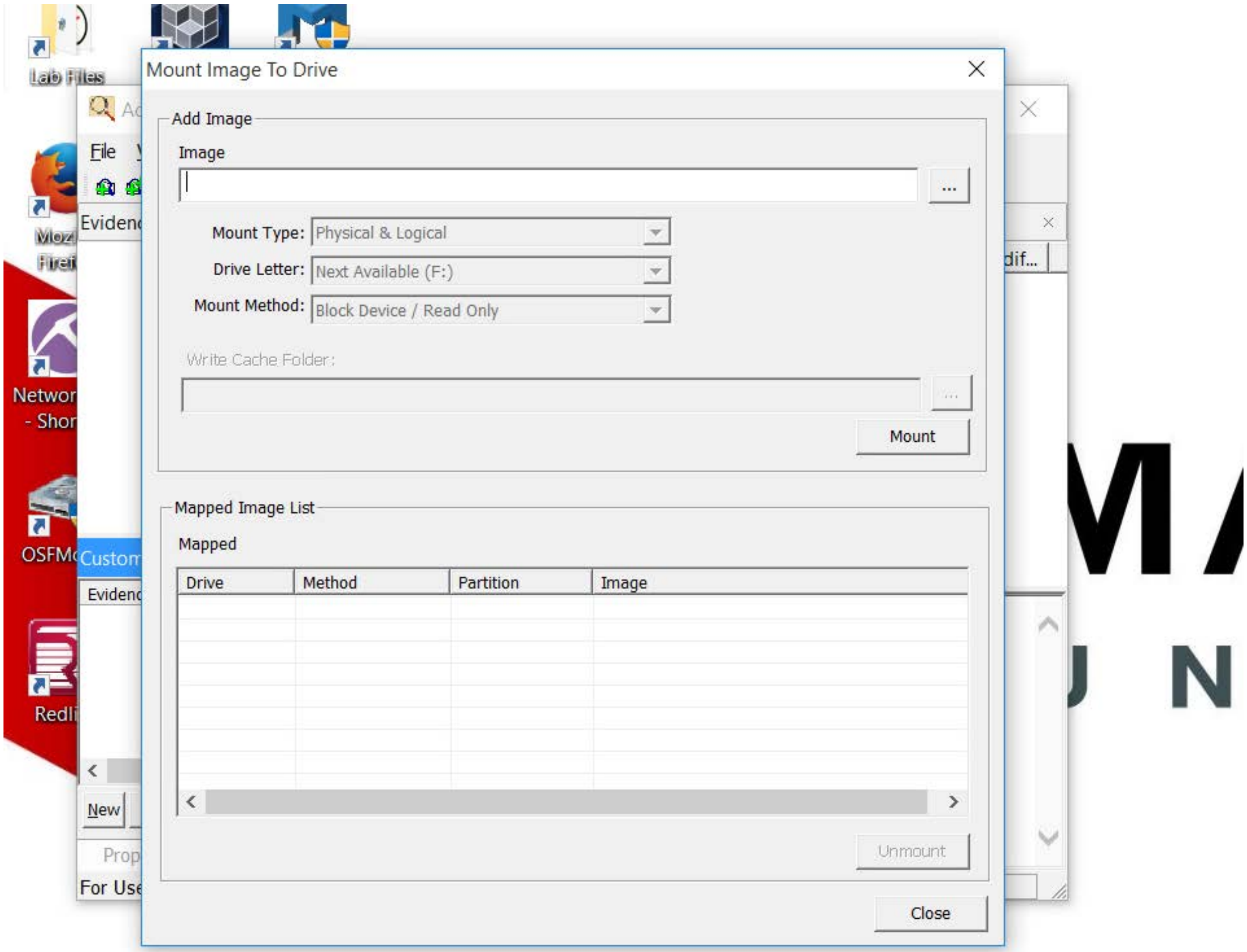
Kiauna Newman Week 6 Windows Registry Analysis 4/22/2018

Use Access Data FTK Imager to mount image to drive



Mount Image To Drive

Add Image

Image:

