Introduction to SMTP

RES, Lecture 4

Olivier Liechti

heig-vd

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 

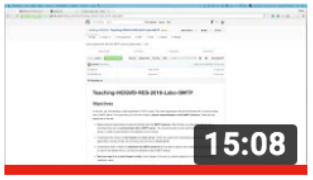
Labo SMTP, part 1

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 mailtrap.io	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

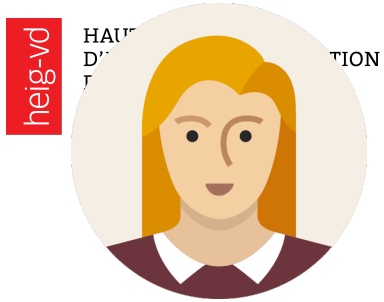
heig-vd
HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

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

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

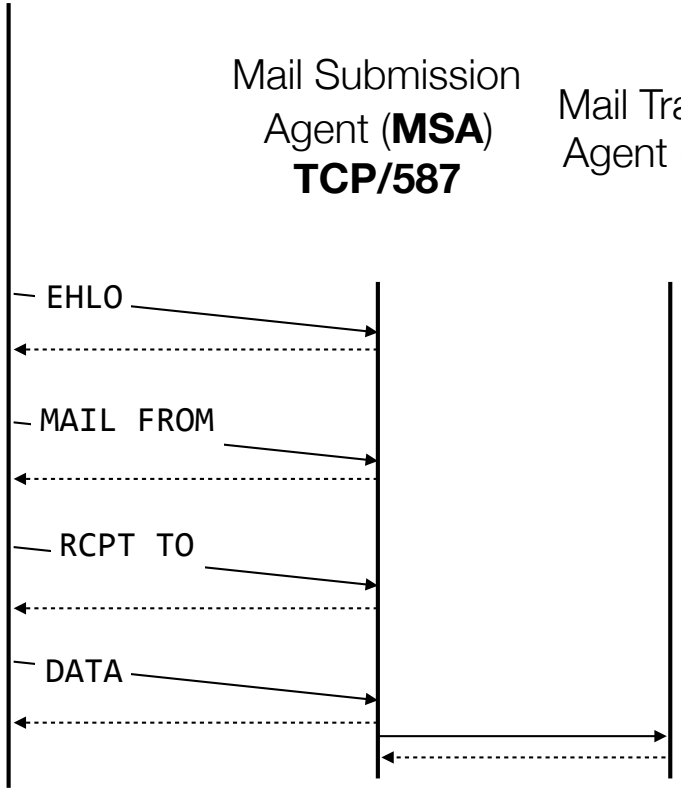
Alice uses **MS Outlook** to check and read her mails.

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.



