《資通安全》

一、為了確保數位證據（Digital Evidence）的完整性及有效性，請說明執行數位鑑識（Digital Forensics）的作業流程及相關內容。（25 分）

命題意旨	本題在測驗考生對於數位鑑識之內容及其流程的掌握度。
答題關鍵	本題解題層次為： 一、先簡單定義數位鑑識之內容。 二、再以條列式說明其流程與執行細項。
考點命中	《高點資通安全講義》第二回，金乃傑編撰，電腦犯罪與數位鑑識部分，頁 69-71。

【擬答】

數位鑑識（Digital Forensics）是針對握有的資料或儲存於電腦的媒體資料應用嚴謹的程序及科技的方法進行蒐證、檢驗、認證、保存與分析，做為日後法庭能據以判別的法律依據的程序。以下說明作業流程及相關內容：

(一)事件辨別：即情報蒐集與案件分析。其目的在於取得所需的資訊與相關資料，也在於預先了解案件的挑戰與可採取的因應之道。內容如下：

1.以 5W1H 蒐集事件基本資料，判斷事件類型是否需要鑑識。

2.若是，則取得「事件處理及鑑識用戶授權書」、「事件鑑識計畫表單」。

3.建立鑑識計畫及團隊。

(二)保存證據：數位證據隨時都可能因為鍵盤或滑鼠的一按而改變。所以到現場的第一步，就要控制好現場，並開始記錄時間與進行調查及鑑識人員對證據的操作，也就是證物鏈（Chain of Custody）的管理。工具如下：

1.現場勘查紀錄工具：攝影機、三腳架

2.證物扣押與保存工具：標籤紙、抗靜電袋

3.消逝性資料取證工具：LiveDetector、NetWitness

(三)檢驗證據：一般電腦文書資料、圖片、聲音等都可以利用許多工具軟體來檢視。然而，最大的問題在於被刪除的檔案，這些被非法者所刪除的檔案有時會是重要的證據資料。因此，便要對磁碟中的剩餘空間（Slack Space）進行檢視，利用工具軟體來進行字串搜尋與檔案重建。工具如下：

1.非消逝性資料取證工具：Logicube Dossier、Helix

2.分析與鑑識工具：Log Parser、Encase、NVIDIA Tesla S1070、Vound Intella

(四)案件分析與陳述：將鑑識結果與非法者之間的關係進行分析。藉由對證據進行分類、比對與個化(Individualization)，檢驗鑑識所得是否可連結到非法者，並藉由所得之證明來推斷出非法者的行為。

(五)呈現結果：在探究證據的來源、成因與非法者的關係時，要排除掉所有可能的替代解釋，來證明己方解釋為唯一解釋，方可明白確定無罪或有罪之假定。在法庭之上，對證據與因果關係些微的懷疑，就足以影響證據是否被採納及告訴是否成立。

二、依部署環境及系統架構的不同，入侵偵測系統（Intrusion Detection System, IDS）可概分為主機端入侵偵測系統（Host IDS）及網路端入侵偵測系統（Network IDS）兩種類型。請分別說明這兩種類型之入侵偵測系統的運作原理及其優缺點。（25 分）

命題意旨	本題在測驗考生對於兩大類入侵偵測系統（主機型及網路型）之運作原理及其優缺點。
答題關鍵	本題解題層次為： 一、先簡單說明入侵偵測系統之定義。 二、再以表格比較主機端及網路端入侵偵測系統之運作原理、優點及缺點。
考點命中	《高點資通安全講義》第一回，金乃傑編撰，網路裝置防護部分，頁 24-25。

【擬答】

入侵偵測系統是由軟體或硬體組成，對行為、安全日誌、稽核資料或其他網路上可以獲得的資訊進行研判、比對，發覺入侵的行為或企圖，並回報給網管人員的安全設備。以下表說明主機端入侵偵測系統與網路端入侵

偵測系統之運作原理及優缺點：

	主機端入侵偵測系統（Host IDS）	網路端入侵偵測系統（Network IDS）
運作原理	佈署在主機或伺服器上，分析主機或伺服器上被呼叫或執行的指令，藉此分析出可能帶有惡意的系統呼叫（System Call）指令。	佈署在一個網段上，監看及分析流經此網段的封包，藉此分析出可能帶有入侵行為。
優點	1.對於事件有較詳盡的紀錄。 2.對加密傳輸可以從主機解開後檢查。 3.不需要另外購置硬體，只需要安裝軟體即可監控。	1.一個網段只需要佈署一台，管理方便。 2.即時蒐集證據難以抹滅。 3.即時通知管理者。 4.對網段中電腦隱形。
缺點	1.大量部屬成本高、管理難。 2.惡意程式可能可以修改 log 抹滅證據。 3.批次檢視 log，通常入侵已經發生。 4.一定要佈署在主機上。	1.無法監看加密連線。 2.IP Spoofing 會造成誤判。 3.可能受到 DOS 攻擊。

三、若網站資訊系統設計不當，將可能遭受 SQL 資料隱碼攻擊（SQL Injection）。請說明造成 SQL 資料隱碼攻擊的原因及其解決方案。（25 分）

命題意旨	本題在測驗考生對於 SQL 隱碼攻擊之原理及解決方法。
答題關鍵	本題解題層次為： 一、先說明 SQL 隱碼攻擊之攻擊原理，並搭配例子說明。 二、再以條列式說明其解決方案。
考點命中	《高點資通安全講義》第一回，金乃傑編撰，應用網站攻擊部分，頁 71-72。

【擬答】

SQL 隱碼攻擊（SQL injection），是發生於應用程式之資料庫層的安全漏洞。

(一)其攻擊原理為在連結資料庫的表單中，加入具有 SQL 語法的特殊用字，破壞原本連接資料庫的 SQL 語法，使得資料庫出現異常，甚至可以為造成授權的使用者或者讓網站印出其他的會員資料。例如網站中原本驗證會員的 SQL 語法為：

