COMPUTER FORENSICS

Trình bày: Nguyễn Xuân Việt – FPT CIO

NỘI DUNG CHÍNH

01 Khái niệm, truy tìm bằng chứng Computer Forensics

02 Window Log

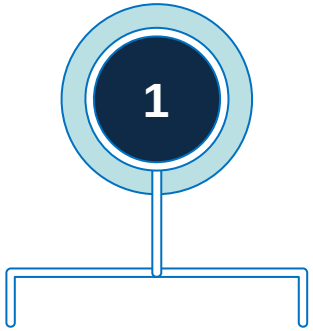
03 Hard Driver Data Recovery

ĐIỀU TRA MÁY TÍNH (COMPUTER FORENSICS)

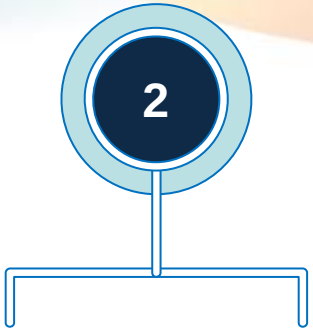
Computer Forensics là: một nhánh của khoa học điều tra số liên quan đến công việc phát hiện, bảo vệ và phân tích thông tin, bằng chứng pháp lý được lưu trữ, truyền tải hoặc được tạo ra bởi một máy tính hoặc mạng máy tính, nhằm đưa ra các suy luận hợp lý để tìm nguyên nhân, giải thích các hiện tượng trong quá trình điều tra.

ĐIỀU TRA MÁY TÍNH (COMPUTER FORENSICS)

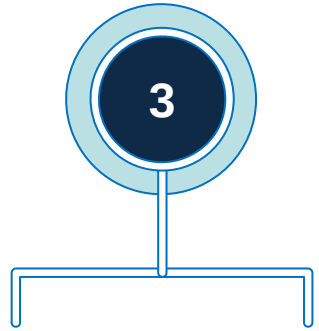
Các bằng chứng có thể tìm thấy trong Computer Forensic như sau:



Điều tra bản ghi (Registry Forensics) là việc trích xuất thông tin và ngữ cảnh từ một nguồn dữ liệu chưa được khai thác qua đó biết được những thay đổi (chỉnh sửa, thêm bớt…) dữ liệu trong bản ghi (Register).



Điều tra bộ nhớ (Memory Forensics) là việc ghi lại bộ nhớ khả biến (bộ nhớ RAM) của hệ thống sau đó tiến hành phân tích làm rõ các hành vi đã xảy ra trên hệ thống. Để xác định các hành vi đã xảy ra trong hệ thống, người ta thường sử dụng kiến trúc quản lý bộ nhớ trong máy tính để ánh xạ, trích xuất các tập tin đang thực thi và cư trú trong bộ nhớ.



Điều tra phương tiện lưu trữ (Disk Forensics) là việc thu thập, phân tích dữ liệu được lưu trữ trên phương tiện lưu trữ vật lý, nhằm trích xuất dữ liệu ẩn, khôi phục các tập tin bị xóa, qua đó xác định người đã tạo ra những thay đổi dữ liệu trên thiết bị được phân tích.

ĐIỀU TRA MÁY TÍNH (COMPUTER FORENSICS)

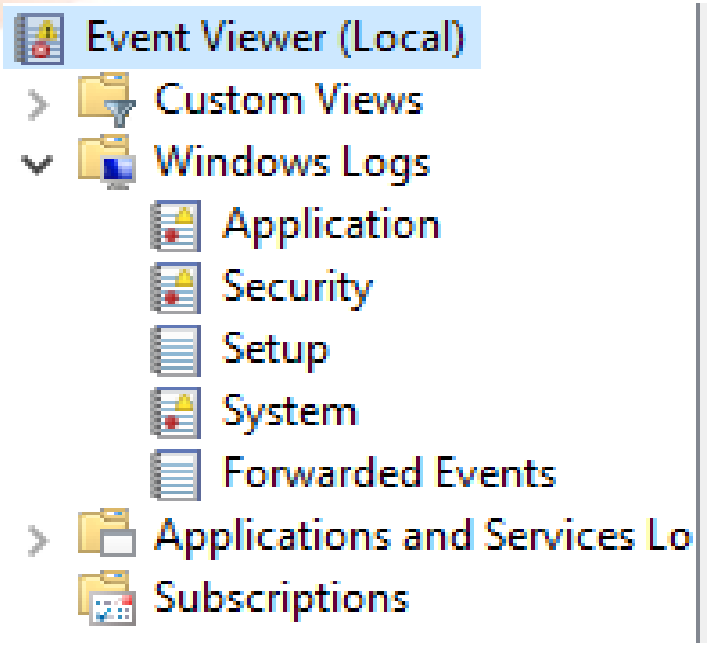
Một số ví dụ các loại điều tra trong điều tra máy tính:

1. Window log
2. Hard Driver Data Recovery
3. Linux log
4. Webserver log, Nginx log

…..

