



Forensic Investigation Report for Clowning About Again

Bachelor of Science with Honours in Cyber Security

COURSEWORK 2

Unit Code: 201IT

Module: Computer Forensic

Lecturer: Ankit Saurabh

Report compiled by

Name: Chun Yoojin

Student Number: 11059949

Campus: Coventry University

Date of investigation: 15 June 2021

Date report compiled: 21 June 2021

Contents Page

1. Information of the Investigator	3
2. Case Background and Executive Summary	3
3. Executive Summary	3
4. Initial Assessment of the Case	4
5. Issues	
Issue #1: Content Relating to Offence	6
Issue #2: Identification	11
Issue #3: Intent	13
Issue #4: Quantity of Files	15
Issue #5: Installed Software	17
6. Conclusion	17
7. References	
Appendix #1: Run Sheet	17
Appendix #2: Timeline of Events	22

1. Information of the Investigator

This following report was conducted by Chun Yoojin who has 2 years in the Computer Science and Cyber Security education focussing on Network Defence, Investigation of Digital Evidence, Hacking and Cyber Security.

- Studying for Bachelor of Science with Honours in Cyber Security.
- Studied for Diploma in Network Defence and Forensic Investigation.
- Certified Ethical Hacking, EC council (97% Pass).
- Certified Hacking and Forensic Investigation, EC council (87% Pass).
- Certified Packet Tracer, Cisco (90% Pass).

2. Case background

Briefing of the case was given to me by Ankit Saurabh on 7th June 2021 with a request that I report him back with my findings related in the case.

The specific issues identified for investigation include:

It is known as illegal to access, own or distribute digital content related in clowns in UK. A witness claimed that the suspect Clark accessed content related to clown illegally at his workplace, and his computer was seized on a formal warrant.

The computer was acquired forensically by FTK Imager, but unfortunately, only logical acquisition was carried out by a junior investigator who owned the forensic image of the computer. While he wiped forensically the original hard drive from the computer, logical acquisition was performed forensically on sound manner.

Suspect Clark claims that he did not access any clown content and the computer was infected with malware by any potential content. However, he admitted that the computer belonged to him, and that he would lock it when he leaves workplace instead of always taking it home.

3. Executive Summary

Investigator is looking forward knowing the following:

- Does Clark access to clown content intentionally?
- Is there anyone who involved in this case?
- Dose Clark distribute clown content to someone else?

The outcome of this investigation:

This case is essentially concerned to own, access or disseminate digital content associated with clowns.

Clark is a suspect of this case, and there is a third party, Jerry Simpson. Clark communicated with Jerry Simpson since 18th June 2018, and he sent a zip file. There were 12 clown files, which are 9 jpeg, 1 mp4, and 2 pdf files in the zip file.

There was web history, which is 35 searching associated with clown content. Keywords that Clark has searched for are clowns, clowns:pdf, party clowns, and clown graphic images. And Clark downloaded jpg, mp4, and pdf files of clown content at 10 web pages in 3 times. The domain of website is scarymommy.com, deavita.net, onlinevideoconverter.com, theconversation.com, docdroid.net, massreview.org, trickortreatmagic.com.au, ebayimg.com, theredshtick.com, and fotosearch.com.

After Clark sent a zip file to Jerry Simpson, he does not want to involve with him anymore. So, he searched how to wipe hard drive in google and YouTube. Eventually, Clark sent an e-mail to his chief that his computer has been hacked and there is dodgy content on his computer.

However, Clark installed TrueCrypt on 7th June 2018 as his chief's suggestion in order to protect data. Furthermore, Clark does not agree that clown content is illegal, while he regards clowns as positive in his journal written on 25th June 2018.

In conclusion, it is for certain that Clark has accessed, owned, and distributed clown content illegally, but he is lying to cover this case.

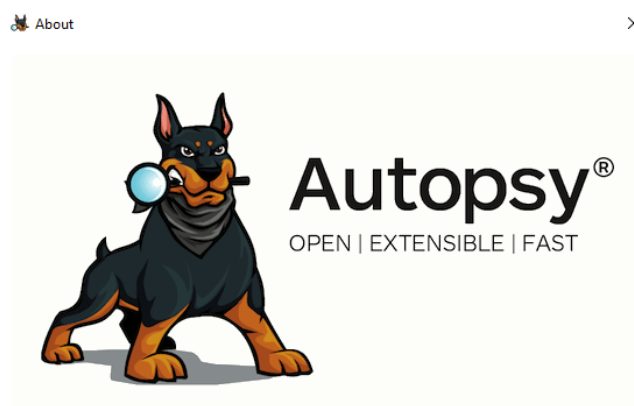
The rest of this report identifies these as Issue 1 to 5.

4. Initial Assessment of the Case

Software to be used in support of the investigation

This investigation will use Autopsy and FTK Imager to analyse Clark's hard drive.

In order to analyse Clark's hard drive and its data, Autopsy 4.18.0 will be used for this investigation. The "Domain Discovery" interface of Autopsy 4.18.0, which is the newest version, is a new method of reviewing web domains. This interface let user to focus on the domain. Below shows the details of the Autopsy.

