

# Windows Forensic Analysis

Dedicated to incident response and computer forensic analysis topics, with respect to Windows 2000, XP, 2003, and Vista operating systems

## WFA: Locating shares in a Windows image

Windows systems record a great deal of user and system activity and information, and much of this information is recorded and maintained automatically, without any user interaction (though some specifics steps may be taken to prevent the data from being recorded). This data can be extremely valuable to a forensic analyst pursuing an investigation.

Users can create shares by opening Windows Explorer, selecting a drive icon or folder, right-clicking and choosing “Sharing and Security...” from the context menu that appears. Users can also use the net share command from the command line to create shares.

### Shares

When examining an image of a Windows system, an analyst may be interested in shares that were available on the system at the time the system was acquired. For example, available shares may be related to another system as part of an examination of multiple systems.

Windows systems maintain information about available shares in the following Registry key:

HKLM\SYSTEM\ControlSet00n\Services\lanmanserver\Shares

### Locating the CurrentControlSet

Within an image, the “CurrentControlSet” key is not visible, as it is volatile (populated by the system at boot), and the analyst will need to mount or access the System Registry hive file within the forensic analysis application being used (i.e., ProDiscover,

EnCase, etc.) and locate the SYSTEM\Select Registry key. The “Current” value identifies which ControlSet00n was loaded as the CurrentControlSet when the system is booted.

Note that default administrative shares<sup>1</sup> (i.e., C\$, D\$, etc.) are not explicitly listed in this key.

Figure 1 illustrates the values within the lanmanserver\Shares key on one system.




 print\$	CSCFlags=0 MaxUses=
 Printer2	CSCFlags=0 MaxUses=
 SharedDocs	CSCFlags=0 MaxUses=

Figure 1

The AutoShareServer<sup>2</sup> (and AutoShareWks) value determines whether or not hidden administrative shares are automatically created on a system. If the value does not exist, or the value is set to 1, then the shares will be created when the system is booted. However, if the value exists and is set to 0, the administrative shares will not be created.

These values can be found beneath the following Registry key:

HKLM\System\ControlSet00n\Services\LanmanServer\Parameters<sup>3</sup>

Note that the AutoShareWks value is not required for Windows 2000<sup>4</sup>. Information available on MS TechNet refers to the

<sup>1</sup> <http://support.microsoft.com/kb/100517>

<sup>2</sup> <http://support.microsoft.com/kb/318755>

<sup>3</sup> <http://support.microsoft.com/kb/245117>

<sup>4</sup> <http://support.microsoft.com/kb/288164>

AutoShareWks value with respect to NT 4.0, and other documentation regarding the topic only refers to the AutoShareServer value on Windows 2000, XP, and 2003.

This same value applies to hidden and other administrative shares (NetLogon, SysVol) available on Windows 2003<sup>5</sup> systems.

Shares appear beneath the lanmanserver\Shares key with value names listed as the names of the shares. These values are multiple string Registry data types and can be easily parsed into their components in order programmatically retrieve path information, etc.

Windows XP Home Edition does not create hidden administrative shares<sup>6</sup>.

### Resources

- MS KB article 141589: *How to Restore Share Definitions To Another Server*<sup>7</sup>

Harlan is a forensic analyst located in the metro DC area, and is the author of three books related to live response and forensic analysis of Windows systems. He also presents at conferences and provides training on those same topics, as well. He can be reached at keydet89@yahoo.com.

---

<sup>5</sup> <http://support.microsoft.com/kb/816524>

<sup>6</sup> <http://support.microsoft.com/default.aspx?kbid=314984>

<sup>7</sup> <http://support.microsoft.com/kb/141589>