

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)

The screenshot shows a Windows environment with a Command Prompt window and a Notepad window.

Command Prompt Window:

```
C:\> whoami /all > sids
C:\> notepad sids
```

Notepad Window (sids - Notepad):

USER INFORMATION

User Name	SID
win-cvttkbe78bp\student	S-1-5-21-2492010294-1904606464-3244937070-1000

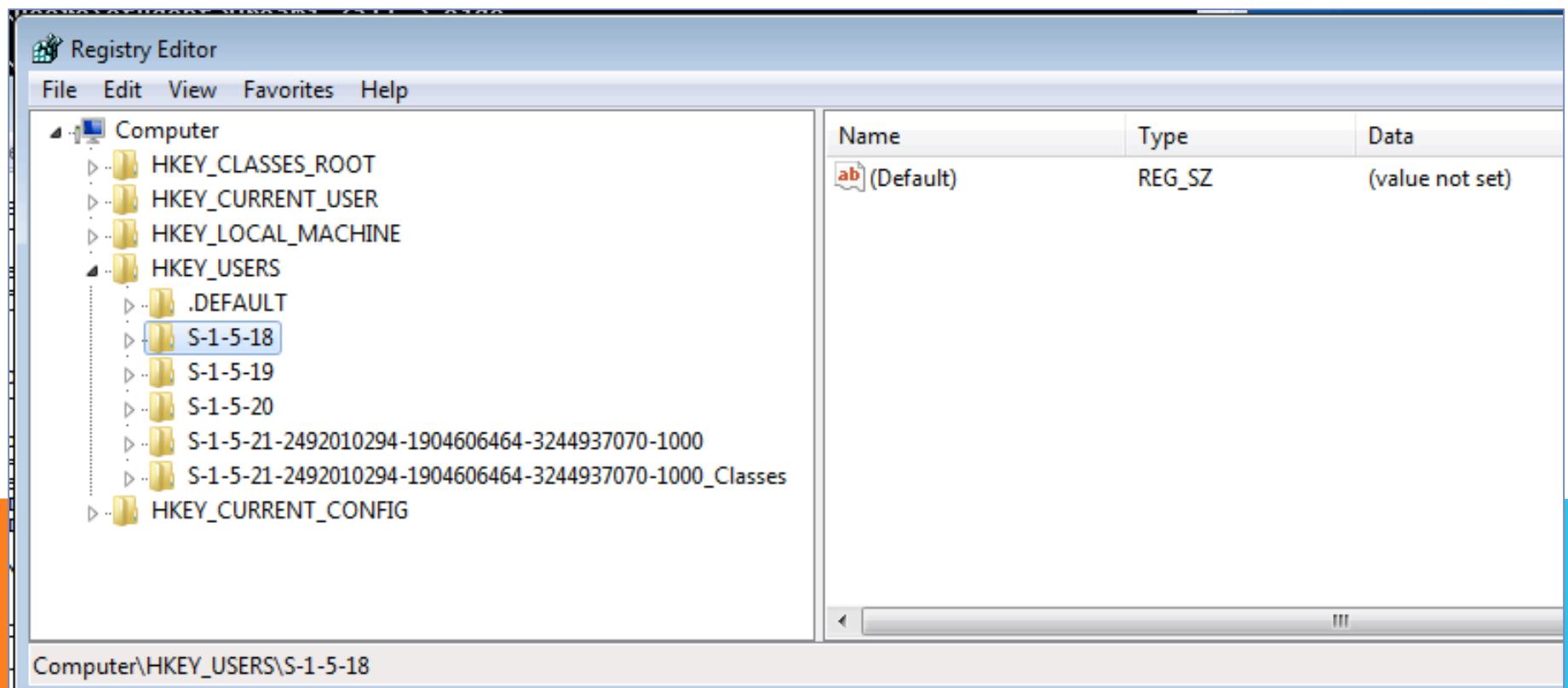
GROUP INFORMATION

Group Name	Type	SID	Attributes
Everyone	Well-known group	S-1-1-0	Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators	Alias	S-1-5-32-544	Group used for deny only
BUILTIN\Users	Alias	S-1-5-32-545	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE	Well-known group	S-1-5-4	Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON	Well-known group	S-1-2-1	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users	Well-known group	S-1-5-11	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization	Well-known group	S-1-5-15	Mandatory group, Enabled by default, Enabled group
LOCAL	Well-known group	S-1-2-0	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication	Well-known group	S-1-5-64-10	Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level	Label	S-1-16-8192	Mandatory group, Enabled by default, Enabled group

PRIVILEGES INFORMATION

Privilege Name	Description	State
SeShutdownPrivilege	Shut down the system	Disabled
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeUndockPrivilege	Remove computer from docking station	Disabled
SeIncreaseWorkingSetPrivilege	Increase a process working set	Disabled
SeTimeZonePrivilege	Change the time zone	Disabled

SIDS DI REGISTRY



WELL-KNOWN SIDS

Link [Ch 5o: Well-known security identifiers in Windows operating systems](#)

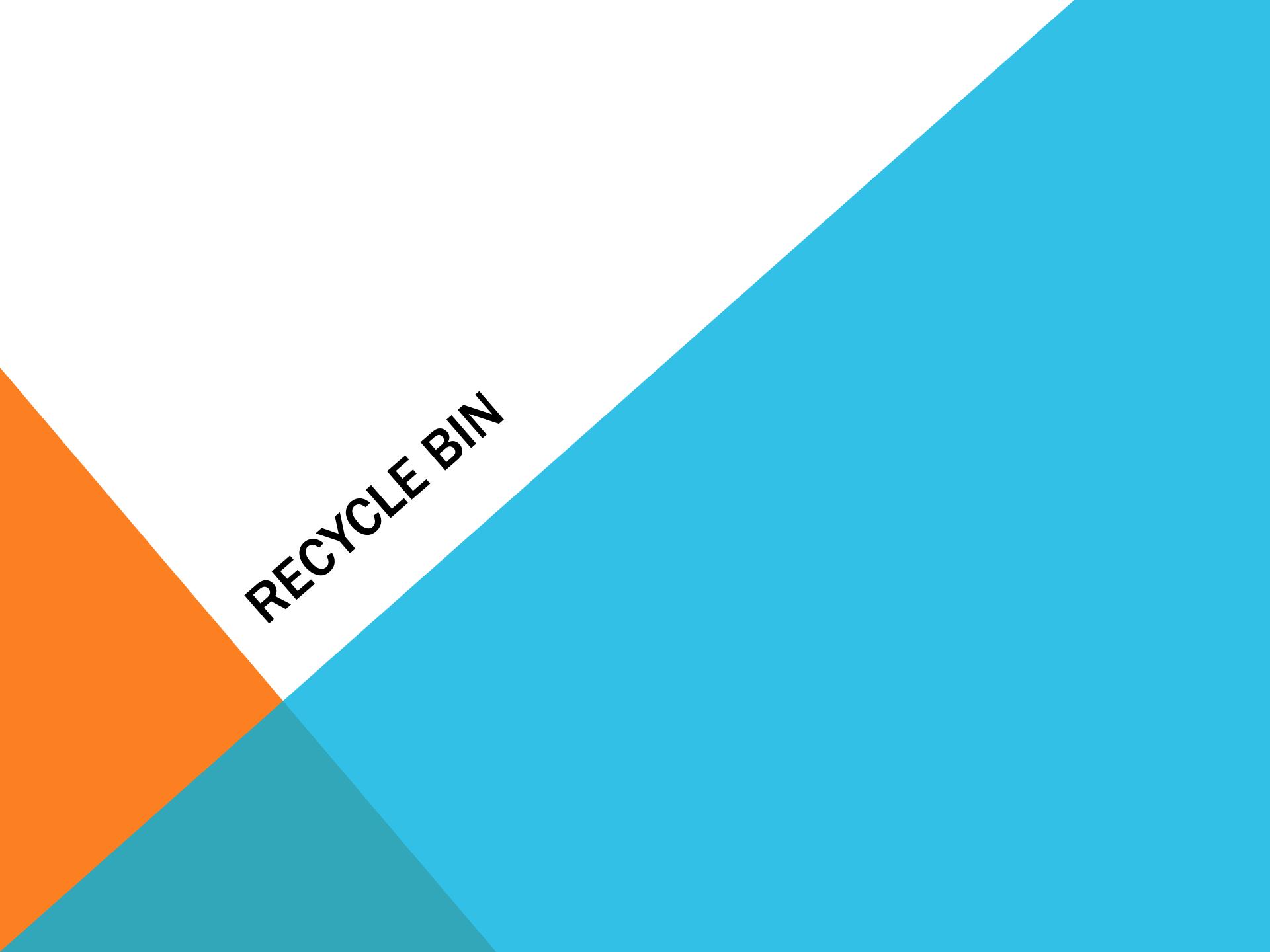
- SID: S-1-5-18
Name: Local System
Description: A service account that is used by the operating system.
- SID: S-1-5-19
Name: NT Authority
Description: Local Service
- SID: S-1-5-20
Name: NT Authority
Description: Network Service
- SID: S-1-5-21*domain*-500
Name: Administrator
Description: A user account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