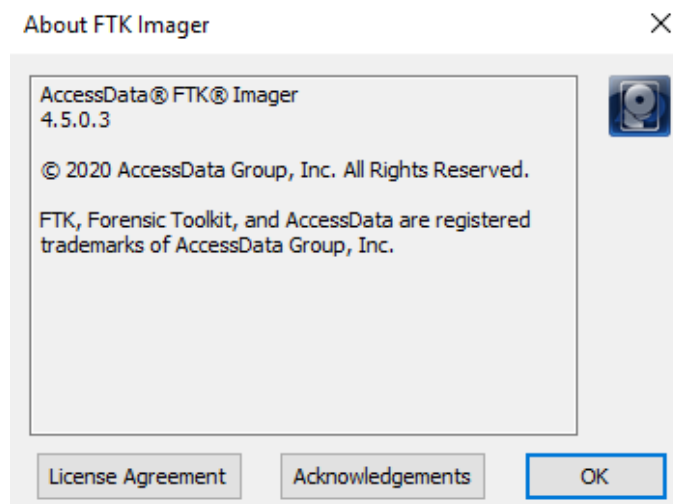


Autopsy™ is a digital forensics platform based on The Sleuth Kit™ and other tools.

- General Information: <http://www.sleuthkit.org>
- Training: <https://www.autopsy.com/support/training/>
- Support: <https://www.sleuthkit.org/support.php>

Copyright © 2003-2020.

Product Version: Autopsy 4.18.0 (RELEASE)
Sleuth Kit Version: 4.10.2
Netbeans RCP Build: 11.3-6b879cb782eaa4f13a731aff82eada11289a66f7
Java: 1.8.0_222-1-objdkbuild; OpenJDK 64-Bit Server VM 25.222-b10
System: Windows 10 version 10.0 running on amd64; Cp1252; en_SG (autopsy)
Userdir: C:\Users\Louis\AppData\Roaming\autopsy



FTK Imager 4.5.0.3 will be used as well as Autopsy. Investigator can preview a data and access electronic evidence to determine. Also, can create forensic images without changing to the original evidence. Below show the details of FTK Imager.

Initial Design Consideration


The investigation strategy is to conduct following steps.


- Understand the case 'Clowning About Again'
- Check workstation for investigation
- Create a new case in Autopsy and add data source of 202.dd
- Investigate the evidence and save and note every evidential value
- Conclude this forensic report with an evidential opinion


5. Issues

Issue #1: Content relating to offence

Clown content has been found in Clark's hard drive and Clark distributed clown content to third party, Jerry Simpson. Following files below are attached as a zip file and sent from Clark to Jerry Simpson, and FireFox is used for searching. There was total 12 files relating to clown content, which are 9 jpg, 1 mp4, and 2 pdf files in a zip file attachment. The files are listed in order of accessing and downloading.


	File Name	Scaryclown.jpg
	File Type	Image/jpeg
	Location	/img_202.dd/Users/computer/Pictures
	Status	Allocated
	MD5	ed873fc7b1f226bda891c1780341cdb2
	SHA-256	a55d63a0caee2637388da648d7ac77679a5b378a7984c264b3e7ec4e3703f9bc
	Modified	2018-06-18 08:20:06 SGT
	Changed	2018-06-18 08:20:06 SGT
	Accessed	2018-06-18 08:20:05 SGT
	Created	2018-06-18 08:20:04 SGT
	Size	58423
Analysis	<p>This file is the first file that Clark has downloaded at 08:20:06 SGT on 18th June 2018.</p> <p>However, Clark has received an e-mail from Jerry Simson that stop clowning about and working like a superman :) at 11:11:33 SGT at the same date. (Issue #2. Identification on e-mail communication)</p> <p>That is, Clark accessed to clown content before Jerry Simpson asks him to send him clown content, and Jerry Simpson has known about it that Clark has been accessing to clown content illegally.</p>	

	File Name	scary-halloween-costumes-ideas-Clown-blood-Halloween-party-costumes-e1410943909179.jpg
	File Type	Image/jpeg
	Location	/img_202.dd/Users/computer/Pictures/scary-halloween-costumes-ideas-Clown-blood-Halloween-party-costumes-e1410943909179.jpg
	Status	Allocated
	MD5	51632444d9845cc6686adcf24e536f77
	SHA-256	c6e12b7edde30a9a3bac012aef57a1ca7babee2c85264963a3397d2869835694
	Modified	2018-06-18 08:21:55 SGT
	Changed	2018-06-18 08:21:55 SGT
	Accessed	2018-06-18 08:21:54 SGT
	Created	2018-06-18 08:21:54 SGT
	Size	59178

	File Name	1492447345937.jpg


	File Type	Image/jpeg
	Location	/img_202.dd/Users/computer/Pictures/1492447345937.jpg
	Status	Allocated
	MD5	3e58af33ebb789d5d81cb4ac613a76c9
	SHA-256	1a2a3db8ac91540e39fe33c90a22672cb6e8028270d30dc686be65484d73f966
	Modified	2018-06-18 08:22:15 SGT
	Changed	2018-06-18 08:22:16 SGT
	Accessed	2018-06-18 08:22:15 SGT
	Created	2018-06-18 08:22:15 SGT
	Size	17134

Above 3 files are located at /img_202.dd/Users/computer/Pictures, and every file is searched in google with keyword 'clowns' and downloaded on 18th June 2018.

	File Name	Clowns dancing.mp4
	File Type	Video/mp4
	Location	/img_202.dd/Users/computer/Downloads/Clowns dancing.mp4
	Status	Allocated
	MD5	071f555cf58073ed4ebfb92915a8491a
	SHA-256	ee52d91c16629c1495b5a4d7d3770b92b6523b64555346082d353727f657ed73
	Modified	2018-06-18 10:45:41 SGT
	Changed	2018-06-18 10:48:12 SGT
	Accessed	2018-06-18 10:45:41 SGT
	Created	2018-06-18 10:45:47 SGT
	Size	3324223
Analysis	<p>Two clowns are dancing in this video, and it is the only video file in Clark's hard drive, and it has been accessed at 10:45:41 SGT on 18th June 2018. Location of this file [Users/computer/Downloads] indicates that Clark has downloaded and owned this clown content obviously.</p> <p>Also, it is evidence of distribution since this file has been sent as a zip file to Jerry Simpson on 9th June 2018.</p>	