WINDOW LOG

Hệ thống logs của hệ điều hành Window cơ bản có 04 thành phần:

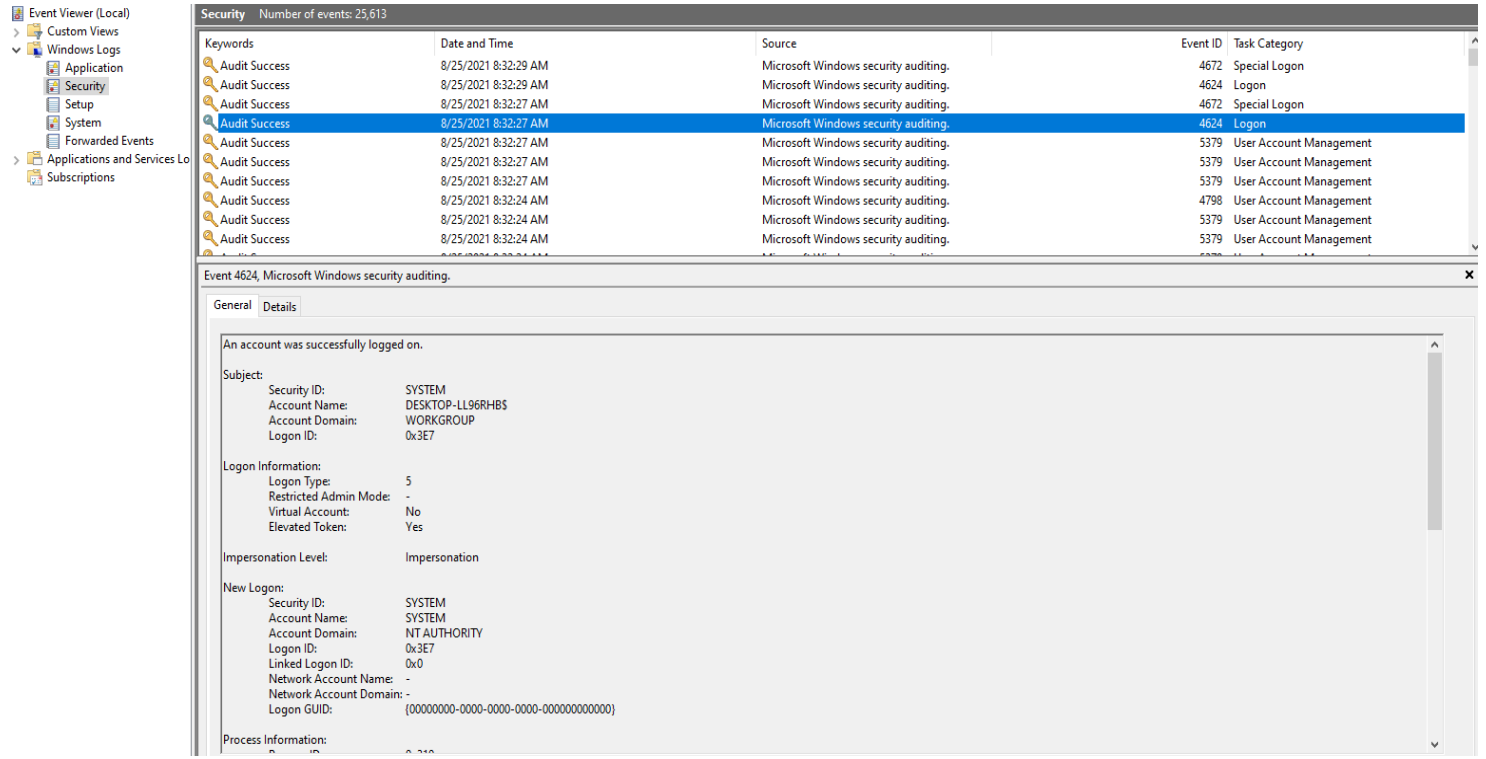


- **Application**: Các sự kiện của các ứng dụng
- **Security**: Các sự kiện đăng nhập/ đăng xuất thành công hay thất bại vào hệ thống. Phần logs này kết hợp với các policy audit giám sát cũng sẽ cung cấp đầy đủ về các sự kiện thêm, sửa, xóa file…
- **Setup**: Các sự kiện khi cài đặt ứng dụng
- **System**: Sự kiện của hệ thống, tắt, bật , enable, disable services

WINDOW LOG

Cấu trúc 1 file log

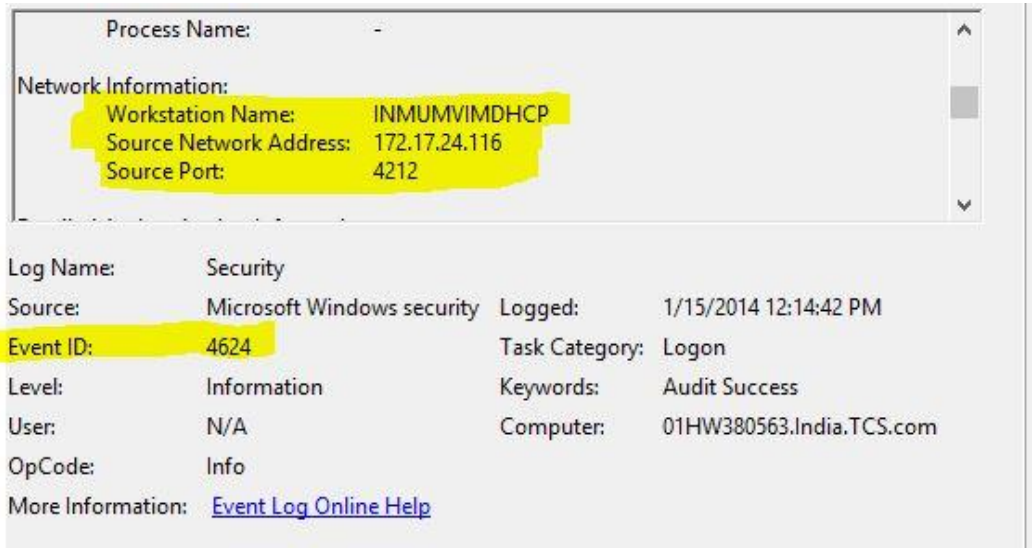
- Event Log của Windows được lưu trữ ở thư mục mặc định tại đường dẫn %systemRoot%\System32\winevt\logs, truy cập vào đây để mở file log hoặc mở Event viewer để xem
- Vào Run → eventvwr



