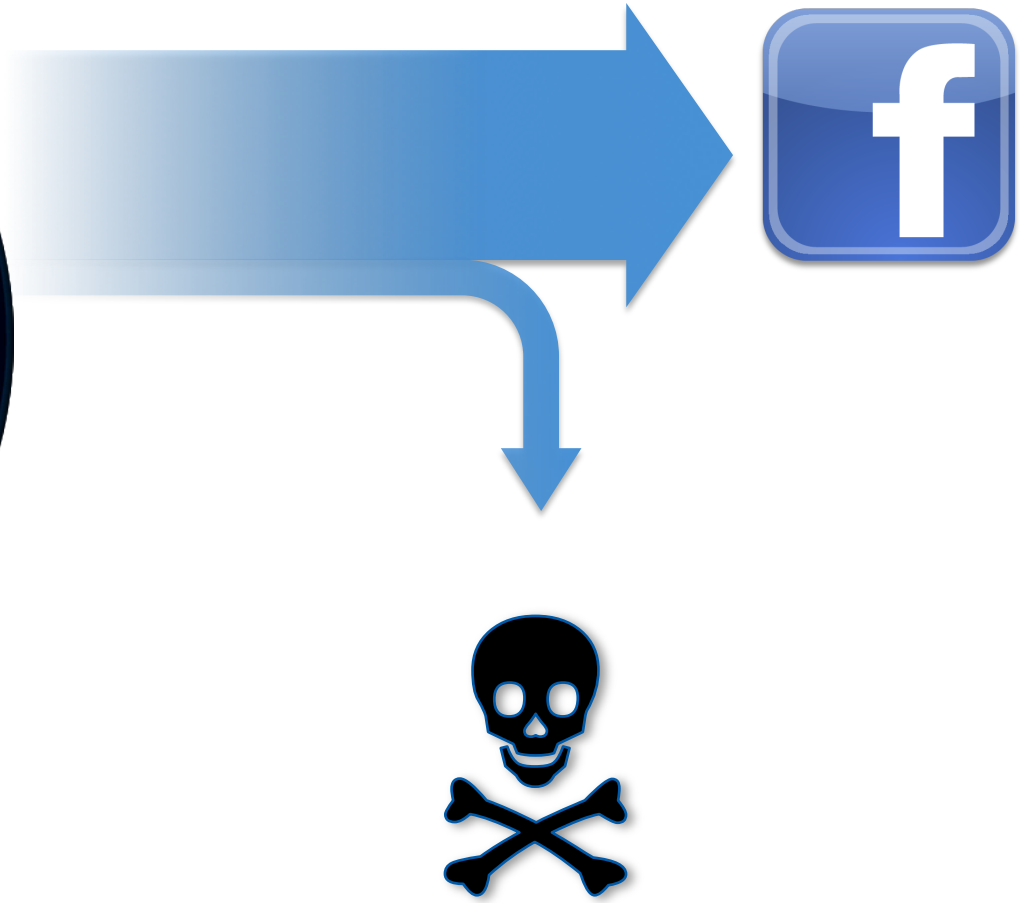
BITSQUATTING

DNS HIJACKING WITHOUT EXPLOITATION

ARTEM DINABURG
DEFCON 19

About Me

The Problem



Affected Platforms

PS3
PlayStation 3

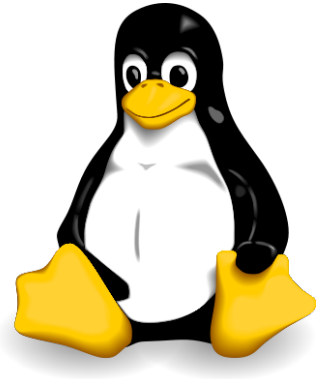
BlackBerry™

PSP
PlayStation®Portable

Microsoft®
Windows™

android

Windows phone



Wii™

symbian

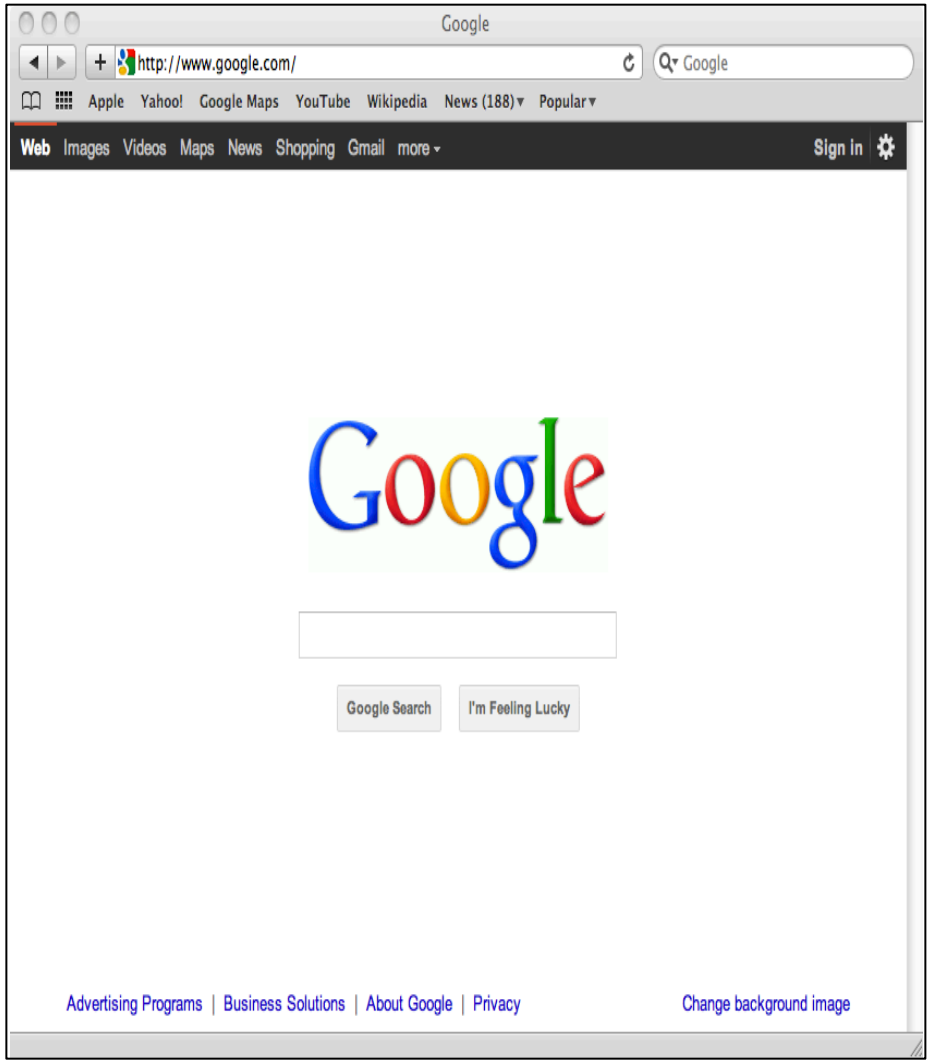

Low
Skill
brother
M
P 4
6 J 5
K E O 3
U ? D D S
K U L E T Y
2 2 I A C M 3

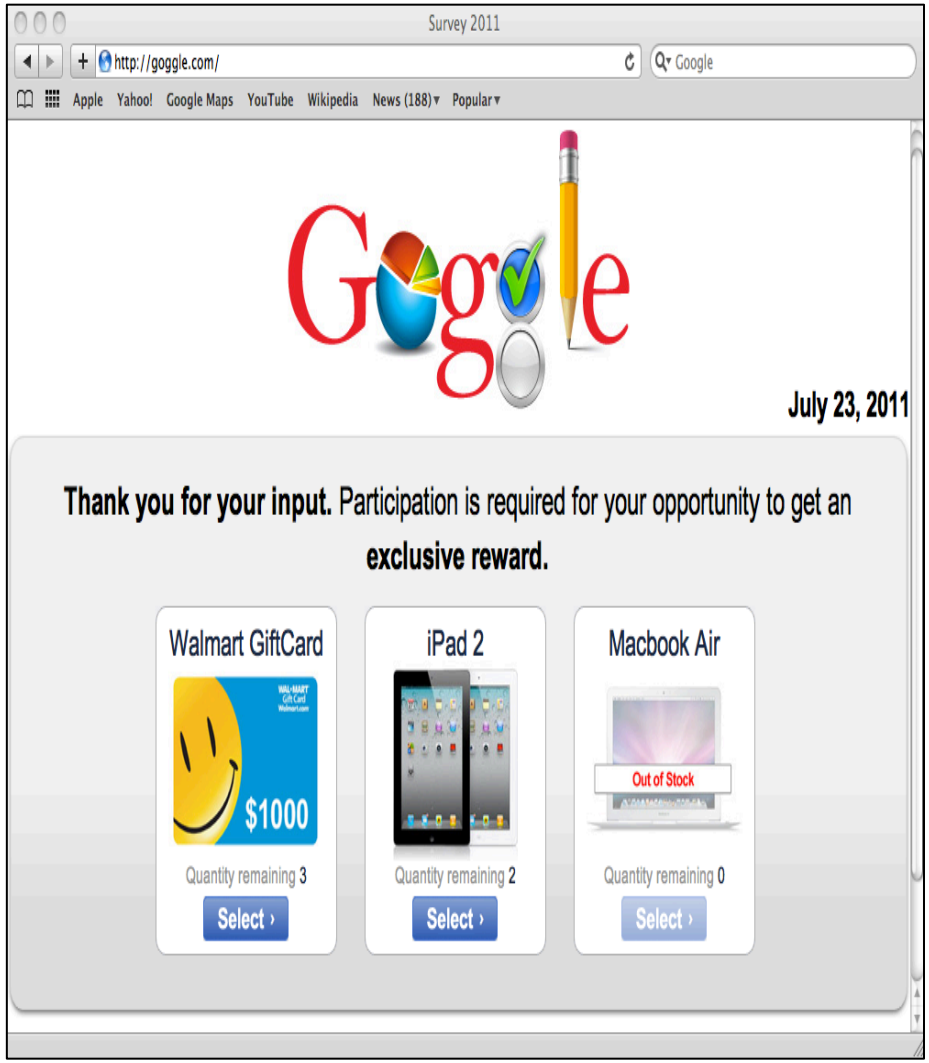

Cheap

Bitsquatting

Like typosquatting, but for bits

Typosquatting





There are

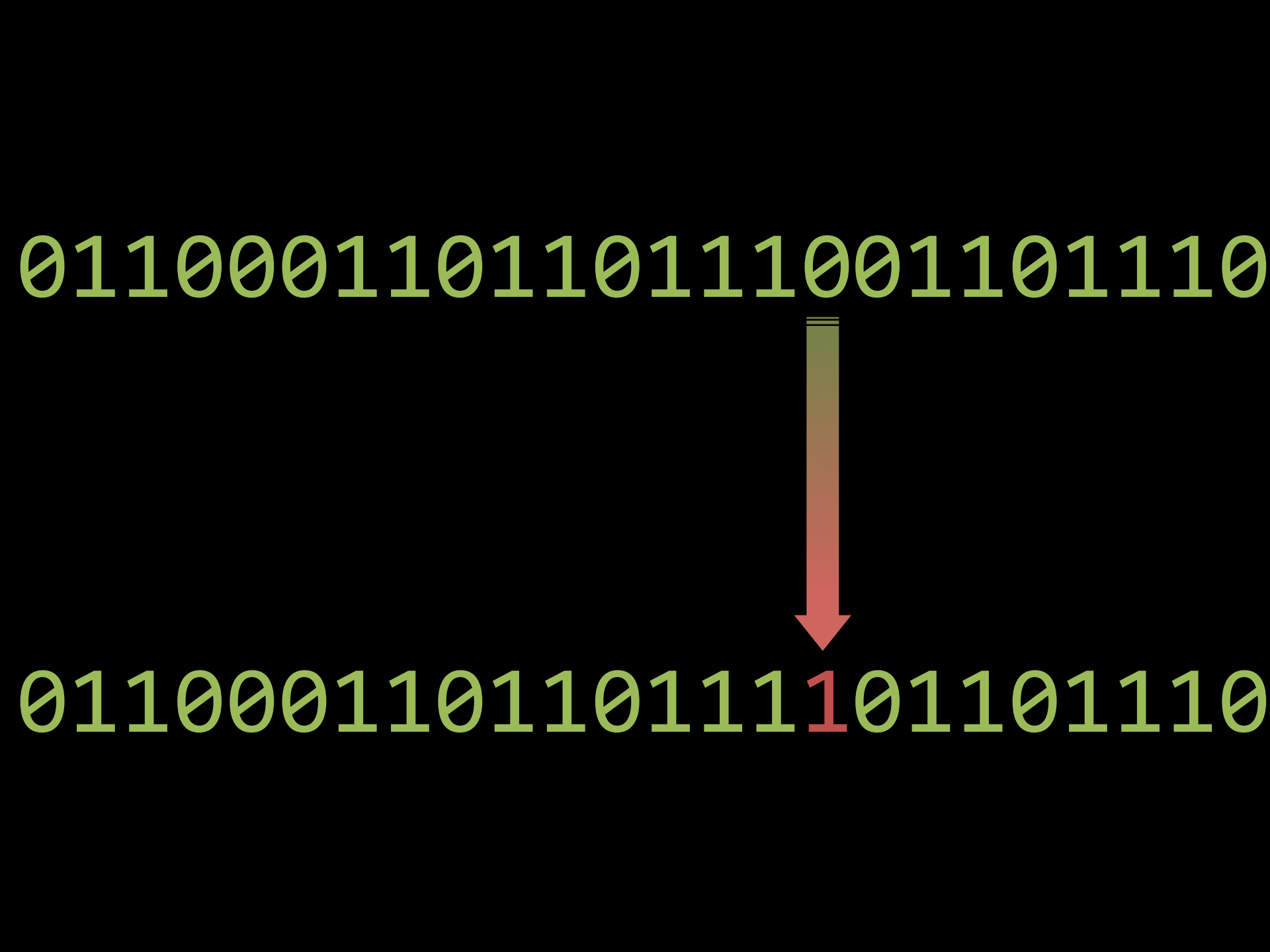
1500 daily DNS requests per person.

