LAB 14

Thầy Mai Hoàng Đỉnh
Trường đại học FPT

Người thực hiện
Đặng Hoàng Nguyên

Lab-Project 13: NetWitness

What You Need

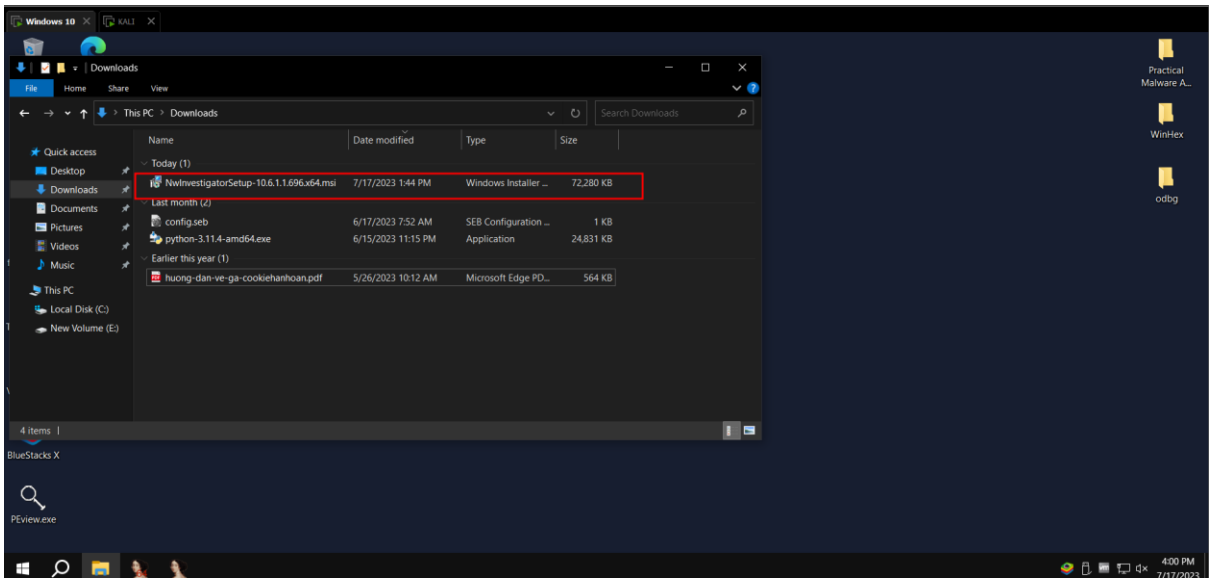
- Chúng ta sẽ sử dụng các máy windows phiên bản cao như là windows 7 hoặc 10 trở lên

Installing NetWitness

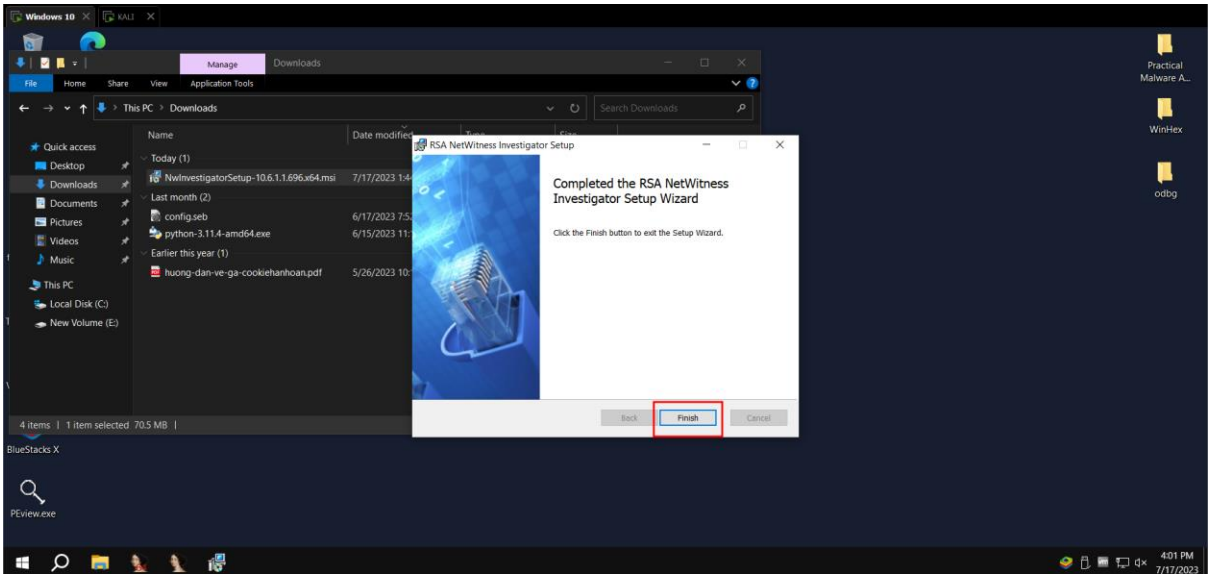
Trong trình duyệt chúng ta sẽ vào trang web này và download

- http://www.emc.com/security/rsa-netwitness.htm#!freeware

Vì một số lý do nên link đã chết nên chúng ta sẽ tìm một nơi khác để Donwload, có thể dung file bên trong file tool trong onedrive mà chúng ta được cung cấp. Sau khi download xong, có một file mang tên là **NwInvestigatorSetup.exe** (131 MB) xuất hiện eben trong thư mục download của chúng ta.



Click đúp vào và chọn những cài đặt mặc định theo như chương trình. Dưới đây là hình sau khi cài đặt thành côgn

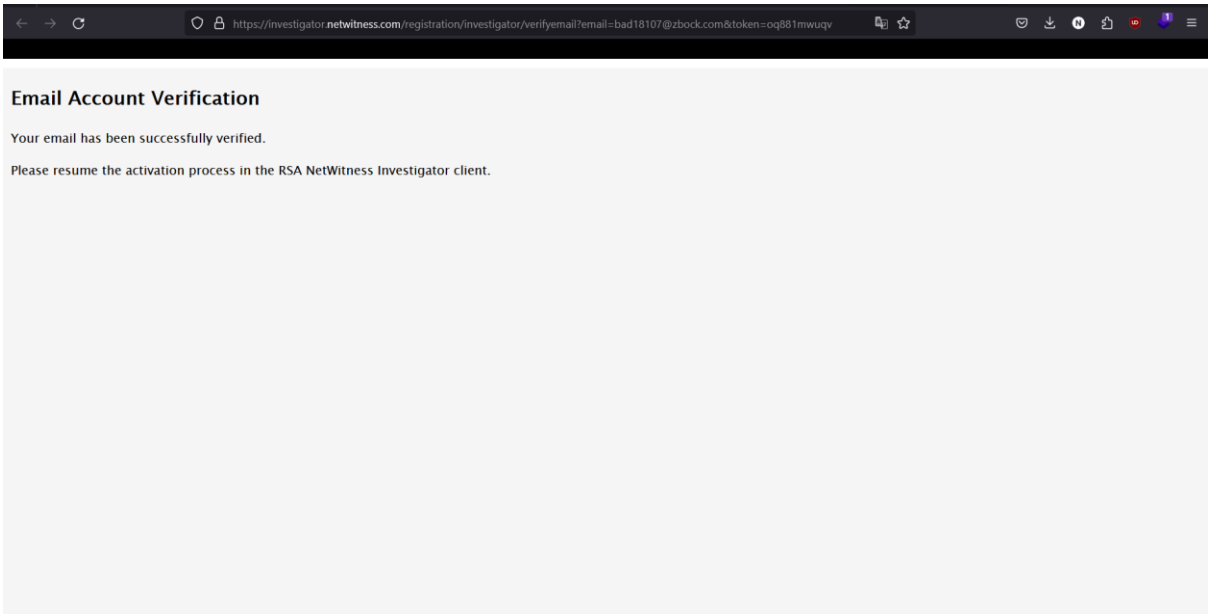


Trên màn hình desktop, nhấn click vào "**NetWitness Investigator 9.6**" icon.

