APPLIED SECURITY™

Windows 7 Forensic Analysis

H. Carvey

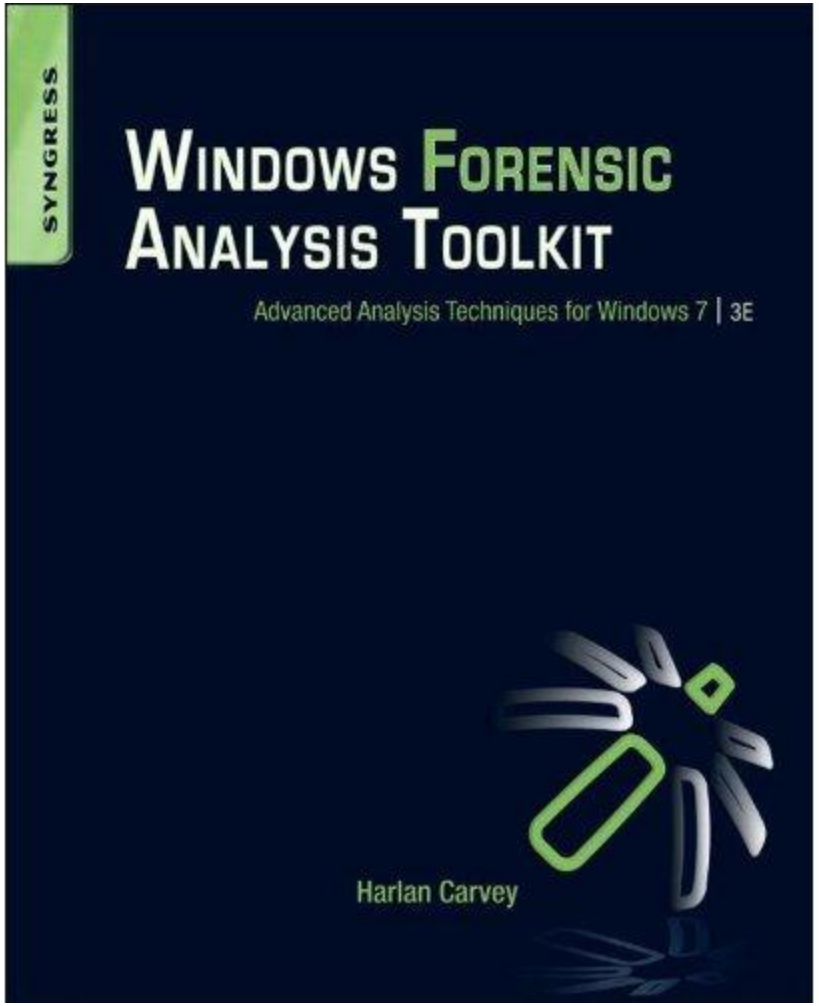
Chief Forensics Scientist, ASI

Who am I?

Chief Forensics Scientist at ASI.
Forensic Nerd.
Published Author.

Why are we here?

To talk about Windows 7 Forensic Analysis



Every time MS has released a new version of Windows, there has been anxiety and trepidation within the DFIR community.

If we take a deep breath, relax, and *follow our processes*, we find each new version of Windows brings with it even more potential sources of evidence, many of which persist even in the face of counter-forensics techniques being used.

- View the system as a system of interconnected components
  - Something that occurs on one component affects others
  - User launches application, UserAssist entry is created/modified, Prefetch file is created/modified, LNK/Jump List file created/modified, etc.
- Locard's Exchange Principle
  - Transfer of digital material when two systems interact, or when user interacts with system
- "*The absence of an artifact where you would expect to find one is itself an artifact*."
- Least Frequency of Occurrence (LFO)

- What is “analysis”? What is it today, and where do we need to go?
  - Analysis = Data extraction/collection/correlation + **interpretation**
- Start with goals and an acquired image
  - Snapshot of a system, “frozen” in time
- Identification and correlation of data sources in order to develop context pursuant to our analysis goals
- We’re mostly familiar with Windows XP, but Windows 7 is now hitting analysts’ desks

