CASE STUDY 2 03-27-2018

AKASH MUKHERJEE
COMPUTER AND NETWORK FORENSICS
UNIVERSITY OF SOUTHERN CALIFORNIA

Table of Contents

I. EXECUTIVE SUMMARY

RIAA has notified that the network at Acme Inc has been utilized for copyright infringement. After analysing the network log [13], it was found the traffic leads to one person, Mr. Flannigan. It was found that VMWare [19] was installed on the system which is against company policy. A Forensic image of one of the Virtual Machines [18] (VMs) was shared for investigation.

Investigation discovered a BitTorrent [2] client software "uTorrent" [17] installed on the system. Further analysing the application data, four torrent files [16] were discovered. These files were used by "uTorrent". In the user download directory, corresponding four folders were identified. Investigating the contents of these files and matching the hashes [8], sources have been identified as torrent. Only one VM was shared for investigation. Examining other VMs might reveal new findings.

II. COMPUTER EVIDENCE ANALYZED

The details of the image files which were shared on Dropbox are given below:

	https://www.dropbox.com/sh/yo958yzsuh0k4y0/AACqFbnsAag6Nb_Lvwu9Vwsra?dl=0
Shared on	Mar 1, 2018 9:30 AM PST
Shared by	Mr. Joseph Greenfield

File name	**MD5** [12]	**SHA1** [15]
BitTorrent.E01	dd8d1a14c1815afd bebcc47090b3f848	0454fb1a89a290611396 04aa81e9ba4d177588c5
BitTorrent.E02	8c89d7d2da719f88 aefdfbfc8b08ba35	7f3570c92a026b1fd0e0 95417dc5c90d572d131f
BitTorrent.E03	5ab500401e6b013c 68c05fcab6058cb2	11958e7a865de31750c4 1ad88d86745e48d93d24
BitTorent.E01.txt	bed6194815683f6b 0f8c5edefd901810	08ed697aa4ab6a89009d 97b2fd502a790aa7ab9f

III. ANALYSIS RESULTS

The aforementioned disk image file has been analyzed to retrieve these basic system information:

- **Operating System:** Windows 7 Professional English
- **Drive Information:** Operating System stored in C drive
- **Username:** Neil Flannigan

The Operating system was installed on C drive. This drive was examined to determine if it contained any pirated content. EnCase [4], Forensic Explorer [6], HashCalc [9], BEncode Editor [1] had been used for this investigation.

a) Investigation for existence any BitTorrent program

The Operating system was identified as Windows 7 by analysing the registry files. Windows 7 does not come with a pre-installed BitTorrent client. Installed programs on the operating system were investigated for presence of any BitTorrent client. Program files is the default path for application installation. Windows also creates user specific AppData folder to store sets of settings per application. Below are the details of findings:

- BitTorrent client 'uTorrent' was discovered in the users download folder. C:\Users\Neil Flannigan\Downloads\uTorrent.exe was created on 02/23/2012 06:58:34 AM UTC.
- From the C:\Users\Neil Flannigan\AppData\Roaming\uTorrent 'uTorrent' was discovered. This file was created on 02/23/2012 06:59:01 AM UTC.
- From Program Files (x86), uTorrent was discovered in the following path: C:\Program Files (x86)\ uTorrent\uTorrent.exe. It was created on 02/23/2012 06:59:01 AM UTC.

b) Investigation for existence of any torrent file

After locating installed torrent client on the system, existence of any torrent files were examined. Torrent files are downloaded from the internet. BitTorrent clients use these torrent files to determine which files/folders will be distributed. Four torrent files were discovered on the system. Information about the identified torrent files on the system are tabulated below:

Name	Extension	Full Path	File Created	Last Written	Last Accessed	Hash (MD5)
Adele Complete Discography [theLEAK].torrent	.torrent	C:\Users\Neil Flannigan\AppData\Roaming\uTorrent\Adele Complete Discography [theLEAK].torrent	02/23/12 07:00:56 AM	02/23/12 07:00:52 AM	02/23/12 07:00:56 AM	03E6DE5ECE18AADE816D811D55A30AB4
Foo Fighters - Discography.torrent	.torrent	C:\Users\Neil Flannigan\AppData\Roaming\uTorrent\ Foo Fighters - Discography.torrent	02/23/12 07:01:49 AM	02/23/12 07:01:47 AM	02/23/12 07:01:49 AM	69B4CE03CB6ADA599B6113099DBB8E1C
The Help DVDRip XviD-DiAMOND.torrent	.torrent	C:\Users\Neil Flannigan\AppData\Roaming\uTorrent\ The	02/23/12 07:04:01 AM	02/23/12 07:03:59 AM	02/23/12 07:04:01 AM	902C271A6EF0D9C0A981D793960FE3C5

