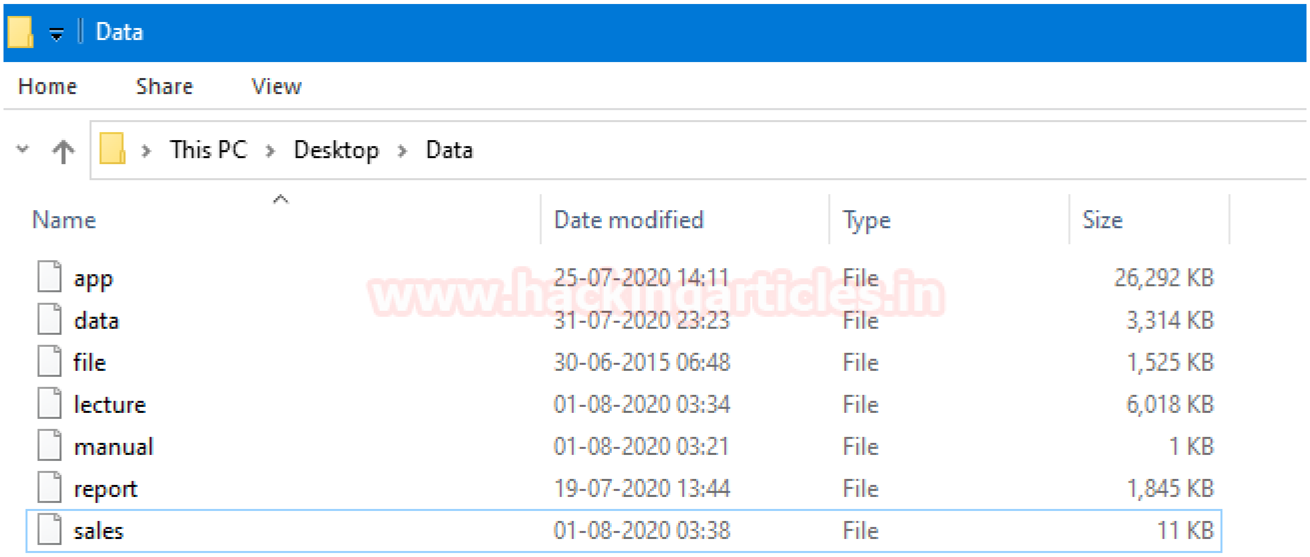
Forensic Investigation: Examine Corrupt File Metadata

August 11, 2020 By Raj Chandel

In this article, we will learn how we can examine a corrupt file with the help of Exiftool to get ahead in a forensic investigation.

Let’s understand a scenario

In this Scenario, a forensic investigator is stuck in a situation. He gets a suspicious folder, where no file has any kind of file extension.



Name	Date modified	Type	Size
app	25-07-2020 14:11	File	26,292 KB
data	31-07-2020 23:23	File	3,314 KB
file	30-06-2015 06:48	File	1,525 KB
lecture	01-08-2020 03:34	File	6,018 KB
manual	01-08-2020 03:21	File	1 KB
report	19-07-2020 13:44	File	1,845 KB
sales	01-08-2020 03:38	File	11 KB

www.hackingarticles.in

Now, he has two options.

1. Examine each file’s hexadecimal values to determine the file type. To know more about this option click here.
2. Extract metadata of the file.

In this article, we will cover the second option. Extract metadata of the file.

Objective: Learn to use the Exiftool metadata extractor in a forensic investigation to examine corrupt files.

Table of Content

- File #4: lecture
- File #5: manual
- File #6: report
- File #7: sales

Conclusion

Introduction to ExifTool

It is an open-source software to reading, writing, and manipulating [image, audio, video, and PDF metadata]. Which is developed by Phil Harvey. It is platform-independent based on Perl library plus a command-line application.

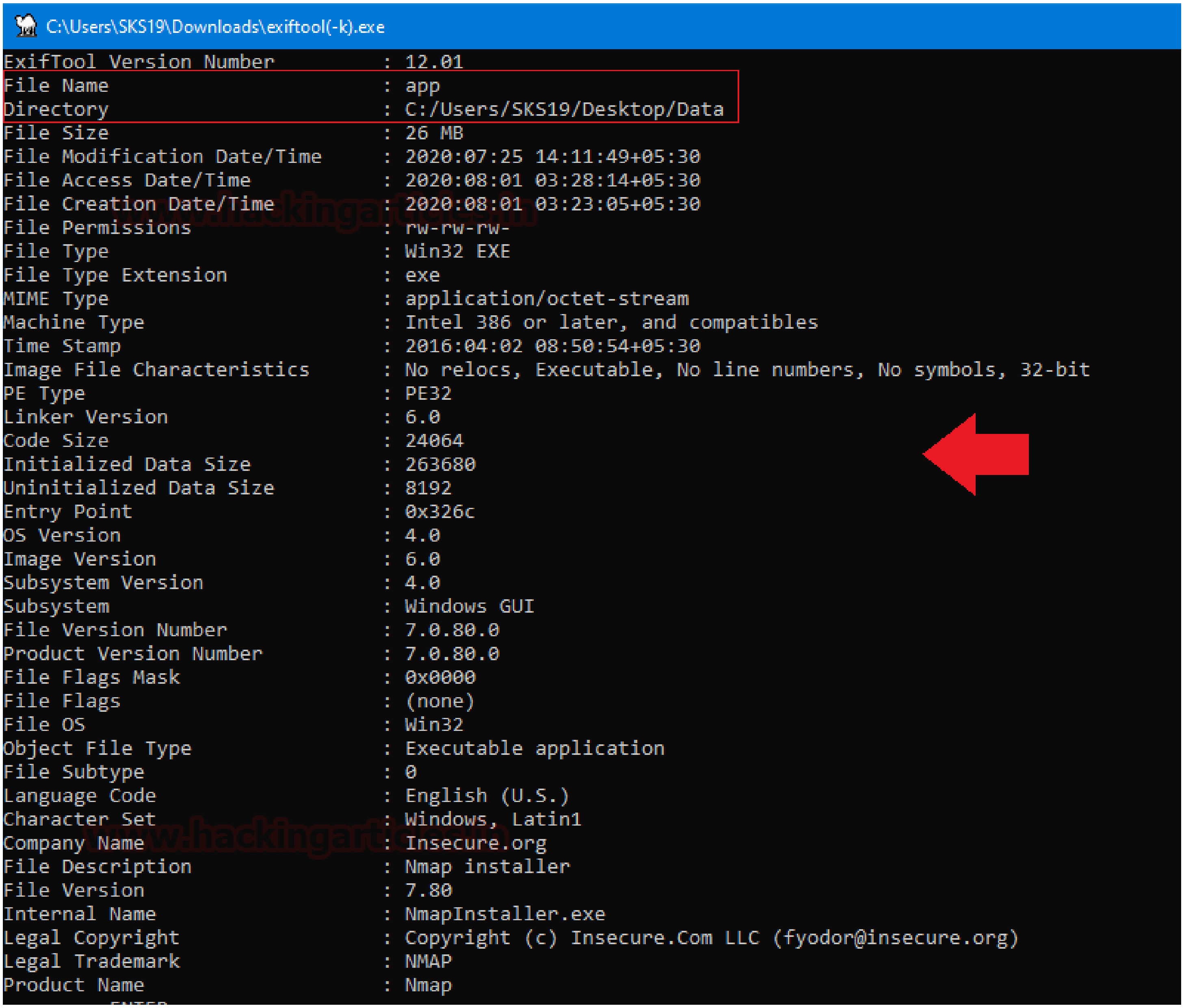
It supports different-different metadata formats including GPS, IPTC, EXIF, XMP, JFIF, ID3, etc. It also gets some maker notes of many digital cameras.

