ï»¿

Forensically interesting spots in the Windows 7, Vista and XP file system and registry

I'm writing this article for two main reasons. First, I've got an anti-forensics class to teach, so I have to learn it anyway. :) 2nd, while I've know the data is there, I did not know it's exact location if someone was to ask me. I've be using tools to recover this information for years, but I wanted to know what the tools were really accessing. For starting this article, I've used Nir's CleanAfterMe tool as sort of a guide, under the assumption that if someone wants to hide an item it must be something a computer forensics investigator would like to know about.

This sort of infromation should be useful to forensics investigators, folks trying to cover their tracks, folks trying to uncover people's track (is my spouse cheating on me?/are my kid looking are porn?) and pen-testers who have physical access to a box. While I'm testing this article on Windows 7, much of it still applies to XP and Vista. This list is NO WHERE NEAR comprehensive. If you have additions, or significant modifications for an entry, I'd be glad to post them and link to your site in the credit info. Please submit your info in a similar format to how I have my entries laid out (that way I can be lazy and just copy and paste).

> A few formatting notes before I begin:
> 1. I'm using "C:\" in the entries for convenience, %SystemRoot% could be located elsewhere, but if you are interested in this material you most likely already know that.
> 2. For versions of Windows before Vista, try replacing "Users" with "Documents and Settings".
> 3. I've also used the Vista/Windows 7 version of the "Application Data"/"AppData" folder. You will have to use "Application Data" instead of AppData on Windows XP. For other file system profile mapping changes, check out the Managing Roaming User Data Deployment Guide.
> 5. To see many of these items, you will have to hit ALT, go to the Tools Menu->Folder options and enable viewing of hidden files and tell Explorer not to hide system files.
> 6. If you see anything in bracket like "<user name>", replace the string with an appropriate value.
> 7. If something does not show up in AppData\Roaming, try AppData\Local or AppData\LocalLow (and of course, vice verse). Keep in mind, somethings will be in Roaming regardless of whether or not you are joined to a domain.

Lot's of information on what files and web sites a user has accessed is repeated over and over again. Just because they wiped one way of finding the data, it does not mean they wiped all of the ways a piece of forensic information can be found. That's one reason why, from an anti-forensics standpoint, using full drive encryption or total drive wiping is far better than using a selective privacy tool like CCLeaner, Cleanafterme, Evidence Eliminator, Window Washer or Cyber Scrub. Now Let's get started.

Windows Explorer

Not to be confused with Internet Explorer, Windows Explorer is the default GUI shell for Windows 7 / Vista / XP. It leaves all sorts of data in the registry and file system for a forensics investigation.

Description: Recently opened files from Windows Explorer
Location: C:\Users\<user name>\AppData\Roaming\Microsoft\Windows\Recent Items
Why you care: It can be quite useful to know what files have been opened recently. Think someone is accessing records of embezzlement? Maybe there is a pointer to the Excel file here that can lead you to where the data has been stored. You may also see links to videos and images in here. I've had this lead to personal embarrassment before while doing a presentation for the ISSA. :)

Entry by: Irongeek, but thanks to Nir.

Description: Network Shortcuts
Location: C:\Users\<user name>\AppData\Roaming\Microsoft\Windows\Network Shortcuts
Why you care: This could show an investigator what fileservers the person is accessing, or on a captured laptop a little about the internal network (useful for pen-testing).
Entry by: Irongeek, but thanks to Nir.

Description: Items recently ran from the "Run" bar
Location:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
Why you care: Useful to know what the person is running using the Windows Run bar, but in Vista and Windows 7 lots of folks use "Search programs and files" text box, which does not show up in this registry key.
Entry by: Irongeek, but thanks to Nir.

Description: ComDlg32 recently opened/saved files
Location: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU
Why you care: This key has sub keys by file extension that can let you know what people have been opening/saving to when the common file save/open dialog comes up. Values are in HEX, but readable if you open them in ASCII view.
Entry by: Irongeek, but thanks to Nir.

Description: ComDlg32 recently opened/saved folders
Location:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU
Why you care: Much like the entry above, but the last folders. Values are in HEX, but readable if you open them in ASCII view.
Entry by: Irongeek, but thanks to Nir.

Description: Recent Docs
Location: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
Why you care: It can be quite useful to know what files have been opened recently. Got to know where people as sticking their data. :)
Entry by: Irongeek, but thanks to Nir.

Description: EXE to main window title cache
Location: HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache
Why you care: Once again, it's useful to know what folks are running on a system, and this might give you an idea what an exe is before you run it yourself (in a VM of course).
Entry by: Irongeek, but thanks to Nir.

Description: User Assist
Location: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
Why you care: This key is suppose to contain information about programs and shortcuts accessed by the Windows GUI, including execution count and the date of last execution, but the way it's stored is less than obvious. Didier Stevens has a tool far parsing the data here:
http://blog.didierstevens.com/programs/userassist/
The version I tested does not seem to work in Windows 7, but Mr. Stevens is on the case.
Entry by: Irongeek, but thanks to Nir and Didier Stevens.

