Case Study –

Name:

Lecturer:

Location:

Contents

1. Summary

This report concerns the allegation made to law enforcement, via a witness, who claims to have seen an individual (Jane Smith) access illegal Lego related content within a place of work. In the state of Western Australia, it is illegal to access, own or distribute digital content relating to "Lego".

A logical image of the suspect's seized laptop was acquired by a junior investigator. The image details are as follows:

Image Name	lego.dd
MD5 Checksum	ece47be96a95dd543f7acf0d583106af
Computer Name	DESKTOP-IQ9AQVC
Device ID	9932a469-56a6-4a89-a955-e2ec14c7cca9
Operating System	OS Drive (Windows 10 Education)
Total Capacity	31,042,785,280 Bytes
Timezone	Australia/Brisbane (UTC+10 hours)

The following software applications were used to perform the investigation:

- OSForensics
- Autopsy
- Scalpel
- FTK
- Steghide and stegcrack
- Kali Linux (e.g. Truecrack, John the ripper)
- Event Log Explorer
- Windows Event Viewer

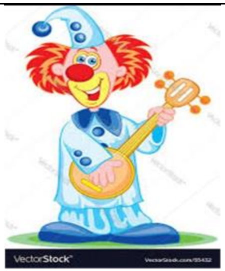
File summary:

File type	**Count**
Images	57686
Videos	50
Audio	286
Documents	68412
Executables	47248

The investigation found the following lego related content

- At least 15 lego related items were downloaded via the Firefox web browser:
    - 10.jph (image) files
    - 2 .png (image) files
    - 1 .mp4 (movie) file
- Two screenshots
-

2. Issue #1: Content Relating to the Offence

	
Filename	index.jpg
Location	\Users\computer\Desktop
Size	15,015 Bytes
Sectors	2,997,704 – 2,997,733
Type	JPEG/JFIF
Created	02/07/2018 09:12:29 AM
Accessed	02/07/2018 09:12:30 AM
Modified	02/07/2018 09:12:30 AM
MD5	64b61cf19e916bc1a40831a17db83b3b
Analysis	Clown in blue suit holding a musical instrument.

Filename	A Little Night Music - Send In The Clowns.pdf
Location	\Users\computer\Downloads
Size	3,146,439 Bytes
Sectors	1st Fragment: 2,496,664 – 2,496,839 2nd Fragment: 35,457,824 – 35,458,231 3rd Fragment: 33,154,304 – 33,155,439 4th Fragment: 31,441,536 – 31,442,503 5th Fragment: 29,081,488 – 29,082,743 6th Fragment: 25,032,024 – 25,033,319 7th: Fragment: 29,596,216 – 29,570,121
Type	PDF
Created	19/06/2018 07:44:24 AM
Accessed	19/06/2018 07:44:24 AM
Modified	19/06/2018 07:44:31 AM
MD5	4f640bc32c0ac35b585a814ee5235df4
Analysis	Musical sheet for clown-themed music.

3. Issue #2: Identification

Evidence obtained during the investigation identifies the suspect, Clark Kent, as the owner of the clown-related content found on the seized laptop.

- The suspect has stated that the seized laptop belongs to him. The following evidence supports this statement: ○ Four emails were found in the Sent Mail folder of the Mozilla Thunderbird email client. The emails were sent from the email account kcent00@gmail.com while the sender was logged in as the “computer” user account. No other emails were sent from other user accounts.
    - ○ The “computer” user account had logged into the system 19 times since the system was installed. No other user account has logged into the laptop.
- The suspect has stated that he does not lock his laptop when away from his desk. Evidence showing that the “computer” user account is not protected by a password supports this statement.
- No evidence was found to suggest that anyone else had logged into the “computer” user account locally, other than Clark Kent.

4.