SELECT * FROM member WHERE id = '$uid' AND passwd = '$pass'

若攻擊者在表單中填入$uid 為 0；$pass 為' OR '1' = '1；則 SQL 語法變為：

SELECT * FROM member WHERE id = '0' AND passwd = '' OR '1' = '1'

由於通常網站管理者的 ID 為 0，且後面 '1' = '1' 一定會成立，因此就能偽裝成管理者登入了。

(二)以下說明解決方案：

1.在設計應用程式時，完全使用參數化查詢（Parameterized Query）來設計資料存取功能。

2.在組合 SQL 字串時，先針對所傳入的參數作字元取代。

3.透過程式語言中特殊的功能，讓使用者輸入的特殊字串被加上反斜線去除其功能。。

4.使用其他更安全的方式連接 SQL 資料庫。例如：已修正過 SQL 資料隱碼問題的資料庫連接元件；例如：ASP.NET 的 SqlDataSource 物件或是 LINQ to SQL。

四、針對資料或系統的資安威脅，可歸納成四種類型：中斷（interruption），亦即阻斷系統連結或服務；截聽（interception），亦即側錄傳輸資料；更改（modification），亦即修改運輸資料或執行程式；偽冒（fabrication），亦即假冒通信個體名義發送偽造訊息。請分別說明防制這四種資安威脅的實務作法。（25 分）

命題意旨	本題在測驗考生對於網路安全中四種威脅（中斷、截聽、更改及偽冒）的防範方法。
答題關鍵	分項以條列式撰寫四種威脅的防範實務做法。
考點命中	1.《高點資通安全講義》第一回，金乃傑編撰，阻斷服務與殭屍網路部分，頁 82-84。 2.《高點資通安全講義》第一回，金乃傑編撰，訊息鑑別碼與雜湊函式部分，頁 13。 3.《高點資通安全講義》第一回，金乃傑編撰，密碼學的整合應用部分，頁 17-19。

【擬答】

以下將資安威脅分之四種類型：中斷、截聽、更改及偽冒，在防治的實務做法說明如下：

(一)中斷（Interruption）：最典型的攻擊為阻斷服務攻擊（DoS, Denial of Service），以 SYN Flooding 而言，可以使用 SCTP（Stream Control Transmission Protocol）通訊協定四向交握建立連線來防止伺服器資源被攻擊者消耗。實務做法為在建立連線前，伺服器將收到用戶端的 TCB（Transmission Control Block）修改後用自己的對稱金鑰加密，儲存到 State COOKIE 中，再透過 INIT-ACK 將 State COOKIE 回傳。當伺服器回應 INIT-ACK 後，會將所有的資訊刪除。當伺服器收到用戶端原封不動的 COOKIE-ECHO 後，使用對稱金鑰解開訊息，再根據 State COOKIE 的資訊配置資源完成連線。另外，亦可使用防火牆、QoS 等技術控制連入伺服器的 IP 或連線數，保障伺服器不受到過量的連線而停止服務。

(二)截聽（Interception）：資料網路傳輸過程中被非法的第三者得知，主要透過加密（Encryption）來防護。如網頁傳輸中使用 HTTPS 對伺服器及瀏覽器中連線加密。實務做法為使用者瀏覽器發出 ClientHello 給 SSL 網站伺服器：告知伺服器瀏覽器可以使用 SSL 加密及演算法版本序號。SSL 伺服器回應 ServerHello，包含伺服器的數位憑證（存放伺服器公鑰及其他伺服器身分認證的資訊）、這次要使用的演算法。使用者瀏覽器傳送加密後的對稱金鑰給伺服器：瀏覽器依照演算法產生一把對稱金鑰（稱為 session key，僅使用於本次加密），並使用伺服器的公鑰將該金鑰加密（因只有伺服器有解密的私密金鑰，故對稱金鑰不會被傳輸過程中破解）。伺服器解開金鑰取出對稱金鑰進行往後互傳資訊的加解密操作。

(三)更改（Modification）：訊息竄改指攻擊者針對網路通訊的內容進行增刪或者更動，常見如透過中間人攻擊（Man-in-the-Middle）竄改訊息。可透過訊息鑑別碼（Message Authentication Code）或雜湊函數（Hashing Function）驗證。訊息鑑別碼的實務做法為以雙方共享的金鑰對欲傳送的資料加密，並將密文最後 8 byte 取出，作為訊息鑑別碼；接收方以相同方式對收到的資料進行加密，再比對訊息鑑別碼是否相同。因為加密的安全性，訊息被更動任何一個 bit 都會產生完全不同的加密結果，因此如果相同，代表訊息在傳輸的過程中沒有被竄改。

(四)偽冒（Fabrication）：在網路活動中以某特定身分傳送訊息，可透過數位簽章（Digital Signature）防治，數位簽章利用公開金鑰基礎建設的機制來保護資料傳遞的完整性、身分認證性與不可否認性的一種通訊安全機制。數位簽章的實務做法為傳送者將與傳送的資料雜湊，以自己的私鑰加密後（稱為數位簽章），連同本文一起傳送給對方。接收者用同樣雜湊函式對收到之本文雜湊，再以傳送者公鑰解開數位簽章，比較兩雜湊結果是否相同。因在公開金鑰基礎建設的基礎下，發送者的私鑰他人不可能擁有，且私鑰加密的文件只有公鑰可解開；故當接收者用發送者公鑰解開文件，就代表文件一定是發送者用自己的私鑰加密的，又由於只有發送者擁有私鑰，故可確定訊息一定事法送者發送的。