





2014

File History Analysis



Windows 8

Who are we?

Kausar Khizra

- Paranoid Yahoo 
- MSDF – UCF
- C | EH AME ACE Security+
- blogger@forensicfocus
- Contact: khizra6@gmail.com,
LinkedIn 

Nasa Quba

- Paranoid Yahoo 
- MSDF – UCF
- C | EH AME ACE Security+
- blogger@forensicfocus
- Contact: nasaquba@gmail.com,
LinkedIn 

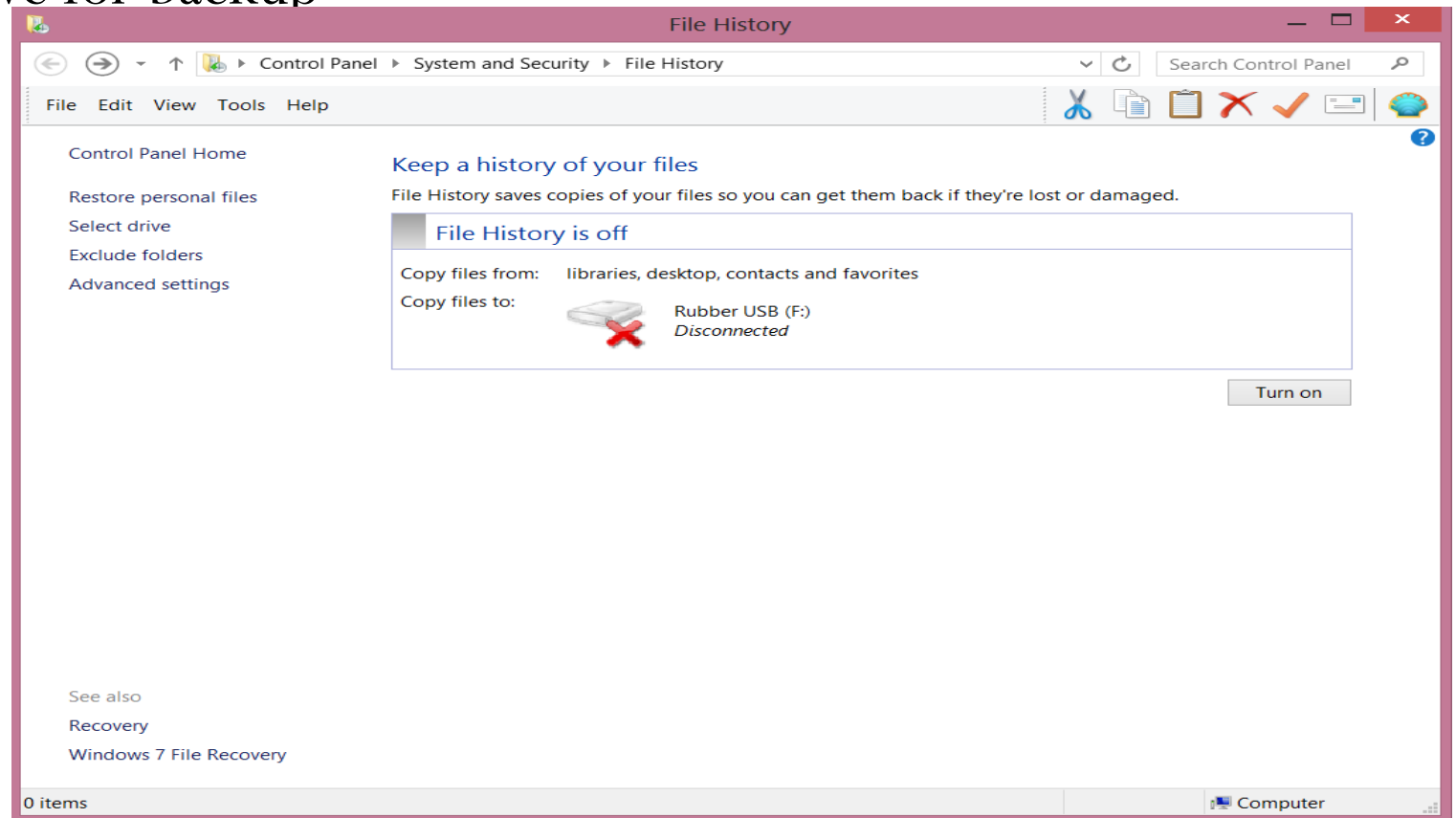
Agenda

- Part 1
 - What is File History (FH)?
 - Why learn FH?
 - How does it work?
 - Comparison of VSS and FH
- Part 2
 - Forensic Analysis
 - Examination of config file, registry and event files

File History Analysis: Part 1

What is File History?

- Backup service introduced in Windows 8
- USN Journal
- Use network or external drive for backup
- Default backup folders
 - Libraries
 - Desktop
 - Contacts
 - Favorites



Why learn File History?

- Regular User
 - Recover deleted and/or previous version(s) of files/folders
- Forensic Examiner
 - Recover deleted and/or previous version(s) of files/folder
 - Find out the external drive in use that may also contain other important data

File History underline principle

- \$UsnJrnl

- Tools

- Fsutil

- JP (Journal Parser) by TZWorks

jp64.exe -partition C -csv -a > output.csv

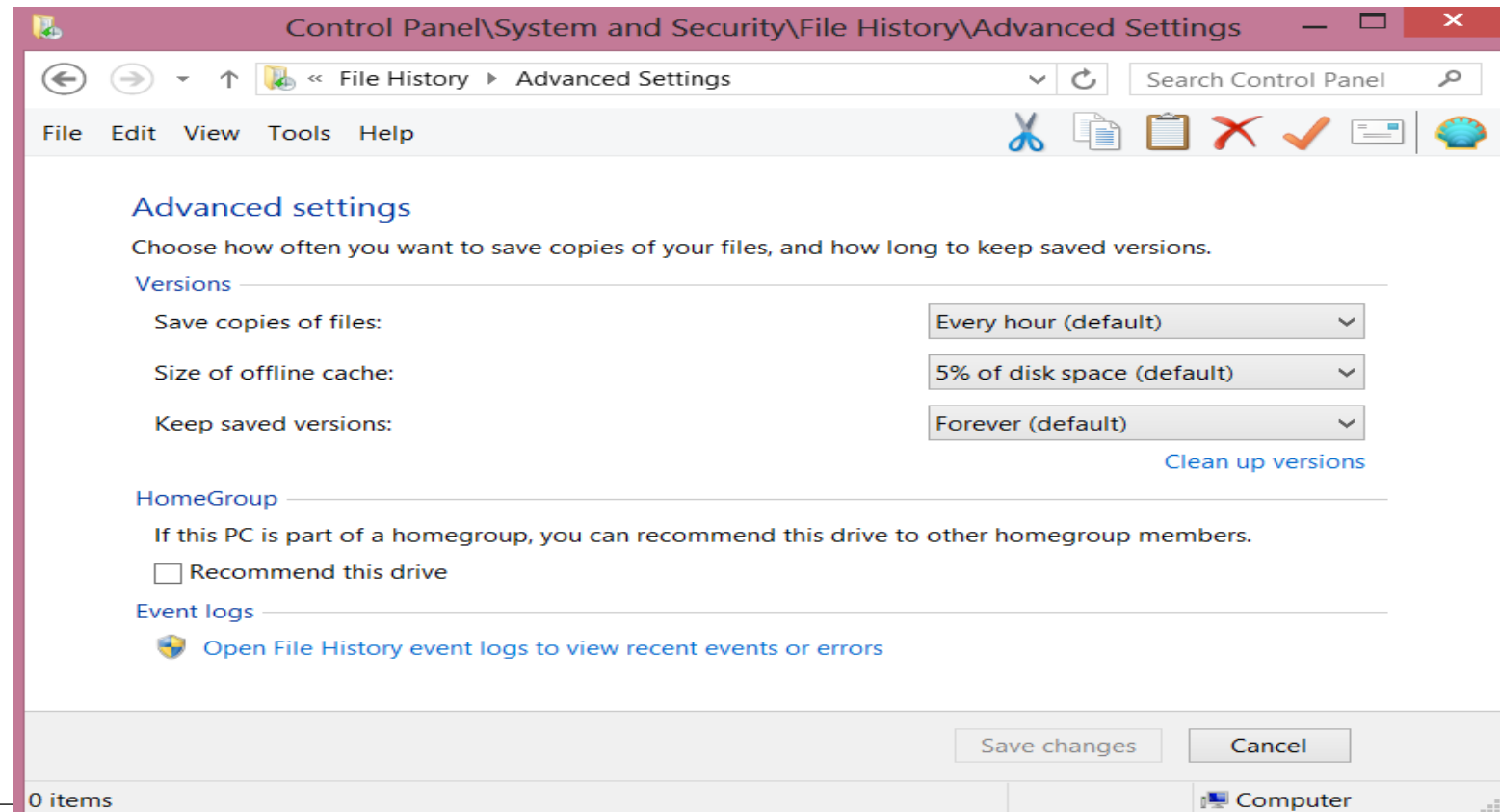
Sample of USN Journal entry when a txt file is created

```
C:\Windows\system32>fsutil usn queryjournal c:
Usn Journal ID       : 0x01ce95800a9eddad
First Usn            : 0x00000000d0240000
Next Usn             : 0x00000000d2485810
Lowest Valid Usn     : 0x000000002da40000
Max Usn              : 0x7fffffffffffffff0000
Maximum Size         : 0x0000000002000000
Allocation Delta     : 0x0000000000400000
Minimum record version supported : 2
Maximum record version supported : 2
```

A	B	C	D	E	F	G	H	I
usndate	time-UTC	MFT entry	seqnum	parent MFT	usn#	attributes	filename	type change
1/1/2014	07:20:48.896	0x000111bf	0x0005	0x00011052	0x00d969d0	archive	abc.txt	file_new_name
1/1/2014	07:20:48.896	0x000111bf	0x0005	0x00011052	0x00d96a20	archive	abc.txt	file_new_name; file_closed

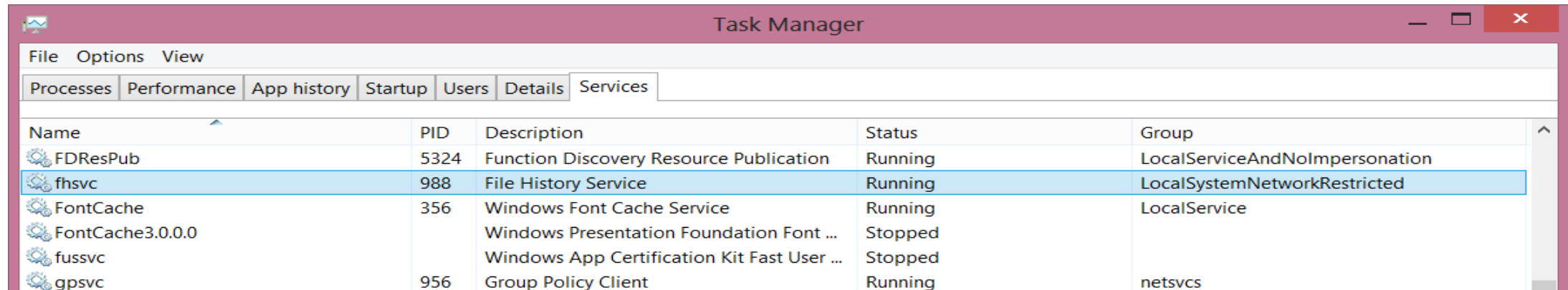
File History settings

- Save Copies - Every 10 min, 15min, 20min, 30min, hour, 3 hours, 6 hours, 12 hours, daily
- Size of offline cache – 2%, 5%, 10%, 20%
- Keep saved versions – 1month, 3 months, 6 months, 9 months, 1 year, 2 years, forever



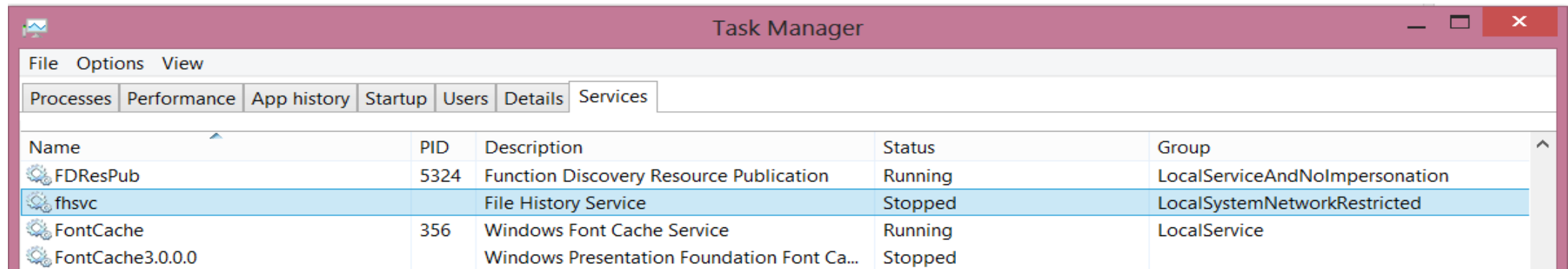
File History service

Service = fhsvc



A screenshot of the Windows Task Manager 'Services' tab. The window title is 'Task Manager'. The 'Services' tab is selected, showing a list of system services. The 'fhsvc' service, 'File History Service', is highlighted in blue. It is running with PID 988 and belongs to the 'LocalSystemNetworkRestricted' group. Other visible services include FDRResPub (running), FontCache (running), FontCache3.0.0.0 (stopped), fustvc (stopped), and gpvc (running).

