Evimetry
Digital forensics at wire speed

Forensic acquisition of modern evidence

A roadmap to what’s changed

Dr. Bradley Schatz
Director, Schatz Forensic

V1.0 – DFRWS-EU 2019

About me

- Dr Bradley Schatz
  - PhD, Digital Forensics (2007) ; BSc, Computer Science
- Schatz Forensic / Evimetry (2009-)
  - Practitioner, R&D, tool vendor
- Research affiliations
  - DFRWS Conference USA, Chair (2019), Technical Program Committee Chair (2017)
  - Journal of Digital Investigation (Editorial Board)
- Practical contributions
  - Volatility Memory Forensics Framework (Vista & Windows 7 support) (2010)
  - AFF4
  - Autopsy (index.dat support)
- Queensland University of Technology
  - Adjunct associate professor, doctoral supervision

This seminar

- Acquisition challenges
- Bottlenecks when dealing with SSD and NVMe
- Rethinking workflow methodology
- Full disk encryption
- Logical imaging
- Locked device forensics

Overarching acquisition challenges

Acquisition challenges increase as we go up the stack

Physical Imaging

- Dominant approaches (E01, RAW)
  - Slow throughput
  - Largely prevents live analysis
  - Poor interoperability for discontinuities (eg. Volatile memory, read errors)
  - Limited extensibility for metadata
- Emerging AFF4 work gaining traction
  - Advances all of the above

Acquisition challenges increase as we go up the stack

Logical Imaging

- No currently widely adopted standard for interoperability
  - L01, AD1, TGZ, ZIP…
- All approaches preserve less metadata than is desirable
  - e.g. File birth time
- Emerging AFF4 work
  - Publishing at DFRWS USA 2019
  - Python implementation github aff4/pyaff4/

Acquisition challenges increase as we go up the stack

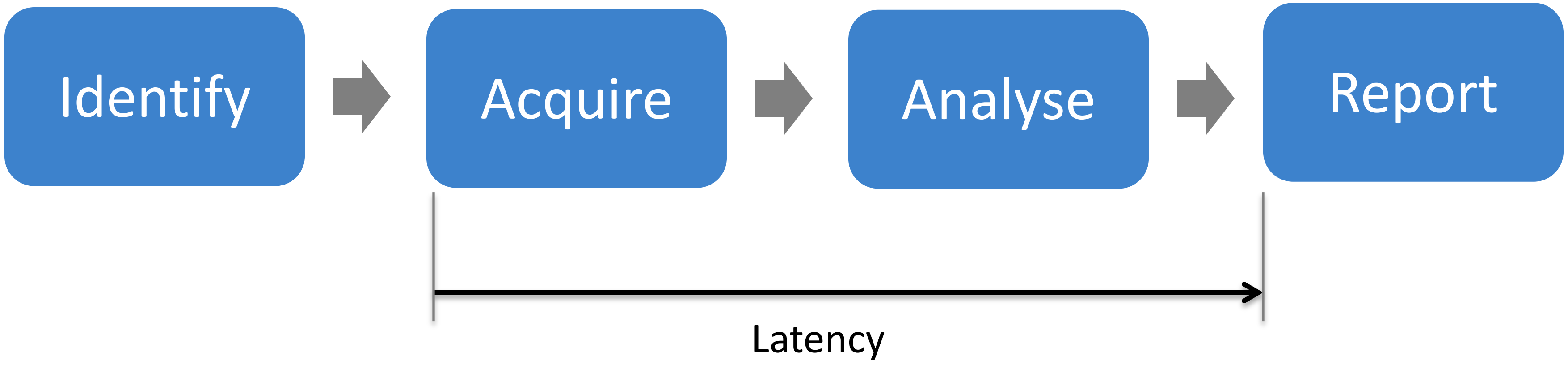
Sub-file Imaging

- We need a forensic imaging approach that scales to large numbers of very small records
  - Results of cloud API calls
  - eg. MAPI properties read via O365 API

Existing physical acquisition is a bottleneck

For fast storage

Current forensic methodology introduces lengthy delays.



Identify

Acquire

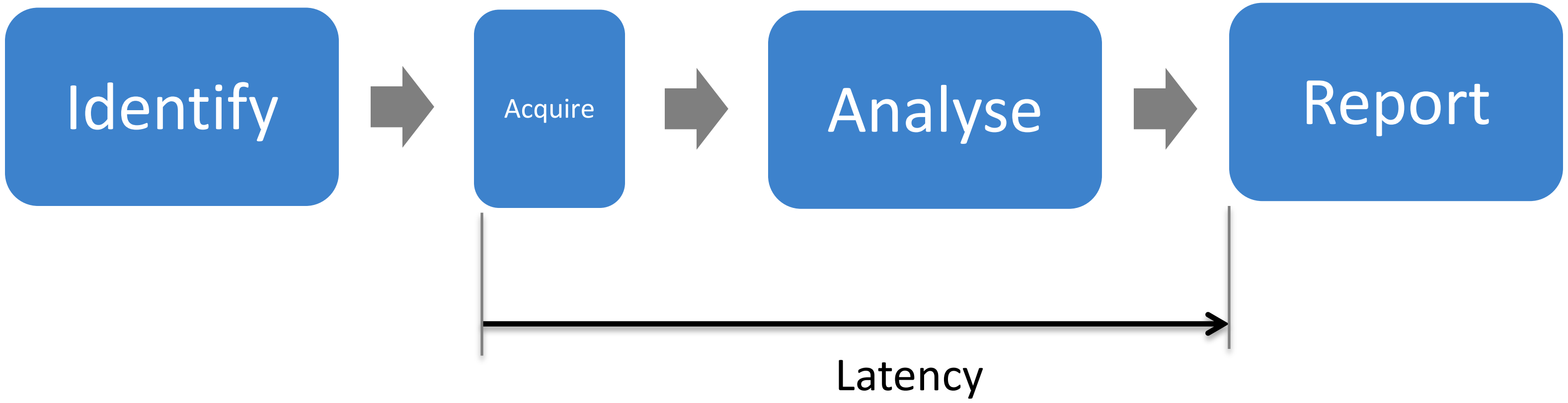
Analyse

Report

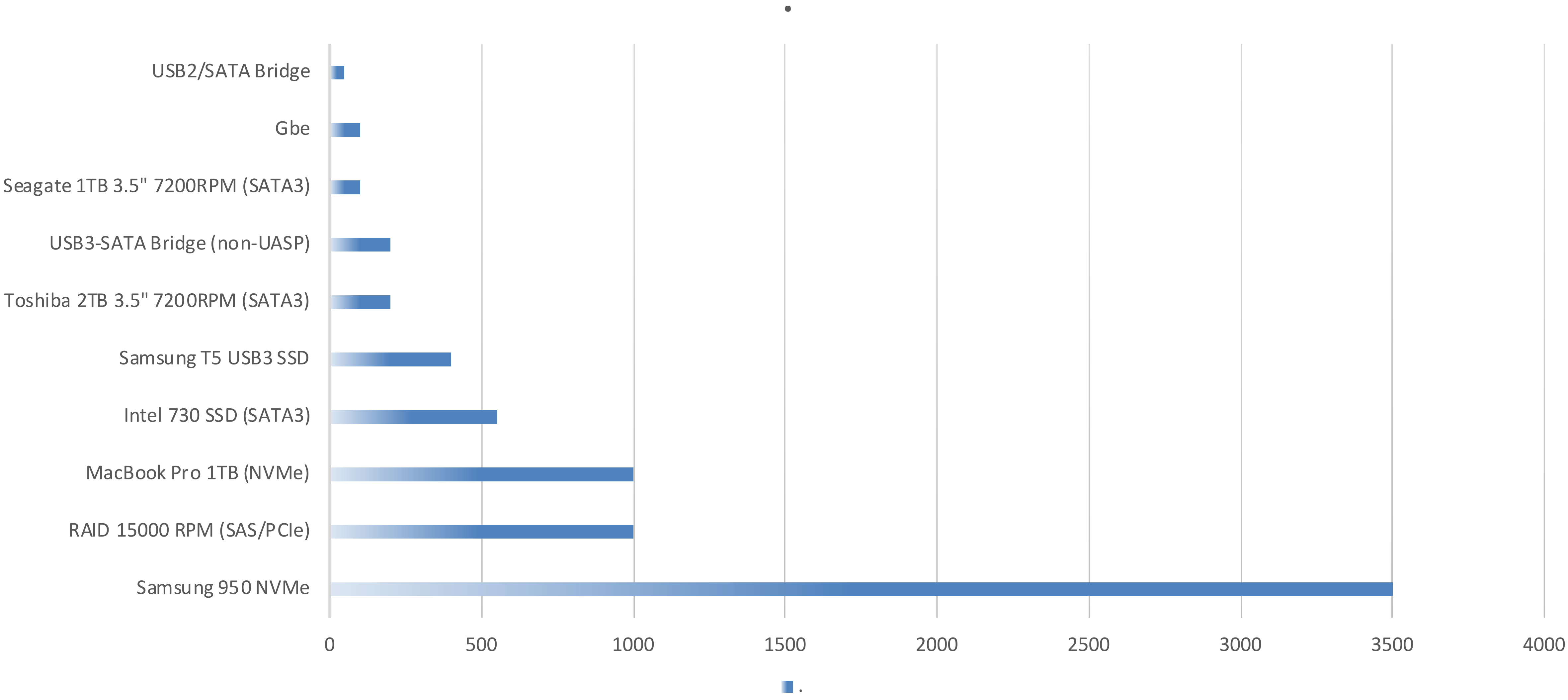
Latency

How can we reduce delays?

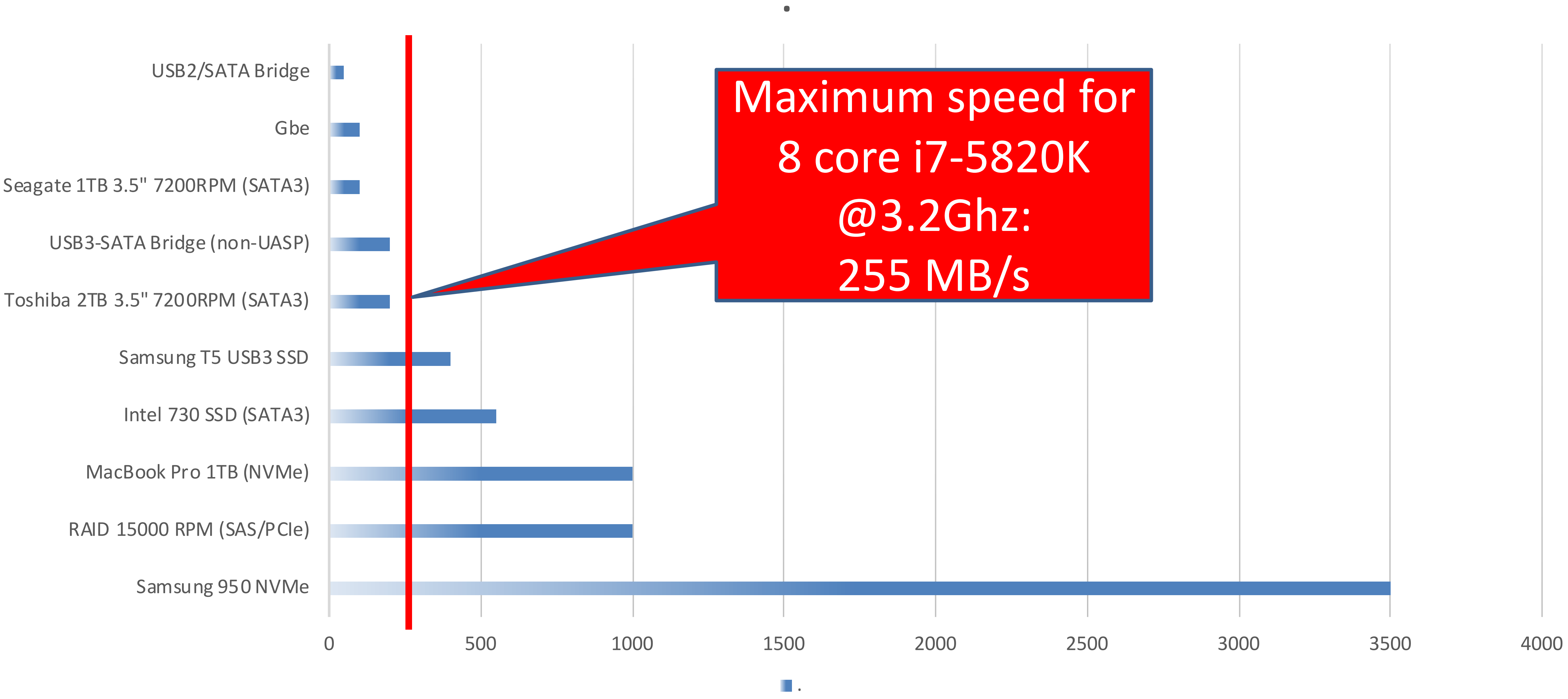
Speed up acquisition?



