LAB16: ***Registry Forensics with RegRipperPlug-ins***

**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.

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
- 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.
- 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
- 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

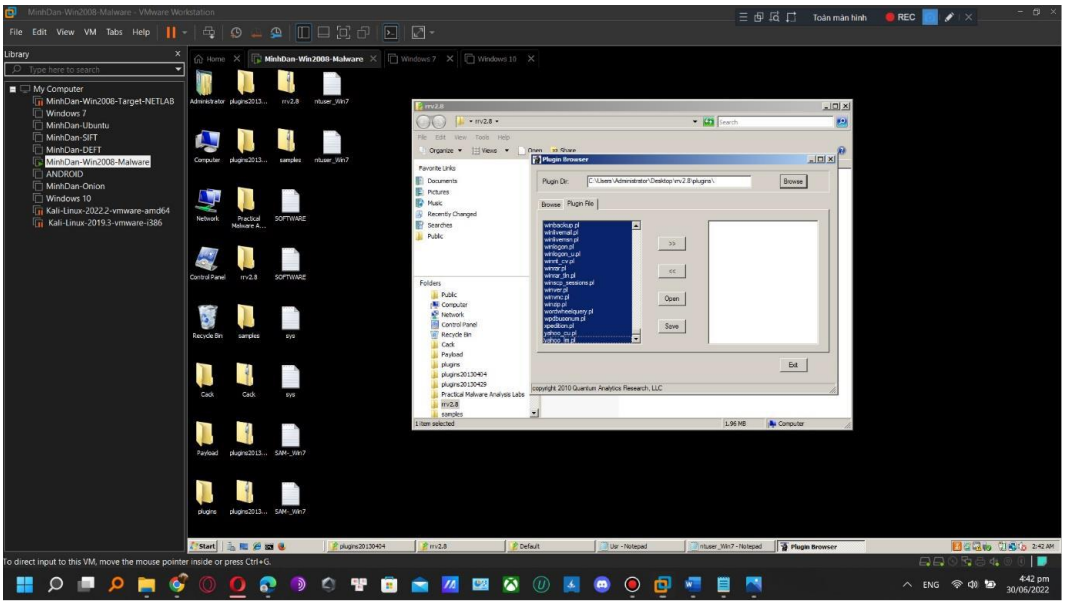
LAB

**Prepare:**

- Viturial Machine : Windows 2008
- 3 files including: Sample , plugins , rrv2.8. Download link is below: https://code.google.com/archive/p/regripp er/downloads

