Network Traffic Analysis

Brian Smith

CIS 3880-101 | Dr. Russell Haines | Cat Bomber Assignment

Intro to Wireshark & PCAPs

Wireshark is an open-source network protocol analyzer

- It captures real-time network traffic and stores it in PCAP files (packet capture
- We then use these to investigate, diagnose, and to detect malicious activity

PCAP files contain Packet Headers, Payloads, and timestamps.

These are essential to incident response and forensic analysis. We can reconstruct network sessions (file transfers, HTTP requests, etc.)

A PCAP file records all network communication, including:

- Source & Destination IP Addresses – Who is communicating?
- Protocols Used – TCP, UDP, HTTP, HTTPS, DNS, etc.
- Packet Size & Timing – Helps detect anomalies (e.g., excessive traffic or embedded data)
- Flags & Status Codes – Indicators of errors or malicious activity
- Payload Data – Possible leaks of sensitive information

Example Use Cases:

1. Detecting malware communicating with a command-and-control (C2) server
2. Identifying unauthorized data transfers or exfiltration
3. Analyzing network slowdowns and failures

How Useful Information can be Extracted

Filters help isolate relevant traffic by displaying only packets that match certain criteria.

This was useful in our case, as we used a filter of “http.request” to browse the POST traffic, which helped us find the affected user.

Wireshark can reassemble network conversations by linking related packets together.

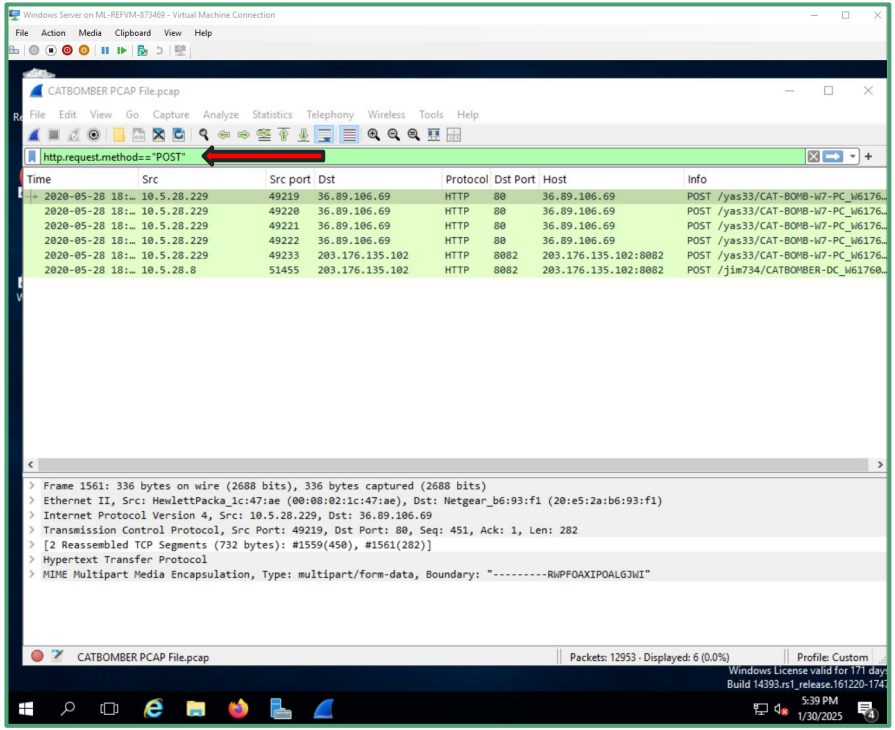
Following a TCP stream of an HTTP request can show user credentials in plaintext.

Every packet contains layers of information, like the Ethernet header, IP header, the transport layer, and the application layer.

We used these detail panes to look for relevant information to the event that the PCAP file saved.