Mount Type: Physical & Logical

Drive Letter: Next Available (F:)

Mount Method: Block Device / Read Only

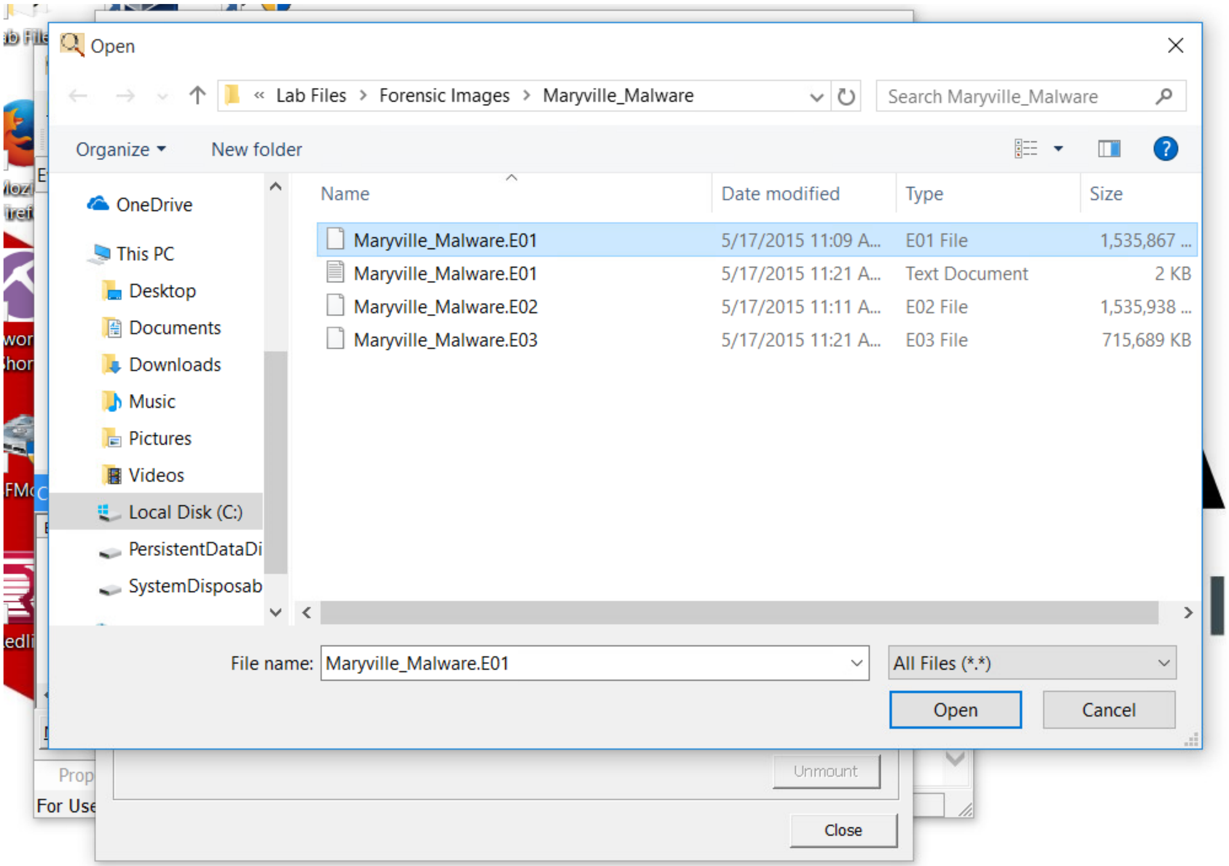
Write Cache Folder:

