Understanding & Unlocking the Power of Apple's BSM Auditing System

Understanding & Unlocking the Power of Apple's BSM Auditing System

Todd Heberlein
Net Squared, Inc.

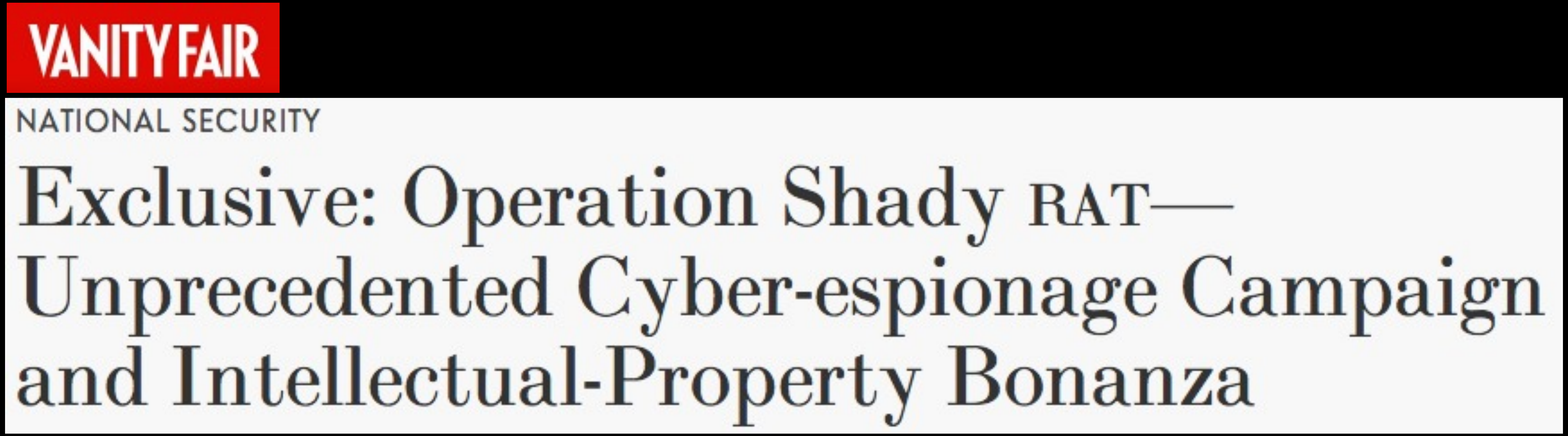
Roadmap of Talk

- Why you need to consider audit trails (instill fear)
- Introduction to Apple's BSM Auditing System (into the weeds)
- Using BSM for detection and forensics (really, it can be very useful)

Act 1: Why You Need Auditing

Act 1: Why You Need Auditing

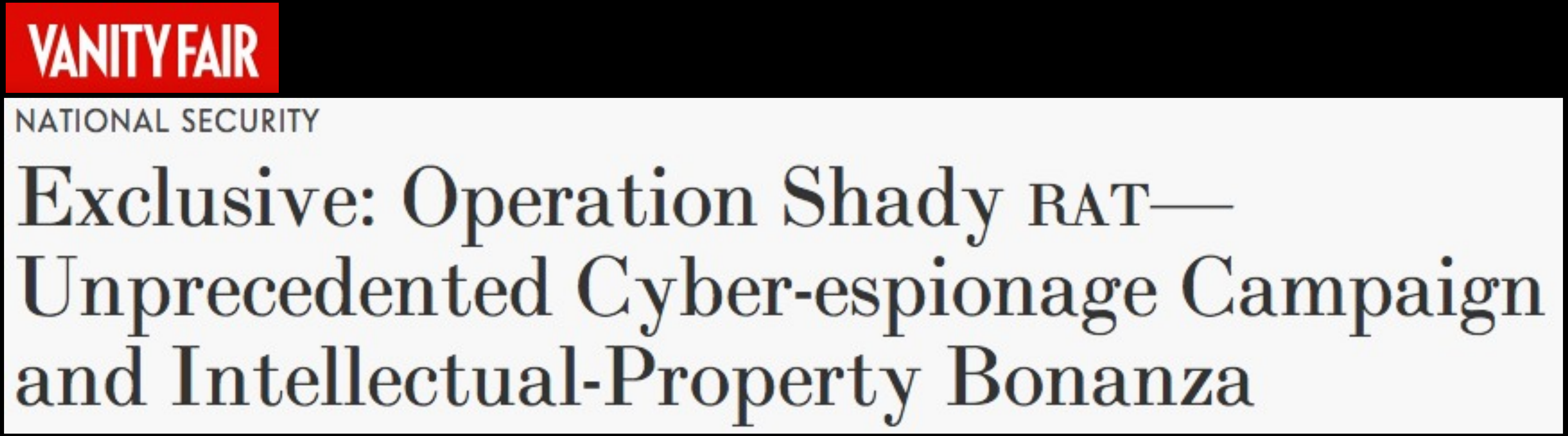
Instill fear



VANITY FAIR

NATIONAL SECURITY

Exclusive: Operation Shady RAT—Unprecedented Cyber-espionage Campaign and Intellectual-Property Bonanza

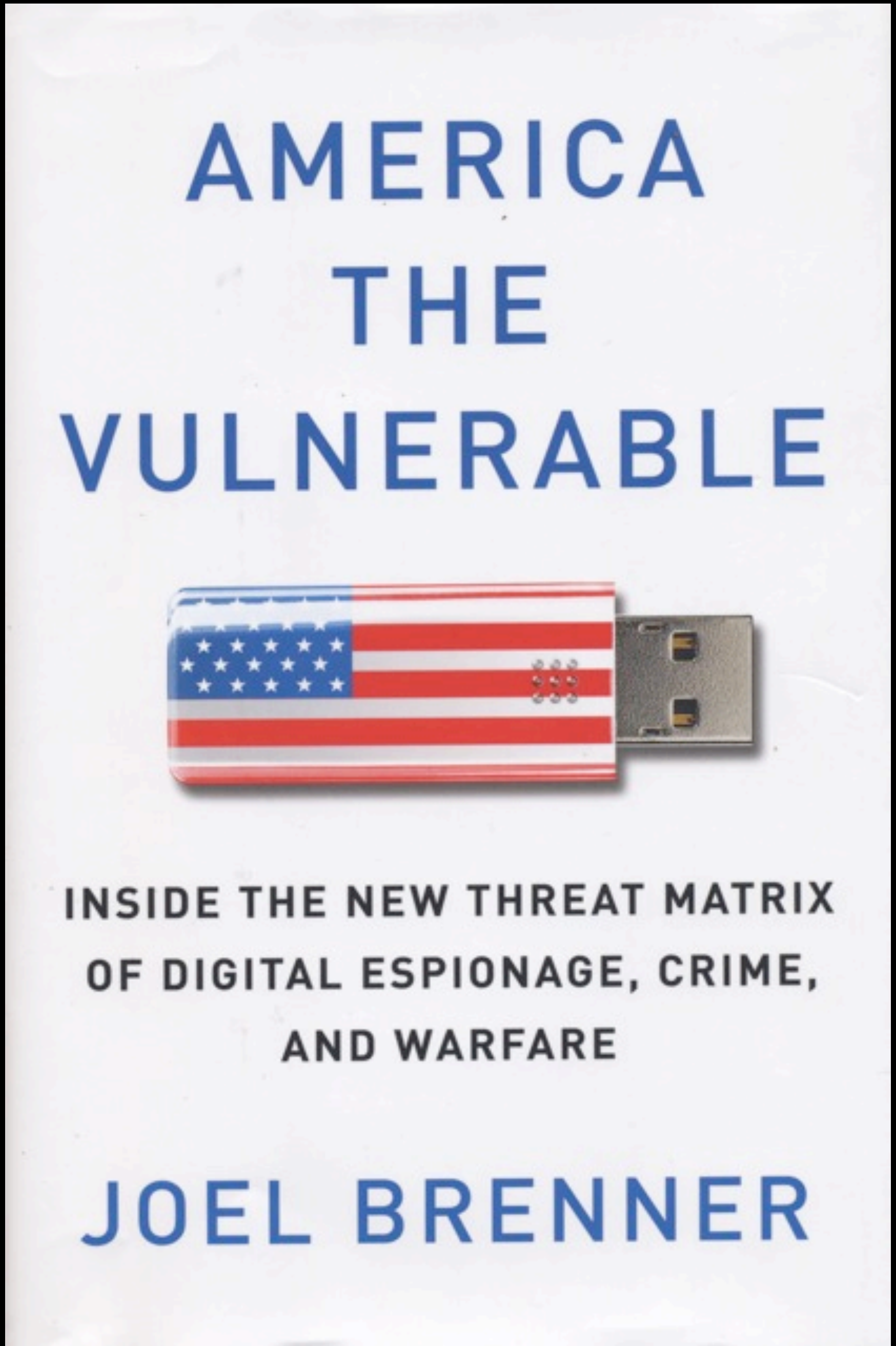


VANITY FAIR

NATIONAL SECURITY

Exclusive: Operation Shady RAT—Unprecedented Cyber-espionage Campaign and Intellectual-Property Bonanza

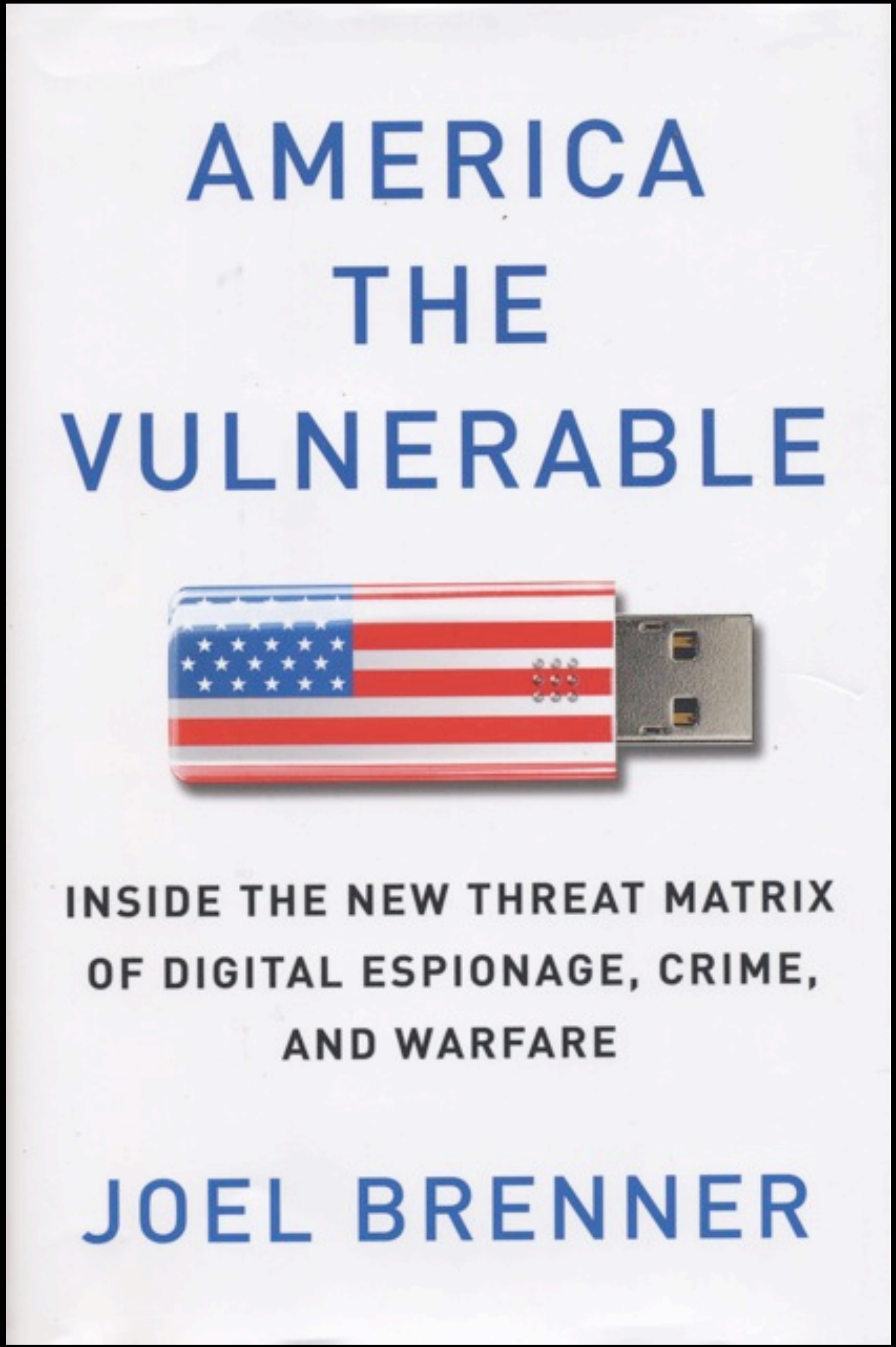
For at least five years, a high-level hacking campaign—dubbed Operation Shady rat—has infiltrated the computer systems of national governments, global corporations, nonprofits, and other organizations, with more than 70 victims in 14 countries. Lifted from these highly secure servers, among other sensitive property: countless government secrets, e-mail archives, legal contracts, and design schematics.



AMERICA THE VULNERABLE

INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE

JOEL BRENNER

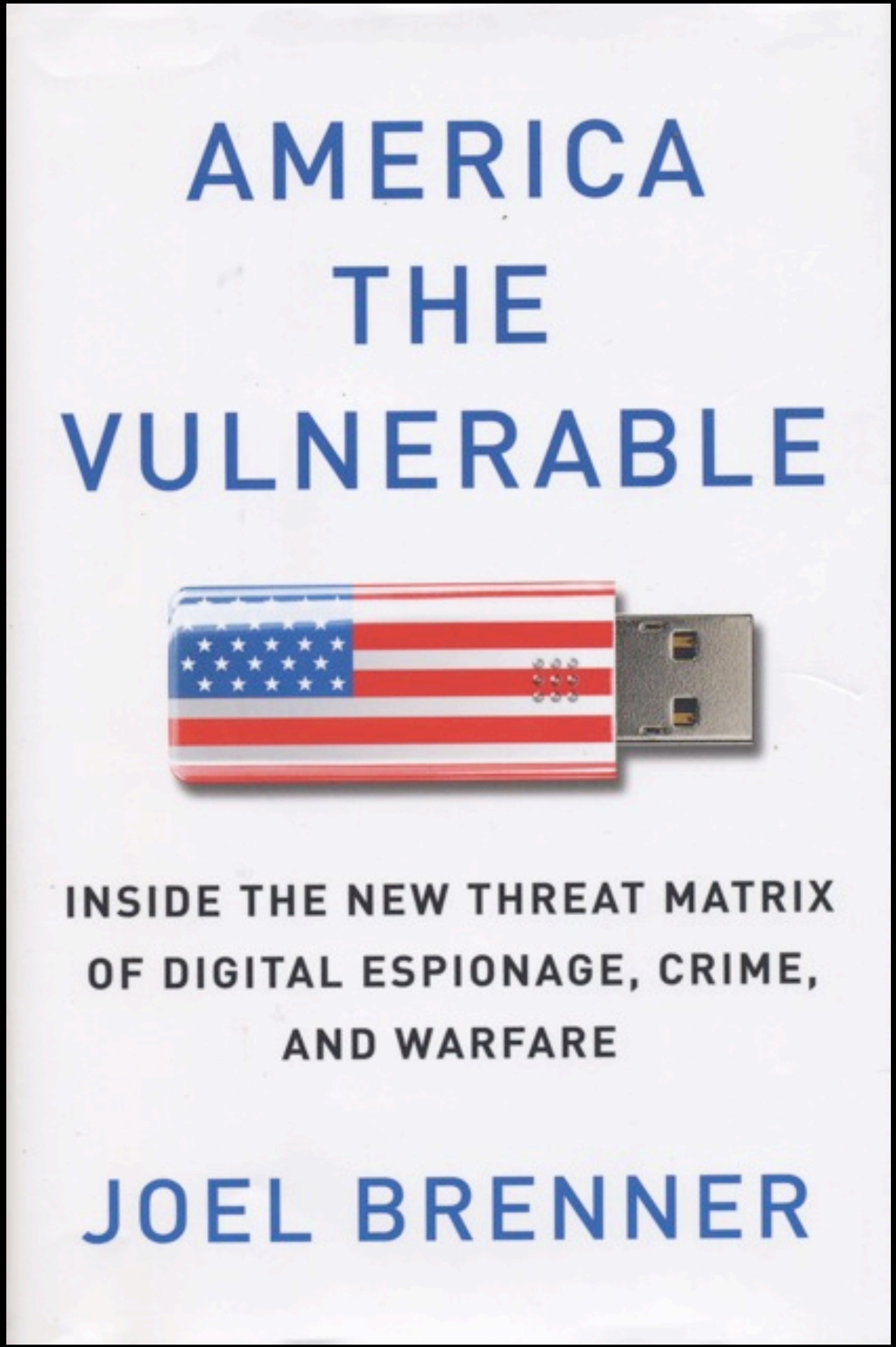


AMERICA THE VULNERABLE

INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE

JOEL BRENNER

In August 2006, Major General William Lord of the air force let the public in on the secret when he mentioned that massive heist of up to twenty terabytes.

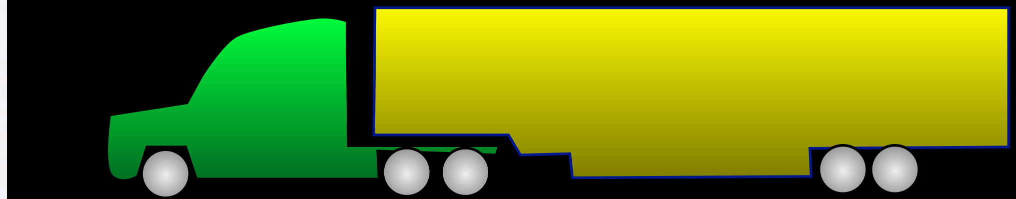


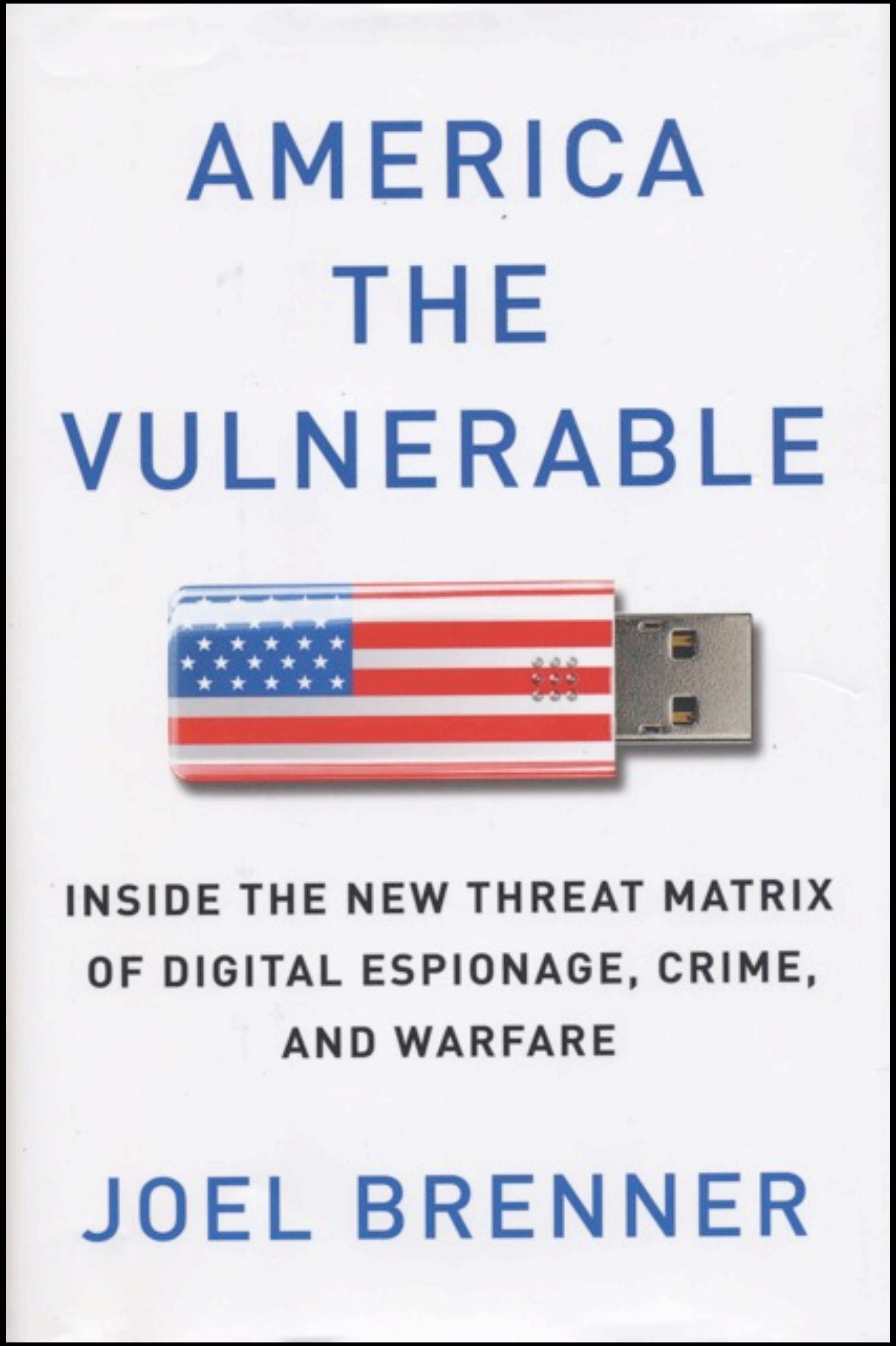
AMERICA THE VULNERABLE

INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE

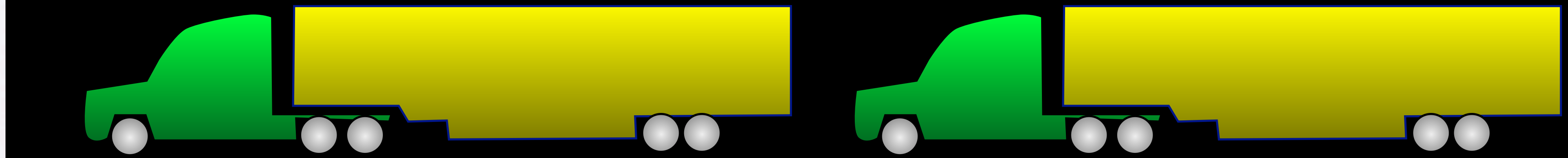
JOEL BRENNER

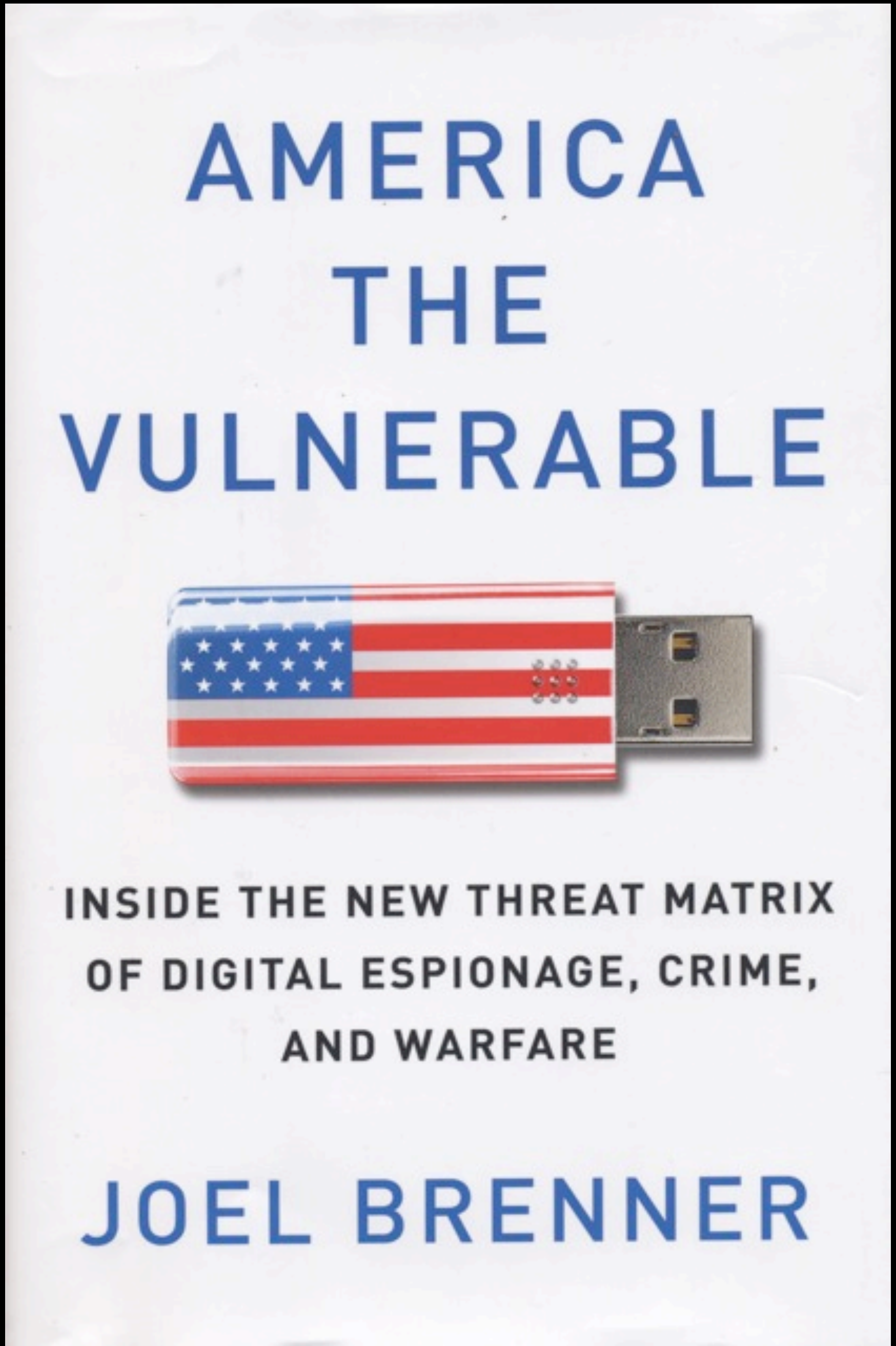
In August 2006, Major General William Lord of the air force let the public in on the secret when he mentioned that massive heist of up to twenty terabytes.




AMERICA THE VULNERABLE
INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE
JOEL BRENNER

In August 2006, Major General William Lord of the air force let the public in on the secret when he mentioned that massive heist of up to twenty terabytes.

