Aspectos operativos SMTP

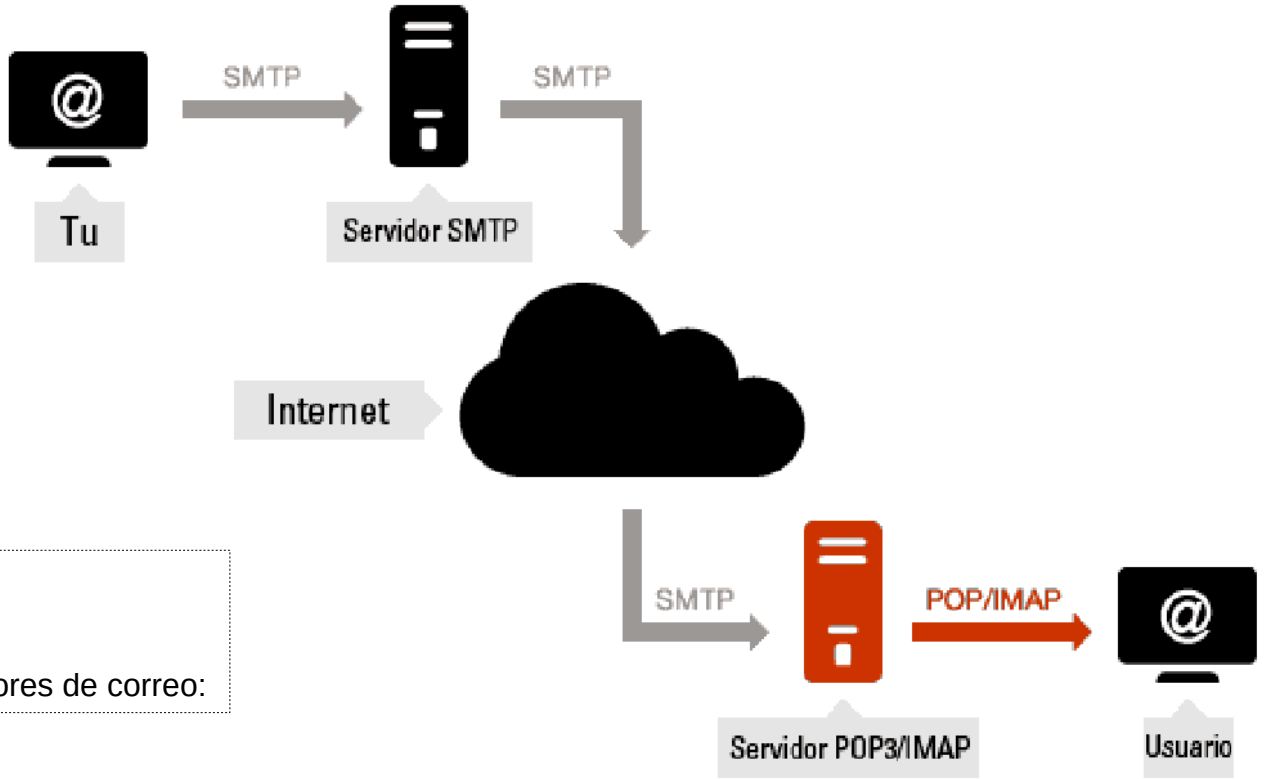
Nicolás Macia

SMTP - Aspectos operativos

- En la investigación de un incidente de SPAM / PHISHING o alguna otra amenaza que requiera comunicaciones de mail, se necesita conocer:
  - La relación del protocolo DNS con el protocolo SMTP
    - Servidores de correo usados para un dominio.
  - El protocolo SMTP
    - Analizar cabeceras de emails recibidos:
      - Para determinar IP que envió el correo
      - Para determinar el servidor SMTP utilizado.
  - Reconocer direccionamiento privado (RFC 1918)

Mensajes de e-mail

- Como se sabe, el envío de mensajes es realizado por un servidor de correo electrónico típicamente utilizando el protocolo SMTP (Puerto 25/TCP)



El mail nmacia@info.unlp.edu.ar
… en general, *@info.unlp.edu.ar

Es gestionalo por alguno de los siguientes servidores de correo:

```
~$ host -t mx info.unlp.edu.ar
info.unlp.edu.ar mail is handled by 20 anubis.unlp.edu.ar.
info.unlp.edu.ar mail is handled by 10 ada.info.unlp.edu.ar.
info.unlp.edu.ar mail is handled by 30 mail.linti.unlp.edu.ar.
~$
```

Anatomía de mensajes de e-mail

- Un mensaje de correo electrónico consta de tres partes distintas:
  - **Envelop**: directivas utilizadas para el efectivo encaminamiento del mensaje;
  - **Encabezados**: directivas informativas que describen las propiedades del mensaje;
  - **Cuerpo del mensaje**: contenido del mensaje de correo electrónico.

