Network Analysis – Malware Compromise

Project Description

In this project, I will be using several tools to analyze a Packet Capture (PCAP) from a scenario provided by Blue Team Labs website.

Software and Tools

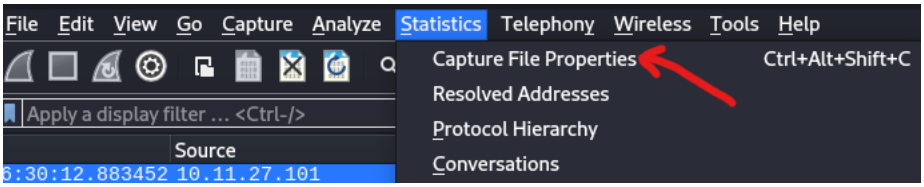
- Kali Linux VM
- Wireshark
- VirusTotal
- Zui

Walkthrough

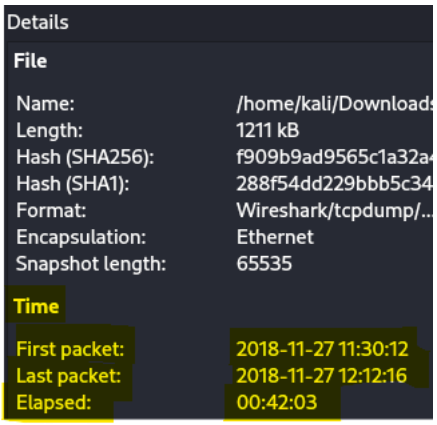
This is the following scenario:

"A SOC Analyst at Umbrella Corporation is going through SIEM alerts and sees the alert for connections to a known malicious domain. The traffic is coming from Sara's computer, an Accountant who receives a large volume of emails from customers daily. Looking at the email gateway logs for Sara's mailbox there is nothing immediately suspicious, with emails coming from customers. Sara is contacted via her phone, and she states a customer sent her an invoice that had a document with a macro, she opened the email and the program crashed. The SOC Team retrieved a PCAP for further analysis."

Using my Kali Linux virtual machine, the first step was to download the PCAP handed to me and open it with Wireshark. Once opened, I went to the *Statistics* tab and clicked on *Capture File Properties.*



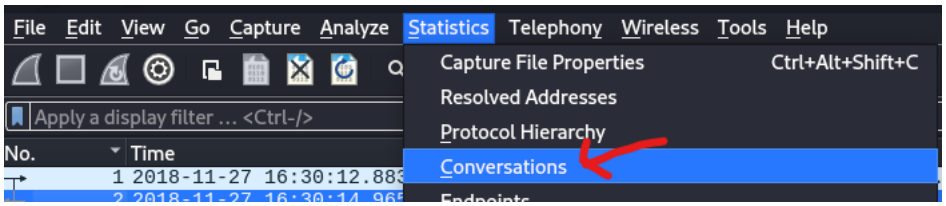
After clicking it, I checked the times of the first and last packet. The reason for checking the times is to make sure the PCAP handed to me was withing the timeframe, and they were.



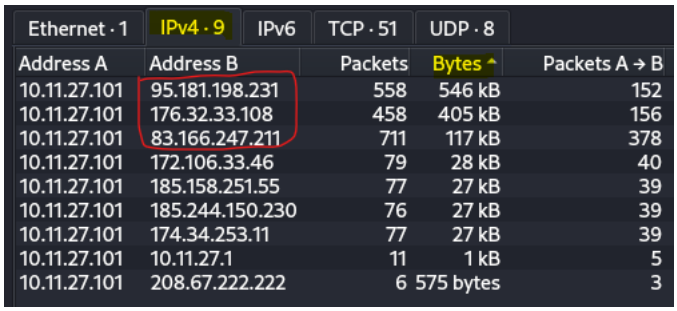
Then, I went to *Statistics --> Protocol Hierarchy* to check what kind of protocols exist in this PCAP. There, I could see some protocols being used like DNS, TLS, and HTTP, as seen in the image below.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes
Frame	100.0	2053	100.0	1178802	3737	0	0
Ethernet	100.0	2053	2.4	28742	91	0	0
Internet Protocol Version 4	100.0	2053	3.5	41060	130	0	0
User Datagram Protocol	0.8	17	0.0	136	0	0	0
Domain Name System	0.8	17	0.1	1253	3	17	1253
Transmission Control Protocol	99.2	2036	94.0	1107611	3511	1706	976962
Transport Layer Security	15.5	318	14.4	169625	537	318	169625
Hypertext Transfer Protocol	0.6	12	76.0	896450	2841	6	2146
Media Type	0.1	2	22.0	259449	822	2	259449
Line-based text data	0.1	3	41.6	489960	1553	3	489960
Data	0.0	1	22.2	261120	827	1	261120

Next, I went to *Statistics --> Conversations:*



From there, I went to the `IPv4•9` tab and sorted the conversations by Bytes, having the highest byte at the top. The top three conversations have an internal IP address of 10.11.27.101 communicating with three external IP addresses as shown below.