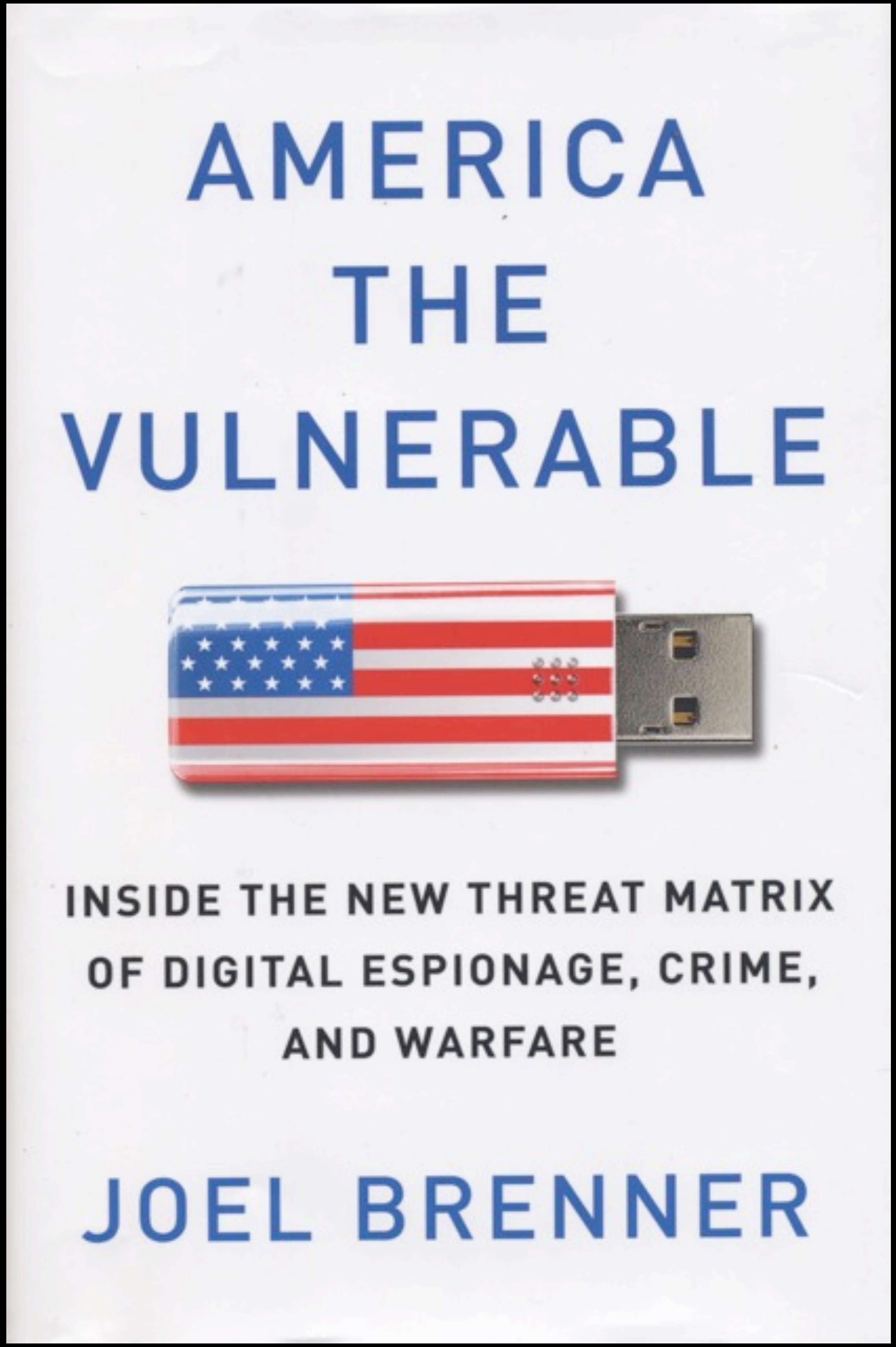




AMERICA THE VULNERABLE

INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE

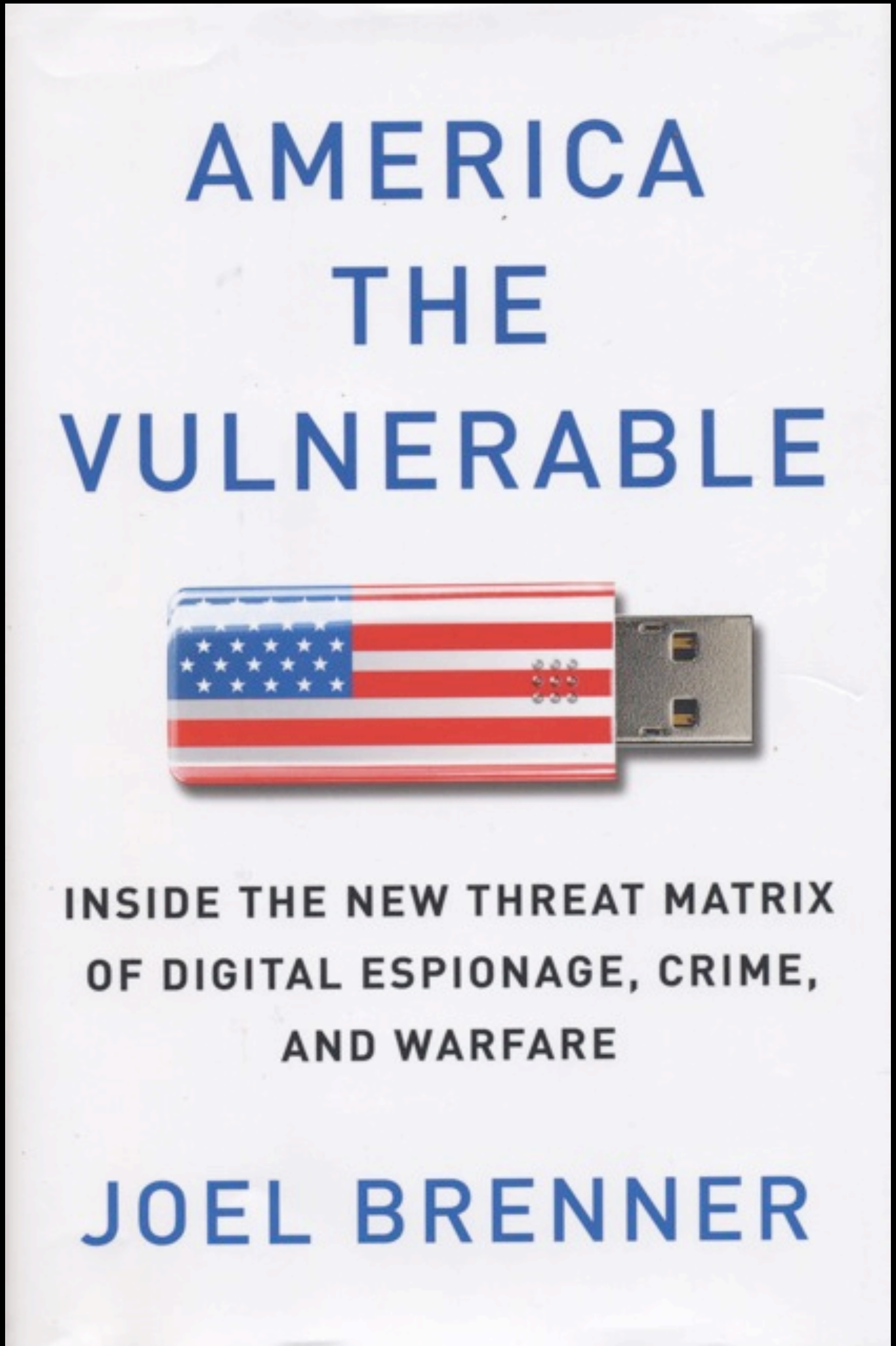
JOEL BRENNER



AMERICA THE VULNERABLE

INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE

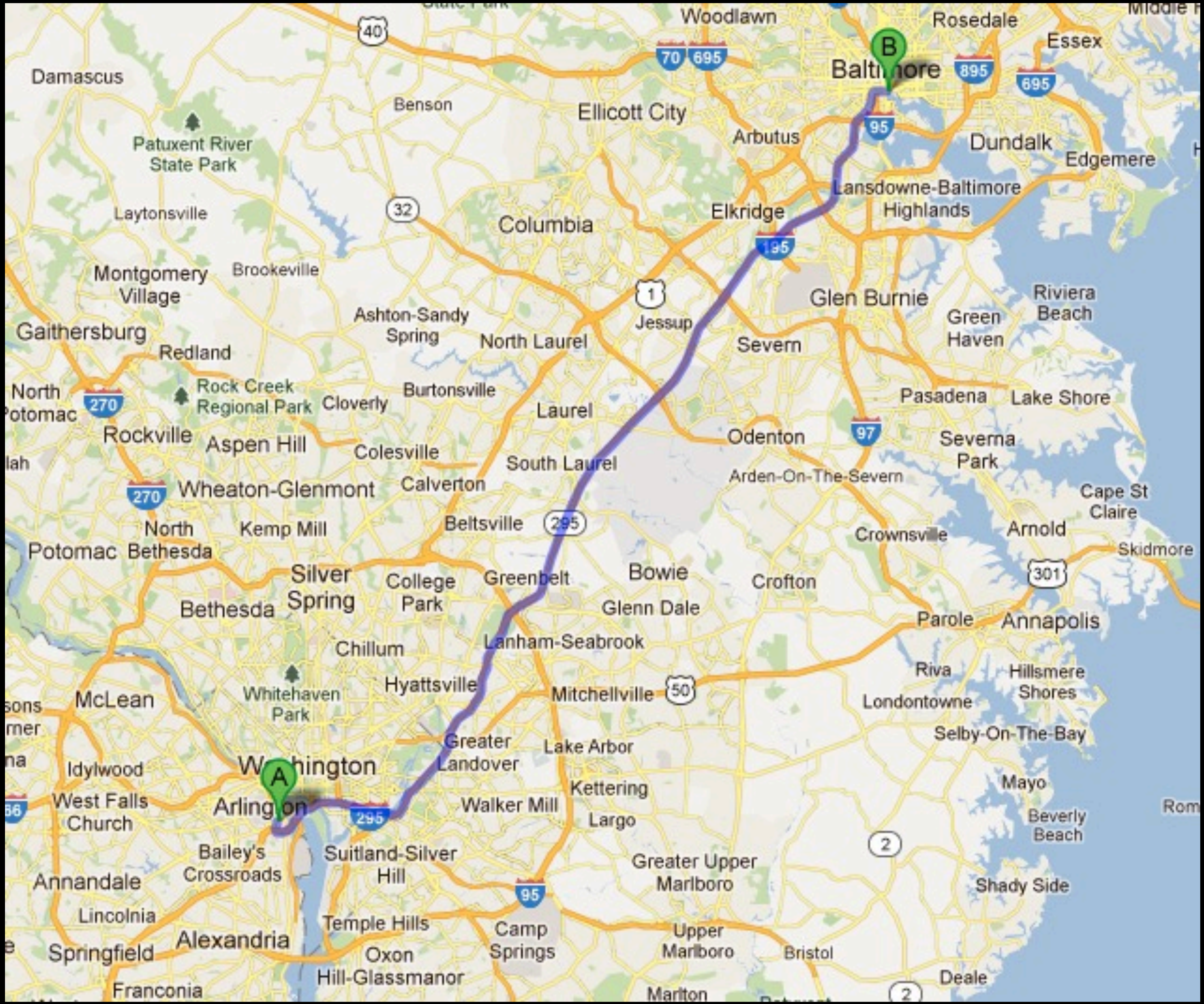
JOEL BRENNER

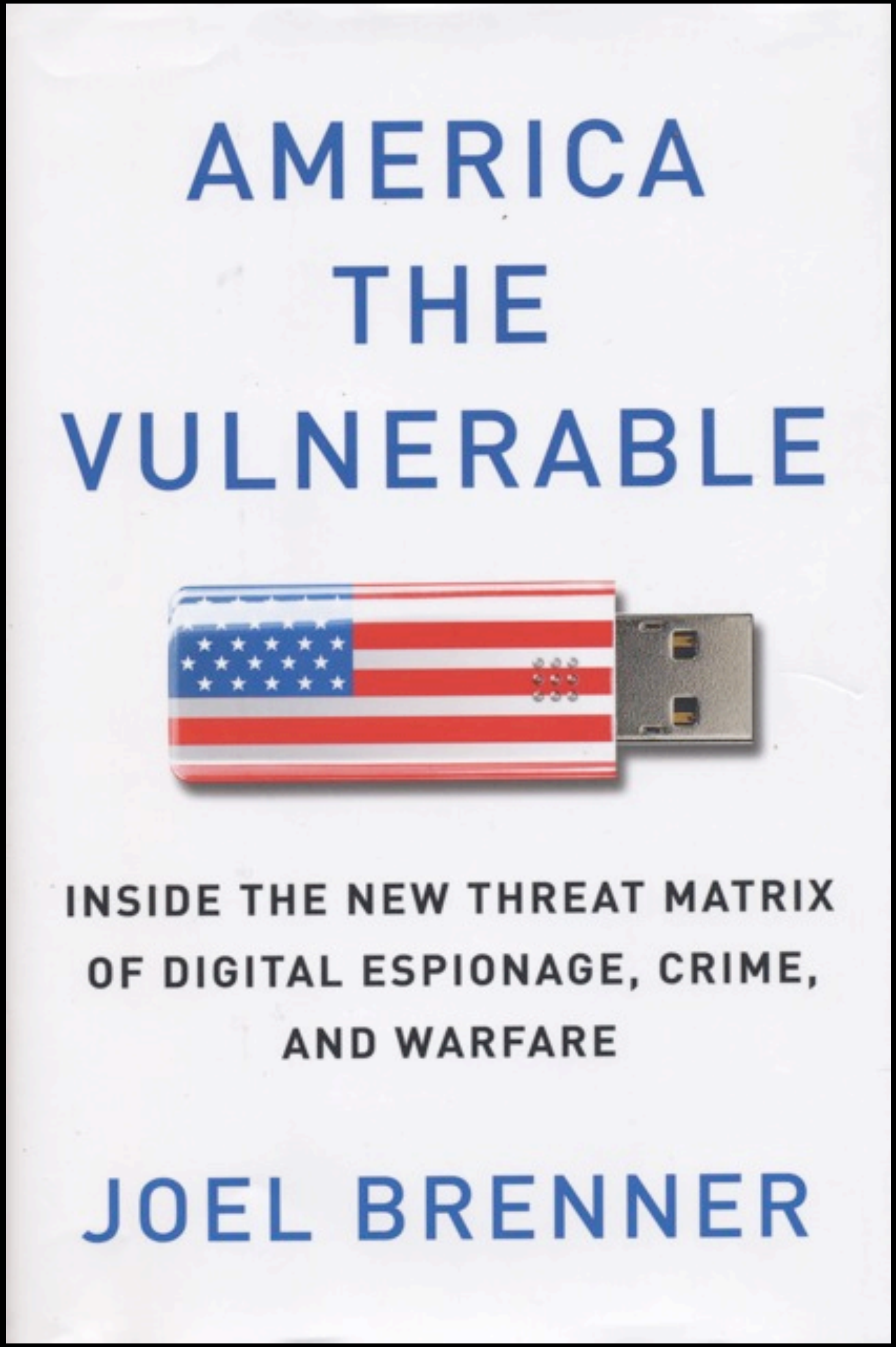


AMERICA THE VULNERABLE

INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE

JOEL BRENNER

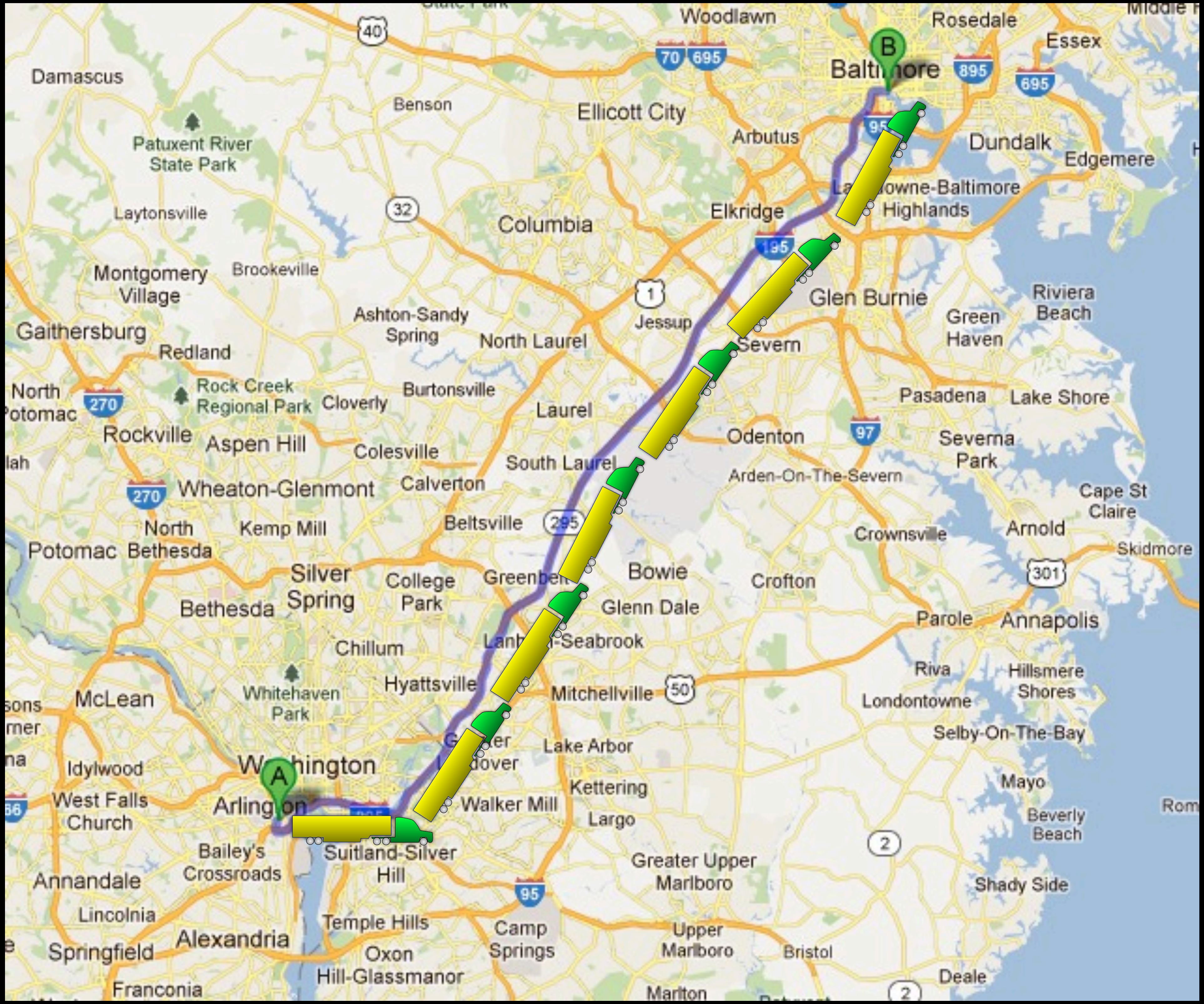




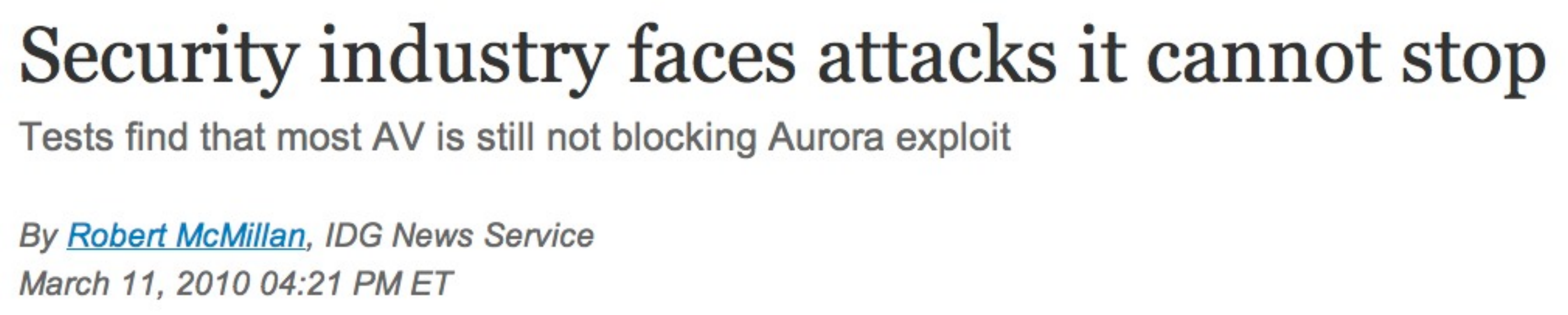
AMERICA THE VULNERABLE

INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE

JOEL BRENNER



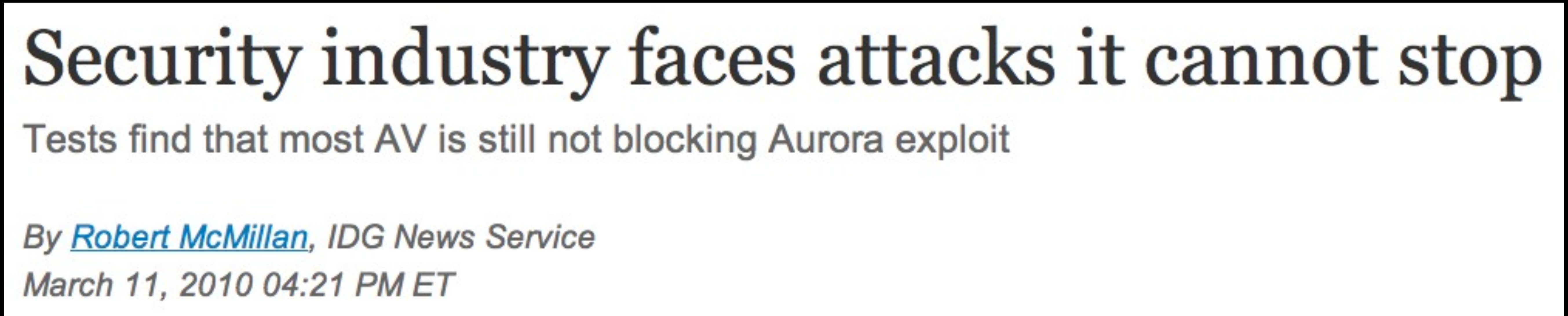
Failure of Existing Technology



Security industry faces attacks it cannot stop

Tests find that most AV is still not blocking Aurora exploit

By Robert McMillan, IDG News Service
March 11, 2010 04:21 PM ET

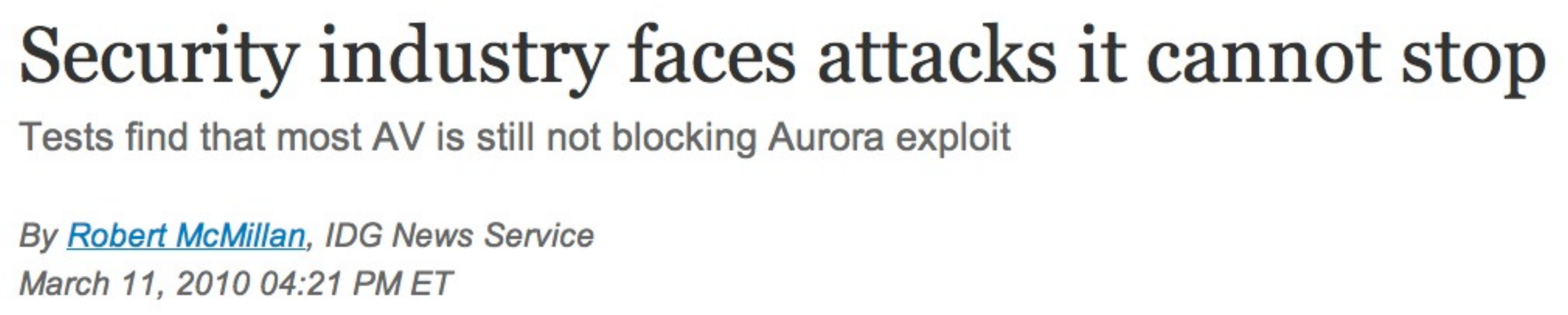


Security industry faces attacks it cannot stop

Tests find that most AV is still not blocking Aurora exploit

By Robert McMillan, IDG News Service
March 11, 2010 04:21 PM ET

> Traditional security products are simply not much help against APT attacks. … All of the victims we've worked with had perfectly installed antivirus. … They all had intrusion detection systems and several had Web proxies scan content.
>
> – Alex Stamos



Security industry faces attacks it cannot stop

Tests find that most AV is still not blocking Aurora exploit

By Robert McMillan, IDG News Service
March 11, 2010 04:21 PM ET

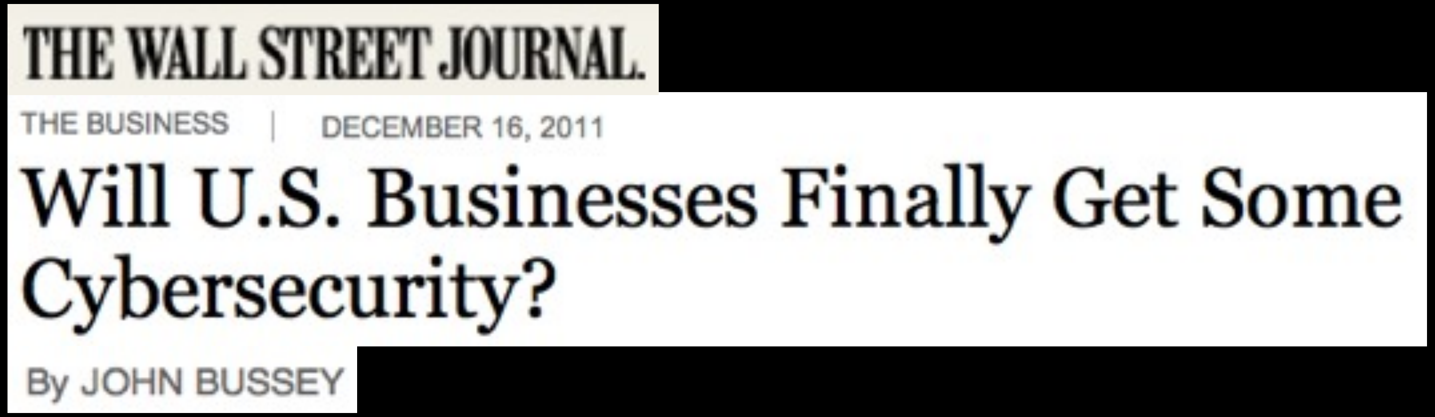
The security industry [is] going to have to think about selling solutions that actually work with this type of environment. Basically nothing that people have bought over the last 16 years is going to help.

– Alex Stamos

Why Are They Failing?

Symantec estimates about 55,000 new malware created each day

Symantec estimates about 55,000 new malware created each day

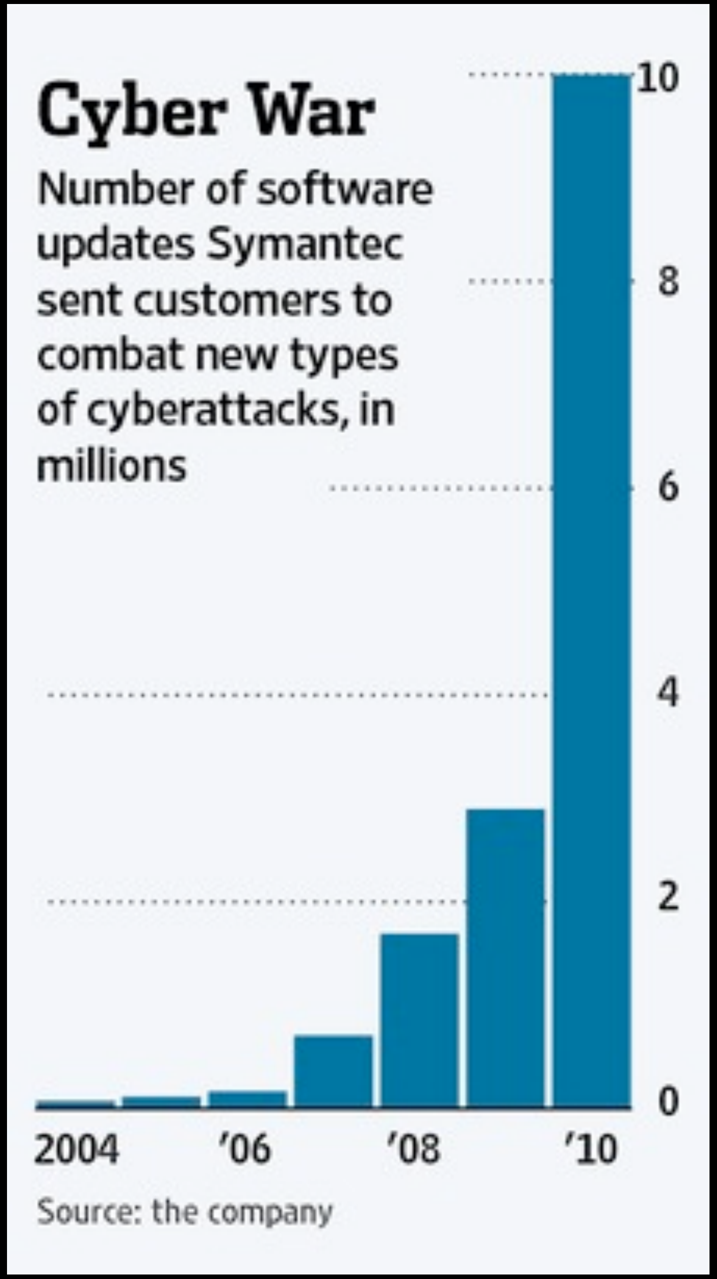


THE WALL STREET JOURNAL.

THE BUSINESS | DECEMBER 16, 2011

Will U.S. Businesses Finally Get Some Cybersecurity?

