# Module 1: Computer Forensics in Today’s world

# LO#01: Understand the Fundamentals of Computer Forensic

Pháp y máy tính đề cập đến một tập hợp các thủ tục và kỹ thuật phương pháp giúp xác định, thu thập, bảo quản, trích xuất, giải thích, tài liệu và trình bày bằng chứng từ thiết bị máy tính, sao cho bất kỳ bằng chứng nào được phát hiện đều được chấp nhận trong quá trình tố tụng pháp lý và / hoặc hành chính

## Mục tiêu:

Theo dõi và truy tố thủ phạm của tội phạm mạng

Thu thập bằng chứng về tội phạm mạng một cách hợp lý về mặt pháp y

Để ước tính tác động tiềm tàng do vụ việc gây ra đối với nạn nhân và xác định ý định của thủ phạm

Để giảm thiểu những tổn thất hữu hình và vô hình cho tổ chức

Để bảo vệ tổ chức khỏi các sự cố tương tự trong tương lai

## Need for Computer Forensic

Để đảm bảo tính toàn vẹn tổng thể và sự tồn tại liên tục của các hệ thống CNTT và cơ sở hạ tầng mạng trong các tổ chức

Để trích xuất, xử lý và giải thích các bằng chứng thực tế để chứng minh hành động của kẻ tấn công tại tòa án

Để theo dõi hiệu quả thủ phạm từ các nơi khác nhau trên thế giới

Để bảo vệ nguồn tài chính của tổ chức và thời gian có giá trị

## Why and When Do You Use Computer Forensics?

Why?

Để thu thập bằng chứng về tội phạm máy tính một cách hợp lý pháp y

Để bảo vệ tổ chức khỏi các sự cố tương tự trong tương lai

Để giảm thiểu những tổn thất hữu hình và vô hình cho tổ chức

Để hỗ trợ việc truy tố thủ phạm của một inciden

When?

Nếu xảy ra vi phạm hợp đồng

Nếu xảy ra hành vi trộm cắp / lạm dụng bản quyền và sở hữu trí tuệ

Trong trường hợp tranh chấp nhân viên hoặc nhân viên bất mãn

Trong trường hợp thiệt hại về tài nguyên

# LO#02: Understand Cybercrimes and their Investigation Procedures

## Types of Cybercrime

Tội phạm mạng được định nghĩa là bất kỳ hành động bất hợp pháp nào liên quan đến thiết bị máy tính, mạng, hệ thống hoặc ứng dụng của nó

Tội phạm mạng có thể được phân thành hai loại dựa trên dòng tấn công:

Tấn công nội bộ (Internal/insider attack)

Đây là một cuộc tấn công được thực hiện trên mạng công ty hoặc trên một máy tính duy nhất bởi một người được ủy thác (người trong cuộc) có quyền truy cập vào mạng

Những người trong cuộc như vậy có thể là nhân viên cũ hoặc hiện tại, đối tác kinh doanh hoặc nhà thầu

Tấn công bên ngoài (External attack)

Kiểu tấn công này xảy ra khi kẻ tấn công từ bên ngoài tổ chức cố gắng truy cập trái phép vào hệ thống máy tính hoặc tài sản thông tin của tổ chức

Những kẻ tấn công này khai thác các lỗ hổng bảo mật hoặc sử dụng các kỹ thuật kỹ thuật xã hội để xâm nhập vào mạng

## Examples of Cybercrime

1. Espionage (Gían điệp)

2. Theft of Intellectual Propert (Trộm cắp tài sản trí tuệ)

3. Manipulation of Data (Thao tác dữ liệu)

4. Trojans Horse Attack

5. Structured Query Language Attack (Tấn công ngôn ngữ truy vấn cấu trúc)

6. Brute-force Attack

7. Phishing/Spoofing

8. Privilege Escalation Attack (tấn công leo thang đặc quyền)

9. Denial of Service Attack

10. Cyber Defamation (Phỉ báng trên mạng)

11. Cyberterroris (Khủng bố mạng)

12. Cyberwarfare (Chiến tranh mạng)

## Impact of Cybercrimes at the Organizational Level (Tác động của tội phạm mạng ở cấp độ tổ chức)

Mất tính bảo mật, tính toàn vẹn và tính sẵn có của thông tin được lưu trữ trong hệ thống tổ chức

Trộm cắp dữ liệu nhạy cảm

Gián đoạn đột ngột hoạt động kinh doanh

Mất niềm tin của khách hàng và các bên liên quan

Thiệt hại đáng kể về danh tiếng

Tổn thất tài chính lớn

Hình phạt phát sinh từ việc không tuân thủ quy định

## Cybercrime Investigation

Việc điều tra bất kỳ tội phạm nào liên quan đến việc thu thập tỉ mỉ các manh mối và bằng chứng pháp y với sự chú ý đến từng chi tiết