It is also available for Windows and macOS package, that does not require Perl setup. We just need to download and unzip the archives then double click on a file to load the software.

We can download this software from **here**.

File #1: app

The First file we got is app. Now, all we need to get its metadata **drag and drop** this corrupt file on the ExifTool .exe file. which name is ‘**exiftool(-k).exe’** in the archive file which we just unzipped.



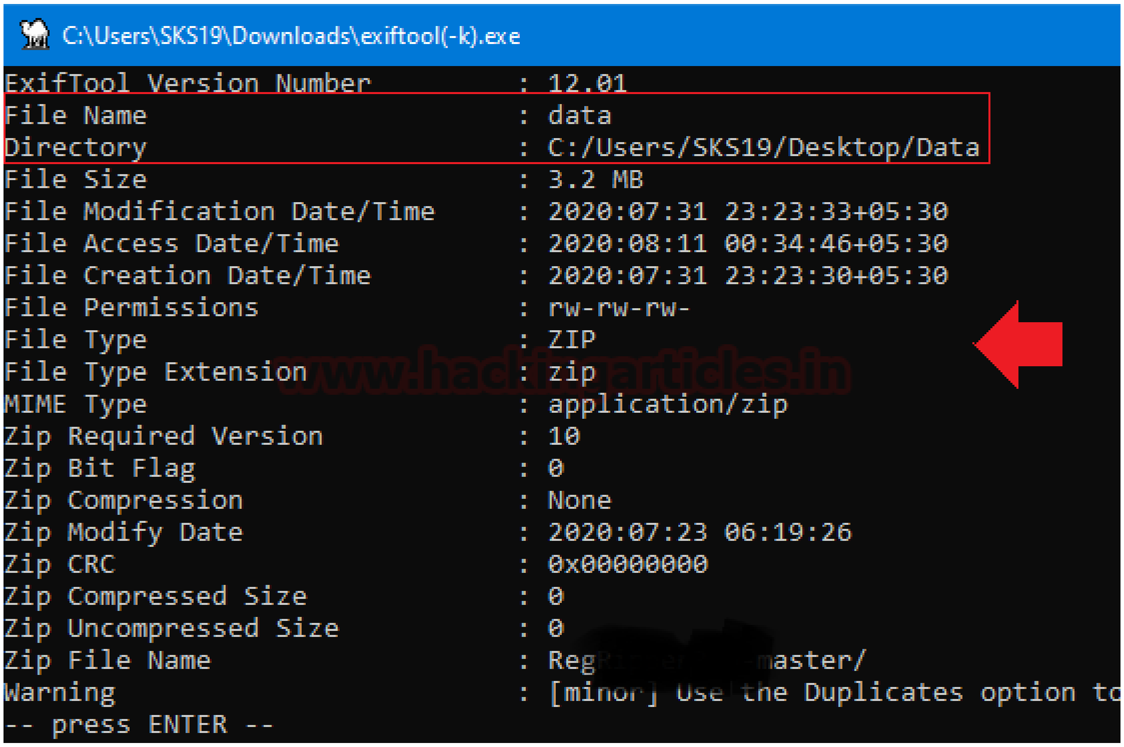
```
ExifTool Version Number         : 12.01
File Name                       : app
Directory                       : C:/Users/SKS19/Desktop/Data
File Size                       : 26 MB
File Modification Date/Time     : 2020:07:25 14:11:49+05:30
File Access Date/Time           : 2020:08:01 03:28:14+05:30
File Creation Date/Time         : 2020:08:01 03:23:05+05:30
File Permissions                : rw-rw-rw-
File Type                       : Win32 EXE
File Type Extension             : exe
MIME Type                       : application/octet-stream
Machine Type                    : Intel 386 or later, and compatibles
Time Stamp                      : 2016:04:02 08:50:54+05:30
Image File Characteristics      : No relocs, Executable, No line numbers, No symbols, 32-bit
PE Type                         : PE32
Linker Version                  : 6.0
Code Size                       : 24064
Initialized Data Size           : 263680
Uninitialized Data Size         : 8192
Entry Point                     : 0x326c
OS Version                      : 4.0
Image Version                   : 6.0
Subsystem Version               : 4.0
Subsystem                       : Windows GUI
File Version Number             : 7.0.80.0
Product Version Number          : 7.0.80.0
File Flags Mask                 : 0x0000
File Flags                      : (none)
File OS                         : Win32
Object File Type                : Executable application
File Subtype                    : 0
Language Code                   : English (U.S.)
Character Set                   : Windows, Latin1
Company Name                    : Insecure.org
File Description                : Nmap installer
File Version                    : 7.80
Internal Name                   : NmapInstaller.exe
Legal Copyright                 : Copyright (c) Insecure.Com LLC (fyodor@insecure.org)
Legal Trademark                 : NMAP
Product Name                    : Nmap
```

As we have captured a few interesting details in this screenshot which helps us in our forensic investigation.

Information	Value
File Name	app
File Directory	C:/Users/SKS19/Desktop/Data
File Size	26 MB
File Modification	2020:07:25 14:11
File Access	2020:08:01 03:28
File Creation	2020:08:01 03:23
File Permissions	rw-rw-rw-
File Type	Win32 EXE
File Description	NMAP
File Version	7:80

File #2: data

The Second file we got is data. Repeat the previous step, to get metadata of this file **drag and drop** this corrupt file on the [exiftool(-k).exe] in the archive file which we just unzipped.

