Registry Editor

Contents

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 11. 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.

```
Emergency Boot Kit version 1.6a (64-bit)

Registered to: User Name
Email:        username@example.com
```

```
┌─────── Emergency Boot Kit ───────┐
│ File manager                 F1  │
│ Windows password wizard      F2  │
│ Registry defrag              F3  │
│ Registry editor              F4  │
│ Mount & boot center          F5  │
│ Partition manager            F6  │
│                                  │
│ Reboot                       F10 │
└──────────────────────────────────┘
```

```
1FileMg 2Passwd 3RegDef 4RegEdi 5MBCent 6PartMg 7      8      9      10Reboot 11      12
```
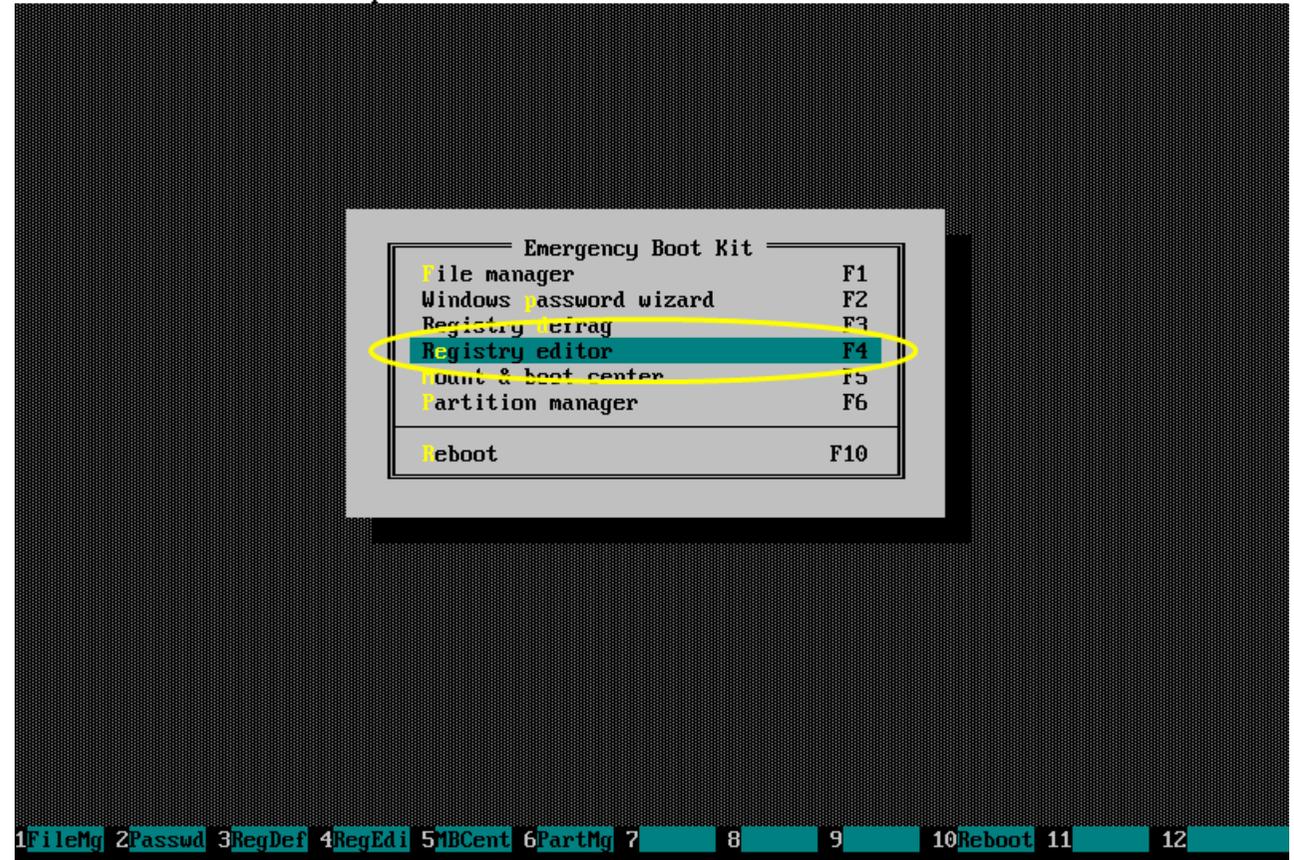
Wait while Registry Editor scans for Windows installations and registry hives. This window will automatically disappear when done.

```
Emergency Boot Kit version 1.6a (64-bit)

Registered to: User Name
Email:         username@example.com
```

```
┌──────────────────── Registry Editor ────────────────────┐
│ Scanning local disks for Windows installations, please wait... │
└──────────────────────────────────────────────────────────┘
```

```
1    2    3    4    5    6    7    8    9    10   11   12
```
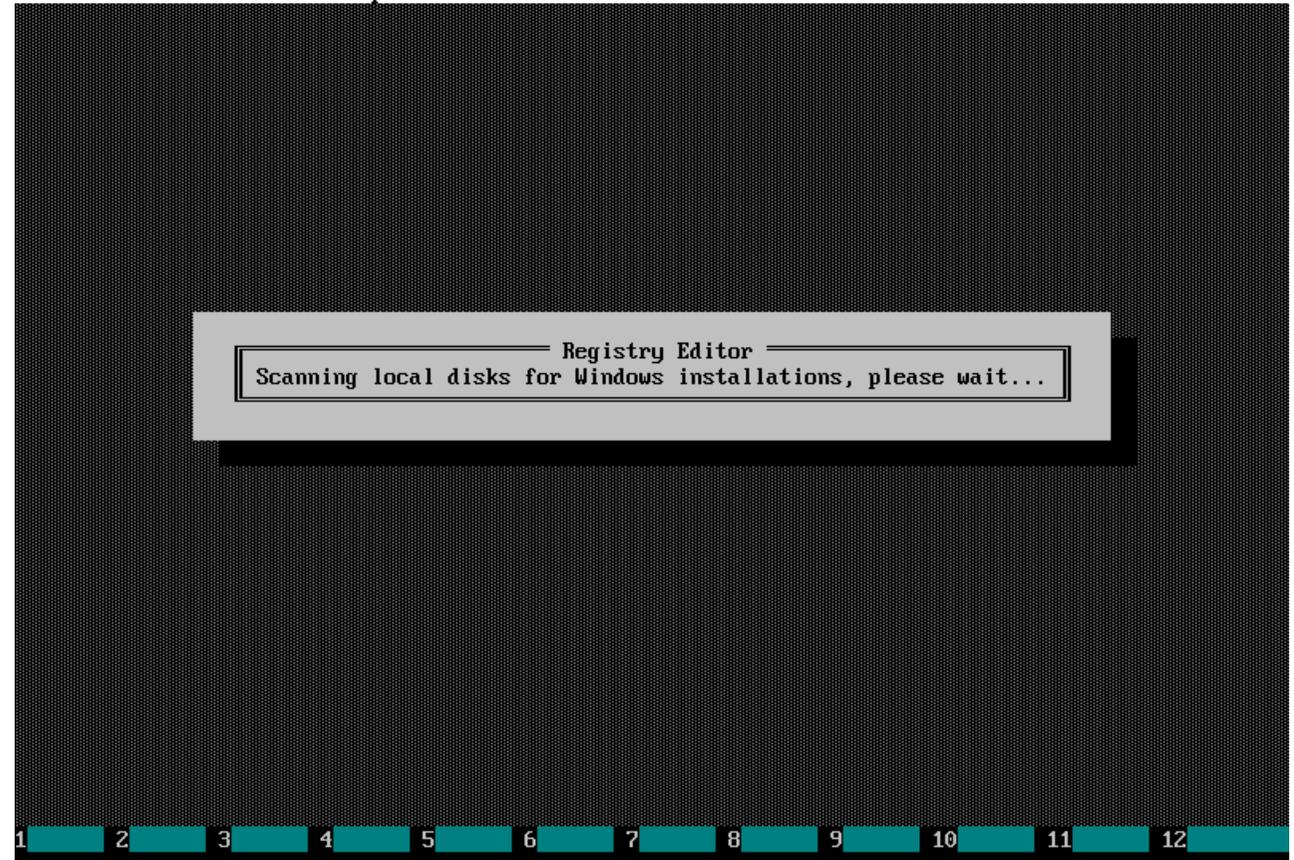
3. How to

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.

```
Emergency Boot Kit version 1.6a (64-bit)

Registered to: User Name
Email:        username@example.com
```

```
══ EmBootKit Registry Editor ══

Choose Windows installation to edit Registry for:

┌──────────────────┬───────────┬──────────────────┬──────────────────┐
│      Disk        │ Disk Size │       OS         │ Installation Date│
├──────────────────┼───────────┼──────────────────┼──────────────────┤
│ D: System Reserved│  499 M   │  Boot Partition  │  26 Jul 2015     │
│ ▶ E:             │   50 G    │  Windows 10      │  26 Jul 2015   ◀ │
└──────────────────┴───────────┴──────────────────┴──────────────────┘

[ ] I would like to override default options and
    specify custom filename of Registry Hive to edit

                                   [ Next > ]  [ Cancel ]
```

```
1    2    3    4    5    6    7    8    9    10    11    12
```
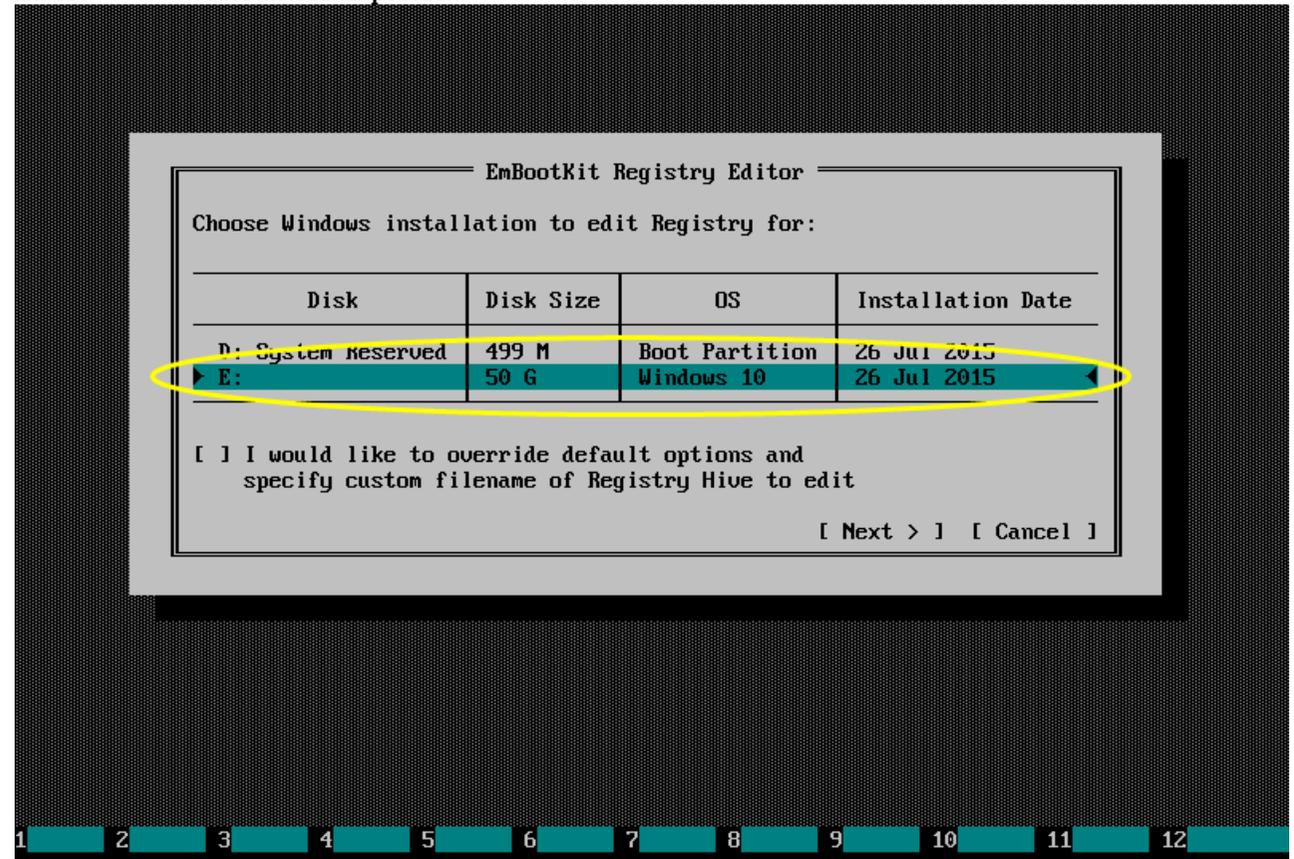
Choose registry hive you want to edit from the list.
We are going to edit
HKEY_LOCAL_MACHINE\SOFTWARE in this example.

```
Emergency Boot Kit version 1.6a (64-bit)

Registered to: User Name
Email:        username@example.com

         ┌──────────── EmBootKit Registry Editor ────────────┐
         │                                                    │
         │  Choose Registry Hive you would like to edit:      │
         │                                                    │
         │  ┌──────────────────────────────────────────────┐ │
         │  │ AMCACHE_HIVE                                  │ │
         │  │ BOOT_CONFIGURATION_DATA_TEMPLATE              │ │
         │  │ HKEY_LOCAL_MACHINE\BBI                        │ │
         │  │ HKEY_LOCAL_MACHINE\COMPONENTS                 │ │
         │  │ HKEY_LOCAL_MACHINE\DRIVERS                    │ │
         │  │ HKEY_LOCAL_MACHINE\ELAM                       │ │
         │  │ HKEY_LOCAL_MACHINE\SAM                        │ │
         │  │ HKEY_LOCAL_MACHINE\SCHEMA                     │ │
         │  │ HKEY_LOCAL_MACHINE\SECURITY                   │ │
         │  │ HKEY_LOCAL_MACHINE\SOFTWARE                   │ │
         │  │ HKEY_LOCAL_MACHINE\SYSTEM                     │ │
         │  │ HKEY_USERS\.DEFAULT                           │ │
         │  │ HKEY_USERS\Default                            │ │
         │  │ HKEY_USERS\LocalService                       │ │
         │  │ HKEY_USERS\NetworkService                     │ │
         │  │ HKEY_USERS\User                               │ │
         │  │ HKEY_USERS\User_Classes                       │ │
         │  └──────────────────────────────────────────────┘ │
         │                                                    │
         │        [ < Back ]  [ Next > ]  [ Cancel ]          │
         │                                                    │
         └────────────────────────────────────────────────────┘

1    2    3    4    5    6    7    8    9    10    11    12
```

6
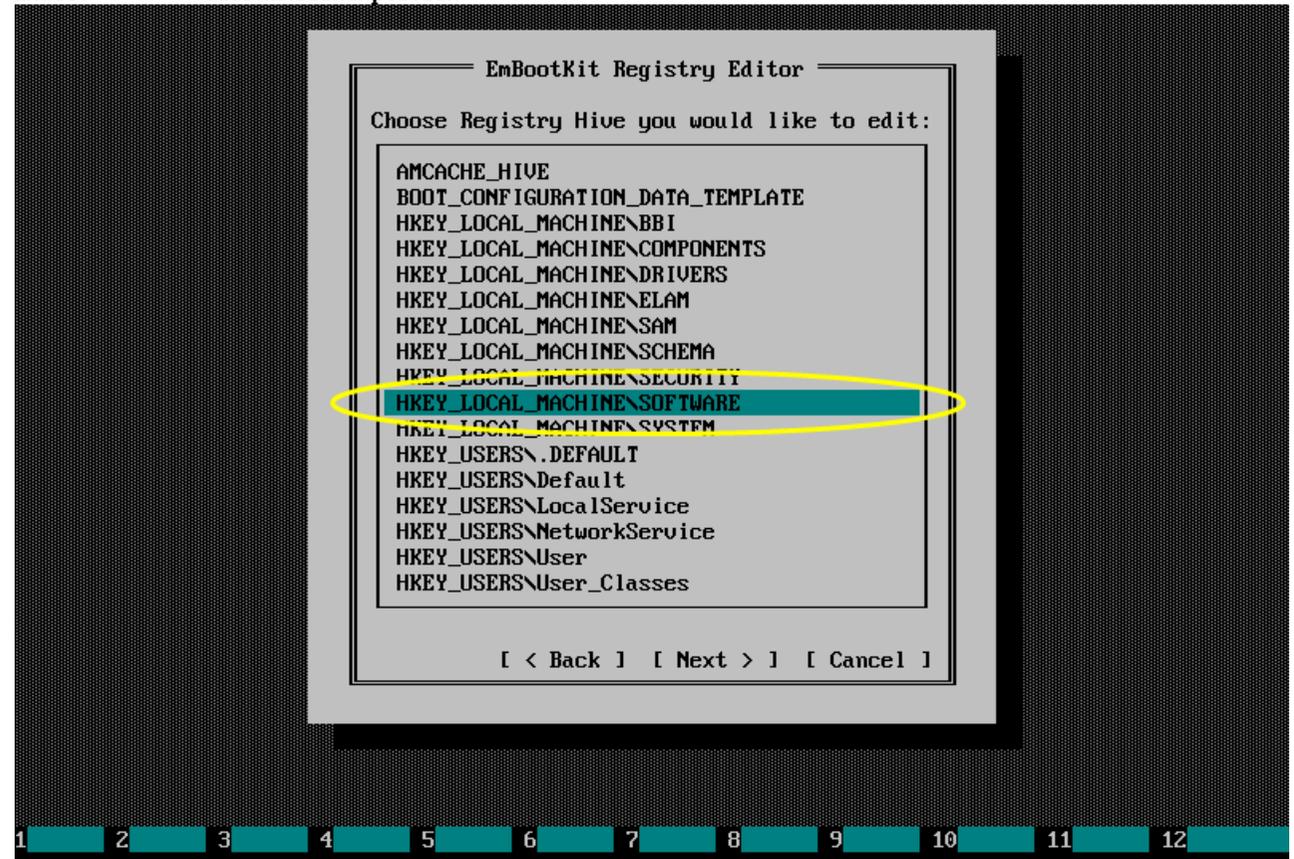
Alternatively, you can set the checkbox to override default options and specify custom filename of registry hive to edit.

```
Emergency Boot Kit version 1.6a (64-bit)

Registered to: User Name
Email:         username@example.com
```

```
┌───────────────────── EmBootKit Registry Editor ─────────────────────┐
│                                                                      │
│  Choose Windows installation to edit Registry for:                   │
│                                                                      │
│   ┌──────────────────┬───────────┬────────────────┬──────────────────┐ │
│   │       Disk       │ Disk Size │       OS       │ Installation Date │ │
│   ├──────────────────┼───────────┼────────────────┼──────────────────┤ │
│   │ D: System Reserved│  499 M    │ Boot Partition │ 26 Jul 2015       │ │
│ ▶ │ E:               │  50 G     │ Windows 10     │ 26 Jul 2015       │ ◀│
│                                                                      │
│   [x] I would like to override default options and                   │
│       specify custom filename of Registry Hive to edit               │
│                                                                      │
│                                            [ Next > ]   [ Cancel ]    │
└──────────────────────────────────────────────────────────────────────┘
```

```
1    2    3    4    5    6    7    8    9    10    11    12
```
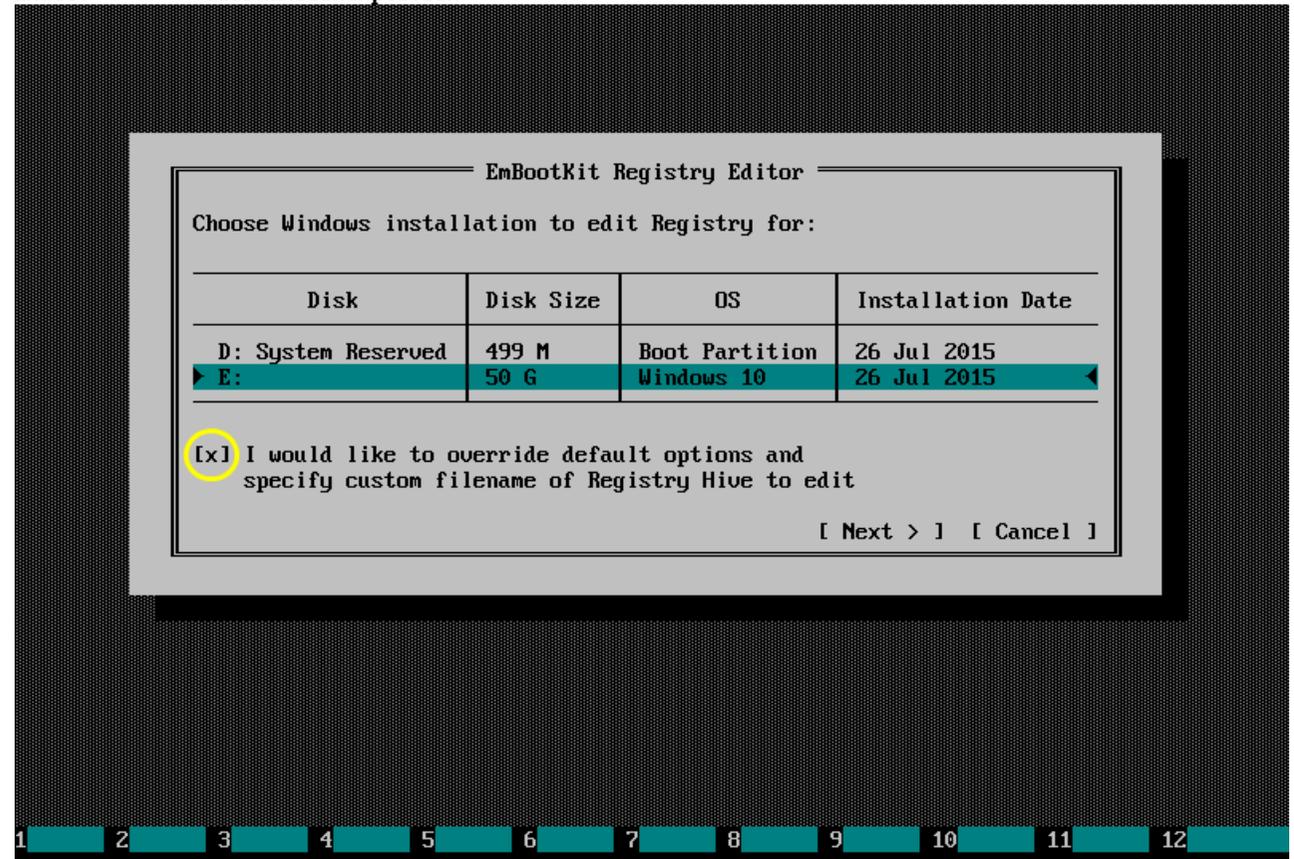
Then a file open dialog will be displayed. Here, using a mouse, you can choose arbitrary location of registry hive and its log (e.g. on the USB thumbdrive).

```
Emergency Boot Kit version 1.6a (64-bit)

Registered to: User Name
Email:         username@example.com
```

```
┌────────────────── EmBootKit Registry Editor ──────────────────┐
│                                                                │
│  Choose Registry Hive you would like to edit:                  │
│                                                                │
│  ◄  │D: HDD 500M│ │E: HDD 50G│ │F: HDD 29G│ │Z: Boot Ramdisk│  │
│     ┌──────────────────────────────────────┐                   │
│     │📂\                                   │                   │
│     │  📄Bin                               │                   │
│     │  📄Devices                           │                   │
│     │  📄KernelModules                     │                   │
│     │  📄Locales                           │                   │
│     │  📄Logs                              │                   │
│     │  📄SharedLibraries                   │                   │
│     │  📄_test                             │                   │
│     │                                      │                   │
│     │                                      │                   │
│     └──────────────────────────────────────┘                   │
│                                                                │
│                       [ < Back ]  [ Next > ]  [ Cancel ]       │
└────────────────────────────────────────────────────────────────┘
```

```
 1      2      3      4      5      6      7      8      9     10     11     12
```