Chắc chắn, ít nhất một thiết bị điện tử sẽ được tìm thấy trong quá trình điều tra, chẳng hạn như máy tính, điện thoại di động, máy in hoặc máy fax

Thiết bị điện tử thu được từ hiện trường vụ án có thể chứa bằng chứng có giá trị và đóng vai trò chính trong việc giải quyết vụ án

Do đó, Thông tin chứa trong thiết bị phải được điều tra một cách hợp lý về mặt pháp y để được tòa án chấp nhận

Các loại vụ án điều tra tội phạm mạng như sau: Criminal (Tội phạm), Civil (dân dụng), Administrative (quản trị)

Các quy trình như thu thập dữ liệu, phân tích và trình bày khác nhau dựa trên loại trường hợp

## Civil vs. Criminal Investigation (Điều tra dân sự và hình sự)

Các vụ án dân sự được đưa ra vì vi phạm hợp đồng và các vụ kiện, trong đó kết quả có tội thường dẫn đến thiệt hại tiền tệ cho nguyên đơn, trong khi các vụ án hình sự thường được đưa ra bởi các cơ quan thực thi pháp luật để đối phó với nghi ngờ vi phạm pháp luật, trong đó kết quả có tội có thể dẫn đến thiệt hại tiền tệ, phạt tù hoặc cả hai

Vụ án hình sự (Criminal case)

Điều tra viên phải tuân theo một tập hợp các quy trình pháp y tiêu chuẩn được pháp luật chấp nhận trong khu vực tài phán tương ứng

Các nhà điều tra, theo lệnh của tòa án, có thẩm quyền cưỡng chế thu giữ các thiết bị máy tính

Cần có báo cáo điều tra chính thức

Các cơ quan thực thi pháp luật có trách nhiệm thu thập và phân tích bằng chứng

Hình phạt là khắc nghiệt và bao gồm phạt tiền, án tù, hoặc cả hai

Tiêu chuẩn chứng minh cần phải rất cao

Rất khó để nắm bắt một số bằng chứng nhất định, ví dụ: bằng chứng thiết bị Hệ thống định vị toàn cầu

Vụ án dân sự (Civil case)

Các nhà điều tra cố gắng cho bên đối diện thấy một số bằng chứng để hỗ trợ các yêu cầu bồi thường và thúc đẩy giải quyết

Tìm kiếm các thiết bị thường dựa trên sự hiểu biết lẫn nhau và cung cấp một cửa sổ thời gian rộng hơn cho bên đối diện để che giấu bằng chứng

Báo cáo ban đầu về bằng chứng nói chung là không chính thức

Nguyên đơn chịu trách nhiệm thu thập và phân tích bằng chứng

Hình phạt bao gồm bồi thường bằng tiề

Chuỗi lưu ký tài liệu kém hoặc không xác định để tìm bằng chứng

Đôi khi, Bằng chứng có thể nằm trong sự kiểm soát của bên thứ ba

## Administrative Investigation (Điều tra hành chính)

Điều tra hành chính thường liên quan đến việc một cơ quan hoặc chính phủ thực hiện các cuộc điều tra để xác định các sự kiện có liên quan đến việc quản lý và thực hiện của chính mình

Điều tra hành chính có bản chất phi hình sự và có liên quan đến hành vi sai trái hoặc hoạt động của nhân viên bao gồm, nhưng không giới hạn ở:

Vi phạm chính sách, quy tắc hoặc giao thức của tổ chức

Lạm dụng tài nguyên hoặc hư hỏng hoặc trộm cắp

Hành vi đe dọa hoặc bạo lực

Thăng chức hoặc tăng lương không đúng cách

Bất kỳ hành vi vi phạm nào cũng có thể dẫn đến hình thức kỷ luật như giáng chức, đình chỉ, thu hồi, phạt và sa thải

Đối với các tình huống như thăng chức, gia tăng, chuyển nhượng, v.v., điều tra hành chính có thể dẫn đến kết quả tích cực (positive), như sửa đổi các chính sách, quy tắc hoặc giao thức hiện có

# LO#03: Understand Digital Evidence (Hiểu bằng chứng kỹ thuật số)

Bằng chứng kỹ thuật số được định nghĩa là "bất kỳ thông tin nào có giá trị chứng minh được lưu trữ hoặc truyền tải dưới dạng kỹ thuật số"

Thông tin kỹ thuật số có thể được tìm thấy trong khi kiểm tra phương tiện lưu trữ kỹ thuật số, giám sát lưu lượng mạng hoặc tạo các bản sao trùng lặp của dữ liệu kỹ thuật số được tìm thấy trong quá trình điều tra pháp y

Bằng chứng kỹ thuật số có tính chất hoàn cảnh và mong manh, điều này gây khó khăn cho một điều tra viên pháp y để theo dõi hoạt động tội phạm

Theo Nguyên tắc trao đổi của Locard, "bất cứ ai hoặc bất cứ điều gì, bước vào hiện trường vụ án đều mang theo một cái gì đó của hiện trường và để lại một cái gì đó của chính họ khi họ rời đi"

## Types of Digital Evidence

Volatile Data (Dữ liệu biến động)

Dữ liệu bị mất ngay khi thiết bị tắt nguồn; Ví dụ bao gồm thời gian hệ thống, (các) người dùng đã đăng nhập, tệp mở, thông tin mạng, thông tin quy trình, ánh xạ quá trình đến cổng, bộ nhớ quy trình, nội dung bảng tạm, thông tin dịch vụ / trình điều khiển, lịch sử lệnh, v.v.