Windows General

Even more Windows Forensics goodness (or badness depending on your perspective).

Description: Temp folder
Location: C:\Users\<user name>\AppData\Local\Temp
Why you care: Lots of programs need a safe place, where the user has permissions, to dump temp data. This is the place to look. They may have wiped/shredded the main file, but there could be a version in this directory depending on how the application works.
Entry by: Irongeek, but thanks to Nir.

Description: Recycle Bin
Location: C:\$Recycle.Bin
Why you care: Do I really need to say?
Entry by: Irongeek, but thanks to Nir.

Description: Last logged on user
Location: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Why you care: Lets you know who logged in last, and may also give you a user name to attack if you're a pen-tester.
Entry by: Irongeek, but thanks to Nir.

Description: Event logs
Location: Should be in C:\Windows\System32\config or C:\Windows\System32\winevt\Logs depending on OS
Why you care: These may be relocated, so do a desktop search for *.evt and *.evtx. Let you know all sorts of things about what is happening on the box.
Entry by: Irongeek.

Description: Last key edited by RegEdit
Location: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit
Why you care: Can be useful to know if the user was tweaking the registry for some purpose (like writing an article on Forensically interesting spots in the Windows 7 file system and registry).
Entry by: Irongeek, but thanks to Nir.

Description: List of Installed USB devices, both connected and unconnected
Location: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB
Why you care: It can be useful to know what USB devices have be connected to a box, and even the vendor and serial number of the device in some cases. Think someone copied the data to a thumbdrive? This may help you trace down what thumbdrive. Think how useful it can be to help tie something a user physical possesses to a box.
Entry by: Irongeek.

Description: List of installed USB storage devices
Location: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR
Why you care: Much like the installed USB devices entry, but just for USB storage. Think someone copied the data to a thumbdrive? This may help you trace down what thumbdrive. CleanAfterMe scrubs HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB but not USBSTOR when I tested last.
Entry by: Irongeek.

Description: SetupAPI Device Log
Location: C:\windows\inf\setupapi.dev.log
Why you care: Log that can help you find out what USB devices have been installed, including thumbdrives. CleanAfterMe scrubs HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB but not this file when I tested last.
Entry by: Irongeek, but thanks to Nir.

Description: Windows Prefetch
Location: C:\Windows\Prefetch
Why you care: Windows Prefetch is a feature in Windows XP and newer system (Including Windows 7) that is ment to speed up commonly executed application and boot load times by recording what on the system is accessed. Mark McKinnon has a tool you might be interested in for parsing this data. Also, you may want to read the Wikipedia entry: http://en.wikipedia.org/wiki/Prefetcher
Entry by: Irongeek, but thanks to Nir and Mark McKinnon.

Internet Explorer

Description: Internet Explorer Temp Folder (IE Cache)
Location: C:\Users\<user name>\AppData\Local\Microsoft\Windows\Temporary Internet Files
Why you care: Look at cached files to see what sort of content people are surfing around for. Also, a great place to start looking if you want to add to your pr0n collection.
Entry by: Irongeek, but thanks to Nir.

Description: IE Cookies
Location: C:\Users\<user name>\AppData\Roaming\Microsoft\Windows\Cookies
Why you care: Let's you know where people have been surfing, and possibly a password or at least a session ID to a website they authenticate to.
Entry by: Irongeek, but thanks to Nir.

Description: Internet Explorer History
Location: C:\Users\<user name>\AppData\Local\Microsoft\Windows\History
Why you care: Again, useful to know what sites someone has visited, when, and how many times.
Entry by: Irongeek, but thanks to Nir.

Description: IE Typed URLs
Location: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedUrls
Why you care: Despite the name, you can not be 100% sure they were typed into the Internet Explorer URL bar, but this can help you distinguished between sites that were manually entered, and ones accessed via a link. The presumption is that if a URL shows up in the TypedURLs key, the person really meant to go there. This is not necessarily the case, just do a search for what happened to poor Julie Amero.
Entry by: Irongeek, but thanks to Nir.

Description: Internet Explorer Forms AutoComplete
Location: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage1
Why you care: This registry key stores autocomplete information for IE, but in an obfuscated form. For old versions of IE try Nir's PSPV, for IE 7 and newer try IE PassView to decode this data.
Entry by: Irongeek, but thanks to Nir.

Description: Internet Explorer Password AutoComplete
Location: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2
Why you care: This registry key stores autocomplete password information for IE, but in an obfuscated form. For old versions of IE try Nir's PSPV, for IE 7 and newer try IE PassView.
Entry by: Irongeek, but thanks to Nir.

Description: Printer spool folder
Location: C:\Windows\System32\spool\PRINTERS
Why you care: Sometimes a print job will get stuck here, and we all know what useful information people sometimes print. To read these spl files you will need the right PCL/PostScript parser. Try some of the tool listed at the bottom of this page: http://www.undocprint.org/formats/winspool/spl
I had ok luck with O&K Printer Viewer and LBV SPLViewer.
Entry by: Irongeek.

