



Australian Government  
Department of Defence



DSD and Open Source Software

Alan Leigh

# About Me



- Information Security Specialist
- Infosec-er for about 8 years
- Defence and Industry
- [alan.leigh@defence.gov.au](mailto:alan.leigh@defence.gov.au)

# About DSD



- Two roles
  - Signals Intelligence (SIGINT)
  - Information (or Cyber) Security
    - Cyber Security Operations Centre
- <http://dsd.gov.au>

# About DSD

A presentation slide featuring a dark blue background with a faint network of binary code and glowing nodes. In the center is a white rectangular area containing the following content:

Australian Government  
Department of Defence  
Intelligence and Security

**PROTECT**



Defence Signals Directorate

## Blackberry Hardening Guide

July 2011

# About DSD



The image shows the cover of a document titled 'iOS Hardening Configuration Guide'. The cover has a blue background with a large, stylized graphic of three interlocking padlocks in the center. Above the padlocks, the word 'PROTECT' is written in a light blue, sans-serif font. At the top left, there is a small version of the Australian Coat of Arms. To its right, the text 'Australian Government' is followed by 'Department of Defence' and 'Intelligence and Security'. The title 'iOS Hardening Configuration Guide' is prominently displayed at the bottom in a large, bold, white font. Below the title, it says 'FOR iPOD TOUCH, iPHONE AND iPAD RUNNING iOS 5.1 OR HIGHER'. At the very bottom, the date 'March 2012' is printed in a small, white font. The entire document is framed by a thick black border.

# About DSD

The collage includes:

- A vertical banner on the left with the Australian Coat of Arms at the top, followed by the text "Defence Signals Directorate" and "Black Ops".
- A horizontal banner below it with the text "iOS Handbooks FOR iPod Touch".
- A large central document titled "PROTECT" with the subtitle "Strategies to Mitigate Targeted Cyber Intrusions".
- The Australian Government Department of Defence Intelligence and Security logo.
- A graphic of a computer monitor with a shield icon.
- Decorative blue squares and the date "OCTOBER 2012".
- Small text at the bottom of the central document: "4. DSD's list of mitigation strategies, first published in February 2010, is revised for 2012 based on DSD's most recent analysis of incidents across the Australian Government. Further details on the mitigation strategies are available at the DSD web page <http://www.dsd.gov.au>. 5. While no single strategy can prevent malicious activity, the effectiveness of implementing the Top 4 strategies remains very high. At least 85% of the intrusions that DSD responded to in 2011 involved adversaries using unsophisticated techniques that would have been mitigated by implementing the Top 4 mitigation strategies as a package. 6. Implementing the Top 4 strategies can be achieved gradually, starting with computers used by the employees most likely to be targeted by intrusions, and eventually extending them to all users. Once this is achieved, organisations can selectively implement additional mitigation strategies based on the risk to their information. 7. This document provides information about mitigation implementation costs and user resistance to help organisations select the best set of strategies for their requirements. 8. These strategies complement the guidance provided in the *Australian Government Information Security Manual (ISM)* available on DSD's web site."
- Text at the bottom right: "Defence Signals Directorate | Reveal Their Secrets – Protect Our Own".

# About DSD

Defence Signals Directorate

iOS Handbooks FOR iPod Touch

BlackBerry Security Manual (ISMS)

Strategies

Introduction

1. Australian government information.
2. A commonly tailored to entice attachments or foot network and disclosure.
3. The Defence Signals Directorate's cyber intrusions. Targeting responding to serial testing for Australia.

Mitigation Strategies

4. DSD's list of the Top 4 most recent mitigation strategies.
5. While no single strategy involved adversaries implementing the Top 4 strategies.
6. Implementing the employees more. Once this is achieved, the risk to their security.
7. This document to help organisations.
8. These strategies Security Manual (ISMS).

Australian Government  
Department of Defence  
Intelligence and Security

CYBER SECURITY OPERATIONS CENTRE

PROTECT

NOVEMBER 2012

## Top 4 mitigation strategies to protect your ICT system

Targeted cyber intrusions remain the biggest threat to government ICT systems. Since opening in early 2010, the Cyber Security Operations Centre (CSOC) has detected and responded to thousands of these intrusions.

You should never assume that your information is of little or no value. Adversaries are not just looking for classified information. A lot of activity observed by the CSOC has an economic focus looking for information about Australia's business dealings, its intellectual property, its scientific data and the government's intentions.

The threat is real, but there are things every organisation can do to significantly reduce the risk of a cyber intrusion. In 2009, based on our analysis of these intrusions, the Defence Signals Directorate produced *Strategies to Mitigate Targeted Cyber Intrusions* – a document that lists a variety of ways to protect an organisation's ICT systems. At least 85% of the intrusions that DSD responded to in 2011 involved adversaries using unsophisticated techniques that would have been mitigated by implementing the Top 4 mitigation strategies as a package.

The Top 4 mitigations are: application whitelisting, patching applications and operating systems and using the latest versions; and minimising administrative privileges. This document is designed to help senior managers in organisations understand the effectiveness of implementing these strategies.

### Application whitelisting

Whitelisting—when implemented correctly—makes it harder for an adversary to compromise an organisation's ICT system. Application whitelisting is a technical measure which only allows specifically authorised applications to run on a system. This helps prevent malicious software and unauthorised applications running.

### Patching systems

A software patch is a small piece of software designed to fix problems or update a computer program. Patching an organisation's system encompasses both the first and second mitigation strategies. It is important to patch both your operating system and applications within a two day timeframe for serious vulnerabilities. Once a vulnerability in an operating system or application is made public, you can expect malware to be developed by adversaries within 48 hours. In some cases, malware has been developed to take advantage of a publicly disclosed vulnerability within eight hours.

There is often a perception that by patching a system without rigorous testing, something is likely to break on the system. In the majority of cases patching will not affect the function of an organisation's ICT system.

Defence Signals Directorate | Reveal Their Secrets – Protect Our Own

Page 1 of 2

# About DSD

**iOS Handbooks FOR iPOD TOUCH**

**Defence Signals Directorate Black Ops**

**Australian Government Department of Defence Intelligence and Security**

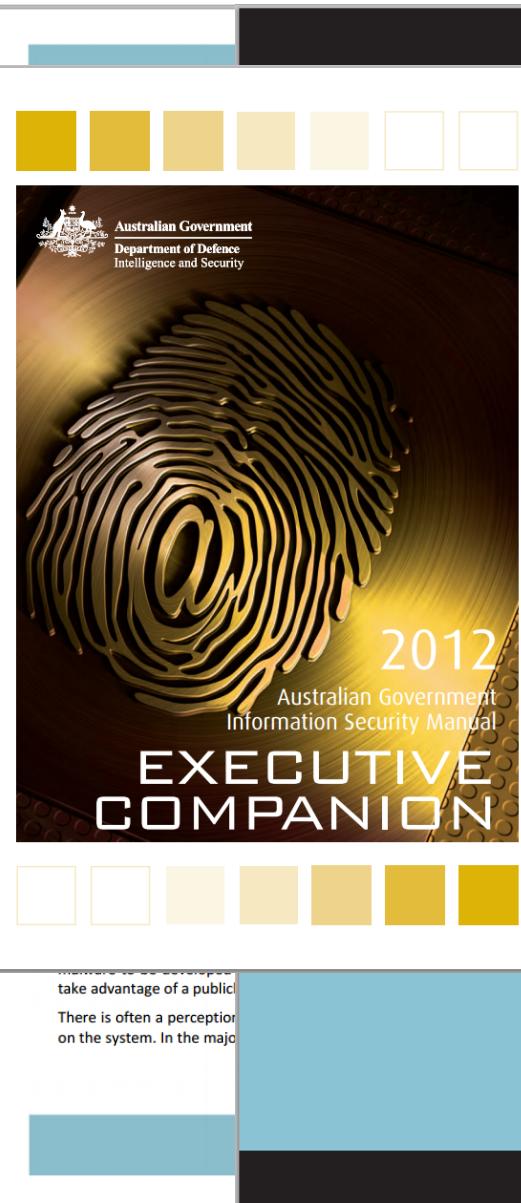
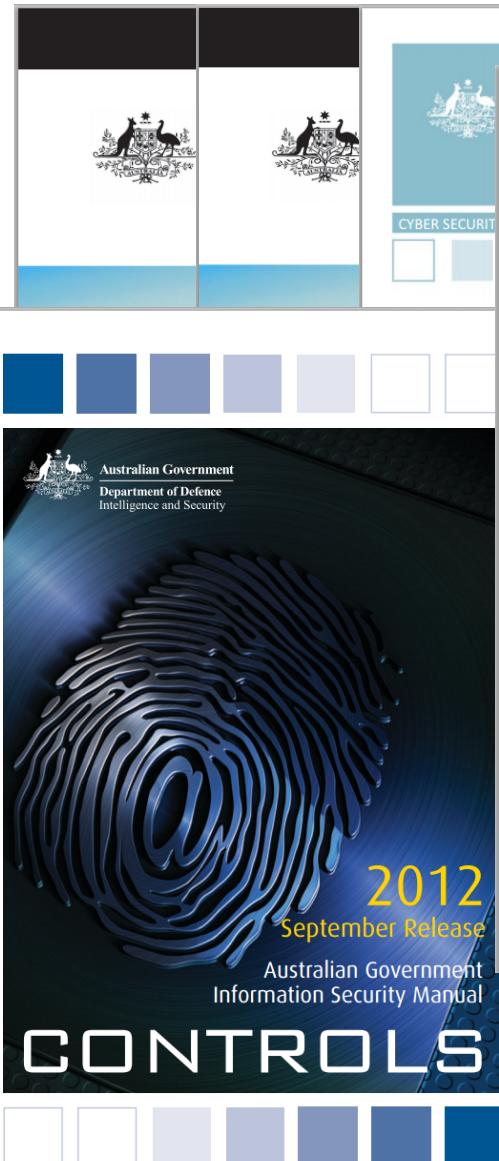
**PROTECT**