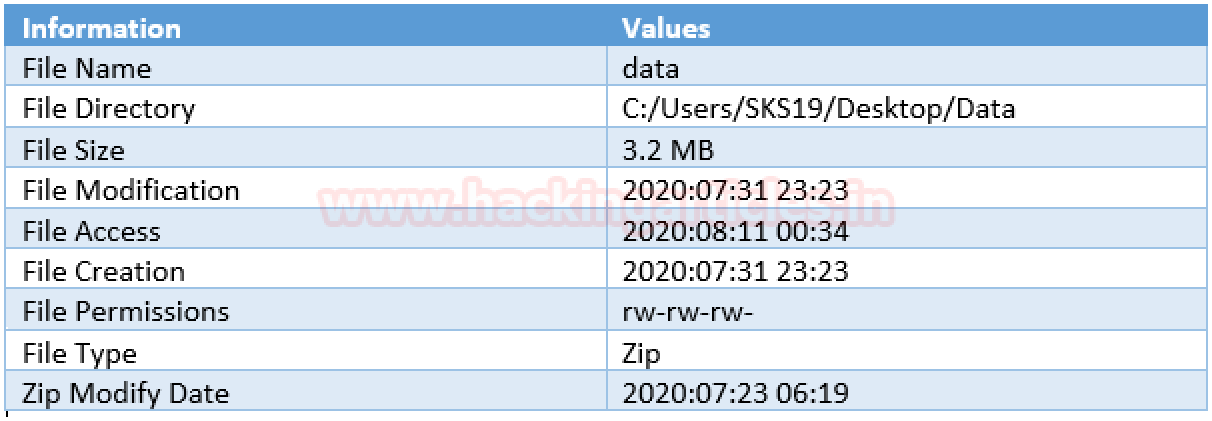


C:\Users\SKS19\Downloads\exiftool(-k).exe

```
ExifTool Version Number         : 12.01
File Name                       : data
Directory                       : C:/Users/SKS19/Desktop/Data
File Size                       : 3.2 MB
File Modification Date/Time     : 2020:07:31 23:23:33+05:30
File Access Date/Time           : 2020:08:11 00:34:46+05:30
File Creation Date/Time         : 2020:07:31 23:23:30+05:30
File Permissions                : rw-rw-rw-
File Type                       : ZIP
File Type Extension             : zip
MIME Type                       : application/zip
Zip Required Version            : 10
Zip Bit Flag                    : 0
Zip Compression                 : None
Zip Modify Date                 : 2020:07:23 06:19:26
Zip CRC                         : 0x00000000
Zip Compressed Size             : 0
Zip Uncompressed Size           : 0
Zip File Name                   : Reg[redacted]master/
Warning                         : [minor] Use the Duplicates option to
-- press ENTER --
```

www.hackingarticles.in

These are the few highlights of this file, which we captured for this investigation process.

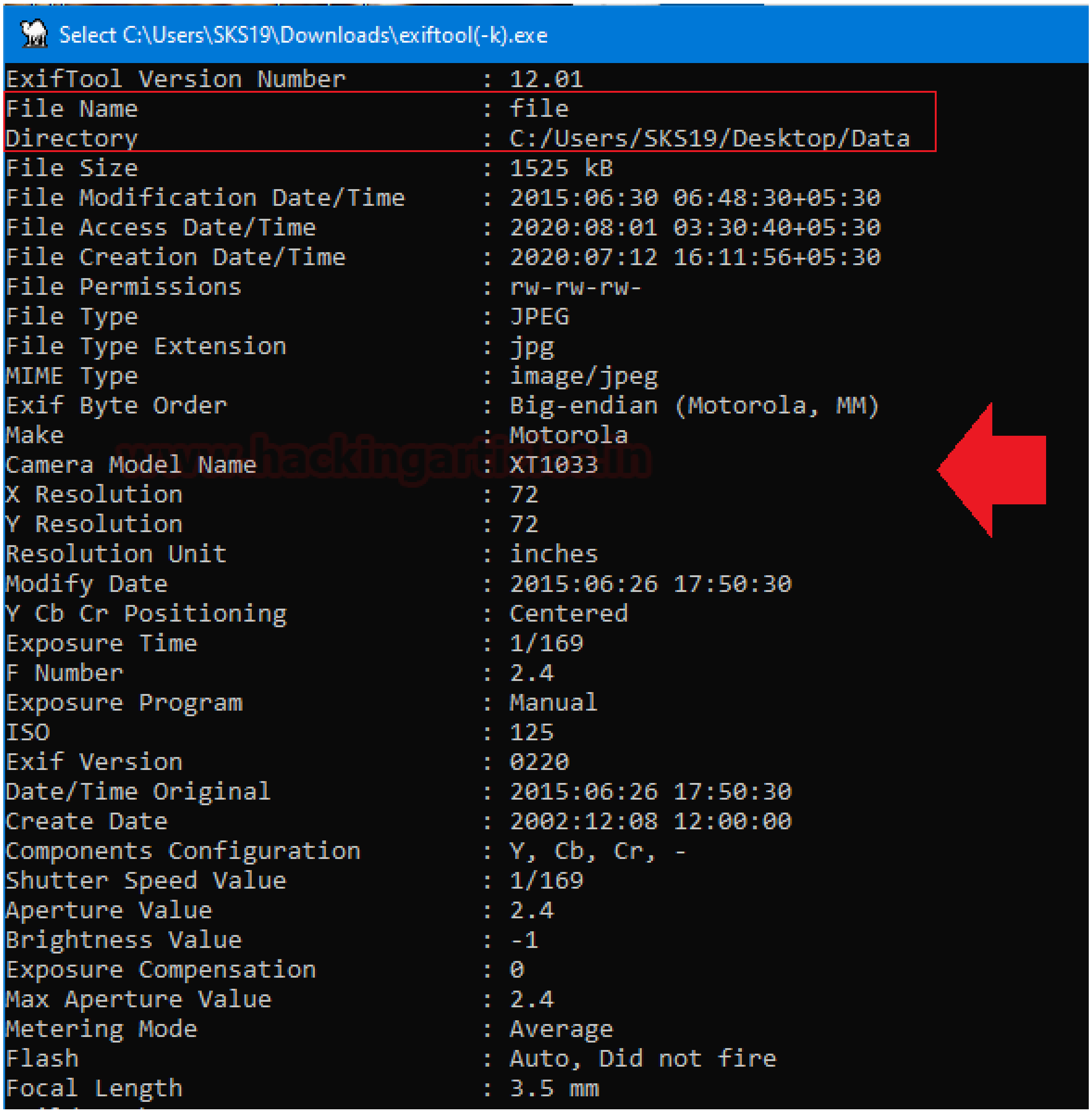


Information	Values
File Name	data
File Directory	C:/Users/SKS19/Desktop/Data
File Size	3.2 MB
File Modification	2020:07:31 23:23
File Access	2020:08:11 00:34
File Creation	2020:07:31 23:23
File Permissions	rw-rw-rw-
File Type	Zip
Zip Modify Date	2020:07:23 06:19

