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：50970　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：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、請說明下列數位證據相關名詞之意涵：（每小題 5 分，共 25 分）
㈠Locard’s exchange principle
㈡Bit stream copy
㈢Write blocking device（Write blocker）
㈣File slack space
㈤Chain of custody

二、有關於數位鑑識中的數位證據識別與保存，請問：
㈠何謂「易揮發證據（Volatile evidence）」？請以最常見的 Windows 作業系統為例，列舉易揮發證據並說明其在犯罪偵查上的可能用途。（15 分）
㈡根據我國政府機關（構）資安事件數位證據保全標準作業程序之規定，於數據封緘作業時有那些程序需遵守？（10 分）

三、數位鑑識工作中包括現場重建（reconstruction of crime）步驟，請問：
㈠此步驟的內容與目的為何？（10 分）
㈡現場重建後的報告中，通常會做 Timeline analysis，Relational analysis 以及 Functional analysis 三種分析報告，請舉例說明此三份分析報告的意涵。（15 分）

四、假設在犯罪現場查扣一台筆電與一個 USB 介面之外接式硬碟，初步檢查發現此外接式硬碟內容含有犯罪證據，而筆電內沒有犯罪證據。因查扣當時該硬碟並未連接筆電，所以某甲雖承認該筆電是他所有，但推說硬碟是行蹤不明的某乙所有，且該硬碟從未連上筆電，以此主張他和犯罪事件無關。面對某甲陳述，請問你會採用那些數位鑑識步驟來證明某甲所述為非？（假設筆電使用 Windows 作業系統。回答本題時請說明該擷取那些證據，使用那些工具以及採取那些步驟。）（25 分）