代號：50870
頁次：1－1

113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及移民行政人員考試試題

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：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。
㈢本科目除專門名詞或數理公式外，應使用本國文字作答。

一、ISO/IEC 27037 為一國際共通標準，該標準所提出的數位證據處理程序分成四個階段。請說明此四個階段主要的工作內容。（25 分）

二、手機取證的方式有分為邏輯提取（Logical Extraction）、檔案系統提取（File System Extraction）以及實體提取（Physical Extraction），請說明三種提取方式差異。而這三種提取方式有一種目前已知道在新型的手機上實務上不可行，請說明其原因。（25 分）

三、美國國家標準技術局（NIST）根據行動裝置鑑識提出其標準流程，請說明 NIST 提出的標準流程，根據這些流程列出一項這流程當中可能會用到的軟硬體工具。（25 分）

四、Windows 的 Event Log 為數位鑑識中尋找證據的重要來源之一，請舉出三種你所知道的 Event Log 以及其 Event ID，並請說明該 Log 代表的意義以及如何用來偵查可能的犯罪行為。（25 分）