sansforensics@siftworkstation: ~/Downloads/Task\_1

$ md5sum EvidenceA.zip

5f561b7e7a009286c55516f5d2914fe6 EvidenceA.zip

sansforensics@siftworkstation: ~/Downloads/Task\_1

$ cat EvidenceA.001 EvidenceA.002 EvidenceA.003 EvidenceA.004 EvidenceA.005 EvidenceA.006 EvidenceA.007 EvidenceA.008 EvidenceA.009 EvidenceA.010 EvidenceA.011 EvidenceA.012 EvidenceA.013 EvidenceA.014 > boathouse.dd

sansforensics@siftworkstation: ~/Downloads/Task\_1

$ img\_stat boathouse.dd

IMAGE FILE INFORMATION

--------------------------------------------

Image Type: raw

Size in bytes: 14155776000

Sector size: 512

sansforensics@siftworkstation: ~/Downloads/Task\_1

$ mmls boathouse.dd

$ fsstat -o 56 boathouse.dd

sansforensics@siftworkstation: ~/Downloads/Task\_1

$ fsstat -o 56 boathouse.dd

FILE SYSTEM INFORMATION

--------------------------------------------

File System Type: NTFS

Volume Serial Number: 84005C50005C4B76

OEM Name: NTFS

Version: Windows XP

METADATA INFORMATION

--------------------------------------------

First Cluster of MFT: 786432

First Cluster of MFT Mirror: 2620376

Size of MFT Entries: 1024 bytes

Size of Index Records: 4096 bytes

Range: 0 - 13456

Root Directory: 5

CONTENT INFORMATION

--------------------------------------------

Sector Size: 512

Cluster Size: 4096

Total Cluster Range: 0 - 5240751

Total Range in Image: 0 - 3455992

Total Sector Range: 0 - 41926022

$AttrDef Attribute Values:

$STANDARD\_INFORMATION (16) Size: 48-72 Flags: Resident

$ATTRIBUTE\_LIST (32) Size: No Limit Flags: Non-resident

$FILE\_NAME (48) Size: 68-578 Flags: Resident,Index

$OBJECT\_ID (64) Size: 0-256 Flags: Resident

$SECURITY\_DESCRIPTOR (80) Size: No Limit Flags: Non-resident

$VOLUME\_NAME (96) Size: 2-256 Flags: Resident

$VOLUME\_INFORMATION (112) Size: 12-12 Flags: Resident

$DATA (128) Size: No Limit Flags:

$INDEX\_ROOT (144) Size: No Limit Flags: Resident

$INDEX\_ALLOCATION (160) Size: No Limit Flags: Non-resident

$BITMAP (176) Size: No Limit Flags: Non-resident

$REPARSE\_POINT (192) Size: 0-16384 Flags: Non-resident

$EA\_INFORMATION (208) Size: 8-8 Flags: Resident

$EA (224) Size: 0-65536 Flags:

$LOGGED\_UTILITY\_STREAM (256) Size: 0-65536 Flags: Non-resident

sansforensics@siftworkstation: ~/Downloads/Task\_1

$ sudo mount -o ro,loop,offset=28672 boathouse.dd /mnt/windows\_mount

sansforensics@siftworkstation: /mnt/windows\_mount

$ rip.pl -r /mnt/windows\_mount/WINDOWS/system32/config/software -p winver

Launching winver v.20200525

winver v.20200525

(Software) Get Windows version & build info

ProductName Microsoft Windows XP

CSDVersion Service Pack 3

BuildLab 2600.xpsp.080413-2111

RegisteredOrganization

RegisteredOwner Jim

InstallDate 2022-08-27 12:13:00Z

sansforensics@siftworkstation: /mnt/windows\_mount

sansforensics@siftworkstation: /mnt/windows\_mount

$ cd Program\ Files/

sansforensics@siftworkstation: /mnt/windows\_mount/Program Files

$ ls

7-Zip 'ComPlus Applications' Messenger 'Mozilla Firefox' 'MSN Gaming Zone' 'Outlook Express' VMware WindowsUpdate

Adobe 'Internet Explorer' 'microsoft frontpage' 'Mozilla Maintenance Service' NetMeeting 'Uninstall Information' 'Windows Media Player' xerox

'Common Files' IrfanView 'Movie Maker' MSN 'Online Services' VideoLAN 'Windows NT'

sansforensics@siftworkstation: /mnt/windows\_mount/Program Files

sansforensics@siftworkstation: /mnt/windows\_mount/RECYCLER

$ cd S-1-5-21-790525478-1220945662-725345543-1003/

sansforensics@siftworkstation: /mnt/windows\_mount/RECYCLER/S-1-5-21-790525478-1220945662-725345543-1003

$ ls -al

total 257

drwxrwxrwx 1 root root 0 Aug 28 05:20 .

drwxrwxrwx 1 root root 0 Aug 28 05:20 ..