System Similarities: XP & Win7

- MFT – little difference
  - Updating file last access time disabled by default starting with Vista
- Registry – same binary structure
- Prefetch files (different offsets, similar format, same data)
- Many apps still maintain (text) logs
- OLE “structured storage”, file-system-within-a-file
  - Office 97 (later versions use different format)
  - Jump Lists, Sticky Notes, IE session restore files
- Hibernation files

- Directory structure
  - "C:\Users" vs. "C:\Documents and Settings"
- XP "Restore Points" => VSCs/"Previous Versions" (Vista+)
- MRUs moved from Registry to Jump Lists
  - CustomDestinations: Header + appended LNK streams
  - AutomaticDestinations: LNK streams managed via OLE file format (+ DestList stream)
- Windows Event Logs (*where do we begin??*)
  - The usual: Application, System, Security
  - LOTS more!
- Win7 includes more artifacts
  - More tracking of user/system activity

Does XP go away?

I say, “nay, nay!”

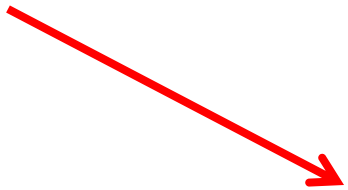
WinXP can be installed on some versions of Windows 7 and run in a virtual environment called “XPMode”. VirtualPC can be installed for free.

Comedian John Pinette

Not only is additional information recorded in Win7 Registry regarding USB devices connected to the system, and WAPs the system was connected to, but we also have sources of historical data:

- RegIdleBackup (every 10 days; doesn't include NTUSER.DAT)
- VSCs

NTUSER.DAT from image…
Thu Jan 21 03:10:26 2010 Z
UEME_RUNPATH:C:\Program Files\Skype\Phone\Skype.exe (14)