Mapped Image List

Mapped

Drive	Method	Partition	Image

Select Maryville_Malware image file from Lab Files

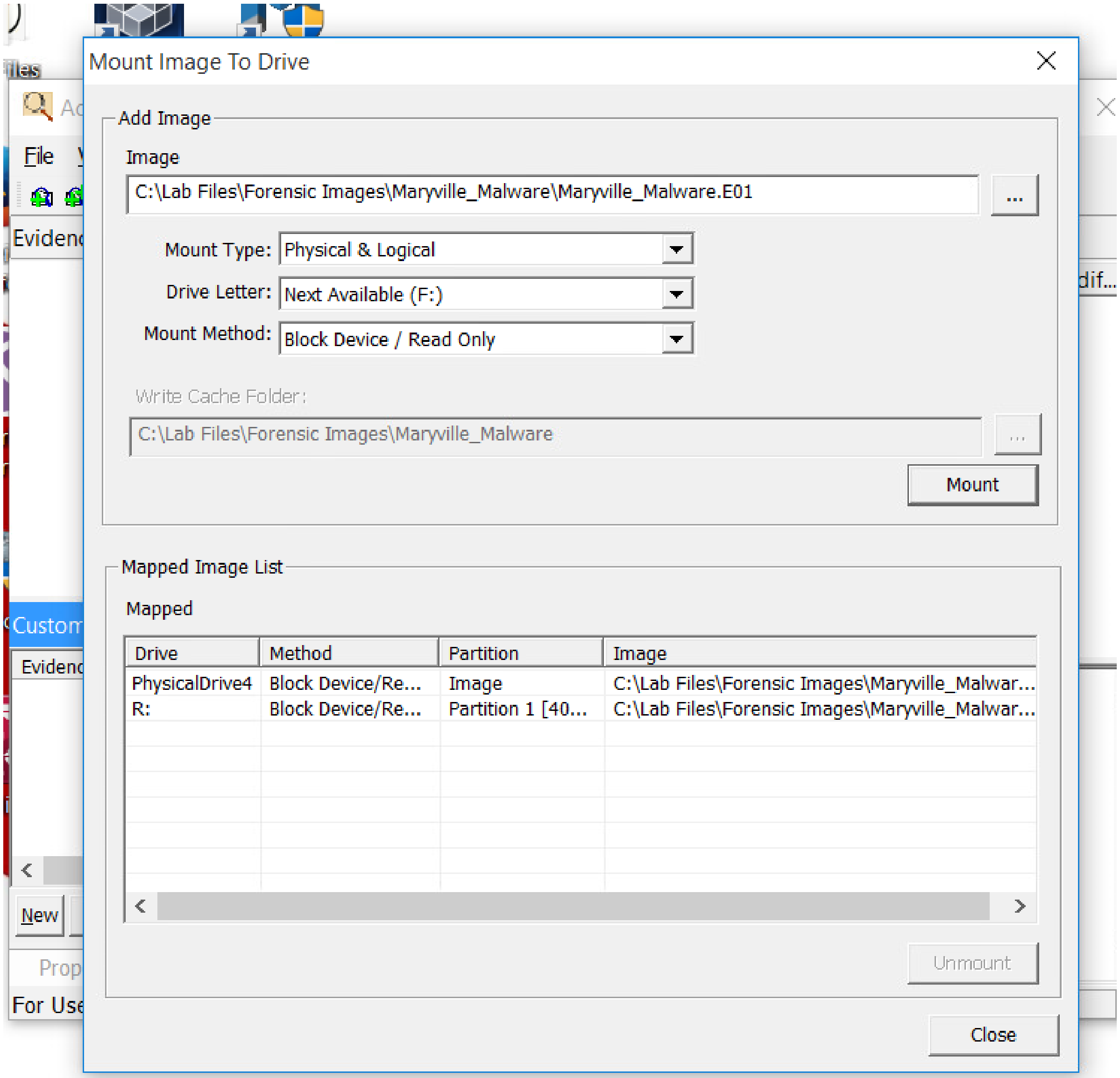


Name	Date modified	Type	Size
Maryville_Malware.E01	5/17/2015 11:09 A...	E01 File	1,535,867 ...
Maryville_Malware.E01	5/17/2015 11:21 A...	Text Document	2 KB
Maryville_Malware.E02	5/17/2015 11:11 A...	E02 File	1,535,938 ...
Maryville_Malware.E03	5/17/2015 11:21 A...	E03 File	715,689 KB

