

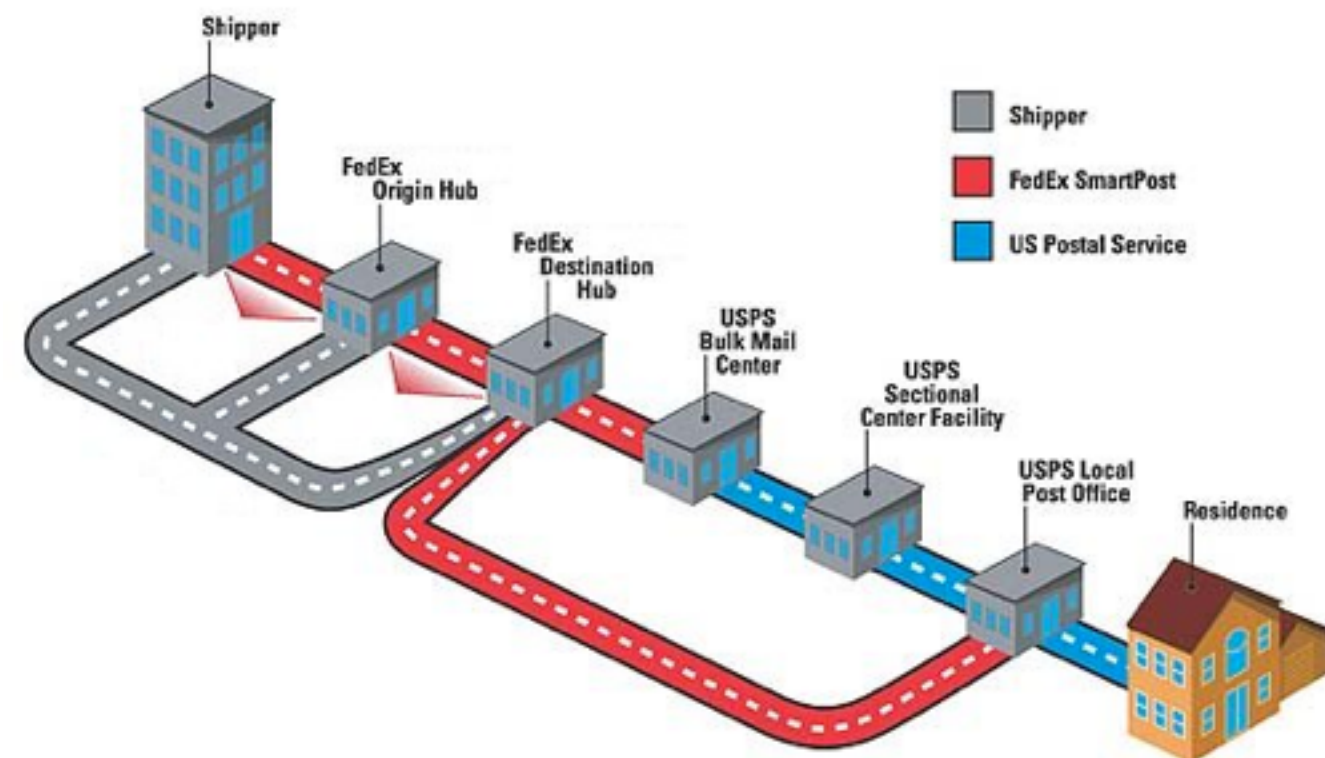
Introduction to SMTP and e-mail

RES, Lecture 3

Olivier Liechti

heig-vd

Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud





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.



