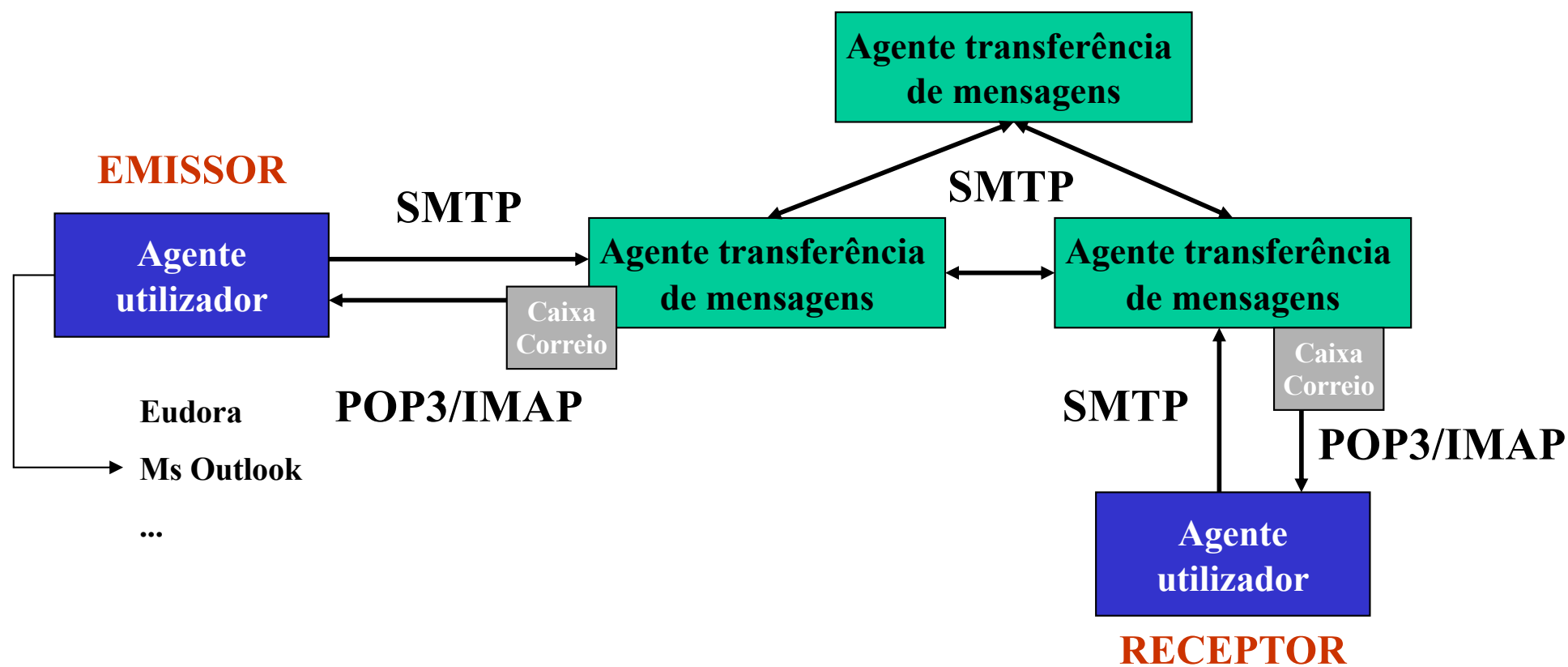


# Protocolos de email: SMTP e POP

- Estudo de dois protocolos de manipulação de mensagens de e-mail
- Análise do formato de mensagens e processo de comunicação

