代號：50870
頁次：2－1

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：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、生成式人工智慧（Generative Artificial Intelligence, Gen AI）技術，已被廣泛應用於製作擬真度極高的虛假資料，同時也被惡意利用來製造偽造證據。面對這種情況，如何有效鑑別與處理偽證據，成為數位鑑識實務中急需解決的重要課題。

㈠請說明生成式 AI 對數位鑑識所可能產生之挑戰。(7 分)

㈡請說明數位鑑識人員可利用那些技術、工具以及如何運用這些技術、工具與程序來辨識、處理及證明偽造內容的存在。(18 分)

二、在數位鑑識調查中，MACE 時間是檔案系統提供的重要時間戳記，可協助重建使用者行為與檔案操作歷程。假設鑑識人員從一位涉嫌內部洩密的員工電腦中，提取出兩份檔案。一份名為 ReportA.docx。另一份名為 ReportB.docx。使用鑑識工具觀察到 A、B 檔案的 MACE 時間分別如表 A 與表 B：

表 A：

屬性	時間
M	2024/12/15 10:22:41
A	2025/01/04 09:03:10
C	2024/12/01 08:45:00
E	2025/01/03 23:58:02

表 B：

屬性	時間
M	2023/11/01 14:05:00
A	2023/12/01 10:00:00
C	2024/01/15 09:30:00
E	2024/01/15 09:30:00

請回答下列問題：

㈠請解釋檔案的 MACE 四個時間戳記分別代表的意義，並說明那一項最容易因系統搬移、下載或複製等操作而改變。（8 分）

㈡根據表 A 與表 B 中的時間資訊，請分別推論這兩份檔案的完整歷程，例如：是否有被複製、打開瀏覽或修改的跡象？並請具體說明理由。（17 分）

三、假設你接到某公司要求調查員工涉嫌內部資料外洩的案件時，鑑識流程的第一步通常會是進行「案件接收與初步分析」。這部分的細項包含了⑴與該公司聯繫確認案件範圍與關鍵目標（特定員工、主機、檔案類型等）⑵了解事件時間點、通報來源與可疑行為。進行完第一步後，請詳細說明接下來所需的步驟，也就是後續你將採取的鑑識調查流程與各細項說明。(25 分)

四、在數位鑑識調查結束後，鑑識人員需撰寫鑑識報告作為最終成果，此報告不僅用於向委託單位呈交結果，也可能作為法庭證據使用。請說明一份具備法庭可採性的數位鑑識報告應包含那些「關鍵內容與結構」？(25 分)