Current generation storage is *fast.* Old generation is *slow.*



In general E01 with compression is a bottleneck for flash based storage

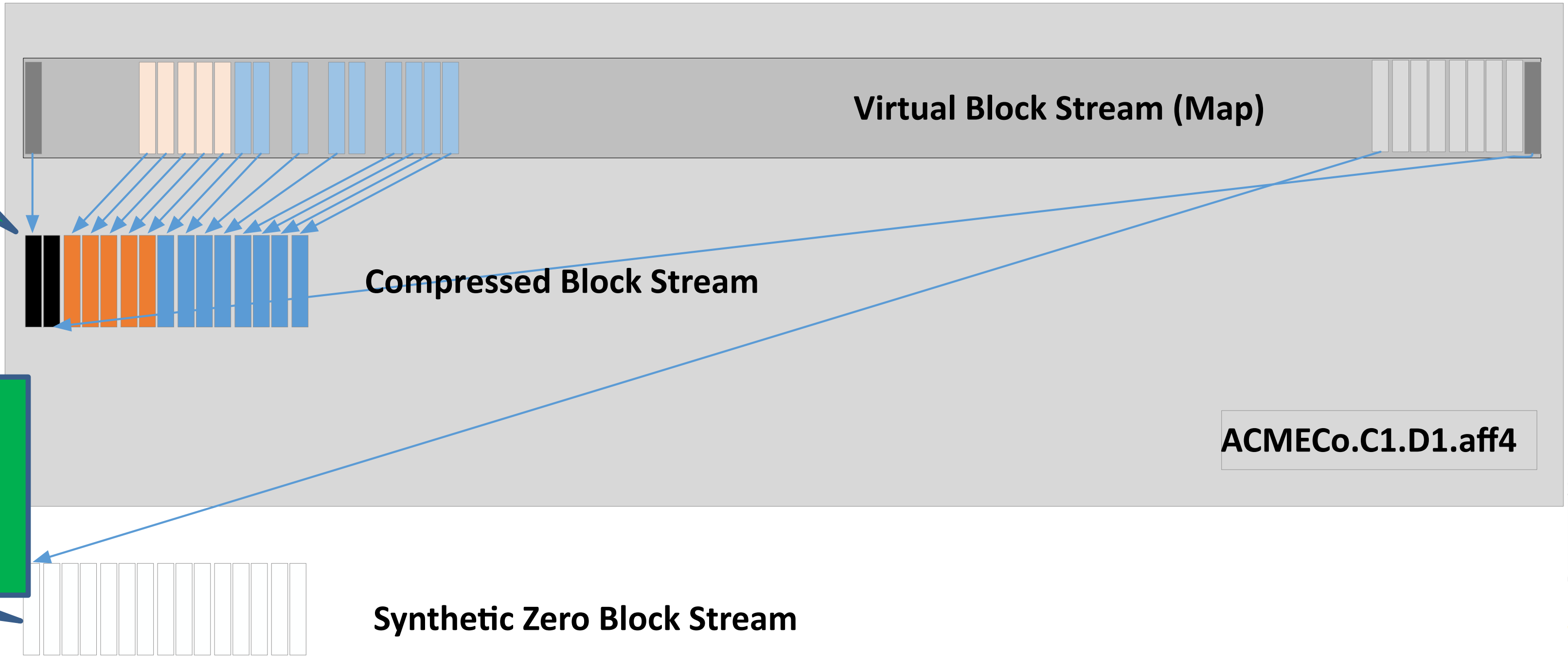


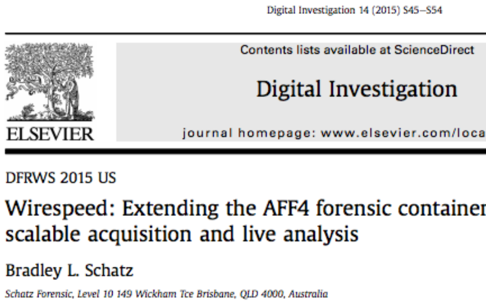
Maximum speed for 8 core i7-5820K @3.2Ghz: 255 MB/s

AFF4 (2015): Virtualisation & lightweight compression algorithms remove the heavyweight compression bottleneck.

Lightweight compression.

Highly efficient sparse data representation.




Digital Investigation 14 (2015) S45–S54

ELSEVIER

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/loca

DFRWS 2015 US

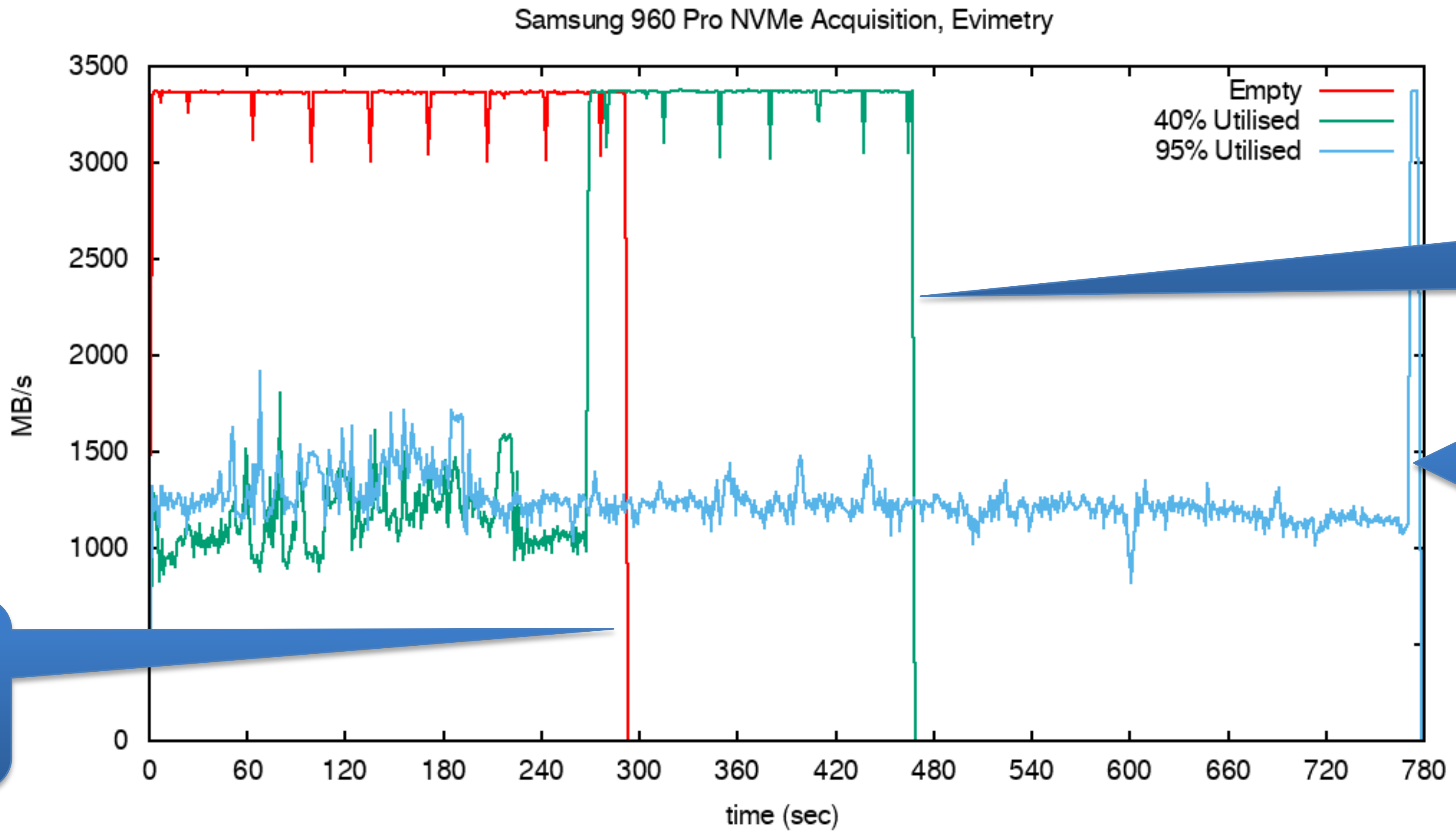
Wirespeed: Extending the AFF4 forensic container
scalable acquisition and live analysis

Bradley L. Schatz

Schatz Forensic, Level 10 149 Wickham Tce Brisbane, QLD 4000, Australia

AFF4/Evimetry shifts acquisition throughput to being CPU & IO limited

1TB NVMe Drive

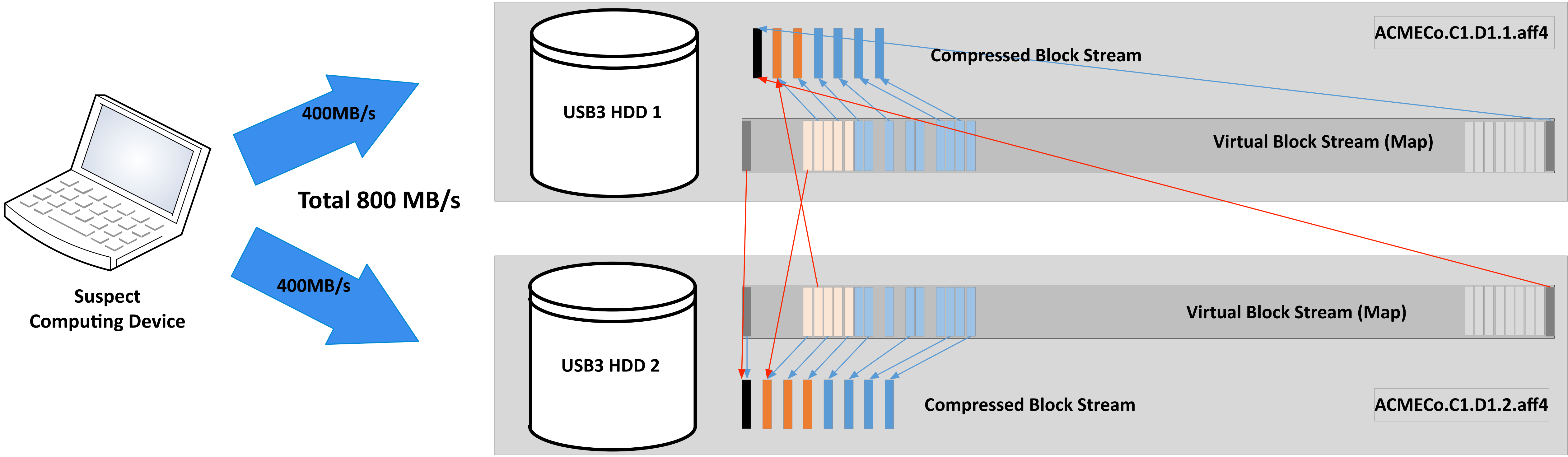


7:48
128 GB/min

12:57
77 GB/min

4:52
200 GB/min

AFF4 Striping enables scalable evidence storage via RAID0-like aggregate throughput