WINDOW LOG

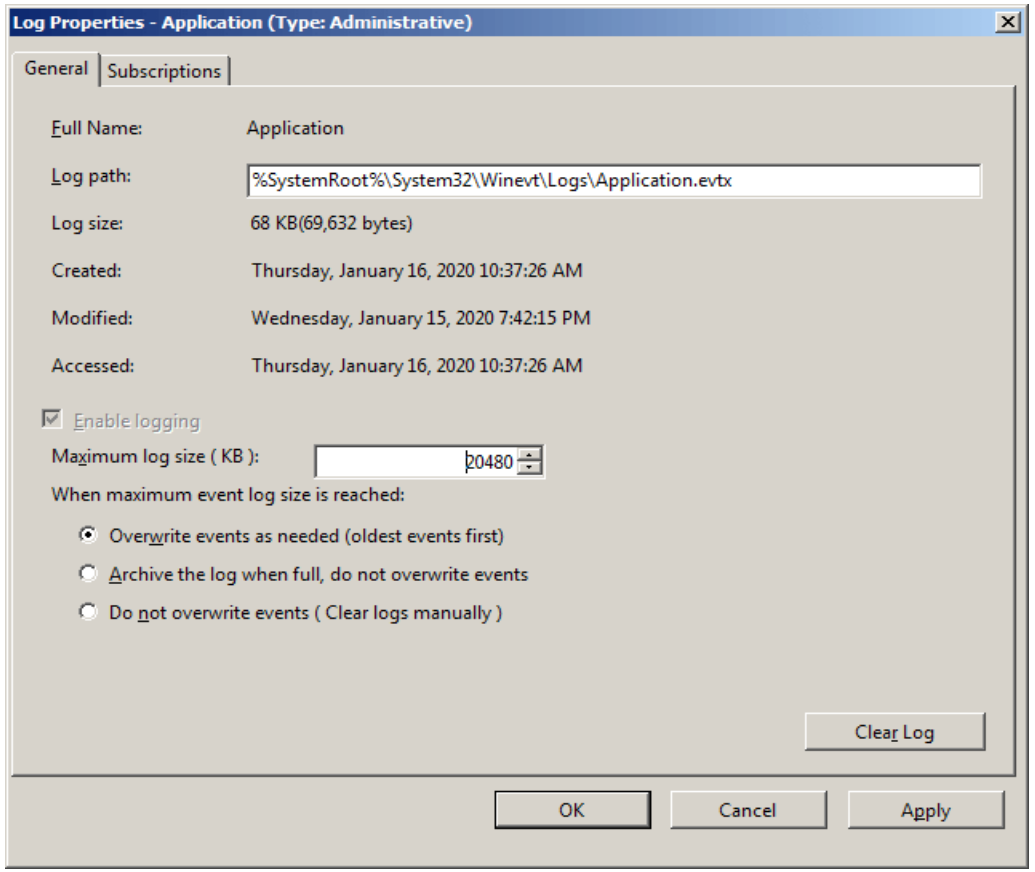
Ví dụ: *1 Event log về xóa file*

#	Tên	Diễn giải
1	Log Name	Tên của log mà sự kiến được lưu trữ, ví dụ như liên quan đến Security thì là Security, nếu là Application thì là Application
2	Source	Là hệ thống/ứng dụng sinh ra log, ví dụ sinh ra bởi McAfee thì là McAfee
3	Event ID	Là mã được gán cho mỗi loại sự kiện (lưu ý trường này để tra cứu)
4	Level	Mức độ của sự kiện, các mức độ Informantion, Error, Warning…
5	User	Là user thực thi liên quan đến sự kiện đang ghi nhận
6	Logged	Thời gian sự kiện được sinh ra
7	Task Category	Là loại danh mục được gán khi log sinh ra, ví dụ: Logon, Audit Policy Change
8	Keywords	Được gán bởi nguồn sự kiện, ví dụ Classic, Audit Success…
9	Computer	Tên máy tính
10	Description	Mô tả chi tiết



