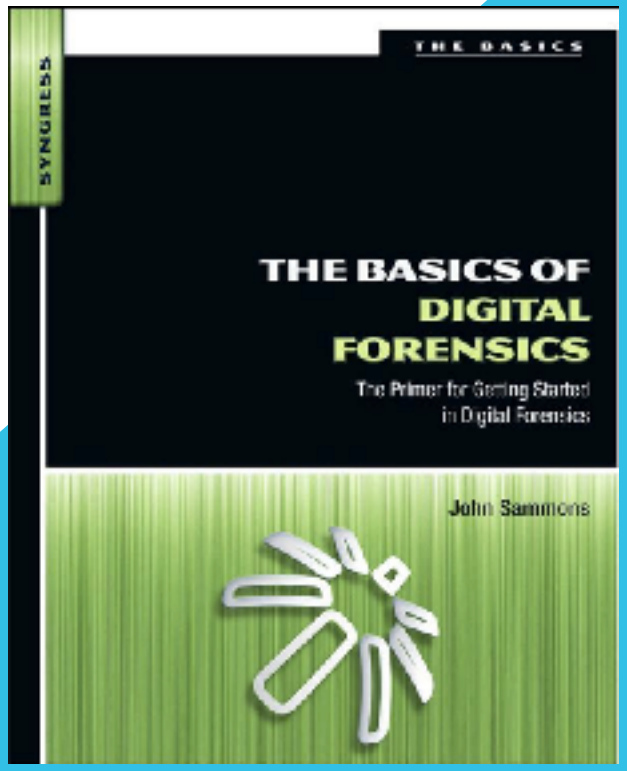


5. WINDOWS SYSTEM ARTIFACTS PART 2

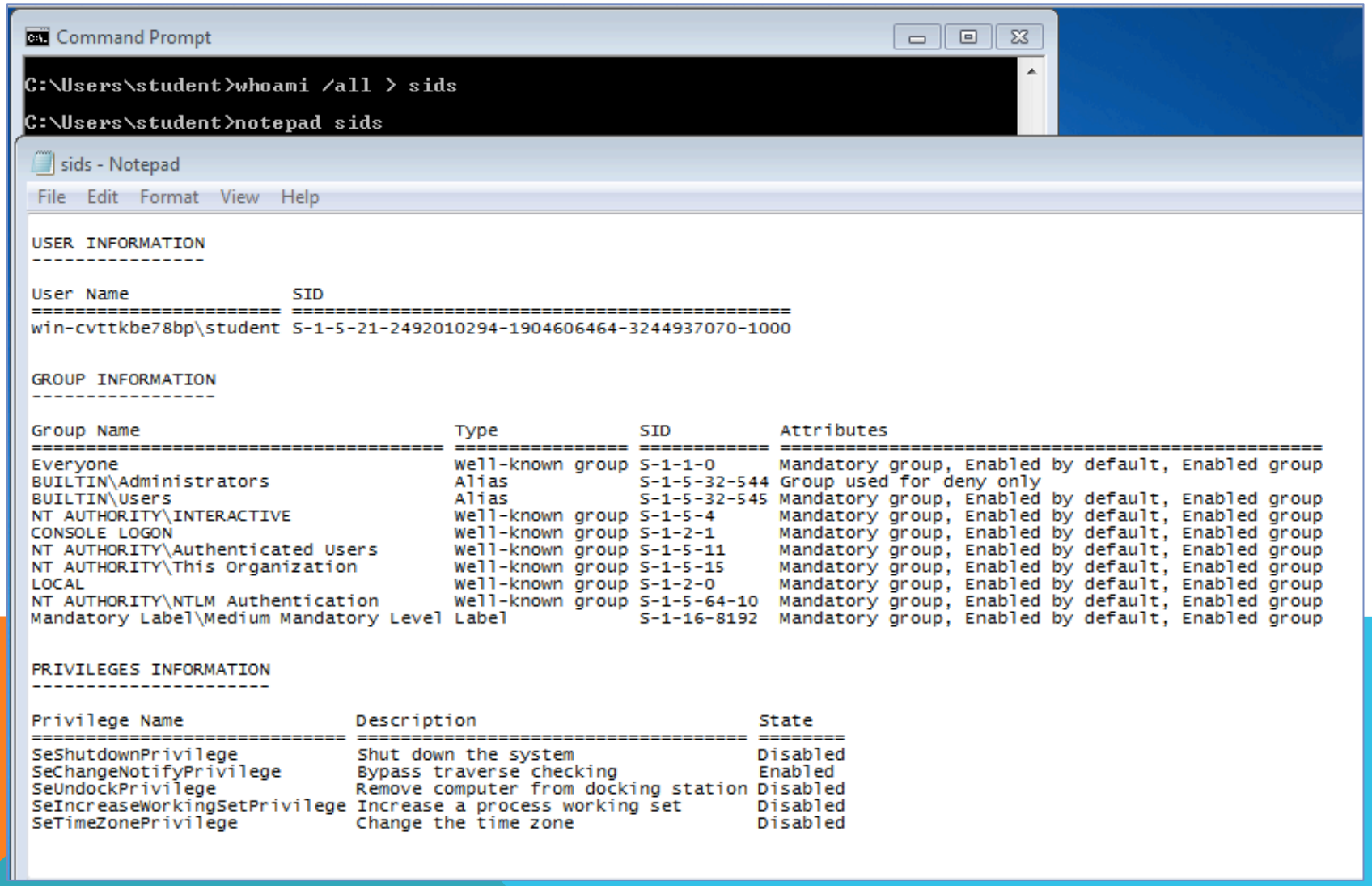
TOPIK

- Attribution
- Recycle Bin
- Metadata
- Thumbnail Images
- Most Recently Used Lists
- Restore Points dan Shadow Copies
- Prefetch dan Link Files

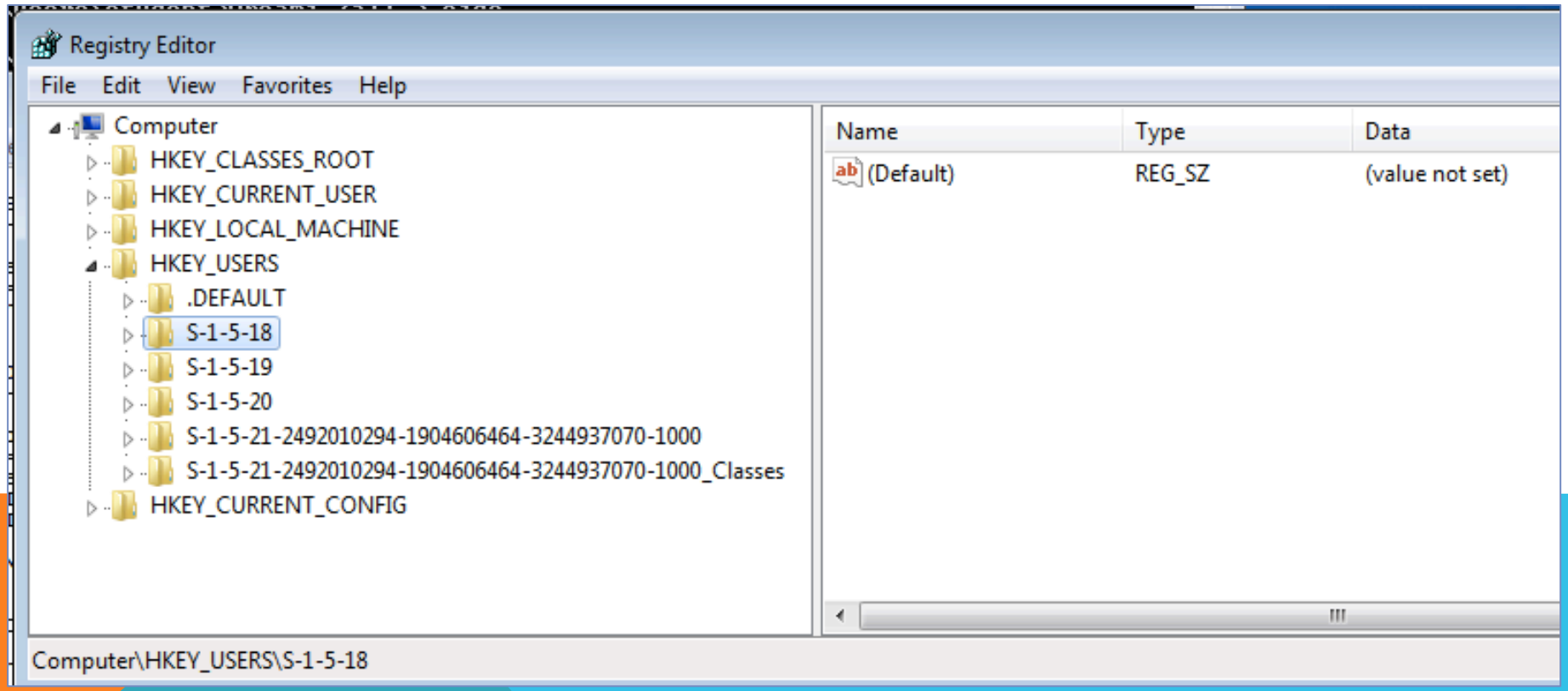
ATTRIBUTION (KAITAN)

