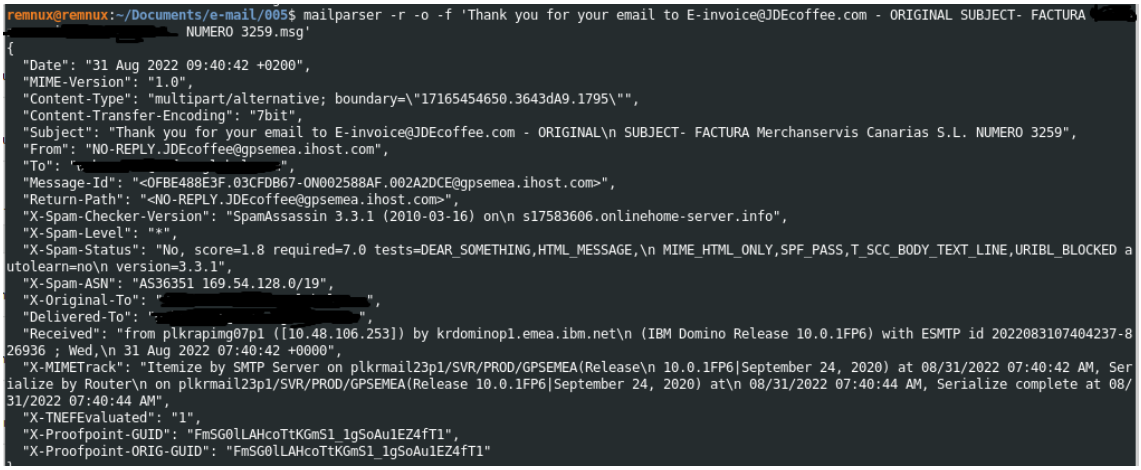
ANÁLISIS FORENSE – E-MAIL - CASO 06

Nos llega un mail un tanto sospechoso con fichero adjunto

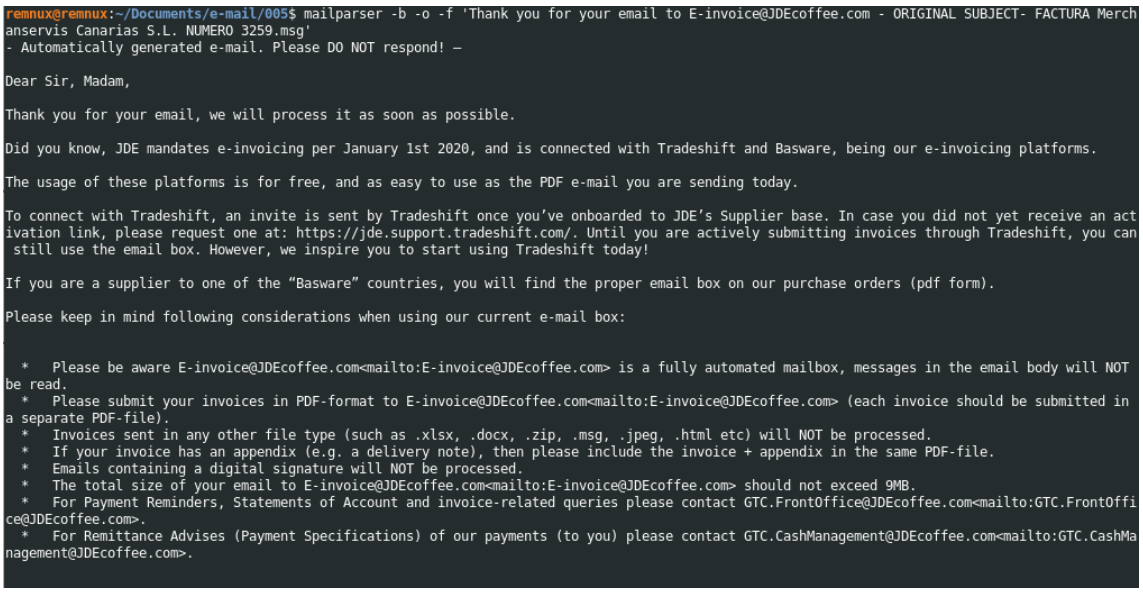
Analizamos el correo en formato eml con la herramienta mailparser, bbtenemos la información de la cabecera del correo:

mailparser -r -o -f ‘‘Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL SUBJECT- FACTURA XXXXXXXX S.L. NUMERO 3259.msg’



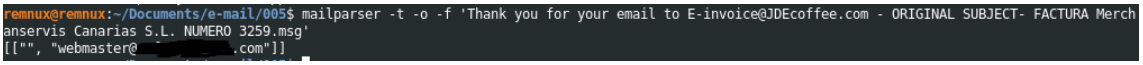
Leemos el cuerpo del mensaje

mailparser -b -o -f ‘‘Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL SUBJECT- FACTURA XXXXXXXX S.L. NUMERO 3259.msg’



Leemos el destinatario del correo

mailparser -t -o -f ‘‘Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL SUBJECT- FACTURA XXXXXXXX S.L. NUMERO 3259.msg’



