|  |
| --- |
| BAN CƠ YẾU CHÍNH PHỦ  **HỌC VIỆN KỸ THUẬT MẬT MÃ**  ¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯  Logo HvKTMM |
| **Phòng chống và điều tra tội phạm máy tính**  Đề tài  **Dịch: Global guidelines for DF laboratories  chapter 6.7**  Chuyên ngành: An toàn thông tin |
| ***Sinh viên* *thực hiện*:**   * Phạm Huy Hùng * Đào Xuân Huy * Nguyễn Công Thắng |
| Hà Nội, 7/12/2019 |

**6. BẢO ĐẢM CHẤT LƯỢNG**

Khi trình bày các báo cáo pháp y tại tòa án, những người khám xét có thể không chỉ được yêu cầu giải thích quá trình nghiên cứu. Họ cũng sẽ được yêu cầu giải thích năng lực của bản thân, thiết bị mà họ sử dụng, phương pháp mà họ chọn, cách thức họ xử lí dấu vết, và nhiều hơn nữa. Điều quan trọng là các thủ tục để giải quyết những vấn đề trên được kiến lập và thực hiện trong DFL.

Phần sau đây giải thích rõ ràng hơn về các thành phần, cũng như sự công nhận cần đạt được.

**6.1. Thành phần đảm bảo chất lượng**

Sự đảm bảo chất lượng cơ bản có thể được tiến hành trong một DFL bao gồm, nhưng không giới hạn:

|  |  |
| --- | --- |
| **Danh sách kiểm tra thành phần đảm bảo chất lượng** | |
| **Phòng thí nghiệm** | a, Tạo một biểu đồ tổ chức ở cấp độ DFL và cấp độ tổ chức.  b, Thực hiện kiểm toán nội bộ hang năm.  c, Thiết lập một thủ tục để giải quyết các khiếu nại nội bộ và bên ngoài.  d, Thiết lập một thủ tục để kiểm soát tài liệu. |
| **Điều kiện cơ sở và môi trường** | a, Thiết lập cơ sở thí nghiệm – truy cập và thoát hiểm.  b, Tạo ra một danh sách truy cập và được giới hạn bởi sử dụng khóa, thẻ nhận dạng cá nhận, hay thiết bị sinh trắc học.  c, Theo dõi môi trường phòng thí nghiệm thường xuyên – nhiệt độ, độ ẩm, độ sạch.  d, Thiết lập một chương trình sức khỏe và an toàn.  e, Thiết lập chính sách khách hàng truy cập.  f, Tiến hành dọn dẹp thường xuyên. |
| **Trang thiết bị** | a, Thiết lập một thủ tục để xử lý, vận chuyển, lưu trữ, sử dụng, sửa chữa, vứt bỏ và bảo trì kế hoạch cho các thiết bị.  b, Trước khi đưa vào sử dụng, đảm bảo rằng các thiết bị đang hoạt động theo thông số kỹ thuật.  c, Thực hiện chương trình bảo trì.  d, Cập nhật chương trình cơ sở theo yêu cầu.  e, Duy trì tài liệu thiết bị, hướng dẫn sử dụng và đảm bảo. |
| **Nhân viên** | a, Trình độ tuyển dụng:   * Tiến hành kiểm tra lý lịch trước khi thuê. * Chuẩn bị mô tả công việc cho nhân viên một khi đã được thuê – Xem ở phần 3.3 Nhân viên.   b, Phát triển và đào tạo chuyên nghiệp:   * Thiết lập một chương trình đào tạo cho nhân viên – xem phần 3.3.4 Phất triển nhân viên. * Gửi nhân viên đào tạo. * Chỉ định các cố vấn cho nhân viên mới được thuê. * Đánh giá năng lực của nhân viên bằng cách tiến hành kiểm tra năng lực cho nhân viên mới được thuê. * Đánh giá mức độ thành thạo của nhân viên hiện có bằng cách tiên hành kiểm tra trình độ hàng năm. * Tham gia các bài kiểm tra trình độ bên ngoài hoặc liên quan phòng thí nghiệm. * Đạt chứng chỉ kĩ thuật.   Thiết lập một chương trình giáo dục liên tục cho nhân viên hiện có để duy trì kỹ năng. |
| **Phương thức pháp y** | a, Thiết lập các SOP để thực hiện các kỳ thi DF.  b, Giữ một tài liệu về các phương thức pháp y, chẳng hạn như tiến hành mua lại trực tiếp, cập nhật và cso sẵn cho người khám xét.  c, Tiến hành xác minh về các phương pháp được giới thiệu để đảm bảo DFL có thể sử dụng chúng đúng cách.  d, Tiến hành xác nhận khi sử dụng bất kỳ phương pháp nào: phương pháp phi tiêu chuẩn, phương pháp phát triển phòng thí nghiệm hoặc phương pháp tiêu chuẩn được sử dụng bên ngoài phạm vi của nó.  e, Để dễ vận hành, sử dụng phương pháp được chấp nhận trên quốc tế trong DFL, chẳng hạn như SWGDE. |
| **Yêu cầu dịch vụ** | Thiết lập và thực hiện một chính sách và thủ tục theo yêu cầu dịch vụ. Điều này bao gồm:   1. Quá trình chấp nhận và từ chối yêu cầu. 2. Quá trình nộp lại yêu cầu. 3. Yêu cầu để có một yêu cầu ngắn gọn và trường hợp khách quan. 4. Sự thừa nhận chính thức từ nhà yêu cầu và người khám xét, chỉ ra rằng cả hai bên đều chấp thuận với công việc trước khi công việc pháp y bắt đầu và sau khi nó được chuyển giao – bằng cách kí một giao kết, trả lời một e- mail hoặc trả lời một lá thư. 5. Các hình thức hoặc phương thức khác được sử dụng để ghi lại yêu cầu.   Xem phụ lục L: Mẫu yêu cầu dịch vụ DFL nội suy cho một mẫu của mẫu yêu cầu. |
| **Xử lí bằng chứng** | Thiết lập và thực hiện một chính sách và thủ tục xử lý bằng chứng. Điều này bao gồm:   1. Bảo quản bằng chứng 2. Ghi nhãn bằng chứng 3. Niêm phong bằng chứng 4. Các mục cần làm tài liệu – bao gồm cả chuỗi hành trình sản phẩm. 5. Các biện pháp phòng ngừa để bảo mật và xử lý các bằng chứng 6. Lưu trữ và lưu giữ   Xem phụ lục K: Xử lý bằng chứng điện tử để biết chi tiết về xử lý bằng chứng. |
| **Kết quả pháp y** | a, Giữ hồ sơ kỹ thuật để hỗ trợ kết quả pháp y. Các hồ sơ phải cho biết ngày và quá trình người khám xét tiến hành. Sửa đổi hồ sơ trước đó phải được theo dõi.  b, Tiến hành rà soát kỹ thuật và hành chính về kết quả pháp y.  c, Ủy quyền kết quả pháp y trước khi nhượng lại cho người yêu cầu  d, Thiết lập một định dạng phổ biến cho một báo cáo pháp y.  Xem phụ lục J: Yêu cầu phổ biến cho báo cáo pháp y  e, Khi cung cấp một ý kiến, nó phải được đánh dấu rõ ràng trong báo cáo pháp y.  f, Thiết lập một quá trình sửa đổi một báo cáo pháp y. |

**6.2. Công nhận DFL**

Kết quả pháp y tác động đến hệ thống tài phán, vì vậy chúng cần phải chính xác và đáng tin cậy. DFL có thể đảm bảo và chứng minh sự tự tin vào kết quả pháp y bằng cách tham gia chương trình kiểm định. Cơ quan công nhận sẽ đánh giá tiến độ DFL trên cơ sở hàng năm để đảm bảo nó đáp ứng tiêu chuẩn toàn cầu.

Mặc dù tham gia chương trình kiểm định được khuyến nghị, nói chung nó là tự nguyện và không bắt buộc ở hầu hết các quốc gia. Một DFL được xen kẽ trong chương trình kiểm định có thể tham khảo cơ quan cộng đồng của chính quốc gia đó để biết chi tiết về quy trình.