- Barang bukti untuk suatu kejadian mudah dicari
  - Kata kunci pencarian
  - gambar
  - Halaman Web yang dilihat
- Mengaitkan lebih sulit
  - Siapa yang menggunakan komputer ketika tindakan dilakukan?
- Satu komputer memiliki beberapa accounts
- Win XP bisa dijalankan oleh Administrator dan Guest
  - Keduanya di-disabled secara default di Windows 7

SID (SECURITY IDENTIFIER)



SIDS DI REGISTRY



WELL-KNOWN SIDS

Link Ch 5o: Well-known security identifiers in Windows operating systems

- SID: S-1-5-18
  Name: Local System
  Description: A service account that is used by the operating system.
- SID: S-1-5-19
  Name: NT Authority
  Description: Local Service
- SID: S-1-5-20
  Name: NT Authority
  Description: Network Service
- SID: S-1-5-21*domain*-500
  Name: Administrator
  Description: A user account for the system administrator. By default, it is the only over the system.

EKSTERNAL DRIVES

- USBSTOR memperlihatkan perangkat USB yang digandeng ke komputer
- Membantu dalam menghubungkan bukti yang ditemukan pada perangkat removable

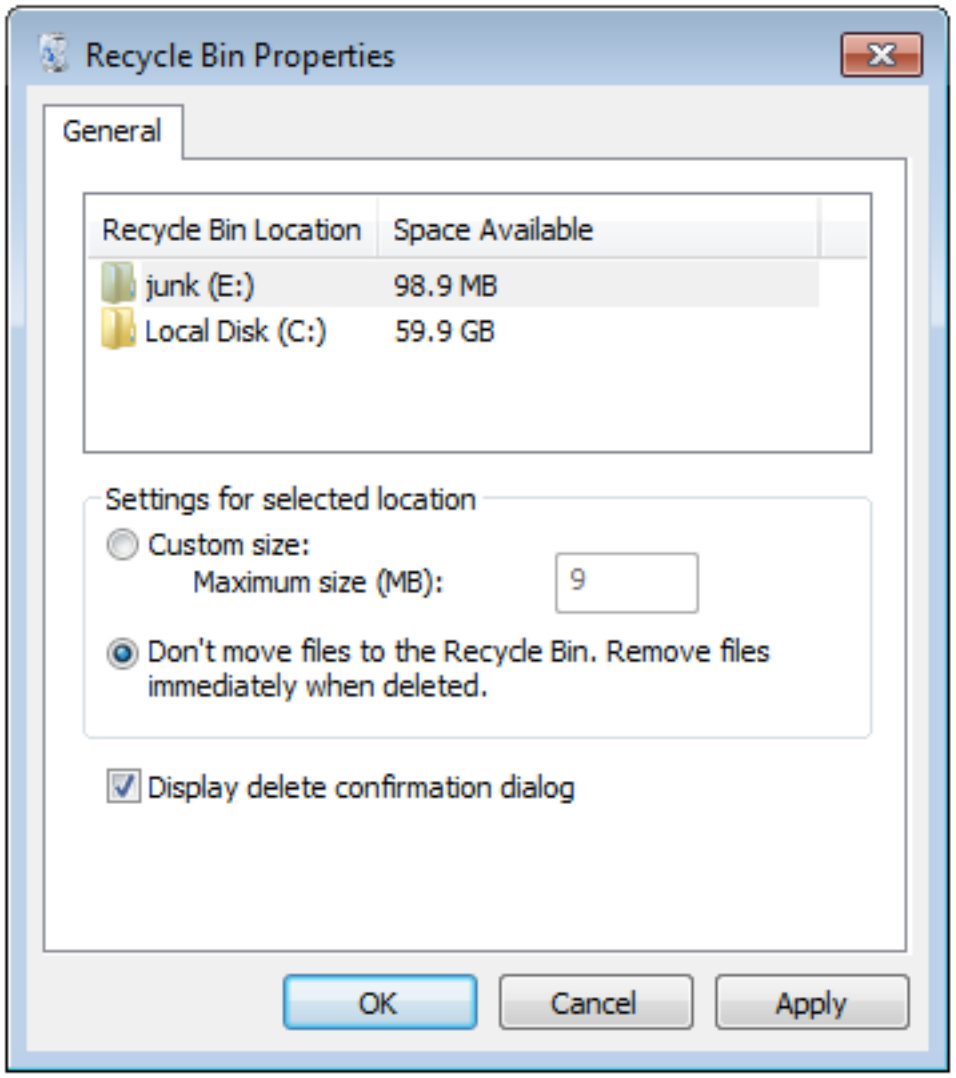
PRINT SPOOLING

- Ketika dokumen dicetak, ada dua files yang dibuat
  - Enhanced Meta File (EMF) yang berisikan image dari dokumen yang akan dicetak
  - Spool File yang berisi informasi mengenai print job
- Biasanya di deleted setelah selesai dicetak, tapi terkadang masih ada pada beberapa systems

RECYCLE BIN

OPERASI RECYCLE BIN

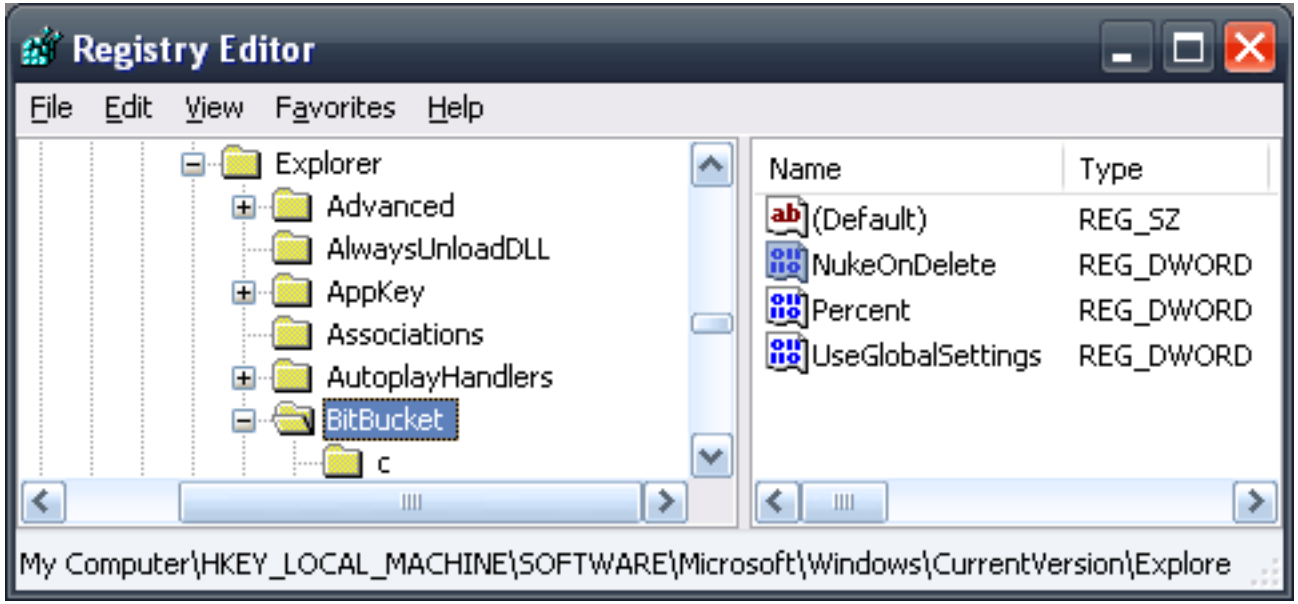
- Tidak semua yang didelete masuk ke Recycle Bin
- Shift+Delete akan mem-bypass Recycle Bin, akan menjalankan "Delete" dari command prompt
- user bisa mendisable Recycle bin pada Recycle Bin Properties



