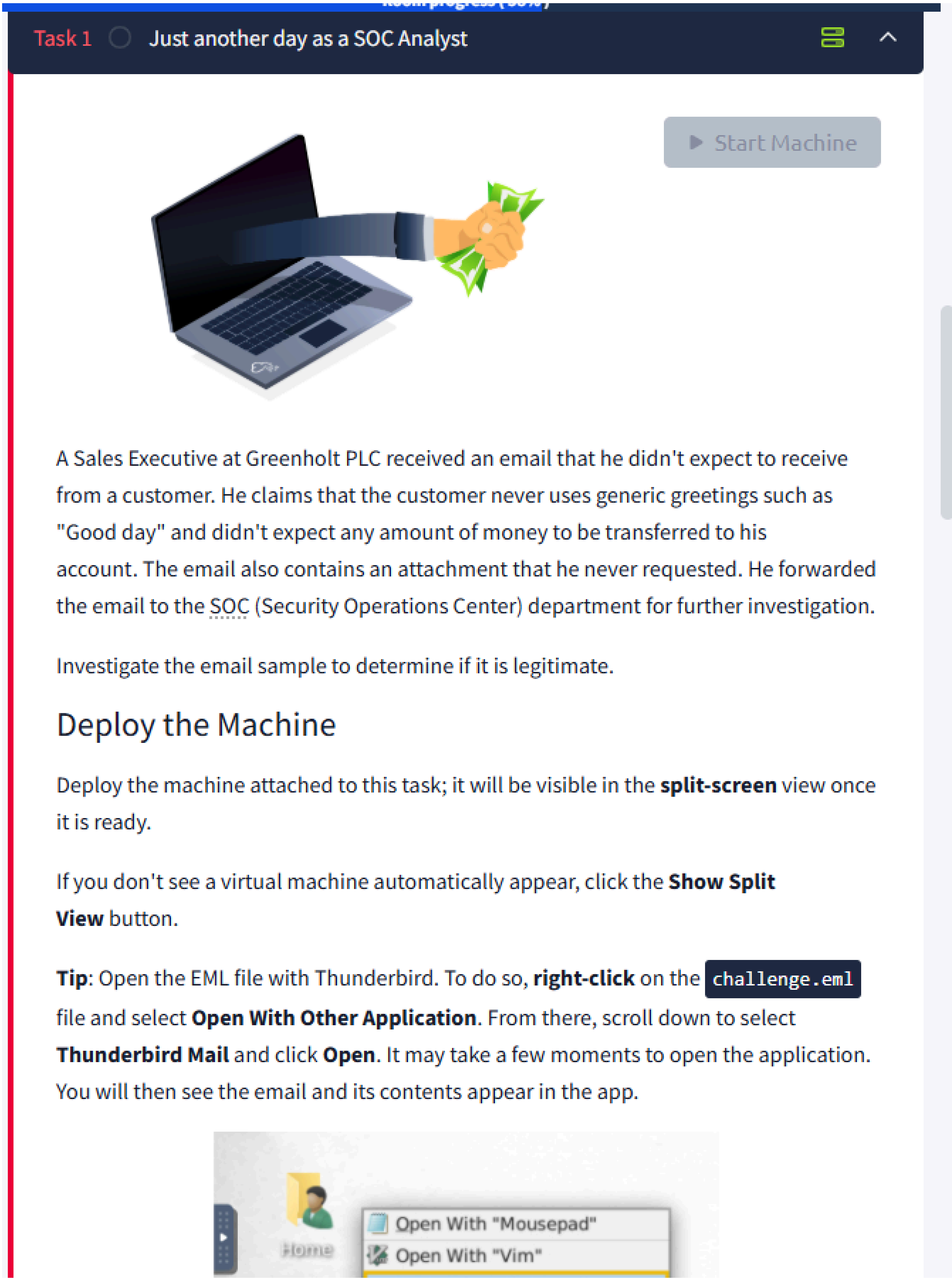
The Greenholt Phish

THM Link: https://tryhackme.com/room/phishingemails5fgjlzxc



A Sales Executive at Greenholt PLC received an email that he didn't expect to receive from a customer. He claims that the customer never uses generic greetings 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 (Security Operations Center) department for further investigation.

Investigate the email sample to determine if it is legitimate.

Deploy the Machine

Deploy the machine attached to this task; it will be visible in the **split-screen** view once it is ready.

If you don't see a virtual machine automatically appear, click the **Show Split View** button.

Tip: Open the EML file with Thunderbird. To do so, **right-click** on the `challenge.eml` file and select **Open With Other Application**. From there, scroll down to select **Thunderbird Mail** and click **Open**. It may take a few moments to open the application. You will then see the email and its contents appear in the app.

Get some information on scenario:

1. Victim is Sales Executive

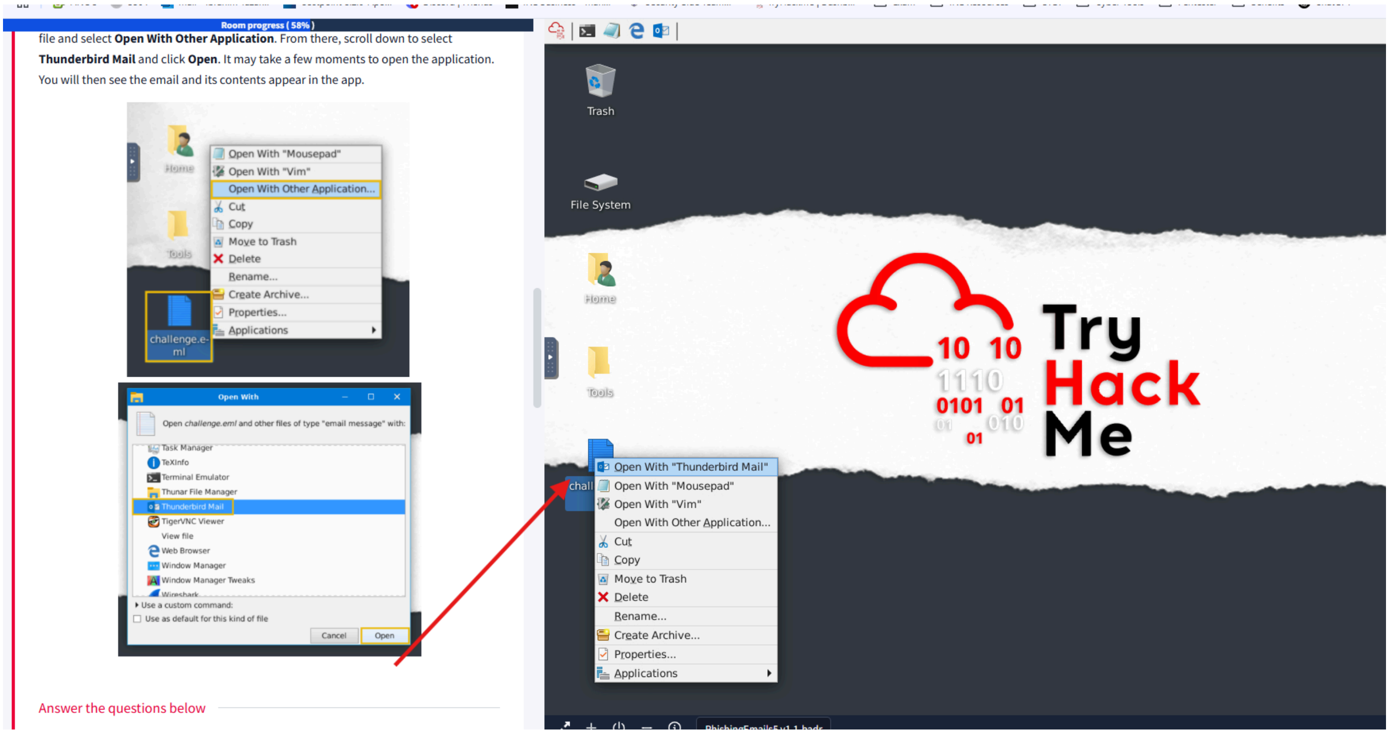
2. The victim didn't expect to receive from a customer

3. Not using Good day

4. Did not expected any money

5.Email contains attachment and never requested

Open email with thunderbird



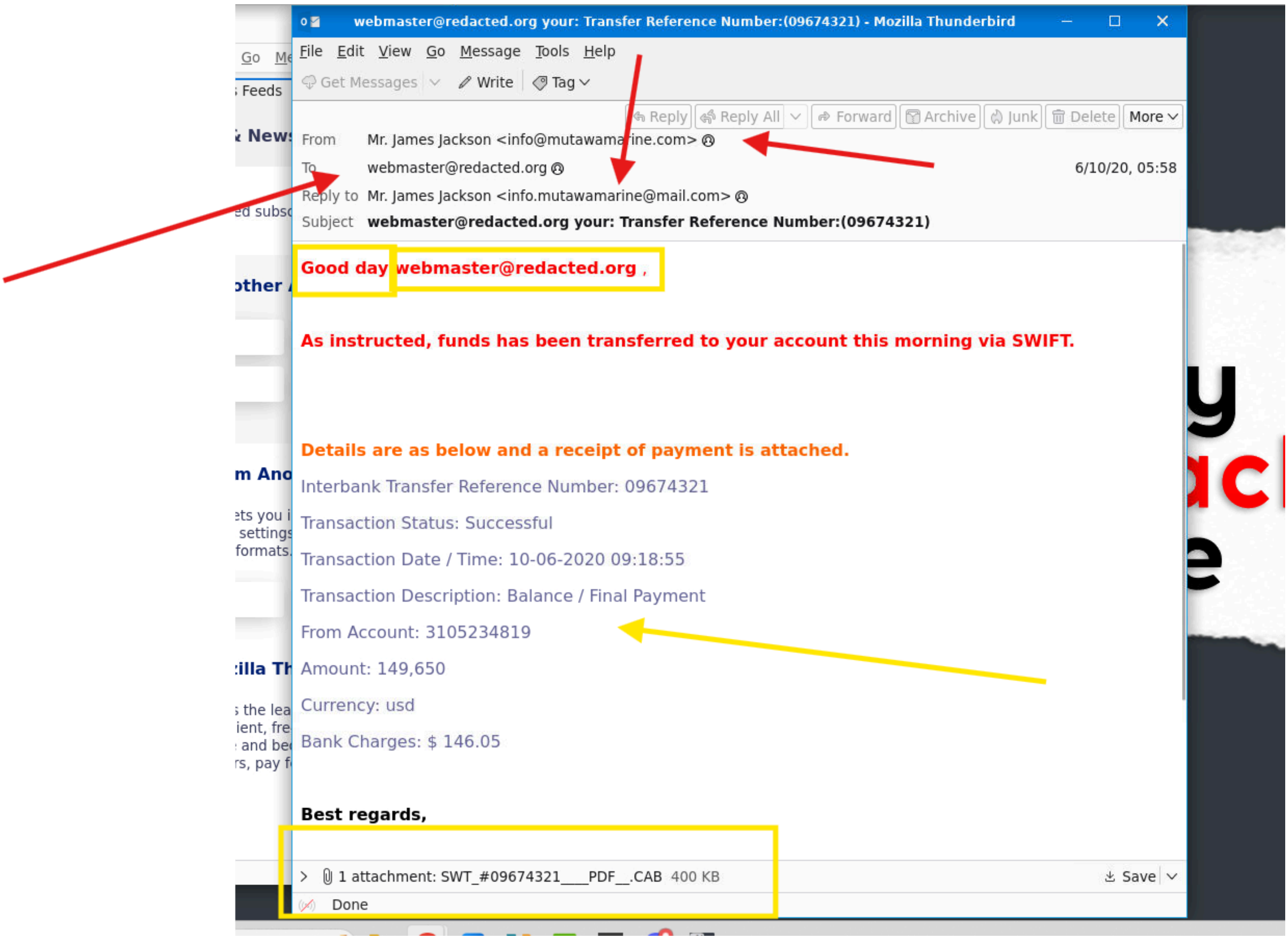
Room progress (58%)

file and select **Open With Other Application**. From there, scroll down to select **Thunderbird Mail** and click **Open**. It may take a few moments to open the application. You will then see the email and its contents appear in the app.

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

Answer the questions below

Start analyzing the email:



webmaster@redacted.org your: Transfer Reference Number:(09674321) - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Tag
Reply
Reply All
Forward
Archive
Junk
Delete
More
Save
Done

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

To webmaster@redacted.org

6/10/20, 05:58

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

Subject **webmaster@redacted.org your: Transfer Reference Number:(09674321)**

Good day webmaster@redacted.org ,

As instructed, funds has been transferred to your account this morning via SWIFT.

Details are as below and a receipt of payment is attached.