	File Name	A Little Night Music – Send In The Clown.pdf
	File Type	Application/pdf
	Location	/img_202.dd/Users/computer/AppData/Roaming/Thunderbird/Profiles/1cug4fub.default/ImapMail/imap.gmail.com/[Gmail].sbd/Sent Mail/k13320412.zip/A Little Night Music - Send In The Clowns.pdf
	Status	Allocated
	MD5	4f640bc32c0ac35b585a814ee5235df4
	SHA-256	a28df73b0fc9d7a814c44e1e9418ab1c2fa6982e15fcdaf6c26cd42f8054aa7a
	Modified	2018-06-19 07:44:31 SGT




	Changed	2018-06-19 07:44:31 SGT
	Accessed	2018-06-19 07:44:24 SGT
	Created	2018-06-19 07:44:24 SGT
	Size	3146439
Analysis	This pdf file is piano sheets of SEND IN THE CLOWNS from the Musical a Little Night Music composed by Stephen Sondheim. I extracted this file from attachment of Clark's sent e-mail on 9 th July 2018 to Simpson. As shown in the Location, Clark used Mozilla Thunderbird to send e-mails, and Gmail was used to send e-mails.	


<p>THE MASSACHUSETTS REVIEW</p> <h3>War of the Clowns</h3> <p>ON THE TWO CLOWNS at themselves in arguing The people would stop, amazed, to watch them. —What's that? they asked. —Who could take them seriously? Radcliffe, the two comedians reported. The arguments were common nonsense, the theme was a nursery And as critic day passed. The following morning, the two remained, obnoxious and outdoing each other. It seemed as though, between them, even yucca soared. In the street, meanwhile, those present were exhilarated with the marketplace. The balloons began swarming their heads with fine-edged and fine-tuned hats. Believing it to be a show, the passersby left coins along the roadside. On the third day, however, the clowns arrived at acts of force. Their blows became a storm, their countenances stung more across air than across bodies. The children mimicked, imitating each other's blows. And they laughed at the two folk, their bodies tripping upon their own sides. And the boys wanted to repay the delightful goodness of the clowns. —Dad, give me some sense to have in the sidewalk. On the fourth day, the jabs and blows grew worse. Beneath their makeup, the faces of the clown began to bleed. Some kids became scared. What that true blood? —It was common, day for their parents scolded them. In fathers of trajectory, some were struck by directorless wallpops. But it was light fun, only serving to add to the laughs. More and more people joined the gallery. —What's going on? Nothing. A friendly unsettling of screams. It's not worth squinting down. They'll see out, it's nothing more than a bit of clowning around. On the fifth day, however, one of the clowns armed himself with a stick. Advancing on his adversary, he discharged a blow that tore off his wig. The other, furious, equipped himself with a symmetrical beating bar and responded with the same damage. The wooden rods whistled through the air in concert and delirium. One of the spectators, unexpectedly, was struck. The man fell, deadhead.</p>	File Name	Couto, Mia.pdf
	File Type	Application/pdf
	Location	/img_202.dd/Users/computer/Downloads/Couto, Mia.pdf
	Status	Allocated
	MD5	4f640bc32c0ac35b585a814ee5235df4
	SHA-256	a28df73b0fc9d7a814c44e1e9418ab1c2fa6982e15fcdaf6c26cd42f8054aa7a
	Modified	2018-06-19 07:46:34 SGT
	Changed	2018-06-19 07:46:34 SGT
	Accessed	2018-06-19 07:46:29 SGT
	Created	2018-06-19 07:46:29 SGT
	Size	118913
Analysis	This file is the Massachusetts Review on War of the Clowns, which is arguing of two clowns.	

Two pdf files are searched in google by keyword 'clowns:pdf' on 19th June 2018. The files were sent as a zip file from Clark to Jerry Simpson on 9th July 2018.


	File Name	kikkii_clown_party_pose.jpg
	File Type	Image/jpeg
	Location	/img_202.dd/Users/computer/Desktop/k13320412.zip
	Status	Allocated
	MD5	76e4975e5efc2a1268584fef7ade5f59
	SHA-256	55e8664e74345336a32b78e620c02426456424fae7a55843eda4a038ea6697df
	Modified	2018-06-19 07:50:08 SGT
	Changed	2018-06-19 07:50:06 SGT
	Accessed	2018-06-19 07:50:08 SGT
	Created	2018-06-19 07:50:05 SGT
	Size	50304

	File Name	s-l1640.jpg
	File Type	Image/jpeg
	Location	/img_202.dd/Users/computer/Pictures/s-l1640.jpg
	Status	Allocated
	MD5	dd42fe966af825567338e4f873cc2f6a
	SHA-256	c3c995ba9d01a4a4374f3afe77e3171150f0111cf3d431a5993cb94073c134b2
	Modified	2018-06-19 07:50:17 SGT


	Changed	2018-06-19 07:50:17 SGT
	Accessed	2018-06-19 07:50:17 SGT
	Created	2018-06-19 07:50:17 SGT
	Size	57620


	File Name	Ronald_mcdonald-e1476200032847-660x330.jpg
	File Type	Image/jpeg
	Location	/img_202.dd/Users/computer/Pictures/Ronald_mcdonald-e1476200032847-660x330.jpg
	Status	Allocated
	MD5	a3f7eb7ba08cb84137a85bf4683c6bca
	SHA-256	e9625404f351b7c0b5c496502f86def285b5a1a4e82c0cf38404d654e58d2a62
	Modified	2018-06-19 07:50:42 SGT
	Changed	2018-06-19 07:50:42 SGT
	Accessed	2018-06-19 07:50:41 SGT
	Created	2018-06-19 07:50:41 SGT
	Size	26494

Clark has searched party clowns at google.com.au on 19th June 2018. And he downloaded kikkii_clown_party_pose.jpg into /img_202.dd/Users/computer/Desktop, and other 2 of clown images into /img_202.dd/Users/computer/Pictures.

