1. DELETED FILES

One important aspect when collecting digital evidence are files which have been deleted. It is better to destroy evidence than hiding them. As such for digital data, deleting the data is a way of destroying the data. Therefore during computer forensic analysis, it is important to recover the deleted files since they can become a crucial piece of evidence.

When a file is created in an operating system, the file is saved in a file system. The file allocation table keeps track of the file created in the file system. Examples of a file allocation table include the FAT, FAT32 and MFT (master file table). The file allocation table allows the operating system to know where the files are located. When a file is deleted, an entry for that file is removed from the file allocation table. Hence the operating system assumes that the file does not exist. However, even if an entry is removed from the file allocation table, the file may still be physically present on the hard disk. Depending on how a file has been deleted, there is still a chance to recover that file.

Before understanding how to recover deleted files, we will go through different ways of deleting a file. One of the most common ways of deleting a file is via the Delete button found on the keyboard. However there are other ways of deleting a file.

1.1 Command Prompt

In Windows, a file can be deleted by using the command **DEL** or erase in command prompt. Below is an example of the DEL command.

A folder contains two files as shown in Figure 3.1

```
C:\Users\Avi\Desktop\Sample>dir
Volume in drive C is OS
Volume Serial Number is F896-E8AD
Directory of C:\Users\Avi\Desktop\Sample
09/04/2018
            13:36
                     <DIR>
                                     •
09/04/2018
            13:36
                     <DIR>
                                     • •
09/04/2018
            13:36
                                  39 hacker.txt
09/04/2018
            13:36
                                  58 test.txt
               2 File(s)
                                      97 bytes
               2 Dir(s) 446,549,147,648 bytes free
```

Figure 3.1

Figure 3.2 shows how to delete the file test.txt using **DEL** command.



Figure 3.2

Figure 3.3 shows how to delete a file, hacker.txt, using *erase* command in command prompt.



Figure 3.3

The **DEL** and erase commands are also used to delete folders, directories and partitions. As stated earlier, the DEL and erase commands remove the file from the file allocation table but the file will still be present on the hard disk which can be recovered using forensic tools.

1.2. Disk Cleanup

Disk Cleanup is a computer system utility software designed to delete files in order to free up disk space on the hard disk. Disk Cleanup searches and analyses files which are rarely or no longer used and, then removes them. Disk Cleanup will look for the following files for deletion:

- Temporary Internet files
- Temporary Windows/System files
- Recycle Bin
- Old Compression files
- Setup log files
- Offline caches
- Downloaded programs
- Unused installed software

Disk Cleanup utility can be accessed in Windows 10 as follows:

Control Panel\All Control Panel Items\Administrative Tools

To Launch Disk Cleanup, click on the icon **Disk Cleanup** and the screen in Figure 3.4 is shown:

🔚 Disk Cleanup for OS (C:)	\times
Disk Cleanup	
You can use Disk Cleanup to free up to 96.5 MB of a space on OS (C:).	disk
Files to delete:	
Downloaded Program Files 0 b	ytes 🔺
Temporary Internet Files 5.46	MB
System created Windows Error Reporti 157	7 KB
Direct X Shader Cache 0 b	ytes
Delivery Optimization Files 0 b	ytes 🗸
Total amount of disk space you gain: 1	10.4 MB
Description	
Downloaded Program Files are ActiveX controls and Java a downloaded automatically from the Internet when you view pages. They are temporarily stored in the Downloaded Prog Files folder on your hard disk.	ipplets certain ram
Clean up system files View Fil	es
ОК	Cancel

Figure 3.4

Then select the categories of files which you want to be removed and click **OK**. Once again the file will be removed from the file allocation table.

1.3 Keyboard Delete and Right-Click Delete

Most users delete a file by pressing the "**Delete**" button. The file will be removed and sent to the Recycle Bin.



Then the Recycle Bin can be emptied by Right-Clicking on the "**Recycle Bin**" Icon and then select the "**Empty Recycle Bin**" as shown in the Figure 3.5. The process of empting a Recycle Bin, will remove the file found in the Recycle Bin from the file allocation table. The file can still be restored through the use of computer forensic tools.



Figure 3.5

1.4 Right-Click on the file and "Delete

The other common way of deleting a file is to Right-Click on the file and then select "**Delete**" as shown in Figure 3.6. Like the keyboard delete, the file will be sent to the Recycle Bin.

	Open	
	Print	
	Edit	
2	Edit with Notepad++	
U	Scan	
D	Shred	
È	Share	
	Open with	>
	Give access to	>
1	WinMerge	
	Add to archive	
	Add to "New Text Document (3).rar"	
	Compress and email	
	Compress to "New Text Document (3).rar" and email	
Ð	Zip and Share (WinZip Express)	
Ð	WinZip	>
	Restore previous versions	
	Send to	>
	Cut	
	Сору	
	Create shortcut	
	Delete	
	Rename	
	Properties	

Figure 3.6

1.5 "Shift+Delete"

Another popular keyboard command which users perform is the "Shift+Delete". The following message is shown when the "Shift+Delete" is performed on a file:

Delete File	\times
Are you sure you want to permanently delete this file? New Text Document (4).txt Type: Text Document Size: 2.83 KB Date modified: 12/04/2018 06:50	
Yes	<u>N</u> o

Figure 3.7

If the user clicks on "YES", the file will bypass the Recycle Bin and will be removed from the file allocation table. The file is not permanently deleted (as suggested by the Figure 3.7) until the file is overwritten on the disk space. However the file will still be available on the hard disk and can be restored using computer forensic tools.

2. **REMOVING DIGITAL INFORMATION**

We have seen different ways of deleting data. Deleting data does not remove the data from the hard disk permanently. It only removes the data from the file allocation table but the data still reside on the hard disk. Using computer forensic tools, those data can be recovered or restored. Even formatting the hard disk will not erase the data permanently considering the amount of computer forensics tools available to recover the data.

So how do we permanently erase the digital data without being able to recover the data? There are two ways to remove the data permanently.

- The first way is to use Erasing software which will delete the files from the file allocation table and overwrite the file location on the disk with a series on zeros and ones. By overwriting the data on the disk, the data will not be restored even using computer forensic tools.
- The second way is to use a degausser. The degausser is a magnet which wipes out all data stored on a magnetic storage device such as the flash drives and storage tapes. The data will permanently be lost.

3. COMPUTER FORENSICS TOOLS

This section introduces a series of tools which can be used to restore a file and is used during the process of acquiring evidence.

3.1 Deleted Digital Data Restoration Tools

Restoration Tools are used to recover data that have been accidentally or intentionally deleted or corrupted. Depending on the software used, different features are available to perform the recovery of the data. However recovery of the data can only be performed if the file has not been overwritten on the disk space.

