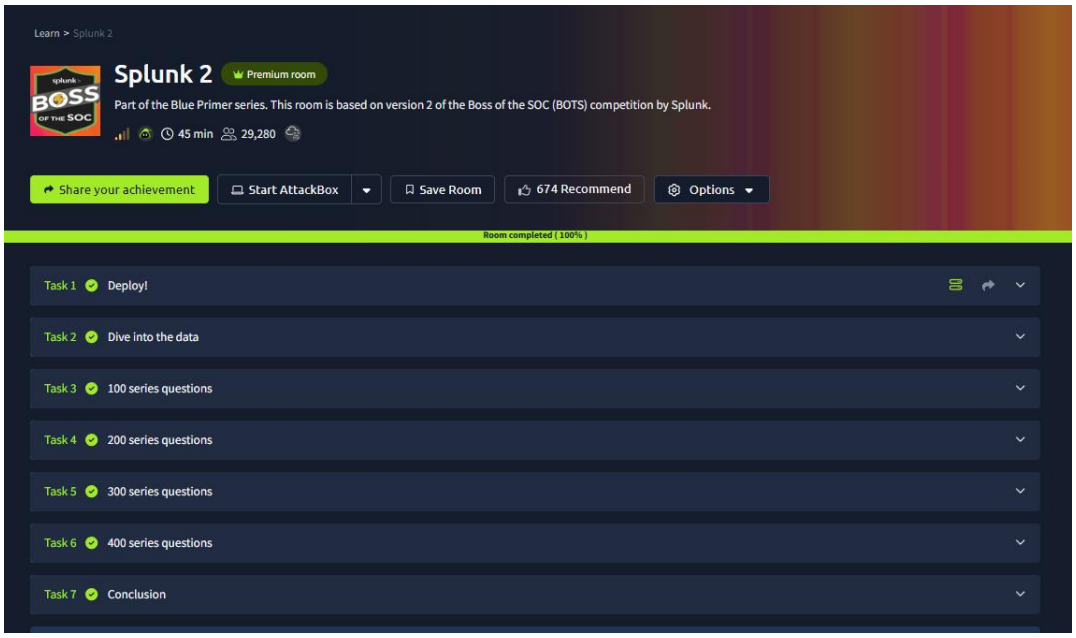
Splunk 2

Platform: tryhackme

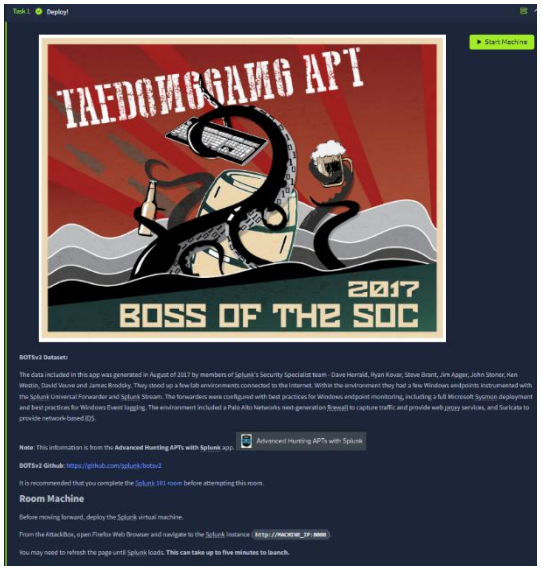
Frome: Asem Reda

Diploma: Cybersecurity 87

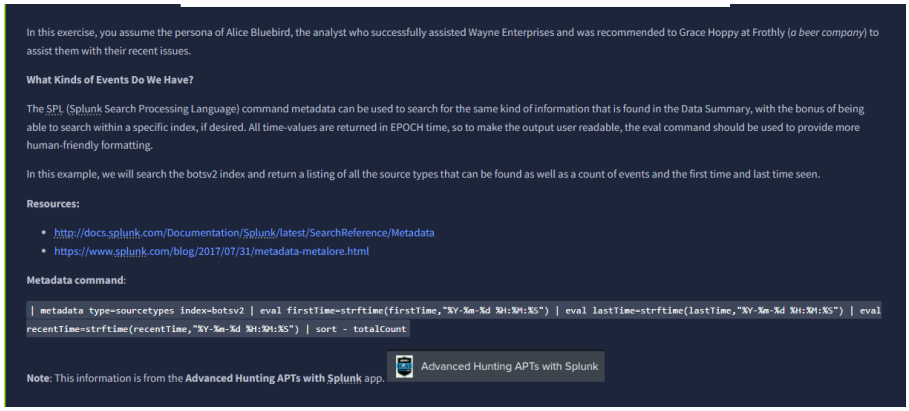
Challenge link: https://tryhackme.com/room/splunk2gcd5



