PRELIMINARY EXAMINATION REPORT
Computer Crime Investigation Section
14F0861
(Zaharie Shah)

Date: 19 MEI 2014 (Sita refer to attachment "User2.txt")

PRELIMINARY EXAMINATION REPORT

Once I got home, I have run the initial inspection
on a computer that is located upstairs in the living room of the house. Computer
when the check is in the situation has been turned on. I've Ob
make checks on the software available on the computer Desktop
before closing the back of the computer. Next, all equipment
Connecting with a computer was seized for further examination in
Police Forensic Laboratory.

INSPECTION REQUIRED
Asked to remove content that can be associated with data loss case
aircraft type Boeing 777-200 owned by Malaysia Airlines (MAS) using code
flight MH370.

EXHIBITS
Goods examined the case are as follows: -
NO. DESCRIPTION QTY exhibits • SIGNS
1 One (1) piece of black computer brand Corsair MK20 6
with five (5) hard drive sizes:
- Seagate Barracuda 80 GB (4LRONY8Y) MK 22
- Western Digital 500 GB (WCAV95097190) MK 23
- Western Digital LTB (WMC1S2825793) MK 24
- Extream SanDisk SSD 240 GB (125,095,402,609) MK 25
- Corsair Force SSD 240 GB (1233071380011540502) MK 26

Exhibit 6 TOTAL

ANALYSIS EQUIPMENT
CASE OF FORENSIC SOFTWARE USED
MK 20 Inspection date and time on the computer via the CMOS settings.

MK 22, MK23, MK24, MK25, MK26

• Forensic Tool Kit (FTK) 4.2
• FTK Imager 3.1

• FTK Registry Viewer 1.6
• Internet Evidence Finder 6.1
• EnCase V6.18

METHODOLOGY ANALYSIS
On March 15, 2014 at 2300hrs computer has been refitted as
an original arrangement of exhibits in a temporary store MH370, 4th Floor, Tower 2,
Bukit Aman. There are all hard drives in the computer has been on image
according to the information source as follows

EXHIBIT	IMAGE ACQUISITION			HASH VALUE	
	DATE	START (HRS)	END (HRS)	MD5	SHA 1
MK 25	16/3/2014	0013	0112	89b6e14013f4d4fce20f546d82fb8904	be495a423c144b9f1a7fbb5704d2089f57a100b8
MK 24	16/3/2014	0323	0721	2761271878d83aba1a2cfa600db9e2d5	468a158d51c02e83d65d1e172892308622a9b1b3
MK 23	16/3/2014	2003	2210	3f6620d33f8701c4d3aad1e8fc0c84e4	b6bb4ab14b9023597c232feb26c9865312ef1f91
MK 26	16/3/2014	0033	0137	ac51fd6590fb510c35688bac6f23bf2a	8d9d2f066742d3a8b30ee5861ee3dcce0ba7be58
MK 22	16/3/2014	1951	2013	faf5a9a87239531ec631a0e14b8c08f4	3f565a05e8632b4ab4dab865ca62f67e9c0a66f6

Each disk has the image using FTK Imager to ensure data integrity
which will be analyzed in the hard drive. Before an image is used, the test
data integrity verification is carried out to ensure that the image is the same Hash Value
and not contaminated.

PRELIMINARY EXAMINATION RESULTS
Once complete disk imaging process implemented, all the exhibits have been
began to be analyzed and the results of the initial inspection on all goods case is like
below:

MK20 (Computer Corsair):
- It was found that there are five (5) of the hard drive inside the computer.
However, only one hard drive is connected (MK26) on
when the computer is stolen.
- Date and time the computer is right with the current time. There are no
damage to computer hardware, and it works well.

MK22 (80GB):
- Hard drive has been formatted on February 20, 2014 @ 0337hrs.

- The software used in the operation of this disk is Microsoft
Windows XP.