By JOHN BUSSEY

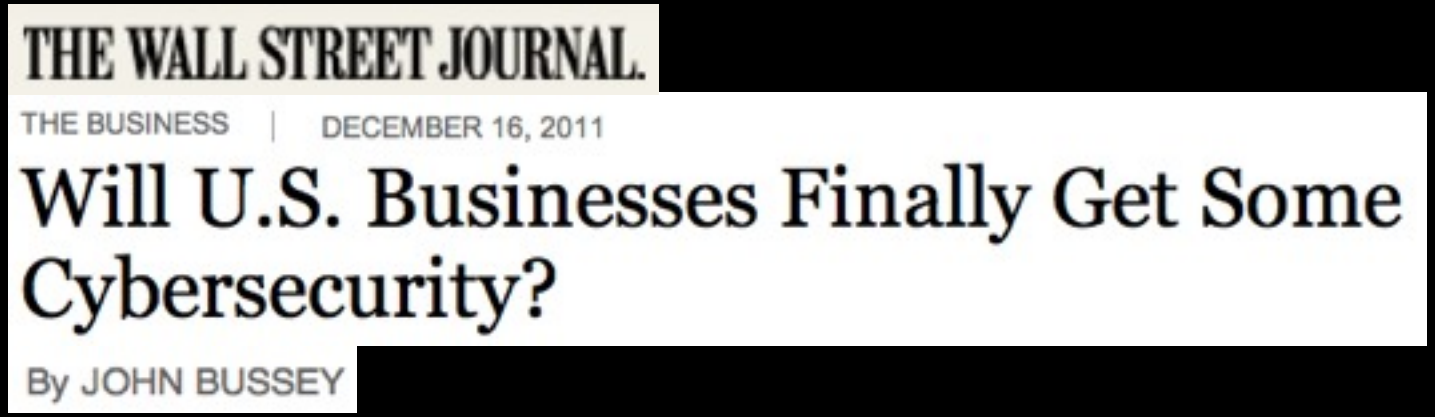


Cyber War

Number of software updates Symantec sent customers to combat new types of cyberattacks, in millions

Source: the company

Symantec estimates about 55,000 new malware created each day

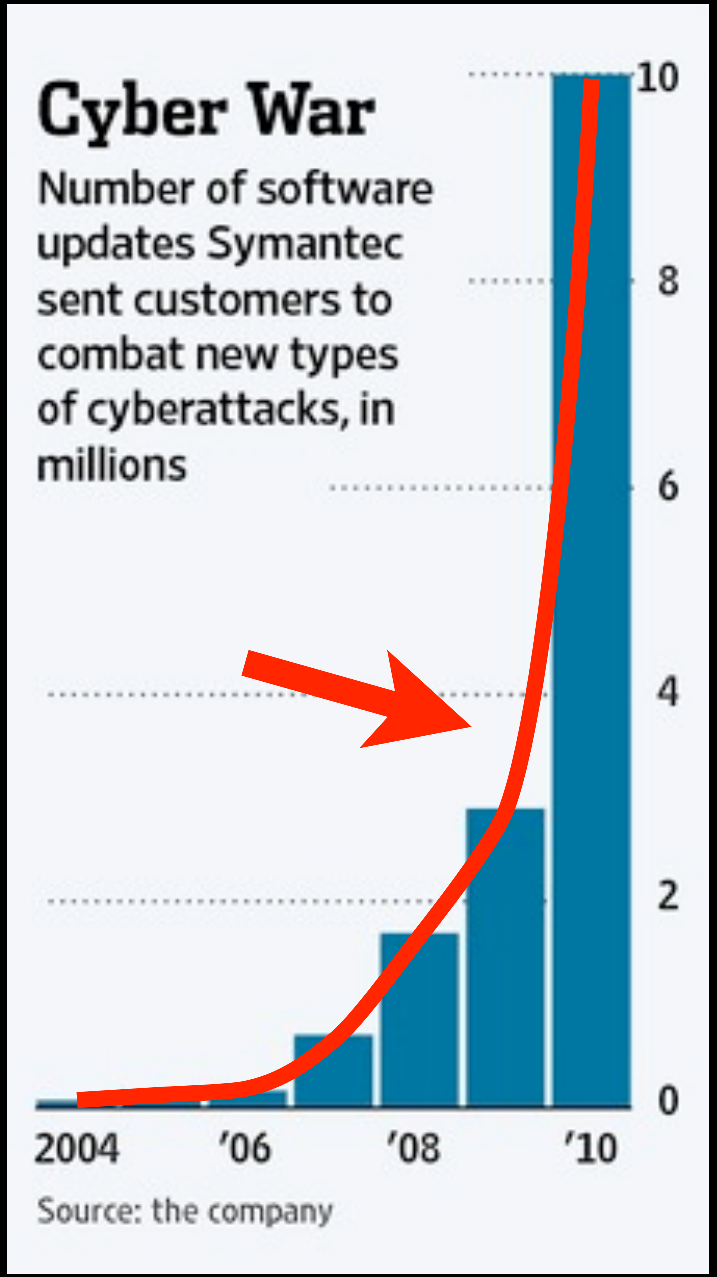


THE WALL STREET JOURNAL.

THE BUSINESS | DECEMBER 16, 2011

Will U.S. Businesses Finally Get Some Cybersecurity?

By JOHN BUSSEY



Cyber War

Number of software updates Symantec sent customers to combat new types of cyberattacks, in millions

Source: the company

> “In our last 50 incidents, 48 of the victim companies learned they were breached from the Federal Bureau of Investigation, the Department of Defense or some other third party.”
>
> – Kevin Mandia

"In our last 50 incidents, 48 of the victim companies learned they were breached from the Federal Bureau of Investigation, the Department of Defense or some other third party."

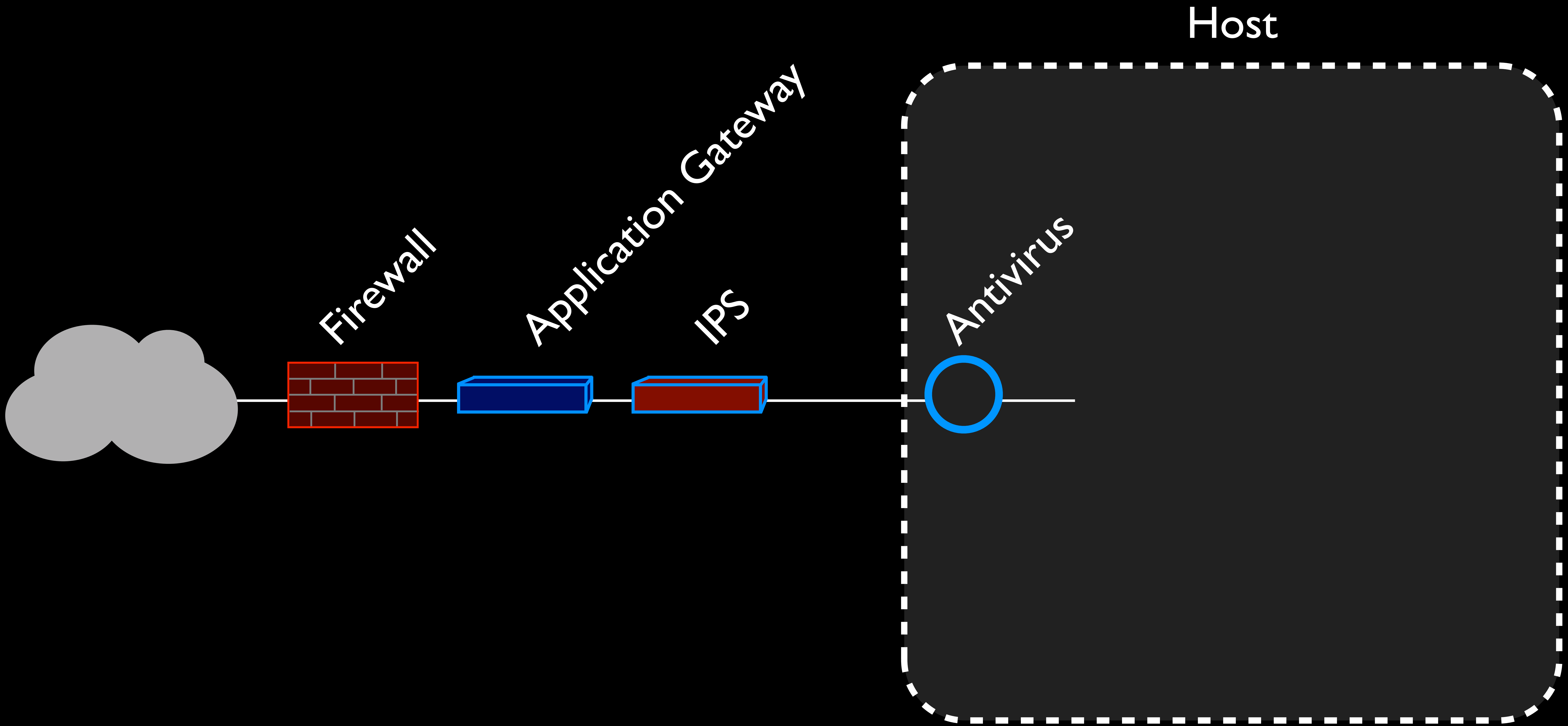
– Kevin Mandia

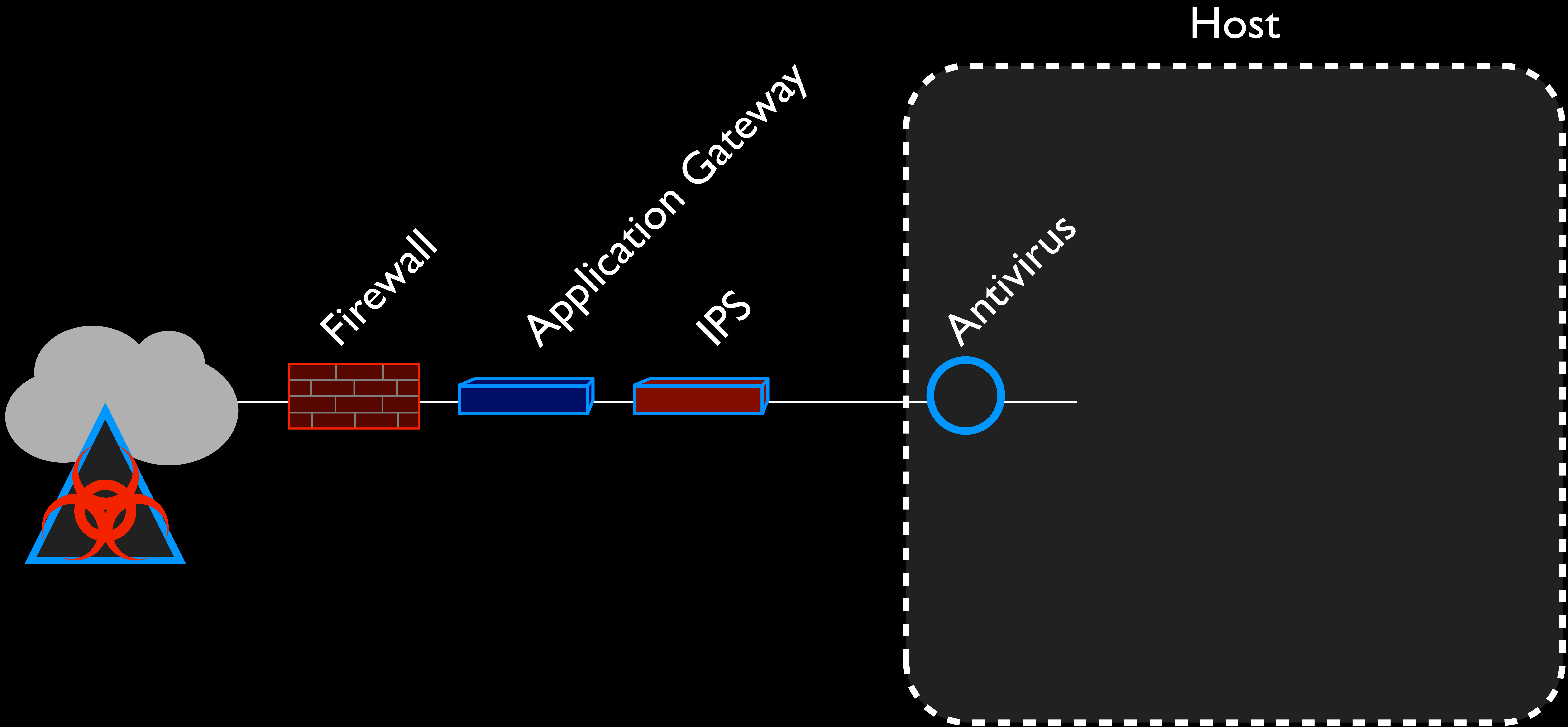
Are you a member of the 96 percent?

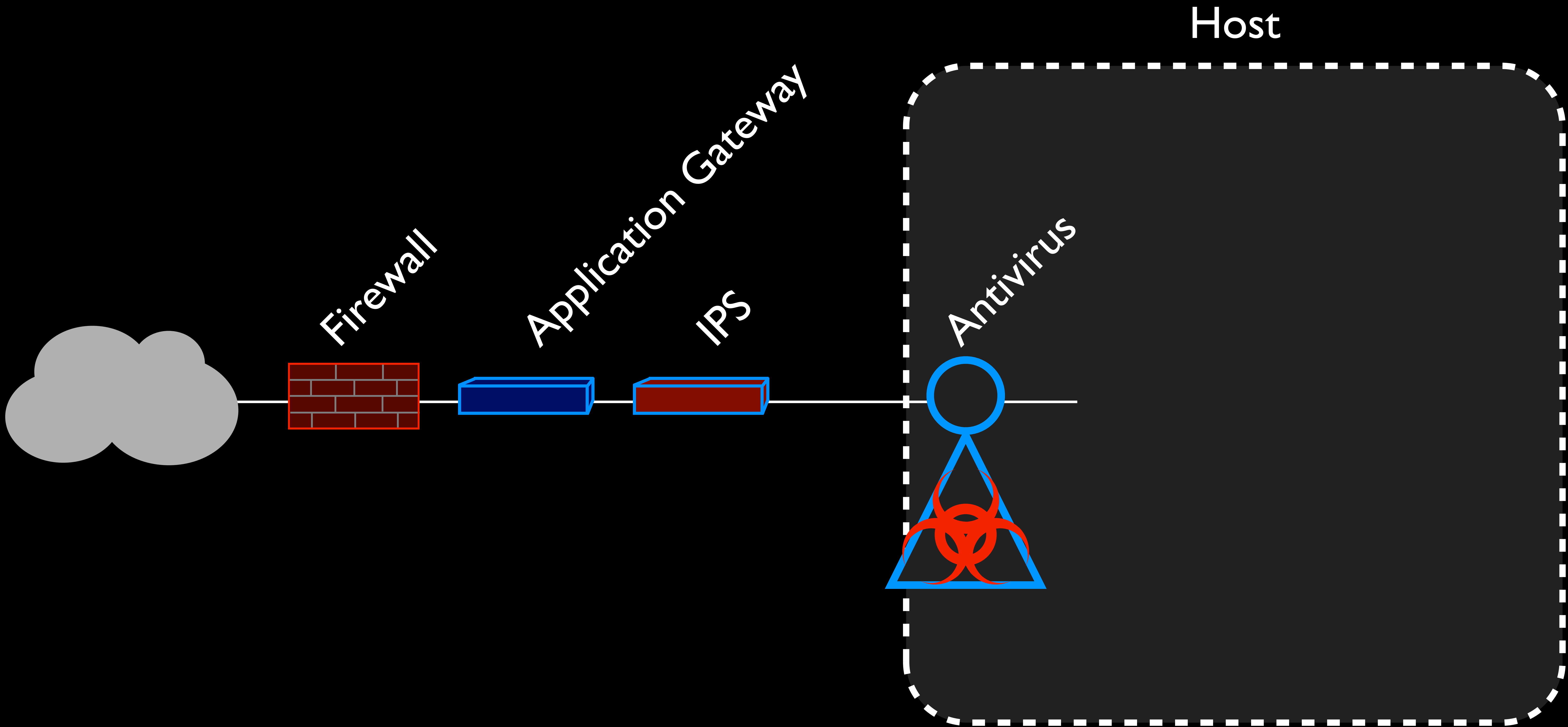
“Signature-based malware detection has been limping along on life support for years”

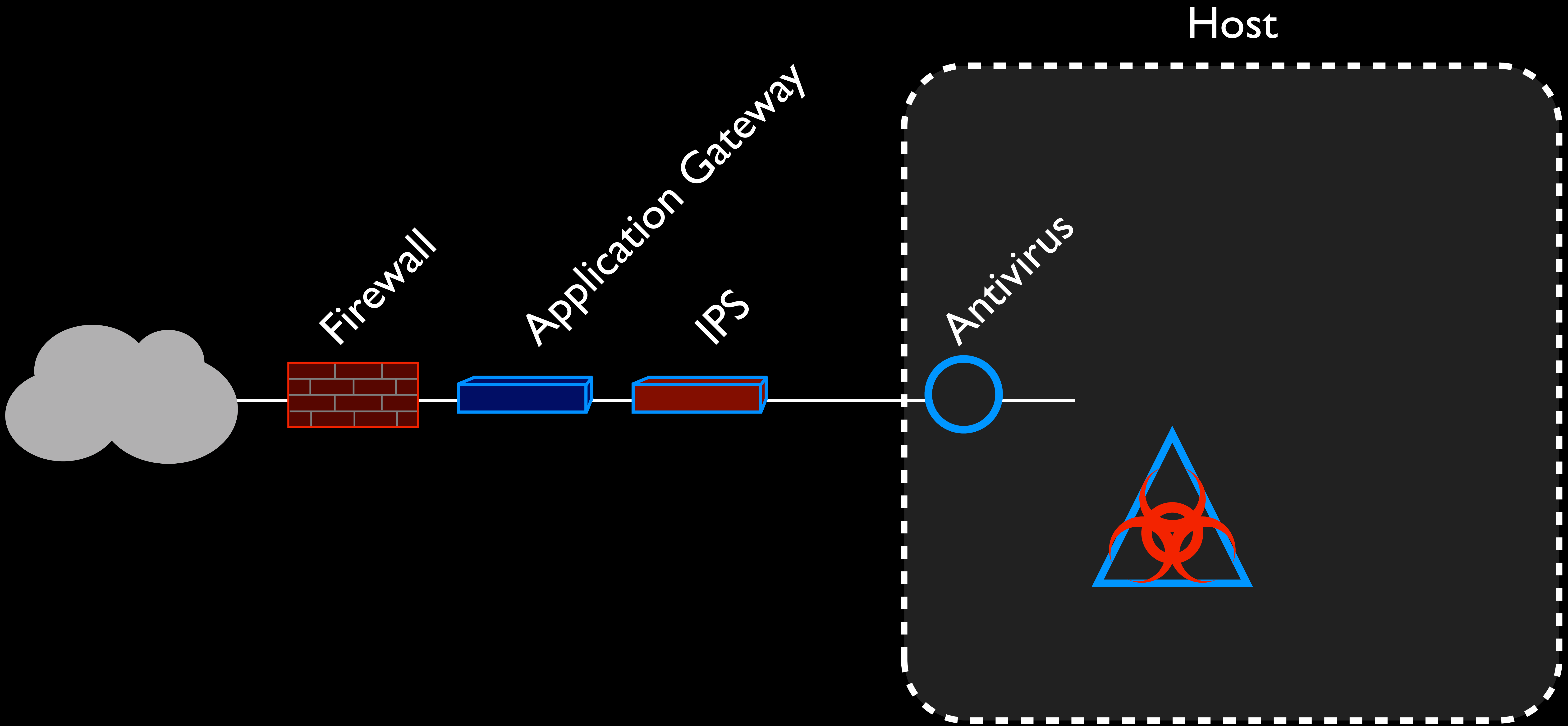
– Gartner research note

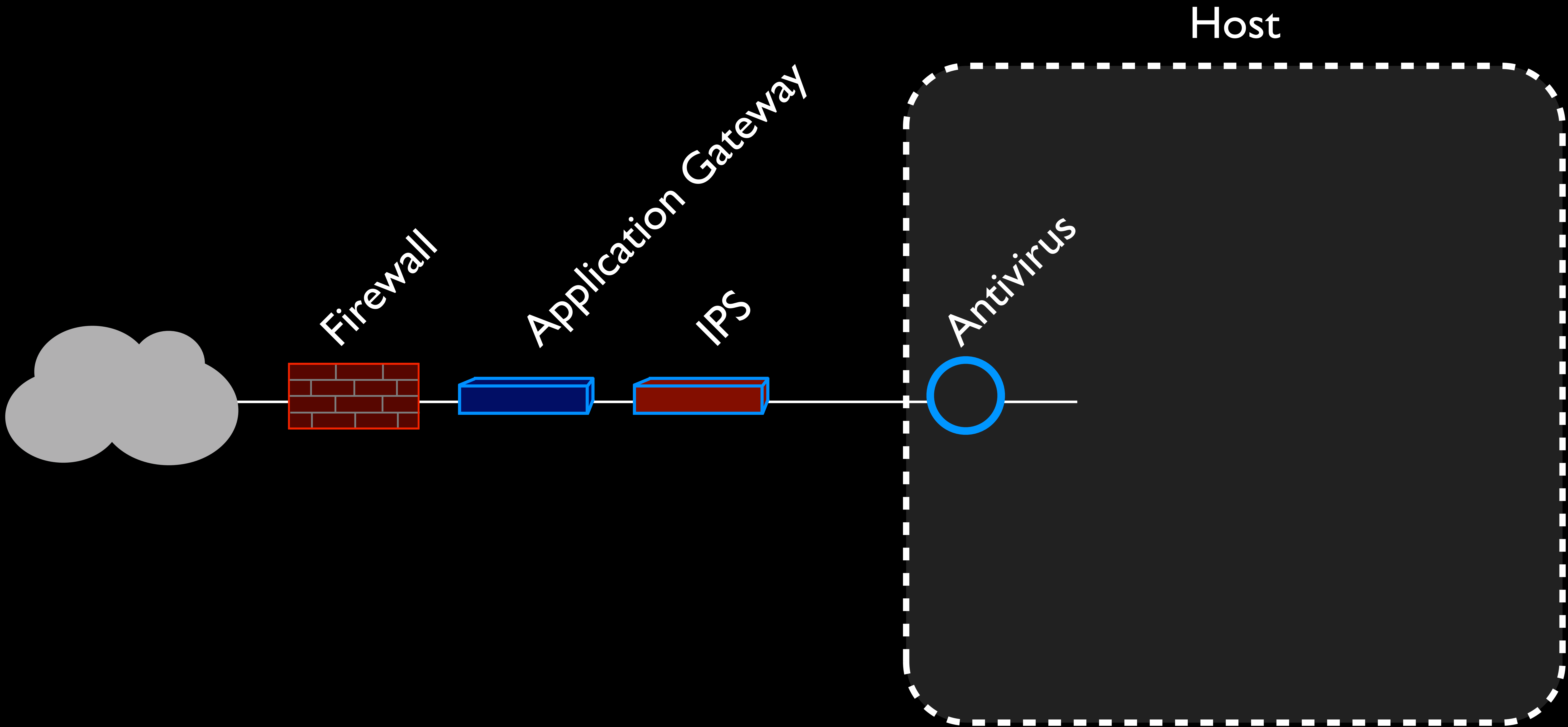
Typical Security Architecture


Host
Firewall
Application Gateway
IPS
Antivirus

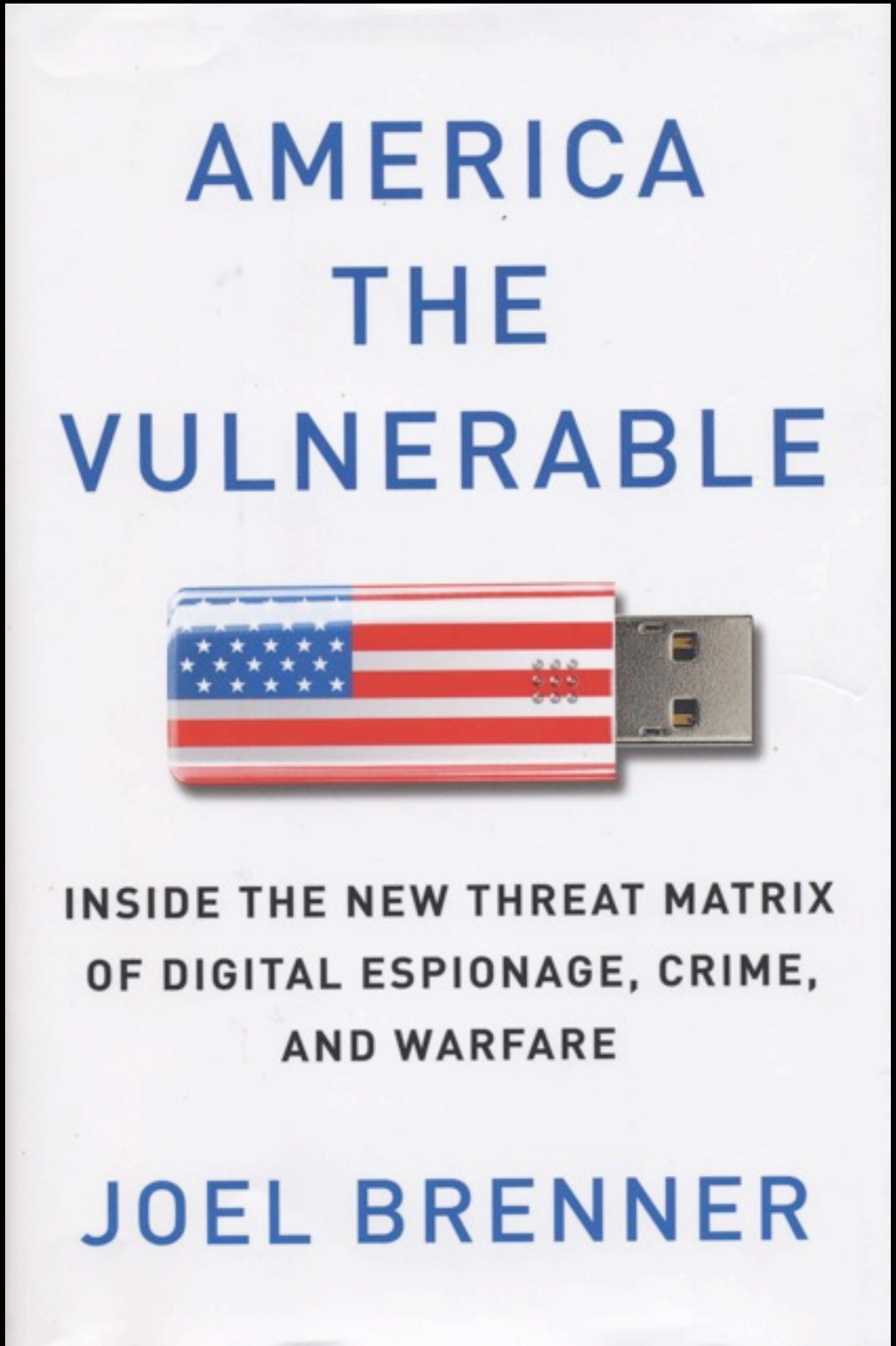

Host
Firewall
Application Gateway
IPS
Antivirus


Firewall
Application Gateway
IPS
Antivirus
Host


Host
Firewall
Application Gateway
IPS
Antivirus


Firewall
Application Gateway
IPS
Antivirus
Host

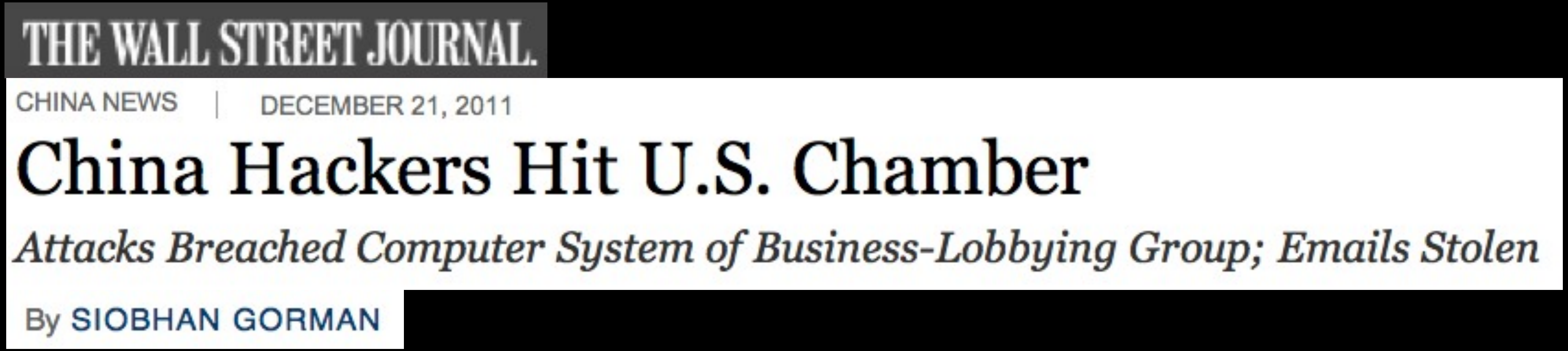
In the Dark


AMERICA THE VULNERABLE

INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE

JOEL BRENNER

We don’t know exactly what data were taken ... the Chinese, on their way out the electronic door, did encrypt [the data].



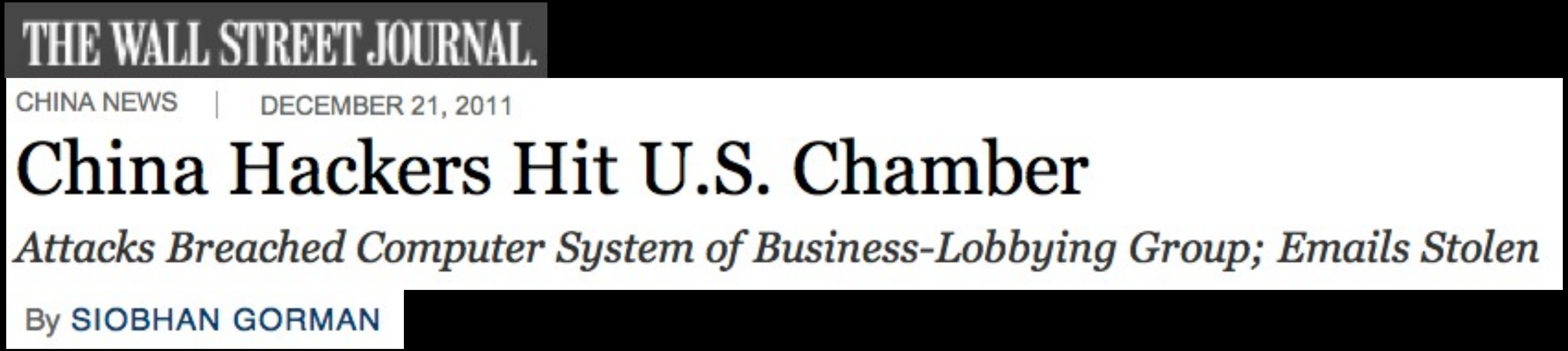
THE WALL STREET JOURNAL.