File name: Maryville_Malware.E01

All Files (*.*)

Save image to R drive



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

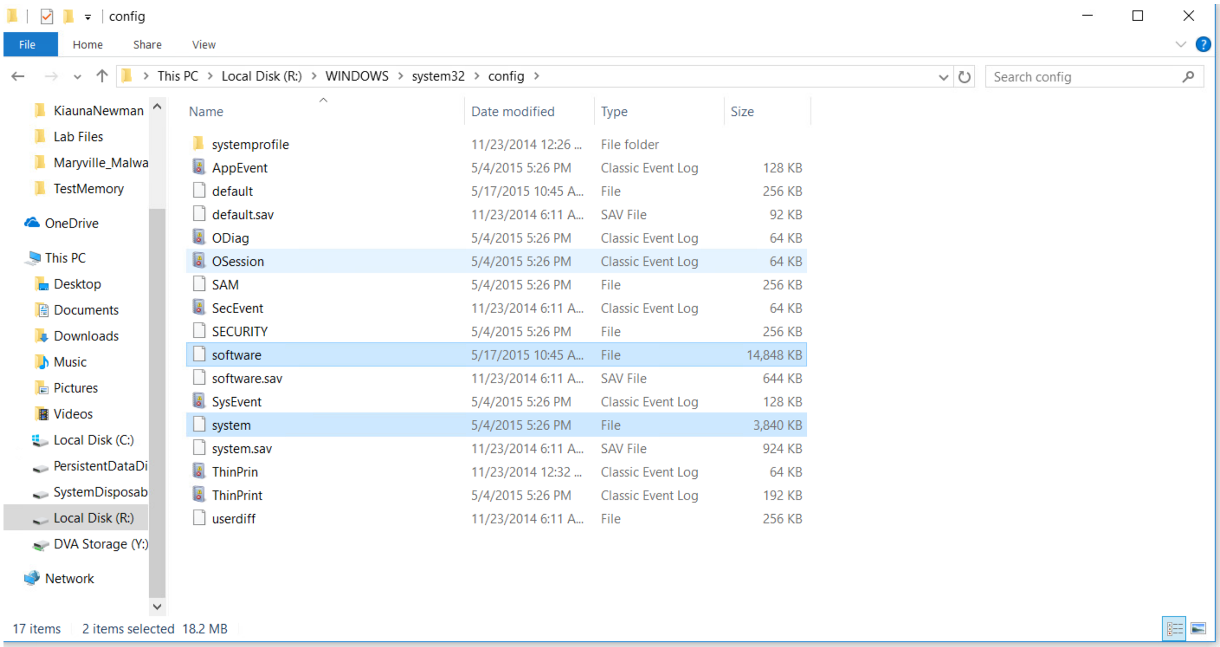
Write Cache Folder: C:\Lab Files\Forensic Images\Maryville_Malware

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...

