FIRMWARE REVERSE ANALYSIS KONSOLE



RED BALLOON SECURITY

{ Ang Cui | a@redballoonsecurity.com }
www.redballoonsecurity.com

WHO AM I

WHAT DO I DO

5TH YEAR PH.D. CANDIDATE
INTRUSION DETECTION SYSTEMS LAB
COLUMBIA UNIVERSITY

WHO AM I
WHAT DO I DO

5TH YEAR PH.D. CANDIDATE
INTRUSION DETECTION SYSTEMS LAB
COLUMBIA UNIVERSITY

CO-FOUNDER AND CEO
RED BALLOON SECURITY INC.
WWW.REDBALLOONSECURITY.COM

WHO AM I
WHAT DO I DO

WHO AM I WHAT DO I DO

5TH YEAR PH.D. CANDIDATE
INTRUSION DETECTION SYSTEMS LAB
COLUMBIA UNIVERSITY

CO-FOUNDER AND CEO
RED BALLOON SECURITY INC.
WWW.REDBALLOONSECURITY.COM

PAST PUBLICATIONS:

- PERVASIVE INSECURITY OF EMBEDDED NETWORK DEVICES. [RAID10]
- A QUANTITATIVE ANALYSIS OF THE INSECURITY OF EMBEDDED NETWORK DEVICES. [ACSAC10]
- KILLING THE MYTH OF CISCO IOS DIVERSITY: TOWARDS RELIABLE LARGE-SCALE EXPLOITATION OF CISCO IOS. [USENIX WOOT 11]
- DEFENDING LEGACY EMBEDDED SYSTEMS WITH SOFTWARE SYMBIOTES. [RAID11]
- FROM PREY TO HUNTER: TRANSFORMING LEGACY EMBEDDED DEVICES INTO EXPLOITATION SENSOR GRIDS. [ACSAC11]

WHO AM I WHAT DO I DO

5TH YEAR PH.D. CANDIDATE
INTRUSION DETECTION SYSTEMS LAB
COLUMBIA UNIVERSITY

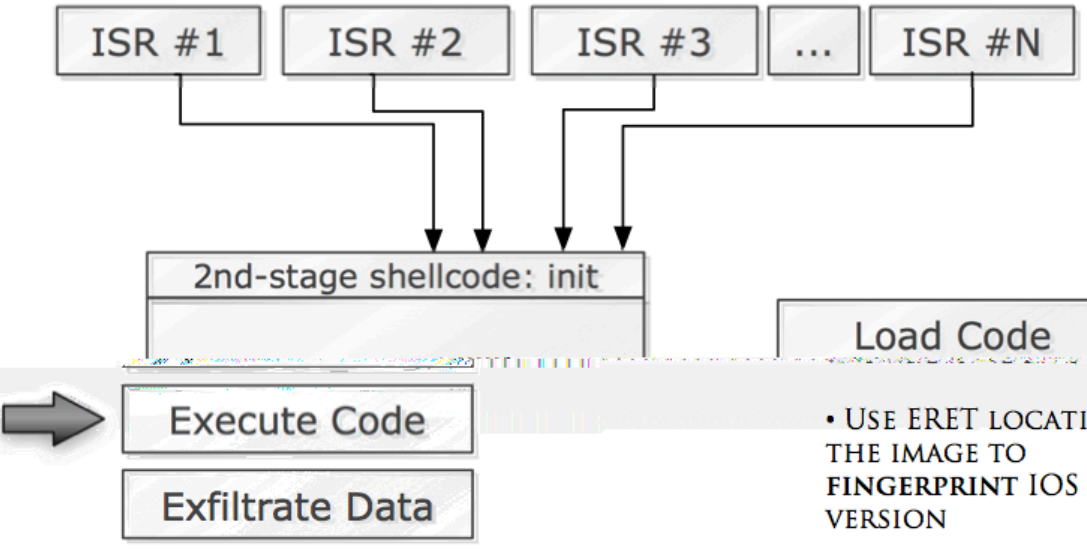
CO-FOUNDER AND CEO
RED BALLOON SECURITY INC.
WWW.REDBALLOONSECURITY.COM

PAST EMBEDDED TINKERINGS:

- INTERRUPT-HIJACK CISCO IOS ROOTKIT

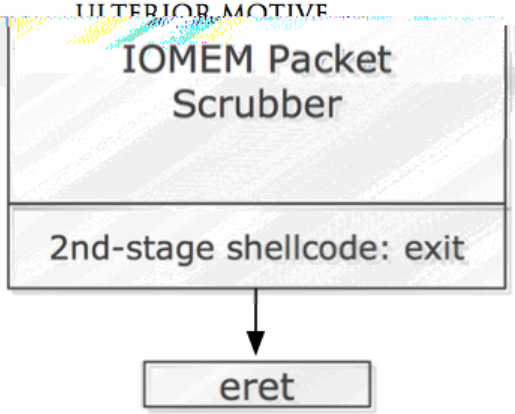
Interrupt-Hijack Rootkit
[BlackHat USA 2011]

- 2nd-stage: Exception Hijack and IOMEM snooping



- The (MIPS) ERET, or Exception-Return is an architecture invariant
- ISR **entry** point is a **binary** invariant, typically found at 0x600080180, etc
- Can just hijack entry point, but there is an ulterior motive

- Use ERET locations in the image to **fingerprint** IOS version



Interrupt-Hijack shellcode frees us from the tyrannies of the watchdog timer.

Perpetual, stealthy execution!

WHO AM I WHAT DO I DO

5TH YEAR PH.D. CANDIDATE
INTRUSION DETECTION SYSTEMS LAB
COLUMBIA UNIVERSITY

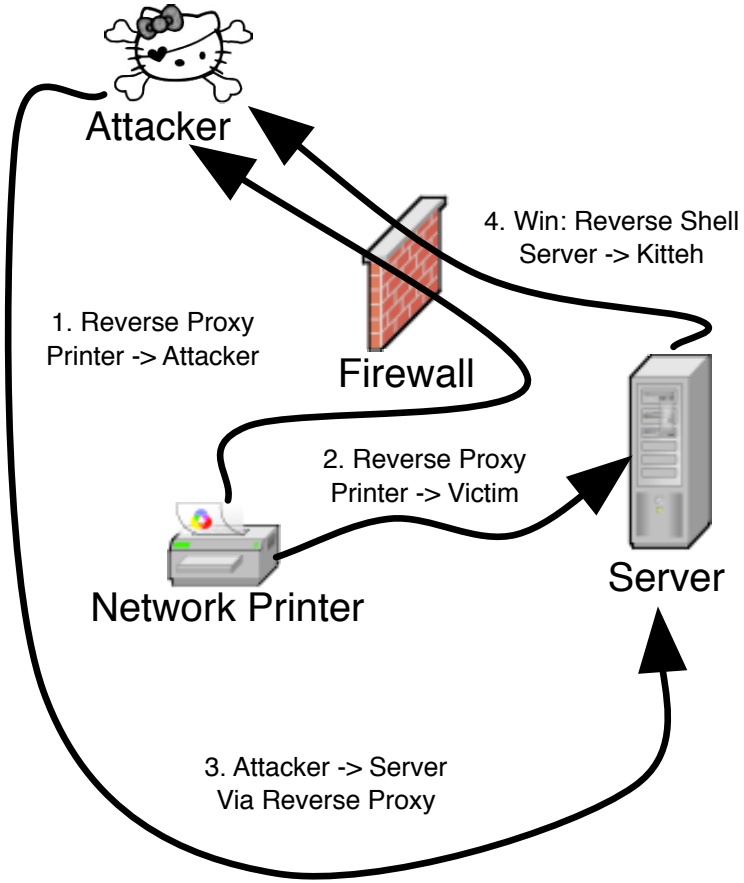
CO-FOUNDER AND CEO
RED BALLOON SECURITY INC.
WWW.REDBALLOONSECURITY.COM

PAST EMBEDDED TINKERINGS:

- INTERRUPT-HIJACK CISCO IOS ROOTKIT
- HP LASERJET PRINTER ROOTKIT

HP-RFU Vulnerability
HP LaserJet 2550 Rootkit
[28C3]





WORKFLOW

[Cisco IOS ROOTKIT]

WORKFLOW

[Cisco IOS ROOTKIT]

[HP LaserJet Rootkit]

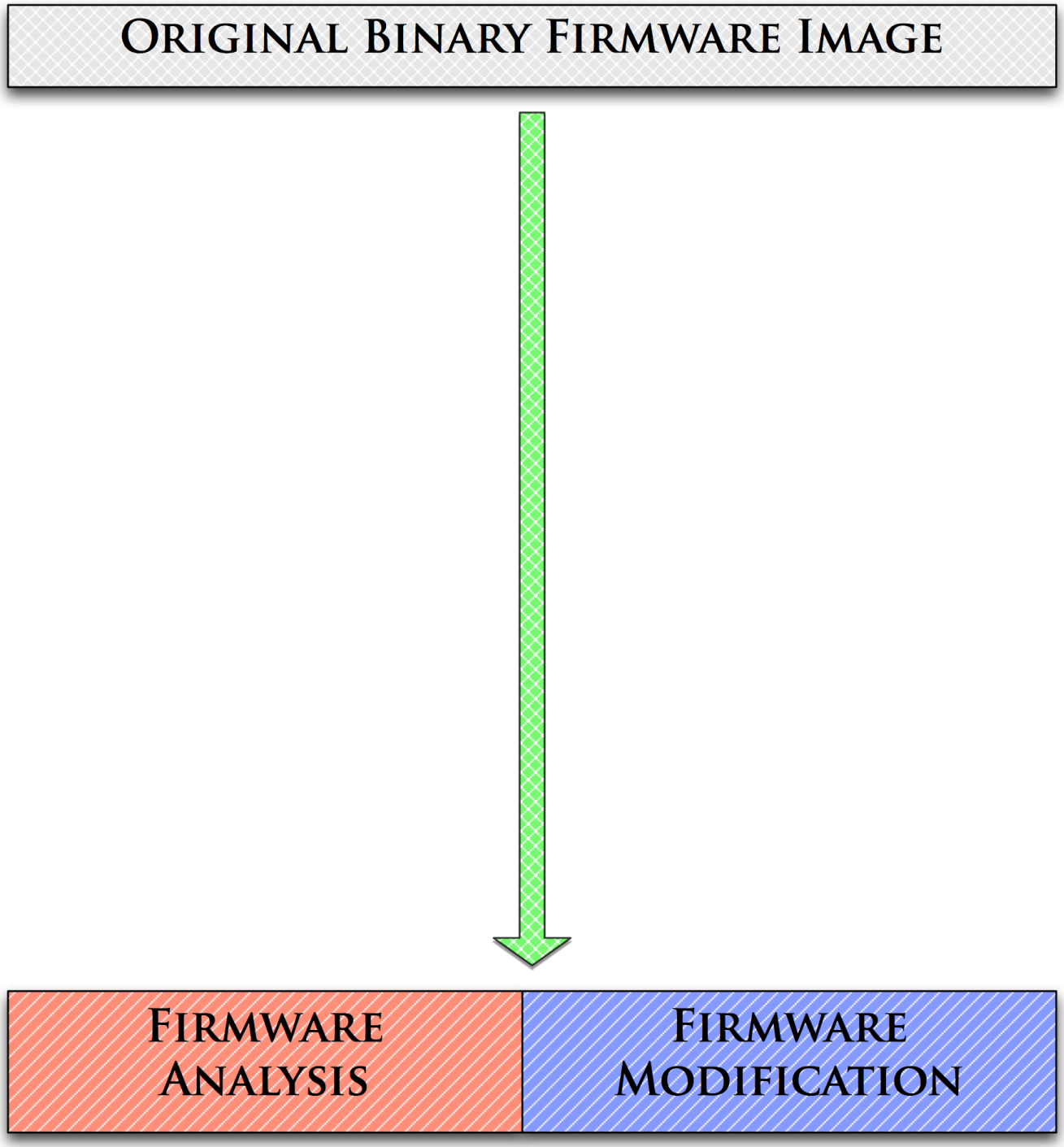
WORKFLOW

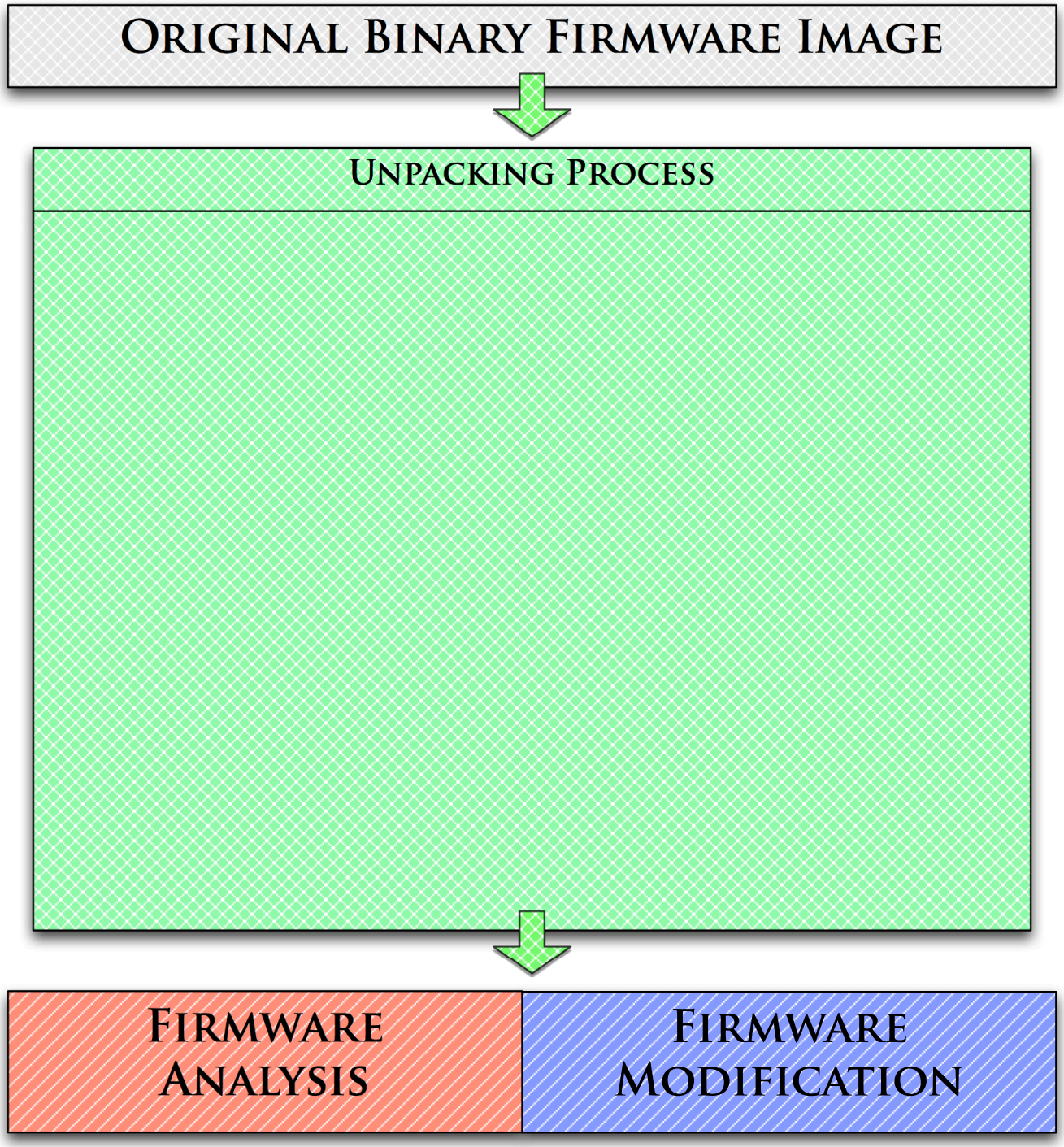
[Cisco IOS ROOTKIT]

