

Introduction to SMTP

RES, Lecture 4

Olivier Liechti



HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD

www.heig-vd.ch

Warning 1

The slides and the webcasts contain examples and demos with **real SMTP servers.**

The behaviour of these servers may change over time. It may also change depending on the network you are connected to (internal, ISP, other ISP).

The main reason why a server might behave differently is the fight between mail administrators and **spammers.**

Warning 2

It is a good thing to experiment with real SMTP servers.

But remember that they are real servers and act responsibly.

Please avoid launching a **surprise denial of service attack** with your accidental infinite loop.

13



Labo SMTP, part 1

Olivier Liechti

14



Labo SMTP, part 2

Olivier Liechti

15



Labo SMTP, part 3

Olivier Liechti

16



Labo SMTP, part 4

Olivier Liechti

- SMTP demo & hints
- SMTP protocol
- Mock server
- Implementation walk-through

Lecture	Lab
09.04 SMTP	10.04 Labo SMTP
16.04 Labo SMTP	17.04 Labo SMTP
30.04 Travail écrit Tout, y compris SMTP	01.05 Labo SMTP Démos

Démo (5 minutes MAX)	
Le labo est terminé et la démo est faite au plus tard la semaine du 29 avril.	1 pt
Le groupe arrive à démarrer un serveur mock dans un container Docker et à expliquer à quoi il sert. Le groupe a aussi configuré le service <u>mailtrap.io</u>	1 pt
Le groupe montre comment configurer la campagne de “pranks” et lance son programme dans un environnement de test (mock mock, mailtrap ou autre). Le groupe explique les résultats.	2 pt
Le groupe montre son repo GitHub. En regardant les commits, on voit qu'il n'y a pas seulement un gros commit à la fin.	1 pt
Une documentation de qualité et conforme aux exigences est fournie dans le repo GitHub.	2 pt



What happens when Bob wants
to **send an e-mail** to Alice?



Bob uses **Thunderbird** to write his mail.



Alice uses **MS Outlook** to check and read her mails.



In the technical specs (RFCs), these programs are called **Mail User Agents (MUA)**

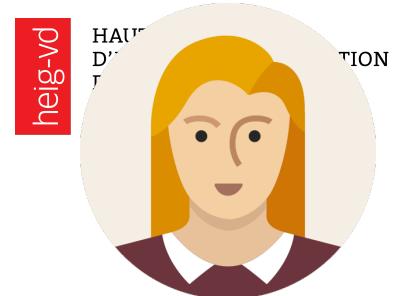


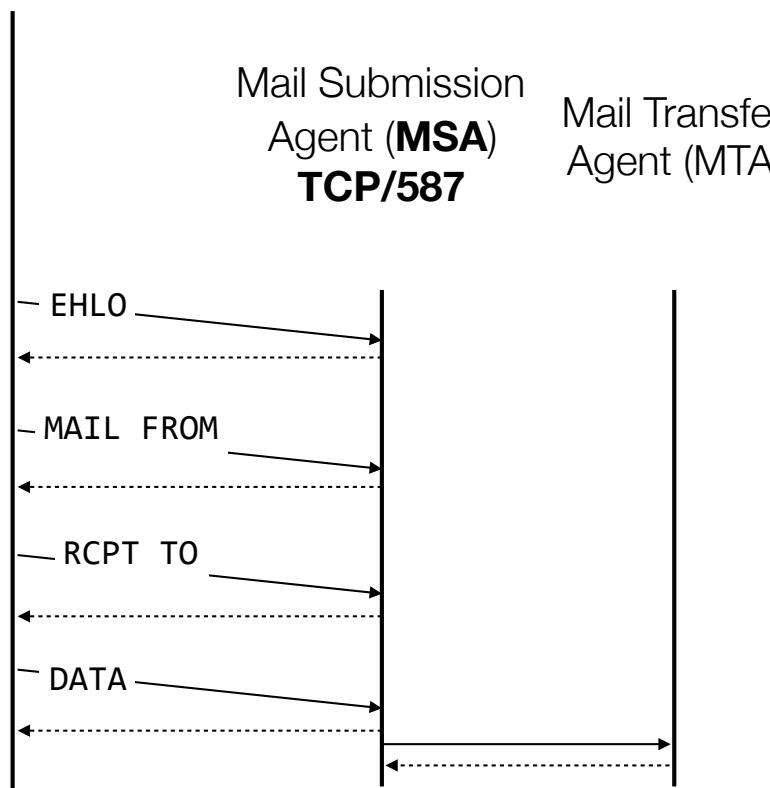


Bob uses his professional e-mail address. His company runs a **MS Exchange Server**.