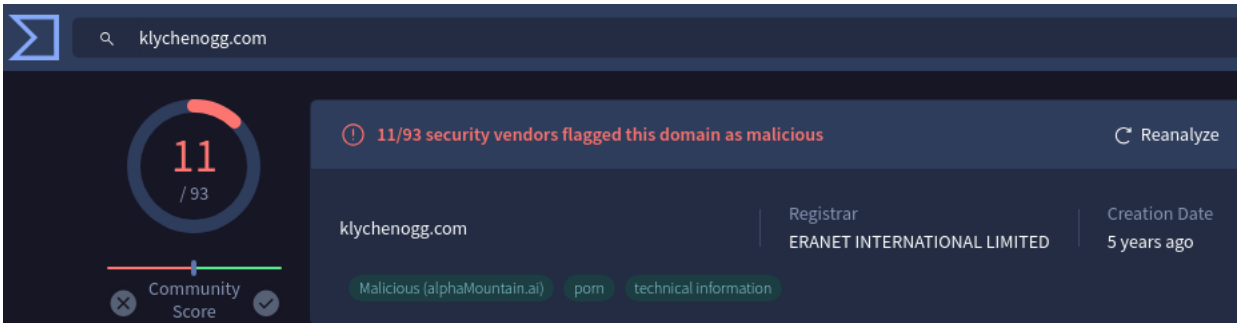


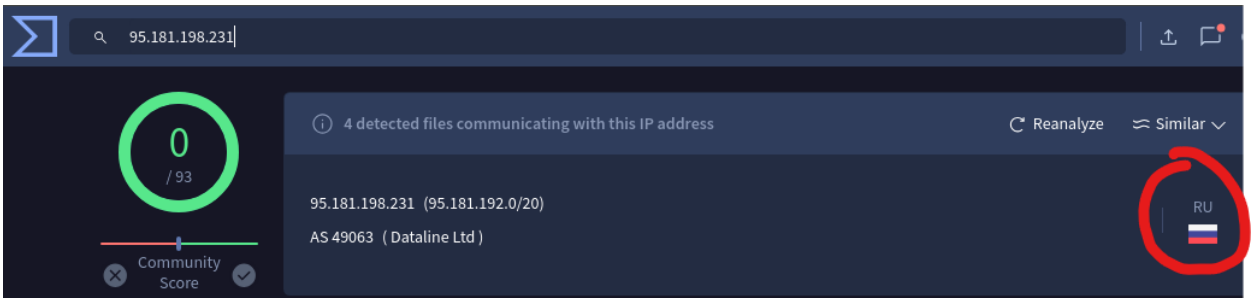
Ethernet · 1 | IPv4 · 9 | IPv6 | TCP · 51 | UDP · 8

Address A	Address B	Packets	Bytes	Packets A → B
10.11.27.101	95.181.198.231	558	546 kB	152
10.11.27.101	176.32.33.108	458	405 kB	156
10.11.27.101	83.166.247.211	711	117 kB	378
10.11.27.101	172.106.33.46	79	28 kB	40
10.11.27.101	185.158.251.55	77	27 kB	39
10.11.27.101	185.244.150.230	76	27 kB	39
10.11.27.101	174.34.253.11	77	27 kB	39
10.11.27.101	10.11.27.1	11	1 kB	5
10.11.27.101	208.67.222.222	6	575 bytes	3

