TRƯỜNG ĐH CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH & TRUYỀN THÔNG

Digital Forensics
Pháp chứng Kỹ thuật số

#1: Overview
Spring 2023

ThS. Lê Đức Thịnh
thinhld@uit.edu.vn

Nội dung trình bày

- Các khái niệm về Digital Forensics (DF)
- Các vấn đề cần quan tâm khi làm về DF
- Nghề DF
- Đạo đức trong DF
- DF trong CTF

Forensics?

- Pháp chứng là một ngành khoa học, nó sử dụng những thành tựu khoa học trong lĩnh vực y học, sinh học, hoá học, vật lí học, tin học... để đáp ứng những yêu cầu của pháp luật trong hoạt động tố tụng hình sự và dân sự thông qua hoạt động giám định khi được các cơ quan trưng cầu.

Edmond Locard

Các công việc của Forensics?

- Điều tra, tìm kiếm các thông tin, dữ liệu nhằm xác định thủ phạm hoặc nguồn gốc phát sinh sự việc.
- Tìm kiếm chứng cứ căn cứ vào các dấu vết còn lại tại hiện trường.
- Căn cứ vào các thông tin trong các tàng thư lưu trữ trong quá khứ.
- Sử dụng các phương pháp điều tra hiện đại và phân tích Logic – đúng pháp luật.

Digital Forensics?

- Pháp chứng kỹ thuật số là tìm kiếm, duy trì và phân tích thông tin trên hệ thống máy tính để tìm kiếm các bằng chứng phục vụ cho việc điều tra tội phạm hay dùng trong các công tác quản trị hệ thống thông tin.
- Mục tiêu cốt lõi của "***Computer Forensic***" là phát hiện, bảo quản, khai thác, tài liệu hóa và đưa ra kết luận về dữ liệu thu thập được. Cần lưu ý rằng dữ liệu phải đảm bảo tính xác thực và được lấy mà không bị hư hại, nếu không dữ liệu đấy sẽ không còn ý nghĩa.

Forensics vs Investigate

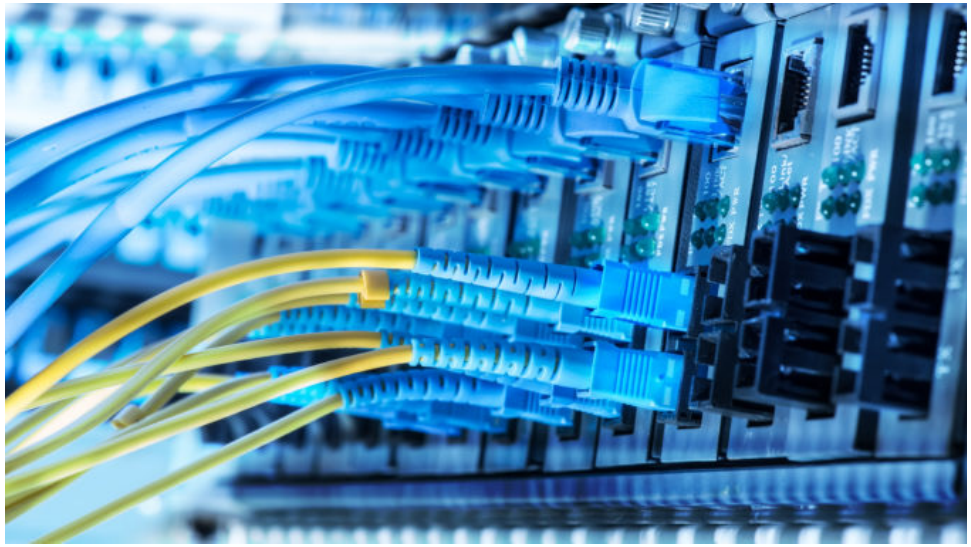
- Pháp chứng giống hay khác điều tra?

Câu hỏi

- Bạn đã từng làm về pháp chứng số trong công việc hàng ngày? Cho ví dụ?

Các lĩnh vực Pháp chứng kỹ thuật số

Bằng chứng số có ở đâu?



Tại sao cần DF?

