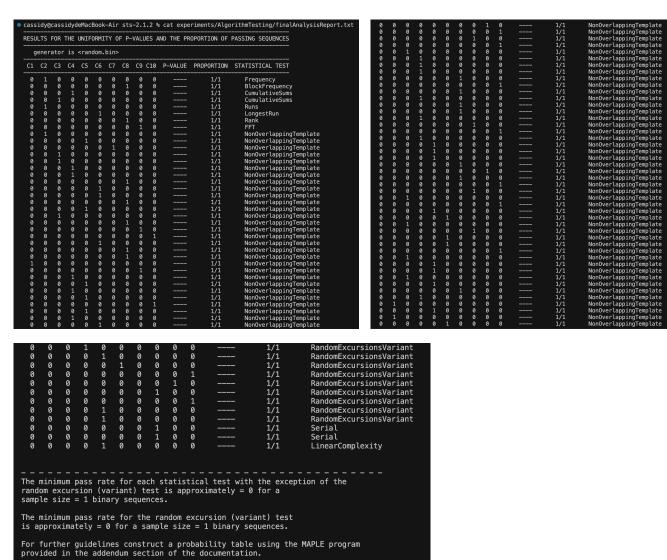
## Cryptography Engineering Quiz.5

a) Write a Python/C++ program to generate 1M bytes of cryptographically secure random numbers. -> import secrets

```
● cassidy@cassidydeMacBook-Air sts-2.1.2 % /usr/local/bin/python3.12 /Users/cassidy/Desktop/1_密碼工程/Quiz05/RNG.py
```

- b) Run the NISTSP800-22 statistical test on your 1M bytes of binary cryptographically secure random numbers and analyze the test results to identify any deviations from the expected statistical properties of random numbers.
  - 1. The progress of running the statistical test

## 2. Capture the result (I only took screenshots of some of it.)



It passed all the static tests, meaning it conforms to every expected statistical property of random numbers. This implies that in the NIST SP800–22 statistical tests, the random number generator passed all tests, demonstrating that the generated random number sequences closely match ideal randomness and perform well across various statistical tests without significant biases or flaws. Therefore, we can confidently assert that the random number sequences generated by this generator possess cryptographic security and can be applied in secure applications requiring high randomness.