**TRAFFIC ANALYSIS EXERCISE - CATBOMBER**

**SCENARIO**

Cấu hình mạng LAN

* Dải mạng LAN:  10.5.28.0/24 (10.5.28.0 through 10.5.28.255)
* Domain:  catbomber.net
* Domain controller:  10.5.28.8 - Catbomber-DC
* Địa chỉ gateway:  10.5.28.1
* Địa chỉ broadcast:   10.5.28.255

**CÂU HỎI**

* Based on the Trickbot infection's HTTP POST traffic, what is the IP address, host name, and user account name for the infected Windows client?
* What is the other user account name and other Windows client host name found in the Trickbot HTTP POST traffic?
* What is the infected user's email password?
* Two Windows executable files are sent in the network traffic.  What are the SHA256 file hashes for these files?

Định nghĩa về trickbot:

TrickBot là một loại Trojan nguy hiểm đã xuất hiện từ khoảng năm 2016. Nó được thiết kế chủ yếu để đánh cắp thông tin tài chính, như thông tin đăng nhập ngân hàng trực tuyến, chi tiết thẻ tín dụng và các dữ liệu nhạy cảm khác từ máy tính bị nhiễm. TrickBot thường lan truyền qua email rác, các tệp đính kèm độc hại hoặc các trang web bị xâm phạm.

Sau khi được cài đặt trên máy tính của nạn nhân, TrickBot có thể thực hiện nhiều hoạt động độc hại, bao gồm ghi lại các phím được nhấn, can thiệp vào trình duyệt và theo dõi mạng. Nó cũng có thể tải xuống các module bổ sung để mở rộng khả năng, chẳng hạn như ransomware hoặc các công cụ truy cập từ xa.

TrickBot đã tấn công cá nhân, doanh nghiệp và tổ chức trên toàn thế giới, gây ra thiệt hại tài chính đáng kể và vi phạm dữ liệu. Nó đã được liên kết với nhiều nhóm tội phạm mạng và đã tiến hóa theo thời gian để tránh phát hiện và cải thiện các kỹ thuật lây nhiễm.

Nói tóm tắt trickbot sẽ làm những việc sau:

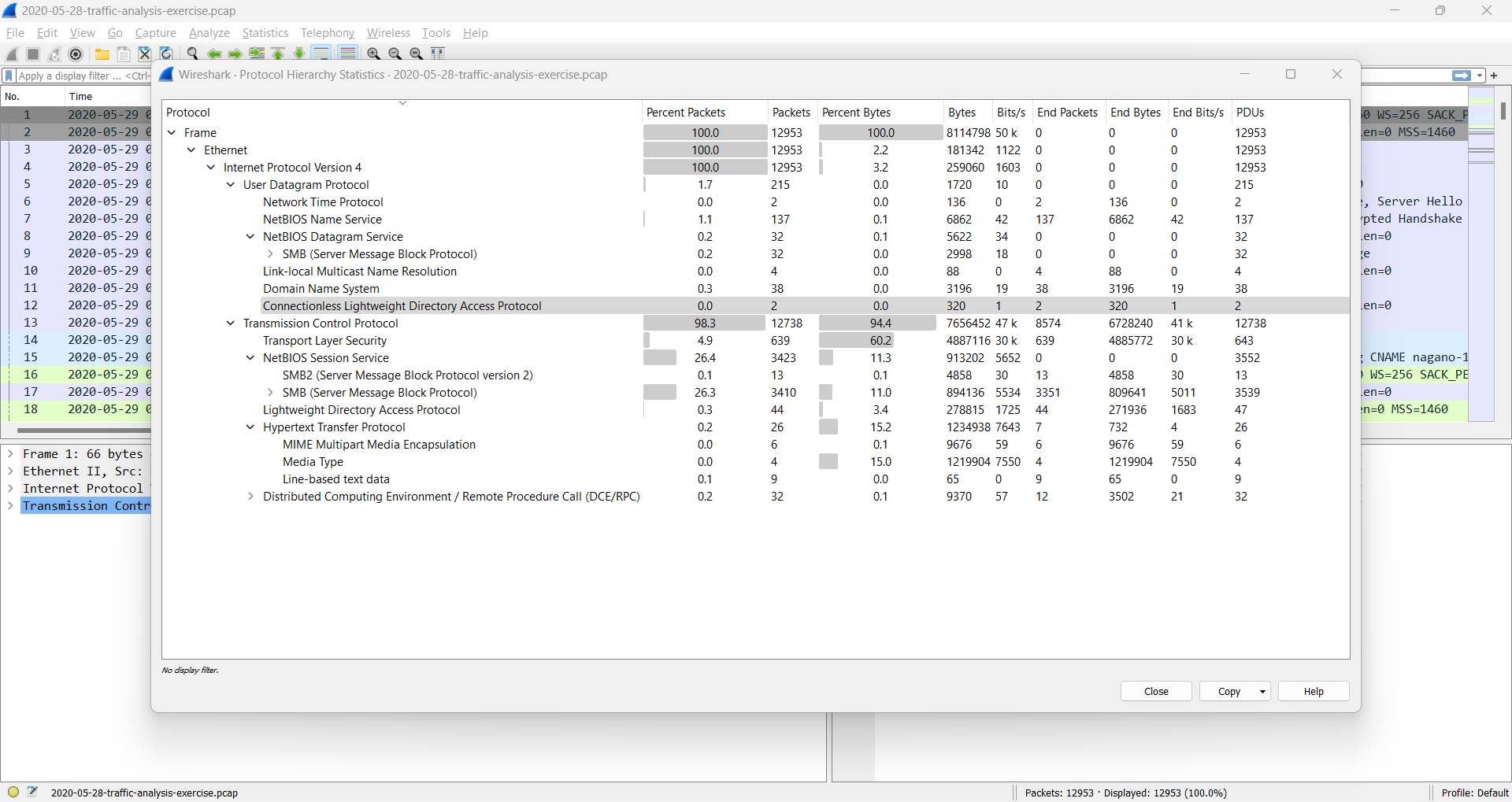
* Load code vào bên trong hệ thống
* Nó sẽ tự nhân bản chính nó vào trong %APPDATA%
* Thu thập thông tin nhạy cảm
* Tự tiêm (inject) code vào bên trong những tiến trình mà chúng đang xử lý
* Nó sẽ trộn lẫn (exflirate) vào thông tin bên trong máy chủ C&C

**Based on the Trickbot infection's HTTP POST traffic, what is the IP address, host name, and user account name for the infected Windows client?**

Để trả lời câu hỏi, chúng ta cần phải phân tích và quan sát về file PCAP mà chúng ta đã thu thập được. Được hiển thị như hình dưới đây:

Như ta có thể thấy được dễ dàng rằng, bên trong gói tin này, cơ bản các PDU đến từ nhiều nguồn khác nhau. Nhưng chúng ta chỉ thấy rằng các gói tin này có trọng tâm chủ yếu ở các giao thức sau:

* Giao thức web: HTTP
* Giao thức mail: SMB



Vì có khá là nhiều gói SMB cũng như là gói HTTP nên chúng ta sẽ suy xét theo từng khía cạnh trước. Đối với gói SMB dùng bằng filter

* “SMB”

