ESTUDIO DEL PROTOCOLO SMTP y POP-3 CON WIRESHARK

Grupo: Martín Gómez, Julio Prado, Daniel Plazas

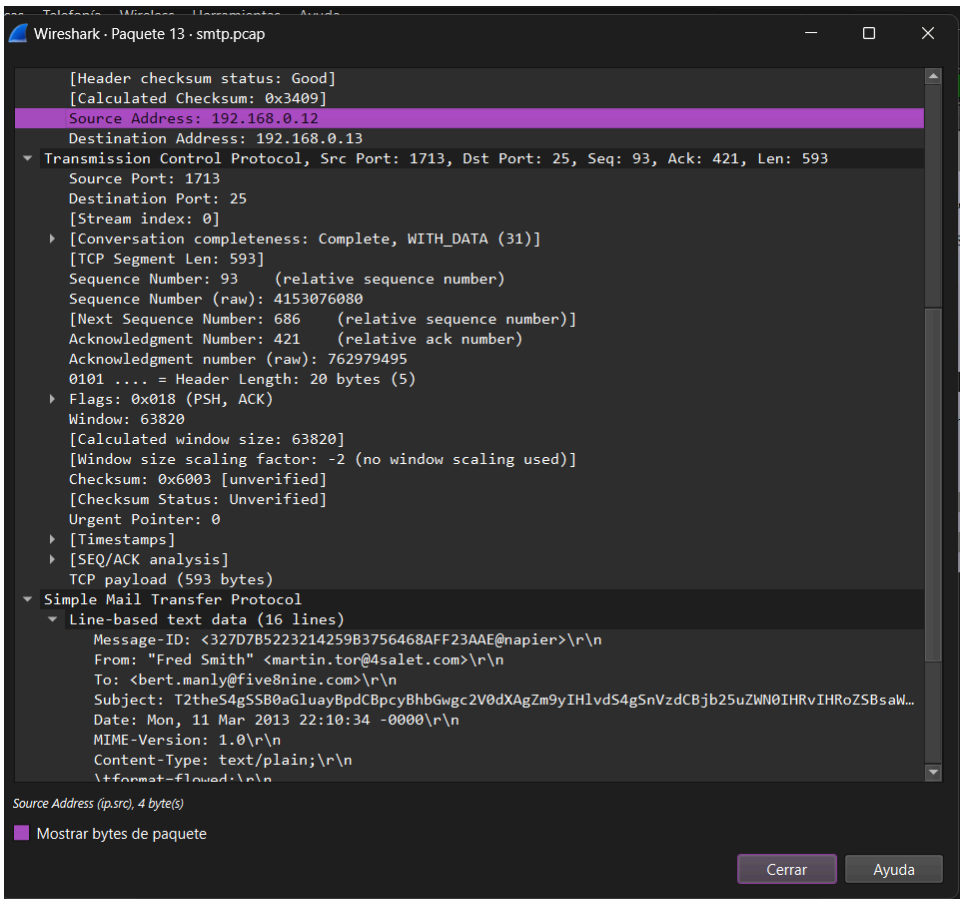
En este taller estudiaremos el funcionamiento de los protocolos SMTP y POP-3, mediante algunas capturas con Wireshark. Proceda de la siguiente manera:

SMTP

Descargue el siguiente archivo y ábralo con wireshark: smtp.zip

Conteste las siguientes preguntas con respecto a la captura:

1. ¿Cuál es la dirección IP y el puerto TCP utilizado por el host que está enviando el correo electrónico?

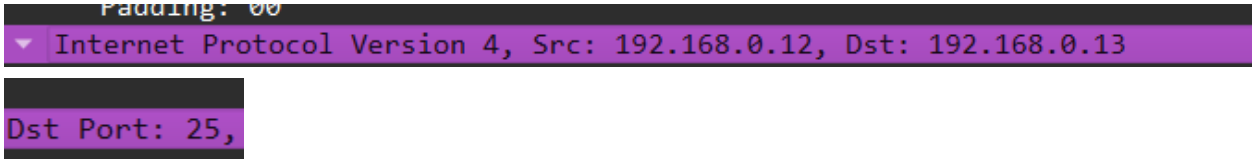


El paquete anterior debe tener como ip de origen la del host interesado en enviar el correo. Esto debido a que su payload incluye información, como el asunto, que solamente puede ser dada por el que quiere enviar el correo.