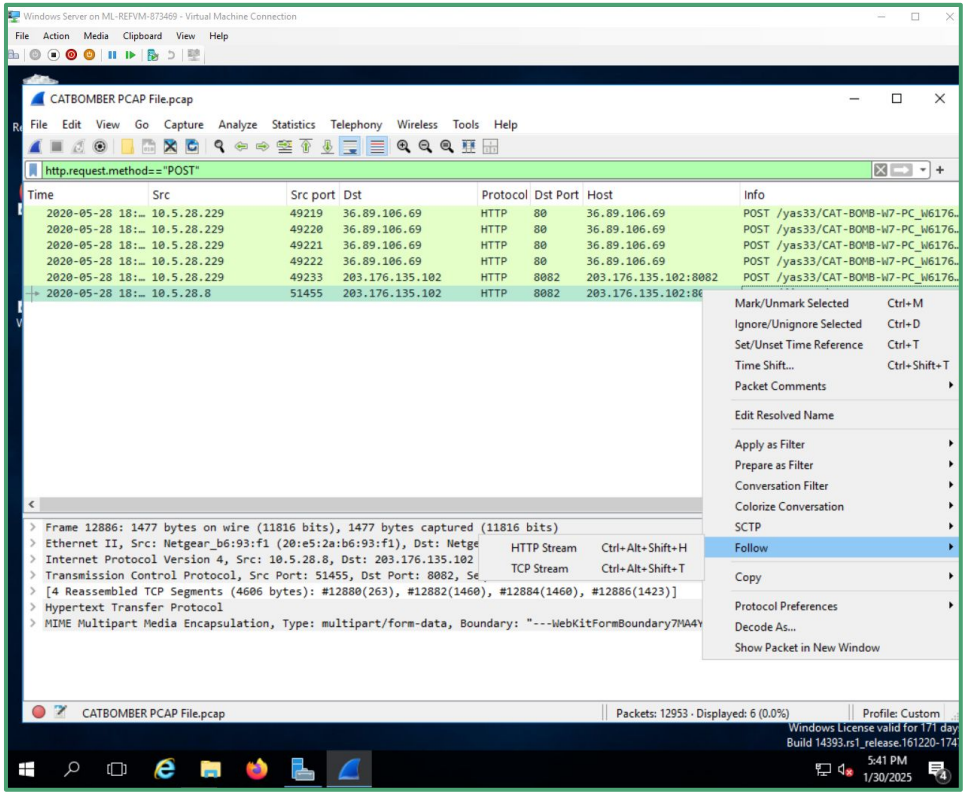
Filters in Wireshark

- There are several ways to use filters, and it depends on what you are looking for and trying to achieve
- In our case, we were looking for trickbot infections, so we had options
- The best filter we used was http.request, which we narrowed by only sorting the POST results, which we further analyzed next



How to Extract Info

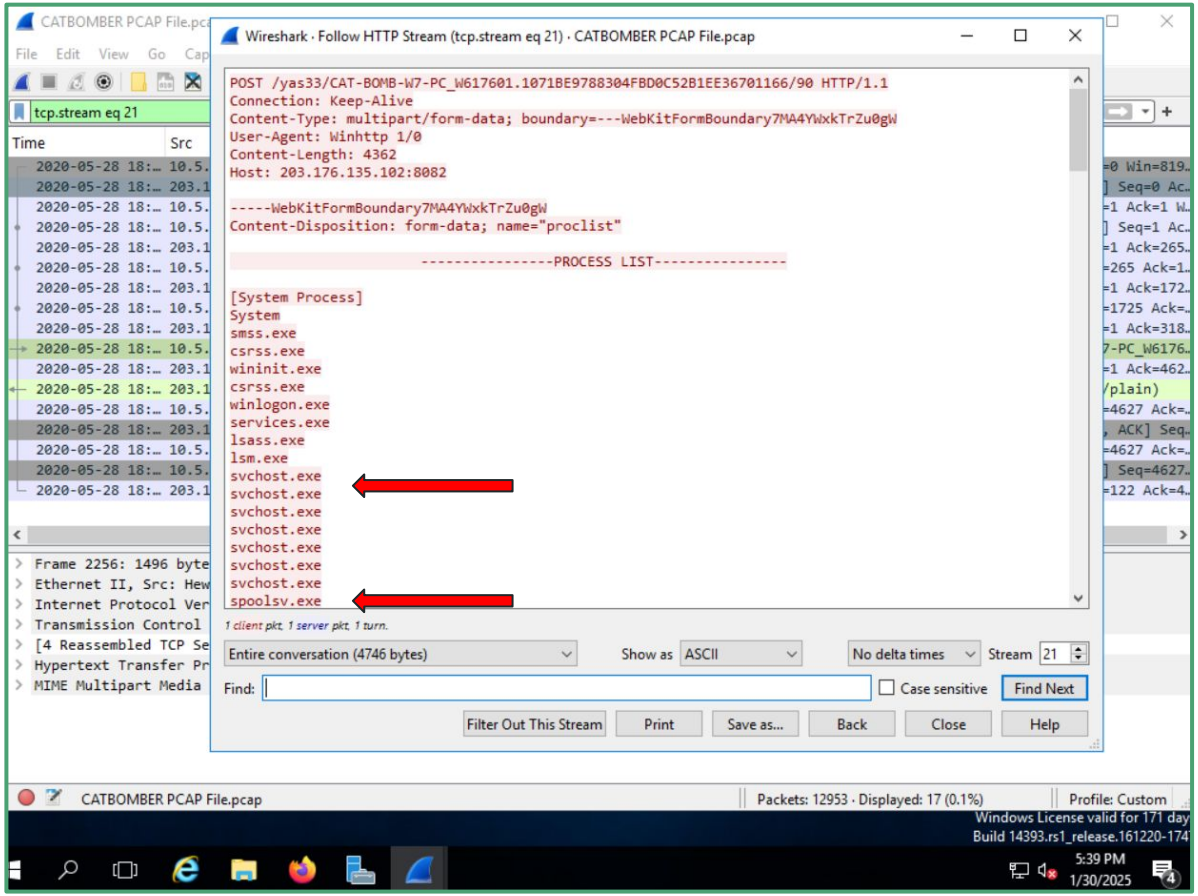
- After using the filter, we aren't left with much usable information... at least on the surface
- If we right click on the result that showed a destination port of 8082, we can "Follow" the HTTP stream of activity
- We can further investigate the event and uncover the infected Windows client
- Trickbots can have recognizable patterns in the POST requests



Extracted Info (2)