CHINA NEWS | DECEMBER 21, 2011

China Hackers Hit U.S. Chamber

Attacks Breached Computer System of Business-Lobbying Group; Emails Stolen

By SIOBHAN GORMAN



THE WALL STREET JOURNAL.

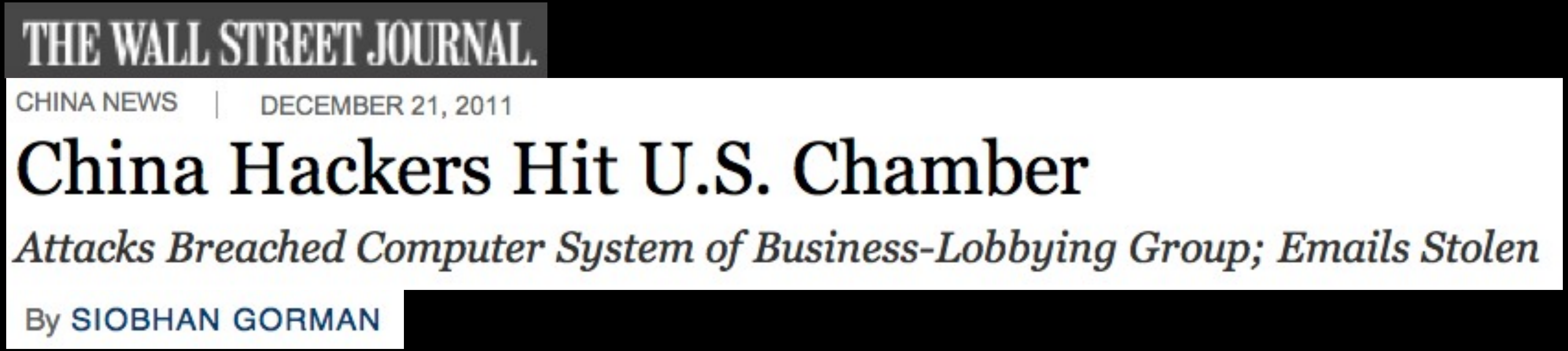
CHINA NEWS | DECEMBER 21, 2011

China Hackers Hit U.S. Chamber

Attacks Breached Computer System of Business-Lobbying Group; Emails Stolen

By SIOBHAN GORMAN

"The Chamber learned of the break-in when the Federal Bureau of Investigation told the group that servers in China were stealing its information"



THE WALL STREET JOURNAL.

CHINA NEWS | DECEMBER 21, 2011

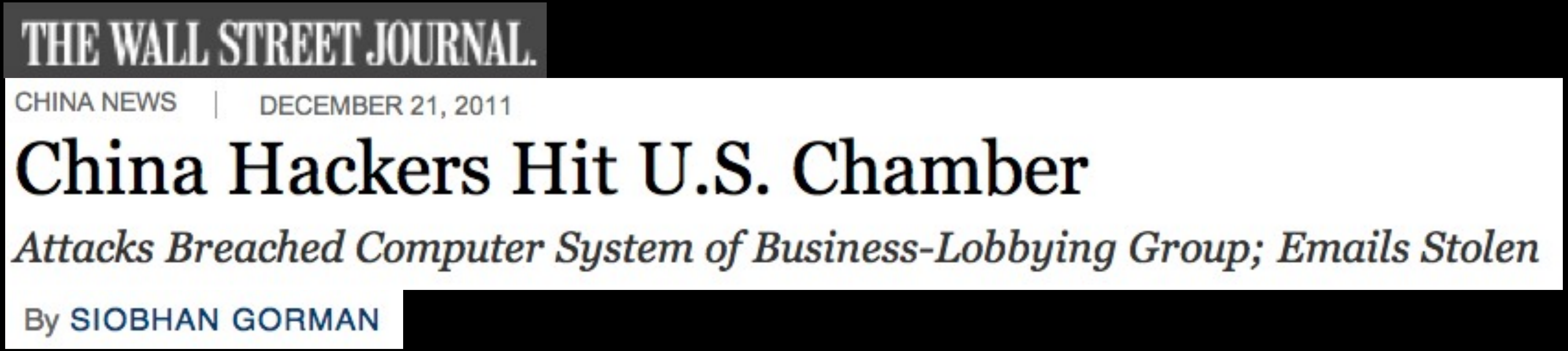
China Hackers Hit U.S. Chamber

Attacks Breached Computer System of Business-Lobbying Group; Emails Stolen

By SIOBHAN GORMAN

"The Chamber learned of the break-in when the Federal Bureau of Investigation told the group that servers in China were stealing its information"

"It isn't clear exactly how the hackers broke in to the Chamber's systems. Evidence suggests they were in the network at least from November 2009 to May 2010."



THE WALL STREET JOURNAL.

CHINA NEWS | DECEMBER 21, 2011

China Hackers Hit U.S. Chamber

Attacks Breached Computer System of Business-Lobbying Group; Emails Stolen

By SIOBHAN GORMAN

“The Chamber learned of the break-in when the Federal Bureau of Investigation told the group that servers in China were stealing its information”

“It isn't clear exactly how the hackers broke in to the Chamber's systems. Evidence suggests they were in the network at least from November 2009 to May 2010.”

“People familiar with the Chamber investigation said it has been hard to determine what was taken before the incursion was discovered” ars technica

Symantec suspected source code breach back in 2006

By Jon Brodkin | Published about 10 hours ago

Symantec suspected in 2006 that its network had been breached, but the company was unable to confirm any data exfiltration until Anonymous started talking publicly about Symantec source code earlier this month.

http://arstechnica.com/business/news/2012/01/symantec-suspected-breach-in-2006-didnt-confirm-until-anonymous-revealed-source-code.ars

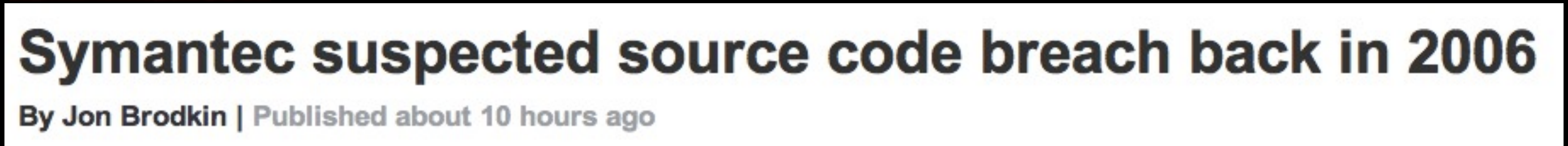
ars technica

Symantec suspected source code breach back in 2006

By Jon Brodkin | Published about 10 hours ago

Symantec spokesperson Cris Paden tells Ars that Symantec "investigated the incident in 2006 but our results were inconclusive."

http://arstechnica.com/business/news/2012/01/symantec-suspected-breach-in-2006-didnt-confirm-until-anonymous-revealed-source-code.ars



Symantec suspected source code breach back in 2006

By Jon Brodkin | Published about 10 hours ago

Symantec has told users of pcAnywhere to disable the product for now unless they simply must use it for business purposes

http://arstechnica.com/business/news/2012/01/symantec-suspected-breach-in-2006-didnt-confirm-until-anonymous-revealed-source-code.ars

But wait, I’ve got a Mac.

Java Update

17 CVEs

Multiple vulnerabilities exist in Java 1.6.0_26, the most serious of which may allow an untrusted Java applet to execute arbitrary code outside the Java sandbox. Visiting a web page containing a maliciously crafted untrusted Java applet may lead to arbitrary code execution with the privileges of the current user.

Safari 5.1.1

CVE-2011-3230

Safari:Visiting a malicious website may lead to arbitrary code execution

CVE-2011-3231

Safari:Visiting a malicious website may lead to arbitrary code execution

35 CVEs

Webkit:Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution

Security Update 2011-006

CVE-2011-3437

ATS: Viewing or downloading a document containing a maliciously crafted embedded font may lead to arbitrary code execution

CVE-2011-0229

ATS: Viewing or downloading a document containing a maliciously crafted embedded font may lead to arbitrary code execution

CVE-2011-0230

ATS: Applications which use the ATSFontDeactivate API may be vulnerable to an unexpected application termination or arbitrary code execution

Security Update 2011-006

CVE-2011-0259

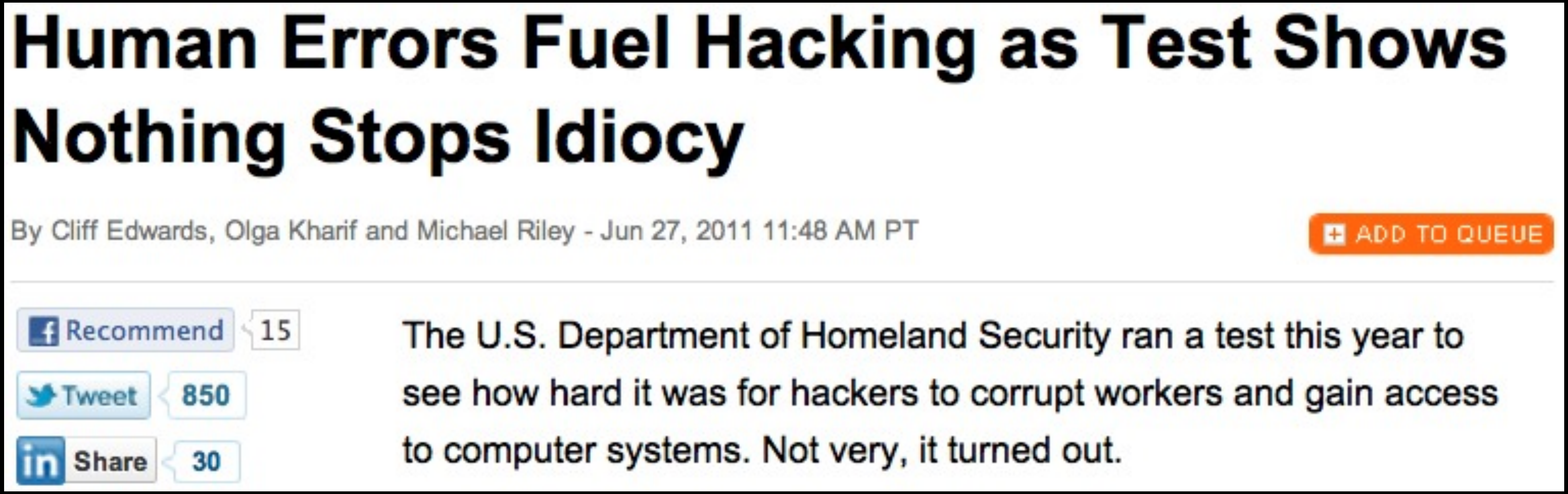
CoreFoundation:Viewing a maliciously crafted website or e-mail message may lead to an unexpected application termination or arbitrary code execution

CVE-2011-0224

CoreMedia:Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution

CVE-2011-3227

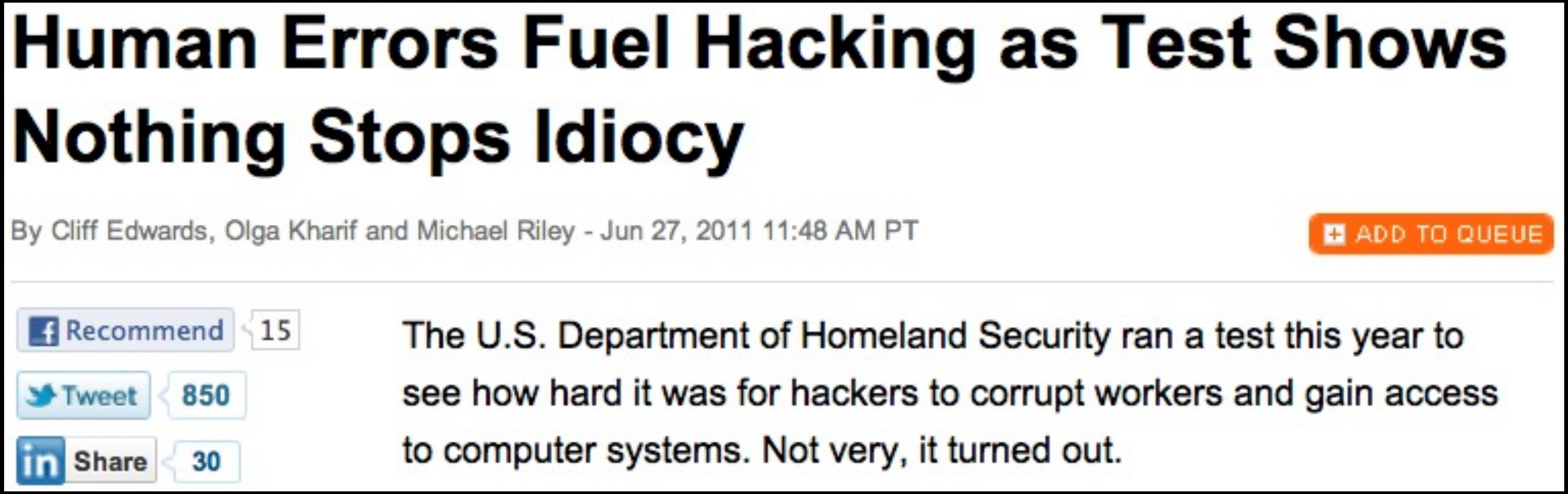
libsecurity:Viewing a maliciously crafted website or e-mail message may lead to an unexpected application termination or arbitrary code execution



Human Errors Fuel Hacking as Test Shows Nothing Stops Idiocy

By Cliff Edwards, Olga Kharif and Michael Riley - Jun 27, 2011 11:48 AM PT

The U.S. Department of Homeland Security ran a test this year to see how hard it was for hackers to corrupt workers and gain access to computer systems. Not very, it turned out.

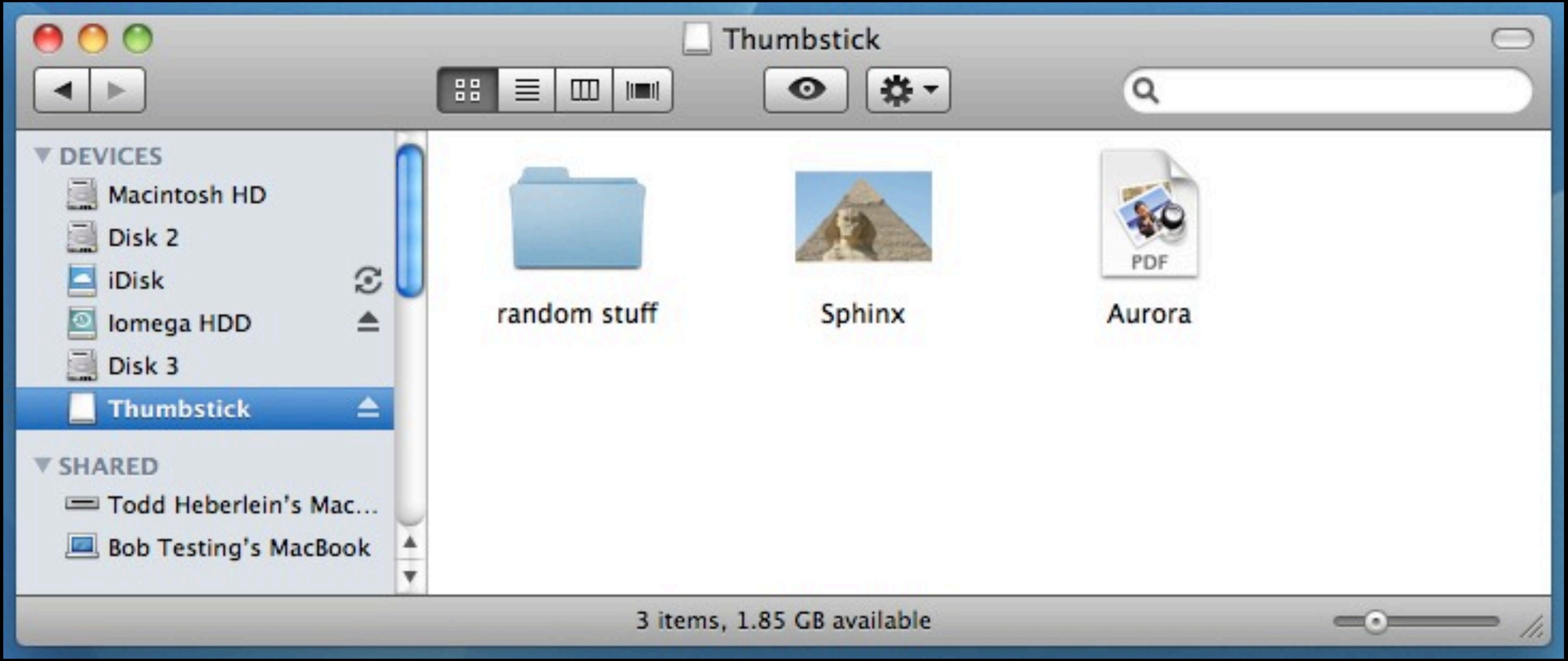


Human Errors Fuel Hacking as Test Shows Nothing Stops Idiocy

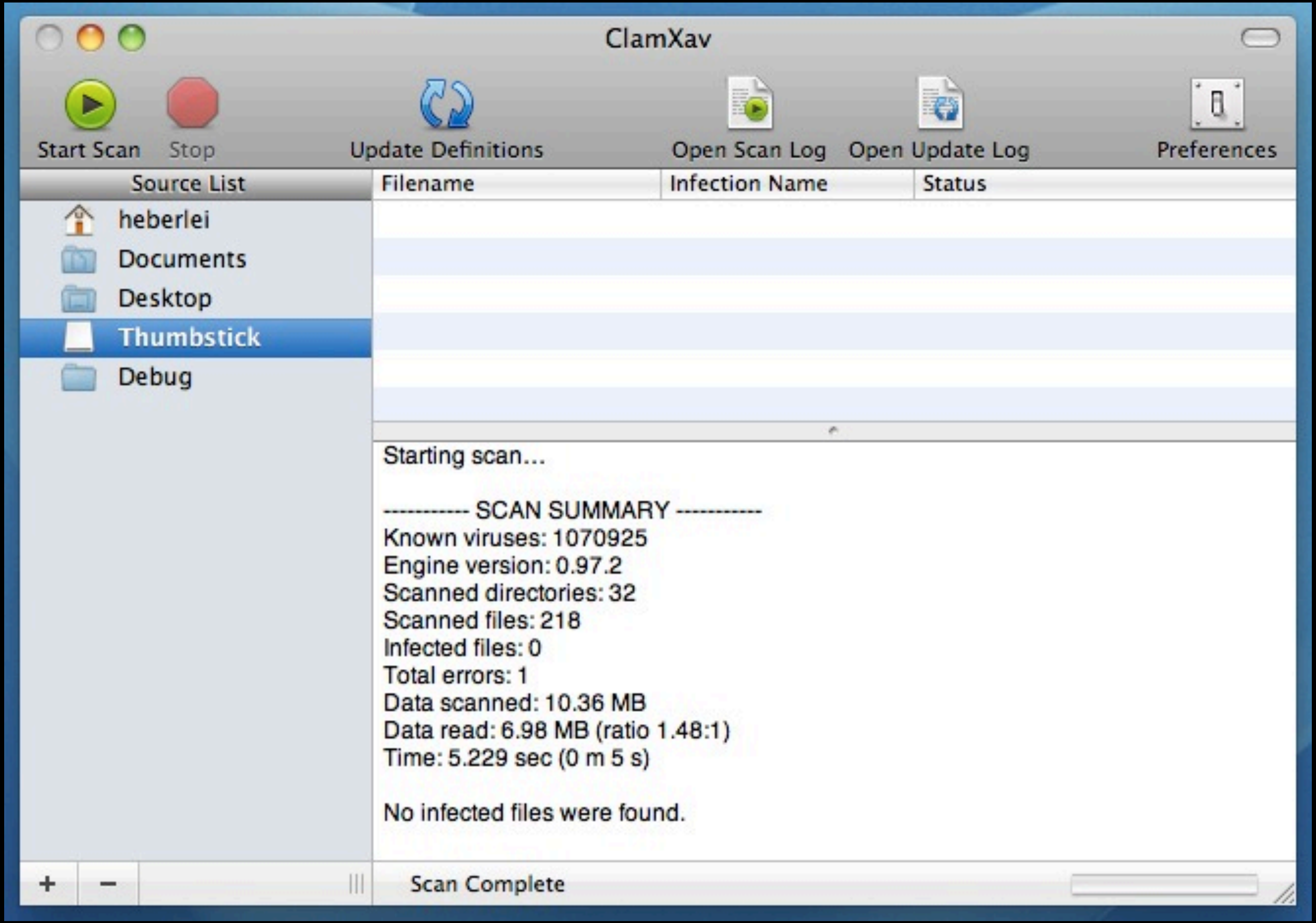
By Cliff Edwards, Olga Kharif and Michael Riley - Jun 27, 2011 11:48 AM PT

The U.S. Department of Homeland Security ran a test this year to see how hard it was for hackers to corrupt workers and gain access to computer systems. Not very, it turned out.

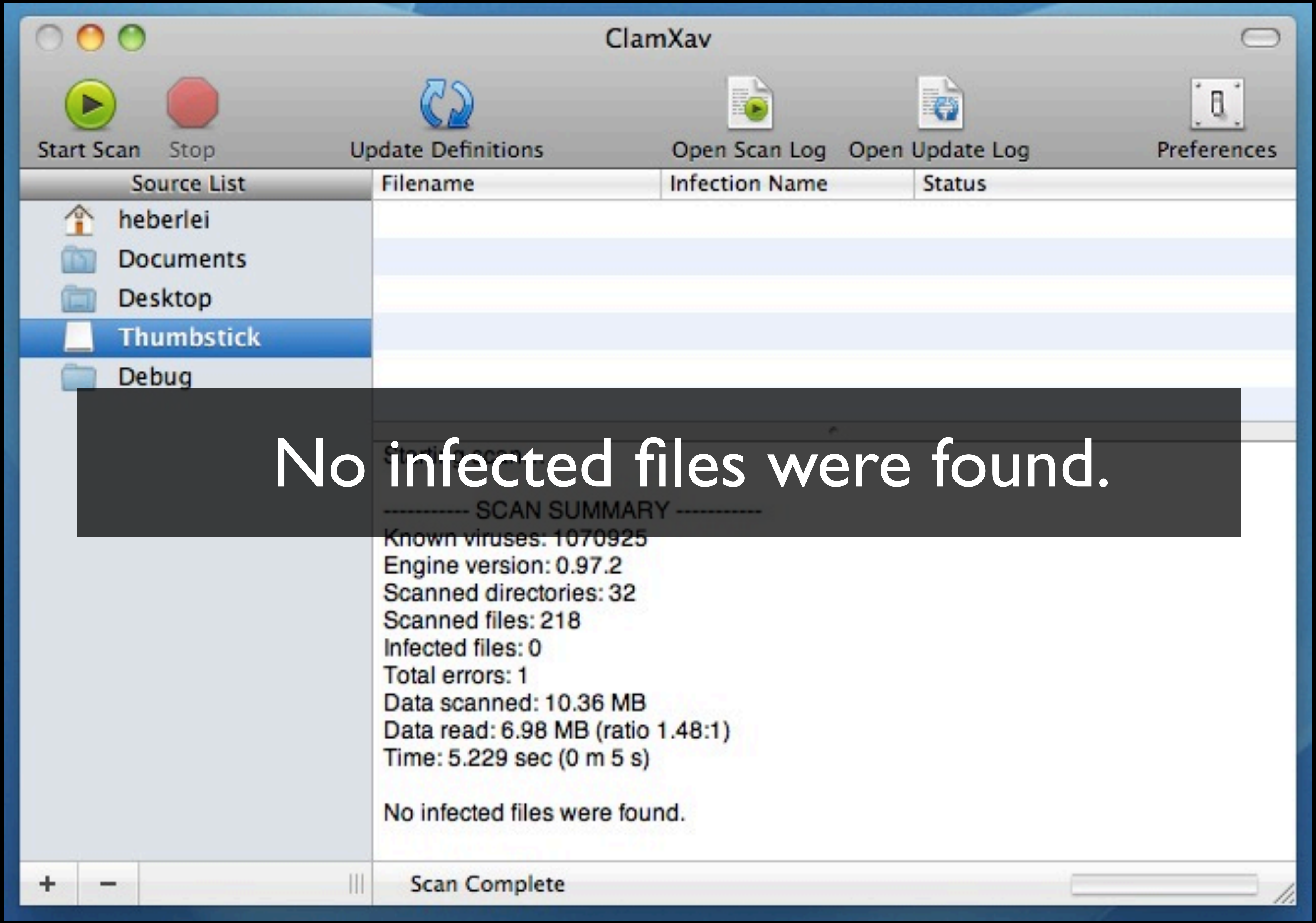
Staff secretly dropped computer discs and USB thumb drives in the parking lots of government buildings and private contractors. Of those who picked them up, 60 percent plugged the devices into office computers, curious to see what they contained. If the drive or CD case had an official logo, 90 percent were installed.



3 items, 1.85 GB available



```
Starting scan...

----------- SCAN SUMMARY -----------
Known viruses: 1070925
Engine version: 0.97.2
Scanned directories: 32
Scanned files: 218
Infected files: 0
Total errors: 1
Data scanned: 10.36 MB
Data read: 6.98 MB (ratio 1.48:1)
Time: 5.229 sec (0 m 5 s)

No infected files were found.
```



No infected files were found.

```
----------- SCAN SUMMARY -----------
Known viruses: 1070925
Engine version: 0.97.2
Scanned directories: 32
Scanned files: 218
Infected files: 0
Total errors: 1
Data scanned: 10.36 MB
Data read: 6.98 MB (ratio 1.48:1)
Time: 5.229 sec (0 m 5 s)

No infected files were found.
```

Whew!

We are safe.

Let’s open the files.

Infection by Image

You are now infected!

Challenge: Write a program that does APT type things

Challenge: Write a program that does APT type things

search for files

Challenge: Write a program that does APT type things

search for files

download & run programs

Challenge: Write a program that does
APT type things

search for files

download & run programs

transmit files across the network

Challenge: Write a program that does APT type things

- search for files
- download & run programs
- transmit files across the network
- schedule for execution

Challenge: Write a program that does APT type things

- search for files
- download & run programs
- transmit files across the network
- schedule for execution

then scan it with AV software

Act 2: Introduction to BSM

Act 2: Introduction to BSM

Down into the weeds

Act 2: Introduction to BSM

Down into the weeds

Take your caffeine shot now

History of BSM

History of BSM

- Sun's Basic Security Module ~1990

History of BSM

- Sun’s Basic Security Module ~1990
- Designed to meet C2 rating in NSA’s Orange Book

History of BSM

- Sun’s Basic Security Module ~1990
- Designed to meet C2 rating in NSA’s Orange Book
- Auditing is...