		Help DVDRip XviD-DiAMOND.torrent				
The Godfather Trilogy Part 1, 2 & 3 DVDRip.torrent	.torrent	C:\Users\Neil Flannigan\AppData\Roaming\uTorrent\ The Godfather Trilogy Part 1, 2 & 3 DVDRip.torrent	02/23/12 07:03:00 AM	02/23/12 07:02:59 AM	02/23/12 07:03:00 AM	445D9E688A7A6E19752C38D447AB74F6

(All timestamps in this table are in UTC)

c) Investigation with User Visited URLs

Internet Explorer was an installed browser on the system. Upon investigating temporary history files on the C:\Users\Neil Flannigan\AppData\Local\Temp\History\ directory, it was discovered that the user had visited the following sites:

a) http://torrentz.eu/a05fe4cf806adff0963977feb8f8fa5c40c1b7a2
b) http://www.utorrent.com/
c) http://www.utorrent.com/downloads/complete?os=win
d) http://kat.ph/foo-fighters-full-discography-t1878308.html
e) http://kat.ph/search/the%20godfather/
f) http://kat.ph/search/adele/
g) http://www.dl-provider.com/download-k:Adele%20Complete%20Discography%20%5BtheLEAK%5D.html?aff.id=1251&aff.subid=8
h) http://kat.ph/adele-discography-complete-2008-2011-t5286136.html
i) http://kat.ph/search/the%20help/

d) Verification of Sources for Copyrighted Materials on disk

The table below lists copyright infringement instances that were examined. Piecewise hash of the content of these files were compared with the information from the discovered torrent files, to verify whether those files were actually downloaded from torrent client or not. Each file is composed of thousands of pieces; first few pieces has been compared to see if they match. Upon match, probability of torrent being the source is high. The table below is per file hash verification for two pieces from each folder under examination.

Downloaded File/Folder Name	Piece Number	Piece length from torrent file	Calculated SHA1 Hash of [piece number] [piece length] bytes	Stored Hash on the torrent file	Full Path	Match/ Mismatch
Adele Complete Discography [theLEAK]	1	131072	f8bfecee9c78c41276d34d0c8491f911260bbc82	f8bfecee9c78c41276d34d0c8491f911260bbc82	C:\Users\Neil Flannigan\Downloads\ Adele Complete Discography [theLEAK]	Match
Adele Complete Discography [theLEAK]	2	131072	58bbae316749504c8b5f8389b0a147ba9b3a74c2	58bbae316749504c8b5f8389b0a147ba9b3a74c2	C:\Users\Neil Flannigan\Downloads\ Adele Complete Discography [theLEAK]	Match
Foo Fighters – Discography	1	1048576	491e9b9ebcdb2ef51eada6e31082ddaa624e7027	491e9b9ebcdb2ef51eada6e31082ddaa624e7027	C:\Users\Neil Flannigan\Downloads\ Foo Fighters – Discography	Match
Foo Fighters - Discography	2	1048576	2cc163bc2e243c451232d44baf4687957a7e13cf	2cc163bc2e243c451232d44baf4687957a7e13cf	C:\Users\Neil Flannigan\Downloads\ Foo Fighters – Discography	Match
The Help DVDRip XviD-DiAMOND	1	2097152	03f6bea02cab933509dd698dac98f6e8ab779b55	03f6bea02cab933509dd698dac98f6e8ab779b55	C:\Users\Neil Flannigan\Downloads\ The Help DVDRip XviD-DiAMOND	Match
The Help DVDRip XviD-DiAMOND	2	2097152	9505a6fd8a0a2eec6a13055152dd530eaeb0ce96	9505a6fd8a0a2eec6a13055152dd530eaeb0ce96	C:\Users\Neil Flannigan\Downloads\ The Help DVDRip XviD-DiAMOND	Match

