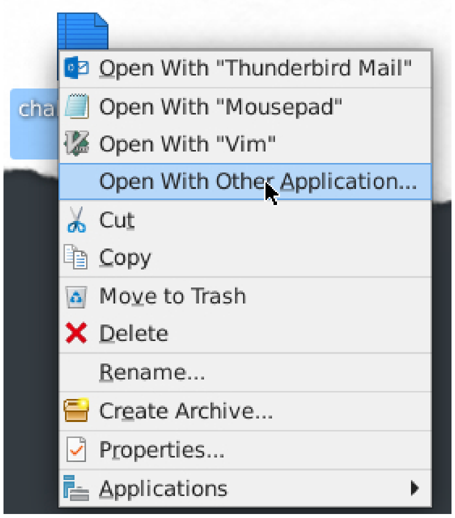
Phishing 5 Writeup

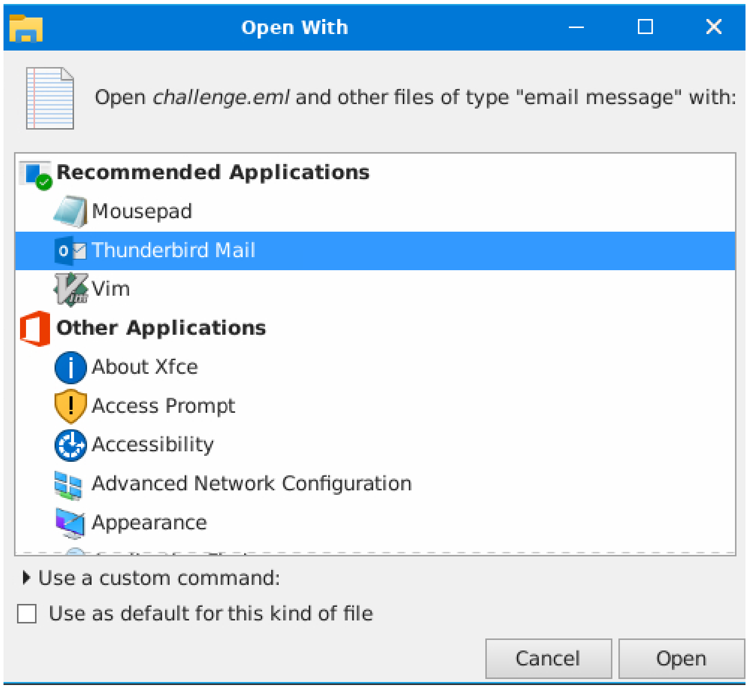
HCRYPT

2/5/22

Instructions say to Open in Thunderbird. I right clicked the file and clicked “Open With Other Application”

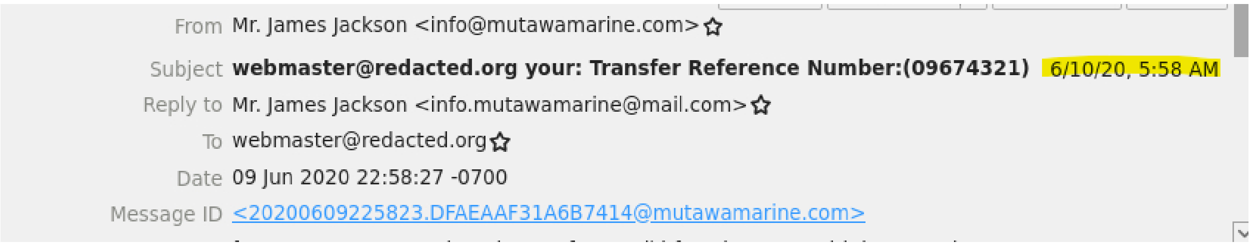


I then scrolled through the list and picked Thunderbird Mail



Open *challenge.eml* and other files of type "email message" with:

Q1: What is the email's timestamp? (answer format: **mm/dd/yy hh:mm)**



From Mr. James Jackson <info@mutawamarine.com>

Subject **webmaster@redacted.org your: Transfer Reference Number:(09674321)** 6/10/20, 5:58 AM

Reply to Mr. James Jackson <info.mutawamarine@mail.com>

To webmaster@redacted.org

Date 09 Jun 2020 22:58:27 -0700

Message ID <20200609225823.DFAEAAF31A6B7414@mutawamarine.com>

Q2: Who is the email from?

Enter the name from the From field.

Q3: What is his email address?

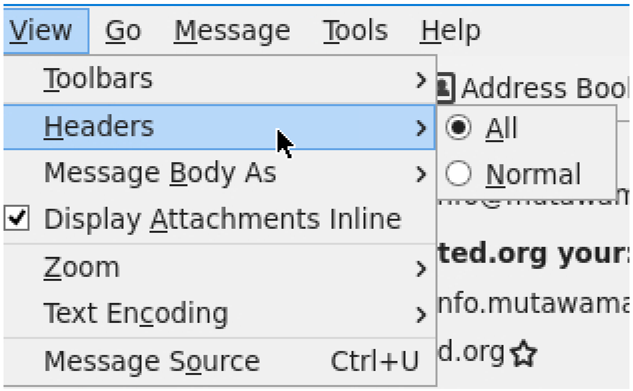
Enter the email address from the From field.