History of BSM

- Sun’s Basic Security Module ~1990
- Designed to meet C2 rating in NSA’s Orange Book
- Auditing is...
- Mac OS 10.3.6 (needed to install Common Criteria Package)

History of BSM

- Sun’s Basic Security Module ~1990
- Designed to meet C2 rating in NSA’s Orange Book
- Auditing is...
- Mac OS 10.3.6 (needed to install Common Criteria Package)
- Installed and running in Mac OS 10.6

History of BSM

- Sun's Basic Security Module ~1990
- Designed to meet C2 rating in NSA's Orange Book
- Auditing is...
- Mac OS 10.3.6 (needed to install Common Criteria Package)
- Installed and running in Mac OS 10.6
- Mac OS, Solaris, FreeBSD

```
$ sudo ls -l /var/audit
$ sudo ls -l /var/audit
```

```
-r--r-----  1 root  wheel   718832466 Jan  5 20:54 20120105164727.20120106045417
-r--r-----  1 root  wheel    99370721 Jan  6 10:48 20120106181312.20120106184851
-r--r-----  1 root  wheel   379564600 Jan  6 15:20 20120106184917.20120106232023
-r--r-----  1 root  wheel    73325596 Jan  8 13:46 20120108210134.not_terminated
```

Crazy File Naming Scheme

```
20120106184917.20120106232023
```

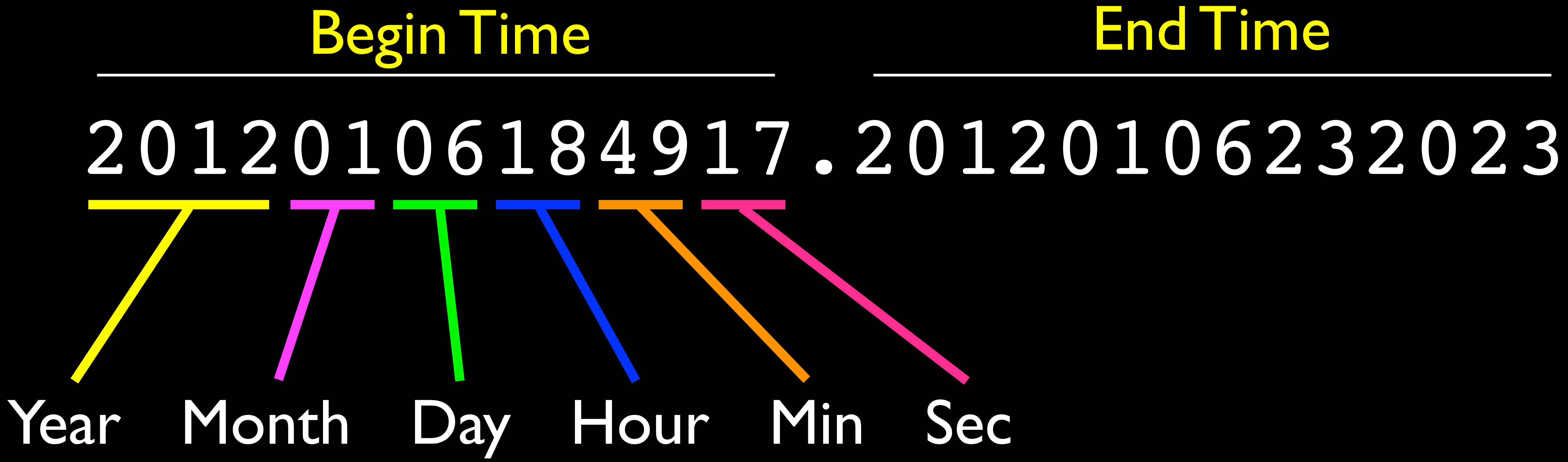
Crazy File Naming Scheme

Begin Time

End Time

```
20120106184917.20120106232023
```

Crazy File Naming Scheme



Begin Time

End Time

20120106184917.20120106232023

Special File Names

Special File Names

`20120108210134.not_terminated`

Special File Names

```
20120108210134.not_terminated
current
```

```
$ ls /etc/security
$ ls /etc/security

audit_class          audit_user
audit_control        audit_warn
audit_event
```

```
$ ls /etc/security

audit_class        audit_user
audit_control      audit_warn
audit_event
```

```
$ sudo cat audit_control
$ sudo cat audit_control

    dir:/var/audit
    flags:all
    minfree:5
    naflags:lo,aa,pc,nt
    policy:cnt,argv
    filesz:4G
    expire-after:40G
```

```
$ sudo cat audit_control

      dir:/var/audit
      flags:all
      minfree:5
      naflags:lo,aa,pc,nt
      policy:cnt,argv
      filesz:4G
      expire-after:40G
```

```
$ sudo cat audit_control

    dir:/var/audit
    flags:all
    minfree:5
    naflags:lo,aa,pc,nt
    policy:cnt,argv
    filesz:4G
    expire-after:40G
```

```
$ sudo cat audit_control

      dir:/var/audit
      flags:all
      minfree:5
      naflags:lo,aa,pc,nt
      policy:cnt,argv
      filesz:4G
      expire-after:40G
```

```
$ sudo cat audit_control

    dir:/var/audit
    flags:all
    minfree:5
    naflags:lo,aa,pc,nt
    policy:cnt,argv
    filesz:4G
    expire-after:40G
```

flags & naflags

flags & naflags

- Flags tell the system what to record

flags & naflags

- Flags tell the system what to record
- Flags are 2-letter combinations like “pc”, “ex”, and “nt”

flags & naflags

- Flags tell the system what to record
- Flags are 2-letter combinations like "pc", "ex", and "nt"
- A flag represents a group of system calls like fork() and exec()

flags & naflags

- Flags tell the system what to record
- Flags are 2-letter combinations like "pc", "ex", and "nt"
- A flag represents a group of system calls like fork() and exec()
- You can fine-tune the flags with the characters +, -, and ^

flags & naflags

- Flags tell the system what to record
- Flags are 2-letter combinations like “pc”, “ex”, and “nt”
- A flag represents a group of system calls like fork() and exec()
- You can fine-tune the flags with the characters +, -, and ^
- Fine tuning flags is hard

flags & naflags

- Flags tell the system what to record
- Flags are 2-letter combinations like “pc”, “ex”, and “nt”
- A flag represents a group of system calls like fork() and exec()
- You can fine-tune the flags with the characters +, -, and ^
- Fine tuning flags is hard
- I stick with “all”

lo, ad, -fr, -fw, -fc, -fd, -cl, -fm

lo, ad, -fr, -fw, -fc, -fd, -cl, -fm

lo	login & logout
ad	administrative
-fr	failed file read
-fw	failed file write
-fc	failed file create
-fd	failed file delete
-cl	failed file close
-fm	failed file attribute modification

lo, ad, -fr, -fw, -fc, -fd, -cl, -fm

lo, ad, -fr, -fw, -fc, -fd, -cl, -fm

The name of the program that was running

lo, ad, -fr, -fw, -fc, -fd, -cl, -fm

The name of the program that was running

Authentication events

lo, ad, -fr, -fw, -fc, -fd, -cl, -fm

The name of the program that was running

Authentication events

Network activity

lo, ad, -fr, -fw, -fc, -fd, -cl, -fm

The name of the program that was running

Authentication events

Network activity

Successful efforts to read your files

```
header,151,11,open(2) - read,0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,2,0x0,flags
path,hello1
path,/Users/heberlei/Tmp/hello1
attribute,100644,heberlei,staff,234881033,228930222,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,3
trailer,151
```

```
header,151,11,open(2) - read,0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,2,0x0,flags
path,hello1
path,/Users/heberlei/Tmp/hello1
attribute,100644,heberlei,staff,234881033,228930222,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,3
trailer,151
```

```
header,151,11,open(2) - read,0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,2,0x0,flags
path,hello1
path,/Users/heberlei/Tmp/hello1
attribute,100644,heberlei,staff,234881033,228930222,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,3
trailer,151
```

```
header,151,11,open(2) - read,0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,2,0x0,flags
path,hello1
path,/Users/heberlei/Tmp/hello1
attribute,100644,heberlei,staff,234881033,228930222,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,3
trailer,151
```

```
header,151,11,open(2) - read,0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,2,0x0,flags
path,hello1
path,/Users/heberlei/Tmp/hello1
attribute,100644,heberlei,staff,234881033,228930222,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,3
trailer,151
```

Gotcha: What program?

```
header,151,11,open(2) - read,0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,2,0x0,flags
path,hello1
path,/Users/heberlei/Tmp/hello1
attribute,100644,heberlei,staff,234881033,228930222,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,3
trailer,151
```

Gotcha: What user?

```
header,151,11,open(2) - read,0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,2,0x0,flags
path,hello1
path,/Users/heberlei/Tmp/hello1
attribute,100644,heberlei,staff,234881033,228930222,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,3
trailer,151
```

Gotcha: How much data?

```
header,68,11,setpgrp(2),0,Tue Jan 10 11:04:18 2012, + 503 msec
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,68

header,156,11,ioctl(2),0,Tue Jan 10 11:04:18 2012, + 503 msec
argument,2,0x4004667a,cmd
argument,3,0x7fff5fbff71c,arg
path,/dev/ttys001
argument,1,0xff,fd
attribute,20620,heberlei,tty,141068340,659,268435457
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,156

header,156,11,ioctl(2),0,Tue Jan 10 11:04:18 2012, + 503 msec
argument,2,0x80047476,cmd
argument,3,0x7fff5fbff79c,arg
path,/dev/ttys001
argument,1,0xff,fd
attribute,20620,heberlei,tty,141068340,659,268435457
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,156

header,141,11,execve(2),0,Tue Jan 10 11:04:18 2012, + 522 msec
exec arg,cp,hello1,hello2
path,/bin/cp
path,/bin/cp
attribute,100555,root,wheel,234881033,24762,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,141

header,143,11,open(2) - read,0,Tue Jan 10 11:04:18 2012, + 522 msec
argument,2,0x0,flags
path,/dev/urandom
path,/dev/urandom
attribute,20666,root,wheel,141068340,586,150994945
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,3
trailer,143

header,124,11,close(2),0,Tue Jan 10 11:04:18 2012, + 522 msec
argument,2,0x3,fd
path,/dev/urandom
attribute,20666,root,wheel,141068340,586,150994945
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,124
```

```
header,94,11,sysctl(3),0,Tue Jan 10 11:04:18 2012, + 522 msec
argument,1,0x0,name
argument,1,0x3,name
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,94

header,94,11,sysctl() - non-admin,0,Tue Jan 10 11:04:18 2012, + 522 msec
argument,1,0x2,name
argument,1,0x75,name
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,94

header,153,11,open(2) - read,write,0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,2,0x2,flags
path,/dev/dtracehelper
path,/dev/dtracehelper
attribute,20666,root,wheel,141068340,588,419430400
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,3
trailer,153

header,161,11,ioctl(2),0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,2,0x80086804,cmd
argument,3,0x7fff5fbfd6f0,arg
path,/dev/dtracehelper
argument,1,0x3,fd
attribute,20666,root,wheel,141068340,588,419430400
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,161

header,129,11,close(2),0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,2,0x3,fd
path,/dev/dtracehelper
attribute,20666,root,wheel,141068340,588,419430400
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,129

header,94,11,sysctl() - non-admin,0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,1,0x1,name
argument,1,0x3b,name
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,94
```

```
header,143,11,open(2) - read,0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,2,0x0,flags
path,/dev/urandom
path,/dev/urandom
attribute,20666,root,wheel,141068340,586,150994945
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,3
trailer,143

header,124,11,close(2),0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,2,0x3,fd
path,/dev/urandom
attribute,20666,root,wheel,141068340,586,150994945
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,124

header,94,11,sysctl(3),0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,1,0x0,name
argument,1,0x3,name
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,94

header,94,11,sysctl() - non-admin,0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,1,0x6,name
argument,1,0x18,name
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,94

header,143,11,open(2) - read,0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,2,0x0,flags
path,/dev/urandom
path,/dev/urandom
attribute,20666,root,wheel,141068340,586,150994945
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,3
trailer,143

header,124,11,close(2),0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,2,0x3,fd
path,/dev/urandom
attribute,20666,root,wheel,141068340,586,150994945
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,124
```

```
header,94,11,sysctl() - non-admin,0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,1,0x6,name
argument,1,0x3,name
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,94

header,101,11,munmap(2),0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,1,0x100139000,addr
argument,2,0xc7000,len
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,101

header,101,11,munmap(2),0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,1,0x100300000,addr
argument,2,0x39000,len
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,101

header,94,11,sysctl(3),0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,1,0x0,name
argument,1,0x3,name
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,94

header,94,11,sysctl() - non-admin,0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,1,0x6,name
argument,1,0x19,name
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,94

header,94,11,sysctl(3),0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,1,0x0,name
argument,1,0x3,name
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,94

header,94,11,sysctl() - non-admin,0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,1,0x6,name
argument,1,0x68,name
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,94
```

```
header,94,11,sysctl(3),0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,1,0x0,name
argument,1,0x3,name
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,94

header,94,11,sysctl() - non-admin,0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,1,0x6,name
argument,1,0x66,name
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,94

header,103,11,umask(2),0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,1,0x1ff,new mask
argument,0,0x12,prev mask
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,18
trailer,103

header,103,11,umask(2),0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,1,0x12,new mask
argument,0,0x1ff,prev mask
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,511
trailer,103

header,101,11,munmap(2),0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,1,0x100300000,addr
argument,2,0x500000,len
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,101

header,101,11,munmap(2),0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,1,0x101000000,addr
argument,2,0x300000,len
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,101

header,151,11,open(2) - read,0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,2,0x0,flags
path,hello1
path,/Users/heberlei/Tmp/hello1
attribute,100644,heberlei,staff,234881033,228930222,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,3
trailer,151
```

```
header,105,11,open(2) - write,creat,trunc,0,Tue Jan 10 11:04:18 2012, + 523
msec
argument,3,0x1a4,mode
argument,2,0x601,flags
path,hello2
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,4
trailer,105

header,160,11,fchmod(2),0,Tue Jan 10 11:04:18 2012, + 523 msec
argument,2,0x180,new file mode
path,/Users/heberlei/Tmp/hello2
argument,1,0x4,fd
attribute,100644,heberlei,staff,234881033,233490254,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,160

header,160,11,fchmod(2),0,Tue Jan 10 11:04:18 2012, + 536 msec
argument,2,0x1a4,new file mode
path,/Users/heberlei/Tmp/hello2
argument,1,0x4,fd
attribute,100600,heberlei,staff,234881033,233490254,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,160

header,160,11,fchmod(2),0,Tue Jan 10 11:04:18 2012, + 536 msec
argument,2,0x1a4,new file mode
path,/Users/heberlei/Tmp/hello2
argument,1,0x4,fd
attribute,100644,heberlei,staff,234881033,233490254,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,160

header,100,11,mac_syscall(2),0,Tue Jan 10 11:04:18 2012, + 536 msec
text,arg: Quarantine
argument,3,0x52,call
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,failure: Unknown error: 250,4294967295
trailer,100
```

```
header,160,11,fchmod(2),0,Tue Jan 10 11:04:18 2012, + 536 msec
argument,2,0x1a4,new file mode
path,/Users/heberlei/Tmp/hello2
argument,1,0x4,fd
attribute,100644,heberlei,staff,234881033,233490254,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,160

header,138,11,close(2),0,Tue Jan 10 11:04:18 2012, + 536 msec
argument,2,0x3,fd
path,/Users/heberlei/Tmp/hello1
attribute,100644,heberlei,staff,234881033,228930222,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,138

header,138,11,close(2),0,Tue Jan 10 11:04:18 2012, + 536 msec
argument,2,0x4,fd
path,/Users/heberlei/Tmp/hello2
attribute,100644,heberlei,staff,234881033,233490254,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,138

header,77,11,exit(2),0,Tue Jan 10 11:04:18 2012, + 536 msec
exit,Error 0,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,77
```

```
header,160,11,fchmod(2),0,Tue Jan 10 11:04:18 2012, + 536 msec
argument,2,0x1a4,new file mode
path,/Users/heberlei/Tmp/hello2
argument,1,0x4,fd
attribute,100644,heberlei,staff,234881033,233490254,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,160

header,138,11,close(2),0,Tue Jan 10 11:04:18 2012, + 536 msec
argument,2,0x3,fd
path,/Users/heberlei/Tmp/hello1
attribute,100644,heberlei,staff,234881033,228930222,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,138

header,138,11,close(2),0,Tue Jan 10 11:04:18 2012, + 536 msec
argument,2,0x4,fd
path,/Users/heberlei/Tmp/hello2
attribute,100644,heberlei,staff,234881033,233490254,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,138

header,77,11,exit(2),0,Tue Jan 10 11:04:18 2012, + 536 msec
exit,Error 0,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,77
```

```
$ cp hello1 hello2
```

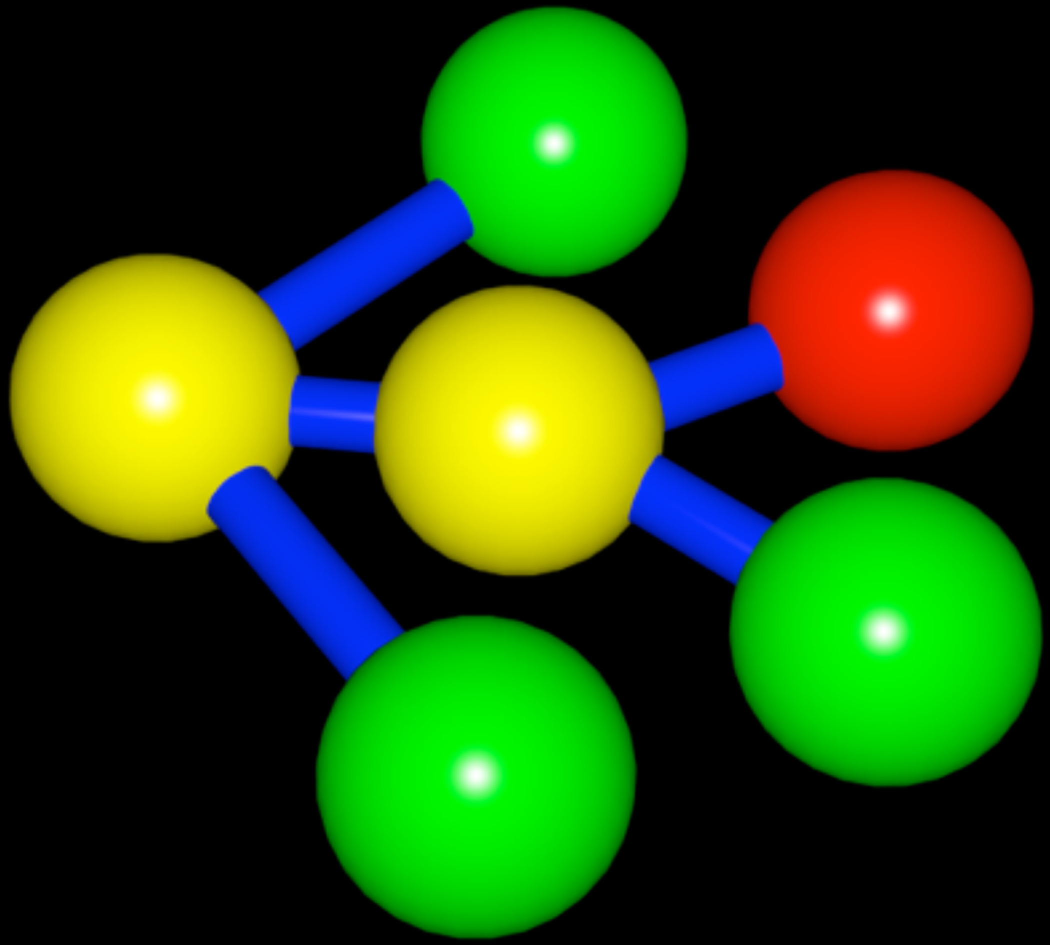
```
header,160,11,fchmod(2),0,Tue Jan 10 11:04:18 2012, + 536 msec
argument,2,0x1a4,new file mode
path,/Users/heberlei/Tmp/hello2
argument,1,0x4,fd
attribute,100644,heberlei,staff,234881033,233490254,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,160

header,138,11,close(2),0,Tue Jan 10 11:04:18 2012, + 536 msec
argument,2,0x3,fd
path,/Users/heberlei/Tmp/hello1
attribute,100644,heberlei,staff,234881033,228930222,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,138

header,138,11,close(2),0,Tue Jan 10 11:04:18 2012, + 536 msec
argument,2,0x4,fd
path,/Users/heberlei/Tmp/hello2
attribute,100644,heberlei,staff,234881033,233490254,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,138

header,77,11,exit(2),0,Tue Jan 10 11:04:18 2012, + 536 msec
exit,Error 0,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,77
```

```
$ cp hello1 hello2
```

41 audit records

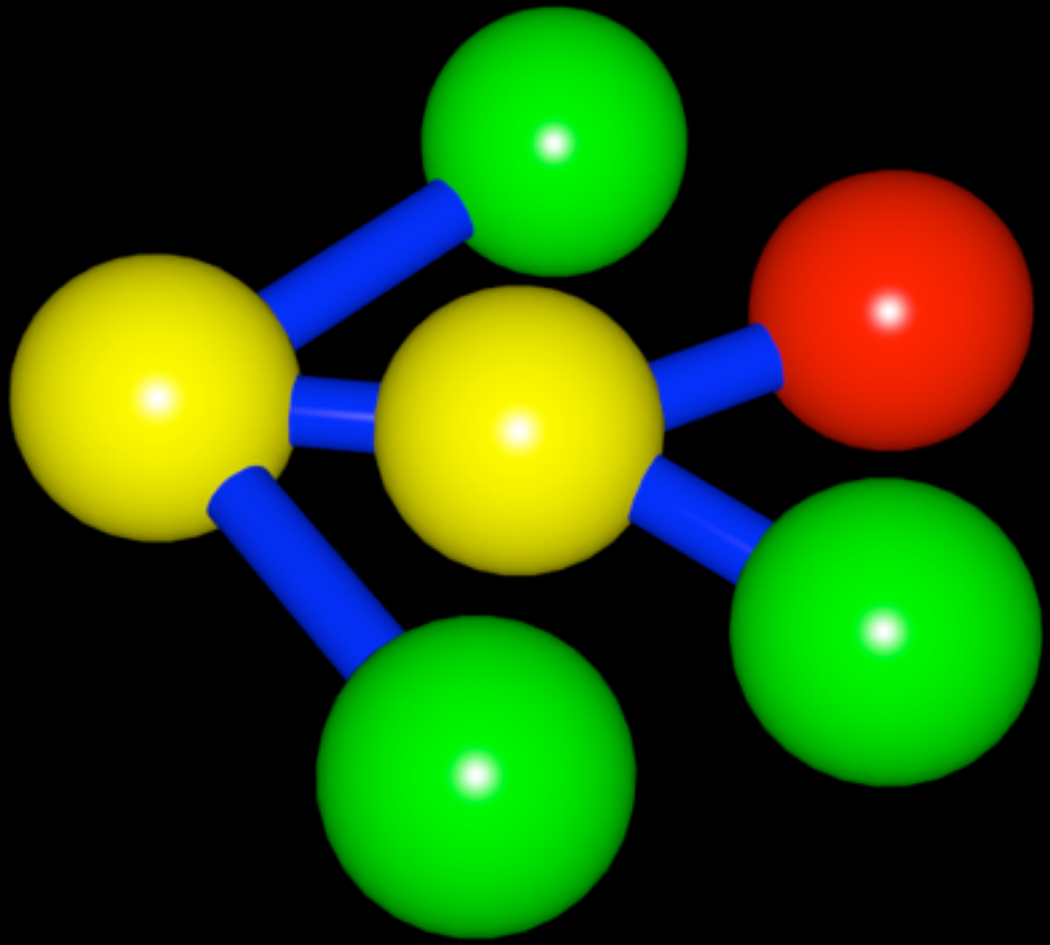
278 lines

Act 3: Up Out of the Weeds



Audit Explorer

Audit Explorer Filter Editor



Audit Explorer

free today

Audit Explorer Filter Editor

free at website

All screenshots are from the sample data sets you can download

All screenshots are from the sample data sets you can download

Tutorial videos for each data set are available from:

http://www.netsq.com/Tools/AuditExplorer/Videos/

Goal:

Goal:

Goal: Convince you that audit data can produce useful information.

Goal:

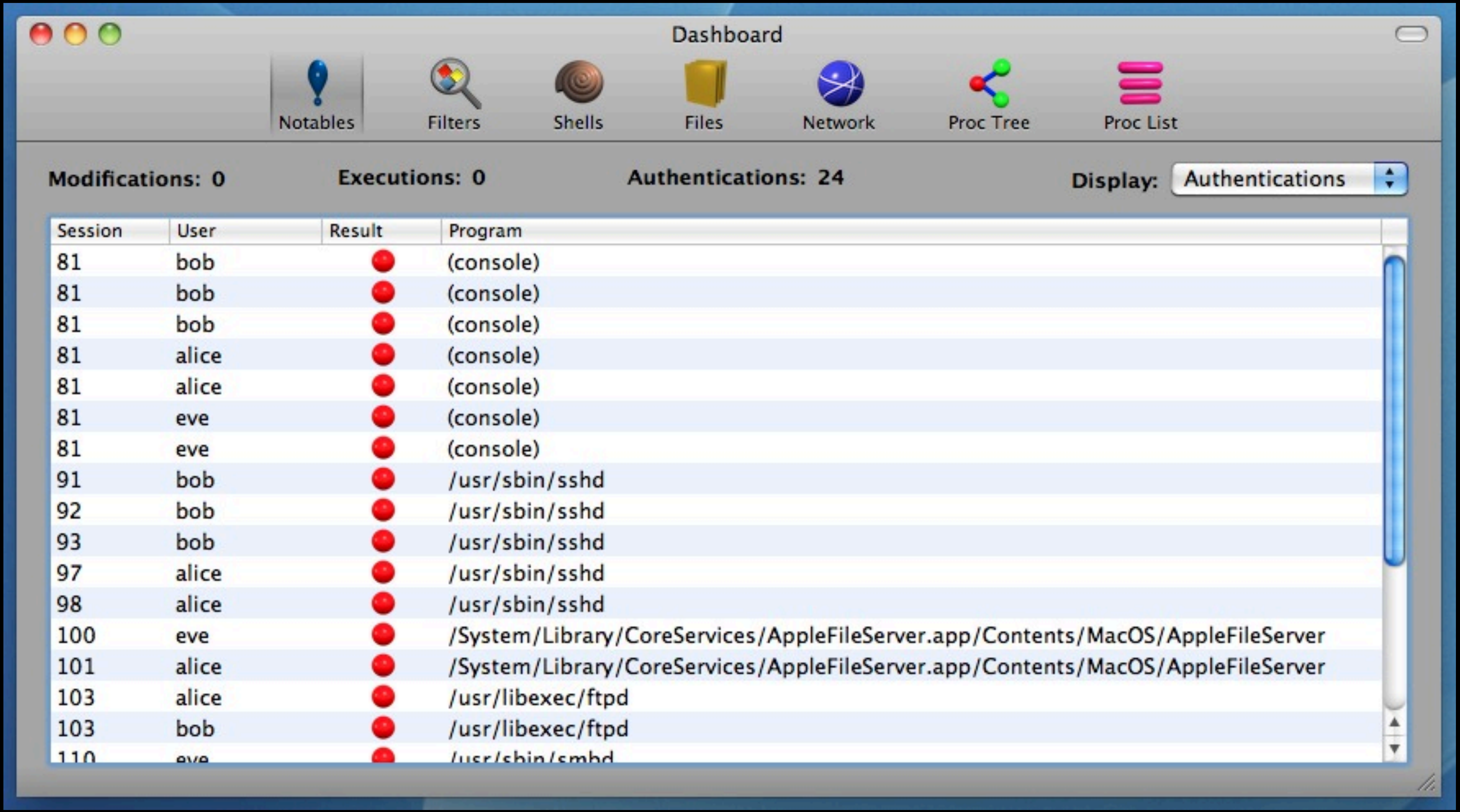
Goal: Convince you that audit data can produce useful information.

Goal: Encourage you to turn on auditing in case “that day” ever does occur.

Goal: Convince you that audit data can produce useful information.

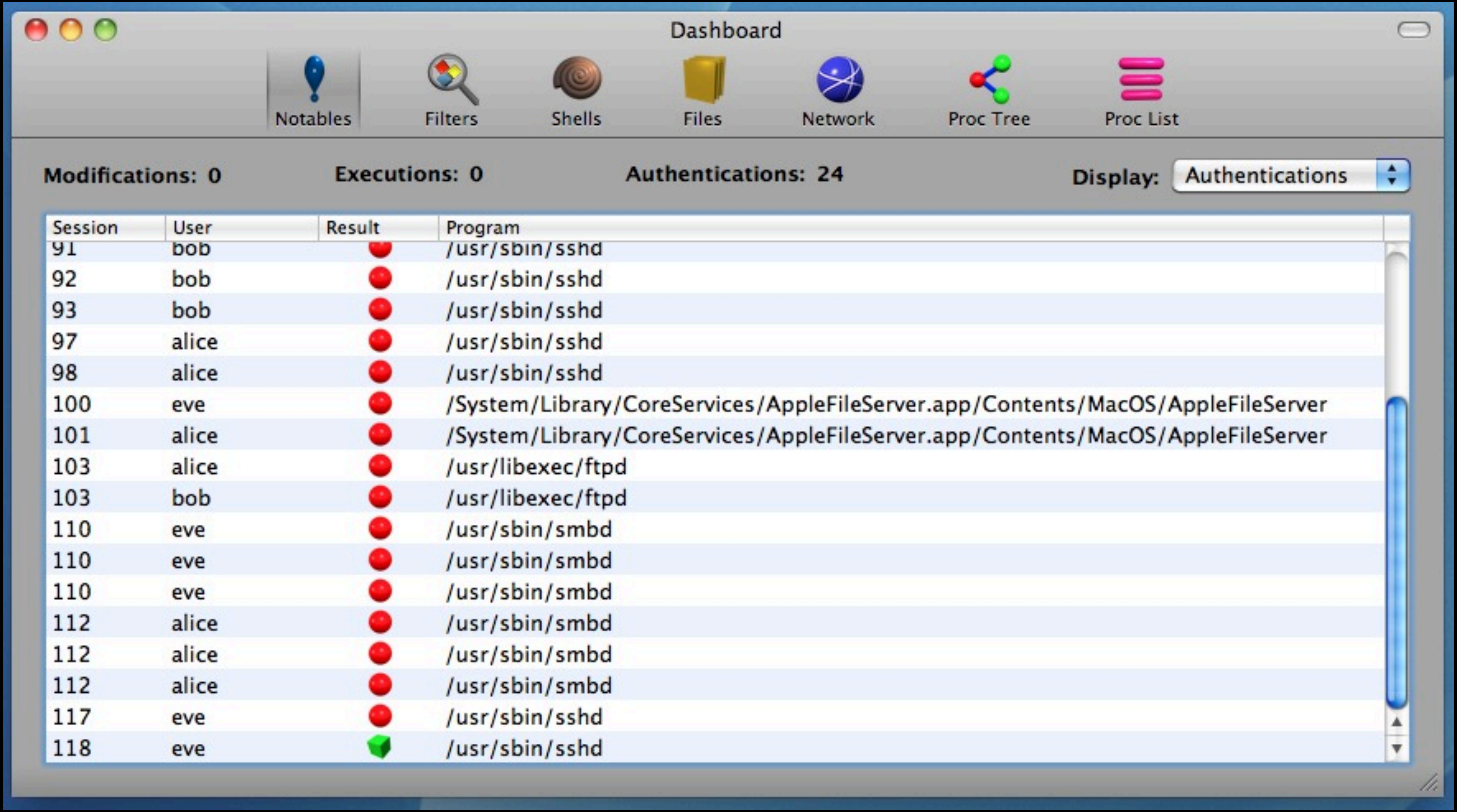
Goal: Encourage you to turn on auditing in case "that day" ever does occur.

