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

Digital Forensics
Pháp chứng Kỹ thuật số

#1: Computer Forensics
Spring 2022

ThS. Lê Đức Thịnh
thinhld@uit.edu.vn

Nội dung trình bày

- Pháp chứng máy tính là gì?
- Pháp chứng máy tính làm gì?
- Các bước thực hiện pháp chứng máy tính?
- Các công cụ hỗ trợ

Computer Forensics?

Computer Forensics?

- Computer Forensic là quá trình thu thập và phân tích thông tin trên các máy tính được sử dụng như là chứng cứ phục vụ cho việc điều tra tội phạm hay dùng trong các công tác quản trị hệ thống thông tin.
- Theo DIBS USA, Inc: *Computer forensic* có nghĩa là khoa học về nghiên cứu và phân tích dữ liệu từ các thiết bị lưu trữ trên máy tính được sử dụng như là chứng cứ trước tòa

Computer Forensics Examples

- Hãy cho các ví dụ về pháp chứng máy tính mà bạn đã thực hiện?

Computer Forensics Examples

- Recovering thousands of deleted emails
- Recovering deleted files
- Performing investigation post employment termination
- Recovering evidence post formatting hard drive
- Performing investigation after multiple users had taken over the system

Computer Forensics Examples

- Find out what external devices have been attached and what users accessed them
- Determine what programs ran
- Recover webpages
- Recover emails and users who read them
- Recover chat logs
- Determine file servers used
- Discover document's hidden history
- Recover phone records and SMS text messages from mobile devices
- Find malware and data collected

File is deleted, what happens?

- Windows Operating System
  - File Allocation Table (FAT)
  - Master File Table (MFT)
- FAT/MFT tells the computer where the file begins and ends
- Deleted pointers to the file
  - FAT/MFT space occupied by the file is mark as available
- The actual data that was contained in the file is not deleted
  - Unallocated space

Tại sao cần Pháp chứng máy tính?

- Máy tính là công cụ của tội phạm truyền thống/CNC

Role of Forensics Investigator

1. Protects the victim's computer from any damage and viruses
2. Determines the extent of damage
3. Gathers evidence in a forensically sound manner
4. Analyzes the evidence data found and protects it from damage
5. Prepares the analysis report
6. Presents acceptable evidence in the court

Ai cần pháp chứng máy tính?

- Cơ quan thực thi pháp luật (Law Enforcement)
- Các tổ chức pháp chứng máy tính tư nhân (Private Computer Forensic Organizations)
- Quân đội (Military)
- Chương trình giáo dục đại học (University Programs)
- Các chuyên gia bảo mật máy tính và công nghệ thông tin (Computer Security and IT Professionals)

Ai cần pháp chứng máy tính?

- **Cơ quan thực thi pháp luật (Law Enforcement)**
  - Công tố viên Hình sự
    - Dựa vào bằng chứng thu được từ máy tính để truy tố nghi phạm và sử dụng làm bằng chứng
  - Các vụ kiện dân sự
    - Dữ liệu cá nhân và doanh nghiệp được phát hiện trên máy tính có thể được sử dụng trong các trường hợp gian lận, ly hôn, quấy rối hoặc phân biệt đối xử.

Ai cần pháp chứng máy tính?

- **Các tổ chức pháp chứng máy tính tư nhân/công ty (Private Computer Forensic Organizations)**
  - Các công ty bảo hiểm
    - Bằng chứng được phát hiện trên máy tính có thể được sử dụng để thanh toán chi phí (gian lận, bồi thường cho người lao động, v.v.)
  - Công ty tư nhân
    - Bằng chứng thu thập được từ máy tính của nhân viên có thể được sử dụng làm bằng chứng trong các trường hợp quấy rối, gian lận và tham ô

Ai cần pháp chứng máy tính?

- **Quân đội (Military)**
  - Kiểm tra, xác định và thu thập bằng chứng
  - Phân tích bằng chứng để thu thập thông tin tình báo nhanh chóng và ứng phó với các sự cố vi phạm an ninh

Ai cần pháp chứng máy tính?

- **Chương trình giáo dục đại học (University Programs)**
  - Cử nhân
  - Thạc sĩ
  - …

Ai cần pháp chứng máy tính?

- **Các chuyên gia bảo mật máy tính và công nghệ thông tin (Computer Security and IT Professionals)**
  - Network traffic
  - Compromised networks
  - Insider threats
  - Disloyal employees
  - Malware
  - Breach of contracts
  - E-mail Fraud/Spam
  - Theft of company documents

FBI Computer Forensics Services

- Comparison again known data
- Transaction sequencing
- Extraction of data
- Recovering deleted data files
- Format conversion
- Keyword searching
- Decrypting passwords
- Analyzing and comparing limited source code

Các bước thực hiện pháp chứng máy tính?

- **Pháp chứng máy tính có 4 bước:**
  - Acquisition
  - Identification
  - Evaluation
  - Presentation

Các bước thực hiện pháp chứng máy tính?

- **Acquisition**
  - Có được quyền sở hữu vật lý hoặc từ xa đối với máy tính
  - Kiểm soát tất cả các liên kết hệ thống, các thiết bị lưu trữ vật lý

Các bước thực hiện pháp chứng máy tính?