NUKEONDELETE REGISTRY KEY

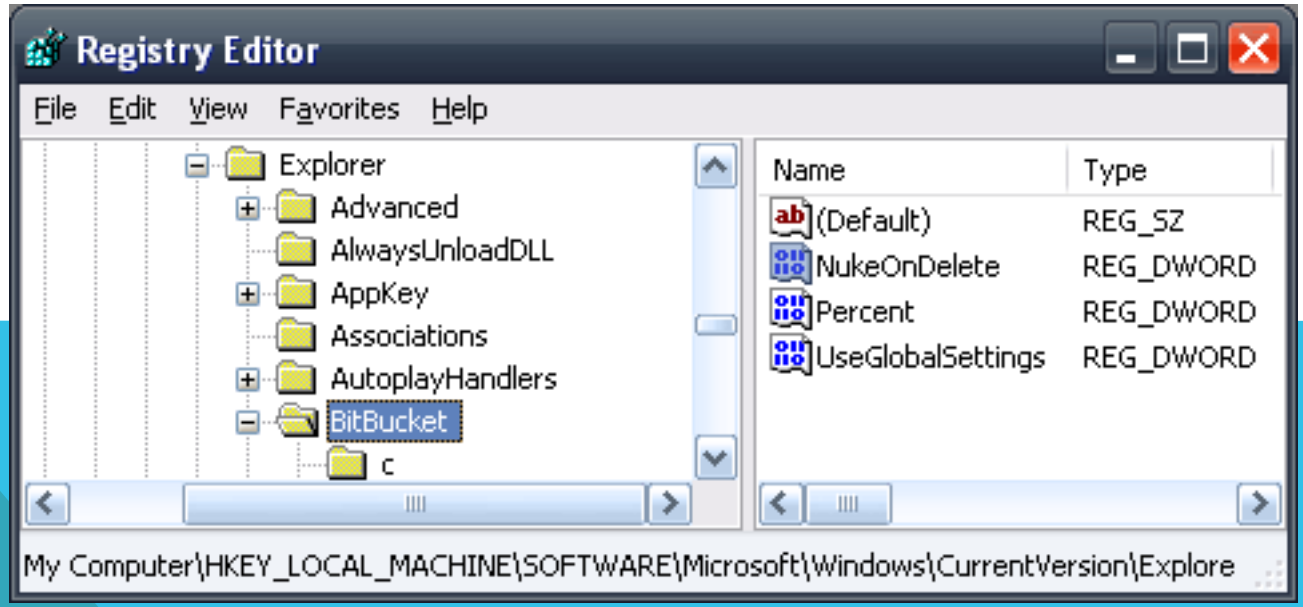
Win XP

(Link
CH 5p: Registry Hack: Enable Or Disable The Recycle Bin At Will!)



Win 7

(Link
Ch 5q: Windows Forensic Analysis DVD Toolkit - Harlan Carvey - Google Books)



METADATA

METADATA

Data tentang data

Metadata File system

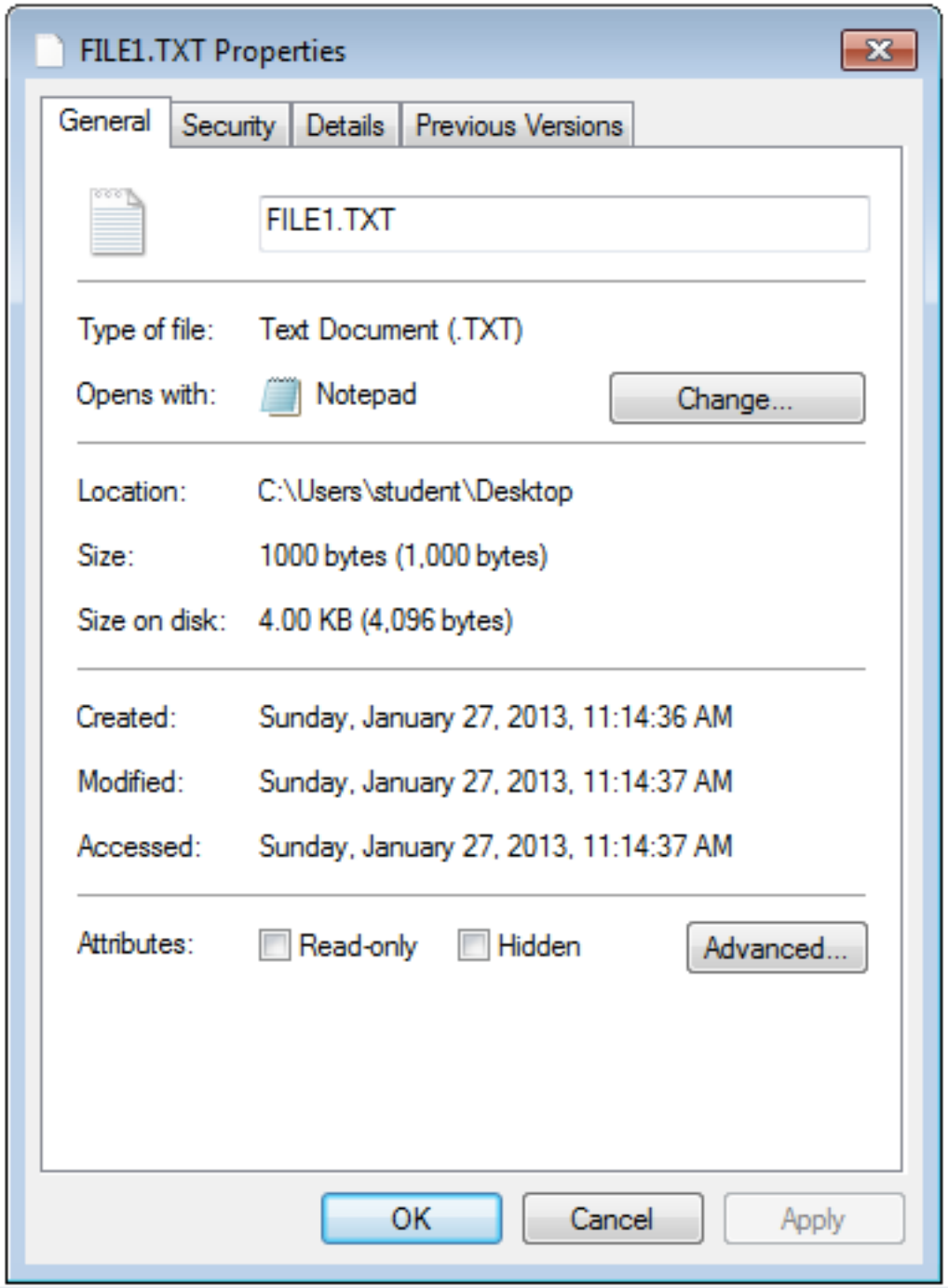
- Timestamps (Created, Modified, Accessed)
- Permissions, owner

metadata Aplikasi

- Author's name
- GPS koordinat
- Nama pemilik Software

TIMESTAMPS

- WARNING: Semua tergantung pada jam system, yang bisa di reset
- Created
- Modified
- Accessed
  - Meskipun jika file tidak dibuka, tapi hanya discan dengan antivirus



MACR TIMES

Sleuthkit memperlihatkan empat timestamps

- Link Ch 5r: The Sleuth Kit and macr timestamps

m – modified (metadata modified about the file)

a – accessed (file itself has been accessed)

c – changed (content of the file has been changed)

b – birth (file created)

PRINSIP TIMESTAMP

- Harus hati-hati
- Lakukan percobaan pada sistem serupa untuk memverifikasi kesimpulan
- Gunakan beberapa alat
- Waspadai perubahan jam sistem

DEMO: JOHN MCAFEE'S PHOTO

regex.info/exif.cgi?dummy=on&imgurl=http%...

