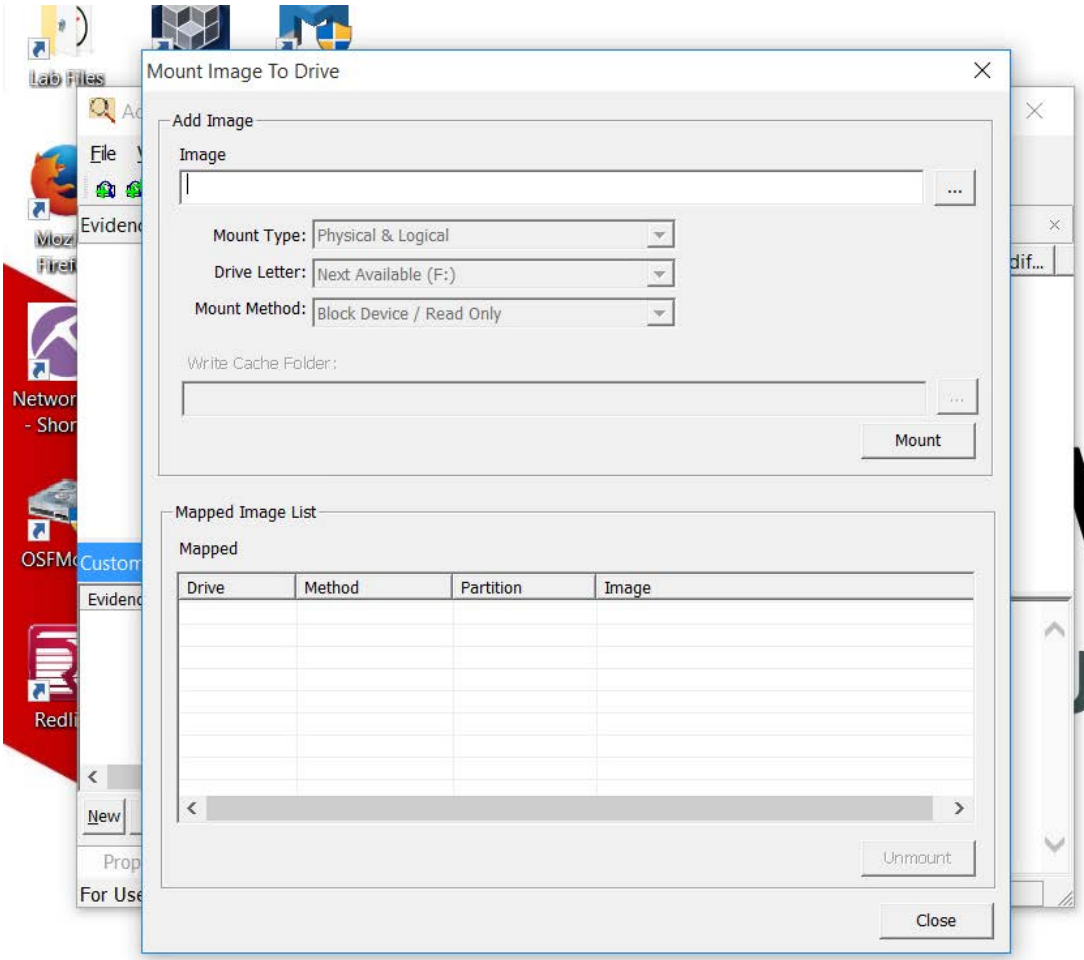
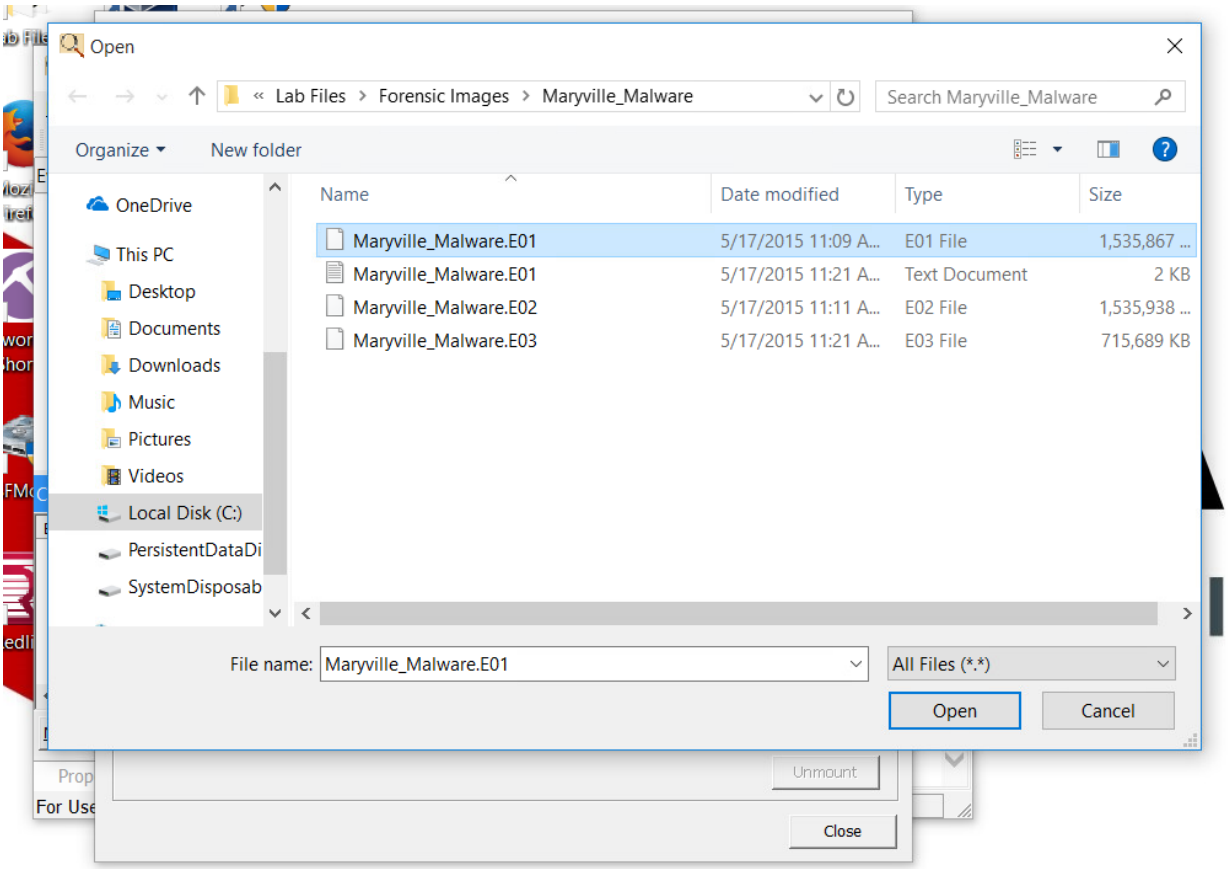
