Tasks on Clyde Barrow Case:

Preparation:
a) Create a new case using EnCase V6, Call it "Windows Artefacts Case"
b) Add Clyde Barrow evidence file "CBARROW.E01" to the case.

Tasks:

1) Locate the Master Boot Record for this evidence file, *Note*: use the disk view using EnCase.

2) Locate the Volume Boot Record and find out the file system type,

3) Do quick google search in order to find the table for NTFS volume boot record structure, DON'T DECODE IT!

4) Locate the NTFS file system files: $MFT, $MFTMirr etc, *Note*: through EnCase table pane.

5) Find and View the $MFT (master file table) records, *Note*: You can view $MFT records by selecting $MFT in the table pane and then by creating a new Text Style (**ISO Latin @1024** bytes i.e. 1024 length). Then you can view the $MFT records properly.

6) Find the record for $LogFile in the $MFT (master file table).

7) List five resident files in the $MFT (master file table) and observe their contents.

   ---

8) Locate and observe the root directory for the user (Clyde)

9) Locate and observe what is inside the folder: C:\Documents and Settings\Clyde\Recent and find link files point to a place outside the C: Drive. Research if you could reason on where are these places?

10) Locate the file called Thumbs.db in the directory C:\Documents and Settings\Clyde\My Documents \My Pictures. In addition view its file structure, *Note: by right click view file structure*, and notice the Money thumbnail file there, try to find this folder!

11) Locate the .SHD and .SPL files:

Note: The Shadow .SHD and Spool files are located under the following directory:

Windows Artefacts\Clyde's HDD\C\WINDOWS\system32\spool\PRINTERS\

A) You can decode the printed documents by selecting the 41 bytes prior to the EMF tag in the .SPL file and then bookmark the selected/highlighted area as Picture Data Type.

Now find the following printed document:

Google Search: explosives Page 1 of 7

Google Groups

Advanced Groups Search Preferences Groups Help

explosives Google Search

Groups search result 2 for explosives

Sponsored Links:

Insults at Laugh.com
Funny & biting insults & comebacks told by professional comics!
laugh.com

Biochemical Warfare
Research biochemical warfare at the world's largest online library.
www.questia.com

Free Database of Ideas
Search and share good ideas $100 Monthly Prize
IdeaExplore.net

From: Brad (Lis1@cris.com) Search Result 2
Subject: The unoffical alt.engr.explosives FAQ
Newsgroups: alt.engr.explosives This is the only article in this thread
Date: 1996/10/06 View: Original Format

OK. I've noticed the requests for basic info and files is on the upswing again, so here is the answer to everything from "What is C4?" to "How do I make nerve gas?"

A Guide to Explosives, Bombs and Chemical Warfare Agents on the World Wide Web
Version .5 Copyright 1996 LIS Publications
Email any comments, additions, or deletion to
lis1@cris.com

Introduction: This FAQ was inspired by the never ending parade of posts on alt.engr.explosives asking for bomb files and where information can be be found on the WWW. Since the only thing more annoying than these questions is the snide attempts at 'witty' answers to them I decided to put together this little file.

B) Find out the website link in which this document was printed. *Note: this is could be found from associated .SHD file.*

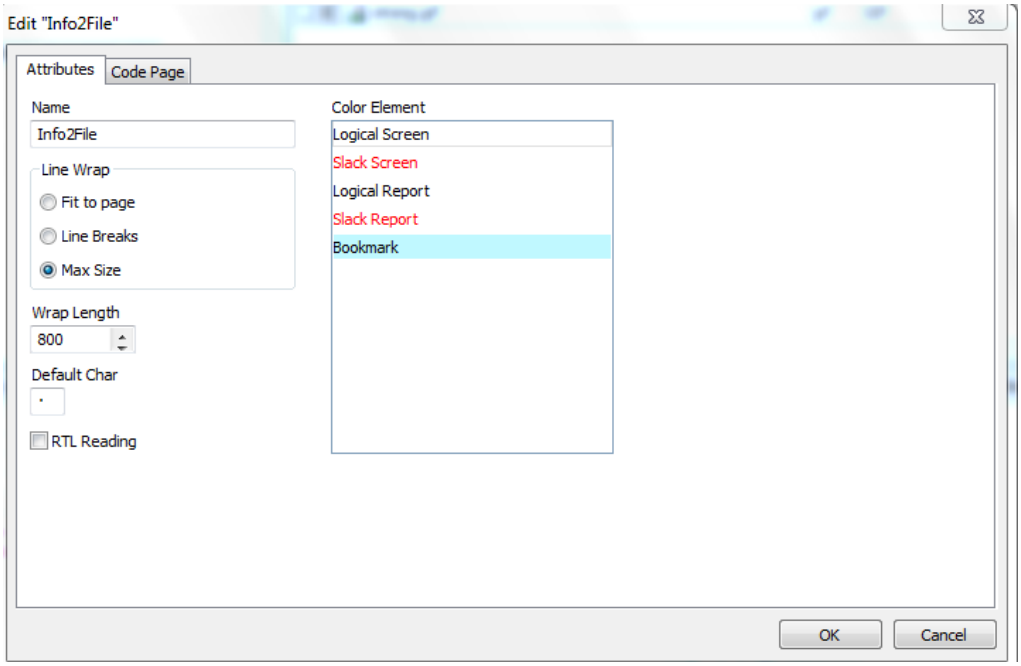
12) Observe the recycle bin folder (Recycler)