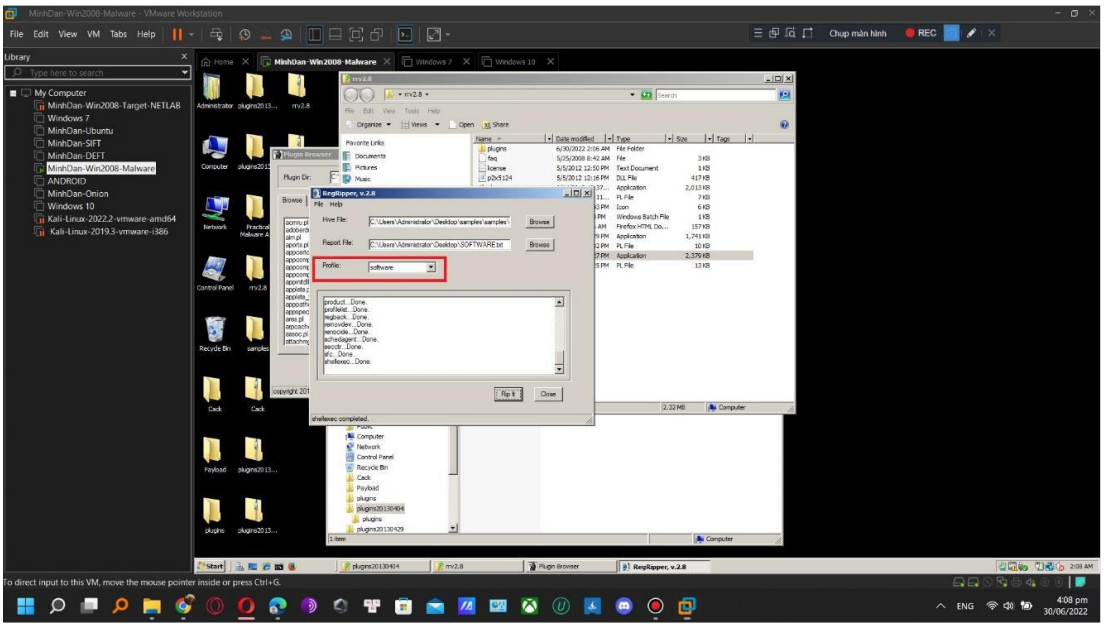
**RegRipper:**

You need to unzip all 3 files above
Note*: if you want to start RegRipper software, you must first import the plugins file.
There will be 2 ways to import:
- Method 1: You copy and paste directly into the file rrv2.8
- Method 2: In the file rrv2.8 there is a program named "pb" and there it will display the interface window so that you can import the plugin's files.

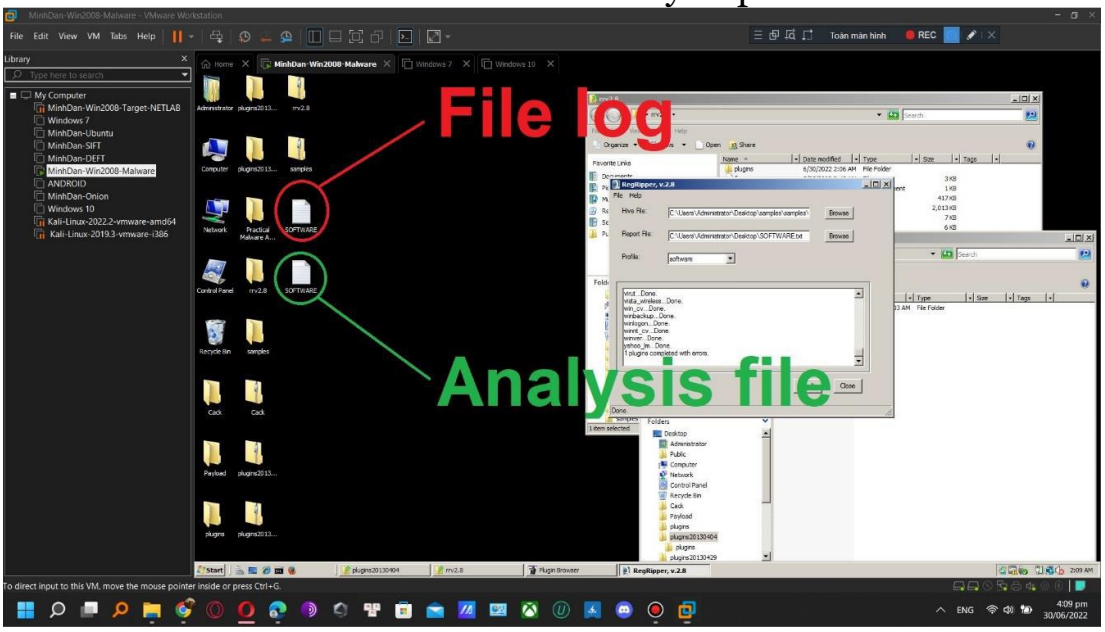



**And here we will conduct the analysis:**
**Analyst file Software:**

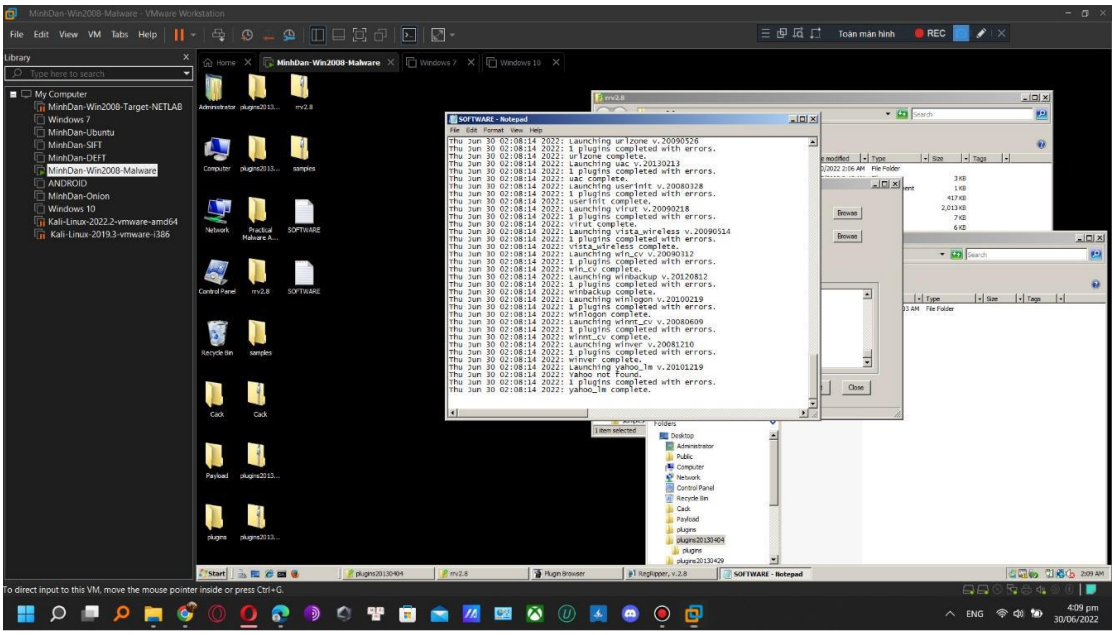
First I will analyze the software file in Win 8
Note: when you analyze any file, you must choose its correct profile. For example, if I am analyzing the file "software", I will choose the profile "software"



