Name:Ramya Ajay

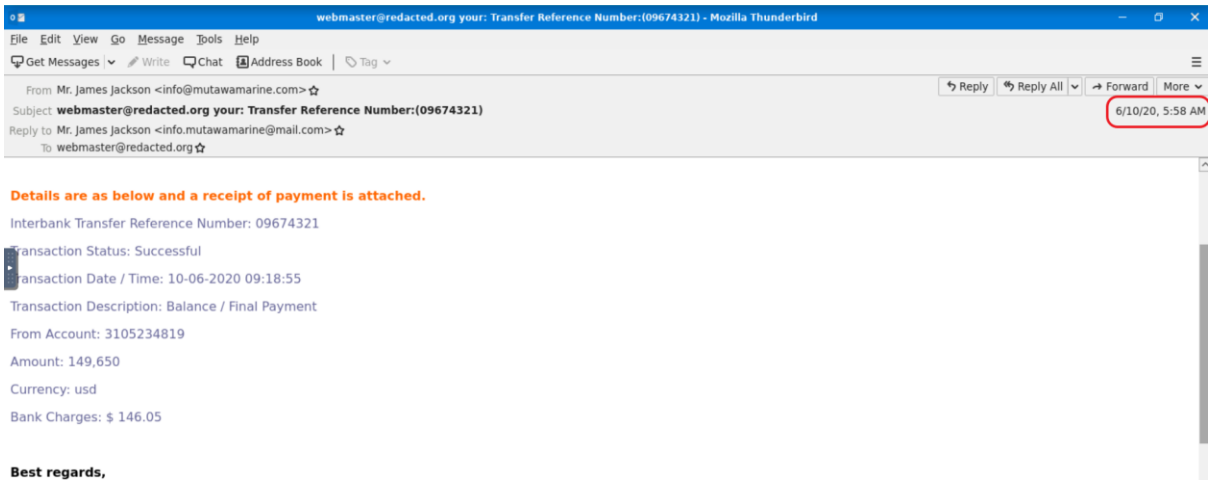
Roll No:CB.EN.P2CYS22004 Greenholt Phish

Task-2:

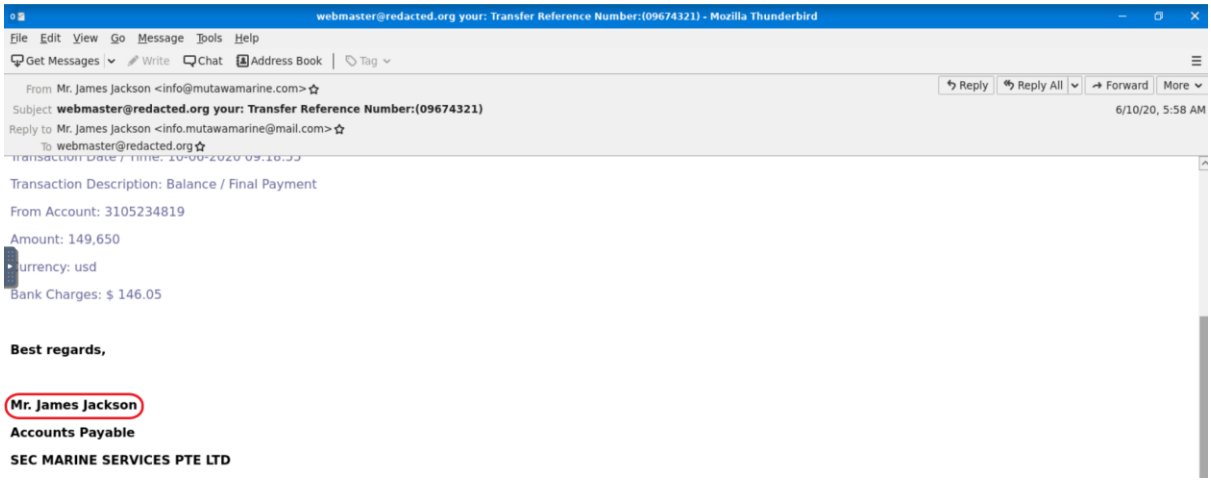
- First open the email with thunderbird

```
ubuntu@ip-10-10-59-13:~/Desktop$ ls
Tools  challenge.eml
ubuntu@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.
```