Most USB3 bridges are a bottleneck for SSD

Manuf.	Read MB/s	Computer interconnect	Drive	Drive interconnect	Circa	Tool
Orico	219	USB3	850 Pro	SATA	2014	1
Orico	247	USB3	850 Pro	SATA	2016	1
Orico	**+ 402**	USB3	850 Pro	SATA	2016	1
Kanex	213	Thunderbolt	850 Pro	eSATA	2015	1
Nexstar	189	USB3	850 Pro	SATA	2014	1
Nexstar	249	USB3	850 Pro	eSATA	2016	1
Probox	*** + 416**	USB3	850 Pro	SATA	2016	1
Samsung T3	**400 +**	USB3		mSATA (internal)	2016	1
Samsung T5	**445**	USB3		mSATA (internal)	2018	2
Startech	**425 +**	USB3.1	850 Pro	SATA	2018	1
Tableau T35u	270	USB3	850 Pro	SATA		2
Tableau T8u	325	USB3		USB3 to T5		2

1. BlackMagicDesign Disk Speed Test 2 Readhammer * Fails under heavy load + UASP

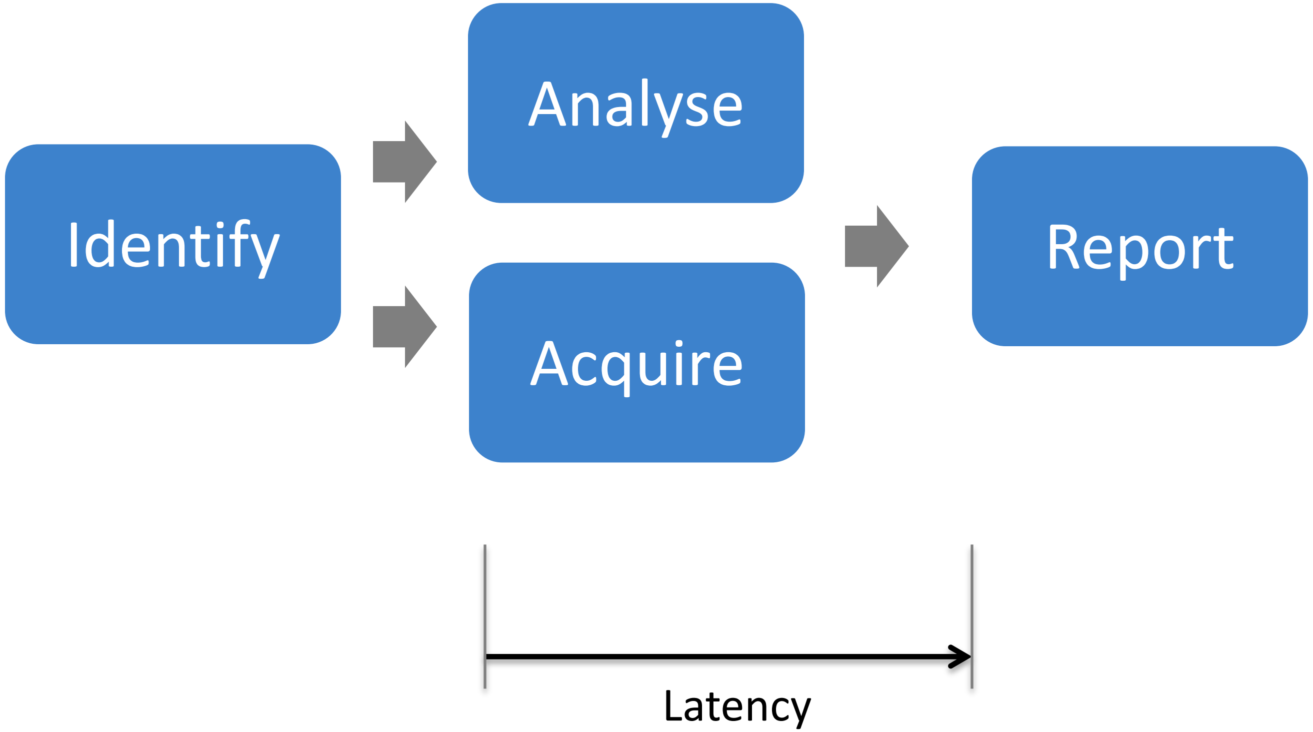
Evimetry
Digital forensics at wire speed

Rethinking workflow

Why defer analysis until acquisition completes?

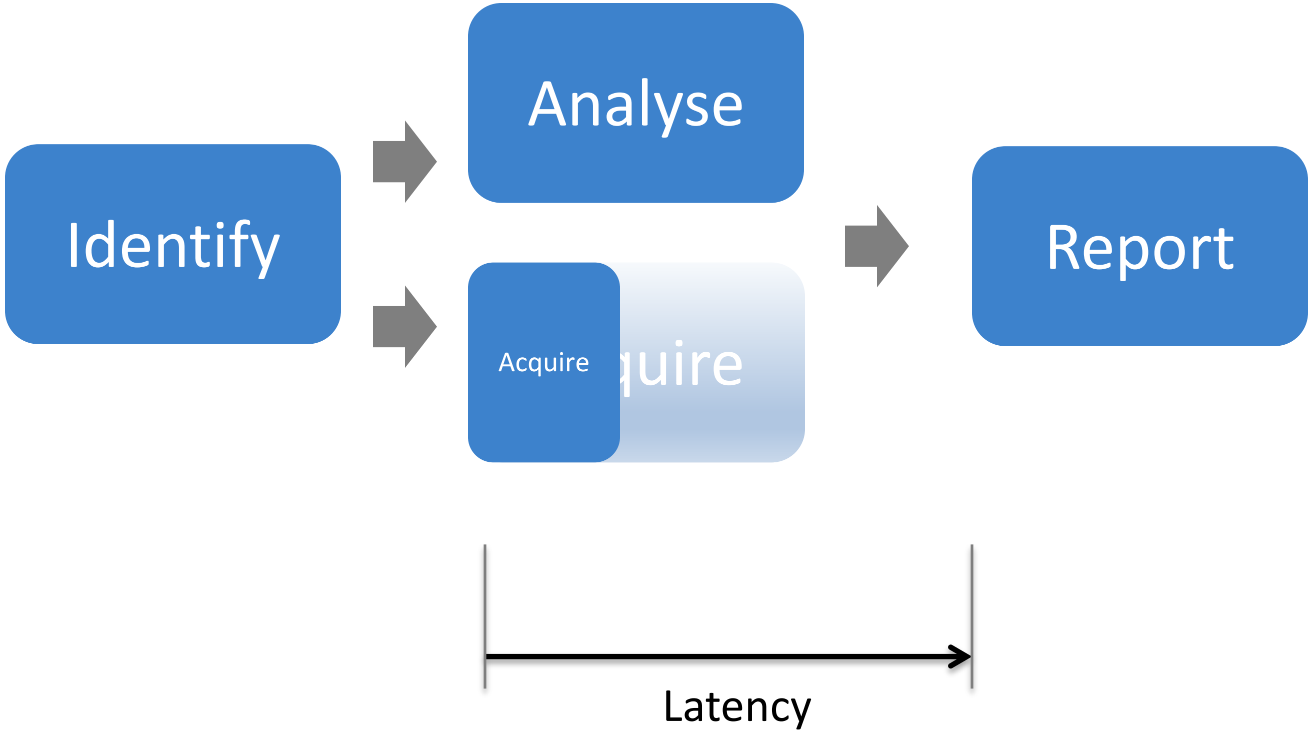
How can we reduce delays?

Why not do analysis and acquisition at the same time?

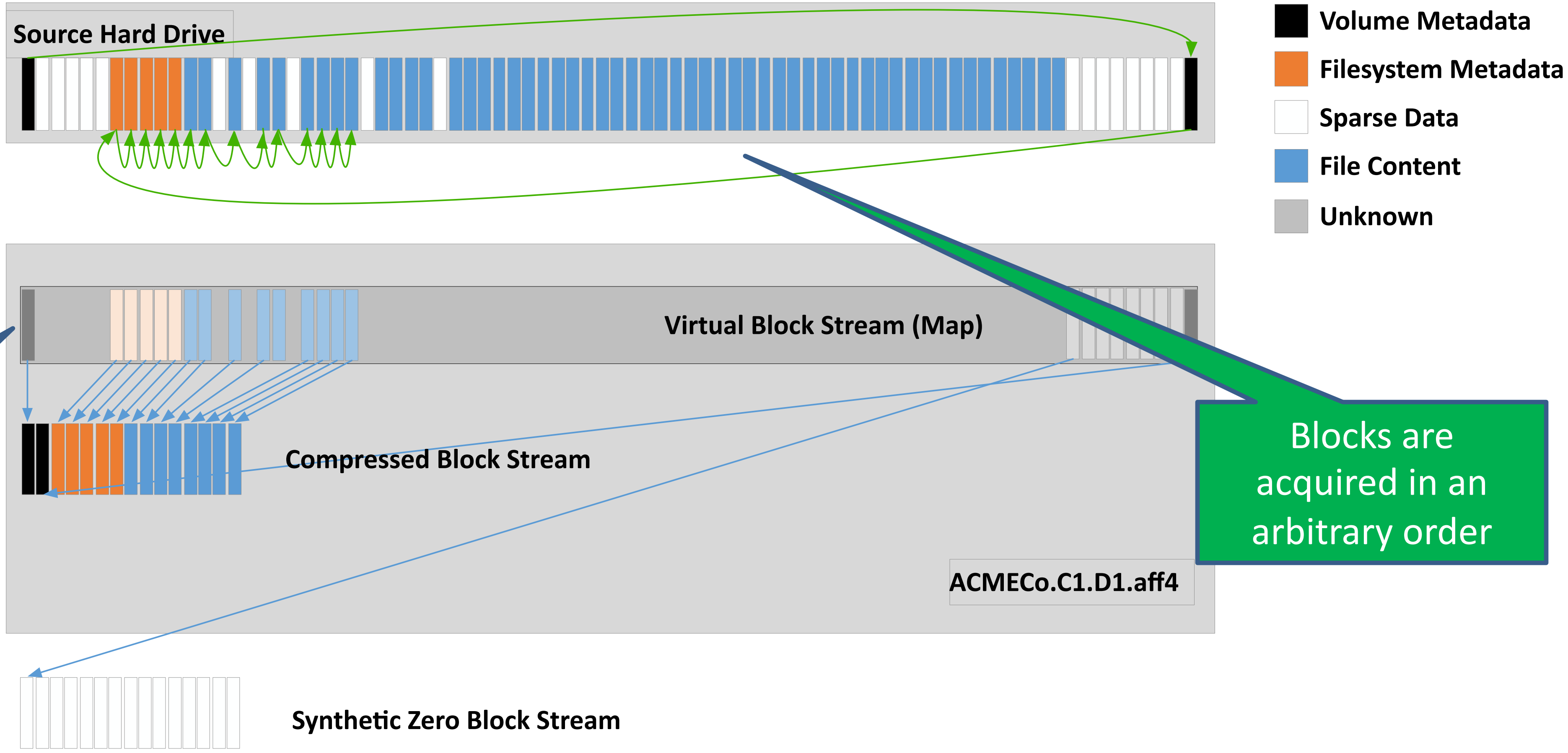


We can have both.

Traditional forensic image formats are the blocker.