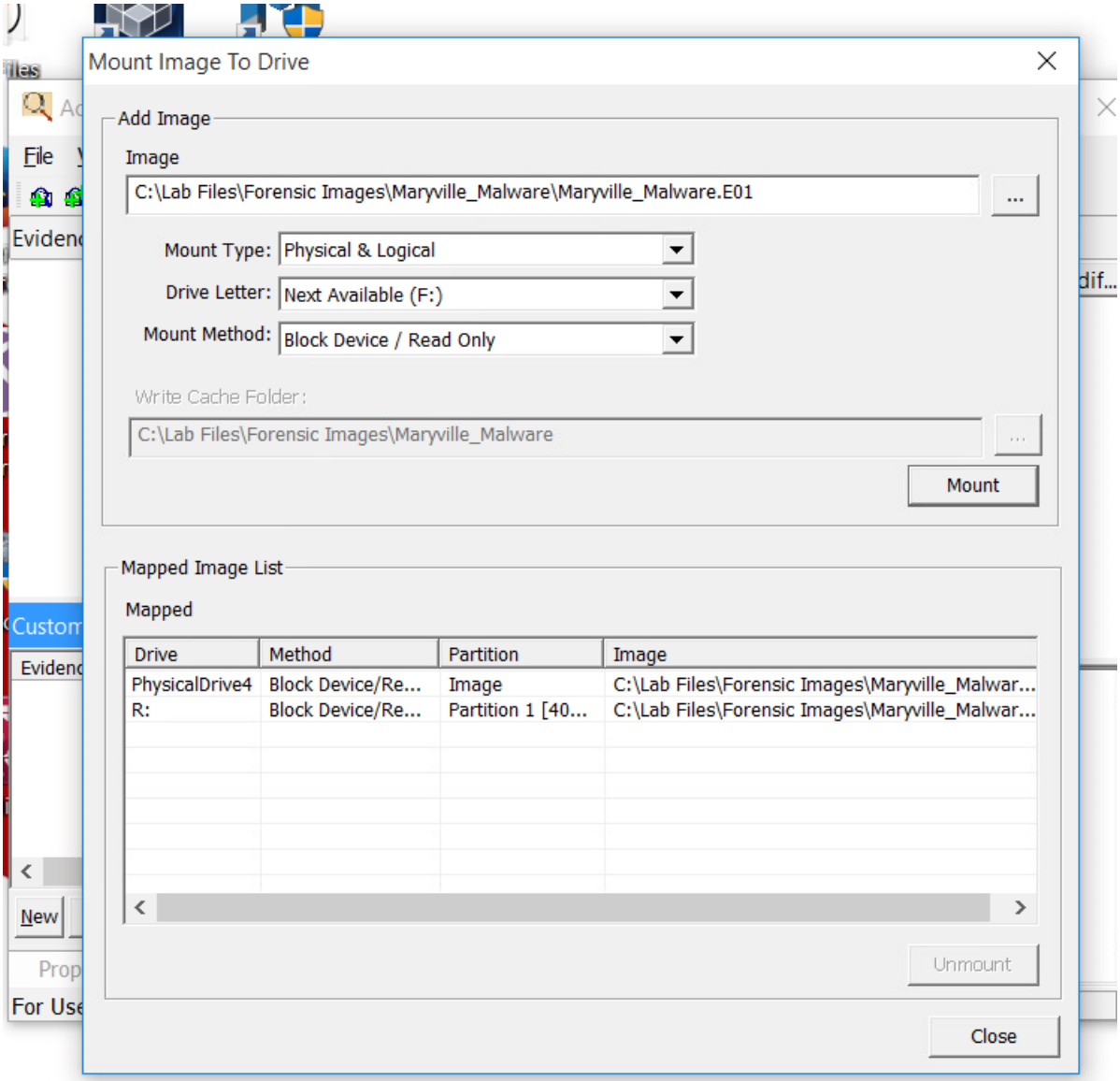