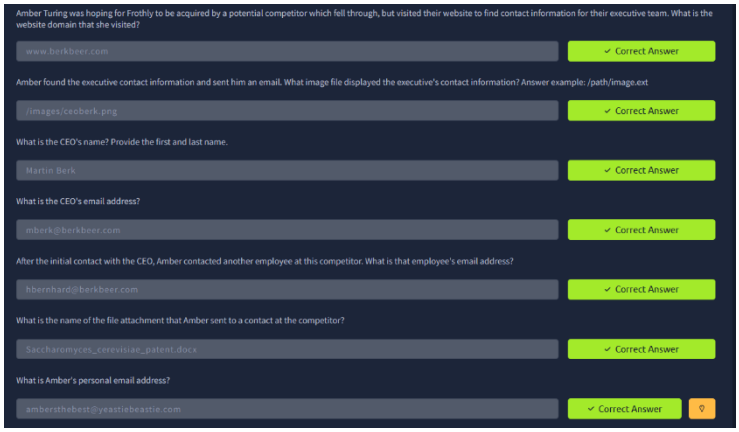
Task 1: Deploy!



Task 2: Dive into the data



Task 3: 100 series questions

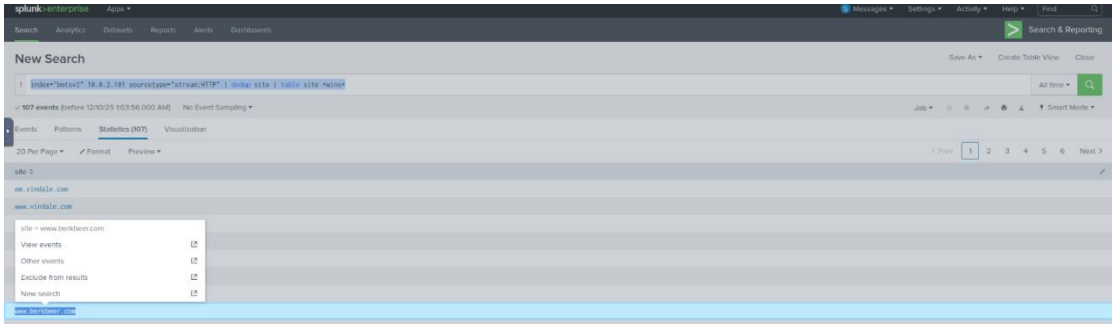


Solution method:

First, we need to get Amber's IP address. We'll do this by using the filter `ndex="botsv2" amber index="botsv2" sourcetype="pan:traffic"`, then going to the `src_ip` list. We'll find it there, and it's 10.0.2.101 , When you scroll down to the sender_email field, you will find her email address, which is aturing@froth.ly

First question:

We will use the filter [index="botsv2" 10.0.2.101 sourcetype="stream:HTTP" | dedup site | table site *wine*] to display the name of the site visited

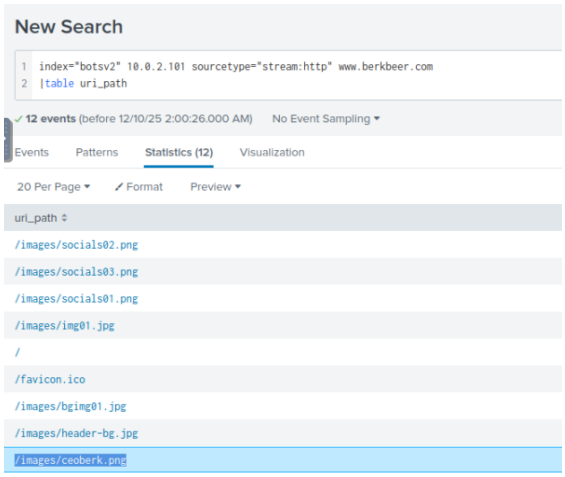


Second question:

We will use this filter to find the image file [index="botsv2" 10.0.2.101 sourcetype="stream:http" www.berkbeer.com

|table uri_path]

We will find it is /images/ceoberk.png because this is what belongs to ceo

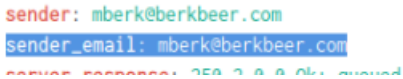


Third question:

We will use this filter to find the CEO's email address: index="botsv2" sourcetype="stream:smtp" berkbeer.com aturing@froth.ly. We will scroll down to sender_email and find it is mberk@berkbeer.com. Therefore, the CEO's name is Martin Berk

Fourth question:

Using the same steps, we will find the CEO's email address , **mberk@berkbeer.com**



