

6.4 FLIGHT SIMULATOR ANALYSIS

6.4.1 Flight Simulator X installation Information on MK26

From the analysis on the MK26 (the main hard-drive of the flight simulator), the installation information of the Flight Simulator X program is as follow:

No	Subject	Detail
1	Name	Flight Simulator X
2	Installation date	20/12/2013
3	Installation Location	C:\fsx19decl31
4	Publisher	Microsoft Gamee Studio
5	Version	10.0 60905

Table 3. *Flight Simulation X* installation on MK 26

6.4.2 Flight SimulatorX stored file analysis

From the Flight Simulator X gameplay that has been simulated, there were seven (7) user stored data that were automatically saved and generated in the user game application folder.

The data formats are shown in Table 4.

No	Data Format	Description
1	Logbook.Bin	Generated when user access to the application
2	FSSAVE	Generated when user save their gameplay
3	FLT	Generated when user save their gameplay
4	WX	Generated when user save their gameplay
5	PLN	Generated when user save their flight planner
6	CFG	Generated when user save their device configuration
7	SPB	Generated when user save their gameplay

Table 4: User stored data

For the analysis, all saved and generated files were analyzed. except the *.CFG files. The *.CFG files are irrelevant because it refers to the device configuration.

6.4.2.1 The Flight Simulator Saved Files In All Exhibits (MK22, MK23, MK24, MK25, MK26)

Flight simulator saved files in all exhibits (MK22, MK23, MK24, MK25 & MK26)

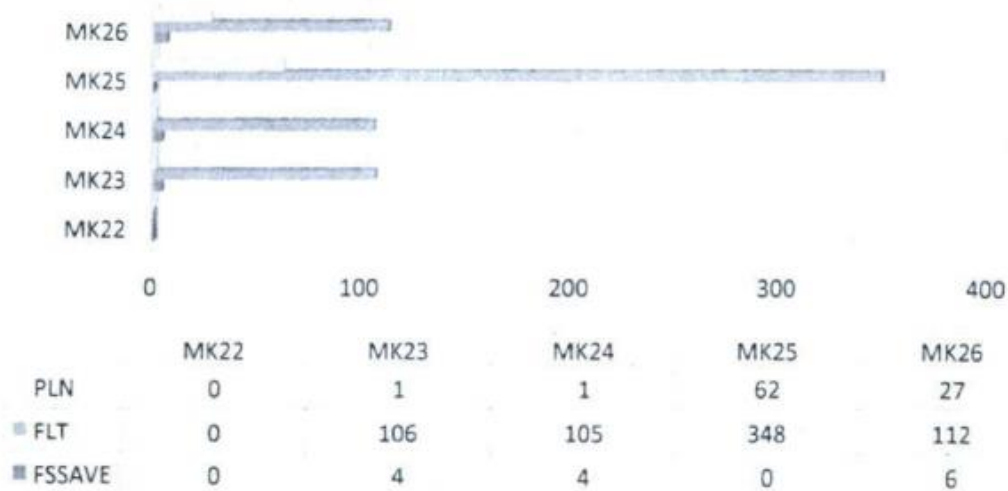


Figure 11. The numbers of *.FSSAVE, *.FLT and *.PLN found on all exhibits.

6.4.2.1 The Flight Simulator Crash Report of the Flight Simulator

On analyzing the MK26, the analysis found traces of where the flight simulator has experienced some application crashes. The crash, when investigated has caused by the Flight Simulator X application. The traces of this information are stored inside the exhibits Windows Event Viewer files. These files are.

- (a) Application.evtx
- (b) ACEEventLog.evtx

In total, four (4) application crash reports that are related to the Flight Simulator X application can be traced with Application Error. These crash reports all stated fsx.exe (The Flight SimulatorX executed file). which experienced the problem. Figure 12 shows the crash reports go found on the fsx.exe inside MK26.

