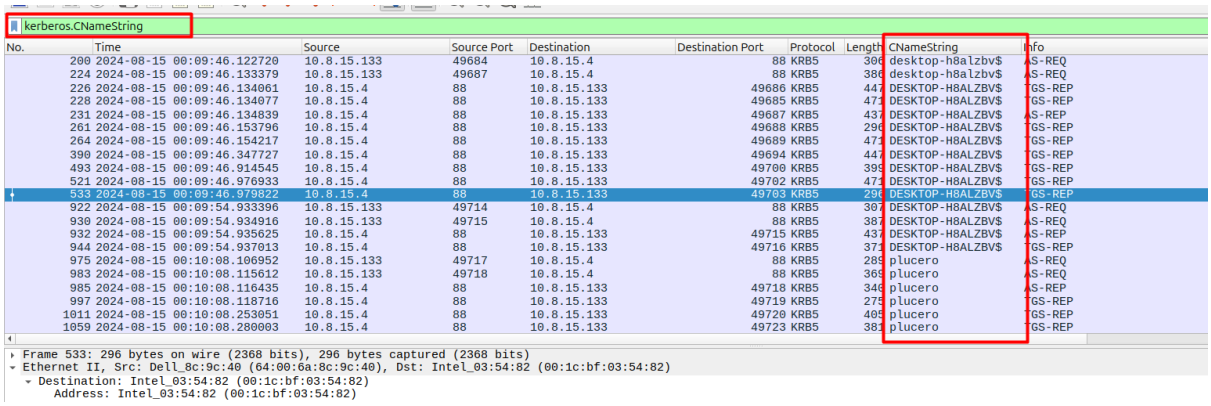
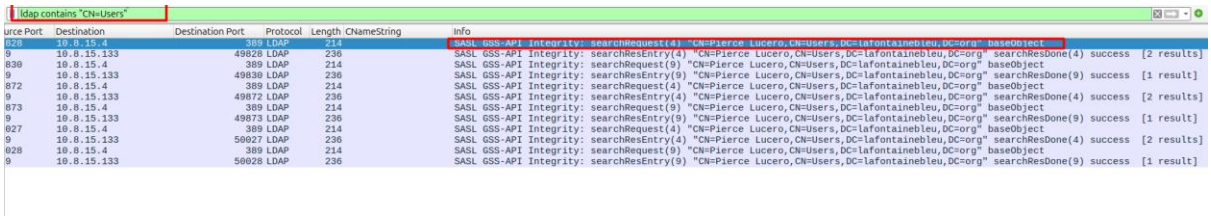
Identify Host and the Client

With Kerberos.CNameString

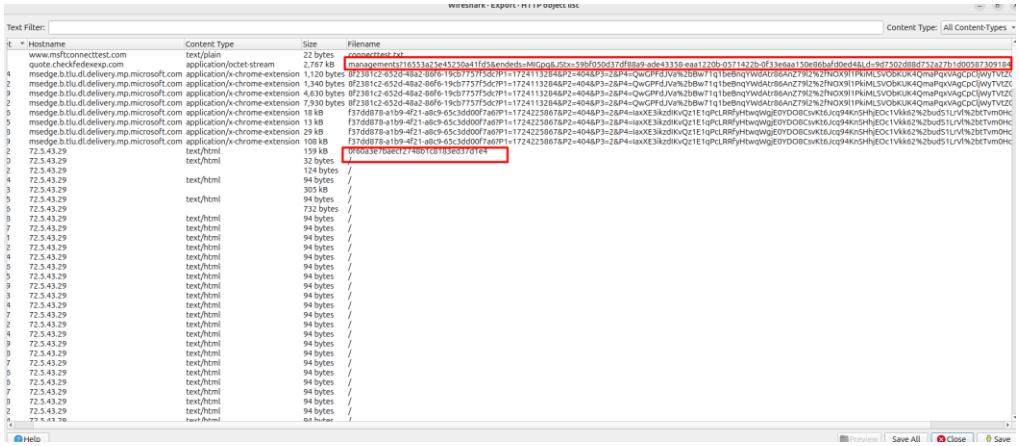


With LDAP



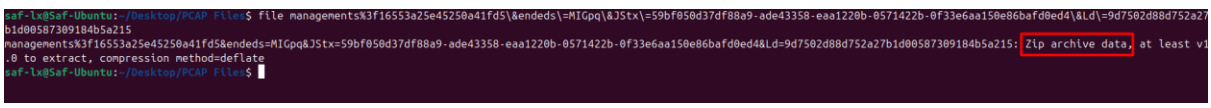
Export the zip file.

