Google: The APT You Have

Todd Heberlein
Net Squared, Inc.
2 Aug 2012

SANS San Francisco
https://www.sans.org/san-francisco-2012/

Practice, Practice, Practice

Todd Heberlein
Net Squared, Inc.
2 Aug 2012

SANS San Francisco
https://www.sans.org/san-francisco-2012/

Overview

Overview

- Thoughts on “Advanced Persistent Threats”

Overview

- Thoughts on “Advanced Persistent Threats”
- What’s next after signatures (back to anomaly detection?)

Overview

- Thoughts on “Advanced Persistent Threats”
- What’s next after signatures (back to anomaly detection?)
- The problem with uncertainty

Overview

- Thoughts on “Advanced Persistent Threats”
- What’s next after signatures (back to anomaly detection?)
- The problem with uncertainty
- From test to diagnosis

Overview

- Thoughts on “Advanced Persistent Threats”
- What’s next after signatures (back to anomaly detection?)
- The problem with uncertainty
- From test to diagnosis
- End of the line for network analysis

Overview

- Thoughts on "Advanced Persistent Threats"
- What's next after signatures (back to anomaly detection?)
- The problem with uncertainty
- From test to diagnosis
- End of the line for network analysis
- Role of audit trails

Overview

- Thoughts on “Advanced Persistent Threats”
- What’s next after signatures (back to anomaly detection?)
- The problem with uncertainty
- From test to diagnosis
- End of the line for network analysis
- Role of audit trails
- Google, the APT, from the audit trail perspective

Thoughts on “Advanced Persistent Threats”

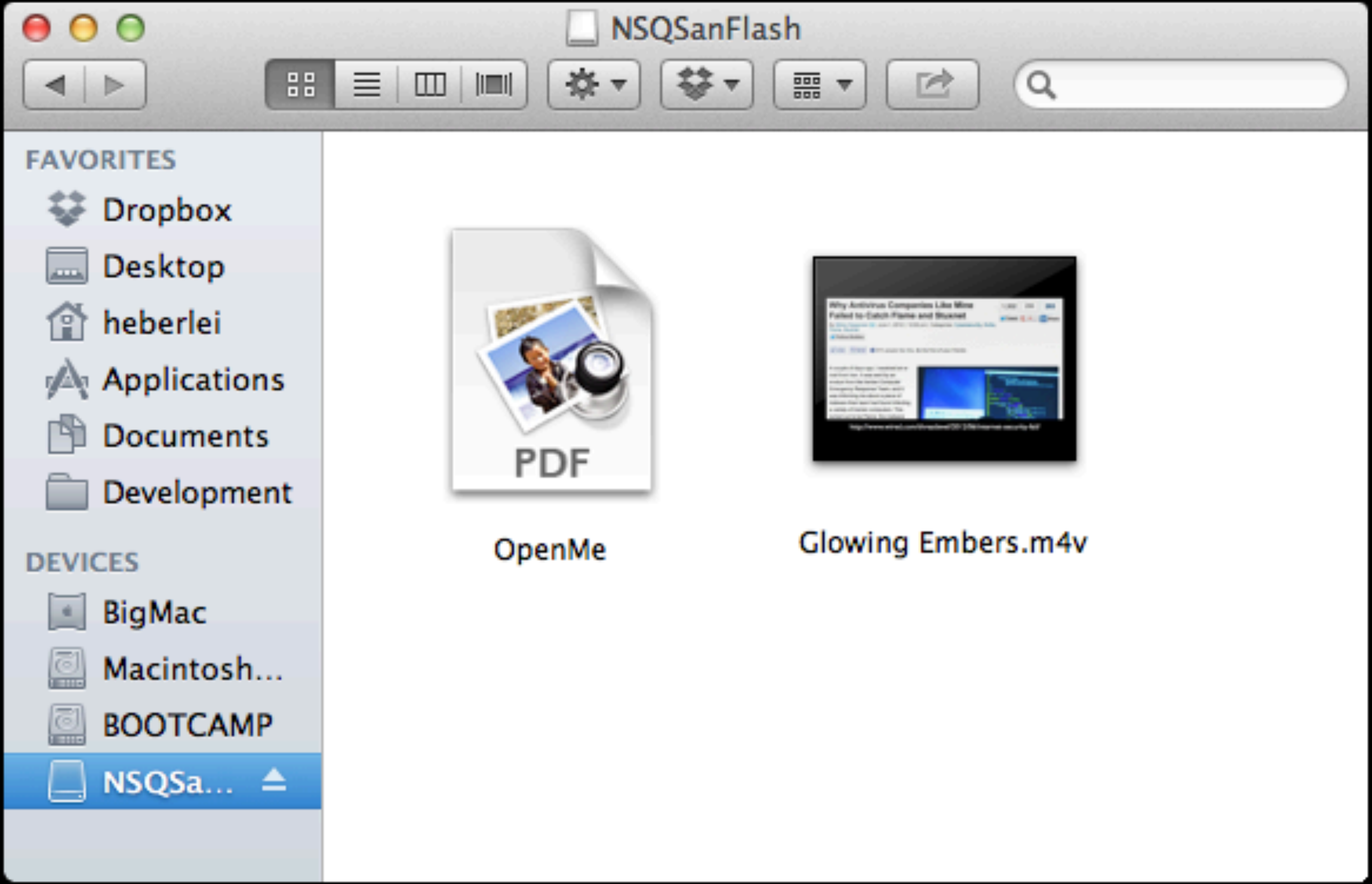
Advanced Persistent Threat

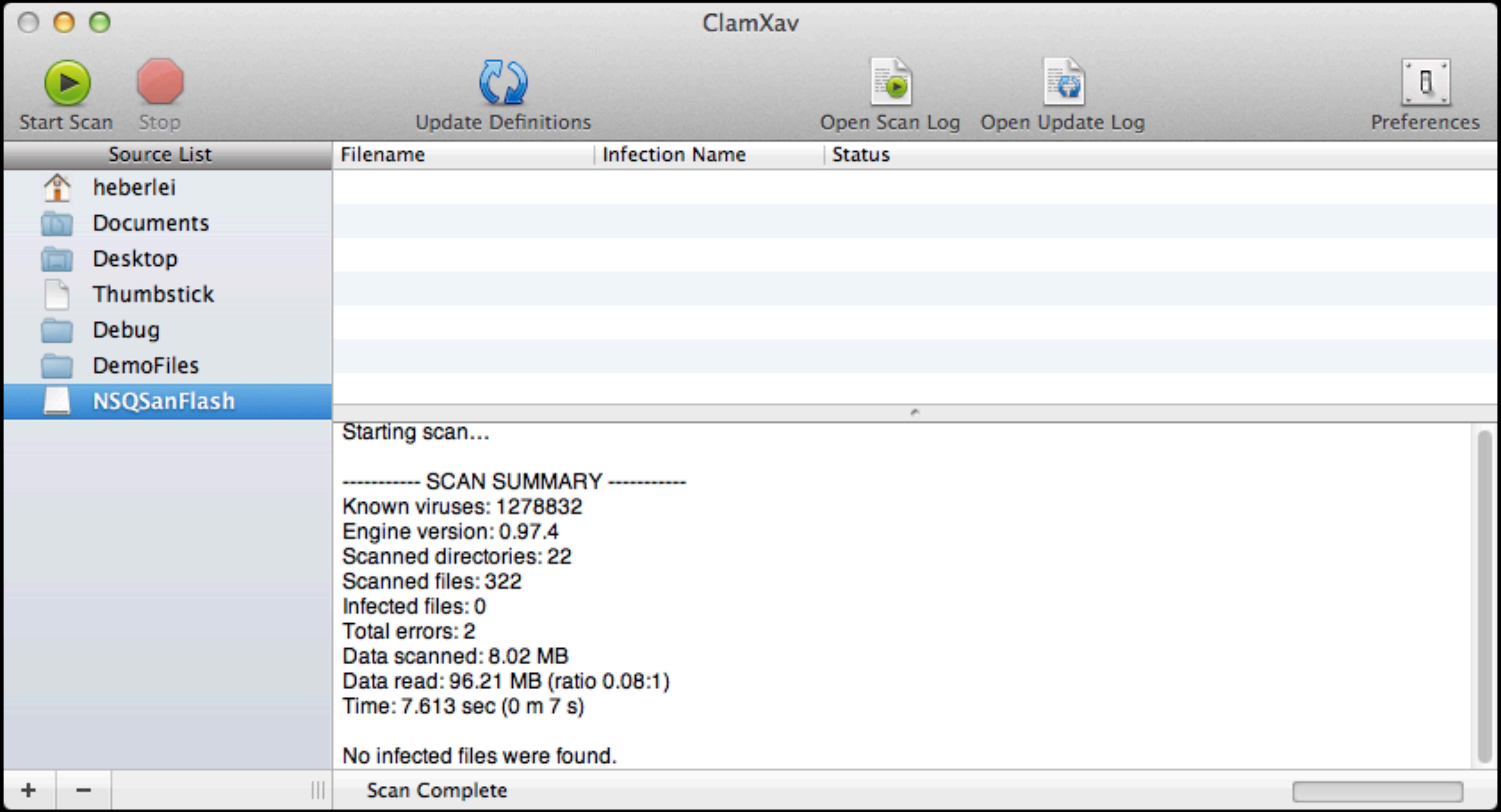
Advanced Persistent Threat

Anything that gets past automated detection / prevention

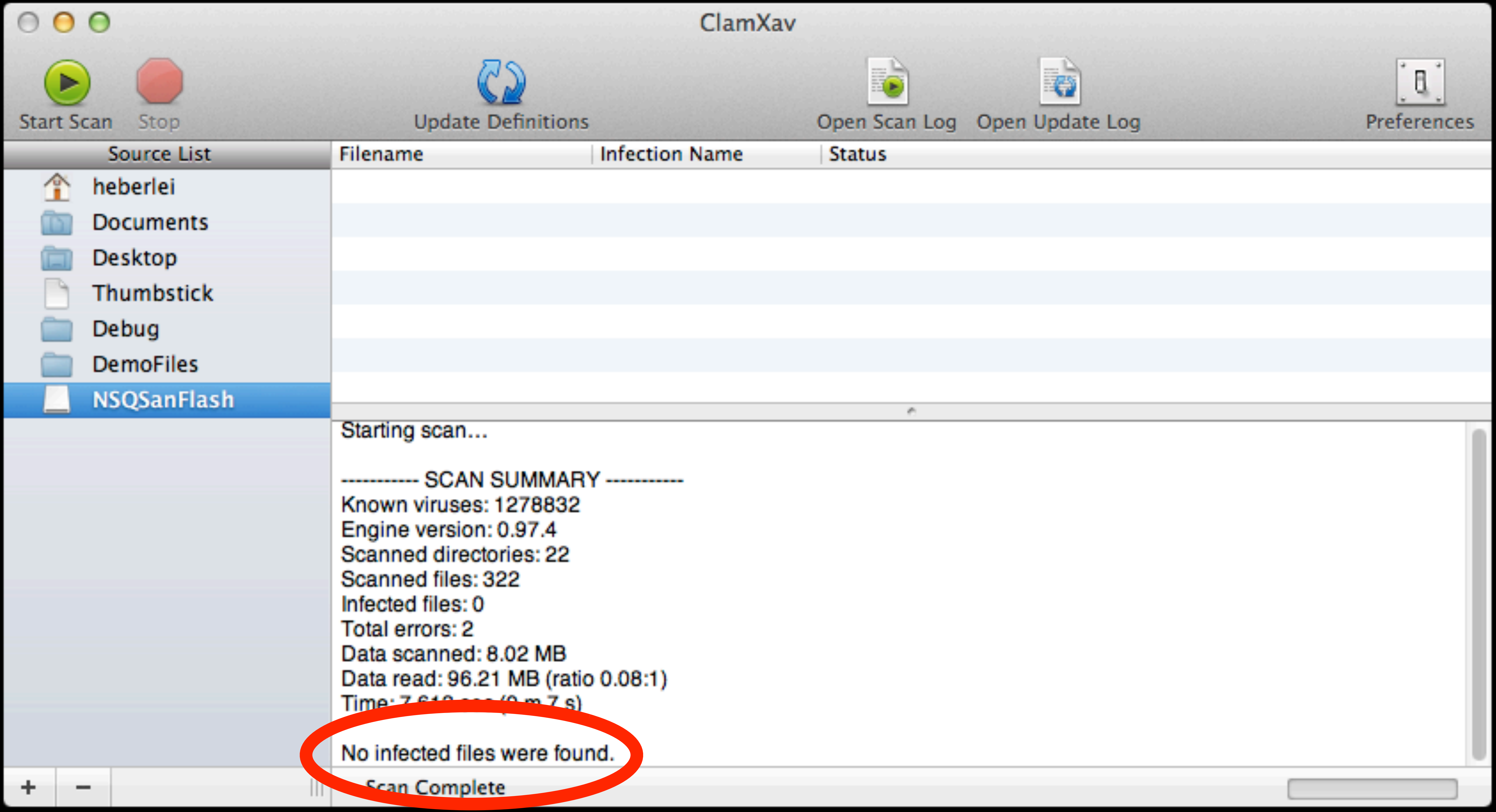
Demo

(PDF Trojan horse)


NSQSanFlash
FAVORITES
Dropbox
Desktop
heberlei
Applications
Documents
Development
DEVICES
BigMac
Macintosh...
BOOTCAMP
NSQSa...
PDF
OpenMe
Glowing Embers.m4v

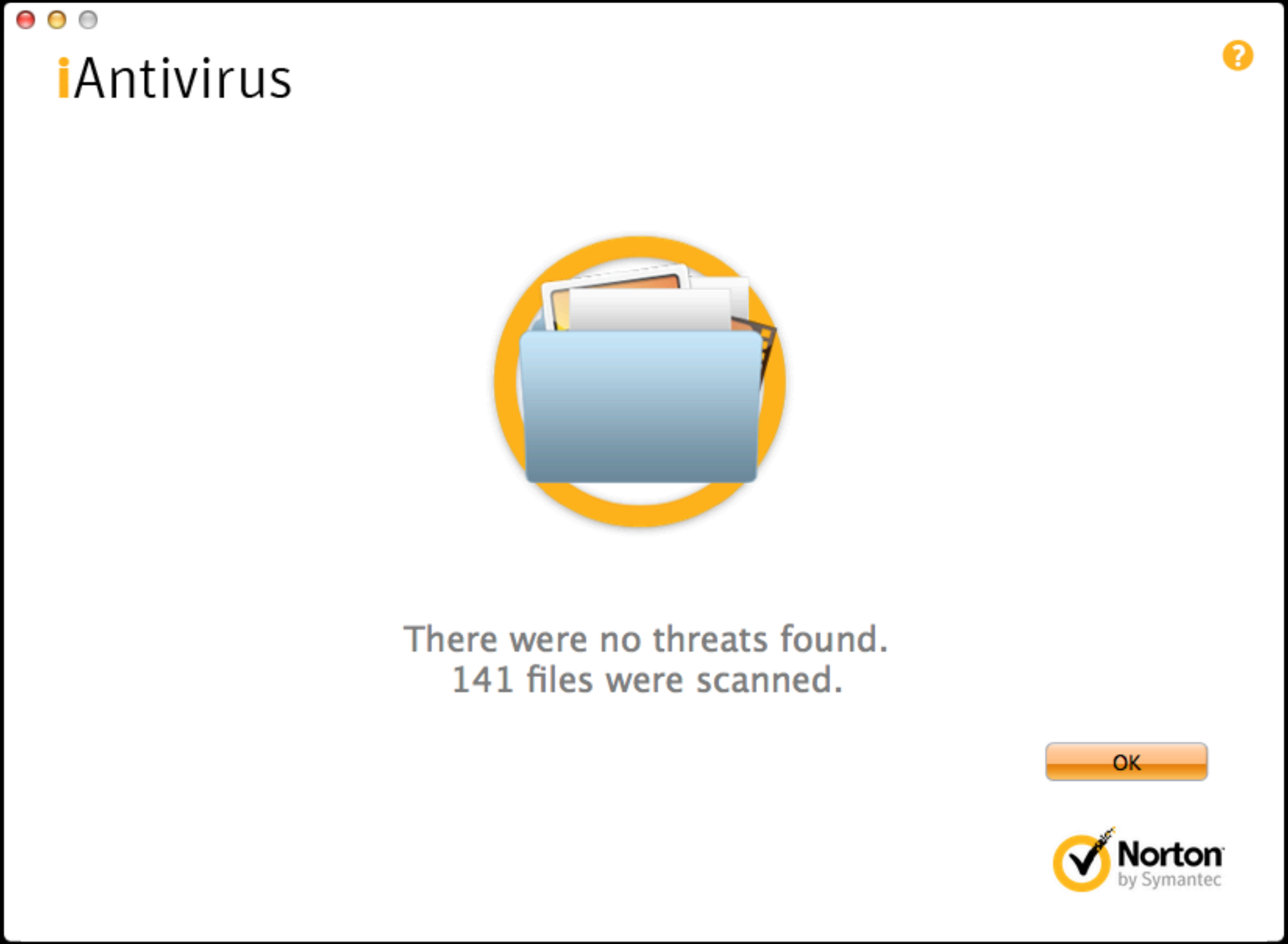


```
Starting scan...

----------- SCAN SUMMARY -----------
Known viruses: 1278832
Engine version: 0.97.4
Scanned directories: 22
Scanned files: 322
Infected files: 0
Total errors: 2
Data scanned: 8.02 MB
Data read: 96.21 MB (ratio 0.08:1)
Time: 7.613 sec (0 m 7 s)

No infected files were found.
```

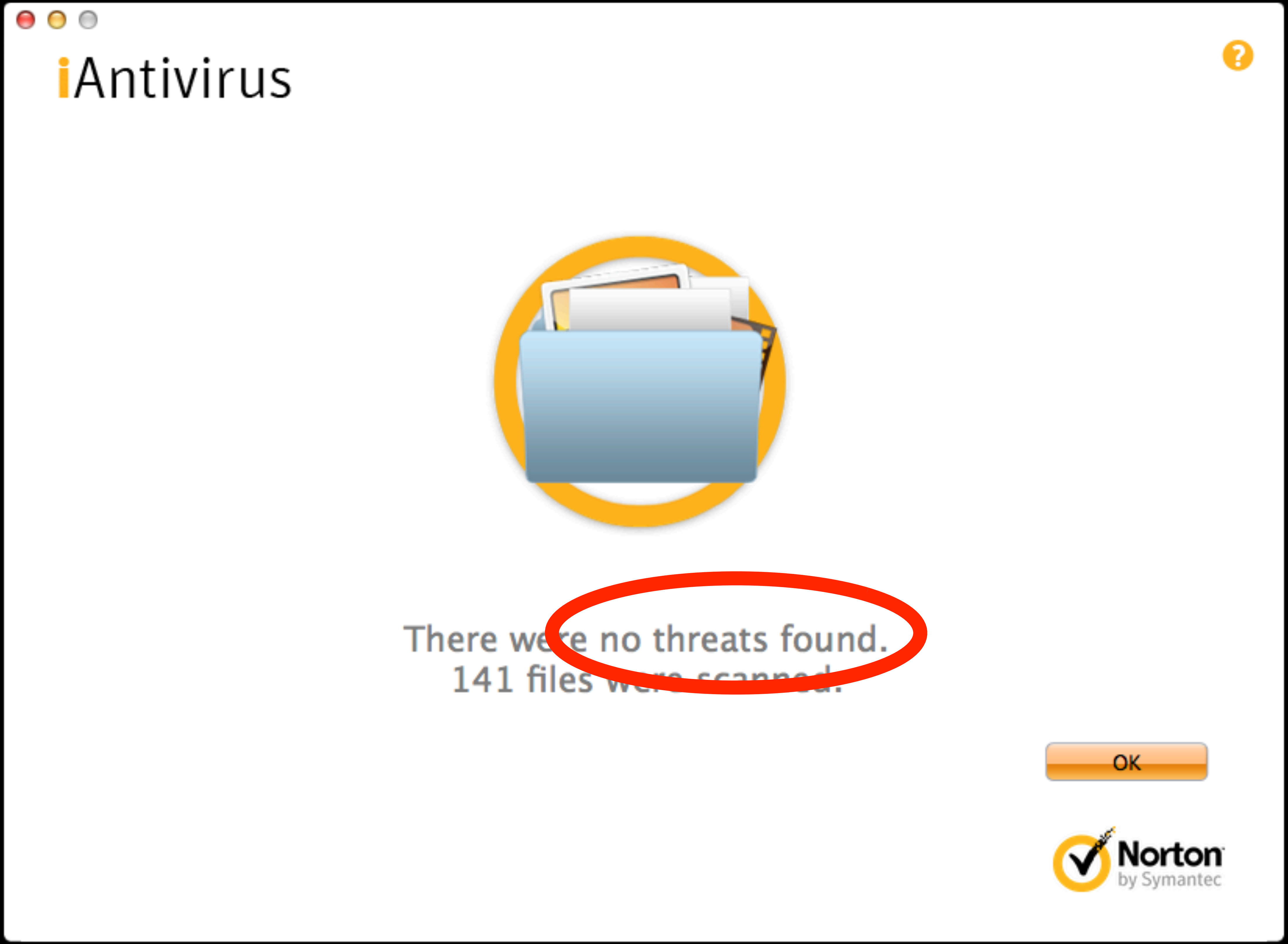


```
Starting scan...

----------- SCAN SUMMARY -----------
Known viruses: 1278832
Engine version: 0.97.4
Scanned directories: 22
Scanned files: 322
Infected files: 0
Total errors: 2
Data scanned: 8.02 MB
Data read: 96.21 MB (ratio 0.08:1)
Time: 7.610 sec (0 m 7 s)

No infected files were found.
```

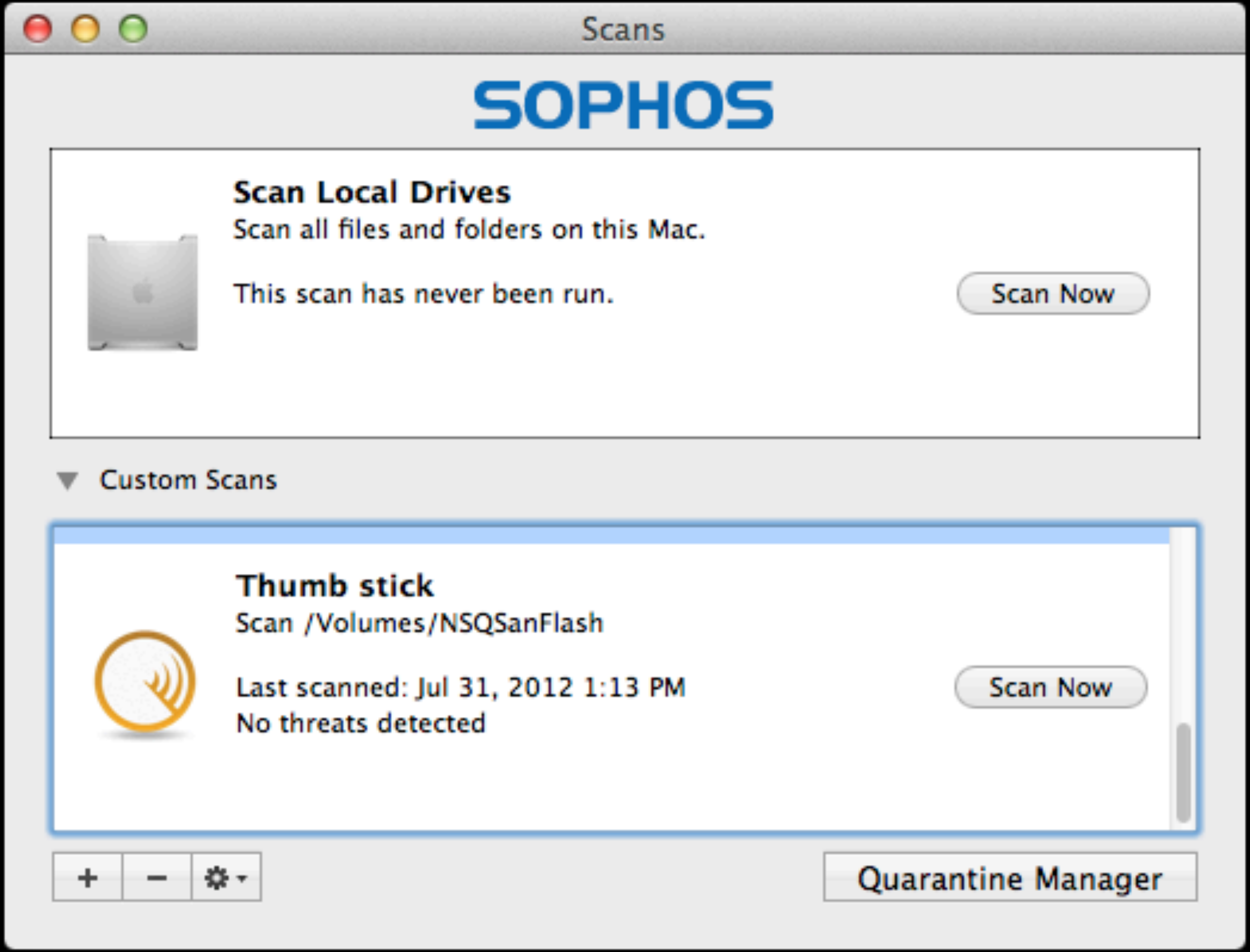
Scan Complete



There were no threats found.
141 files were scanned.



There were no threats found.
141 files were scanned.



Scans

SOPHOS

Scan Local Drives

Scan all files and folders on this Mac.

This scan has never been run.

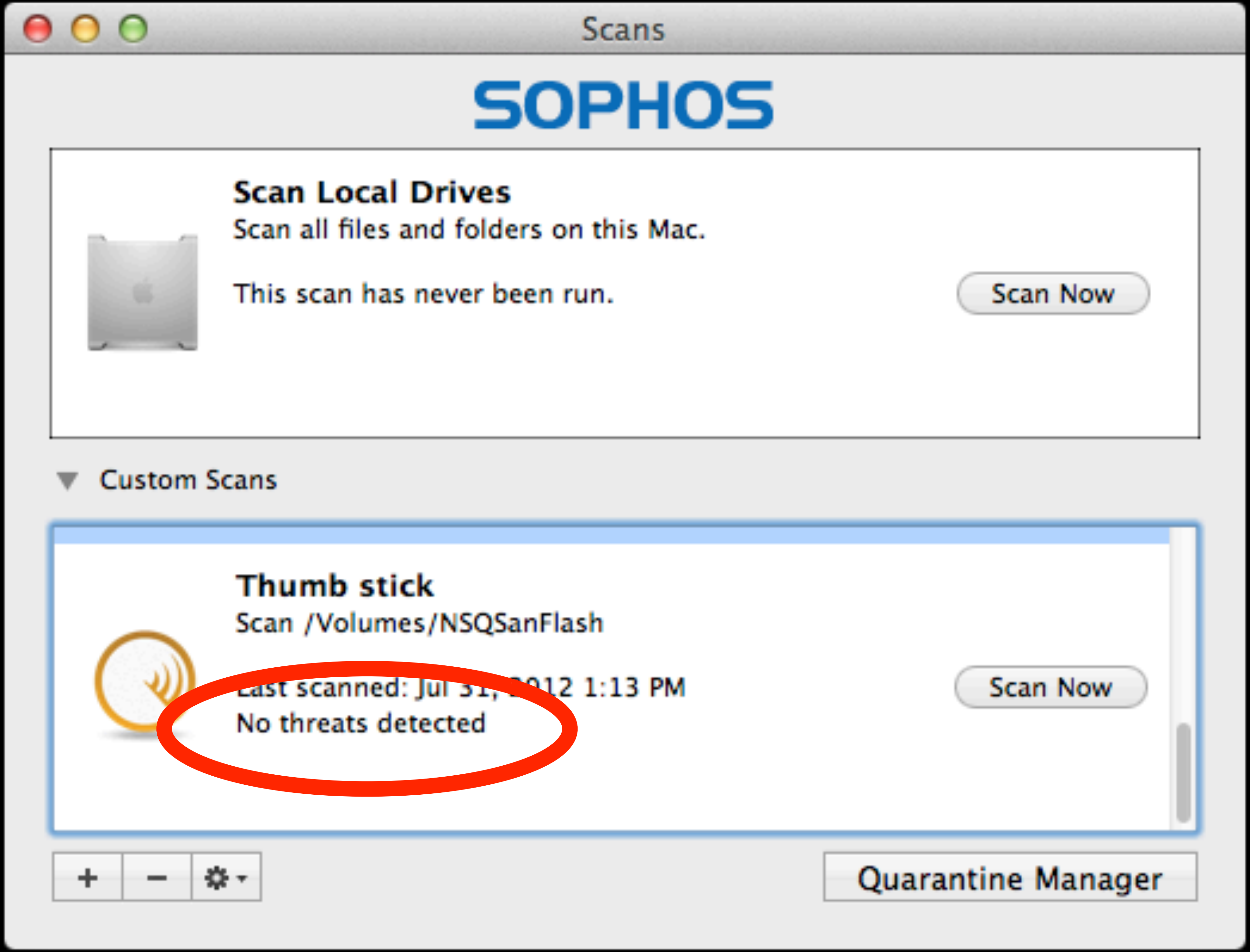
▼ Custom Scans

Thumb stick

Scan /Volumes/NSQSanFlash

Last scanned: Jul 31, 2012 1:13 PM

No threats detected



Scan Local Drives

Scan all files and folders on this Mac.

This scan has never been run.

Thumb stick

Scan /Volumes/NSQSanFlash

Last scanned: Jul 31, 2012 1:13 PM

No threats detected

```
int main(int argc, char *argv[])
{
    @autoreleasepool {

        /* Open embedded PDF File */
        NSBundle *myBundle = [NSBundle mainBundle];
        NSString *filepath = [NSString stringWithFormat:
                              @"%@/Contents/Resources/Aurora.pdf",
                              [myBundle bundlePath]];
        [[NSWorkspace sharedWorkspace] openFile:filepath];

        /* Do Trojan-y stuff */
        FILE* fp = fopen("/Users/heberlei/Demo/HelloWorld.txt", "w");
        if (fp != NULL) {
            fprintf(fp, "Free Kevin!");
            fclose(fp);
        }
    }
    exit(0);
    return NSApplicationMain(argc, (const char **)argv);
}
```

“Advanced” Attack ??

“Advanced” Attack ??

- OS is fully patched system

“Advanced” Attack ??

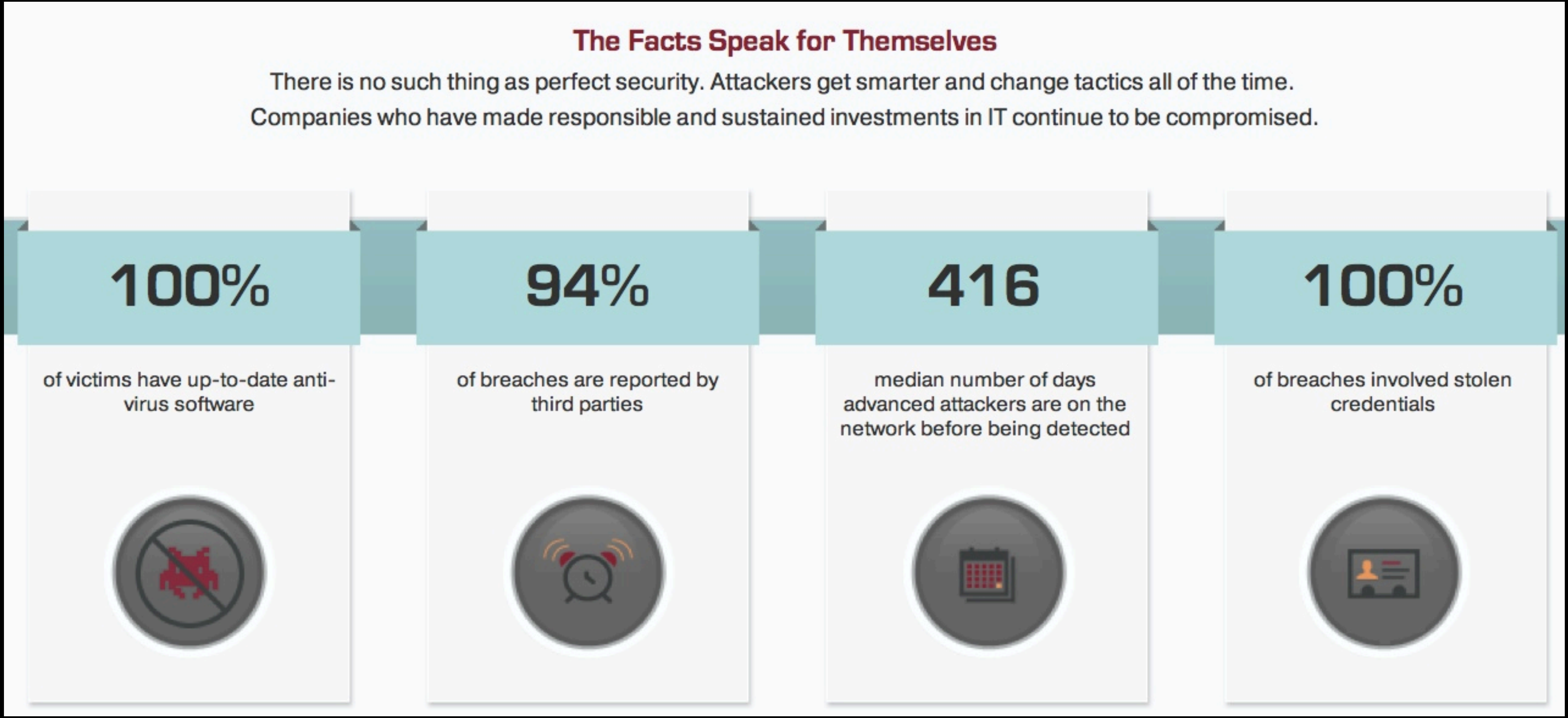
- OS is fully patched system
- Gatekeeper is on

“Advanced” Attack ??

- OS is fully patched system
- Gatekeeper is on
- My three AV systems say everything is good

“Advanced” Attack ??

- OS is fully patched system
- Gatekeeper is on
- My three AV systems say everything is good
- Minutes to write



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/

Advanced Persistent Threat

Advanced Persistent Threat

1: Relentless until successful

Not a crime of opportunity

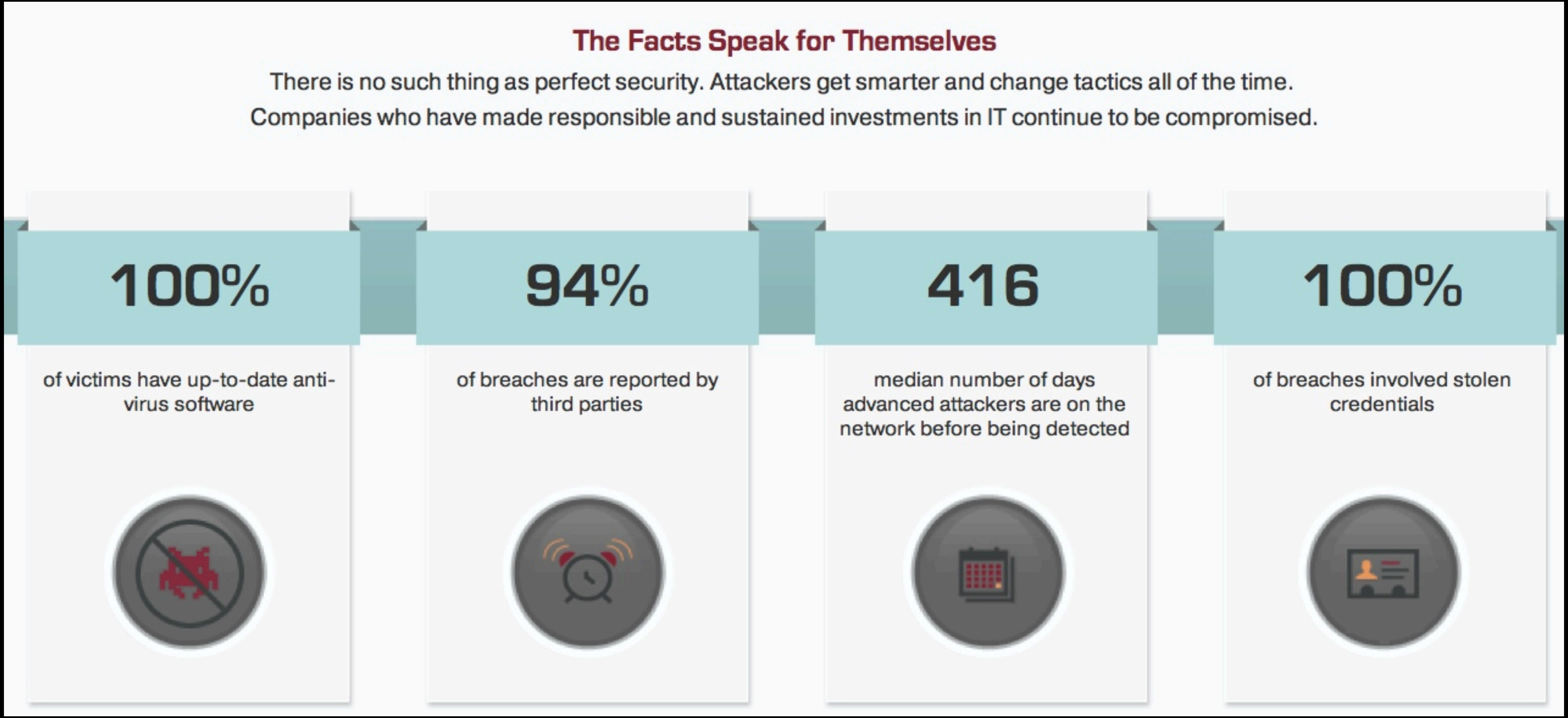
Advanced Persistent Threat

1: Relentless until successful

Not a crime of opportunity

2: Long-lived

No longer a smash and grab



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

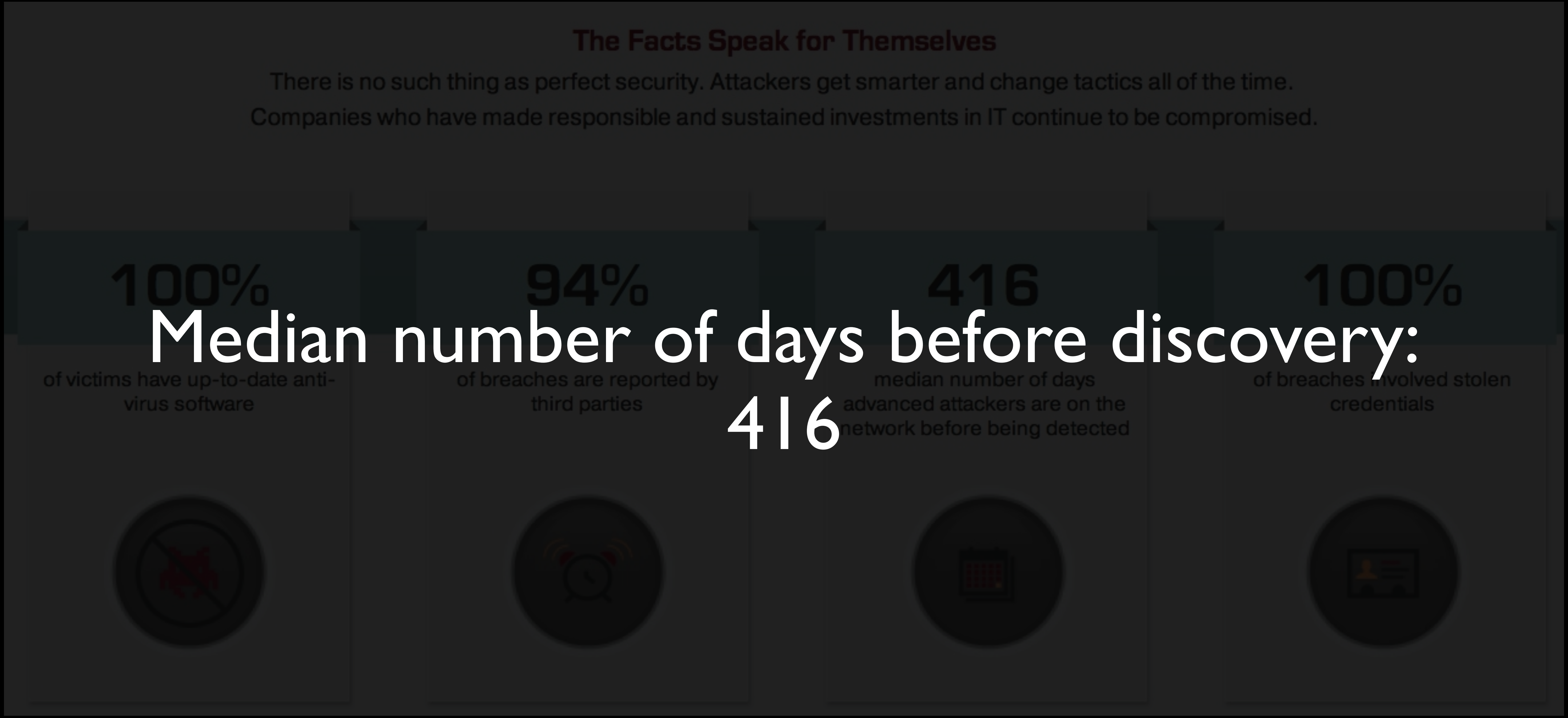
median number of days advanced attackers are on the network before being detected