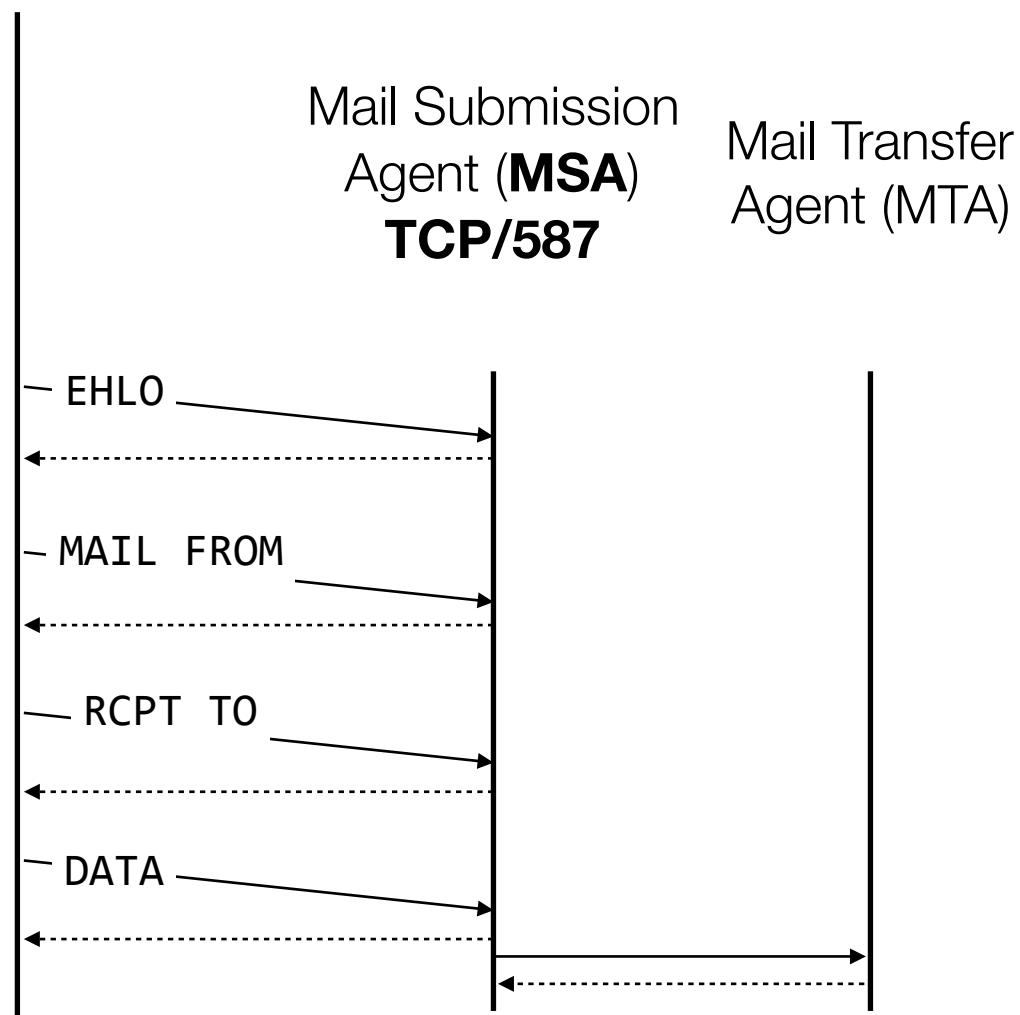


Bob writes a message to “**alice.res@gmail.com**”. He pushes on the “Send” button.

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.