www.hackingarticles.in

File #3: file

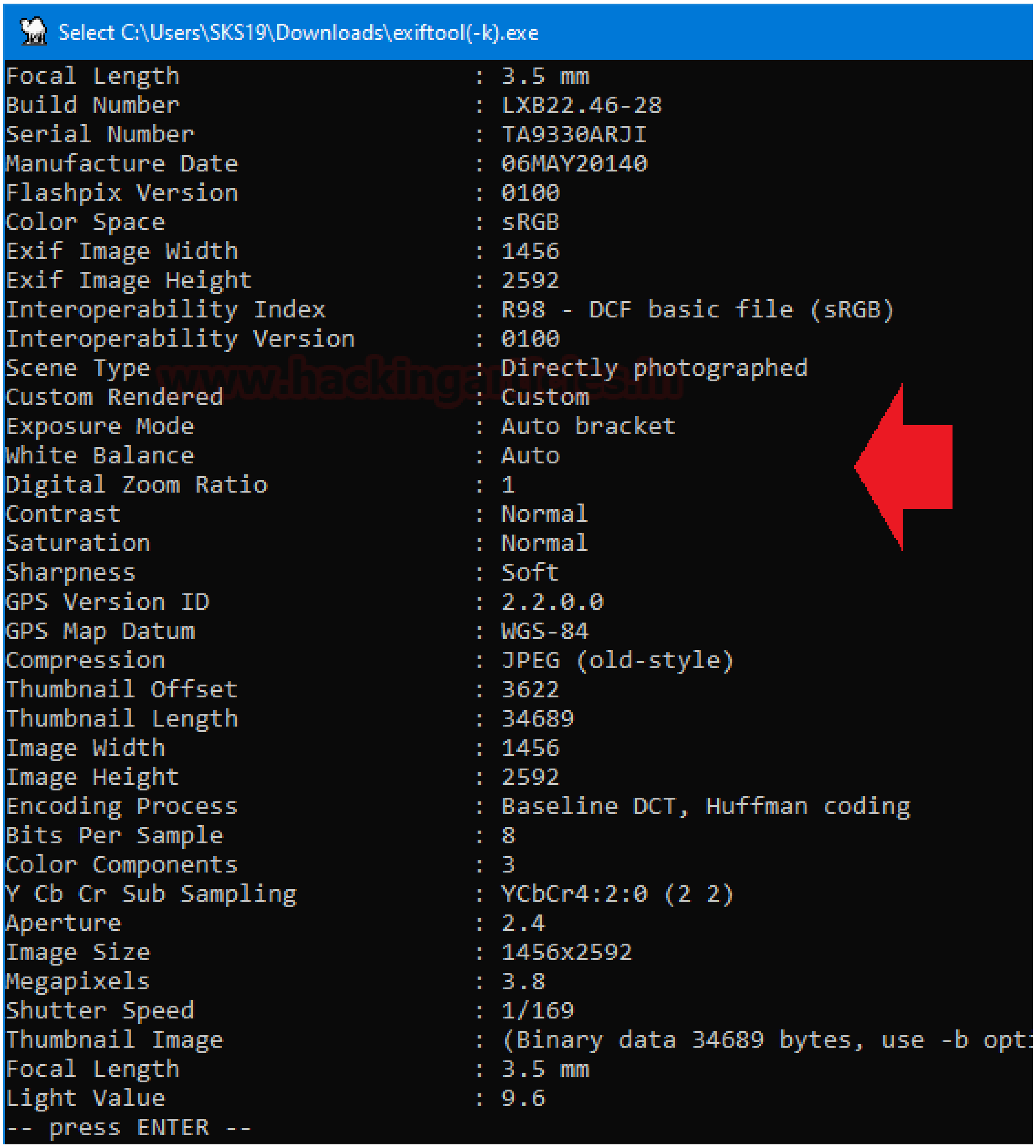
The Third file we got is the file. Repeat the previous step, to get metadata of this file **drag and drop** this corrupt file on the [exiftool(-k).exe] in the archive file which we just unzipped.



```
ExifTool Version Number         : 12.01
File Name                       : file
Directory                       : C:/Users/SKS19/Desktop/Data
File Size                       : 1525 kB
File Modification Date/Time     : 2015:06:30 06:48:30+05:30
File Access Date/Time           : 2020:08:01 03:30:40+05:30
File Creation Date/Time         : 2020:07:12 16:11:56+05:30
File Permissions                : rw-rw-rw-
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : Motorola
Camera Model Name               : XT1033
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Modify Date                     : 2015:06:26 17:50:30
Y Cb Cr Positioning             : Centered
Exposure Time                   : 1/169
F Number                        : 2.4
Exposure Program                : Manual
ISO                             : 125
Exif Version                    : 0220
Date/Time Original              : 2015:06:26 17:50:30
Create Date                     : 2002:12:08 12:00:00
Components Configuration        : Y, Cb, Cr, -
Shutter Speed Value             : 1/169
Aperture Value                  : 2.4
Brightness Value                : -1
Exposure Compensation           : 0
Max Aperture Value              : 2.4
Metering Mode                   : Average
Flash                           : Auto, Did not fire
Focal Length                    : 3.5 mm
```

