RED BALLOON SECURITY

FRAK: Firmware Reverse Analysis Konsole

Ang Cui
a@redballoonsecurity.com

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

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

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

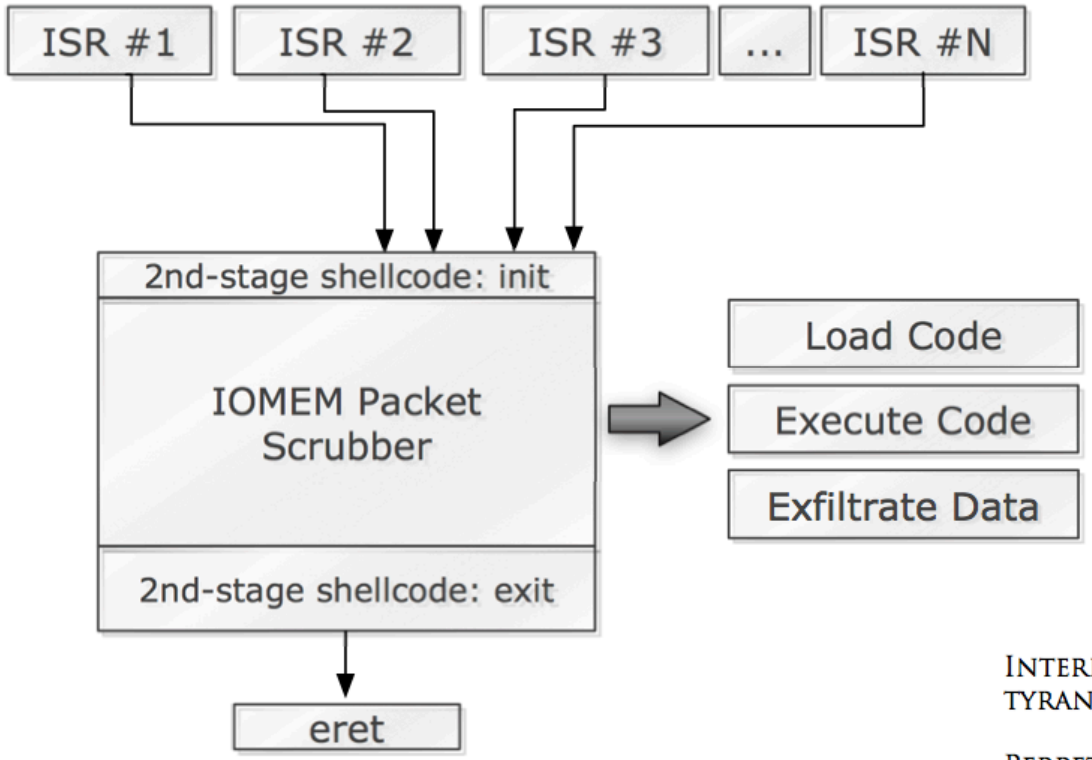
PAST EMBEDDED TINKERINGS:

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

Interrupt-Hijack Shellcode

[BlackHat USA 2011]

- 2nd-stage: Exception Hijack and IOMEM snooping

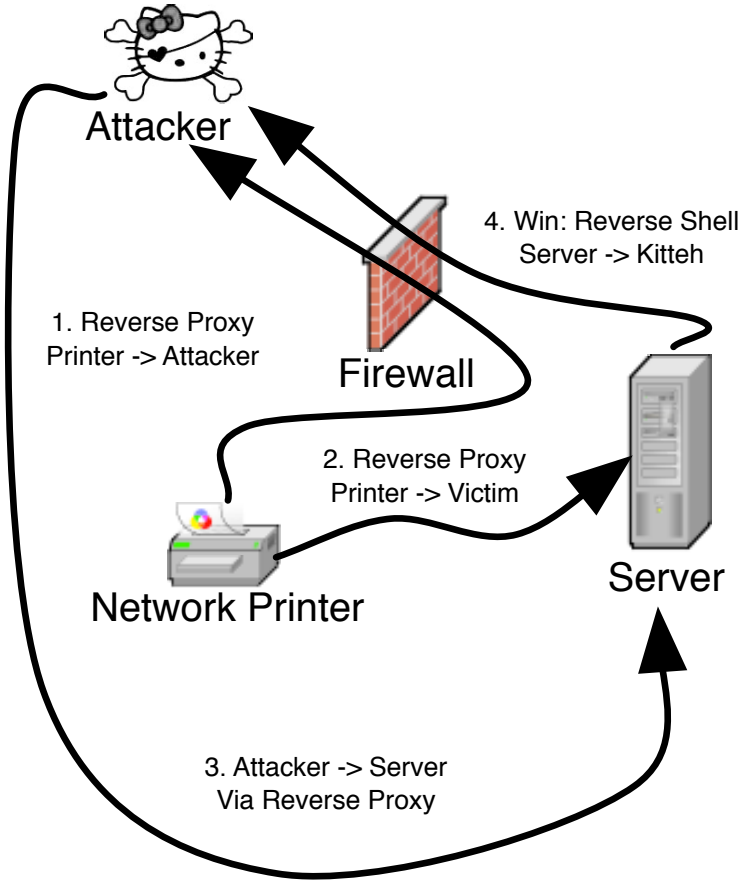


- The (MIPS) ERET, or Exception-Return is an architecture invariant
- ISR **entry** point is a **binary** invariant, typically found at 0x600080180, etc
- Can just hijack entry point, but there is an ulterior motive
- Use ERET locations in the image to **fingerprint** IOS version