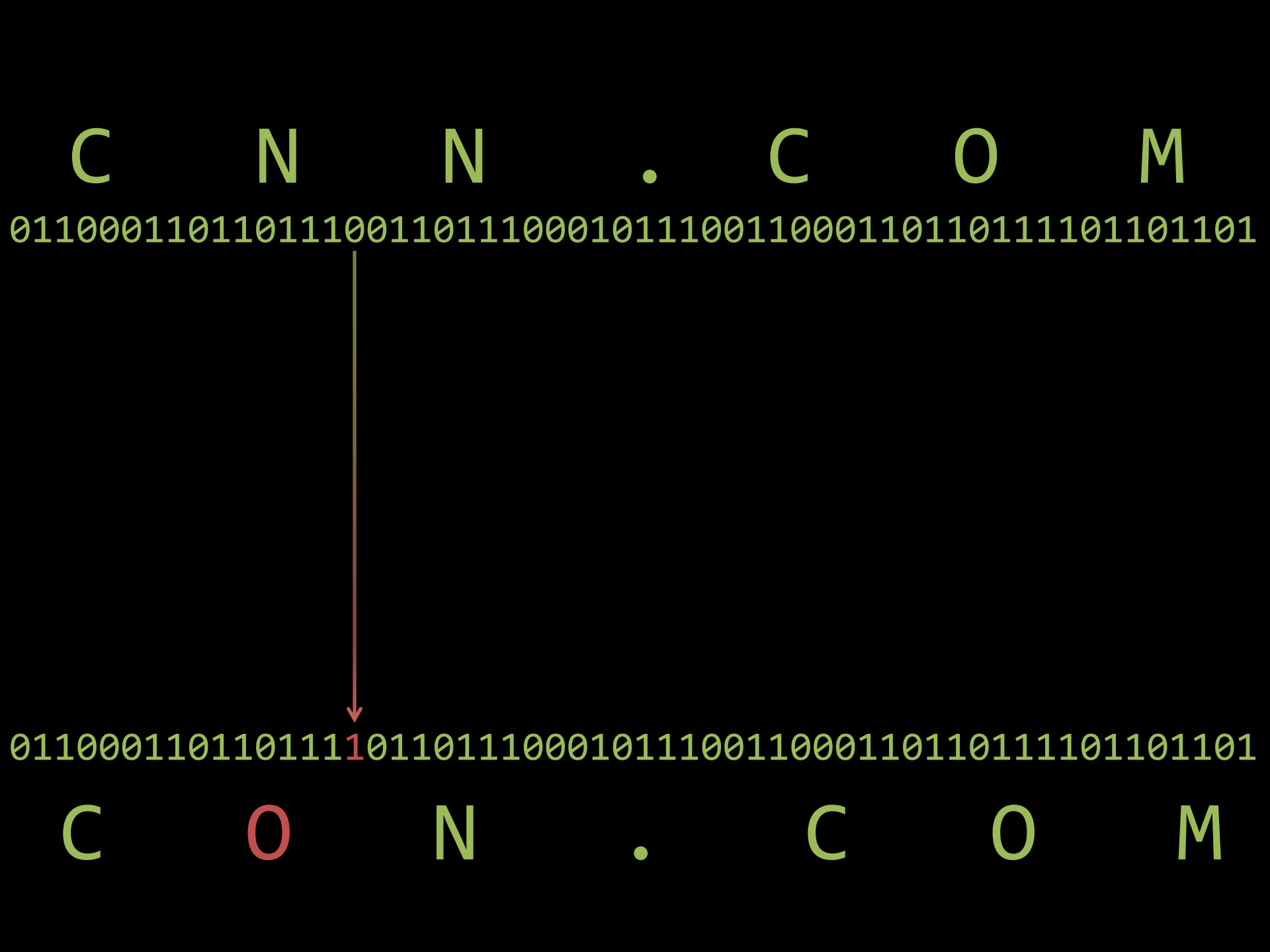
Humans type

3 of them.


HAL 9000


1
0
0
1

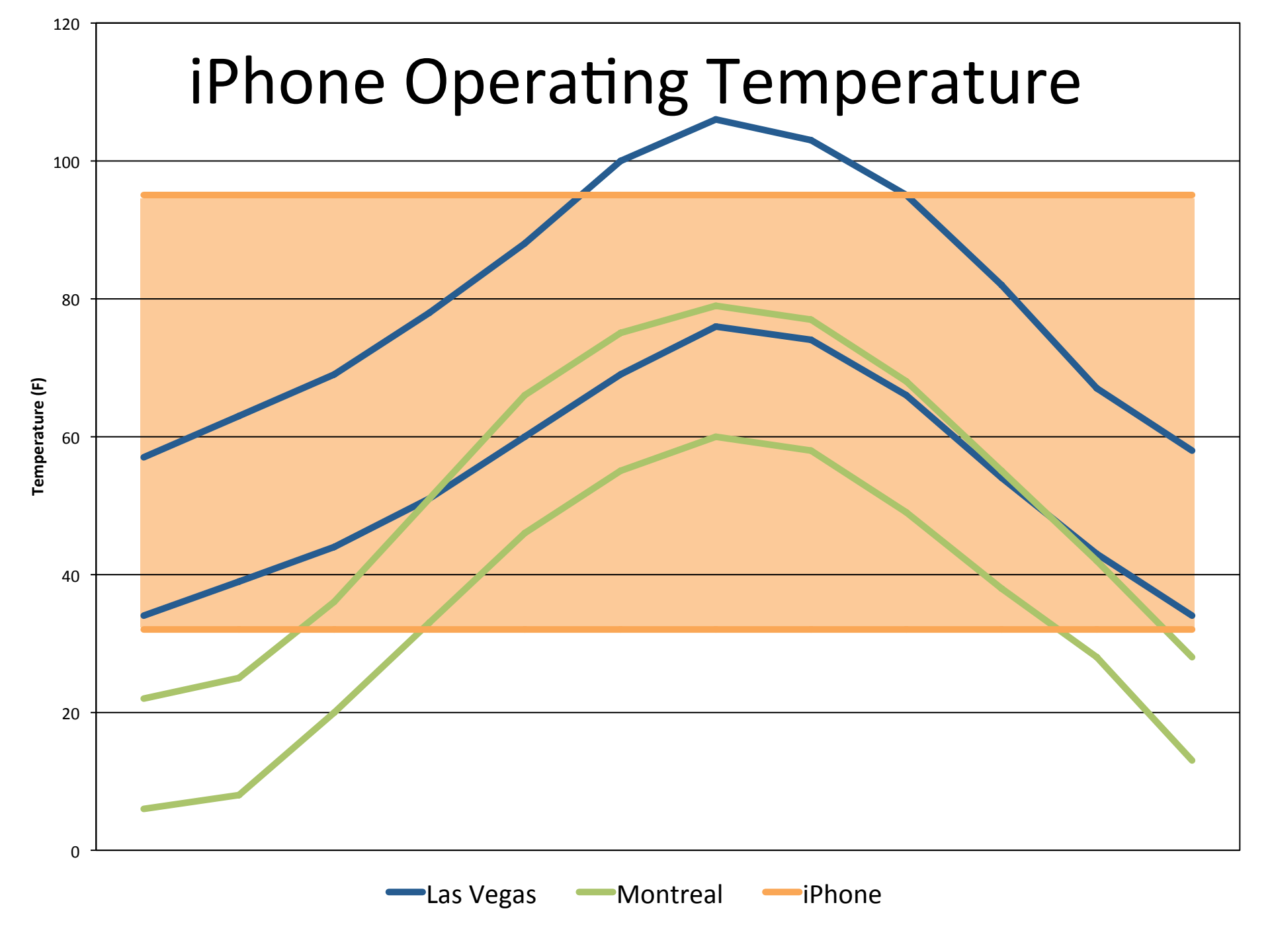

01100011011011100110111
01100011011011110110111


C N N . C O M
01100011011011100110111000101110011000110110111101101101
01100011011011110110111000101110011000110110111101101101
C O N . C O M

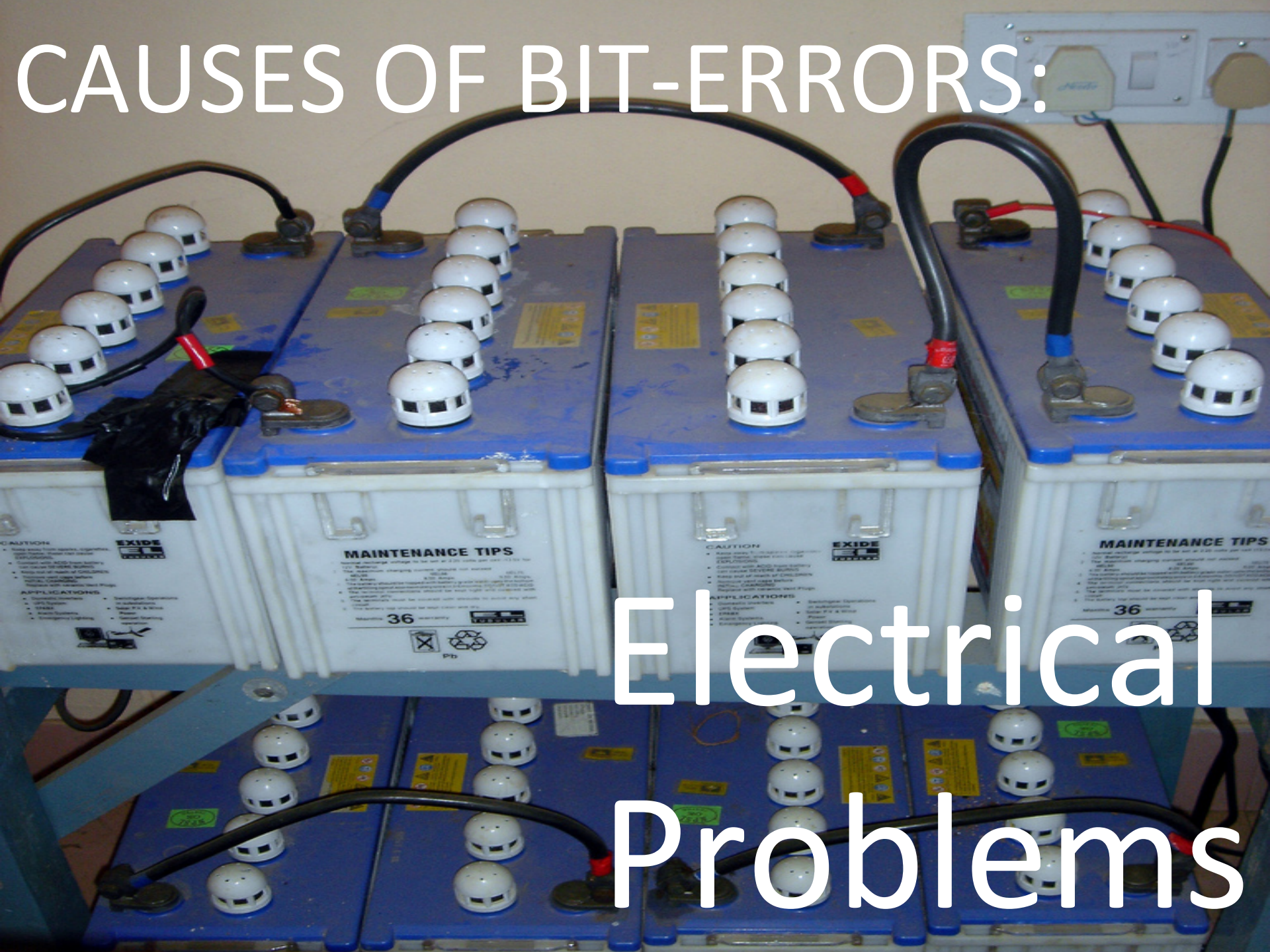

54C

CAUSES OF BIT-ERRORS:

Heat


iPhone Operating Temperature
120
100
80
60
40
20
0
Temperature (F)
Las Vegas
Montreal
iPhone

CAUSES OF BIT-ERRORS:



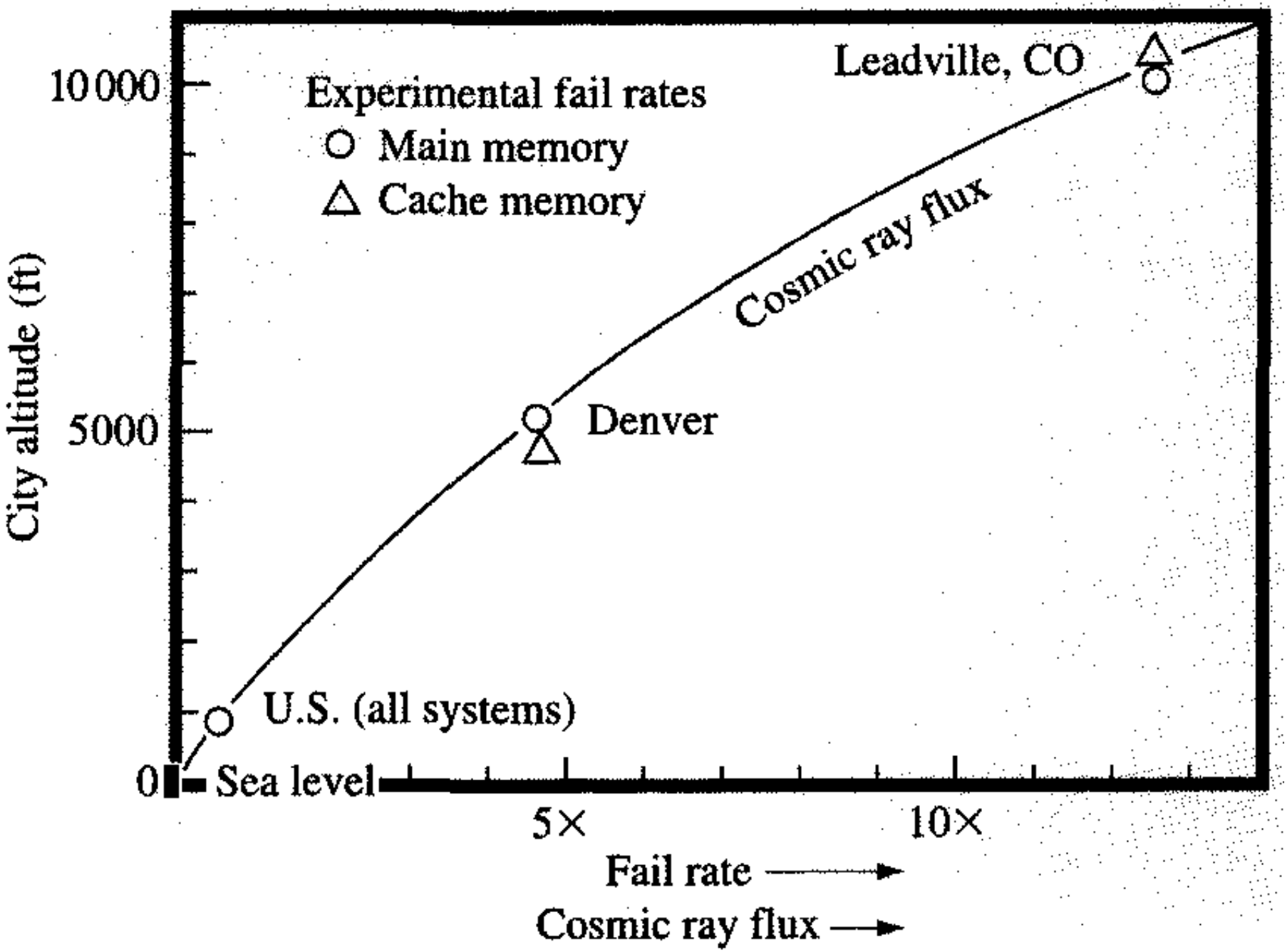
Electrical Problems

CAUSES OF BIT-ERRORS:

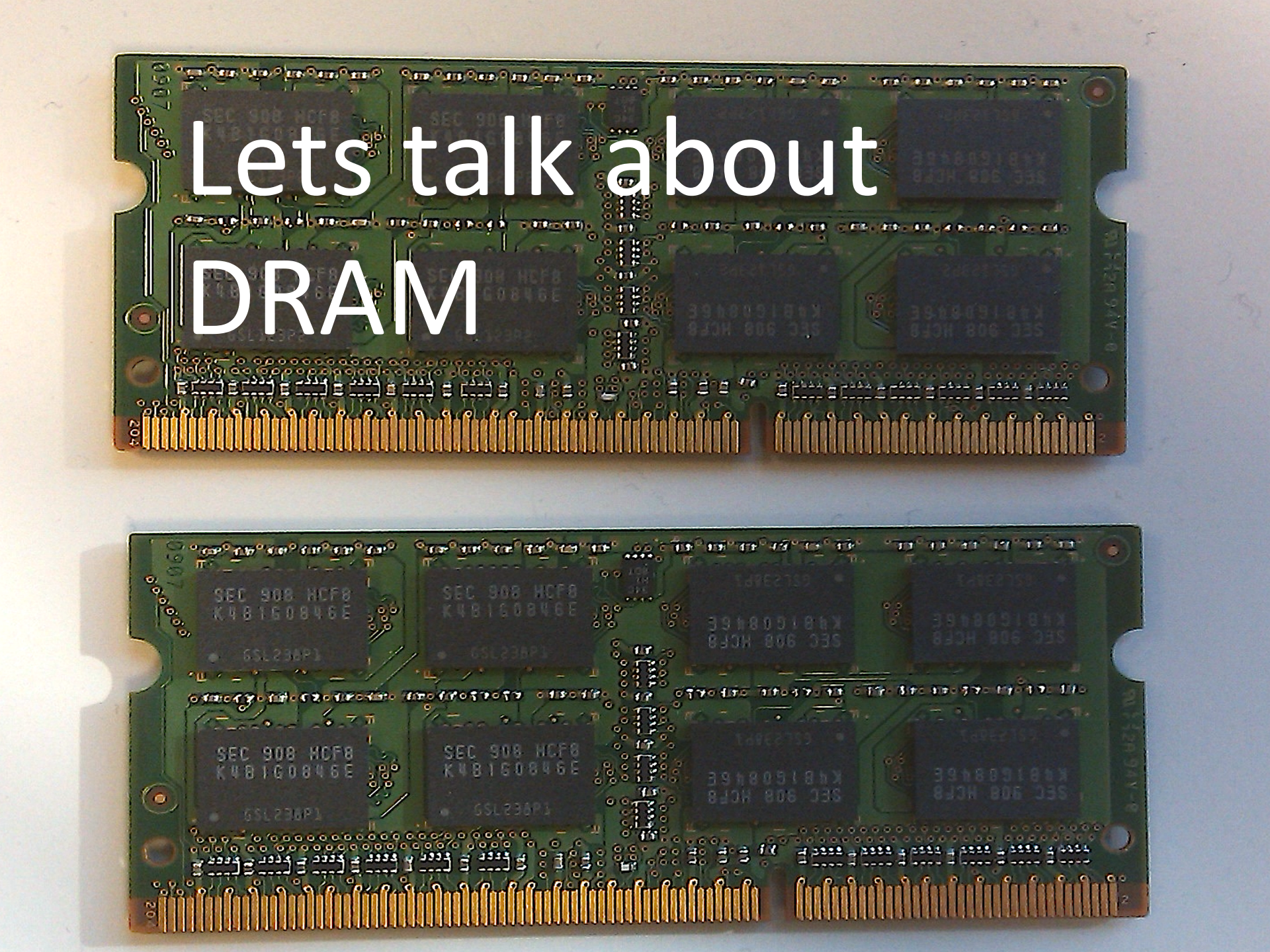
Defects

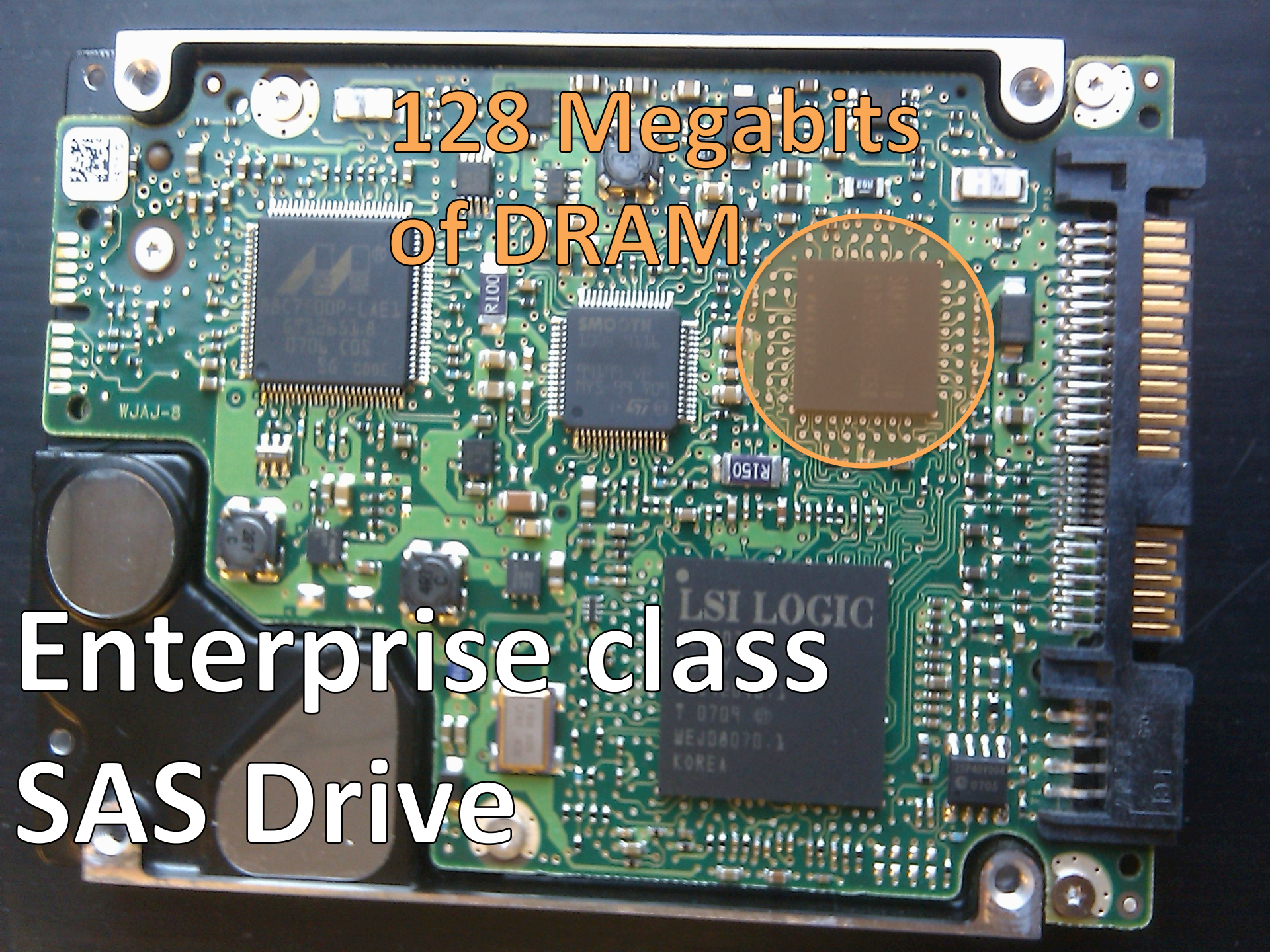
CAUSES OF BIT-ERRORS:

Cosmic Rays

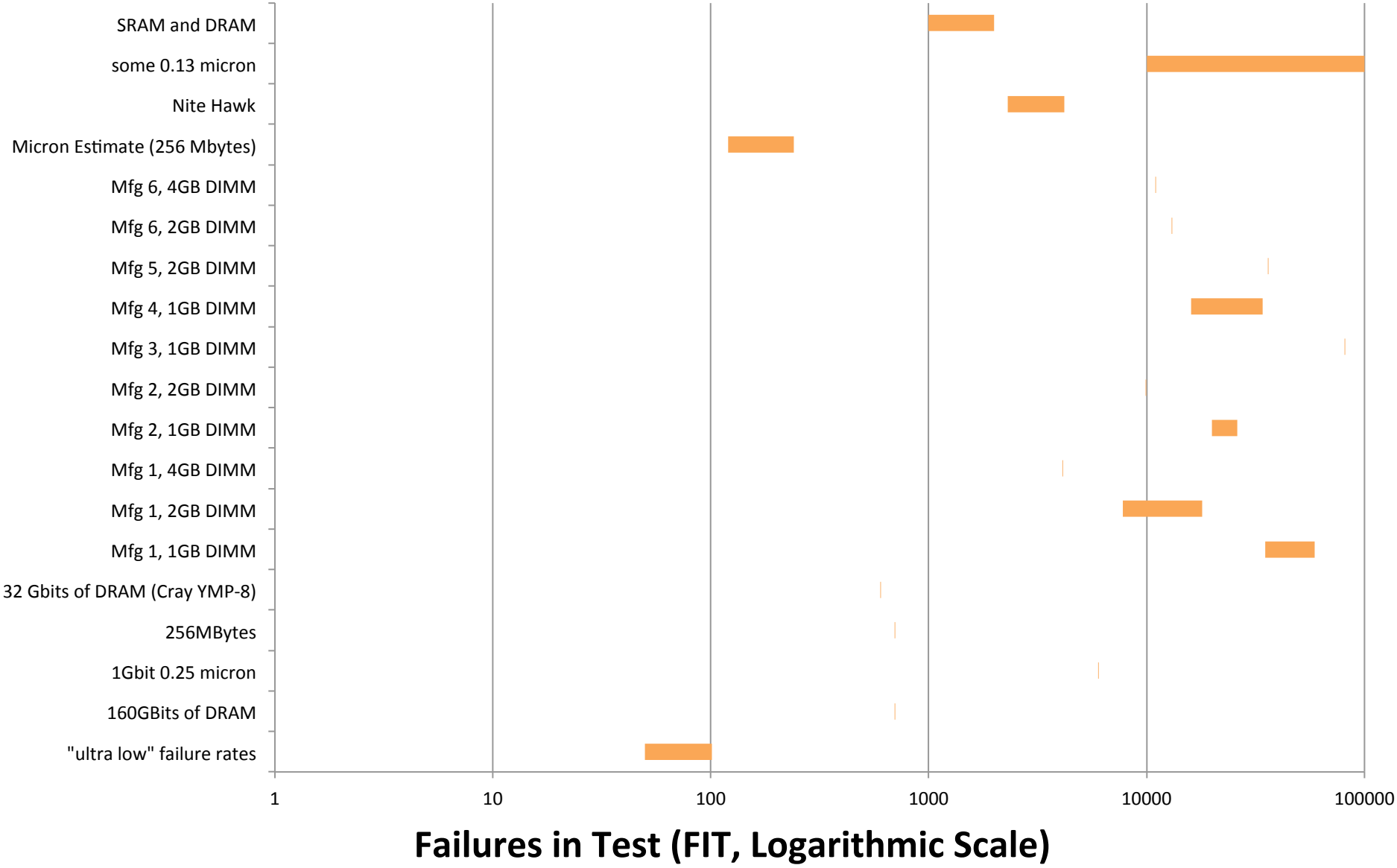


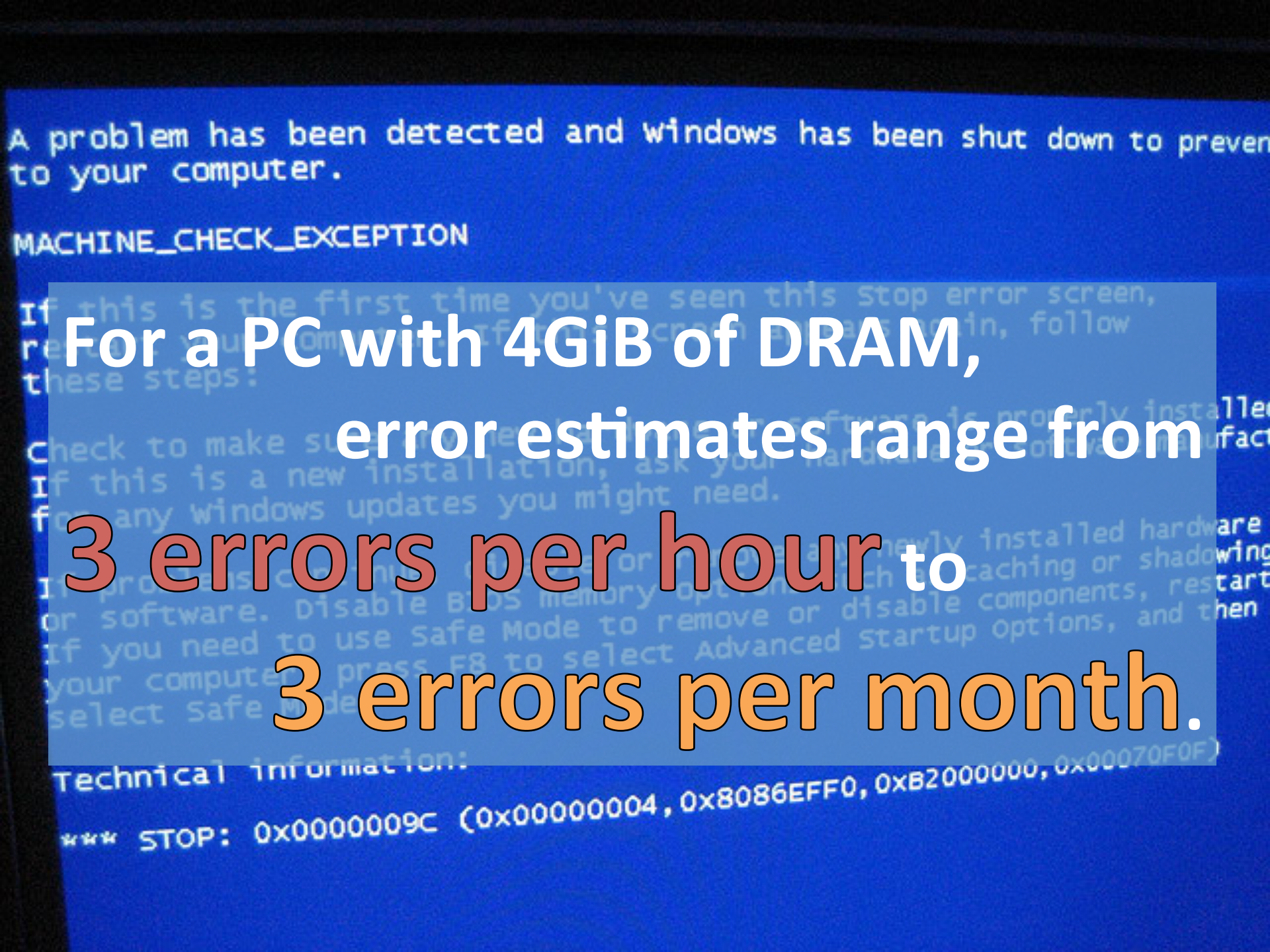
IBM Journal of Research and Development, vol. 40, no. 1, page 13


Lets talk about
DRAM

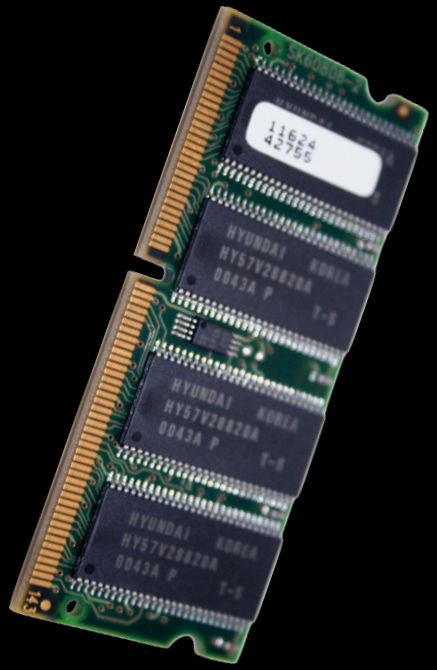

128 Megabits
of DRAM
LSI LOGIC
Enterprise class
SAS Drive

DRAM Failure Rates




A problem has been detected and windows has been shut down to preven
to your computer.
MACHINE_CHECK_EXCEPTION
For a PC with 4GiB of DRAM,
error estimates range from
3 errors per hour to
3 errors per month.
Technical information:
*** STOP: 0x0000009C (0x00000004,0x8086EFF0,0xB2000000,0x

×


HYUNDAI
HY57V28820A
HYUNDAI
HY57V28820A
HYUNDAI
HY57V28820A

=

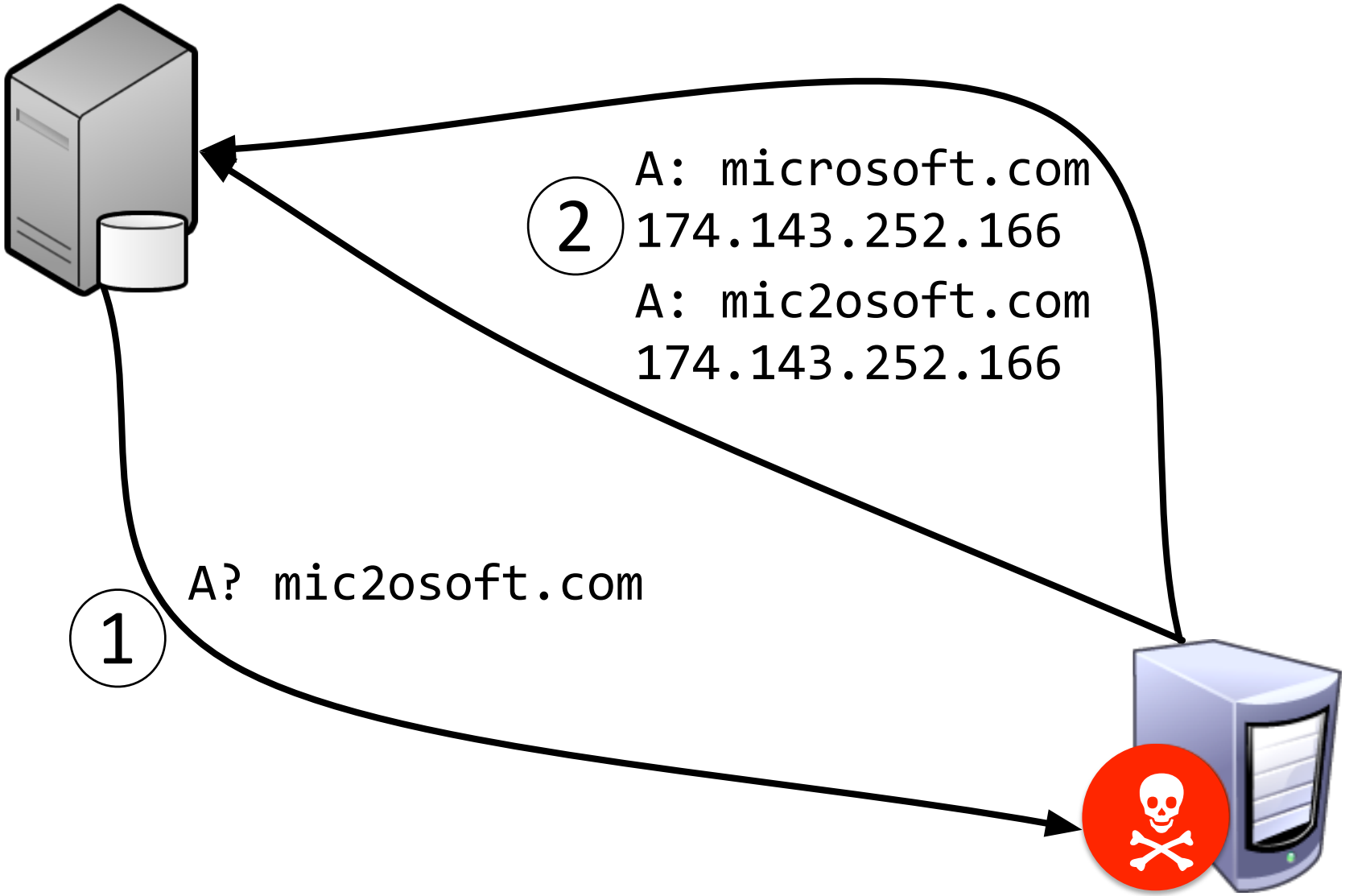
600 PiB

Experiment: Step 1

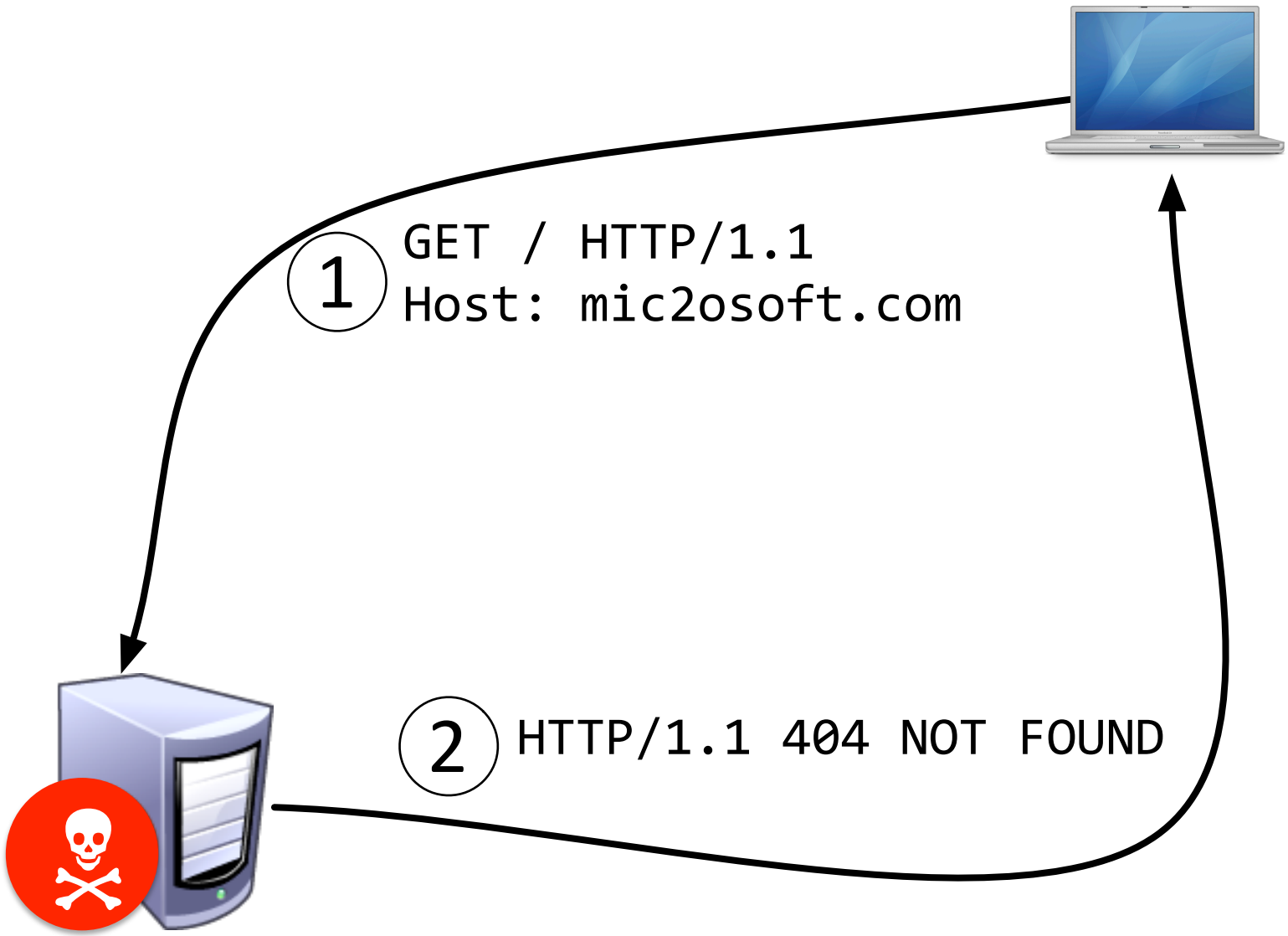
ikamai.net
aeazon.com
a-azon.com
amazgn.com
microsmft.com
micrgsoft.com
miarosoft.com
iicrosoft.com
microsnft.com
mhcrosoft.com
eicrosoft.com
mic2osoft.com
micro3oft.com
doublechick.net
do5bleclick.net
doubleslick.net