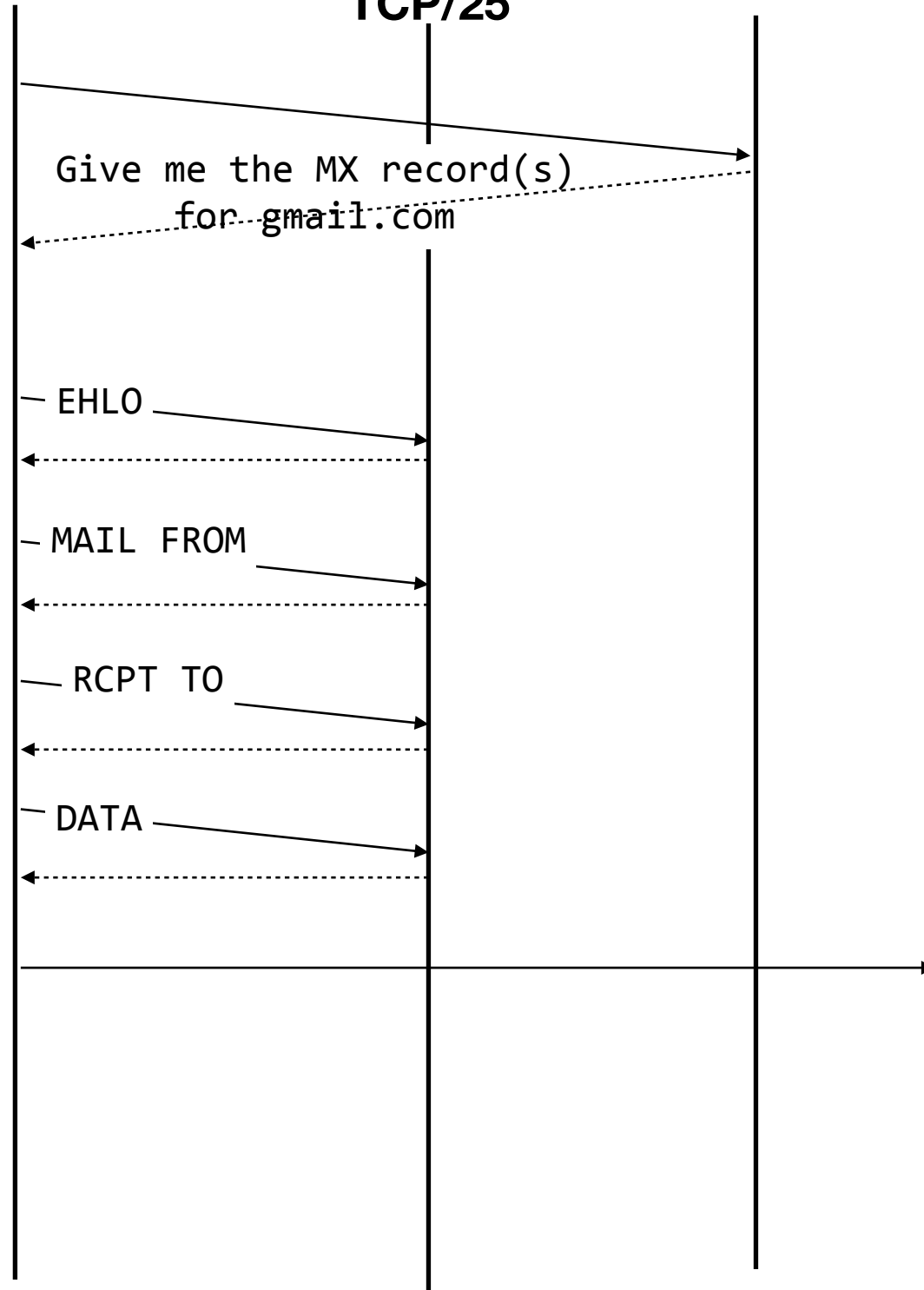


Mail Transfer
Agent (MTA)

Mail Transfer
Agent (MTA)

DNS

TCP/25



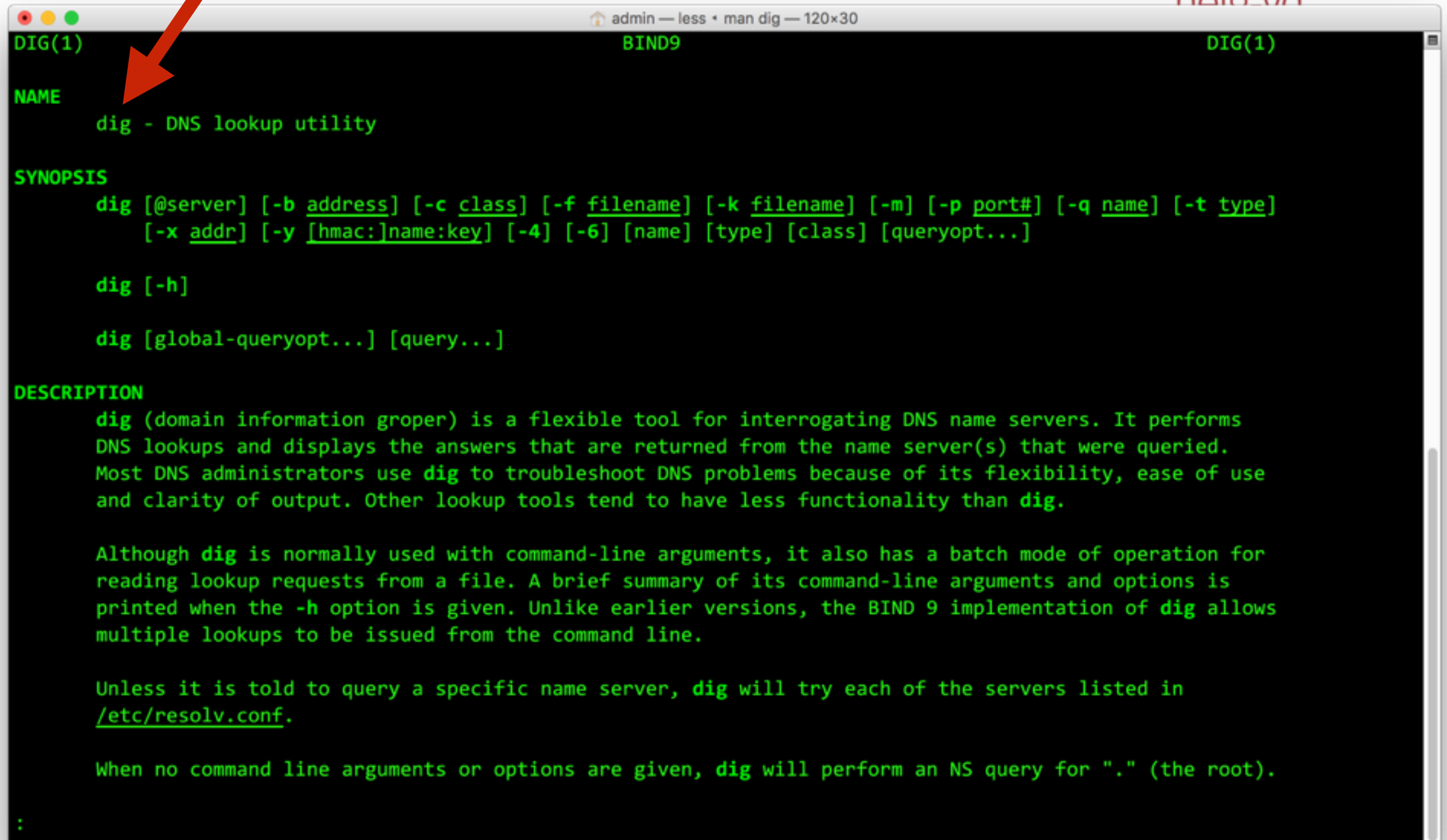
Bob's MTA initially does not know where to forward the mail...

