

Name: Ramya Ajay

Roll No: CB.EN.P2CYS22004

Greenholt Phish

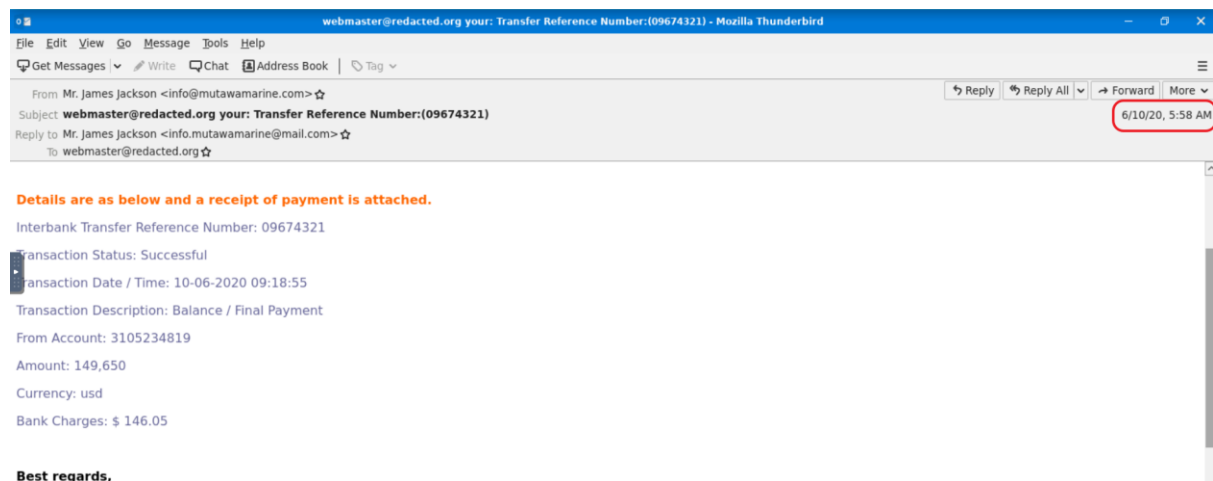
Task-2:

- First open the email with thunderbird

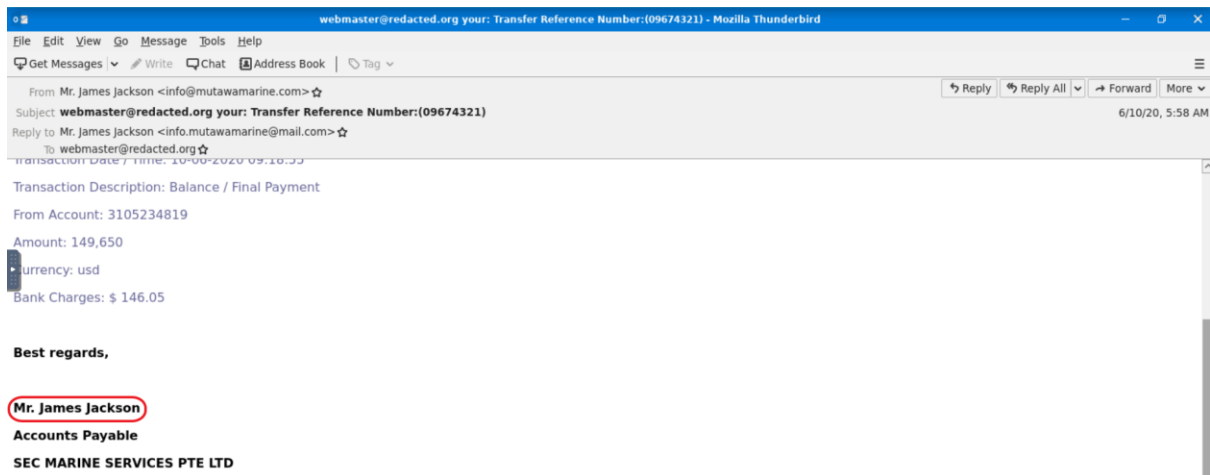
```
juntu@ip-10-10-59-13:~/Desktop$ ls
fools challenge.eml
juntu@ip-10-10-59-13:~/Desktop$ thunderbird challenge.eml

(thunderbird:1503): Gtk-WARNING **: 06:18:31.377: Theme parsing error: gtk-contained.css:305:58: Using one color stop with linear-gradient() is deprecated.
(thunderbird:1503): Gtk-WARNING **: 06:18:31.398: Theme parsing error: gtk-contained.css:312:58: Using one color stop with linear-gradient() is deprecated.
(thunderbird:1503): Gtk-WARNING **: 06:18:31.398: Theme parsing error: gtk-contained.css:331:58: Using one color stop with linear-gradient() is deprecated.
(thunderbird:1503): Gtk-WARNING **: 06:18:31.399: Theme parsing error: gtk-contained.css:338:67: Using one color stop with linear-gradient() is deprecated.
(thunderbird:1503): Gtk-WARNING **: 06:18:31.400: Theme parsing error: gtk-contained.css:658:68: Using one color stop with linear-gradient() is deprecated.
(thunderbird:1503): Gtk-WARNING **: 06:18:31.400: Theme parsing error: gtk-contained.css:666:69: Using one color stop with linear-gradient() is deprecated.
(thunderbird:1503): Gtk-WARNING **: 06:18:31.400: Theme parsing error: gtk-contained.css:688:62: Using one color stop with linear-gradient() is deprecated.
(thunderbird:1503): Gtk-WARNING **: 06:18:31.400: Theme parsing error: gtk-contained.css:696:71: Using one color stop with linear-gradient() is deprecated.
(thunderbird:1503): Gtk-WARNING **: 06:18:31.440: Theme parsing error: gtk-contained.css:1787:62: Using one color stop with linear-gradient() is deprecated.
(thunderbird:1503): Gtk-WARNING **: 06:18:31.440: Theme parsing error: gtk-contained.css:1794:71: Using one color stop with linear-gradient() is deprecated.
(thunderbird:1503): Gtk-WARNING **: 06:18:31.441: Theme parsing error: gtk-contained.css:1813:62: Using one color stop with linear-gradient() is deprecated.
(thunderbird:1503): Gtk-WARNING **: 06:18:31.441: Theme parsing error: gtk-contained.css:1820:71: Using one color stop with linear-gradient() is deprecated.
[calBackendLoader] Using Thunderbird's libical backend
(thunderbird:1503): dconf-CRITICAL **: 06:18:36.089: unable to create directory '/home//.cache/xdg/dconf': Permission denied. dconf will not work properly.
(thunderbird:1503): dconf-CRITICAL **: 06:18:36.089: unable to create directory '/home//.cache/xdg/dconf': Permission denied. dconf will not work properly.
(thunderbird:1503): dconf-CRITICAL **: 06:18:36.093: unable to create directory '/home//.cache/xdg/dconf': Permission denied. dconf will not work properly.
```

