《資訊管理與資通安全》

一、電腦設備和網際網路已成為新興的犯罪工具或媒介，因此，面臨訴訟爭議時，常會涉及數位證據的運用：

(一)何謂數位鑑識？（10分）

(二)何謂證據同一性？（10分）

(三)當第一線人員取證檔案做證據時，請列出什麼情境，該檔案是有證據能力的；而什麼情境，該檔案是沒有證據能力的？（5分）

試題評析	隨著科技技術的發達，其也演變成許多犯罪的溫床，嘗試找出數位證據與保留數位證據的課題也益趨重要。此題非常具有鑑別度，答題上同學要熟記上課所說的網路鑑識與數位鑑識基本概念與意義外也要有舉例的能力。答題的心法上除了基本概念外，也要舉出靠近生活中的應用與例子，除了可以幫助同學記憶與理解外，同時也是獲得高分的關鍵。
考點命中	《高點‧高上資訊管理與資通安全講義》第三回，蕭老師編撰，頁58-59。

答：

(一)主要在針對數位裝置中的內容進行調查與復原，數位鑑識一開始等同於電腦鑑識，但現在已經擴展到調查所有能夠儲存數位資料的裝置。數位鑑識的調查結果有非常多元的應用，最常見的用途是當作電子偵查的部分程式，在刑事或民事法庭之上，支援或排除犯罪假設。數位鑑識也能在企業部門應用，例如公司內部調查或侵入調查。除了用來確認犯罪的直接證據以外，數位鑑識也能夠用來確認特定嫌疑犯與案件的關係、確認不在場證明或其證詞、理解其意圖、追查來源、或是判定檔案的真偽。調查的技術層面依照數位裝置的類型可區分為以下幾個分支：電腦鑑識、網路鑑識、鑑識資料分析以及行動裝置鑑識。一般典型的鑑識程式包含數位裝置的收押、鑑識成像(forensic imaging)獲取、數位媒體分析、以及製作報告列為證物。其也衍生出許多不同的類別：

1.電腦鑑識：主要包含電腦、嵌入式系統及隨身碟等數位證物鑑識，主要進行還原、解讀及分析儲存裝置內殘存檔案，重建及還原事件過程或與取得案情相關證據。

2.行動裝置鑑識：主要在還原行動裝置內遭刪除資料或證據，與前項差異在於行動裝置的儲存裝置通常燒焊於主機板，且型號、種類因裝置廠牌型號等均不盡相同，因此行動裝置上資料擷取與保存之難度較電腦主機高。3.網路鑑識：主要監錄網路設備透過網路路由傳送封包內容及網路設備紀錄檔，透過分析擷取封包、網路設備及電腦主機系統日誌檔（Log File）等方式，追查及還原駭客入侵事件。

4.資料分析鑑識：分析結構化資料找出可疑犯罪事證。

5.資料庫鑑識：資料庫鑑識主要針對資料庫及其元資料（metadata）進行鑑識分析，運用資料庫內容、日誌檔及記憶體資料等進行案發重建。

(二)指呈現於法庭用來證明待證事實之證據與原始證據兩者必須一致，亦即證據是否有可採用價值之程序，在提出該項數位證據前，提出者必須要證明數位證據符合真實性要求。要證明證據的同一性，就在於證據鍊的控管，在數位鑑識主要分為兩個層面來談，一為實體證物，另一為數位證物內含的數位資料；由於數位證據具有抽象、易破壞、消逝等特性，因此數位證據同一性往往成為訴訟攻防的重點，數位鑑識人員為避免不必要爭議，加上數位證據具有可無損複製等特性，因此通常會以重製原件方式產生證物副本，並以證物副本進行鑑識工作，避免更動原件並將原件封存供第三方複驗；因此「原件不可變動」成為數位鑑識人員及司法人員最高原則及鑑識程序鐵律。

(三)證據能力即是證據得提出於法庭調查，以供作認定犯罪事實之用，所應具備之資格；此項資格必須證據與待證事實具有自然關聯性，符合法定程式，且未受法律之禁止或排除，始能具備。因此證據能力主要規範證據取得是否合法取得及與待證事實有相當關聯性。根據國國家司法研究院以下情況為具有「證據能力」：