Name	PID	Description	Status	Group
FDRResPub	5324	Function Discovery Resource Publication	Running	LocalServiceAndNoImpersonation
fhsvc	988	File History Service	Running	LocalSystemNetworkRestricted
FontCache	356	Windows Font Cache Service	Running	LocalService
FontCache3.0.0.0		Windows Presentation Foundation Font ...	Stopped	
fustvc		Windows App Certification Kit Fast User ...	Stopped	
gpvc	956	Group Policy Client	Running	netshvc

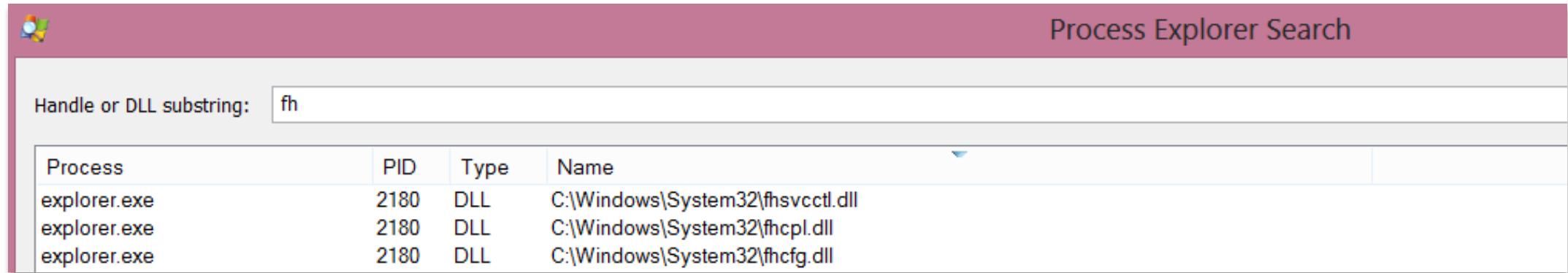


A second screenshot of the Windows Task Manager 'Services' tab, showing the same list of services but with the 'fhsvc' service status changed to 'Stopped'. The 'fhsvc' service is still highlighted in blue. All other services and their details remain the same as in the first screenshot.

Name	PID	Description	Status	Group
FDRResPub	5324	Function Discovery Resource Publication	Running	LocalServiceAndNoImpersonation
fhsvc		File History Service	Stopped	LocalSystemNetworkRestricted
FontCache	356	Windows Font Cache Service	Running	LocalService
FontCache3.0.0.0		Windows Presentation Foundation Font Ca...	Stopped	

File History DLLs

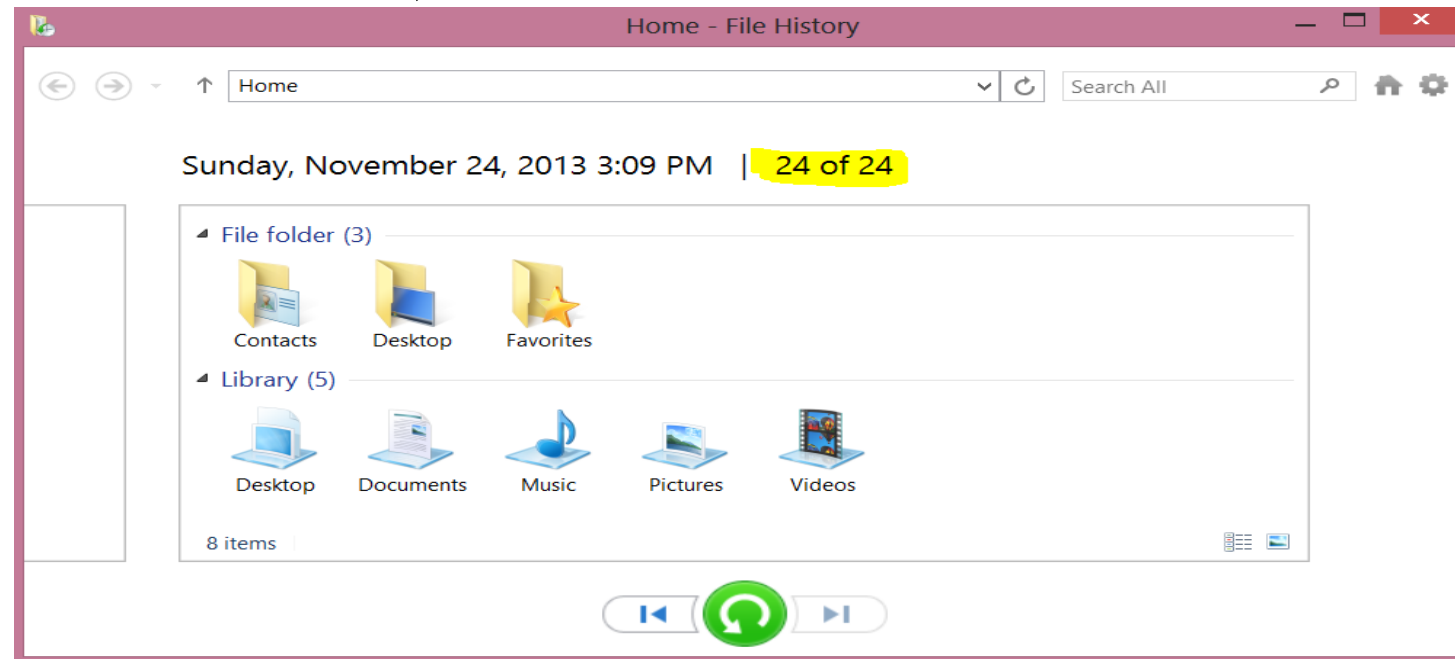
fhcfg.dll, fhcpl.dll, fhsvcctl.dll

A screenshot of the 'Process Explorer Search' window. The title bar is purple and contains the text 'Process Explorer Search'. Below the title bar is a search input field with the text 'fh'. Below the input field is a table with four columns: 'Process', 'PID', 'Type', and 'Name'. The table contains three rows of data, all for the process 'explorer.exe' with PID 2180 and Type DLL. The names of the DLLs are 'C:\Windows\System32\fhsvcctl.dll', 'C:\Windows\System32\fhcpl.dll', and 'C:\Windows\System32\fhcfg.dll'.

Process	PID	Type	Name
explorer.exe	2180	DLL	C:\Windows\System32\fhsvcctl.dll
explorer.exe	2180	DLL	C:\Windows\System32\fhcpl.dll
explorer.exe	2180	DLL	C:\Windows\System32\fhcfg.dll

How does it work?

- Utilize USN Journal to track changes and saves file revisions on backup location
- Saves the amended version with appended date/time. Example:
 - MyABC (2013_10_03 03_37_37).doc
 - MyABC (2013-11_03 04_55_20).doc



File History states

- Turned OFF
- Turned ON
 - Case 1: Media/network drive available/online
 - Case 2: Media/network drive NOT available/online – Cache

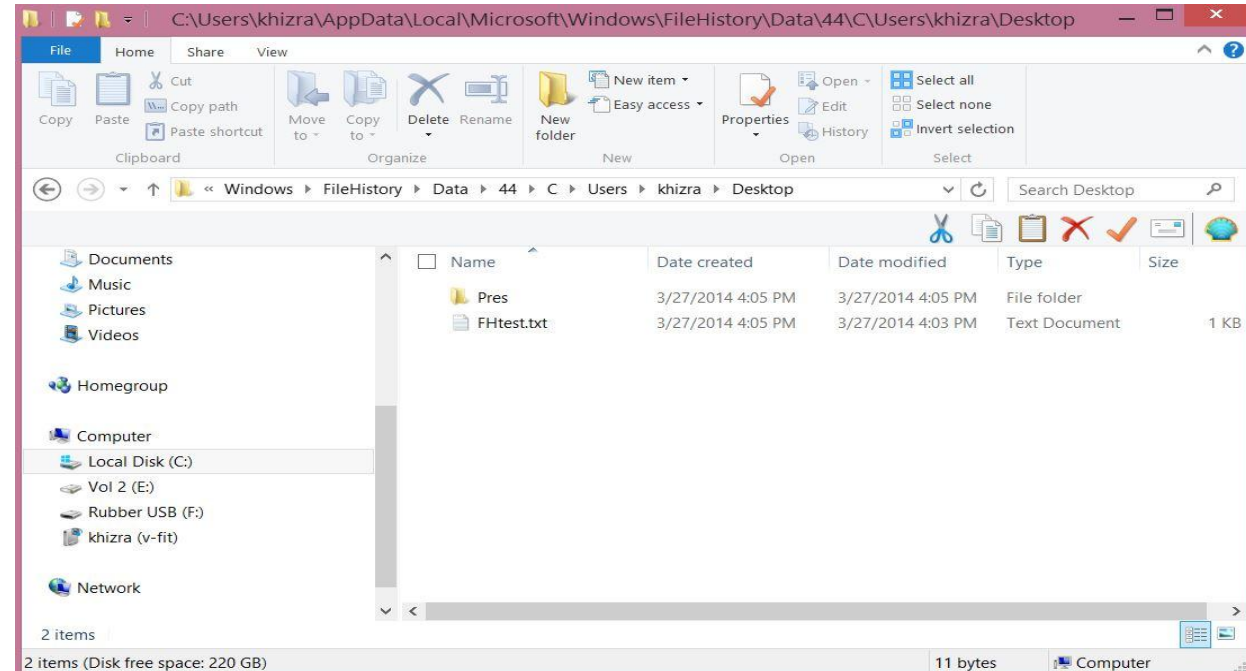
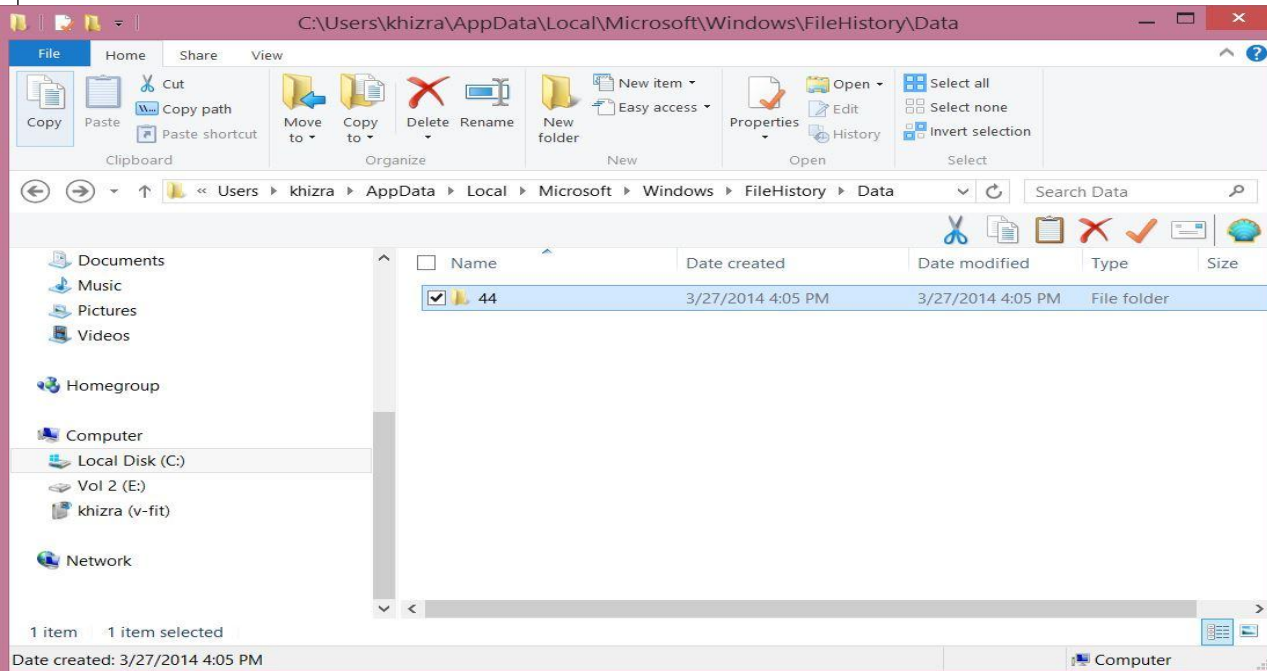
Where is this cache?

