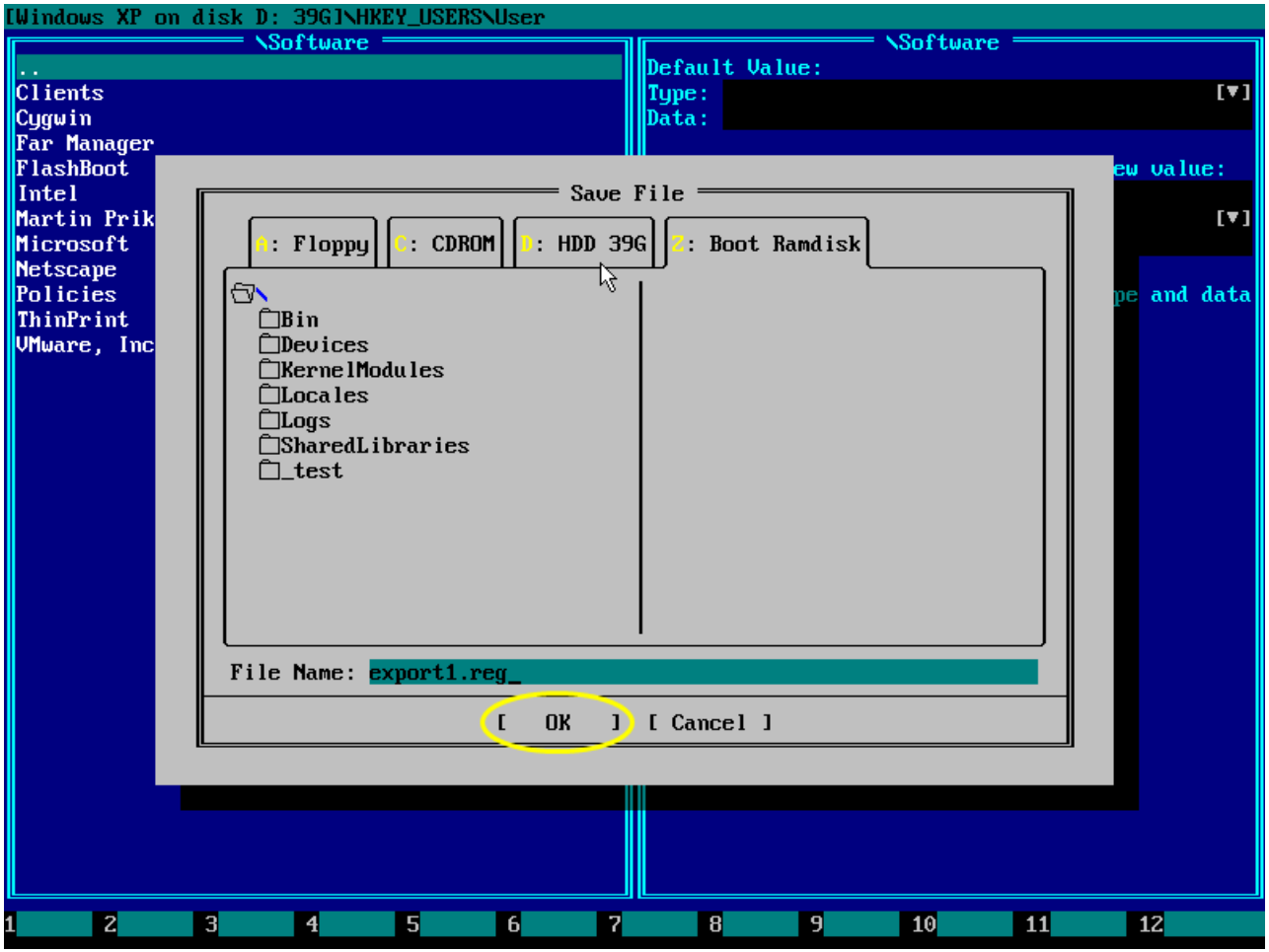


Popup window like this will be shown on the screen. You may type the file name or click *[...]* button to open file save window.

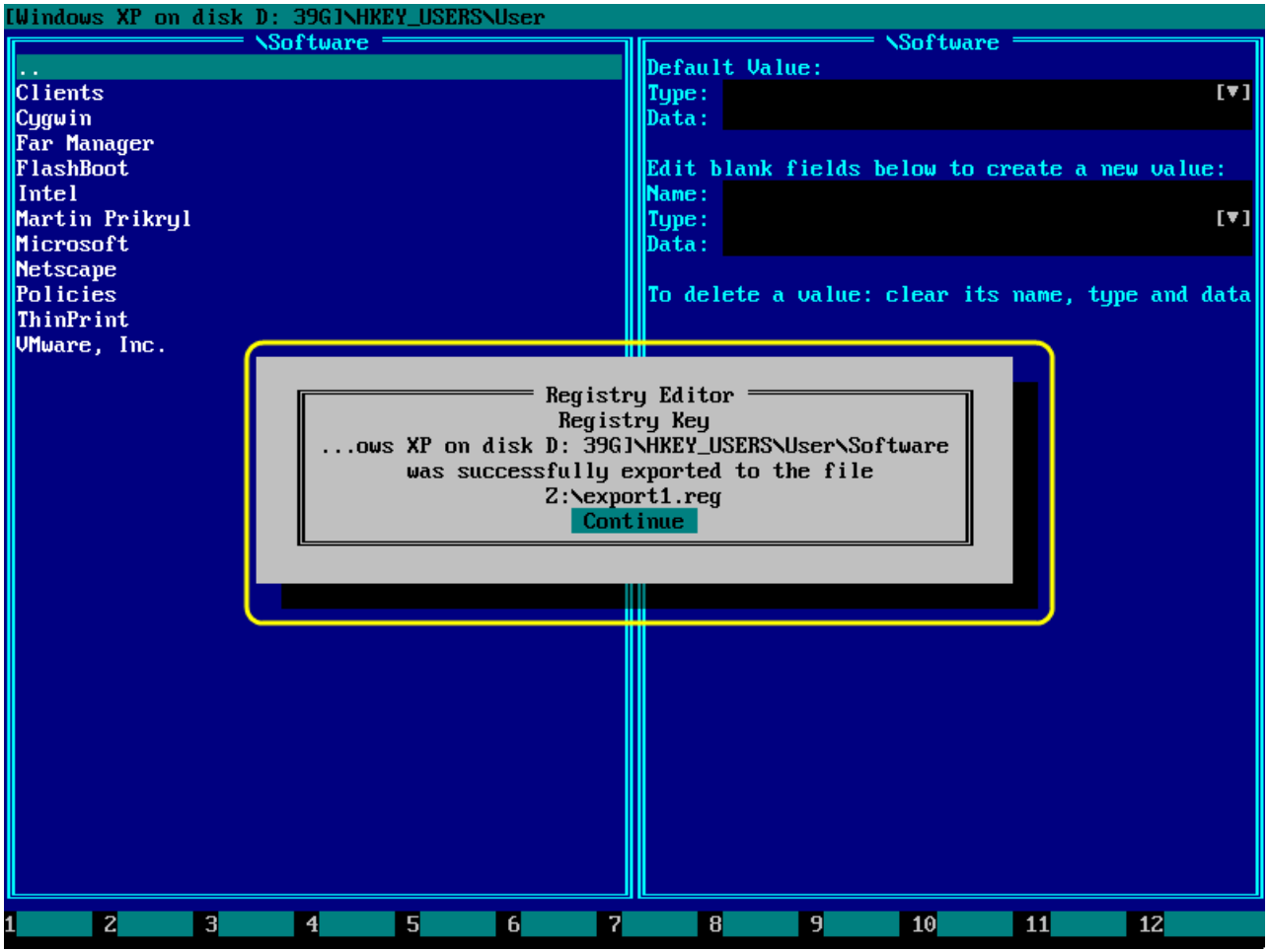
Also you may choose binary format here (if you would like to preserve full registry information: security descriptors, flags, key statistics etc).