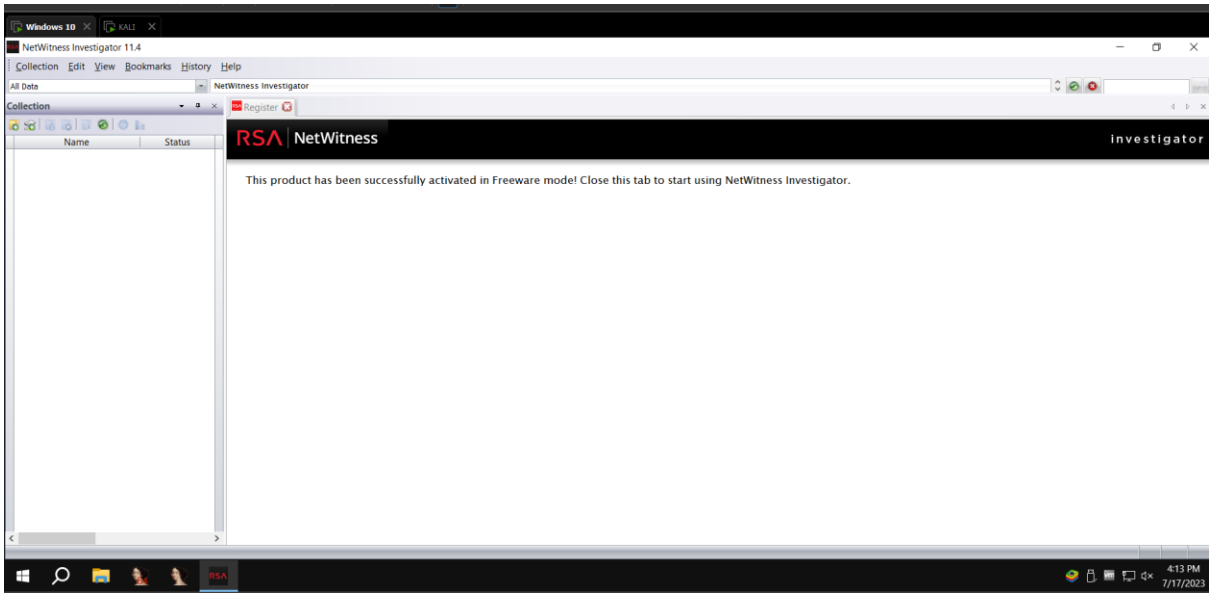
Khi chương trình bắt đầu chạy, một cnarh báo được xuấ hiện lên và báo "Revocation information for the security certificate for this site is not available...". Nhấn **Yes** để bỏ qua các cảnh báo

Điền thông tin vào bên trong phần submit

Sau đó check mail cho activation code, làm theo chỉ dẫn đẻ kích hoạt tài khoản NetWitness



NetWitness đã được kích hoạt, xem như hình dưới đây:

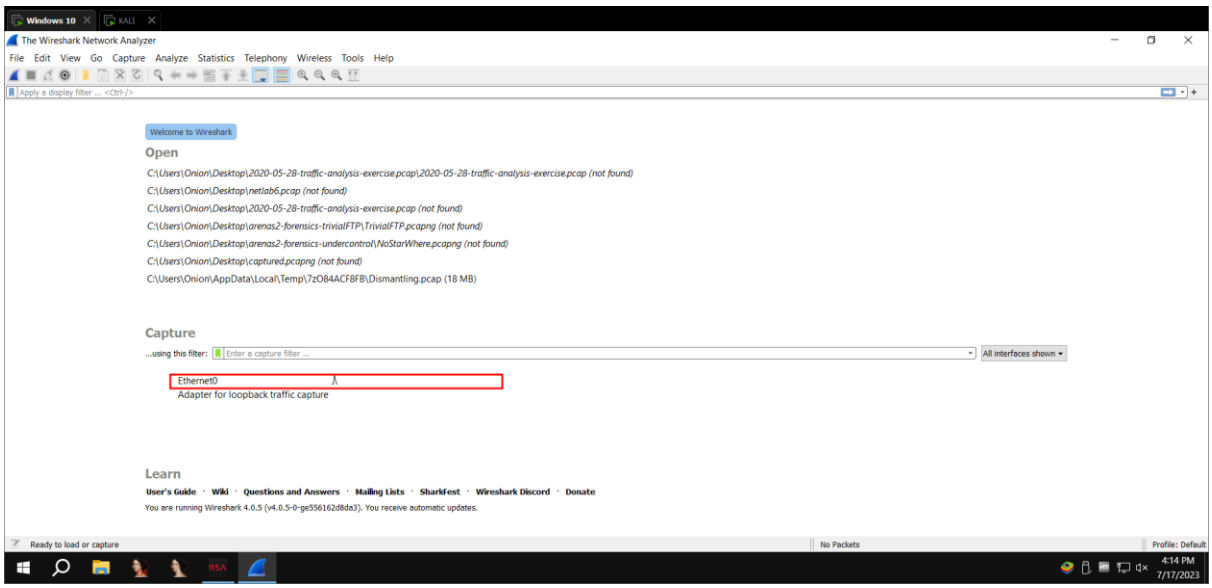


Getting Wireshark

Nếu chúng ta không có wireshark hãy cài theo đường dẫn bên dưới

- http://www.wireshark.org/

Chạy Wireshar và chọn phần card nic nào có thể đi ra bằng internet

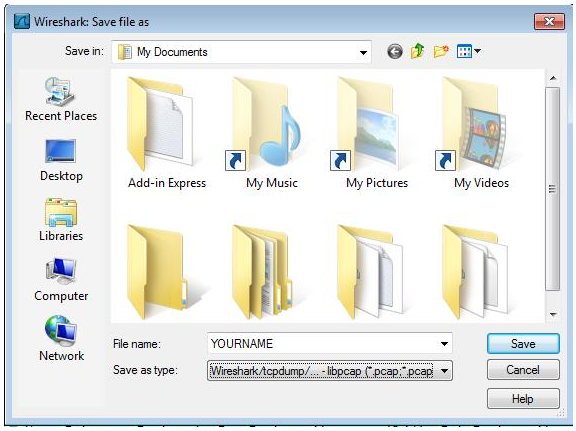


Gathering Evidence

Mở trình duyệt lên và làm theo các bước sau

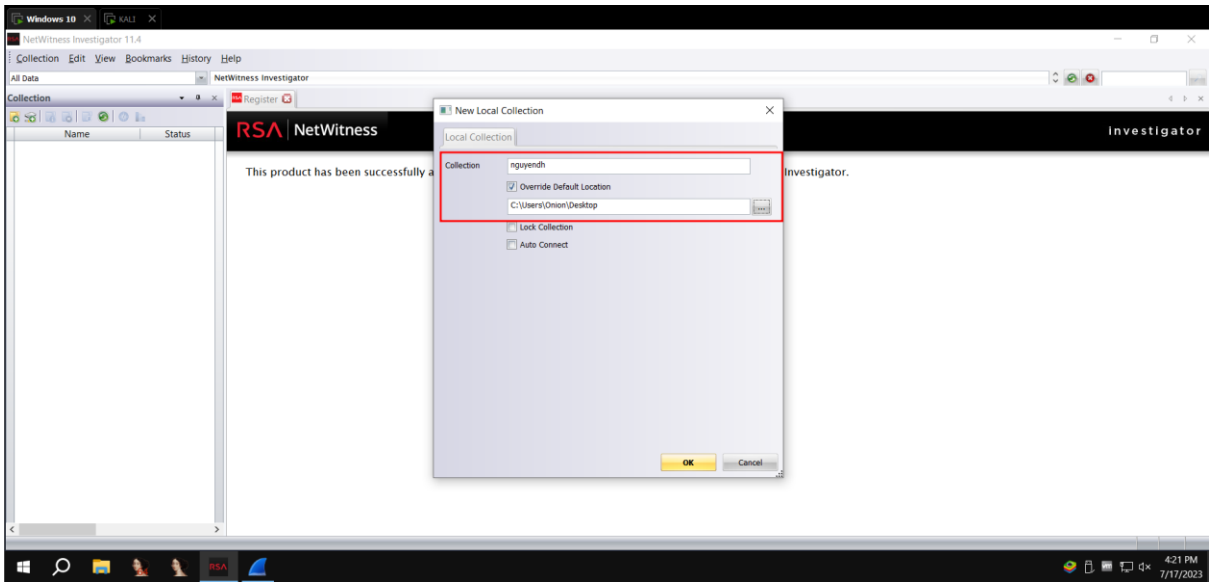
- Vào bên trong http://en.wikipedia.org/ và đăng nhập vào tài khoản wiki của chúng ta
- Trong Wikipedia, chúng ta tìm mới nhóm “Anonymous” và load về phần hoạt động
  - Sau đó tìm tới trang này: http://samsclass.info

Sau đó ngừng lại và lưu dưới tên của mình. Trong trường hợp này sẽ là nguyendh.pcap



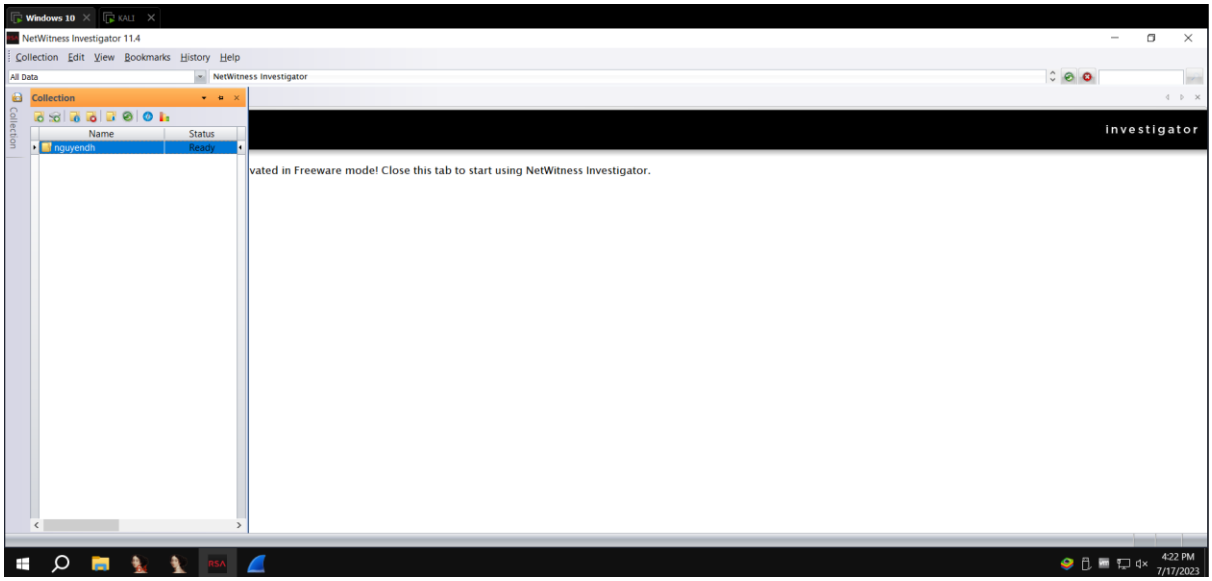
Importing the Evidence into NetWitness

Trong NetWitness, tỏng menu bar, nhấn **Collection**, "**New Local Collection**". Như hình bên dưới



