BITSQUATTING

DNS HIJACKING WITHOUT EXPLOITATION

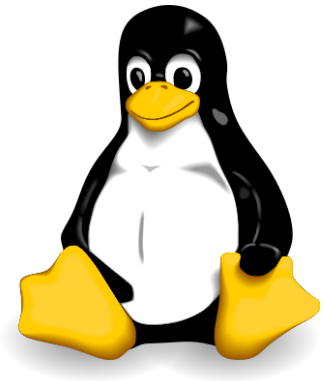
ARTEM DINABURG

artem@dinaburg.org
artem.dinaburg@raytheon.com

The Problem

android

Affected Platforms



Wii

PlayStation 3

symbian

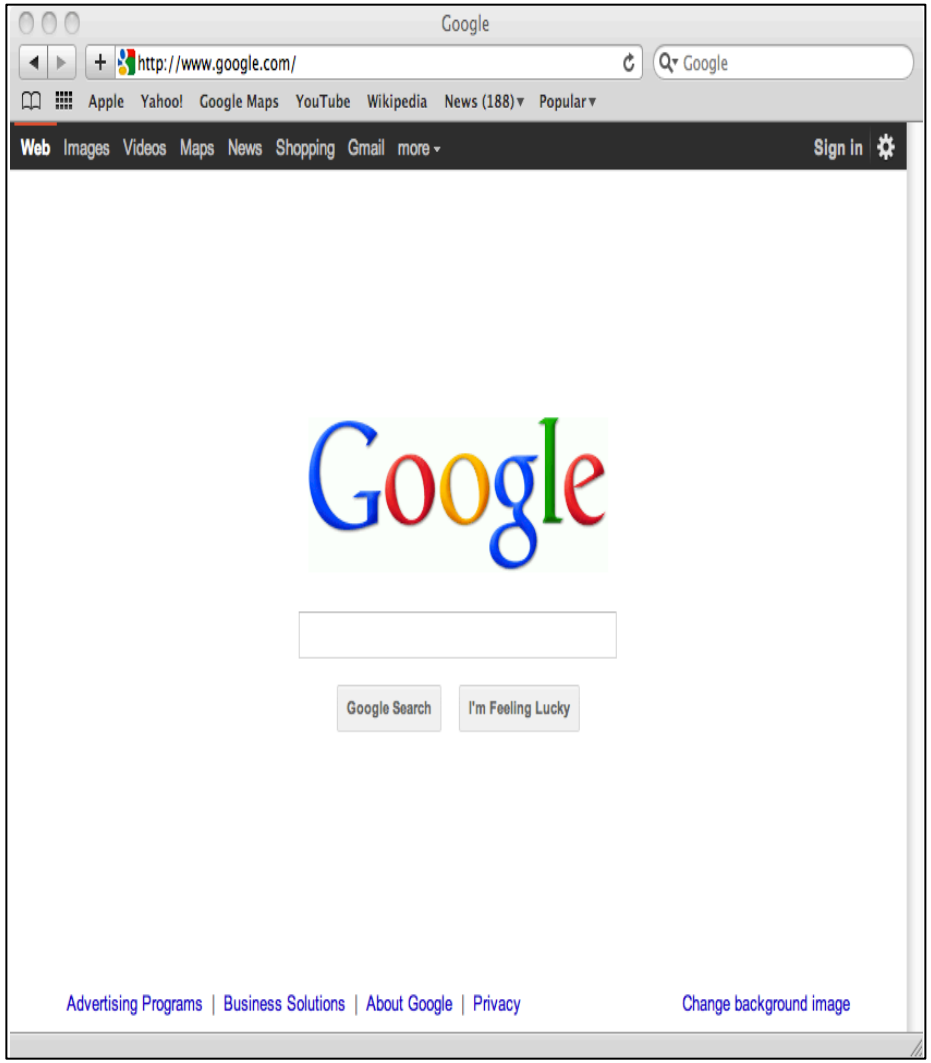

brother
Skill Level:
Easy


Price:
Cheap

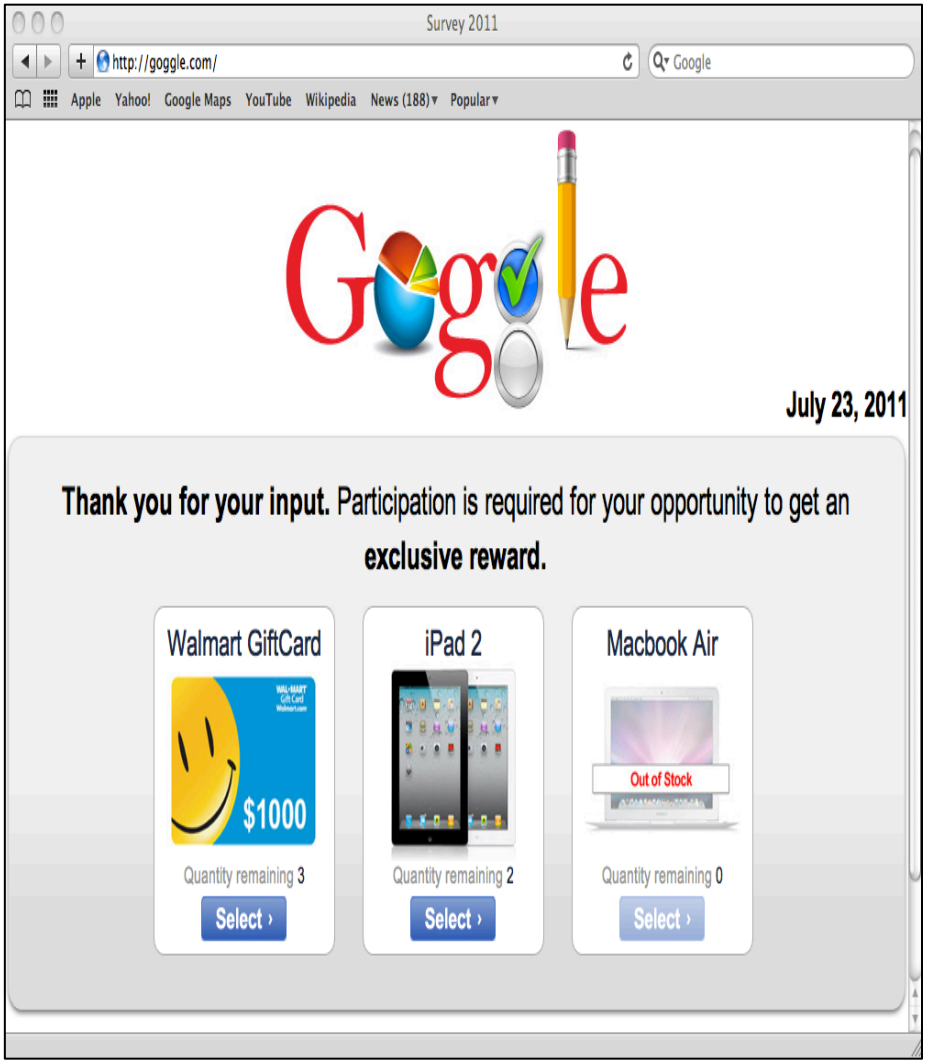
Bitsquatting

Like typosquatting, but for bits

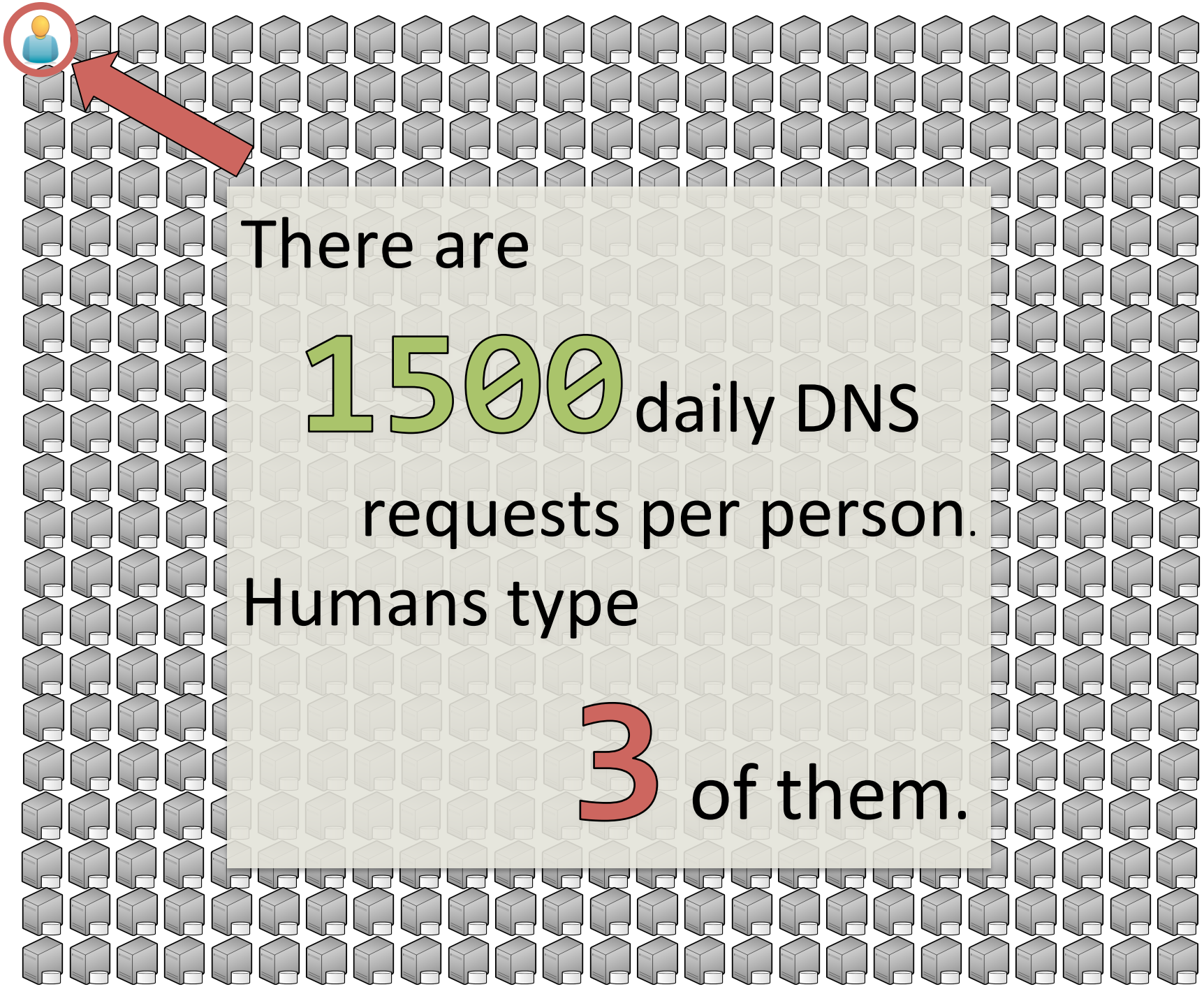
GOOGLE



GOGGLE

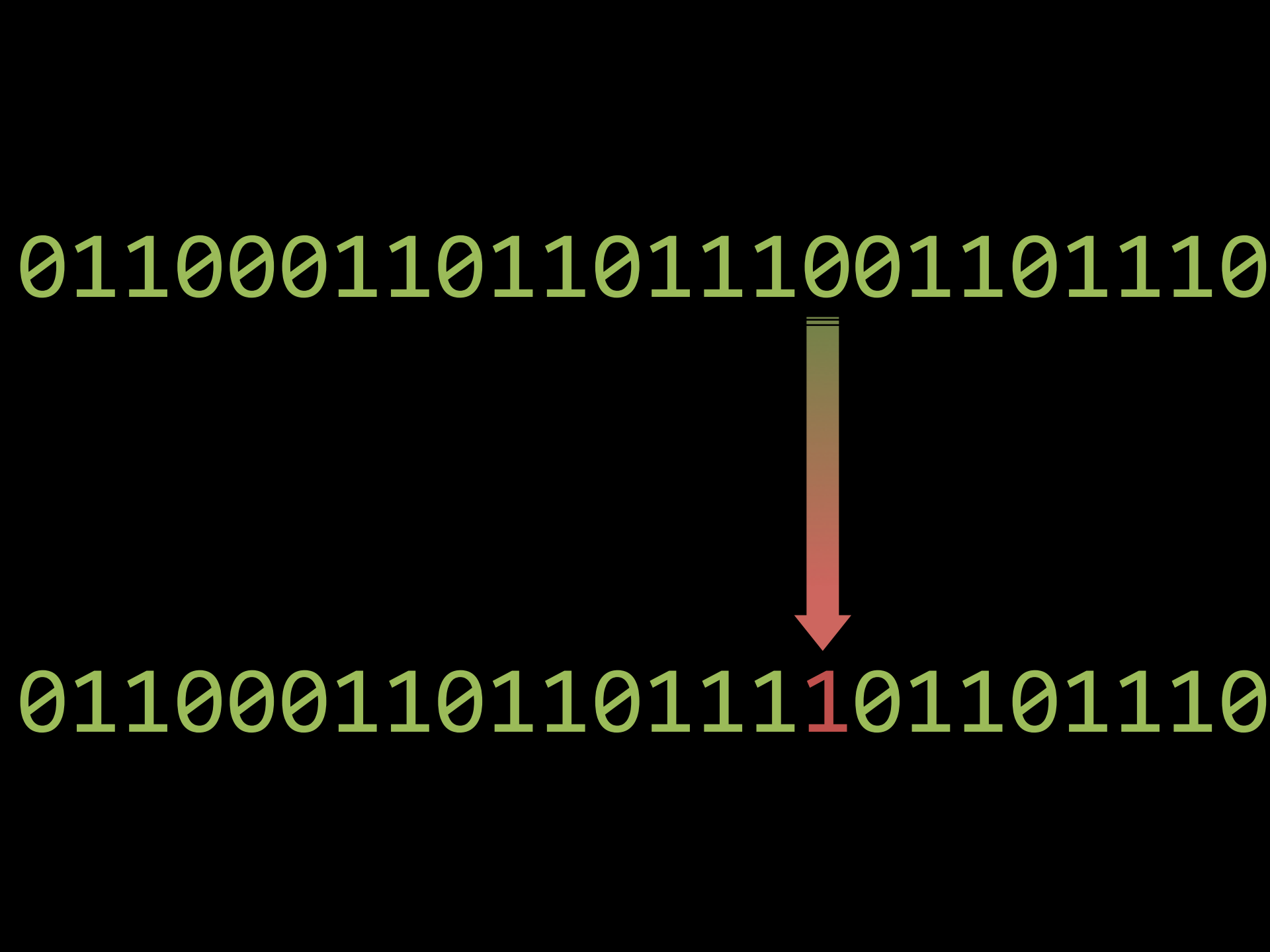


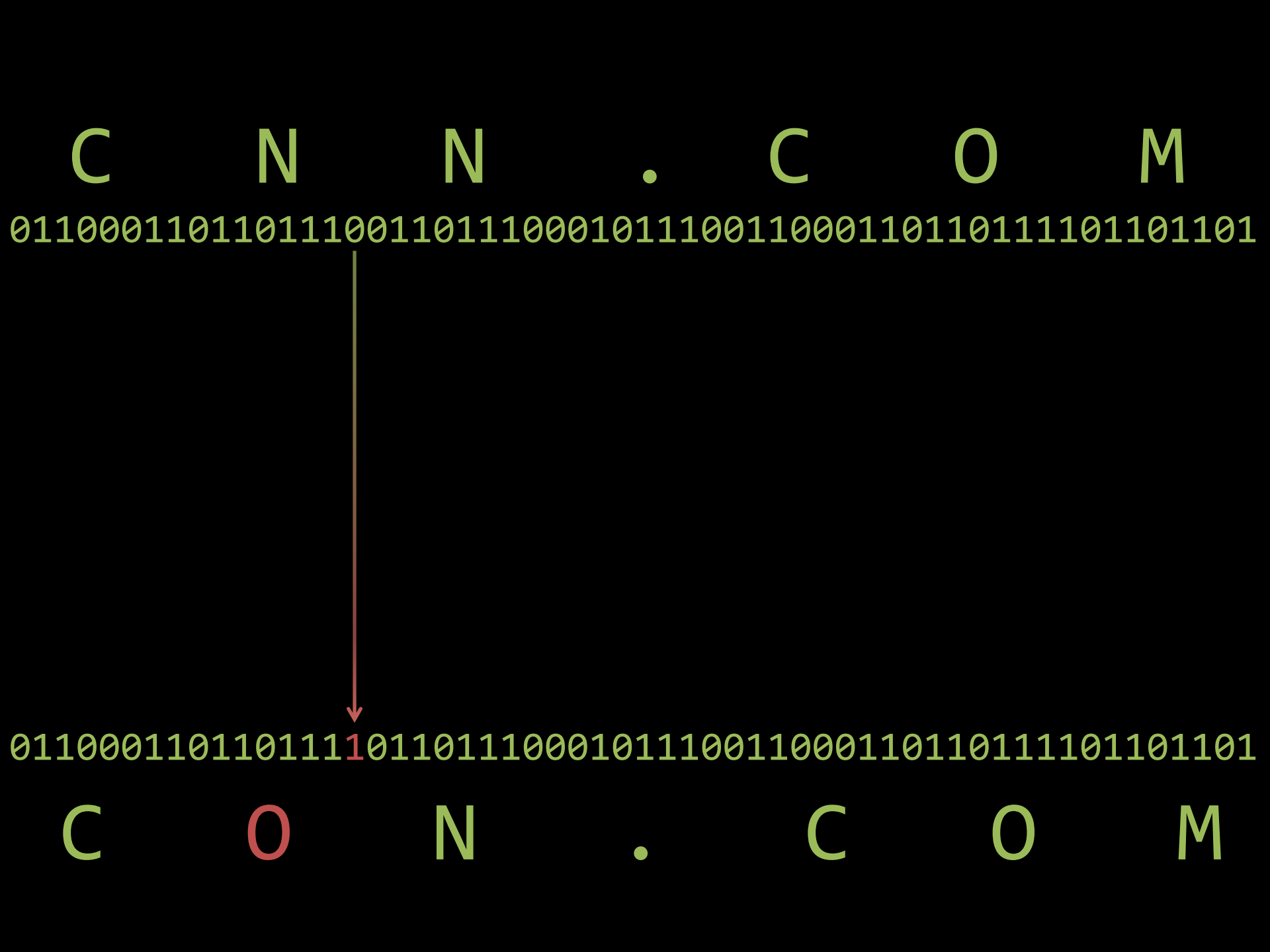

NO TYPING
Apple
Yahoo!
Google Maps
Web
Images
Videos
Maps
News
Shopping
Advertising Programs
Business Solutions
About Google
Privacy
Change background image
Google
July 23, 2011
reward.
Macbook Air
Quantity remaining 3
Quantity remaining 0
Select ›
Select ›


There are
1500 daily DNS
requests per person.
Humans type
3 of them.

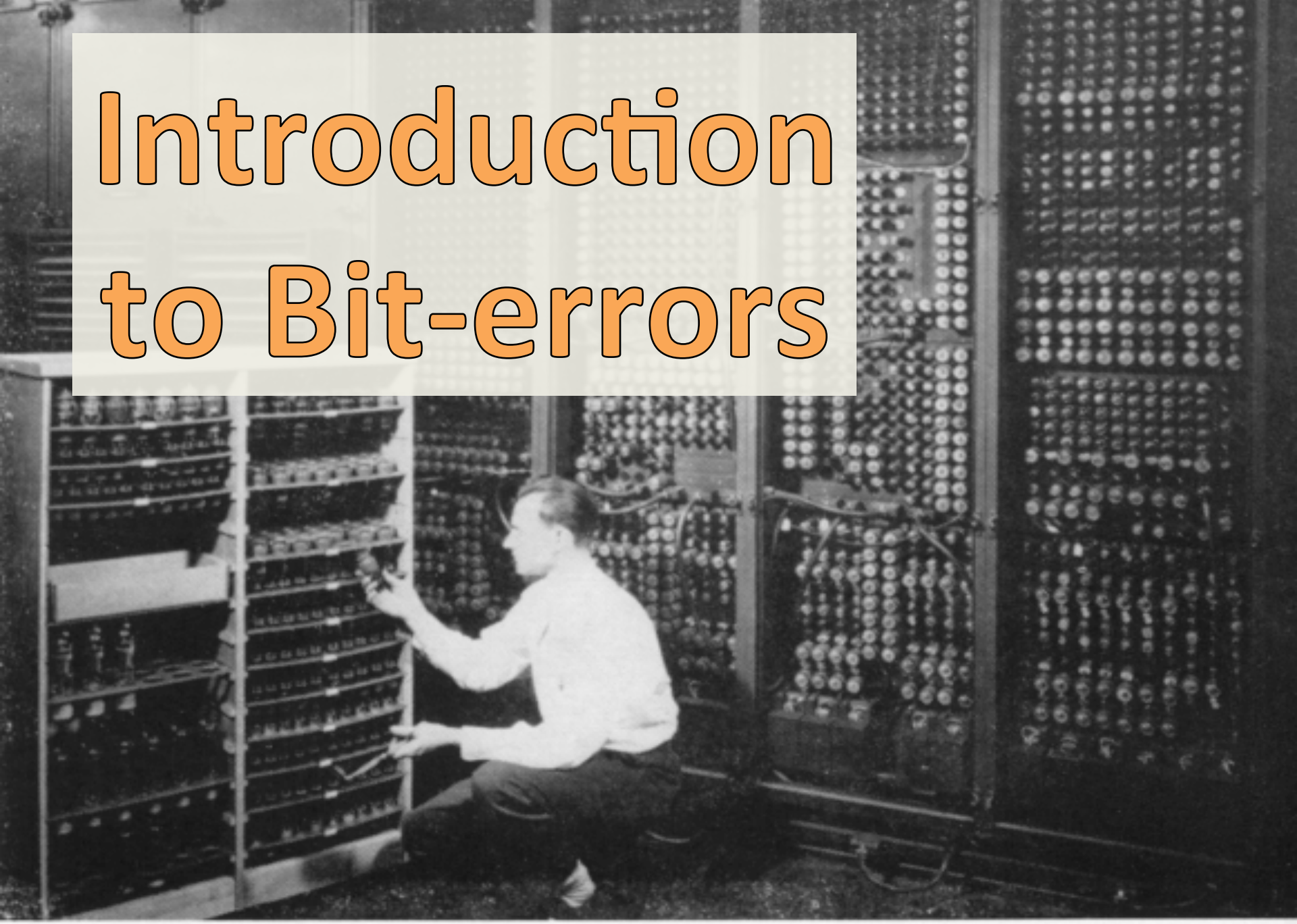
Computer Hardware Errors


1
0
0
1

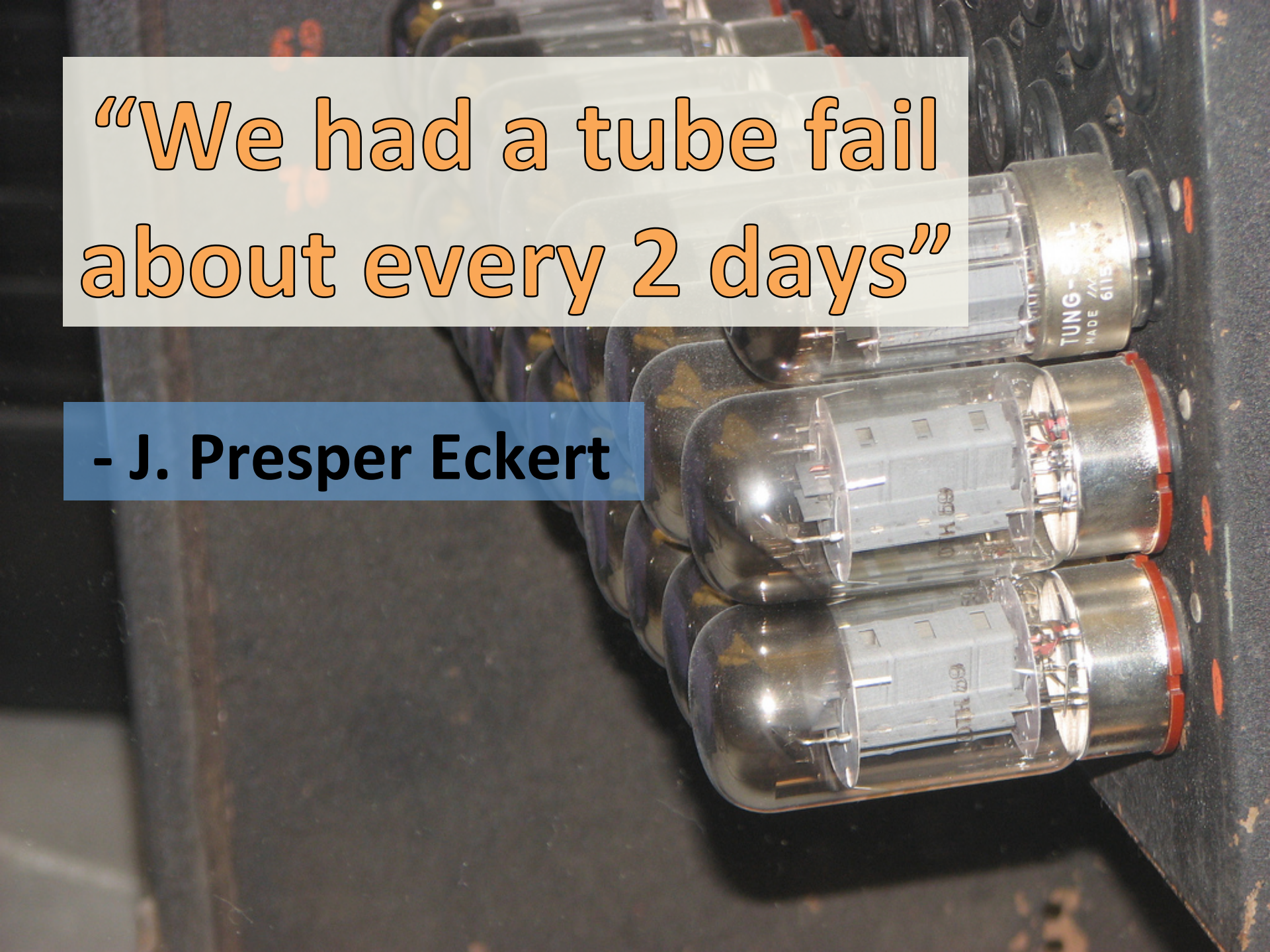

01100011011011100110111
01100011011011110110111

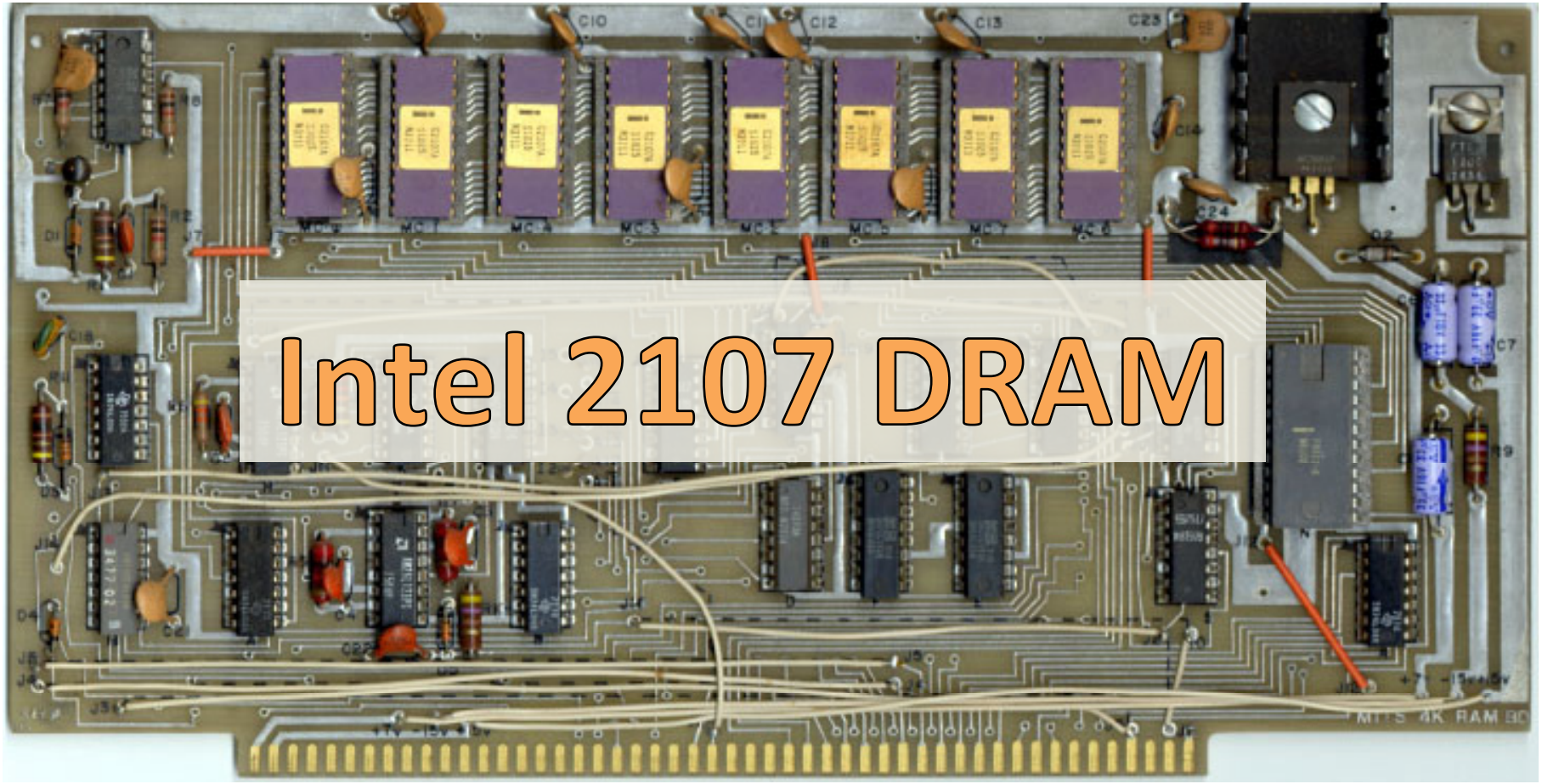

C N N . C O M
01100011011011100110111000101110011000110110111101101101
01100011011011110110111000101110011000110110111101101101
C O N . C O M

Introduction to Bit-errors



Replacing a bad tube meant checking among ENIAC's 19,000 possibilities.