3.1.1 Data Recovery Pro

Data Recovery Pro software (Data Recovery Pro, 2018) is a free evaluation software which can be used to recover deleted files. To use the Advance features, the users need to make a purchase. For example, to recover a file, the user needs to register for this feature. The software provides the following features:

- Restoration of deleted email and deleted email attachments
- Recovery of files from a recently formatted or partitioned disk
- Restoration of a large variety of file types (Binary files or compressed files)
- Restoration of files from peripheral storage devices (such as USB)
- Recovery of Windows system files.

Below are screen shots of searching and recovering a deleted file.

- 1. Download and install the software from http://www.datarecoverydownload.com/download/
- 2. As an example, create a folder on your Desktop and rename it as "Example".



3. In the folder "Example", create a Word Document file and name it as "TestExample.doc".

		E	
💭 🖓 🕨 Example		✓ Search Example	Q
Organize 🔻 👿 Open 👻 Share with 🔻	Print Burn New folder	8=	- 🔳 🔞
⊿ 🔆 Favorites	Name	Date modified Type	Size
🧮 Desktop	TestExample.docx	16-Apr-18 12:02 PM Microsoft Word D	0 KB
🐌 Downloads 强 Recent Places			

4. On the TestExample.doc, click on the file and press "Shift+Delete"



5. Press "Yes". The file will not be sent to the Recycle Bin, and the folder Example will be empty. At this moment, we may think that we have "permanently" lost the file. However, at this stage we can still restore the file using the tool Data Recovery Pro. As mentioned, the file has an entry removed from the file allocation table and is still on the disk space unless the file is overwritten. To recover the file, run the program Data Recovery Pro.

Powered by ParetoL	
	Microsoft Partner
🕲 Scan	SELECT THE SCAN YOU WANT TO USE:
Advanced	• QUICK SCAN: Quickly scans the selected drive for easily recovered files.
t 🕑 Email	Drive: C: Optional: You can specify filename to look for. Search for: File Types: All
1	O FULL SCAN: Scans your computer and all connected devices.
	Optional: You can specify filename or text content to look for. Search for: File Types: All
	O GUIDED SCAN: Guides you through the selection of file or email recovery.
Why the beetle? Scarab beetles have amazing ability to recover discarded ite and re-use them.	an START SCAN

6. Press "Start Scan". After the software has scanned the disks, the following screen will be presented:

Powered by ParetoLogic	zovery Pro	Microsoft Part	ner		ABOUT HELP
😟 Scan	Scan > Select Items	To Recover			
Advanced	To expand a category listed below cl the item. You can filter the results by associated check box and click the R	ick the + sign. You ca r entering text in the Fi ecover button.	in get a preview Iter results box.	by placing your m To recover items	ouse cursor over select the
Email			Filter results:		×
	Name	Location Size	Date Created	Date Accessed	Date Modified
	Local Disk (C:) Documents Text Files Compressed Files Folders Binary Files Other Files			Items	Found: 872 4 Items 11 Items 3 Items 10 Items 4 Items 840 Items
Why the beetle? Scarab beetles have an amazing ability to recover discarded items	Total items found: 872 File Recovery Location: C\Users\admin\D	esktop\Recovered Items	Filtered items sel	lected for recover	y: 0 of 872 (0 bytes)

7. Expand the "Documents" and the TestExample.docx will be available.

Powered by ParetoLogic	covery Pro	Microsoft Partner	ABOUT HELP
Scan	Scan > Select Items To expand a category listed below the item. You can filter the results b associated check box and click the	5 TO Recover click the + sign. You can get a preview by placing your m by entering text in the Filter results box. To recover items Recover button.	ouse cursor over select the
Email	Name Local Disk (C:) Coursests Local Disk (C:) Labsheet 17 1D_Array.pdf Starsmple.docx TestExample.docx Starsmple.docx Starsmes Compressed Files Compressed	Location Size Date Created Date Accessed Items Items Items Items C:\Users\ 75.5 2017/02/08 10:5 2017/02/08 10:59: C:\admin 162 b 2018/04/16 12:0 2018/04/16 12:04: C:\admin 162 b 2018/04/16 12:0 2018/04/16 12:04: C:\admin 162 b 2018/04/16 11:5 2018/04/16 11:54:	Date Modified Found: 872 4 Items
Why the beetle? Scarab beetles have an amazing ability to recover discarded items and re-use them.	Total items found: 872 File Recovery Location: CAUsers\admin\	Filtered items selected for recovery Desktop\Recovered Items Change Location CANCEL	r: 0 of 872 (0 bytes) RECOVER

8. Click on TestExample.docx and press the button "Recover". Since we are using a free version, this feature will not be available until we register the product. But we have illustrated how tools can recover deleted files.

Name		Location	Size	Date Created	Date Accessed	Date Modified
	Disk (C:)				Items	Found: 872
Docume	nts		75.5	2017 (22 (22 12	5 0047 (00 (00 40 50	4 Items
Labsheet	t_1/_1D_Array.pdf	C:\Users\	/5.5	2017/02/08 10	:5 2017/02/08 10:59:.	2017/02/08 10:
🗌 ~\$stExan	nple.docx	C:\admin	162 b	2018/04/16 12	:0 2018/04/16 12:04:.	2018/04/16 12:
TestExan	nple.docx	C:\admin	12.3	2018/04/16 12	:0 2018/04/16 12:04:.	2018/04/16 12:
C ~\$DELET	F. d	Chadrain	162.6	2012/04/16 11	:5 2018/04/16 11:54:.	2018/04/16 11:
🕀 🗍 Text File	Data Recovery Pro			×		11 Items
 Compres Folders Binary Fi Other Fil 	To recover items you must Click OK to register.	register the p	oroduct.			3 Items 10 Items 4 Items 840 Items
Total items fou	10, 072		OK	erca nems se	elected for recovery	: 1 of 872 (12.3 KB)
File Recovery Loo	cation: C:\Users\admin\Deskto	p\Recovered I	tems 🖸	nange Location	CANCEL	RECOVER

3.1.2 **Recuva**

Recuva (CCleaner, 2018) is a freeware for Windows which allows the restoration of files which have been deleted from the computer. Files which have been deleted from the Recycle Bin, Memory cards and external drives can be recovered. Recuva allows users to destroy files such that they are not recovered by other software restoration tools (it overwrites the disk space where the file is located.) Below are the features which Recuva offers:

- Graphical User Interface to scan the disk to select files to be recovered.
- The software can be run on a flash drive.
- Recover all types of files.
- Supports different file allocation table systems such as FAT16, FAT32, NTFS, • NTFS5.
- Recover files from removable memory cards.

Let's now see how Recuva works:

- 1. Download and Install Recuva from https://www.ccleaner.com/recuva. Select the Free Version.
- 2. Following from the previous example (of the deleted file TestExample.docx), we would like to recover the later file after the "Shift+Delete" has been pressed.
- 3. Run Recuva and Press "Next".

