102年公務人員特種考試警察人員考試、
102年公務人員特種考試一般警察人員考試及　代號：51070　全一頁
102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、何謂數位證據之同一性（Identity）？其與證據能力及證明力有何關聯性？另數位證據之證據方法有那些？請舉例詳細說明。（25分）

二、由於網際網路及各種通訊產業（如 Skype）的發達，使得犯罪不斷翻新；傳統電話詐欺也由於網路電話 VoIP（Voice Over Internet Protocol）的發展，使得撥打詐騙電話成本大幅降低及發生數量增加；且 VoIP 比傳統電話更難以查出犯罪源頭，請說明 VoIP 網路電話詐欺犯罪之類型、通訊管道、鑑識程序及犯罪組織結構等？且統合繪出 VoIP 網路電話詐欺犯罪流程及偵查鑑識流程？並說明如何運用犯罪偵查理論結合到 VoIP 網路電話詐欺犯罪偵辦機制。（25分）

三、「易揮發證據」是指當主機重新啟動時或正常使用下將會消失/被覆蓋/改變之資料，如記憶體載入內容或網路狀態等資訊即屬此類。請說明於 Windows 中之「確認系統時間」、「目前運行中程序」、「目前開啟檔案」、「與何主機（Host or IP address）相關」、「目前登入使用者」及「目前開啟連結與網路狀態」等項目為何為「易揮發證據」？（30分）

四、請按照 ISO/IEC 27037 的定義，列出處理數位證據（Digital Evidence）的 4 個主要步驟，並請略為說明之。（20分）