- Hiện nay việc hệ thống CNTT là công cụ phục vụ gần như mọi lĩnh vực trong cuộc sống.
- Pháp chứng kỹ thuật số thực hiện:
  - Điều tra tội phạm sử dụng các phương pháp kỹ thuật số với máy tính
  - Xác định, khai thác các tài liệu chứng cứ máy tính được lưu trữ hoặc còn lưu vết.
  - Bằng chứng kỹ thuật số có thể được sử dụng để phân tích tội phạm máy tính và trên mạng.

Tính pháp lý của bằng chứng số?

PHẢI CÓ LUẬT QUY ĐỊNH RÕ RÀNG

> *"Law enforcement personnel must properly preserve digital evidence to make it suitable for presentation in court."*

Inspector Cameron is the commanding officer of the Suffolk County, New York, Police Department's Special Patrol Bureau in Ronkonkoma.

Nếu nhân viên điều tra không thể kiểm soát toàn bộ hệ thống máy tính, bằng chứng họ tìm được sẽ không được công nhận.

Các vấn đề cần quan tâm trong DF

- Đảm bảo tính toàn vẹn của dữ liệu: Ghi lại tất cả các bước của quá trình, dùng để cung cấp bằng chứng rằng công việc điều tra có bảo vệ thông tin của hệ thống máy tính mà không làm thay đổi hoặc làm hỏng chúng.
- Phương pháp thực hiện phù hợp với môi trường cần làm pháp chứng.
- Khôi phục lại càng nhiều thông tin bị xóa càng tốt bằng cách sử dụng các ứng dụng có thể tìm kiếm và truy hồi dữ liệu bị xóa.

Các vấn đề cần quan tâm trong DF

- Tìm kiếm thông tin của tất cả các file ẩn
- Giải mã và truy cập các file được bảo vệ
- Phân tích các khu vực đặc biệt trên ổ đĩa máy tính, bao gồm các phần thường khó có thể tiếp cận
- Thông tin được ẩn giấu (steganography)

Công nghệ trong DF

- Phần mềm: mã nguồn đóng/mở
- Phần cứng

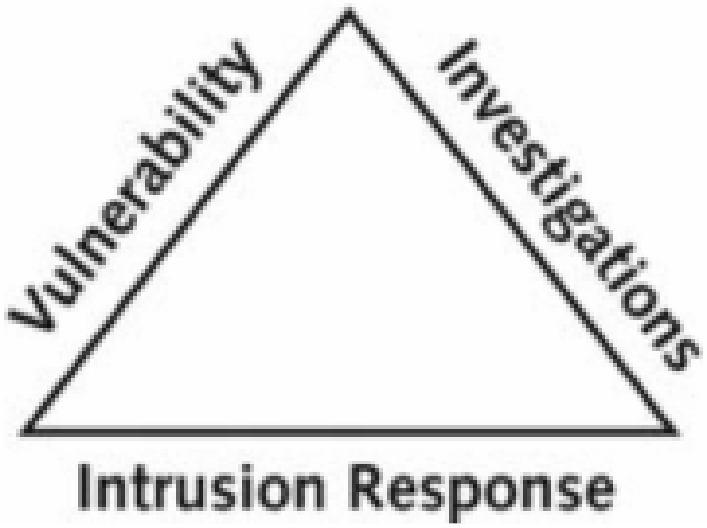
Các vấn đề về điều tra

- Điều tra viên phải có lệnh của Tòa án mới được tìm kiếm thông tin trên một máy tính tình nghi.
- Lệnh của Tòa án cần chỉ rõ nơi điều tra viên được phép tìm kiếm và loại bằng chứng mà họ có thể tìm.
- Điều tra viên chỉ được làm theo lệnh và tìm kiếm những gì mà họ cho rằng đáng nghi ngờ.

Các vấn đề về điều tra

- Điều tra viên kiểm soát hệ thống máy tính để chắc chắn rằng thiết bị và dữ liệu được an toàn
- Điều tra viên cần phải nắm quyền bảo mật để không có một cá nhân nào có thể truy cập máy tính và thiết bị lưu trữ đang được kiểm tra.
- Nếu hệ thống máy tính có kết nối với Internet, điều tra viên phải kiểm soát được việc kết nối này.
- Chú ý: Bản nguyên gốc cần được bảo quản và không được động đến.

