Amal Jyothi College of Engineering
Kanjirappally, Kerala

MAGIC RESCUE

MCA SEMINAR REPORT

Submitted in the partial fulfillment of the requirements for the Award of the Degree in

Master of Computer Applications

By

SHARON KURIAN

Reg. No.:LAJC17MCA038

Under The Guidance Of

Ms. DILU MARIYA JOSEPH

November 2019

DEPARTMENT OF COMPUTER APPLICATIONS
AMAL JYOTHI COLLEGE OF ENGINEERING
KANJIRAPPALLY

CERTIFICATE

This is to certify that the seminar report, "**MAGIC RESCUE"** is *the bonafide work of* **SHARON KURIAN** (Reg.No: LAJC17MCA038) *in partial fulfillment of the requirements for the award of the Degree of Master of Computer Applications under APJ Abdul Kalam Technological University during the year 2019.*

Ms. Dilu Mariya Joseph
Internal Guide

Ms. Shelly Shiju George
Coordinator

Fr. Rubin Thottupuram
Head of the Department

ACKNOWLEDGEMENT

First and foremost, I thank God Almighty for his eternal love and protection throughout the seminar, I take this opportunity to express my gratitude to all who helped me in completing this seminar successfully. It has been said that gratitude is the memory of heart. I wish to express my sincere gratitude to our Manager **Rev. Fr. Dr. Mathew Paikatt** and our Principal **Dr. Z. V. Lakaparambil** for providing good faculty for guidance.

I owe a great depth of gratitude towards our Head of the Computer Application Department **Fr. Rubin Thottupuram** for helping me. I extend my whole hearted thanks to the Seminar Coordinator **Ms. Shelly Shiju George** for her valuable suggestions and for overwhelming concern and guidance from the beginning to the end of the Seminar. I would also like to express sincere gratitude to my Guide**, Ms. Dilu Mariya Joseph** for her inspiration and helping hand.

I thank to our beloved teachers for their corporation and suggestions that helped me throughout the seminar. I express my thanks to all my friends and classmates for their interest ,dedication, and encouragement shown towards the seminar. I convey my family for the moral support ,suggestions, and encouragement to make this venture a success.

Sharon Kurian

ABSTRACT

Magic rescue is an open source utility for recovering data after logical corruption, accidental deletion or even repairing damaged files. It is a command line tool. It has proved to be one of the most reliable, in fact, it's so reliable that it continues to be carried by most major distributions despite the fact that it has been unmaintained for several years. A day will probably come when it is obsolete, but, meanwhile, it remains a standard recovery tool.

Magic Rescue works by reading a file's magic bytes or magic pattern – that is, the unique signature that designates each file type. This signature is often, but not always, within the very first bites of a file. If it is not, then you can use a hex editor to find it. It is mostly used by the file command, often behind the scenes. Magic Rescue uses it's collection of recipes to recognize the magic bytes in all deleted files of a particular type then saves deleted files to an output directory where they can be sorted

CONTENTS

1. INTRODUCTION

1.1 KALI LINUX

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. It was developed by Mati Aharoni and Devon Kearns of offensive security through the rewrite of Backtrack, their previous information security testing Linux distribution based on Knoppix. The third core developer Raphael Hertzog joined them as a Debian expert. Kali Linux was released on the 13th march, 2013 as a complete ,top to bottom. Rebuild of Backtrack Linux, adhering completely to Debian development standards.

Kali Linux is one of the best open-source security packages of an ethical hacker, containing a set of tools divided by categories. Kali Linux can be installed in a machine as an Operating System. Installing Kali Linux is a practical option as it provides more options to work and combine the tools.

- Provides More than 600 penetrating testing tools.
- OS Family –Unix Like
- Working State- Active
- Platform –x86,x86-64,armel,armhf
- Kernel Type-Monolithic kernel (Linux)
- Default UI –GNOME3

1.2 PENETRATION TESTING

Penetration testing, also called pen testing or ethical hacking, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit. Penetration testing can be automated with software applications or performed manually. Either way, the process involves gathering information about the target before the test, identifying possible entry points, attempting to break in -- either virtually or for real -- and reporting back the findings.

The main objective of penetration testing is to identify security weaknesses. Penetration testing can also be used to test an organization's security policy, its adherence to compliance requirements, its employees' security awareness and the organization's ability to identify and respond to security incidents. Penetration tests are also sometimes called white hat attacks because in a pen test, the good guys are attempting to break in.