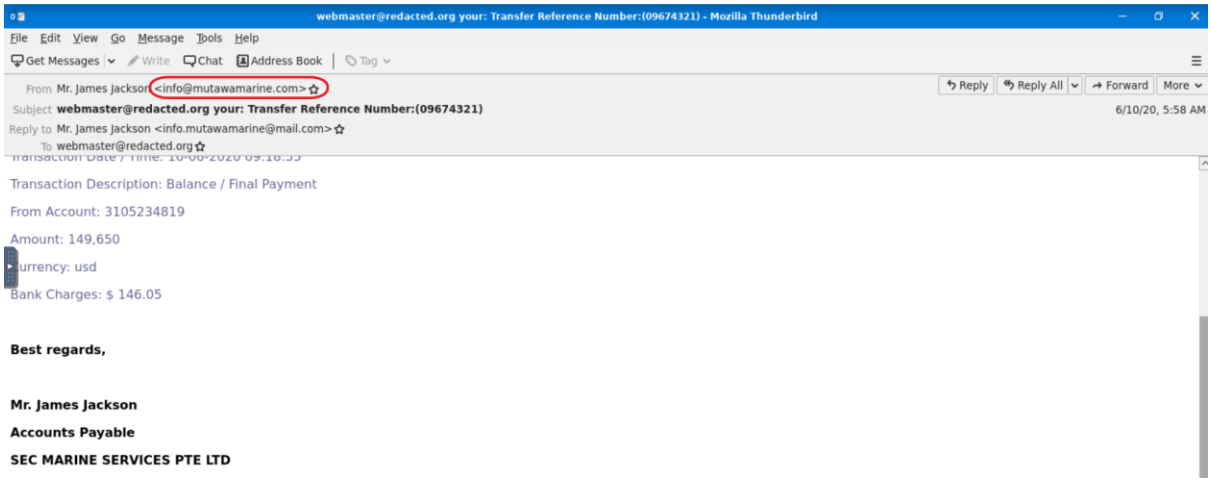
a) What is the email's timestamp? (answer format: mm/dd/yyyy hh:mm)



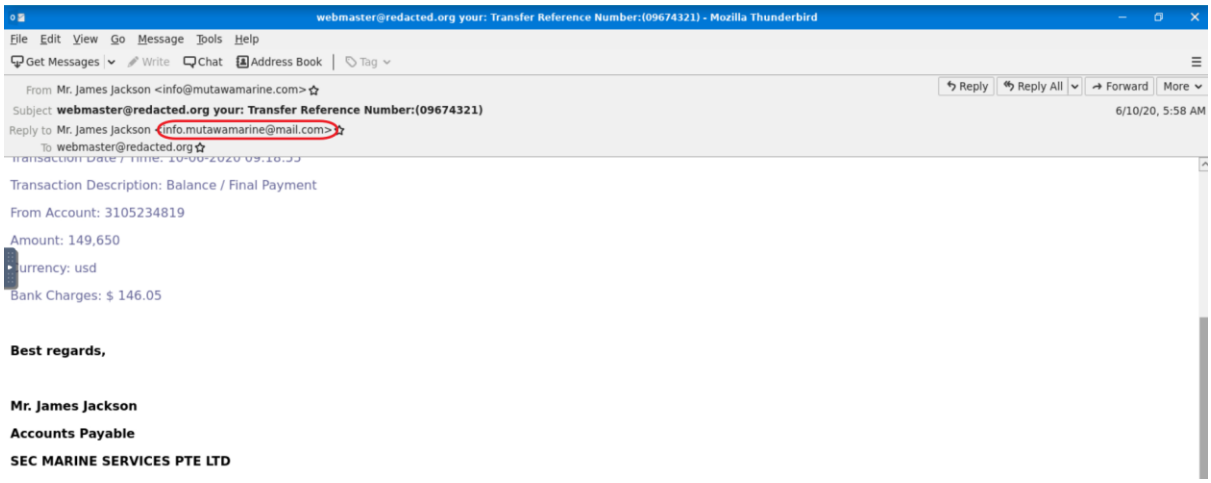
b) Who is the email from?



