代號：38480
頁次：1－1

109年公務人員高等考試三級考試試題

類　　科：資訊處理
科　　目：資訊管理與資通安全
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、電腦設備和網際網路已成為新興的犯罪工具或媒介，因此，面臨訴訟爭議時，常會涉及數位證據的運用：
㈠何謂數位鑑識？（10分）
㈡何謂證據同一性？（10分）
㈢當第一線人員取證檔案做證據時，請列出什麼情境，該檔案是有證據能力的；而什麼情境，該檔案是沒有證據能力的？（5分）

二、電腦系統或網路設備，或多或少都有弱點存在，為防止駭客進行惡意入侵，系統應有相對的防禦工具：
㈠何謂網路型入侵偵測系統？（5分）
㈡說明網路型入侵偵測系統，其部署位置及運作狀況（可以示意圖表示），並陳述其優缺點。（10分）
㈢當資訊人員遇到攻擊封包或病毒，於企業內迅速擴散時，未更新的主機不斷的散布攻擊封包，資訊人員必須與時間競爭，其處理方法為何？（10分）

三、何謂儲存型跨站攻擊（Stored Cross-Site Scripting（XSS））/反射型跨站攻擊（Reflected Cross-Site Scripting（XSS））？依攻擊者（Attacker）、目標網站（Website）、受害者（User）分別說明出其關係（可以示意圖表示），並描述其攻擊步驟。（25分）

四、專家系統（Expert System）是一種在特定領域內，具有專家水平解決問題能力的程式系統：
㈠專家系統主要由6個部分構成，請說明該6個部分之關係（可以示意圖表示），並描述各部分之功能。（20分）
㈡說明專家系統和人工智慧的關係。（5分）