Laboratory Report
IST602: Digital Forensics

Examination Number: 1 Date: 9/8/19
Examiner's Name: Akshay Chaurasia

Examination or Validation Tasking:

On 05/18/16, the vice-president of ForCorp Inc. delivered a copy of the forensic image of a disc, serial number #SU09082019, along with a letter to me.

The vice-president provided the following summary of the case:

"For the past several months, we have been conducting an investigation of an employee concerning the possible theft of our proprietary company information. It is believed that this employee removes corporate information in electronic form and passes it on to our competitors a company called BadCo.

This employee, Sally Smith is believed to be preparing to transfer some of ForCorp's proprietary information to BadCo. A BadCo employee, Joe Doaks has been developed as a possible contact for Smith.

An informant has recently obtained a disk which may assist us in our investigation. The informant was not able to keep the disk, but was able to make a forensic image, a copy of which is attached.**"**

They requested that an examination be conducted to identify if there is any information concerning Sally Smith, BadCo, Joe Doaks on this disk. They also requested to identify the file name, location, type of application used to create the information and any other useful information that can be determined from this data.

Forensic Question(s): [Use Inman & Rudin Paradigm]

1. Identify relevant information concerning Sally Smith, BadCo, and Joe Doaks
2. Locate all document file
3. Recover and examine the files
4. Locate any references to Sally Smith, BadCo, and Joe Doaks
5. Associate files, media, computer, IP address with Sally Smith, BadCo, and Joe Doaks

Laboratory Report
IST602: Digital Forensics

Examination Number: 1 Date: 9/8/19
Examiner's Name: Akshay Chaurasia

Steps Taken:

1. A new case (forensic image #SU09082019), was opened in Norton Diskedit Tool Kit version 1.2 and the image was indexed.
2. A search for the deleted files was conducted
3. The deleted objects were recovered using a set of pre-defined procedures, approved by the company (ForpCorp Inc)
4. Each of the data identified, was examined for metadata and exported to CDROM, which was then mounted on the E:\ drive for further review
5. An examination of the recovered objects was conducted

Results: The search for the deleted files was conducted with the following objects were found in the root Directory A:\ (Line number 3 of the Steps Taken)

- A file of the type TXT: **σFILE**
- A file of the type DOC: **σFILE**
- A Folder: **σCEBERG**

The folder had the following objects:

- A file of the type TXT: **σFILE**
- A file of the type DOC: **σFILE**

After recovering these files, we found the following information/metadata (Line no 4 of the Steps Taken)

Name	File Type	File Size	Date Modified	Time Modified	Location
!File	TXT	1 KB	4/2/2004	10:08 AM	A:/
!File	DOC	20 KB	4/3/2004	10:08 AM	A:/
!CEBERG	Folder		4/5/2004	03:08 PM	A:/
!File	TXT	1 KB	4/5/2004	11:09 PM	A:/!CEBERG
!File	DOC	20 KB	4/6/2004	11:10 PM	A:/!CEBERG

A review of the recovered DOC files in the Microsoft Word (Office 2019 version) reveals that the DOC files were created by Sally Smith **(See appendix B and D).** These files have been placed on a CDROM marked SUDF09082019" and provided to the contributor.

Laboratory Report
IST602: Digital Forensics

Examination Number: 1 Date: 9/8/19
Examiner's Name: Akshay Chaurasia

Conclusions:

The recovered files show that Sally Smith and Joe Doaks were associated. The TXT type files, show that Joe Doaks initiated the conversation and asked Sally for the information that might help BadCo. Two DOC type files, which were recovered, were created by Sally **(See appendix B and D)**. In these files, she is addressing to Joe's query regarding "Iceberg", which seems to be ForCorp's information.

Opinions:

In my opinion, Sally Smith was providing Joe Doaks with the ForCorp's internal information which Joe Doaks planed to use for BadCo's benefit.

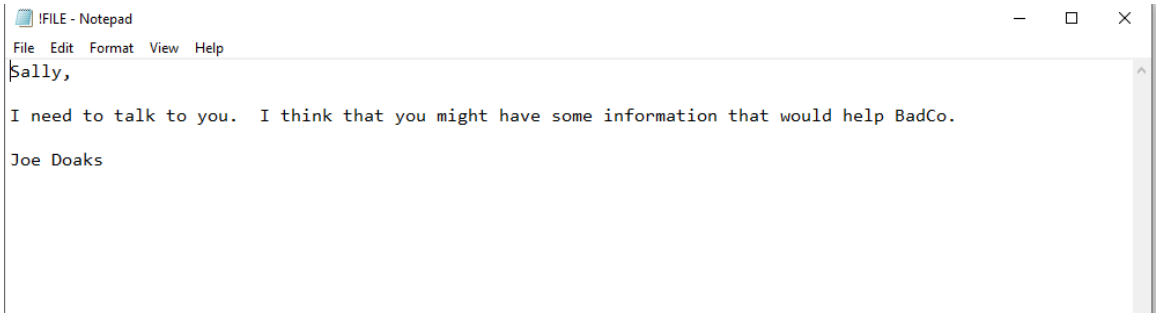
Certification:

I hereby certify that the work presented above was personally performed by me and the opinions and conclusions stated are my own and based upon the work that I performed.

