# DIGITAL FORENSICS

Trình bày: Nguyễn Xuân Việt – FPT CIO

# NỘI DUNG CHÍNH

01 Khái niệm, mục tiêu, nhiệm vụ của Digital Forensics

02 Đặc tính và truy tìm Bằng chứng số

03 Các bước thực hiện Điều tra số

04 Các loại hình Điều tra số và một số ví dụ

# CÁC KHÁI NIỆM TRONG DIGITAL FORENSICS


**Digital Forensics** là một nhánh của khoa học điều tra, với mục đích truy tìm và phân tích các tài liệu chứa trong các thiết bị số, thường gọi là “tài liệu số”, để tìm ra các bằng chứng số (Digital Evidence).

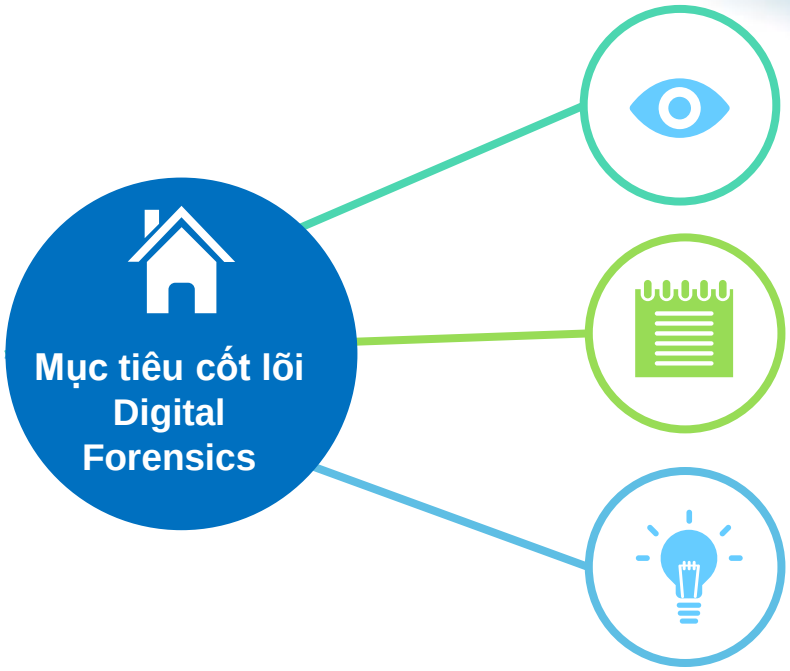
# CÁC KHÁI NIỆM TRONG DIGITAL FORENSICS

## Digital Evidence


- **Digital Evidence (Bằng chứng số)** hay còn gọi là **Electronic Evidence (Bằng chứng điện tử),** là mọi thông tin có giá trị pháp lý được lưu trữ, được truyền dẫn trong dạng thức số và có giá trị pháp lý trước tòa

**Bằng chứng số** là các bằng chứng ở dạng thức số, nó được khôi phục, hay được tìm thấy, trong các thiết bị số – thường là các thiết bị liên quan với máy tính, điện thoại, IoT….

# MỤC TIÊU CỦA DIGITAL FORENSICS




Phát hiện, bảo quản, khai thác dữ liệu thu thập được

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.

**Nguyên tắc**: Khi bạn làm việc với máy tính hay một hệ thống thông tin, tất cả hành động của bạn đều bị ghi vết lại hay từ chuyên môn gọi là Log

# NHIỆM VỤ CỦA DIGITAL FORENSICS

- **Nhiệm vụ của điều tra số** là áp dụng sự hiểu biết về khoa học và công nghệ để truy tìm, khôi phục, khảo sát và phân tích các bằng chứng có nguồn gốc số.
- Bằng chứng tìm được phải có giá trị pháp lý trước tòa.