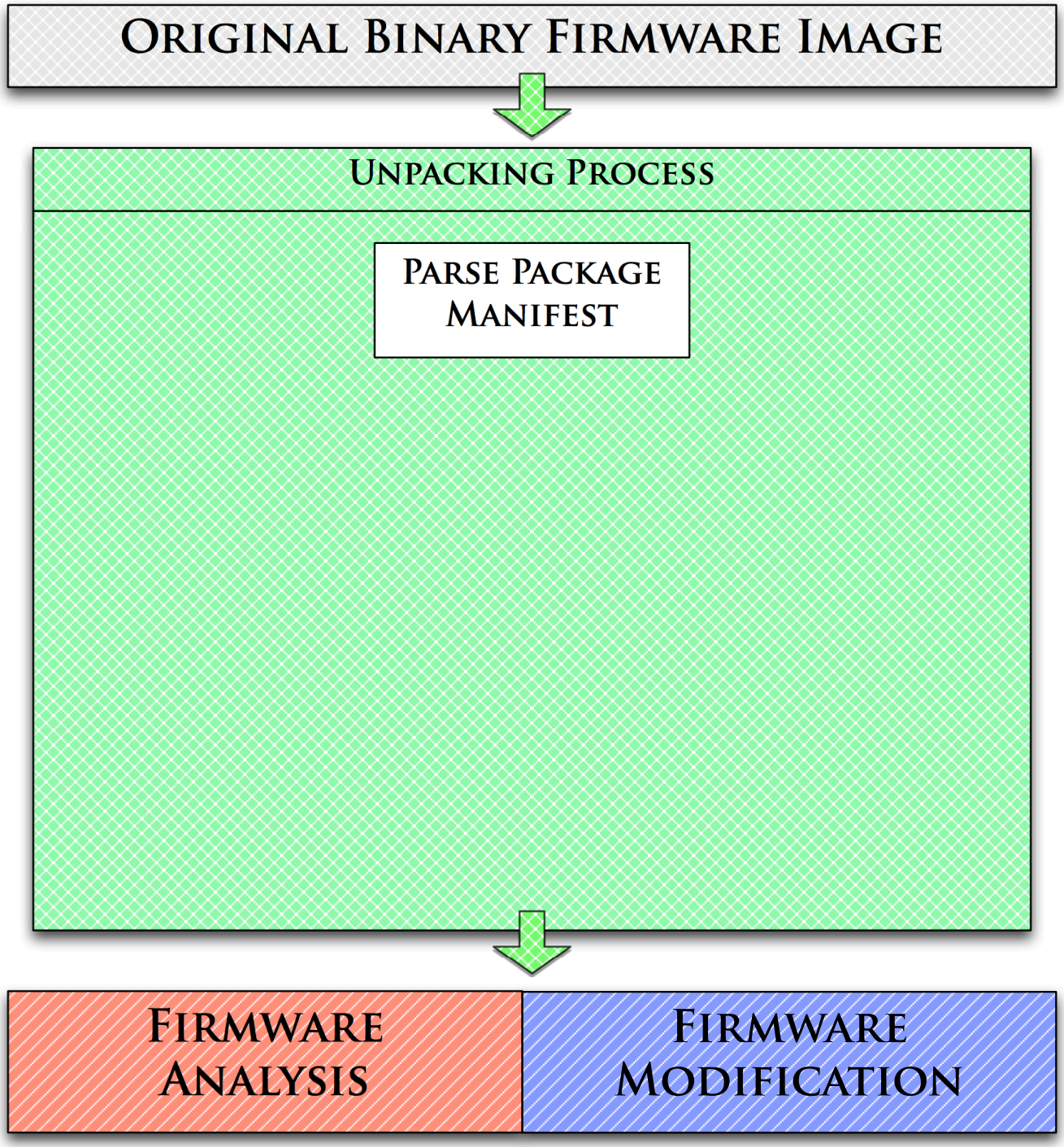
[HP LaserJet Rootkit]

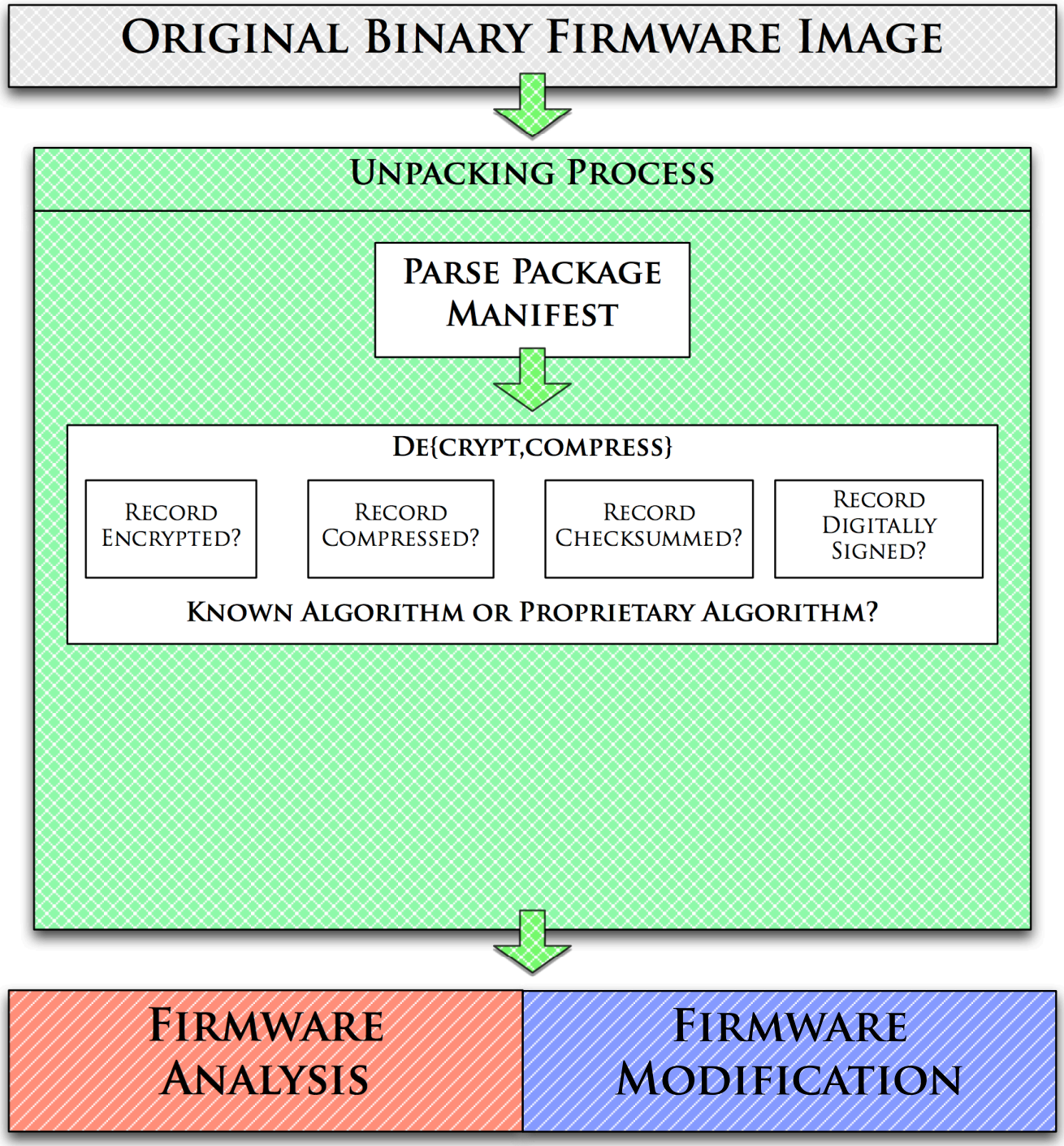
[Software Symbiotes for Routers, Phones, Printers]

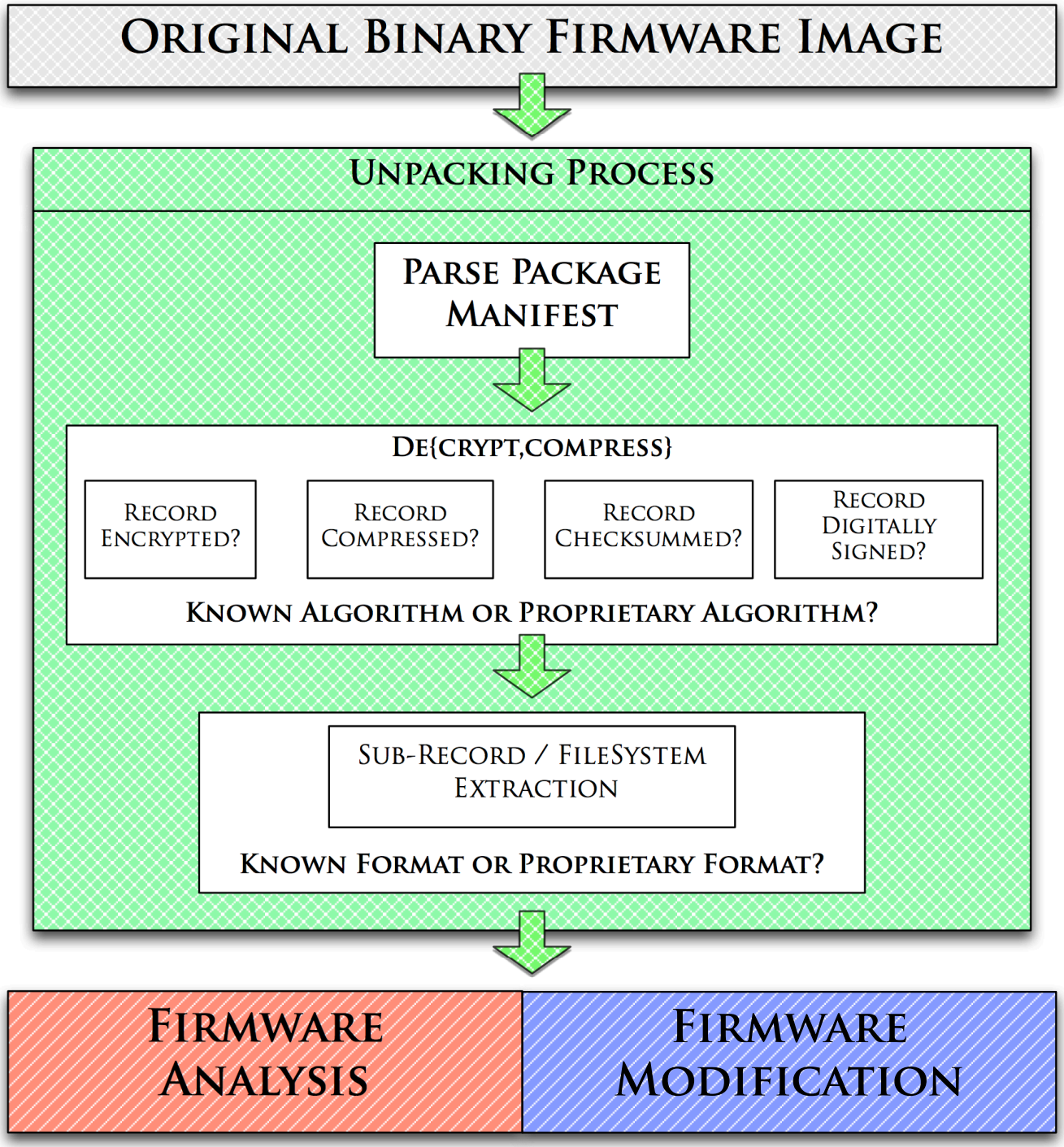
Original Binary Firmware Image

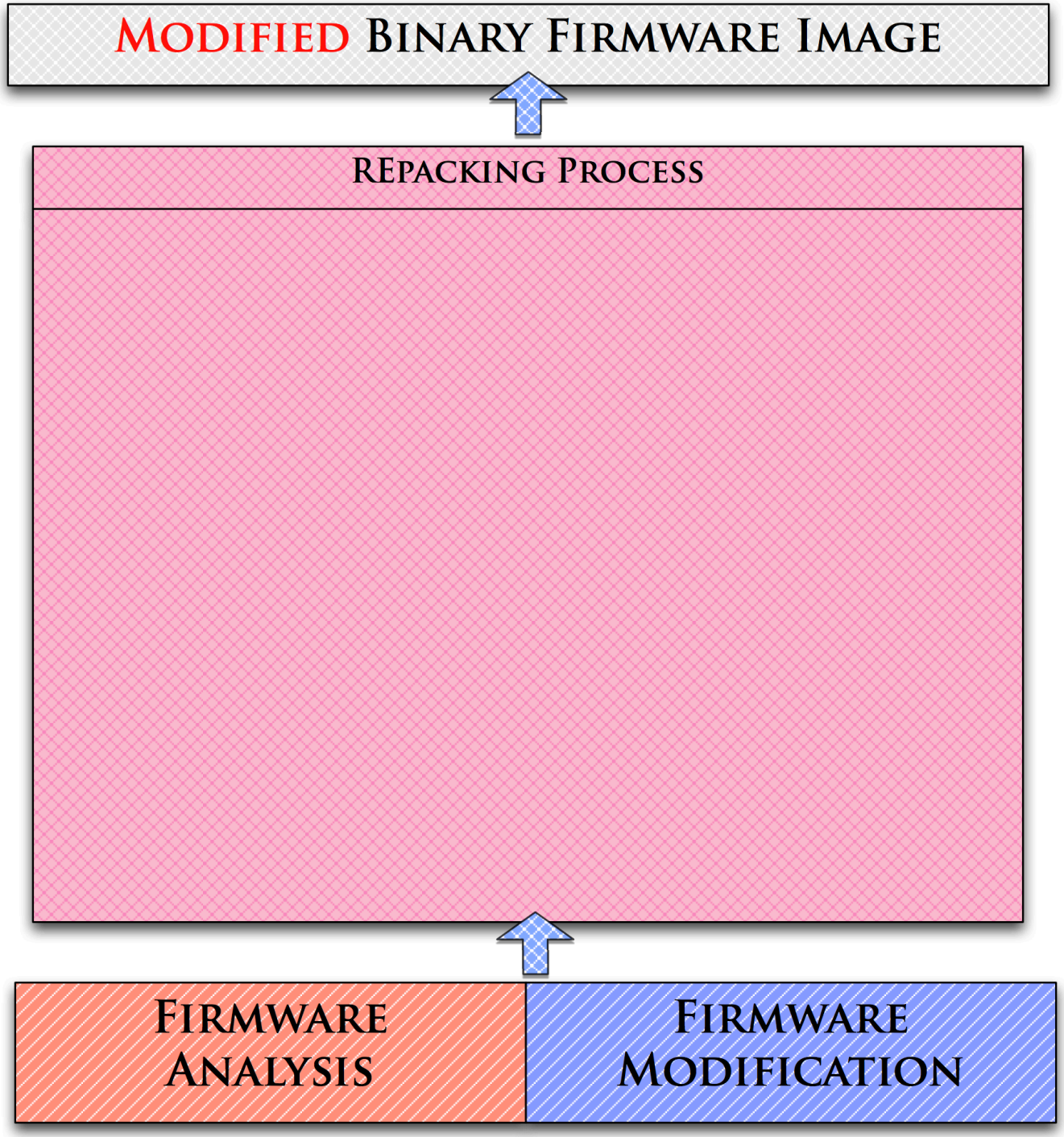

Original Binary Firmware Image
Firmware Analysis
Firmware Modification

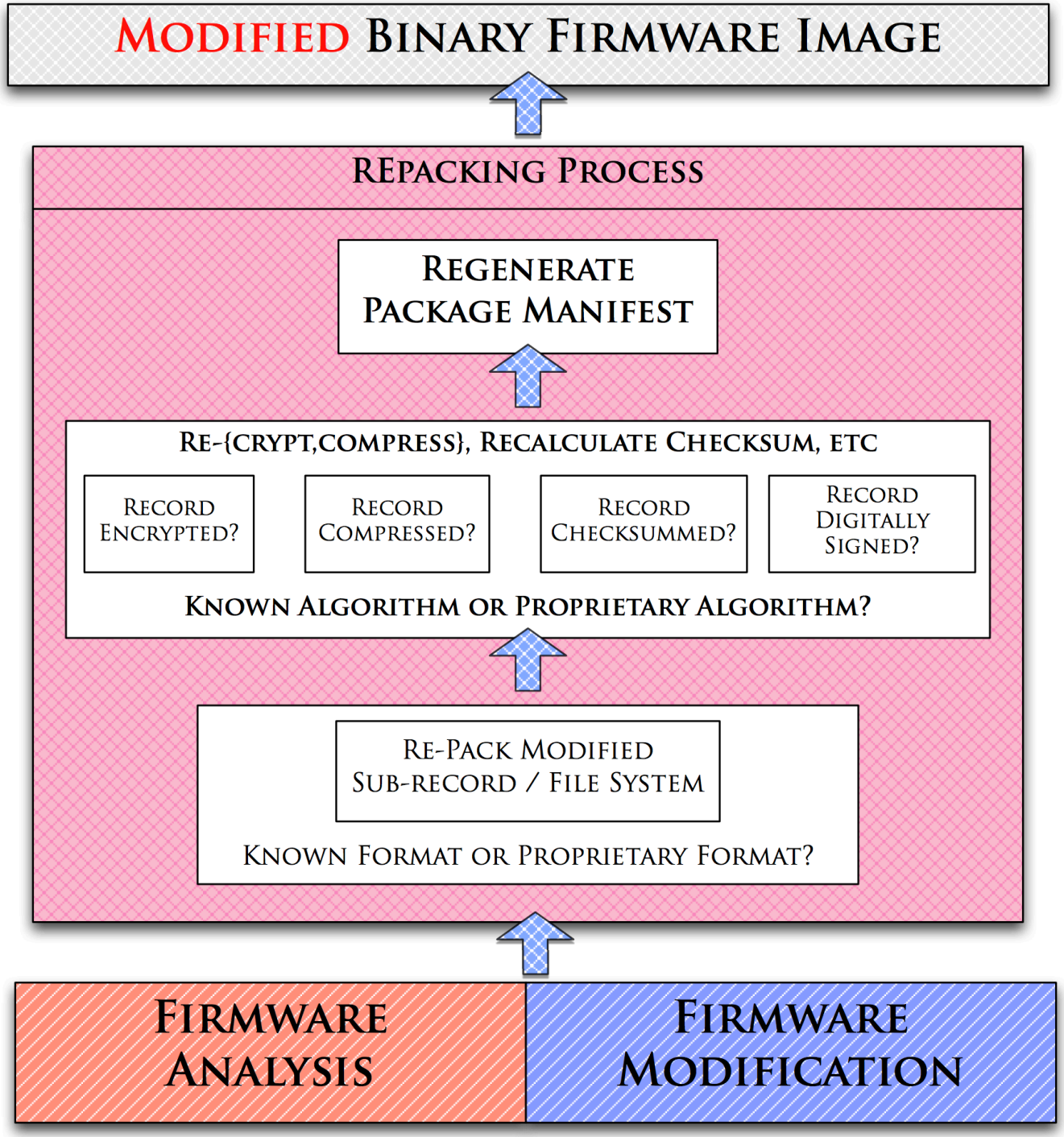

Original Binary Firmware Image
Unpacking Process
Firmware Analysis
Firmware Modification