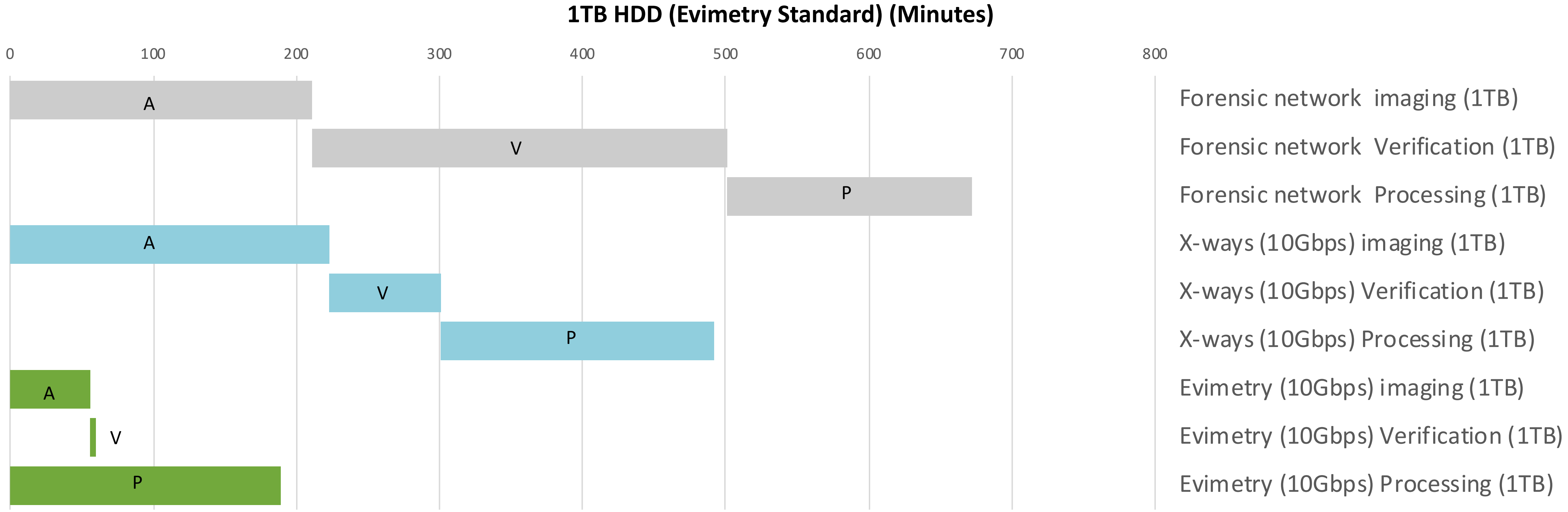
AFF4: The *non-linear bitstream image* closes the gap between analysis and acquisition.



Key advance: Virtualisation

Blocks are acquired in an arbitrary order

Analysis/Processing during Acquisition gives answers hours & days earlier per device



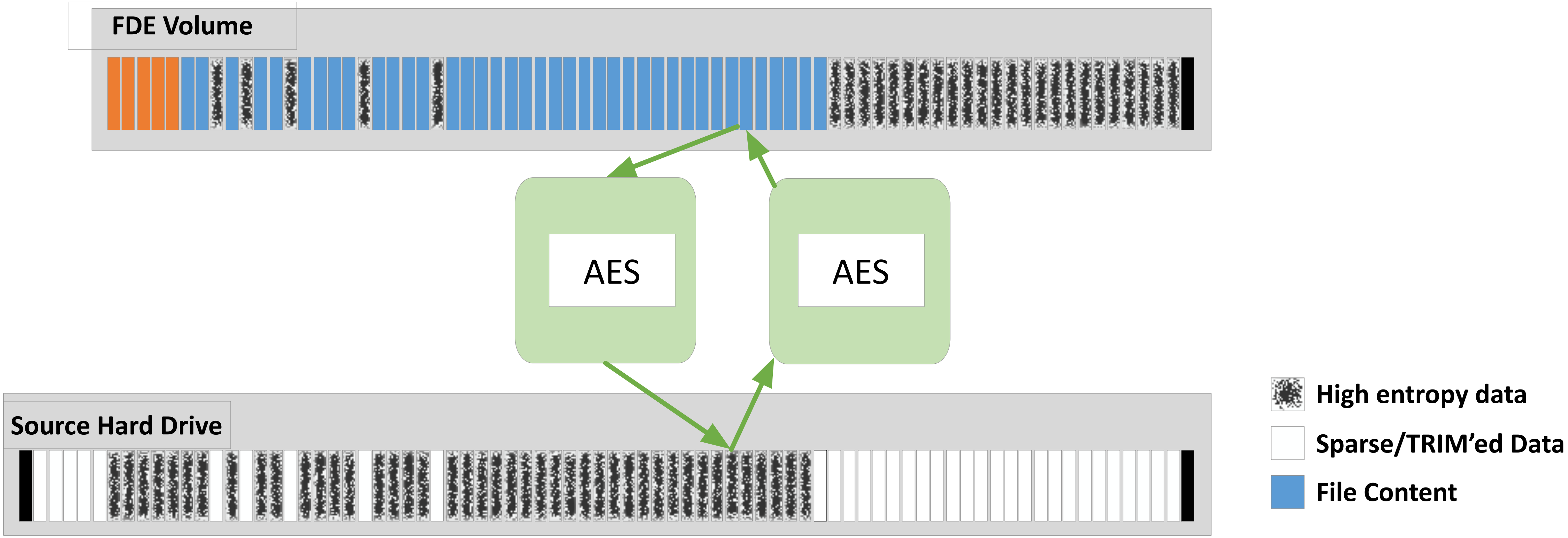
* Independent testing conducted by UK based regulator

Evimetry
Digital forensics at wire speed

Full Disk Encryption on flash

Physical is far more efficient that decrypted physical

FDE encrypts cleartext data for storage



FDE Volume

AES

AES

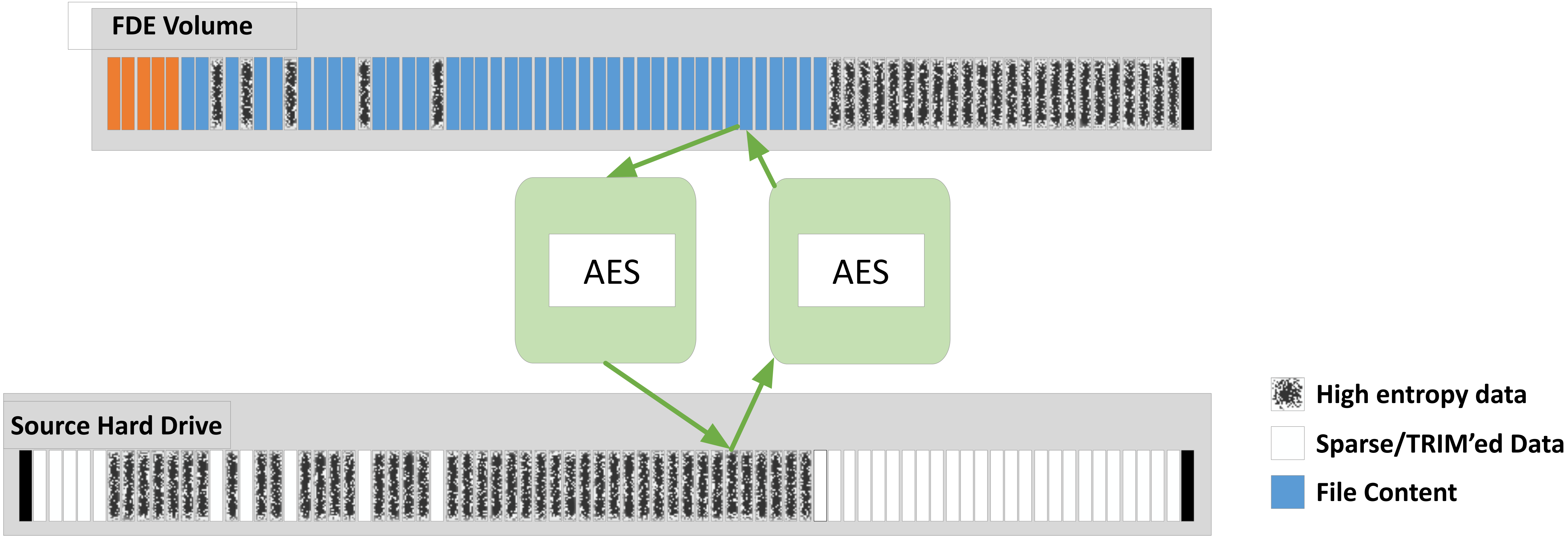
Source Hard Drive

▨ High entropy data

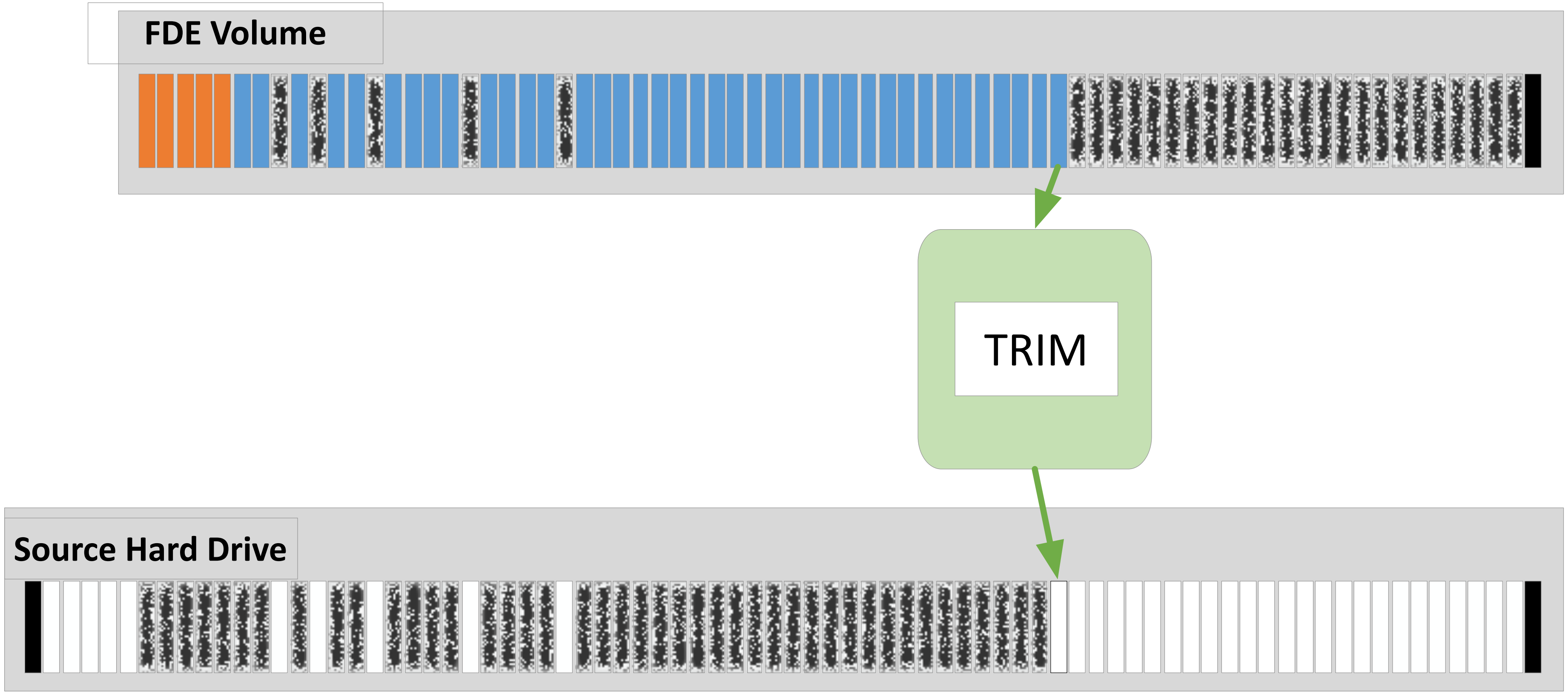
□ Sparse/TRIM’ed Data

🟦 File Content

What about unallocated data?