**IMPLEMENTING DSD'S TOP FOUR FOR WINDOWS ENVIRONMENTS**

**November 2011**



# About DSD



# DSD and Open Source



**fedora**<sup>®</sup>



**django**

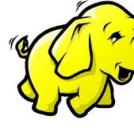


**Scala**



 **python**<sup>™</sup>



 **hadoop**



- <http://code.google.com/p/pyflag>
- GPLed
- Interesting uses:
  - <http://memeover.arkem.org/2012/02/identifying-computers-behind-nat-with.html>
  - <http://www.dfrws.org/2008/proceedings/p112-cohen.pdf>

- <http://sourceforge.net/projects/spillguard/>
- GPLed
- Designed to help prevent “data spills”
  - C++ (Was VB .Net ...)
  - MS Office Plugin (COM Add-In)

# SpillGuard

marking\_in\_header - Microsoft Word

File Edit View Insert Format Tools Table Window Help

Type a question for help

100% Read Calibri

NOTCLASSIFIED

SpillGuard Classification Checker has found a possible classification breach

This file was NOT saved since it contains the following classification markings that are higher than this computer can handle:

NOTCLASSIFIED (located in a header in section 1)

OK

Draw AutoShapes Page 1 Sec 1 1/5 At 1" Ln 1 Col 1 REC TRK EXT OVR English (U.S.)

marking\_in\_header ... SpillGuard Classifica... 3:55 PM

# SpillGuard

Event Viewer

File Action View Help

Event Viewer (Local)

- Custom Views
- Windows Logs
  - Application
  - Security
  - Setup
  - System
  - Forwarded Events
- Applications and Services
- Subscriptions

Application 17 Events

Level	Date and Time	Source	Event ID	Task Category	User	Computer
Warning	8/9/2008 3:56:02 PM	SpillGuard	0	Classification Breach	mypc\steve	mypc
Warning	8/9/2008 3:55:57 PM	SpillGuard	0	Classification Breach	mypc\steve	mypc
Warning	8/9/2008 3:55:48 PM	SpillGuard	0	Classification Breach	mypc\steve	mypc
Warning	8/9/2008 3:54:15 PM	SpillGuard	0	Classification Breach	mypc\steve	mypc
Information	8/9/2008 3:53:22 PM	SpillGuard	0	Classification Breach	mypc\steve	mypc

Event 0, SpillGuard

General Details

On Saturday 09 August 2008 at 03:56:02 PM  
(Saturday 09 August 2008 at 05:56:02 UTC/GMT/Zulu)  
the userid 'steve'  
using the computer named 'MYPUPER'  
using the computer with DNS name 'mypc'  
in the computer domain 'mypc'  
attempted to print the file named:  
'C:\test\_cases\word\marking\_in\_header\marking\_in\_header.doc'  
which contained the following disallowed classification markings:  
NOTCLASSIFIED (located in a header in section 1)

Log Name:	Application
Source:	SpillGuard
Event ID:	0
Level:	Warning
User:	mypc\steve
OpCode:	
More Information:	<a href="#">Event Log Online Help</a>

Actions

- Application
  - Open Saved Log...
  - Create Custom Vi...
  - Import Custom Vi...
  - Clear Log...
  - Filter Current Log...
  - Properties
  - Find...
  - Save Events As...
  - Attach a Task To ...
  - View
  - Refresh
  - Help
- Event 0, SpillGuard
  - Event Properties
  - Attach Task To T...
  - Copy
  - Save Selected Eve...
  - Refresh
  - Help

Event Viewer 3:59 PM

# WhiteTrash

- <http://whitetrash.sourceforge.net>
- GPLed
- Dynamic whitelisting proxy (using Squid, Django)



# WhiteTrash

Whitetrash Internet Access Request Form - Mozilla Firefox

Whitetrash Internet Access Re... 

<https://whitetrash/whitelist/addentry?url=http%3A//www.slashdot.org/&domain=www.slas>    Google  

 **WHITE TRASH**

Dynamic Web Whitelisting For Squid

Host Requested:

Protocol:

Client Username: al

News and Current Affairs

This site is not currently in the whitelist. If you have a genuine need to access this site please enter a business requirement or comment for this domain:

By clicking "I Agree" below you are agreeing to have the information above stored on a list of whitelisted websites with YOUR UNIQUE USERNAME at this address

I Agree

Using Firefox? Grab the whitetrash add-on [here](#)

# WhiteTrash

Slashdot: News for nerds, stuff that matters - Mozilla Firefox

slashdot.org

Slashdot Stories Slash Boxes Comments

Nickname:

Password: 6-20 characters long

Public Terminal

[Log In](#) [Forgot your password?](#)

<http://> [Log in with OpenID](#)

[Close](#)

- [Stories](#)
- [Submissions](#)
- [Popular](#)
- [Blog](#)

[Slashdot](#)

- [Ask Slashdot](#)
- [Book Reviews](#)
- [Games](#)
- [Idle](#)
- [YRO](#)
- [Cloud](#)
- [Hardware](#)
- [Linux](#)
- [Management](#)

X

# WhiteTrash

Slashdot: News for nerds, stuff that matters - Mozilla Firefox

slashdot.org

Slashdot Stories Slash Boxes Comments

Nickname:

Password: 6-20 characters long

Public Terminal

[Log In](#) [Forgot your password?](#)

<http://> [Log in with OpenID](#)

[Close](#)

[Stories](#)  
[Submissions](#)  
[Popular](#)  
[Blog](#)

[Slashdot](#)

- [Ask Slashdot](#)
- [Book Reviews](#)
- [Games](#)
- [Idle](#)
- [YRO](#)
- [Cloud](#)
- [Hardware](#)
- [Linux](#)
- [Management](#)

About Whitetrash...  
Options...

slashdot.org:a.fsdn.com  
slashdot.org:slashdot.org  
slashdot.org:rss.slashdot.org  
slashdot.org:www.google-analytics.com  
slashdot.org:widget-cdn.rpxnow.com  
slashdot.org:ad.doubleclick.net

# WhiteTrash

Slashdot (15) - Mozilla Firefox

slashdot.org

Slashdot ★

stories submissions popular blog ask slashdot book reviews games idle yro cloud hardware linux management mobile science security storage

MIT Warned of a JSTOR Death Sentence Due To Swartz

Posted by Unknown Lamer on Tuesday January 22, @05:01AM from the stewards-of-knowledge-locked-safe-within-their-walls dept.

theodp writes

"The NY Times takes a look at how MIT ensnared Aaron Swartz, but doesn't shed much light on how the incident became a Federal case with Secret Service involvement. Still, the article is interesting with its report that 'E-mails among M.I.T. officials that Tuesday in January 2011 highlight the pressures university officials felt' from JSTOR, which is generally viewed as a good guy in the incident. From the story: 'Ann J. Wolpert, the director of libraries, wrote to Ellen Finnie Duranceau, the official who was receiving JSTOR's complaints: "Has there ever been a situation similar to this when we brought in campus police? The magnitude, systematic and careful nature of the abuses could be construed as approaching criminal action. Certainly, that's how JSTOR views it.'" Less than a week later, a Google search reveals, Duranceau notified the MIT community that immediate changes to JSTOR access had to be made lest the University be subjected to a JSTOR 'death sentence.' Because JSTOR has recently reported excessive, systematic downloading of articles at MIT,' the post warned, 'we need to add a new layer of access control. This is the only way to prevent recurrence of the abuse and therefore the only way to ensure ongoing access to this valuable resource for the MIT Community.' The post concludes, 'The incidents that prompted this change involved the use of a robot, which is prohibited by JSTOR's Terms and Conditions of Use. ...Continued access to JSTOR and other resources is dependent on the MIT Community complying with these policies.' Hope you enjoyed that freewheeling culture while it lasted, kids — now Everything is a Crime."

Read the 28 comments

crime yro copyright

How Facebook Will Power Graph Search

Follow us:

Slashdot Poll

When Was the Last Time You Used a Landline Phone?

Today  
 This Week  
 This Month  
 This Year  
 Over a Year  
 Never  
 What's a Landline Phone?

Read the 159 comments

Voted on 9874 times.