Level	Date and Time	Source	Event ID	Task Category
Information	12/19/2013 1:06:54 PM	NET Runtime Optimizati...	1130	None
Application Error	1/23/2014 8:56:26 PM	Application Error	1000	Application Crashing Events
Application Error	1/23/2014 7:53:21 PM	Application Error	1000	Application Crashing Events
Application Error	1/23/2014 5:44:33 PM	Application Error	1000	Application Crashing Events
Information	12/19/2013 7:06:16 PM	AudioAPIControlService	3	None
Information	12/20/2013 6:42:49 AM	AudioAPIControlService	3	None
Information	1/23/2014 7:12:06 PM	AudioAPIControlService	3	None
Information	12/19/2013 7:07:58 PM	AudioAPIControlService	3	None

Log Name	Source	Level	Date and Time	Event ID	Task Category	Keywords	User	Computer	OpCode
Application	Application Error	Error	12/20/2013 6:42:49 AM	1000	Application Crashing Events	Classic	N/A	fs43dec13-PC	

```

Faulting application name: fs4.exe, version: 12.0.0.0, time stamp: 0a46e014
Faulting module name: uiautomationcore.dll, version: 7.0.0.0, time stamp: 0a46e014
Exception code: 0x60000005
Fault offset: 0a000e51a
Faulting process id: 0x7fc
Faulting application start time: 0a11c4e0f23ad409
Faulting application path: C:\fs43dec13\fs4.exe
Faulting module path: C:\Windows\system32\uiautomationcore.dll
Report ID: 773a4af-6062-11e7-9640-d171760b2a0c
  
```

Figure 12. The crash report

On examining the date of the crash, the analysis found the crash reports generated on these dates and times

- (a) 1/23/2014 5:44:33 PM
- (b) 1/23/2014 7:53:21 PM
- (c) 12/20/2013 6:42:49 PM
- (d) 1/23/2014 8:56:26 PM

Further investigation via Internet activity analysis of the MK26 shows that there are traces of activities that searching for the solutions to solve the problems. The following Figure 13 shows the screen capture of the activities on 20th December 2013 that shows during the time 2140 the Internet is being used to search for the Windows crashed solutions.

6.4.3.1 *Logbook.Bin* 20 Feb 2014 @ 11:07 am

Date	Time	Aircraft	From	To	Landings	Day	Night	Instr	Total
2/21/2014	12:54 AM	BOEING B738	WMKK		0	0.0	0.1	0.0	0.1

Details | Delete entry | Column subtotals: 0 | 0.0 | 0.1 | 0.0 | 0.1

Table 4: *Logbook.Bin* data table

The log data shows that the *Flight Simulator X* was played once on 21 February 2014. The log file was last accessed on 20 Feb 2014 at 11:07 am.

6.4.3.2 *Logbook.Bin* 01 Feb 2014 @ 02:28 am

Date	Time	Aircraft	From	To	Landings	Day	Night	Instr	Total
2/1/2014	2:49 PM	Douglas DC3	CYZF	CBXS	1	0.1	0.0	0.0	0.1
2/1/2014	2:45 PM	Douglas DC3	CYZF	CYZF	1	0.0	0.0	0.0	0.0
2/1/2014	2:48 PM	Douglas DC3	CYZF		4	0.3	0.0	0.1	0.3
2/1/2014	3:02 PM	Douglas DC3		CYZF	1	0.1	0.0	0.1	0.1

Column subtotals: 7 0.5 0.0 0.2 0.5

Table 5: *Logbook.Bin* data table

The log data shows that the Flight Simulator X was played four (4) times on 1 February 2014 from 2:45 pm until 3:02 pm.

The log file was last accessed on 01 Feb 2014 at 02:28 am.

6.4.3.3 Logbook.Bin 23 Jan 2014 @ 08:56 pm

Logbook entries									
Date	Time	Aircraft	From	To	Landings	Day	Night	Instr	Total
12/20/2013	11:29 AM	BOEING B738		WMKP	1	0.1	0.0	0.0	0.1
12/21/2013	11:29 AM	BOEING B738			0	0.0	0.0	0.0	0.0
12/21/2013	11:29 AM	BOEING B738		WMKP	2	0.3	0.0	0.0	0.3
12/21/2013	11:21 AM	BOEING B738	WMKP	WMKP	1	0.1	0.0	0.0	0.1
1/24/2014	3:16 PM	BOEING B77L	WMKK	WMKK	1	0.3	0.0	0.0	0.3
1/24/2014	3:14 PM	BOEING B77L	WMKK		0	0.2	0.0	0.0	0.2
1/24/2014	3:32 PM	BOEING B77L	WMKK		0	0.2	0.0	0.0	0.2
1/24/2014	3:19 PM	BOEING B77L	WMKK		0	0.1	0.0	0.0	0.1
1/24/2014	3:23 PM	BOEING B77L			0	0.0	0.0	0.0	0.0

