DIGITAL FORENSICS INVESTIGATION REPORT

COMPUTER FORENSICS - PSB201IT

CASE : 202-PSB201IT-LE-20210607

INVESTIGATOR : YANG, HEETAK (LESLIE) - 11059972

Table of Contents

Summary

Although accessing clown content is illegal in Singapore, law enforcement has reported that witnesses have seen access to clown content. Upon approval of the official warrant, the computer in question was confiscated from work. The computer was then forensically acquired using the FTK Imager. The problem was that only logical acquisitions were executed, the original hard drive was forensically erased. Nevertheless, the logical argument was performed in a forensically sound manner.

The suspect, Clark negates accessed to the clown content, but Clark testified that the confiscated computer belonged to him. He stated that he did not lock it when he was away from the computer and that he was infected with malware.

As a digital forensics' consultant, I was tasked with investigating Clark's computer files that were duly confiscated. Therefore, I analyse the obtained image file 202.dd to collect and analyse all the evidence. Evidence includes file systems, photos, document files, email history, web browsing history, web browsing history, web download history, web cookies, remote access logs, and installed malware. The primary tool used for the investigation was Autopsy, which was analysed based on SGT's time. In the case of the drawn image, the data protection chain was safely protected using Write Blocking using regedit.msc, and the tool basically used for the investigation was Autopsy, and the time of SGT was taken as the standard.

Next are the disk image details found through Autopsy, CertUtil.

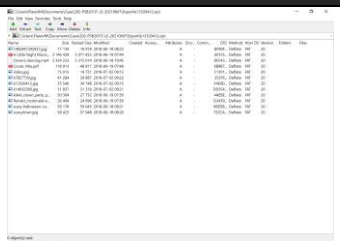
Basic Information			
Name	202.dd	**Image Type**	Raw (DD File)
Source data size	19881000960 bytes	**Source Type**	Logical
Bytes per sector	512	**Sector Count**	38,830,080
MD5	15f5d5224b4bed8a97b6fc0c2a7ecfbc		
SHA1	e710298646c46ee8ff70a96cd4d28423fe274eeb		
SHA256	63e1d27a9a36f0d6c5fc4305197c39e83491220d11bead185bebd29c5ce31871		
Autopsy - Data Source			
Name	202.dd	**Type**	Image
Size	19881000960 bytes (19.88 GB)	**Image Type**	Raw Single
Unallocated Space	883534801 bytes (883.1 MB)	**Sector Count**	38,830,080
Time Zone	Asia/Singapore – SGT (GMT +8:00)	**Sector Size**	512 bytes
Files	426294	**Results**	19694
MD5	15f5d5224b4bed8a97b6fc0c2a7ecfbc		
SHA1	e710298646c46ee8ff70a96cd4d28423fe274eeb		
SHA256	63e1d27a9a36f0d6c5fc4305197c39e83491220d11bead185bebd29c5ce31871		
Case Name/No.	202-PSB201IT-LE-20210607 / 001		
Autopsy - Operating System Information			
Computer Name	DESKTOP-MMAUQ8G	**Version**	Windows_NT
Architecture	AMD64	**Program Name**	Windows Home
Product ID	00326-10000-00000-AA693	**Date/Time**	2017-05-08 23:53:51

Issue #1 - Presentation of content relating to offence

Evidence is related clown content found after Autopsy analysis of the contents of Clark's laptop imaged as a 202.dd file. All data related to Clown stored inside have been investigated and analysed and recorded. A total of 18 violations were identified on user who username is computer in the 202.dd file.

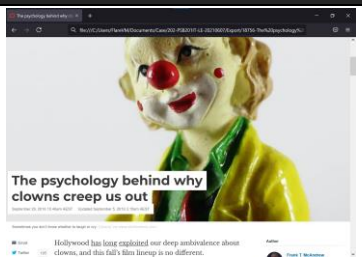
Evidence 1			
	**Name**	Index.jpg	
	Source of Path	/img_202.dd/Users/computer/Desktop/index.jpg	
	MIME Type	Image/jpeg	
	Size	15015 bytes	
	MD5	64b61cf19e916bc1a40831a17db83b3b	
	SHA-256	4f921d8db4b7cff9ee643c3ff7b52e794d75714fff30720ca58959825580a395	
	Internal ID	18731	
Modified	2018-07-02 09:12:30 SGT	**Created**	2018-07-02 09:12:29 SGT
Accessed	2018-07-02 09:12:30 SGT	**Changed**	2018-07-02 09:12:30 SGT
Analysis Comments	Illustration of a clown in green clothes and hat who has orange hair and has instruments like mandolin downloaded via Firefox to the Desktop folder.		

Evidence 2			
	**Name**	k13320412.jpg	
	Source of Path	/img_202.dd/Users/computer/Desktop/k13320412.jpg	
	MIME Type	Image/jpeg	
	Size	35546 bytes	
	MD5	e5ab36f6264d22714a88d53338469f95	
	SHA-256	9b083e21010e596163ff87740421540387dd571fe70995569748489a74da6739	
	Internal ID	18734	
Modified	2018-07-02 09:15:08 SGT	**Created**	2018-07-02 09:15:08 SGT
Accessed	2018-07-02 09:15:08 SGT	**Changed**	2018-07-02 09:15:08 SGT
Analysis Comments	Illustration of a clown in green clothes and hat who has orange hair was downloaded via Firefox to the Desktop folder. It downloaded from https://fscomps.fotosearch.com/compc/CSP/CSP992/a-clown-wearing-a-green-costume-clipart__k13320412.jpg		

Evidence 3			
	**Name**	k13320412.zip	
	Source of Path	/img_202.dd/Users/computer/Desktop/k13320412.zip	
	MIME Type	application/zip	
	Size	6743961 bytes	
	MD5	0d02f72a78dc200911804a801555715a	
	SHA-256	b22bd5875880528522d39c8405598e2d8cb61203079199fd2eaf961a68b89ca6	
	Internal ID	18737	
Modified	2018-07-09 11:23:45 SGT	**Created**	2018-07-09 11:23:58 SGT
Accessed	2018-07-09 11:23:45 SGT	**Changed**	2018-07-09 11:23:45 SGT
Analysis Comments	Several downloaded clown related contents have been zipped. Compressed files are a total of 12 files such as 1492447345937.jpg, A Little Night Music - Send In The Clowns.pdf, Clowns dancing.mp4, Couto, Mia.pdf, index.jpg, k7827739.jpg, k14032380.jpg, k14032380.jpg, kikkii_clown_party_pose.jpg, Ronald_mcdonald-e1476200032847-660x330.jpg, scary-halloween-costumes-ideas-Clown-blood-Halloween-party-costumes-e1410943909179.jpg and scaryclown.jpg.		

Evidence 4			
	**Name**	k14032380.jpg	
	Source of Path	/img_202.dd/Users/computer/Desktop/k14032380.jpg	
	MIME Type	Image/jpeg	
	Size	31837 bytes	
	MD5	913cb94539abfe8de858ce16c0a40e99	
	SHA-256	0cf32624479f6084c6fa52315917707645e1228bf3b709fb05adb560ab417bff	
	Internal ID	18739	
Modified	2018-07-02 09:21:52 SGT	**Created**	2018-07-02 09:21:52 SGT
Accessed	2018-07-02 09:21:52 SGT	**Changed**	2018-07-02 09:21:53 SGT
Analysis Comments	Illustration of a head-only clown in purple hat who has orange hair was downloaded via Firefox to the Desktop folder. It downloaded from https://fscomps.fotosearch.com/compc/CSP/CSP992/clown-face-clipart__k14032380.jpg		

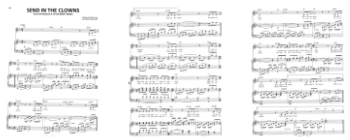
Evidence 5			
	**Name**	k7827739.jpg	
	Source of Path	/img_202.dd/Users/computer/Desktop/k7827739.jpg	
	MIME Type	Image/jpeg	
	Size	41284 bytes	
	MD5	39db918c4014d3a64fabbc17a2fe49a7	
	SHA-256	9b67b8a39b5cc1c8d3d5634869605f5d202cfecc4258aa516b1307cd73f5aa4a	
	Internal ID	18742	
Modified	2018-07-02 09:22:15 SGT	**Created**	2018-07-02 09:22:14 SGT
Accessed	2018-07-02 09:22:14 SGT	**Changed**	2018-07-02 09:22:15 SGT
Analysis Comments	Illustration of a head-only clown in blue hat who has green hair was downloaded via Firefox to the Desktop folder. It downloaded from https://fscomps.fotosearch.com/compc/CSP/CSP782/clown-clip-art__k7827739.jpg		

Evidence 6			
	**Name**	The psychology behind why clowns creep us out.htm	
	Source of Path	/img_202.dd/Users/computer/Documents/html/The psychology behind why clowns creep us out.htm	
	MIME Type	text/html	
	Size	133474 bytes	
	MD5	bb08e6c26b974d09ea0de8fc416277bc	
	SHA-256	0816cb10a3b5c15121f14b20a953bce2b497eff2c02cc0fb7ce4c6aac89518ce	
	Internal ID	18756	
Modified	2018-06-18 10:51:17 SGT	**Created**	2018-06-18 10:51:11 SGT
Accessed	2018-06-18 10:51:15 SGT	**Changed**	2018-06-18 10:51:17 SGT
Analysis Comments	As the web was archived, a clown doll photo with content from clown in the Document folder was saved together. It archived from http://theconversat ion.com/the-psychology-behind-why-clowns-creep-us-out-65936		

Evidence 7			
	**Name**	image-20160926-31853-1jvhtv4.jpg	
	Source of Path	/img_202.dd/Users/computer/Documents/html/The psychology behind why clowns creep us out_files/image-20160926-31853-1jvhtv4.jpg	
	MIME Type	Image/jpeg	
	Size	22894 bytes	
	MD5	98741fa7cb0b1b74bcc9b7e1d63d2fd0	
	SHA-256	6bdd5e1c651931ea76d6faa2da382c0fe204b741ba3130fcf0b300bbc3d6b16c	
	Internal ID	18773	
Modified	2018-06-18 10:51:12 SGT	**Created**	2018-06-18 10:51:12 SGT
Accessed	2018-06-18 10:51:12 SGT	**Changed**	2018-06-18 10:51:12 SGT

Analysis Comments	As the web was archived, a clown that looked like an artwork in the Document folder was saved together. It downloaded from http://theconversation.com/the-psychology-behind-why-clowns-creep-us-out-65936