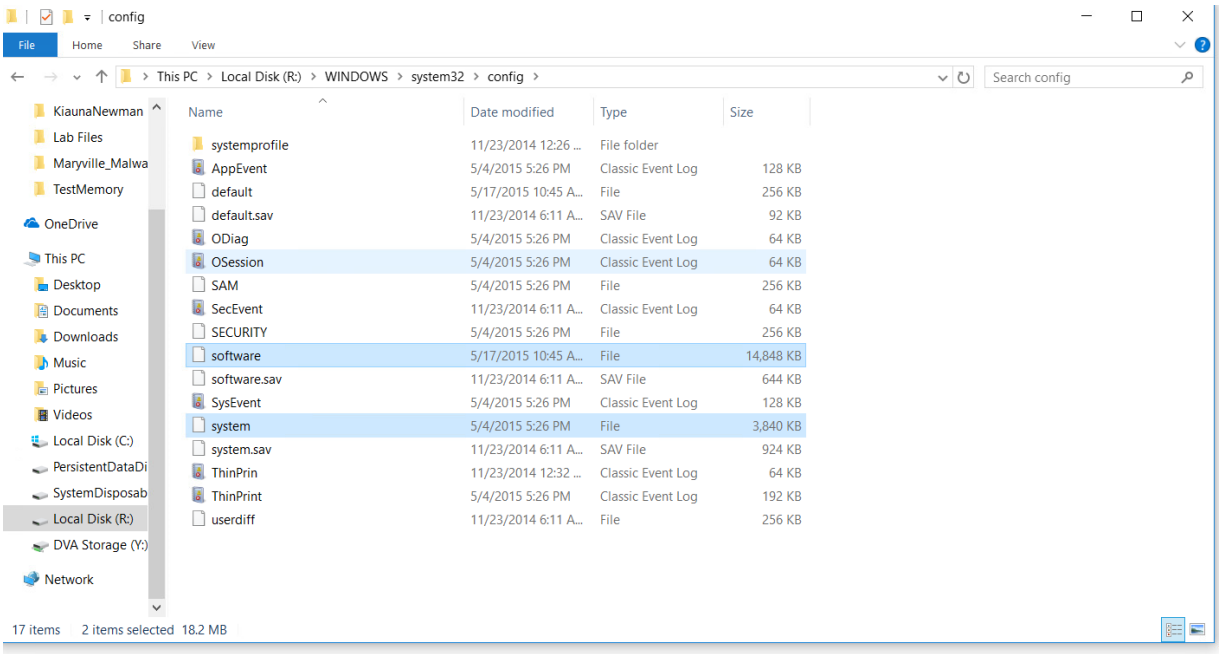
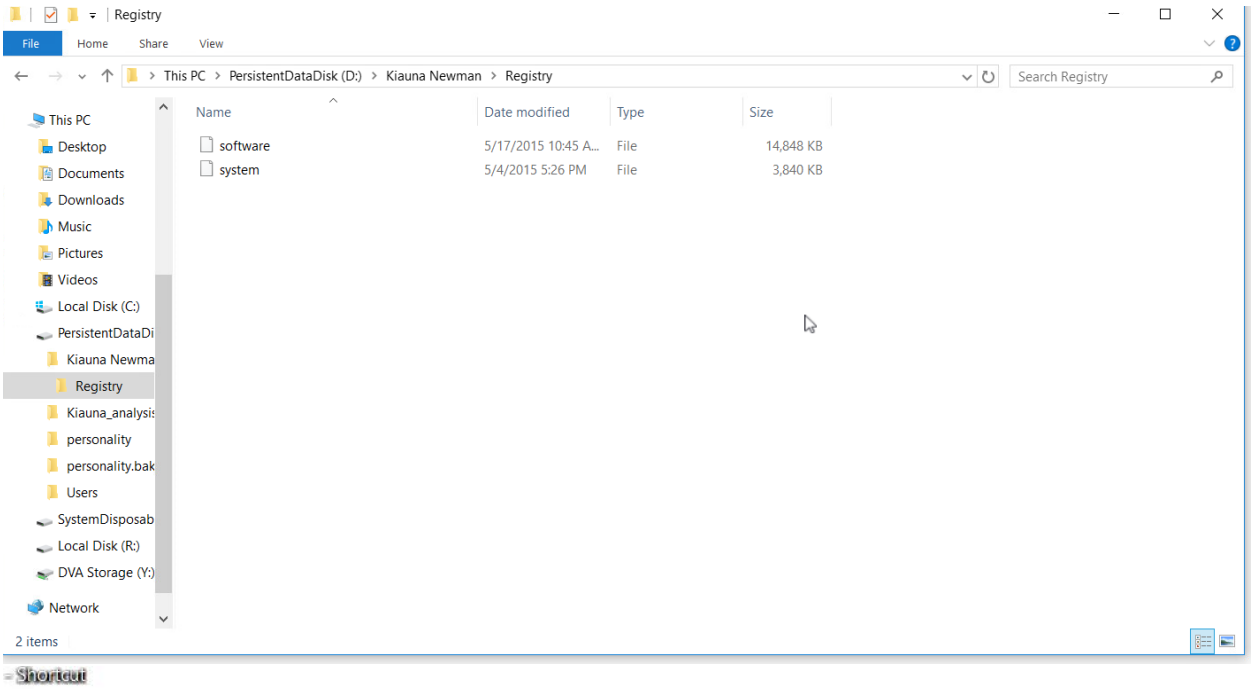