| | Column subtotals: 5 1.2 0.0 0.0 1.2

Table 6: Logbook.Bin data table

The log data shows that the Flight SimulatorX was played nine (9) times
 The Flight Simulator X was played once on 20 December 2013 at 11:29 am.
 Three (3) times on 21 December 2013 from 11:21 until 11:29 am and five (5)
 times on 24 January 2014 from 3:14 pm until 3:32 pm.

The log was last accessed on 23 Jan 2014 at 08 56 pm.

6.4.4 Flight

6.4.4 Flight Simulator X deleted file analysis

From the simulation gameplay, the deleted files consist of *. FSSAVE.

*.FLT, *.WX and *.SPB file format.

The deleted files are as below:

No	File Name	Last Accessed	Simulation findings
1	"Previous flight" *.FSSAVE *.FLT	15/3/2014 @ 10.44pm	Simulation was successful. The saved gameplay consists of a new start game and contain irrelevant information on the flight plan.
2	"Previous flight" *.FSSAVE *.FLT *.WX	20/2/2014 @ 10.55am	Simulation is unsuccessful because the file was overwritten
3	"Previous flight" *.FSSAVE *.FLT *.WX	8/12/2013 @ 06.07pm	Simulation is unsuccessful because the file was overwritten
4	"Previous flight" *.FSSAVE *.FLT *.WX	11/12/2013 @ 10.02am	Simulation is unsuccessful because the file was overwritten
5	"Program generated temporary flight" *.FSSAVE *.FLT *.WX	20/2/2014 @ 11.06am	Simulation is unsuccessful because the file was overwritten
6	"Program generated temporary flight" *.FSSAVE *.FLT	8/12/2013 @ 06.49pm	Simulation is unsuccessful because the file was overwritten
	*.WX		

