

ESTUDIO DEL PROTOCOLO SMTP y POP-3 CON WIRESHARK

Grupo: Martín Gómez, Julio Prado, Daniel Plazas

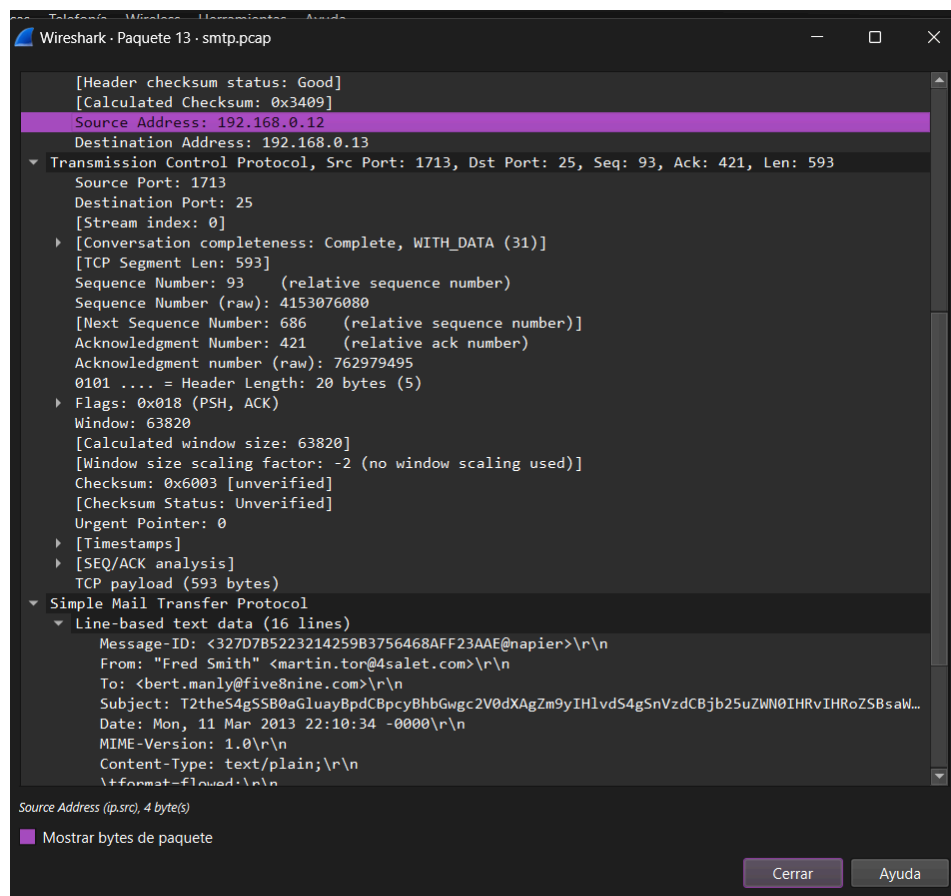
En este taller estudiaremos el funcionamiento de los protocolos SMTP y POP-3, mediante algunas capturas con Wireshark. Proceda de la siguiente manera:

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?

```
Padding: 00
▼ Internet Protocol Version 4, Src: 192.168.0.12, Dst: 192.168.0.13

Dst Port: 25,
```

IP:192.168.0.13

PUERTO:25

3. ¿Quién envía el correo electrónico?

```
▼ Simple Mail Transfer Protocol
  ▼ Line-based text data (16 lines)
    Message-ID: <327D7B5223214259B3756468AFF23AAE@napier>\r\n
    From: "Fred Smith" <martin.tor@4salet.com>\r\n
    To: <bert.manly@five8nine.com>\r\n
```

Nombre: Fren Smith

Correo: martin.tor@4salet.com

4. ¿Quién recibe el correo electrónico?

```
▼ Simple Mail Transfer Protocol
  ▼ Line-based text data (16 lines)
    Message-ID: <327D7B5223214259B3756468AFF23AAE@napier>\r\n
    From: "Fred Smith" <martin.tor@4salet.com>\r\n
    To: <bert.manly@five8nine.com>\r\n
```

Correo:"bert.manly@five8nine.com"