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/

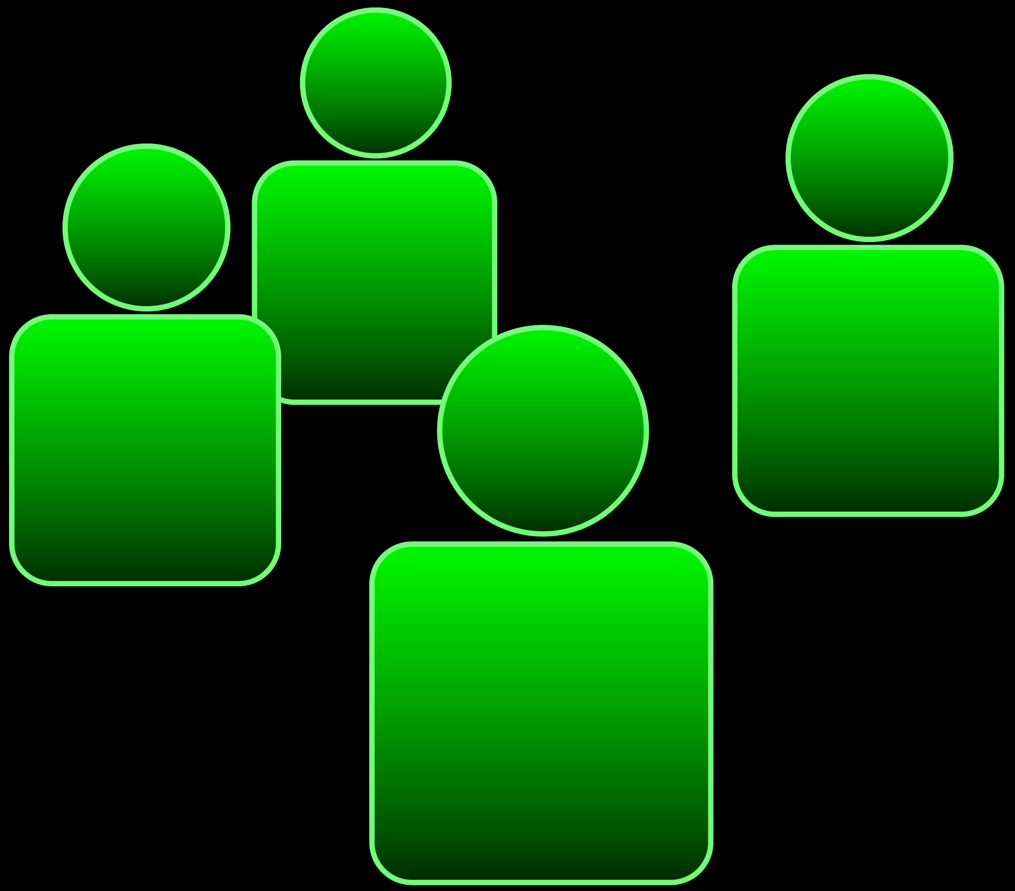
Advanced Persistent Threat

Advanced Persistent Threat

A Threat is like Soylent Green

Advanced Persistent Threat

It’s made of people



Advanced Persistent Threat

SECURELIST

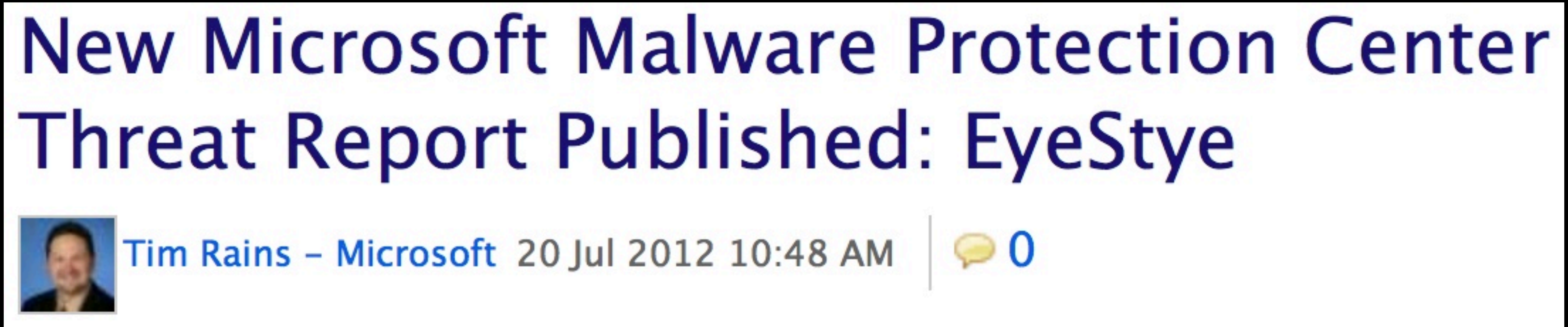
Internet threat level: 1

Home → Analysis → 21 May 2012 → IT Threat Evolution: Q1 2012

"Although patching is effective against this ['fileless' bot] and similar threats, ..."

http://www.securelist.com/en/analysis/204792231/IT_Threat_Evolution_Q1_2012

Advanced Persistent Threat

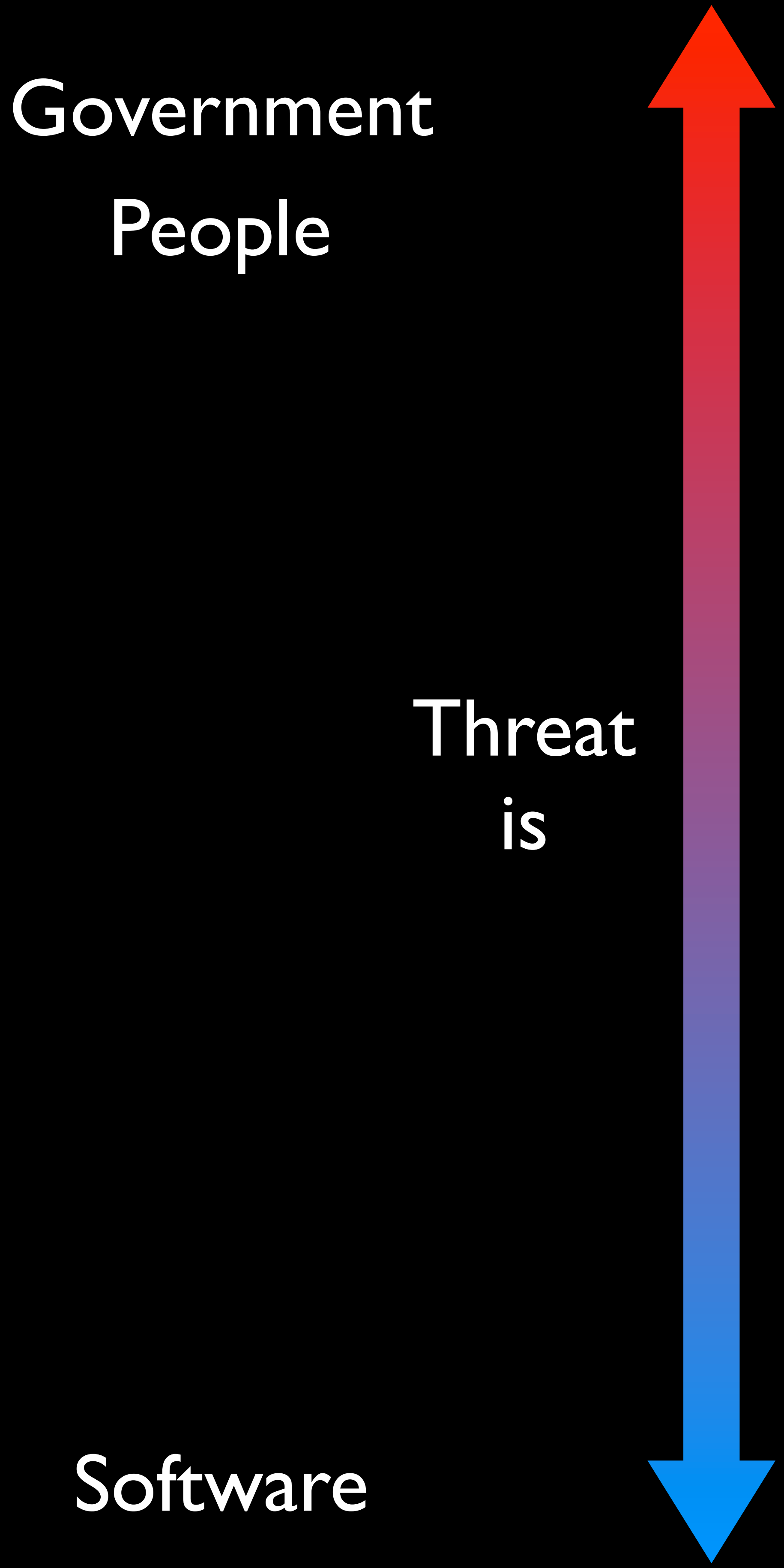


New Microsoft Malware Protection Center Threat Report Published: EyeStye

Tim Rains - Microsoft 20 Jul 2012 10:48 AM | 0

"Four specific families of threats contributed to the steep rise in the malware infection rates ..."

http://blogs.technet.com/b/security/archive/2012/07/20/new-microsoft-malware-protection-center-threat-report-published-eyestye.aspx

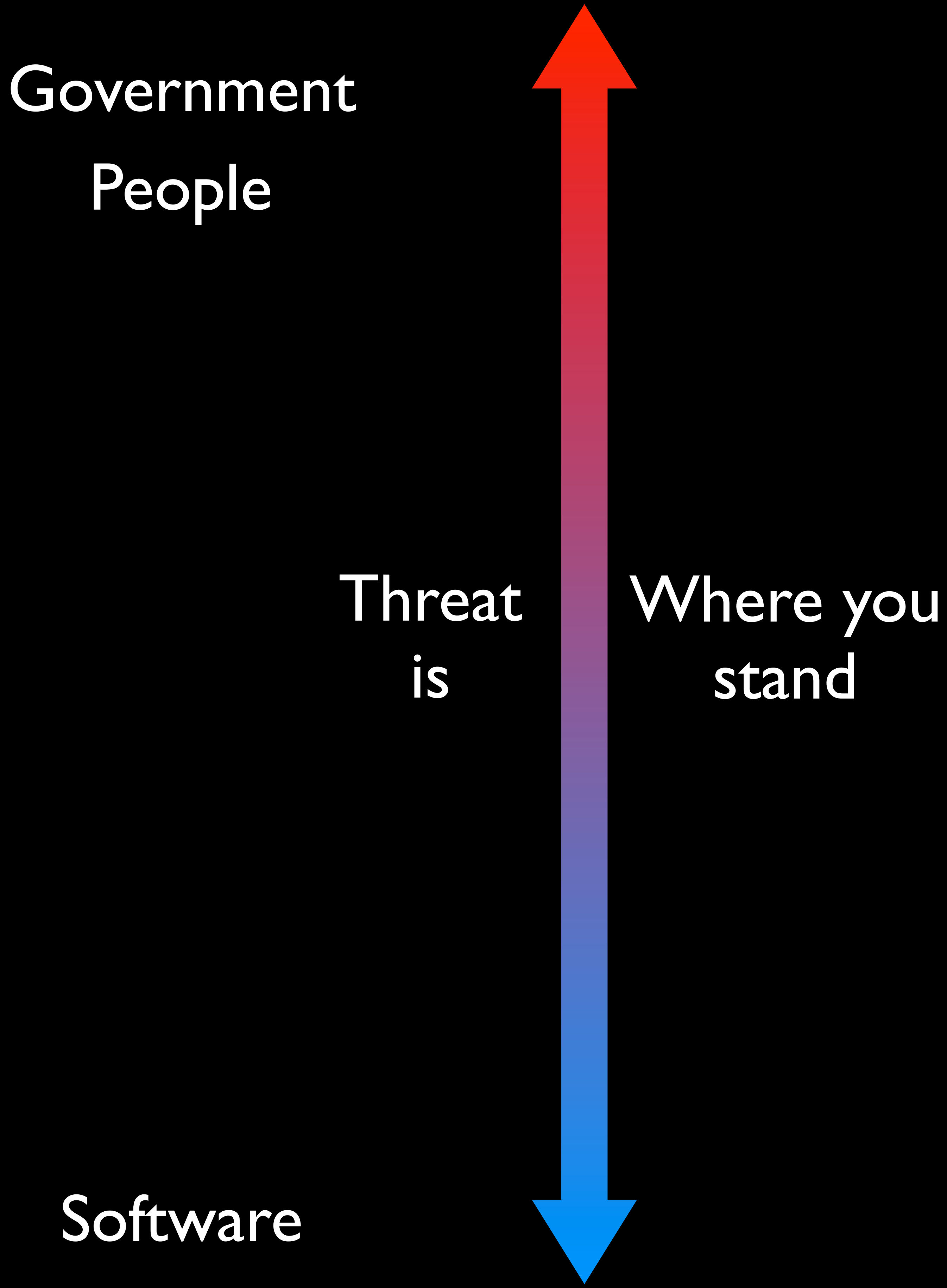


Government

People

Threat
is

Software



Government

People

Threat is

Where you stand

Software

POTUS

Cyber Command

Hunters, large security service

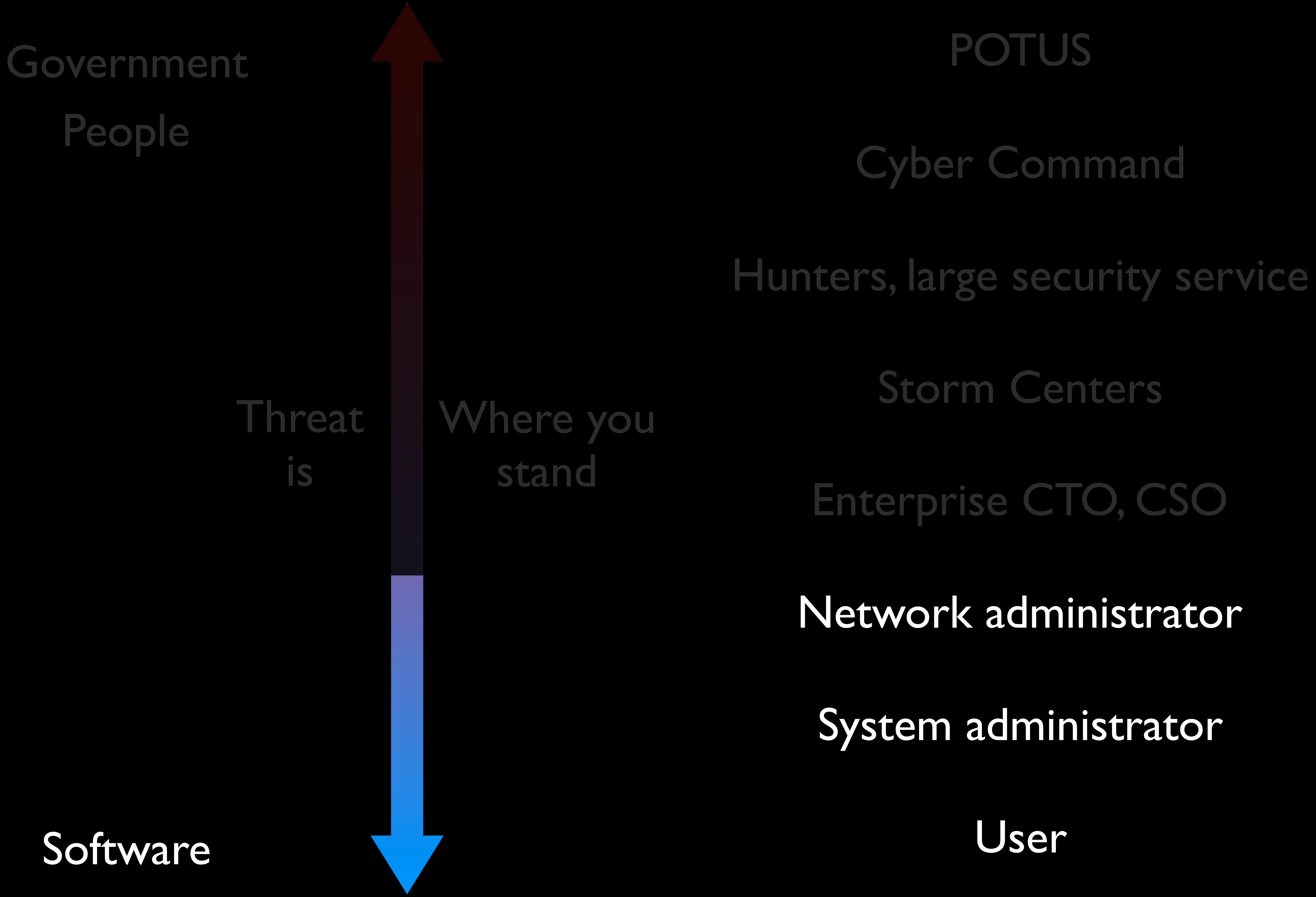
Storm Centers

Enterprise CTO, CSO

Network administrator

System administrator

User



Government

People

Threat is

Software

Where you stand

POTUS

Cyber Command

Hunters, large security service

Storm Centers

Enterprise CTO, CSO

Network administrator

System administrator

User

What’s next after signatures
(back to anomaly detection?)

APTs require a new, “fuzzier” detection strategy

APTs require a new, "fuzzier" detection strategy

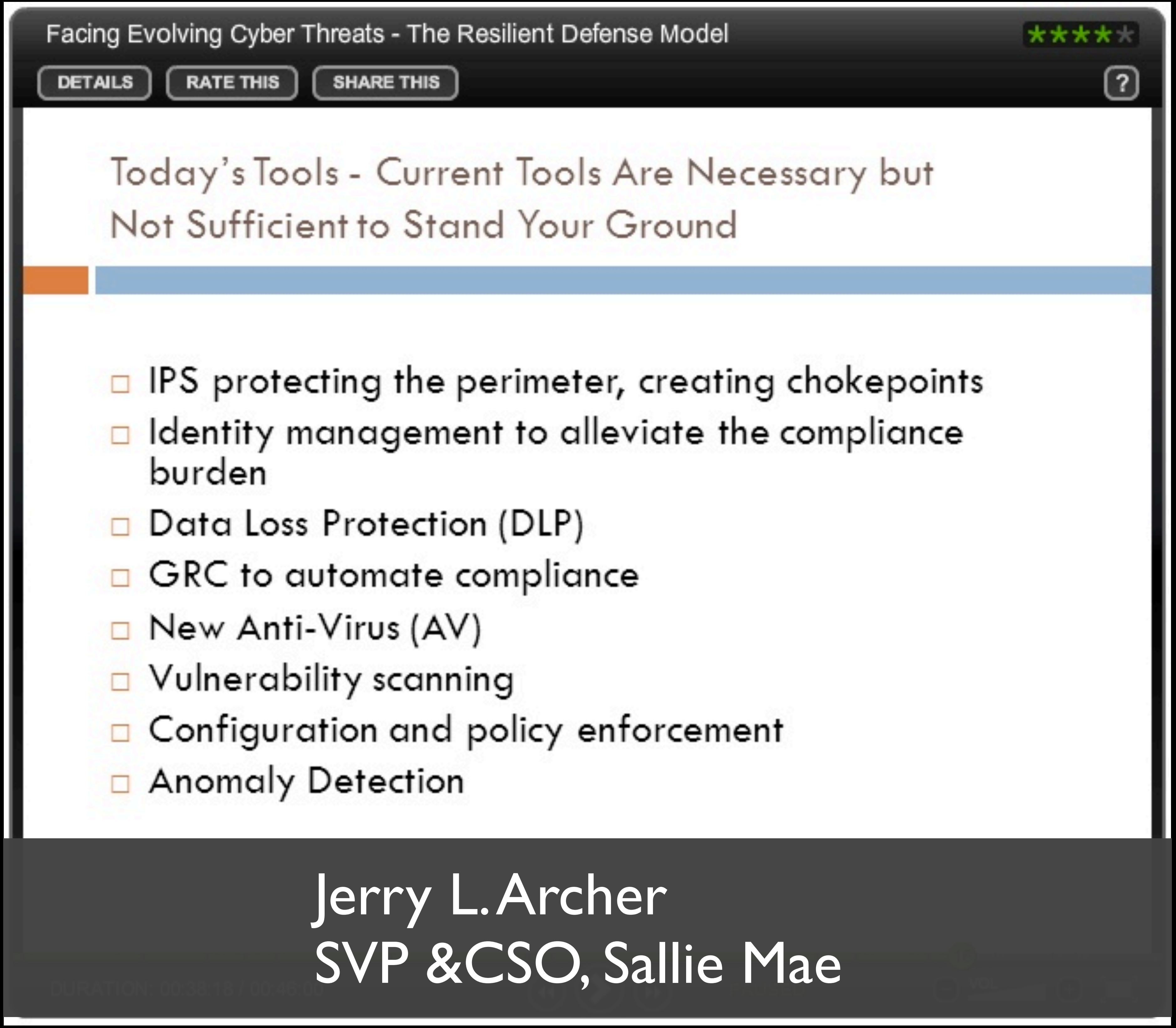
WAS: Yes No

APTs require a new, “fuzzier” detection strategy

WAS:	Yes	No	
NOW:	Yes	No	Maybe

New “fuzzy” detection approaches will make your jobs difficult

BrightTALK™



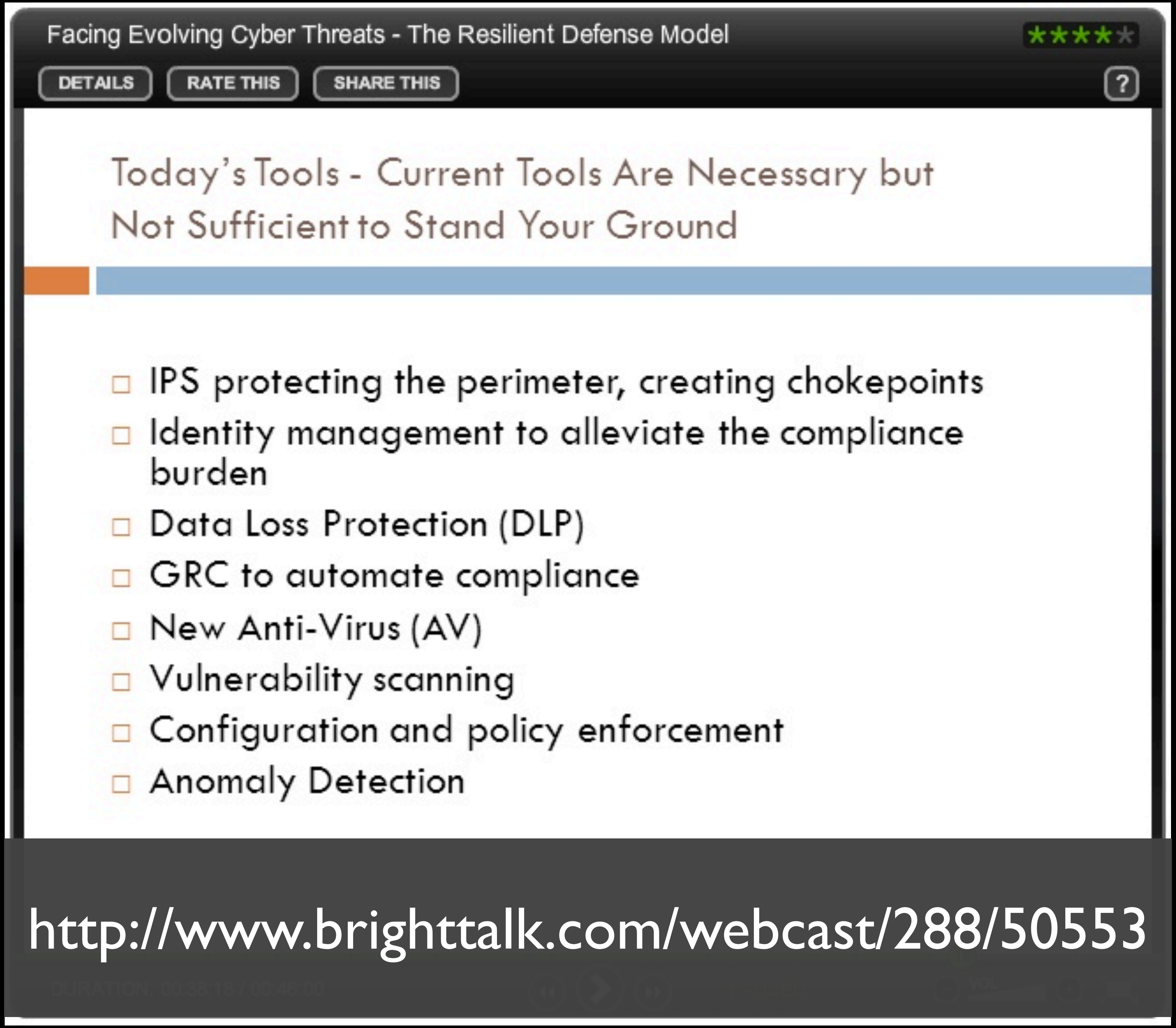
Facing Evolving Cyber Threats - The Resilient Defense Model

Today's Tools - Current Tools Are Necessary but Not Sufficient to Stand Your Ground

- □ IPS protecting the perimeter, creating chokepoints
- □ Identity management to alleviate the compliance burden
- □ Data Loss Protection (DLP)
- □ GRC to automate compliance
- □ New Anti-Virus (AV)
- □ Vulnerability scanning
- □ Configuration and policy enforcement
- □ Anomaly Detection

Jerry L. Archer
SVP &CSO, Sallie Mae

BrightTALK™



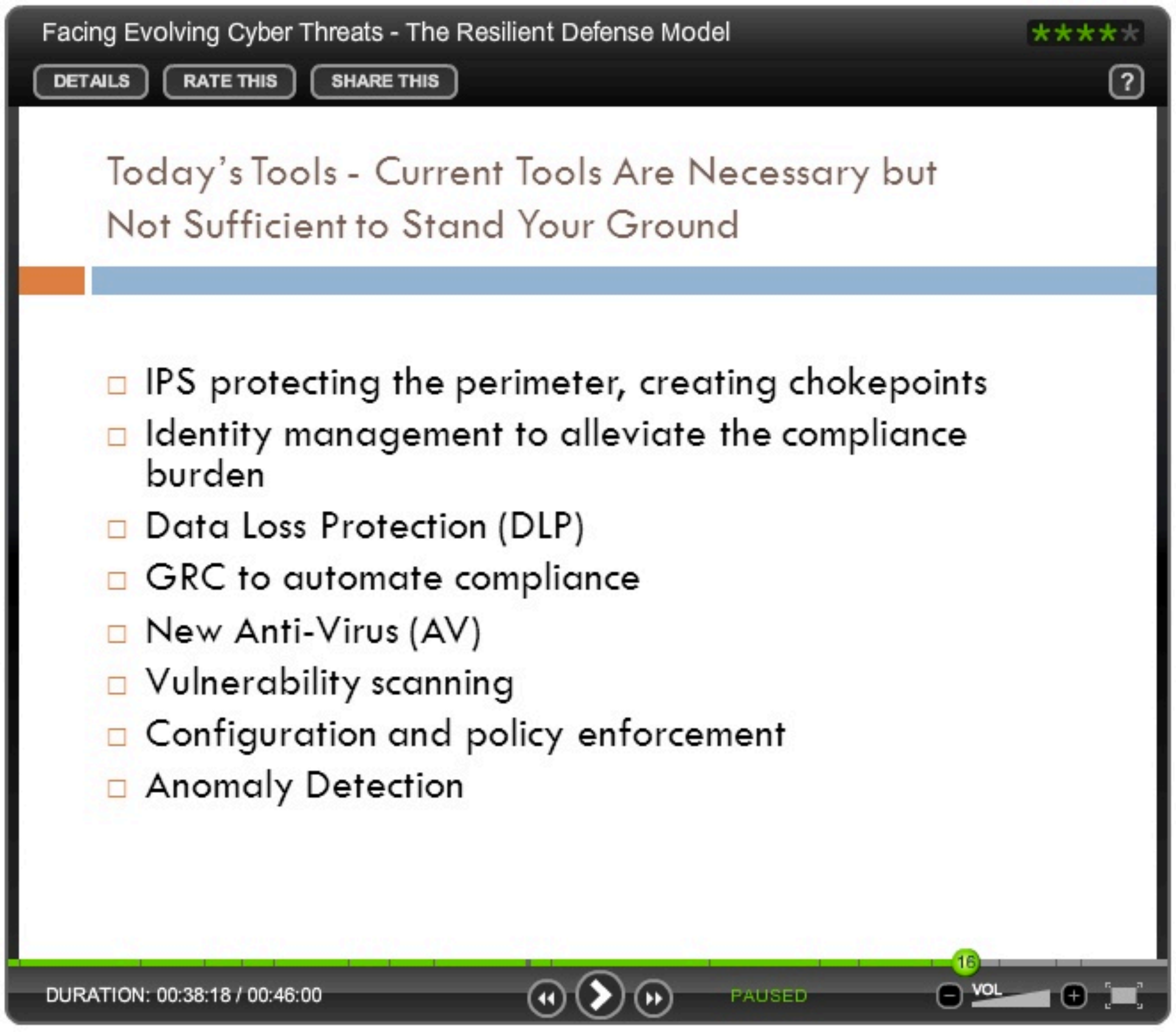
Facing Evolving Cyber Threats - The Resilient Defense Model

Today's Tools - Current Tools Are Necessary but Not Sufficient to Stand Your Ground

- □ IPS protecting the perimeter, creating chokepoints
- □ Identity management to alleviate the compliance burden
- □ Data Loss Protection (DLP)
- □ GRC to automate compliance
- □ New Anti-Virus (AV)
- □ Vulnerability scanning
- □ Configuration and policy enforcement
- □ Anomaly Detection

http://www.brighttalk.com/webcast/288/50553

BrightTALK™



Facing Evolving Cyber Threats - The Resilient Defense Model

Today's Tools - Current Tools Are Necessary but Not Sufficient to Stand Your Ground

- □ IPS protecting the perimeter, creating chokepoints
- □ Identity management to alleviate the compliance burden
- □ Data Loss Protection (DLP)
- □ GRC to automate compliance
- □ New Anti-Virus (AV)
- □ Vulnerability scanning
- □ Configuration and policy enforcement
- □ Anomaly Detection

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

Gartner’s Magic Quadrant for Endpoint Protection Platforms

Dec 11, 2010

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

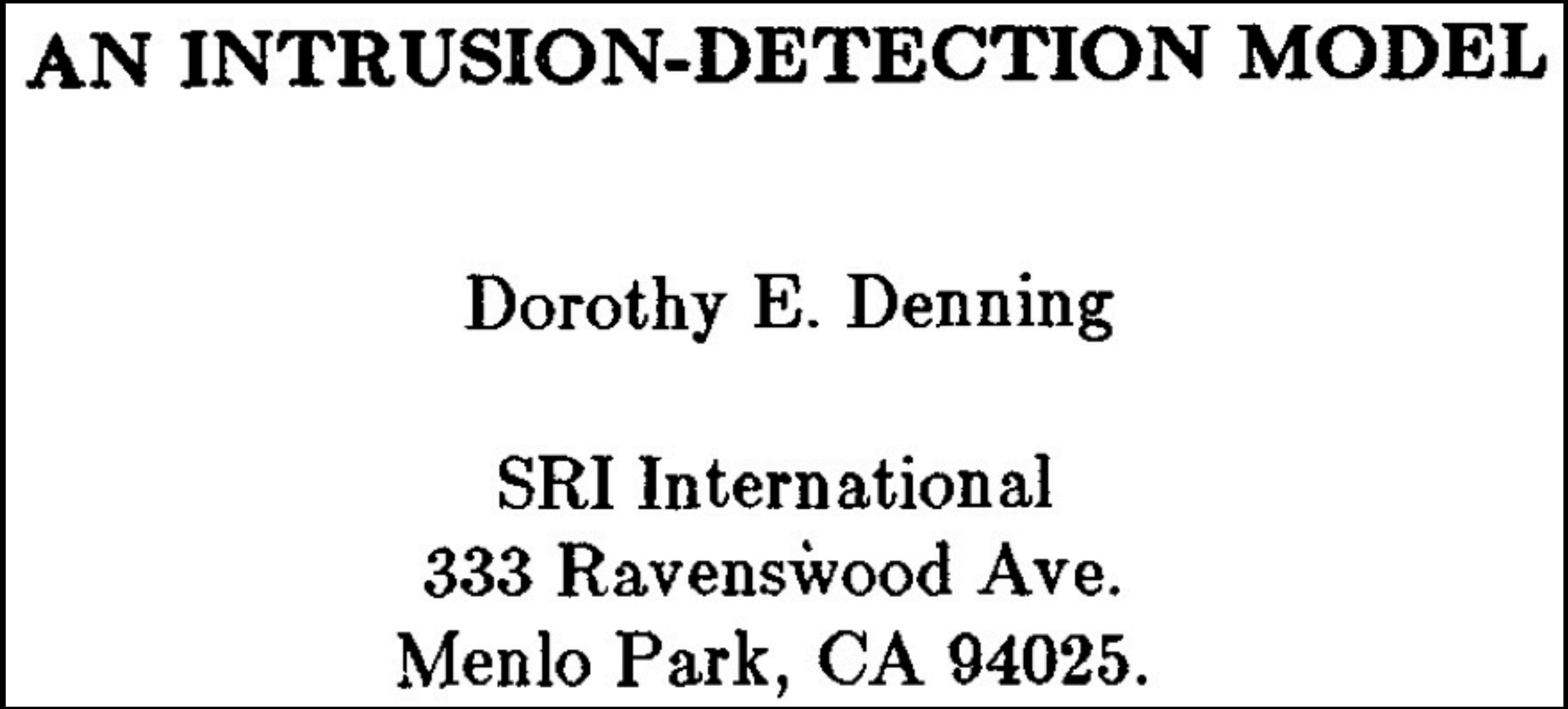
Gartner’s Magic Quadrant for Endpoint Protection Platforms

Dec 11, 2010

“Signature-based defenses don’t work anymore.”

Peter Kuper: VCs renewing their love affair with security companies

May 16, 2012



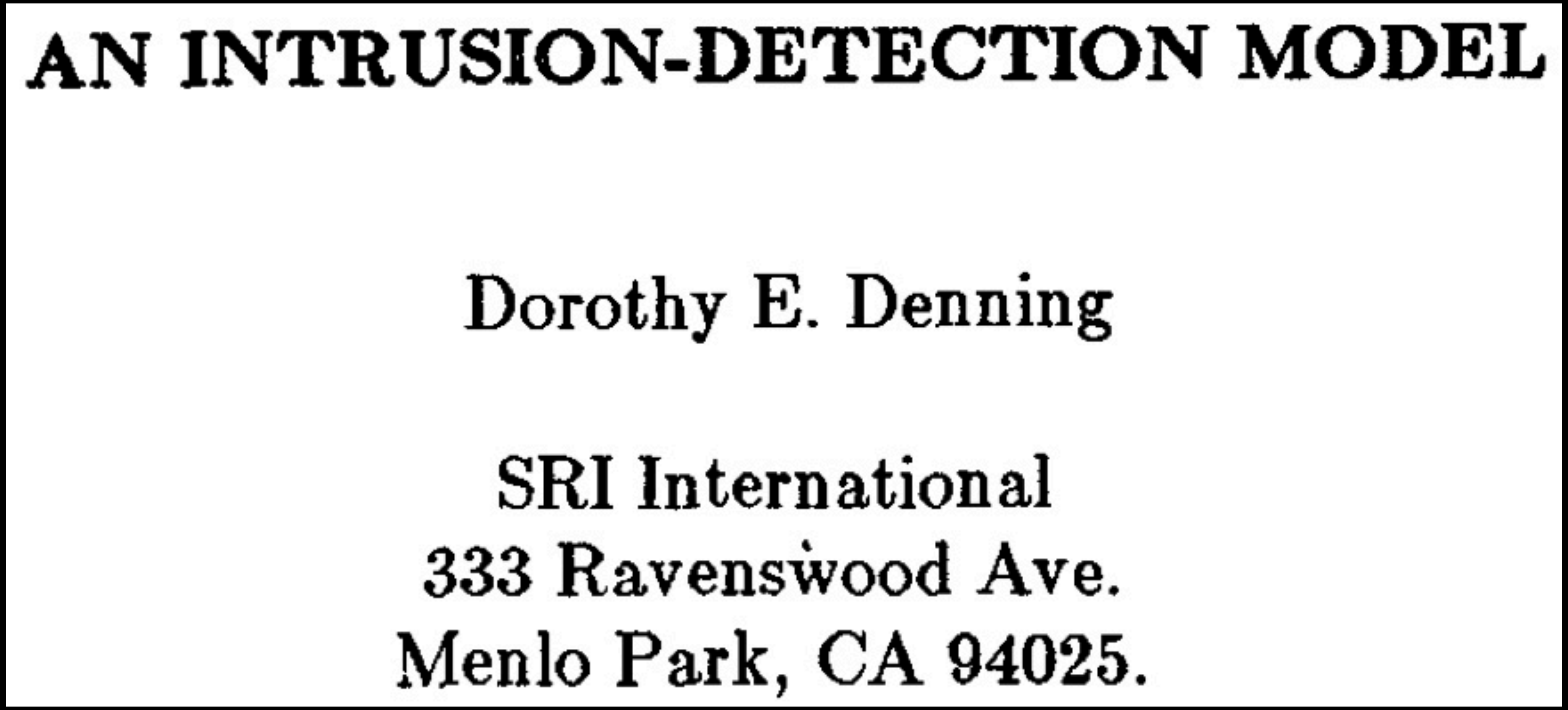
AN INTRUSION-DETECTION MODEL

Dorothy E. Denning

SRI International
333 Ravenswood Ave.
Menlo Park, CA 94025.

"The model is based on the hypothesis that exploitation of a system's vulnerabilities involves abnormal use of the system; therefore, security violations could be detected from abnormal patterns of system usage."

– 1986



AN INTRUSION-DETECTION MODEL

Dorothy E. Denning

SRI International
333 Ravenswood Ave.
Menlo Park, CA 94025.

"The model is based on the hypothesis that exploitation of a system's vulnerabilities involves abnormal use of the system; therefore, security violations could be detected from abnormal patterns of system usage."

– 1986

The SRI IDES Statistical Anomaly Detector

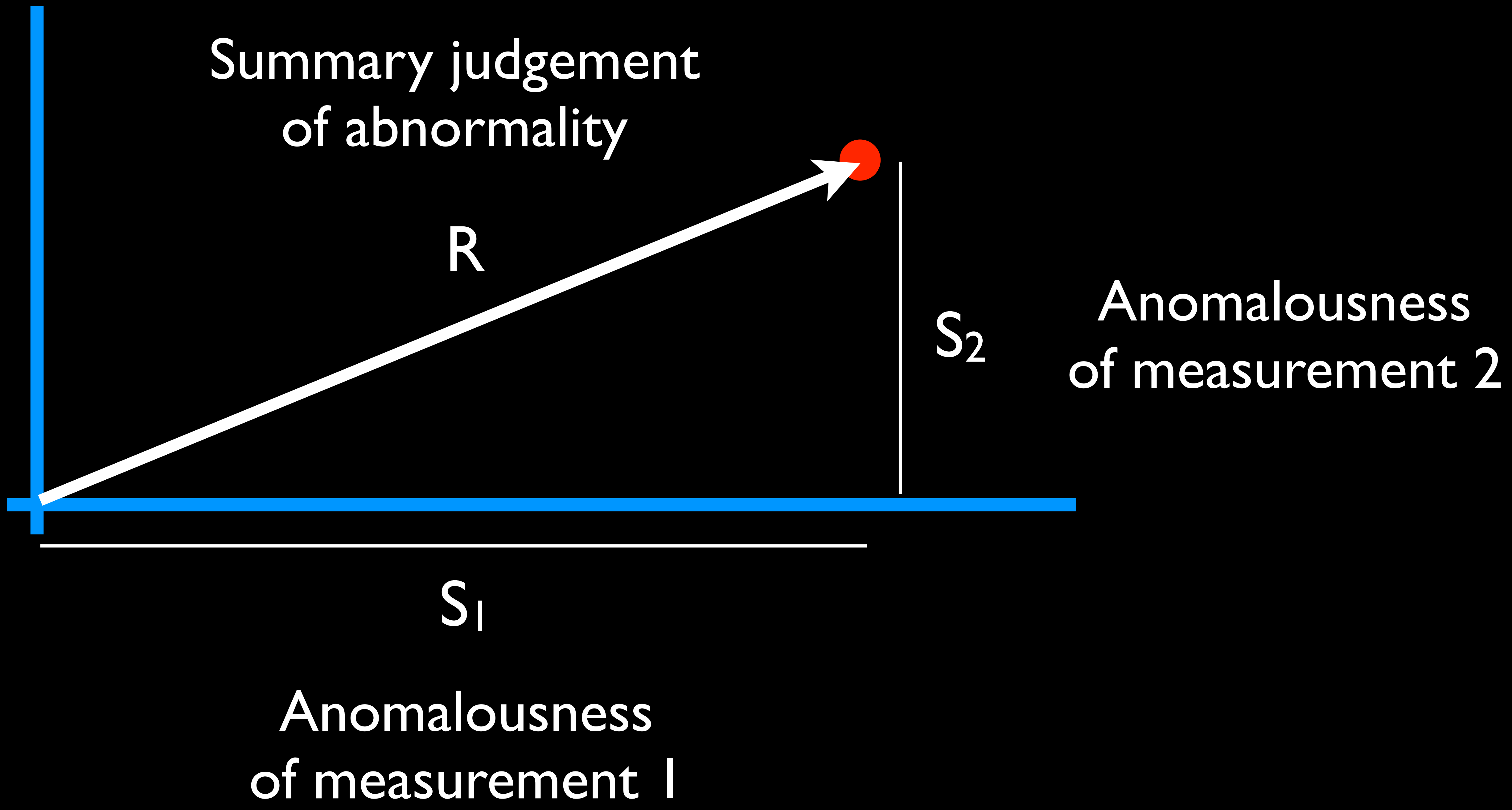
“The IS statistic is itself a summary judgement of many measures.”

$$IS = (\underset{\substack{\uparrow \\ \text{Anomalousness} \\ \text{of measurement 1}}}{S_1},\underset{\substack{\uparrow \\ \text{Anomalousness} \\ \text{of measurement 2}}}{S_2},\ldots,S_n)\ \underset{\substack{\uparrow \\ \text{Inverse of} \\ \text{correlation matrix}}}{C^{-1}}\ (S_1,S_2,\ldots,S_n)^t$$

– 1991

$$R^2 = S_1^2 + S_2^2$$

$$IS = R^2$$


Summary judgement of abnormality
R
S_2
Anomalousness of measurement 2
S_1
Anomalousness of measurement 1

Simple Pythagorean equation only makes sense if all measurements are independent

In reality, “independence” is almost never the case

Inverse correlation matrix used to address this issue

Simple Pythagorean equation only makes sense if all measurements are independent

In reality, “independence” is almost never the case

Inverse correlation matrix used to address this issue

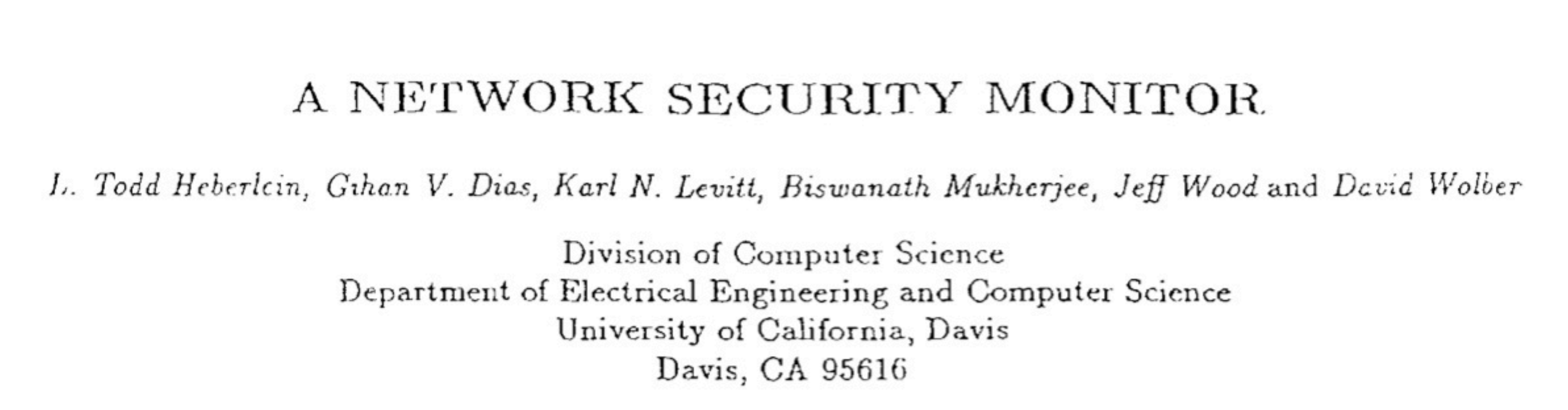
I was told the inverse correlation matrix was removed because it made it too difficult for operators to understand the results

Simple Pythagorean equation only makes sense if all measurements are independent

In reality, “independence” is almost never the case

Inverse correlation matrix used to address this issue

I was told the inverse correlation matrix was removed because it made it too difficult for operators to understand the results



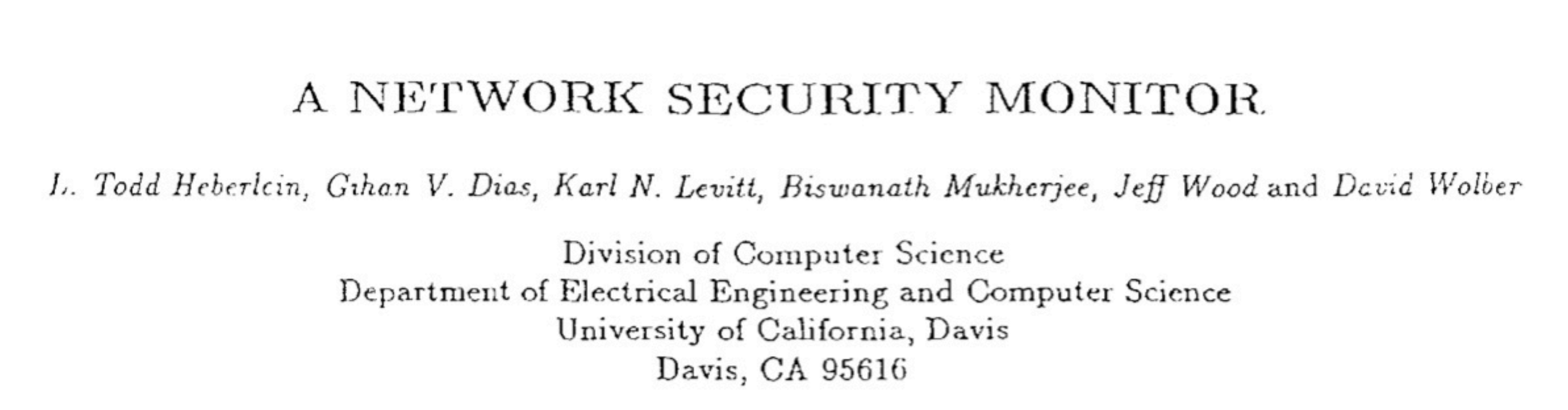
A NETWORK SECURITY MONITOR

L. Todd Heberlein, Gihan V. Dias, Karl N. Levitt, Biswanath Mukherjee, Jeff Wood and *David Wolber*

Division of Computer Science
Department of Electrical Engineering and Computer Science
University of California, Davis
Davis, CA 95616

Published: May 1990

Our basic strategy is to develop profiles of usage of network resources and then compare current usage patterns with the historical profile to determine possible security violations.