[CLEAR IMAGE]

From Web
Image URL:
View Image At Url
From File

Jeffrey's Exif Viewer
(help)

Drag this button to your button bar, then while on a page displaying an image, just click the button in the bar to view the image's Exif data
Exif

You also might be interested in the Chrome extension someone made to interface to my online Exif viewer

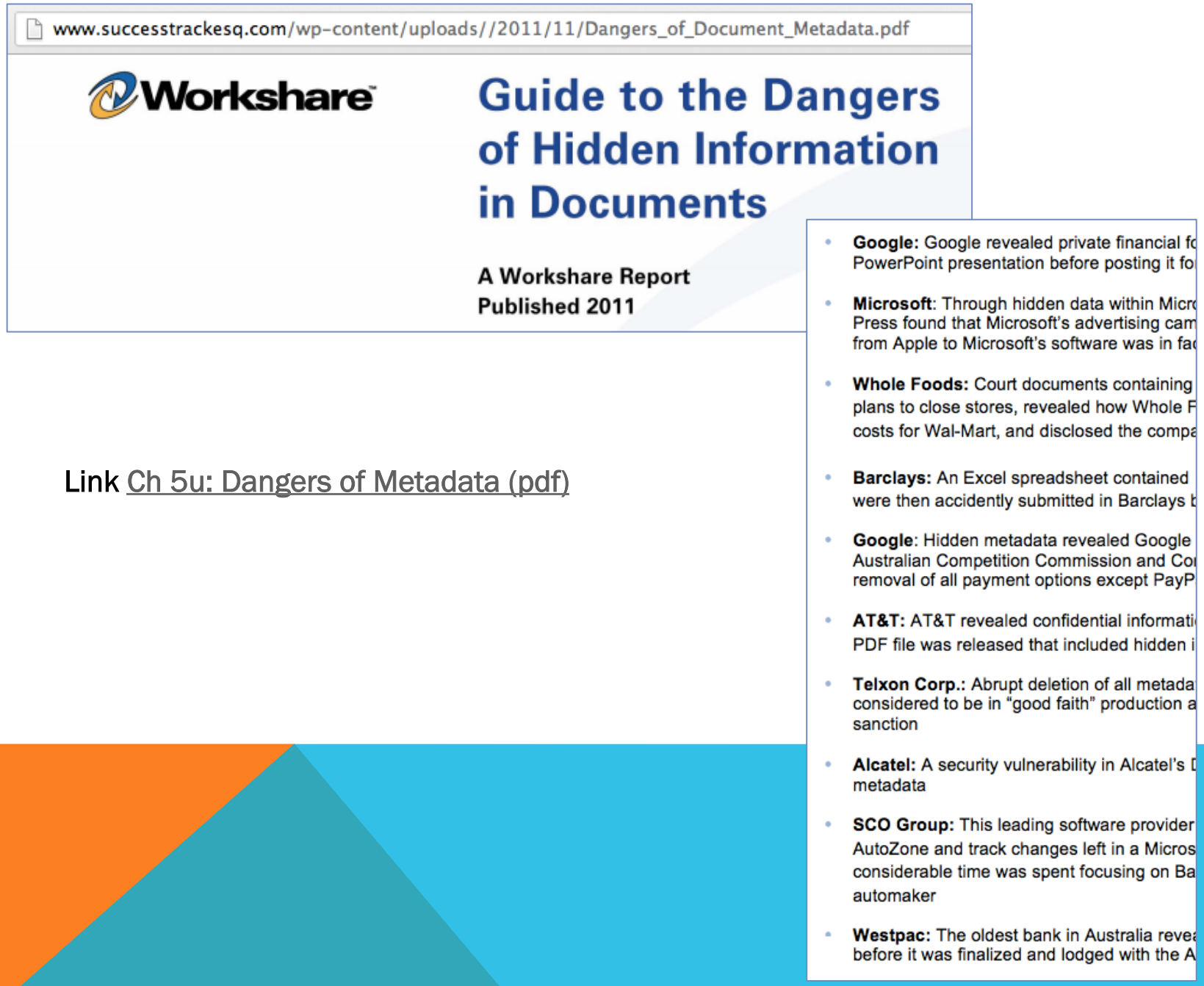
Some of my other stuff
· My Blog · "Camera Stuff" · "Photo Tech"
· Desktop Backgrounds · Pretty Photos

Basic Image Information

Camera:	Apple iPhone 4S
Lens:	4.3 mm
Exposure:	Auto exposure, Program AE, 1/20 sec, f/2.4, ISO 125
Flash:	Off, Did not fire
Date:	**December 3, 2012** 12:26:00PM (timezone not specified) (3 months, 23 hours, 7 minutes, 36 seconds ago, assuming image timezone of 6 hours behind GMT)
Location:	Latitude/longitude: **15°** 39' 29.4" North, **88°** 59' 31.8" West (15.658167, -88.992167) Map via embedded coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (also see the Google Maps pane below) Altitude: 7.152159468 m Timezone guess from earthtools.org: 6 hours behind GMT

Exif Viewer

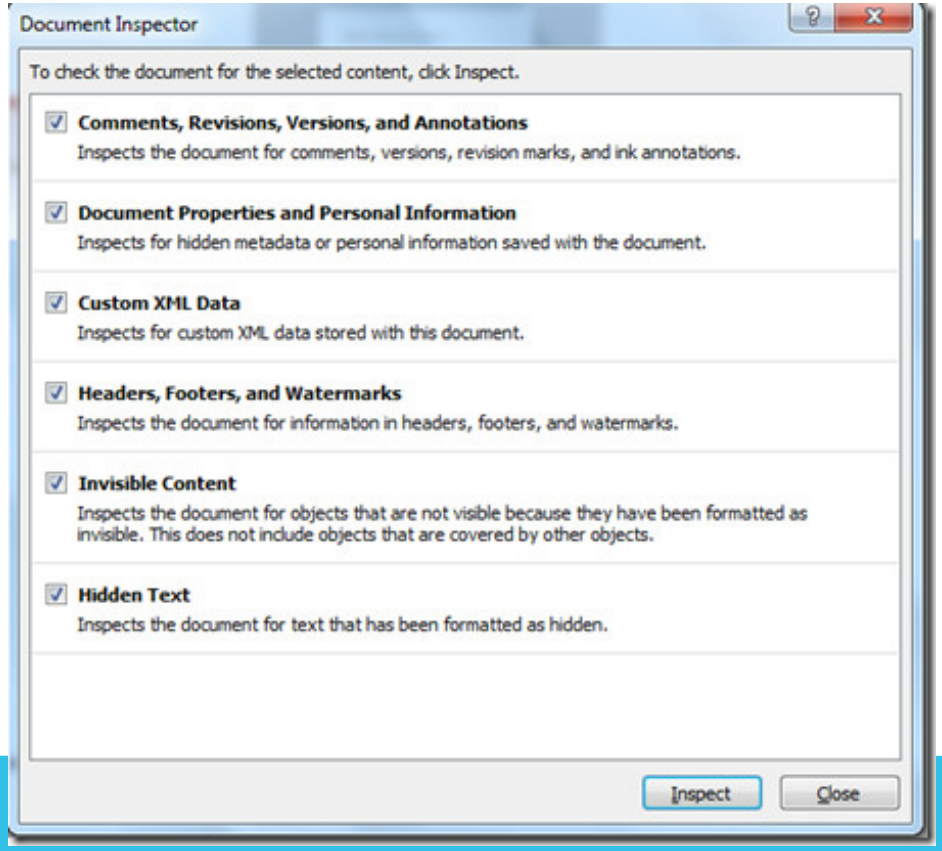
- Link Ch 5t: Jeffrey's Exif viewer



Link Ch 5u: Dangers of Metadata (pdf)

REMOVING METADATA

- Microsoft Office Document Inspector
- Link Ch 5v: Microsoft Office 2010 Document Inspector
- Tools Iain
- Link Ch 5w: Metadata removal tool - Wikipedia