8
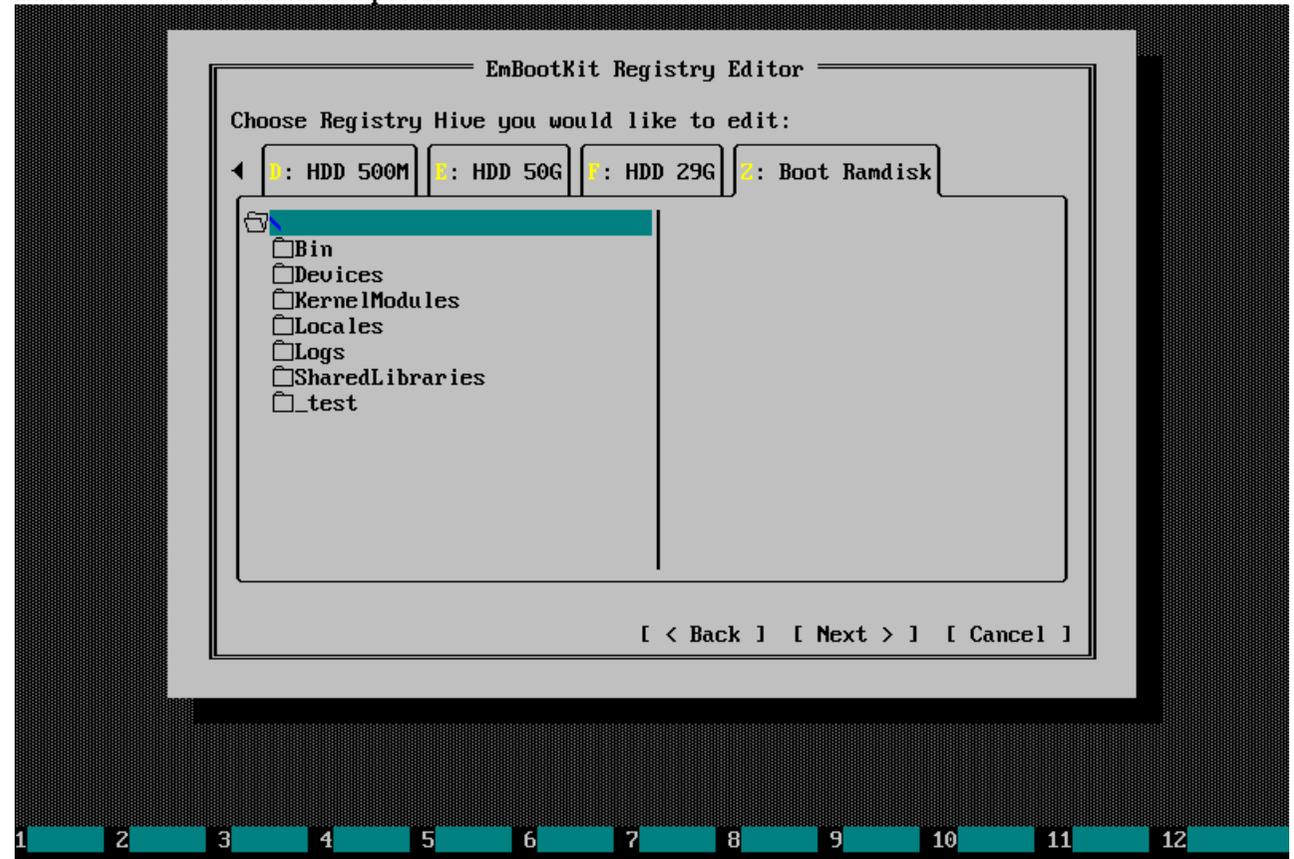
Regardless of the way registry hive was open, when Registry Editor loads it, you should see the screen like this.

```
[Windows 10 on disk E: 50G]\HKEY_LOCAL_MACHINE\SOFTWARE

 Classes                          Default Value:
 Clients                          Type:                         [▼]
 Dell                             Data:
 Intel
 Macromedia                       Edit blank fields below to create a new value:
 Microsoft                        Name:
 ODBC                             Type:                         [▼]
 OEM                              Data:
 Partner
 Policies                         To delete a value: clear its name, type and data
 RegisteredApplications
 Wow6432Node




 1        2Save   3Export 4Import 5Diff   6Rename 7Create 8Delete 9RawMod 10Exit  11      12Search
```

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.

```
[Windows 10 on disk E: 50G]\HKEY_LOCAL_MACHINE\SOFTWARE

Classes                              Default Value:
Clients                              Type:                          [▼]
Dell                                 Data:
Intel
Macromedia                           Edit blank fields below to create a new value:
Microsoft                            Name:
ODBC                                 Type:                          [▼]
OEM                                  Data:
Partner
Policies                             To delete a value: clear its name, type and data
RegisteredApplications
Wow6432Node

                       ═══ Registry Editor ═══
              You've made changes to the hive since the last save
                  Save     Don't save    Continue editing

1     2     3     4     5     6     7     8     9     10    11    12
```

10

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.

```
[Windows 10 on disk E: 50G]\HKEY_LOCAL_MACHINE\SOFTWARE

 Classes                           Default Value:
 Clients                           Type:                        [▼]
 Dell                              Data:
 Intel
 Macromedia                        Edit blank fields below to create a new value:
 Microsoft                         Name:
 ODBC                              Type:                        [▼]
 OEM                               Data:
 Partner
 Policies                          To delete a value: clear its name, type and data
 RegisteredApplications
 Wow6432Node


                          ╺═ Registry Editor ═╸
                          Postvalidating and saving registry hive
                             E:\Windows\System32\config\SOFTWARE




 1         2Save    3Export 4Import 5Diff    6Rename 7Create 8Delete 9RawMod 10Exit  11        12Search
```

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.

```
[Windows 10 on disk E: 50G]\HKEY_LOCAL_MACHINE\SOFTWARE
╔══════════════ \RegisteredApplications ══════════════╗   ╔══════════════ \RegisteredApplications ══════════════╗
║..                                                   ║   ║Default Value:                                       ▲
║                                                     ║   ║Type:                                          [▼]   ║
║                                                     ║   ║Data:                                                ║
║                                                     ║   ║                                                     ║
║                                                     ║   ║Value #1:                                            ║
║                                                     ║   ║Name: File Explorer                                  ║
║                                                     ║   ║Type: REG_SZ                                   [▼]   ║
║                                                     ║   ║Data: SOFTWARE\Microsoft\Windows\CurrentVersion\    ║
║                                                     ║   ║      Explorer\Capabilities                          ║
║                                                     ║   ║                                                     ║
║                                                     ║   ║Value #2:                                            ║
║                                                     ║   ║Name: Internet Explorer                              ║
║                                                     ║   ║Type: REG_SZ                                   [▼]   ║
║                                                     ║   ║Data: SOFTWARE\Microsoft\Internet Explorer\Capab    ║
║                                                     ║   ║      ilities                                        ║
║                                                     ║   ║                                                     ║
║                                                     ║   ║Value #3:                                            ║
║                                                     ║   ║Name: Paint                                          ║
║                                                     ║   ║Type: REG_SZ                                   [▼]   ║
║                                                     ║   ║Data: SOFTWARE\Microsoft\Windows\CurrentVersion\    ║
║                                                     ║   ║      Applets\Paint\Capabilities                     ║
║                                                     ║   ║                                                     ║
║                                                     ║   ║Value #4:                                            ║
║                                                     ║   ║Name: Windows Address Book                           ║
║                                                     ║   ║Type: REG_SZ                                   [▼]   ║
║                                                     ║   ║Data: Software\Clients\Contacts\Address Book\Cap    ║
║                                                     ║   ║      abilities                                      ║
║                                                     ║   ║                                                     ║
║                                                     ║   ║Value #5:                                            ║
║                                                     ║   ║Name: Windows Disc Image Burner                      ║
║                                                     ║   ║Type: REG_SZ                                   [▼]   ║
║                                                     ║   ║Data: Software\Microsoft\IsoBurn\Capabilities        ▼
╚═════════════════════════════════════════════════════╝   ╚═════════════════════════════════════════════════════╝
1        2Save    3Export 4Import 5Diff   6Rename 7Create 8Delete 9RawMod 10Exit  11         12Search
```

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*.