Interbank Transfer Reference Number: 09674321

Transaction Status: Successful

Transaction Date / Time: 10-06-2020 09:18:55

Transaction Description: Balance / Final Payment

From Account: 3105234819

Amount: 149,650

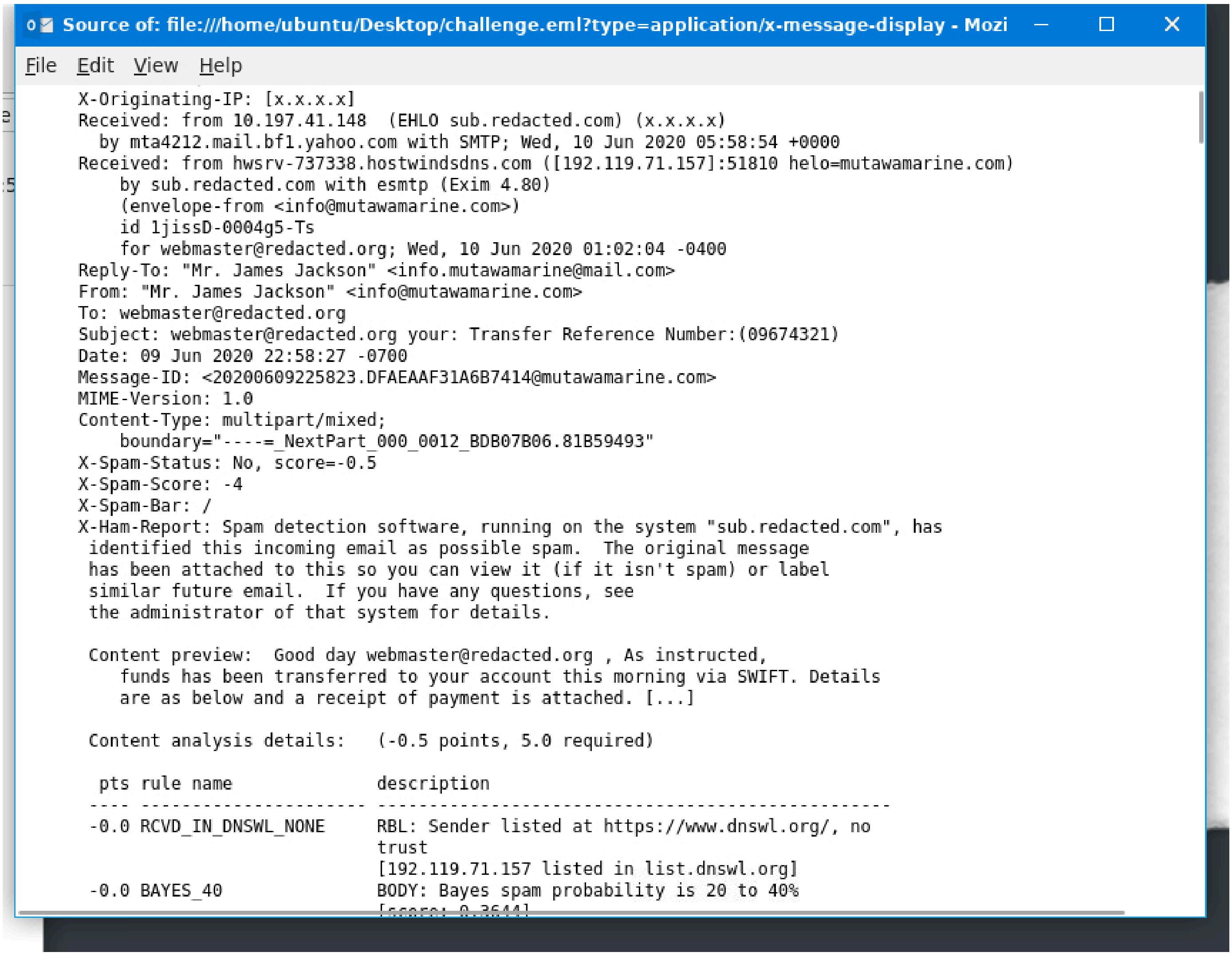
Currency: usd

Bank Charges: $ 146.05

Best regards,

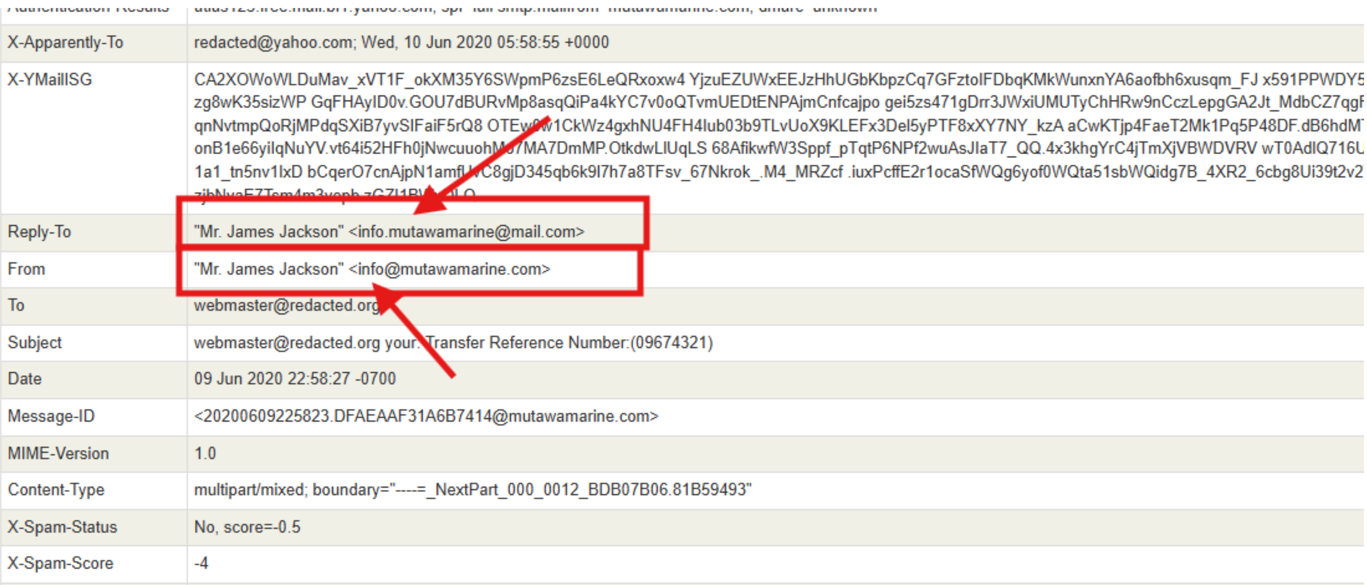
1 attachment: SWT_#09674321___PDF__.CAB 400 KB

coming from: info@mutawamarine.com

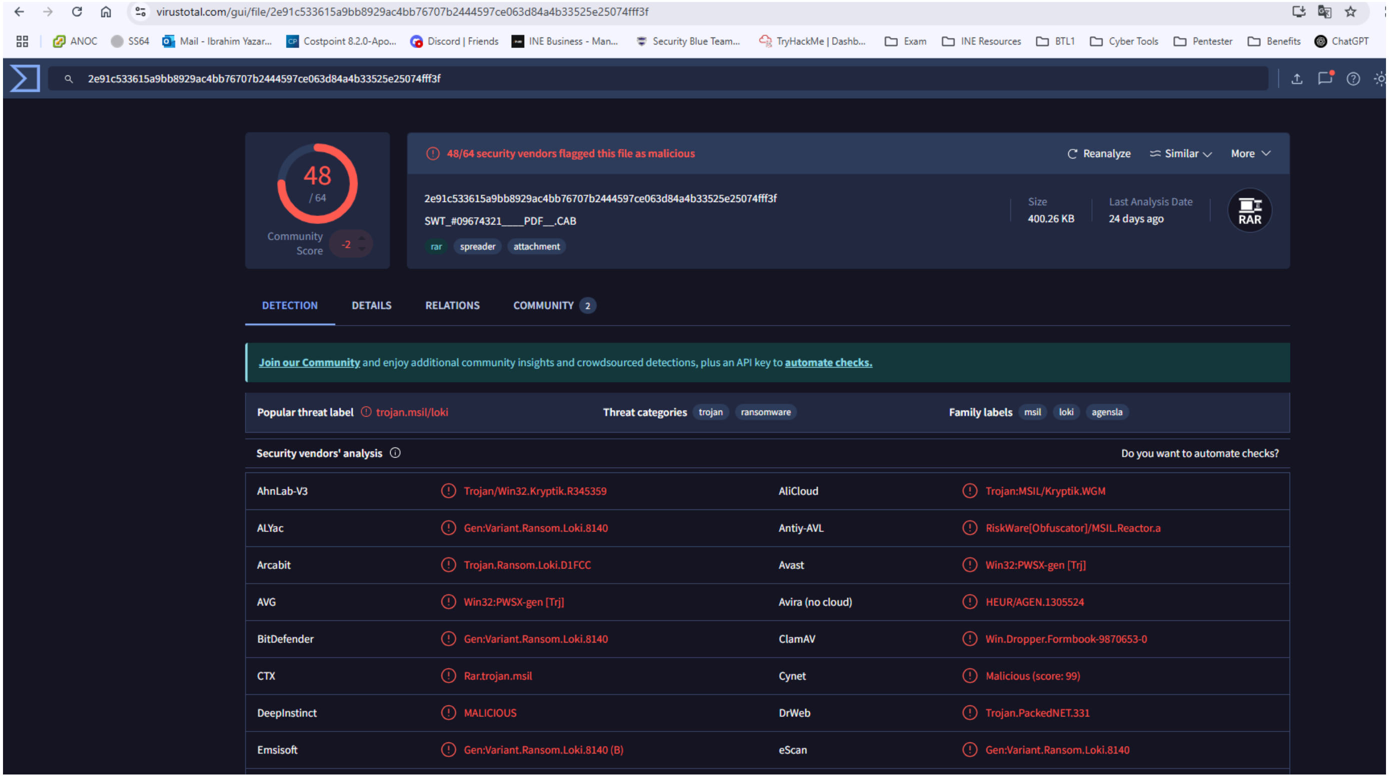

Source of: file:///home/ubuntu/Desktop/challenge.eml?type=application/x-message-display - Mozi
File Edit View Help

```
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=mutawamarine.com)
    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
Message-ID: <20200609225823.DFAEAAF31A6B7414@mutawamarine.com>
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="----=_NextPart_000_0012_BDB07B06.81B59493"
X-Spam-Status: No, score=-0.5
X-Spam-Score: -4
X-Spam-Bar: /
X-Ham-Report: Spam detection software, running on the system "sub.redacted.com", has
 identified this incoming email as possible spam.  The original message
 has been attached to this so you can view it (if it isn't spam) or label
 similar future email.  If you have any questions, see
 the administrator of that system for details.

 Content preview:  Good day webmaster@redacted.org , As instructed,
    funds has been transferred to your account this morning via SWIFT. Details
    are as below and a receipt of payment is attached. [...]

 Content analysis details:   (-0.5 points, 5.0 required)

  pts rule name              description
 ---- ---------------------- --------------------------------------------------
 -0.0 RCVD_IN_DNSWL_NONE     RBL: Sender listed at https://www.dnswl.org/, no
                             trust
                             [192.119.71.157 listed in list.dnswl.org]
 -0.0 BAYES_40               BODY: Bayes spam probability is 20 to 40%
                             [score: 0.3644]
```

SPF Alignment — The SPF Alignment is PASS only when “Return-Path” And “From” domain is same. Different between which helps us understand email could be spoofed



Authentication-Results	atlas125.free.mail.bf1.yahoo.com; spf=fail smtp.mailfrom=mutawamarine.com; dmarc=unknown
X-Apparently-To	redacted@yahoo.com; Wed, 10 Jun 2020 05:58:55 +0000
X-YMailISG	CA2XOWoWLDuMav_xVT1F_okXM35Y6SWpmP6zsE6LeQRxoxw4 YjzuEZUWxEEJzHhUGbKbpzCq7GFztolFDbqKMkWunxnYA6aofbh6xusqm_FJ x591PPWDY5 zg8wK35sizWP GqFHAyID0v.GOU7dBURvMp8asqQiPa4kYC7v0oQTvmUEDtENPAjmCnfcajpo gei5zs471gDrr3JWxiUMUTyChHRw9nCczLepgGA2Jt_MdbCZ7qgF qnNvtmpQoRjMPdqSXiB7yvSIFaiF5rQ8 OTEw0w1CkWz4gxhNU4FH4lub03b9TLvUoX9KLEFx3Del5yPTF8xXY7NY_kzA aCwKTjp4FaeT2Mk1Pq5P48DF.dB6hdMT onB1e66yilqNuYV.vt64i52HFh0jNwcuuohM67MA7DmMP.OtkdwLlUqLS 68AfikwfW3Sppf_pTqtP6NPf2wuAsJlaT7_QQ.4x3khgYrC4jTmXjVBWDVRV wT0AdIQ716U 1a1_tn5nv1lxD bCqerO7cnAjpN1amfLVC8gjD345qb6k9I7h7a8TFsv_67Nkrok_.M4_MRZcf .iuxPcffE2r1ocaSfWQg6yof0WQta51sbWQidg7B_4XR2_6cbg8Ui39t2v2 zjbNvaE7Tcm4m3vcph.zGZI1BW.JLO
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
Message-ID	<20200609225823.DFAEAAF31A6B7414@mutawamarine.com>
MIME-Version	1.0
Content-Type	multipart/mixed; boundary="----=_NextPart_000_0012_BDB07B06.81B59493"
X-Spam-Status	No, score=-0.5
X-Spam-Score	-4



virustotal.com/gui/file/2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f

2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f

48 / 64

Community Score -2

48/64 security vendors flagged this file as malicious

2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f

SWT_#09674321____PDF__.CAB

rar spreader attachment

Size 400.26 KB

Last Analysis Date 24 days ago

RAR

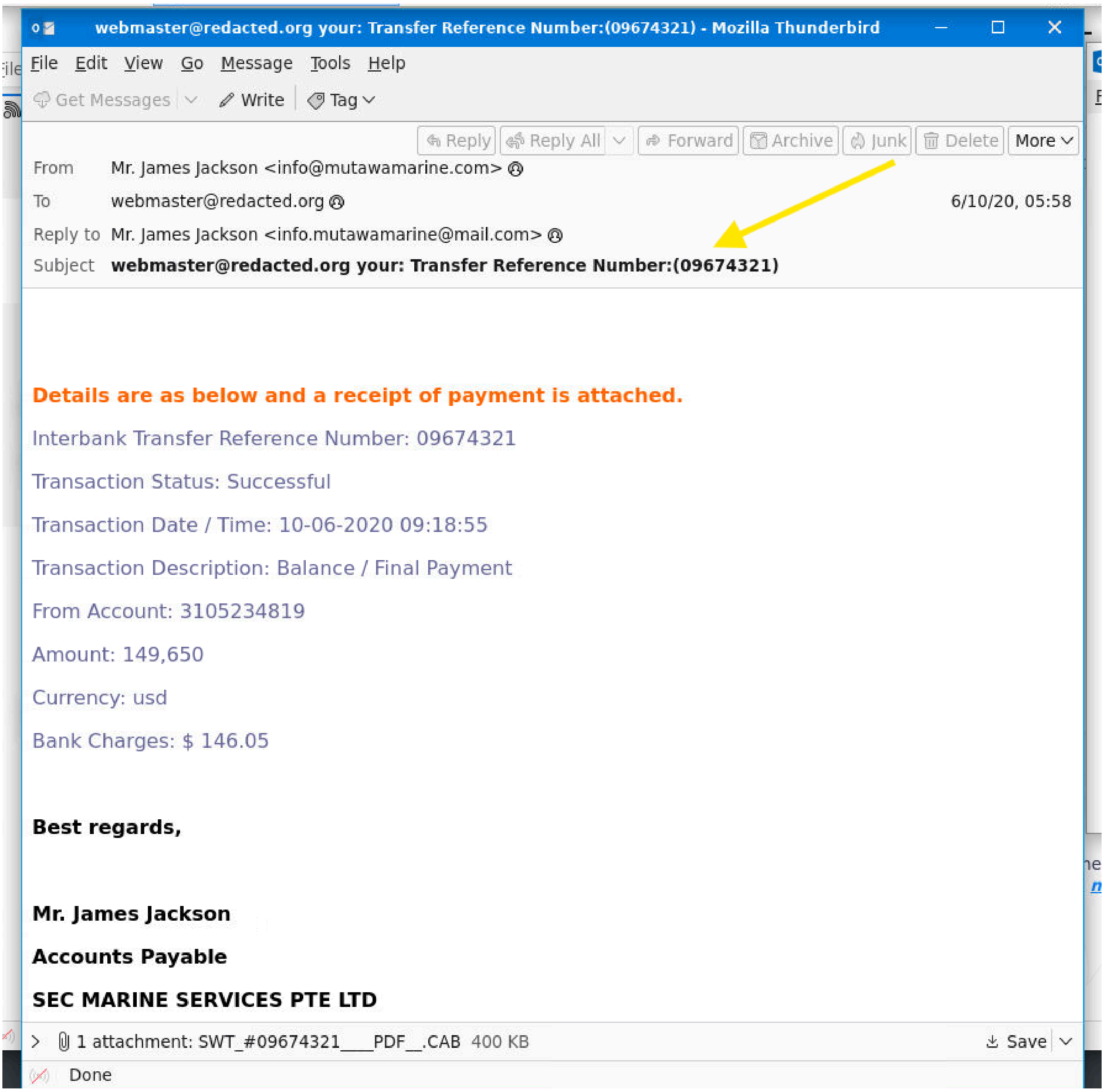
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.msil/loki   Threat categories trojan ransomware   Family labels msil loki agensla

Security vendors' analysis   Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Kryptik.R345359	AliCloud	Trojan:MSIL/Kryptik.WGM
ALYac	Gen:Variant.Ransom.Loki.8140	Antiy-AVL	RiskWare[Obfuscator]/MSIL.Reactor.a
Arcabit	Trojan.Ransom.Loki.D1FCC	Avast	Win32:PWSX-gen [Trj]
AVG	Win32:PWSX-gen [Trj]	Avira (no cloud)	HEUR/AGEN.1305524
BitDefender	Gen:Variant.Ransom.Loki.8140	ClamAV	Win.Dropper.Formbook-9870653-0
CTX	Rar.trojan.msil	Cynet	Malicious (score: 99)
DeepInstinct	MALICIOUS	DrWeb	Trojan.PackedNET.331
Emsisoft	Gen:Variant.Ransom.Loki.8140 (B)	eScan	Gen:Variant.Ransom.Loki.8140

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



webmaster@redacted.org your: Transfer Reference Number:(09674321) - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Tag
Reply
Reply All
Forward
Archive
Junk
Delete
More

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

To webmaster@redacted.org

6/10/20, 05:58

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

Subject **webmaster@redacted.org your: Transfer Reference Number:(09674321)**

Details are as below and a receipt of payment is attached.