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

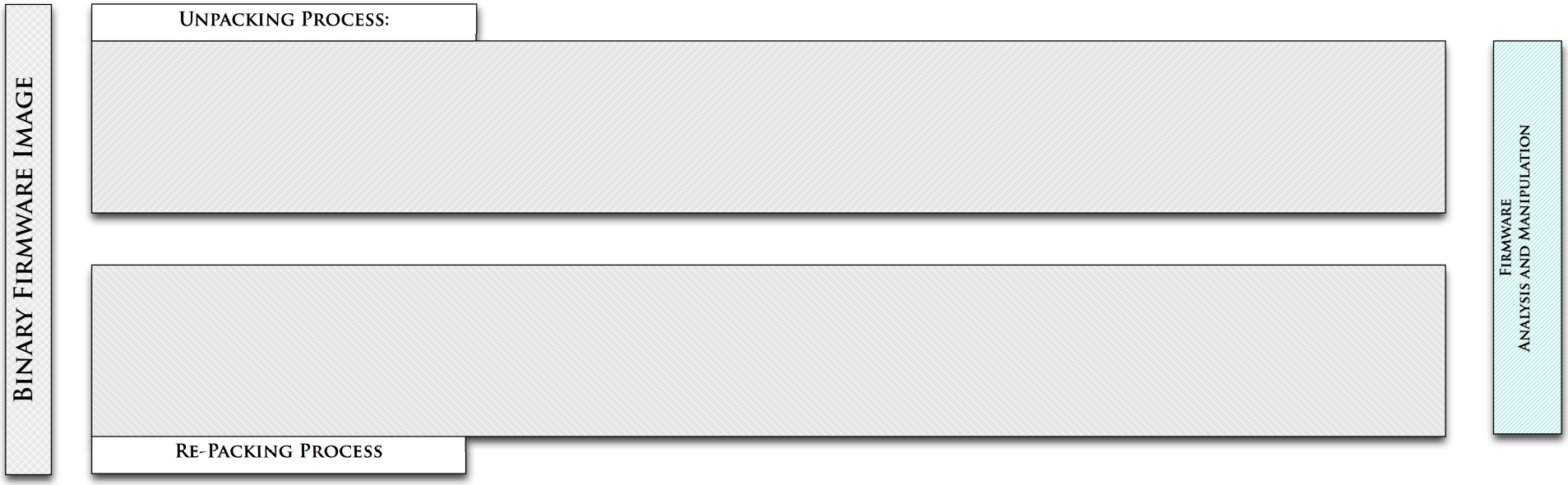
Perpetual, stealthy execution!

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



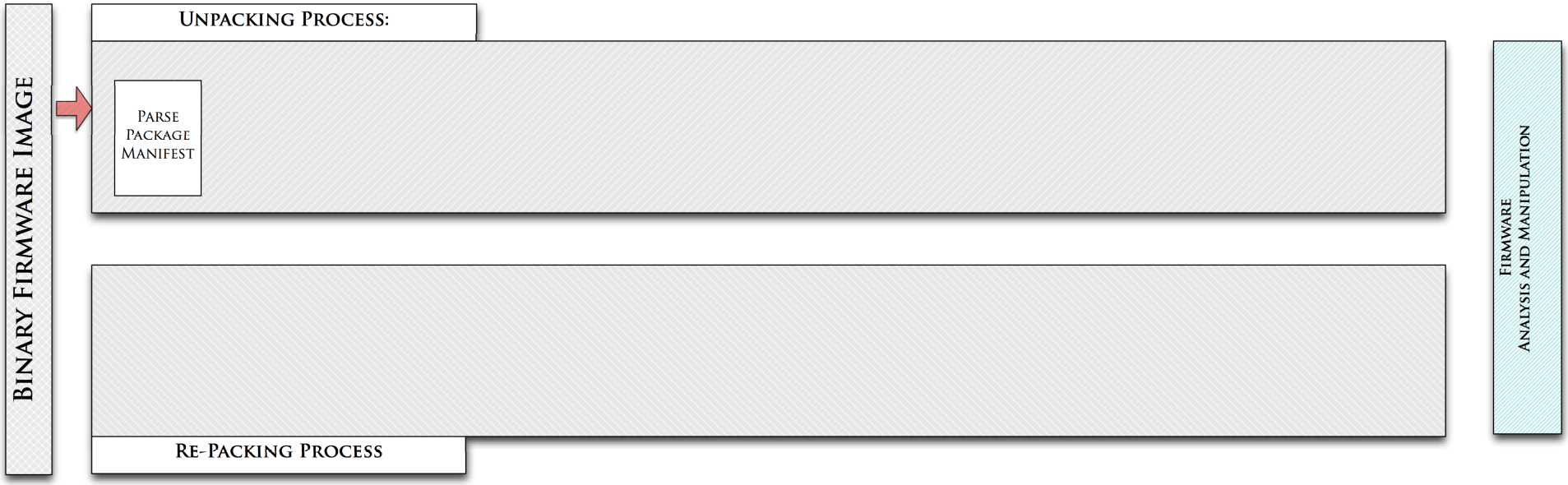
WORKFLOW

[XYZ Embedded {Offense|Defense}]



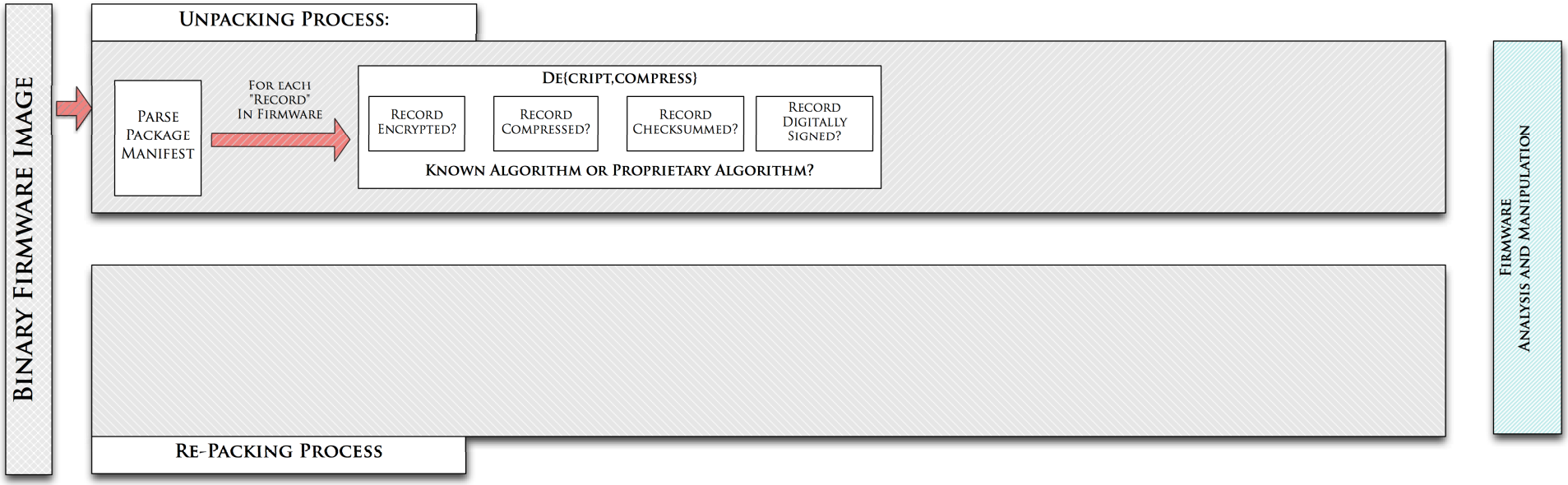
WORKFLOW

[XYZ Embedded {Offense|Defense}]