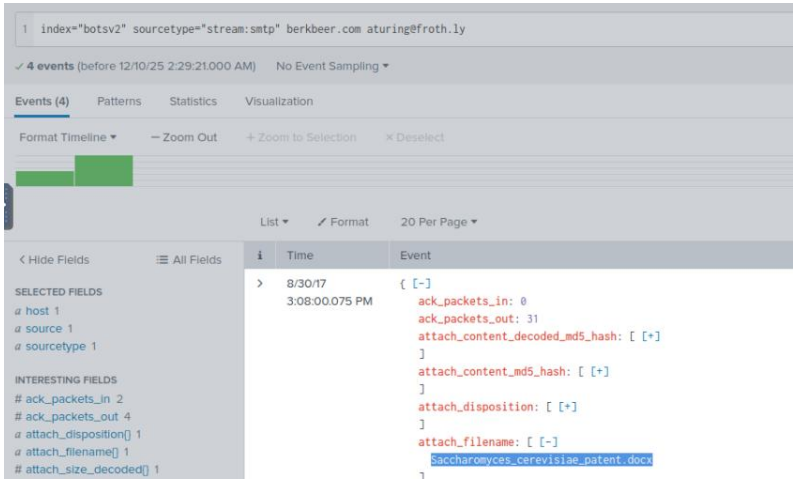
Fifth question:

Using the same filter as the previous question, we will go down to receiver_email and find that the email address is hbernhard@berkbeer.com

```
]
receiver_email: [ [-]
  hbernhard@berkbeer.com
]
```

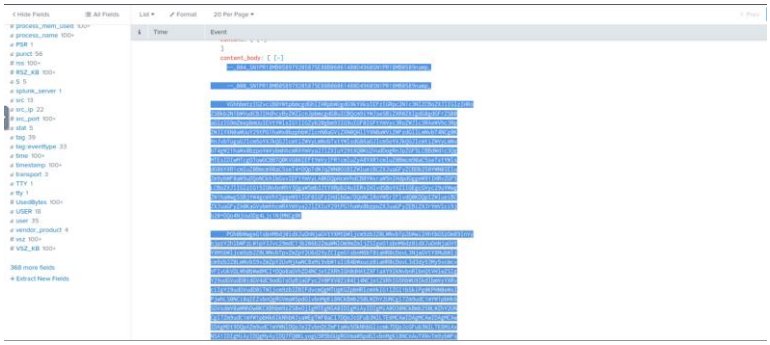
Sixth question:

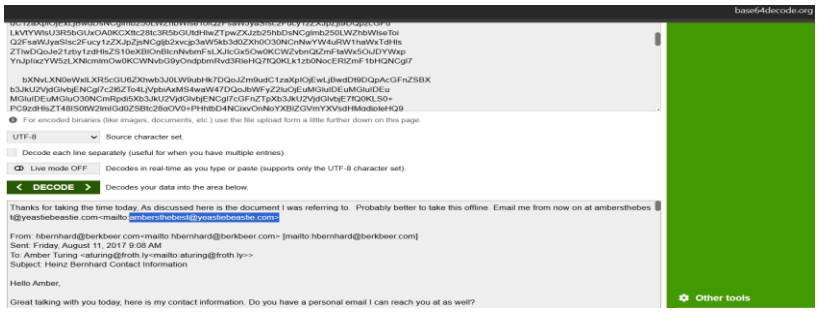
Using the same filter as the previous question, we will go to attach_disposition and find that the filename is Saccharomyces_cerevisiae_patent.docx



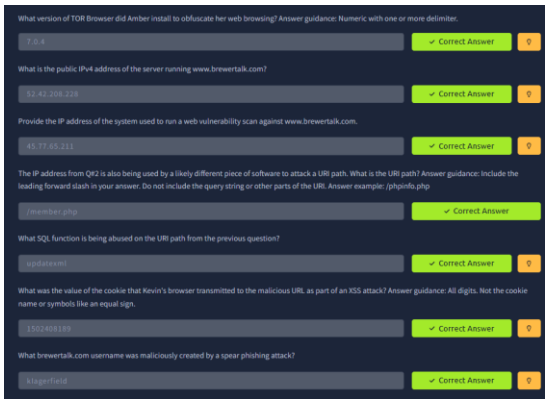
Seventh question:

We will use the filter index="botsv2" amber, then scroll down to content_body, then take the base64 hash and go to a website to decode it, for example, https://www.base64decode.org/, then the email will appear



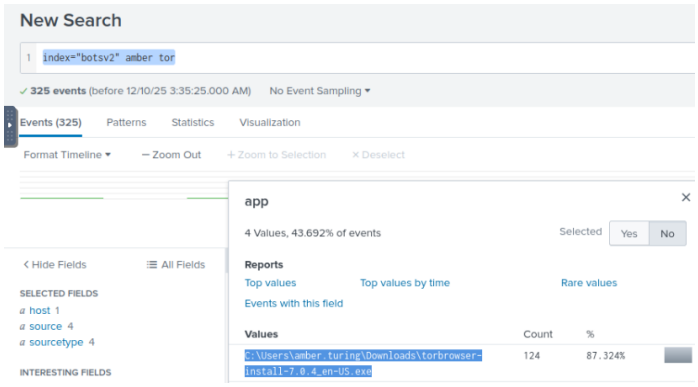


Task 4: 200 series questions



First question:

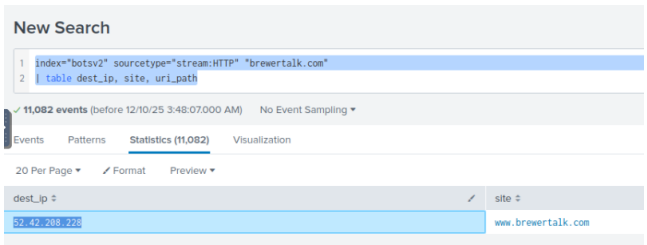
We will use the filter index="botsv2" amber tor, then we will go to the app field in Interesting Fields. We will find the version number, which is 7.0.4



Second question:

We will use the filter **index="botsv2" sourcetype="stream:HTTP" "brewertalk.com**

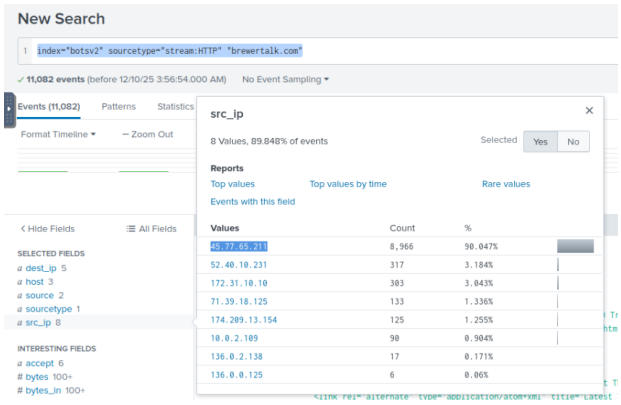
|table dest_ip, site, uri_path to find the IP address, and it will be the first one: **52.42.208.228**



Third question:

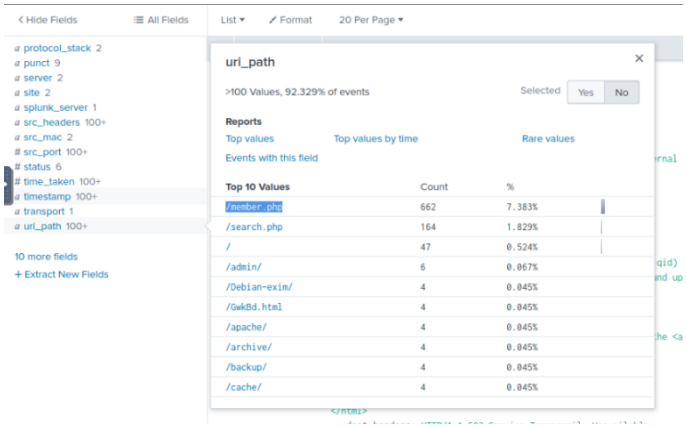
We will use the filter index="botsv2" sourcetype="stream:HTTP" "brewertalk.com"

Then we will go to Selected Fields and open src_ip. We will find that the IP address is 45.77.65.211



Fourth question:

We will use the filter index="botsv2" sourcetype="stream:HTTP" 45.77.65.211. Then we go to the Interesting Fields list and scroll down to uri_path. We will find that **/member.php**



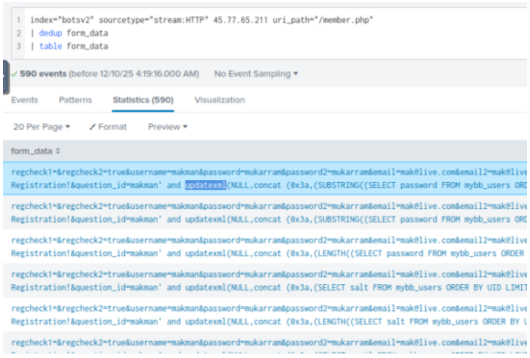
Fifth question:

We will use the filter index="botsv2" sourcetype="stream:HTTP" 45.77.65.211 "uri_path="/member.php

|dedup form_data

|table form_data

And we will find that the SQL function being abused on the URI path is **updatexml**



Sixth question:

We will use the filter index="botsv2" Kevin /member.php

|dedup cookie

|table cookie

Then we will find the

value of the cookie

which will be: 1502408189

Seventh question:

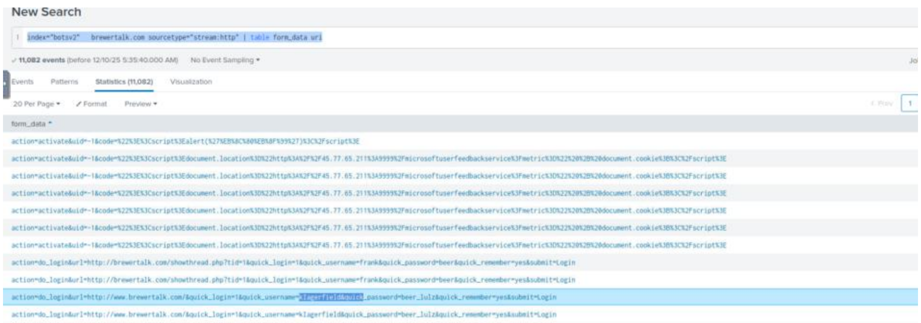
We will use the filter index="botsv2" brewertalk.com sourcetype="stream:http" | table form_data uri

Then we will search for the username and find it is klagerfield

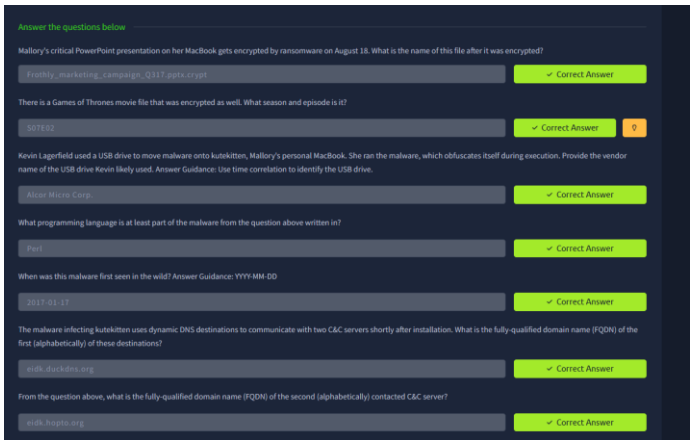
Why did we use `form_data`? Because the username only appears in

`form_data`

Because creating a new user is done through a registration form



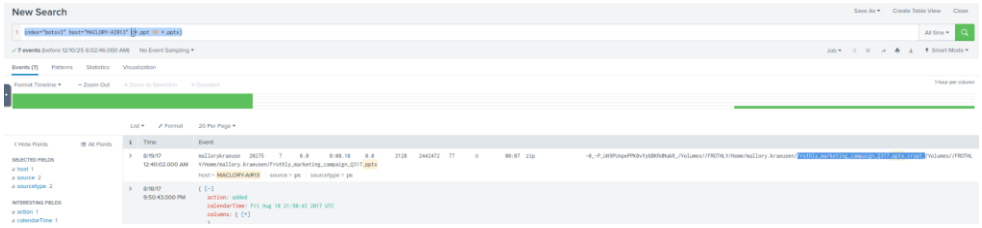
Task 5: 300 series questions



First question:

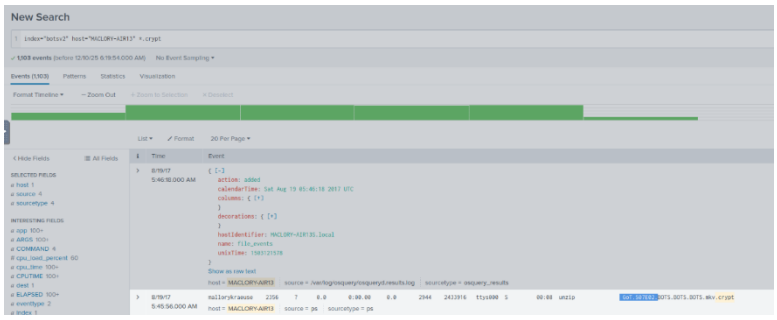
Initially, we will use the filter index="botsv2" host="MACLORY-AIR13" (*.ppt OR *.pptx)

Then, the name of the critical presentation file will appear on the first line.
_Frothly_marketing_campaign_Q317.pptx.crypt



Second question:

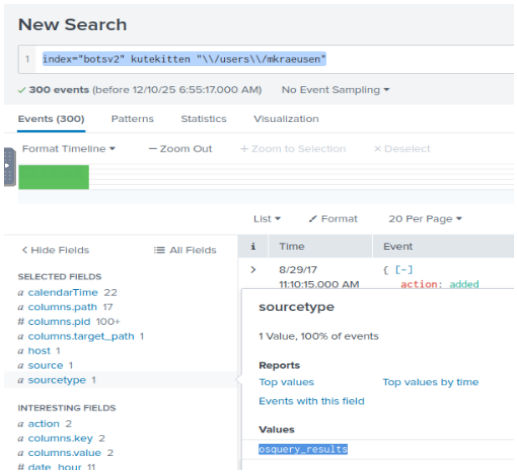
First, we'll use the filter index="botsv2" host="MACLORY-AIR13" *.crypt. Then we'll see the season and episode, which will be S07E02



