106年公務人員特種考試司法人員、法務部調查局調查人員、國家安全局國家安全情報人員、海岸巡防人員及移民行政人員考試試題　代號：10960　全一頁

考 試 別：司法人員
等　　別：三等考試
類 科 組：檢察事務官電子資訊組
科　　目：資通安全
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、為了確保數位證據（Digital Evidence）的完整性及有效性，請說明執行數位鑑識（Digital Forensics）的作業流程及相關內容。（25 分）

二、依部署環境及系統架構的不同，入侵偵測系統（Intrusion Detection System, IDS）可概分為主機端入侵偵測系統（Host IDS）及網路端入侵偵測系統（Network IDS）兩種類型。請分別說明這兩種類型之入侵偵測系統的運作原理及其優缺點。（25 分）

三、若網站資訊系統設計不當，將可能遭受 SQL 資料隱碼攻擊（SQL Injection）。請說明造成 SQL 資料隱碼攻擊的原因及其解決方案。（25 分）

四、針對資料或系統的資安威脅，可歸納成四種類型：中斷（interruption），亦即阻斷系統連結或服務；截聽（interception），亦即側錄傳輸資料；更改（modification），亦即修改傳輸資料或執行程式；偽冒（fabrication），亦即假冒通信個體名義發送偽造訊息。請分別說明防制這四種資安威脅的實務作法。（25 分）