Because that day will occur.



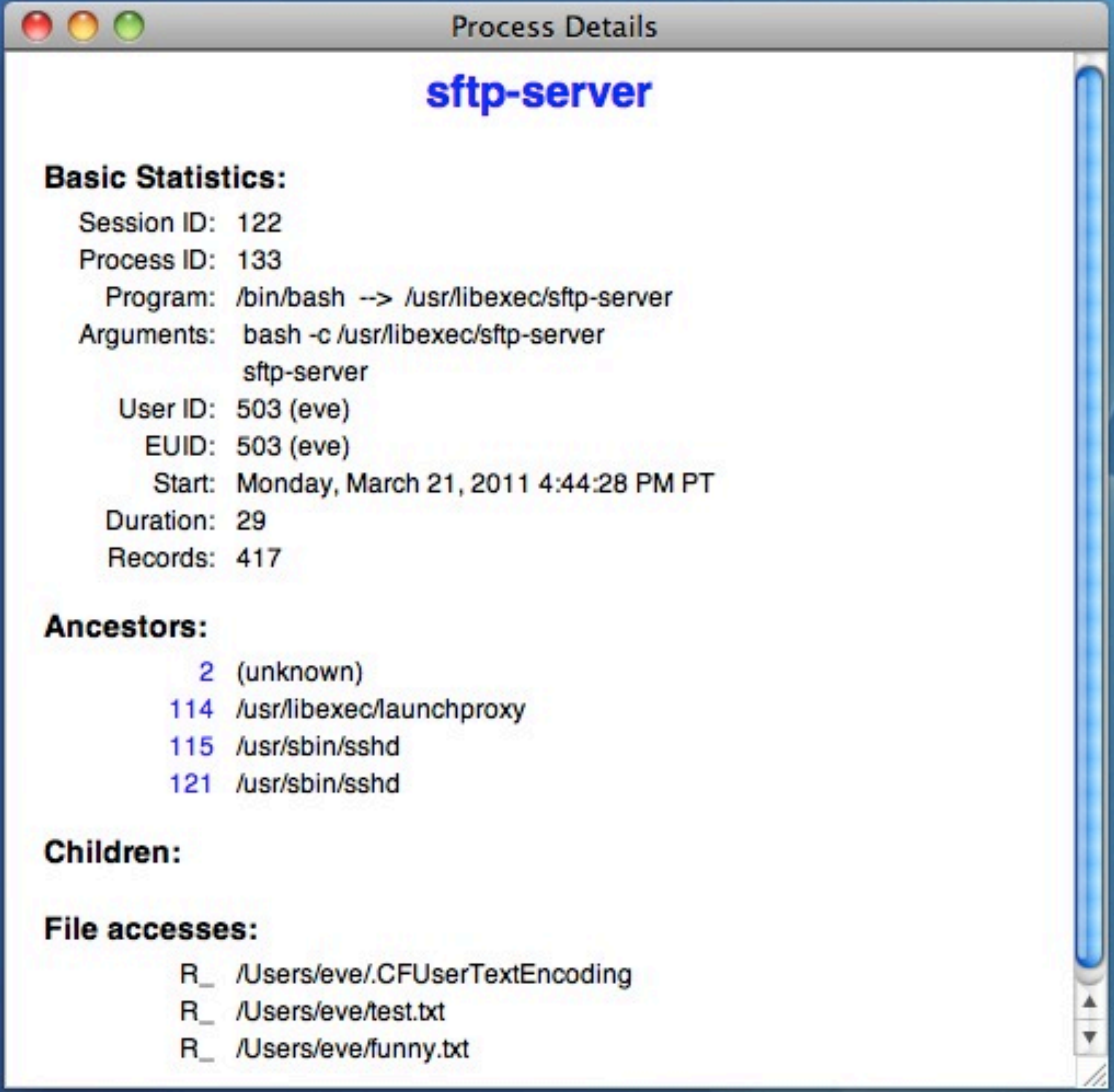
Modifications: 0 Executions: 0 Authentications: 24 Display: Authentications

Session	User	Result	Program
81	bob	●	(console)
81	bob	●	(console)
81	bob	●	(console)
81	alice	●	(console)
81	alice	●	(console)
81	eve	●	(console)
81	eve	●	(console)
91	bob	●	/usr/sbin/sshd
92	bob	●	/usr/sbin/sshd
93	bob	●	/usr/sbin/sshd
97	alice	●	/usr/sbin/sshd
98	alice	●	/usr/sbin/sshd
100	eve	●	/System/Library/CoreServices/AppleFileServer.app/Contents/MacOS/AppleFileServer
101	alice	●	/System/Library/CoreServices/AppleFileServer.app/Contents/MacOS/AppleFileServer
103	alice	●	/usr/libexec/ftpd
103	bob	●	/usr/libexec/ftpd
110	eve	●	/usr/sbin/smbd



Modifications: 0 **Executions: 0** **Authentications: 24** **Display:** Authentications

Session	User	Result	Program
91	bob	🔴	/usr/sbin/sshd
92	bob	🔴	/usr/sbin/sshd
93	bob	🔴	/usr/sbin/sshd
97	alice	🔴	/usr/sbin/sshd
98	alice	🔴	/usr/sbin/sshd
100	eve	🔴	/System/Library/CoreServices/AppleFileServer.app/Contents/MacOS/AppleFileServer
101	alice	🔴	/System/Library/CoreServices/AppleFileServer.app/Contents/MacOS/AppleFileServer
103	alice	🔴	/usr/libexec/ftpd
103	bob	🔴	/usr/libexec/ftpd
110	eve	🔴	/usr/sbin/smbd
110	eve	🔴	/usr/sbin/smbd
110	eve	🔴	/usr/sbin/smbd
112	alice	🔴	/usr/sbin/smbd
112	alice	🔴	/usr/sbin/smbd
112	alice	🔴	/usr/sbin/smbd
117	eve	🔴	/usr/sbin/sshd
118	eve	🟩	/usr/sbin/sshd



Process Details

sftp-server

Basic Statistics:

Session ID: 122
Process ID: 133
Program: /bin/bash --> /usr/libexec/sftp-server
Arguments: bash -c /usr/libexec/sftp-server
sftp-server
User ID: 503 (eve)
EUID: 503 (eve)
Start: Monday, March 21, 2011 4:44:28 PM PT
Duration: 29
Records: 417

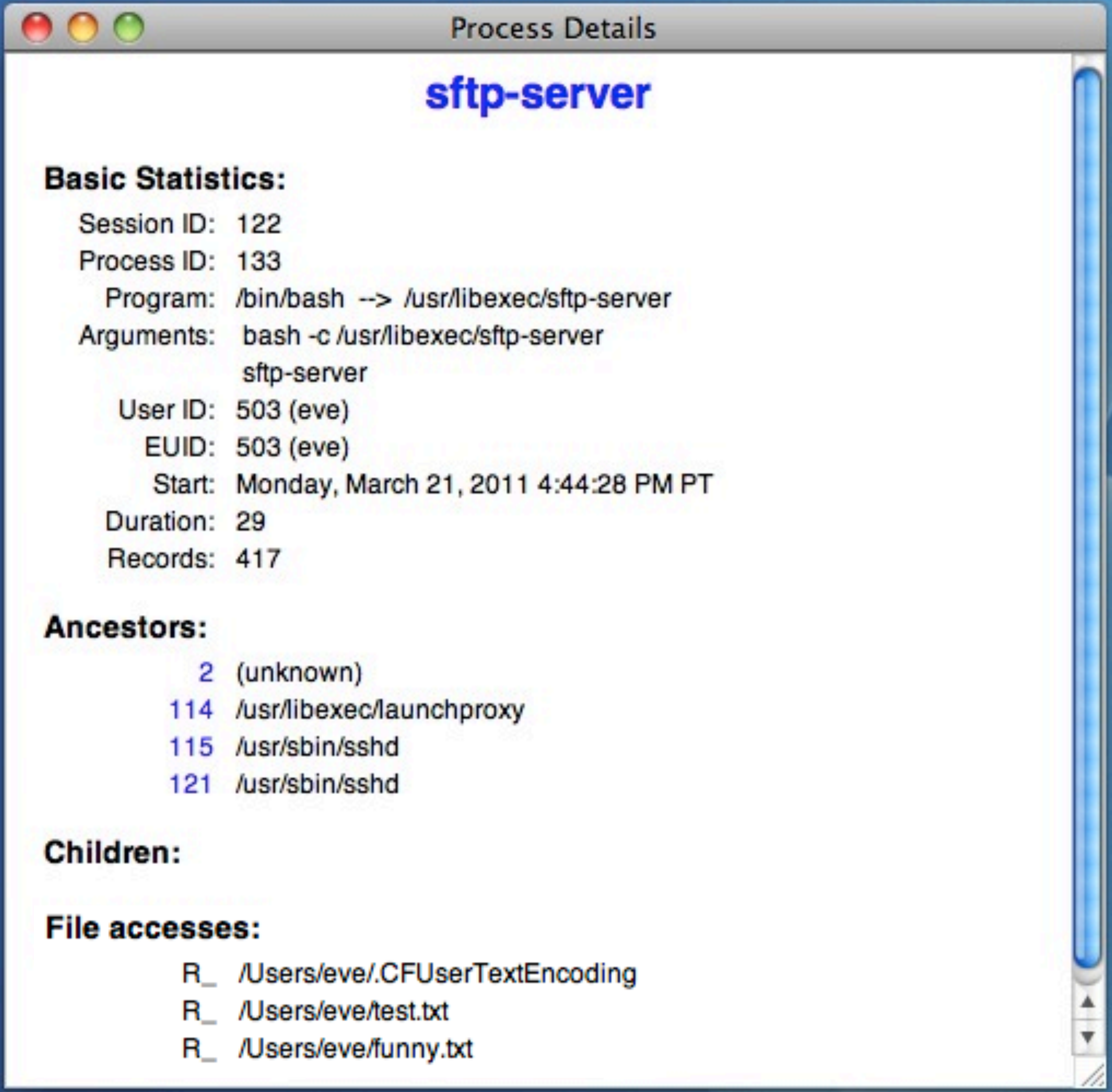
Ancestors:

2 (unknown)
114 /usr/libexec/launchproxy
115 /usr/sbin/sshd
121 /usr/sbin/sshd

Children:

File accesses:

R_ /Users/eve/.CFUserTextEncoding
R_ /Users/eve/test.txt
R_ /Users/eve/funny.txt



sftp-server

Basic Statistics:

Session ID: 122
Process ID: 133
Program: /bin/bash --> /usr/libexec/sftp-server
Arguments: bash -c /usr/libexec/sftp-server
sftp-server
User ID: 503 (eve)
EUID: 503 (eve)
Start: Monday, March 21, 2011 4:44:28 PM PT
Duration: 29
Records: 417

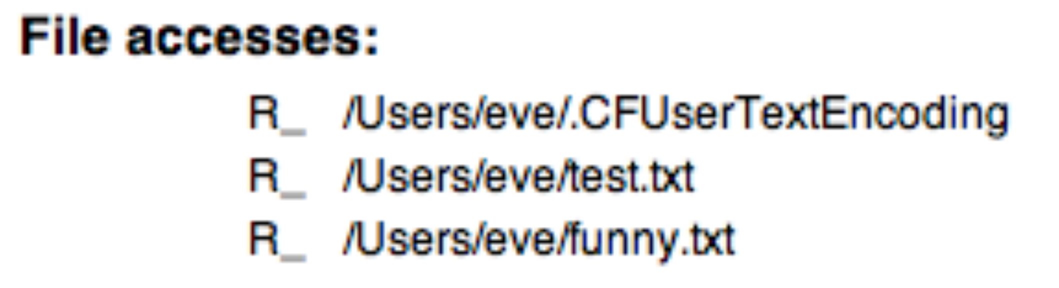
Ancestors:

2	(unknown)
114	/usr/libexec/launchproxy
115	/usr/sbin/sshd
121	/usr/sbin/sshd

Children:

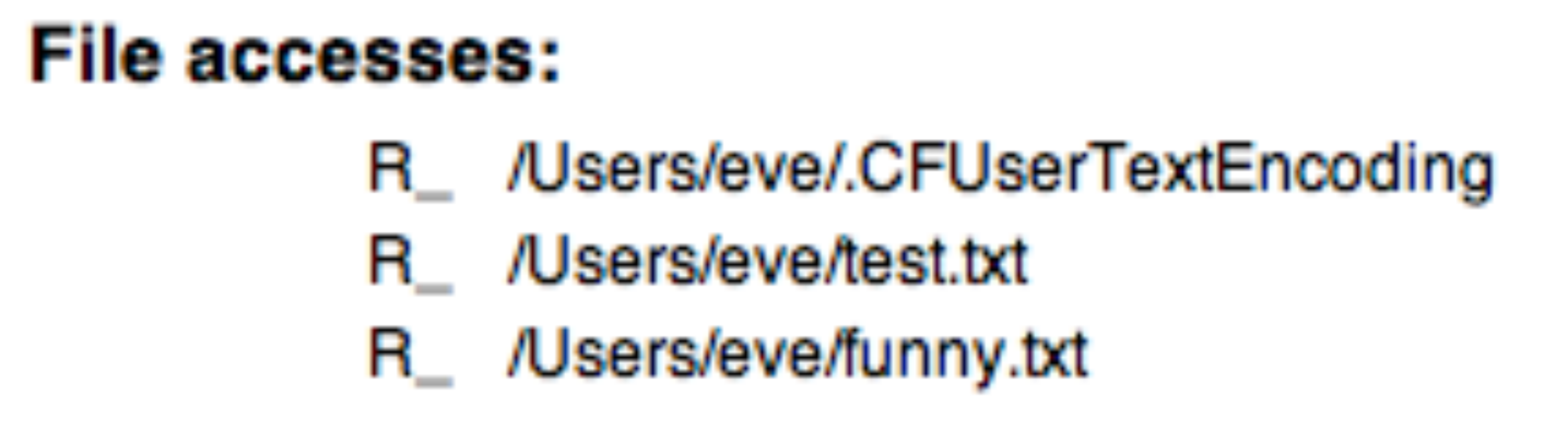
File accesses:

R_	/Users/eve/.CFUserTextEncoding
R_	/Users/eve/test.txt
R_	/Users/eve/funny.txt



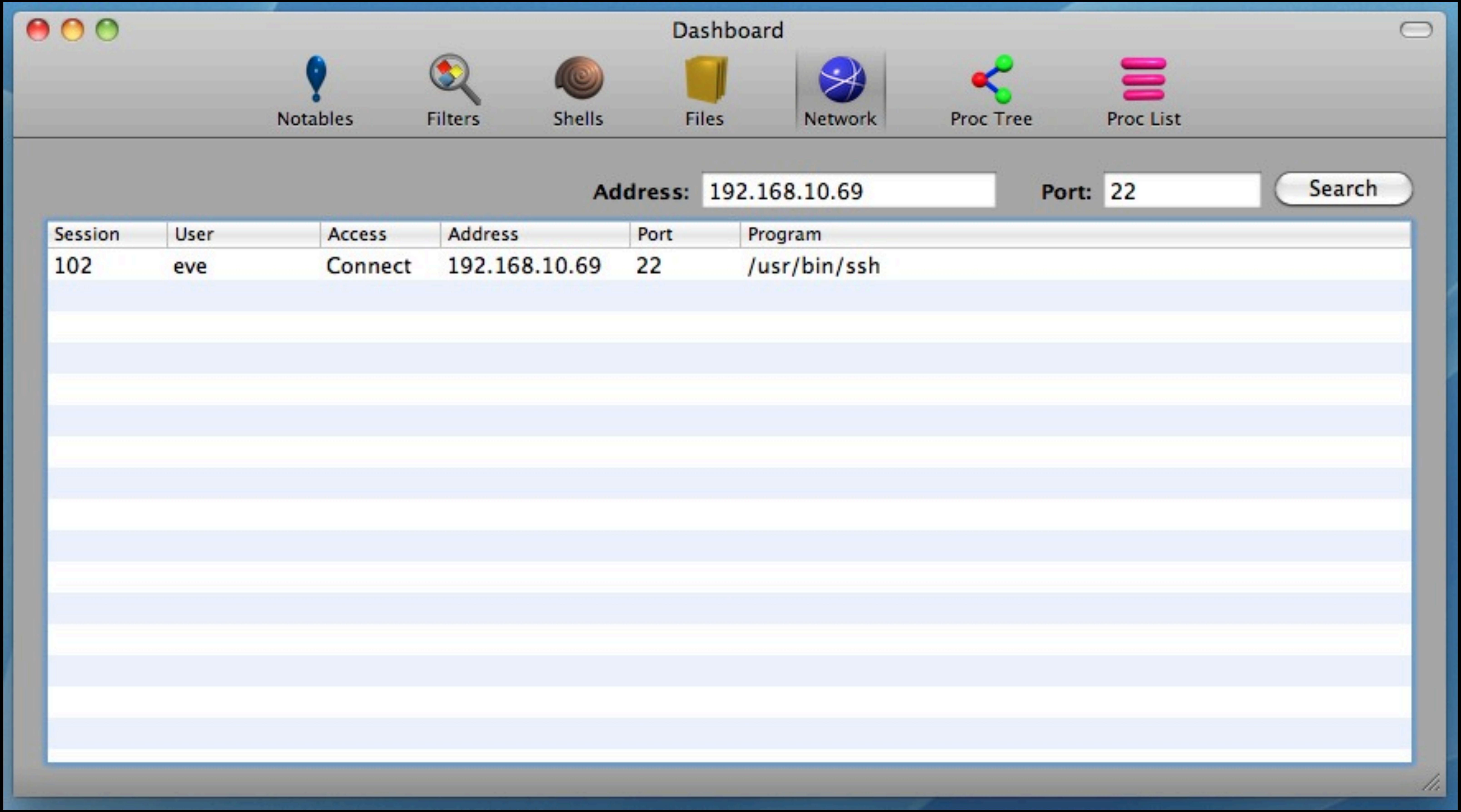
File accesses:

```
        R_   /Users/eve/.CFUserTextEncoding
        R_   /Users/eve/test.txt
        R_   /Users/eve/funny.txt
```



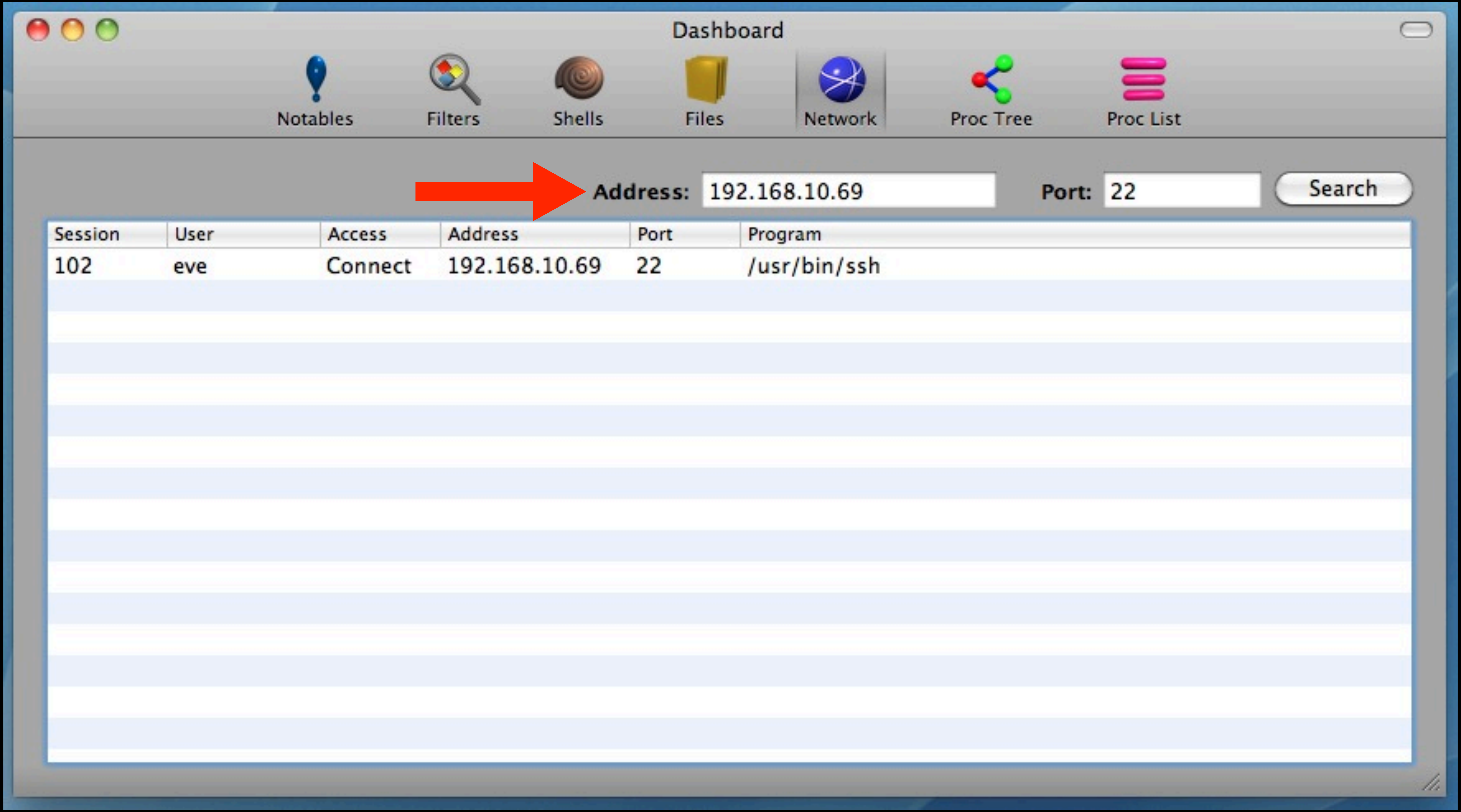
File accesses:

```
R_   /Users/eve/.CFUserTextEncoding
R_   /Users/eve/test.txt
R_   /Users/eve/funny.txt
```



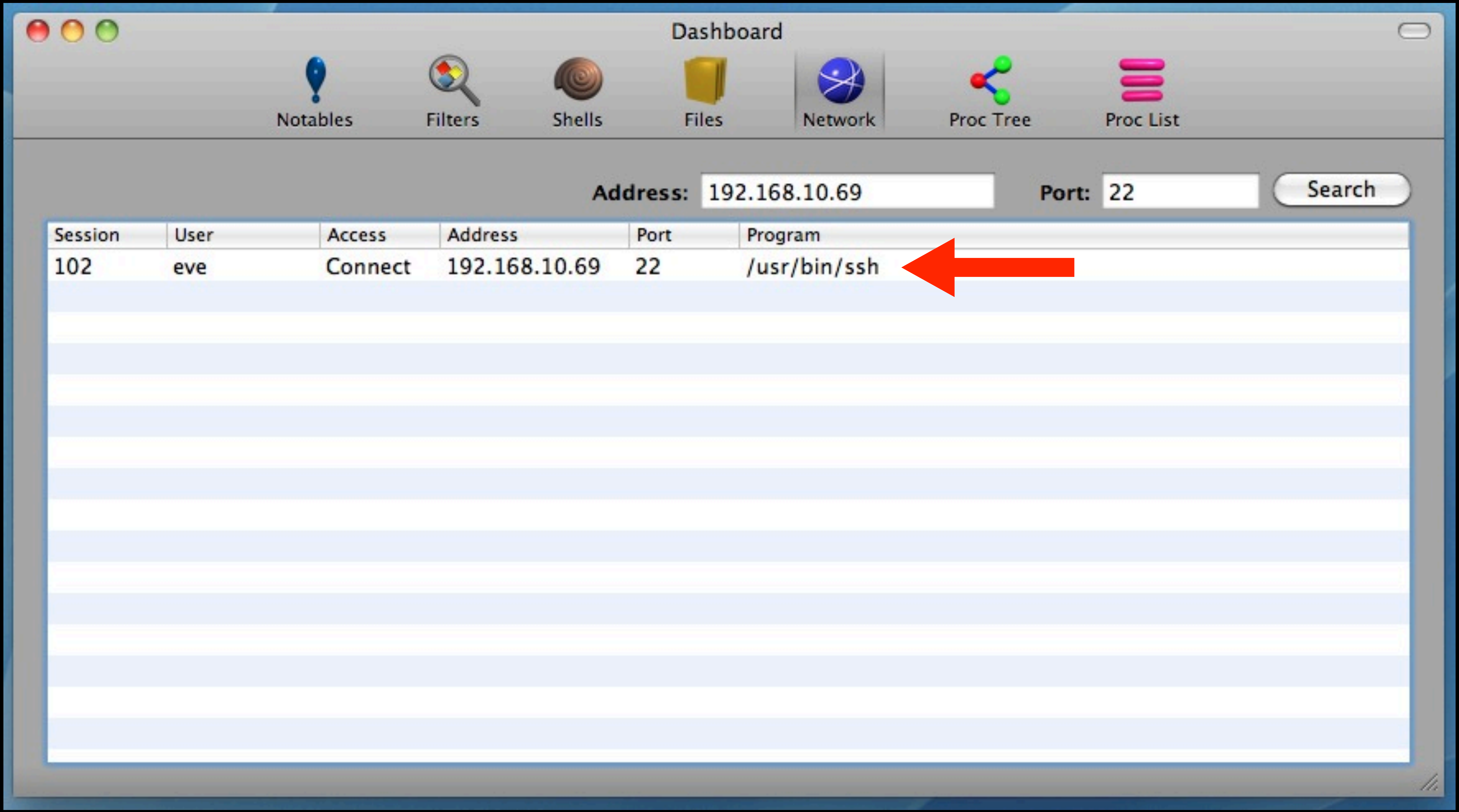
Address: 192.168.10.69 Port: 22

Session	User	Access	Address	Port	Program
102	eve	Connect	192.168.10.69	22	/usr/bin/ssh



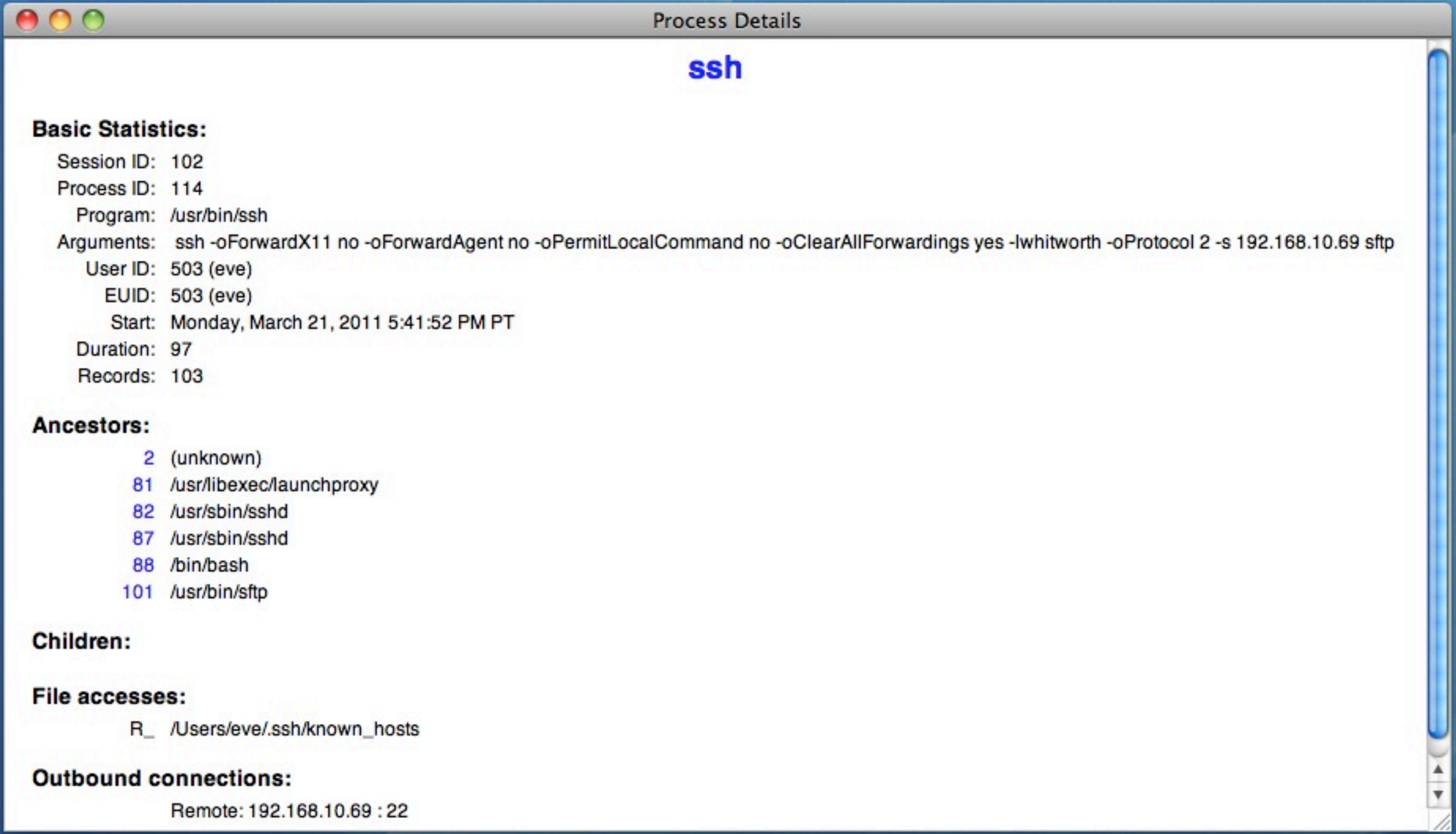
Address: 192.168.10.69 Port: 22

Session	User	Access	Address	Port	Program
102	eve	Connect	192.168.10.69	22	/usr/bin/ssh