- **Identification**
  - Xác định dữ liệu có thể được khôi phục
  - Truy xuất dữ liệu theo phương thức điện tử bằng bộ công cụ/phần mềm pháp chứng máy tính khác nhau

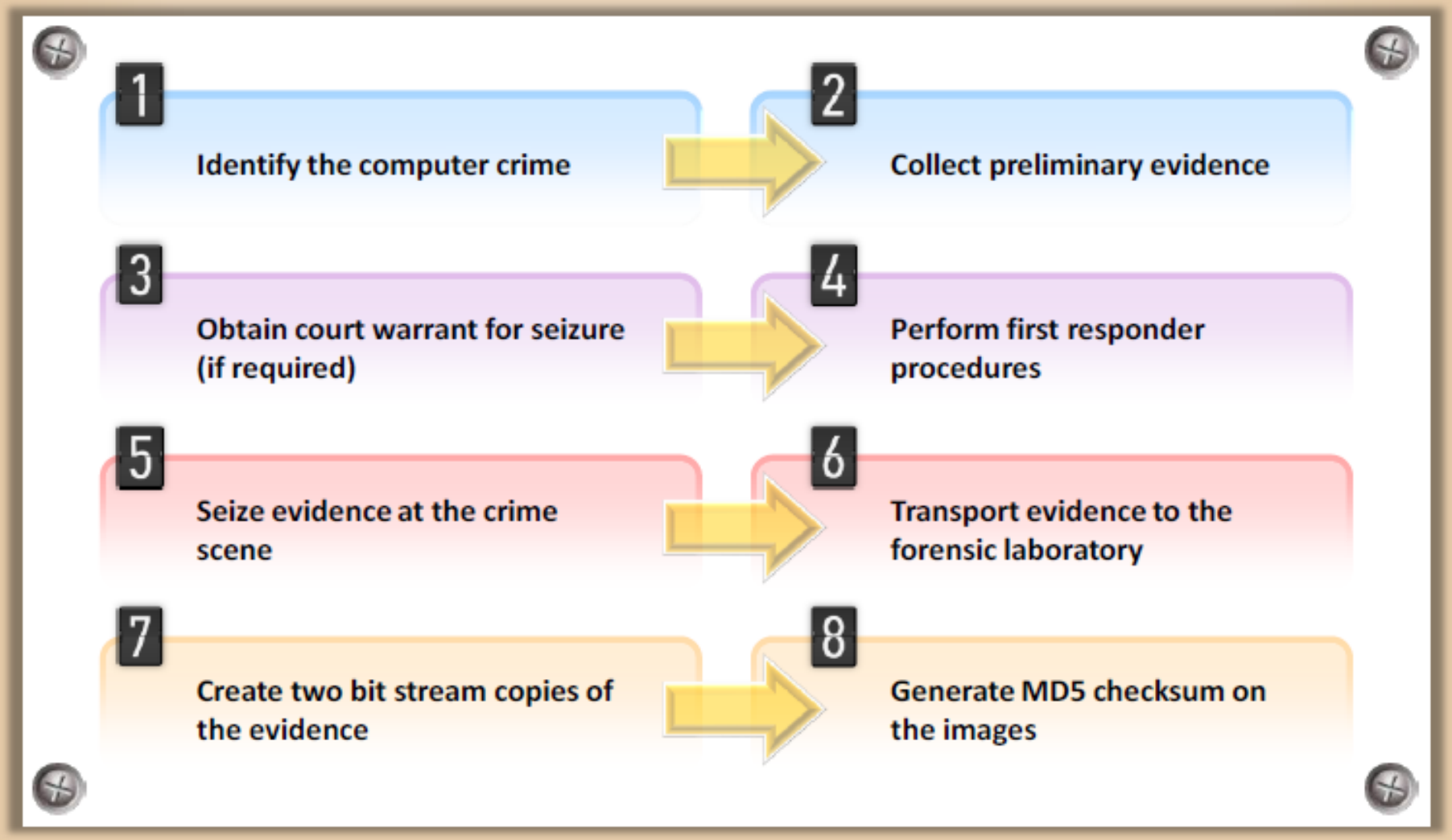
Các bước thực hiện pháp chứng máy tính?

- **Evaluation**
  - Đánh giá thông tin/dữ liệu khôi phục lại
  - Cách thức sử dụng dữ liệu/thông tin đó để làm bằng chứng trong truy tố trước tòa hoặc chấm dứt việc làm hay không

Các bước thực hiện pháp chứng máy tính?

