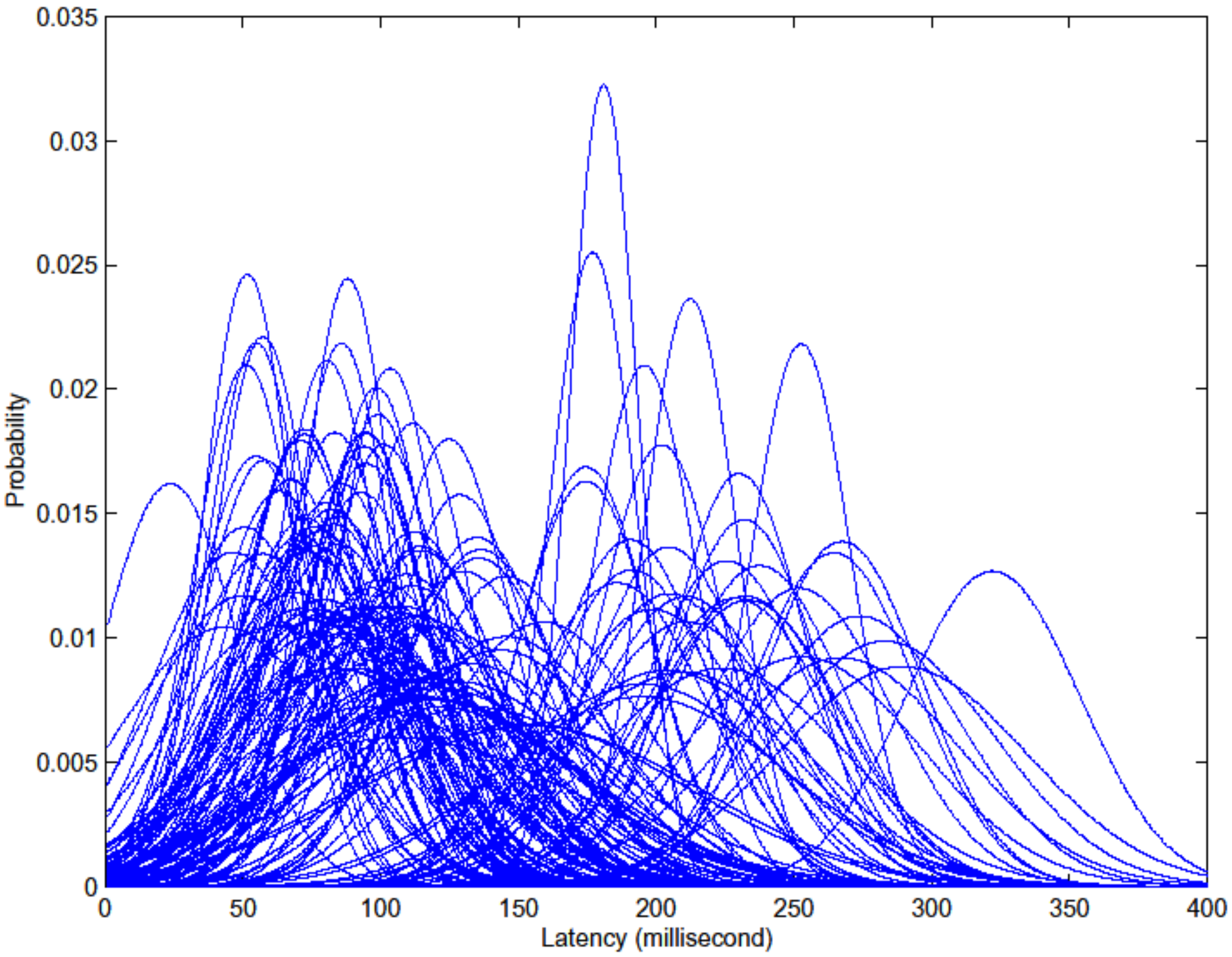


Figure 5: Estimated Gaussian distributions of all 142 character pairs collected from a user.

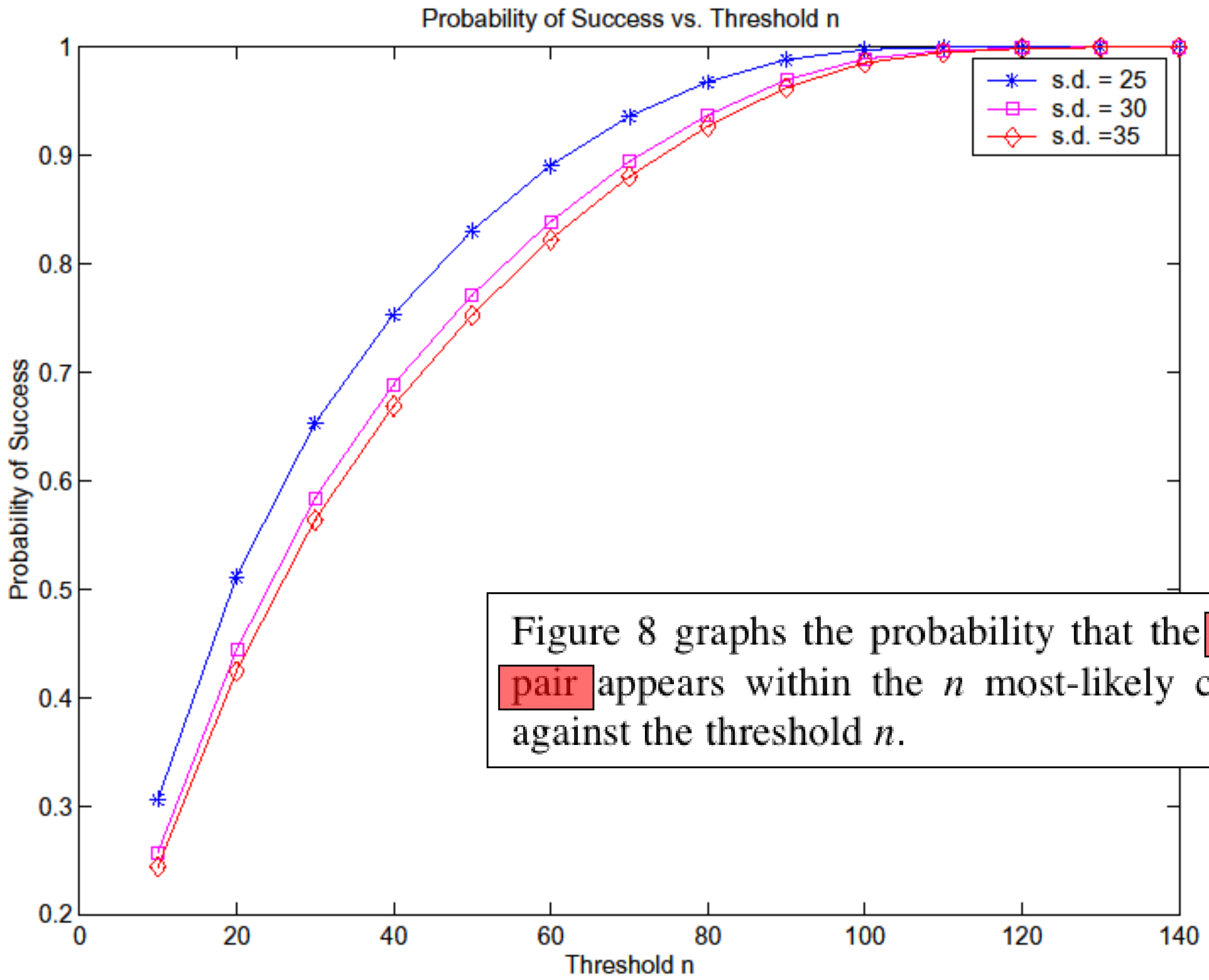


Figure 8 graphs the probability that the real character pair appears within the *n* most-likely character pairs against the threshold *n*.

Figure 8: The probability that the *n*-Viterbi algorithm outputs the correct ~~password~~ before the first *n* guesses, graphed as a function of *n*.

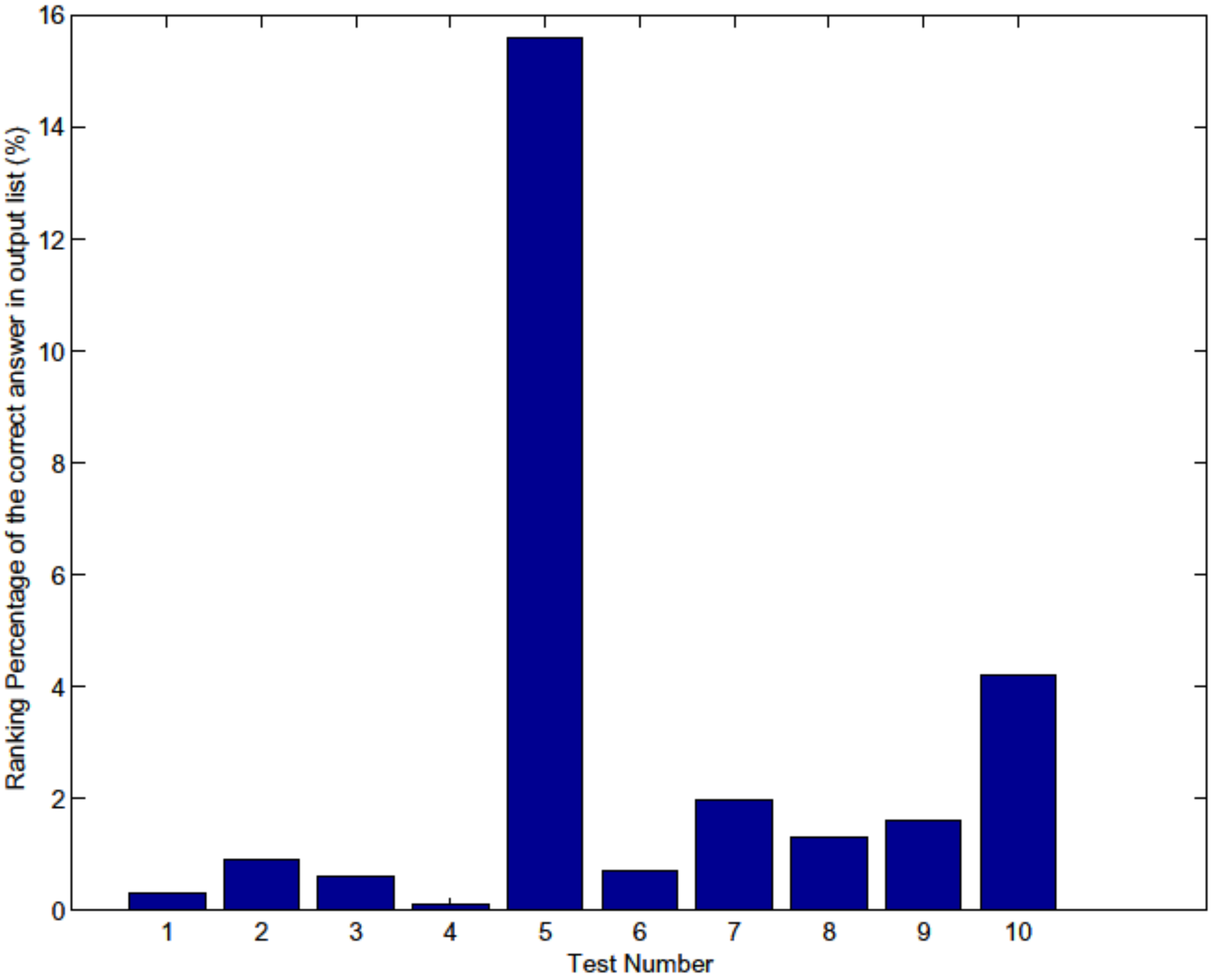
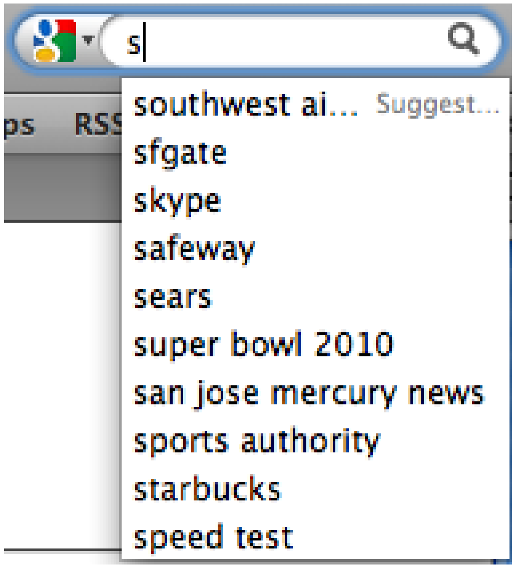


Figure 10: The percentage of the password space tried by Herbivore in 10 tests before finding the right password.

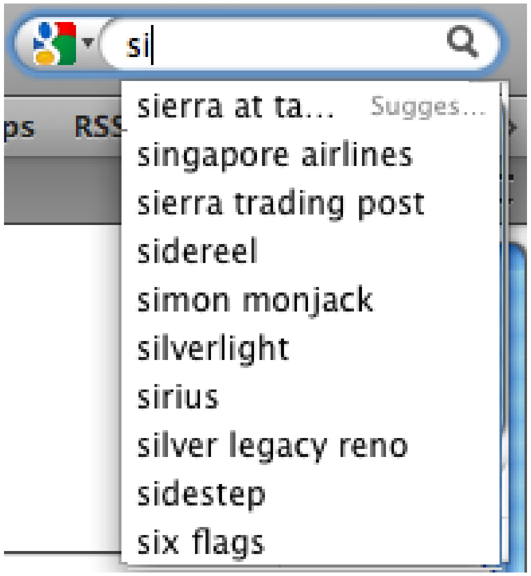
Training Set	Test Set	Test Cases				
		Password 1	Password 2	Password 3	Password 4	Password 5
User 1	User 1	15.6%	0.7%	2.0%	1.3%	1.6%
User 1	User 2	62.3%	15.2%	7.0%	14.8%	0.3%
User 1	User 3	6.4%	N/A	1.8%	3.1%	4.2%
User 1	User 4	1.9%	31.4%	1.1%	0.1%	28.8%
User 2	User 1	4.9%	1.3%	1.6%	12.3%	3.1%
User 2	User 2	30.8%	15.0%	2.8%	3.7%	2.9%
User 2	User 3	4.7%	N/A	5.3%	6.7%	38.4%
User 2	User 4	0.7%	16.8%	3.9%	0.6%	5.4%

Table 1: Success rates for password inference with multiple users. The numbers are the percentage of the search space the attacker has to search before he finds the right password.