Các vấn đề về điều tra



(Theo CHFI)

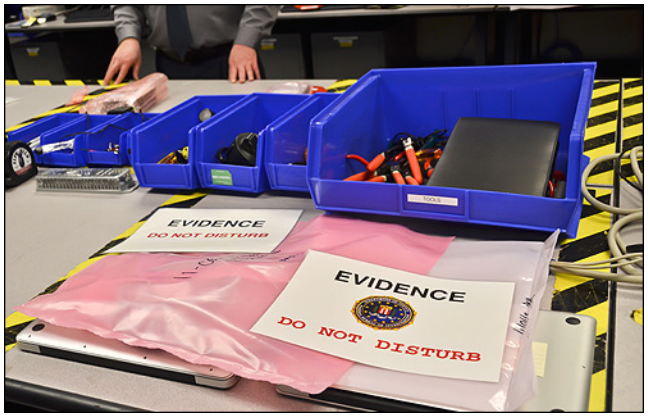
- Các điều tra viên thường hoạt động theo một nhóm gồm các chuyên gia có kiến thức trong lĩnh vực an ninh mạng và máy tính nhằm bảo vệ chứng cứ an toàn. Các nhóm này sẽ tiến hành công việc tùy theo chức năng và trình độ chuyên môn bao gồm 3 công việc chính
- Yếu tố căn bản của điều tra:
  - Đánh giá các điểm nhạy cảm và quản lý rũi ro.
  - Dò tìm xâm phạm hệ thống mạng máy tính trái phép và phản ứng lại các sự cố khẩn cấp.
  - Quá trình điều tra máy tính.

Các vấn đề về điều tra

- Điều tra viên tìm kiếm tất cả các file có trong hệ thống máy tính, bao gồm các file đã được mã hóa, được bảo vệ bằng mật khẩu, được ẩn hoặc bị xóa nhưng có thể khôi phục.
- Điều tra viên nên sao chép lại tất cả các file của hệ thống, bao gồm các fiel có trong ổ đĩa của máy tính hay file từ các ổ cứng cắm ngoài.
- Điều tra viên chỉ nên làm việc với các bản copy của các file khi tìm kiếm bằng chứng bởi khi truy cập các file có thể thay đổi.