A NETWORK SECURITY MONITOR

L. Todd Heberlein, Gihan V. Dias, Karl N. Levitt, Biswanath Mukherjee, Jeff Wood and *David Wolber*

Division of Computer Science
Department of Electrical Engineering and Computer Science
University of California, Davis
Davis, CA 95616

Published: May 1990

Our basic strategy is to develop profiles of usage of network resources and then compare current usage patterns with the historical profile to determine possible security violations.

6 PERFORMANCE OF THE N.S.M.

We had several goals to accomplish with the early prototype of the NSM. Among these were ... a determination of the types and number of problems reported.

6 PERFORMANCE OF THE N.S.M.

We had several goals to accomplish with the early prototype of the NSM. Among these were ... a determination of the types and number of problems reported.

The biggest concern was the detection of unusual activity which was not obviously an attack.

The biggest concern was the detection of unusual activity which was not obviously an attack.

The biggest concern was the detection of unusual activity which was not obviously an attack.

we often did not have any supporting evidence to prove or disprove that an attack had occurred

The biggest concern was the detection of unusual activity which was not obviously an attack.

we often did not have any supporting evidence to prove or disprove that an attack had occurred

False Positive Paradox

False Positive Paradox

A system with 99.9% accuracy

False Positive Paradox

A system with 99.9% accuracy

can be wrong 90% of the time

Depends on the underlying distribution of the data, and that can be different from location to location and at one location across time

Labeled Data Paradox

Labeled Data Paradox

A system that performs extremely well with labeled data

Labeled Data Paradox

A system that performs extremely well with labeled data

can suck in real life

In the end, we need to move from a positive test to a diagnoses, and complex statistical analyses can be difficult to understand

Labeled Data Paradox

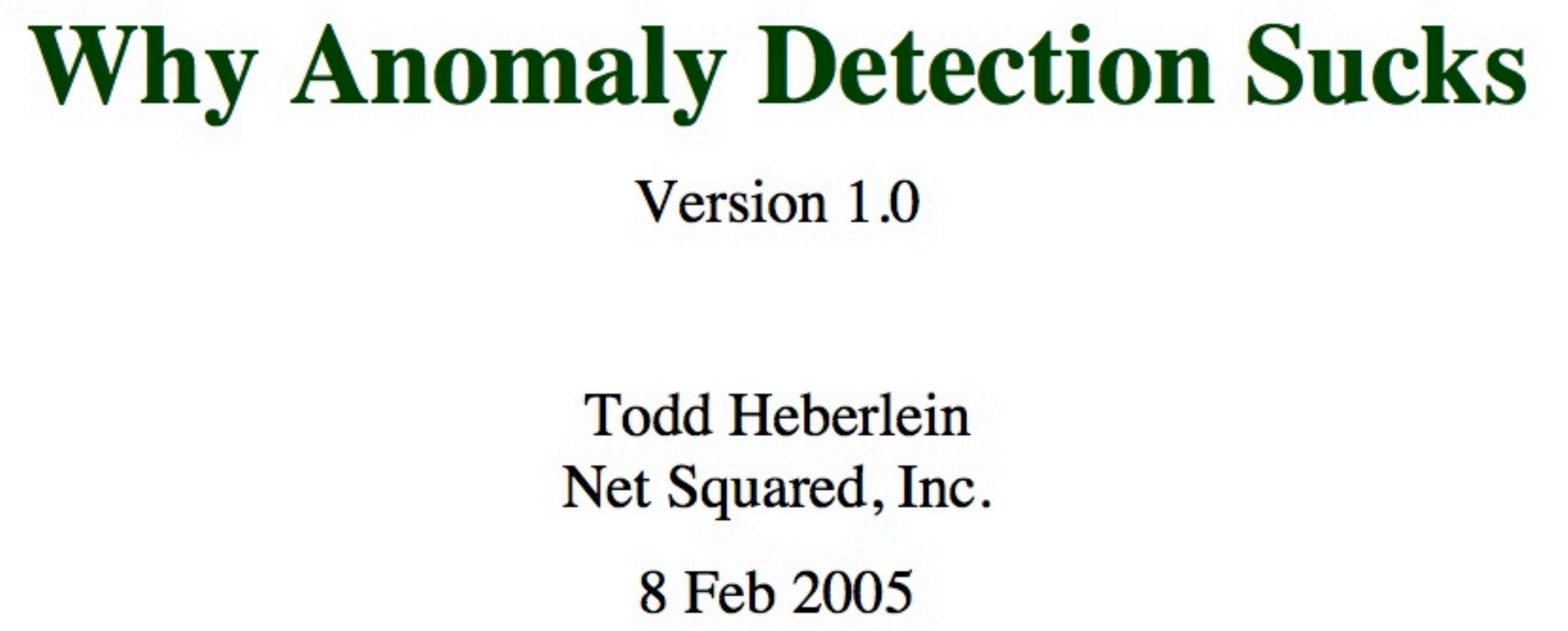
A system that performs extremely well with labeled data

can suck in real life

In the end, we need to move from a positive test to a diagnoses, and complex statistical analyses can be difficult to understand

The problem with uncertainty

Uncertainty causes anxiety



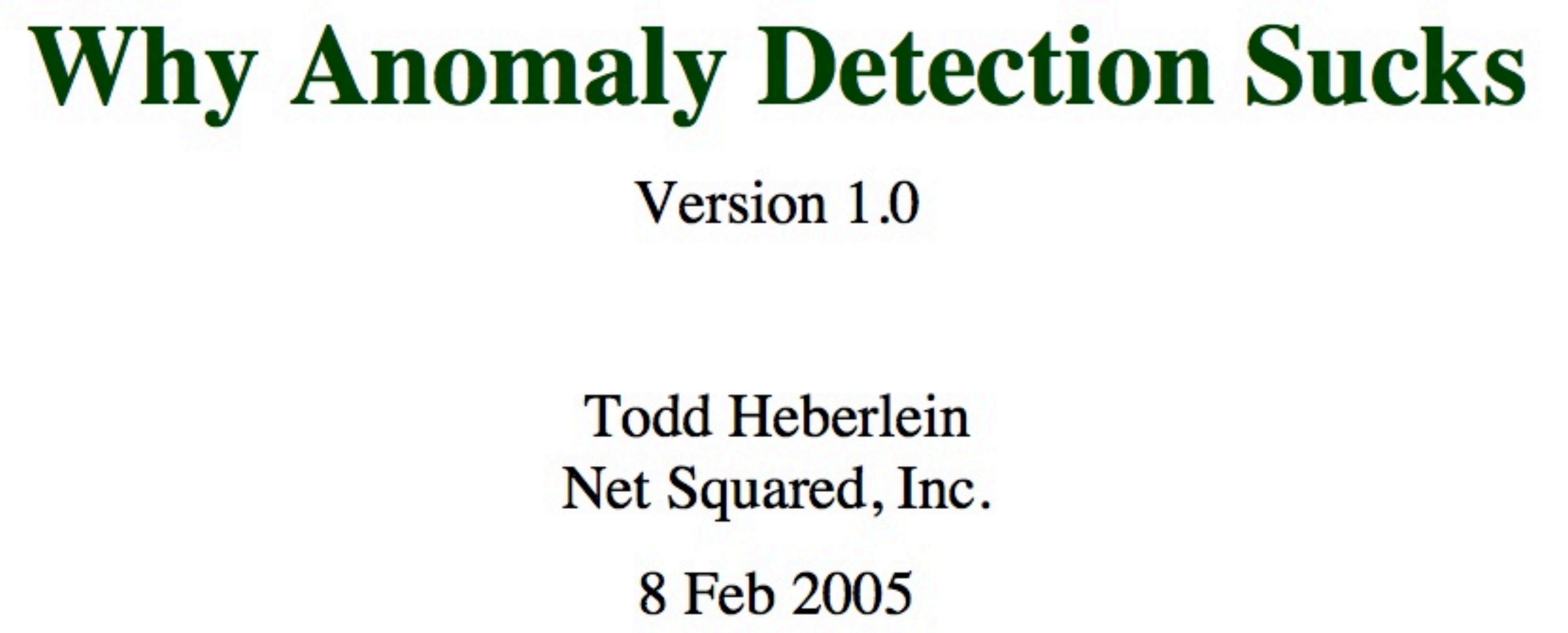
Why Anomaly Detection Sucks

Version 1.0

Todd Heberlein
Net Squared, Inc.

8 Feb 2005

"However, despite these apparent advantages that anomaly-based techniques have over signature-based techniques, signature-based techniques have enjoyed considerably more operational success than anomaly techniques."



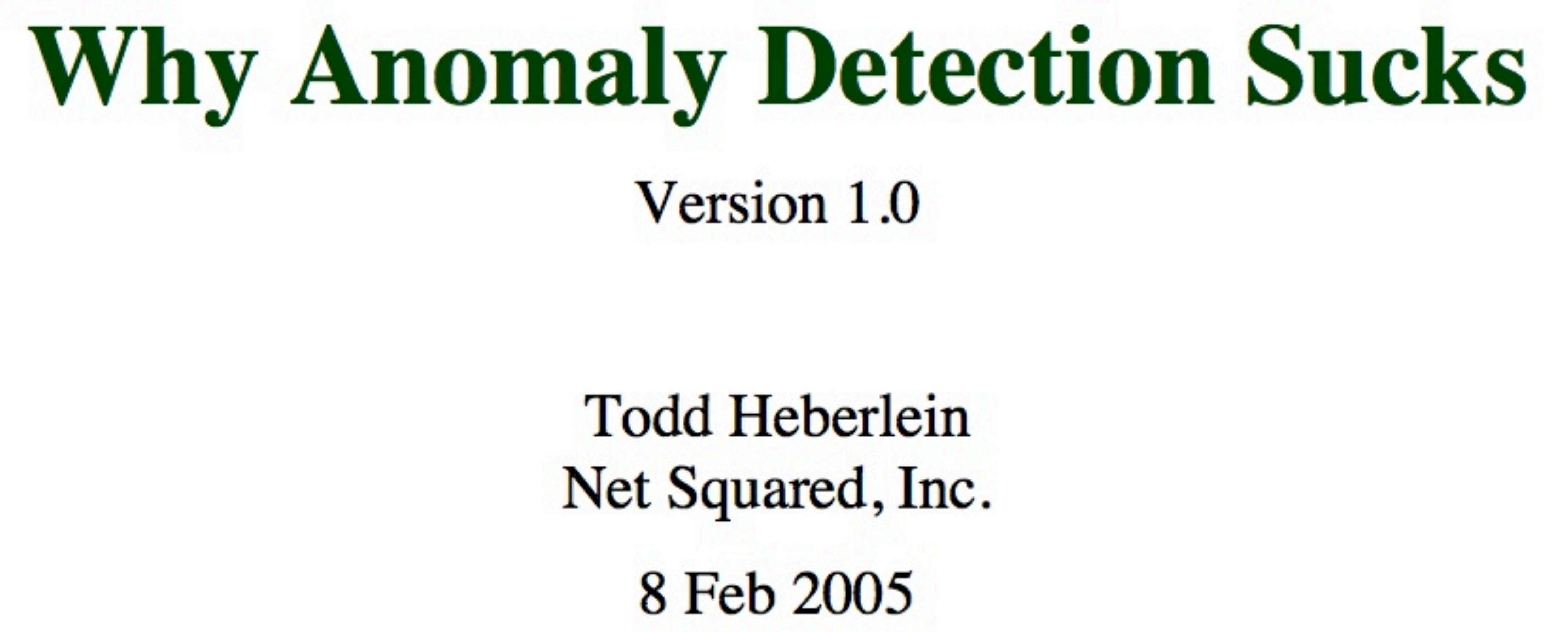
Why Anomaly Detection Sucks

Version 1.0

Todd Heberlein
Net Squared, Inc.

8 Feb 2005

"However, despite these apparent advantages that anomaly-based techniques have over signature-based techniques, signature-based techniques have enjoyed considerably more operational success than anomaly techniques."



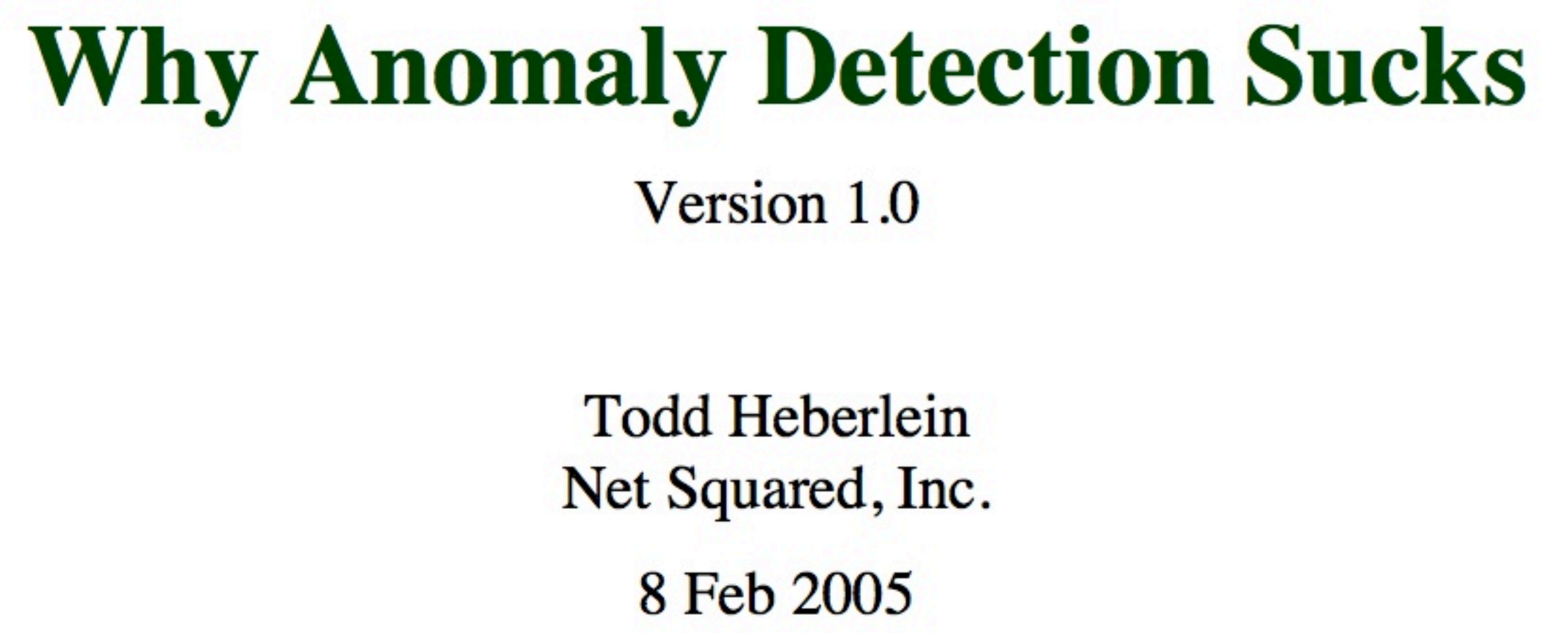
Why Anomaly Detection Sucks

Version 1.0

Todd Heberlein
Net Squared, Inc.

8 Feb 2005

"Why haven't we seen more success in anomaly-based techniques? Because anomaly detection sucks for users. Anomaly detection tends to produce non-actionable reports, requires the user to devote hours to understand the underlying cause of the report, and ultimately may leave the user with no resolution but plenty of angst."



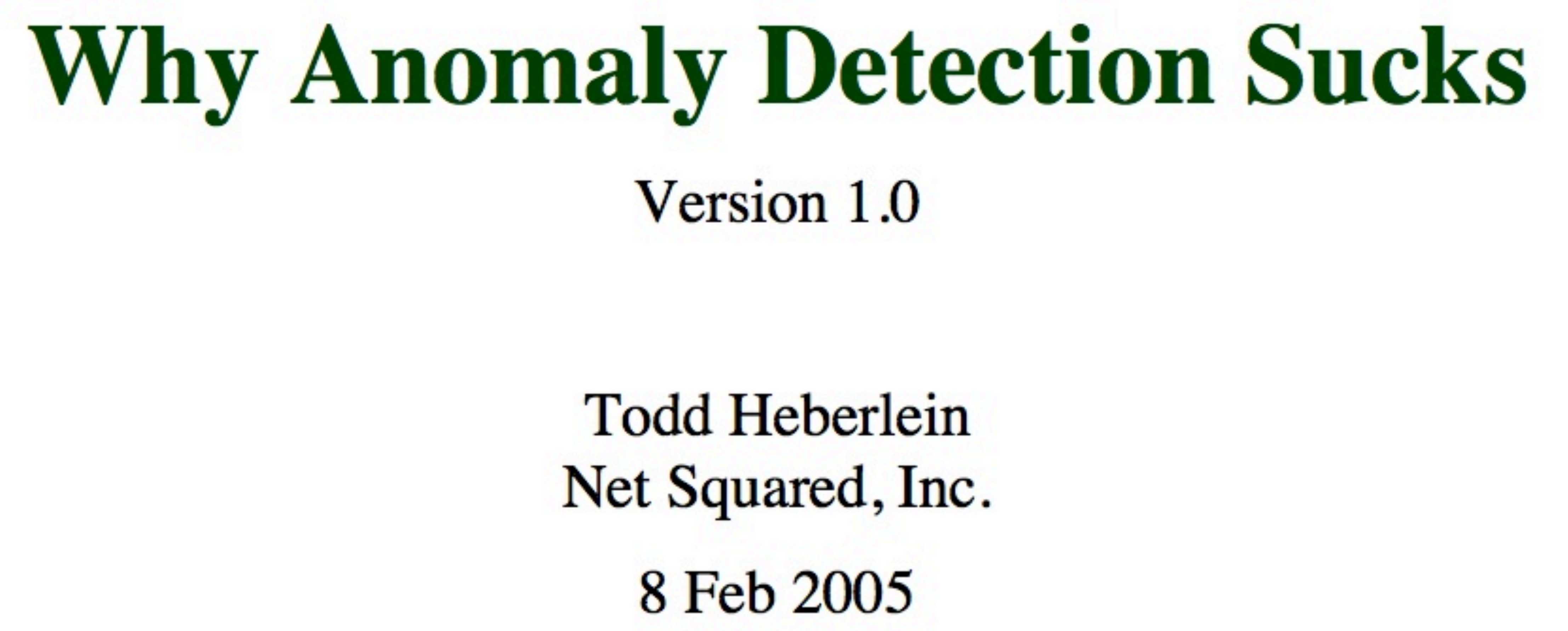
Why Anomaly Detection Sucks

Version 1.0

Todd Heberlein
Net Squared, Inc.

8 Feb 2005

"Why haven't we seen more success in anomaly-based techniques? Because anomaly detection sucks for users. Anomaly detection tends to produce non-actionable reports, requires the user to devote hours to understand the underlying cause of the report, and ultimately may leave the user with no resolution but plenty of angst."



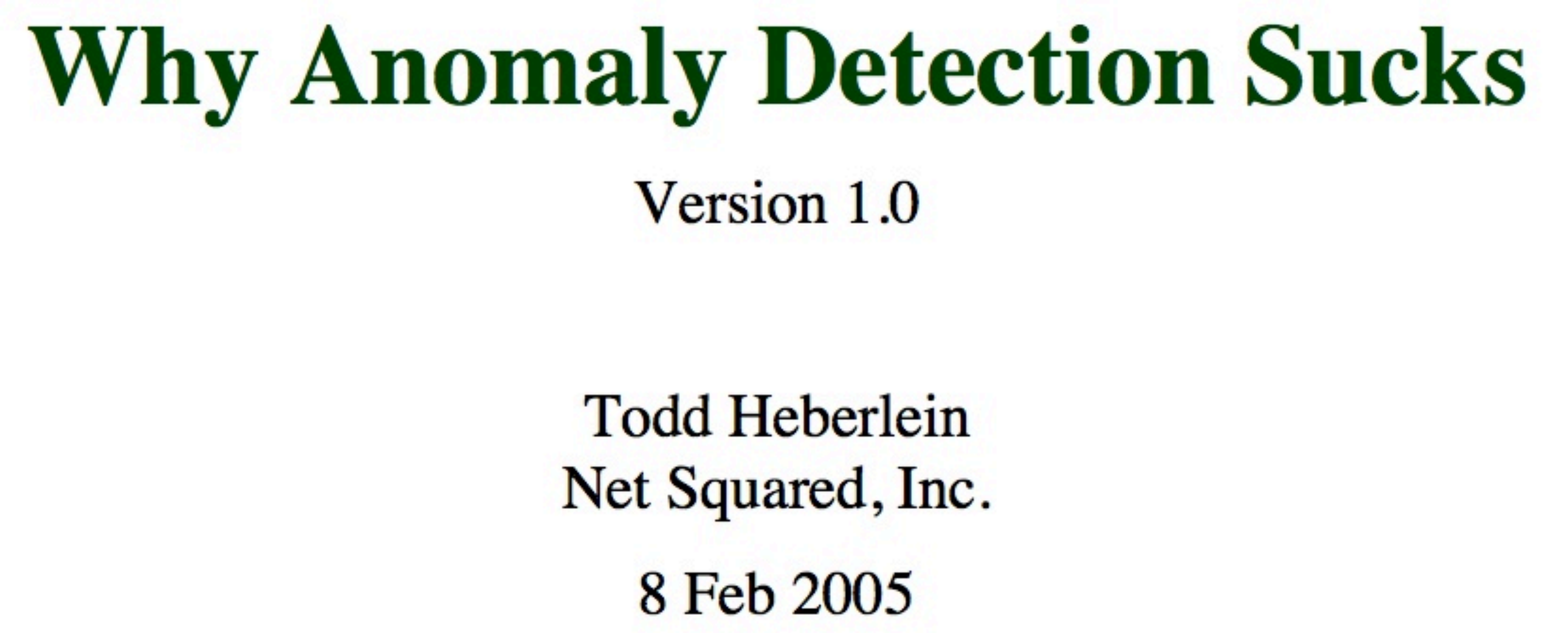
Why Anomaly Detection Sucks

Version 1.0

Todd Heberlein
Net Squared, Inc.

8 Feb 2005

“Why haven’t we seen more success in anomaly-based techniques? Because anomaly detection sucks for users. Anomaly detection tends to produce non-actionable reports, requires the user to devote hours to understand the underlying cause of the report, and ultimately may leave the user with no resolution but plenty of angst.”



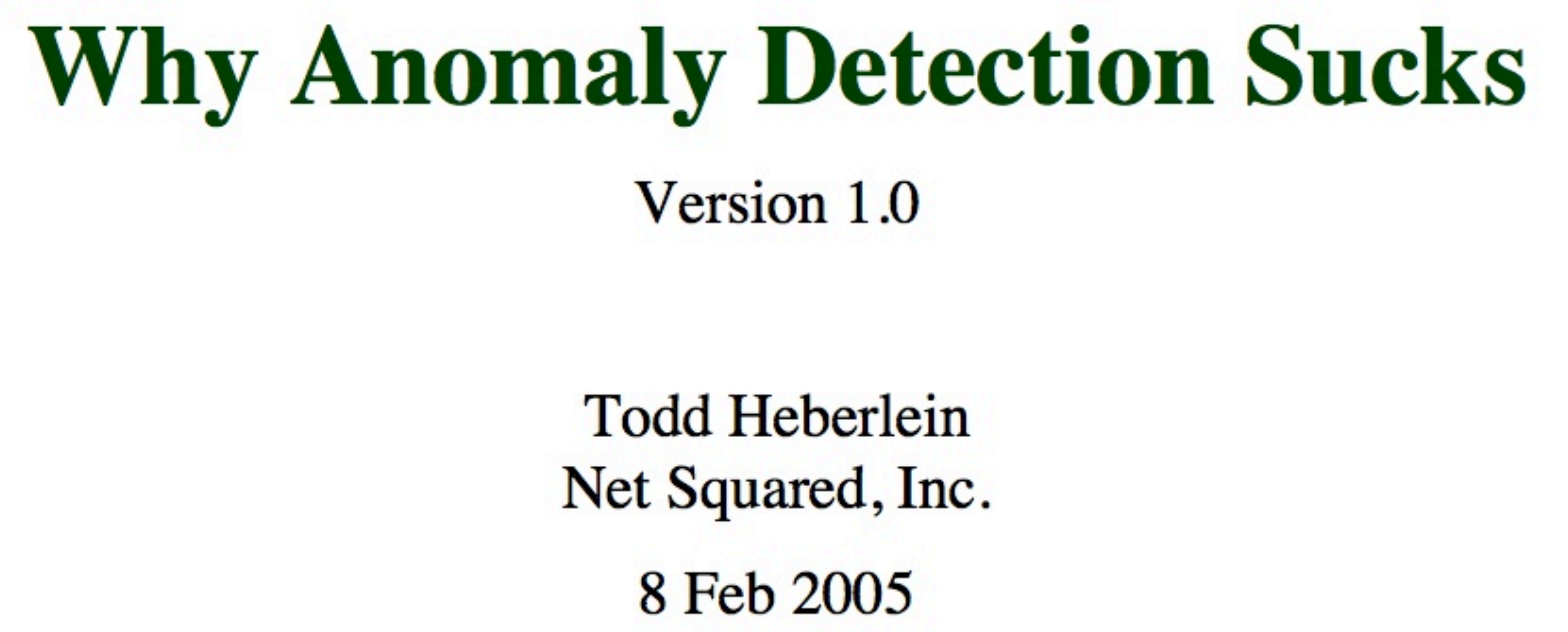
Why Anomaly Detection Sucks

Version 1.0

Todd Heberlein
Net Squared, Inc.

8 Feb 2005

"Why haven't we seen more success in anomaly-based techniques? Because anomaly detection sucks for users. Anomaly detection tends to produce non-actionable reports, requires the user to devote hours to understand the underlying cause of the report, and ultimately may leave the user with no resolution but plenty of angst."



Why Anomaly Detection Sucks

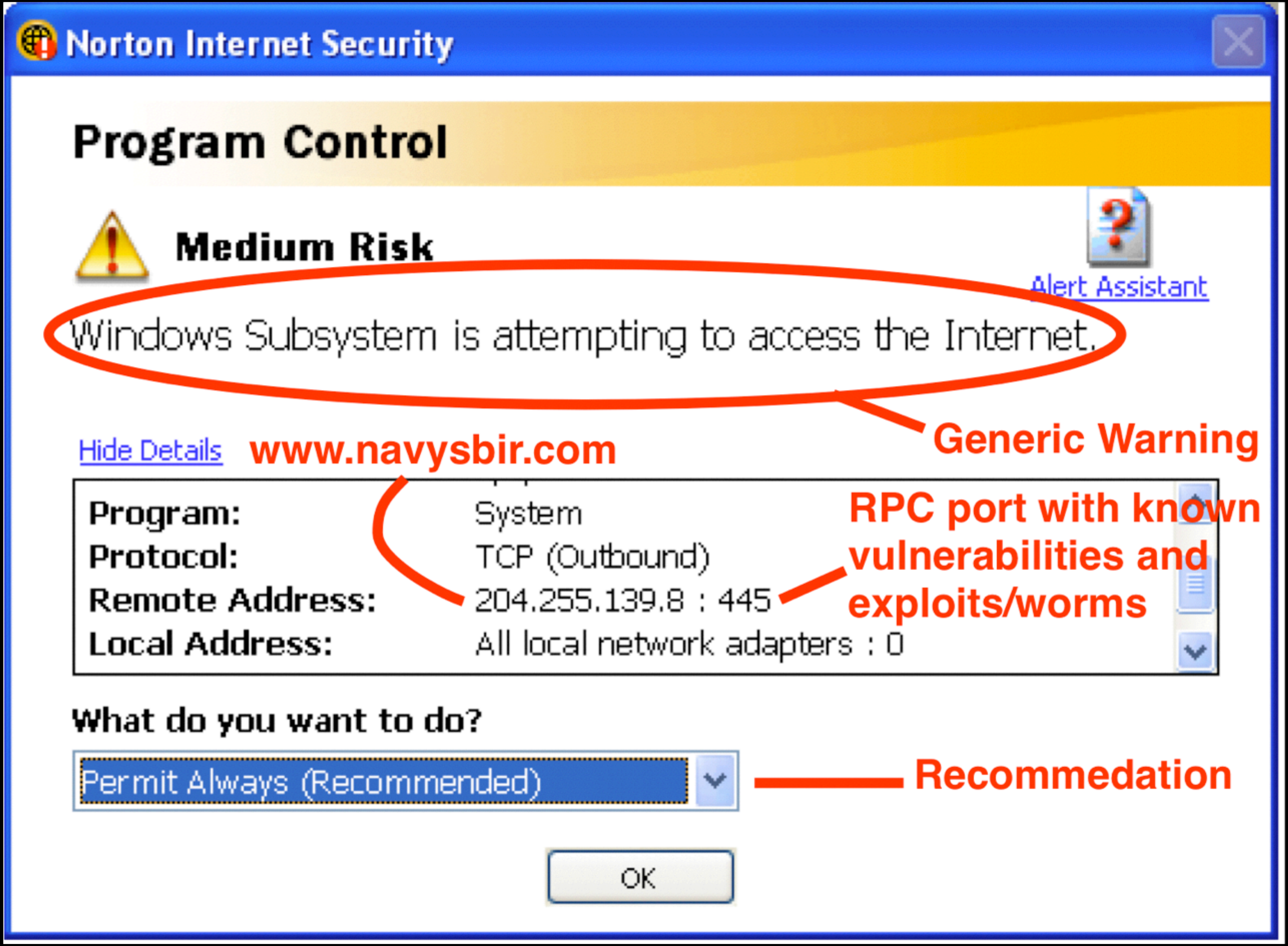
Version 1.0

Todd Heberlein
Net Squared, Inc.

8 Feb 2005

"Why haven't we seen more success in anomaly-based techniques? Because anomaly detection sucks for users. Anomaly detection tends to produce non-actionable reports, requires the user to devote hours to understand the underlying cause of the report, and ultimately may leave the user with no resolution but plenty of angst."

Information	Signature	Anomaly
Target:	128.131.7.2 : 161	128.131.7.2 : 161
Attacker:	128.120.56.31 : 5611	128.120.56.31 : 5611
Attack Name:	xdr_router_crash	unknown
Vulnerability ID:	CVE-2002-0391	unknown
Vulnerable:	Yes	unknown
Damage:	Crashes Cisco routers	unknown
Link to Patch:	Cisco_patch	none
Details:	Security Focus	none



Program Control

Medium Risk

Windows Subsystem is attempting to access the Internet.

Program:	System
Protocol:	TCP (Outbound)
Remote Address:	204.255.139.8 : 445
Local Address:	All local network adapters : 0

What do you want to do?

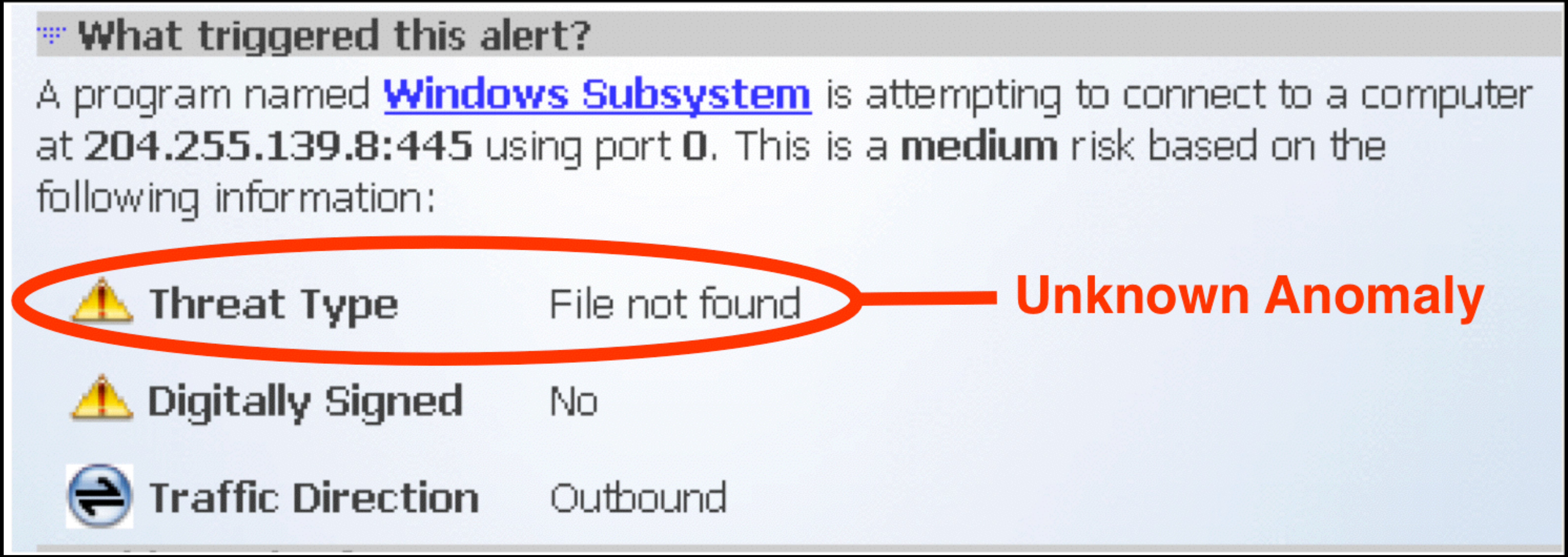
Permit Always (Recommended)

Generic Warning

www.navysbir.com

RPC port with known vulnerabilities and exploits/worms

Recommendation



What triggered this alert?

A program named Windows Subsystem is attempting to connect to a computer at **204.255.139.8:445** using port **0**. This is a **medium** risk based on the following information:

⚠	**Threat Type**	File not found
⚠	**Digitally Signed**	No
⇄	**Traffic Direction**	Outbound

Unknown Anomaly

The rest of the story...

The rest of the story...

“You can never step into the same river twice”

– Heraclitus of Ephesus (535 - 475 BC)

The rest of the story...

“You can never step into the same river twice”

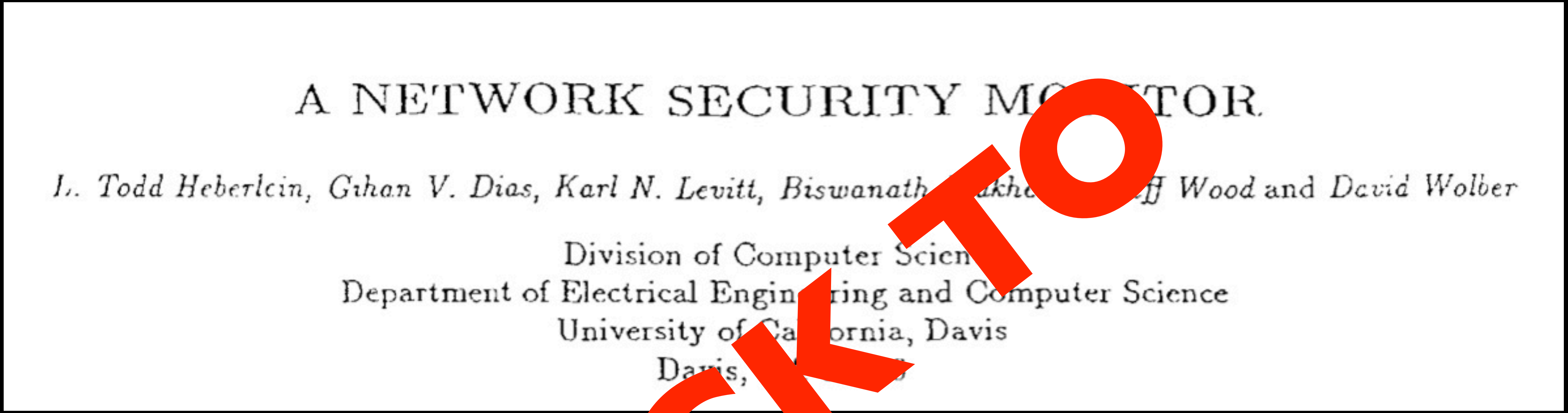
– Heracklitus of Ephesus (535 - 475 BC)

“You can never boot the same system twice”

– Todd

From test to diagnosis

BACK TO



A NETWORK SECURITY MONITOR

L. Todd Heberlein, Gihan V. Dias, Karl N. Levitt, Biswanath Mukherjee, Jeff Wood and *David Wolber*

Division of Computer Science
Department of Electrical Engineering and Computer Science
University of California, Davis
Davis,

Published: May 1990

One possible solution would be to save the actual data crossing the connection, so that an exact recording of what had happen would exist.

One possible solution would be to save the actual data crossing the connection, so that an exact recording of what had happen would exist.

One possible solution would be to save the actual data crossing the connection, so that an exact recording of what had happen would exist.

A second solution would be to examine audit trails generated by one of the hosts concerned

One possible solution would be to save the actual data crossing the connection, so that an exact recording of what had happen would exist.