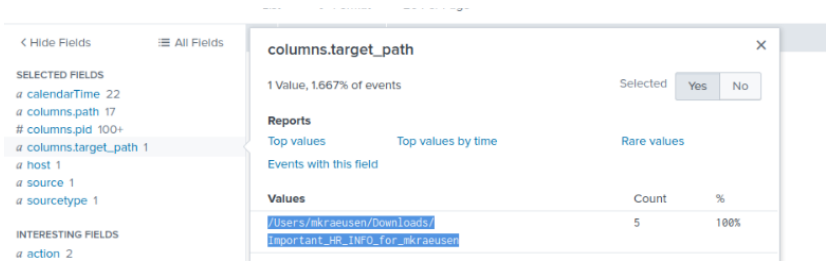
Third question:

First, we'll use the filter index="botsv2" kutekitten "\\/users\\/mkraeusen", then go to Selected Fields and choose sourcetype

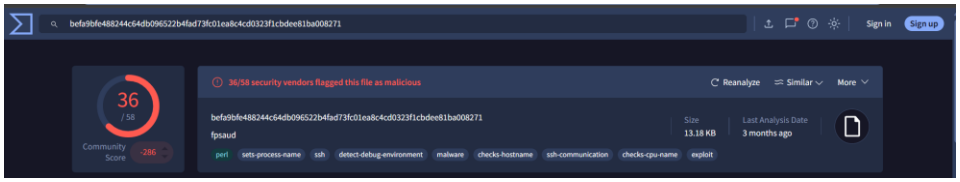
then osquery_results



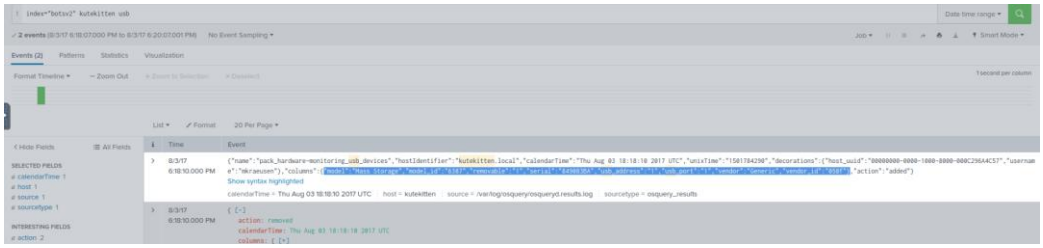
Then we go to columns.target_path and select the first option

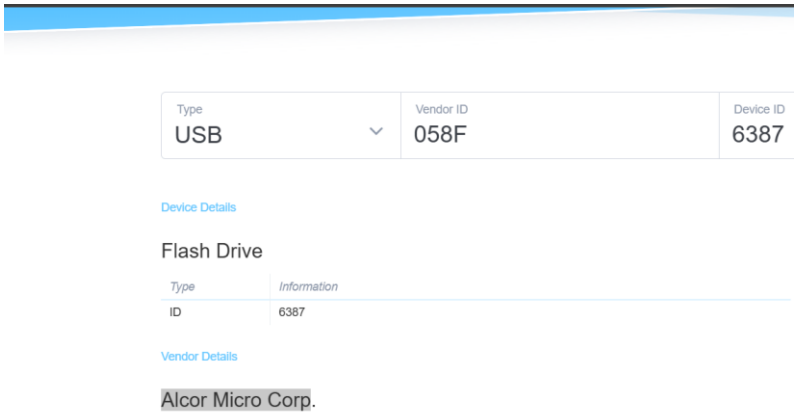


Then we go down to the last event, take the hash, and go to VirusTotal to verify it



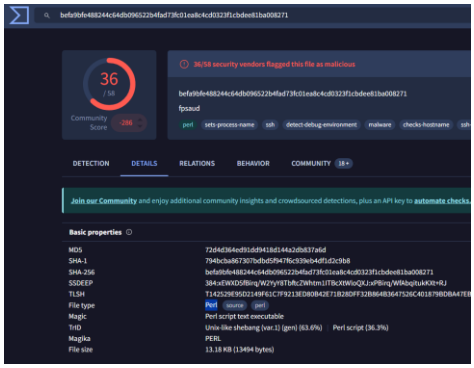
First, we'll change the event time to the last minute. Then, we'll use the keyword "usb". Next, we'll take "model_id":"6387" and "vendor_id":"058f" and go to the DeviceHunt website to retrieve the USB name





Fourth question:

Go back to VirusTotal, then go to Details, and you will find the answer. perl

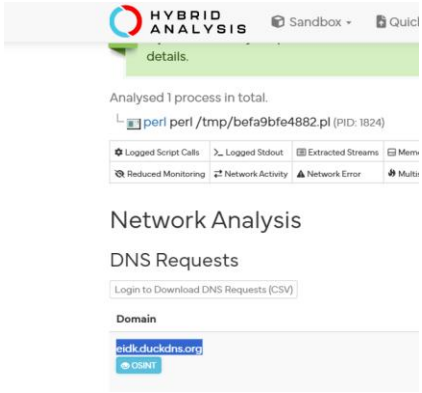


Fifth question:

You will find the answer in the same place as the previous question 2017-01-17

Sixth question:

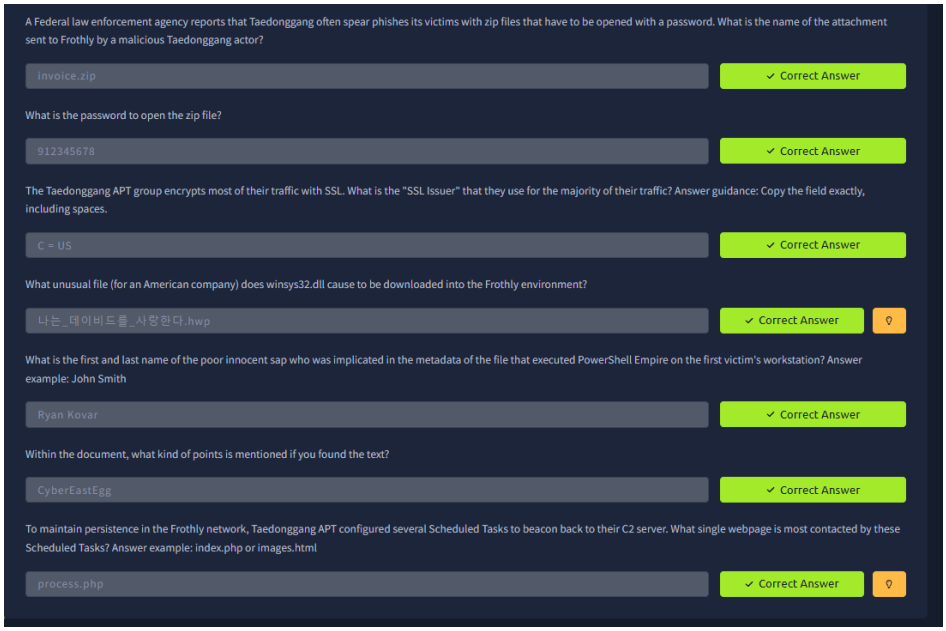
Go to the hybrid-analysis website. Then enter the hash and scroll down to Network Analysis. You will find the answer at eidk.duckdns.org



Seventh question:

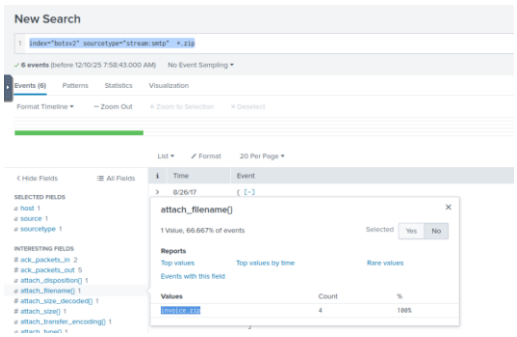
In the same way as the previous question, you will find the answer below: eidk.hopto.org

Task 6: 400 series questions



Question 1:

We will use the filter index="botsv2" sourcetype="stream:smtp" *.zip. Then we will go to the Selected Fields list, then to attach_filename{}, and then we will find the attachment name invoice.zip



Question 2:

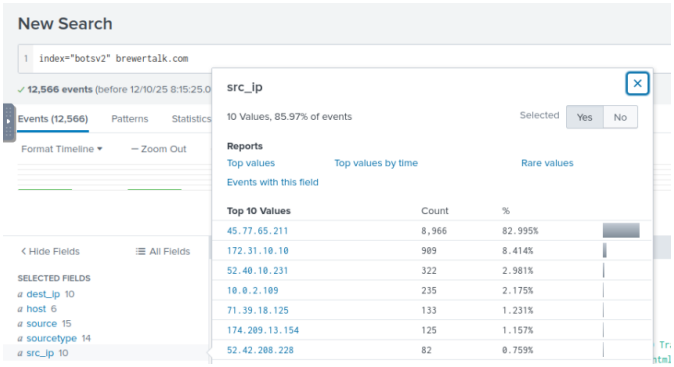
First, we'll use the filter index="botsv2" sourcetype="stream:smtp" *.zip ""attach_filename{}"="invoice.zip

Then, we'll click on "Show as raw text" at the end of the first event, and then we'll search for the password, which will be 912345678