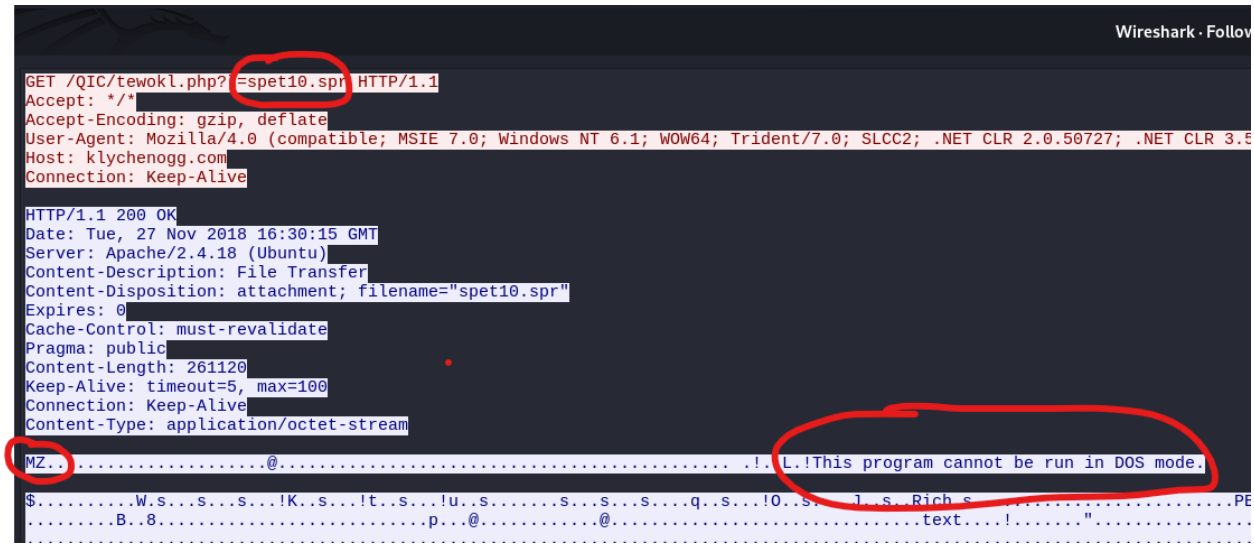
I went back to Wireshark and checked the first packet, which is a standard query out to the domain `klychenogg.com`. Underneath it, there's a response from this domain with the IP address `95.181.198.231`, which is one of the top IPs from the conversations.

Using both the domain and IP address, I visited VirusTotal to analyze them. As seen in the images below, the domain `klychenogg.com` showed a total of eleven vendors flagging it as malicious. While the IP address `95.181.198.231` had zero flags, it showed its location at Russia, which can help us confirm if the client does business with Russia or not.

