代號：50970
頁次：1－1

109年公務人員特種考試警察人員、一般警察人員考試及109年特種考試交通事業鐵路人員考試試題

考 試 別：警察人員考試
等　　別：三等考試
類 科 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、在行動通訊普及的今天，可能會有人利用手機等行動通訊設備在社群媒體（如在 LINE）上進行犯罪行為。
㈠請依攻擊方式對社群媒體犯罪作分類，並舉例說明之。（5 分）
㈡請問偵查社群媒體犯罪的證據，必須從那裡取得？蒐證的範圍又應該包括那些？（10 分）
㈢何謂社群媒體快照（Social Snapshot）的數位取證方法？採用這種資料收集方法的理由為何？（10 分）

二、㈠一個良好的數位鑑識軟體應該具有那些特色？（10 分）
㈡鑑識軟體 FTK 的主要工具有那些？請說明其功用。（15 分）

三、㈠要作網路即時資料的鑑識就必須進行封包分析。請問鑑識時應檢視那些重點？（10 分）
㈡在網路攻擊事件中，可能有某機構（如銀行）電腦或行動通訊設備被植入惡意程式，作為竊取機敏資料的手段。請說明如何佈署蒐證環境以便即時分析網路封包來偵查此類攻擊事件；並繪圖說明此類攻擊行為的即時資料分析流程。（15 分）

四、㈠為什麼網路位址在數位鑑識中是很重要的衡量因素？（5 分）
㈡網際網路的位址（IP Address）大致可分為那幾類？對每一類在數位取證時應注意那些要點？（20 分）