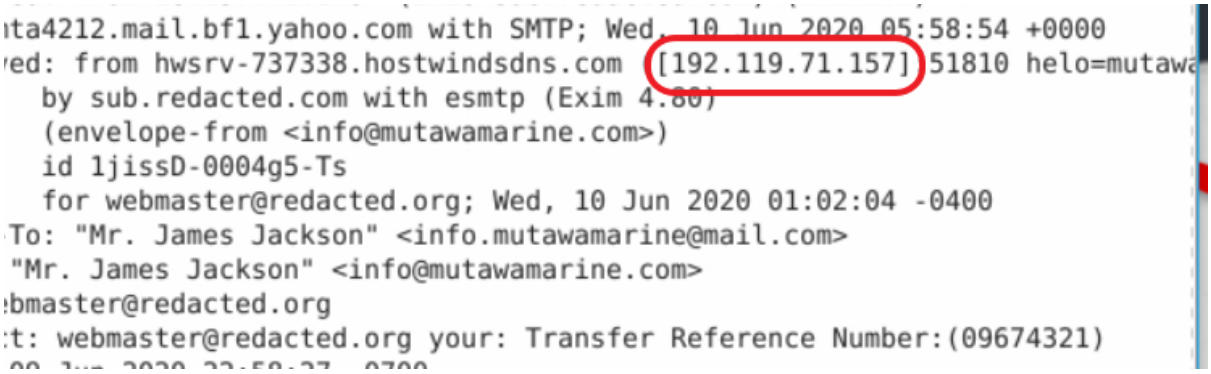
c) What is his email address?



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



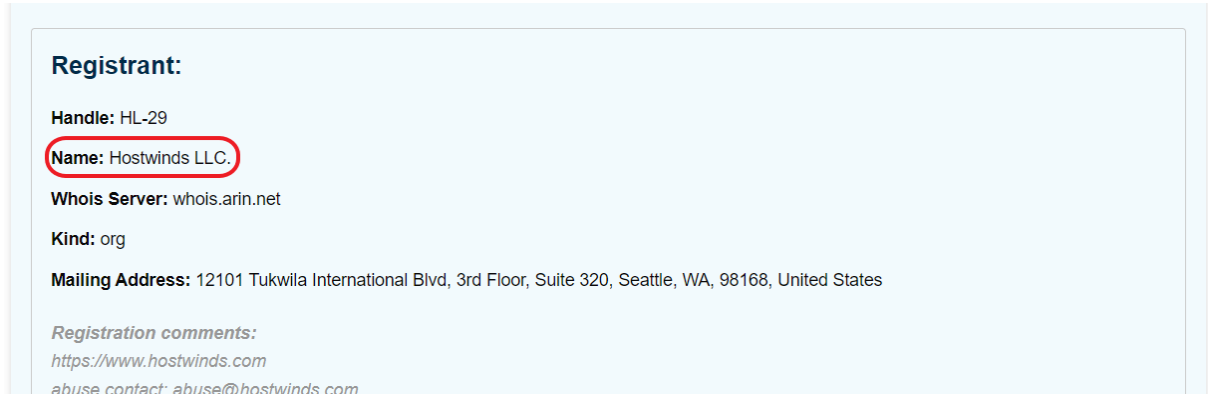
e) What is the Originating IP?



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

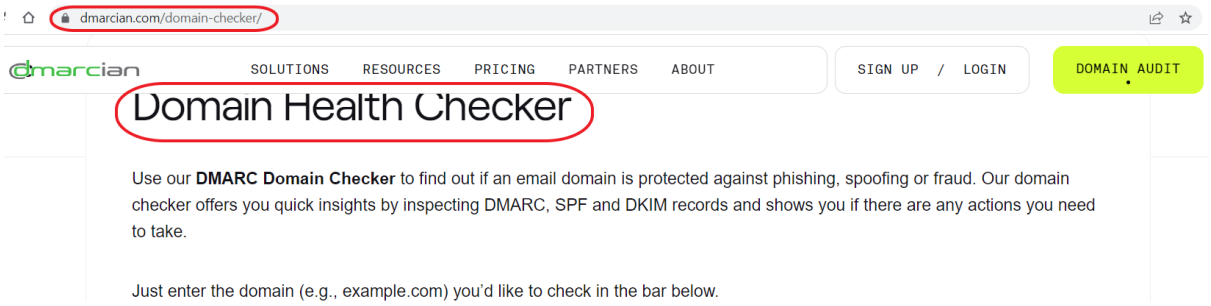
- First we go into the WHOIS lookup and enter the originating IP there