13
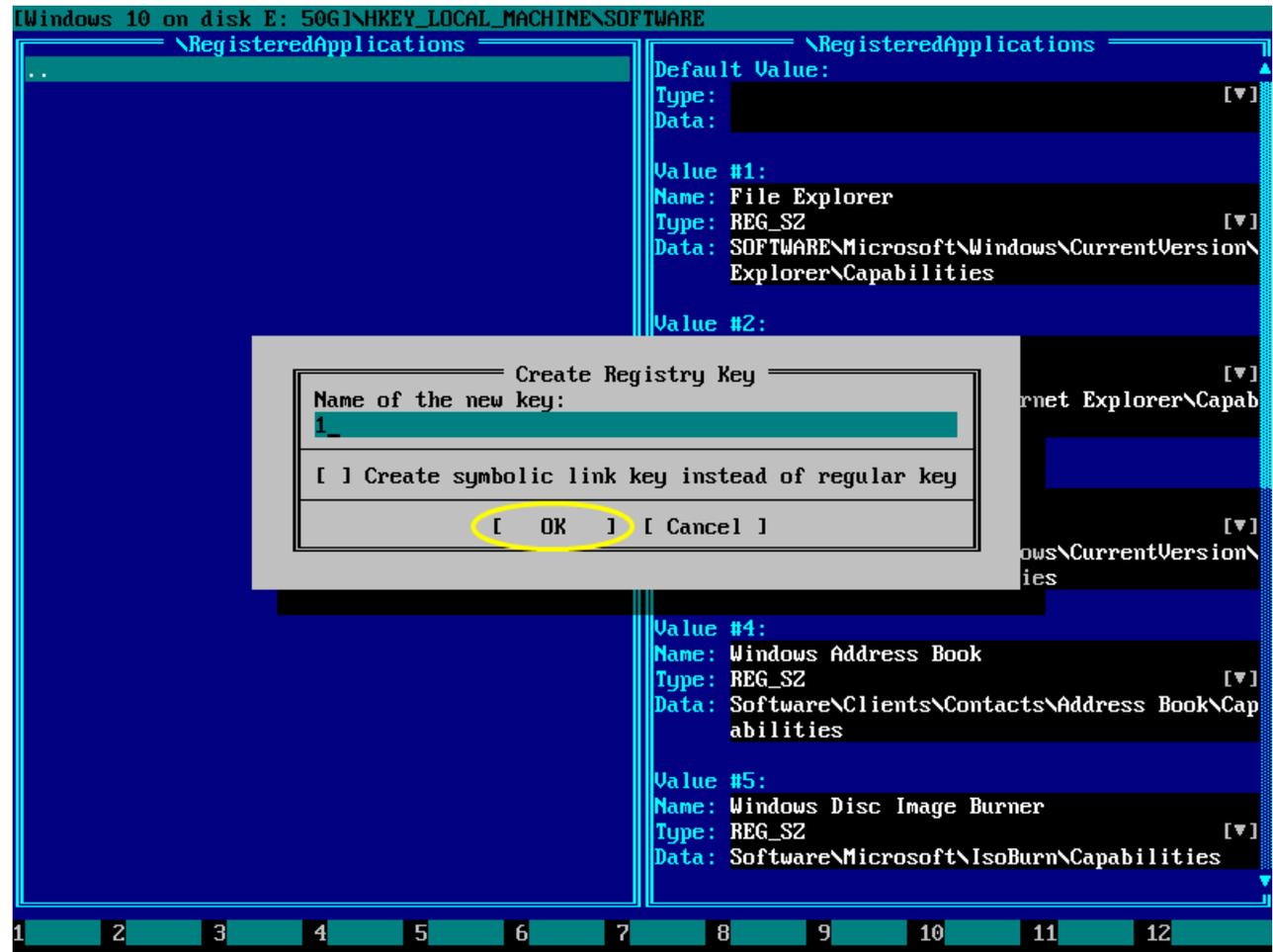
New key with specified name has been created.

```
[Windows 10 on disk E: 50G]\HKEY_LOCAL_MACHINE\SOFTWARE
┌─────────── \RegisteredApplications ──────────┐  ┌─────────── \RegisteredApplications ──────────┐
│                                              │  │Default Value:                                │▲
│ 1                                            │  │Type:                                     [▼]│
│                                              │  │Data:                                         │
│                                              │  │                                              │
│                                              │  │Value #1:                                     │
│                                              │  │Name: File Explorer                           │
│                                              │  │Type: REG_SZ                              [▼]│
│                                              │  │Data: SOFTWARE\Microsoft\Windows\CurrentVersion\│
│                                              │  │      Explorer\Capabilities                   │
│                                              │  │                                              │
│                                              │  │Value #2:                                     │
│                                              │  │Name: Internet Explorer                       │
│                                              │  │Type: REG_SZ                              [▼]│
│                                              │  │Data: SOFTWARE\Microsoft\Internet Explorer\Capab│
│                                              │  │      ilities                                 │
│                                              │  │                                              │
│                                              │  │Value #3:                                     │
│                                              │  │Name: Paint                                   │
│                                              │  │Type: REG_SZ                              [▼]│
│                                              │  │Data: SOFTWARE\Microsoft\Windows\CurrentVersion\│
│                                              │  │      Applets\Paint\Capabilities              │
│                                              │  │                                              │
│                                              │  │Value #4:                                     │
│                                              │  │Name: Windows Address Book                    │
│                                              │  │Type: REG_SZ                              [▼]│
│                                              │  │Data: Software\Clients\Contacts\Address Book\Cap│
│                                              │  │      abilities                               │
│                                              │  │                                              │
│                                              │  │Value #5:                                     │
│                                              │  │Name: Windows Disc Image Burner               │
│                                              │  │Type: REG_SZ                              [▼]│
│                                              │  │Data: Software\Microsoft\IsoBurn\Capabilities │▼
└──────────────────────────────────────────────┘  └──────────────────────────────────────────────┘
1        2Save    3Export 4Import 5Diff    6Rename 7Create 8Delete 9RawMod 10Exit  11        12Search
```
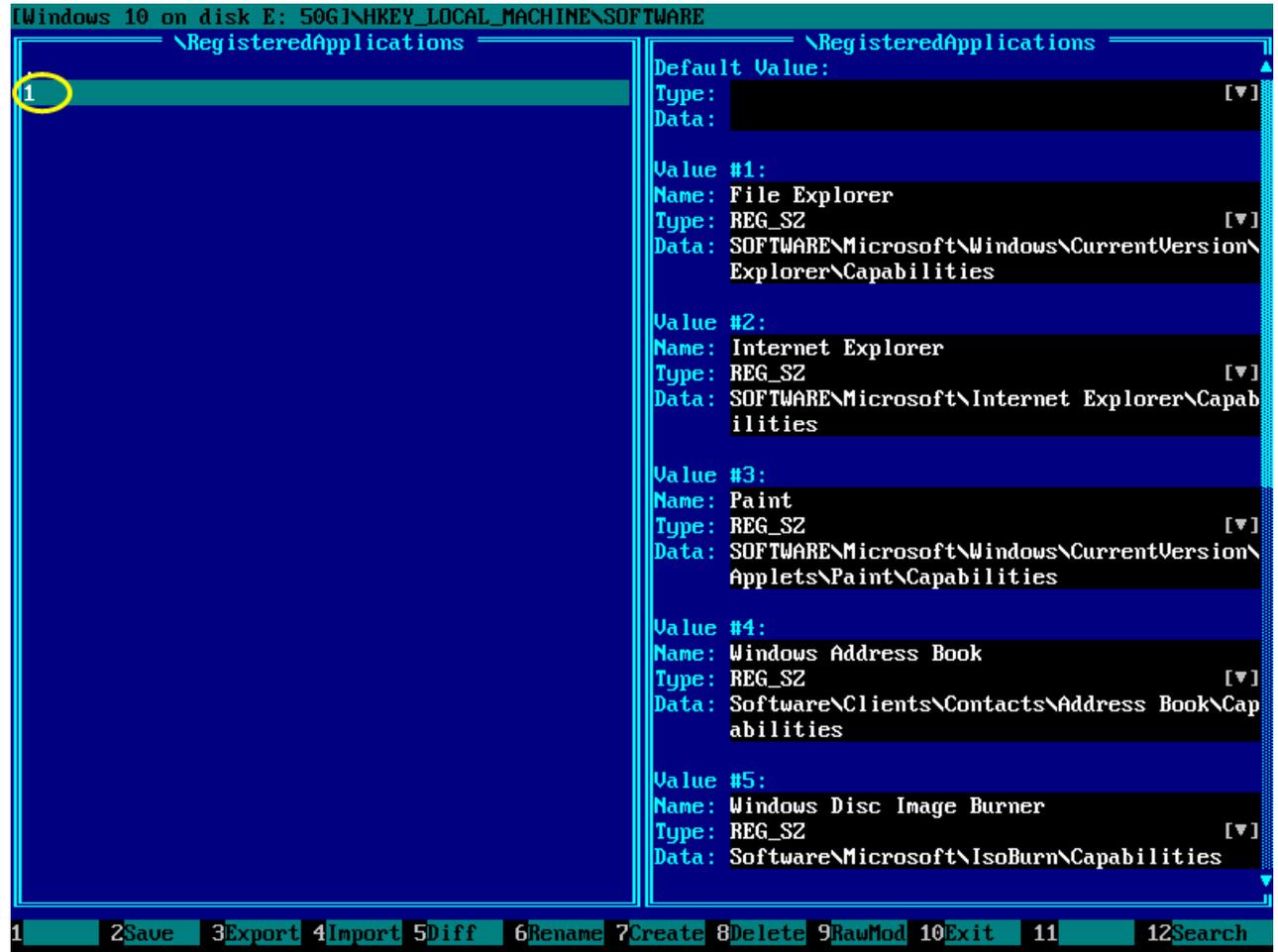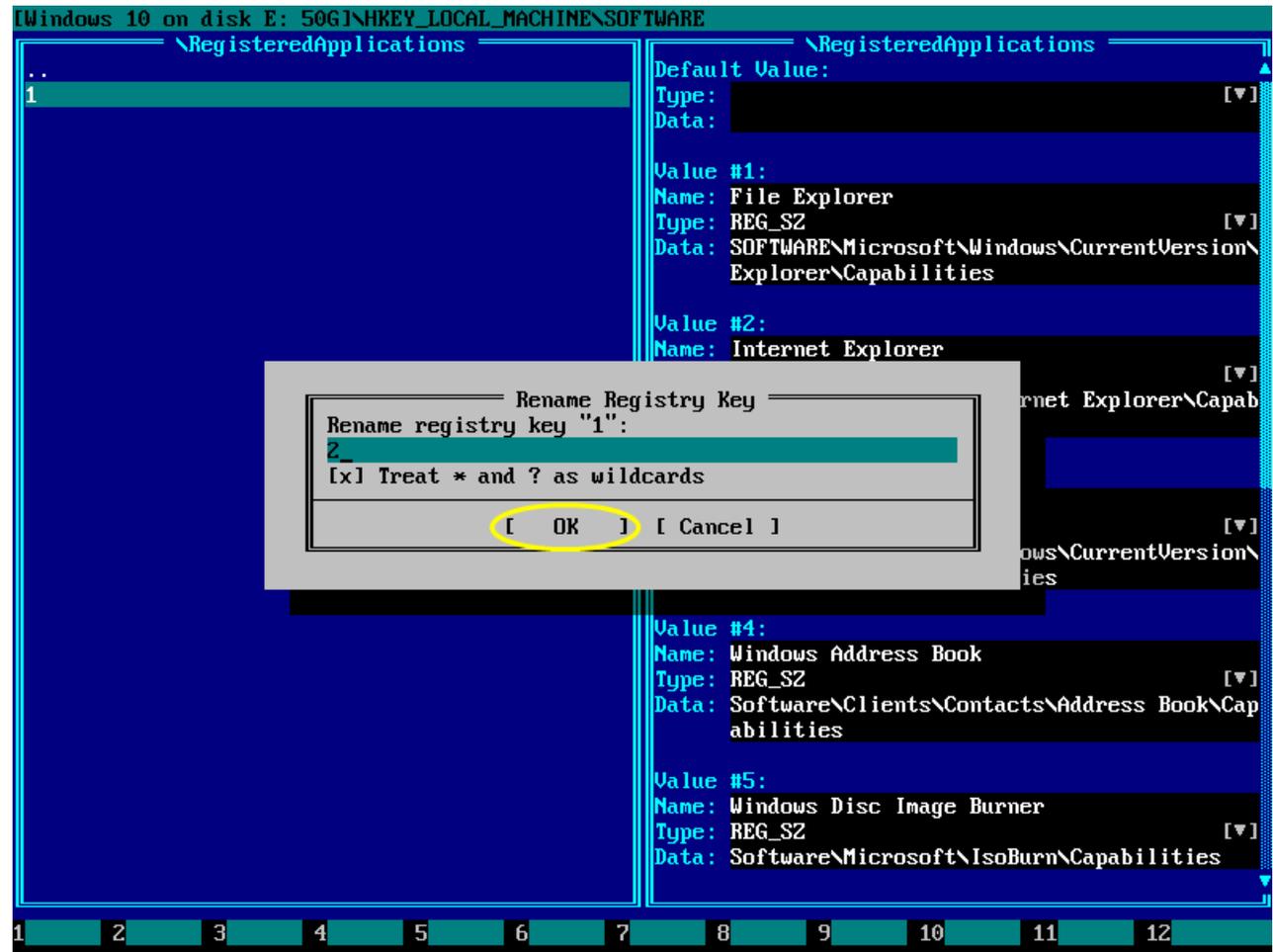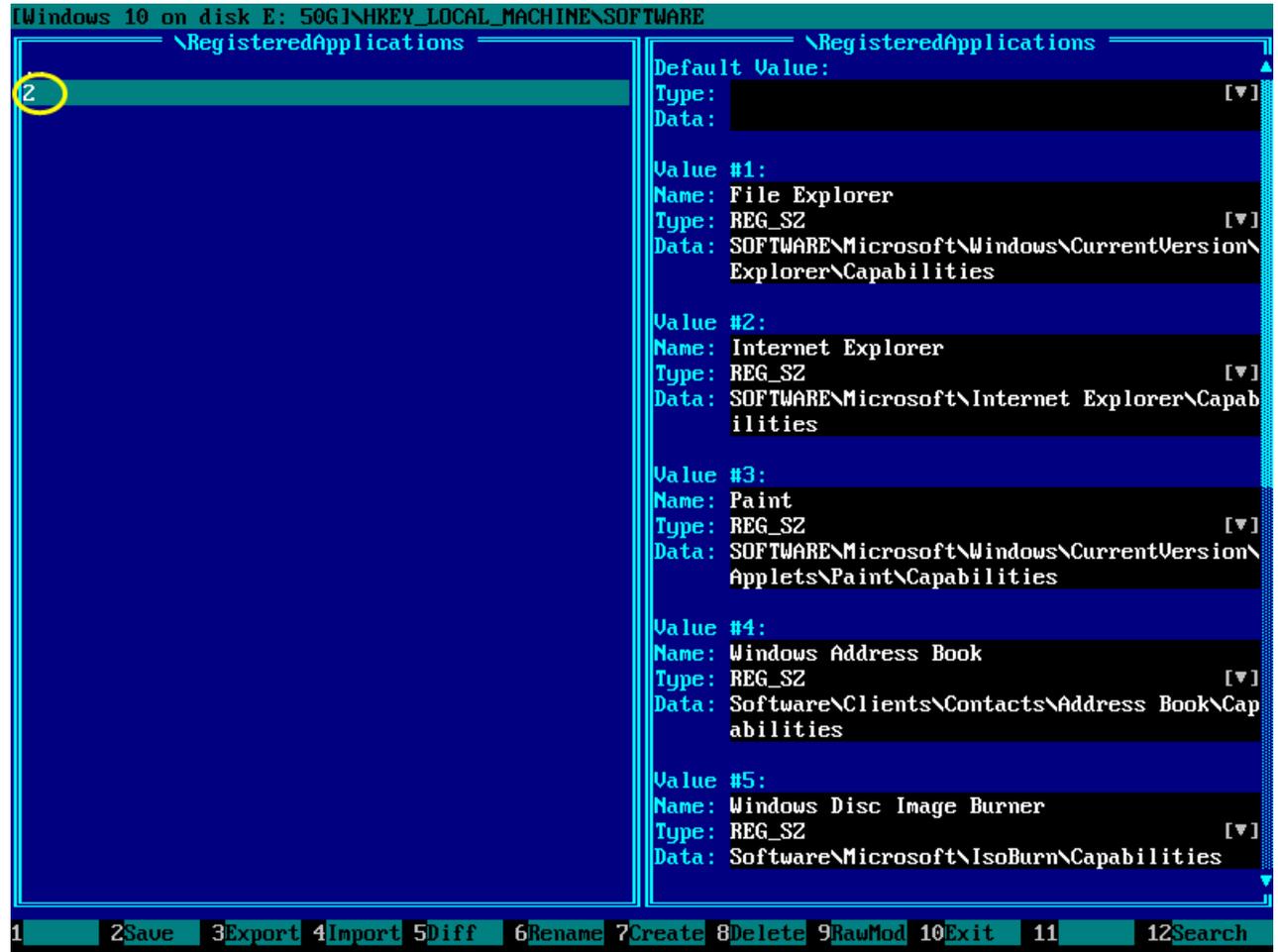
3.6. Rename registry key

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*.

```
[Windows 10 on disk E: 50G]\HKEY_LOCAL_MACHINE\SOFTWARE
       \RegisteredApplications            \RegisteredApplications
..                                  Default Value:
1                                   Type:                        [▼]
                                    Data:

                                    Value #1:
                                    Name: File Explorer
                                    Type: REG_SZ                  [▼]
                                    Data: SOFTWARE\Microsoft\Windows\CurrentVersion\
                                          Explorer\Capabilities

                                    Value #2:
                                    Name: Internet Explorer
                                                                 [▼]
                    Rename Registry Key            rnet Explorer\Capab
         Rename registry key "1":
         2_
         [x] Treat * and ? as wildcards

              [   OK   ]  [ Cancel ]                              [▼]
                                          ows\CurrentVersion\
                                          ies

                                    Value #4:
                                    Name: Windows Address Book
                                    Type: REG_SZ                  [▼]
                                    Data: Software\Clients\Contacts\Address Book\Cap
                                          abilities

                                    Value #5:
                                    Name: Windows Disc Image Burner
                                    Type: REG_SZ                  [▼]
                                    Data: Software\Microsoft\IsoBurn\Capabilities

  1      2      3      4      5      6      7      8      9     10    11    12
```
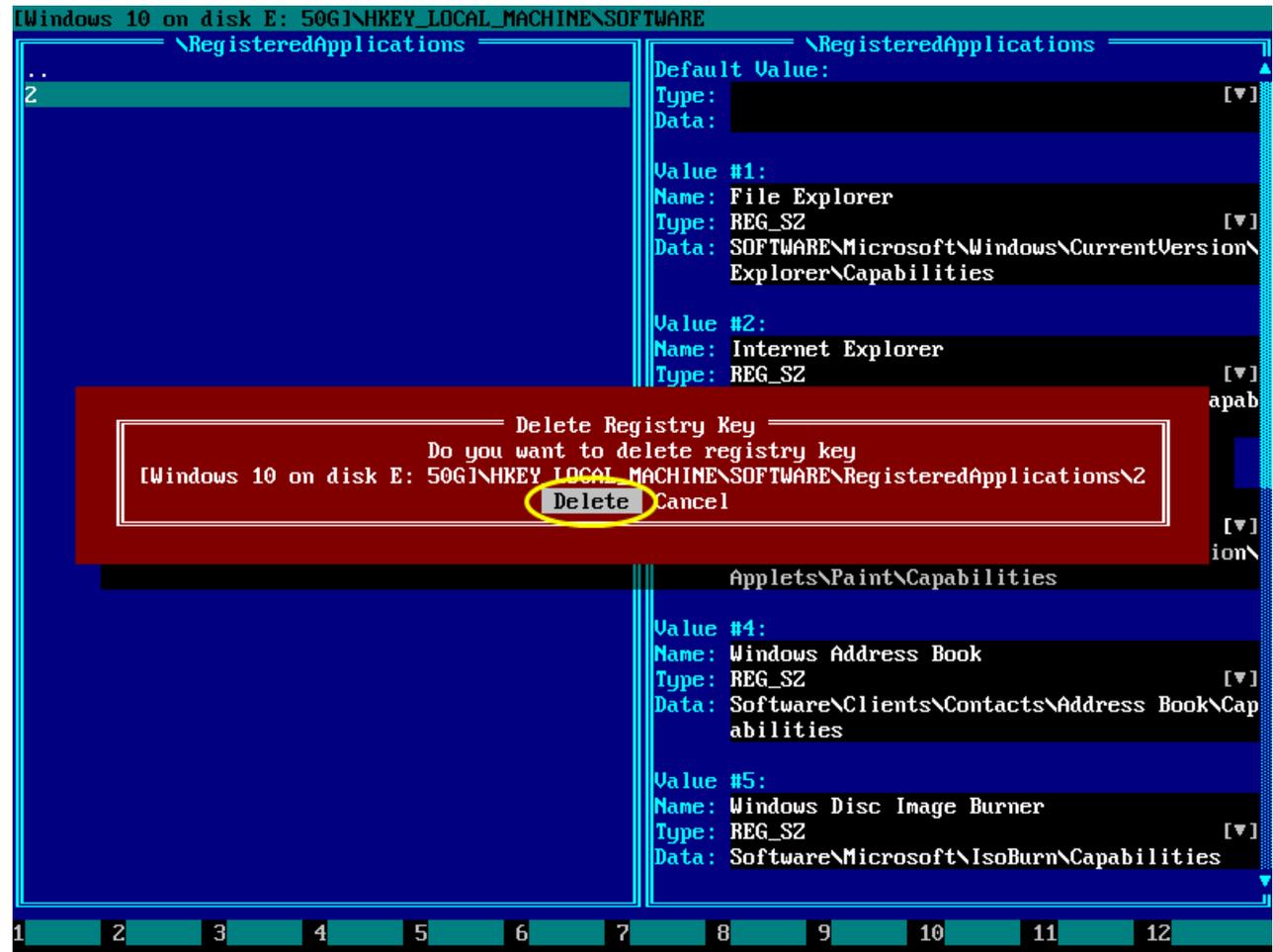
15

A key has been renamed.

```
[Windows 10 on disk E: 50G]\HKEY_LOCAL_MACHINE\SOFTWARE
═══ \RegisteredApplications ═══          ═══ \RegisteredApplications ═══
                                         Default Value:
 2                                       Type:                         [▼]
                                         Data:

                                         Value #1:
                                         Name: File Explorer
                                         Type: REG_SZ                  [▼]
                                         Data: SOFTWARE\Microsoft\Windows\CurrentVersion\
                                               Explorer\Capabilities

                                         Value #2:
                                         Name: Internet Explorer
                                         Type: REG_SZ                  [▼]
                                         Data: SOFTWARE\Microsoft\Internet Explorer\Capab
                                               ilities

                                         Value #3:
                                         Name: Paint
                                         Type: REG_SZ                  [▼]
                                         Data: SOFTWARE\Microsoft\Windows\CurrentVersion\
                                               Applets\Paint\Capabilities

                                         Value #4:
                                         Name: Windows Address Book
                                         Type: REG_SZ                  [▼]
                                         Data: Software\Clients\Contacts\Address Book\Cap
                                               abilities

                                         Value #5:
                                         Name: Windows Disc Image Burner
                                         Type: REG_SZ                  [▼]
                                         Data: Software\Microsoft\IsoBurn\Capabilities

1        2Save    3Export 4Import 5Diff    6Rename 7Create 8Delete 9RawMod 10Exit  11        12Search
```
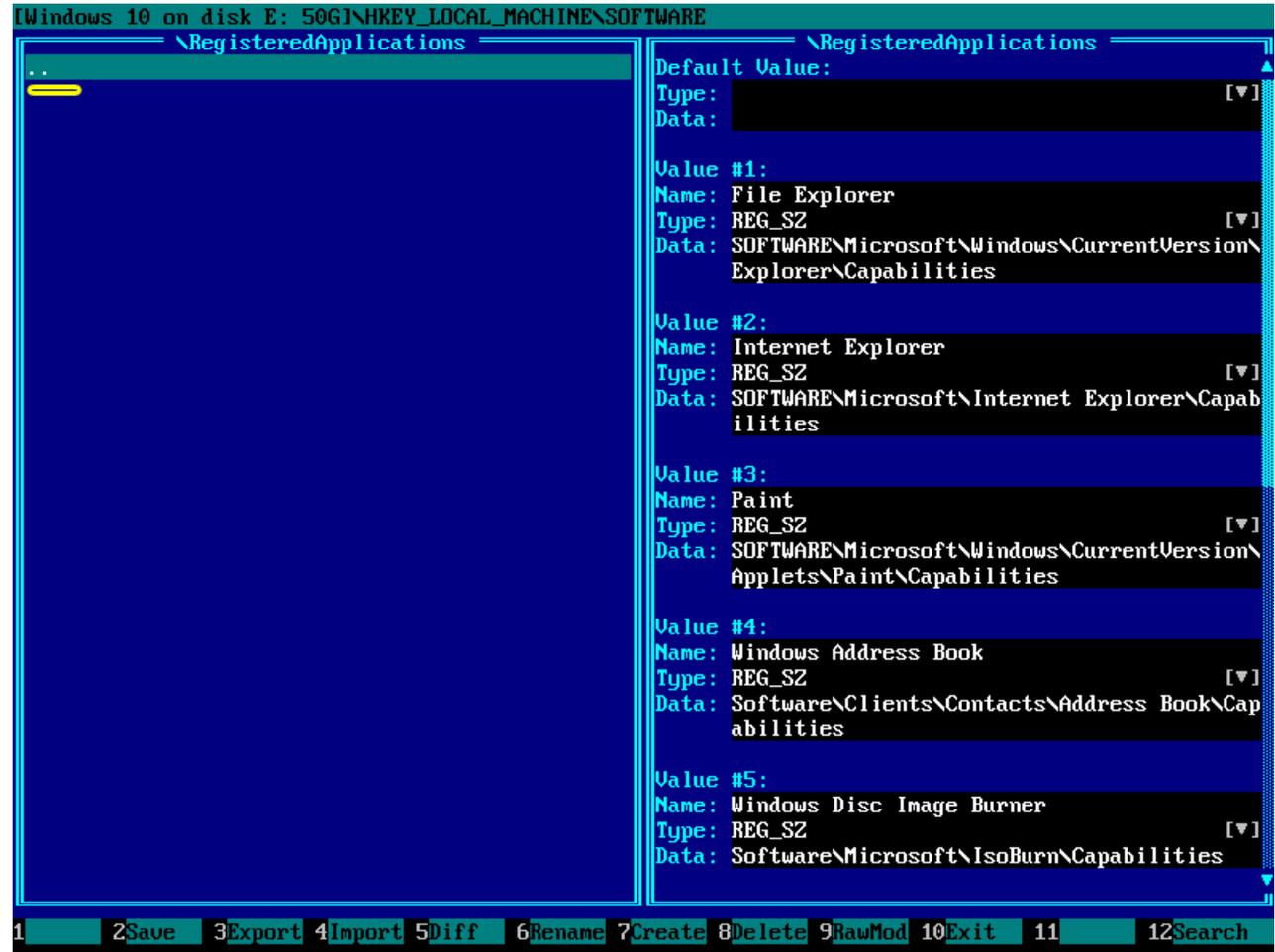
3.7. Delete registry key