Evidence 8

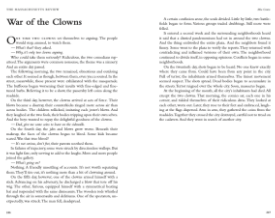


Name	A Little Night Music - Send In The Clowns.pdf		
Source of Path	/img_202.dd/Users/computer/Downloads/A Little Night Music - Send In The Clowns.pdf		
MIME Type	application/pdf		
Size	3146439 bytes		
MD5	4f640bc32c0ac35b585a814ee5235df4		
SHA-256	a28df73b0fc9d7a814c44e1e9418ab1c2fa6982e15fcdaf6c26cd42f8054aa7a		
Internal ID	18846		
Modified	2018-06-19 07:44:31 SGT	**Created**	2018-06-19 07:44:24 SGT
Accessed	2018-06-19 07:44:24 SGT	**Changed**	2018-06-19 07:44:31 SGT
Analysis Comments	The sheet music which has 3 pages related to Clown was downloaded via Firefox to the Downloads folder. It downloaded from https://www.docdroid.net/file/download/bbvy/ a-little-night-music-send-in-the-clowns.pdf		

Evidence 9

Name	Clowns dancing.mp4		
Source of Path	/img_202.dd/Users/computer/Downloads/Clowns dancing.mp4		
MIME Type	video/mp4		
Size	3324223 bytes		
MD5	071f555cf58073ed4ebfb92915a8491a		
SHA-256	ee52d91c16629c1495b5a4d7d3770b92b6523b64555346082d353727f657ed73		
Internal ID	18849		
Modified	2018-06-18 10:45:47 SGT	**Created**	2018-06-18 10:45:41 SGT
Accessed	2018-06-18 10:45:41 SGT	**Changed**	2018-06-18 10:48:12 SGT
Analysis Comments	A video of two clowns dancing to a song was converted from the web to mp4 and downloaded via Firefox to the Downloads folder.		

Evidence 10


War of the Clowns

Name	Couto, Mia.pdf		
Source of Path	/img_202.dd/Users/computer/Downloads/Couto, Mia.pdf		
MIME Type	application/pdf		
Size	118913 bytes		
MD5	96ac7e4f3c457773557837a2bf36368c		
SHA-256	47b65063f56caefef0edb68627a65a8fca76fb202bf90dc6882dd4cce8c75ace		
Internal ID	18852		
Modified	2018-06-19 07:46:34 SGT	**Created**	2018-06-19 07:46:29 SGT
Accessed	2018-06-19 07:46:29 SGT	**Changed**	2018-06-19 07:46:34 SGT
Analysis Comments	The pdf article called War of the Clowns was downloaded via Firefox to the Downloads folder. It downloaded from https://www.massreview.org/sites/default/files/Couto,%20Mia.pdf		

Evidence 11

Name	1492447345937.jpg
Source of Path	/img_202.dd/Users/computer/Pictures/1492447345937.jpg
MIME Type	Image/jpeg
Size	17134 bytes
MD5	3e58af33ebb789d5d81cb4ac613a76c9
SHA-256	1a2a3db8ac91540e39fe33c90a22672cb6e8028270d30dc686be65484d73f966

	Internal ID	18924	
Modified	2018-06-18 08:22:15 SGT	**Created**	2018-06-18 08:22:15 SGT
Accessed	2018-06-18 08:22:15 SGT	**Changed**	2018-06-18 08:22:15 SGT
Analysis Comments	A picture of Donald Trump dressed as a clown in a red shirt and hat was downloaded via Firefox to the Pictures folder. It downloaded from https://static1.squarespace.com/static/530becede4b093256168fba5/t/58f4f06d15d5db5e25316c1e/1492447345937/		

Evidence 12			
	**Name**	kikkii_clown_party_pose.jpg	
	Source of Path	/img_202.dd/Users/computer/Pictures/kikkii_clown_party_pose.jpg	
	MIME Type	Image/jpeg	
	Size	50304 bytes	
	MD5	76e4975e5efc2a1268584fef7ade5f59	
	SHA-256	55e8664e74345336a32b78e620c02426456424fae7a55843eda4a038ea6697df	
	Internal ID	18932	
Modified	2018-06-19 07:50:06 SGT	**Created**	2018-06-19 07:50:05 SGT
Accessed	2018-06-19 07:50:06 SGT	**Changed**	2018-06-19 07:50:06 SGT
Analysis Comments	Picture of an upper body clown in rainbow wig and clothes was downloaded via Firefox to the Pictures folder. It downloaded from http://www.trickortreatmagic.com.au/img/kikkii_clown_party_pose.jpg		

Evidence 13			
	**Name**	Ronald_mcdonald-e1476200032847-660x330.jpg	
	Source of Path	/img_202.dd/Users/computer/Pictures/Ronald_mcdonald-e1476200032847-660x330.jpg	
	MIME Type	Image/jpeg	
	Size	26494bytes	
	MD5	a3f7eb7ba08cb84137a85bf4683c6bca	
	SHA-256	e9625404f351b7c0b5c496502f86def285b5a1a4e82c0cf38404d654e58d2a62	
	Internal ID	18935	
Modified	2018-06-19 07:50:42 SGT	**Created**	2018-06-19 07:50:41 SGT
Accessed	2018-06-19 07:50:41 SGT	**Changed**	2018-06-19 07:50:42 SGT
Analysis Comments	A picture of a McDonald's clown running was downloaded via Firefox to the Pictures folder.		

Evidence 13			
	**Name**	s-l640.jpg	
	Source of Path	/img_202.dd/Users/computer/Pictures/s-l640.jpg	
	MIME Type	Image/jpeg	
	Size	57620 bytes	
	MD5	dd42fe966af825567338e4f873cc2f6a	
	SHA-256	c3c995ba9d01a4a4374f3afe77e3171150f0111cf3d431a5993cb94073c134b2	
	Internal ID	18938	
Modified	2018-06-19 07:50:17 SGT	**Created**	2018-06-19 07:50:17 SGT
Accessed	2018-06-19 07:50:17 SGT	**Changed**	2018-06-19 07:50:17 SGT
Analysis Comments	Picture of a head-only clown in rainbow wig and clothes was downloaded via Firefox to the Pictures folder. It downloaded from https://ssli.ebayimg.com/images/g/2vUAAOSwxp9W8gwu/s-l640.jpg		

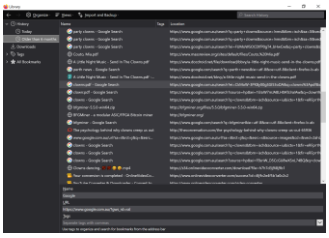
Evidence 15		
	**Name**	scary-halloween-costumes-ideas-Clown-blood-Halloween-party-costumes-e1410943909179.jpg
	Source of Path	/img_202.dd/Users/computer/Pictures/scary-halloween-costumes-ideas-Clown-blood-Halloween-party-costumes-e1410943909179.jpg
	MIME Type	Image/jpeg

		Size	59178 bytes	
		MD5	51632444d9845cc6686adcf24e536f77	
		SHA-256	c6e12b7edde30a9a3bac012aef57a1ca7babee2c85264963a3397d2869835694	
		Internal ID	18945	
Modified	2018-06-18 08:21:55 SGT		**Created**	2018-06-18 08:21:54 SGT
Accessed	2018-06-18 08:21:54 SGT		**Changed**	2018-06-18 08:21:55 SGT
Analysis Comments	A picture of Scary clown with bloody red hair in a white shirt who came out with both hands was downloaded via Firefox to the Pictures folder. It downloaded from https://deavita.net/wp-content/uploads/2014/09/scary-halloween-costumes-ideas-Clown -blood-Halloween-party-costumes-e1410943909179.jpg			

Evidence 16

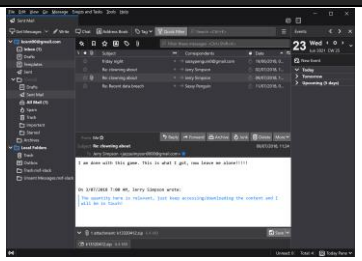
Name	scaryclown.jpg		
Source of Path	/img_202.dd/Users/computer/Pictures/scaryclown.jpg		
MIME Type	Image/jpeg		
Size	58423 bytes		
MD5	ed873fc7b1f226bda891c1780341cdb2		
SHA-256	a55d63a0caee2637388da648d7ac77679a5b378a7984c264b3e7ec4e3703f9bc		
Internal ID	18948		
Modified	2018-06-18 08:20:06 SGT	**Created**	2018-06-18 08:20:04 SGT
Accessed	2018-06-18 08:20:05 SGT	**Changed**	2018-06-18 08:20:06 SGT
Analysis Comments	A picture of scary clown with sharp teeth and black area around eyes was downloaded via Firefox to the Pictures folder. It downloaded from http://www.scarymommy.com/wp-content/uploads/2016/10/scaryclown.jpg? w=697		

Evidence 17



Name	Firefox		
Source of Path	/img_202.dd/Users/computer/AppData/Roaming/Mozilla/Firefox		
MIME Type	- (Folder)		
Size	35321179 bytes		
MD5	-		
SHA-256	-		
Internal ID	17619		
Modified	2018-05-02 10:32:23 SGT	**Created**	2018-05-02 10:32:23 SGT
Accessed	2018-05-02 10:32:23 SGT	**Changed**	2018-05-02 10:32:23 SGT
Analysis Comments	As a web search history csv file, clown content was accessed through Firefox and the files were downloaded. It has 158 Files and 47 Folders in the Firefox folder.		

Evidence 18



Name			
Source of Path	/img_202.dd/Users/computer/AppData/Roaming/Thunderbird/Profiles/1cug4fub.default/ImapMail/imap.gmail.com/[Gmail].sbd/Sent Mail		
MIME Type	File System		
Size	9245667 bytes		
MD5	70b6b0b9caffa5489bbb980c36be9d23		
SHA-256	f12d808031870c89feb7bb32ad8d90cd0c4fd0477f541197248d589f28c5d6dd		
Internal ID	18605		
Modified	2018-07-11 08:11:52 SGT	**Created**	2018-06-19 07:49:36 SGT
Accessed	2018-06-19 07:49:36 SGT	**Changed**	2018-07-11 08:11:52 SGT
Analysis Comments	Distributed the k13320412.zip file with the clown contents compressed via email at . 2018-07-09 11:24:08 to jazzasimpson0000@gmail.com.		