- Caches when media is temporarily unavailable
- Location of this cache data is

C:\Users\(\username)\AppData\Local\Microsoft\Windows\FileHistory\Data

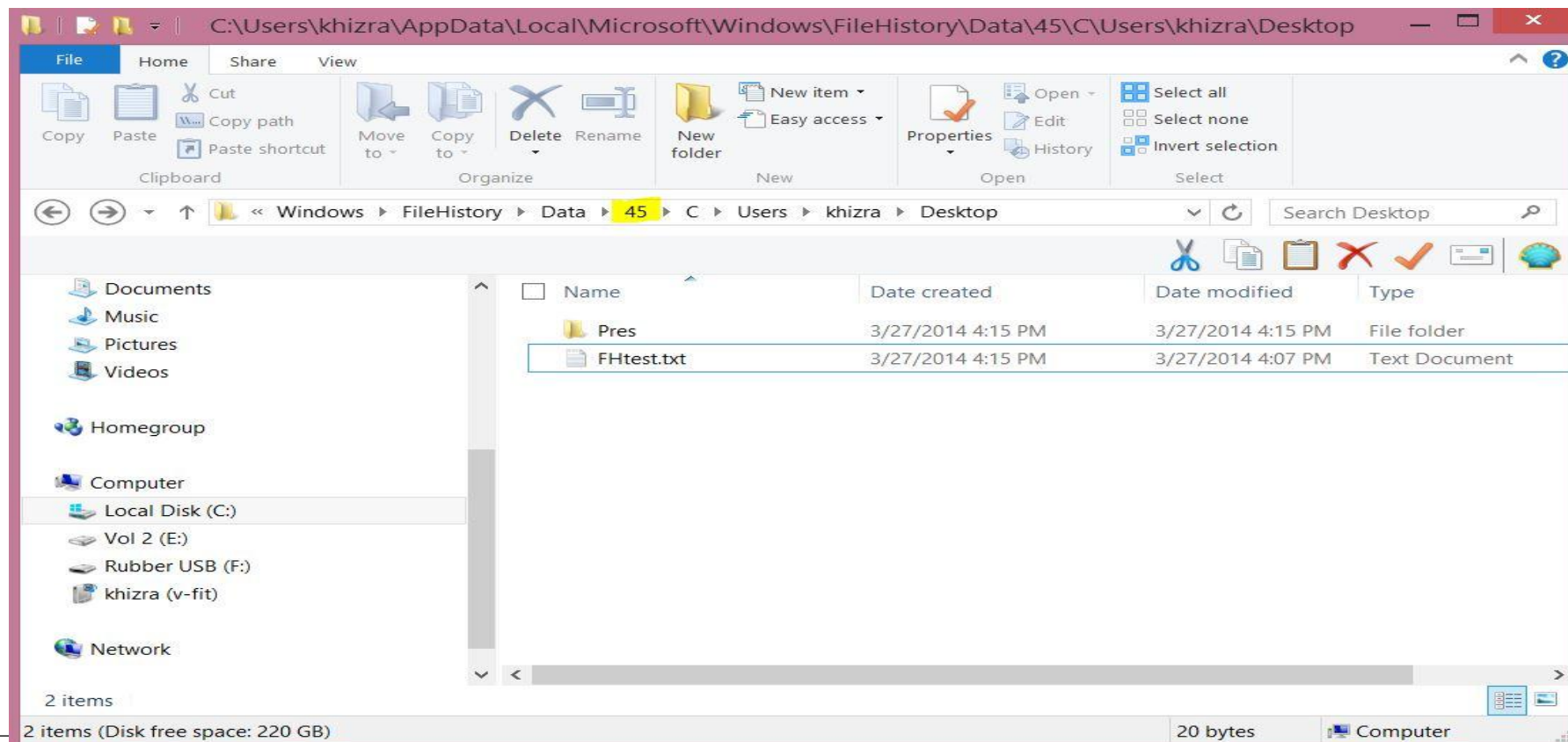
Example

- FH is set to run after every 10 minutes
- Create a file FHtest.txt at **4:03 p.m.**
 - Run FH manually without media at **4:05 p.m.**
 - Folder 44 created



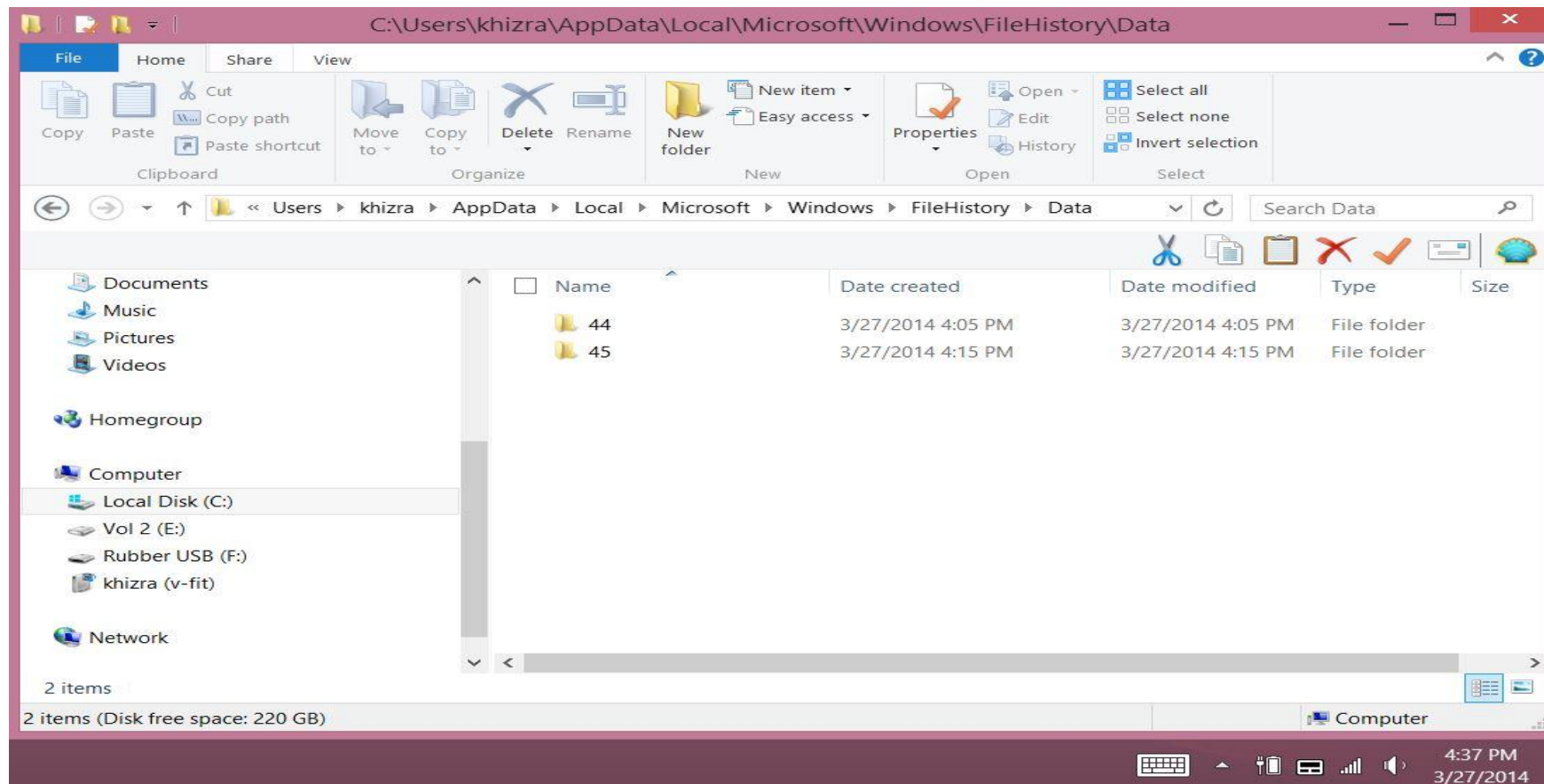
Example contd..

- Modified file FHtest.txt and saved it at **4:07** p.m.
- FH runs automatically at **4:15** p.m.
- Folder 45 is created



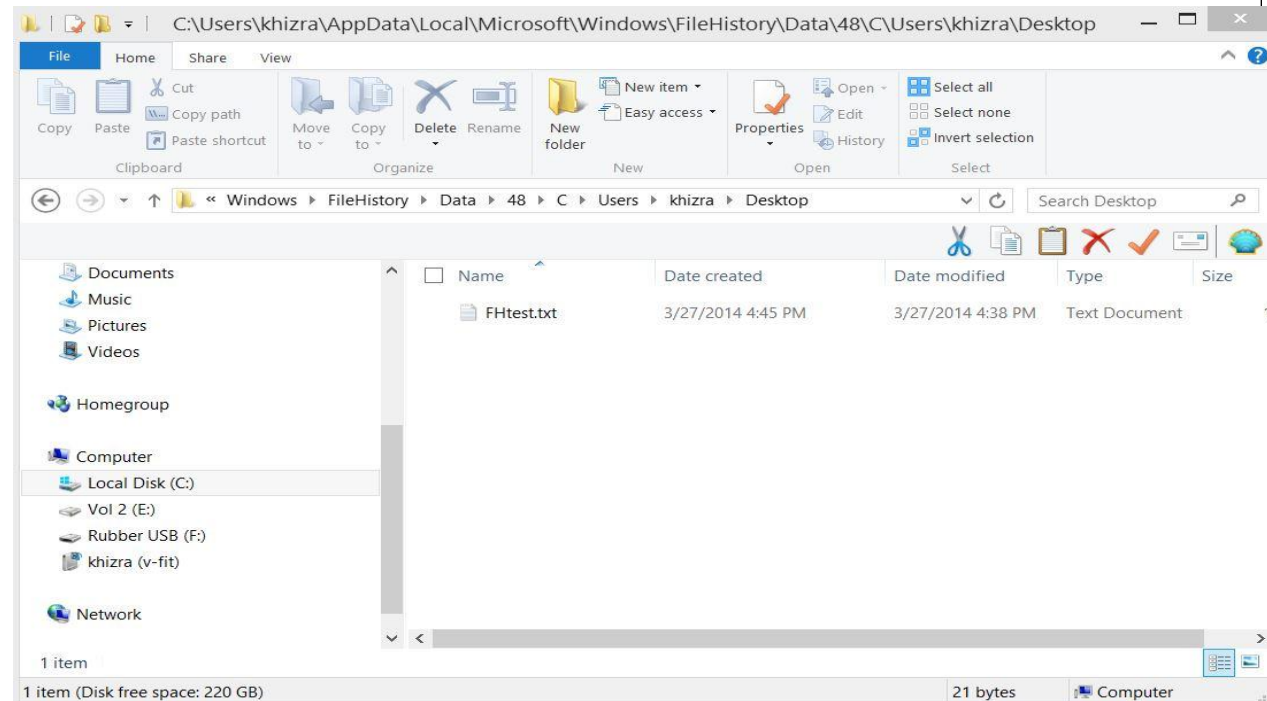
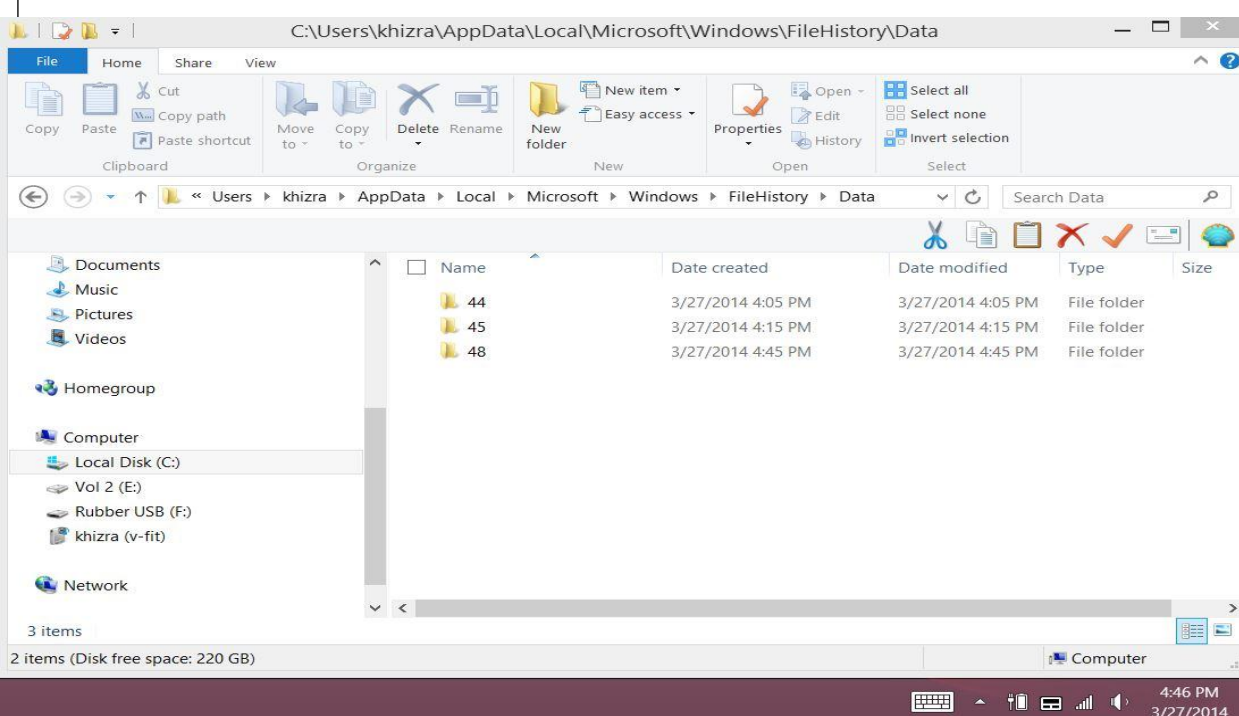
Example contd..