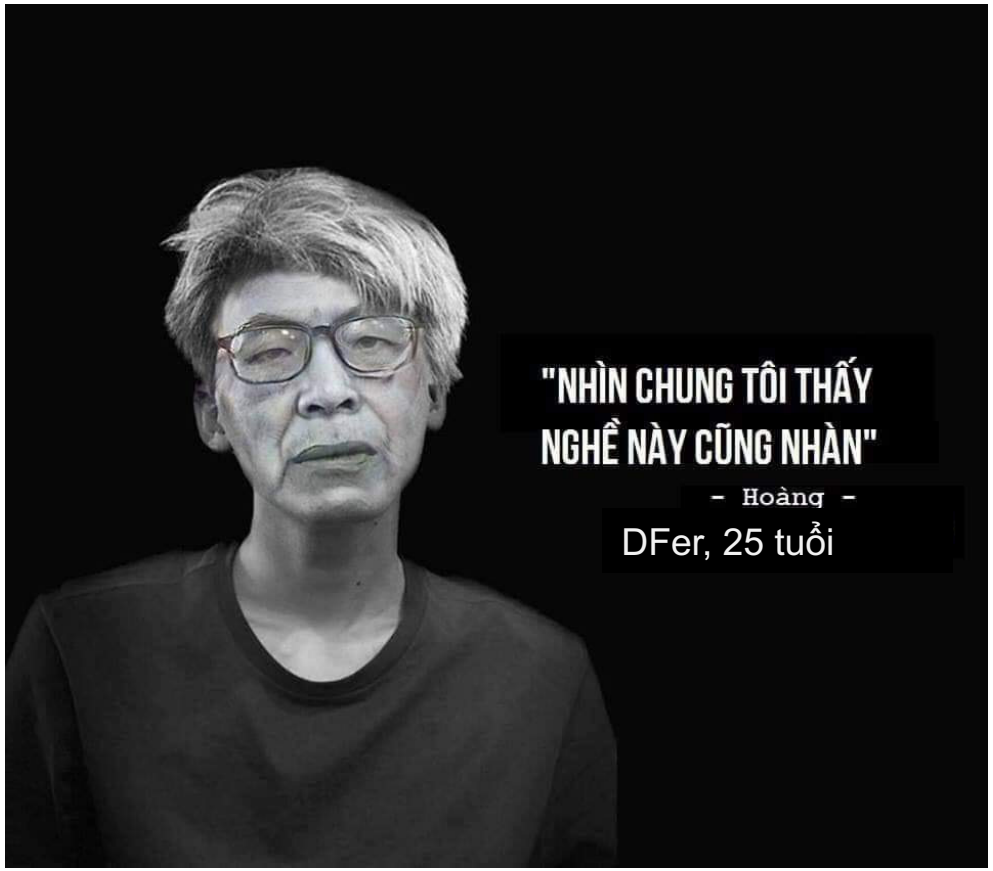
Dữ liệu số và pháp chứng số

- Dữ liệu số thu được từ các ổ đĩa trên máy tính hoặc từ các thiết bị lưu trữ khác chưa thể là bằng chứng số.
- Để có được bằng chứng, điều tra viên phải thực hiện quá trình khảo sát và phân tích dữ liệu ban đầu.
- Nếu tìm được dữ liệu, điều tra viên phải "ráp" chúng lại với nhau để đưa ra được bằng chứng số.



Nghề pháp chứng số

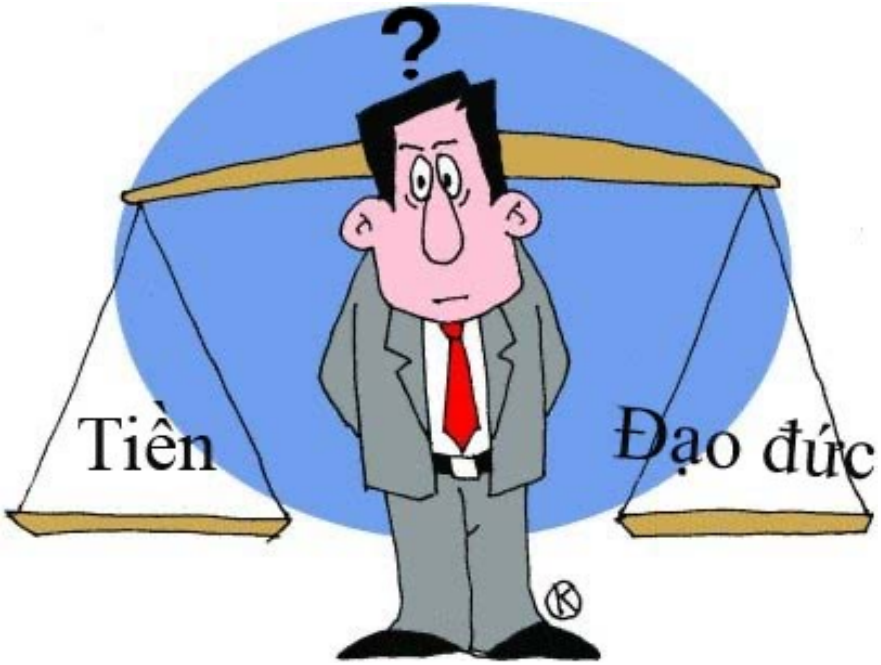
- Trong công quyền
- Trong dân sự
  - Tổ chức
  - Cá nhân



VNCERT

- Trung tâm Ứng cứu khẩn cấp Máy tính Việt Nam (Vietnam Computer Emergency Response Team - VNCERT) thực hiện chức năng điều phối và tổ chức các hoạt động phản ứng nhanh các sự cố máy tính cho mạng Internet Việt Nam.
- VNCERT có trách nhiệm điều phối các hoạt động ứng cứu sự cố máy tính trong toàn quốc, cảnh báo kịp thời các vấn đề về an toàn mạng máy tính
- VNCERT có trách nhiệm xây dựng, phối hợp xây dựng các tiêu chuẩn kỹ thuật về an toàn mạng máy tính, thúc đẩy hình thành hệ thống ứng cứu khẩn cấp Máy tính (CERT) trong các cơ quan, tổ chức, doanh nghiệp
- Website: http://www.vncert.gov.vn
- Ngoài ra còn các tổ chức: cục ATTT – Bộ TTTT, VNISA, … các tổ chức/doanh nghiệp CNTT có liên quan