Recuva Wizard	×				
	Welcome to the Recuva Wizard				
	This wizard will help you recover your deleted files. Just answer a few simple questions and Recuva does the rest.				
	If you don't want to use this wizard, simply press Cancel and you will have access to the advanced features of Recuva.				
Do not show this Wizard on s	startup.				
	< Back Next > Cancel				

4. Select "Document" and Press "Next".

Recuva Wizard	— ×
File type What sort of files are you trying to recover?	
All Files Show all files.	
Pictures Show only files of common image formats, such as digital camera photos.	
Music Show only files of common audio formats, like MP3 player files.	
Documents Show only files of common office document formats, such as Word and Excel file	iles.
Video Show only video files, like digital camera recordings.	
Compressed Show only compressed files.	
Emails Show only emails from Thunderbird, Outlook Express, Windows Mail and Micros Outlook.	soft
< Back Next >	Cancel

5. Select "In a Specific Location" and press "Next".

Recuva Wizard 🔤	
File location Where were the files?	
 I'm not sure Search everywhere on this computer. On my media card or iPod 	
Search any removable drives (except CDs and floppies) for deleted files. The model of the search user documents folders.	
In the Recycle Bin Search for files deleted from the Recycle Bin.	
In a specific location	
C:\ Browse	
On a CD / DVD	
< Back Next > Cancel	

6. Enable "Deep Scan" and Press "Start".



7. The results are shown below. To recover the file, check the file to be recovered and press "Recover" button.

🚳 Pi	🗧 Piriform Recuva						
4	Recuva Microsoft Wir Intel Core i3-	1 .com v1. ndows 7 Ent 2100 CPU @	53. 1087 (64-bit) erprise 64-bit SP1 9 3. 10GHz, 4.0GB RA	۱M, Intel HD G	raphics Family	Ò	
Selec For th	t the files you want to F ne best results, restore	Recover by the files to	ticking the boxes and a different drive.	then pressing	g Recover.	Switch to advanced mode	
	Filename	Path	Last Modified	Size	State	Comment	
	[000001].xlsx	C:\?\	Unknown	1,238 KB	Excellent	No overwritten clusters detected.	
	[000002].xlsx	C:\?\	Unknown	1,160 KB	Excellent	No overwritten clusters detected.	
1	[000003].docx	C:\?\	Unknown	12 KB	Excellent	No overwritten clusters detected.	
	[000004].xlsx	C:\/?\	Unknown	1,238 KB	Excellent	No overwritten clusters detected.	
•		1					
[C:] N	[C:] NTFS, 195 GB. Cluster size: 4096. File record size: 1024. Found 4 file(s) in 53.79 seconds.						
<u>Onlin</u>	Online Help Check for updates						

3.1.3 Autopsy

Autopsy (Carrier, B. 2018) is a computer forensic tool to analyse hard disk and smart phones. Autopsy is an Open Source Digital Forensic tool which allows the user to develop customised modules in Java or Python. Autopsy uses the Sleuth Kit which contains a collection of command line programs and C library in order to analyse hard disk and to recover files. Autopsy provides a range of features to enable a computer forensics analyst to conduct his/her investigation. Autopsy also provides Analysis and Reporting features.

Some of the features provided in the Analysis part are listed below:

- Registry Analysis
- Email Analysis
- Geo location analysis of JPEG files.
- Web Analysis
- Video Analysis
- File Recovery
- Multi-User collaboration
- File Type Detection.
- SMS, Call logs Analysis.

3.1.4 WinUndelete

WinUndelete (WinRecovery Software, 2018) is a recovery tool which enables users to recover their deleted files. The deleted files can be recovered from the hard disk, external drive, floppy disk and memory card from a digital device. It supports both the FAT and NTFS file system.

Below is a list of situations which WinUndelete can be used to recover files:

- Restores files after the recycle bin has been emptied.
- Restores files after a command prompt delete or a "Shift+Delete".
- Restores files from a network share.
- Restores files after a Move or Cut command.

3.1.5 Ontrack EasyRecovery

Ontrack (Ontrack, 2018) provides a series of software recovery tools on a trial basis and allows users to recover deleted files and data from formatted and corrupted disks. Furthermore Ontrack provides software for email recovery, SharePoint recovery, SQL recover and Mobile phone recovery software for Windows and Mac.

As we can see, there are many software available to recover delete files. However recovery is only possible if the disk space where the file is residing has not been overwritten.

4. DELETED PARTITIONS RECOVERY

Dividing a hard disk into different volumes is known as partitioning. Each partition is labelled as a drive letter by the operating system and becomes a logical drive as shown in Figure 3.8. Each logical drive can be formatted to support different operating systems as well as to use different file systems (either FAT16, FAT32, NTFS). Partitioning is performed for increased performance and management of data. For each partition created, an entry is performed in the partition table. Therefore when a partition is deleted, the entry is removed from the partition table (and the space becomes unallocated). To restore the partition, forensic software tools can be employed. Those tools usually search for the boot sector in order to restore the partition. This section introduces some of the tools used to restore a partition.



Figure 3.8

To manage and view the partitions on a hard disk in Windows, follow the steps below:

- Go to Control Panel
- Select Administrative tools



• Click on "Computer Management".

Control Panel 🕨 All Co	ontrol Panel Items Administrative Tools
Burn	
	Name
	Recomponent Services
	🛃 Computer Management
es	📷 Data Sources (ODBC)
	🗿 desktop.ini
	冠 Event Viewer
4	💦 iSCSI Initiator
	🔁 Local Security Policy
	Performance Monitor
	🕞 Print Management
	😹 Services
	🛃 System Configuration
	😥 Task Scheduler
	🔗 Windows Firewall with Advanced Security
C:)	🔊 Windows Memory Diagnostic
ie (D:)	😹 Windows PowerShell Modules

• Select "Disk Management".



• Upon clicking on "Disk Management", the utility will show all the logical drives available and their properties. In this example, there are five partitions (System Reserved, C:, D:, two healthy partitions and an unallocated partitions). The C: logical drive is the Boot volume, that is, it contains the files to start up the computer. The C: logical drive is also the Page File and Crash Dump volume, meaning that it contains all the memory dump output.