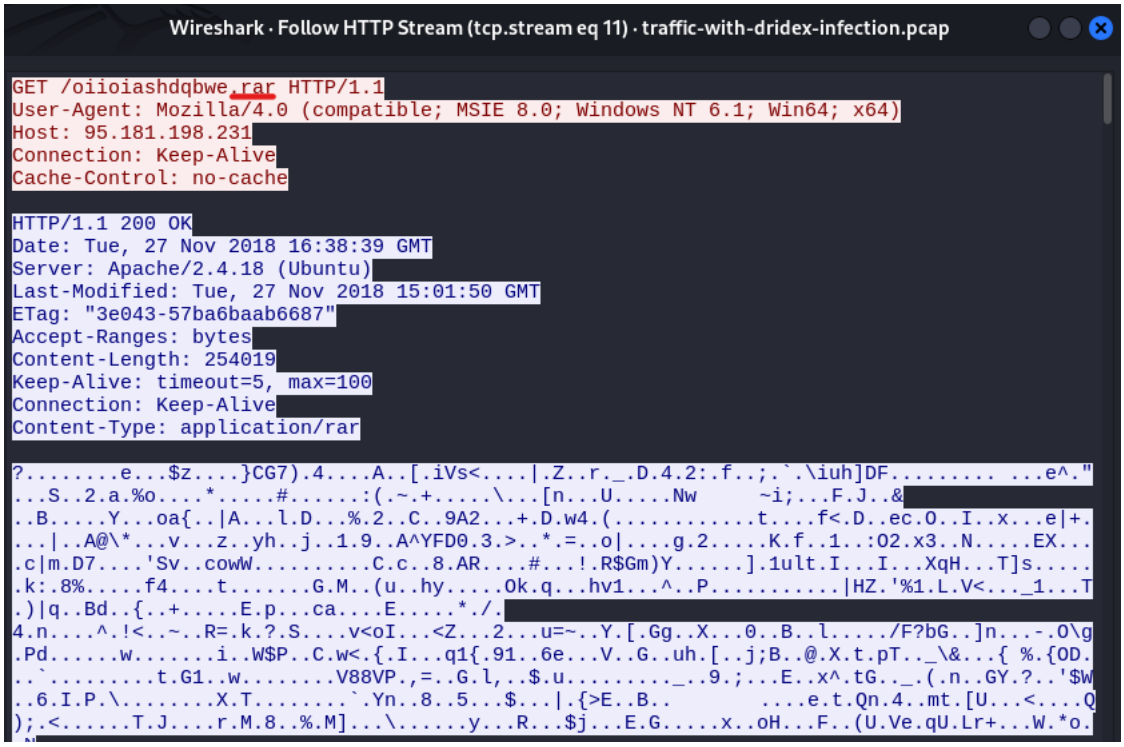




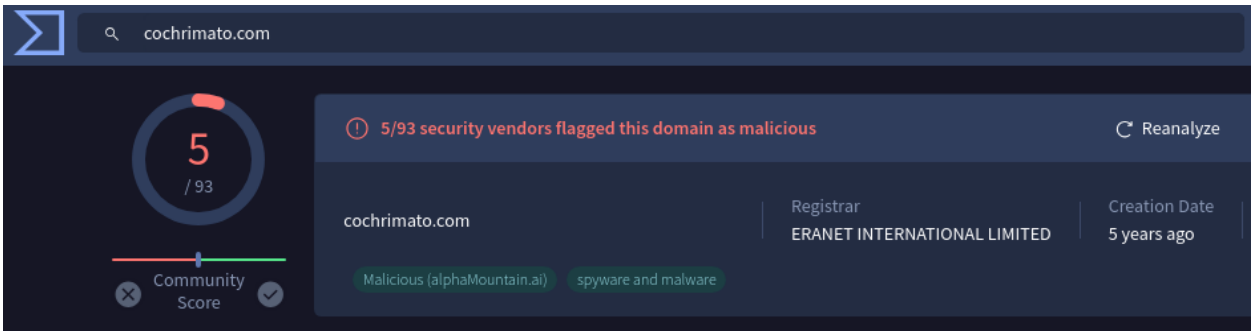
Going back to the PCAP, packet No. 6 shows the first ***HTTP GET*** request which occurred on 16:30:15. When I clicked ***Follow --> HTTP Stream*** on this packet, it showed that the request has a file towards ***spet.10.spr*** and the file response packet shows an MZ header with the string "***This program cannot be run in DOS mode***." as shown below.

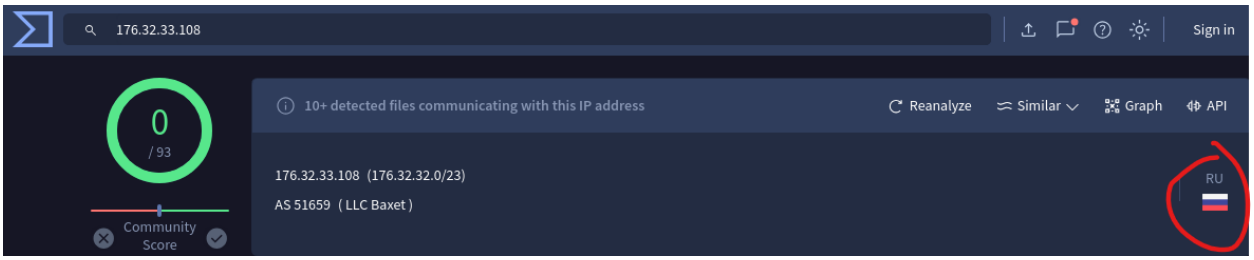


From the conversations, I started checking on the first top IP address, which is `95.181.198.231`, and the *HTTP* protocol on Wireshark. After applying filters, I received two results: packet No. 6 and No. 911. I have already checked No. 6, which leaves me only No. 911. When I clicked ***Follow --> HTTP Stream*** on this packet, it showed a request for a .rar file, and a large group of characters that does not provide much information.