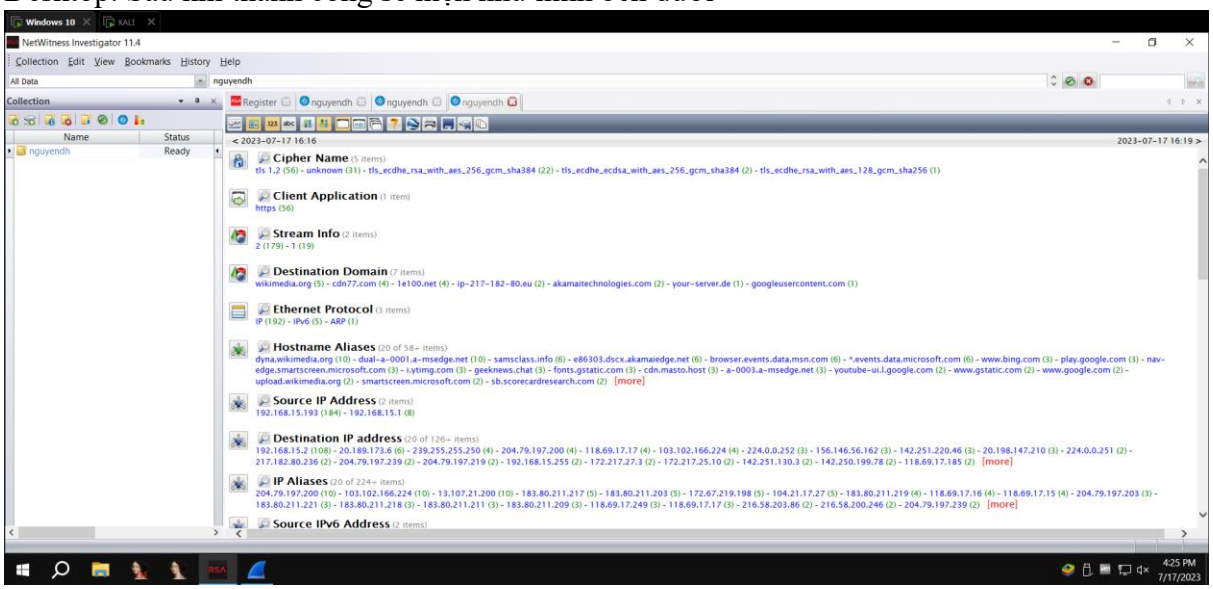
Nhấn ok

Trong thanh bên trái của NetWitness, nhấn chuột vào nguyendh như hình bên dưới:



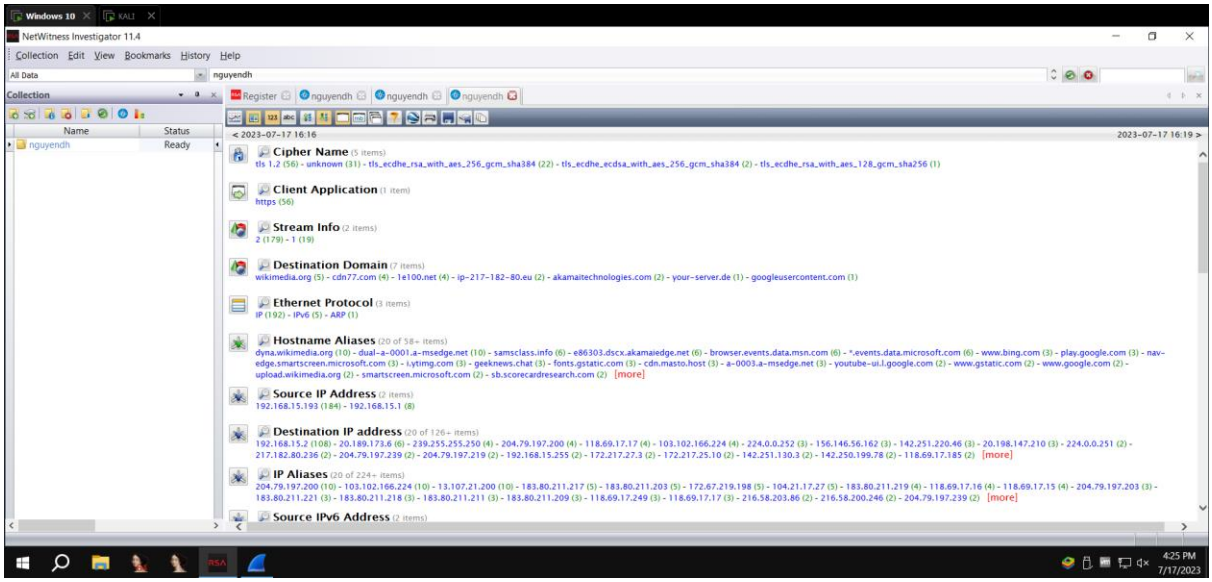
Trong NetWitness, từ thanh menu nhấn chọn **Collection**, "**Import Packets**".

Trỏ tới phần file pcap mà chúng ta đang sử dụng. Trong trường hợp này sẽ được lưu tại Desktop. Sau khi thành công sẽ hiện như hình bên dưới



Analyzing Evidence

Trong phần Collecctions của NetWitness, nhán chuột vào nguyendh, có một bảng báo cáo được xuất hiện như hình dưới đây



Có một số thứ chúng ta sẽ cần phải để ý ở phía bên dưới

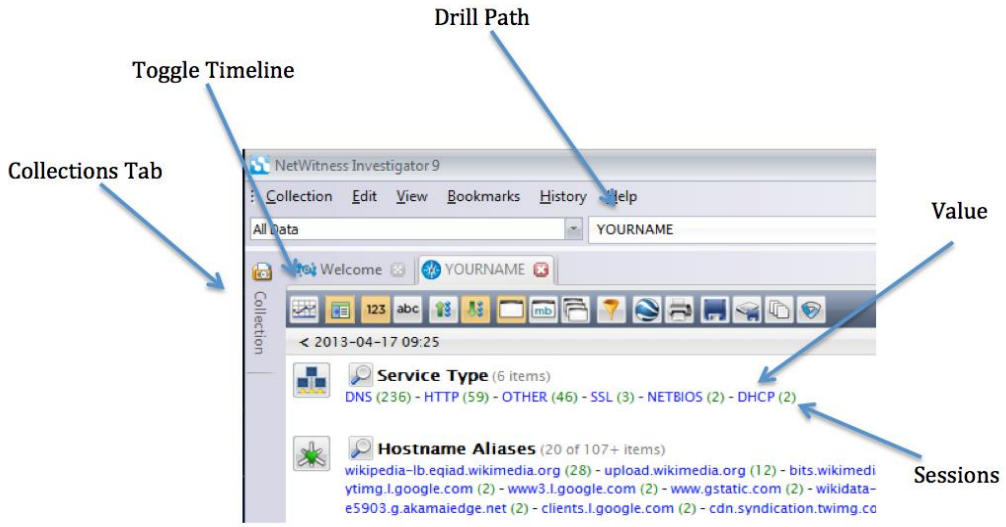
● Tab Collections đã thu nhỏ về phía bên trái để không cản trở

● Nút Toggle Timeline hiển thị biểu đồ dữ liệu

● Đường đi Drill Path hiển thị các bộ lọc đã được áp dụng để loại bỏ dữ liệu không quan trọng - hiện tại chúng ta đang xem tất cả dữ liệu trong bộ sưu tập YOURNAME.