Lab Files
Mount Image To Drive
Add Image
Image
Mount Type:
Physical & Logical
Drive Letter:
Next Available (F:)
Mount Method:
Block Device / Read Only
Write Cache Folder:
Mount
Mapped Image List
Mapped
Drive
Method
Partition
Image
Unmount
Close
File
New

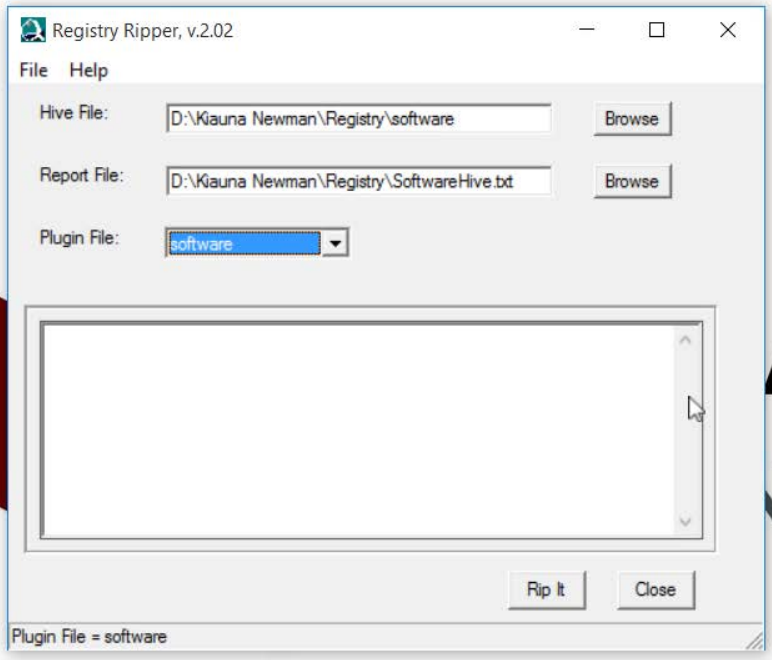

Open
« Lab Files › Forensic Images › Maryville_Malware
Search Maryville_Malware
Organize
New folder
OneDrive
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
PersistentDataDi
SystemDisposab
Name
Date modified
Type
Size
Maryville_Malware.E01
5/17/2015 11:09 A...
E01 File
1,535,867 ...
Maryville_Malware.E01
5/17/2015 11:21 A...
Text Document
2 KB
Maryville_Malware.E02
5/17/2015 11:11 A...
E02 File
1,535,938 ...
Maryville_Malware.E03
5/17/2015 11:21 A...
E03 File
715,689 KB
File name: Maryville_Malware.E01
All Files (*.*)
Open
Cancel
Unmount
Close