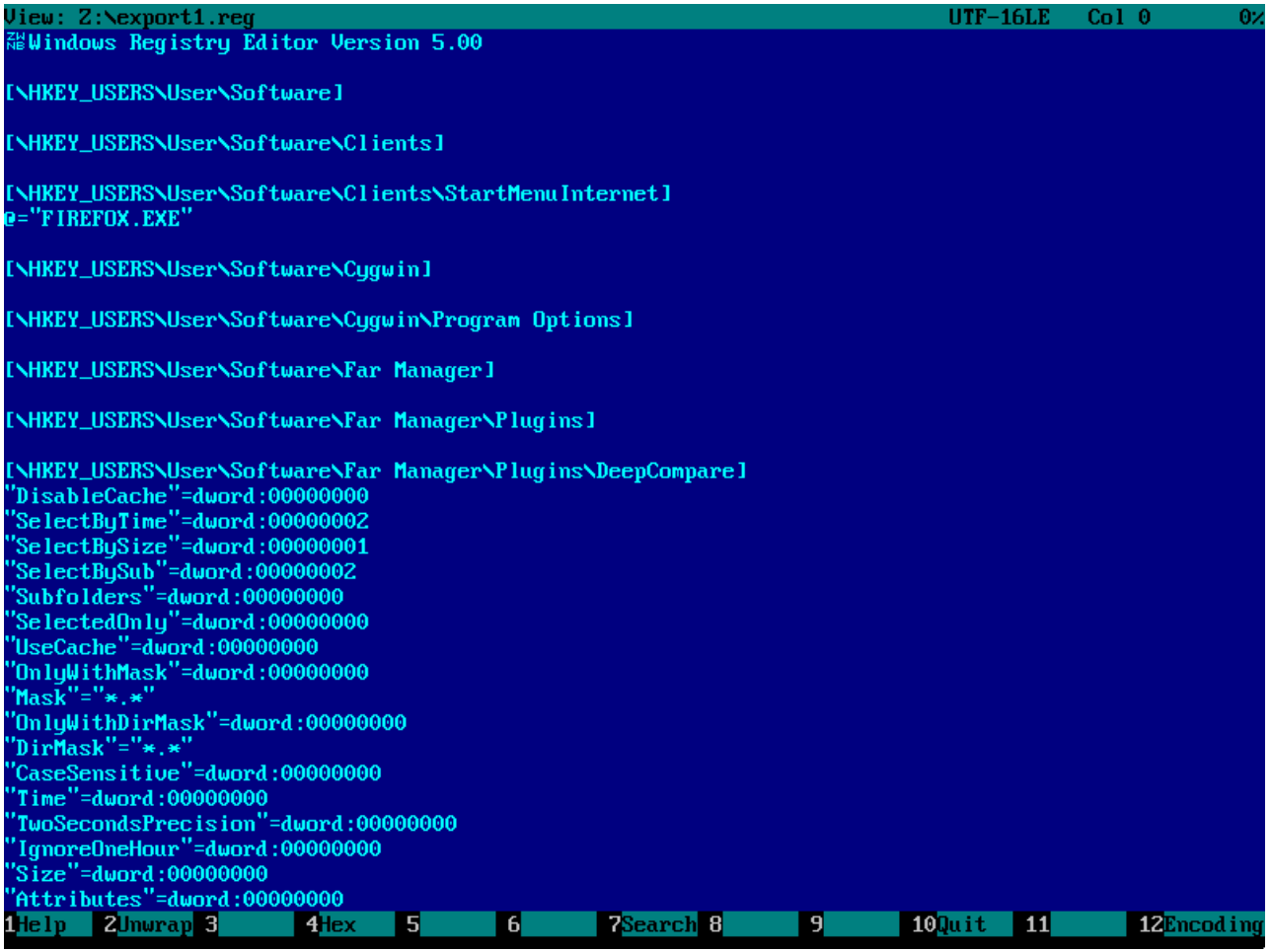
Choose a disk and folder to save registry dump and click *OK* button (twice: in this window and in the parent window).



If current registry key was exported successfully, a message like this will be shown.



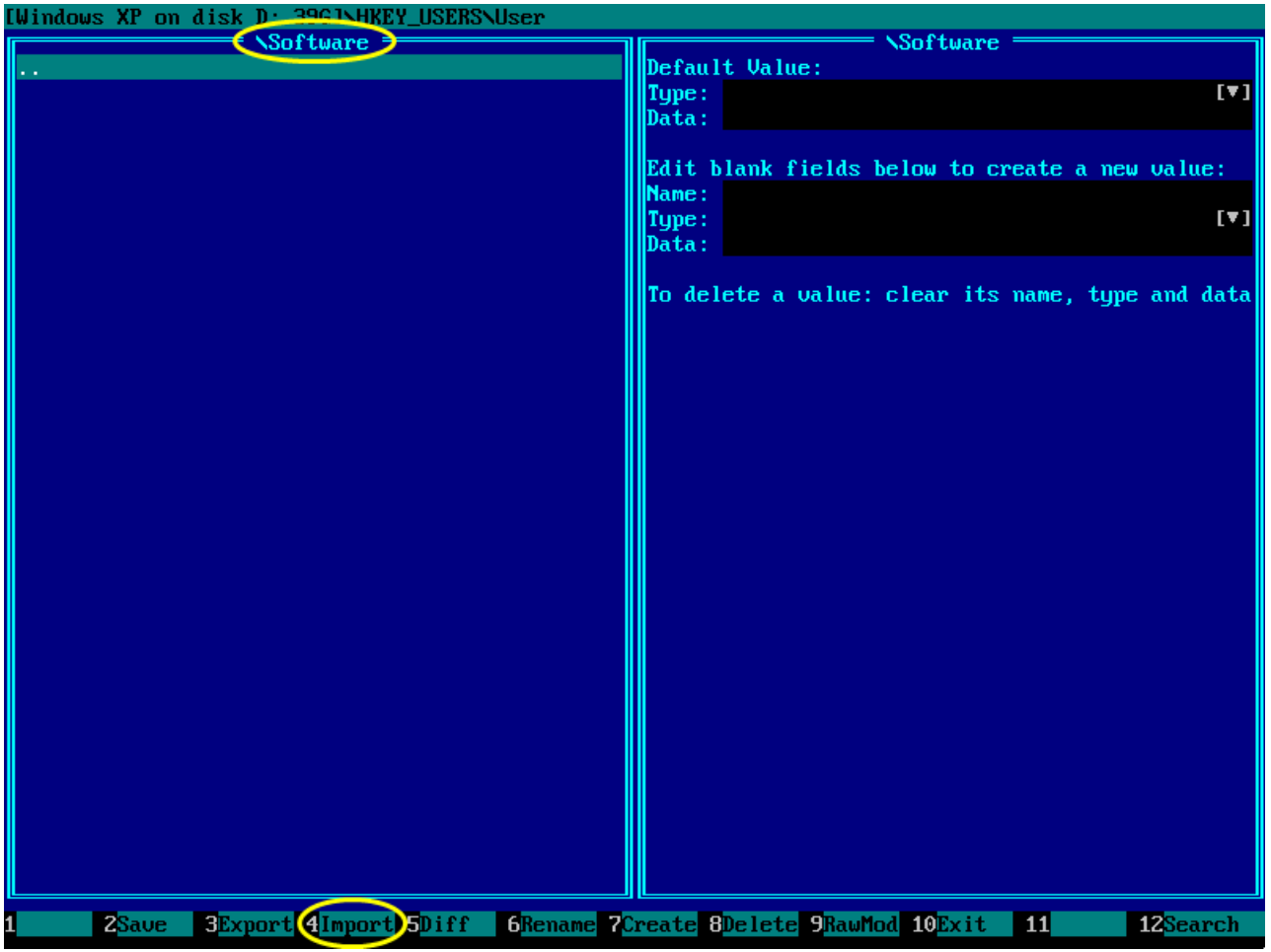
Format of the exported file is compatible with *regedit.exe* (for text-mode exports).