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*.
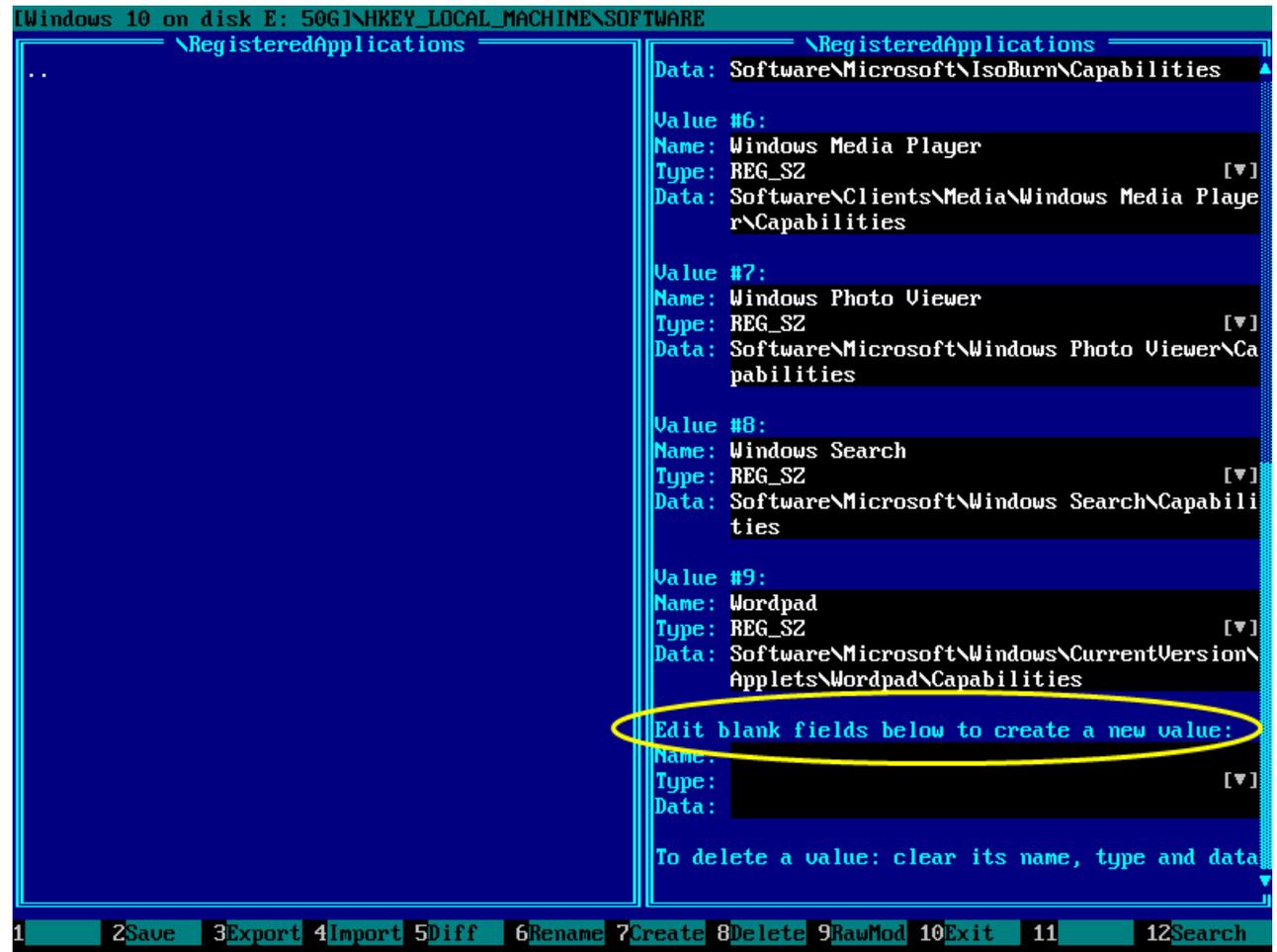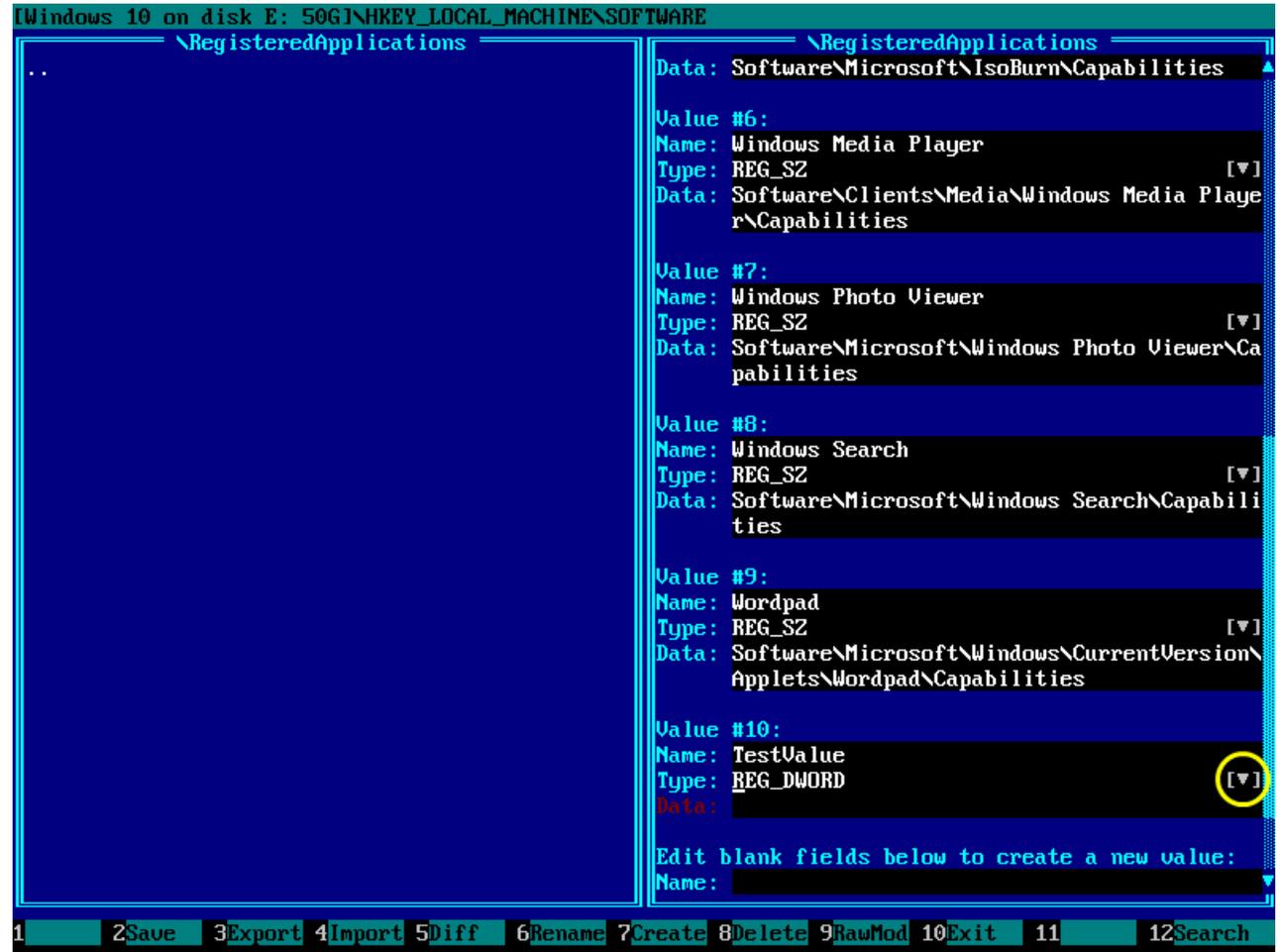
A key has been deleted.

```
[Windows 10 on disk E: 50G]\HKEY_LOCAL_MACHINE\SOFTWARE
┌──────────── \RegisteredApplications ────────────┐  ┌──────────── \RegisteredApplications ────────────┐
│..                                                │  │Default Value:                                    ▲
│                                                  │  │Type:                                        [▼]  │
│                                                  │  │Data:                                             │
│                                                  │  │                                                  │
│                                                  │  │Value #1:                                         │
│                                                  │  │Name: File Explorer                               │
│                                                  │  │Type: REG_SZ                                 [▼]  │
│                                                  │  │Data: SOFTWARE\Microsoft\Windows\CurrentVersion\  │
│                                                  │  │      Explorer\Capabilities                       │
│                                                  │  │                                                  │
│                                                  │  │Value #2:                                         │
│                                                  │  │Name: Internet Explorer                           │
│                                                  │  │Type: REG_SZ                                 [▼]  │
│                                                  │  │Data: SOFTWARE\Microsoft\Internet Explorer\Capab  │
│                                                  │  │      ilities                                     │
│                                                  │  │                                                  │
│                                                  │  │Value #3:                                         │
│                                                  │  │Name: Paint                                       │
│                                                  │  │Type: REG_SZ                                 [▼]  │
│                                                  │  │Data: SOFTWARE\Microsoft\Windows\CurrentVersion\  │
│                                                  │  │      Applets\Paint\Capabilities                  │
│                                                  │  │                                                  │
│                                                  │  │Value #4:                                         │
│                                                  │  │Name: Windows Address Book                        │
│                                                  │  │Type: REG_SZ                                 [▼]  │
│                                                  │  │Data: Software\Clients\Contacts\Address Book\Cap  │
│                                                  │  │      abilities                                   │
│                                                  │  │                                                  │
│                                                  │  │Value #5:                                         │
│                                                  │  │Name: Windows Disc Image Burner                   │
│                                                  │  │Type: REG_SZ                                 [▼]  │
│                                                  │  │Data: Software\Microsoft\IsoBurn\Capabilities     ▼
└──────────────────────────────────────────────────┘  └──────────────────────────────────────────────────┘
1        2Save    3Export 4Import 5Diff    6Rename 7Create 8Delete 9RawMod 10Exit   11        12Search
```

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.

```
[Windows 10 on disk E: 50G]\HKEY_LOCAL_MACHINE\SOFTWARE
╔════════ \RegisteredApplications ════════╗ ╔═════════ \RegisteredApplications ════════╗
║..                                        ║ ║Data: Software\Microsoft\IsoBurn\Capabilities  ▲
║                                          ║ ║
║                                          ║ ║Value #6:
║                                          ║ ║Name: Windows Media Player
║                                          ║ ║Type: REG_SZ                          [▼]
║                                          ║ ║Data: Software\Clients\Media\Windows Media Playe
║                                          ║ ║      r\Capabilities
║                                          ║ ║
║                                          ║ ║Value #7:
║                                          ║ ║Name: Windows Photo Viewer
║                                          ║ ║Type: REG_SZ                          [▼]
║                                          ║ ║Data: Software\Microsoft\Windows Photo Viewer\Ca
║                                          ║ ║      pabilities
║                                          ║ ║
║                                          ║ ║Value #8:
║                                          ║ ║Name: Windows Search
║                                          ║ ║Type: REG_SZ                          [▼]
║                                          ║ ║Data: Software\Microsoft\Windows Search\Capabili
║                                          ║ ║      ties
║                                          ║ ║
║                                          ║ ║Value #9:
║                                          ║ ║Name: Wordpad
║                                          ║ ║Type: REG_SZ                          [▼]
║                                          ║ ║Data: Software\Microsoft\Windows\CurrentVersion\
║                                          ║ ║      Applets\Wordpad\Capabilities
║                                          ║ ║
║                                          ║ ║Edit blank fields below to create a new value:
║                                          ║ ║Name:
║                                          ║ ║Type:                                 [▼]
║                                          ║ ║Data:
║                                          ║ ║
║                                          ║ ║To delete a value: clear its name, type and data
╚══════════════════════════════════════════╝ ╚═══════════════════════════════════════════╝
 1        2Save    3Export 4Import 5Diff   6Rename 7Create 8Delete 9RawMod 10Exit  11        12Search
```

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.

```
[Windows 10 on disk E: 50G]\HKEY_LOCAL_MACHINE\SOFTWARE
        \RegisteredApplications                    \RegisteredApplications
..                                    Data: Software\Microsoft\IsoBurn\Capabilities  ▲

                                      Value #6:
                                      Name: Windows Media Player
                                      Type: REG_SZ                            [▼]
                                      Data: Software\Clients\Media\Windows Media Playe
                                            r\Capabilities

                                      Value #7:
                                      Name: Windows Photo Viewer
                                      Type: REG_SZ                            [▼]
                                      Data: Software\Microsoft\Windows Photo Viewer\Ca
                                            pabilities

                                      Value #8:
                                      Name: Windows Search
                                      Type: REG_SZ                            [▼]
                                      Data: Software\Microsoft\Windows Search\Capabili
                                            ties

                                      Value #9:
                                      Name: Wordpad
                                      Type: REG_SZ                            [▼]
                                      Data: Software\Microsoft\Windows\CurrentVersion\
                                            Applets\Wordpad\Capabilities

                                      Value #10:
                                      Name: TestValue
                                      Type: REG_DWORD                         [▼]
                                      Data:

                                      Edit blank fields below to create a new value:
                                      Name:                                      ▼
1        2Save   3Export 4Import 5Diff    6Rename 7Create 8Delete 9RawMod 10Exit  11        12Search
```

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.

```
[Windows 10 on disk E: 50G]\HKEY_LOCAL_MACHINE\SOFTWARE
═══ \RegisteredApplications ═══        ═══ \RegisteredApplications ═══
..                                     Data: Software\Microsoft\IsoBurn\Capabilities

                                       Value #6:
                                       Name: Windows Media Player
                                       Type: REG_SZ                          [▼]
                                       Data: Software\Clients\Media\Windows Media Playe
                                             r\Capabilities

                                       Value #7:
                                       Name: Windows Photo Viewer
                                       Type: REG_SZ                          [▼]
                                       Data: Software\Microsoft\Windows Photo Viewer\Ca
                                             pabilities

                                       Value #8:
                                       Name: Windows Search
                                       Type: REG_SZ                          [▼]
                                       Data: Software\Microsoft\Windows Search\Capabili
                                             ties

                                       Value #9:
                                       Name: Wordpad
                                       Type: REG_SZ                          [▼]
                                       Data: Software\Microsoft\Windows\CurrentVersion\
                                             Applets\Wordpad\Capabilities

                                       Value #10:
                                       Name: TestValue
                                       Type: REG_DWORD                       [▼]
                                       Data: 1_

                                       Edit blank fields below to create a new value:
                                       Name:
 1        2Save    3Export 4Import 5Diff    6Rename 7Create 8Delete 9RawMod 10Exit  11        12Search
```

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.

```
[Windows 10 on disk E: 50G]\HKEY_LOCAL_MACHINE\SOFTWARE
========= \RegisteredApplications =========        ====== \RegisteredApplications ======
..                                          Data: Software\Clients\Media\Windows Media Playe▲
                                                  r\Capabilities

                                            Value #7:
                                            Name: Windows Photo Viewer
                                            Type: REG_SZ                              [▼]
                                            Data: Software\Microsoft\Windows Photo Viewer\Ca
                                                  pabilities

                                            Value #8:
                                            Name: Windows Search
                                            Type: REG_SZ                              [▼]
                                            Data: Software\Microsoft\Windows Search\Capabili
                                                  ties

                                            Value #9:
                                            Name: Wordpad
                                            Type: REG_SZ                              [▼]
                                            Data: Software\Microsoft\Windows\CurrentVersion\
                                                  Applets\Wordpad\Capabilities

                                            Value #10:
                                            Name: TestValue
                                            Type: REG_DWORD                           [▼]
                                            Data: 2_

                                            Edit blank fields below to create a new value:
                                            Name:
                                            Type:                                     [▼]
                                            Data:

                                            To delete a value: clear its name, type and data

1        2Save    3Export 4Import 5Diff    6Rename 7Create 8Delete 9RawMod 10Exit  11      12Search
```

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.

23
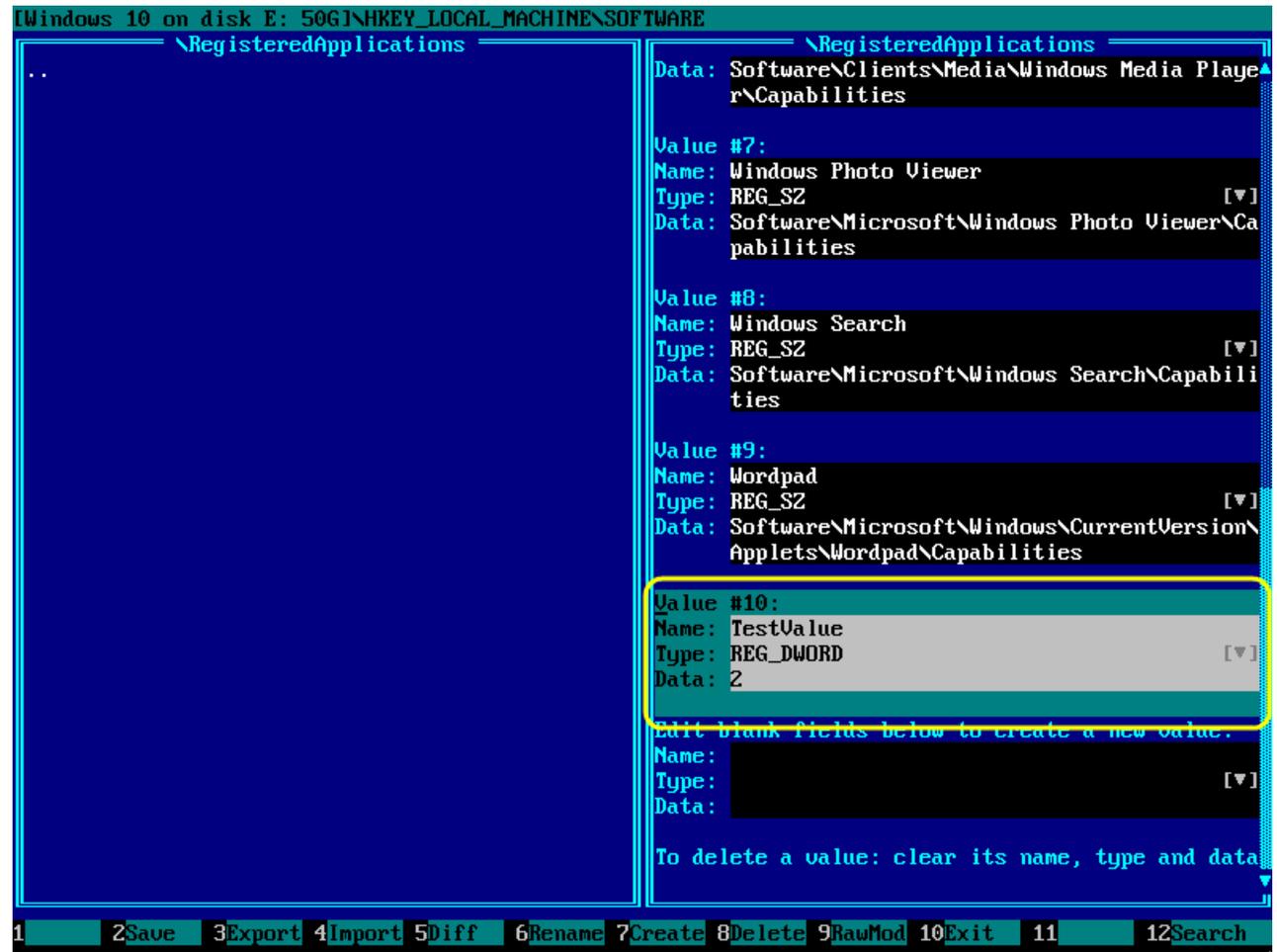
3.11. Copy or move registry value(s) between two keys via the clipboard