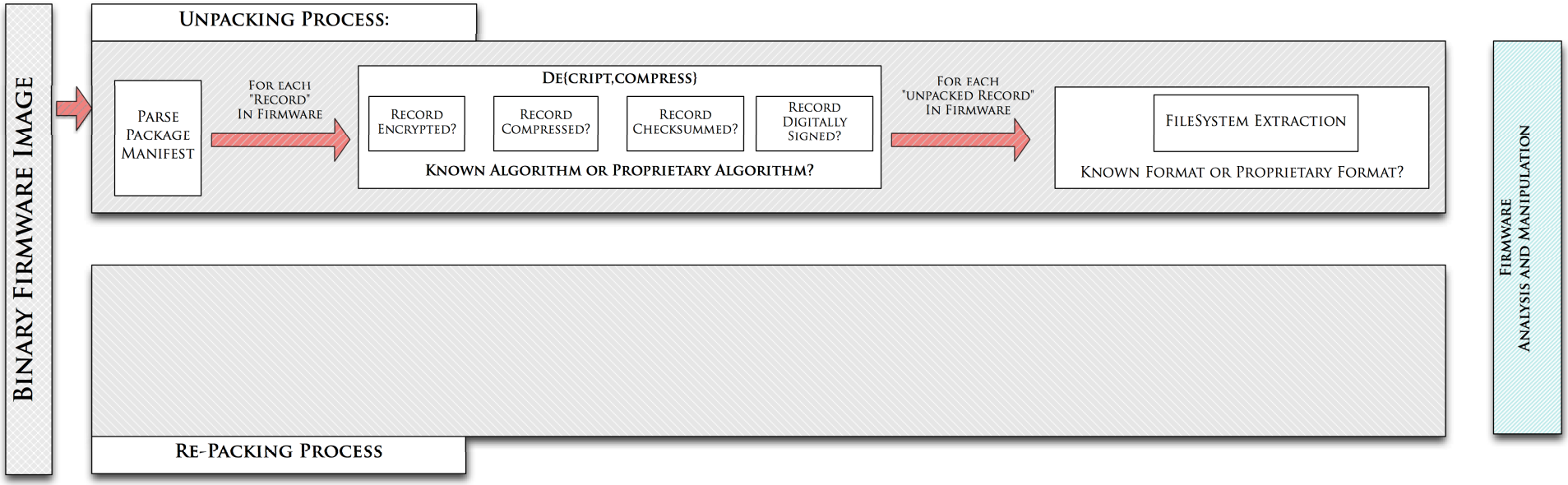
WORKFLOW

[XYZ Embedded {Offense|Defense}]



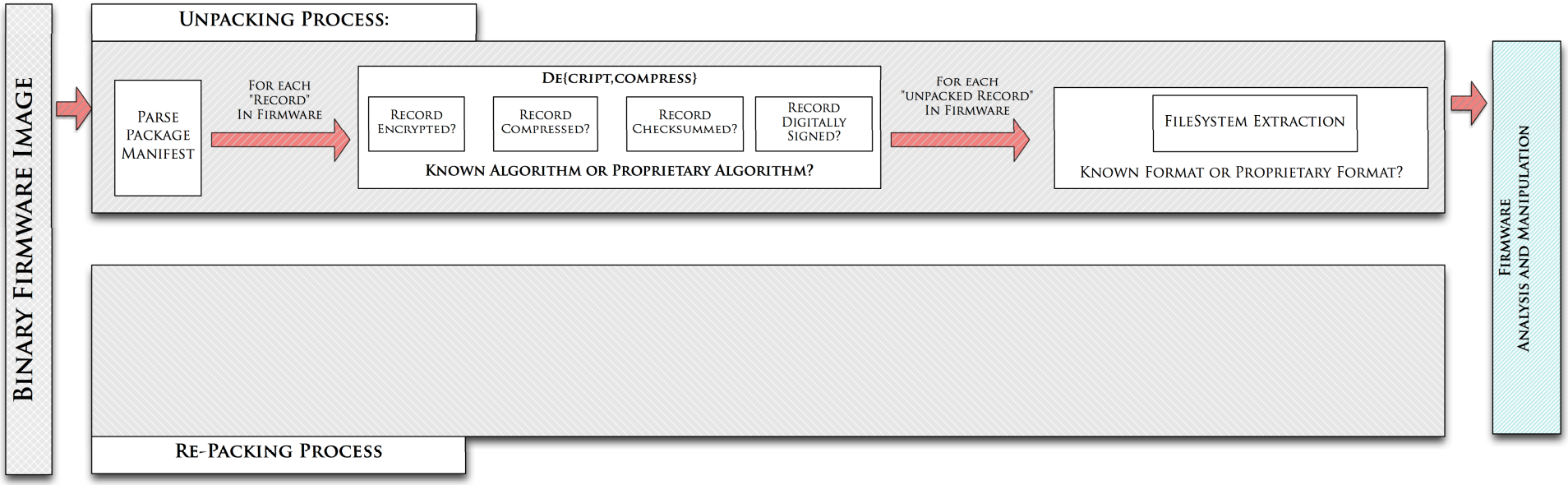
WORKFLOW

[XYZ Embedded {Offense|Defense}]