Non-volatile Data (Dữ liệu ko biến động)

Dữ liệu vĩnh viễn được lưu trữ trên các thiết bị lưu trữ thứ cấp như đĩa cứng và thẻ nhớ; Ví dụ bao gồm các tệp ẩn, không gian chùng, tệp hoán đổi, tệp index.dat, cụm chưa được phân bổ, phân vùng không sử dụng, phân vùng ẩn, cài đặt đăng ký, nhật ký sự kiện, v.v.

## Vai trò của bằng chứng kỹ thuật số

Ví dụ về các trường hợp bằng chứng kỹ thuật số có thể hỗ trợ điều tra viên pháp y trong việc truy tố hoặc bào chữa cho nghi phạm:

1. Trộm cắp danh tính

2. Các cuộc tấn công độc hại vào chính hệ thống máy tính

3. Rò rỉ thông tin

4. Truyền tải trái phép thông tin

5. Trộm cắp bí mật thương mại

6. Sử dụng/lạm dụng Internet

7. Sản xuất tài liệu, tài khoản giả mạo

8. Mã hóa trái phép/ mật khẩu bảo vệ tài liệu

9. Lạm dụng hệ thống

10. Liên lạc qua email giữa các nghi phạm / âm mưu

## Sources of Potential Evidence (Nguồn bằng chứng tiềm năng)

Tệp do người dùng tạo (User-Created Files)

Sổ địa chỉ (address books)

Tệp cơ sở dữ liệu (database files)

Tệp phương tiện (hình ảnh, đồ họa, âm thanh, video, v.v.) – Media files

Tệp Tài liệu (văn bản, bảng tính, bản trình bày, v.v.) – Documents files

Dấu trang Internet, mục yêu thích, v.v

User-Protected Files (Tệp đc người dùng bảo vệ)

Compressed files Tệp nén

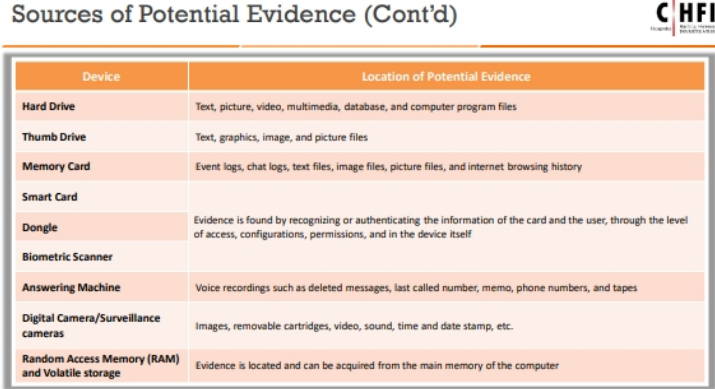
Misnamed files Tệp bị đặt sai tên

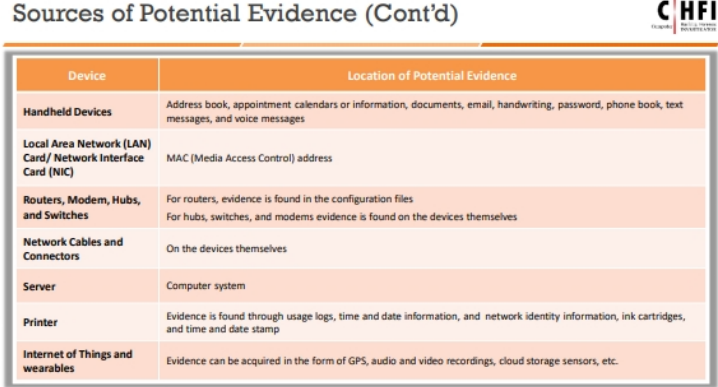
Encrypted files Tệp bị mã hóa

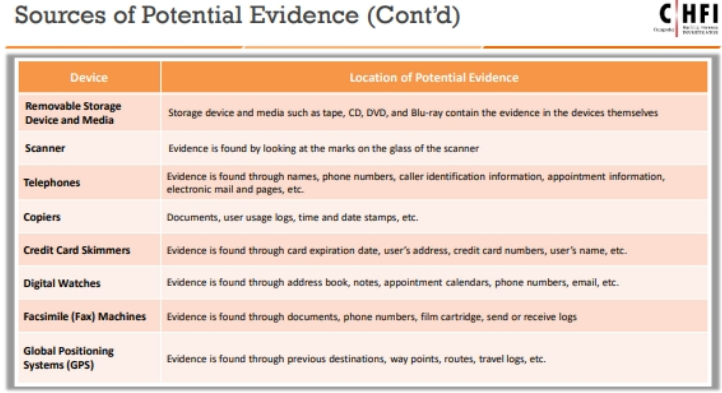
Password-protected files Tệp đc bảo vệ = mật khaiar