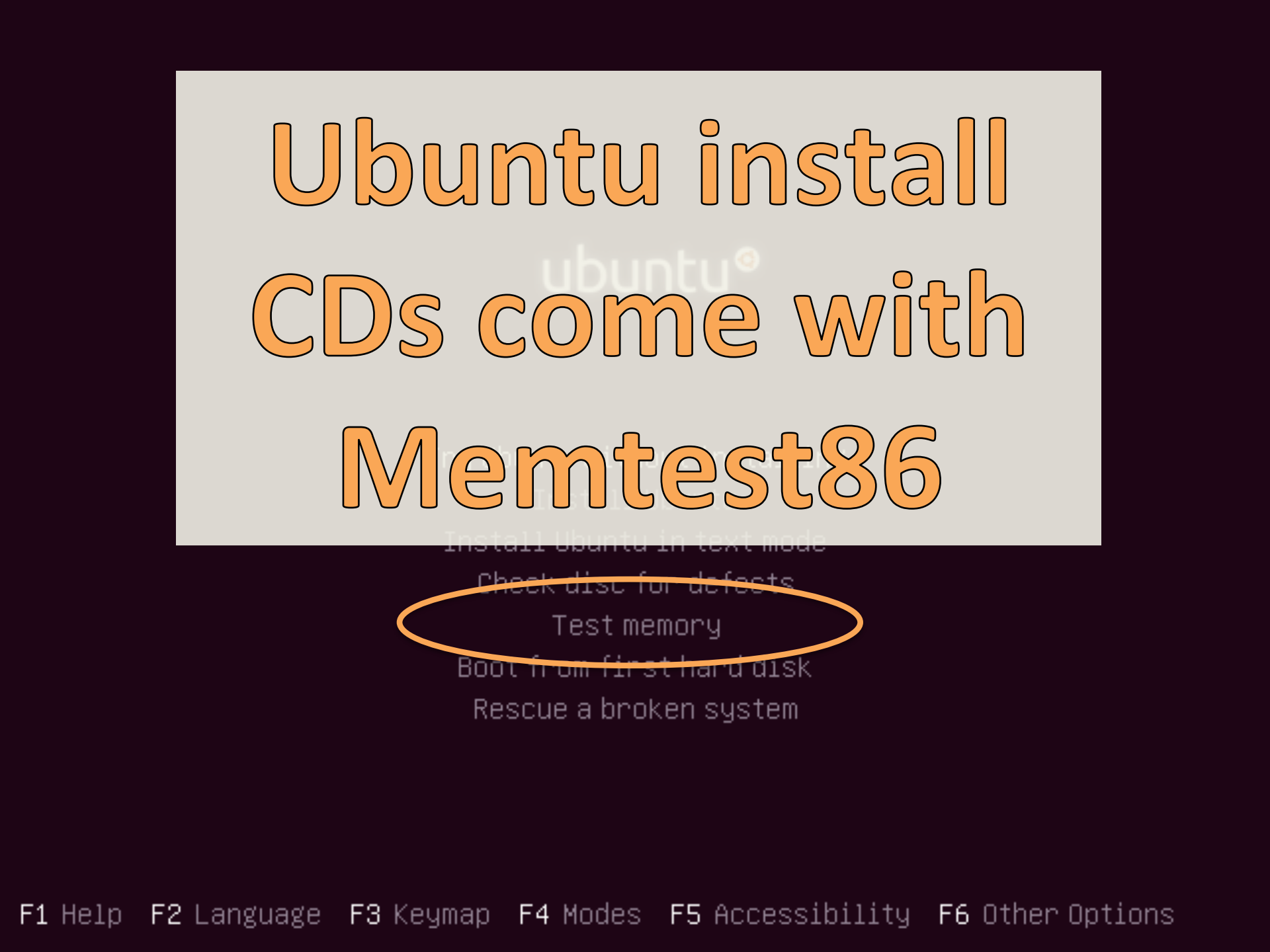

"We had a tube fail about every 2 days"
- J. Presper Eckert

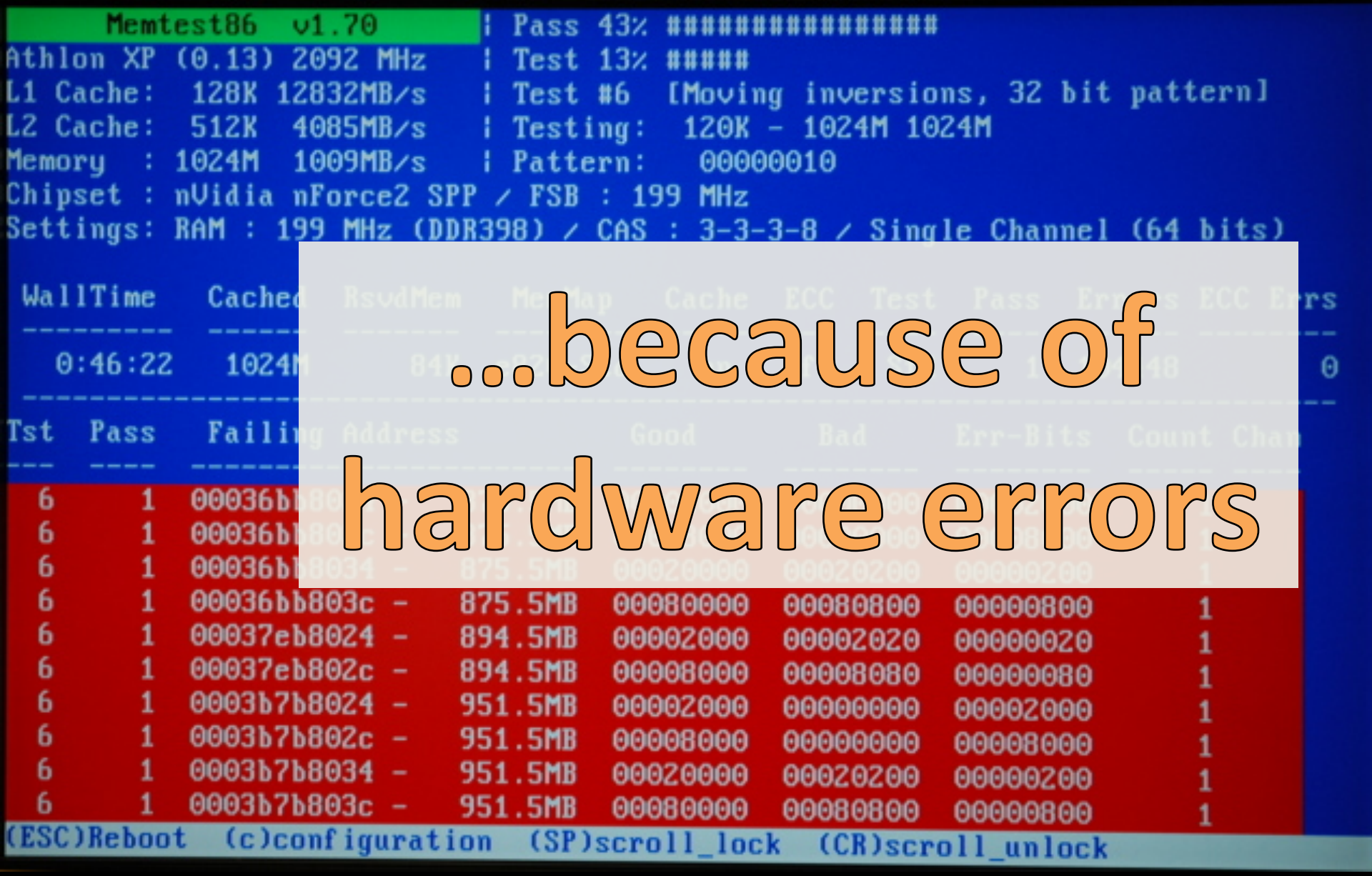


MITS Altair 8800 4K Ram Board, Rev 0 with 8 Intel C2107A DRAMs

Cache Contamination

Ubuntu install CDs come with Memtest86

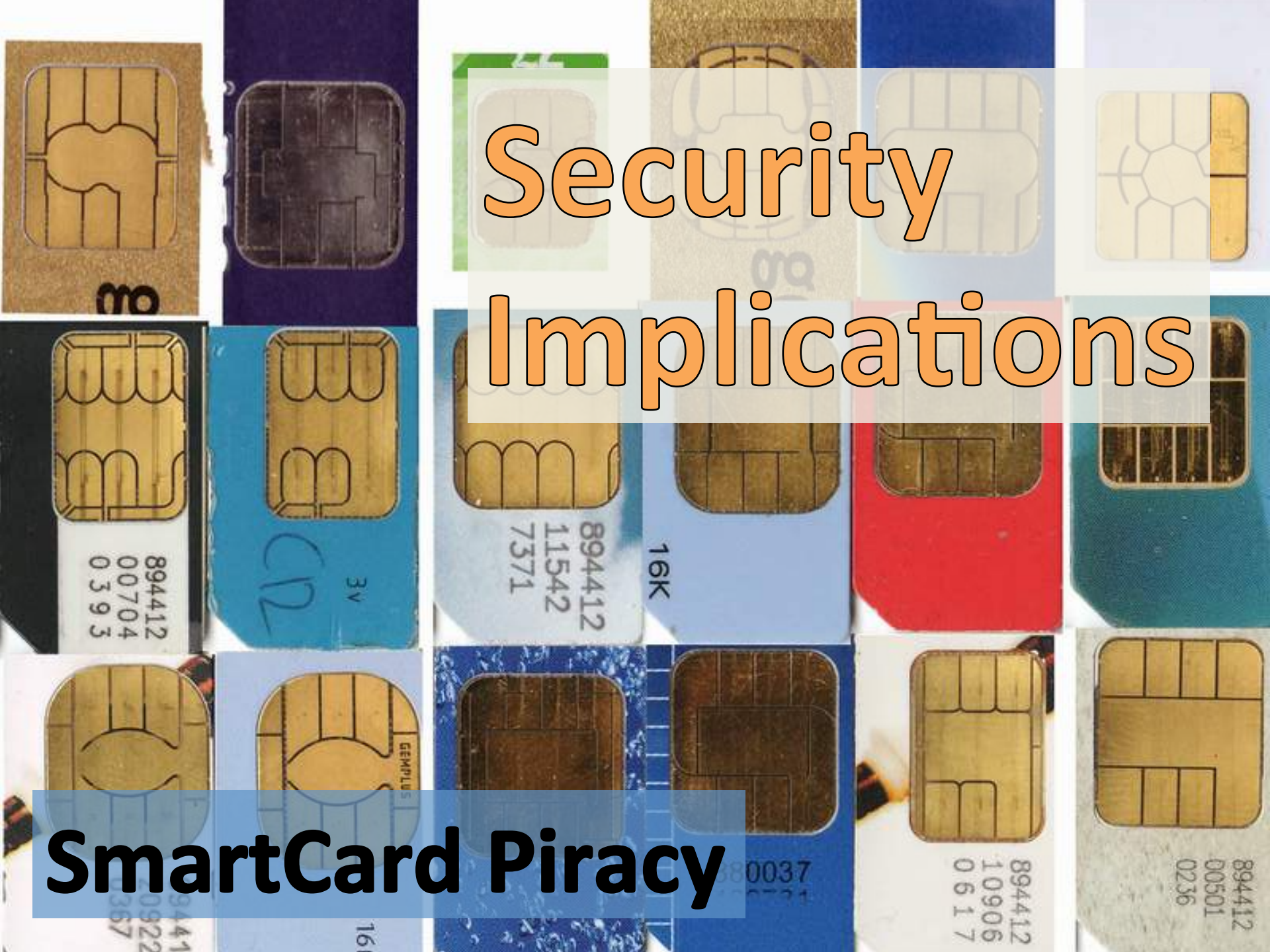


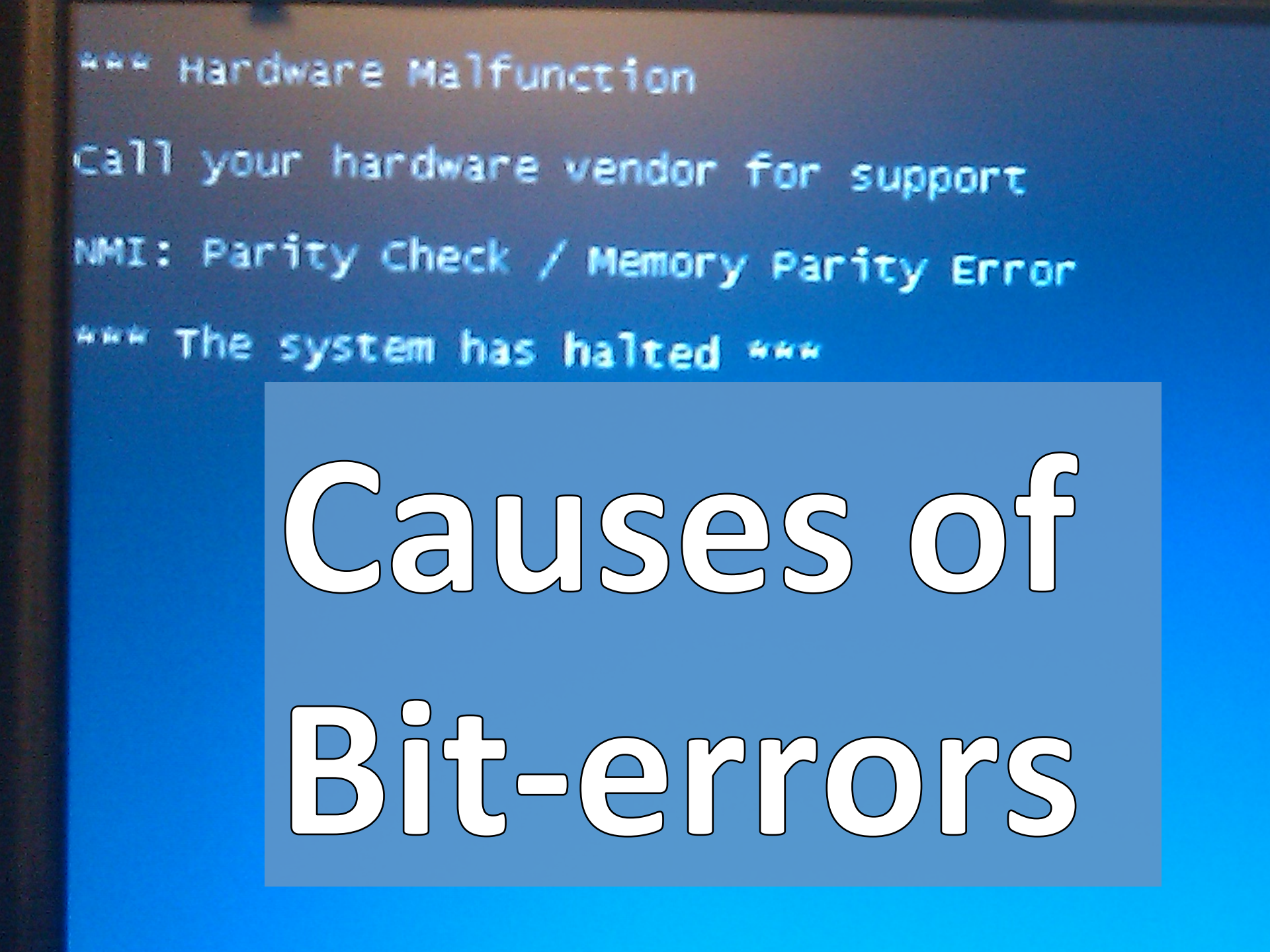


...because of hardware errors


Security
Implications


Security
Implications
JVM Sandbox Escape


Security
Implications
SmartCard Piracy


*** Hardware Malfunction
Call your hardware vendor for support
NMI: Parity Check / Memory Parity Error
*** The system has halted ***
Causes of
Bit-errors

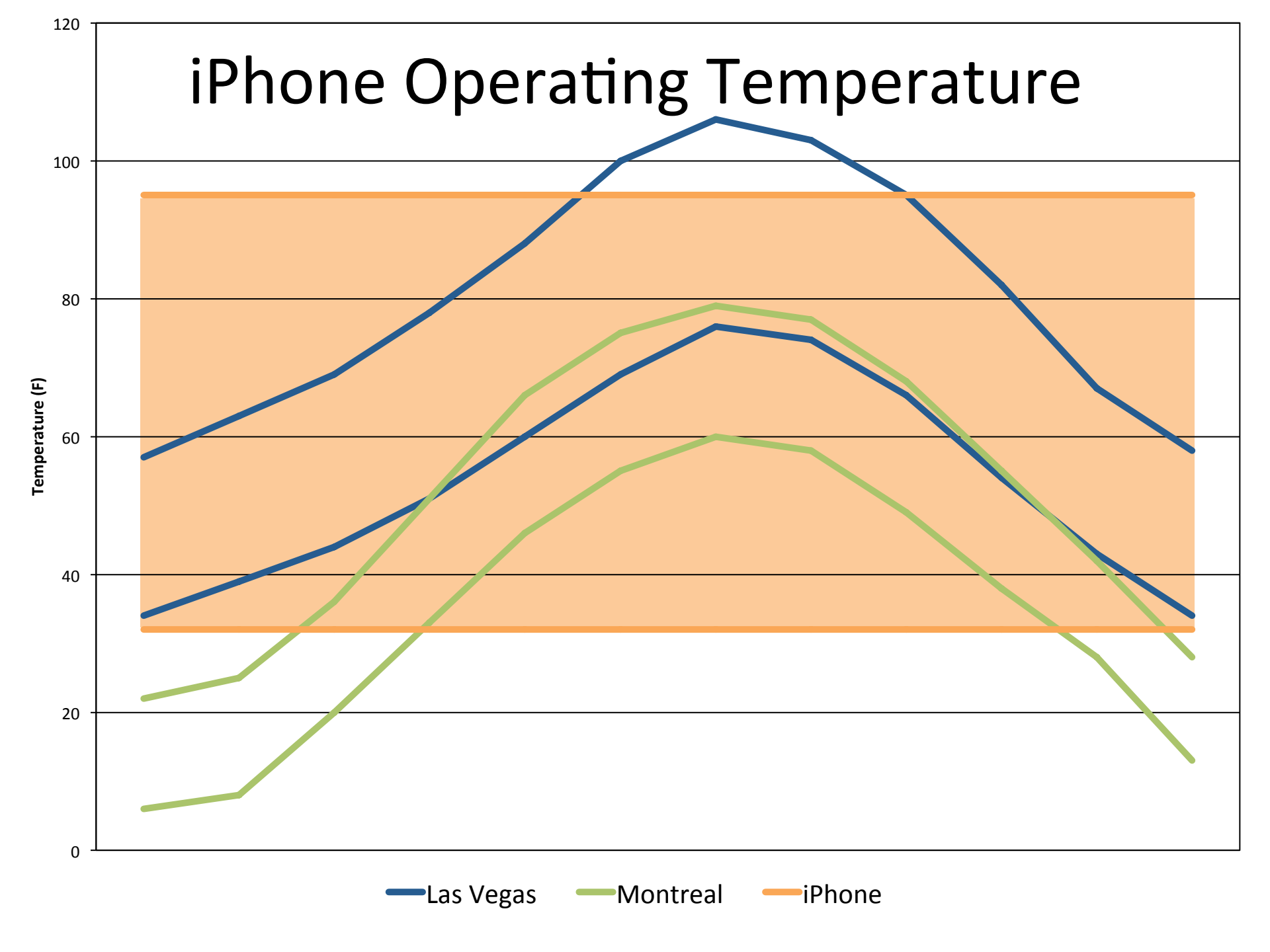
CAUSES OF BIT-ERRORS:

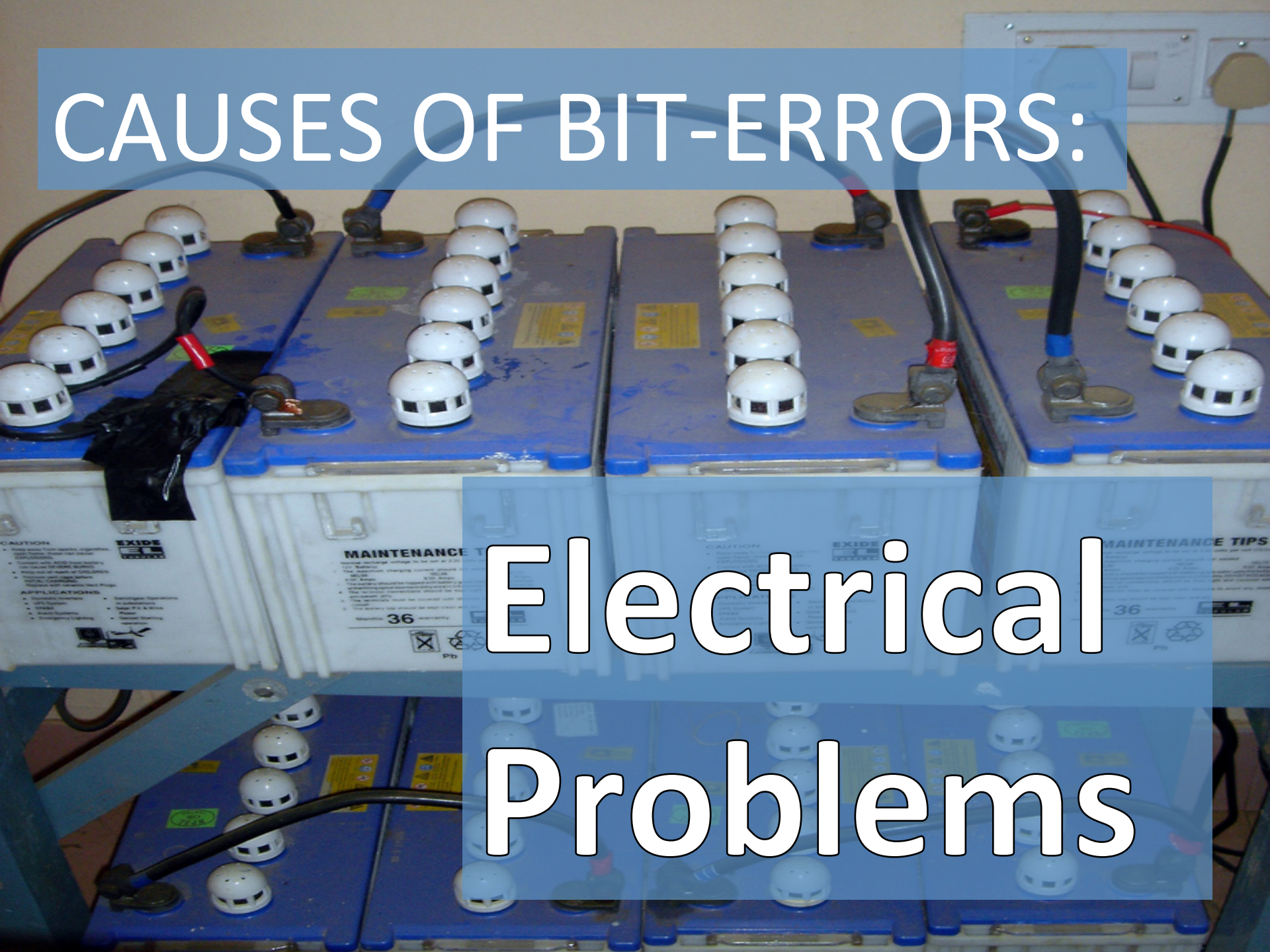
Heat

Temperature

iPhone needs to cool down
before you can use it.