1.在證物蒐集、保全及運送過程中不可變更證據。

2.數位證據只能由受過訓練之專業人員進行檢驗。

3.數位證據在擷取、運送過程之處理細節及步驟、裝置狀態等必須詳細記錄及保存，供作日後重新檢視時

使用。而沒有證據能力的即是違反以上原則之證物，則代表沒有證據能力。例如：有竄改疑慮的磁碟、不完整且可能有被修改的對話紀錄…等皆是沒有證據能力。

【參考書目】《數位鑑識「原件不可變動原則」之適用—由行動裝置鑑識與電腦鑑識差異探討》，陳詰昌編著。

二、電腦系統或網路設備，或多或少都有弱點存在，為防止駭客進行惡意入侵，系統應有相對的防禦工具：

(一)何謂網路型入侵偵測系統？（5分）

(二)說明網路型入侵偵測系統，其部署位置及運作狀況（可以示意圖表示），並陳述其優缺點。（10分）

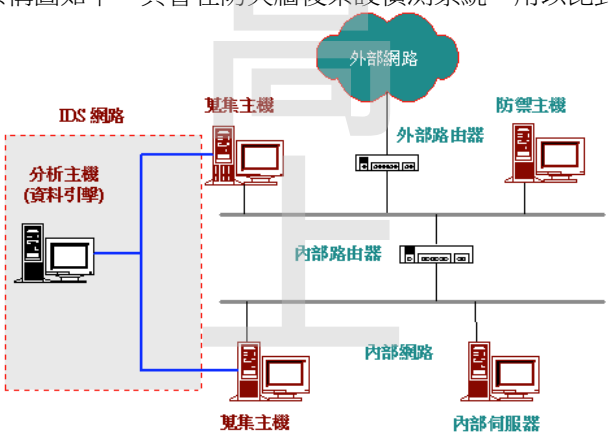
(三)當資訊人員遇到攻擊封包或病毒，於企業內迅速擴散時，未更新的主機不斷的散布攻擊封包，資訊人員必須與時間競爭，其處理方法為何？（10分）

試題評析	此題為傳統的入侵偵測系統的延伸題型，同學在答題上最有困難的應該屬第二小題，此題概念上要想到分散的處理方式與防火牆的結合，正是此題的搶分關鍵。 第三題是屬於日常生活應用類型，只要依照課堂上所講述的觀察到被攻擊時的即時處理方式回答即可。

答：

(一)網路型入侵偵測系統（Network Intrusion Detection System，NIDS）主要是由一個或多個偵測器，加上收集與分析資料的主控臺所組成，可以分析每個通過的網路封包，並與已知的攻擊特徵進行比對，如果符合某項攻擊特徵，系統就會啟動防護機制，例如發簡訊或命令防火牆中斷該連線。

(二)網路型入侵偵測系統其架構圖如下，其會在防火牆後架設偵測系統，用以比對可疑特徵。



其優點可以分為以下幾點：

1.分析主機採用較高速的處理設備，並且不用處理蒐集訊務的工作，可以提高許多處理能力。

2.僅負責蒐集訊務的主機並不需要很昂貴的伺服主機，只要一般個人電腦層次的工作站即可，即可節省成本並達到預期成效。

3.分散分析主機與搜集主機可以減少被攻擊的機會與攻擊後的損害。

常見的缺點如下：

(1)入侵偵測系統本身也是一個主機設備，必須經由 TCP/IP 裝置才能蒐集網路上流通的訊息，主機通常包含大量待搜尋的資料，因此，極可能成為被入侵對象。

(2)沒有主動防禦的能力：IDS只有告警的能力，無法主動防禦入侵行為。

(3)加密封包無法辨識：越來越多攻擊用加密封包，使得網路型入侵偵測系統監控網路流量的能力產生盲點，如果封包加密，就無法辨識其內容，也就無法進行分析。

(三)當發現系統的感染已經擴散時，可以用以下方法杜絕：

1.中斷網路連線：中斷該電腦的網路連線，避免災情擴大，這是最簡單易做的處理方式，雖然大多數使用者意識到被加密勒索軟體綁架時，通常災害也已經發生了，但將受害主機隔離這個步驟，仍是不可少的首要處置動作。

2.立馬關機：立刻持續按壓電源鍵，強迫電腦進行關機動作。之後可將該電腦的硬碟取出，透過外接方式將其中的未被加密的檔案保存下來。

3.緊急宣導並清查：負責IT相關的人員也要立即跟其他部門或同事宣導，提升大家的警覺性，並一一檢視各臺電腦是否也有受害，並通知所有同仁有狀況立即回報。

4.評估災情：評估災情是相當必要的一點，知道哪些資料被加密了，才能了解企業損失範圍與嚴重性，同時也要清查這些檔案是否有備份，是否能夠將檔案復原。

5.系統重灌，並加強軟體防護：若是災情不大，沒有太多重要檔案被加密，或是都有安全備份可以將檔案復原，僅有部分資料需重建，此時，多半使用者會選擇將被感染的電腦硬碟格式化，重灌系統，讓電腦回復成乾淨的原始狀態。然而，最好在重灌前，也清查受害電腦本身的預防措施，像是Windows作業系統是否安裝更新程式，是否安裝防毒軟體，防毒軟體的防護功能是否全部都開啟。因為，除了已知病毒的防護，還要提升未知病毒與最新攻擊的防護力。