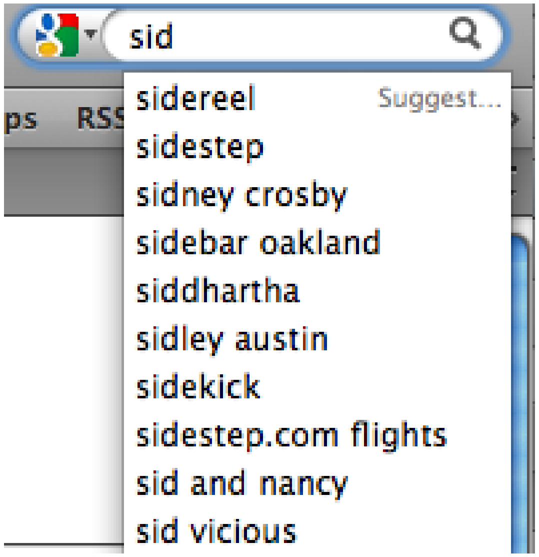
s

southwest ai... Suggest...
sfgate
skype
safeway
sears
super bowl 2010
san jose mercury news
sports authority
starbucks
speed test



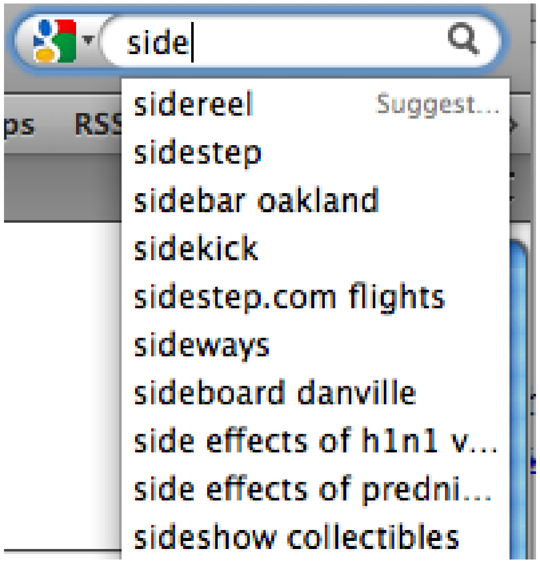
si

sierra at ta... Sugges...
singapore airlines
sierra trading post
sidereel
simon monjack
silverlight
sirius
silver legacy reno
sidestep
six flags



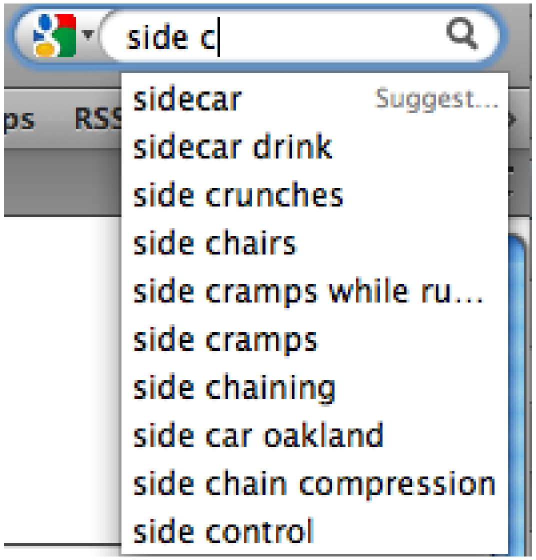
sid

sidereel Suggest...
sidestep
sidney crosby
sidebar oakland
siddhartha
sidley austin
sidekick
sidestep.com flights
sid and nancy
sid vicious



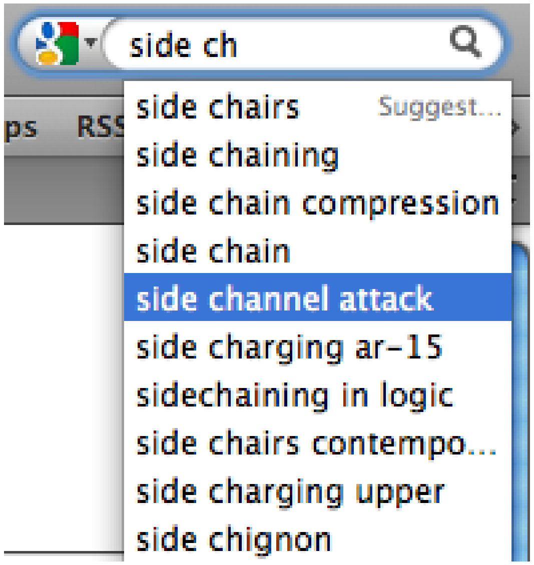
side

sidereel Suggest...
sidestep
sidebar oakland
sidekick
sidestep.com flights
sideways
sideboard danville
side effects of h1n1 v...
side effects of predni...
sideshow collectibles



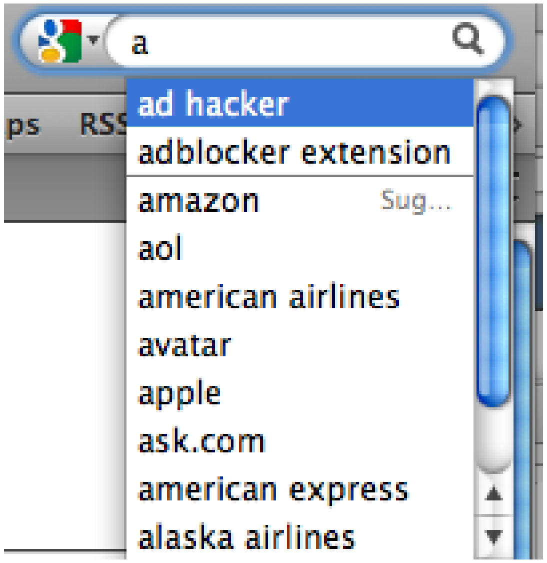
side c

sidecar Suggest...
sidecar drink
side crunches
side chairs
side cramps while ru...
side cramps
side chaining
side car oakland
side chain compression
side control



side ch

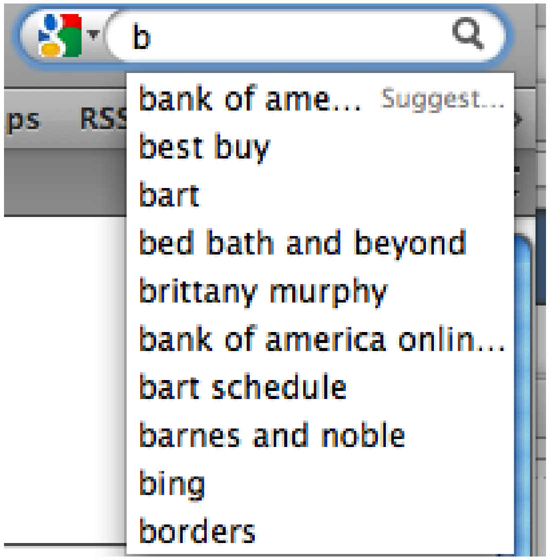
side chairs Suggest...
side chaining
side chain compression
side chain
side channel attack
side charging ar-15
sidechaining in logic
side chairs contempo...
side charging upper
side chignon



a

ad hacker
adblocker extension
amazon Sug…
aol
american airlines
avatar
apple
ask.com
american express
alaska airlines

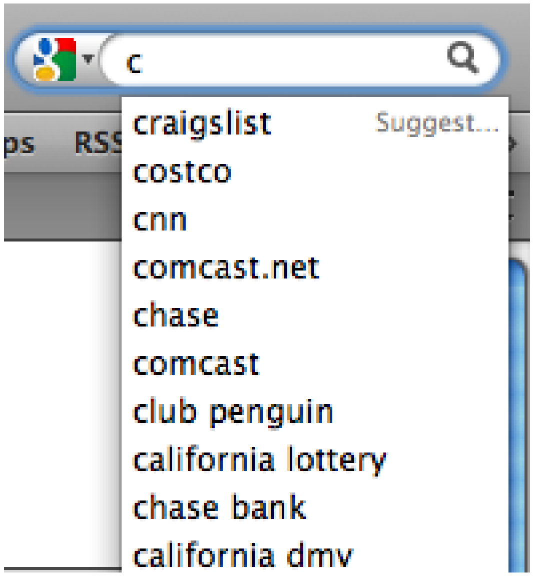
102 chars.



b

bank of ame… Suggest…
best buy
bart
bed bath and beyond
brittany murphy
bank of america onlin…
bart schedule
barnes and noble
bing
borders

125 chars.

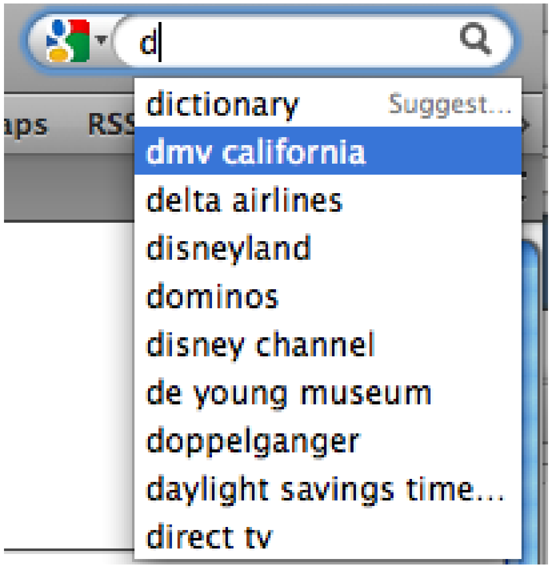


c

craigslist Suggest…
costco
cnn
comcast.net
chase
comcast
club penguin
california lottery
chase bank
california dmv

107 chars.

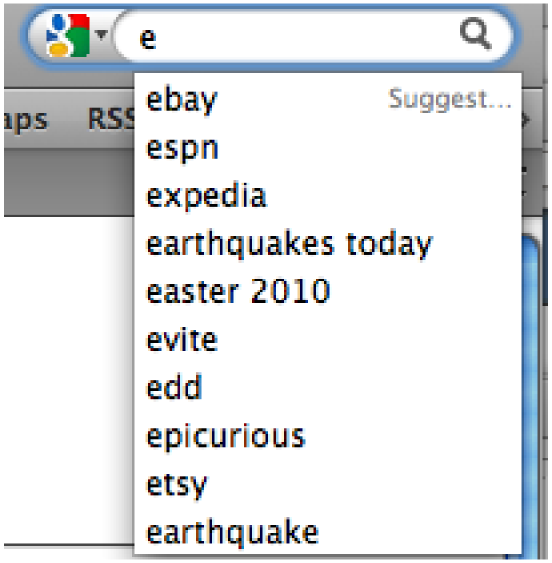
136 chars.



d

dictionary Suggest…
dmv california
delta airlines
disneyland
dominos
disney channel
de young museum
doppelganger
daylight savings time…
direct tv

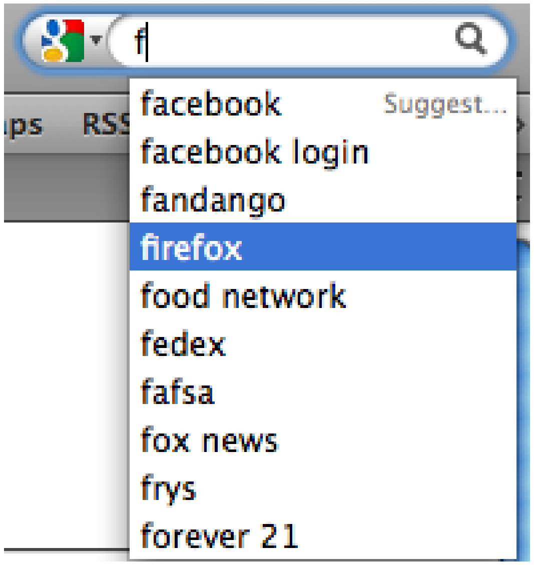
101 chars.



e

ebay Suggest…
espn
expedia
earthquakes today
easter 2010
evite
edd
epicurious
etsy
earthquake

102 chars.



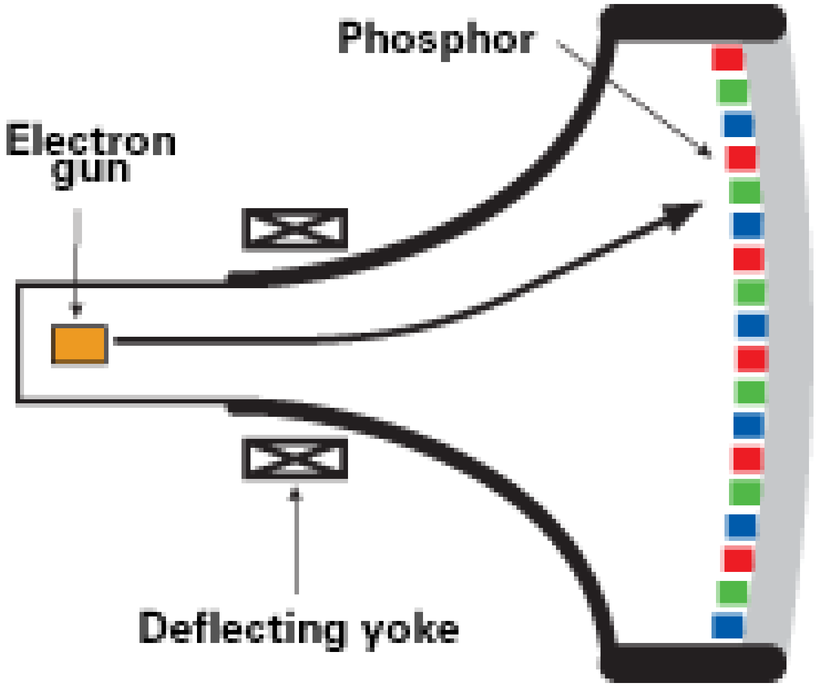
f

facebook Suggest…
facebook login
fandango
firefox
food network
fedex
fafsa
fox news
frys
forever 21

