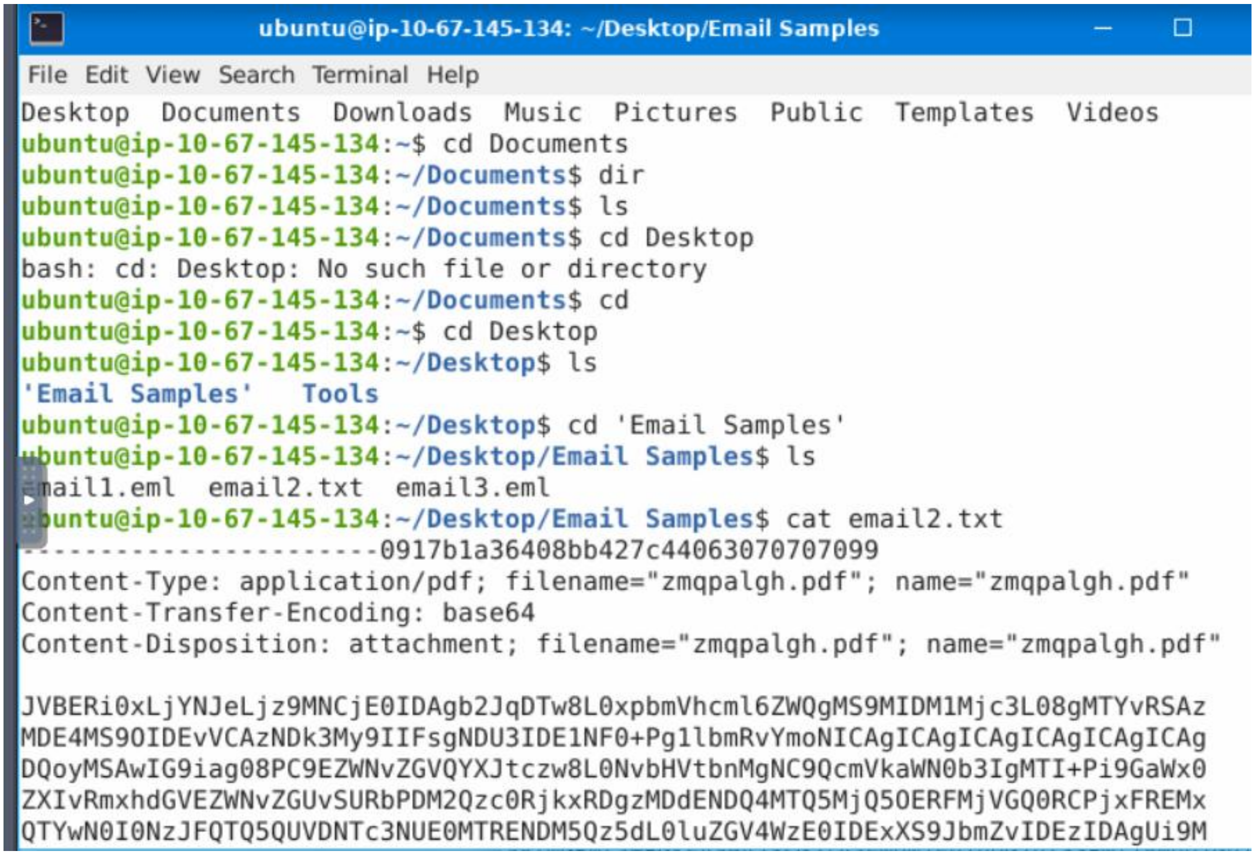
Phishing Analysis Fundamentals 2026/01/11