# Arquitetura



# Arquitetura

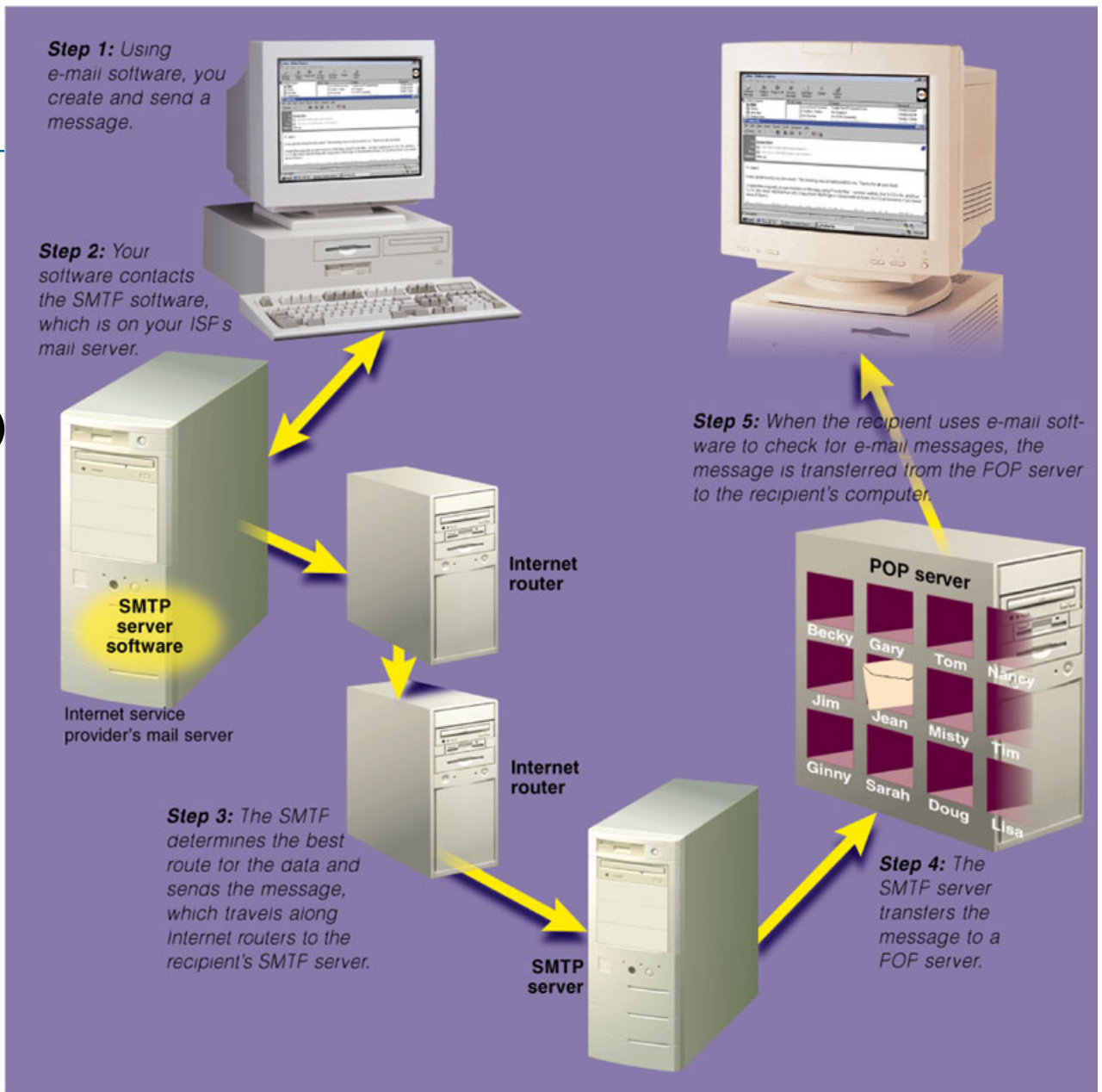
MUA (*Mail User Agent*)

MTA (*Mail Transport Agent*)

