Terremark WorldWide

Harlan Carvey
Vice President, Secure Information Services

BEYOND AVAILABILITY

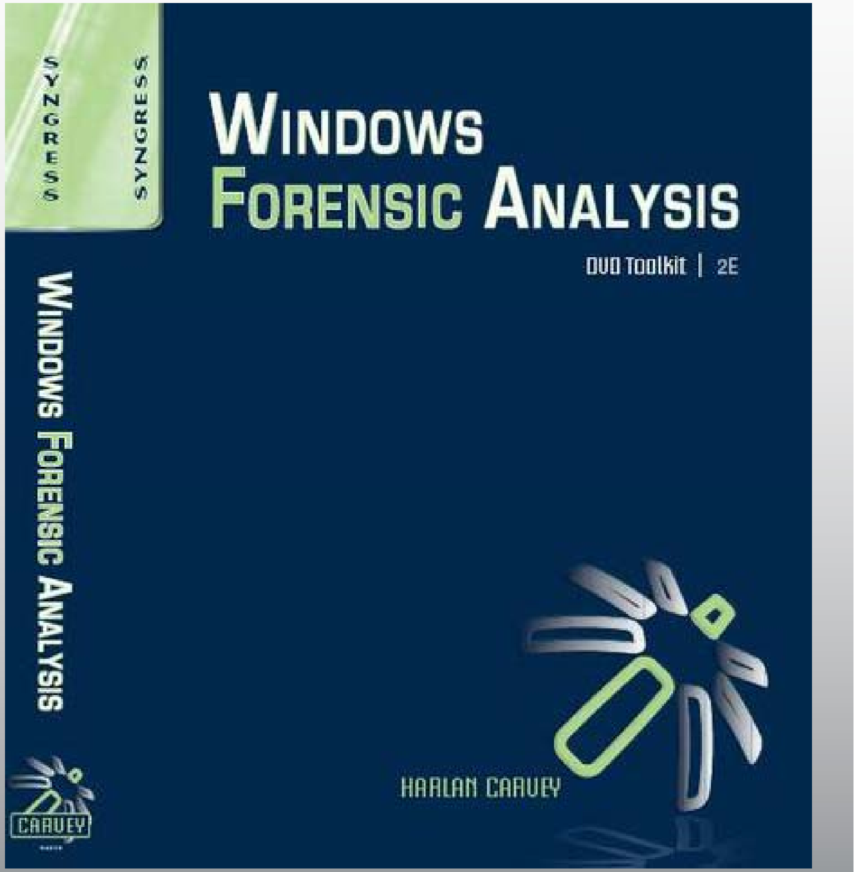
Using Free & Open-Source Tools To Create Timelines

TSK/Open Source Conference, 9 June 2010

Who am I?

- Forensicy guy for Terremark Worldwide (NASDAQ:TMRK), a leading global provider of IT infrastructure services delivered on the industry's most robust and advanced operations platform.

- Incident responder and forensic analyst, author of several ***open source*** tools (including *RegRipper*), books (*Windows Forensic Analysis*), articles (*Hakin9*), etc.



Creating Timelines

- Why would we do that?
- How are timelines useful?
- Why would we use open source & free tools?

Creating Timelines

- Increase confidence/context
- Can share timeline data without exposing sensitive data
- Optimize analysis
- Perform analysis in parallel, aid in scoping, etc.
- Provide a view of data that is not available anywhere else
- Use during IR (selective files) or image analysis

Creating Timelines

- Five Field Format
- ***Time*** – Normalized to GMT/UTC
- ***Source*** – What is the source of the data
- ***System/Host*** – Which system is this from?
- ***User***
- ***Description***
- Separator – Pipe, comma, whatever

```
Fri Jun 18 23:49:59 2004 Z
  FILE     System1   - MA.E C:/WINDOWS/Prefetch/RPCALL.EXE-394030D7.pf

Fri Jun 18 23:49:53 2004 Z
  FILE     System1   - MA.E C:/Documents and Settings/vmware/Local Settings/Temp
  FILE     System1   - MACE C:/WINDOWS/Prefetch/PING.EXE-31216D26.pf

Fri Jun 18 23:49:49 2004 Z
  PREF     System1   - PING.EXE-31216D26.pf last run (1)
  PREF     System1   - RPCALL.EXE-394030D7.pf last run (2)
  PREF     System1   - SMS.EXE-01DC4541.pf last run (2)
  FILE      System1   - ...E C:/Documents and Settings/vmware/NTUSER.DAT
  FILE      System1   - MACE C:/WINDOWS/Prefetch/SMS.EXE-01DC4541.pf
  FILE      System1   - ..C. C:/WINDOWS/Prefetch/RPCALL.EXE-394030D7.pf
  FILE      System1   - M..E C:/WINDOWS/system32/inetsrv
  FILE      System1   - .A.. C:/WINDOWS/system32/ping.exe
  REG       System1  vmware - UserAssist: UEME_RUNPATH:C:\System Volume
     Information\_restore{..}\RP2\snapshot\Repository\FS\sms.exe (1)
  REG      System1  vmware - HKCU\..\Run: RPC Drivers ->
     C:\WINDOWS\System32\inetsrv\rpcall.exe
```

Tools

- TSK tools (mmls, fls, blkls)
- Pasco – IE index.dat files
- Perl
- LOTS of customized programming may be required, given the sources (and not available in commercial tools)
- Output of open source and free tools == intermediate format

Data Sources

- Time-based data sources on Windows systems – there are a ***LOT*** of them!
- Depending upon your analysis goals, you may not need all of them.
- Using multiple sources provides context
- Using multiple data sources increases the relative confidence level of the timeline, as some sources are less mutable than others ($SIA vs. $FNA, Registry key LastWrite times, etc.)

Data Sources

- File system
  - Fls – Directly from image
  - Perl – FTK Imager directory listing
  - MFT/$FILE_NAME attribute
  - Dave Kovar’s analyzemft.py
- Prefetch files
- INFO2
- EVT/EVTX
  - Evt – Evtrpt.pl/Evtparse.pl
  - Andreas Schuster’s tools
  - LogParser + Perl
- Registry - RegRipper
- Windows shortcut/*.lnk files

Data Sources

- XP Restore Points/rp.log
- Scheduled Task – SchedLgu.txt, *.job files
- Mrt.log, AV logs
- IIS web server logs

- log2timeline (part of SIFT)

Time Formats

- Need to address all of these, as appropriate
- String (“1/6/2009”)
- 32-bit *nix epoch time
- 64-bit FILETIME
- 128-bit SYSTEMTIME

Factors that influence timelines…

- Temporal proximity
- Understanding what you’re looking for
- Understanding the system
- There is such a thing as too much…
- JUST DO IT!

Questions?

Harlan Carvey

VP, SIS, Terremark

Hcarvey[at]terremark.com