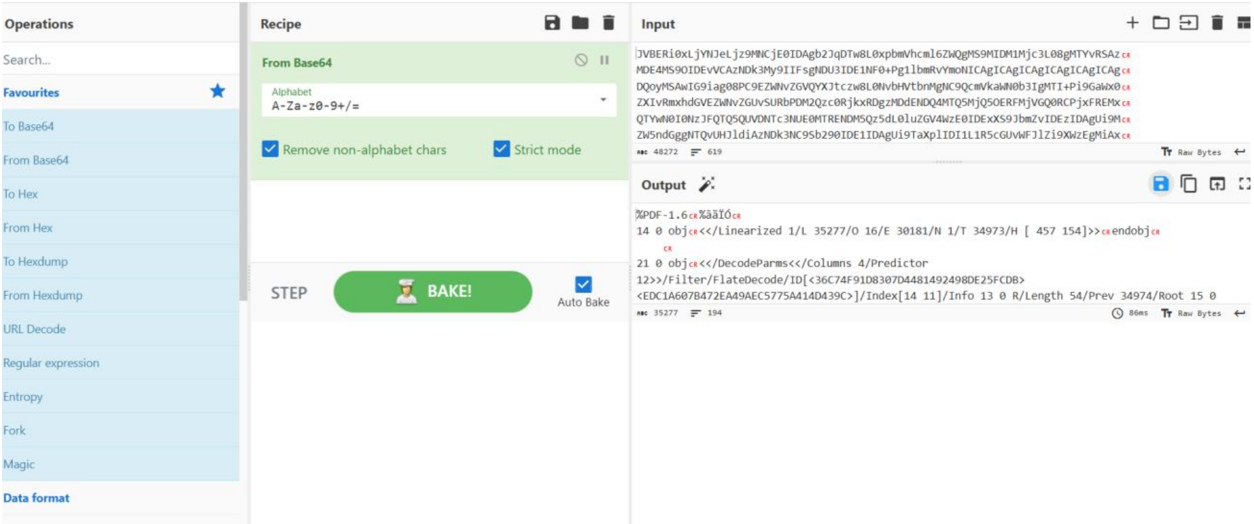
Scenario 1: In the attached virtual machine, view the information in email2.txt and reconstruct the PDF using the base64 data. What is the text within the PDF?


ubuntu@ip-10-67-145-134: ~/Desktop/Email Samples
File Edit View Search Terminal Help

```
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
ubuntu@ip-10-67-145-134:~$ cd Documents
ubuntu@ip-10-67-145-134:~/Documents$ dir
ubuntu@ip-10-67-145-134:~/Documents$ ls
ubuntu@ip-10-67-145-134:~/Documents$ cd Desktop
bash: cd: Desktop: No such file or directory
ubuntu@ip-10-67-145-134:~/Documents$ cd
ubuntu@ip-10-67-145-134:~$ cd Desktop
ubuntu@ip-10-67-145-134:~/Desktop$ ls
'Email Samples'   Tools
ubuntu@ip-10-67-145-134:~/Desktop$ cd 'Email Samples'
ubuntu@ip-10-67-145-134:~/Desktop/Email Samples$ ls
email1.eml  email2.txt  email3.eml
ubuntu@ip-10-67-145-134:~/Desktop/Email Samples$ cat email2.txt
-----------------------0917b1a36408bb427c44063070707099
Content-Type: application/pdf; filename="zmqpalgh.pdf"; name="zmqpalgh.pdf"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="zmqpalgh.pdf"; name="zmqpalgh.pdf"

JVBERi0xLjYNJeLjz9MNCjE0IDAgb2JqDTw8L0xpbmVhcml6ZWQgMS9MIDM1Mjc3L08gMTYvRSAz
MDE4MS9OIDEvVCAzNDk3My9IIFsgNDU3IDE1NF0+Pg1lbmRvYmoNICAgICAgICAgICAgICAgICAg
DQoyMSAwIG9iag08PC9EZWNvZGVQYXJtczw8L0NvbHVtbnMgNC9QcmVkaWN0b3IgMTI+Pi9GaWx0
ZXIvRmxhdGVEZWNvZGUvSURbPDM2Qzc0RjkxRDgzMDdEND Q4MTQ5MjQ5OERFMjVGQ0RCPjxFREMx
QTYwN0I0NzJFQTQ5QUVDNTc3NUE0MTRENDM5Qz5dL0luZGV4WzE0IDExXS9JbmZvIDEzIDAgUi9M
```

I opened up the terminal. Moved through the directories and opened the file in the relevant directory then went on to finding the hash.