WINDOW LOG

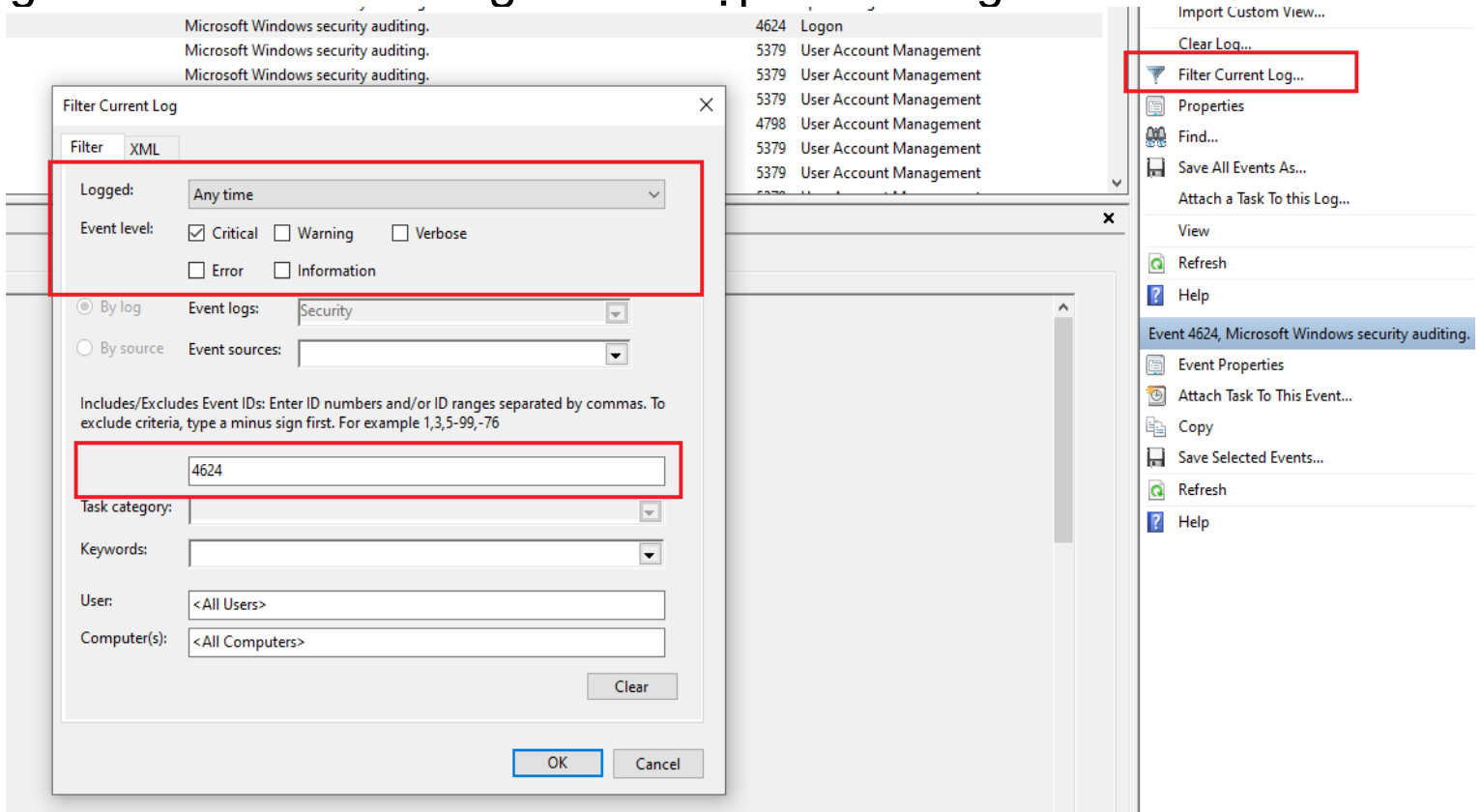
- Kích thước tối đa của mỗi file log là 20MB.
- Khi file log quá giới hạn các bản ghi cũ sẽ bị xóa bỏ. Tùy thuộc vào mục đích chúng ta có thể cấu hình tăng kích thước này lên.



WINDOW LOG

Cách tra cứu window log

- Sử dụng công cụ filter log để lọc các event nghi ngờ liên quan đến việc tấn công
- Vào event log → Filter Current Log… và nhập các thông tin cần tra cứu



WINDOW LOG

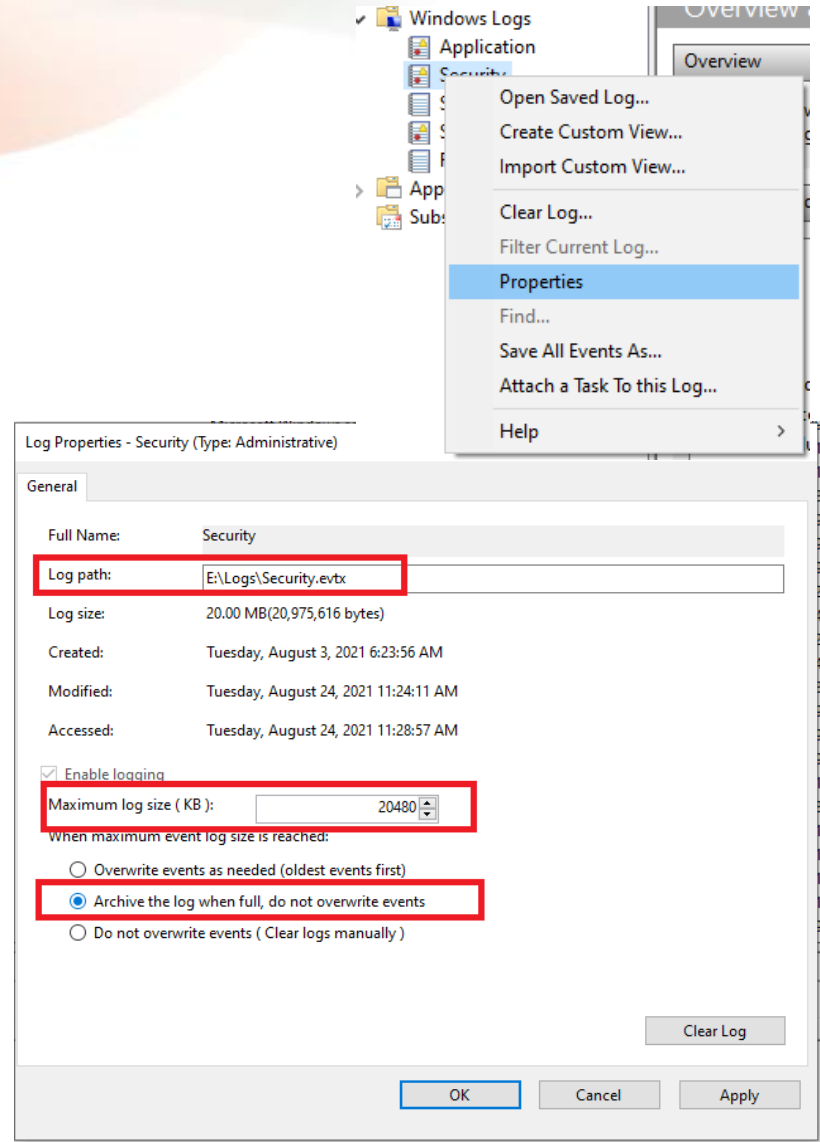
Cấu hình thời gian lưu trữ log:

- Phần log cần được cấu hình đủ lâu để các thông tin được lưu trữ đầy đủ. Chuột phải vào phần Security log → Properties

✓ **Log path:** Chuyển sang ổ lưu trữ khác ổ E, hoặc ổ D. Không lưu ở ổ C

✓ **Maximum log size (KB):** Dung lượng 1 file log tối đa là 20MB - 20248KB

✓ **Archive the log when full, do not overwrite events**: Không xóa log mà tách log ra thành từng file và không xóa file này



Một số loại log cần phải tra cứu

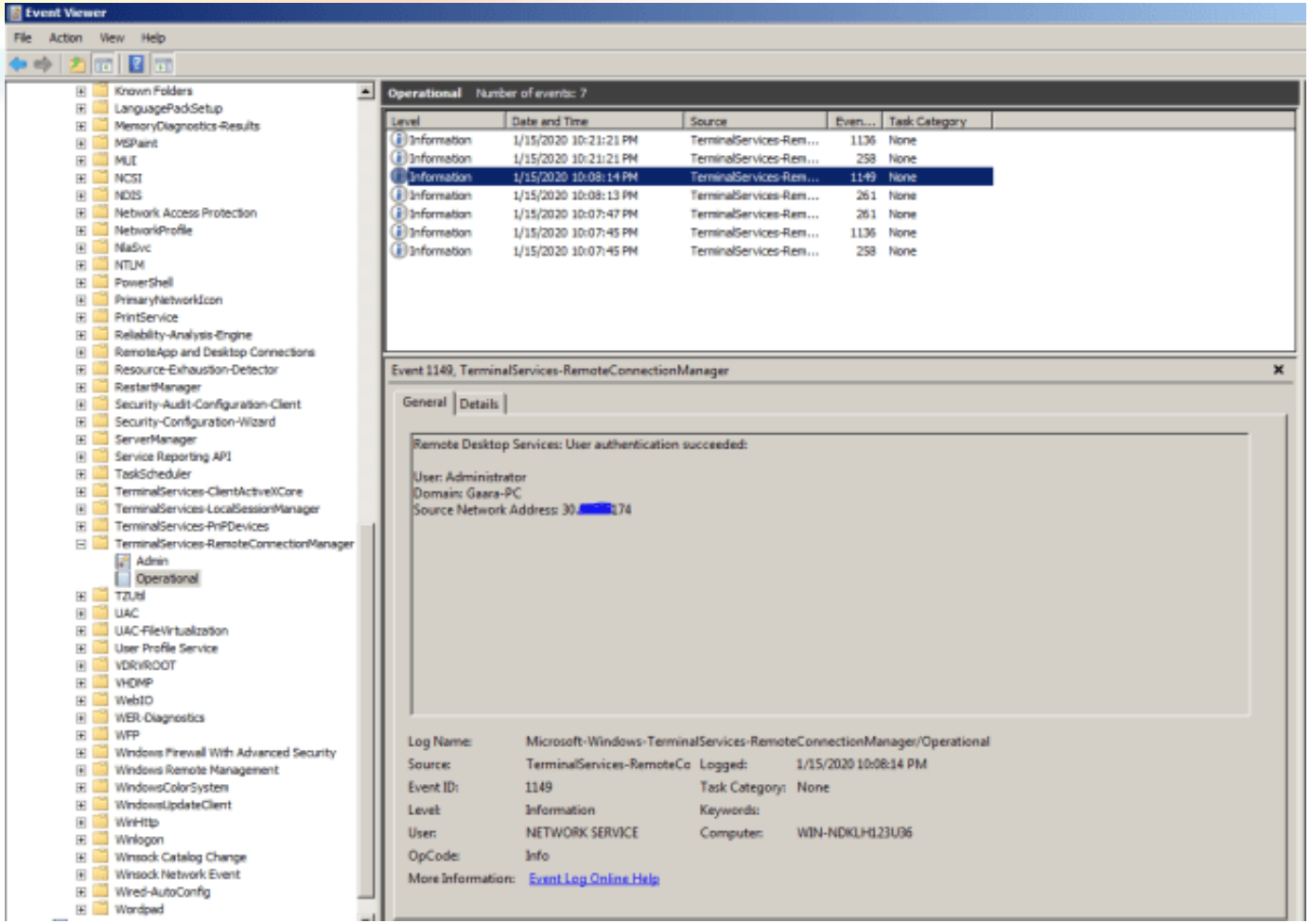
1. Lịch sử Remote Desktop (Event ID = 1149)
2. Lịch sử đăng nhập, đăng xuất (EventID = 4624, 4634, 4676)
3. Lịch sử cài đặt service (Event ID = 7045)

WINDOW LOG

Lịch sử Remote Desktop

(Event ID = 1149)

- Tìm các event mã 1149 để xem lịch sử remote desktop, từ đây chúng ta có thể thấy được rất nhiều thông tin hưu ích như: Địa chỉ IP, User, Domain, thời điểm remote vào server.
- Ví dụ sau thấy được: Máy tính bị remote thông qua Administrator bằng máy có tên Gaara-PC, IP 30.x.x.174 vào lúc 10:08:14 PM ngày 11/01/2020.