- **Presentation**
  - Trình bày bằng chứng được phát hiện theo cách mà luật sư, nhân viên/quản lý không chuyên về kỹ thuật có thể hiểu được.
  - Phù hợp với quy định của Pháp luật

Key Steps in Forensics Investigation (Cont'd)



Key Steps in Forensics Investigation

9 Maintain a chain of custody

10 Store the original evidence in a secure location

11 Analyze the image copy for evidence

12 Prepare a forensic report

13 Submit the report to the client

14 If required, attend the court and testify as an expert witness

Computer Forensic Requirements

- **Hardware**
  - Familiarity with all internal and external devices/components of a computer
  - Thorough understanding of hard drives and settings
  - Understanding motherboards and the various chipsets used
  - Power connections
  - Memory
- **BIOS**
  - Understanding how the BIOS works
  - Familiarity with the various settings and limitations of the BIOS

Computer Forensic Requirements

- **Operation Systems**
  - Windows 3.1/95/98/ME/NT/2000/2003/XP/Vista/7/8/10
  - DOS
  - UNIX
  - LINUX
  - VAX/VMS
- **Software**
  - Familiarity with most popular software packages such as Office
- **Forensic Tools**
  - Familiarity with computer forensic techniques and the software packages that could be used

Các lưu ý quan trọng

- Tuân thủ quy trình, thủ tục pháp lý: không làm ảnh hưởng đến mức độ tin cậy và tính pháp lý của bằng chứng.
- Xem xét, xử lý mọi chứng cứ dù là nhỏ nhất vì nó sẽ được sử dụng trước tòa.
- Ghi nhận toàn bộ quá trình (documentation)
- Chuỗi giám định (Chain of Custody)

Chain of Custody?

- Nhiệm vụ của một chuyên gia điều tra máy tính là truy tìm các chứng cứ số trên những máy tính khả nghi để tập hợp đầy đủ các thông tin và đưa ra bản án trước tòa.
- Các chứng cứ được tìm thấy trên một máy tính sẽ được tập trung trên một máy tính khác, vì vậy ngoài việc sao chép các chứng cứ số một cách chính xác thì điều tra viên cần tiến hành công việc theo các mô hình hợp lý để tạo ra *một chuỗi chứng cứ khoa học, hợp lệ* gọi là *chain of custody*

Chain of Custody

Chain of custody is a legal document that demonstrates the progression of evidence as it travels from original evidence location to the forensic laboratory

Functions

- Governs the collection, handling, storage, testing, and disposition of evidence
- Safeguards against tampering with or substitution of evidence
- Documents that these steps have been carried out

The chain of custody form should identify:

- Sample collector
- Sample description, type, and number
- Sampling data and location
- Any custodians of the sample

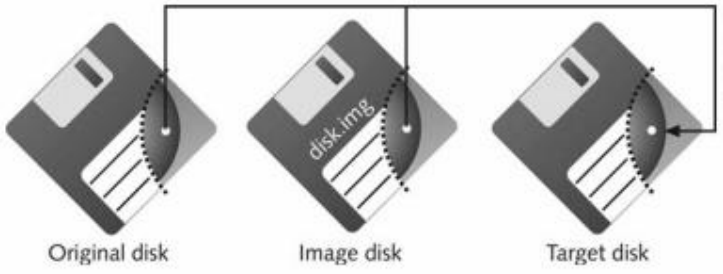
Chain of Custody Form

Case No. #			
Client Ref. #			
Client Item #		Description:	
Make:	Model:	Serial #	Other Identifying #
Client Item #		Description:	
Make:	Model:	Serial #	Other Identifying #
Client Item #		Description:	
Make:	Model:	Serial #	Other Identifying #
Client Item #		Description:	
Make:	Model:	Serial #	Other Identifying #

Client Item #'s	Date/Time	Released By	Received By	Reason
	Date	Name/Client	Name/Client	
	Time	Signature	Signature	

Các lưu ý quan trọng

- Sao chép từng bit một (Bit-Stream Copy) ra bản sao để xử lý trên bản sao đó.
  - Sao chép chính xác theo từng bit (*bit-by-bit)* hay còn gọi là *sector copy* cho dù các thông tin ẩn hay bị xóa của thư mục cũng được sao chép
  - Phương pháp này cho toàn bộ dữ liệu trên đĩa cứng sẽ tạo ra các ảnh đĩa hay bit-stream image
  - Tools: Norton Ghost, Acronis True Image, …