Alice uses her private address. She has an account (and a **mailbox**) on the **Google gmail** infrastructure.





Bob writes a message to “**alice.res@gmail.com**”. He pushes on the “Send” button.

The Exchange Server is made of **2 logical components**: the **MSA** and the **MTA**.

Bob’s MUA asks Bob’s MSA to deliver the mail. It uses the **SMTP** protocol for that purpose and (should) use TCP port 587.

After enforcing **usage policies**, the MSA delegates the work to the MTA. We don’t know how.

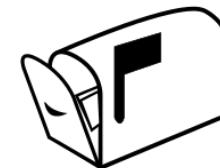


Mail Transfer
Agent (MTA)

Mail Transfer
Agent (MTA)

TCP/25

DNS



Give me the MX record(s)
for **gmail.com**

EHLO

MAIL FROM

RCPT TO

DATA

Bob's MTA initially does not know where to forward the mail...

It issues a **DNS** query to get a list of **MX records** for Alice's domain (**gmail.com**).

When Bob's MTA knows the IP address of Alice's MTA, it uses the **SMTP** protocol once more to forward the message. TCP **port 25** is used in this case.

When Alice's MTA receives the mail, it stores it in Alice's **mailbox** (for later retrieval).

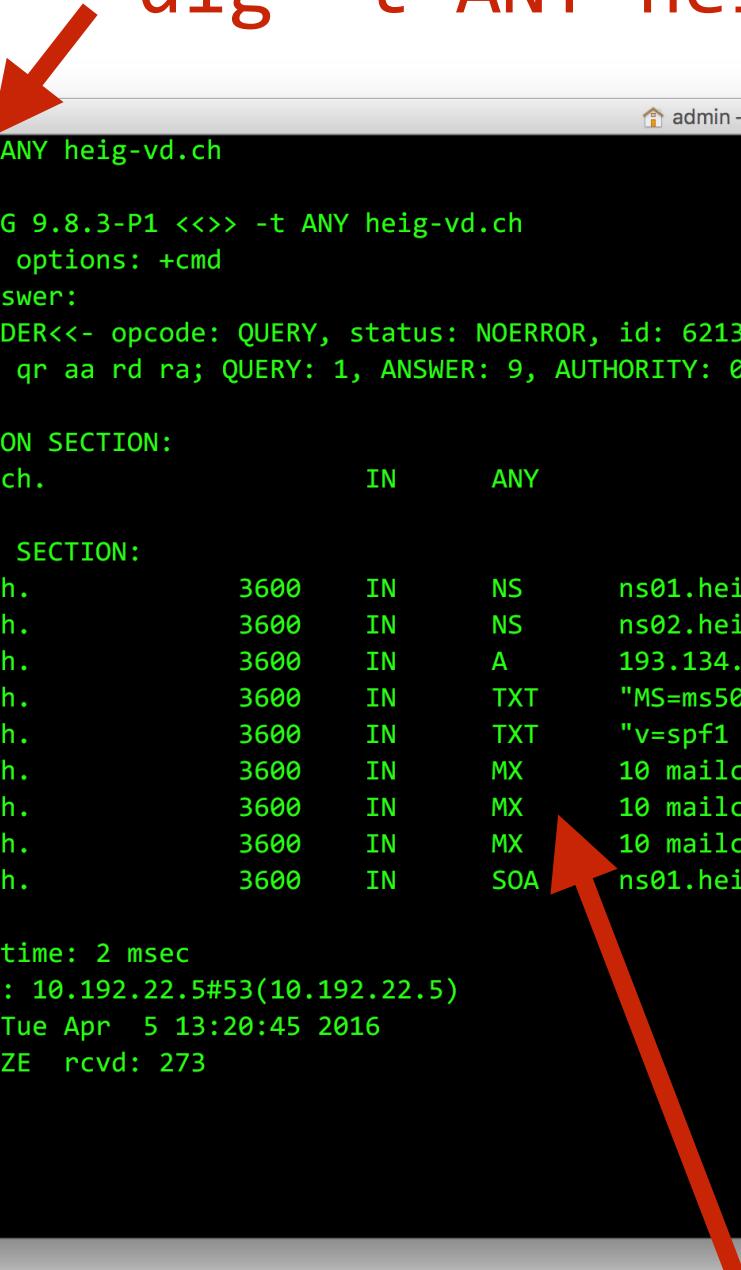
dig



```
DIG(1)                                admin — less < man dig — 120x30          HAUTE ÉCOLE  
                                         BIND9                                     D'INGÉIERIE ET DE GESTION  
NAME                                     DIG(1)  
dig - DNS lookup utility  
SYNOPSIS  
dig [@server] [-b address] [-c class] [-f filename] [-k filename] [-m] [-p port#] [-q name] [-t type]  
[-x addr] [-y [hmac:]name:key] [-4] [-6] [name] [type] [class] [queryopt...]  
  
dig [-h]  
  
dig [global-queryopt...] [query...]  
  
DESCRIPTION  
dig (domain information groper) is a flexible tool for interrogating DNS name servers. It performs  
DNS lookups and displays the answers that are returned from the name server(s) that were queried.  
Most DNS administrators use dig to troubleshoot DNS problems because of its flexibility, ease of use  
and clarity of output. Other lookup tools tend to have less functionality than dig.  
  
Although dig is normally used with command-line arguments, it also has a batch mode of operation for  
reading lookup requests from a file. A brief summary of its command-line arguments and options is  
printed when the -h option is given. Unlike earlier versions, the BIND 9 implementation of dig allows  
multiple lookups to be issued from the command line.  
  
Unless it is told to query a specific name server, dig will try each of the servers listed in  
/etc/resolv.conf.  
  
When no command line arguments or options are given, dig will perform an NS query for "." (the root).  
:
```