Vote

Most Discussed

830 New York Pistol Permit Owner List Leaked

660 How Much Beef Is In Your Burger?

533 Ask Slashdot: How Do I Get My Spouse To Start Gaming With Me?

526 Student Expelled From Montreal

☐ Whitetrash Whitelist +

← 🔒 <https://whitetrash/whitelist/view/list/>



Dynamic Web Whitelisting For Squid

**VIEW WHITELIST**

**NOT-WHITELISTED**

**DELETE ENTRIES**

**ADD ENTRY**

**ADMIN LOGIN**

**DOWNLOAD CA**

**LOGOUT**

ID	Whitelisted Domain	Hits	First Whitelisted	Last Accessed
43	a.fsdn.com	48	2013-01-22 22:27:12	2013-01-22 22:28:21
42	slashdot.org	5	2013-01-22 22:24:35	2013-01-22 22:28:24
37	ichef.bbci.co.uk	64	2013-01-22 22:22:23	2013-01-22 22:22:34
35	static.bbci.co.uk	78	2013-01-22 22:22:22	2013-01-22 22:22:45
34	bbc.co.uk	8	2013-01-22 22:22:10	2013-01-22 22:22:43
15	theage.com.au	163	2013-01-22 22:21:14	2013-01-22 22:22:54
3	cnn.com	4	2013-01-22 22:02:26	2013-01-22 22:02:36

# Pronghorn

- <http://github.com/pronghorn/pronghorn>
- GPLed
- Block classifier

- <http://www.dfrws.org>
- Since 2001
- Academics, forensics practitioners, etc.
- Annual challenge

# 2012 Challenge

- Block classification tool
- Must be open sourced
- With extras
  - May contain a file system
  - Concurrency
  - Container support (e.g. a PDF inside a zip inside a ...)
- `./toolname <file> <block size> <cores>`

# Pronghorn

- C
- FUSE
- ZeroMQ & Protobufs
- Third party libraries
  - The Sleuthkit



# FUSE

- Filesystem in userspace
- <http://fuse.sourceforge.net>
- Lots of cool examples:
  - <http://sourceforge.net/apps/mediawiki/fuse/index.php?title=FileSystems>

# The Sleuthkit

- <http://sleuthkit.org>
- Excellent set of tools



```
alan@toshiba:~/Desktop/workspace/scratch$ istat -o 63 ./test.dd 4
Directory Entry: 4
Allocated
File Attributes: File, Archive
Size: 193263
Name: DSC_9227.jpg

Directory Entry Times:
Written:      Sun Nov 18 12:32:36 2012
Accessed:     Sun Nov 18 00:00:00 2012
Created:      Sun Nov 18 12:47:47 2012

Sectors:
1609562 1609563 1609564 1609565 1609566 1609567 1609568 1609569
1609570 1609571 1609572 1609573 1609574 1609575 1609576 1609577
```

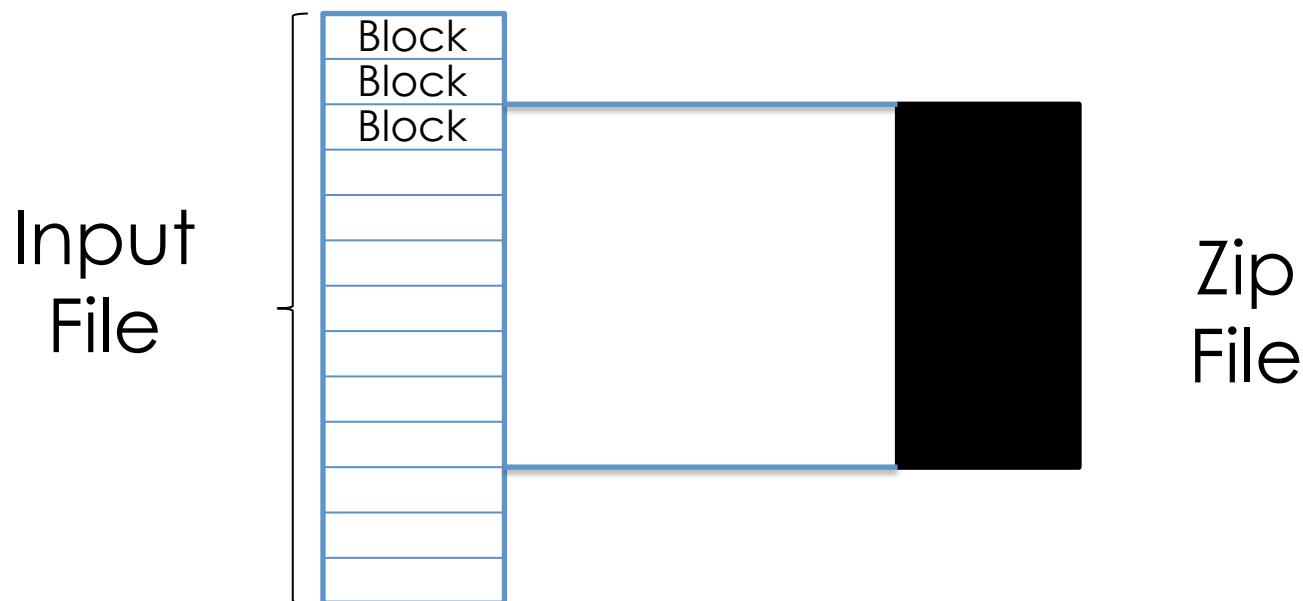


- <http://www.zeromq.org>
- Sockets but awesome
- You just
  - ...
  - socket.bind('tcp://\*:1234')
  - ...
- And then
  - ...
  - zmq\_connect(zmq\_socket, "tcp://localhost:1234")
  - zmq\_msg\_send(zmq\_msg, zmq\_socket)
  - ...

# Protocol Buffers

- <http://code.google.com/p/protobuf/>
- We started with JSON (and it's still an option when you compile)
  - Easy to debug
  - Slow
- Protobufs showed a big speed up!

# The Problem



# One Approach

- Have as many options as possible
  - FUSE!
- Everything becomes a path
  - Anything that can open / analyse a file can be used

# Rawmount

- We can take a source to be processed (input.dd) and “rawmount” it:
  - rawmount -o file=input.dd /mnt/point
- The entire input.dd at any offset of any size can be accessed as a file:

```
# This is the data at offset 4096  
/mnt/point/4096  
  
# This is the first 1024 bytes at 4096  
/mnt/point/4096-1024  
  
# This is exactly the same as input.dd  
/mnt/point/0
```

- Quick Demo Time!