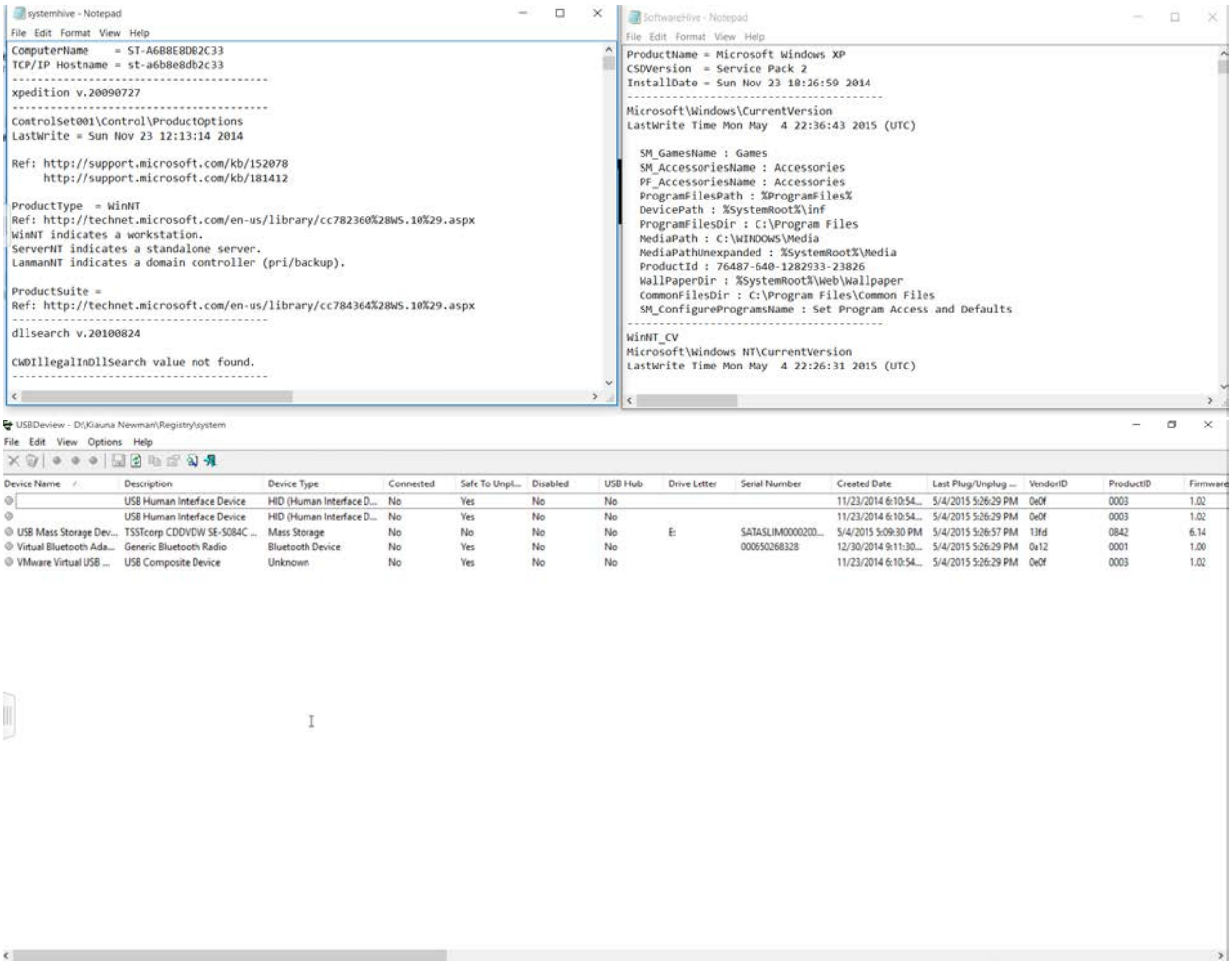

Mount Image To Drive
Add Image
Image
C:\Lab Files\Forensic Images\Maryville_Malware\Maryville_Malware.E01
...
Mount Type:
Physical & Logical
Drive Letter:
Next Available (F:)
Mount Method:
Block Device / Read Only
Write Cache Folder:
C:\Lab Files\Forensic Images\Maryville_Malware
...
Mount
Mapped Image List
Mapped
Drive
Method
Partition
Image
PhysicalDrive4
Block Device/Re...
Image
C:\Lab Files\Forensic Images\Maryville_Malwar...
R:
Block Device/Re...
Partition 1 [40...
C:\Lab Files\Forensic Images\Maryville_Malwar...
Unmount
Close


config
File
Home
Share
View
This PC › Local Disk (R:) › WINDOWS › system32 › config ›
Search config
KiaunaNewman
Lab Files
Maryville_Malwa
TestMemory
OneDrive
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
PersistentDataDi
SystemDisposab
Local Disk (R:)
DVA Storage (Y:)
Network
Name
Date modified
Type
Size
systemprofile 11/23/2014 12:26 ... File folder
AppEvent 5/4/2015 5:26 PM Classic Event Log 128 KB
default 5/17/2015 10:45 A... File 256 KB
default.sav 11/23/2014 6:11 A... SAV File 92 KB
ODiag 5/4/2015 5:26 PM Classic Event Log 64 KB
OSession 5/4/2015 5:26 PM Classic Event Log 64 KB
SAM 5/4/2015 5:26 PM File 256 KB
SecEvent 11/23/2014 6:11 A... Classic Event Log 64 KB
SECURITY 5/4/2015 5:26 PM File 256 KB
software 5/17/2015 10:45 A... File 14,848 KB
software.sav 11/23/2014 6:11 A... SAV File 644 KB
SysEvent 5/4/2015 5:26 PM Classic Event Log 128 KB
system 5/4/2015 5:26 PM File 3,840 KB