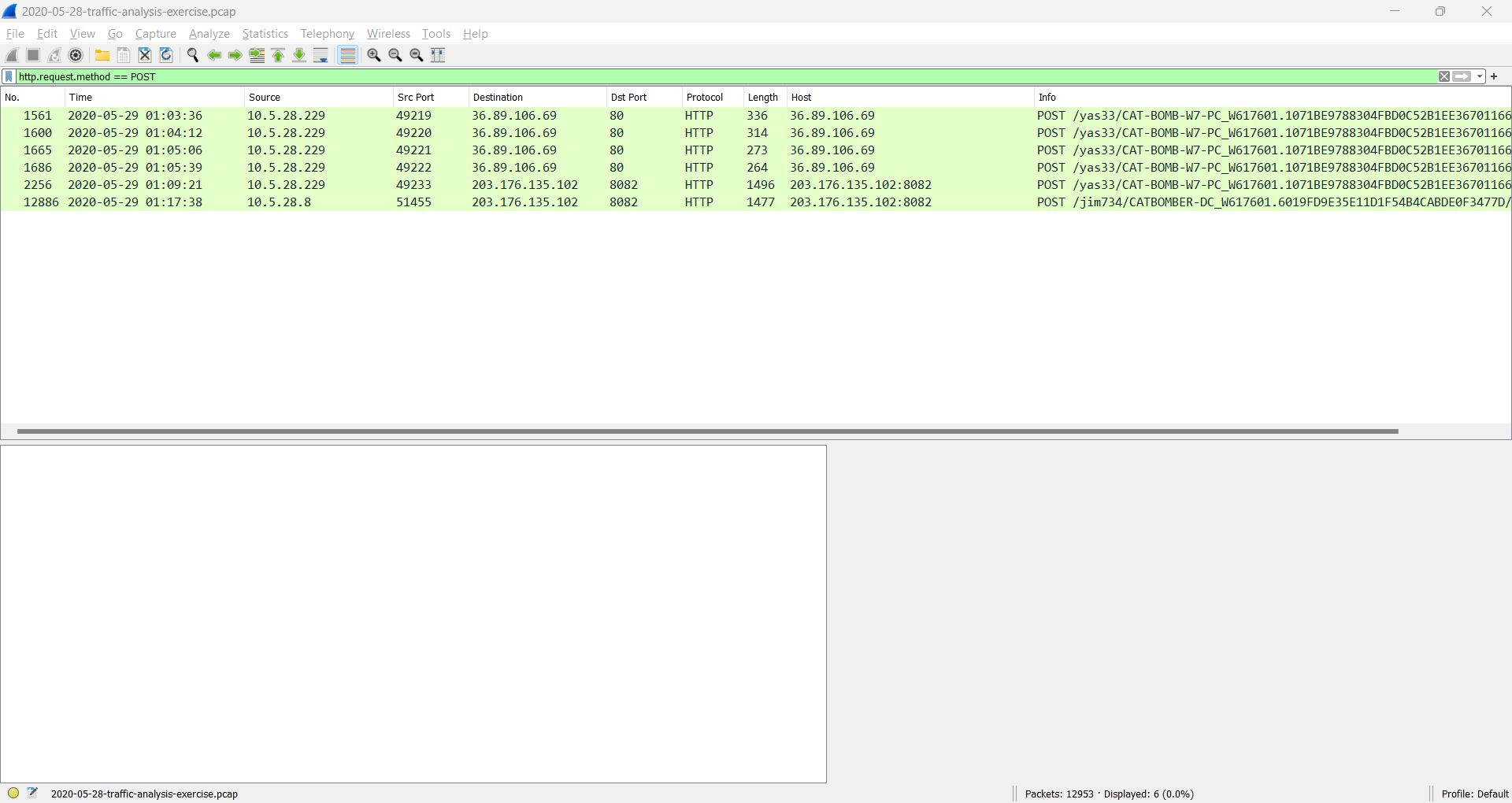
Ta có thể thấy được rằng theo filter này với giao thức được dung là UDP thì cũng không có gì lạ xảy ra đối với gói các gói tin SMB

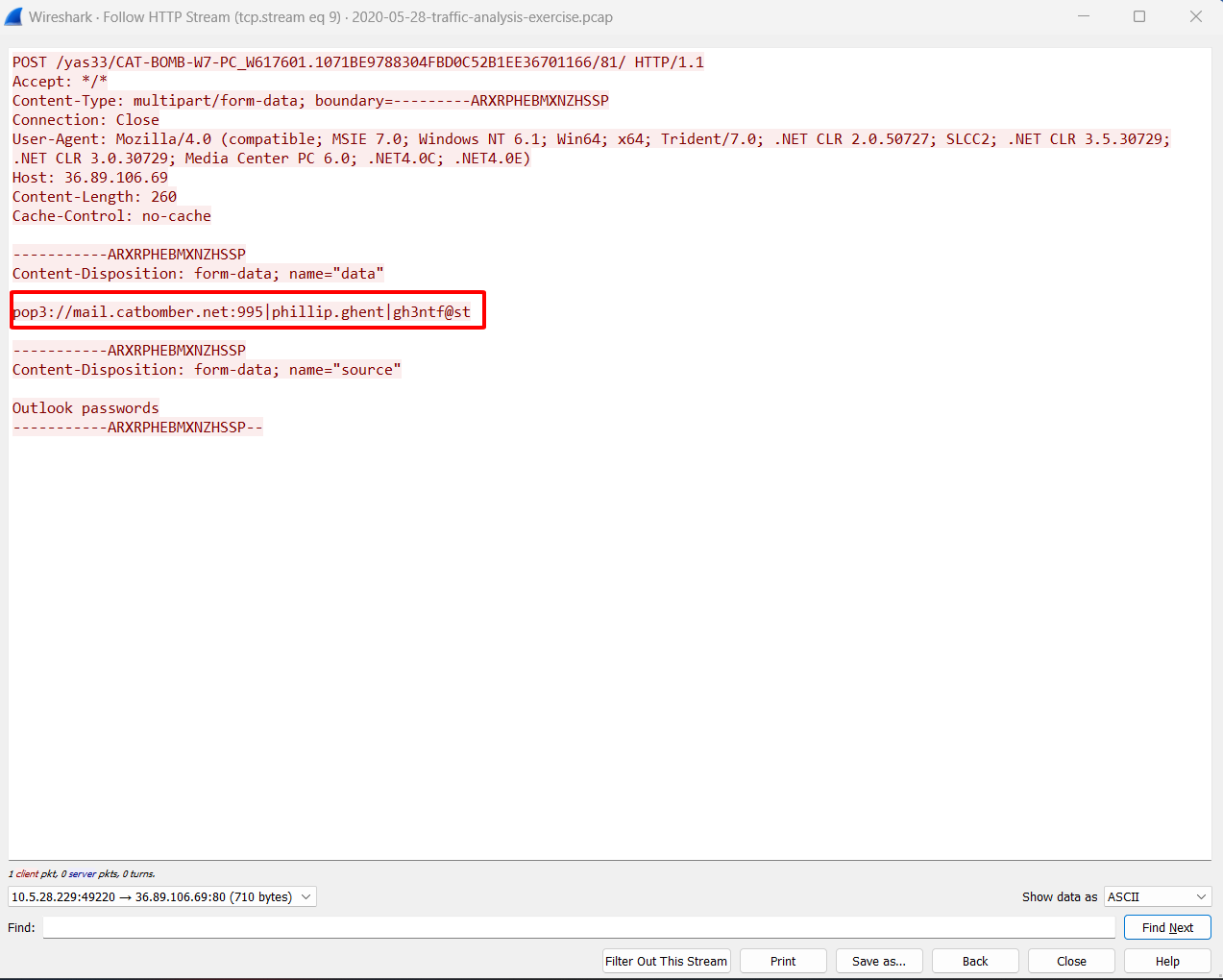
Đến với các gói tin HTTP ta thấy rằng có rất nhiều gói PDU. Nhưng ta sẽ chú trọng vào các gói như HTTP GET và HTTP POST. Hai method này khá là quan trọng trong việc truyền đi thông tin tương tác giữa client và server, cũng có thể là tương tác giữa victim và hacker.