www.hackingarticles.in

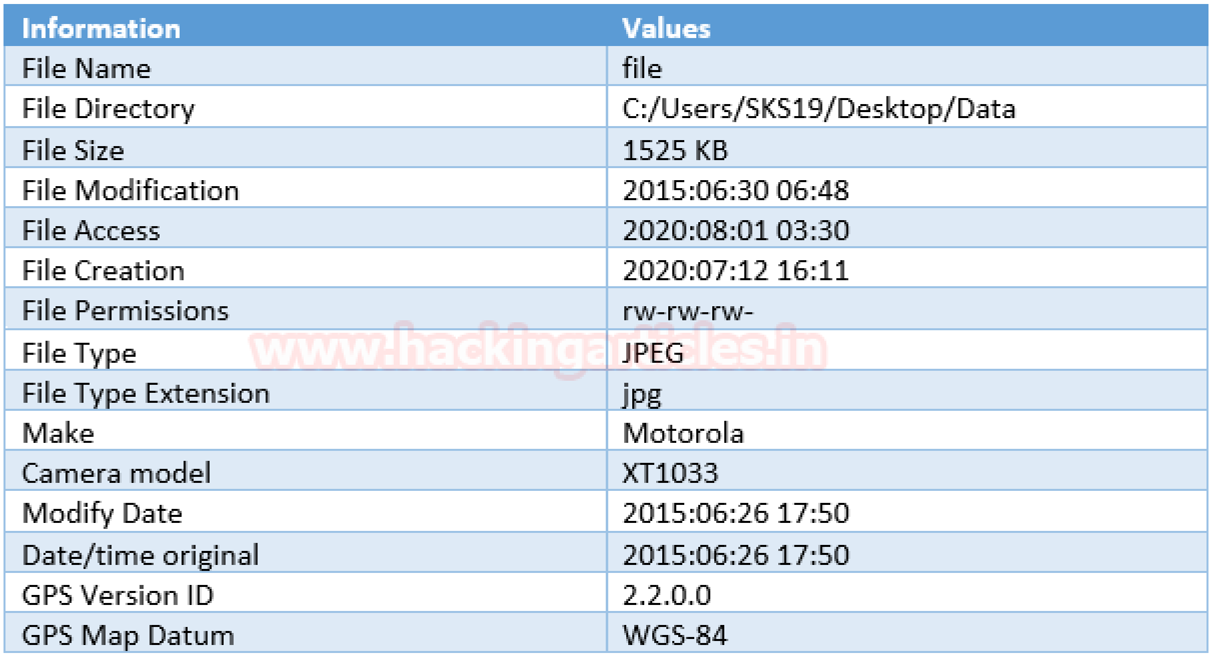
Now, few more interesting details regarding this file.



Select C:\Users\SKS19\Downloads\exiftool(-k).exe

```
Focal Length                    : 3.5 mm
Build Number                    : LXB22.46-28
Serial Number                   : TA9330ARJI
Manufacture Date                : 06MAY20140
Flashpix Version                : 0100
Color Space                     : sRGB
Exif Image Width                : 1456
Exif Image Height               : 2592
Interoperability Index          : R98 - DCF basic file (sRGB)
Interoperability Version        : 0100
Scene Type                      : Directly photographed
Custom Rendered                 : Custom
Exposure Mode                   : Auto bracket
White Balance                   : Auto
Digital Zoom Ratio              : 1
Contrast                        : Normal
Saturation                      : Normal
Sharpness                       : Soft
GPS Version ID                  : 2.2.0.0
GPS Map Datum                   : WGS-84
Compression                     : JPEG (old-style)
Thumbnail Offset                : 3622
Thumbnail Length                : 34689
Image Width                     : 1456
Image Height                    : 2592
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Aperture                        : 2.4
Image Size                      : 1456x2592
Megapixels                      : 3.8
Shutter Speed                   : 1/169
Thumbnail Image                 : (Binary data 34689 bytes, use -b opt
Focal Length                    : 3.5 mm
Light Value                     : 9.6
-- press ENTER --
```

As we have captured a few interesting details in these screenshots which helps us in our forensic investigation.

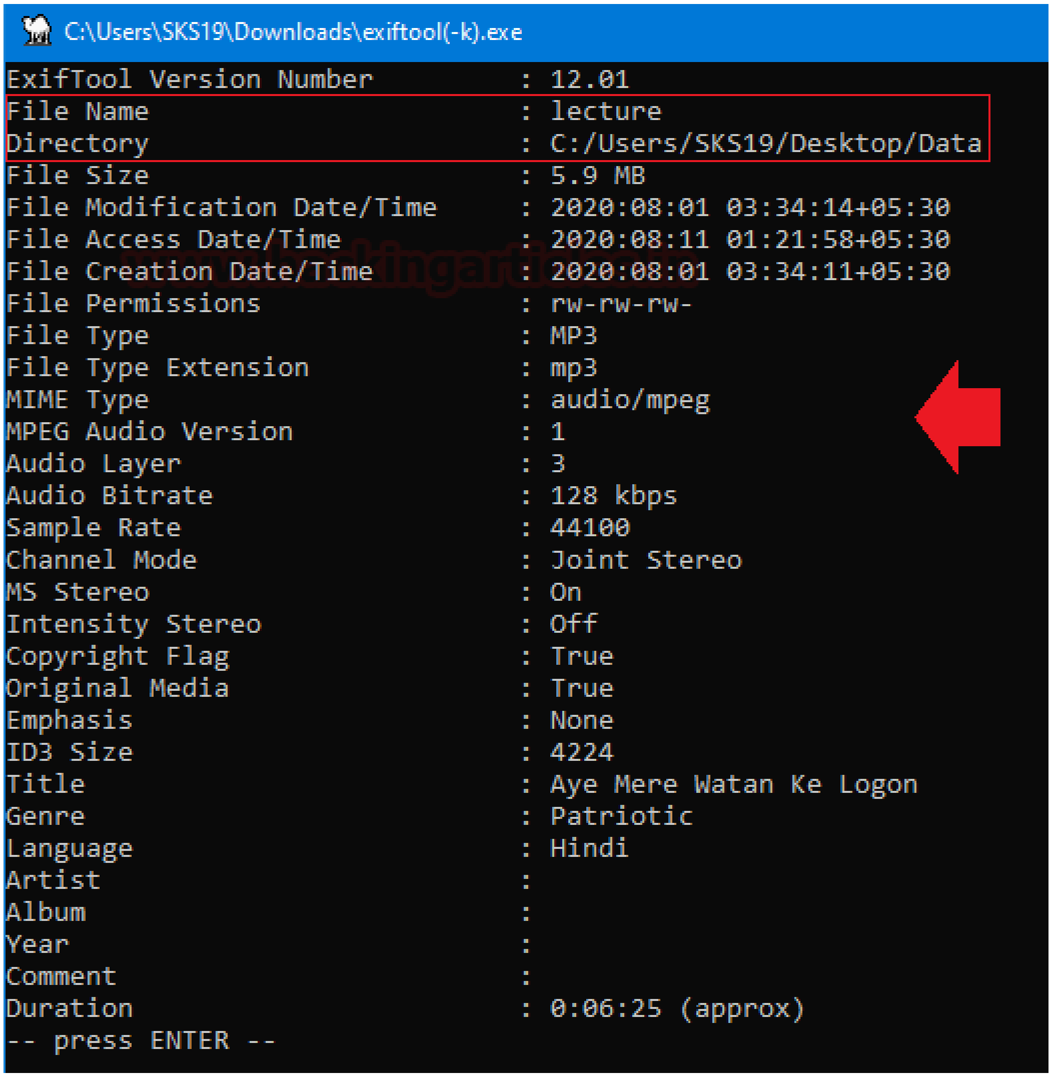


Information	Values
File Name	file
File Directory	C:/Users/SKS19/Desktop/Data
File Size	1525 KB
File Modification	2015:06:30 06:48
File Access	2020:08:01 03:30
File Creation	2020:07:12 16:11
File Permissions	rw-rw-rw-
File Type	JPEG
File Type Extension	jpg
Make	Motorola
Camera model	XT1033
Modify Date	2015:06:26 17:50
Date/time original	2015:06:26 17:50
GPS Version ID	2.2.0.0
GPS Map Datum	WGS-84

