

110年公務人員特種考試警察人員、一般警察人員、
國家安全局國家安全情報人員考試及110年特種考試
交通事業鐵路人員、退除役軍人轉任公務人員考試試題

考試別：警察人員考試
等 別：三等考試
類科組別：警察資訊管理人員
科 目：數位鑑識執法
考試時間：2 小時

座號：_____

※注意：(一)禁止使用電子計算器。

(二)不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。

(三)本科目除專門名詞或數理公式外，應使用本國文字作答。

- 一、反鑑識(anti-forensic)定義為何？(7分)反鑑識有四個目的為何？(8分)
反鑑識手法有那五種？(10分)
- 二、何謂惡意程式(malware)的定義？(7分)惡意程式鑑識分析分成那兩種？(10分)請列舉四種惡意程式鑑識工具。(8分)
- 三、如何調查 Google 雲端硬碟服務，請說明可以使用那些數位鑑識工具？(13分)對映到那些數位跡證？(12分)
- 四、請用四向連接理論(4-way linkage theory)和羅卡交換原理(locard's exchange principle)，先繪示意圖(11分)，再配合圖形說明證據對於破案的功用。(14分)