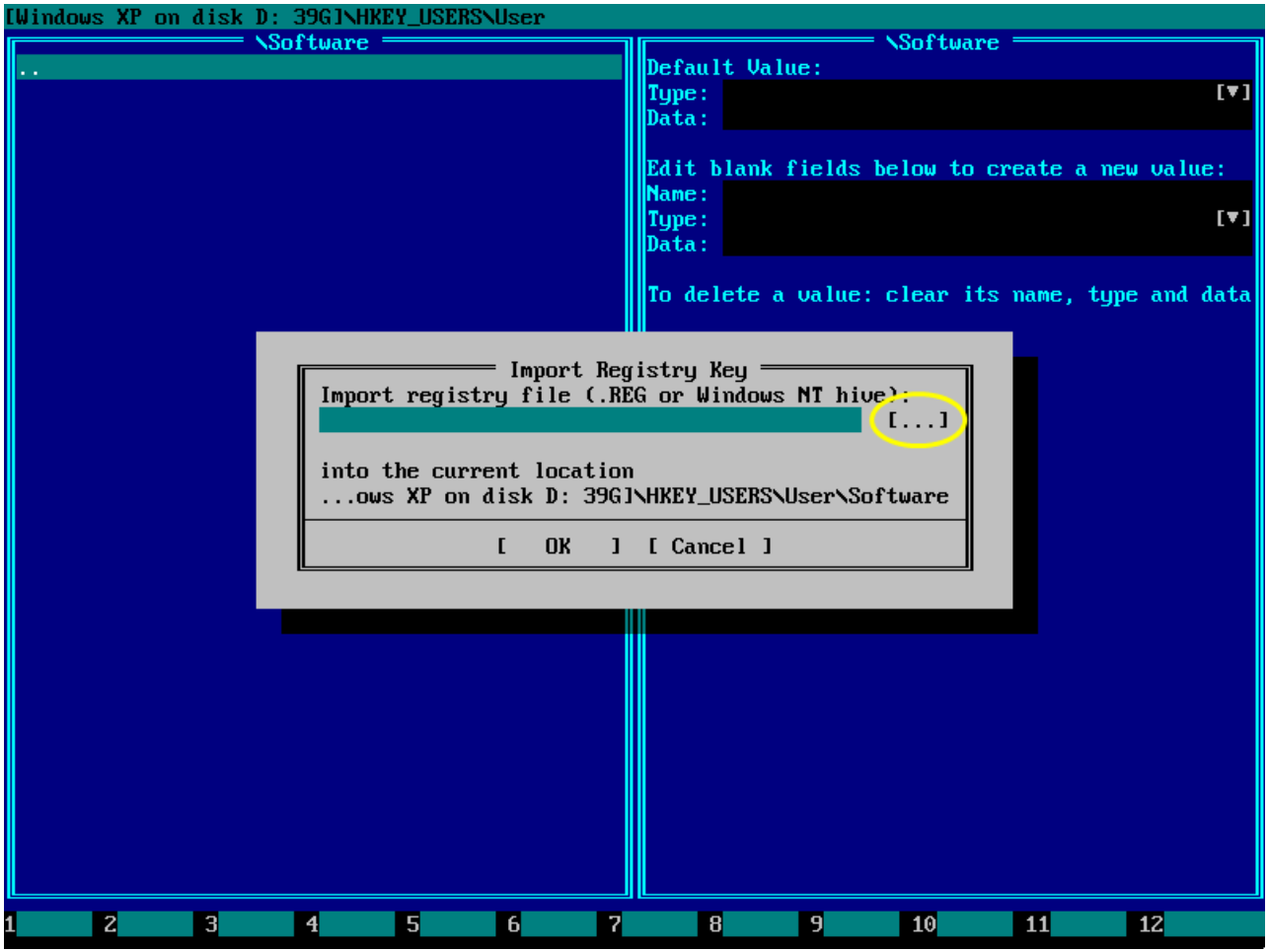
3.15. Import registry key with subkeys and values

Navigate to the registry key you want to import. Make sure it exists and empty. Use **F8** to delete an old key and **F7** to create a new key if necessary.

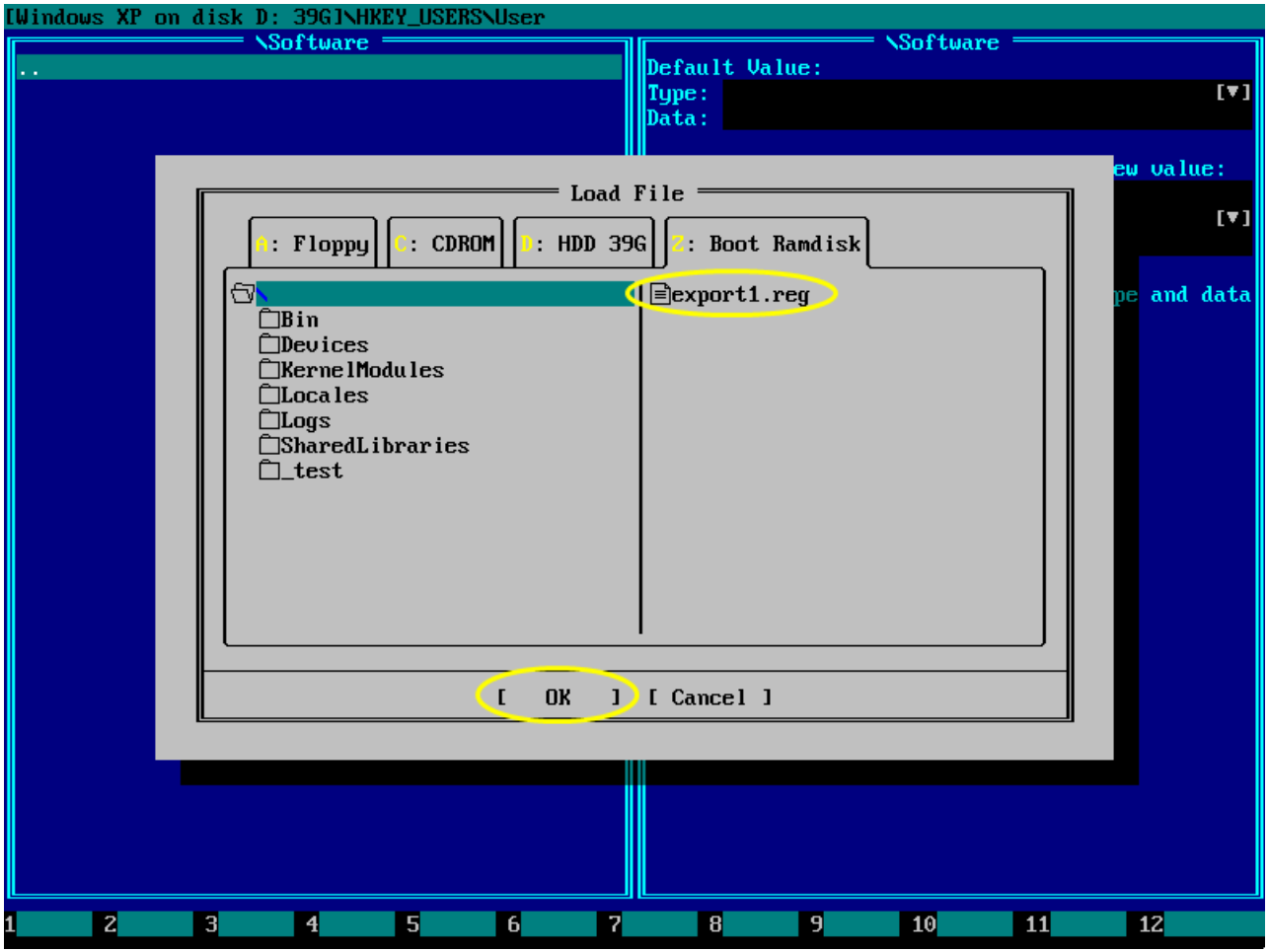
Then press **F4** to begin import of the current key from external file.