Deletion/formatting causes TRIM with flash storage

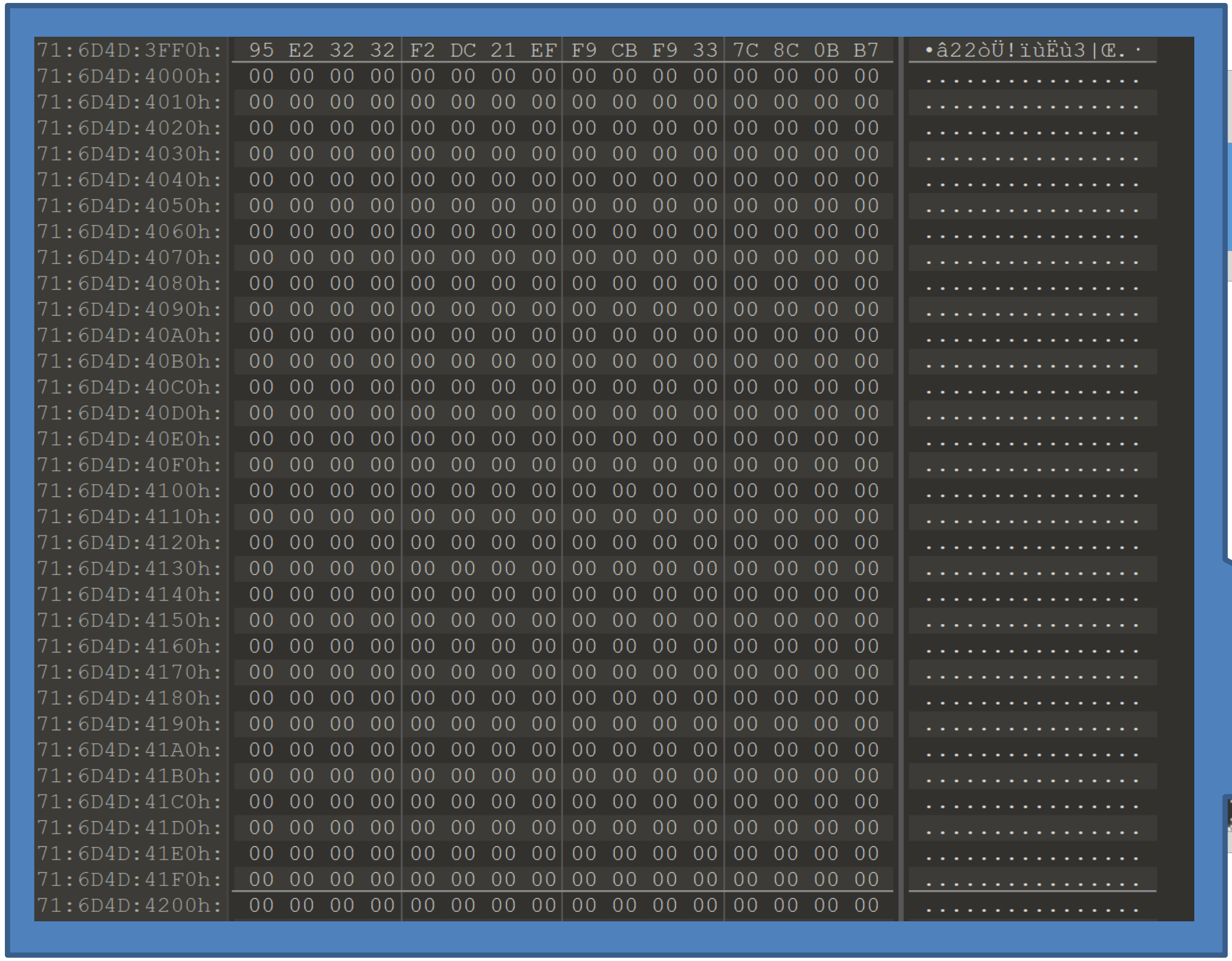


▨ High entropy data

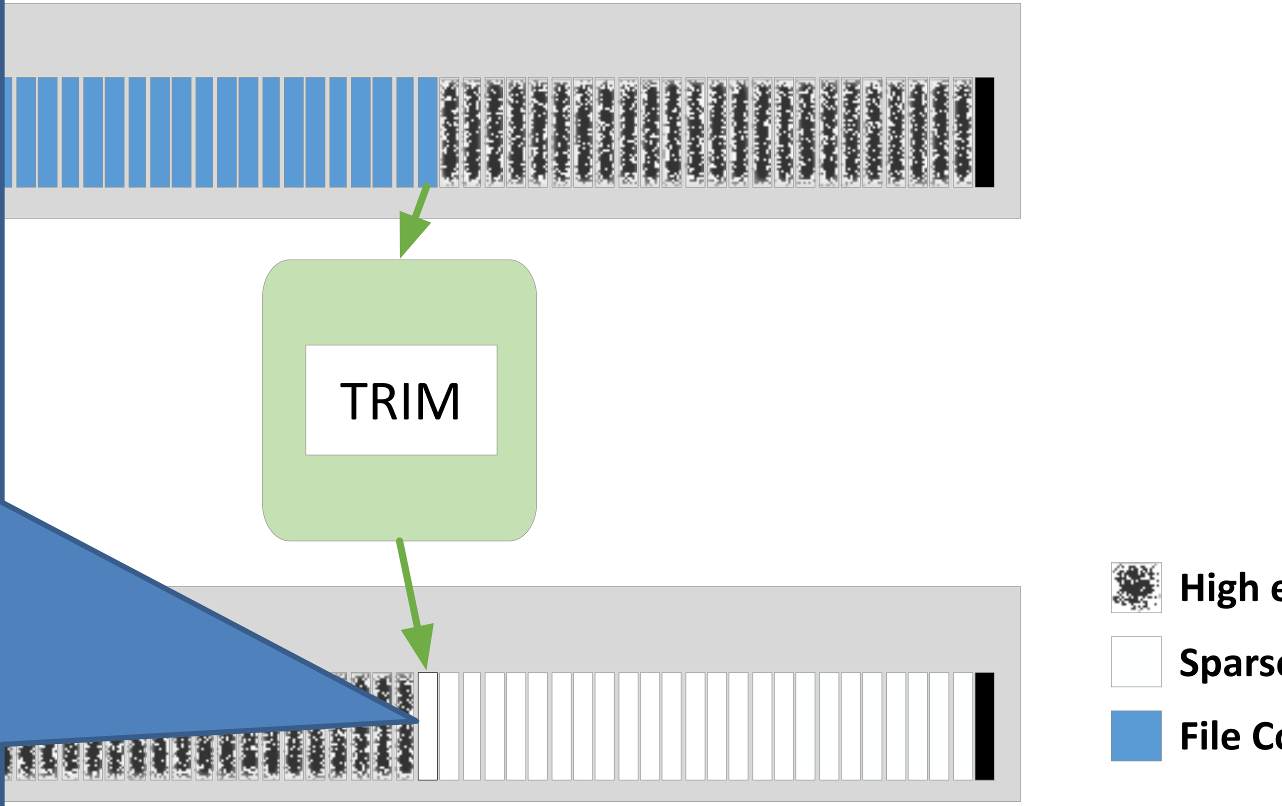
□ Sparse/TRIM'ed Data

🟦 File Content

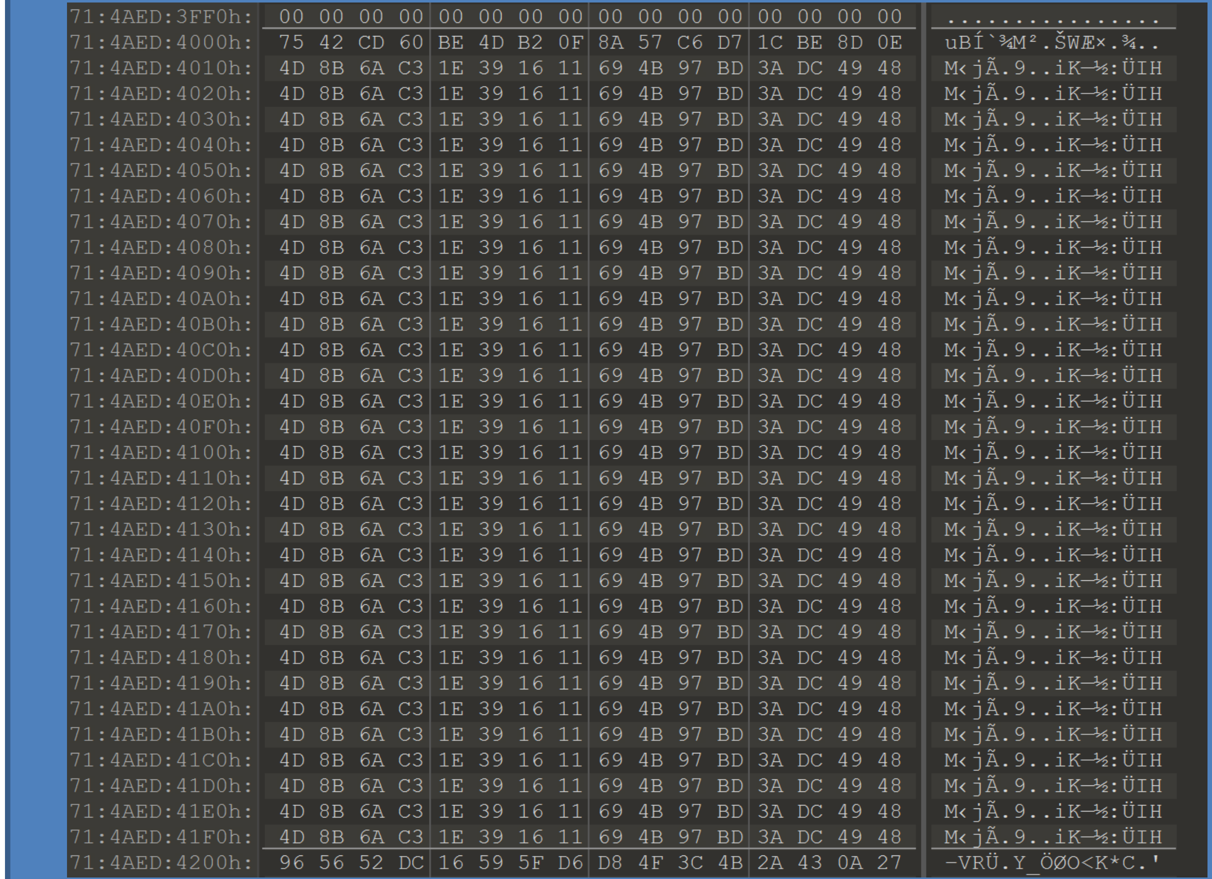
Deletion/formatting causes TRIM with flash storage