Issue #3: Intent

Each clown-related image, video, document and web page was intentionally downloaded to the suspects computer via the Firefox web browser. The clown-related content was first searched for from the Firefox web browser using Google and Youtube prior to being downloaded. In the case of the video file found on the suspects computer, the video hosted on Youtube was converted to a downloadable video format using an online video converter before being downloaded. An exception to this fact is the clown image "index.jpg". Although the image was created on the hard disk during the same time period that other clown activity was taking place, no evidence that is was downloaded via the web browser could be found on the laptop image.

The following browser activity supporting the fact that the evidence was intentionally downloaded is presented.

Date / Time	Filename	Details
18/06/2018 8:19:33 AM	scaryclown.jpg	Google search for "clowns" executed in Firefox.
18/06/2018 8:19:40 AM		Image results tab within Google clicked on.
18/06/2018 8:19:47 AM		"scaryclown.jpg" clicked on within Google image results.
18/06/2018 8:20:04 AM		"scaryclown.jpg" downloaded from "http://www.scarymommy.com/wpcontent/uploads/2016/10/scaryclown.jpg?w=697" to suspect's laptop.
18/06/2018 8:21:54 AM	scary-halloween-costumesideas-Clown-bloodHalloween-party-costumese1410943909179.jpg	"https://deavita.net/wp-content/uploads/2014/09/scary-halloweencostumes-ideas-Clown-blood-Halloween-party-costumese1410943909179.jpg" visited in Firefox.
18/06/2018 8:21:54 AM		"scary-halloween-costumes-ideas-Clown-blood-Halloween-party-costumese1410943909179.jpg" downloaded to suspect's laptop.
18/06/2018 8:22:07 AM	1492447345937.jpg	"1492447345937.jpg" clicked on within Google image results in Firefox.
18/06/2018 8:22:15 AM		"1492447345937.jpg" downloaded from "https://static1.squarespace.com/static/530becede4b093256168fba5 /t/58f4f06d15d5db5e25316c1e/1492447345937/" to suspect's laptop.

Issue #4: Distribution

Evidence presented below shows that Clark Kent sent an email to Jerry Simpson with a zip file (archive) attachment containing clown-related images that were previously downloaded. The zip file was created minutes before the email was sent.

Date / Time	Event	Details
9/07/2018 11:12:37 AM	"computer" user account logon.	
9/07/2018 11:22:58 AM	Zip file created.	Zip file archive k13320412.zip is created at \Users\computer\Desktop.
9/07/2018 11:23:45 AM	Zip file last modified.	Final file added to k13320412.zip archive.
9/07/2018 11:24:08 AM	An email is sent by Clark Kent including	From: kcent00@gmail.com To: jazzasimpson0000@gmail.com

5.

<table>
<tr>
<td></td>
<td>k13320412.zip as an attachment.</td>
<td>
<table>
<tr><td>Time Sent:</td><td>9/07/2018 11:24:08 AM</td></tr>
<tr><td>Subject:</td><td>Re: clowning about</td></tr>
<tr><td>Body:</td><td>I am done with this game. This is what I got, now leave me alone!!!!!</td></tr>
<tr><td>Attachments:</td><td>k13320412.zip. Contents of k13320412.zip:
• 1492447345937.jpg
• A Little Night Music - Send In The Clowns.pdf
• Clowns dancing.mp4
• Couto, Mia.pdf
• index.jpg
• k7827739.jpg
• k13320412.jpg
• k14032380.jpg
• kikkii_clown_party_pose.jpg
• Ronald_mcdonald-e1476200032847-660x330.jpg □ scaryclown.jpg
• scary-halloween-costumes-ideas-Clown-bloodHalloween-party-costumes-e1410943909179.jpg</td></tr>
</table>
</td>
</tr>
<tr>
<td>9/07/2018 11:27:45 AM</td>
<td>“computer” user account logoff.</td>
<td></td>
</tr>
</table>

Issue #5: Motive

Evidence found during the course of the investigation and presented below, indicates that the suspect’s motive for downloading the clown-related content was because he blackmailed. He received 3 threatening letters telling him to download the clown-related content for another party, else they would reveal a secret about Clark which could potentially be damaging for the suspect.

□ 2 entries were made in the Clark Kent’s personal journal, Journal.doc, referring to the suspect receiving a USB “stick” (device) from an unknown party.