	File Name	k13320412.jpg
	File Type	image/jpeg
	Location	/img_202.dd/Users/computer/Desktop/k13320412.jpg
	Status	Allocated
	MD5	e5ab36f6264d22714a88d53338469f95
	SHA-256	9b083e21010e596163ff87740421540387dd571fe70995569748489a74da6739
	Modified	2018-07-02 09:15:08 SGT
	Changed	2018-07-02 09:15:08 SGT
	Accessed	2018-07-02 09:15:08 SGT
	Created	2018-07-02 09:15:08 SGT
	Size	35546

	File Name	k14032380.jpg
	File Type	image/jpeg
	Location	/img_202.dd/Users/computer/Desktop/k14032380.jpg
	Status	Allocated
	MD5	913cb94539abfe8de858ce16c0a40e99
	SHA-256	0cf32624479f6084c6fa52315917707645e1228bf3b709fb05adb560ab417bff
	Modified	2018-07-02 09:21:52 SGT

	Changed	2018-07-02 09:21:53 SGT
	Accessed	2018-07-02 09:21:52 SGT
	Created	2018-07-02 09:21:52 SGT
	Size	31837

	File Name	k7827739.jpg
	File Type	image/jpeg
	Location	/img_202.dd/Users/computer/Desktop/k7827739.jpg
	Status	Allocated
	MD5	39db918c4014d3a64fabbc17a2fe49a7
	SHA-256	9b67b8a39b5cc1c8d3d5634869605f5d202cfec4258aa516b1307cd73f5aa4a
	Modified	2018-07-02 09:22:15 SGT
	Changed	2018-07-02 09:22:15 SGT
	Accessed	2018-07-02 09:22:14 SGT
	Created	2018-07-02 09:22:14 SGT
	Size	41284
	Analysis	This file is last downloaded file at 09:22:15 SGT on 2 nd July 2018.

Clark searched clown graphic images at google.com.au on 2nd July 2018 and downloaded 3 image files at fotosearch.com. The files were found by searching keyword 'clown graphic' in google. Saved files on the Desktop has been sent to Jerry Simpson as a zip file with other 9 more jpg, mp4, and pdf files downloaded during 18th and 19th June 2018.

Issue #2: Identification

- **Identification on E-mail communication**
 - **E-mail communication with Jerry Simpson**

E-mail Communication			
From	Jazzasimpson0000@gmail.com	To	Kcent00@gmail.com
Date/Time	2018-06-18 11:11:33 SGT	Subject	clowning about
Body	stop clowning about and start working like a super man :)		
Analysis	There was a web history about clown searching started at 08:20:05 GST on 18 th June 2018. And Jerry Simpson sent an e-mail that stop clowning about and start working like a Super Man. Clark insisted that his computer has been hacked, and Jerry Simpson seemed to know Clark has searched clowns in google. Therefore, if Clark's computer is really hacked, Jerry Simpson can be a suspect who hacked Clark's computer.		

E-mail Communication 2			
From	Kcent00@gmail.com	To	Jazzasimpson0000@gmail.com
Date/Time	2018-07-02 10:20:09 SGT	Subject	Re: clowning about
Body	<p>How many am I send you and how do I get it to you?</p> <p>On 18/06/2018 11:11 AM, Jerry Simpson wrote: > stop clowning about and start working like a super man :)</p>		
Analysis	This e-mail is an obvious evidence of intent of this case. Clark replied to Jerry Simpson that how many contents he needs, as Clark wanted to distribute clown content to Jerry Simpson.		

E-mail Communication 3			
From	Jazzasimpson0000@gmail.com	To	Kcent00@gmail.com
Date/Time	2018-07-03 07:00:50 SGT	Subject	Re: clowning about
Body	The quantity here is relevant, just keep accessing/downloading the content and I will be in touch!		
Analysis	Jerry Simpson is a third party who involved in this case. He asked Clark to keep accessing and downloading to the content.		

E-mail Communication 4			
From	Kcent00@gmail.com	To	Jazzasimpson0000@gmail.com
Date/Time	2018-07-09 11:24:08 SGT	Subject	Re: clowning about
Body	<p>I am done with this game. This is what I got, now leave me alone!!!!</p> <p>On 3/07/2018 7:00 AM, Jerry Simpson wrote: > The quantity here is relevant, just keep accessing/downloading the > content and I will be in touch!</p>		
Analysis	In this e-mail, there was a zip file attachment of 12 clown content. The files are 9 jpg files, 1 mp4 file, and 2 pdf files associated with clown. This is the conclusive evidence that Clark has distributed clown content illegally.		

E-mail Communication 5			
From	Jazzasimpson0000@gmail.com	To	Kcent00@gmail.com
Date/Time	2018-07-10 09:41:42 SGT	Subject	Re: clowning about
Body	<p>No, no, you are not done, I want more, more clown content!</p> <p>On Mon, Jul 9, 2018 at 11:24 AM, Clark <kcent00@gmail.com> wrote: I am done with this game. This is what I got, now leave me alone!!!!</p> <p>On 3/07/2018 7:00 AM, Jerry Simpson wrote: The quantity here is relevant, just keep accessing/downloading the content and I will be in touch!</p>		
Analysis	Clark does not want to contact with Jerry Simpson anymore, but Simpson asked Clark that download clown content more.		