IP: 192.168.0.12

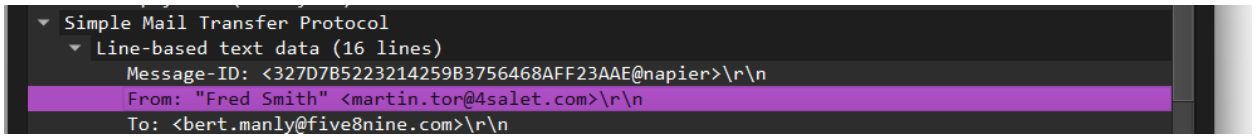
PUERTO: 1731

2. ¿Cuál es la dirección IP y el puerto TCP utilizado por el servidor SMTP?



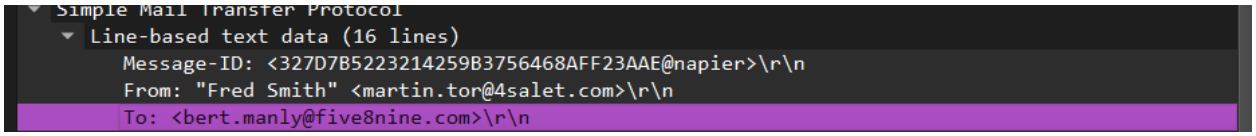
IP:192.168.0.13
PUERTO:25

3. ¿Quién envía el correo electrónico?



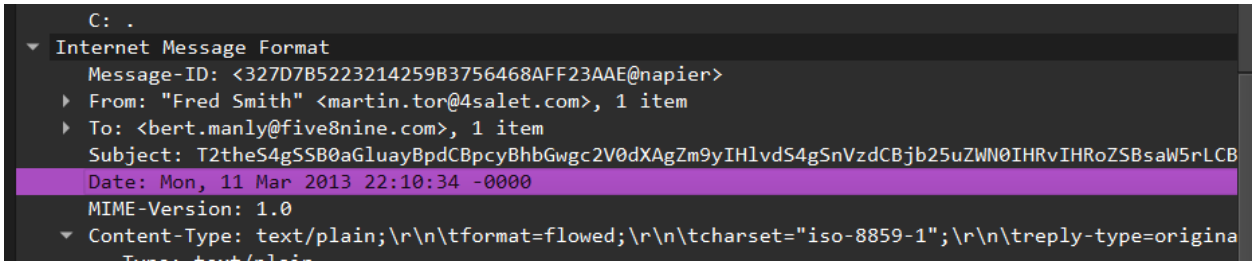
Nombre: Fren Smith
Correo: martin.tor@4salet.com

4. ¿Quién recibe el correo electrónico?



Correo:"bert.manly@five8nine.com

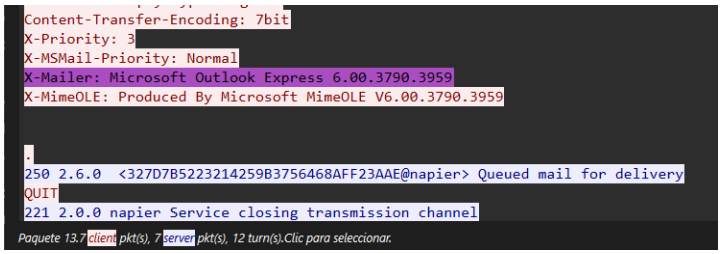
5. ¿Cuándo se envió el correo electrónico?



Fecha: Mon, 11 Mar 2013 22:10:34 -0000

6. ¿Cuál es el cliente utilizado para enviar el correo electrónico?

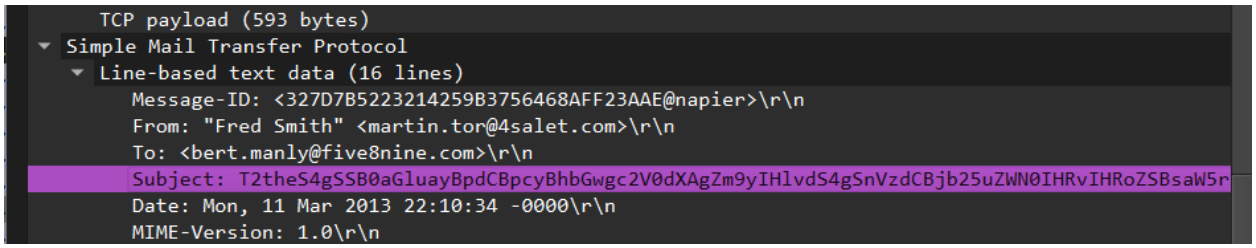
De acuerdo a una búsqueda rápida en internet, en el contexto de SMTP, un cliente de correo electrónico hace referencia a un programa que puedes usar para enviar, recibir y gestionar tus correos. (https://es.wikipedia.org/wiki/Cliente_de_correo_electr%C3%B3nico)
En este caso.