Đạo đức với DF



Đạo đức với DF

- Đạo đức đang là những kiến thức như những tiêu chuẩn, những quy tắc, những định hướng cho các cư xử được chấp nhận bởi luân lý hay xã hội, ví dụ như: sự trung thực, sự tin cậy, hay hành động vì sự tiến bộ xã hội.
- Đạo đức được có thể tổng kết như "những quy tắc của tính trung thực", Đạo đức là cơ sở cho sự trung thực trong kinh doanh và tính nhà nghề trong kỹ thuật.
- Tại Hoa Kỳ, DFCB (Digital Forensics Certification Board) có ra bản quy tắc đạo đức và chuẩn mực trong xử lý công việc cho nghề Pháp chứng kỹ thuật số.

Đạo đức với DF

- Cá nhân hành nghề Pháp chứng kỹ thuật số không tham gia vào bất cứ hành vi có hại cho nghề nghiệp bao gồm trình bày sai kỹ thuật hoặc biến dạng, hành vi giả mạo hoặc trình bày sai lạc về thông tin trong lĩnh vực chuyên môn
- Cần tránh tất cả các xung đột lợi ích, cần tuân thủ tất cả các yêu cầu hợp pháp của tòa án có thẩm quyền;
- Cần cho thấy không có sự thiên vị đối với những phát hiện, không bày tỏ chính kiến đối với sự có tội hay sự vô tội của bất kỳ bên nào.
- Không tiết lộ bất kỳ dữ liệu mật thu được mà không có yêu cầu thích hợp từ cấp có thẩm quyền hoặc yêu cầu của tòa án có thẩm quyền.

Đạo đức với DF

- Cần kiểm tra và xem xét kỹ lưỡng tất cả các thông tin (trừ khi có giới hạn theo lệnh tòa án hoặc cấp có thẩm quyền).
- Chỉ đưa ra các ý kiến và các kết luận theo đúng kết quả thu được bằng cách sử dụng các công cụ phù hợp được xác nhận.
- Làm báo cáo hoặc làm chứng trung thực trong mọi vấn đề và không cố ý trình bày sai lạc bản chất bất kỳ thông tin nào, không giữ lại bất cứ thông tin nào vì làm như vậy có thể bóp méo sự thật.
- Chỉ chấp nhận thực hiện công việc khi có tin tưởng hoàn thành với năng lực chuyên môn của mình.

Đạo đức với DF

- Cá nhân hành nghề Pháp chứng kỹ thuật số cần xử lý tất cả các tang vật và các thông tin có giá trị chứng cứ với sự cẩn thận cần thiết để đảm bảo tính toàn vẹn của chúng.
- Cần có đủ hiểu biết về bản chất của vấn đề công việc điều tra, cần hiểu được yêu cầu chuyên môn của công việc điều tra, hiểu rõ các hạn chế và trách nhiệm của tất cả các bên.
- Các kết luận khi đưa ra cần được đảm bảo bởi các bằng chứng và thông tin một cách đầy đủ và hoàn chỉnh.
- Cần liên tục phấn đấu nâng cao kỹ năng và kiến thức để duy trì năng lực và các chuẩn nghề nghiệp.
- Cần tôn trọng các đồng nghiệp, không xuyên tạc về những khả năng lý thuyết và thực hành của đồng nghiệp

Các chứng chỉ DF

Capture The Flag – CTF

Forensics

Cryptography

Web Exploitation

Reverse Engineering

Binary Exploitation

Forensics in CTF

Các dạng phổ biến về forensics trong CTF challenge:

- format analysis,
- steganography,
- memory dump analysis,
- or network packet capture analysis
- …

Q&A

"Somebody broke into your computer, but it looks like the work of an inexperienced hacker."


Copyright 2006 by Randy Glasbergen.
www.glasbergen.com
GLASBERGEN
"No fingerprints, no picture ID, no Social Security number.
I'm afraid your baby presents a serious security risk."

TRƯỜNG ĐH CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH & TRUYỀN THÔNG

Digital Forensics
Pháp chứng Kỹ thuật số

#1: Overview
Spring 2023

ThS. Lê Đức Thịnh
thinhld@uit.edu.vn