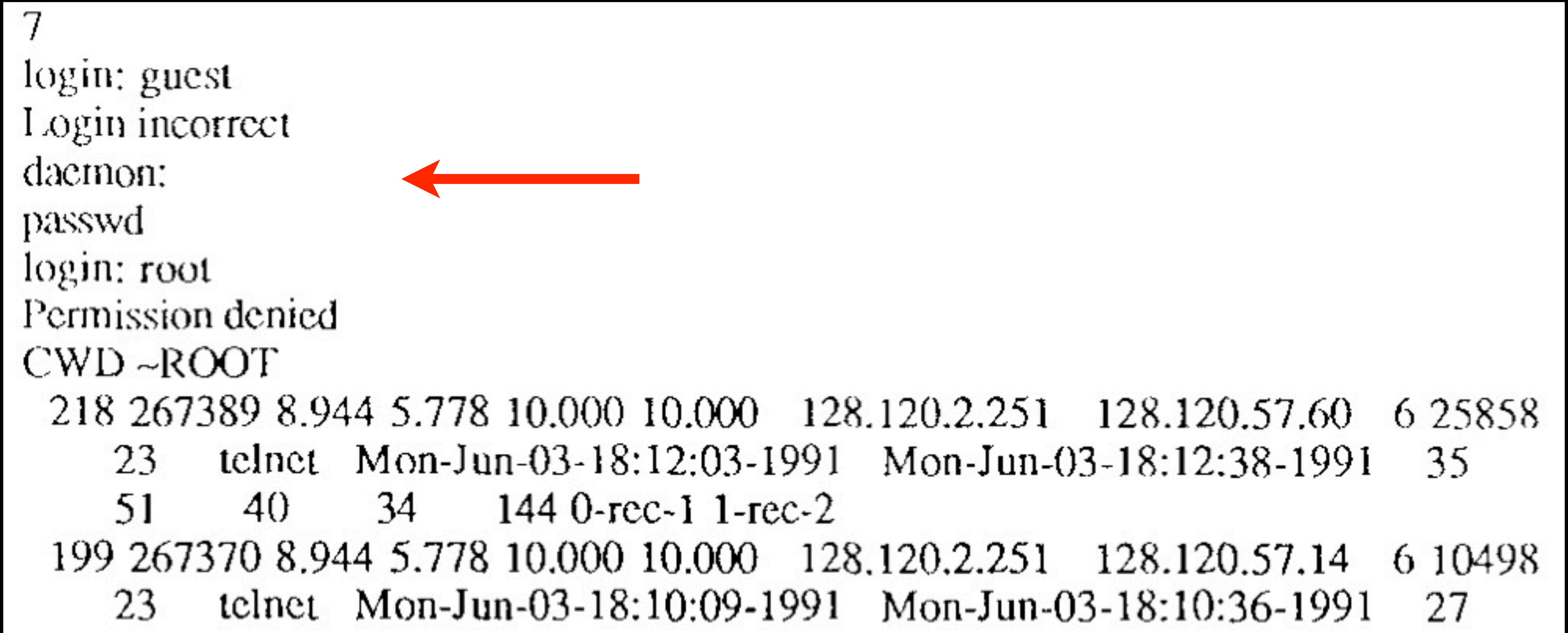
A second solution would be to examine audit trails generated by one of the hosts concerned

Towards Detecting Intrusions in a Networked Environment

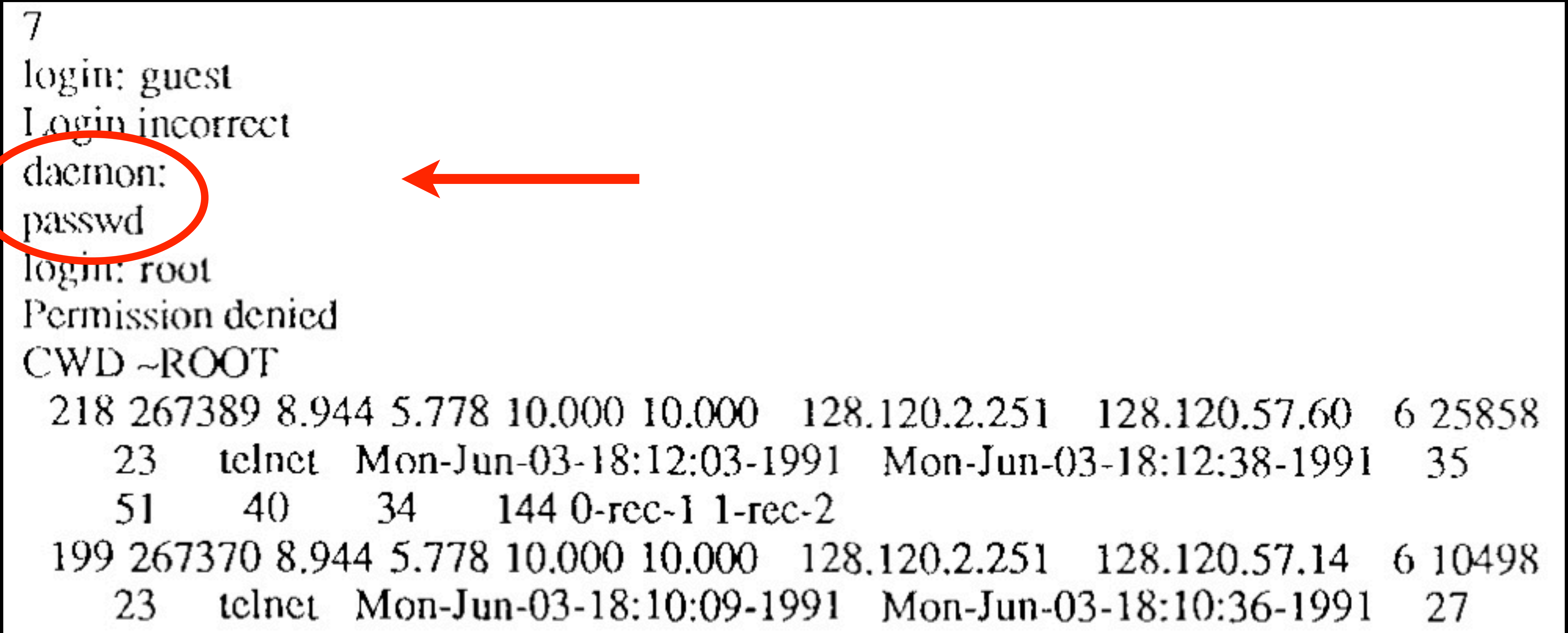
L. Todd Heberlein

Division of Computer Science
Report No: CSE-91-23
June 1991

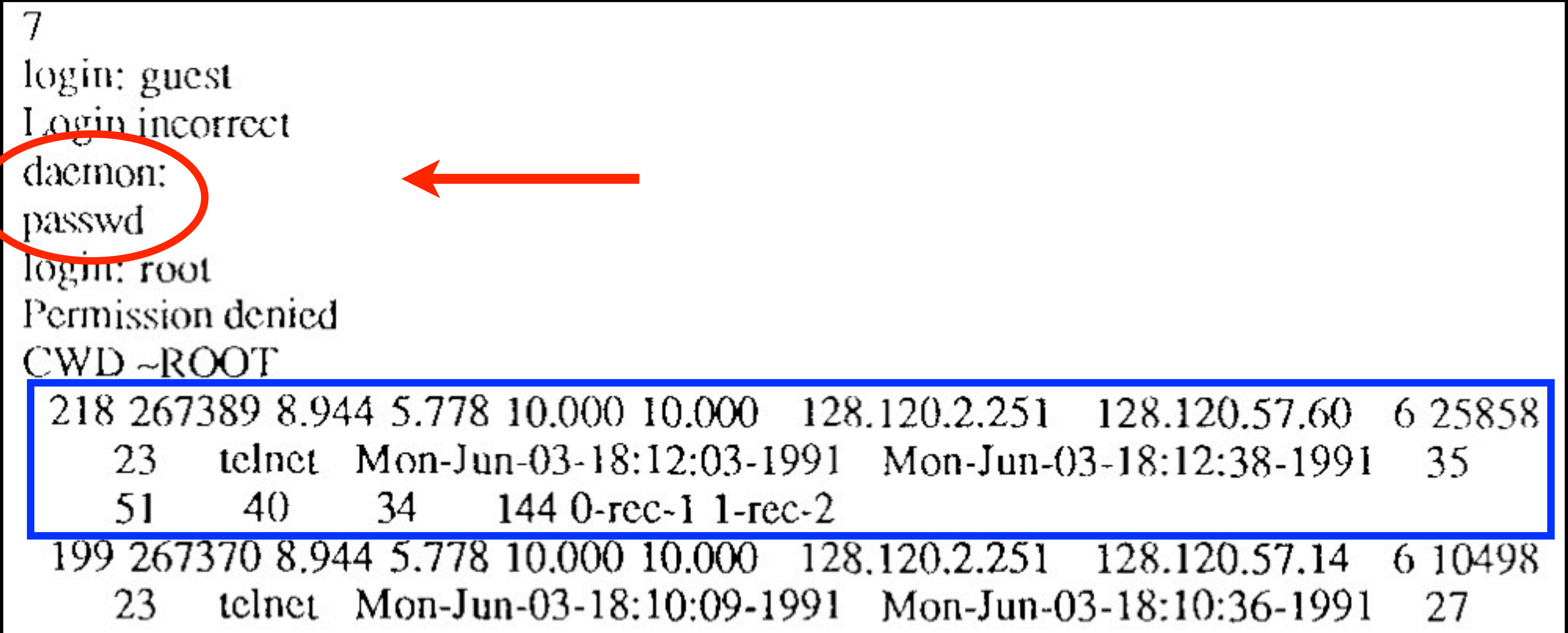
```
7
login: guest
Login incorrect
daemon:
passwd
login: root
Permission denied
CWD ~ROOT
  218 267389 8.944 5.778 10.000 10.000   128.120.2.251   128.120.57.60   6 25858
      23     telnet   Mon-Jun-03-18:12:03-1991   Mon-Jun-03-18:12:38-1991    35
      51       40       34       144 0-rec-1 1-rec-2
  199 267370 8.944 5.778 10.000 10.000   128.120.2.251   128.120.57.14   6 10498
      23     telnet   Mon-Jun-03-18:10:09-1991   Mon-Jun-03-18:10:36-1991    27
```



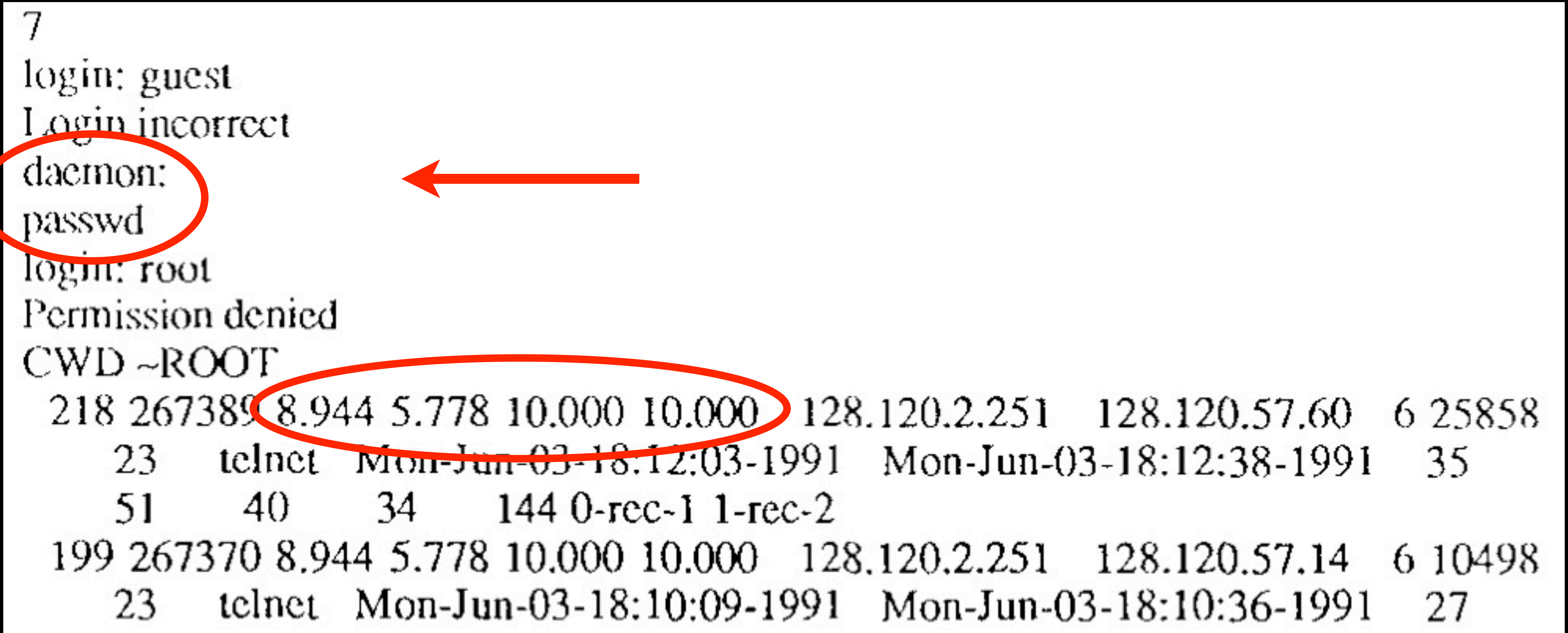
```
7
login: guest
Login incorrect
daemon:
passwd
login: root
Permission denied
CWD ~ROOT
  218 267389 8.944 5.778 10.000 10.000   128.120.2.251   128.120.57.60   6 25858
      23     telnet   Mon-Jun-03-18:12:03-1991   Mon-Jun-03-18:12:38-1991    35
      51       40       34       144 0-rec-1 1-rec-2
  199 267370 8.944 5.778 10.000 10.000   128.120.2.251   128.120.57.14   6 10498
      23     telnet   Mon-Jun-03-18:10:09-1991   Mon-Jun-03-18:10:36-1991    27
```



```
7
login: guest
Login incorrect
daemon:
passwd
login: root
Permission denied
CWD ~ROOT
  218 267389 8.944 5.778 10.000 10.000    128.120.2.251    128.120.57.60    6 25858
      23      telnet   Mon-Jun-03-18:12:03-1991   Mon-Jun-03-18:12:38-1991    35
      51        40        34       144 0-rec-1  1-rec-2
  199 267370 8.944 5.778 10.000 10.000    128.120.2.251    128.120.57.14    6 10498
      23      telnet   Mon-Jun-03-18:10:09-1991   Mon-Jun-03-18:10:36-1991    27
```



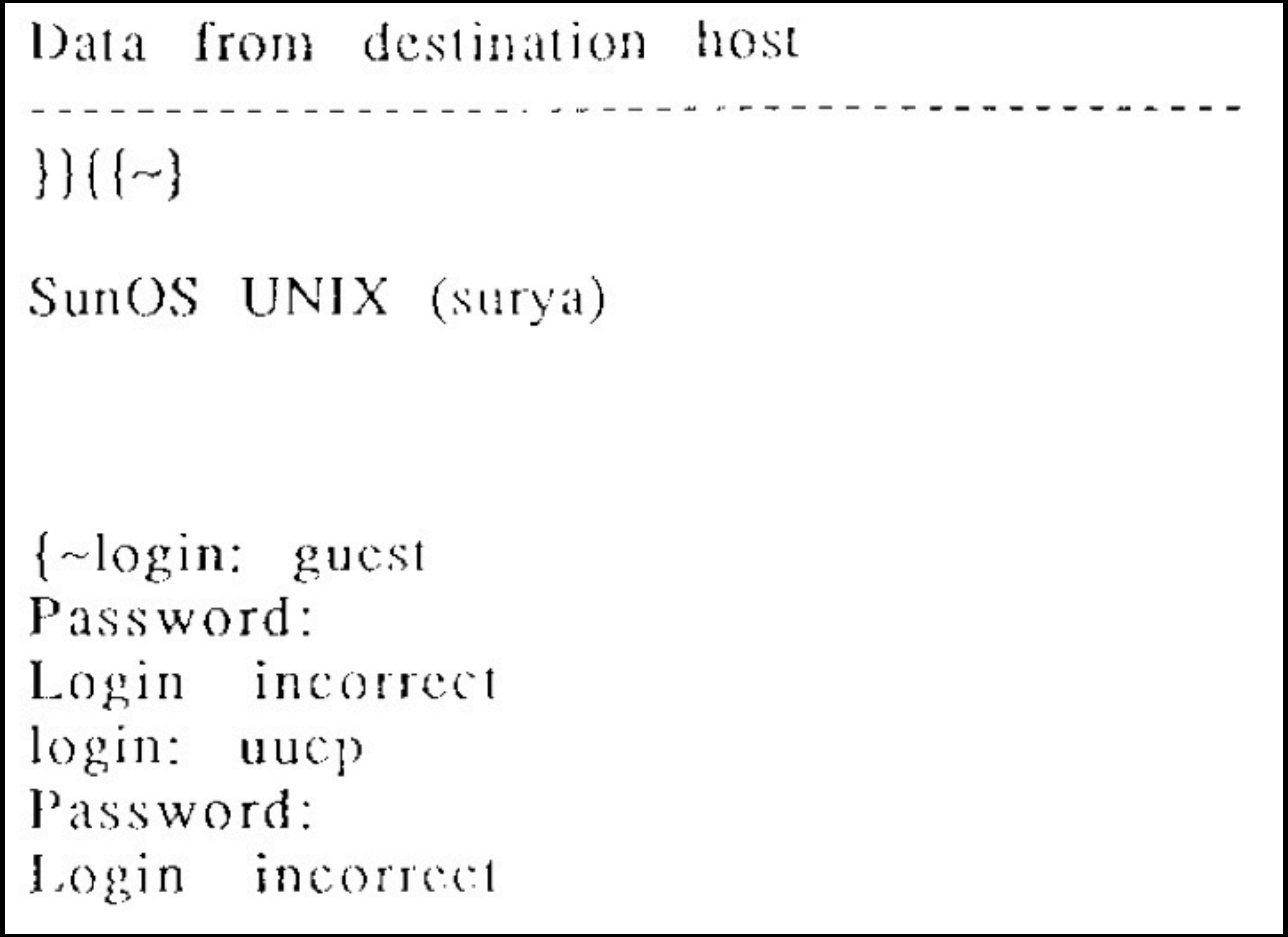
```
7
login: guest
Login incorrect
daemon:
passwd
login: root
Permission denied
CWD ~ROOT
 218 267389 8.944 5.778 10.000 10.000   128.120.2.251   128.120.57.60   6 25858
     23     telnet   Mon-Jun-03-18:12:03-1991   Mon-Jun-03-18:12:38-1991    35
     51       40       34       144 0-rec-1 1-rec-2
 199 267370 8.944 5.778 10.000 10.000   128.120.2.251   128.120.57.14   6 10498
     23     telnet   Mon-Jun-03-18:10:09-1991   Mon-Jun-03-18:10:36-1991    27
```



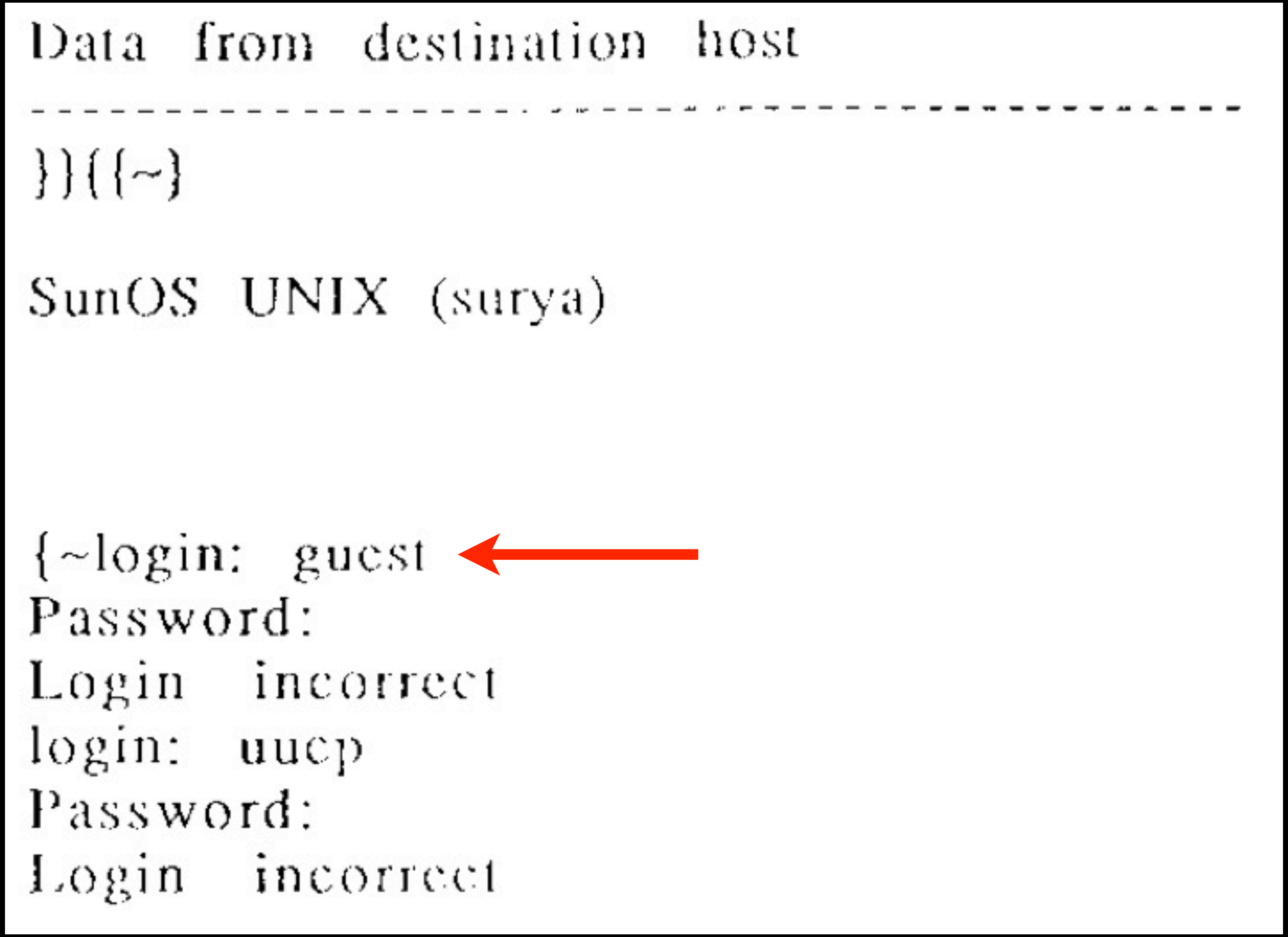
```
7
login: guest
Login incorrect
daemon:
passwd
login: root
Permission denied
CWD ~ROOT
  218 267389 8.944 5.778 10.000 10.000   128.120.2.251   128.120.57.60   6 25858
      23    telnet   Mon-Jun-03-18:12:03-1991   Mon-Jun-03-18:12:38-1991   35
      51      40      34      144 0-rec-1 1-rec-2
  199 267370 8.944 5.778 10.000 10.000   128.120.2.251   128.120.57.14   6 10498
      23    telnet   Mon-Jun-03-18:10:09-1991   Mon-Jun-03-18:10:36-1991   27
```

TRANSCRIPT

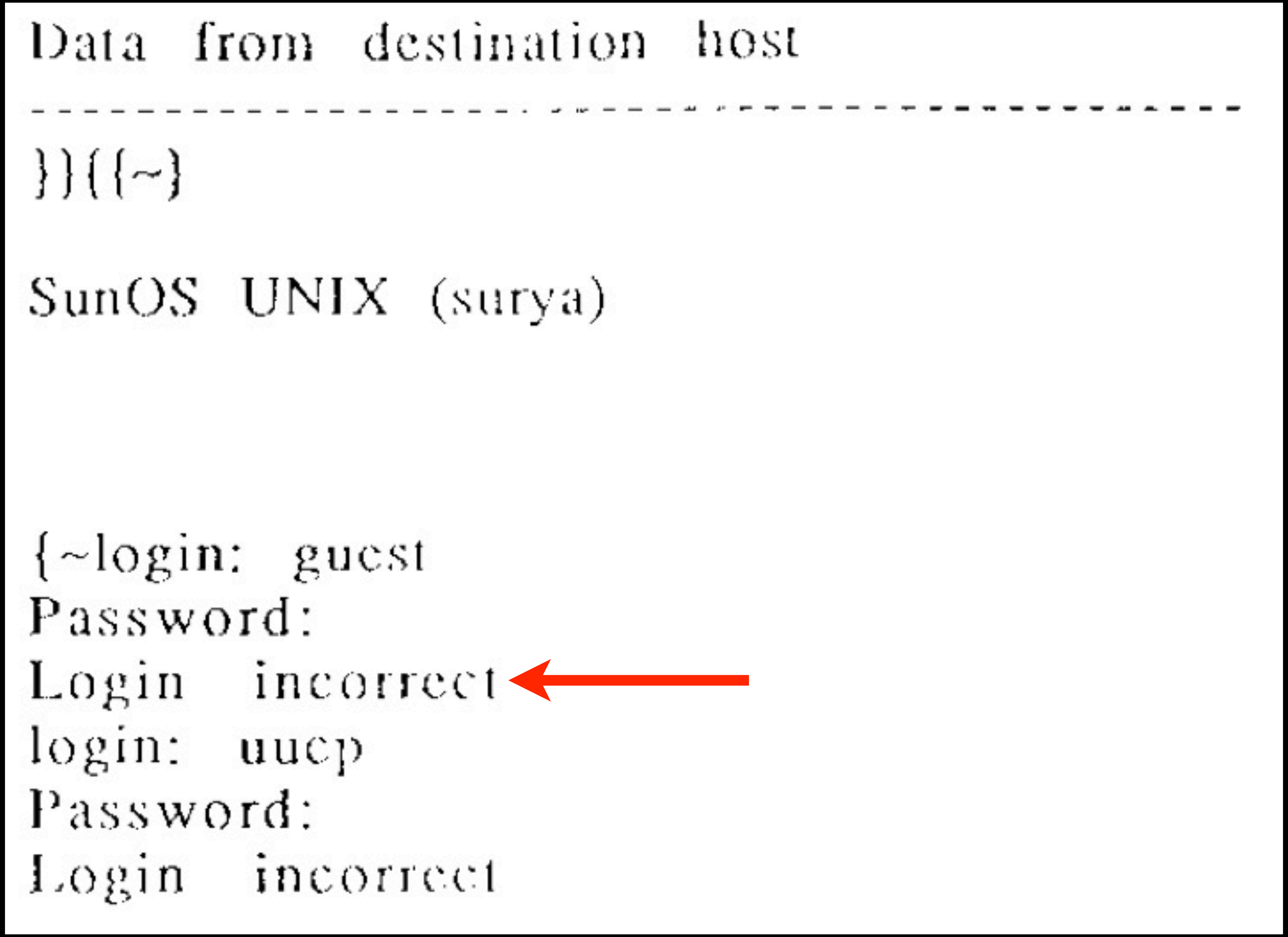
```
For connection file:   warn91-6-3
and connection index:  218

Initiating host:   128.120.2.251
Destination host:  128.120.57.60
Service:           telnet

Start time:  Mon-Jun-03-18:12:03-1991
End time:     Mon-Jun-03-18:12:38-1991

Warning level:  8.944
words matched from initiating host:
words matched from destination host:
        Login incorrect    2
        login: guest    1
```



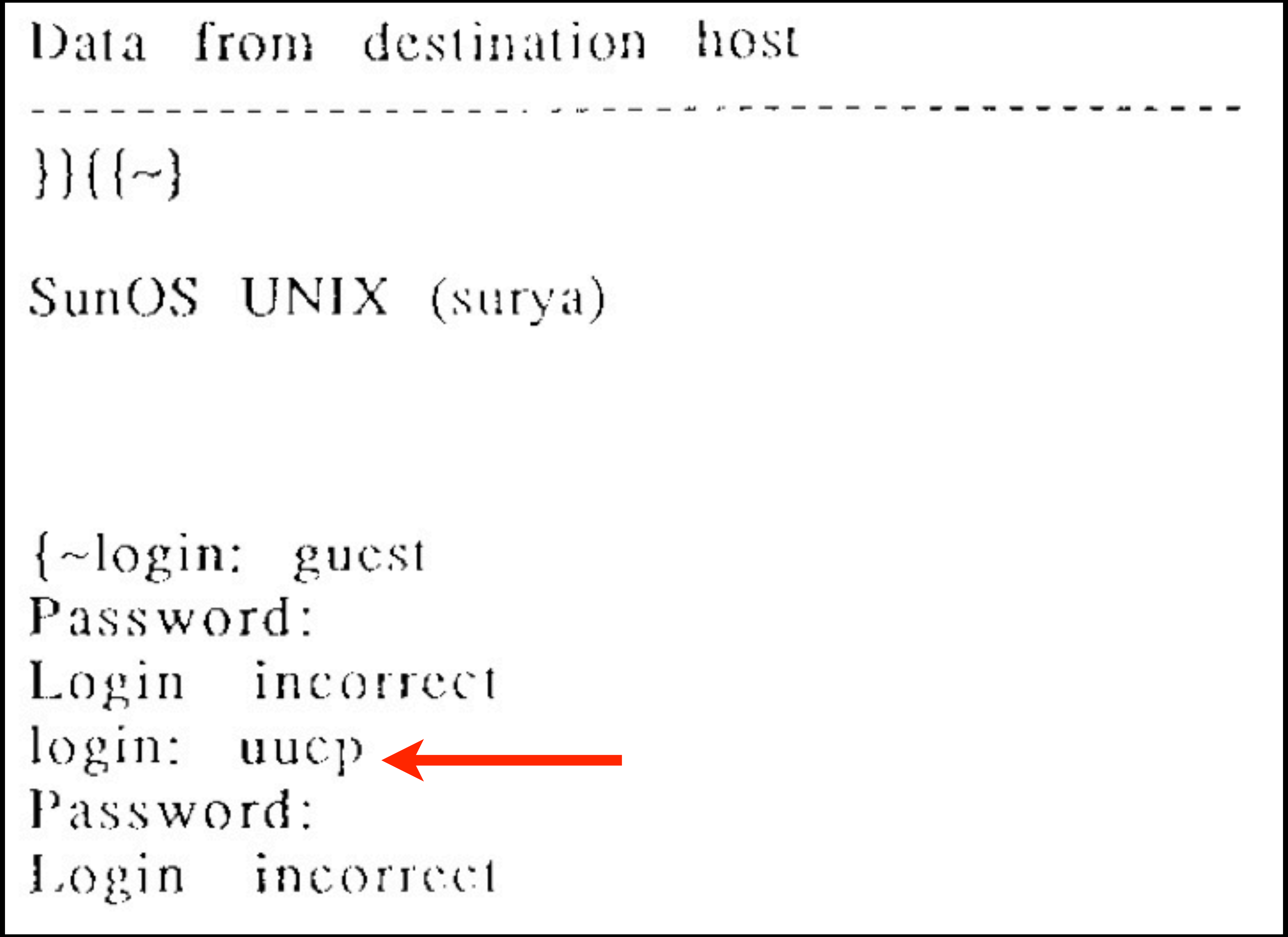
```
Data from destination host
---------------------------------------------------
}}{{~}

SunOS UNIX (surya)



{~login: guest
Password:
Login incorrect
login: uucp
Password:
Login incorrect
```



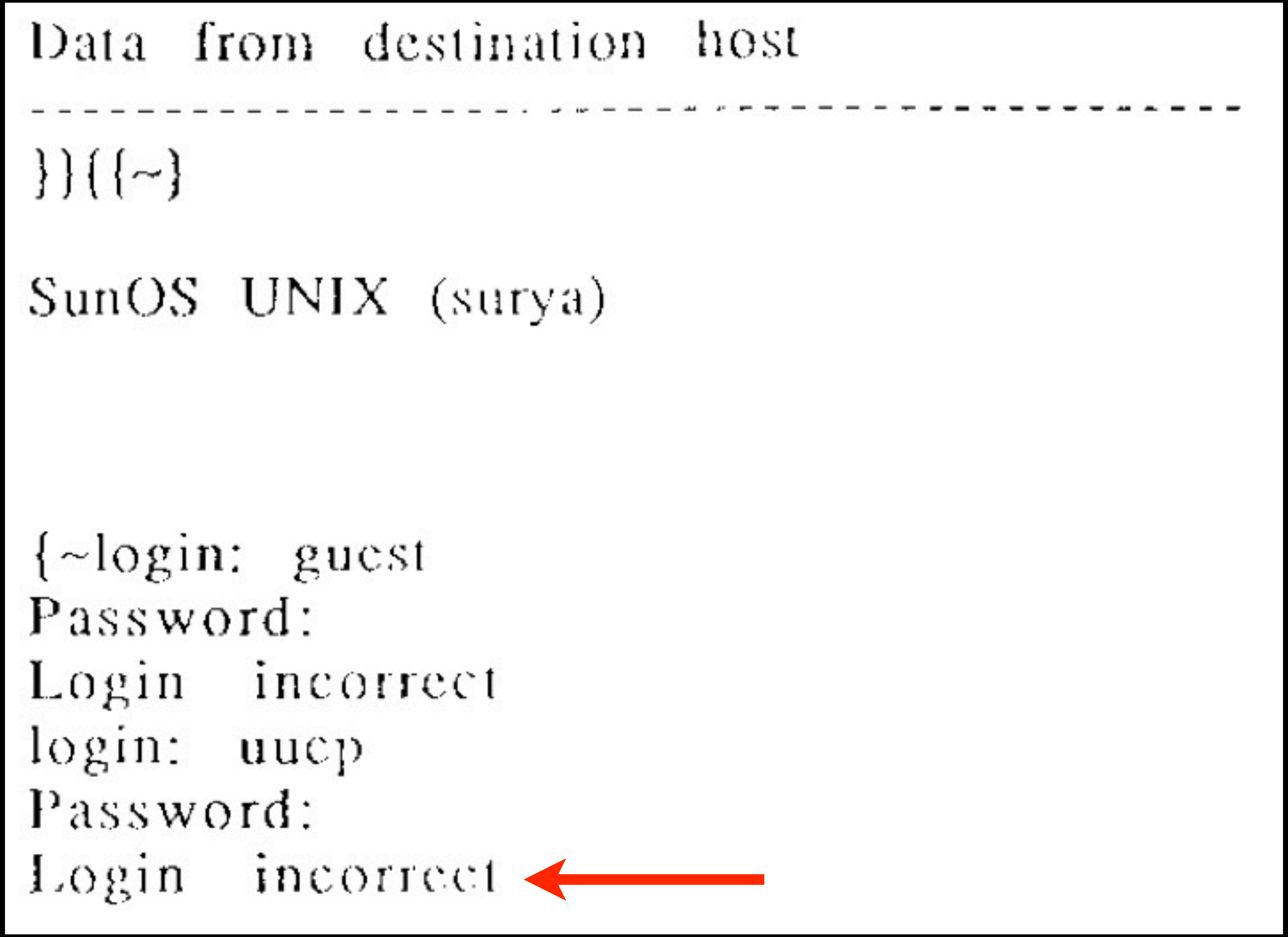
```
Data from destination host
------------------------------------------------
}}{{~}

SunOS UNIX (surya)



{~login: guest
Password:
Login incorrect
login: uucp
Password:
Login incorrect
```



```
Data  from  destination  host
-------------------------------------------------------
}}{{~}

SunOS  UNIX  (surya)




{~login:  guest
Password:
Login   incorrect
login:  uucp
Password:
Login   incorrect
```



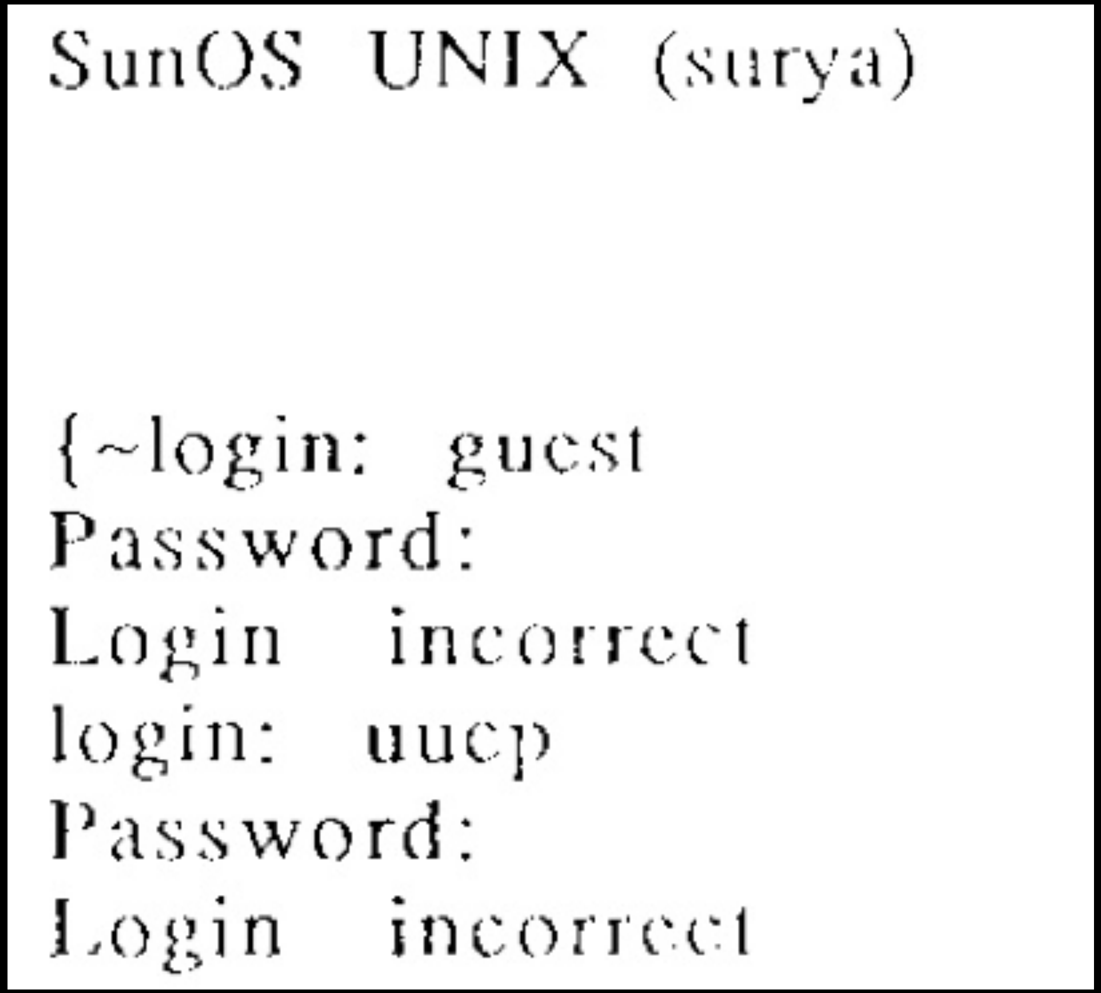
```
Data from destination host
------------------------------------------------------------
}}{{~}

SunOS UNIX (surya)



{~login: guest
Password:
Login incorrect
login: uucp
Password:
Login incorrect
```



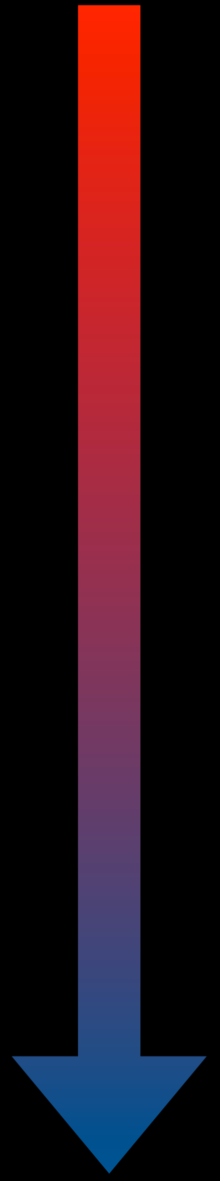
```
Data from destination host
--------------------------------------------------------
}}{{~}

SunOS UNIX (surya)



{~login: guest
Password:
Login incorrect
login: uucp
Password:
Login incorrect
```

Session 218 Warning: 8.9 Alert

Session 218 Warning: 8.9 Alert

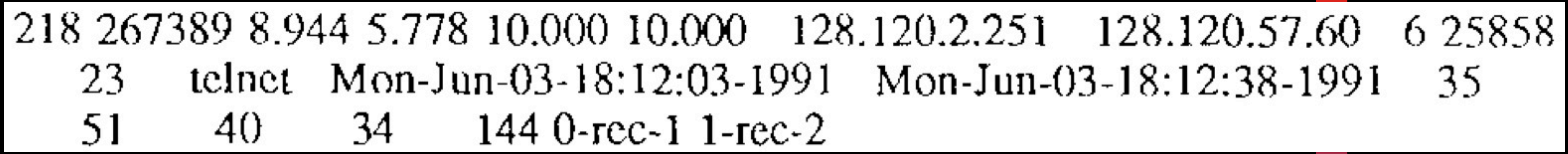


```
SunOS UNIX (surya)



{~login:  guest
Password:
Login  incorrect
login:  uucp
Password:
Login  incorrect
```

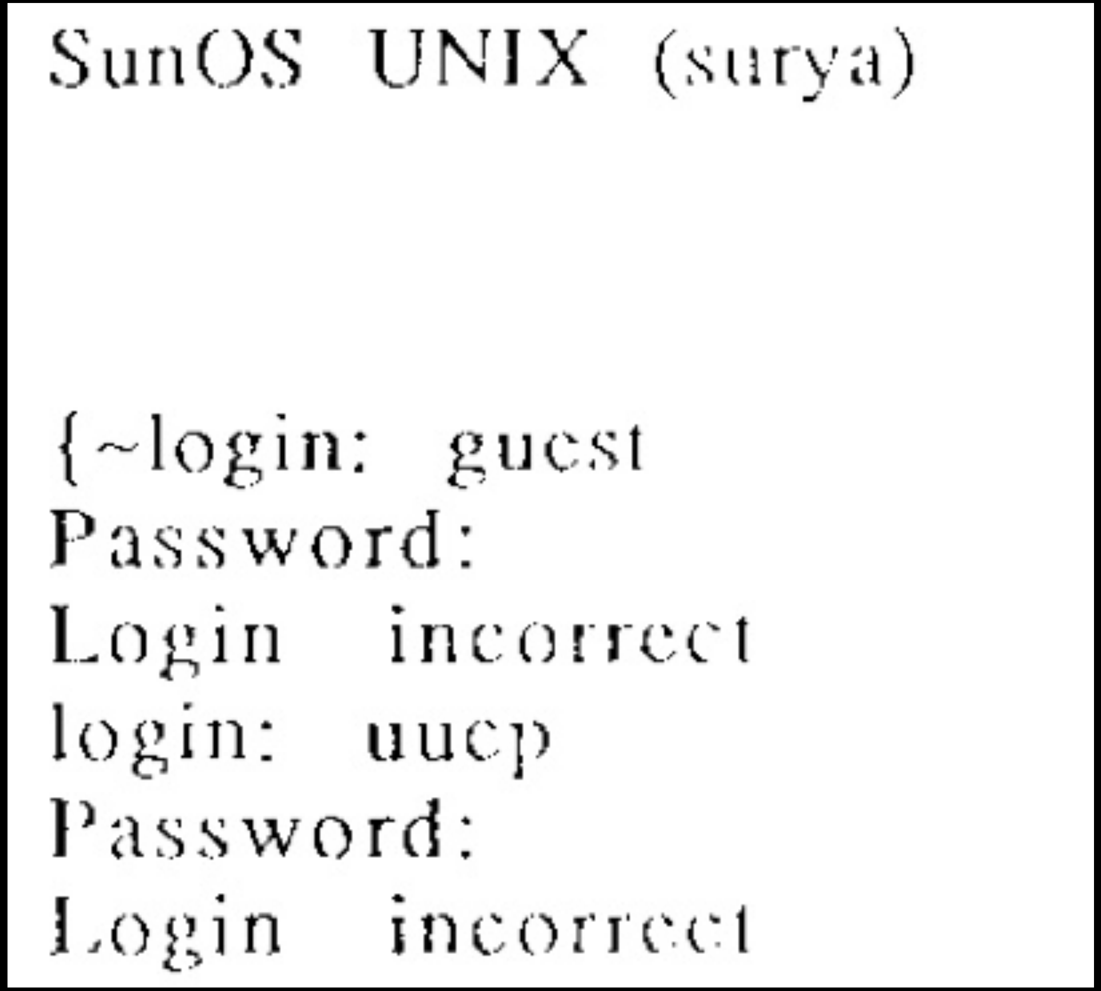


Diagnosis

Session 218   Warning: 8.9   Alert



```
218 267389 8.944 5.778 10.000 10.000   128.120.2.251   128.120.57.60   6 25858
    23     telnet   Mon-Jun-03-18:12:03-1991   Mon-Jun-03-18:12:38-1991   35
    51       40       34       144 0-rec-1 1-rec-2
```

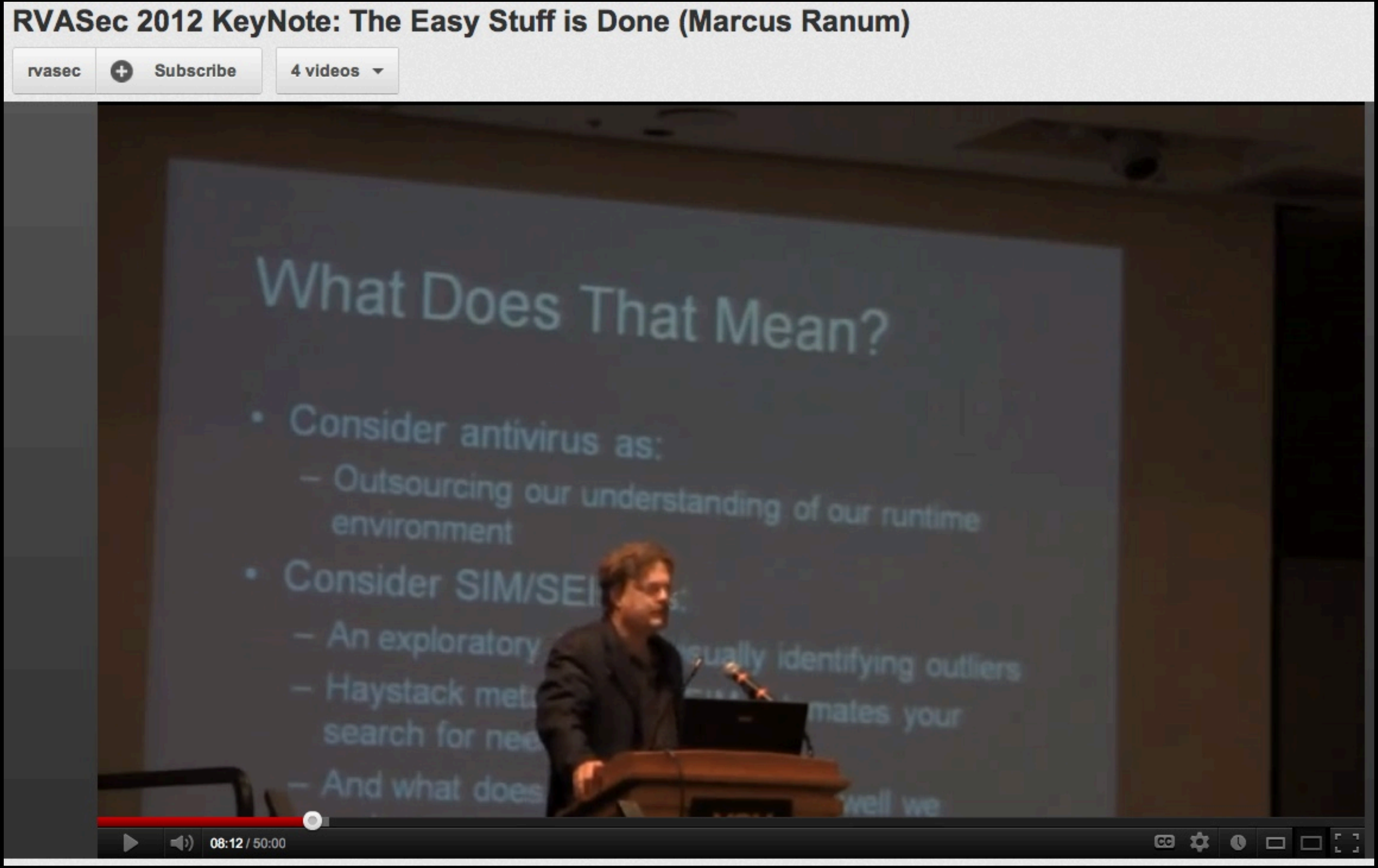


```
SunOS UNIX (surya)



{~login:  guest
Password:
Login  incorrect
login:  uucp
Password:
Login  incorrect
```

Diagnosis

End of the line for network analysis

New “fuzzy” detection approaches will make your jobs difficult



RVASec 2012 KeyNote: The Easy Stuff is Done (Marcus Ranum)

What Does That Mean?