MK23 (500GB) and MK24 (1 TB):
- This hard drive is used as a data backup application that stores and some
software simulation games airplane like Xplane 10, Microsoft Flight
Simulation X (FSX) and Microsoft Flight Simulation 9 (MFS9).
- Results of inspections on record in RecycleBin file (file deleted) have been found
one file "User2.txt" who has a record list of online accounts together
password to. This file has been deleted on February 20th, 2014 @ 1130hrs. result
inspections on some ID that was found in the file, it was found that
it is a valid password and can be used.
However, no information source that could help the case is found.
(Sita refer to the appendix "User2.txt")

Figure analysis document "User2.txt"
There are 77 items in the document "User2.txt". Here is a summary breakdown
information source being derived from such documents;
- 11 items related to the user ID and password for the various types of forum flight
simulation.
- 7 items related to fund ID password 4 types of email. The following is
breakdown by type;
o Hotmail (3), Gmail (2), live (1), MAS (1)
• - 3 items are associated with ID and password and bank account online.
o Maybank (2), paypal (1)
- 28 items related to hobbies and Do It Yourself (DIY)
- 8 items associated with the account and password work (MAS)
- 2 items related to online book store.
- 5 item ID and password associated with your mobile phone
- 8 items associated with the user ID and password account social media sites
o Skype (1), facebook (4), youtube (2), tweeter (1)
- 5 items associated with the user ID and password online shopping account.

Inspection on account of the online book store. Zaharie on site
Mobipocket is found that he has 4 ebook on account
The. Here is the ebook is meant. (Sua refer to the appendix "ebook")
0

Further checks on the deleted file has led to the discovery of a folder
"777twintower". This folder has been deleted on December 18, 2013 @ 2249hrs.
Inside this folder has found some pictures of computer simulation and installation
the images show a MAS aircraft that fly heading towards Kuala Lumpur Tower and KLCC.
These images have been taken from the computer screen to play a simulated airplane. The
assessment believed that the owners of these computers have taken one of those images

for the purpose of being used as an icon on the account. Skype: catalinapby.
(Sita refer to the appendix "777twintower")

Narre Gate Si n cdified Type: e
Asiakulldone; docx 26 / 11.3 = 5.2212 Pi, i h ii cft Office RCR ... 55 4: F
KULasialdone.docx '5/52012 11:24 Pf l M: rrsoft Office.,. 33 KB
- It was found that the owner of the computer is very much like to use the word PBY Catalina in daily activities. Therefore, the word is used to search for documents on the hard drive is analyzed. Search results using keywords "PBY Catalina", was discovered by 2 Microsoft Word has data regarding flight route notes.
•
(Sita refer to the appendix "PBY Catalina"
- There is a record of the search word "allah hit me one more time" through the pages Search http: //www.goog! e.co.uk dated December 2, 2010 @ 1706hrs. No details More details regarding these words are found from these case goods.

MK25 (240GB):
- This hard drive using the Operating System of Microsoft Windows 7 Ultimate and Microsoft Flight Simulation software have been in the Install a 9 on 23 December 2013.
• - On February 20, 2014 has been in the gaming software Uninstall.

