Lab 16: Registry Forensics with RegRipper Plug-ins

Because teaching teaches
teachers to teach

Registry

- Introduction to the window registry.
- Introduction to RegRipper.
- Analysis of Registry files with RegRipper.

Introduction to the window registry

- The window registry is a hierarchical database that stores the configuration setting of the OS, apps, users, and devices.
- It is a valuable source of the information about the system, the installed and executed programs, the users' activities and connected devices.
- Registry artifacts could also reveal the presence of malware.

Introduction to the window registry

- 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

Introduction to the window registry

- The SAM hive contains the user’s settings and hashed passwords.
- Security contains the system security settings.
- Software stores the window and program configuration.
- System stores the information about the system and the connected devices.

Introduction to the window registry

- The registry has two basic elements: keys and values.
- Keys are containers that could include other keys and/or values.
- Values are defined by a name, a type and the associated data value.
- Most important root key is the HKLY_LOCAL_MACHINE where the main registry hives are mapped as subkeys.

Introduction to RegRipper

- RegRipper is a tool to extract and analyze data from the registry.
- It is written by Perl
- RegRipper executes plugins to parse the registry an extract data.

Analysis of Registry files with RegRipper

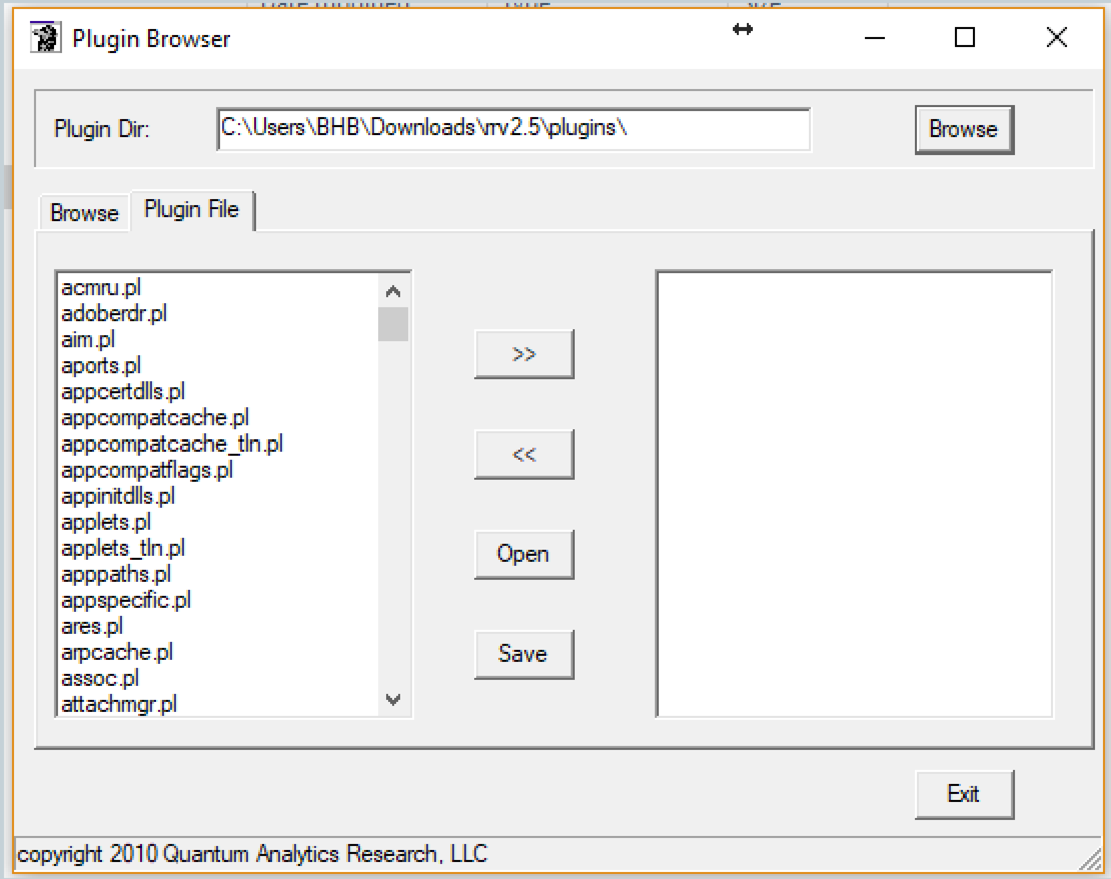
- Download RegRipper, plugins and sample data on https://code.google.com/archive/p/regripper/downloads

Analysis of Registry files with RegRipper

- The plugins are Perl scripts that are contributed by the forensics community. During your forensics case investigations, it extracting information from a particular part of the registry frequently.
- We use available plugins