EKSTERNAL DRIVES

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

PRINT SPOOLING

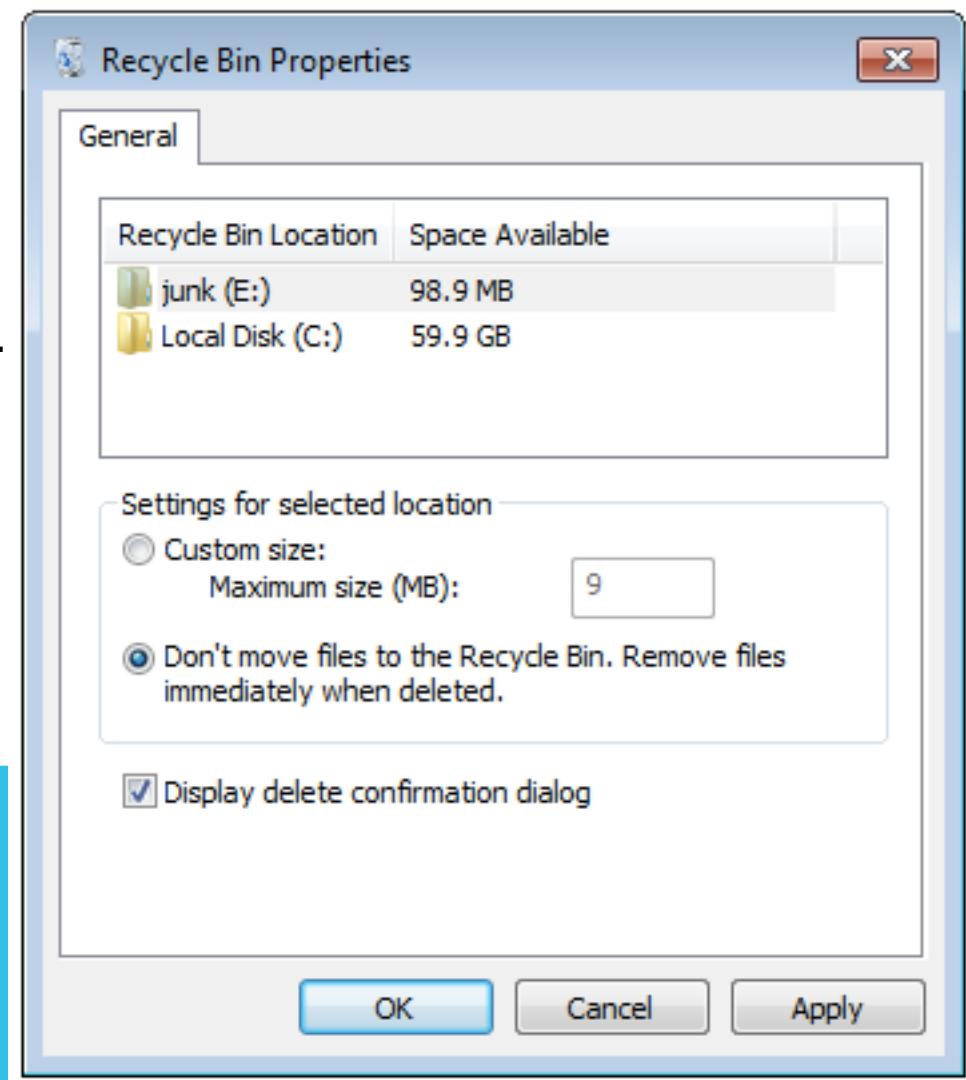
- Ketika dokumen dicetak, ada dua files yang dibuat
 - Enhanced Meta File (EMF) yang berisikan image dari dokumen yang akan dicetak
 - Spool File yang berisi informasi mengenai print job
- Biasanya di deleted setelah selesai dicetak, tapi terkadang masih ada pada beberapa systems