Một số lợi ích đáng chú ý của việc được công nhận là:

|  |  |
| --- | --- |
| **Lợi ích của phòng thí nghiệm kiểm định** | |
| 1 | Đảm bảo sự tín nhiệm trong kết quả pháp y  Khi một DFL nhận được nhiều trường hợp trong một năm, nói chung là khó khăn cho các phòng thí nghiệm để theo dõi hiệu suất của các công việc pháp y và của khám xét. Tiêu chuẩn ISO 17025 xác định quá trình giám sát khía cạnh chất lượng của kết quả pháp y.  Với sự kiểm định, quá trình này sẽ được kiểm định hàng năm để đảm bảo phòng thí nghiệm tiếp tục duy trì hiệu quả hoạt động. Ngoài ra, quá trình quản lý và kiểm tra các bằng chứng phải tuân theo tiêu chuẩn quốc tế, cung cấp sự tín nhiệm cho các bên liên quan trong kết quả pháp y do DFL sản xuất. |
| 2 | Hệ thống hơn với các quy trình được tiêu chuẩn hóa  Một DFL với một số người khám xét phải đảm bảo rằng mỗi người tuân theo cùng một bộ quy trình. Điều này là để đảm bảo rằng những lời chứng thực tại tòa án được thống nhất giữa mỗi người khám xét đến từ cùng một DFL, do đó tạo điều kiện cho sự hiểu biết ngay lập tức của công tố viên, thẩm phán và nhân viên tòa án khác. Việc chứng nhận gọn gang này đảm bảo DFL thiết lập các quy trình chuẩn, và cũng đảm bảo người khám xét thực hiện chúng |
| 3 | Sản xuất kết quả chất lượng  Một trong những yêu cầu trong ISO 17025 là để tiến hành cải tiến liên tục cho các quá trình phòng thí nghiệm. DFL có thể được hưởng lợi ích từ việc kiểm định bằng cách tiếp tục tiến hành cải tiến và đảm bảo phòng thí nghiệm tạo ra kết quả chất lượng hơn. Một ví dụ về việc thực hiện như vậy là lời khai của tòa án giám sát. Người khám xét có thể cải thiện phương thức trình bày của họ tại tòa án nếu họ được giám sát và cung cấp thông tin phản hồi mang tính xây dựng |

7. Tóm tắt

Bằng chứng điện tử đã đặt ra những thách thức đối với việc điều tra một số trường hợp, do bản chất của nó, đó là duy nhất và khác với các loại bằng chứng truyền thống. Do đó, nó phải được xử lý với sự quan tâm đúng mức Mục đích của tài liệu này là cung cấp các hướng dẫn tiêu chuẩn cho ban quản lý của một DFL, và để kiểm tra bằng chứng điện tử. Điều này là để đảm bảo rằng điện tử bằng chứng và kết quả do các quốc gia thành viên INTERPOL tạo ra được chấp nhận ở các nước khác quyền tài phán. Giám khảo và quản lý DFL phải luôn cố gắng cập nhật các phương pháp, hướng dẫn, và thủ tục với những tiến bộ hiện tại trong công nghệ. Chỉ sau đó chúng ta có thể cùng nhau hạ bệ tội phạm và phục vụ công lý vì nó cần được phục vụ.

PHỤ LỤC A: KIỂM TRA KỸ NĂNG DFL

Sau đây là khuyến nghị về các kỹ năng cho DFL . Người đọc cần lưu ý

rằng danh sách này không đầy đủ và cần được cập nhật theo thời gian.