6.保存現場狀況，請求支援：如果想找防毒、資安專家進一步協助，他們也都有提供產品的售後服務，請他們協助了解受害情況也是一種方式。同時，記得也要保存一臺受害主機，以便提供分析環境。

【參考書目】
圖表取自《資訊與網路安全概論》，粘添壽編著。

三、何謂儲存型跨站攻擊（Stored Cross-Site Scripting（XSS））/反射型跨站攻擊（Reflected Cross-Site Scripting（XSS））？依攻擊者（Attacker）、目標網站（Website）、受害者（User）分別說明出其關係（可以示意圖表示），並描述其攻擊步驟。（25分）

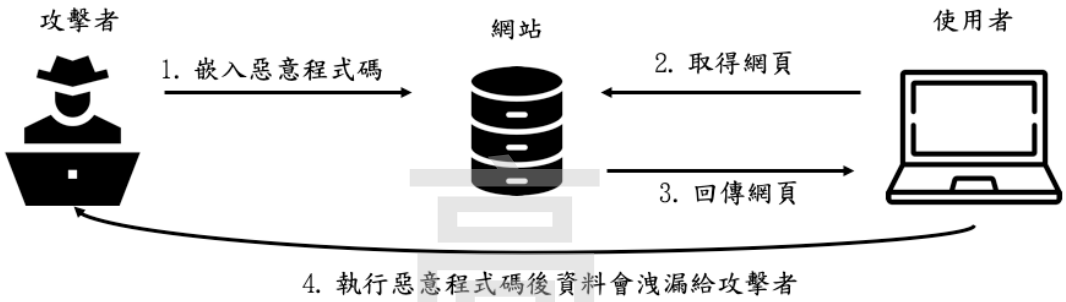
試題評析	此題是傳統的跨站型攻擊考題的延伸，同學在答題時切勿直接悶著頭開始回答儲存型與反射型，建議先將XSS做簡單的描述後再針對兩者的攻擊模式與差異做介紹。 此題高分的關鍵是要有圖片的搭配才可以明確的表達理念，再來是利用上課攻擊手法的補充，來詳細說明攻擊者方式。

答：

XSS 俗稱 JavaScript Injection ，指讓攻擊者執行惡意的程式片段，以達成其攻擊或是竊取資料的目的。事實上也包括 Java、VBScript、ActiveX、Flash，甚至是 HTML 等。攻擊者會在網站上植入惡意的程式碼，使得使用者在訪問該網頁時，同時會執行該惡意程式碼。這將可能導致攻擊者可擷取使用者的私密網頁內容、對談或是透過擷取 Cookie 或 Session 資料而假冒使用者為合法使用者等。

(一)儲存型跨站攻擊：

指遭到被保存在伺服器資料庫中的 JavaScript 代碼引起的攻擊。Stored XSS 就是讓 JavaScript 可以儲存在網站資料庫中，最常見的例子就是網站留言板或是訊息。由於留言板的方式較無限制，因此駭客就可以把程式碼放在留言板中，等待下一個瀏覽該留言板的受害者。



攻擊步驟：

1.攻擊者將惡意代碼注入到目標網站的數據庫中。

2.用戶打開目標網站時，網站服務端將惡意程式碼從資料庫中取出，並存在於HTML中返回給使用者之瀏覽器。

3.用戶瀏覽器接收到響應後解析執行，混在其中的惡意代碼也被執行。

4.惡意代碼竊取用戶數據並發送到攻擊者的網站，或者冒充用戶的行為，調用目標網站接口執行攻擊者指定的操作。

(二)反射型跨站攻擊：

網站會反應使用者所輸入的 URL（含 JavaScript 代碼）引起的攻擊。當攻擊者發現某個網站可以執行預期的惡意程式碼時，攻擊者就可以把受害 (被植入 JavaScript)網站的 URL 透過釣魚的方式或是郵件傳送給被害人。當被害人點擊該 URL時，就會看到且執行該 JavaScript。由於需要用戶主動打開惡意的URL才能生效，攻擊者往往會結合多種手段誘導用戶點擊。