Downloaded File/Folder Name	Piece Number	Piece length from torrent file	Calculated SHA1 Hash of [piece number] [piece length] bytes	Stored Hash on the torrent file	Full Path	Match/ Mismatch
The Godfather Trilogy Part 1, 2 & 3 DVDRip	1	4194304	575d7f647f17278477ed95ba19aa78674f30b7b6	575d7f647f17278477ed95ba19aa78674f30b7b6	C:\Users\Neil Flannigan\Downloads\ The Godfather Trilogy Part 1, 2 & 3 DVDRip	Match
The Godfather Trilogy Part 1, 2 & 3 DVDRip	2	4194304	fac8e34c2577e25e40ecb526ca3f95dca6a7cba5	fac8e34c2577e25e40ecb526ca3f95dca6a7cba5	C:\Users\Neil Flannigan\Downloads\ The Godfather Trilogy Part 1, 2 & 3 DVDRip	Match

IV. INVESTIGATIVE LEADS

48 more torrent files were found on C:\Users\Neil Flannigan\Downloads\ The Godfather Trilogy Part 1, 2 & 3 DVDRip\TSV Torrents\ directory. Initially it was mentioned that VMWare was installed on the computer. Forensic image of one of the VMs was shared for investigation. Further investigating other VMs might lead to new findings. BitTorrent is a peer-to-peer file sharing protocol. While users download a particular content, they are a part of a bigger network. Further investigations of network log can be done to check whether any kinds of files were being shared.

V. CONCLUSIONS

RIAA notified that the network of Acme Inc were utilized in copyright infringement. Network logs were directed towards a single user, Mr. Flannigan. Forensic image of one of VMs installed on Mr. Flannigan's computer has been investigated for any instance of copyright infringement. Windows 7 was installed as the operating system.

Investigation of the image revealed a BitTorrent client "uTorrent" installed on the system. Four folders were found on the disk engaging copyright piracy. It has been established that those files were indeed downloaded onto the system via BitTorrent client 'uTorrent' installed on the system.

VI. RECOMMENDATIONS

Pirated content has been found on Mr. Flannigan's computer. This should be reported to the higher management to take further actions as suitable.