🌆 Computer Management													- 6 2
File Action View Help													
🗢 🔿 🙋 🗔 🖬 🐼 🗙 🖆	f 🖻 🔍 😼												
Computer Management (Local) Computer Management (Local) Computer Tools Computer Tools Computer Tools Computer Viewer Co	Volume	Layout 1 Simple E Simple E Simple E Simple E Simple E	Type File System Si Sasic H Basic H Basic NTFS H Basic NTFS H Basic NTFS H	tatus lealthy (Primar lealthy (Boot, F lealthy (Primar lealthy (System	y Partition) y Partition) 'age File, Crash Dump, Primary Pa y Partition) y, Active, Primary Partition)	Ca 79. 1.8 rtition) 19! 97. 100	pacity Free 66 GB 79.60 6 GB 1.86 5.40 GB 2.94 47 GB 12.79 0 MB 70 M	Space % F 5 GB 100 GB 100 GB 2 % 9 GB 13 % 1B 70 %	Free Fault Tol 1% No 1% No 5 No % No % No % No % No % No	erance Ov 0% 0% 0% 0%	erhead		Actions Disk Management More Actions
 Storage Disk Management Services and Applications 	Disk 0 Basic 465.76 GB Online	New Volume (D:) 97.47 GB NTFS Healthy (Primary Partition)	79.66 GB Healthy (I	Primary Partiti	ion) 1.4	86 GB ealthy (Primary	Pi 91.27 (Unallo	5B cated					
	CD-ROM 0 DVD (E:) No Media												
	SCD-ROM 1 DVD (F:) No Media												
Volume Layou	it Type File	System	Status				Capacity	Free S	pace % F	ree Fai	ult Toleran	ice Over	head
📼 Simpl	le Basic		Healthy (Prima	ry Partition	i)		79.66 GB	79.66	GB 100	% No)	0%	
🗀 Simpl	le Basic		Healthy (Prima	ry Partition	i)		1.86 GB	1.86 G	B 100	% No)	0%	
(C:) Simpl	e Basic NTF	s	Healthy (Boot, I	Page File, (Crash Dump, Primary Pa	rtition)	195.40 GB	3 2.94 G	iB 2 %	No)	0%	
New Volume (D:) Simpl	e Basic NTF	s	Healthy (Prima	ry Partition	i)		97.47 GB	12.79	GB 13 9	6 No)	0%	
System Reserved Simpl	e Basic NTF	s	Healthy (Systen	n, Active, F	rimary Partition)		100 MB	70 MB	3 70 9	6 No	•	0%	
				1		1							
Basic System 465.76 GB 100 MB Online Healthy	n Re (C:) 8 N1 195.40 GE 9 (S: Healthy (3 NTFS Boot, Pag	ge File, Crash D	New Vo 97.47 GE Healthy	o lume (D:) 3 NTFS (Primary Partition)	79.66 (Health	3B y (Primaŋ	y Partitio	n) 1.8	36 GB ealthy (Pr	rimary Pi	91.27 GE Unalloca	3 ated

• To delete a partition, Right-Click on the "volume" and select "**Delete**". As stated earlier, deleting a partition or volume, does not necessary mean that the partition has been permanently removed. It can still be recovered through the use of computer forensics recovery software.

												1	1
Volume	Layout	Туре	File System	Status					Capacity	Free Space	% Free	Fault Toleran	ce Overhead
	Simple	Basic		Healthy ((Primary	Partition)			79.66 GB	79.66 GB	100 %	No	0%
	Simple	Basic		Healthy ((Primary	Partition)			1.86 GB	1.86 GB	100 %	No	0%
🕞 (C:)	Simple	Basic	NTFS	Healthy ((Boot, Pa	ige File, Crash Dump, Prin	nary Par	tition)	195.40 GB	2.94 GB	2 %	No	0%
🕞 New Volume (D:)	Simple	Basic	NTFS	Healthy ((Primary	Partition)			97.47 GB	12.79 GB	13 %	No	0%
System Reserved	Simple	Basic	NTFS	Healthy ((System,	Active, Primary Partition)			100 MB	70 MB	70 %	No	0%
Disk 0					_								
Basic	System R	la (C	:)			New Volume (D:)						_	at at at
405.70 GB	100 MB N	195 0 195	40 GB NTFS	na Filo. C	rach D	97.47 GB NTFS	5//	/9.66 (iB (Drimon)	Dartition)	1.80 G	B (Drimon (D)	91.27 GB
	rieditity (.			ige rile, Ci			9777	rieaiun	y (Fillinaly	Partition	riealu	iy (Fillinaly Fi	onanocated
							Ope	n					
CD-ROM 0							Explo	ore					
DVD (E:)							Mar	k Partitio	n as Active	2			
No Media							Char	nge Driv	e Letter and	d Paths			
							Form	nat					
CD-ROM 1							Exter	nd Volu	ne				
DVD (F:)							Shrir	nk Volur	ne				
							الم الم	Minner					
No Media							Add	wintor					
							Dele	te Volur	ne				
							Prop	perties					
							Help	0					

4.1 Deleted Partitions Restoration Tools

When a partition or volume is erased/deleted, the entry in the partition table is removed. Removing an entry from the partition table does not mean that the partition has been purged permanently. The partition may still be available on the disk. The partition can be recovered through the use of partition recovery software tools as long as the partition has not been overwritten on the disk space. The main thrust of the partition recovery software tool is to find the boot sector of the deleted partition and restore the partition by making an entry in the partition table. This section will highlight some of the partition recovery tools by computer forensic analyst to recovery deleted partitions.

4.1.1. EaseUS Partition Recovery Wizard

EaseUS (EaseUS, 2018) is a partition recovery tool used to restore deleted partitions. This tool scans several areas in the disk to search the location of the deleted partition. The software recovers deleted, lost and damaged FAT, NTFS, HFS, HFS+, HFSX, Ext2, Ext3 partitions under Windows.

4.1.2 Active@ Partition Recovery

Active@ Partition Recovery (LSoft Technologies, 2018) is a freeware to restore deleted and damaged partitions in Windows, Linux and DOS. Some of the main features of Active@ Partition Recovery are as follows:

- Partition Recovery- Restore deleted, lost and damaged partition.
- Provide three types of scanning: QuickScan (for searching and restoring recently deleted partitions), SuperScan (searching and restoring for partitions which have been deleted a long time ago) and Last Chance (searching and restoring severely damaged partitions).
- Backing up of partitions.
- Fixing damaged Partition Table and Master Boot Record (it contains all information on the disk partitions).
- Recover IDE, SATA, eSATA, SSD, SCSI, RAID, USB Flash Disks and Memory Cards.

4.1.3 Partition Find and Mount

Partition Find and Mount (A-FF Labs, 2018) is a software tool to search and mount lost partition in a read-only mode in order to prevent malware from altering the information.

The main features of Partition Find and Mount are as follows:

- It supports all versions of NTFS and FAT file systems.
- The software scans the hard disk for specific signatures belonging to the deleted or lost partition.
- It scans both the Master Boot Record and other information which will lead to the deleted or lost partition. As such, three scans are provided: Fast Intellectual Scan, Normal Scan and Thorough Scan,
- It does not work with badly damaged disk.

5. DATA ACQUISITION SOFTWARE

During computer forensic analysis, the analyst needs to use software tools in order to examine the data/information/evidence without modifying the data. Most of the data acquisition tools will duplicate the data/information/evidence such that it can be analysed without the risk of tampering the data/information/evidence. This section will preview some of the data acquisition tools used by computer forensic analyst.

5.1 Forensic Toolkit

Forensic Tookit (AccessData, 2018) is a computer forensics tool used to scan the hard disk for searching, and locating deleted files and emails. The Forensic Toolkit provides a standalone disk imaging tool (FTK Imager) used to duplicate the hard disk information. The FTK Imager replicates the hard disk as an image and then calculates the hash value using Message Digest algorithm: 5 (MD5). The MD5 ensures the integrity of the data. The image can then be used for analysis purposes. The image can be transferred to another machine for examination and can be saved under different image file format (for example DD/RAW).