Hidden files Tệp ẩn

Steganography







## Rules of Evidence (Quy tắc chứng cứ)

1. Understandable: Chứng cứ phải rõ ràng và dễ hiểu đối với thẩm phán

2. Admissible: Chứng cứ phải liên quan đến thực tế đang được chứng minh

3. Authentic: Chứng cứ phải có thật và phù hợp liên quan đến vụ việc

4. Reliable: Không được nghi ngờ gì về tính xác thực hoặc tính xác thực của bằng chứng

5. Complete: Bằng chứng phải chứng minh hành động hoặc sự vô tội của kẻ tấn công

## Best Evidence Rule

Nó nói rằng tòa án chỉ cho phép chứng cứ gốc của một tài liệu, hình ảnh hoặc ghi âm tại phiên tòa chứ không phải là một bản sao. Tuy nhiên, bản sao có thể được chấp nhận làm bằng chứng, miễn là tòa án thấy lý do của bên gửi bản sao là xác thực.

Nguyên tắc cơ bản của quy tắc bằng chứng tốt nhất là bằng chứng ban đầu được coi là bằng chứng tốt nhất.

# LO#04: Understand Forensic Readiness, Incident Response, and the Role of SOC (Security Operations Center) in Computer Forensic

## Role of SOC in Computer Forensics (Vai trò của SOC trong pháp y máy tính)

Trung tâm điều hành bảo mật (SOC) là đơn vị tập trung liên tục theo dõi và phân tích các hoạt động đang diễn ra trên hệ thống thông tin của một tổ chức như mạng, máy chủ, thiết bị đầu cuối, cơ sở dữ liệu, ứng dụng, trang web, v.v. để tìm kiếm sự bất thường

Nhóm SOC đóng vai trò là điểm ban đầu để phát hiện và xác nhận sự cố

Sau khi xác nhận sự cố, nhóm ứng phó sự cố thu thập bằng chứng và cung cấp cho nhóm pháp y, sau đó bắt đầu điều tra pháp y

# LO#05: Identify the Roles and Responsibilities of a Forensic Investigator (Xác định vai trò và trách nhiệm của một điều tra viên pháp y)

## Need for a Forensic Investigator

Cybercrime Investigation (Điều tra tội phạm mạng): Các nhà điều tra pháp y, nhờ vào kỹ năng và kinh nghiệm của họ, giúp các tổ chức và cơ quan thực thi pháp luật điều tra và truy tố thủ phạm của tội phạm mạng

Sound Evidence Handling (Xử lý bằng chứng âm thanh): Nếu một người thiếu kinh nghiệm kỹ thuật kiểm tra bằng chứng, nó có thể trở nên không thể chấp nhận được tại tòa án của pháp luật

Incident Handling and Response (Xử lý và ứng phó sự cố): Các nhà điều tra pháp y giúp các tổ chức duy trì sự sẵn sàng pháp y và thực hiện xử lý và ứng phó sự cố hiệu quả

## Roles and Responsibilities of a Forensics Investigator

Điều tra viên pháp y thực hiện các nhiệm vụ sau:

Xác định mức độ thiệt hại trong quá trình phạm tội

Phục hồi dữ liệu có giá trị điều tra từ các thiết bị máy tính liên quan đến tội phạm

Thu thập bằng chứng một cách hợp pháp Đảm bảo rằng bằng chứng không bị hư hại dưới bất kỳ hình thức nào

Tạo ra một hình ảnh của bằng chứng gốc mà không giả mạo nó để duy trì tính toàn vẹn của nó

Hướng dẫn các quan chức thực hiện cuộc điều tra; Đôi khi, điều tra viên pháp y có thể được yêu cầu đưa ra bằng chứng và mô tả quy trình liên quan đến khám phá của nó

Tái tạo lại các đĩa bị hỏng hoặc các thiết bị lưu trữ khác và phát hiện thông tin ẩn trên máy tính

Phân tích dữ liệu bằng chứng tìm thấy

Chuẩn bị báo cáo phân tích

Cập nhật tổ chức về các phương pháp tấn công khác nhau và kỹ thuật khôi phục dữ liệu, và duy trì hồ sơ của họ

Giải quyết vấn đề tại tòa án của pháp luật và cố gắng thắng kiện bằng cách làm chứng trước tòa

## What Makes a Good Computer Forensics Investigator?

Kỹ năng phỏng vấn để thu thập thông tin sâu rộng về vụ án từ khách hàng hoặc nạn nhân, nhân chứng và nghi phạm