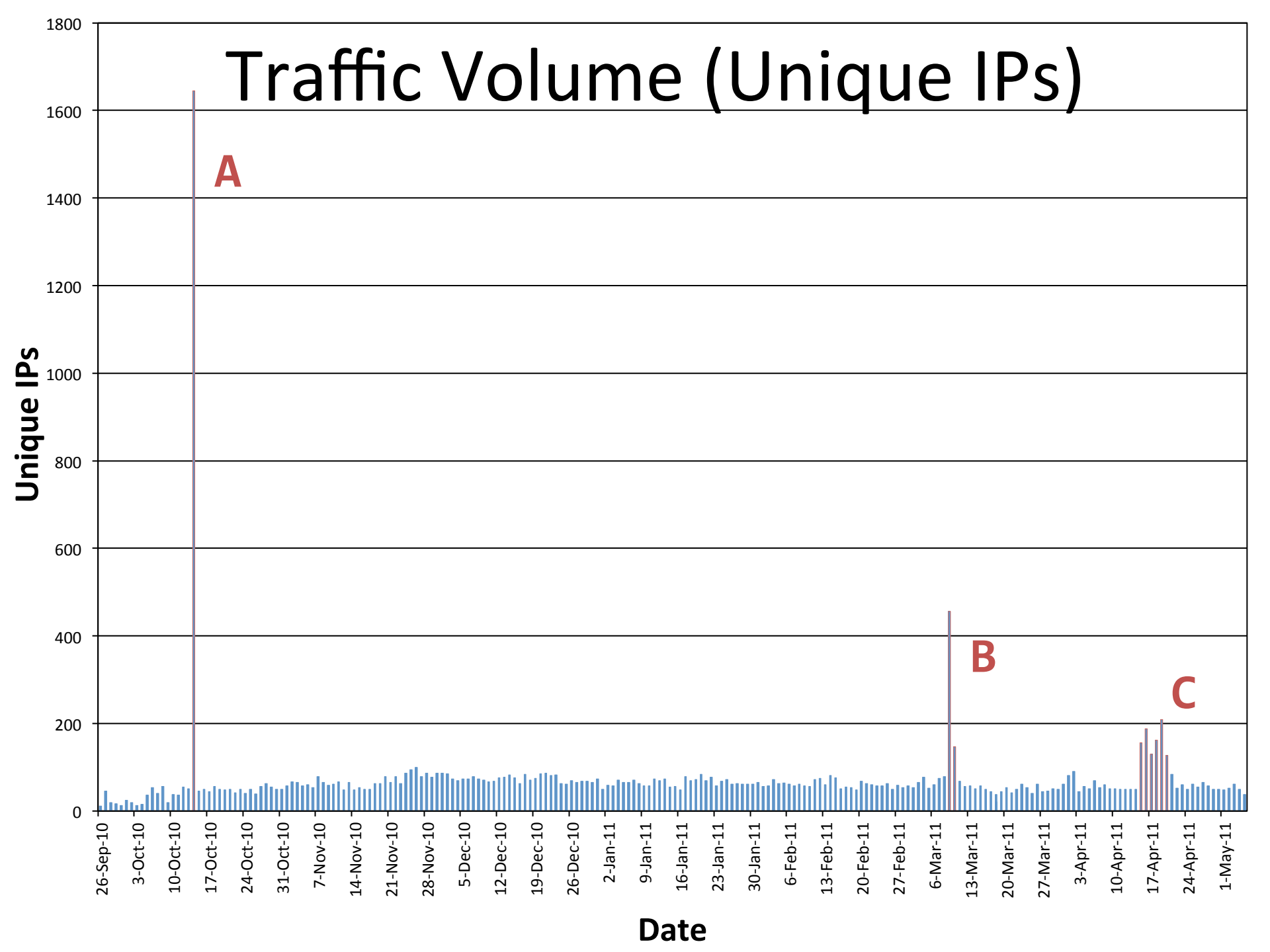
li6e.com
0mdn.net
2-dn.net
2edn.net
2ldn.net
2mfn.net
2mln.net
2odn.net
6mdn.net
fbbdn.net
fbgdn.net
gbcdn.net
fjcdn.net
dbcdn.net
roop-servers.net
gmaml.com

Experiment, Step 2

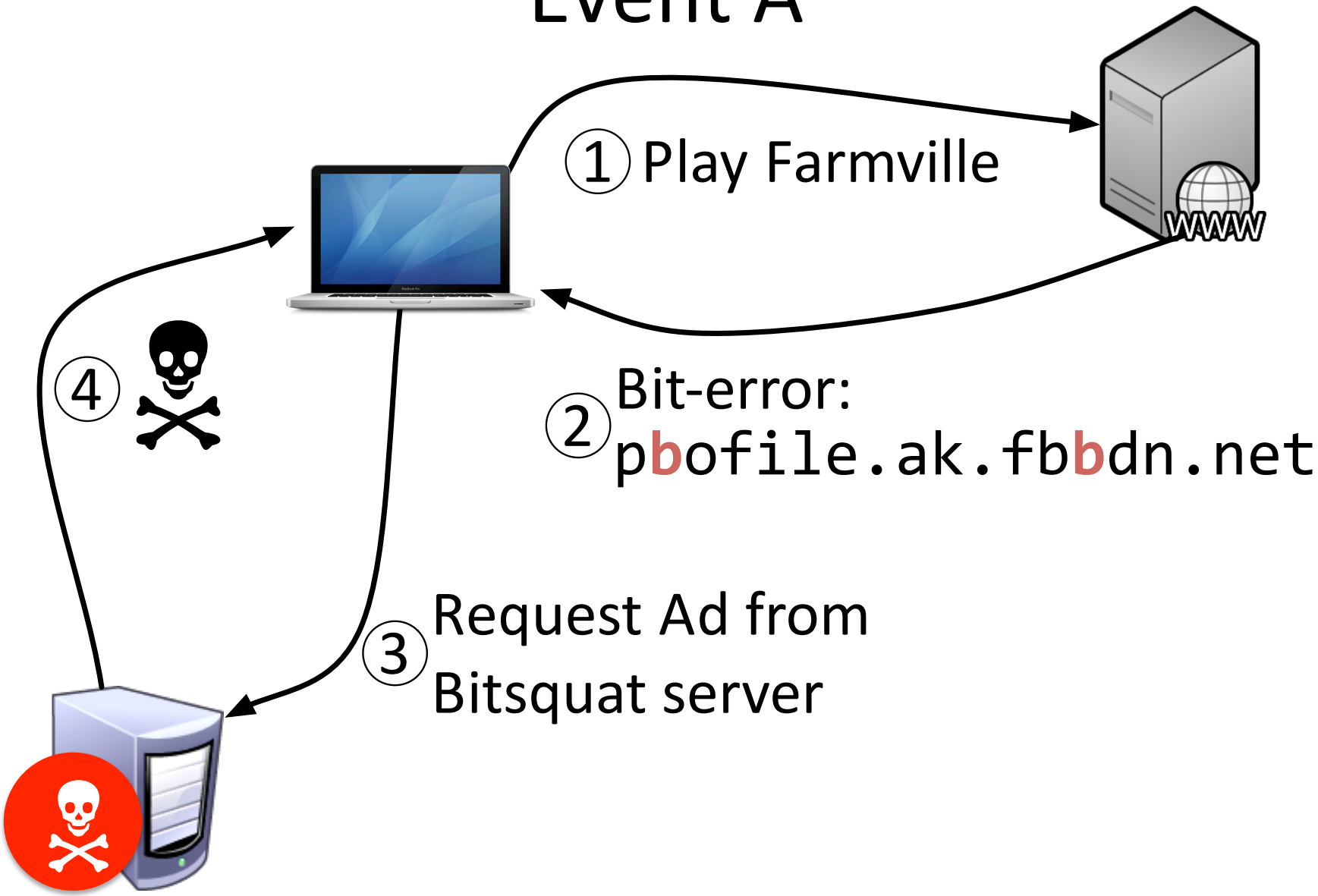


Experiment, Step 3

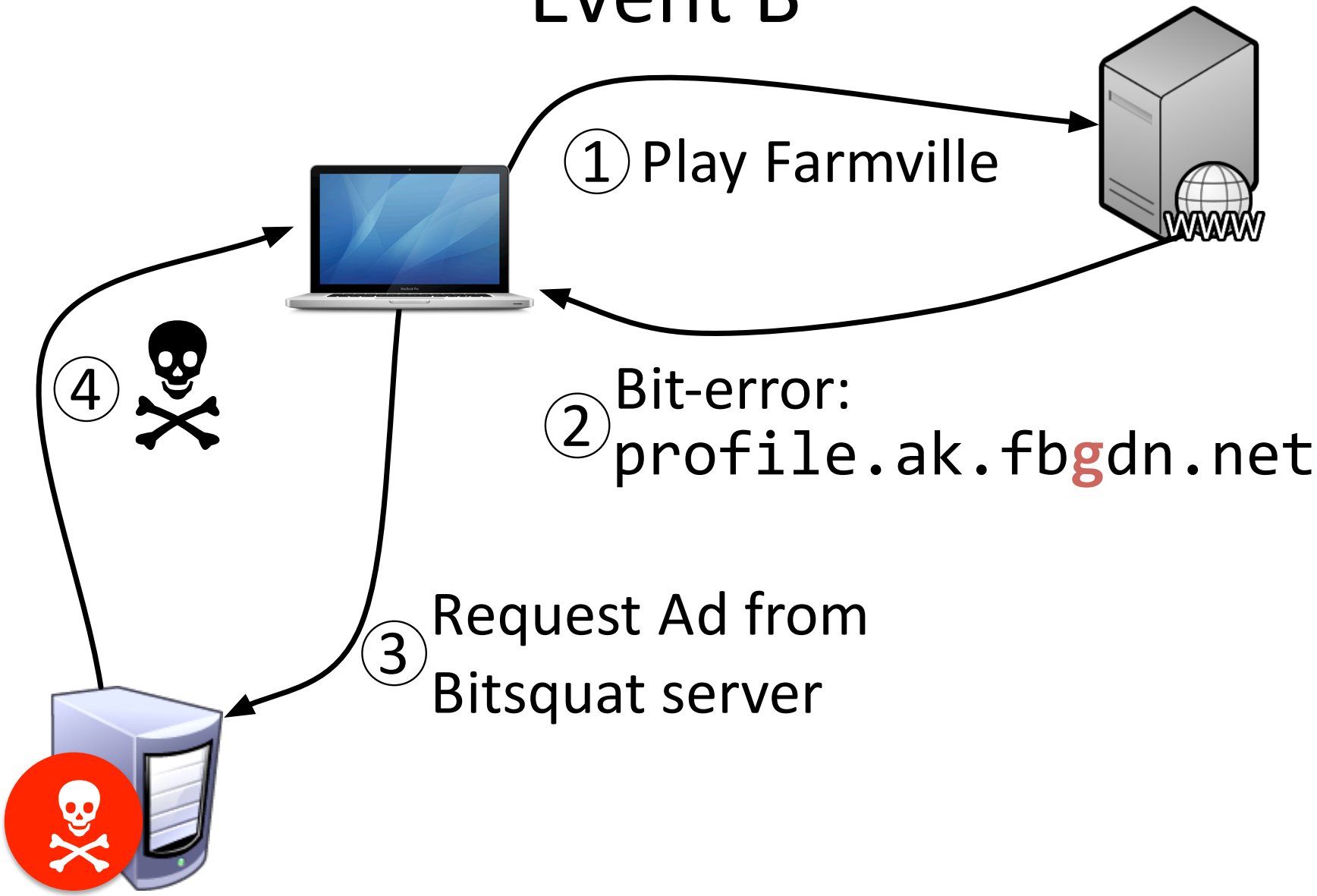



Traffic Volume (Unique IPs)
Unique IPs
1800
1600
1400
1200
1000
800
600
400
200
0
A
B
C
26-Sep-10
3-Oct-10
10-Oct-10
17-Oct-10
24-Oct-10
31-Oct-10
7-Nov-10
14-Nov-10
21-Nov-10
28-Nov-10
5-Dec-10
12-Dec-10
19-Dec-10
26-Dec-10
2-Jan-11
9-Jan-11
16-Jan-11
23-Jan-11
30-Jan-11
6-Feb-11
13-Feb-11
20-Feb-11
27-Feb-11
6-Mar-11
13-Mar-11
20-Mar-11
27-Mar-11
3-Apr-11
10-Apr-11
17-Apr-11
24-Apr-11
1-May-11
Date

