Windows “Artifacts”

Comp 199

Admin

- Current Events in information security
  - See web
- Questions?

Windows

- Why windows first?
  - Its still everywhere
    - Perhaps 90% of desktop?
    - Gartner: 35% of all user computing – see web
    - Ubiquitous in workplace.
    - As likely as any other system to have to be examined
  - Its sitting in most of the labs on campus

Deleted Data

- As you know
  - Delete doesn't remove data
  - Just 'loses' where it is on the disk
  - Marks it available to overwrite.
  - Recoverable through 'file carving'
    - Manually examine bits on sectors of hard drive
      - Look for file 'header' data
      - Impractical in large drives
    - Have a tool do this for us
      - The way mostly done today
      - Tool range from free but obscure to ~$1000 (small business grade to thousands (enterprise grade)

Low Power Modes

- Sleep vs Hibernation
  - Both power conservation modes
- Sleep
  - Conserve energy while able to get everything back ASAP
  - Small amount of electricity flowing through RAM
    - Volatile/Working memory – nothing really saved
- Hibernation
  - Shuts down all the power, but saves state of computer (open programs, files etc)
  - Writes a file called hiberfil.sys: on drive - recoverable

Windows Registry

- The repository for configuration information
  - Old days: configuration files (.cfg)
  - Nearly all user config and preferences stored in registry now
    - What does that tell us?
    -

Windows Registry

- The repository for configuration information
  - Old days: configuration files (.cfg)
  - Nearly all user config and preferences stored in registry now
    - What does that tell us?
    - At least: where the user likes to store stuff
    - What programs are used/installed.
    - Recent searches using IE (not firefox)
  - Also includes lists of usb devices and hardware ids
    - Anything connected to the computer recently.
    - How does this help?

Print Spooling

- Printing description
  - Enhanced metadata
  - Spl (spool file)
  -

Recycle Bin

- Stuff that's sent to the trash can
  - Lots of users never bother emptying it
  - Often plenty to look through for such users.
- Bypass the recycle bin with <shift><delete>
- Registry
  - NukeOnDelete
  - Look for this reg key to see if user is always deleting.

Metadata

- We spent a class on this last week
  - But to review:
    - Data about who worked on a file hidden in the file itself.
  - Often people/corporations want to remove it:
    - legitimate
    - Before making documents public
      - Don't want to have people pointing fingers at one employee who typed up the policy/finding etc.
    - Lots of tools to scrub/mess with metadata these days.

Thumbnail Cache

- Windows makes small versions of your images
  - thumbs.db (older versions)
  - thumbcache.db (newer versions)
  - Retains thumbnails after originals deleted.
  - What sorts of stuff can this help with?

Most Recently Used

- You've all seen how windows tries to help you out
  - Look at menu
  - Folder full of shortcuts
  - Even if original is gone
  -

Backup data

- Restore points and shadow copies
  - Much like mac OS time machine
  - Can restore a system to a previous state (restore points) from data stored in shadow copies
  - http://www.sevenforums.com/tutorials/166102-shad
  -
  - http://encase-forensic-blog.guidancesoftware.com/
  -

Reading