Notruf


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

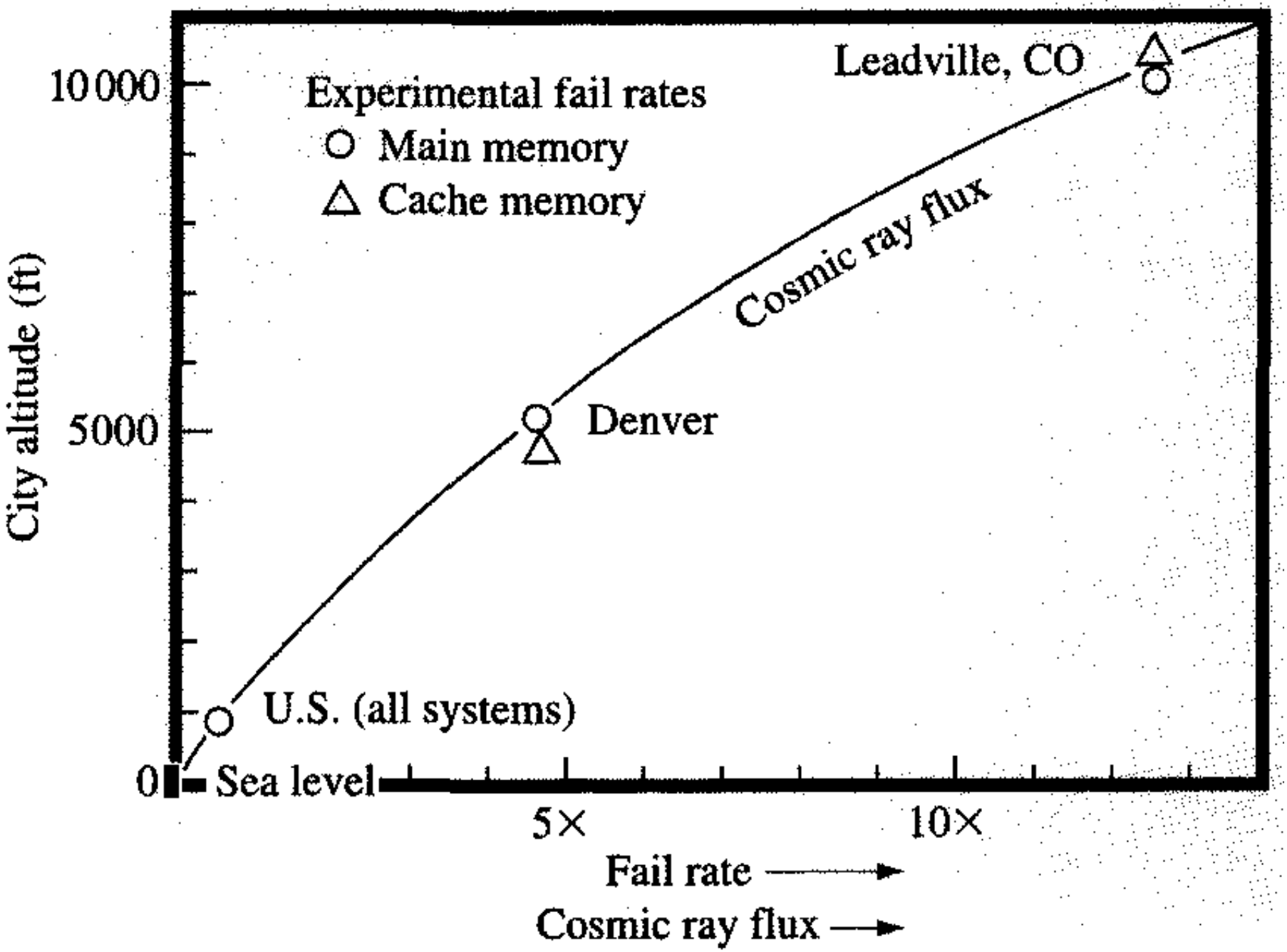

CAUSES OF BIT-ERRORS:
Electrical Problems

CAUSES OF BIT-ERRORS:

Defects

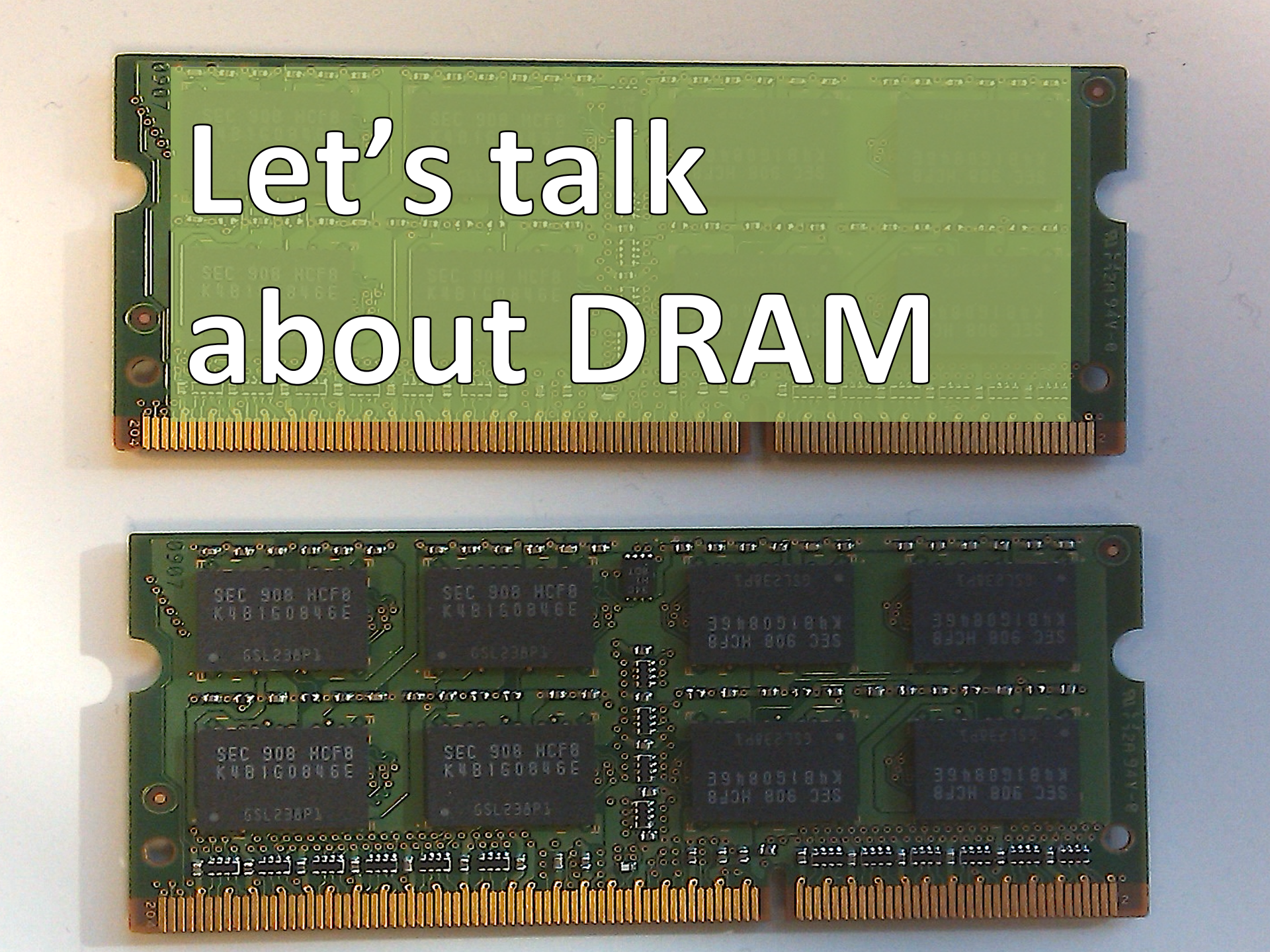
CAUSES OF BIT-ERRORS:

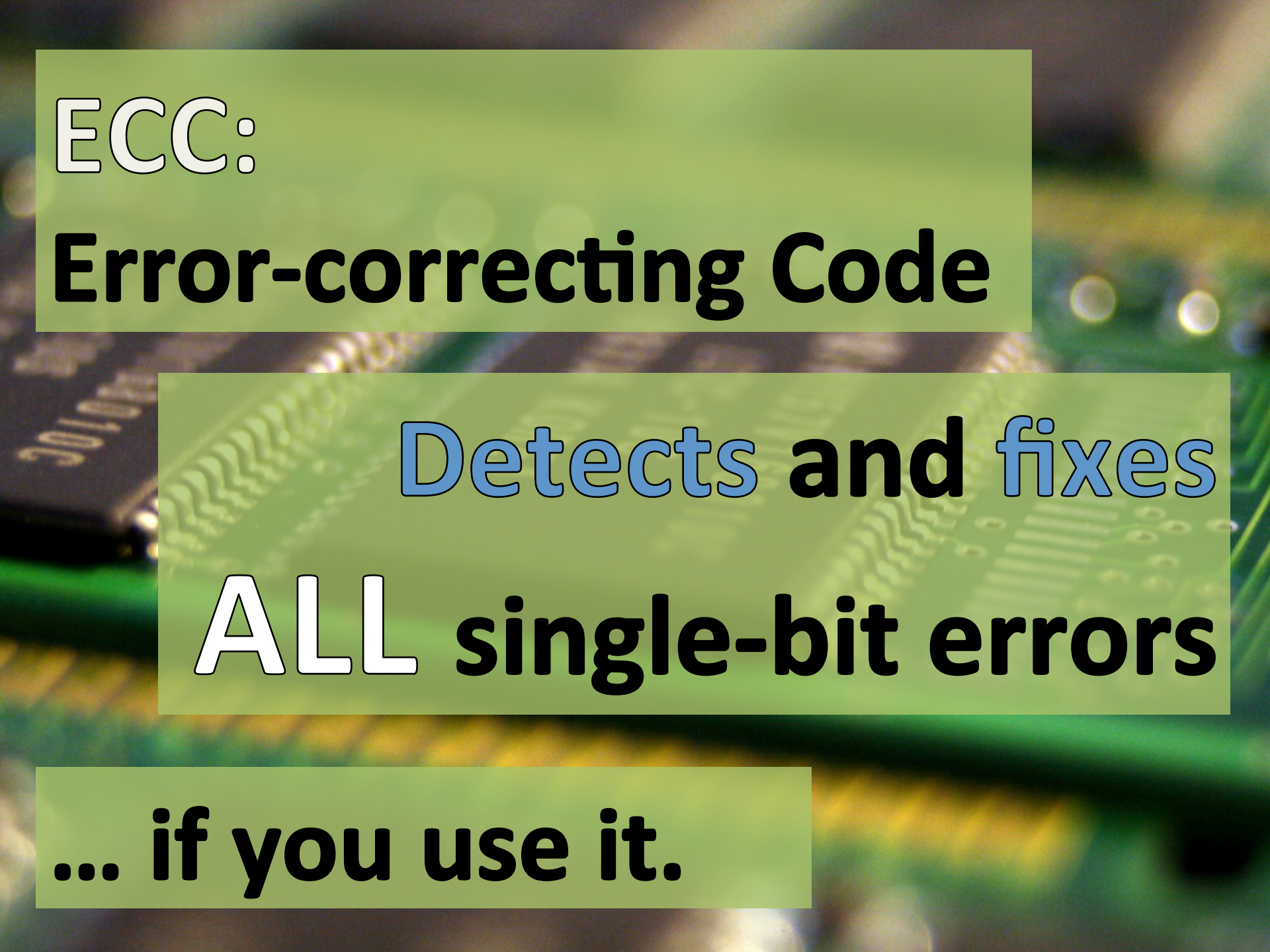
Cosmic Rays

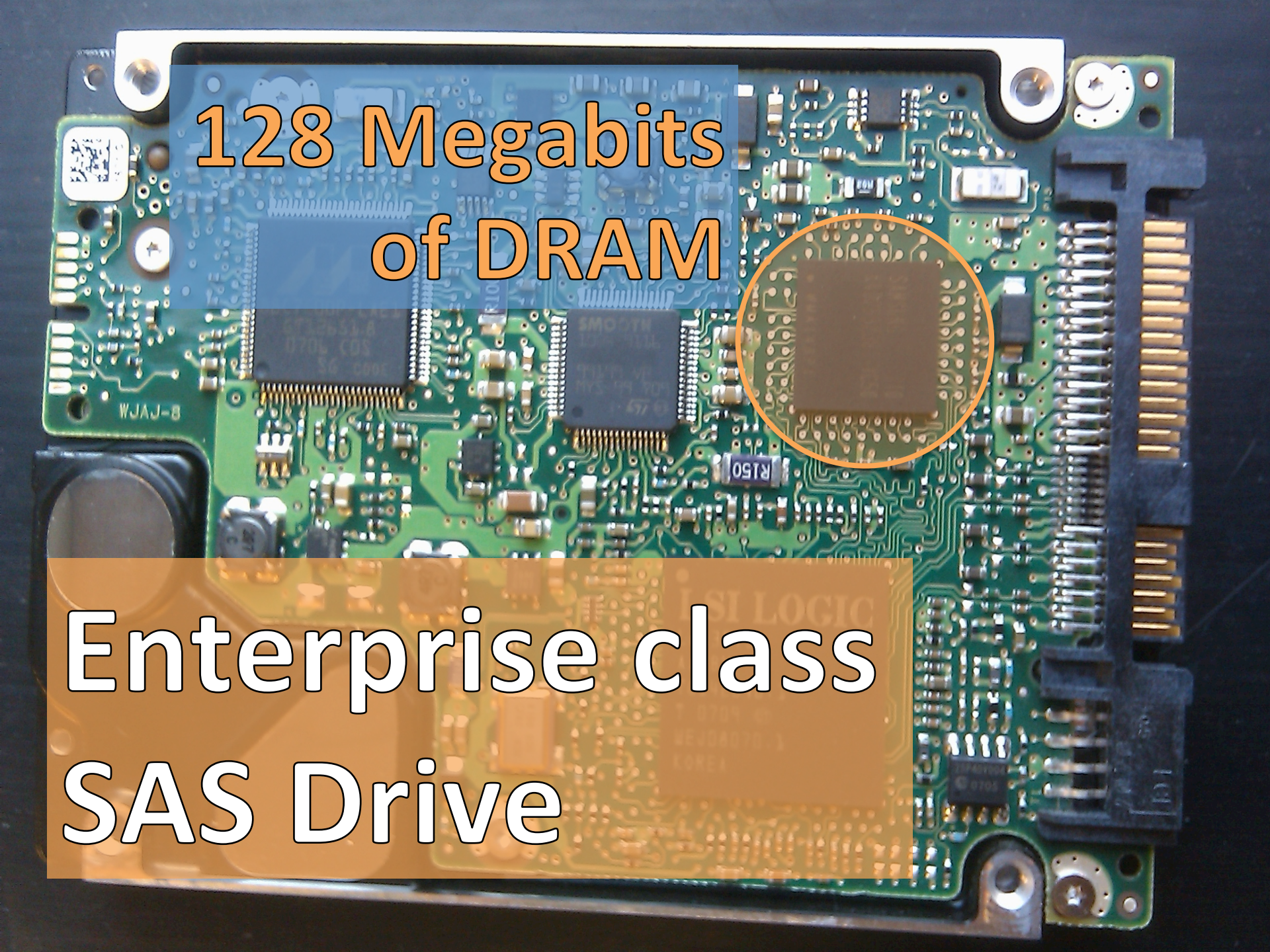


IBM Journal of Research and Development, vol. 40, no. 1, page 13

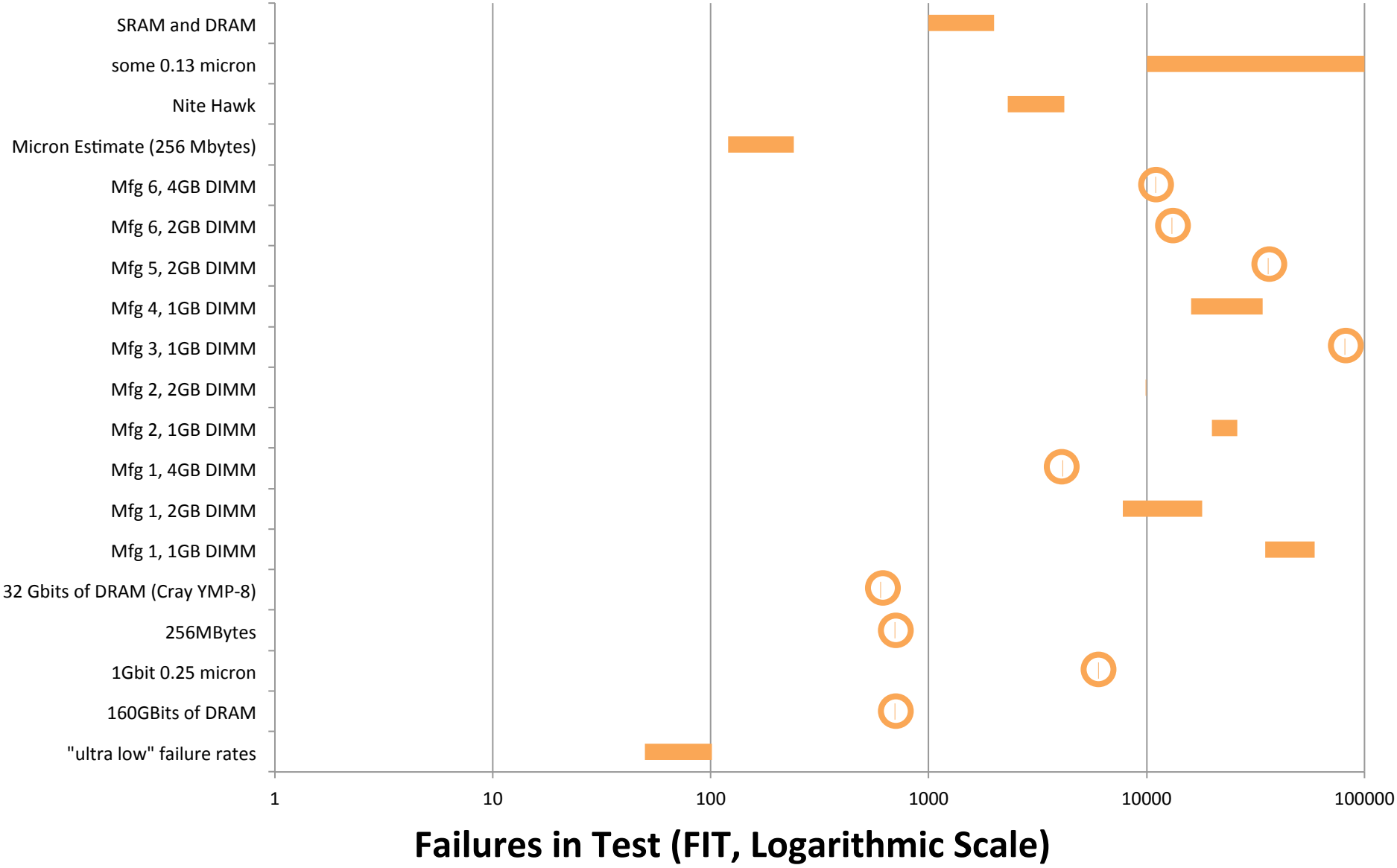

What's the
real cause?

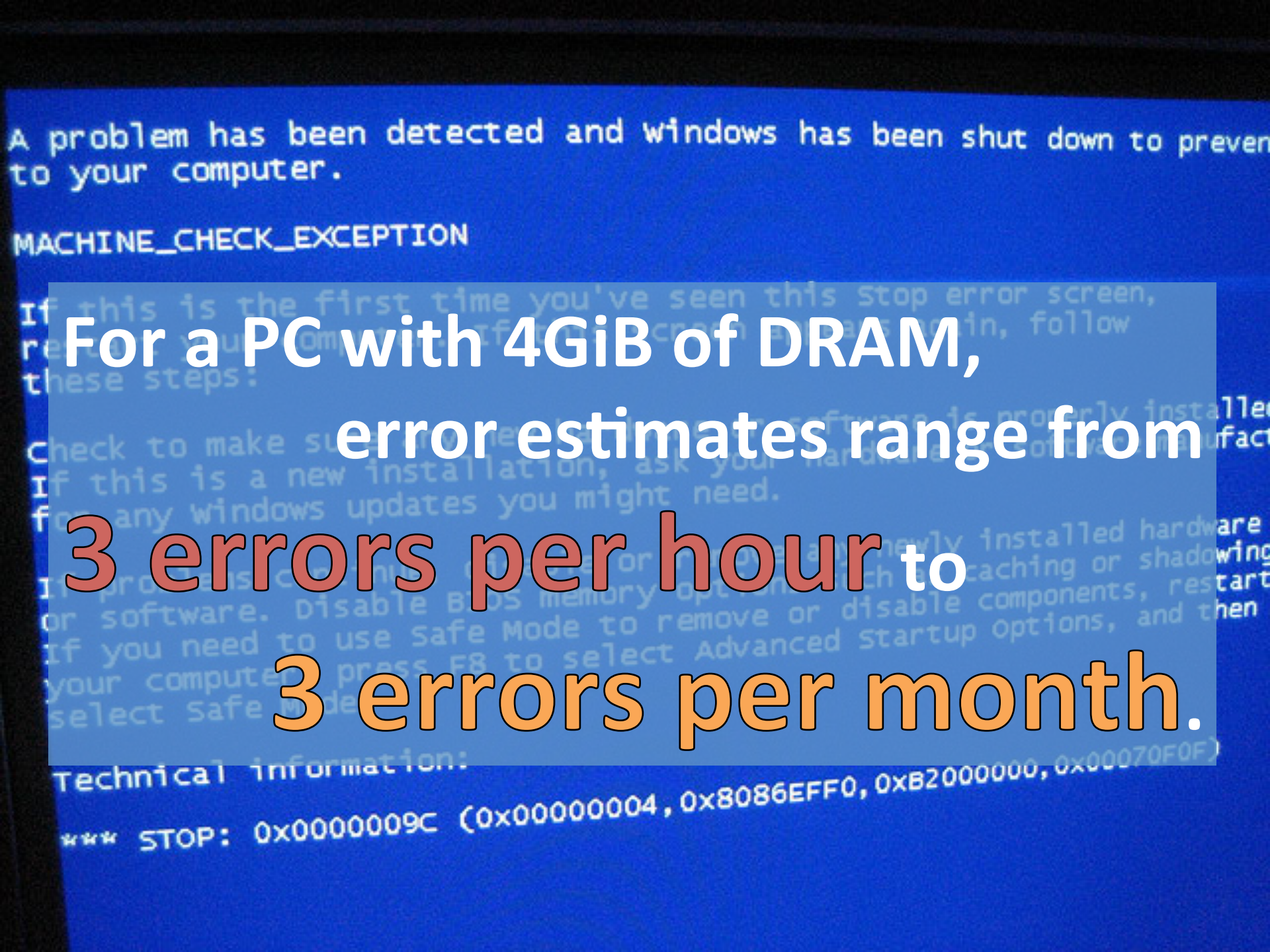

Let’s talk
about DRAM


ECC:
Error-correcting Code
Detects and fixes
ALL single-bit errors
... if you use it.

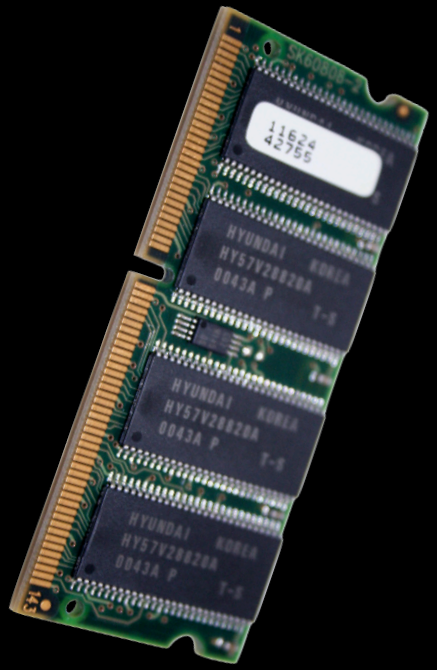

128 Megabits
of DRAM
Enterprise class
SAS Drive

DRAM Failure Rates



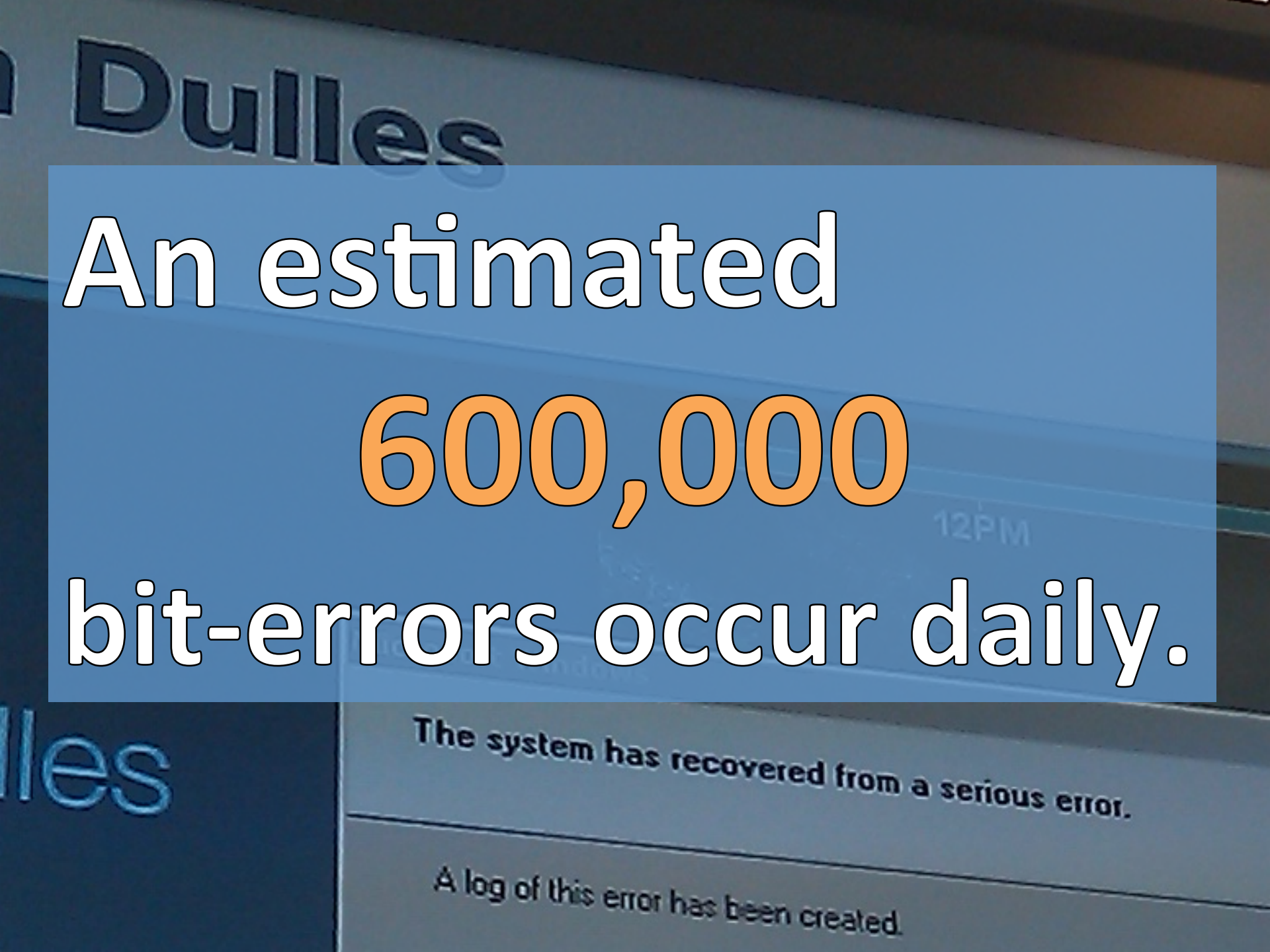

A problem has been detected and windows has been shut down to preven
to your computer.
MACHINE_CHECK_EXCEPTION
For a PC with 4GiB of DRAM,
error estimates range from
3 errors per hour to
3 errors per month.
Technical information:
*** STOP: 0x0000009C (0x00000004,0x8086EFF0,0xB2000000,0x

×


HYUNDAI
HY57V28820A
HYUNDAI
HY57V28820A
HYUNDAI
HY57V28820A

=

600 PiB


Dulles
An estimated
600,000
bit-errors occur daily.
The system has recovered from a serious error.
A log of this error has been created.