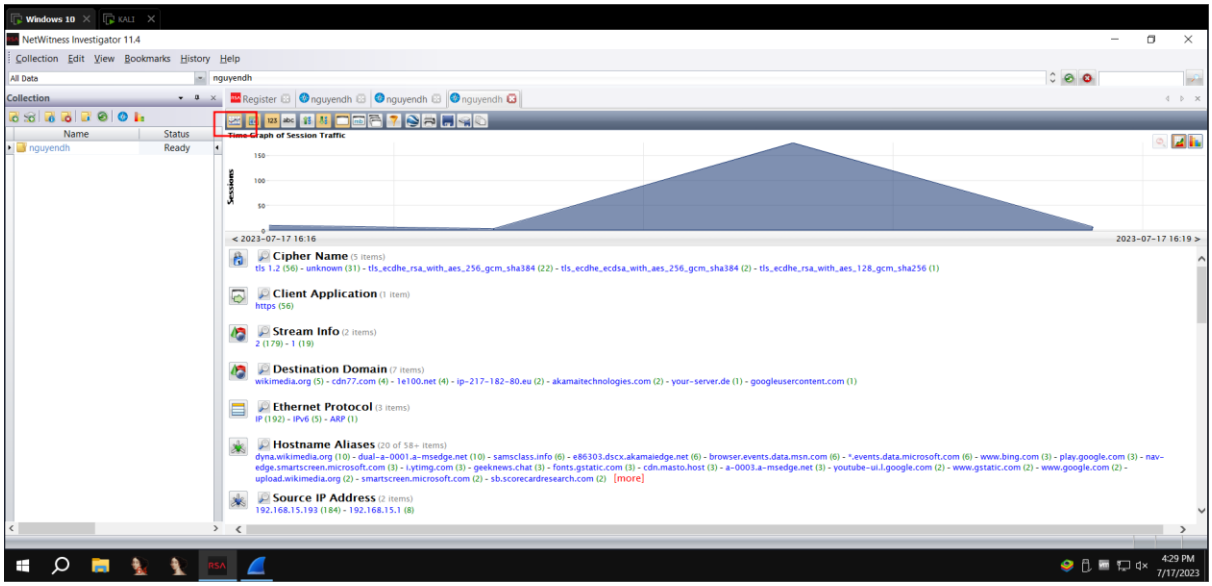
● Trong Báo cáo, xuất hiện các cặp mục: Một Giá trị theo sau là số phiên trong ngoặc đơn, ví dụ DHCP (2).

Vì không biết edit nên sẽ dung hình của đề đã cho



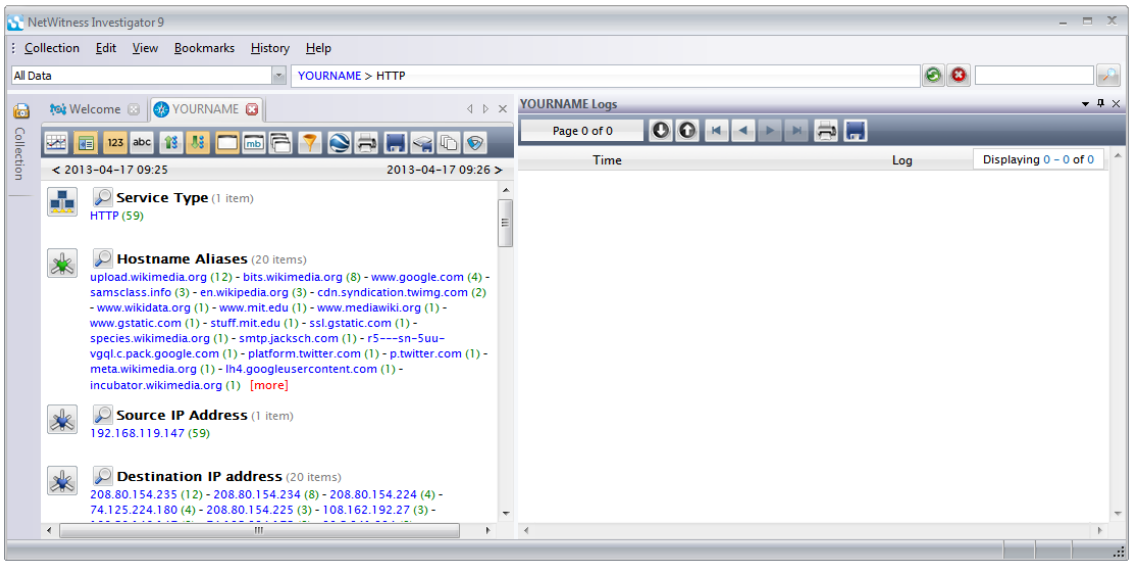
Nhấn chọn vào nút **Toggle Timeline** để nhìn thấy Timeline, như hình bên dưới.

Biểu đồ này hiển thị lưu lượng dữ liệu dưới dạng đồ thị và có thể được sử dụng để tập trung vào các khoảng thời gian cụ thể. Tuy nhiên, trong dự án này, nó không hữu ích, vì vậy hãy nhấp vào nút "Toggle Timeline" một lần nữa để ẩn nó đi.

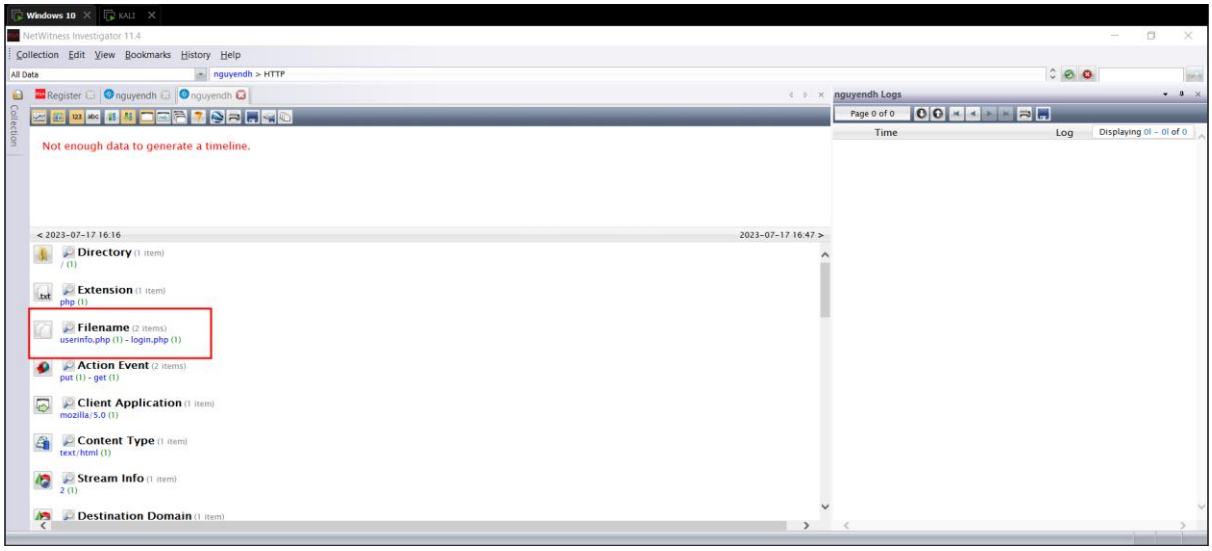


Finding the Login account

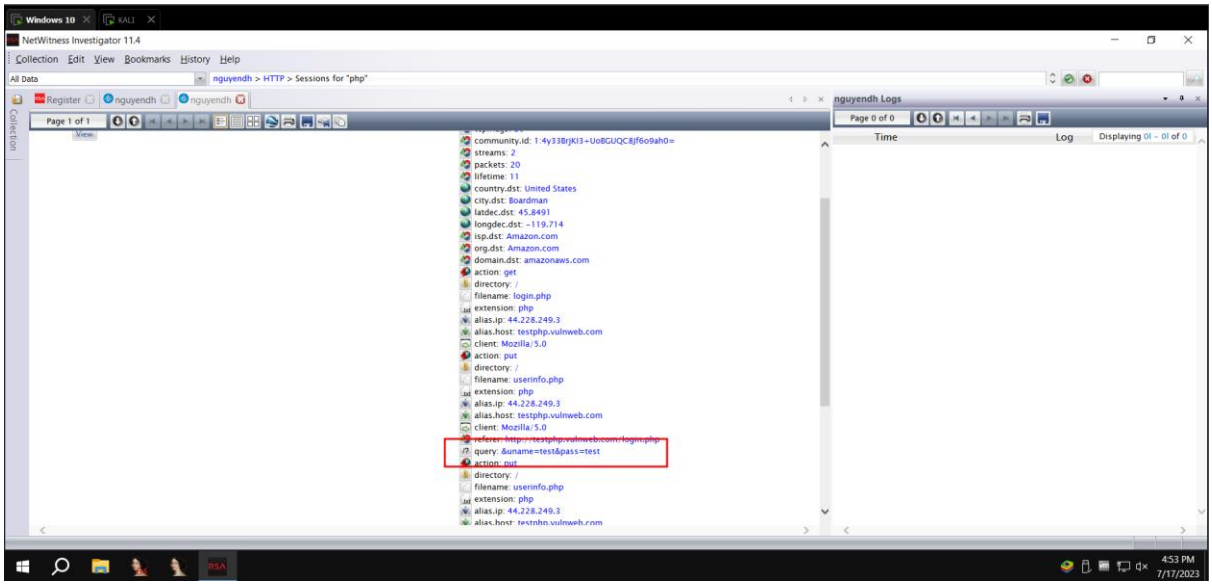
Trong phần đầu của Báo cáo, có tiêu đề "Service type", hãy nhấp vào liên kết màu xanh dương có chữ HTTP. Điều này sẽ lọc ra tất cả lưu lượng không phải là HTTP. Được hiển thị như hình dưới đây



Bây giờ chúng ta sẽ tiên shanfg xem các gói http



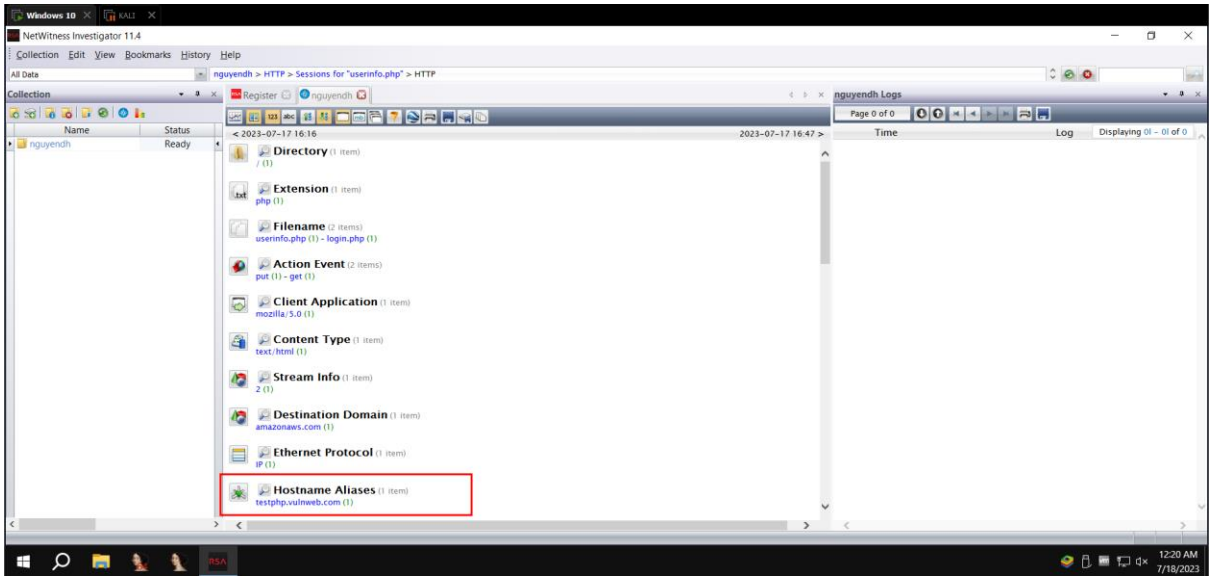
Vào trong phần query chúng ta sẽ thấy được phần uname và password là test, đây là phần mà chúng ta nhập vào bên trong web để login thành công



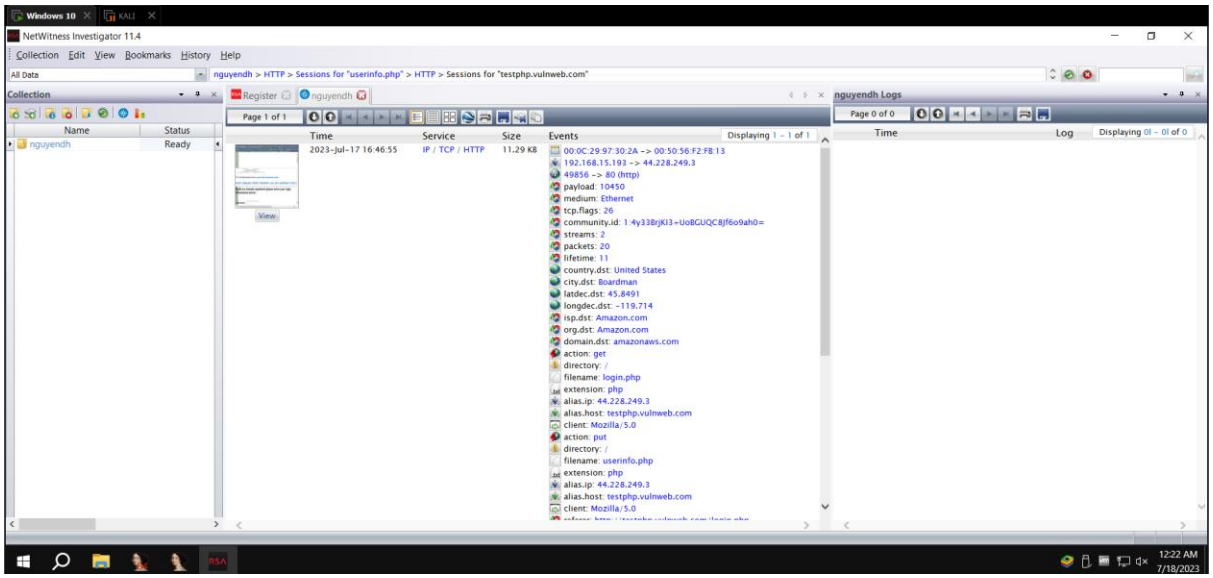
Viewing a Reconstruction

Phía trên của NetWitness, trong phần Drill Path, nhấn vào phần **HTTP**.

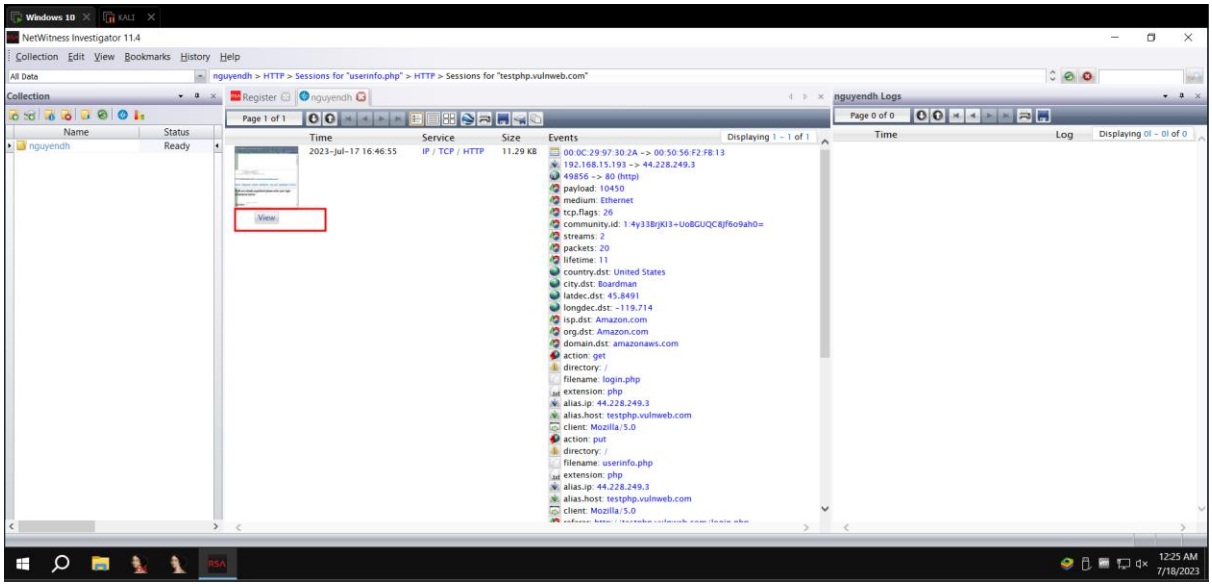
Trong phần "Hostname Aliases" , nhấn chọn vào **testphp.vulnweb.info**



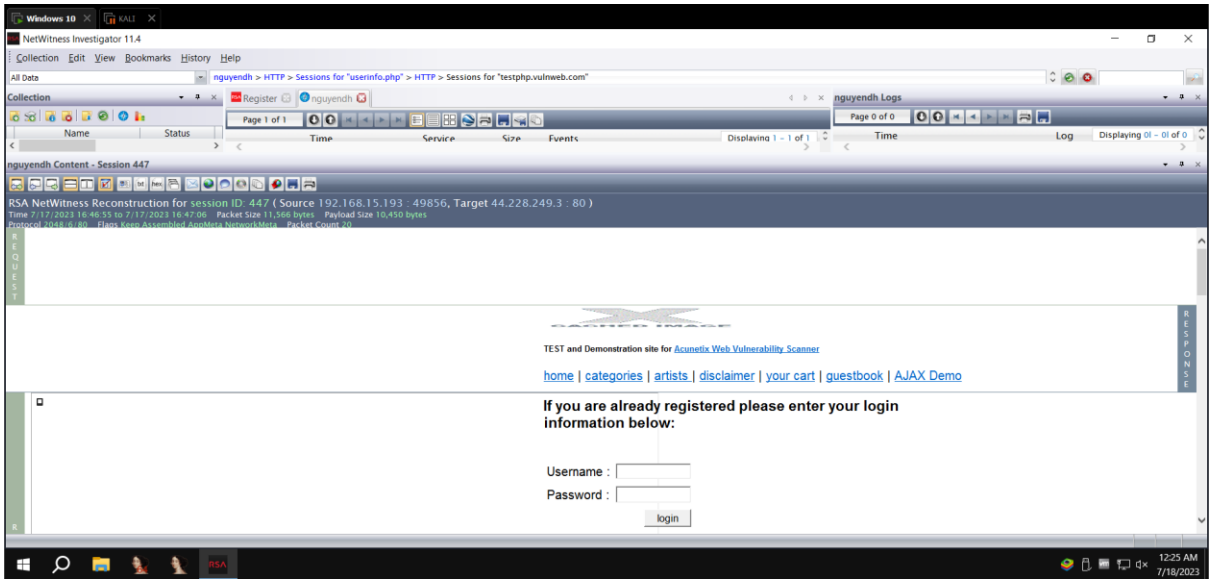
Nhấn vào phần số kế bên chữ testphp.vulnweb.com để có thể xem các thông tin về web đó như hình bên dưới



