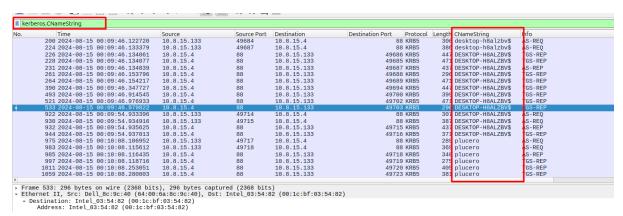
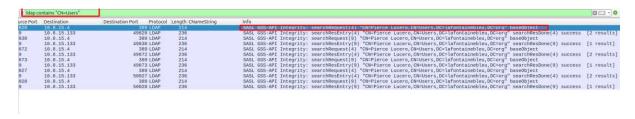
Identify Host and the Client

With Kerberos.CNameString

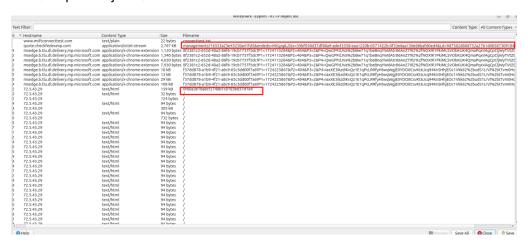


With LDAP



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.

```
ssf-lugSsf-Ubunter: / Deskton/PCAP Files$ sha256sum managements%3f16553a25e45250a41fd5\@endeds\=MIGpq\@35tx\=59bf050d37df88a9-ade43358-eaa1220b-0571422b-0f33e6aa150e86bafd0ed4\&Ld\=9d7502d88d7
52a27b1d0058730918db5a215
799853fcfr6008f70f1a3599629139dfb5f9902733404dd499e2e736ea1dc6fc5
managements%3f16553a25e45250a41fd5&endeds=MIGpq\@35tx=59bf050d37df88a9-ade43358-eaa1220b-0571422b-0f33e6aa150e86bafd0ed4&Ld=9
d7502d88d752a27b1d00587309184b5a215
saf-lugSaf-Ubuntu:-/Desktop/PCAP Files$
```

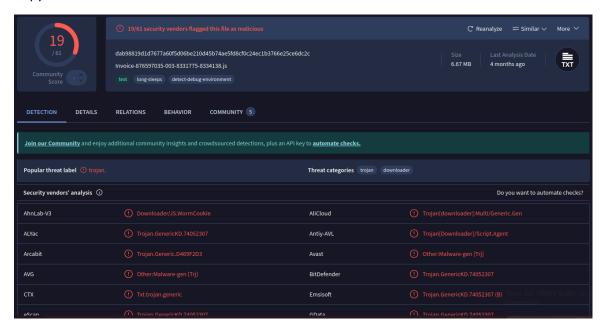
Shown above: sha256 hash of the zip file

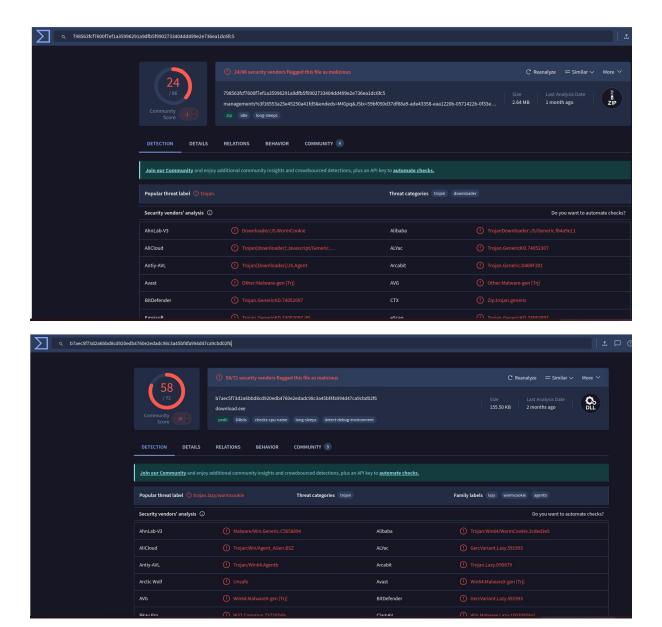
Shown above: sha256 hash of the js file inside zip file

```
saf-lx@Saf-Ubuntu:~/Desktop/PCAP Files$ file 0f60a3e7baecf2748b1c8183ed37d1e4
0f60a3e7baecf2748b1c8183ed37d1e4: PE32+ executable (DLL) (GUI) x86-64, for MS Windows, 7 sections
saf-lx@Saf-Ubuntu:~/Desktop/PCAP Files$
```

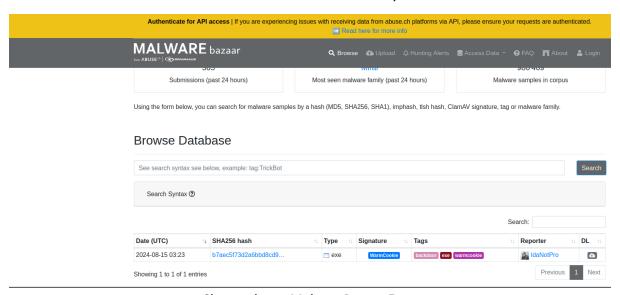
Shown above: sha256 hash of the dll file

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.