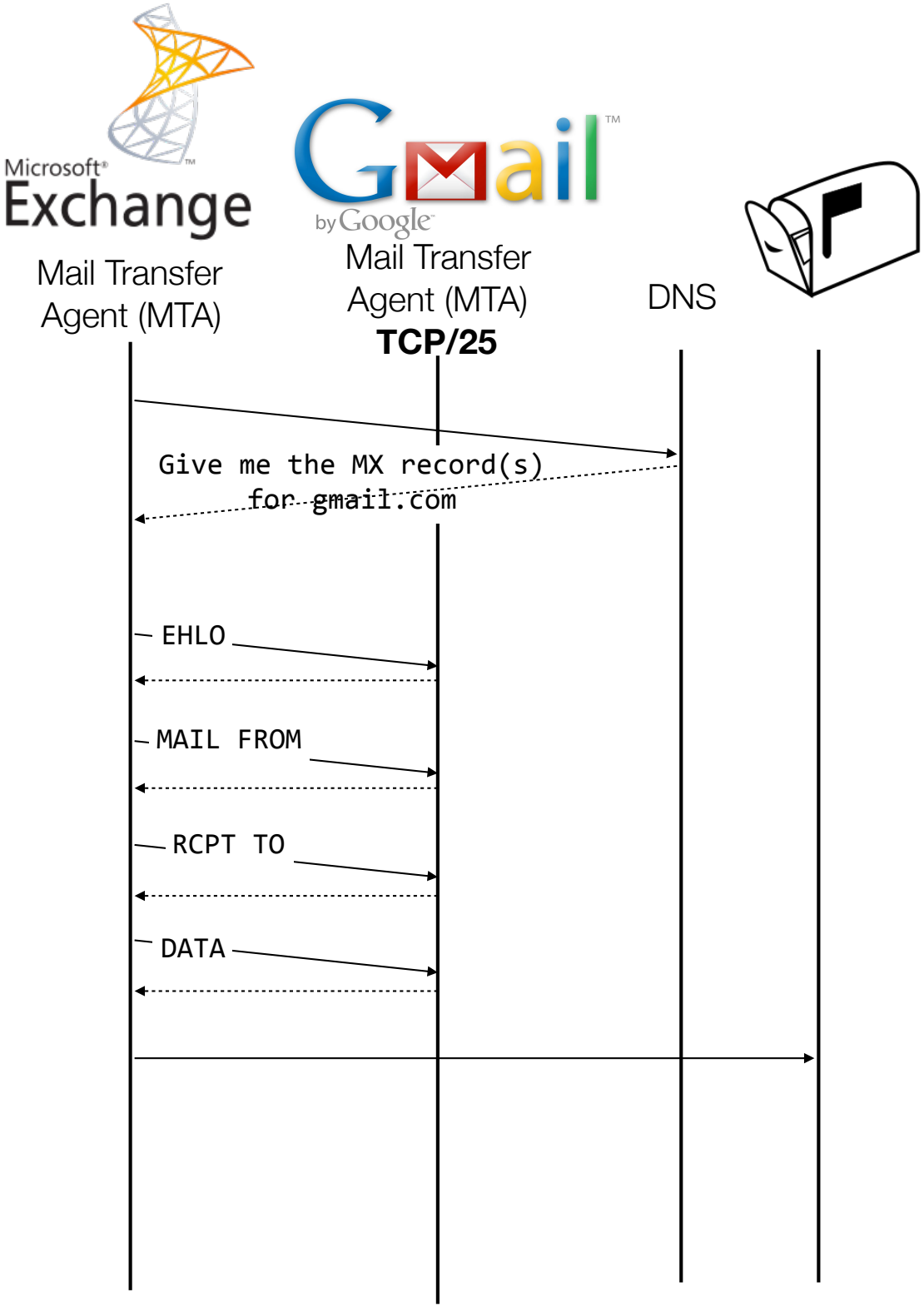
heig-vd
HAUTE ÉCOLE D'INGÉNIERIE ET DE GESTION DU CANTON DE VAUD
www.heig-vd.ch

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.