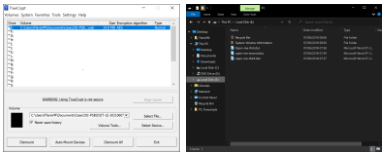
Issue #2 - Identification

These contents of the ownership and use of the evidence found in the 202.dd is organised.

Issue #2.1 - Identification on Documents and Files

Direct/indirect evidence that the user of this computer is Clark, and that he has the computer and clown content.

Identification File 1			
	**Name**	Journal.doc	
	Source of Path	/img_202.dd/Users/computer/Documents/Journal.doc	
	MIME Type	application/msword	
	Size	50176 bytes	
	MD5	c53b7d63c8a0787b897584819a4f8d0f	
	SHA-256	7285b7e39f0f8f5ff21ea9e102673067355df894cf21687726d043242f54523c	
	Internal ID	18806	
Modified	2018-07-11 08:16:20 SGT	**Created**	2018-05-02 12:23:52 SGT
Accessed	2018-05-02 12:23:52 SGT	**Changed**	2018-07-11 08:16:20 SGT
Analysis Comments	Open the file, Personal Journal is written as the title, and a diary is written on it. This doc file is from January 10, 2016, mentions Clown on June 25, 2018. It is assumed to be a diary written by a computer user.		

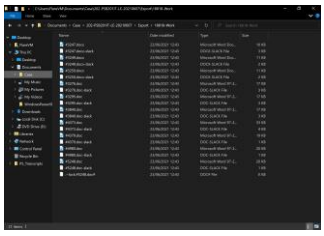
Identification File 2			
	**Name**	usb	
	Source of Path	/img_202.dd/Users/computer/Desktop/usb	
	MIME Type	application/octet-stream	
	Size	26214400 bytes	
	MD5	a77ee19d8c6264e88098bafc0b36805e	
	SHA-256	becdc7f3004e29287b2891e3baaaa1e7ceac65eda27efe5bcdeeb1ef205d1751	
	Internal ID	18745	
Modified	2018-06-07 08:55:36 SGT	**Created**	2018-06-07 08:55:35 SGT
Accessed	2018-06-07 08:55:35 SGT	**Changed**	2018-06-07 08:55:36 SGT
Case Name/No.	202-PSB201IT-LE-20210607-exported-usb		
Analysis Comments	This file has been analysed by Autopsy as Encryption Suspected and appears to be an encrypted file. It was created on June 7th, and at 08:51:39 that day, a USB of a JumpDrive V10 model made by Lexar Media, Inc. was connected to a computer. Also, there is TrueCrypt as an installed tool related to encryption, and when I see that it was installed at 00:53:48 on the same day, there is a high probability that it was encrypted through TrueCrypt. As a result of analysing the file, there were three files: Open-me-first.doc, open-me-second.doc and open-me-third.doc.		

Identification File 2-1			
	**Name**	open-me-first.doc	
	Source of Path	/img_202-PSB201IT-LE-20210607-exported-usb.001/Open-me-first.doc	
	MIME Type	application/msword	
	Size	431616 bytes	
	MD5	11fc9766f78b9857a2c0977f808a4a52	
	SHA-256	63acc7a8de327e83ece3578de835ada35de490fee580508e1cbda0111d95cdf3	
	Internal ID	11	
Modified	2018-06-07 07:38:46 SGT	**Created**	2018-06-07 08:56:26 SGT

Accessed	2018-06-07 00:00:00 SGT	**Changed**	0000-00-00 00:00:00
Analysis Comments	A single image of a graffiti attempt written on the red wall with the words SUPERMAN IS CLARK KEN- is attached along with a message saying that he attempted a graffiti attempt.		

Identification File 2-2			
	**Name**	open-me-second.doc	
	Source of Path	/img_202-PSB201IT-LE-20210607-exported-usb.001/open-me-second.doc	
	MIME Type	application/msword	
	Size	270336 bytes	
	MD5	2a05c5354973779060b986120263918d	
	SHA-256	fbfc5be5083b4012b5e9327e746a93fcffa93209343434aa26807f51630d2ec7	
	Internal ID	13	
Modified	2018-06-07 07:39:28 SGT	**Created**	2018-06-07 08:56:26 SGT
Accessed	2018-06-07 00:00:00 SGT	**Changed**	0000-00-00 00:00:00
Analysis Comments	An image is attached along with the text "A potential news story?", and SUPERMANS'S SECRET IDENTITY REVEALED! Contains a page from a Daily Planet article from June 17, 2015 called Man of Steel Dwelt Among Us as Daily Planet Reporter Clark Kent.		

Identification File 2-3			
	**Name**	open-me-third.doc	
	Source of Path	/img_202-PSB201IT-LE-20210607-exported-usb.001/open-me-third.doc	
	MIME Type	application/msword	
	Size	197120 bytes	
	MD5	6ce69cfd6b83dab704c354e7ec139c5f	
	SHA-256	8f48695e068efec37450e9026c9998f429b896919c486ef252ca70c81db70331	
	Internal ID	14	
Modified	2018-06-07 07:37:44 SGT	**Created**	2018-06-07 08:56:26 SGT
Accessed	2018-06-18 00:00:00 SGT	**Changed**	0000-00-00 00:00:00
Analysis Comments	In this last document in the usb file, this file, along with a picture of SHALL WE PLAY GAME?, says that he is very interested in Clown and wants to find it instead. Otherwise, Clark will reveal this to Superman and it is a blackmail that puts his parents at risk.		

Identification File 3			
	**Name**	#3247.doc to #5248.doc	
	Source of Path	/img_202.dd/Users/computer/Documents/Work/	
	MIME Type	application/msword	
	Size	-	
	MD5	-	
	SHA-256	-	
	Internal ID	-	
Analysis Comments	There are documents that wrote as a Daily Planet reporter in folders related to work. It says “by Clark Kent” at the top of all text.		

Issue #2.2 - Identification on Email Communication

Here is an Identification from an email stored on 202.dd. Users use Gmail and receive and send emails through the Thunderbird client program. I checked the contents of 11 emails, and 5 of them can be identified.

Identification Email 1			
E-Mail From	no-reply@accounts.google.com	**E-Mail To**	kcent00@gmail.com

Subject	Your password changed	**Date/Time**	2018-05-02 07:51:54 SGT
Message (Plaintext)	Your password changed Hi Klark, The password for your Google Account kcent00@gmail.com was recently changed. Don't recognize this activity? Click here for more information on how to recover your account. The Google Accounts team This email can't receive replies. For more information, visit the Google Accounts Help Center. You received this mandatory email service announcement to update you about important changes to your Google product or account. © 2018 Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA		
Attachments	-		
Size	79863 bytes	**MD5**	4ede63d85050332ba45a74c048fd2843
Internal ID	18583	**SHA-256**	cecf5e10ce695d8cb97debcd07d90b06717a408c3780e990e6b76959f6bf844a
Analysis Comments	The mail owner has been contacted by Google because password has been changed. Since the recipient's Gmail ID is kcent00 and Hi Klark is written in the body, it is assumed that Clark is the owner of this email and the person who logged in by entering the password.		

Identification Email 2			
E-Mail From	no-reply@accounts.google.com	**E-Mail To**	kcent00@gmail.com
Subject	Security alert	**Date/Time**	2018-05-03 08:04:54 SGT
Message (Plaintext)	Klark Cent New device signed in to kcent00@gmail.com Your Google Account was just signed in to from a new Windows device. You're getting this email to make sure it was you. CHECK ACTIVITY You received this email to let you know about important changes to your Google Account and services. © 2018 Google Inc.,1600 Amphitheatre Parkway, Mountain View, CA 94043, USA		
Attachments	-		
Size	79863 bytes	**MD5**	4ede63d85050332ba45a74c048fd2843
Internal ID	18583	**SHA-256**	cecf5e10ce695d8cb97debcd07d90b06717a408c3780e990e6b76959f6bf844a
Analysis Comments	The mail owner logged into new device and have been contacted by Google. As the body of this email says Klark Cent, it is likely that Clark is the owner of this email.		

Identification Email 3			
E-Mail From	Sassypenguin0@gmail.com	**E-Mail To**	kcent00@gmail.com
Subject	Recent data breach	**Date/Time**	2018-05-03 08:12:35 SGT
Message (Plaintext)	Clark, As a result of our recent minor security breach I am asking everyone to protect their data, Jimmy here suggested using a tool TrueCrypt. You're a clever boy, I'm sure you can figure out how to use it. Regards, Chief		
Attachments	-		
Size	79863 bytes	**MD5**	4ede63d85050332ba45a74c048fd2843
Internal ID	18583	**SHA-256**	cecf5e10ce695d8cb97debcd07d90b06717a408c3780e990e6b76959f6bf844a
Analysis Comments	The mail owner received a work-related email from my boss. The inscription of Clark at the beginning of the text suggests that Clark is the owner of this email.		

Identification Email 4			
E-Mail From	kcent00@gmail.com	**E-Mail To**	jazzasimpson0000@gmail.com
Subject	Re: clowning about	**Date/Time**	2018-07-09 11:24:08 SGT
Message	I am done with this game. This is what I got, now leave me alone!!!!!		

(Plaintext)	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!		
Attachments	/img_202.dd/Users/computer/AppData/Roaming/Thunderbird/Profiles/1cug4fub.default/ImapMail/imap.gmail.com/[Gmail].sbd/Sent Mail/k13320412.zip		
Size	9245667 bytes	**MD5**	70b6b0b9caffa5489bbb980c36be9d23
Internal ID	18605	**SHA-256**	f12d808031870c89feb7bb32ad8d90cd0c4fd0477f541197248d589f28c5d6dd
Analysis Comments	The mail owner sent an email to jazzasimpson0000@gmail.com with k13320412.zip attached to the email. Clark confirmed that he owns Clown content that is illegal and that he distributes it himself.		

Identification Email 5			
E-Mail From	jazzasimpson0000@gmail.com	**E-Mail To**	kcent00@gmail.com
Subject	Re: clowning about	**Date/Time**	2018-07-10 09:41:42 SGT
Message (Plaintext)	No, no, you are not done, I want more, more clown content! 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!!!!! 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!		
Attachments	-		
Size	79863 bytes	**MD5**	4ede63d85050332ba45a74c048fd2843
Internal ID	18583	**SHA-256**	cecf5e10ce695d8cb97debcd07d90b06717a408c3780e990e6b76959f6bf844a
Analysis Comments	Jerry Simpson who have received Clown want more material. Clark is sharing material with jazzasimpson0000@gmail.com for some reason.		