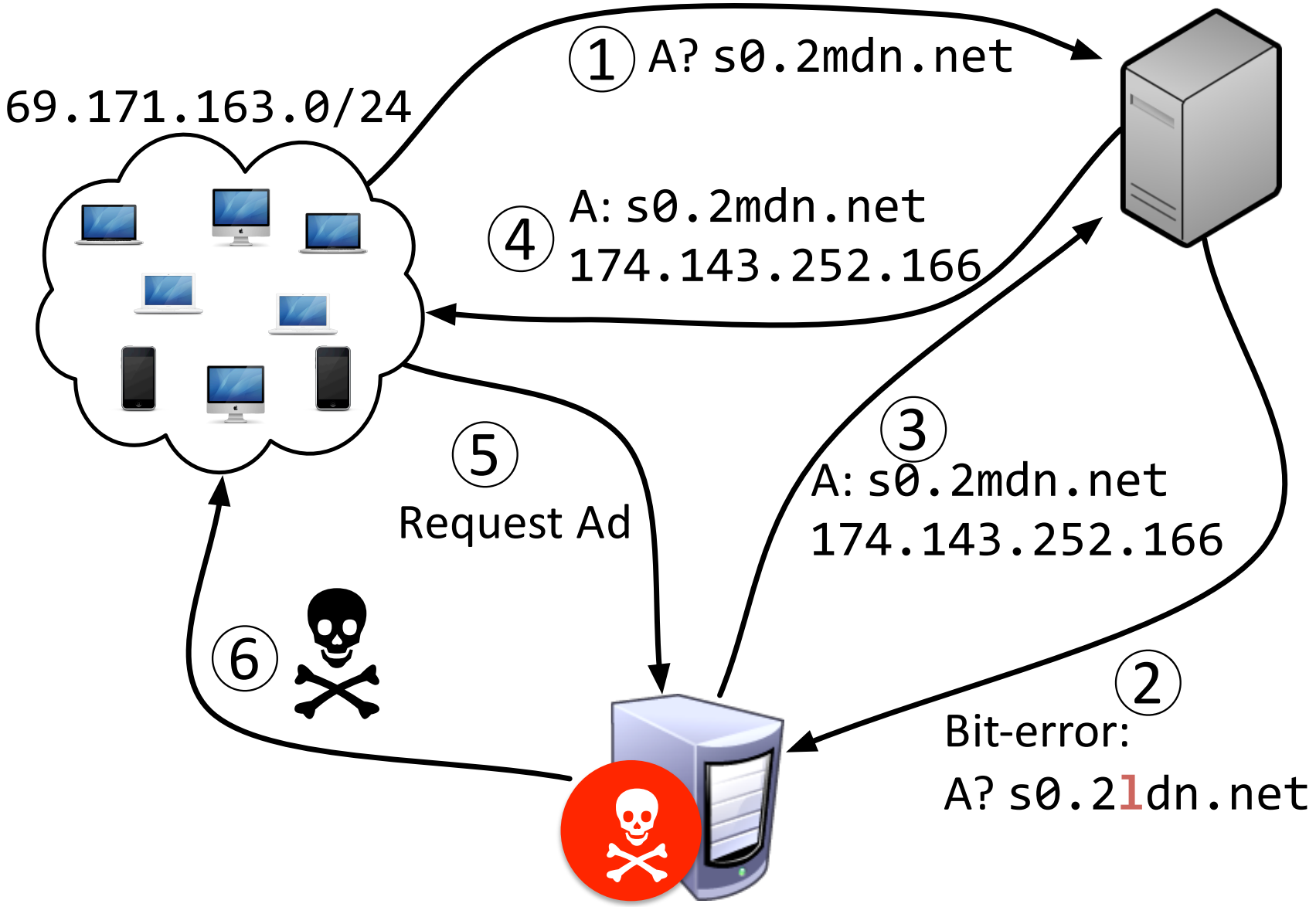
Event A

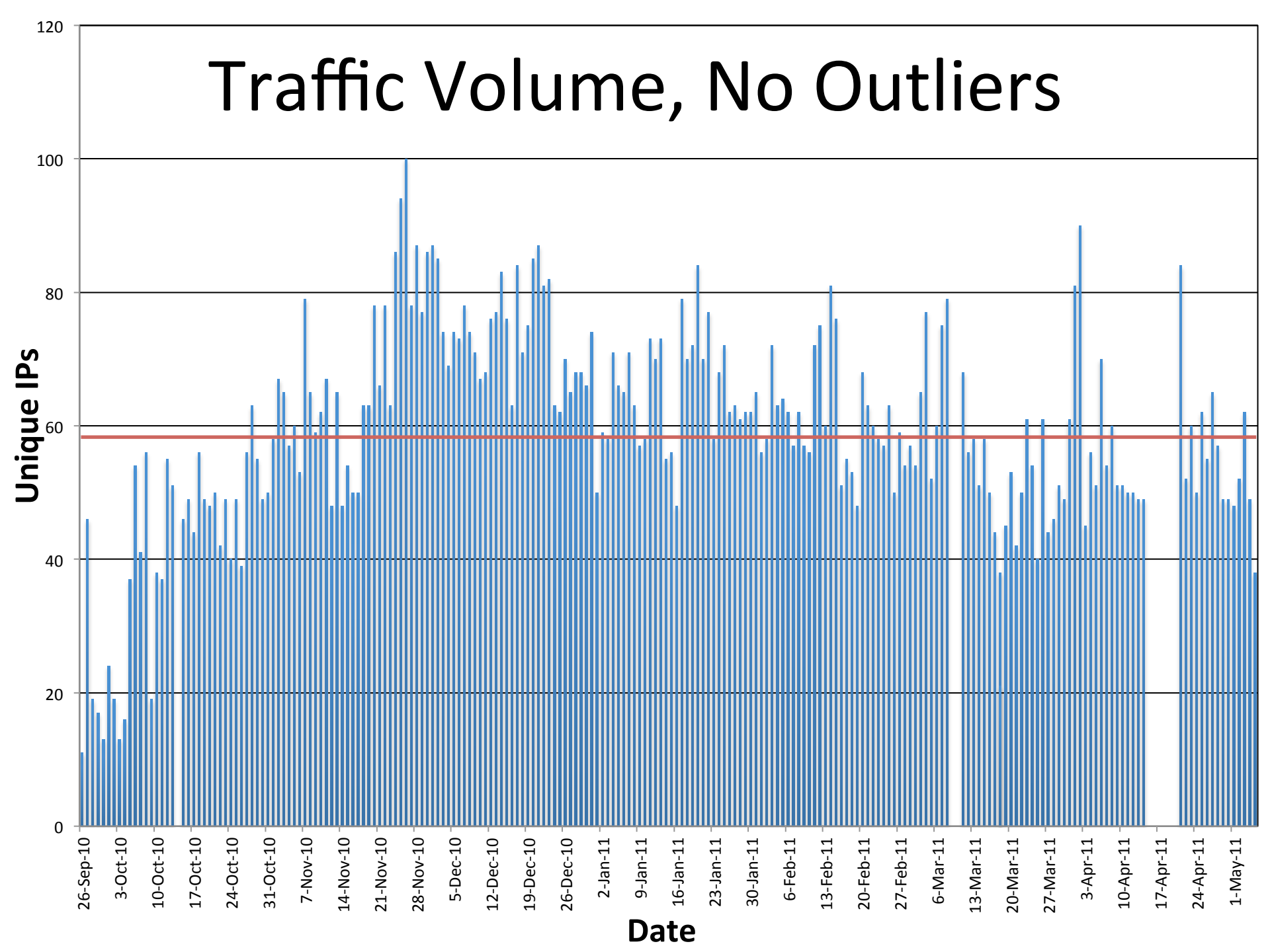

① Play Farmville
WWW
② Bit-error:
pbofile.ak.fbbdn.net
③ Request Ad from
Bitsquat server
④

Event B

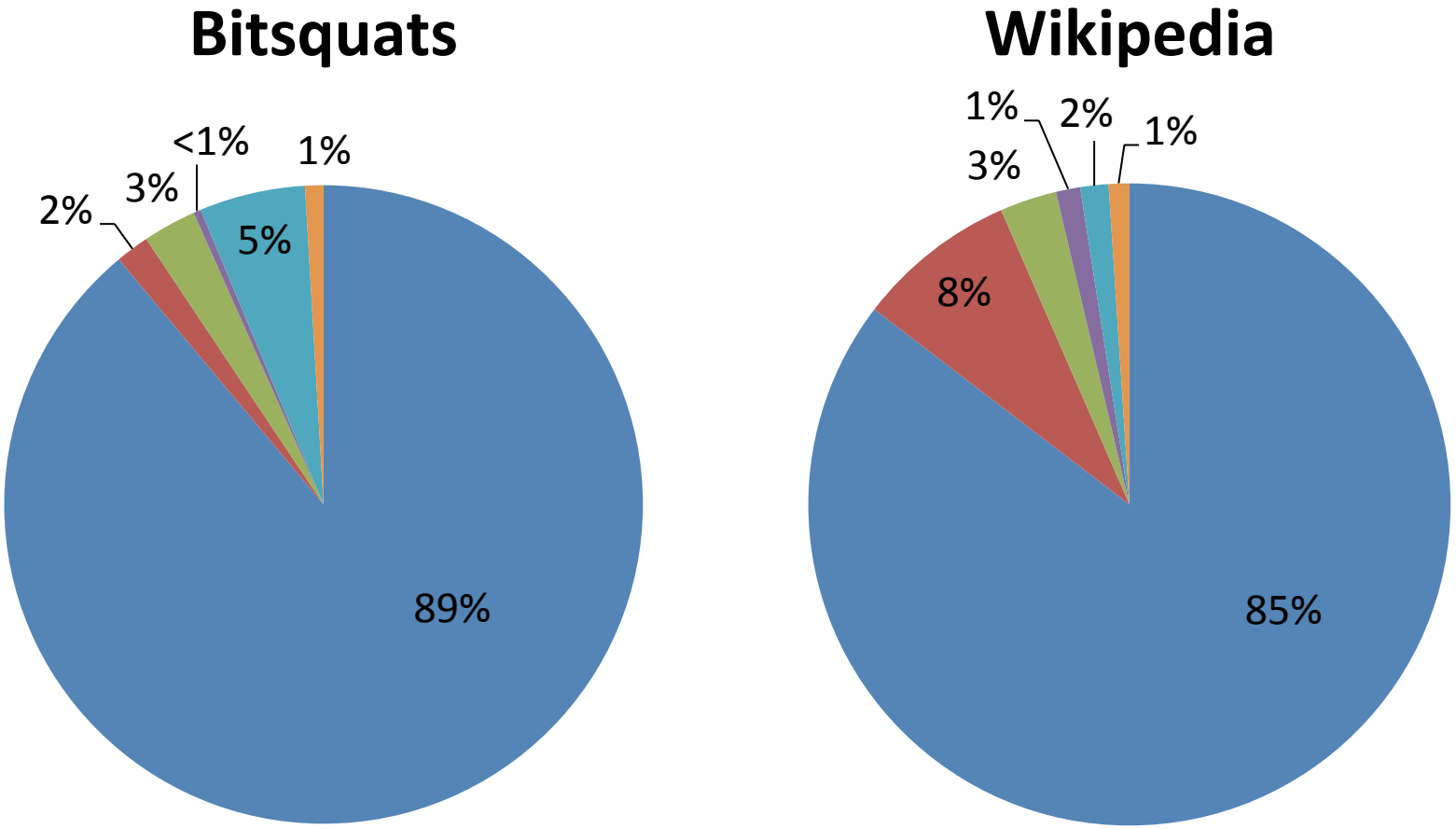

① Play Farmville
WWW
② Bit-error:
profile.ak.fbgdn.net
③ Request Ad from
Bitsquat server
④

Event C

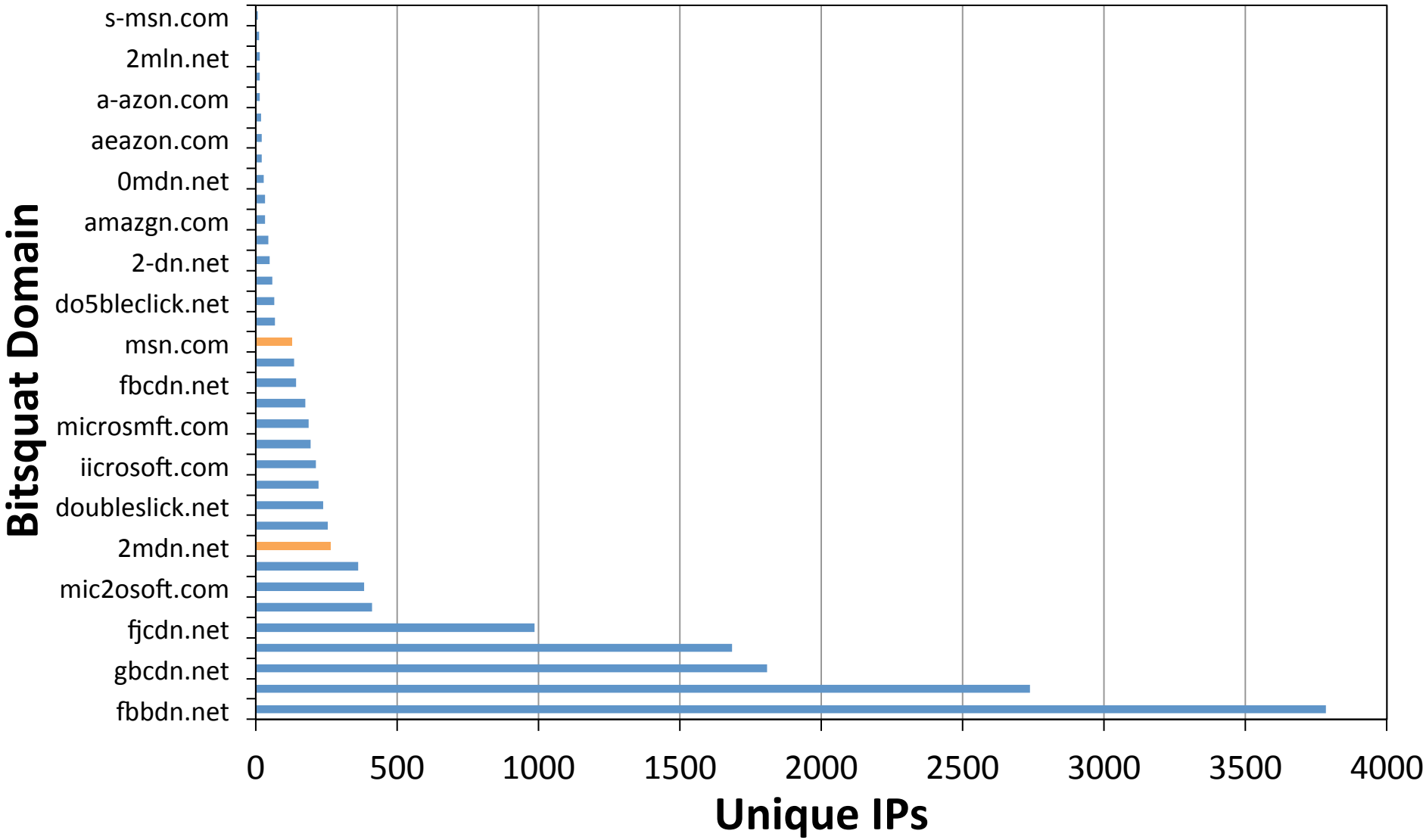

69.171.163.0/24
1 A? s0.2mdn.net
4 A: s0.2mdn.net
174.143.252.166
3 A: s0.2mdn.net
174.143.252.166
5 Request Ad
6
2 Bit-error:
A? s0.2ldn.net