SMTP  
POP3  
IMAP

} Protocolos

## HOW AN E-MAIL MESSAGE TRAVELS FROM THE SENDER TO THE RECEIVER



# MUA e MTA

- **MUA (*Mail User Agent*)**

- aplicação necessária para «enviar» ou «receber» as mensagens

Ex.: pine, mail, Microsoft Outlook, Mozilla Mail

- **MTA (*Mail Transport Agent*)**

- aplicação que leva a mensagem até ao seu destino

Ex.: sendmail

# Formato de uma mensagem (2)

Return-Path: <ei07787@student.estg.iplei.pt>  
Received: from student.estg.iplei.pt (localhost.localdomain [127.0.0.1])  
by student.student.estg.ipleiria.pt (8.12.3/8.12.3) with ESMTP id  
gBBKQqNA026221  
for <vmc@estg.iplei.pt>; Wed, 11 Dec 2002 20:26:52 GMT  
From: "Pedro Miguel da Silva Pires" <ei07787@student.estg.iplei.pt>  
To: vmc@estg.iplei.pt  
Subject: Ip's  
Date: Wed, 11 Dec 2002 21:26:52 +0100  
Message-Id: <20021211202652.M80637@student.estg.iplei.pt>  
X-Mailer: Webmail Alunos - Centro de Informática 20020827  
X-OriginatingIP: 192.168.246.45 (ei07787)  
Status:

CABEÇALHO

CRLF

Ola Professor  
aqui esta mais uma das vertentes q se pode usar nos ips  
...

CORPO

# Cabeçalho de uma mensagem (1)

Campo	Significado
To:	Destinatário(s)
Cc:	Destinatário(s) secundário(s)
Bcc:	Cópia “cega”
From:	Remetente
Sender:	Máquina que envia
Received:	Agentes que transferiram a mensagem
Return-Path:	Caminho de regresso ao remetente

(...)

# Cabeçalho de uma mensagem (4)

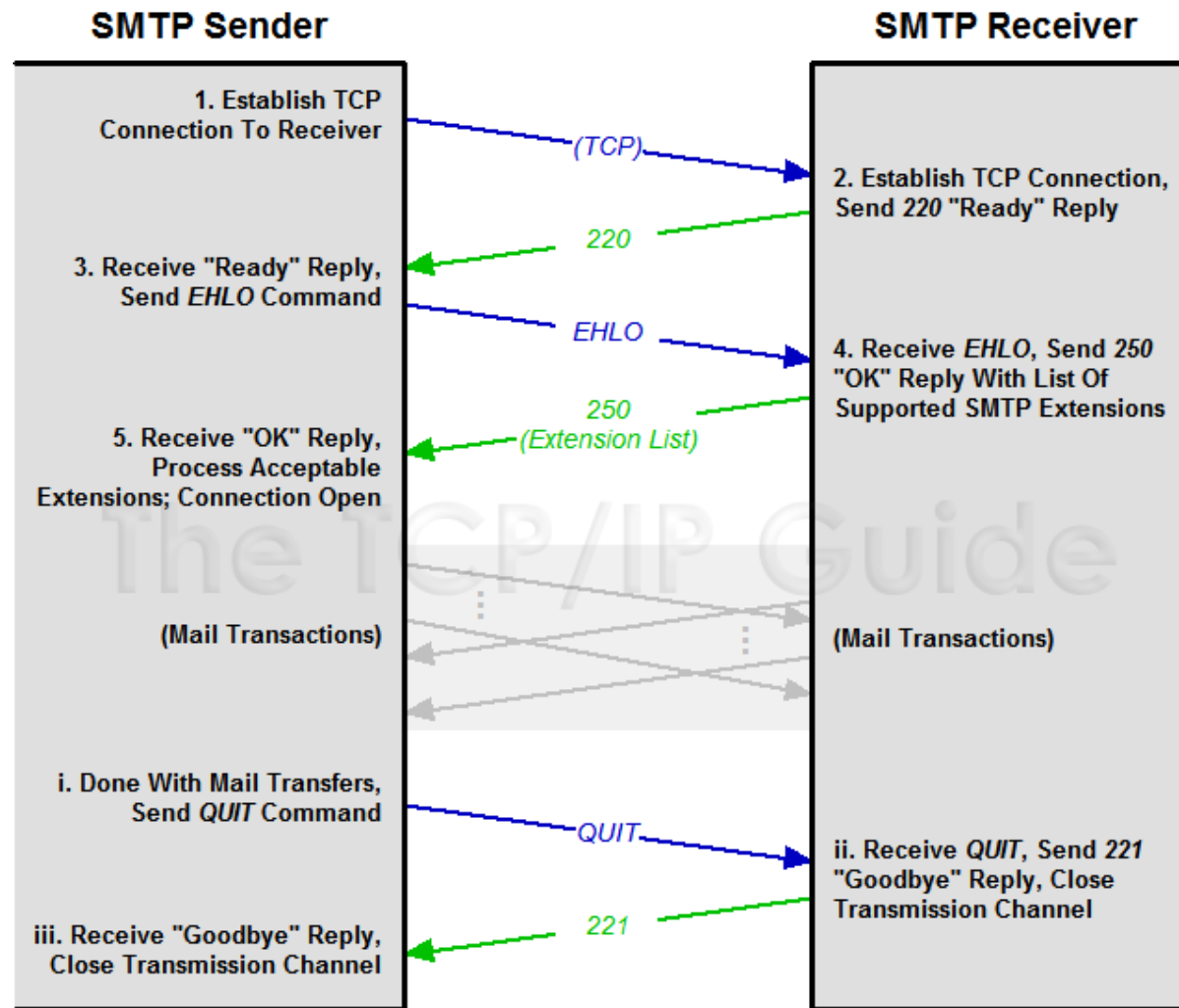
```
mail.estg.iplei.pt - PuTTY
From: Vitor Carreira <vmc@estg.iplei.pt>
Subject: Ficheiro Powerpoint em anexo
Mime-Version: 1.0
Content-Type: multipart/mixed;
          boundary="====_193484826=="
X-MailScanner: Found to be clean

-----_193484826==_
Content-Type: text/plain; charset="us-ascii"; format=flowed

-----_193484826==_
Content-Type: application/octet-stream; name="SDP_2002_2003_sem_1_cap_6c_[Protocolos SMTP_POP3].ppt";
x-mac-type="534C4433"; x-mac-creator="50505433"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="SDP_2002_2003_sem_1_cap_6c_[Protocolos SMTP_POP3].ppt"

OM8R4KGxGuEAAAAAAAAAAAAAAAAAAAAAPgADAP7/CQAGAAAAAAAAAAAAAAAAEAAAAbAEAAAAAAAAAA
EAAAIQEAAAEAAAD+////AAAAAGkBAABqAQAAawEAAHoBAAD////////////////////////////////////
////////////////////////////////////
"/var/spool/mail/vmc" 5523L, 355310C                               1948,76      35%
```