- Consider antivirus as:
  - Outsourcing our understanding of our runtime environment
- Consider SIM/SE
  - An exploratory … sually identifying outliers
  - Haystack met … mates your search for nee
  - And what does … well we

http://www.youtube.com/watch?v=UxipQv7vs0s

“If I’m doing something nasty to your network, the one thing I am going to do: everything I possibly can to not look like an outlier.”

– 08:12

"If I'm doing something nasty to your network, the one thing I am going to do: everything I possibly can to not look like an outlier."

– 08:12

"I am not going to do all the dumb stuff that the SEIM manufacturers are counting on me to do."

– 08:24

"If I'm doing something nasty to your network, the one thing I am going to do: everything I possibly can to not look like an outlier."

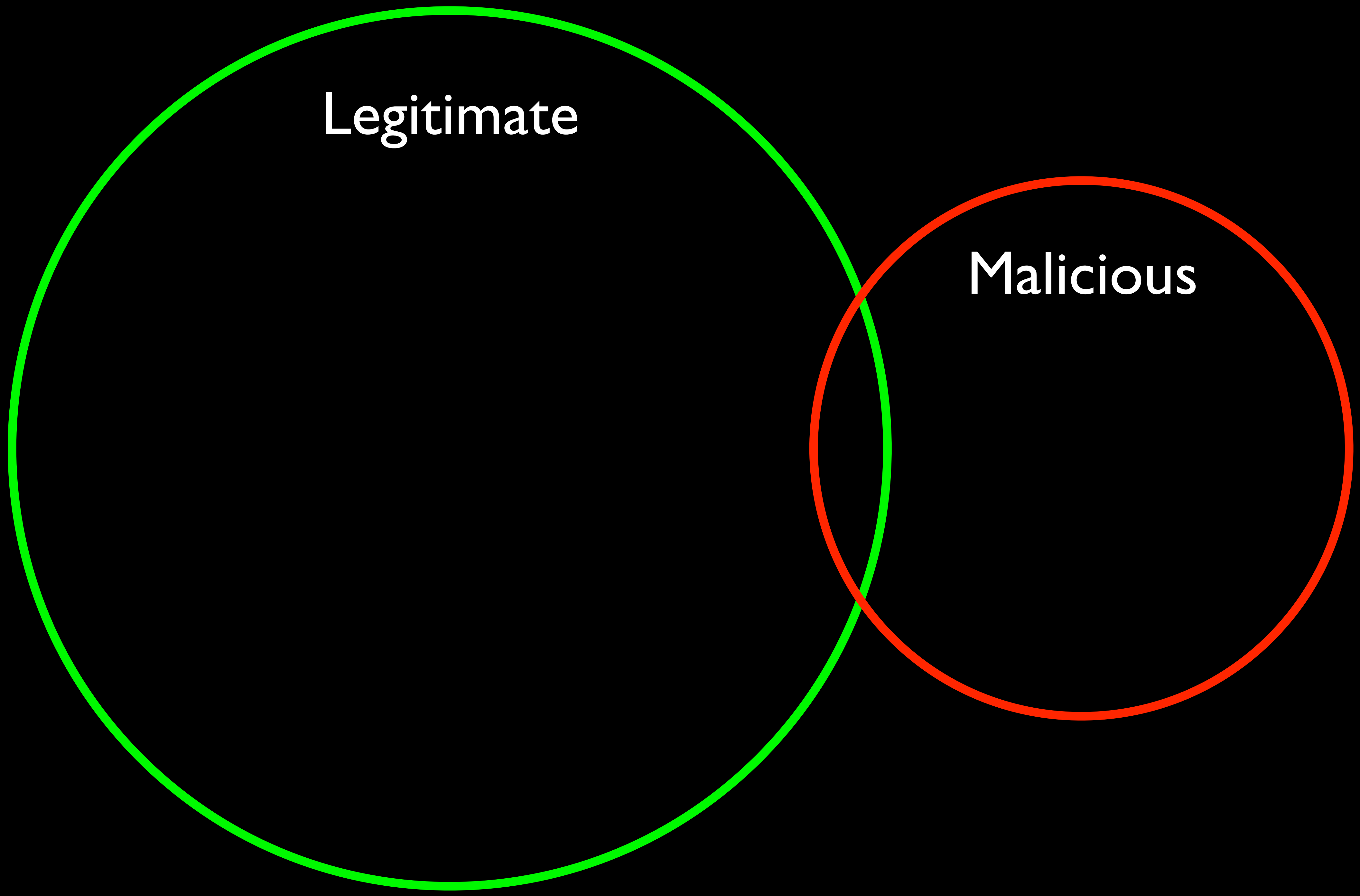
– 08:12

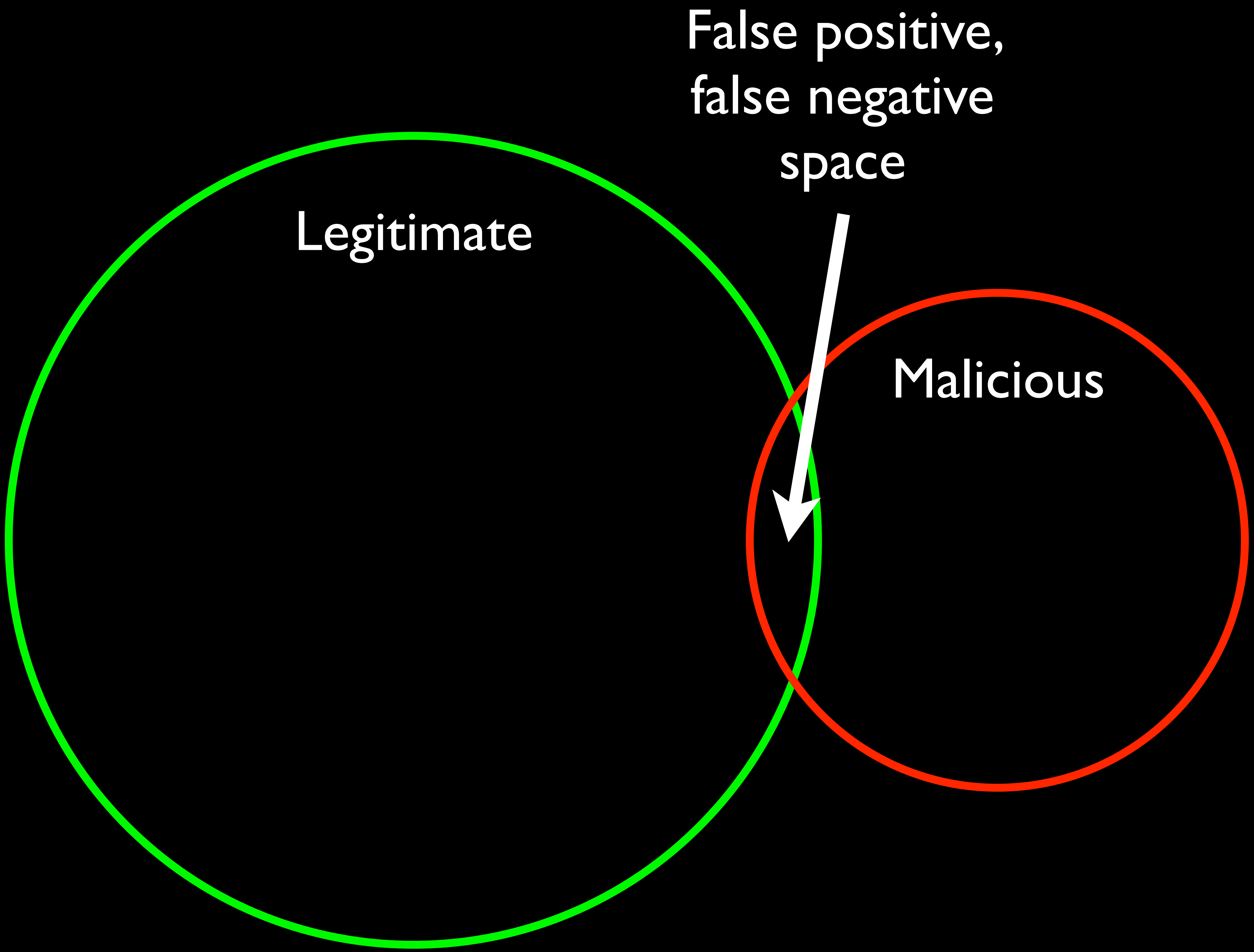
"I am not going to do all the dumb stuff that the SEIM manufacturers are counting on me to do."

– 08:24

"I am going to look like hay, and you gotta figure out how to deal with this."

– 08:58


Legitimate
Malicious

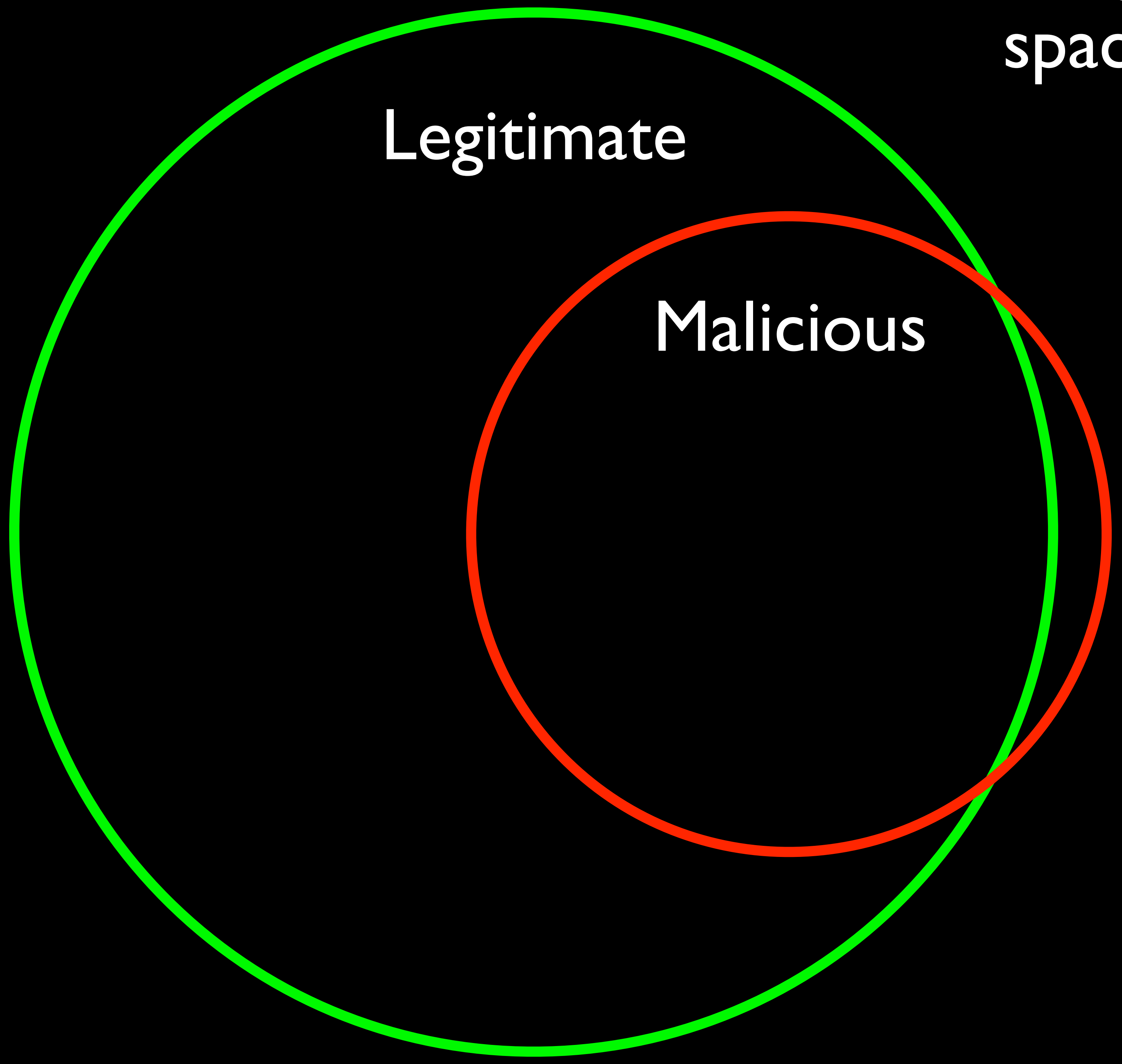


False positive, false negative space

Legitimate

Malicious

False positive,
false negative
space



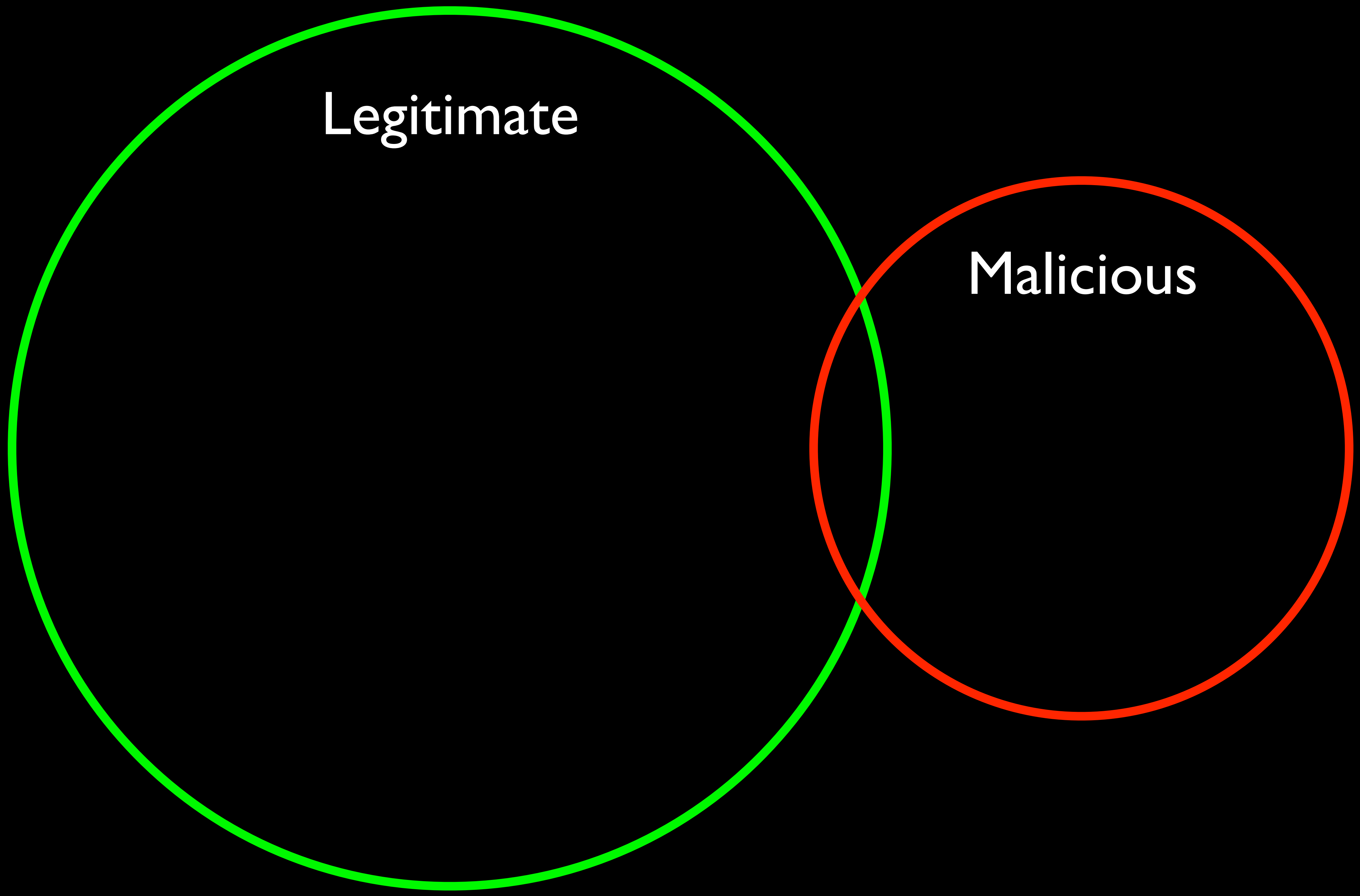
Legitimate

Malicious

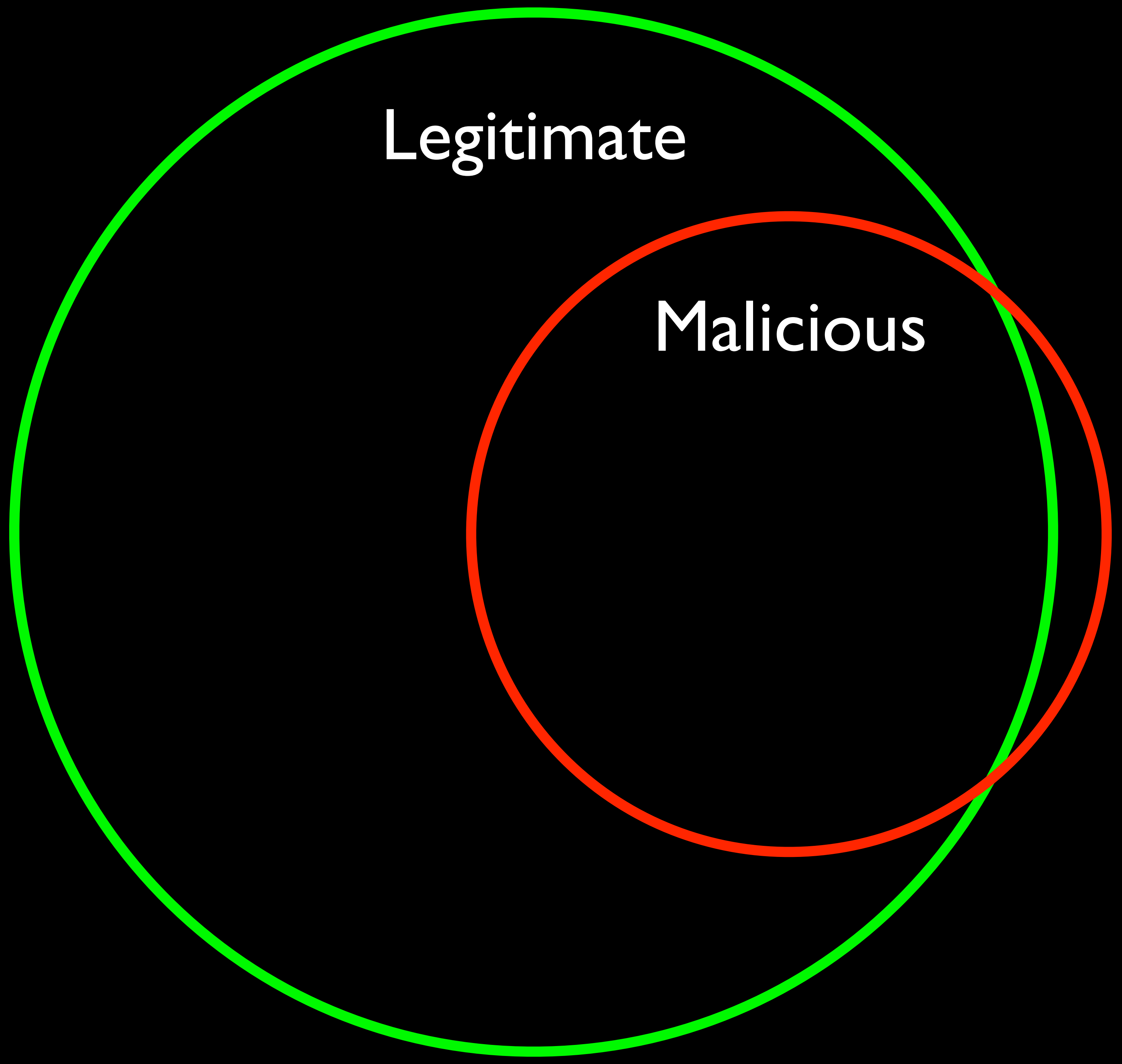
Network vs. Host

Network vs. Host

Claim: It is easier for the adversary to do this...

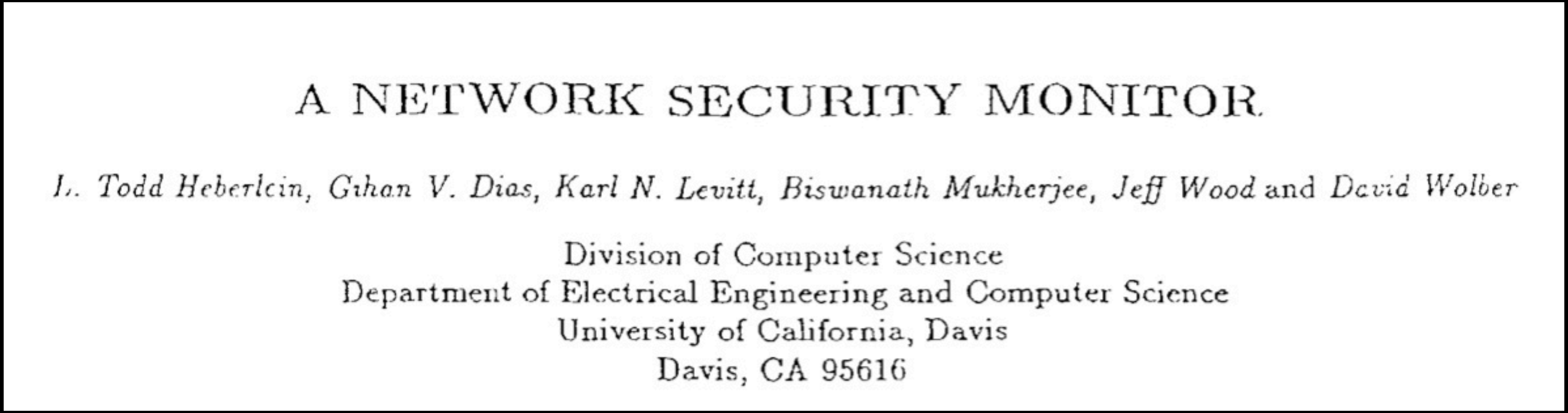


Legitimate
Malicious


Legitimate
Malicious

Network vs. Host

... with network-centric sensors



A NETWORK SECURITY MONITOR

L. Todd Heberlein, Gihan V. Dias, Karl N. Levitt, Biswanath Mukherjee, Jeff Wood and *David Wolber*

Division of Computer Science
Department of Electrical Engineering and Computer Science
University of California, Davis
Davis, CA 95616

Published: May 1990

“A second solution would be to examine audit trails generated by one of the hosts concerned”

Reaching Past the Low Hanging Fruit

Todd Heberlein

Net Squared, Inc.

[redacted]

SANS 99

10 May 1999

[redacted]

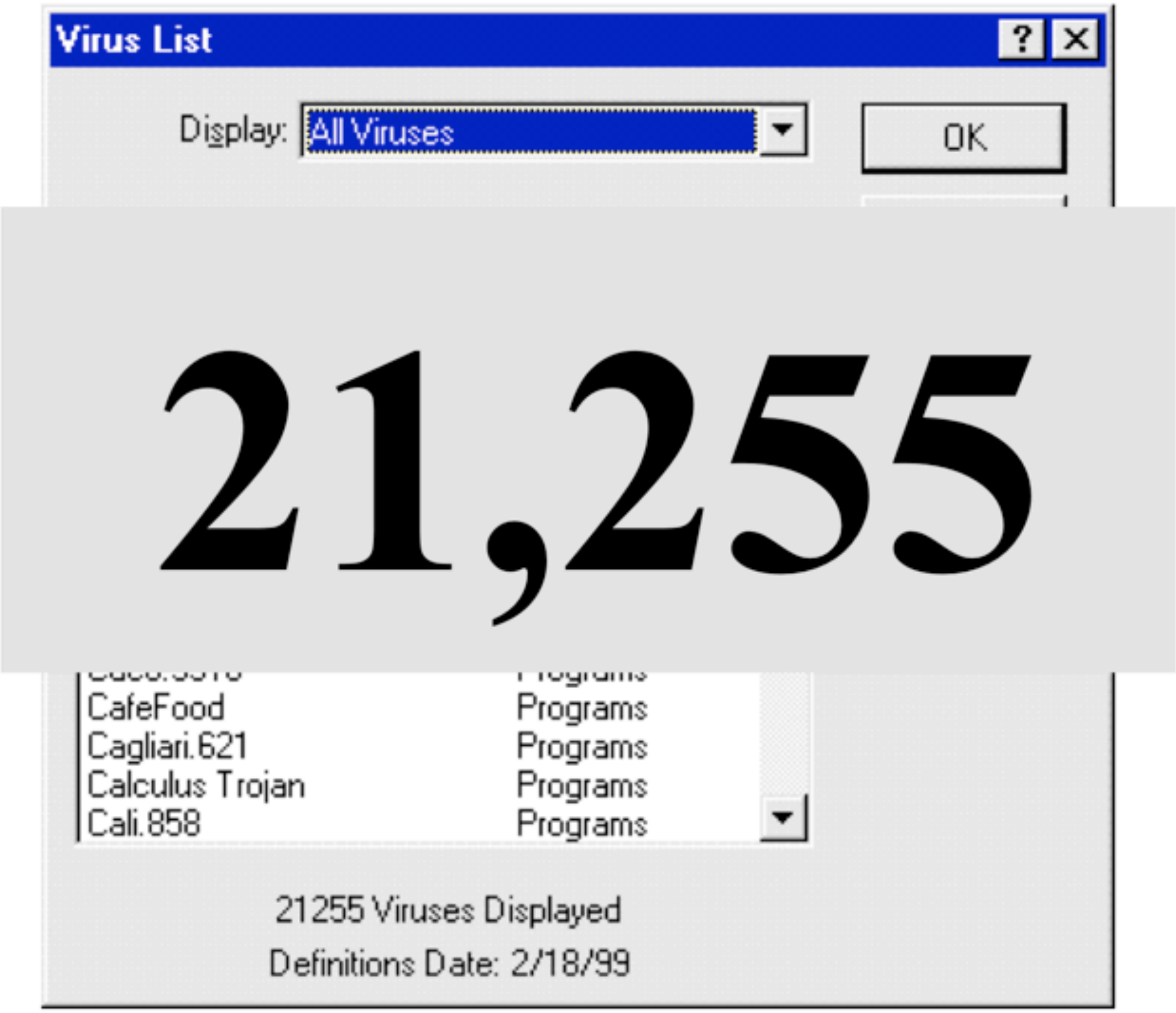
Detecting New Attacks

- Generally easier from the host (opinion!)
- Generic signatures
  - illegal transition to root
- Sequence-based detection
  - Profiling programs, not people
- StackGuard
- Specification-based detection
- Forensics, data mining, discovery

Detecting New Attacks

- Generally easier from the host (opinion!)
- Generic signatures
  - illegal transition to root
- Sequence-based detection
  - Profiling programs, not people
- StackGuard
- Specification-based detection
- Forensics, data mining, discovery

Tens of Thousands of Signatures

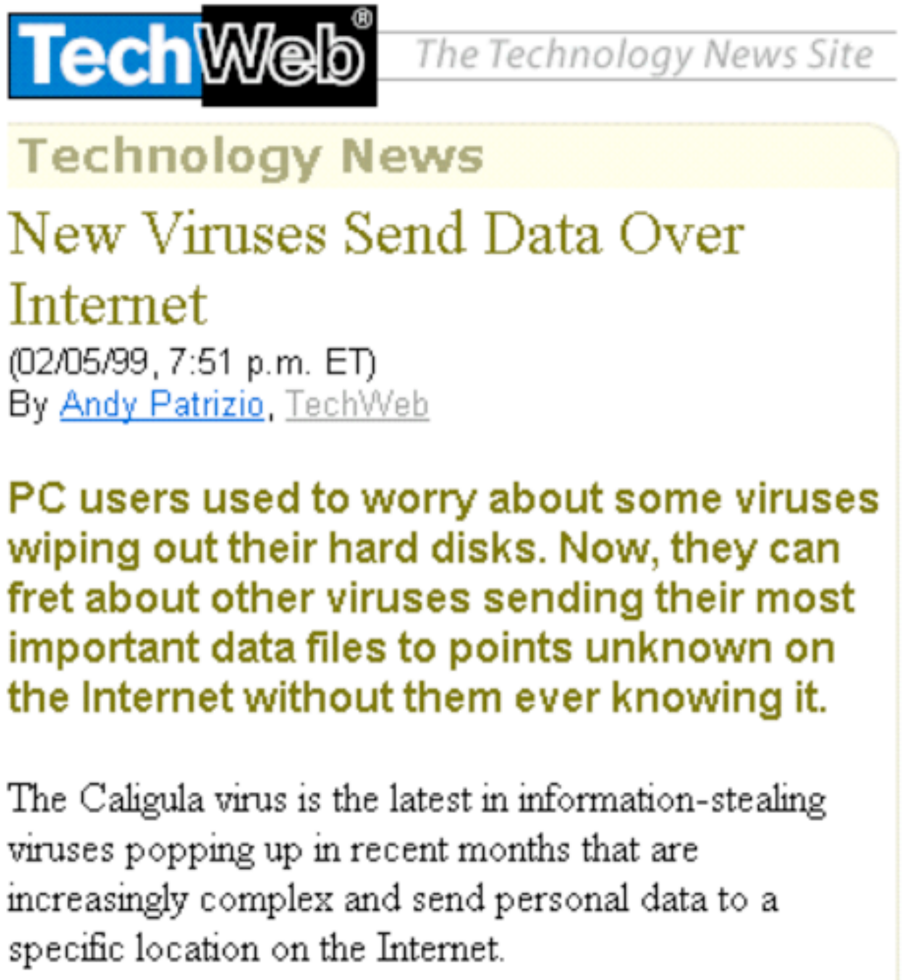


21,255

CafeFood	Programs
Cagliari.621	Programs
Calculus Trojan	Programs
Cali.858	Programs

21255 Viruses Displayed

Definitions Date: 2/18/99



Technology News

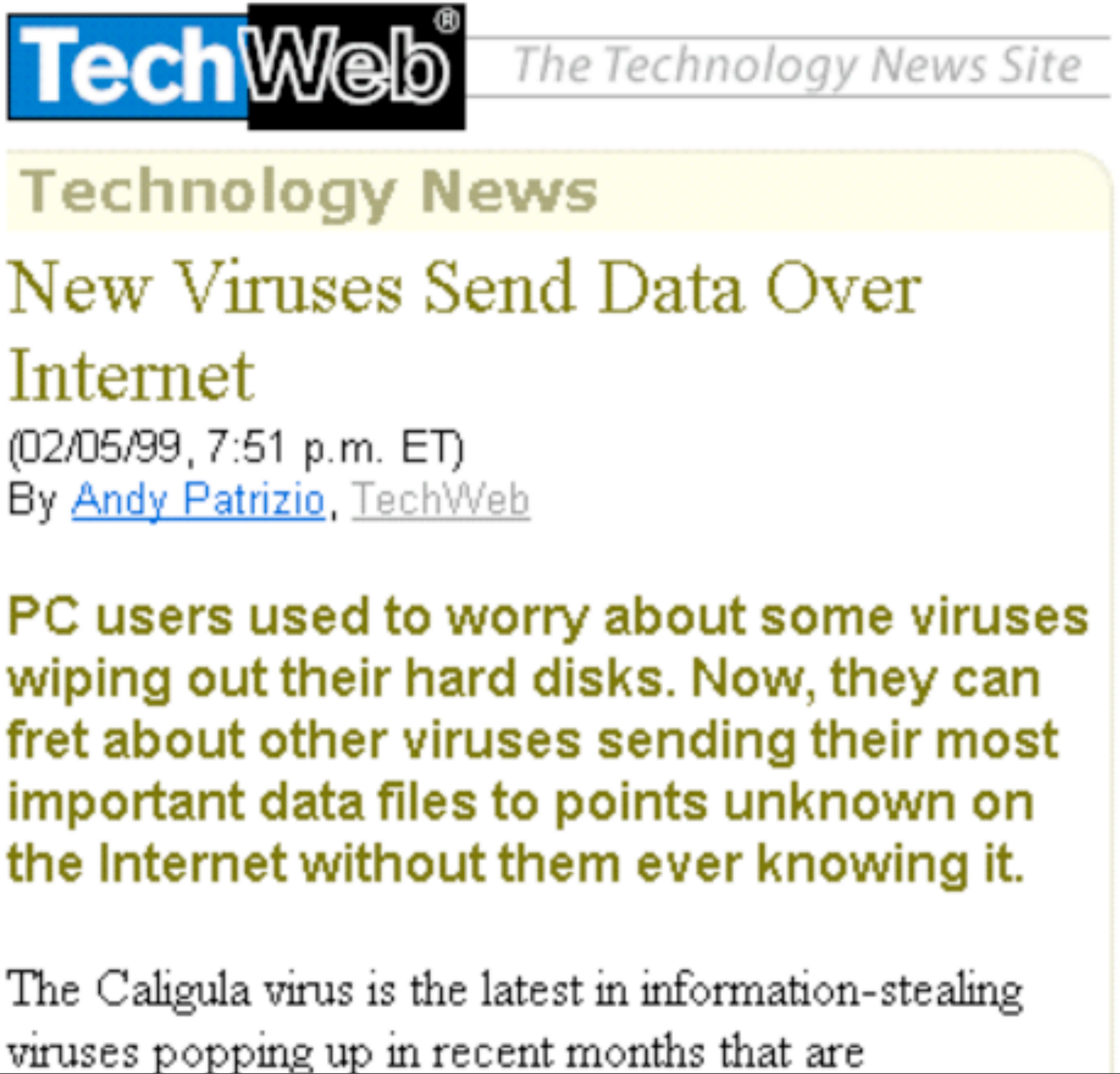
New Viruses Send Data Over Internet

(02/05/99, 7:51 p.m. ET)
By Andy Patrizio, TechWeb

PC users used to worry about some viruses wiping out their hard disks. Now, they can fret about other viruses sending their most important data files to points unknown on the Internet without them ever knowing it.

The Caligula virus is the latest in information-stealing viruses popping up in recent months that are increasingly complex and send personal data to a specific location on the Internet.

255



Technology News

New Viruses Send Data Over Internet

(02/05/99, 7:51 p.m. ET)
By Andy Patrizio, TechWeb

PC users used to worry about some viruses wiping out their hard disks. Now, they can fret about other viruses sending their most important data files to points unknown on the Internet without them ever knowing it.

The Caligula virus is the latest in information-stealing viruses popping up in recent months that are

Three Examples

Three Examples

- Glowing Embers (based on Google's software update)

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

Three Examples

- Glowing Embers (based on Google's software update)

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

- SNSCat (any public channel can be a C&C Server)

  http://www.blackhat.com/html/bh-us-12/bh-us-12-briefings.html#Gunter

Three Examples

- Glowing Embers (based on Google’s software update)

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

- SNSCat (any public channel can be a C&C Server)

  http://www.blackhat.com/html/bh-us-12/bh-us-12-briefings.html#Gunter

- Dropbox

```
$ cp '2012 SANS 08.key' ~/Dropbox/.foo/.
```

Three Examples

- Glowing Embers (based on Google's software update)

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

- SNSCat (any public channel can be a C&C Server)

  http://www.blackhat.com/html/bh-us-12/bh-us-12-briefings.html#Gunter

- Dropbox

```
$ cp '2012 SANS 08.key' ~/Dropbox/.foo/.
```

The Role of Auditing

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

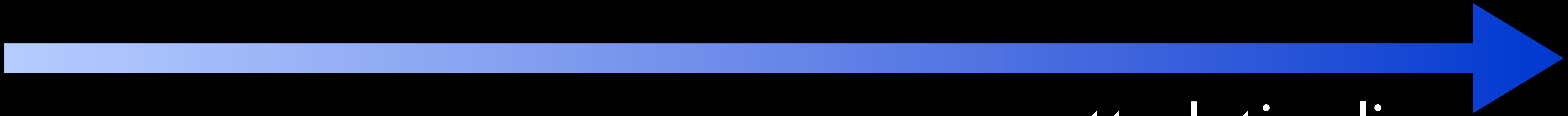
Disk Forensics

Memory Forensics

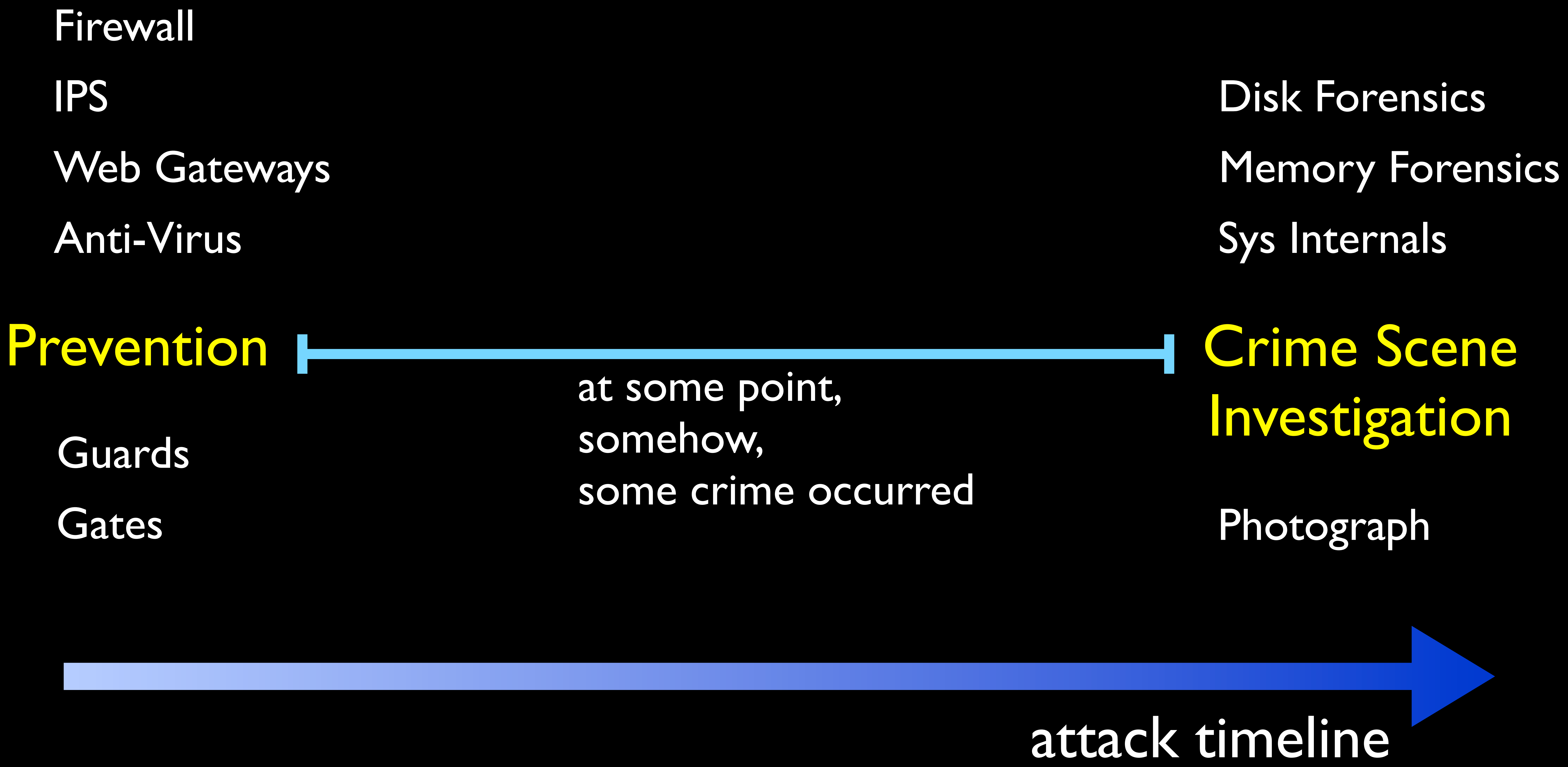
Sys Internals

Crime Scene Investigation

Photograph



attack timeline



Firewall

IPS

Web Gateways

Anti-Virus

Prevention

Guards

Gates

at some point,
somehow,
some crime occurred

Disk Forensics

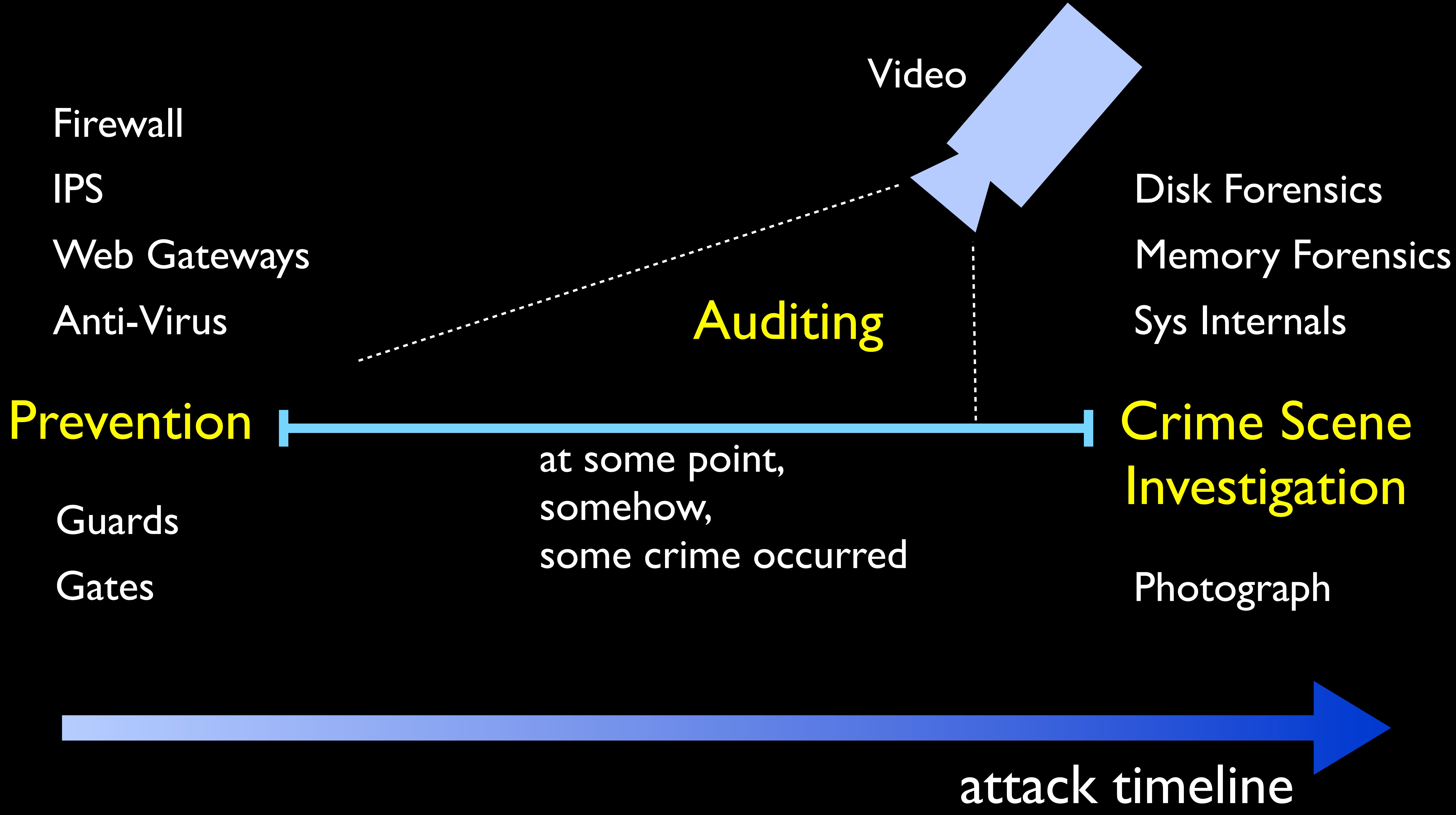
Memory Forensics

Sys Internals

Crime Scene
Investigation

Photograph

attack timeline



Video

Firewall

IPS

Web Gateways

Anti-Virus

Auditing

Disk Forensics

Memory Forensics

Sys Internals

Prevention

Crime Scene Investigation

at some point,
somehow,
some crime occurred

Guards

Gates

Photograph

attack timeline

Demo

(Audit Viewer)