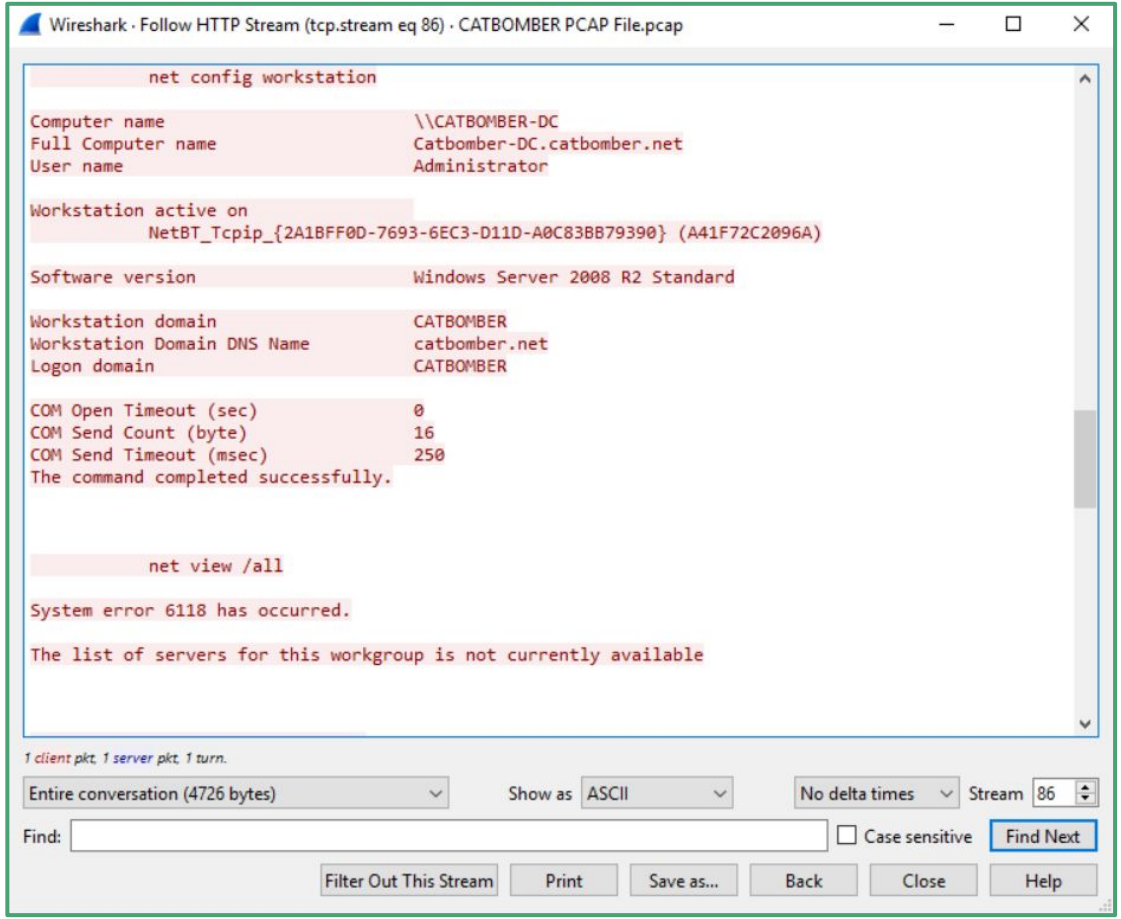
- By following the HTTP stream, we accessed the active process list that the computer is running
- Most of these are normal…
- But Spoolsv.exe and svchost.exe are known to be manipulated in trickbot events

We will investigate these further!



Extracted Info (3)

- Further down the HTTP stream results, we find that there are conspicuous commands that indicate a trickbot machine's presence on our network
- Net config workstation, net view/all, and domain_trusts are all commands that reveal relationships involving trust within the system, which threat actors can abuse to move through a network system
- Some TrickBot samples have used HTTP over ports 447 and 8082 for C2