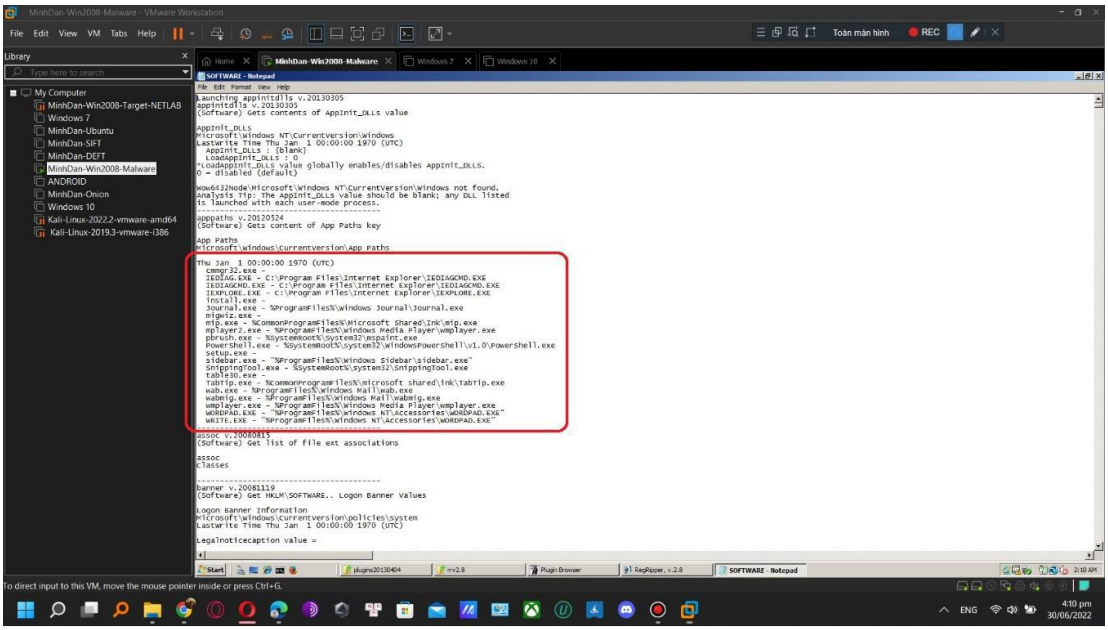
**First file:** it is a log file that stores the analysis actions on the software file.
**Second file:** it's the result after an analysis process.