Analysis of Registry files with RegRipper

- Import plugins



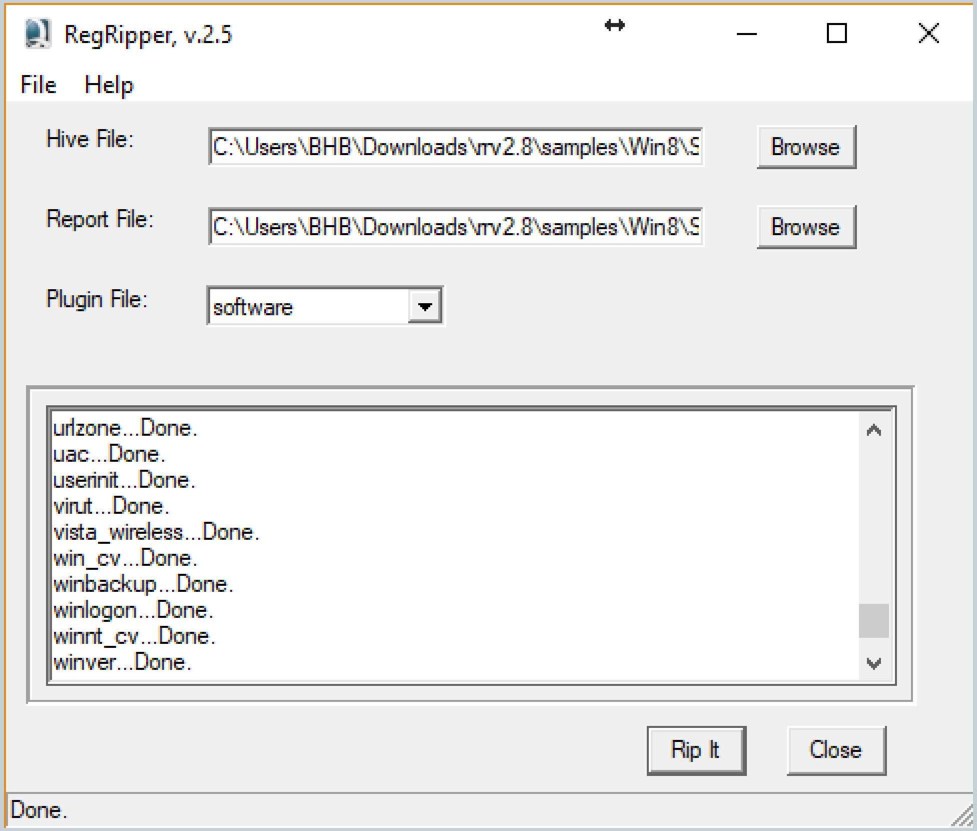
Plugin Dir: C:\Users\BHB\Downloads\rrv2.5\plugins\

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

copyright 2010 Quantum Analytics Research, LLC

Analysis of Registry files with RegRipper

- Run sample



Hive File: C:\Users\BHB\Downloads\rrv2.8\samples\Win8\S

Report File: C:\Users\BHB\Downloads\rrv2.8\samples\Win8\S

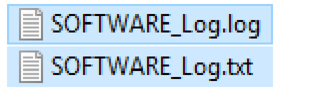
Plugin File: software

```
urlzone...Done.
uac...Done.
userinit...Done.
virut...Done.
vista_wireless...Done.
win_cv...Done.
winbackup...Done.
winlogon...Done.
winnt_cv...Done.
winver...Done.
```