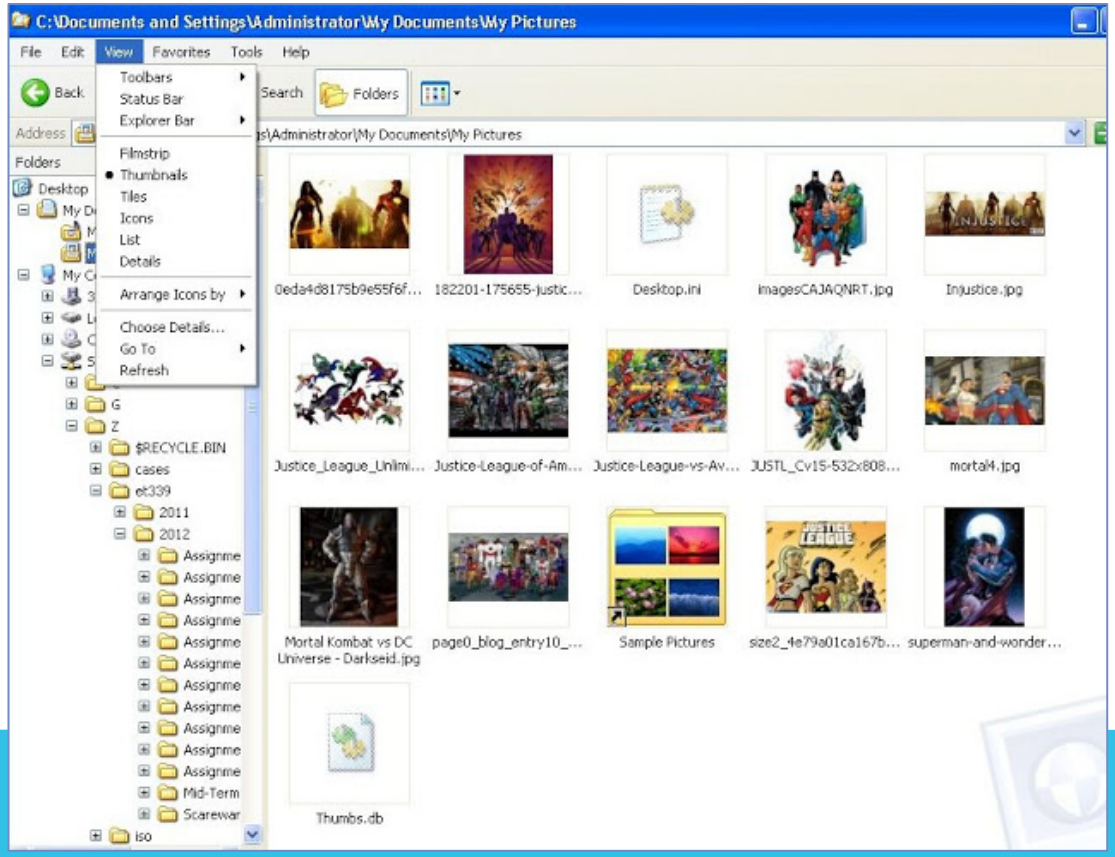
THUMBNAIL CACHE

WINDOWS XP THUMBNAILS

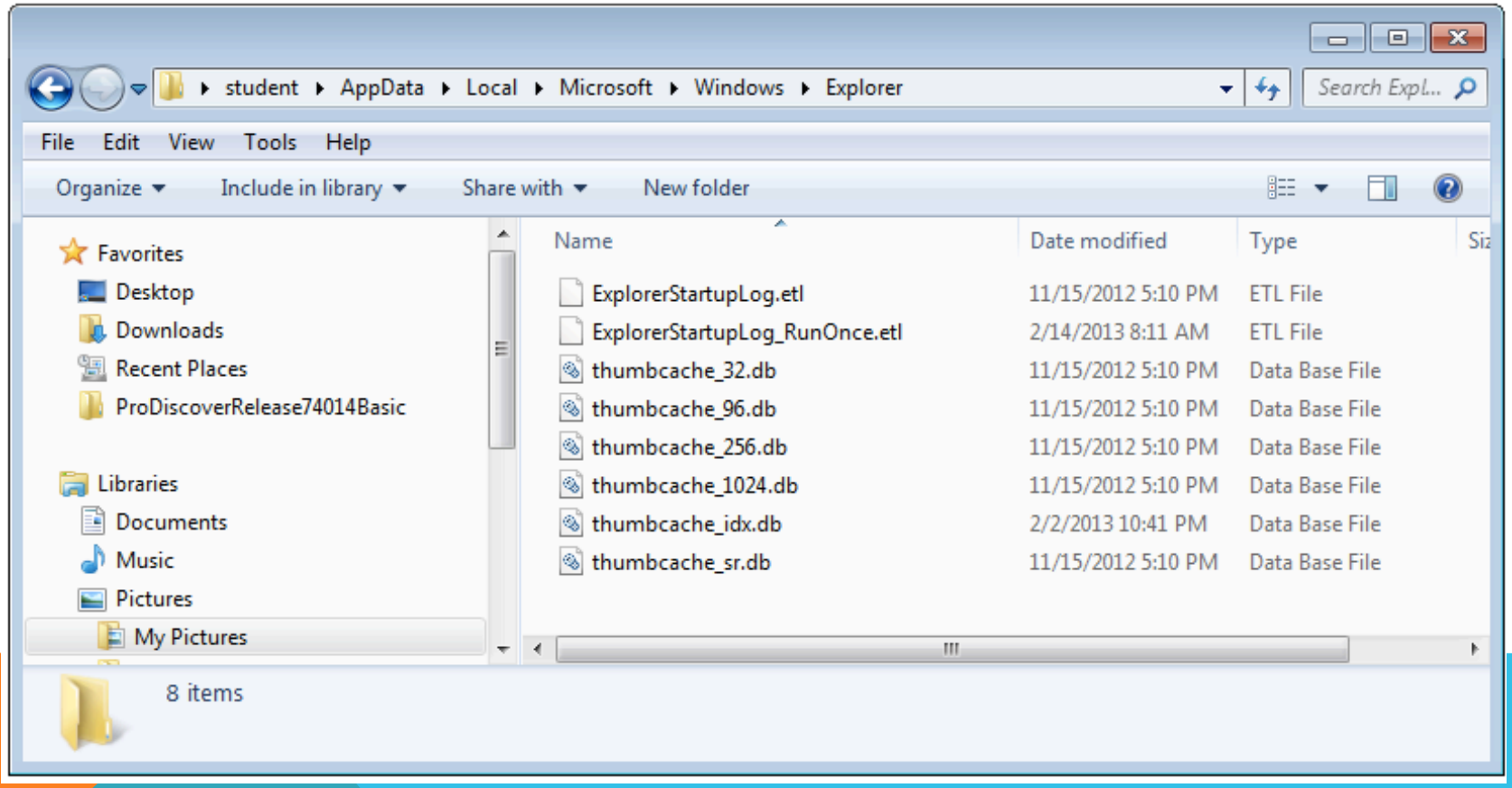
Thumbs.db

- File tersembunyi di folder yang sama dalam bentuk gambar

- Image dari link Ch 5x: ESCForensics: Analyzing Thumbcache



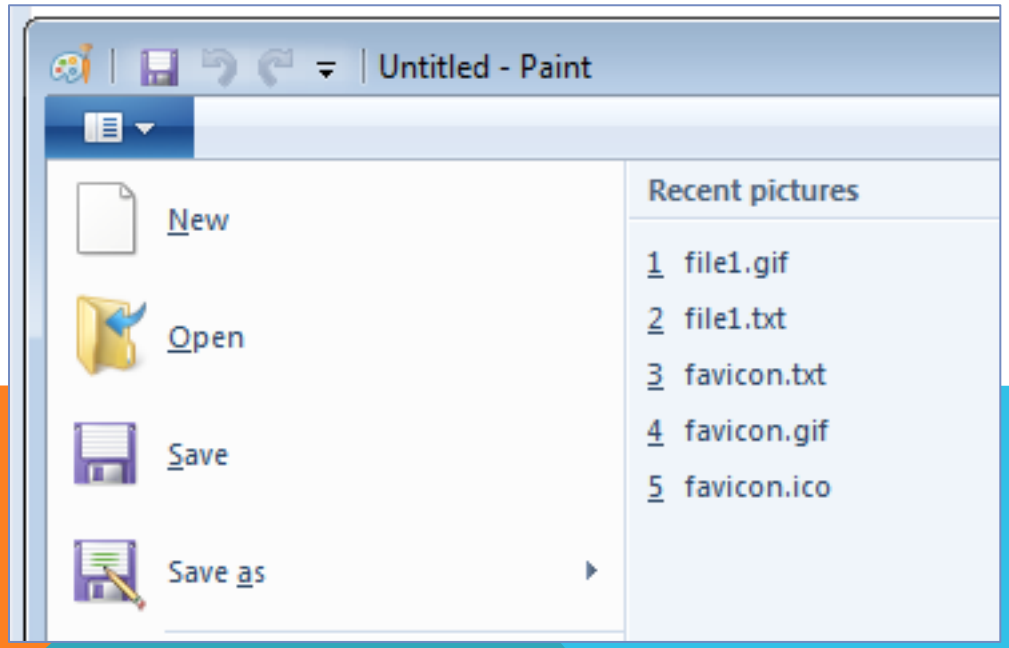
WINDOWS 7 THUMBNAILS

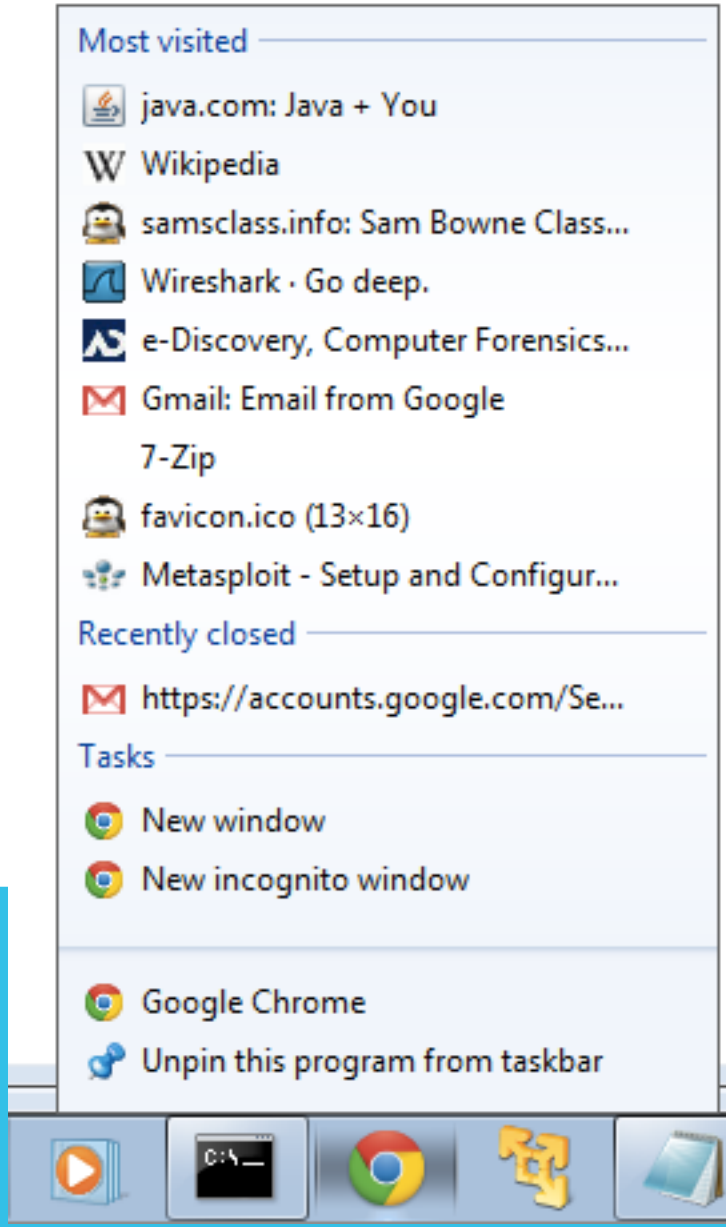


To view these, see tool at link Ch 5x

MOST RECENTLY USED

- Klik kanan Tombol taskbar pada Windows 7
- Klik ikon File Dalam paint
- Banyak lagi, di tempat-tempat lain

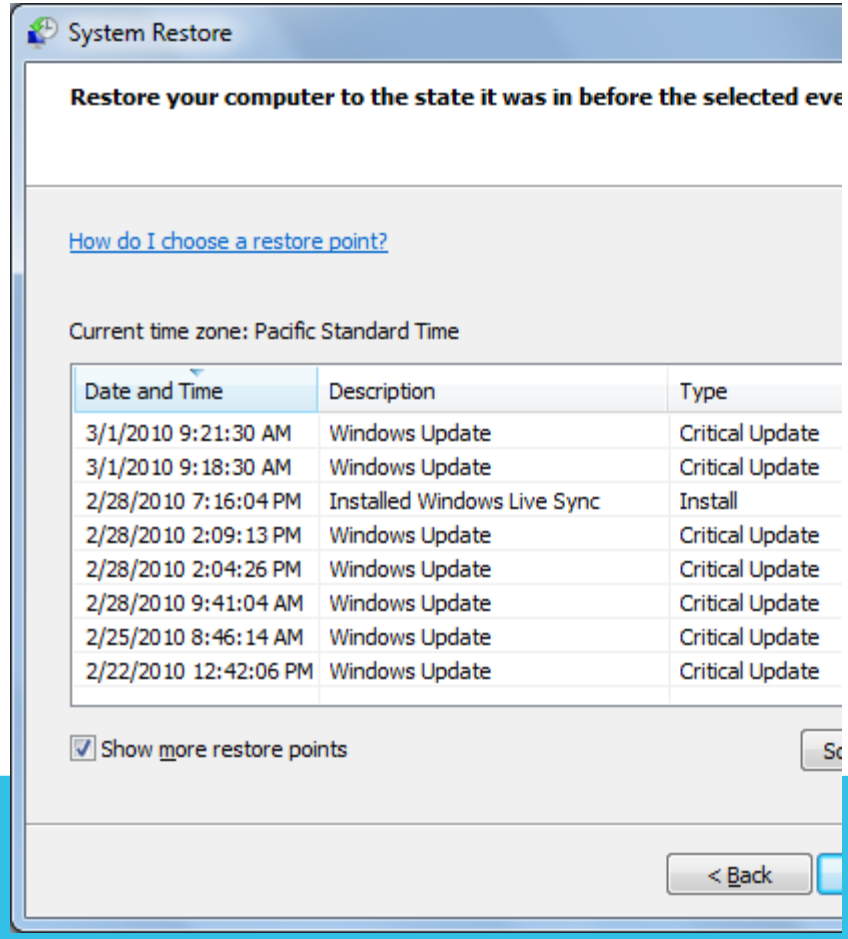




SYSTEM RESTORE