KEEP OUT
EXPERIMENT
IN
PROGRESS

Experiment: Step 1

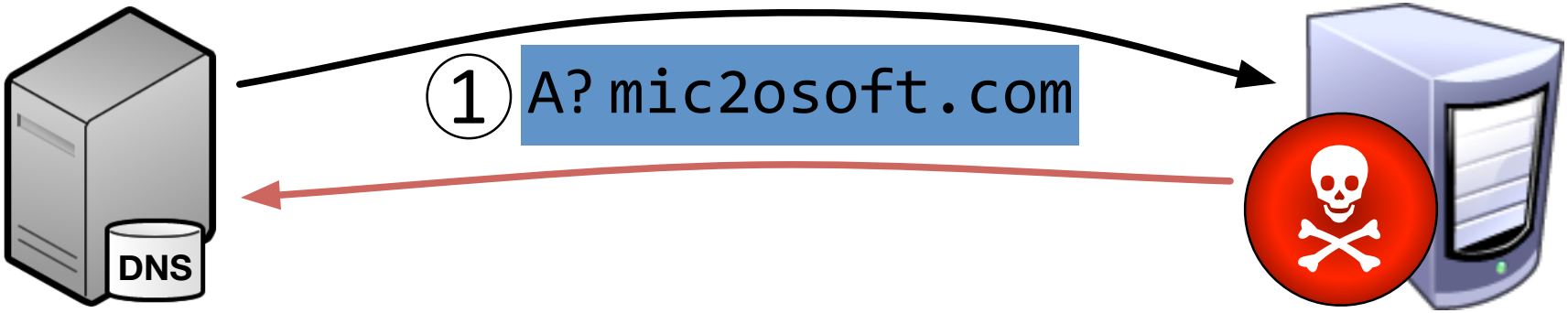
ikamai.net
aeazon.com
a-azon.com
amazgn.com
microsmft.com
micrgsoft.com
miarosoft.com
iicrosoft.com
microsnft.com
mhcrosoft.com
eicrosoft.com
mic2osoft.com
micro3oft.com
doublechick.net
do5bleclick.net
doubleslick.net

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

1 A? mic2osoft.com

Experiment: Step 2

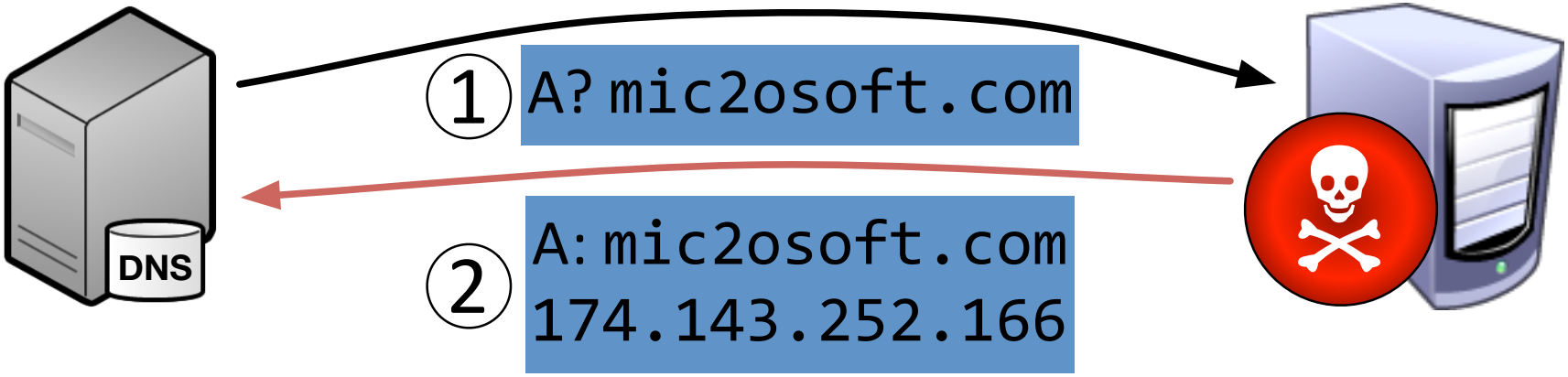


2

A: mic2osoft.com

174.143.252.166

Experiment: Step 2



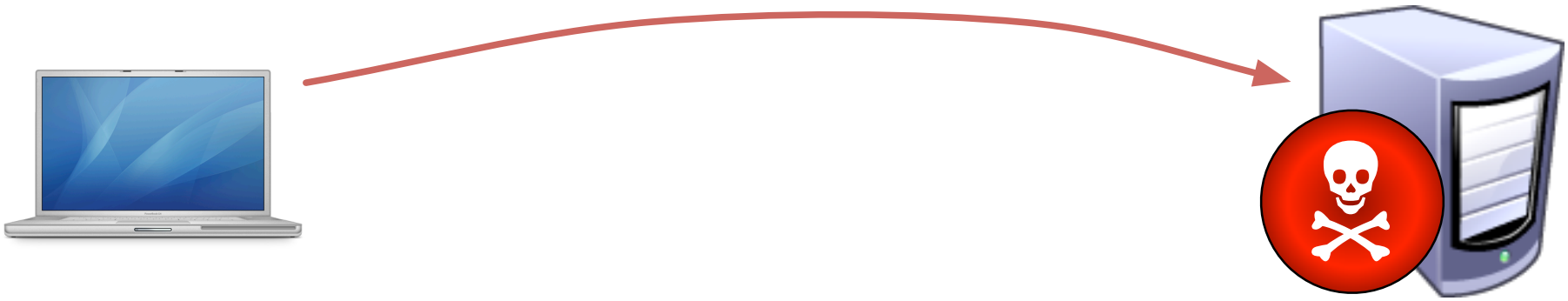
3

A: microsoft.com

174.143.252.166

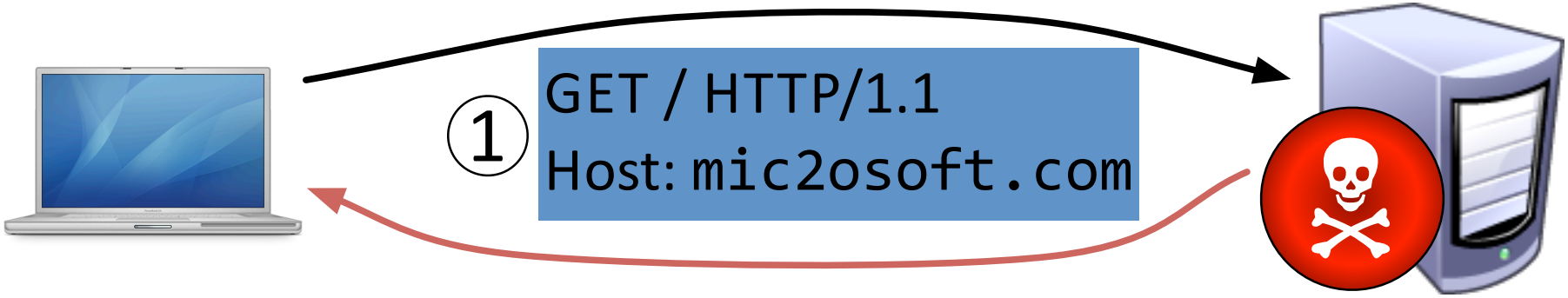
Experiment: Step 2

Experiment: Step 3



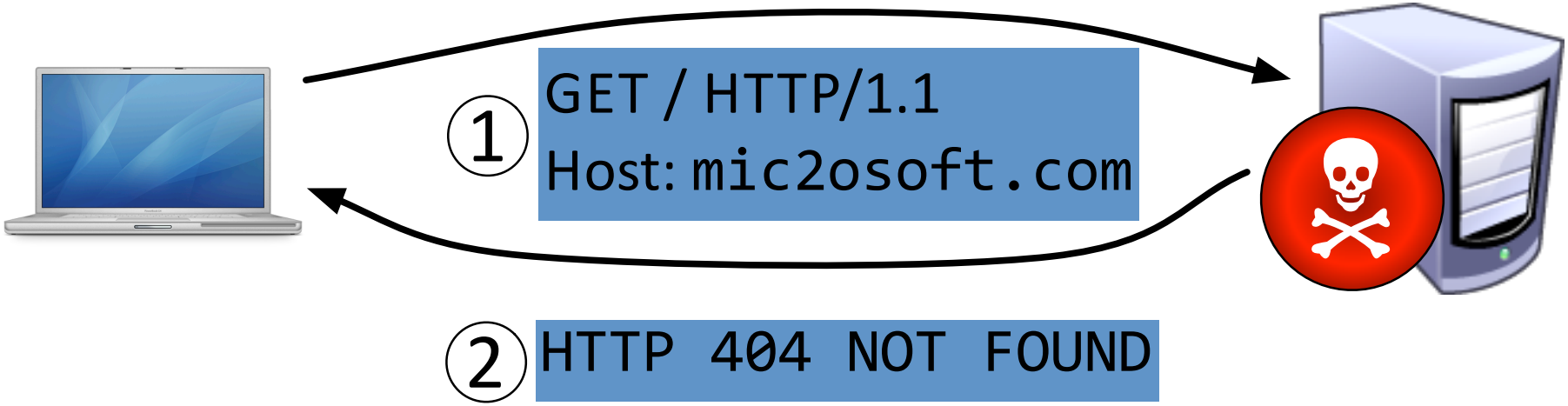
① GET / HTTP/1.1
Host: mic2osoft.com

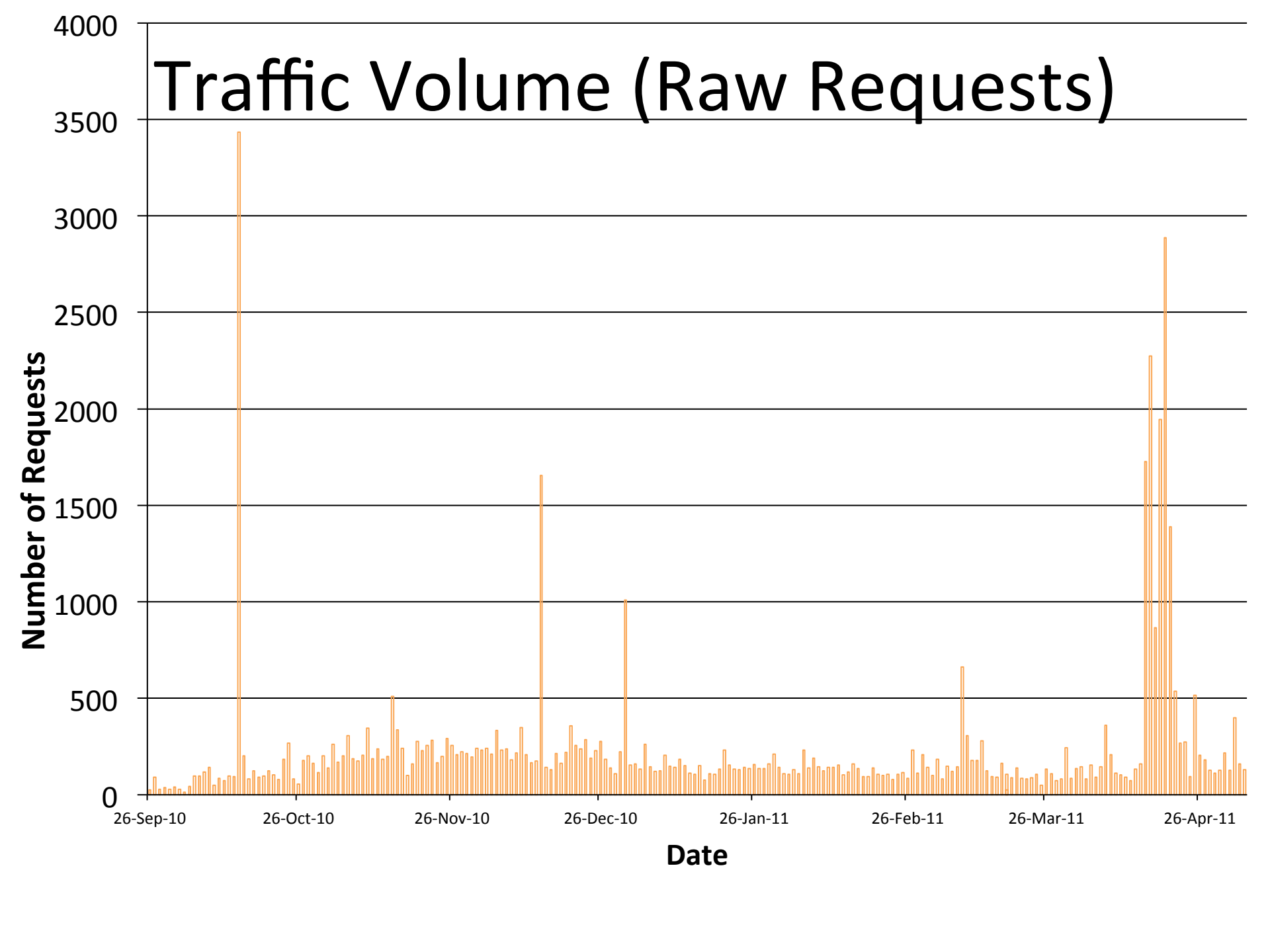
Experiment: Step 3

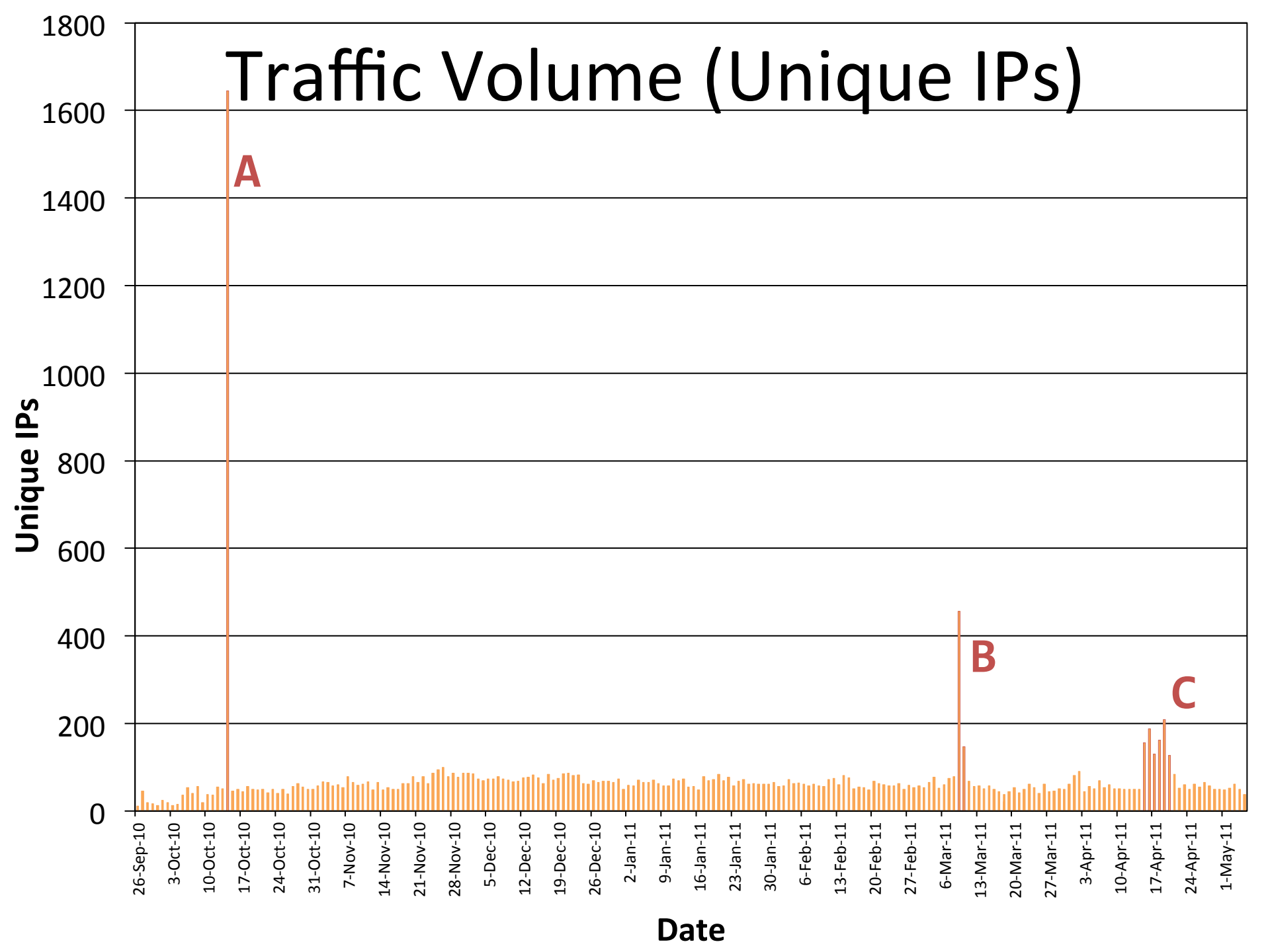


② HTTP 404 NOT FOUND

Experiment: Step 3



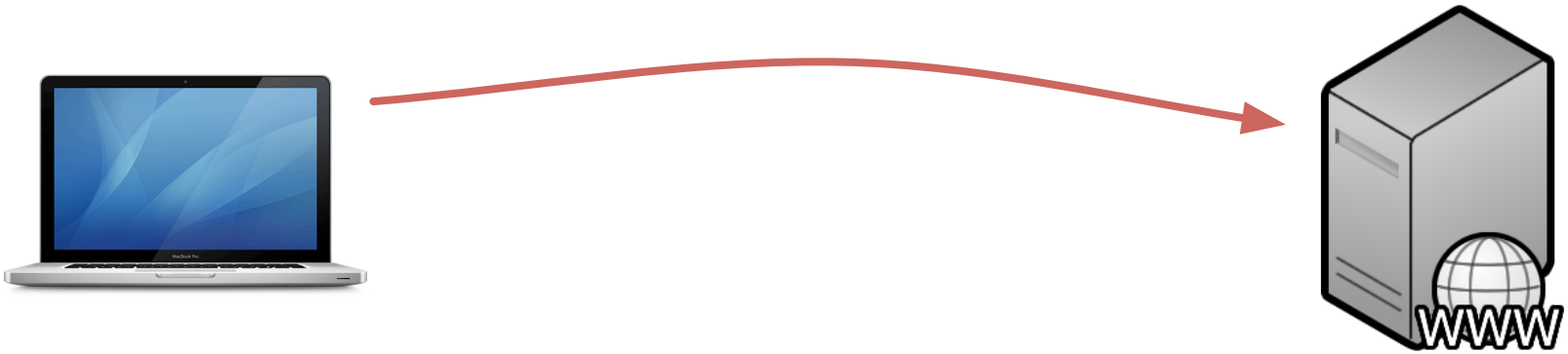

Traffic Volume (Raw Requests)
4000
3500
3000
2500
2000
1500
1000
500
0
Number of Requests
26-Sep-10
26-Oct-10
26-Nov-10
26-Dec-10
26-Jan-11
26-Feb-11
26-Mar-11
26-Apr-11
Date