Issue #2.3 - Identification on Hidden File

I found in Internet history that the StegHide program was downloaded, and it was confirmed to be downloaded to the download folder. StegHide is a steganography tool that allows to hide text or files in files such as images. This reason I scanned all the files which is steganography files, but could not find any hidden files by steganography.

Issue #3 - Intent

The user of this computer has done something illegal by gaining access to Clown. However, it is different whether the user did the illegal act solely out of his or her own will, or whether it was caused by threats or malware rather than by the user's own will. So overall, I need to look at and analyse deeply the patterns of files and emails and computer users.

Issue #3.1 - Motive

The motive for the misconduct is seen as blackmail. When analysing the encrypted USB through TrueCrypt, three files came out (reference: Identification File 2 to 2-3), and the contents were that if know that Clark is Superman, and if do not want to be identified, collect clown's data and send it to him. A similar pattern can be seen with email.

Issue #3.2 - Another Possibility

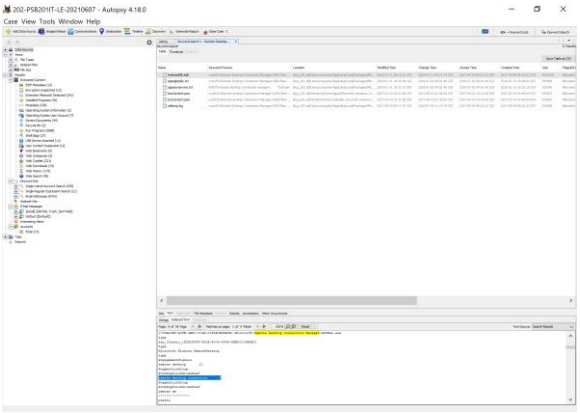
In the content of the last email, Clark sent an email to his boss claiming to have been hacked. Also, he testified stated the possibility of hacking when laptop confiscated. It is a consistent statement, so it is worth checking.

Claim to have been hacked			
E-Mail From	kcent00@gmail.com	**E-Mail To**	sassypenguin0@gmail.com
Subject	Re: Recent data breach	**Date/Time**	2018-07-11 08:11:46 SGT
Message (Plaintext)	Hi Chief, 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! On 3/05/2018 8:12 AM, Sassy Penguin wrote: > Clark, > > As a result of our recent minor security breach I am asking everyone > to protect their data, Jimmy here suggested using a tool TrueCrypt. > You're a clever boy, I'm sure you can figure out how to use it. > > Regards, > > Chief		
Attachments	-		
Size	9245667 bytes	**MD5**	70b6b0b9caffa5489bbb980c36be9d23
Internal ID	18605	**SHA-256**	f12d808031870c89feb7bb32ad8d90cd0c4fd0477f541197248d589f28c5d6dd

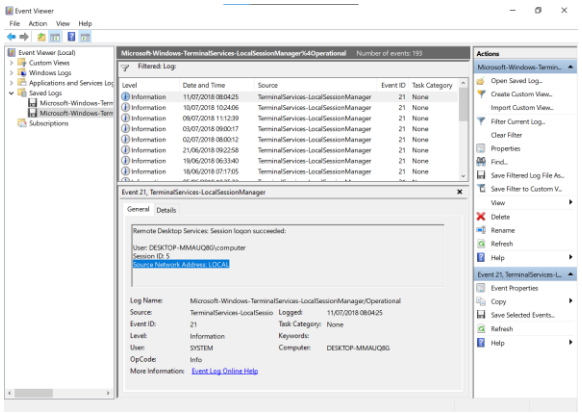
Issue #3.2.1 - Possibility of Remote Control

First, someone other than the computer owner, Clark, may have remotely controlled and used this computer. This reason, I looked at remote applications, remote client programs, and Windows' own remote permission.

When I did the Keyword Search to the check the IndexedDB.edb and edbtmp.log of the Remote Desktop Connection Manager in Autopsy, the program installed or downloaded for remote access, the remote desktop connection appears as 0 with the same result. There is no trace of access through Remote Desktop Connection Manager.



Left. Autopsy - Log check Remote Desktop Connection Manager



Right. VirusTotal - Search bfgminer-5.5.0-win64.zip

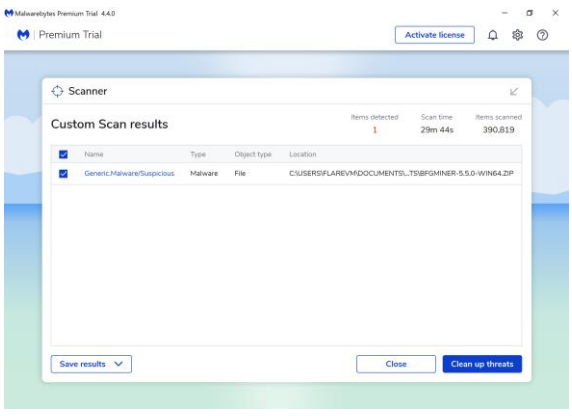
Additionally, I checked the event log by extracting Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx. I found several logs with Event ID 21 (Remote Desktop Services: Session logon succeeded), but all the results were “Source Network Address: LOCAL”. Therefore, there was no trace of remote access.

Issue #3.2.2 - Possibility of Malware Infection

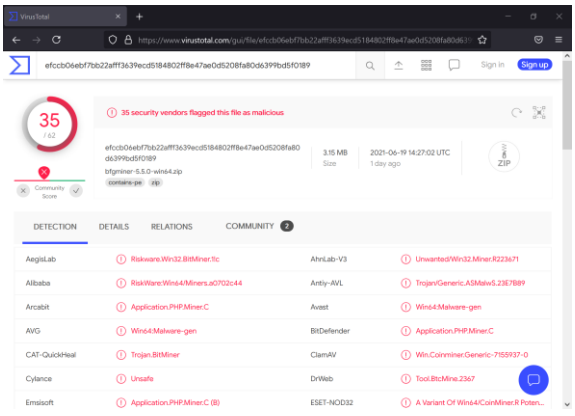
Second, it may be infected with malware or opened backdoor. Clark’s identity as Superman may have been leaked from this computer via malware, or the malware could have opened a backdoor to allow remote manipulation or misconduct. This reason, I extracted all the files in the topmost folder of 202.dd and scanned them for malware.

Malware Detected	
Type	File
Detail	Generic.Malware/Suspicious, C:\USERS\FLAREVM\DOCUMENTS\CASE\TEMP\202FILES\5062-USERS \COMPUTER\DOCUMENTS\BFGMINER-5.5.0-WIN64.ZIP, No Action By User, 0, 392686, 1.0.41967, , shuriken, , 81BA60673B661515BDA4EBFE9E668AFE, EFCCB06EBF7BB22AFFF3639ECD5184802FF8E4 7AE0D5208FA80D6399BD5F0189

I used Malwarebytes to be scanned for malware. According to search and analysis, it is a common bitcoin mining program, and 35 out of 62 commercial antivirus and security programs have classified it as a risky file. However, it is not considered to be a backdoor or malicious malware.



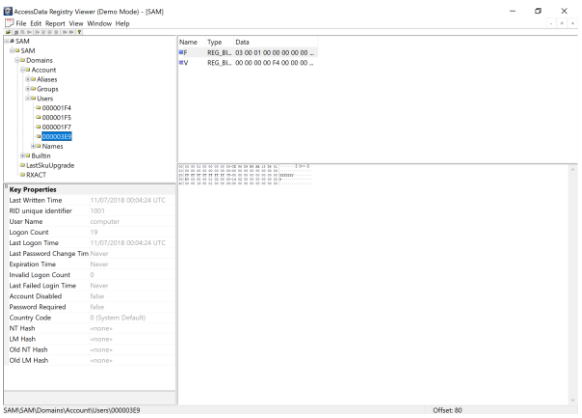
Left. Malwarebytes - San 202.dd’s files



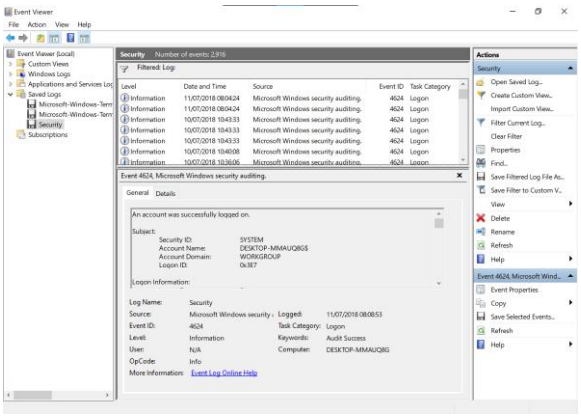
Right. VirusTotal - Search bfgminer-5.5.0-win64.zip

Issue #3.2.3 - Possibility of Physically

Finally, a social engineering hack or maybe someone else used it when Clark left this laptop unattended. When the SAM file was extracted from Autopsy and analysed with AccessData Registry Viewer, there were a total of 19 logins and Password Required was set to false, indicating that there was no password. I looked at Security.evtx for Event ID 4624 (Logon) for more information but did not find any singularities. However, since there is no password, Clark may have been using the computer while he was away. It is unlikely, but just to be sure, look for company recorded videos like CCTV or other witnesses when the time logon.



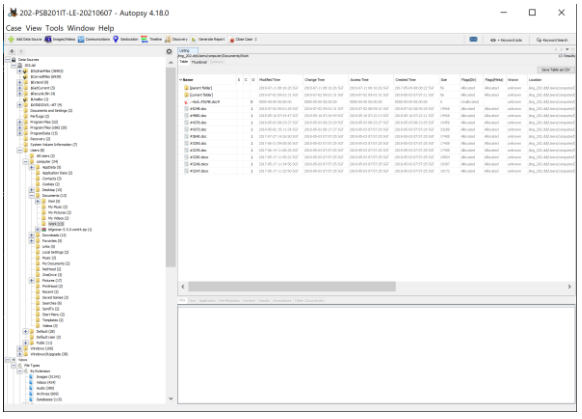
Left. AccessData Registry Viewer - SAM



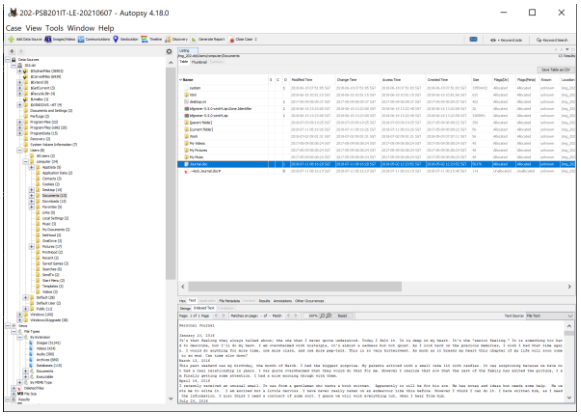
Right. Event Viewer - Security.evtx

Issue #3.3 - Life Routine of Computer User

As there may have been physical access, I should check the life routine of the computer user. Check the Work folder in the Documents containing the contents of his work, there are a total of 10 files with docx and doc extension that appear to be the documents that the article was written in. The Created Time is 7:00 am or 8:00 am. It seems Clark work start time about 7:00 in the morning.