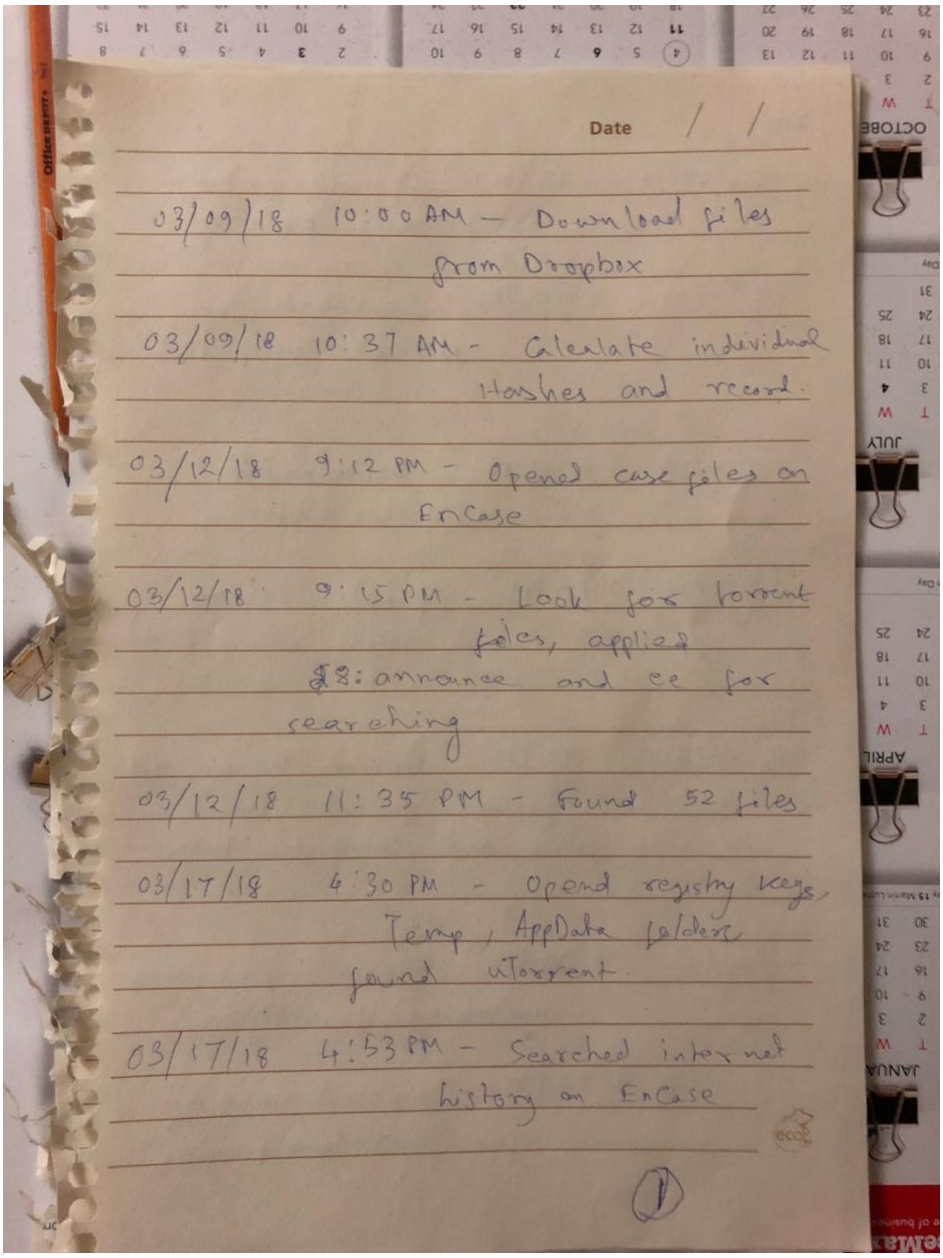
VII. REFERENCES

[1] https://www.howtogeek.com/318177/what-is-the-appdata-folder-in-windows/
[2] https://www.pcworld.com/article/2690709/windows/whats-in-the-hidden-windows-appdata-folder-and-how-to-find-it-if-you-need-it.html
[3] http://cdn.ttgtmedia.com/searchSecurityUK/downloads/RH6_Acorn.pdf
[4] http://www.forensicfocus.com/Forums/viewtopic/p=6585373/
[5] https://repository.royalholloway.ac.uk/file/b3857527-37ee-d134-e6c2-409c75d2605a/1/RHUL-MA-2008-04.pdf
[6] https://www.markscanlon.co/papers/ProjectMaelstrom.pdf
[7] https://community.spiceworks.com/topic/121790-how-do-i-find-users-internet-history-on-windows-7
[8] http://whatis.techtarget.com/definition/log-log-file
[9] https://en.wikipedia.org/wiki/Virtual_machine
[10] https://en.wikipedia.org/wiki/Torrent_file

VIII. GLOSSARY

Bencode Editor	Tool used for parsing torrent files.
BitTorrent	A protocol for peer-to-peer file sharing.
Byte	Collection of 8 binary digits (0s/1s).
EnCase	Digital Forensic investigation tool from Guidance Software.
Extension	Identifiers for a particular file to render using proper application
Forensic Explorer	Digital Forensic investigation tool.
Hard Disk	Storage device used for Read/Write.
Hash	Digital fingerprint used to verify integrity of a file.
HashCalc	Hash calculator tool.
Image File	Copy of a hard disk copied bit by bit in purpose of use it for forensic investigations.
Internet History	System or application specific files that indicate visited URLs in the past.
MD5	Message Digest algorithm to verify integrity of a file. Generates 128 bits unique fingerprint.

Network Log	Timestamped documentation of events in a network architecture.
Operating System	Central manager to all resources to a computer.
SHA1	Algorithm to verify integrity of a file. Generates 160 bits unique fingerprint.
Torrent Files	Used to download content using BitTorrent client. Has an extension ".torrent".
uTorrent	A BitTorrent client, software that end users use to download content.
Virtual Machine (VM)	Emulation of a computer system that allows running multiple Operating System on a single machine .
VMWare	Virtualization software provider.



Date / /

03/09/18 10:00 AM – Download files from Dropbox

03/09/18 10:37 AM – Calculate individual Hashes and record.