|  |  |  |  |
| --- | --- | --- | --- |
| Danh mục | Đề tài | Kỹ năng |  |
| Nền tàng | Nền tảng máy tính | Cách tổ chức của máy tính, lưu trữ dữ liệu như thế nào; Bits & bytes; Sự phát triển của kỹ thuật số và hệ thống lưu trữ |  |
| File hệ thống | Số thập phân; số thập phận hệ mười sáu; nhị phân;endian; Sectors, cluster, slack space; Metadata, data, filename; FAT,  NTFS, EXT, HFS. |  |
| Giới thiệu về cuộc điều tra | Thực thi pháp luật và các cơ quan quản lý;Giới thiệu về khoa học pháp y, điện tử bằng chứng và bản chất của nó; Thể loại bằng chứng điện tử; Phương pháp luận;Thuật ngữ pháp y. |  |
| Nhận biết | Thu nhập thông tin | Thu thập sự thật của vụ án trực tuyến; Bảo quản  các sự kiện thu thập được. |  |
| Bộ sưu tập và kiểm tra | Bộ sưu tập và kiểm tra | Vai trò phản hồi đầu tiên và SOP; Đã chết mua lại và mua lại trực tiếp; Lựa chọn phương pháp thu thập dữ liệu tốt nhất; Bộ ba phương pháp; Công cụ xử lý. |  |
| Phân tích | Phục hồi dữ liệu | Công nghệ lưu trữ; Đĩa cứng bị hư và các triệu chứng ổ đĩa flash; Hợp lý và  phục hồi thể chất; Công cụ phục hồi dữ liệu; Phục hồi dữ liệu bằng các công cụ. |  |
|  | Pháp y máy tính | Hệ điều hành công nghệ; Metadata,  đăng ký, hiện vật; Khai thác dữ liệu; Dữ liệu  phân tích; Kỹ thuật ẩn dữ liệu; phân tích  cho các bộ dữ liệu lớn; Phân tích bộ nhớ |  |
|  | Pháp y điện thoại di động | Công nghệ điện thoại di động và sự phát triển người dùng, nhà cung cấp viễn thông công nghệ, loại dữ liệu, thu nhận và công cụ phân tích, bảo quản dữ liệu. |  |
|  | Pháp y mạng | Các loại mạng, tập tin lịch sử Internet và cookies, thông tin người dùng, mạng công cụ pháp y, đọc gói tin. |  |
|  | Âm thanh, Video và  Pháp y hình ảnh | Hiểu biết về công nghệ, tăng cường xác thực tập tin |  |
|  | Công nghệ mới nổi: - Pháp y truyền thông xã hội  - Pháp y cơ sở dữ liệu  - Pháp y Drone  - Pháp y xe cộ  - Pháp y shipbourne  - Pháp y tiền điện tử  - Pháp y sinh trắc học | Hiểu biết về công nghệ, truy cập dữ liệu từ thiết bị, khai thác dữ liệu, phân tích dữ liệu, giải thích dữ liệu, báo cáo và phát hiện |  |
| Trình bày | Viết báo cáo | Định dạng của báo cáo, kết quả hiệu quả trình bày trước các bên liên quan. |  |
|  | Tòa án Law & Mock | Pháp luật liên quan đến vụ án, luật quốc tế, hợp tác quốc tế, trình bày lời khai của chuyên gia tại tòa án, Giới thiệu về cơ cấu tòa án, đệ trình điện tử chứng cứ trước tòa. |  |
| Phép lịch sự | Phép lịch sự | Quy tắc đạo đức nghề nghiệp, đạo đức & phi- quy tắc đạo đức ứng xử. |  |
| Sự quản lý phòng thí nghiệm | Quản lý chất lượng | Hiểu tiêu chuẩn, tiến hành kiểm toán, hệ thống quản lý chất lượng |  |
| An toàn và sức khỏe | Xác định các mối nguy hiểm về sức khỏe và sự an toàn,  biện pháp tự bảo vệ. |

PHỤ LỤC B: KIỂM TRA THIẾT BỊ DFL CƠ BẢN

Sau đây là danh sách đề xuất các thiết bị cơ bản mà DFL nên sở hữu. Người đọc nên

lưu ý rằng danh sách này là không đầy đủ và nhiều hơn nữa có thể được yêu cầu tùy theo tính chất của các trường hợp nhận.

|  |  |  |
| --- | --- | --- |
|  | Mục |  |
| 1 | Laptop |  |
| 2 | Phần mềm phân tích máy tính |  |
| 3 | Phần mềm khôi phục dữ liệu |  |
| 4 | Phần mềm phân tích thiết bị di động |  |
| 5 | Phần mềm phân tích vật phẩm Internet |  |
| 6 | Phần mềm máy ảo |  |
| 7 | Phần cứng hình ảnh |  |
| 8 | Hệ thống lắp ghép |  |
| 9 | Viết chặn |  |
| 10 | Phương tiện lưu trữ trống - để lưu trữ dữ liệu được trích xuất từ ​​điện tử bằng chứng trong ngắn hạn và dài hạn:  • Ổ đĩa bút  • Đĩa cứng ngoài  • Đĩa cứng  • Máy chủ |  |
| 11 | Bộ công cụ PC |  |
| 12 | Mở rộng cáp điện |  |
| 13 | Máy in |  |
| 14 | Máy hủy tài liệu |  |

