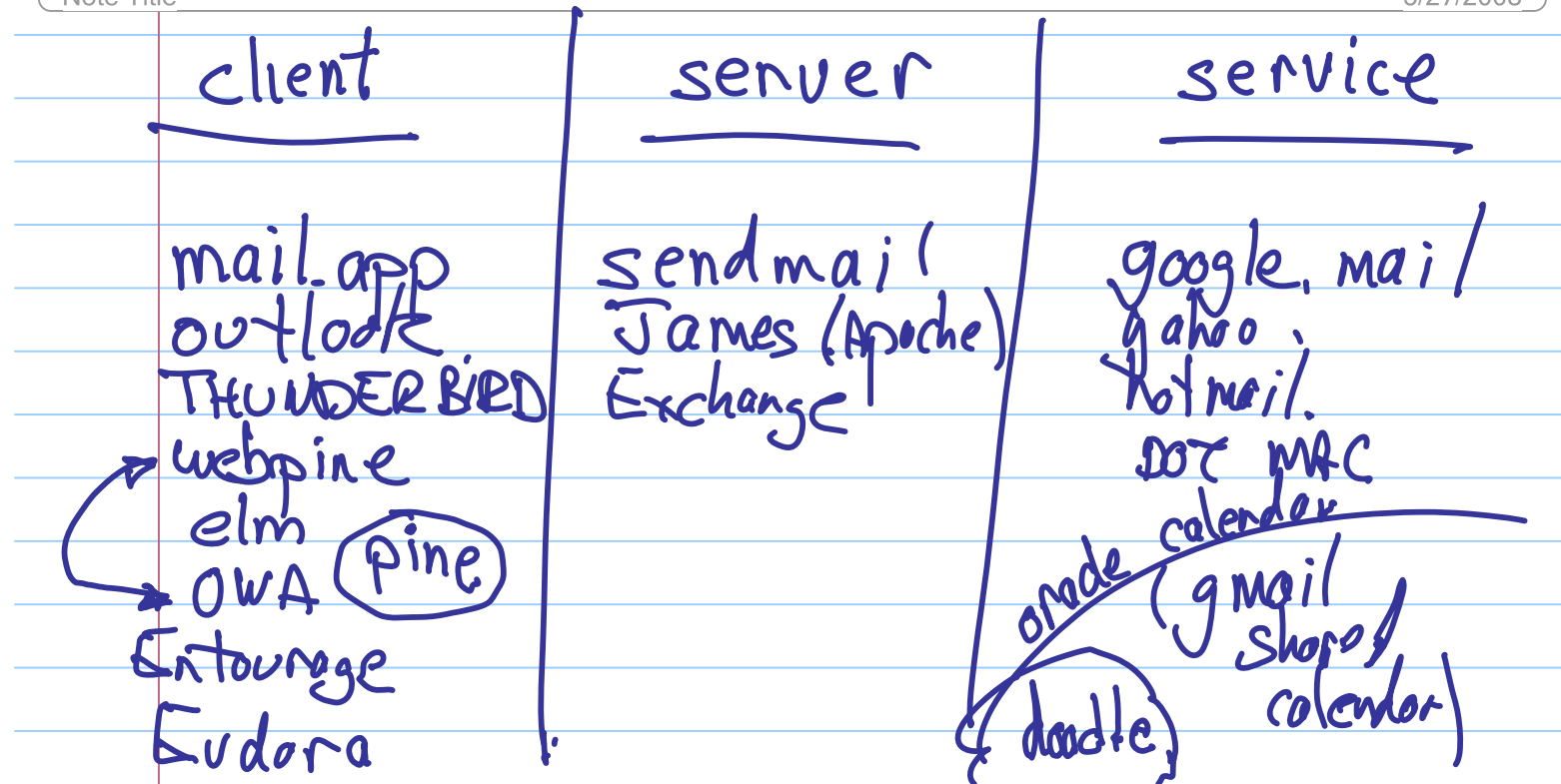


Lesson_17_Email

Note Title

5/27/2008



you



connect to ISP