File → Export Object → HTTP



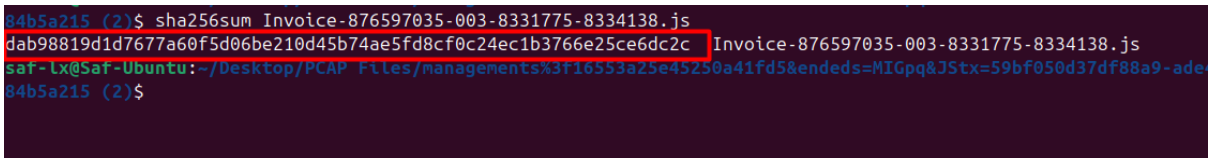
Save this file and export to your machine.

Extract the file type and hashes

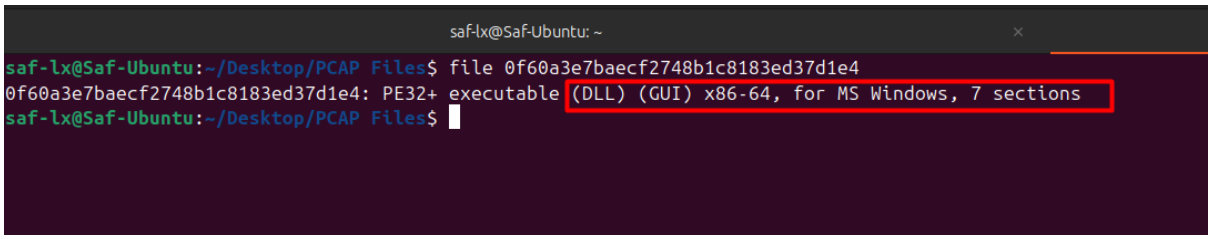


Shown above: File type is zip achieve data.