Purpose of penetration testing

The primary goal of a pen test is to identify weak spots in an organization's security posture, as well as measure the compliance of its security policy, test the staff's awareness of security issues and determine whether -- and how -- the organization would be subject to security disasters.

Penetration test strategies

- Targeted Testing - Testing team working together.
- External Testing - Targets externally visible servers or devices.
- Internal Testing - Attack behind the firewall.
- Blind Testing - Simulates the actions of a real attacker.

Targeted testing is performed by the organization's IT team and the penetration testing team working together. It's sometimes referred to as a "lights turned on" approach because everyone can see the test being carried out.

External testing targets a company's externally visible servers or devices including domain name servers, email servers, web servers or firewalls. The

objective is to find out if an outside attacker can get in and how far they can get in once they've gained access.

Internal testing mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause.

Blind testing simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team performing the test beforehand. Typically, the pen testers may only be given the name of the company. Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive.

Benefit of Penetration Testing

- Intelligently manage vulnerabilities.
- Avoid the cost of network downtime.
- Meet regulatory requirements and avoid fines.
- Preserve corporate image and customer loyalty.

1.3 DIGITAL FORENSICS

Keeping in mind that forensics is a science, digital forensics requires that one follow appropriate best practices and procedures in an effort to produce the same results time and time again providing proof of evidence, preservation, and integrity which can be replicated ;if called upon to do so.

Although many people may not be performing digital forensics to be used as evidence in a court of law, it is best to practice in such a way as can be accepted and presented in a court of law. The main purpose of adhering to best-practices set by organizations specializing in digital forensics and incident response is to maintain the integrity of the evidence for the duration of the investigation. In the event that the investigator's work must be scrutinized and critiqued by another or an opposing party, the results found by the investigator must be able to be recreated, thereby proving the integrity of the investigation. The purpose of this is to ensure that your methods can be repeated and, if dissected or scrutinized, produce the same results time and again.

2. MAGIC RESCUE

2.1 INTRODUCTION TO MAGIC RESCUE

Magic rescue is an open source utility for recovering data after logical corruption, accidental deletion or even repairing damaged files. It is a command line tool. The user doesn't need to know about data recovery techniques. Although this is a text only tool, the command line is simplistic to use. Menus are logically presented and the language easy to understand. Navigation is easy using the up, down, left and right cursor.

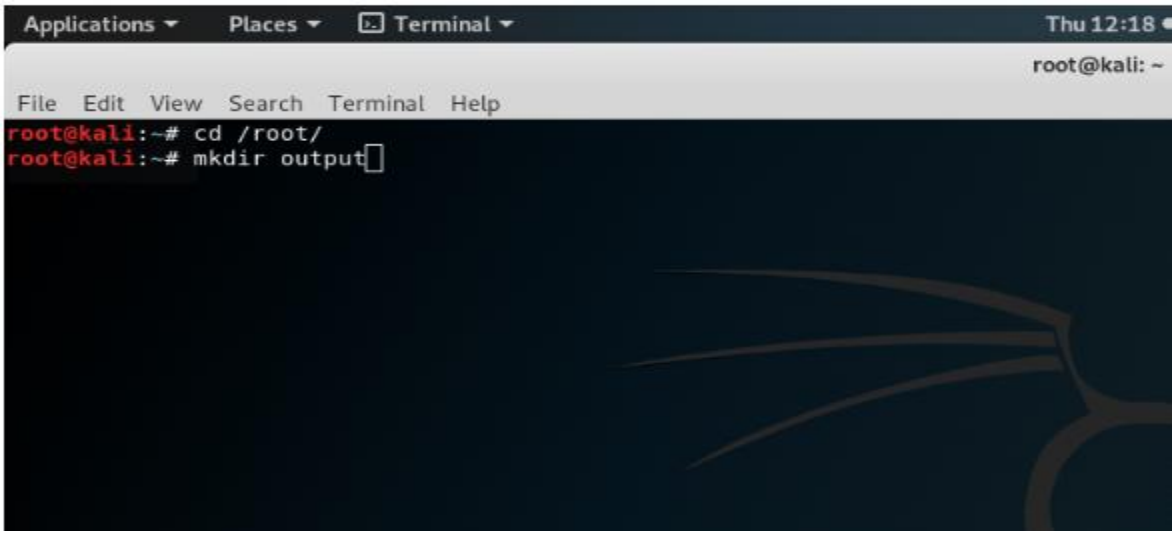
Magic Rescue works by reading a file's magic bytes or magic pattern- that is, the unique signature that designates each file type. This signature is often, but not always, within the very first bites of a file. It is mostly used by the file command, often behind the scenes. Magic Rescue uses its collection of recipes to recognize the magic bytes in all deleted files of a particular type then saves deleted files to an output directory where they can be sorted.