Nhấn vào phần view trong phần như dưới đây để có thể tái hiện lại trang web đó như hình bên dưới đây:

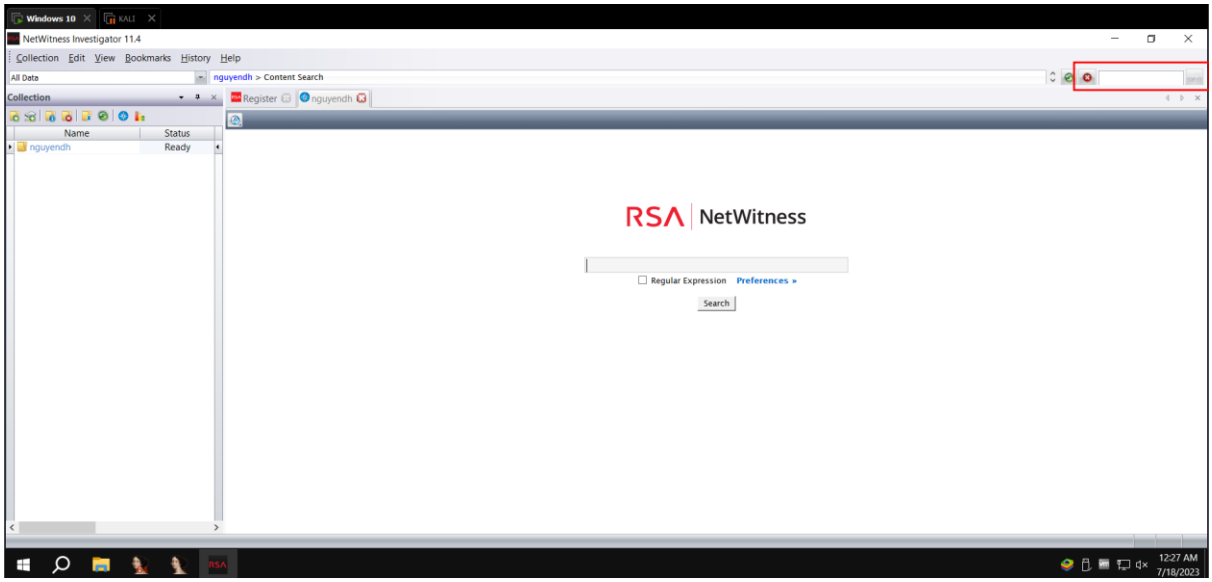


Chúng ta có thể thấy ằng bây giờ netwitness sẽ tự build lại một trang web dựa trên gói http của chúng ta

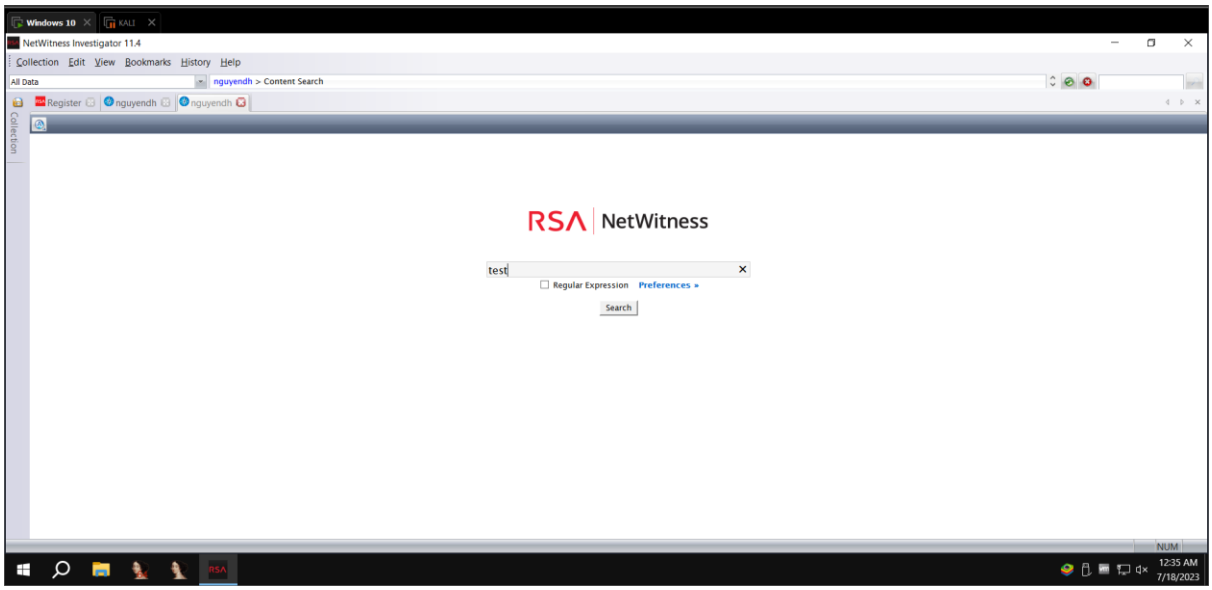


Searching

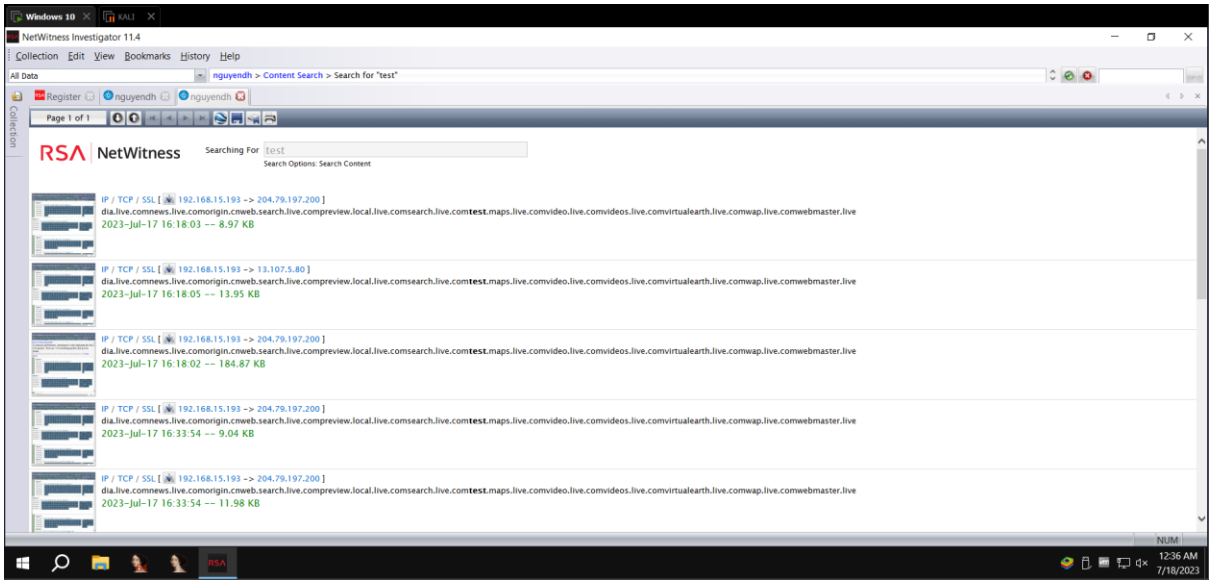
Trên cùng của NetWitness, chúng ta sẽ nhấn vào phần YOURNAME, trong tường hợp này là nguyendh. Bên tay phải, nhấn phần kính lúp như hình bên dưới đây



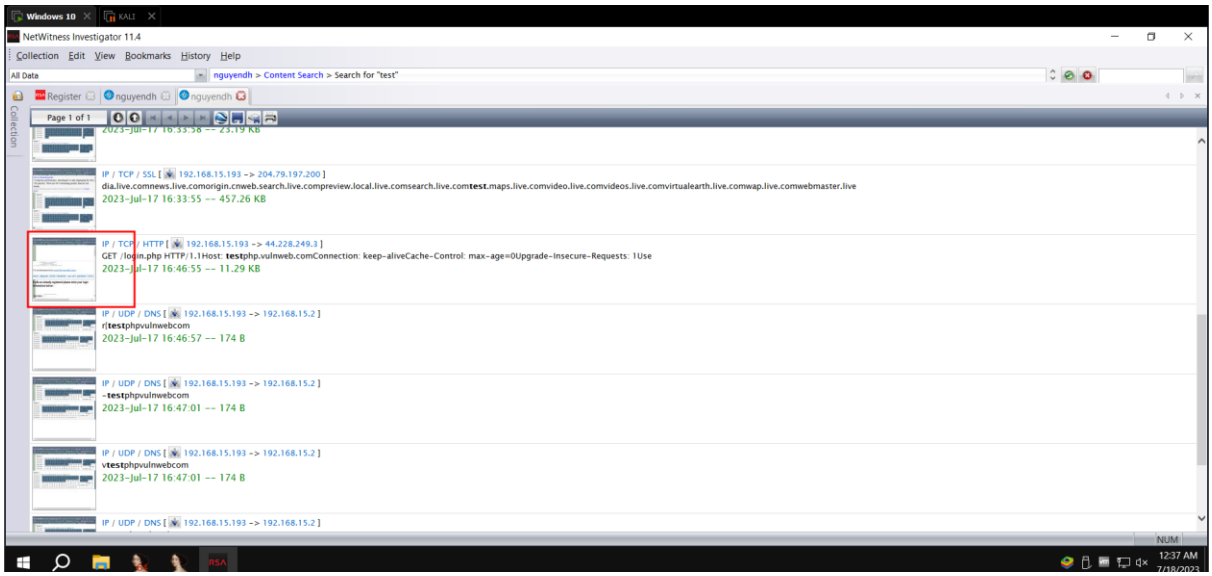
Click và nhấn search “test” để tìm tới cái web mà chúng ta đã sử dụng để đăng nhập