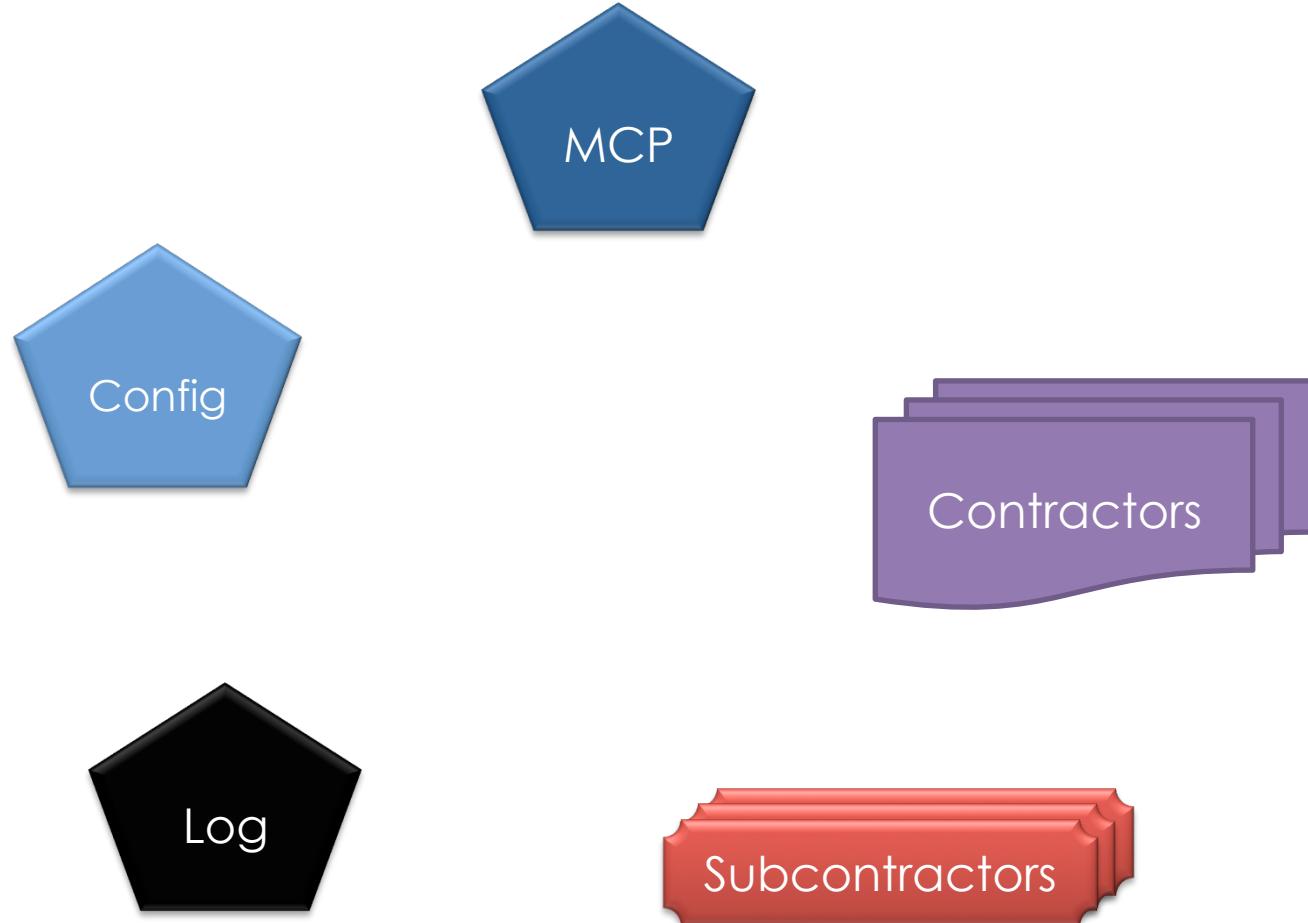
# \*mount

- We use this exact model for other “mounters” to find nested files.
  - e.g. We write a zip mounter
  - `zipmount -o file=/mnt/point/4096 /mnt/point/4096:mnt-zip/`
- Then
  - `/mnt/point/4096:mnt-zip/1`
  - Would be the first file in the zip
- The FUSE mounting can continue!

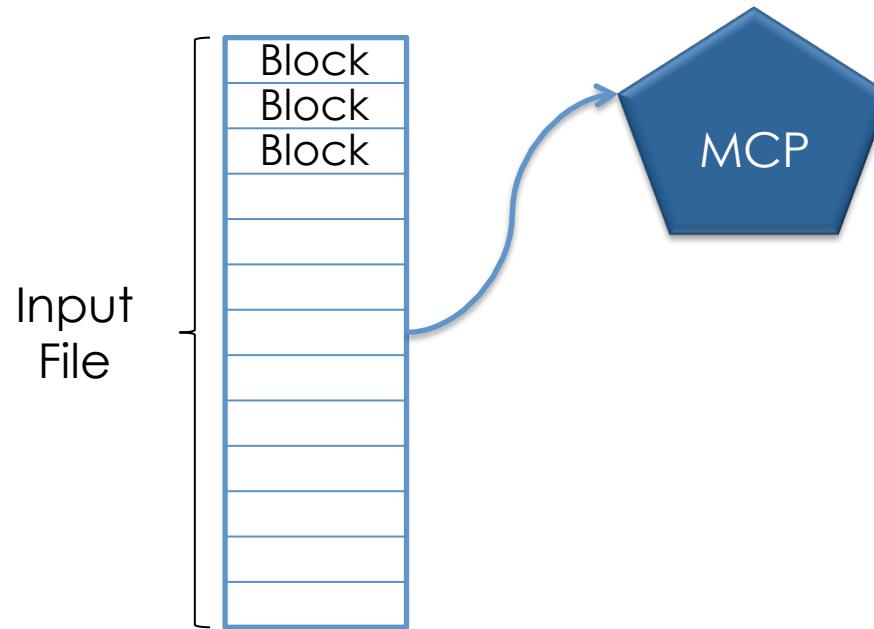
# \*mount

- We developed FUSE mounts for:
  - “Rawmount”
  - OLE
  - PDF
  - File Systems
  - Compressed Files
  - Images
- (We can analyse other data types, they just can't have children...)

