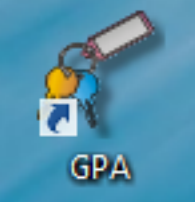
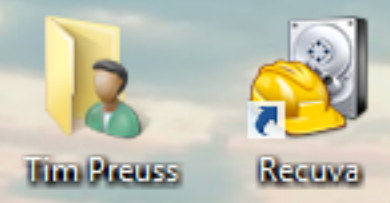


Windows 8.0 Registry Basics

This presentation shows creating a batch file to backup the registry. The presentation shows the permission settings in the the registry.

Preuss

3/12/2014



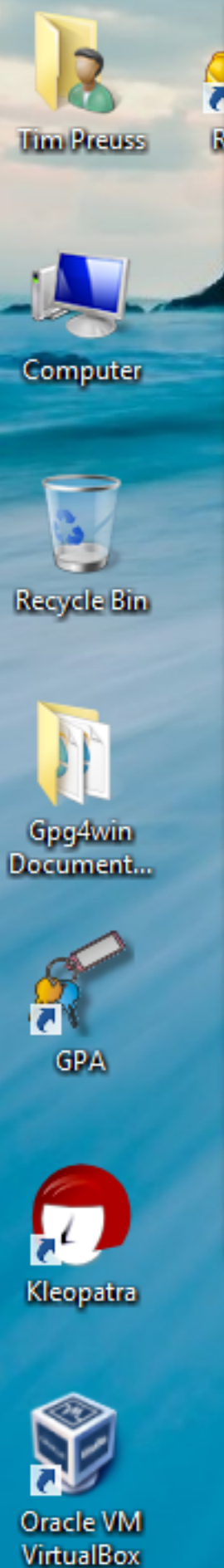
The presentation logs in as a non-administrative logon.



Untitled - Notepad

File Edit Format View Help

The presentation opens Notepad to create a batch file.



Untitled - Notepad

File Edit Format View Help

```
REM This will backup the registry to c:\regback
REM This uses the reg /? help system
REM This batch file must be run as administrator
REM Preuss 3/12/2014

REM This will create the folder c:\regback
md c:\regback
REM This will backup the hive HKLM and overwrite the old file
reg export HKLM c:\regback\hkml_bak.reg /y
REM This will backup the hive HKCU and overwrite the old file
reg export HKCU c:\regback\hkcu_bak.reg /y
REM This will backup the hive HKCR and overwrite the old file
reg export HKCR c:\regback\hkcr_bak.reg /y
REM This will backup the hive HKU and overwrite the old file
reg export HKU c:\regback\hku_bak.reg /y
REM This will backup the hive HKCC and overwrite the old file
reg export HKCC c:\regback\hkcc_bak.reg /y
REM This will let us know the batch file is done.
Echo 'All Done'
REM This will cause the system to wait for us.
pause
```

The registry creates the following batch file contents.



Player



Untitled - Notepad

File Edit Format View Help

```
REM This will backup the registry to c:\regback
REM This uses the reg /? help system
REM This batch file must be run as administrator
REM Preuss 3/12/2014
```

```
REM This will create the folder c:\regback
md c:\regback
```

```
REM This will backup the hive HKLM
reg export HKLM c:\regback\hklm_ba
```

```
REM This will backup the hive HKCU
reg export HKCU c:\regback\hkcu_ba
```

```
REM This will backup the hive HKCR
reg export HKCR c:\regback\hkcr_ba
```

```
REM This will backup the hive HKU
reg export HKU c:\regback\hku_bak.
```

```
REM This will backup the hive HKCC
reg export HKCC c:\regback\hkcc_ba
```

```
REM This will let us know the batch file
Echo 'All Done'
```

```
REM This will cause the system to wait
pause
```

Save As

Navigation icons: back, forward, up, down. Path: << My Document... >> batch_files. Search: Search batch_files

Organize New folder

★ Favorites

- Desktop
- Downloads
- Recent places

Libraries

- Documents
- Music
- Pictures
- Videos

Computer

Name

Date modified

Type

Name	Date modified	Type
logon_test.bat	9/27/2013 10:48 AM	Windows Batch File
logon-list.bat	12/10/2013 2:34 PM	Windows Batch File
prod2.bat	9/26/2013 3:17 PM	Windows Batch File
test_ipv4.bat	2/28/2014 4:38 PM	Windows Batch File
test_ipv6.bat	3/11/2014 4:56 PM	Windows Batch File

File name: regback.bat

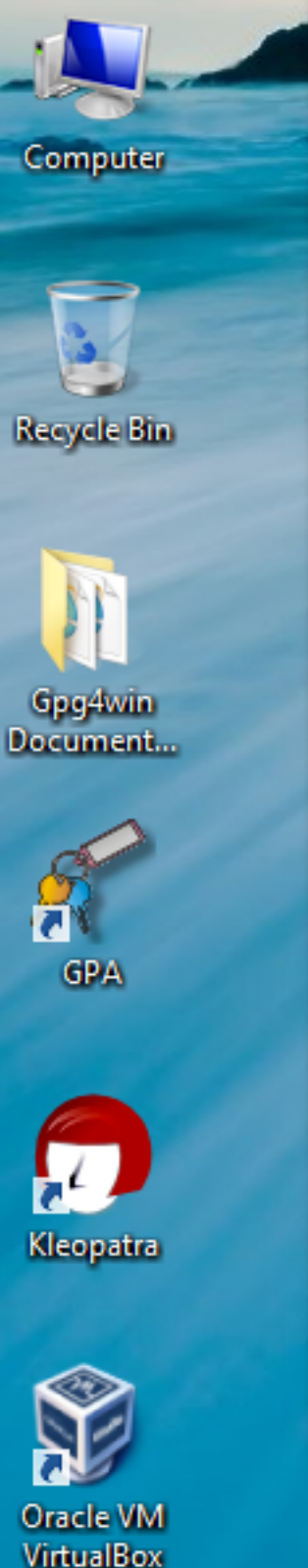
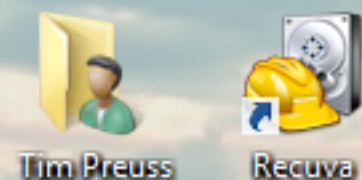
Save as type: All Files (*.*)

Hide Folders

Encoding: ANSI

The registry saves the batch file as regback.bat. Remember to change Save as type: All Files (*.*)

12:47 PM
3/12/2014



C:\Users\tim_p_000\Documents\batch_files

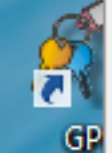
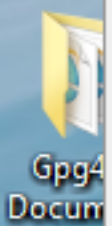
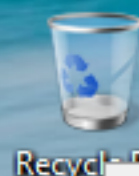
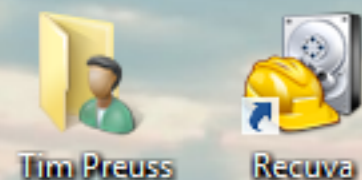
File Home Share View

Libraries Documents batch_files

Name	Date modified	Type	Size
logon_test.bat	9/27/2013 10:48 AM	Windows Batch File	40 KB
logon-list.bat	12/10/2013 2:34 PM	Windows Batch File	1 KB
prod2.bat	9/26/2013 3:17 PM	Windows Batch File	1 KB
regback.bat	3/12/2014 12:48 PM	Windows Batch File	1 KB
		Windows Batch File	2 KB
		Windows Batch File	2 KB

6 items

The batch file regback.bat is available for use.



Application Tools C:\Users\tim_p_000\Documents\batch_files

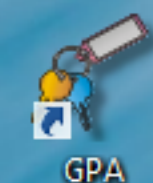
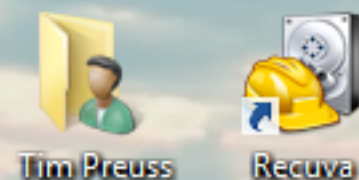
File Home Share View Manage

Libraries Documents batch_files Search batch_files

Name	Date modified	Type	Size
logon_test.bat	9/27/2013 10:48 AM	Windows Batch File	40 KB
logon-list.bat	12/10/2013 2:34 PM	Windows Batch File	1 KB
prod2.bat	9/26/2013 3:17 PM	Windows Batch File	1 KB
regback.bat	3/12/2014 12:48 PM	Windows Batch File	1 KB
pv4.bat	2/28/2014 4:38 PM	Windows Batch File	2 KB
pv6.bat	3/11/2014 4:56 PM	Windows Batch File	2 KB

- Open
- Edit
- Print
- Run as administrator
- Create PDF and Bitmap Files with 7-Zip
- Sign and encrypt
- More GpgEX options
- Share with
- Send to
- Cut
- Copy
- Create shortcut
- Delete
- Rename
- Open file location
- Properties

The presentation right clicks on regback.bat and selects Run as Administrator.



Application Tools C:\Users\tim_p_000\Documents\batch_files

File Home Share View Manage

Libraries Documents batch_files Search batch_files

C:\Windows\System32\cmd.exe

```

C:\Windows\system32>reg export HKCR c:\regback\hkcr_bak.reg /y
The operation completed successfully.

C:\Windows\system32>REM This will backup the hive HKU and overwrite the old file

C:\Windows\system32>reg export HKU c:\regback\hku_bak.reg /y
The operation completed successfully.

C:\Windows\system32>REM This will backup the hive HKCC and overwrite the old file

C:\Windows\system32>reg export HKCC c:\regback\hkcc_bak.reg /y
The operation completed successfully.

C:\Windows\system32>REM This will let us know the batch file is done.

C:\Windows\system32>Echo æAll Doneff
æAll Doneff

C:\Windows\system32>REM This will cause the system to wait for us.

C:\Windows\system32>pause
Press any key to continue . . .

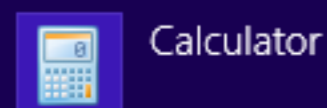
```

6 items | 1 item selected 875 bytes

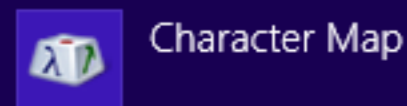
Regback.bat is complete. The presentation presses the spacebar to continue.

Apps

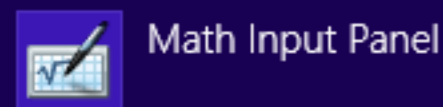
Windows Accessories



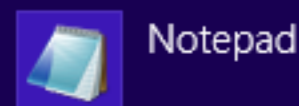
Calculator



Character Map



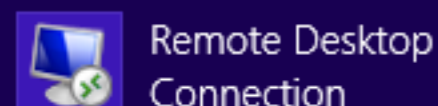
Math Input Panel



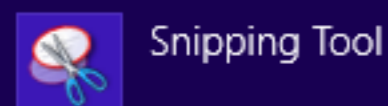
Notepad



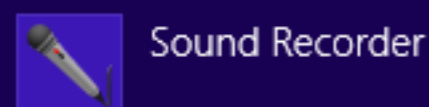
Paint



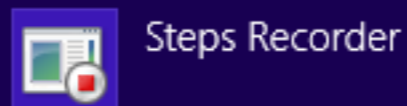
Remote Desktop Connection



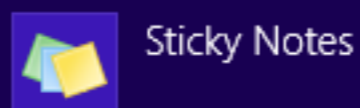
Snipping Tool



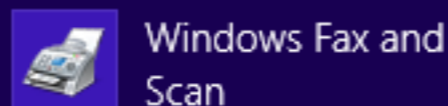
Sound Recorder



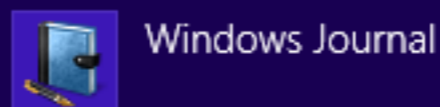
Steps Recorder



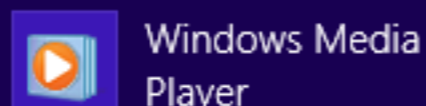
Sticky Notes



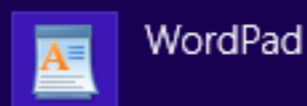
Windows Fax and Scan



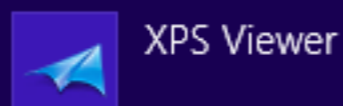
Windows Journal



Windows Media Player

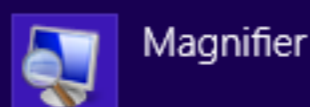


WordPad

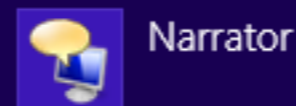


XPS Viewer

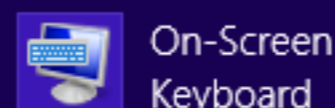
Windows Ease of Access



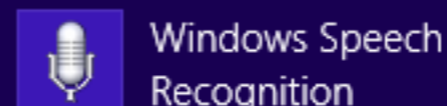
Magnifier



Narrator

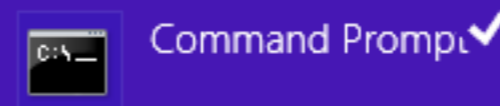


On-Screen Keyboard



Windows Speech Recognition

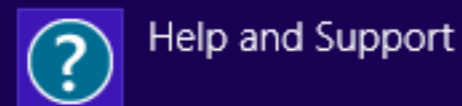
Windows System



Command Prompt



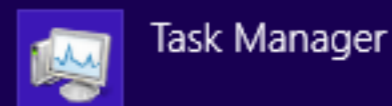
Computer



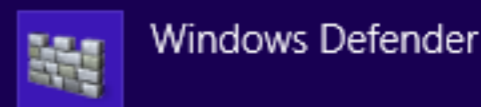
Help and Support



Run



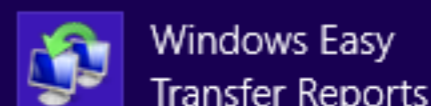
Task Manager



Windows Defender



Windows Easy Transfer



Windows Easy Transfer Reports



Unpin from Start



Unpin from taskbar



Open new window



Run as administrator

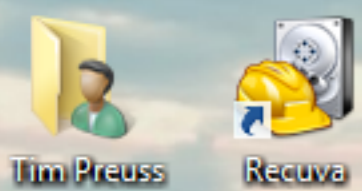


Open file location



All apps

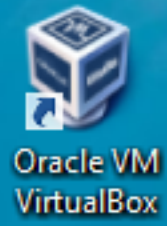
The presentation opens the Start Menu. At the Start Menu, the presentation open all applications.
The presentation right clicks the Command Prompt. The presentation selects Run as Administrator.

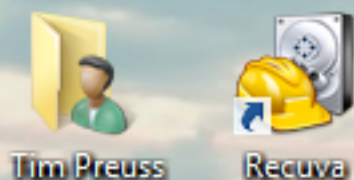


Administrator: Command Prompt

```
C:\Windows\system32>cd %USERPROFILE%  
C:\Users\Snuffy>_
```

The presentation changes to the current logon home directory.



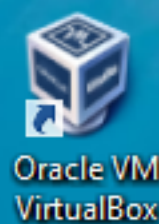
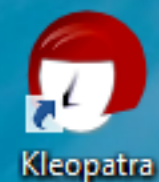


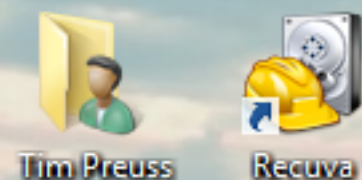
Administrator: Command Prompt

```
C:\Windows\System32>cd %USERPROFILE%  
C:\Users\Snuffly>md temp  
C:\Users\Snuffly>cd temp  
C:\Users\Snuffly\temp>
```

The presentation creates a temp directory in the current logon home directory.