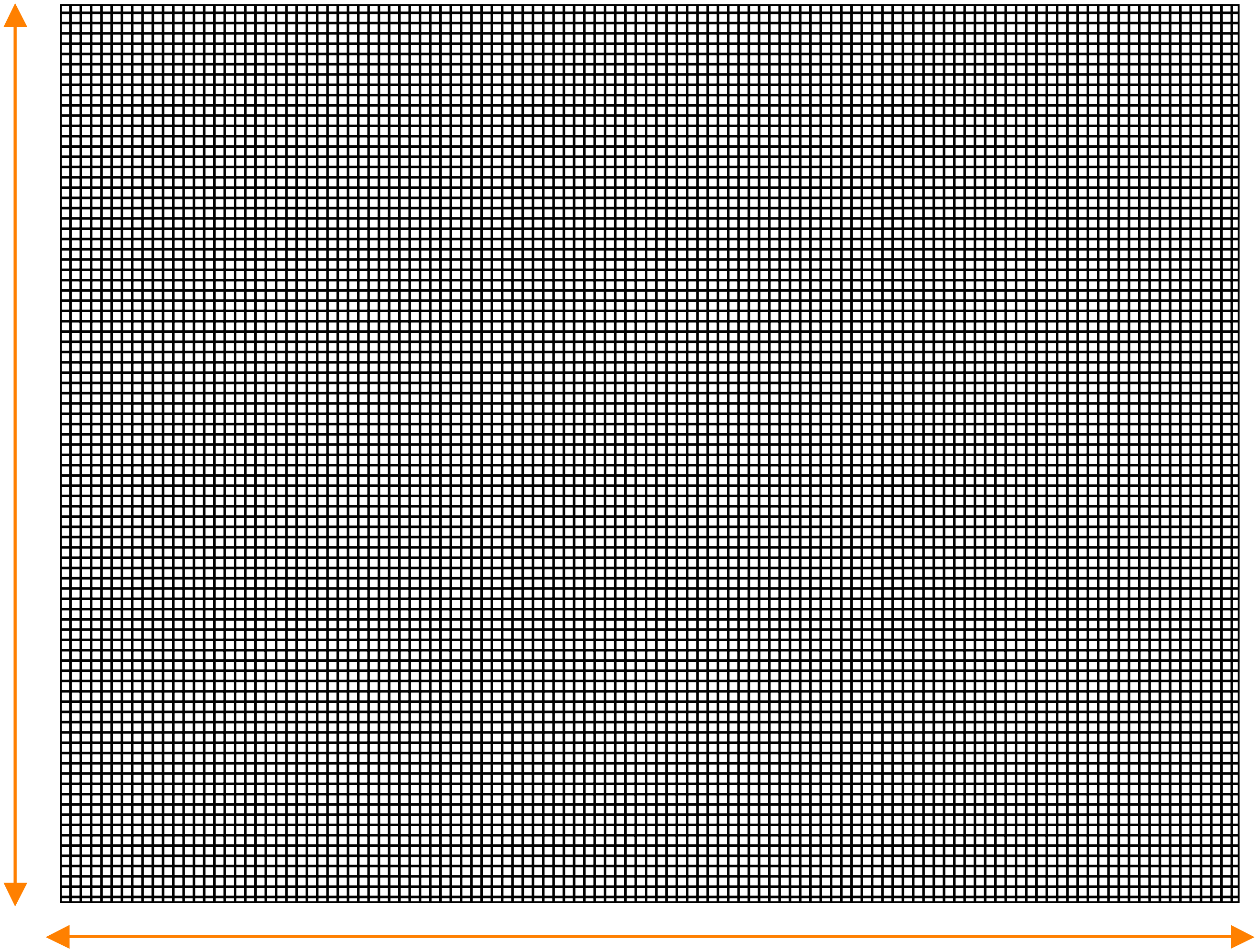
FOM Fiber Optic Modem
DCB
PWR TxD RxD
EM1
DET1
EM2
DET2

LED Indicator	Class I	Class II	Class III
Modems and Modem-Like Devices			
ANP Model 100 short-haul modem, TD indicator			●
ANP SDLC card, TD indicator			●
CASE/Datatel DCP3080 CSU/DSU, TD indicator			●
Hayes Smartmodem OPTIMA 14400, SD indicator			●
Hayes Smartmodem OPTIMA 9600, SD indicator			●
Motorola Codex 6740 Hex TP card, TD indicator			●
Motorola Codex 6740 TP Proc card, TD indicator			●
MultiTech MultiModem V32, TD indicator			●
Practical Peripherals PM14400FXMT fax modem, TX and RX indicators		●	
SimpLAN IS433-S printer sharing device, front panel LEDs			●
Telemet SDR-1000 Satellite Data Receiver, Data indicator			●
V.32bis modem simulator, TD indicator			●
WAN Devices			
Cisco 4000 IP router, Fast Serial TD indicator			●
Cisco 4000 IP router, front panel LED		●	
Cisco 7000 IP router, Fast Serial TD indicator			●
Cisco 7000 IP router, front panel LED		●	
Stratacom IPX SDP5080A, RXD indicator		●	
Verilink FT1 DSU/CSU, Pulses indicator		●	
Westel 3110-30 DS1 Connector, Pulses indicator		●	

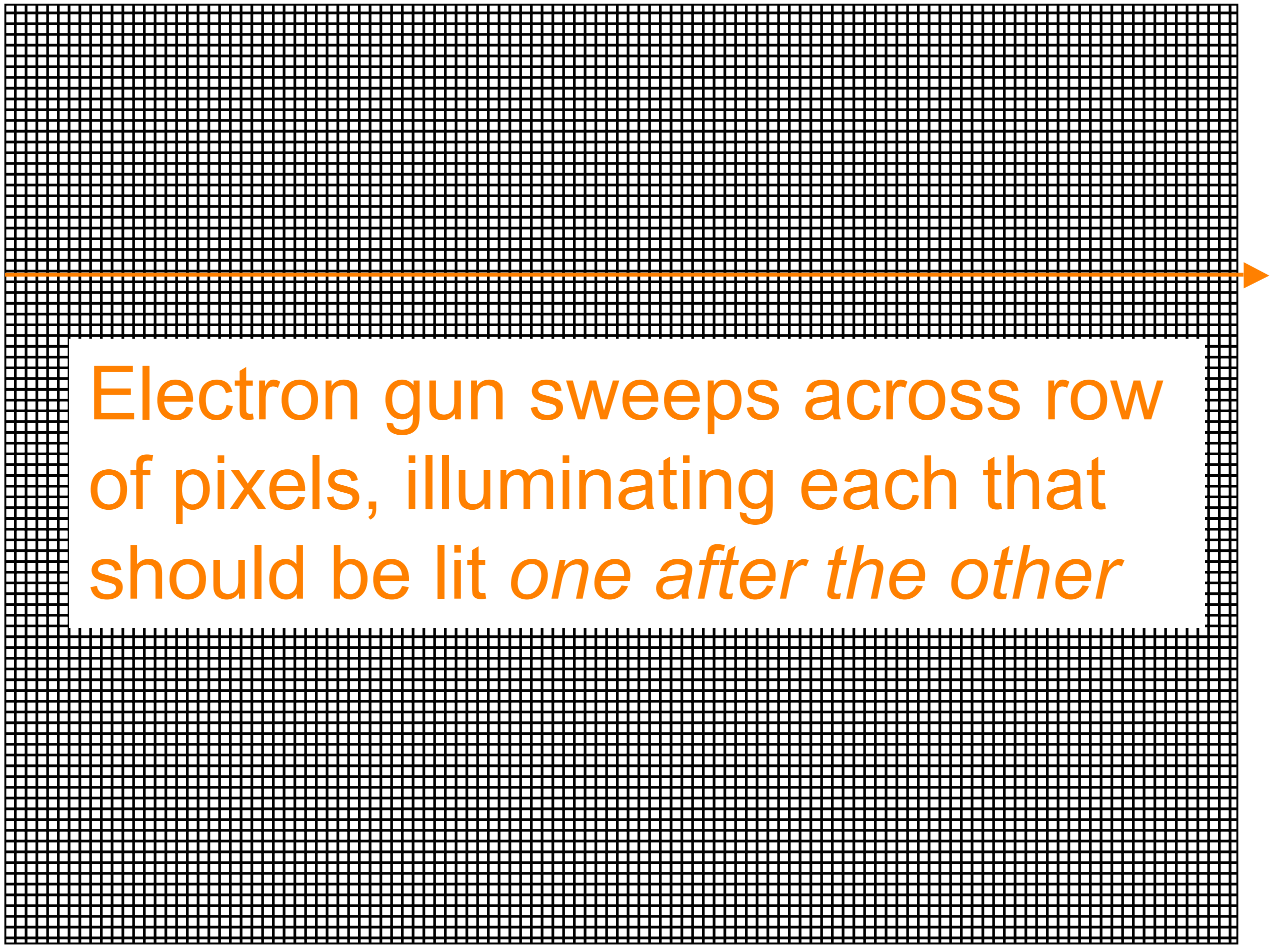
CRT



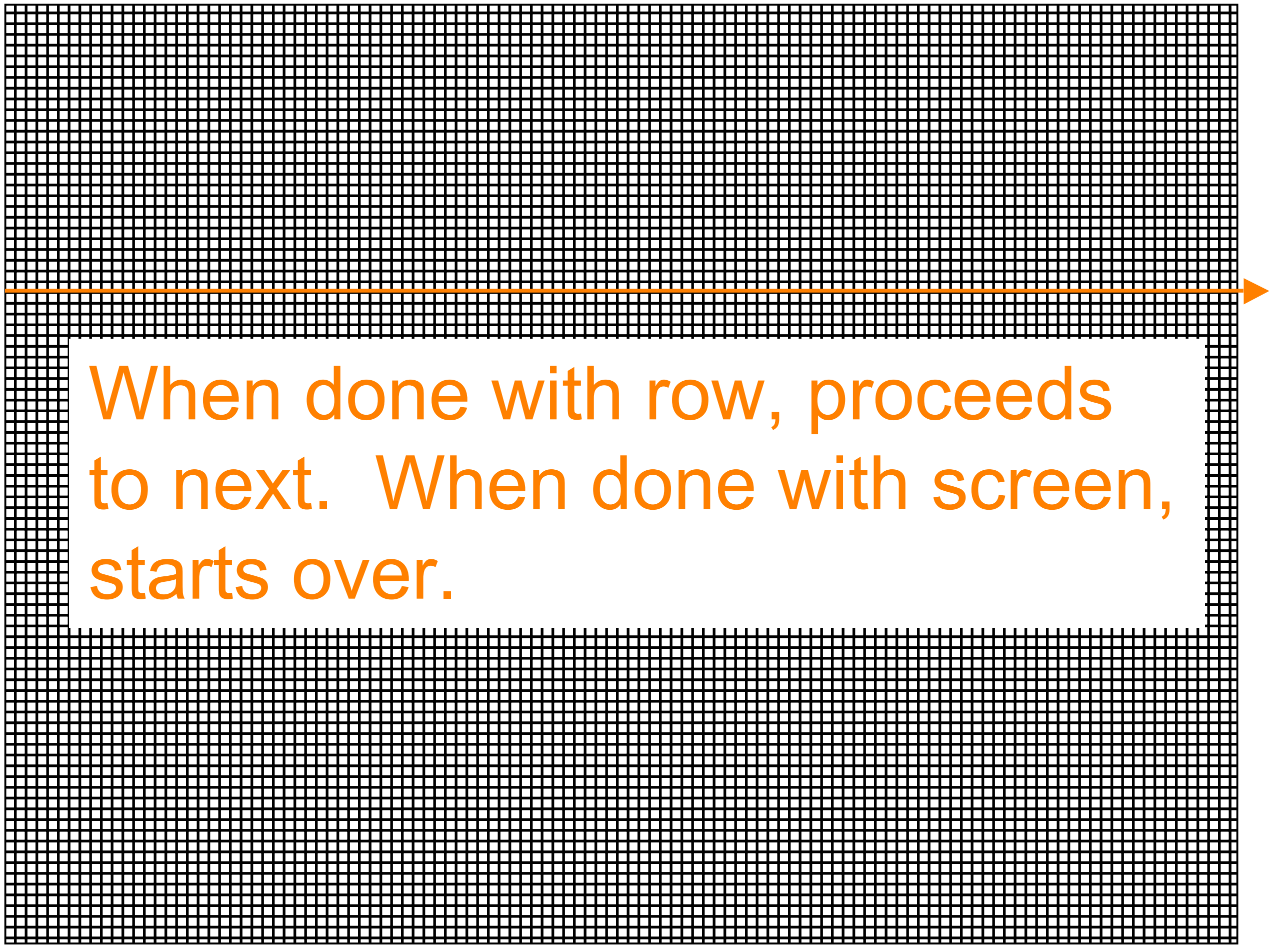
CRT display is made up of
an array of phosphor pixels



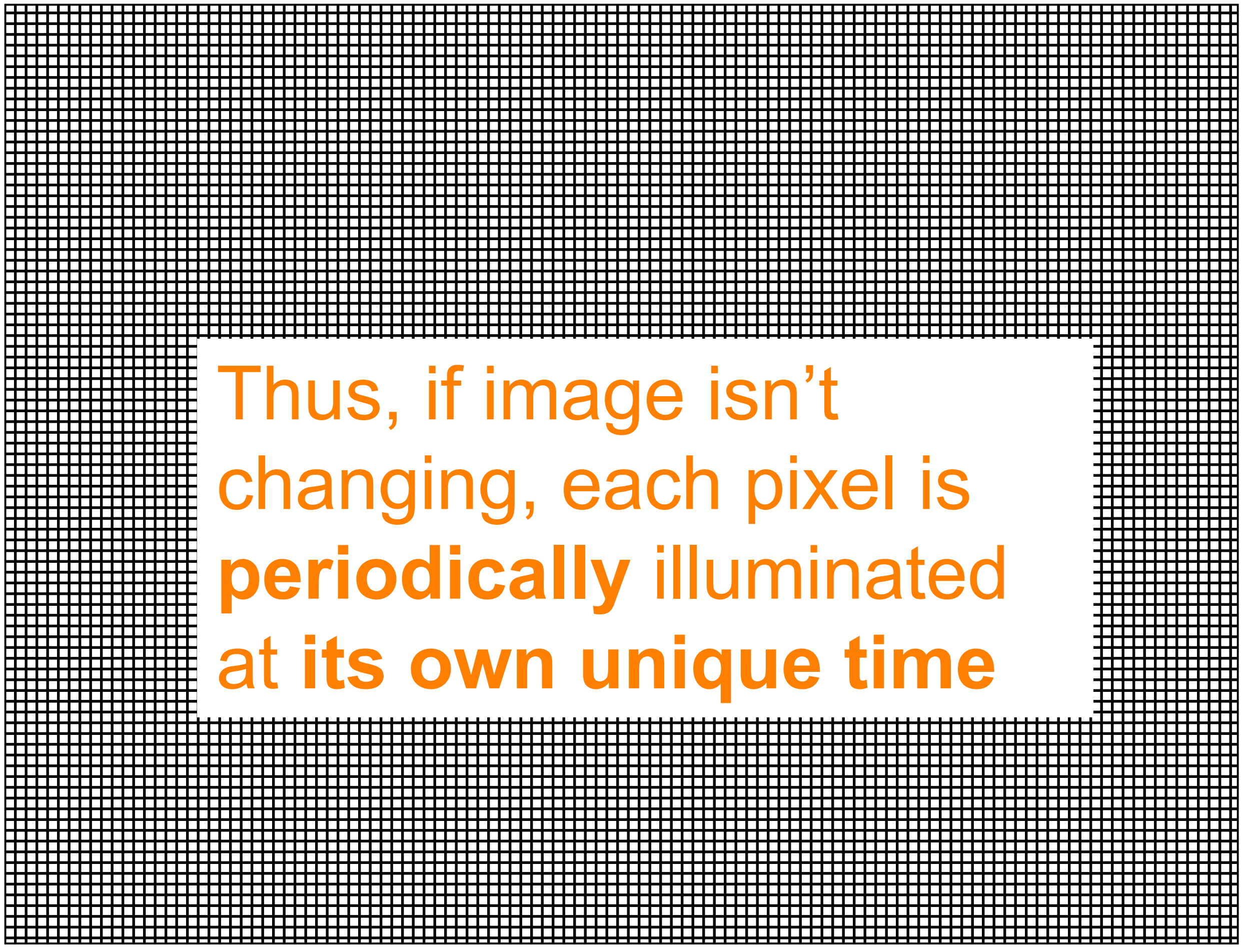
640x480 (say)