Traffic Volume, No Outliers
Unique IPs
Date
120
100
80
60
40
20
0
26-Sep-10
3-Oct-10
10-Oct-10
17-Oct-10
24-Oct-10
31-Oct-10
7-Nov-10
14-Nov-10
21-Nov-10
28-Nov-10
5-Dec-10
12-Dec-10
19-Dec-10
26-Dec-10
2-Jan-11
9-Jan-11
16-Jan-11
23-Jan-11
30-Jan-11
6-Feb-11
13-Feb-11
20-Feb-11
27-Feb-11
6-Mar-11
13-Mar-11
20-Mar-11
27-Mar-11
3-Apr-11
10-Apr-11
17-Apr-11
24-Apr-11
1-May-11

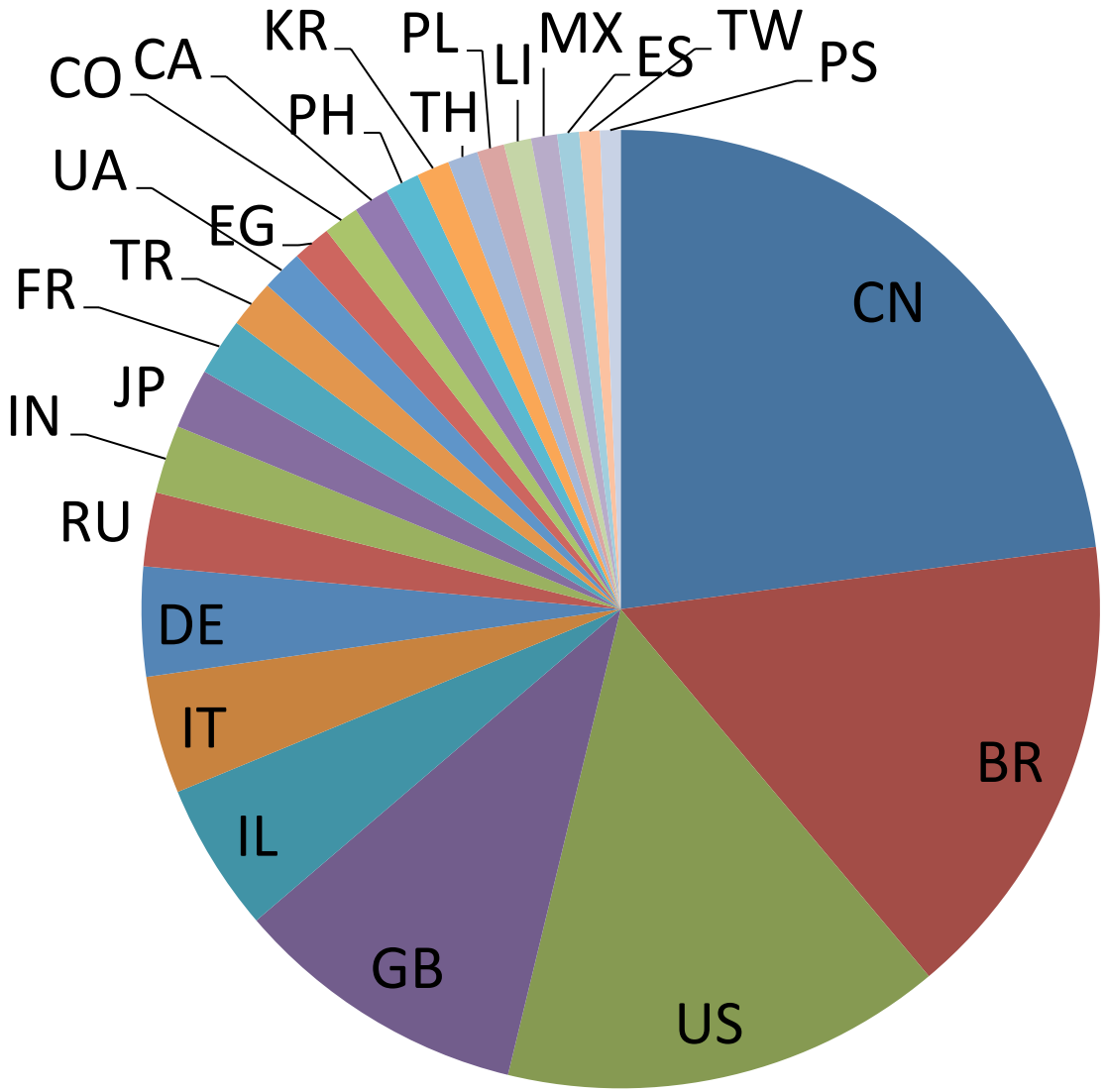
OS Statistics



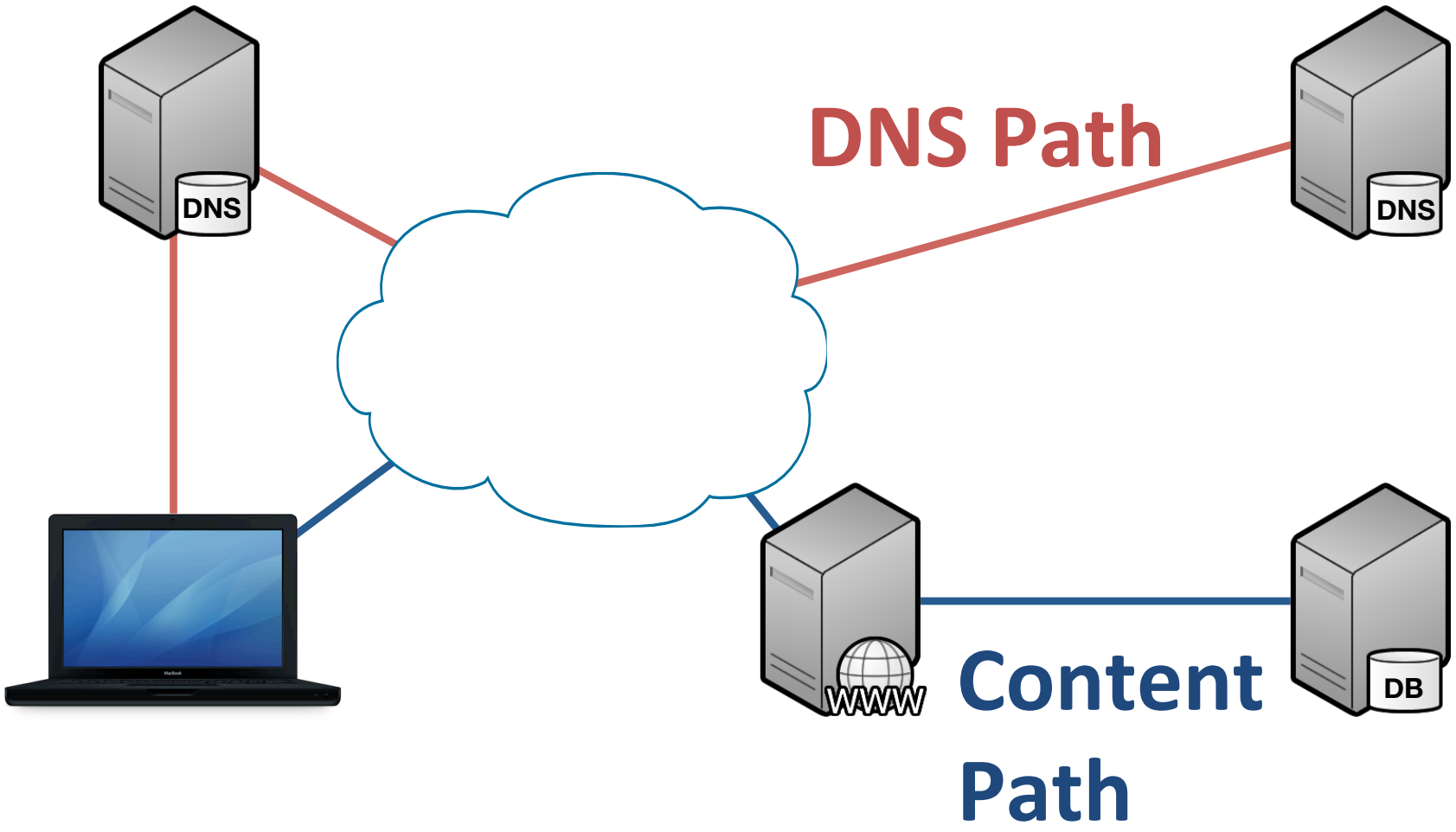
Bitsquat Popularity



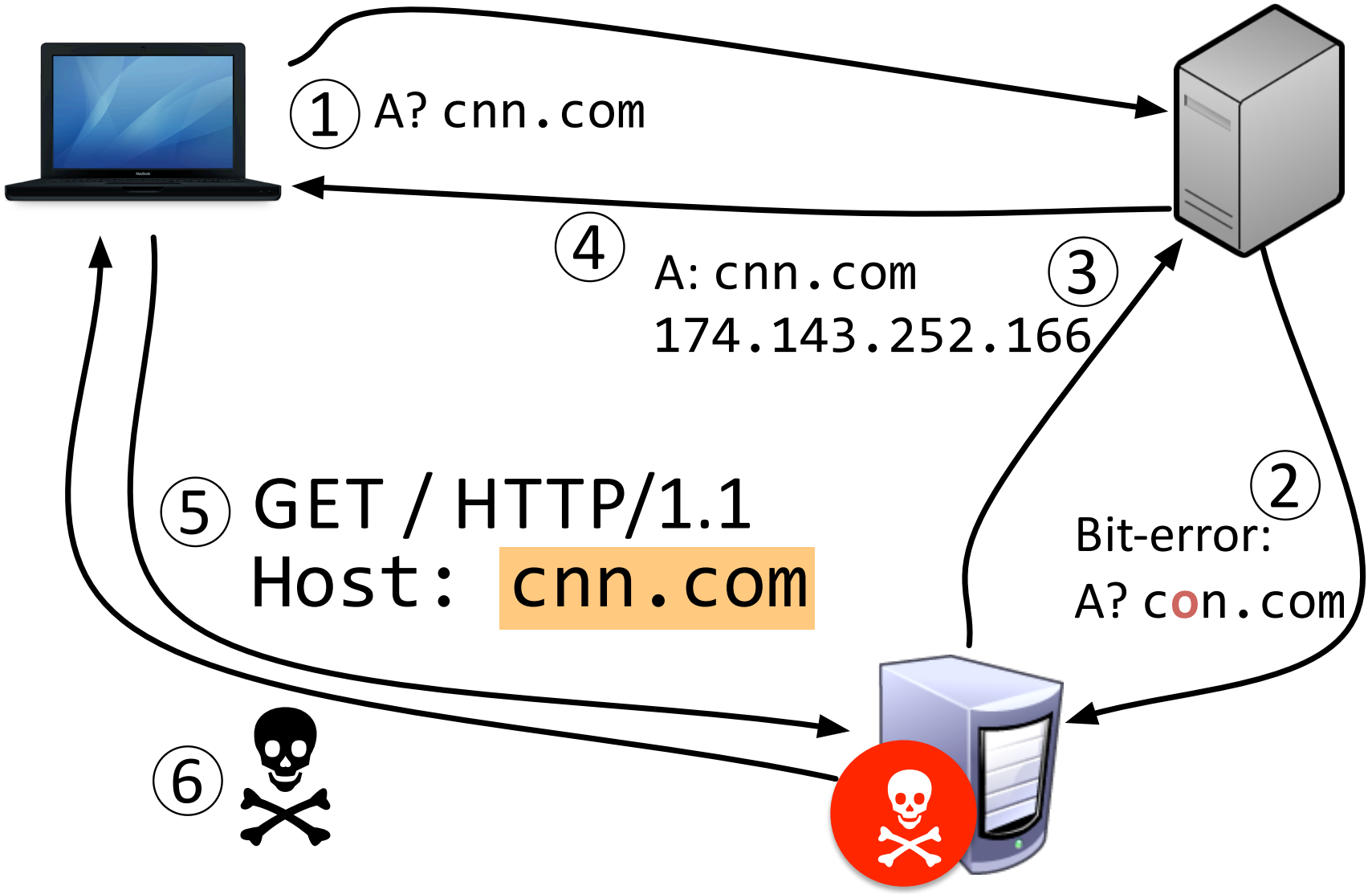
Visitors by Country (bitsquats of Microsoft.com)