# Pronghorn Components

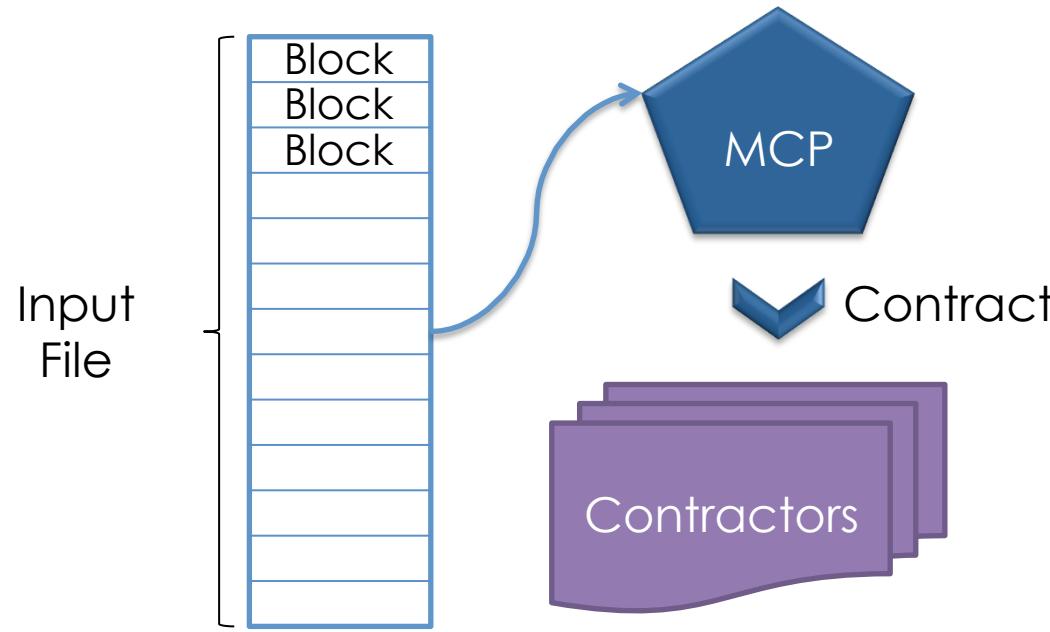


# Pronghorn Workflow



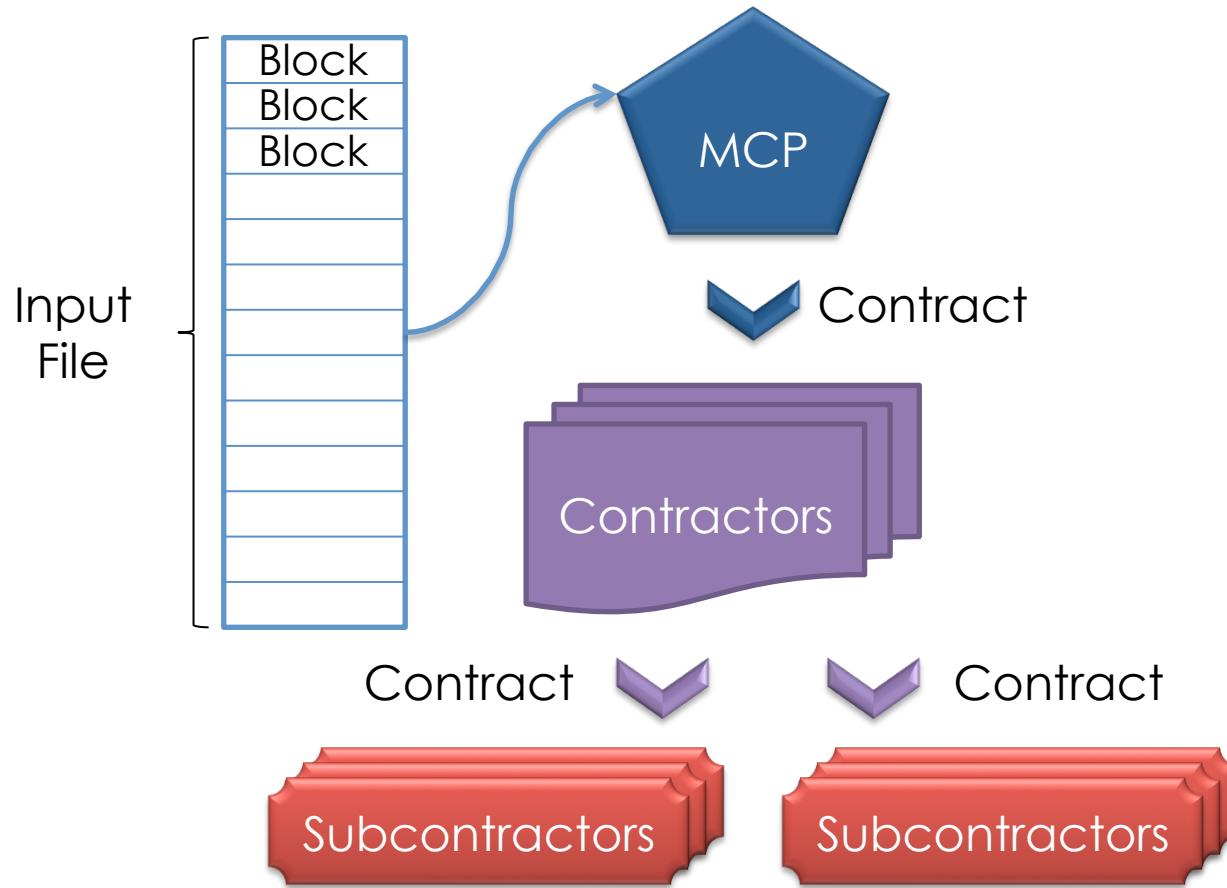
The MCP consumes blocks

# Pronghorn Workflow



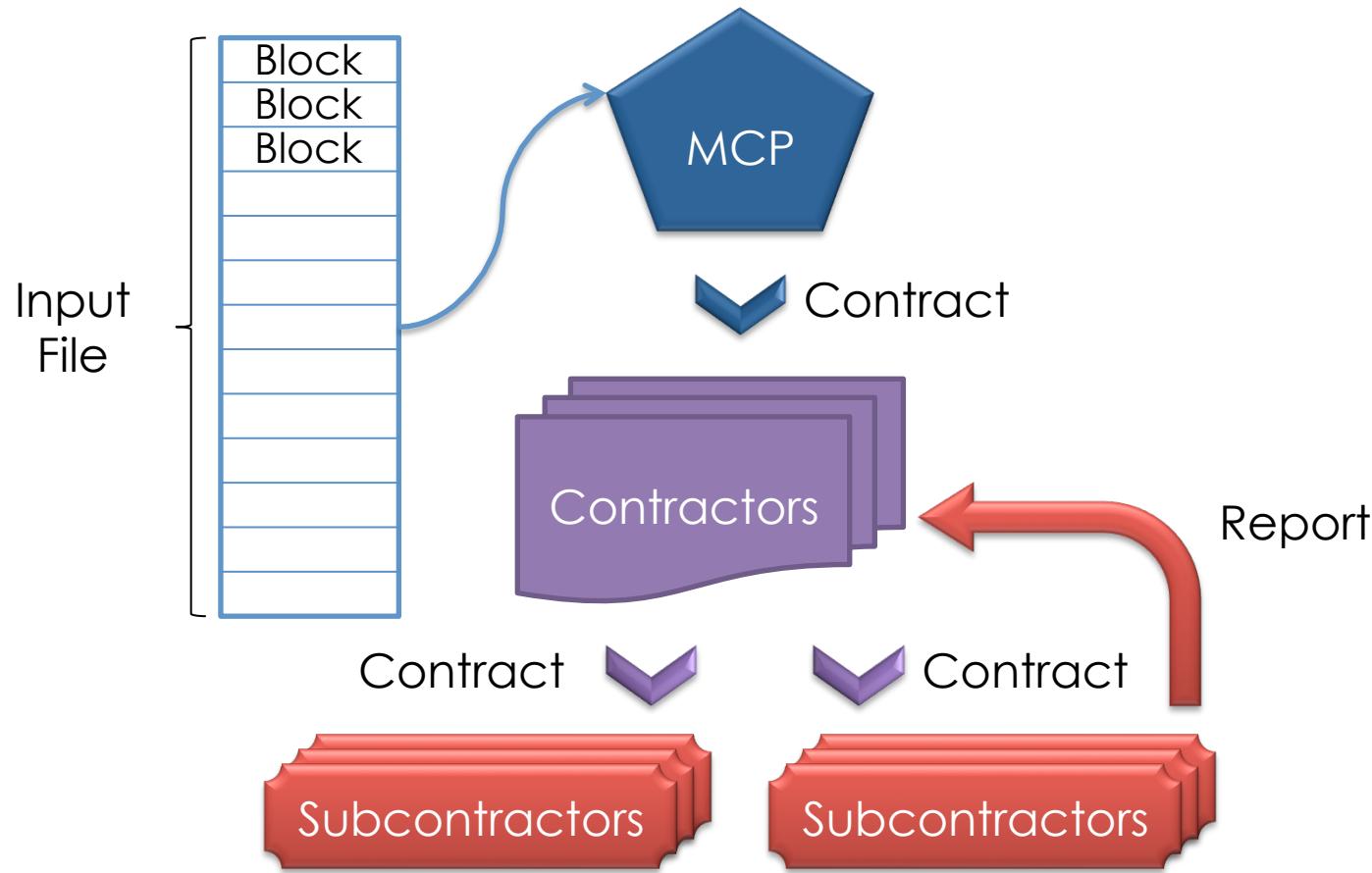
The MCP generates contracts and spawns contractors