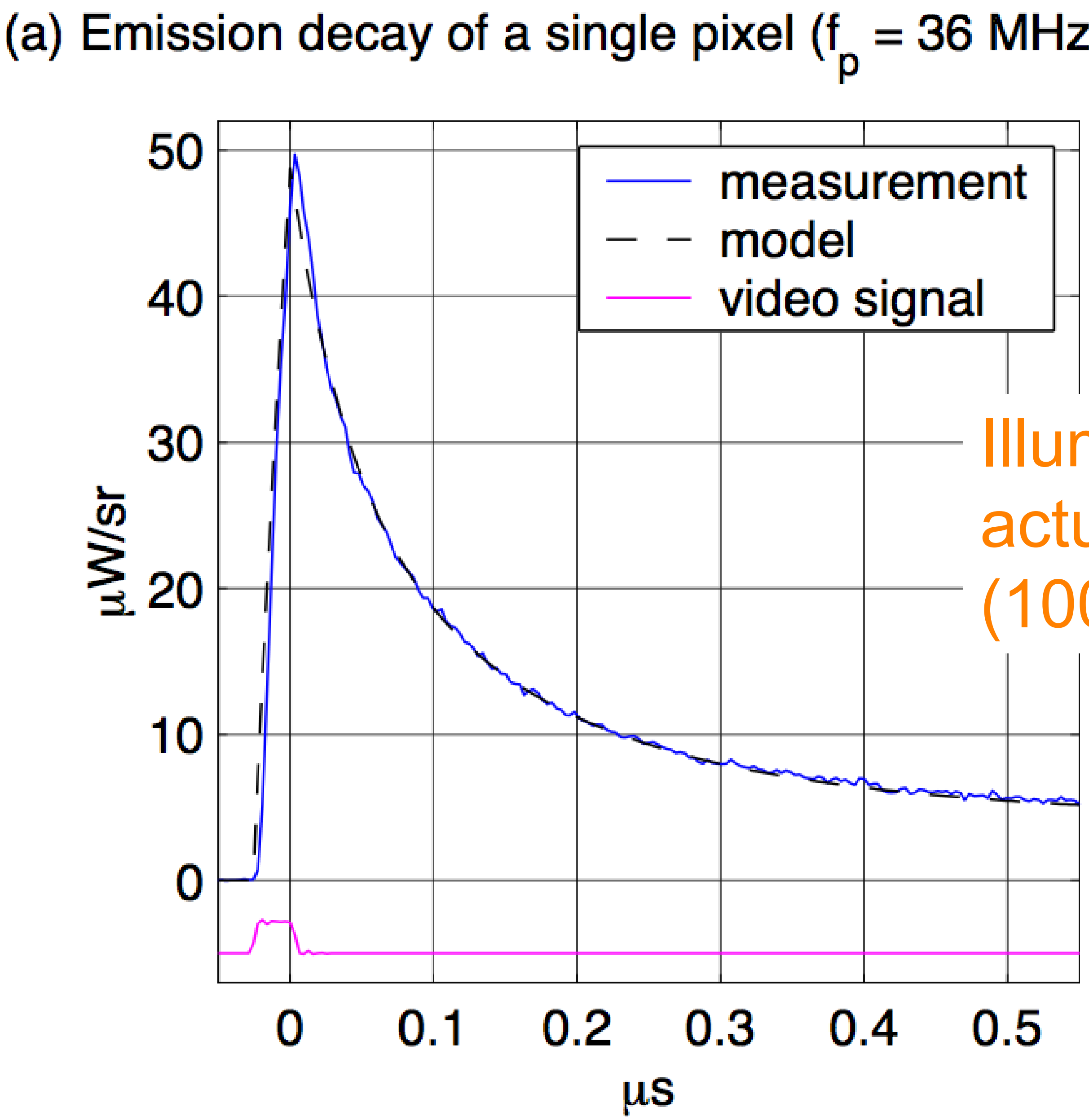
Electron gun sweeps across row of pixels, illuminating each that should be lit *one after the other*



When done with row, proceeds to next. When done with screen, starts over.

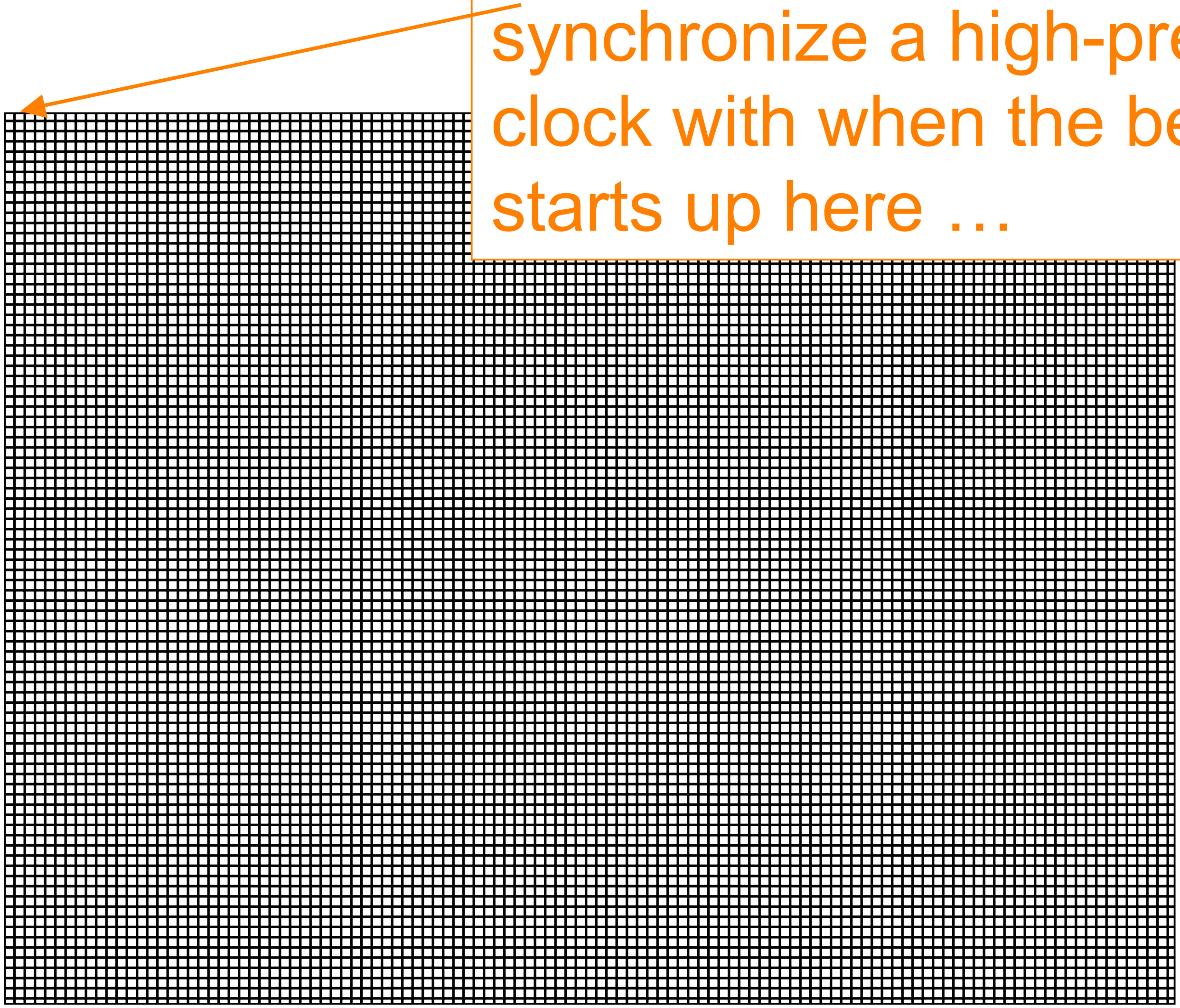


Thus, if image isn't changing, each pixel is **periodically** illuminated at **its own unique time**

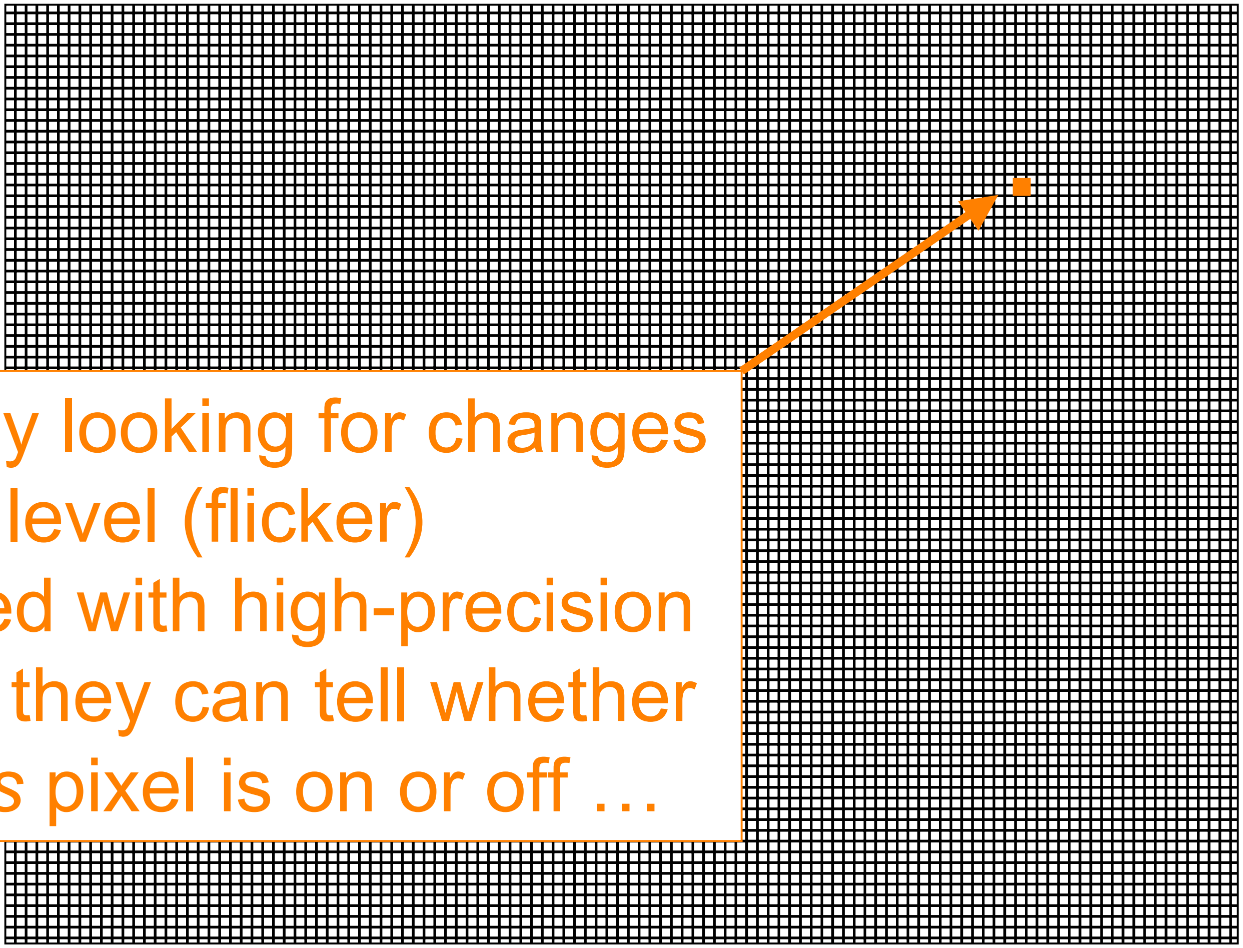


(a) Emission decay of a single pixel (f_p = 36 MHz)

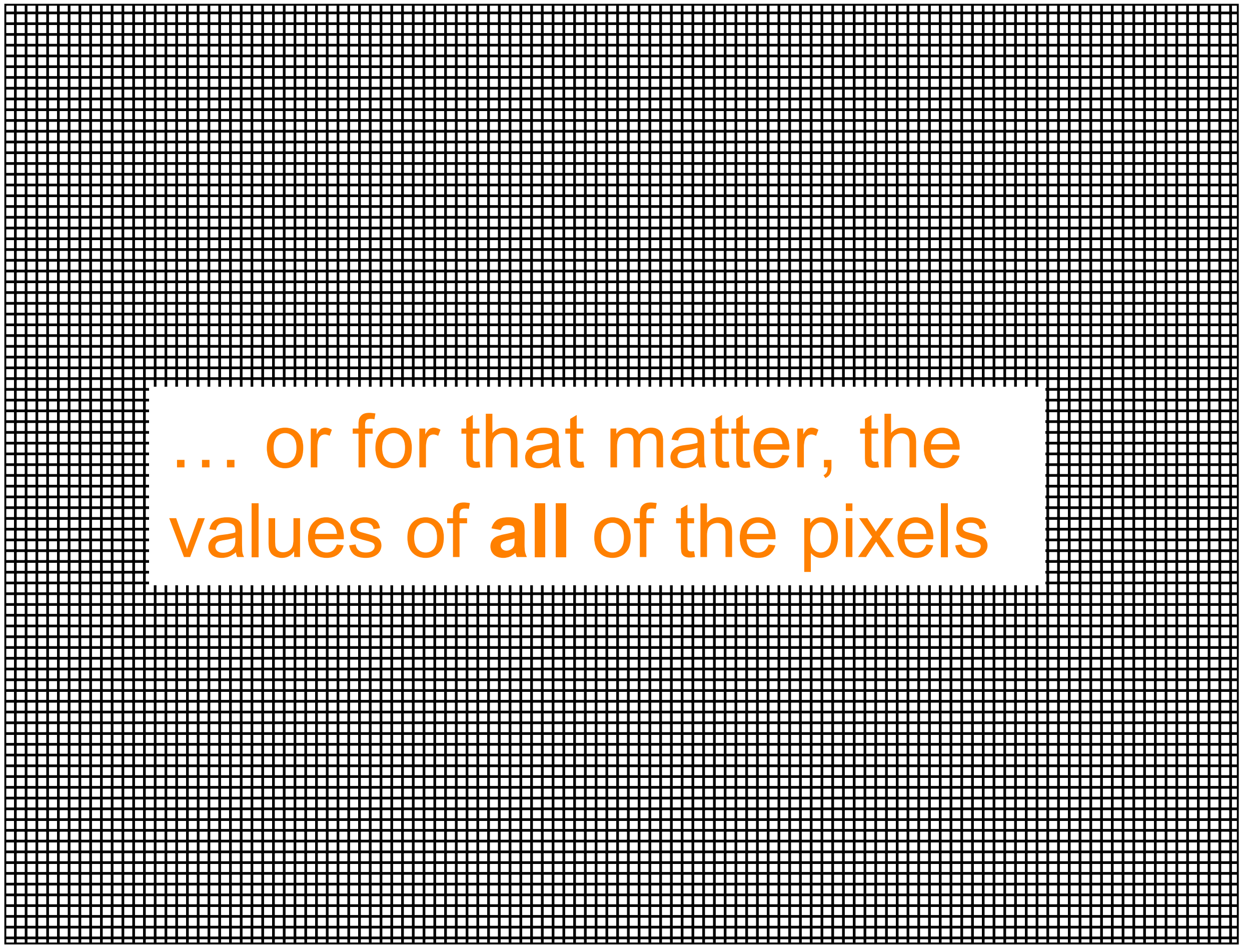
Illumination is actually short-lived (100s of nsec).