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

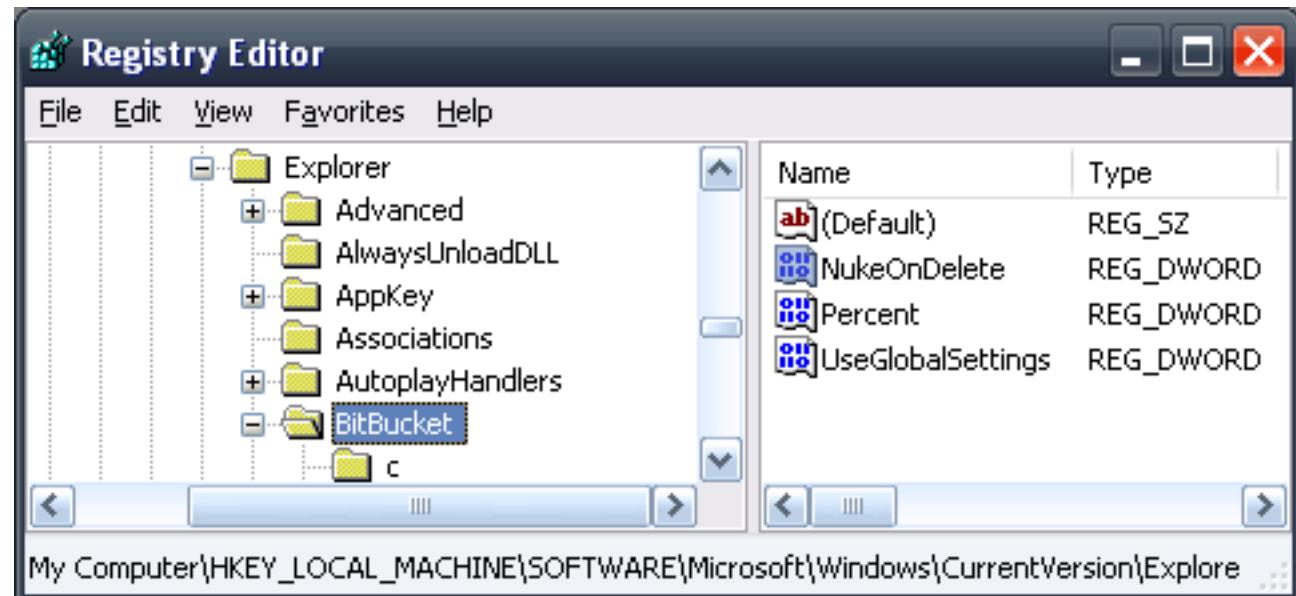


NUKEONDELETE REGISTER KEY

Win XP

(Link

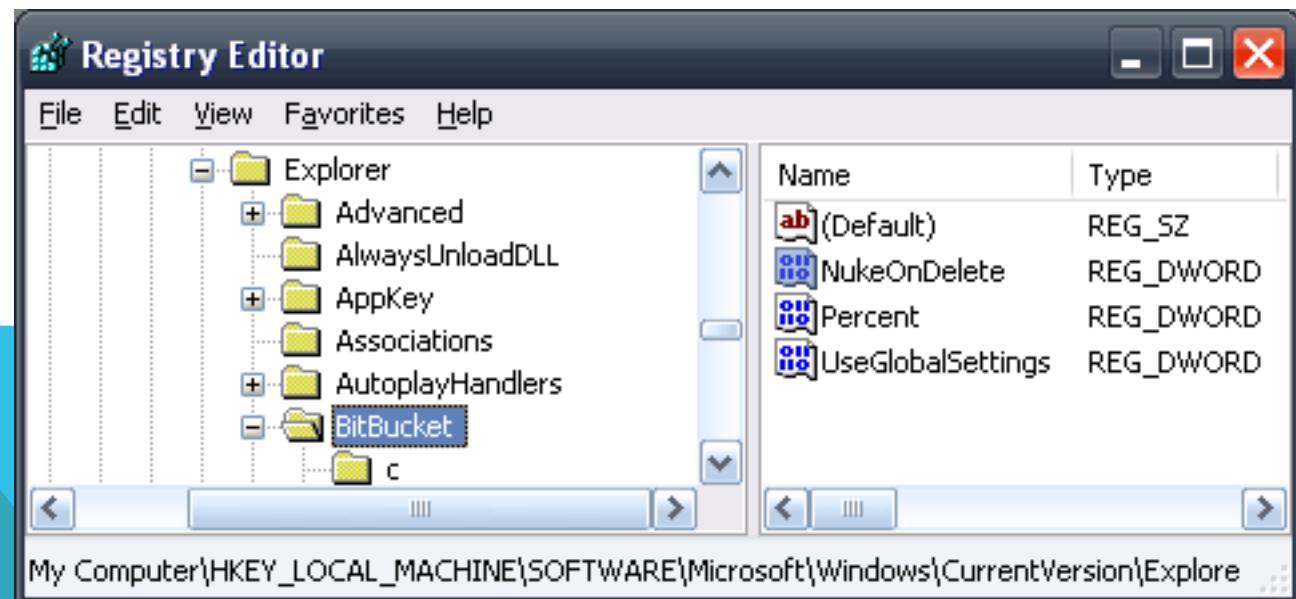
[CH 5p: Registry
Hack: Enable Or
Disable The
Recycle Bin At
Will!!\)](#)



Win 7

(Link

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





METADATA

METADATA

Data tentang data

Metadata File system

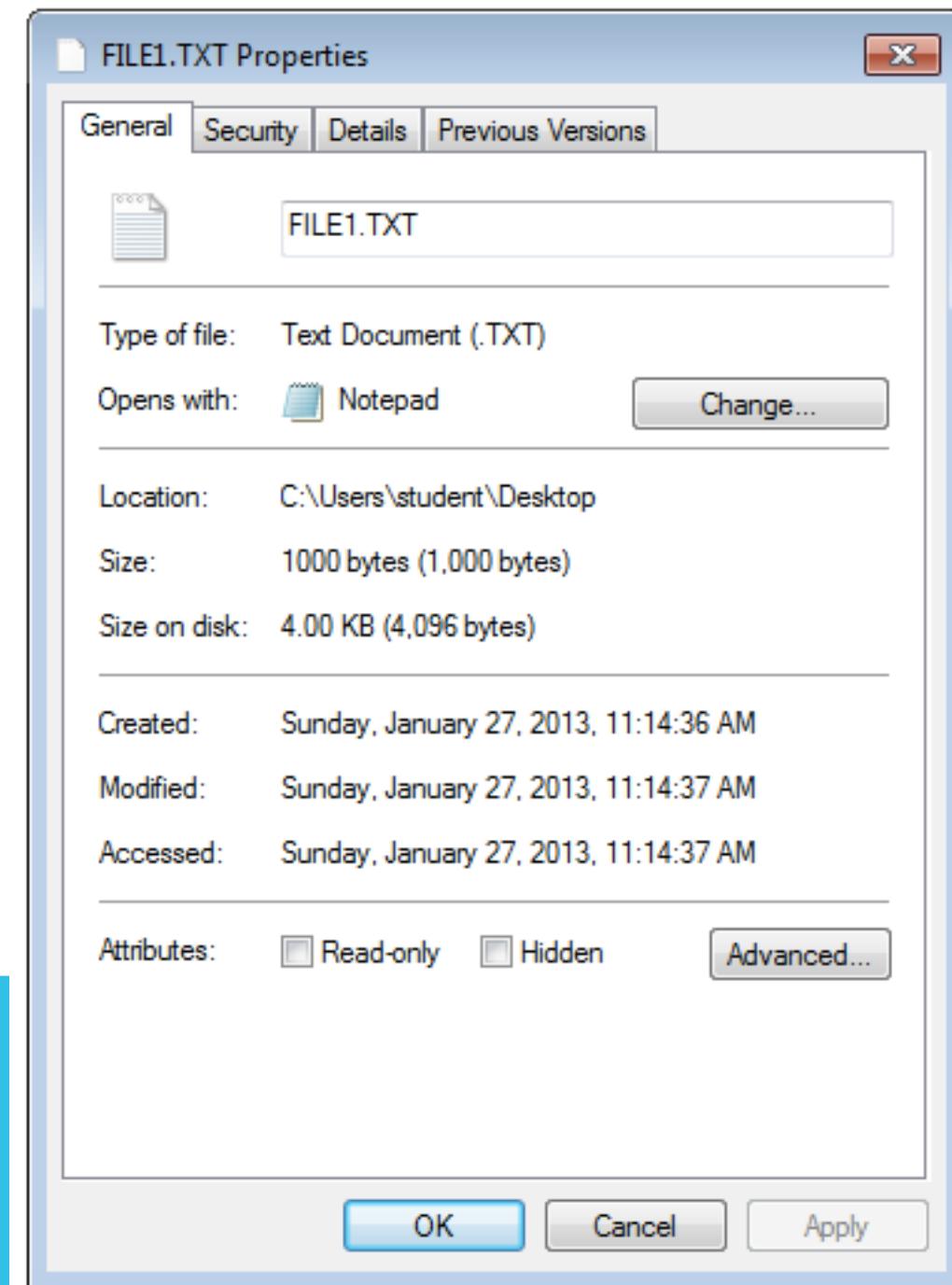
- Timestamps (Created, Modified, Accessed)
- Permissions, owner

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 memerlukan 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%... 4⁴

[CLEAR IMAGE]

From Web
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

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](#)

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](#)



Guide to the Dangers of Hidden Information in Documents

A Workshare Report
Published 2011

Link Ch 5u: Dangers of Metadata (pdf)

- **Google:** Google revealed private financial information from a PowerPoint presentation before posting it for public review.
- **Microsoft:** Through hidden data within Microsoft Word documents, Press found that Microsoft's advertising campaign to lure customers from Apple to Microsoft's software was in fact a success.
- **Whole Foods:** Court documents containing hidden information revealed plans to close stores, disclosed how Whole Foods' acquisition of Wild Oats cost \$100 million, and disclosed the company's secret negotiations with Wal-Mart.
- **Barclays:** An Excel spreadsheet contained sensitive information about a merger between two companies. The spreadsheet was then accidentally submitted in Barclays bid document.
- **Google:** Hidden metadata revealed Google's plan to remove payment options from its Australian Competition Commission and Consumer Protection website. Google removed all payment options except PayPal.
- **AT&T:** AT&T revealed confidential information about its mobile broadband network in a PDF file that was released that included hidden information.
- **Telxon Corp.:** Abrupt deletion of all metadata from a document was considered to be in "good faith" production and did not result in a sanction.
- **Alcatel:** A security vulnerability in Alcatel's DNA software was discovered in 2009. The company failed to fix the bug because it did not consider the metadata to be important.
- **SCO Group:** This leading software provider filed a class action suit against AutoZone and track changes left in a Microsoft Word document. The suit was dismissed because considerable time was spent focusing on Battlestar Galactica rather than the automaker.
- **Westpac:** The oldest bank in Australia revealed sensitive information about a merger before it was finalized and lodged with the Australian Securities Exchange.