Windows Has Good Auditing Too

Windows 7 Audit Trails: Exfiltration of the Swift

http://www.netsq.com/Podcasts/Data/2010/TheSwift/

Windows 7 Audit Trails: An Introduction

http://www.netsq.com/Documents/Windows_Auditing4.pdf

Analyzing Windows EVTX Logs

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

Google, the APT,
from the audit trail perspective

Audit Explorer Tutorial Videos

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

The Advanced Persistent Threat You Have: Google Chrome

http://www.netsq.com/Research/Single.php?stuff=papers&num=23

The Making of "The Advanced Persistent Threat You Have: Google Chrome"

http://www.netsq.com/Research/Single.php?stuff=papers&num=24

Why Google Update

Why Google Update

- C&C agent that wakes up periodically and checks for new commands

Why Google Update

- C&C agent that wakes up periodically and checks for new commands
- Blends in with normal traffic

Why Google Update

- C&C agent that wakes up periodically and checks for new commands
- Blends in with normal traffic
- Downloads commands and executes them

Why Google Update

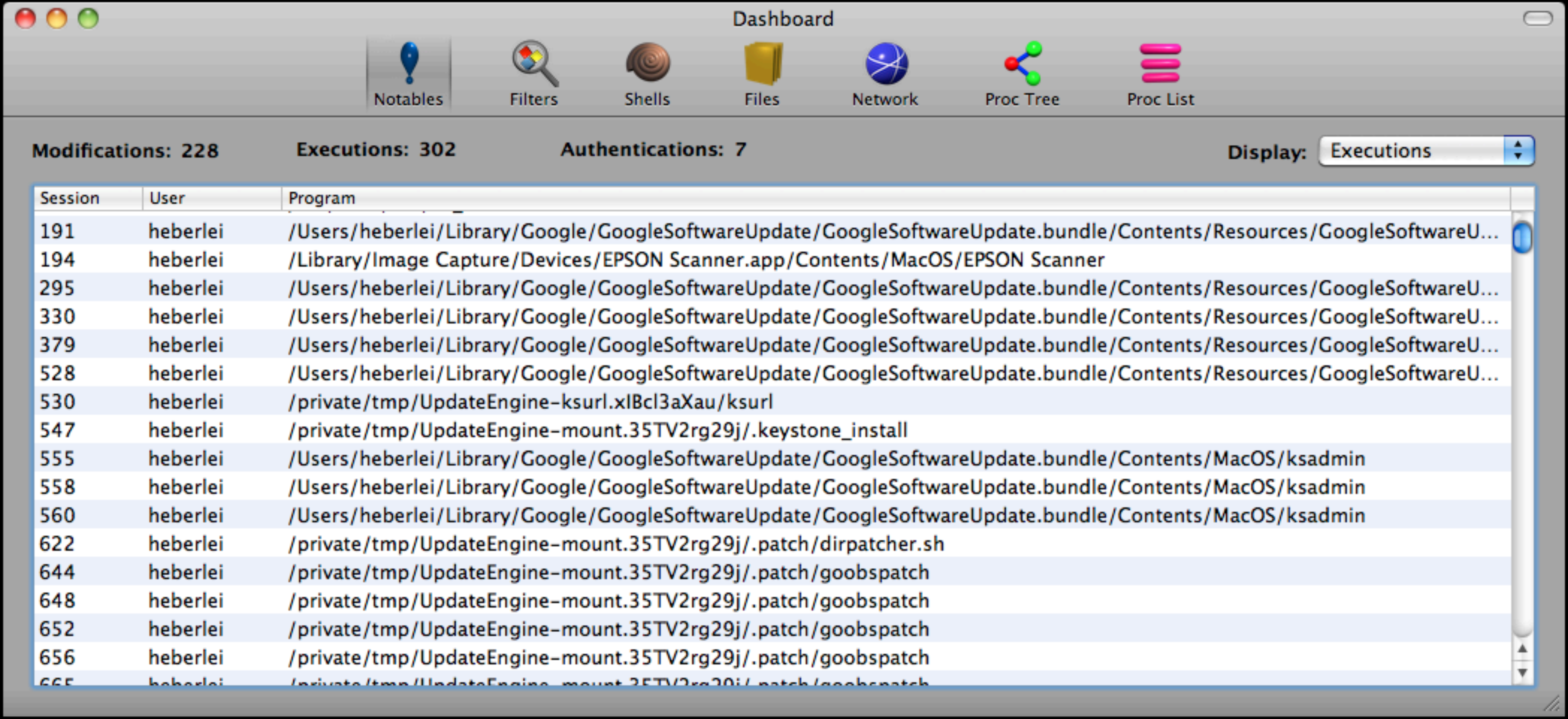
- C&C agent that wakes up periodically and checks for new commands
- Blends in with normal traffic
- Downloads commands and executes them
- Modifies security-critical software on your system

Why Google Update

- C&C agent that wakes up periodically and checks for new commands
- Blends in with normal traffic
- Downloads commands and executes them
- Modifies security-critical software on your system
- Gets rid of the evidence

Why Google Update

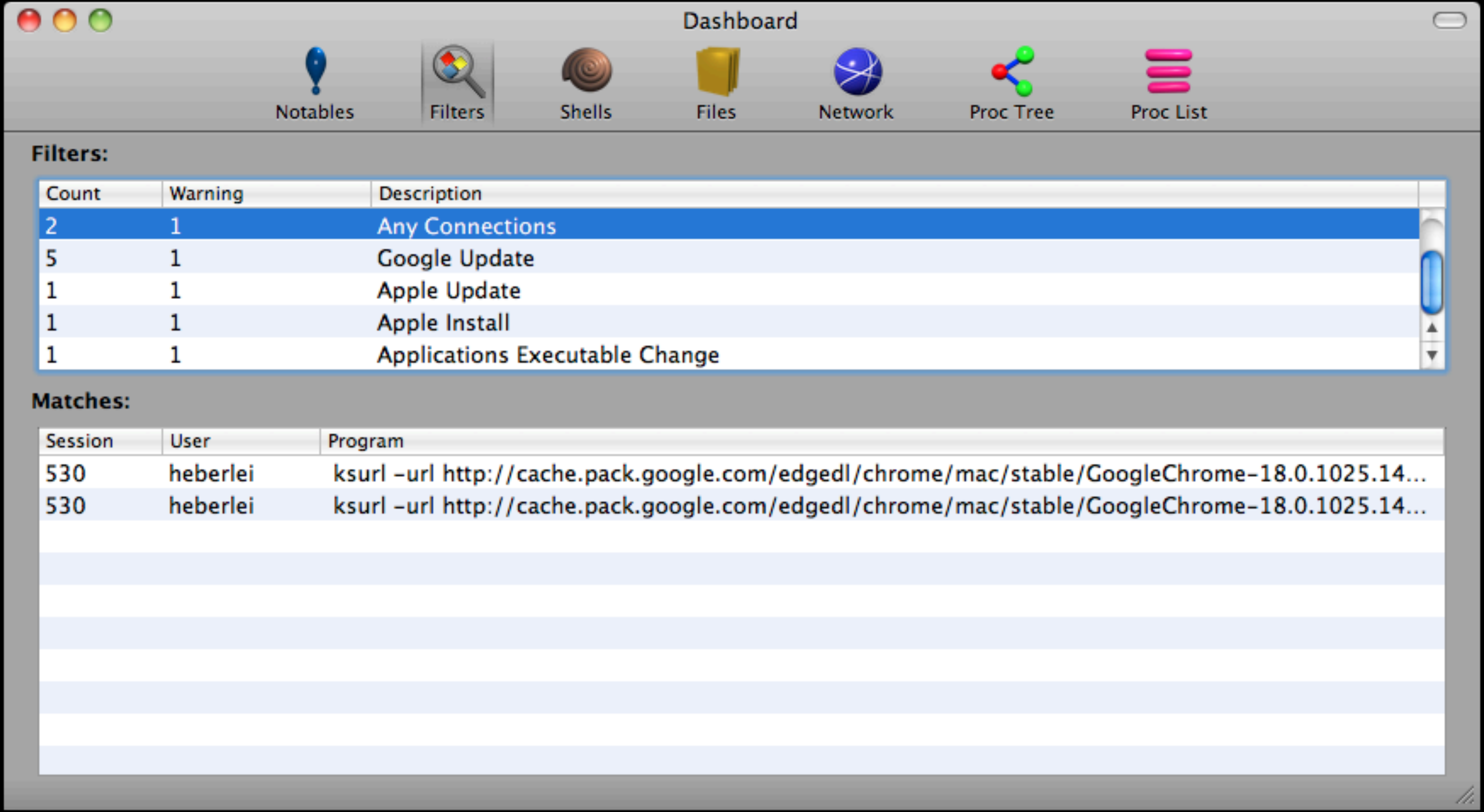
- C&C agent that wakes up periodically and checks for new commands
- Blends in with normal traffic
- Downloads commands and executes them
- Modifies security-critical software on your system
- Gets rid of the evidence
- If you can’t analyze this, can you analyze real APTs?



Modifications: 228 **Executions: 302** **Authentications: 7**

Display: Executions

Session	User	Program
191	heberlei	/Users/heberlei/Library/Google/GoogleSoftwareUpdate/GoogleSoftwareUpdate.bundle/Contents/Resources/GoogleSoftwareU...
194	heberlei	/Library/Image Capture/Devices/EPSON Scanner.app/Contents/MacOS/EPSON Scanner
295	heberlei	/Users/heberlei/Library/Google/GoogleSoftwareUpdate/GoogleSoftwareUpdate.bundle/Contents/Resources/GoogleSoftwareU...
330	heberlei	/Users/heberlei/Library/Google/GoogleSoftwareUpdate/GoogleSoftwareUpdate.bundle/Contents/Resources/GoogleSoftwareU...
379	heberlei	/Users/heberlei/Library/Google/GoogleSoftwareUpdate/GoogleSoftwareUpdate.bundle/Contents/Resources/GoogleSoftwareU...
528	heberlei	/Users/heberlei/Library/Google/GoogleSoftwareUpdate/GoogleSoftwareUpdate.bundle/Contents/Resources/GoogleSoftwareU...
530	heberlei	/private/tmp/UpdateEngine-ksurl.xlBcl3aXau/ksurl
547	heberlei	/private/tmp/UpdateEngine-mount.35TV2rg29j/.keystone_install
555	heberlei	/Users/heberlei/Library/Google/GoogleSoftwareUpdate/GoogleSoftwareUpdate.bundle/Contents/MacOS/ksadmin
558	heberlei	/Users/heberlei/Library/Google/GoogleSoftwareUpdate/GoogleSoftwareUpdate.bundle/Contents/MacOS/ksadmin
560	heberlei	/Users/heberlei/Library/Google/GoogleSoftwareUpdate/GoogleSoftwareUpdate.bundle/Contents/MacOS/ksadmin
622	heberlei	/private/tmp/UpdateEngine-mount.35TV2rg29j/.patch/dirpatcher.sh
644	heberlei	/private/tmp/UpdateEngine-mount.35TV2rg29j/.patch/goobspatch
648	heberlei	/private/tmp/UpdateEngine-mount.35TV2rg29j/.patch/goobspatch
652	heberlei	/private/tmp/UpdateEngine-mount.35TV2rg29j/.patch/goobspatch
656	heberlei	/private/tmp/UpdateEngine-mount.35TV2rg29j/.patch/goobspatch
665	heberlei	/private/tmp/UpdateEngine-mount.35TV2rg29j/.patch/goobspatch

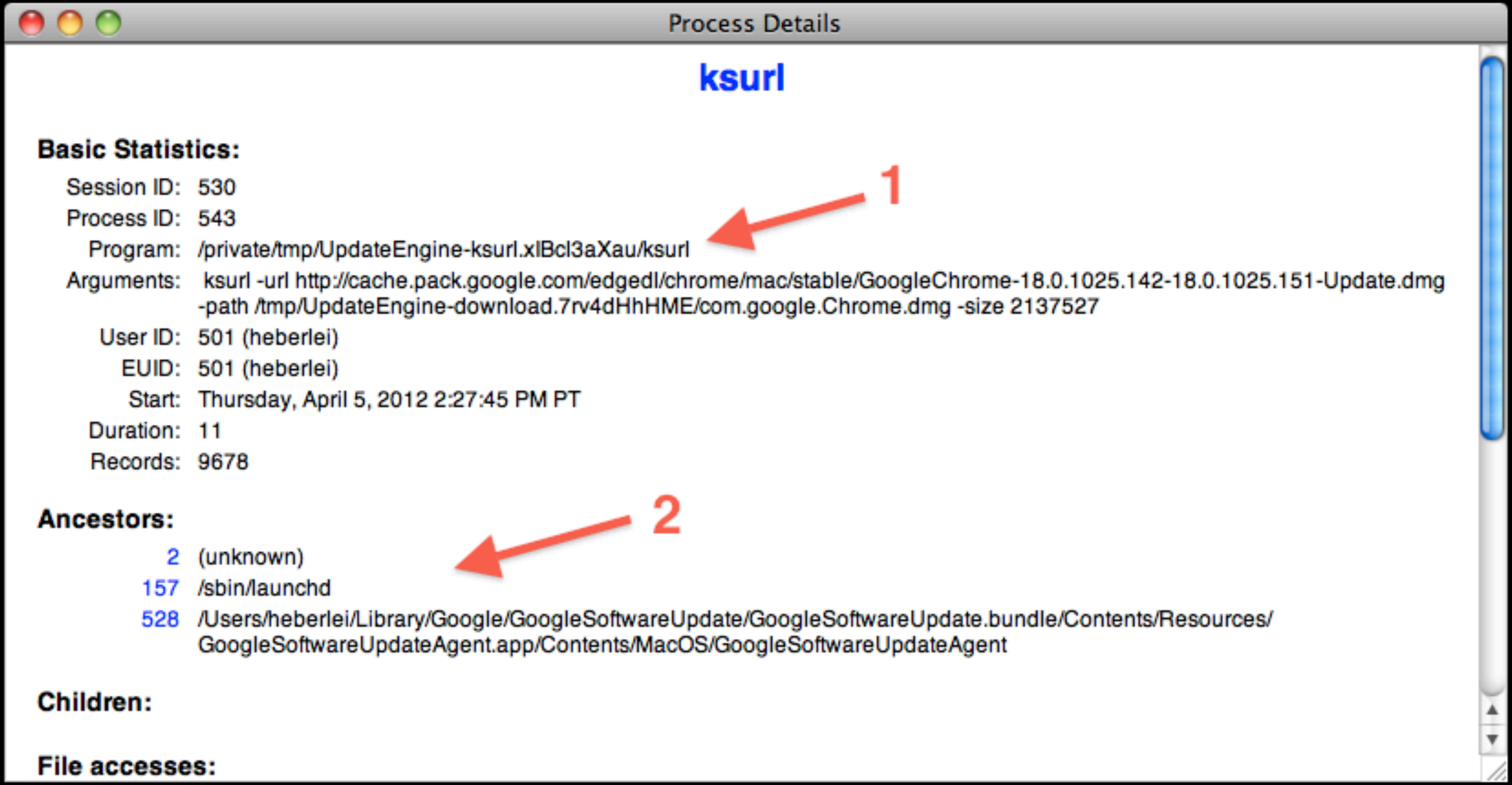


Filters:

Count	Warning	Description
2	1	Any Connections
5	1	Google Update
1	1	Apple Update
1	1	Apple Install
1	1	Applications Executable Change

Matches:

Session	User	Program
530	heberlei	ksurl -url http://cache.pack.google.com/edgedl/chrome/mac/stable/GoogleChrome-18.0.1025.14...
530	heberlei	ksurl -url http://cache.pack.google.com/edgedl/chrome/mac/stable/GoogleChrome-18.0.1025.14...



ksurl

Basic Statistics:

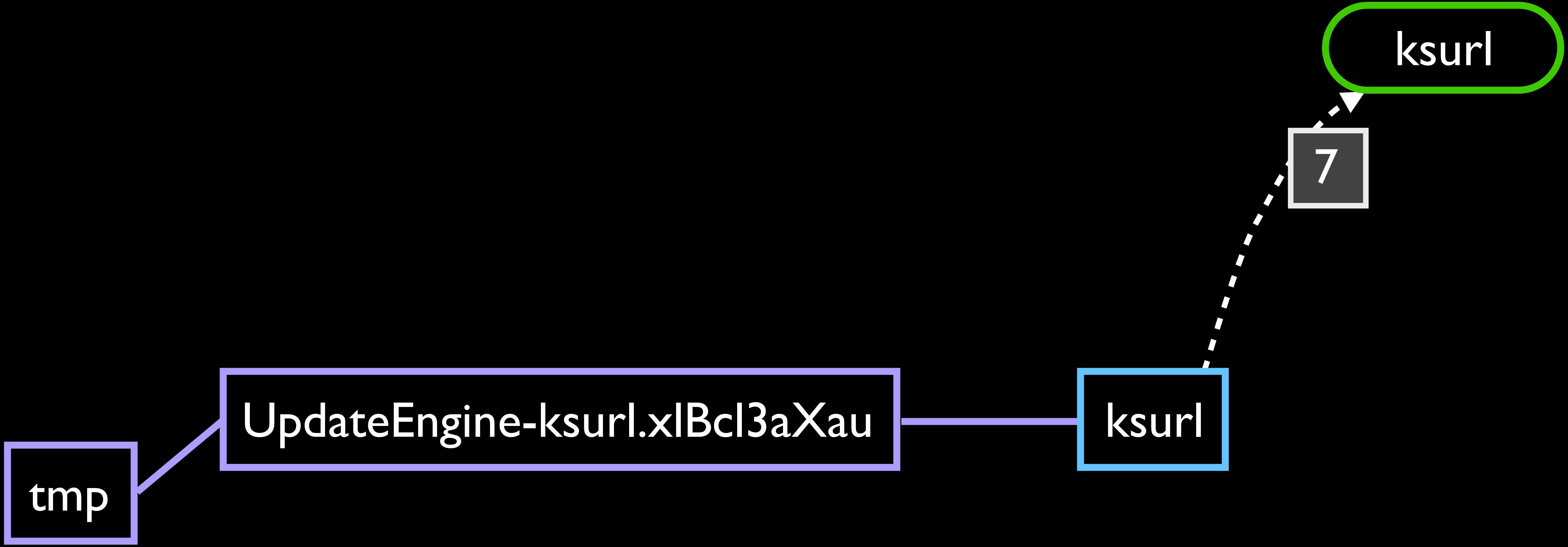
Session ID:	530
Process ID:	543
Program:	/private/tmp/UpdateEngine-ksurl.xlBcl3aXau/ksurl
Arguments:	ksurl -url http://cache.pack.google.com/edgedl/chrome/mac/stable/GoogleChrome-18.0.1025.142-18.0.1025.151-Update.dmg -path /tmp/UpdateEngine-download.7rv4dHhHME/com.google.Chrome.dmg -size 2137527
User ID:	501 (heberlei)
EUID:	501 (heberlei)
Start:	Thursday, April 5, 2012 2:27:45 PM PT
Duration:	11
Records:	9678

Ancestors:

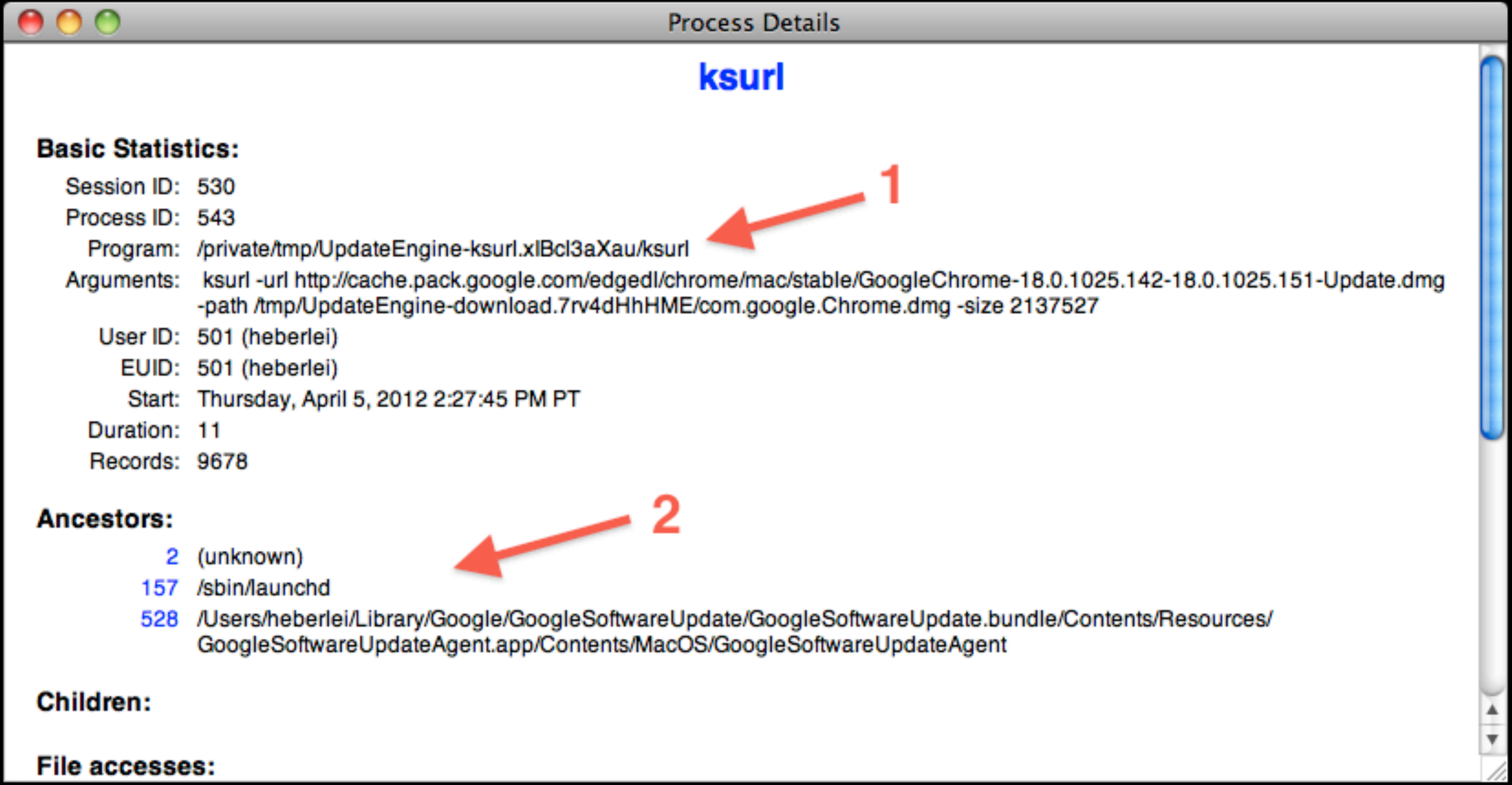
2	(unknown)
157	/sbin/launchd
528	/Users/heberlei/Library/Google/GoogleSoftwareUpdate/GoogleSoftwareUpdate.bundle/Contents/Resources/GoogleSoftwareUpdateAgent.app/Contents/MacOS/GoogleSoftwareUpdateAgent

Children:

File accesses:



ksurl
7
UpdateEngine-ksurl.xlBcl3aXau
ksurl
tmp



ksurl

Basic Statistics:

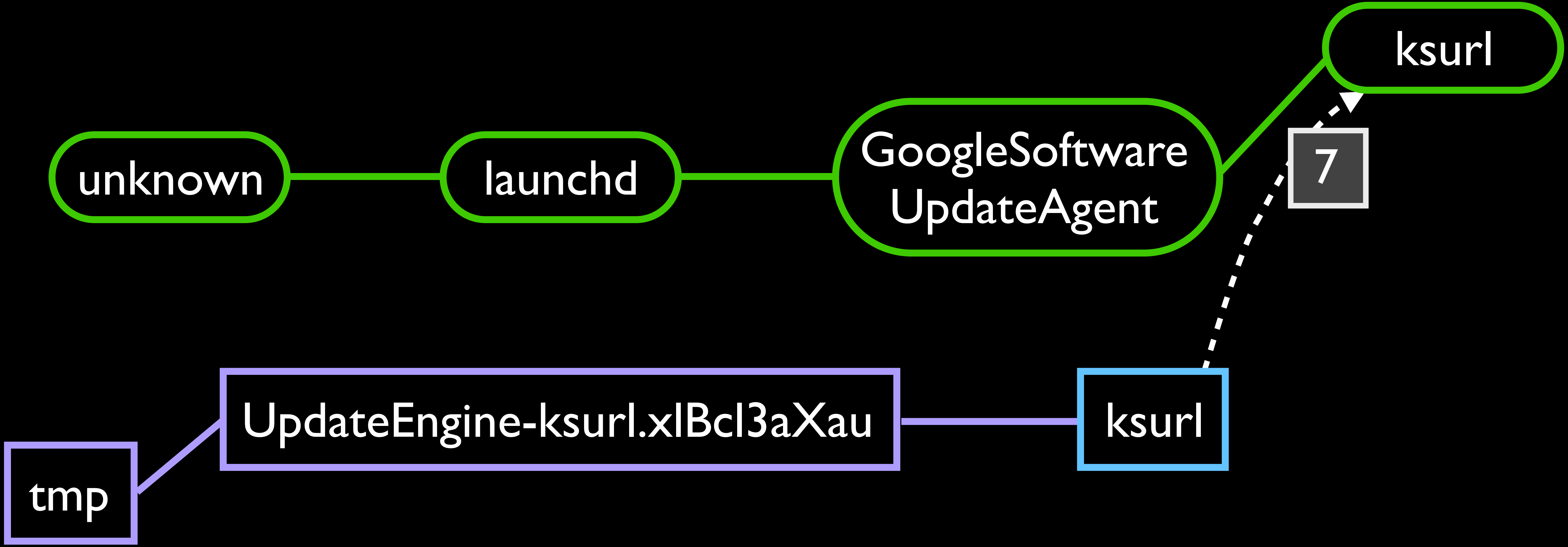
```
   Session ID:  530
   Process ID:  543
      Program:  /private/tmp/UpdateEngine-ksurl.xlBcl3aXau/ksurl
    Arguments:   ksurl -url http://cache.pack.google.com/edgedl/chrome/mac/stable/GoogleChrome-18.0.1025.142-18.0.1025.151-Update.dmg
                -path /tmp/UpdateEngine-download.7rv4dHhHME/com.google.Chrome.dmg -size 2137527
      User ID:  501 (heberlei)
         EUID:  501 (heberlei)
        Start:  Thursday, April 5, 2012 2:27:45 PM PT
     Duration:  11
      Records:  9678
```

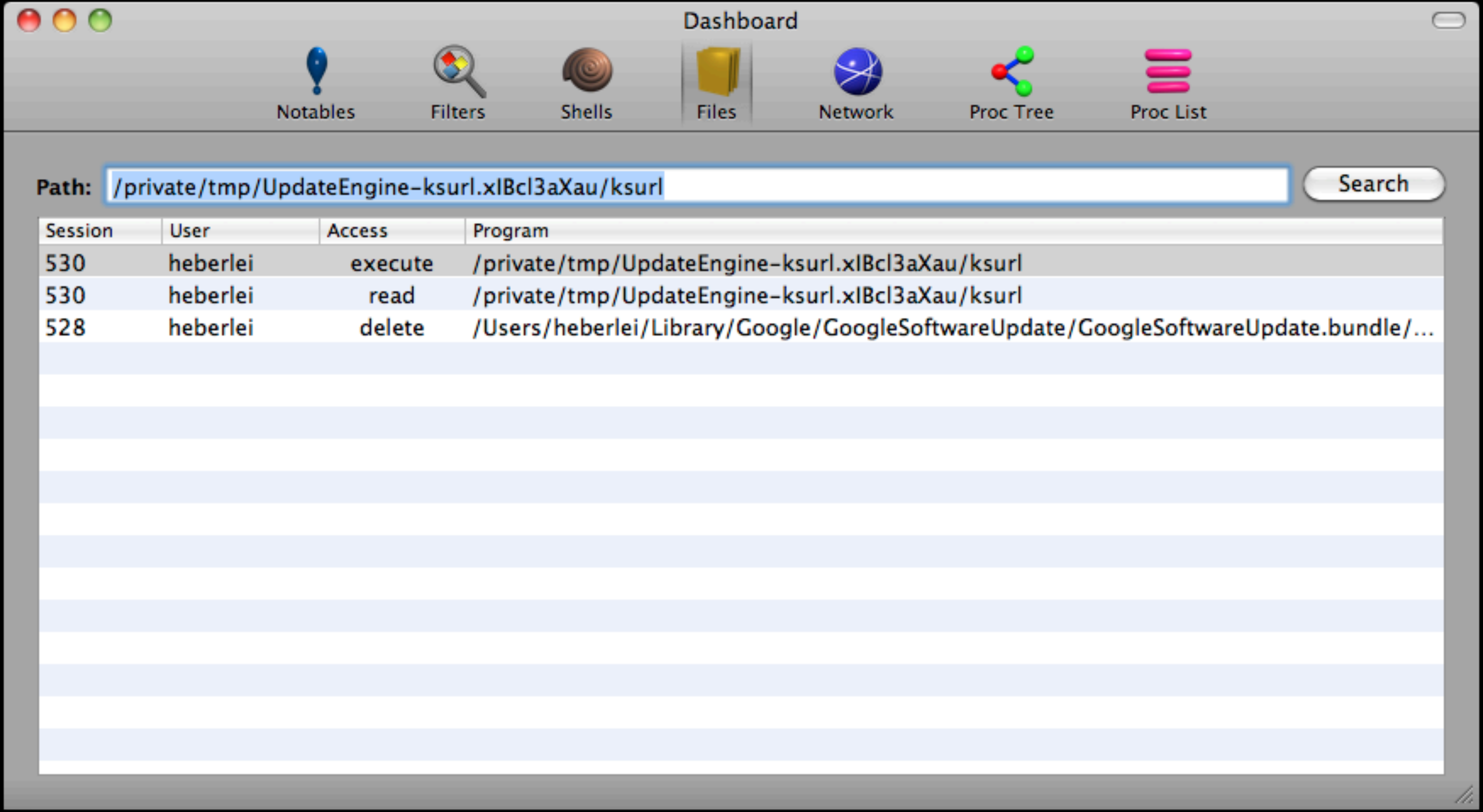
Ancestors:

```
            2   (unknown)
          157   /sbin/launchd
          528   /Users/heberlei/Library/Google/GoogleSoftwareUpdate/GoogleSoftwareUpdate.bundle/Contents/Resources/
                GoogleSoftwareUpdateAgent.app/Contents/MacOS/GoogleSoftwareUpdateAgent
```

Children:

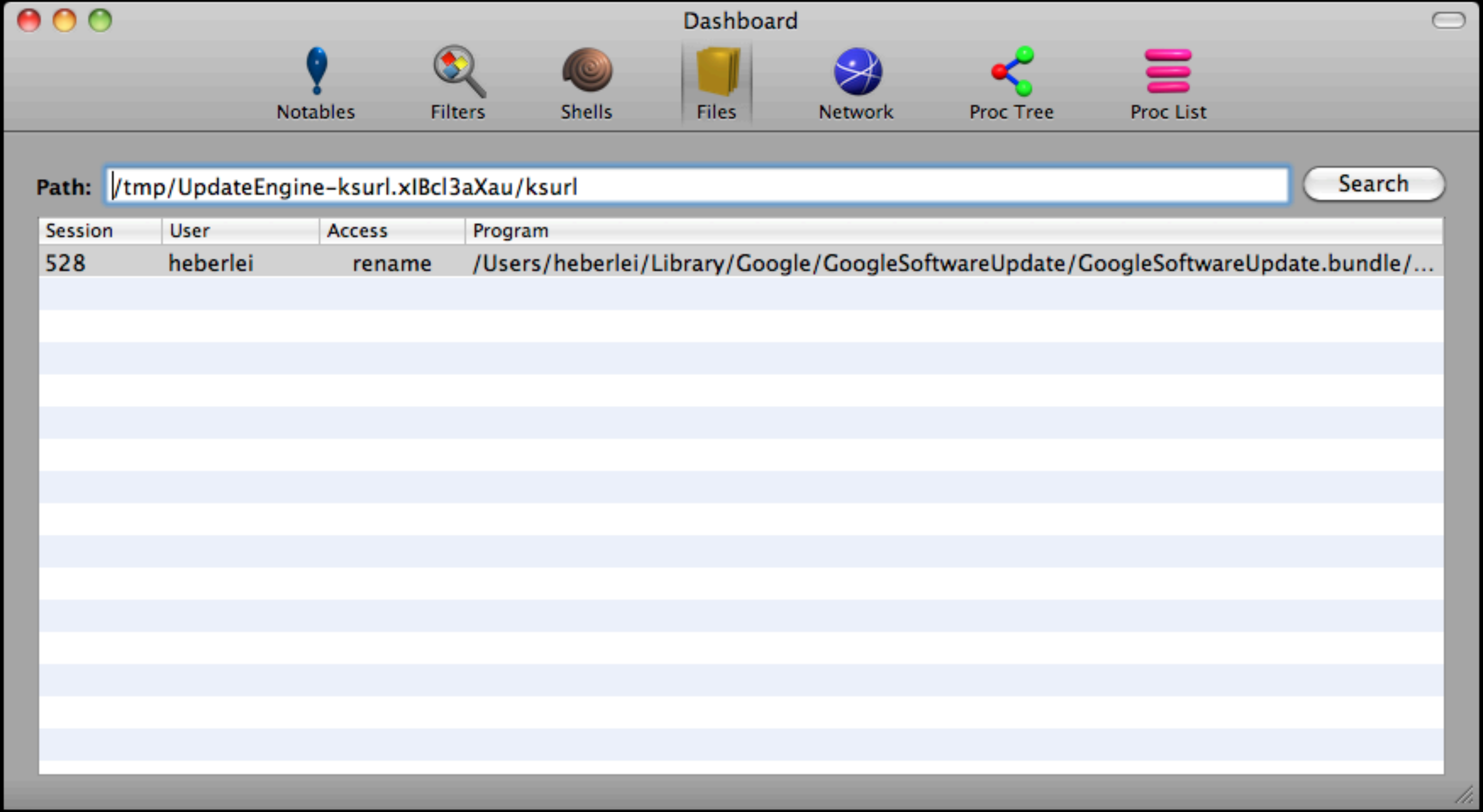
File accesses:


ksurl
unknown
launchd
GoogleSoftware UpdateAgent
7
tmp
UpdateEngine-ksurl.xlBcl3aXau
ksurl



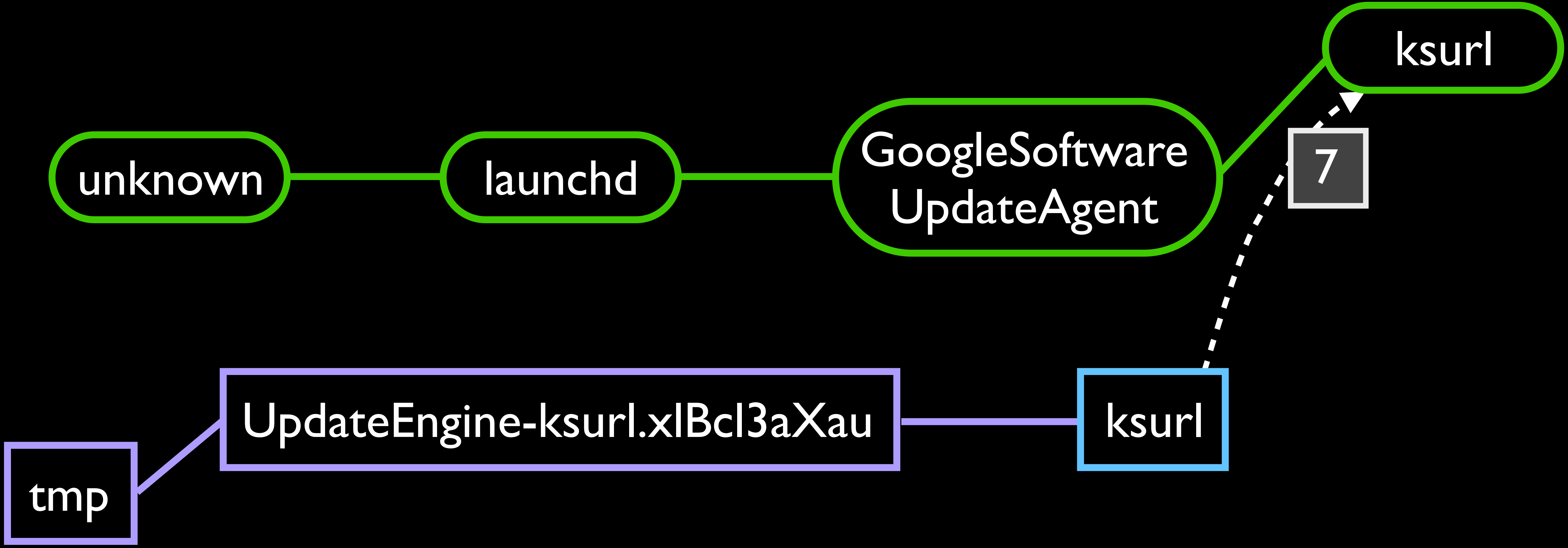
Path: /private/tmp/UpdateEngine-ksurl.xIBcl3aXau/ksurl

Session	User	Access	Program
530	heberlei	execute	/private/tmp/UpdateEngine-ksurl.xIBcl3aXau/ksurl
530	heberlei	read	/private/tmp/UpdateEngine-ksurl.xIBcl3aXau/ksurl
528	heberlei	delete	/Users/heberlei/Library/Google/GoogleSoftwareUpdate/GoogleSoftwareUpdate.bundle/...