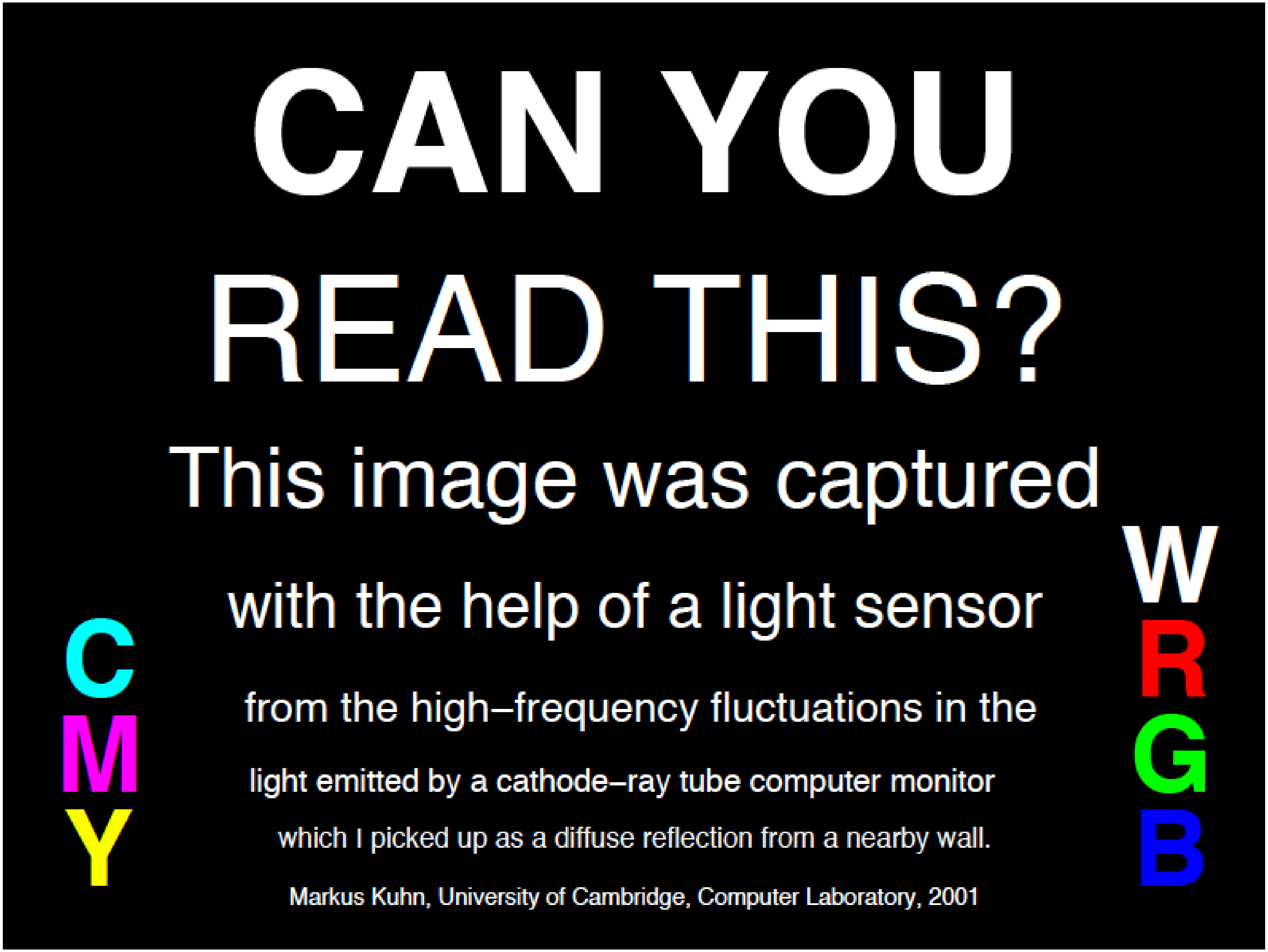
So if eavesdropper can synchronize a high-precision clock with when the beam starts up here …



Then by looking for changes in light level (flicker) matched with high-precision timing, they can tell whether say *this* pixel is on or off …



… or for that matter, the values of **all** of the pixels



CAN YOU

READ THIS?

This image was captured

with the help of a light sensor

from the high–frequency fluctuations in the

light emitted by a cathode–ray tube computer monitor

which I picked up as a diffuse reflection from a nearby wall.

Markus Kuhn, University of Cambridge, Computer Laboratory, 2001

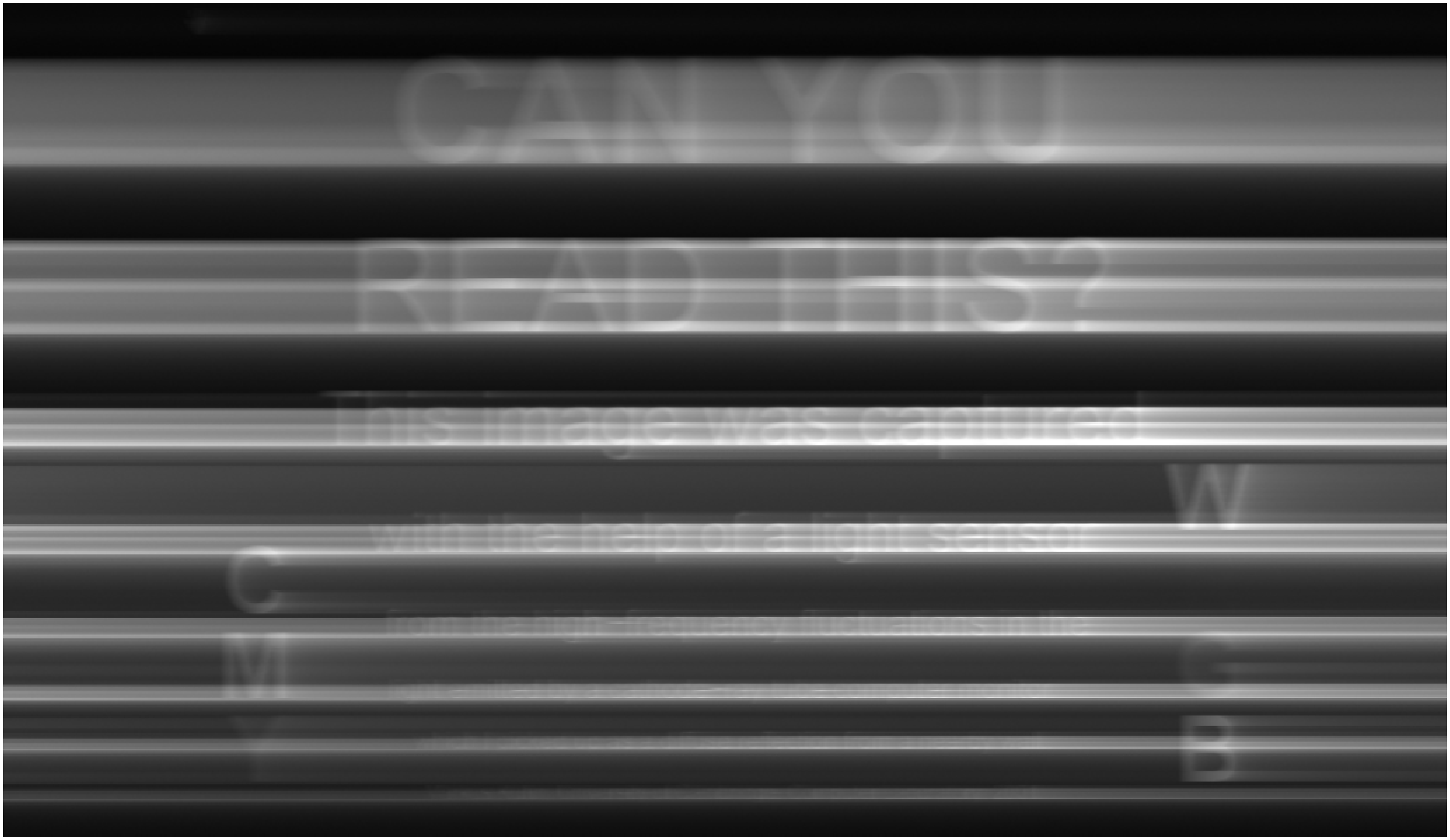
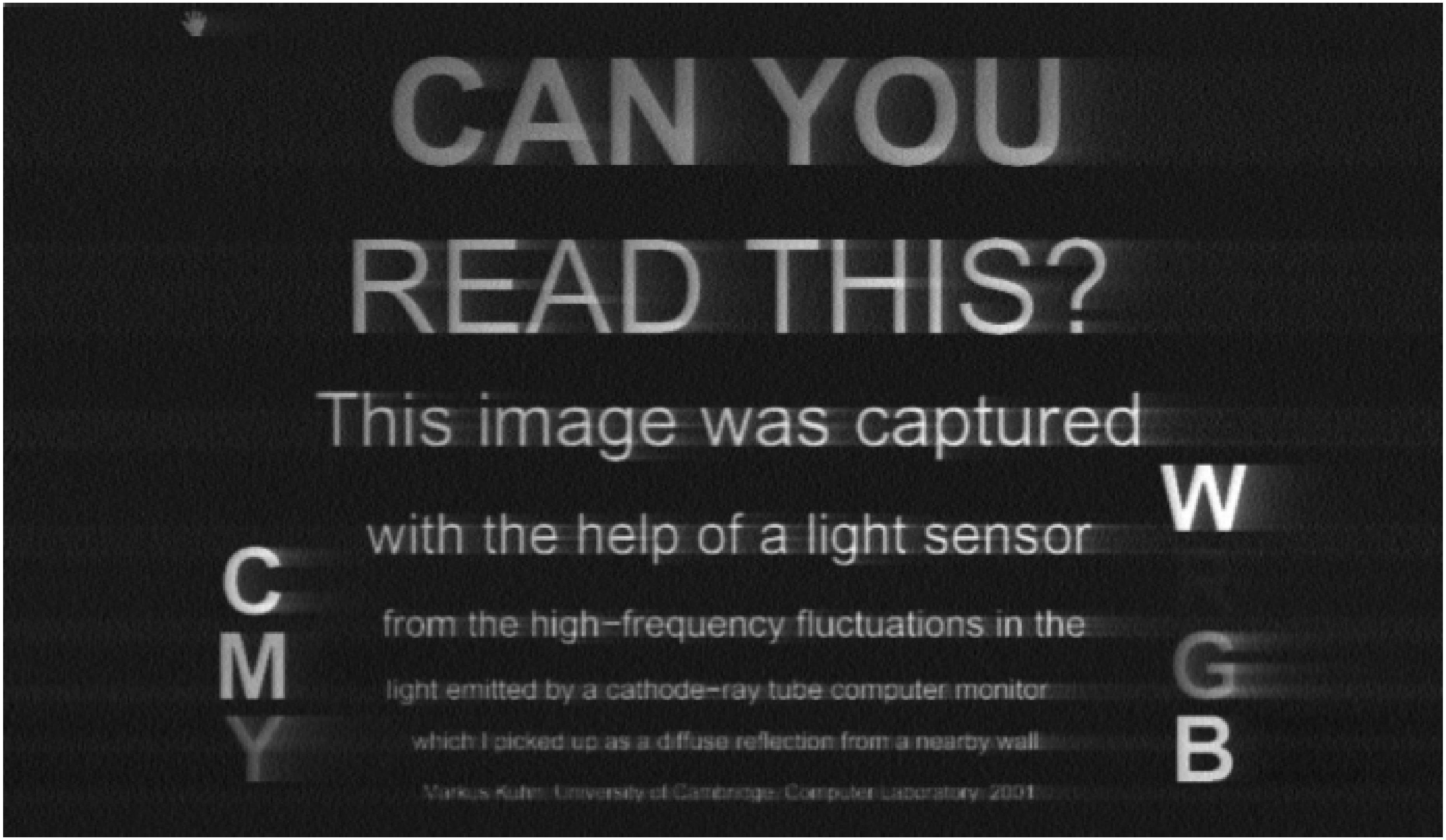

CAN YOU
READ THIS?
This image was captured
with the help of a light sensor
from the high-frequency fluctuations in the
C
M
Y
W
G
B

Figure 6.9: Unprocessed photomultiplier output after diffuse reflection from a wall



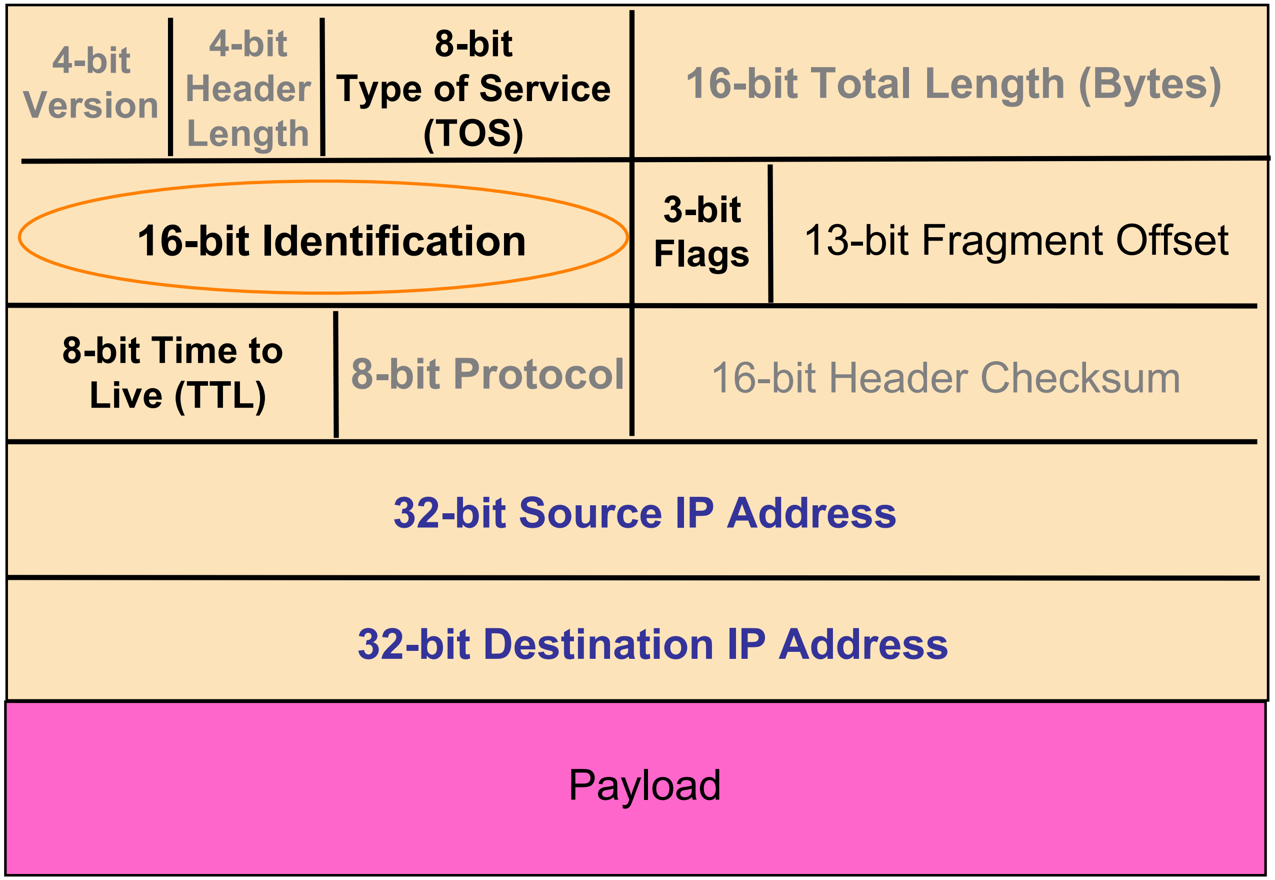
CAN YOU READ THIS?