Q4: What email address will receive a reply to this email?

Enter email address from Reply To field.

Q5: What is the Originating IP?

Click View, Headers, All to see full headers



Scroll to bottom Received From. Headers are typically read from bottom to top.

Q6: Who is the owner of the Originating IP? (Do not include the "." in your answer.)

Go to https://arin.net and search the IP address. This is a US based IP. Enter the legal company name.

Q7: What is the SPF record for the Return-Path domain?

My preference is https://mxtoolbox.com but there are other websites that provide SPF information. https://centralops.net is great for DNS WHOIS and has the SPF record. https://Internet.nl is also good for profiling domains and websites.

Q8: What is the DMARC record for the Return-Path domain?

Tool of choice: https://dmarcian.com/dmarc-inspector/ www.intranet.nl also has it.

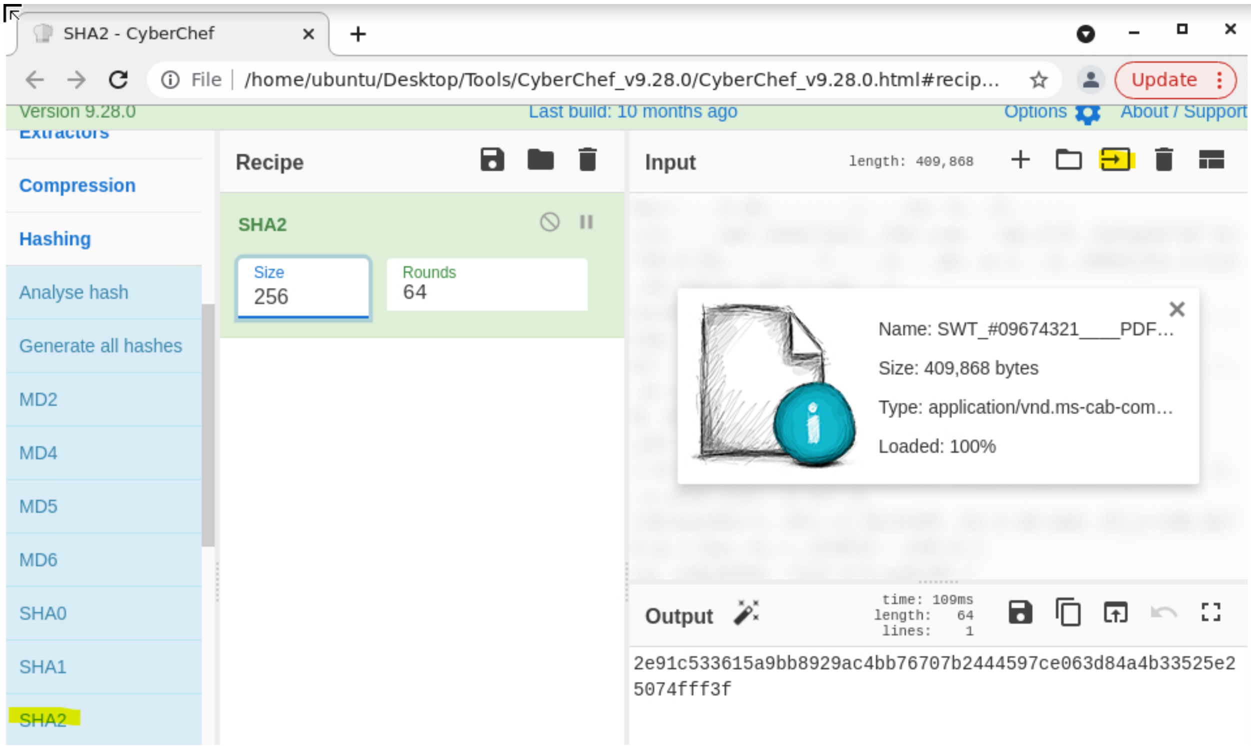
Q9: What is the name of the attachment?

Transcribe it from the bottom of the email or copy it from the text based version of the email. Copying might be better because it is hard to judge the number of attachments.

Q10: What is the SHA256 hash of the file attachment?

Bunch of ways to do this. Ideally, the file won't be saved on the local machine and task will be run from a hardened machine. In this case, open the browser and go to CyberChef.

Upload the file on the top right box. (Mouse-over text says "Open file as input.") Click Hashing on the left and click SHA2. Make sure to change the size. You can also search for SHA2.



/home/ubuntu/Desktop/Tools/CyberChef_v9.28.0/CyberChef_v9.28.0.html#recip...

SHA2

Size 256

Rounds 64

length: 409,868

Name: SWT_#09674321____PDF...

Size: 409,868 bytes

Type: application/vnd.ms-cab-com...

Loaded: 100%

```
time: 109ms
length:    64
 lines:     1
```

```
2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e2
5074fff3f
```

Q11: What is the attachments file size? (Don't forget to add "KB" to your answer, **NUM KB**)

Hint says to obtain hash and use open source resource. I used VirusTotal. Make sure to copy hash from CyberChef rather than previous THM answer. The displayed answer may be truncated.

Q12: What is the actual file extension of the attachment?

Clear the recipe in CyberChef and search for "Detect File Type."