TryHackMe: The Greenholt Phish

The following writeup covers the Greenholt Phish room on TryHackMe. It is part of the SOC level 1 path and involves analysing a malicious email. This room is aimed at beginners, and I recommend giving it a try even if you have no experience with email analysis.

Scenario: A Sales Executive at Grenholt PLC received an email that he didn't expect to receive from a customer. He claims that the customer never uses generic greeting such as "Good day" and didn't expect any amount of money to be transferred to his account. The email also contains an attachment that he never requested. He forwarded the email to the SOC department for further investigation.

What is the Transfer Reference Number listed in the email's Subject?

Once you have opened the challenge.eml file in Thunderbird, you can find the transfer reference number at the end of the subject line:

Who is the email from?

The from address can also be seen in the email header:

As the question is asking for the name and not the entire email address, the answer is Mr. James Jackson.

What is his email address?

Once again, if you inspect the email header (or the image above) you can see the email address. You can right click the 'From' line to save the email address.

What email address will receive a reply to this email?

This can be found in the 'Reply to' line:

As you can see, the reply address appears to be imitating Mr. James Jackson which is highly suspicious and likely indicates that Mr. Jacksons' legitimate email is being spoofed.

What is the Originating IP?

If you click 'More' and then view source in Thunderbird, you can inspect the raw email and see all the headers. If you scroll down, right before the main contents of the email, you can find the originating IP of the email:

```
 26Z1BWUDLQ-
X-Originating-IP: [x.x.x.x]
Received: from 10.197.41.148  (EHLO sub.redacted.com) (x.x.x.x)
  by mta4212.mail.bf1.yahoo.com with SMTP; Wed, 10 Jun 2020 05:58:54 +0000
Received: from hwsrv-737338.hostwindsdns.com ([192.119.71.157]:51810 helo=mutawa
    by sub.redacted.com with esmtp (Exim 4.80)
    (envelope-from <info@mutawamarine.com>)
    id 1jissD-0004g5-Ts
    for webmaster@redacted.org; Wed, 10 Jun 2020 01:02:04 -0400
Reply-To: "Mr. James Jackson" <info.mutawamarine@mail.com>
From: "Mr. James Jackson" <info@mutawamarine.com>
To: webmaster@redacted.org
Subject: webmaster@redacted.org your: Transfer Reference Number:(09674321)
Date: 09 Jun 2020 22:58:27 -0700
```

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

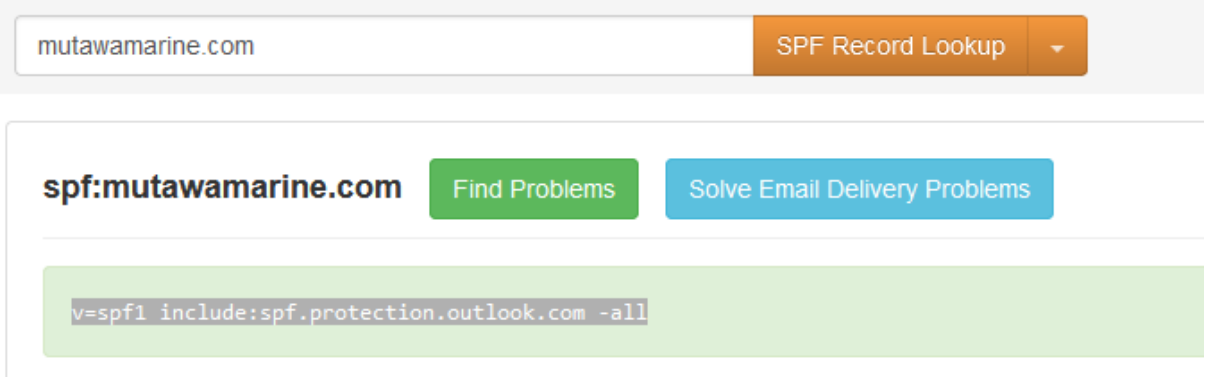
Unfortunately, the whois data has changed since whenever this room was name, the current organisation is not the correct answer.

```
NetRange:       192.119.64.0 - 192.119.127.255
CIDR:           192.119.64.0/18
NetName:        HOSTWINDS-18-2
NetHandle:      NET-192-119-64-0-1
Parent:         NET192 (NET-192-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS54290
Organization:   Hostwinds LLC. (HL-29)
RegDate:        2012-11-12
Updated:        2021-09-23
Comment:        https://www.hostwinds.com
Comment:        Abuse Contact: abuse@hostwinds.com
Ref:            https://rdap.arin.net/registry/ip/192.119.64.0
```

The answer is Hostwinds LLC.

