代號：50830
頁次：1－1

114年公務人員特種考試警察人員、一般警察人員、國家安全局國家安全情報人員、移民行政人員考試及114年特種考試退除役軍人轉任公務人員考試試題

考 試 別：警察人員考試
等　　別：三等考試
類科組別：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、請論述及比較網路犯罪偵查與傳統犯罪偵查在偵查目標、證據形式和方法上的主要異同。（10 分）並請具體說明傳統偵查方法（如訪談、情資蒐集、臥底）如何在網路犯罪偵查的背景下進行應用和調整？（15 分）

二、請說明犯罪偵查及知識工程化的基本原則及偵查技術有那些？（10 分）另欲使犯罪偵查工作走向知識化、科學化、系統化及合理化的道路，應具備下列五大階段（鑑定化階段、概念化階段、正規化階段、實作及測試階段、證實階段），請詳細舉例說明（如第一銀行 ATM 盜領案），並繪圖說明之。（15 分）

三、數位鑑識在「重建數位犯罪事件的發生過程」或「還原數位犯罪事實」方面扮演核心角色。請詳細說明時間軸分析（Timeline Analysis）、關聯分析（Relational analysis）和功能分析（Functional analysis）這三種特殊技術如何通過偵查及分析數位證據，幫助科技偵查（刑事）人員拼湊出犯罪圖景，並回答案件的「人、事、時、地、物、原因」等要素。（25 分）

四、請說明依循 ISO/IEC 27043：2015 國際標準來進行資安犯罪事件偵查程序的四大階段程序（包含準備程序、開始程序、獲取程序、調查程序）為何？並請舉例及繪圖表說明之。（25 分）（ISO/IEC 27043：2015 Incident Investigation Principles and Processes 之國際資安事件偵查原則與程序標準）