

SMTP - Memo

DIG

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

Fait un requête DNS et le retour permet de trouvé les serveur smtp

```
; <<>> DiG 9.10.3-P4-Debian <<>> -t ANY heig-vd.ch
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38885
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 11, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;heig-vd.ch.                IN  ANY

;; ANSWER SECTION:
heig-vd.ch.      3600    IN  SOA ns01.heig-vd.ch. domain.heig-vd.ch. 2014142674 10800 3600
2419200 900
heig-vd.ch.      3600    IN  MX  10 mailcl5.heig-vd.ch.
heig-vd.ch.      3600    IN  MX  20 mailcl0.heig-vd.ch.
heig-vd.ch.      3600    IN  MX  10 mailcl3.heig-vd.ch.
heig-vd.ch.      3600    IN  MX  10 mailcl4.heig-vd.ch.
heig-vd.ch.      3600    IN  TXT "v=spf1 ip4:193.134.216.180/30 mx ~all"
heig-vd.ch.      3600    IN  TXT "MS=ms50694826"
heig-vd.ch.      3600    IN  TXT "v=spf1 ip4:193.134.216.180/30 ip4:193.134.218.105
ip4:193.134.216.126 ip4:193.134.216.121 mx ~all"
heig-vd.ch.      3600    IN  A   193.134.222.245
heig-vd.ch.      3600    IN  NS  ns02.heig-vd.ch.
heig-vd.ch.      3600    IN  NS  ns01.heig-vd.ch.

;; Query time: 2 msec
;; SERVER: 10.192.22.5#53(10.192.22.5)
;; WHEN: Tue Apr 10 11:08:28 CEST 2018
;; MSG SIZE rcvd: 418
```

MX (Mail eXange) sont les serveurs SMTP.

Telnet

On peut ensuite discuter avec le serveur avec telnet

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

```
> EHLO local
250-mailcl0.heig-vd.ch Hello james-pc.einet.ad.eivd.ch [10.192.115.77]
250-SIZE 20480000
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP
> MAIL FROM:<james.smith@heig-vd.ch>
> RCPT TO:<jeremie.chatillon@heig-vd.ch>
> DATA
> From:bill.gates@msft.com
> To:olivier.liechti@heig-vd.ch
> Subject:Hi!

Hello buddy,
Give me your money
.
```

- **EHLO**: Init  la communication et normalement on donne le nom du serveur qui essaie de se connecter
 - HELO est une ancienne version
 - Ca nous donne les commandes disponibles sur le serveur
- En cas de demande de login, il faut donner le nom d'utilisateur et le mdp en **base 64** (<https://www.base64encode.org/>)
 - En ligne de commande (Linux)

```
echo -n '<motAEncoder>' | base64
```

OpenSSL

Possible de le faire avec Open SSL:

```
openssl s_client -starttls smtp -crlf -connect mailcl0.heig-vd.ch:25
```

Mail testing

<https://mailtrap.io/>