system.sav 11/23/2014 6:11 A... SAV File 924 KB
ThinPrin 11/23/2014 12:32 ... Classic Event Log 64 KB
ThinPrint 5/4/2015 5:26 PM Classic Event Log 192 KB
userdiff 11/23/2014 6:11 A... File 256 KB
17 items
2 items selected 18.2 MB


Registry
File
Home
Share
View
This PC > PersistentDataDisk (D:) > Kiauna Newman > Registry
Search Registry
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
PersistentDataDi
Kiauna Newma
Registry
Kiauna_analysis
personality
personality.bak
Users
SystemDisposab
Local Disk (R:)
DVA Storage (Y:)
Network
Name
Date modified
Type
Size
software
5/17/2015 10:45 A...
File
14,848 KB
system
5/4/2015 5:26 PM
File
3,840 KB
2 items

- Shortcut


Registry Ripper, v.2.02
File
Help
Hive File:
D:\Kiauna Newman\Registry\software
Browse
Report File:
D:\Kiauna Newman\Registry\SoftwareHive.txt
Browse
Plugin File:
software
Rip It
Close
Plugin File = software



What is the hostname of the suspect system?

st-a6b8e8db2c33

When was the Operating System installed?

Sunday November 23,2014 at 18:26:59

Are Terminal Services enabled?

yes

a. TSEnalbed= 1
   1= enabled (Terminal Services enabled)
   in system hive text file.

ControlSet001\Control\Terminal Server

What is the Remote Desktop Listening Port?

3389

What is the serial number of the CDROM device previously connected to the system?

SATASLIM0000200…

What is the IP address of the suspect system?

172.16.89.131

What is the system's active time bias?

5 Hours

When was the system last shutdown?

Monday May 4, 2015 at 22:26:10