2.2 SETTING UP

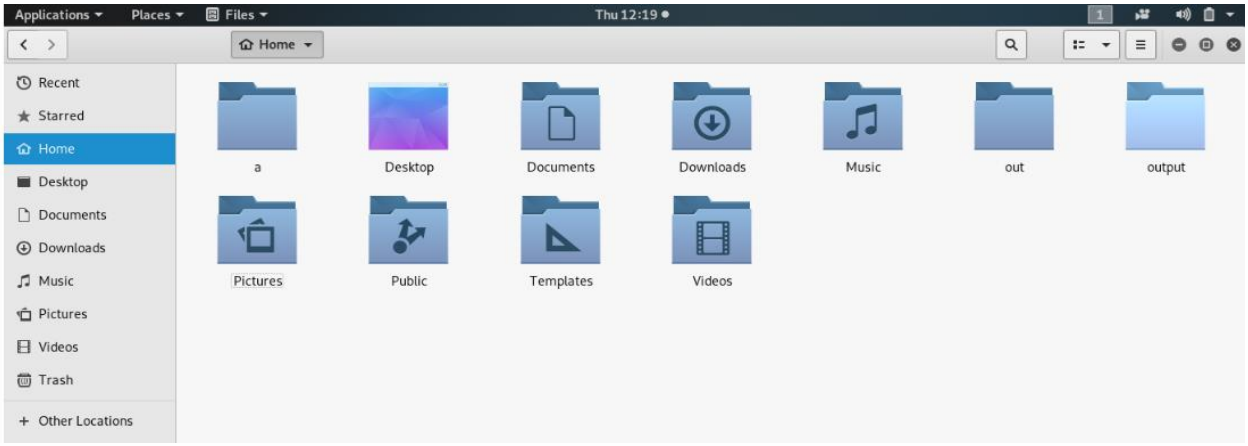
Before you start to use Magic Rescue, you need two things:

- A directory to hold recovered files

  Create a directory : $mkdir directoryname



The output folder is created in root folder



To prevent feedback loops that can trash the system and possibly overwrite the files you are trying to recover, the directory should not be on the block device you are searching. If your system only has one partition, consider mounting a flash drive or external hard drive to hold the directory. If you have multiple partitions, you need to make sure that the directory is on a partition that has as much free space as you need for the recovered files.

- A recipe file

A recipe file is a small script that recognizes the characteristic pattern of a file format's header. If you are familiar with different file types, use the recipes installed with Magic Rescue in /usr/share/magicrescue/recipes, or search the Internet for a specific recipe. The latest version comes with recipes for identifying avi, elf, gimp-xcf, gzip, jpeg, mp3, Microsoft office, perl, png and zip files, as well as Open Office.org files, and files with the GNU General Public License in the header. These recipes are also useful as examples if you need to write your own recipe.

Recipes

- Where offset is a decimal integer saying how many bytes from the beginning of the file this data is located, operation refers to a built-in match operation in magicrescue ,and parameter is specific to that operation.

- String: The parameter is a character sequence that may contain escape sequence such as \xFF
- Char: A parameter is single charactered byte or escape sequence.
- Int32: Both value and bitmask are expressed as 8 character hex strings. Bitmask will be ANDed with the data, and the result will be compared to value. The byte order is as you see it in the hex editor ie big-endian.
- Extension ext: Mandatory, specify extension eg: jpg
- Command: mandatory, when all the match operation succeed, this command will be executed to extract the file from the block device. Command is passed to the shell with the device's file descriptor(to the right byte) on stdin. The shell $1 will contain the file its output should written to and it must respect this. Otherwise magicrescue cannot tell whether it succeeded.
- Rename: used to rename to something more meaningful.

1 Min_output_file(size): default 100 output file less than this will be deleted.

2 #Extracts jpeg files with the JFIF magic bytes. These are usually created by #graphics manipulation programs.