Shown above: sha256 hash of the zip file

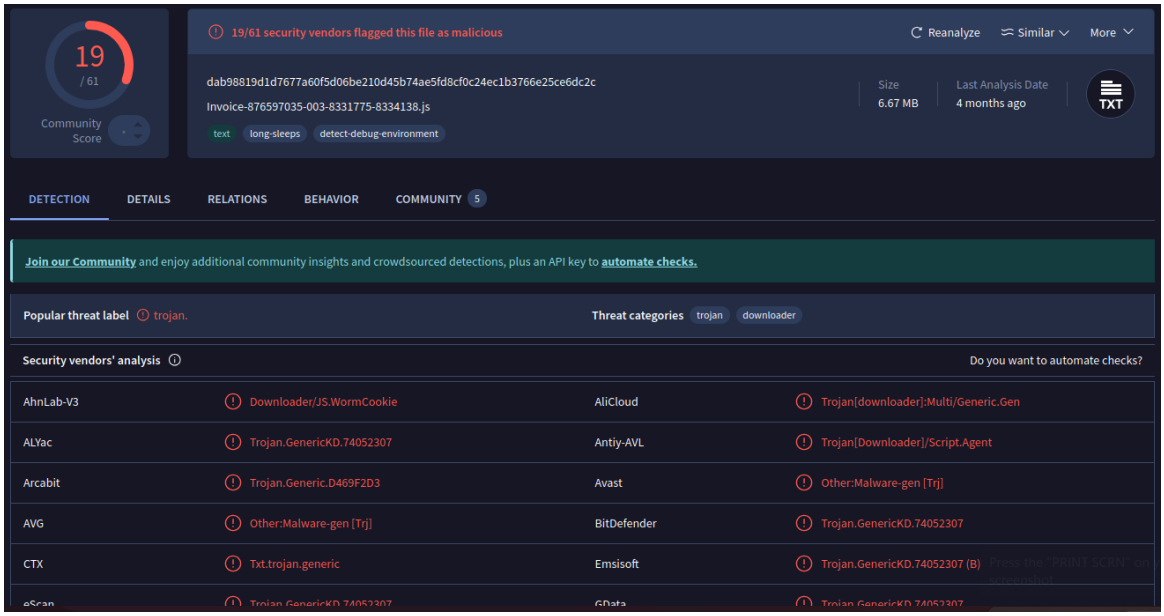


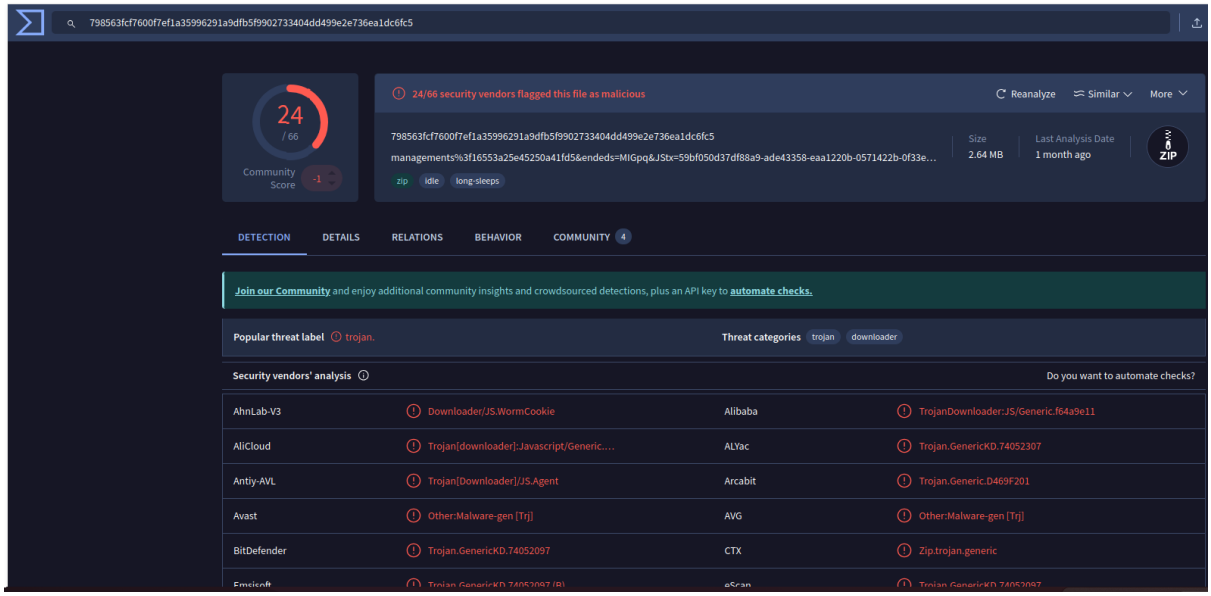
Shown above: sha256 hash of the js file inside zip file