- No changes were made on the file FHtest.txt for the next **20 minutes** (2 events of FH service)
- No new folders created



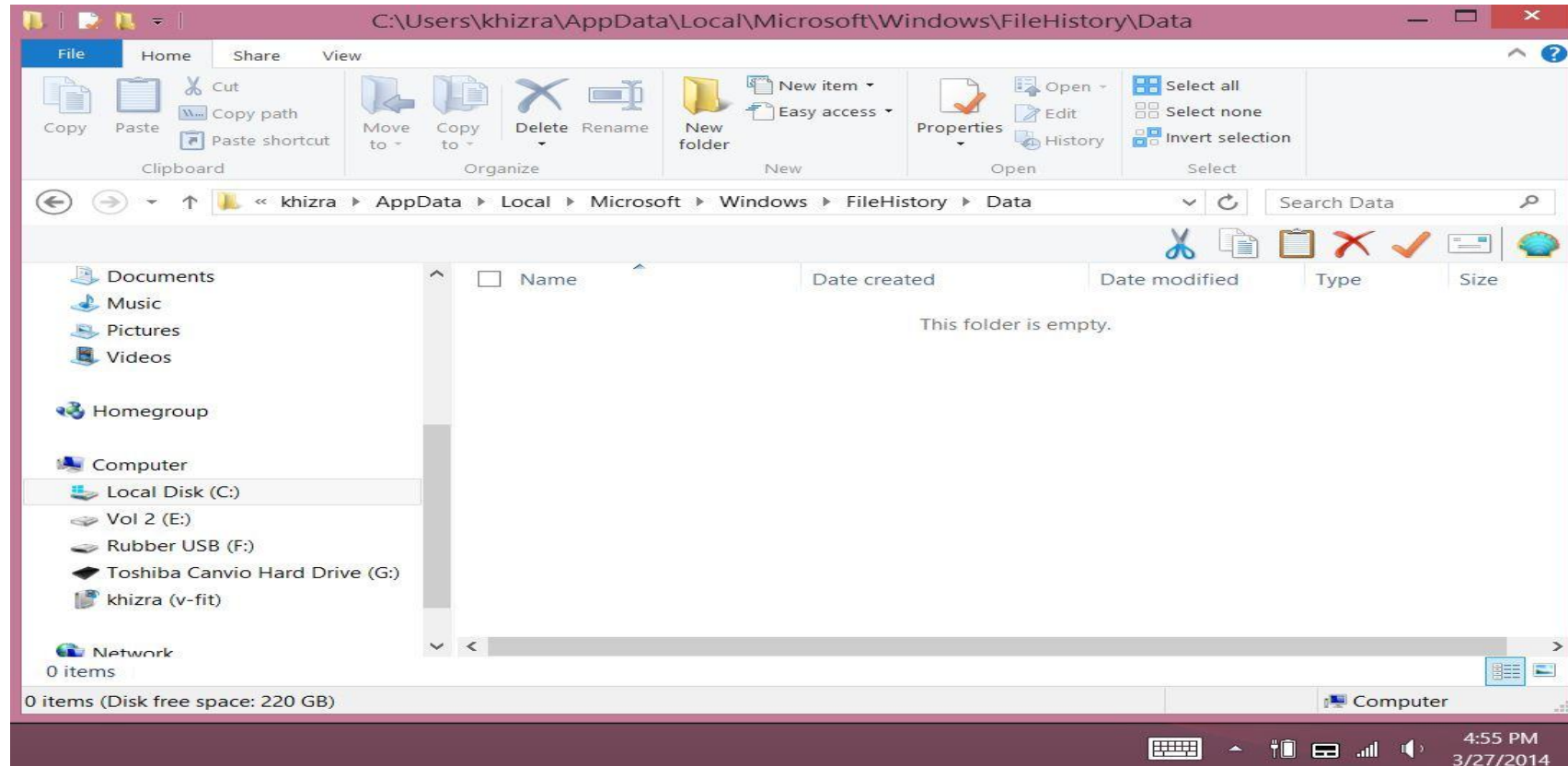
Example contd..

- Some changes done on FHtest.txt at 4:38 p.m.
- New folder 48 is created – at 4:45 p.m.
- Sequence did not break even when no changes were made



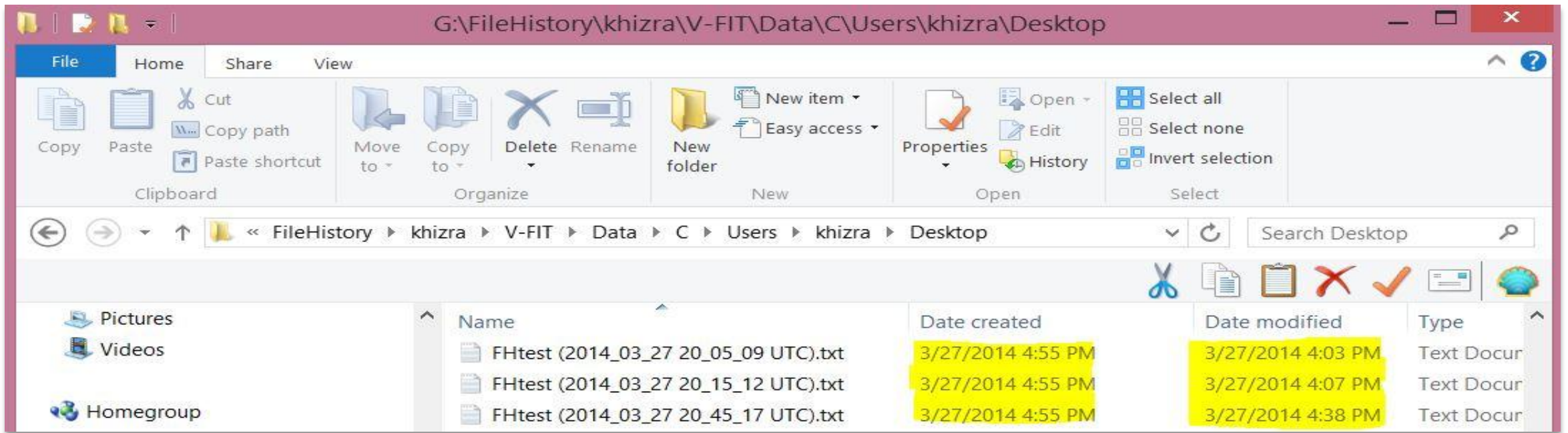
Example contd..

- Now Toshiba (External Drive) is inserted and FH runs at 4:55 p.m. again
- All folders disappeared



Example contd..

- Cache emptied into the external drive
- Notice the Date Modified and Date Created



What was there for backup before?

- Volume Shadow Copy Service (VSS)
- Different underlying working principle - Block level backup