Depends on jpegtran from libjpeg: http://freshmeat.net/projects/libjpeg/

To find formatted external device go to

terminal → $fdisk –l

```
Applications ▾   Places ▾   Terminal ▾                                Thu 12:23 ●
                                                                     root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# fdisk -l
Disk /dev/sda: 931.5 GiB, 1000204886016 bytes, 1953525168 sectors
Disk model: WDC WD10JPVX-60J
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disklabel type: dos
Disk identifier: 0xfc515ad7

Device     Boot      Start        End    Sectors   Size Id Type
/dev/sda1  *          2048    1026047    1024000   500M  7 HPFS/NTFS/exFAT
/dev/sda2          1026048  171763711  170737664  81.4G  7 HPFS/NTFS/exFAT
/dev/sda3        171763712 1840273407 1668509696 795.6G  7 HPFS/NTFS/exFAT
/dev/sda4       1840275454 1953523711  113248258    54G  5 Extended
/dev/sda5       1840275456 1945307135  105031680  50.1G 83 Linux
/dev/sda6       1945309184 1953523711    8214528   3.9G 82 Linux swap / Solaris

Partition 4 does not start on physical sector boundary.

Disk /dev/sdb: 7.6 GiB, 8110768128 bytes, 15841344 sectors
Disk model: v210w
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: dos
Disk identifier: 0x9b16c420

Device     Boot Start      End  Sectors  Size Id Type
/dev/sdb1  *     2048 15841279 15839232  7.6G  c W95 FAT32 (LBA)
root@kali:~#
```

2.3 BASIC OPTIONS

- **-b option:** Using this option you can usually get better performance, but fewer files will be found. In particular, files with leading garbage (eg: many mp3 files) and files contained inside other files are likely to be skipped. Also, some file systems don't align small files to block boundaries. So those won't be found this way either,

  If you don't know your file system's block size ,just use the value 512,which is almost always the hardware sector size.

- **-d directory**: Specify directory to store recovery files.

- **-r recipe:** Mandatory, Recipe name, file or directory. Specify this as either a plain name (eg. Jpeg-jfif)or path (eg.recipes/jpeg-jfif). If it doesn't find such a file in the current directory, it will look in ./recipes and PREFIX/share/magicrescue/recipes, where PREFIX is the path you installed to eg. /usr/local.

  If recipe is a directory, all files in that directory will be treated as recipes.

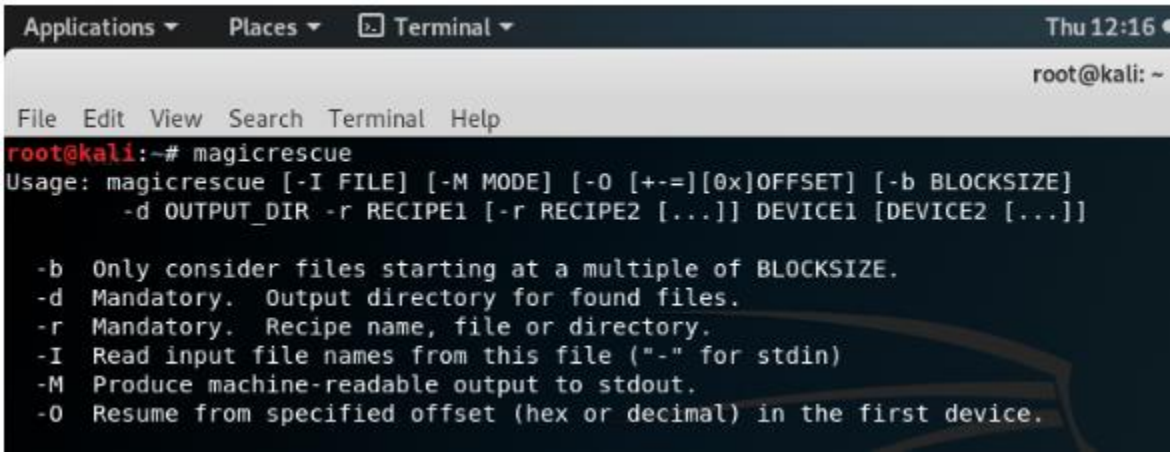
- **-M** : Produce machine-readable output to stdout.

- **-o** : Resume from specified offset (hex or decimal) in the first device.