Kỹ năng nghiên cứu để biết lý lịch và các hoạt động liên quan đến khách hàng hoặc nạn nhân, nhân chứng và nghi phạm

Duy trì độ chính xác hoàn hảo của các thử nghiệm được thực hiện và hồ sơ của chúng

Kiên nhẫn và sẵn sàng làm việc nhiều giờ

Kỹ năng viết tuyệt vời để chi tiết hóa các phát hiện trong báo cáo

Kỹ năng phân tích mạnh mẽ để tìm bằng chứng và liên kết nó với nghi phạm Thông minh

Kỹ năng giao tiếp để giải thích những phát hiện của họ cho khán giả

Vẫn được cập nhật về các phương pháp mới và công nghệ pháp y

Thành thạo nhiều nền tảng máy tính (bao gồm Windows, Macintosh và Linux)

Kiến thức về các công nghệ, phần cứng và phần mềm khác nhau

Phát triển và duy trì liên lạc với các chuyên gia máy tính, mạng và điều tra

Trung thực, đạo đức và tuân thủ pháp luật

Có kiến thức về các luật liên quan đến vụ án

Khả năng kiểm soát cảm xúc khi xử lý vấn đề gây phẫn nộ

Chuyên môn đa ngành liên quan đến cả vụ án hình sự và dân sự

## Accessing Computer Forensics Resource

Tham gia các nhóm thảo luận và hiệp hội khác nhau để truy cập các tài nguyên liên quan đến pháp y máy tính

Các hiệp hội cung cấp thông tin pháp y máy tính:

Mạng lưới điều tra viên công nghệ máy tính <http://www.ctin.org>

Hiệp hội điều tra tội phạm công nghệ cao <https://www.htcia.org>

Mạng lưới các chuyên gia pháp y máy tính và các chuyên gia khác

Các dịch vụ tin tức dành cho pháp y máy tính cũng có thể là một nguồn tài nguyên mạnh mẽ

Các tài nguyên khác: Tạp chí của các nhà điều tra pháp y Nghiên cứu trường hợp thực tế

# Module 02: Computer Forensics Investigation Process

# LO#01: Understand the Forensic Investigation Process and its Importance (Hiểu quy trình điều tra pháp y và tầm quan trọng của nó)

Mục tiêu kiểm tra / điều tra

Các nhà điều tra nên có một ý tưởng rõ ràng về các mục tiêu của việc kiểm tra trước khi tiến hành điều tra

Họ nên có một sự hiểu biết kỹ thuật sâu sắc về hoạt động bên trong của những gì đang được kiểm tra

Họ nên có khả năng thực hiện một cách tiếp cận có hệ thống để kiểm tra bằng chứng dựa trên yêu cầu được đưa ra, ví dụ, Yêu cầu của luật sư

Xây dựng giả thuyết / Tiêu chí

Nếu khách hàng đã hỏi bạn một câu hỏi, hãy suy nghĩ về nó. Làm thế nào bạn có thể chứng minh (giả thuyết) hoặc bác bỏ (giả thuyết null) nó. Ví dụ: nếu bạn được yêu cầu kiểm tra cài đặt Dropbox trên ổ cứng nghi ngờ, hãy xem xét:

Hệ điều hành (0S) được cài đặt, vì các tạo tác cần kiểm tra

Cài đặt Dropbox khác nhau đối với mỗi hệ điều hành

Nghiên cứu trước đây vì nó có thể giúp bạn nếu nó có sẵn cho câu hỏi đã cho

Dựa trên những cân nhắc trên, hãy thiết lập một hình thức lý luận sẽ giúp bạn hình thành một giả thuyết Ví dụ đã cho, Giả thuyết có thể như sau: Hệ điều hành được cài đặt là Windows 10 Dropbox được cho là được cài đặt trên hệ thống nếu các tạo tác của nó nằm trong các thư mục: C: Users Admin AppData Roaming hoặc C: Program Files (x86) hoặc C: Program Files

Lựa chọn công cụ

Các công cụ pháp y kỹ thuật số bao gồm:

-Phần mềm hoặc phần cứng

-Thương mại hoặc mã nguồn mở

-Được thiết kế cho các mục đích cụ thể hoặc với chức năng rộng hơn

Tốt hơn là xem xét các công cụ thương mại có giá trị thị trường lớn hơn các công cụ nguồn mở Sử dụng các công cụ được thiết kế cho các mục đích cụ thể sẽ cho phép một cuộc điều tra đa dạng và chuyên sâu diễn ra

Sử dụng nhiều công cụ xác nhận các phát hiện, do đó nâng cao độ tin cậy của bằng chứng

Xem xét và đánh giá kết quả

Xem xét kết quả của bạn từ các quan điểm khác nhau và truyền đạt kết quả cho khách hàng với những kỳ vọng thực tế về lý do và cách bạn đạt được kết quả của mình