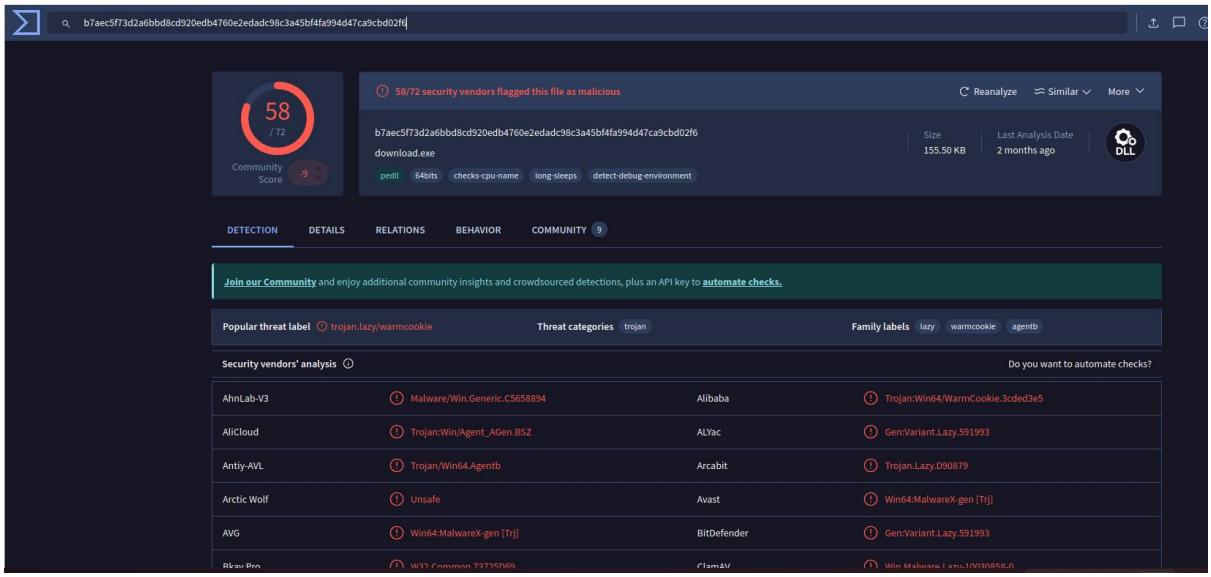


Shown above: sha256 hash of the dll file

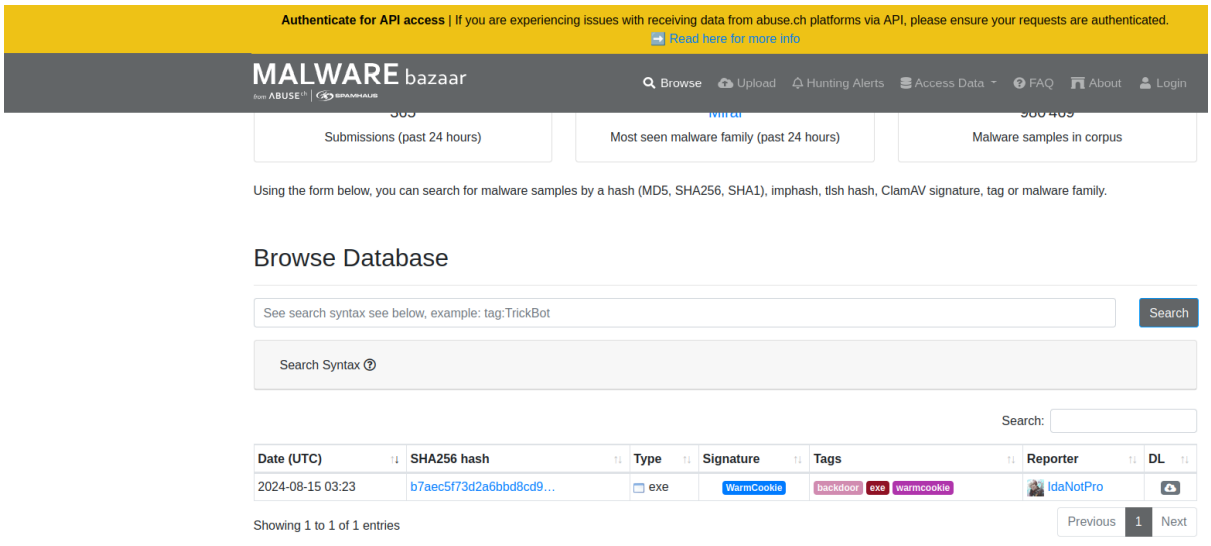
Copy the extracted hashes in **VirusTotal** and **MalwareBazaar**







Shown above: VirusTotal Entry



Shown above: MalwareBazaar Entry

The VirusTotal entry for this DLL, zip and js file indicates a crowd-sourced YARA rule identifies this as WarmCookie. The MalwareBazaar analysis of this file also identifies it as WarmCookie.