Leemos el remitente del correo

mailparser -m -o -f ‘'Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL SUBJECT- FACTURA XXXXXXXX S.L. NUMERO 3259.msg’

```
remnux@remnux:~/Documents/e-mail/005$ mailparser -m -o -f 'Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL SUBJECT- FACTURA Merch
anservis Canarias S.L. NUMERO 3259.msg'
[["", "NO-REPLY.JDEcoffee@gpsemea.ihost.com"]]
```

Vemos el asunto del correo

mailparser -u -o -f ‘'Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL SUBJECT- FACTURA XXXXXXXX S.L. NUMERO 3259.msg’

```
remnux@remnux:~/Documents/e-mail/005$ mailparser -u -o -f 'Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL SUBJECT- FACTURA Merch
anservis Canarias S.L. NUMERO 3259.msg'
Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL
 SUBJECT- FACTURA Merchanservis Canarias S.L. NUMERO 3259
```

Exportamos todos los ficheros adjuntos en el correo

mailparser -sa -ap ./ -o -f 'Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL SUBJECT- FACTURA Merchanservis Canarias S.L. NUMERO 3259.msg'

```
remnux@remnux:~/Documents/e-mail/005$ mailparser -sa -ap ./ -o -f 'Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL SUBJECT- FACTU
RA Merchanservis Canarias S.L. NUMERO 3259.msg'
remnux@remnux:~/Documents/e-mail/005$ ls -al
total 72
drwxrwxr-x 2 remnux remnux  4096 may 24 07:15  .
drwxrwxr-x 7 remnux remnux  4096 may 24 06:07  ..
-rw-rw-r-- 1 remnux remnux 10853 may 24 07:15  eozoaxvyza.rtf
-rwxrwxrwx 1 remnux remnux 53248 may 21 02:48 'Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL SUBJECT- FACTURA Merchanservis Can
arias S.L. NUMERO 3259.msg'
```

Vemos que se ha generado un document en formato rtf

Analizamos el tipo de fichero

file eozoaxvyza.rtf

```
remnux@remnux:~/Documents/e-mail/005$ file eozoaxvyza.rtf
eozoaxvyza.rtf: Rich Text Format data, version 1, ANSI
```

Analizamos el fichero por si tiene algún documento incrustado

rtfobj eozoaxvyza.rtf

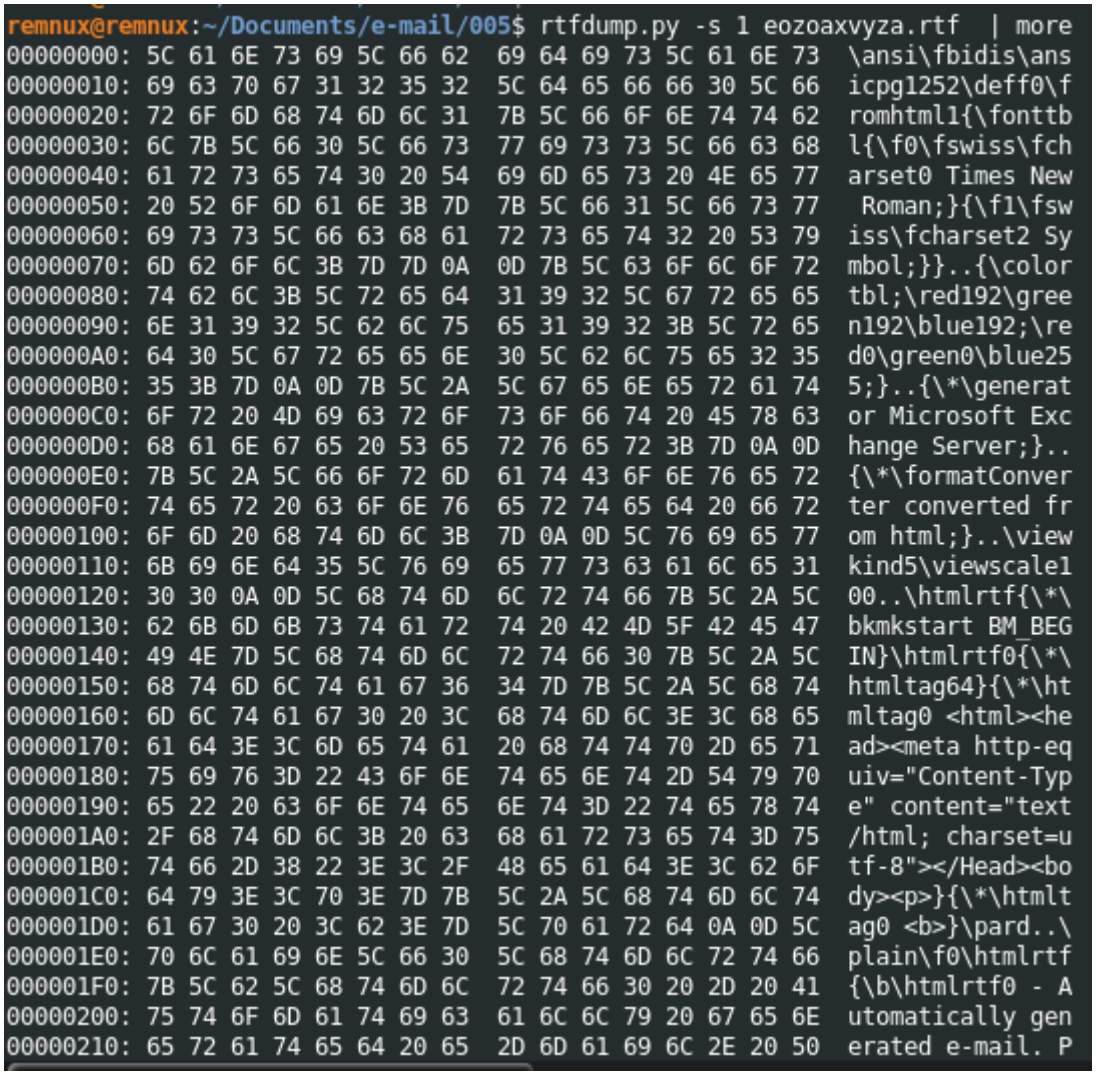
```
remnux@remnux:~/Documents/e-mail/005$ rtfobj eozoaxvyza.rtf
rtfobj 0.60.1 on Python 3.8.10 - http://decalage.info/python/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

===============================================================================
File: 'eozoaxvyza.rtf' - size: 10853 bytes
---+----------+-----------------------------------------------------------
id |index     |OLE Object
---+----------+-----------------------------------------------------------
```