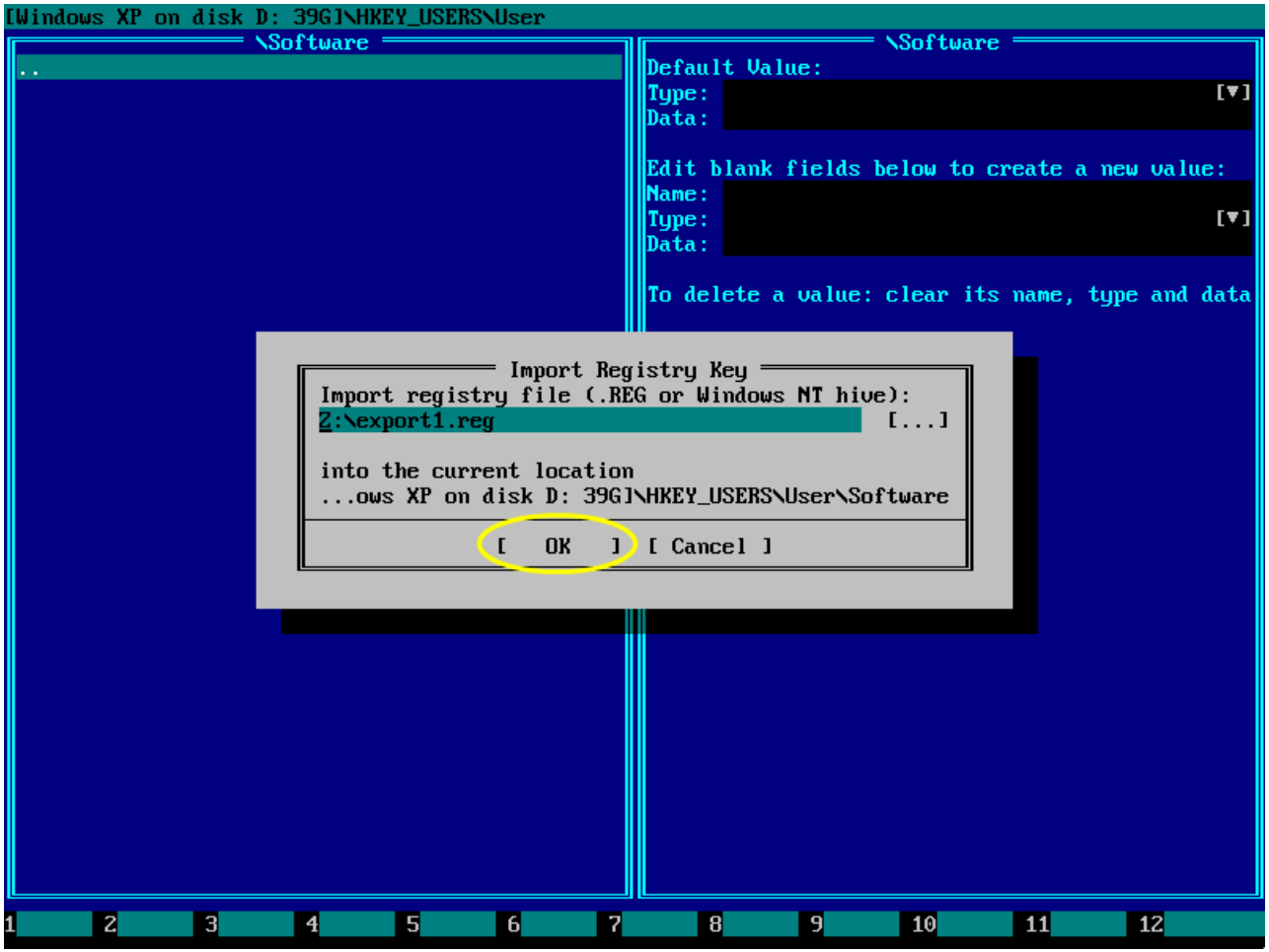
Enter full file name to import here or click *[...]* to browse for file.



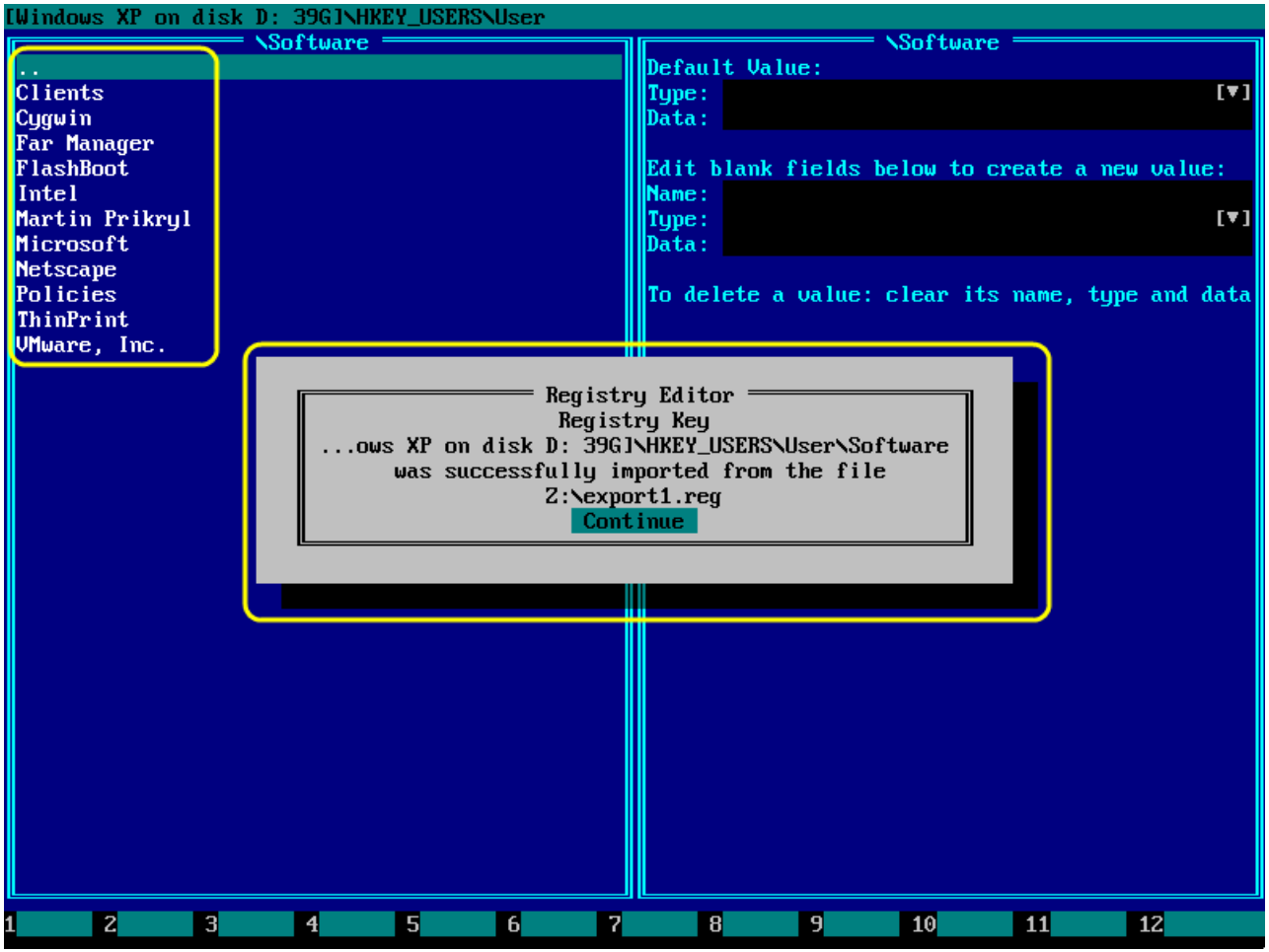
Choose disk, folder, file, and press **Enter** or click *OK*.



Make sure everything is correct and click *OK*.