Original Binary Firmware Image
Unpacking Process
Parse Package Manifest
Firmware Analysis
Firmware Modification


Original Binary Firmware Image
Unpacking Process
Parse Package Manifest
De{crypt,compress}
Record Encrypted?
Record Compressed?
Record Checksummed?
Record Digitally Signed?
Known Algorithm or Proprietary Algorithm?
Firmware Analysis
Firmware Modification

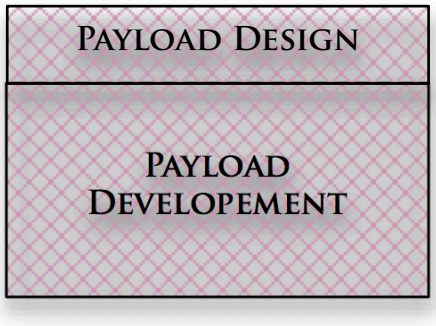

Original Binary Firmware Image
Unpacking Process
Parse Package Manifest
De{crypt,compress}
Record Encrypted?
Record Compressed?
Record Checksummed?
Record Digitally Signed?
Known Algorithm or Proprietary Algorithm?
Sub-Record / FileSystem Extraction
Known Format or Proprietary Format?
Firmware Analysis
Firmware Modification


Modified Binary Firmware Image
Repacking Process
Firmware Analysis
Firmware Modification

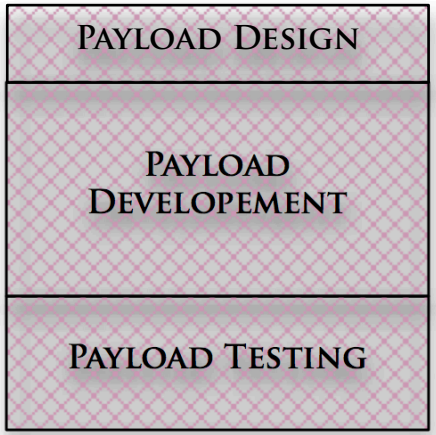

Modified Binary Firmware Image
REpacking Process
Regenerate Package Manifest
Re-{crypt,compress}, Recalculate Checksum, etc
Record Encrypted?
Record Compressed?
Record Checksummed?
Record Digitally Signed?
Known Algorithm or Proprietary Algorithm?
Re-Pack Modified Sub-record / File System
Known Format or Proprietary Format?
Firmware Analysis
Firmware Modification

Reasons why Ang stays home on Friday night

Reasons why Ang stays home on Friday night



Reasons why Ang stays home on Friday night



Reasons why Ang stays home on Friday night

Payload Design

Payload Developement

Payload Testing

STARE

@

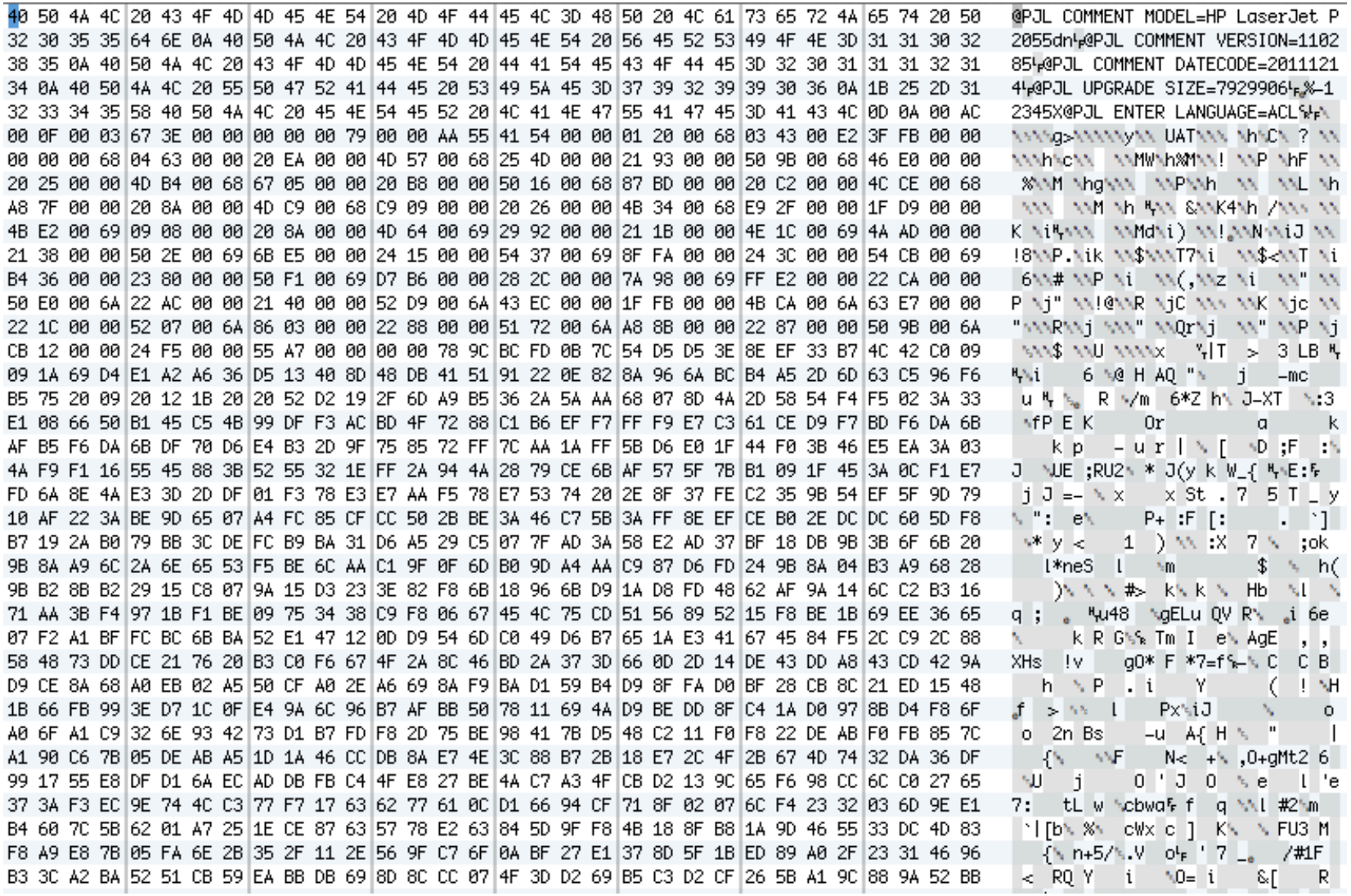
BINARY

BLOB

Reasons why Ang stays home on Friday night

frak.redballoonsecurity.com

a@redballoonsecurity.com



SUCH MYSTERY!

Payload Design

Payload Developement

Payload Testing

STARE

@

BINARY

BLOB



THIS PART



Payload Design

Payload Developement

Payload Testing

STARE

@

BINARY

BLOB



This part Is IMPORTANT

FRAK

IRMWARE EVERSE NALYSIS ONSOLE

[Better Living Through Software Engineering]