# Protocolo SMTP: Introdução

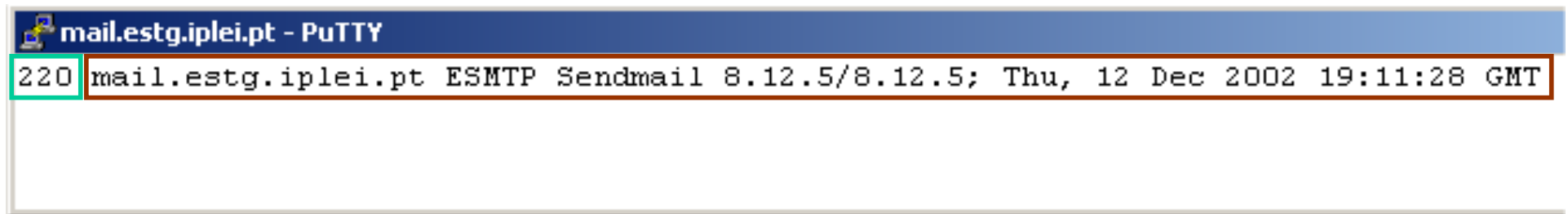
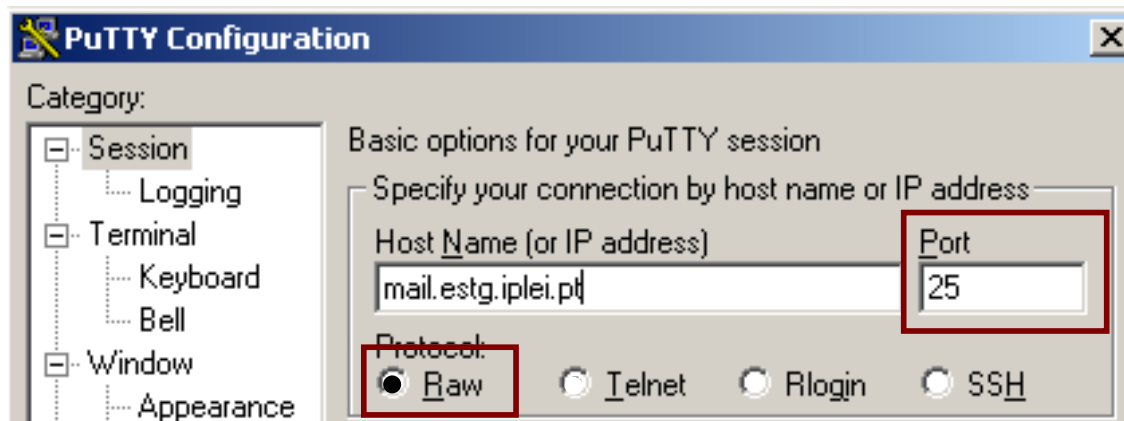