nslookup is another command for querying DNS

dig -t ANY heig-vd.ch



```
$ dig -t ANY heig-vd.ch

; <>> DiG 9.8.3-P1 <>> -t ANY heig-vd.ch
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62138
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 9, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;heig-vd.ch.          IN      ANY

;; ANSWER SECTION:
heig-vd.ch.        3600    IN      NS      ns01.heig-vd.ch.
heig-vd.ch.        3600    IN      NS      ns02.heig-vd.ch.
heig-vd.ch.        3600    IN      A       193.134.220.23
heig-vd.ch.        3600    IN      TXT    "MS=ms50694826"
heig-vd.ch.        3600    IN      TXT    "v=spf1 ip4:193.134.216.180/30 mx ~all"
heig-vd.ch.        3600    IN      MX      10 mailcl2.heig-vd.ch.
heig-vd.ch.        3600    IN      MX      10 mailcl1.heig-vd.ch.
heig-vd.ch.        3600    IN      MX      10 mailcl0.heig-vd.ch.
heig-vd.ch.        3600    IN      SOA     ns01.heig-vd.ch. domain.heig-vd.ch. 2014141923 10800 3600 2419200 900

;; Query time: 2 msec
;; SERVER: 10.192.22.5#53(10.192.22.5)
;; WHEN: Tue Apr  5 13:20:45 2016
;; MSG SIZE  rcvd: 273

$
```

MX records point to the SMTP servers for the domain

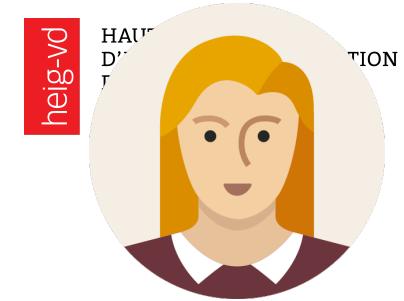


SMTP
587

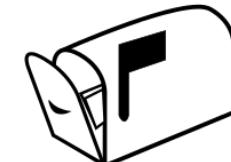


In the last step, Alice's MUA uses another protocol (e.g. IMAP, POP3) to fetch mails from the mailbox.

SMTP
25



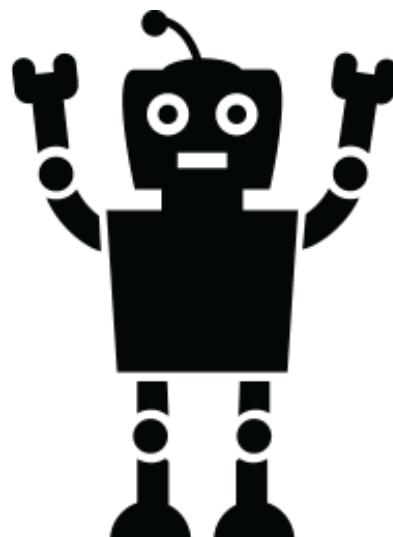
IMAP/POP3





Let's be human Exchange Servers
(and play the role of Bob's MTA).