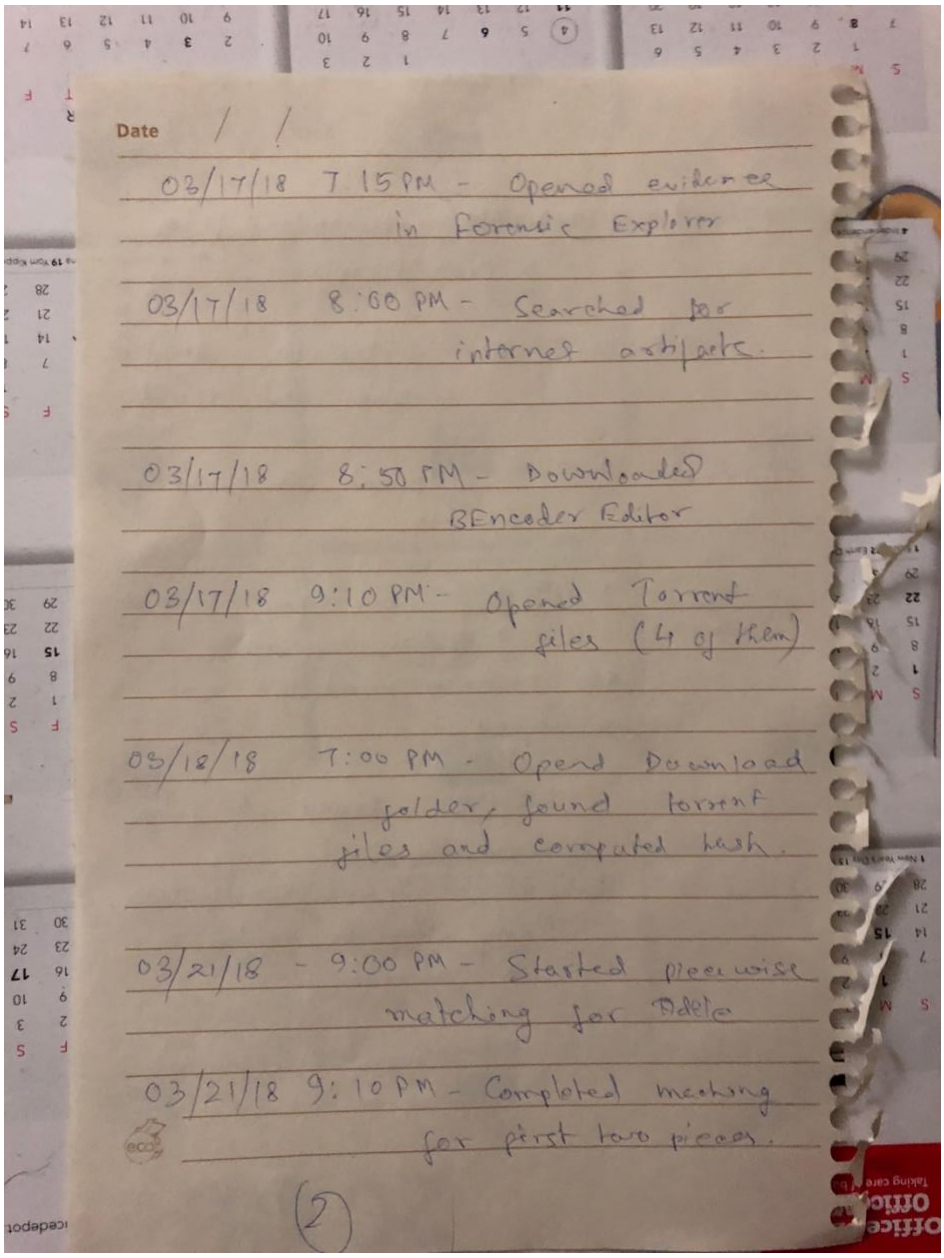
03/12/18 9:12 PM – Opened case files on EnCase

03/12/18 9:15 PM – Look for torrent files, applied ~~22~~: announce and cc for searching

03/12/18 11:35 PM – Found 52 files

03/17/18 4:30 PM – Opend registry keys, Temp, AppData folders, found uTorrent.

03/17/18 4:53 PM – Searched internet history on EnCase



Date / /

03/17/18 7:15 PM - Opened evidence in Forensic Explorer

03/17/18 8:00 PM - Searched for internet artifacts.