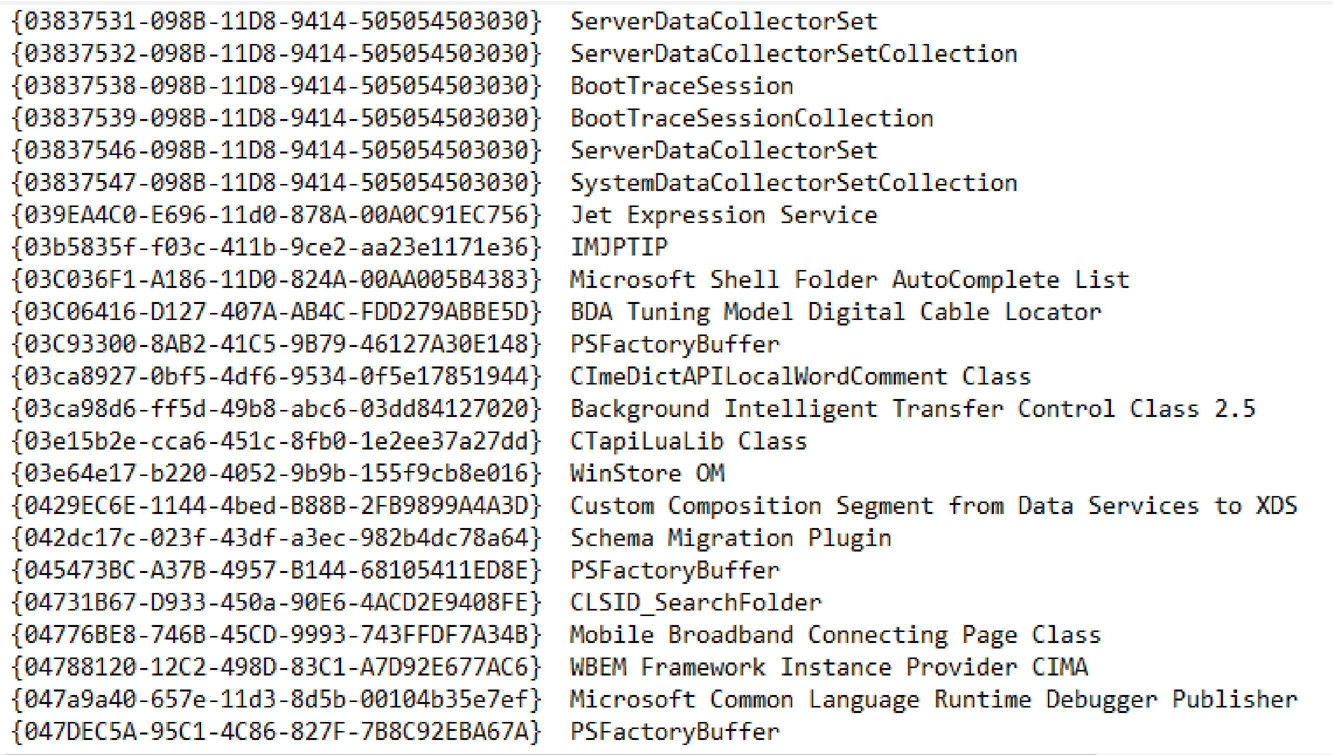
Done.

Analysis of Registry files with RegRipper

- Output:



SOFTWARE_Log.log
SOFTWARE_Log.txt



```
{03837531-098B-11D8-9414-505054503030}  ServerDataCollectorSet
{03837532-098B-11D8-9414-505054503030}  ServerDataCollectorSetCollection
{03837538-098B-11D8-9414-505054503030}  BootTraceSession
{03837539-098B-11D8-9414-505054503030}  BootTraceSessionCollection
{03837546-098B-11D8-9414-505054503030}  ServerDataCollectorSet
{03837547-098B-11D8-9414-505054503030}  SystemDataCollectorSetCollection
{039EA4C0-E696-11d0-878A-00A0C91EC756}  Jet Expression Service
{03b5835f-f03c-411b-9ce2-aa23e1171e36}  IMJPTIP
{03C036F1-A186-11D0-824A-00AA005B4383}  Microsoft Shell Folder AutoComplete List
{03C06416-D127-407A-AB4C-FDD279ABBE5D}  BDA Tuning Model Digital Cable Locator
{03C93300-8AB2-41C5-9B79-46127A30E148}  PSFactoryBuffer
{03ca8927-0bf5-4df6-9534-0f5e17851944}  CImeDictAPILocalWordComment Class
{03ca98d6-ff5d-49b8-abc6-03dd84127020}  Background Intelligent Transfer Control Class 2.5
{03e15b2e-cca6-451c-8fb0-1e2ee37a27dd}  CTapiLuaLib Class
{03e64e17-b220-4052-9b9b-155f9cb8e016}  WinStore OM
{0429EC6E-1144-4bed-B88B-2FB9899A4A3D}  Custom Composition Segment from Data Services to XDS
{042dc17c-023f-43df-a3ec-982b4dc78a64}  Schema Migration Plugin
{045473BC-A37B-4957-B144-68105411ED8E}  PSFactoryBuffer
{04731B67-D933-450a-90E6-4ACD2E9408FE}  CLSID_SearchFolder
{04776BE8-746B-45CD-9993-743FFDF7A34B}  Mobile Broadband Connecting Page Class
{04788120-12C2-498D-83C1-A7D92E677AC6}  WBEM Framework Instance Provider CIMA
{047a9a40-657e-11d3-8d5b-00104b35e7ef}  Microsoft Common Language Runtime Debugger Publisher
{047DEC5A-95C1-4C86-827F-7B8C92EBA67A}  PSFactoryBuffer
```

Conclusions

- 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.
- Computer crimes pose preposterous threats to modern society, as computers are omnipresent. These crimes can be: *fraud*, *intrusions*, *unavailability attacks*, *piracy*, etc. Computer forensic investigators locate *inculpatory* and *exculpatory* evidence from a suspect's computer system. When they encounter a Windows box, Windows registry proves to be a critical source of information during the investigation.

Q & A