RESTORE POINTS

- Windows 7 membuat restore point setiap 7 hari secara default
  - XP dan Vista melakukannya setiap hari
- Restore point dibuat oleh layanan Shadow Copy, yang dapat menyalin file bahkan saat file sedang digunakan

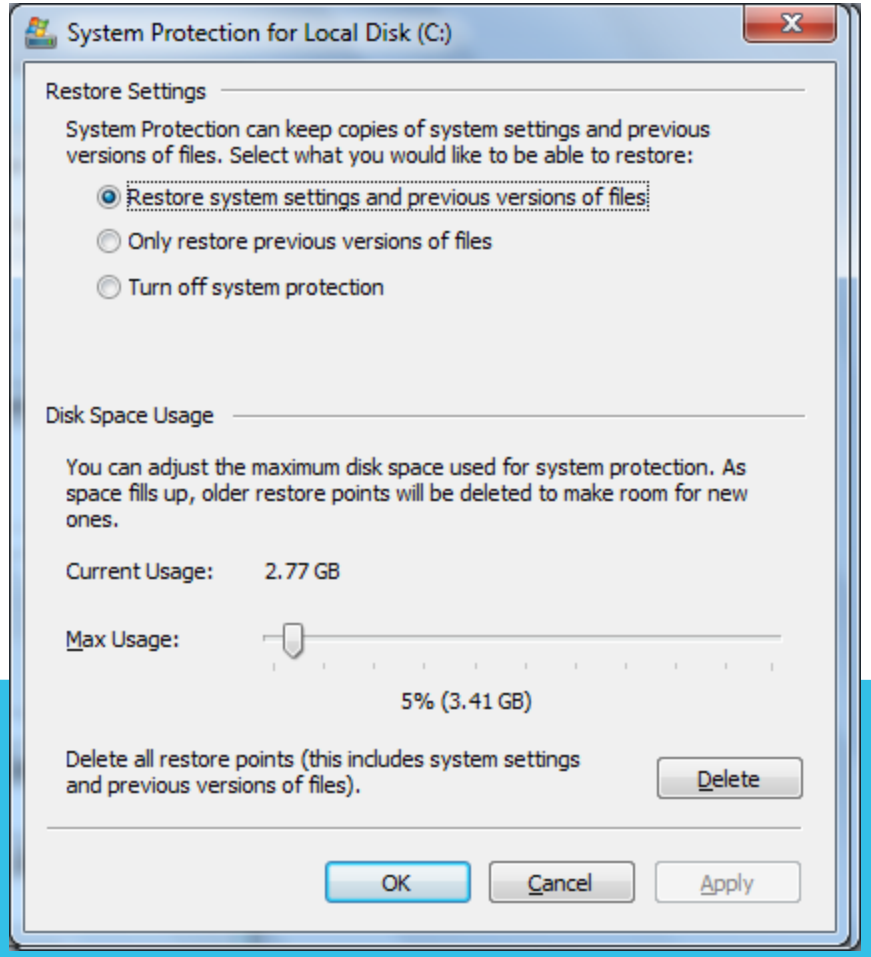


KAPAN RESTORE POINT DIBUAT

- Saat Sebuah aplikasi diinstal dengan Vista kompatibel atau Win 7 installer
- Saat Windows Update
- Saat System Restore dilakukan
  - Restore Point dibuat terlebih dahulu sehingga System Restore bisa dikembalikan
- Windows Backup
  - Restore Point dibuat sebagai bagian dari proses backup

