ENPM687 – Digital Forensics and Incidence Responses

Assignment – 3

Author – Syed Mohammad Ibrahim

UMD ID: iamibi

UID: 118428369

Email: iamibi@umd.edu

1. Where did you find the message?

A. The message was located at the location

/img_Virtual Disk.vmdk/vol_vol2/RECYCLER/S-1-5-21-1214440339-1060284298-725345543-500/Dc1.rtf

2. What did it say?

A. The following message was present in the file

```
Obi Wan,

I hope you are well.  In my next communication I will send to you the
location of the secret rebel base.  Take care!

- Leia Organa
```

3. What was the file format?

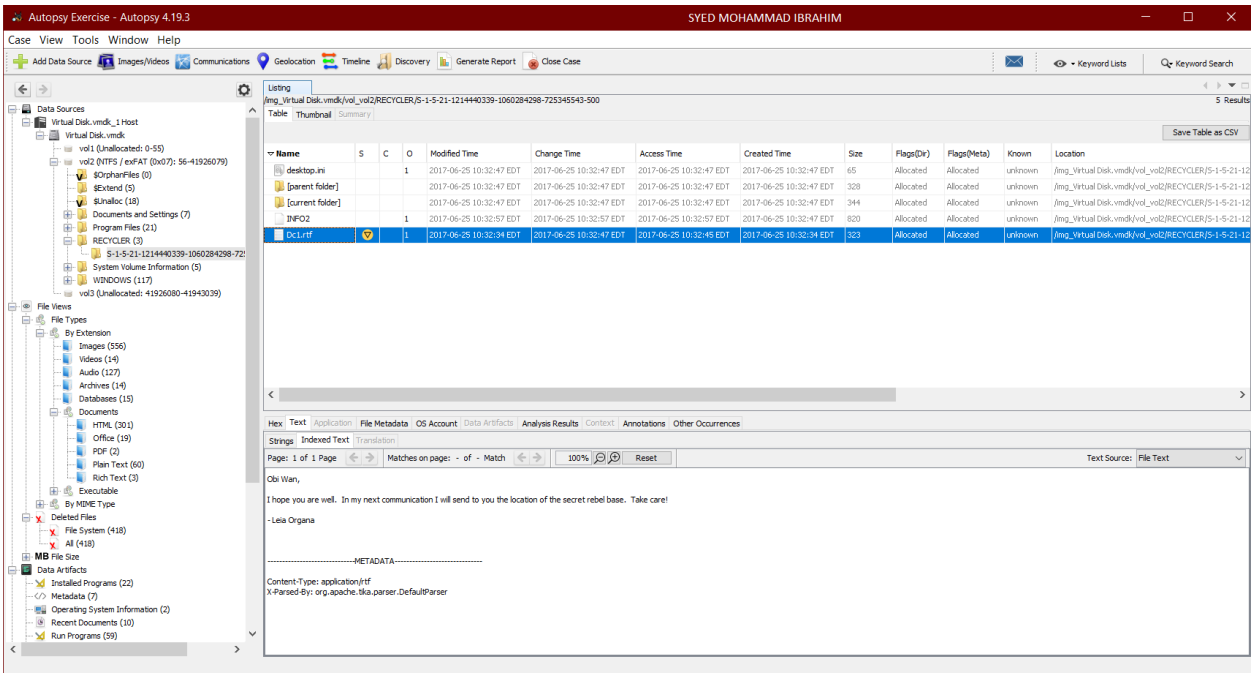
A. The file format was Rich Text Format (RTF)

4. What was the original file name?

A. The original files are hinted as part of INFO2 file which is present in the same directory. The content of INFO2 file indicates the following:

```
C:\Documents and Settings\Administrator\My Documents\secret.rtf
C:\Documents and Settings\Administrator\My Documents\secret.rtf
```

Which points to a secrets file that may have sensitive information.


Autopsy Exercise - Autopsy 4.19.3
SYED MOHAMMAD IBRAHIM
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
Virtual Disk.vmdk_1 Host
Virtual Disk.vmdk
vol1 (Unallocated: 0-55)
vol2 (NTFS / exFAT (0x07): 56-41926079)
$OrphanFiles (0)
$Extend (5)
$Unalloc (18)
Documents and Settings (7)
Program Files (21)
RECYCLER (3)
S-1-5-21-1214440339-1060284298-725
System Volume Information (5)
WINDOWS (117)
vol3 (Unallocated: 41926080-41943039)
File Views
File Types
By Extension
Images (556)
Videos (14)
Audio (127)
Archives (14)
Databases (15)
Documents
HTML (301)
Office (19)
PDF (2)
Plain Text (60)
Rich Text (3)
Executable
By MIME Type
Deleted Files
File System (418)
All (418)
MB File Size
Data Artifacts
Installed Programs (22)
Metadata (7)
Operating System Information (2)
Recent Documents (10)
Run Programs (59)
Listing
/img_Virtual Disk.vmdk/vol_vol2/RECYCLER/S-1-5-21-1214440339-1060284298-725345543-500
5 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
Size
Flags(Dir)
Flags(Meta)
Known
Location
desktop.ini
[parent folder]
[current folder]
INFO2
Dc1.rtf
2017-06-25 10:32:47 EDT
2017-06-25 10:32:57 EDT
2017-06-25 10:32:34 EDT
2017-06-25 10:32:45 EDT
Allocated
unknown
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Strings
Indexed Text
Translation
Page: 1 of 1 Page
Matches on page: - of - Match
100%
Reset
Text Source: File Text
Obi Wan,
I hope you are well. In my next communication I will send to you the location of the secret rebel base. Take care!
- Leia Organa
----------METADATA----------
Content-Type: application/rtf
X-Parsed-By: org.apache.tika.parser.DefaultParser