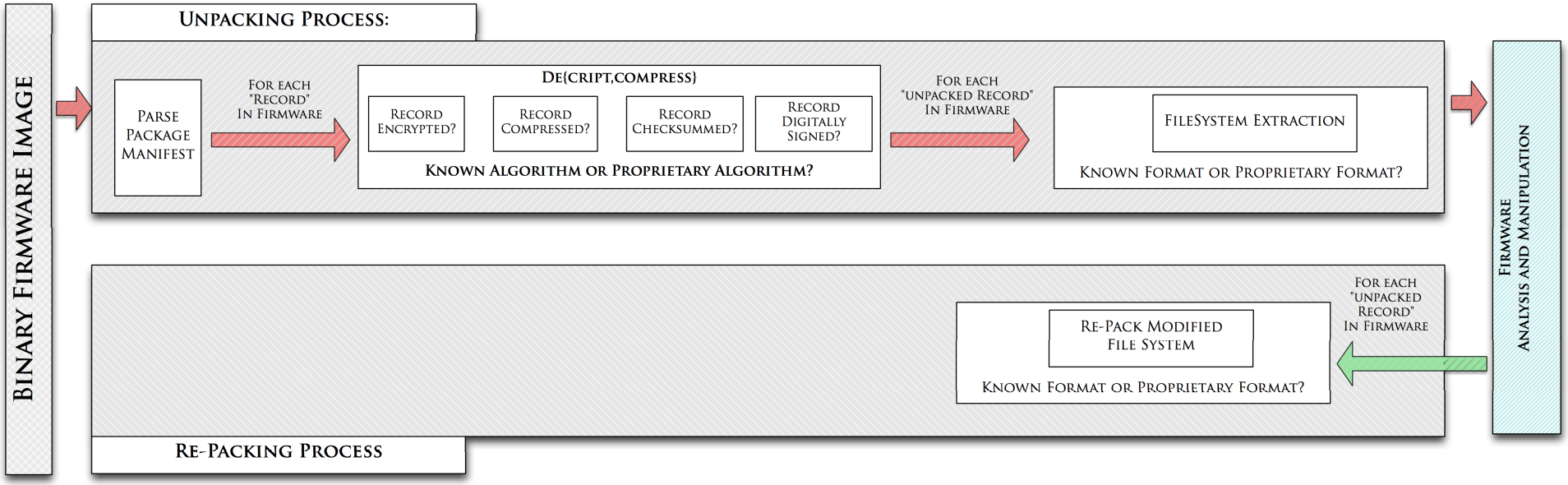
WORKFLOW

[XYZ Embedded {Offense|Defense}]



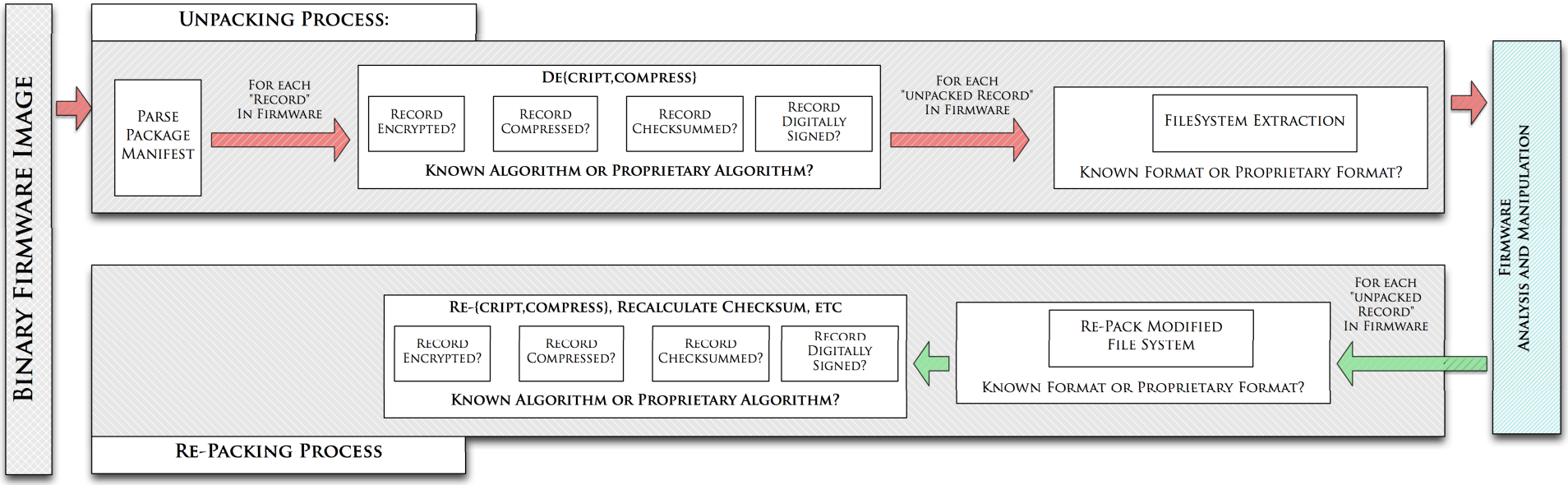
WORKFLOW

[XYZ Embedded {Offense|Defense}]