Payload Design

Payload Developement

Payload Testing

STARE

@

BINARY

BLOB



THIS PART



FRAK

IRMWARE EVERSE NALYSIS ONSOLE

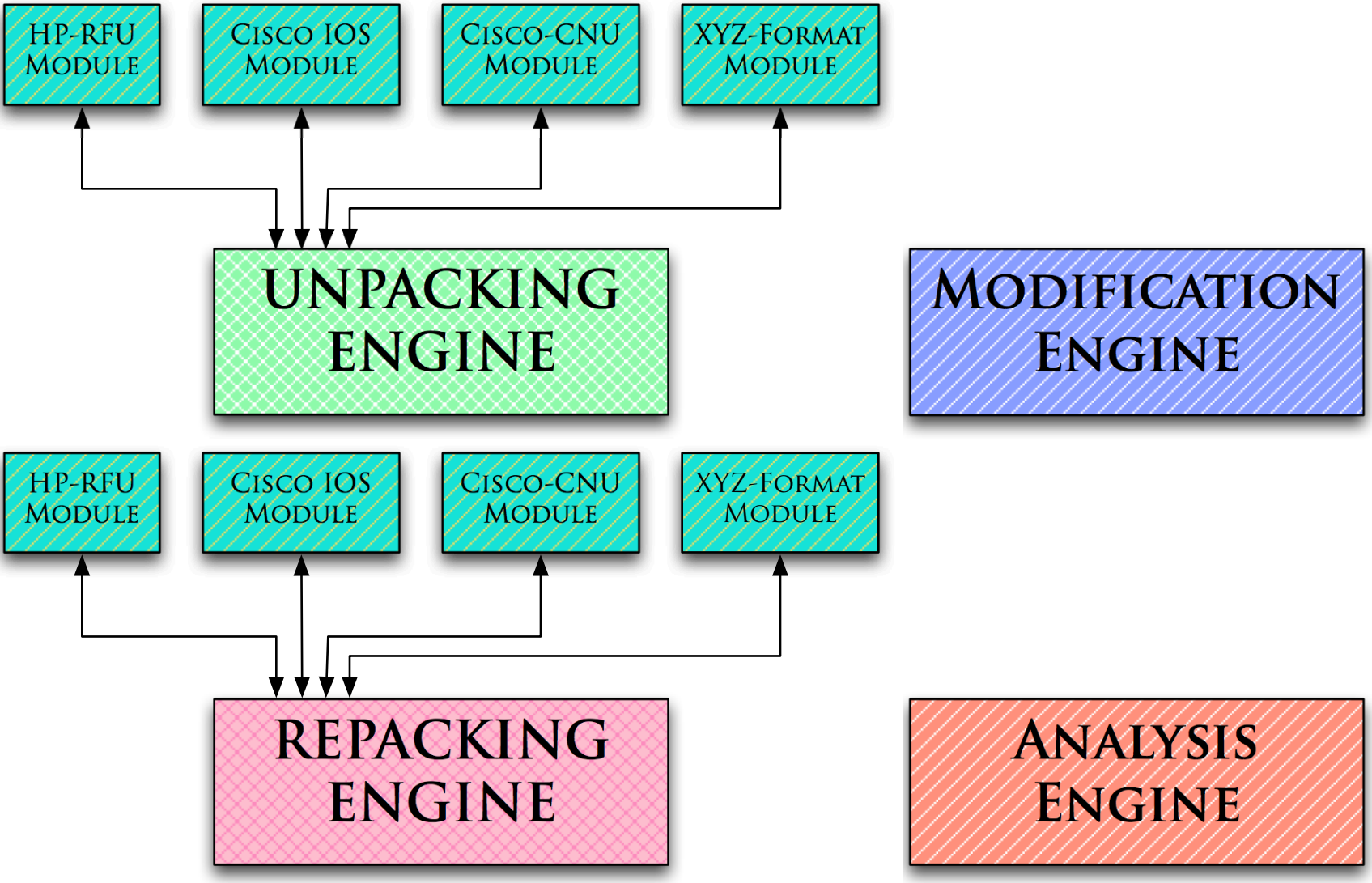
UNPACKING ENGINE

MODIFICATION ENGINE

REPACKING ENGINE

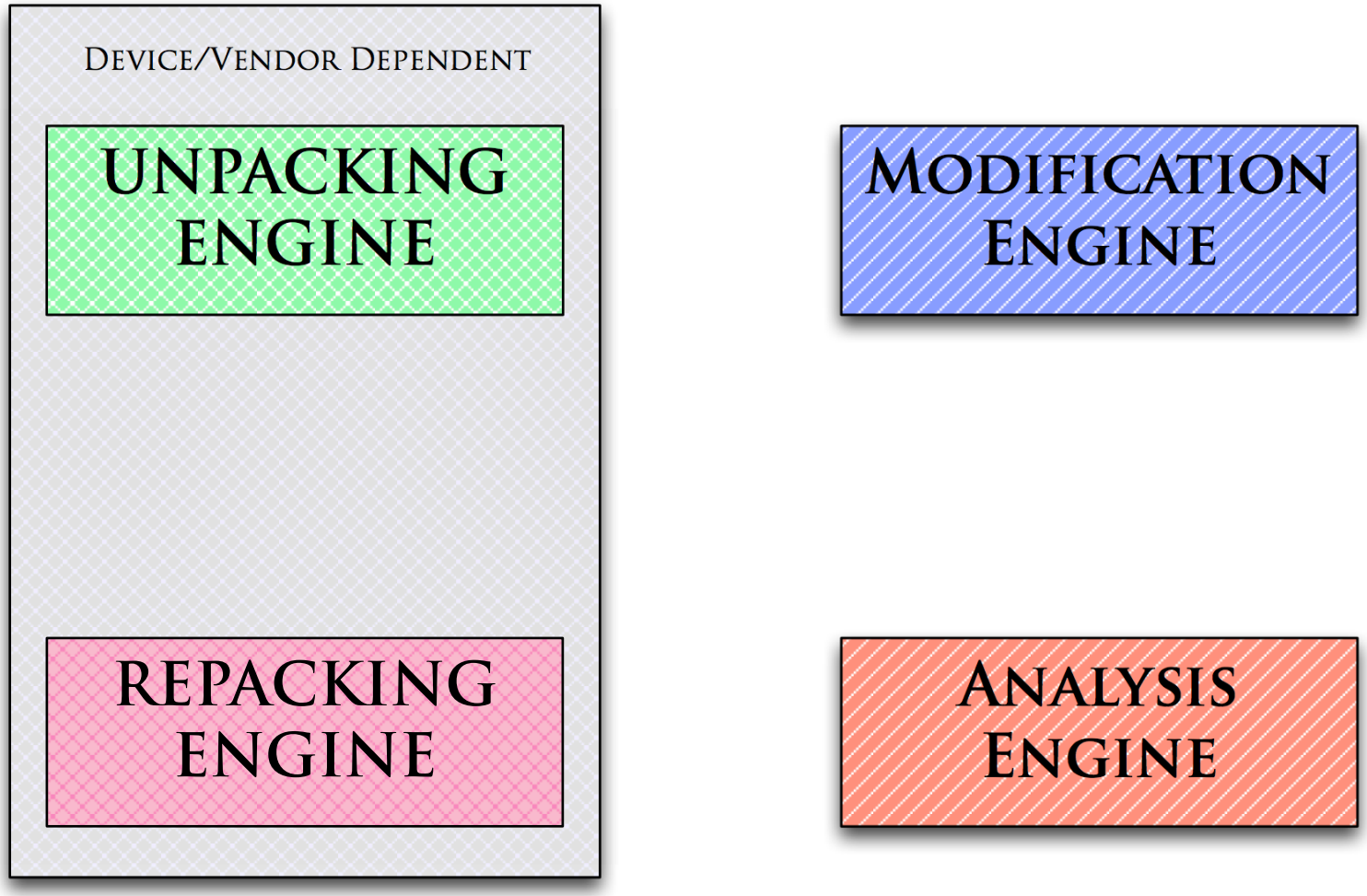
ANALYSIS ENGINE

FRAK
FIRMWARE EVERSE NALYSIS ONSOLE



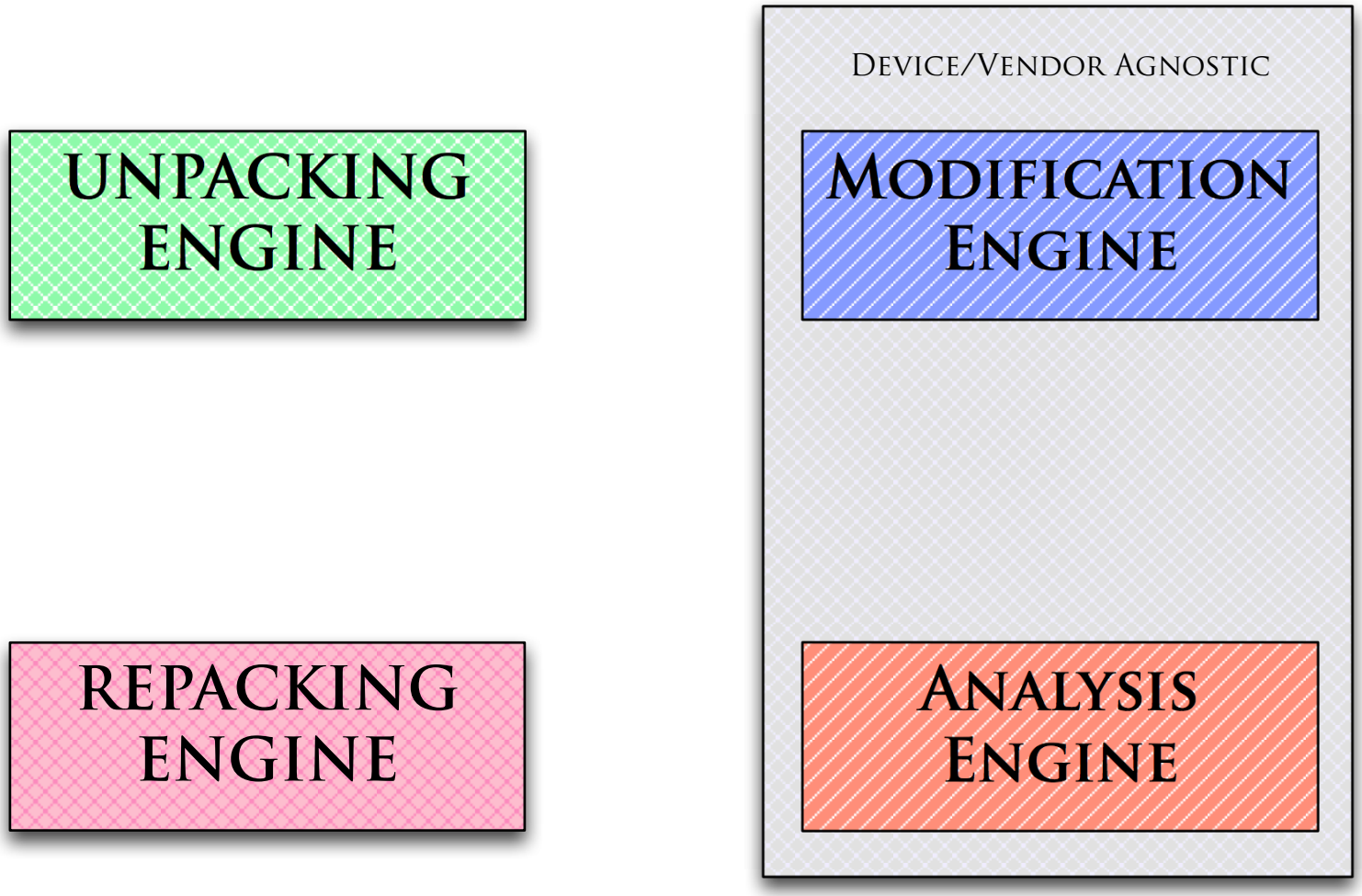
FRAK

FIRMWARE REVERSE ANALYSIS TOOLKIT



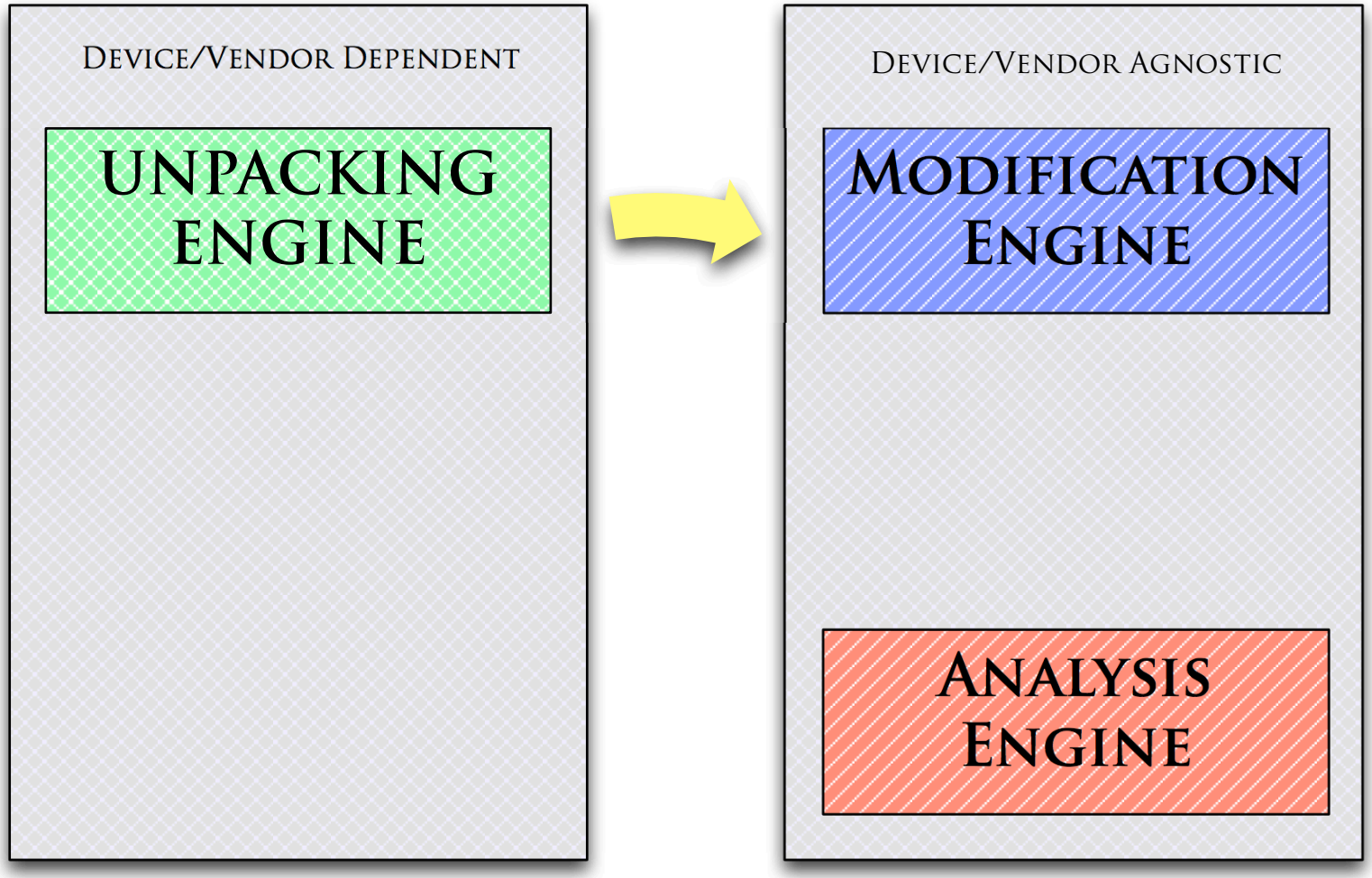
FRAK

FIRMWARE EVERSE NALYSIS ONSOLE

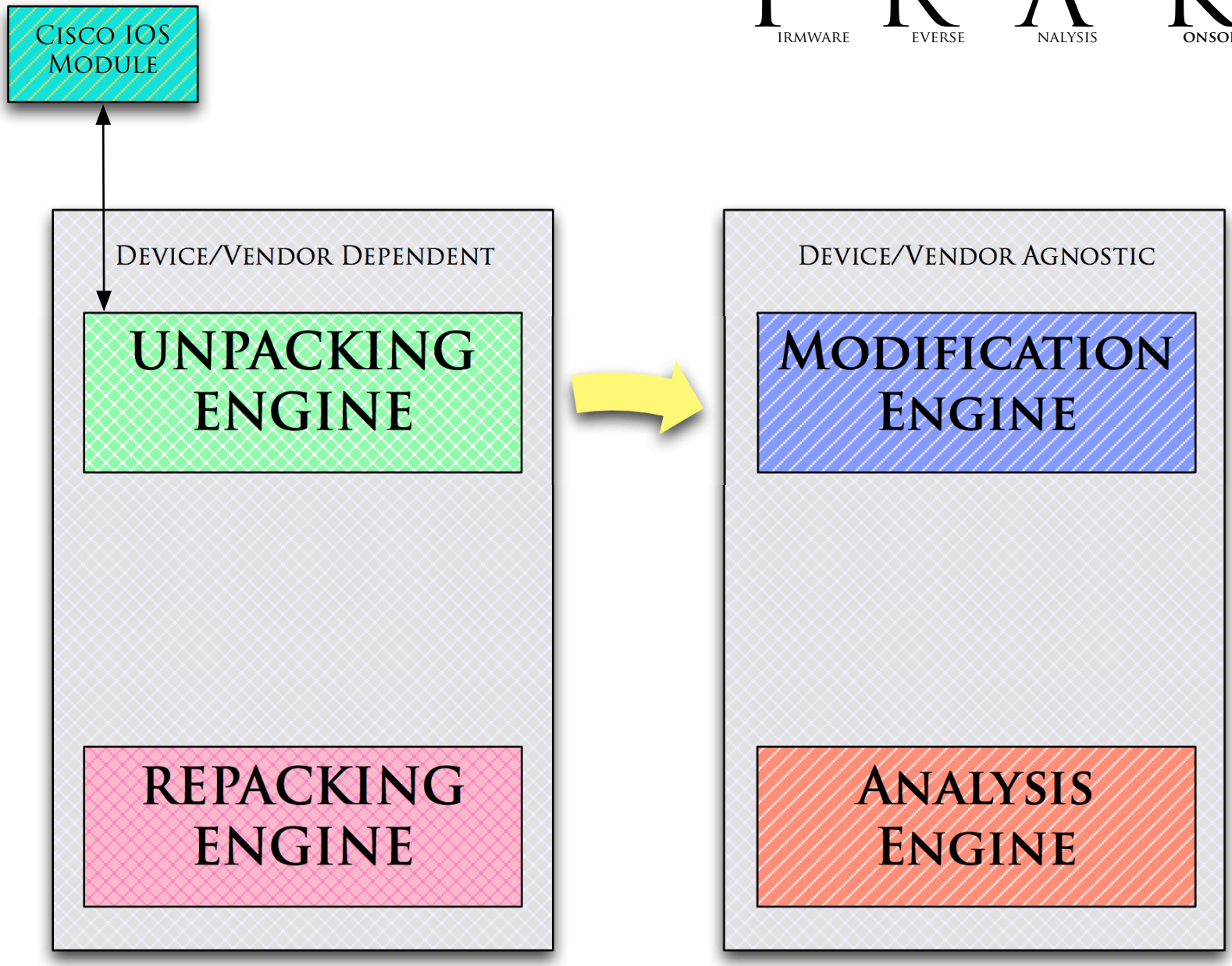


FRAK

FIRMWARE REVERSE ANALYSIS KONSOLE

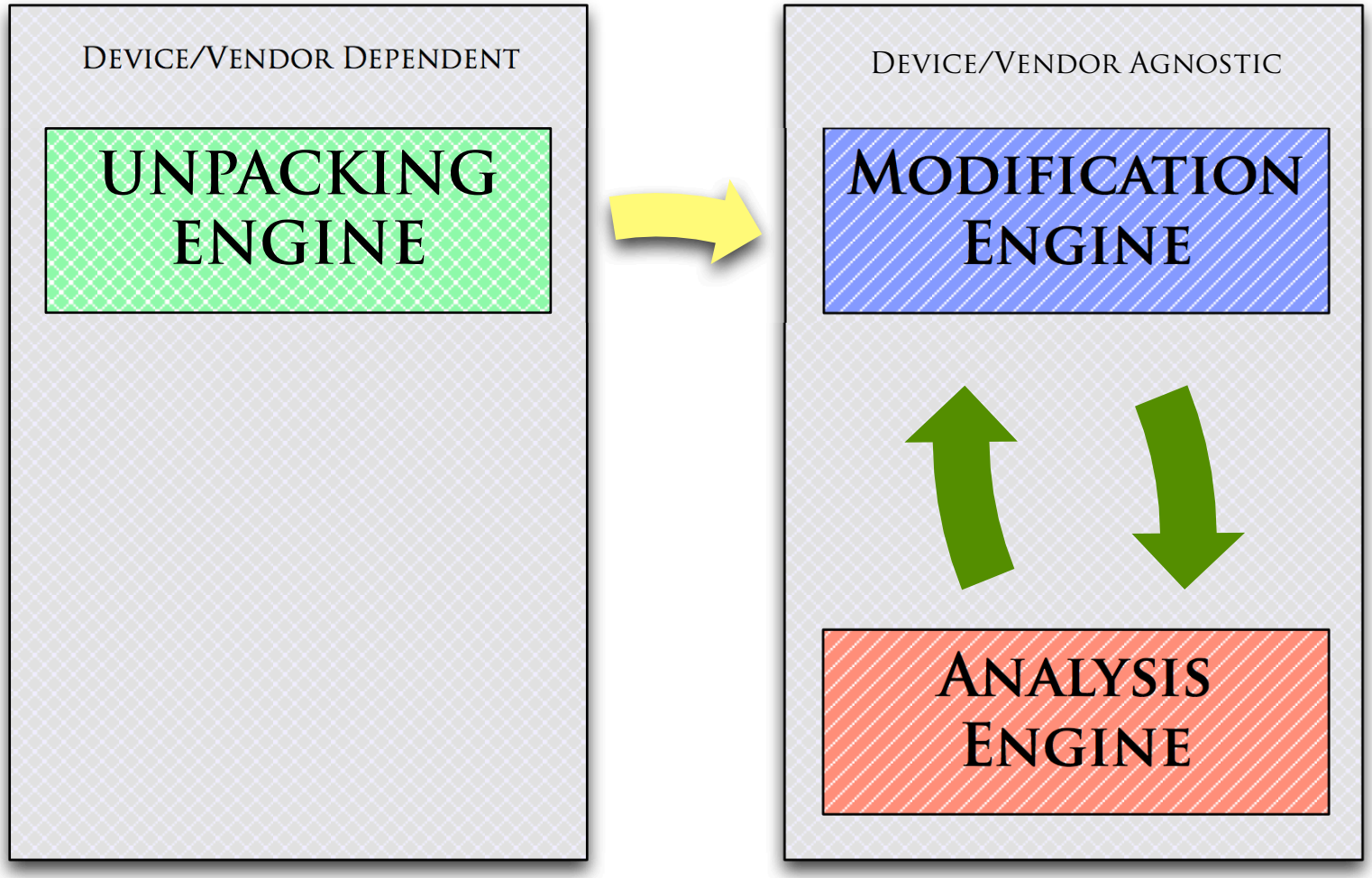


FRAK
FIRMWARE REVERSE ANALYSIS KONSOLE



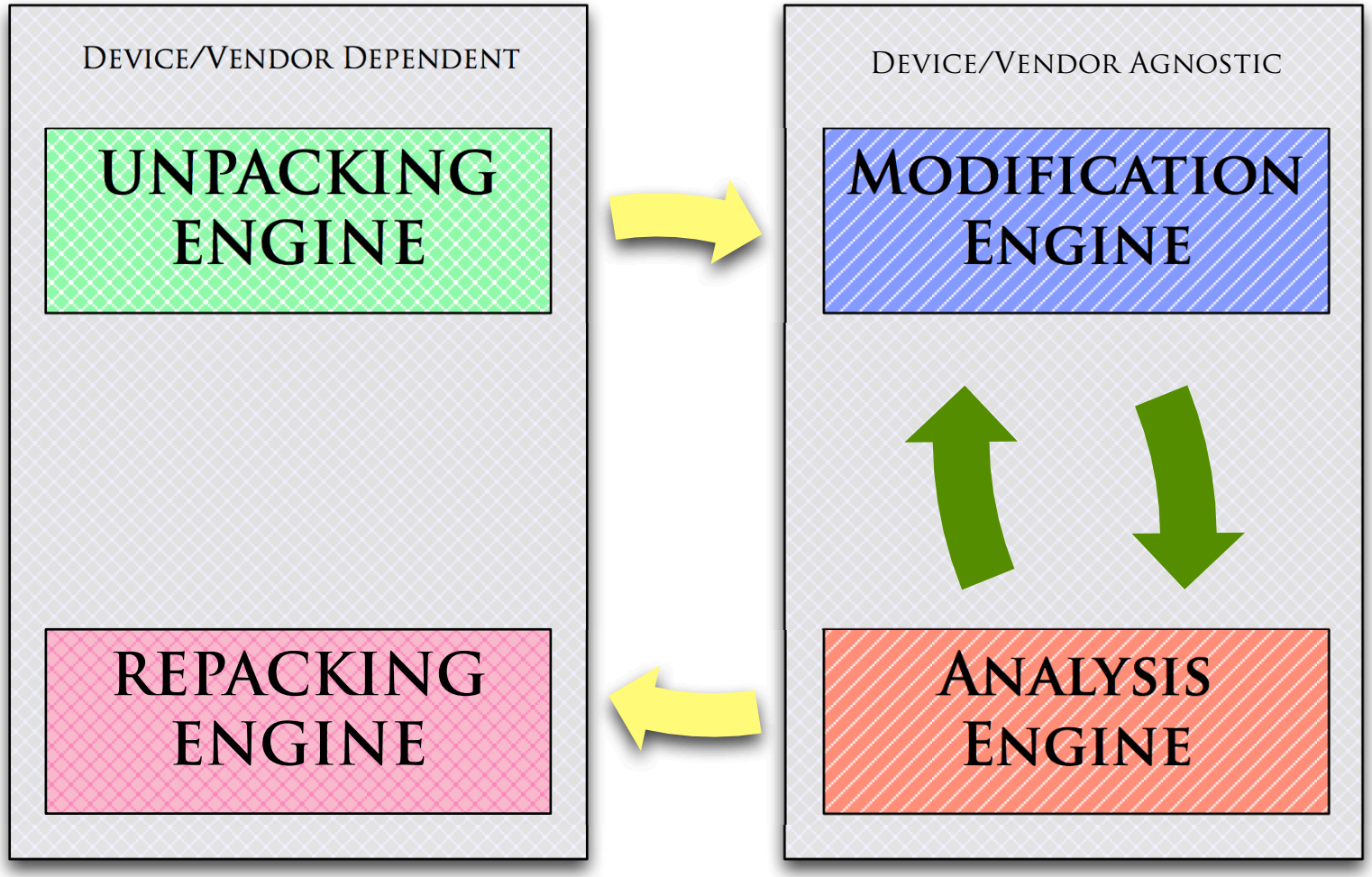
FRAK

FIRMWARE REVERSE ANALYSIS KONSOLE



FRAK

FIRMWARE REVERSE ANALYSIS KONSOLE



FRAK

IRMWARE EVERSE NALYSIS ONSOLE

[Better Living Through Software Integration]

FRAK

IRMWARE EVERSE NALYSIS ONSOLE

[Better Living Through Software Integration]



F R A K

IRMWARE EVERSE NALYSIS ONSOLE

[Better Living Through Software Integration]





F R A K

IRMWARE EVERSE NALYSIS ONSOLE

[Better Living Through Software Integration]

