



INVESTIGATING WINDOWS ENVIRONMENT---PART 2

CONDUCTING A WINDOWS INVESTIGATION.

- Review all pertinent logs.
- **Perform keyword searches.**
- Review relevant files.
- Identify unauthorized user accounts or groups.
- Identify rogue processes and services.
- Look for unusual or hidden files/directories.
- Check for unauthorized access points.
- Examine jobs run by the Scheduler service.
- Analyze trust relationships.
- Review security identifiers.



PERFORM KEYWORD SEARCHES

- **String searches** can be conducted on the logical file structure or at the physical level to examine the contents of an entire drive
- disk-search tools perform physical-level string search of the drive.
- These tools require that you boot the target system from a controlled boot floppy or other media

TOOLS

- **DtSearch**
- **EnCase**
(Both supports physical level string search)



THINGS TO FOCUS

- You must pick the exact words that provide useful results.
- your string search should not adequately minimize the focus of your investigation.

CONDUCTING A WINDOWS INVESTIGATION.

- Review all pertinent logs.
- Perform keyword searches.
- **Review relevant files.**
- Identify unauthorized user accounts or groups.
- Identify rogue processes and services.
- Look for unusual or hidden files/directories.
- Check for unauthorized access points.
- Examine jobs run by the Scheduler service.
- Analyze trust relationships.
- Review security identifiers.



REVIEW RELEVANT FILES

IDEA

Windows systems write input and output to so many files at a time that almost all actions taken on the system leave some trace of their occurrence

SOURCES

Temp files

cache files,

a Registry that keeps track of recently used files,

a Recycle Bin, maintains deleted files



WHAT TO DO

- It is important to recognize files by their extensions as well as by their true file headers
- .doc, .tmp, .log, .txt, .wpd, .gif, .exe and .jpg extensions should be known.

TOOLS

EnCase provides viewing capability for many file types.

Quickview Plus (fileviewer)



The goal for an investigator is to know which files might be relevant to the current incident

DIFFERENT TYPE OF FILES ARE DEALT DIFFERENTLY



1. INCIDENT TIME AND TIME/DATE STAMPS

- You will need to scour **network-based logs** or use oral testimony to identify a range of time when an incident must have occurred.
- “action days”—days when relevant activities took place.
- Once you identify these active, relevant timeframes, you can review the time/date stamps encapsulated within those timeframes.
- Another way is to use **the dir** command to get a directory listing that includes file access, modification, and creation times.
- Tool lists all directories and files, along with last access time, modified time, and creation time.

TOOL
USED

FileList

2. PROPRIETARY EMAIL FILES

- common email clients—Outlook, Netscape Messenger, and AOL

IDEA

- you must use the appropriate client software to view the suspect's email



NETSCAPE MESSENGER MAIL

- Netscape maintains mail messages in a plain text file.
Path to find netscape
- *\Program Files\Netscape\Users\<User Account>\Mail.*
- Each Netscape mailbox supports :
index file (extension .snm)
message-text file (no extension)

Each mail folder stored as a file either as :

INBOX: stores inbox files

SENT: stores sent messages

- To view the contents of these files, open the files in WordPad or any other text editor.



MICROSOFT OUTLOOK MAIL

- maintains mail messages in a proprietary format
- Outlook files on Windows 2000 path
- *Settings \ <User Account> \ Local Settings \ Application Data \ Microsoft \ Outlook directories.*
- *File extension *.pst(personal folder files)*
- The *.pst files can **archive** all folders within Outlook—the Calendar, Deleted Items, Drafts, Inbox, Journal, Notes, Outbox, Sent Items, and Tasks—**except the Contacts folder.**
- To view another system's .pst files
copy them to your forensic workstation and then open the files using the Outlook Client



3.DELETED FILES AND DATA

- **PURPOSE**

recovery of lost files that might have been deleted by malicious users to cause damage

Different ways to recover

- Using undelete tools
- Restoring files located in the Recycle Bin
- Recovering .tmp files
- Using low-level tools to repair the file system



3.USING UNDELETE TOOLS

- undelete utilities require the use of the native operating system, and they will restore the files in place.
- Unfavourable practice as you are overwriting unallocated space that may contain valuable info.

TOOLS USED

File Scavenger :undelete files as long as the space they occupy on the hard drive has not been used by more recent I/O storage.

Norton Utilities Protect:acts as a replacement for the Recycle Bin
protect all deleted files, including files deleted under a command prompt, and to automatically delete them after a specified number of days.



4.RECYCLE BIN

- prevents accidental deletion of files
- Captures only files deleted from Windows Explorer and other Recycle Bin–aware apps.
- Command-line deletions and files deleted on a shared network drive **do not** get stored in RB.