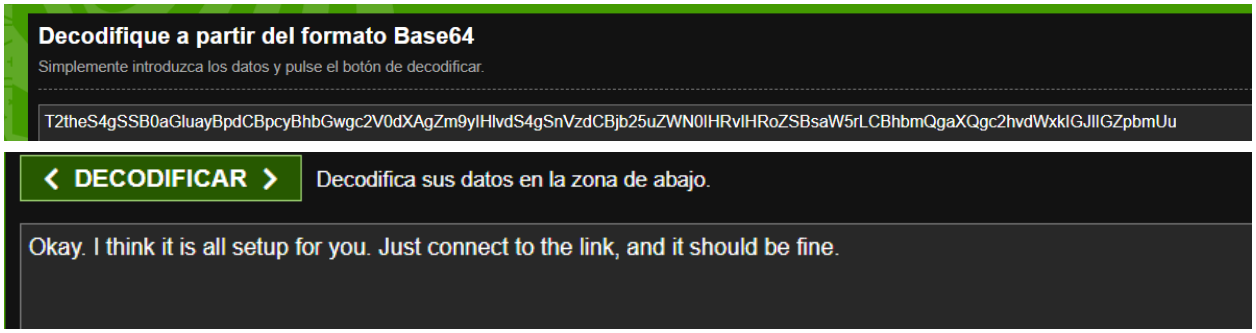
Se ve un campo que dice X-Mailer. Este, precisamente, indica el software utilizado. Podemos ver dice Microsoft Outlook Express, por ende, es este el cliente de correo electrónico utilizado.

7. ¿Cuál es el asunto y el mensaje del correo electrónico?

El campo del asunto estaba codificado en base 64.



Si usamos una pagina que decodifica esto, obtenemos que

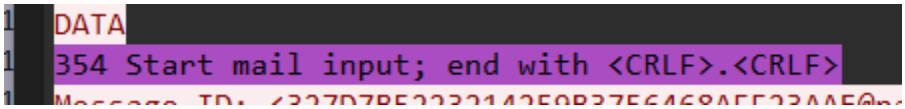


Asunto:Okay. I think it is all setup for you. Just connect to the link, and it should be fine.

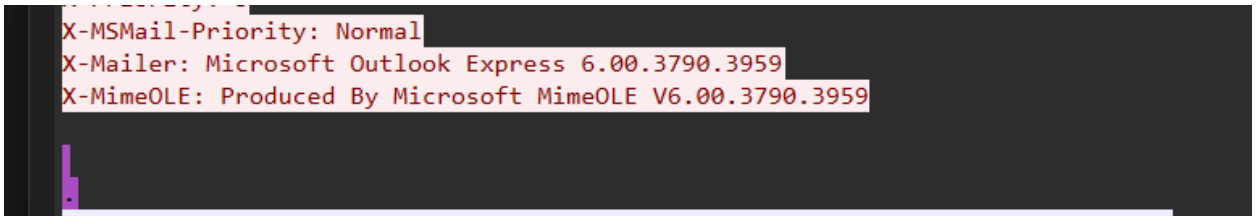
Por otro lado, aparentemente el mensaje no tiene contenido. No hay nada en la comunicación tcp que nos indique eso.

8. ¿Qué carácter especial utiliza SMTP para terminar el mensaje?

El servidor envió un mensaje con este contenido.



El cliente finalizó su mensaje de esta forma.



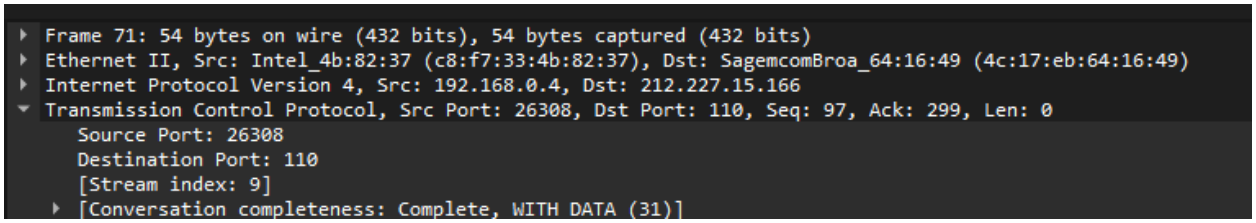
Por tanto, el carácter especial utilizado debe ser el punto (.) .