Kết luận và xây dựng ý kiến

Kết luận là phán đoán dựa trên các sự kiện

Ví dụ, Cài đặt Dropbox trên hệ thống có thể được xác nhận về việc xác định các hiện vật của nó ở các vị trí được tìm thấy trong quá trình điều tra

Ý kiến là phán đoán hoặc niềm tin mà không có sự chắc chắn hoặc bằng chứng. Nó chỉ dựa trên khoa học và / hoặc kinh nghiệm

Ví dụ: dựa trên đánh giá của một số hiện vật, bạn có thể xác định chính xác thời điểm Dropbox được cài đặt

Nếu bạn phải làm chứng tại phiên tòa, bạn phải chuẩn bị để giải thích cách bạn đi đến kết luận hoặc ý kiến của mình

## Importance of the Forensic Investigation Process

Vì bằng chứng kỹ thuật số có bản chất mong manh, việc tuân theo các hướng dẫn nghiêm ngặt và quy trình điều tra pháp y kỹ lưỡng để đảm bảo tính toàn vẹn của bằng chứng là rất quan trọng để chứng minh một vụ án tại tòa án của pháp luật

Quá trình điều tra pháp y cần tuân thủ phải tuân thủ luật pháp địa phương và các tiền lệ đã được thiết lập. Bất kỳ vi phạm / sai lệch nào cũng có thể gây nguy hiểm cho cuộc điều tra hoàn chỉnh.

Các nhà điều tra phải tuân theo một tập hợp các bước có thể lặp lại và được ghi chép đầy đủ sao cho mọi lần lặp lại phân tích đều cung cấp cùng một phát hiện; Nếu không, những phát hiện của cuộc điều tra có thể bị vô hiệu trong quá trình kiểm tra chéo tại tòa án của pháp luật

# LO#02: Understand the Pre-investigation Phase (Hiểu giai đoạn tiền điều tra)

## Setting Up a Computer Forensics Lab

Phòng thí nghiệm pháp y máy tính (CFL) là một địa điểm chứa các công cụ, công cụ phần mềm và phần cứng, và các trạm pháp y cần thiết để tiến hành điều tra dựa trên máy tính liên quan đến bằng chứng thu thập được

Cân nhắc lập kế hoạch & lập ngân sách

Số trường hợp dự kiến

Loại điều tra

Nhân lực

Yêu cầu thiết bị và phần mềm

Cân nhắc thiết kế vật lý & kết cấu

Quy mô phòng thí nghiệm

Tiếp cận các dịch vụ thiết yếu

Ước tính không gian cho khu vực làm việc và lưu trữ bằng chứng

Hệ thống sưởi, thông gió và điều hòa không khí

Work area consideration

Yêu cầu máy trạm

Môi trường xung quanh Internet, mạng và đường dây liên lạc

Hệ thống chiếu sáng và nguồn điện khẩn cấp

Cân nhắc bảo mật vật lý

Đăng nhập điện tử

Hệ thống báo động xâm nhập

Hệ thống dập lửa

Giám sát hệ thống dập lửa

Cân nhắc về nguồn nhân lực

Số lượng nhân sự cần thiết

Đào tạo và chứng nhận

Cấp phép phòng thí nghiệm pháp y

Chứng nhận ASCLD / LAB

Chứng nhận ISO / IEC 17025

## Building the Investigation Team (Xây dựng đoàn điều tra)

Giữ cho nhóm nhỏ để bảo vệ tính bảo mật của cuộc điều tra và bảo vệ chống rò rỉ thông tin

Xác định các thành viên trong nhóm và phân công trách nhiệm cho họ

Đảm bảo rằng mọi thành viên trong nhóm đều có sự giải phóng mặt bằng và ủy quyền cần thiết để thực hiện các nhiệm vụ được giao

Chỉ định một thành viên trong nhóm làm trưởng nhóm kỹ thuật cho cuộc điều tra

Những người tham gia vào một nhóm điều tra

Photographer (Nhiếp ảnh gia): Hình ảnh hiện trường vụ án và bằng chứng thu thập được

Incident Responder (Ứng phó sự cố): Chịu trách nhiệm về các biện pháp cần thực hiện khi có sự cố xảy ra

Incident Analyzer (Máy phân tích sự cố): Phân tích các sự cố dựa trên sự xuất hiện của chúng

Evidence Examiner/Investigator (Người kiểm tra bằng chứng/ điều tra viên): Kiểm tra bằng chứng thu được và sắp xếp các bằng chứng hữu ích

Evidence Documenter (Tài liệu bằng chứng): Ghi lại tất cả các chứng cứ và các giai đoạn có mặt trong quá trình điều tra

Evidence Manager (Người quản lý bằng chứng): Quản lý bằng chứng theo cách được chấp nhận tại tòa án của pháp luật

Evidence Witness (Nhân chứng chứng cứ): Đưa ra ý kiến chính thức dưới dạng lời khai tại tòa án của pháp luật