This image was captured with the help of a light sensor from the high-frequency fluctuations in the light emitted by a cathode-ray tube computer monitor which I picked up as a diffuse reflection from a nearby wall

Markus Kuhn, University of Cambridge, Computer Laboratory, 2001

Photomultiplier + high-precision timing + deconvolution to remove noise

IP Header Side Channel



4-bit Version

4-bit Header Length

8-bit Type of Service (TOS)

16-bit Total Length (Bytes)

16-bit Identification

3-bit Flags

13-bit Fragment Offset

8-bit Time to Live (TTL)

8-bit Protocol

16-bit Header Checksum

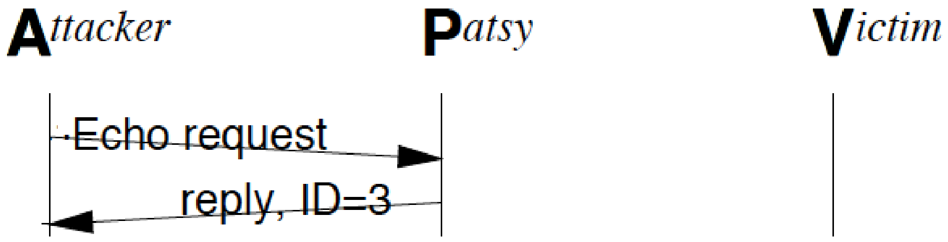
32-bit Source IP Address

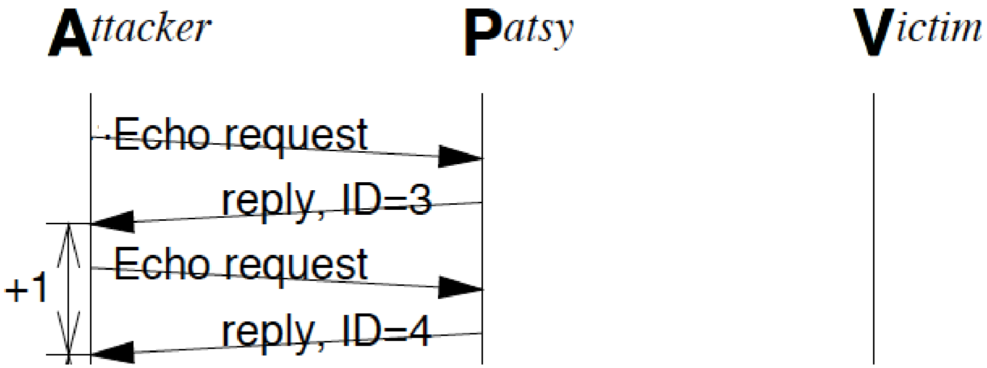
32-bit Destination IP Address

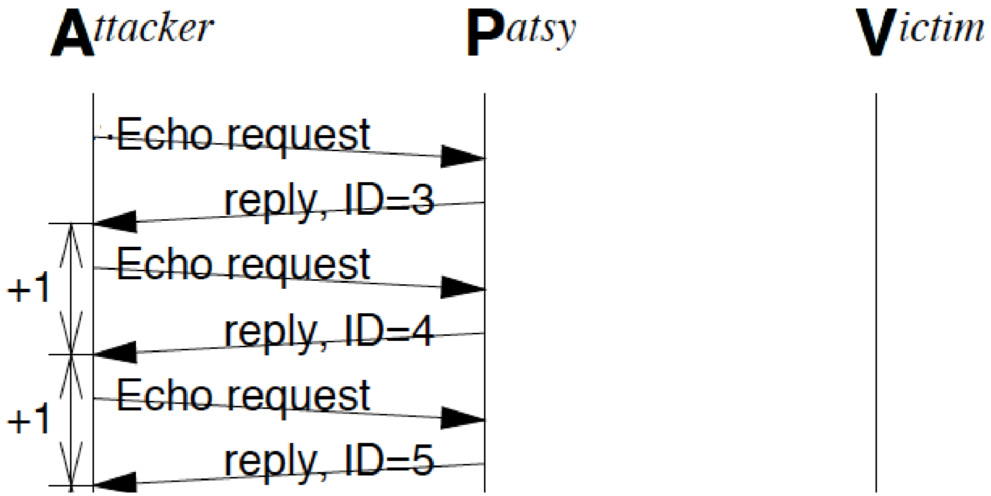
Payload

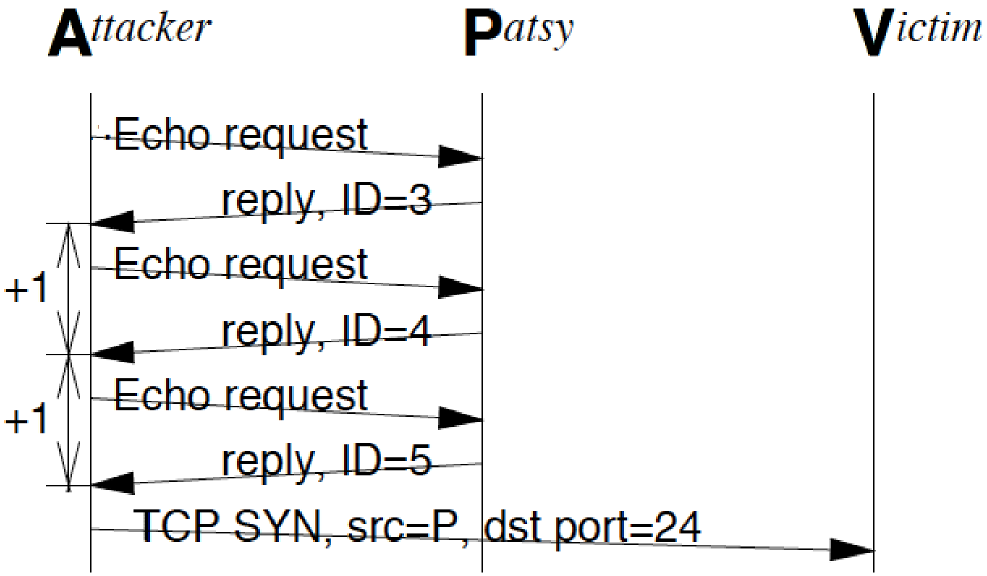
ID field is supposed to be unique per IP packet.

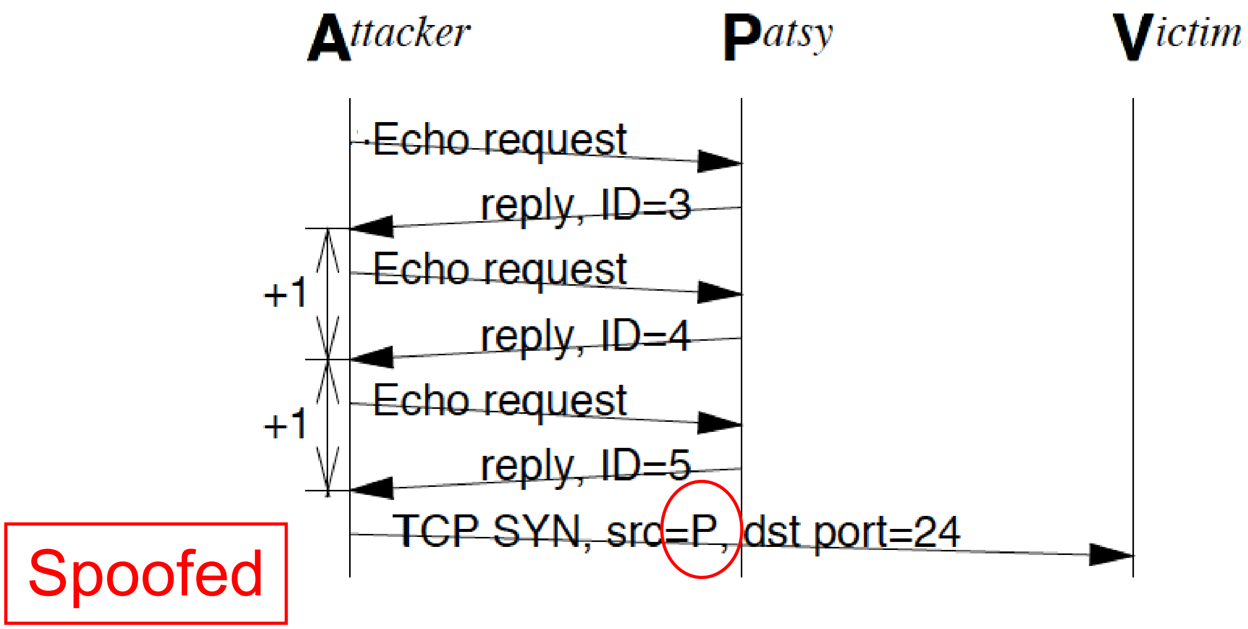
One easy way to do this: **increment** it each time system sends a new packet.

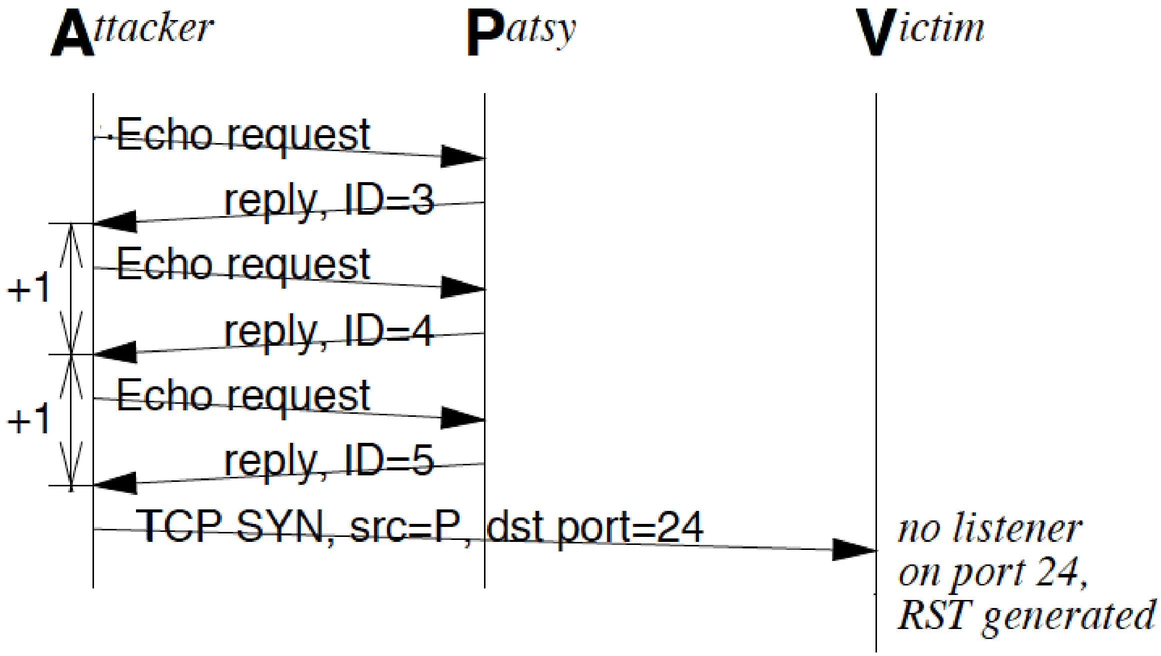

Attacker
Patsy
Victim
Echo request
reply, ID=3

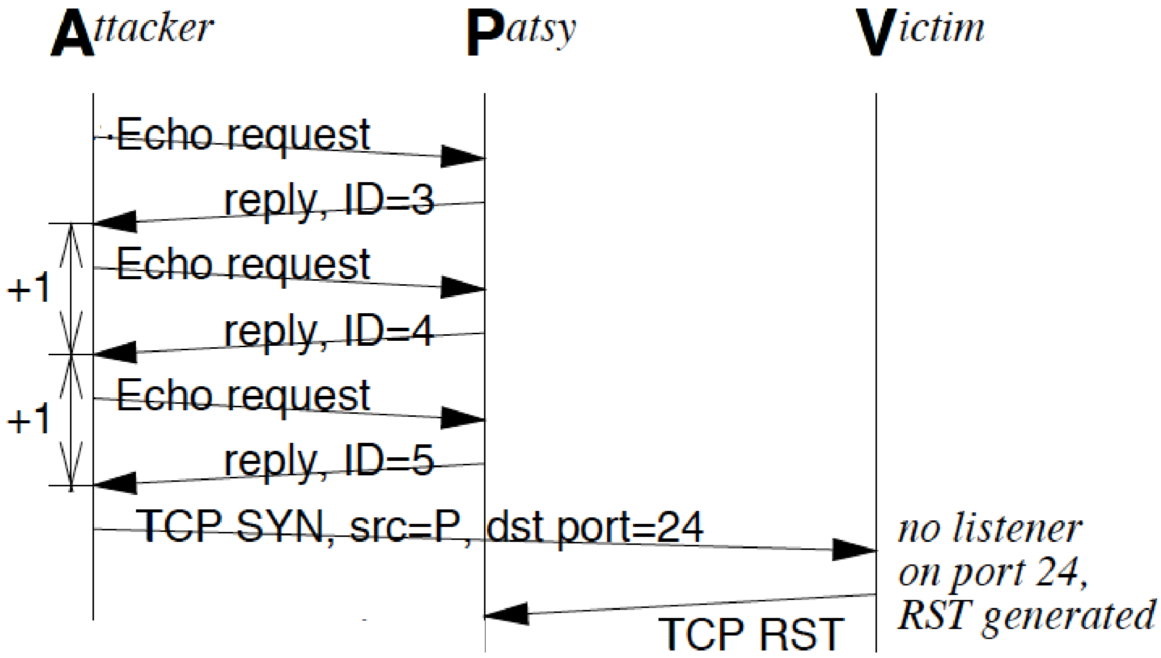

Attacker
Patsy
Victim
Echo request
reply, ID=3
+1
Echo request
reply, ID=4

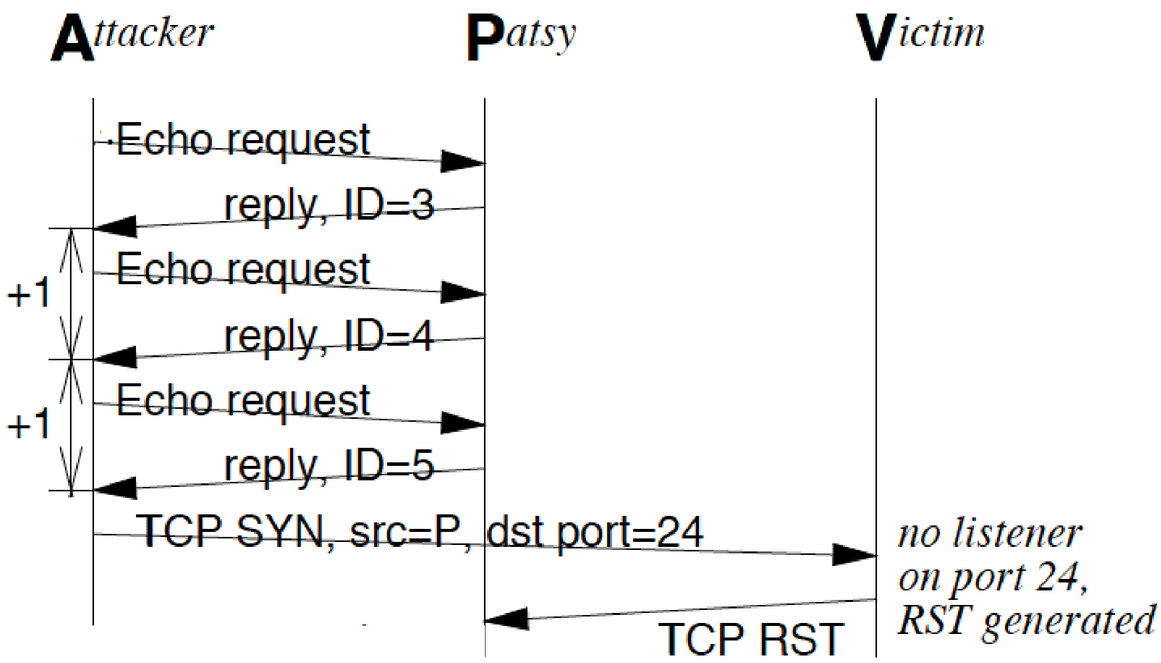

Attacker
Patsy
Victim
Echo request
reply, ID=3
+1
Echo request
reply, ID=4
+1
Echo request
reply, ID=5