REMOVING METADATA

- Microsoft Office Document Inspector

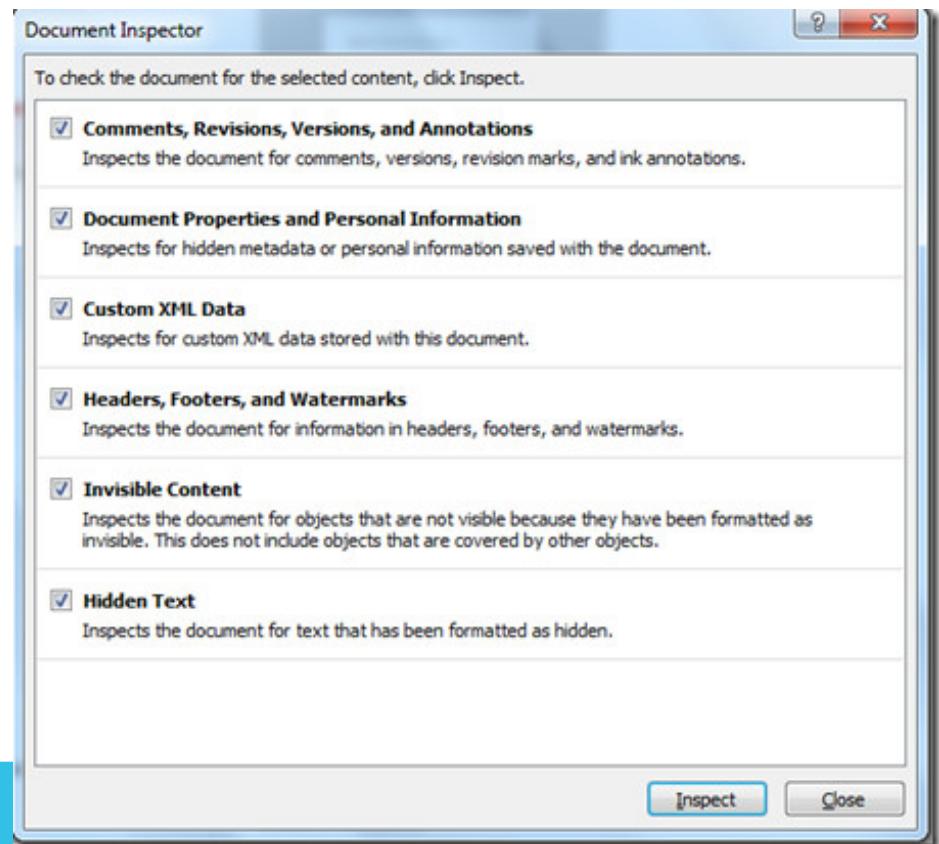
- Link Ch

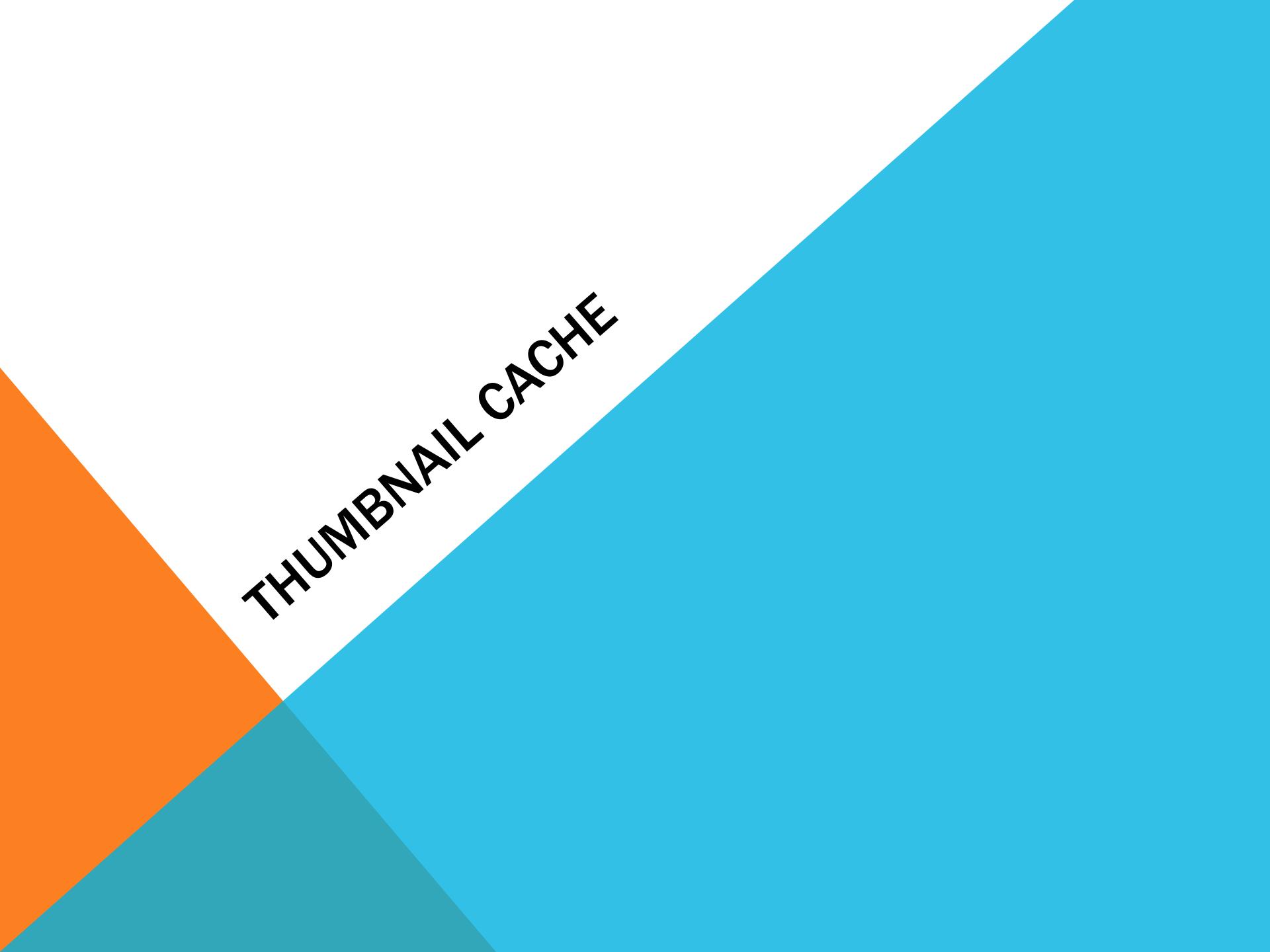
Ch 5v: Microsoft Office 2010 Document Inspector