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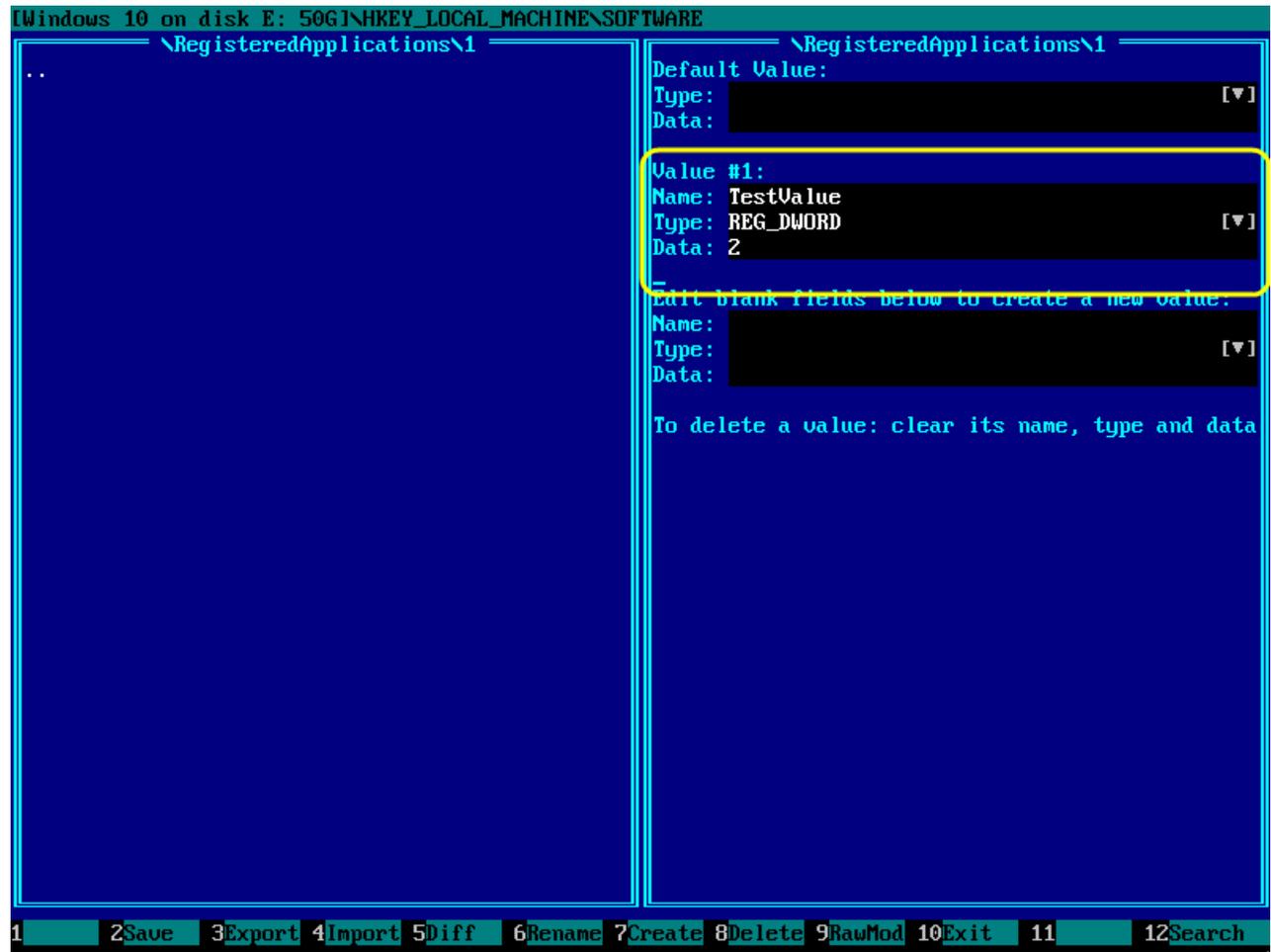
3.12. Edit key class name and other properties in the raw mode

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

```
[Windows 10 on disk E: 50G]\HKEY_LOCAL_MACHINE\SOFTWARE
╔════════ \RegisteredApplications\1 ════════╗ ╔════════ \RegisteredApplications\1 ════════╗
║..                                         ║ ║Default Value:                             ║
║                                           ║ ║Type:                                  [▼]  ║
║                                           ║ ║Data:                                      ║
║                                           ║ ║                                           ║
║                                           ║ ║Value #1:                                  ║
║                                           ║ ║Name: TestValue                            ║
║                                           ║ ║Type: REG_DWORD                        [▼]  ║
║                                           ║ ║Data: 2                                    ║
║                                           ║ ║                                           ║
║                                           ║ ║Edit blank fields below to create a new value: ║
║                                           ║ ║Name:                                      ║
║                                           ║ ║Type:                                  [▼]  ║
║                                           ║ ║Data:                                      ║
║                                           ║ ║                                           ║
║                                           ║ ║To delete a value: clear its name, type and data ║
║                                           ║ ║                                           ║
╚═══════════════════════════════════════════╝ ╚═══════════════════════════════════════════╝
1      2Save    3Export 4Import 5Diff    6Rename 7Create 8Delete 9RawMod 10Exit  11      12Search
```
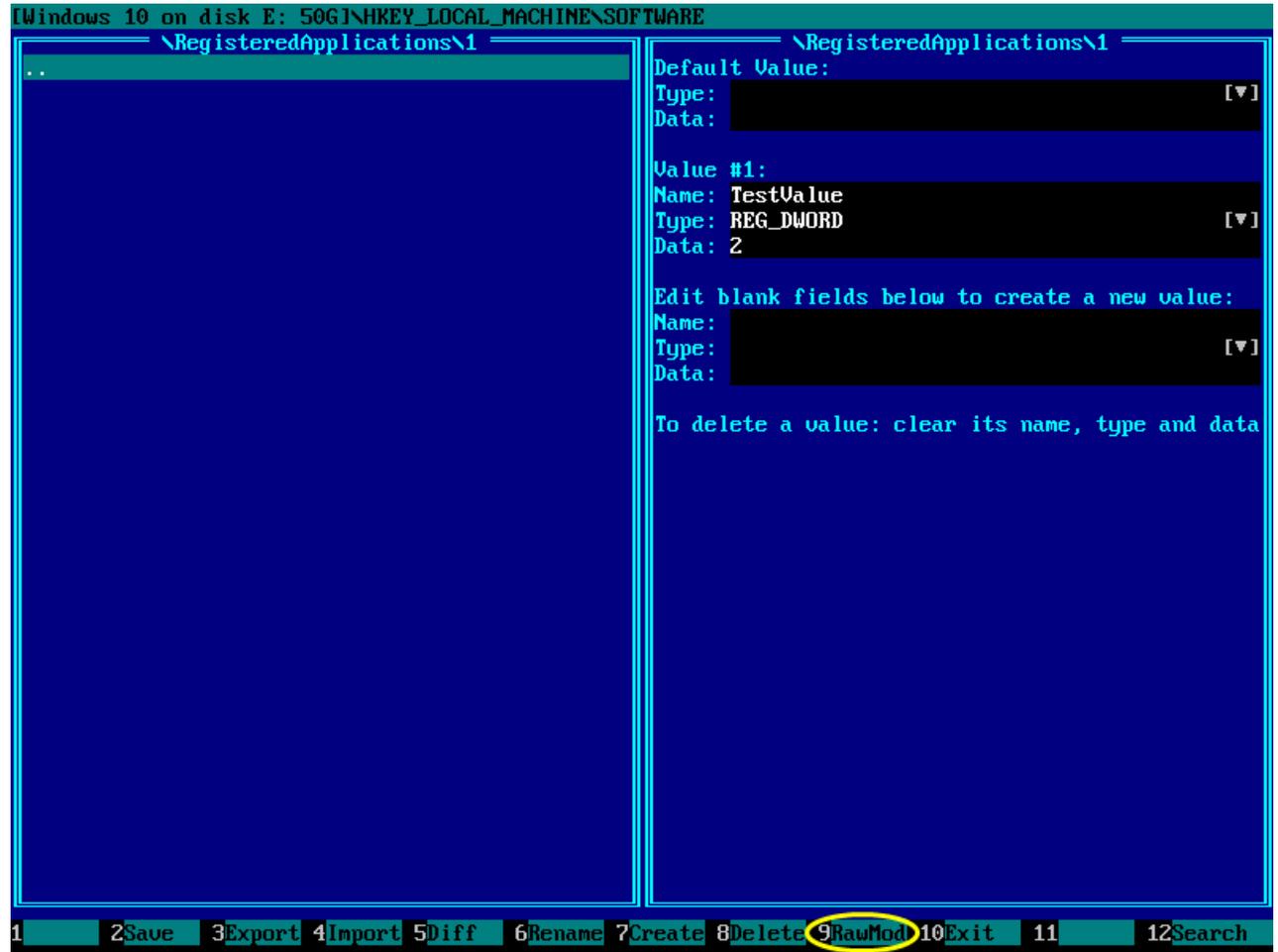
Right panel will switch into the raw mode (much more detailed than standard mode).

You can use **F9** at any moment to switch back to standard mode.
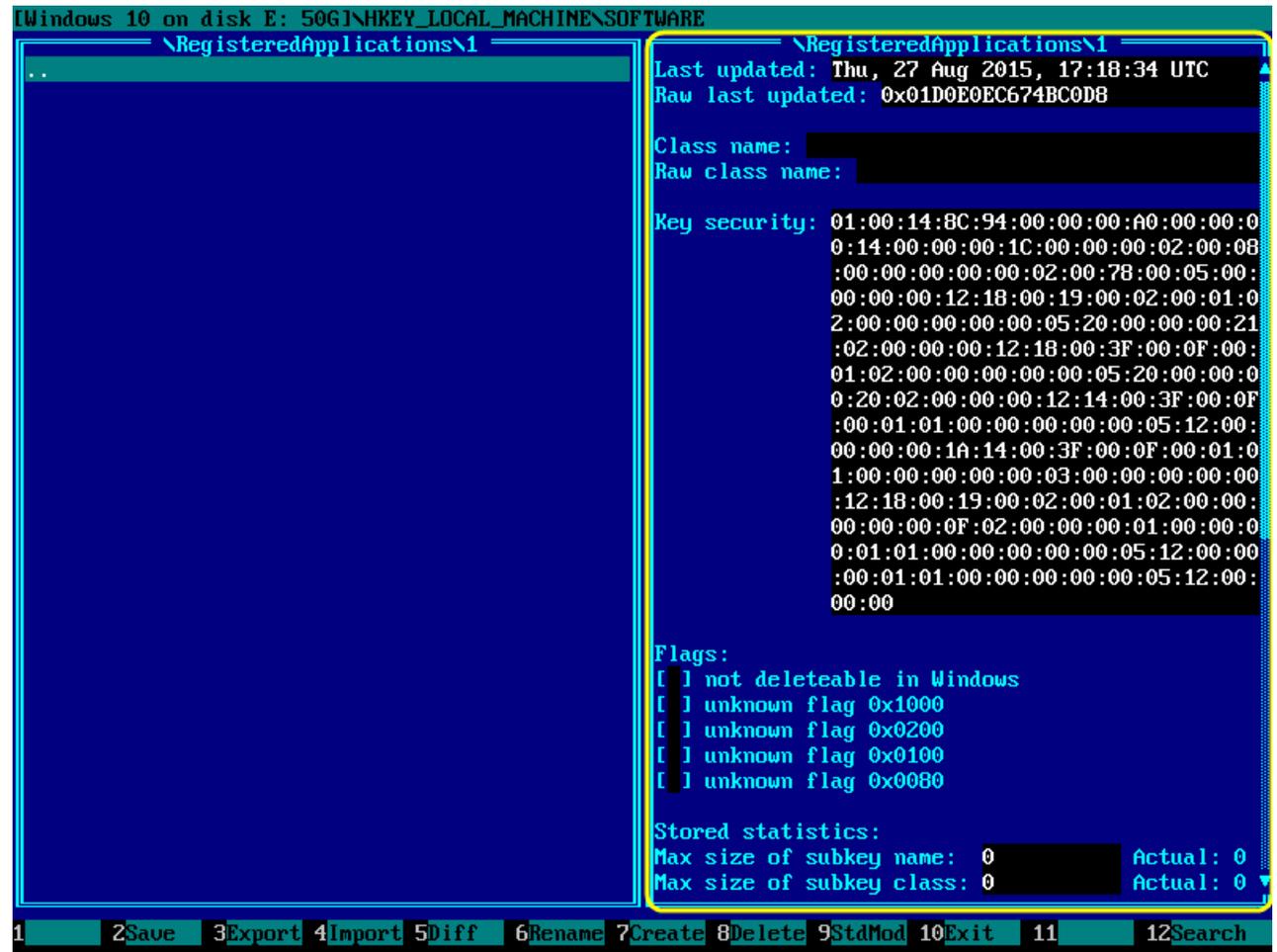
```
[Windows 10 on disk E: 50G]\HKEY_LOCAL_MACHINE\SOFTWARE
════ \RegisteredApplications\1 ════         ════ \RegisteredApplications\1 ════
..                                          Last updated: Thu, 27 Aug 2015, 17:18:34 UTC
                                            Raw last updated: 0x01D0E0EC674BC0D8

                                            Class name:
                                            Raw class name:

                                            Key security: 01:00:14:8C:94:00:00:00:A0:00:00:0
                                                          0:14:00:00:00:1C:00:00:00:02:00:08
                                                          :00:00:00:00:00:02:00:78:00:05:00:
                                                          00:00:00:12:18:00:19:00:02:00:01:0
                                                          2:00:00:00:00:00:05:20:00:00:00:21
                                                          :02:00:00:00:12:18:00:3F:00:0F:00:
                                                          01:02:00:00:00:00:00:05:20:00:00:0
                                                          0:20:02:00:00:00:12:14:00:3F:00:0F
                                                          :00:01:01:00:00:00:00:00:05:12:00:
                                                          00:00:00:1A:14:00:3F:00:0F:00:01:0
                                                          1:00:00:00:00:00:03:00:00:00:00:00
                                                          :12:18:00:19:00:02:00:01:02:00:00:
                                                          00:00:00:0F:02:00:00:00:01:00:00:0
                                                          0:01:01:00:00:00:00:00:05:12:00:00
                                                          :00:01:01:00:00:00:00:00:05:12:00:
                                                          00:00

                                            Flags:
                                            [ ] not deleteable in Windows
                                            [ ] unknown flag 0x1000
                                            [ ] unknown flag 0x0200
                                            [ ] unknown flag 0x0100
                                            [ ] unknown flag 0x0080

                                            Stored statistics:
                                            Max size of subkey name:  0        Actual: 0
                                            Max size of subkey class: 0        Actual: 0
1        2Save    3Export 4Import 5Diff    6Rename 7Create 8Delete 9StdMod 10Exit  11        12Search
```
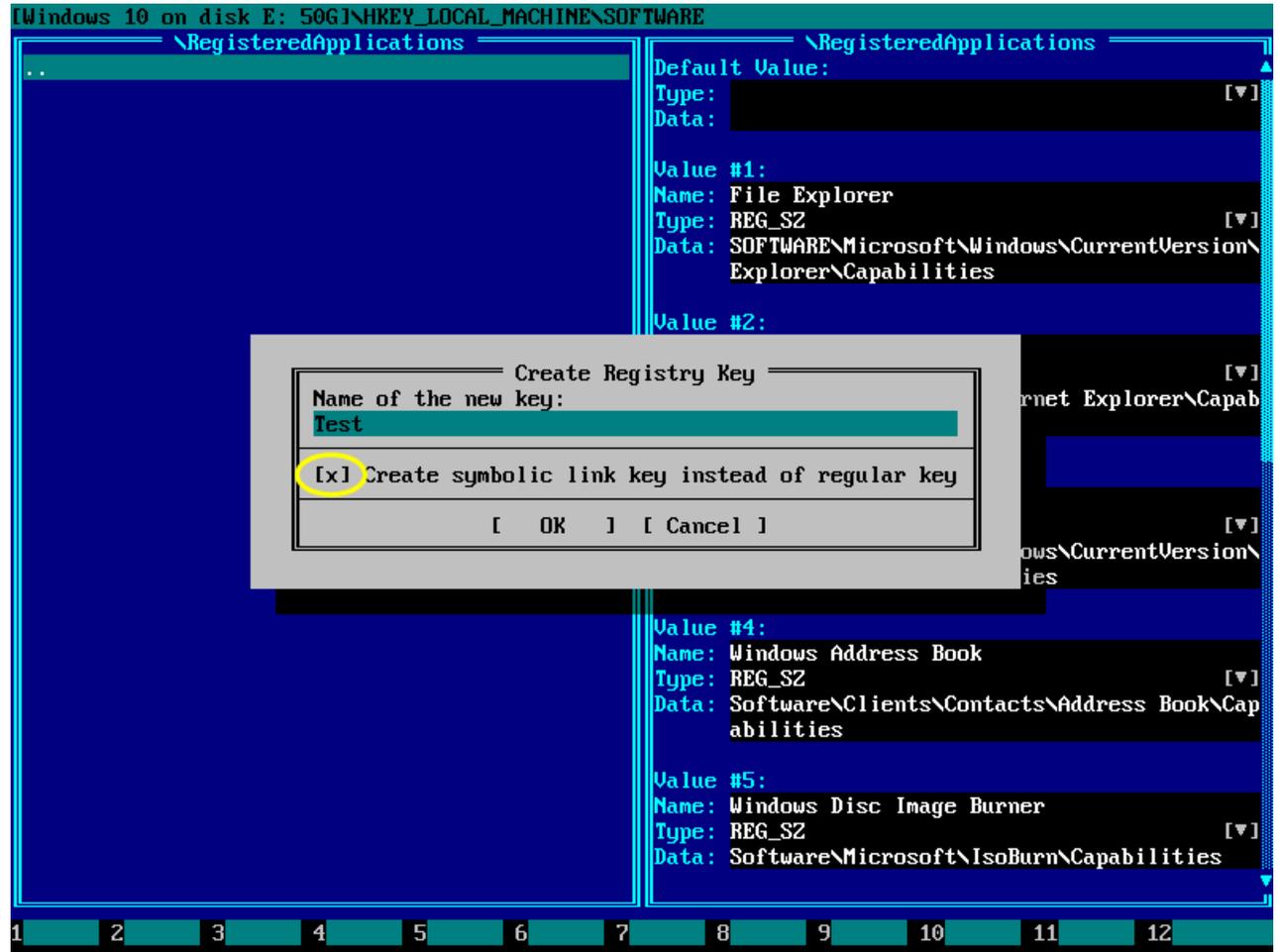
Press **Tab** to make right panel active.

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.

```
[Windows 10 on disk E: 50G]\HKEY_LOCAL_MACHINE\SOFTWARE
========= \RegisteredApplications\1 =========        ======== \RegisteredApplications\1 ========
..                                                   Last updated: Thu, 27 Aug 2015, 17:18:34 UTC
                                                     Raw last updated: 0x01D0E0EC674BC0D8

                                                     Class name: myclassname_
                                                     Raw class name: 006D:0079:0063:006C:0061:0073:00
                                                                     73:006E:0061:006D:0065

                                                     Key security: 01:00:14:8C:94:00:00:00:A0:00:00:0
                                                                   0:14:00:00:00:1C:00:00:00:02:00:08
                                                                   :00:00:00:00:00:02:00:78:00:05:00:
                                                                   00:00:00:12:18:00:19:00:02:00:01:0
                                                                   2:00:00:00:00:00:05:20:00:00:00:21
                                                                   :02:00:00:00:12:18:00:3F:00:0F:00:
                                                                   01:02:00:00:00:00:00:05:20:00:00:0
                                                                   0:20:02:00:00:00:12:14:00:3F:00:0F
                                                                   :00:01:01:00:00:00:00:00:05:12:00:
                                                                   00:00:00:1A:14:00:3F:00:0F:00:01:0
                                                                   1:00:00:00:00:00:03:00:00:00:00:00
                                                                   :12:18:00:19:00:02:00:01:02:00:00:
                                                                   00:00:00:0F:02:00:00:00:01:00:00:0
                                                                   0:01:01:00:00:00:00:00:05:12:00:00
                                                                   :00:01:01:00:00:00:00:00:05:12:00:
                                                                   00:00

                                                     Flags:
                                                     [ ] not deleteable in Windows
                                                     [ ] unknown flag 0x1000
                                                     [ ] unknown flag 0x0200
                                                     [ ] unknown flag 0x0100
                                                     [ ] unknown flag 0x0080

                                                     Stored statistics:
                                                     Max size of subkey name:  0            Actual: 0
1        2Save    3Export 4Import 5Diff    6Rename 7Create 8Delete 9StdMod 10Exit   11         12Search
```

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.

```
[Windows 10 on disk E: 50G]\HKEY_LOCAL_MACHINE\SOFTWARE
┌───────── \RegisteredApplications ─────────┐  ┌────────── \RegisteredApplications ──────────
..                                              Default Value:
                                                Type:                              [▼]
                                                Data:

                                                Value #1:
                                                Name: File Explorer
                                                Type: REG_SZ                       [▼]
                                                Data: SOFTWARE\Microsoft\Windows\CurrentVersion\
                                                      Explorer\Capabilities

                                                Value #2:
                    ┌─────────── Create Registry Key ───────────┐              [▼]
                    │ Name of the new key:                      │   rnet Explorer\Capab
                    │ Test                                      │
                    │                                           │
                    │ [x] Create symbolic link key instead of regular key │
                    │                                           │
                    │        [   OK   ]  [ Cancel ]             │              [▼]
                    └───────────────────────────────────────────┘   ows\CurrentVersion\
                                                                 ies

                                                Value #4:
                                                Name: Windows Address Book
                                                Type: REG_SZ                       [▼]
                                                Data: Software\Clients\Contacts\Address Book\Cap
                                                      abilities

                                                Value #5:
                                                Name: Windows Disc Image Burner
                                                Type: REG_SZ                       [▼]
                                                Data: Software\Microsoft\IsoBurn\Capabilities

 1      2      3      4      5      6      7      8      9      10     11     12
```