www.hackingarticles.in

File #4: lecture

The fourth file we got is the lecture. Repeat the previous step, to get metadata of this file **drag and drop** this corrupt file on the [exiftool(-k).exe] in the archive file which we just unzipped.



C:\Users\SKS19\Downloads\exiftool(-k).exe

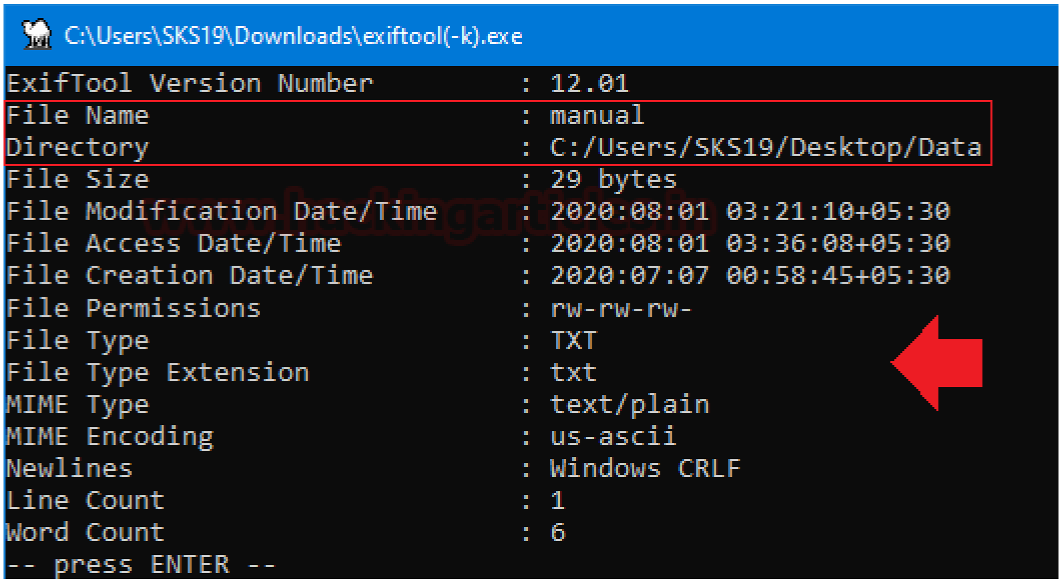
```
ExifTool Version Number         : 12.01
File Name                       : lecture
Directory                       : C:/Users/SKS19/Desktop/Data
File Size                       : 5.9 MB
File Modification Date/Time     : 2020:08:01 03:34:14+05:30
File Access Date/Time           : 2020:08:11 01:21:58+05:30
File Creation Date/Time         : 2020:08:01 03:34:11+05:30
File Permissions                : rw-rw-rw-
File Type                       : MP3
File Type Extension             : mp3
MIME Type                       : audio/mpeg
MPEG Audio Version              : 1
Audio Layer                     : 3
Audio Bitrate                   : 128 kbps
Sample Rate                     : 44100
Channel Mode                    : Joint Stereo
MS Stereo                       : On
Intensity Stereo                : Off
Copyright Flag                  : True
Original Media                  : True
Emphasis                        : None
ID3 Size                        : 4224
Title                           : Aye Mere Watan Ke Logon
Genre                           : Patriotic
Language                        : Hindi
Artist                          :
Album                           :
Year                            :
Comment                         :
Duration                        : 0:06:25 (approx)
-- press ENTER --
```

These are the few highlights of this file, which we captured for this investigation process.

Information	Values
File Name	lecture
File Directory	C:/Users/SKS19/Desktop/Data
File Size	5.9 MB
File Modification	2020:08:01 03:34
File Access	2020:08:11 01:24
File Creation	2020:08:01 03:34
File Permissions	rw-rw-rw-
File Type	mp3
MIME Type	Audio/mpeg
Title	Aye Mere Watan Ke Logon
Duration	0:06:25 [approx]

File #5: manual

The fifth file we got is the manual. Repeat the previous step, to get metadata of this file **drag and drop** this corrupt file on the [exiftool(-k).exe] in the archive file which we just unzipped.



```
ExifTool Version Number         : 12.01
File Name                       : manual
Directory                       : C:/Users/SKS19/Desktop/Data
File Size                       : 29 bytes
File Modification Date/Time     : 2020:08:01 03:21:10+05:30
File Access Date/Time           : 2020:08:01 03:36:08+05:30
File Creation Date/Time         : 2020:07:07 00:58:45+05:30
File Permissions                : rw-rw-rw-
File Type                       : TXT
File Type Extension             : txt
MIME Type                       : text/plain
MIME Encoding                   : us-ascii
Newlines                        : Windows CRLF
Line Count                      : 1
Word Count                      : 6
-- press ENTER --
```