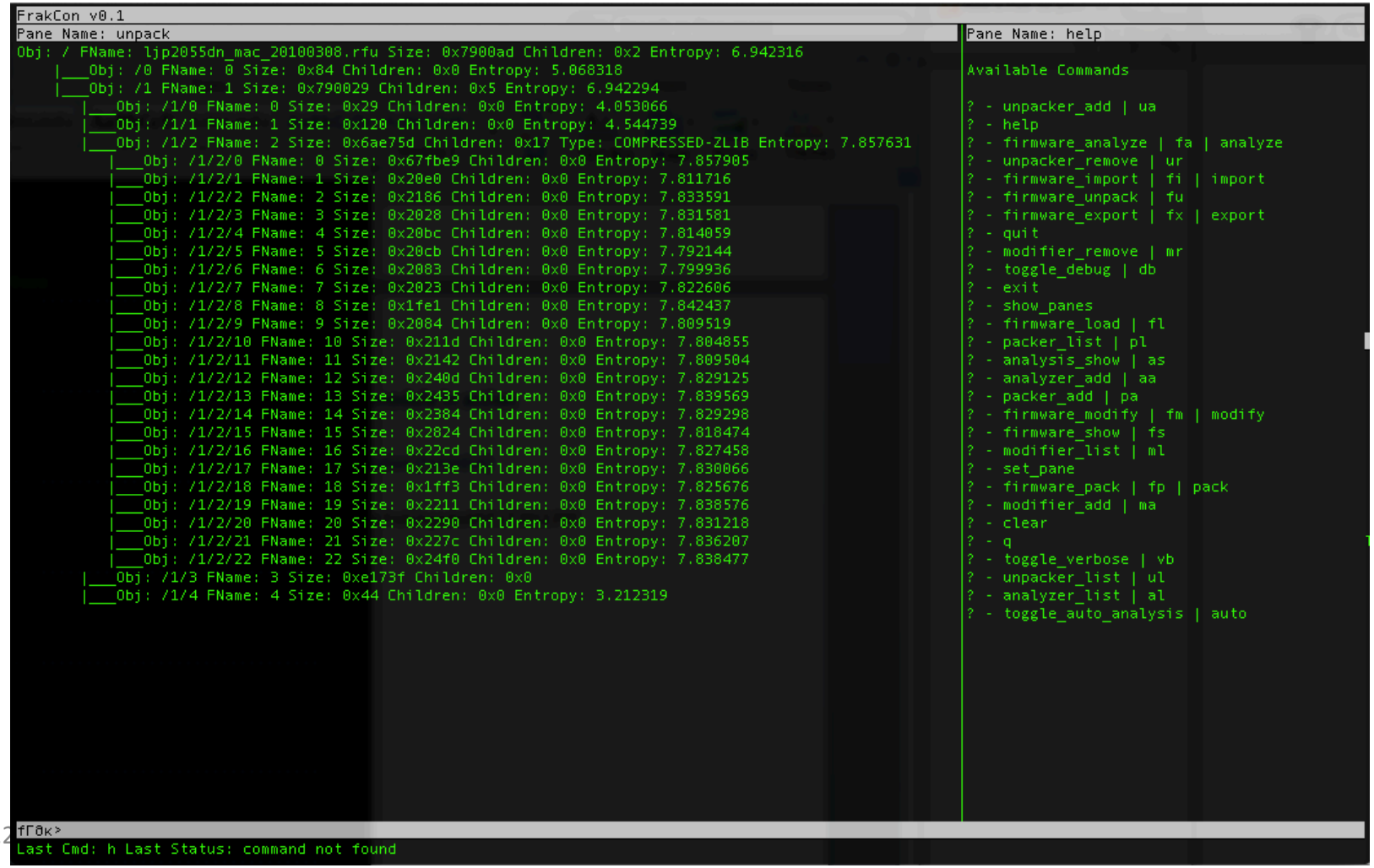






More integration on the way

KONSOLE


FrakCon v0.1
Pane Name: unpack
Obj: / FName: ljp2055dn_mac_20100308.rfu Size: 0x7900ad Children: 0x2 Entropy: 6.942316
|___Obj: /0 FName: 0 Size: 0x84 Children: 0x0 Entropy: 5.068318
|___Obj: /1 FName: 1 Size: 0x790029 Children: 0x5 Entropy: 6.942294
|___Obj: /1/0 FName: 0 Size: 0x29 Children: 0x0 Entropy: 4.053066
|___Obj: /1/1 FName: 1 Size: 0x120 Children: 0x0 Entropy: 4.544739
|___Obj: /1/2 FName: 2 Size: 0x6ae75d Children: 0x17 Type: COMPRESSED-ZLIB Entropy: 7.857631
|___Obj: /1/2/0 FName: 0 Size: 0x67fbe9 Children: 0x0 Entropy: 7.857905
|___Obj: /1/2/1 FName: 1 Size: 0x20e0 Children: 0x0 Entropy: 7.811716
|___Obj: /1/2/2 FName: 2 Size: 0x2186 Children: 0x0 Entropy: 7.833591
|___Obj: /1/2/3 FName: 3 Size: 0x2028 Children: 0x0 Entropy: 7.831581
|___Obj: /1/2/4 FName: 4 Size: 0x20bc Children: 0x0 Entropy: 7.814059
|___Obj: /1/2/5 FName: 5 Size: 0x20cb Children: 0x0 Entropy: 7.792144
|___Obj: /1/2/6 FName: 6 Size: 0x2083 Children: 0x0 Entropy: 7.799936
|___Obj: /1/2/7 FName: 7 Size: 0x2023 Children: 0x0 Entropy: 7.822606
|___Obj: /1/2/8 FName: 8 Size: 0x1fe1 Children: 0x0 Entropy: 7.842437
|___Obj: /1/2/9 FName: 9 Size: 0x2084 Children: 0x0 Entropy: 7.809519
|___Obj: /1/2/10 FName: 10 Size: 0x211d Children: 0x0 Entropy: 7.804855
|___Obj: /1/2/11 FName: 11 Size: 0x2142 Children: 0x0 Entropy: 7.809504
|___Obj: /1/2/12 FName: 12 Size: 0x240d Children: 0x0 Entropy: 7.829125
|___Obj: /1/2/13 FName: 13 Size: 0x2435 Children: 0x0 Entropy: 7.839569
|___Obj: /1/2/14 FName: 14 Size: 0x2384 Children: 0x0 Entropy: 7.829298
|___Obj: /1/2/15 FName: 15 Size: 0x2824 Children: 0x0 Entropy: 7.818474
|___Obj: /1/2/16 FName: 16 Size: 0x22cd Children: 0x0 Entropy: 7.827458
|___Obj: /1/2/17 FName: 17 Size: 0x213e Children: 0x0 Entropy: 7.830066
|___Obj: /1/2/18 FName: 18 Size: 0x1ff3 Children: 0x0 Entropy: 7.825676
|___Obj: /1/2/19 FName: 19 Size: 0x2211 Children: 0x0 Entropy: 7.838576
|___Obj: /1/2/20 FName: 20 Size: 0x2290 Children: 0x0 Entropy: 7.831218
|___Obj: /1/2/21 FName: 21 Size: 0x227c Children: 0x0 Entropy: 7.836207
|___Obj: /1/2/22 FName: 22 Size: 0x24f0 Children: 0x0 Entropy: 7.838477
|___Obj: /1/3 FName: 3 Size: 0xe173f Children: 0x0
|___Obj: /1/4 FName: 4 Size: 0x44 Children: 0x0 Entropy: 3.212319
Pane Name: help
Available Commands
? - unpacker_add | ua
? - help
? - firmware_analyze | fa | analyze
? - unpacker_remove | ur
? - firmware_import | fi | import
? - firmware_unpack | fu
? - firmware_export | fx | export
? - quit
? - modifier_remove | mr
? - toggle_debug | db
? - exit
? - show_panes
? - firmware_load | fl
? - packer_list | pl
? - analysis_show | as
? - analyzer_add | aa
? - packer_add | pa
? - firmware_modify | fm | modify
? - firmware_show | fs
? - modifier_list | ml
? - set_pane
? - firmware_pack | fp | pack
? - modifier_add | ma
? - clear
? - q
? - toggle_verbose | vb
? - unpacker_list | ul
? - analyzer_list | al
? - toggle_auto_analysis | auto
fΓθk>
Last Cmd: h Last Status: command not found

F R A

IRMWARE EVERSE NALYSIS

FRA

IRMWARE EVERSE NALYSIS

Unpack, Analyze, Modify, Repack: Cisco IOS

```
test_img = "..//test-data/cisco-ios/c7200-a3jk9s-mz.124-25d.bin"
fmObj = FirmwareObject(fName=test_img)
fmObj.registerUnpacker(FrakUnpackerFactory.giveUnpacker("cisco-ios-unpacker"))
fmObj.unpack()
childObj = fmObj.getFirmwareObj("/1")
childObj.registerUnpacker(FrakUnpackerFactory.giveUnpacker("generic-unzip-unpacker"))
childObj.unpack()

meat = fmObj.getFirmwareObj('/1/0')
meat.registerModifier(FrakModifierFactory.giveModifier('cisco-ios-showversion-modifier'))
meat.modify()

childObj.registerPacker(FrakPackerFactory.givePacker("pkzip-packer"))
childObj.pack()

fmObj.registerPacker(FrakPackerFactory.givePacker("cisco-ios-packer"))
result = fmObj.pack()

print "tada!"
```

Payload Design

Payload Developement

Payload Testing

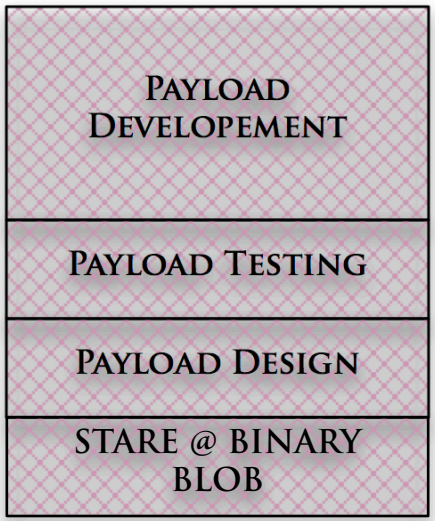
STARE

@

BINARY

BLOB

Without FRAK!

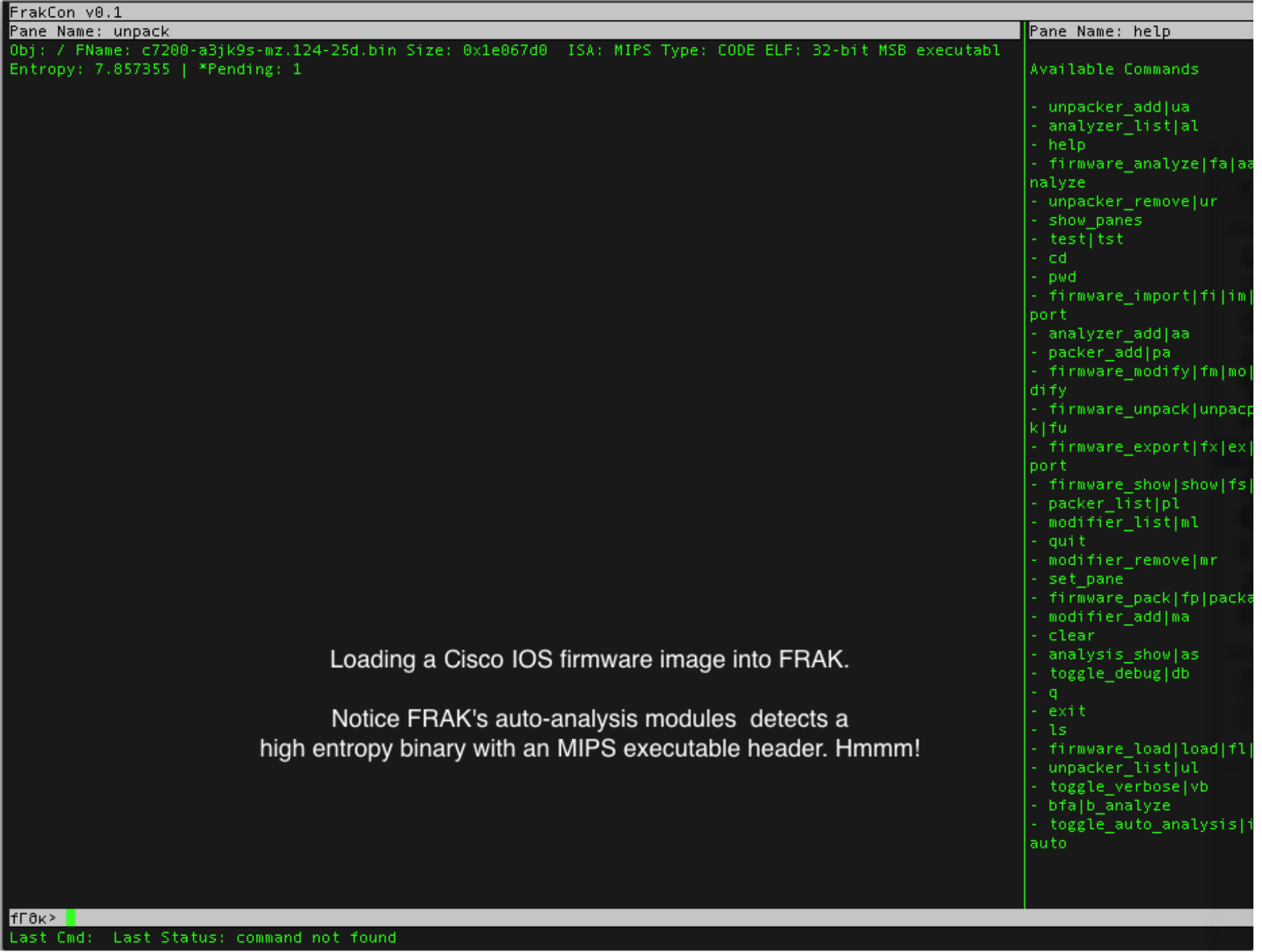

Payload Developement
Payload Testing
Payload Design
STARE @ BINARY BLOB

With FRAK!

ENOUGH TALK

DEMO TIME

- Packer/Repacker for Cisco IOS, HP-RFU
- Automagic Binary Analysis
- IDA-Pro Integration
- Entropy-related Analysis
- Automated IOS/RFU Rootkit Injection


FrakCon v0.1
Pane Name: unpack
Obj: / FName: c7200-a3jk9s-mz.124-25d.bin Size: 0x1e067d0 ISA: MIPS Type: CODE ELF: 32-bit MSB executabl
Entropy: 7.857355 | *Pending: 1
Loading a Cisco IOS firmware image into FRAK.
Notice FRAK's auto-analysis modules detects a
high entropy binary with an MIPS executable header. Hmmm!
Pane Name: help
Available Commands
- unpacker_add|ua
- analyzer_list|al
- help
- firmware_analyze|fa|aa
nalyze
- unpacker_remove|ur
- show_panes
- test|tst
- cd
- pwd
- firmware_import|fi|im|
port
- analyzer_add|aa
- packer_add|pa
- firmware_modify|fm|mo|
dify
- firmware_unpack|unpacp
k|fu
- firmware_export|fx|ex|
port
- firmware_show|show|fs|
- packer_list|pl
- modifier_list|ml
- quit
- modifier_remove|mr
- set_pane
- firmware_pack|fp|packa
- modifier_add|ma
- clear
- analysis_show|as
- toggle_debug|db
- q
- exit
- ls
- firmware_load|load|fl|
- unpacker_list|ul
- toggle_verbose|vb
- bfa|b_analyze
- toggle_auto_analysis|t
auto
fΓθκ>
Last Cmd: Last Status: command not found



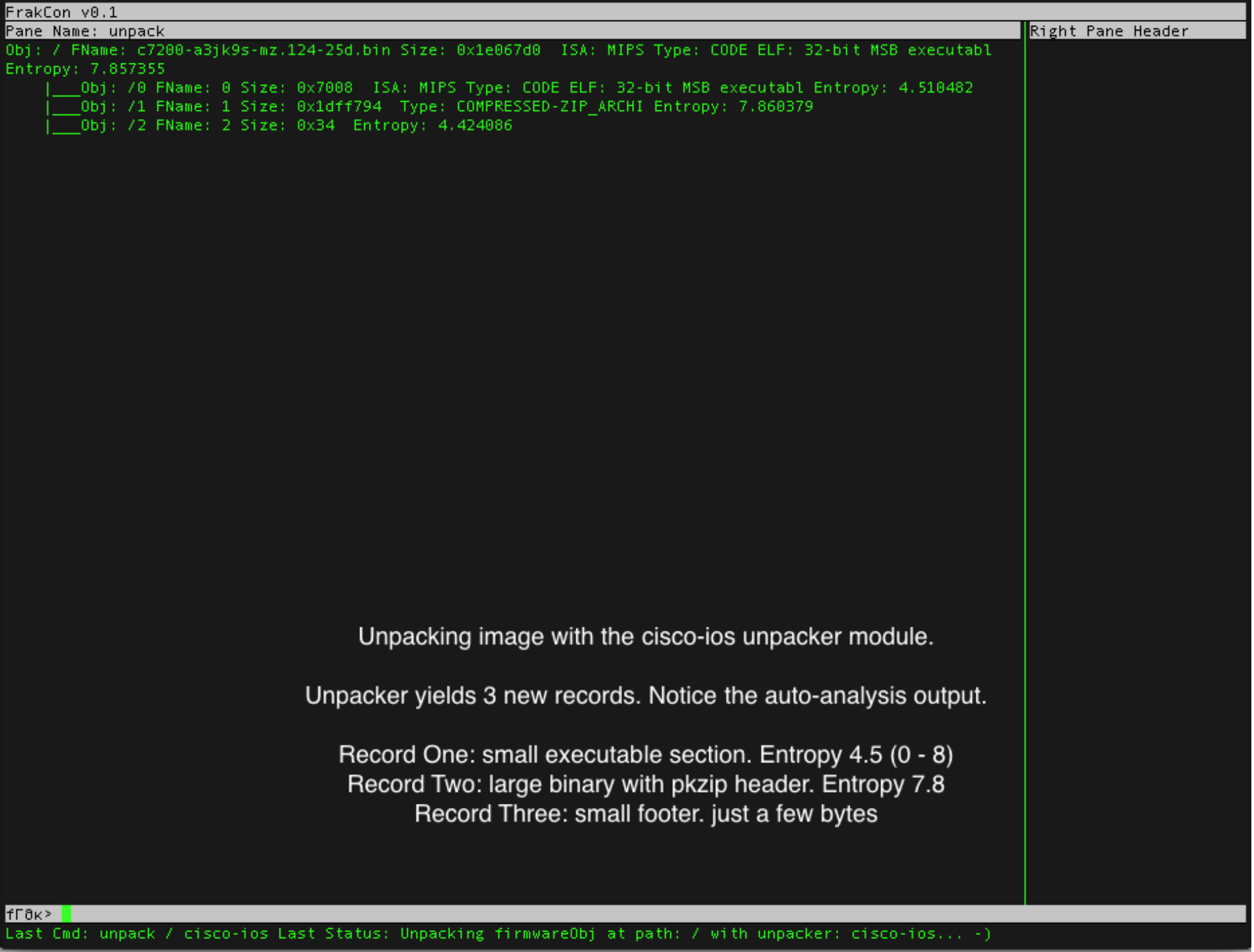
Entropy map of firmware image.