# Pronghorn Workflow



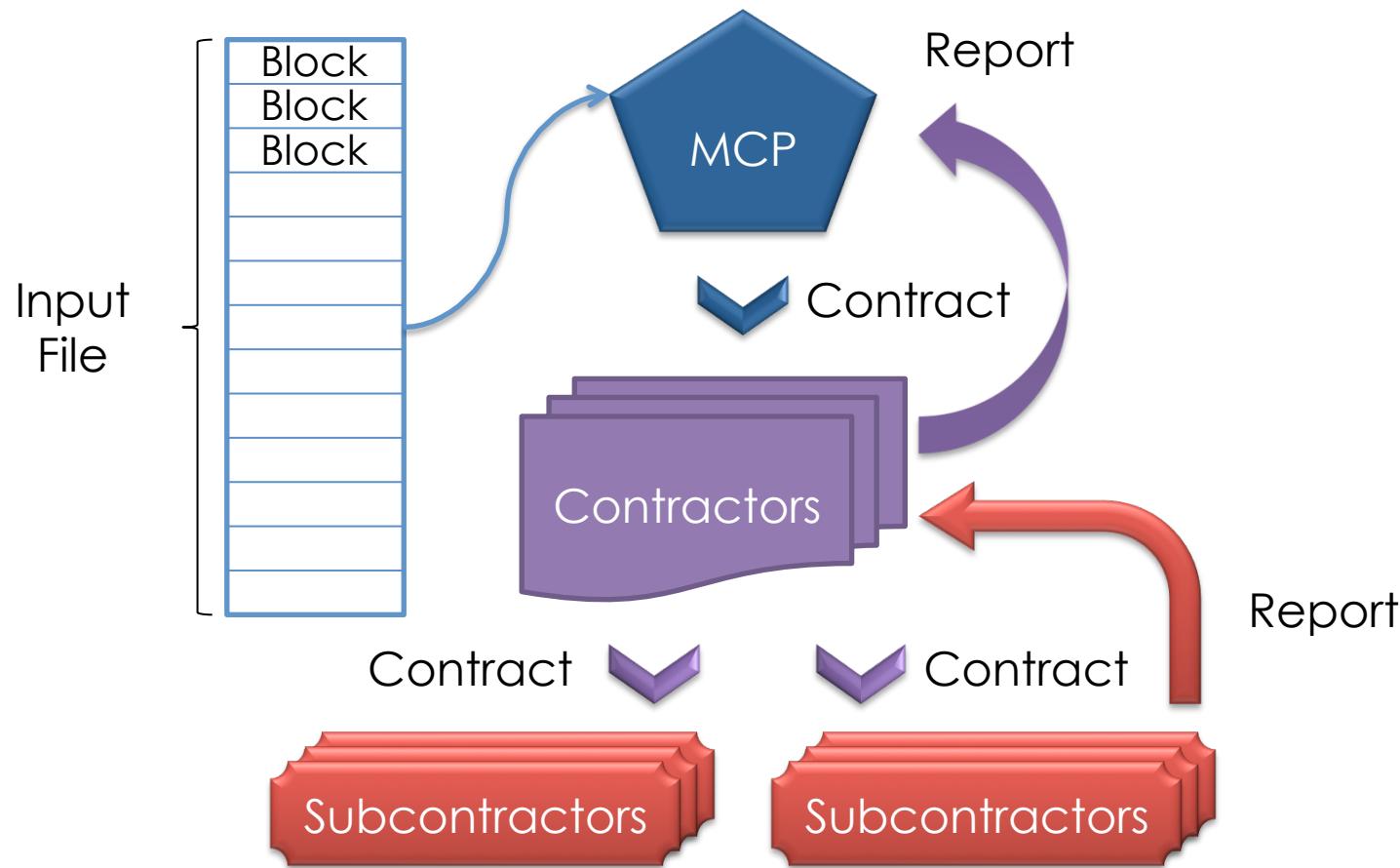
Contractors spawn subcontractors

# Pronghorn Workflow



Subcontractors report their findings

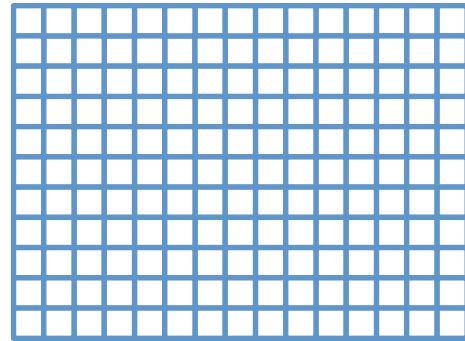
# Pronghorn Workflow



Contractors assess and report to MCP

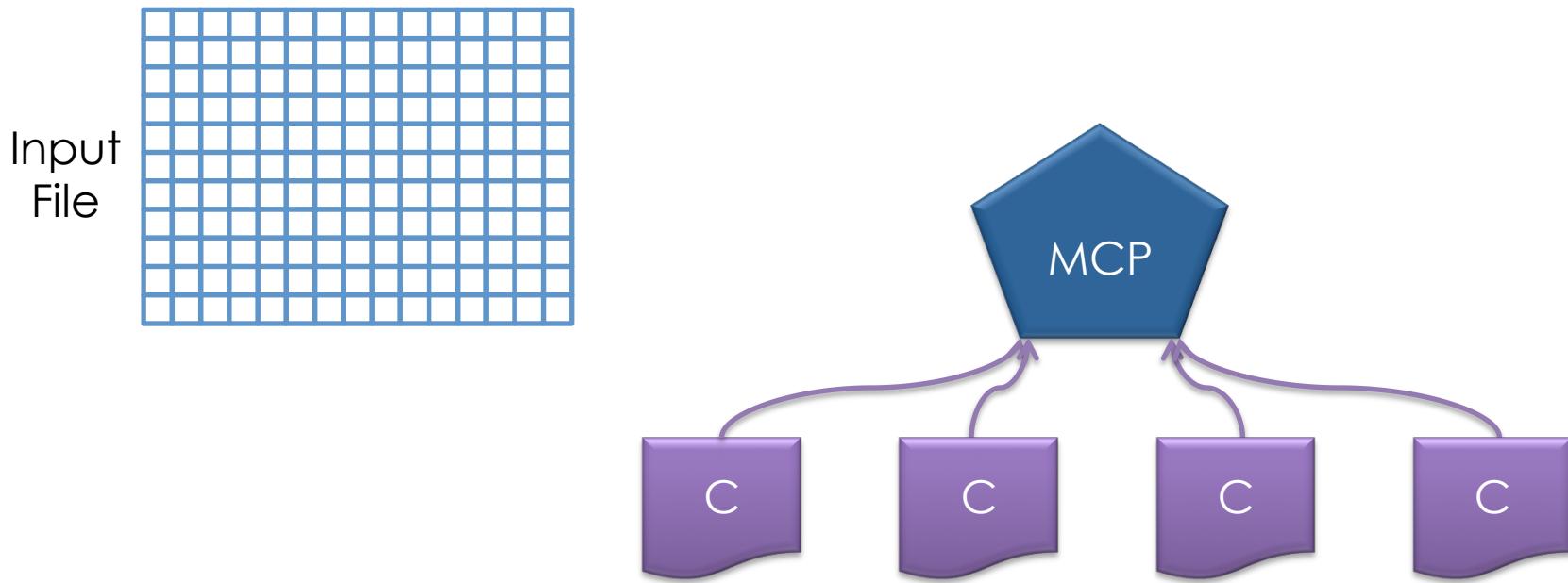
# Pronghorn Example

Input  
File



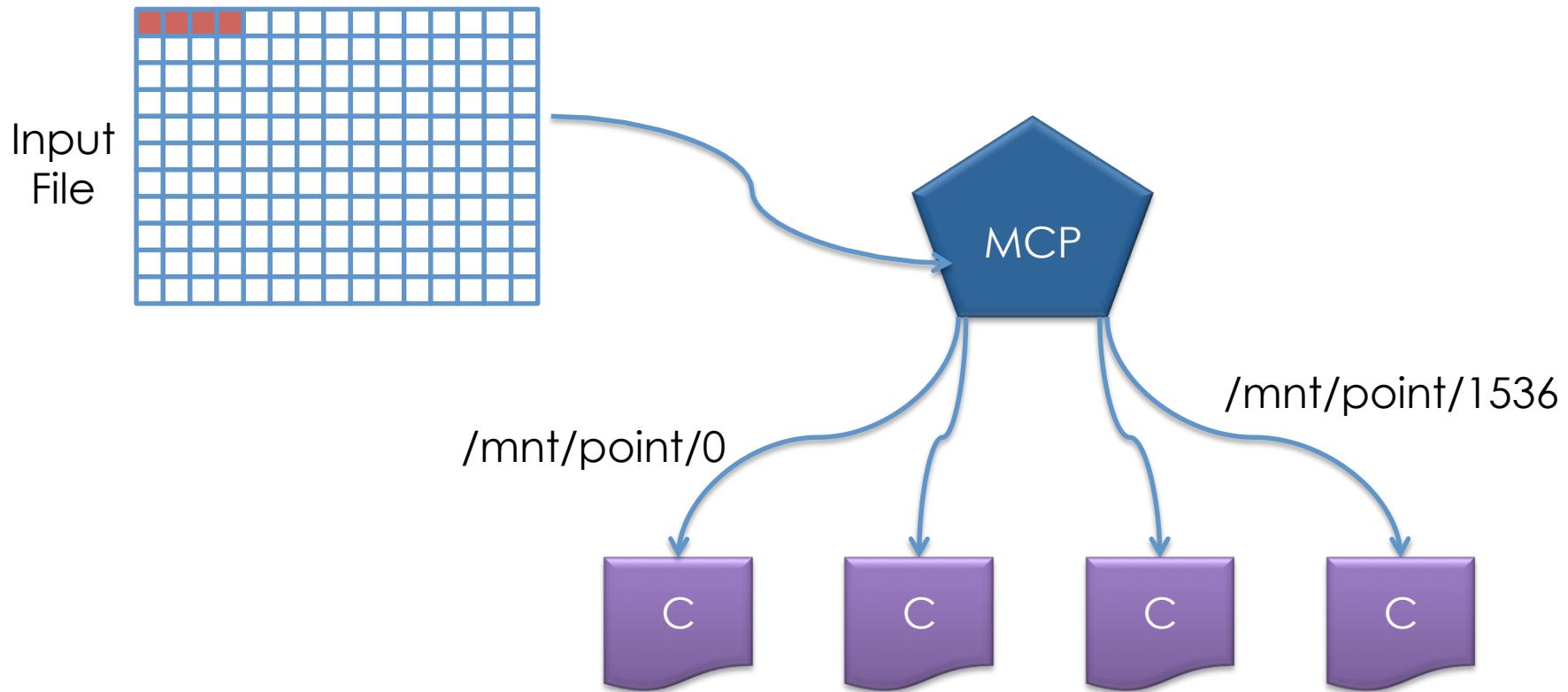
The MCP takes an input file

# Pronghorn Example



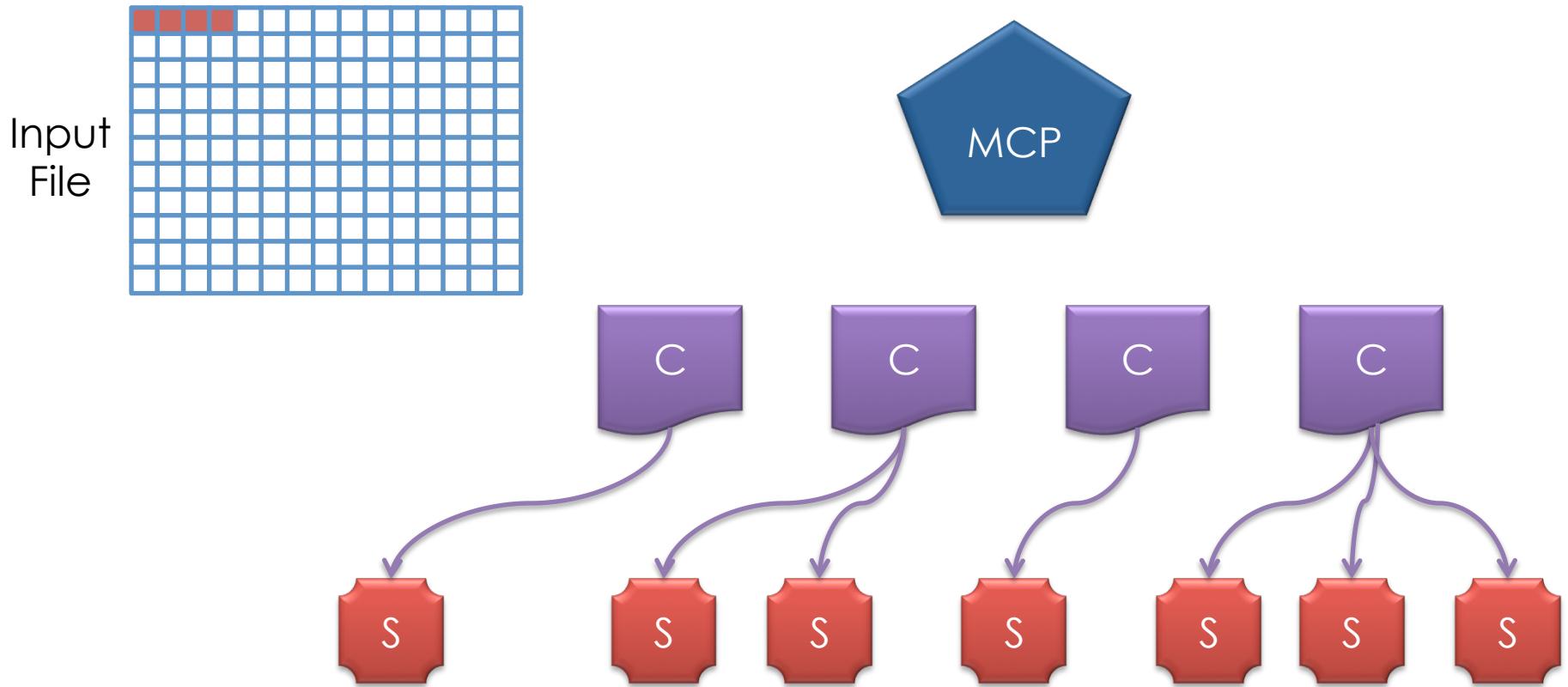
Contractors spawned, request contract

# Pronghorn Example



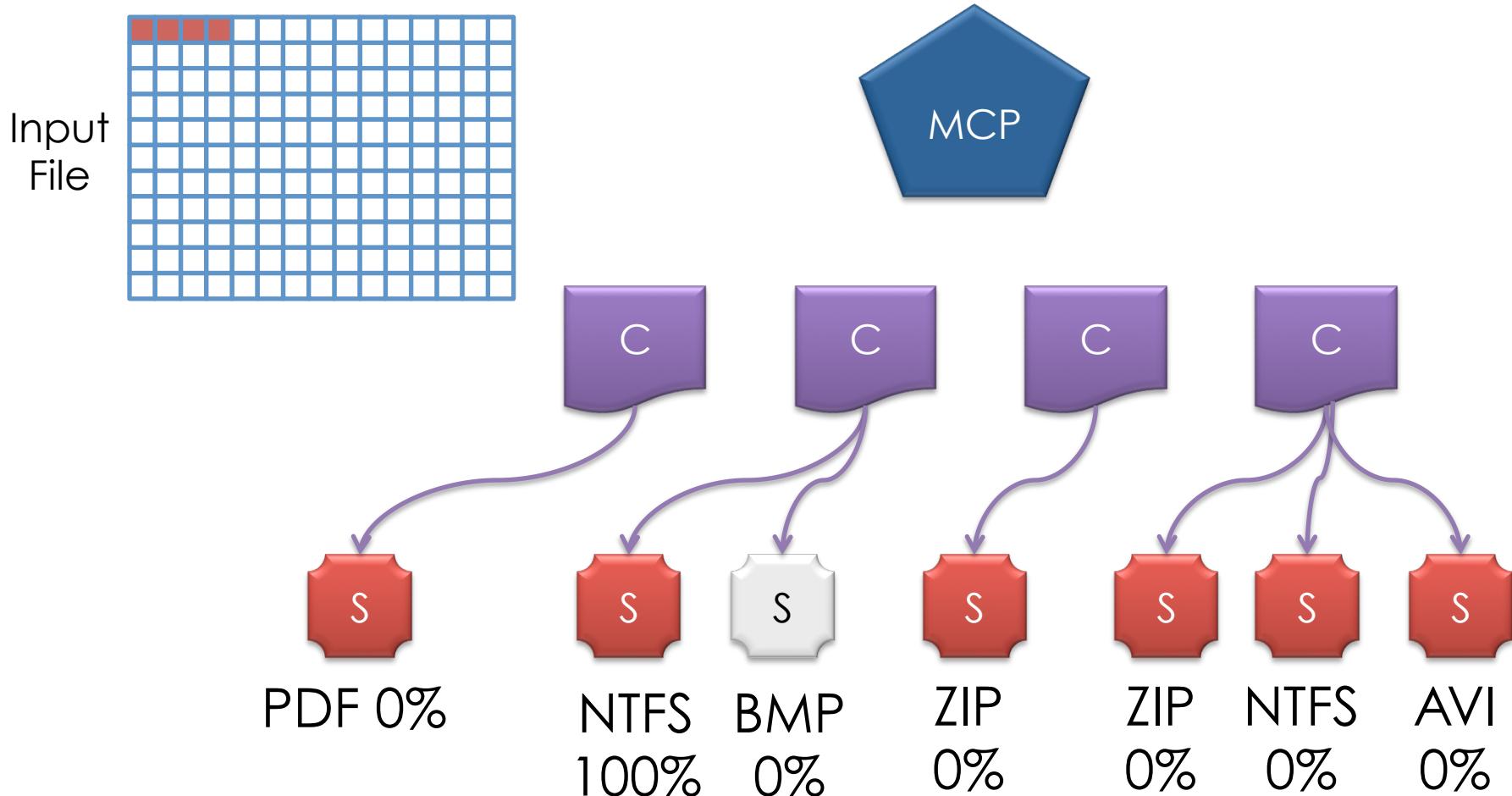
MCP allocates contract per contractor