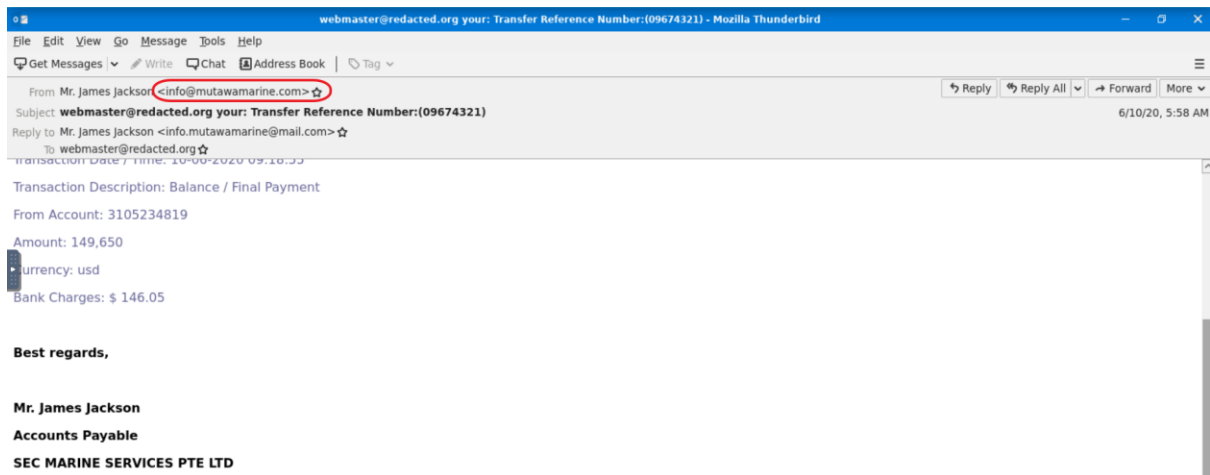
a) What is the email's timestamp? (answer format: mm/dd/yyyy hh:mm)