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**).
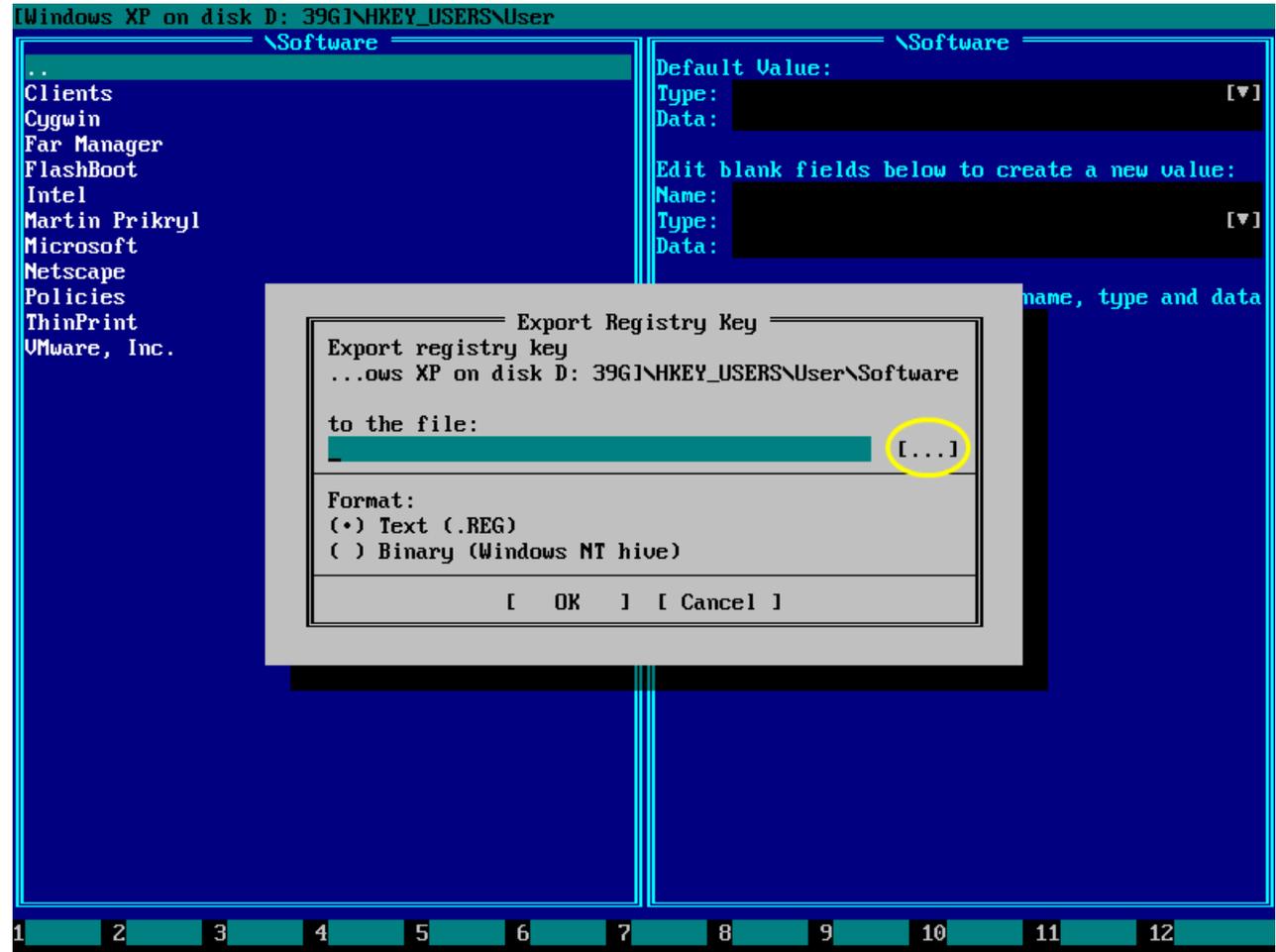
```
[Windows 10 on disk E: 50G]\HKEY_LOCAL_MACHINE\SOFTWARE
┌─────── \RegisteredApplications\Test ───────┐┌────── \RegisteredApplications\Test ──────┐
│..                                          ││Symbolic link target:                     │
│                                            ││                                          │
│                                            ││                                          │
│                                            ││                                          │
│                                            ││                                          │
│                                            ││                                          │
└────────────────────────────────────────────┘└──────────────────────────────────────────┘
 1       2Save    3Export 4Import 5Diff    6Rename 7Create 8Delete 9RawMod 10Exit  11        12Search
```
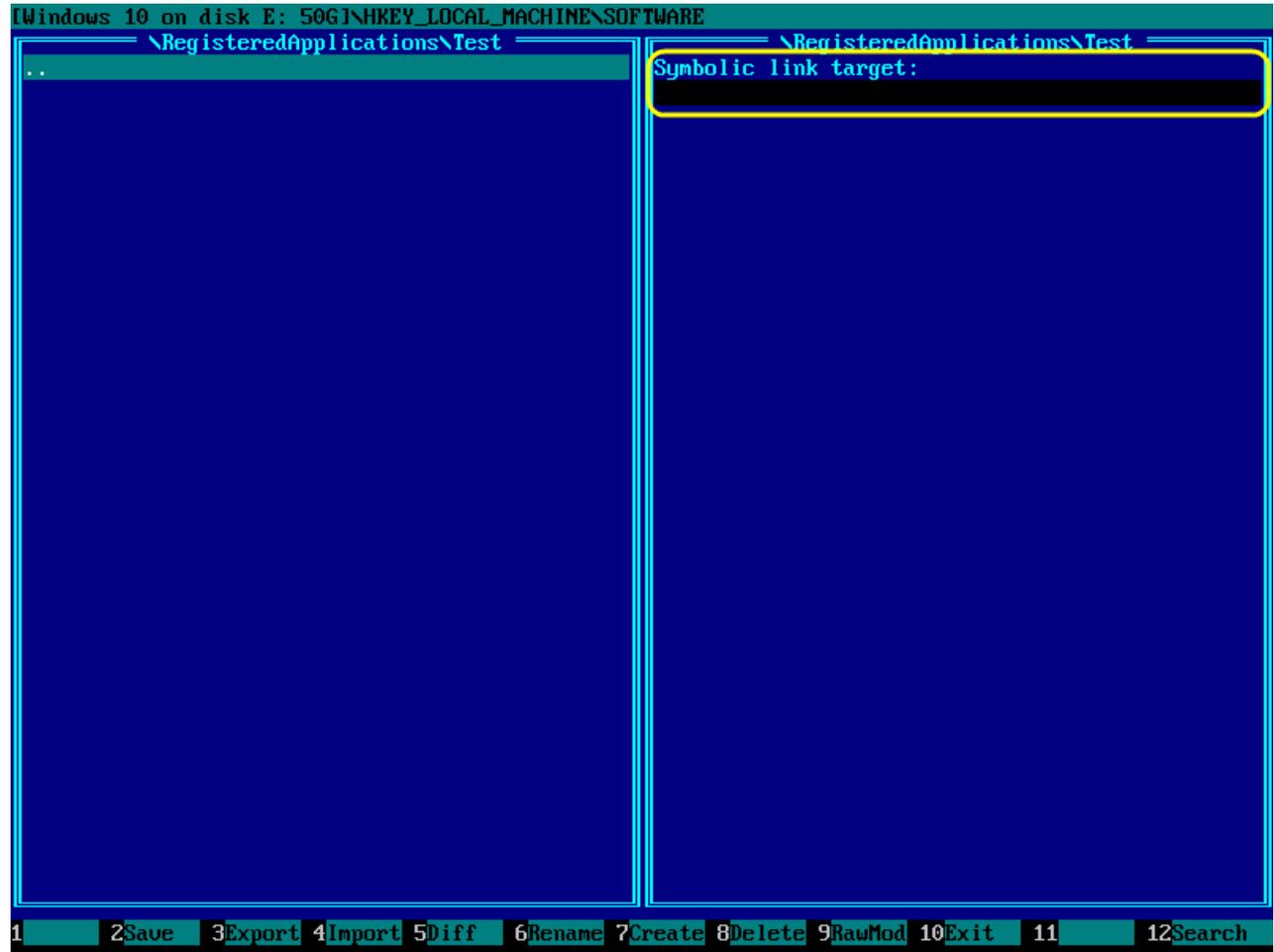
3.14. Export registry key with subkeys and values

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

```
[Windows XP on disk D: 39G]\HKEY_USERS\User
┌──────────────────\Software─────────────────┐  ┌─────────────────\Software─────────────────┐
│..                                           │  │Default Value:                             │
│Clients                                      │  │Type:                                [▼]   │
│Cygwin                                       │  │Data:                                      │
│Far Manager                                  │  │                                           │
│FlashBoot                                    │  │Edit blank fields below to create a new value:│
│Intel                                        │  │Name:                                      │
│Martin Prikryl                               │  │Type:                                [▼]   │
│Microsoft                                    │  │Data:                                      │
│Netscape                                     │  │                                           │
│Policies                                     │  │To delete a value: clear its name, type and data│
│ThinPrint                                    │  │                                           │
│VMware, Inc.                                 │  │                                           │
│                                             │  │                                           │
└─────────────────────────────────────────────┘  └───────────────────────────────────────────┘
1       2Save   3Export 4Import 5Diff   6Rename 7Create 8Delete 9RawMod 10Exit 11        12Search
```
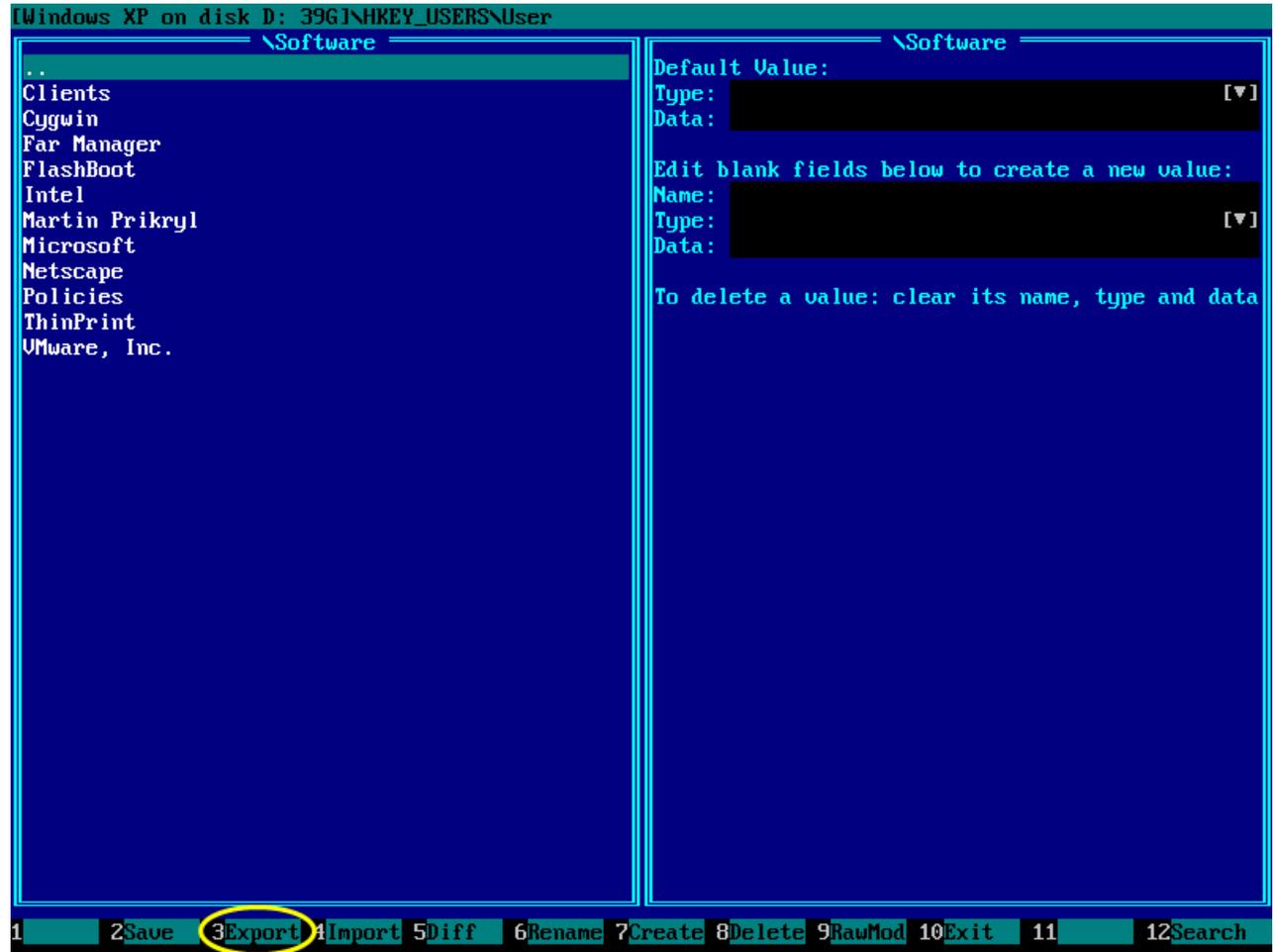
Popup window like this will be shown on the screen. You may type the file name or click *[...]* button to open file save window.

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

```
[Windows XP on disk D: 39G]\HKEY_USERS\User
                    \Software                                           \Software
..                                               Default Value:
Clients                                          Type:                            [▼]
Cygwin                                           Data:
Far Manager
FlashBoot                                        Edit blank fields below to create a new value:
Intel                                            Name:
Martin Prikryl                                   Type:                            [▼]
Microsoft                                        Data:
Netscape
Policies                                                       name, type and data
ThinPrint
VMware, Inc.           ═══════ Export Registry Key ═══════
                     Export registry key
                     ...ows XP on disk D: 39G]\HKEY_USERS\User\Software

                     to the file:
                     _                                         [...]

                     Format:
                     (•) Text (.REG)
                     ( ) Binary (Windows NT hive)

                            [   OK   ]  [ Cancel ]



 1      2       3       4       5       6       7       8      9      10     11      12
```

Choose a disk and folder to save registry dump and click *OK* button (twice: in this window and in the parent window).
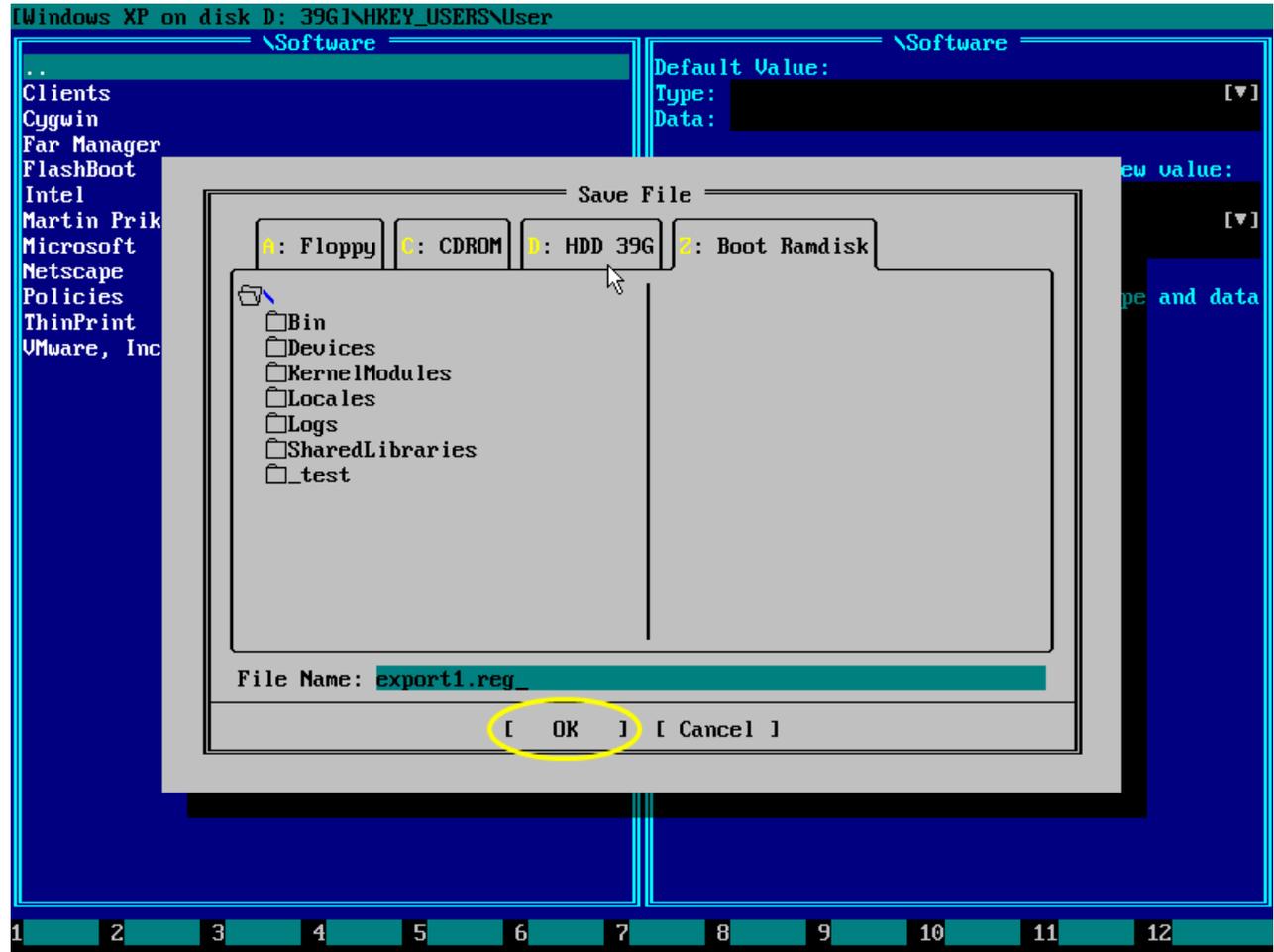
If current registry key was exported successfully, a message like this will be shown.
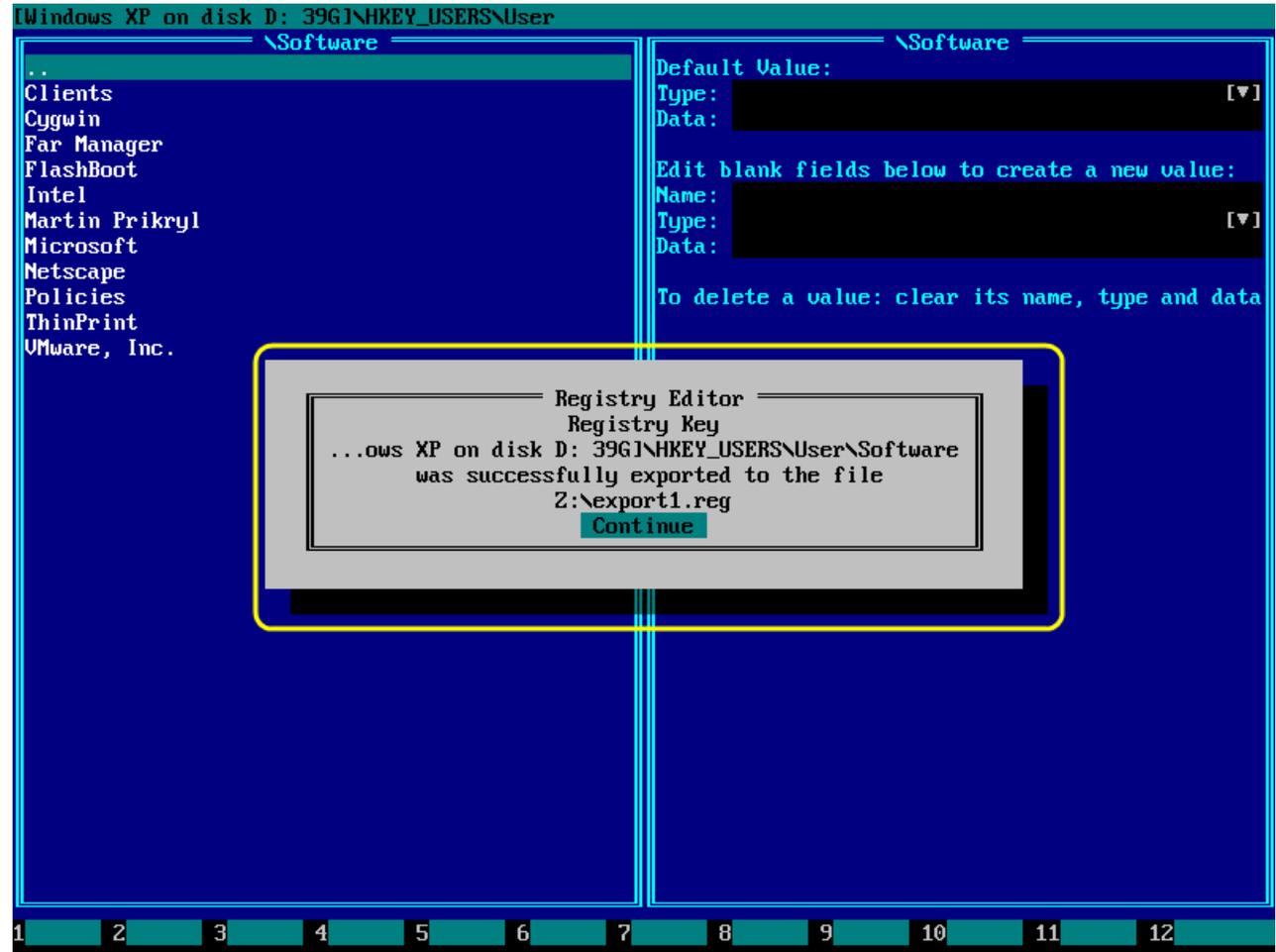
Format of the exported file is compatible with
regedit.exe (for text-mode exports).

```
View: Z:\export1.reg                                        UTF-16LE   Col 0        0%
ZH
NE Windows Registry Editor Version 5.00

[\HKEY_USERS\User\Software]

[\HKEY_USERS\User\Software\Clients]

[\HKEY_USERS\User\Software\Clients\StartMenuInternet]
@="FIREFOX.EXE"

[\HKEY_USERS\User\Software\Cygwin]

[\HKEY_USERS\User\Software\Cygwin\Program Options]

[\HKEY_USERS\User\Software\Far Manager]

[\HKEY_USERS\User\Software\Far Manager\Plugins]

[\HKEY_USERS\User\Software\Far Manager\Plugins\DeepCompare]
"DisableCache"=dword:00000000
"SelectByTime"=dword:00000002
"SelectBySize"=dword:00000001
"SelectBySub"=dword:00000002
"Subfolders"=dword:00000000
"SelectedOnly"=dword:00000000
"UseCache"=dword:00000000
"OnlyWithMask"=dword:00000000
"Mask"="*.*"
"OnlyWithDirMask"=dword:00000000
"DirMask"="*.*"
"CaseSensitive"=dword:00000000
"Time"=dword:00000000
"TwoSecondsPrecision"=dword:00000000
"IgnoreOneHour"=dword:00000000
"Size"=dword:00000000
"Attributes"=dword:00000000
1Help   2Unwrap 3      4Hex    5      6      7Search 8      9      10Quit  11     12Encoding
```