5.2 EnCase Forensics

EnCase Forensics (Guidance Software, 2018) is a computer forensic tool used to collect information, analyse the data, report the findings and preserve the data. For preservation of the data, EnCase Forensics duplicates the original drive or media and then generates a MD5 hash values for the image as well as providing a Cyclic Redundancy Check (CRC) values to the data. The MD5 and CRC ensure that the data have not been modified and ensure the validity of the information. While duplicating the original drive, the analyst can specify which part of the drive (for example the C: or D: drive) or the types of files to be duplicated

Once the image has been produced, the computer forensics analyst can replicate the image to be analysed simultaneously by different examiners. Furthermore, EnCase Forensics provides the following features:

- Automation tools in order to speed up the investigation process
- Analysis features such as file signature, hash and log analysis
- Scanning in Unicode, binary Big Endian/Little Endian
- Reporting features
- Email and Internet Analysis

5.3 Data Dumper

Data Dumper (dd) is a UNIX utility tool for imaging a hard drive. dd replicates a computer's hard disk as an image for examination purpose. It is a command line tool and requires an understanding of the syntax to execute the command. dd can replicate information across files, devices, partitions and volume. Table 3.1 shows a list of command which can be executed by dd.

Table 3.1: dd Command

Data transfer forms of dd	
blocks=\$(isosize -d 2048 /dev/sr0) dd if=/dev/sr0 of=isoimage.iso bs=2048 count=\$blocks status=progress	Creates an ISO disk image from a CD-ROM, DVD or Blu-ray disk. ^[8]
dd if=system.img of=/dev/sdc bs=4096 conv=noerror	Restores a hard disk drive (or an SD card, for example) from a previously created image.
dd if=/dev/sda2 of=/dev/sdb2 bs=4096 conv=noerror	Clones one partition to another.
dd if=/dev/ad0 of=/dev/ad1 bs=1M conv=noerror	Clones a hard disk drive "ad0" to "ad1".

Source: dd Command (Wikipedia, 2018)

5.4 Mount Image Pro

Mount Image Pro (GetData, 2018) is a computer forensic tool which enables the computer forensic analyst to mount different forensic images or physical devices under Windows. The mounted image can then be analysed thoroughly by allowing the investigators to quickly browse the content in the image and running third party programs (virus scanners, keyword indexing tools and data restoration software) on the mounted image. Mount Image Pro supports a large variety of file image format such as

- EnCase .E01, EX01, .L01, .LX01
- AccessData .AD1
- DD and RAW images (Unix/Linux)
- Forensic File Format .AFF
- NUIX .MFS01
- ProDiscover
- Safeback v2
- SMART
- XWays .CTR
- VMWare
- Xways Container File

6. WINDOWS REGISTRY ANALYSIS

During an investigation, a computer forensics analyst needs to examine the Microsoft Windows Registry. The Microsoft Window Registry contains a large variety of information pertaining to the computer system. It contains useful information after someone has utilised the computer system. According to Microsoft, "the registry is a system-defined database in which applications and system components store and retrieve configuration data. The data stored in the registry varies according to the version of Microsoft Windows. Applications use the registry API to retrieve, modify, or delete registry data" (Microsoft, 2018).

Apart from storing valuable information on devices (hardware), it can also store a variety of information on the user's activity (such as which devices are connected to the computer system, which software was installed and uninstalled on the computer system by the user, to which wireless access point the computer has been connected to). Collecting these information is significant during an investigation.

The Windows Registry is a hierarchical database which contains information which is essential for the operation of the operation system (OS) and applications running on the computer system. The information is arranged in a tree structure and each node in the tree is known as a *key*. Each *key* contains both the *subkeys* and data entries known as *values (the values can be 0, 1 or hexadecimal)*. However, there are five main *key* nodes known as hives.

The five hives are:

- i. HKEY_USERS: maintain all the user profiles on the computer system
- ii. HKEY_CURRENT_USER: maintain the profile of the currently logged-on user
- iii. HKEY_CLASSES_ROOT: Application configuration data to open files
- iv. HKEY_CURRENT_CONFIG: startup system hardware information
- v. HKEY_LOCAL_MACHINE: hardware and software configuration settings.

Figure 3.9 shows the Windows registry structure. To access the registry, type "regedit" in the "search windows"



Figure 3.9: Windows Registry

6.1 Investigating the Windows Registry

During an investigation process, examining the Windows Registry will provide valuable information which can assist the investigation or can be used as a piece of evidence. This section will provide the common location which the computer analyst examines to retrieve information.

6.1.1 Autorun Programs

Autorun programs are programs which are launched during the bootup of the computer system. The Windows Registry provides all the programs which are launched during the booting of the computer system as well as the location where the program resides on the computer system. It is important to look at the registry in order to search for malware in the computer system which could have compromised the computer system or the computer system has been used to launch an attack through the use of a Trojan. Below is a list of paths where a computer forensic analyst will examine the registry:

- HKEY_LOCAL_MACHINE \Software\Microsoft\Windows\CurrentVersion\Runonce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

Figure 3.10 shows an example of HKEY_LOCAL_MACHINE \Software\Microsoft\Windows\CurrentVersion\Run output.

📑 Registry Editor											
File Edit View Favorites Help											
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run											
> PushNotifications	^	Name	Туре	Data							
		ab (Default)	REG SZ	(value not set)							
> Reliability		ab IAStoricon	REG_SZ	"C:\Program Files\Intel\Intel(R) Rapid Storage Technology\IAStorlconLaunch.exe"							
> RetailDemo		ab IgfxTray	REG SZ	"C:\Windows\system32\igfxtray.exe"							
Kun		ab QuickSet	REG_SZ	c:\Program Files\Dell\QuickSet\QuickSet.exe							
Saarch		ab RtHDVBg	REG_SZ	"C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe" /MAXX5							
SecondaryAuthFactor		ab RTHDVCPL	REG_SZ	"C:\Program Files\Realtek\Audio\HDA\RtkNGUI64.exe" -s							
> Security and Maintenance		ab SecurityHealth	REG_EXPAND_SZ	%ProgramFiles%\Windows Defender\MSASCuiL.exe							
> SettingSync		ab SynTPEnh	REG_EXPAND_SZ	%ProgramFiles%\Synaptics\SynTP\SynTPEnh.exe							
> Setup		ab TrueColor UI	REG_SZ	C:\Program Files\TrueColor\TrueColorUI.exe							
		ab) tvncontrol	REG_SZ	"C:\Program Files\TightVNC\tvnserver.exe" -controlservice -slave							

Figure 3.10: Example of Location for Autorun Program

(HKEY_LOCAL_MACHINE \Software\Microsoft\Windows\CurrentVersion\Run)

6.1.2 Most Recently Used Entries

Most Recently Used contains all the entries made by the user while performing a specific action. For example, if the user has been using the RUN command (Figure 3.11), the following Registry Entries, HKEY_CURRENT_USER\Software\Microsoft\Windows\ CurrentVersion\Explorer\RunMRU will show all the actions the user has been performing while using the RUN program. Figure 3.12 illustrates the RunMRU access in the Windows Registry.