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

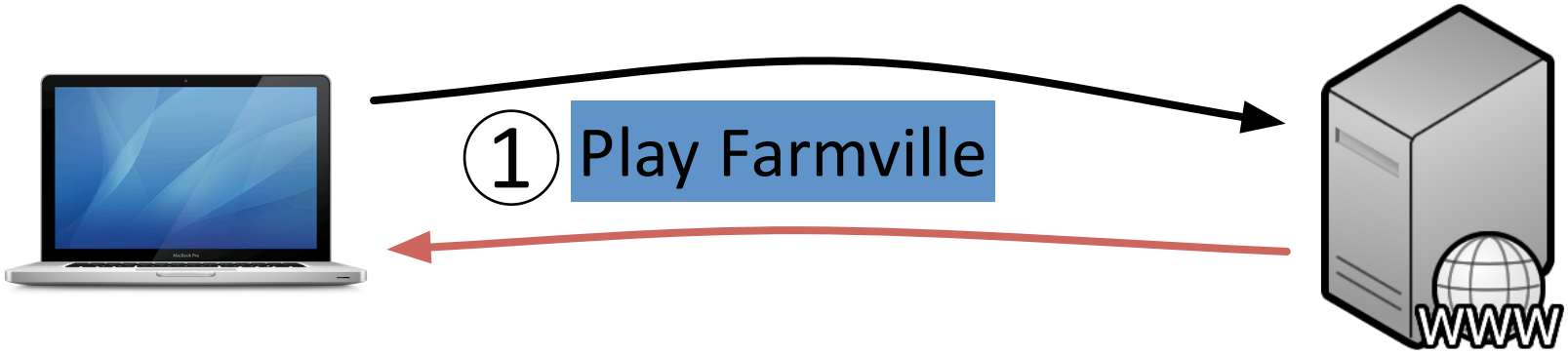
Event A

1300

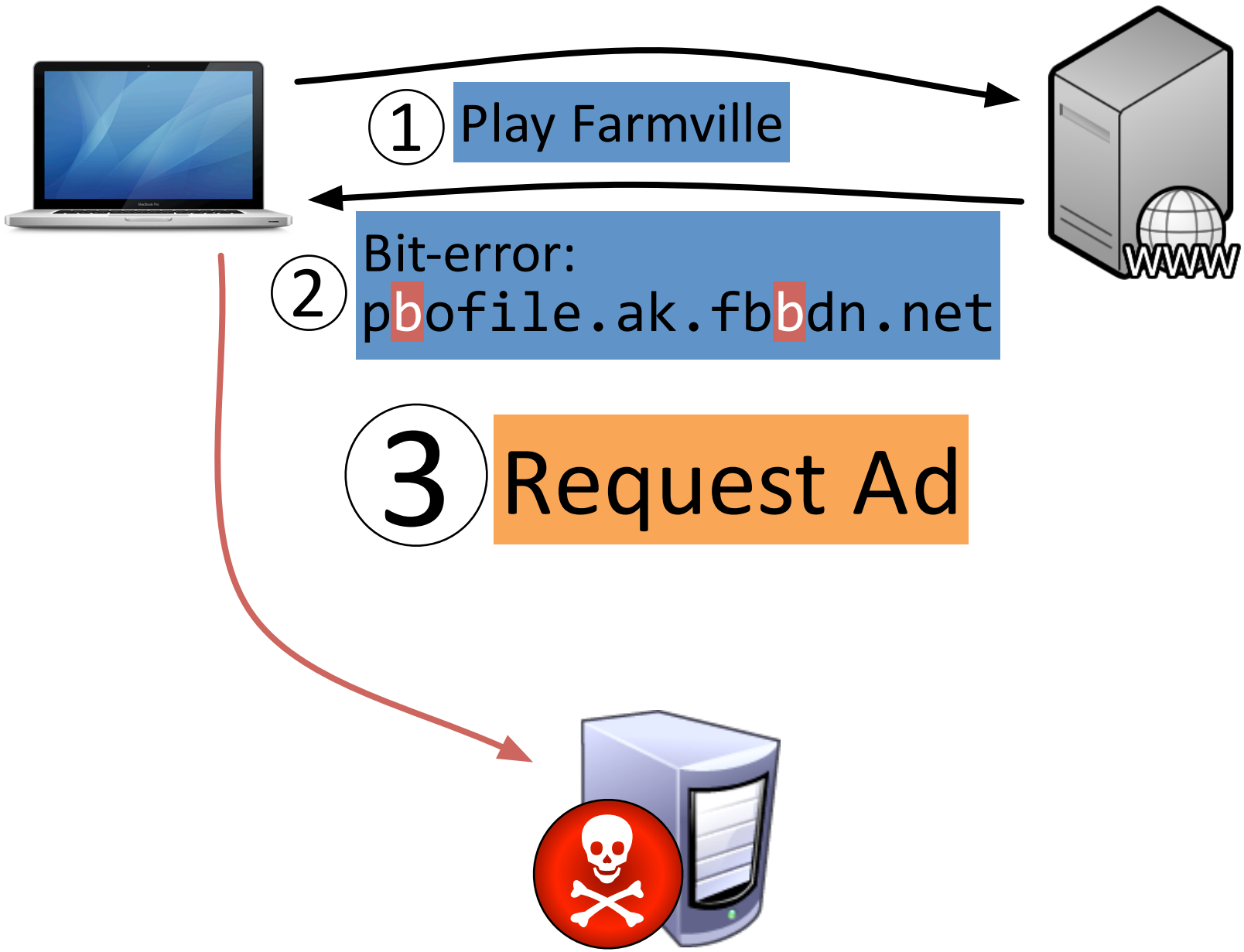
Unique IPs

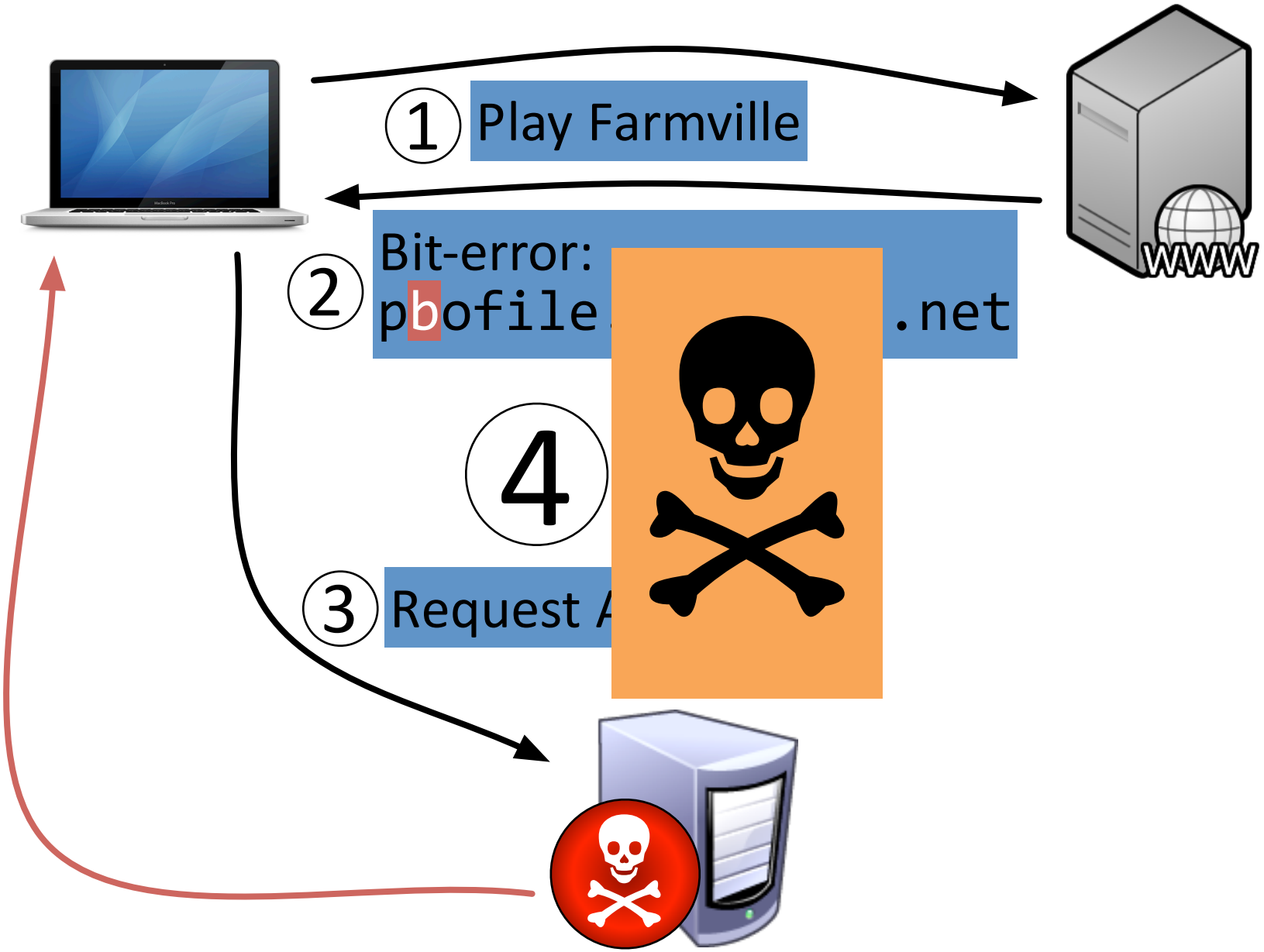


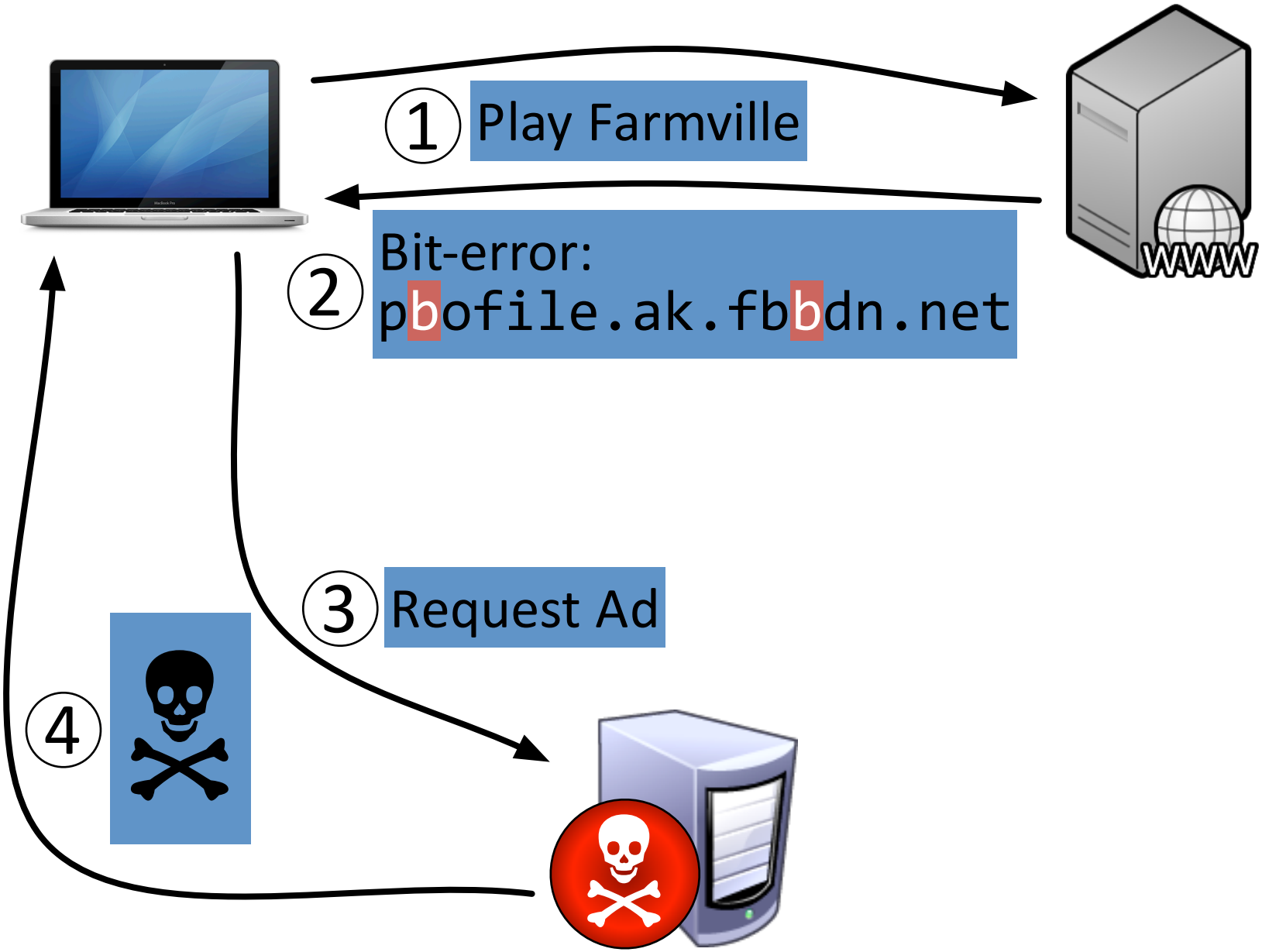
1 Play Farmville



② Bit-error:
pbofile.ak.fbbdn.net


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

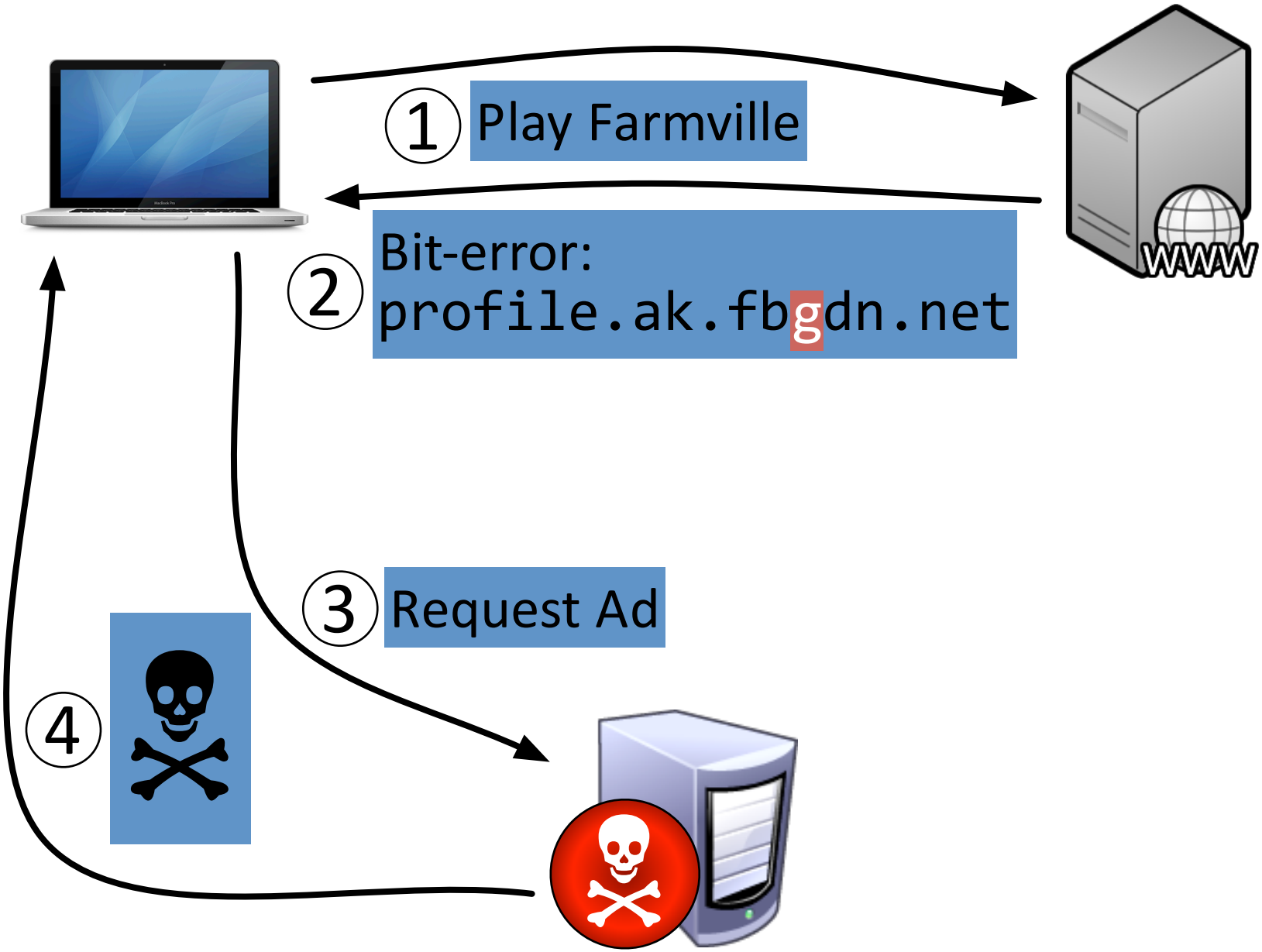

1 Play Farmville
WWW
2 Bit-error:
pbofile
.net
4
3 Request A


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

Event B

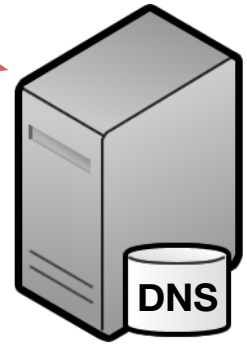
156

Unique IPs

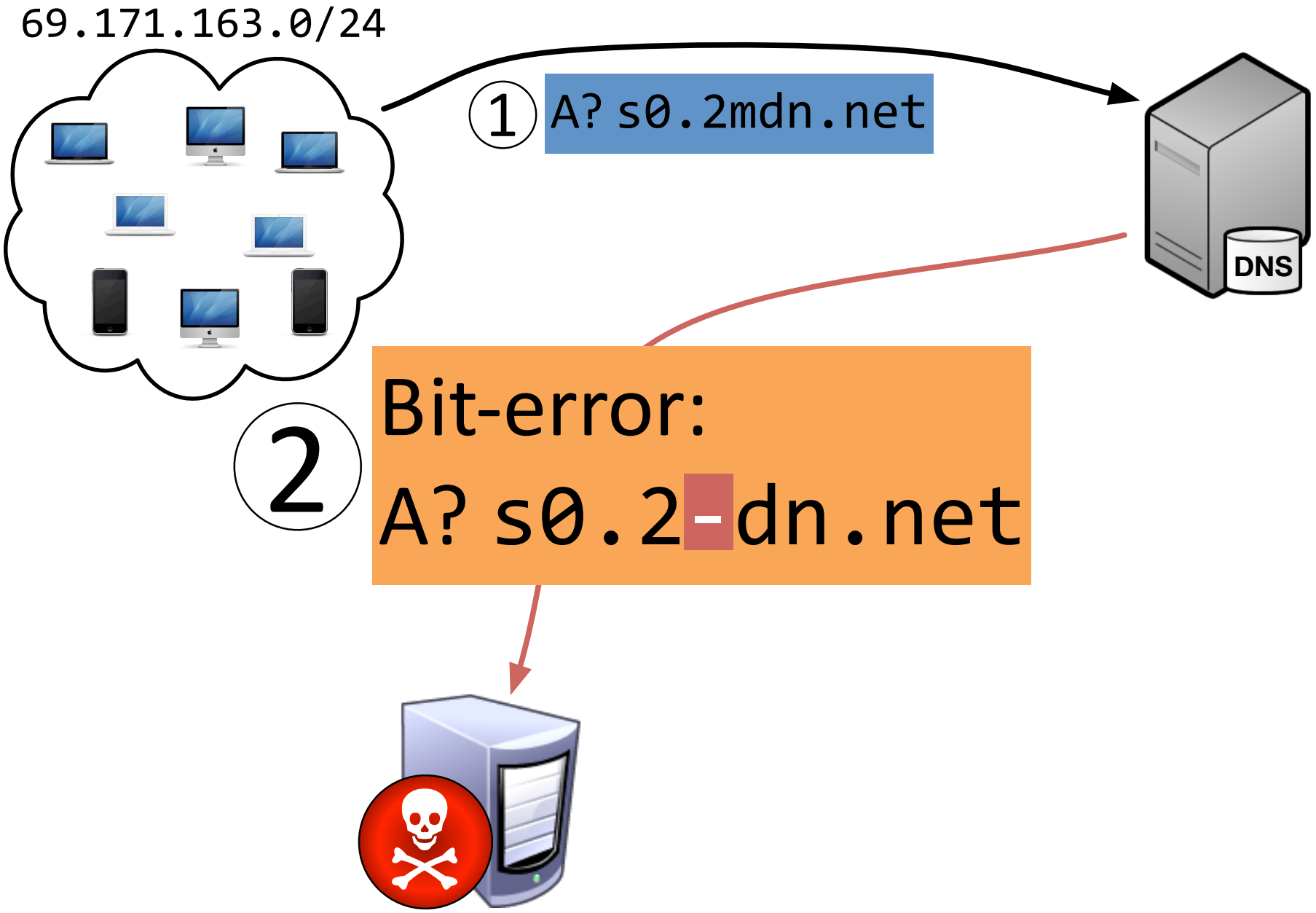

1 Play Farmville
2 Bit-error:
profile.ak.fbgdn.net
3 Request Ad
4
WWW

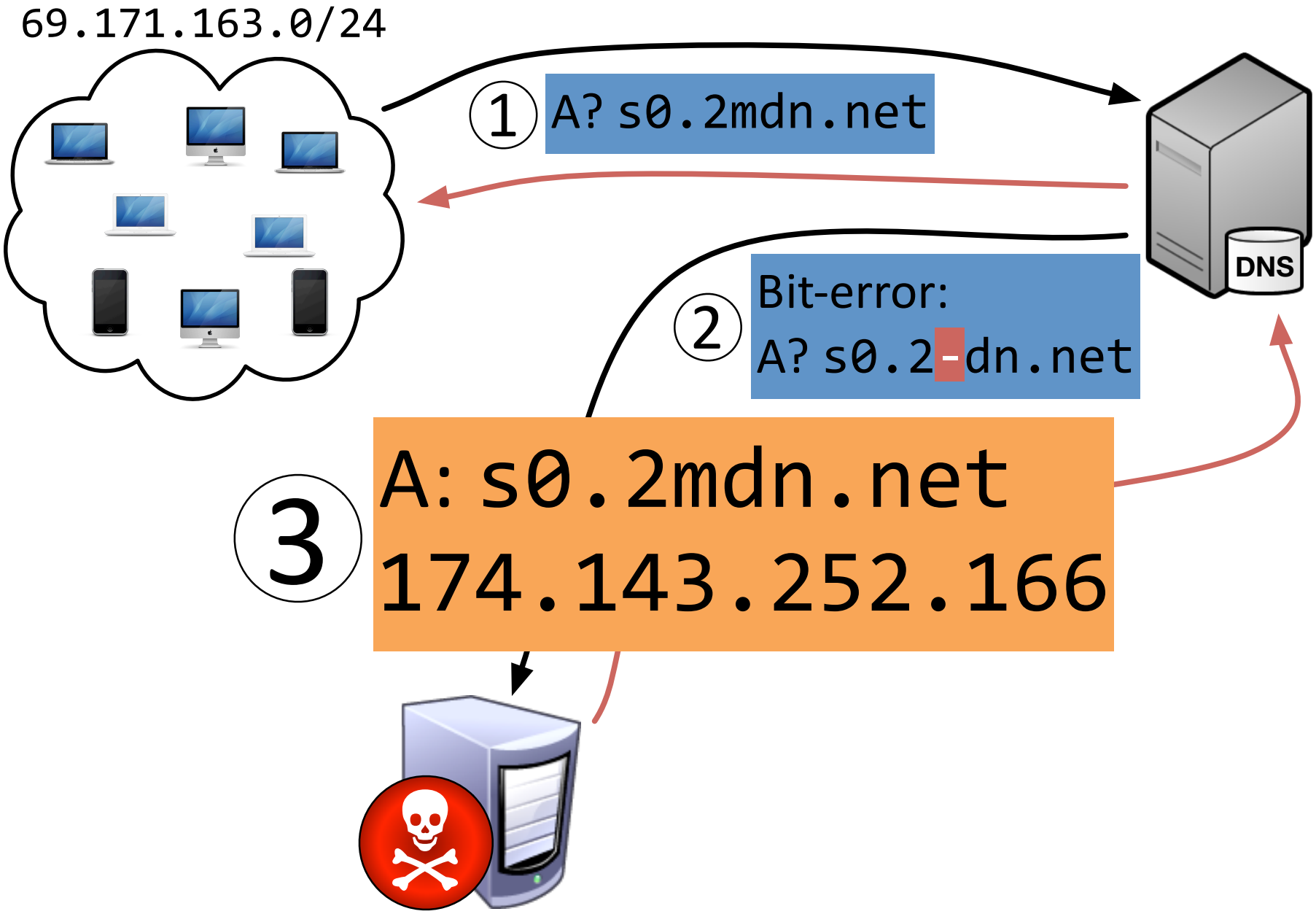

Event C
246
Unique IPs
POISON

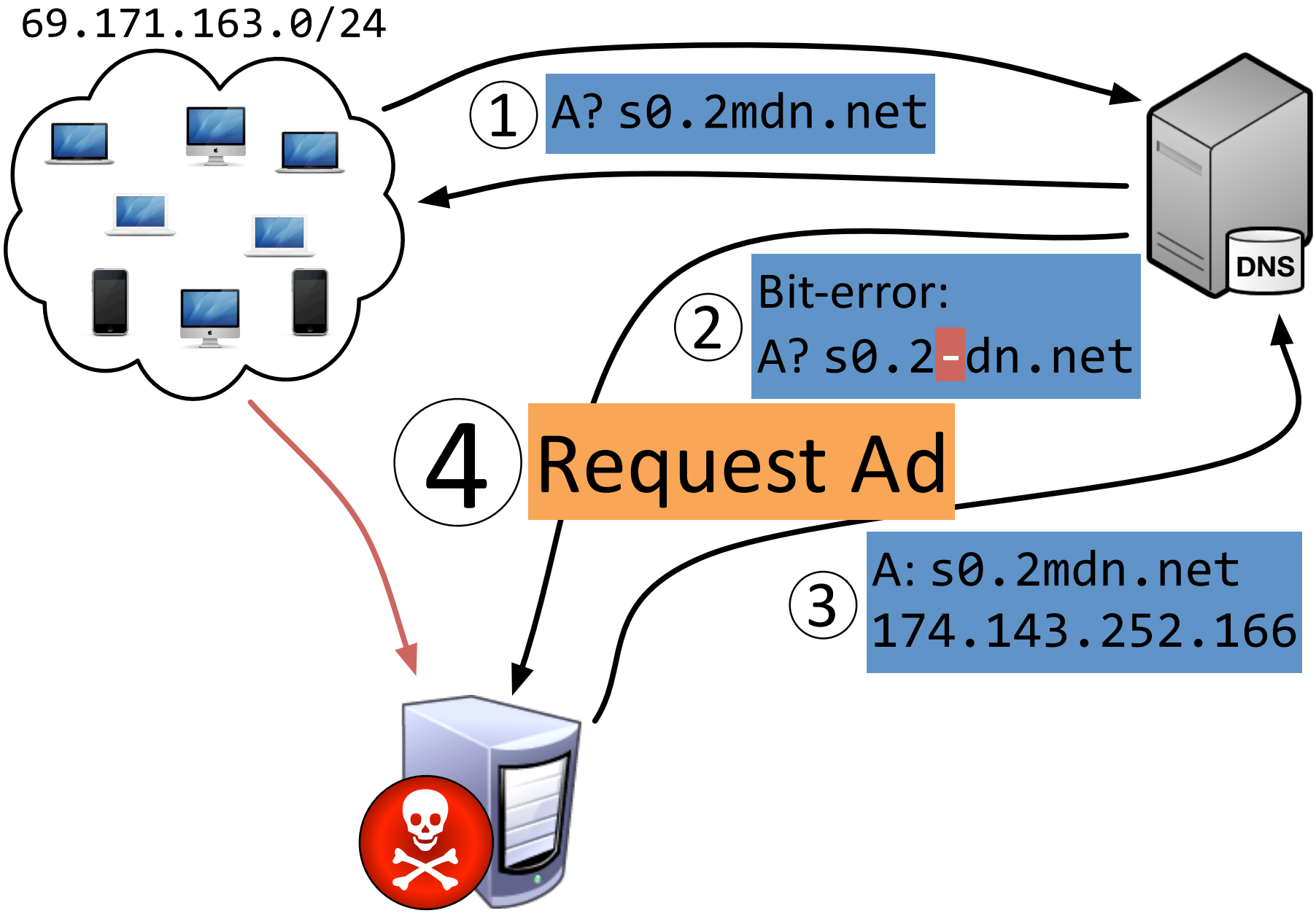
69.171.163.0/24

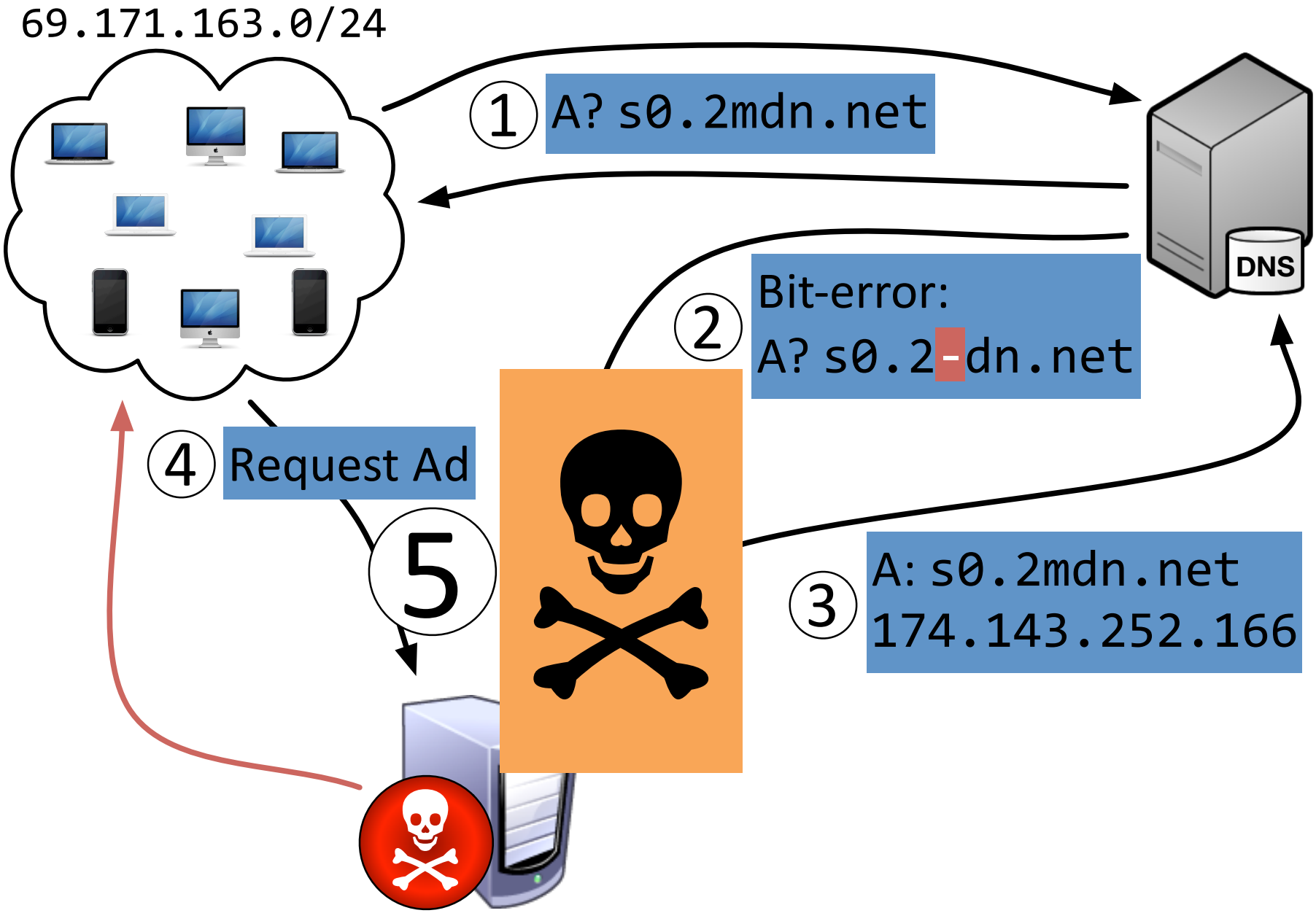


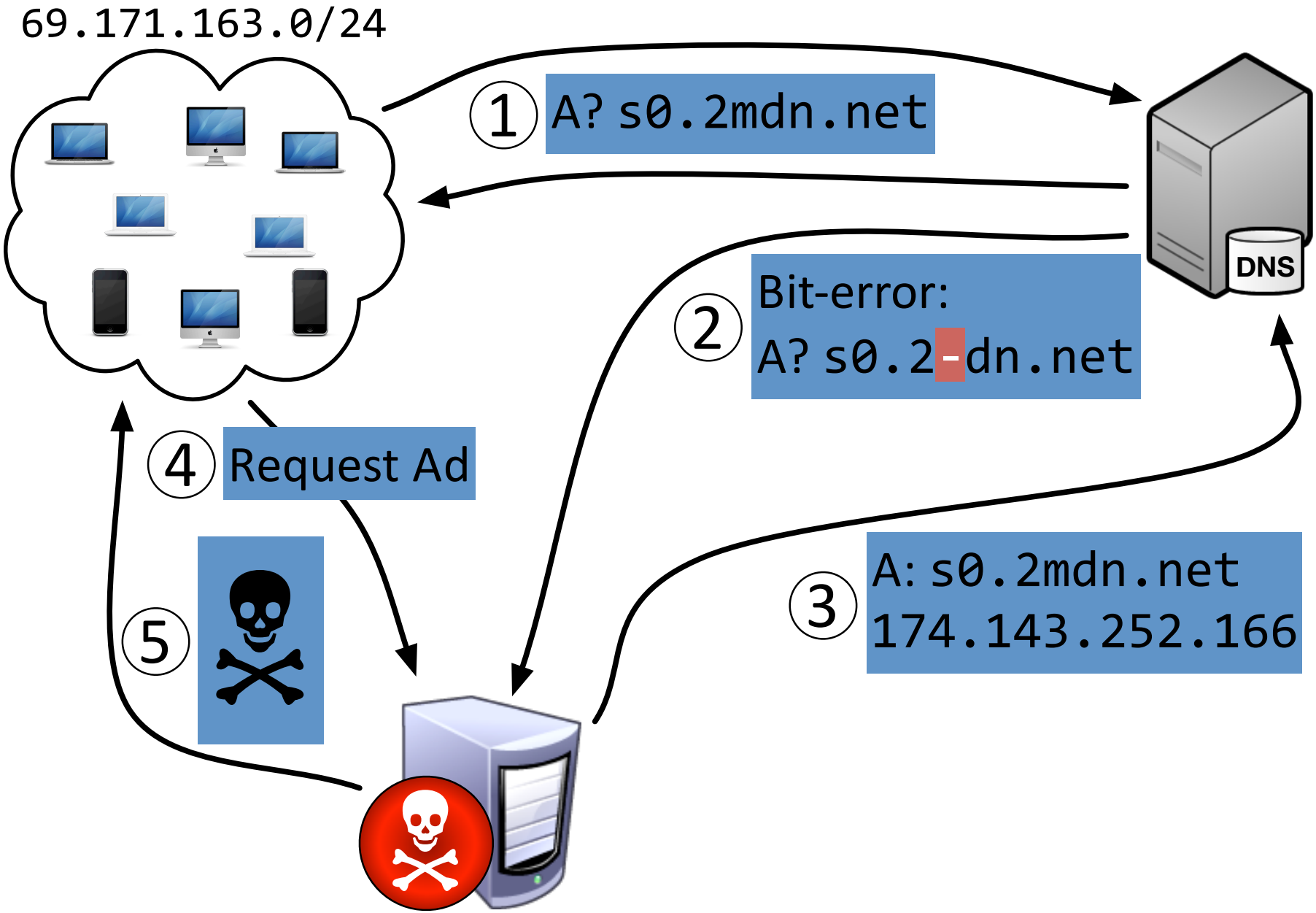
1 A? s0.2mdn.net

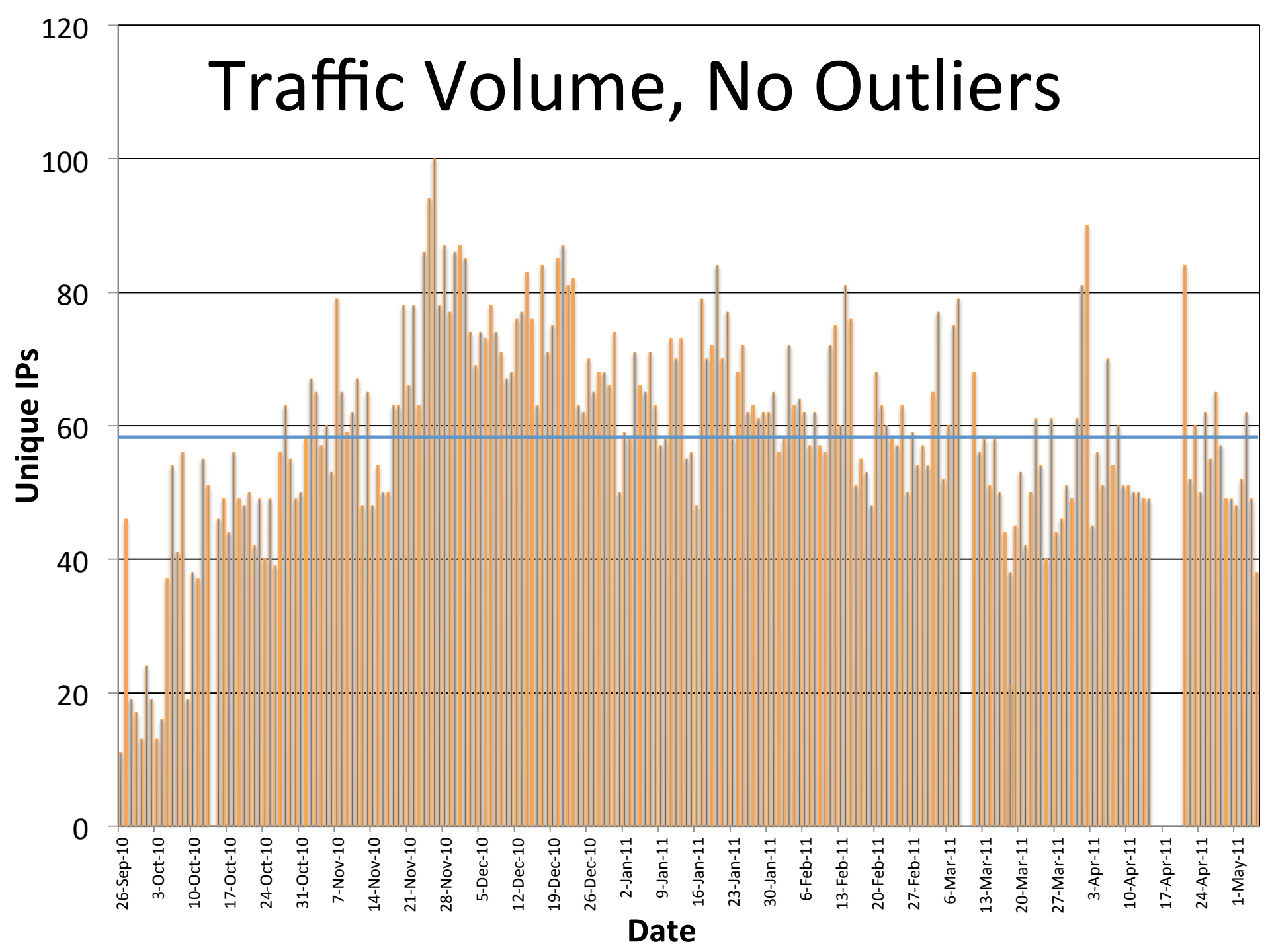

69.171.163.0/24
1
A? s0.2mdn.net
DNS
2
Bit-error:
A? s0.2-dn.net

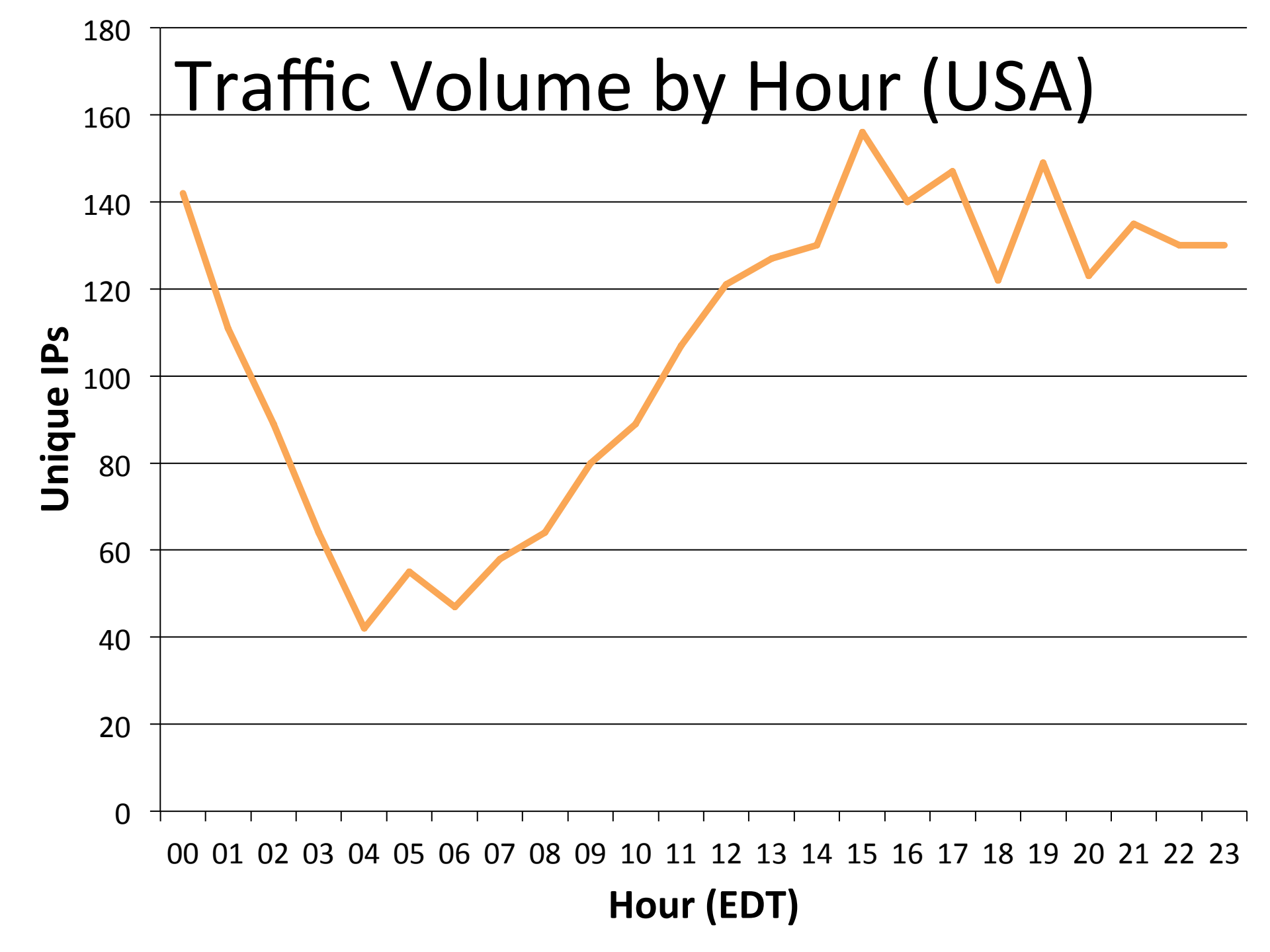