- **E-mail communication with Clark's Chief**

E-mail Communication 1			
From	Kcent00@gmail.com	To	sassypenguin0@gmail.com

Date/Time	2018-07-11 08:11:46 SGT	Subject	Recent data breach
Body	<p>Hi Chief,</p> <p>I go to work today and I think my computer has been hacked. There is all this dodgy content on the computer that I didn't put there. I don't know what to do...I will come by your office in a few minutes!</p> <p>On 3/05/2018 8:12 AM, Sassy Penguin wrote:</p> <p>> Clark,</p> <p>></p> <p>> As a result of our recent minor security breach I am asking everyone</p> <p>> to protect their data, Jimmy here suggested using a tool TrueCrypt.</p> <p>> You're a clever boy, I'm sure you can figure out how to use it.</p> <p>></p> <p>> Regards,</p> <p>></p> <p>> Chief</p>		
Analysis	Clark is telling a lie to his chief that he does not download any clown content and his computer has been hacked. He wants to avoid from this case and is asking for his chief's help.		

- **Document saved on PC**

File Name	Journal.doc
File Type	application/MSword
Location	/image_202.dd/Users/computer/Documents/Journal.doc
Status	Allocated
MD5	c53b7d63c8a0787b897584819a4f8d0f
SHA-256	7285b7e39f0f8f5ff21ea9e102673067355df894cf21687726d043242f54523c
Accessed	2018-05-02 12:23:52 SGT
Created	2018-05-02 12:23:52 SGT
Modified	2018-07-11 08:16:20 SGT
Changed	2018-07-11 08:16:20 SGT
Size	50176

June 25, 2018

Why are pictures of clowns illegal? I mean they are just scary, dangerous, life threatening clowns that typically appear in horror movies. I wonder if you would ever see a clown with a red balloon that would be very funny and secretive.

This file is a journal of Clark created on 2nd May 2018. On 25th June 2018, there is a Clark's opinion on clown. In this journal, it can be regarded as that Clark does not agree that clown content is illegal, rather, he is thinking of clown positively. This file was discovered from Documents/Office folder in Autopsy.

Issue #3: Intent

- Internet history by FireFox

Following chart shows that Clark downloaded clown content illegally and proves his allegation.

Keyword/date	Download clown content		
	Domain	File name	Time/URL
Clowns 2018-06-18	Scarymommy.com	Scaryclown.jpg	08:20:05 SGT http://www.scarymommy.com/wp-content/uploads/2016/10/scaryclown.jpg?w=697
	Deavita.net	scary-halloween-costumes-ideas-Clown-blood-Halloween-party-costumes-e1410943909179.jpg	08:21:54 SGT https://deavita.net/wp-content/uploads/2014/09/scary-halloween-costumes-ideas-Clown-blood-Halloween-party-costumes-e1410943909179.jpg
	onlinevideoconverter.com	Clowns dancing.mp4	10:45:41 SGT https://s34.onlinevideoconverter.com/download?file=h7h7d3j9i8j9b1
	theconversation.com	The psychology behind why clowns creep us out	10:50:27 SGT http://theconversation.com/the-psychology-behind-why-clowns-creep-us-out-65936
Clowns:pdf 2018-06-19	docdroid.net	A Little Night Music - Send In The Clowns.pdf	07:44:24 SGT https://www.docdroid.net/file/download/bbvya/a-little-night-music-send-in-the-clowns.pdf
	massreview.org	Couto, Mia.pdf	07:45:24 SGT https://www.massreview.org/sites/default/files/Couto,%20Mia.pdf
Party clowns 2018-06-19	trickortreatmagic.com.au	kikkii_clown_party_pose.jpg	07:50:06 SGT http://www.trickortreatmagic.com.au/img/kikkii_clown_party_pose.jpg
	ebayimg.com	s-l640.jpg	07:50:17 SGT

			https://ssli.ebayimg.com/images/g/2vUAAOSwpx9W8gwu/s-l640.jpg
	theredshtick.com	Ronald_mcdonald-e1476200032847-660x330.jpg	07:50:41 SGT http://theredshtick.com/wp-content/uploads/2016/10/Ronald_mcdonald-e1476200032847-660x330.jpg
Clown graphic images 2018-07-02	fotosearch.com	k13320412.jpg	09:15:08 SGT https://fscomps.fotosearch.com/compc/CSP/CSP992/a-clown-wearing-a-green-costume-clipart__k13320412.jpg
		Clipart of Clown face k14032380 - Search Clip Art, Illustration Murals, Drawings and Vector EPS Graphics Images - k14032380.eps	09:21:35 SGT https://www.fotosearch.com/CSP992/k14032380/
		Clip Art of clown k7827739 - Search Clipart, Illustration Posters, Drawings, and EPS Vector Graphics Images - k7827739.eps	09:21:57 SGT https://www.fotosearch.com/CSP782/k7827739/

Clark has been searching clown content on 18th and 19th June, and 2nd July. He used FireFox to search and download clown content. He approached to clown content in 3 times and searched 4 keywords associated with clown. The keywords Clark searched in google are 'clowns' on 18th June, 'clowns:pdf' and party clowns on 19th June, and clown graphic images on 2nd July 2018.

Following chart proves Clark accessed and owned clown content intentionally as he tried to wipe evidence he accessed and owned.