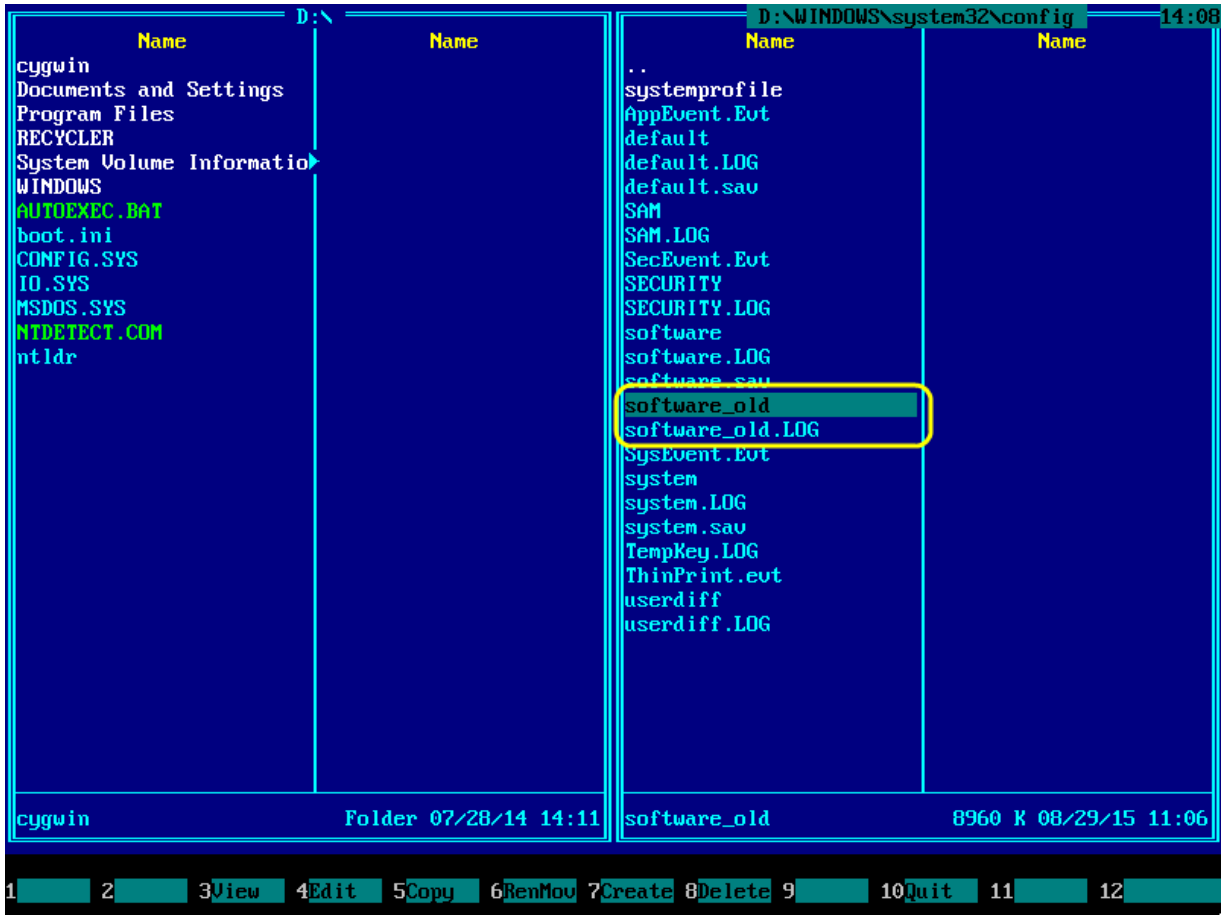
If current registry key was imported successfully, its subkeys and values will be shown immediately and also a message like this will be shown.



3.16. Create difference report for a registry hive

You may find useful to compare your registry before and after installing certain software. This example shows how to compare *HKEY_LOCAL_MACHINE\SOFTWARE* registry hive before and after installing *WinRar*.

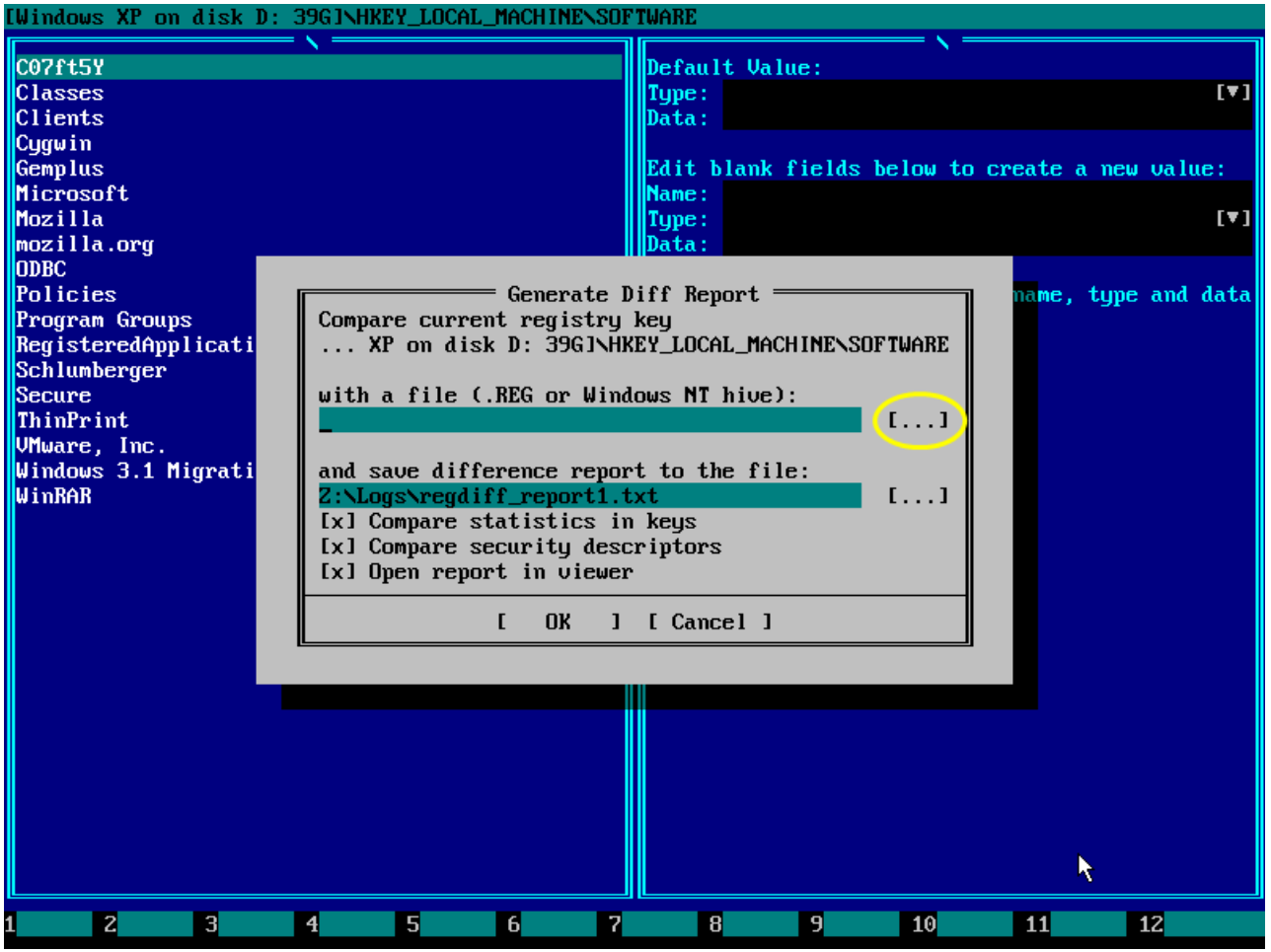
Before installing software you are going to examine, run EmBootKit File Manager and save backup copy of the relevant registry hive(s) and log(s). Refer to “Introduction to File Manager” volume of Emergency Boot Kit user guide (https://www.prime-expert.com/embootkit/user_guide/embootkit_file_intro.pdf) if necessary.