- Tools Iain

- Link

Ch 5w: Metadata removal tool - Wikipedia





THUMBNAIL CACHE

WINDOWS XP THUMBNAILS

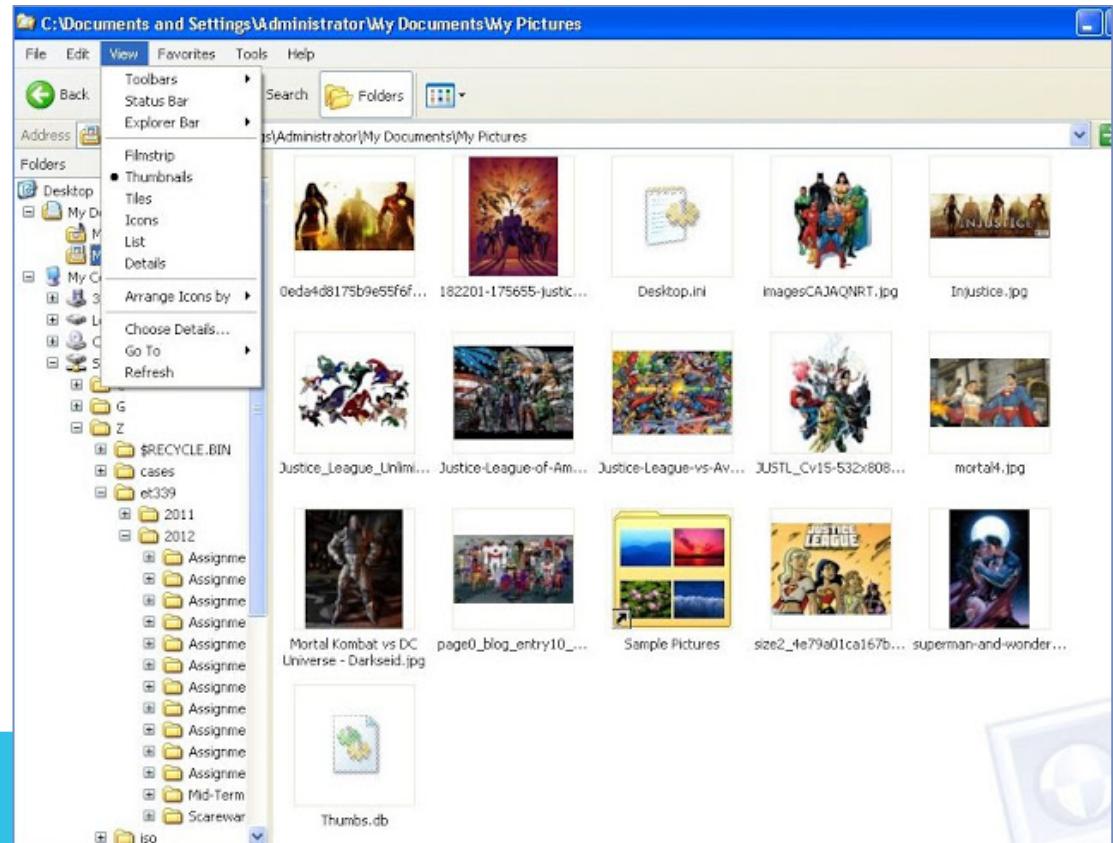
Thumbs.db

- File tersembunyi di folder yang sama dalam bentuk gambar