Question 3:

First, we need to find the attacker's IP address. Remember, there was an IP address scanning brewertalk.com. We'll use the filter index="botsv2" brewertalk.com

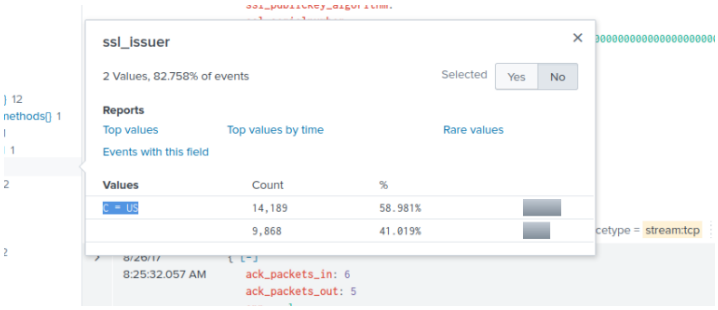
Then, we'll go to src_ip, and the IP address will be 45.77.65.211



Then we will use the filter index="botsv2" sourcetype="stream:tcp" 45.77.65.211

Then go down to ssl_issuer

After that you will find the answer C = US



Question 4:

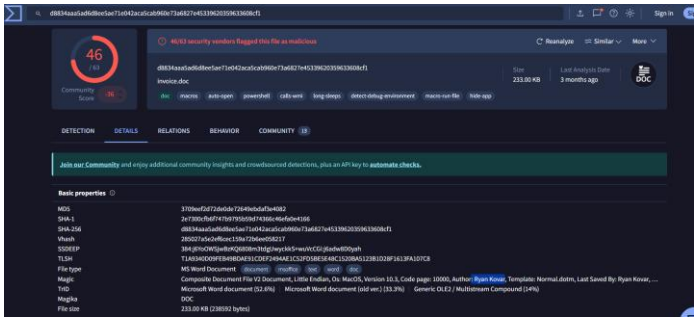
First, we'll use the filter index="botsv2" sourcetype="stream:ftp"

Then we'll go to method and then RETR to narrow down the search

After that, we'll go to filename and then find the unusual filename

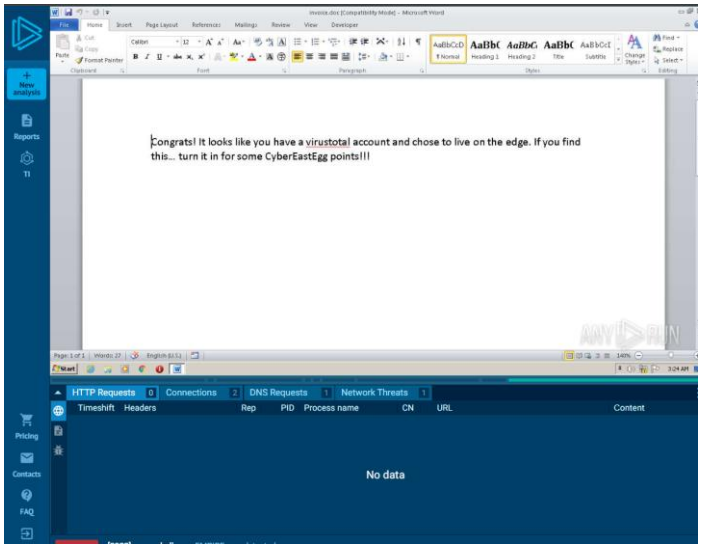
Question 5:

Using the hash of the malicious file, we will access the VirusTotal website and find the answer, which is Ryan Kovar



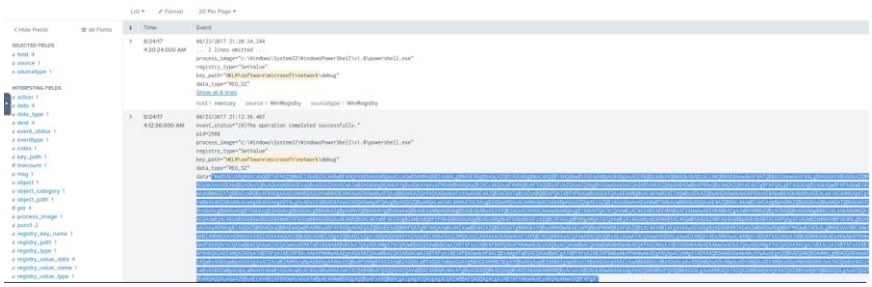
Question 6:

Go to app.any.run and you will find the answer CyberEastEgg



Question 7:

We will use the filter index="botsv2" HKLM\\Software\\Microsoft\\Network. Then we will go down to any event and look at the data. We will see that it is in base64 format. We will go to decompile it, and after that, the output will appear as process.php



Task 7: Conclusion