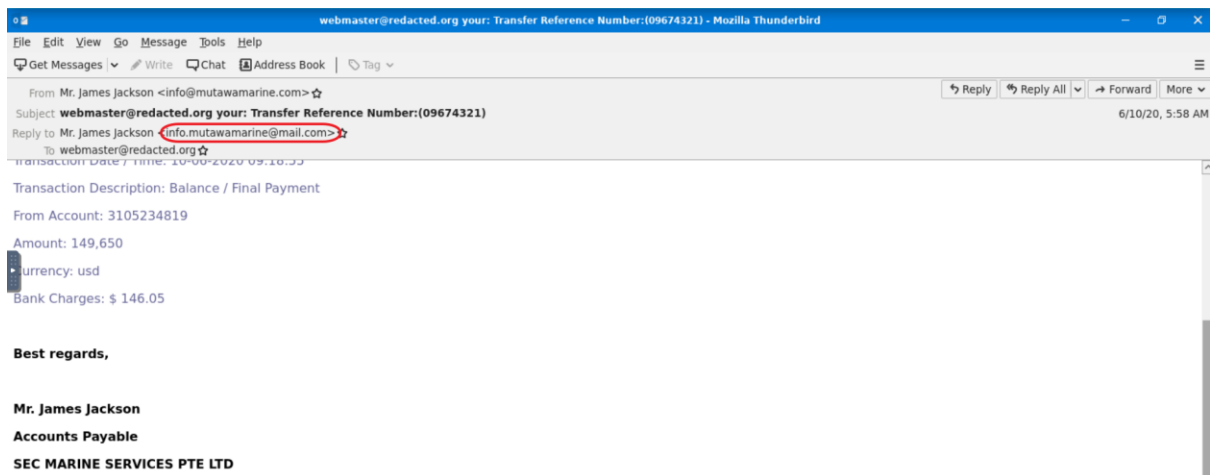
b) Who is the email from?



c) What is his email address?



d) What email address will receive a reply to this email?



e) What is the Originating IP?

```
ta4212.mail.bf1.yahoo.com with SMTP; Wed, 10 Jun 2020 05:58:54 +0000
red: 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
To: "Mr. James Jackson" <info.mutawamarine@mail.com>
"Mr. James Jackson" <info@mutawamarine.com>
bmaster@redacted.org
t: webmaster@redacted.org your: Transfer Reference Number:(09674321)
00 Jun 2020 03:58:37 0700
```

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

- First we go into the WHOIS lookup and enter the originating IP there

lookup.icann.org/en/lookup

العربية 简体中文 English Français Русский Español

ICANN | LOOKUP

Registration data lookup tool

Enter a domain name or an Internet number resource (IP Network or ASN) [Frequently Asked Questions \(FAQ\)](#)

192.119.71.157

Lookup

By submitting any personal data, I acknowledge and agree that the personal data submitted by me will be processed in accordance with the ICANN Privacy Policy and agree to abide by the website Terms of Service and

- Then we get the domain name as

Registrant:

Handle: HL-29

Name: Hostwinds LLC.

Whois Server: whois.arin.net

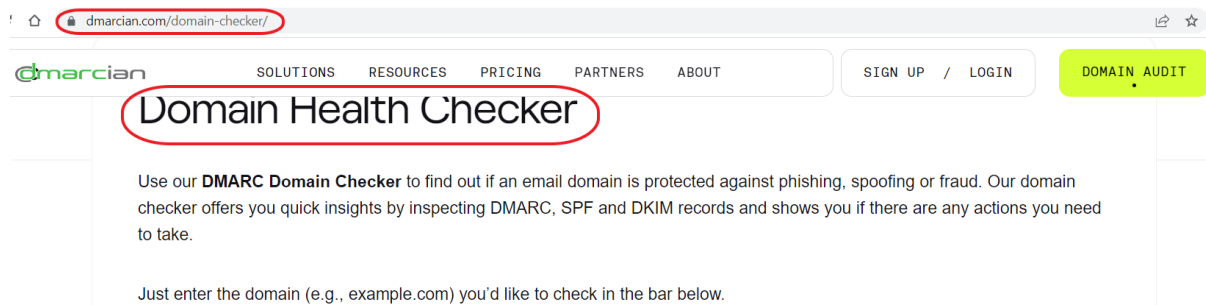
Kind: org

Mailing Address: 12101 Tukwila International Blvd, 3rd Floor, Suite 320, Seattle, WA, 98168, United States

Registration comments:
<https://www.hostwinds.com>
abuse contact: abuse@hostwinds.com