Comparison

Volume Shadow Copy Service

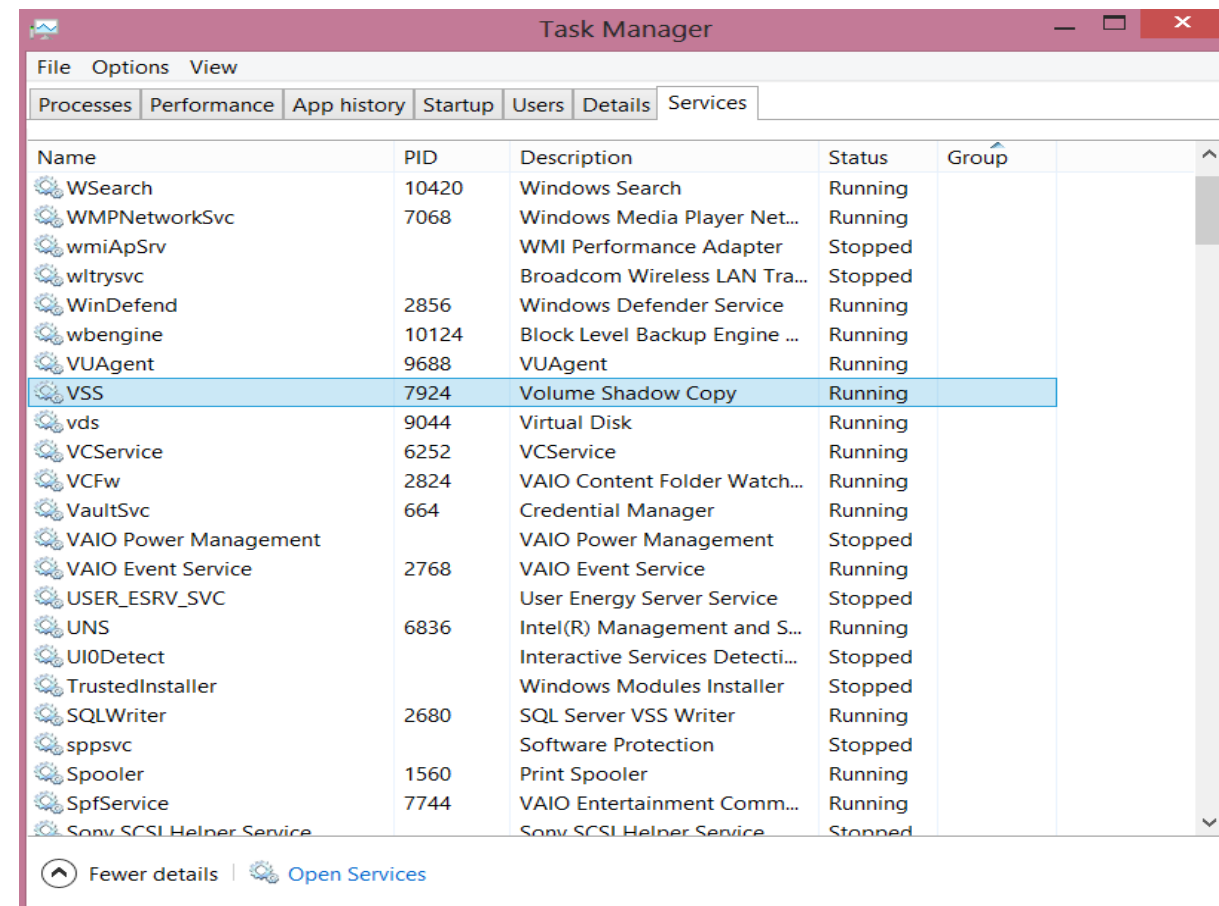
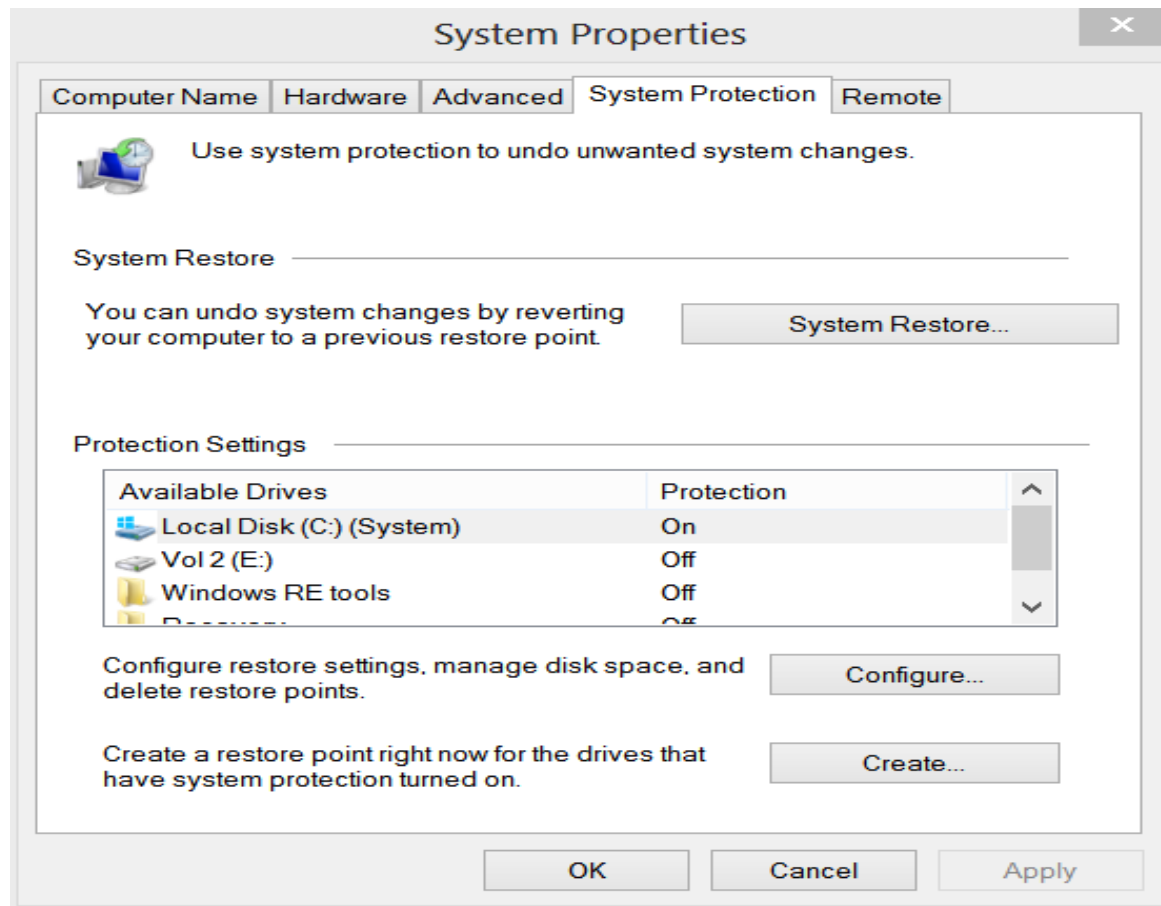
- Block level backup
- No limitation of backing up files/folders on the drive
- Good for recovering system older state — system files
- Takes the snapshot of the entire file-system and saves the modified content only
- Typically saves the copies on local disk
- Does support cloud drives

File History

- File level backup
- Limitation of backing up only files under certain folders i.e. Libraries, Desktop, Contacts and Favorites.
- Good for recovering user files/folders
- Employs USN journal feature of NTFS
- Meant to save the copies on external storage media
- Does not support backing up cloud sync drives (Onedrive exception) e.g. Google drive

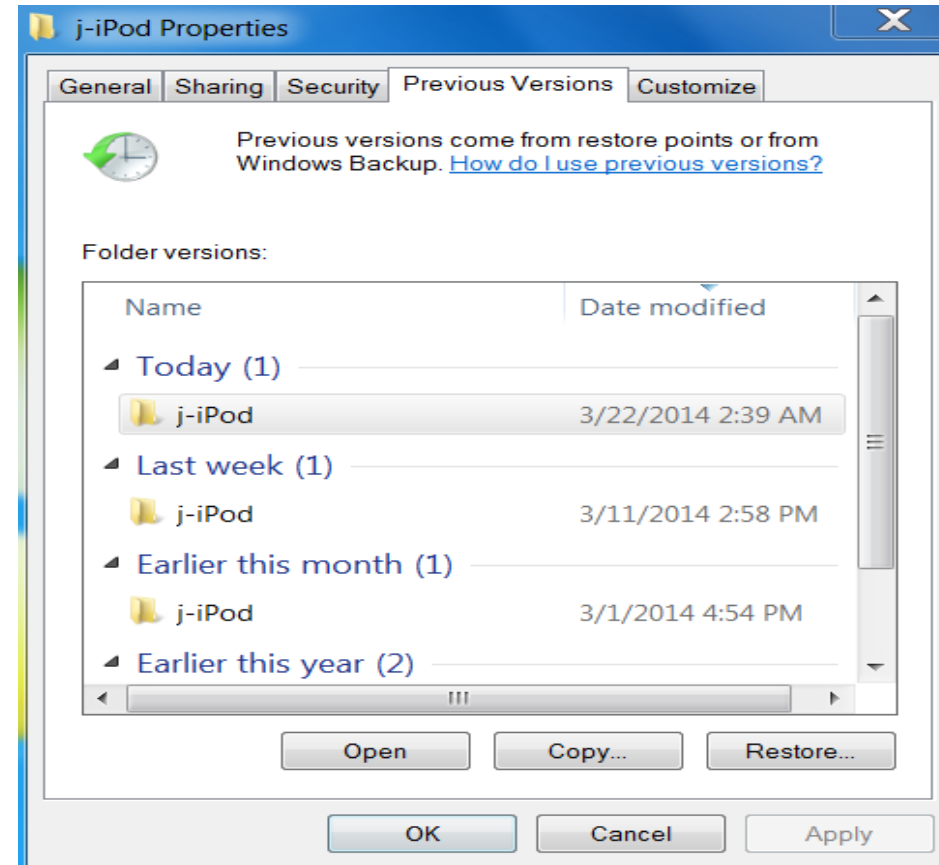
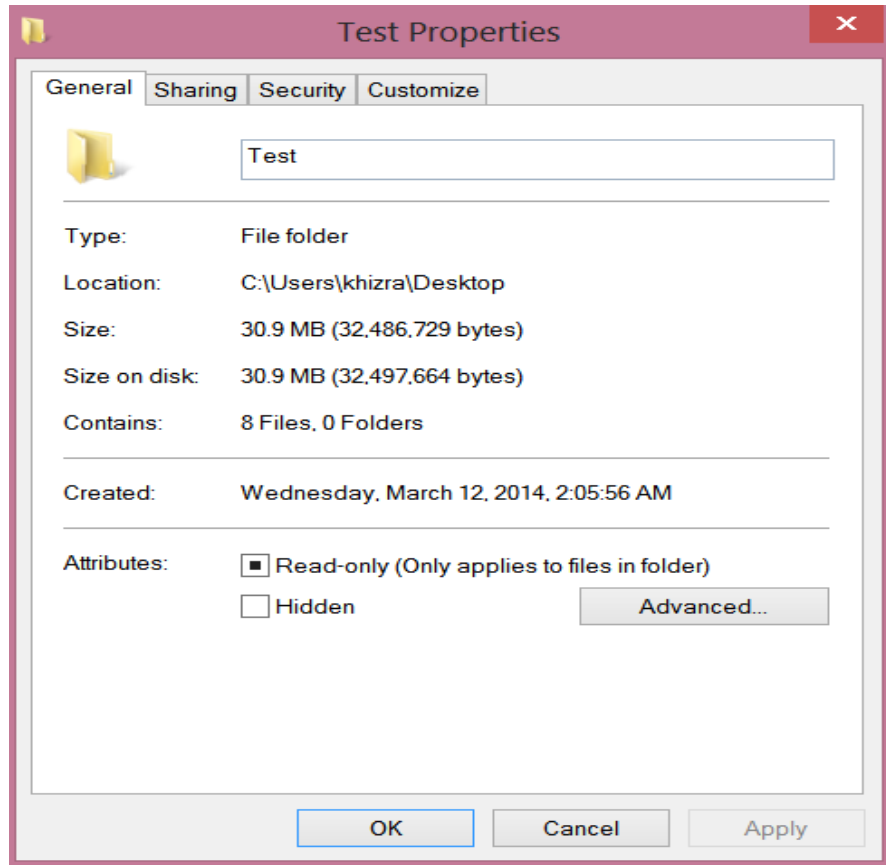
Is VSS gone completely?

No, this service is still running on Windows 8



Why the confusion then?

- The feature to recover the older versions is not there
- But to create restore points and restoring systems, Windows 8 is still using VSS



File History Analysis: Part 2

Forensic analysis

- Config file examination
- Registry examination
- Event log examination
- File History folders/files time stamp

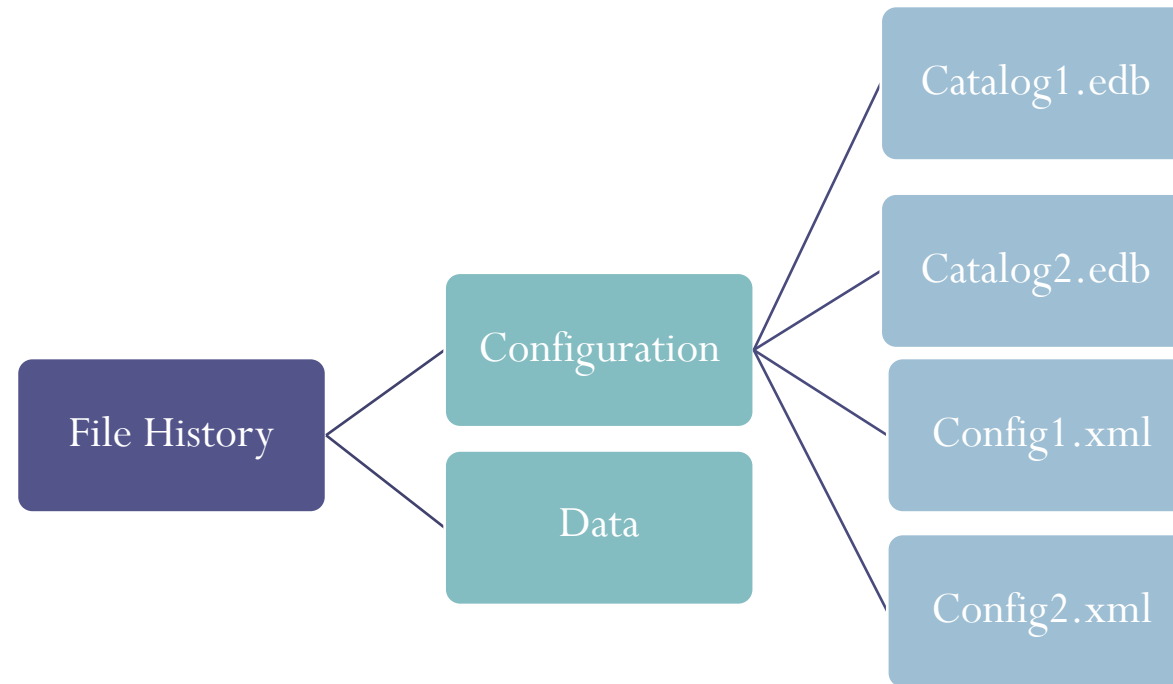
Inquisitive aspect

- When did the FH first run?
- When did the FH last run?
- What is the current state of service - ON/OFF?
- What is the name and type of device used to backup?
- What is the time set for automatic trigger?
- Which folders are excluded?
- What is the retention policy?
- When did the FH last copy files?

When did the File History first run?