-rwxrwxrwx 1 root root 176 Aug 20 09:24 Dc1.txt

-rwxrwxrwx 1 root root 256110 Aug 20 08:12 Dc2.zip

-rwxrwxrwx 1 root root 65 Aug 28 05:20 desktop.ini

-rwxrwxrwx 1 root root 1620 Aug 28 05:29 INFO2

sansforensics@siftworkstation: /mnt/windows\_mount/RECYCLER/S-1-5-21-790525478-1220945662-725345543-1003

Following clues in the Recycler using information in INFO2 note1.txt and note2.txt was found in “Documents and Settings/Jim/My Documents”

sansforensics@siftworkstation: /mnt/windows\_mount/Documents and Settings/Jim/My Documents

$ cat note1.txt

If I let you know where I??m going, I won??t be on holiday

sansforensics@siftworkstation: /mnt/windows\_mount/Documents and Settings/Jim/My Documents

$ cat note2.txt

Desperate times, desperate measures.

sansforensics@siftworkstation: /mnt/windows\_mount/Documents and Settings/Jim/My Documents

sansforensics@siftworkstation: /mnt/windows\_mount

$ grep -ir "NTUSER.DAT" /mnt/windows\_mount

/mnt/windows\_mount/Documents and Settings/Administrator/Local Settings/Temp/vminst.log:2022-08-27 22:15:35| tools-build-4448491| HUWin32LoadUserProfile: Calling load hive HKEY\_USERS Default User - C:\Documents and Settings\Default User\ntuser.dat

Binary file /mnt/windows\_mount/Documents and Settings/Administrator/Local Settings/Temp/vmware-Administrator/000021be/setup.exe matches

Binary file /mnt/windows\_mount/Documents and Settings/Administrator/Local Settings/Temp/vmware-Administrator/000021be/setup64.exe matches

Binary file /mnt/windows\_mount/Documents and Settings/Administrator/Local Settings/Temp/{FC5F4DCF-B54A-435E-8B0D-737BB373ED69}~setup/VMware Tools.msi matches

Binary file /mnt/windows\_mount/System Volume Information/\_restore{731BCC79-6ED7-45BA-85C2-36CEA956508F}/RP2/A0000023.msi matches

Binary file /mnt/windows\_mount/WINDOWS/system32/access.cpl matches

Binary file /mnt/windows\_mount/WINDOWS/system32/dllcache/access.cpl matches

Binary file /mnt/windows\_mount/WINDOWS/system32/dllcache/migisma.dll matches

Binary file /mnt/windows\_mount/WINDOWS/system32/dllcache/cplexe.exe matches

Binary file /mnt/windows\_mount/WINDOWS/system32/dllcache/imjp81.ime matches

Binary file /mnt/windows\_mount/WINDOWS/system32/dllcache/imjp81k.dll matches

Binary file /mnt/windows\_mount/WINDOWS/system32/dllcache/imjpcic.dll matches

Binary file /mnt/windows\_mount/WINDOWS/system32/dllcache/imjpcus.dll matches

Binary file /mnt/windows\_mount/WINDOWS/system32/dllcache/imjpdct.dll matches

Binary file /mnt/windows\_mount/WINDOWS/system32/dllcache/imjpdsvr.exe matches

Binary file /mnt/windows\_mount/WINDOWS/system32/dllcache/imjpmig.exe matches

Binary file /mnt/windows\_mount/WINDOWS/system32/dllcache/imjprw.exe matches

Binary file /mnt/windows\_mount/WINDOWS/system32/dllcache/imjputy.exe matches

Binary file /mnt/windows\_mount/WINDOWS/system32/dllcache/imjputyc.dll matches

Binary file /mnt/windows\_mount/WINDOWS/system32/dllcache/imjpinst.exe matches

Binary file /mnt/windows\_mount/WINDOWS/system32/dllcache/srrstr.dll matches

Binary file /mnt/windows\_mount/WINDOWS/system32/dllcache/srsvc.dll matches

Binary file /mnt/windows\_mount/WINDOWS/system32/srrstr.dll matches

Binary file /mnt/windows\_mount/WINDOWS/system32/srsvc.dll matches

Binary file /mnt/windows\_mount/WINDOWS/system32/usmt/migisma.dll matches

Binary file /mnt/windows\_mount/WINDOWS/Installer/14753.msi matches

sansforensics@siftworkstation: /mnt/windows\_mount