69.171.163.0/24
1
A? s0.2mdn.net
DNS
2
Bit-error:
A? s0.2-dn.net
3
A: s0.2mdn.net
174.143.252.166


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

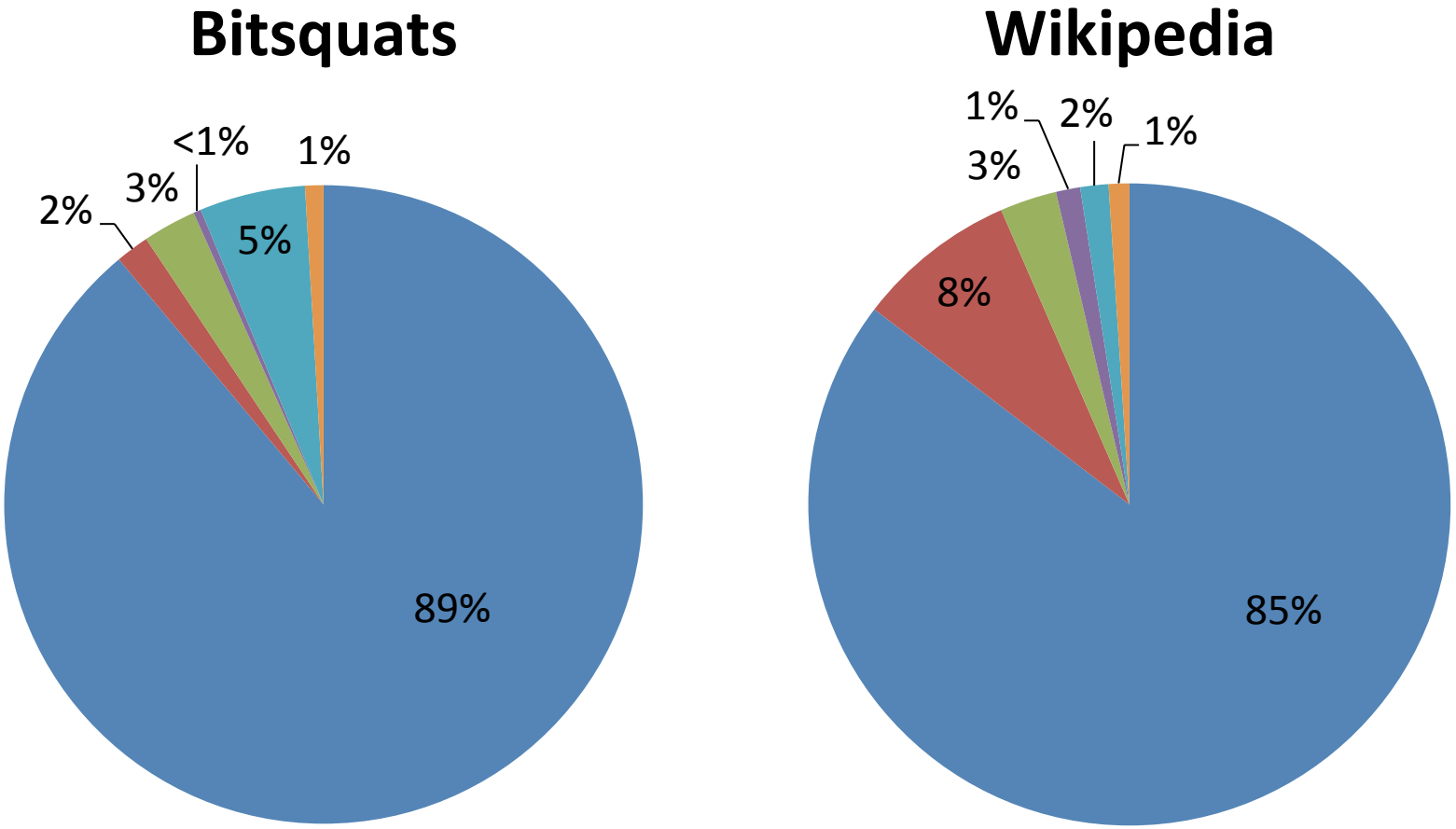

69.171.163.0/24
1
A? s0.2mdn.net
DNS
2
Bit-error:
A? s0.2-dn.net
3
A: s0.2mdn.net
174.143.252.166
4
Request Ad
5


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

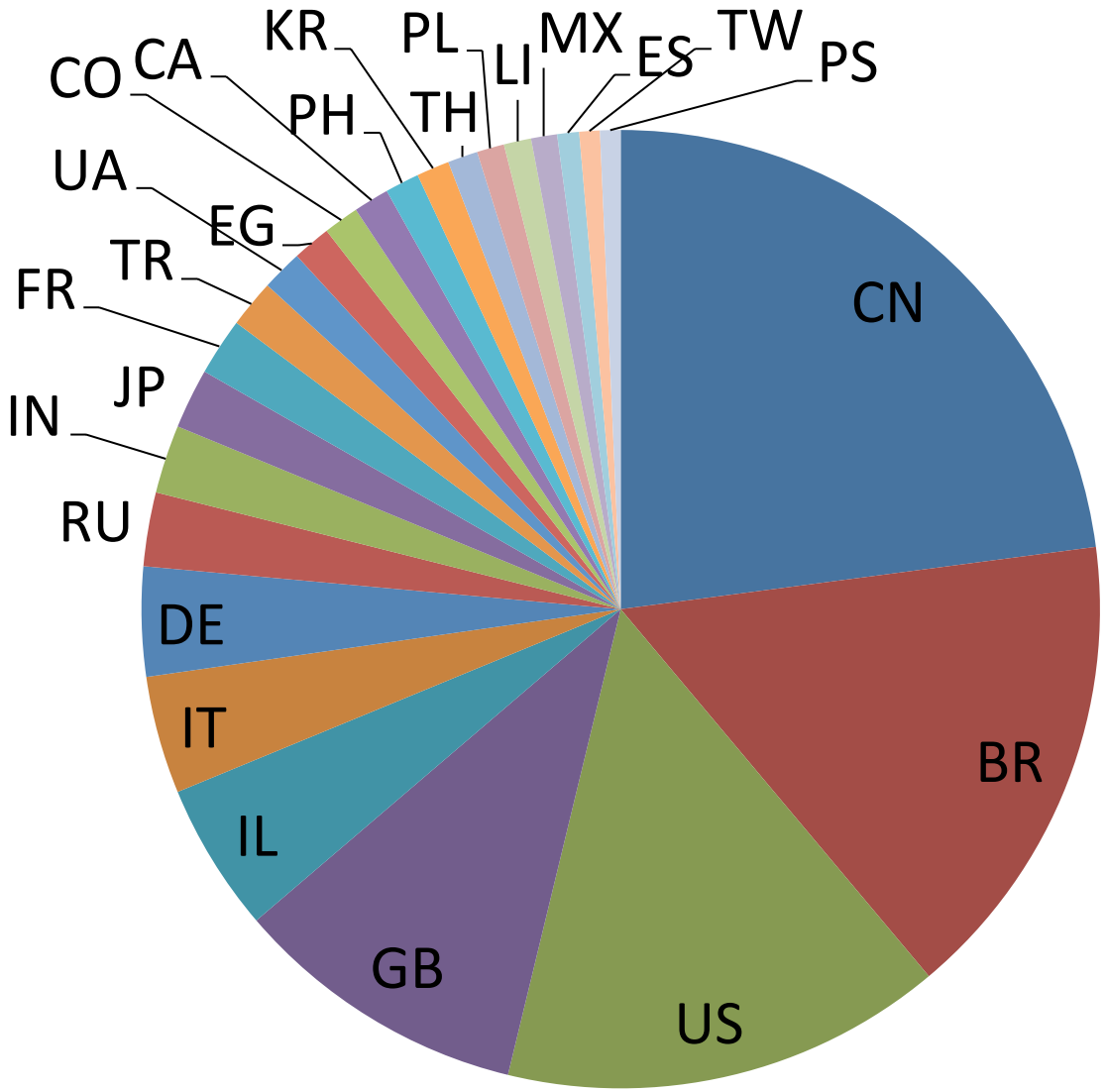

Traffic Volume, No Outliers
Unique IPs
120
100
80
60
40
20
0
26-Sep-10
3-Oct-10
10-Oct-10
17-Oct-10
24-Oct-10
31-Oct-10
7-Nov-10
14-Nov-10
21-Nov-10
28-Nov-10
5-Dec-10
12-Dec-10
19-Dec-10
26-Dec-10
2-Jan-11
9-Jan-11
16-Jan-11
23-Jan-11
30-Jan-11
6-Feb-11
13-Feb-11
20-Feb-11
27-Feb-11
6-Mar-11
13-Mar-11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


Traffic Volume by Hour (USA)
Unique IPs
180
160
140
120
100
80
60
40
20
0
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23
Hour (EDT)

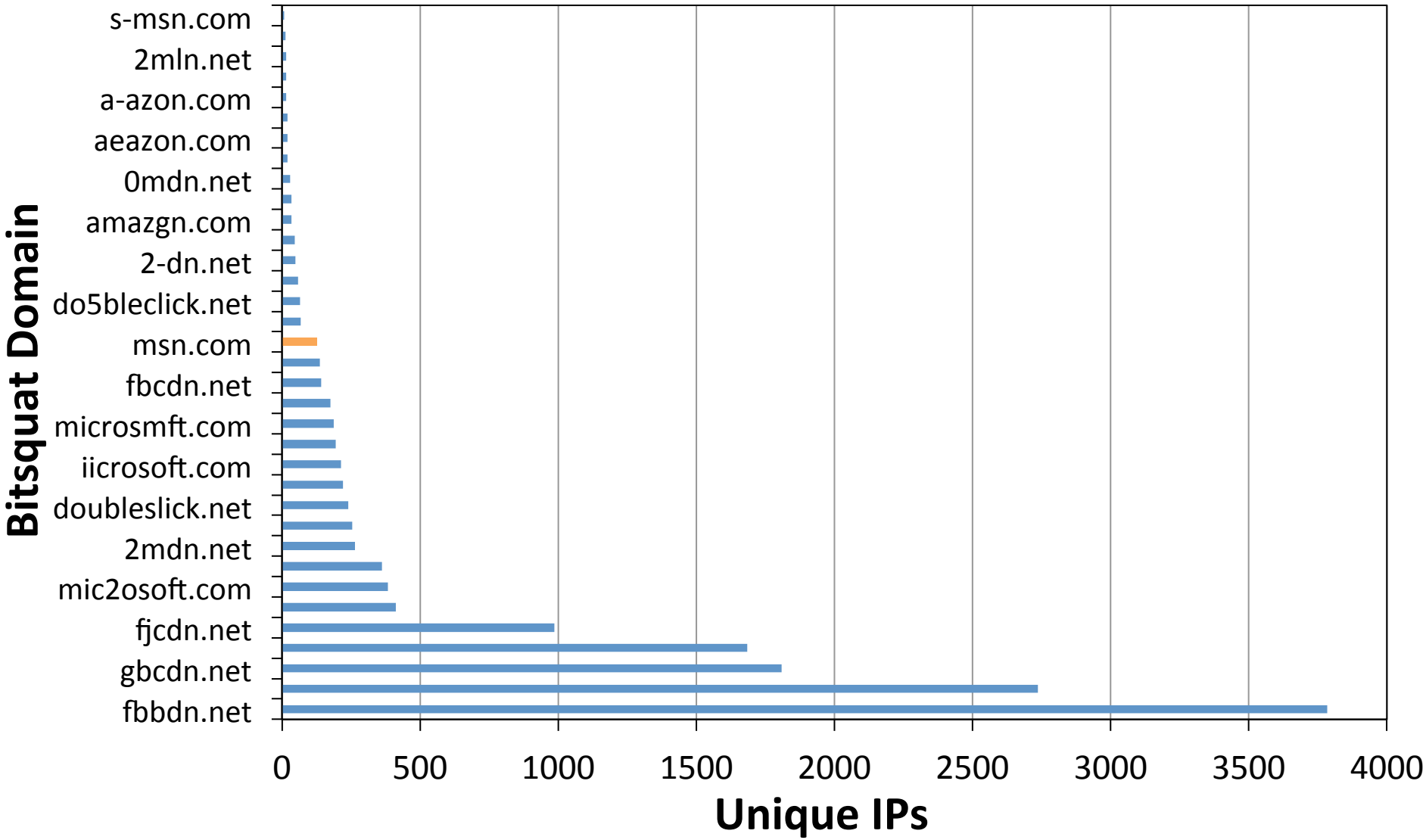
OS Statistics



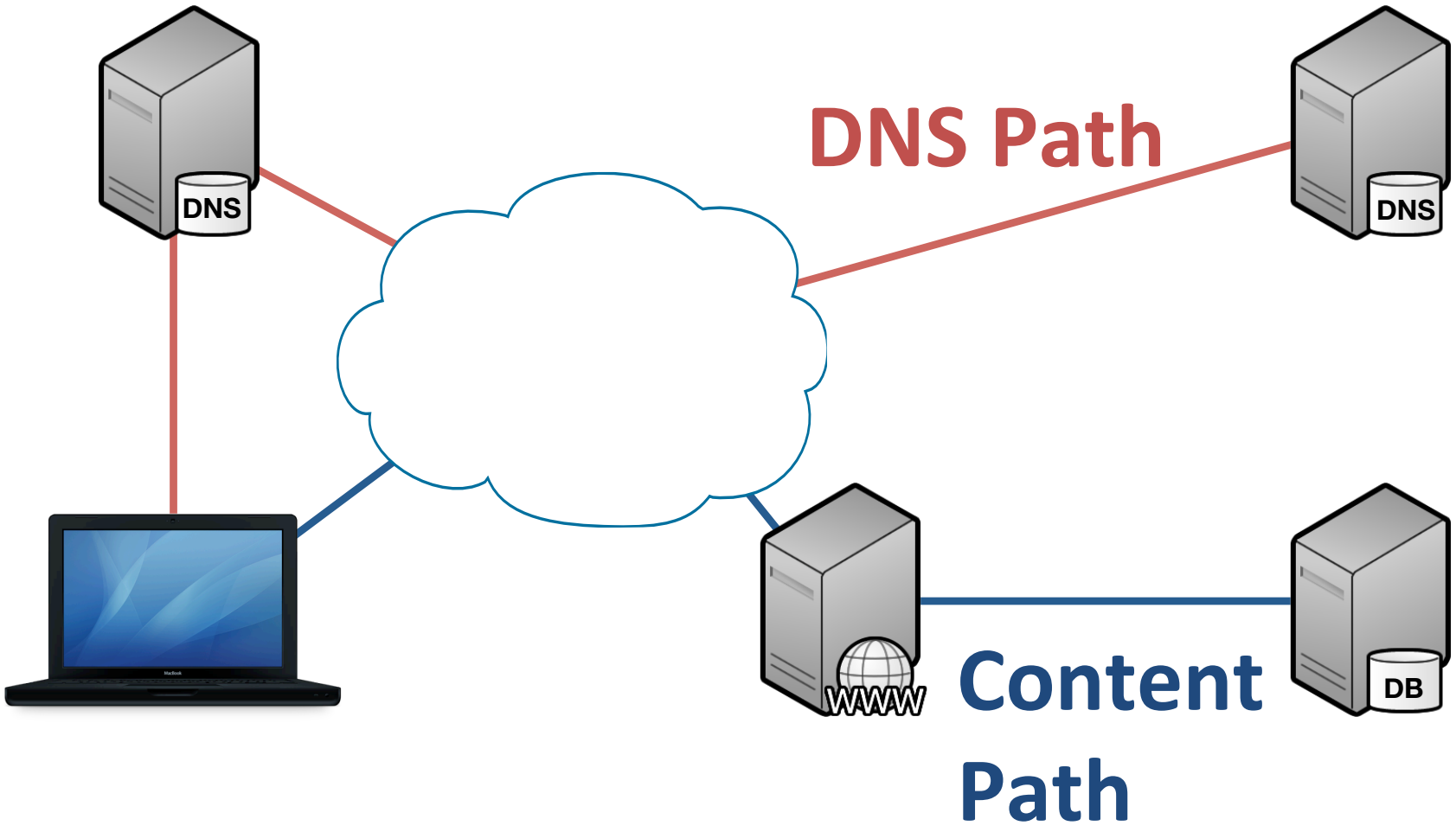
Visitors by Country (bitsquats of microsoft.com)