Path: /tmp/UpdateEngine-ksurl.xlBcl3aXau/ksurl

Session	User	Access	Program
528	heberlei	rename	/Users/heberlei/Library/Google/GoogleSoftwareUpdate/GoogleSoftwareUpdate.bundle/...



unknown

launchd

GoogleSoftware UpdateAgent

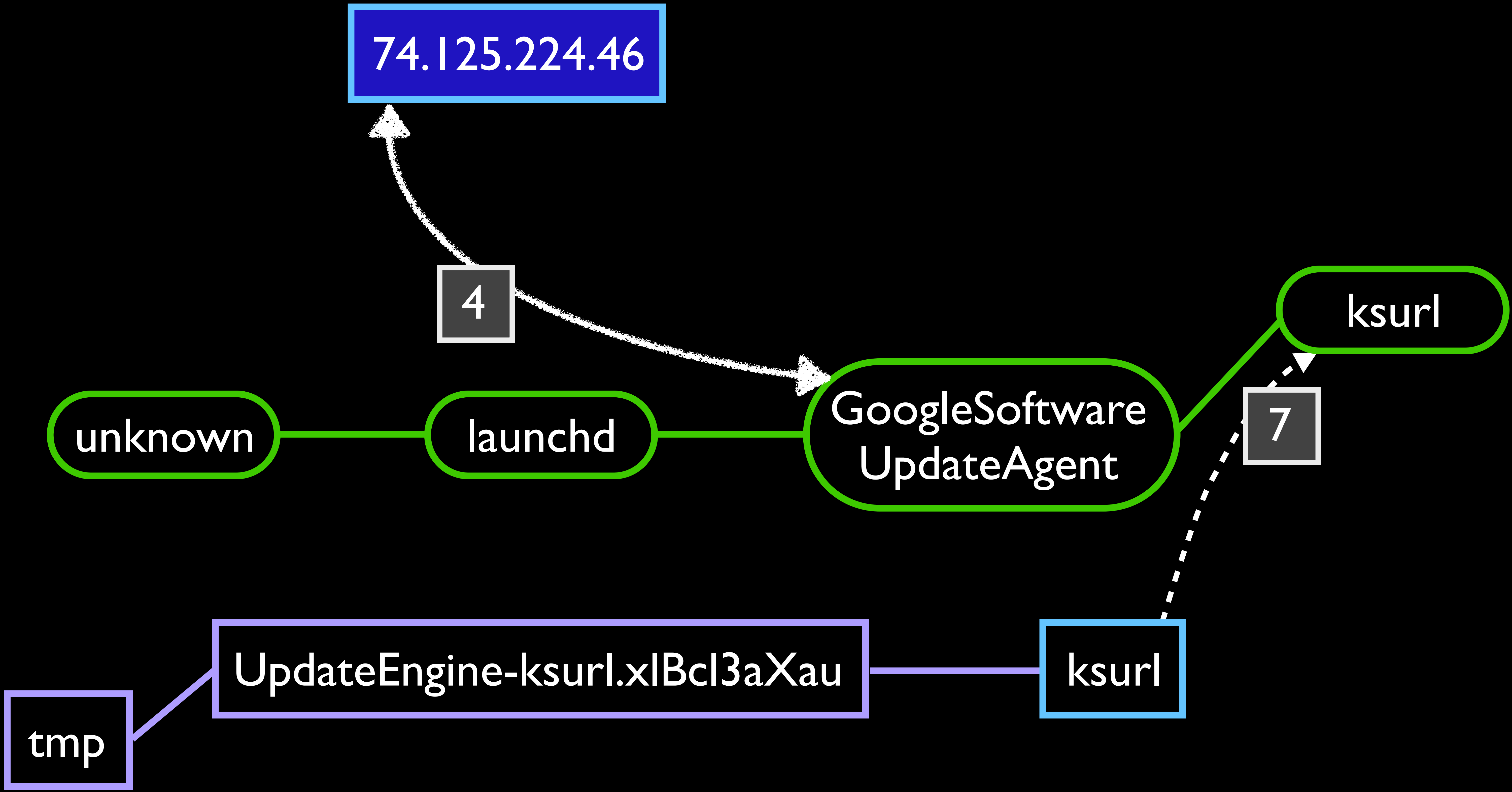
ksurl

7

tmp

UpdateEngine-ksurl.xlBcl3aXau

ksurl



74.125.224.46

4

ksurl

unknown

launchd

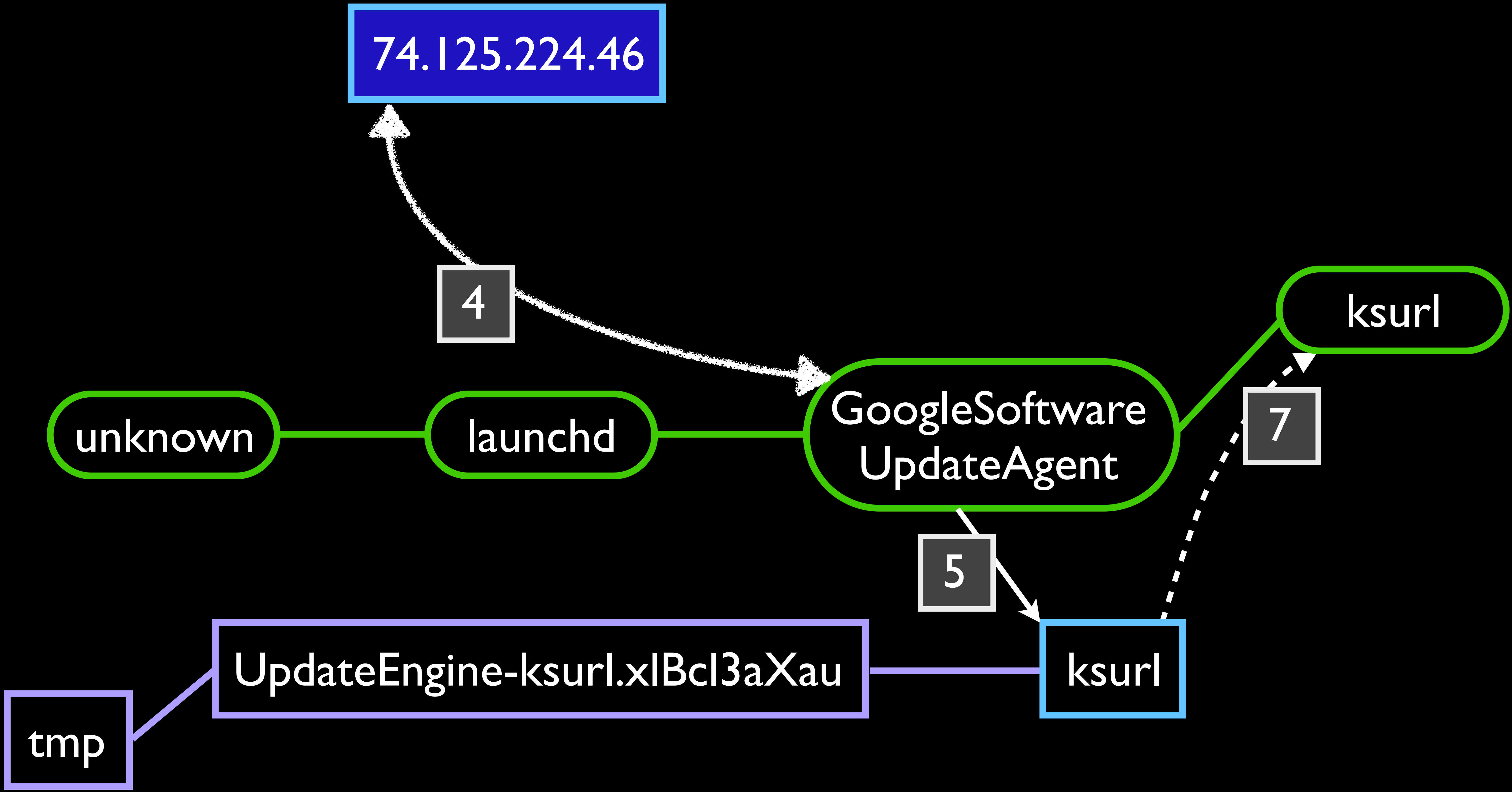
GoogleSoftware UpdateAgent

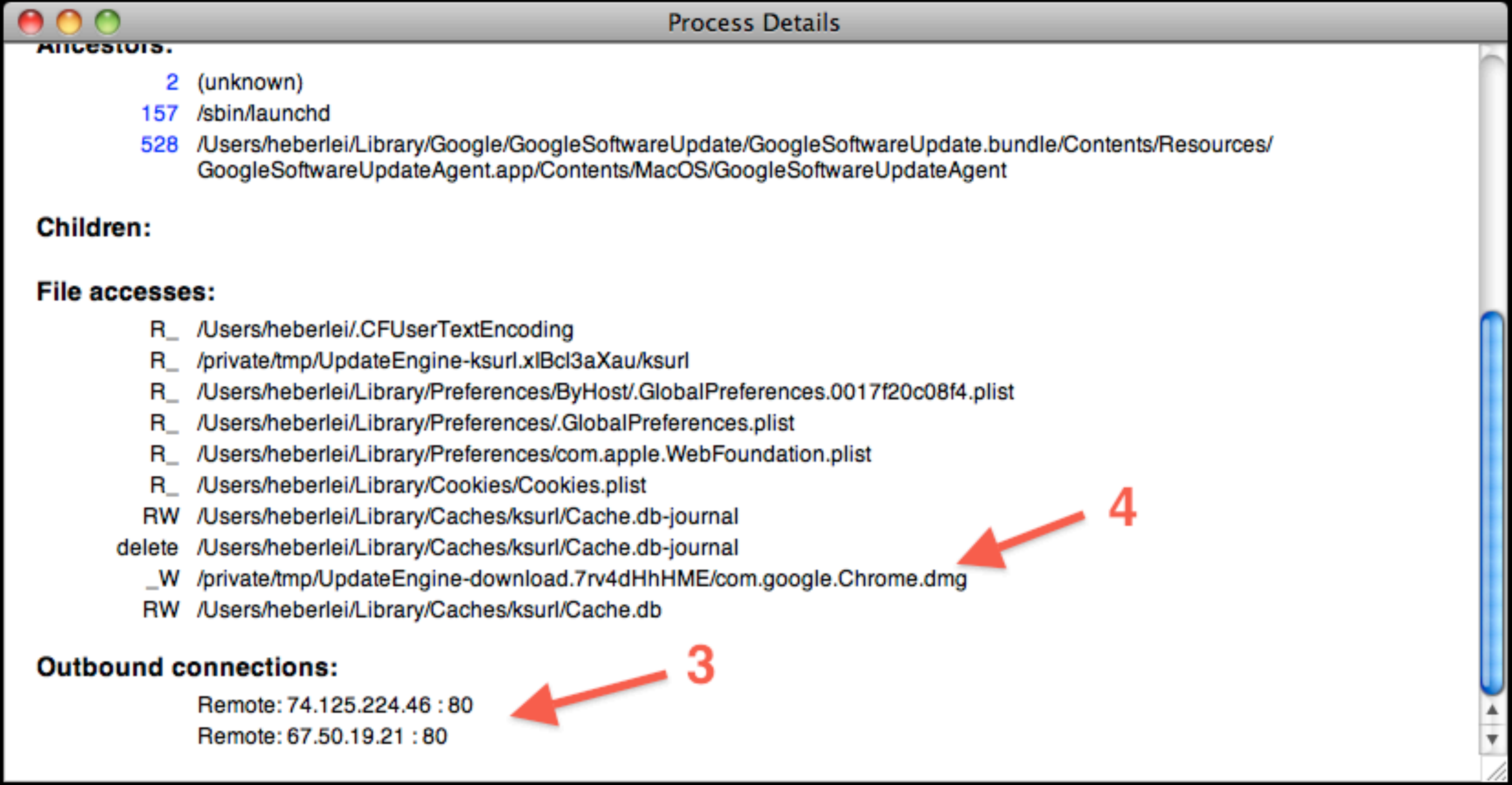
7

tmp

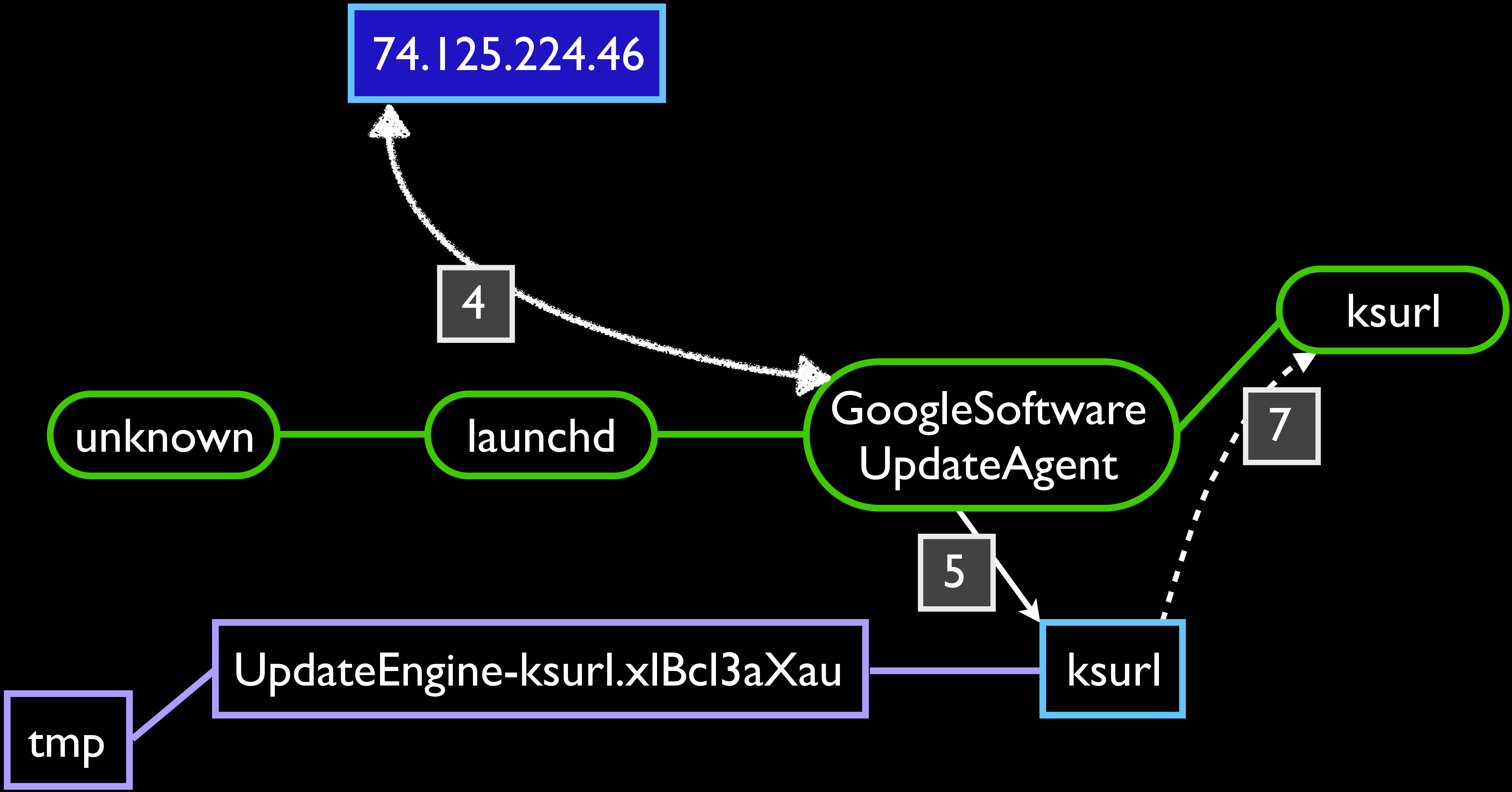
UpdateEngine-ksurl.xlBcl3aXau

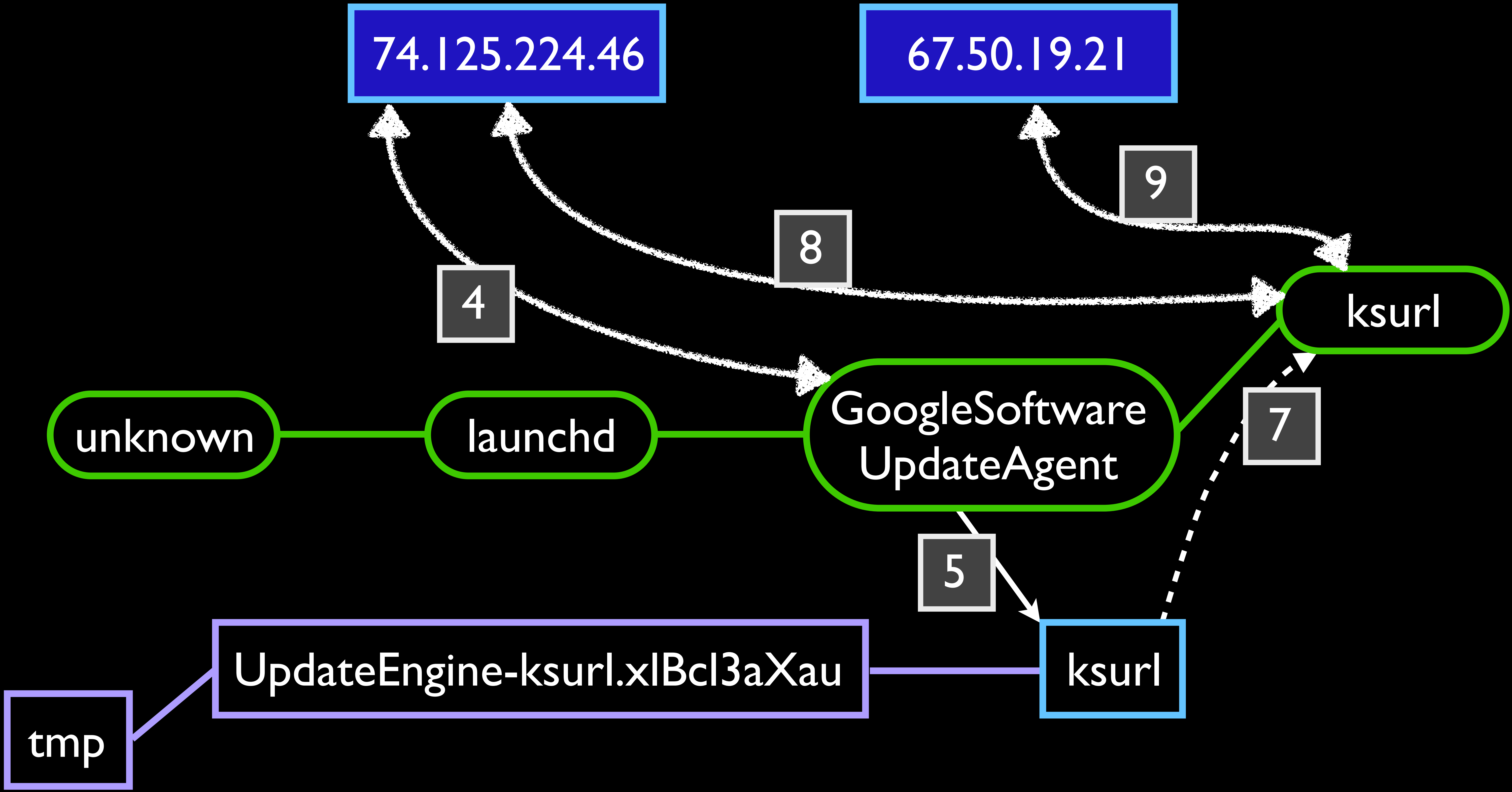
ksurl


74.125.224.46
4
ksurl
unknown
launchd
GoogleSoftware
UpdateAgent
7
5
UpdateEngine-ksurl.xlBcl3aXau
ksurl
tmp



```
Ancestors:
              2  (unknown)
            157  /sbin/launchd
            528  /Users/heberlei/Library/Google/GoogleSoftwareUpdate/GoogleSoftwareUpdate.bundle/Contents/Resources/
                 GoogleSoftwareUpdateAgent.app/Contents/MacOS/GoogleSoftwareUpdateAgent

Children:

File accesses:
             R_  /Users/heberlei/.CFUserTextEncoding
             R_  /private/tmp/UpdateEngine-ksurl.xlBcl3aXau/ksurl
             R_  /Users/heberlei/Library/Preferences/ByHost/.GlobalPreferences.0017f20c08f4.plist
             R_  /Users/heberlei/Library/Preferences/.GlobalPreferences.plist
             R_  /Users/heberlei/Library/Preferences/com.apple.WebFoundation.plist
             R_  /Users/heberlei/Library/Cookies/Cookies.plist
             RW  /Users/heberlei/Library/Caches/ksurl/Cache.db-journal
         delete  /Users/heberlei/Library/Caches/ksurl/Cache.db-journal
             _W  /private/tmp/UpdateEngine-download.7rv4dHhHME/com.google.Chrome.dmg
             RW  /Users/heberlei/Library/Caches/ksurl/Cache.db

Outbound connections:
                 Remote: 74.125.224.46 : 80
                 Remote: 67.50.19.21 : 80
```


74.125.224.46
4
ksurl
unknown
launchd
GoogleSoftware
UpdateAgent
7
5
UpdateEngine-ksurl.xlBcl3aXau
ksurl
tmp



74.125.224.46

67.50.19.21

9

8

4

ksurl

GoogleSoftware UpdateAgent

7

unknown

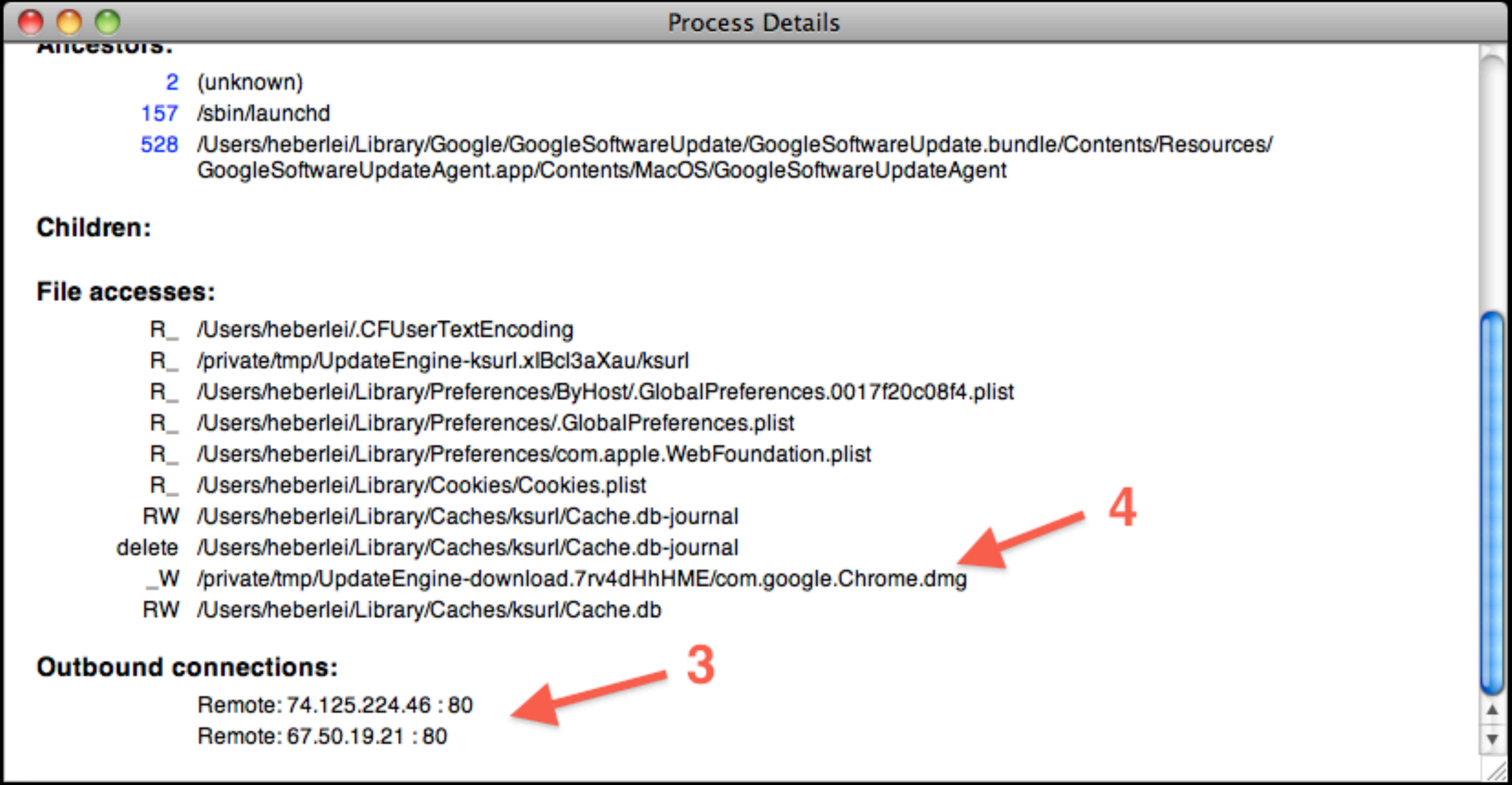
launchd

5

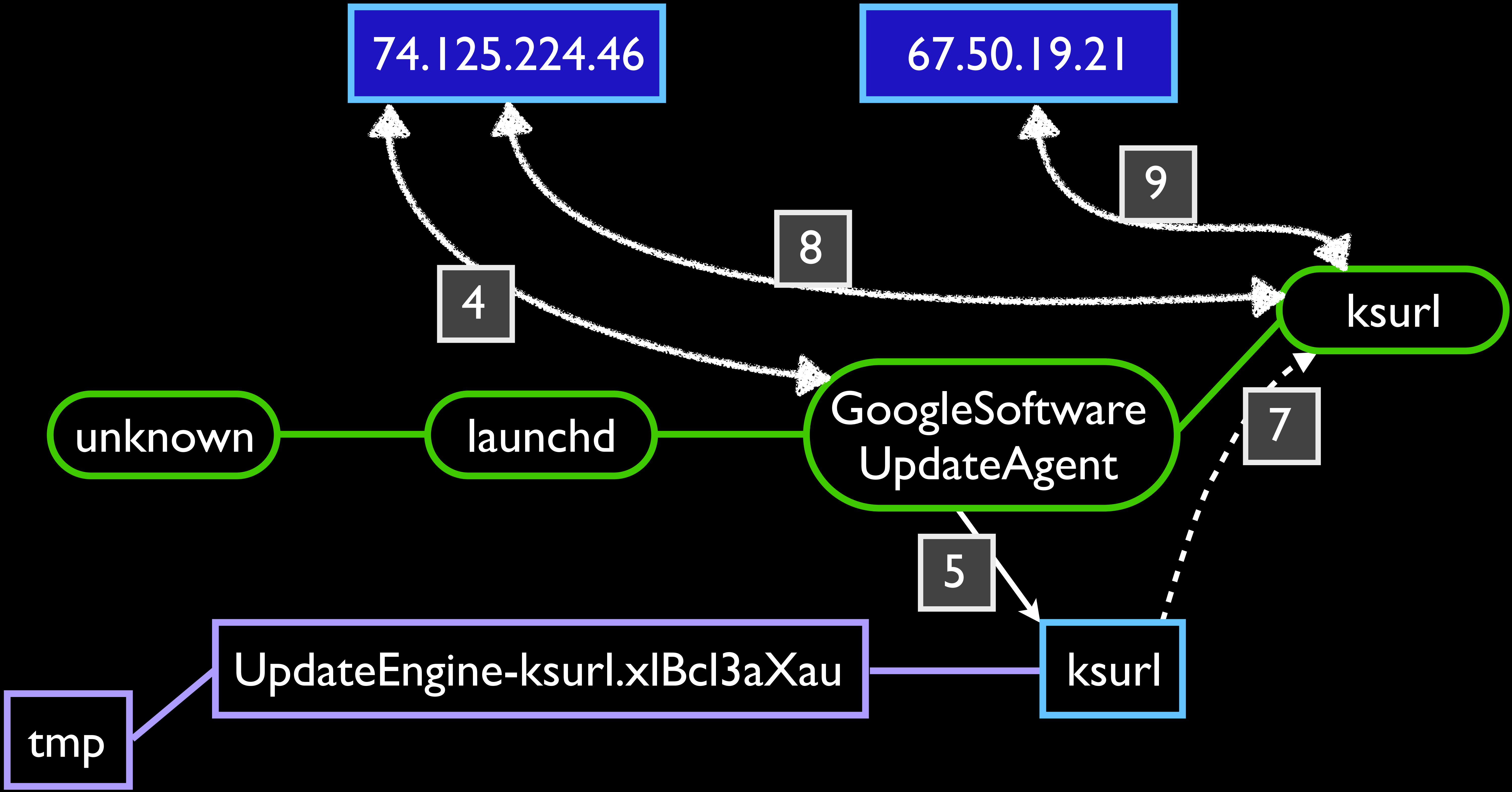
UpdateEngine-ksurl.xlBcl3aXau

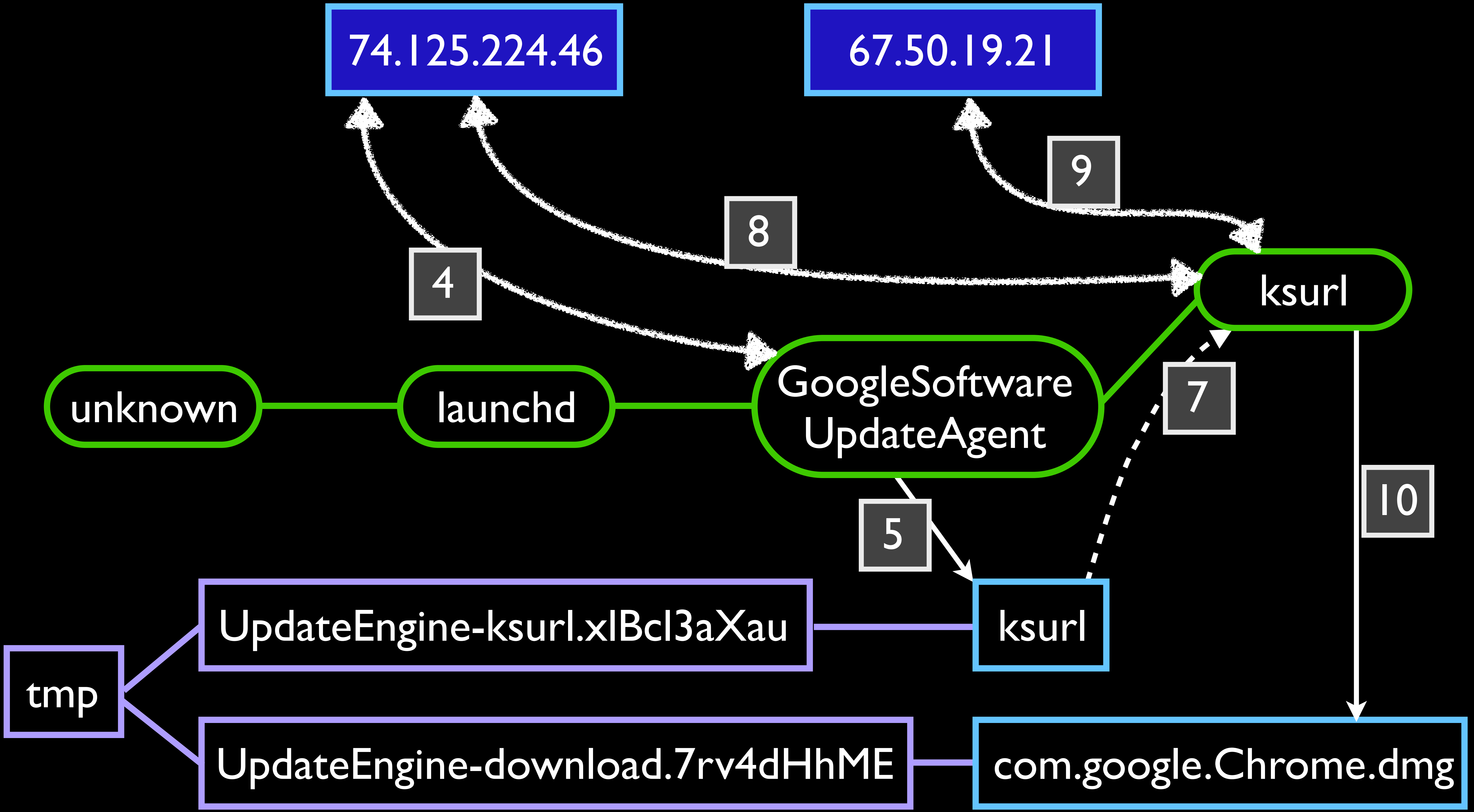
ksurl

tmp



```
Ancestors:
        2  (unknown)
      157  /sbin/launchd
      528  /Users/heberlei/Library/Google/GoogleSoftwareUpdate/GoogleSoftwareUpdate.bundle/Contents/Resources/
           GoogleSoftwareUpdateAgent.app/Contents/MacOS/GoogleSoftwareUpdateAgent

Children:

File accesses:
       R_  /Users/heberlei/.CFUserTextEncoding
       R_  /private/tmp/UpdateEngine-ksurl.xlBcl3aXau/ksurl
       R_  /Users/heberlei/Library/Preferences/ByHost/.GlobalPreferences.0017f20c08f4.plist
       R_  /Users/heberlei/Library/Preferences/.GlobalPreferences.plist
       R_  /Users/heberlei/Library/Preferences/com.apple.WebFoundation.plist
       R_  /Users/heberlei/Library/Cookies/Cookies.plist
       RW  /Users/heberlei/Library/Caches/ksurl/Cache.db-journal
   delete  /Users/heberlei/Library/Caches/ksurl/Cache.db-journal
       _W  /private/tmp/UpdateEngine-download.7rv4dHhHME/com.google.Chrome.dmg
       RW  /Users/heberlei/Library/Caches/ksurl/Cache.db

Outbound connections:
           Remote: 74.125.224.46 : 80
           Remote: 67.50.19.21 : 80
```


74.125.224.46
67.50.19.21
9
8
4
ksurl
unknown
launchd
GoogleSoftware UpdateAgent
7
5
UpdateEngine-ksurl.xlBcl3aXau
ksurl
tmp



74.125.224.46

67.50.19.21

9

8

ksurl

4

GoogleSoftware UpdateAgent

unknown

launchd

7

10

5

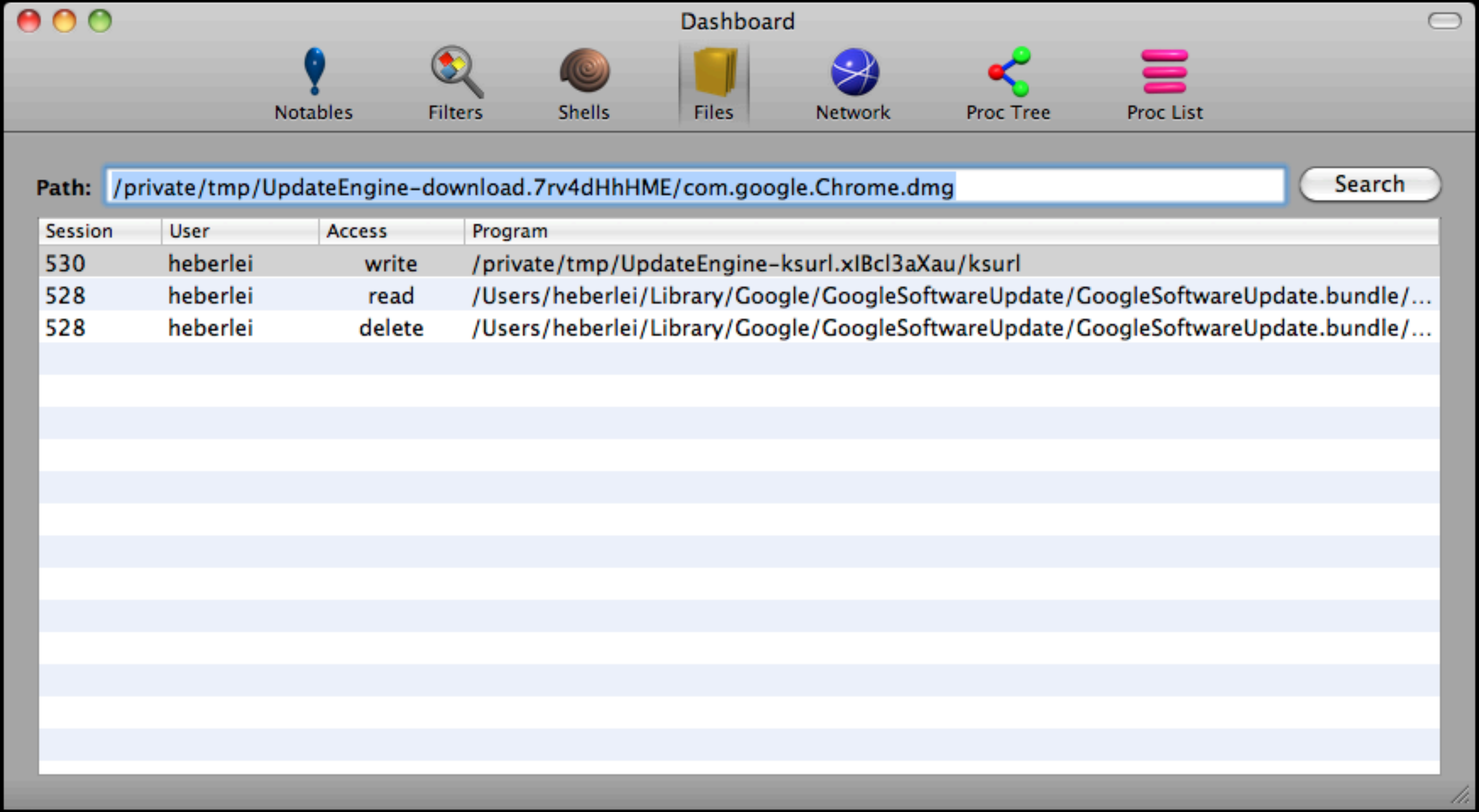
UpdateEngine-ksurl.xlBcl3aXau

ksurl

tmp

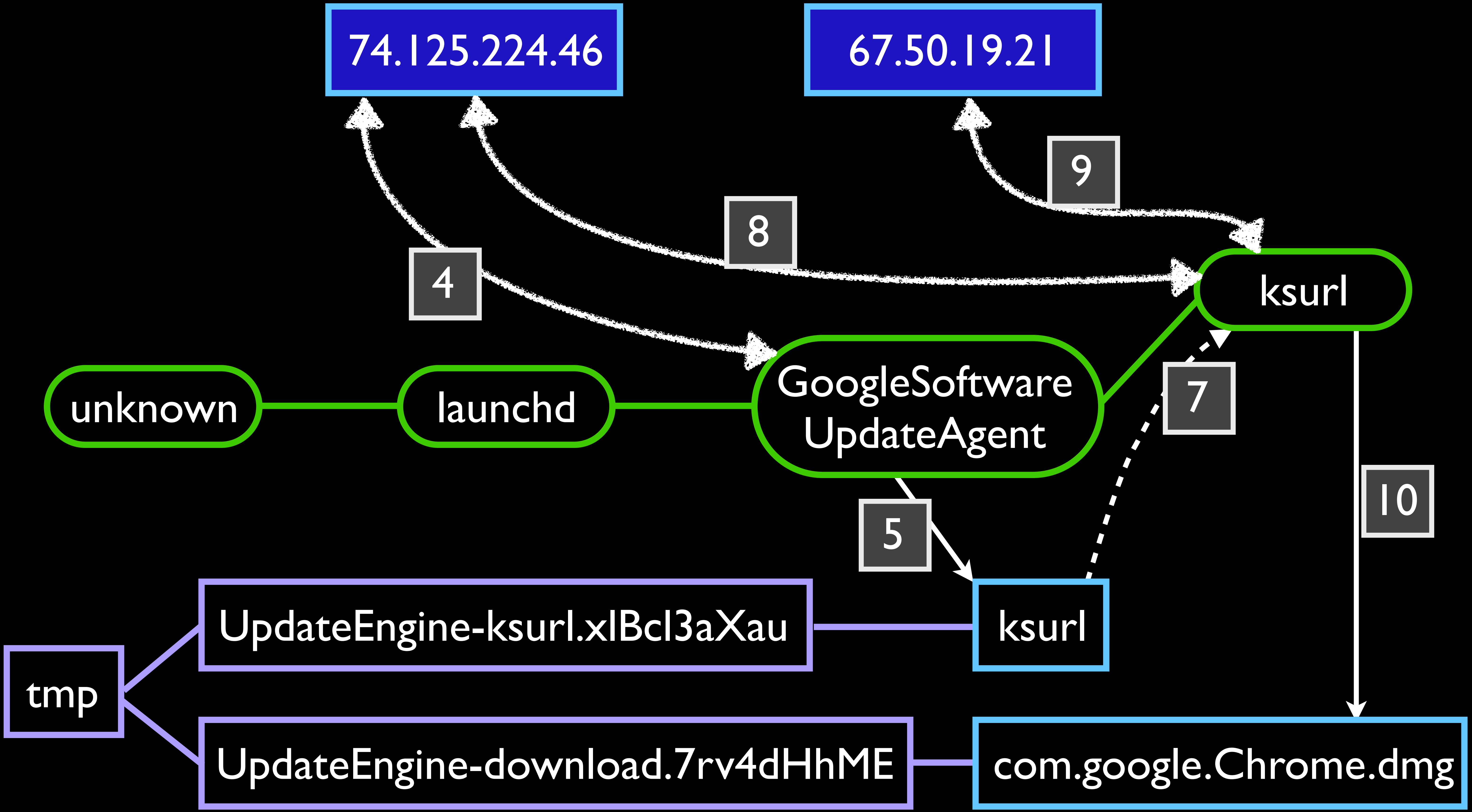
UpdateEngine-download.7rv4dHhME

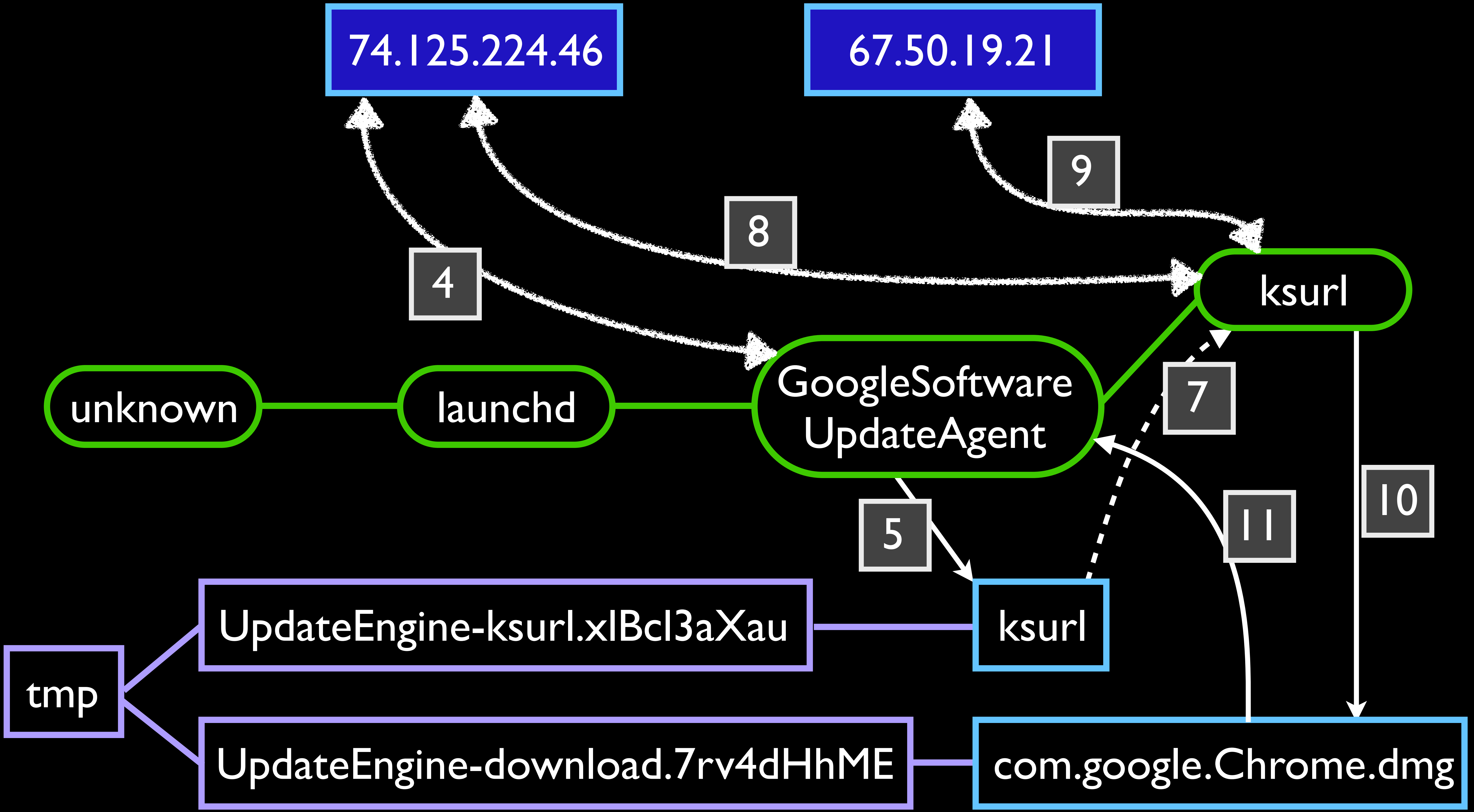
com.google.Chrome.dmg



Path: /private/tmp/UpdateEngine-download.7rv4dHhHME/com.google.Chrome.dmg

Session	User	Access	Program
530	heberlei	write	/private/tmp/UpdateEngine-ksurl.xIBcl3aXau/ksurl
528	heberlei	read	/Users/heberlei/Library/Google/GoogleSoftwareUpdate/GoogleSoftwareUpdate.bundle/...
528	heberlei	delete	/Users/heberlei/Library/Google/GoogleSoftwareUpdate/GoogleSoftwareUpdate.bundle/...


