99年公務人員特種考試警察人員考試及
99年特種考試交通事業鐵路人員考試試題

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、當數位（電腦）鑑識人員協助蒐集某公司網路設備被駭客入侵之數位證據時，發現該公司之防火牆、路由器、伺服器及電腦等相關設備之系統時間不一致。
㈠試說明為何網路與電腦等設備一段時間後，會產生系統時間不一致的情形。（5 分）
㈡試說明如何解決該公司網路與電腦設備系統時間不一致之情形，使設備時間可以保持正確的狀態。（5 分）
㈢接題目㈡，若透過網際網路解決系統時間不一致問題，該公司防火牆及電腦如何設定（電腦作業系統可以是 Windows XP、7 或 Linux，擇一作業系統作答）？（15 分）

二、電信通信紀錄是調查或蒐集證據的依據，「電信法」第 7 條電信事業處理有關機關（構）查詢通信紀錄，交通部在「第二類電信事業管理規則」第 4 章通信設備維運之管理，第 27 條條文中訂定經營者對於調查或蒐集證據，電信通信紀錄應至少有保存期間。
㈠本條文規範網際網路接取服務，其電信通信紀錄除用戶識別帳號外，包含有那些項目，試說明之。（15 分）
㈡試說明這些項目的至少保存期。（15 分）

三、數位證據的蒐集是鑑識處理的一環，資安事件即時性資訊的取得，常以資料複製的方式進行，以不影響原始證據為原則。
㈠對於網路交換器設備，試說明兩種常用的方式進行即時數位證據的蒐集，並比較優缺點。（15 分）
㈡ Linux 環境下，試說明如何完成整顆硬碟或 partition 備份及針對檔案系統進行差異性備份。（10 分）

四、「電腦處理個人資料保護法」，民國 84 年 8 月 11 日經總統公布施行。
㈠請說明該法案制定的目的。（10 分）
㈡請說明今（99）年修正的主要項目及目的。（10 分）