Network Capture Task

WE Innovate

Prepared By Omar Hassan

You work as an analyst at a (SOC). Someone contacts your team to report a coworker has downloaded a suspicious file after searching for **Google Authenticator.**

- LAN segment range: **10.1.17[.]0/24** (**10.1.17[.]0** through **10.1.17[.]255**)
- Domain: **bluemoontuesday[.]com**
- Active Directory (AD) domain controller: **10.1.17[.]2 - WIN-GSH54QLW48D**
- AD environment name: **BLUEMOONTUESDAY**
- LAN segment gateway: **10.1.17[.]**1
- LAN segment broadcast address: **10.1.17[.]255**

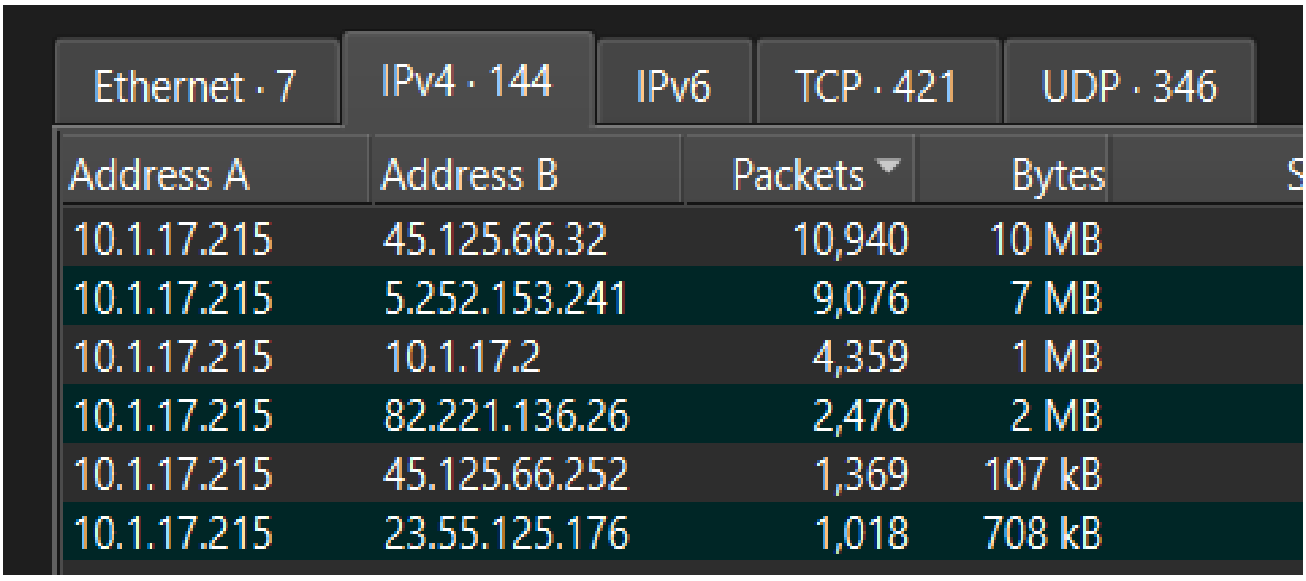
TASK

For this exercise, answer the following questions for your incident report:

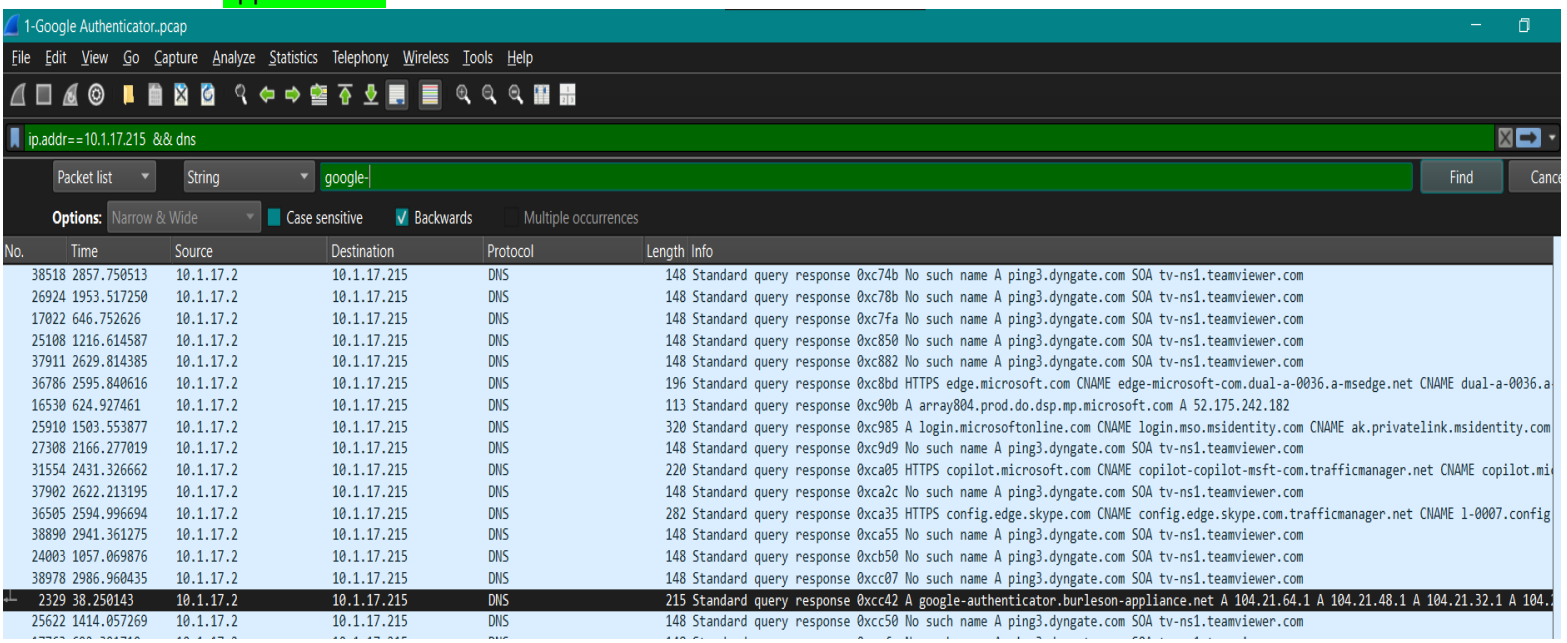
- What is the IP address of the infected Windows client?
- What is the mac address of the infected Windows client?
- What is the host name of the infected Windows client?
- What is the user account name from the infected Windows client?
- What is the likely domain name for the fake Google Authenticator page?
- What are the IP addresses used for C2 servers for this infection?

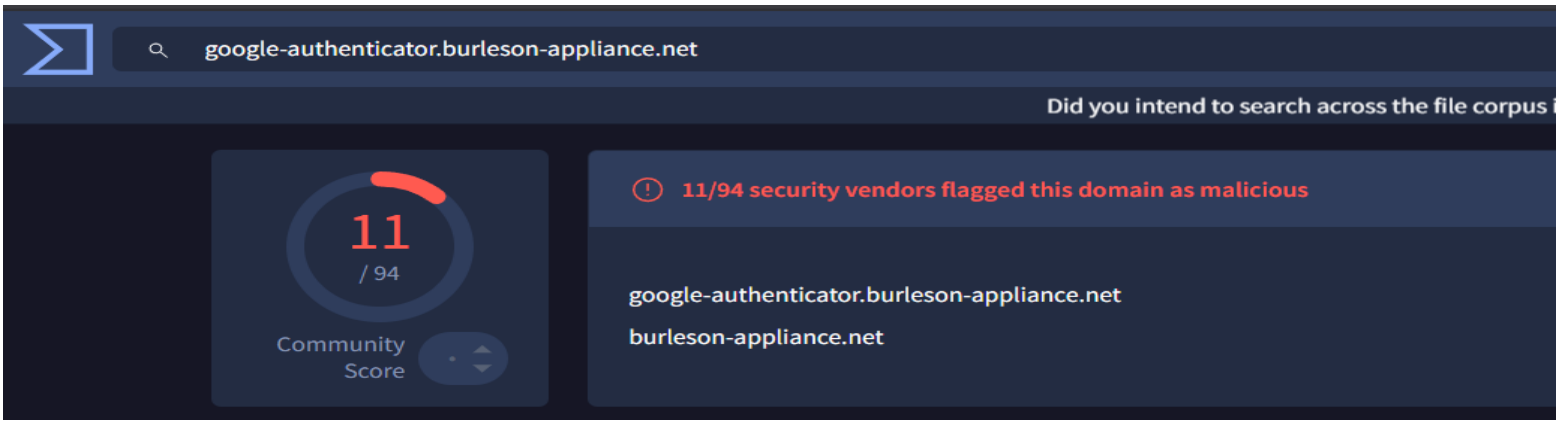
---

1. My first thought is to look into the conversation tab to get a summary or any clue about the IPs that we have. Statistics > Conversations