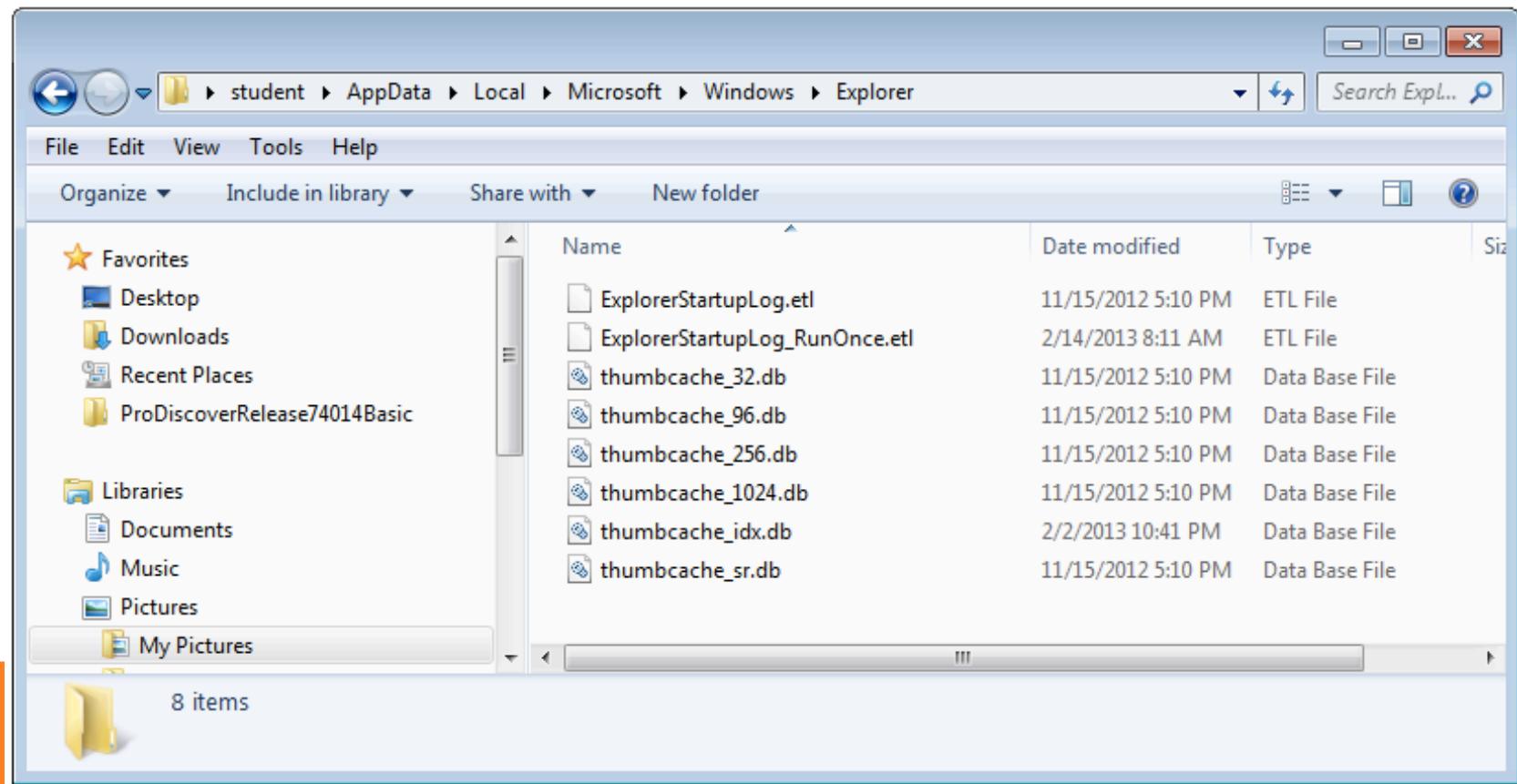
■ Image dari link

Ch 5x:

ESCForensics:
Analyzing
Thumbcache



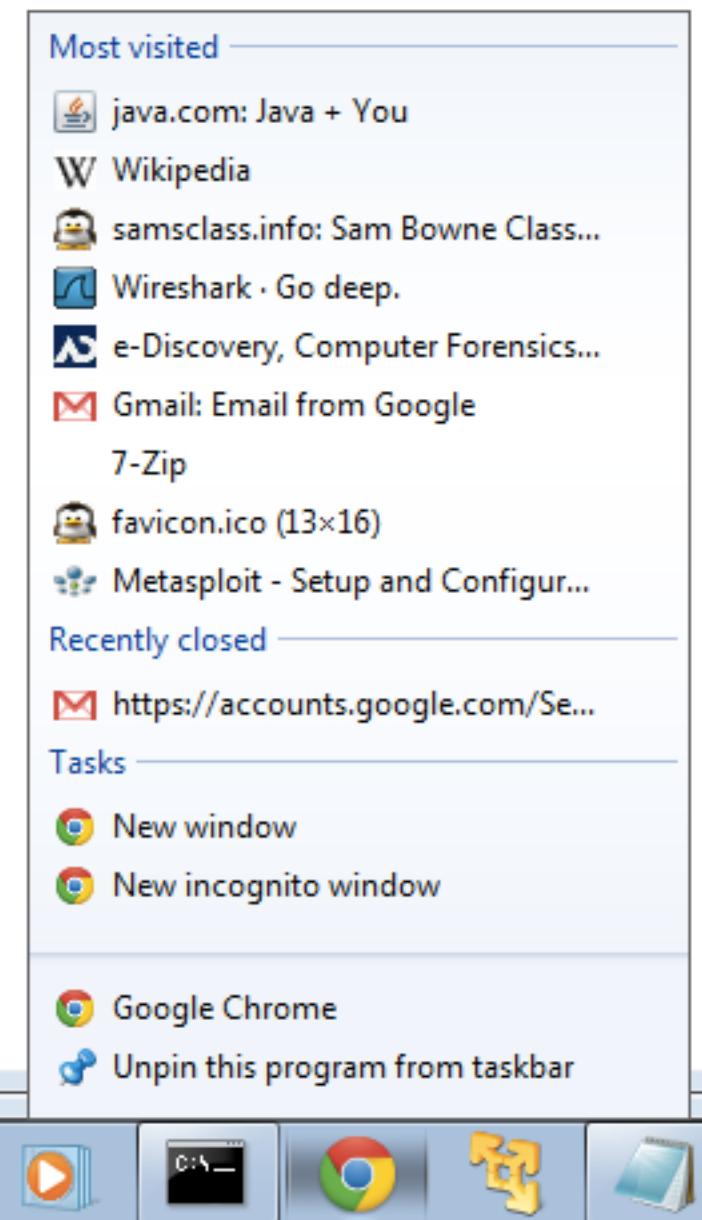
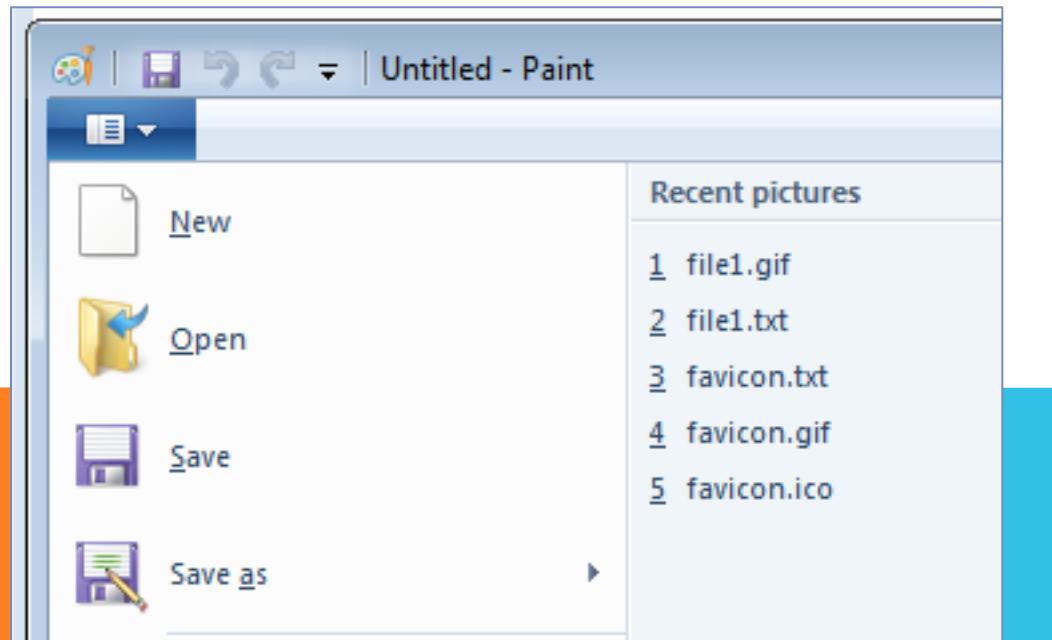
WINDOWS 7 THUMBNAILS