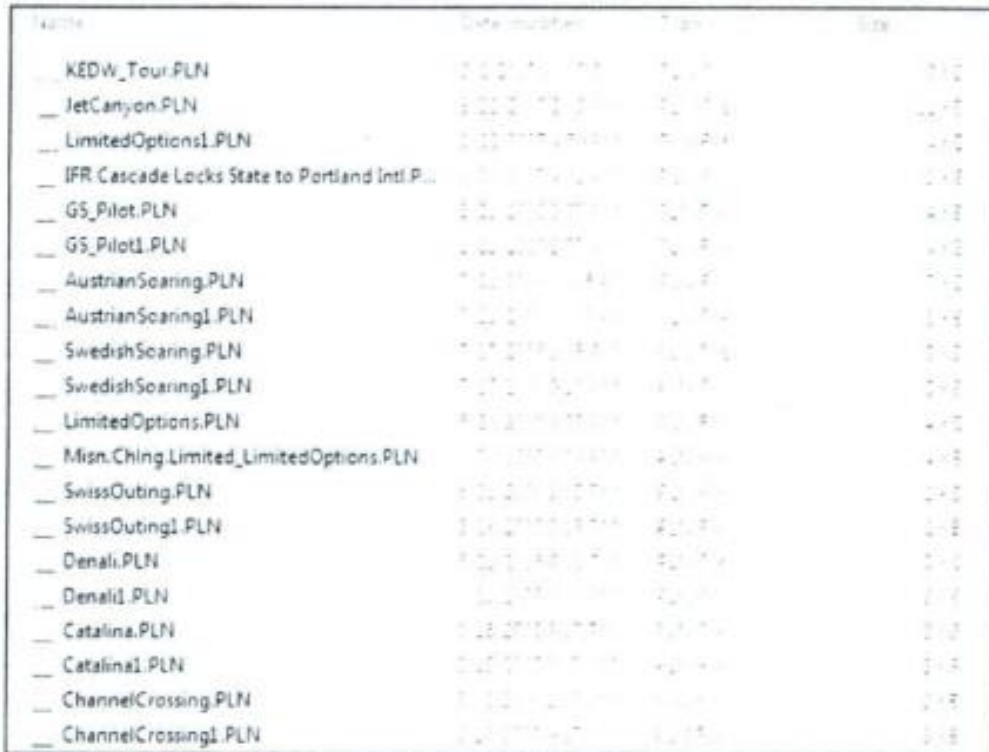
Table 7: Simulation gameplay results

6.4.5 Flight planner file analysis

The flight planner file is generated and stored as *.PLN format. This file is generated when user creates a flight plan in the simulator.

The analysis shows no relevant *.PLN file found on the exhibit. This is irrelevant because the fast modified timestamp recorded was in year 2006 and 2007.

The details are shown in the following screenshot.



Name	Date modified	Type	Size
— KEDW_Tour.PLN	11/22/2007 11:58 AM	File	2 KB
— JetCanyon.PLN	11/22/2007 11:58 AM	File	2 KB
— LimitedOptions1.PLN	11/22/2007 11:58 AM	File	2 KB
— IFR_Cascade Locks State to Portland Intl.PLN	11/22/2007 11:58 AM	File	2 KB
— GS_Pilot.PLN	11/22/2007 11:58 AM	File	2 KB
— GS_Pilot1.PLN	11/22/2007 11:58 AM	File	2 KB
— AustrianSoaring.PLN	11/22/2007 11:58 AM	File	2 KB
— AustrianSoaring1.PLN	11/22/2007 11:58 AM	File	2 KB
— SwedishSoaring.PLN	11/22/2007 11:58 AM	File	2 KB
— SwedishSoaring1.PLN	11/22/2007 11:58 AM	File	2 KB
— LimitedOptions.PLN	11/22/2007 11:58 AM	File	2 KB
— Misc.Ching.Limited_LimitedOptions.PLN	11/22/2007 11:58 AM	File	2 KB
— SwissOuting.PLN	11/22/2007 11:58 AM	File	2 KB
— SwissOuting1.PLN	11/22/2007 11:58 AM	File	2 KB
— Denali.PLN	11/22/2007 11:58 AM	File	2 KB
— Denali1.PLN	11/22/2007 11:58 AM	File	2 KB
— Catalina.PLN	11/22/2007 11:58 AM	File	2 KB
— Catalina1.PLN	11/22/2007 11:58 AM	File	2 KB
— ChannelCrossing.PLN	11/22/2007 11:58 AM	File	2 KB
— ChannelCrossing1.PLN	11/22/2007 11:58 AM	File	2 KB


Screenshot 1: Flight planner file found in the exhibit.






6.4.6 Flight Simulator Coordinates Analysis

The new objective of the investigation is to analyze seven (7) coordinates that can be found in the MK25 exhibit. All the referred seven coordinates are found located inside the exhibit's System Volume.

Information. These coordinates along with other flight information are found in consistent with the Flight Simulator *.FLT saved files. In the *.FLT the fast activity of the flight simulation progress are recorded. The saved information includes the last coordinates, the latitude, the plane's heading, bank, pitch and the fuel's volume.

In order to investigate the given the coordinates. a simulation of simulation flight planning was conducted. For that purpose, a simulator saved file is generated on a separate flight simulator, which is build for the case avionic simulation. The coordinate information along with other corresponding flight configuration is then replaced into the generated saved file. The created flight plan from the information is then viewed and screen-captured.