2.4 WORKING OF MAGIC RESCUE

- To see all the options in Magic Rescue.

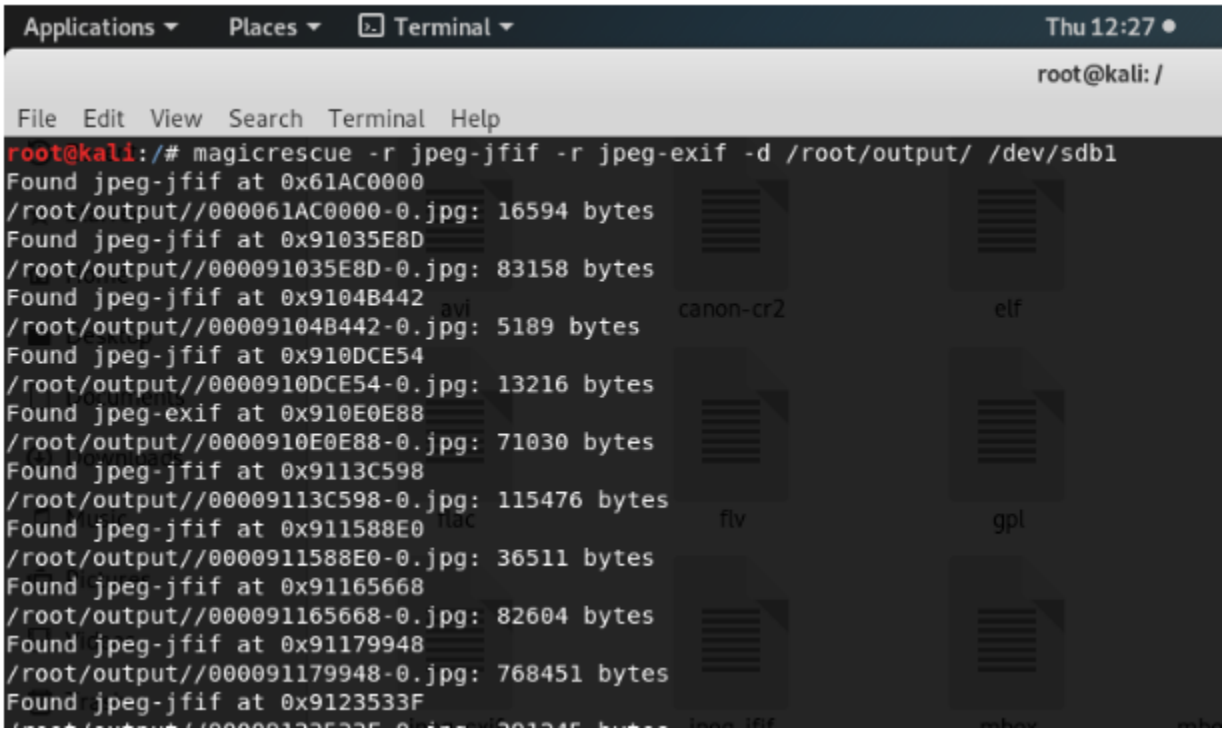
  $magicrescue



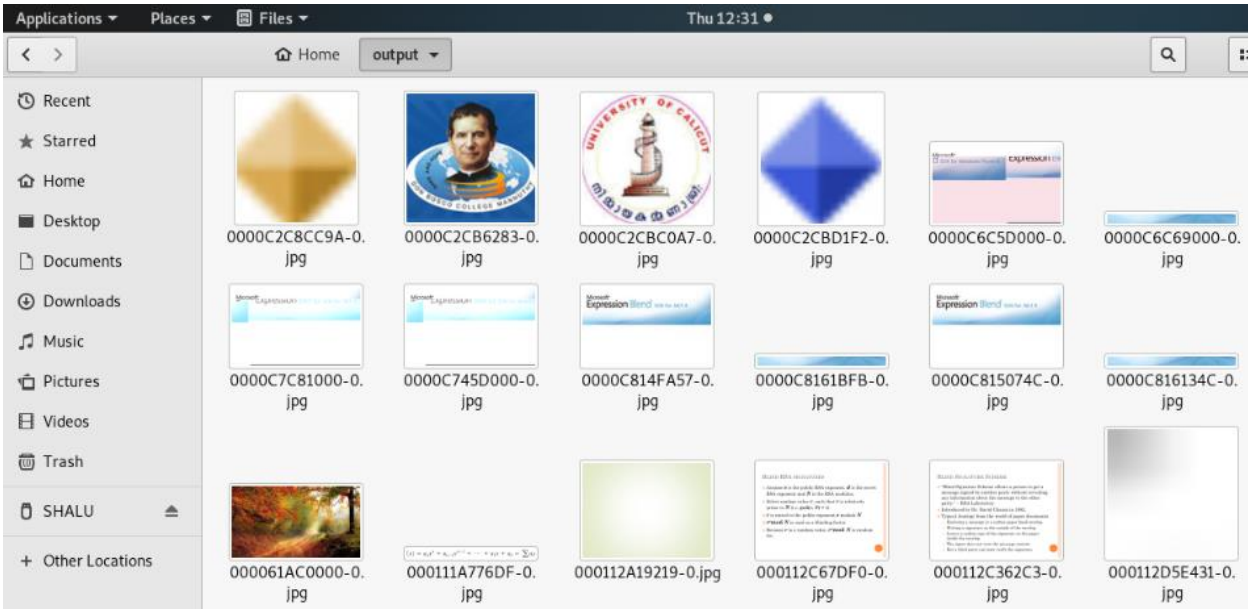
- $magicrescue –r jpeg-jfif –r jpeg-exif –d /root/output/ /dev/sdb1

  -r : Recipe name, file or directory.

  -o : output file name.



The recovered images can be seen in output directory.



2.5 UTILITIES AFTER SEARCH

The -O parameter is especially useful if you have to use Ctrl-C to interrupt a long search. If you note the current position of search , you can use -O = position or position to continue the search later from the position where it stopped. Magicrescue includes utilities in /usr/share/magicresue/tools.

By using the command dupemap delete resultdirectory ,you can eliminate all duplicate files in your result directory.