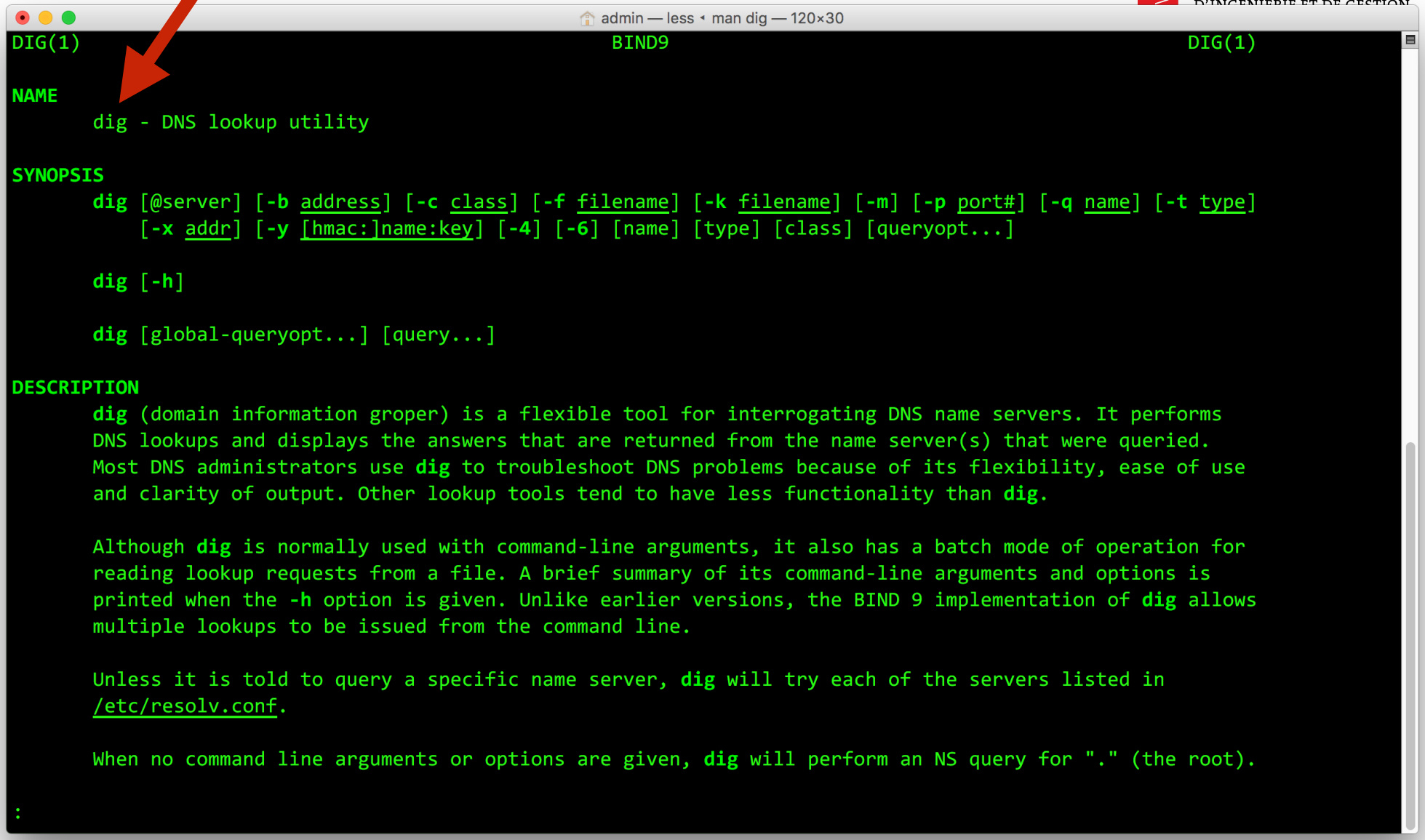
Bob's MTA initially does not know where to forward the mail…

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



`nslookup` is another command for querying DNS

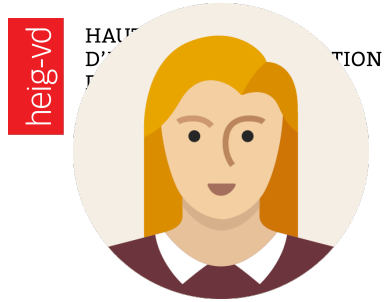
dig -t ANY heig-vd.ch

HAUTE ÉCOLE D'INGÉNIERIE ET DE GESTION

admin — -bash --login — 120×30

```
$ 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

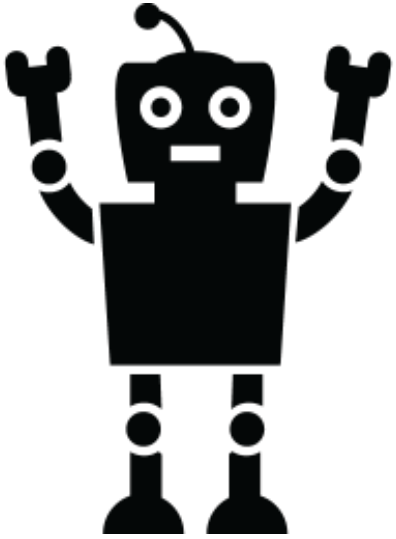
In the last step, Alice's MUA uses another protocol (e.g. IMAP, POP3) to fetch mails from the mailbox.

IMAP/POP3

SMTP
25

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~~

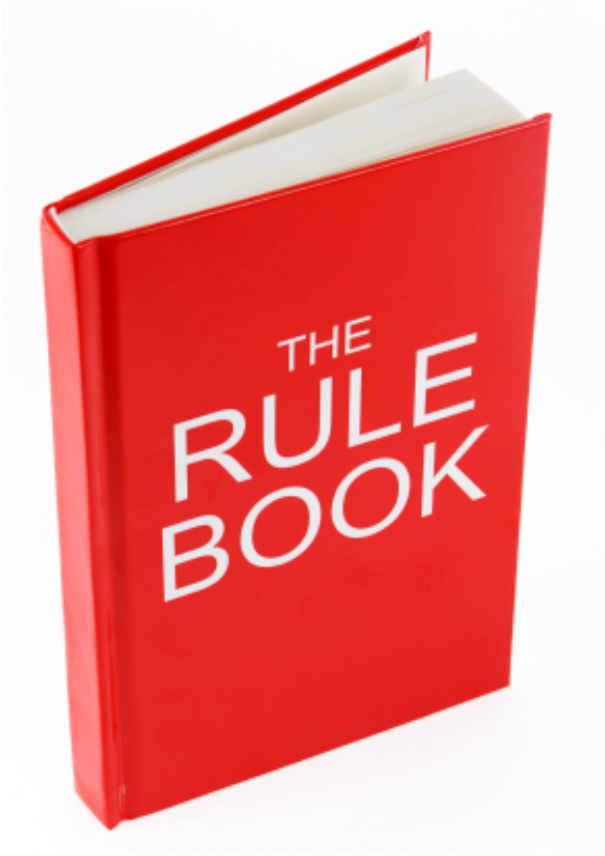
```
openssl s_client -starttls smtp -crlf -connect
mail01.heig-vd.ch:25 (or use 465)
```