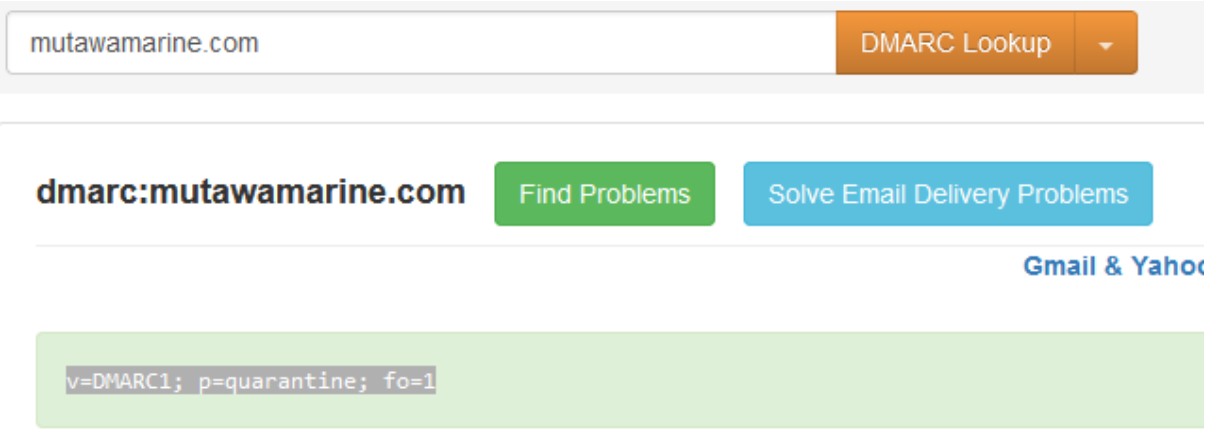
What is the SPF record for the Return-Path domain?

The return path domain is mutawamarine.com which you can find in the email header, using mxtoolbox and their SPF Record Lookup I was able to find their spf record:



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

Using the information from the previous question, along with the same tool, you can determine the DMARC record for the Return-Path domain:



What is the name of the attachment?

You can find the name of the attachment in the raw email source or through using Thunderbird:

```
------=_NextPart_000_0012_BDB07B06.81B59493
Content-Type: application/octet-stream; name="SWT_#09674321____PDF__.CAB"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="SWT_#09674321____PDF__.CAB"
```

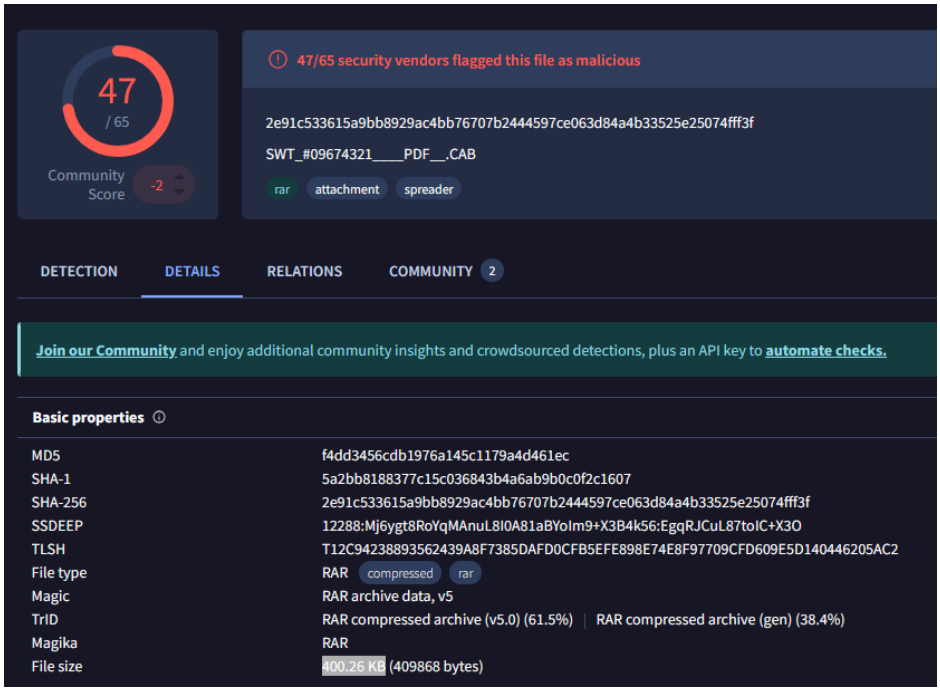
What is the SHA256 hash of the file attachment?

Once you have saved the attachment, navigate to the saved directory and enter the following command to get the SHA256 hash of the attachment:

```
ubuntu@ip-10-10-42-168:~/Desktop$ ls
SWT_#09674321____PDF__.CAB  Tools  challenge.eml
ubuntu@ip-10-10-42-168:~/Desktop$ sha256sum SWT_#09674321____PDF__.CAB
2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f  SWT_#09674321____PDF__.CAB
```

What is the attachments file size?

If you enter the SHA256 hash into VirusTotal and navigate to the details section, you can determine the file size of the attachment (400.26 KB):



What is the actual file extension of the attachment?

There would be several ways to go about answering this question, however, I just used the file command:

```
ubuntu@ip-10-10-42-168:~/Desktop$ file SWT_#09674321____PDF__.CAB
SWT_#09674321____PDF__.CAB: RAR archive data, v5
```

The Greenholt Phish was a wonderful learning experience for those (like myself) who are new to analysing phishing emails. Through completing all the tasks, I was able to learn a lot about fundamental email analysis. If you need any help with this room, feel free to reach out to me.