A) Find how many users' deleted items?

B) Locate the Money folder in the recycler and then research the image to find a copy of the folder.

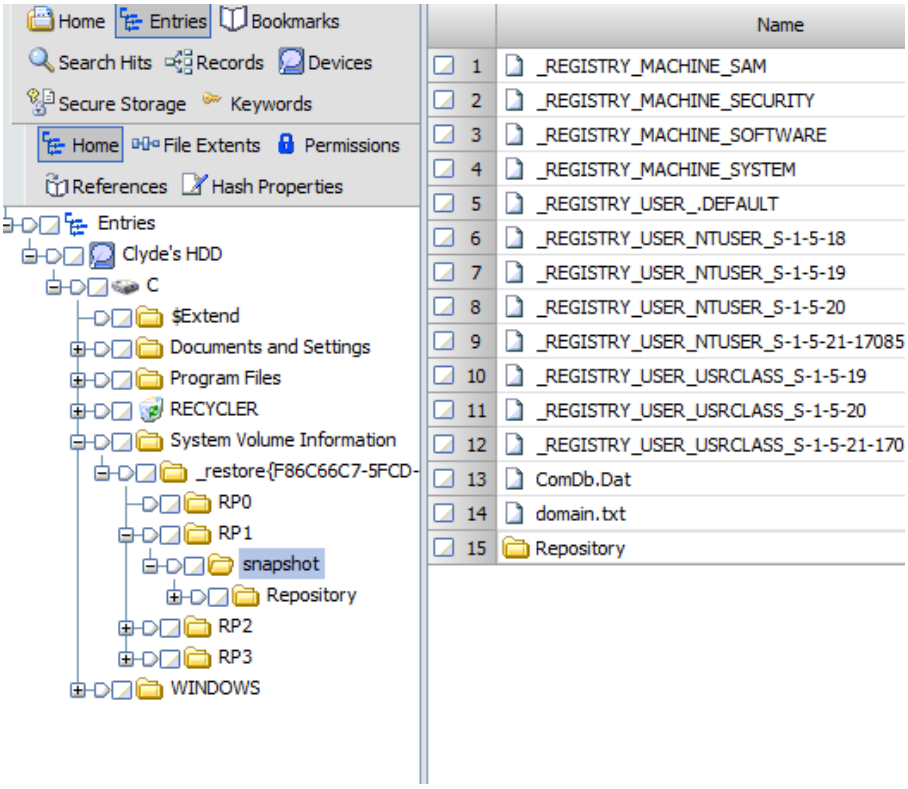
C) Locate the Info2 file in the recycler and

(i) Create a text style to handle 800 bytes record length: by going to Filter Pane > Text Styles tab > Choose ISO Latin Folder and right click on it > Choose new. Name:Info2File@800 and change Wrap length to 800 and in the code page tab choose other radio button and select Western European (Windows) code page. Click Okay