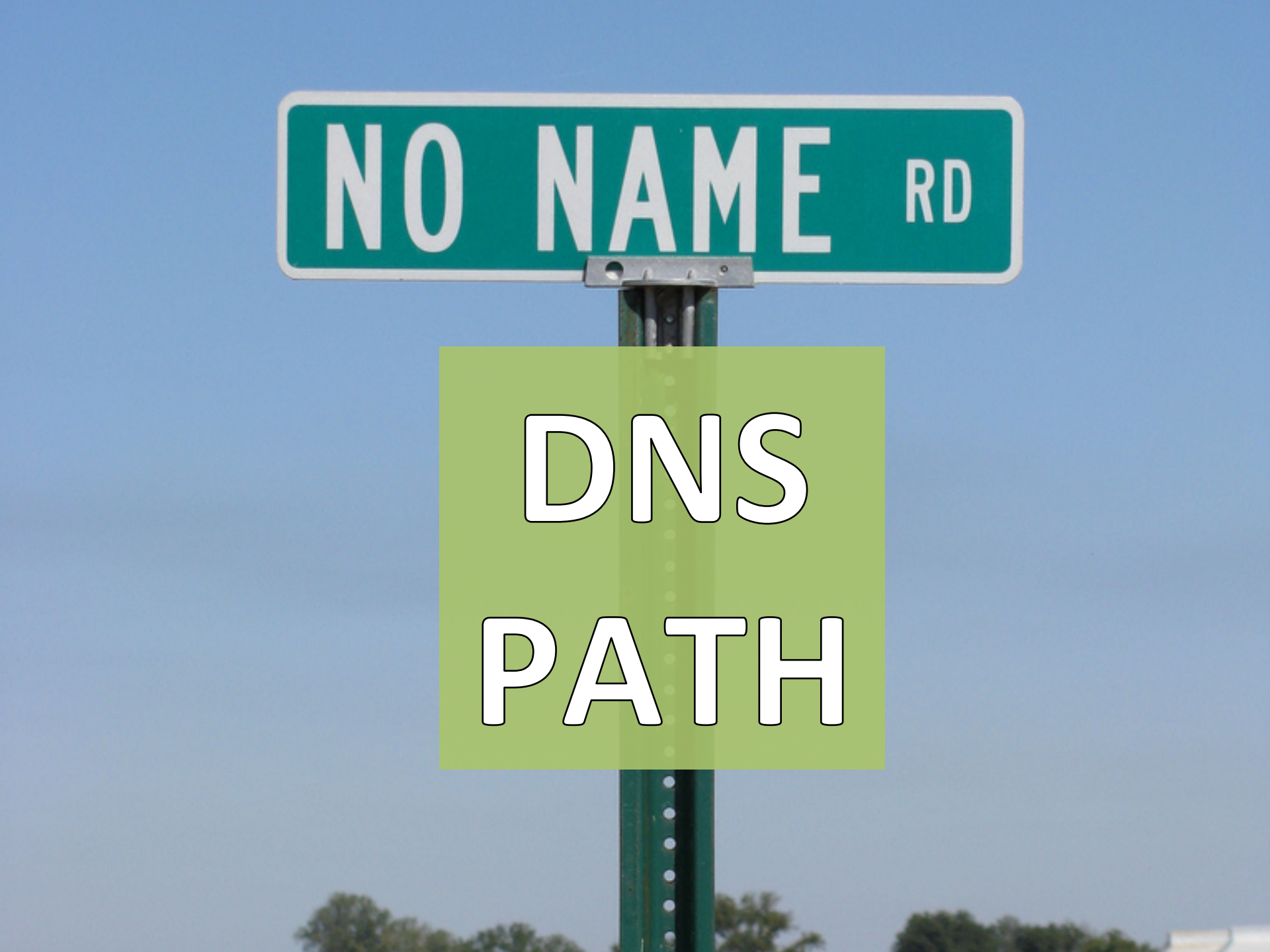


Bitsquat Popularity



Where Bit-errors Happen

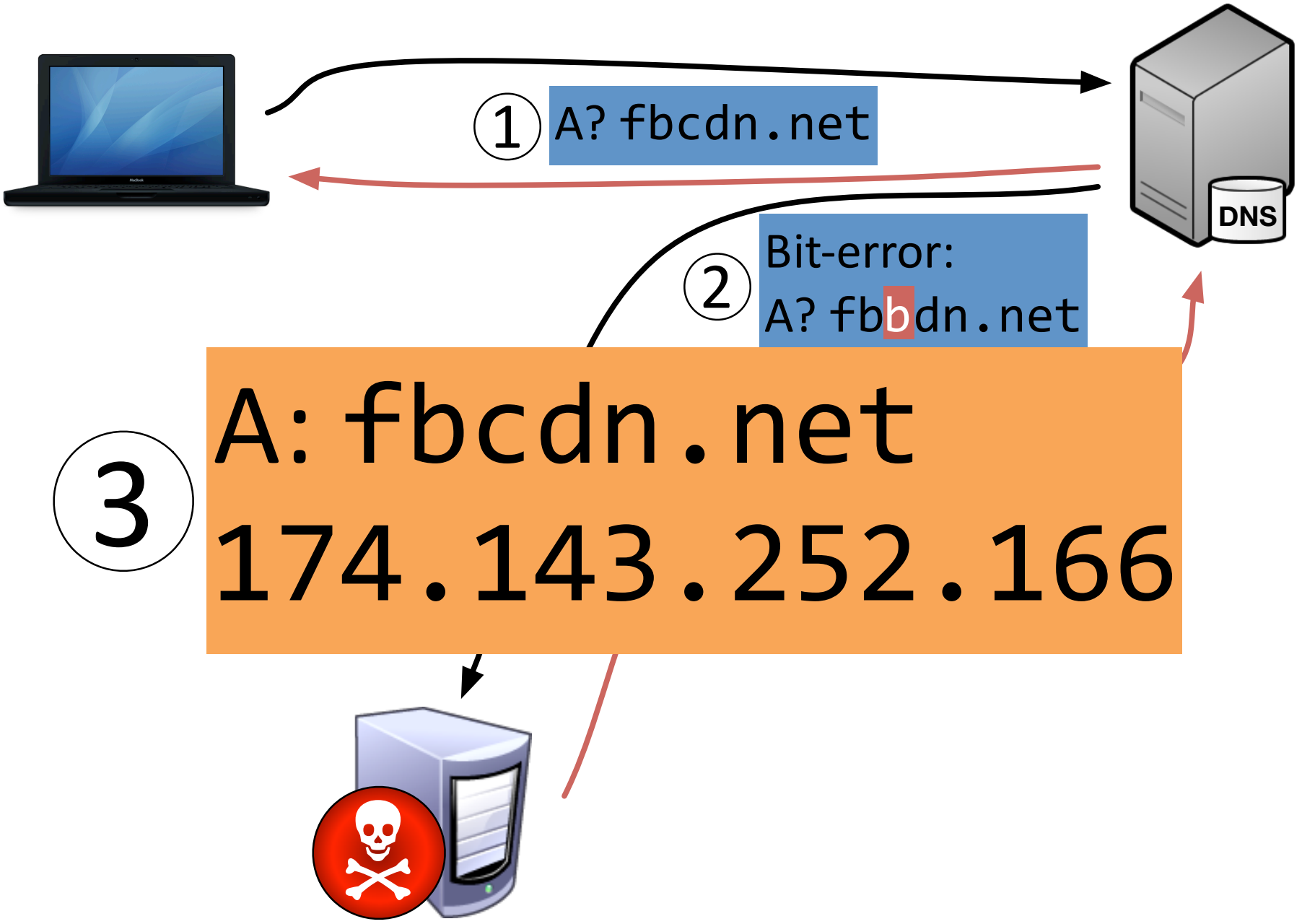


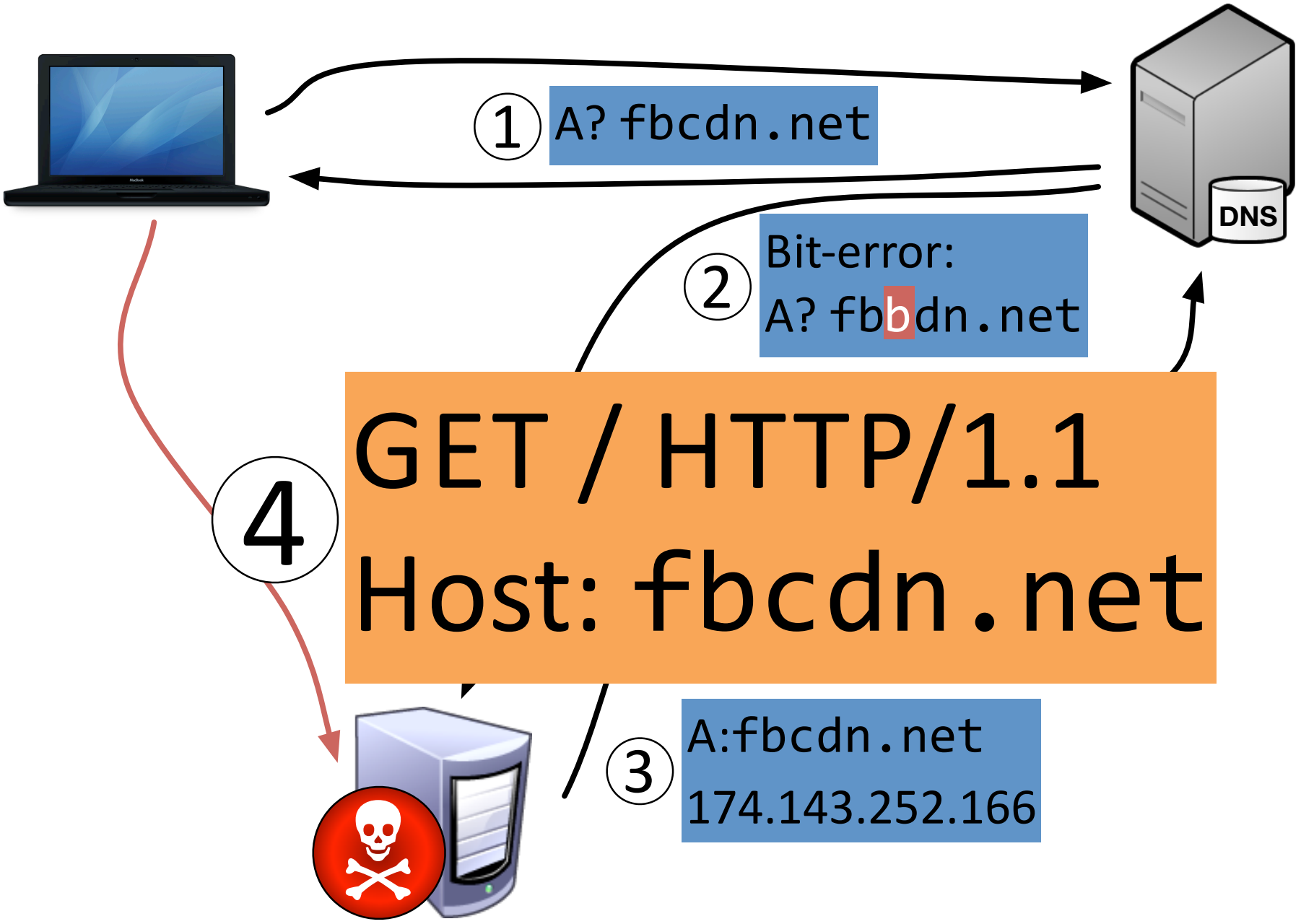

NO NAME RD
DNS
PATH

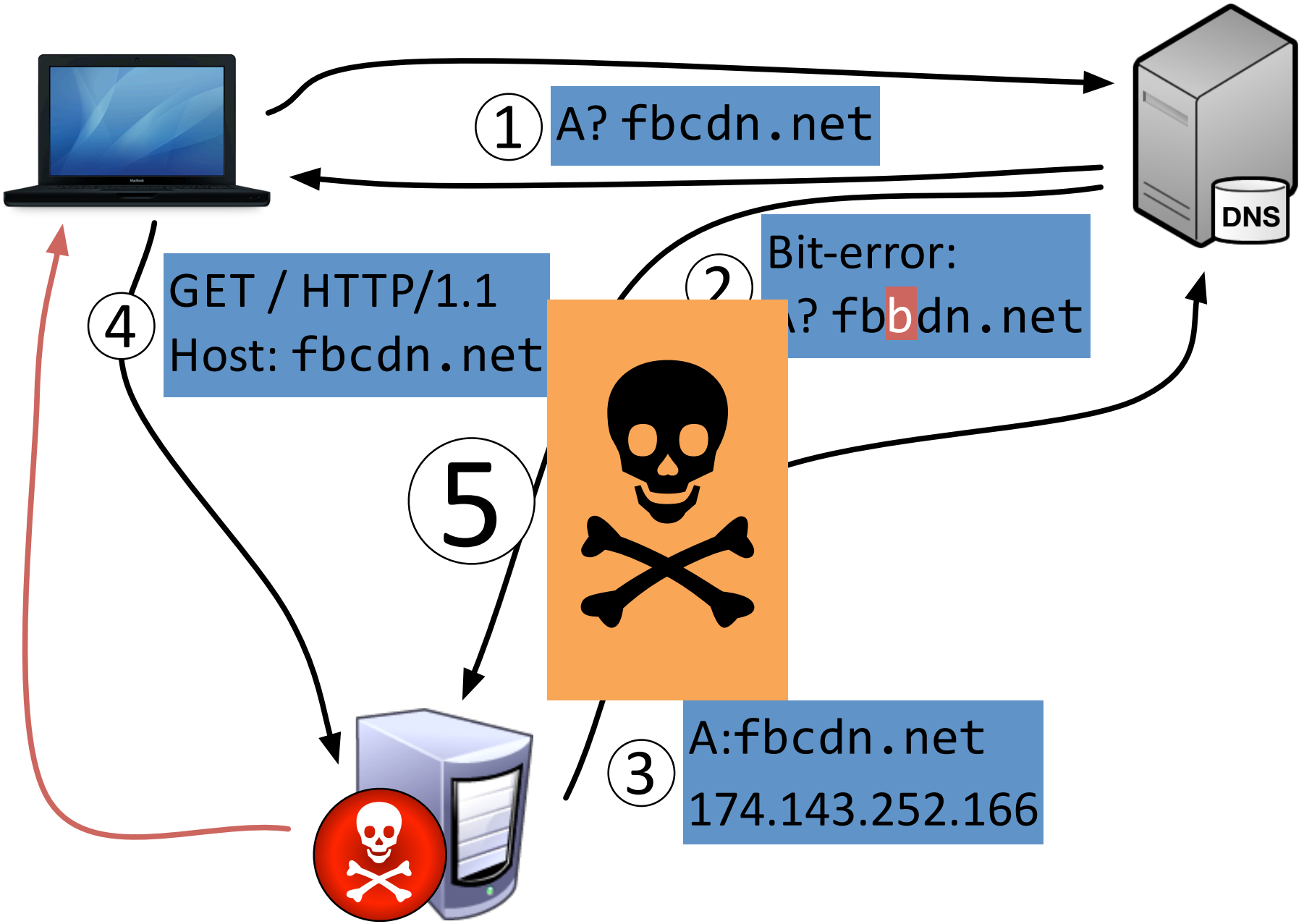
1 A? fbcdn.net

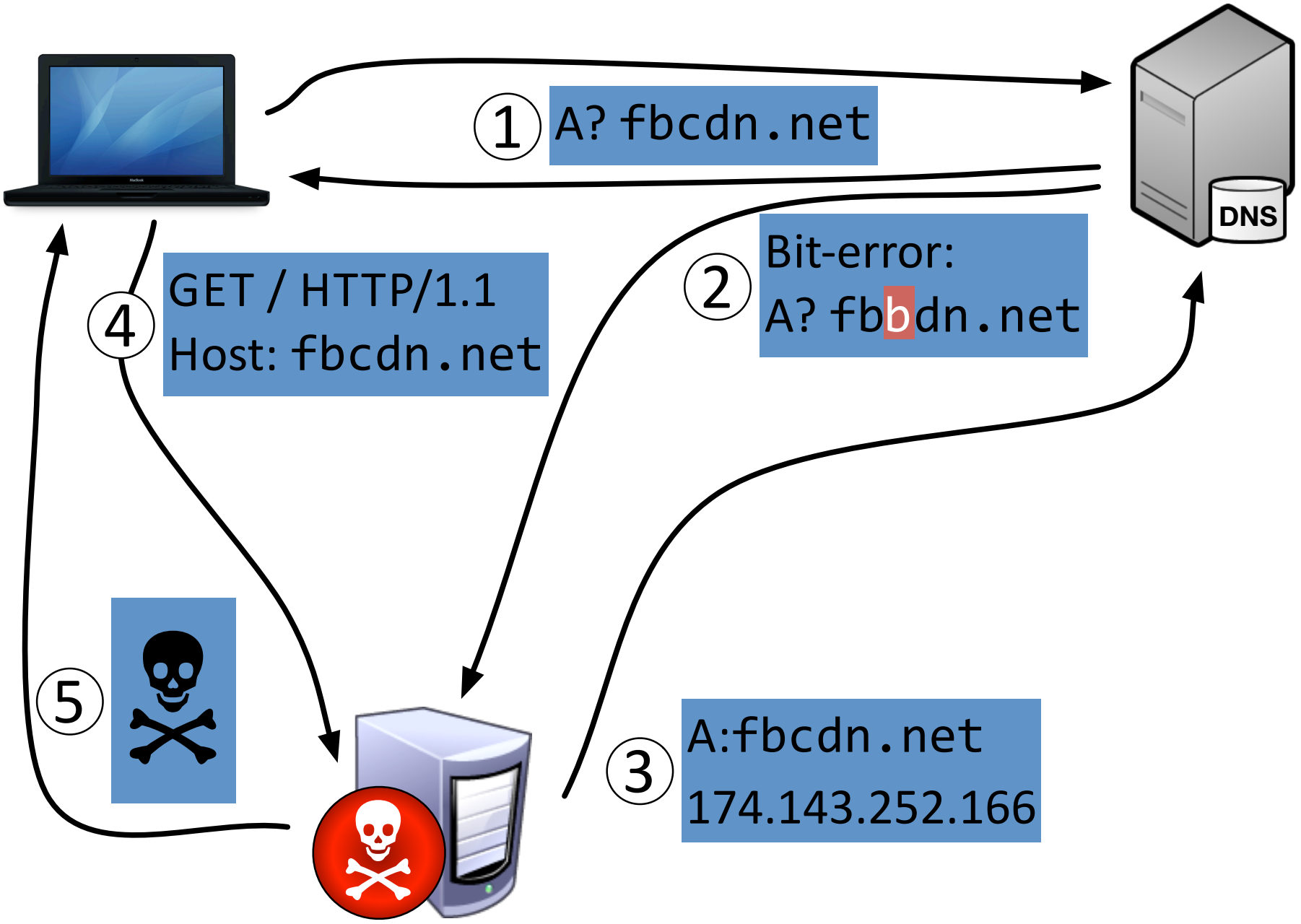
① A? fbcdn.net

② Bit-error:
A? fbbdn.net

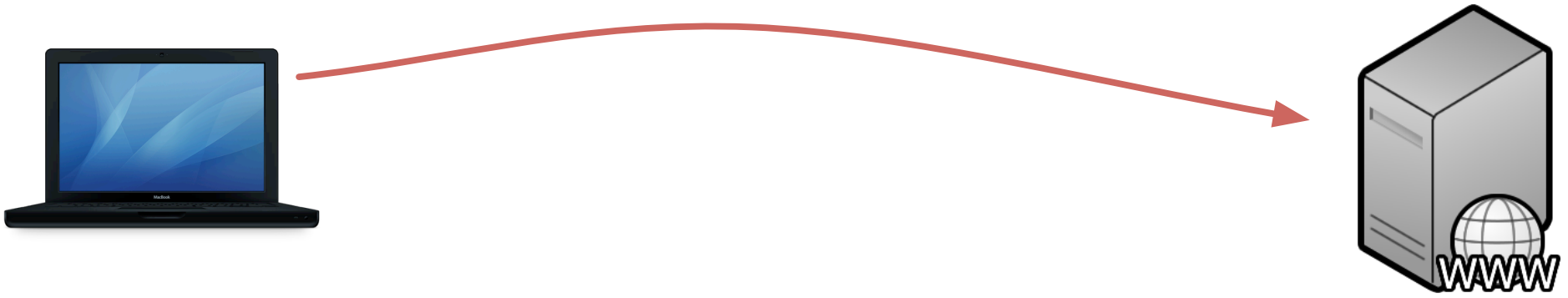

1
A? fbcdn.net
DNS
2
Bit-error:
A? fbbdn.net
3
A: fbcdn.net
174.143.252.166


1
A? fbcdn.net
DNS
2
Bit-error:
A? fbbdn.net
GET / HTTP/1.1
Host: fbcdn.net
4
3
A:fbcdn.net
174.143.252.166

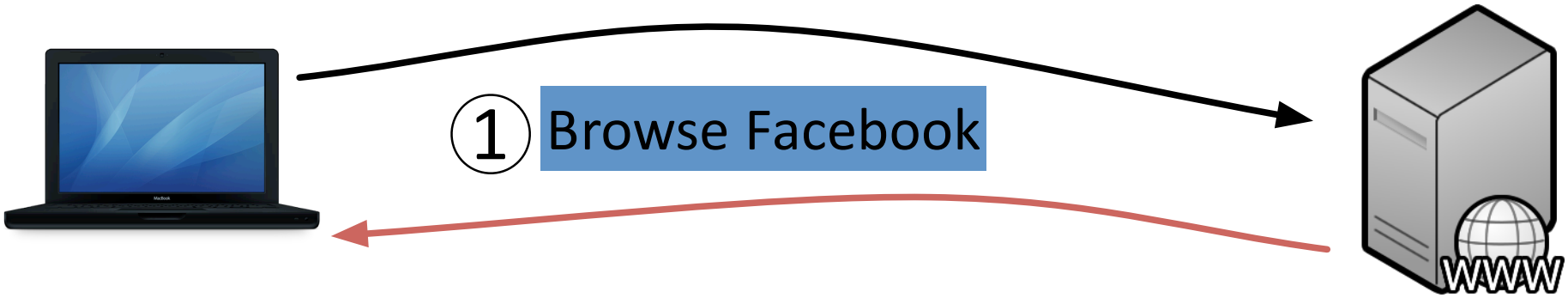

1
A? fbcdn.net
DNS
2
Bit-error:
A? fbbdn.net
4
GET / HTTP/1.1
Host: fbcdn.net
5
3
A:fbcdn.net
174.143.252.166


1
A? fbcdn.net
DNS
2
Bit-error:
A? fbbdn.net
4
GET / HTTP/1.1
Host: fbcdn.net
5
3
A:fbcdn.net
174.143.252.166

Content Path

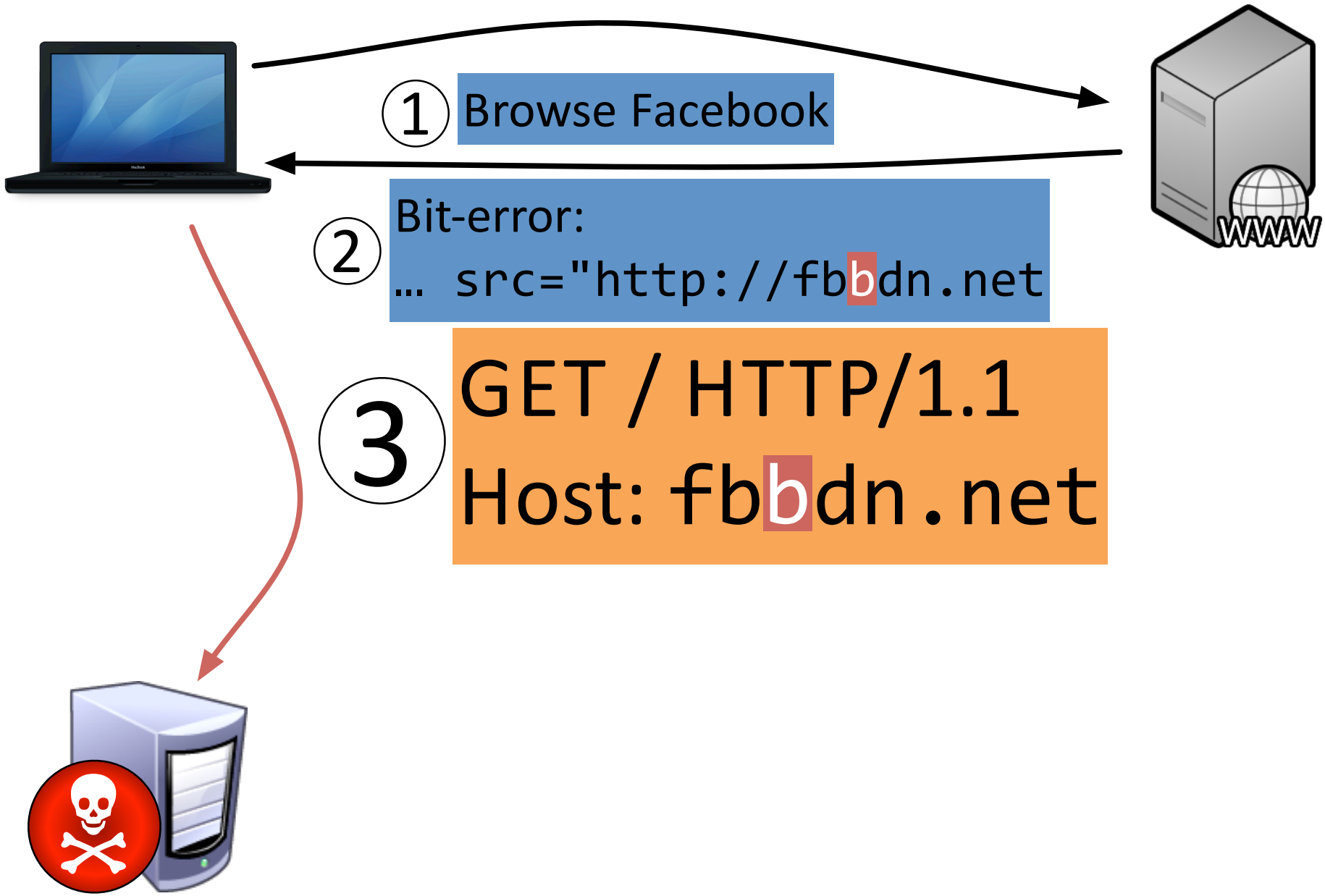


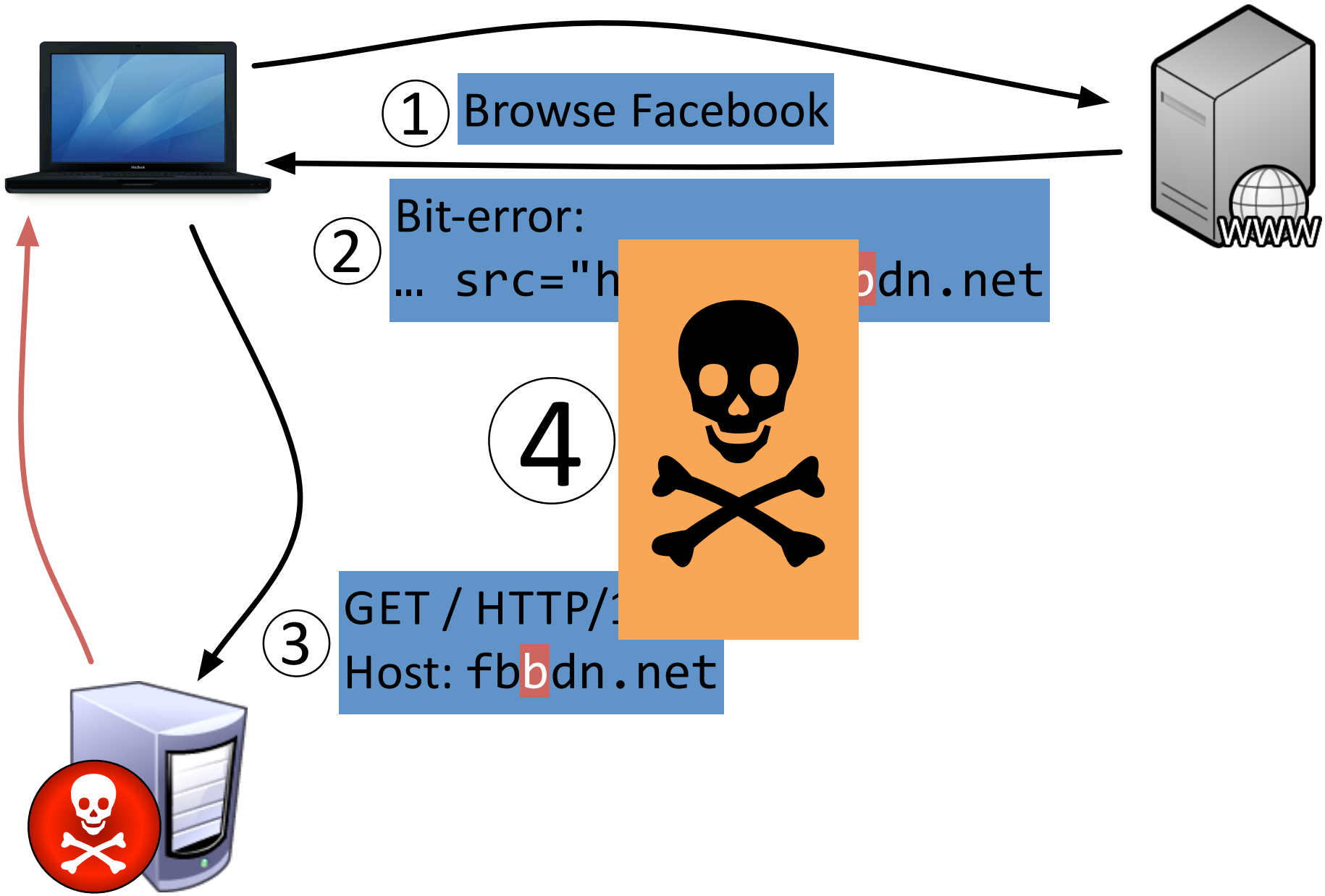
① Browse Facebook

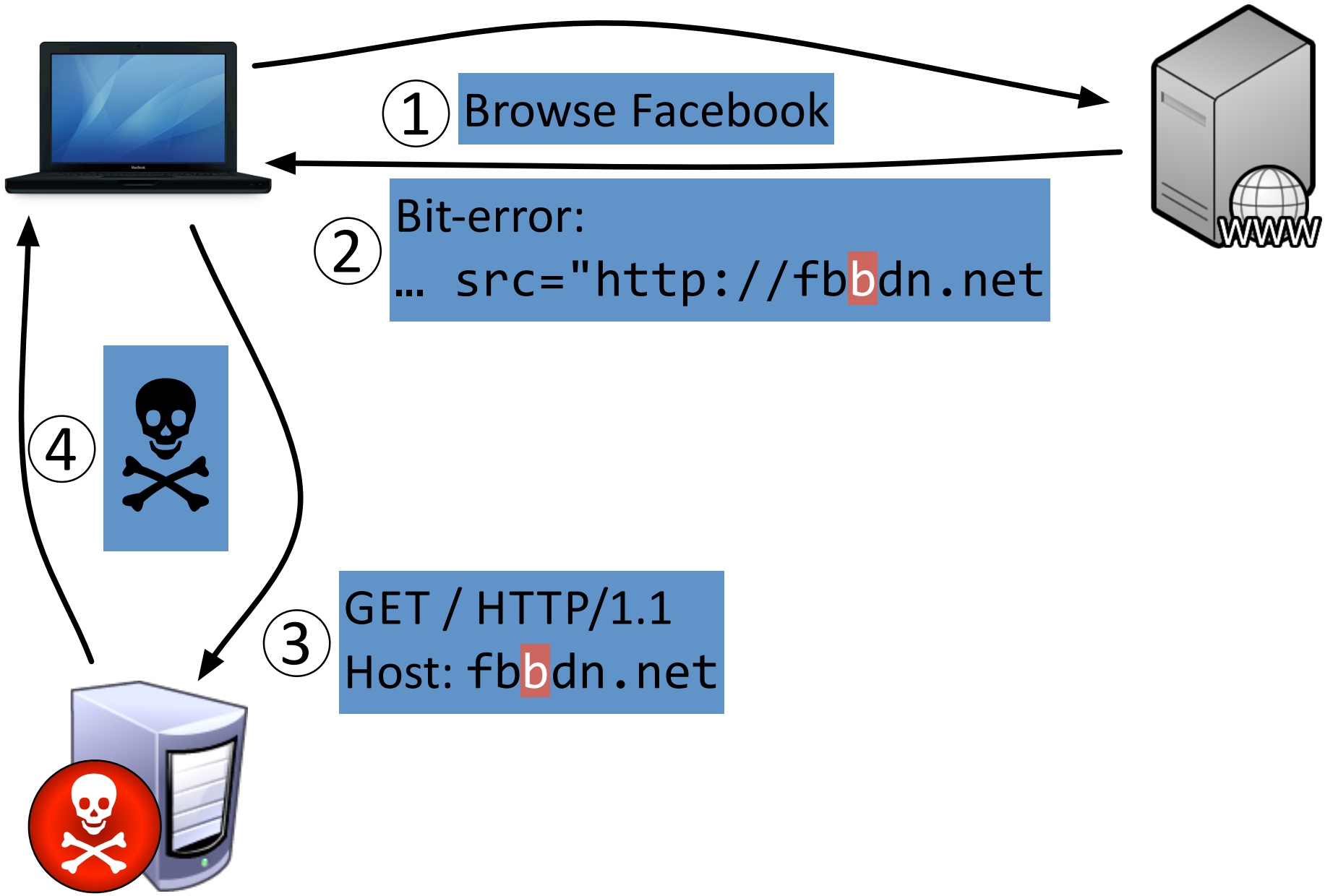


② Bit-error:

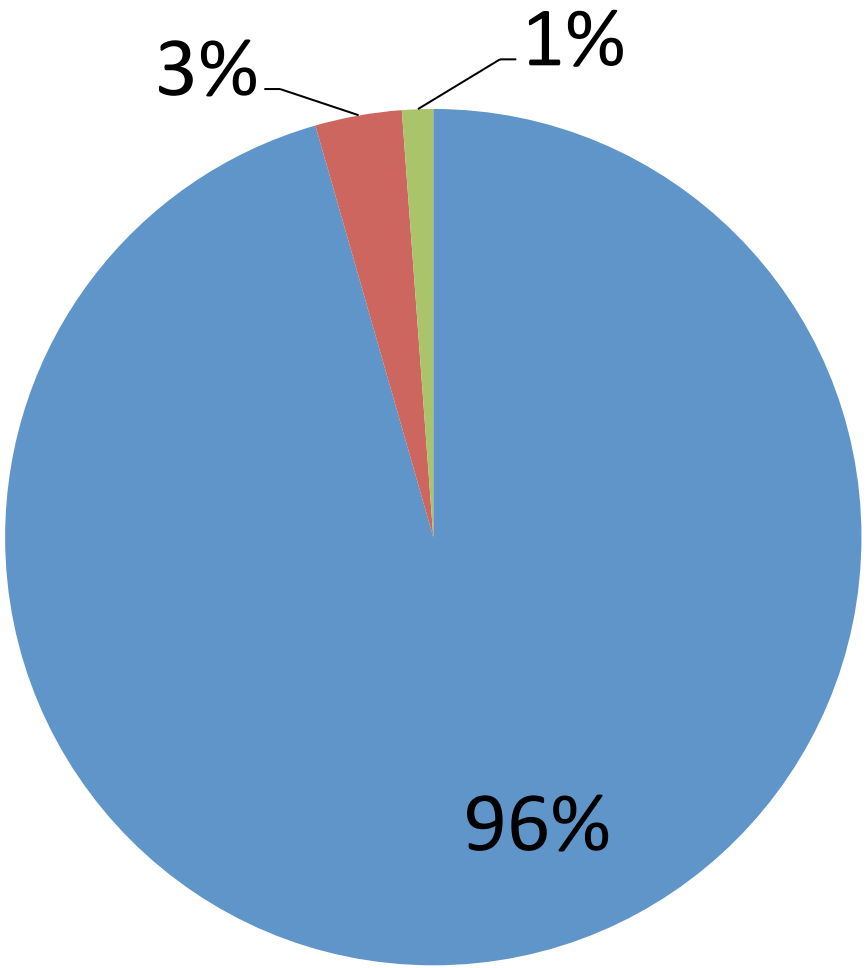
… src="http://fbbdn.net


1 Browse Facebook
2 Bit-error:
… src="http://fbbdn.net
3 GET / HTTP/1.1
Host: fbbdn.net
WWW


1 Browse Facebook
2 Bit-error:
… src="h bdn.net
4
3 GET / HTTP/1
Host: fbbdn.net
WWW


1 Browse Facebook
2 Bit-error:
… src="http://fbbdn.net
3 GET / HTTP/1.1
Host: fbbdn.net
4
WWW

Domain in HTTP Host Header



Bitsquat **Original** **Other**


ax.init.itunes.apple.com
ax.init.itunes.apple.com
.edgesuite.net
a771.da1.akamai.net
96.17.171.168

Real Example: Other Domains

ax.init.itunes.apple.com 81.225.40.xxx "GET /WebObjects/MZInit.woa/wa/initiateSession?ix=2 HTTP/1.1" 404 202 "-" "iTunes-iPhone/4.1 (4; 16GB)"

mmv.admob.com 109.175.185.xxx "GET /static/iphone/img/app@2x.png HTTP/1.1" "Mozilla/5.0 (iPhone; U; CPU iPhone OS 4_1 like Mac OS X; HW iPhone2,1; en_gb) AppleWebKit/525.18.1 (KHTML, like Gecko) (AdMob-iSDK-20101108; iphoneos4.2)"

lifestyle.msn.com 70.91.78.xxx "GET /article_toolbar_your_home.aspx HTTP/1.1" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; GTB6.6; (R1 1.5); .NET CLR 1.0.3705; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.04506.648; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)"

emea.rel.msn.com 194.50.104.xxx "GET /default.aspx?di=10230&pi=95517&ps=33229&pageid=8522097&mk=ru-ru&tp=http%3A%2F%2Fru.msn.com%2F&fk=default&gp=S&optkey=default&parsergroup=hops HTTP/1.1" 404 184 "http://ru.msn.com/?ocid=iehp" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET4.0C; .NET4.0E; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)"

Real Examples: Facebook

static.ak.fjcdn.net 109.242.50.xxx "GET /rsrc.php/z67NS/hash/4ys0envq.js HTTP/1.1" "http://www.facebook.com/profile.php?id=xxxxxxxxxx" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; WOW64; Trident/4.0; GTB6.5; SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.0.30729; .NET CLR 3.5.30729; InfoPath.2; Hotbar 11.0.78.0; OfficeLiveConnector.1.5; OfficeLivePatch.1.3; AskTbZTV/5.8.0.12304)"

b.static.ak.dbcdn.net 122.168.204.xxx "GET /rsrc.php/zk/r/70eOUKPXS_5.js HTTP/1.1" "http://www.facebook.com/home.php?sk=lf" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"

static.ak.fbbdn.net 194.98.30.xxx "GET /rsrc.php/yq/r/ypBeM1b0IFS.js HTTP/1.1" "http://m.facebook.com/home.php?refsrc=m.facebook.com%2Fid02.qnitabxn.site.prd.miyowa.net%2FSD2q10oklmcvyqv0v45s1zz4z452DS%2Fhome.aspx&refid=7&m_sess=soz7CzQ1-lOioUPsT&_rdr" "Mozilla/5.0 (Linux; U; Android 2.1-update1; fr-fr; GT-I5800 Build/ECLAIR) AppleWebKit/530.17 (KHTML, like Gecko) Version/4.0 Mobile Safari/530.17"

Real Examples: Windows Update

download.iicrosoft.com 91.198.175.xxx "GET /v9/windowsupdate/redir/muv4wuredir.cab?1010161718 HTTP/1.1" "Windows-Update-Agent"

www.update.microsnft.com 201.144.5.xxx "HEAD /v9/windowsupdate/selfupdate/wuident.cab?1011010912 HTTP/1.1" "Windows-Updatf-Agent"

beta.update.microsmft.com 113.117.249.xxx "GET /microsoftupdate/v6/default.aspx?1290162381 HTTP/1.1" "http://beta.update.microsoft.com/microsoftupdate/v6/default.aspx" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0; GTB6.6; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30618)"