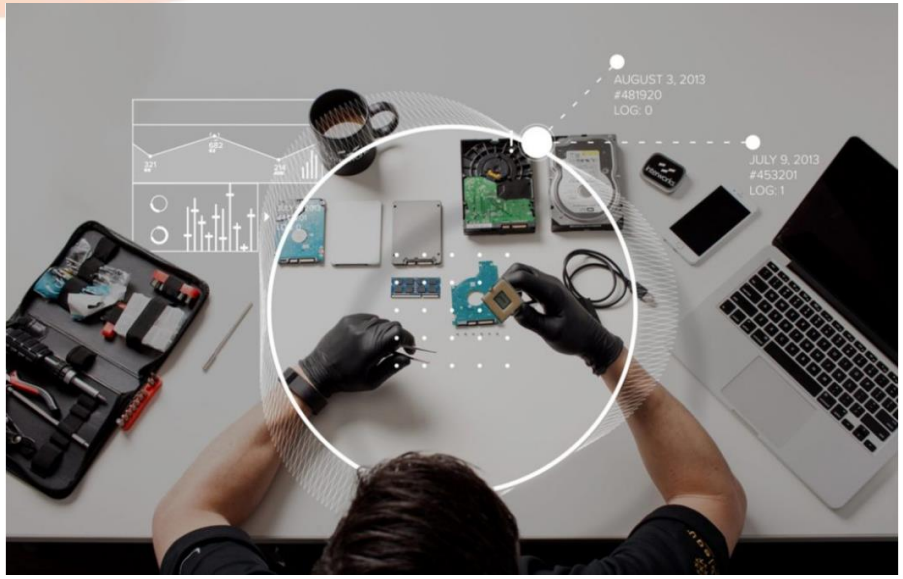
# ĐẶC TÍNH CỦA BẰNG CHỨNG SỐ

1. Admissible (tính thừa nhận)
2. Authentic (tính xác thực)
3. Reliable (tính tin cậy)
4. Believable (tính đáng tin)

# TRUY TÌM BẰNG CHỨNG SỐ

Để có được bằng chứng số, nhân viên điều tra phải:

1. Thực hiện quá trình khảo sát
2. Phân tích dữ liệu ban đầu.
3. Nếu tìm được dữ liệu, họ phải xâu chuỗi chúng lại với nhau để đưa ra được bằng chứng