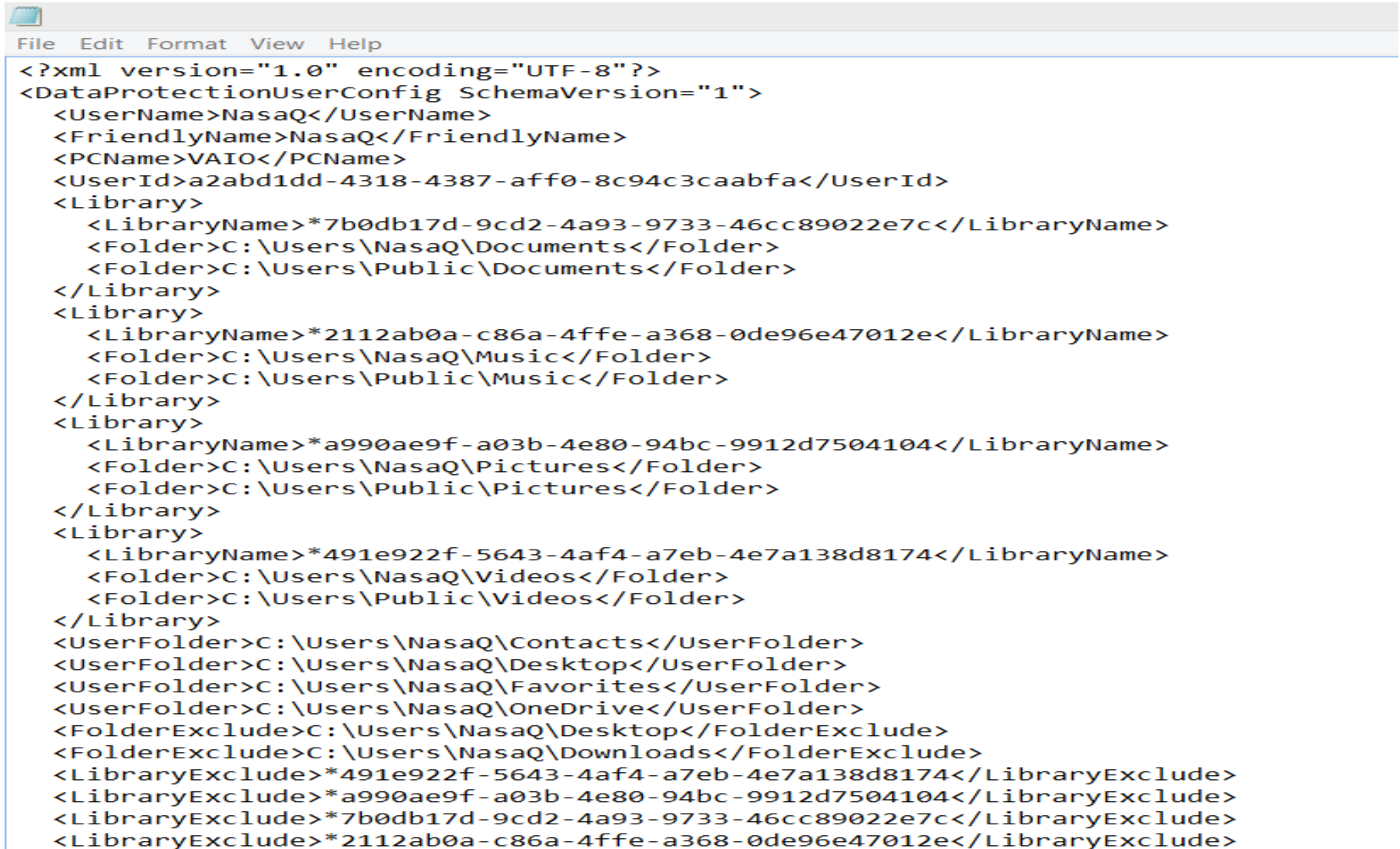
File History files/folders timestamps

C:\Users\Username\AppData\Local\Microsoft\Windows\FileHistory (date created/date modified)



Examination of a sample config file

C:\Users\Username\AppData\Local\Microsoft\Windows\FileHistory\Configuration\Config1.xml

A screenshot of a text editor window displaying an XML file. The window has a menu bar with 'File', 'Edit', 'Format', 'View', and 'Help'. The XML content is as follows:

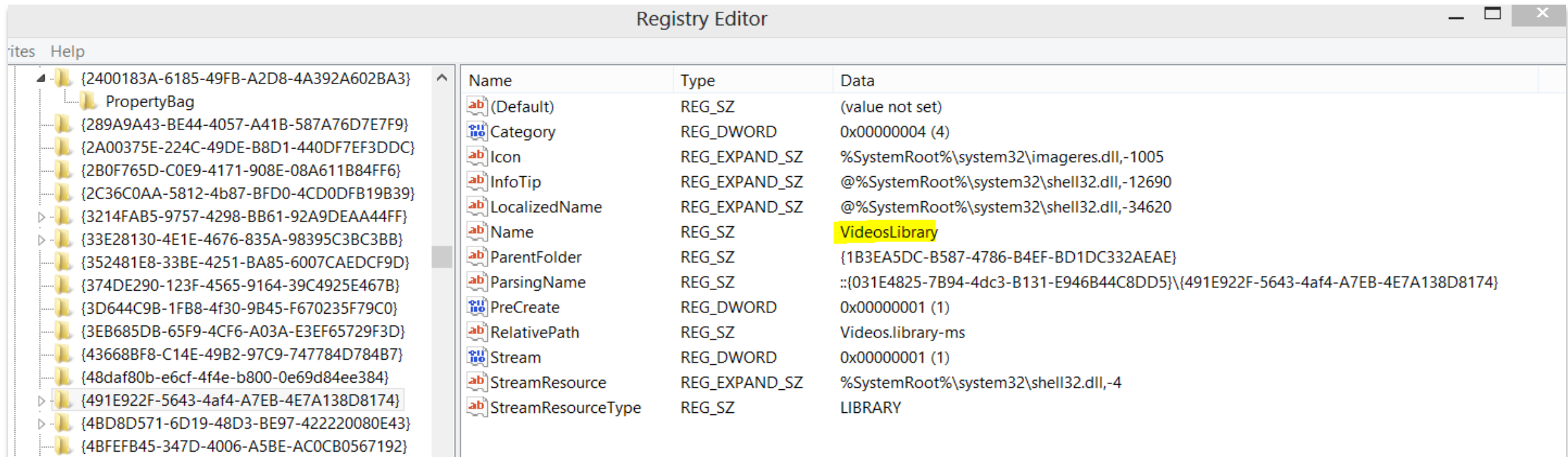
```
<?xml version="1.0" encoding="UTF-8"?>
<DataProtectionUserConfig SchemaVersion="1">
  <UserName>NasaQ</UserName>
  <FriendlyName>NasaQ</FriendlyName>
  <PCName>VAIO</PCName>
  <UserId>a2abd1dd-4318-4387-aff0-8c94c3caabfa</UserId>
  <Library>
    <LibraryName>*7b0db17d-9cd2-4a93-9733-46cc89022e7c</LibraryName>
    <Folder>C:\Users\NasaQ\Documents</Folder>
    <Folder>C:\Users\Public\Documents</Folder>
  </Library>
  <Library>
    <LibraryName>*2112ab0a-c86a-4ffe-a368-0de96e47012e</LibraryName>
    <Folder>C:\Users\NasaQ\Music</Folder>
    <Folder>C:\Users\Public\Music</Folder>
  </Library>
  <Library>
    <LibraryName>*a990ae9f-a03b-4e80-94bc-9912d7504104</LibraryName>
    <Folder>C:\Users\NasaQ\Pictures</Folder>
    <Folder>C:\Users\Public\Pictures</Folder>
  </Library>
  <Library>
    <LibraryName>*491e922f-5643-4af4-a7eb-4e7a138d8174</LibraryName>
    <Folder>C:\Users\NasaQ\Videos</Folder>
    <Folder>C:\Users\Public\Videos</Folder>
  </Library>
  <UserFolder>C:\Users\NasaQ\Contacts</UserFolder>
  <UserFolder>C:\Users\NasaQ\Desktop</UserFolder>
  <UserFolder>C:\Users\NasaQ\Favorites</UserFolder>
  <UserFolder>C:\Users\NasaQ\OneDrive</UserFolder>
  <FolderExclude>C:\Users\NasaQ\Desktop</FolderExclude>
  <FolderExclude>C:\Users\NasaQ\Downloads</FolderExclude>
  <LibraryExclude>*491e922f-5643-4af4-a7eb-4e7a138d8174</LibraryExclude>
  <LibraryExclude>*a990ae9f-a03b-4e80-94bc-9912d7504104</LibraryExclude>
  <LibraryExclude>*7b0db17d-9cd2-4a93-9733-46cc89022e7c</LibraryExclude>
  <LibraryExclude>*2112ab0a-c86a-4ffe-a368-0de96e47012e</LibraryExclude>
```

Which folders are excluded?

- Library (Document, Music, Pictures, Videos), Favorites, Contact, Desktop, Onedrive (Not old Skydrive)
- <FolderExclude>C:\Users\NasaQ\Desktop</FolderExclude>
- <FolderExclude>C:\Users\NasaQ\OneDrive</FolderExclude>
- <FolderExclude>C:\Users\NasaQ\Downloads</FolderExclude>
- <LibraryExclude>*491e922f-5643-4af4-a7eb-4e7a138d8174</LibraryExclude>
- <LibraryExclude>*a990ae9f-a03b-4e80-94bc-9912d7504104</LibraryExclude>
- <LibraryExclude>*7b0db17d-9cd2-4a93-9733-46cc89022e7c</LibraryExclude>

Which folders are excluded? contd..

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{491E922F-5643-4af4-A7EB-4E7A138D8174}



What is the current state of FH service - ON or OFF?

```
- <RetentionPolicies>
    <RetentionPolicyType>DISABLED</RetentionPolicyType>
    <MinimumRetentionAge>12</MinimumRetentionAge>
</RetentionPolicies>
<DPFrequency>3600</DPFrequency>
<DPStatus>ENABLED</DPStatus>
- <Target>
    <TargetName>TOSHIBA EXT</TargetName>
    <TargetUrl>H:\</TargetUrl>
    <TargetVolumePath>\\?\Volume{174bfe69-2583-11e
    <TargetDriveType>FIXED</TargetDriveType>
```

What is the name and type of device used to backup?

```
- <RetentionPolicies>
  <RetentionPolicyType>DISABLED</RetentionPolicyType>
  <MinimumRetentionAge>12</MinimumRetentionAge>
</RetentionPolicies>
<DPFrequency>3600</DPFrequency>
<DPStatus>ENABLED</DPStatus>
- <Target>
  <TargetName>TOSHIBA EXT</TargetName>
  <TargetUrl>H:\</TargetUrl>
  <TargetVolumePath>\\?\Volume{174bfe69-2583-11e
  <TargetDriveType>FIXED</TargetDriveType>
```


What is the time set for automatic trigger?

Frequency of the File History service run. The time is in seconds. By default, the DPFrequency is 3600 (60*60=1 hr)

```
- <RetentionPolicies>
    <RetentionPolicyType>DISABLED</RetentionPolicyType>
    <MinimumRetentionAge>12</MinimumRetentionAge>
</RetentionPolicies>
<DPFrequency>3600</DPFrequency>
<DPStatus>ENABLED</DPStatus>
- <Target>
    <TargetName>TOSHIBA EXT</TargetName>
    <TargetUrl>H:\</TargetUrl>
    <TargetVolumePath>\\?\Volume{174bfe69-2583-11e
    <TargetDriveType>FIXED</TargetDriveType>
```

What is the retention policy?

- By default it is 'Forever' and that means retention policy is disabled.