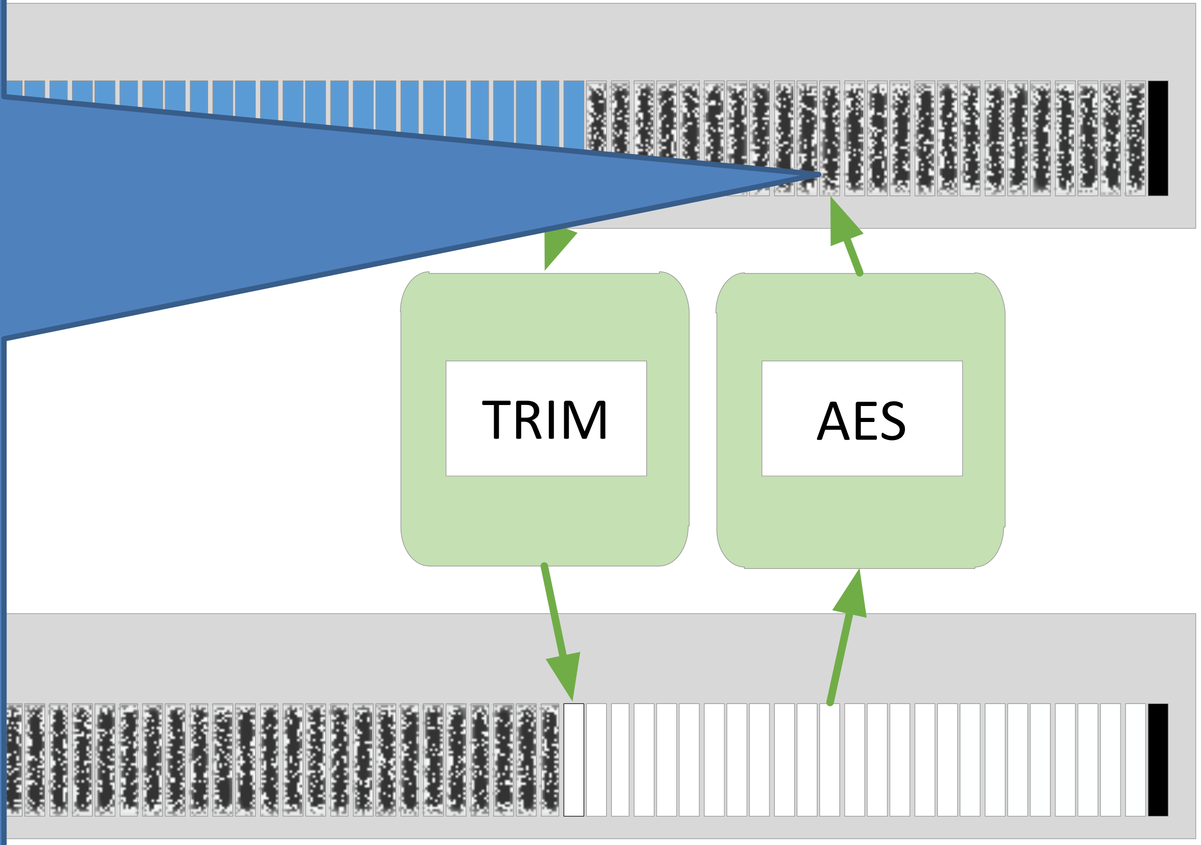
```
71:6D4D:3FF0h:  95 E2 32 32 F2 DC 21 EF F9 CB F9 33 7C 8C 0B B7  •â22òÜ!ïùËù3|Œ.·
71:6D4D:4000h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:4010h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:4020h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:4030h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:4040h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:4050h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:4060h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:4070h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:4080h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:4090h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:40A0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:40B0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:40C0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:40D0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:40E0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:40F0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:4100h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:4110h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:4120h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:4130h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:4140h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:4150h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:4160h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:4170h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:4180h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:4190h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:41A0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:41B0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:41C0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:41D0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:41E0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:41F0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:6D4D:4200h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```



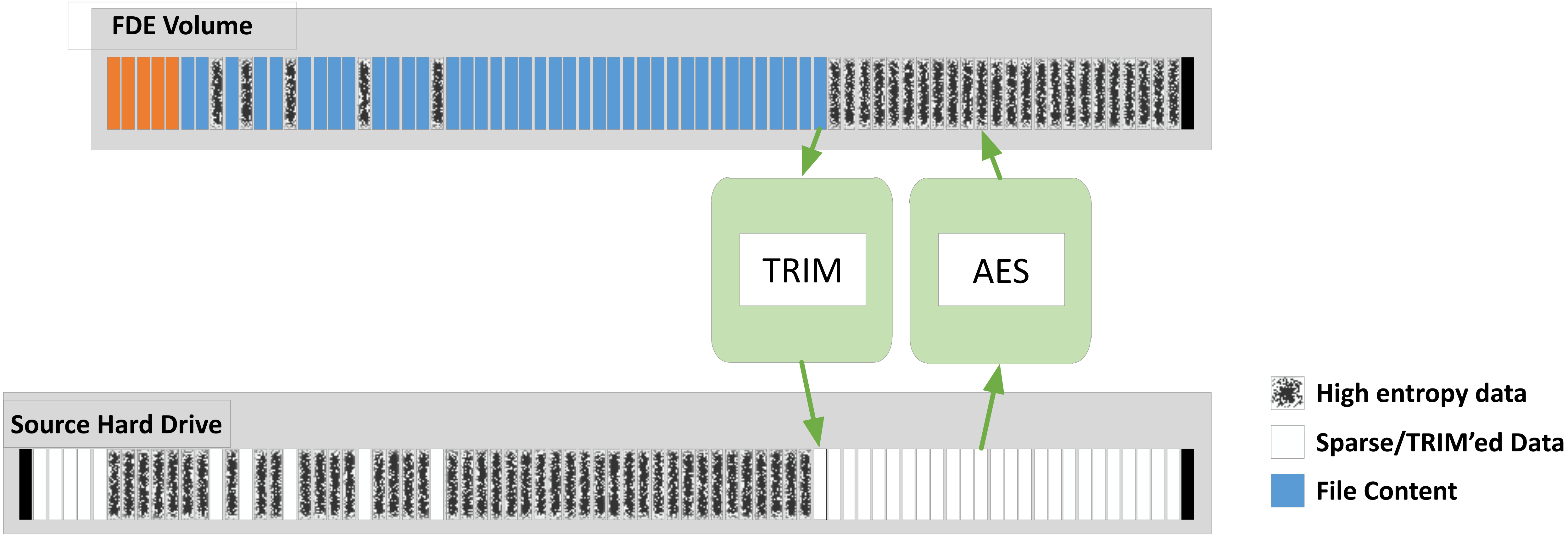
TRIM’ed blocks are re-encrypted on read



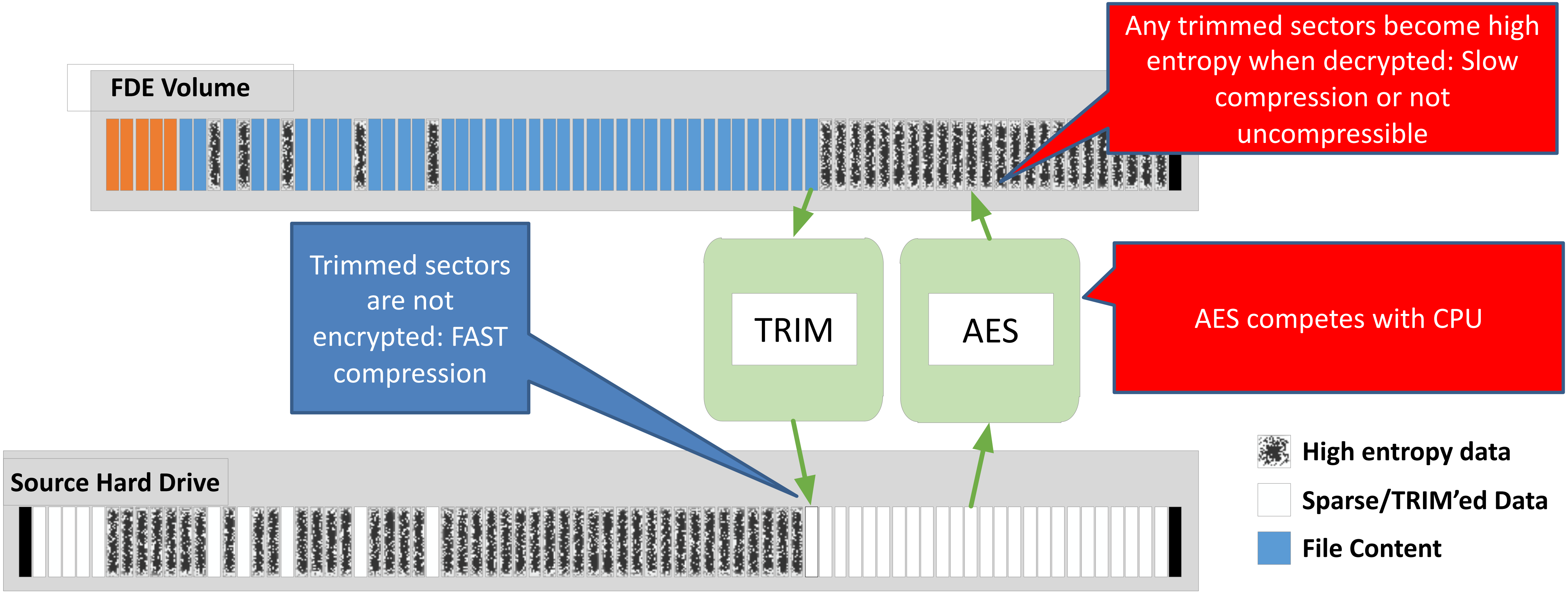
```
71:4AED:3FF0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
71:4AED:4000h:  75 42 CD 60 BE 4D B2 0F 8A 57 C6 D7 1C BE 8D 0E  uBÍ`¾M².ŠWÆ×.¾..
71:4AED:4010h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:4020h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:4030h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:4040h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:4050h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:4060h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:4070h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:4080h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:4090h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:40A0h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:40B0h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:40C0h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:40D0h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:40E0h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:40F0h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:4100h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:4110h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:4120h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:4130h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:4140h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:4150h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:4160h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:4170h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:4180h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:4190h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:41A0h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:41B0h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:41C0h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:41D0h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:41E0h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:41F0h:  4D 8B 6A C3 1E 39 16 11 69 4B 97 BD 3A DC 49 48  M‹jÃ.9..iK—½:ÜIH
71:4AED:4200h:  96 56 52 DC 16 59 5F D6 D8 4F 3C 4B 2A 43 0A 27  –VRÜ.Y_ÖØO<K*C.'
```



Which do we acquire?



Which do we acquire? *Unencrypted ?*

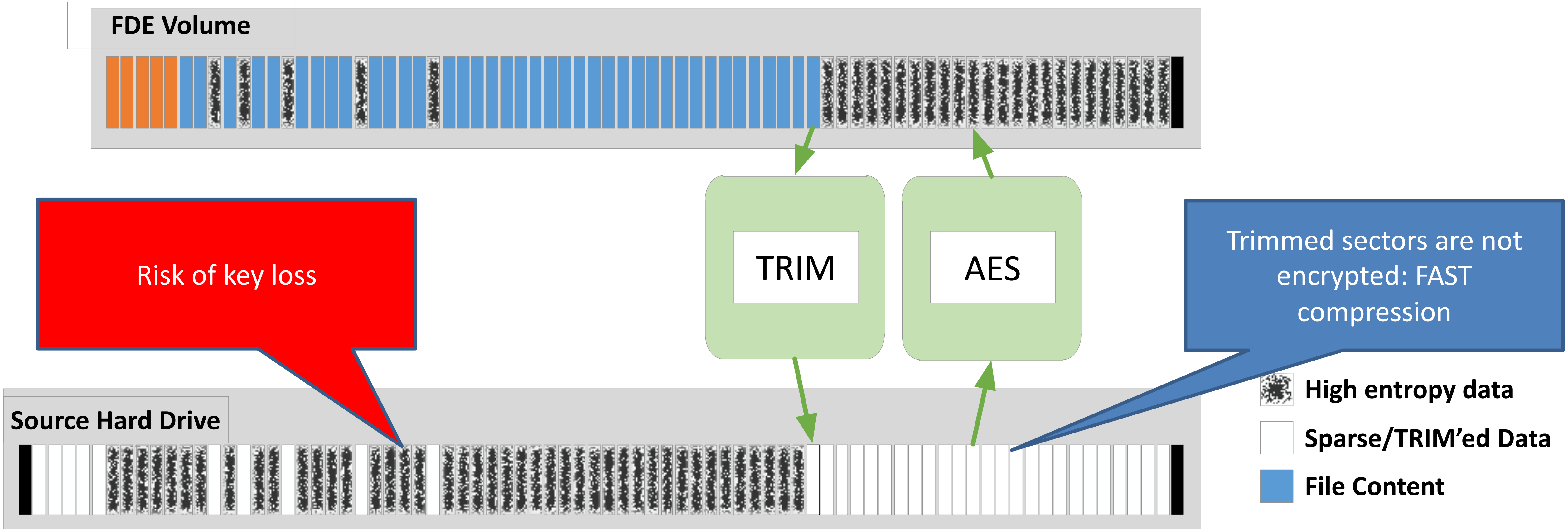


Any trimmed sectors become high entropy when decrypted: Slow compression or not uncompressible

Trimmed sectors are not encrypted: FAST compression

AES competes with CPU

Which do we acquire? *Physical ?*



Risk of key loss

Trimmed sectors are not encrypted: FAST compression

In summary

- Decrypted volume
  - Resulting image is same size as volume
  - Slower imaging, copying and verification
- Physical
  - Acquisition is far faster
  - Resulting image is proportional to sparse size
  - Acquisition of sparse >3 x faster than data (NVME)
  - Verification of sparse takes sub-seconds with AFF4

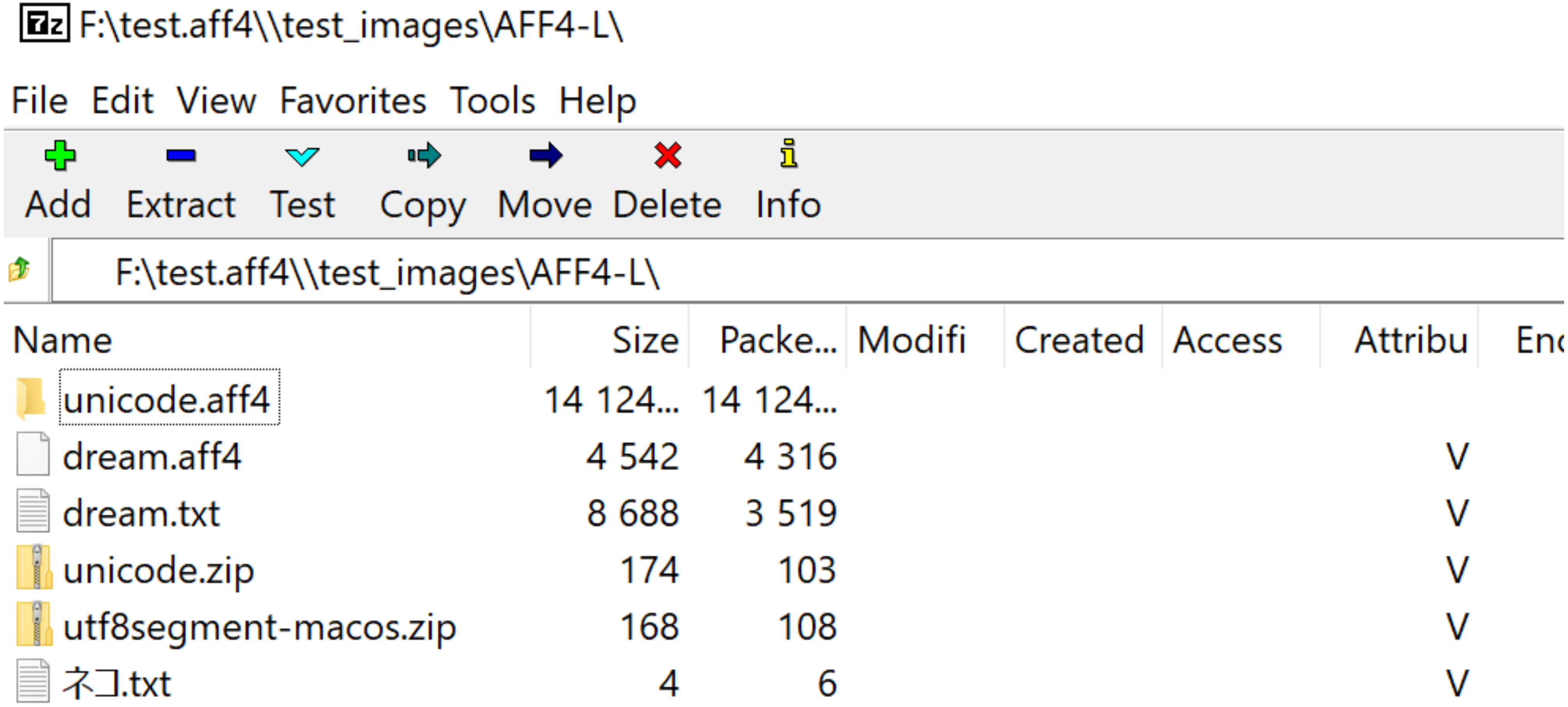
AFF4 Logical Imaging

AFF4 Logical Imaging

Code available now in the pyaff4 github