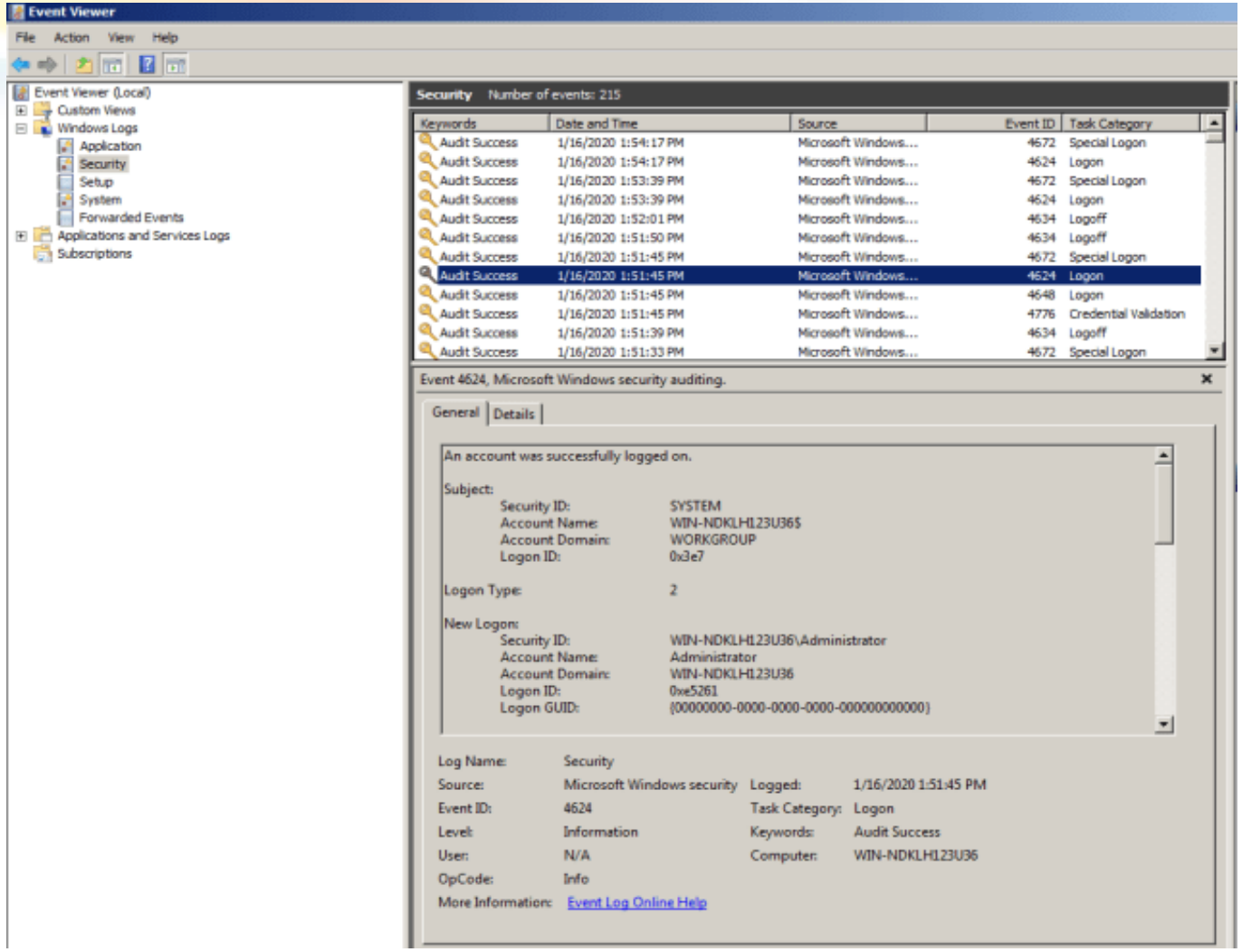


WINDOW LOG

Lịch sử Remote Desktop

(EventID = 4624, 4634, 4676)

- Tìm mã 4024 (logon), 4034 (logoff), 4676 (xác thực) để xem lịch sử đăng nhập, đăng xuất.
- Ví dụ sau thấy được: Thời điểm đăng nhập, đăng xuất, thành công hay thất bại, IP…