**File log**

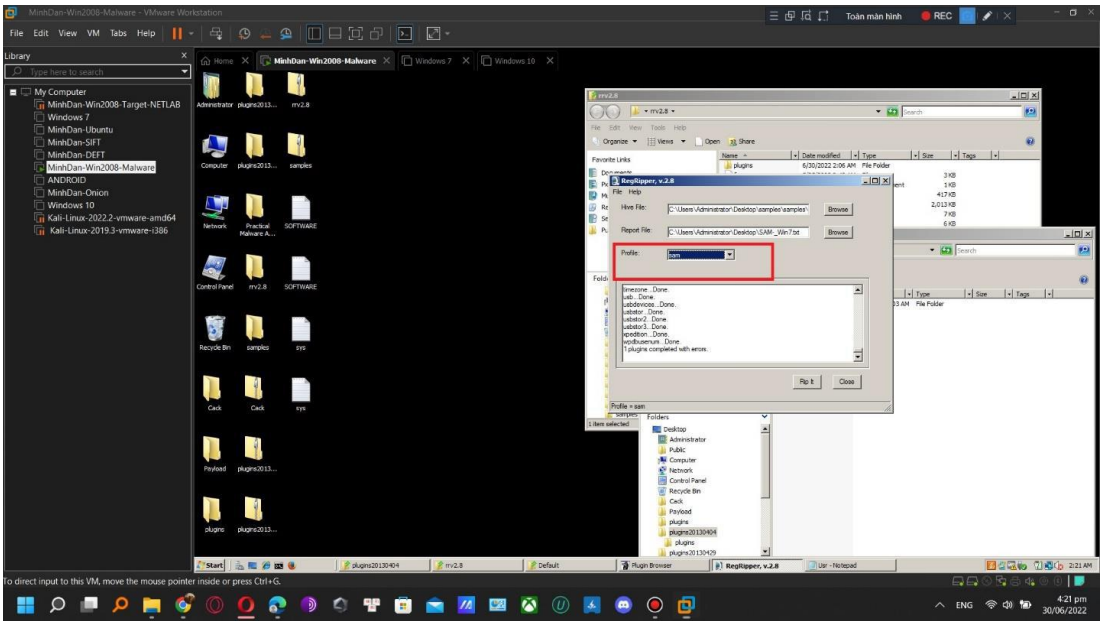


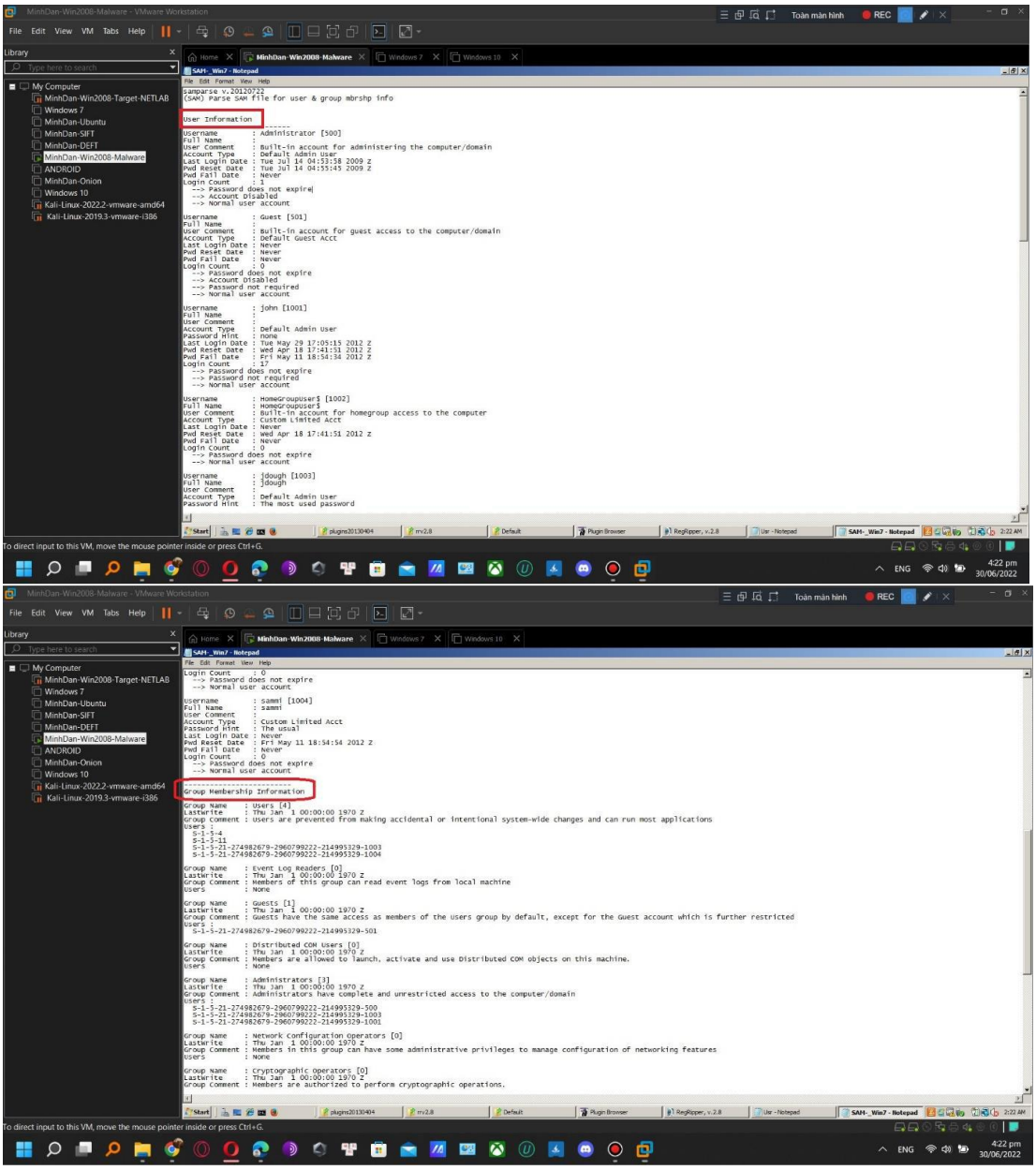
In the second file, we can easily recognize the .exe files and its location in Win 8