```
git clone --recurse-submodules
https://github.com/aff4/pyaff4.git
python aff4.py -r --create-logical test.aff4
./test_images/AFF4-L/
Creating AFF4Container: file://test.aff4 <aff4://05e730d3-
f6de-4961-9e9a-a30d5043a562>
     Adding: ./test_images/AFF4-L/
     Adding: ./test_images/AFF4-L/dream.aff4
     Adding: ./test_images/AFF4-L/dream.txt
     Adding: ./test_images/AFF4-L/unicode.aff4
     Adding: ./test_images/AFF4-L/unicode.zip
     Adding: ./test_images/AFF4-L/utf8segment-macos.zip
     Adding: ./test_images/AFF4-L/ネコ.txt
```

AFF4 Logical Images are viewable in 7Zip and WinRAR



F:\test.aff4\\test_images\AFF4-L\

F:\test.aff4\\test_images\AFF4-L\

Name	Size	Packe...	Modifi	Created	Access	Attribu	Enc
unicode.aff4	14 124...	14 124...					
dream.aff4	4 542	4 316				V	
dream.txt	8 688	3 519				V	
unicode.zip	174	103				V	
utf8segment-macos.zip	168	108				V	
ネコ.txt	4	6				V	

Evimetry

Digital forensics at wire speed

Exploitation-oriented forensics

iOS acquisition completeness is dwindling
*For private practice examiners

- Current backup-based logical imaging
  - No email,
  - No SQLite WAL files
  - Large swaths of filesystem and useful traces missing
- * CAIS/Greykey
  - Will produce complete logical images for govt. licencees
  - Will they assist in Civil matters? Not in my experience.

Exploitation/Jailbreaking is increasingly being used in civil forensic practice

- Forensic questions
  - Was my phone compromised?
  - Can I get deleted text messages?
  - What time was a voice message first recorded?
  - Deleted data recovery (SQLite WAL)
  - Inaccessible information

iOS jailbreaking in forensics: literature

- Elcomsoft suggest the following jailbreaks to enable running their software

  iOS 10:
  - h3lix (iOS 10.0-10.3.3), 32-bit devices, https://h3lix.tihmstar.net/
  - Meridian (iOS 10.0-10.3.3), 64-bit devices, https://meridian.sparkes.zone/

  iOS 11:
  - LiberIOS (iOS 11.0-11.1.2), 64-bit devices, http://newosxbook.com/liberios/
  - Electra (iOS 11.0-11.1.2), 64-bit devices, https://coolstar.org/electra/

- Sara Edwards* suggests the following, with an open source methodology

  iOS 11:
  - LiberIOS (iOS 11.), 64-bit devices
  - Meridian (iOS 10), 64-bit devices

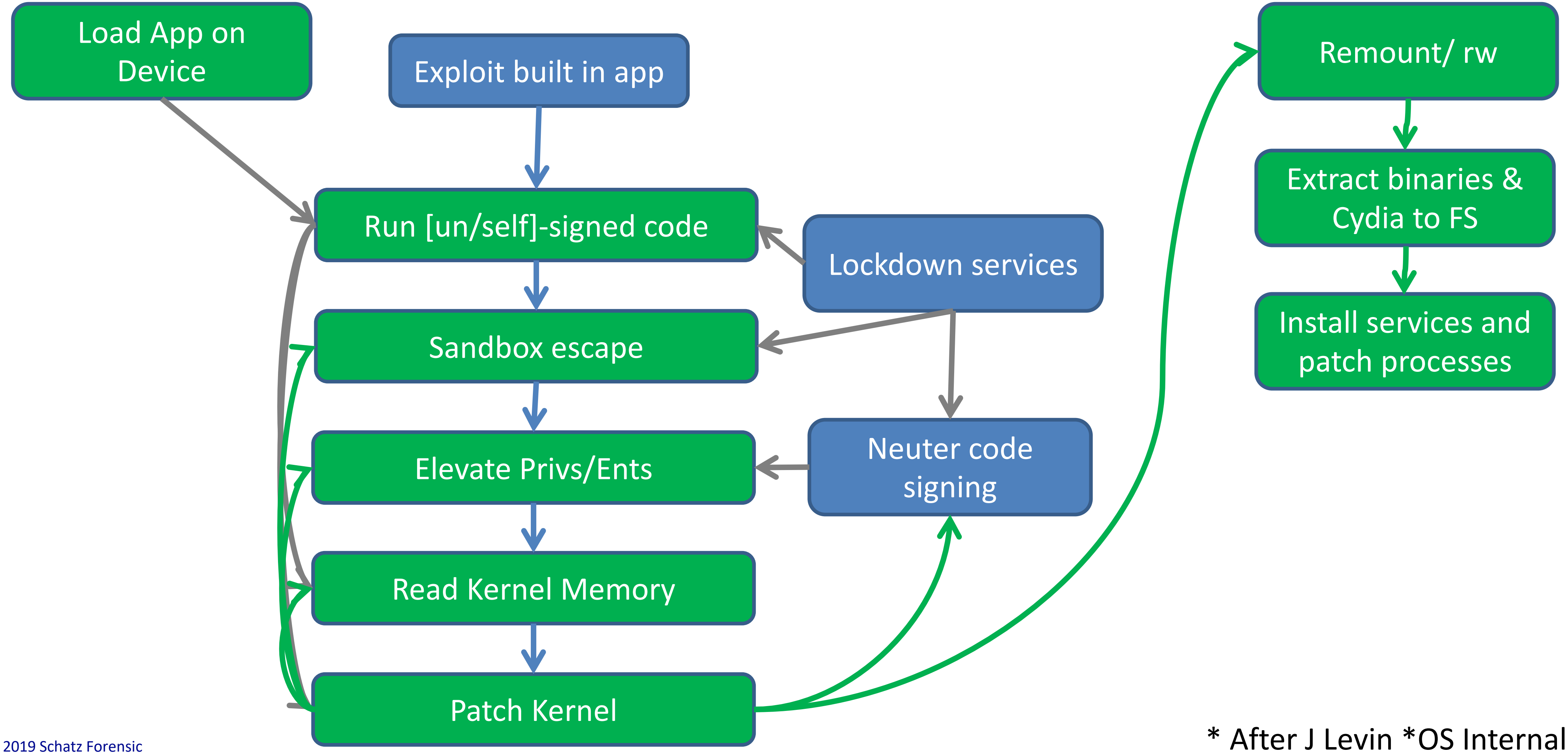
  * See “iOS imaging on the Cheap”

Current approaches in a nutshell

- Download jailbreak from internet
- Install and run jailbreak on the suspect iPhone*
- Install SSHD using Cydia
- Use SCP or netcat to copy the filesystem

* After you have tested it on a similar phone

Recent jailbreak operation



* After J Levin *OS Internals Volume 3

How can I tell if an iPhone **IS** jailbroken

- SSH available on port 22 (or other)
- -or- bash bound to a TCP port (drive via nc)
  - – More work here needed scanning the port range of an iPhone
- AFC service allows full access

Jailbreaking installs significant amounts of untrusted code on the suspect device

- /Applications/Cydia.app
- /bin and /usr/bin
- /var/stash & /var/lib/cydia - Cydia artefacts
- /var/mobile/Library/Preferences/com.saurik.Cydia.plist.
- /var/MobileDevice/ProvisioningProfiles : provisioning profiles
- /usr/libexec/cydia/*

Other traces include provisioning profiles