🖅 Run	×
٨	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	↓ ✓
	OK Cancel <u>B</u> rowse

Figure 3.11: RUN Command

📑 Registry Editor											
File Edit View Favori	ites Help										
Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU											
	PhotoPrintingWizard	Name	Туре								
	Pimvolatile	ab) (Default)	REG_SZ								
	RecentDocs	a) a	REG_SZ								
	Ribbon	ab) b	REG_SZ								
	RupMPH	ab) c	REG_SZ								
	Search	ab) d	REG_SZ								
	SearchPlatform	ab) e	REG_SZ								
	SessionInfo	ab) f	REG_SZ								
	Shell Folders	ab) g	REG_SZ								
	Shutdown	ab) h	REG_SZ								
	StartPage	abji	REG_SZ								
	StartupApproved	ab j	REG_SZ								
	StreamMRU	k	REG_SZ								
× ×	Streams	abi	REG_SZ								
	StuckRects2	ab) m	REG_SZ								
	StuckRects3	📃 赴 MRUList	REG_SZ								
	Taskband	ab n	REG_SZ								
	TypedPaths	abo	REG_SZ								
	User Shell Folders		-								

Figure 3.12: RunMRU Registry

6.1.3 Wireless Network Access

The Windows Registry records all the access points which the computer system has been connected to. It records the network SSID (Service Set Identifier). The latter information can be accessed as follows:

$HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Network\List\Profiles.$

Figure 3.13 shows all the SSID which the computer system has connected to. The Profile Name shows the SSID.

Figure 3.13: Wireless Network Access.

6.1.4 Connected USB Devices

To know all the USB devices which have been connected to the computer system, the following path is used on the registry: HKEY_LOCAL_MACHINE \SYSTEM\ControlSet00x\Enum\USBSTOR. The latter stores all the information with respect to the USB devices as shown in Figure 3.14. One important piece of information is the Device ID. The Device ID is a unique number which is provided by the manufacturer. Hence it is possible to trace the USB.

🏦 Regist	ry Editor												
File Edi	ile Edit View Favorites Help												
Compute	Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&\ven_TOSHIBA&Prod_TransMemory&Rev_1.00\0022CFF68D85C140D2095908&0												
	>	{5d624f94-8850-40c3-a3fa-a4fd2080baf3}	^ N	Vame	Туре	Data							
	>	ACPI	a	(Default)	REG SZ	(value not set)							
	>	ACPI_HAL	ŝ	Address	REG_DWORD	0x00000001 (1)							
	>	BTH	1	Capabilities	REG_DWORD	0x00000010 (16)							
	>	DISPLAY	a	ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}							
			a	CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW GenDisk							
			1	ConfigFlags	REG_DWORD	0x00000000 (0)							
	5	PCI	a	🖢 ContainerID	REG_SZ	{20dffe40-83a0-5bff-9f54-828cb70e074c}							
	>	ROOT	a	DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive							
	>	SCSI	a	Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0002							
	>	STORAGE	a	EriendlyName	REG_SZ	TOSHIBA TransMemory USB Device							
	>	SW SW	a a	HardwarelD	REG_MULTI_SZ	USBSTOR\DiskTOSHIBA_TransMemory1.00 USBSTOR\DiskTOSHIBA_TransMe							
	>	SWD	a	≜ Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Standard disk drives)							
	>	USB	a	Service	REG_SZ	disk							
	>	USBPRINT											
	~	USBSTOR											
		Dick8iVan 8/Prod USP Elsch Mamon/8/Pay PMAP											
		Disk&Ven_ceneral&Prod_USB_Flash_Wentoryckev_PMAP											
		Disk@Ven_Kingston@Prod_DataTraveler_2.0@Rev_1.00											
		Disk&Ven TOSHIBA&Prod TransMemory&Rev 1.00											
		> 0022CFF6BD85C140D209590B&0		Dovice									
		> 0022CFF6BD85C140E6526812&0		Device ID									

Figure 3.14: USB Devices

6.1.5 Browser (Internet Explorer)

The default browser proposed by Windows is Internet Explorer. To obtain some initial information on the Internet Explorer used on the computer system, this can be obtained as follows: HKEY_CURRENT_USER\Software\Microsoft\ Internet Explorer\Main. The latter provides the user default settings such as the default search page and start page information as illustrated in Figure 3.15.

📑 Registry Editor												
File Edit View Favorites Help												
Computer\HKEY_CURRENT_USER\Softw	Computer\HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main											
> LowRegistry	Name	Туре	Data									
Main FeatureContro WindowsSear MAO Settings MenuExt MINIE New Windows PageSetup PhishingFilter	DownloadWindowPlacement DownloadWindowPlacement EdgeSwitchingOSBuildNumber DEnable Browser Extensions FullScreen ElEIORunOnceCompletionTime ElEIORunOncePerInstallCompleted ImageStoreRandomFolder	REG_BINARY REG_BINARY REG_SZ REG_SZ REG_SZ REG_BINARY REG_DWORD REG_SZ	01 00 00 00 2c 00 00 00 00 00 00 00 00 00 00 00 00 83 ff ff 00 83 ff ff 10586.th2_release.160802-1857 yes no fa db 30 f2 03 8e d3 01 0x00000001 (1) qig0brq									
······································	Local Page Wews Feed First Run Experience WoupdateCheck	REG_SZ REG_DWORD REG_DWORD	C:\Windows\system32\blank.htm 0x00000000 (0) 0x00000001 (1)									
Repld	Play_Animations Play_Background_Sounds	REG_SZ REG_SZ	yes yes									
- Security - Services - Settings - Setup - SiteMode	Save_session_nistory_on_exit Search Page SearchBandMigrationVersion Show_FullURL Show_StatusBar Show_ToolBar	REG_SZ REG_DWORD REG_SZ REG_SZ REG_SZ	http://go.microsoft.com/fwlink/?LinkId=54896 0x00000001 (1) no yes yes									
StorageTelemetr Suggested Sites TabbedBrowsing	Show_URLinStatusBar Show_URLToolBar Start Page Start Page Start Page	REG_SZ REG_SZ REG_SZ REG_SZ	yes yes http://go.microsoft.com/fwlink/p/?LinkId=619797&p http://www.msn.com/?pc=UE01&ocid=UE01DHP									

Figure 3.15: Internet Explorer

Besides to obtain information on the URL typed, the following registry path can be examined:

HKEY_CURRENT_USER\Software\Microsoft\ Internet Explorer\TypedURLs.