Firefox

I Did these tests in Firefox 3.5 (mostly). Results may vary. Take a look at anything in C:\Users\<user name>\AppData\Local\Mozilla\Firefox\Profiles\<some profile number>.default\, but especially *.sqllite files.

Description: Firefox Cached Pages
Location: C:\Users\<user name>\AppData\Local\Mozilla\Firefox\Profiles\<some profile number>.default\Cache
Why you care: While IE stored its cache in easy to read file names, Firefox makes it a little harder. You will have to open up these files to look at their headers to see what they are, or use a tool like MozillaCacheVeiwer. Files with names like _CACHE_001_ are good for looking at the banners of recently accessed sites (so you can see the server type and the like), which will be useful to a pen-tester wanting to fingerprint system. "_CACHE_MAP_" seems to be an index of items in the cache, but I've not looked into it enough yet myself. Check out http://www.securityfocus.com/infocus/1832 for more info on _CACHE_MAP_. Of course, these _CACHE_ files are also awesome for attaching dates to server access.
Entry by: Irongeek, but thanks to Nir.

Description: Firefox Form History File
Location: C:\Users\<user name>\AppData\Roaming\Mozilla\Firefox\Profiles\<some profile number>.default\formhistory.sqlite
Why you care: This file has tons of information about web forms filled out in Firefox, when they were filled out, and what with. This is an SQLLite file that contains the browsing history for Firefox/Mozilla. You can use the Open Source app SQLLiteStudio to read the file. For other SQLLite tools, check out this site.
Entry by: Irongeek.

Description: Firefox Passwords File
Location: C:\Users\<user name>\AppData\Roaming\Mozilla\Firefox\Profiles\<some profile number>.default\signons.sqlite
Why you care: This SQLLite file should contain Firefox's stored passwords. Nir has a tool for grabbing Firefox passwords, but it failed on my Firefox 3.5.2 installation (you can still use Firefox itself to see the password, under security options). You can use the SQLLiteStudio app to read the file, but the

information is obfuscated. For other SQLLite tools, check out this site. Even if you can't find the passwords, you can find "Disabled hosts", which may tell you what sites the owner sees as too sensitive to store passwords for.
Entry by: Irongeek.

Description: Firefox Cookies
Location: C:\Users\<user name>\AppData\Roaming\Mozilla\Firefox\Profiles\<some profile number>.default\cookies.sqlite
Why you care: Let's you know where people have been surfing, and possible a password or at least a session ID to a website they authenticate to. You can use the SQLLiteStudio to read the file, or Nir's Cookie viewer.
Entry by: Irongeek, but thanks to Nir.

Other Apps

These are items that may not fit in other categorizes. Just about anything in "C:\Users\<user name>\AppData\" is worth taking a look at.

Description: Recently Opened Office Docs
Location: C:\Users\<user name>\AppData\Roaming\Microsoft\Office\Recent
Why you care: Yet another way to see what files someone has been accessing. Notice how it's hard to cover all activity tracks?
Entry by: Irongeek, but thanks to Nir.

Description: Files recently accessed by Windows Media Player
Location: HKEY_CURRENT_USER\Software\Microsoft\MediaPlayer\Player\RecentFileList
Why you care: I could not get this one to work in Windows 7, maybe it has moved?
Entry by: Irongeek, but thanks to Nir.

Description: Offline Outlook Mailbox
Location: C:\Users\<user name>\AppData\Local\Microsoft\Outlook\outlook.ost
Why you care: Here is were your Outlook 2007 mailbox is stored, and email is always a useful source of forensic information. If you find a freeware or open source parser please let me know (my quick search only showed commercial ones). Byte Bucket suggested this http://www.five-ten-sg.com/libpst/ but I have yet to test it.
Entry by: Irongeek.

Description: Temp folder for Outlook attachments
Location: C:\Users\<user name>\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\<random value>\
Why you care: Here is were Outlook 2007 sometimes puts attachments you directly open from an email. If you are trying to find the exact location of this

folder, look in the reg key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Outlook\Security
Entry by: Irongeek.

Description: Flash Cookies Location
Location: C:\Users\<user name>\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\<random value>\
Why you care: So, you deleted all of the cookies you browsers have so folks can't track where you have been, but what about cookie that Adobe Flash makes at times? Lots of wiping software seems to miss this area, and it's a great way to know where someone has been.
Entry by: Irongeek.

More to come...

Change log:
11/03/2014: Fixed a misnamed folder @ppolstra found (Recent Items).
9/24/2009: Worked on formatting and added entries for "Temp folder for Outlook attachments", "Flash Cookies Location" and "Printer spool folder". I also added a menu so you can quickly find the entry you are looking for.
8/13/2009: First posted.

If you would like to republish one of the articles from this site on your webpage or print journal please contact IronGeek.