- Then we get the domain name as

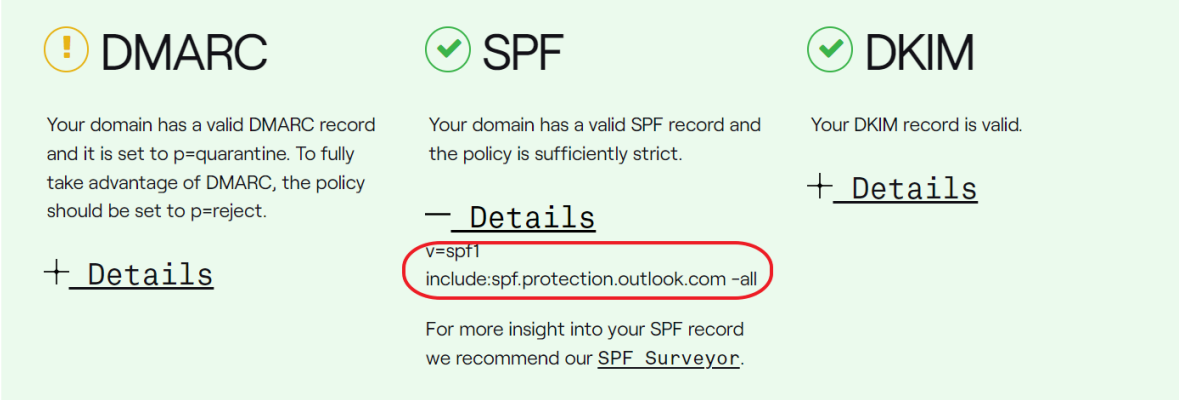


g) What is the SPF record for the Return-Path domain?

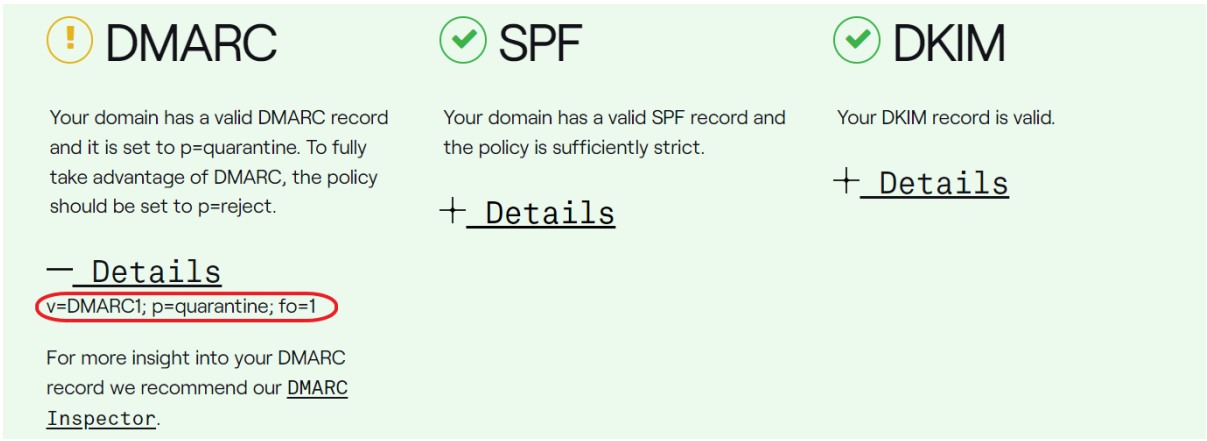
- First we go to a domain checker website