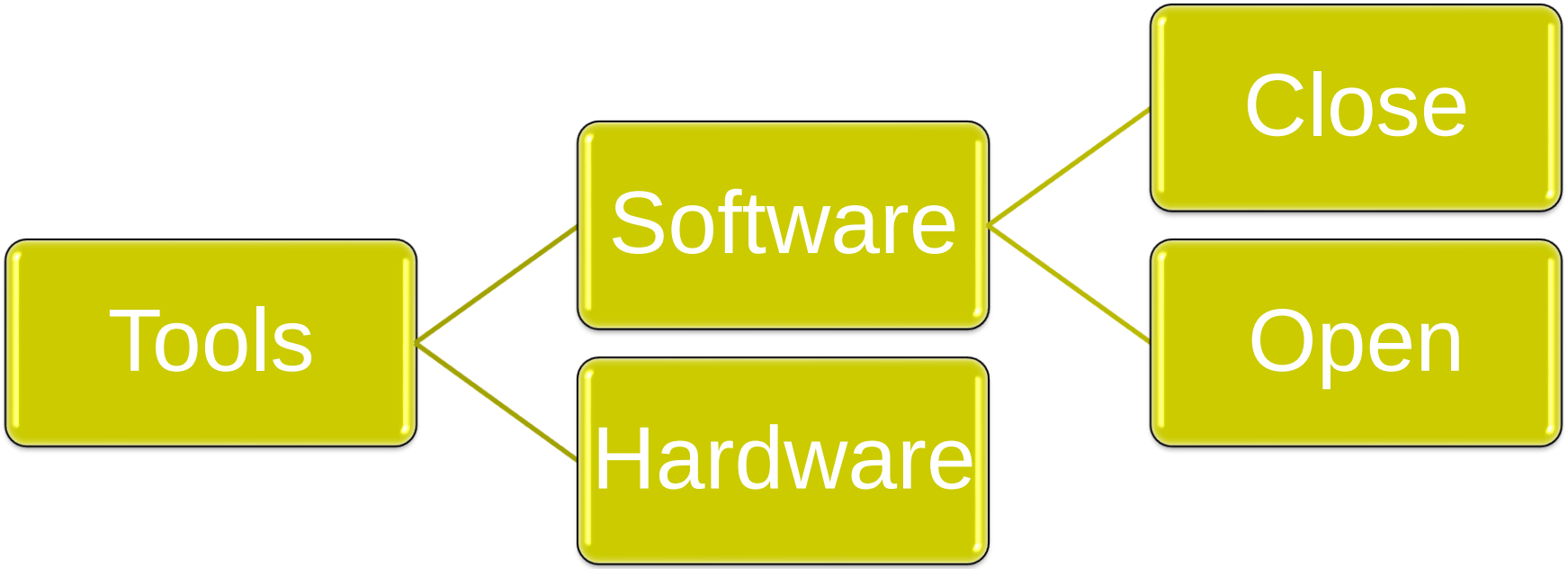
Các lưu ý quan trọng

- Bảo vệ bằng chứng an toàn → rất quan trọng
  - Vì chúng sẽ dùng là bằng chứng để truy tố trước toà hay là cơ sở cho các quyết định kỹ luật, kiểm điểm, …

Cần tránh khi điều tra

- Changing data
  - Changing time or date stamps
  - Changing files
- Overwriting unallocated disk space
  - This can happen when re-booting

Computer Forensic Tools



Computer Forensic Tools

- **Phần cứng chuyên dụng:**
  - Là một phần không thể thiếu được của các điều tra viên
  - Đảm bảo các tính năng: An toàn, chính xác, tốc độ cao.
  - Được trang bị trong các phòng Forensic Lab hoặc có thể mang theo điều tra viên.

Computer Forensic Tools

- Thiết bị chép đĩa cứng cầm tay ImageMASSter Solo-3

- Thiết bị dễ dàng mang theo, có khả năng chép tới 2 ổ đĩa, tới 3GBytes/phút. Tương thích với hầu hết các kết nối, kiểm tra và bảo mật đồng thời
- Đảm bảo các tính năng: An toàn, chính xác, tốc độ cao.

Computer Forensic Tools

- Bảng T8-R2 dành cho USB

- Sử dụng để ghi, đọc các thẻ nhớ USB, ổ đĩa USB
- Đảm bảo các tính năng: An toàn, chính xác, tốc độ cao

Computer Forensic Tools

- RoadMASSter-3
- Có khả năng đọc, backup, tìm kiếm thông tin nhanh chóng, an toàn
- Tương thích với hầu hết các kết nối, kiểm tra và bảo mật đồng thời

Computer Forensic Tools

- **FRED**: **F**orensic **R**ecovery of **E**vidence **D**evice
- Đơn giản chỉ cần lấy các ổ đĩa cứng cắm chúng vào Fred và điều tra viên có được các bằng chứng kỹ thuật số.
- Làm việc với IDE/EIDE/ATA/SATA/ATAPI/SAS/ Firewire/USB hard drives

Computer Forensic Tools

Phần mềm:

- Các phần mềm mã nguồn đóng
  - COFEE
  - Categoriser 4 Pictures
  - EnCase
  - ProDiscover
  - X-Ways Forensic
- Các phần mềm mã nguồn mở
  - Sleuth Kit
  - Wireshark
- Chạy các nền tảng Linux, Unix, OS X, Solaris, Windows