74.125.224.46
67.50.19.21
9
8
4
ksurl
7
unknown
launchd
GoogleSoftware UpdateAgent
5
10
UpdateEngine-ksurl.xIBcl3aXau
ksurl
tmp
UpdateEngine-download.7rv4dHhME
com.google.Chrome.dmg



74.125.224.46

67.50.19.21

9

8

4

ksurl

unknown

launchd

GoogleSoftware
UpdateAgent

7

5

11

10

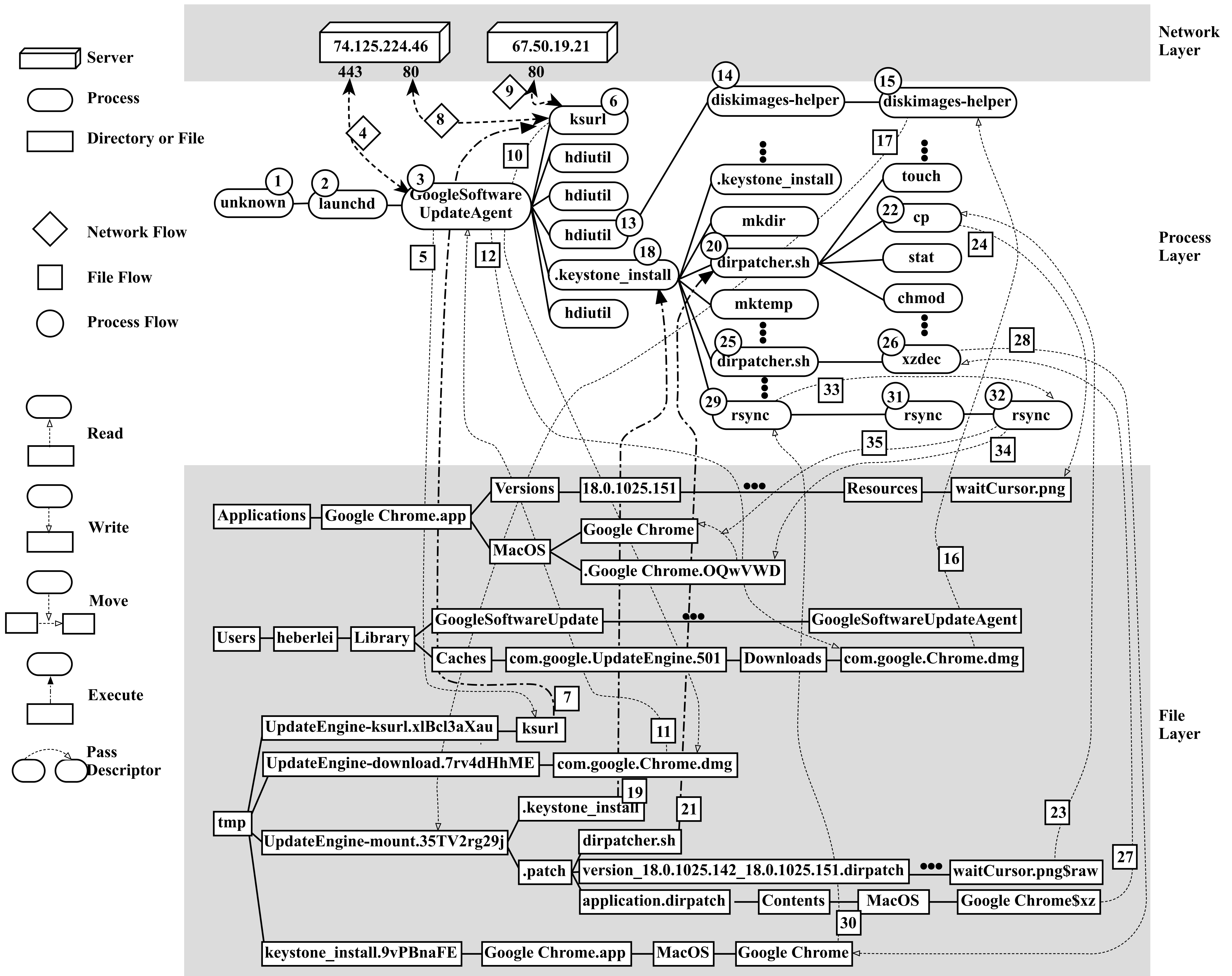
tmp

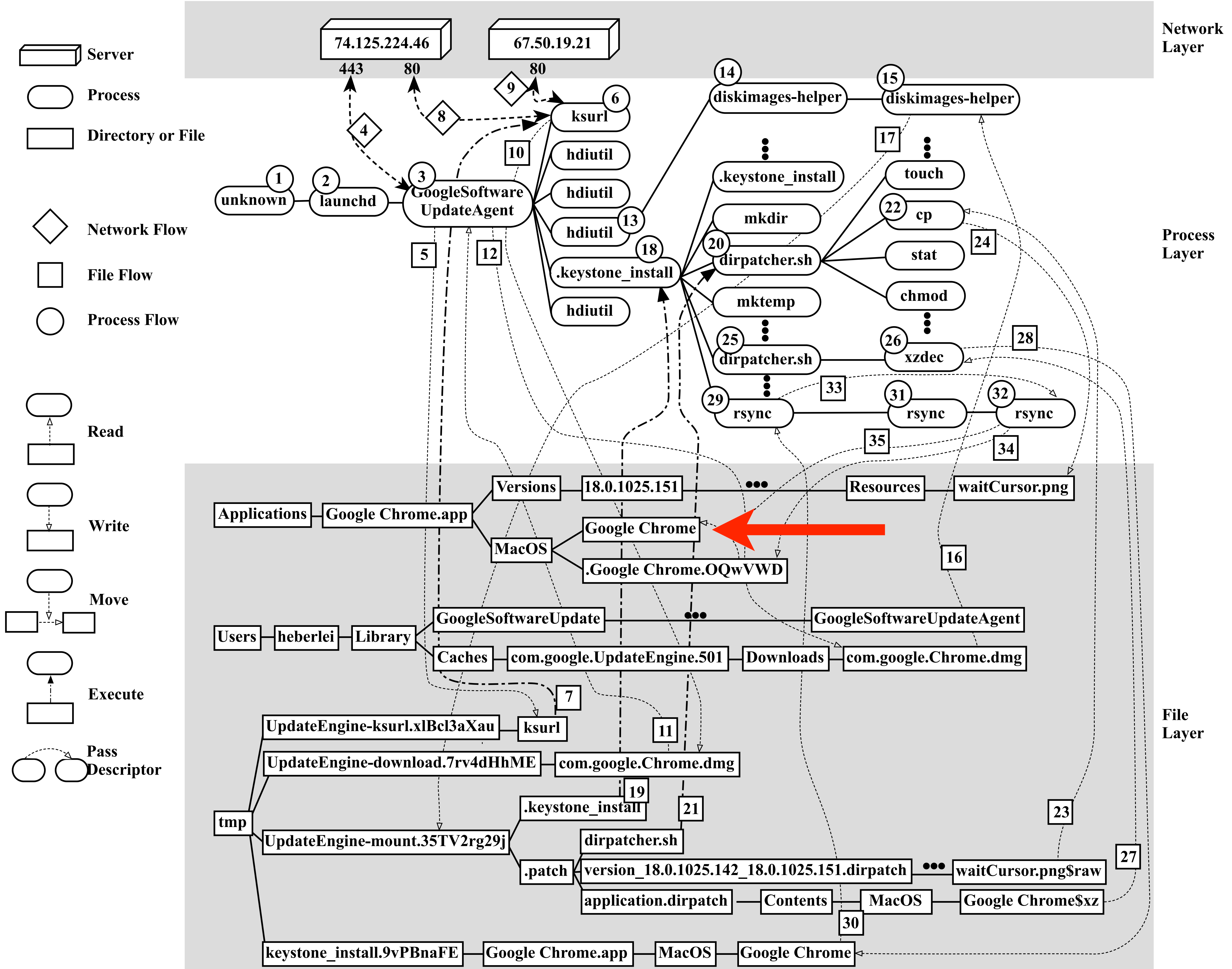
UpdateEngine-ksurl.xlBcl3aXau

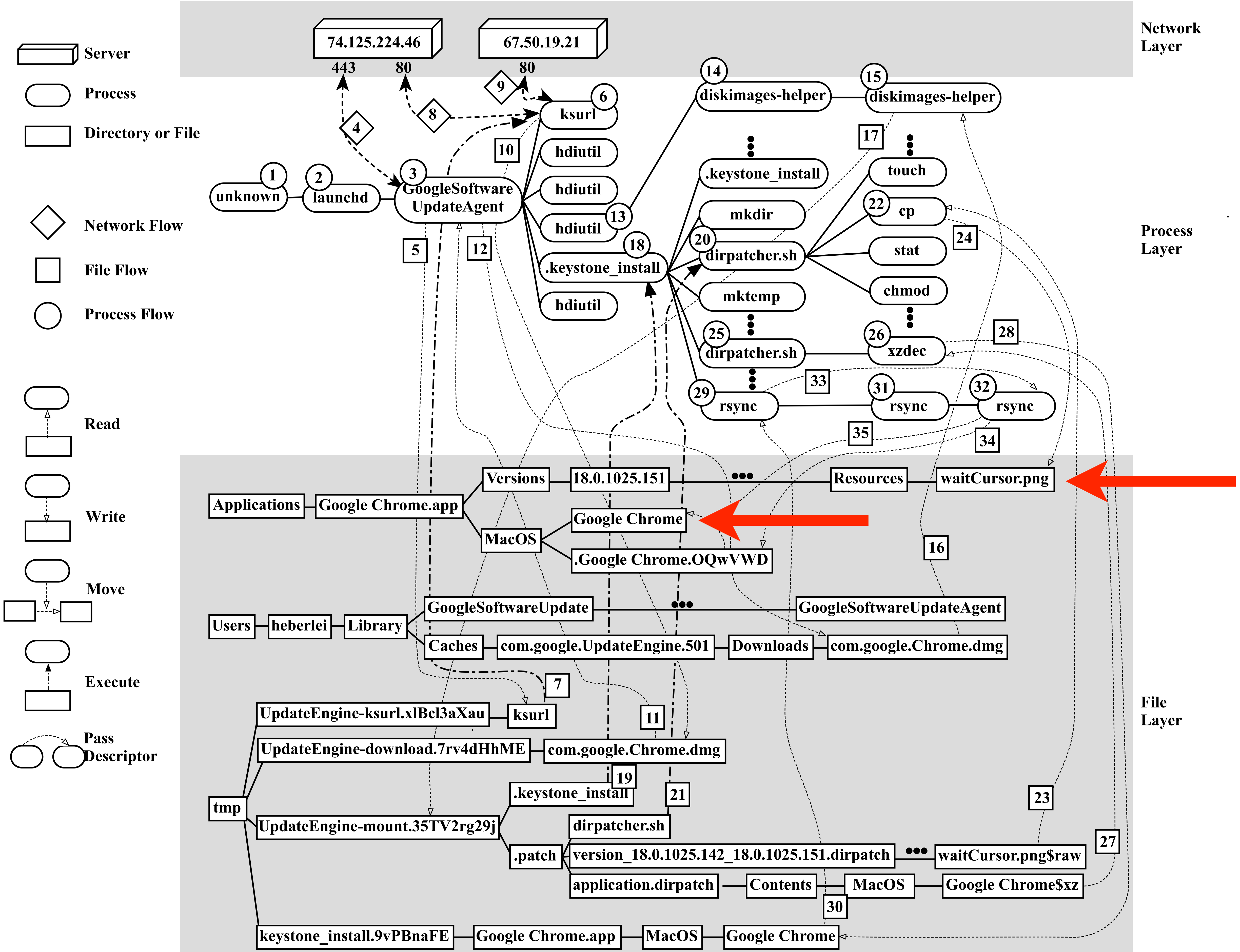
ksurl

UpdateEngine-download.7rv4dHhME

com.google.Chrome.dmg


Server
Process
Directory or File
Network Flow
File Flow
Process Flow
Read
Write
Move
Execute
Pass Descriptor
Network Layer
Process Layer
File Layer
74.125.224.46
443
80
67.50.19.21
80
1
unknown
2
launchd
3
GoogleSoftware UpdateAgent
4
5
6
ksurl
7
8
9
10
hdiutil
hdiutil
hdiutil
13
hdiutil
11
12
18
.keystone_install
14
diskimages-helper
15
diskimages-helper
16
17
.keystone_install
mkdir
20
dirpatcher.sh
mktemp
touch
22
cp
stat
chmod
24
25
dirpatcher.sh
26
xzdec
28
29
rsync
31
rsync
32
rsync
33
34
35
Applications
Google Chrome.app
Versions
18.0.1025.151
Resources
waitCursor.png
MacOS
Google Chrome
.Google Chrome.OQwVWD
Users
heberlei
Library
GoogleSoftwareUpdate
GoogleSoftwareUpdateAgent
Caches
com.google.UpdateEngine.501
Downloads
com.google.Chrome.dmg
tmp
UpdateEngine-ksurl.xlBcl3aXau
ksurl
UpdateEngine-download.7rv4dHhME
com.google.Chrome.dmg
19
UpdateEngine-mount.35TV2rg29j
.keystone_install
21
dirpatcher.sh
.patch
version_18.0.1025.142_18.0.1025.151.dirpatch
waitCursor.png$raw
23
27
application.dirpatch
Contents
MacOS
Google Chrome$xz
30
keystone_install.9vPBnaFE
Google Chrome.app
MacOS
Google Chrome


Server
Process
Directory or File
Network Flow
File Flow
Process Flow
Read
Write
Move
Execute
Pass Descriptor
Network Layer
Process Layer
File Layer
74.125.224.46
443
80
67.50.19.21
80
unknown
launchd
GoogleSoftware UpdateAgent
ksurl
hdiutil
hdiutil
hdiutil
hdiutil
.keystone_install
hdiutil
diskimages-helper
diskimages-helper
.keystone_install
mkdir
dirpatcher.sh
mktemp
dirpatcher.sh
rsync
touch
cp
stat
chmod
xzdec
rsync
rsync
Applications
Google Chrome.app
Versions
18.0.1025.151
Resources
waitCursor.png
MacOS
Google Chrome
.Google Chrome.OQwVWD
Users
heberlei
Library
GoogleSoftwareUpdate
GoogleSoftwareUpdateAgent
Caches
com.google.UpdateEngine.501
Downloads
com.google.Chrome.dmg
tmp
UpdateEngine-ksurl.xlBcl3aXau
ksurl
UpdateEngine-download.7rv4dHhME
com.google.Chrome.dmg
UpdateEngine-mount.35TV2rg29j
.keystone_install
dirpatcher.sh
.patch
version_18.0.1025.142_18.0.1025.151.dirpatch
waitCursor.png$raw
application.dirpatch
Contents
MacOS
Google Chrome$xz
keystone_install.9vPBnaFE
Google Chrome.app
MacOS
Google Chrome
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35



Server

Process

Directory or File

Network Flow

File Flow

Process Flow

Read

Write

Move

Execute

Pass Descriptor

Network Layer

Process Layer

File Layer

74.125.224.46
443
80

67.50.19.21
80

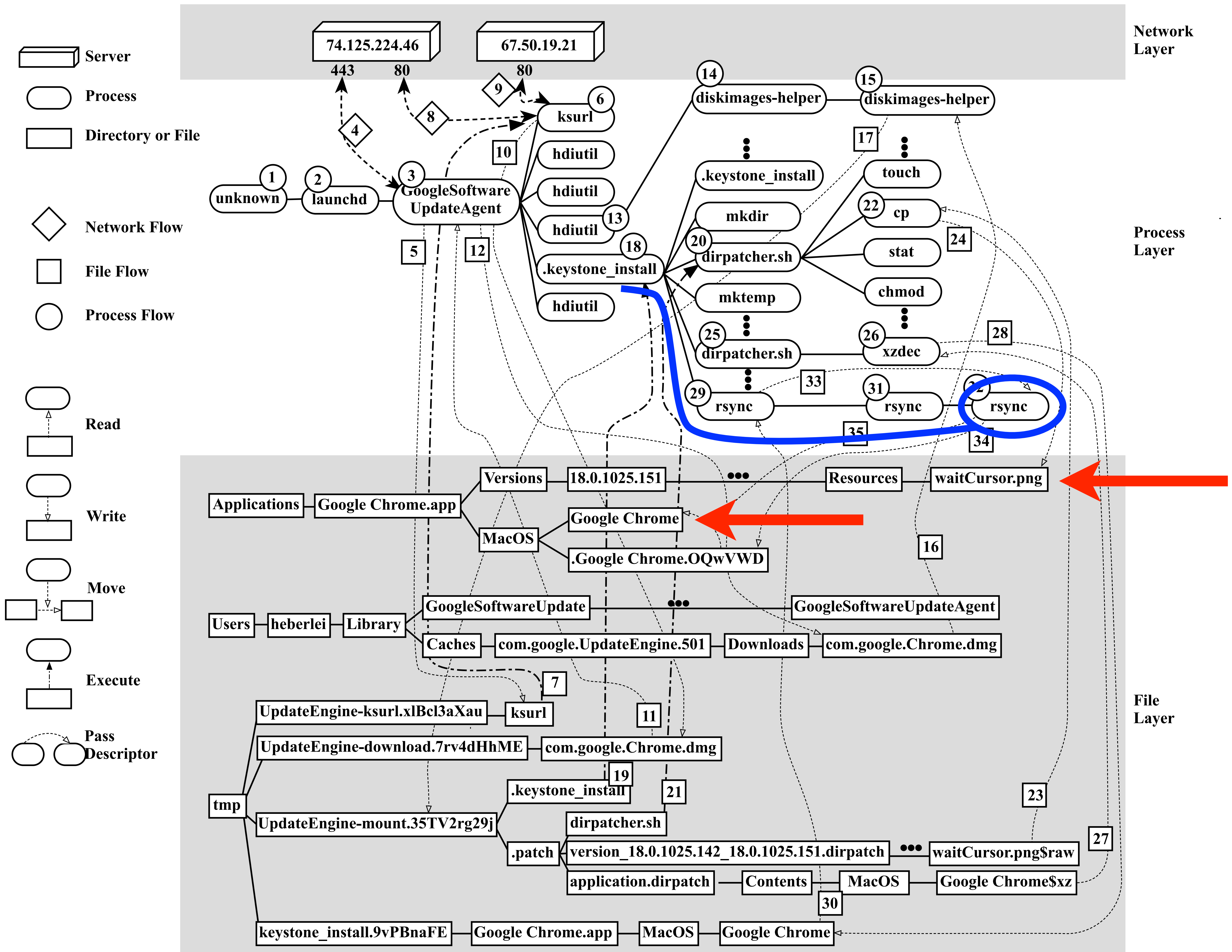
1 unknown
2 launchd
3 GoogleSoftware UpdateAgent
4
5
6 ksurl
7
8
9
10
11
12
13
14 diskimages-helper
15 diskimages-helper
16
17
18 .keystone_install
19
20 dirpatcher.sh
21
22 cp
23
24
25 dirpatcher.sh
26 xzdec
27
28
29 rsync
30
31 rsync
32 rsync
33
34
35

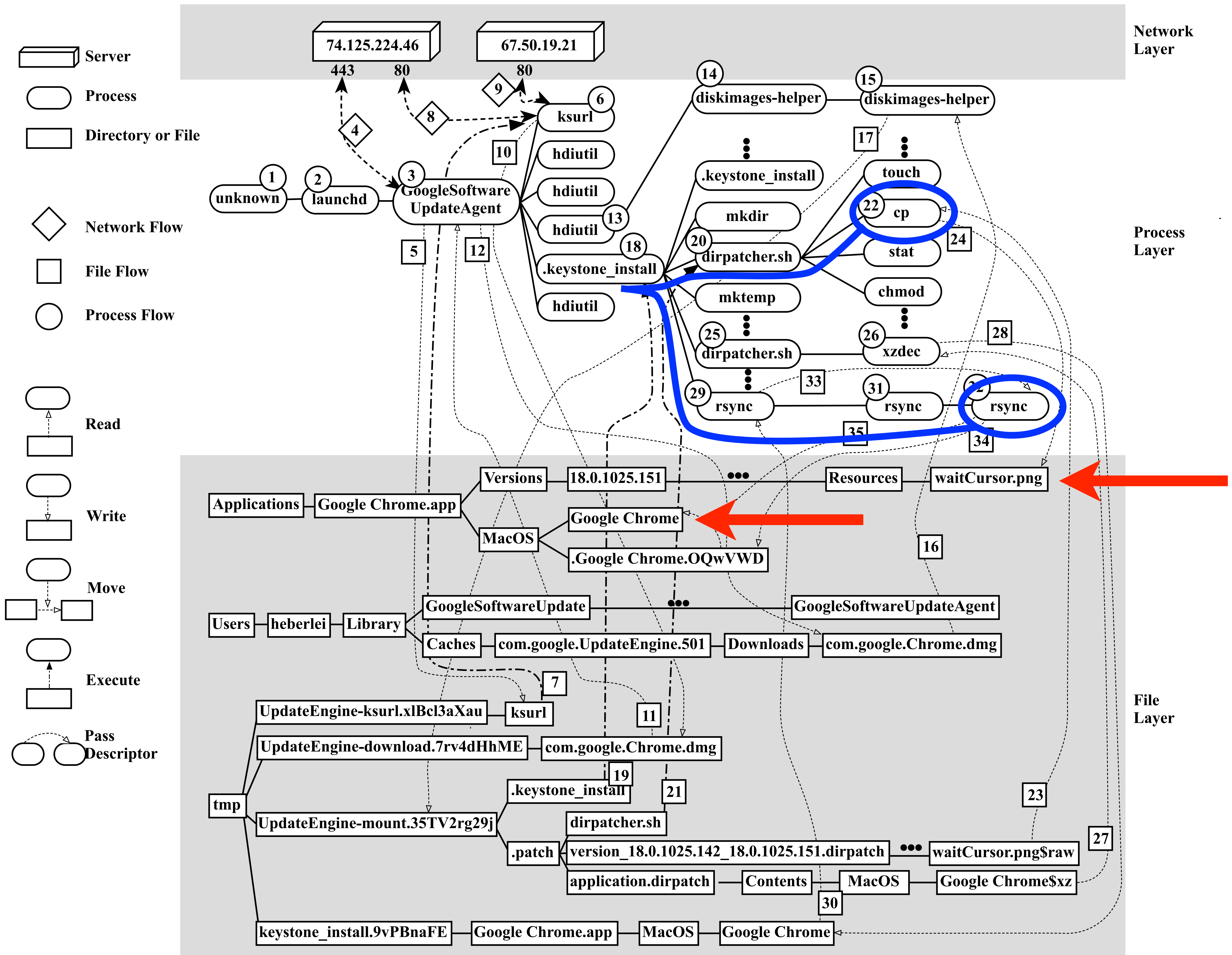
hdiutil
hdiutil
hdiutil
hdiutil
hdiutil
.keystone_install
mkdir
mktemp
touch
stat
chmod

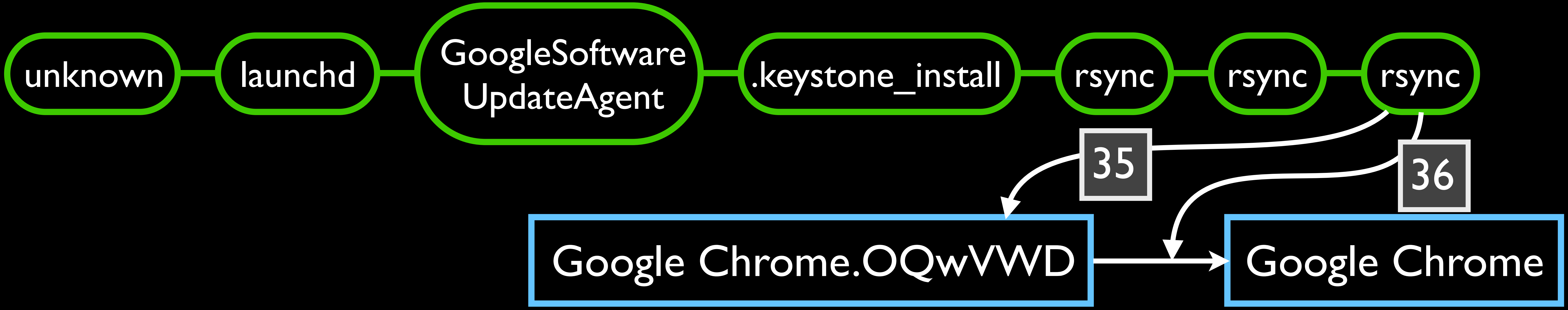
Applications
Google Chrome.app
Versions
18.0.1025.151
Resources
waitCursor.png
MacOS
Google Chrome
.Google Chrome.OQwVWD

Users
heberlei
Library
GoogleSoftwareUpdate
GoogleSoftwareUpdateAgent
Caches
com.google.UpdateEngine.501
Downloads
com.google.Chrome.dmg

tmp
UpdateEngine-ksurl.xlBcl3aXau
ksurl
UpdateEngine-download.7rv4dHhME
com.google.Chrome.dmg
UpdateEngine-mount.35TV2rg29j
.keystone_install
dirpatcher.sh
.patch
version_18.0.1025.142_18.0.1025.151.dirpatch
waitCursor.png$raw
application.dirpatch
Contents
MacOS
Google Chrome$xz
keystone_install.9vPBnaFE
Google Chrome.app
MacOS
Google Chrome

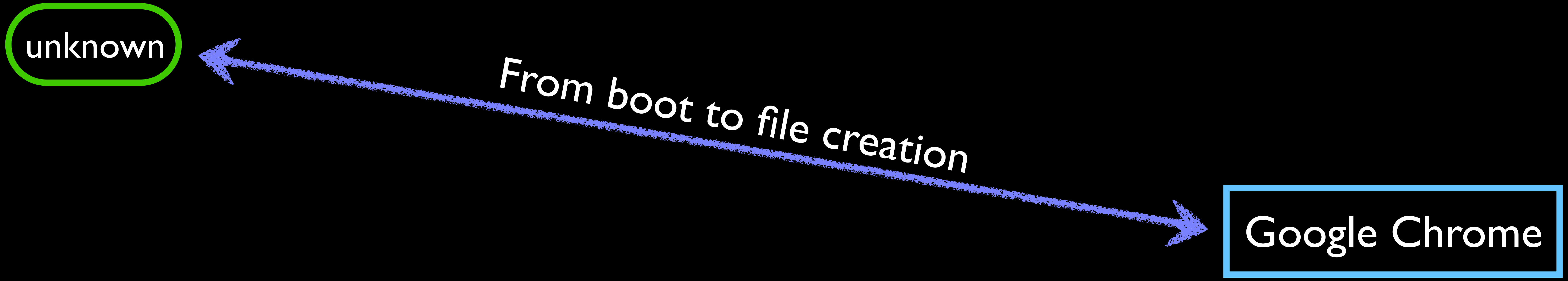

Server
Process
Directory or File
Network Flow
File Flow
Process Flow
Read
Write
Move
Execute
Pass Descriptor
Network Layer
Process Layer
File Layer
74.125.224.46
443
80
67.50.19.21
80
unknown
launchd
GoogleSoftware UpdateAgent
ksurl
hdiutil
hdiutil
hdiutil
.keystone_install
hdiutil
diskimages-helper
diskimages-helper
.keystone_install
mkdir
dirpatcher.sh
mktemp
dirpatcher.sh
rsync
touch
cp
stat
chmod
xzdec
rsync
rsync
Applications
Google Chrome.app
Versions
18.0.1025.151
Resources
waitCursor.png
MacOS
Google Chrome
.Google Chrome.OQwVWD
Users
heberlei
Library
GoogleSoftwareUpdate
GoogleSoftwareUpdateAgent
Caches
com.google.UpdateEngine.501
Downloads
com.google.Chrome.dmg
tmp
UpdateEngine-ksurl.xlBcl3aXau
ksurl
UpdateEngine-download.7rv4dHhME
com.google.Chrome.dmg
UpdateEngine-mount.35TV2rg29j
.keystone_install
dirpatcher.sh
.patch
version_18.0.1025.142_18.0.1025.151.dirpatch
waitCursor.png$raw
application.dirpatch
Contents
MacOS
Google Chrome$xz
keystone_install.9vPBnaFE
Google Chrome.app
MacOS
Google Chrome
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35


Server
Process
Directory or File
Network Flow
File Flow
Process Flow
Read
Write
Move
Execute
Pass Descriptor
Network Layer
Process Layer
File Layer
74.125.224.46
443
80
67.50.19.21
80
1
unknown
2
launchd
3
GoogleSoftware UpdateAgent
4
5
6
ksurl
7
8
9
10
hdiutil
hdiutil
hdiutil
hdiutil
hdiutil
11
12
13
14
diskimages-helper
15
diskimages-helper
16
17
18
.keystone_install
19
20
dirpatcher.sh
21
.keystone_install
mkdir
mktemp
touch
22
cp
stat
chmod
23
24
25
dirpatcher.sh
26
xzdec
27
28
29
rsync
30
31
rsync
32
rsync
33
34
35
Applications
Google Chrome.app
Versions
18.0.1025.151
Resources
waitCursor.png
MacOS
Google Chrome
.Google Chrome.OQwVWD
Users
heberlei
Library
GoogleSoftwareUpdate
GoogleSoftwareUpdateAgent
Caches
com.google.UpdateEngine.501
Downloads
com.google.Chrome.dmg
tmp
UpdateEngine-ksurl.xlBcl3aXau
ksurl
UpdateEngine-download.7rv4dHhME
com.google.Chrome.dmg
UpdateEngine-mount.35TV2rg29j
.keystone_install
dirpatcher.sh
.patch
version_18.0.1025.142_18.0.1025.151.dirpatch
waitCursor.png$raw
application.dirpatch
Contents
MacOS
Google Chrome$xz
keystone_install.9vPBnaFE
Google Chrome.app
MacOS
Google Chrome


unknown
launchd
GoogleSoftware UpdateAgent
.keystone_install
rsync
rsync
rsync
35
36
Google Chrome.OQwVWD
Google Chrome

unknown

Google Chrome



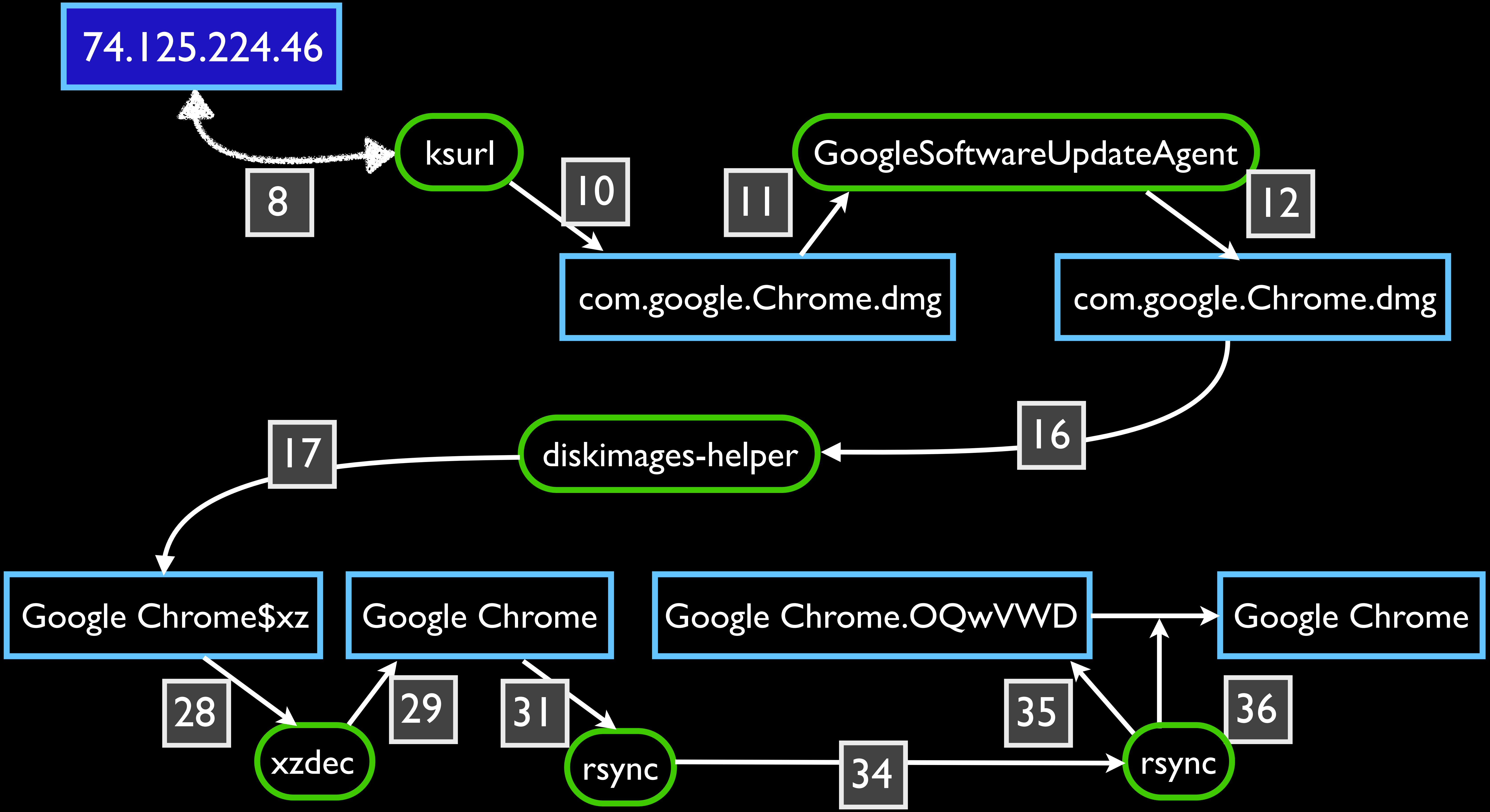
unknown

From boot to file creation

Google Chrome

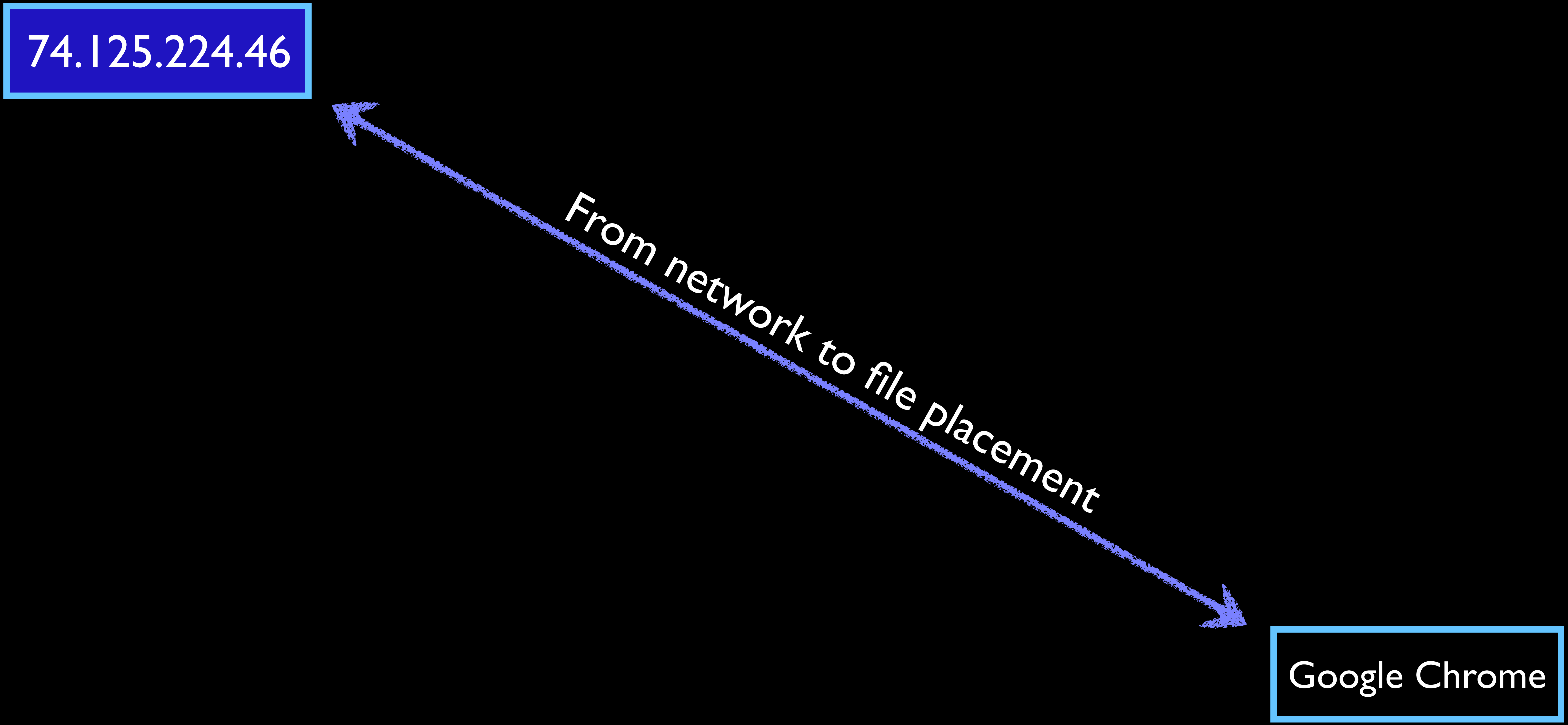
74.125.224.46

Google Chrome


74.125.224.46
8
ksurl
10
com.google.Chrome.dmg
11
GoogleSoftwareUpdateAgent
12
com.google.Chrome.dmg
16
diskimages-helper
17
Google Chrome$xz
Google Chrome
Google Chrome.OQwVWD
Google Chrome
28
xzdec
29
31
rsync
34
35
rsync
36

74.125.224.46

Google Chrome



74.125.224.46

From network to file placement

Google Chrome

Why Audit

Why Audit

- Programs may not exist in memory for very long

Why Audit

- Programs may not exist in memory for very long
- Programs may not exist on the system for very long

Why Audit

- Programs may not exist in memory for very long
- Programs may not exist on the system for very long
- Need to identify what was stolen and what was modified

Why Audit

- Programs may not exist in memory for very long
- Programs may not exist on the system for very long
- Need to identify what was stolen and what was modified
- Modern OSes have pretty good auditing, but we must provide feedback

Why Audit cont...

Why Audit cont...

- Network analysis is reaching the end of the line

Why Audit cont...

- Network analysis is reaching the end of the line
- Get on the host

Why Audit cont...

- Network analysis is reaching the end of the line
- Get on the host
- Yes, No, Maybe; It is a brave new world, and you must do the diagnosis

Why Audit cont...

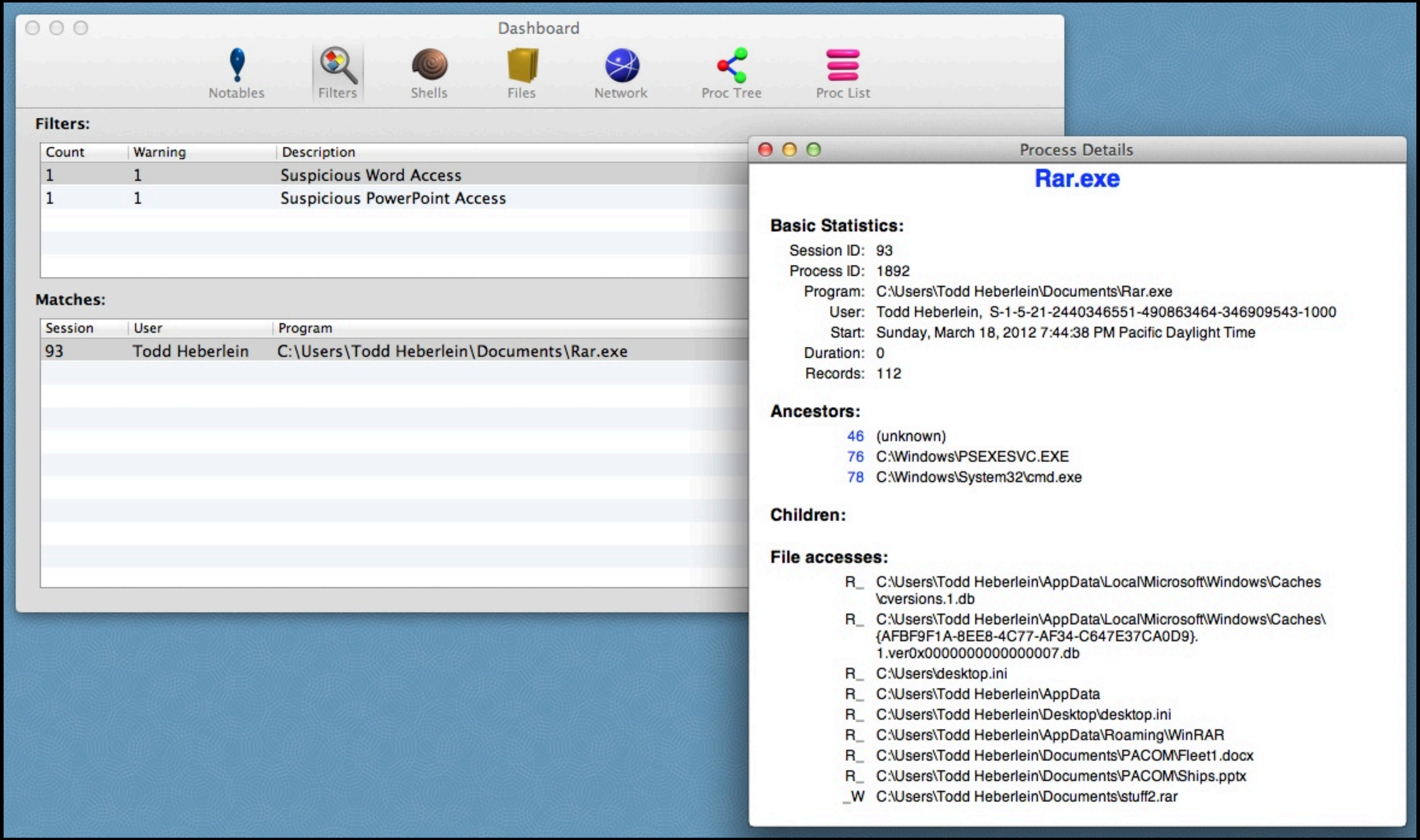
- Network analysis is reaching the end of the line
- Get on the host
- Yes, No, Maybe; It is a brave new world, and you must do the diagnosis
- Practice in real-world environment with lots of noise

Contact me: Todd Heberlein

web: www.NetSQ.com

email: LTH@NetSQ.com

email: todd_heberlein@mac.com



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

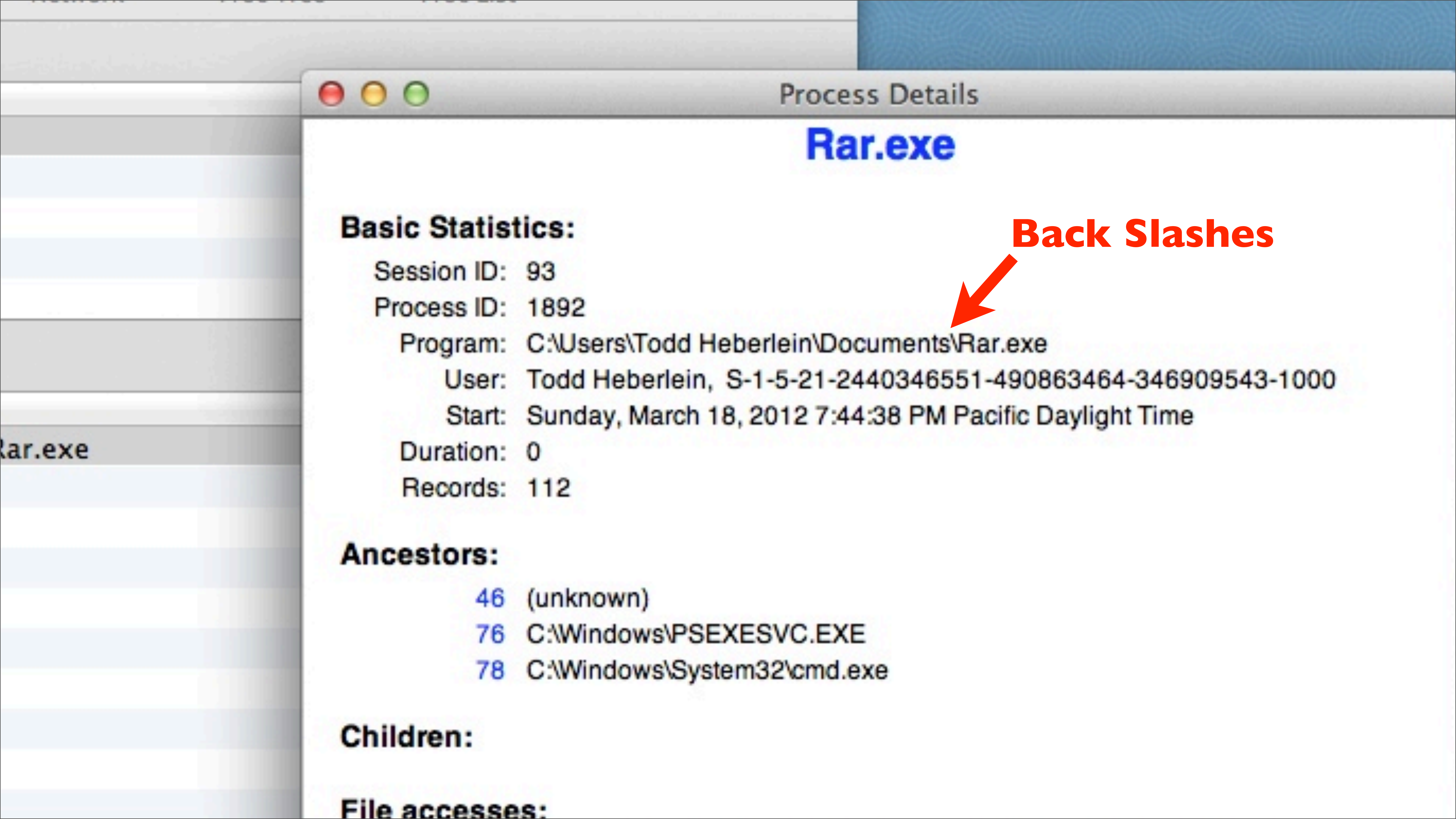
Ancestors:

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



Back Slashes

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: