Lab 7-2: Registry Forensics with RegRipper Plug-ins

Registry:

The window registry is a hierarchical database that houses the OS, apps, users, and device setup settings.

Information on the system, installed and running programs, user activity, and connected devices can all be found there.

The registry is a composed of binary data files also called “hive”.

• The main registry hives are SAM, Security, Software, and system.

• They are located under the C:\windows\system32\config

• There are also specific user’s hives NTUSER.DAT, and URSCLASS.DAT

These are located under the user’s profile

Keys and values are the registry's two fundamental building blocks.

Containers for other keys and/or values include keys.

Names, types, and the corresponding data value serve to define values.

The HKLY_LOCAL_MACHINE root key, where the primary registry hives are mapped as subkeys, is the most significant one.

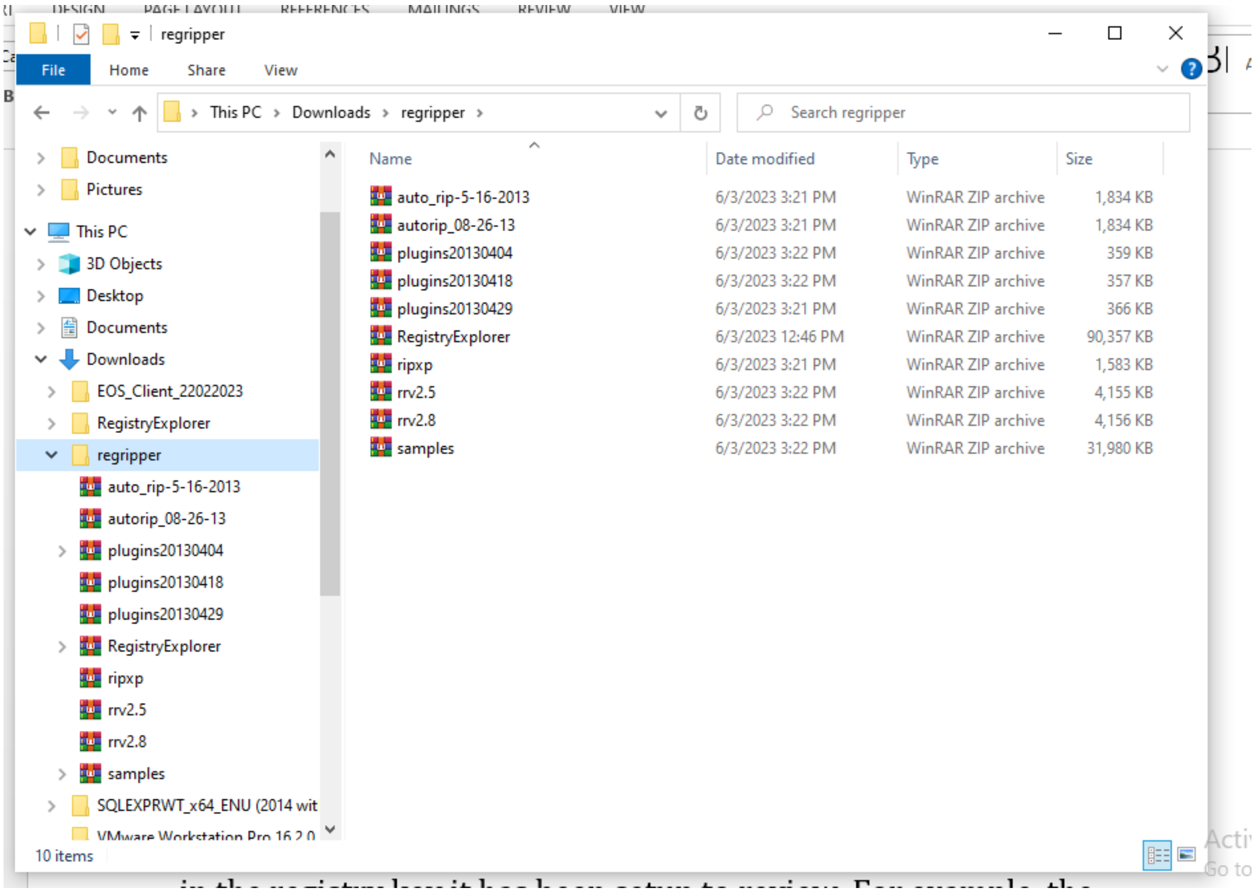
RegRipper:

RegRipper uses plugins to extract information out of the registry files. Each plugin has been created to handle the data that is stored in the registry key it has been setup to review. For example, the plugins will decode the ROT-13 encrypted data and translate binary data to ASCII.

The forensics community contributes Perl scripts as the plugins. It regularly extracts data from a certain area of the registry during your forensics case investigations.

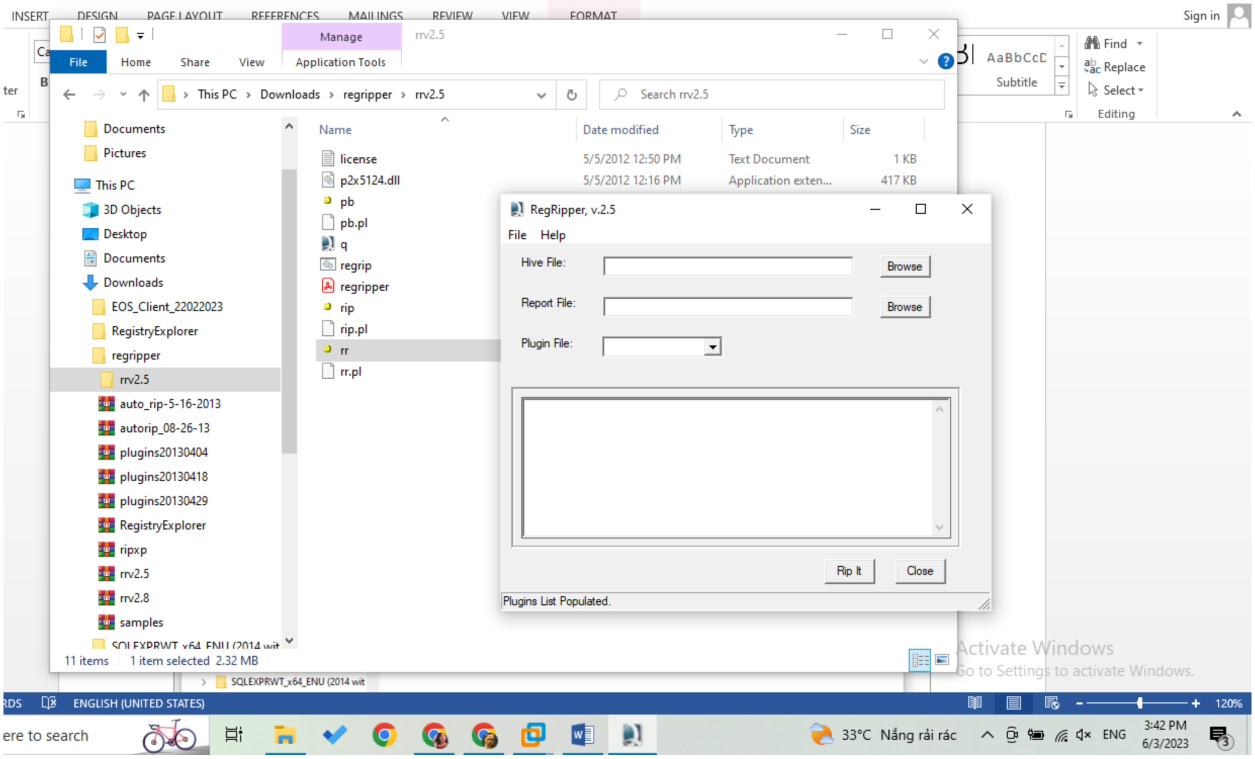
We use available plugins

I have just downloaded all the files and put them into a folder named **regripper**



Name	Date modified	Type	Size
auto_rip-5-16-2013	6/3/2023 3:21 PM	WinRAR ZIP archive	1,834 KB
autorip_08-26-13	6/3/2023 3:21 PM	WinRAR ZIP archive	1,834 KB
plugins20130404	6/3/2023 3:22 PM	WinRAR ZIP archive	359 KB
plugins20130418	6/3/2023 3:22 PM	WinRAR ZIP archive	357 KB
plugins20130429	6/3/2023 3:21 PM	WinRAR ZIP archive	366 KB
RegistryExplorer	6/3/2023 12:46 PM	WinRAR ZIP archive	90,357 KB
ripxp	6/3/2023 3:21 PM	WinRAR ZIP archive	1,583 KB
rrv2.5	6/3/2023 3:22 PM	WinRAR ZIP archive	4,155 KB
rrv2.8	6/3/2023 3:22 PM	WinRAR ZIP archive	4,156 KB
samples	6/3/2023 3:22 PM	WinRAR ZIP archive	31,980 KB

After that we extract the file **rrv2.5** then double-click into **rr:**

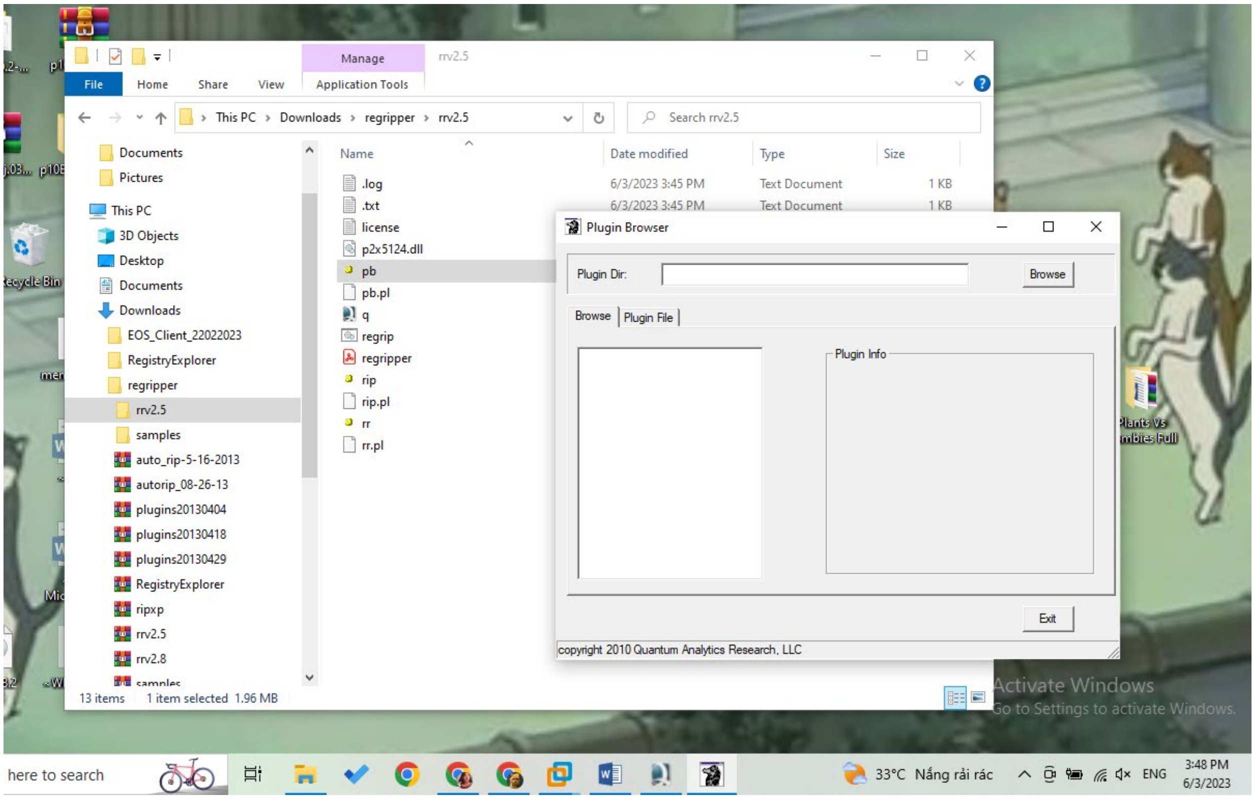


Name	Date modified	Type	Size
license	5/5/2012 12:50 PM	Text Document	1 KB
p2x5124.dll	5/5/2012 12:16 PM	Application exten...	417 KB
pb			
pb.pl			
q			
regrip			
regripper			
rip			
rip.pl			
rr			
rr.pl			

Plugins List Populated.

⇨ Here is the display that we are going to execute

Open **pb** to browse the needed files



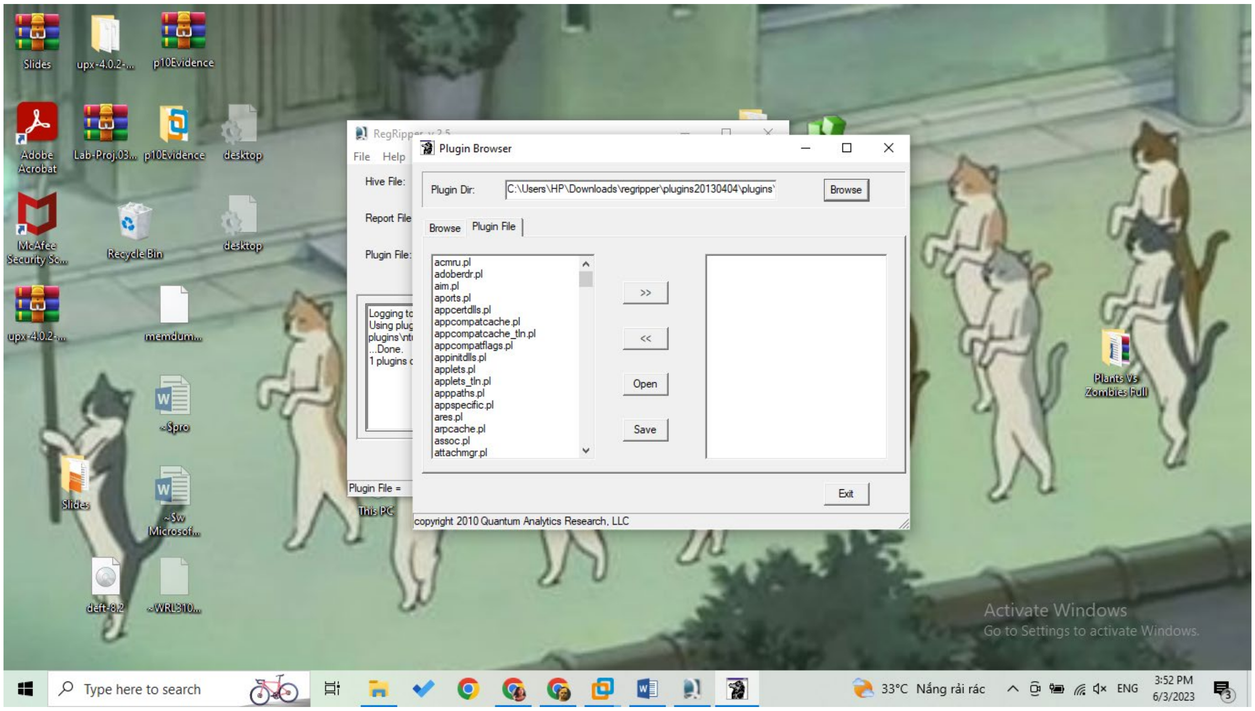
Name	Date modified	Type	Size
.log	6/3/2023 3:45 PM	Text Document	1 KB
.txt	6/3/2023 3:45 PM	Text Document	1 KB
license			
p2x5124.dll			
pb			
pb.pl			
q			
regrip			
regripper			
rip			
rip.pl			
rr			
rr.pl			

copyright 2010 Quantum Analytics Research, LLC

Browse any files then check the plugins

Use << >> for copy the between 2 displays

Open or save when we need

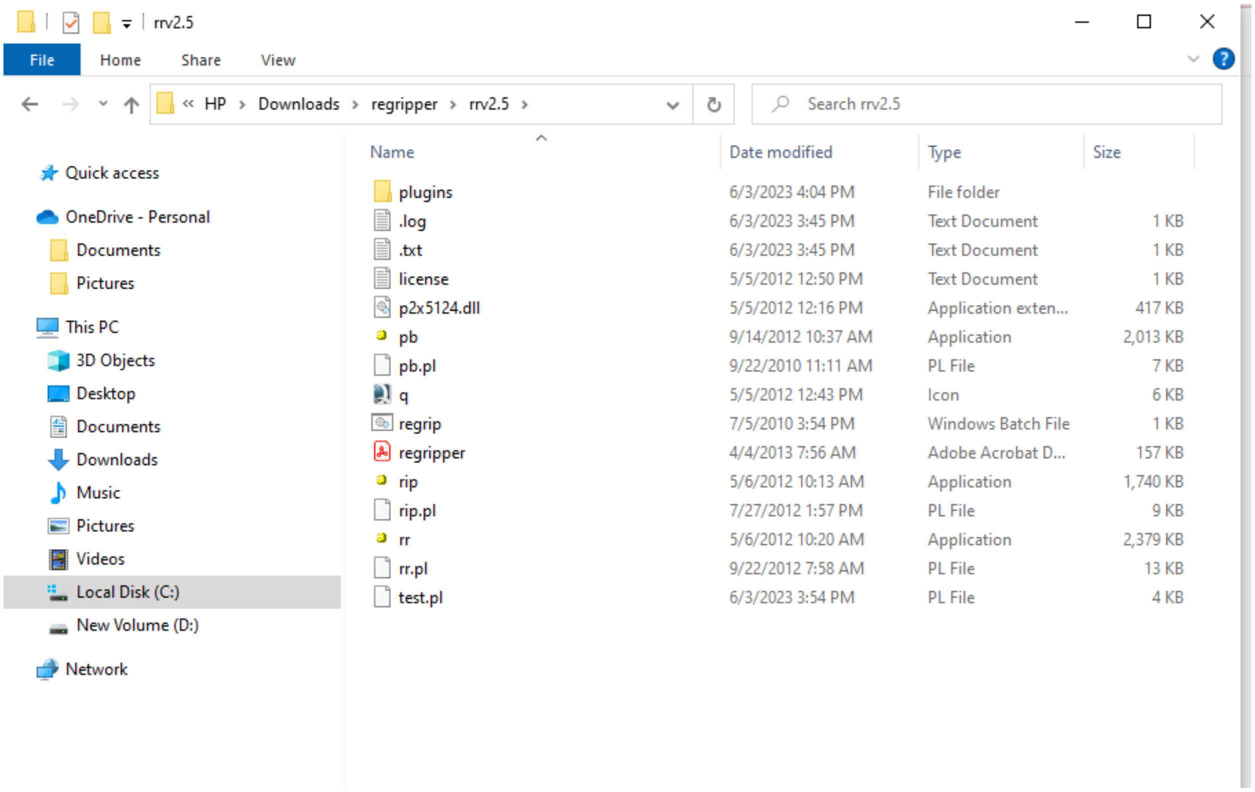


Plugin Dir: C:\Users\HP\Downloads\regripper\plugins20130404\plugins\

```
Logging tc
Using plug
plugins\nt
...Done.
1 plugins c
```

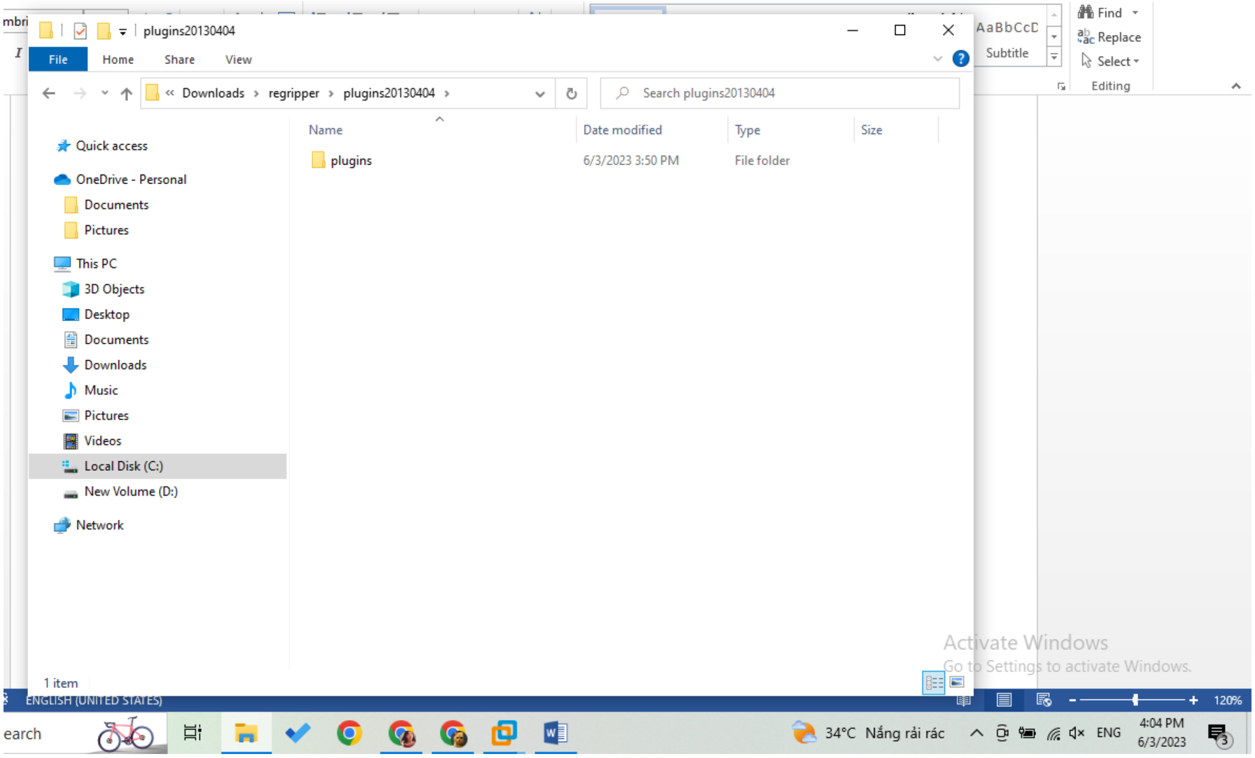
```
acmru.pl
adoberdr.pl
aim.pl
aports.pl
appcertdlls.pl
appcompatcache.pl
appcompatcache_tln.pl
appcompatflags.pl
appinitdlls.pl
applets.pl
applets_tln.pl
apppaths.pl
appspecific.pl
ares.pl
arpcache.pl
assoc.pl
attachmgr.pl
```

Then at the moment we open the folder rrv2.5, we should see the plugins folder here. The thing we have to do is that copy that folder



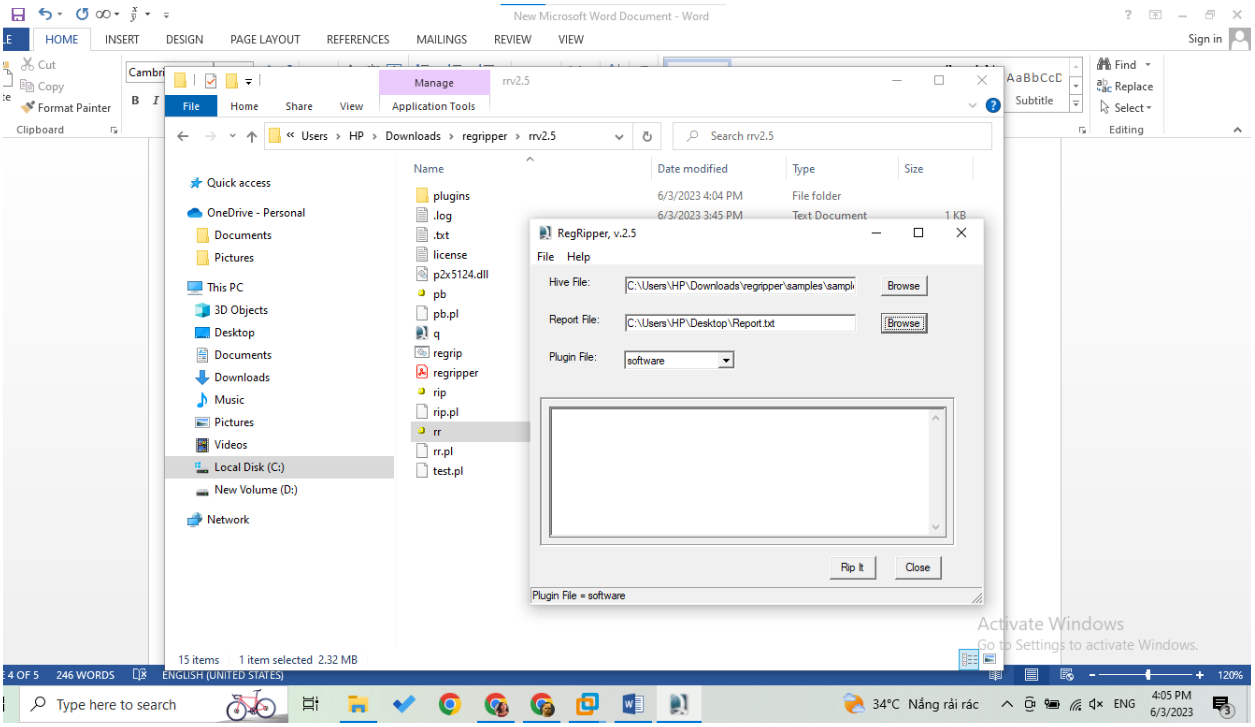
Name	Date modified	Type	Size
plugins	6/3/2023 4:04 PM	File folder	
.log	6/3/2023 3:45 PM	Text Document	1 KB
.txt	6/3/2023 3:45 PM	Text Document	1 KB
license	5/5/2012 12:50 PM	Text Document	1 KB
p2x5124.dll	5/5/2012 12:16 PM	Application exten...	417 KB
pb	9/14/2012 10:37 AM	Application	2,013 KB
pb.pl	9/22/2010 11:11 AM	PL File	7 KB
q	5/5/2012 12:43 PM	Icon	6 KB
regrip	7/5/2010 3:54 PM	Windows Batch File	1 KB
regripper	4/4/2013 7:56 AM	Adobe Acrobat D...	157 KB
rip	5/6/2012 10:13 AM	Application	1,740 KB
rip.pl	7/27/2012 1:57 PM	PL File	9 KB
rr	5/6/2012 10:20 AM	Application	2,379 KB
rr.pl	9/22/2012 7:58 AM	PL File	13 KB
test.pl	6/3/2023 3:54 PM	PL File	4 KB