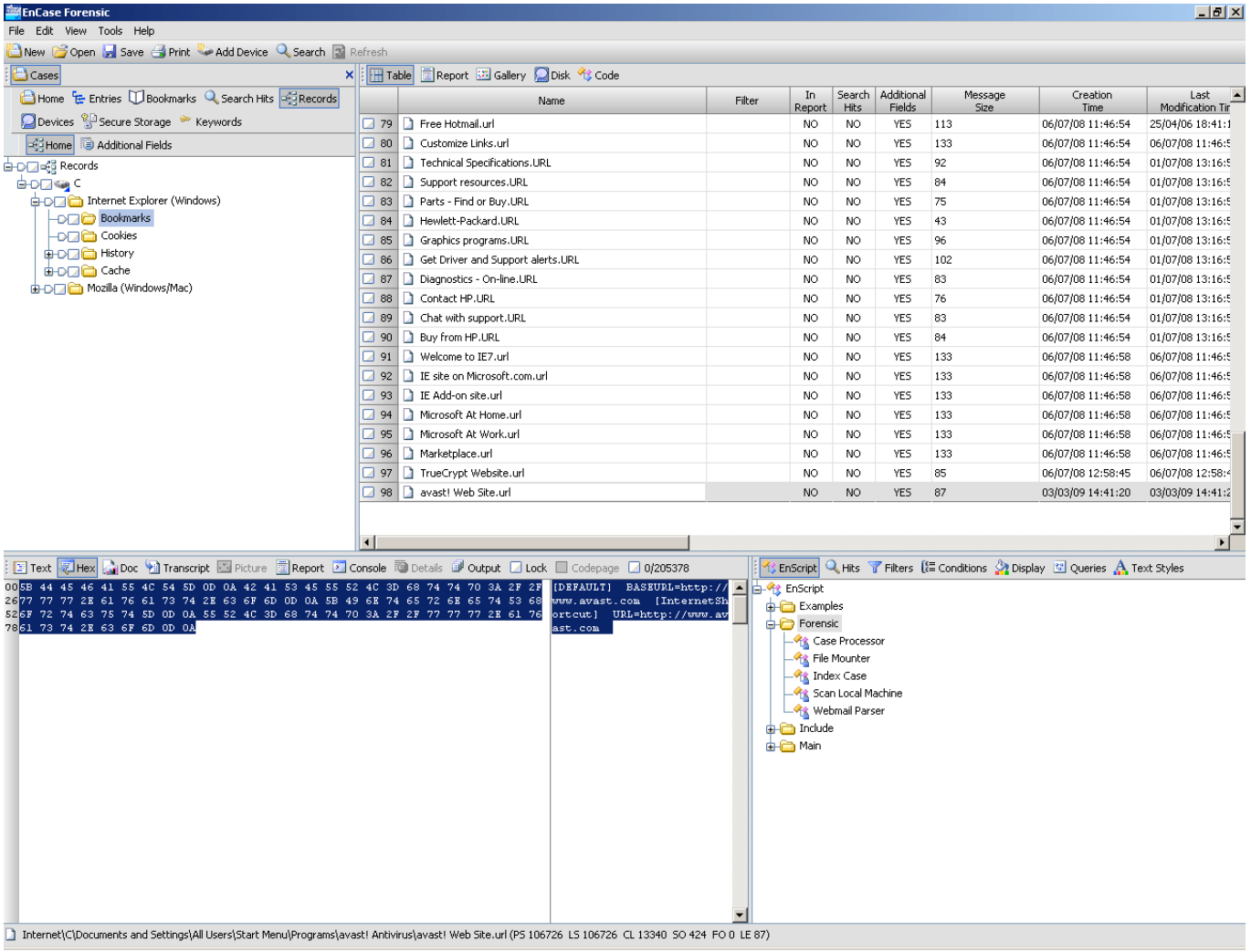
Computer Forensic Tools

- Software Tools:
  - Imaging Software
    - Creates an exact copy of the hard drive (a hash is used for checking)
    - Called also bitstream copy
  - Disk Deep Searching Software
- The forensics tool that is chosen must have been successfully used in court cases:
  - Encase
  - Forensic Toolkit (FTK)

Encase

- Encase is a computer forensics tool widely used by law enforcement agencies
- It allows:
  - Imaging
  - Write Blocking
  - Hash calculation
  - Locating hidden drives and partitions
  - Locating hidden files
  - Multiple location searching