<RetentionPolicies>

<RetentionPolicyType>DISABLED</RetentionPolicyType>

<MinimumRetentionAge>24</MinimumRetentionAge>

</RetentionPolicies>

months

- If one changes the policy to 1 year, it would reflect on the config file as follows

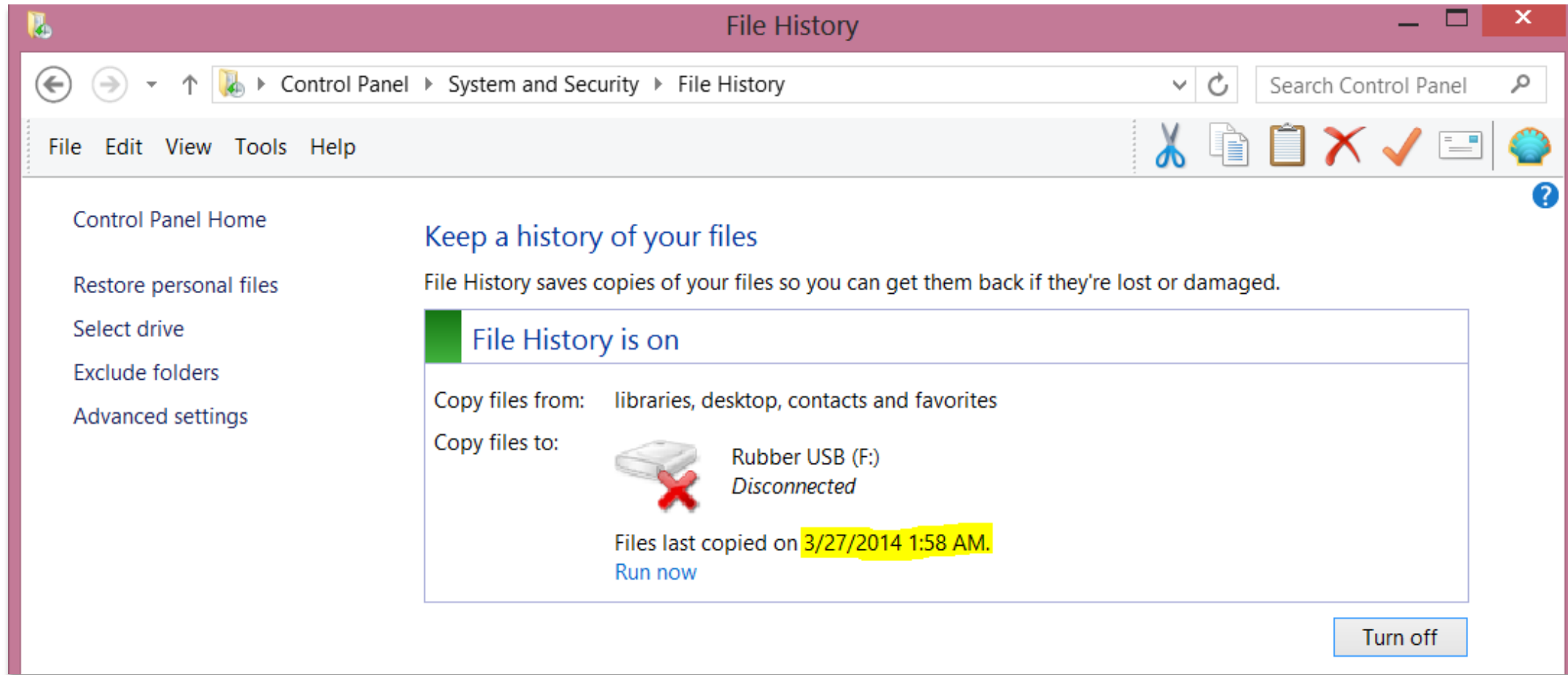
<RetentionPolicies>

<RetentionPolicyType>AGELIMIT</RetentionPolicyType>

<MinimumRetentionAge>12</MinimumRetentionAge>

</RetentionPolicies>

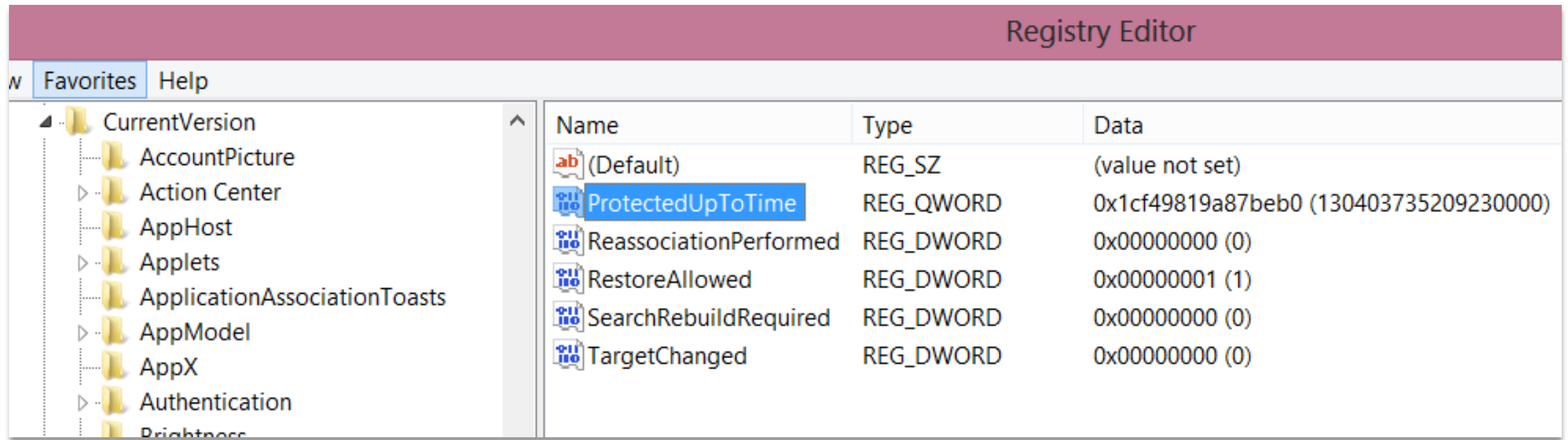
When did the File History last copy files?



When did the File History last copy files? contd..

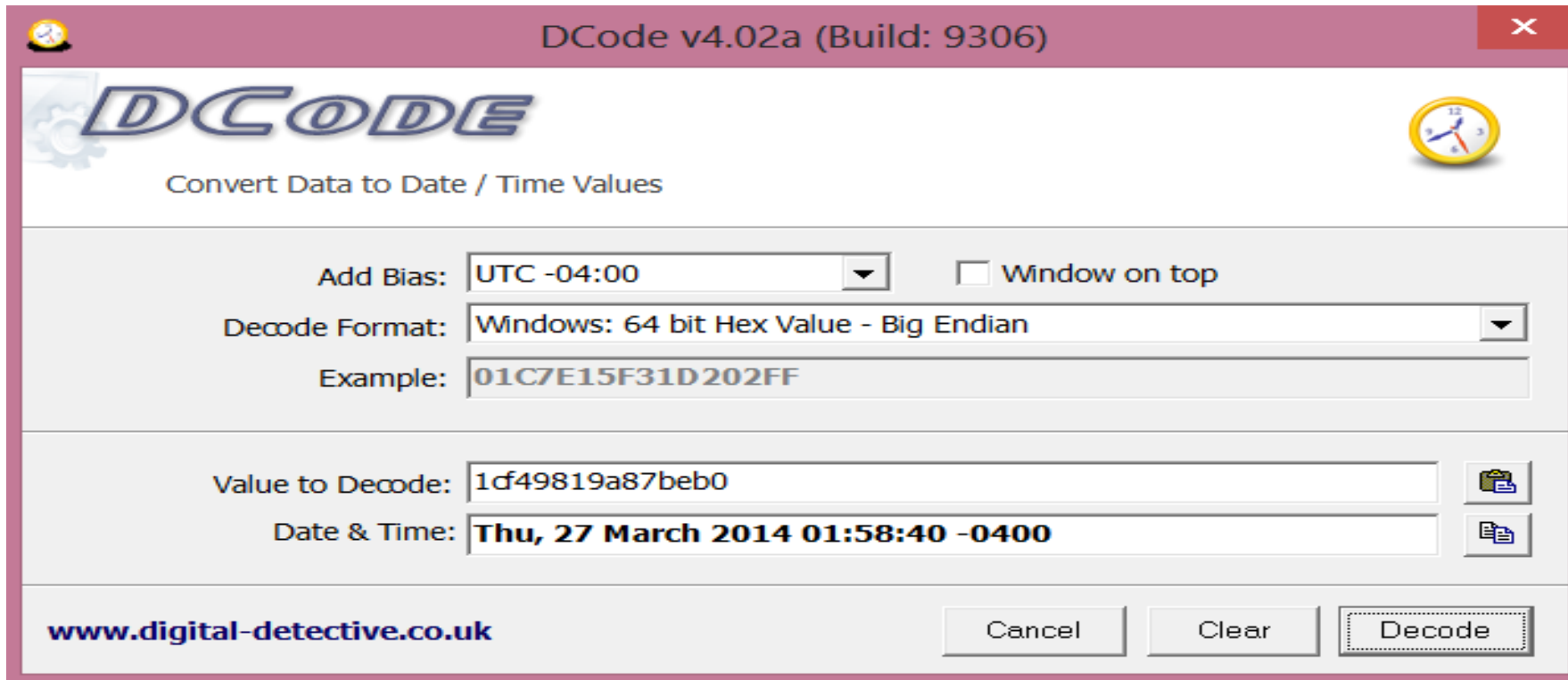
Registry Examination

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\FileHistory



When did the File History last copy files? contd..

Decoding time 64 bit ProtectedUpToTime value



DCode v4.02a (Build: 9306)

DCODE
Convert Data to Date / Time Values

Add Bias: UTC -04:00 ☐ Window on top

Decode Format: Windows: 64 bit Hex Value - Big Endian

Example: 01C7E15F31D202FF

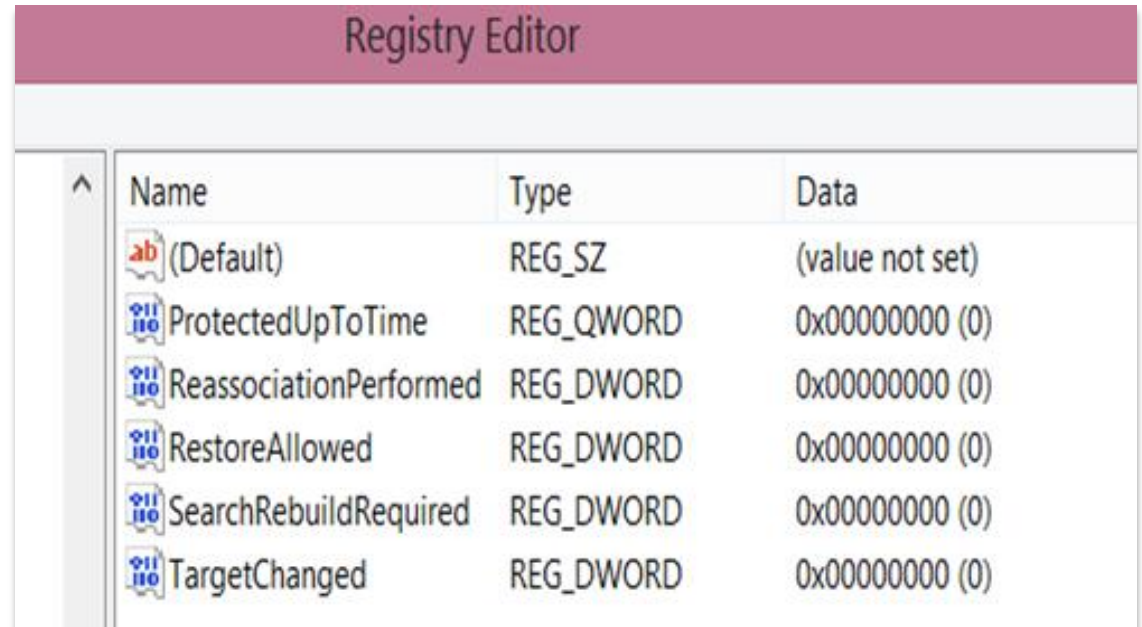
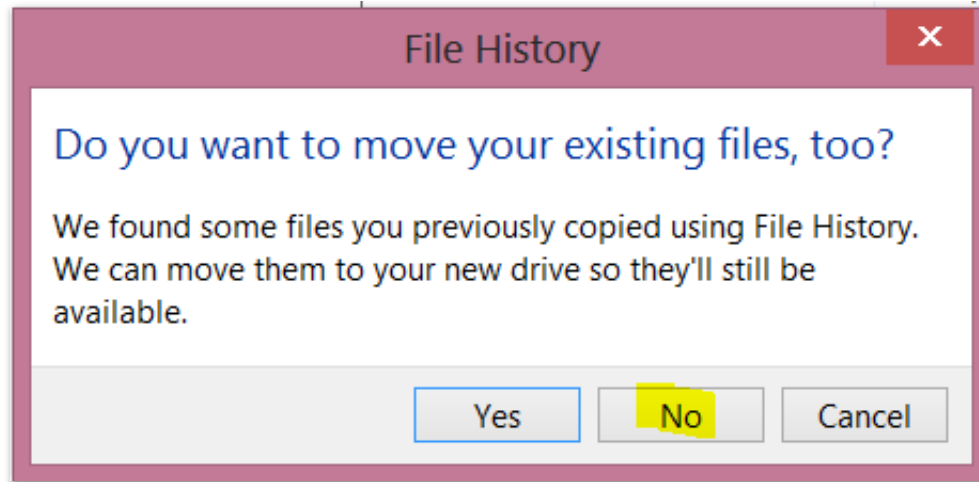
Value to Decode: 1cf49819a87beb0

Date & Time: **Thu, 27 March 2014 01:58:40 -0400**

www.digital-detective.co.uk Cancel Clear Decode

When did the File History last copy files? contd..