Address: 192.168.10.69 Port: 22

Session	User	Access	Address	Port	Program
102	eve	Connect	192.168.10.69	22	/usr/bin/ssh



ssh

Basic Statistics:

Session ID: 102
Process ID: 114
Program: /usr/bin/ssh
Arguments: ssh -oForwardX11 no -oForwardAgent no -oPermitLocalCommand no -oClearAllForwardings yes -lwhitworth -oProtocol 2 -s 192.168.10.69 sftp
User ID: 503 (eve)
EUID: 503 (eve)
Start: Monday, March 21, 2011 5:41:52 PM PT
Duration: 97
Records: 103

Ancestors:

2 (unknown)
81 /usr/libexec/launchproxy
82 /usr/sbin/sshd
87 /usr/sbin/sshd
88 /bin/bash
101 /usr/bin/sftp

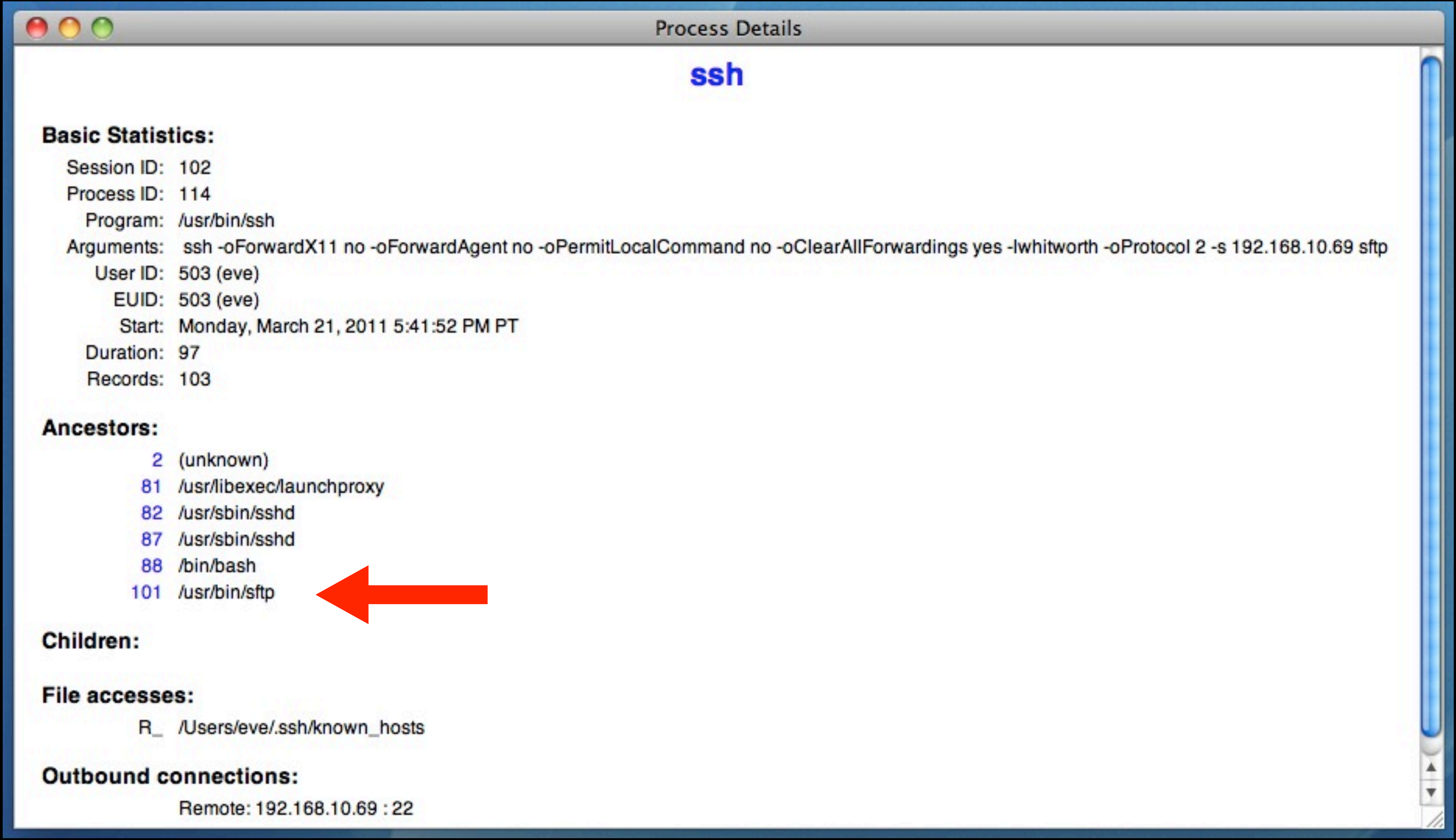
Children:

File accesses:

R_ /Users/eve/.ssh/known_hosts

Outbound connections:

Remote: 192.168.10.69 : 22



ssh

Basic Statistics:

Session ID: 102
Process ID: 114
Program: /usr/bin/ssh
Arguments: ssh -oForwardX11 no -oForwardAgent no -oPermitLocalCommand no -oClearAllForwardings yes -lwhitworth -oProtocol 2 -s 192.168.10.69 sftp
User ID: 503 (eve)
EUID: 503 (eve)
Start: Monday, March 21, 2011 5:41:52 PM PT
Duration: 97
Records: 103

Ancestors:

2 (unknown)
81 /usr/libexec/launchproxy
82 /usr/sbin/sshd
87 /usr/sbin/sshd
88 /bin/bash
101 /usr/bin/sftp

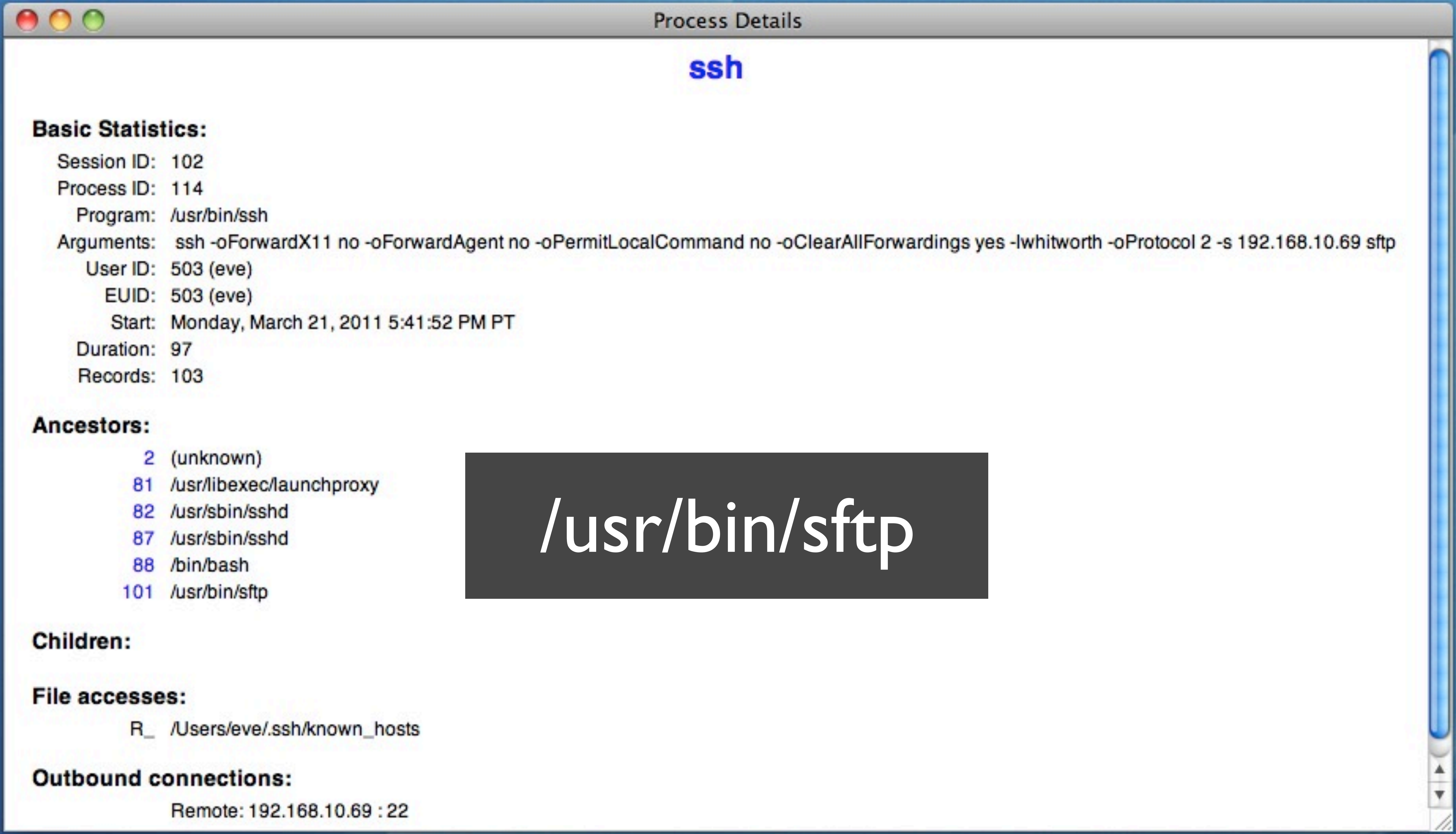
Children:

File accesses:

R_ /Users/eve/.ssh/known_hosts

Outbound connections:

Remote: 192.168.10.69 : 22



ssh

Basic Statistics:

```
  Session ID:  102
  Process ID:  114
     Program:  /usr/bin/ssh
   Arguments:   ssh -oForwardX11 no -oForwardAgent no -oPermitLocalCommand no -oClearAllForwardings yes -lwhitworth -oProtocol 2 -s 192.168.10.69 sftp
     User ID:  503 (eve)
        EUID:  503 (eve)
       Start:  Monday, March 21, 2011 5:41:52 PM PT
    Duration:  97
     Records:  103
```

Ancestors:

```
          2   (unknown)
         81   /usr/libexec/launchproxy
         82   /usr/sbin/sshd
         87   /usr/sbin/sshd
         88   /bin/bash
        101   /usr/bin/sftp
```

Children:

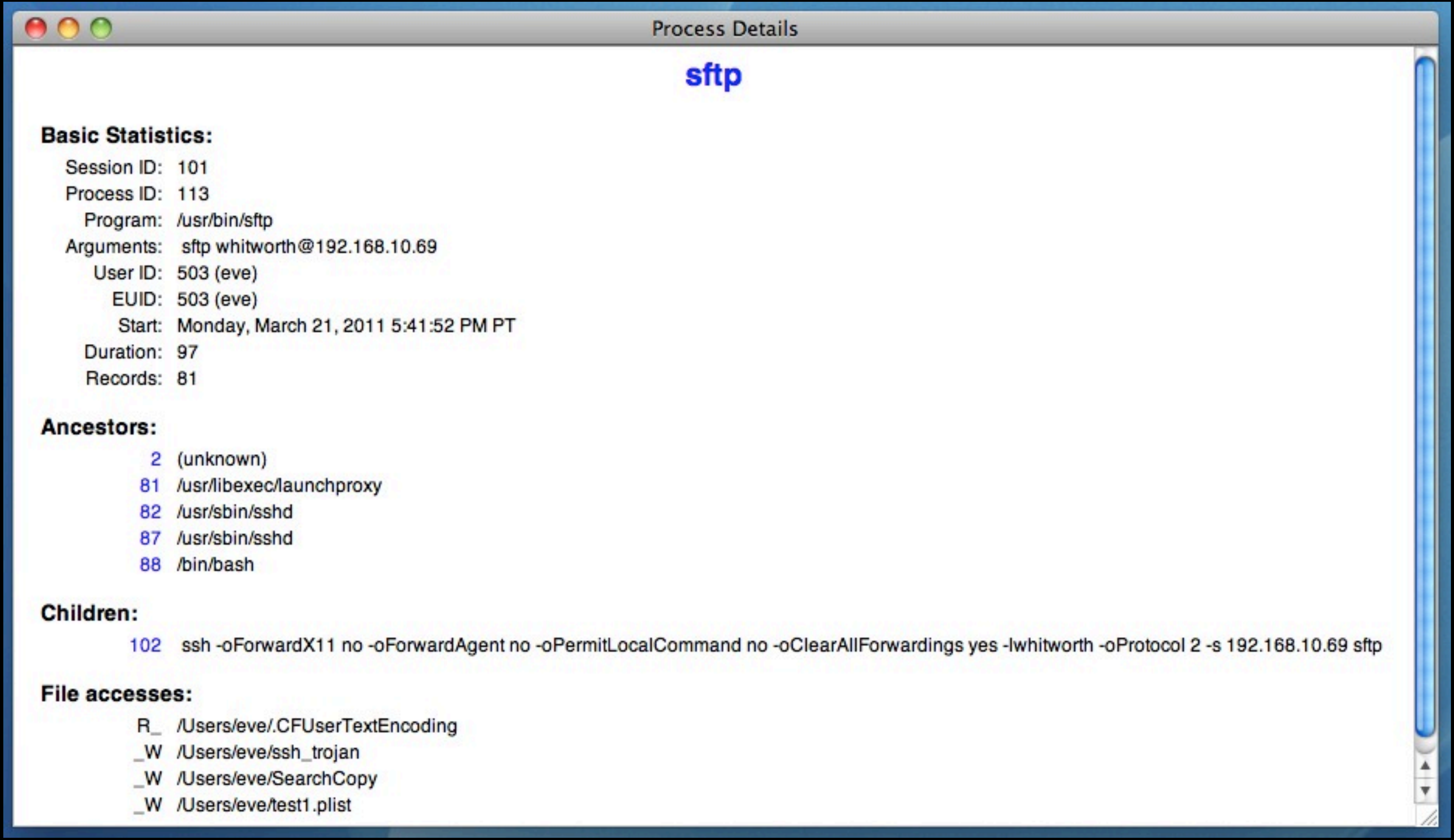
File accesses:

```
         R_   /Users/eve/.ssh/known_hosts
```

Outbound connections:

```
              Remote: 192.168.10.69 : 22
```

/usr/bin/sftp



sftp

Basic Statistics:

Session ID: 101
Process ID: 113
Program: /usr/bin/sftp
Arguments: sftp whitworth@192.168.10.69
User ID: 503 (eve)
EUID: 503 (eve)
Start: Monday, March 21, 2011 5:41:52 PM PT
Duration: 97
Records: 81

Ancestors:

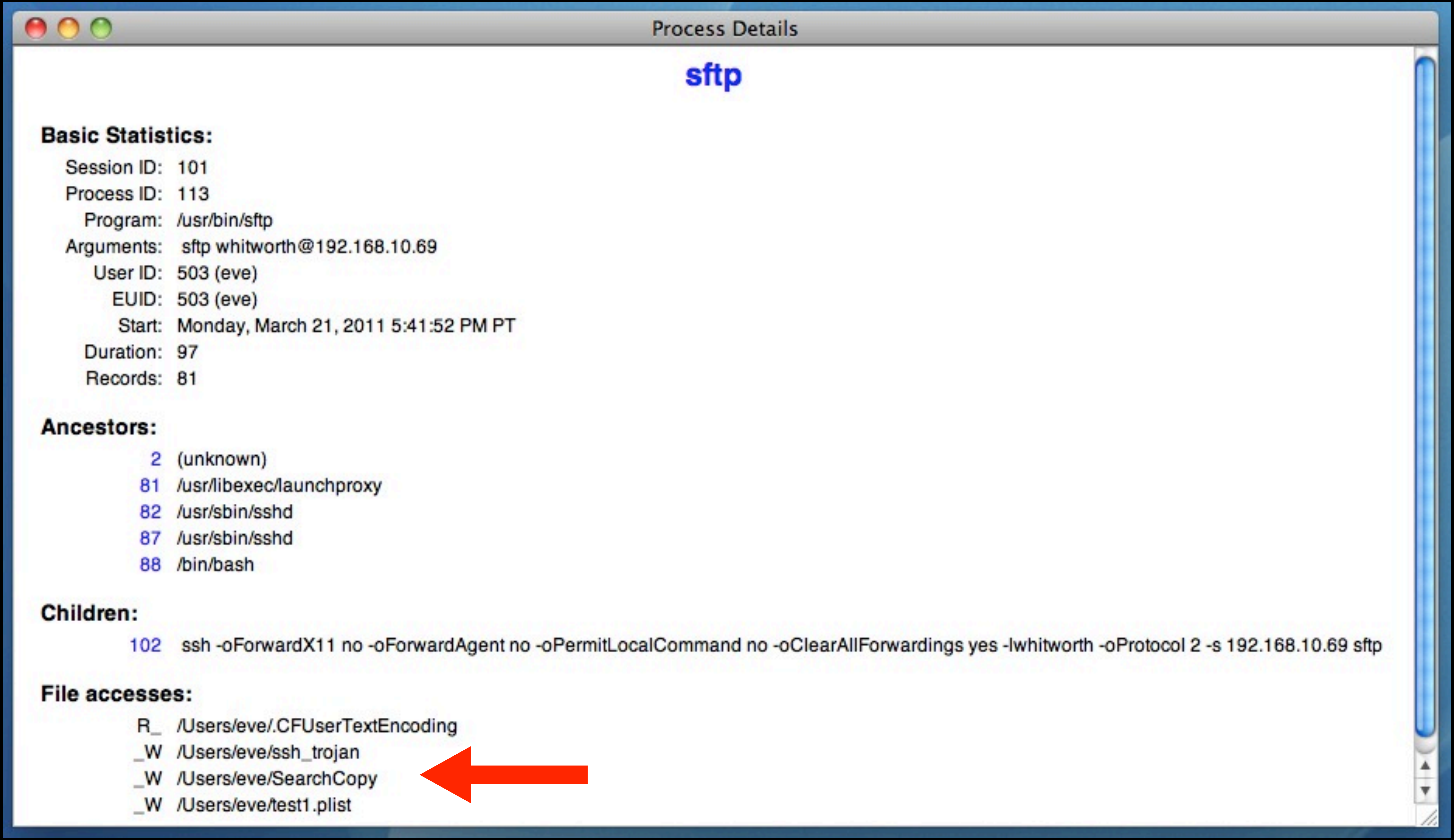
2 (unknown)
81 /usr/libexec/launchproxy
82 /usr/sbin/sshd
87 /usr/sbin/sshd
88 /bin/bash

Children:

102 ssh -oForwardX11 no -oForwardAgent no -oPermitLocalCommand no -oClearAllForwardings yes -lwhitworth -oProtocol 2 -s 192.168.10.69 sftp

File accesses:

R_ /Users/eve/.CFUserTextEncoding
_W /Users/eve/ssh_trojan
_W /Users/eve/SearchCopy
_W /Users/eve/test1.plist



sftp

Basic Statistics:

Session ID: 101
Process ID: 113
Program: /usr/bin/sftp
Arguments: sftp whitworth@192.168.10.69
User ID: 503 (eve)
EUID: 503 (eve)
Start: Monday, March 21, 2011 5:41:52 PM PT
Duration: 97
Records: 81

Ancestors:

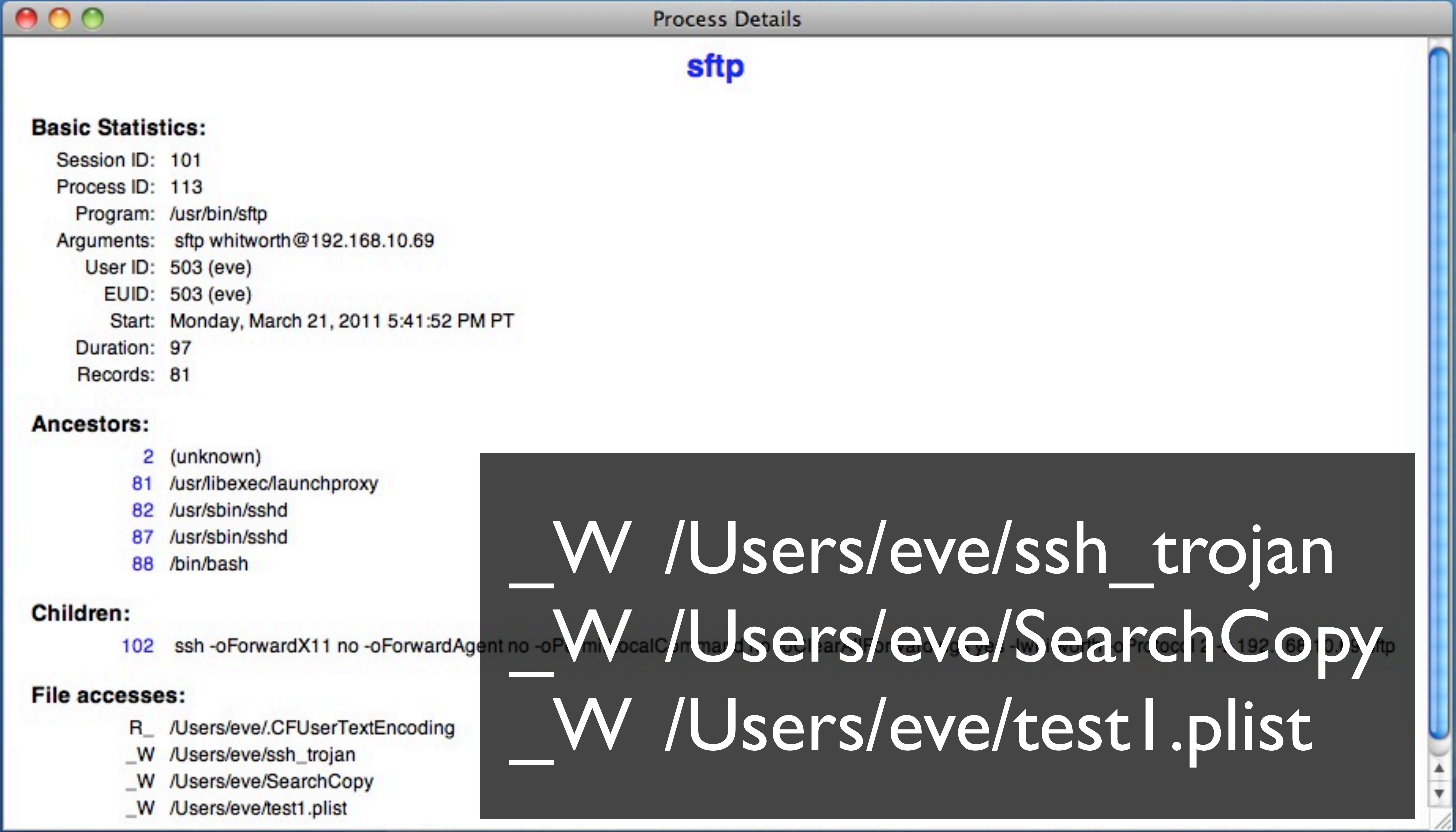
2	(unknown)
81	/usr/libexec/launchproxy
82	/usr/sbin/sshd
87	/usr/sbin/sshd
88	/bin/bash

Children:

102	ssh -oForwardX11 no -oForwardAgent no -oPermitLocalCommand no -oClearAllForwardings yes -lwhitworth -oProtocol 2 -s 192.168.10.69 sftp

File accesses:

R_	/Users/eve/.CFUserTextEncoding
_W	/Users/eve/ssh_trojan
_W	/Users/eve/SearchCopy
_W	/Users/eve/test1.plist



sftp

Basic Statistics:

Session ID:	101
Process ID:	113
Program:	/usr/bin/sftp
Arguments:	sftp whitworth@192.168.10.69
User ID:	503 (eve)
EUID:	503 (eve)
Start:	Monday, March 21, 2011 5:41:52 PM PT
Duration:	97
Records:	81

Ancestors:

2	(unknown)
81	/usr/libexec/launchproxy
82	/usr/sbin/sshd
87	/usr/sbin/sshd
88	/bin/bash

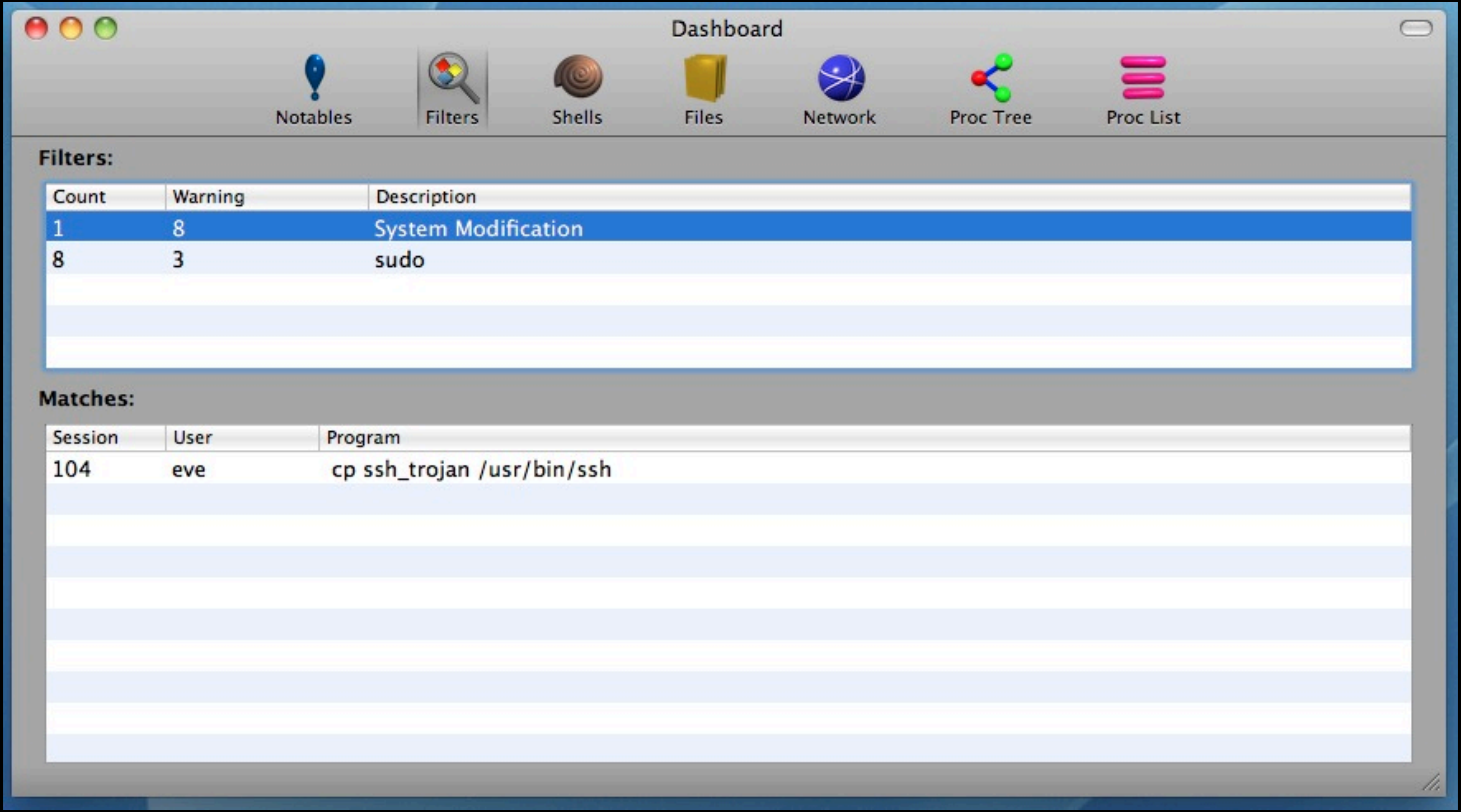
Children:

102 ssh -oForwardX11 no -oForwardAgent no -oP

File accesses:

R_	/Users/eve/.CFUserTextEncoding
_W	/Users/eve/ssh_trojan
_W	/Users/eve/SearchCopy
_W	/Users/eve/test1.plist