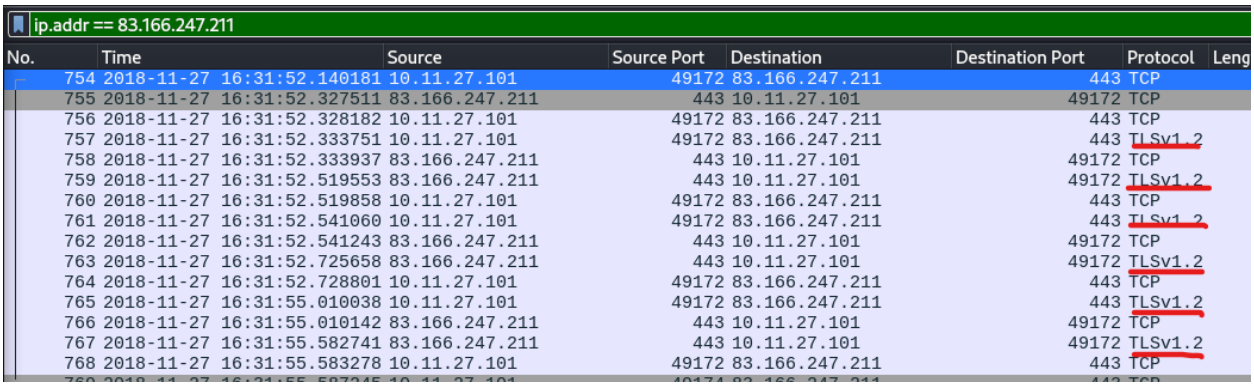


Now, I'll check the second IP address from the top three conversations. On the filter bar, I filtered the IP by typing `ip.addr == 176.32.33.108`. The first HTTP GET request shows after a three-way TCP handshake. This GET request shows that it is getting an image. When I clicked ***Follow --> HTTP Stream*** on this packet, it showed a .avi file on a host named `cochrimato.com`. I checked this domain on VirusTotal and it showed five vendors flagging it as malicious. Then, I checked the IP `176.32.33.108` on VirusTotal. While it showed 0 flags, its location is also from Russia.





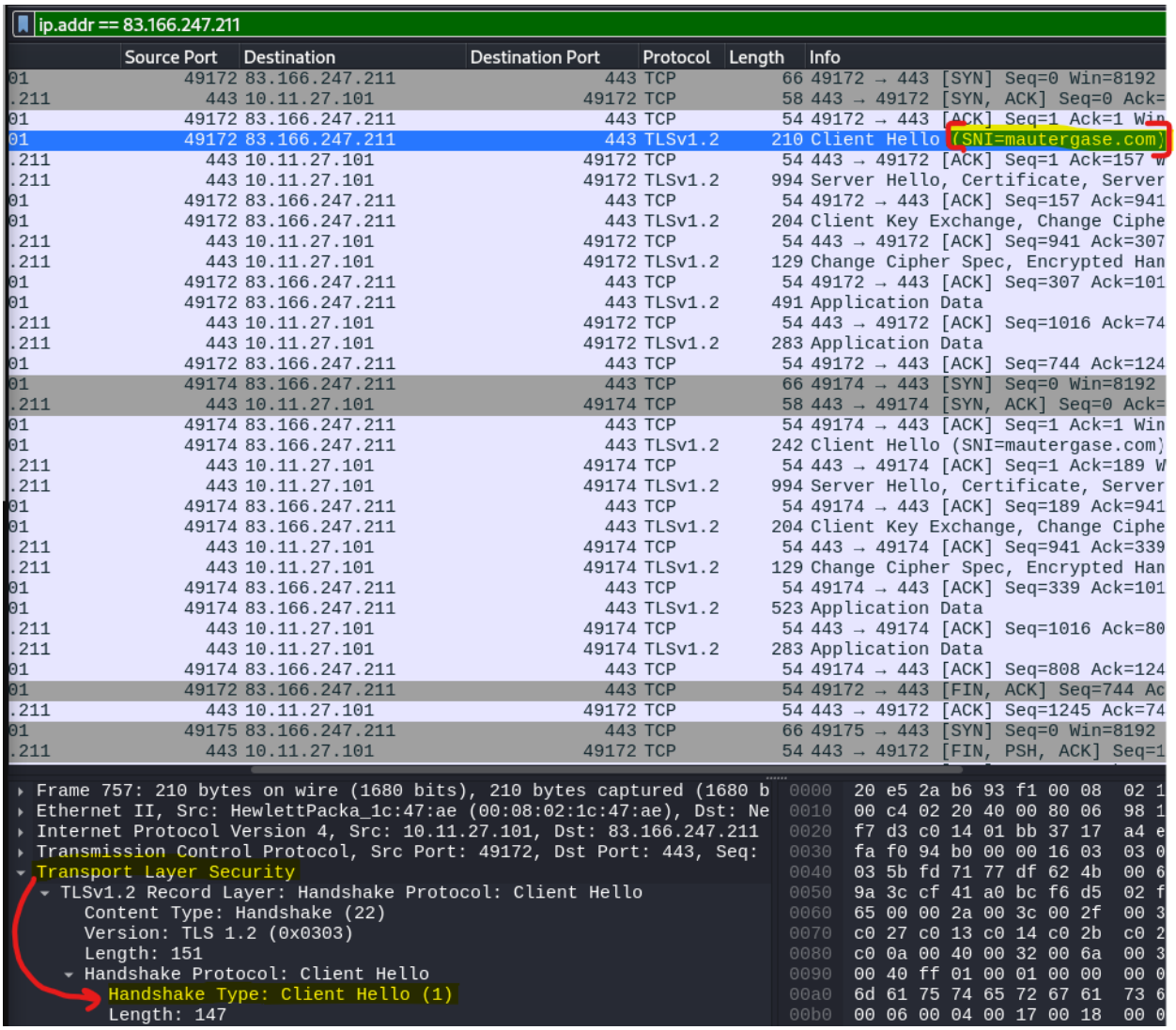
Then, I proceeded to filter the last IP address from the conversations. After filtering by using `ip.addr == 83.166.247.211`, I noticed that all packets are encrypted based on the protocol that has been used, which is TLSv1.2.