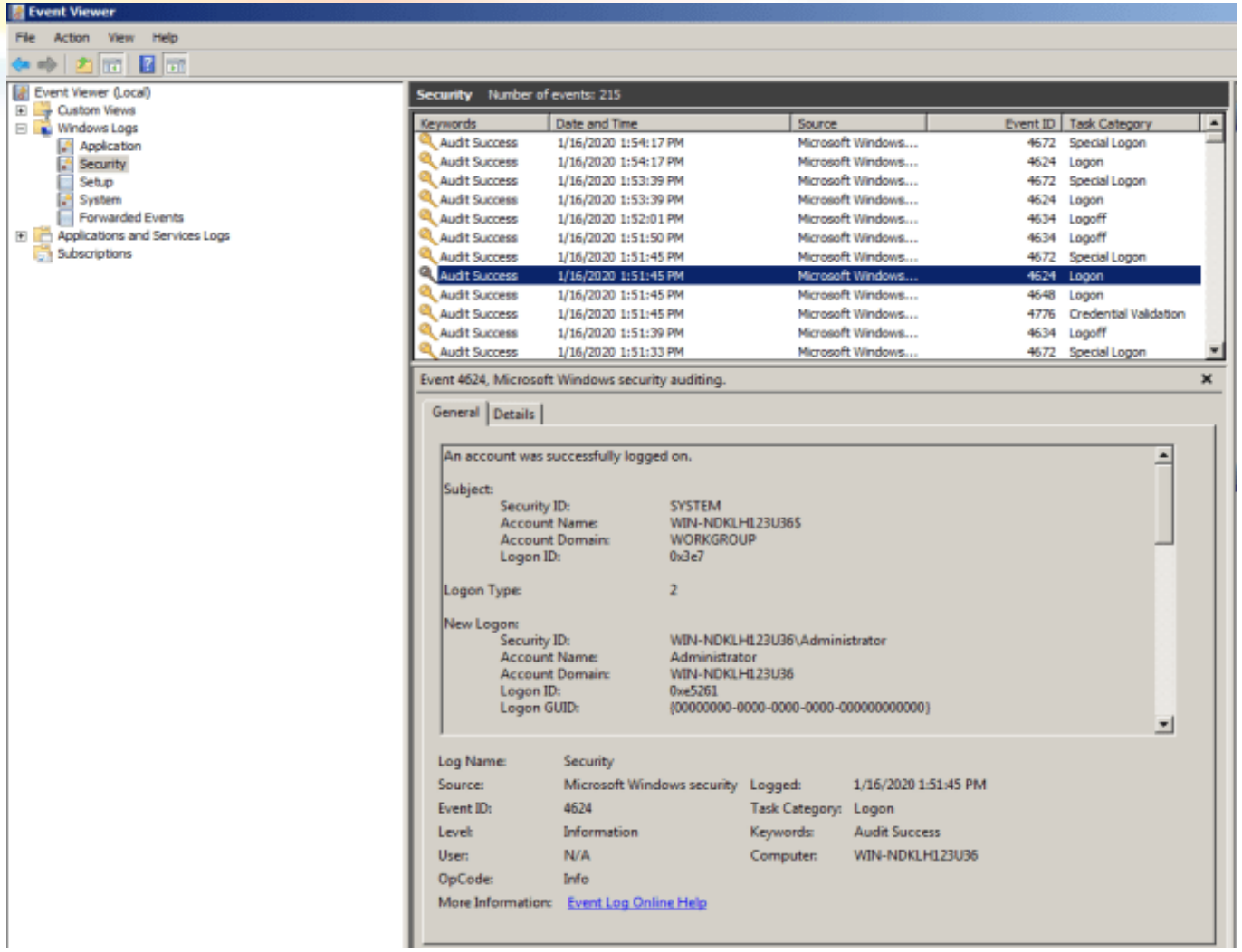


WINDOW LOG

Lịch sử cài đặt service

(Event ID = 7045)

- Tìm mã 4024 (logon), 4034 (logoff), 4676 (xác thực) để xem lịch sử đăng nhập, đăng xuất.
- Ví dụ sau thấy được: Thời điểm đăng nhập, đăng xuất, thành công hay thất bại, IP…



HARD DRIVE DATA RECOVERY

Trong quá trình điều tra bằng chứng số, một số trường hợp phải thực hiện khôi phục lại dữ liệu trong các thiết bị lưu trữ, HDD, SSD, USB

HARD DRIVE DATA RECOVERY

Khi xác định cần lấy dữ liệu của 1 ổ cứng, cần thực hiện ngay:

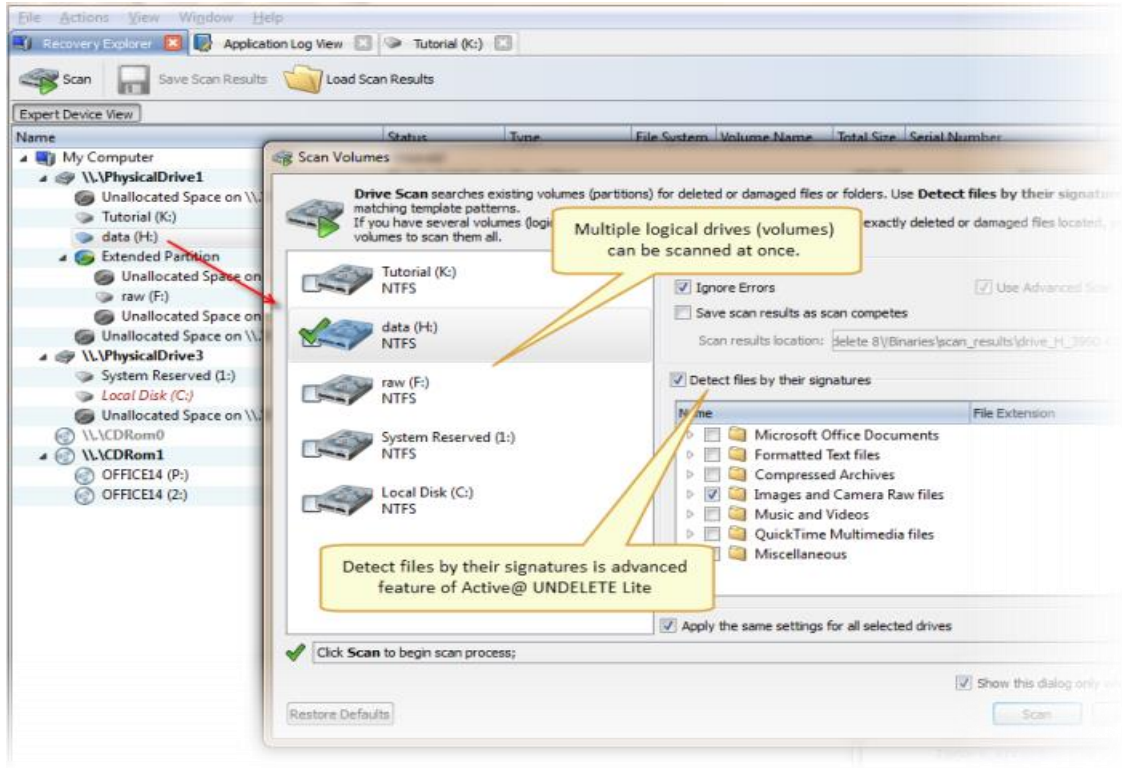
- Dừng các hành động copy, restart thao tác trên máy có ổ cần lấy dữ liêu
- Shutdown máy tính hiện đang sử dụng ổ cứng cần lấy dữ liệu
- Tháo ổ cứng cần lấy dữ liệu lắp sang 1 máy tính khác và cài phần mềm recover trên ổ cứng của máy tính mới này