## Analyst file SAM:

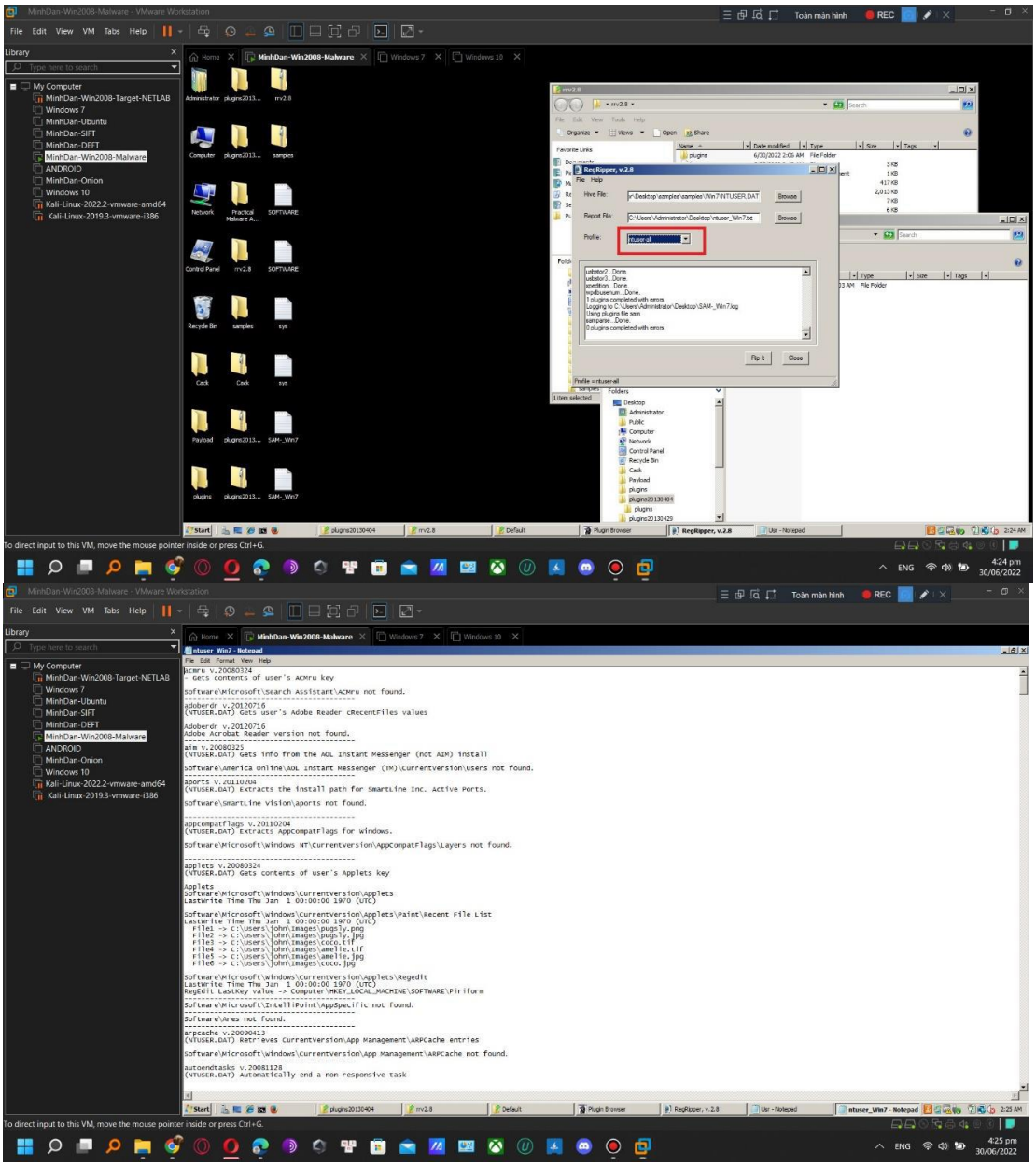
And next we will continue to analyze the SAM file in Windows 7. As you all know, the SAM file is the file that stores the user's and group membership's password, inforamtion, etc ...