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

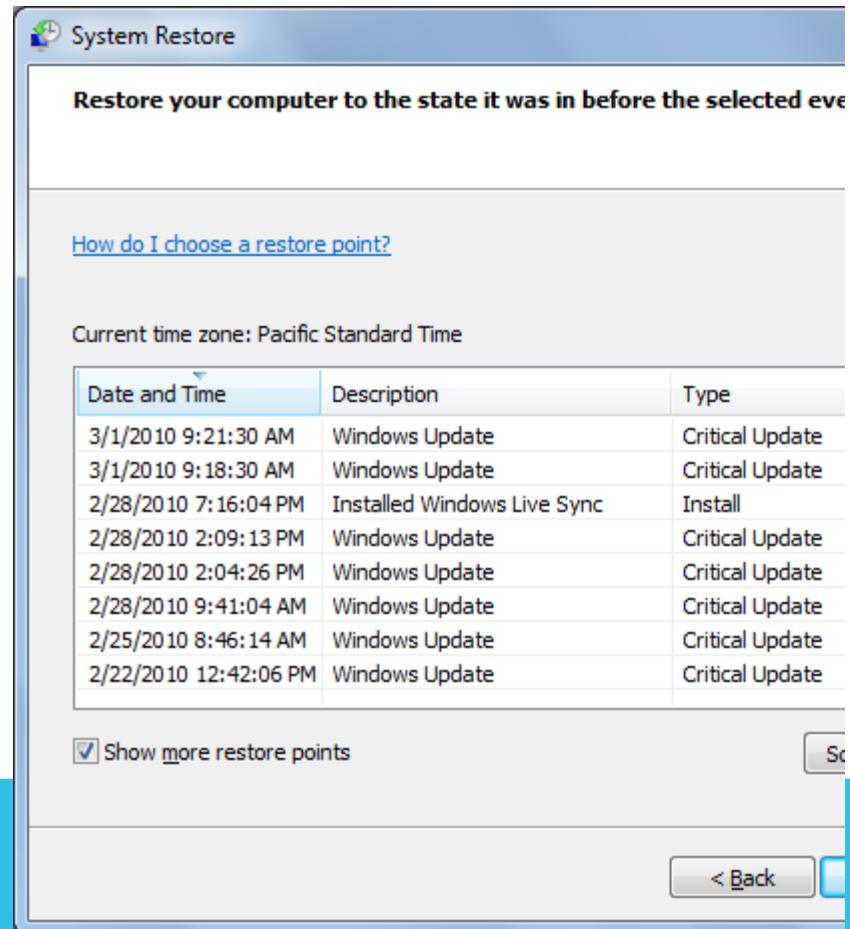




SYSTEM RESTORE

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

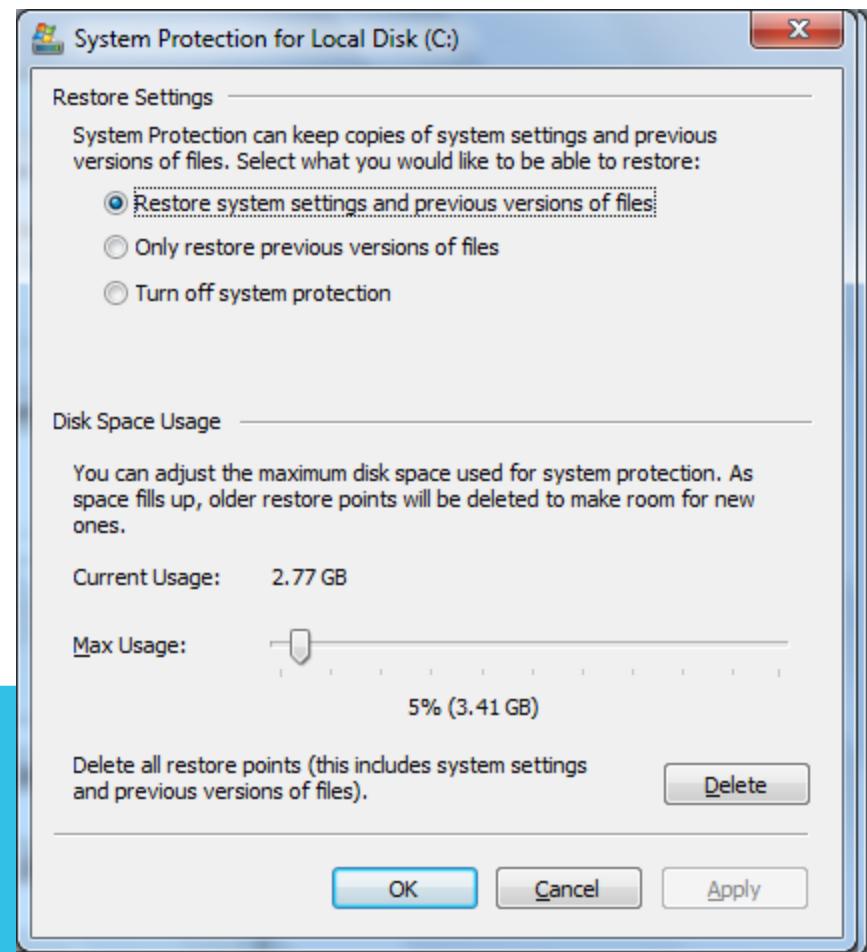


KAPAN RESTORE POINT DIBUAT

- 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

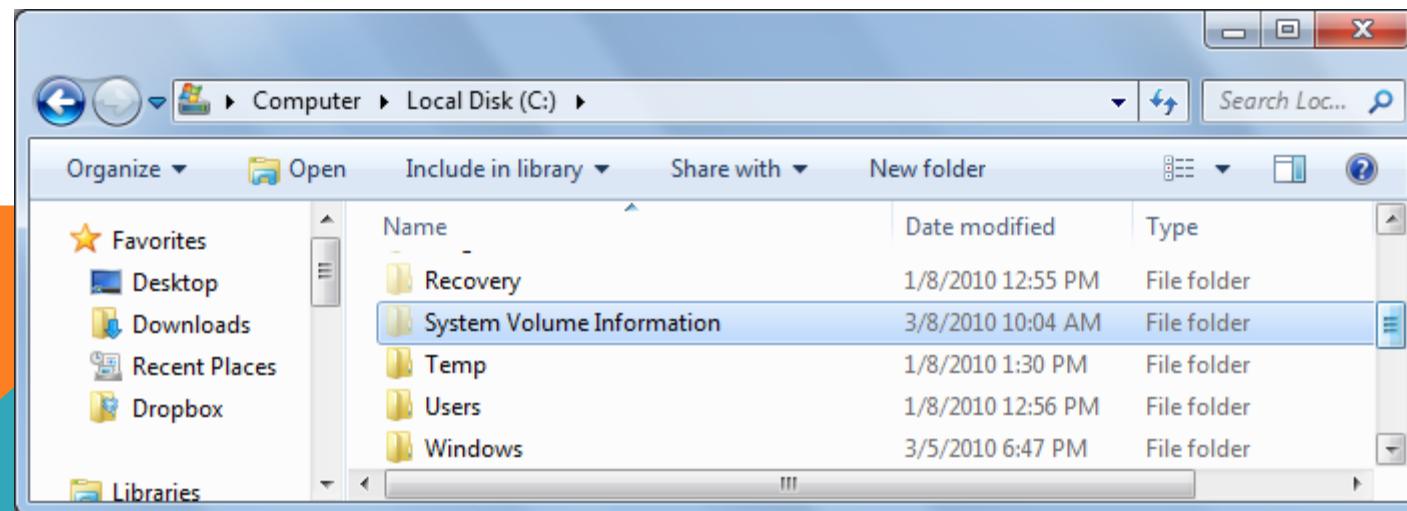
- Klik Configure
- Pilih apakah akan memonitor sistem settings atau hanya file
- "System Settings" mencakup Registry dan banyak jenis file sistem lainnya



SYSTEM RESTORE FILES

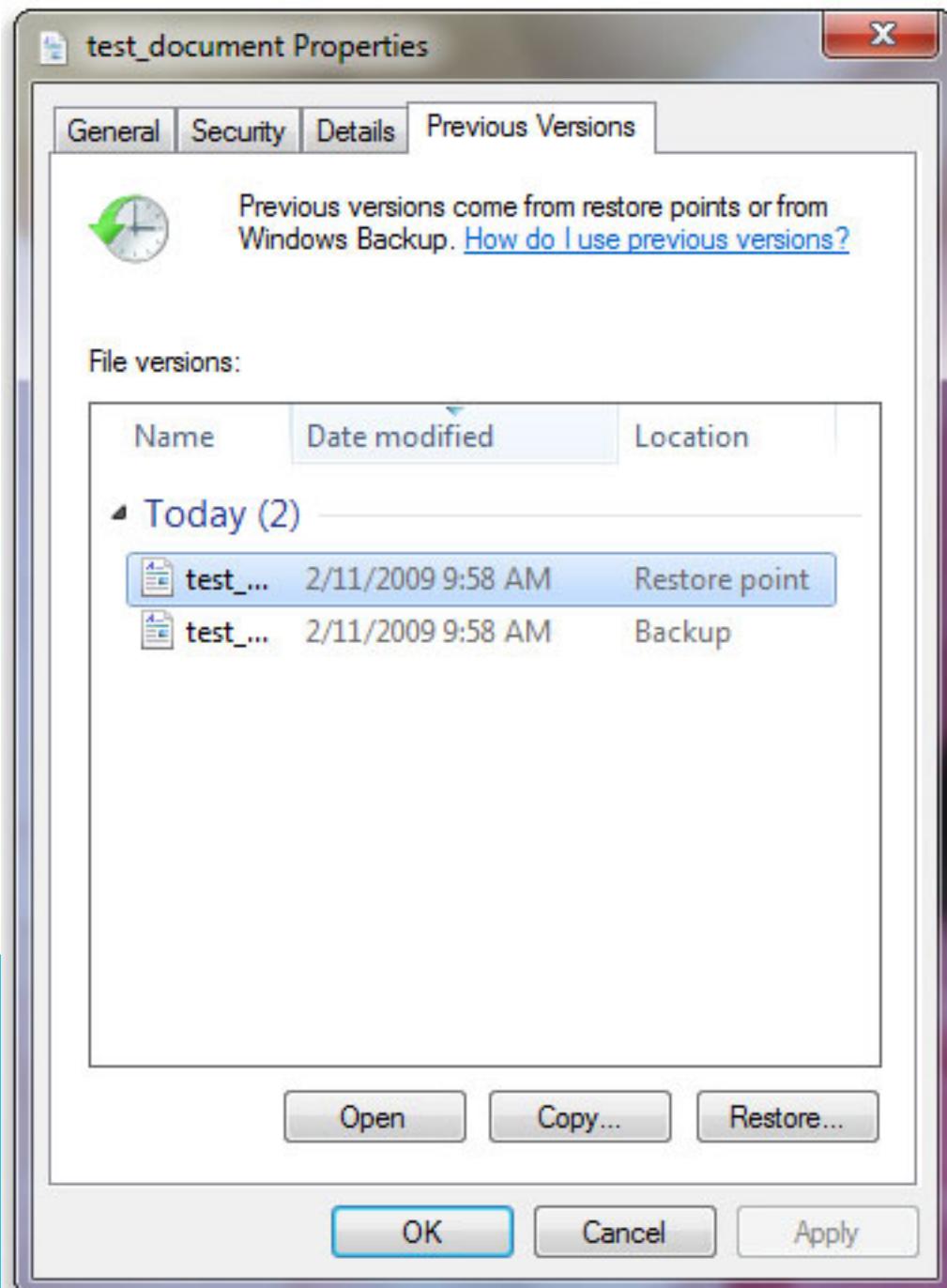
Letaknya di C:\System Volume Information