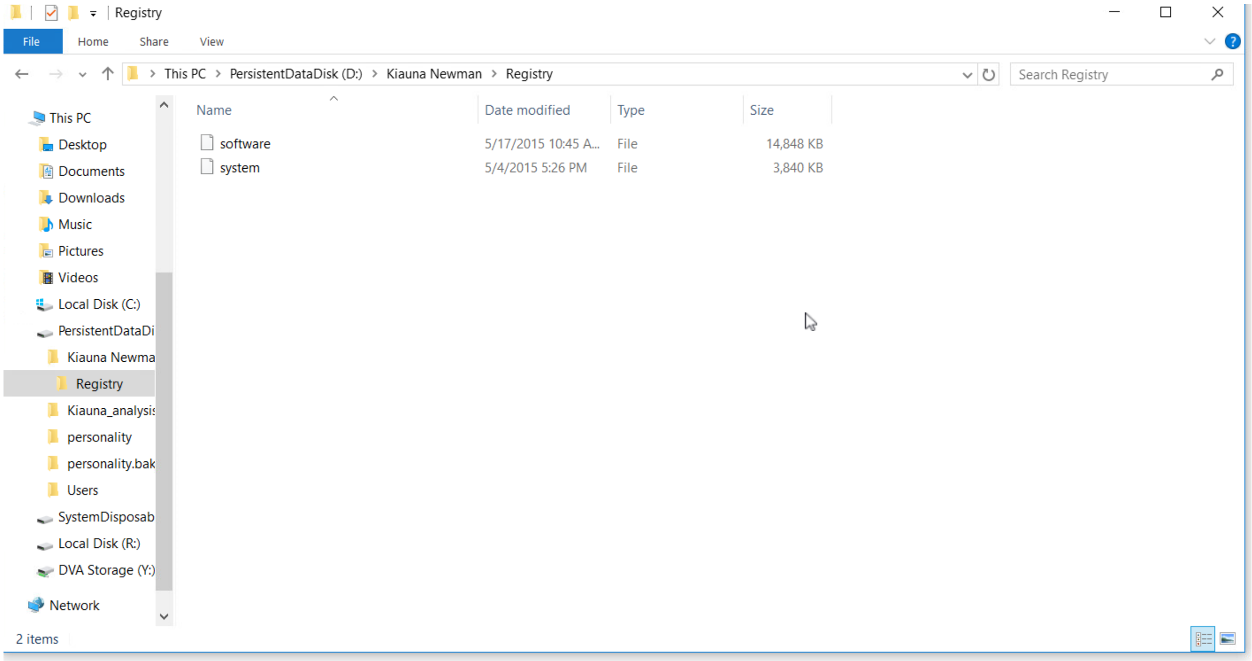
Screenshot of software and system hives in config folder.



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

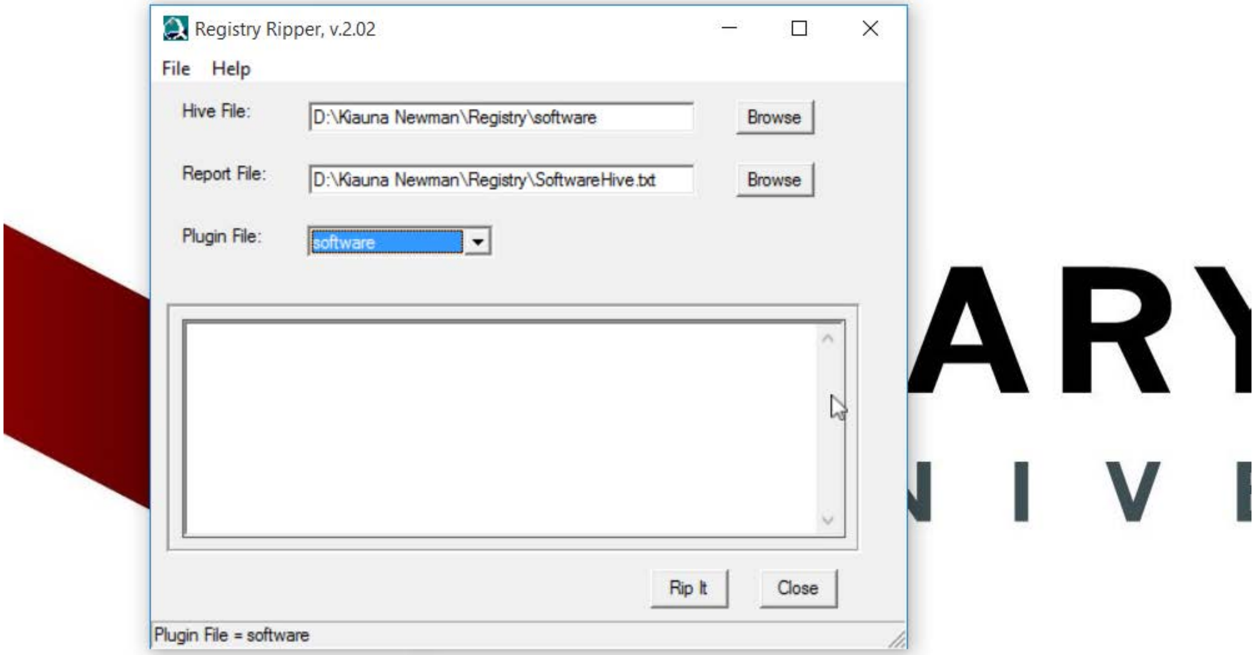
17 items 2 items selected 18.2 MB

Export software and system hive to registry folder located on the D Drive



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

Use registry ripper for software and system hives.



