**PeCan+ 2022 CTF – Advanced Question- Digital Forensic**

Australian Federal Police has been investigating drug trafficking across Australia and Jacky is one of the mastermind criminals behind this criminal syndicate. Police tried to locate him for a long time and after more than 6 months of hard-working police were able to track down Jacky’s drug operation warehouse in Melbourne. When the police arrived for the raid Jacky rushed to his office avoiding police warnings and tried to burn some documents near his computer. By the time the police caught him most parts of the document were burnt. However, they managed to recover some parts of the document. Police seized his phone and computer as evidence along with the burnt document and handed them over to the forensic team.

**Exhibit A – Burnt document**



6 114 105 115 98 97 110 101 32 36 53 48 44 48 48 48 32 65 99 99

Officer 1 – Were you able to crack the code on the burnt document?

Officer 2 – Yeah, I did. It says xxxxxxxxx. But still, some details are missing.

Officer 1 – Hmmm, we have his hard drive, right?? Why don’t you give it a go?

Answer

Decrypted line (ASCII encoding) - risbane $50,000 Acc 🡪 This is a Bank Account number in Brisbane and $50,000 had been transferred to this account by a foreign account number. Then a hint is given to search the hard drive and they can use Brisbane as the keyword to search. In the hard drive, there are text files naming Brisbane, Melbourne, Adelaide and Perth. They seem to be empty but when examining the file details, they can find that files hold some storage capacity on the hard drive. Information regarding this criminal syndicate is hidden in the slack space/unallocated space. Students can. Find it using Forensic analysis tools such as DiskView, WinHex, and Hex Workshop.