5. ¿Cuándo se envió el correo electrónico?

```
C: .
▼ Internet Message Format
  Message-ID: <327D7B5223214259B3756468AFF23AAE@napier>
  ▶ From: "Fred Smith" <martin.tor@4salet.com>, 1 item
  ▶ To: <bert.manly@five8nine.com>, 1 item
  Subject: T2theS4gSSB0aGluayBpdCBpcyBhbGwgc2V0dXAgZm9yIHlvdS4gSnVzdCBjb25uZWNOIHRvIHRoZSBsaW5rLCB
  Date: Mon, 11 Mar 2013 22:10:34 -0000
  MIME-Version: 1.0
  ▼ Content-Type: text/plain;\r\n\tformat=flowed;\r\n\tcharset="iso-8859-1";\r\n\treply-type=origina
  Type: text/plain
```

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.

```

Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.3790.3959
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.3959

.
250 2.6.0 <327D7B5223214259B3756468AFF23AAE@napier> Queued mail for delivery
QUIT
221 2.0.0 napier Service closing transmission channel
Paquete 13.7 client pkt(s), 7 server pkt(s), 12 turn(s). Clic para seleccionar.

```

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.

```

TCP payload (593 bytes)
  Simple Mail Transfer Protocol
    Line-based text data (16 lines)
      Message-ID: <327D7B5223214259B3756468AFF23AAE@napier>\r\n
      From: "Fred Smith" <martin.tor@4salet.com>\r\n
      To: <bert.manly@five8nine.com>\r\n
      Subject: T2theS4gSSB0aGluayBpdCBpcyBhbGwgc2V0dXAgZm9yIHlvdS4gSnVzdCBjb25uZWNOIHRvIHRoZSBsaW5r
      Date: Mon, 11 Mar 2013 22:10:34 -0000\r\n
      MIME-Version: 1.0\r\n

```

Si usamos una pagina que decodifica esto, obtenemos que

Decodifique a partir del formato Base64
 Simplemente introduzca los datos y pulse el botón de decodificar.

T2theS4gSSB0aGluayBpdCBpcyBhbGwgc2V0dXAgZm9yIHlvdS4gSnVzdCBjb25uZWNOIHRvIHRoZSBsaW5rLmV0dXAgZm9yIHlvdS4gSnVzdCBjb25uZWNOIHRvIHRoZSBsaW5r

< DECODIFICAR > Decodifica sus datos en la zona de abajo.

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

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.

```

1 DATA
1 354 Start mail input; end with <CRLF>.<CRLF>
1 Message-ID: <327D7B5223214259B3756468AFF23AAE@napier>

```

El cliente finalizó su mensaje de esta forma.

```

X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.3790.3959
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.3959
.

```

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?

```
▶ Frame 71: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
▶ Ethernet II, Src: Intel_4b:82:37 (c8:f7:33:4b:82:37), Dst: SagemcomBroa_64:16:49 (4c:17:eb:64:16:49)
▶ Internet Protocol Version 4, Src: 192.168.0.4, Dst: 212.227.15.166
▼ Transmission Control Protocol, Src Port: 26308, Dst Port: 110, Seq: 97, Ack: 299, Len: 0
  Source Port: 26308
  Destination Port: 110
  [Stream index: 9]
  ▶ [Conversation completeness: Complete, WITH DATA (31)]
```

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?

```
▶ Frame 70: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
▶ Ethernet II, Src: SagemcomBroa_64:16:49 (4c:17:eb:64:16:49), Dst: Intel_4b:82:37 (c8:f7:33:4b:82:37)
▶ Internet Protocol Version 4, Src: 212.227.15.166, Dst: 192.168.0.4
▼ Transmission Control Protocol, Src Port: 110, Dst Port: 26308, Seq: 298, Ack: 97, Len: 0
  Source Port: 110
  Destination Port: 26308
```

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

3. ¿Qué buzón de correo se está accediendo?

```
86 150.664860 212.227.15.166 192.168.0.4 POP 145 S: +OK mailbox "digitalinvestigator@networksims.com" has 3 messages (19191 octets) H mimap15
```

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

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

```
Post Office Protocol
▼ +OK mailbox "digitalinvestigator@networksims.com" has 3 messages (19191 octets) H mimap13\r\n
  Response indicator: +OK
  Response description: mailbox "digitalinvestigator@networksims.com" has 3 messages (19191 octets) H mimap13
```

Hay 3 mensajes en la bandeja de entrada.