Vì thế ta sẽ sử dụng filter sau để có thể xem được thông tin của các gói POST:

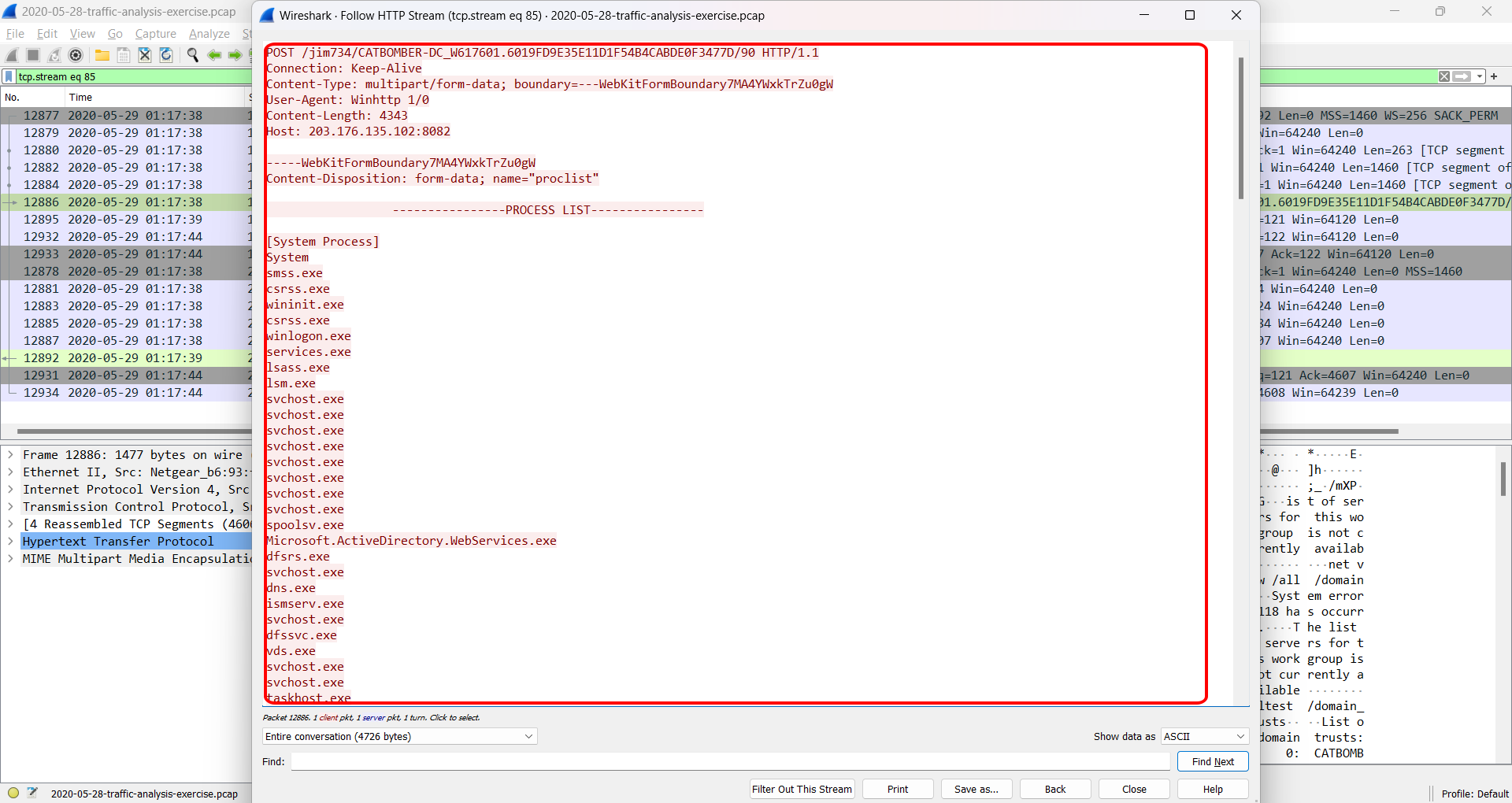
* http.request.method == POST

Filter này sẽ xuất hiện những gói tin có phương thức chuyển đi đó chính là POST. Ta sẽ có kết quả là có 6 PDU chứa method là POST. Theo nhận định ban đầu, ta có thể thấy rõ là từ địa chỉ ip 10.5.28.229 gửi request tới hai địa chỉ đó chính là địa chỉ của port web với ip là 36.89.106.69 và địa chỉ tiếp theo là 203.176.135.102 với port 8082

Bắt đầu theo các stream ( luồng) từ các PDU trên, thì ta có thể thấy rằng các gói gửi request từ 10.5.28.229 tới 36.89.106.69 có chứa một số thông tin như quan trọng như là địa chỉ mail pop3



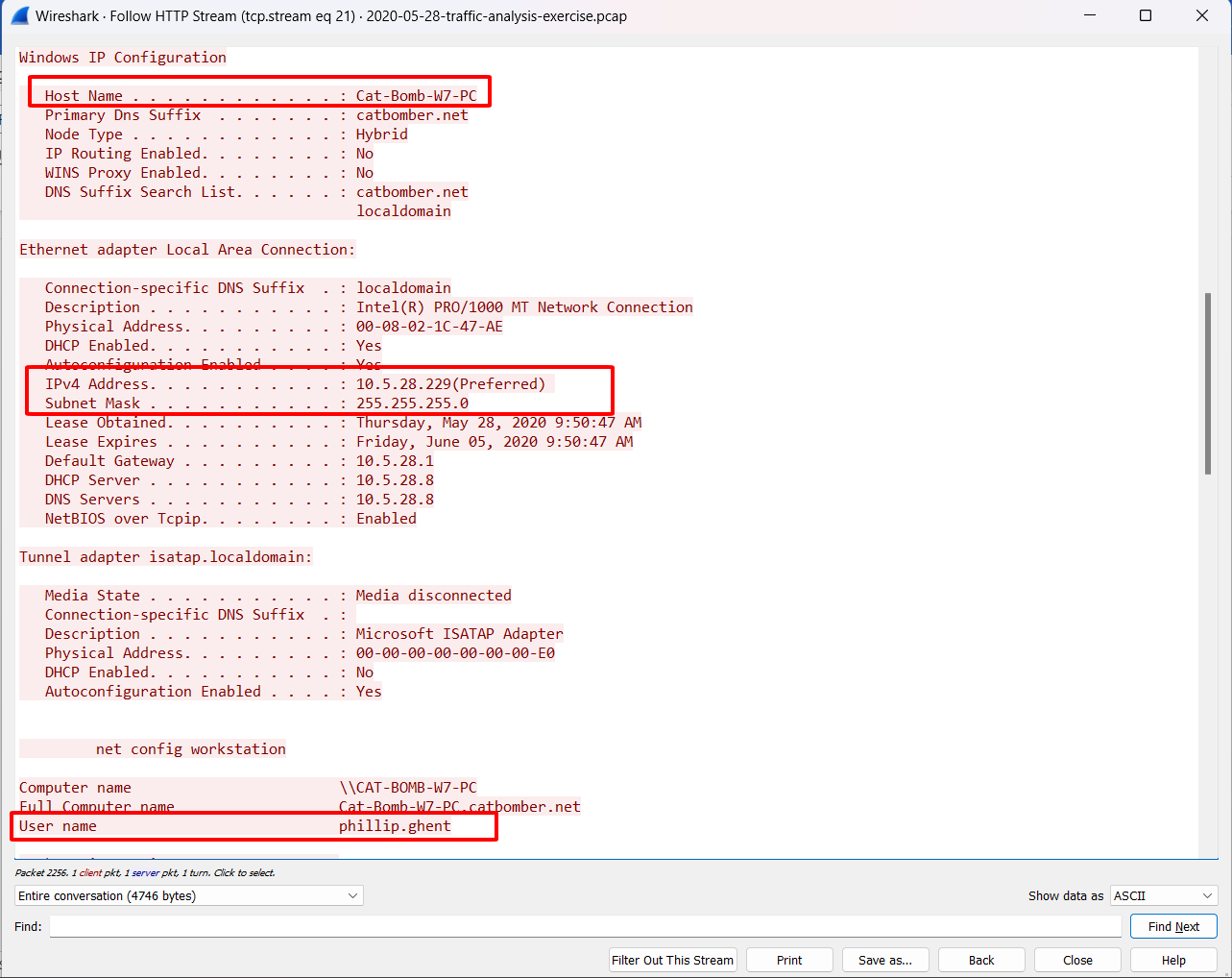
Tiếp theo ta sẽ tiếp tục tra đến phần http request tới địa chỉ 203.176.135.102 với port 8082 thì thật rất bất ngờ khi xem request tới địa chỉ đó thì lại là thông tin của cmd



Ta có thể thấy như hình trên, khi xét stream của nó thì từ máy nạn nhân đã gửi các thông tin như là thông tin các process đang chạy trên máy, các câu lệnh cmd như là **ipconfig /all, net config workstation, net view /all,…** ngoài ra còn có các câu lệnh khác nữa,…

Vì thế dựa vào các command bên trên, ta có thể biết được rằng username, IP và hostname của máy bị nhiễm.

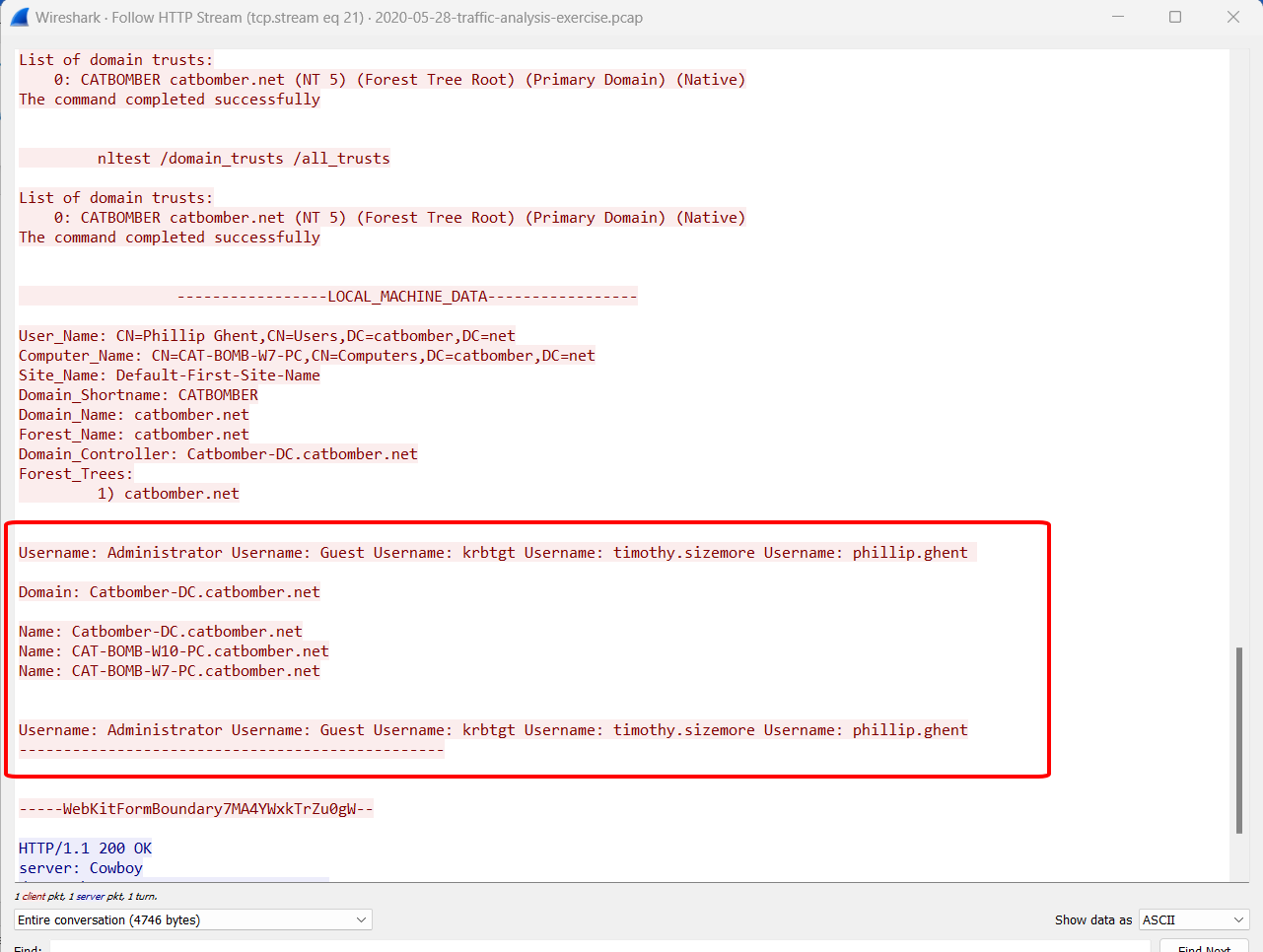
* IP nhiễm: 10.5.28.229
* Host name: Cat-Bomb-W7-PC
* Username: phillip.ghent



Như ta thấy trên hình, lý do vì sao mà không chọn đáp án là gói http.request,method của 10.5.28.8 bởi vì đây là máy chủ control, có trách nhiệm trỏ DNS cho các máy khác bên trong server.

**What is the other user account name and other Windows client host name found in the Trickbot HTTP POST traffic?**

Dựa theo tiếp vào thông tin của các gói HTTP POST request, ta kéo xuống, sẽ thấy được sẽ có các account khác có bên trong máy của nạn nhân được hiển thị như hình dưới đây:



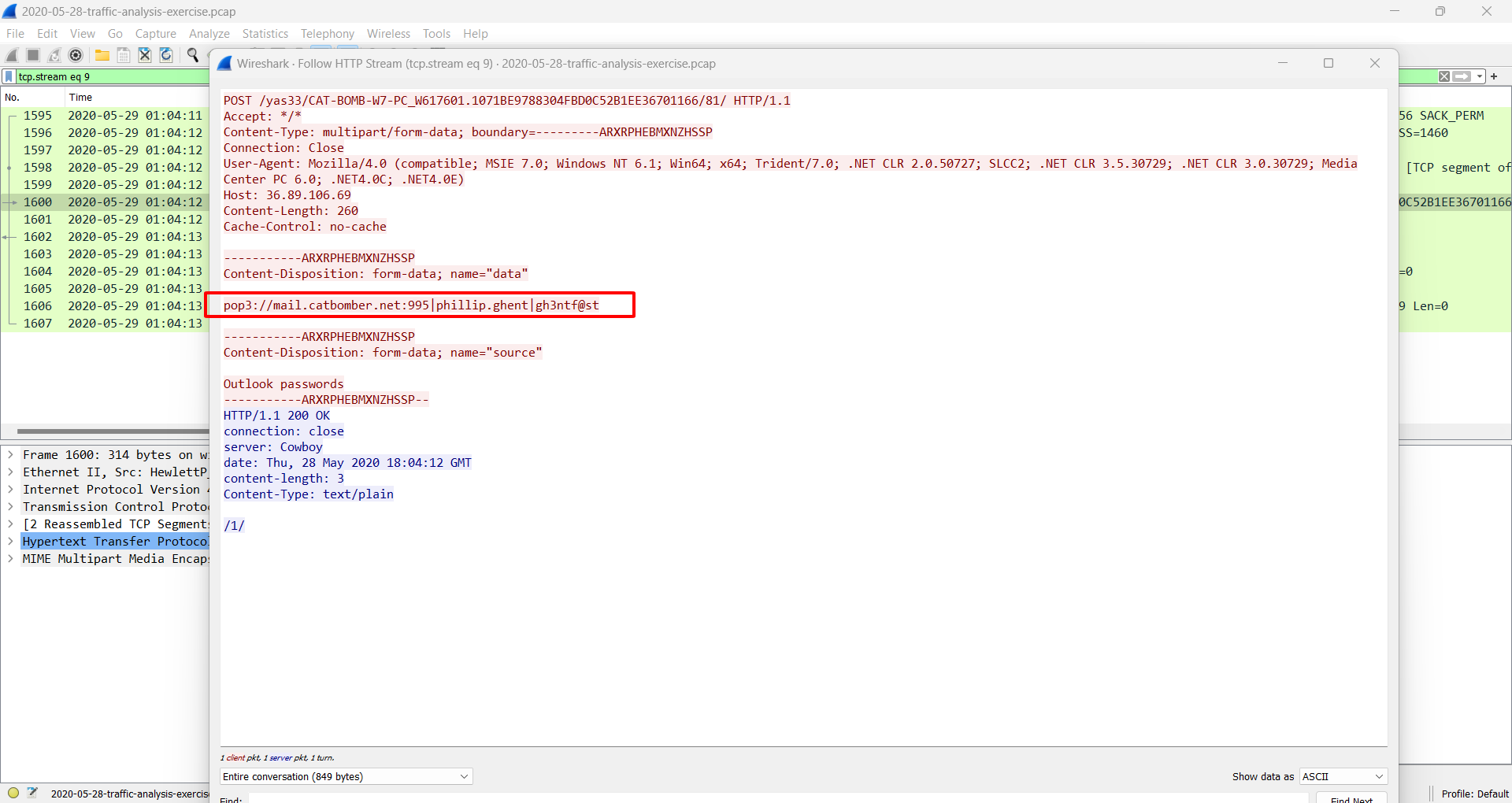
**What is the infected user's email password?**

Dựa trên các filter, khi ta xác định được máy đã bị nhiễm virus thì bây giờ chúng ta sẽ dung filter để thu nhỏ phạm vi lại, sử dụng filter sau:

* http.request.method == POST and ip.src==10.5.28.229

Sau khi filter xong, ta thấy có một TCP stream thứ 9 chứa các thông tin quan trọng về mail, địa chỉ mail pop3. Chúng ta có thể dung filter sau:

* tcp.stream eq 9

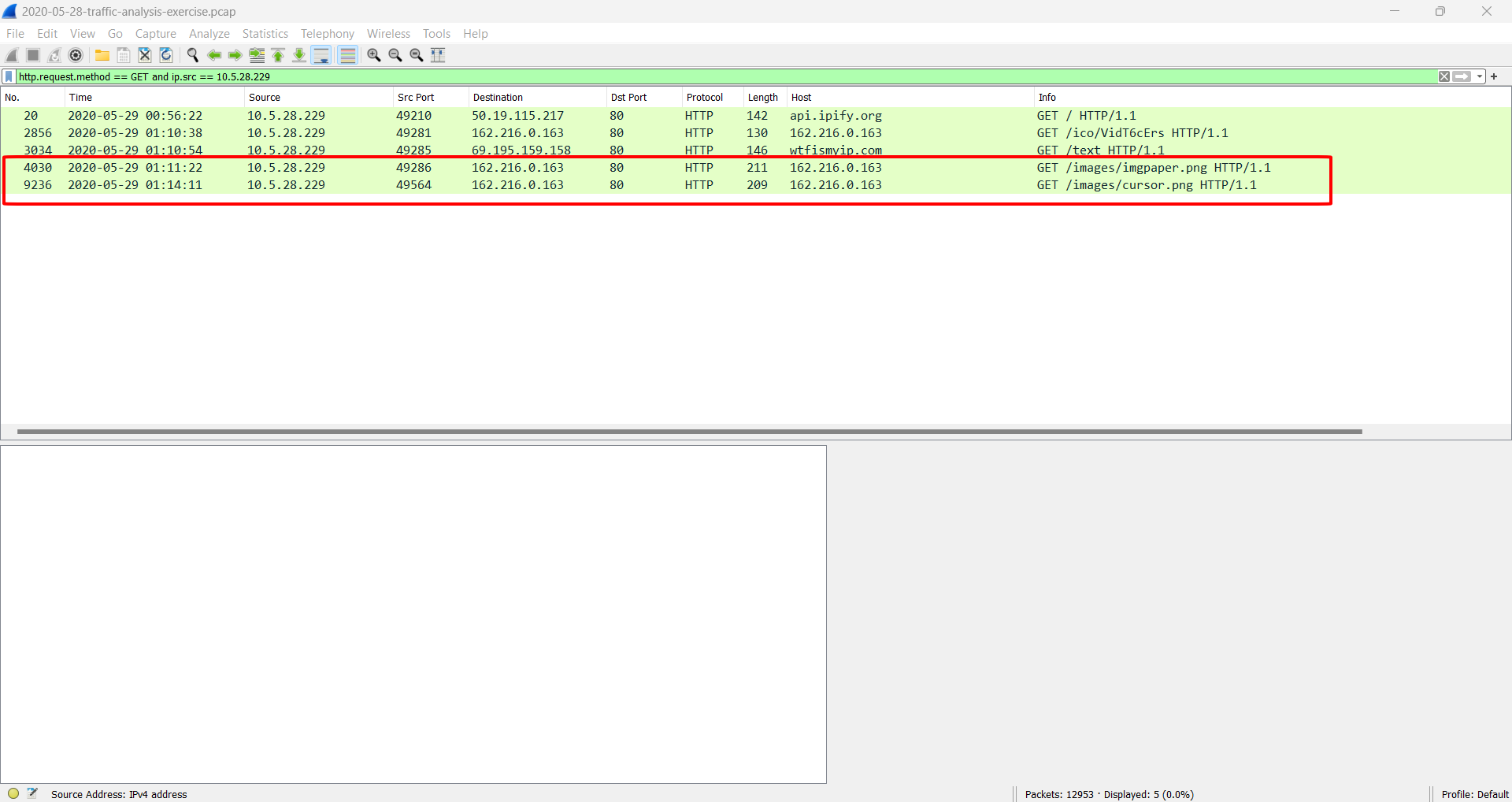


**Two Windows executable files are sent in the network traffic.  What are the SHA256 file hashes for these files?**

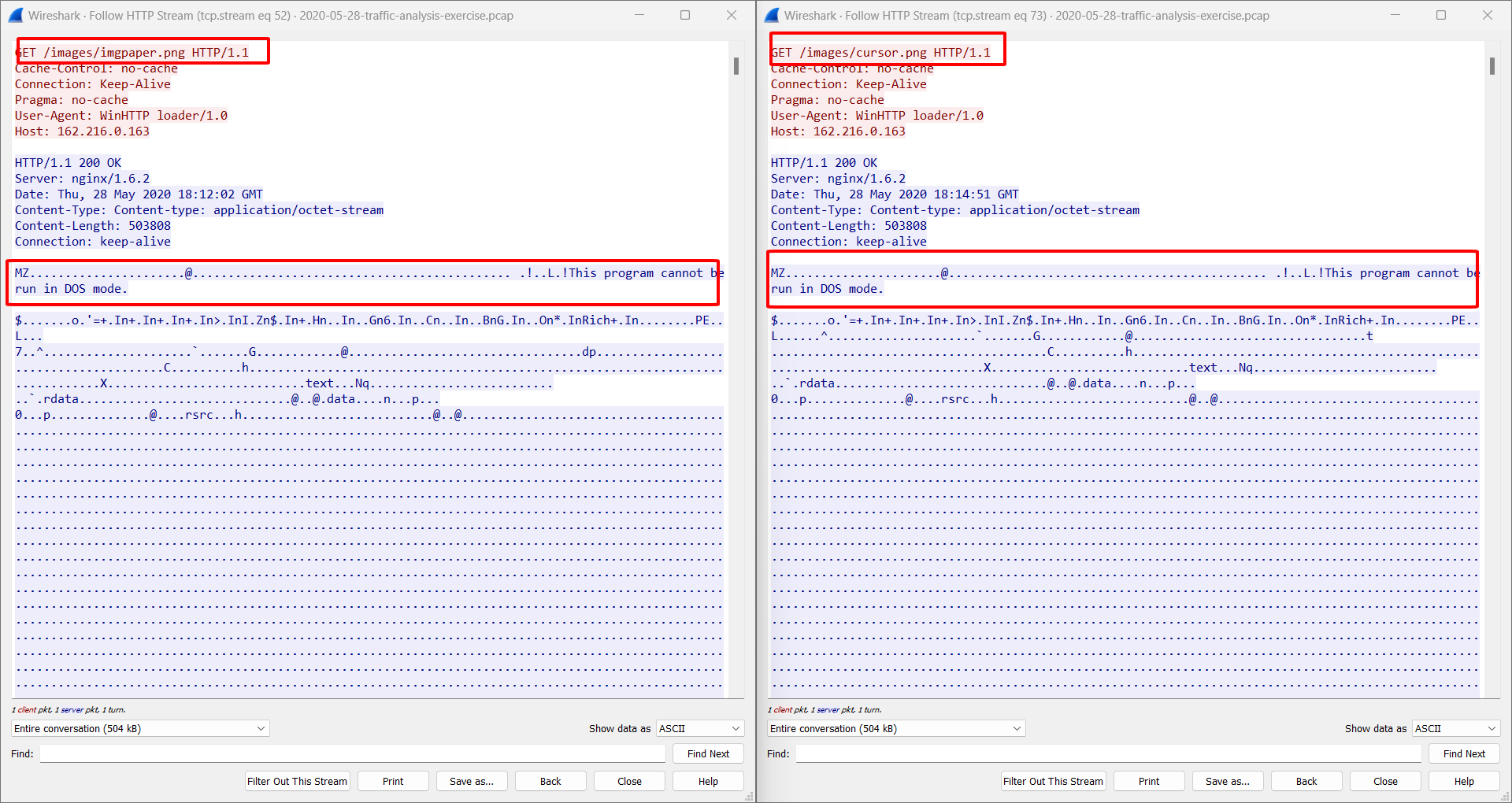
Bây giờ chúng ta sẽ phân tích chuyện gì đã xảy ra trước khi máy bị nhiễm virus. Chúng ta sẽ bắt đầu filter những gói mà máy nạn nhân GET về thông qua câu lệnh sau:

* http.request.method == GET and ip.src == 10.5.28.229

Ta có được các kết quả như sau:

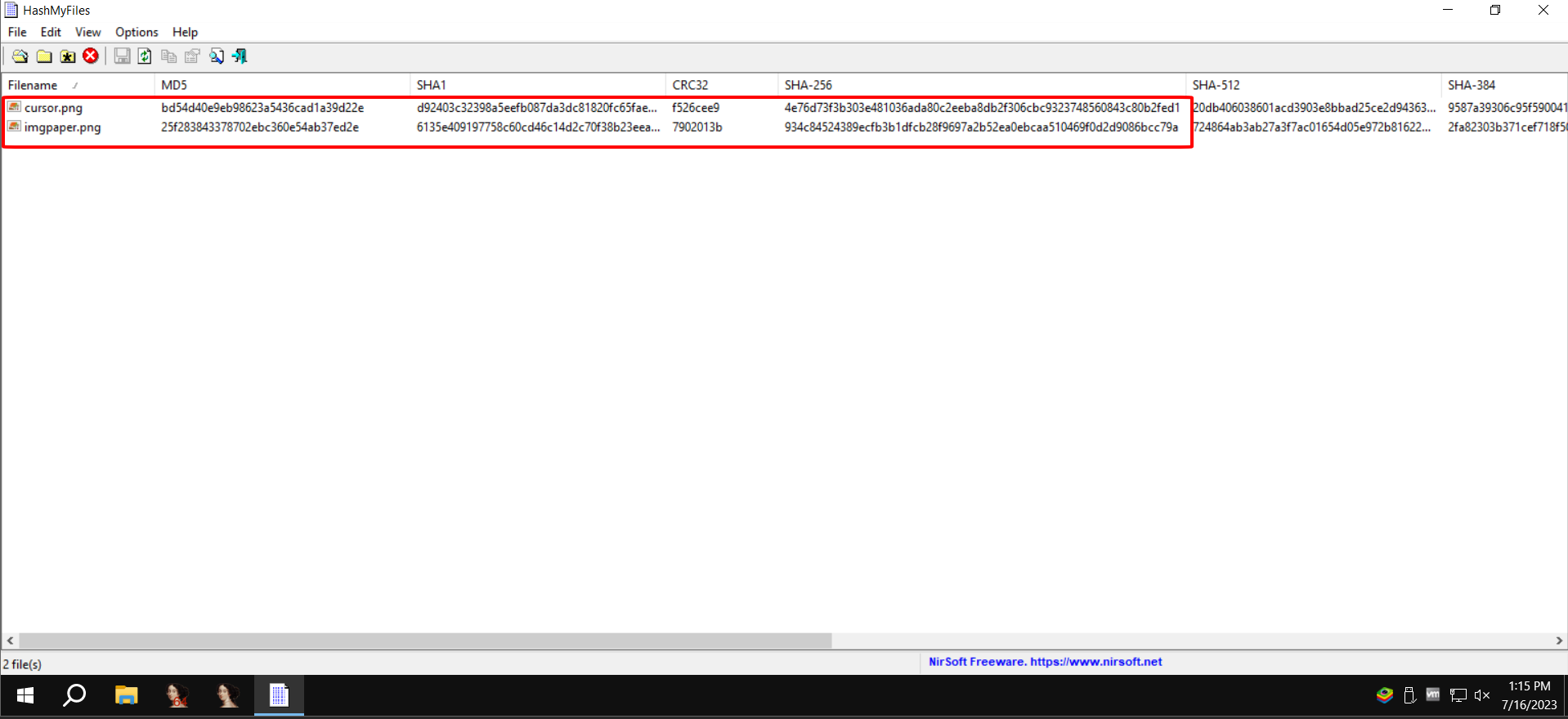


Có hai gói pdu khá là khả nghi, khi xem stream của nó, ta có được thông tin như sau:



Ta thấy được rằng đây không phải là một file png bình thường, mà đây là một file exe nhưng mà đã được đổi định dạng thành png. Chúng ta có thể dễ dàng biết đưuọc rằng, sau khi tải xuống, nạn nhân đã click vào hai file png đã tải xuống như vậy là đã kích hoạt được con malware này.