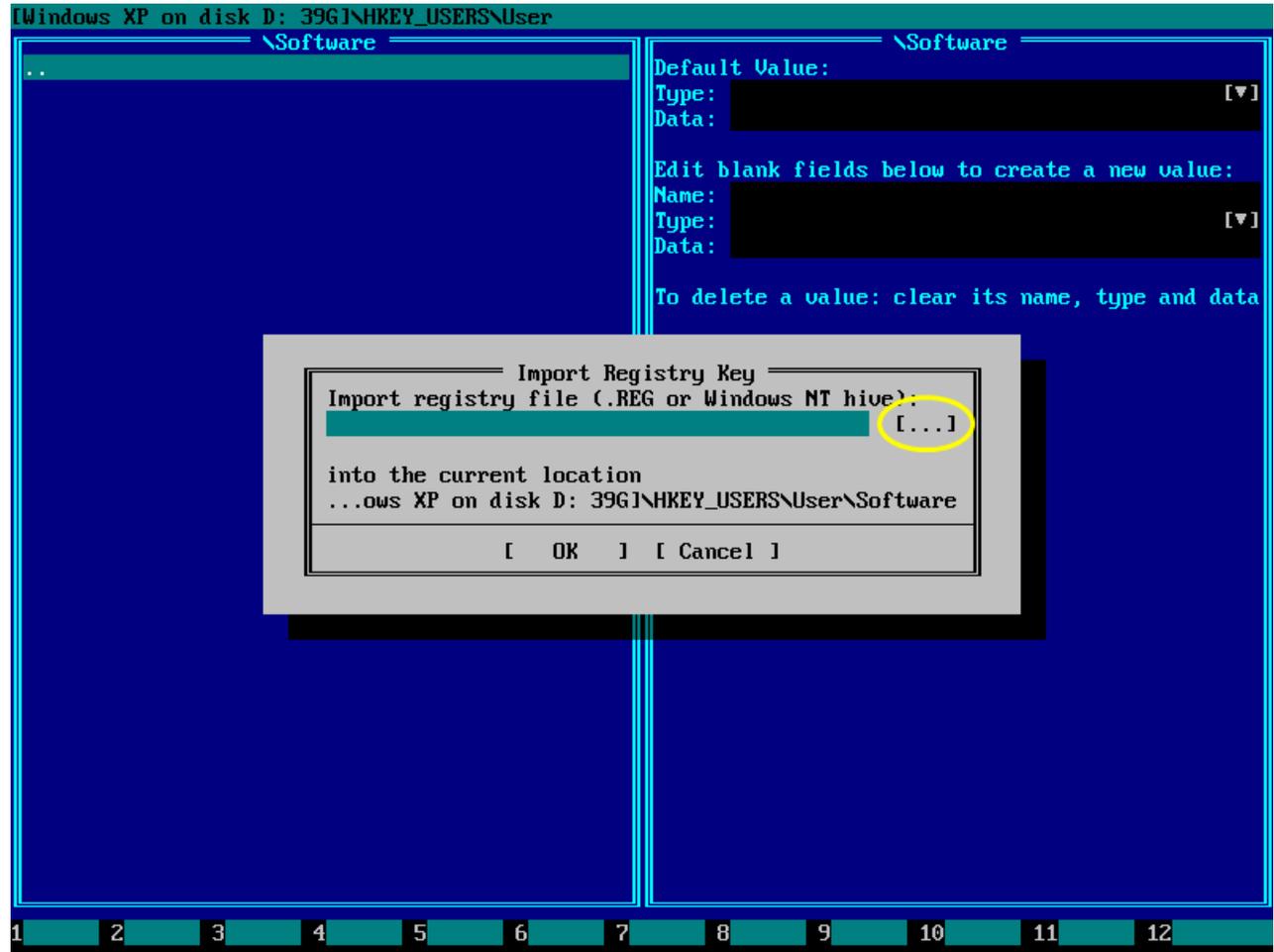## 3.15. Import registry key with subkeys and values

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.

```
[Windows XP on disk D: 39G]\HKEY_USERS\User
                    \Software                              ═ \Software ═
..                                          Default Value:
                                            Type:                          [▼]
                                            Data:

                                            Edit blank fields below to create a new value:
                                            Name:
                                            Type:                          [▼]
                                            Data:

                                            To delete a value: clear its name, type and data




1        2Save    3Export 4Import 5Diff   6Rename 7Create 8Delete 9RawMod 10Exit  11      12Search
```
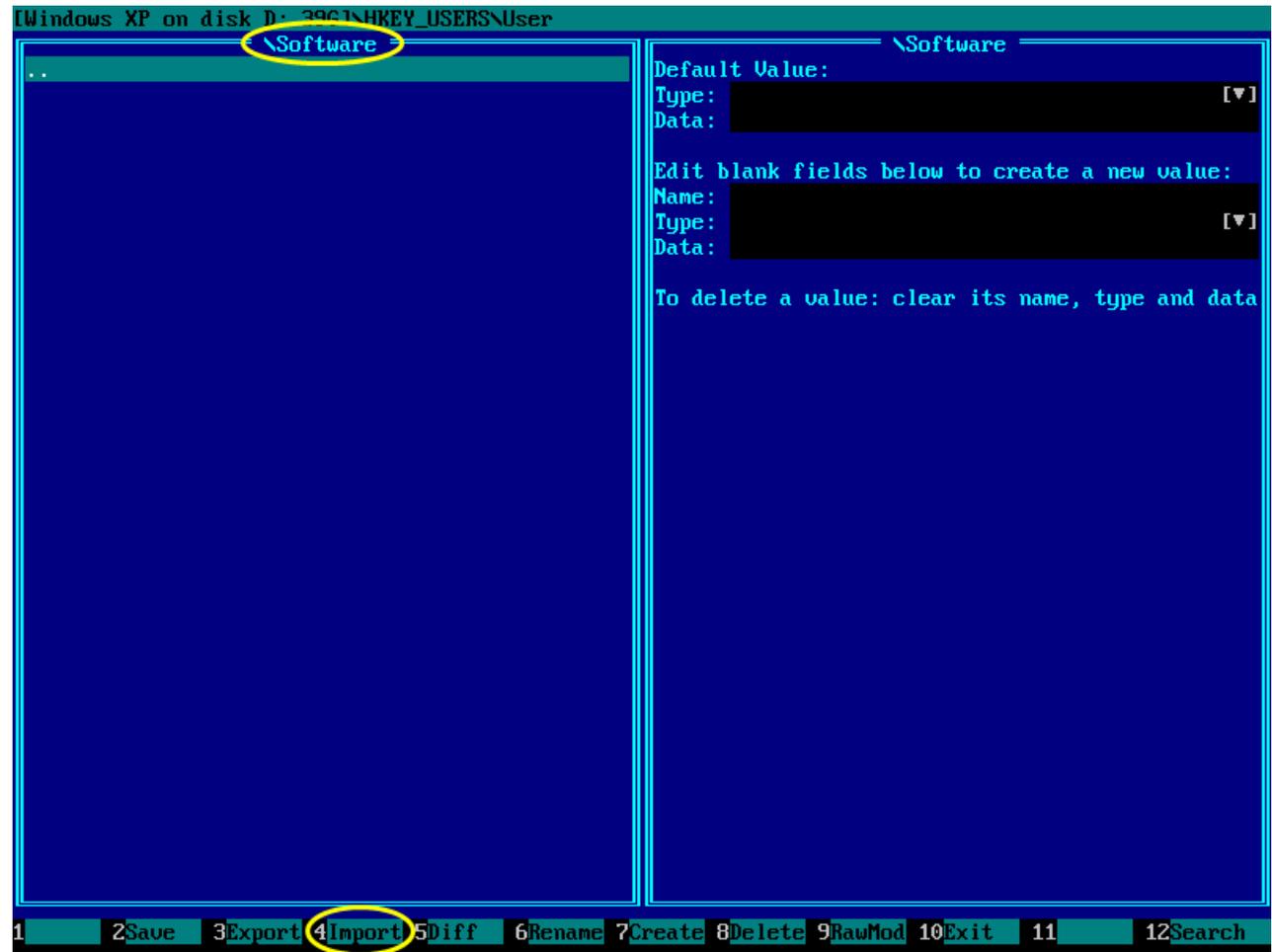
Enter full file name to import here or click *[...]* to browse for file.

```
[Windows XP on disk D: 39G]\HKEY_USERS\User
┌──────────────── \Software ────────────┐   ┌──────────── \Software ──────┐
..                                           Default Value:
                                             Type:                    [▼]
                                             Data:

                                             Edit blank fields below to create a new value:
                                             Name:
                                             Type:                    [▼]
                                             Data:

                                             To delete a value: clear its name, type and data

              ┌──────────────── Import Registry Key ────────────────┐
              │ Import registry file (.REG or Windows NT hive):      │
              │                                              [...]    │
              │                                                       │
              │ into the current location                            │
              │ ...ows XP on disk D: 39G]\HKEY_USERS\User\Software    │
              │                                                       │
              │         [   OK   ]  [ Cancel ]                        │
              └───────────────────────────────────────────────────────┘

 1      2       3      4      5      6      7      8      9     10     11     12
```
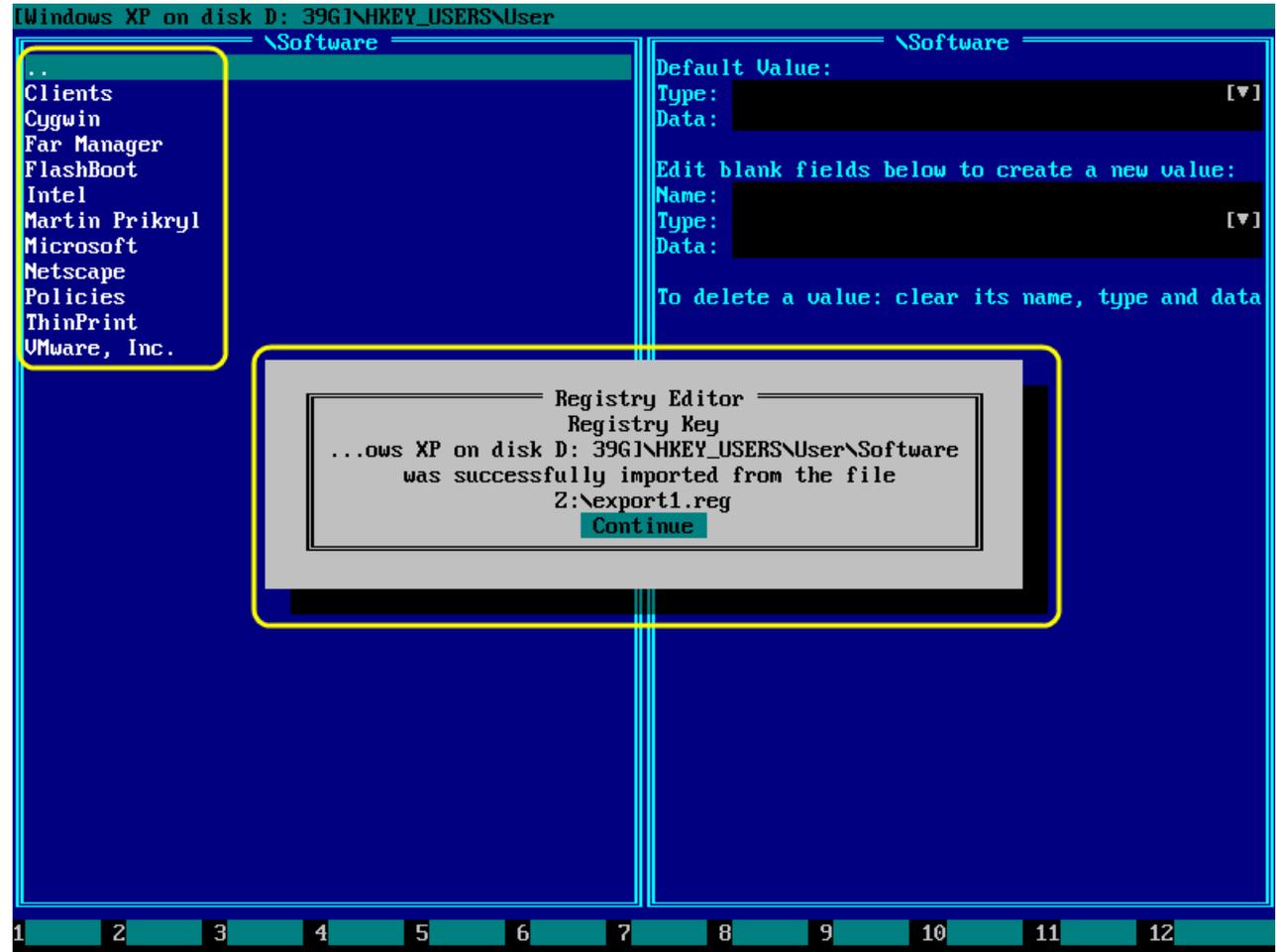
Choose disk, folder, file, and press **Enter** or click *OK*.
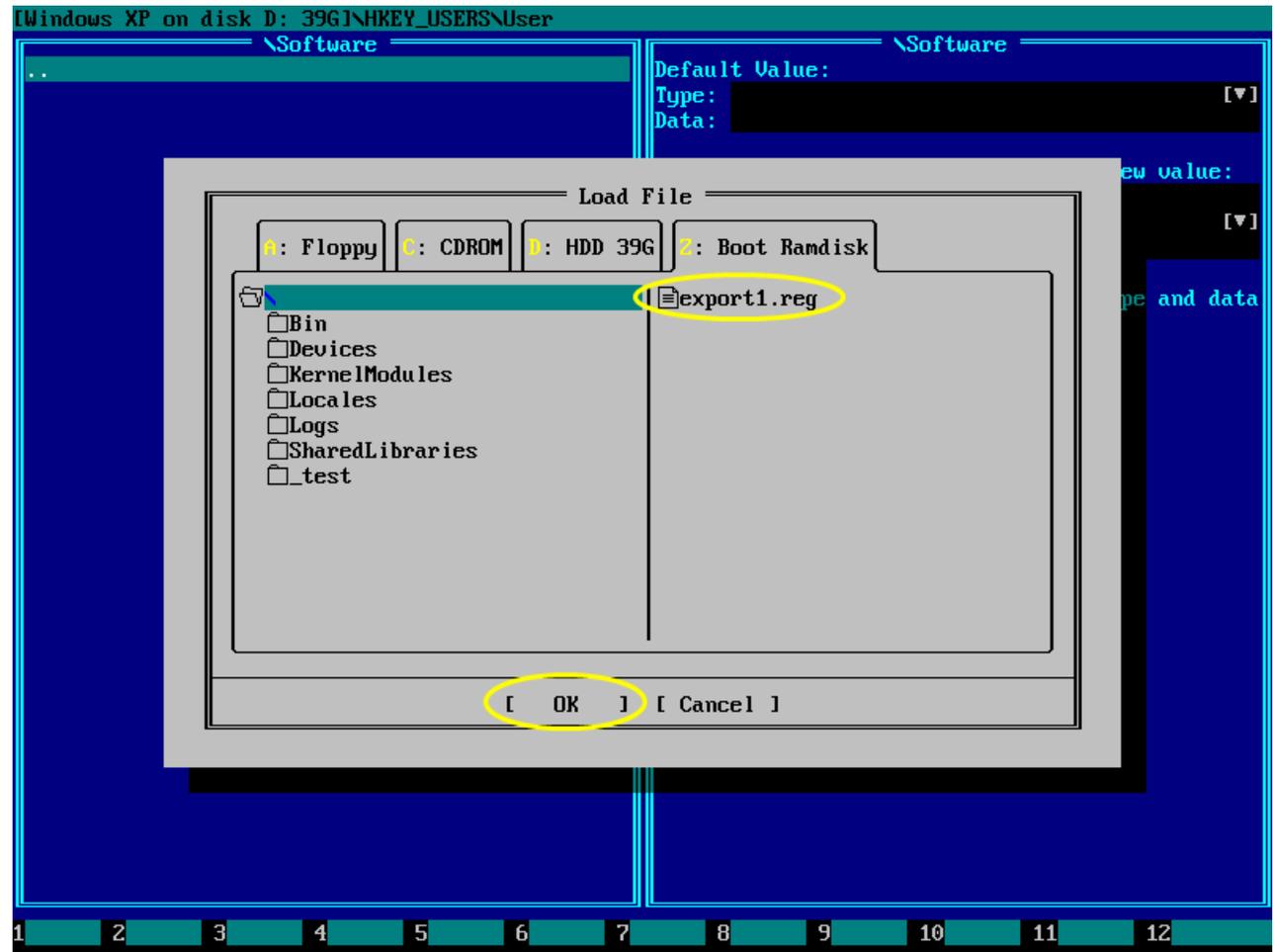
Make sure everything is correct and click *OK*.
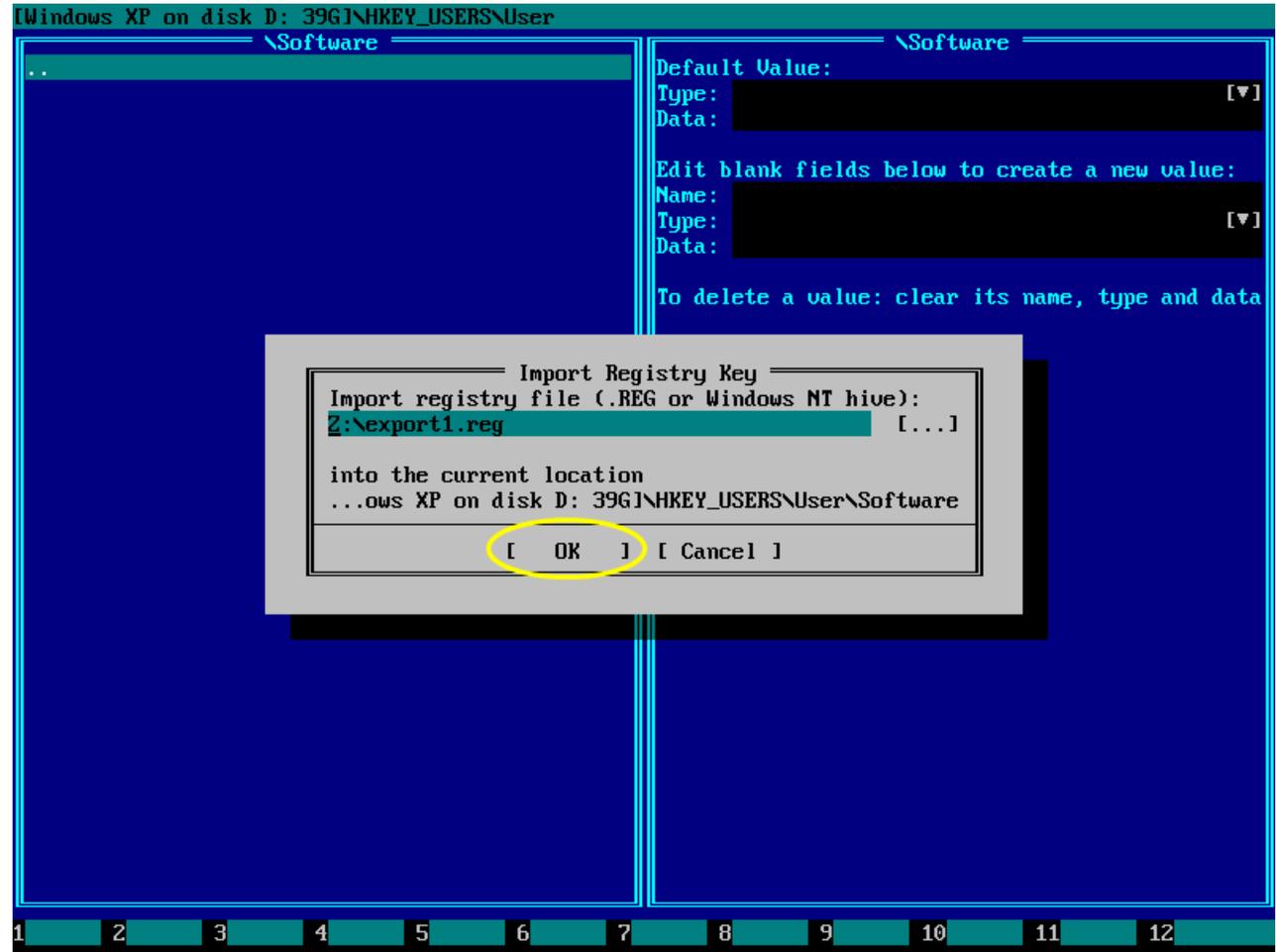
If current registry key was imported successfully, its subkeys and values will be shown immediately and also a message like this will be shown.