Left. Autopsy - Check files in Documents/Work folder



Right. Autopsy - Check Journal File in Documents folder

Other than that, I found a file of Jernal.doc in the Documents folder, and when I open the file, it says Personal Journal as the title. A total of 4 items related to the incident were found in the diary. First, I confirmed that the laptop is currently analysing was provided by the company Daily Planet on 2nd May. And on the 5th June he received a strange phone call related

to a graffiti message along with a phone call saying he had left the USB file on Clark's desk. Clark seems to have discovered a white USB Stick on 7th June, and it is presumed that the white USB Stick was encrypted with TrueCrypt. Finally, on 25th June, there is a diary entry about Clown. He mentions Clown in his diary, and there may also be some connection to Clown found on this computer.

Personal Journal Contents related Investigation 1	
Date	May 2, 2018
Contents	My work laptop died today. This is quite unfortunate, so many years of work lost. Fortunately the Daily Planet was able to provide me with a new laptop very quickly, allowing me to recommence work quickly.

Personal Journal Contents related Investigation 2	
Date	May 5, 2018
Contents	Received a strange phone call today, from someone claiming that I will get a USB stick dropped on my desk and something about a graffiti message in an alleyway downtown. I've searched the city and I can't find anything that this could relate to. Hopefully nothing dangerous is going to happen!

Personal Journal Contents related Investigation 3	
Date	May 7, 2018
Contents	So I arrived at work today, only to find a white USB stick sitting on my keyboard. I don't feel brave enough to actually open it and view its content. So I've decided to look into this and find out just what the hell is actually going on.

Personal Journal Contents related Investigation 4	
Date	May 25, 2018
Contents	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.

Issue #3.4 - Flow of Events

These are the contents that have been analysed in depth based on the research and analysis contents. This is an investigation into how Clark searched for and received Clown after receiving the blackmail.

Issue #3.4.1 - Searching History

Below is Clark's internet log. Clark, who allegedly received threats through the white USB stick, subsequently searched for clowns and downloaded the content.

Description	Date Accessed	Domain	URL	Download	Browser
Search clown contents: Images	2018-06-18 08:19:33 SGT	google.com.au	https://www.google.com.au/search?q=clowns&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiuvoDm99vbAhXFxbwKHd4fCTAQ_AUICigB&biw=1366&bih=654		Firefox
Search clown contents: Images	2018-06-18 08:19:40 SGT	google.com.au	https://www.google.com.au/search?q=clowns&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiuvoDm99vbAhXFxbwKHd4fCTAQ_AUICigB&biw=1366&bih=654		Firefox
Search clown contents: Images	2018-06-18 08:19:47 SGT	google.com.au	https://www.google.com.au/search?q=clowns&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiuvoDm99vbAhXFxbwKHd4fCTAQ_AUICigB&biw=1366&bih=654#imgrc=NybuyqBjXaUlKM:		Firefox
Download clown contents: One image	2018-06-18 08:20:05 SGT	scarymommy.com	http://www.scarymommy.com/wp-content/uploads/2016/10/scaryclown.jpg?w=697	scaryclown.jpg	Firefox
Search clown contents: Images	2018-06-18 08:21:44 SGT	google.com.au	https://www.google.com.au/search?q=clowns&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiuvoDm99vbAhXFxbwKHd4fCTAQ_AUICigB&biw=1366&bih=654#imgdii=mgrj3X4r4cbnOM:&imgrc=NybuyqBjXaUlKM:		Firefox

Download clown contents: One image	2018-06-18 08:21:54 SGT	deavita.net	https://deavita.net/wp-content/uploads/2014/09/scary-halloween-costumes-ideas-Clown-blood-Halloween-party-costumes-e1410943909179.jpg	scary-halloween-costumes-ideas-Clown-blood-Halloween-party-costumes-e1410943909179.jpg	Firefox
Search clown contents: Images	2018-06-18 08:22:07 SGT	google.com.au	https://www.google.com.au/search?q=clowns&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiuvoDm99vbAhXFxbwKHd4fCTAQ_AUICigB&biw=1366&bih=654#imgrc=DlSRrLg9KhoM3M:		Firefox
Download clown contents: One image	2018-06-18 08:22:15 SGT	squarespace-cdn.com	https://static1.squarespace.com/static/530becede4b093256168fba5/t/58f4f06d15d5db5e25316c1e/1492447345937/	1492447345937.jpg	Firefox
Download clown contents: One video	2018-06-18 10:45:41 SGT	onlinevideoconverter.com	https://s34.onlinevideoconverter.com/download?file=h7h7d3j9i8j9b1	Clowns dancing.mp4	Firefox
Search clown contents: Images	2018-06-18 10:49:48 SGT	google.com.au	https://www.google.com.au/search?source=hp&ei=FBsnW_D5CcGU8wXSnL74BQ&q=clowns&oq=clowns&gs_l=psy-ab.3..0l10.540512.546587.0.547447.6.5.0.1.1.0.488.1315.2-3j0j1.4.0....0...1c.1.64.psy-ab..1.5.1339...0i131k1.0.BRYG_MxOlG8		Firefox
Search clown contents: Images	2018-06-18 10:49:59 SGT	google.com.au	https://www.google.com.au/search?q=clowns&tbm=isch&source=iu&ictx=1&fir=eRFpr1NqiLvKbM%253A%252CbE7-MYPR4TzxkM%252C_&usg=__M5KIb9MjgDJSW3TXd2FmSmMsAIo%3D&sa=X&ved=0ahUKEwj_nvywmdzbAhWJxrwKHYiMDnUQ9QEILTAC#imgrc=eRFpr1NqiLvKbM:		Firefox
Search clown contents: Images	2018-06-18 10:50:14 SGT	google.com.au	https://www.google.com.au/search?q=clowns&tbm=isch&source=iu&ictx=1&fir=eRFpr1NqiLvKbM%253A%252CbE7-MYPR4TzxkM%252C_&usg=__M5KIb9MjgDJSW3TXd2FmSmMsAIo%3D&sa=X&ved=0ahUKEwj_nvywmdzbAhWJxrwKHYiMDnUQ9QEILTAC#imgrc=ARyyzxZnesrefM:		Firefox
Search clown contents: Books	2018-06-18 10:50:25 SGT	google.com.au	https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&ved=2ahUKEwiAiNK9mdzbAhXHx7wKHfVPA6cQjxx6BAgBEAI&url=http%3A%2F%2Ftheconversation.com%2Fthe-psychology-behind-why-clowns-creep-us-out-65936&psig=AOvVaw2wW6d1yGeZFS1hcIFksN9f&ust=1529376459486490		Firefox
Search clown contents: Books	2018-06-18 10:50:27 SGT	theconversation.com	http://theconversation.com/the-psychology-behind-why-clowns-creep-us-out-65936		Firefox
Download clown contents: Web archive	2018-06-18 10:51:11 SGT	theconversation.com	http://theconversation.com/the-psychology-behind-why-clowns-creep-us-out-65936	The psychology behind why clowns creep us out.htm	Firefox
Search clown contents: Images	2018-06-18 13:38:44 SGT	google.com.au	https://www.google.com.au/search?q=clowns&tbm=isch&source=iu&ictx=1&fir=eRFpr1NqiLvKbM%253A%252CbE7-MYPR4TzxkM%252C_&usg=__M5KIb9MjgDJSW3TXd2FmSmMsAIo%3D&sa=X&ved=0ahUKEwj_nvywmdzbAhWJxrwKHYiMDnUQ9QEILTAC#imgrc=87u-hT1adnEHFM:		Firefox
Search clown contents: PDF	2018-06-19 07:43:19 SGT	google.com.au	https://www.google.com.au/search?source=hp&ei=1EIoW7mJA8LH0ATclraIAw&q=clown%3Apdf&oq=clown%3Apdf&gs_l=psy-ab.3...38853.42318.0.42834.9.9.0.0.0.0.401.916.2-2j0j1.3.0....0...1c.1.64.psy-ab..6.2.673...0j0i131k1.0.drFi2diLkvk		Firefox
Search clown contents: PDF	2018-06-19 07:43:30 SGT	google.com.au	https://www.google.com.au/search?ei=CkMoW-3PK8yX0gSGl53oDA&q=clowns%3Apdf&oq=clowns%3Apdf&gs_l=psy-ab.3...5304.5304.0.6754.1.1.0.0.0.0.0.0..0.0....0...1c.1.64.psy-ab..1.0.0....0.Y3lF1BjeHs4		Firefox
Search clown contents: PDF	2018-06-19 07:43:52 SGT	google.com.au	https://www.google.com.au/search?ei=CkMoW-3PK8yX0gSGl53oDA&q=clowns%3Apdf&oq=clowns%3Apdf&gs_l=psy-ab.3...5304.5304.0.6754.1.1.0.0.0.0.0.0..0.0....0...1c.1.64.psy-ab..1.0.0....0.Y3lF1BjeHs4		Firefox
Search clown contents: PDF	2018-06-19 07:44:24 SGT	docdroid.net	https://www.docdroid.net/file/download/bbvy/a-little-night-music-send-in-the-clowns.pdf		Firefox
Search clown contents: PDF	2018-06-19 07:44:29 SGT	docdroid.net	https://www.docdroid.net/file/download/bbvy/a-little-night-music-send-in-the-clowns.pdf	A Little Night Music - Send In The Clowns.pdf	Firefox
Search clown contents: PDF	2018-06-19 07:45:24 GMT	massreview.org	https://www.massreview.org/sites/default/files/Couto,%20Mia.pdf		Firefox
Search clown contents: PDF	2018-06-19 07:46:29 SGT	massreview.org	https://www.massreview.org/sites/default/files/Couto,%20Mia.pdf		Firefox
Search clown contents: PDF	2018-06-19 07:46:33 SGT	massreview.org	https://www.massreview.org/sites/default/files/Couto,%20Mia.pdf	Couto, Mia.pdf	Firefox
Search clown contents: About party	2018-06-19 07:47:29 SGT	google.com.au	https://www.google.com.au/search?ei=FUMoW5OCDfP0gT4_bHwCw&q=party+clowns&oq=party+clowns&gs_l=psy-ab.3..0i67k1j0l9.23387.29229.0.29883.21.17.0.0.0.0.426.2400.2-6j1j1.8.0....0...1c.1.64.psy-ab..13.7.2139...0i131k1.0.82-Y-oNLJOM		Firefox
Search clown contents: Images about party	2018-06-19 07:49:38 SGT	google.com.au	https://www.google.com.au/search?q=party+clowns&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiFs4u_st7bAhWGFJQKHVLEBJwQ_AUICigB&biw=1366&bih=631		Firefox
Search clown contents: Images about party	2018-06-19 07:49:45 SGT	google.com.au	https://www.google.com.au/search?q=party+clowns&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiFs4u_st7bAhWGFJQKHVLEBJwQ_AUICigB&biw=1366&bih=631#imgrc=NIM0dE5m6FWlFM:		Firefox
Download clown contents: One image	2018-06-19 07:50:06 SGT	trickortreatmagic.com.au	http://www.trickortreatmagic.com.au/img/kikkii_clown_party_pose.jpg	kikkii_clown_party_pose.jpg	Firefox
Search clown contents: Images about party	2018-06-19 07:50:09 SGT	google.com.au	https://www.google.com.au/search?q=party+clowns&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiFs4u_st7bAhWGFJQKHVLEBJwQ_AUICigB&biw=1366&bih=631#imgdii=pKQBnbqVycPXbM:&imgrc=NIM0dE5m6FWlFM:		Firefox
Download clown contents: One image	2018-06-19 07:50:17 SGT	ebayimg.com	https://ssli.ebayimg.com/images/g/2vUAAOSwxp9W8gwu/s-l640.jpg	s-l640.jpg	Firefox
Search clown contents: Images about party	2018-06-19 07:50:27 SGT	google.com.au	https://www.google.com.au/search?q=party+clowns&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiFs4u_st7bAhWGFJQKHVLEBJwQ_AUICigB&biw=1366&bih=631#imgrc=wLdR8wRUYun2-M:		Firefox