6.1.6 Recently Used Documents

The Windows registry provides information on the user activities such as recent used document on the computer system. To obtain the latter information, the following registry path should be used: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentD ocs as illustrated by Figure 3.16.

📑 Registry Editor												
File Edit View Favorites Help												
Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs												
	PhotoPrintingWizard /	^ Name	Туре	Data								
	PImVolatile	88 102	REG BINARY	41 00 4e 00 4e 00 45 00 58 00 20 00 34 00 20 00 42 00 53 00 43								
	RecentDocs	88 103	REG BINARY	41 00 73 00 73 00 69 00 67 00 6e 00 6d 00 65 00 6e 00 74 00 2d								
	RestartCommands	105	REG BINARY	53 00 65 00 63 00 6f 00 6e 00 64 00 53 00 65 00 6d 00 65 00 73								
	Ribbon	106	REG BINARY	4d 00 53 00 63 00 20 00 41 00 74 00 74 00 65 00 6e 00 64 00 61								
	RunMRU	88 107	REG RINARY									
	Search	90 100										
	SearchPlatform	00100	REG_BINARY									
	SeccionInfo	109	REG_BINARY	74 00 65 00 63 00 68 00 6e 00 69 00 71 00 75 00 65 00 73 00 2d								

Figure 3.16: Recently Used Documents

To obtain further information on a particular document, right-click on the Name (for example 103) as shown in Figure 3.17. On the right hand side, you can have the document name and thus you may search for this document.