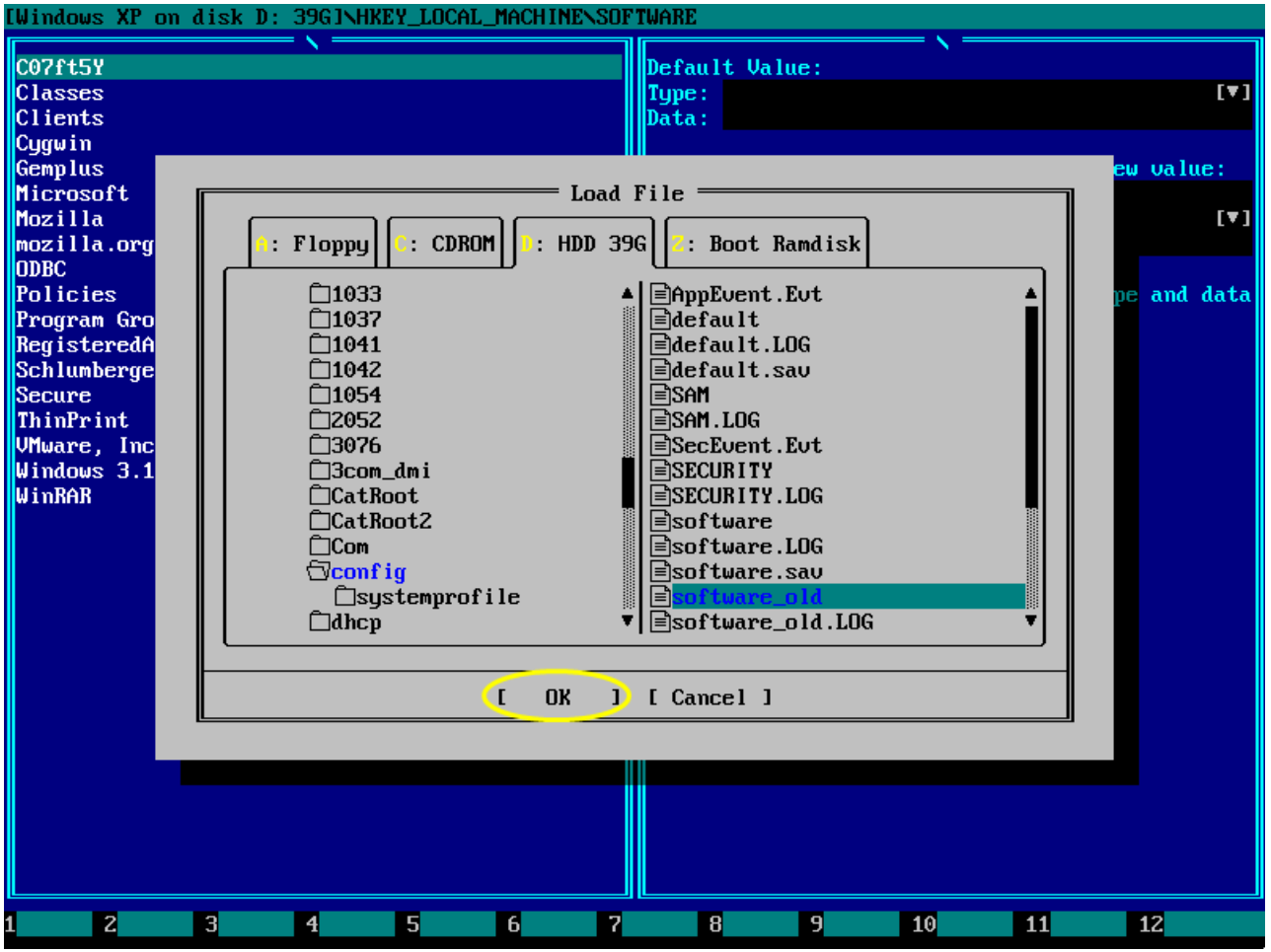
After installing software you are going to examine, run EmBootKit Registry Editor and open the relevant registry hive as explained above.

Then press **F5** to open registry diff tool.

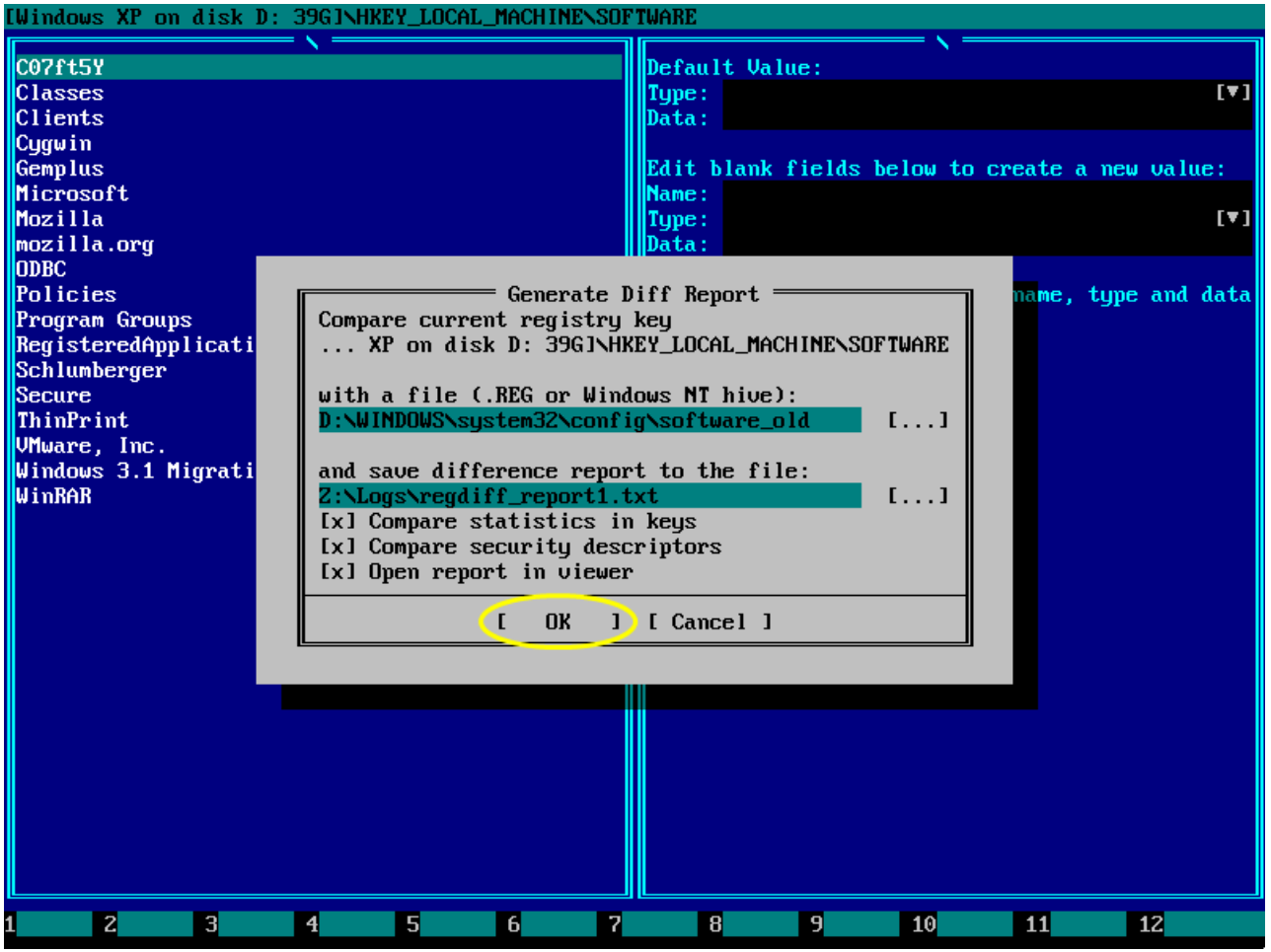
Click *[...]* button to browse for backup copy of the relevant registry hive(s) you saved earlier.