PHỤ LỤC C: MẪU HÌNH THỨC ĐĂNG KÝ TRƯỜNG HỢP

|  |  |
| --- | --- |
| Yêu cầu thông tin cơ quan | |
| Tên:  Chức danh:  Số điện thoại:  Email: | Chi nhánh/Đơn vị:  Nơi làm việc:  Số trường hợp người yêu cầu:  Số trường hợp DFL: |

|  |
| --- |
| Thông tin trường hợp: |
| Trường hợp phía sau: |
| Trường hợp cụ thể: |

|  |
| --- |
| Các điều khoản và điều kiện |
| 1. Lựa chọn phương pháp: DFL sẽ chọn phương pháp tốt nhất hiện có để tiến hành phân tích pháp y kỹ thuật số |
| 1. Tuyên bố bảo mật: DFL đảm bảo rằng bất kỳ thông tin nào được cung cấp bởi người yêu cầu và bất kỳ thông tin nào được thu thập từ công việc được thực hiện sẽ được xử lý với CẤU TẠO CHIẾN LƯỢC |
| 1. Thiệt hại hoặc mất lợi nhuận: DFL sẽ không chịu trách nhiệm cho bất kỳ triển lãm bị thiệt hại hoặc mất lợi nhuận do Người yêu cầu gây ra liên quan đến công việc được thực hiện. DFL, tuy nhiên, sẽ có biện pháp phòng ngừa, chăm sóc và các bước hợp lý trong việc giữ gìn tính toàn vẹn của bằng chứng mọi lúc |
| 1. Triển lãm bị bỏ rơi hoặc không có yêu cầu: Triển lãm Không được yêu cầu hoặc bị bỏ rơi tại địa điểm của DFL trong hơn 30 ngày sau khi liên lạc được thực hiện với Người yêu cầu sẽ được xử lý theo quyết định của DFL. DFL sẽ không chịu trách nhiệm cho triển lãm còn lại trong quyền sở hữu của mình sau 30 ngày. DFL, tuy nhiên, sẽ thông báo cho Người yêu cầu trước khi xử lý tang vật. |

|  |  |
| --- | --- |
| Người yêu cầu | DFL |
| Tôi đã đọc, hiểu và đồng ý với các điều khoản và điều kiện.  Ngày: | Tên:  Ngày: |

PHỤ LỤC D: MẪU HÌNH THỨC ĐĂNG KÝ XUẤT HIỆN

Mục A: Nhận triển lãm

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Nhãn hiệu DFL triển lãm | Người sáng tạo | Tư cách | Mô tả | Số seri |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |  |
| --- | --- |
| Người yêu cầu | DFL |
| Tên:  Ngày: | Tên:  Ngày: |

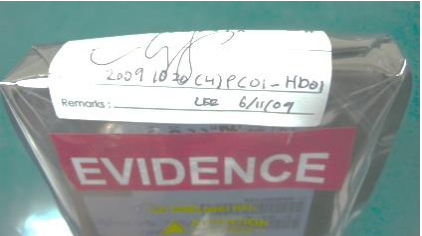
Mục B: Trở lại triển lãm

Tôi đã đồng ý rằng DFL đã trả lại tất cả các tang vật được liệt kê trong Phần A cho tôi. Khi ký vào cột trên, cả hai bên đã đồng ý rằng công việc đã hoàn thành và vụ việc được ký kết.

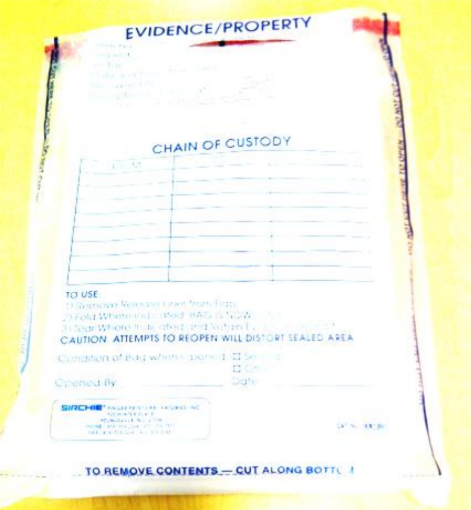
|  |  |
| --- | --- |
| Người yêu cầu | DFL |
| Tên:  Ngày: | Tên:  Ngày: |

