代號：50860
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：電腦犯罪偵查
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、為評估系統遭受攻擊所受到的影響，多採用 CIA triad（資安鐵三角）方式評估受攻擊所遭受的衝擊程度。請說明何謂 CIA？若網站伺服器遭受 SQL 注入（SQL injection）攻擊，試以 CIA 說明其遭受到的影響，並說明 SQL 注入攻擊之原理，以及如何防範此類之攻擊。（25 分）

二、許多組織與企業遭受勒索軟體攻擊，被要求支付大量贖金。請說明勒索軟體攻擊原理，並說明其加密檔案之原理與技術、和如何偵查與分析此類攻擊事件。（25 分）

三、警察機關執行資訊數位化行之有年，因此累積大量犯罪資料；另一方面，在電腦犯罪案件蒐證中也收集到大量的數位證據。警調單位為追查與蒐集電腦犯罪相關資訊，可能會利用公開情資 OSINT（Open Source Intelligence），協助偵查。請說明何謂公開情資，並舉 2 項公開情資應用案例，說明公開情資如何協助偵查電腦犯罪。（25 分）

四、惡意軟體分析乃偵查電腦犯罪案件之重要步驟之一，請說明惡意軟體之類型與傳播方式，並舉例說明之。（25 分）

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）

代號：50830
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：警政資訊管理與應用
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本科目得以本國文字或英文作答。

一、路口監視器影像的比對可以利用人工智慧技術自動比對來取代人力，請說明影響人工智慧比對正確性的關鍵因素。（10 分）如果你來開發此項人工智慧系統，請說明所使用的人工智慧平台與工具、人工智慧模型、資料集如何收集、註解、訓練、測試與建置過程。（15 分）

二、請說明目前警政資訊系統對於民眾的個資在對內部及對外部的保護措施及相關規範。（10 分）並提出如何精進目前民眾個資保護機制之警政作業程序、技術細節及系統架構。（15 分）

三、網路詐騙犯罪常以虛擬貨幣作為支付工具，請說明目前常見的虛擬貨幣支付流程及現行警政系統的偵查機制。（10 分）就你認為，如何加強反制機制來加強防堵，請從警政作業程序、法規及資通訊技術來加以說明。（15 分）

四、請說明現行勤務指揮工作可以透過那些資通訊技術來加以輔助以提升效率。（10 分）如果讓你來開發一個提升勤務指揮工作效率的系統，請說明其功能與目標、系統架構、資料流程及相關演算法。（15 分）