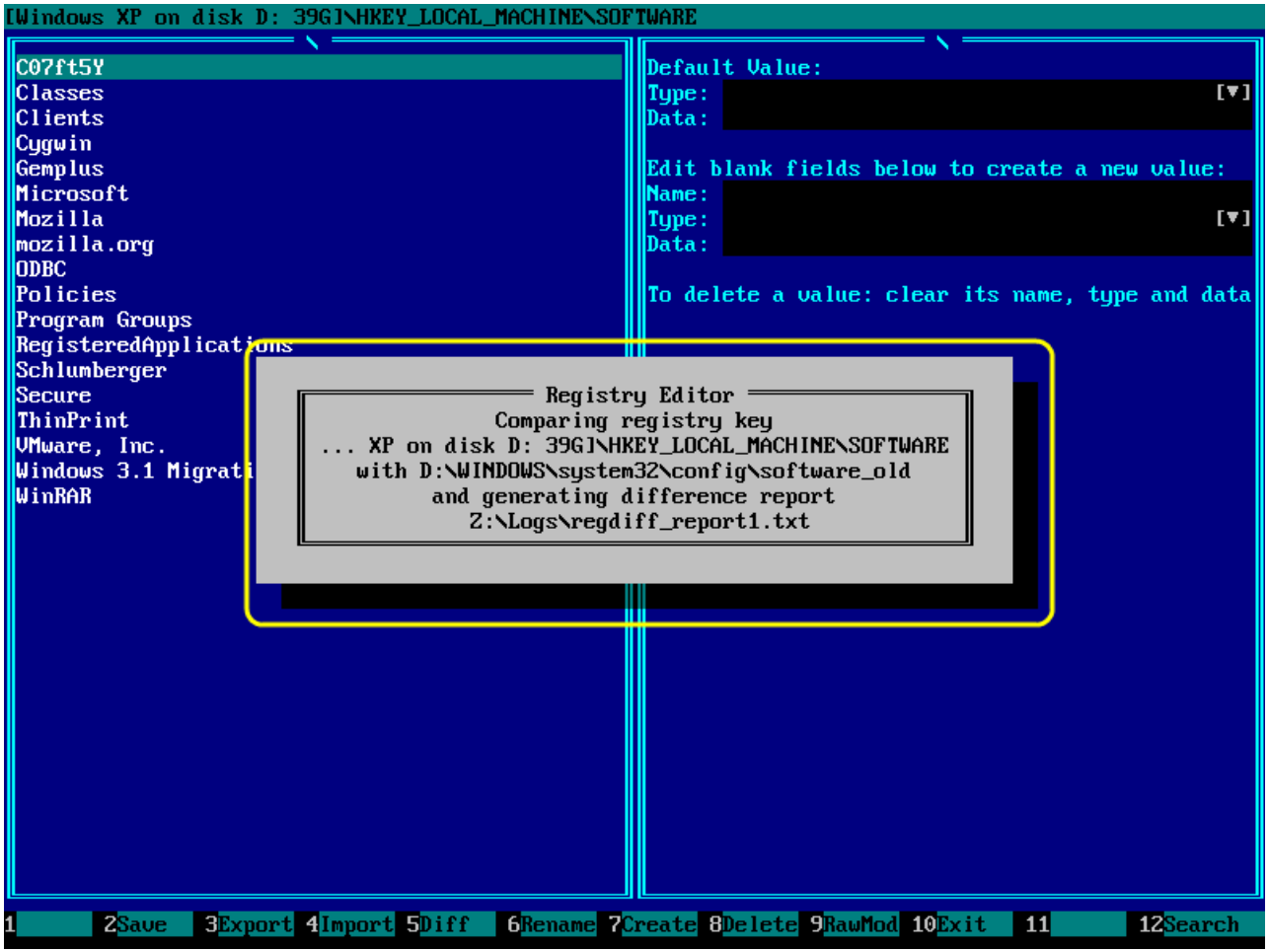
Choose drive, path, filename and click *OK* button to confirm.



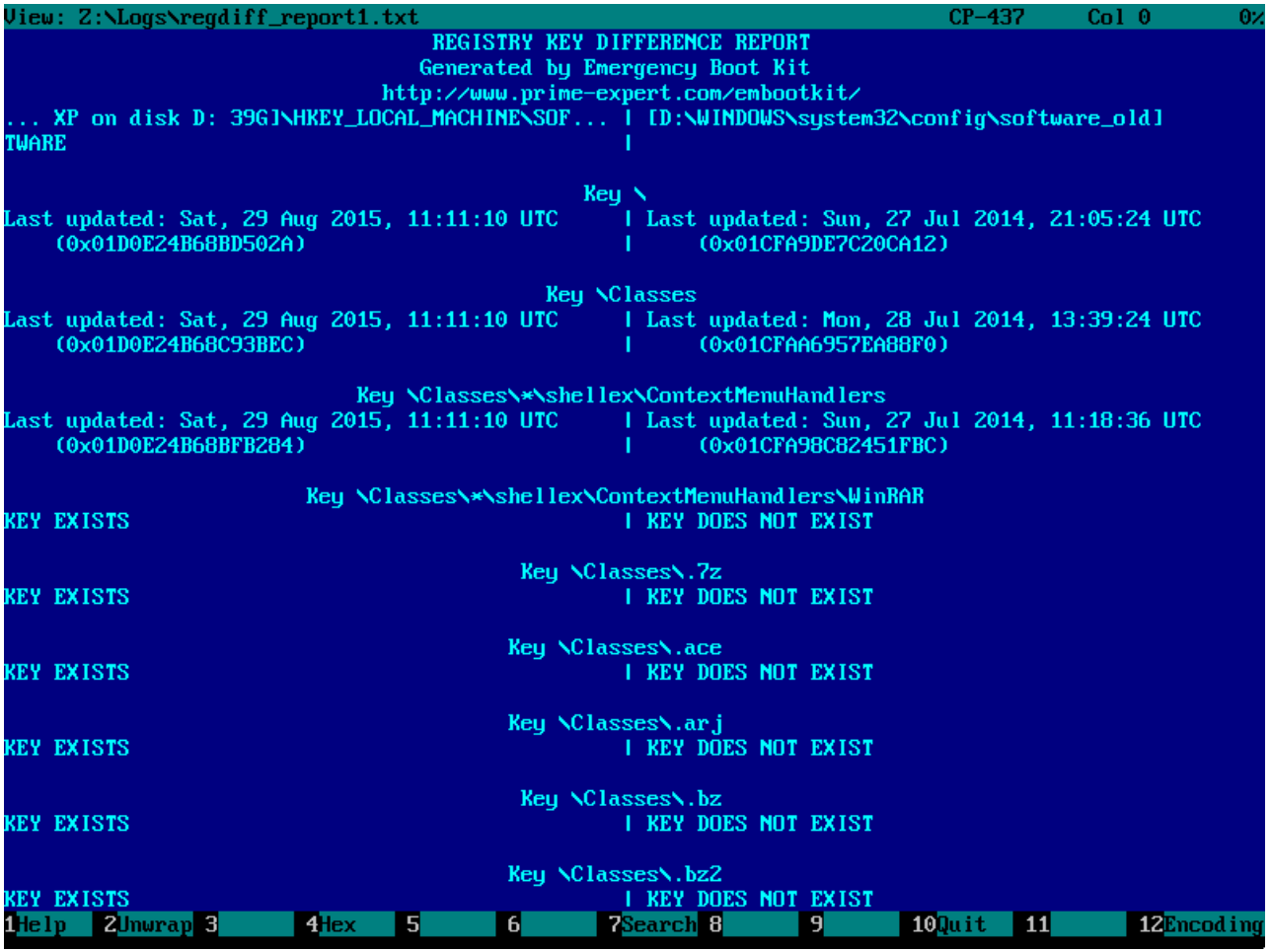
Verify options and click *OK* button to confirm.



EmBootKit Registry Editor will compare two registry hives and automatically close this window when done.