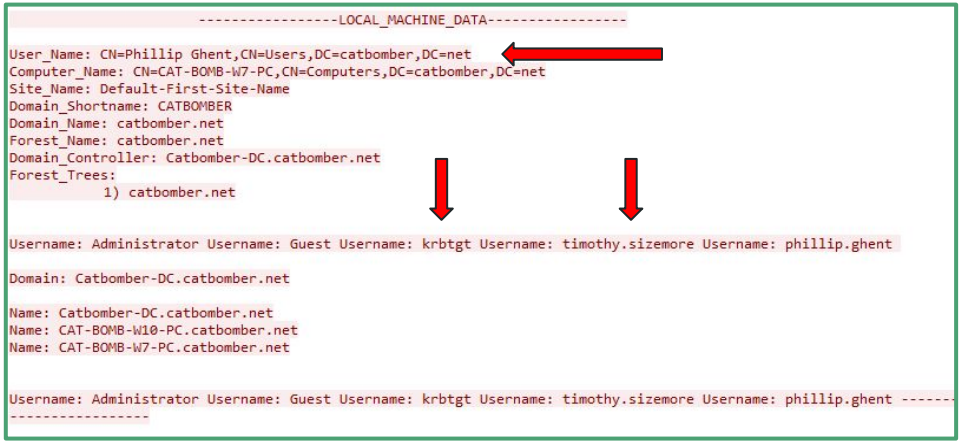


System Information

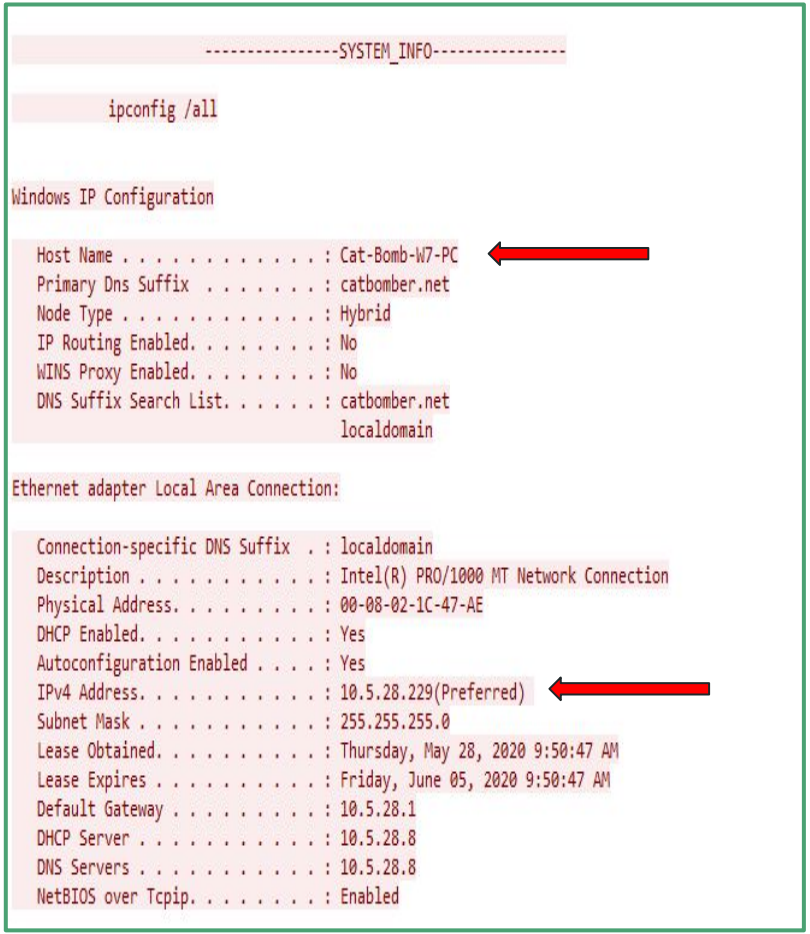
Based on the Trickbot infection's HTTP POST traffic, what is the IP address, host name, and user account name for the infected Windows client?

The HTTP stream also included the information about the Windows client that was affected:

- IP Address - 10.5.28.229
- Hostname - Cat-Bomb-W7-PC
- User Account Name - phillip.ghent
- Other User Account Names - Administrator, Guest, krbtgt, timothy.sizemore
- Other Windows Client Host Names - CAT-BOMB-W10-PC, Catbomber-DC.catbomber.net (the domain controller)