Download clown contents: One image	2018-06-19 07:50:41 SGT	theredshtick.com	http://theredshtick.com/wp-content/uploads/2016/10/Ronald_mcdonald-e1476200032847-660x330.jpg	Ronald_mcdonald-e1476200032847-660x330.jpg	Firefox
Search clown contents: Images about graphic	2018-07-02 09:11:05 SGT	google.com.au	https://www.google.com.au/search?source=hp&ei=YXk5W7bUPJWmoATexrIDQ&q=clown+graphic+images&oq=clown+graphic+images&gs_l=psy-ab.3..0i22i30k1.421688.427272.0.428795.20.12.0.4.4.0.385.1339.2-1j3.4.0....0...1c.1.64.psy-ab..12.8.1451...0j0i131k1j0i22i10i30k1.0.yGR8iVnBIC8		Firefox
Search clown contents: Images about graphic	2018-07-02 09:11:13 SGT	Google	https://www.google.com.au/search?q=clown+graphic+images&tbm=isch&source=iu&ictx=1&fir=cWnTWtwYVjMpGM%253A%252Cjo5mNgyJoLtFiM%252C_&usg=___wi5k2guiQlVeOTyCqrjyrNcanE%3D&sa=X&ved=0ahUKEwiQ1lyxnf_bAhXMZt4KHQ7tCG0Q9QEIMzAF#imgrc=cWnTWtwYVjMpGM:		Firefox
Search clown contents: Images about graphic	2018-07-02 09:14:32 SGT	google.com.au	https://www.google.com.au/search?q=clown+graphic+images&tbm=isch&source=iu&ictx=1&fir=cWnTWtwYVjMpGM%253A%252Cjo5mNgyJoLtFiM%252C_&usg=___wi5k2guiQlVeOTyCqrjyrNcanE%3D&sa=X&ved=0ahUKEwiQ1lyxnf_bAhXMZt4KHQ7tCG0Q9QEIMzAF#imgdii=YVkOASE-CJtH_M:&imgrc=cWnTWtwYVjMpGM:		Firefox
Search clown contents: Images about graphic	2018-07-02 09:14:36 SGT	google.com.au	https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&ved=2ahUKEwjet_yTnv_bAhWXMt4KHWVXDcgQjRx6BAgBEAU&url=https%3A%2F%2Fwww.fotosearch.com%2FCSP992%2Fk13320412%2F&psig=AOvVaw1Nhlc7aZAD10V7Pe-8sMMQ&ust=1530580121422621		Firefox
Search clown contents: Images about graphic	2018-07-02 09:14:38 SGT	fotosearch.com	https://www.fotosearch.com/CSP992/k13320412/		Firefox
Download clown contents: One image	2018-07-02 09:15:08 SGT	fotosearch.com	https://fscomps.fotosearch.com/compc/CSP/CSP992/a-clown-wearing-a-green-costume-clipart__k13320412.jpg	k13320412.jpg	Firefox
Search clown contents: Images about graphic	2018-07-02 09:21:35 SGT	fotosearch.com	https://www.fotosearch.com/CSP992/k14032380/		Firefox
Download clown contents: One image	2018-07-02 09:21:52 SGT	fotosearch.com	https://fscomps.fotosearch.com/compc/CSP/CSP992/clown-face-clipart__k14032380.jpg	k14032380.jpg	Firefox
Search clown contents: Images about graphic	2018-07-02 09:21:57 SGT	fotosearch.com	https://www.fotosearch.com/CSP782/k7827739/		Firefox
Download clown contents: One image	2018-07-02 09:22:14 SGT	fotosearch.com	https://fscomps.fotosearch.com/compc/CSP/CSP782/clown-clip-art__k7827739.jpg	k7827739.jpg	Firefox

Issue #3.4.2 - Electronic Communication

Jerry Simpson, who is presumed to be the blackmailer, continued to request clown-related content from Clark, and Clark compressed 12 of the 13 clown contents downloaded with Firefox which are images, video, pdf files, and content into a zip file to send it to Jerry Simpson.

Email Communication 1			
E-Mail From	jazzasimpson0000@gmail.com	**E-Mail To**	kcent00@gmail.com
Subject	clowning about	**Date/Time**	2018-06-18 11:11:35 SGT
Message (Plaintext)	stop clowning about and start working like a super man :)		
Attachments	-		
Size	79863 bytes	**MD5**	4ede63d85050332ba45a74c048fd2843
Internal ID	18583	**SHA-256**	cecf5e10ce695d8cb97debcd07d90b06717a408c3780e990e6b76959f6bf844a
Analysis Comments	It is presumed that it is a blackmail company that puts blackmail on a USB It is considered to be a mockery of Superman and to investigate Clown, and since there was no talk of sending Clown contents to the usb file, it seems that the blackmailer was going to contact him by email first.		

Email Communication 2			
E-Mail From	kcent00@gmail.com	**E-Mail To**	jazzasimpson0000@gmail.com
Subject	Re: clowning about	**Date/Time**	2018-07-02 10:20:09 SGT
Message (Plaintext)	How many am I send you and how do I get it to you? On 18/06/2018 11:11 AM, Jerry Simpson wrote: > stop clowning about and start working like a super man :)		
Attachments	-		
Size	9245667 bytes	**MD5**	70b6b0b9caffa5489bbb980c36be9d23
Internal ID	18605	**SHA-256**	f12d808031870c89feb7bb32ad8d90cd0c4fd0477f541197248d589f28c5d6dd

Analysis Comments	After being threatened, Clark appears to be asking the blackmailer how much clown's content he should obtain.

Email Communication 3			
E-Mail From	jazzasimpson0000@gmail.com	**E-Mail To**	kcent00@gmail.com
Subject	Re: clowning about	**Date/Time**	2018-07-03 07:03:50 SGT
Message (Plaintext)	The quantity here is relevant, just keep accessing/downloading the content and I will be in touch!		
Attachments	-		
Size	79863 bytes	**MD5**	4ede63d85050332ba45a74c048fd2843
Internal ID	18583	**SHA-256**	cecf5e10ce695d8cb97debcd07d90b06717a408c3780e990e6b76959f6bf844a
Analysis Comments	The blackmailer instructs Clark to continue accessing and downloading Clown content.		

Email Communication 4			
E-Mail From	kcent00@gmail.com	**E-Mail To**	jazzasimpson0000@gmail.com
Subject	Re: clowning about	**Date/Time**	2018-07-09 11:24:08 SGT
Message (Plaintext)	I am done with this game. This is what I got, now leave me alone!!!!! 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!		
Attachments	/img_202.dd/Users/computer/AppData/Roaming/Thunderbird/Profiles/1cug4fub.default/ImapMail/imap.gmail.com/[Gmail].sbd/Sent Mail/k13320412.zip		
Size	9245667 bytes	**MD5**	70b6b0b9caffa5489bbb980c36be9d23
Internal ID	18605	**SHA-256**	f12d808031870c89feb7bb32ad8d90cd0c4fd0477f541197248d589f28c5d6dd
Analysis Comments	After collecting data of Clowns various contents, Clark compresses the zip file and distributes clown's material to the blackmailer. Clark seems to have a hard time with this.		

Email Communication 5			
E-Mail From	jazzasimpson0000@gmail.com	**E-Mail To**	kcent00@gmail.com
Subject	Re: clowning about	**Date/Time**	2018-07-10 09:41:42 SGT
Message (Plaintext)	No, no, you are not done, I want more, more clown content! 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!!!!! 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!		
Attachments	-		
Size	79863 bytes	**MD5**	4ede63d85050332ba45a74c048fd2843
Internal ID	18583	**SHA-256**	cecf5e10ce695d8cb97debcd07d90b06717a408c3780e990e6b76959f6bf844a
Analysis Comments	Despite receiving clown contents, the blackmailer continues to say that he wants clown's material. If he does not continue, it is likely that Clark's identity will be revealed.		