But instead of forwarding the mail
to gmail, let's forward the mail via
the **HEIG-VD's SMTP** server.



```
dig -t MX heig-vd.ch
```

```
heig-vd.ch. 600 IN MX 10 mail01.heig-vd.ch.
```

```
telnet mailcl0.heig-vd.ch 25
```

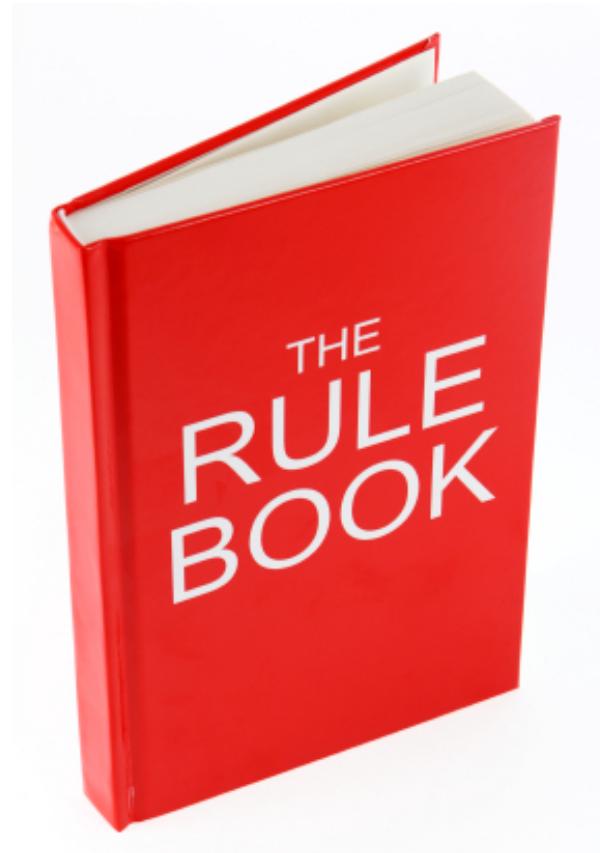
```
openssl s_client -starttls smtp -crlf -connect  
mail01.heig-vd.ch:25 (or use 465)
```

```
EHLO mycompany.com
```

```
$ telnet mailcl10.heig-vd.ch 25
mailcl10.heig-vd.ch: nodename nor servname provided, or not known
$ telnet mailcl0.heig-vd.ch 25
Trying 193.134.216.181...
Connected to mailcl0.heig-vd.ch.
Escape character is '^]'.
220 heig-vd.ch ESMTP MailCleaner (Enterprise Edition 2016.01) Tue, 05 Apr 2016 14:18:24
+0200
EHLO mycompany.com
250-heig-vd.ch Hello mbp-de-admin.einet.ad.eivd.ch [10.192.116.92]
250-SIZE 20480000
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP
MAIL FROM: bob@bob.com ← SMTP command != Message header
250 OK
RCPT TO: olivier.liechti@wasabi-tech.com
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
From: bob@areyousure.com ←
To: olivier.liechti@wasabi-tech.com
Subject: demo

Ok. Cool. Bye.

.
250 OK id=1anPx9-0003KC-BC
quit
221 heig-vd.ch closing connection
Connection closed by foreign host.
```



The Specs

<https://tools.ietf.org/html/rfc5321>

Table of Contents

1.	Introduction	5
1.1.	Transport of Electronic Mail	5
1.2.	History and Context for This Document	5
1.3.	Document Conventions	6
2.	The SMTP Model	7
2.1.	Basic Structure	7
2.2.	The Extension Model	9
2.2.1.	Background	9
2.2.2.	Definition and Registration of Extensions	10
2.2.3.	Special Issues with Extensions	11
2.3.	SMTP Terminology	11
2.3.1.	Mail Objects	11
2.3.2.	Senders and Receivers	12
2.3.3.	Mail Agents and Message Stores	12
2.3.4.	Host	13
2.3.5.	Domain Names	13
2.3.6.	Buffer and State Table	14
2.3.7.	Commands and Replies	14
2.3.8.	Lines	14
2.3.9.	Message Content and Mail Data	15
2.3.10.	Originator, Delivery, Relay, and Gateway Systems	15
2.3.11.	Mailbox and Address	15
2.4.	General Syntax Principles and Transaction Model	16
3.	The SMTP Procedures: An Overview	17
3.1.	Session Initiation	18
3.2.	Client Initiation	18
3.3.	Mail Transactions	19
3.4.	Forwarding for Address Correction or Updating	21
3.5.	Commands for Debugging Addresses	22
3.5.1.	Overview	22
3.5.2.	VRFY Normal Response	24
3.5.3.	Meaning of VRFY or EXPN Success Response	25
3.5.4.	Semantics and Applications of EXPN	26
3.6.	Relaying and Mail Routing	26
3.6.1.	Source Routes and Relaying	26
3.6.2.	Mail eXchange Records and Relaying	26
3.6.3.	Message Submission Servers as Relays	27
3.7.	Mail Gateways	28
3.7.1.	Header Fields in Gateways	28
3.7.2.	Received Lines in Gateways	29
3.7.3.	Addresses in Gateways	29
3.7.4.	Other Header Fields in Gateways	29
3.7.5.	Envelopes in Gateways	30
3.8.	Terminating Sessions and Connections	30
3.9.	Mailing Lists and Aliases	31
3.9.1.	Alias	31