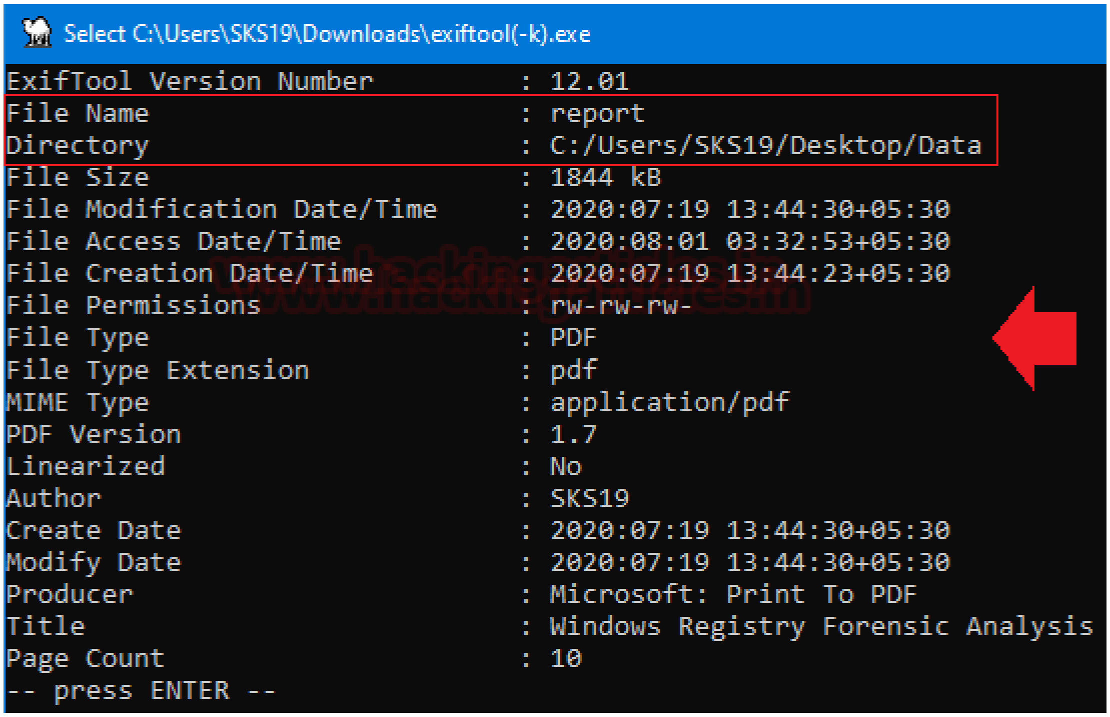
As we have captured a few interesting details in this screenshot which helps us in forensic investigation.

Information	Values
File Name	manual
File Directory	C:/Users/SKS19/Desktop/Data
File Size	29 bytes
File Modification	2020:08:01 03:21
File Access	2020:08:01 03:36
File Creation	2020:07:07 00:58
File Permissions	rw-rw-rw-
File Type	txt
Line Count	1
Word Count	6

www.hackingarticles.in

File #6: report

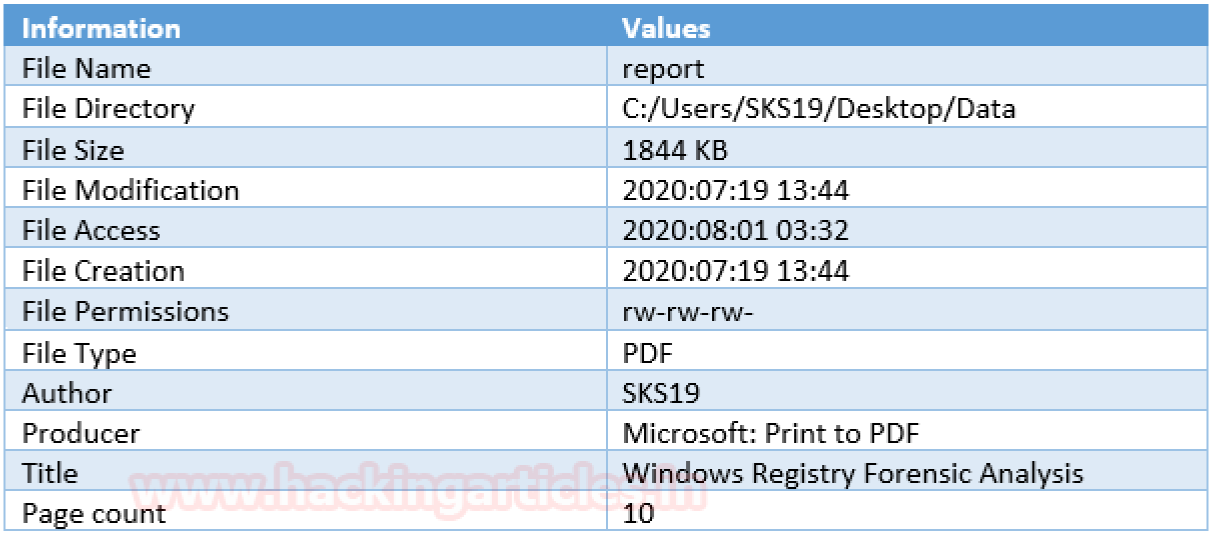
The Second last file we got is the report. Repeat the above steps just **drag and drop** this corrupted file on to [exiftool(-k).exe] to get its metadata details.



```
ExifTool Version Number         : 12.01
File Name                       : report
Directory                       : C:/Users/SKS19/Desktop/Data
File Size                       : 1844 kB
File Modification Date/Time     : 2020:07:19 13:44:30+05:30
File Access Date/Time           : 2020:08:01 03:32:53+05:30
File Creation Date/Time         : 2020:07:19 13:44:23+05:30
File Permissions                : rw-rw-rw-
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.7
Linearized                      : No
Author                          : SKS19
Create Date                     : 2020:07:19 13:44:30+05:30
Modify Date                     : 2020:07:19 13:44:30+05:30
Producer                        : Microsoft: Print To PDF
Title                           : Windows Registry Forensic Analysis
Page Count                      : 10
-- press ENTER --
```

www.hackingarticles.in

These are the few highlights of this file, which we captured for this investigation process.