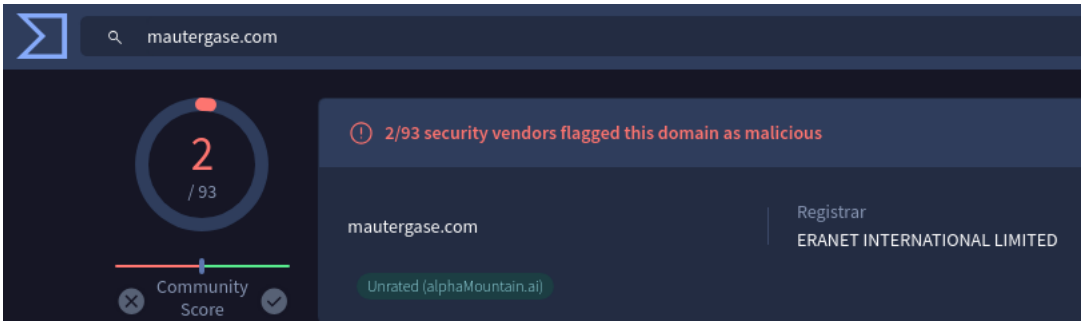
ip.addr == 83.166.247.211

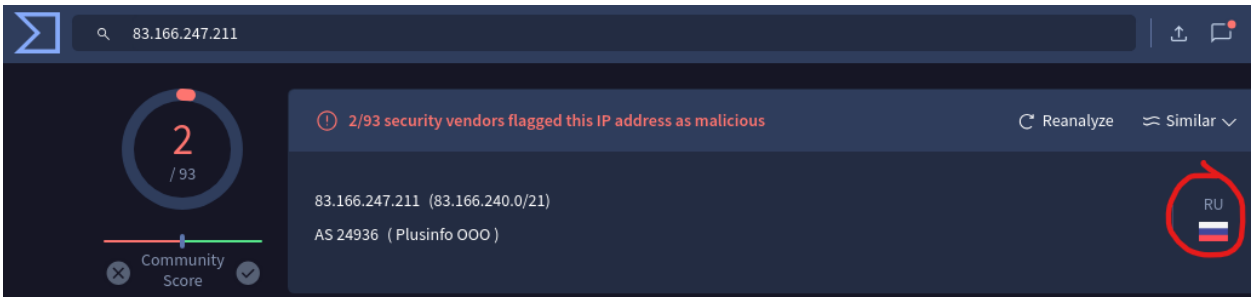
No.	Time	Source	Source Port	Destination	Destination Port	Protocol	Leng
754	2018-11-27 16:31:52.140181	10.11.27.101	49172	83.166.247.211	443	TCP	
755	2018-11-27 16:31:52.327511	83.166.247.211	443	10.11.27.101	49172	TCP	
756	2018-11-27 16:31:52.328182	10.11.27.101	49172	83.166.247.211	443	TCP	
757	2018-11-27 16:31:52.333751	10.11.27.101	49172	83.166.247.211	443	TLSv1.2	
758	2018-11-27 16:31:52.333937	83.166.247.211	443	10.11.27.101	49172	TCP	
759	2018-11-27 16:31:52.519553	83.166.247.211	443	10.11.27.101	49172	TLSv1.2	
760	2018-11-27 16:31:52.519858	10.11.27.101	49172	83.166.247.211	443	TCP	
761	2018-11-27 16:31:52.541060	10.11.27.101	49172	83.166.247.211	443	TLSv1.2	
762	2018-11-27 16:31:52.541243	83.166.247.211	443	10.11.27.101	49172	TCP	
763	2018-11-27 16:31:52.725658	83.166.247.211	443	10.11.27.101	49172	TLSv1.2	
764	2018-11-27 16:31:52.728801	10.11.27.101	49172	83.166.247.211	443	TCP	
765	2018-11-27 16:31:55.010038	10.11.27.101	49172	83.166.247.211	443	TLSv1.2	
766	2018-11-27 16:31:55.010142	83.166.247.211	443	10.11.27.101	49172	TCP	
767	2018-11-27 16:31:55.582741	83.166.247.211	443	10.11.27.101	49172	TLSv1.2	
768	2018-11-27 16:31:55.583278	10.11.27.101	49172	83.166.247.211	443	TCP	

To see what the internal IP is trying to access, I expanded one of the packets that contained an **`SNI`** field within the **`Client Hello`** packet (No. 757 in this case), starting from the Transport Layer Security dropdown to the Handshake Protocol as shown below.