# Pronghorn Example



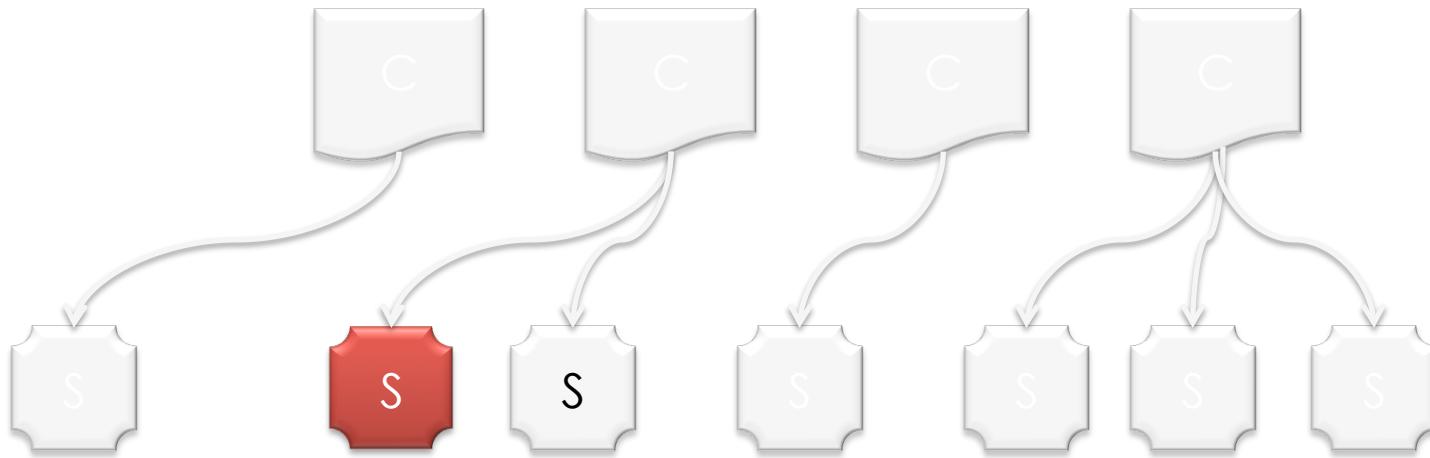
Contractors spawn relevant subcontractors

# Pronghorn Example



Subcontractors perform analysis

# Pronghorn Example



**NTFS - Confidence: 100%**

**New Contracts Found:**

/mnt/point/512:mnt-ntfs/1  
/mnt/point/512:mnt-ntfs/2  
/mnt/point/512:mnt-ntfs/3  
/mnt/point/512:mnt-ntfs/4

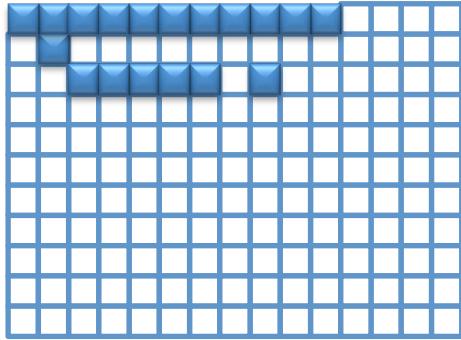
**Additional Blocks Claimed:**

3-10, 16, 32-36, 38

Subcontractors can return additional info

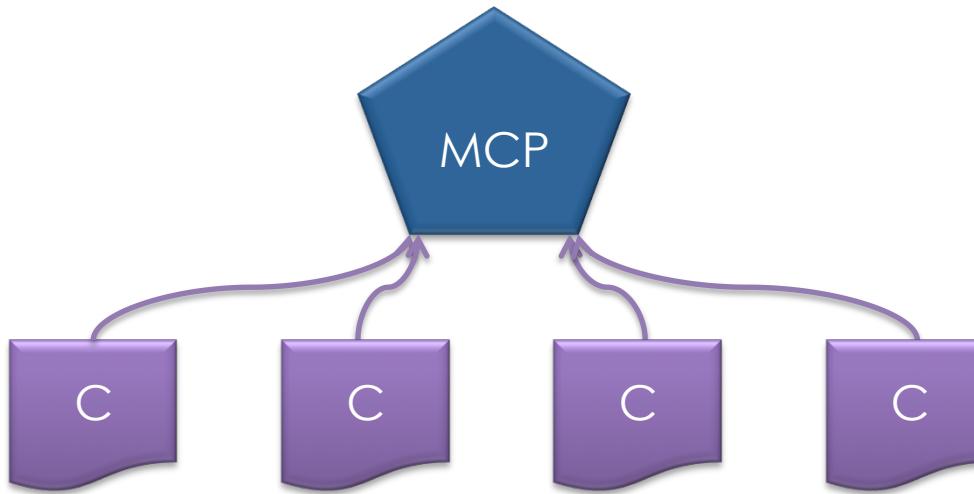
# Pronghorn Example

Input  
File



Contract queue:

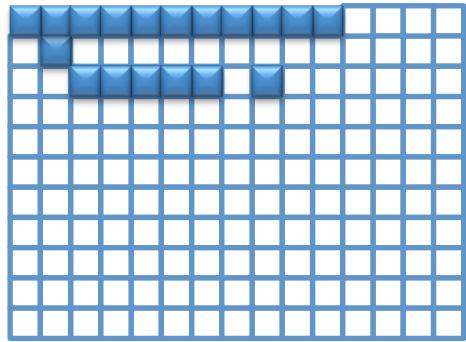
/mnt/point/512:mnt-ntfs/1  
/mnt/point/512:mnt-ntfs/2  
/mnt/point/512:mnt-ntfs/3  
/mnt/point/512:mnt-ntfs/4



Reported back to MCP, state tracked

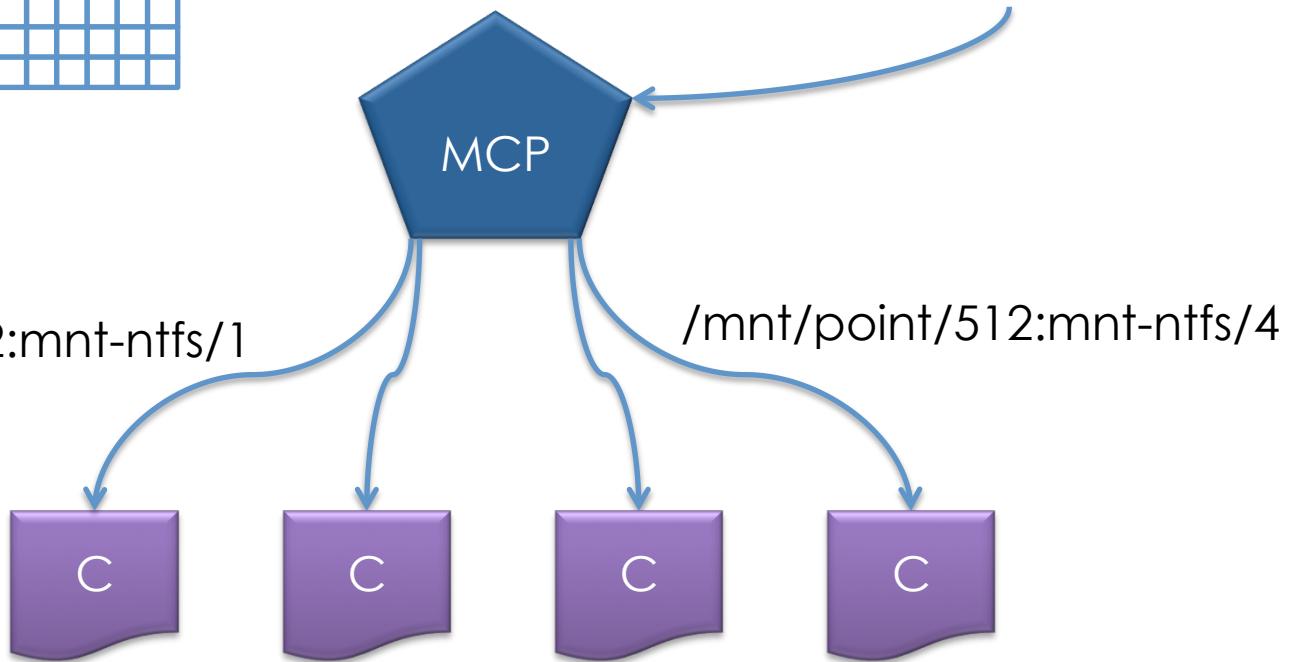
# Pronghorn Example

Input  
File:



/mnt/point/512:mnt-ntfs/1

Contract queue:  
/mnt/point/512:mnt-ntfs/1  
/mnt/point/512:mnt-ntfs/2  
/mnt/point/512:mnt-ntfs/3  
/mnt/point/512:mnt-ntfs/4



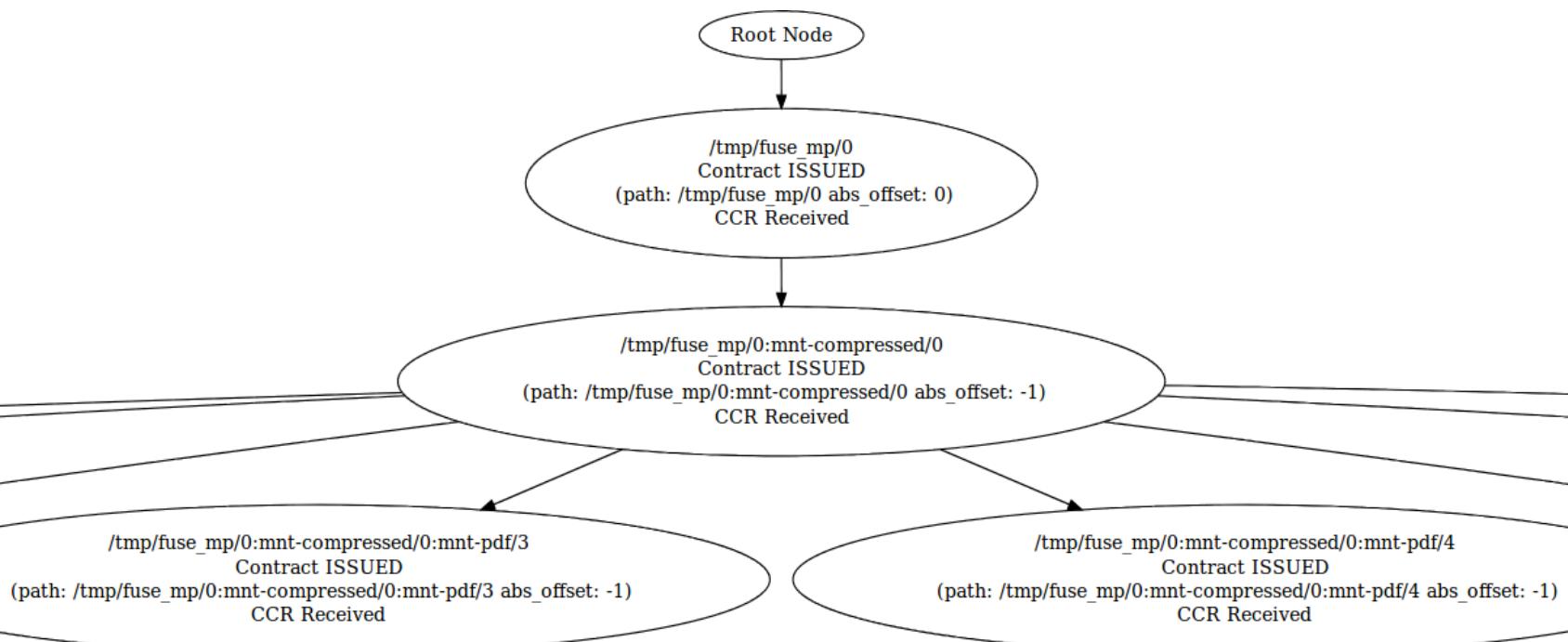
New contracts issued, queued first

# Pronghorn Example

- Demo Time
  - Install:
    - cmake .
    - make
    - sudo make install (optional)

# Some Features

- Intelligent un-mounting



# Some Features

- All over zeroMQ at runtime (can dynamically get/set)
- Has the basics:
  - general.log\_verbosity=ERROR
- And some less basic (but very handy) options:
  - subcontractor\_sleuth.valgrind\_opts=/usr/bin/valgrind, --log-file=/tmp/sk.log

# Pronghorn Summary



- Use Cases
- Easily Extensible
- Nested Fuse
- Concurrent

# Challenge Results

- Didn't win...



Cheetah Run by Mark Dumont and made available under a Creative Commons 2.0 Attribution license, retrieved from: <http://www.flickr.com/photos/wcdumonts/7400969208/>

Pronghorn Antelope by George Ulrich and made available under a Creative Commons 2.0 Attribution license, retrieved from: <http://www.flickr.com/photos/birdwatcher/323815066/>

# Conclusions

- **Don't** run this on any machine you care about!
- BUT
- Pronghorn explored some new concepts, pushed a few boundaries, hopefully produced a useful tool!



Australian Government  
Department of Defence



# Questions?

[dsd.gov.au](http://dsd.gov.au)



Australian Government  
Department of Defence



The End.

[dsd.gov.au](http://dsd.gov.au)

# Squid Redirection



- Allows redirection / rewriting of URLs via an external program
  - Squid passes requests to arbitrary program
- Of “upside-down-ternet” fame

- Start at the first FUSE mount
- Remembering the ZIP example
  - Assume we have a library that can operate on “files”
  - We rawmount the input and present the library with a “file”