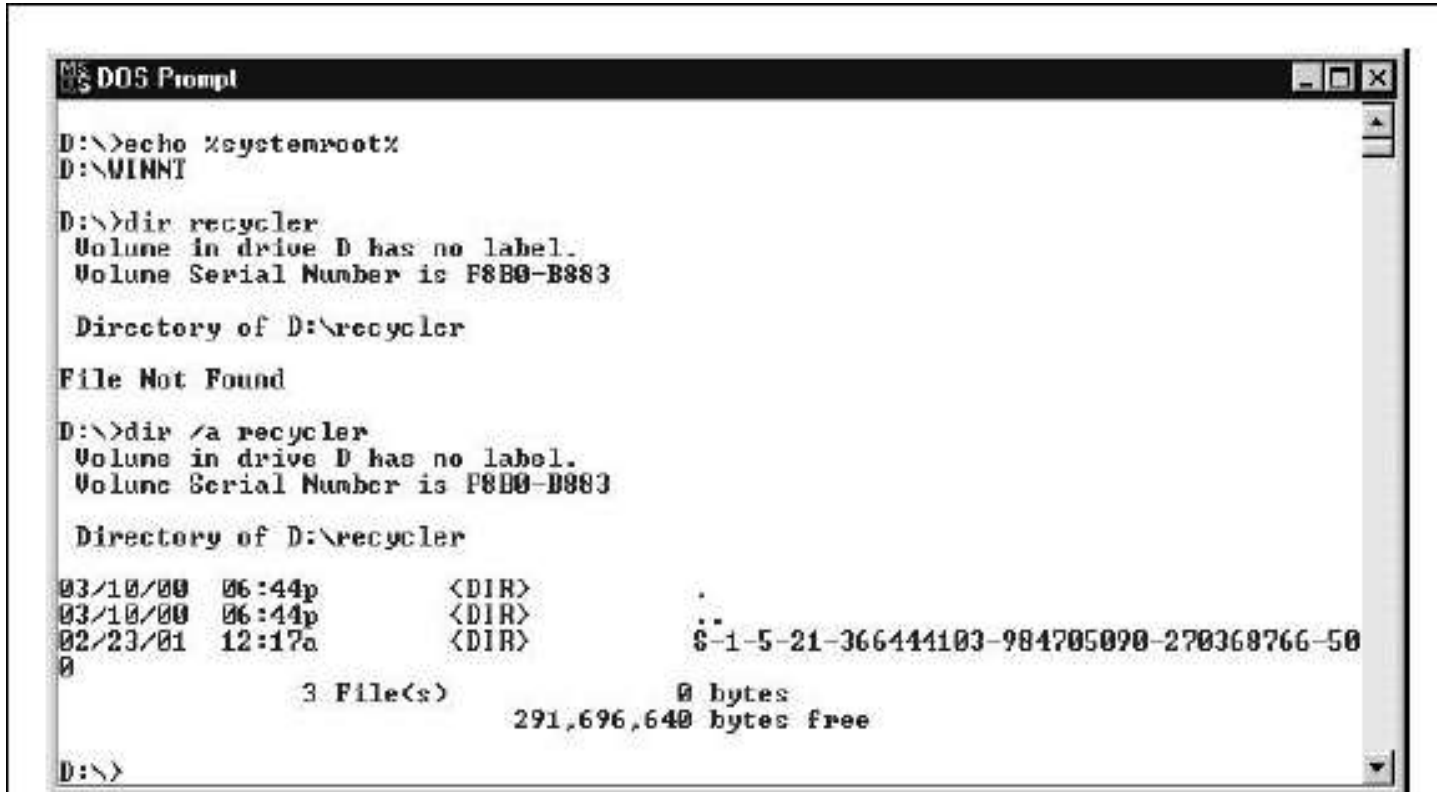


PROCESS OF RESTORING FILES FROM RECYCLE BIN

1. find the hidden Recycle Bin directories.
2. You can find the contents of the RecycleBin by going to the **root directory of a partition (drive letter,/a)**
3. change directories into the hidden RECYCLER directory.



- dir command requires the /a extension to list the hidden RECYCLER directory.
- Dir allows us to view all subdirectories.



```
DOS Prompt
D:\>echo %systemroot%
D:\WINNT

D:\>dir recycler
Volume in drive D has no label.
Volume Serial Number is F8B0-B883

Directory of D:\recycler

File Not Found

D:\>dir /a recycler
Volume in drive D has no label.
Volume Serial Number is F8B0-B883

Directory of D:\recycler

03/10/00  06:44p      <DIR>      .
03/10/00  06:44p      <DIR>      ..
02/23/01  12:17a      <DIR>      $-1-5-21-366444103-984705090-270368766-50
0

          3 File(s)              0 bytes
          291,696,640 bytes free

D:\>
```

Figure 12-4. Viewing the contents of the RECYCLER directory

5.TEMPORARY FILES

- the files which may originate with any of the activity undergoing windows like creation ,deletion ,moving of a file in/from a system.
- ***File extension *.tmp***
- These files recovery may reveal year-old documents that were deleted, old PowerPoint presentations,and files that were received as attachments.



6.BACKUP FILE RECOVERY

- The evidence that is **missing** from the system you are investigating may be found in any of the backup tapes.

TOOLS USED:

Windows NT's NTBACKUP.EXE

creates a log file recording the

- ❖ date of the backup
- ❖ how many files were backed up
- ❖ how many files were skipped during the backup process,
- ❖ how many errors were recorded
- ❖ how long the backup took to finish.

PROCESS

search for BACKUP.LOG, or simply *.log, and determine whether it was created by NTBACKUP.