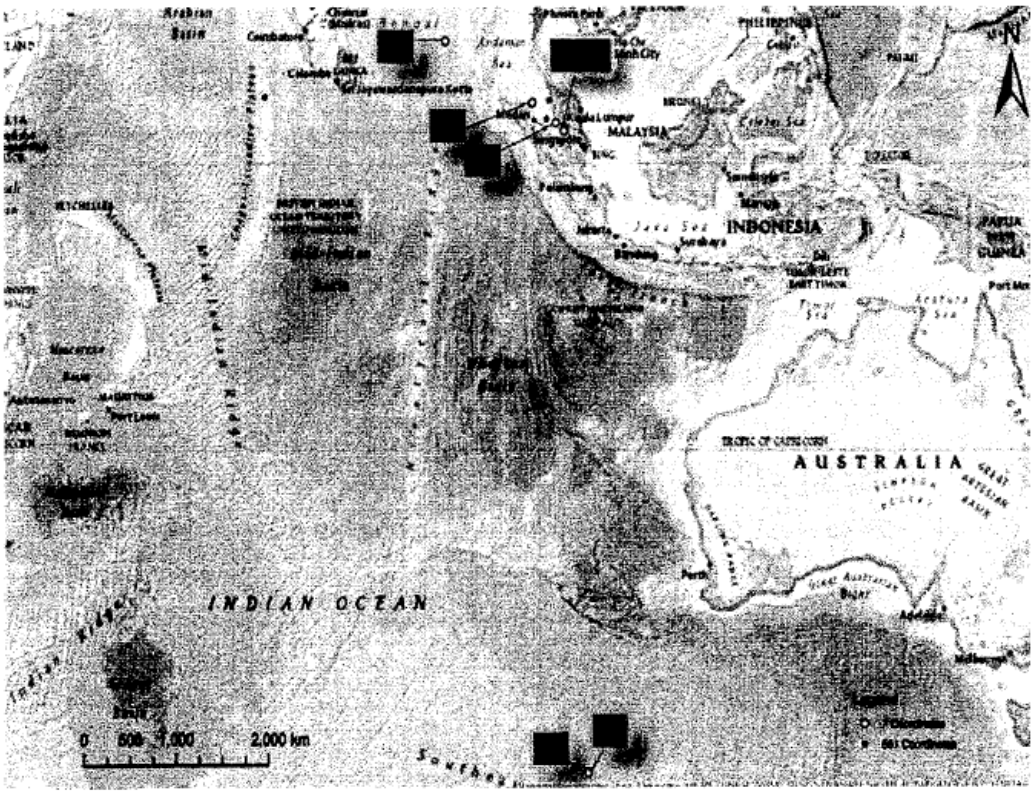
MK26 (240GB):
- This hard drive using the Operating System of Microsoft Windows 7 Ultimate and have Microsoft Flight Simulation X which has been in Install at 20 Software December 2013. The game was open (run) as much as 22 times in This computer.
- There are 5 Logbook.BIN found deleted files and only 3 of these file was found to have record data simulation game. Log dated March 15, 2014 is the date I have made the analysis on the hard drive directly to the editors make sure the computer is functioning properly after the seizure was made. following 5 are details of the log file

Last Accessed File Record
Logbook.BIN
03/15/2014 @ 2244hrs No log recorded
20/02/2014 @ 1107hrs 1 log recorded
01/02/2014 @ 1428hrs 4 log recorded
23/1/2014 @ 2056hrs 9 log recorded
09/12/2013 @ 1813hrs No log recorded