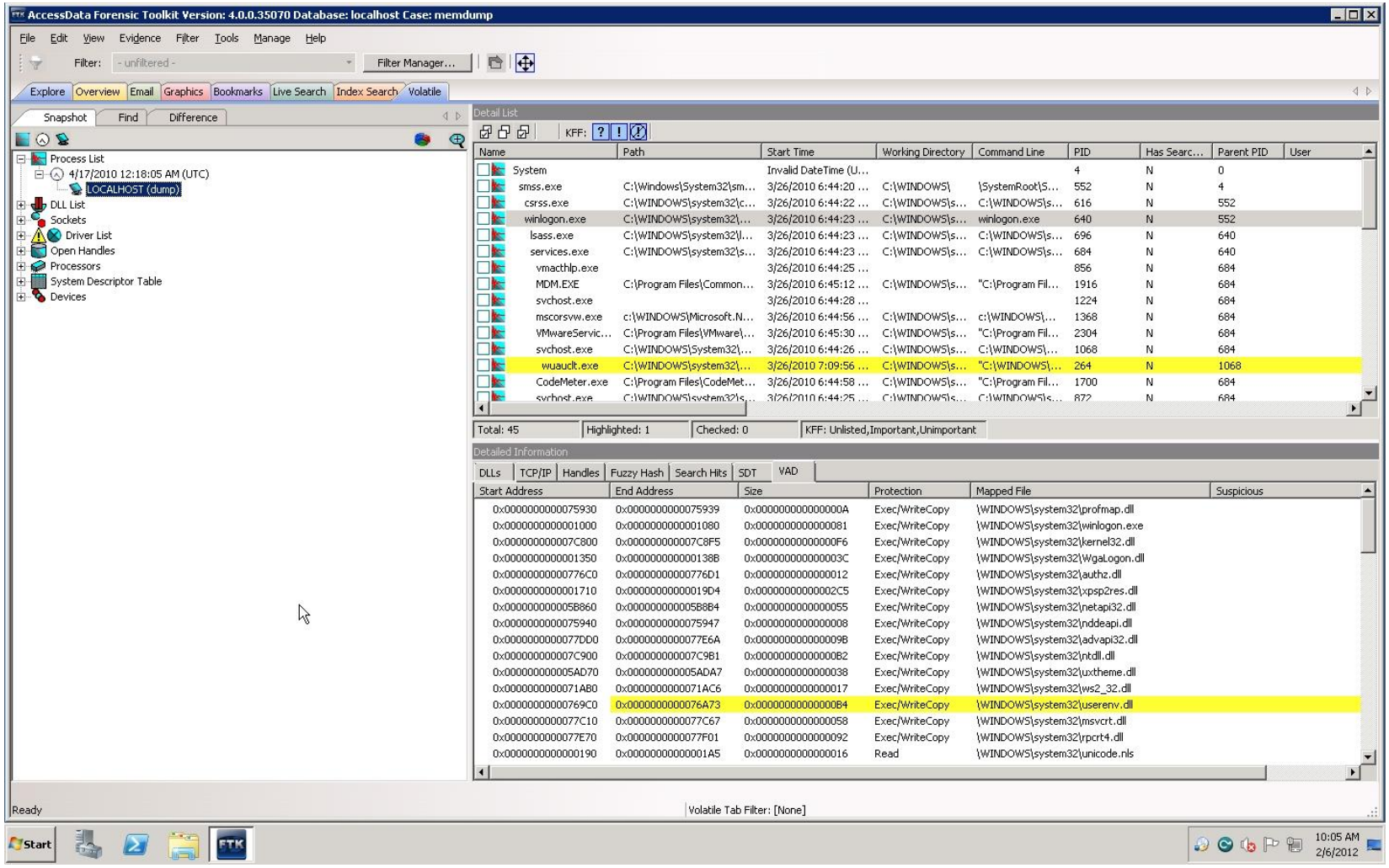
Encase


EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases
Home Entries Bookmarks Search Hits Records
Devices Secure Storage Keywords
Home Additional Fields
Records
C
Internet Explorer (Windows)
Bookmarks
Cookies
History
Cache
Mozilla (Windows/Mac)
Table Report Gallery Disk Code
Name Filter In Report Search Hits Additional Fields Message Size Creation Time Last Modification Tir
79 Free Hotmail.url NO NO YES 113 06/07/08 11:46:54 25/04/06 18:41:1
80 Customize Links.url NO NO YES 133 06/07/08 11:46:54 06/07/08 11:46:5
81 Technical Specifications.URL NO NO YES 92 06/07/08 11:46:54 01/07/08 13:16:5
82 Support resources.URL NO NO YES 84 06/07/08 11:46:54 01/07/08 13:16:5
83 Parts - Find or Buy.URL NO NO YES 75 06/07/08 11:46:54 01/07/08 13:16:5
84 Hewlett-Packard.URL NO NO YES 43 06/07/08 11:46:54 01/07/08 13:16:5
85 Graphics programs.URL NO NO YES 96 06/07/08 11:46:54 01/07/08 13:16:5
86 Get Driver and Support alerts.URL NO NO YES 102 06/07/08 11:46:54 01/07/08 13:16:5
87 Diagnostics - On-line.URL NO NO YES 83 06/07/08 11:46:54 01/07/08 13:16:5
88 Contact HP.URL NO NO YES 76 06/07/08 11:46:54 01/07/08 13:16:5
89 Chat with support.URL NO NO YES 83 06/07/08 11:46:54 01/07/08 13:16:5
90 Buy from HP.URL NO NO YES 84 06/07/08 11:46:54 01/07/08 13:16:5
91 Welcome to IE7.url NO NO YES 133 06/07/08 11:46:58 06/07/08 11:46:5
92 IE site on Microsoft.com.url NO NO YES 133 06/07/08 11:46:58 06/07/08 11:46:5
93 IE Add-on site.url NO NO YES 133 06/07/08 11:46:58 06/07/08 11:46:5
94 Microsoft At Home.url NO NO YES 133 06/07/08 11:46:58 06/07/08 11:46:5
95 Microsoft At Work.url NO NO YES 133 06/07/08 11:46:58 06/07/08 11:46:5
96 Marketplace.url NO NO YES 133 06/07/08 11:46:58 06/07/08 11:46:5
97 TrueCrypt Website.url NO NO YES 85 06/07/08 12:58:45 06/07/08 12:58:4
98 avast! Web Site.url NO NO YES 87 03/03/09 14:41:20 03/03/09 14:41:2
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 0/205378
EnScript Hits Filters Conditions Display Queries Text Styles
EnScript
Examples
Forensic
Case Processor
File Mounter
Index Case
Scan Local Machine
Webmail Parser
Include
Main
Internet\C\Documents and Settings\All Users\Start Menu\Programs\avast! Antivirus\avast! Web Site.url (PS 106726 LS 106726 CL 13340 SO 424 FO 0 LE 87)

Forensic Toolkit (FTK)

- Forensic Toolkit (FTK) allows to:
  - Create images of hard drives
  - Analyze the registry
  - Scan slack space for file fragments
  - Inspect emails
  - Identify steganography
  - Crack passwords

Forensic Toolkit (FTK)



Bộ phần mềm Sleuth Kit

- Sleuth Kit là phần mềm mã nguồn mở
- Sleuth Kit là một bộ các công cụ (tools) phần mềm pháp chứng hỗ trợ trong điều tra kỹ thuật số
- Các công cụ trong Sleuth Kit là các công cụ dòng lệnh để sử dụng với Linux, Unix, OS X, Solaris, Windows.
- Cùng với Sleuth Kit hiện có Autopsy cung cấp một giao diện đồ họa với các hệ điều hành Windows, Linux, OS X.