```
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
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.
```

SMTP command
!=
Message header

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



The Specs

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

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

Table of Contents

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

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
```

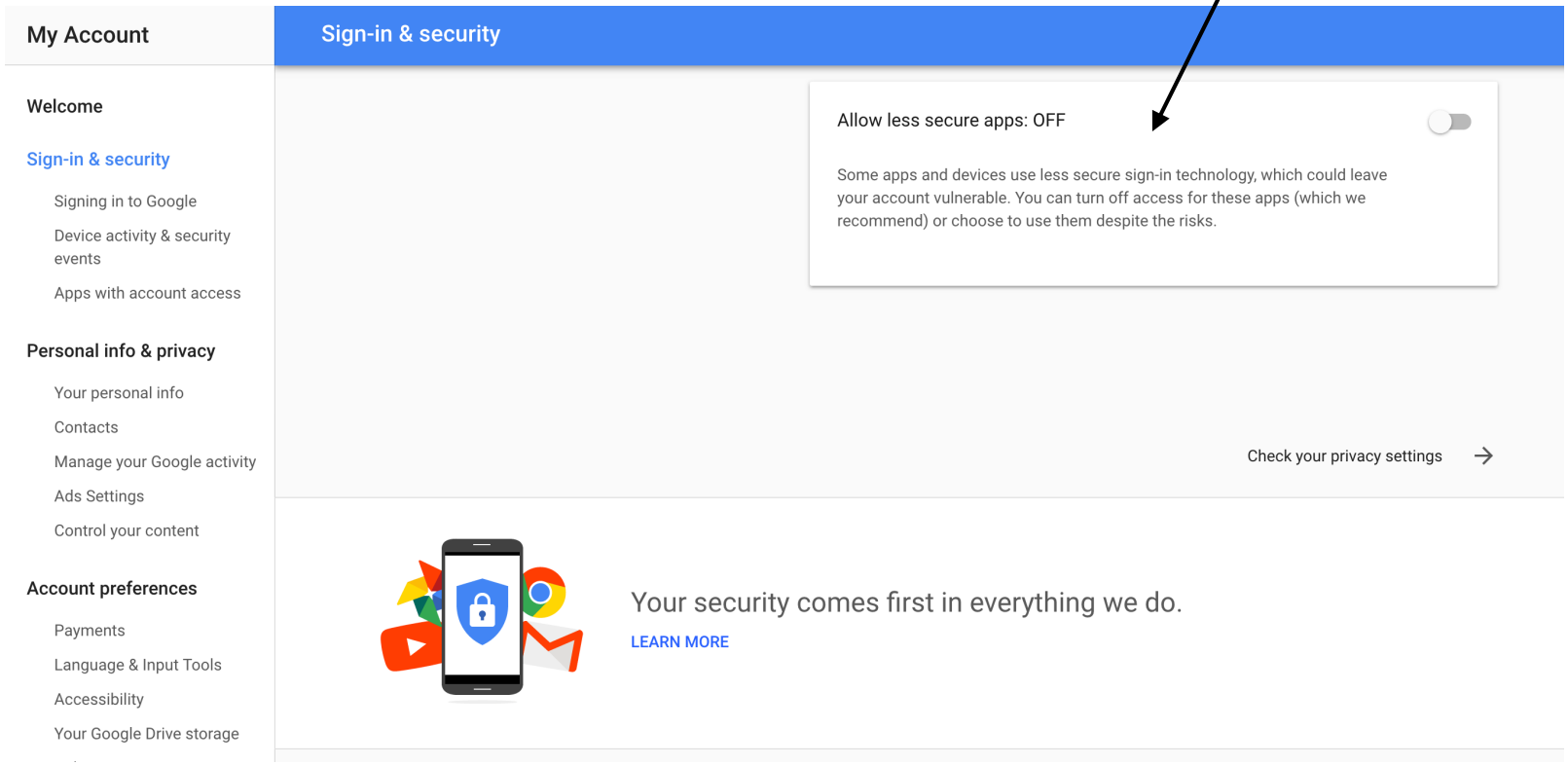
heig-vd
HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