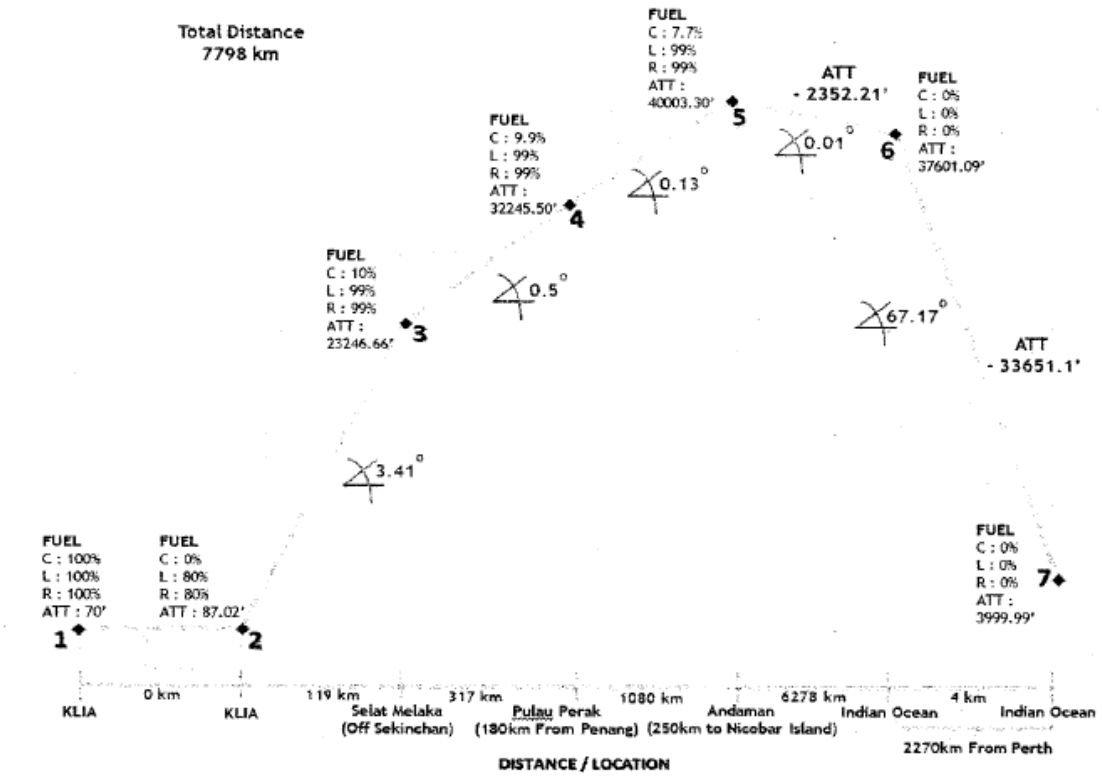
Analysis Over Game Microsoft Flight Simulator X (Mk25 & MK26):

Found that whenever games Flight Simulator X is played, it will
produces 7 types of files associated with the game. Information regarding 7
These files are as follows:
Data Format Description
Logbook.BIN It will result when the user opens the application game.
* .FSSAVE It will result when the user save the game.
* .FLT It will result when the user save the game.
* .WX It will result when the user save the game.
* .PLN It will result when the user save the flight plan.
* .cfg It will result when the user save the hardware configuration.
* .SPB It will result when the user save the game.
The results of all inspections on the hard drive of the computer, it was found that
there were 668 file types * .FLT whole. The highest number is in
Mk25 hard drive which there were 348 files * .FLT. Followed by the hard drive MK26
112 files, hardsik MK23 K24 of 106 files and 105 files.
Many of files * .FLT this is a file that exists during the installation of the game
, -., Microsoft Flight Simulator X and it's not necessarily the file that is created from
The game was played after installation

* .FLT This file containing the configuration and location coordinates flight game
in play during the game at the save. The assessment has found 2
coordinate the approaches available MH370 search location. in
Altogether there are 7 including 2 coordinate coordinate earlier believed
relate to each other. This is based on the name of the aircraft
stated in its configuration is the same, "PSS Boeing 777-200LR Malaysia
No VC ". All coordinates were found in a file Volume Shadow
Information (VSI) named {OOd7ef6c-8bcb-1Ie3-b3f7-ee8a9181afad} {3808876bc176-
4e48-b7ae-04046e6cc752} dated February 3, 2014. This is the VSI File
a file that stores information when a state computer
the computer is in an unused or ideally more than 15 minutes.
Therefore, it can not be ascertained that all the 7 coordinate is from
* .FLT the same file. (Sita refer to the appendix "Coordinates")
- Here is the mapping on 7 coordinates is:



Here is a summary on 7 coordinates specified by configuration
contained in files * .FLT found.
- Based on the readings of fuel, it was found that seemed coordinates 1, 2 and 3
is not connected despite the addition of altitude between the three
coordinates. le
- Coordinates 3, 4, 5, 6 and 7 look like fuel and connected for reading
altitude is consistent with the distance between the two coordinates.
- However, all the readings obtained may be modified by the player
this game at any time during the game. By changing the game
setting during the game also can produce as reading * .FLT
obtained above.



SUMMARY

The results of the examination of the goods were found that no any activity outside the common. The overall computer use to host gaming Flight Simulator only. Nor has any information source which directly indicates there any plans to eliminate MH370 found.