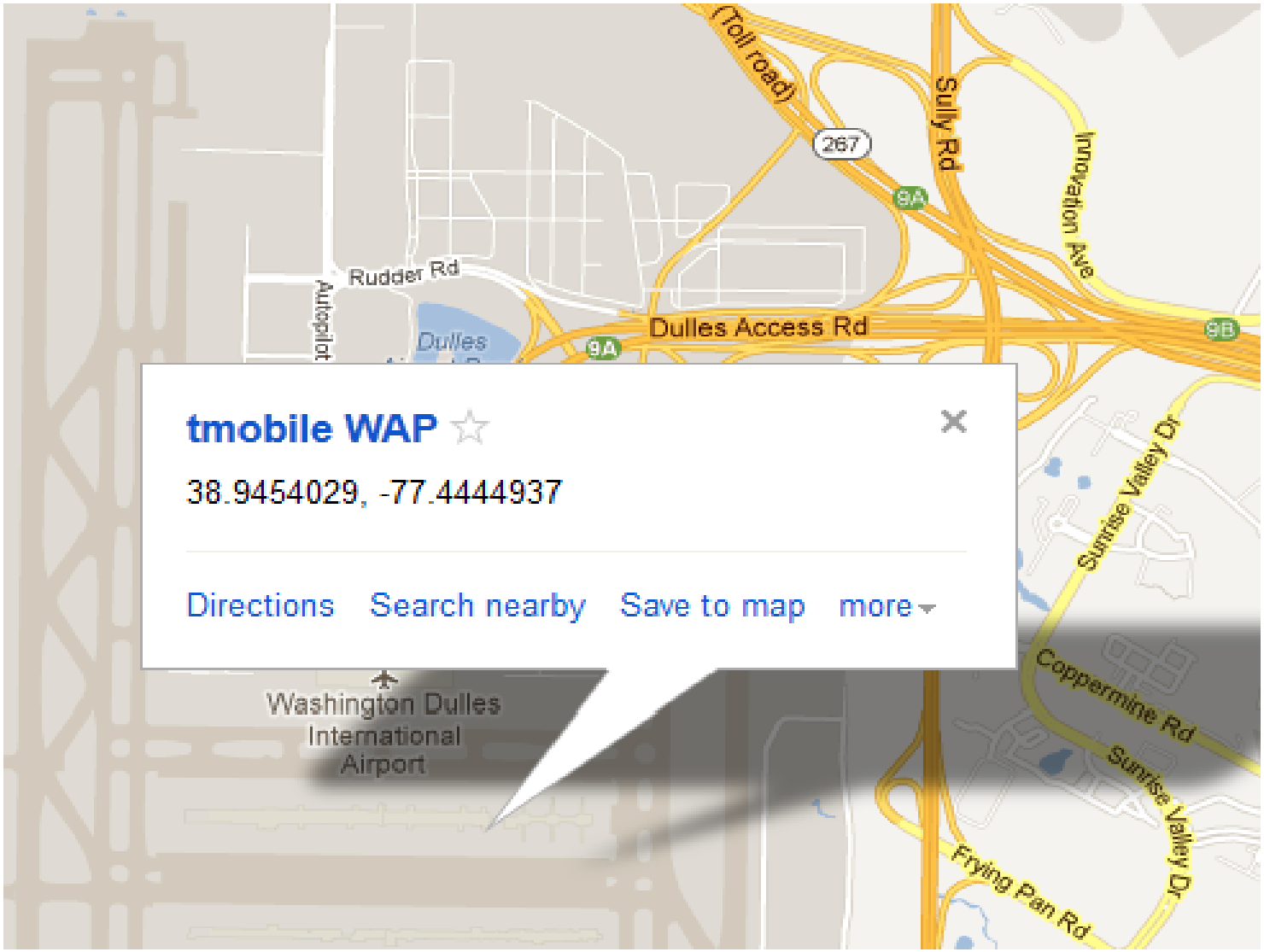


NTUSER.DAT from VSC…
Fri Jan 8 04:13:40 2010 Z
UEME_RUNPATH:C:\Program Files\Skype\Phone\Skype.exe (8)

Windows records the MAC address of WAPs to which the system has connected. Extract this information, and perform lookups to get lat./long., for plotting on Google Maps/Earth.

DATE LAST CONNECTED:	MON FEB 18 11:02:48 2008
DATE CREATED:	SAT FEB 16 12:02:15 2008
DEFAULT GATEWAY MAC:	00-0F-66-58-41-ED