<http://www.tcpiptide.com/>



# Protocolo SMTP: Iniciar sessão

- Fase de *handshake* → cliente estabelece uma ligação para o porto 25
- O servidor pode responder com:
  - código 220 + espaço + **informação complementar**, se a ligação foi aceite
  - código 554 se a ligação foi rejeitada. Neste caso, o cliente deverá enviar a mensagem QUIT



# SMTP: Outro exemplo de envio

```
$ telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.
220 mail.ipleiria.pt ESMTP Sendmail 8.12.5/8.12.5; Wed, 13 Nov 2002
    02:20:01 GMT
helo mail
250 mail.ipleiria.pt Hello localhost.localdomain [127.0.0.1], pleased to
    meet you
mail from: antunes@ipleiria.pt
250 2.1.0 antunes@ipleiria.pt... Sender ok
rcpt to: antunes@ipleiria.pt
250 2.1.5 antunes@ipleiria.pt... Recipient ok
data
354 Enter mail, end with "." on a line by itself
Teste do mail
.
250 2.0.0 gAD2K1Rv016861 Message accepted for delivery
quit
221 2.0.0 mail.ipleiria.pt closing connection
Connection closed by foreign host.
```

# Mensagem recebida

Return-Path: <antunes@ipleiria.pt>

Received: from mail (localhost.localdomain [127.0.0.1])  
by mail.ipleiria.pt (8.12.5/8.12.5) with SMTP id  
gAD2K1Rv016861