Envelop

- Es invisible al usuario. No es parte del mensaje.
- El envelop determina dónde se entregará el mensaje de correo electrónico.
- En la comunicación SMTP se utilizan las directivas para indicar el origen y el destino del mensaje.
  - mail from: <jose@yahoo.com>
  - rcpt to: <pepito@gmail.com>

- Si no es posible entregar el mensaje, el mismo se devuelve a la dirección de origen especificada con:
  - mail from: <jose@yahoo.com>

Encabezados

- Los encabezados del mensaje de correo electrónico están especificados en la RFC 5322.
- Tales directivas describen información del mensaje como por ejemplo:
  - Fecha y hora de envío,
  - Servidores de correo electrónico por los que el correo fue pasando
  - From: | To: | Subject: | Date: | Reply-To: | y mucha mas...

… luego de los encabezados viene el cuerpo del mensaje, que es el contenido del mensaje propiamente dicho.

Análisis de encabezados

- El análisis del encabezados de correo electrónico consiste en examinar ciertos datos presentes en los mensajes de correo.

- Los datos mas interesantes en la evaluación de un incidente de seguridad son:
  - IP de origen del remitente
  - IP del servidor de e-mail utilizado
  - Dirección de e-mail a la que será respondido el mensaje
  - Fecha y hora del envío del mensaje

```
 1 Return-Path: <anon@anon.net>
 2 X-Original-To: cert@intra.esr.rnp.br
 3 Delivered-To: cert@intra.esr.rnp.br
 4 Received: from mail.esr.rnp.br (mail.esr.rnp.br [10.10.10.10])
 5         (using TLSv1 with cipher AECDH-AES256-SHA (256/256 bits))
 6         (No client certificate requested)
 7         by intra.esr.rnp.br (Postfix) with ESMTPS id 9CCF04CEB46
 8         for <cert@intra.esr.rnp.br>; Fri, 4 Oct 2013 16:47:56 -0300 (BRT)
 9 Received: by mail.esr.rnp.br (Postfix)
10         id 5F71941AB1D; Fri, 4 Oct 2013 16:47:56 -0300 (BRT)
11 Delivered-To: cert@esr.rnp.br
12 Received: from rota5.anonnet.net (rota4.anonnet.net [10.1.1.1])
13         (using TLSv1 with cipher DHE-DSS-AES256-SHA (256/256 bits))
14         (No client certificate requested)
15         by mail.esr.rnp.br (Postfix) with ESMTPS id 52EB441AA74
16         for <cert@esr.rnp.br>; Fri, 4 Oct 2013 16:47:56 -0300 (BRT)
17 Received: from [10.10.2.1] (port=17213 helo=SXXXNIP005)
18         by sh.anonnet.net with esmtpa (Exim 4.80)
19         (envelope-from <anon@anon.net>)
20         id 1VSB6d-0048UJ-Kv
21         for cert@esr.rnp.br; Fri, 04 Oct 2013 16:32:07 -0300
22 Return-Receipt-To: “Reportador de incidentes :: anon DATACENTER” <anon@anon.net>
23 User-Agent: KMail/4.8.5 (Linux/3.2.0-54-generic; KDE/4.8.5; x86_64; ; )
24 MessageId: 4234xDfAF
25 Message-Id: <201312011813.rB1ID7V3020559>
26 Date: Fri, 04 Oct 2013 16:32:00 -0300
27 Subject: comprometimento de sistemas
28 From: anon@anon.net
```

Analicemos un ejemplo

Envelop vs Encabezado

Es importante recordar que las directivas del envelop del mensaje son totalmente independientes de los encabezados:

- Por ejemplo, es posible usar la directiva de envelop:
  mail from: <jose@yahoo.com>
  y la directiva de encabezado:
  From: tujefe@gmail.com

- Este tipo de inconsistencias son bastante utilizadas por los atacantes para falsear el origen de los mensajes.

