installed applications. For example, the RecentDocs key within each user's Registry hive file may contain references to file types unique to particular applications long after the user has deleted the application itself. In addition, there may be remnants of the application having been installed via the Registry, for example if the uninstall routine does not perform a complete cleanup, or if the user deletes the application files without removing the Registry entries. All of these sources can provide the analyst with a history of activity on the system.

Resources

- **WFA: The UserAssist Registry Keys Explained**

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.

and the App Paths key contained subkeys that referenced the previous AOL installation. Applications that do not do a complete and comprehensive job of clean up during an uninstall operation may leave indications of having been installed in this key.

Dr. Watson Logs

When an application crashes, a Dr. Watson log and a memory dump file will be generated. For each application crash, a new memory dump will be created, but the Dr. Watson log file will be appended to, maintaining a historical archive of processes running at various times throughout the lifetime of the system. The Dr. Watson log file is named "drwtsn32.log" and is located (by default) in the following directory (Windows 2000, XP, and 2003):

Documents and Settings\
All Users\Application Data\Microsoft\
Dr Watson

While the drwtsn32.log file contains the timestamp for each application dump, as well as a listing of processes running on the system at the time of the application crash, the processes are listed by name only, without the full path to the executable image, as illustrated in the following listing:

```
 296 issch.exe
 456 DVDLauncher.exe
 492 hpztsb07.exe
1668 AOLSoftware.exe
1704 ViewMgr.exe
1632 aim6.exe
3816 firefox.exe
3720 svchost.exe
 700 uedit32.exe
2216 cmd.exe
1828 perl.exe
3572 drwtsn32.exe
```

However, the information that is available in the process list would give an indication of applications running on the system at the time of the application crash.

Memory Sources

With the release of the Volatility[3] 1.3, forensic analysts have been granted access to additional sources of historical information on systems. This version of the memory analysis framework, released in August 2008, allows the analyst to access crash dumps as well as hibernation files, both of which contain information about applications that had been running on the system at one time. Crash dumps are created when an application crashes and the Dr. Watson debugger steps in. As previously mentioned, the drwtsn32.log file contains a great deal of historical information, as it is appended to during each crash dump, and the user.dmp file simply contains the binary contents of the latest crash dump itself.

In addition, Matthieu Suiche has done a considerable amount of work on the SandMan[4] project, meant to understand and parse the format of hibernation files. This capability has been incorporated into Volatility, providing an analyst with the capability of examining the full contents of RAM at a point in the past. This can give the analyst a clear view of applications and processes that were running at that point in time, as well as processes that had recently exited.

Summary

Various artifacts on Windows systems may be useful to the analyst attempting to determine if certain applications had been installed at one point, launched (may be able to determine which user launched the application), and later deleted. Artifacts within the file system as well as the Registry can provide the analyst with clues as to what applications may have been deleted from the system.

There may be other avenues available to the analyst to locate indicators of previously

[3] https://www.volatilesystems.com/default/volatility
[4] http://sandman.msuiche.net/

sources of login data, which may not be available. Prefetch files are not associated with a specific user, but they do provide an indicator of applications that had been run on the system.

UserAssist Keys
The UserAssist keys are found in the following path:

HKCU\Software\Microsoft\Windows\
CurrentVersion\Explorer\UserAssist

The specific subkey of interest to the analyst is:

{75048700-EF1F-11D0-9888-
006097DEACF9}\Count

This key pertains to user activity associated with the "Active Desktop", or more appropriately the user shell. Values beneath the Count key are (by default) ROT-13 "encrypted", and many of these values contain data that indicates the number of times that the application had been launched, as well as the last time it was launched. Translating these value names and data may provide the analyst with information about applications that had been installed on the system at one time.

This information is also available in the NTUSER.DAT Registry hive files maintained in the XP Restore Points.

MUICache Registry Key
The MUICache Registry key is located within every user's NTUSER.DAT hive file in the following location:

Software\Microsoft\Windows\
ShellNoRoam\MUICache

There isn't a great deal of documentation regarding the purpose of the MUICache key, or under what conditions it may be modified. However, many of the values beneath this key may be added after applications have been run on the system. Parsing the value names from within this key for those that contain executable extensions (.exe, .bat, etc.) may give the analyst indications of applications that had been run on the system at some point in the past, along with their complete path within the file system. However, the values within this Registry key do not have timestamps associated with them (aside from the key's LastWrite time) so there is very little data to pinpoint a timeframe for when the application had been run.

App Paths
There is not a great deal of documentation about the functionality and purpose of the AppPaths Registry key:

HKLM\Software\Microsoft\Windows\
CurrentVersion\App Paths

MS KB article 148375[1] indicates that "the shell launches applications using ShellExecute, which calls CreateProcess after setting the environment block for the application using AppPaths". However, aside from that, there isn't a great deal of documentation as to the purpose and use of the key. MS KB article 555472[2] indicates that the App Paths Registry key may be searched when attempting to launch applications. Other sources at MS further indicate that scripts can be added to the App Paths Registry key so that they can be launched from the Run box, which seems to say that the App Paths key may function much like the PATH environment variable, in that when an application is launched, that the paths listed in the environment variable are searched.

This Registry key (and its subkeys) can provide indications of applications that had been installed at one point, but were deleted. In several cases, there have been no indications of AOL software on the system, although it had been installed at one time,

[1] http://support.microsoft.com/kb/148375
[2] http://support.microsoft.com/kb/555472

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 deleted applications in a Windows image

Windows systems record a great deal of systems and user activity, 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.

There may be times when an analyst needs to determine whether or not an application had been installed and used on a system, and then later deleted or removed in some manner. This can have a significant impact on an investigation, perhaps due to files found on the system, or to network traffic captured during incident response activities. There are several locations on Windows systems where artifacts of deleted applications may reside, and may be useful to the analyst.

XP Restore Points

For Windows XP systems only, Restore Points will contain a great deal of historical data. Besides being created every 24 hrs by default (referred to as System Checkpoints), Restore Points may also be created when software applications are installed, particularly as part of Microsoft Installer (MSI) installation packages. A Restore Point may also be created when that package is removed. For example, two consecutive Restore Points on a test system provided the following reasons for the RP creation:

Removed ProDiscover IR 4.8a
Installed ProDiscover IR 4.84

From this information (retrieved from the rp.log file found within each Restore Point), the analyst can determine when some applications were removed.

In addition to the rp.log files, Restore Points also contain portions of Software, System, and NTUSER.DAT Registry hive files. Both the Software hive file and the NTUSER.DAT hive files found within the Restore Points will contain historical data regarding installed applications and, as explained in a later section of this article, applications that had been run by the user.

Prefetch Files

Another artifact unique to Windows XP systems is the Prefetch file. Windows XP, by default, performs application prefetching (and like Windows 2003, also performs boot prefetching). As a result of the application prefetch process, a Prefetch file is created in the Windows\Prefetch directory. This Prefetch file begins with the name of the executable image file launched, and ends with the .pf extension. This file contains certain metadata, to include the number of times that application had been launched (offset 0x90), and the last time the application was launched (offset 0x78).

The Prefetch directory has a limit of 128 .pf files. This means that once there are 128 .pf files in the Prefetch directory, .pf files are no longer created. If a user on the system had run an application at one point and a .pf file was created, then that file may still be available for review (if a user didn't delete the .pf file).

The drawback of using Prefetch files as an indicator of past activity is that the analyst will have to correlate the last run time extracted from the Prefetch file with other