6.

Issue #6: Quantity of Files

The following file numbers and statistics have been taken from the following working directories used by the suspect:

- \Users\computer\Desktop
- \Users\computer\Documents
- \Users\computer\Pictures

Filetype	# of Files	# of Files Related to the Offence	% of Filetype Related to the Offence
.DOC / .DOCX	11	0	0.00%
.EXE	1	0	0.00%
.GIF	1	0	0.00%
.HTM	3	1	33.33%
.JPG	19	11	57.89%

8. Issue #7: Installed Software Related to the Investigation

Software	Software Purpose	Usage Count	Last Run Date / Time	Investigation Details
Mozilla Firefox 60.0.2	Internet web browser.	42	11/07/2018 8:09:09 AM	Firefox was the primary tool used by the suspect to access clown web content and download a number of clown-related images, documents and a video.
Mozilla Thunderbird 52.8.0	Email client.	10	11/07/2018 8:09:28 AM	Mozilla Thunderbird was used by the suspect for work-related emails as well as for distributing clown-related content.

9. Timeline of Events

The timeline below presents the following activity:

- “computer” user account logon periods for the days that clown content was accessed
- Clown-content download events via the Firefox web browser
- Events that identify the suspect, Clark Kent, including sending of emails and editing of documents
  - Laptop system information events:
    ○ Windows 10 installation ○ “computer” user account
    creation ○ Final recorded system event prior to system
    seizure.

10. Running Sheet

10.1. Collection

Date / Time	Task Details	Duration
27/08/2018 09:00 AM	Download laptop logical image (182.dd) archive files (7 Zip) from *https://blackboard.ecu.edu.au/webapps/blackboard/content/listContent.jsp?course_id=_649340_1&content_id=_5810467_1&mode=reset* and ensure the integrity of each file using Quick Hash, MD5 and the 182-md5.txt file provided on the download page. **Results from Quick Hash and MD5:** 182.7z.001: 90bc13ee6fc8d727b8ef4d15f8ea0113 182.7z.002: 2027ab6f49b6d18ef4c42c3ec04ab070 182.7z.003: 00bab1e957bf58ef31c131f79e917851 182.7z.004: 38c8c03f254131c11462fbfe33e95e39 182.7z.005: 970961797afa65420441decc6f561440 182.7z.006: 0be7b6cadd0bd5ce1e1830833bd8ba1c 182.7z.007: 03fb8aed700bbd7f0f051e7b8a5f07ed 182.7z.008: 793b3b07a8b9d32c21a820caa27439ef 182.7z.009: 2eda3a0e19090a2ff5ecb8426db44344 182.7z.010: 0a3a889ec5c583e58d14f226ee79d07e 182.7z.011: dcc2d89f6f9962edc9f987eeb3f34f41 182.7z.012: 695b32f630df008f23376ad5c31eaf21 182.7z.013: eff60512189034622dc7b88f00a44e39 182.7z.014: 4131f8d9c30f83912d5bb82b8b57e32d 182.7z.015: 734a55ba4c459214375515dac0d4191b	1 hour
27/08/2018 10:00 AM	Extract 182.dd image from archive files and ensure the integrity of the image file using Quick Hash and MD5. **Result from Quick Hash and MD5:** 182.dd MD5 hash = 15f5d5224b4bed8a97b6fc0c2a7ecfbc	10 mins
27/08/2018 10:10 AM	Make working copy of downloaded image, move copy to the case working directory and verify integrity of the copy using Quick Hash and MD5. **Result from Quick Hash and MD5:** 182.dd.working MD5 hash = 15f5d5224b4bed8a97b6fc0c2a7ecfbc	5 mins
27/08/2018 10:15 AM	Make backup copy of downloaded image, move backup to the backup folder and verify integrity of the backup using Quick Hash and MD5. **Result from Quick Hash and MD5:** 182.dd.backup MD5 hash = 15f5d5224b4bed8a97b6fc0c2a7ecfbc	5 mins