Alternatively, magicsort resultdirectory uses the file command to move each unique result in the directory to a separate file directory.

2.6 ADVANTAGES AND DISADVANTAGES

- Avoid duplication files.
- Although subject to certain limitations, such as how recently a file was deleted and the availability of a definition for the header of a given format.

3. RECOVERY OF .txt EXTENSION FILES

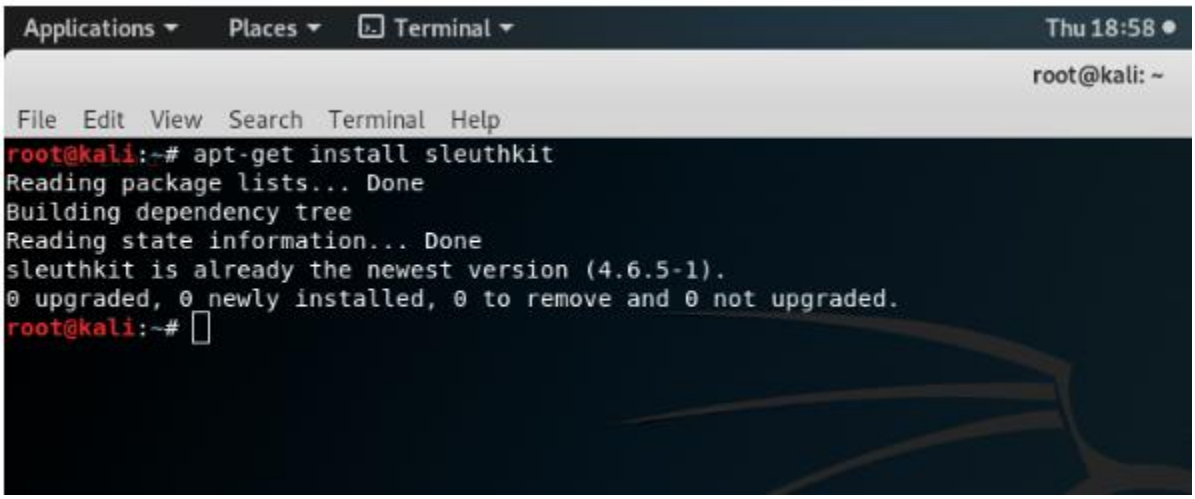
SLEUTHKIT is a recovery tool which is used to recover the .txt files which are deleted from the USB devices such as pendrives or memory cards. It is used in computer forensic for the recovery of text files. Sleuthkit is a C library and collection of command line file and volume system forensic filesystem analysis. One of the most basic use-cases is the recovery of files that have been deleted.