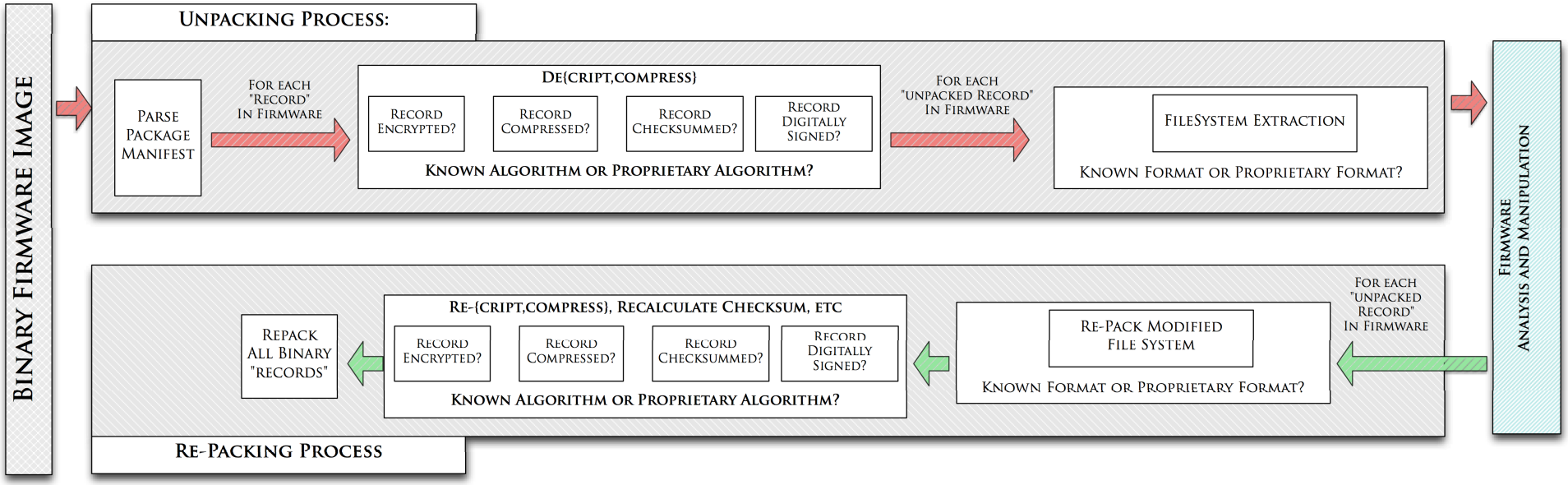
WORKFLOW

[XYZ Embedded {Offense|Defense}]



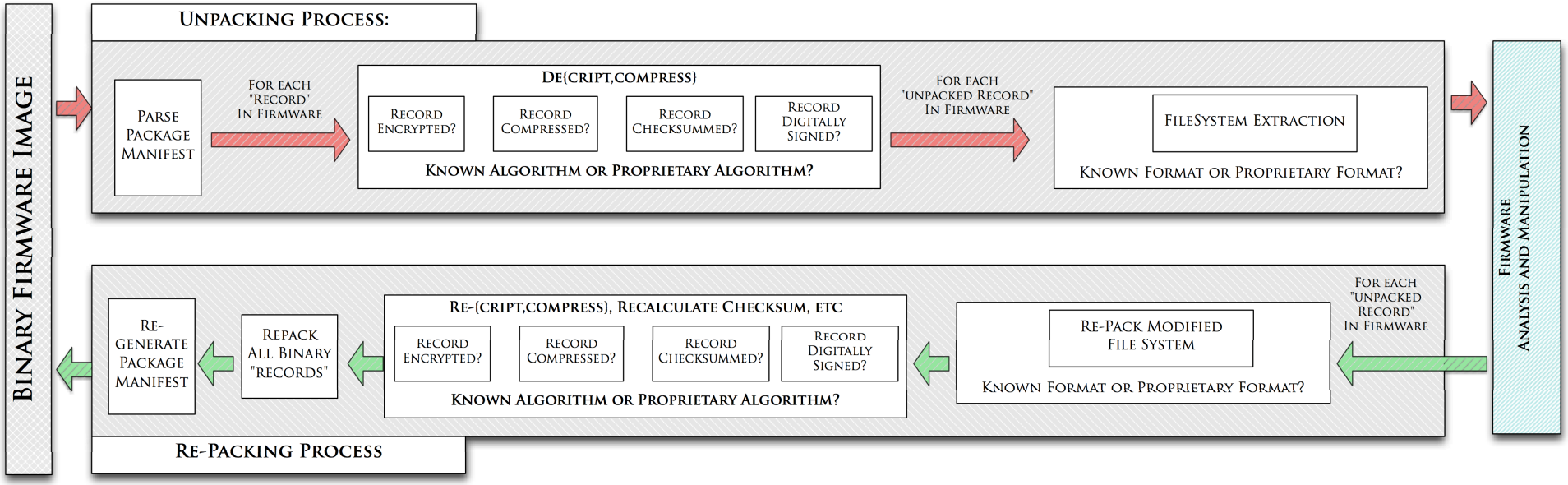
WORKFLOW

[XYZ Embedded {Offense|Defense}]

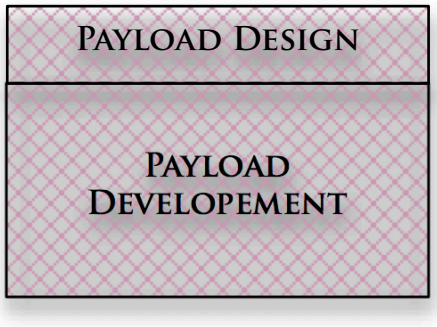


WORKFLOW

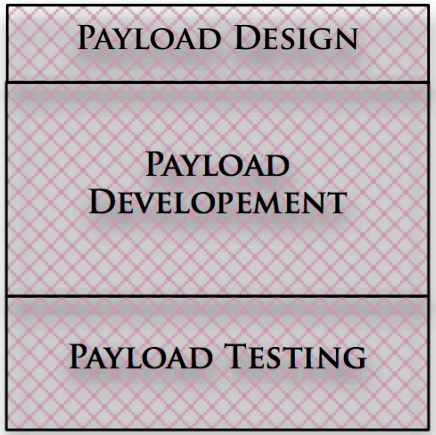
[XYZ Embedded {Offense|Defense}]