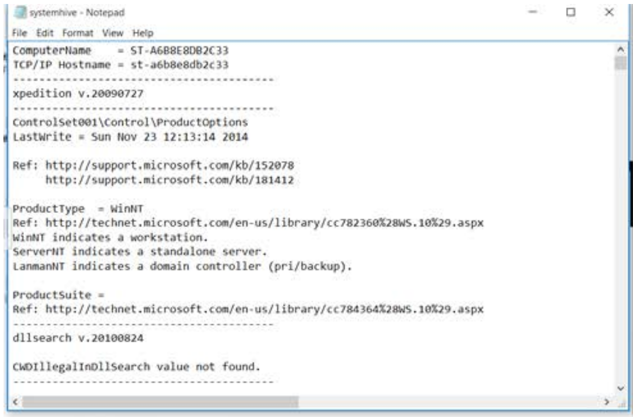
Hive File: D:\Kiauna Newman\Registry\software

Report File: D:\Kiauna Newman\Registry\SoftwareHive.txt

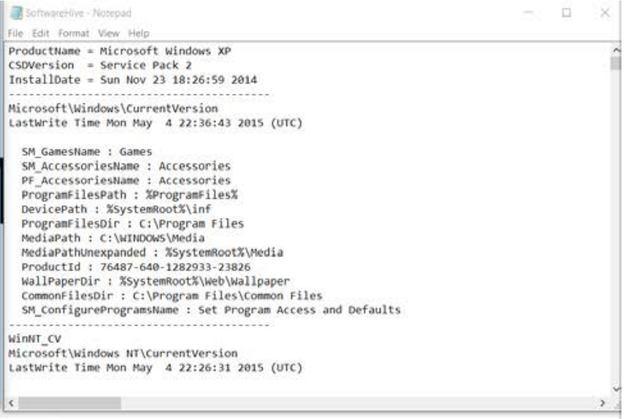
Plugin File: software

Plugin File = software

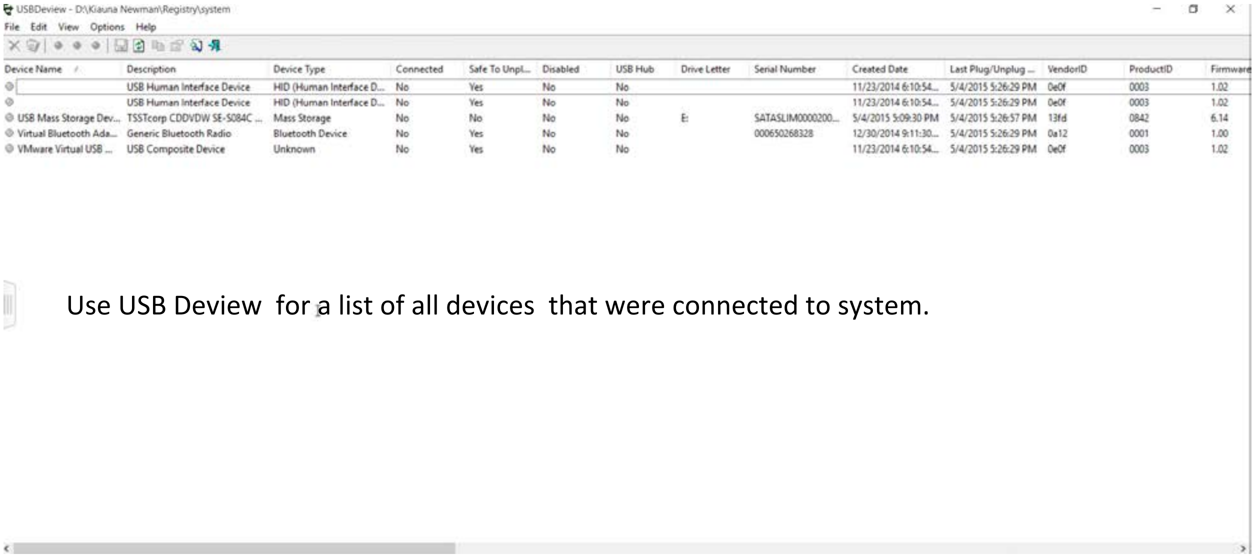
System and software hives results in a text document.



```
ComputerName    = ST-A6B8E8DB2C33
TCP/IP Hostname = st-a6b8e8db2c33
----------------------------------------
xpedition v.20090727
----------------------------------------
ControlSet001\Control\ProductOptions
LastWrite = Sun Nov 23 12:13:14 2014

Ref: http://support.microsoft.com/kb/152078
     http://support.microsoft.com/kb/181412

ProductType  = WinNT
Ref: http://technet.microsoft.com/en-us/library/cc782360%28WS.10%29.aspx
WinNT indicates a workstation.
ServerNT indicates a standalone server.
LanmanNT indicates a domain controller (pri/backup).

ProductSuite =
Ref: http://technet.microsoft.com/en-us/library/cc784364%28WS.10%29.aspx
----------------------------------------
dllsearch v.20100824

CWDIllegalInDllSearch value not found.
----------------------------------------
```



```
ProductName = Microsoft Windows XP
CSDVersion  = Service Pack 2
InstallDate = Sun Nov 23 18:26:59 2014
----------------------------------------
Microsoft\Windows\CurrentVersion
LastWrite Time Mon May  4 22:36:43 2015 (UTC)

  SM_GamesName : Games
  SM_AccessoriesName : Accessories
  PF_AccessoriesName : Accessories
  ProgramFilesPath : %ProgramFiles%
  DevicePath : %SystemRoot%\inf