for antunes@ipleiria.pt; Wed, 13 Nov 2002 02:20:46 GMT

Date: Wed, 13 Nov 2002 02:20:01 GMT

From: "antunes@ipleiria.pt" <antunes@ipleiria.pt>

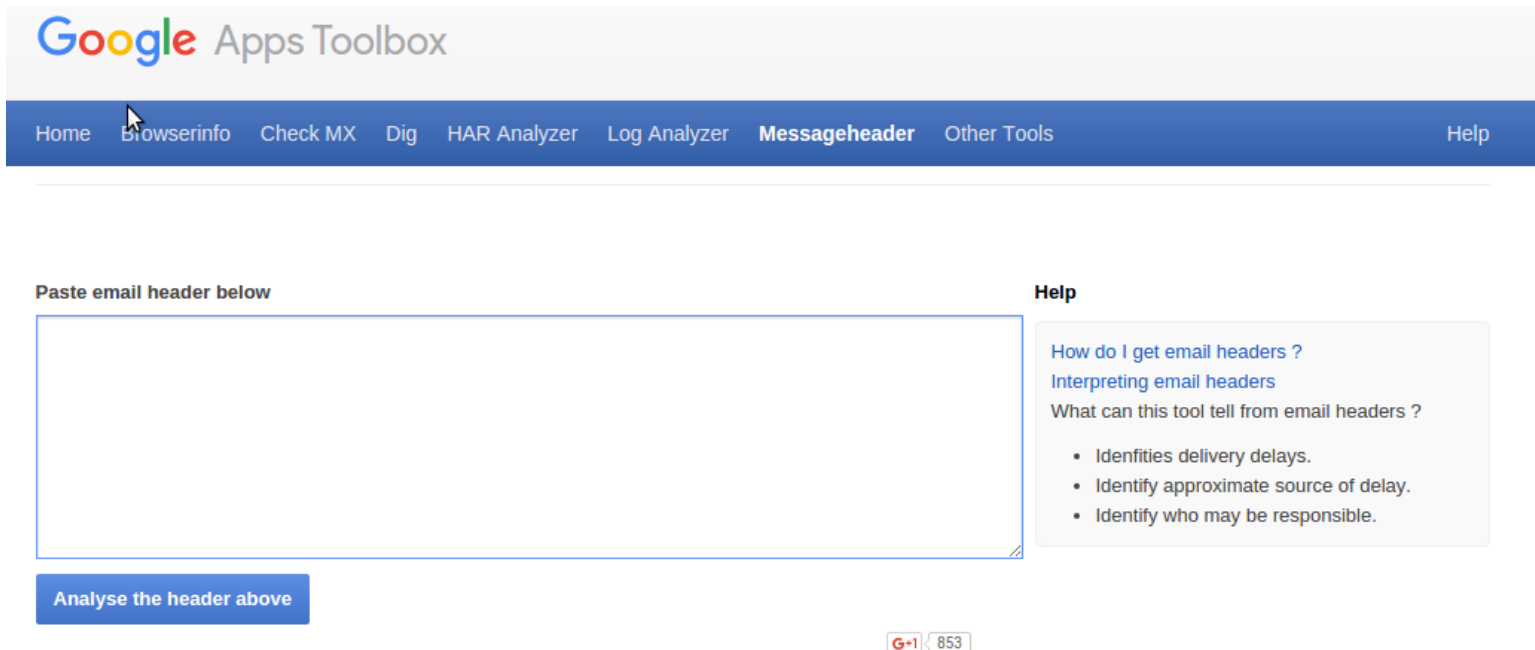
Message-Id: <200211130220.gAD2K1Rv016861@mail.ipleiria.pt>

X-AntiVirus: scanned for viruses by AMaViS 0.2.1  
(<http://amavis.org/>)

Teste do mail

# Campo «Received»

`https://toolbox.googleapps.com/apps/messageheader/`



The screenshot shows the Google Apps Toolbox interface for the Messageheader tool. At the top, the Google logo is followed by "Apps Toolbox". Below this is a navigation bar with links: Home, Browserinfo, Check MX, Dig, HAR Analyzer, Log Analyzer, Messageheader (which is highlighted), Other Tools, and Help. The main content area is divided into two sections. On the left, under the heading "Paste email header below", there is a large empty text box for pasting email headers. Below this text box is a blue button labeled "Analyse the header above". On the right, under the heading "Help", there is a light gray box containing links for "How do I get email headers ?", "Interpreting email headers", and "What can this tool tell from email headers ?". Below these links is a bulleted list of capabilities: "Identifies delivery delays.", "Identify approximate source of delay.", and "Identify who may be responsible.". At the bottom center of the interface, there is a small Google+ icon followed by the number "853".

Google Apps Toolbox

Home Browserinfo Check MX Dig HAR Analyzer Log Analyzer **Messageheader** Other Tools Help

Paste email header below

Help

How do I get email headers ?  
Interpreting email headers  
What can this tool tell from email headers ?

- Identifies delivery delays.
- Identify approximate source of delay.
- Identify who may be responsible.