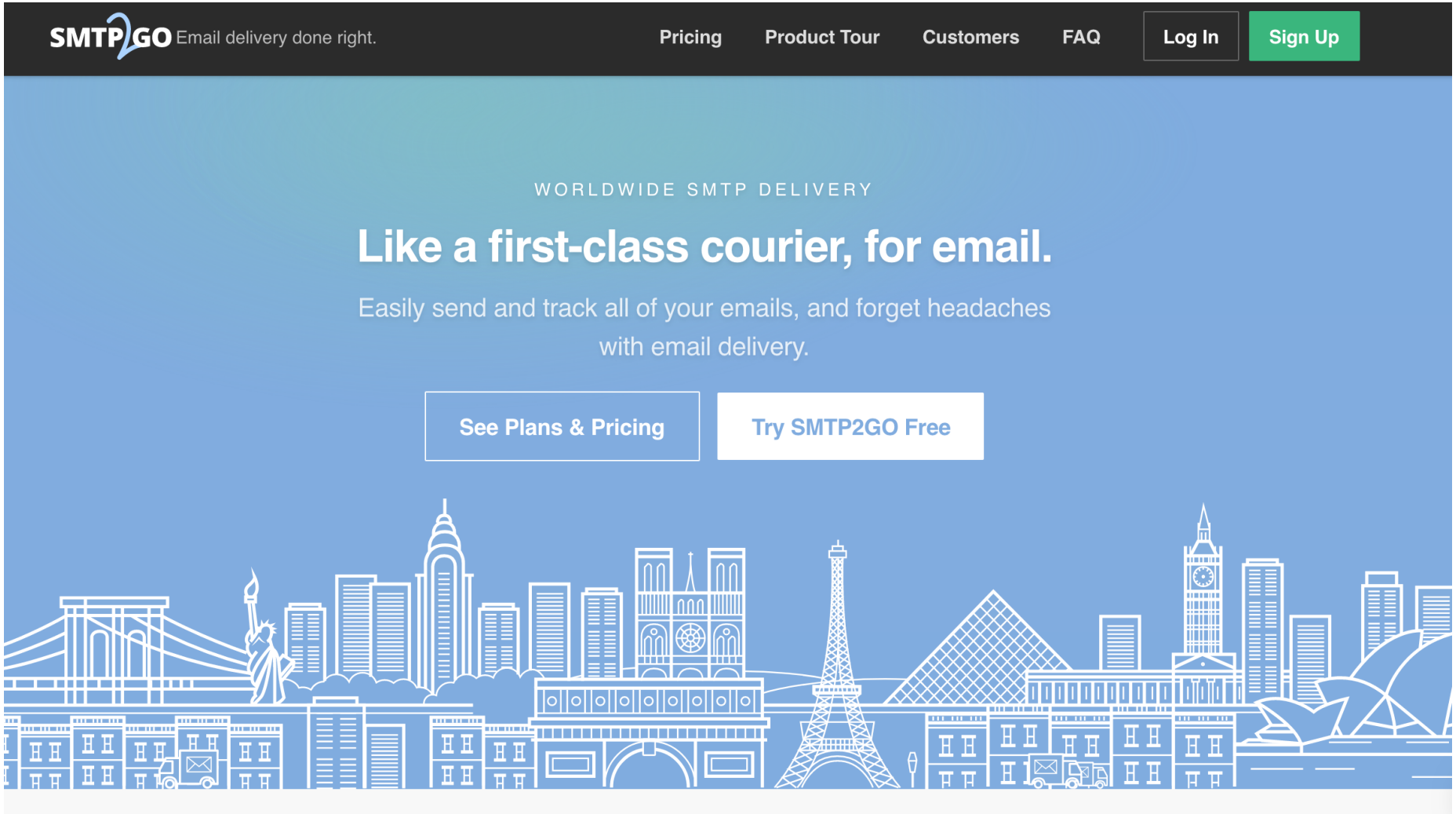
SMTP Servers for experiments

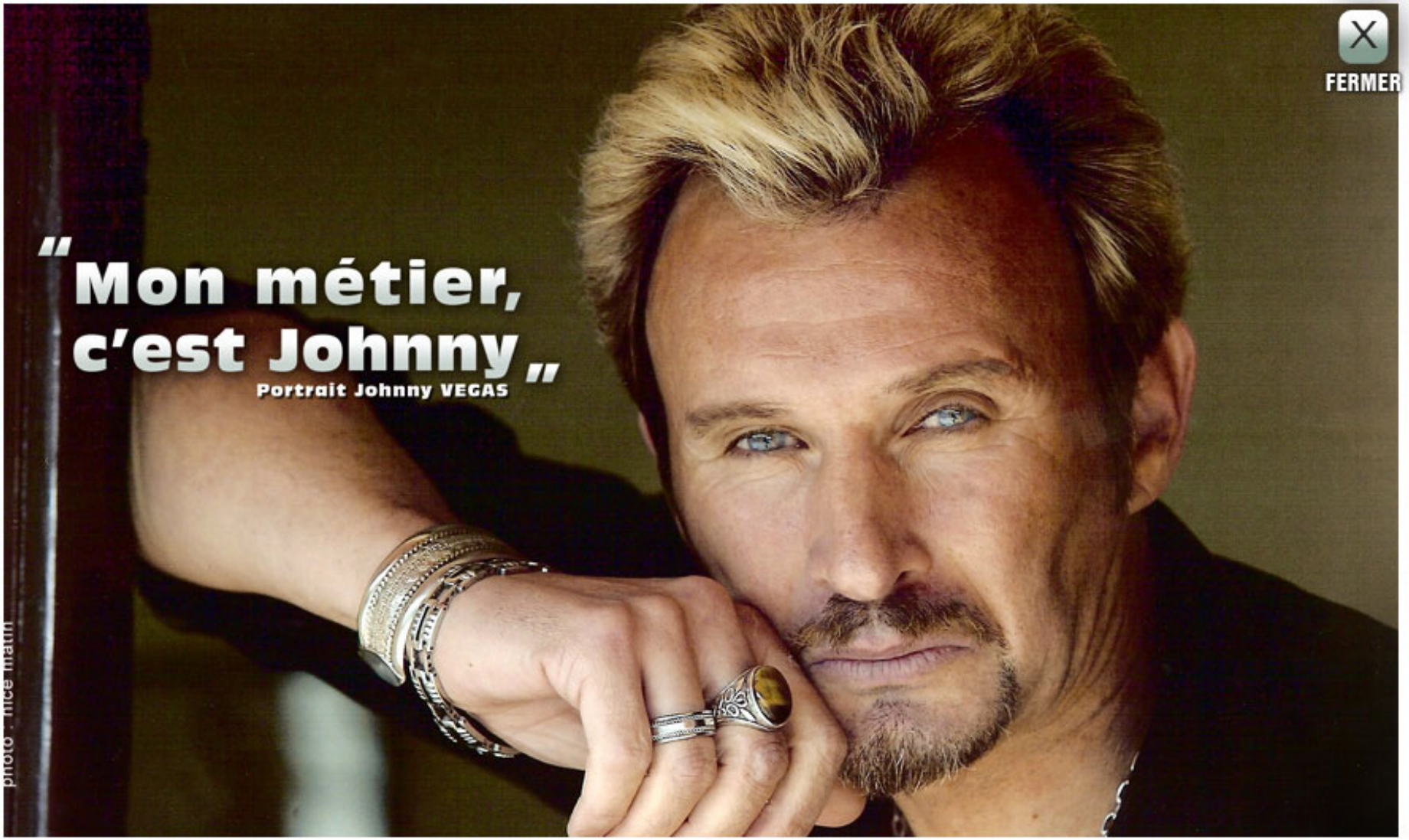

Mon site | Mes liens | Bienvenue LIECHTI Olivier
heig-vd
HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch
Quicklinks
La boîte à outils des services HEIG-VD
Services
Départements
Ra&D
Académique
Campus
Infrastructure
Liens
Conseil représentatif
Rechercher
Intranet HEIG-VD > Services > 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, por 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.