In addition, I analysed the logs of the mIRC software used for other communication. But there is no meaningful information for just running it.

mIRC log Communication			
Source of Path	/img_202.dd/Users/computer/AppData/Roaming/mIRC/logs/status.AustNet.log		
Session Start	Tue Jul 03 09:18:02 2018	**Session Close**	Tue Jul 03 09:19:05 2018
Modified	2018-07-03 09:19:06 SGT	**Created**	2018-07-03 09:18:02 SGT
Accessed	2018-07-03 09:18:02 SGT	**Changed**	2018-07-03 09:19:06 SGT
Size	3609 bytes	**MD5**	787e6e5276fadf882716b5eeda3747dd
Internal ID	17596	**SHA-256**	8ab88d6db05779fdcfe498a397480e5f300eb0d2470dbb22e658c92fea51154b

Issue #4 - Quantity of Files

The following is the analysis of the 202.dd submitted as evidence with Autopsy. Files with name and hash value are the same, but files in other locations are counted as different files.

File Types	Number of Files in System	Number of Files Related to Illegal: Clown	Percentage
Images	51341	29	0.056%
Videos	434	3	0.691%
Audio	380	4	1.052%
Archives	669	2	0.298%
Database	115	0	0%
Documents: HTML	905	1	0%
Documents: Office	27	0	0%
Documents: PDF	13 (7)	8 (4)	61.5% (57.1%)
Documents: Pain Text	325	0	0%
Documents: Rich Text	91	0	0%
Executable File: .exe	3098	0	0%
Executable File: .dll	21574	0	0%
Executable File: .bat	20	0	0%
Executable File: .cmd	10	0	0%
Executable File: .com	23	0	0%

Issue #5 - Installed Software

A list of programs installed by the computer user. The date of installation of the first programs is 18th March 2017. However, in Autopsy OS Information, the date the OS was installed is 8th May 2017, so it is shown as a program that was installed by default in Windows. And I did not find anything unusual in programs prior to 2nd May 2018, which judged to have occurred since then. It seems that have installed Windows OS and made basic settings so that can use this computer immediately later. Below is a list of programs installed after 2nd May.

Program Name	Installed Date/Time	Description
Mozilla Maintenance Service v.59.0.3	2018-05-02 02:32:06 SGT	This program is necessary to automatically update Mozilla programs. It is installed when Firefox and Thunderbird are installed.
OpenOffice 4.1.5 v.4.15.9789	2018-05-03 00:13:25 SGT	This is the program need to use documents.
Mozilla Thunderbird 52.8.0 (x86 en-US) v.52.8.0	2018-06-07 00:00:43 SGT	The program used to receive and send email.
TrueCrypt v.7.1a	2018-06-07 00:53:48 SGT	It was used to encrypt the content threatened with a USB stick into a USB file.
Mozilla Maintenance Service v.60.0.2.6730	2018-06-18 02:40:11 SGT	Mozilla Maintenance Service v.59.0.3 has been updated.
Mozilla Firefox 60.0.2 (x64 en-US) v.60.0.2	2018-06-18 23:54:58 SGT	Used to web searching and download materials or programs.

Appendix A - Running Sheet

List of software used for investigation.

Software Name	Version	Frequency	Software Name	Version	Frequency
VMWare Fusion	12.1.2 (17964953)	Frequently	TrueCrypt	7.2	1 time
Windows 10	20H2 v2 x64	Frequently	LibreOffice	7.1.4	Frequently
Flare VM	v3.0.1	Frequently	Firefox	89.0.1 (x64)	Frequently
Kali Linux	2021.2 (amd64)	3 times	Thunderbird	78.0.11	2 times
Autopsy	4.18.0	Frequently	Malwarebytes	4.4.117	1 time
FTK Imager	4.5.0	1 time	VirusTotal	-	1 time
Registry Viewer	2.0.0	1 time	John the Ripper	1.9.0	1 time
Event Viewer	-	1 time	TrueCrack	v3.6	1 time
CertUtil	-	Frequently	Firefox Decrypt	1.0.0	1 time
WinMD5	v1.20	Frequently	StegSeek	V0.6	1 time
7 Zip	19.00 (2019-02-21)	3 times	StegSecret	beta v0.1	1 time

This is a record of investigation and times are written in terms of SGT.

Date Time	Events	Justification	Action/Description
15th June 2021 16:19 52m	Installing Windows 10 in a Virtual Environment with VMware Fusion	Build a forensic environment isolated from the host OS to prevent risks to prevent risks.	Install a new Windows 10 VM via File/New in VM Ware Fusion. Specifications are as follows: - CPU 6 cores - RAM 8192MiB - Disk Size 150 GiB Since Flare VM is going to be installed, the Username is FlareVM and the password is set to flarevm. In addition, update OS then, installs FTK Imager, Registry Viewer, 7 Zip, WinMD5, Thunderbird, Firefox, LibreOffice.
15th June 2021 17:11 24m	Installing Kali Linux in a Virtual Environment with VMware Fusion	Kali Linux was used when analysis or cracking was required in other Linux environments.	Install in the same way as Windows. When installing, it must specify Debian 10 x64 and install it. - CPU 4 cores - RAM 6144MiB - Disk Size 120GiB In the options during installation, click the Advance installation option.
15th June 2021 17:35 132m	Installing Flare VM in the Windows 10	Flare VM is set up as the environment mainly used by the Blue Team on Windows 7 or higher OS, and software.	1. Download files from Github: fireeye/flare-vm to Desktop 2. Run powershell with administrator privileges 3. Disable Windows Security - Disable real-time protection - Disable cloud-delivered protection - Disable automatic sample submission > cd C:\Users\FlareVM\Desktop\flare-vm > Unblock-File .\install.ps1 > Set-ExecutionPolicy Unrestricted > .\install.ps1 -password flarevm 4. Take a VM snapshot after installation.
15th June 2021 19:48 5m	Write Blocker Settings through Software	Prevent information leakage and ensure data integrity when creating images by writing-protecting the input external hard drive or Flash Drive.	1. Power Key (Win key) + R 2. Enter: regedite.exe 3. Create StorageDevicePolicies in Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control with New/Key 4. Create WriteProtect with New/DWORD (32-bit) Value in StorageDevicePolices 5. Change the Value data to 1 through Modify

15th June 2021 19:53 1m	Make Case folder	Setting up a location for Investigation.	Create a Case folder in the Documents folder.
15th June 2021 19:53 8m	Image extract at 202.7z	Extract images for Investigate.	Create an Image folder in the Case folder and put files 202.7z.001 to 202.7.008 7 Unzip the 202.dd file with a zip program.
15th June 2021 20:01 5m	Get hash value with CertUtil	Securing integrity by obtaining hash values of MD5, SHA-1 and SHA-256.	Run Powershell. > cd .\Documents\Case\Image\ > certutil -hashfile 202.dd md5 > certutil -hashfile 202.dd sha1 > certutil -hashfile 202.dd sha256 MD5:15f5d5224b4bed8a97b6fc0c2a7ecfbc SHA1: e710298646c46ee8ff70a96cd4d28423fe274eeb SHA256:63e1d27a9a36f0d6c5fc4305197c39e83491220d11bead185bebd29c5ce31871
16th June 2021 09:10 268m	Create a case with Autopsy	Prerequisite for image analysis and Investigate with Autopsy.	1. Run Autopsy and click New Case 2. Be careful not to duplicate names Case Name: 202-PSB201IT-LE-20210607 Base Directory: C:\Users\FlareVM\Documents\Case 3. Case Number: 001 Name: Leslie Phone: +6592741428 Email: leselsey@outlook.com Noted: Clowning About Again↵ First Forensics (Created 16th June 2021) 4. Disk Image or VM File 5. Path: C:\Users\FlareVM\Documents \Case\Image\202.dd Time zone: (GMT +8:00) Asia/Singapore MD5:15f5d5224b4bed8a97b6fc0c2a7ecfbc SHA1: e710298646c46ee8ff70a96cd4d28423fe274eeb SHA256:63e1d27a9a36f0d6c5fc4305197c39e83491220d11bead185bebd29c5ce31871 6. Select All
16th June 2021 15:08 4m	Integrity check	Integrity check to see if Check for data corruption.	Easily check 202.dd file integrity with WinMD5 Integrity check for 202.dd even inside Autopsy
16th June 2021 15:12 17m	Browse user folders	By default, files are saved in Desktop, Documents, Downloads, Pictures, and Videos, so check first.	Autopsy's Result - Recent documents identified various violations. Based on this, the following clown contents were found. Most of the file metadata contains the URL path from where it was downloaded. Desktop (5): index.jpg, k13320412.jpg, k13320412.zip, k14032380.jpg, k7827739.jpg Document (2): The psychology behind why clowns creep us out.htm, image-20160926-31853-1jvhtv4.jpg Downloads (3): Little Night Music - Send In The Clowns.pdf, Clowns dancing.mp4, Couto, Mia.pdf Pictures (6): 1492447345937.jpg, kikkii_clown_party_pose.jpg, Ronald_mcdonald-e1476200032847-660x330.jpg, s-l640.jpg, scary-halloween-costumes-ideas-Clown-blood-Halloween-party-costumes-e1410943909179.jpg, cary-halloween-costumes-ideas-Clown-blood-Halloween-party-costumes-e1410943909179.jpg
16th June 2021	Investigate about web	Investigate browser and browsing: web history, search, cookie and bookmarks.	First, check Results - Web History in Autopsy. It can see that Edge and Firefox are both used as browsers, and Edge appears to have been used for Windows-related updates or to open files with a browser. In the case of Firefox, it seems that it was used for general browser purposes, and I checked