Attacker
Patsy
Victim
Echo request
reply, ID=3
Echo request
+1
reply, ID=4
Echo request
+1
reply, ID=5
TCP SYN, src=P, dst port=24

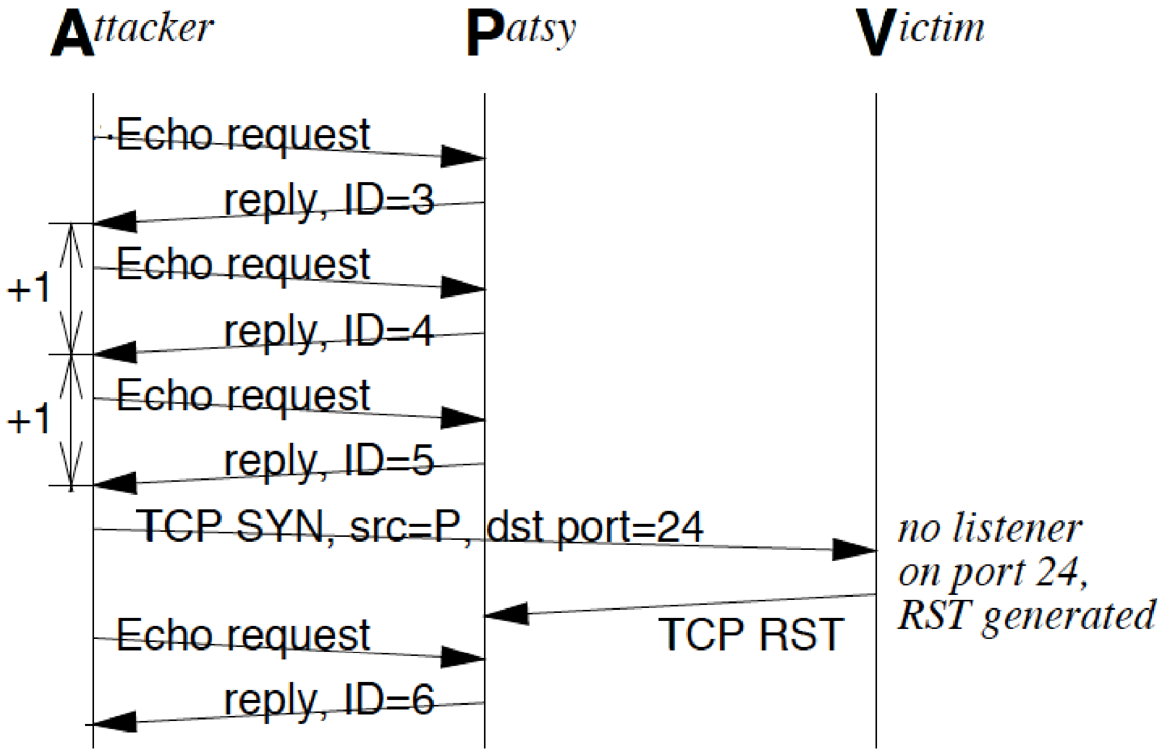

Attacker
Patsy
Victim
Echo request
reply, ID=3
+1
Echo request
reply, ID=4
+1
Echo request
reply, ID=5
TCP SYN, src=P, dst port=24
Spoofed

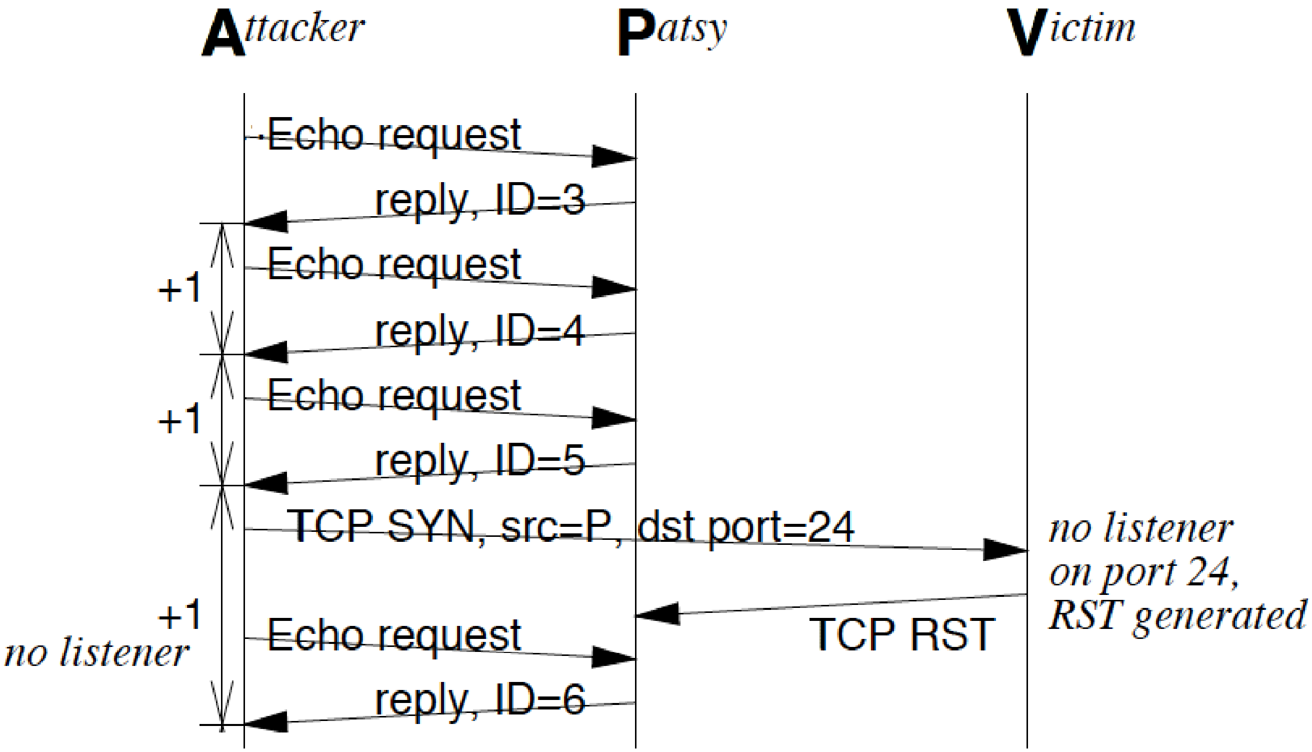

Attacker
Patsy
Victim
Echo request
reply, ID=3
+1
Echo request
reply, ID=4
+1
Echo request
reply, ID=5
TCP SYN, src=P, dst port=24
no listener
on port 24,
RST generated

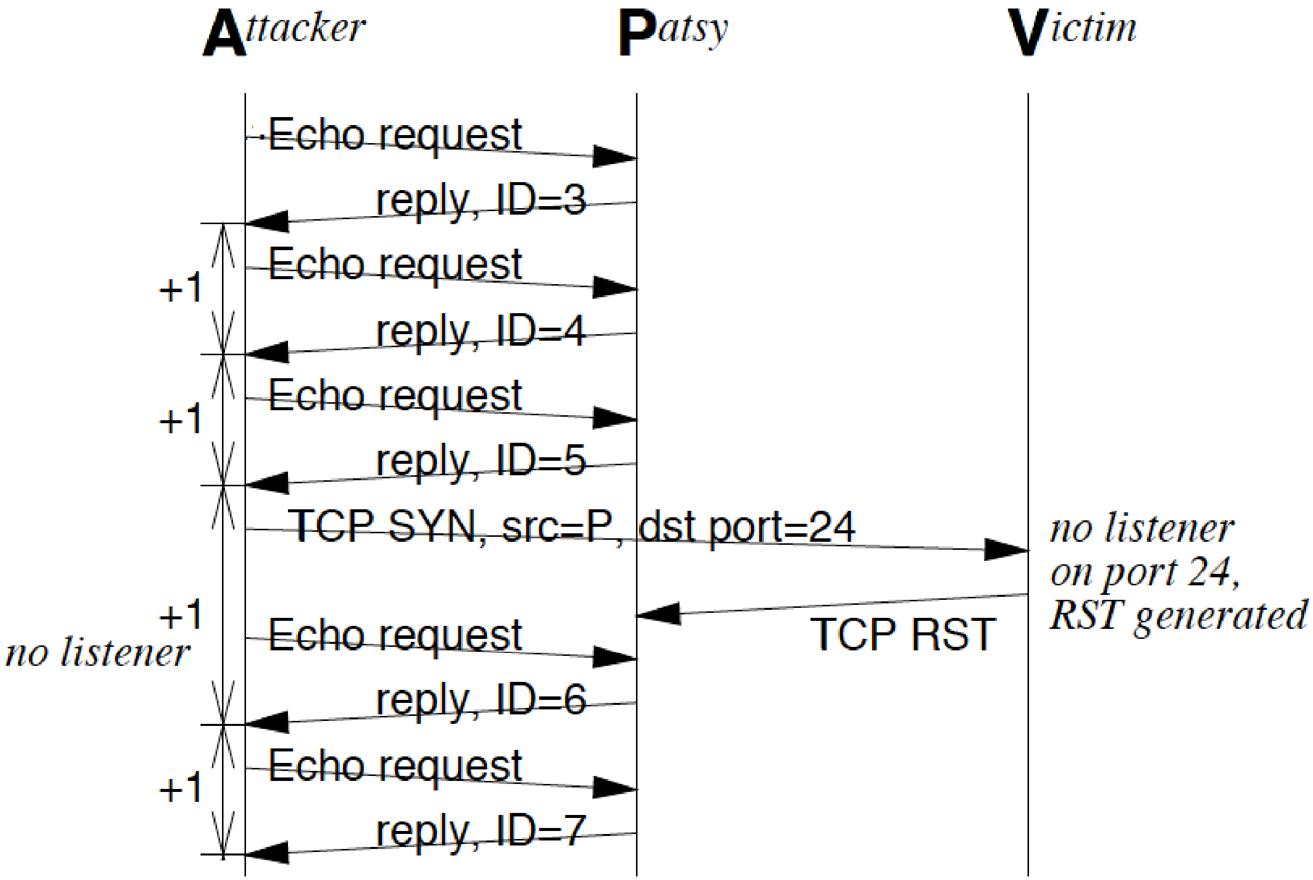

Attacker
Patsy
Victim
Echo request
reply, ID=3
+1
Echo request
reply, ID=4
+1
Echo request
reply, ID=5
TCP SYN, src=P, dst port=24
no listener
on port 24,
RST generated
TCP RST

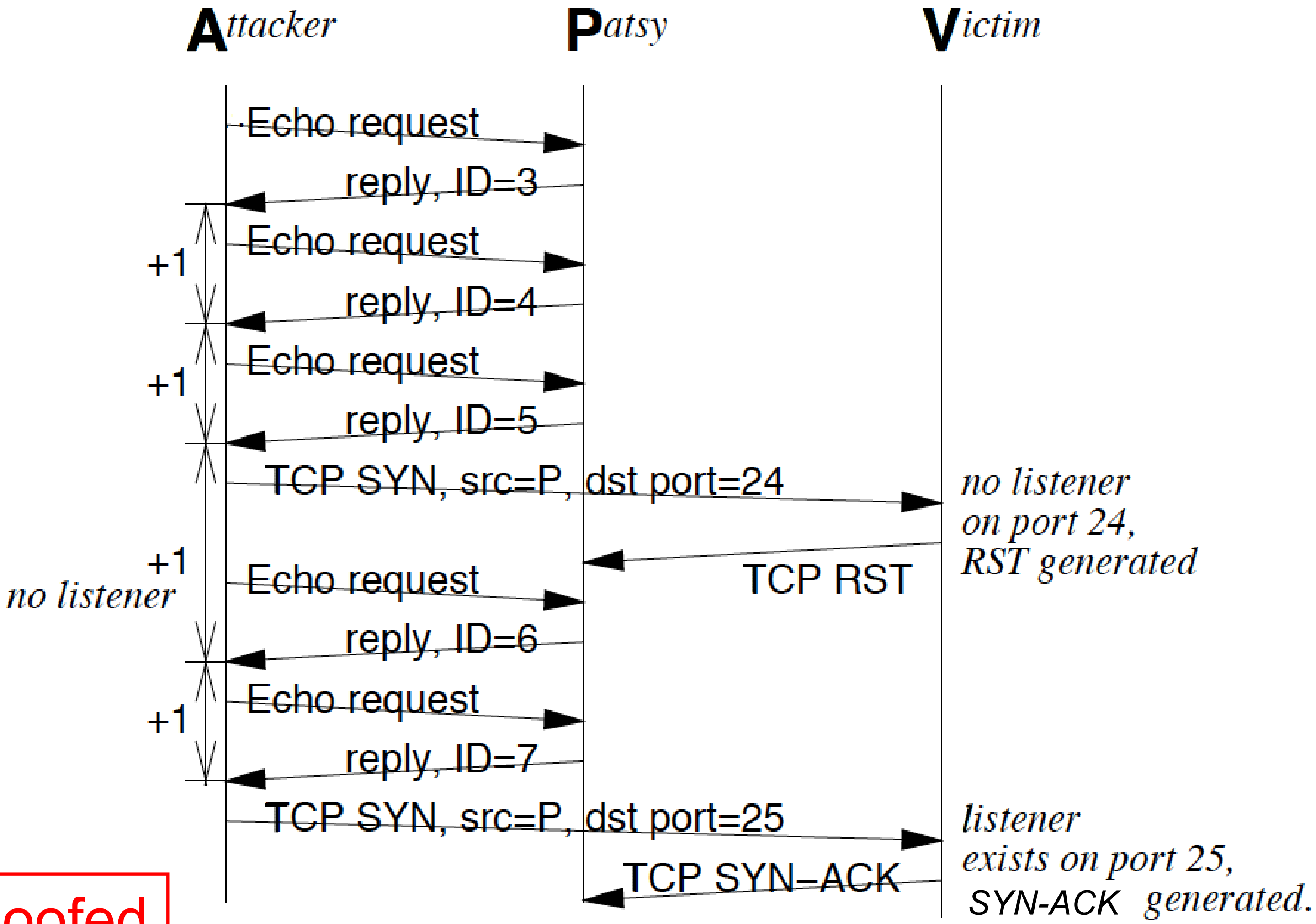


Upon receiving RST,
Patsy ignores it and does
nothing, per TCP spec.