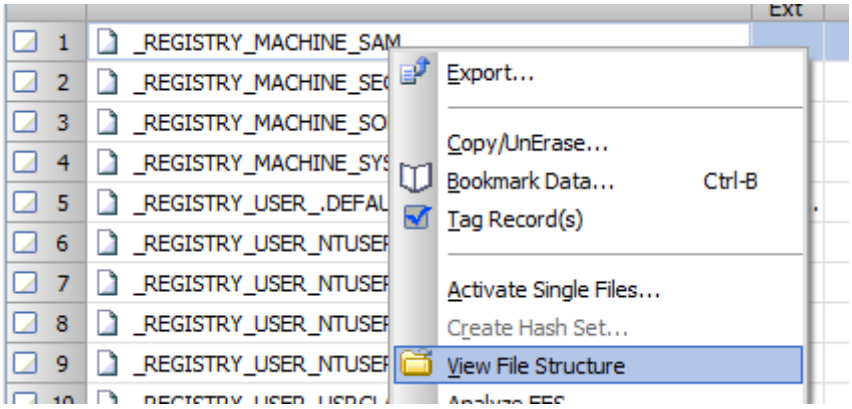


(ii) View the Info2 file using the newly created text style.

13) Observe to the store point directories created as shown in the following figure! *Note: these files can be examined as registry files.*



Note: You view the registry file structure by right click on it and view file structure, DON'T DECODE IT NOW!



14) Locate three compound files in the case thumbs.db, .doc and .zip and view their files structures

A) For thumbs.db explore the images inside.

B) For the zipped file explore the files inside.

C) For the document file explore metadata of the file.

15) Explore the following Registry Hives.

NTUSER.DAT Registry HIV

Note: Can be found under Documents and Settings\Clyde
To view the NTUSER.DAT structure, right click and choose view file structure.

1) View recently used files organized in groups:
   NTUSER.DAT\NTRegistry\$$$PROTO.HIV\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

2) View Types URLs
   NTUSER.DAT\NTRegistry\$$$PROTO.HIV\Software\Microsoft\Internet Explorer\TypedURLs

3) List of applications and filenames of the most recent files opened in windows
   NTUSER.DAT\NTRegistry\$$$PROTO.HIV\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU

4) Most recent saved (or copied) files
   NTUSER.DAT\NTRegistry\$$$PROTO.HIV\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU

Software Registry HIV

Note: Can be found under Windows\system32\config

5) Quick list of installed programs, have a look at Adobe Photoshop 6.0
   Software\NTRegistry\Microsoft\Windows\CurrentVersion\Uninstall

6) Quick list of .EXE files and the path of the executables
   Software\NTRegistry\Microsoft\Windows\CurrentVersion\App Paths

7) Microsoft Windows Installation Information
   Software\Microsoft\WindowsNT\CurrentVersion\

8) Files to run on windows startup
   Software\NTRegistry\Microsoft\Windows\CurrentVersion \Run

System Registry HIV (System)

Note: Can be found under Windows\system32\config

9) Computer name under the System HIV
NTRegistry\$$$PROTO.HIV\System\CurrentControlSet001\Control\ComputerName

10) Last shutdown time
NTRegistry\$$$PROTO.HIV\System\CurrentControlSet001\Control\Windows\ShutDownTime
Select 8 bytes and book mark > choose Windows Dates and Time.

11) View mounted devices
NTRegistry\$$$PROTO.HIV\System\MountedDevices\

Or
NTRegistry\$$$PROTO.HIV\System\CurrentControlSet\Enum\USBSTORE\

16) Going back to Documents and Settings \Clyde\Recent\ , You have investigated previously, bookmark the following recently opened file. D:\Secret\Good Stuff\Keepers\0uro_difate004.jpg

17) Locate the partition table in the MBR (master boot record) and decode it using EnCase. **Note: by selecting/highlighting 64 byes backward starting from the byte before the bytes 55 AA "signature" and then right click on selected bytes and bookmark data > choose windows > partition entry**
   A) Find the volumes types.
   B) Find Volume Boot Record positions.
   C) Find the starting CHS (Cylinder, Head, Sector) Addresses.

18) Create and search for the following two keywords: (MSDOS5.1 and MSWIN4.1).
   A) Select the two keywords and perform keywords search.
   B) Bookmark your findings related volume boot records.

19) Locate the volume slack entry under the NTFS mounted volume in EnCase and find the backup Volume Boot Record (VBR) for the first volume. *Note: by going directly to the disk view while selecting the volume slack entry.*

20) Locate the Extended Partition Sector. *Note: is the next sector after the backup VBR.*
    A) Decode the partition table.
    B) Find out the file system type of the deleted/hidden partition.
    C) Find out the starting CHS.
    D) Find out the relative starting sector.
21) Locate the VBR for the discovered partition and right click on it and choose add partition.

22) Navigate the discovered partition to discover more evidence.

End of Lab