Interbank Transfer Reference Number: 09674321

Transaction Status: Successful

Transaction Date / Time: 10-06-2020 09:18:55

Transaction Description: Balance / Final Payment

From Account: 3105234819

Amount: 149,650

Currency: usd

Bank Charges: $ 146.05

Best regards,

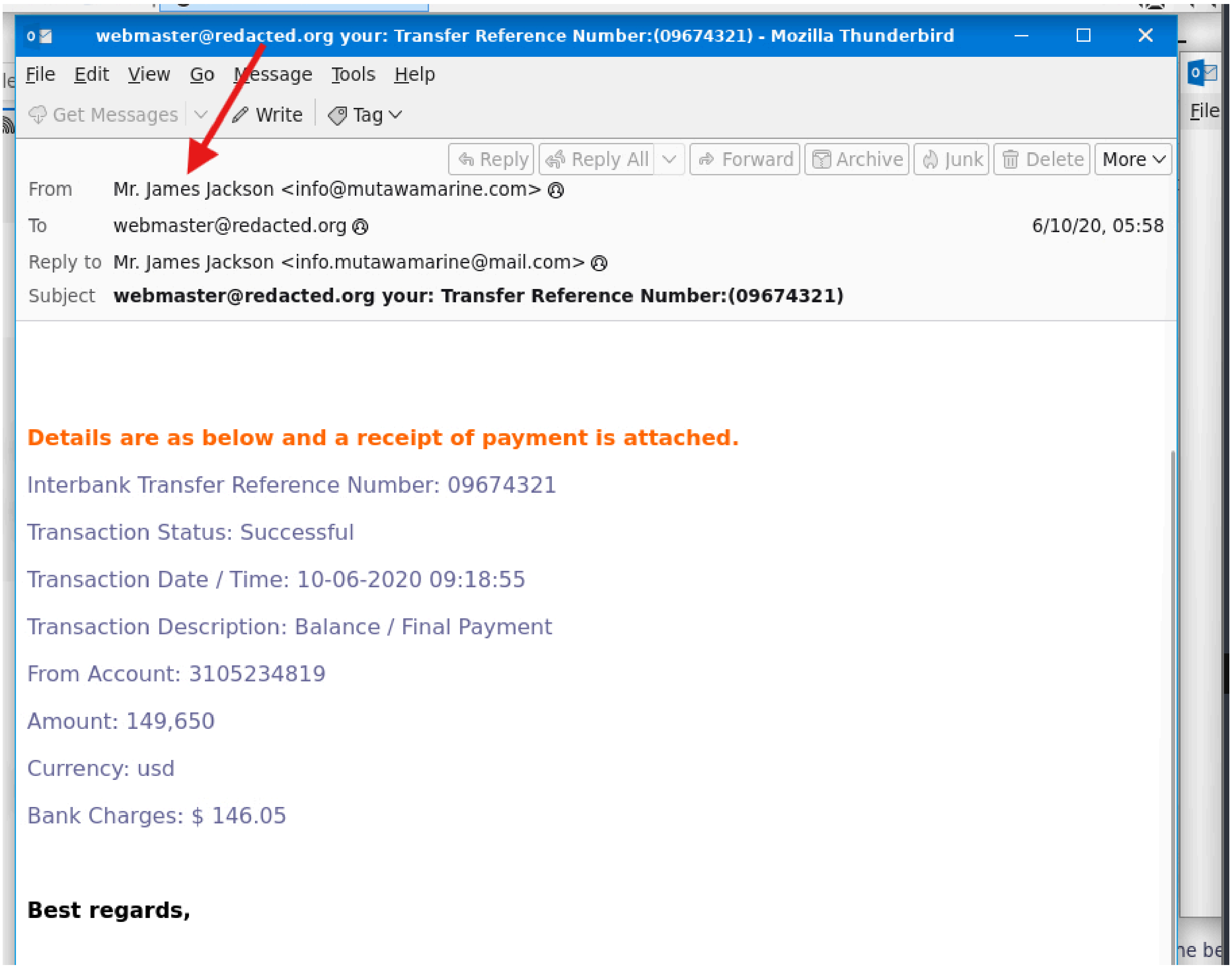
Mr. James Jackson

Accounts Payable

SEC MARINE SERVICES PTE LTD

1 attachment: SWT_#09674321___PDF__.CAB 400 KB

Who is the email from?



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

To webmaster@redacted.org

6/10/20, 05:58

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

Subject **webmaster@redacted.org your: Transfer Reference Number:(09674321)**

Details are as below and a receipt of payment is attached.

Interbank Transfer Reference Number: 09674321

Transaction Status: Successful

Transaction Date / Time: 10-06-2020 09:18:55

Transaction Description: Balance / Final Payment

From Account: 3105234819

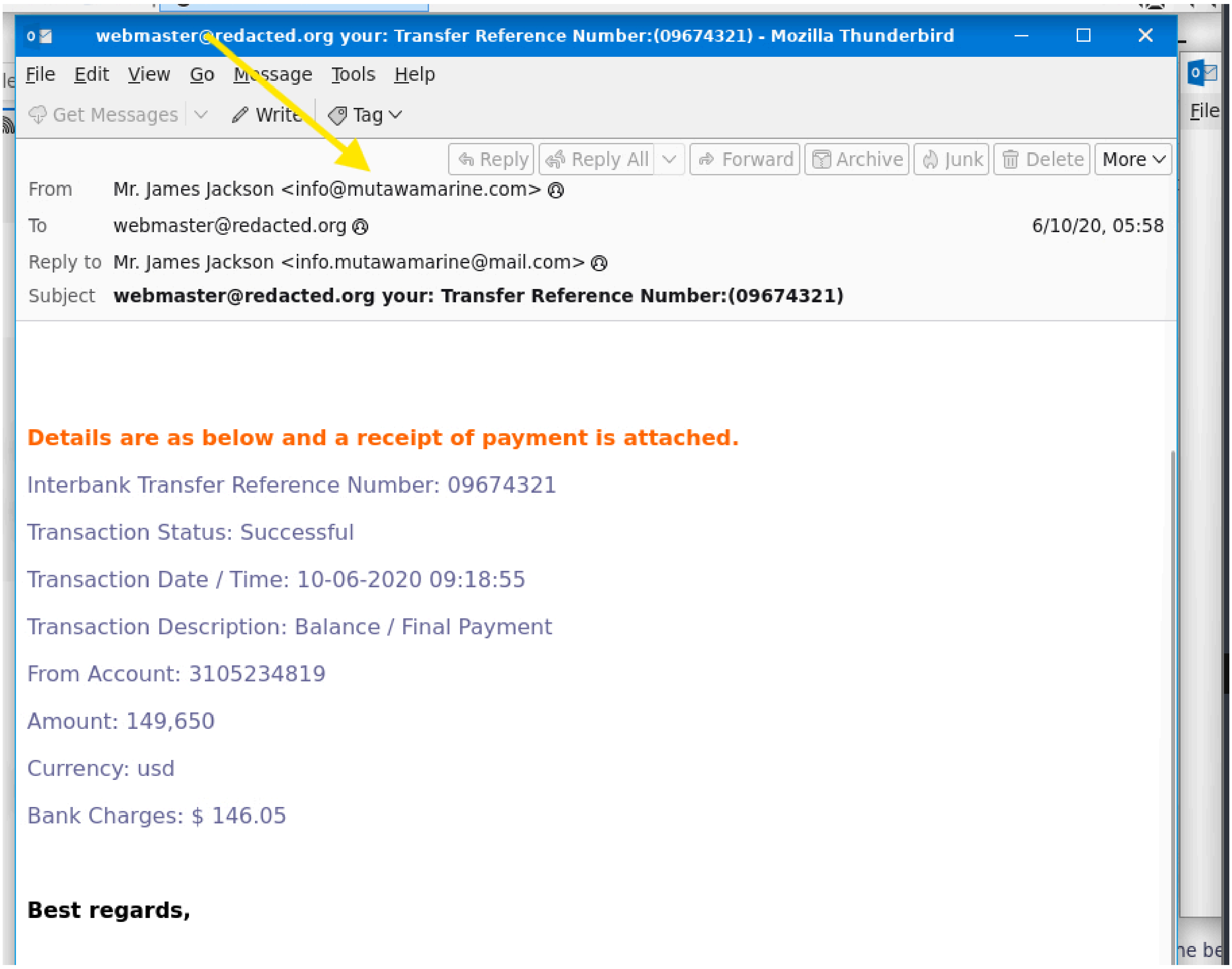
Amount: 149,650

Currency: usd

Bank Charges: $ 146.05

Best regards,

What is his email address?


webmaster@redacted.org your: Transfer Reference Number:(09674321) - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Tag
Reply
Reply All
Forward
Archive
Junk
Delete
More

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

To webmaster@redacted.org 6/10/20, 05:58

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

Subject **webmaster@redacted.org your: Transfer Reference Number:(09674321)**

Details are as below and a receipt of payment is attached.

Interbank Transfer Reference Number: 09674321

Transaction Status: Successful

Transaction Date / Time: 10-06-2020 09:18:55

Transaction Description: Balance / Final Payment

From Account: 3105234819

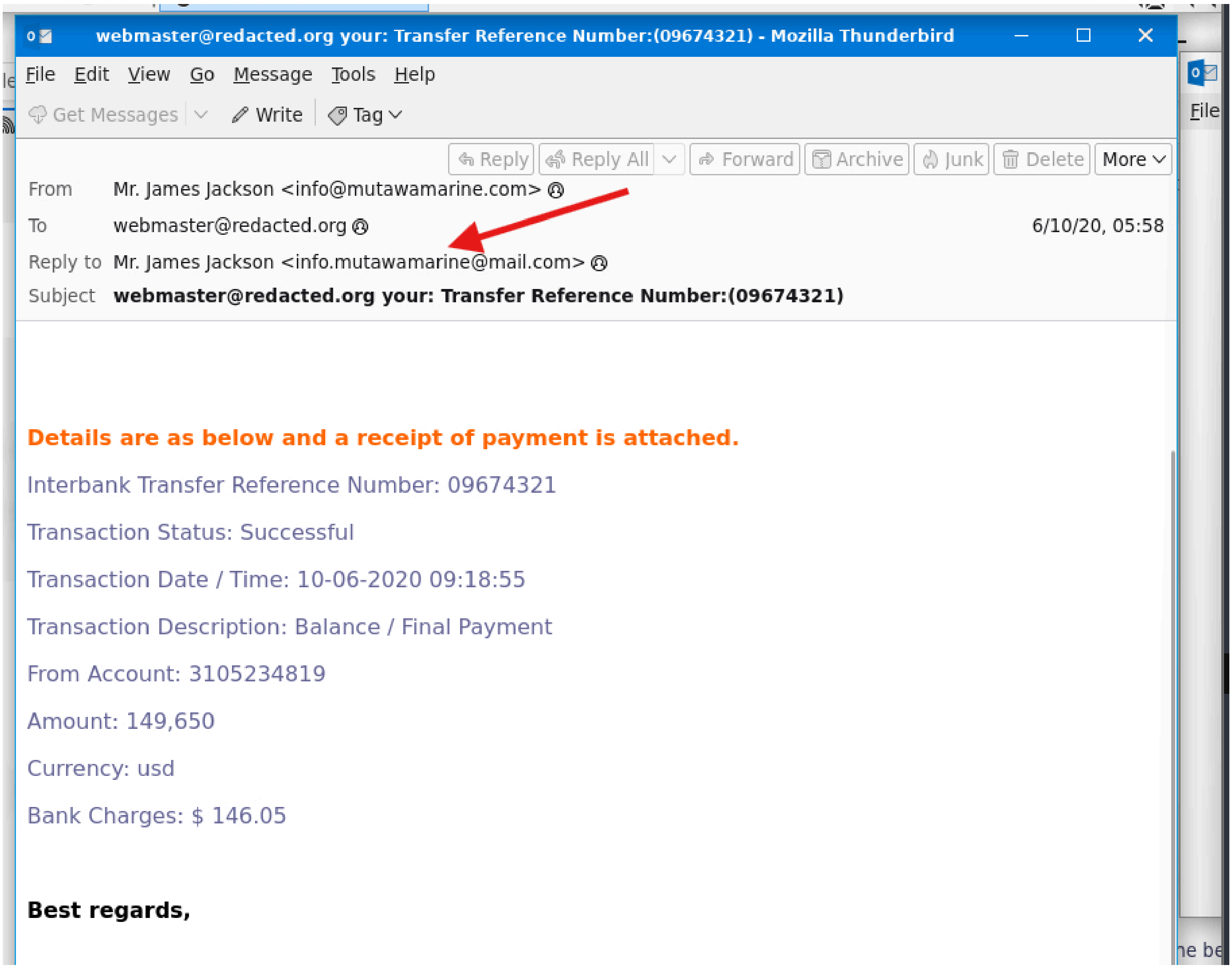
Amount: 149,650

Currency: usd

Bank Charges: $ 146.05

Best regards,

What email address will receive a reply to this email?


webmaster@redacted.org your: Transfer Reference Number:(09674321) - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Tag
Reply
Reply All
Forward
Archive
Junk
Delete
More

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

To webmaster@redacted.org

6/10/20, 05:58

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

Subject **webmaster@redacted.org your: Transfer Reference Number:(09674321)**

Details are as below and a receipt of payment is attached.

Interbank Transfer Reference Number: 09674321

Transaction Status: Successful

Transaction Date / Time: 10-06-2020 09:18:55

Transaction Description: Balance / Final Payment

From Account: 3105234819

Amount: 149,650

Currency: usd

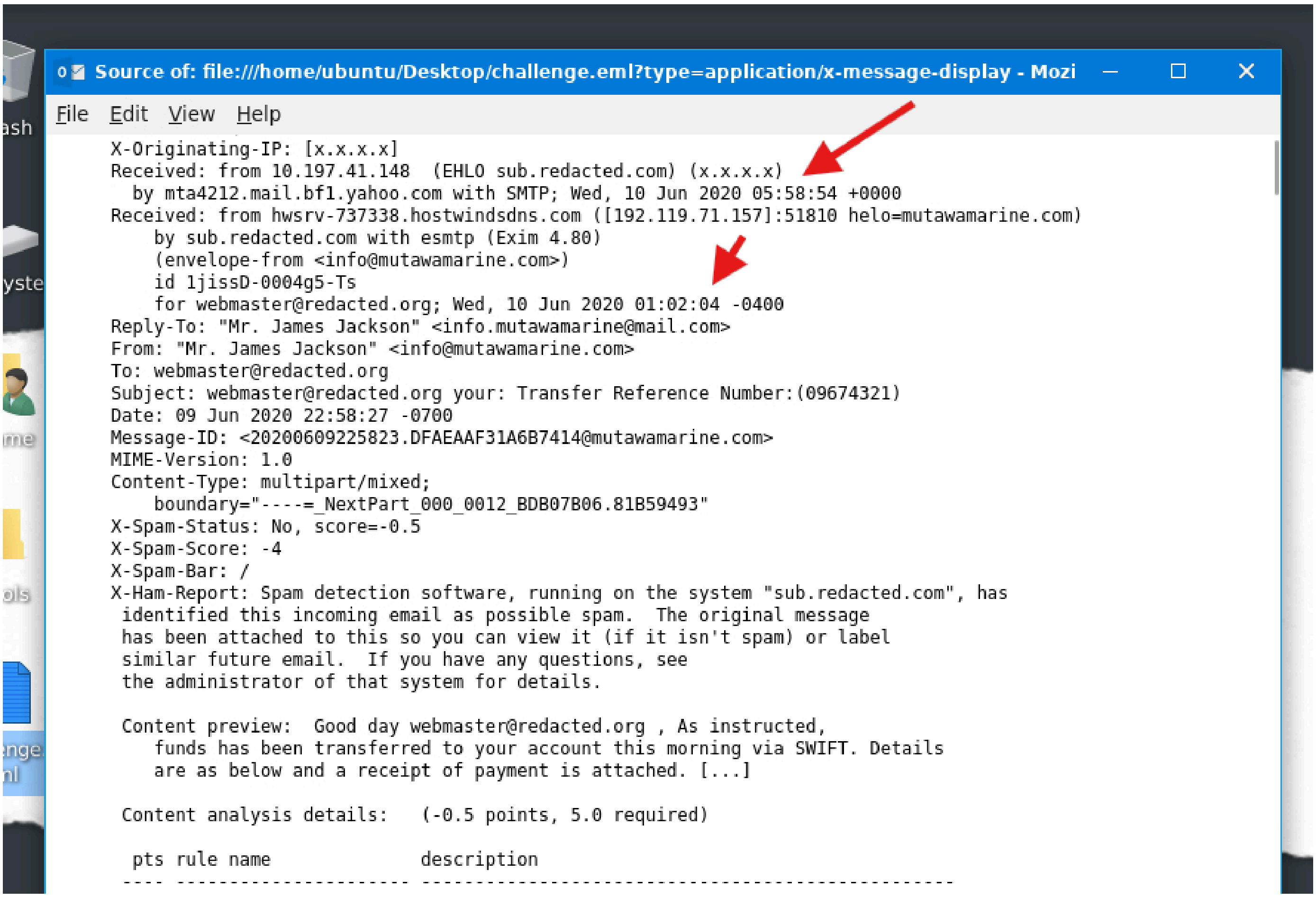
Bank Charges: $ 146.05

Best regards,

What is the Originating IP?