HARD DRIVE DATA RECOVERY

- **Các phần mềm khôi phục dữ liệu cơ bản (mất phí)**
  - ✓ EaseUS Data Recovery Wizard https://www.easeus.com/datarecoverywizardpro/?x-clickref=1011lhuPH7dG
  - ✓ OnTrack EasyRecovery https://www.ontrack.com/en-us/data-recovery/software
  - ✓ Active@Undelete http://www.active-undelete.com/lite.htm
- **Phần mềm khôi phục dữ liệu chuyên dụng**
  - ✓ PC300 là một trong những phần mềm hàng đầu được nhiều cơ quan an ninh trên thế giới sử dụng: PC-3000 Portable III Systems || Professional Hardware-Software Solutions for Data Recovery & Digital Forensics. ACE Lab, the Czech Republic (acelaboratory.com)

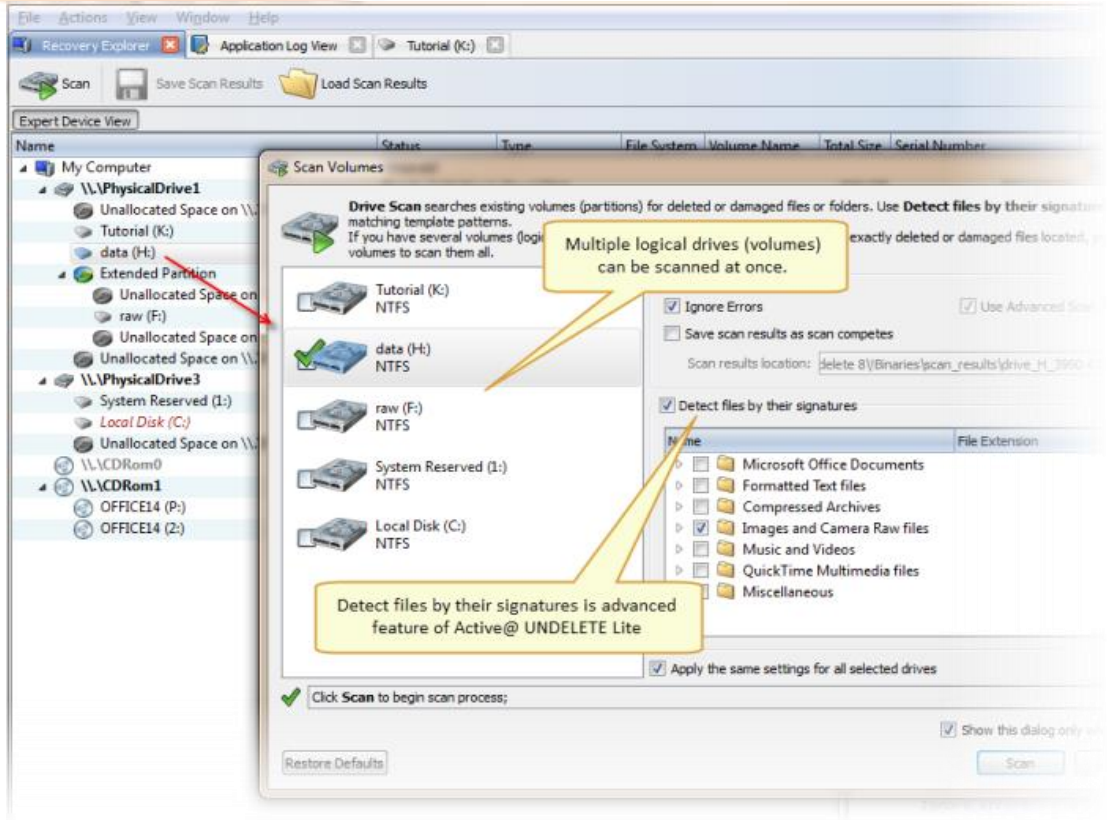
HARD DRIVE DATA RECOVERY

- Khi sử dụng các phần mềm cơ bản sẽ có 2 chế độ: **Logical Scan (Volume)** và **Hardisk scan (Advanced scan)**
- **Logical Scan (Volume)**: Scan những file, thư mục bị xóa mà chưa bị ghi đè, đang còn MFT
  - ✓ *Ưu điểm*: Scan nhanh, view được cấu trúc file, thư mục, tỉ lệ file bị lỗi thấp
  - ✓ *Nhược điểm*: Không lấy được các file nếu bị mất MFT



HARD DRIVE DATA RECOVERY

- **Hardisk scan (Advanced scan)**
  - *Ưu điểm:* Scan ở mức block nên sẽ tìm được những file đã bị xóa cả MFT hoặc 1 phần của file bị ghi đè
  - *Nhược điểm:* Scan lâu, không hệ thống lại thành thư mục nên kết quả trả ra sẽ khó để tìm kiếm hoăc phân loại, dữ liệu khôi phục có thể không toàn vẹn



Thank You !