get mail from mail server

johnb@



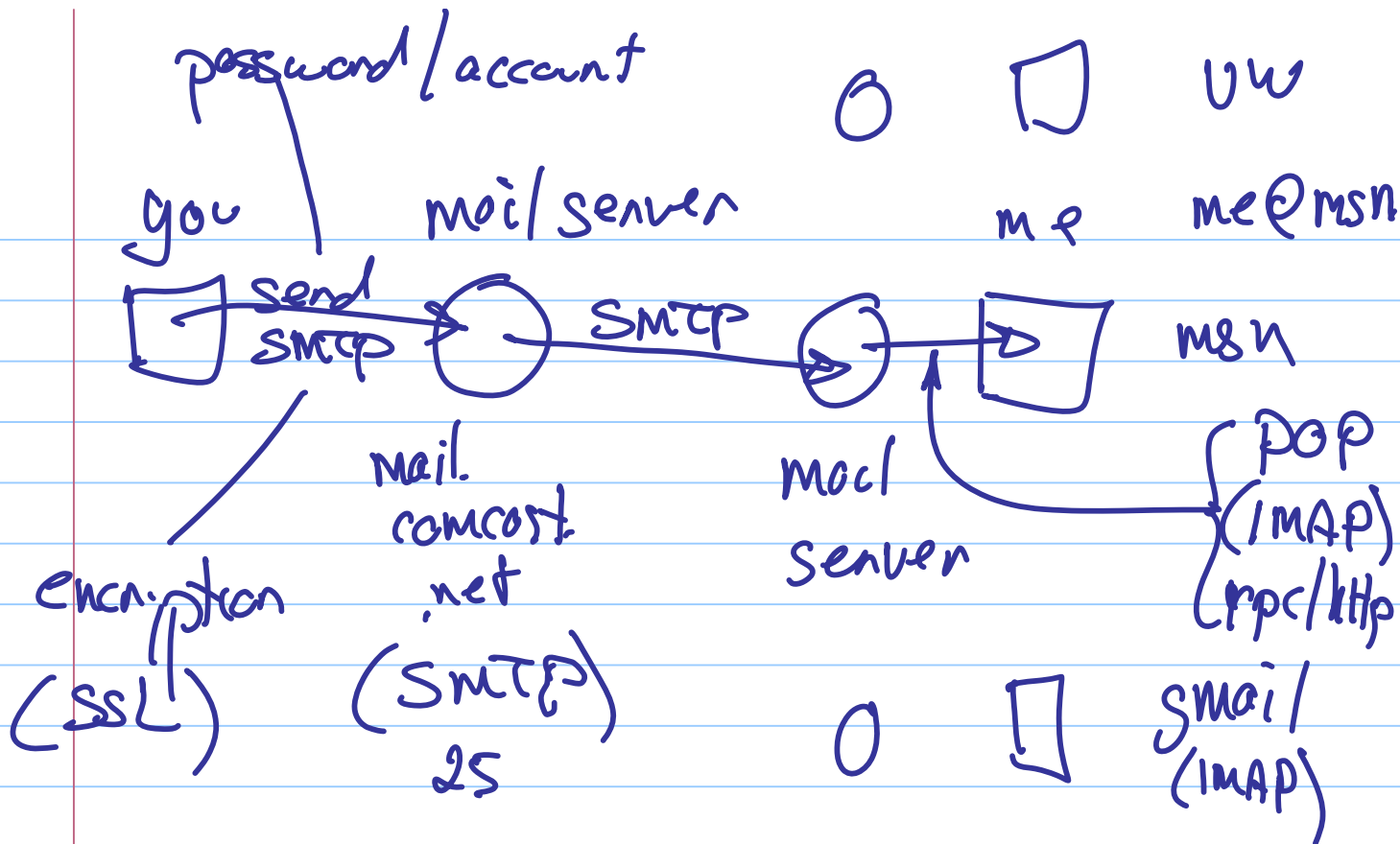
hpbu jpb
└─┬─┘

store your email
in "mailboxes"