Search Engine/date	Try to destroy evidence		
	Domain	Keyword	Time/URL
Google.com 2018-07-10	Google.com.au	Erasing data	10:28:47 SGT https://www.google.com.au/search?source=hp&ei=ExIEW6f9Jo_U-Qb0o5XwDA&q=erasing+data&oq=erasing+data&gs_l=psy-ab.3..0l10.24700.26135.0.26879.12.7.0.0.0.0.431.719.2-1j0j1.2.0....0...1c.1.64.psy-ab..10.2.714....0.tQLZw7pCpRI
		Erase hard disk	10:42:10 SGT https://www.google.com.au/search?ei=PxlEW4CeE8Pp0ASZu45w&q=erase+hard+disk&oq=erase+hard+disk&gs_l=psy-ab.3..0l10.796092.798455.0.799102.15.10.0.0.0.0.610.2082.3-3j1j1.5.0....0...1c.1.64.psy-ab..10.5.2077....0.fmPn8X84ao4
Youtube.com 2018-07-10	Youtube.com	How to Wipe Your Hard Drive: a Geek squad 2 Minute Miracle	10:43:08 SGT https://www.youtube.com/watch?v=ewisIDG-K-E

Clark searched how to wipe his data and hard disk to destroy evidence of this case. He searched at google.com and youtube.com.

Issue #4: Quantity of Files

File Type		Number of files related in this case	Number of files in the system
By Extension	Images	12	51341
	Videos	4	434
	Audio	4	380
	Archives	0	669
	Databases	0	115
Documents	HTML	2	905
	Office	1	27
	PDF	9	13
	Plain Text	0	325
	Rich Text	0	91
Deleted Files	File System	0	47823
	All	0	54809
Total Quantity of Files		32	181702

A total of 181702 files have been found in the system, and 32 of them were associated with Clown content. Image file is mentioned at issue #1. Both video and audio files' name are clown dancing, and audio files are from video file 'clowns dancing.mp4.' Also, there were 2 HTML and 1 doc file in office folder. The doc file is Clark's journal about clown shown above. This chart proves that Clark owned clown content personally.

Attachments below prove quantity of files.

- Audio

Find and Replace

Find what: clown

Options >>

Find All Find Next Close

Book	Sheet	Name	Cell	Value	Formula
Audio 20210624104529.csv	Audio 20210624104529	\$A\$301		Clowns dancing.mp4:Zone.Identifier	
Audio 20210624104529.csv	Audio 20210624104529	\$A\$302		Clowns dancing.mp4	
Audio 20210624104529.csv	Audio 20210624104529	\$A\$380		Clowns dancing.mp4	
Audio 20210624104529.csv	Audio 20210624104529	\$A\$381		Clowns dancing.mp4	

- PDF

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Met Known)	Location	MDS Hash SHA-256	H-MIME Typ	Extension		
2	A Little Night Music - Send In The Clowns.pdf	2018-06-19 07:44:31 SGT	2018-06-19 07:44:31 SGT	2018-06-19 07:44:24 SGT	2018-06-19 07:44:24 SGT	3146439	Allocated	Allocated unknown	/img_202_4f640bc32 a28df730c applicatio	pdf				
3	A Little Night Music - Send In The Clowns.pdf:Zone.Identifier	2018-06-19 07:44:31 SGT	2018-06-19 07:44:31 SGT	2018-06-19 07:44:24 SGT	2018-06-19 07:44:24 SGT	26	Allocated	Allocated unknown	/img_202_1b0cf34d9 eac0951: text/plain	pdf				
4	Couto, Mia.pdf	2018-06-19 07:46:34 SGT	2018-06-19 07:46:34 SGT	2018-06-19 07:46:29 SGT	2018-06-19 07:46:29 SGT	118913	Allocated	Allocated unknown	/img_202_96ac7e4f3 47b65083f applicatio	pdf				
5	Couto, Mia.pdf:Zone.Identifier	2018-06-19 07:46:34 SGT	2018-06-19 07:46:34 SGT	2018-06-19 07:46:29 SGT	2018-06-19 07:46:29 SGT	26	Allocated	Allocated unknown	/img_202_1b0cf34d9 eac0951: text/plain	pdf				
6	TrueCrypt User Guide.pdf	2018-06-07 08:53:48 SGT	2018-06-07 08:53:48 SGT	2018-06-07 08:53:48 SGT	2018-06-07 08:53:48 SGT	523969	Allocated	Allocated unknown	/img_202_60b1ea96 739d7a00i applicatio	pdf				
7	manual.pdf	2003-10-15 16:34:04 SGT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	61507	Allocated	Allocated unknown	/img_202_1240cc90c 55cbfae16 applicatio	pdf				
8	manual_es.pdf	2003-10-15 16:34:08 SGT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	63678	Allocated	Allocated unknown	/img_202_84ccc8a6c ebf264d2i applicatio	pdf				
9	A Little Night Music - Send In The Clowns.pdf	2018-06-19 07:44:32 SGT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3146439	Allocated	Allocated unknown	/img_202_4f640bc32 a28df730c applicatio	pdf				
10	Couto, Mia.pdf	2018-06-19 07:46:36 SGT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	118913	Allocated	Allocated unknown	/img_202_96ac7e4f3 47b65083f applicatio	pdf				
11	A Little Night Music - Send In The Clowns.pdf	2018-06-19 07:44:32 SGT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3146439	Allocated	Allocated unknown	/img_202_4f640bc32 a28df730c applicatio	pdf				
12	Couto, Mia.pdf	2018-06-19 07:46:36 SGT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	118913	Allocated	Allocated unknown	/img_202_96ac7e4f3 47b65083f applicatio	pdf				
13	manual.pdf	2003-10-15 16:34:04 SGT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	61507	Allocated	Allocated unknown	/img_202_1240cc90c 55cbfae16 applicatio	pdf				
14	manual_es.pdf	2003-10-15 16:34:08 SGT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	63678	Allocated	Allocated unknown	/img_202_84ccc8a6c ebf264d2i applicatio	pdf				