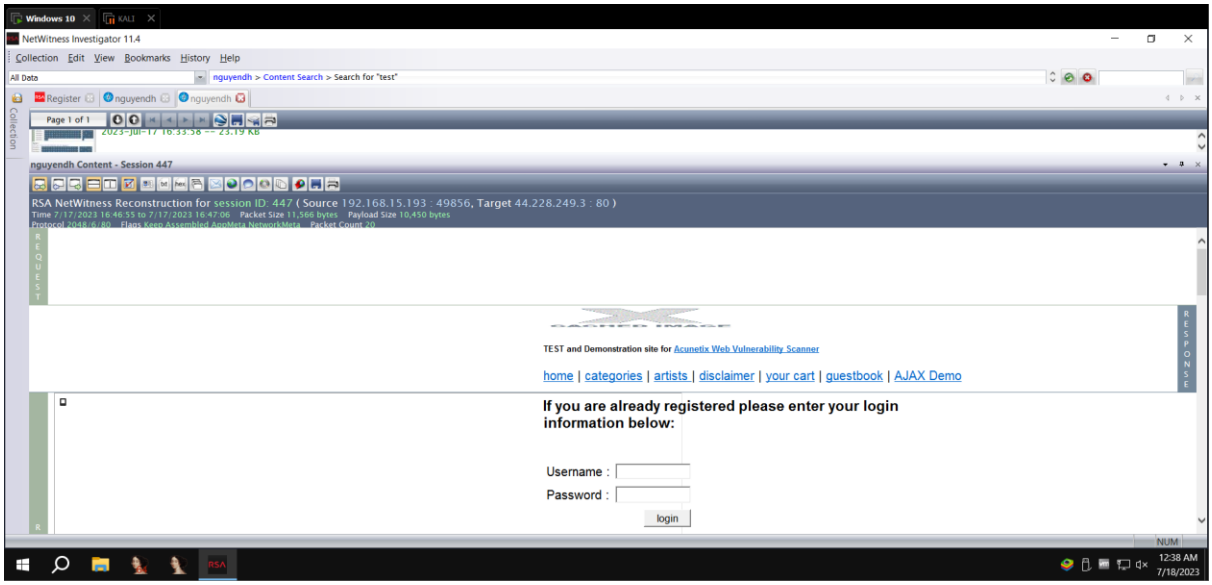


Có một số báo cáo về việc tìm thấy test bên trong những gói tin khác nhau như hình dưới đây



Click vào chỗ như hình bên dưới thì netwitness sẽ tự động reconstruct lại trang web cho chúng ta





Lab-Project 14: Finding Items with NetWitness

Getting the PCAP File

Tải file pcap theo đườn dẫn dưới đây:

3items.pcap

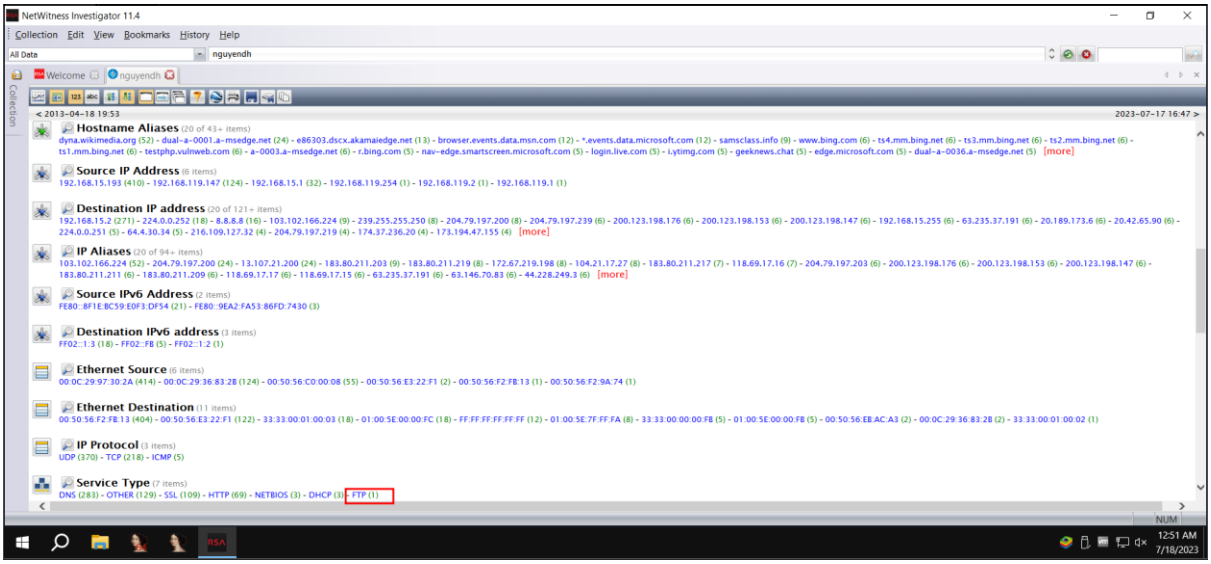
Kiểm tra MD5 của file bằng HashCalcc. Nếu đúng thì giá trị của md5 sẽ là 45094695ea765c54bfe80393d2d68f24.

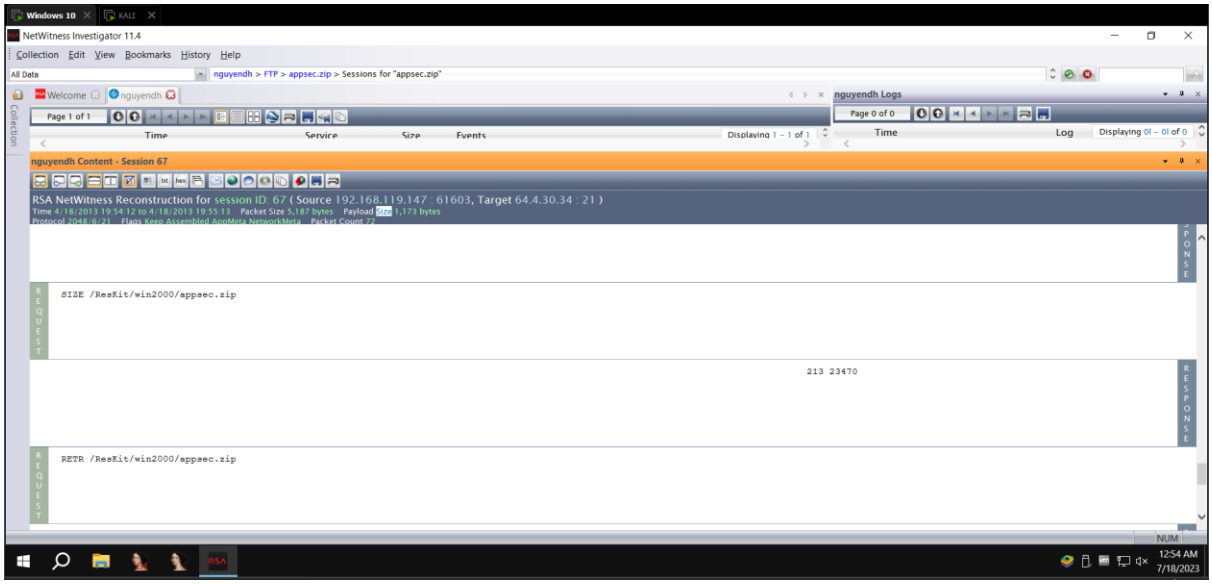
Task

Load file vào bên trong netwitness

FTP Download

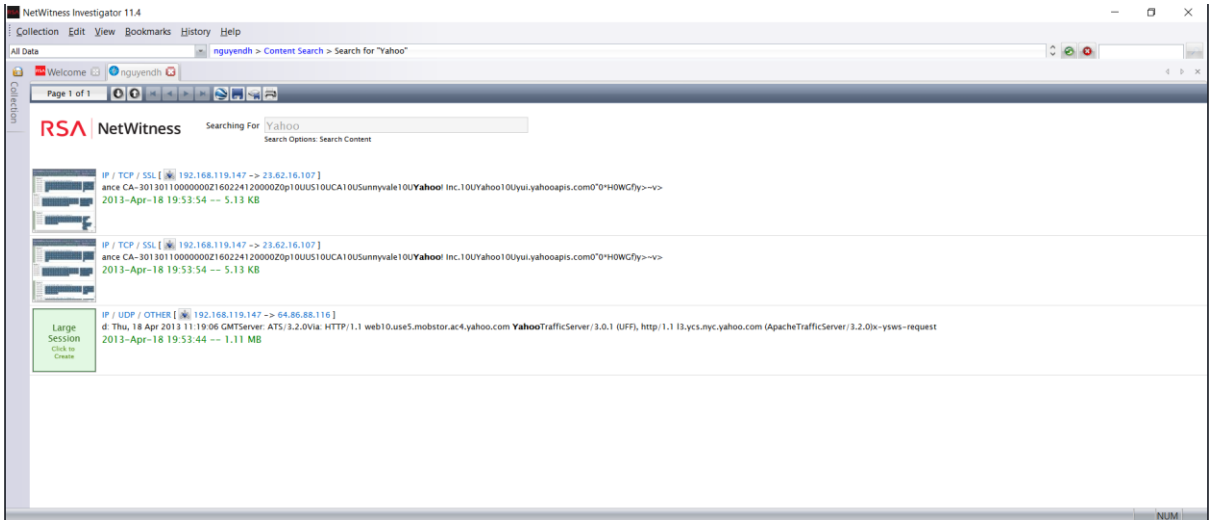
Vào bên trong phần service type, chọn vào phần FTP