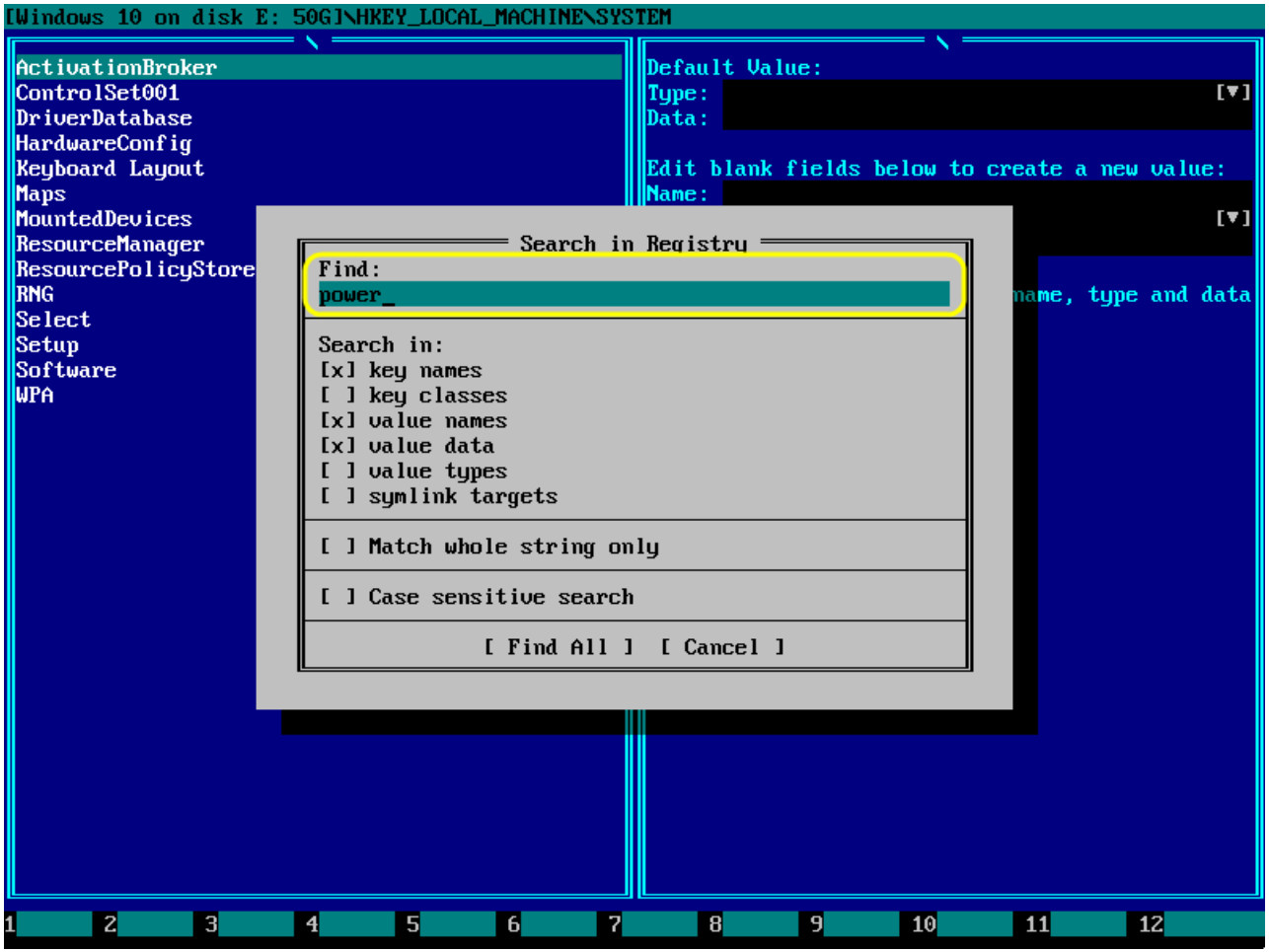
Comparison result will look like this.



3.17. Search in a registry hive

To search in a registry hive, press **F12**.

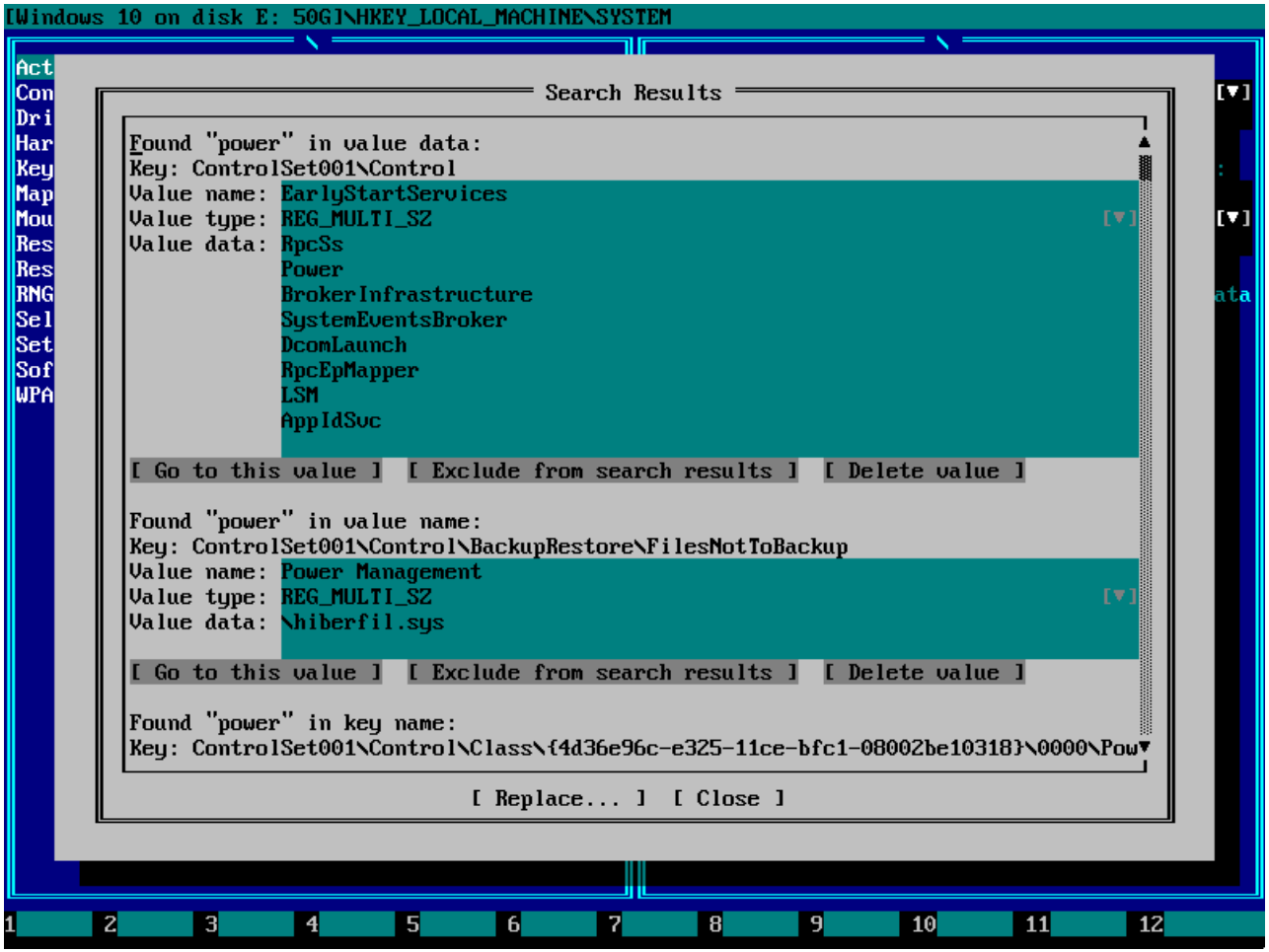
Set search term and options in dialog window and then press **Enter** or click *Find All* button.



Search results will look like this. You may edit keys and values and delete them right here, in search results window.

You may apply replace operation to all remaining search results. To do this, click *Replace...* button.

Exclude from search results buttons can be used to perform partial replace.



Search & Replace dialog will look like this.