File Edit View Favorites Help Computer/HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs Data PintVolatile PintVolatile RecentDocs RecentDocs RestartCommands Ref_BINARY 41 00 4e 00 4e 00 45 00 58 00 20 00 34 00 20 00 42 00 53 0 Ribbon RestartCommands RestartCommands X Ribbon Edit Binary Value X Value name: Search Search SessionInfo SessionInfo 103 StartPage 0010 6E 00 6D 00 65 00 g. n. m. e. StartPage StartPage 0018 30 031 00 37 00 6D 0 1.7 7 0 Streams G020 32 00 31 00 37 00 6D 0 1.8 0 StreamS G030 65 00 73 00 73 00 7.7 7.7 7.7 7.7 7.7 </th <th>📕 R</th> <th>egistry</th> <th>/ Editor</th> <th>r</th> <th></th>	📕 R	egistry	/ Editor	r													
Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs Data PhotoPrintingWizard Name Type Data PlmVolatile RecentDocs 102 REG_BINARY 41 00 4e 00 4e 00 45 00 58 00 20 00 34 00 20 00 42 00 53 0 RestartCommands RestartCommands Edit Binary Value X RunMRU Search 103 Value name: X Value data: 0000 41 00 73 00 73 00 69 00 A . s . s . s . 1 . A Search Search 0010 6E 00 6D 00 65 00 g . n . m . e . A Search 9010 6E 00 74 00 2D 00 73 . 00 69 00 A . s . s . s . 1 . A StartPage 0010 6E 00 74 00 2D 00 73 . 00 65 00 g	File	Edit	View	F	avori	tes Help											
PhotoPrintingWizard Name Type Data PImVolatile RecentDocs REG_BINARY 41 00 4e 00 4e 00 45 00 58 00 20 00 34 00 20 00 42 00 53 0 RestartCommands RestartCommands Ref_BINARY 41 00 73 00 73 00 69 00 67 00 6e 00 6d 00 65 00 6e 00 74 0 Ribbon Ribbon Edit Binary Value X RunMRU Search Value name: X Search Value data: Value data: X 0000 41 00 73 00 69 00 A s . s . s . i . A s . s . i . Shutdown StartPage 0010 6E 00 73 00 69 00 A s . s . s . i . A s . s . s . i . StartPage 0010 6E 00 73 00 69 00 1 2 . 001 2 . 0020 32. 00 1 2 . 0030 65 000 65 00 00 1	Com	nputer\	HKEY_	CU	RREN	T_USER\Software	\Microsoft\	Windows\C	CurrentV	ersion\E	xplorer\l	RecentD	ocs				
PlmVolatile ID2 REG_BINARY 41 00 4e 00 4e 00 45 00 58 00 20 00 34 00 20 00 42 00 53 00 20 00 34 00 20 00 42 00 53 00 20 00 74 00 66 00 64 00 65 00 6e 00 64 00 65 00 6e 00 74 00 73 00 73 00 69 00 67 00 6e 00 64 00 65 00 6e 00 74 00 74 00 73 00 73 00 69 00 67 00 6e 00 64 00 65 00 6e 00 74 00 73 00 73 00 69 00 67 00 6e 00 64 00 65 00 6e 00 74 00 73 00 73 00 69 00 73 00 69 00 73 00 69 00 73 00 69 00 73 00 69 00 73 00 69 00 73 00 69 00 73 00 69 00 74 00 65 00 8g · n · m · e · 0 73 00 73 00 69 00 65 00 8g · n · m · e · 0 74 00 65 00 8g · n · m · e · 0 74 00 73 00 65 00 8g · n · m · e · 0 74 00 73 00 74 00 73 00 73 00 74 00 75 00 7					>	PhotoPrintingV	Vizard 🔨 🔨	Name		Тур	e		Data				
RecentDocs Ref_BINARY 41 00 73 00 73 00 69 00 67 00 6e 00 6d 00 65 00 6e 00 74 0 Ribbon Edit Binary Value X RunMRU Search Value name: X Search Value data: X X Walue data: 0000 67 00 6E 00 6D 00 65 00 g: n . m . e . N Shutdown StartPage 0010 6E 00 73 00 69 00 A . s . s . s . i . A StartPage 0010 6E 00 73 00 69 00 A . s . s . s . i . A StartPage 0010 6E 00 73 00 69 00 1. 7 2 StartupApprov 0018 30 00 31 00 38 02 0 1. 7 0030 65 00 1. 8 0 1. 8 0 1. 8 1. 8 1. 8 1. 8 1. 8 1. 8 1. 8 1. 8 1. 8					>	PImVolatile		88 102		REG	BINAR	/	41 00	4e 00 4	e 00 45 00	0 58 00 20 00 34 00 20 00 42	00 53 00
RestartCommande RestartCommande RestartCommande RestartCommande Ribbon Edit Binary Value X RunMRU Search Value name: SearchPlatform 103 SessionInfo SessionInfo Shutdown 6000 6000 41 00 73 00 69 00 A. s . s . s . i . A. s . s . s . i . Shutdown 6008 67 00 6E 00 00 32 00 n. t 2 . A. s . s . s . i . A. s . s . s . i . StartpAge 6010 6E 00 31 00 37 00 20 0 1. 7 StartpAge 6018 30 00 31 00 38 60 2. 0 . 1 . 8 . StreamMRU 628 2D 00 73 00 65 00 e. s . t . e . 6030 65 00 73 00 65 00 e. s . t . e . StreamS 6030 65 00 73 00 74 00 65 00<					>	RecentDocs		88 103		REG	BINAR	v	41.00	73 00 7	3 00 69 00	0 67 00 6e 00 6d 00 65 00 6e	00 74 00
Ribbon Edit Binary Value X RunMRU Search Value name: X SearchPlatform SearchPlatform 103 X SessionInfo Value data: Value data: Value data: V StartPage 0010 6E 00 73 00 69 00 A. s . s . s . i . A. s . s . s . i A. s . s . s . i						RestartComma	nds			THE O	DUNKIN		4100	15 00 1.	5 00 05 00		
						Ribbon	Edit Binary	Value									- × (
Search Value name: SearchPlatform 103 SessionInfo SessionInfo SessionInfo Value data: Shell Folders 0000 41 00 73 00 69 00 A . s . s . s . i . A Shell Folders 0000 41 00 73 00 69 00 A . s . s . s . i . A Shutdown 0008 67 00 6E 00 6D 00 65 00 g . n . m . e . A StartPage 0010 6E 00 74 00 2D 00 32 00 n . t 2 . StartupApprov 0018 30 00 31 00 38 00 2.0 1 . 8 . StreamMRU 0028 2D 00 73 00 65 00 e . s . t . e . . Streams 0030 65 00 73 00 74 00 65						RunMRU											
SearchPlatform 103 SessionInfo SessionInfo Shell Folders 0000 41 00 73 00 69 00 A.ss.ss.i. A.ss.ss.i. Shutdown 0008 67 00 6E 00 6D 00 65 00 g.n.m.e.e. StartPage 0010 6E 00 74 00 2D 00 32 00 n.t.r 2. StartupApprov 0018 30 00 31 00 38 00 2. 0.1.r.7 8. StreamMRU 0020 32 00 31 00 65 00 60 00 1.s. 8. Streams 0030 65 00 73 00 65 00 e.s.t.e.m. 9038 72 00 20 20 20 7 2 1 8. 1 9 Streams 0030 65 00 73 00 74 00 65 00 e.s.t.t.e. 9 1					>	Search	Value name	e									2
SessionInfo Value data: Shell Folders 0000 41 00 73 00 69 00 A . s . s . i . 000 A . s . s . i . 0000 A . s . s . i . 0000 A . s . s . i . 0000 A . s . s . i . 0000 A . s . s . i . 0000 A . s . s . s . i . 0000 A . s . s . s . i . 0000 A . s . s . s . i . 0000 0000 A . s . s . s . i . 0000 A . s . s . s . i . 0000 A . s . s . s . i . 0000 A . s . s . s . i . 0000 A . s . s . s . i . 0000 A . s . s . s . i . 0000 A . s . s . s . i . 0000 A . s . s . s . i . 0000 A . s . s . s . i . 0000 A . s . s . s . i . 0000 A . s . s . s . i . 0000 A . s . s . s . i . 0000 A . s . s . s . i . 0000 A . s . s . s . s . i . s . s . s . i . 0000 A . s . s . s . s . s . s . s . s . s .					>	SearchPlatform	103										
Shell Folders 0000 41 00 73 00 73 00 69 00 A . s . s . i . Shutdown 0008 67 00 6E 00 6D 00 65 00 g . n . m . e . StattPage 0010 6E 00 74 00 2D 00 32 00 n . t 2 . . StattupApprov 0018 30 00 31 00 37 00 6D 00 0 1. 7 . StreamMRU 0020 32 00 73 00 65 00 0 1. 7 . StreamS 0020 32 00 73 00 65 00 0 1. 7 StreamS 0030 65 00 73 00 65 00					>	SessionInfo	Value data:										}
Shutdown 0000 41 00 73 00 73 00 69 00 A . s . s . 1 . Shutdown 0008 67 00 6E 00 6D 00 65 00 g . n . m . e . StartPage 0010 6E 00 74 00 2D 00 32 00 n . t 2 . StartupApprov 0018 30 00 31 00 37 00 2D 00 0 1 . 7 StreamMRU 0020 32 00 73 00 65 00 0 1 . 7 StreamMRU 0028 2D 00 73 00 65 00 00						Shell Folders		44		72		72)
StartPage 0000 00 00 01 00 01 00 01 00 01 00 01 00 02 00 02 00 n <td< th=""><th></th><th></th><th></th><th></th><th></th><th>Shutdown</th><th>0000</th><th>41</th><th>00</th><th>/3 6E</th><th>00</th><th>73 6D</th><th>00</th><th>69</th><th>00</th><th>A.S.S.1. g p m e</th><th></th></td<>						Shutdown	0000	41	00	/3 6E	00	73 6D	00	69	00	A.S.S.1. g p m e	
StartupApprov 0018 30 00 31 00 37 00 2D 00 0 1.7 StreamMRU 0020 32 00 30 00 31 00 38 00 2.0.1 1.8 . StreamMRU 0028 2D 00 73 00 65 00 00 ss.e.m. Streams 0030 65 00 73 00 74 00 65 00 e.ss.t.e. m. StuckRects2 0038 72 00 20 00 32 00 20 00 2.0 c.s.t.e.						StartPage	0010	6F	00	74	00	20	00	32	00	g	e
StreamMRU 0020 32 00 30 00 31 00 38 00 2 0 1 8 Stream 0028 2D 00 73 00 65 00 6D 00 - .s .e m Streams 0030 65 00 73 00 74 00 65 00 e .s .t .e . StuckRects2 0038 72 00 20 00 32 00 2E 00 r .e . .e .e<					5	StartupApprov	0018	30	00	31	00	37	00	2D	00	0.1.7	
Streams 0028 2D 00 73 00 65 00 6D 00 s.e.m. Streams 0030 65 00 73 00 74 00 65 00 e.s.t.e. Streams 0038 72 00 20 00 32 00 2E 00 r2.i.					1	StreamMRU	0020	32	00	30	00	31	00	38	00	2.0.1.8.	
Observe Observe <t< th=""><th></th><th></th><th></th><th></th><th></th><th>Streams</th><th>0028</th><th>2D</th><th>00</th><th>73</th><th>00</th><th>65</th><th>00</th><th>6D</th><th>00</th><th>s.e.m.</th><th></th></t<>						Streams	0028	2D	00	73	00	65	00	6D	00	s.e.m.	
Stuckhetts2 0038 72 00 20 00 32 00 2E 00 r 2.,					1	StuckRects?	0030	65	00	73	00	74	00	65	00	e.s.t.e.	ĺ.
						StuckRocts2	0038	72	00	20	00	32	00	2E	00	r2	ľ
						Taskhand	0040	64 86	00	32	00	65	00	00	00	¶ 2	1
					2	Taskoand	0050	00	00	00	00	00	00	41	73	J A <	2
19pedraths 19458 73 69 67 6F 6D 65 6F 74 signment						TypedPaths	0058	73	69	67	6F	60	65	6F	74	sionment	× 1
User Shell Fold						User Shell Fold										OK Can	al
UserAssist					2	UserAssist										Can	

Figure 3.17: In depth Information for a Particular File