Akshay Chaurasia
Signature

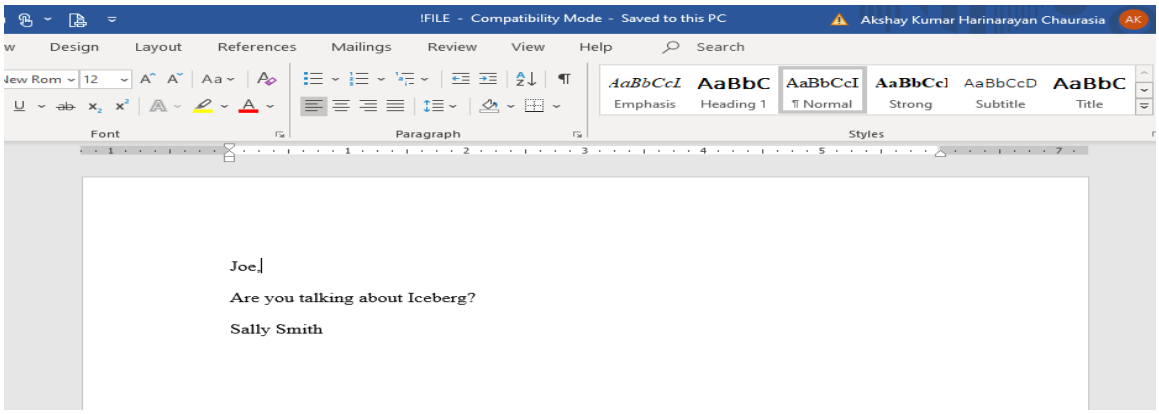
Appendix A

The recovered file, "!File" of type TXT was created by Joe Doaks. It was addressed to Sally Smith. This TXT file was recovered from the directory A:/ of the forensic image which was provided by the vice-president of the ForCorp Inc. In the TXT file, it can be seen that Joe Doaks was asking Sally Smith for some information that would benefit BadCo. Below is the screenshot of the content of !File.TXT.



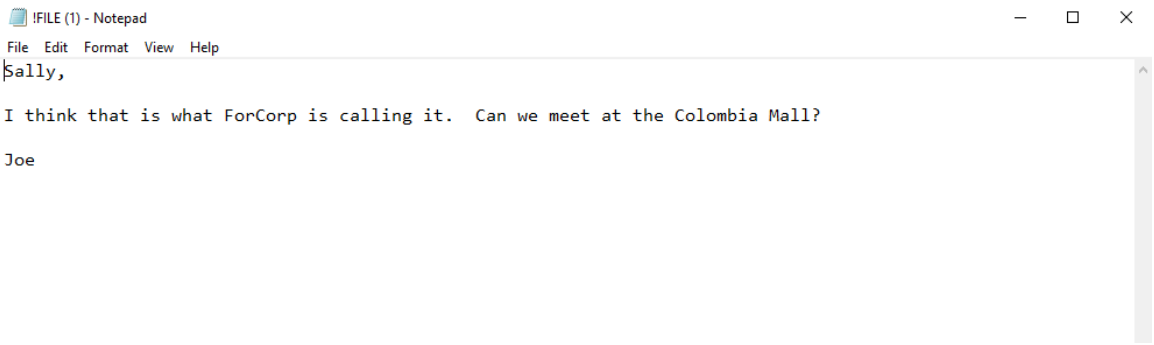
Appendix B

The recovered file, "!File" of type DOC was created by Sally Smith. It was addressed to Joe Doaks. This DOC file was recovered from the directory A:/ of the forensic image which was provided by the vice-president of the ForCorp Inc. In the TXT file, it can be seen that Sally Smith replied to Joe Doaks' query for some information that would benefit BadCo. Below is the screenshot of the content of !File.DOC.



Appendix C

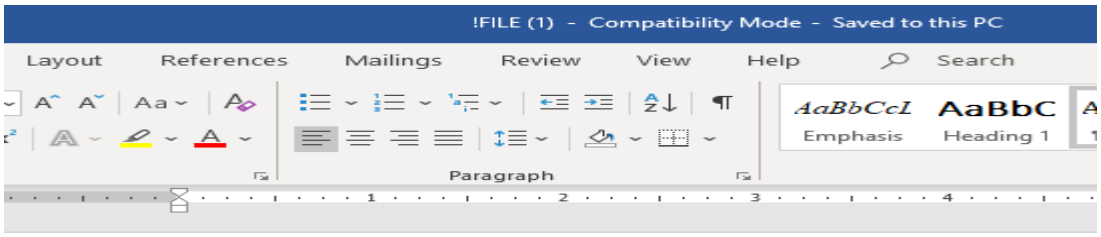
The third recovered file, "!File" of type TXT was created by Joe Doaks. It was addressed to Sally Smith. This TXT file was inside the folder "!CEBERG" and was recovered from the directory A:/!CEBERG of the forensic image which was provided by the vice-president of the ForCorp Inc. In this TXT file, it can be seen that Joe is asking Sally to meet at the Columbia Mall. Below is the screenshot of the content of !File.TXT.



Examination Number: 1 Date: 9/8/19
Examiner's Name: Akshay Chaurasia

Appendix D

The fourth recovered file, "!File" of type DOC was created by Sally Smith. It was addressed to Joe Doaks. This DOC file was inside the folder "!CEBERG" and was recovered from the directory A:/!CEBERG of the forensic image which was provided by the vice-president of the ForCorp Inc. In the TXT file, it can be seen that Sally Smith agreed to meet Joe Doaks on Saturday afternoon in front of Hechts. Below is the screenshot of the content of !File.DOC.



OK, this Saturday at Noon in front of Hechts