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

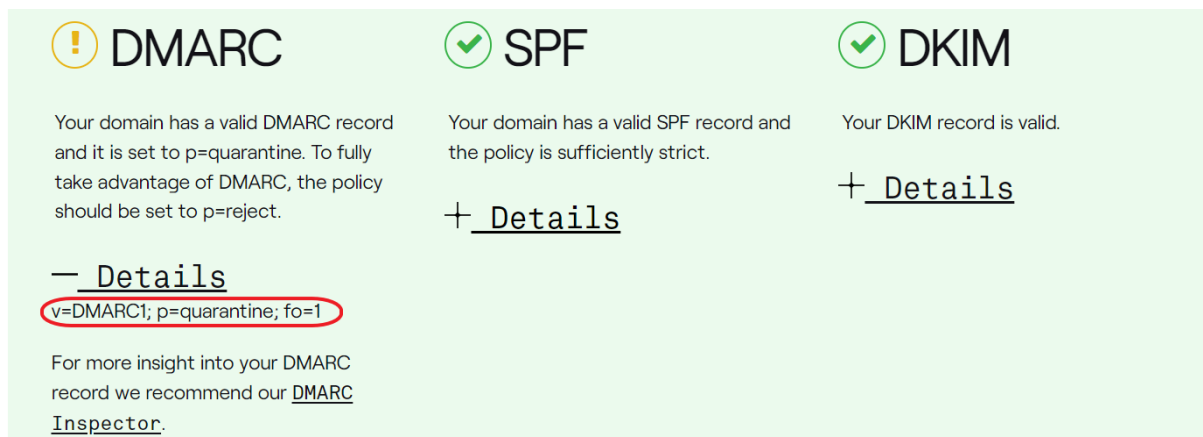
- First we go to a domain checker website



- We enter the domain name there

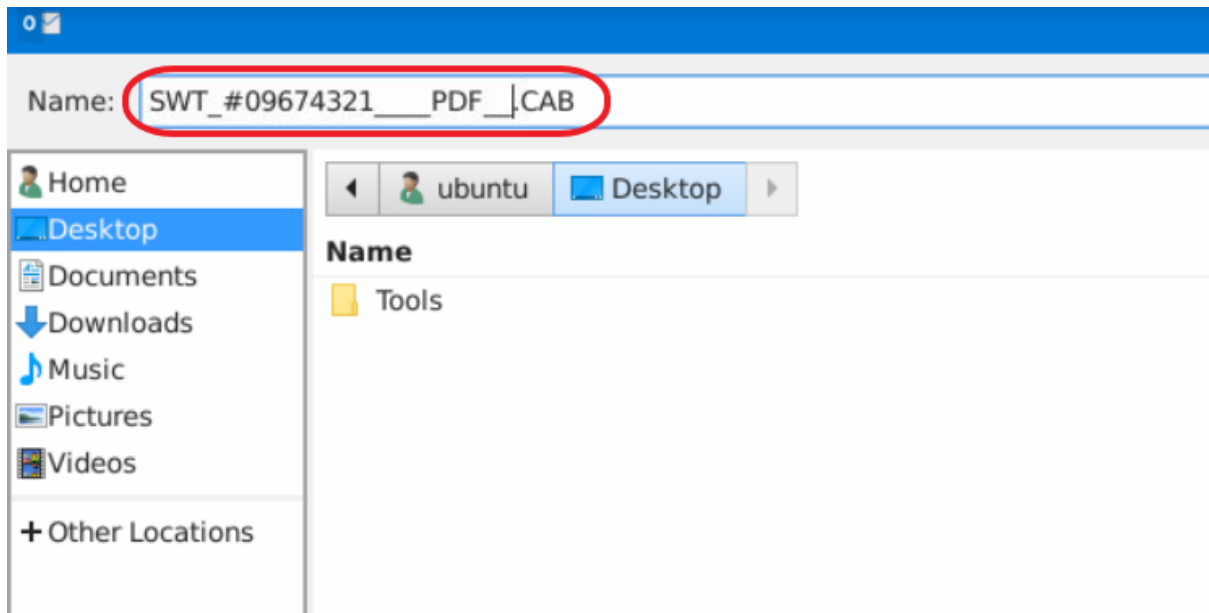


h) What is the DMARC record for the Return-Path domain?



i) What is the name of the attachment?

- Now we try to save the file to get the filename



j) What is the SHA256 hash of the file attachment?

```
webmaster@redacted.org your: Transfer Reference Number:(09
ubuntu@ip-10-10-173-172: ~/Desktop
File Edit View Search Terminal Help
ubuntu@ip-10-10-173-172:~/Desktop$ ls
SWT_#09674321__PDF__.CAB  Tools  challenge.eml
ubuntu@ip-10-10-173-172:~/Desktop$ sha256dump SWT_#09674321__PDF__.CAB
sha256dump: command not found
ubuntu@ip-10-10-173-172:~/Desktop$ sha256sum SWT_#09674321__PDF__.CAB
2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f SWT_#09674321__PDF__.CAB
ubuntu@ip-10-10-173-172:~/Desktop$
```

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

- 400.26 KiB

l) What is the actual file extension of the attachment?

- RAR