15:19 85m			the fact that it was downloaded and searched for clown. Based on this, Result - Web Download checks which files were downloaded to which path. Additionally, I can easily check which search was performed and when in Result - Web Search. And in Result - Web Bookmarks I can find that one clown related bookmarks have been registered.
16th June 2021 16:44 29m	Investigate installed software	Investigate what software is installed and how it was used.	can check the list of installed software in Autopsy's Result - Installed Programs. The first many programs were installed on 2017-3-18, but it seems to be an application that was pre-installed in the OS. Various programs have been installed since 2018-5-2, so it seems to using started at 2nd May. In addition, Mozilla Maintenance Service was installed, and it is presumed that Thunderbird and Firefox were installed, and OpenOffice necessary for other tasks was installed. Another noteworthy thing is that TrueCrypt and the mIRC program are installed.
16th June 2021 17:13 1m	Investigate Recycle Bin	Investigate what files were trying to delete.	Both the Firefox installation file and the TrueCrypt installation file that were on the desktop were registered in the Recycle Bin. I couldn't figure out any other strange things.
16th June 2021 17:13 6m	Investigate email	Email Investigation and Violation Detection.	There are three patterns of using e-mail. - Notification email from Google: 3 - About sassypenguin0@gmail.com: 3 - About jazzasimpson0000@gmail.com: 5 For the first two emails, it's password and an email from Google telling signed in on new device. Checking the emails suggests that the user's email address is kcent00@gmail.com and the owner's name is Clark. And I found the clue Clark <kcent00@gmail.com> in E-Mail Messages Artifact. I also sent an email to jazzasimpson0000@gmail.com on 28-07-09 11:24:08, which appears to have attached k13320412.zip. There are 12 clown contents in the contents, so I found the circumstance that the clown contents were distributed.
16th June 2021 17:20 32m	Inference exploration	Gathering data to proceed with the investigation.	There's a Works folder in Documents, a report related to work. And it is written by Clark Kent. The creation time is between 7 and 8 am, so Clark appears to be working in the morning. And the Journal document file, the title is Personal Journal, where various diaries are written. There is also about clown on 25th June. But before that, it sad got a strange phone call on 5th June, and after got a White USB stick on 7th June.
16th June 2021 17:52 7m	Investigate USB flash drive	According to Personal Journal, he received a white USB stick on the 7th June. It's an investigation into what's weird.	Look at USB Device Attached in Autopsy, I can see that a product called JumpDrive V10 made by Lexa Media, Inc. was connected on 2018-06-07 08:51:39. Device ID is 844BF5082FBF9B8537E, for more accurate confirmation, this flash drive must be confiscated as evidence. Look at Encryption Suspected afterward, I can guess that a file called usb was created here on 2018-06-07 08:55:35, but it seems that the white USB stick has been encrypted. Among the installed programs list, TrueCrypt is the only program that encrypts, and it is assumed that TrueCrypt is encrypted because it is possible to install TrueCrypt in the Desktop folder where the usb file is located. According to information from Installed Programs, TrueCrypt was installed on 2018-06-07 00:53:48. Looking at the log in /img_202.dd/Users/computer/AppData/Roaming/TrueCrypt/Configuration.xml, the file was created 2018-06-07 08:54:45, Modified changed 2018-06-18 13:39: 06, it seems that the last decryption was done on 18th June.
16th June 2021	Crack usb encryption password	Crack the password to investigate the file that supposedly encrypted the white USB stick.	1. Extract the usb file from Autopsy 2. After moving to Kali Linux Desktop, check the integrity 3. Crack the password 3-1. Dictionary attack via TrueCrack

19:32
12m
			$ truecrack -t ~/Desktop/usb -w /usr/share/wordlists/seclists/Passwords/Common-Credentials/10-million-password-list-top-1000000.txt
			3-2. Rainbow Table Attack with John the Ripper
			$ cd /usr/share/john
			$ ./truecrypt2john.py ~/Desktop/usb > ~/Desktop/usb-hash.txt
			$ john ~/Desktop/usb-hash.txt --wordlist=/usr/share/seclists/Passwords/Cracked-Hashes/milw0rm-dictionary.txt
			$ john --show /home/kali/Desktop/usb-hash.txt
			4. The same password crack result is output for both: planet

16th June 2021 19:44 3m	Get usb file image for forensics	Creating usb images for evidence and digital forensics	1. Check the integrity of the extracted usb file. 2. After installing TrueCrypt, mount the usb file on the E: drive. Enter the password as planet. 3. Image the E: drive with FTK Imager for evidence collection and analysis. 3-1. Logical Image 3-2. Add > Raw (dd) 3-3. Case Number: 001 Evidence Number: 202-PSB201IT-LE-20210607-Identification_File_2 Unique Description: 202-PSB201IT-LE-20210607-exported-usb Examiner: Leslie Notes: USB image of 202.dd 4. The hash value of the generated image. MD5:54ac5fe8df089341f71700e9738f722a SHA1:de74e8af890410d8fc63cdd3525cbd6556595000 SHA256:af80326efdbf08063ae664fad8ea7b74f19e6e6b2d4360d11f2ccd926e196978
16th June 2021 19:47 4m	Investigate usb file	Analyse the created usb image with Autopsy to use it as analysis and evidence	1. Created images are made through Autopsy. Same as 202.dd, with the following differences. Case Name: 202-PSB201IT-LE-20210607-exported-usb Case Number: 001 Noted: Encrypted usb file by TrueCrypt in 202.dd image↵ Investigation by creating an image file after decryption 2. There are 3 files inside- Open-me-first.doc, open-me-second.doc, open-me-third.doc. As a result of checking the contents, it is considered black mail.
16th June 2021 19:51 11m	Investigate email again	Re-investigation of blackmail from email with information obtained from usb file.	The 3 files from the usb are seen as the first threat. It appears that subsequent contact was made via email. The username that appears to be Blackmailer is jazzasimpson0000@gmail.com and the name appears as Jerry Simpson. Also I found the clue Jerry Simpson <jazzasimpson0000@gmail.com> in E-Mail Messages Artifact. I've had a total of five emails with Clark, and it's Jerry Simpson that Clark sent the clown's content to.

16th June 2021
 	
20:03
15m
	Try to penetrate email	Investigation to identify outliers and obtain further.	1. Extract the folder /img_202.dd/Users/computer/AppData/Roaming/Thunderbird/Profiles/1cug4fub.default from Autopsy
			2. Compress as a zip file with 7 Zip program
			3. Move to Kali Linux's Desktop and unzip it
			4. Extract ID and PW through firefox_decrypt
			$ git clone https://github.com/unode/firefox_decrypt.git
			$ python3 ~/firefox_decrypt/firefox_decrypt.py ~/Desktop/1cug4fub.default
			5. Execution result
			Website: oauth://accounts.google.com
			Username: 'kcent00@gmail.com'
			Password: '1/sI6VtwQbGlkZtt-joYOF6BNUSAMB2lu_H_sCa5qq5WY'
			6. Check directly through Thunderbird$ sudo apt install -y thunderbird && thunderbird
			CTL-C
			$ cd ~/.thunderbird && cp -r [namecode].default-dafult [namecode].default-dafult.bck

			$ rm -rf [namecode].default-dafult/*
			$ cp -r ~/Desktop/1cug4fub.default/* [namecode].default-dafult
			$ thunderbird
			Checked email, but nothing special. Also, I tried to access Gmail, but I couldn't access my Gmail account like the contents of the email saying “Password has been changed”.

16th June 2021 20:18 4m	Investigation mIRC	Check the log file as there may have been additional threats or clown distribution with mIRC chat program.	Autopsy's Installed Program says that it was installed on 2018-07-03 01:13:51. Check the log file in /img_202.dd/Users/computer/AppData/Roaming/mIRC/logs/status.AustNet.log. But there are nothing unusual information.
16th June 2021 20:22 37m	Investigation of remote control possibilities	Investigation into being hacked 1, also prove that no one else has used it.	Among the installed programs or downloaded programs, tools related to remote control are not visible. It might have done it the other way around, so Autopsy searches the Remote Desktop Connection Manager with Keyword Search. I can check two files, IndexedDB.edb and edbtmp.log, and “remote desktop connection 0” is written in the contents of both files. Additionally, I checked the event log. Extract /img_202.dd/Windows/System32/winevt/Logs/Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx and check it through Event Viewer. I checked all the contents of Event ID 21 through Filter, but all result values were Source Network Address: LOCAL.
16th June 2021 21:00 56m	Malware Diagnostics	Investigation into being hacked 2, also prove that no one else has used it.	Autopsy extracts all files in 202.dd. Create a Temp/202files folder in the Case folder and extract it there. After extracting, Malwarebytes is installed and then the 202files file is scanned for viruses.One file was confirmed: bfgminer-5.5.0-win64.zip Checked it through VirusTotal, but it doesn’t seem to be related to hacking with a Bitcoin mining program.
16th June 2021 21:56 52m	Check the number of logons and time	Investigation into being hacked 3, also prove that no one else has used it.	Extract /img_202.dd/Windows/System32/config/SAM and open it with AccessData Registry Viewer. I can see that the user name in SAM/Domains/Account/Users/000003E9 is computer. However, I can confirm that there is no password because Password Required is set to false. The Logon Count is 19, and based on this, I will have to check the event log directly to see if there is an abnormal connection. Extract the /img_202.dd/Windows/System32/winevt/Logs /Security.evtx file and open it with Event Viewer. After that, I filtered and looked at Event ID 4624, but couldn't find anything odd. However, I'm not sure if Clark was the only one with access to this computer. It would be nice to secure witnesses or company CCTV that he didn't touch to do exactly that.
17th June 2021 16:10 8m	Check use CLI	Check if something has been done via CMD or PowerShell	There are no logs in CMD log. If used PowerShell, there should be /img_202.dd/Users/Computer/AppData/Roaming/Microsoft /Windows/PowerShell/PSReadLine/ConsoleHost_history.txt, but since the PowerShell folder doesn't even exist, it seems that PowerShell has never been run.

17th June 2021
16:18
37m
	Scan and check steganography	steghide-0.5.1-win32.zip is downloaded to the download folder at 2018-07-02.	Additionally, I didn’t find any evidence that the steghide-0.5.1-win32.zip archive was decompressed, and it is presumed that it was not used as there is no trace of use by the CLI program. However, to confirm exactly scan all files use StegSecret which is steganography decoder tool. It analysed a total of 141 files in /img_202.dd/Users/computer except the AppData folder. Detected 1 file, but it was steghide-0.5.1-win32.zip, so couldn't find steganography files.
			Moreover, I checked some of the main files manually. Install StegSeek on Kali Linux, an integrated tool that can find out the contents of StegHide and even unlock the password if there is.
			$ sudo apt install libmhash-dev libmcrypt-dev libjpeg-dev zlib1g-dev git build-essential cmake
			$ git clone https://github.com/RickdeJager/stegseek.git

			$ cd stegseek && mkdir -p build
			$ cd build && cmake -DCMAKE_BUILD_TYPE=Release ..
			$ make && sudo make install
			$ stegseek [file] /usr/share/wordlists/seclists/Passwords /Common-Credentials/10-million-password-list-top-1000000.txt
			However, couldn't find anything either.

17th June 2021 16:55 17m	Browse violations by file type	Investigation of additional and what percentage of the total files were violated.	Check the number of files by type in 202.dd through Autopsy's Views - File Type. Afterwards, check all clown-related violations here as well. I checked the keyword search and manual search properly.

Appendix B - Timeline of Events

Here is the timeline of the incident.