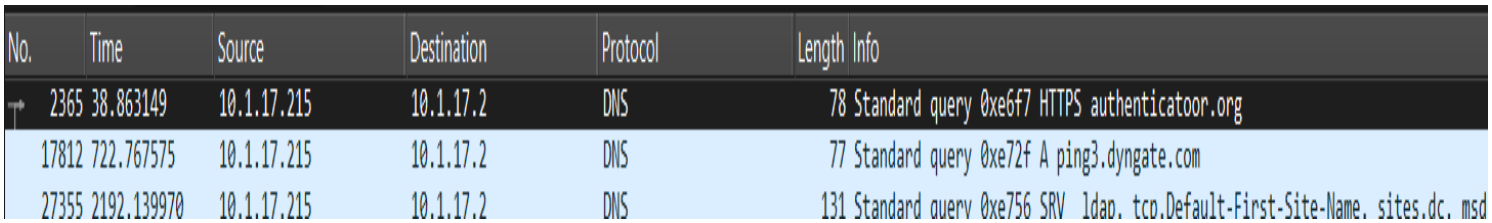


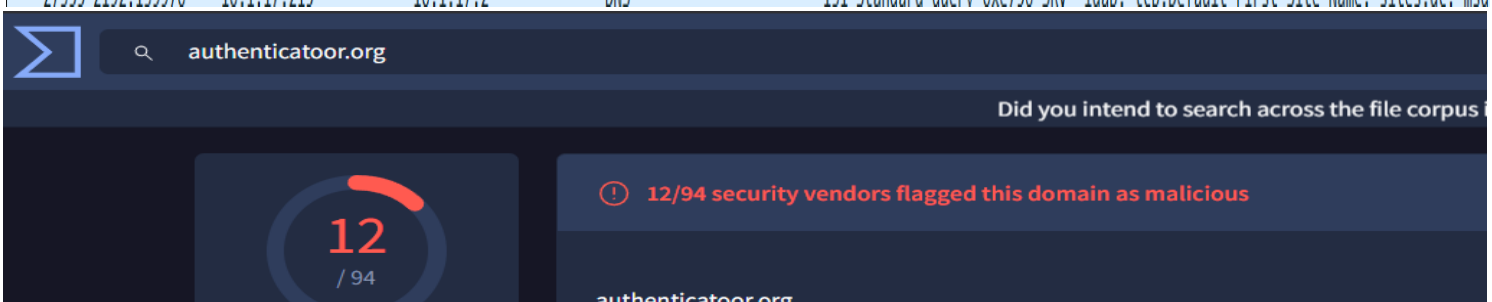
2. There is something going on with ip 10.1.17.215 which is in LAN segment range , therefore I will search for this specific IP and then filter using dns and search for ‘google-’ to see if there is an impersonation going on , fake google authenticator : google-authenticator.burleson-appliance.net.