PHỤ LỤC E: MẪU PHÂN BIỆT XUẤT HIỆN

Các cuộc triển lãm, một đĩa cứng được đặt trong một túi nhựa chống tĩnh điện và một nhãn dán chống giả mạo được đặt tại việc mở túi. Các giám khảo sau đó đặt tên anh/cô ấy viết tắt trên nhãn dán, cùng với nhãn triển lãm ngày và thời gian mà cuộc triển lãm là niêm phong.



Trong mẫu này, văn kiện đặt trong một túi nhựa chống làm giả. Chi tiết về văn kiện,giám khảo và chuỗi quyền nuôi con có sẵn trên túi nhựa.



PHỤ LỤC F: CÔNG TRÌNH LỰA CHỌN DỮ LIỆU

Một Bảng tính thu thập dữ liệu tiêu chuẩn sẽ được sử dụng trong bất kỳ hoạt động thu thập pháp y (hình ảnh) nào của một ổ cứng hoặc loại phương tiện truyền thông khác.

Image Acquisition Worksheet

|  |
| --- |
| Thông tin trường hợp |
| ID dự án (1): |
| Tên dự án / vấn đề (2): |
| Tên người giám sát (3): |
| Giám đốc dự án (5): |

|  |
| --- |
| MỤC TIÊU THÔNG TIN MÁY TÍNH |
| Vị trí của hệ thống (6): |
| Kiểu hệ thống (7): ☐Desktop ☐Laptop ☐Server ☐Other: |
| Loại bằng chứng(8): ☐Hard Drive ☐CD/DVD ☐Floppy ☐RAID ☐Other: |
| Trạng thái hệ thống (9): ☐On ☐Off ☐Logged On ☐Other: |
| BIOS Ngày /Thời gian (10): |
| Ngày giờ hiện tại (11): |
| Tổng số ổ cứng trong CPU (12): |
| Ổ cứng bị xóa bởi (13): |
| Ảnh chụp (14): ☐Yes ☐No – Lí do: |

Tán Thành

Tôi ủy quyền (nhập tên cơ quan) (và đại diện của họ) để sở hữu tất cả các thiết bị máy tính cần thiết cho cuộc điều tra của họ. (4)  
Chữ ký Vị trí

In tên Thời gian

(xx) Xem ghi chú hướng dẫn

|  |  |  |
| --- | --- | --- |
|  | Máy tính | Ổ cứng/khác |
| Người sáng tác: |  |  |
| Số mẫu |  |  |
| Mã số: |  |  |

|  |
| --- |
| Thông tin hình ảnh |
| Mua lại bởi (21): |
| Vị trí hình ảnh (22): |
| Phương pháp (23): ☐ EnCase (v. ) ☐ FTK (v. ) ☐ X-Ways:                                  ☐ dd Image ☐ Logical File Copy ☐ Other: |
| Phần cứng mua lại: ☐ Writeblocker ☐ Firewire W/B ☐ Bootdisk ☐  Direct Connection  ☐ SCSI-IDE W/B ☐ Xover Cable ☐ Other: |
| Bằng chứng truyền thông (25): ☐ Hard Drive ☐ Other: |
| Mã số (25): |
| Số ID ổ đĩa bằng chứng (25): |
| Kích cỡ ổ cứng: GB MB |
| Kích cỡ của ảnh: |
| Xác nhận ảnh: |
| Giá trị băm (30): |

|  |
| --- |
| GHI CHÚ  Phần này có sẵn để thêm ghi chú không được bao gồm trong tiêu chuẩn hình thức hoặc để mở rộng khi ghi chú, tức là các loại lỗi nhận được, các sự cố gặp phải trong quá trình quá trình hình ảnh. |
|  |
|  |
|  |

Hướng dẫn

THÔNG TIN TRƯỜNG HỢP

1. ID dự án - đề cập đến số được chỉ định cho vấn đề.

2. Tên vật chất - dùng để chỉ tên mã Tên của người được chỉ định bởi người quản lý dự án.

3. Tên người giám sát - dùng để chỉ người dùng cuối được gán máy tính.

4. Đồng ý - nếu cần có sự đồng ý để có được máy, hãy lấy chữ ký của người đó

Phát hành máy.