03/17/18 8:50 PM - Downloaded BEncoder Editor

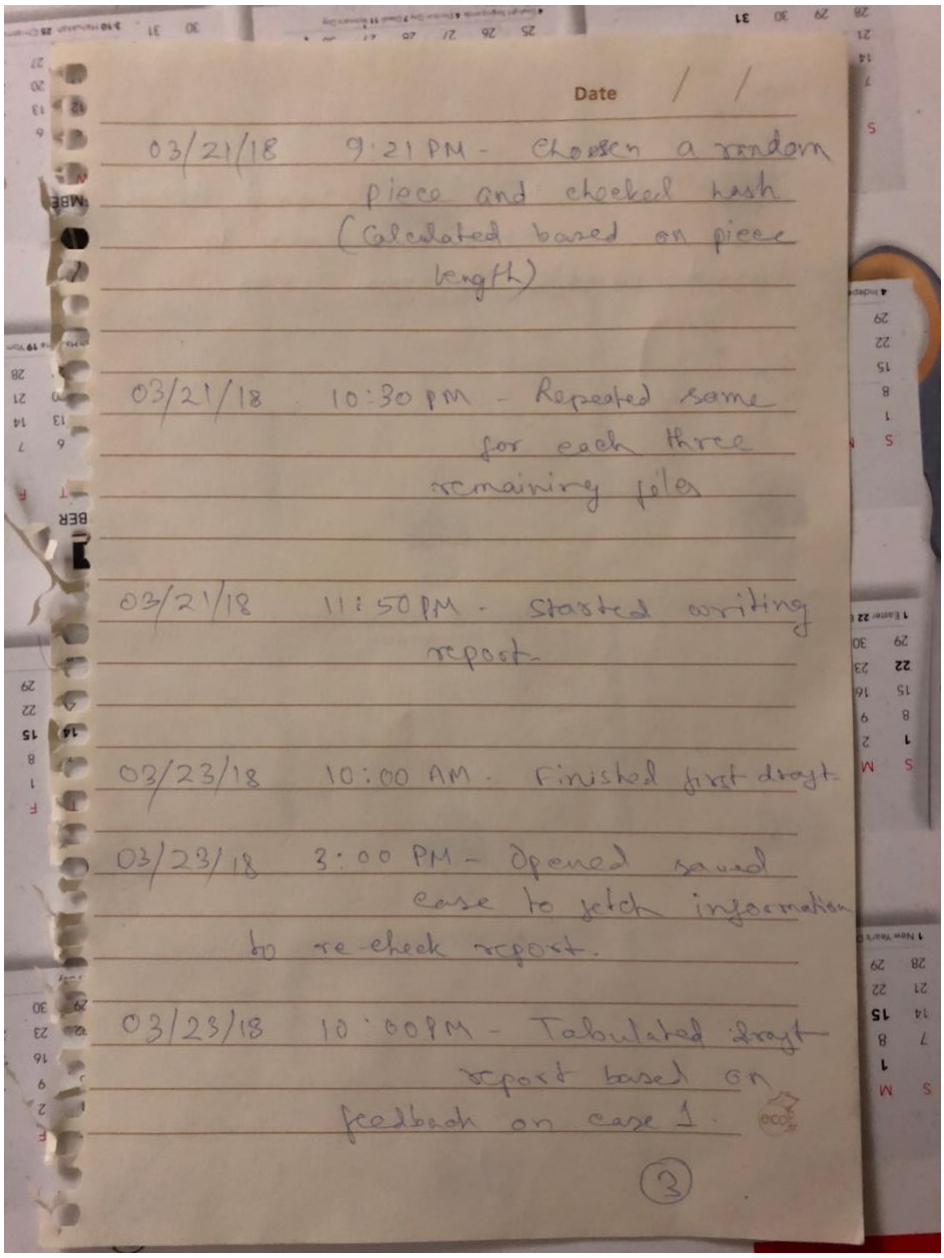
03/17/18 9:10 PM - Opened Torrent files (4 of them)

03/18/18 7:00 PM - Opend Download folder, found torrent files and computed hash.

03/21/18 - 9:00 PM - Started piecewise matching for Ddele

03/21/18 9:10 PM - Completed matching for first two pieces.