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

Reasons why Ang stays home on Friday night

Payload Design

Payload Developement

Payload Testing

STARE @ BINARY BLOB

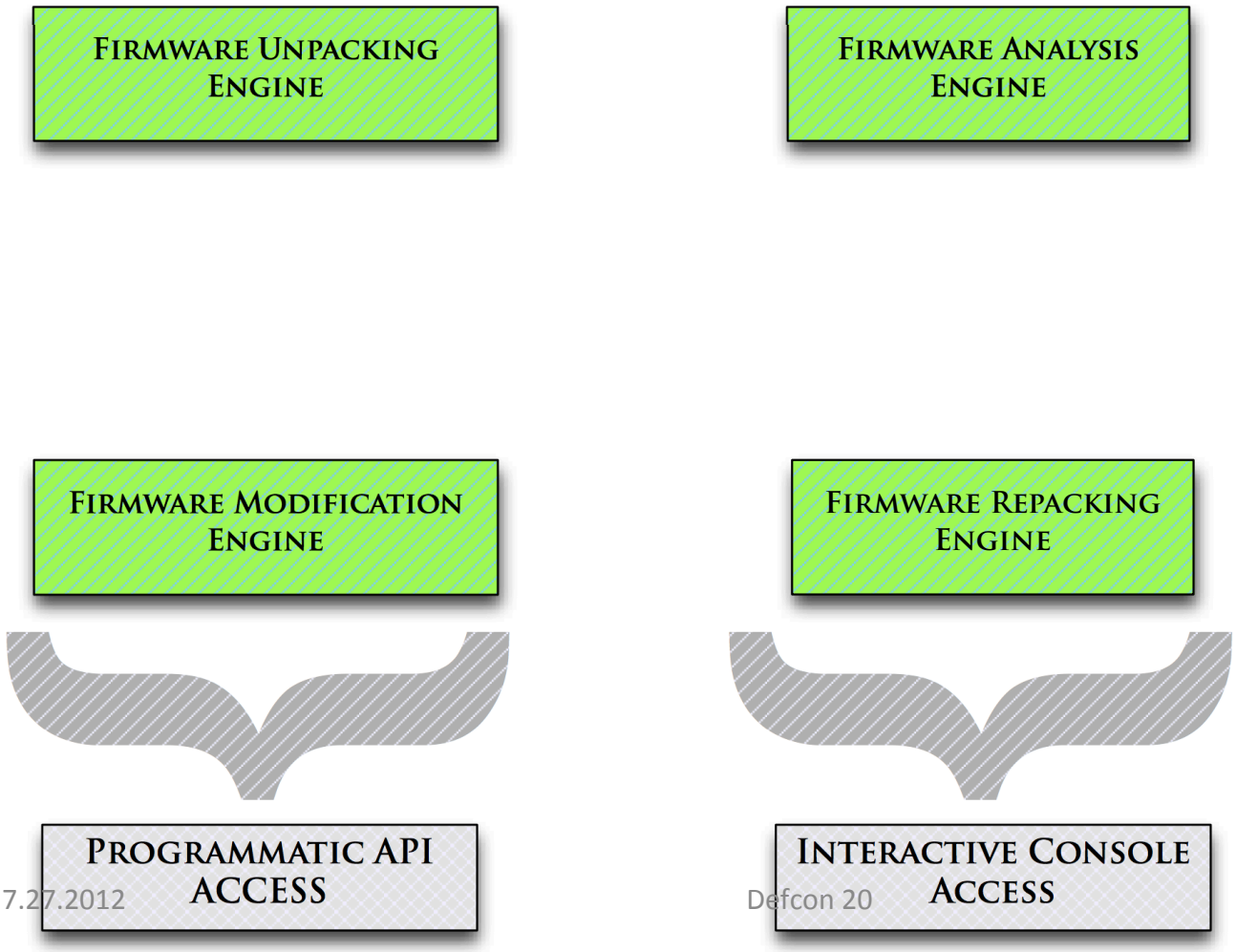
THIS PART

FIRMWARE REVERSE ANALYSIS KONSOLE

[Better Living Through Software Engineering]