5. Trình quản lý - dùng để chỉ Người quản lý dự án được chỉ định dẫn dắt vụ việc.

MỤC TIÊU MÁY TÍNH THÔNG TIN

6. Vị trí của Hệ thống - địa chỉ của trang web, có thể bao gồm số văn phòng nếu máy tính được sử dụng

trực tiếp từ một văn phòng.

7. Loại hệ thống - cho biết máy có phải là máy tính để bàn, máy tính xách tay, máy chủ, v.v. Nếu thiết bị

là một ổ đĩa độc lập, hãy kiểm tra ’các loại khác và ghi vào drive ổ đĩa độc lập.

8. Loại bằng chứng - đánh dấu thiết bị được chụp / sao chép.

9. Trạng thái hệ thống - cho biết liệu máy nghi ngờ đã bật, tắt, đăng nhập, v.v. Nếu

Máy đang bật, cho biết ai đã tắt máy.

10. Ngày / Giờ của BIOS - đề cập đến bios từ máy nghi ngờ.

11. Ngày / Giờ hiện tại - đề cập đến ngày và giờ từ máy tính của giám khảo.

12. Tổng số ổ đĩa cứng trong máy tính - tự giải thích.

13. Ổ cứng bị xóa bởi - cho biết ai đã tháo rời máy tính.

14. Ảnh đã chụp - vui lòng cho biết liệu ảnh đã được chụp từ máy tính chưa và

ổ cứng Nếu câu trả lời là không, bạn phải giải thích tại sao không có bức ảnh nào được chụp.

MÁY VI TÍNH

15. Nhà sản xuất máy tính mục tiêu - loại máy và kích thước của ổ cứng.

16. Số mô hình - số mô hình của máy tính.

17. Số sê-ri - số sê-ri từ máy tính. Nếu có nhiều hơn một số sê-ri trên

máy, sao chép tất cả chúng CỨNG DRIVE / KHÁC.

18. Nhà sản xuất - loại ổ cứng.

19. Số Model - số model của ổ cứng.

20. Số sê-ri - số sê-ri từ ổ cứng. Nếu có nhiều số sê-ri tồn tại,

sao chép tất cả

THÔNG TIN LỰA CHỌN (điều này sẽ được hoàn thành hai lần, một cho mỗi hình ảnh).

21. Được mua bởi - đề cập đến người kiểm tra đã mua thiết bị.

22. Vị trí hình ảnh - cho biết máy có được chụp tại chỗ không, trong Phòng thí nghiệm - cho biết

phòng thí nghiệm nào, v.v.

23. Phương pháp mua lại - cho biết loại phần mềm được sử dụng để chụp ảnh thiết bị. Ghi chú

số phiên bản của phần mềm được sử dụng.

24. Phần cứng mua lại - cho biết loại mua lại, cho dù bạn đã sử dụng viết

khối thiết bị, cáp chéo, đĩa khởi động, vv

25. Evidence Media - dùng để chỉ ổ đĩa nơi hình ảnh sẽ được đặt. Chỉ ra ổ đĩa

Nhãn, số sê-ri và Số ID ổ đĩa bằng chứng.

26. Kích thước ổ đĩa - tổng kích thước ổ cứng tính bằng GB hoặc MB.

27. Kích thước của hình ảnh - cho biết tổng kích thước của hình ảnh (KHÔNG phải kích thước của ổ cứng), biểu thị

dù là GB hay MB.

28. Hình ảnh được xác minh - khi hình ảnh được hoàn thành và xác minh, hãy chọn hộp CÓ.

29. Lỗi - cho biết nếu có bất kỳ lỗi nào được tìm thấy trong quá trình xác minh. Nếu vậy, sử dụng

Ghi chú của Nhật Bản Phần trên mặt sau của tờ để ghi lại các lỗi cụ thể.

30. Giá trị băm - ghi lại giá trị băm được tạo trong quá trình tạo ảnh. Hãy chắc chắn kiểm tra

rằng giá trị băm mua lại và giá trị băm xác minh khớp.