POP-3

Descargue el siguiente archivo y ábralo con wireshark: pop3.zip

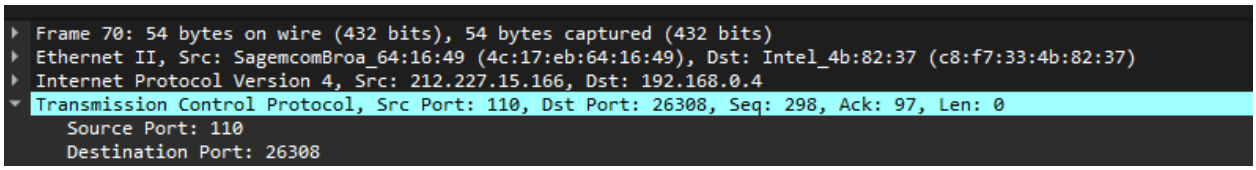
Conteste las siguientes preguntas con respecto a la captura:

1. ¿Cuál es la dirección IP y el puerto TCP utilizado por el host que está enviando el correo electrónico?



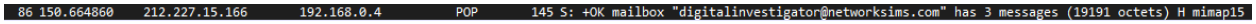
La ip es 192.168.0.4, y el puerto es 26308

2. ¿Cuál es la dirección IP y el puerto TCP utilizado por el servidor POP-3?



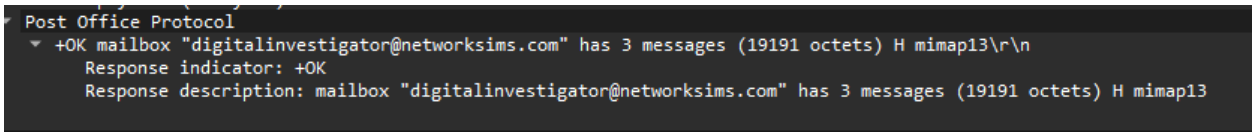
La ip es 212.227.15.166, y está utilizando el puerto 110.

3. ¿Qué buzón de correo se está accediendo?



Se esta accediendo al buzón de correo de digitalinvestigator@networksims.com.

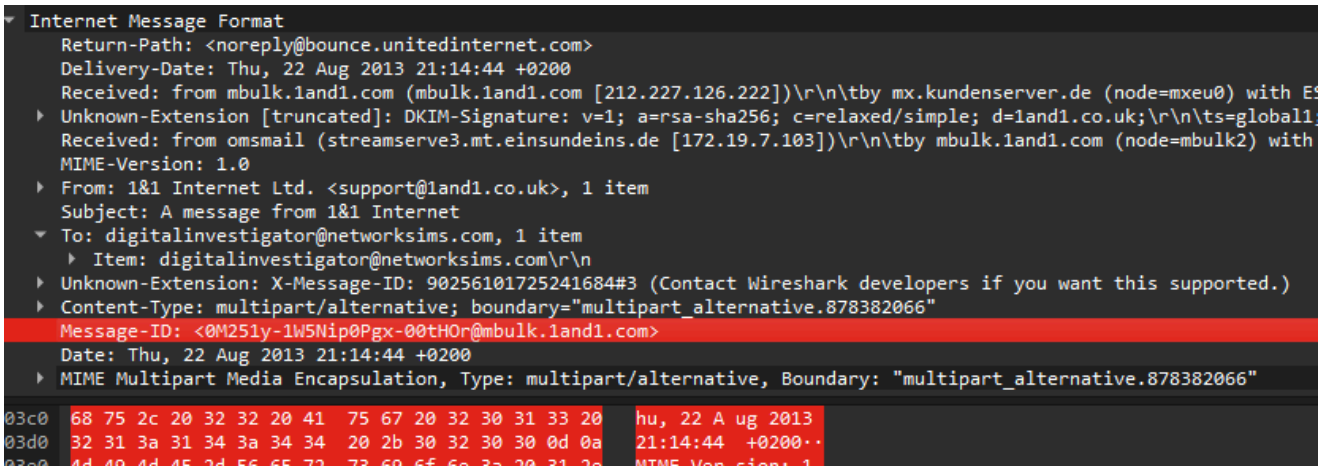
4. ¿Cuántos mensajes hay en la bandeja de entrada?



Hay 3 mensajes en la bandeja de entrada.