Registry – Wi-Fi Geo-location



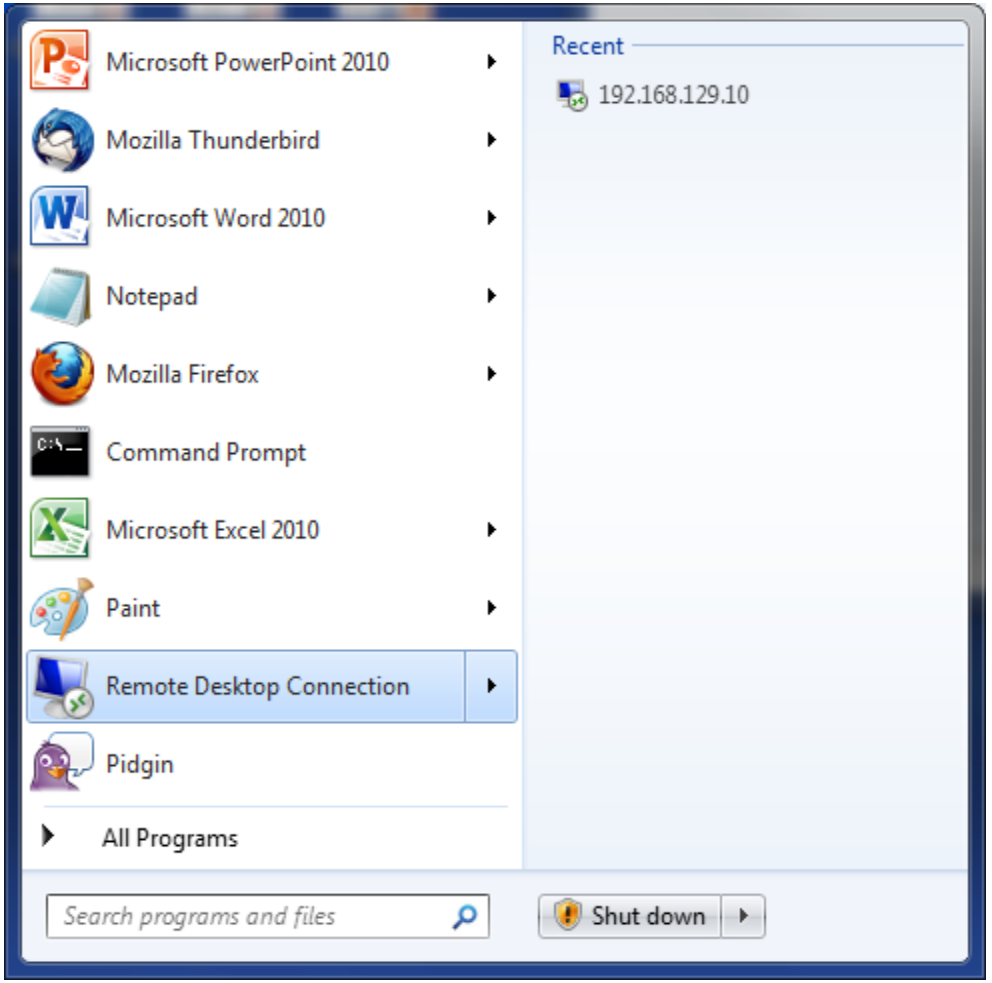
- More sources of time stamped data
  - "Usual suspects"
  - New files and/or formats that contain metadata (i.e., Jump Lists, etc.)
  - "New" Registry keys/values
  - "New" locations where data is stored, "new" structures to hold that data
  - Pertinent to timeline analysis

- More focus has been put toward understanding available data sources
  - Ex: Finding MAC addresses in the Registry
  - Finding additional time stamped data (again…timelines)
  - Finding additional sources of data that relate to various ***categories*** of activity (i.e., file accesses, program execution, etc.)

Windows tracks a great deal of user and system activity.

Many artifacts:

- …are created automatically by the operating system
- …persist beyond application removal/file deletion
- …previous versions of those artifacts can be found in VSCs



There is more data available to answer questions:

- Which application used/accessed this file?
  - Registry analysis (RecentDocs), Jump Lists, etc.
- File Accesses
  - Jump Lists, LNK files, Registry MRUs, log files, etc.
- USB device analysis
  - Registry (Software, System, NTUSER.DAT hives) + setupapi.dev.log + Windows Event Log (System)
- Who put those files there?
  - “Trojan Defense” -> Registry + Jump Lists + Prefetch + etc.
- Program Execution
- Did the user burn a CD/DVD?
  - Registry + Prefetch + ?

Summary – What to look forward to…

- Look at Windows as a “system”
  - Intentional activity in one part of the system can create unintentional artifacts in another part
- More data sources
  - More metadata embedded in some file formats
- What do we need?
  - More research
  - More community involvement
  - Share your questions… someone may have an answer

Windows 8

- New file system (ReFS)
- New Registry “stuff”
  - TypedURLsTime key
- IE: index.dat -> ESE database
  - Other browsers already use databases (SQLite)
- Access via Windows Live Account (also used to access MS’s “cloud”)
- Already some great work done by Kenneth Johnson and Amanda Thomson

Questions?

H. Carvey

harlanc@appliedsec.com

keydet89@yahoo.com

http://windowsir.blogspot.com