- We enter the domain name there

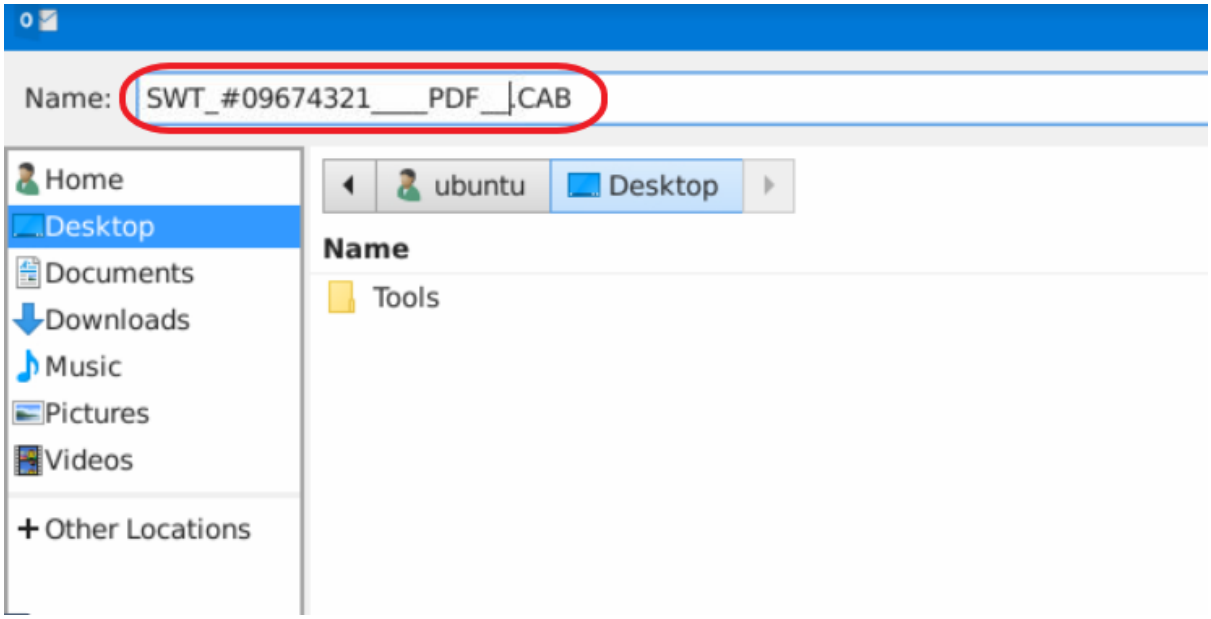


h) What is the DMARC record for the Return-Path domain?

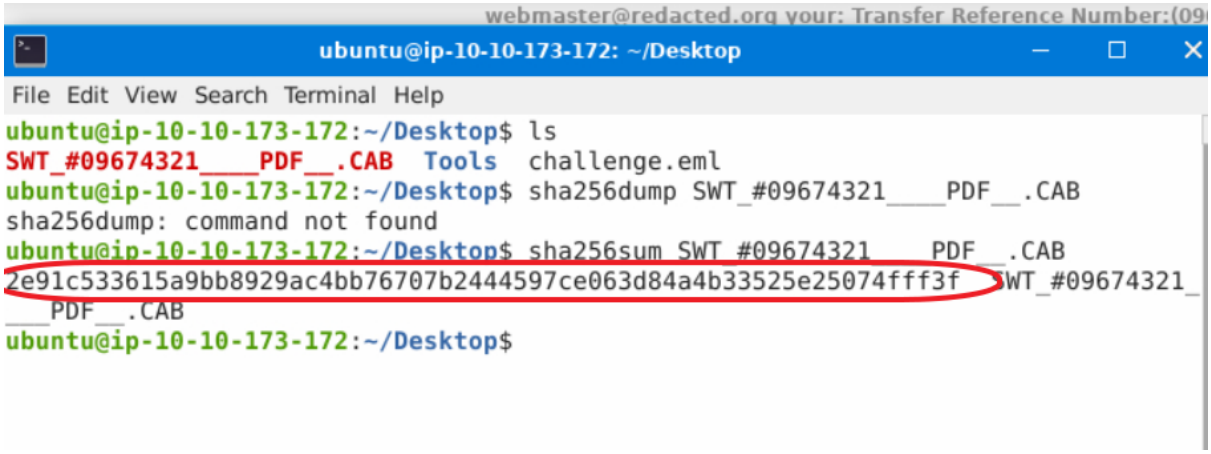


i) What is the name of the attachment?

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



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



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