local folders

from other mail
server

from another client



DNS nslookup msn.com

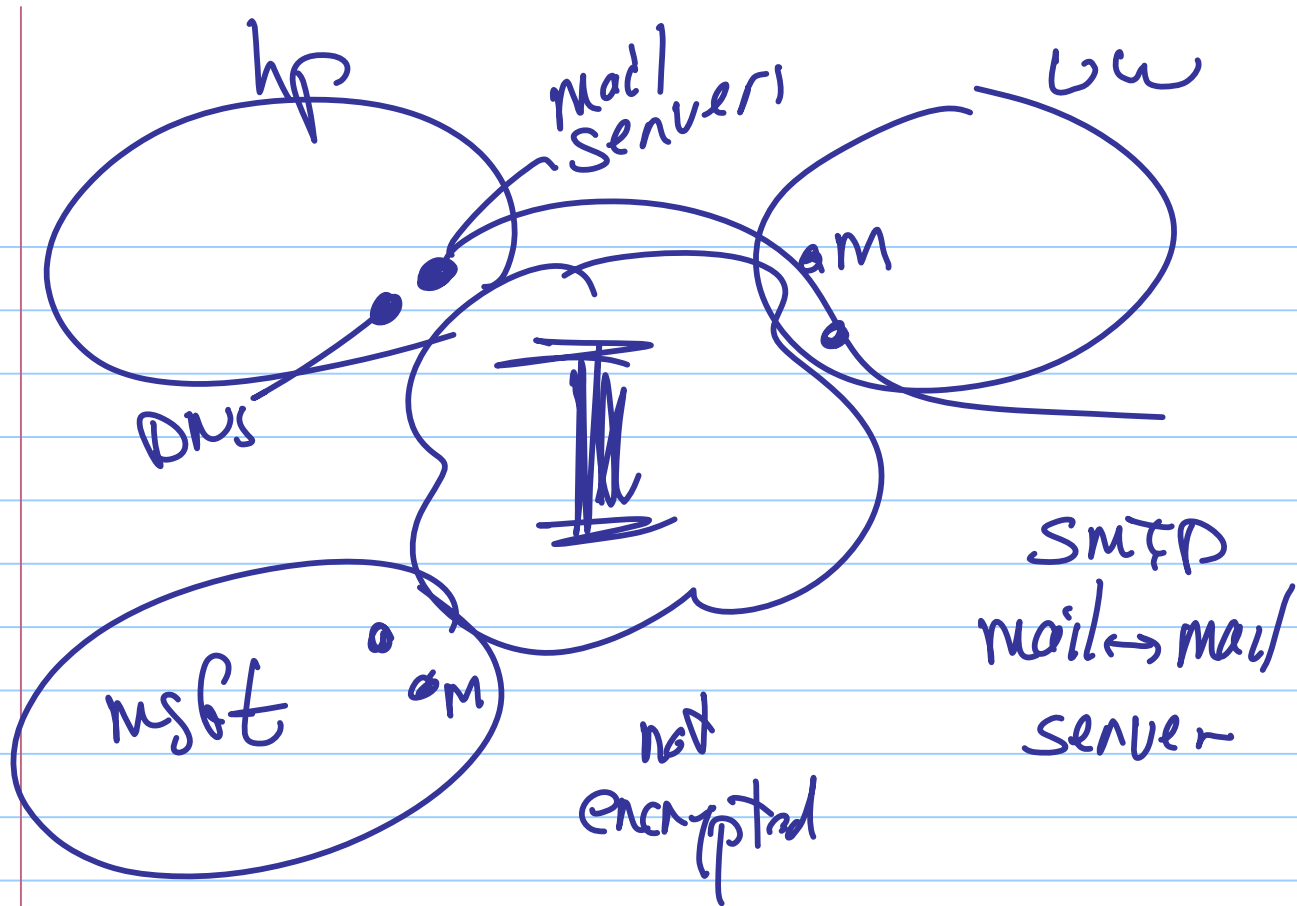
nslookup 10.10.10.10

MX (mail exchange)