Commands Used:

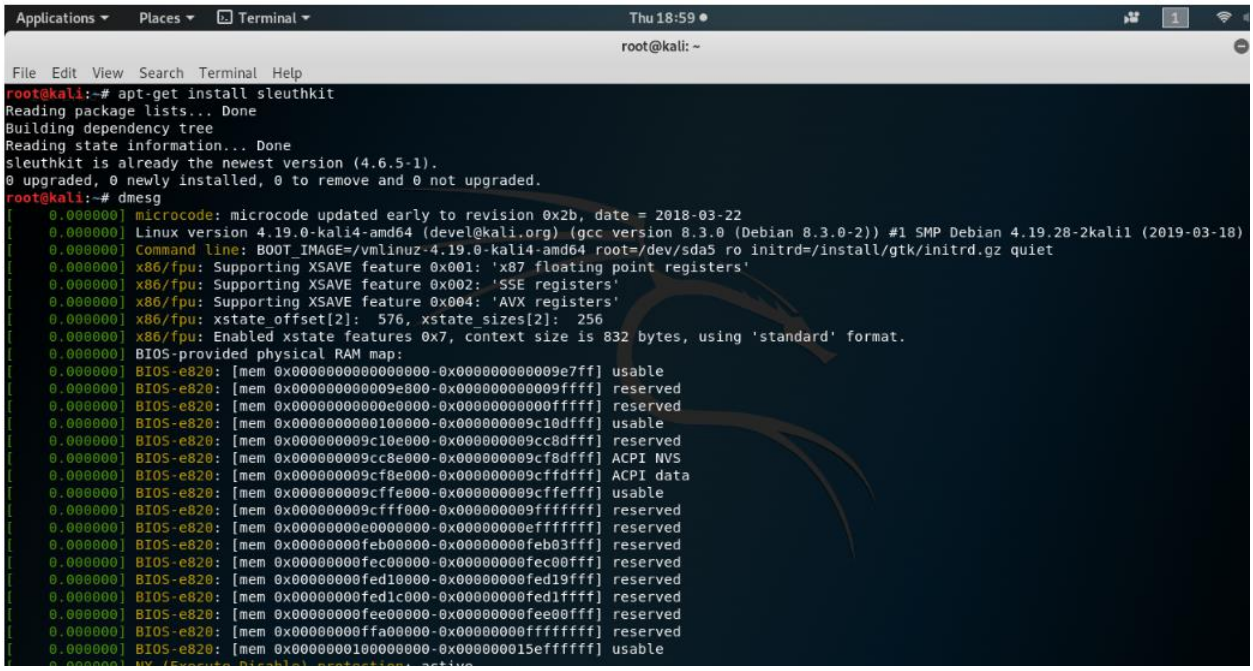
- apt –get install sleuthkit
- dmesg
- ls/dev/sdb
- mmls/dev/sdb
- fsstat –o 32/dev/sdb
- fls –o 32/dev/sdb
- icat –o 32/dev/sdb 10

3.1 WORKING

- Installing the sleuthkit
  apt-get install sleuthkit



- To write the kernel message in Linux
  dmseg



- Listing the hard disk detected
  ls /dev/sdb.

```
[  894.063696]  sdb: sdb1
[  894.068944] sd 2:0:0:0: [sdb] Attached SCSI removable disk
[ 4172.112382] usb 2-3: USB disconnect, device number 4
[ 4174.234999] usb 2-3: new high-speed USB device number 5 using xhci_hcd
[ 4174.449957] usb 2-3: New USB device found, idVendor=03f0, idProduct=5607, bcdDevice= 2.00
[ 4174.449963] usb 2-3: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[ 4174.449967] usb 2-3: Product: v210w
[ 4174.449971] usb 2-3: Manufacturer: HP
[ 4174.449974] usb 2-3: SerialNumber: 201507077160000000000EFD
[ 4174.451570] usb-storage 2-3:1.0: USB Mass Storage device detected
[ 4174.452939] scsi host2: usb-storage 2-3:1.0
[ 4175.457157] scsi 2:0:0:0: Direct-Access     hp       v210w            1100 PQ: 0 ANSI: 4
[ 4175.457817] sd 2:0:0:0: Attached scsi generic sg2 type 0
[ 4175.459385] sd 2:0:0:0: [sdb] 15841344 512-byte logical blocks: (8.11 GB/7.55 GiB)
[ 4175.461021] sd 2:0:0:0: [sdb] Write Protect is off
[ 4175.461029] sd 2:0:0:0: [sdb] Mode Sense: 23 00 00 00
[ 4175.462651] sd 2:0:0:0: [sdb] Write cache: disabled, read cache: enabled, doesn't support DPO or FUA
[ 4175.471843]  sdb: sdb1
[ 4175.477297] sd 2:0:0:0: [sdb] Attached SCSI removable disk
root@kali:~# ls /dev/sdb
/dev/sdb
root@kali:~#
```