1. **Identify the First "Received" Header**: Email headers usually contain multiple "Received" lines, which track the servers that handled the email as it was transmitted. The **first "Received" line typically indicates the originating server.**
2. **Locate the IP Address**: In the first "Received" line, look for the IP address following the `from` keyword. This is the IP address from which the email was originally sent.

For finding which Received is first we can check the tyime and identify the first email.

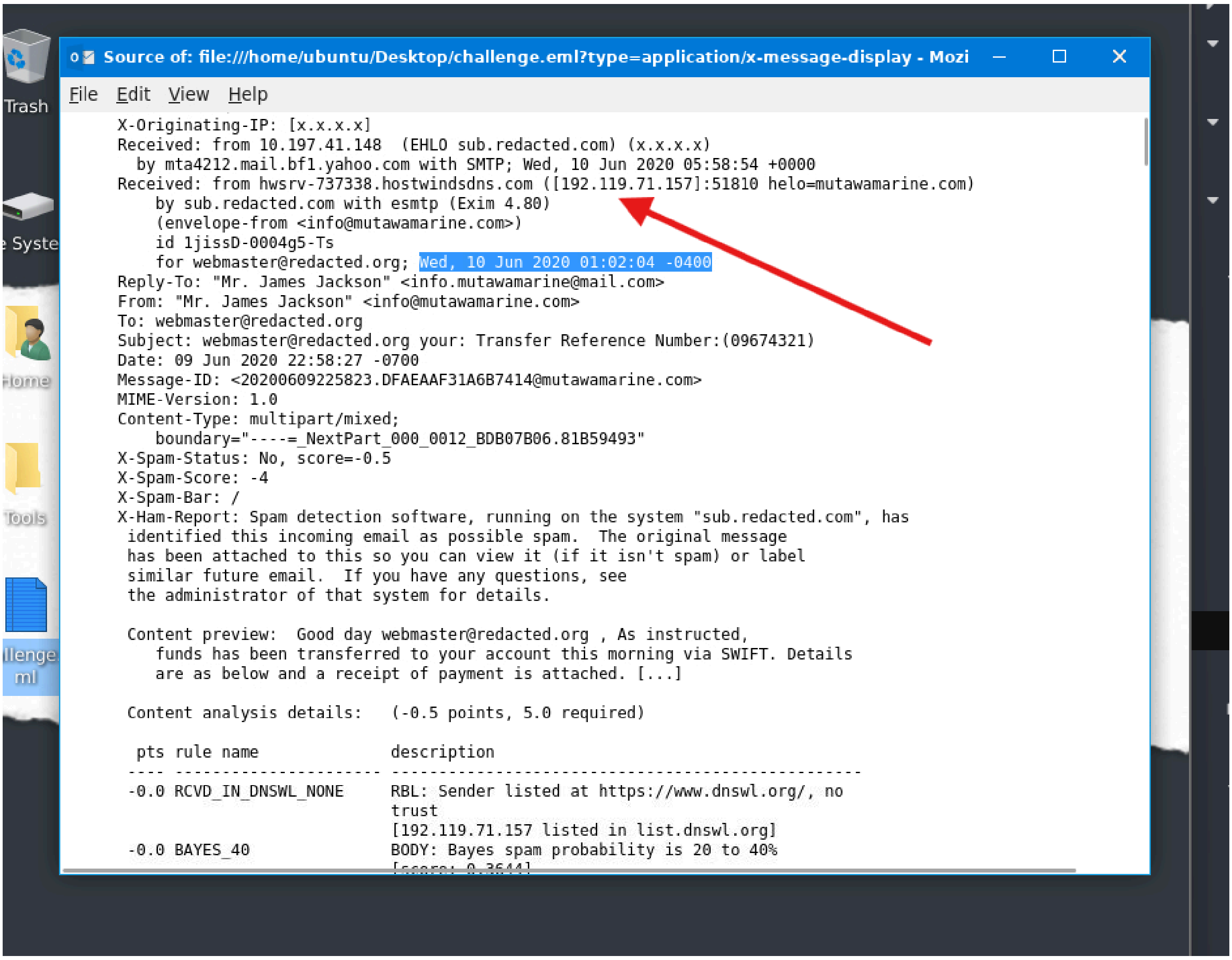

Source of: file:///home/ubuntu/Desktop/challenge.eml?type=application/x-message-display - Mozi
File
Edit
View
Help
ash
yste
me
ols
nge
nl

```
    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=mutawamarine.com)
        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
    Message-ID: <20200609225823.DFAEAAF31A6B7414@mutawamarine.com>
    MIME-Version: 1.0
    Content-Type: multipart/mixed;
        boundary="----=_NextPart_000_0012_BDB07B06.81B59493"
    X-Spam-Status: No, score=-0.5
    X-Spam-Score: -4
    X-Spam-Bar: /
    X-Ham-Report: Spam detection software, running on the system "sub.redacted.com", has
     identified this incoming email as possible spam.  The original message
     has been attached to this so you can view it (if it isn't spam) or label
     similar future email.  If you have any questions, see
     the administrator of that system for details.

     Content preview:  Good day webmaster@redacted.org , As instructed,
        funds has been transferred to your account this morning via SWIFT. Details
        are as below and a receipt of payment is attached. [...]

     Content analysis details:   (-0.5 points, 5.0 required)

      pts rule name              description
     ---- ---------------------- --------------------------------------------------
```

times are different time and we need to convert UTC time zone

Wed, 10 Jun 2020 05:58:54 +0000 --> Wed, 10 Jun 2020 05:58:54 +0000 UTC

Wed, 10 Jun 2020 01:02:04 -0400 --> Wed, 10 Jun 2020 05:02:04 UTC


Source of: file:///home/ubuntu/Desktop/challenge.eml?type=application/x-message-display - Mozi
File Edit View Help
Trash
Syste
Home
Tools
llenge
ml

```
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=mutawamarine.com)
    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
Message-ID: <20200609225823.DFAEAAF31A6B7414@mutawamarine.com>
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="----=_NextPart_000_0012_BDB07B06.81B59493"
X-Spam-Status: No, score=-0.5
X-Spam-Score: -4
X-Spam-Bar: /
X-Ham-Report: Spam detection software, running on the system "sub.redacted.com", has
 identified this incoming email as possible spam.  The original message
 has been attached to this so you can view it (if it isn't spam) or label
 similar future email.  If you have any questions, see
 the administrator of that system for details.

 Content preview:  Good day webmaster@redacted.org , As instructed,
    funds has been transferred to your account this morning via SWIFT. Details
    are as below and a receipt of payment is attached. [...]

 Content analysis details:   (-0.5 points, 5.0 required)

  pts rule name              description
 ---- ---------------------- --------------------------------------------------
 -0.0 RCVD_IN_DNSWL_NONE     RBL: Sender listed at https://www.dnswl.org/, no
                             trust
                             [192.119.71.157 listed in list.dnswl.org]
 -0.0 BAYES_40               BODY: Bayes spam probability is 20 to 40%
                             [score: 0.3644]
```

Based on the provided headers:

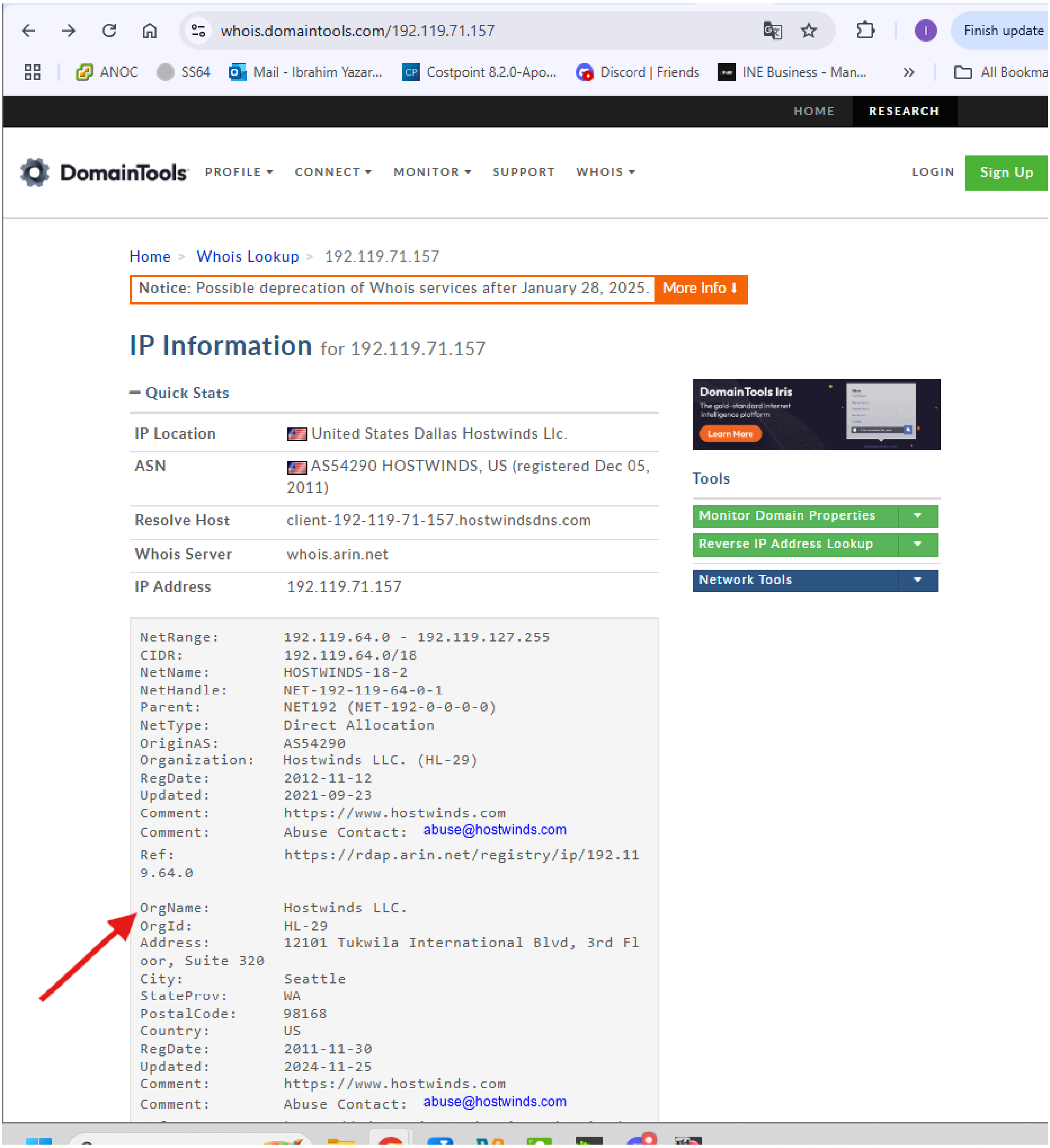
- **Received from hwsrv-737338.hostwindsdns.com ([192.119.71.157]:51810 helo=mutawamarine.com)**: This line indicates that the email was originally sent from the server `hwsrv-737338.hostwindsdns.com` with the IP address 192.119.71.157.

Therefore, the **Originating IP** is **192.119.71.157**.

```
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
```

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

Go to https://whois.domaintools.com/ and copy paste IP adress



Home > Whois Lookup > 192.119.71.157

Notice: Possible deprecation of Whois services after January 28, 2025. More Info ⬇

IP Information for 192.119.71.157

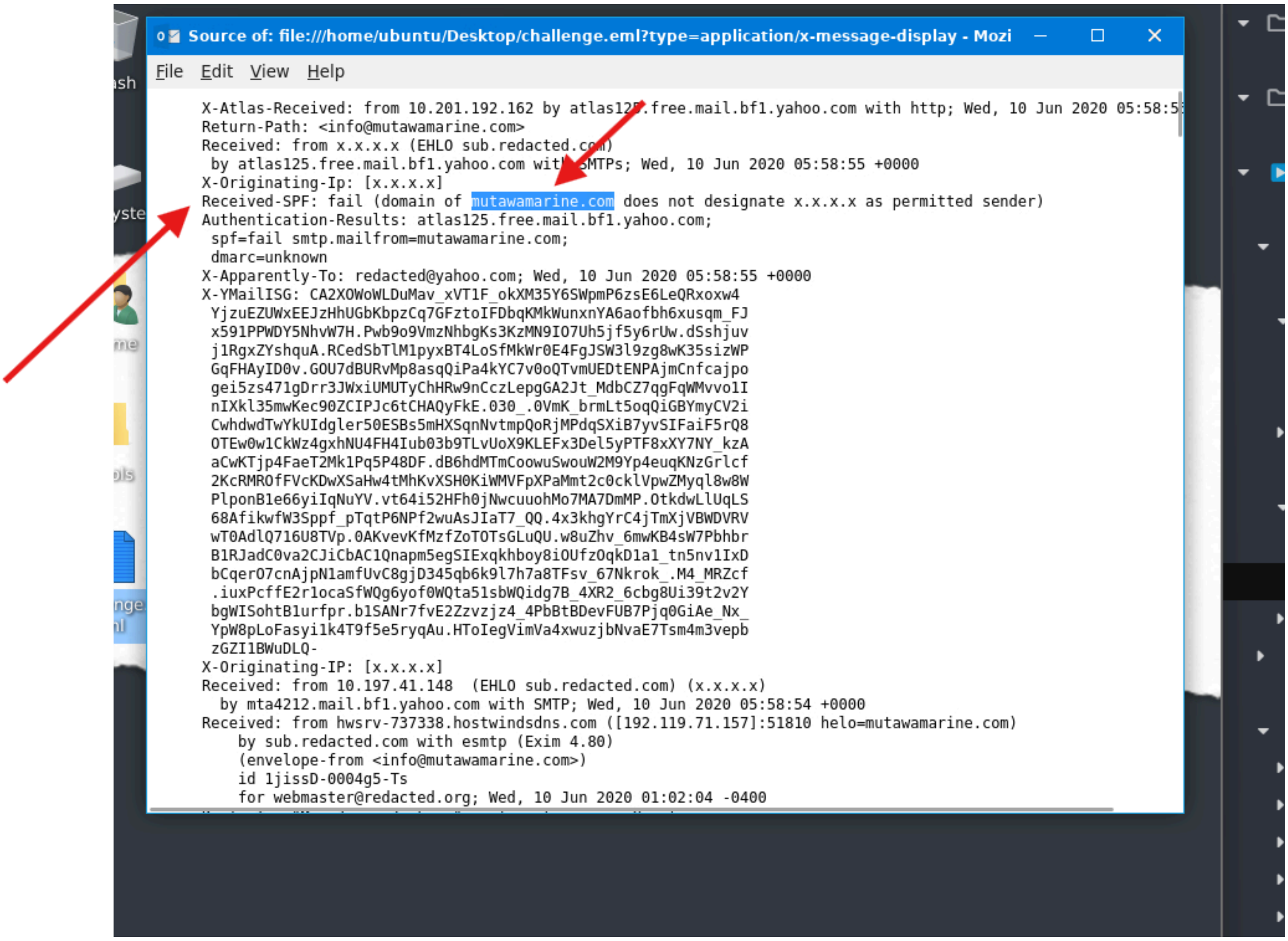
− Quick Stats

IP Location	United States Dallas Hostwinds Llc.
ASN	AS54290 HOSTWINDS, US (registered Dec 05, 2011)
Resolve Host	client-192-119-71-157.hostwindsdns.com
Whois Server	whois.arin.net
IP Address	192.119.71.157

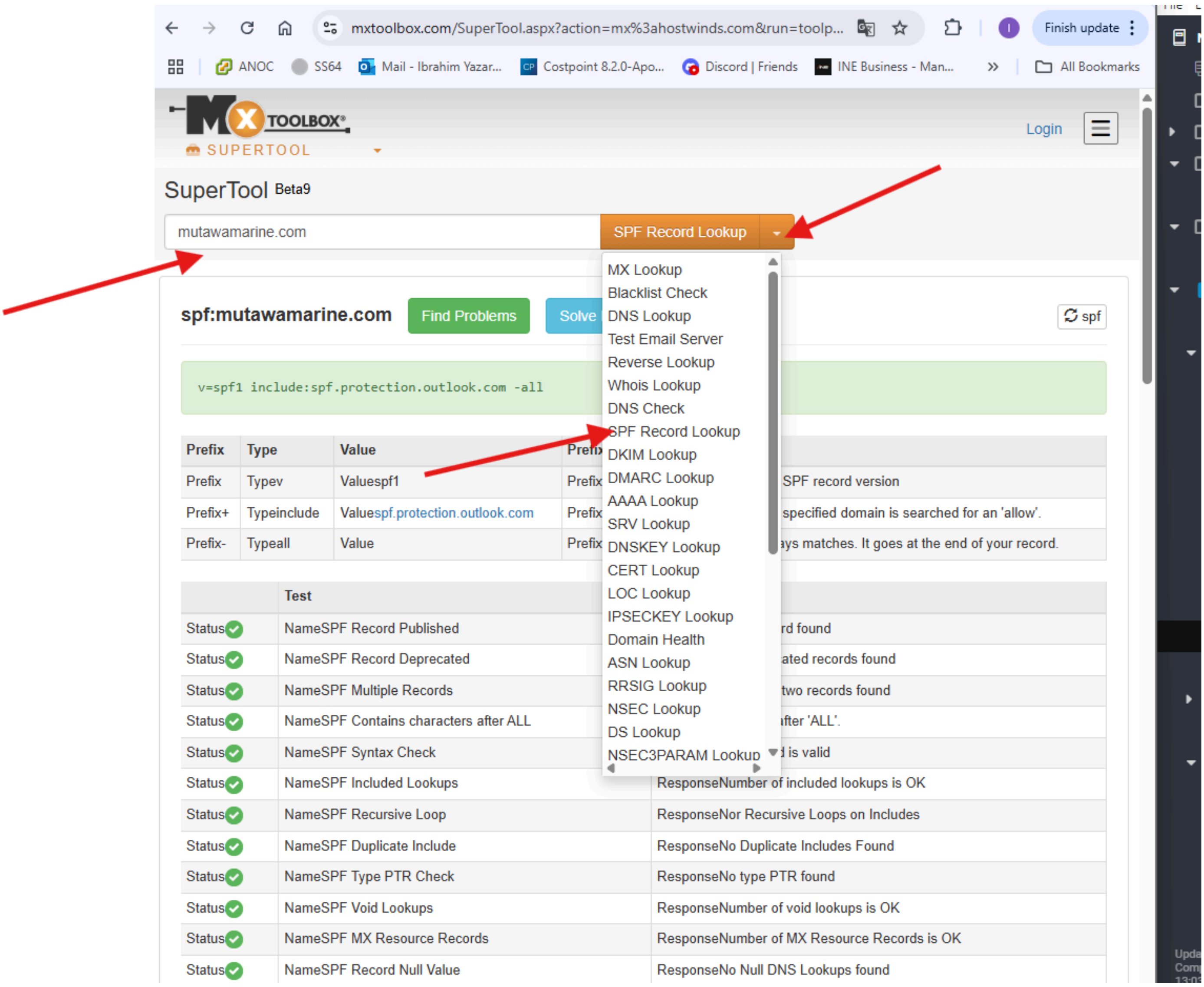
```
NetRange:       192.119.64.0 - 192.119.127.255
CIDR:           192.119.64.0/18
NetName:        HOSTWINDS-18-2
NetHandle:      NET-192-119-64-0-1
Parent:         NET192 (NET-192-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS54290
Organization:   Hostwinds LLC. (HL-29)
RegDate:        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/192.11
9.64.0

OrgName:        Hostwinds LLC.
OrgId:          HL-29
Address:        12101 Tukwila International Blvd, 3rd Fl
oor, Suite 320
City:           Seattle
StateProv:      WA
PostalCode:     98168
Country:        US
RegDate:        2011-11-30
Updated:        2024-11-25
Comment:        https://www.hostwinds.com
Comment:        Abuse Contact: abuse@hostwinds.com
```

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

Go to MXtool box https://mxtoolbox.com/ copy and pasted the domain name


Source of: file:///home/ubuntu/Desktop/challenge.eml?type=application/x-message-display - Mozi
File
Edit
View
Help

```
X-Atlas-Received: from 10.201.192.162 by atlas125.free.mail.bf1.yahoo.com with http; Wed, 10 Jun 2020 05:58:5
Return-Path: <info@mutawamarine.com>
Received: from x.x.x.x (EHLO sub.redacted.com)
 by atlas125.free.mail.bf1.yahoo.com with SMTPs; Wed, 10 Jun 2020 05:58:55 +0000
X-Originating-Ip: [x.x.x.x]
Received-SPF: fail (domain of mutawamarine.com does not designate x.x.x.x as permitted sender)
Authentication-Results: atlas125.free.mail.bf1.yahoo.com;
 spf=fail smtp.mailfrom=mutawamarine.com;
 dmarc=unknown
X-Apparently-To: redacted@yahoo.com; Wed, 10 Jun 2020 05:58:55 +0000
X-YMailISG: CA2XOWoWLDuMav_xVT1F_okXM35Y6SWpmP6zsE6LeQRxoxw4
 YjzuEZUWxEEJzHhUGbKbpzCq7GFztoIFDbqKMkWunxnYA6aofbh6xusqm_FJ
 x591PPWDY5NhvW7H.Pwb9o9VmzNhbgKs3KzMN9IO7Uh5jf5y6rUw.dSshjuv
 j1RgxZYshquA.RCedSbTlM1pyxBT4LoSfMkWr0E4FgJSW3l9zg8wK35sizWP
 GqFHAyID0v.GOU7dBURvMp8asqQiPa4kYC7v0oQTvmUEDtENPAjmCnfcajpo
 gei5zs471gDrr3JWxiUMUTyChHRw9nCczLepgGA2Jt_MdbCZ7qgFqWMvvo1I
 nIXkl35mwKec90ZCIPJc6tCHAQyFkE.030_.0VmK_brmLt5oqQiGBYmyCV2i
 CwhdwdTwYkUIdgler50ESBs5mHXSqnNvtmpQoRjMPdqSXiB7yvSIFaiF5rQ8
 OTEw0w1CkWz4gxhNU4FH4Iub03b9TLvUoX9KLEFx3Del5yPTF8xXY7NY_kzA
 aCwKTjp4FaeT2Mk1Pq5P48DF.dB6hdMTmCoowuSwouW2M9Yp4euqKNzGrlcf
 2KcRMROfFVcKDwXSaHw4tMhKvXSH0KiWMVFpXPaMmt2c0cklVpwZMyql8w8W
 PlponB1e66yiIqNuYV.vt64i52HFh0jNwcuuohMo7MA7DmMP.OtkdwLlUqLS
 68AfikwfW3Sppf_pTqtP6NPf2wuAsJIaT7_QQ.4x3khgYrC4jTmXjVBWDVRV
 wT0AdlQ716U8TVp.0AKvevKfMzfZoTOTsGLuQU.w8uZhv_6mwKB4sW7Pbhbr
 B1RJadC0va2CJiCbAC1Qnapm5egSIExqkhboy8iOUfzOqkD1a1_tn5nv1IxD
 bCqerO7cnAjpN1amfUvC8gjD345qb6k9l7h7a8TFsv_67Nkrok_.M4_MRZcf
 .iuxPcffE2r1ocaSfWQg6yof0WQta51sbWQidg7B_4XR2_6cbg8Ui39t2v2Y
 bgWISohtB1urfpr.b1SANr7fvE2Zzvzjz4_4PbBtBDevFUB7Pjq0GiAe_Nx_
 YpW8pLoFasyi1k4T9f5e5ryqAu.HToIegVimVa4xwuzjbNvaE7Tsm4m3vepb
 zGZI1BWuDLQ-
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=mutawamarine.com)
    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
```



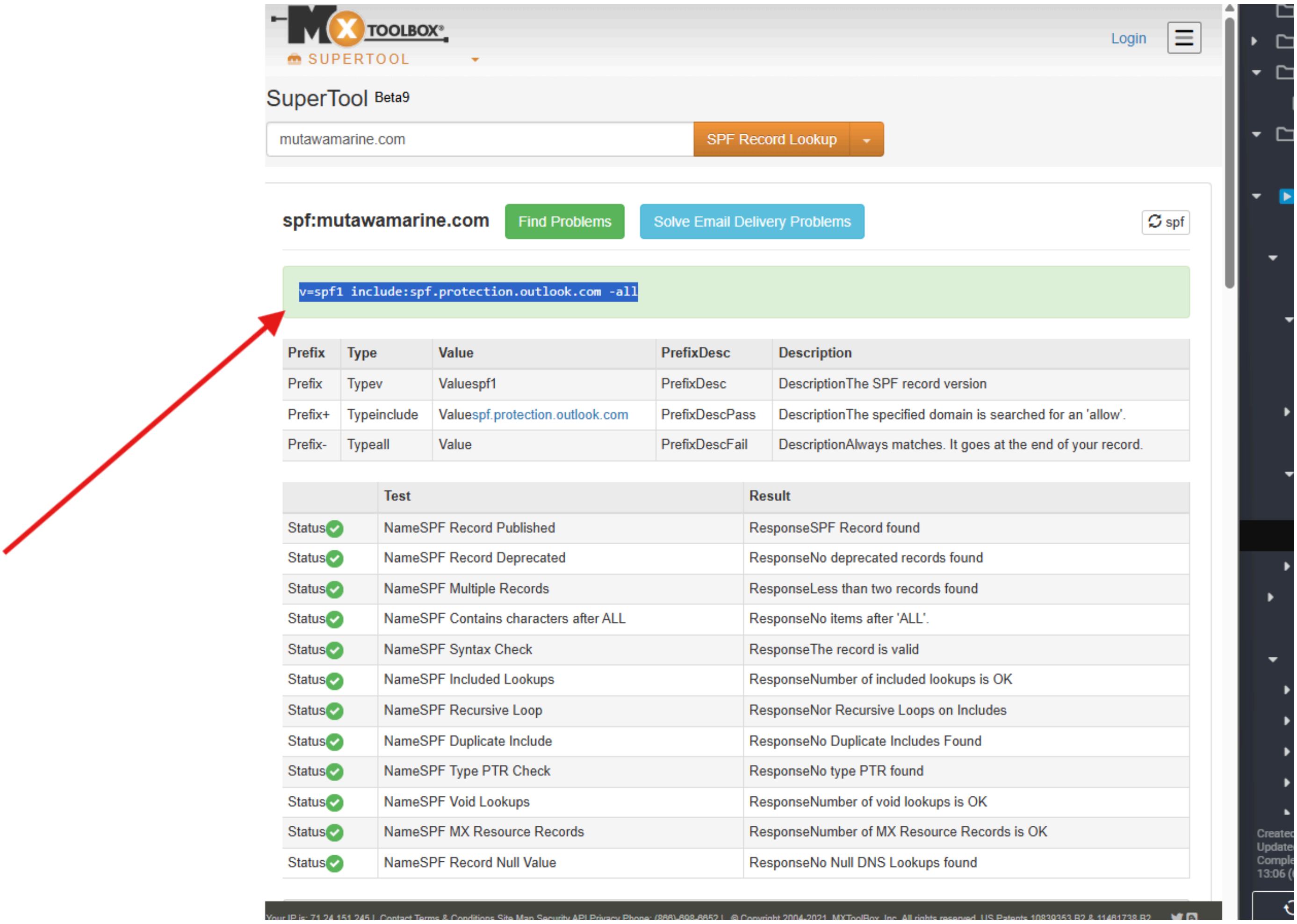
mutawamarine.com

spf:mutawamarine.com

```
v=spf1 include:spf.protection.outlook.com -all
```

Prefix	Type	Value	Prefix	
Prefix	Typev	Valuespf1	Prefix	SPF record version
Prefix+	Typeinclude	Valuespf.protection.outlook.com	Prefix	specified domain is searched for an 'allow'.
Prefix-	Typeall	Value	Prefix	ays matches. It goes at the end of your record.

	Test	
Status✓	NameSPF Record Published	rd found
Status✓	NameSPF Record Deprecated	ated records found
Status✓	NameSPF Multiple Records	two records found
Status✓	NameSPF Contains characters after ALL	after 'ALL'.
Status✓	NameSPF Syntax Check	d is valid
Status✓	NameSPF Included Lookups	ResponseNumber of included lookups is OK
Status✓	NameSPF Recursive Loop	ResponseNor Recursive Loops on Includes
Status✓	NameSPF Duplicate Include	ResponseNo Duplicate Includes Found
Status✓	NameSPF Type PTR Check	ResponseNo type PTR found
Status✓	NameSPF Void Lookups	ResponseNumber of void lookups is OK
Status✓	NameSPF MX Resource Records	ResponseNumber of MX Resource Records is OK
Status✓	NameSPF Record Null Value	ResponseNo Null DNS Lookups found



```
v=spf1 include:spf.protection.outlook.com -all
```

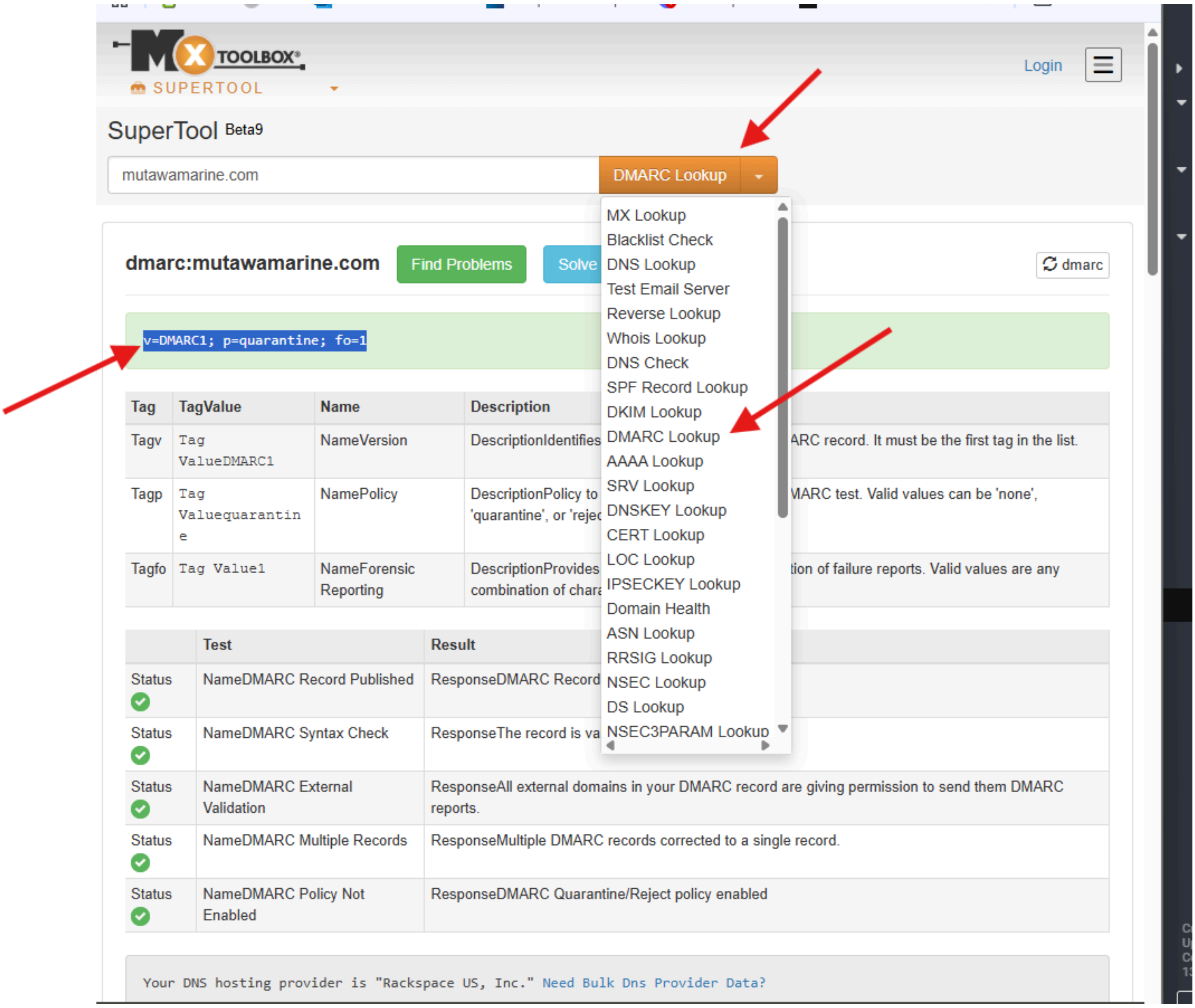
Prefix	Type	Value	PrefixDesc	Description
Prefix	Typev	Valuespf1	PrefixDesc	DescriptionThe SPF record version
Prefix+	Typeinclude	Valuespf.protection.outlook.com	PrefixDescPass	DescriptionThe specified domain is searched for an 'allow'.
Prefix-	Typeall	Value	PrefixDescFail	DescriptionAlways matches. It goes at the end of your record.

	Test	Result
Status✓	NameSPF Record Published	ResponseSPF Record found
Status✓	NameSPF Record Deprecated	ResponseNo deprecated records found
Status✓	NameSPF Multiple Records	ResponseLess than two records found
Status✓	NameSPF Contains characters after ALL	ResponseNo items after 'ALL'.
Status✓	NameSPF Syntax Check	ResponseThe record is valid
Status✓	NameSPF Included Lookups	ResponseNumber of included lookups is OK
Status✓	NameSPF Recursive Loop	ResponseNor Recursive Loops on Includes
Status✓	NameSPF Duplicate Include	ResponseNo Duplicate Includes Found
Status✓	NameSPF Type PTR Check	ResponseNo type PTR found
Status✓	NameSPF Void Lookups	ResponseNumber of void lookups is OK
Status✓	NameSPF MX Resource Records	ResponseNumber of MX Resource Records is OK
Status✓	NameSPF Record Null Value	ResponseNo Null DNS Lookups found

Your IP is: 71.24.151.245 | Contact Terms & Conditions Site Map Security API Privacy Phone: (866)-698-6652 | © Copyright 2004-2021, MXToolBox, Inc. All rights reserved. US Patents 10839353 B2 & 11461738 B2
Createc
Update
Comple
13:06 (

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

Same steps with SPF but this time select DMARC on drop box



SuperTool Beta9

mutawamarine.com | DMARC Lookup

dmarc:mutawamarine.com Find Problems Solve dmarc

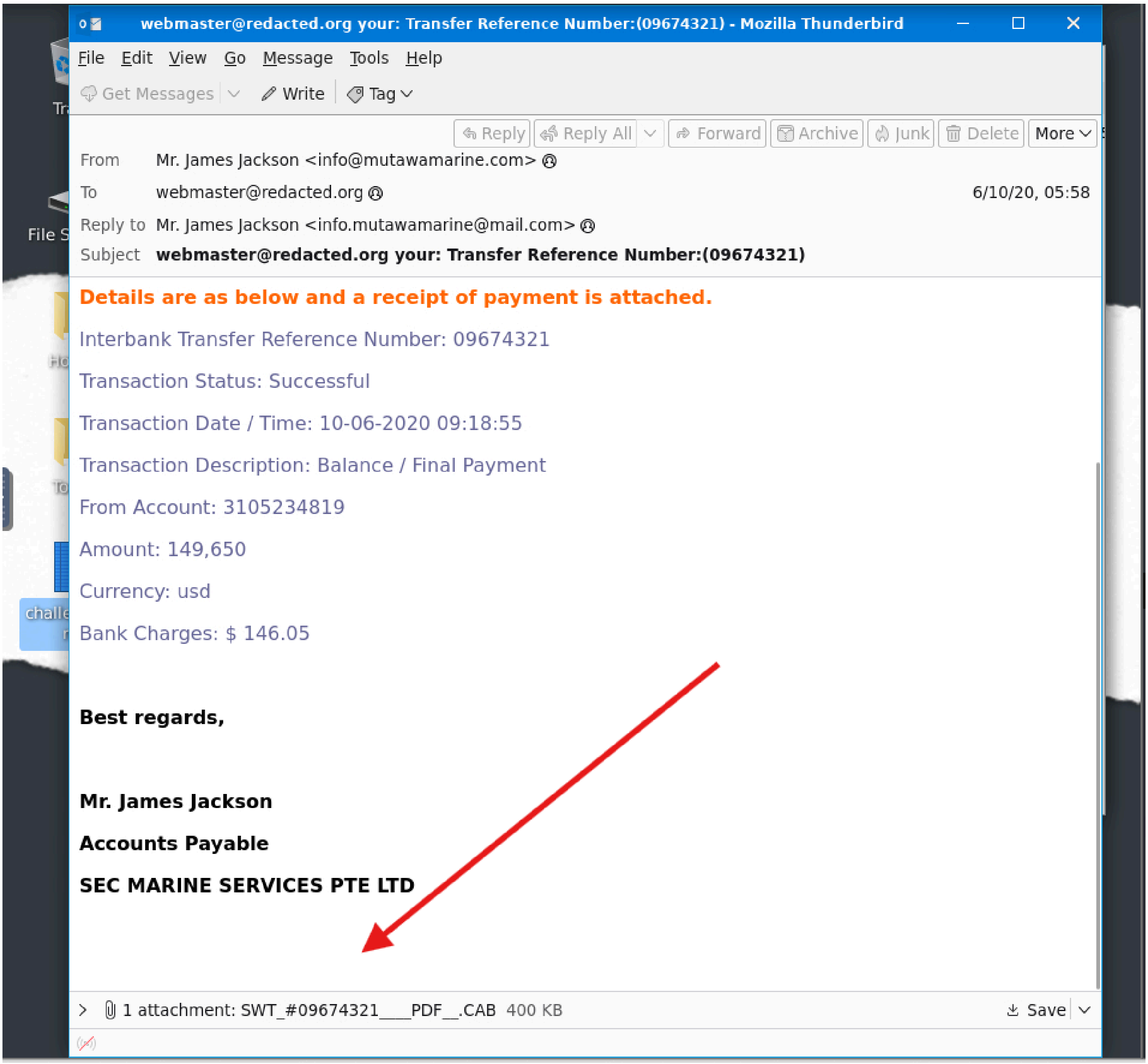
```
v=DMARC1; p=quarantine; fo=1
```

Tag	TagValue	Name	Description
Tagv	Tag ValueDMARC1	NameVersion	DescriptionIdentifies ARC record. It must be the first tag in the list.
Tagp	Tag Valuequarantine	NamePolicy	DescriptionPolicy to MARC test. Valid values can be 'none', 'quarantine', or 'rejec
Tagfo	Tag Value1	NameForensic Reporting	DescriptionProvides tion of failure reports. Valid values are any combination of chara

	Test	Result
Status ✓	NameDMARC Record Published	ResponseDMARC Record
Status ✓	NameDMARC Syntax Check	ResponseThe record is va
Status ✓	NameDMARC External Validation	ResponseAll external domains in your DMARC record are giving permission to send them DMARC reports.
Status ✓	NameDMARC Multiple Records	ResponseMultiple DMARC records corrected to a single record.
Status ✓	NameDMARC Policy Not Enabled	ResponseDMARC Quarantine/Reject policy enabled

```
Your DNS hosting provider is "Rackspace US, Inc." Need Bulk Dns Provider Data?
```

What is the name of the attachment?



webmaster@redacted.org your: Transfer Reference Number:(09674321) - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Tag
Reply
Reply All
Forward
Archive
Junk
Delete
More
Save

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

To webmaster@redacted.org

6/10/20, 05:58

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

Subject **webmaster@redacted.org your: Transfer Reference Number:(09674321)**

Details are as below and a receipt of payment is attached.

Interbank Transfer Reference Number: 09674321

Transaction Status: Successful

Transaction Date / Time: 10-06-2020 09:18:55

Transaction Description: Balance / Final Payment

From Account: 3105234819

Amount: 149,650

Currency: usd

Bank Charges: $ 146.05

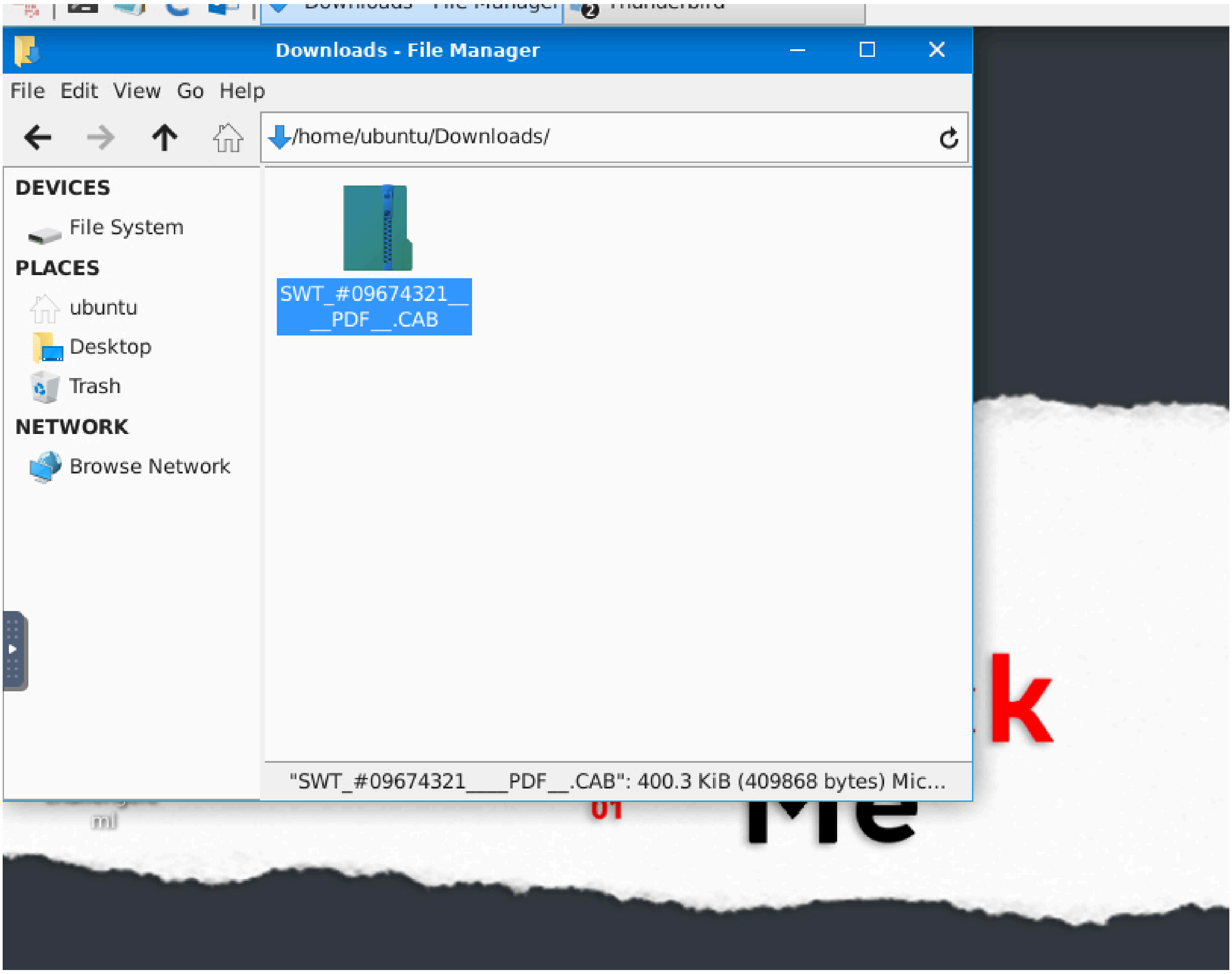
Best regards,

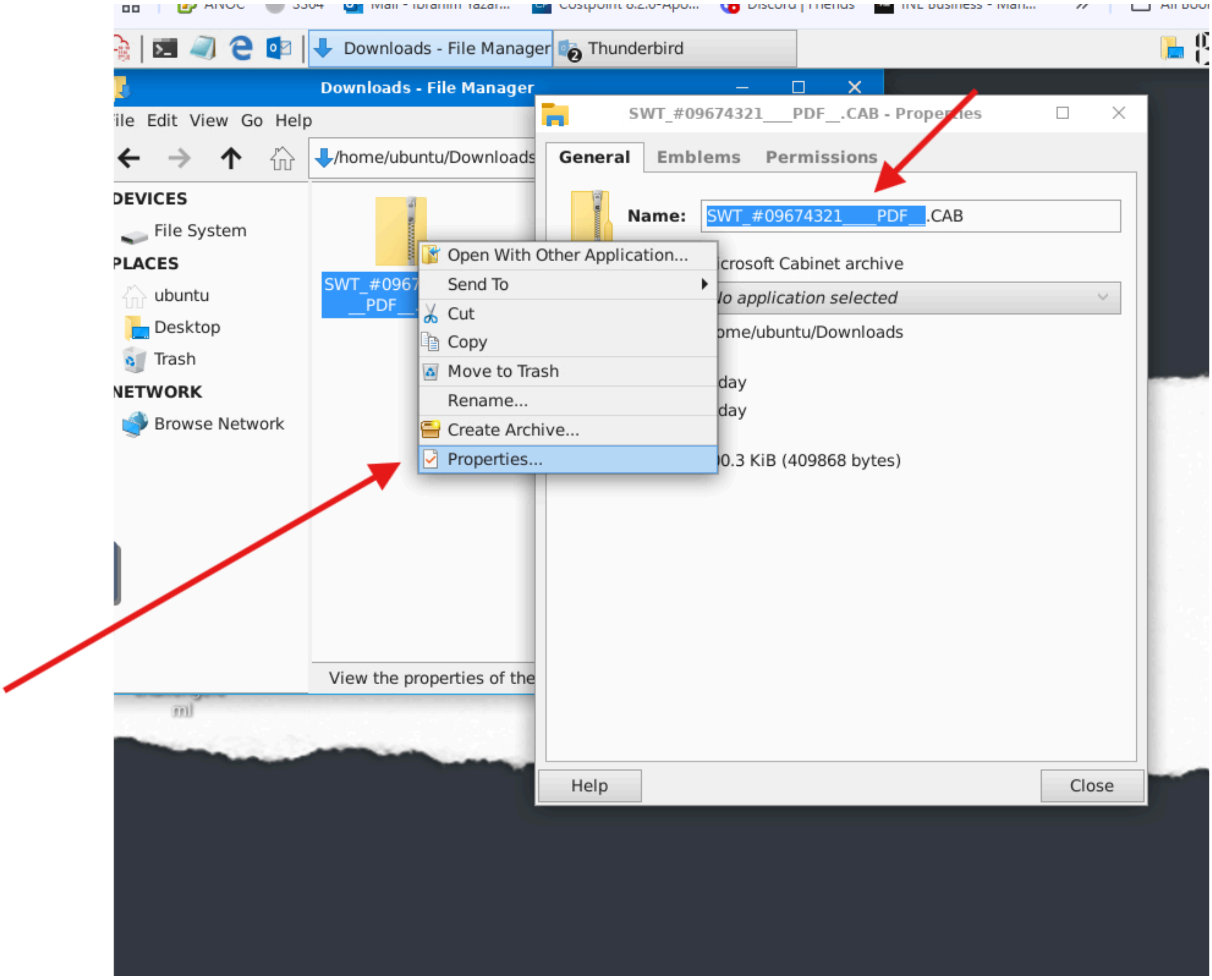
Mr. James Jackson

Accounts Payable

SEC MARINE SERVICES PTE LTD

1 attachment: SWT_#09674321___PDF__.CAB 400 KB





Name: SWT_#09674321___PDF__.CAB

icrosoft Cabinet archive

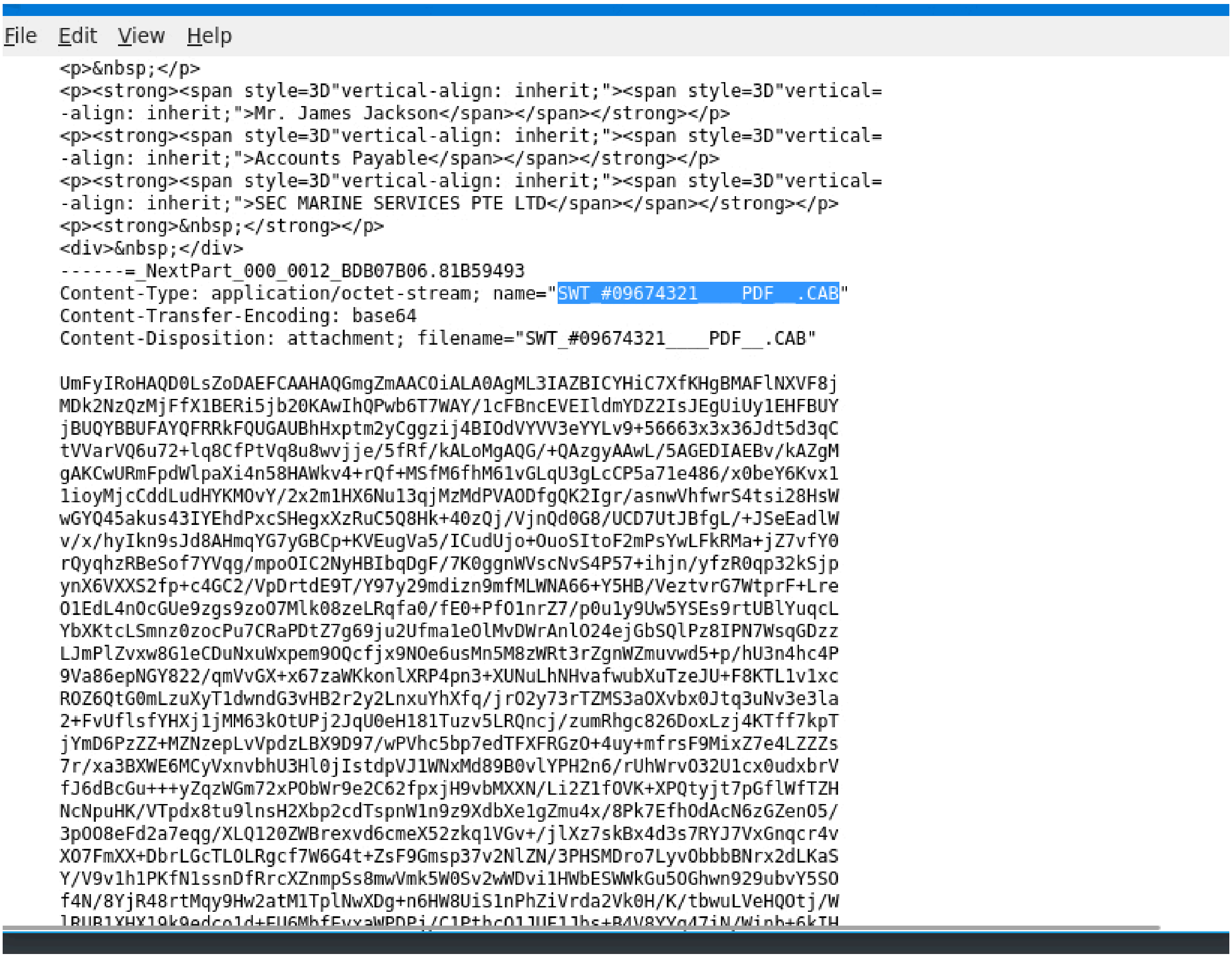
lo application selected

ome/ubuntu/Downloads

day

day

)0.3 KiB (409868 bytes)



```
<p>&nbsp;</p>
<p><strong><span style=3D"vertical-align: inherit;"><span style=3D"vertical=
-align: inherit;">Mr. James Jackson</span></span></strong></p>
<p><strong><span style=3D"vertical-align: inherit;"><span style=3D"vertical=
-align: inherit;">Accounts Payable</span></span></strong></p>
<p><strong><span style=3D"vertical-align: inherit;"><span style=3D"vertical=
-align: inherit;">SEC MARINE SERVICES PTE LTD</span></span></strong></p>
<p><strong>&nbsp;</strong></p>
<div>&nbsp;</div>
------=_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"
```

```
UmFyIRoHAQD0LsZoDAEFCAAHAQGmgZmAACOiALA0AgML3IAZBICYHiC7XfKHgBMAFlNXVF8j
MDk2NzQzMjFfX1BERi5jb20KAwIhQPwb6T7WAY/1cFBncEVEIldmYDZ2IsJEgUiUy1EHFBUY
jBUQYBBUFAYQFRRkFQUGAUBhHxptm2yCggzij4BIOdVYVV3eYYLv9+56663x3x36Jdt5d3qC
tVVarVQ6u72+lq8CfPtVq8u8wvjje/5fRf/kALoMgAQG/+QAzgyAAwL/5AGEDIAEBv/kAZgM
gAKCwURmFpdWlpaXi4n58HAWkv4+rQf+MSfM6fhM61vGLqU3gLcCP5a71e486/x0beY6Kvx1
1ioyMjcCddLudHYKMOvY/2x2m1HX6Nu13qjMzMdPVAODfgQK2Igr/asnwVhfwrS4tsi28HsW
wGYQ45akus43IYEhdPxcSHegxXzRuC5Q8Hk+40zQj/VjnQd0G8/UCD7UtJBfgL/+JSeEadlW
v/x/hyIkn9sJd8AHmqYG7yGBCp+KVEugVa5/ICudUjo+OuoSItoF2mPsYwLFkRMa+jZ7vfY0
rQyqhzRBeSof7YVqg/mpoOIC2NyHBIbqDgF/7K0ggnWVscNvS4P57+ihjn/yfzR0qp32kSjp
ynX6VXXS2fp+c4GC2/VpDrtdE9T/Y97y29mdizn9mfMLWNA66+Y5HB/VeztvrG7WtprF+Lre
O1EdL4nOcGUe9zgs9zoO7Mlk08zeLRqfa0/fE0+PfO1nrZ7/p0u1y9Uw5YSEs9rtUBlYuqcL
YbXKtcLSmnz0zocPu7CRaPDtZ7g69ju2Ufma1eOlMvDWrAnlO24ejGbSQlPz8IPN7WsqGDzz
LJmPlZvxw8G1eCDuNxuWxpem9OQcfjx9NOe6usMn5M8zWRt3rZgnWZmuvwd5+p/hU3n4hc4P
9Va86epNGY822/qmVvGX+x67zaWKkonlXRP4pn3+XUNuLhNHvafwubXuTzeJU+F8KTL1v1xc
ROZ6QtG0mLzuXyT1dwndG3vHB2r2y2LnxuYhXfq/jrO2y73rTZMS3aOXvbx0Jtq3uNv3e3la
2+FvUflsfYHXj1jMM63kOtUPj2JqU0eH181Tuzv5LRQncj/zumRhgc826DoxLzj4KTff7kpT
jYmD6PzZZ+MZNzepLvVpdzLBX9D97/wPVhc5bp7edTFXFRGzO+4uy+mfrsF9MixZ7e4LZZZs
7r/xa3BXWE6MCyVxnvbhU3Hl0jIstdpVJ1WNxMd89B0vlYPH2n6/rUhWrvO32U1cx0udxbrV
fJ6dBcGu+++yZqzWGm72xPObWr9e2C62fpxjH9vbMXXN/Li2Z1fOVK+XPQtyjt7pGflWfTZH
NcNpuHK/VTpdx8tu9lnsH2Xbp2cdTspnW1n9z9XdbXe1gZmu4x/8Pk7EfhOdAcN6zGZenO5/
3pOO8eFd2a7eqg/XLQ120ZWBrexvd6cmeX52zkq1VGv+/jlXz7skBx4d3s7RYJ7VxGnqcr4v
XO7FmXX+DbrLGcTLOLRgcf7W6G4t+ZsF9Gmsp37v2NlZN/3PHSMDro7LyvObbbBNrx2dLKaS
Y/V9v1h1PKfN1ssnDfRrcXZnmpSs8mwVmk5W0Sv2wWDvi1HWbESWWkGu5OGhwn929ubvY5SO
f4N/8YjR48rtMqy9Hw2atM1TplNwXDg+n6HW8UiS1nPhZiVrda2Vk0H/K/tbwuLVeHQOtj/W
lRUB1XHX19k9edco1d+FU6MbfFvxaWPDPj/C1PthcO1JUF1Jhs+B4V8YYq47iN/Winh+6kTH
```

What is the SHA256 hash of the file attachment?

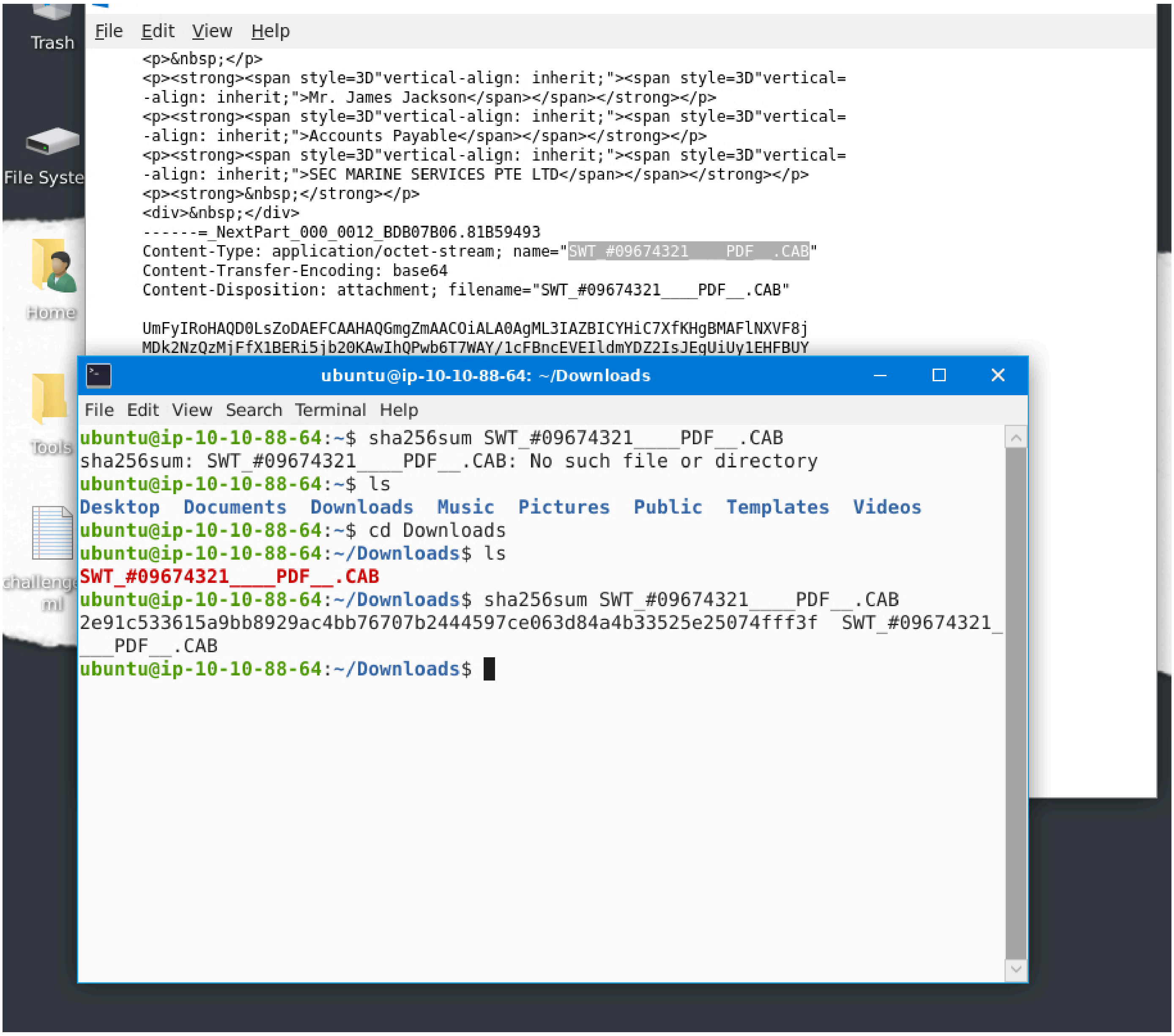
sha256sum SWT_#09674321___*PDF*_.CAB

sha256sum <file>

md5sum <file>

sha1sum <file>

sha512sum <file>

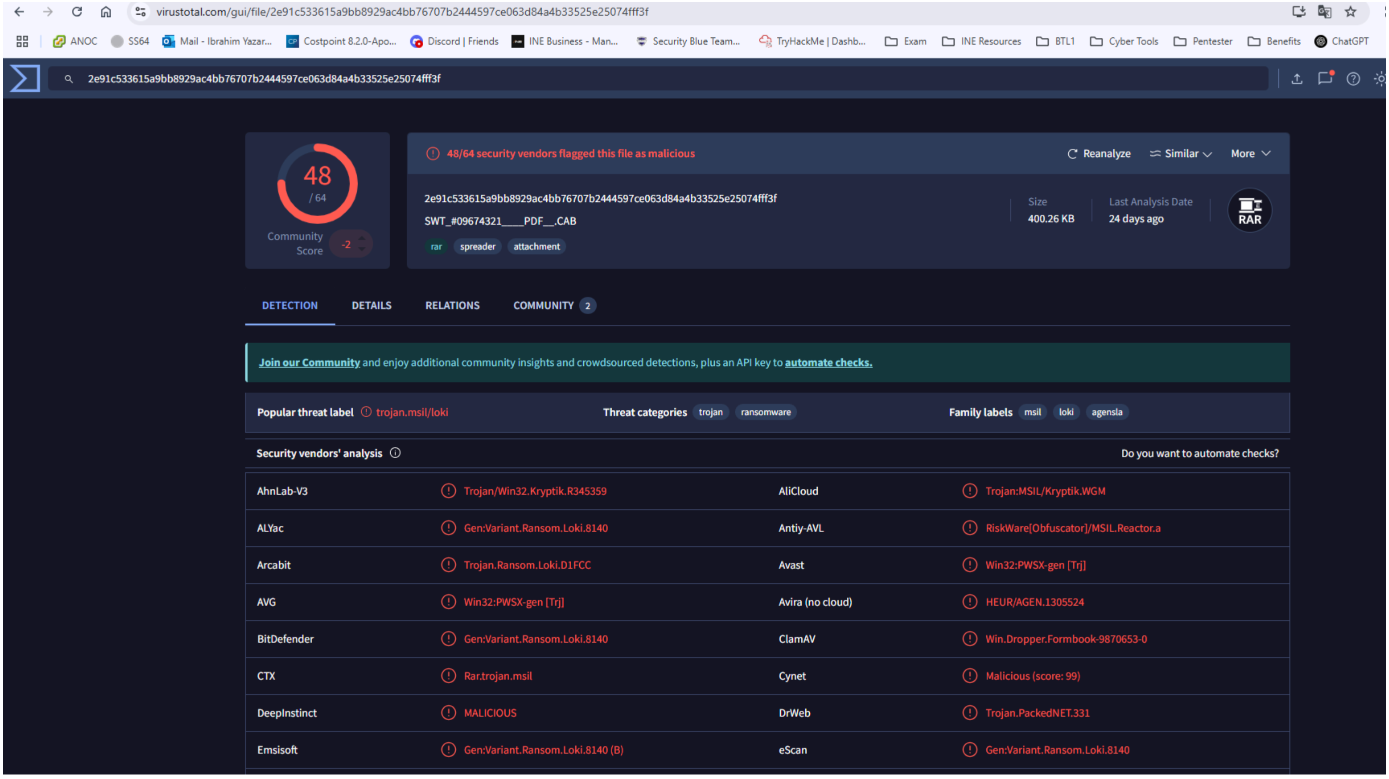


```
<p>&nbsp;</p>
<p><strong><span style=3D"vertical-align: inherit;"><span style=3D"vertical=
-align: inherit;">Mr. James Jackson</span></span></strong></p>
<p><strong><span style=3D"vertical-align: inherit;"><span style=3D"vertical=
-align: inherit;">Accounts Payable</span></span></strong></p>
<p><strong><span style=3D"vertical-align: inherit;"><span style=3D"vertical=
-align: inherit;">SEC MARINE SERVICES PTE LTD</span></span></strong></p>
<p><strong>&nbsp;</strong></p>
<div>&nbsp;</div>
------=_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"
```

UmFyIRoHAQD0LsZoDAEFCAAHAQGmgZmAACOiALA0AgML3IAZBICYHiC7XfKHgBMAFlNXVF8j
MDk2NzQzMjFfX1BERi5jb20KAwIhQPwb6T7WAY/1cFBncEVEIldmYDZ2IsJEqUiUy1EHFBUY

ubuntu@ip-10-10-88-64: ~/Downloads
File Edit View Search Terminal Help

```
ubuntu@ip-10-10-88-64:~$ sha256sum SWT_#09674321____PDF__.CAB
sha256sum: SWT_#09674321____PDF__.CAB: No such file or directory
ubuntu@ip-10-10-88-64:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
ubuntu@ip-10-10-88-64:~$ cd Downloads
ubuntu@ip-10-10-88-64:~/Downloads$ ls
SWT_#09674321____PDF__.CAB
ubuntu@ip-10-10-88-64:~/Downloads$ sha256sum SWT_#09674321____PDF__.CAB
2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f  SWT_#09674321_
___PDF__.CAB
ubuntu@ip-10-10-88-64:~/Downloads$ 
```



48/64 security vendors flagged this file as malicious

2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f

SWT_#09674321____PDF__.CAB

rar spreader attachment

Size 400.26 KB

Last Analysis Date 24 days ago

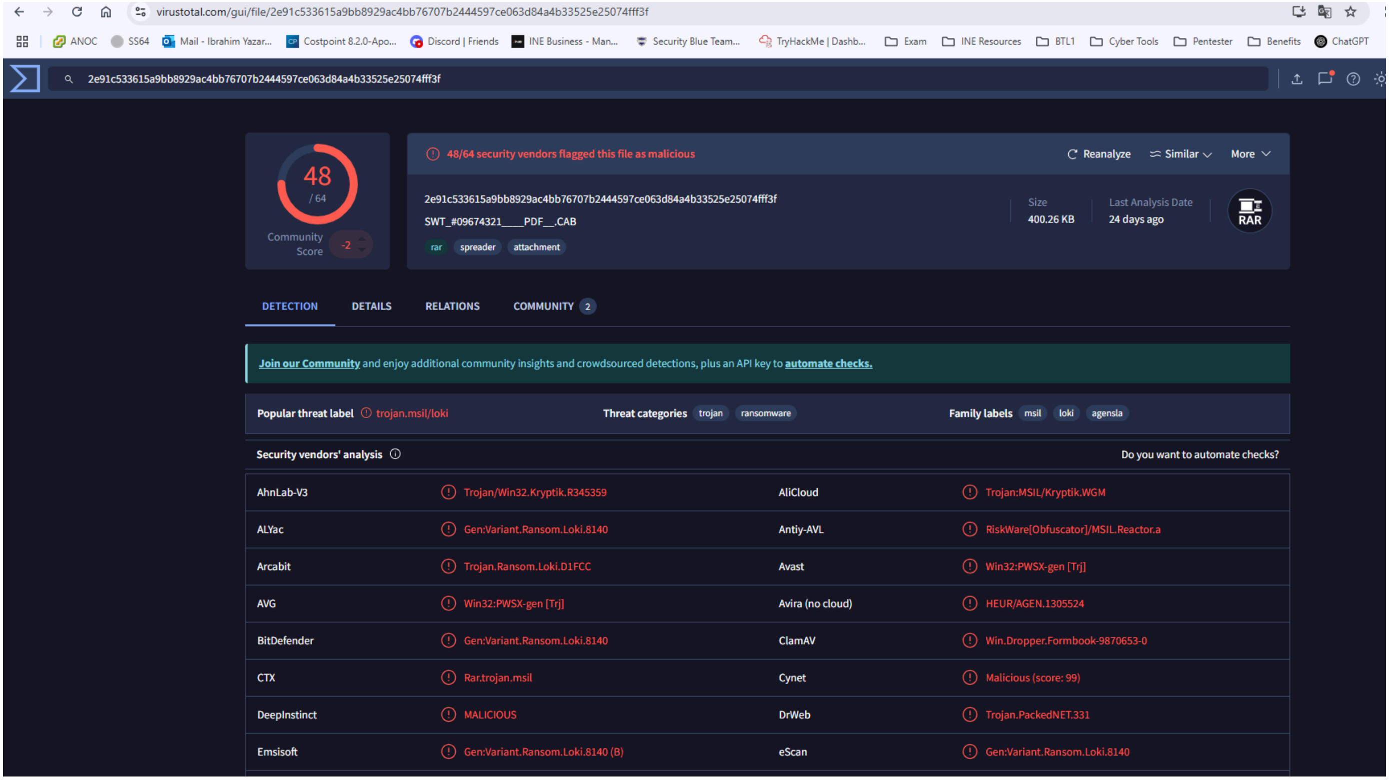
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.msil/loki Threat categories trojan ransomware Family labels msil loki agensla

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Kryptik.R345359	AliCloud	Trojan:MSIL/Kryptik.WGM
ALYac	Gen:Variant.Ransom.Loki.8140	Antiy-AVL	RiskWare[Obfuscator]/MSIL.Reactor.a
Arcabit	Trojan.Ransom.Loki.D1FCC	Avast	Win32:PWSX-gen [Trj]
AVG	Win32:PWSX-gen [Trj]	Avira (no cloud)	HEUR/AGEN.1305524
BitDefender	Gen:Variant.Ransom.Loki.8140	ClamAV	Win.Dropper.Formbook-9870653-0
CTX	Rar.trojan.msil	Cynet	Malicious (score: 99)
DeepInstinct	MALICIOUS	DrWeb	Trojan.PackedNET.331
Emsisoft	Gen:Variant.Ransom.Loki.8140 (B)	eScan	Gen:Variant.Ransom.Loki.8140

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



48/64 security vendors flagged this file as malicious

2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f

SWT_#09674321____PDF__.CAB

rar spreader attachment

Size 400.26 KB

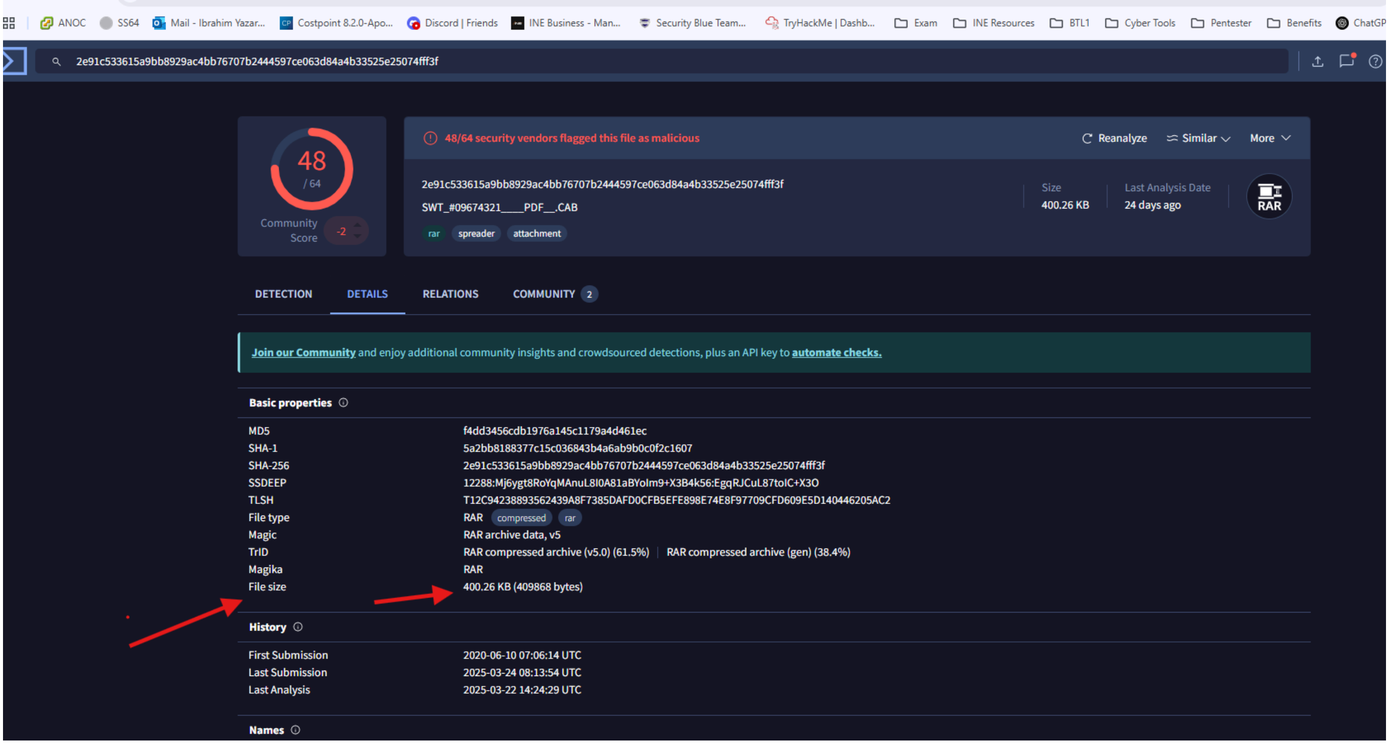
Last Analysis Date 24 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.msil/loki — Threat categories trojan ransomware — Family labels msil loki agensla

Security vendors' analysis — Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Kryptik.R345359	AliCloud	Trojan:MSIL/Kryptik.WGM
ALYac	Gen:Variant.Ransom.Loki.8140	Antiy-AVL	RiskWare[Obfuscator]/MSIL.Reactor.a
Arcabit	Trojan.Ransom.Loki.D1FCC	Avast	Win32:PWSX-gen [Trj]
AVG	Win32:PWSX-gen [Trj]	Avira (no cloud)	HEUR/AGEN.1305524
BitDefender	Gen:Variant.Ransom.Loki.8140	ClamAV	Win.Dropper.Formbook-9870653-0
CTX	Rar.trojan.msil	Cynet	Malicious (score: 99)
DeepInstinct	MALICIOUS	DrWeb	Trojan.PackedNET.331
Emsisoft	Gen:Variant.Ransom.Loki.8140 (B)	eScan	Gen:Variant.Ransom.Loki.8140



48/64 security vendors flagged this file as malicious

2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f

SWT_#09674321____PDF__.CAB

rar spreader attachment

Size 400.26 KB

Last Analysis Date 24 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

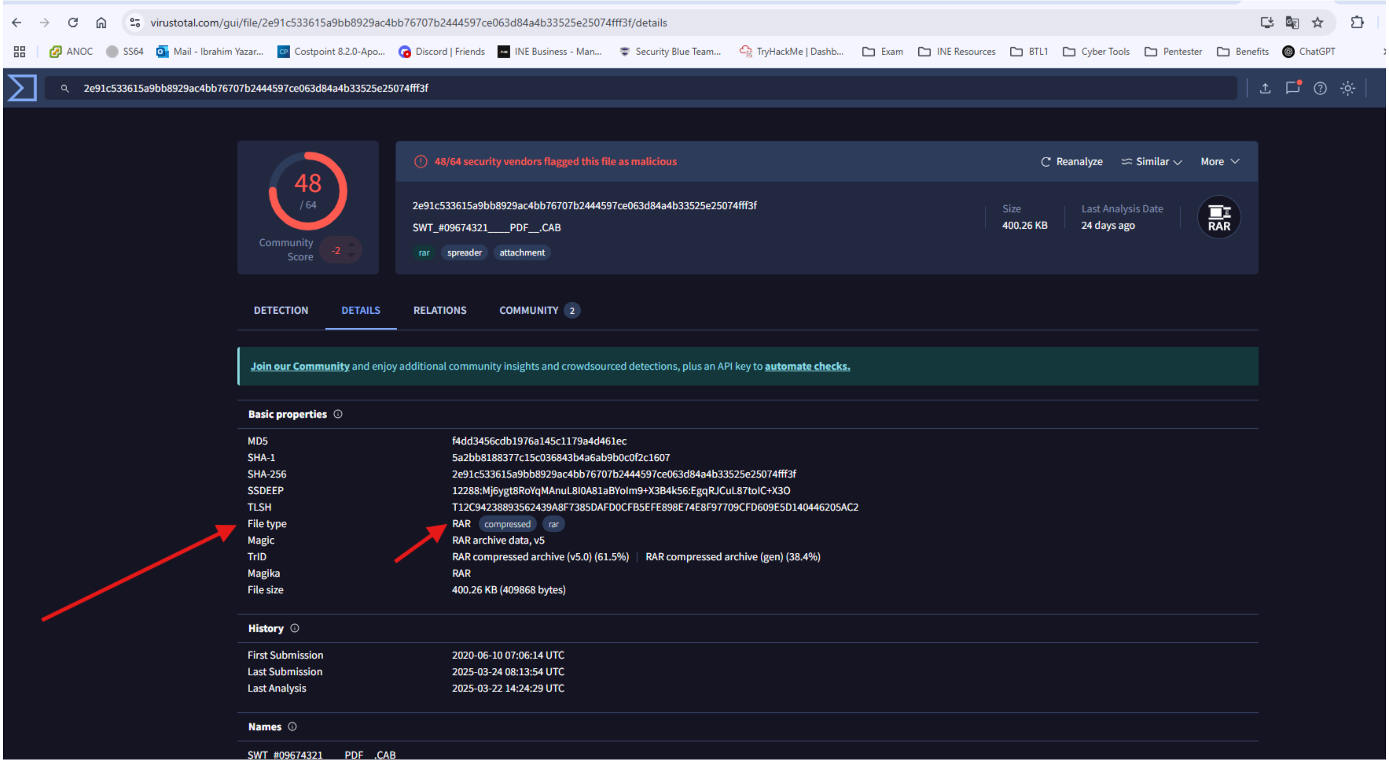
MD5	f4dd3456cdb1976a145c1179a4d461ec
SHA-1	5a2bb8188377c15c036843b4a6ab9b0c0f2c1607
SHA-256	2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f
SSDEEP	12288:Mj6ygt8RoYqMAnuL8I0A81aBYoIm9+X3B4k56:EgqRJCuL87toIC+X3O
TLSH	T12C94238893562439A8F7385DAFD0CFB5EFE898E74E8F97709CFD609E5D140446205AC2
File type	RAR compressed rar
Magic	RAR archive data, v5
TrID	RAR compressed archive (v5.0) (61.5%) | RAR compressed archive (gen) (38.4%)
Magika	RAR
File size	400.26 KB (409868 bytes)

History

First Submission	2020-06-10 07:06:14 UTC
Last Submission	2025-03-24 08:13:54 UTC
Last Analysis	2025-03-22 14:24:29 UTC

Names

What is the actual file extension of the attachment?



48/64 security vendors flagged this file as malicious

2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f

SWT_#09674321____PDF__.CAB

rar spreader attachment

Size 400.26 KB

Last Analysis Date 24 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

MD5	f4dd3456cdb1976a145c1179a4d461ec
SHA-1	5a2bb8188377c15c036843b4a6ab9b0c0f2c1607
SHA-256	2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f
SSDEEP	12288:Mj6ygt8RoYqMAnuL8I0A81aBYoIm9+X3B4k56:EgqRJCuL87toIC+X3O
TLSH	T12C94238893562439A8F7385DAFD0CFB5EFE898E74E8F97709CFD609E5D140446205AC2
File type	RAR compressed rar
Magic	RAR archive data, v5
TrID	RAR compressed archive (v5.0) (61.5%) | RAR compressed archive (gen) (38.4%)
Magika	RAR
File size	400.26 KB (409868 bytes)

History

First Submission	2020-06-10 07:06:14 UTC
Last Submission	2025-03-24 08:13:54 UTC
Last Analysis	2025-03-22 14:24:29 UTC

Names

SWT_#09674321___PDF__.CAB