(a) lookup MX for msn.com

(b) lookup IP of that MX

(c) send mail to IP.



dig
nslookup any

malpego

> set type = mx

> hp.com

smtp.hp.com

several

rot 13

(SSL accelerator = hardware)

PGP S/MIME public } keys
 private }

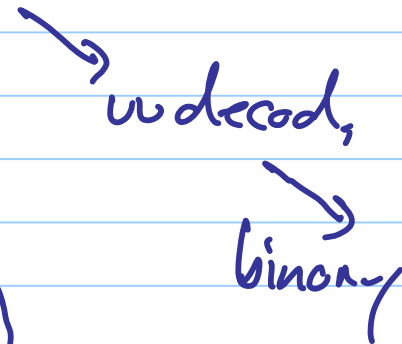
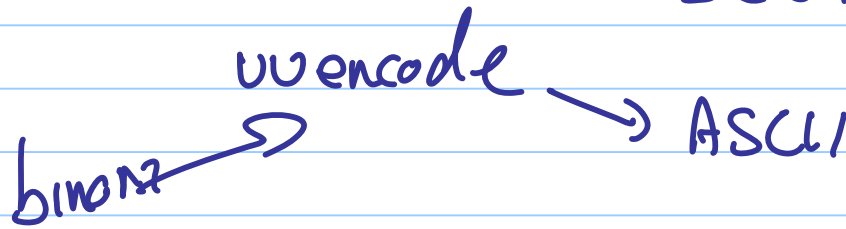
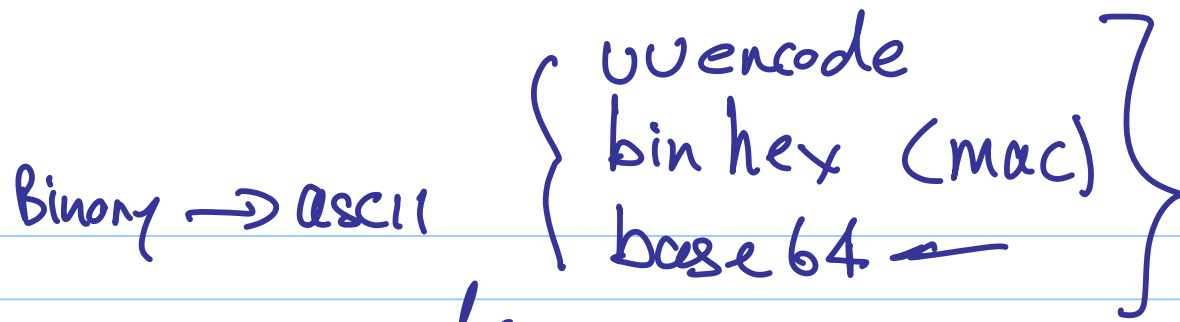
{ sign } email
 { encrypt }

SMTP (simple) protocol
text command line

A →
B →
C →

} ASCII code
7-bit
printable
characters

cannot send binary directly



attachment (> 1 of them)

MIME (simple ASCII headers)

view in RAW mode.

smtp headers

are they specified?

check time stamps

SPAM

-(4-400)

google hock
johnny long

Google

"axls-cgi"

john@blammers.org

john AT blammers
DOT org

john NOSPAM@blammers
.org

use obfuscators
javascript
html obfuscator

email → image

mailto:

anti - spam

- spam assassin

- thunder bird



Jay's demo : laptop + BackTrack 3
sendmail / running

rename host : gmail.com
php script

sent SPAM to himself

<http://johnny.ihackstuff.com/>