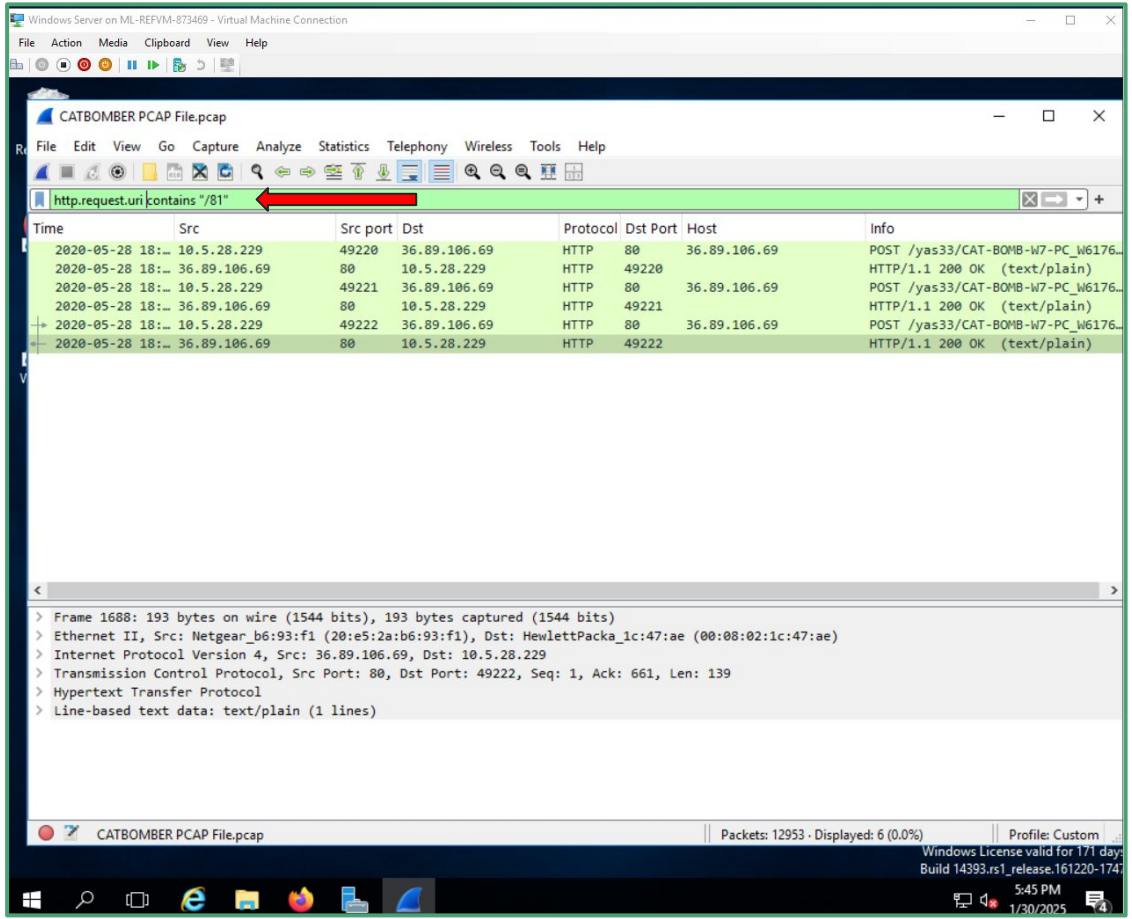
```
----------------LOCAL_MACHINE_DATA----------------

User_Name: CN=Phillip Ghent,CN=Users,DC=catbomber,DC=net
Computer_Name: CN=CAT-BOMB-W7-PC,CN=Computers,DC=catbomber,DC=net
Site_Name: Default-First-Site-Name
Domain_Shortname: CATBOMBER
Domain_Name: catbomber.net
Forest_Name: catbomber.net
Domain_Controller: Catbomber-DC.catbomber.net
Forest_Trees:
          1) catbomber.net

Username: Administrator Username: Guest Username: krbtgt Username: timothy.sizemore Username: phillip.ghent

Domain: Catbomber-DC.catbomber.net

Name: Catbomber-DC.catbomber.net
Name: CAT-BOMB-W10-PC.catbomber.net
Name: CAT-BOMB-W7-PC.catbomber.net


Username: Administrator Username: Guest Username: krbtgt Username: timothy.sizemore Username: phillip.ghent ------
----------------
```



```
----------------SYSTEM_INFO----------------

        ipconfig /all


Windows IP Configuration