Bộ phần mềm Sleuth Kit

- Địa chỉ: http://www.sleuthkit.org
- Với Autopsy, sử dụng giao diện Windows thực hiện các thao tác một cách dễ dàng
- Ghi lại các case (vụ án) điều tra riêng biệt
- Cho phép cứu các file bị hỏng.

Bộ phần mềm Sleuth Kit

- Các công cụ (tool) trong Sleuth Kit cho phép kiểm tra hệ thống tập tin của một máy tính nghi ngờ dưới dạng không xâm nhập vào.
- Các công cụ (tool) về File System cho phép kiểm tra cách bố trí của ổ đĩa và phương tiện truyền thông khác.
- Với những công cụ liên quan đến partition, ta có thể xác định nơi mà các partition được định vị và giải nén chúng để có thể phân tích với các công cụ phân tích File System.

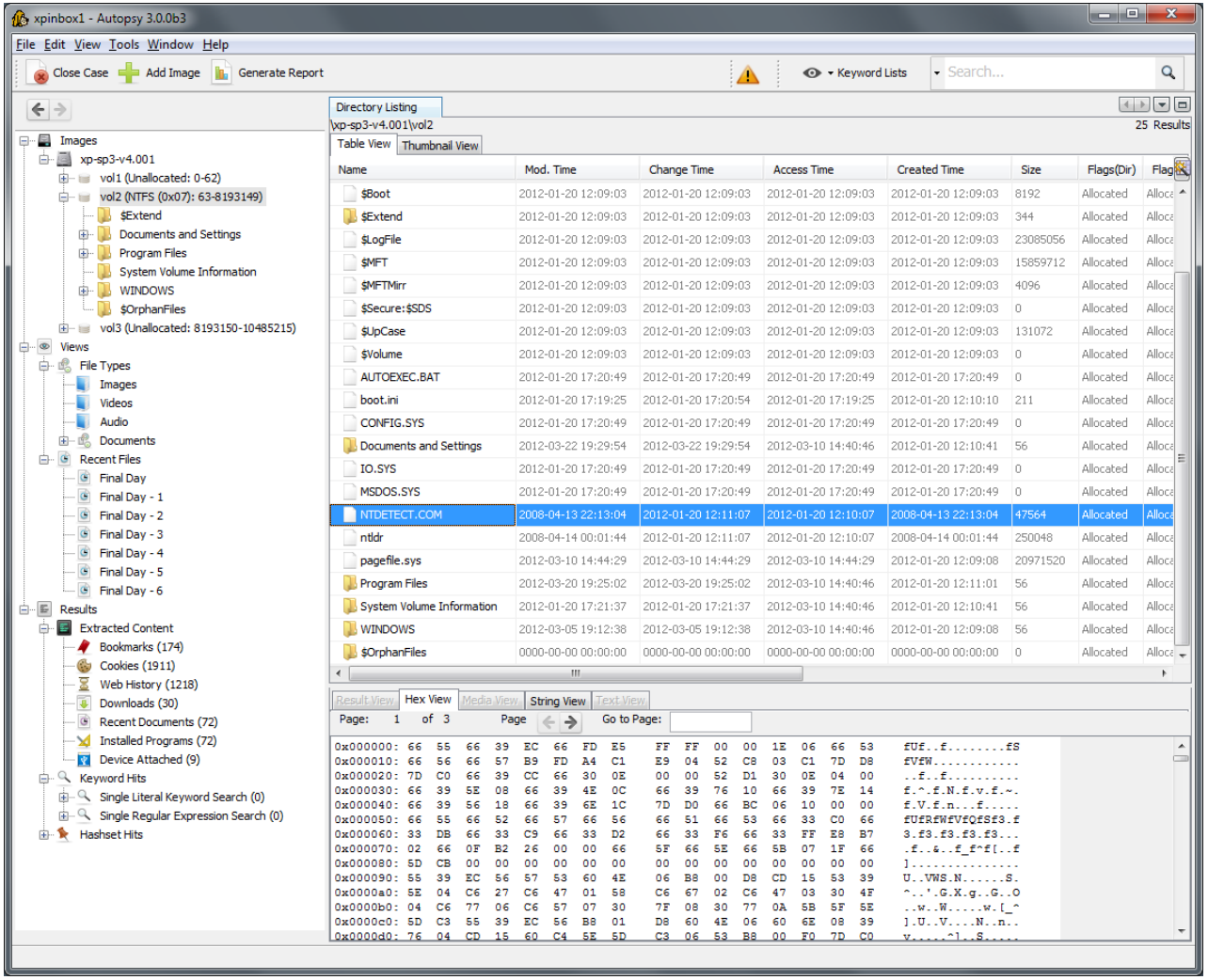
Bộ phần mềm Sleuth Kit

- Autopsy là một phần mềm pháp chứng kỹ thuật số với giao diện đồ họa của Sleuth Kit
- Autopsy có thể được sử dụng bởi các chuyên gia pháp chứng, những điều tra viên, những chuyên viên các công ty để điều tra những gì đã xảy ra trên máy tính.
- Autopsy cho phép phân tích sự kiện theo thời gian: trình bày các sự kiện truy cập tới File system theo trình tự với giao diện đồ họa.