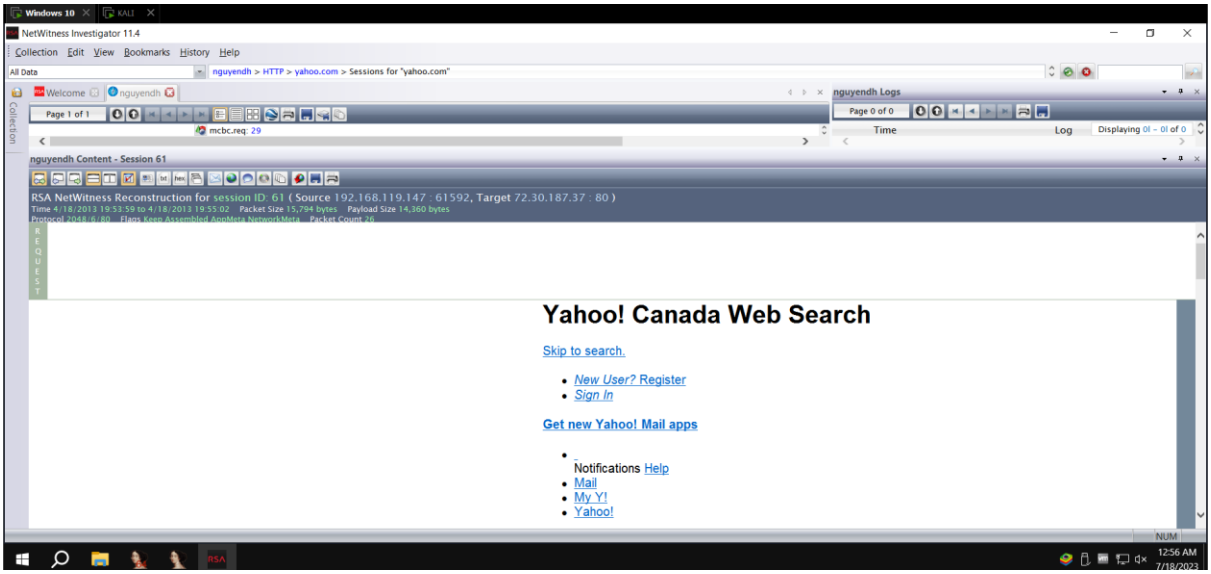


Yahoo Search

Trong phần search, search chữ “Yahoo” và ta sẽ ra được các kết quả như sau:

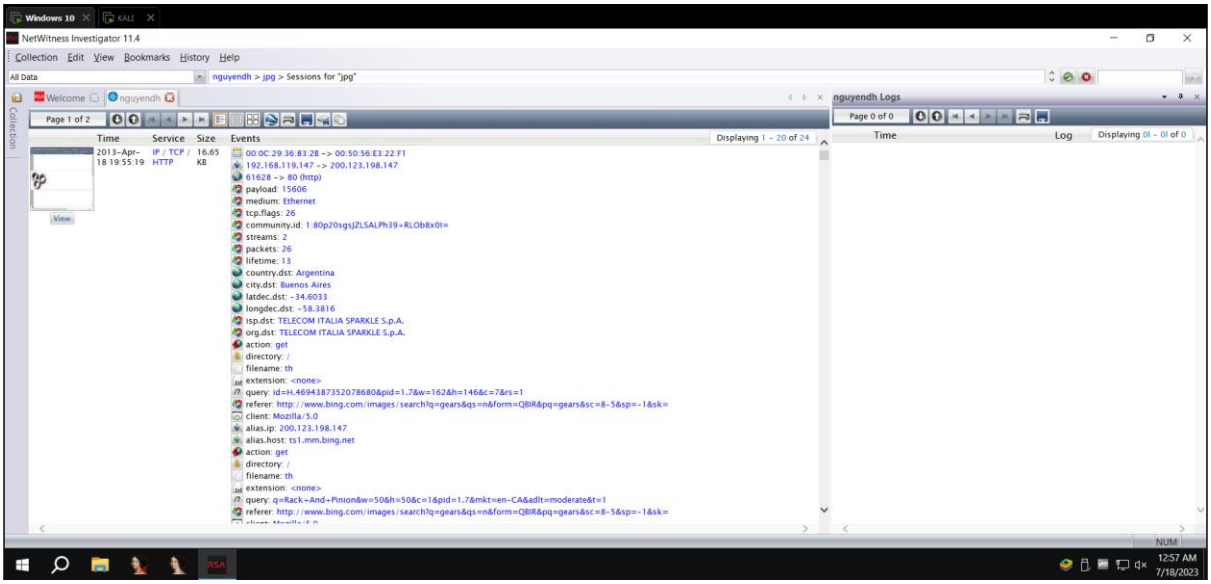


Ta có kết quả như sau khi nhấn vào View của các tab

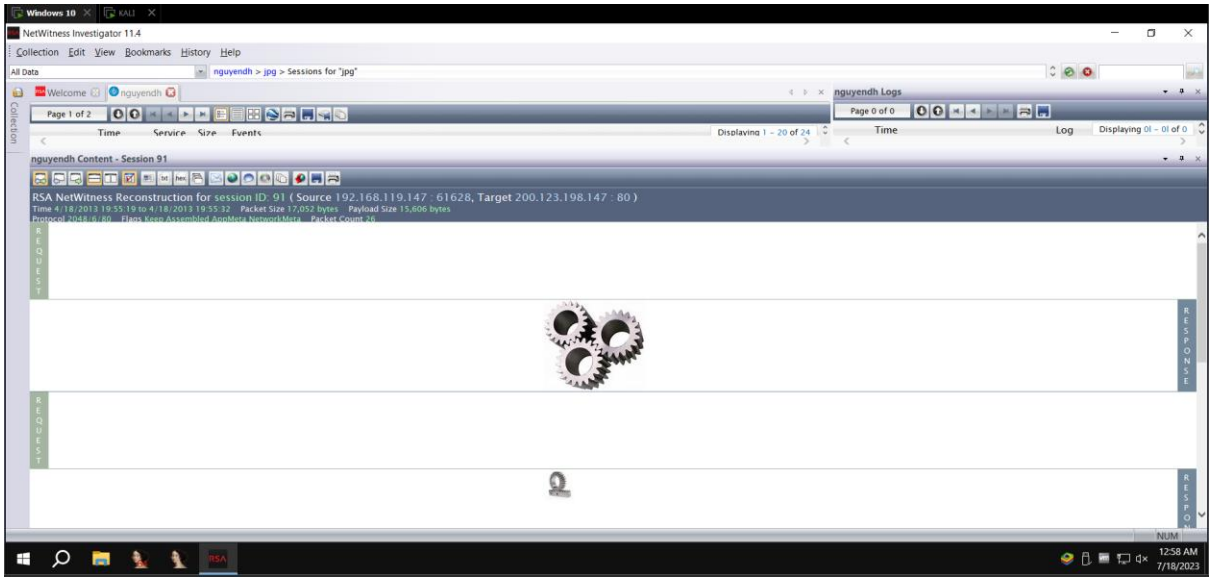


Gear Image

Vào lại bên trong phần trang chủ, và search “jpg” ta có kết quả nhưu sau:



Để xem rõ hơn thì nhấn vào phần view để có kết quả rõ hơn


Windows 10
KALI
NetWitness Investigator 11.4
Collection Edit View Bookmarks History Help
All Data
nguyendh > jpg > Sessions for "jpg"
Welcome
nguyendh
Page 1 of 2
Time Service Size Events
Displaying 1 - 20 of 24
nguyendh Logs
Page 0 of 0
Time Log
Displaying 0 - 0 of 0
nguyendh Content - Session 91
RSA NetWitness Reconstruction for session ID: 91 (Source 192.168.119.147 : 61628, Target 200.123.198.147 : 80)
Time 4/18/2013 19:55:19 to 4/18/2013 19:55:32 Packet Size 17,052 bytes Payload Size 15,606 bytes
REQUEST
RESPONSE
NUM
12:58 AM
7/18/2023