- HTML

Find and Replace

Find what: clown

Find Replace

Issue #5: Installed Software

Date/Time	Program Name	Data Source	Analysis
2017-03-19 02:30:02 SGT	MPlayer2	202.dd	It has been used for watching clowns dancing.mp4.
2018-05-02 02:32:06 SGT	Mozilla Maintenance Service v.59.0.3	202.dd	Clark installed this software to maintain Mozilla program.
2018-06-07 00:00:43 SGT	Mozilla Thunderbird 52.8.0 (x86 en-US) v.52.8.0	202.dd	It was installed for sending e-mail to communicate with Jerry Simpson.
2018-06-07 00:53:48 SGT	TrueCrypt v.7.1a	202.dd	It was installed as Clark's chief has suggested to install to protect data.
2018-06-18 02:40:11 SGT	Mozilla Maintenance Service v.60.0.2.6730	202.dd	Clark installed newest software of Mozilla Maintenance Service to maintain Mozilla program.
2018-06-18 23:54:58 SGT	Mozilla Firefox 60.0.2 (x64 en-US) v.60.0.2	202.dd	It was installed to search and download illegal clown content.

6. Conclusion

In this investigation, few evidence has been found, which is indicating that Clark is a prime suspect of this case.

- Clark used FireFox to search and download clown content, which is excellent at security and protecting user privacy.
- There was web history that Clark accessed to and downloaded various clown content.
- As shown in e-mail communication 2 with Jerry Simpson, Clark asked that 'how many am I send you and how do I get it to you?' to distribute clown content intentionally.
- In Clark's sent mail, there was a zip file attachment of 12 clown content. It was sent to Jerry Simpson on 9th July 2018.
- In Clark's journal, Clark is thinking of clown positively and does not agree that clown content is illegal.
- Clark tried to wipe his hard drive to erase every evidence of this case.

Every evidence is for certain that Clark accessed, owned, and distributed to clown content intentionally and illegally. In addition, Clark is telling lie to his chief that he did not put any clown content into his computer and his computer has been hacked.

Plus, there is a third party involved in this case, who is Jerry Simpson, and he asked Clark to send clown content more.

In conclusion, Clark's allegation is obviously proven as a guilty and Jerry Simpson is involved in this case as well.

7. References

Appendix #1: Run Sheet

Activity	Date/Time /Duration	Outcome	Notes
Download a copy of file	15/06/2021 09:18 (0:04:02)	Successful	Downloaded a copy of files from Clark's hard drive and saved at E:\Coventry\CF\CW2\evidence\202.
Extract file	17/06/2021 11:11 (0:27:03)	Successful	Extracted downloaded files by 7-zip. Name: 202 Date modified: 11/07/2018 08:25 Type: DD File Size: 4,193,280 KB
Add image	18/06/2021 23:52 (0:12:32)	Successful	Added image of 202.dd to FTK Imager.
Create directory listing	19/06/2021 01:59	Failed	Created directory listing to search keywords related in this case. Status: Failure: cached_drive_image: read_blocks: index out of bounds
Resume process	19/06/2021 02:26	Successful	Deleted all files and resumed from downloading a copy of files from Clark's hard drive.
Create case	20/06/2021 01:42 (0:12:44)	Successful	Created case 001.aff in white colour 4GB USB. Drive/Image Verify Results: Sector count: 7862272 MD5 Hash: c4c1eb0ae7f2b7b9043461c3d58ee00b SHA1 Hash: a636b607f8985ce73970eb1374d92ca0a35e0564 Bad Sector: No bad sectors found
Add evidence item	20/06/2021 02:10 (0:10:09)	Successful	Added evidence item to FTK Imager (Logical Drive).
Export file	20/06/2021 02:29	Failed	Exported image file of internet explorer of root from FTK Imager.
Export disk image	20/06/2021 03:11 (0:08:00)	Successful	Exported disk image of root from FTK Imager. Sector count: 8386560 MD5 Hash: aee8aa6f93da67717bd5896f3aa052b2 SHA1 Hash: 7267d7446ba9339b429fc806b1fd333612fe032e Bad Sector: No bad sectors found
Create case	20/06/2021 03:25	Successful	Created a new case to Autopsy.

Add data source	20/06/2021 03:32	failed	Added data source to Autopsy. Status: No files were found for the selected filters.
Add evidence item	20/06/2021 03:46	Successful	Added evidence item to FTK Imager (Image file).
Export disk image	20/06/2021 03:49 (0:05:18)	Successful	Exported disk image of 202.dd from FTK Imager.
Create case	20/06/2021 04:01	Successful	Created a new case to Autopsy. New folder named Cache, Config, Export, Log, ModuleOutput and Reports, and new files named 001.aut, autopsy.db and SolrCore.properties have been created. 21 Files, 25 Folders Size: 869 KB (890,012 bytes) Size on disk: 888 KB (909,312 bytes)
Add data source	20/06/2021 04:02	Failed	Add data source to Autopsy. Nothing can be found.
Create case	20/06/2021 15:55	Successful	Created a new case
Add data source	20/06/2021 15:56 (0:00:04)	Failed	Data source added (Non-critical errors encountered). Errors occurred while ingesting image. 1. Error reading image file (tsk_fs_read: Offset missing in partial image: 17334617088)) (Error walking directory in file system at offset 0) 2. Error reading image file (tsk_fs_block_get: Address missing in partial image: 1062116)) (TskAutoDbJava::addFsInfoUnalloc: error walking fs unalloc blocks, fs id: 2) Possible Incomplete Image: Error reading file system at offset 19,880,992,768
Resume process	20/06/2021 17:39 (0:01:17)	Failed	Deleted all files and proceed from creating disk image (AFF) to FTK Imager. 202.dd is from E:\Coventry\CF\CW2\evidence\202. Status: Low Disk Space Warning FTK Imager need 117359 MB to write the next image segment.
Resume process	21/06/2021 06:00	Successful	Deleted all files related in this case.