Envelop vs Encabezado Protocolo SMTP

comandos
respuesta

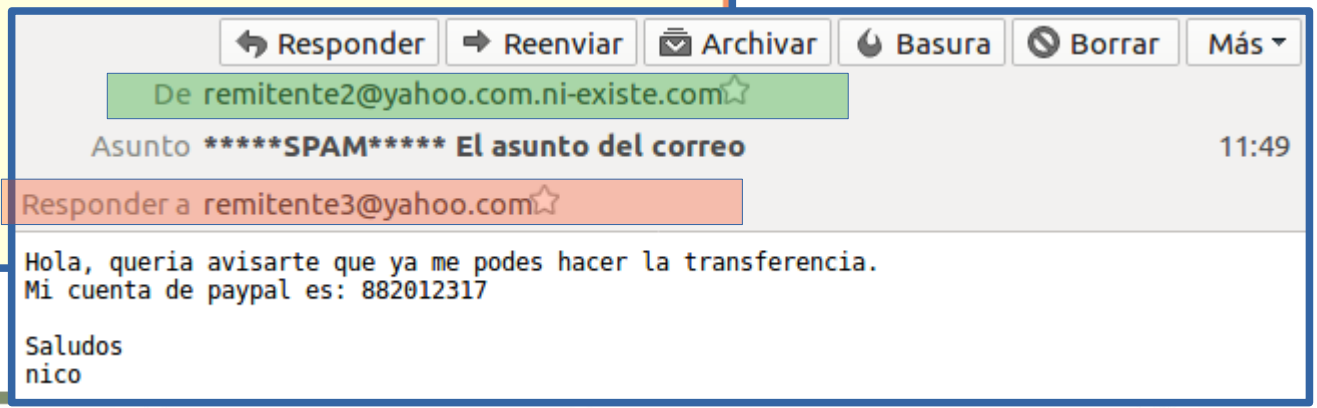
```
nico@nico-PORTEGE-Z30-B: ~
nico@nico-PORTEGE-Z30-B:~$ telnet mail.cert.unlp.edu.ar 25
Trying 163.10.40.194...
Connected to mail.cert.unlp.edu.ar.
Escape character is '^]'.
220 mail.cert.unlp.edu.ar ESMTP Postfix (Debian/GNU)
helo 192.168.0.68
250 mail.cert.unlp.edu.ar
mail from: remitente1@yahoo.com
250 2.1.0 Ok
rcpt to: nmacia@cert.unlp.edu.ar
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: El asunto del correo
From: remitente2@yahoo.com.ni-existe.com
Reply-to: remitente3@yahoo.com
Hola, queria avisarte que ya me podes hacer la transferencia.
Mi cuenta de paypal es: 882012317

Saludos
nico
.

250 2.0.0 Ok: queued as 1DF03281C1
500 5.5.2 Error: bad syntax
quit
221 2.0.0 Bye
Connection closed by foreign host.
nico@nico-PORTEGE-Z30-B:~$
```

Envelop vs Encabezado Protocolo SMTP

```
nico@nico-PORTEGE-Z30-B: ~
nico@nico-PORTEGE-Z30-B:~$ telnet mail.cert.unlp.edu.ar 25
Trying 163.10.40.194...
Connected to mail.cert.unlp.edu.ar.
Escape character is '^]'.
220 mail.cert.unlp.edu.ar ESMTP Postfix (Debian/GNU)
helo 192.168.0.68
250 mail.cert.unlp.edu.ar
mail from: remitente1@yahoo.com
250 2.1.0 Ok
rcpt to: nmacia@cert.unlp.edu.ar
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: El asunto del correo
From: remitente2@yahoo.com.ni-existe.com
Reply-to: remitente3@yahoo.com
Hola, queria avisarte que ya me podes hacer la transferencia.
Mi cuenta de paypal es: 882012317

Saludos
nico
.

250 2.0.0 Ok: queued as 1DF03281C1
500 5.5.2 Error: bad syntax
quit
221 2.0.0 Bye
Connection closed by foreign host.
nico@nico-PORTEGE-Z30-B:~$
```