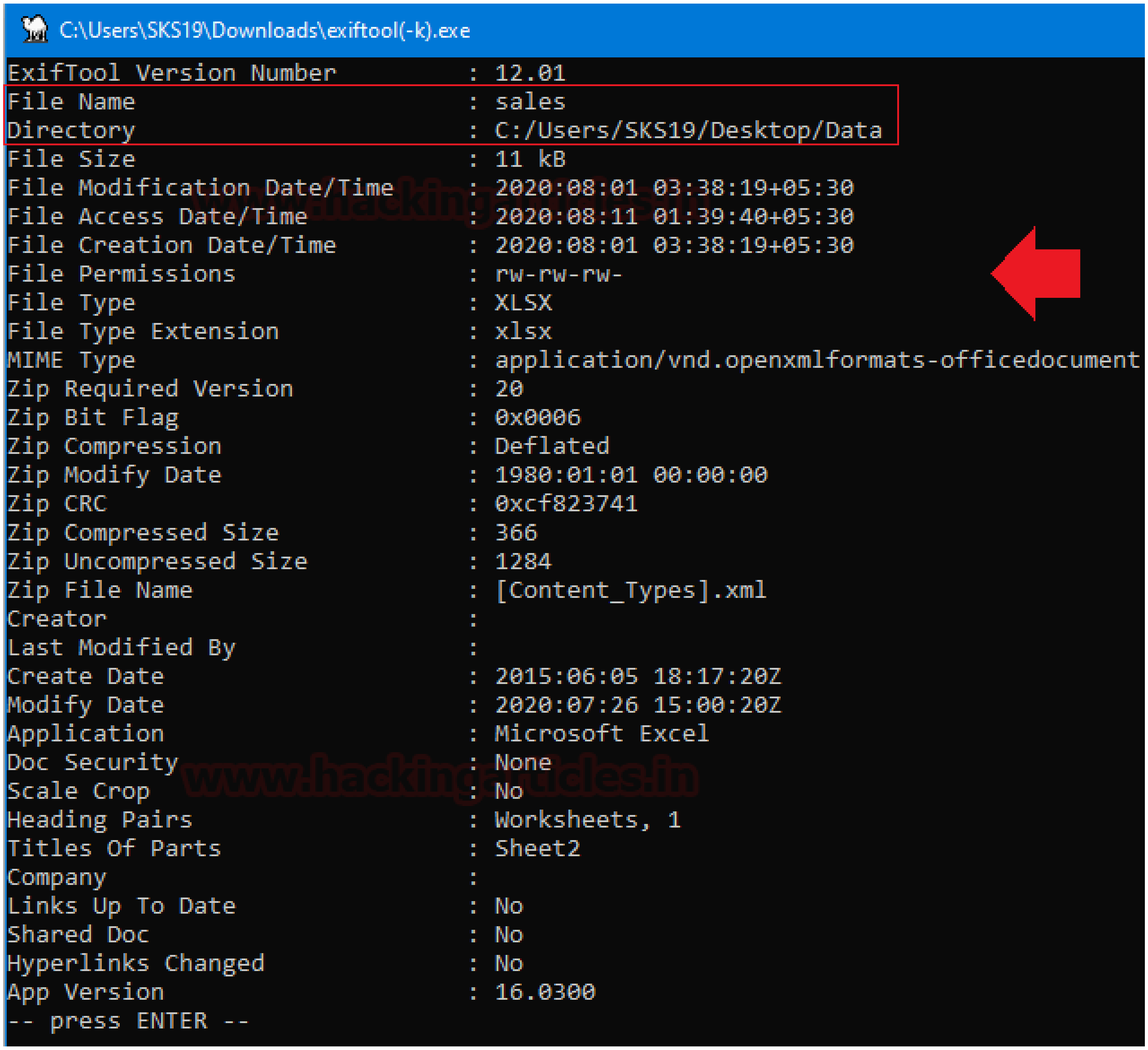


Information	Values
File Name	report
File Directory	C:/Users/SKS19/Desktop/Data
File Size	1844 KB
File Modification	2020:07:19 13:44
File Access	2020:08:01 03:32
File Creation	2020:07:19 13:44
File Permissions	rw-rw-rw-
File Type	PDF
Author	SKS19
Producer	Microsoft: Print to PDF
Title	Windows Registry Forensic Analysis
Page count	10

www.hackingarticles.in

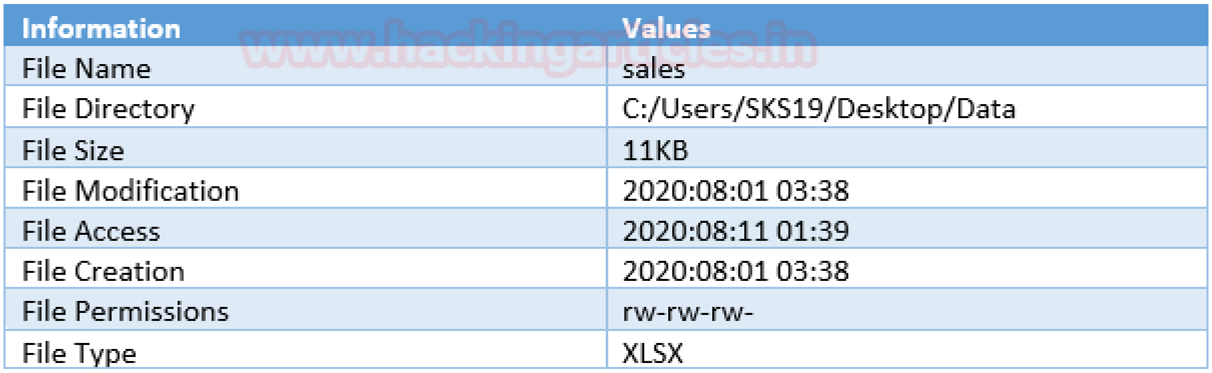
File #7: sales

The last file we got is sales. Repeat the above steps just **drag and drop** this corrupted file on to [exiftool(-k).exe] to get its metadata details.



```
ExifTool Version Number         : 12.01
File Name                       : sales
Directory                       : C:/Users/SKS19/Desktop/Data
File Size                       : 11 kB
File Modification Date/Time     : 2020:08:01 03:38:19+05:30
File Access Date/Time           : 2020:08:11 01:39:40+05:30
File Creation Date/Time         : 2020:08:01 03:38:19+05:30
File Permissions                : rw-rw-rw-
File Type                       : XLSX
File Type Extension             : xlsx
MIME Type                       : application/vnd.openxmlformats-officedocument
Zip Required Version            : 20
Zip Bit Flag                    : 0x0006
Zip Compression                 : Deflated
Zip Modify Date                 : 1980:01:01 00:00:00
Zip CRC                         : 0xcf823741
Zip Compressed Size             : 366
Zip Uncompressed Size           : 1284
Zip File Name                   : [Content_Types].xml
Creator                         :
Last Modified By                :
Create Date                     : 2015:06:05 18:17:20Z
Modify Date                     : 2020:07:26 15:00:20Z
Application                     : Microsoft Excel
Doc Security                    : None
Scale Crop                      : No
Heading Pairs                   : Worksheets, 1
Titles Of Parts                 : Sheet2
Company                         :
Links Up To Date                : No
Shared Doc                      : No
Hyperlinks Changed              : No
App Version                     : 16.0300
-- press ENTER --
```

As we have captured a few interesting details in this screenshot which helps us in our forensic investigation.



Information	Values
File Name	sales
File Directory	C:/Users/SKS19/Desktop/Data
File Size	11KB
File Modification	2020:08:01 03:38
File Access	2020:08:11 01:39
File Creation	2020:08:01 03:38
File Permissions	rw-rw-rw-
File Type	XLSX

Conclusion

Overall Exiftool can become quite handy in these kinds of Forensic Investigation, where a Forensic Investigator doesn’t have any clue about the file types. This method can help him to proceed further in the Investigation.