Attorney (Luật sư): Cung cấp dịch vụ hỗ trợ pháp lý

## Understanding the Hardware and Software Requirements of a Forensic Lab (Hiểu các yêu cầu phần cứng và phần mềm của phòng thí nghiệm pháp y)

Một phòng thí nghiệm pháp y kỹ thuật số nên có tất cả các công cụ phần cứng và phần mềm cần thiết để hỗ trợ quá trình điều tra, bắt đầu từ tìm kiếm và thu giữ bằng chứng đến báo cáo kết quả phân tích

Hardware

Hai hoặc nhiều máy trạm pháp y có sức mạnh xử lý và RAM tốt

Cáp chuyên dụng

Trình chặn ghi

Máy sao chép ổ đĩa

Lưu trữ và khôi phục thiết bị

Hệ thống khử trùng phương tiện

Các thiết bị khác cho phép các công cụ phần mềm pháp y hoạt động

Bộ công cụ phần cứng pháp y máy tính, chẳng hạn như Gói phản hồi đầu tiên của Paraben, Máy ảnh đĩa DeepSpar, Máy trạm pháp y FRED, v.v

Software

Hệ điều hành

Công cụ khám phá dữ liệu

Công cụ bẻ khóa mật khẩu

Công cụ thu thập

Máy phân tích dữ liệu

Công cụ khôi phục dữ liệu

Trình xem tệp (Hình ảnh và đồ họa

Công cụ chuyển đổi loại tệp

Phần mềm bảo mật và tiện ích

Các công cụ phần mềm pháp y máy tính như Wireshark, Cain và Abel, FTK của Access Data, v.v

## Validating Laboratory Software and Hardware (Xác thực phần mềm và phần cứng phòng thí nghiệm)

Các công cụ pháp y phải trải qua quá trình xác nhận trước khi sử dụng chúng cho một trường hợp cũng như mỗi lần chúng được sửa đổi hoặc cập nhật

Một công cụ được cho là được xác nhận nếu nó hoạt động chính xác, đáng tin cậy và mang lại kết quả chính xác

Tất cả các công cụ phần mềm (từ hệ điều hành đến ứng dụng) trong phòng thí nghiệm pháp y phải luôn có giấy phép

Cập nhật công cụ lên phiên bản mới nhất của chúng, Kiểm tra chức năng của chúng và xác nhận chúng phải là một quá trình liên tục

Các thiết bị phần cứng phải ở trong tình trạng hoạt động và phải được bảo trì đúng cách

Mỗi lần công cụ được kiểm tra, điều tra viên cần ghi lại phương pháp kiểm tra, kết quả và lý thuyết liên quan đến thiết kế thử nghiệm

Nên tích hợp duy trì, kiểm toán, lập hồ sơ và chứng minh sự tuân thủ giấy phép vào quy trình vận hành tiêu chuẩn phòng thí nghiệm (SOP)

Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) đã khởi động Dự án Kiểm tra Công cụ Pháp y Máy tính (CFTT), thiết lập một "phương pháp để kiểm tra các công cụ phần mềm pháp y máy tính bằng cách phát triển các thông số kỹ thuật chung của công cụ, quy trình kiểm tra, tiêu chí kiểm tra, bộ thử nghiệm và phần cứng thử nghiệm

## Ensuring Quality Assurance (Đảm bảo chất lượng)

Đảm bảo chất lượng đóng một vai trò quan trọng trong việc đảm bảo chất lượng dịch vụ tổng thể mà một đơn vị pháp y cung cấp

Sau các quy trình được ghi chép đầy đủ, có hệ thống để đảm bảo chất lượng cũng hoạt động như một bằng chứng về thực tế rằng cuộc điều tra pháp y đã được thực hiện với chất lượng và tiêu chuẩn cao nhất có thể, dẫn đến kết quả đáng tin cậy

Steps to Ensure Quality Assurance in Forensic Lab Operations (Các bước đảm bảo đảm bảo chất lượng trong hoạt động pháp y)

1. Sắp xếp đào tạo chính thức, tài liệu

2. Xác nhận thiết bị và ghi lại nó

3. Tiến hành kiểm tra năng lực hàng năm cho điều tra viên

4. Thực hiện theo các tiêu chuẩn và / hoặc kiểm soát thích hợp trong trường hợp

5. Có các chính sách và thủ tục để điều tra pháp y hiệu quả

6. Đạt được chứng nhận ASCLD / LAB và / hoặc chứng nhận ISO / IEC 17025

7. Thực hiện đánh giá chất lượng và đánh giá hệ thống quản lý chất lượng

8. Đảm bảo an ninh thực vật

9. Đảm bảo health và an toàn

10. Xem xét, cập nhật và lập hồ sơ chính sách và tiêu chuẩn hàng năm

# LO#03: Understand First Response

## First Response Basics

Thuật ngữ người phản ứng đầu tiên đề cập đến một người đến hiện trường vụ án trước