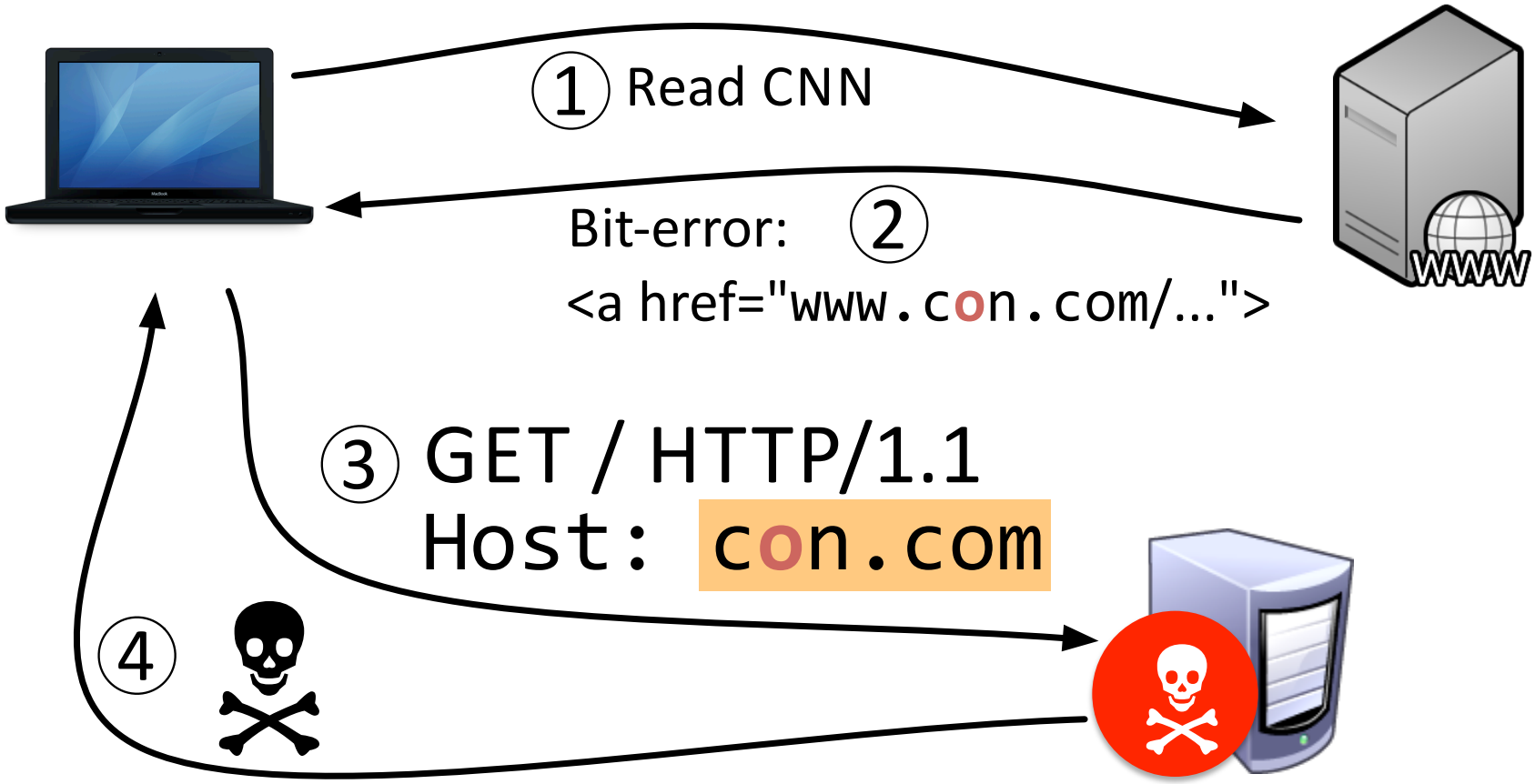
Where Bit-errors Happen



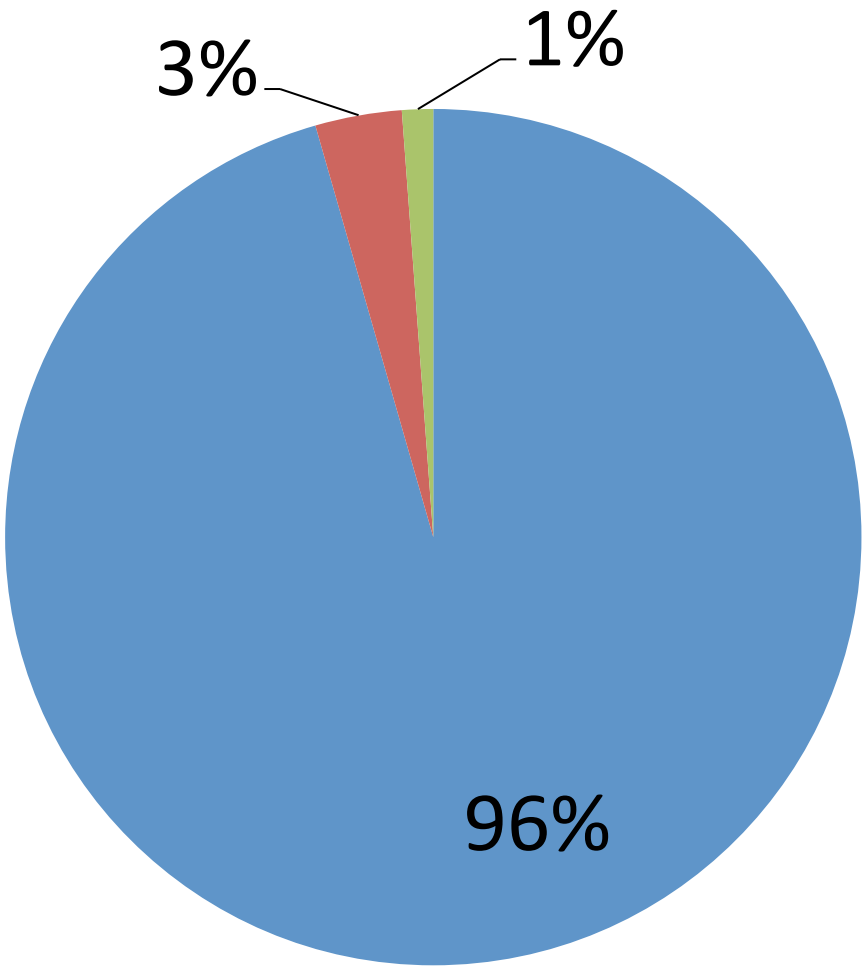
Bit-errors on the DNS Path



Bit-errors on the Content Path



Domain in HTTP Host Header

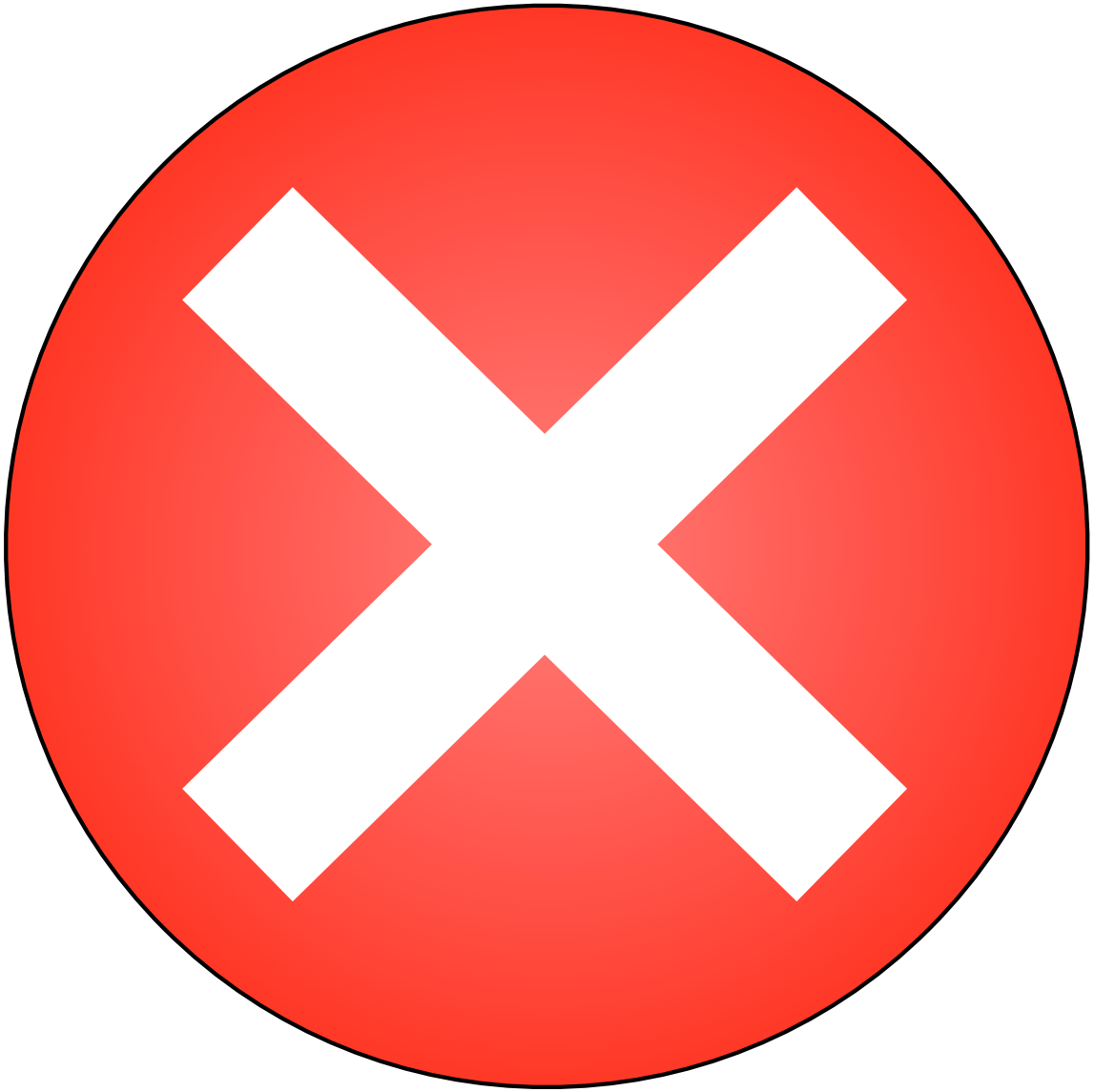


Bitsquat Original Other

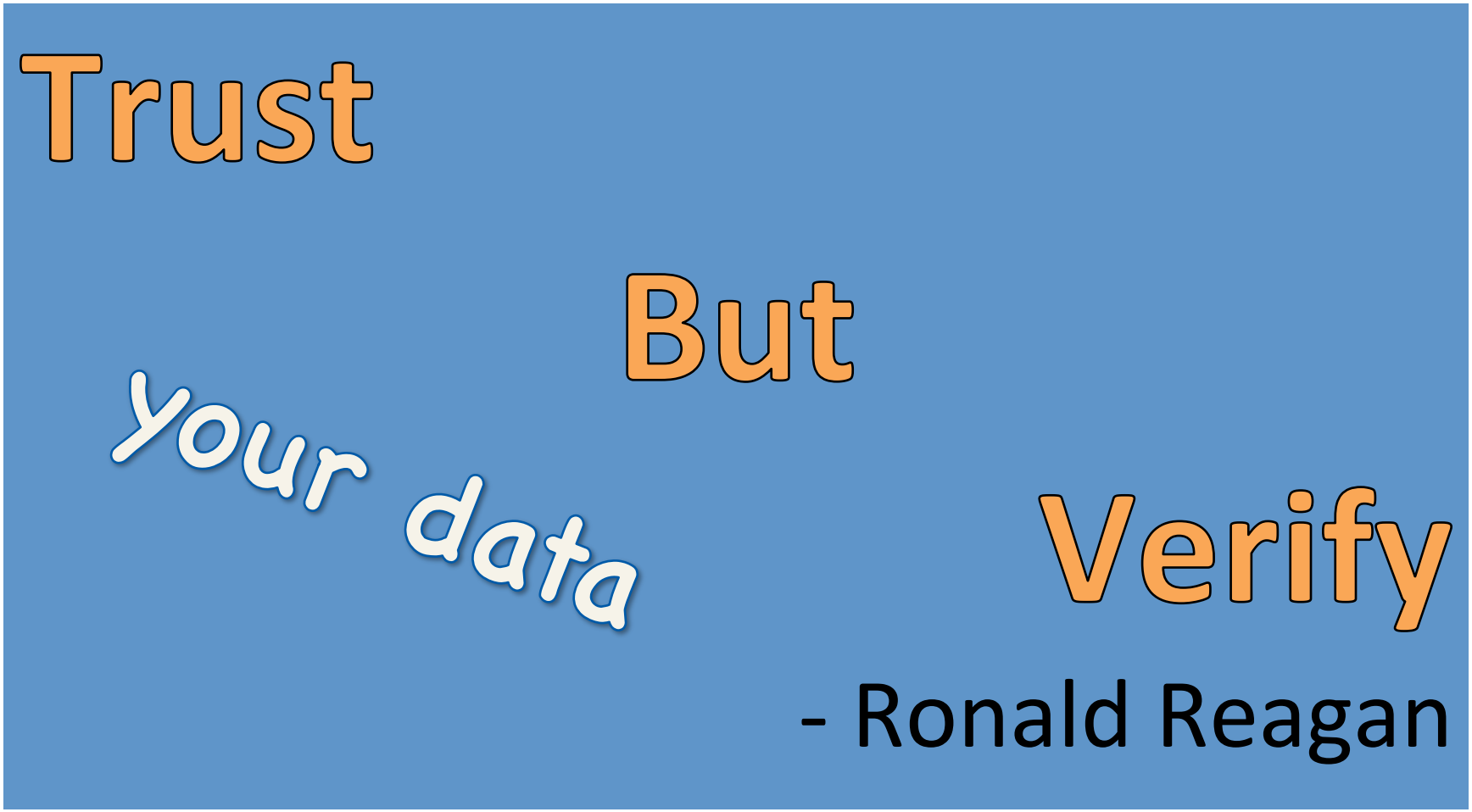
Mitigations

ECC ON EVERYTHING

Mitigations



Mitigations



Questions?

Image Attribution

- Slide 3: Earth. NASA
- Slide 4: Logos © their respective owners
- Slide 5: Childrens Blocks. Flickr User: lobo235
- Slide 6: Dollar bills. Flickr User: Images_of_Money
- Slide 10: HAL 9000 © Warner Brothers Pictures
- Slide 14: Heat Lamp. “Using memory errors to attack a virtual machine” by Govindavajhala and Appel, IEEE S&P 2003
- Slide 15: Desert Sun. Flickr User: Steve & Jemma Copley
- Slide 17: Backup Power. David Robinson. Flickr User: dgrobinson
- Slide 18: Fake Capacitor. Found on Internet, likely from chinauser.cn
- Slide 19: Homunculus Nebula. NASA
- Slide 21: DRAM. Self
- Slide 22: SAS Drive. Self
- Slide 24: BSOD. Wayne Williamson. Flickr User: ka3vo
- Slide 25: Blue Marble. NASA