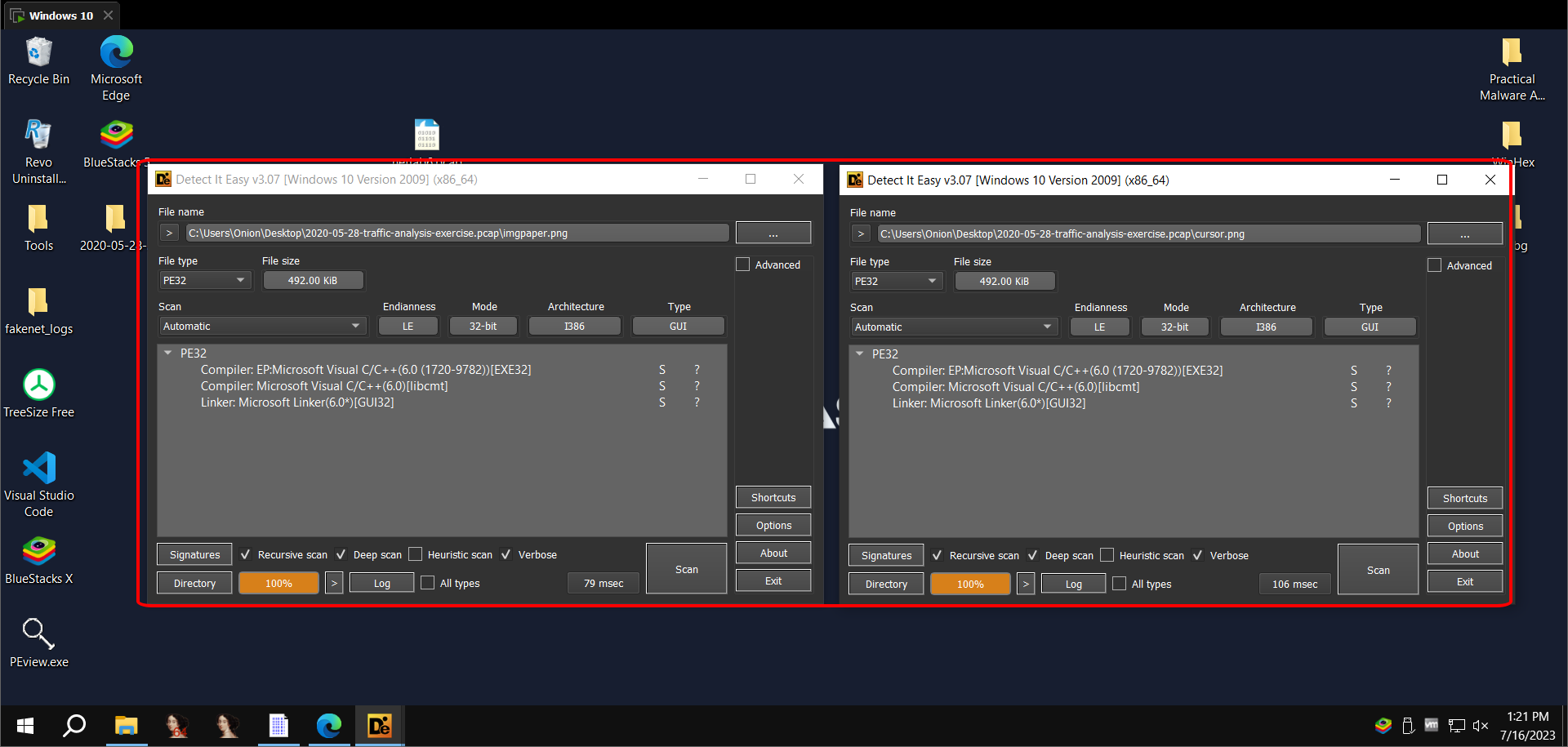
Chúng ta sẽ 2 file này thông qua Export Object của wireshark, Check mã hash sha256 của chúng ta có được:



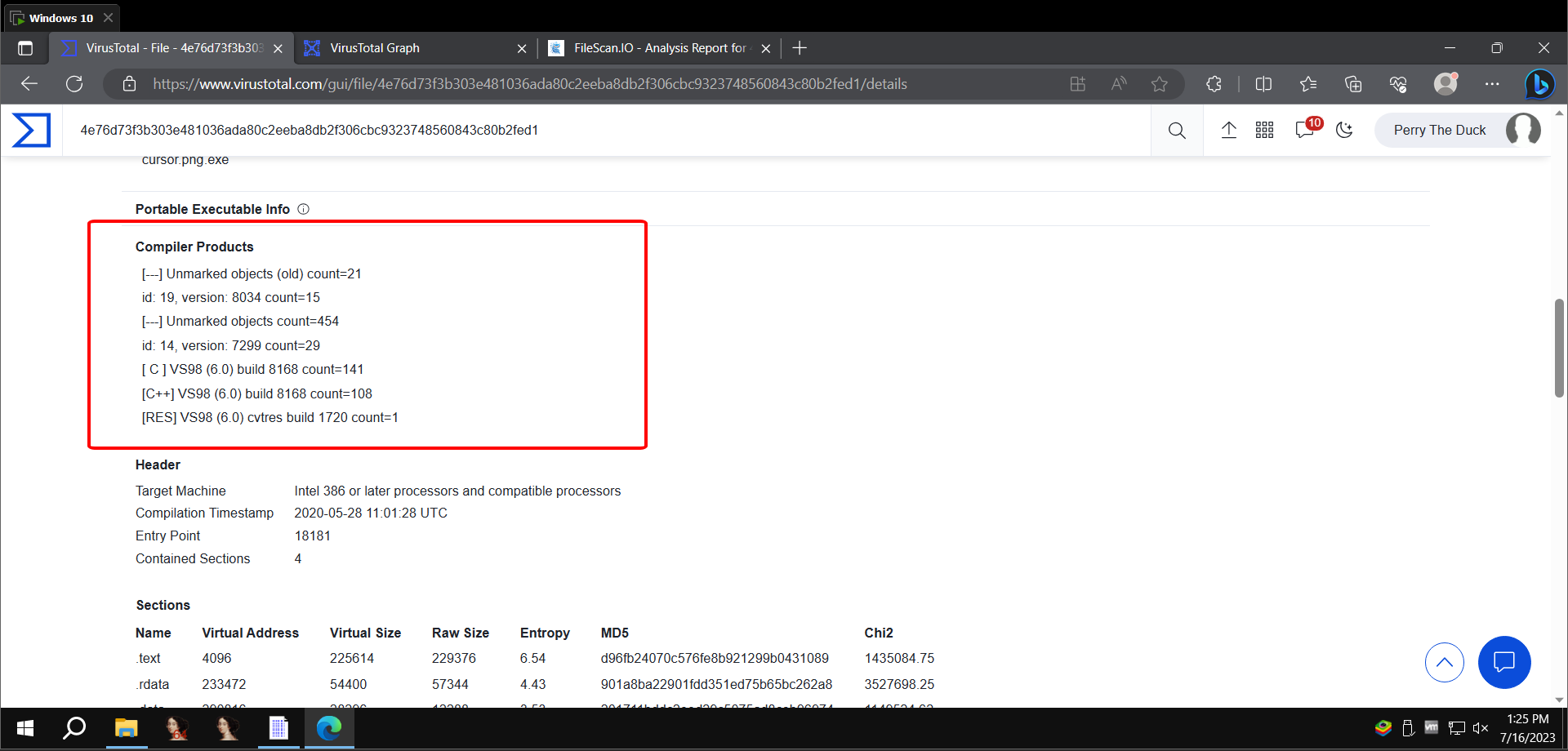
* Cursor.png: 4e76d73f3b303e481036ada80c2eeba8db2f306cbc9323748560843c80b2fed1
* Image.png: 934c84524389ecfb3b1dfcb28f9697a2b52ea0ebcaa510469f0d2d9086bcc79a

Tiếp theo chúng ta sẽ bắt đầu tiến hành phân tích hai con này bằng phương pháp phân tihcs tĩnh xem sẽ có những gì. Vì đây là một file đã bị packed, không phải dạng packed thông thường nên rất khó đẻ có thể unpack được chúng. Nên chúng ta sẽ phân tích bằng các phân tích tĩnh