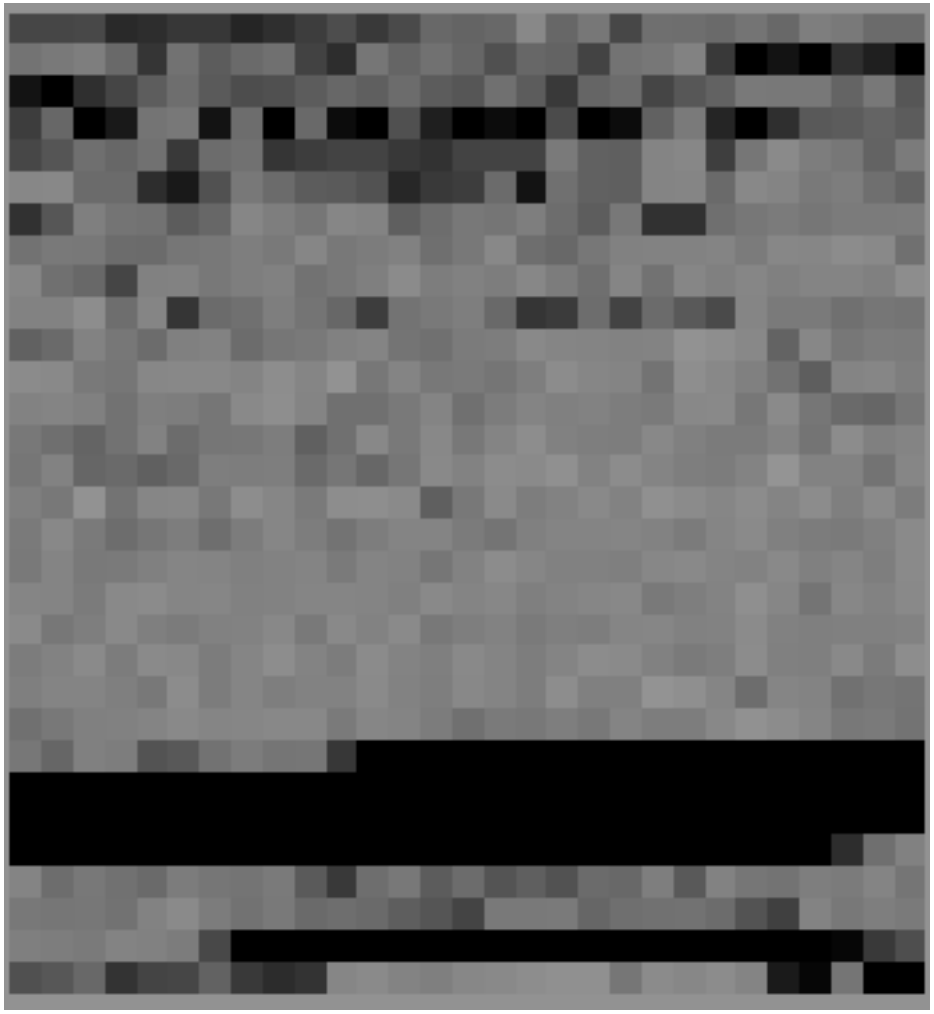
White: high entropy data
Black: low entropy data

Small low random header and footer.

Large amount of random data.

Hmm!


FrakCon v0.1
Pane Name: unpack
Right Pane Header
Obj: / FName: c7200-a3jk9s-mz.124-25d.bin Size: 0x1e067d0 ISA: MIPS Type: CODE ELF: 32-bit MSB executabl
Entropy: 7.857355
|___Obj: /0 FName: 0 Size: 0x7008 ISA: MIPS Type: CODE ELF: 32-bit MSB executabl Entropy: 4.510482
|___Obj: /1 FName: 1 Size: 0x1dff794 Type: COMPRESSED-ZIP_ARCHI Entropy: 7.860379
|___Obj: /2 FName: 2 Size: 0x34 Entropy: 4.424086
Unpacking image with the cisco-ios unpacker module.
Unpacker yields 3 new records. Notice the auto-analysis output.
Record One: small executable section. Entropy 4.5 (0 - 8)
Record Two: large binary with pkzip header. Entropy 7.8
Record Three: small footer. just a few bytes
fΓθκ>
Last Cmd: unpack / cisco-ios Last Status: Unpacking firmwareObj at path: / with unpacker: cisco-ios... -)

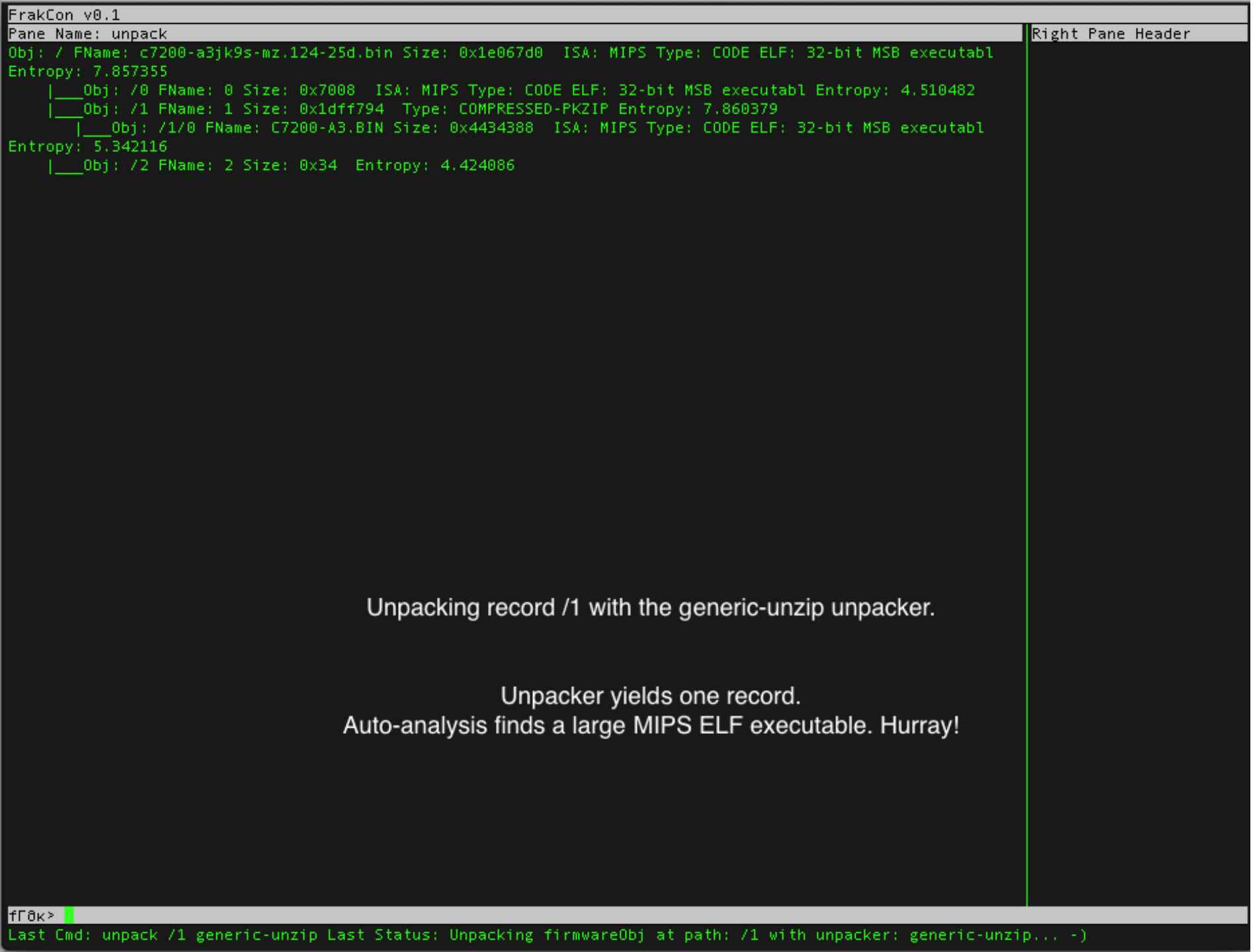


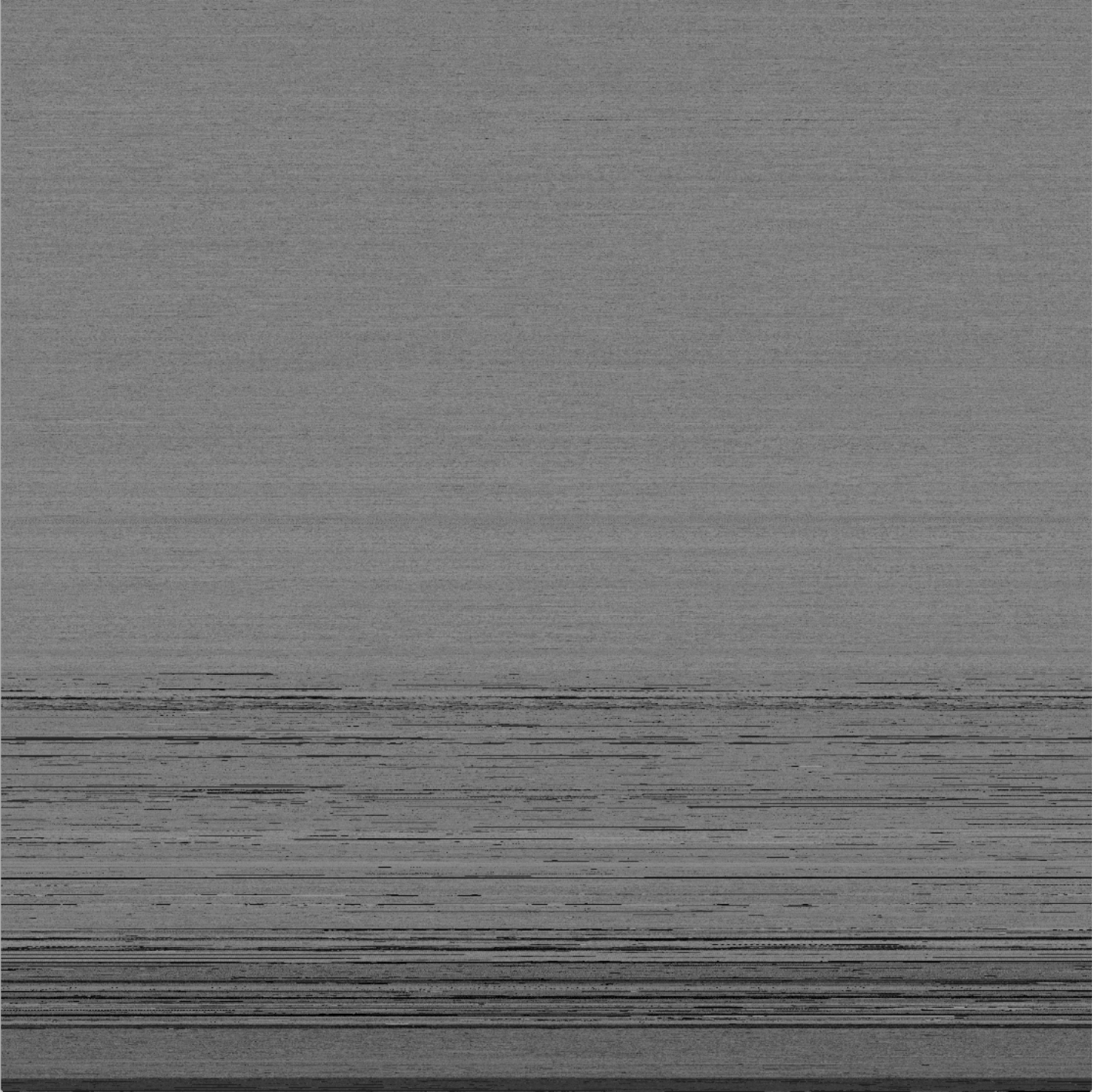
Entropy map of header.

Look familiar?

Let’s unpack the middle pkzip record.