Phản ứng đầu tiên đối với bất kỳ sự cố an ninh nào có thể được thực hiện bởi một đến ba nhóm cá nhân khác nhau, những người có các kỹ năng khác nhau và có thể thực hiện các nhiệm vụ khác nhau dựa trên loại và mức độ nghiêm trọng của sự cố:

-Phản ứng đầu tiên của nhân viên không phải pháp y

-Phản ứng đầu tiên của quản trị viên hệ thống / mạng

-Phản ứng đầu tiên của nhân viên pháp y phòng thí nghiệm

Trong mọi trường hợp, bất cứ ai ngoại trừ pháp y đủ điều kiện không được phép Các nhà phân tích thực hiện bất kỳ nỗ lực nào để thu thập hoặc khôi phục dữ liệu từ bất kỳ hệ thống máy tính hoặc thiết bị nào chứa thông tin điện tử

Bất kỳ nỗ lực nào để khôi phục dữ liệu của những người chưa được đào tạo đều có thể làm tổn hại đến tính toàn vẹn của các tệp hoặc dẫn đến các tệp không được chấp nhận trong thủ tục hành chính hoặc pháp lý

## First Response by Non-forensics Staff (Phản ứng đầu tiên của nhân viên không pháp y)

Nhân viên pháp y không có trách nhiệm bảo vệ hiện trường vụ án và đảm bảo rằng nó vẫn ở trạng thái an toàn cho đến khi nhóm pháp y khuyên khác

Họ nên ghi chú và chụp ảnh hiện trường và những người có mặt để bàn giao cho đội pháp y tham dự

Khu vực xung quanh liên quan đến vụ việc cũng phải được bảo vệ cùng với các hệ thống máy tính hoặc các thiết bị điện tử khác

## First Response by System/Network Administrators (Phản hồi đầu tiên của quản trị viên hệ thống / mạng)

Khi quản trị viên hệ thống phát hiện ra sự cố, nó phải được báo cáo theo quy trình báo cáo sự cố tổ chức hiện tại

Quản trị viên hệ thống không nên thực hiện bất kỳ hành động nào trừ khi được chỉ đạo bởi người quản lý sự cố / nhiệm vụ hoặc một trong những nhà phân tích pháp y được chỉ định cho vụ việc

Dựa trên sự cố đã xảy ra, quản trị viên hệ thống / mạng có thể thực hiện các biện pháp sau:

-Ghi lại những gì trên màn hình nếu máy tính được bật

-Chuyển các bản sao của nhật ký hệ thống lên một phương tiện sạch

-Nếu một cuộc tấn công đang diễn ra được phát hiện, hãy tìm kiếm sự chấp thuận của quản lý cấp cao trước khi tắt nguồn bất kỳ hệ thống máy tính nào

-Cách ly các hệ thống máy tính hoặc các thiết bị kỹ thuật số khác khỏi việc sử dụng thêm hoặc giả mạo

-Ghi lại mọi chi tiết liên quan đến sự cố

## First Response by Laboratory Forensics Staff (Phản ứng đầu tiên của nhân viên pháp y phòng thí nghiệm)

1. Ghi lại cảnh tội phạm điện tử

-Chụp ảnh hiện trường

-Phác thảo hiện trường

2. Thu thập thông tin sự cố

-Đặt câu hỏi

-Thực hiện các cuộc phỏng vấn cá nhân

3. Lập kế hoạch tìm kiếm và thu giữ

-Nhận lệnh khám xét để khám xét và thu giữ

-Kiểm tra các vấn đề về sự đồng ý

-Lấy chữ ký của nhân chứng

4. Xác định và thu thập bằng chứng điện tử

-Tiến hành khám xét hiện trường ban đầu

-Bảo vệ và đánh giá hiện trường vụ án

-Thu giữ chứng cứ

-Xử lý các thiết bị đã tắt nguồn hoặc bật nguồn tại thời điểm thu giữ

5. Bao bì bằng chứng điện tử

-Lấp đầy bảng điều khiển ở mặt trước của túi bằng chứng với các chi tiết thích hợp

-Tránh gấp và trầy xước các thiết bị lưu trữ

-Dán nhãn các thùng chứa bằng chứng một cách thích hợp

6. Vận chuyển bằng chứng điện tử

-Đảm bảo xử lý và vận chuyển bằng chứng đúng cách đến phòng thí nghiệm pháp y

-Đảm bảo "Chuỗi hành trình" được tuân thủ nghiêm ngặt

# LO#04: Understand the Investigation Phase (Hiểu giai đoạn điều tra)

## Phương pháp điều tra pháp y máy tính (Computer Forensics Investigation)

1. Ghi lại hiện trường vụ án điện tử

2. Tìm kiếm và thu giữ

3. Bảo quản chứng cứ

4. Thu thập dữ liệu

5. Phân tích dữ liệu

6. Phân tích trường hợp

7. Báo cáo

8. Làm chứng với tư cách là nhân chứng chuyên gia