

100年公務人員特種考試一般警察人員考試、
100年公務人員特種考試警察人員考試及 代號：50960
100年特種考試交通事業鐵路人員考試試題

全一頁

等 別：三等警察人員考試

類 科：警察資訊管理人員

科 目：電腦犯罪偵查

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。

- 一、請說明何謂數位證據 (Digital Evidence) ? (10分) 數位證據有何特性? (10分)
數位證據與一般實體證據有何差異? (5分)
- 二、藉由犯罪現場跡證的評估，以分析犯罪者的特徵 (Characteristics)，乃犯罪剖繪 (Criminal Profiling) 的重點工作之一。請以 Unix 作業系統入侵的偵查為例，說明如何從被入侵的系統，蒐集數位跡證及分析入侵者的特徵。(25分)
- 三、計算機檔案系統中的資料，可以分為檔案系統類別 (File System Category)、檔案名稱類別 (File Name Category)、詮釋資料類別 (Metadata Category)、內容類別 (Content Category) 及應用系統類別 (Application Category)。請分別說明其意義與偵查價值。(每一資料類別5分，共25分)
- 四、請說明查緝電腦犯罪案件時，在執行電腦搜索應遵守與注意事項為何? 試依據相關法律規範與作業規定說明之。(25分)