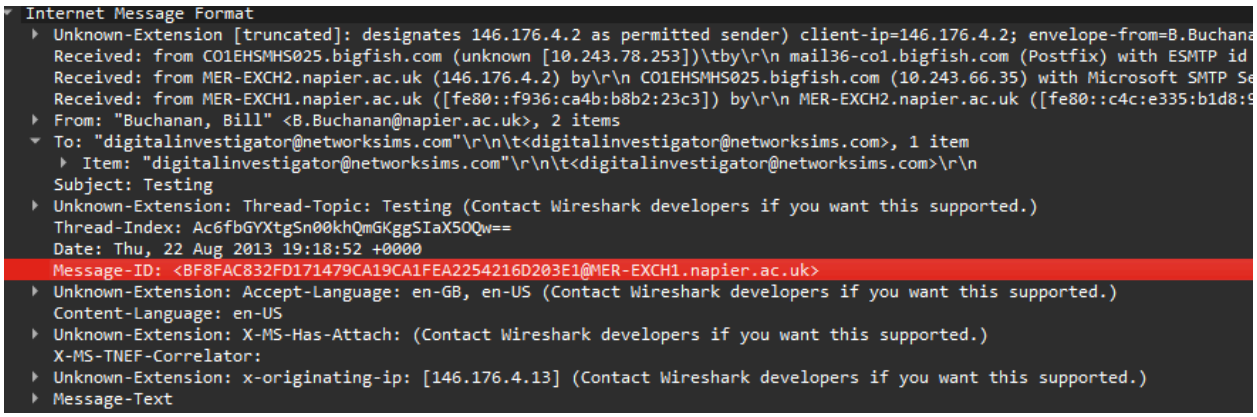
5. Indique los identificadores de cada uno de los mensajes.

Mensaje1:



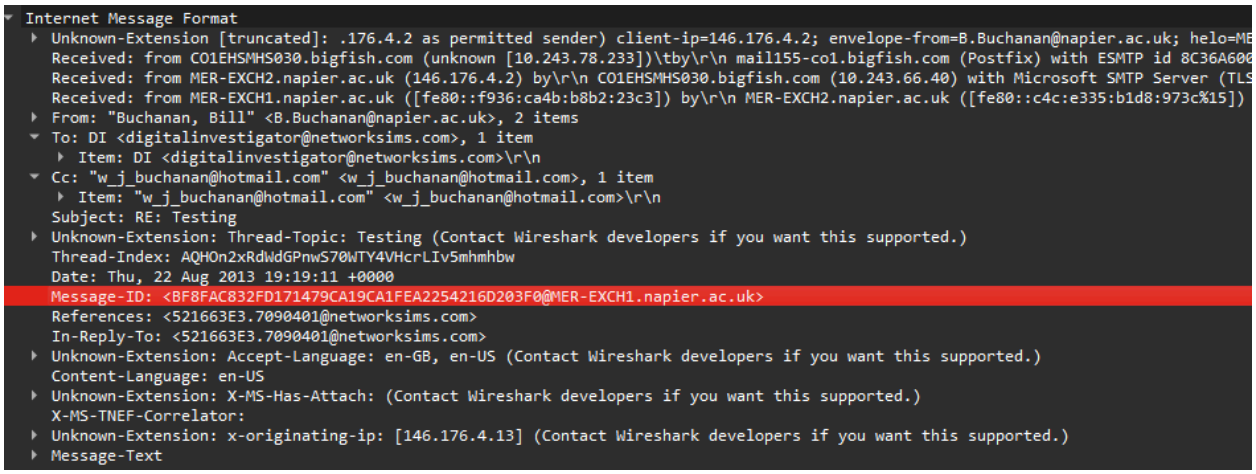
Message-ID: <0M251y-1W5Nip0Pgx-00tHOr@mbulk.1and1.com>

Mensaje 2:



Message-ID: <BF8FAC832FD171479CA19CA1FEA2254216D203E1@MER-EXCH1.napier.ac.uk>

Mensaje 3:



Message-ID: <BF8FAC832FD171479CA19CA1FEA2254216D203F0@MER-EXCH1.napier.ac.uk>

6. Para cada uno de los mensajes establezca quién los envió, cuál es el asunto y su contenido.

Mensaje 1:

Enviado por:

```
▸ From: 1&1 Internet Ltd. <support@1and1.co.uk>, 1 item
```

Asunto:

```
Subject: A message from 1&1 Internet
```

Contenido:

```
▸ Unknown-Extension [truncated]: KY5D\r\n Z0e9QXdXccdaSZ6BR1UnVkOnC9JpU+1WQGrrAgWr
▾ Message-Text
    --multipart_alternative.878382066
    Content-Type: text/plain; charset=utf-8
    Content-Transfer-Encoding: quoted-printable

    Hello and welcome to your new e-mail account!

    Thank you for using 1&1 Internet e-mail services for your e-mail account.=
    =20
    We'd like to take this opportunity to tell you about a feature that is=20
    included in 1&1 e-mail services.=20

    WebMail 2.0
    -----------
    Which e-mail client are you using? Is it as flexible and easy to use as=20
    1&1 WebMail?

    Try WebMail today. You can reach your e-mail account from any browser=20
    and without installing any software.=20

    - Access to your e-mail from any browser. Log in to your account at
      https://email.1and1.co.uk
    - WebMail is an integral part of 1&1 e-mail services. There are no=20
      additional fees for using WebMail and there is no software to set up.
    - Keep track of your appointments with your calendar, auto-responder and=20
      password management directly accessible for each mailbox.=20
    - Professional and versatile layout which we've based on MailXchange,=20
      a communication and collaboration solution for businesses.
```

```
▼ Message-Text
    For help using WebMail please visit our FAQ:
    http://faq.1and1.co.uk/search/go.php?t=3Dn49907=20

    Enjoy the flexibility of using 1&1 WebMail as either your primary e-mail=20
    account or in addition to your local e-mail client.=20

    Best regards,

    Registered at Cardiff, Company number 3953678  - VAT No GB 752539027
    Aquasulis House, 10-14 Bath Road, Slough, Berkshire, SL1 3SA, United Kingdo=
    m

    --multipart_alternative.878382066
    Content-Type: text/html; charset=utf-8
    Content-Transfer-Encoding: quoted-printable

    <html>
    <body>
    Hello and welcome to your new e-mail account!
    <br/>
    <br/>
    Thank you for using 1&amp;amp;1 Internet e-mail services for=20
    your e-mail account. We'd like to take this opportunity
    to tell you about a feature that is included in 1&amp;amp;1=20
    e-mail services.=20
    <br/>
    <br/>
    WebMail 2.0
    <br/>-----------<br/>
    Which e-mail client are you using?
    Is it as flexible and easy to use as 1&amp;amp;1 WebMail?=20
    <br/>
    <br/>
    Try WebMail today. You can reach your e-mail account from=20
    any browser and without installing any software.=20
    <br/>
    <br/>
    <ul>
    <li>Access to your e-mail from any browser. Log in to your account at
    <a href=3D"https://email.1and1.co.uk">https://email.1and1.co.uk</a></li>
    <li>WebMail is an integral part of 1&amp;amp;1 e-mail services. There are no=20
    additional fees for using W
```

Mensaje 2:

Enviado por:

```
From: "Buchanan, Bill" <B.Buchanan@napier.ac.uk>, 2 items
```

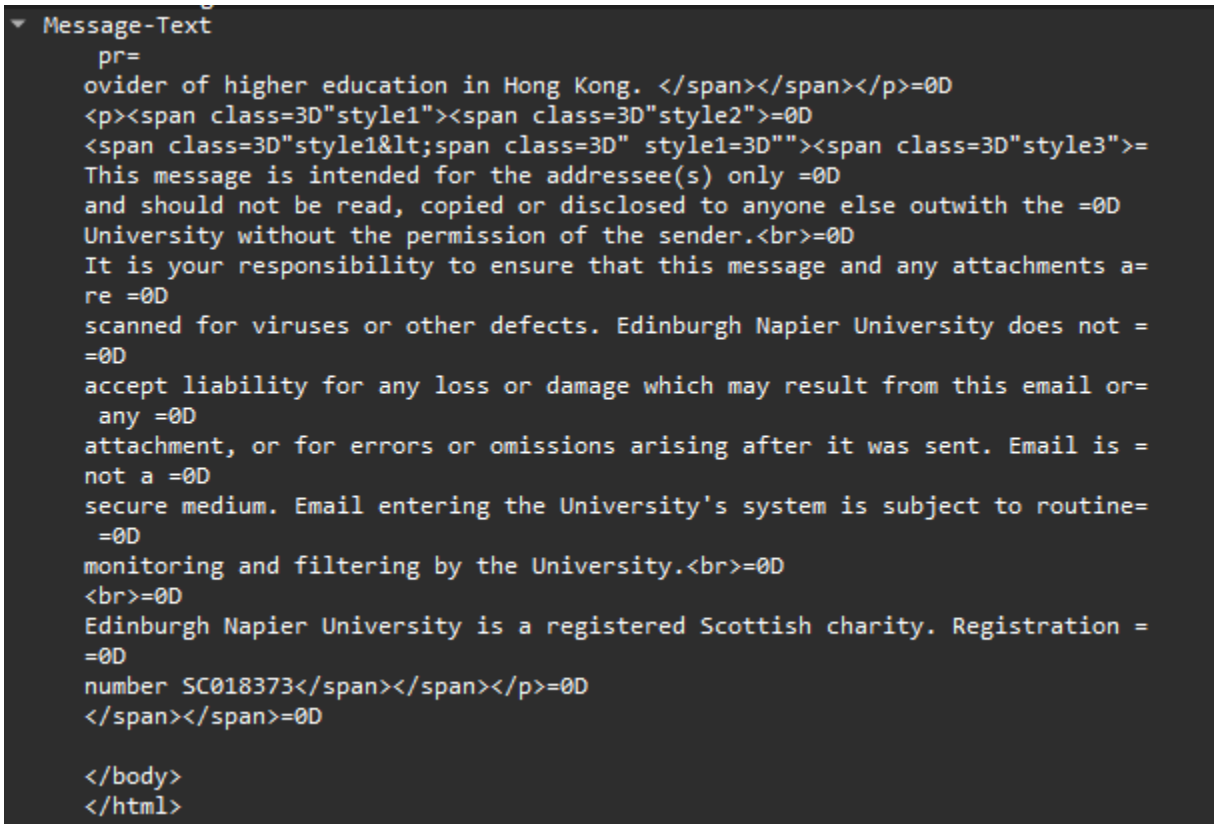
Asunto:

```
Subject: Testing
```

Contenido:

```
Content-Transfer-Encoding: quoted-printable

How are you tooo.....

I am fine.

DI 2


Edinburgh Napier University offers industry informed courses which combine =
the optimum balance of theory and practice to equip graduates for success i=
n today's competitive global job market. 92.3% of our graduates are in work=
 or further study within six months of leaving. With over 17,000 students f=
rom over 110 countries, we are an international University and are also pro=
ud to be the largest UK provider of higher education in Hong Kong.

This message is intended for the addressee(s) only
and should not be read, copied or disclosed to anyone else outwith the Univ=
ersity without the permission of the sender. It is your responsibility to e=
nsure that this message and any attachments are scanned for viruses or othe=
r defects. =

Edinburgh Napier University does not accept liability for any loss or
damage which may result from this email or any attachment, or for errors or=
 omissions arising after it was sent. Email is not a secure medium. Email e=
ntering the University's system is subject to ro
```

```
@page WordSection1
 {size:612.0pt 792.0pt;
 margin:72.0pt 72.0pt 72.0pt 72.0pt;}
div.WordSection1
 {page:WordSection1;}
--></style><!--[if gte mso 9]><xml>
<o:shapedefaults v:ext=3D"edit" spidmax=3D"1026" />
</xml><![endif]--><!--[if gte mso 9]><xml>
<o:shapelayout v:ext=3D"edit">
<o:idmap v:ext=3D"edit" data=3D"1" />
</o:shapelayout></xml><![endif]-->
</head>
<body lang=3D"EN-GB" link=3D"#0563C1" vlink=3D"#954F72">
<div class=3D"WordSection1">
<p class=3D"MsoNormal">How are you tooo&#8230;..<o:p></o:p></p>
<p class=3D"MsoNormal"><o:p> </o:p></p>
<p class=3D"MsoNormal">I am fine.<o:p></o:p></p>
<p class=3D"MsoNormal"><o:p> </o:p></p>
<p class=3D"MsoNormal">DI 2<o:p></o:p></p>
</div>
<br clear=3Dall> <head>=0D
<style type=3D"text/css"> .style1 { font-family: Arial; } .style2 { font-si=
ze: 9.0pt; } .style3 { color: #000000; } </style>=0D
</head>=0D
<p><span class=3D"style1"><span class=3D"style2">Edinburgh Napier Universit=
y offers industry informed courses which combine the optimum balance of the=
ory and practice to equip graduates for success in today's competitive glob=
al job market. 92.3% of our graduates are in work or further study within s=
ix months of leaving. With over 17,000 students from over 110 countries, we=
 are an international University and are also proud to be the largest UK
```



Mensaje 3:

Enviado por:

From: "Buchanan, Bill" <B.Buchanan@napier.ac.uk>, 2 items

Asunto:

Subject: RE: Testing

Contenido:

Message-Text

Thanks for the email.