- To display the partition table layout of a volume system (partition tables)
  mmls /dev/sdb

```
root@kali:~# ls /dev/sdb
/dev/sdb
root@kali:~# mmls /dev/sdb
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0015841279   0015839232   Win95 FAT32 (0x0c)
003:  -------   0015841280   0015841343   0000000064   Unallocated
root@kali:~#
```

- To display general details of a file system
  fsstat –o *2048* **/dev/sdb**

```
Applications ▾   Places ▾   Terminal ▾                    Thu 19:02 ●
                                                          root@kali: ~
File  Edit  View  Search  Terminal  Help
003:   0015841280   0015841343   0000000064   Unallocated
root@kali:~# fsstat -o 2048 /dev/sdb
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT32

OEM Name: MSDOS5.0
Volume ID: 0x3cf4abaf
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory): SHALU
File System Type Label: FAT32
Next Free Sector (FS Info): 1141968
Free Sector Count (FS Info): 13549544

Sectors before file system: 2048

File System Layout (in sectors)
Total Range: 0 - 15839231
* Reserved: 0 - 1893
** Boot Sector: 0
** FS Info Sector: 1
** Backup Boot Sector: 6
* FAT 0: 1894 - 17330
* FAT 1: 17331 - 32767
* Data Area: 32768 - 15839231
** Cluster Area: 32768 - 15839231
*** Root Directory: 32768 - 32775

METADATA INFORMATION
--------------------------------------------
Range: 2 - 252903430
Root Directory: 2

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 2 - 1975809
```

- To display file names of recently deleted files

  fls –o 2048 /dev/sdb

```
root@kali:~# fls -o 2048 /dev/sdb
r/r 3:  SHALU       (Volume Label Entry)
d/d 6:  System Volume Information
d/d 7:  1
r/r * 9:        .goutputstrea
d/d 11: .Trash-0
r/r * 14:       ASSIGNMEN1.docx
r/r * 17:       .goutputstream-RERV8Z
r/r 19: Foremost.docx
r/r 24: IT 2[2019]HQ DVDScr -Multi Auds1.1GB.mkv
r/r 30: Irupathiyonnaam Noottaandu [Malayalam]2019 @MZ_MOVIES.mkv
r/r 35: [FILM CITY]-Brothers.Day.2019.Mala.PreDVD.1.4GB.mkv
r/r 40: 2001360_July_Kaatril__2019__HDRip_400MB.mkv
r/r 46: Dear.Zindagi.2016.720p.DvDRip.x264-NBY-[moviezplanet.org].mkv
r/r 47: BOOTEX.LOG
r/r * 50:       magicrescue xseminar.docx
r/r * 51:       _WRD2356.tmp
r/r 54: magicrescue xseminar.docx
v/v 252903427:  $MBR
v/v 252903428:  $FAT1
v/v 252903429:  $FAT2
V/V 252903430:  $OrphanFiles
root@kali:~#
```

- To output the contents of file:

  icat –o 2048 /dev/sdb 13

```
?>root@kali:~/Desktop# icat -o 32 /dev/sdb 60
magicrescude
root@kali:~/Desktop#
```

4. CONCLUSION

Magic rescue is an open source utility for recovering data after logical corruption, accidental deletion or even repairing damaged files. It is not meant to be a universal application for file recovery. It will give good results when you are extracting known file types from an unusable file system.

5. REFERENCE

- http://www.linux.com/news/when-files-disappear-magic-rescue-saves-day
- http://www.irongeek.com/i.php?page=backtrack-3-man/magicrescue
- http://www.linux-magazine.org/sleuthkit.org/man/icat.html