Statement in the matter of Operation COVINA

Name	Peter John REID
Occupation	Senior Digital Forensic Examiner
Date	28/07/2021

STATES:

1. This statement made by me accurately sets out the evidence that 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 will be liable to prosecution if I have wilfully stated in it anything that I know to be false or do not believe to be true.

2. I acknowledge having read ACT Court Procedures Rules 2006, Schedule 1, being the "Expert witness code of conduct", and fully agree to abide by its contents, both in relation to this statement and any subsequent evidence I present before the court.

3. I declare that I have made all inquiries on matters relevant to my area of expertise that I believe desirable and appropriate, and to the best of my knowledge, no matter of significance that is relevant has been withheld from the court.

4. My full name is Peter John REID. I am a Senior Digital Forensic Examiner with the Australian Federal Police (AFP) located at the AFP Forensic Facility in Majura in the Australian Capital Territory (ACT).

5. I have been involved professionally in the Information Technology (IT) field since 1980 holding positions in hardware and software development and IT infrastructure design and deployment.

6. I have been involved in the forensic examination of electronic evidence since August 2010.

7. My duties as a Senior Digital Forensic Examiner include the provision of assistance to the AFP and external agencies with the identification, preservation, examination, analysis reporting of computers, mobile phones, smartphones, communications equipment

storage media, as well as the installation, maintenance and development of equipment and software used to conduct forensic examinations.

8. I hold a Graduate Diploma of Digital Forensics and a Graduate Certificate of Computer Security, both obtained from Edith Cowan University in Western Australia.

9. I also hold a number of industry qualifications and have undertaken industry based training courses in digital forensics.

10. I am currently certified as a Computer Forensic Analyst (GCFA), a Network Forensic Analyst (GNFA) and hold the Advanced Smartphone Forensics Certification (GASF) awarded by the Global Information Assurance Certification (GIAC).

11. I have completed computer forensic industry based training courses in X-Ways Software Technology's X–Ways Forensics, Guidance Software's EnCase software, SANS FOR508: Advanced Digital Forensics, Incident Response and Threat Hunting, SANS FOR572: Advanced Network Forensics and Analysis and SANS FOR585: Smartphone Forensic Analysis In-Depth.

12. In addition I have completed forensic training courses in mobile electronic devices including Micro Systemation's .XRY and hold the following certifications awarded by Cellebrite, CUFM: Certified UFED (Universal Forensic Extraction Device) Field Manager, CUFO: Certified UFED Field Operator, CASA: Certified Advanced Smartphone Analysis, CCOM: Cellebrite Certified Operations Manager, CCPA: Cellebrite Certified Physical Analyst

13. I have previously testified in the ACT Supreme Court on the results of my analysis of digital evidence.

14. On 15 March 2021 about 09:30 am, I attended the Belconnen Police Station in the ACT and met with Detective Leading Senior Constable (D/LSC) Trent MADDERS (AFP10857) and Senior Constable (SC) Emma FRIZZELL (AFP12896) in order to extract the contents of a mobile phone.

15. About 10:21 am, that same date, I was informed by D/LSC MADDERS that I was no longer required as the phone was unable to be provided by the owner that day.

16. On 21 April 2021, AFP Seizure 3624845/001 was submitted for examination in relation to Police Real-Time Online Management Information System (PROMIS) case 6381473.

17. About 4:10 pm, I commenced an examination of AFP Seizure 3624845/001 which was identified as an Apple XS Max iPhone, model A2101, bearing IMEI[1] 357299099071224. This phone will now be referred to as '*iPhone Xs Max – LEHRMANN'* in this statement.

18. My examination comprised of a physical identification and examination of the hardware and internal components, where possible, forensic acquisition of all accessible data held on the items when possible, a verification of the integrity of the acquired data and the production of electronic case files for each seized item. These examinations were recorded through contemporaneous notes, digital photographs and report logs from the verified forensic examination tools utilised.

19. On 23 April 2021, a copy of the data extracted from the '*iPhone Xs Max – LEHRMANN'* was made available for review.

20. On 26 May 2021 about 09:30 am, I attended the Belconnen Police Station in the ACT and met with D/LSC MADDERS and SC FRIZZELL.

21. About 09:40 am I was handed a mobile phone by D/LSC MADDERS I now believe to belong to a person I was introduced to as Ms Brittany HIGGINS.