From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars ☑ Strict mode

☑ Auto Bake

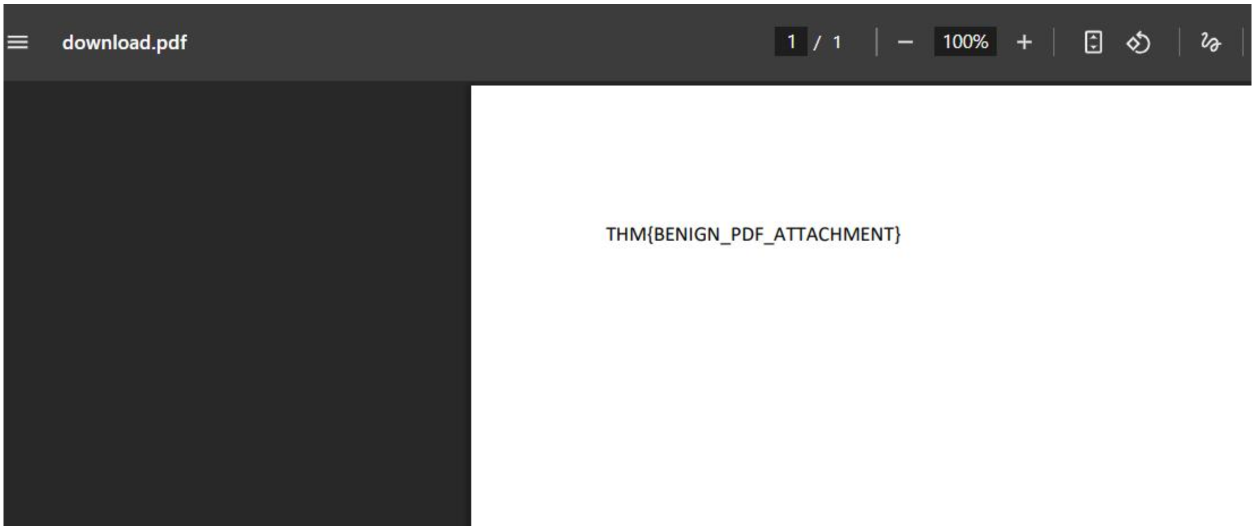
JVBERi0xLjYNJeLjz9MNCjE0IDAgb2JqDTw8L0xpbmVhcml6ZWQgMS9MIDM1Mjc3L08gMTYvRSAz␍
MDE4MS9OIDEvVCAzNDk3My9IIFsgNDU3IDE1NF0+Pg1lbmRvYmoNICAgICAgICAgICAgICAgICAg␍
DQoyMSAwIG9iag08PC9EZWNvZGVQYXJtczw8L0NvbHVtbnMgNC9QcmVkaWN0b3IgMTI+Pi9GaWx0␍
ZXIvRmxhdGVEZWNvZGUvSURbPDM2Qzc0RjkxRDgzMDdENDQ4MTQ5MjQ5OERFMjVGQ0RCPjxFREMx␍
QTYwN0I0NzJFQTQ5QUVDNTc3NUE0MTRENDM5Qz5dL0luZGV4WzE0IDExXS9JbmZvIDEzIDAgUi9M␍
ZW5ndGggNTQvUHJldiAzNDk3NC9Sb290IDE1IDAgUi9TaXplIDI1L1R5cGUvWFJlZi9XWzEgMiAx␍

48272 619

```
%PDF-1.6␍%âãÏÓ␍
14 0 obj␍<</Linearized 1/L 35277/O 16/E 30181/N 1/T 34973/H [ 457 154]>>␍endobj␍
    ␍
21 0 obj␍<</DecodeParms<</Columns 4/Predictor
12>>/Filter/FlateDecode/ID[<36C74F91D8307D4481492498DE25FCDB>
<EDC1A607B472EA49AEC5775A414D439C>]/Index[14 11]/Info 13 0 R/Length 54/Prev 34974/Root 15 0
```

35277 194 86ms

I then copied the hash only from the file, opened up **Cyberchef** and pasted it in the input section. Looked through the operations on the left side to find the **From Base64** operation and used it as the recipe and clicked bake. I then looked at the output and clicked on the download file as pdf.