Download file	21/06/2021 07:46 (0:15:00)	Successful	Downloaded a copy of zip files named 202.7z.001-008 into host PC.
Unzip file	21/06/2021 08:03	Failed	Extracted all downloaded files to C:\Users\Genie\Desktop\Forensic Investigation. Status: There is not enough space on the disk.
Clear apps	21/06/2021 08:08	Clear	Uninstalled program files in the PC.
Unzip file	21/06/2021 08:27 (0:02:24)	Successful	Extracted all downloaded files to C:\Users\Genie\Desktop\Forensic Investigation.
Unzip 202.dd	21/06/2021 08:30 (0:02:20)	Failed	Extracted 202.dd file to C:\Users\Genie\Desktop\Forensic Investigation. Status: There is not enough space on the disk. Deleted all files and empty Recycle Bin by mistake.
Download file	21/06/2021 08:41 (0:15:00)	Successful	Downloaded a copy of zip files named 202.7z.001-008 into E:\Forensic Investigation.
Unzip file	21/06/2021 09:33 (6:20:00)	Failed	Extracted a copy of zip files into E:\Foensic Investigation. Cannot set length for output file. There is not enough space on the disk. E:\Forensic Investigation\202.dd. Repeated deleting and downloading files until 15:53 and failed all. Went to buy a new laptop.
Download Software	22/06/2021 10:02 (1:05:00)	Successful	Downloaded Software, which is Autopsy, FTK Imager, and 7zip.
Download file	22/06/2021 11:08	Successful	Downloaded a copy of zip files named 202.7z.001-008 into E:\Downloads.
Unzip file	22/06/2021 11:11 (0:05:44)	Successful	Extracted files to E:\Downloads.
Unzip 202.dd	22/06/2021 11:20	Failed	Extracted 202.dd to E:\Downloads. Status: Cannot create symbolic link: A required privilege is not held by the client. E:\Downloads\Users\All Users. Deleted all files and ran 7zip as Admin.

Download file	22/06/2021 11:36 (0:03:00)	Successful	Downloaded a copy of zip files named 202.7z.001-008 into E:\Downloads in right order from 001 to 008.
Unzip file	22/06/2021 11:40	Failed	Extracted 202.7z.001. Status: E:\Downloads\202.7z.001 202.7z Cannot open the file as [7z] archive. Unexpected end of data.
Unzip file	22/06/2021 11:45 (0:10:39)	Successful	Extracted 202.7z.001 file into E:\Downloads. Extracted 202.dd file into E:\Downloads.
Add case and data source	22/06/2021 11:57 (0:06:11)	Successful	Added a new case to Autopsy 4.18.0. Added data source to Autopsy 4.18.0. Status: Data source has been added to the local database. Files are being analysed.
Investigate evidence image	22/06/2021 12:04	Found	Found evidence images associated with clown at /img_202.dd/Users/computer/Pictures using Autopsy.
Extract evidence images	22/06/2021 17:17	Successful	Extracted evidence images both relating and not relating to clown.
Investigate video	22/06/2021 18:15	Found	Found clowns dancing.mp4 in video folder of view in Autopsy.
Add evidence image	23/06/2021 17:15	Successful	Added evidence images found from Autopsy to FTK Imager to examine Hash and MAC time.
Investigate clown image	23/06/2021 17:34 (0:40:00)	Found	Explored Autopsy to find clown image by using keyword search in Autopsy. Status: 153 image files of clown have been searched in Clark's hard drive.
Investigate e-mail communication	23/06/2021 18:24 (1:40:11)	Found	Found e-mail communication of Clark and Jerry Simpson. There was total 5 communication, and 1 zip file attachment of 12 clown content which are jpg, mp4 and pdf file. This is the concise evidence that Clark has distributed clown content illegally.
Autopsy error	24/06/2021 20:01 (1:40:00)	Error	Autopsy program had an error. Saved case and exited Autopsy. Configured system and restarted PC.
Open case	24/06/2021 21:41	Successful	Opened 202.dd case in Autopsy.
Investigate doc	24/06/2021 21:55 (0:5:06)	Found	Found Clark's journal in Documents/Office folder in Autopsy.

			Clark wrote his opinion down about clown that clown is not bad content.
Investigate pdf folder	24/06/2021 22:05 (0:03:00)	Found	Found pdf files related in clown content in pdf folder in Autopsy.
Investigate web history	24/06/2021 22:18 (0:04:00)	Found	Found web history Clark has searched clown content in google.com and downloaded clown content in various web pages. Clark used FireFox.
Investigate software	24/06/2021 22:32 (0:22:00)	Found	Found installed software involved in this case.
Save case	25/06/2021 05:02	Saved	Saved case and exit Autopsy.

Appendix #2: Timeline of Events

2018-06-18	Clark received an e-mail from Jerry Simpson.
2018-06-18	Clark installed FireFox and searched clown content at google.com.
2018-06-19	Clark continued searching and downloading clown content.
2018-06-25	Clark wrote a journal down about clown.
2018-07-02	Clark had interest in Jerry Simpson's e-mail and replied to him.
2018-07-03	Simpson instigated accessing/downloading clown content to Clark.
2018-07-09	Clark sent a zip file attachment of clown content to Jerry Simpson.
2018-07-10	Jerry Simpson asked Clark that send clown content more.
2018-07-10	Clark searched how to wipe hard drive and data at google.com and youtube.com.
2018-07-11	Clark sent an e-mail to his chief that his computer has been hacked and there is dodgy content inside.