MinhDan-Win2008-Malware - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
MinhDan-Win2008-Target-NETLAB
Windows 7
MinhDan-Ubuntu
MinhDan-SIFT
MinhDan-DEFT
MinhDan-Win2008-Malware
ANDROID
MinhDan-Onion
Windows 10
Kali-Linux-2022.2-vmware-amd64
Kali-Linux-2019.3-vmware-i386
Home
MinhDan-Win2008-Malware
Windows 7
Windows 10
RegRipper, v.2.8
Hive File:
Report File:
Profile:
Rip It
Close
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ENG
4:21 pm
30/06/2022




## Analyst file NTUSER.DAT:

And finally the file that I want to demo for you is the ntuser.dat file. This is a setup file that configures the user's kernels or may include user accounts.


MinhDan-Win2008-Malware - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
MinhDan-Win2008-Target-NETLAB
Windows 7
MinhDan-Ubuntu
MinhDan-SIFT
MinhDan-DEFT
MinhDan-Win2008-Malware
ANDROID
MinhDan-Onion
Windows 10
Kali-Linux-2022.2-vmware-amd64
Kali-Linux-2019.3-vmware-i386
RegRipper, v.2.8
Hive File:
Report File:
Profile:
ntuser-all
Rip it
Close
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
4:24 pm
30/06/2022


MinhDan-Win2008-Malware - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
MinhDan-Win2008-Target-NETLAB
Windows 7
MinhDan-Ubuntu
MinhDan-SIFT
MinhDan-DEFT
MinhDan-Win2008-Malware
ANDROID
MinhDan-Onion
Windows 10
Kali-Linux-2022.2-vmware-amd64
Kali-Linux-2019.3-vmware-i386
ntuser_Win7 - Notepad
acmru v.20080324
- Gets contents of user's ACMru key
Software\Microsoft\Search Assistant\ACMru not found.
adoberdr v.20120716
(NTUSER.DAT) Gets user's Adobe Reader cRecentFiles values
Adoberdr v.20120716
Adobe Acrobat Reader version not found.
aim v.20080325
(NTUSER.DAT) Gets info from the AOL Instant Messenger (not AIM) install
Software\America Online\AOL Instant Messenger (TM)\CurrentVersion\Users not found.
aports v.20110204
(NTUSER.DAT) Extracts the install path for SmartLine Inc. Active Ports.
Software\SmartLine Vision\aports not found.
appcompatflags v.20110204
(NTUSER.DAT) Extracts AppCompatFlags for Windows.
Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers not found.
applets v.20080324
(NTUSER.DAT) Gets contents of user's Applets key
Applets
Software\Microsoft\Windows\CurrentVersion\Applets
LastWrite Time Thu Jan 1 00:00:00 1970 (UTC)
Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Recent File List
LastWrite Time Thu Jan 1 00:00:00 1970 (UTC)
File1 -> C:\Users\John\Images\pugsly.png
File2 -> C:\Users\John\Images\pugsly.jpg
File3 -> C:\Users\John\Images\coco.tif
File4 -> C:\Users\John\Images\amelie.tif
File5 -> C:\Users\John\Images\amelie.jpg
File6 -> C:\Users\John\Images\coco.jpg
Software\Microsoft\Windows\CurrentVersion\Applets\Regedit
LastWrite Time Thu Jan 1 00:00:00 1970 (UTC)
RegEdit LastKey value -> Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Piriform
Software\Microsoft\IntelliPoint\AppSpecific not found.
Software\Ares not found.
arpcache v.20090413
(NTUSER.DAT) Retrieves CurrentVersion\App Management\ARPCache entries
Software\Microsoft\Windows\CurrentVersion\App Management\ARPCache not found.
autoendtasks v.20081128
(NTUSER.DAT) Automatically end a non-responsive task
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
4:25 pm
30/06/2022