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

Mensaje1:

```

Internet Message Format
  Return-Path: <noreply@bounce.unitedinternet.com>
  Delivery-Date: Thu, 22 Aug 2013 21:14:44 +0200
  Received: from mbulk.1and1.com (mbulk.1and1.com [212.227.126.222])\r\n\tby mx.kundenserver.de (node=mxu0) with ESMTP id 1W5Nip0Pgx-00tHOr@mbulk.1and1.com
  Unknown-Extension [truncated]: DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=1and1.co.uk;\r\n\tts=global1; s=global1; h=from:to:subject:date:message-id; b=
  Received: from omsmail (streamserve3.mt.einsundeins.de [172.19.7.103])\r\n\tby mbulk.1and1.com (node=mbulk2) with ESMTP id 1W5Nip0Pgx-00tHOr@mbulk.1and1.com
  MIME-Version: 1.0
  From: 1&1 Internet Ltd. <support@1and1.co.uk>, 1 item
  Subject: A message from 1&1 Internet
  To: digitalinvestigator@networksims.com, 1 item
    Item: digitalinvestigator@networksims.com\r\n
  Unknown-Extension: X-Message-ID: 90256101725241684#3 (Contact Wireshark developers if you want this supported.)
  Content-Type: multipart/alternative; boundary="multipart_alternative.878382066"
  Message-ID: <0M251y-1W5Nip0Pgx-00tHOr@mbulk.1and1.com>
  Date: Thu, 22 Aug 2013 21:14:44 +0200
  MIME multipart Media Encapsulation, Type: multipart/alternative, Boundary: "multipart_alternative.878382066"

```

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

Mensaje 2:

```

Internet Message Format
  Unknown-Extension [truncated]: designates 146.176.4.2 as permitted sender) client-ip=146.176.4.2; envelope-from=B.Buchanan@napier.ac.uk; helo=MER-EXCH2.napier.ac.uk
  Received: from CO1EHSMS025.bigfish.com (unknown [10.243.78.253])\tby\r\n mail36-co1.bigfish.com (Postfix) with ESMTP id 1W5Nip0Pgx-00tHOr@mbulk.1and1.com
  Received: from MER-EXCH2.napier.ac.uk (146.176.4.2) by\r\n CO1EHSMS025.bigfish.com (10.243.66.35) with Microsoft SMTP Server (TLS) id 14.0.100.0, Thu, 22 Aug 2013 19:18:52 +0000
  Received: from MER-EXCH1.napier.ac.uk ([fe80::f936:ca4b:b8b2:23c3]) by\r\n MER-EXCH2.napier.ac.uk ([fe80::c4c:e335:b1d8:973c%15]) with Microsoft SMTP Server (TLS) id 14.0.100.0, Thu, 22 Aug 2013 19:18:52 +0000
  From: "Buchanan, Bill" <B.Buchanan@napier.ac.uk>, 2 items
  To: "digitalinvestigator@networksims.com" <digitalinvestigator@networksims.com>, 1 item
    Item: "digitalinvestigator@networksims.com" <digitalinvestigator@networksims.com>\r\n
  Subject: Testing
  Unknown-Extension: Thread-Topic: Testing (Contact Wireshark developers if you want this supported.)
  Thread-Index: Ac6fbGYXtgSn00khQmGKggSiaX50Qw==
  Date: Thu, 22 Aug 2013 19:18:52 +0000
  Message-ID: <BF8FAC832FD171479CA19CA1FEA2254216D203E1@MER-EXCH1.napier.ac.uk>
  Unknown-Extension: Accept-Language: en-GB, en-US (Contact Wireshark developers if you want this supported.)
  Content-Language: en-US
  Unknown-Extension: X-MS-Has-Attach: (Contact Wireshark developers if you want this supported.)
  X-MS-TNEF-Correlator:
  Unknown-Extension: x-originating-ip: [146.176.4.13] (Contact Wireshark developers if you want this supported.)
  Message-Text