THM{BENIGN_PDF_ATTACHMENT}

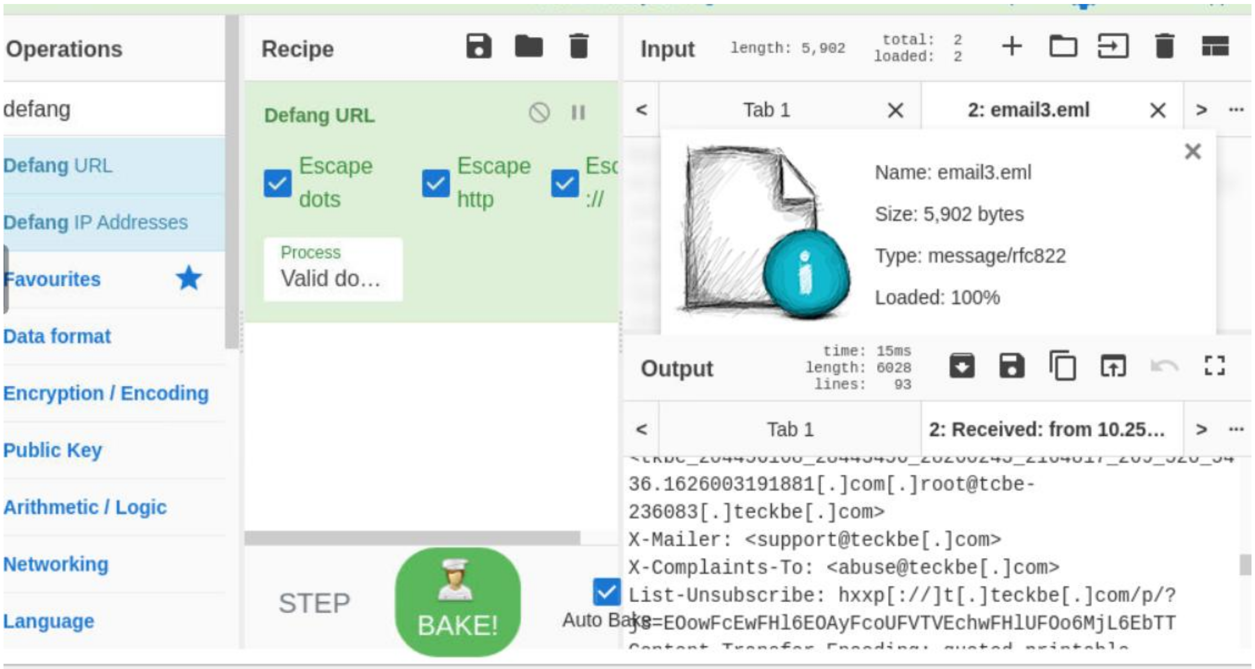
I opened up the downloaded file and managed to get the flag.

Scenario 2: Hyperlinks and IP addresses should be 'defanged'. Defanging is a way of making the URL/domain or email address unclickable to avoid accidental clicks, which may result in a serious security breach. It replaces special characters, like "@" in the email or "." in the URL, with different characters. For example, a highly suspicious domain, http://www.suspiciousdomain.com, will be changed to hxxp[://]www[.]suspiciousdomain[.]com before forwarding it to the SOC team for detection. CyberChef is a great tool that can help you with defanging, try it out for the following questions!

Analyze the email titled email3.eml within the virtual machine and answer the questions below.

Note: Alexa is the victim, and Billy is the analyst assigned to the case. Alexa forwarded the email to Billy for analysis.

Step 1: What is the website for the - CLICK HERE URL in a defanged format? (e.g. https://website.thm)



Defang URL

☑ Escape dots ☑ Escape http ☑ Esc ://

Process: Valid do…

Input length: 5,902 total: 2 loaded: 2

Name: email3.eml
Size: 5,902 bytes
Type: message/rfc822
Loaded: 100%

Output time: 15ms length: 6028 lines: 93

```
36.1626003191881[.]com[.]root@tcbe-
236083[.]teckbe[.]com>
X-Mailer: <support@teckbe[.]com>
X-Complaints-To: <abuse@teckbe[.]com>
List-Unsubscribe: hxxp[://]t[.]teckbe[.]com/p/?
js=EOowFcEwFHl6EOAyFcoUFVTVEchwFHlUFOo6MjL6EbTT
```

For this, I opened up **Cyberchef** again and clicked input then navigated to the **email3.eml** file to be the file we work on. I then went on the left side to the operations and selected the **Defang**

URL operation and brought it the ‘Recipe’ section and clicked ‘**BAKE!**’. I then scrolled through the output till I came across the defanged link - **hxxp[://]t[.]teckbe[.]com**.

Conclusion Summary

This exercise reinforced the core fundamentals of phishing analysis by simulating real-world SOC workflows. In Scenario 1, I successfully extracted and decoded Base64-encoded data from a phishing email to reconstruct a malicious PDF, demonstrating the ability to safely handle encoded attachments and validate their contents without direct execution. Using tools such as the Linux terminal and CyberChef, I was able to identify the hidden message within the document, highlighting the importance of decoding and file reconstruction techniques in email-based threat investigations.

Scenario 2 focused on the safe handling and analysis of malicious links through URL defanging. By analyzing a suspicious email and using CyberChef to defang embedded URLs, I ensured potentially harmful links were rendered non-clickable before being shared for further investigation. This scenario emphasized the importance of operational safety, accurate artifact handling, and proper communication when escalating phishing incidents within a SOC environment.

Overall, these scenarios strengthened my understanding of phishing analysis techniques, secure handling of malicious artifacts, and the practical use of industry-standard tools, aligning closely with real-world SOC analyst responsibilities.