代號：41560
頁次：1－1

113年公務人員特種考試司法人員、法務部調查局調查人員及海岸巡防人員考試試題

考 試 別：調查人員
等　　別：三等考試
類 科 組：資訊科學組
科　　目：資訊安全實務
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、請回答下列有關數位鑑識之問題：

㈠在數位鑑識（Digital Forensics）標準作業程序中，何謂資料採集（Data Acquisition）？（15分）

㈡在某次數位鑑識調查中，資安事件調查員成功從犯罪現場獲取了數位證據，調查人員現在必須保存這些數位證據以便進一步分析。為了確保數位證據的完整性，調查人員應優先考慮採取那些行動？（10分）

二、請回答下列問題：

㈠資安調查人員正在對從受害系統取得的某惡意程式之可執行檔進行分析，該調查人員是否可以在無原始程式碼的情況下對可執行檔進行逆向工程？如果是，其步驟為何？（15分）

㈡說明軟體逆向工程（Software Reverse Engineering）之目的為何？（10分）

三、請回答下列問題：

㈠在網路安全攻擊中，何謂 Session Hijacking Attack？何謂 IP Spoofing？以上兩者之關係為何？（15分）

㈡說明什麼是 sniffing？其目的為何？（10分）

四、請回答下列關於資訊安全之問題：

㈠攻擊者不斷尋找利用傳送訊息進行破壞的新威脅。請說明 phishing、vishing 與 smishing 之差異。（15分）

㈡簡述何謂 S/MIME（Secure/Multipurpose Internet Mail Extensions）？（10分）