ENPM697 – Digital Forensics and Incidence Responses

Autopsy Exercise

Author – Syed Mohammad Ibrahim

UMD ID: iamibi

UID: 118428369

Email: iamibi@umd.edu

1. What was interesting to you (with where you found it)

A. The secrets.rtf file was interesting as it potentially held secrets surrounding the credentials. I found it under the Deleted Files category where in the system it was located under

/img_Virtual Disk.vmdk/vol_vol2/Documents and Settings/Administrator/My Documents/secrets.rtf

Another interesting file that I found was Dc1.rtf located at

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

It contained the following message:

```
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
```

2. Why it was interesting

A. The files were interesting because they suggested information that can be leveraged by an attacker or malicious actor for exploiting the system or to the very least a user on the system.

3. What do you suspect it could reveal to you or how it could potentially help in an actual investigation.

A. As an investigator, it will help me understand the clues on how an attacker may have compromised the account or maybe recover the secrets for further analysis on a system that is locked out maybe.