RFC 5321

SMTP

October 2008

3.9.2.	List	31
4.	The SMTP Specifications	32
4.1.	SMTP Commands	32
4.1.1.	Command Semantics and Syntax	32
4.1.2.	Command Argument Syntax	41
4.1.3.	Address Literals	43
4.1.4.	Order of Commands	44
4.1.5.	Private-Use Commands	46
4.2.	SMTP Replies	46
4.2.1.	Reply Code Severities and Theory	48
4.2.2.	Reply Codes by Function Groups	50
4.2.3.	Reply Codes in Numeric Order	52
4.2.4.	Reply Code 502	53
4.2.5.	Reply Codes after DATA and the Subsequent <CRLF>.<CRLF>	53
4.3.	Sequencing of Commands and Replies	54
4.3.1.	Sequencing Overview	54
4.3.2.	Command-Reply Sequences	55
4.4.	Trace Information	57
4.5.	Additional Implementation Issues	61
4.5.1.	Minimum Implementation	61
4.5.2.	Transparency	62
4.5.3.	Sizes and Timeouts	62
4.5.3.1.	Size Limits and Minimums	62
4.5.3.1.1.	Local-part	63
4.5.3.1.2.	Domain	63
4.5.3.1.3.	Path	63
4.5.3.1.4.	Command Line	63
4.5.3.1.5.	Reply Line	63
4.5.3.1.6.	Text Line	63
4.5.3.1.7.	Message Content	63
4.5.3.1.8.	Recipients Buffer	64
4.5.3.1.9.	Treatment When Limits Exceeded	64
4.5.3.1.10.	Too Many Recipients Code	64
4.5.3.2.	Timeouts	65
4.5.3.2.1.	Initial 220 Message: 5 Minutes	65
4.5.3.2.2.	MAIL Command: 5 Minutes	65
4.5.3.2.3.	RCPT Command: 5 Minutes	65
4.5.3.2.4.	DATA Initiation: 2 Minutes	66
4.5.3.2.5.	Data Block: 3 Minutes	66
4.5.3.2.6.	DATA Termination: 10 Minutes	66
4.5.3.2.7.	Server Timeout: 5 Minutes	66
4.5.4.	Retry Strategies	66
4.5.5.	Messages with a Null Reverse-Path	68
5.	Address Resolution and Mail Handling	69
5.1.	Locating the Target Host	69
5.2.	IPv6 and MX Records	71
6.	Problem Detection and Handling	71

[RFC 5321](#)

SMTP

October 2008

D.1. A Typical SMTP Transaction Scenario

This SMTP example shows mail sent by Smith at host bar.com, and to Jones, Green, and Brown at host foo.com. Here we assume that host bar.com contacts host foo.com directly. The mail is accepted for Jones and Brown. Green does not have a mailbox at host foo.com.

```
S: 220 foo.com Simple Mail Transfer Service Ready
C: EHLO bar.com
S: 250-foo.com greets bar.com
S: 250-8BITMIME
S: 250-SIZE
S: 250-DSN
S: 250 HELP
C: MAIL FROM:<Smith@bar.com>
S: 250 OK
C: RCPT TO:<Jones@foo.com>
S: 250 OK
C: RCPT TO:<Green@foo.com>
S: 550 No such user here
C: RCPT TO:<Brown@foo.com>
S: 250 OK
C: DATA
S: 354 Start mail input; end with <CRLF>.<CRLF>
C: Blah blah blah...
C: ...etc. etc. etc.
C: .
S: 250 OK
C: QUIT
S: 221 foo.com Service closing transmission channel
```