Coordinate 1		Lat: N003 24' 54.5139" Long: E100 53' 08.0655" Alt: +023246.66 Pitch: -4.9106726878513466 Bank: 0.034406561147416663 Head: -54.695636084553669
Coordinate 2		Lat: N005 06' 41.8671" Long: E098 35' 16.6071" Alt: +032245.59 Pitch: -3.4555031385607284 Bank: 0.013861149596148268 Head: -45.250100604877538

		
Coordinate 3		<p>Lat: N010 10' 59.2526"</p> <p>Long: E090 13' 28.2634"</p> <p>Alt: +040003.30</p> <p>Pitch: -4.2944037824614547</p> <p>Bank: 20.090691288853577</p> <p>Head: -104.53043838745208</p>
Coordinate 4		<p>Lat: S045 05' 06.8357"</p> <p>Long: E104 08' 43.9576"</p> <p>Alt: +037651.09</p> <p>Pitch: -1.0317193939326563</p> <p>Bank: -10.919122594496264</p> <p>Head: 178.22112415976278</p>
Coordinate 5		<p>Lat: S045 07' 38.5993"</p> <p>Long: E104 08' 28.9998"</p> <p>Alt: +003999.99</p> <p>Pitch: -5.8628661170360177</p> <p>Bank: -2.8745090090967582</p> <p>Head: -167.01121541228284</p>
Coordinate 6		<p>Lat: N002 44' 52.6561"</p> <p>Long: E101 43' 20.3843"</p> <p>Alt: +000070.00</p> <p>Pitch: 0.09999999922536331</p> <p>Bank: 0</p> <p>Head: -33.850522687426981</p>


Coordinate 7		Lat: N002 44' 52.6669" Long: E101 43' 20.3771" Alt: +000087.02 Pitch: 0.22114109021911346 Bank: 0.0037822773834368952 Head: -33.850552925641708
--------------	-----------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------

Table 8: Coordinate analysis results

6.4.7 The date and time of computer activity given by the investigation officer.

Based on the information given by the investigating officer, there is a hit on the keyword search from the exhibit (MK26). Below is the detail of the search hit.

```

01242337@Search@Machet
01242337@kust@use@
01242337@FL@age@
01242337@
01242337@ATC_Agent@Manager@
01242337@@Number@of@Agent@#
01242337@
01242337@ATC_Aircraft@Manager@
01242337@@Number@of@Aircraft@#
01242337@
01242337@ATC_Mess@ng@System@
01242337@@Agency@Node@
01242337@
01242337@Data@Time@Season@
01242337@@Season@=Winter@
01242337@@Year@=2014@
01242337@@Year@=2014@
01242337@@Hour@=0@
01242337@@Hour@=0@
01242337@@Hour@=0@
01242337@@Hour@=0@
01242337@
01242337@Panel@ 1@
01242337@@Screen@On@Coords@= 0, 0, 0, 1
01242337@@On@do@Coords@= 0, 0, 0, 1
01242337@@Is@do@=False@
01242337@@On@do@=False@
01242337@@Is@do@=False@
01242337@ID@=0@
01242337@@Is@do@=
01242337@
01242337@Panel@ 2@
01242337@@Screen@On@Coords@= 0, 0, 0, 1
01242337@@On@do@Coords@= 0, 0, 0, 1
01242337@@Is@do@=False@
01242337@@On@do@=False@
01242337@@Is@do@=False@
01242337@ID@=0@
01242337@@Is@do@=

```

Screenshot 2: The result of the search hit

Analysis on the FSX shows that there is a menu that can set the game to a desired season, date and time. Please refer to 5.3.2.4 for the details of the setting. After the setting was saved, the same pattern was found in the *.FLT files. Please refer to Screenshot 3 for the detail of the *.FLT content.



```
date:messeason
Range=Short
Altitude=0
Flags=0

[ATC_AgentManager]
NumberofAgents=0

[ATC_AircraftManager]
NumberofAircraft=0

[ATC_MessageSystem]
FrequencyNodes=0

[DateTimeSeason]
Season=Winter
Year=2014
Day=02
Hours=0
Minutes=54
Seconds=17

[Panel.1]
ScreenUniCoords=0, 0, 0, 0
WorldCoords=0, 0, 0, 0
Visible=False
Undocked=False
HiddenOn=False
m_u=
```

Screenshot 3: The content of the simulated *.FLT saved file.

To confirm the findings and to verify that all the coordinates given are coming from the *.FLT saved files, comparison analysis is carried out. For the analysis, the extracted information that contains the coordinates is compared with created saved files from the reconstructed flight. The comparison analysis shows that the extracted information is consistent with the *.FLT content Figure 12 shows the result.



Figure 13. Comparison analysis between extracted information with the saved files from the reconstructed flight simulator.