The presentation changes the default directory to c:\users\snuffly\temp.





Tim Preuss

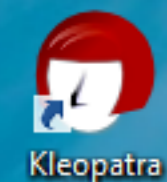
Recuva

Administrator: Command Prompt

```
C:\Windows\System32>cd %USERPROFILE%  
C:\Users\Snuffly>md temp  
C:\Users\Snuffly>cd temp  
C:\Users\Snuffly\temp>regedit_
```

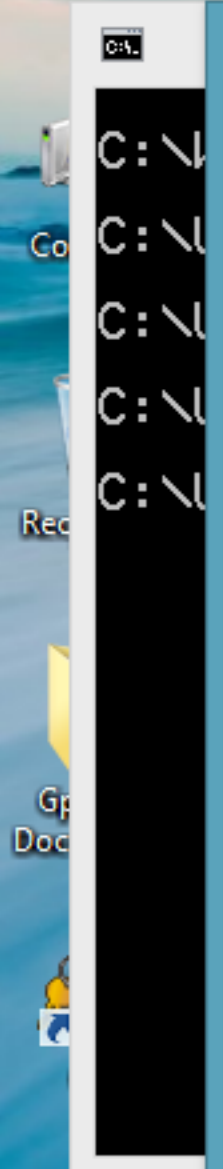
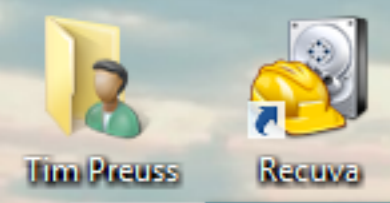
The presentation issues the regedit command. This will allow viewing and editing of the registry.

This can be dangerous.



Kleopatra

Oracle VM
VirtualBox12:52 PM
3/12/2014



Registry Editor

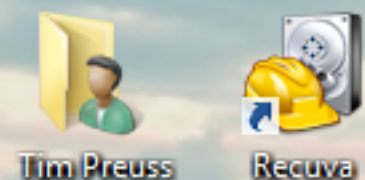
File Edit View Favorites Help

- Computer
 - HKEY_CLASSES_ROOT
 - HKEY_CURRENT_USER
 - HKEY_LOCAL_MACHINE
 - HKEY_USERS
 - HKEY_CURRENT_CONFIG

Name	Type	Data
------	------	------

The presentation successfully opened the registry editor.





Registry Editor

File Edit View Favorites Help

Name	Type	Data
HKEY_CLASSES_ROOT	REG_SZ	(value not set)

Computer

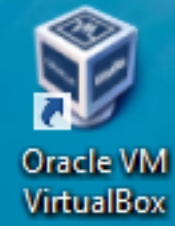
- HKEY_CLASSES_ROOT
- HKEY_CURRENT_CONFIG
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

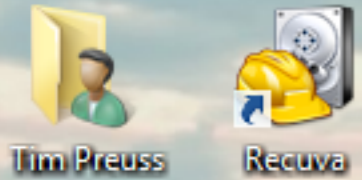
Computer\HKEY_CLASSES_ROOT

- Expand
- New
- Find...
- Delete
- Rename
- Export
- Permissions...
- Copy Key Name

The presentation right click on the hive, HKEY_CLASSES_ROOT.

The presentation selects Permissions to view the permission settings for this hive.





Registry Editor

File Edit View Favorites Help

Name	Type	Data
HKEY_CLASSES_ROOT		(value not set)

Permissions for HKEY_CLASSES_ROOT

Security

Group or user names:

- ALL APPLICATION PACKAGES
- CREATOR OWNER
- SYSTEM
- Administrators (WIN8-VICTIM02\Administrators)
- Users (WIN8-VICTIM02\Users)

Add... Remove

Permissions for ALL APPLICATION PACKAGES

	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Special permissions	<input type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced.

[Learn about access control and permissions](#)

OK Cancel Apply

The presentation views the permission settings.