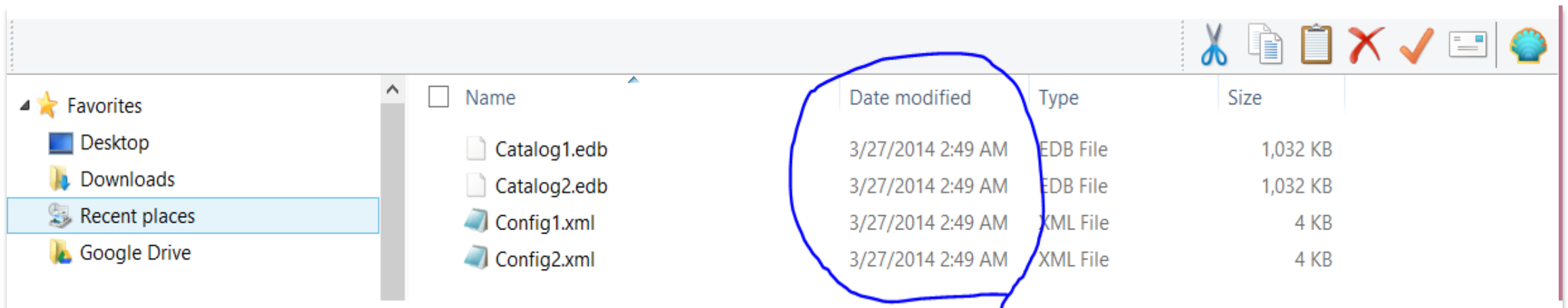
ProtectedUptoTime zeroes out

A Windows Registry Editor window showing a list of registry values. The title bar says "Registry Editor". The table has three columns: "Name", "Type", and "Data". The values listed are (Default), ProtectedUptoTime, ReassociationPerformed, RestoreAllowed, SearchRebuildRequired, and TargetChanged. The "ProtectedUptoTime" value is highlighted in yellow, and its data is "0x00000000 (0)".

Name	Type	Data
(Default)	REG_SZ	(value not set)
ProtectedUptoTime	REG_QWORD	0x00000000 (0)
ReassociationPerformed	REG_DWORD	0x00000000 (0)
RestoreAllowed	REG_DWORD	0x00000000 (0)
SearchRebuildRequired	REG_DWORD	0x00000000 (0)
TargetChanged	REG_DWORD	0x00000000 (0)

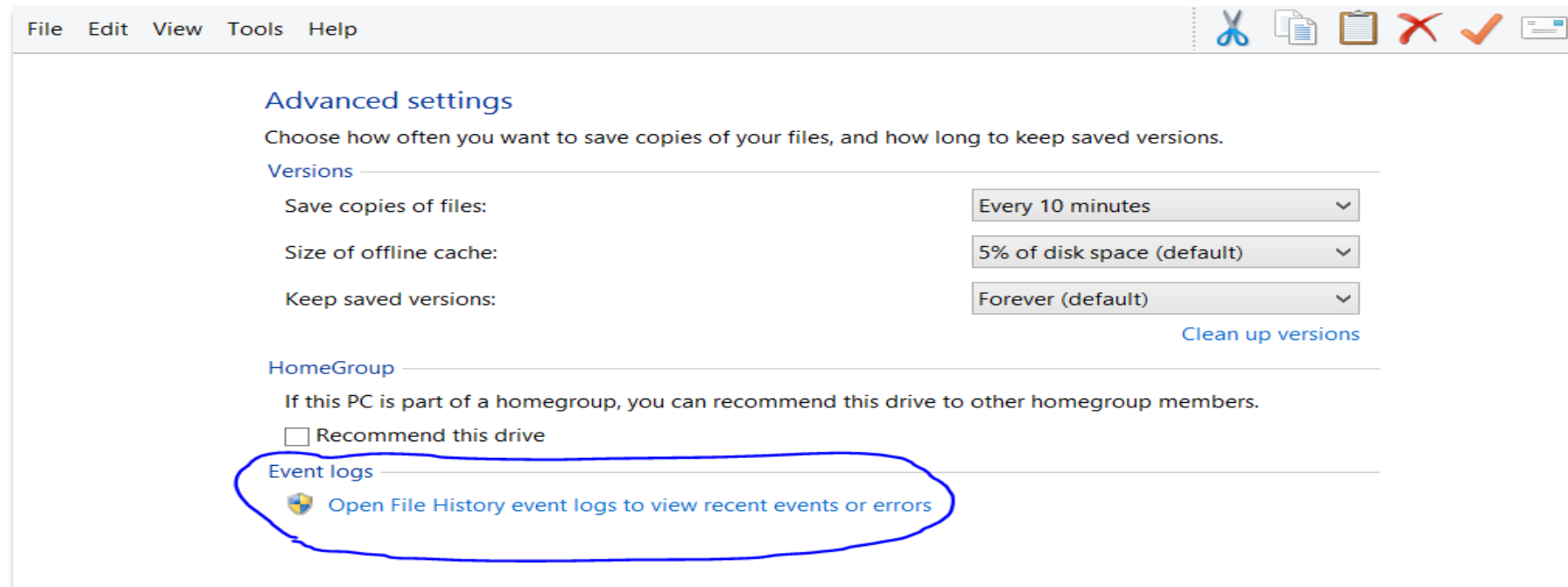
When did the File History last run?

- Case 1: When last copied time = FH last run time
- Case 2: When last copied time \neq FH last run time

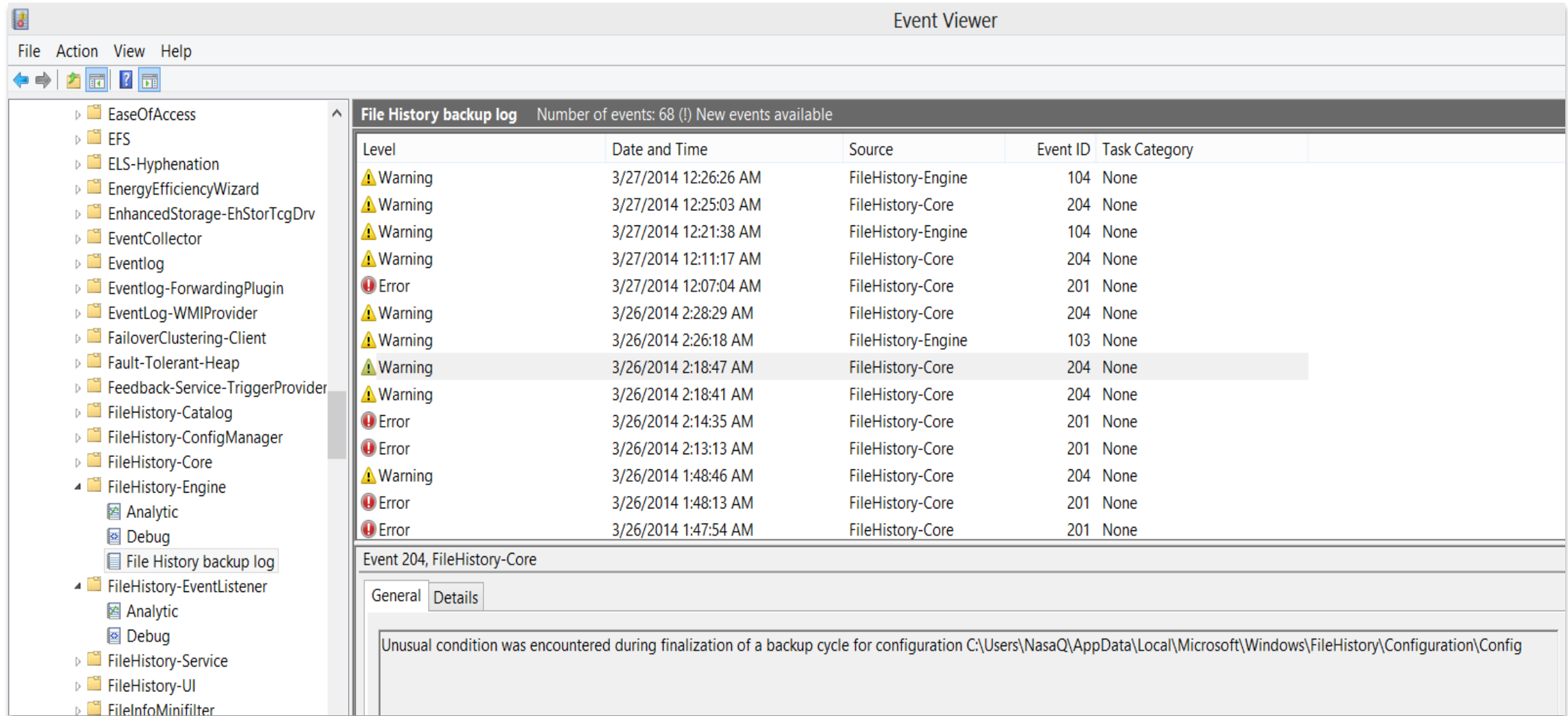


Event log analysis

- Event Viewer OR
- Under Advanced settings



Event log analysis contd..



The screenshot displays the Windows Event Viewer application. The left-hand pane shows a tree view of system logs, with 'FileHistory-Engine' expanded to show 'File History backup log'. The right-hand pane displays a list of events from this log. The events are as follows:

Level	Date and Time	Source	Event ID	Task Category
Warning	3/27/2014 12:26:26 AM	FileHistory-Engine	104	None
Warning	3/27/2014 12:25:03 AM	FileHistory-Core	204	None
Warning	3/27/2014 12:21:38 AM	FileHistory-Engine	104	None
Warning	3/27/2014 12:11:17 AM	FileHistory-Core	204	None
Error	3/27/2014 12:07:04 AM	FileHistory-Core	201	None
Warning	3/26/2014 2:28:29 AM	FileHistory-Core	204	None
Warning	3/26/2014 2:26:18 AM	FileHistory-Engine	103	None
Warning	3/26/2014 2:18:47 AM	FileHistory-Core	204	None
Warning	3/26/2014 2:18:41 AM	FileHistory-Core	204	None
Error	3/26/2014 2:14:35 AM	FileHistory-Core	201	None
Error	3/26/2014 2:13:13 AM	FileHistory-Core	201	None
Warning	3/26/2014 1:48:46 AM	FileHistory-Core	204	None
Error	3/26/2014 1:48:13 AM	FileHistory-Core	201	None
Error	3/26/2014 1:47:54 AM	FileHistory-Core	201	None

The bottom pane shows the details for 'Event 204, FileHistory-Core'. The 'General' tab is selected, displaying the following message:

Unusual condition was encountered during finalization of a backup cycle for configuration C:\Users\NasaQ\AppData\Local\Microsoft\Windows\FileHistory\Configuration\Config

References

- Bright, P. (2012, July 10). *A step back in time with Windows 8's File History*. Retrieved November 20, 2013, from ars technica: <http://arstechnica.com/information-technology/2012/07/a-step-back-in-time-with-windows-8s-file-history/>
- Microsoft. (2013, November 16). *New File History feature*. Retrieved November 17, 2013, from Windows Dev Center-Desktop: [http://msdn.microsoft.com/en-us/library/windows/desktop/hh848055\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/hh848055(v=vs.85).aspx)
- Microsoft. (n.d.). *Set up a drive for File History*. Retrieved November 13, 2013, from Windows: <http://windows.microsoft.com/en-us/windows-8/set-drive-file-history>
- OMeally, Y. (2009, April 21). *Technet Blogs*. Retrieved November 10, 2013, from System Center Configuration Manager Team Blog: <http://blogs.technet.com/b/configmgrteam/archive/2009/04/21/how-configuration-manager-backup-uses-the-volume-shadow-copy-service.aspx>
- Sinofsky, S. (2012, July 10). *MSDN Blogs*. Retrieved November 15, 2013, from Protecting user files with File History: <http://blogs.msdn.com/b/b8/archive/2012/07/10/protecting-user-files-with-file-history.aspx>

The End – Thank you!

Question/Comments?