Details:
Prof. William Buchanan, PhD, FBCS, FIET,
CEng, BSc (Hons), Cisco Regional Instructor,
Address:
Professor of Computing, IIDI/School of Computing,
Edinburgh Napier University, =

10 Colinton Road, Edinburgh. EH10 5DT
Tel: =

My New Web:
Youtube:
LinkedIn:
Twitter:
+44 (0)131 455 2759 =

http://asecuritysite.com
http://youtube.com/billatnapier
http://www.linkedin.com/in/billatnapier
http://twitter.com/billatnapier
Web:
http://buchananweb.co.uk
Research page: =

http://www.iidi.napier.ac.uk/c/people/peopleid/79
Skype
billatnapier

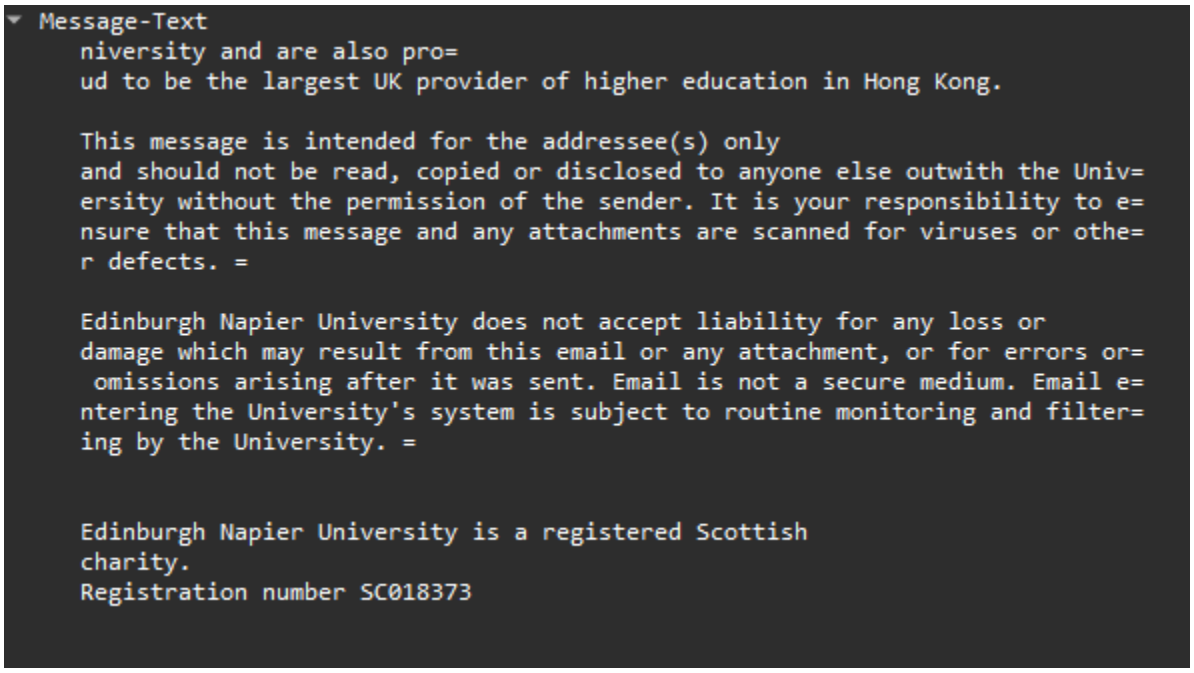
-----Original Message-----
From: DI [mailto:digitalinvestigator@networksims.com] =

Sent: 22 August 2013 20:18
To: Buchanan, Bill
Cc: w_j_buchanan@hotmail.com
Subject: Testing

Hello ... how are you?

Bill.

Edinburgh Napier University offers industry informed courses which combine =
the optimum balance of theory and practice to equip graduates for success i=
n today's competitive global job market. 92.3% of our graduates are in work=
 or further study within six months of leaving. With over 17,000 students f=
rom over 110 countries, we are an international U



7. ¿Qué comando utiliza POP-3 para obtener un mensaje en específico?

El comando utilizado por el protocolo POP3 para obtener un mensaje específico es el comando "RETR". Este comando se utiliza para recuperar (retrieve) un mensaje específico del servidor POP3. El comando RETR se sigue de un número de mensaje que identifica el mensaje que se desea recuperar. Por ejemplo, en los mensajes de esta práctica se usó RETR 1, RETR 2, y RETR 3 para obtener los tres correos.