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)                                BIND9                                DIG(1)

NAME
    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.

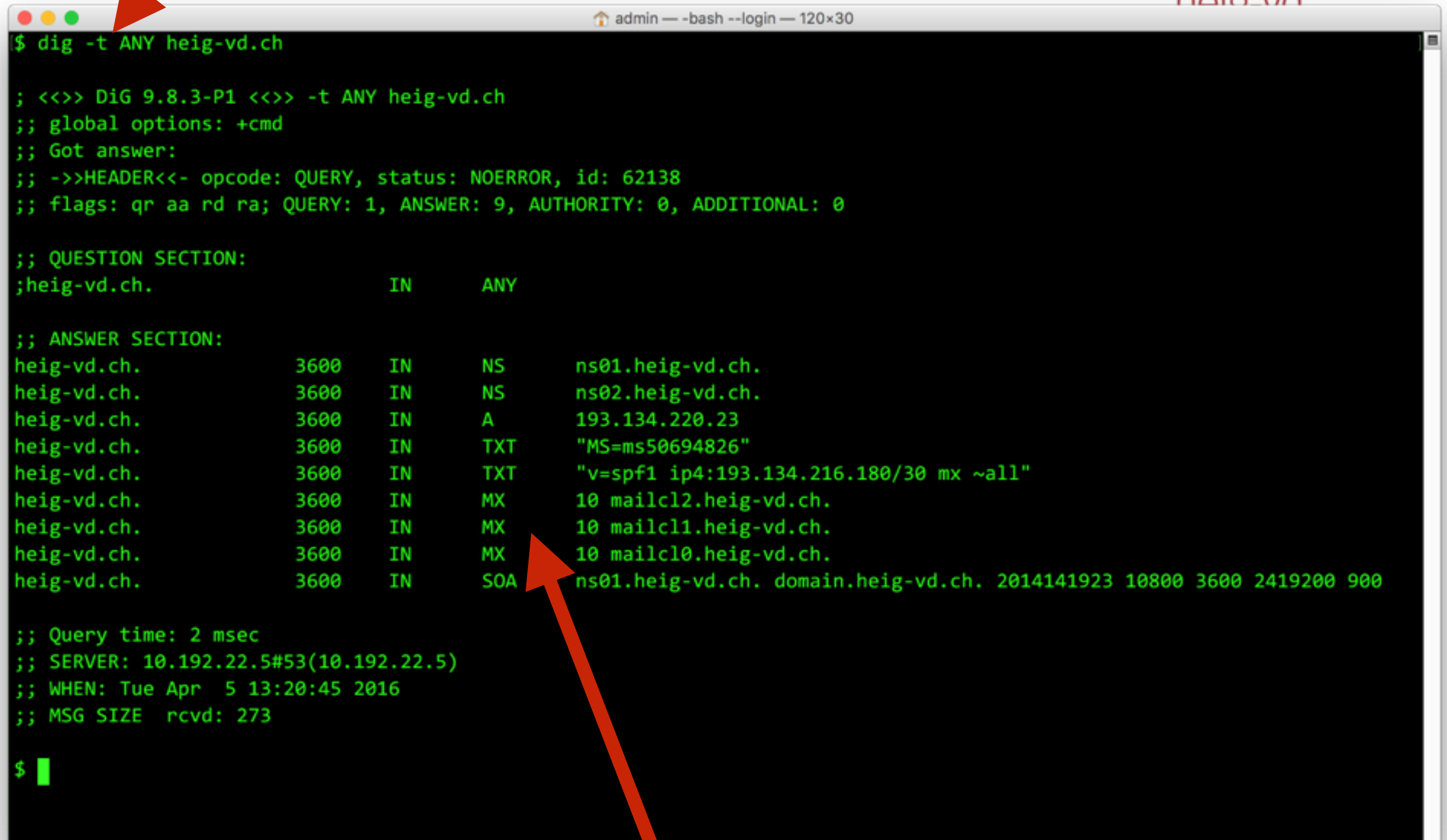
    Although dig is normally used with command-line arguments, it also has a batch mode of operation for
    reading lookup requests from a file. A brief summary of its command-line arguments and options is
    printed when the -h option is given. Unlike earlier versions, the BIND 9 implementation of dig 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