RESTORE SETTINGS

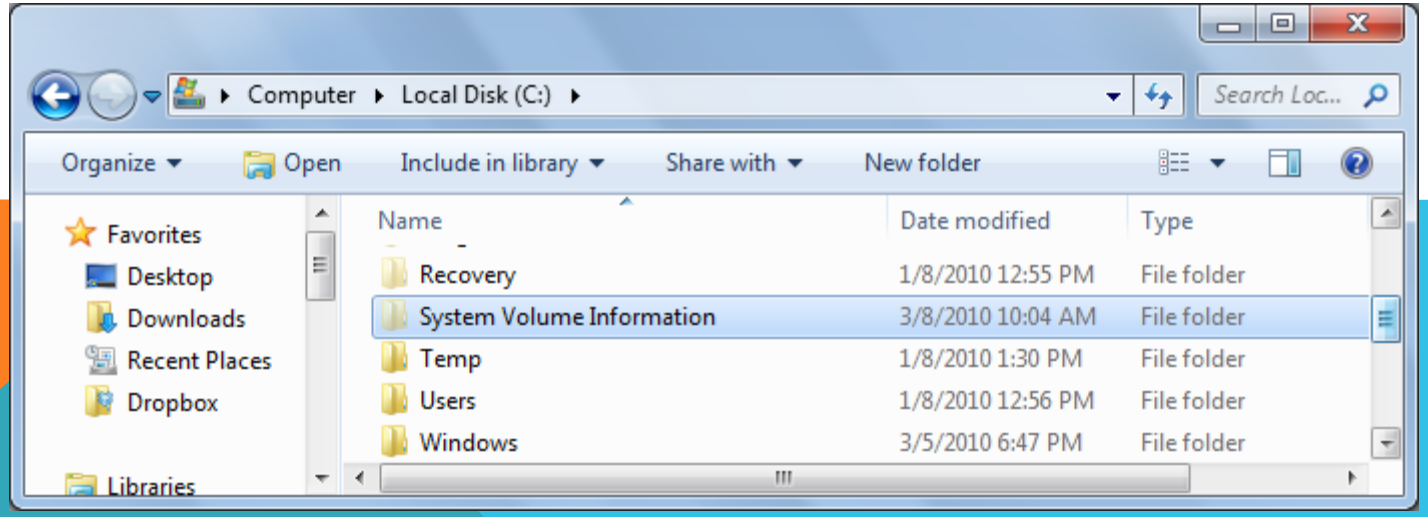
- Klik Configure
- Pilih apakah akan memonitor sistem settings atau hanya file
- "System Settings" mencakup Registry dan banyak jenis file sistem lainnya



SYSTEM RESTORE FILES

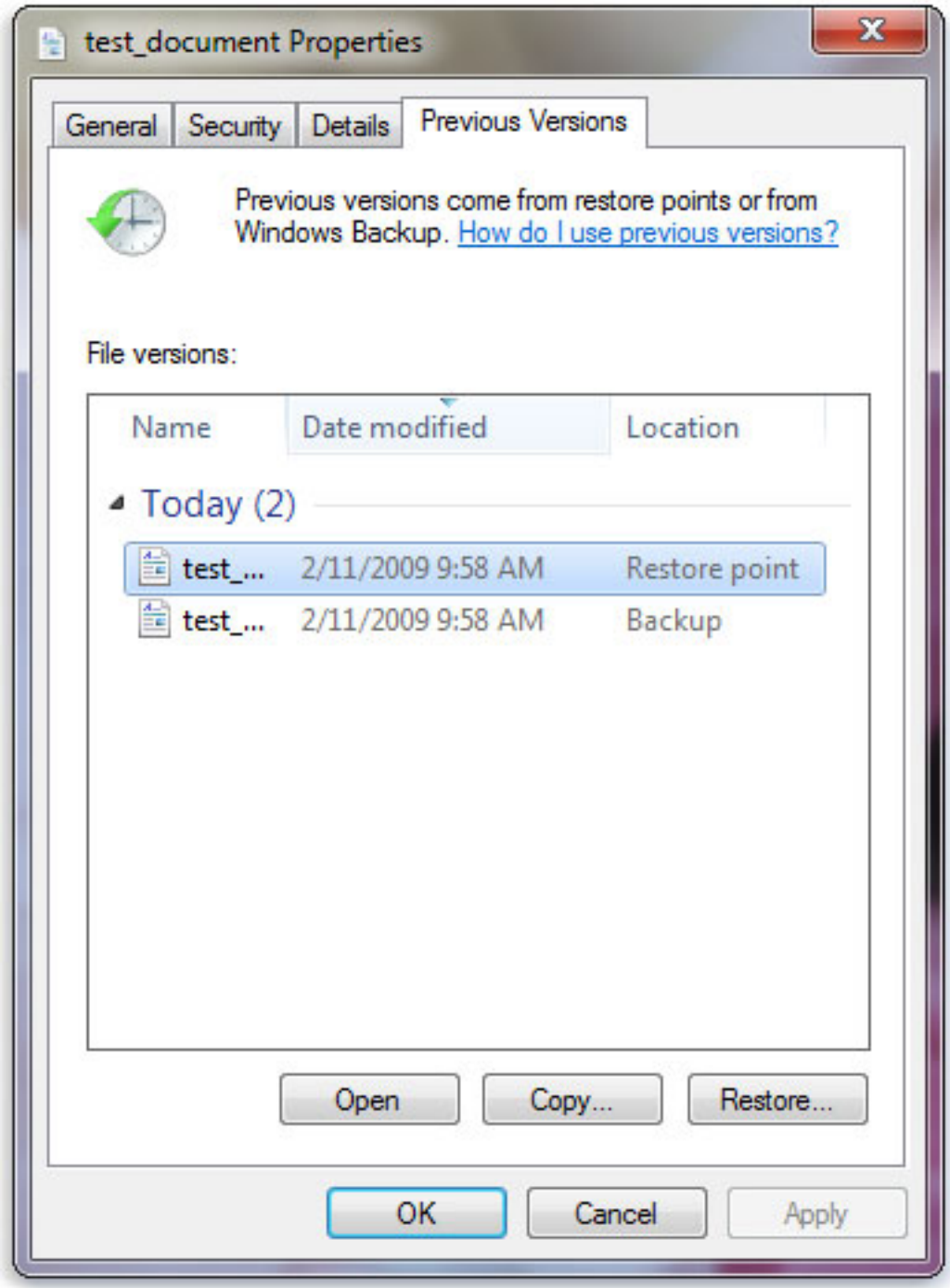
Letaknya di C:\System Volume Information

- Anda tidak dapat membuka folder ini, atau bahkan mengambil kepemilikan folder
- folder hanya ditujukan untuk System access