   Host Name . . . . . . . . . . . . : Cat-Bomb-W7-PC
   Primary Dns Suffix  . . . . . . . : catbomber.net
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : catbomber.net
                                       localdomain

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-08-02-1C-47-AE
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.5.28.229(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, May 28, 2020 9:50:47 AM
   Lease Expires . . . . . . . . . . : Friday, June 05, 2020 9:50:47 AM
   Default Gateway . . . . . . . . . : 10.5.28.1
   DHCP Server . . . . . . . . . . . : 10.5.28.8
   DNS Servers . . . . . . . . . . . : 10.5.28.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Exfiltrated Passwords

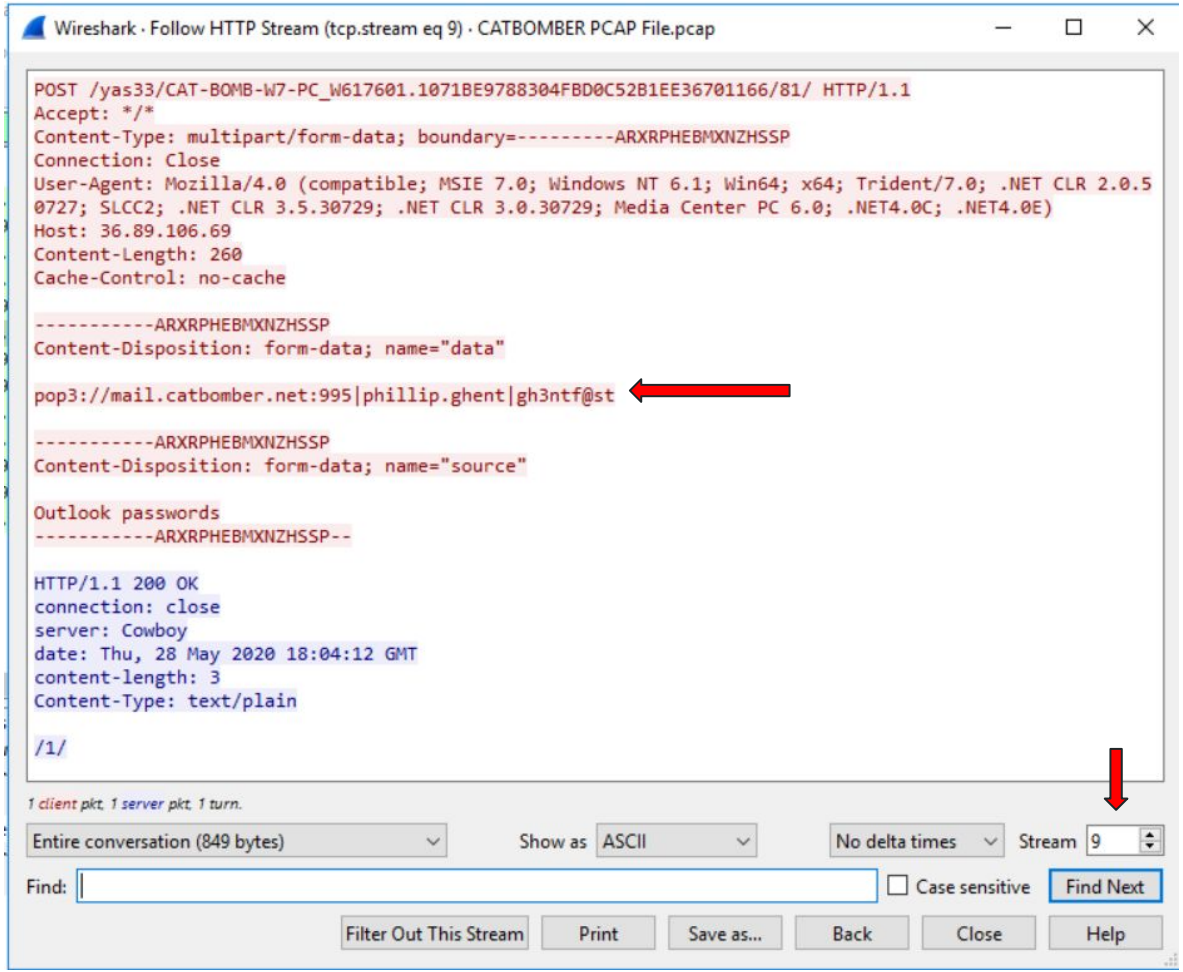
- Applying this filter in Wireshark helps identify HTTP traffic with /81 in the URI