Analyse the header above

853

# Protocolo POP3: Introdução (2)

## Modelo Cliente-Servidor

Utiliza um porto “bem-conhecido”: **110**

A resposta do servidor consiste em:

Sucesso: **+OK** <Mensagem de sucesso>

Erro: **-ERR** <Mensagem de erro>



O acesso à caixa de correio é realizada em 3 etapas:

- 1 – Autenticação
- 2 – Transacções (processamento dos pedidos dos clientes)
- 3 – Actualização (efectua a actualização da caixa de correio)

# Protocolo POP3: Autenticação (1)

- Autenticação tem início quando um cliente estabelece uma ligação para o porto 110
- Enquanto o servidor permanecer no estado de autenticação apenas aceita a seguinte sequência de comandos:

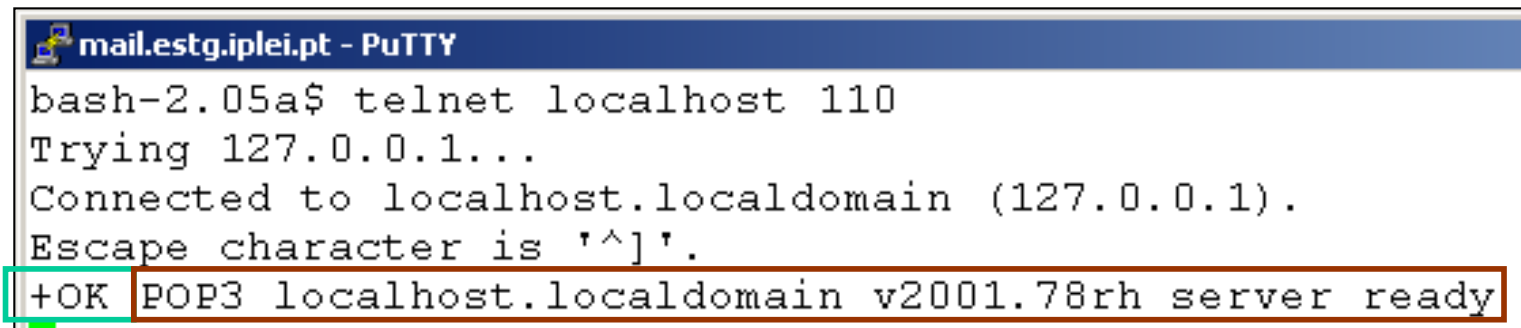
**USER** <nome da caixa de correio (nome do utilizador)>

**PASS** <senha>

**O servidor responde com:**

O código **+OK<espaço>mensagem de boas vindas**, se a ligação foi aceite

O código **+ERR<espaço>mensagem de erro**, se a ligação não foi aceite



```
mail.estg.iplei.pt - PuTTY
bash-2.05a$ telnet localhost 110
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.
+OK POP3 localhost.localdomain v2001.78rh server ready
```

# Protocolo POP3: Autenticação (2)

Para se autenticar o utilizador terá que executar:

1 – Executar o comando **USER**

**USER**<espaço><nome da caixa de correio (nome do utilizador)>

2 – Ao qual o servidor responderá com:

**+OK** <mensagem a pedir a senha>

3 – Executar o comando **PASS**

**PASS**<espaço><senha>

4 – Ao qual o servidor responderá com:

```
bash-2.05a$ telnet localhost 110
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.
+OK POP3 localhost.localdomain v2001.78rh server ready
1 USER vmc
2 +OK User name accepted, password please
3 PASS
4 +OK Mailbox open, 24 messages
```

**Password em clear text!!**

# Protocolo POP3: Transacções (2)

## Alguns exemplos (STAT, LIST e RETR)

```
STAT
+OK 24 512235
LIST 22
+OK 22 397
RETR 22
+OK 397 octets
Return-Path: <batatas@quintal.net>
Received: from batatas (proxy.iplei.pt [193.137.239.227])
        by mail.estg.iplei.pt (8.12.5/8.12.5) with SMTP id gBCKDHN4021921;
        Thu, 12 Dec 2002 20:28:47 GMT
Date: Thu, 12 Dec 2002 20:13:17 GMT
From: batatas@quintal.net
Message-Id: <200212122028.gBCKDHN4021921@mail.estg.iplei.pt>
X-MailScanner: Found to be clean
Status: RO

Ola,

mensagem de teste
.
```