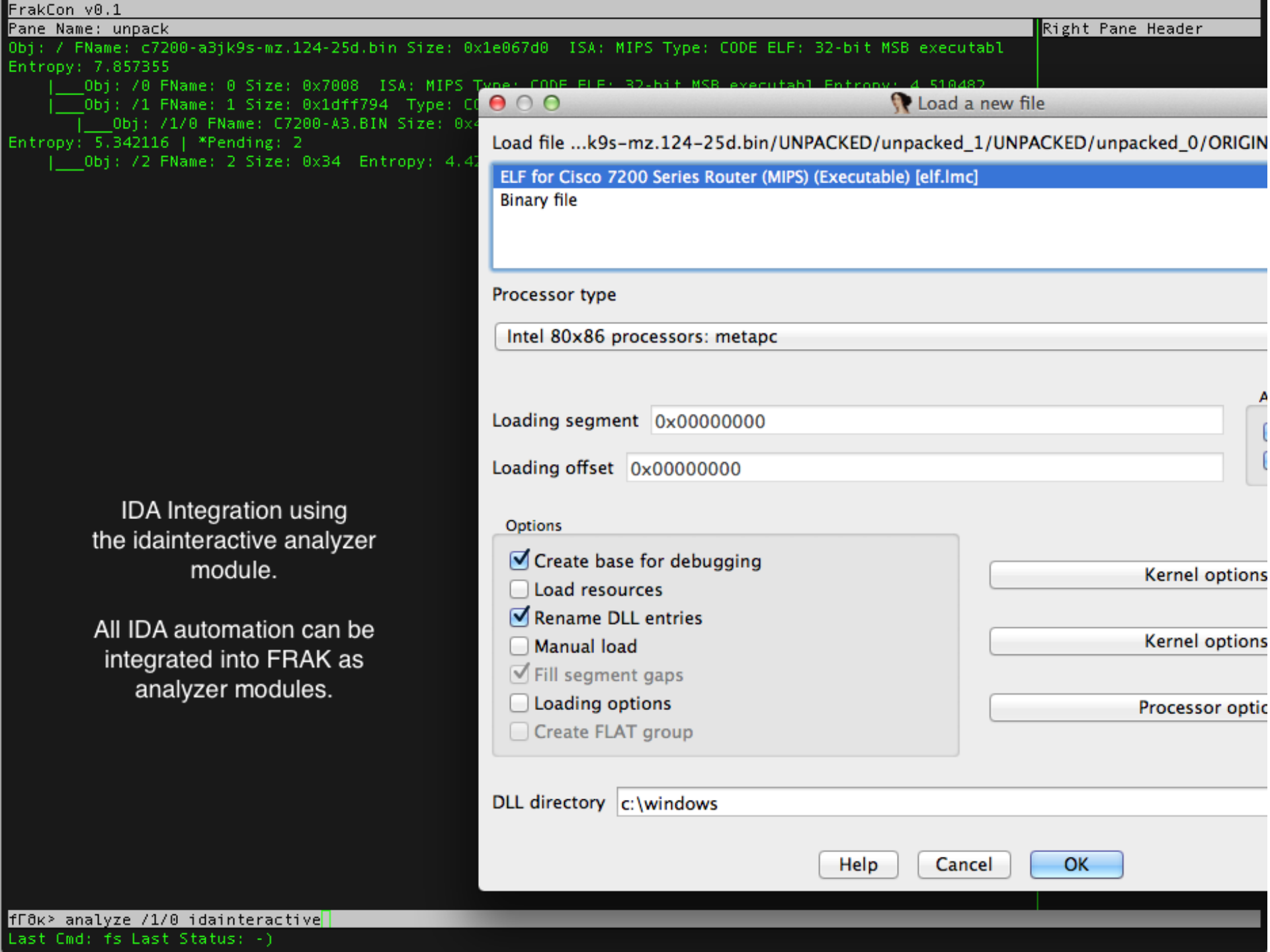
cmd: unpack /1 generic-unzip

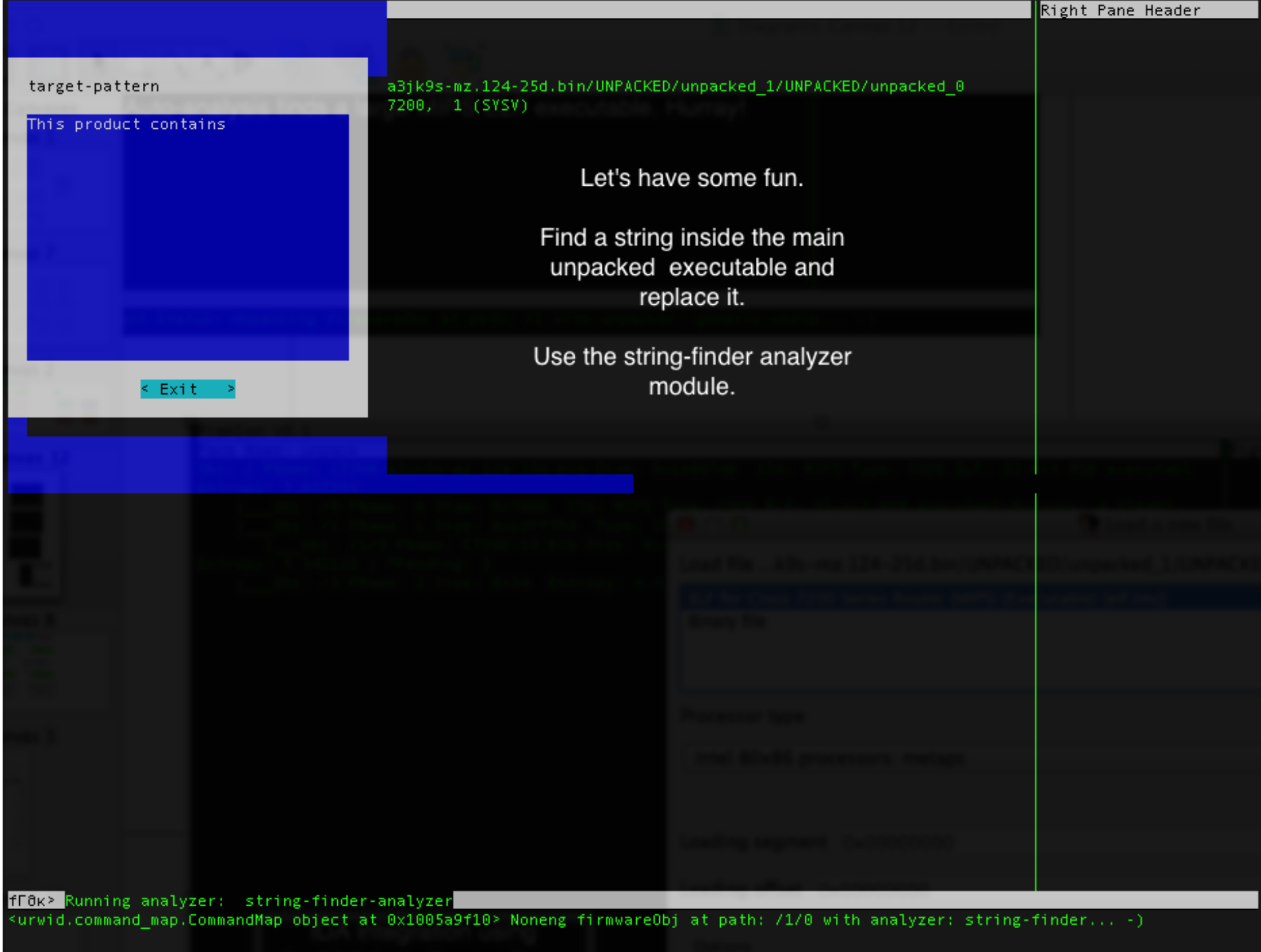

FrakCon v0.1
Pane Name: unpack
Right Pane Header
Obj: / FName: c7200-a3jk9s-mz.124-25d.bin Size: 0x1e067d0 ISA: MIPS Type: CODE ELF: 32-bit MSB executabl
Entropy: 7.857355
|___Obj: /0 FName: 0 Size: 0x7008 ISA: MIPS Type: CODE ELF: 32-bit MSB executabl Entropy: 4.510482
|___Obj: /1 FName: 1 Size: 0x1dff794 Type: COMPRESSED-PKZIP Entropy: 7.860379
|___Obj: /1/0 FName: C7200-A3.BIN Size: 0x4434388 ISA: MIPS Type: CODE ELF: 32-bit MSB executabl
Entropy: 5.342116
|___Obj: /2 FName: 2 Size: 0x34 Entropy: 4.424086
Unpacking record /1 with the generic-unzip unpacker.
Unpacker yields one record.
Auto-analysis finds a large MIPS ELF executable. Hurray!
fr0k>
Last Cmd: unpack /1 generic-unzip Last Status: Unpacking firmwareObj at path: /1 with unpacker: generic-unzip... -)

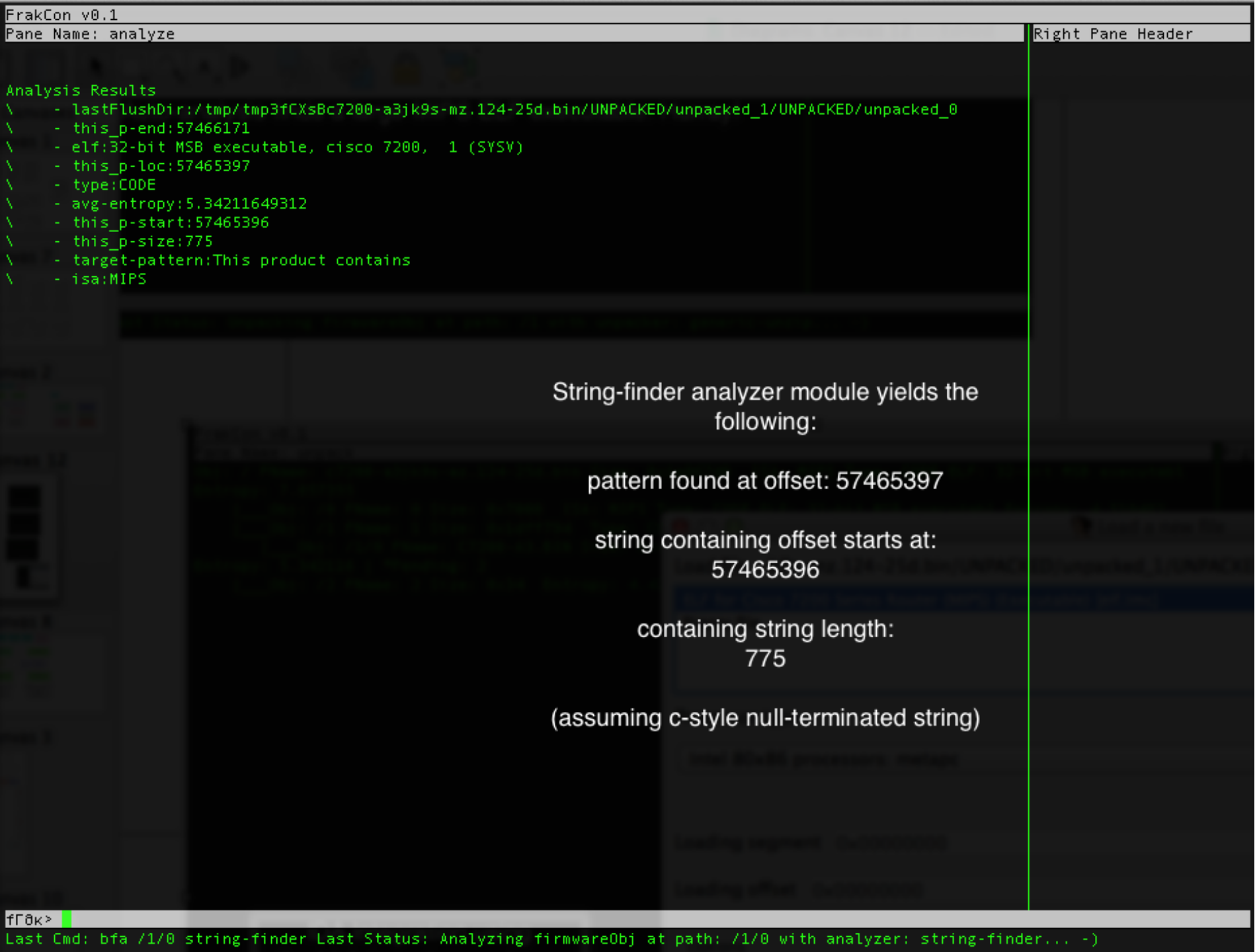


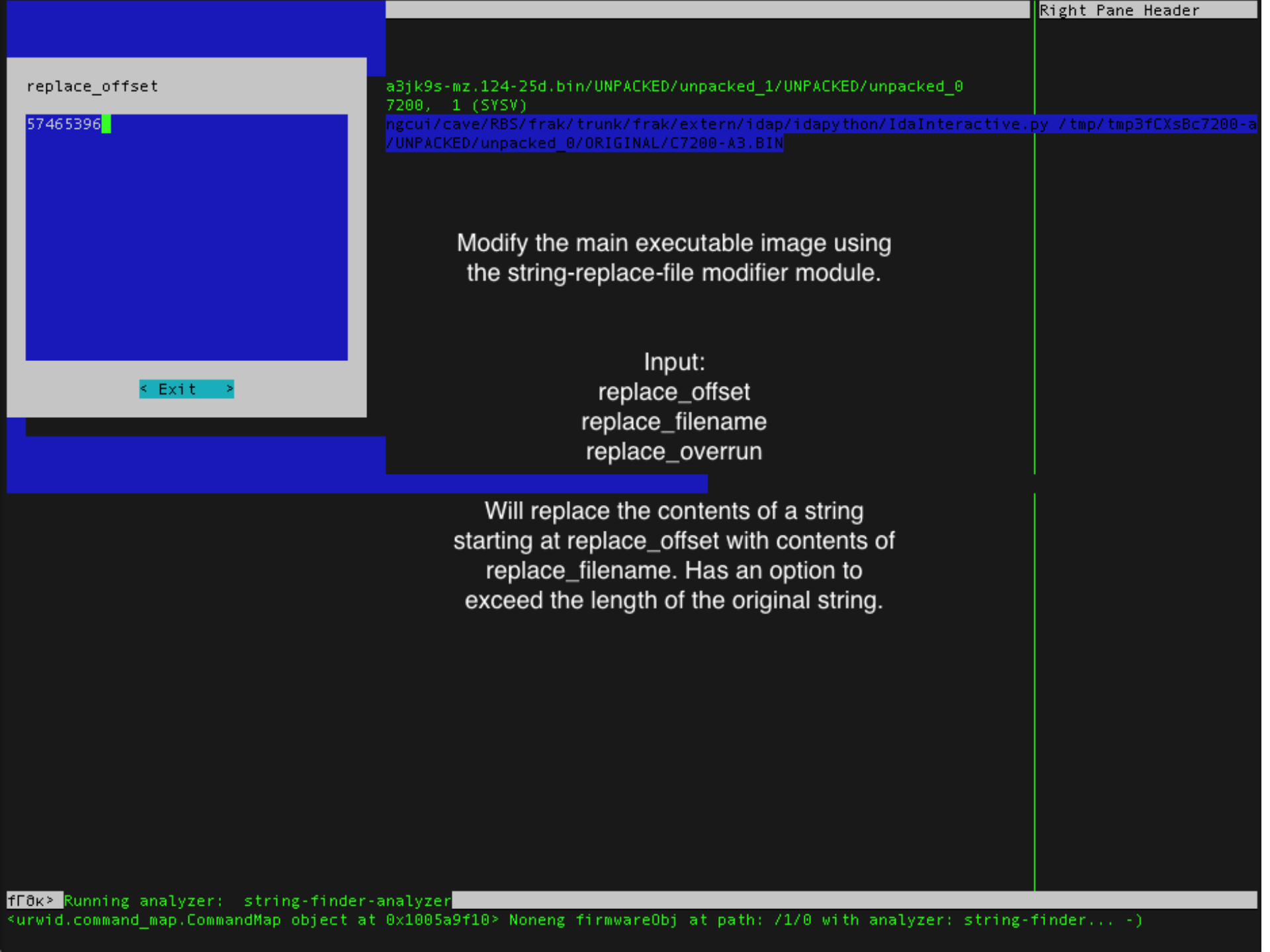
Entropy map of unzipped record.

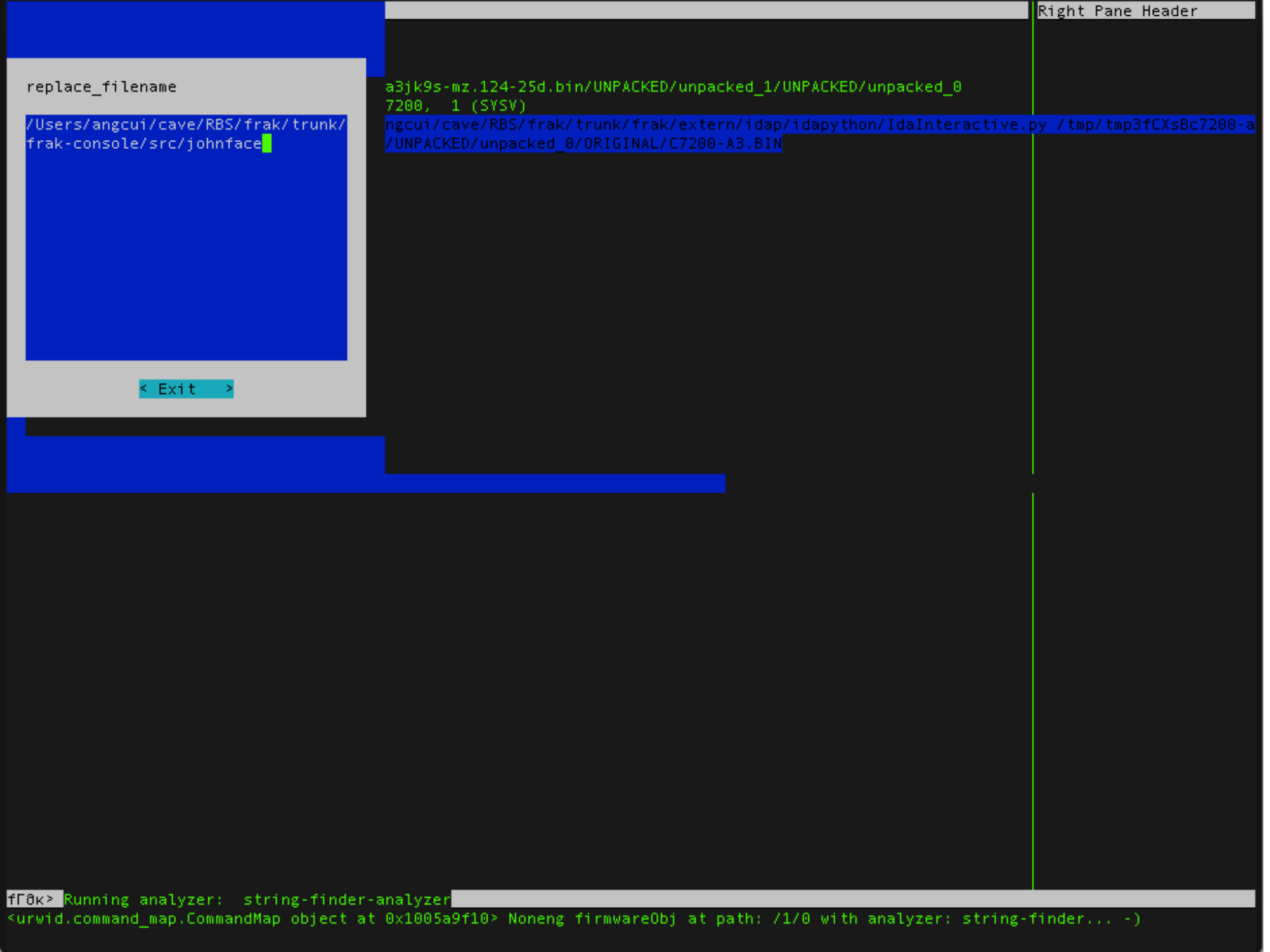
Does the structure look familiar?