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.

```
[Windows XP on disk D: 39G]\HKEY_LOCAL_MACHINE\SOFTWARE
  ┌────────────────────────────────────┐  ┌────────────────────────────
  │C07ft5Y                             │  │Default Value:
  │Classes                             │  │Type:                    [▼]
  │Clients                             │  │Data:
  │Cygwin                              │  │
  │Gemplus                             │  │Edit blank fields below to create a new value:
  │Microsoft                           │  │Name:
  │Mozilla                             │  │Type:                    [▼]
  │mozilla.org                         │  │Data:
  │ODBC                                │  │
  │Policies                            │        name, type and data
  │Program Groups    ┌──────── Generate Diff Report ────────┐
  │RegisteredApplicati│ Compare current registry key         │
  │Schlumberger       │ ... XP on disk D: 39G]\HKEY_LOCAL_MACHINE\SOFTWARE │
  │Secure             │                                      │
  │ThinPrint          │ with a file (.REG or Windows NT hive):│
  │VMware, Inc.       │ _                              [...] │
  │Windows 3.1 Migrati│                                      │
  │WinRAR             │ and save difference report to the file:│
                      │ Z:\Logs\regdiff_report1.txt    [...] │
                      │ [x] Compare statistics in keys       │
                      │ [x] Compare security descriptors     │
                      │ [x] Open report in viewer            │
                      │                                      │
                      │     [   OK   ]  [ Cancel ]           │
                      └──────────────────────────────────────┘
```

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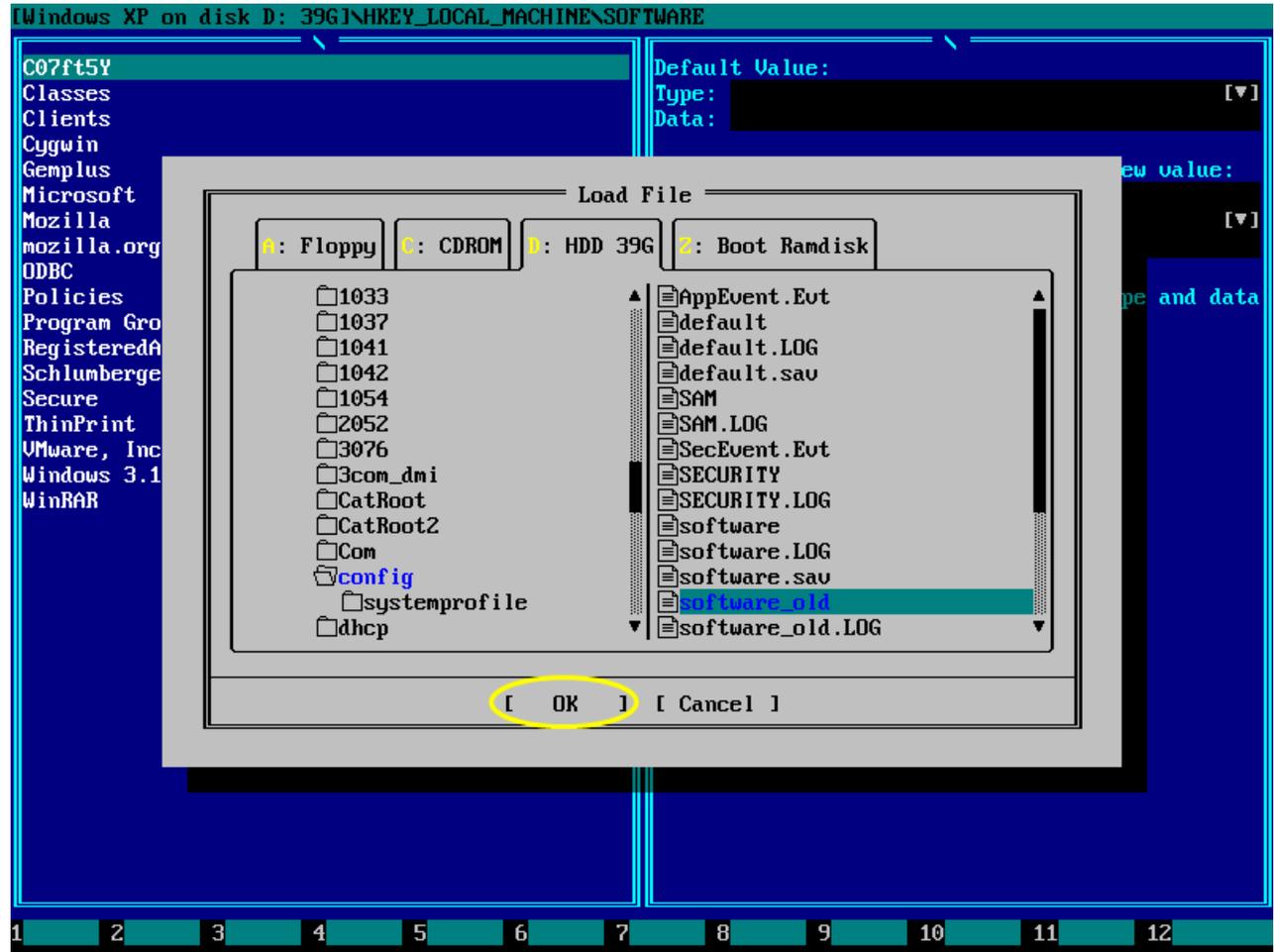
Verify options and click *OK* button to confirm.

```
[Windows XP on disk D: 39G]\HKEY_LOCAL_MACHINE\SOFTWARE

C07ft5Y                              Default Value:
Classes                              Type:                              [▼]
Clients                              Data:
Cygwin
Gemplus                              Edit blank fields below to create a new value:
Microsoft                            Name:
Mozilla                              Type:                              [▼]
mozilla.org                          Data:
ODBC
Policies                   ═══════ Generate Diff Report ═══════    name, type and data
Program Groups         Compare current registry key
RegisteredApplicati    ... XP on disk D: 39G]\HKEY_LOCAL_MACHINE\SOFTWARE
Schlumberger
Secure                 with a file (.REG or Windows NT hive):
ThinPrint              D:\WINDOWS\system32\config\software_old      [...]
VMware, Inc.
Windows 3.1 Migrati    and save difference report to the file:
WinRAR                 Z:\Logs\regdiff_report1.txt                  [...]
                       [x] Compare statistics in keys
                       [x] Compare security descriptors
                       [x] Open report in viewer

                              [   OK   ] [ Cancel ]


 1      2      3      4      5      6      7      8      9      10     11     12
```

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

```
[Windows XP on disk D: 39G]\HKEY_LOCAL_MACHINE\SOFTWARE

C07ft5Y                              Default Value:
Classes                              Type:                       [▼]
Clients                              Data:
Cygwin
Gemplus                              Edit blank fields below to create a new value:
Microsoft                            Name:
Mozilla                              Type:                       [▼]
mozilla.org                          Data:
ODBC
Policies                             To delete a value: clear its name, type and data
Program Groups
RegisteredApplications
Schlumberger
Secure                  ┌───────────── Registry Editor ─────────────┐
ThinPrint               │            Comparing registry key           │
VMware, Inc.            │ ... XP on disk D: 39G]\HKEY_LOCAL_MACHINE\SOFTWARE │
Windows 3.1 Migrati     │   with D:\WINDOWS\system32\config\software_old    │
WinRAR                  │           and generating difference report       │
                        │           Z:\Logs\regdiff_report1.txt            │
                        └─────────────────────────────────────────────┘


1        2Save    3Export 4Import 5Diff    6Rename 7Create 8Delete 9RawMod 10Exit  11       12Search
```

44

Comparison result will look like this.
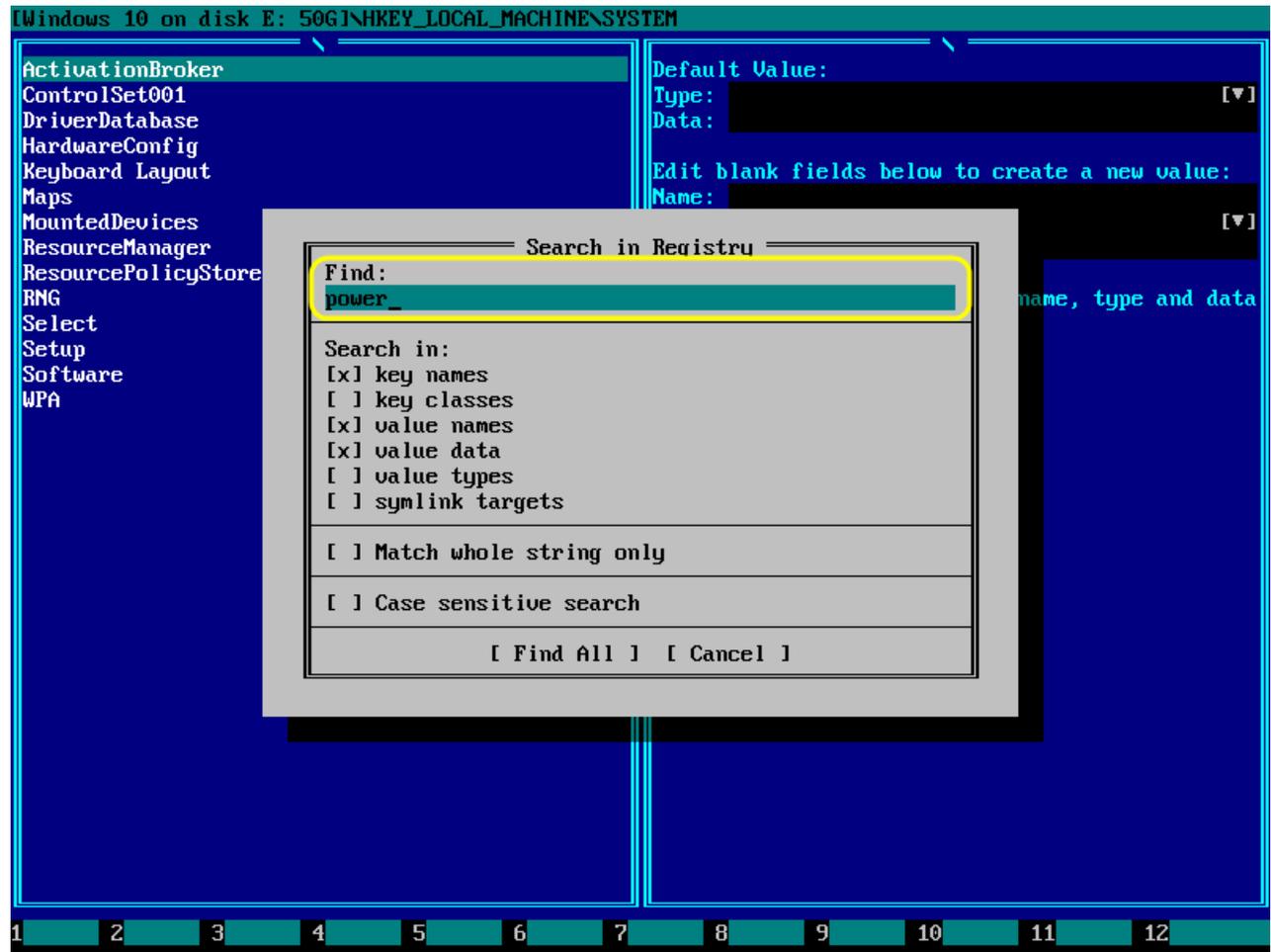
```
View: Z:\Logs\regdiff_report1.txt                                CP-437    Col 0        0%
                         REGISTRY KEY DIFFERENCE REPORT
                         Generated by Emergency Boot Kit
                          http://www.prime-expert.com/embootkit/
... XP on disk D: 39G]\HKEY_LOCAL_MACHINE\SOF... | [D:\WINDOWS\system32\config\software_old]
TWARE                                             |


                                 Key \
Last updated: Sat, 29 Aug 2015, 11:11:10 UTC     | Last updated: Sun, 27 Jul 2014, 21:05:24 UTC
    (0x01D0E24B68BD502A)                          |     (0x01CFA9DE7C20CA12)


                               Key \Classes
Last updated: Sat, 29 Aug 2015, 11:11:10 UTC     | Last updated: Mon, 28 Jul 2014, 13:39:24 UTC
    (0x01D0E24B68C93BEC)                          |     (0x01CFAA6957EA88F0)


                   Key \Classes\*\shellex\ContextMenuHandlers
Last updated: Sat, 29 Aug 2015, 11:11:10 UTC     | Last updated: Sun, 27 Jul 2014, 11:18:36 UTC
    (0x01D0E24B68BFB284)                          |     (0x01CFA98C82451FBC)


               Key \Classes\*\shellex\ContextMenuHandlers\WinRAR
KEY EXISTS                                        | KEY DOES NOT EXIST


                              Key \Classes\.7z
KEY EXISTS                                        | KEY DOES NOT EXIST


                              Key \Classes\.ace
KEY EXISTS                                        | KEY DOES NOT EXIST


                              Key \Classes\.arj
KEY EXISTS                                        | KEY DOES NOT EXIST


                              Key \Classes\.bz
KEY EXISTS                                        | KEY DOES NOT EXIST


                              Key \Classes\.bz2
KEY EXISTS                                        | KEY DOES NOT EXIST
1Help   2Unwrap 3       4Hex   5       6       7Search 8       9       10Quit  11      12Encoding
```

45

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.

```
[Windows 10 on disk E: 50G]\HKEY_LOCAL_MACHINE\SYSTEM
 ActivationBroker                        Default Value:
 ControlSet001                           Type:                      [▼]
 DriverDatabase                          Data:
 HardwareConfig
 Keyboard Layout                         Edit blank fields below to create a new value:
 Maps                                    Name:
 MountedDevices                                                     [▼]
 ResourceManager
 ResourcePolicyStore                              name, type and data
 RNG          ═════════════ Search in Registry ══════════════
 Select         Find:
 Setup          power_
 Software
 WPA            Search in:
                [x] key names
                [ ] key classes
                [x] value names
                [x] value data
                [ ] value types
                [ ] symlink targets

                [ ] Match whole string only

                [ ] Case sensitive search

                       [ Find All ]   [ Cancel ]

  1       2       3       4       5       6       7       8       9       10      11      12
```

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.

```
[Windows 10 on disk E: 50G]\HKEY_LOCAL_MACHINE\SYSTEM
Act                                                                  [▼]
Con  ═══════════════════════ Search Results ══════════════════
Dri
Har  Found "power" in value data:                              ▲
Key  Key: ControlSet001\Control
Map  Value name: EarlyStartServices
Mou  Value type: REG_MULTI_SZ                          [▼]      [▼]
Res  Value data: RpcSs
Res              Power
RNG              BrokerInfrastructure                               ata
Sel              SystemEventsBroker
Set              DcomLaunch
Sof              RpcEpMapper
WPA              LSM
                 AppIdSvc

     [ Go to this value ]  [ Exclude from search results ]  [ Delete value ]

     Found "power" in value name:
     Key: ControlSet001\Control\BackupRestore\FilesNotToBackup
     Value name: Power Management
     Value type: REG_MULTI_SZ                          [▼]
     Value data: \hiberfil.sys

     [ Go to this value ]  [ Exclude from search results ]  [ Delete value ]

     Found "power" in key name:
     Key: ControlSet001\Control\Class\{4d36e96c-e325-11ce-bfc1-08002be10318}\0000\Pow▼

                      [ Replace... ]  [ Close ]


  1      2      3      4      5      6      7      8      9     10     11     12
```

Search & Replace dialog will look like this.

```
[Windows 10 on disk E: 50G]\HKEY_LOCAL_MACHINE\SYSTEM
┌─────────────────────── Search Results ───────────────────────┐
│ Found "power" in value data:                               ▲  │
│ Key: ControlSet001\Control                                    │
│ Value name: EarlyStartServices                                │
│ Value type: REG_MULTI_SZ                                      │
│ Value data: RpcSs                                             │
│             Power                                             │
│             BrokerInfrastructure                             │
│       ┌─────────────── Replace in Registry ───────────────┐   │
│       │ Replace search string                             │   │
│       │     "power"                                       │   │
│       │ with                                              │   │
│ [ Go to│    power                                         │   │
│       │                                                   │   │
│ Found "p│ for all remaining search results               │   │
│ Key: Con│ (renaming key to empty string = deleting key)   │   │
│ Value na│                                                 │   │
│ Value ty│         [ Replace All ]   [ Cancel ]            │   │
│ Value da└───────────────────────────────────────────────┘   │
│ [ Go to this value ]   [ Exclude from search results ]   [ Delete value ] │
│                                                               │
│ Found "power" in key name:                                    │
│ Key: ControlSet001\Control\Class\{4d36e96c-e325-11ce-bfc1-08002be10318}\0000\Pow▼ │
│                 [ Replace... ]   [ Close ]                    │
└───────────────────────────────────────────────────────────────┘
```