INDEPENDENT COMMISSION AGAINST CORRUPTION

STATEMENT IN THE MATTER OF: Operation AERO

PLACE: **ICAC office**

NAME: **Martin Frewen**

ADDRESS: **Level 7, 255 Elizabeth Street, Sydney NSW**

OCCUPATION: **Electronic Evidence Analyst**

DATE: **5 July 2019**

States: -

---

1. This statement made by me accurately sets out the evidence which I would be prepared, if necessary, to give in Court as a witness. The statement is true to the best of my knowledge and belief, and I make it knowing that, if it is tendered in evidence, I shall be liable to prosecution if I have wilfully stated in it anything which I know to be false or do not believe to be true.

2. I am 41 years of age. I have worked in the field of digital forensics since 2015 and have been working with ICAC in the capacity of Electronic Evidence Analyst since January 2018. I hold the following certifications:
   - IACIS[1] Certified Forensic Computer Examiner (CFCE)
   - IACIS Certified Mobile Device Examiner (CMDE)
   - Cellebrite Certified Physical Analyst (CCPA)
   - Nuix eDiscovery Specialist

[1] IACIS - International Association for Computer Investigative Specialists

Signature _____ Witness _____

STATEMENT IN THE MATTER OF: Operation AERO
NAME: Martin Frewen

3. On 23 August 2018, ICAC Investigator Phil Vickery submitted a request to the ICAC digital forensics team for analysis of the following property items to determine if and when they had been wiped or reinstalled with the Microsoft Windows operating system:

Property Number	Description
E18-0093-AS-2-14-PR-0001	Silver Toshiba Satellite P50t-B laptop S/N: 8E075197S
E18-0093-AS-2-14-PR-0002	HP Pavilion All-in-one PC Model: 24 – b015a S/N: 8CC63512T3

4. System generated files on computers running the Microsoft Windows 10 Operating System hold information which can be used to determine usage and installation details for that computer. These system files include the Windows registry which is a database of settings for the Windows system, users, and software applications residing on it.

5. The specific location of the information relating to the version of a Microsoft Windows 10 based computer is at the following registry key: **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProductName.** This registry key was located on both property items, and the value of this key on both was "Windows 10 Home". This can infer that both property items had Windows 10 Home edition installed when provided to ICAC.

Signature _____ Witness _____

6. The specific location of the information relating to the installation date of a Microsoft Windows 10 based computer is at the following registry key:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\InstallDate

7. It should be noted that the "InstallDate" registry value can be updated when a major Windows software update is installed and therefore cannot be used in isolation to determine the date the Windows system was installed.

8. Property number E18-0093-AS-2-14-PR-0001 contains a hard drive divided into 9 partitions (storage areas). Two storage partitions are for "user data", and seven other smaller partitions used for system recovery, system booting, or diagnostics.

9. Of the two "user data" storage partitions, one was used for the Microsoft Windows 10 Home edition operating system. This partition contains registry keys including the "InstallDate" entry, and the install date recorded is 12 May 2018 6:35:11pm.

10. Other system generated files can add more confidence that the value represented in the "InstallDate" registry key accurately reflects the install date/time. The "Master File Table" (MFT) is a system generated file which is created at the time the storage partition is created, and records an entry for each file on the storage partition. The $Volume entry in the MFT is the third entry in the MFT and shows

Signature _____ Witness _____

the creation time is 12 May 2018 at 6:11:14pm. This value would not be updated if a major Windows update was applied. The difference in time between the $Volume record and the "InstallDate" registry key value is consistent with what is the expected length of time to perform the Windows installation.

11. The other user storage partition contained files which predate the install date determined from the first user storage partition. The earliest file residing on this partition was a video file titled "GuangZhou/20170625晚会A.mp4". This file was created on the storage partition on 21 October 2017 at 1:21pm. The $MFT record entry for $Volume on that storage partition shows the creation time is at 1:27:51pm on 17 September 2017.

12. One possible explanation for the date discrepancies between the two user partitions is that a Windows installation had occurred on 17 September 2017 which resulted in creating two user partitions. On 12 May 2018 the Windows installation process was run again to install across the same storage area previously occupied by original Windows installation. This would overwrite data on that partition without affecting the other partitions.

13. Property number E18-0093-AS-2-14-PR-0002 was running the Microsoft Windows 10 Home edition operating system, and the install date was 8 July 2018 9:46:52pm. The MFT record entry for $Volume shows the creation time is 8 July

Signature _____ Witness _____

2018 at 11:07:30pm. This value would not be updated if a major Windows update was applied as it would require a format of the partition to update this. One possible explanation for how the partition creation time is later than the Windows install time is that the date/time on the computer was not accurate at the start of the installation, and was corrected during the installation process.

14. It is not possible to determine the accuracy of the date/time setting on the property items at the time the Microsoft Windows operating system was installed.

15. System log files show the last use of this Windows system was on 9 July 2018 at 9:36:25am. This is supported by the value of the following registry key **HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Windows\ShutdownTime**, which provides the last shutdown time as 9 July 2018 at 9:36:31am which is less than one day after it was installed with the Windows operating system.

16. Information from Hewlett Packard indicate the warranty for this computer expired on 15 May 2018. The minimum warranty period for a new computer system provided by Hewlett Packard is one year. It is possible that the computer had been used during the course of the warranty period including 2017 up to the install date of 8 July 2018. Applying forensic data recovery methods against the same storage partition as the current install could add weight to this hypothesis, should new files be identified.

Signature _____ Witness _____