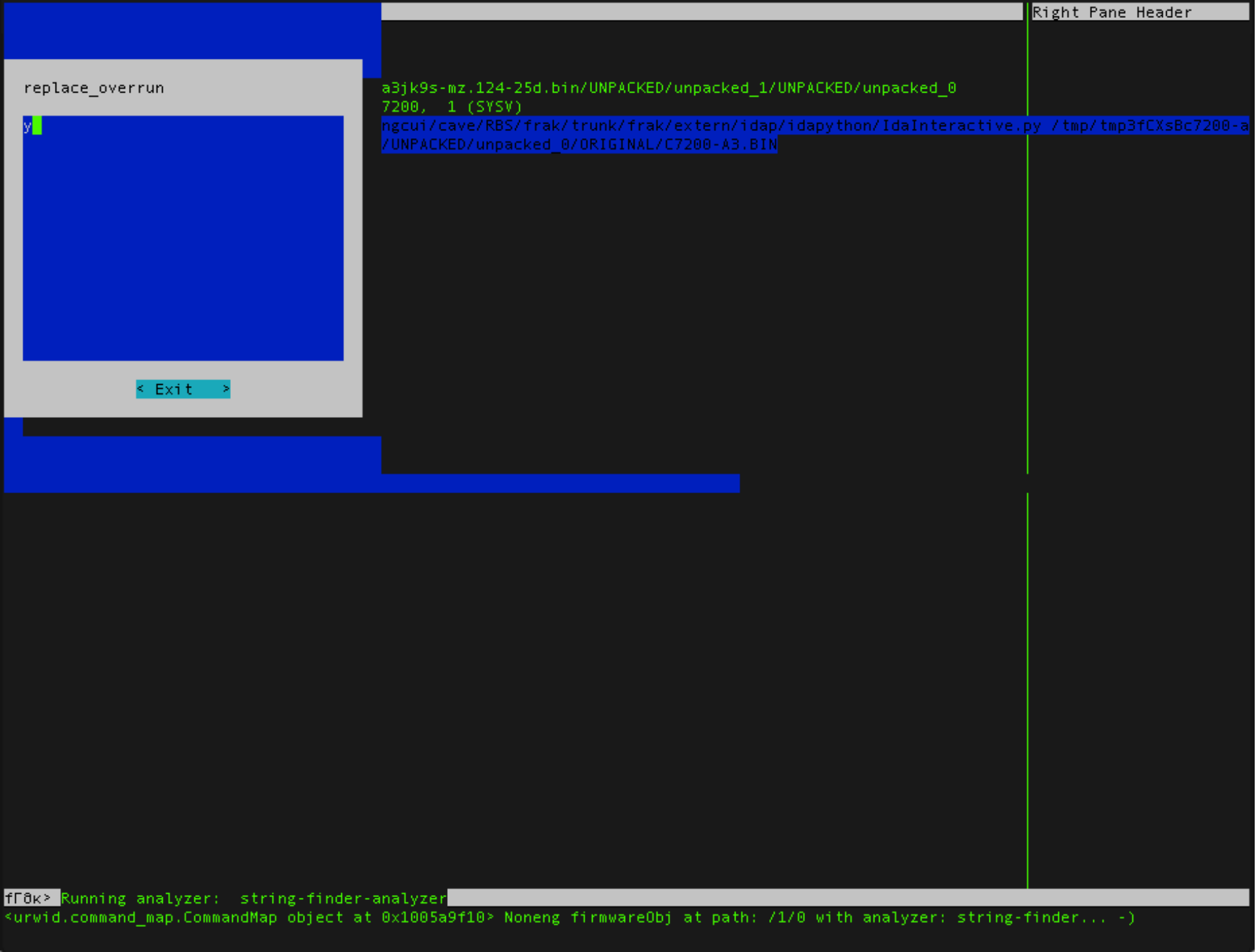

FrakCon v0.1
Pane Name: unpack
Right Pane Header
Obj: / FName: c7200-a3jk9s-mz.124-25d.bin Size: 0x1e067d0 ISA: MIPS Type: CODE ELF: 32-bit MSB executabl
Entropy: 7.857355
|___Obj: /0 FName: 0 Size: 0x7008 ISA: MIPS Type: CODE ELF: 32-bit MSB executabl Entropy: 4.510482
|___Obj: /1 FName: 1 Size: 0x1dff794 Type: C
|___Obj: /1/0 FName: C7200-A3.BIN Size: 0x
Entropy: 5.342116 | *Pending: 2
|___Obj: /2 FName: 2 Size: 0x34 Entropy: 4.4
IDA Integration using the idainteractive analyzer module.
All IDA automation can be integrated into FRAK as analyzer modules.
Load a new file
Load file ...k9s-mz.124-25d.bin/UNPACKED/unpacked_1/UNPACKED/unpacked_0/ORIGIN
ELF for Cisco 7200 Series Router (MIPS) (Executable) [elf.lmc]
Binary file
Processor type
Intel 80x86 processors: metapc
Loading segment 0x00000000
Loading offset 0x00000000
Options
Create base for debugging
Load resources
Rename DLL entries
Manual load
Fill segment gaps
Loading options
Create FLAT group
Kernel options
Kernel options
Processor optio
DLL directory c:\windows
Help
Cancel
OK
fΓθκ> analyze /1/0 idainteractive
Last Cmd: fs Last Status: -)

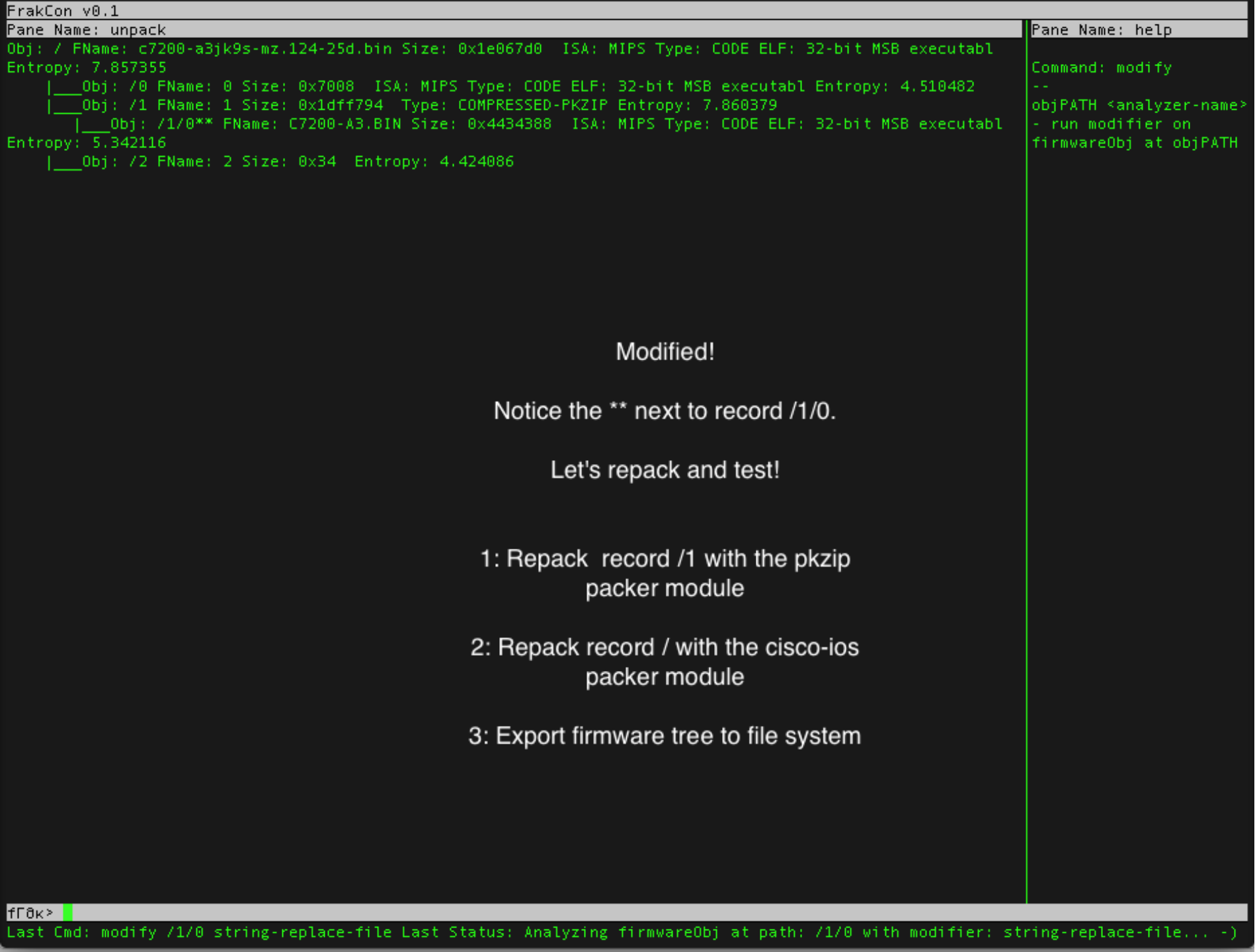

Right Pane Header
target-pattern
This product contains
< Exit >
a3jk9s-mz.124-25d.bin/UNPACKED/unpacked_1/UNPACKED/unpacked_0
7200, 1 (SYSV)
Let's have some fun.
Find a string inside the main unpacked executable and replace it.
Use the string-finder analyzer module.
fΓθκ> Running analyzer: string-finder-analyzer
<urwid.command_map.CommandMap object at 0x1005a9f10> Noneng firmwareObj at path: /1/0 with analyzer: string-finder... -)


FrakCon v0.1
Pane Name: analyze
Right Pane Header
Analysis Results
\ - lastFlushDir:/tmp/tmp3fCXsBc7200-a3jk9s-mz.124-25d.bin/UNPACKED/unpacked_1/UNPACKED/unpacked_0
\ - this_p-end:57466171
\ - elf:32-bit MSB executable, cisco 7200, 1 (SYSV)
\ - this_p-loc:57465397
\ - type:CODE
\ - avg-entropy:5.34211649312
\ - this_p-start:57465396
\ - this_p-size:775
\ - target-pattern:This product contains
\ - isa:MIPS
String-finder analyzer module yields the following:
pattern found at offset: 57465397
string containing offset starts at: 57465396
containing string length: 775
(assuming c-style null-terminated string)
fΓθκ>
Last Cmd: bfa /1/0 string-finder Last Status: Analyzing firmwareObj at path: /1/0 with analyzer: string-finder... -)


Right Pane Header
replace_offset
57465396
< Exit >
a3jk9s-mz.124-25d.bin/UNPACKED/unpacked_1/UNPACKED/unpacked_0
7200, 1 (SYSV)
ngcui/cave/RBS/frak/trunk/frak/extern/idap/idapython/IdaInteractive.py /tmp/tmp3fCXsBc7200-a
/UNPACKED/unpacked_0/ORIGINAL/C7200-A3.BIN
Modify the main executable image using
the string-replace-file modifier module.
Input:
replace_offset
replace_filename
replace_overrun
Will replace the contents of a string
starting at replace_offset with contents of
replace_filename. Has an option to
exceed the length of the original string.
fΓθκ> Running analyzer: string-finder-analyzer
<urwid.command_map.CommandMap object at 0x1005a9f10> Noneng firmwareObj at path: /1/0 with analyzer: string-finder... -)


Right Pane Header
replace_filename
/Users/angcui/cave/RBS/frak/trunk/
frak-console/src/johnface
< Exit >
a3jk9s-mz.124-25d.bin/UNPACKED/unpacked_1/UNPACKED/unpacked_0
7200, 1 (SYSV)
ngcui/cave/RBS/frak/trunk/frak/extern/idap/idapython/IdaInteractive.py /tmp/tmp3fCXsBc7200-a
/UNPACKED/unpacked_0/ORIGINAL/C7200-A3.BIN
fΓθκ> Running analyzer: string-finder-analyzer
<urwid.command_map.CommandMap object at 0x1005a9f10> Noneng firmwareObj at path: /1/0 with analyzer: string-finder... -)


Right Pane Header
replace_overrun
y
< Exit >
a3jk9s-mz.124-25d.bin/UNPACKED/unpacked_1/UNPACKED/unpacked_0
7200, 1 (SYSV)
ngcui/cave/RBS/frak/trunk/frak/extern/idap/idapython/IdaInteractive.py /tmp/tmp3fCXsBc7200-a
/UNPACKED/unpacked_0/ORIGINAL/C7200-A3.BIN
fΓ∂κ> Running analyzer: string-finder-analyzer
<urwid.command_map.CommandMap object at 0x1005a9f10> Noneng firmwareObj at path: /1/0 with analyzer: string-finder... -)


FrakCon v0.1
Pane Name: unpack
Obj: / FName: c7200-a3jk9s-mz.124-25d.bin Size: 0x1e067d0 ISA: MIPS Type: CODE ELF: 32-bit MSB executabl
Entropy: 7.857355
|___Obj: /0 FName: 0 Size: 0x7008 ISA: MIPS Type: CODE ELF: 32-bit MSB executabl Entropy: 4.510482
|___Obj: /1 FName: 1 Size: 0x1dff794 Type: COMPRESSED-PKZIP Entropy: 7.860379
|___Obj: /1/0** FName: C7200-A3.BIN Size: 0x4434388 ISA: MIPS Type: CODE ELF: 32-bit MSB executabl
Entropy: 5.342116
|___Obj: /2 FName: 2 Size: 0x34 Entropy: 4.424086
Pane Name: help
Command: modify
--
objPATH <analyzer-name>
- run modifier on
firmwareObj at objPATH
Modified!
Notice the ** next to record /1/0.
Let's repack and test!
1: Repack record /1 with the pkzip
packer module
2: Repack record / with the cisco-ios
packer module
3: Export firmware tree to file system
fΓõκ>
Last Cmd: modify /1/0 string-replace-file Last Status: Analyzing firmwareObj at path: /1/0 with modifier: string-replace-file... -)

I wonder what the johnface file contained. Hrm...

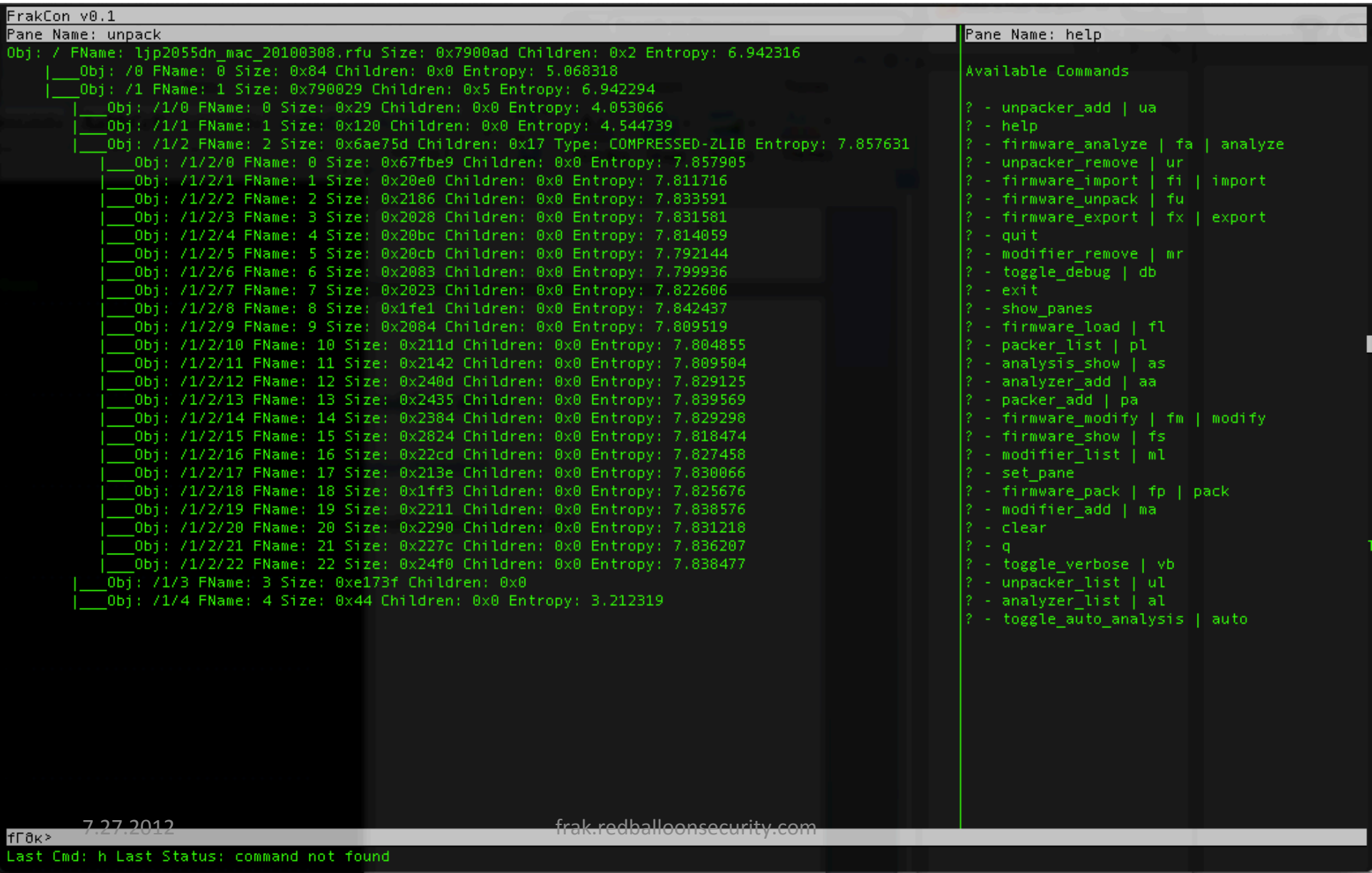
Let's fire up dynamips and find out.



-)

a@redballoonsecurity.com

Frak unpacking A HP-RFU Image



FRAK is still WIP. For Early Access

Contact

frak-join@lists.redballoonsecurity.com

FRAK is still WIP. For Early Access

Contact

frak-join@lists.redballoonsecurity.com

FRAK Page: http://frak.redballoonsecurity.com

FRAK is still WIP. For Early Access

Contact

frak-join@lists.redballoonsecurity.com

FRAK Page: http://frak.redballoonsecurity.com

Thank you DARPA Cyber Fast Track!



{ Ang Cui | a@redballoonsecurity.com }
www.redballoonsecurity.com