- This filter narrows down the traffic, making it easier to locate sensitive information
- Data exfiltration can also occur through other methods like SMTP, FTP, and more, depending on the type of stolen information



Exfiltrated Passwords

By using that filter, we:

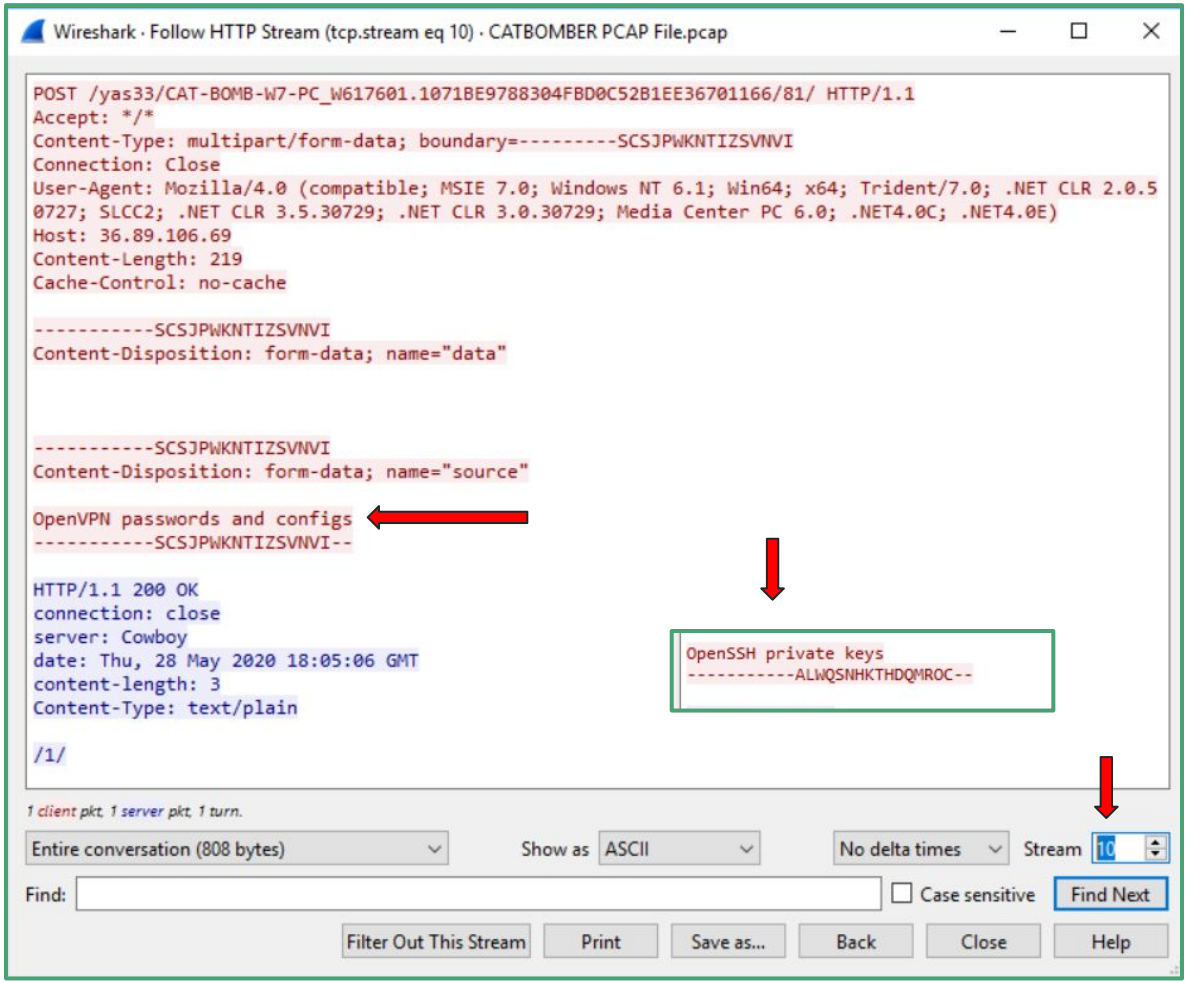
- Recovered the stolen information, which is Phillip's Outlook Email Password
- His password is gh3ntf@st
- If we stream up one or two more...



Exfiltrated Passwords

We can see that OpenVPN passwords and configs are also being stolen.

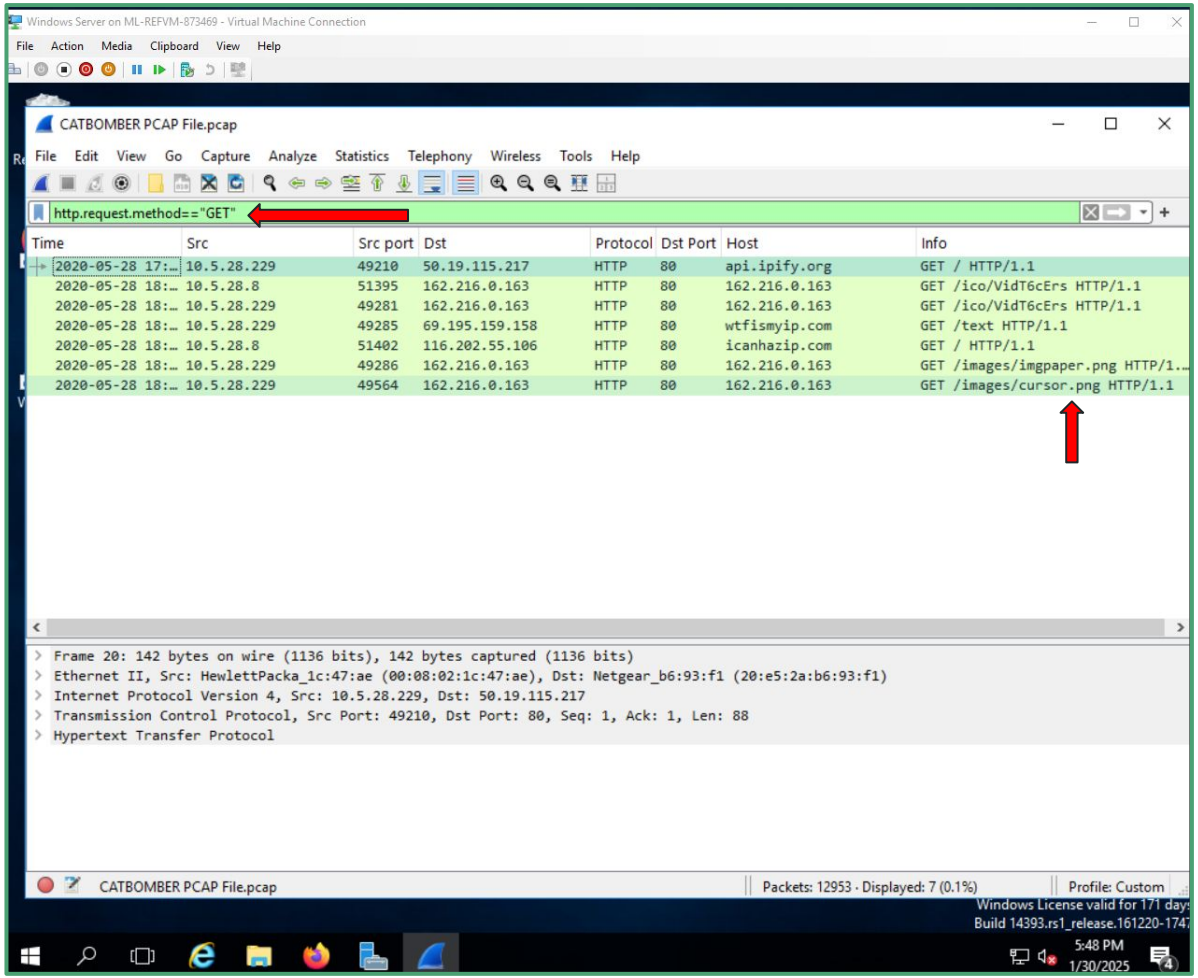
If we go to stream 11, we can also see that an Open SSH private key is being stolen by the Trickbot infection



Suspicious Files

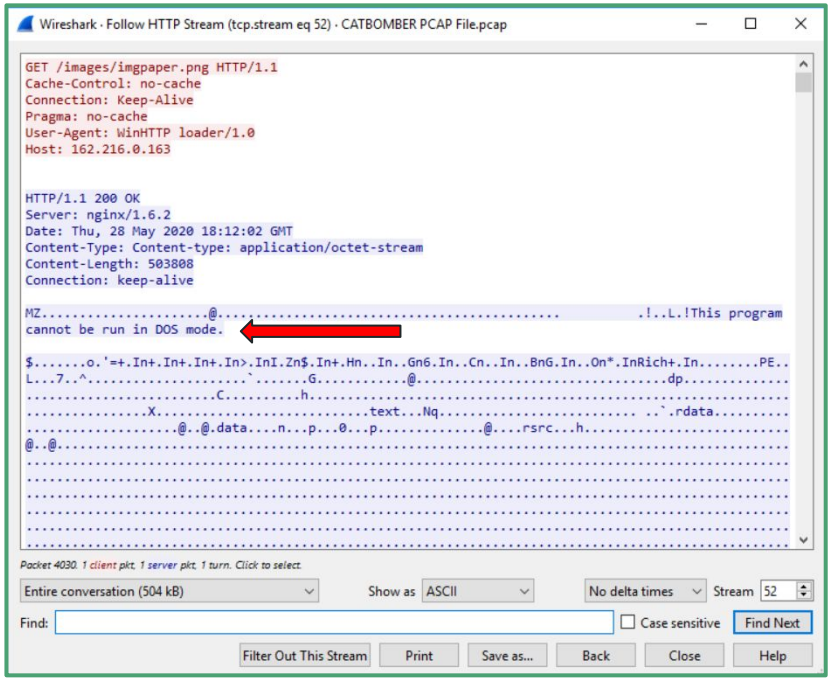
When we apply another filter, the GET filter, we can look for suspicious files

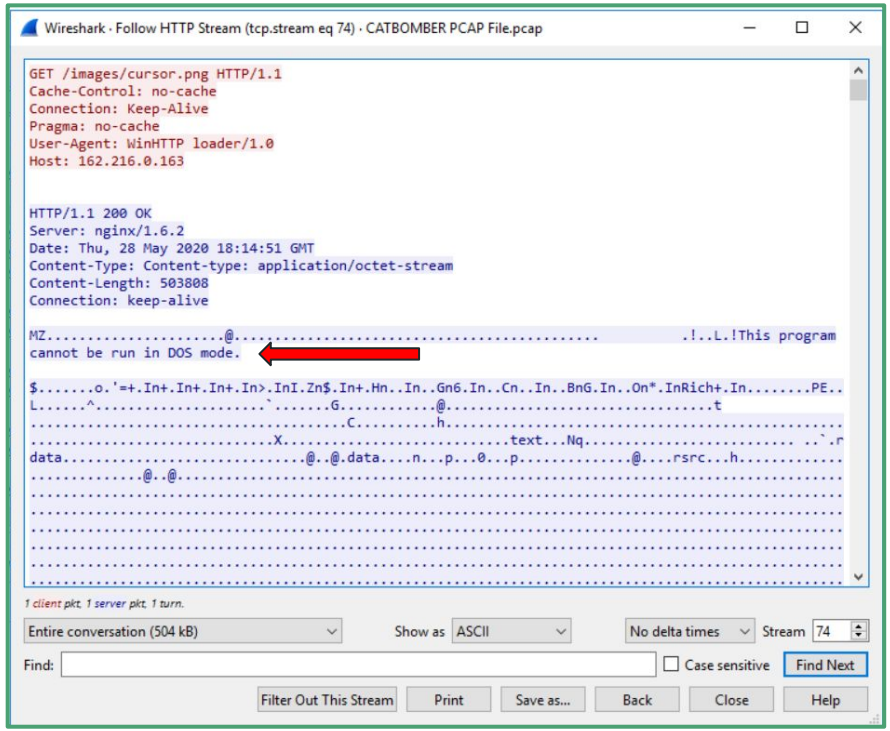
- When we skim through the packets, we can see that there are two .png files that were sent