Envelop vs Encabezado
Falseando el destinatario

```
nico@nico-PORTEGE-Z30-B: ~
nico@nico-PORTEGE-Z30-B:~$ telnet mail.cert.unlp.edu.ar 25
Trying 163.10.40.194...
Connected to mail.cert.unlp.edu.ar.
Escape character is '^]'.
220 mail.cert.unlp.edu.ar ESMTP Postfix (Debian/GNU)
helo 192.168.0.68
250 mail.cert.unlp.edu.ar
mail from: remitente1@yahoo.com
250 2.1.0 Ok
rcpt to: nmacia@cert.unlp.edu.ar
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: El asunto del correo
From: remitente2@yahoo.com.ni-existe.com
Reply-to: remitente3@yahoo.com
Hola, queria avisarte que ya me podes hacer la transferencia.
Mi cuenta de paypal es: 882012317

Saludos
nico
.

250 2.0.0 Ok: queued as 1DF03281C1
500 5.5.2 Error: bad syntax
quit
221 2.0.0 Bye
Connection closed by foreign host.
nico@nico-PORTEGE-Z30-B:~$
```



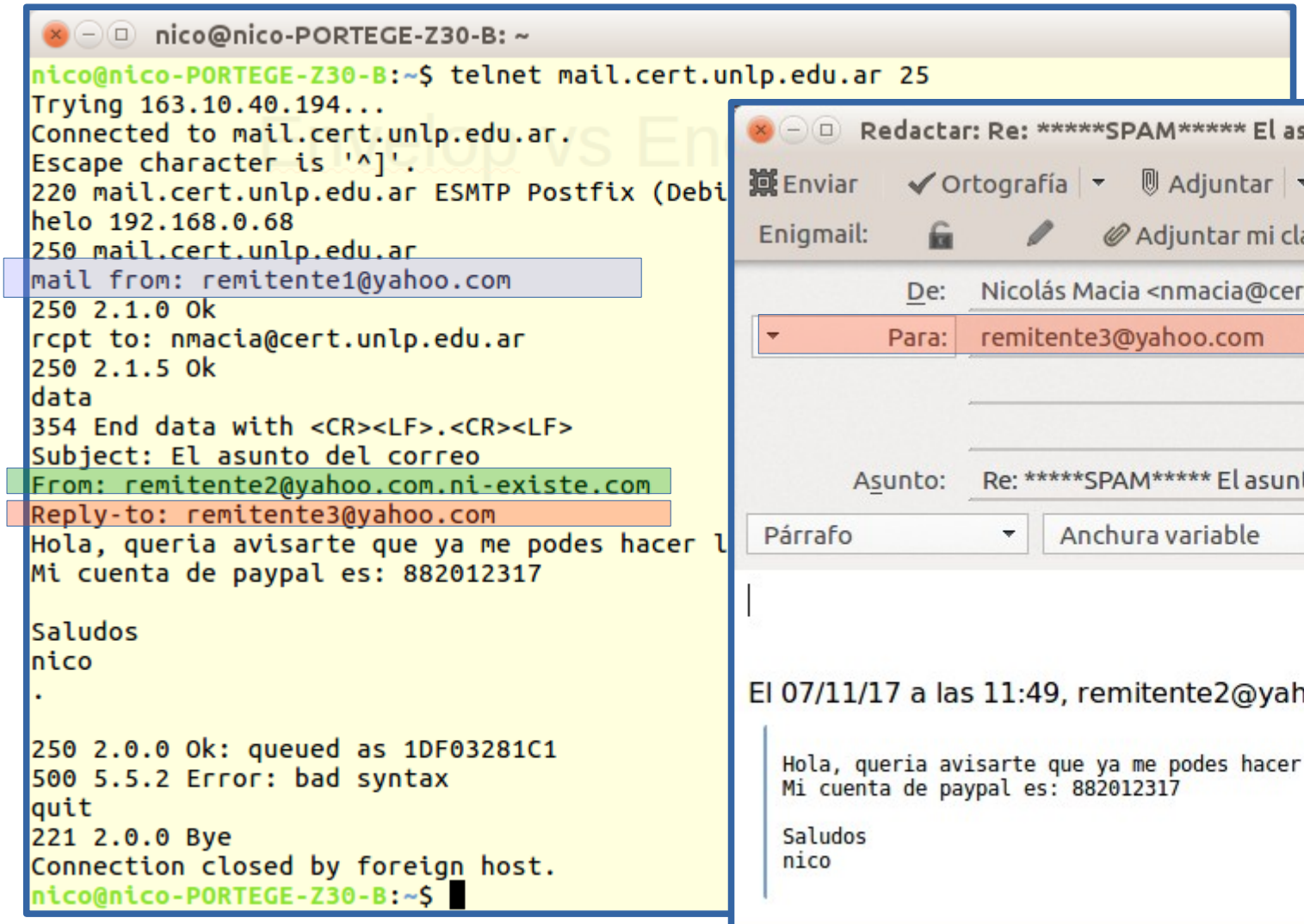
Envelop vs Encabezado SMTP / encabezados

```
nico@nico-PORTEGE-Z30-B: ~
nico@nico-PORTEGE-Z30-B:~$ telnet mail.cert.unlp.edu.ar 25
Trying 163.10.40.194...
Connected to mail.cert.unlp.edu.ar.
Escape character is '^]'.
220 mail.cert.unlp.edu.ar ESMTP Postfix (Debian/G
helo 192.168.0.68
250 mail.cert.unlp.edu.ar
mail from: remitente1@yahoo.com
250 2.1.0 Ok
rcpt to: nmacia@cert.unlp.edu.ar
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: El asunto del correo
From: remitente2@yahoo.com.ni-existe.com
Reply-to: remitente3@yahoo.com
Hola, queria avisarte que ya me podes hacer la tr
Mi cuenta de paypal es: 882012317

Saludos
nico
.

250 2.0.0 Ok: queued as 1DF03281C1
500 5.5.2 Error: bad syntax
quit
221 2.0.0 Bye
Connection closed by foreign host.
nico@nico-PORTEGE-Z30-B:~$
```

```
Return-Path: <remitente1@yahoo.com>
X-Original-To: nmacia@cert.unlp.edu.ar
Delivered-To: nmacia@cert.unlp.edu.ar