SMTP Servers for experiments

Mon site | Mes liens | Bienvenue LIECHTI Olivier

Quicklinks
La boîte à outils des services HEIG-VD 

heig-vd HAUTE ÉCOLE D'INGÉNIERIE ET DE GESTION DU CANTON DE VAUD www.heig-vd.ch

Services Départements Ra&D Académique Campus Infrastructure Liens Conseil représentatif Rechercher 

Intranet HEIG-VD > Services > Informatique > Poste de travail > Messagerie > Configuration > **SMTP**

Webmail
Outlook
Configuration
Exchange
IMAP
POP
SMTP
LDAP
Archivage
Spam
Mailing
Réservation salles

Le protocole SMTP est utilisé lors de l'envoi des mails. Il est complémentaire aux protocoles POP et IMAP qui ne s'occupent que de la réception.

L'adresse de notre serveur SMTP est :

smtp.heig-vd.ch

Attention, pour lutter contre le spam ainsi que pour des raisons de sécurité, notre serveur smtp, comme bien d'autres, n'autorisent l'envoi d'e-mails que depuis l'intérieur de notre réseau (ou via vpn). Depuis chez vous, il faut utiliser le serveur smtp de votre fournisseur d'accès internet.

Pour en savoir plus : [wikipedia](#)

ATTENTION !!
Pour le moment, la connexion IMAP impose d'activer le SLL.



With this default setup, you will not be able to login with your user id / password.

My Account Sign-in & security

Welcome

Sign-in & security

- Signing in to Google
- Device activity & security events
- Apps with account access

Personal info & privacy

- Your personal info
- Contacts
- Manage your Google activity
- Ads Settings
- Control your content

Check your privacy settings →

Allow less secure apps: OFF 

Some apps and devices use less secure sign-in technology, which could leave your account vulnerable. You can turn off access for these apps (which we recommend) or choose to use them despite the risks.

Account preferences

- Payments
- Language & Input Tools
- Accessibility
- Your Google Drive storage

 Your security comes first in everything we do.
[LEARN MORE](#)



Email delivery done right.

[Pricing](#) [Product Tour](#) [Customers](#) [FAQ](#)

[Log In](#)

[Sign Up](#)

WORLDWIDE SMTP DELIVERY

Like a first-class courier, for email.

Easily send and track all of your emails, and forget headaches
with email delivery.

[See Plans & Pricing](#)

[Try SMTP2GO Free](#)





**“Mon métier,
c'est Johnny,”**

Portrait Johnny VEGAS

photo - nice matin

X
FERMER

Mock Servers

tweakers-dev / MockMock

Code Issues 2 Pull requests 4 Projects 0 Wiki Insights

Watch 10 Unstar 39 Fork 24

A mock SMTP server built with Java

MockMock Home MockMock on Github

I've got 24 mails for you. Nice! [Delete all](#)

From	To	Subject
John Doe <someone@example.org>	Some Dude <dude@examp...	Well, this is a nice subject...
John Doe <someone@example.org>	Some Dude <dude@examp...	LOL omg!
John Doe <someone@example.org>	Some Dude <dude@examp...	The iPhone 5 is huge!
John Doe <someone@example.org>	Some Dude <dude@examp...	Did you see the new MockMock version already?
John Doe <someone@example.org>	Some Dude <dude@examp...	Well, this is a nice subject...
John Doe <someone@example.org>	Some Dude <dude@examp...	Well, this is a nice subject...
John Doe <someone@example.org>	Some Dude <dude@examp...	Did you see the new MockMock version already?



The image shows the Mailtrap homepage. At the top, there is a navigation bar with links: HOW IT WORKS, PRICING, API, BLOG, FAQ, and HELP. There are also Log in and Sign up buttons. Below the navigation bar is a large, stylized illustration of a teal, anthropomorphic character with a wide, toothy grin, wearing a black fedora and a black and white striped suit. The character is holding a newspaper and a smartphone. A black net-like object is draped over its shoulder. Several small, sad-looking envelope icons are floating around the character. To the right of the character, there is a large smartphone displaying a similar envelope icon. Below the smartphone, the word "SAFE" is written in a large, bold, teal font, followed by the tagline "email testing for dev teams" in a smaller, italicized font. At the bottom left, there is a laptop screen showing a video player interface with the text "See How it Works", "Watch", and "Video". The overall theme is playful and professional.