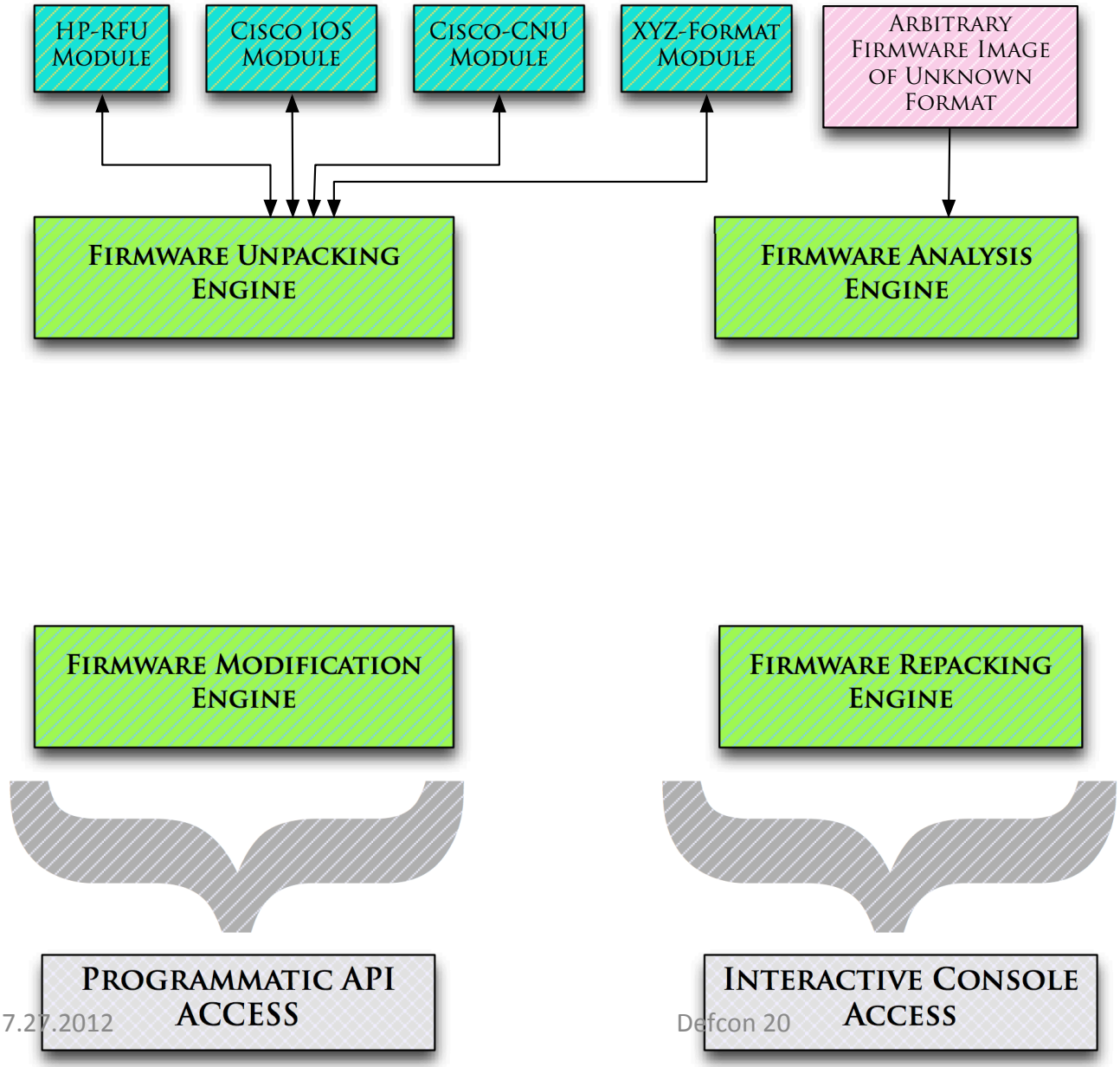
FRAK

IRMWARE EVERSE NALYSIS ONSOLE



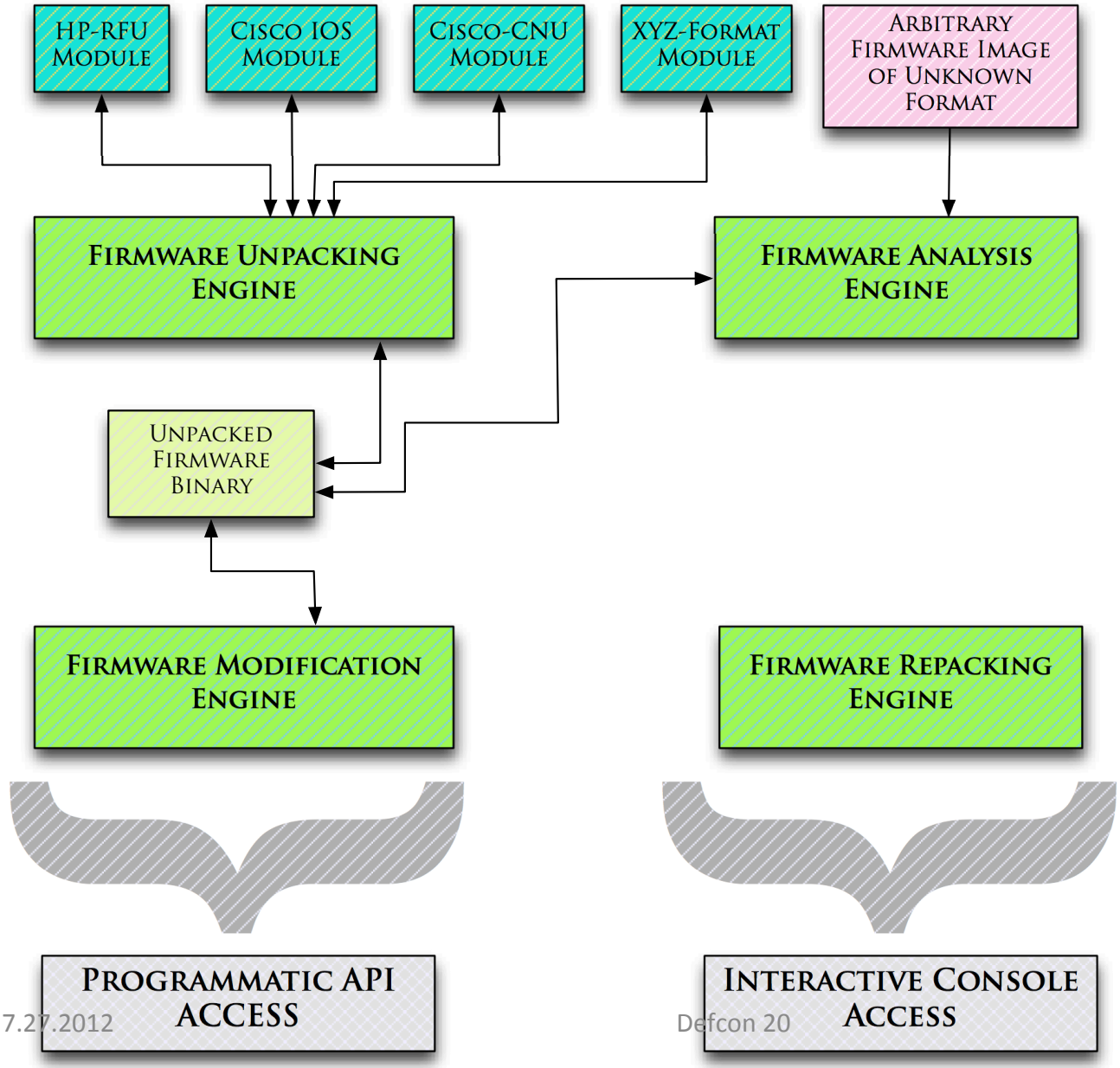
FRAK

FIRMWARE EVERSE NALYSIS ONSOLE



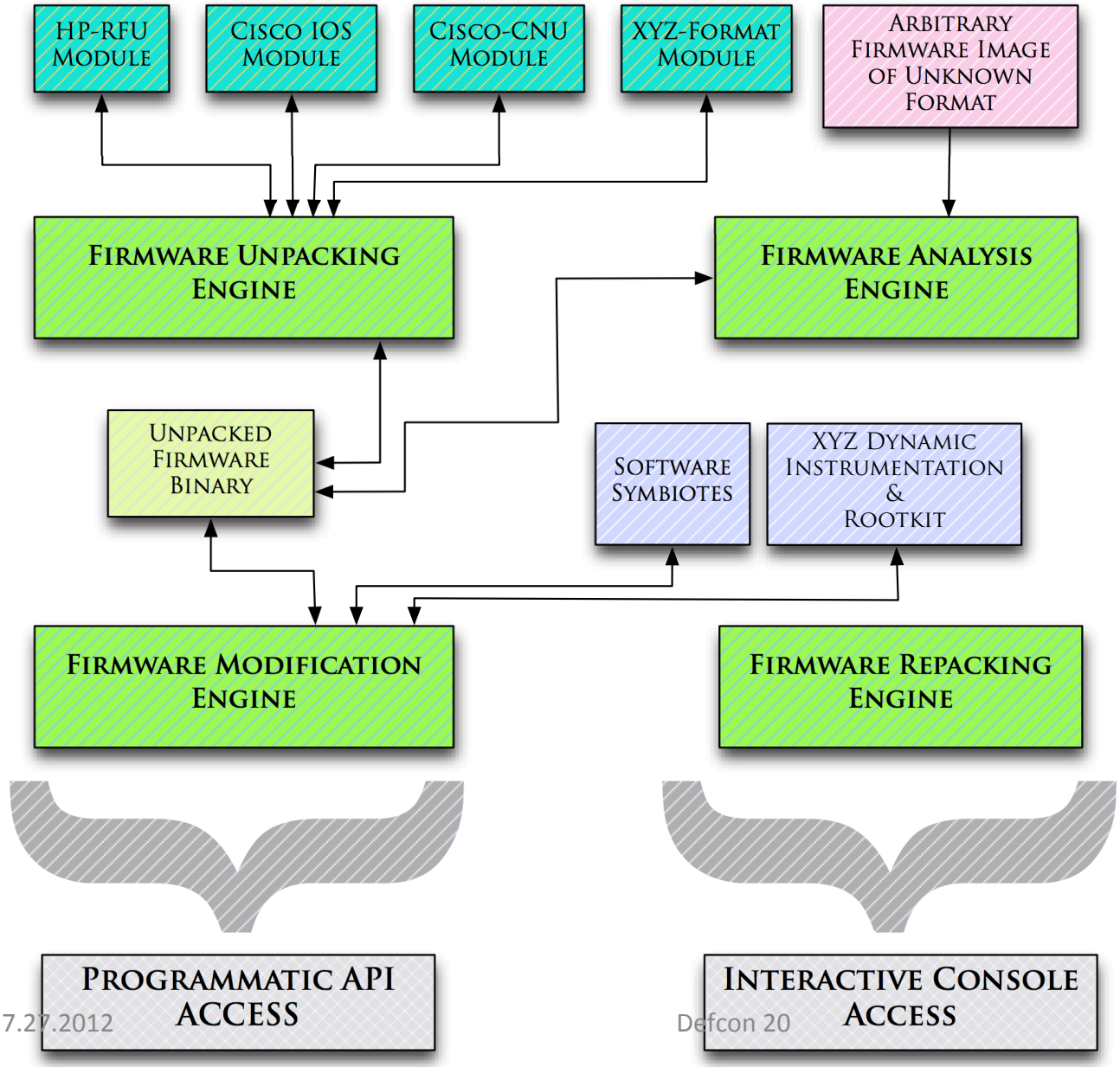
FRAK

FIRMWARE REVERSE ANALYSIS KONSOLE



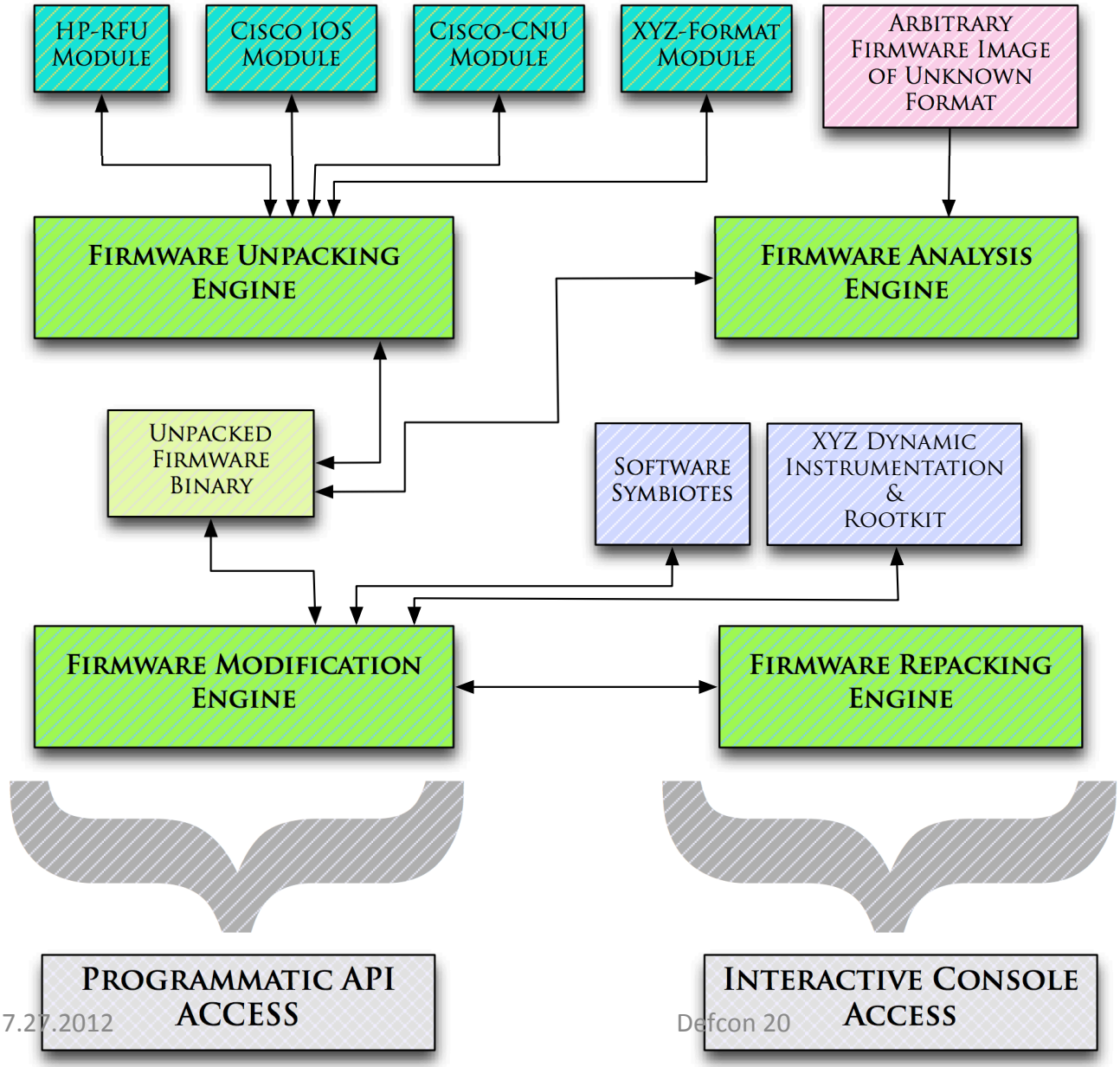
FRAK

IRMWARE EVERSE NALYSIS ONSOLE



FRAK

IRMWARE EVERSE NALYSIS ONSOLE



FRAK

IRMWARE EVERSE NALYSIS ONSOLE

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!"
```

Reasons why Ang stays home on Friday night

Payload Developement

Payload Testing

Payload Design

STARE @ BINARY BLOB

THIS PART

Thanks FRAK!

Demos

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

FRAK 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
```

```
fr0k>
Last Cmd: h Last Status: command not found
```

FRAK is still WIP. For Early Access

Contact

Frak-request@redballoonsecurity.com


PUT THE FUN