And go to plugins20130404 folder to paste the folder plugins as following



Name	Date modified	Type	Size
plugins	6/3/2023 3:50 PM	File folder	

Then open rr tool, browse the sample, choose plugins file as software => press rip it



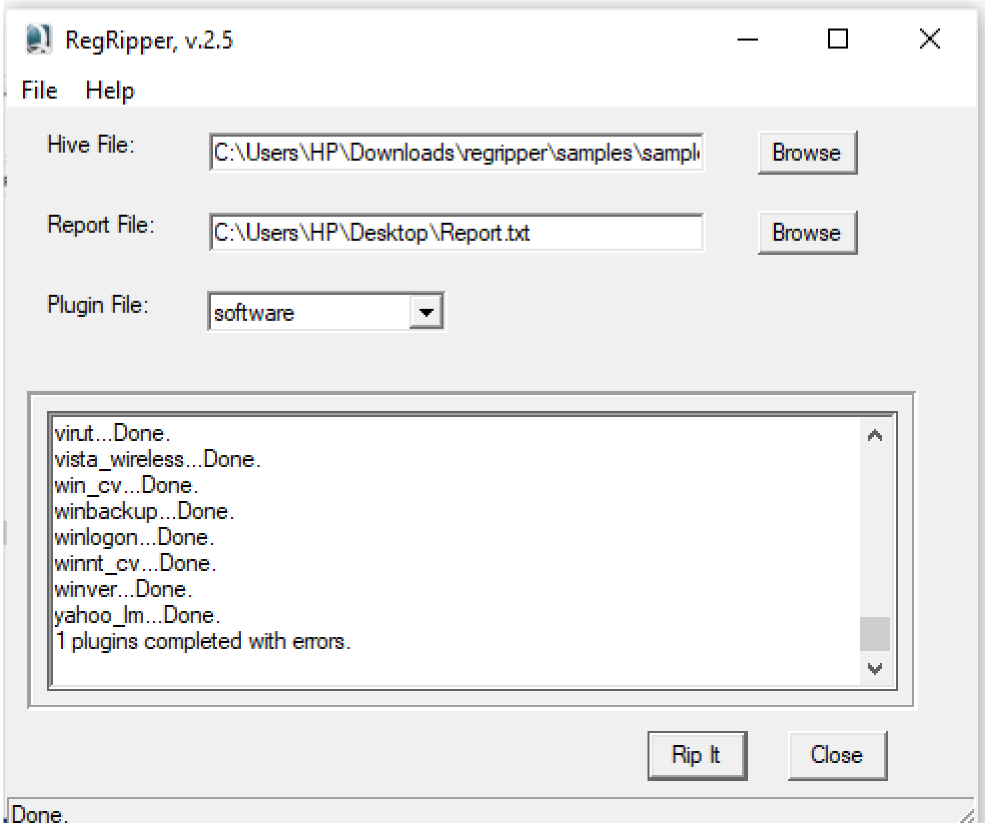
RegRipper, v.2.5

Hive File: C:\Users\HP\Downloads\regripper\samples\sampl

Report File: C:\Users\HP\Desktop\Report.txt

Plugin File: software

Plugin File = software



Hive File: C:\Users\HP\Downloads\regripper\samples\sampl

Report File: C:\Users\HP\Desktop\Report.txt

Plugin File: software

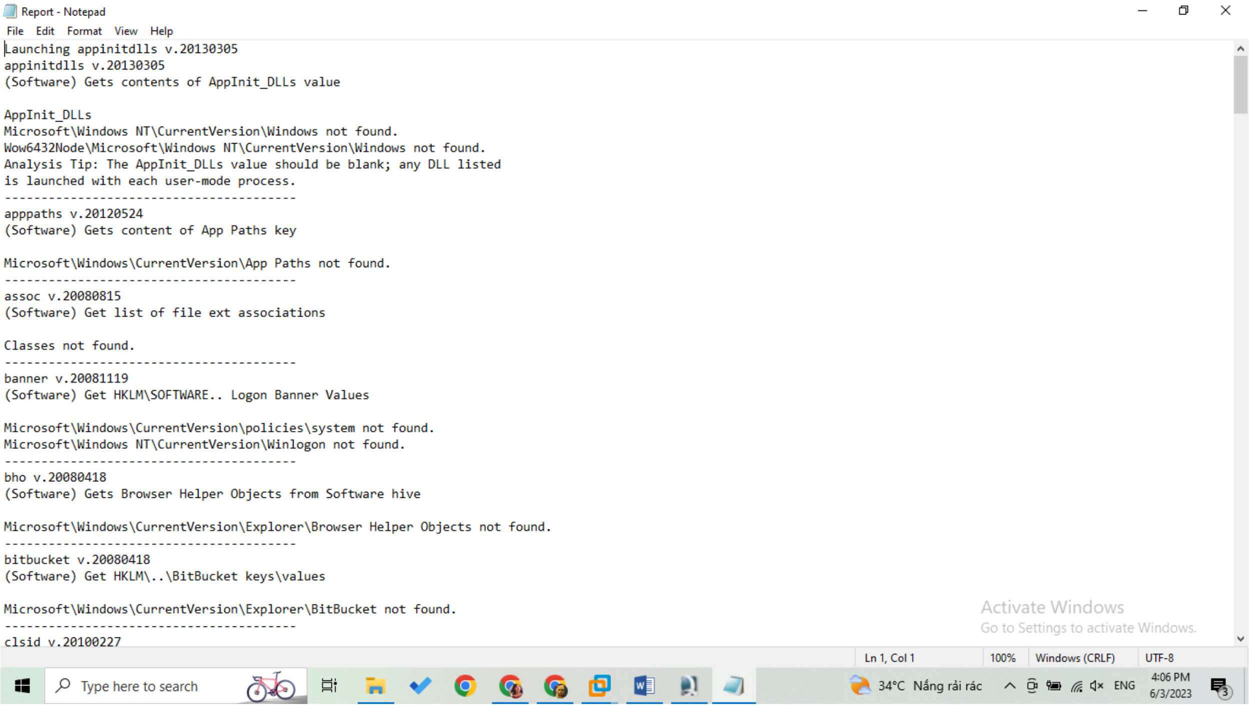
```
virut...Done.
vista_wireless...Done.
win_cv...Done.
winbackup...Done.
winlogon...Done.
winnt_cv...Done.
winver...Done.
yahoo_lm...Done.
1 plugins completed with errors.
```

Done.

- ⇨ Process was done
- ⇨ Save it and name report

On our desktop gonna extract a new txt file named report

Open the that text file:



```
Launching appinitdlls v.20130305
appinitdlls v.20130305
(Software) Gets contents of AppInit_DLLs value

AppInit_DLLs
Microsoft\Windows NT\CurrentVersion\Windows not found.
Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows not found.
Analysis Tip: The AppInit_DLLs value should be blank; any DLL listed
is launched with each user-mode process.
----------------------------------------
apppaths v.20120524
(Software) Gets content of App Paths key

Microsoft\Windows\CurrentVersion\App Paths not found.
----------------------------------------
assoc v.20080815
(Software) Get list of file ext associations

Classes not found.
----------------------------------------
banner v.20081119
(Software) Get HKLM\SOFTWARE.. Logon Banner Values

Microsoft\Windows\CurrentVersion\policies\system not found.
Microsoft\Windows NT\CurrentVersion\Winlogon not found.
----------------------------------------
bho v.20080418
(Software) Gets Browser Helper Objects from Software hive

Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects not found.
----------------------------------------
bitbucket v.20080418
(Software) Get HKLM\..\BitBucket keys\values

Microsoft\Windows\CurrentVersion\Explorer\BitBucket not found.
----------------------------------------
clsid v.20100227
```

⇨ That was the way forensic science team make evidence report.

These are only a handful of the plugins available with the RegRipper tool used in Windows registry forensics. The beauty of this tool lies in its flexibility and scalability.

When they encounter a Windows box, Windows registry proves to be a critical source of information during the investigation