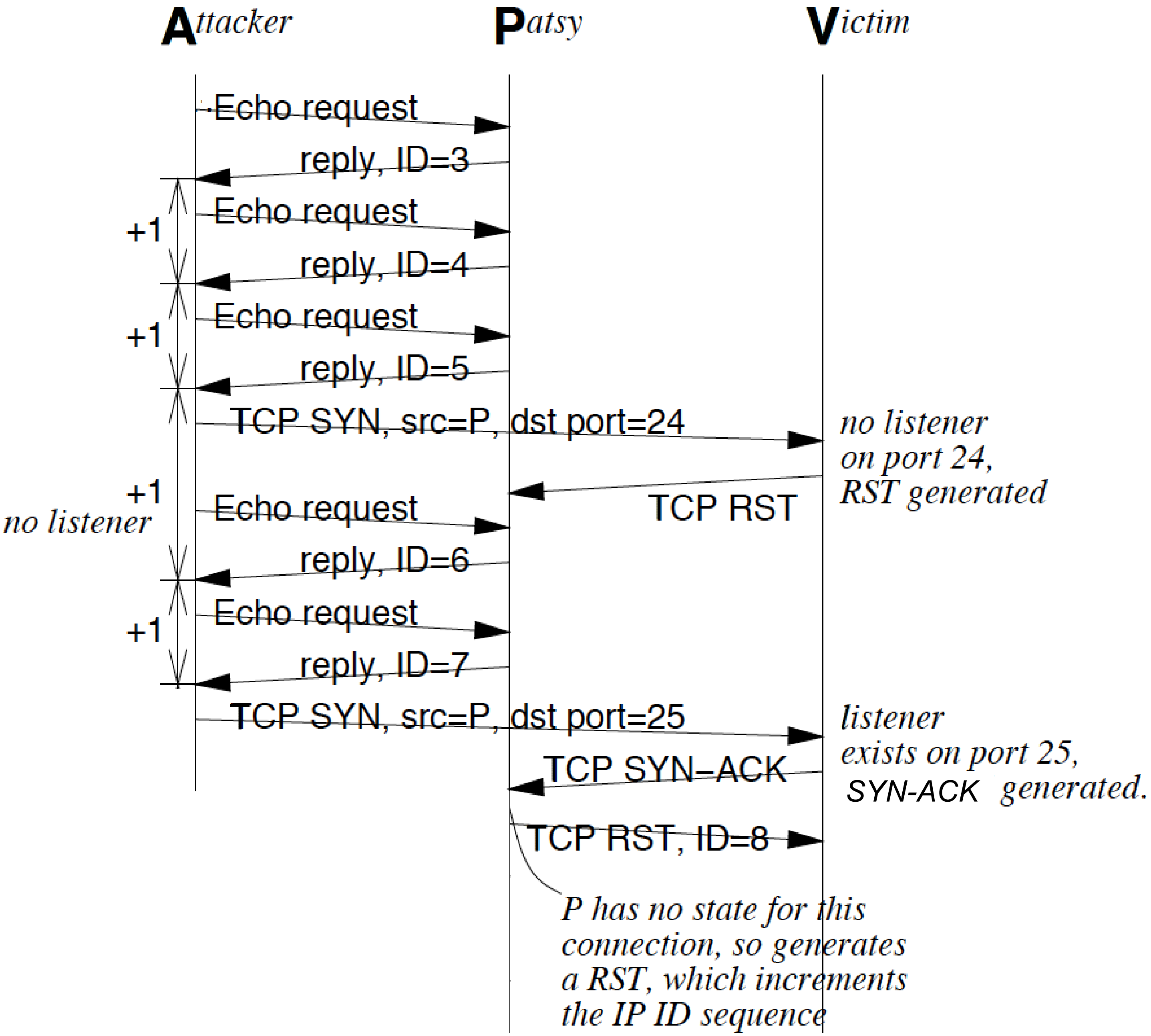

Attacker
Patsy
Victim
Echo request
reply, ID=3
+1
Echo request
reply, ID=4
+1
Echo request
reply, ID=5
TCP SYN, src=P, dst port=24
no listener
on port 24,
RST generated
TCP RST
Echo request
reply, ID=6

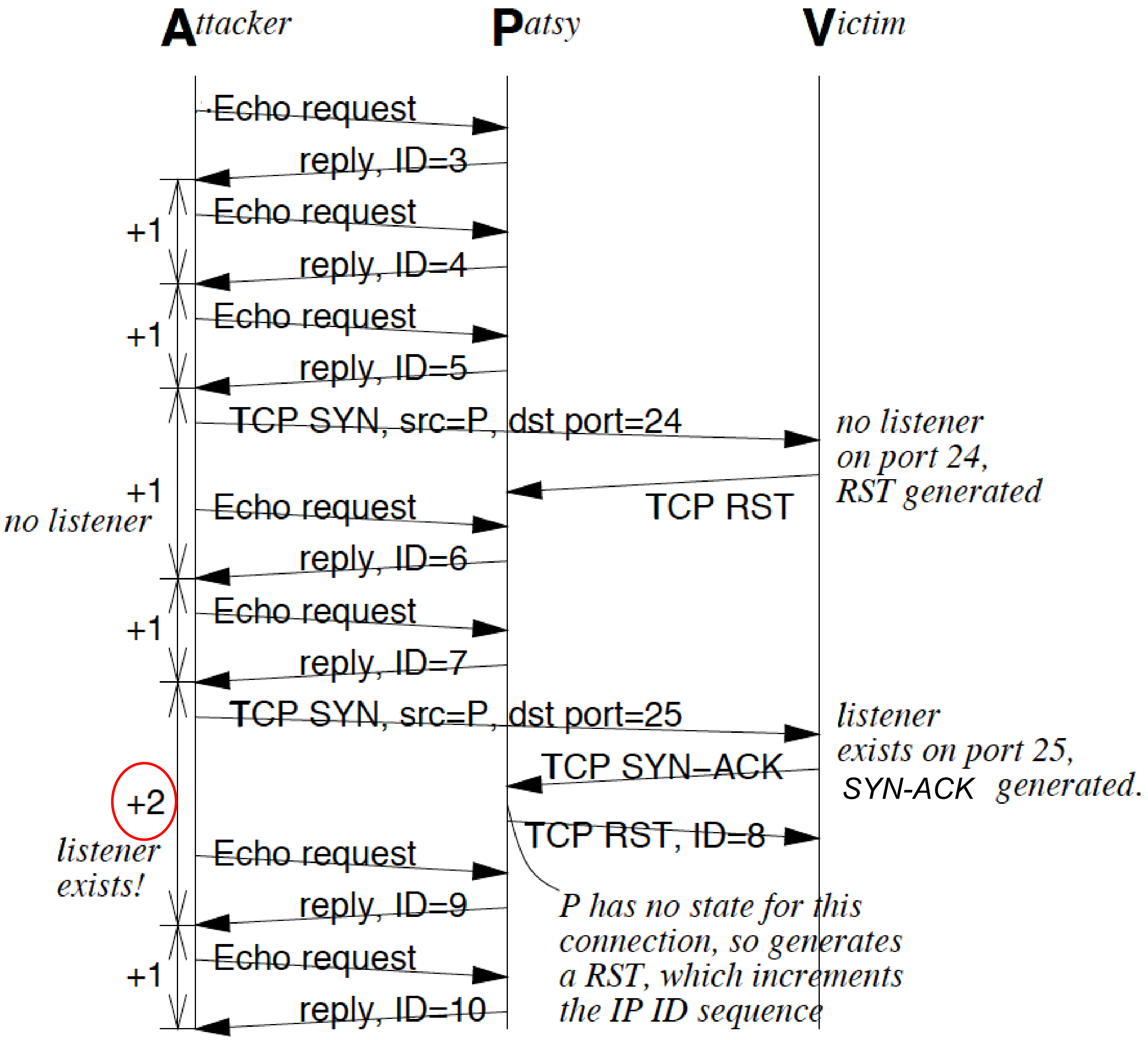

Attacker
Patsy
Victim
Echo request
reply, ID=3
+1
Echo request
reply, ID=4
+1
Echo request
reply, ID=5
TCP SYN, src=P, dst port=24
no listener
on port 24,
RST generated
TCP RST
+1
no listener
Echo request
reply, ID=6

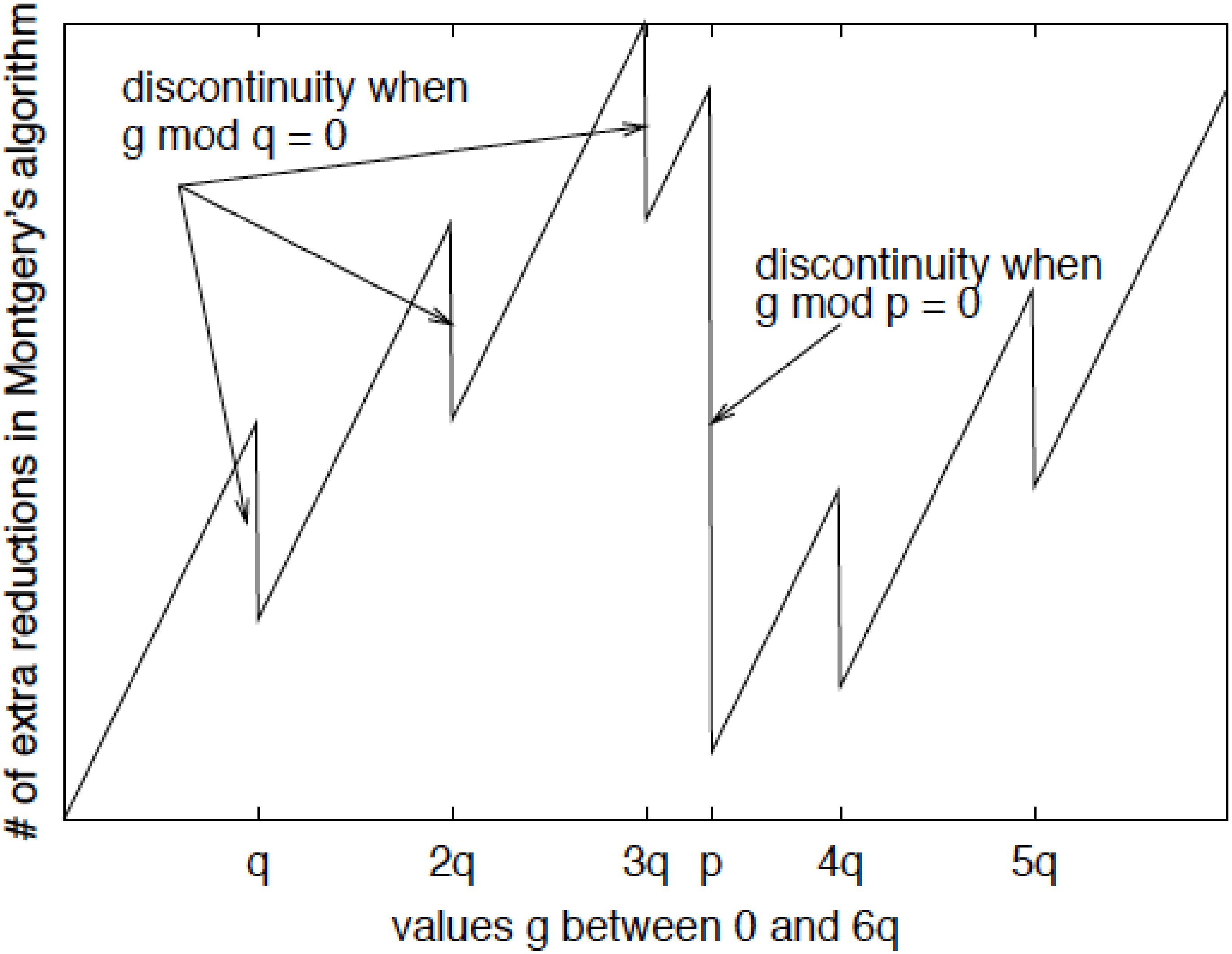

Attacker
Patsy
Victim
Echo request
reply, ID=3
+1
Echo request
reply, ID=4
+1
Echo request
reply, ID=5
TCP SYN, src=P, dst port=24
no listener
on port 24,
RST generated
+1
no listener
Echo request
TCP RST
reply, ID=6
+1
Echo request
reply, ID=7


Attacker
Patsy
Victim
Echo request
reply, ID=3
+1
Echo request
reply, ID=4
+1
Echo request
reply, ID=5
TCP SYN, src=P, dst port=24
no listener
on port 24,
RST generated
TCP RST
+1
no listener
Echo request
reply, ID=6
+1
Echo request
reply, ID=7
TCP SYN, src=P, dst port=25
listener
exists on port 25,
SYN-ACK generated.
TCP SYN–ACK

Spoofed


Attacker
Patsy
Victim
Echo request
reply, ID=3
Echo request
+1
reply, ID=4
Echo request
+1
reply, ID=5
TCP SYN, src=P, dst port=24
no listener
on port 24,
RST generated
TCP RST
+1
no listener
Echo request
reply, ID=6
Echo request
+1
reply, ID=7
TCP SYN, src=P, dst port=25
listener
exists on port 25,
SYN-ACK generated.
TCP SYN–ACK
TCP RST, ID=8
P has no state for this
connection, so generates
a RST, which increments
the IP ID sequence


Attacker
Patsy
Victim
Echo request
reply, ID=3
+1
Echo request
reply, ID=4
+1
Echo request
reply, ID=5
TCP SYN, src=P, dst port=24
no listener
on port 24,
RST generated
TCP RST
+1
no listener
Echo request
reply, ID=6
+1
Echo request
reply, ID=7
TCP SYN, src=P, dst port=25
listener
exists on port 25,
SYN-ACK generated.
TCP SYN–ACK
+2
listener
exists!
TCP RST, ID=8
Echo request
reply, ID=9
P has no state for this
connection, so generates
a RST, which increments
the IP ID sequence
+1
Echo request
reply, ID=10


discontinuity when
g mod q = 0
discontinuity when
g mod p = 0
# of extra reductions in Montgery's algorithm
q
2q
3q
p
4q
5q
values g between 0 and 6q