107年公務人員特種考試警察人員、一般警察人員考試及
107年特種考試交通事業鐵路人員考試試題　　代號：50950　　全一頁

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：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、數位證據（Digital Evidence）之意義為何與有何特性？（5分）如何分類並請繪圖說明。（10分）在犯罪偵查過程中，不論是傳統犯罪或電腦網路犯罪常見用來證明待證事實之數位證據有那些？（10分）

二、資通安全（資安）是一種風險管理的概念，需要控制可能產生的資安風險，需透過資安預防（Prevention）、資安防護（Protection）、證據保全（Preservation）與專業鑑識（Presentation）等四大構面（4P's Model），落實以風險管理為核心的資安防禦策略，請詳細說明這四大構面內容及控制機制，並繪圖說明之。（25分）

三、請試述下列名詞之意涵：（每小題5分，共25分）
㈠ Legal Hold
㈡ Ransomware Worm
㈢ APT（Advanced Persistent Threat）
㈣ Cybercrime
㈤ Distributed Denial of Service Attack

四、何謂網路詐欺犯罪模式及偵查模式？（5分）其常見網路詐欺型態及手法為何？（5分）又警察人員如何偵辦此網路詐欺犯罪？（5分）另如何針對網路詐欺發展一有效整合之偵查機制，請詳細舉例說明，並繪圖之。（10分）