Received: by mail.cert.unlp.edu.ar (Postfix, from userid 112)
    id 6C3712824E; Tue,  7 Nov 2017 11:49:45 -0300 (-03)
X-Spam-Checker-Version: SpamAssassin 3.3.2 (2011-06-06) on
    mail.cert.unlp.edu.ar
X-Spam-Flag: YES
X-Spam-Level: *******
X-Spam-Status: Yes, score=7.2 required=6.0 tests=BAYES_00,
    FREEMAIL_FORGED_REPLYTO,FREEMAIL_REPLYTO_END_DIGIT,FSL_HELO_BARE_IP_1,
    MISSING_DATE,MISSING_HEADERS,MISSING_MID,REPLYTO_WITHOUT_TO_CC,TVD_RCVD_IP,
    TVD_RCVD_IP4 shortcircuit=no autolearn=no version=3.3.2
X-Spam-Report:
    *  0.0 TVD_RCVD_IP4 Message was received from an IPv4 address
    *  0.0 TVD_RCVD_IP Message was received from an IP address
    *  0.2 FREEMAIL_REPLYTO_END_DIGIT Reply-To freemail username ends in digit
    *      (remitente3[at]yahoo.com
    )
    *  1.0 MISSING_HEADERS Missing To: header
    * -1.9 BAYES_00 BODY: Bayes spam probability is 0 to 1%
    *      [score: 0.0000]
    *  0.5 MISSING_MID Missing Message-Id: header
    *  2.3 FSL_HELO_BARE_IP_1 FSL_HELO_BARE_IP_1
    *  1.6 REPLYTO_WITHOUT_TO_CC REPLYTO_WITHOUT_TO_CC
    *  1.4 MISSING_DATE Missing Date: header
    *  2.1 FREEMAIL_FORGED_REPLYTO Freemail in Reply-To, but not From
Received: from 192.168.0.68 (maquina78.linti.unlp.edu.ar [163.10.10.78])
    by mail.cert.unlp.edu.ar (Postfix) with SMTP id 1DF03281C1
    for <nmacia@cert.unlp.edu.ar>; Tue,  7 Nov 2017 11:47:51 -0300 (-03)
Subject: *****SPAM***** El asunto del correo
From: remitente2@yahoo.com.ni-existe.com
Reply-to: remitente3@yahoo.com
X-Spam-Prev-Subject: El asunto del correo
Message-Id: <20171107144945.6C3712824E@mail.cert.unlp.edu.ar>
Date: Tue,  7 Nov 2017 11:49:45 -0300 (-03)

Hola, queria avisarte que ya me podes hacer la transferencia.
Mi cuenta de paypal es: 882012317
```

