98年公務人員特種考試警察人員考試、98年特種考試交通事業鐵路人員考試及98年公務人員特種考試民航人員考試試題　代號：30830　全一頁

等　　別：三等考試
類　　科：警察資訊管理人員
科　　目：數位鑑識
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。

一、解釋名詞：（每小題 5 分，共 25 分）
㈠ Evidence Acquisition
㈡ MAC（Media Access Control）Address
㈢ Hidden Data
㈣Computer-related Evidence
㈤ Standard Operating Procedures（SOPs）

二、簡答題：（每小題 5 分，共 25 分）
㈠當數位證據（Digital Evidence）在電腦鑑識實驗室內作鑑驗時，會採用原始證據或複製證據來為之呢？請說明理由。
㈡當鑑識人員欲取得已關機電腦內硬碟檔案資料時，應如何做呢？
㈢在何種情況下，偵查或鑑識人員所取得之數位證據將會適用到排除法則（Exclusionary Rule）？
㈣在法庭上如何證明偵查或鑑識人員所取得之數位證據是不被污染過的？
㈤在個人電腦 DOS 作業系統環境下，鑑識人員經由輸入一條指令和參數，以便可以找出並開啟被嫌犯所隱藏與唯讀的檔案或子目錄名稱等數位證據，試寫出此指令與其參數？

三、電腦（數位）鑑識人員在鑑驗各種不同犯罪類型和數位儲存媒體時可能會採取不同的鑑定方法，並且會遵循一些共通證據的萃取和證物保管之準則。請回答下列各問題：（每小題 5 分，共 25 分）
㈠指出並說明電腦證據（Computer Evidence）的兩個種類與其內涵。
㈡何謂萃取（Extraction）。
㈢詳述進行邏輯萃取（Logical Extraction）階段的步驟內容。
㈣寫出保管鏈（Chain of Custody）的主要目的。
㈤寫出如何維護好證物保管鏈。

四、現今世界各國執法機關和法院所認可的數位鑑識專業軟體 EnCase，主要用於人工操作和自動化處理以取得數位證據。請回答下列各問題：
㈠試從物理狀態、法律和犯罪等三個觀點，來闡述數位證據的意義。（9 分）
㈡刑事偵查人員在偵辦「車手集團洗錢案」過程中依法扣押到兩個可疑檔案：「車手洗錢.txt」和「車手通聯紀錄.txt」。試利用 EnCase 所提供的 EnScript Language，來撰寫一個數位證據自動化搜尋擷取程式，以便試圖在這些檔案內容中找到有：「桶子」或「公機」或「過水」或「漂白」或「0910123456」等關鍵字，並可顯示含有這些關鍵字的該列完整內容於輸出畫面上。（假設這些檔案存在某一 Case 檔案內並已經被開啟）（16 分）