PREVIOUS VERSIONS

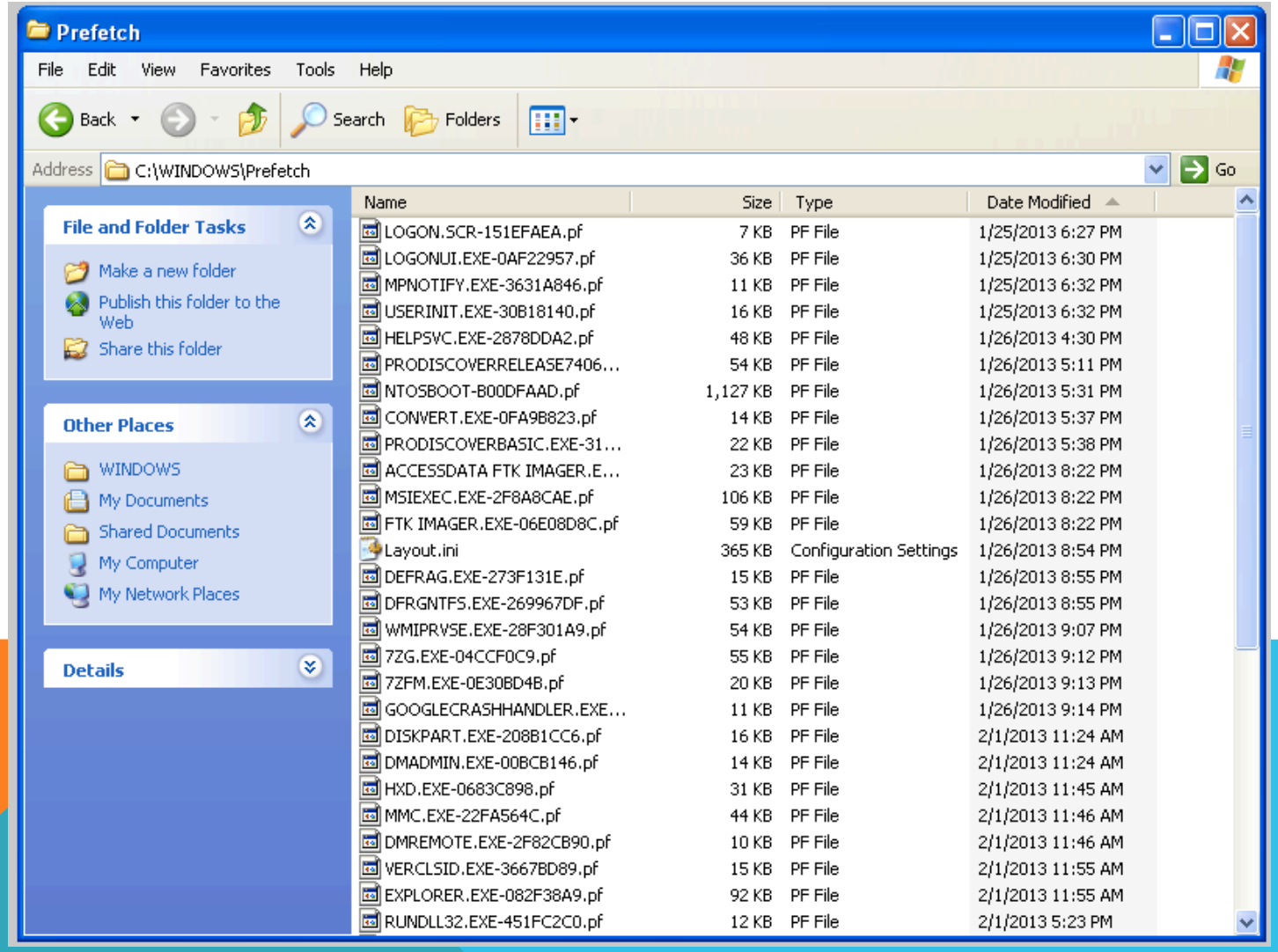
gambar from microsoft.com



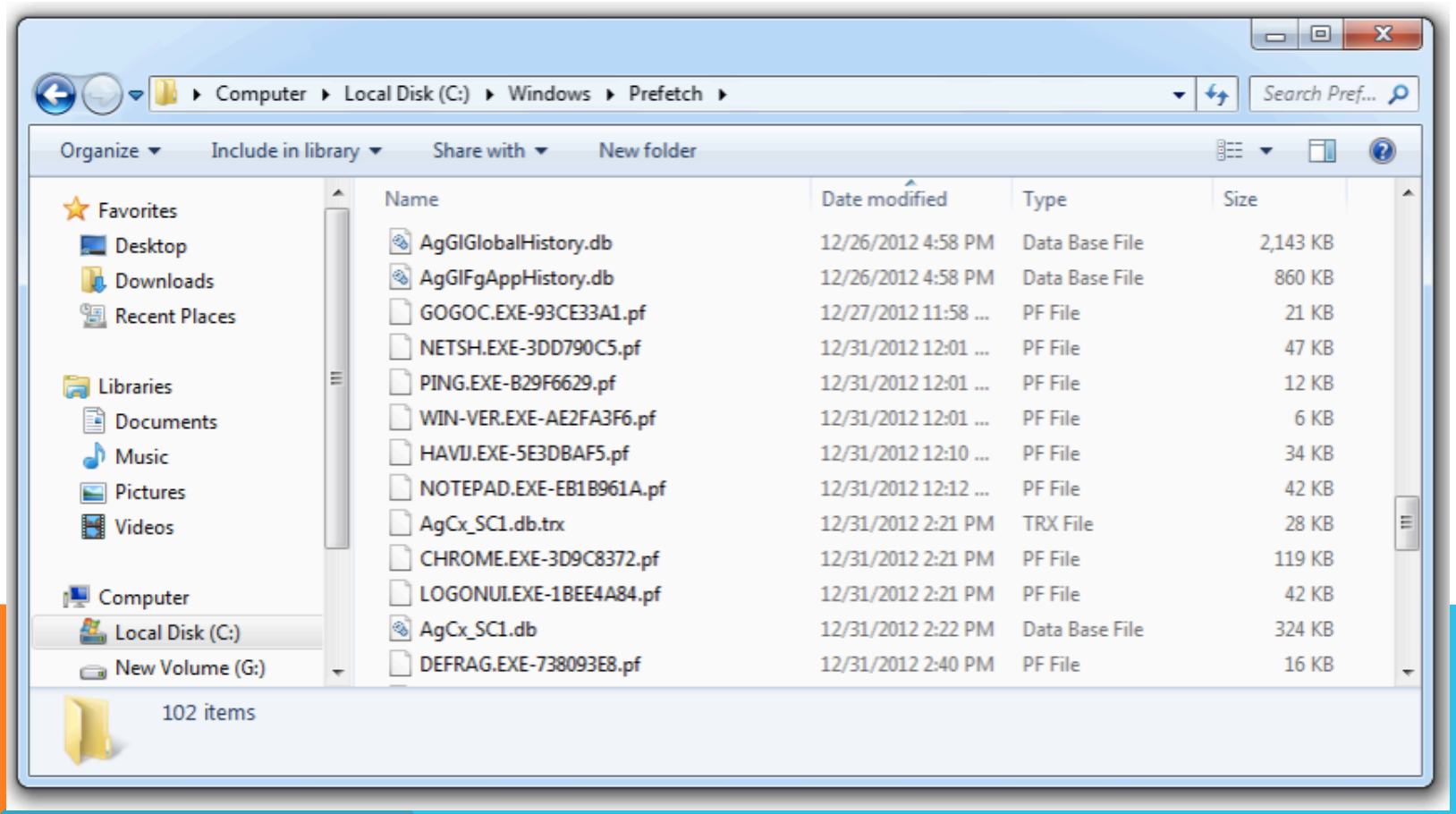
PREFETCH

- Untuk membuat komputer Windows lebih cepat
- Shortcuts untuk program yang sering dibuka disimpan dalam folder Prefetch
- Gunakan Viewers Prefetch untuk membantu membaca file
- Formatnya berbeda di Win XP dan Win 7/Vista
  - Links Ch 5y: Prefetch Parser
    Ch 5z: What is the prefetch folder?

PREFETCH DI WIN XP



PREFETCH DI WIN 7



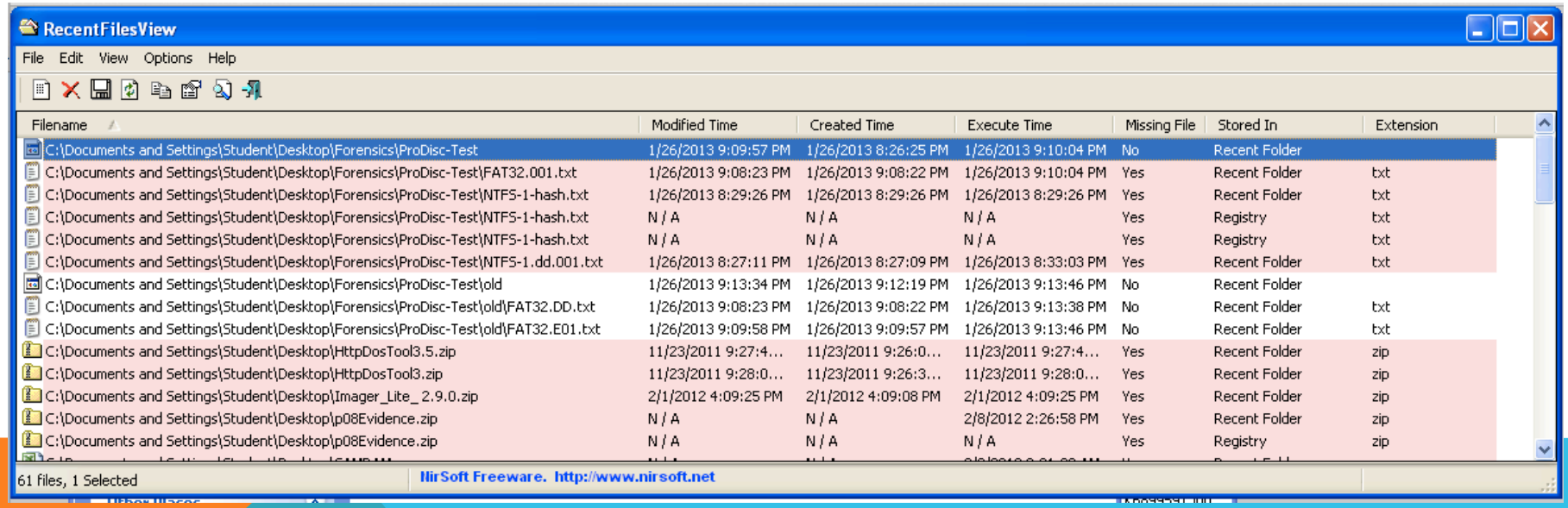
LINK FILES

- SHORTCUT ke program dan file lainnya
- Shortcut memiliki time dan date stamp
- Link pada folder "Recent Files” untuk network shares bahkan bisa berisi alamat MAC dari server!

RECENT FILES VIEWER

Berjalan di Win XP & Win 7

Link Ch 5z1: RecentFilesView - View the list of recently opened files



PROGRAM YANG DIINSTAL

- Memberikan informasi mengenai aktivitas pengguna
- Program yang baru dihapus juga dapat menjadi barang bukti penting
- Jejak program yang dihapus dapat ditemukan dalam
  - folder Program
  - Links
  - file prefetch