22. About that same time I sighted a consent form allowing me to perform an extraction of the Apple iPhone.

23. I moved the iPhone to an adjacent interview room to commence my examination and an extraction.

24. The phone was identified as an Apple iPhone Xs Max, model A2097, bearing IMEI 357224094849978. This phone will now be referred to as '*iPhone Xs Max – HIGGINS'*.

25. About 09:58 am, I commenced an extraction of the '*iPhone Xs Max – HIGGINS'*.

26. About 12:08 pm, I handed the phone back to Ms HIGGINS.

27. About 1:36 pm, I created a verified copy of the extraction.

28. On 27 May 2021, I made the contents of the '*iPhone Xs Max – HIGGINS'* available for review.

29. On 22 July 2021, about 10:00 am, I attended the Winchester Police Complex in the ACT and met with SC FRIZZELL.

[1] IMEI – International Mobile Equipment Identity

.....
Initials

30. About 10:15 am, I was handed AFP Seizures 3632871/001 and 3632871/002.

31. AFP Seizures 3632871/001 is a black Apple iPhone.

32. AFP Seizures 3632871/002 is a black Apple iPhone contained in a case bearing the initials "BMH".

33. About 11:05 am, I commenced examinations of both aforementioned seizures.

34. I was unable to extract the contents of either seizure as the PIN numbers provided were unsuccessful in unlocking either device at that time. Further unlock codes were available but were not attempted due to a wait time required by one seizure.

35. About 12:10 pm, I had a conversation with SC FRIZZELL and, as a result of that conversation, I returned to the AFP Forensic Facility at Majura in the ACT, in possession of both seizures.

36. About 1:59 pm, I continued my examination of AFP Seizures 3632871/001 and 3632871/002.

37. About 4:00 pm that same date, none of the provided unlock codes were unsuccessful. I then suspended my examinations.

38. On 26 July 2021, D/SLC MADDERS informed me that he had completed his review of the two phones identified as '*iPhone Xs Max – LEHRMANN'* and '*iPhone Xs Max – HIGGINS'*.

39. About 1:31 pm I received an email from SC FRIZZELL requesting that I download two (2) images of interest from an iCloud account. The credentials for the account were provided in the email.

40. About 4:10 pm I attempted to login to the iCloud account, however it required two factor authentication which prevented me from accessing the account at that time.

41. As a result of D/LSC MADDERS's review of the phone referred to as '*iPhone Xs Max – LEHRMANN',* I created copies of;
    - Four (4) chat conversations
        - Titled "*Identified Chat 1 – BL.pdf"* to *"Identified Chat 4 – BL.pdf" (respectively)*
        - Located in folders "*Identified Chat 1*" to "*Identified Chat 4*" *(respectively)*
    - Three (3) email items
        - Titled "*Identified Email 1 – BL.pdf"* to *"Identified Email 3 – BL.pdf" (respectively)*
        - Located in folders "Identified Email 1" to "Identified Email 3" (respectively)

.....
Initials

- An Excel spreadsheet *'iPhone Xs Max – LEHRMANN - Identified Chat Items of Interest.xlsx'*
- An Excel spreadsheet *'iPhone Xs Max – LEHRMANN - Identified Email Items of Interest.xlsx'*

42. As a result of D/LSC MADDERS's review of the phone referred to as *'iPhone Xs Max – HIGGINS,* I created copies of;
    - Sixteen (16) chat conversations
        - Titled "*Identified Chat 1 – BH.pdf"* to *"Identified Chat 6 – BH.pdf" (respectively)*
        - Located in folders "*Identified Chat 1*" to "*Identified Chat* 6" *(respectively)*
    - An Excel spreadsheet *'iPhone Xs Max – HIGGINS - Identified Chat Items of Interest.xlsx'*

43. On 27 July 2021, I created copies of the aforementioned chats, emails and spreadsheets on a digital versatile disc (DVD), which is attached to this statement as **APPENDIX A.**

44. About 11:15 am, I received an email from SC FRIZZELL authorising me to download files of interest from a Google account.

45. About 12:10 I accessed the iCloud account and located the two files of interest referenced in SC FRIZZELL's email.

46. I downloaded the two (2) files and, at the request of SC FRIZZELL, reviewed the metadata contained within each file which are images. From the information available to me at the time, I was unable to ascertain the date and time the images were taken.

47. About 12:20 pm, SC FRIZZELL requested I download all available data from Google Drive File Storage associated with the Google account.

48. About 3:00 pm the download of the Google Drive had completed.

49. I read this statement before I signed it.

_____ *(Signature)*

Peter John REID
AFP20609
Majura Forensic Facility
28/07/2021