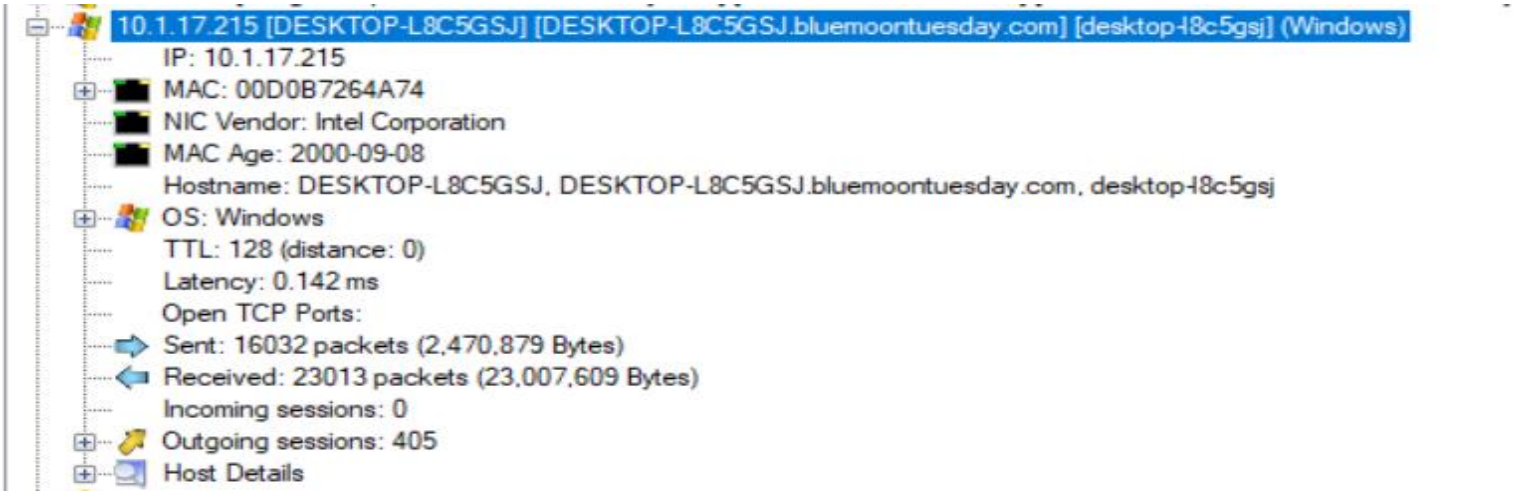


3. And then I managed to find another one , so probably there are more that malicious domain , notice the extra o ?

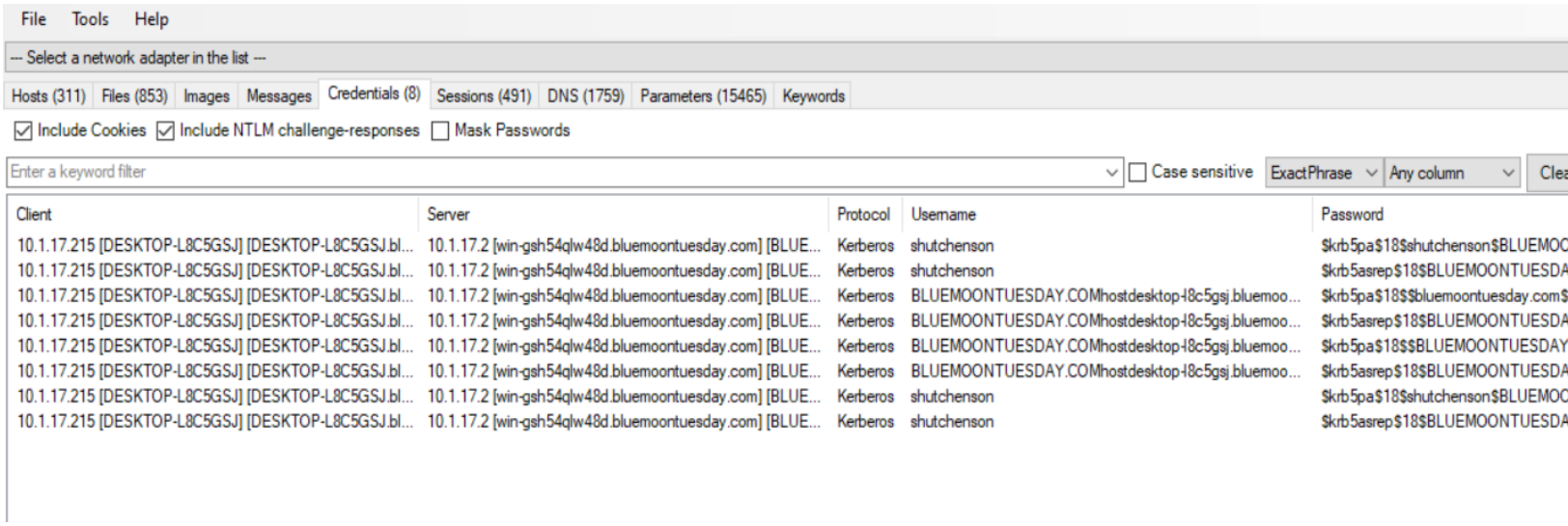




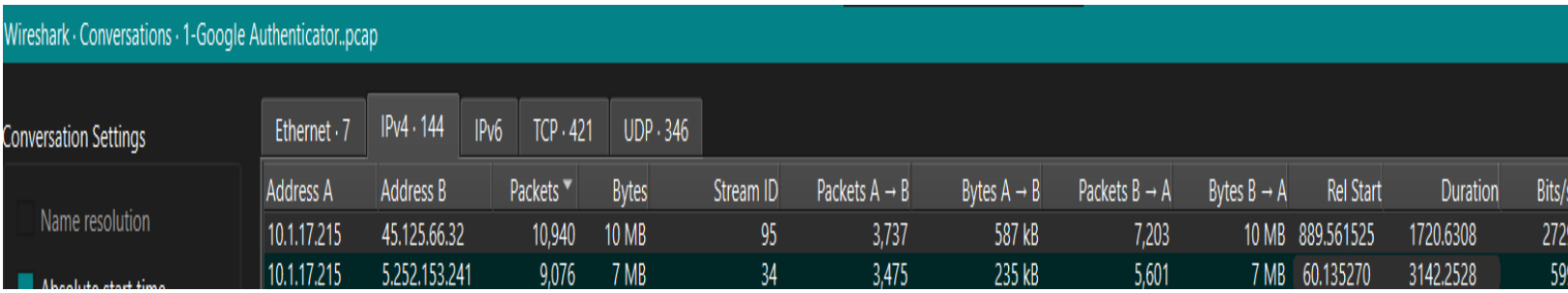
5. So therefore we can find that the infected host is indeed 10.1.17.215 and for the rest of the info I will use network miner for ease. (Everything is displayed about this host)



6. We can also get the username with passwords too using the credentials tab



7. Now the remaining question "What are the IP addresses used for C2 servers for this infection?" I suspect those two because they are out of the LAN and have the most packets but we will do further investigation.



8. I inspect both IPs and find some suspicious commands in the query using http filter & ip.addr

ip.addr== 5.252.153.241 && http

No.	Time	Source	Destination	Protocol	Length	Info
39370	3170.494838	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
39377	3176.097646	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
39386	3181.340731	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
39397	3186.535218	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
39404	3191.727993	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
39413	3196.921867	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
39424	3202.128240	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