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

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




SMTP2GO 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



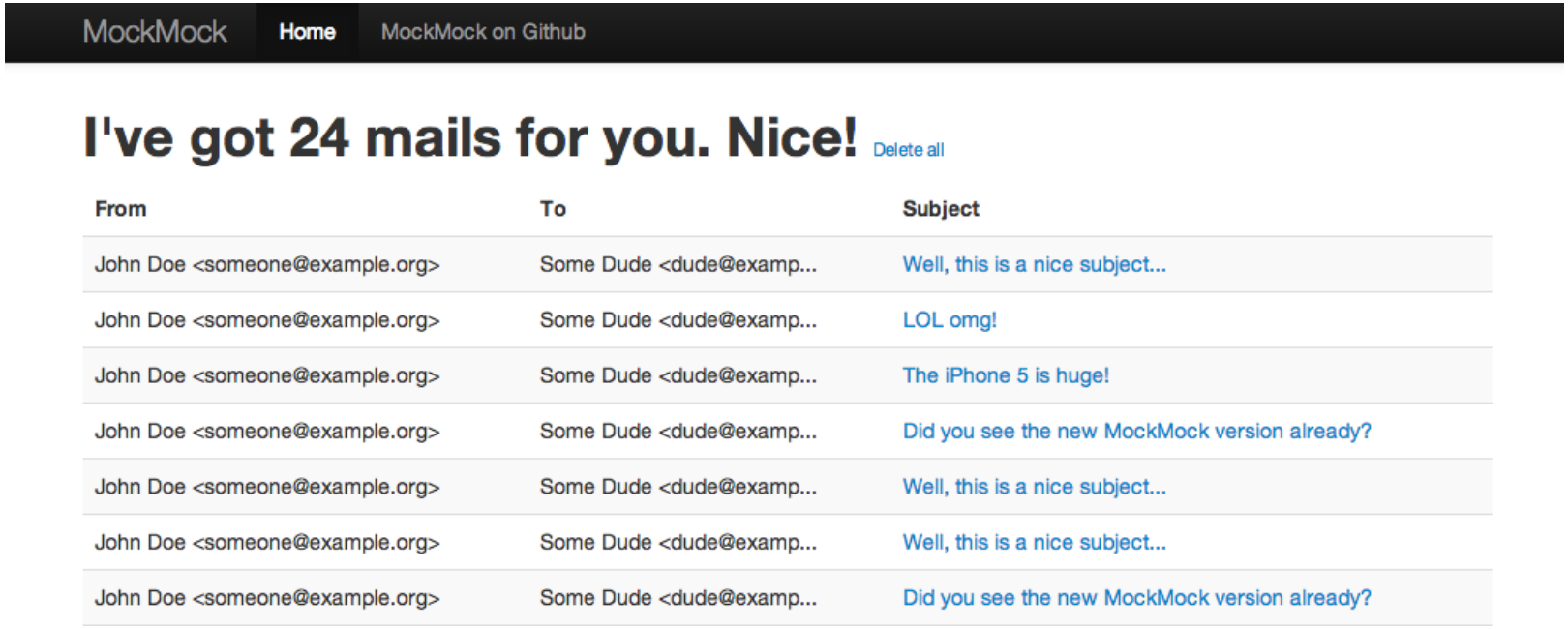
Mock Servers

tweakers-dev / **MockMock**

Watch 10 | Unstar 39 | Fork 24

Code | Issues 2 | Pull requests 4 | Projects 0 | Wiki | Insights

A mock SMTP server built with Java




mailtrap
HOW IT WORKS
PRICING
API
BLOG
FAQ
HELP
Log in
Sign up
railsware
SAFE
email testing
for dev teams
See How it Works
Watch
Video