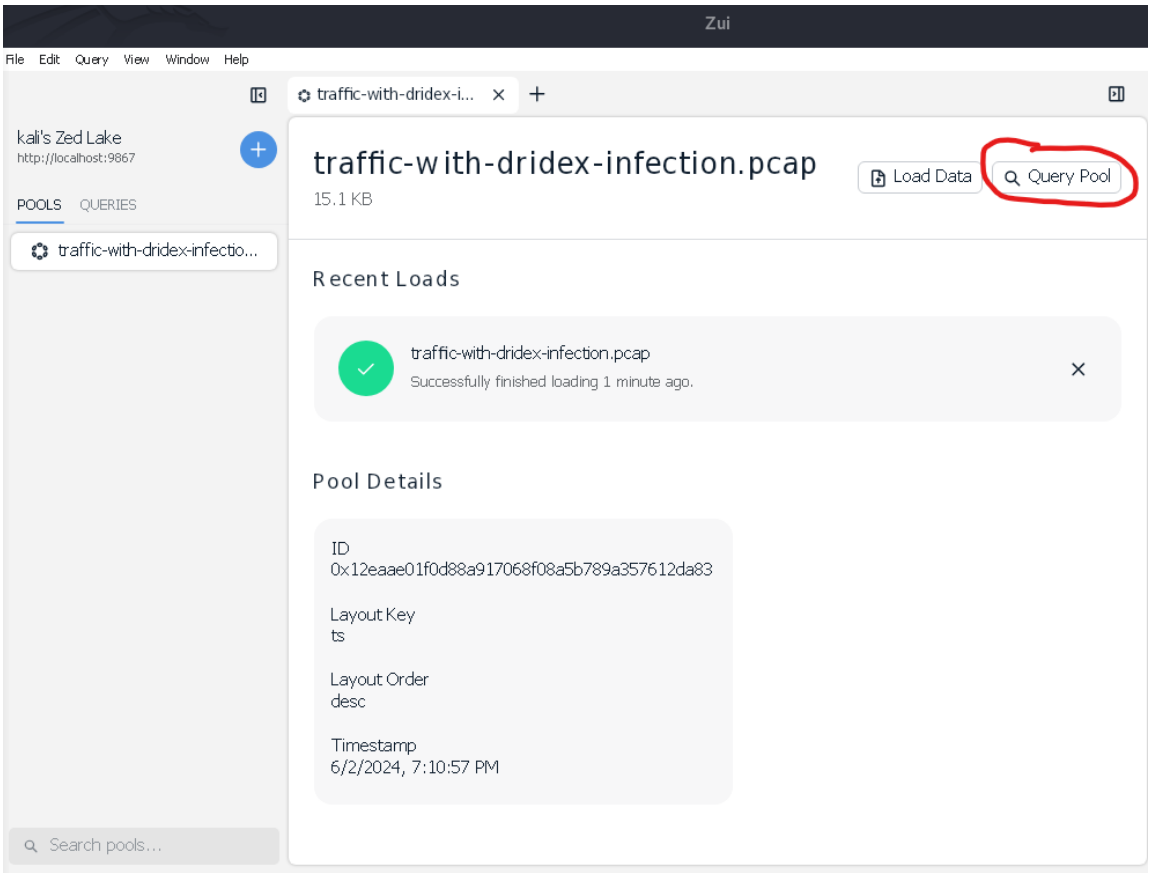


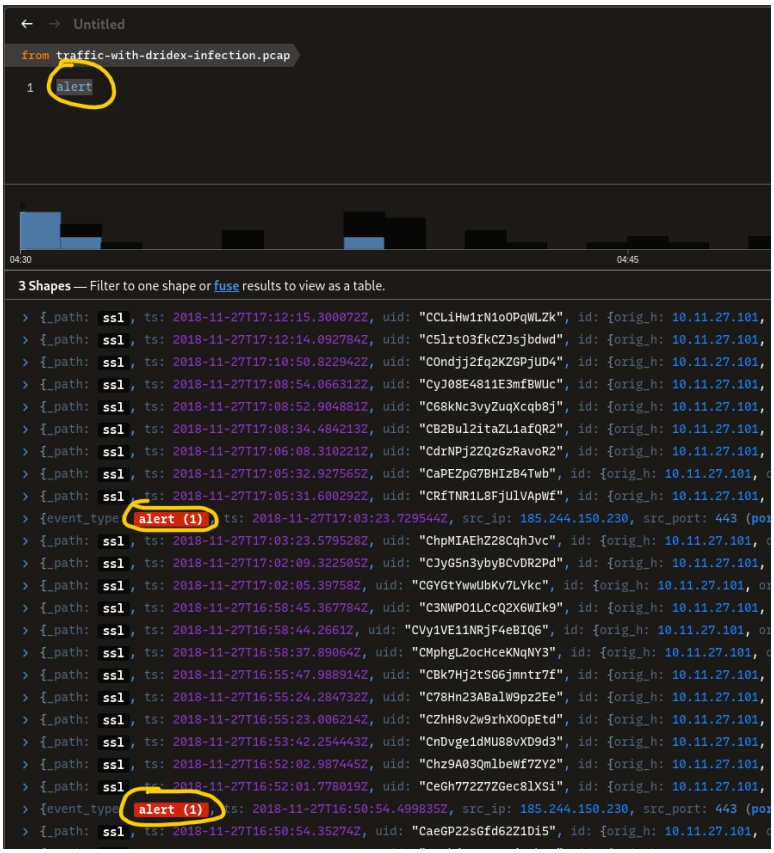
Since the **`SNI`** field had a value of "*mautergase.com*", I investigated this domain in VirusTotal, and it showed a total of two vendors flagging it as malicious. I also checked the IP `83.166.247.211` on VirusTotal. It had two vendors flagging it as malicious and, like the previous two IPs, it's also from Russia.



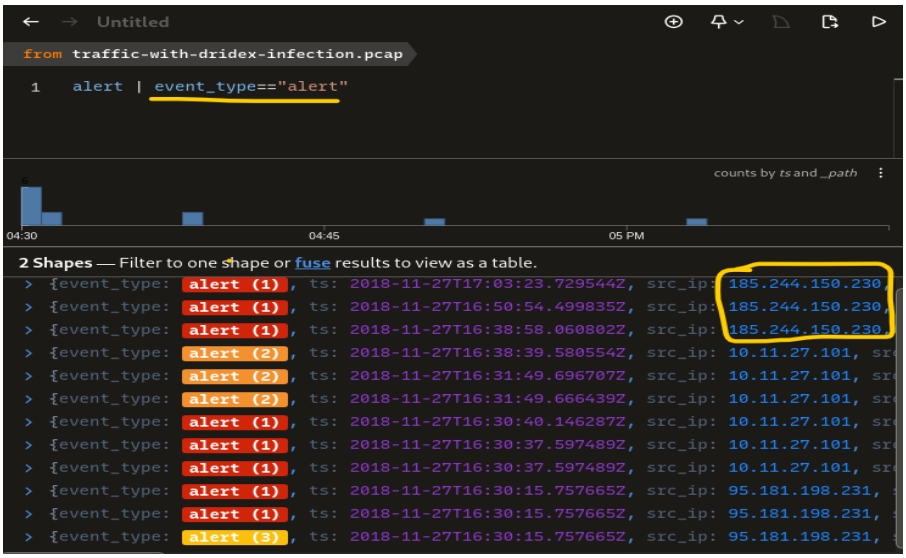


To further investigate this PCAP, I used another tool called Zui, which is like a combination of Zeek and Suricata. After loading the PCAP, I clicked on *Query Tool* to start querying. When I queried **`alerts`**, Zui displayed alerts and some SSL traffic.





Considering the fact that I was interested in seeing only the alerts that this PCAP has generated, I clicked on one of the alerts, clicked on **`event_type`**, and applied it as a filter. After that, Zui displayed all alerts and we can see a new IP address `185.244.150.230`, as seen below.



Lastly, after I expanded the earliest event of the alert from IP *185.244.150.23*, it showed some interesting information. As seen in the image below, the **signature** field had a message saying: "ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)"; and the **category** field had the following message: "Domain Observed Used for C2 Detected". With these findings, it is highly confirmed that Sarah's computer has been infected with a Dridex malware.


```
{
  event_type: alert (1),
  ts: 2018-11-27T16:38:58.060802Z,
  src_ip: 185.244.150.230,
  src_port: 443 (port=(uint16)),
  dest_ip: 10.11.27.101,
  dest_port: 49186 (port=(uint16)),
  vlan: null ([uint16]),
  proto: "TCP",
  app_proto: "tls",
  alert: {
    severity: 1 (uint16),
    signature: "ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)",
    category: "Domain Observed Used for C2 Detected",
    action: "allowed",
```