  ProgramFilesDir : C:\Program Files
  MediaPath : C:\WINDOWS\Media
  MediaPathUnexpanded : %SystemRoot%\Media
  ProductId : 76487-640-1282933-23826
  WallPaperDir : %SystemRoot%\Web\Wallpaper
  CommonFilesDir : C:\Program Files\Common Files
  SM_ConfigureProgramsName : Set Program Access and Defaults
----------------------------------------
WinNT_CV
Microsoft\Windows NT\CurrentVersion
LastWrite Time Mon May  4 22:26:31 2015 (UTC)
```


USBDeview - D:\Kiauna Newman\Registry\system
File Edit View Options Help

Device Name	Description	Device Type	Connected	Safe To Unpl...	Disabled	USB Hub	Drive Letter	Serial Number	Created Date	Last Plug/Unplug ...	VendorID	ProductID	Firmware
	USB Human Interface Device	HID (Human Interface D...	No	Yes	No	No			11/23/2014 6:10:54...	5/4/2015 5:26:29 PM	0e0f	0003	1.02
	USB Human Interface Device	HID (Human Interface D...	No	Yes	No	No			11/23/2014 6:10:54...	5/4/2015 5:26:29 PM	0e0f	0003	1.02
USB Mass Storage Dev...	TSSTcorp CDDVDW SE-S084C ...	Mass Storage	No	No	No	No	E:	SATASLIM0000200...	5/4/2015 5:09:30 PM	5/4/2015 5:26:57 PM	13fd	0842	6.14
Virtual Bluetooth Ada...	Generic Bluetooth Radio	Bluetooth Device	No	Yes	No	No		000650268328	12/30/2014 9:11:30...	5/4/2015 5:26:29 PM	0a12	0001	1.00
VMware Virtual USB ...	USB Composite Device	Unknown	No	Yes	No	No			11/23/2014 6:10:54...	5/4/2015 5:26:29 PM	0e0f	0003	1.02

Use USB Deview for a list of all devices that were connected to system.

Questions

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