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



PREVIOUS VERSIONS

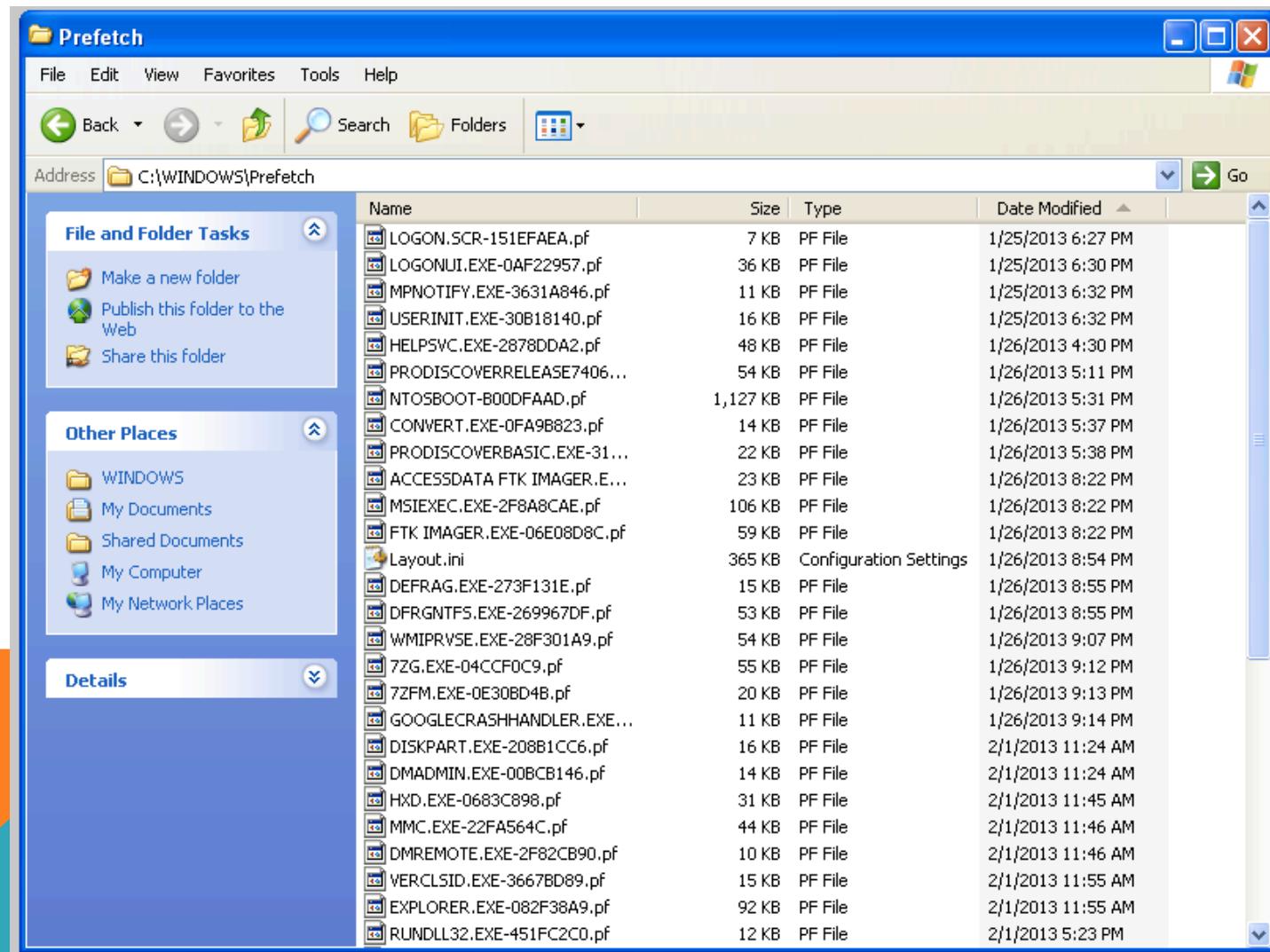
gambar from microsoft.com



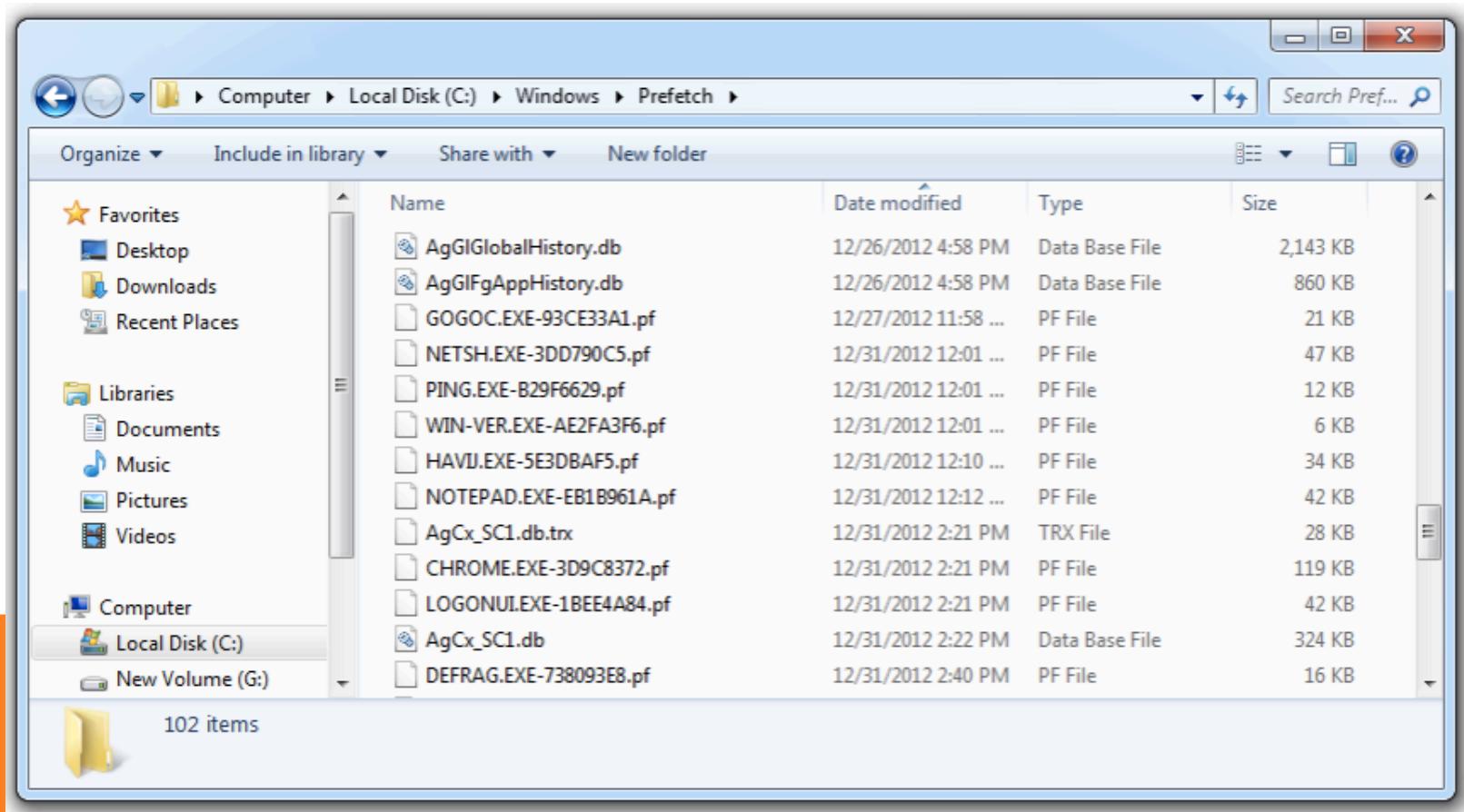
PREFETCH

- 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](#)

Filename	Modified Time	Created Time	Execute Time	Missing File	Stored In	Extension
C:\Documents and Settings\Student\Desktop\Forensics\ProDisc-Test	1/26/2013 9:09:57 PM	1/26/2013 8:26:25 PM	1/26/2013 9:10:04 PM	No	Recent Folder	
C:\Documents and Settings\Student\Desktop\Forensics\ProDisc-Test\FAT32.001.txt	1/26/2013 9:08:23 PM	1/26/2013 9:08:22 PM	1/26/2013 9:10:04 PM	Yes	Recent Folder	txt
C:\Documents and Settings\Student\Desktop\Forensics\ProDisc-Test\NTFS-1-hash.txt	1/26/2013 8:29:26 PM	1/26/2013 8:29:26 PM	1/26/2013 8:29:26 PM	Yes	Recent Folder	txt
C:\Documents and Settings\Student\Desktop\Forensics\ProDisc-Test\NTFS-1-hash.txt	N / A	N / A	N / A	Yes	Registry	txt
C:\Documents and Settings\Student\Desktop\Forensics\ProDisc-Test\NTFS-1-hash.txt	N / A	N / A	N / A	Yes	Registry	txt
C:\Documents and Settings\Student\Desktop\Forensics\ProDisc-Test\NTFS-1.dd.001.txt	1/26/2013 8:27:11 PM	1/26/2013 8:27:09 PM	1/26/2013 8:33:03 PM	Yes	Recent Folder	txt
C:\Documents and Settings\Student\Desktop\Forensics\ProDisc-Test\old	1/26/2013 9:13:34 PM	1/26/2013 9:12:19 PM	1/26/2013 9:13:46 PM	No	Recent Folder	
C:\Documents and Settings\Student\Desktop\Forensics\ProDisc-Test\old\FAT32.DD.txt	1/26/2013 9:08:23 PM	1/26/2013 9:08:22 PM	1/26/2013 9:13:38 PM	No	Recent Folder	txt
C:\Documents and Settings\Student\Desktop\Forensics\ProDisc-Test\old\FAT32.E01.txt	1/26/2013 9:09:58 PM	1/26/2013 9:09:57 PM	1/26/2013 9:13:46 PM	No	Recent Folder	txt
C:\Documents and Settings\Student\Desktop\HttpDosTool3.5.zip	11/23/2011 9:27:4...	11/23/2011 9:26:0...	11/23/2011 9:27:4...	Yes	Recent Folder	zip
C:\Documents and Settings\Student\Desktop\HttpDosTool3.zip	11/23/2011 9:28:0...	11/23/2011 9:26:3...	11/23/2011 9:28:0...	Yes	Recent Folder	zip
C:\Documents and Settings\Student\Desktop\Imager_Lite_2.9.0.zip	2/1/2012 4:09:25 PM	2/1/2012 4:09:08 PM	2/1/2012 4:09:25 PM	Yes	Recent Folder	zip
C:\Documents and Settings\Student\Desktop\p08Evidence.zip	N / A	N / A	2/8/2012 2:26:58 PM	Yes	Recent Folder	zip
C:\Documents and Settings\Student\Desktop\p08Evidence.zip	N / A	N / A	N / A	Yes	Registry	zip

61 files, 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>

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