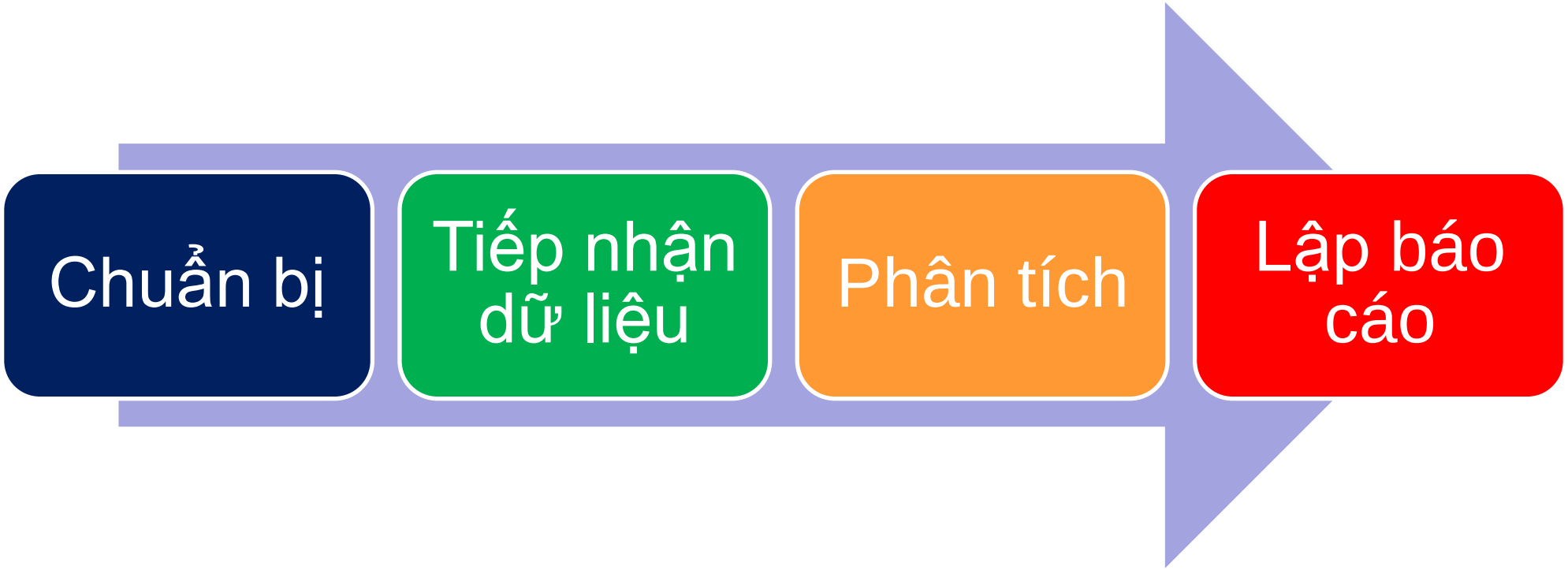

**Chú ý:** Dữ liệu số thu được từ các ổ đĩa trên máy tính hoặc từ các thiết bị lưu trữ khác chưa thể là bằng chứng số

# Ví trí có thể tìm thấy bằng chứng số

1. Trong các tập tin lịch sử truy cập Internet
2. Trong các tập tin tạm sinh ra từ truy cập Internet
3. Tại không gian đĩa chưa cấp phát
4. Nơi lưu trữ các thiết lập tập tin, cấu trúc thư mục, tên tập tin
5. Giá trị thời gian của tập tin
6. Ẩn/nhúng trong phần mềm/phần cứng bổ sung
7. Trong các tập tin chia sẻ
8. Ẩn trong các e-mail
9. …..

# CÁC BƯỚC THỰC HIỆN ĐIỀU TRA SỐ

Theo SANS (SysAdmin, Audit, Networking, and Security) - công ty chuyên đào tạo an toàn thông tin và an ninh mạng, một cuộc điều tra số thường bao gồm 4 gian đoạn: *Chuẩn bị (Preparation), tiếp nhận dữ liệu hay còn gọi là ảnh hóa tang vật (Acquisition), phân tích (analysis) và lập báo cáo (Reporting)*



# CÁC BƯỚC THỰC HIỆN ĐIỀU TRA SỐ

***Preparation:*** Bước này thực hiện việc mô tả lại thông tin hệ thống, những gì đã xảy ra, các dấu hiệu, để xác định phạm vi điều tra, mục đích cũng như các tài nguyên cần thiết sẽ sử dụng trong suốt quá trình điều tra

***Acquisition:*** Đây là bước tạo ra một bản sao chính xác các sector hay còn gọi là nhân bản điều tra các phương tiện truyền thông, xác định rõ các nguồn chứng cứ sau đó thu thập và bảo vệ tính toàn vẹn của chứng cứ

***Analysis:*** Đây là giai đoạn các chuyên gia sử dụng các phương pháp nghiệp vụ, các kỹ thuật cũng như công cụ khác nhau để trích xuất, thu thập và phân tích các bằng chứng thu được

***Reporting:*** Sau khi thu thập được những chứng cứ có giá trị và có tính thuyết phục thì tất cả phải được tài liệu hóa lại rõ ràng, chi tiết và báo cáo lại cho bộ phận có trách nhiệm xử lý chứng cứ thu được, các chuyên gia phân tích phải đưa ra các kỹ thuật điều tra, các công nghệ, phương thức được sử dụng, cũng như các chứng cứ thu được, tất cả phải được giải thích rõ ràng trong báo cáo quá trình điều tra

**1. Chuẩn bị** **2. Tiếp nhận dữ liệu** **3. Phân tích** **4. Lập báo cáo**

# CÁC LOẠI HÌNH ĐIỀU TRA SỐ

**Điều tra số được chia thành một số loại hình chính sau:**

01 Điều tra máy tính (Computer Forensics)

02 Điều tra mạng (Network Forensics)

03 Điều tra số Email (Email Forensics)

04 Điều tra ứng dụng (Application Forensics)

05 Điều tra thiết bị di động (Mobile Device Forensics)

# Thank You !