13677	129.210334	10.1.17.215	5.252.153.241	HTTP	176	GET /1517096937?k=message%20=%20startup%20shortcut%20created;%20%20status%20=%20success; HTTP/1.1
19292	881.889559	10.1.17.215	5.252.153.241	HTTP	174	GET /1517096937?k=script:%20RunRH,%20status:%20OK,%20message:%20PS%20process%20started HTTP/1.1
28335	2413.352160	10.1.17.215	5.252.153.241	HTTP	174	GET /1517096937?k=script:%20RunRH,%20status:%20OK,%20message:%20PS%20process%20started HTTP/1.1
33356	2577.662979	10.1.17.215	5.252.153.241	HTTP	174	GET /1517096937?k=script:%20RunRH,%20status:%20OK,%20message:%20PS%20process%20started HTTP/1.1
5031	60.297799	10.1.17.215	5.252.153.241	HTTP	371	GET /api/file/get-file/264872 HTTP/1.1
5063	62.145732	10.1.17.215	5.252.153.241	HTTP	144	GET /api/file/get-file/29842.ps1 HTTP/1.1
13643	128.827817	10.1.17.215	5.252.153.241	HTTP	113	GET /api/file/get-file/TV HTTP/1.1
8002	124.998139	10.1.17.215	5.252.153.241	HTTP	121	GET /api/file/get-file/TeamViewer HTTP/1.1
12890	128.458764	10.1.17.215	5.252.153.241	HTTP	133	GET /api/file/get-file/Teamviewer_Resource_fr HTTP/1.1
13671	128.984576	10.1.17.215	5.252.153.241	HTTP	118	GET /api/file/get-file/pas.ps1 HTTP/1.1
5033	60.464642	5.252.153.241	10.1.17.215	HTTP	819	HTTP/1.1 200 OK
5071	62.309349	5.252.153.241	10.1.17.215	HTTP	555	HTTP/1.1 200 OK
8000	124.958915	5.252.153.241	10.1.17.215	HTTP	444	HTTP/1.1 200 OK

9. There are a lot of suspicious things especially the highlighted packet therefore 5.252.153.241 is a suspicious c2.