攻擊步驟：

1.攻擊者構造出含惡意代碼的 URL

2.使用者打開帶有惡意代碼的 URL 時，網站服務端將惡意代碼從 URL 中取出並拼接在 HTML 中返回給瀏覽器。

3.用戶瀏覽器接收到響應後解析執行，混在其中的惡意代碼也被執行。

4.惡意代碼竊取用戶數據並發送到攻擊者的網站，或者冒充用戶的行為，調用目標網站接口執行攻擊者指定的操作。

四、專家系統（Expert System）是一種在特定領域內，具有專家水平解決問題能力的程式系統：

(一)專家系統主要由6個部分構成，請說明該6個部分之關係（可以示意圖表示），並描述各部分之功能。（20分）

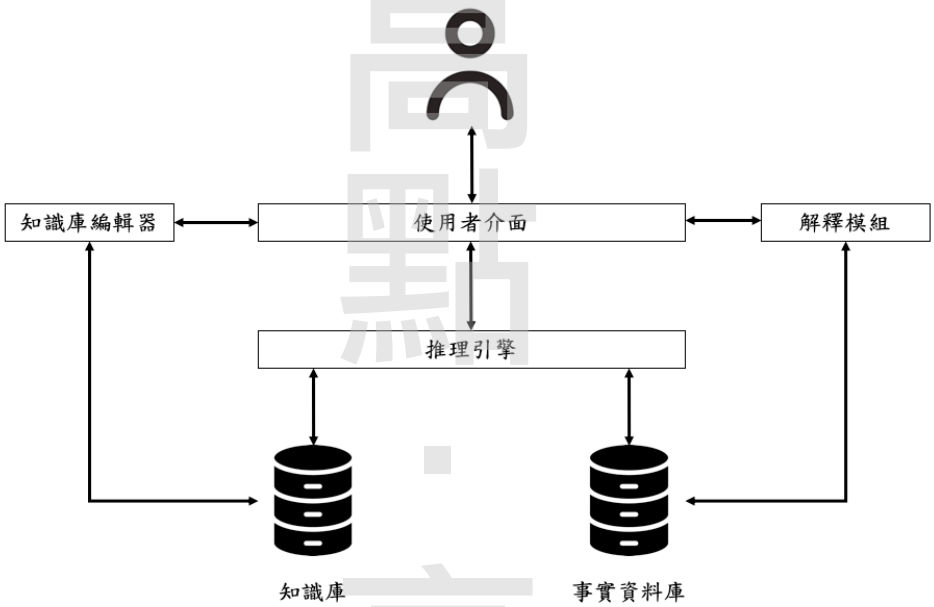
(二)說明專家系統和人工智慧的關係。（5分）

試題評析	人工智慧的蓬勃發展造成相關的議題變成現在的當紅考題。此題在答題上依照講義的元件說明並搭配圖示即可在第一小題獲得不錯的分數。 第二小題是更深入的解釋題，當下看到可能會略顯訝異，但只要回想專家系統就是想要模擬人工智慧，也是人工智慧早期且最成功的商業化應用後，即可無礙的解答。

考點命中	《高點・高上資訊管理與資通安全講義》第二回，蕭老師編撰，頁152-153。

答：

(一)此類具有專門知識和經驗的計算機智能程序系統，專家系統相當於知識庫加上推理引擎，因此專家系統也被稱為基於知識的系統。一個專家系統必須具備「領域專家級知識」、「模擬專家思維」和「達到專家級的水平」。



1.使用者介面：可讓使用者與系統交談，接受來自使用者的自然語言並解譯給系統，也提供一個友善的選單系統。

2.推理引擎：是系統的心臟，它使用知識庫和事實資料庫來推理所要採取的動作。

3.知識庫：為一堆的知識，是基於與專門技術相關領域的專家會談結果。

4.事實資料庫：專家系統中的事實資料庫是案例式的。對每一個案例，使用者輸入有效的或量測的資料到事實資料庫中，以便讓推理引擎使用於該特別案例。

5.解釋系統：用來解釋推理引擎所得結論背後的原理。

6.知識庫編輯器：可能沒有包含於所有的系統中，它是用來更新知識庫。

(二)專家系統是早期人工智慧的一個重要分支，一般採用人工智慧中的知識表示和知識推理技術來模擬通常由領域專家才能解決的複雜問題，而專家系統的產生給了人工智慧一個在工商業上應用極佳的平台。

專家系統包含一套複雜的電腦程式，運用知識來解決特定領域中的問題，它也和人類專家一樣，使用符號邏輯與經驗法則來尋找答案。根據專家系統之特性，專家系統與傳統模擬（Simulation）程式有極顯著之相似性，將專家系統與模擬相結合，可提升經營之效率及效用。