```

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

Mensaje 3:

```

Internet Message Format
  Unknown-Extension [truncated]: .176.4.2 as permitted sender) client-ip=146.176.4.2; envelope-from=B.Buchanan@napier.ac.uk; helo=MER-EXCH2.napier.ac.uk
  Received: from CO1EHSMS030.bigfish.com (unknown [10.243.78.233])\tby\r\n mail155-co1.bigfish.com (Postfix) with ESMTP id 8C36A600
  Received: from MER-EXCH2.napier.ac.uk (146.176.4.2) by\r\n CO1EHSMS030.bigfish.com (10.243.66.40) with Microsoft SMTP Server (TLS) id 14.0.100.0, Thu, 22 Aug 2013 19:19:11 +0000
  Received: from MER-EXCH1.napier.ac.uk ([fe80::f936:ca4b:b8b2:23c3]) by\r\n MER-EXCH2.napier.ac.uk ([fe80::c4c:e335:b1d8:973c%15]) with Microsoft SMTP Server (TLS) id 14.0.100.0, Thu, 22 Aug 2013 19:19:11 +0000
  From: "Buchanan, Bill" <B.Buchanan@napier.ac.uk>, 2 items
  To: DI <digitalinvestigator@networksims.com>, 1 item
    Item: DI <digitalinvestigator@networksims.com>\r\n
  Cc: "w_j_buchanan@hotmail.com" <w_j_buchanan@hotmail.com>, 1 item
    Item: "w_j_buchanan@hotmail.com" <w_j_buchanan@hotmail.com>\r\n
  Subject: RE: Testing
  Unknown-Extension: Thread-Topic: Testing (Contact Wireshark developers if you want this supported.)
  Thread-Index: AQHOn2xRdWdGPnwS70WY4VHcrLiv5mhmbw
  Date: Thu, 22 Aug 2013 19:19:11 +0000
  Message-ID: <BF8FAC832FD171479CA19CA1FEA2254216D203F0@MER-EXCH1.napier.ac.uk>
  References: <521663E3.7090401@networksims.com>
  In-Reply-To: <521663E3.7090401@networksims.com>
  Unknown-Extension: Accept-Language: en-GB, en-US (Contact Wireshark developers if you want this supported.)
  Content-Language: en-US
  Unknown-Extension: X-MS-Has-Attach: (Contact Wireshark developers if you want this supported.)
  X-MS-TNEF-Correlator:
  Unknown-Extension: x-originating-ip: [146.176.4.13] (Contact Wireshark developers if you want this supported.)
  Message-Text

```

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 20e9Qxdxccc0as26BK10hVKh0nc9Jpu+1wQ6rFagw
▼ 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.
  20
```

▼ Message-Text

For help using WebMail please visit our FAQ:
<http://faq.1and1.co.uk/search/go.php?t=3Dn49907>

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

Best regards,

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

--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&1 Internet e-mail services for your e-mail account. We'd like to take this opportunity to tell you about a feature that is included in 1&1 e-mail services.
<br/>
<br/>
WebMail 2.0
<br/>-----<br/>
Which e-mail client are you using?
Is it as flexible and easy to use as 1&1 WebMail?
<br/>
<br/>
Try WebMail today. You can reach your e-mail account from any browser and without installing any software.
<br/>
<br/>
<ul>
<li>Access to your e-mail from any browser. Log in to your account at
<a href="https://email.1and1.co.uk">https://email.1and1.co.uk</a></li>
<li>WebMail is an integral part of 1&1 e-mail services. There are no 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 in 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 from over 110 countries, we are an international University and are also proud 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 University without the permission of the sender. It is your responsibility to ensure that this message and any attachments are scanned for viruses or other 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 entering the University's system is subject to review.

@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…</p></p>

<p class=3D"MsoNormal"><o:p> </o:p></p>

<p class=3D"MsoNormal">I am fine.</p></p>

<p class=3D"MsoNormal"><o:p> </o:p></p>

<p class=3D"MsoNormal">DI 2</p></p>

</div>

<br clear=3Dall> <head>=0D

<style type=3D"text/css"> .style1 { font-family: Arial; } .style2 { font-size: 9.0pt; } .style3 { color: #000000; } </style>=0D

</head>=0D

<p>Edinburgh Napier University offers industry informed courses which combine the optimum balance of theory and practice to equip graduates for success in 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 from over 110 countries, we are an international University and are also proud to be the largest UK


```
▼ Message-Text
  pr=
  ovider of higher education in Hong Kong. </span></span></p>=0D
  <p><span class=3D"style1"><span class=3D"style2">=0D
  <span class=3D"style1&lt;span class=3D" style1=3D""><span class=3D"style3">=
  This message is intended for the addressee(s) only =0D
  and should not be read, copied or disclosed to anyone else outwith the =0D
  University without the permission of the sender.<br>=0D
  It is your responsibility to ensure that this message and any attachments a=
  re =0D
  scanned for viruses or other defects. Edinburgh Napier University does not =
  =0D
  accept liability for any loss or damage which may result from this email or=
  any =0D
  attachment, or for errors or omissions arising after it was sent. Email is =
  not a =0D
  secure medium. Email entering the University's system is subject to routine=
  =0D
  monitoring and filtering by the University.<br>=0D
  <br>=0D
  Edinburgh Napier University is a registered Scottish charity. Registration =
  =0D
  number SC018373</span></span></p>=0D
  </span></span>=0D

  </body>
  </html>
```

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

▼ Message-Text
niversity 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 routine monitoring and filter=
ing by the University. =

Edinburgh Napier University is a registered Scottish
charity.
Registration number SC018373

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.