_W /Users/eve/ssh_trojan
_W /Users/eve/SearchCopy
_W /Users/eve/test1.plist

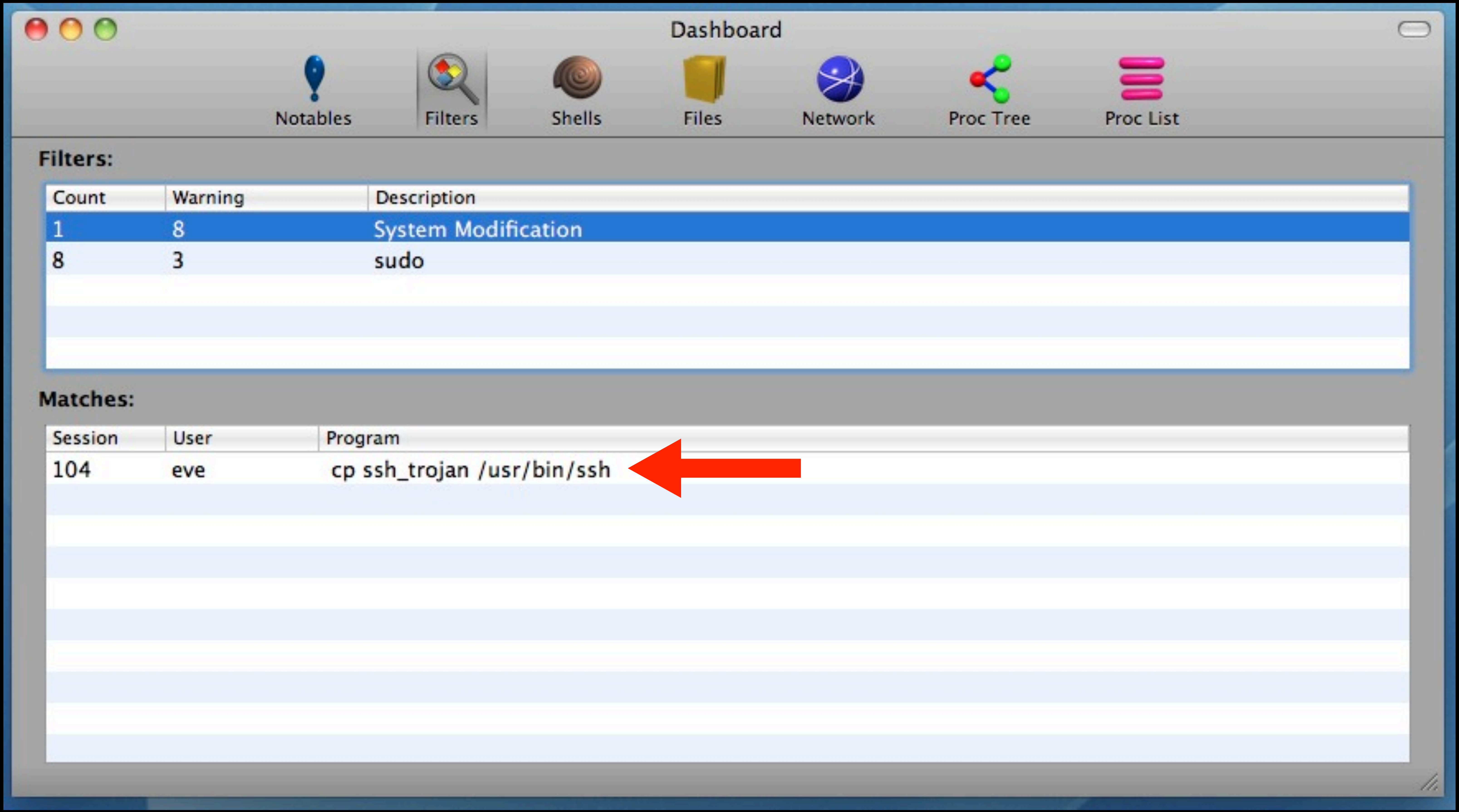


Filters:

Count	Warning	Description
1	8	System Modification
8	3	sudo

Matches:

Session	User	Program
104	eve	cp ssh_trojan /usr/bin/ssh

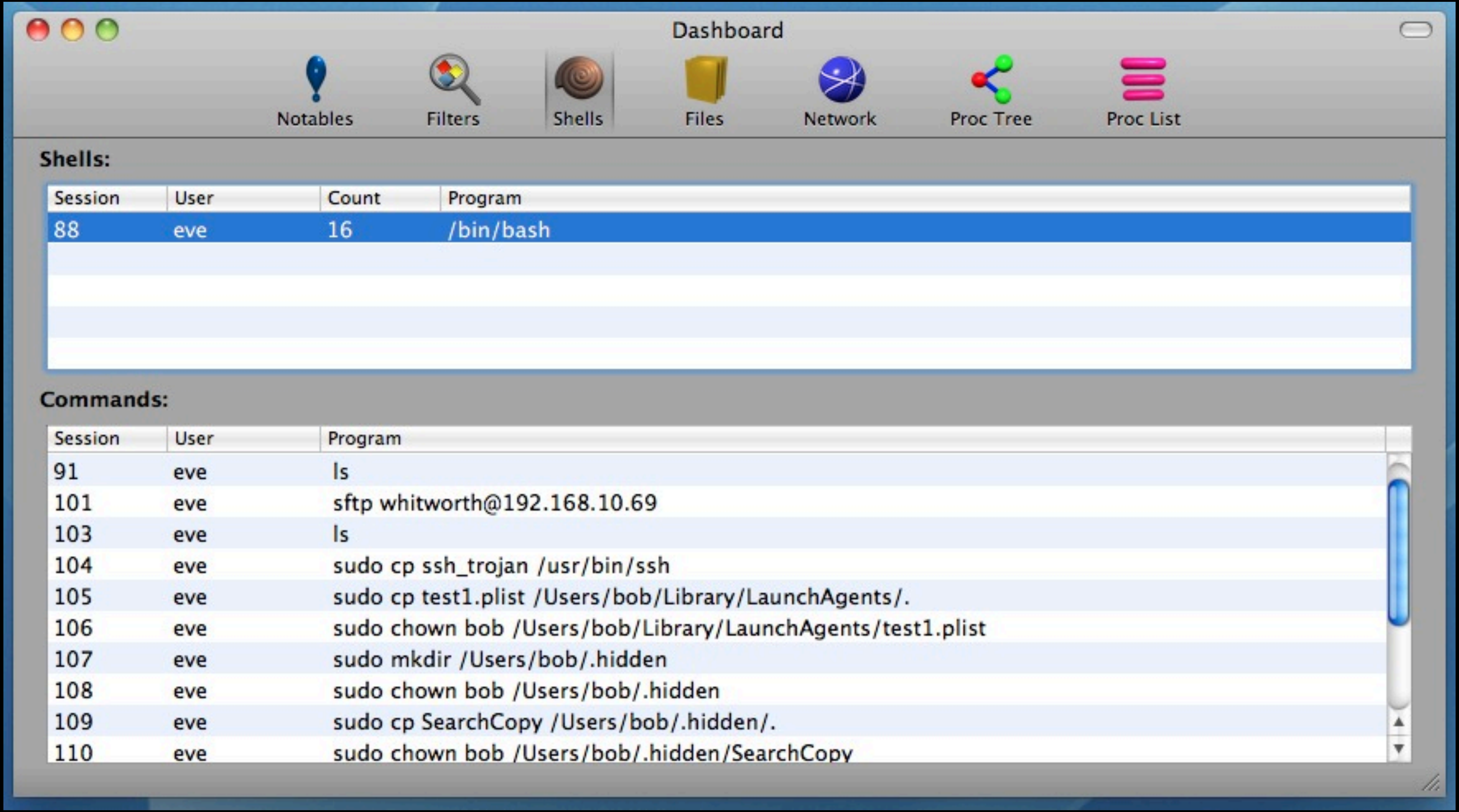


Filters:

Count	Warning	Description
1	8	System Modification
8	3	sudo

Matches:

Session	User	Program
104	eve	cp ssh_trojan /usr/bin/ssh

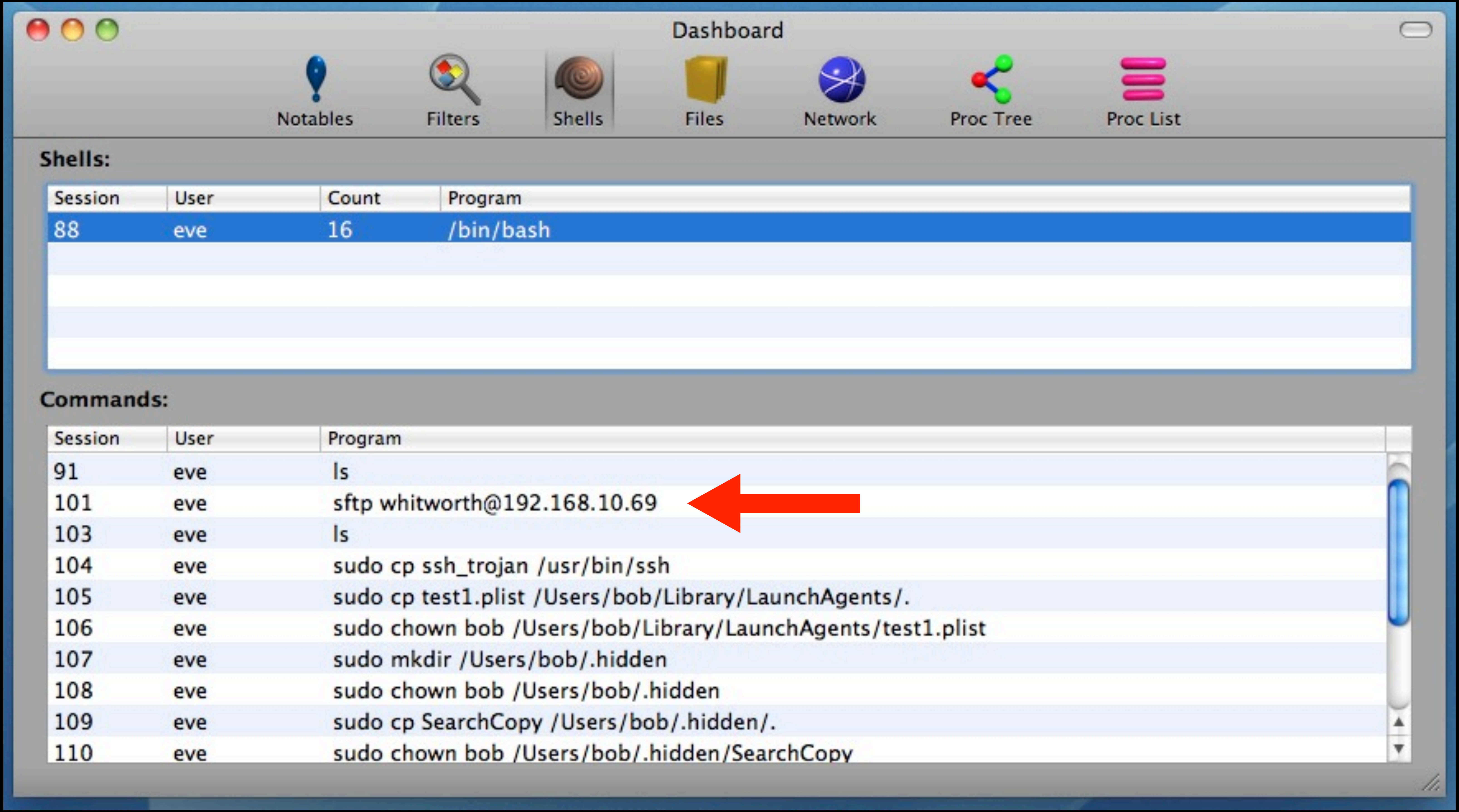


Shells:

Session	User	Count	Program
88	eve	16	/bin/bash

Commands:

Session	User	Program
91	eve	ls
101	eve	sftp whitworth@192.168.10.69
103	eve	ls
104	eve	sudo cp ssh_trojan /usr/bin/ssh
105	eve	sudo cp test1.plist /Users/bob/Library/LaunchAgents/.
106	eve	sudo chown bob /Users/bob/Library/LaunchAgents/test1.plist
107	eve	sudo mkdir /Users/bob/.hidden
108	eve	sudo chown bob /Users/bob/.hidden
109	eve	sudo cp SearchCopy /Users/bob/.hidden/.
110	eve	sudo chown bob /Users/bob/.hidden/SearchCopy

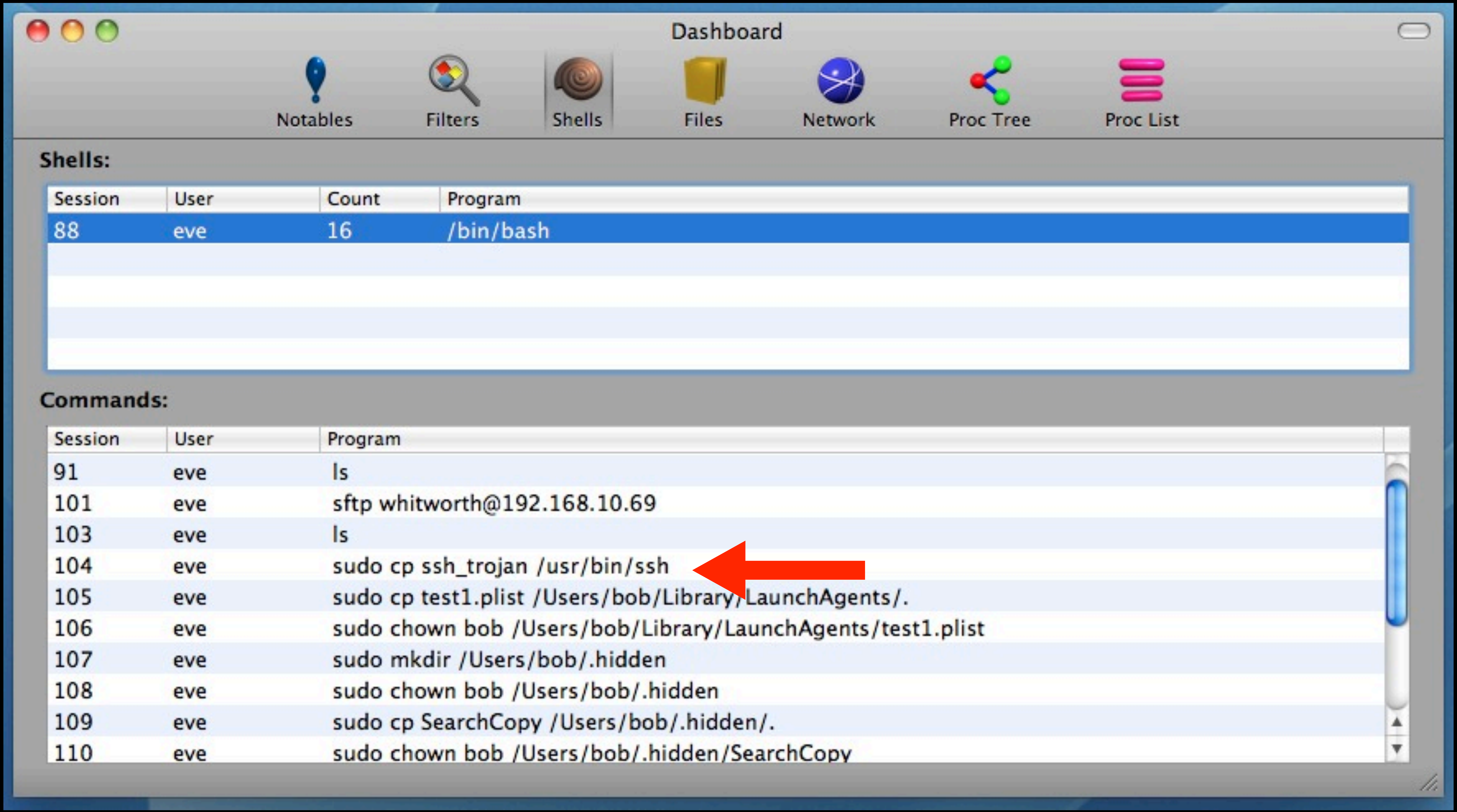


Shells:

Session	User	Count	Program
88	eve	16	/bin/bash

Commands:

Session	User	Program
91	eve	ls
101	eve	sftp whitworth@192.168.10.69
103	eve	ls
104	eve	sudo cp ssh_trojan /usr/bin/ssh
105	eve	sudo cp test1.plist /Users/bob/Library/LaunchAgents/.
106	eve	sudo chown bob /Users/bob/Library/LaunchAgents/test1.plist
107	eve	sudo mkdir /Users/bob/.hidden
108	eve	sudo chown bob /Users/bob/.hidden
109	eve	sudo cp SearchCopy /Users/bob/.hidden/.
110	eve	sudo chown bob /Users/bob/.hidden/SearchCopy

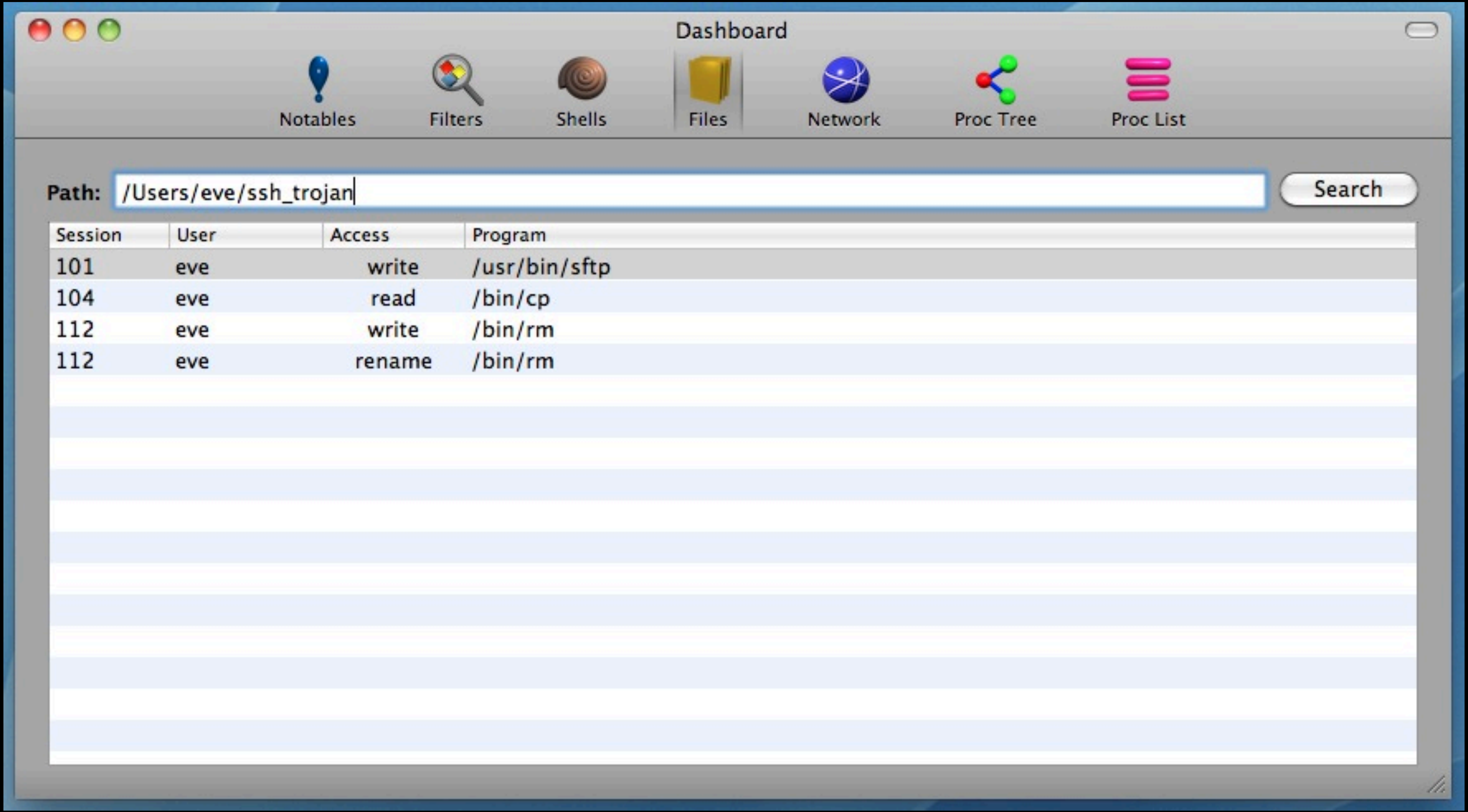


Shells:

Session	User	Count	Program
88	eve	16	/bin/bash

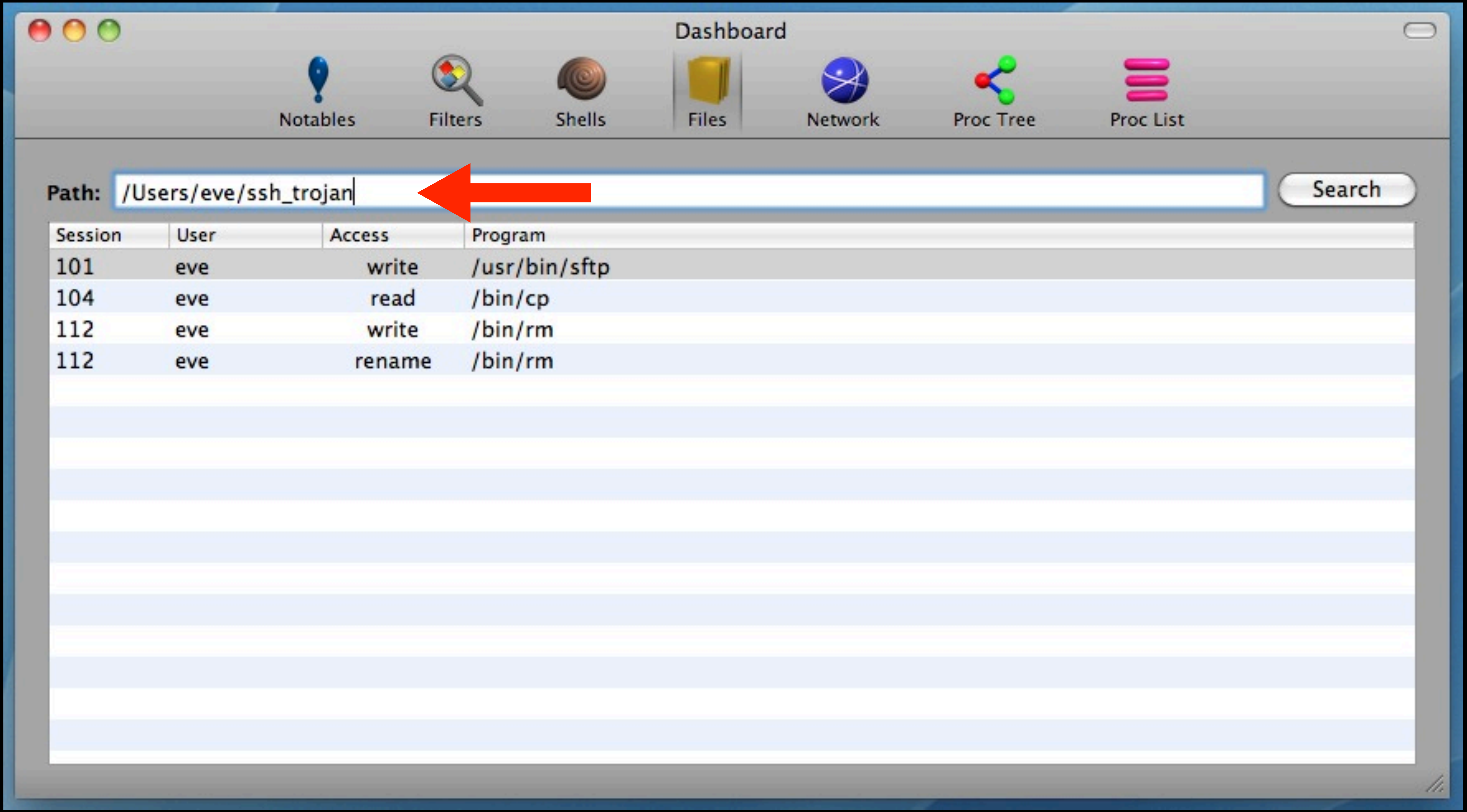
Commands:

Session	User	Program
91	eve	ls
101	eve	sftp whitworth@192.168.10.69
103	eve	ls
104	eve	sudo cp ssh_trojan /usr/bin/ssh
105	eve	sudo cp test1.plist /Users/bob/Library/LaunchAgents/.
106	eve	sudo chown bob /Users/bob/Library/LaunchAgents/test1.plist
107	eve	sudo mkdir /Users/bob/.hidden
108	eve	sudo chown bob /Users/bob/.hidden
109	eve	sudo cp SearchCopy /Users/bob/.hidden/.
110	eve	sudo chown bob /Users/bob/.hidden/SearchCopy



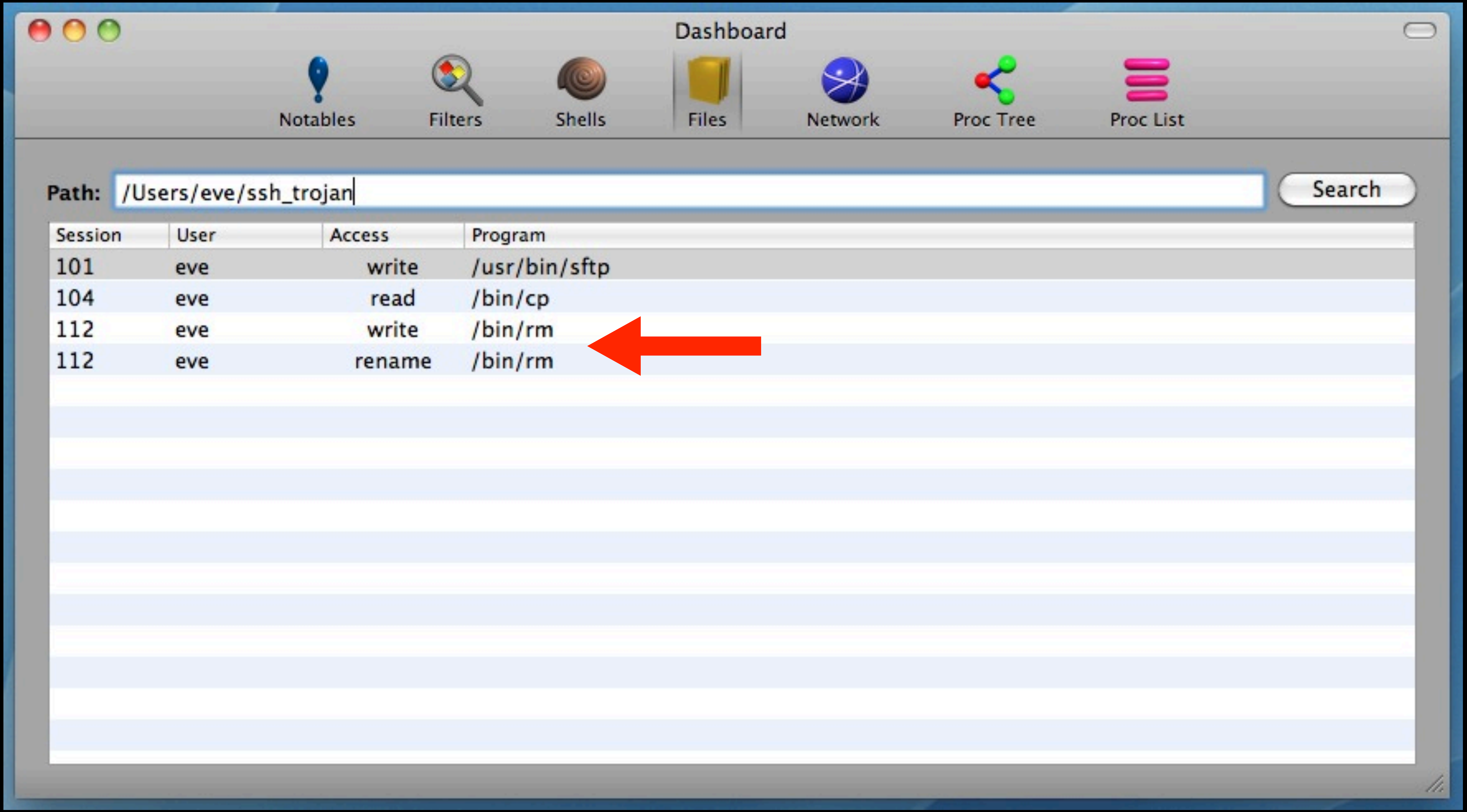
Path: /Users/eve/ssh_trojan

Session	User	Access	Program
101	eve	write	/usr/bin/sftp
104	eve	read	/bin/cp
112	eve	write	/bin/rm
112	eve	rename	/bin/rm



Path: /Users/eve/ssh_trojan

Session	User	Access	Program
101	eve	write	/usr/bin/sftp
104	eve	read	/bin/cp
112	eve	write	/bin/rm
112	eve	rename	/bin/rm



Path: /Users/eve/ssh_trojan

Session	User	Access	Program
101	eve	write	/usr/bin/sftp
104	eve	read	/bin/cp
112	eve	write	/bin/rm
112	eve	rename	/bin/rm

Conclusions

Conclusions

- Your current security architecture is ineffective against modern attacks

Conclusions

- Your current security architecture is ineffective against modern attacks
- As Mac owners, we've been lucky!

Conclusions

- Your current security architecture is ineffective against modern attacks
- As Mac owners, we’ve been lucky!
- Your Mac has a powerful auditing system installed & running called BSM

Conclusions

- Your current security architecture is ineffective against modern attacks
- As Mac owners, we’ve been lucky!
- Your Mac has a powerful auditing system installed & running called BSM
- Default BSM analysis tools are arcane and mind numbing

Conclusions

- Your current security architecture is ineffective against modern attacks
- As Mac owners, we've been lucky!
- Your Mac has a powerful auditing system installed & running called BSM
- Default BSM analysis tools are arcane and mind numbing
- Better tools are starting to make their way to market

Thank you!

Thank you!

todd_heberlein@mac.com

LTH@NetSQ.com