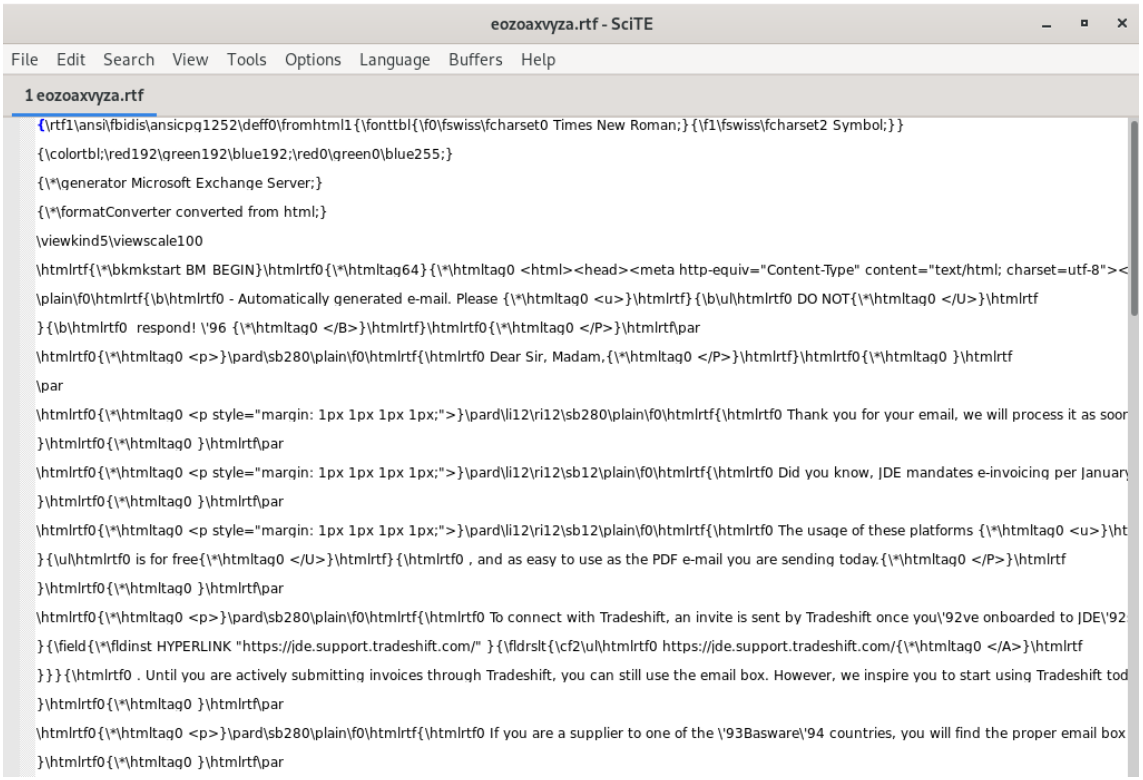
No contiene ningún objecto incrustado malicioso

Mostramos el contenido del fichero rtf

rtfdump.py -s 1 eozoaxvyza.rtf



Abrimos el fichero con un visor de texto



Software:

Remmux

Aplicación:

emlAnalyzer

Mailparser

Rtfdump

Rtfobj

Fuente:

Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL SUBJECT- FACTURA Merchanservis Canarias S.L. NUMERO 3259.zip