PHỤ LỤC J: YÊU CẦU CHUNG CHO BÁO CÁO PHÁP Y

|  |  |  |
| --- | --- | --- |
| Yêu cầu chung cho báo cáo pháp y | | |
| 1 | | Chức vụ |
| 2 | | Tên và địa chỉ của phòng thí nghiệm |
| 3 | | Địa điểm thu thập và kiểm tra diễn ra |
| 4 | | Số trang và dấu hiệu kết thúc trang |
| 5 | | Tên người yêu cầu và thông tin liên lạc |
| 6 | | Phương pháp sử dụng đối với trường hợp |
| 7 | | Mô tả bằng chứng điện tử |
| 8 | | Ngày mà DFL nhận được bằng chứng |
| 9 | Ngày thi | |
| 10 | Ngày phát hành báo cáo | |
| 11 | Kết quả pháp y | |
| 12 | Tên và chức năng của người ủy quyền báo cáo | |

PHỤ LỤC K: XỬ LÝ SỰ KIỆN ĐIỆN TỬ

Sau đây là một gợi ý cơ bản để xử lý bằng chứng điện tử.

|  |  |
| --- | --- |
| Danh sách kiểm tra xử lý bằng chứng điện tử | |
| 1 | Nhãn  • Bằng chứng phải được dán nhãn duy nhất sau khi được gửi đến DFL. Nếu khó Đặt nhãn trên bằng chứng, DFL có thể dán nhãn lên con dấu bằng chứng.  • Nhãn phải ở trong suốt thời gian tồn tại của bằng chứng trong DFL.  • Nhãn cũng phải có khả năng theo dõi các mục phụ. Ví dụ: DFL-MP01 cho điện thoại di động và DFL-MP01-SIM01 cho thẻ Sim có trong điện thoại. |
| 2 | Niêm phong  • Bằng chứng phải được niêm phong bằng cách sử dụng một thùng chứa thích hợp.  • Container phải có khả năng phát hiện bất kỳ quyền truy cập nào được đưa ra bằng chứng.  • Con dấu phải được ký và ghi ngày tháng bởi Người kiểm tra.  • Mỗi lần truy cập bằng chứng, người làm như vậy phải niêm phong lại bằng chứng, một khi quá trình xử lý hoàn tất, mang chữ ký của anh ấy / cô ấy và ngày tháng. |
| 3 | Tài liệu  • Một hồ sơ đầy đủ các bằng chứng điện tử phải được thiết lập. Mục được ghi lại bao gồm  loại bằng chứng, số sê-ri, nhà sản xuất, bất kỳ lỗi và bất kỳ nhãn.  • Danh sách hàng tồn kho bằng chứng cũng phải được thiết lập trong DFL.  • Một chuỗi hồ sơ lưu ký phải được thiết lập cho từng mẩu bằng chứng điện tử.  Tối thiểu nó phải chứa một nhãn duy nhất, tên viết tắt và ngày. |
| 4 | Không bỏ mặc  • Bằng chứng không trong quá trình kiểm tra do Examiner Vay nghỉ phép dài hạn hoặc  Giám khảo tập trung vào các trường hợp ưu tiên cao không được bỏ mặc trong DFL. Nó  phải được lưu trữ đúng cách để tránh ô nhiễm.  • Bằng chứng cũng không được bỏ mặc trong quá trình vận chuyển. |
| 5 | Tránh xa nguồn ô nhiễm  • Bằng chứng điện tử phải được thực hiện đúng cách chăm sóc và được giữ cách xa nguồn ô nhiễm, chẳng hạn như nước, nhiệt, độ ẩm cực cao và trường điện từ. |
| 6 | Lưu trữ  • Bằng chứng điện tử phải được lưu trữ ở nơi an toàn, với quyền truy cập hạn chế. • Phải lưu giữ hồ sơ đăng ký và kiểm tra bằng chứng từ Phòng lưu trữ cập nhật. |
| 7 | Sự bảo tồn  • Phải sao chép bằng chứng điện tử gốc để bảo vệ tính toàn vẹn của  bằng chứng gốc.  • Giá trị băm của bằng chứng gốc và bản sao của nó phải giống nhau.  • Kiểm tra và phân tích phải được tiến hành trên bản sao bằng chứng điện tử. |