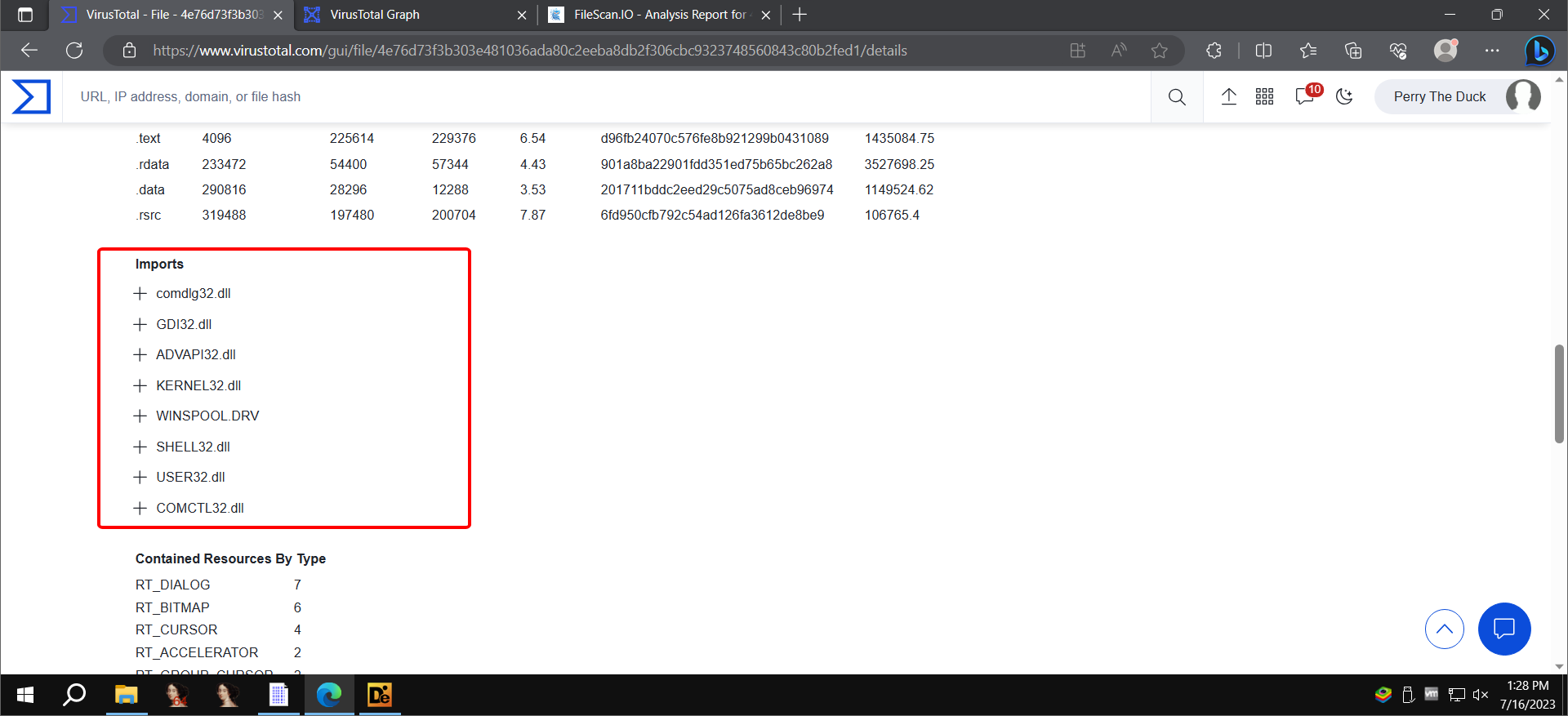
Sử dụng detect it easy để xem chúng sử dụng phiên bản gì để code, ta có kết quả như sau:



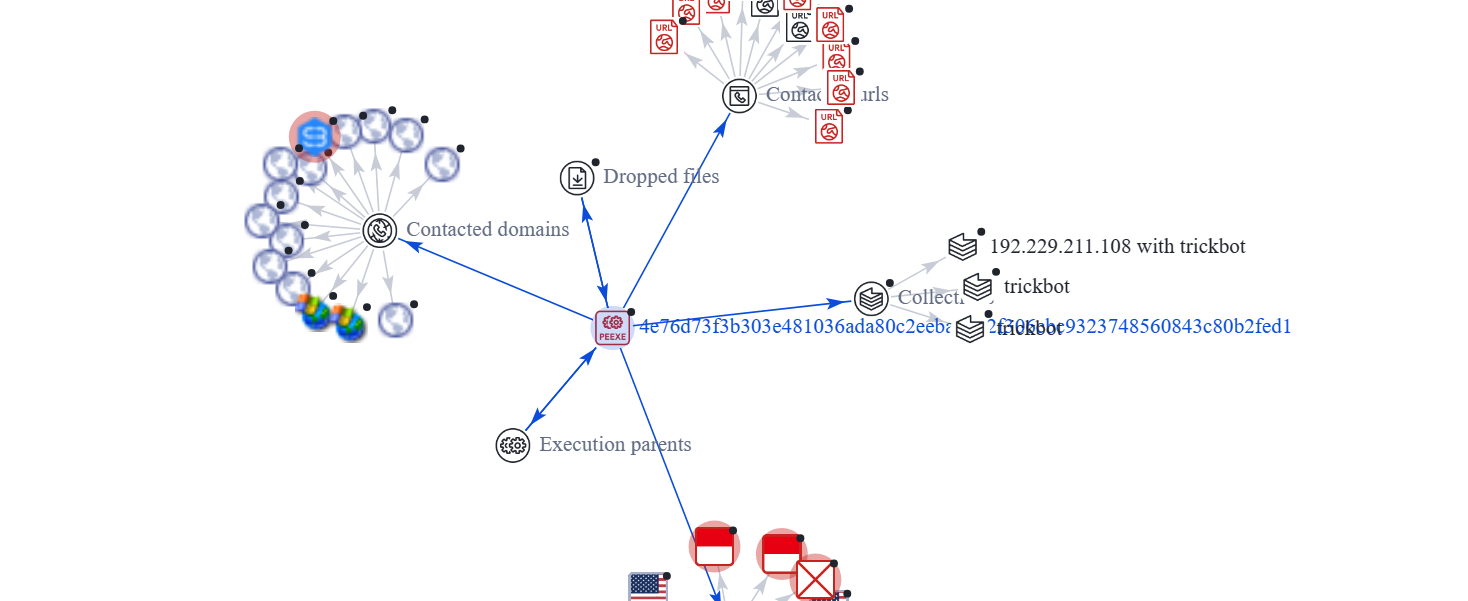
Cả hai đều phân tích sử dụng ngôn ngữ lập trình C/C++. Vì detect it easy là một chương trình false positive nên chúng ta sẽ đem lên Virus total để xxem rằng trên đó phân tích như thế nào.



Thì cũng như die, nó cũng nhận rằng file được viết bằng ngôn ngữ C/C++. Ngoài ra có các dlls được sử dụng như là: comdlg32.dll, GD32.dll, KERNEL32.dll, SHELL32.dll,..



Theo như Virustotal, đây là biểu đồ thể hiện hành vi của chúng



Ngoài ra nếu muốn xem thêm hành vi đó, đã có một bài tổng hợp tại anyrun theo link dưới đây:

* <https://any.run/report/4e76d73f3b303e481036ada80c2eeba8db2f306cbc9323748560843c80b2fed1/7d18e981-be4d-4ce0-a564-7b39d2b5185c>
* <https://app.any.run/tasks/7d18e981-be4d-4ce0-a564-7b39d2b5185c/>