(2)



Date / /

03/21/18 9:21 PM - Choosen a random piece and checked hash (Calculated based on piece length)

03/21/18 10:30 PM - Repeated same for each three remaining files

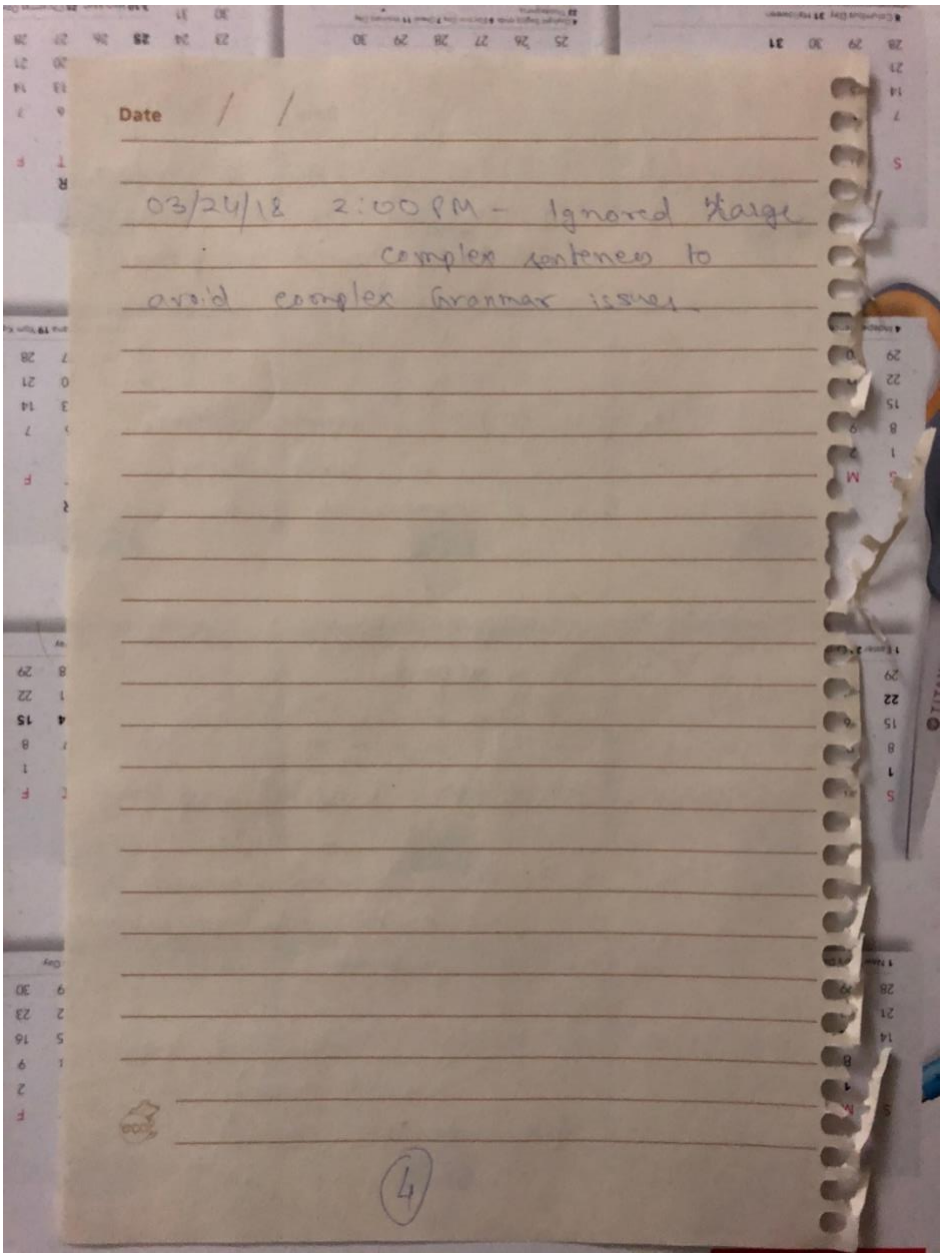
03/21/18 11:50 PM - Started writing report.

03/23/18 10:00 AM - Finished first draft

03/23/18 3:00 PM - Opened saved case to fetch information to re-check report.

03/23/18 10:00PM - Tabulated draft report based on feedback on case 1.

(3)


Date / /
03/24/18 2:00 PM - Ignored large complex sentences to avoid complex Grammar issues.
4