download.microsoft.com 91.13.83.xxx "HEAD /WM/MicrosoftUpdate/redir/duredir.cab HTTP/1.1" "Windows-Mobile-Device-Update-Agent"

msgr.dlservice.mic2osoft.com 213.178.224.xxx "GET /download/A/6/1/A616CCD4-B0CA-4A3D-B975-3EDB38081B38/ar/wlsetup-cvr.exe HTTP/1.1" 404 268 "-" "Microsoft BITS/6.6"

Real Examples: Webmail

sn110w.snt110.mail.li6e.com 187.92.218.xxx "GET /mail/clear.gif HTTP/1.1" "http://sn110w.snt110.mail.live.com/mail/InboxLight.aspx?FolderID=00000000-0000-0000-0000-000000000001&n=xxxxxxxxx" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; GTB6.5; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)"

secure.s%28ared.li6e.com 190.95.125.xxx "GET /_/F$Live.SiteContent.Messenger/4.2.57151/Messenger.html HTTP/1.1" 404 215 "http://bl145w.blu145.mail.live.com/default.aspx?wa=wsignin1.0" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.3 (KHTML, like Gecko) Chrome/6.0.472.63 Safari/534.3"

s0.2ldn.net 66.82.9.xxx "GET /879366/flashwrite_1_2.js HTTP/1.1" "http://webmail.satx.rr.com/_uac/adpage.html" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; HPNTDF; AskTB5.2)"

Real Examples: Crash Reports

watson.microsnft.com 115.143.103.xxx "GET /StageOne/acrord32_exe/9_3_3_177/msvcr80_dll/8_0_50727_3053/00008aa0.htm?OS=5.1.2600.2.00010100.3.0&lcid=1042 HTTP/1.1" "MSDW"

watson.microsnft.com 187.73.247.xxx "GET /StageOne/notepad_exe/5_1_2600_5512/uxtheme_dll/6_0_2900_5512/00004b43.htm?OS=5.1.2600.2.00010100.3.0&lcid=1046 HTTP/1.1" "MSDW"

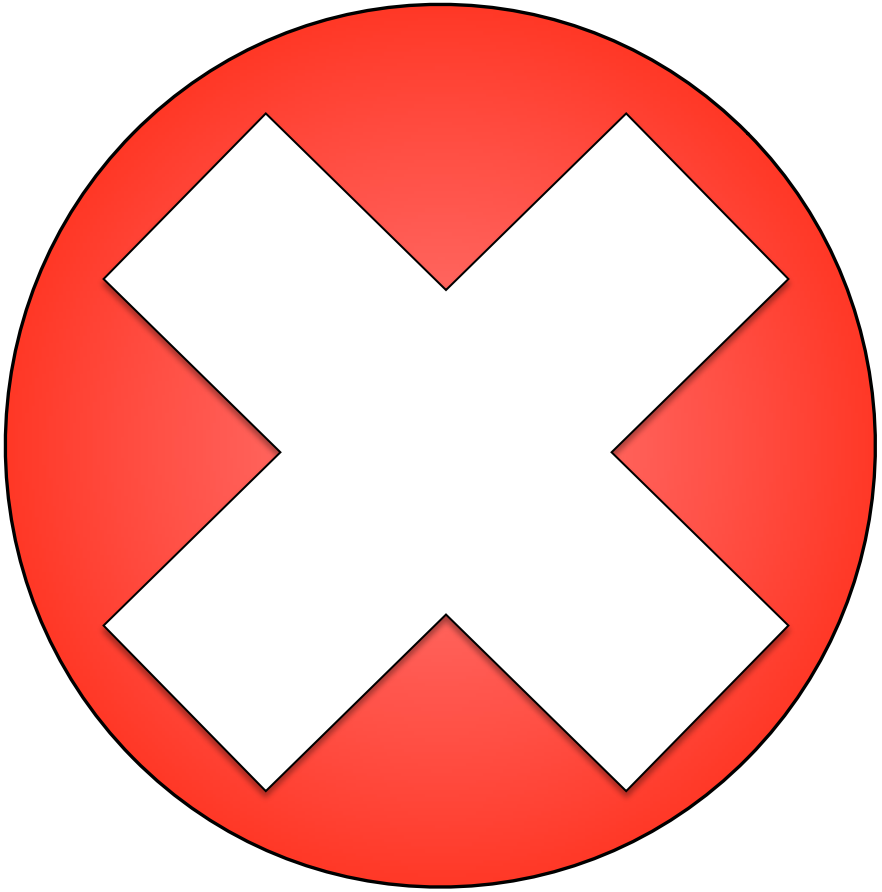
watson.mic2osoft.com 202.156.10.xxx "GET /StageOne/Generic/FaultTolerantHeap/SearchIndexer_exe/7_0_7600_16385/4A5BD212/ffffbaad.htm?LCID=18441&OS=6.1.7600.2.00010100.0.0.48.16385&SM=System%20manufacturer&SPN=System%20Product%20Name&BV=1456 HTTP/1.1" "MSDW”

Mitigations

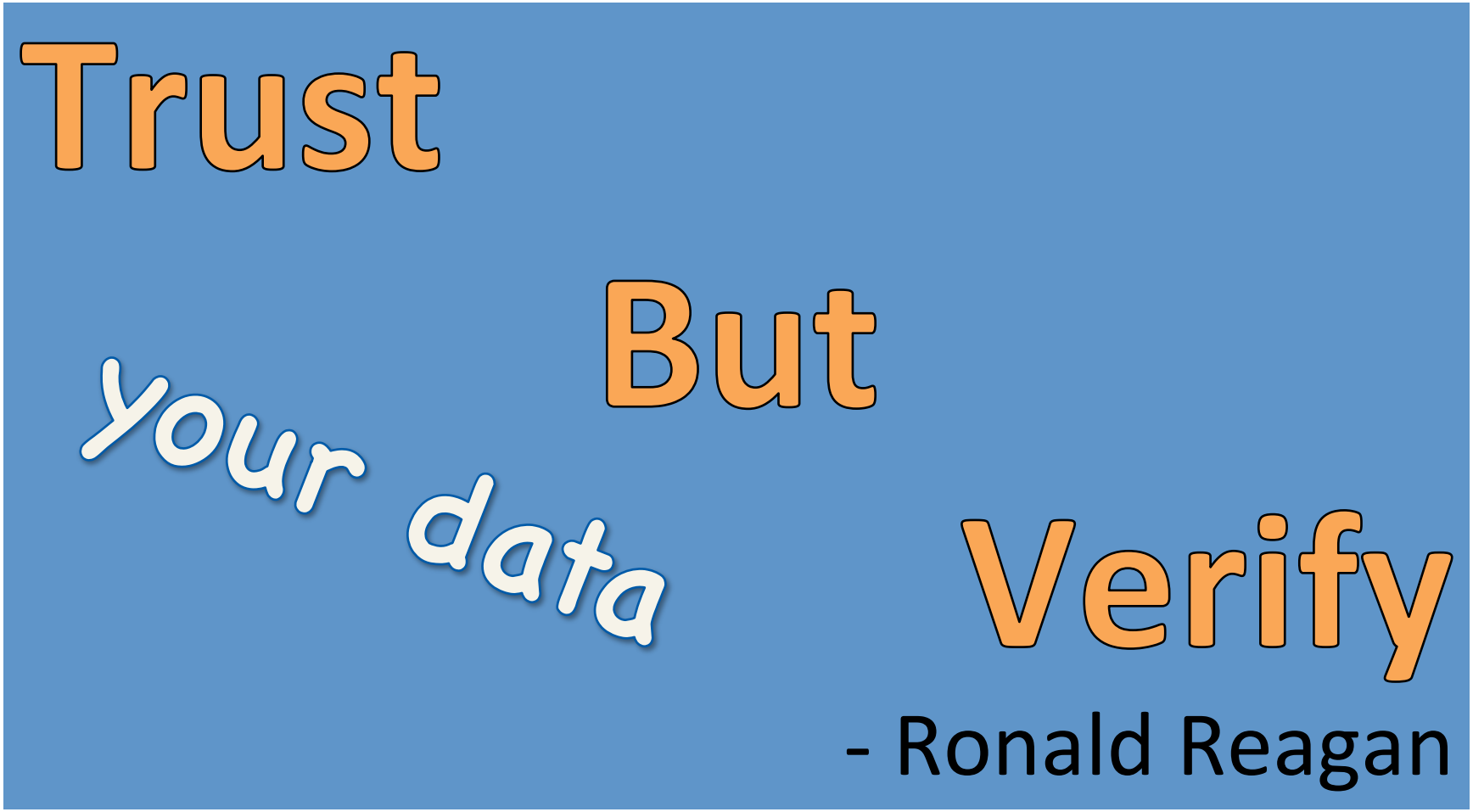
ECC ON EVERYTHING

Mitigations

Pre-Register Domains



Mitigations



Future Research

June 20, 2011
For Immediate Rele

DEF.CON ?

ICANN Approves Historic Change to Internet's Domain Name System

Plan to Launch New Generic Top-Level Domains Is Approved in Singapore

Special Thanks

Robert Edmonds

Paul Royal

Aaron LeMasters

Raytheon Rosslyn Office

Patient and Supportive Reviewers

Defcon 19 Staff

Image Attribution

- Slide 2: LOLPWND Plate © by Eli Christman. Flickr User: Gamma Man
- Slide 3: Earth © by NASA
- Slide 4: Logos © their respective owners
- Slide 5: Childrens Blocks © by Flickr User: lobo235
- Slide 6: Dollar bills © by Flickr User: Images_of_Money
- Slide 11: HAL 9000 © Warner Brothers Pictures
- Slide 15: Man replacing ENIAC Vacuum Tubes © US Army
- Slide 16: Eniac Vacuum Tubes © Erik Pitti. Flickr User: epitti.
- Slide 17: MITS Altair RAM board image © 2005 George M. Phillips Jr.
- Slide 18: Sun UltraSparc II Processor © by Konstantin Lanzet. Wikimedia user: Appaloosa
- Slide 20: Fighting with RAM © by Flickr User: elecnix
- Slide 21: Gate with no fence © by Flickr User: apasciuto
- Slide 22: Heat Lamp. "Using memory errors to attack a virtual machine" by Govindavajhala and Appel, IEEE S&P 2003
- Slide 23: Smart Cards © by Hywel Clatworthy. Wikimedia user: Dacs
- Slide 24: Parity Check Error. Self.
- Slide 25: Desert Sun © by Flickr User: Steve & Jemma Copley
- Slide 28: Backup Power © by David Robinson. Flickr User: dgrobinson
- Slide 29: Fake Capacitor. Found on Internet, likely from chinauser.cn
- Slide 30: Homunculus Nebula © by NASA
- Slide 42: Mystery Box © by Flickr User: TEDxNJLibraries
- Slide 33: DRAM. Self
- Slide 34: RAM © by Flickr User: comedy_nose
- Slide 35: SAS Drive. Self
- Slide 37: BSOD © by Wayne Williamson. Flickr User: ka3vo
- Slide 38: Blue Marble. NASA
- Slide 39: Error at airport. Self.
- Slide 51,57: Farmville Ice Cream © Flickr User: Urban Hippie Love
- Slide 59: Poison © Flickr User: shawnzrossi
- Slide 72: No Name Road © Flickr User: NatalieMaynor
- Slide 79: Contents May Creep © Flickr User: CursedThing
- Slide 86: Chain © Max Klingensmith. Flickr User: mklingo

Bitsquat Identification Tool

http://www.dinaburg.org