```
bradleys-iPad:/private/var/tmp/bootstrap/bin root# ls -l /var/MobileDevice/ProvisioningProfiles
total 32
-rw-r--r-- 1 mobile mobile 7614 Jan 24  2018 08806c56-9074-4931-86a4-cc162dceb903
-rw-r--r-- 1 mobile mobile 7593 Jan 29  2018 3bcb7785-f9db-4065-94c9-b22350545df3
-rw-r--r-- 1 mobile mobile 7473 Jan 25  2018 71a534c4-d32c-44fc-92c3-d1163a4ca702
-rw-r--r-- 1 mobile mobile 7774 Nov 11 19:03 7b1d1b07-4e32-4a8f-a4f3-0dc4fc273f14
```

What are the risks of jailbreaking?

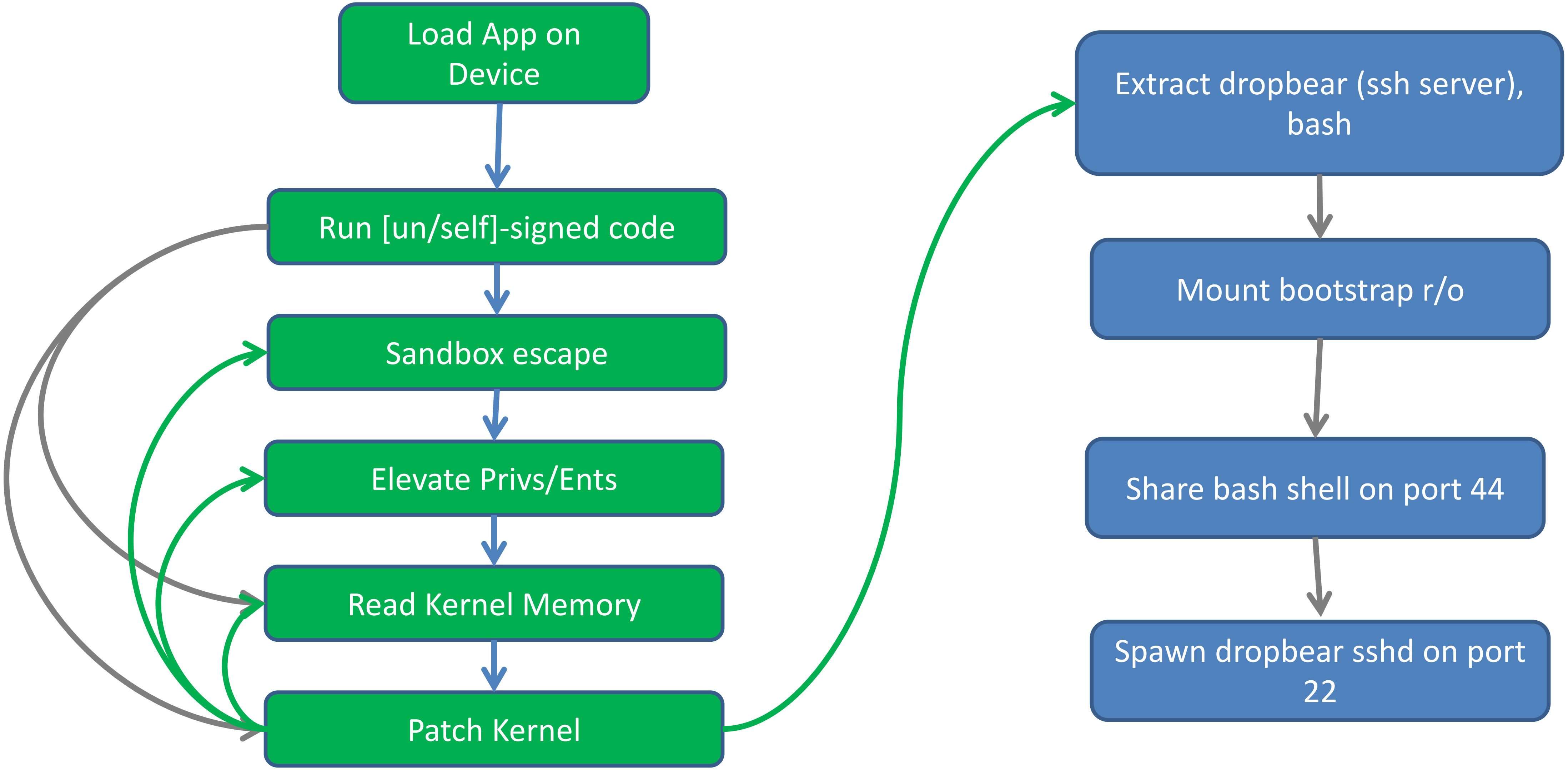
- Uncertain provenance of jailbreak and accompanying 3rd party binaries
- Jailbreak collides with prior jailbreak rendering phone inaccessible
- Jailbreak overwrites traces of prior jailbreak
- Arguments re forensic soundness
- Widespread timestamp overwriting
  - Stashing (OS file relocation) [1]
  - More of an issue with Pangu era jailbreaks
- Partition resizing ?

- [1] https://www.theiphonewiki.com/wiki//private/var/stash

Forensic jailbreak prototype 1

- Overriding goals:
  - Minimise changes to filesystem
  - Don’t overwrite existing jailbreak traces
  - Don’t collide (eg TCP listening port) with existing jailbreaks
  - Don’t remount root as R/W
- Theory
  - Load minimal SSH server and rely on SFTP for file enumeration/copy

Forensic jailbreak prototype 1


Load App on Device
Run [un/self]-signed code
Sandbox escape
Elevate Privs/Ents
Read Kernel Memory
Patch Kernel
Extract dropbear (ssh server), bash
Mount bootstrap r/o
Share bash shell on port 44
Spawn dropbear sshd on port 22

Forensic jailbreak prototype 1

persistent changes made

- Load app on device:
  - new name - PhoenixShell.app
- Extract to /private/var/tmp/
  - bash
  - dropbear
- Create folder under /private/var/tmp/
  - bootstrap (PhoenixShell.app/bootstrap.dmg mounted here)

Forensic jailbreak prototype 1:

Client side usage

- In one shell

```
neon:~ bradley$ iproxy 4444 44
waiting for connection
```

- In another

```
neon:pyaff4 bradley$ nc localhost 4444
bradleys-iPad:/ root#
```

- Manually
  - Use ssh, tar, stat for examination

Forensic jailbreak prototype 1

Automated client side acquisition

- Establish python/paramiko SSH connection
- Upload stat to tmp folder on device using unique name
- Enumerate filesystem metadata and store in AFF4 image
- Supplement filesystem metadata with file creation time metadata from stat
- Copy file content using SCP into AFF4 image

Forensic jailbreak protptype 1

AFF4 Logical Image Contents

```
neon:phoenixShell bradley$ unzip -l /tmp/iPad.aff4
Archive:  /tmp/iPad.aff4
aff4://2b1e5aae-b7cf-42f4-bdcb-c1c8aa4e94ab
  Length      Date    Time    Name
---------  ---------- -----   ----
   154048  00-00-1980 00:00   /usr/bin/brctl
    52240  00-00-1980 00:00   /usr/bin/arch
    87856  00-00-1980 00:00   /usr/bin/captoinfo
    49856  00-00-1980 00:00   /usr/bin/cfversion
     4374  00-00-1980 00:00   information.turtle
     6558  00-00-1980 00:00   /usr/bin/apt-key
     3667  00-00-1980 00:00   /usr/bin/c_rehash
     6822  00-00-1980 00:00   /usr/bin/bashbug
       28  00-00-1980 00:00   version.txt
       43  00-00-1980 00:00   container.description
---------                     -------
   365492                     10 files
```

Forensic jailbreak technique – try #1:

AFF4 Logical Metadata

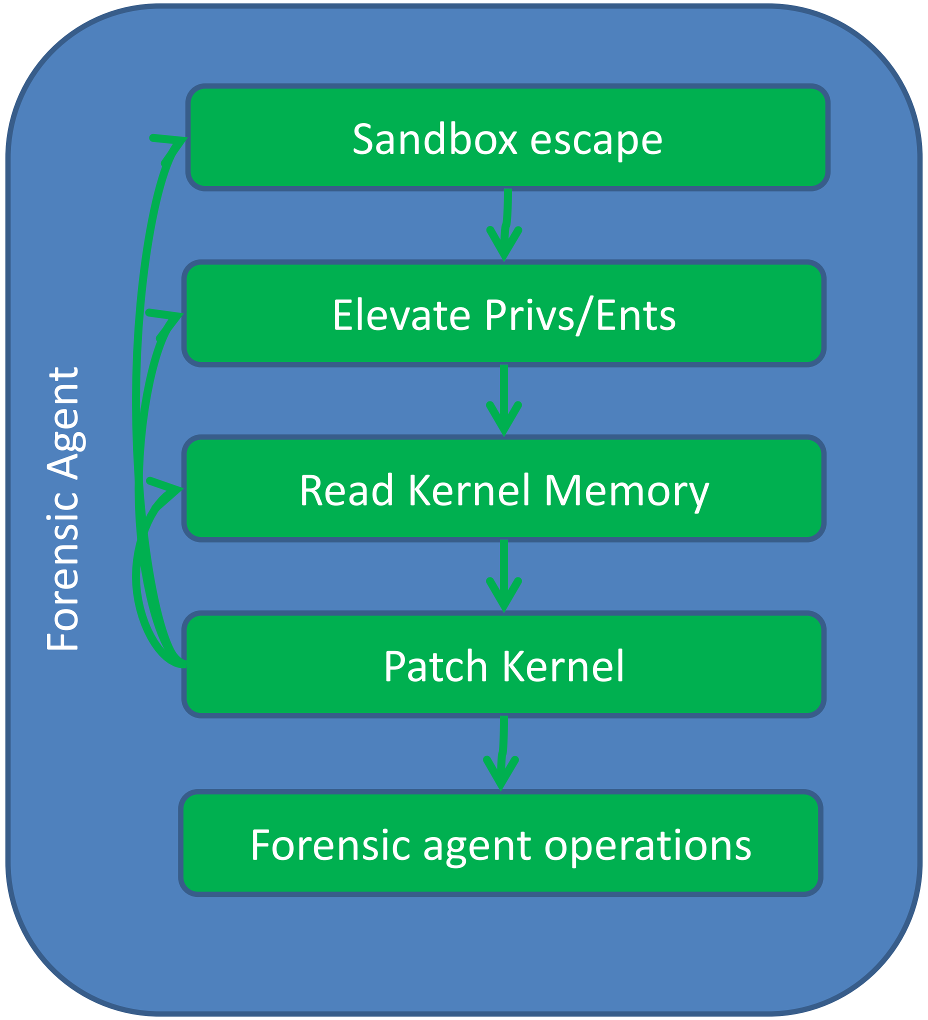
```
<aff4://685faddc-be15-429e-b240-6bd002e1196b//.fseventsd/00000000002a9441> a aff4:FileImage,
        aff4:Image ;
    aff4:birthTime "2018-11-23T16:33:48+10:00"^^xsd:datetime ;
    aff4:hash "ff928ebb6fc2efcf6f7d02619c3d832a"^^aff4:MD5,
        "61e09a12ff94516d334ac311e4c08144f37604bc"^^aff4:SHA1 ;
    aff4:lastAccessed "2018-11-23T16:33:48+10:00"^^xsd:datetime ;
    aff4:lastWritten "2018-11-23T16:33:48+10:00"^^xsd:datetime ;
    aff4:originalFileName "/.fseventsd/00000000002a9441"^^xsd:string ;
    aff4:recordChanged "2018-11-23T16:33:48+10:00"^^xsd:datetime ;
    aff4:size 23047 .
```

Forensic jailbreak prototype 1:
Limitations

- Needs complex jailbreak to run SSH server, bash & stat
- Uncertain operation in presence of still-running jailbreak
- Medium impact on changes to filesystem

Forensic jailbreak prototype 2:

- Encapsulate exploitation in same process as forensic agent
- Less complex jailbreak needed
- No third party binaries needed
- Minimal impact on suspect filesystem



Evimetry

Digital forensics at wire speed

FINISH

Acknowledgements

- Michael Cohen & Simson Garfinkel
  - Early AFF4 research collaborators
- Michael Cohen
  - Ongoing AFF4 standardisation collaborator
- Qld. Dept. Science Technology & Innovation
  - Ignite Innovation funding
- Our licencees and supporters
- @siguza
  - Forensic jailbreaking collaborator

Evimetry

Digital forensics at wire speed

Contact

Dr Bradley Schatz
https://evimetry.com/
bradley@evimetry.com
@blschatz