Envelop vs Encabezado

Manipulando el e-mail de respuesta



Procesamiento de encabezados

- Hay herramientas en línea que simplifican el proceso de inspección de los encabezados de e-mail.
  - https://mxtoolbox.com/EmailHeaders.aspx
  - https://toolbox.googleapps.com/apps/messageheader/
- Sin embargo, el funcionamiento puede no ser el adecuado.

En los encabezados la verdad está!!!

Saber leerlos tu debes!!!

Análisis de encabezados

```
Return-Path: <remitente1@yahoo.com>
X-Original-To: nmacia@cert.unlp.edu.ar
Delivered-To: nmacia@cert.unlp.edu.ar
Received: by mail.cert.unlp.edu.ar (Postfix, from userid 112)
    id 6C3712824E; Tue,  7 Nov 2017 11:49:45 -0300 (-03)
X-Spam-Checker-Version: SpamAssassin 3.3.2 (2011-06-06) on
    mail.cert.unlp.edu.ar
X-Spam-Flag: YES
X-Spam-Level: *******
X-Spam-Status: Yes, score=7.2 required=6.0 tests=BAYES_00,
    FREEMAIL_FORGED_REPLYTO,FREEMAIL_REPLYTO_END_DIGIT,FSL_HELO_BARE_IP_1,
    MISSING_DATE,MISSING_HEADERS,MISSING_MID,REPLYTO_WITHOUT_TO_CC,TVD_RCVD_IP,
    TVD_RCVD_IP4 shortcircuit=no autolearn=no version=3.3.2
X-Spam-Report:
    *  0.0 TVD_RCVD_IP4 Message was received from an IPv4 address
    *  0.0 TVD_RCVD_IP Message was received from an IP address
    *  0.2 FREEMAIL_REPLYTO_END_DIGI
    *      (remitente3[at]yahoo.com
    )
    *  1.0 MISSING_HEADERS Missing
    * -1.9 BAYES_00 BODY: Bayes spa
    *      [score: 0.0000]
    *  0.5 MISSING_MID Missing Mess
    *  2.3 FSL_HELO_BARE_IP_1 FSL_H
    *  1.6 REPLYTO_WITHOUT_TO_CC RE
    *  1.4 MISSING_DATE Missing Dat
    *  2.1 FREEMAIL_FORGED_REPLYTO Freemail in Reply-To, but not From
Received: from 192.168.0.68 (maquina78.linti.unlp.edu.ar [163.10.10.78])
    by mail.cert.unlp.edu.ar (Postfix) with SMTP id 1DF03281C1
    for <nmacia@cert.unlp.edu.ar>; Tue,  7 Nov 2017 11:47:51 -0300 (-03)
Subject: *****SPAM***** El asunto del correo
From: remitente2@yahoo.com.ni-existe.com
Reply-to: remitente3@yahoo.com
X-Spam-Prev-Subject: El asunto del correo
Message-Id: <20171107144945.6C3712824E@mail.cert.unlp.edu.ar>
Date: Tue,  7 Nov 2017 11:49:45 -0300 (-03)

Hola, queria avisarte que ya me
Mi cuenta de paypal es: 8820123

Saludos
nico
```

Responder | Reenviar | Archivar | Basura | Bor

De remitente2@yahoo.com.ni-existe.com

Asunto *******SPAM***** El asunto del correo**

Responder a remitente3@yahoo.com

```
Hola, queria avisarte que ya me podes hacer la transferencia.
Mi cuenta de paypal es: 882012317

Saludos
nico
```

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	maquina78.linti.unlp.edu.ar 192.168.0.68	mail.cert.unlp.edu.ar	SMTP	11/7/2017 2:47:51 PM	✓
2	2 minutes	userid	mail.cert.unlp.edu.ar		11/7/2017 2:49:45 PM	

#	Delay	From *		To *	Protocol	Time received
0	-114 sec	maquina78.linti.unlp.edu.ar	→	mail.cert.unlp.edu.ar	SMTP	7/11/2017 11:47:51 GMT-3