- PNG files can often be used to package malware containing viruses



Suspicious Files

We can see that these files can't be run in DOS mode, indicating a spoofed .png file. These executable files mask as image files to bypass security.



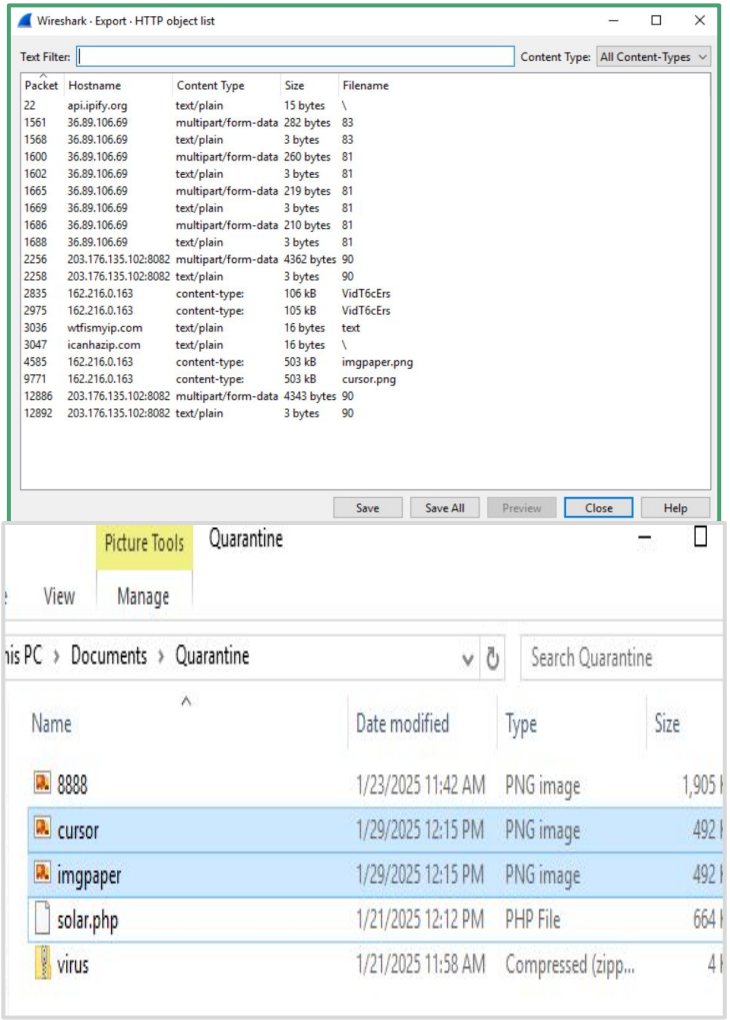


Hashes

We save the virus file to a quarantined folder on our VM.

This folder doesn't have Windows Defender set up or turned on for it, so we are able to use this to store the file while we check it for further information.

We will use TotalVirus to do so.



Hashes

- We upload the virus files to TotalVirus
- Reports that they are both malicious malware
- The hashes are given to us by VirusTotal, but powershell is also an option
- File Hashes:
  - 934c84524389ecfb3b1dfcb28f9697a2b52ea0ebcaa510469f0d2d9086bcc79a
  - 4e76d73f3b303e481036ada80c2eeba8db2f306cbc9323748560843c80b2fed1