Các tính năng của Autopsy

- Băm lọc (Hash Filtering): đánh dấu các tập tin có vấn đề và bỏ qua các tập tin tốt.
- Phân tích pháp chứng với File system: cho phép khôi phục các tập tin từ hầu hết các định dạng phổ biến.
- Tìm kiếm theo từ khóa - chỉ mục từ khóa tìm kiếm để tìm các tập tin có đề cập đến các từ có liên quan.
- Khai thác các thông tin sử dụng Web: cho phép trích xuất lịch sử truy cập Web, đánh dấu, tìm cookie từ trình duyệt Firefox, Chrome, và IE.
- Đa phương tiện - trích xuất dạng EXIF (Exchangeable image file format) từ các ảnh và video.

Các tính năng của Autopsy



Biểu mẫu điều tra "*multi-evidence form*"

Corporation X
Security Investigations
This form is to be used for one to ten pieces of evidence

Case No.:		Investigating Organization:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

	Description of evidence:	Vendor Name	Model No./Serial No.
Item #1			
Item #2			
Item #3			
Item #4			
Item #5			
Item #6			
Item #7			
Item #8			
Item #9			
Item #10			

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Item #	Evidence Processed by	Disposition of Evidence	Date/Time
			Page __ of ___

Biểu mẫu điều tra "*single-evidence form*"

Metropolis Police Bureau
High-tech Investigations Unit
This form is to be used for only one piece of evidence.
Fill out a separate form for each piece of evidence.

Case No.:		Unit Number:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

Item # ID	Description of evidence:	Vendor Name	Model No./Serial No.

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Evidence Processed by	Disposition of Evidence	Date/Time
		Page __ of ___

Thông tin cơ bản trên Biểu mẫu

- **Số hiệu của quá trình điều tra** – Số thứ tự do tổ chứ đặt khi phát động cuộc điều tra.
- **Tên của tổ chức cần điều tra.**
- **Tên của điều tra viên.**
- **Mô tả tình huống** – Mô tả vắn tắt về tình huống, sự việc. Ví dụ công việc cần làm là “Tìm kiếm bằng chứng vi phạm nội quy doanh nghiệp” hay “Phục hồi dữ liệu sau thảm họa”.

Thông tin cơ bản trên Biểu mẫu

- **Vị trí mà chứng cứ được thu thập** – Vị trính chính xác mà chứng cứ được tìm thấy, nếu sử dụng biểu mẫu multi-evidence nên tạo một form mới cho mỗi vị trí.
- **Mô tả chứng cứ** – Ví dụ ‘đĩa cứng, dung lượng 200 GB” hay “một ổ USB dung lượng 1 GB”, trên multi-evidence cần mô tả riêng cho từng chứng cứ thu thập được.
- **Tên nhà sản xuất, số hiệu của thiết bị** – Ví dụ Maxtor, là tên nhà sản xuất của đĩa cứng thu được và số serial của ổ đĩa

Thông tin cơ bản trên Biểu mẫu

- **Tên của người thu thập được chứng cứ** – Là người đã tìm được các chứng cứ cũng như sẽ chịu trách nhiệm vận chuyển, lưu trữ chứng cứ thích hợp.
- **Ngày và thời gian chứng cứ được thu thập.**
- **Chứng cứ cần được lưu giữ vào nơi an toàn** – Xác định vị trí hay thiết bị để cất giữ chứng cứ một cách an toàn.

Thông tin cơ bản trên Biểu mẫu

- **Liệt kê số hiệu của chứng cứ, tên điều tra viên và thời gian thực hiện.**
- **Đánh số trang** – hồ sơ dùng để lưu trữ tất cả chứng cứ với những vị trí khác nhau cần được đánh số trang cẩn thận.

Conclusion

- Computer Forensics helps determine the WHO, WHAT, WHEN, and WHERE related to a computer-based crime or violation.
- Who uses Computer Forensics
- Situations to use Computer Forensics
- Computer Forensic Software

References

- CHFIv8
- http://www.sleuthkit.org
- Computer forensics, Đàm Quang Hồng Hải
- Computer forensics, Kelsey Bretz
- Computer forensics, Bassel Kateeb, Tim Altimus
- …

Bài tập

1. Tìm hiểu kỹ thuật về đĩa cứng: HDD vs SSD, các loại cổng kết nối, volume, partition, …?
2. Tìm hiểu và trình bày chi tiết kỹ thuật của File System trên 03 nền tảng Windows, Linux, MacOS?

- Yêu cầu:
  - Thực hiện theo nhóm đồ án, tất cả các nhóm đều thực hiện
  - Soạn và **giải thích chi tiết** trên PowerPoint (.pptx)
  - Thời gian thực hiện: 01 tuần (tính từ)
  - Nộp trên moodle môn học

Q&A

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

Digital Forensics
Pháp chứng Kỹ thuật số

#1: Computer Forensics
Spring 2022

ThS. Lê Đức Thịnh
thinhld@uit.edu.vn