A terminal window titled 'admin - bash --login - 120x30' displays the output of a 'dig' command. A red arrow points from the command 'dig -t ANY heig-vd.ch' at the top to the terminal input. Another red arrow points from the 'MX' records in the output to the text 'MX records' at the bottom. The output shows various DNS records including NS, A, TXT, and MX for the domain 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

$
```

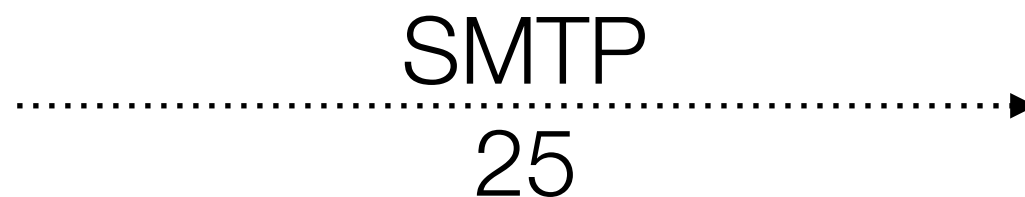
MX records point to the SMTP servers for the domain



SMTP
587



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



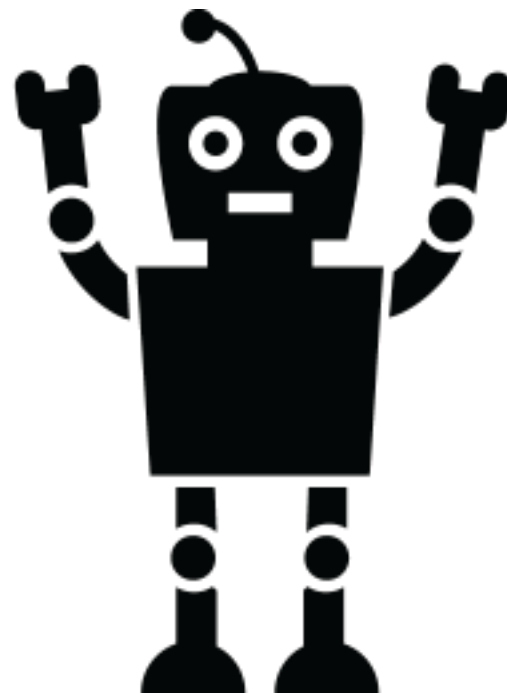
IMAP/POP3





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. 3600 INMX 10 mailcl0.heig-vd.ch.
```

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

```
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



FERMER

**"Mon métier,
c'est Johnny,"**
Portrait Johnny VEGAS

photo : nice main

Mock Servers