《資訊安全實務》

試題評析	本次命題數位鑑識考了 35 分，除此之外，本科目數位鑑識 106 年考了 25 分，105 年考了 20 分，104 年考了 30 分，103 年考了 20 分，顯示數位鑑識近五年來一直都是本科目的命題重點，學員不可不慎！
考點命中	第二題：《高點・高上資訊安全實務講義》二回，張又中編撰。 第三題：《高點・高上資訊安全實務講義》一回，張又中編撰，頁 1-3～4、1-6。 第四題：《高點・高上資訊安全實務講義》一回，張又中編撰。

一、在建置數位簽章（digital signature）時，應使用對稱式的加密（symmetric encryption）方法或是非對稱式的加密（asymmetric encryption）方法？（5分）其原因為何？（10分）

【擬答】

根據我國電子簽章法第二條，數位簽章的定義指將電子文件以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰加以驗證者。因此，應使用具私密金鑰與公開金鑰的非對稱式加密方法。

二、若發覺一部電腦運作不正常，有被植入惡意程式（malware）的可能，請根據不同類型惡意程式的性質，來論述應如何判斷這部電腦所被植入的惡意程式是屬於那一類型，並說明應如何處理。（30分）

【擬答】

惡意程式的種類如下：

1.電腦病毒(Virus)
2.電腦蠕蟲(Worm)
3.後門程式(Backdoor)
4.特洛伊木馬(Trojan Horse)
5.惡意程式隱匿技術(Rookit)
6.網頁惡意程式(Webpage Malware)
7.間諜軟體(Spyware)
8.廣告軟體(Adware)
9.勒索病毒(Ransomware)
10.SQL Injection

當發覺一部電腦運作不正常時，可由其感染管道、感染方式、感染後的行為來辨識其被植入的惡意程式是屬於哪一類型。以電腦病毒為例，其透過被動式(如拷貝檔案)感染，並可能造成電腦資料的損毀。

電腦病毒的處理方式如下：

1.架設防火牆
2.安裝防毒軟體
3.定期備份資料
4.定期更新系統
5.不任意點選超連結
6.定期進行病毒掃瞄
7.使用合法授權軟體
8.關閉電子郵件預覽功能
9.不閱讀來路不明的電子郵件
10.定時更新病毒碼和掃描引擎
11 開啟檔案或資料前先以防毒軟體掃描

12.不需要使用網路資源時，關閉網路連線
13.不隨便開放目錄分享，避免被當作入侵或感染的管道

三、試論述數位鑑識（digital forensics）和傳統鑑識（traditional forensics）在處理程序上的相似性和差異性（10分），並論述這兩種類型的鑑識所處理證據在性質上的主要差異。（5分）

【擬答】

數位鑑識為透過標準的數位證據採證流程，將電腦、網路設備中的數位證據加以保存，並整合相關數位證據進行分析、比對，還原事件發生的原始面貌。與傳統鑑識相較，處理程序相似如下：

1.蒐集
2.檢驗
3.分析
4.報告
5.呈現

然而，由於數位證據具有以下特性：

1.易遭竄改性
2.復原可能性
3.難以萃取與保存
4.無法直接感知與理解
5.不易證實其來源與完整性

因此，數位鑑識的作法是將原始電磁紀錄拷貝後，再針對拷貝的電磁紀錄進行分析。故需證明原始數位證據與檢驗分析的數位證據兩者相同，可用雜湊值(Hash Value)來達成。而非如傳統鑑識，直接對原始跡證進行鑑識。

四、當一企業內發生電腦犯罪時，可由企業自己或執法單位來進行數位鑑識，請說明若由企業自己來做時，各列舉一個優點和一個缺點（10分）；而當由執法單位來做數位鑑識時，亦各列舉一個優點和一個缺點。（10分）

【擬答】

數位鑑識進行單位	企業自己	執法單位
優點	✦ 保護企業機密資料 由企業自己進行數位鑑識，可確保機密或敏感資料不會外洩。	✦ 具公正第三方效力 藉由嚴謹的數位鑑識程序，所獲得之鑑識結果，具有公正第三方之效力。
缺點	✦ 不具公正第三方效力 企業自行數位鑑識，所得到之鑑識結果並未獲得公正第三方之背書。	✦ 特殊領域之專業可能不足 當牽涉特殊領域的專業時，由於執法單位並非該領域之專家，專業知識可能不足。

五、實務上使用的防火牆可分成好幾種類型，請分別說明各類型防火牆的功能。（20分）

【擬答】

(一)封包過濾防火牆(Packet-filtering Firewall)

第一代防火牆，提供網路層封包篩選的基本功能，依據定義好的存取規則過濾每個流經的 IP 封包，以決定是否允許或阻止該封包的通過。

(二)狀態檢視防火牆(Stateful Inspection Firewall)

一種動態封包過濾的防火牆技術，持續追蹤連接狀態直到結束連線為止。會建立每個連線的狀態表，然後根據前後關聯狀況來允許或拒絕封包通過。

(三)代理防火牆(Proxy Firewall)

強調用戶端必須與代理伺服器接洽，再透過其與目的主機連線，而非直接讓用戶端連接目的主機。

(四)混合型防火牆(Hybrid Firewall)

套用多種封包過濾篩選方式，可加強安全性。