103年公務人員特種考試警察人員考試
103年公務人員特種考試一般警察人員考試　　代號：50970　全一頁
103年特種考試交通事業鐵路人員考試試題

等　　別：三等警察人員考試
類　　科：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：㈠禁止使用電子計算器。
㈡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、請試述下列數位證據相關名詞之意涵：（每小題 5 分，共 25 分）
㈠ BitLocker
㈡ Dynamic Link Library
㈢ WinPcap
㈣ MD5
㈤ SQLite

二、㈠數位多媒體鑑識有兩個主要任務：防偽鑑定及來源鑑定，請說明數位音訊鑑識內容及方法。（15 分）
㈡在雲端硬碟服務鑑識方面，請以 Google Drive 為例，任舉四種操作模式下，說明會留下那些殘餘數據在用戶端設備上。（10 分）

三、㈠ ISO/IEC 27037 是 ISO 國際標準組織針對數位證據識別、蒐集、擷取和保存所訂定之參考指南，目前雲端安全聯盟的事件管理與鑑識工作小組發布了「Mapping the forensic standard ISO/IEC 27037 to Cloud Computing」，請說明在數位證據處理方面，ISO/IEC 27037 如何映對到雲端鑑識。（15 分）
㈡社群網站的使用越來越普及，數位鑑識面臨了新的問題與挑戰，請以 Facebook 為例，說明社群網站數位證據的特性及鑑識的方法。（10 分）

四、㈠數位多媒體鑑識有兩個主要任務：防偽鑑定及來源鑑定，請說明數位影像鑑識內容及方法。（15 分）
㈡請任舉四種 Web proxy，並說明如何偵查 Web proxy 之數位證據。（10 分）