black hat USA 2017

JULY 22-27, 2017
MANDALAY BAY / LAS VEGAS

POLITECNICO MILANO 1863
DIPARTIMENTO DI ELETTRONICA INFORMAZIONE E BIOINGEGNERIA

TREND MICRO™

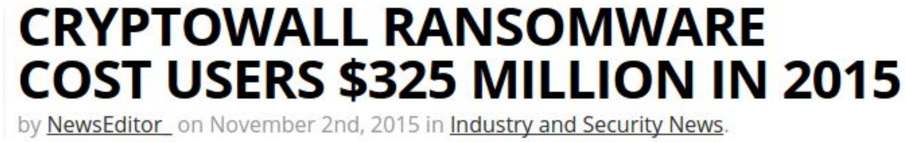
ShieldFS: The Last Word in Ransomware Resilient Filesystems

Andrea Continella, Alessandro Guagnelli, Giovanni Zingaro, Giulio De Pasquale,
Alessandro Barenghi, Stefano Zanero, **Federico Maggi**

* US patent pending

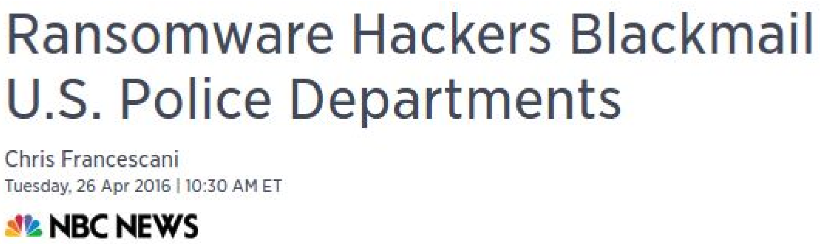
#BHUSA / @BLACKHATEVENTS

2016-17 the "years of extortion"



CRYPTOWALL RANSOMWARE COST USERS $325 MILLION IN 2015

by NewsEditor on November 2nd, 2015 in Industry and Security News.

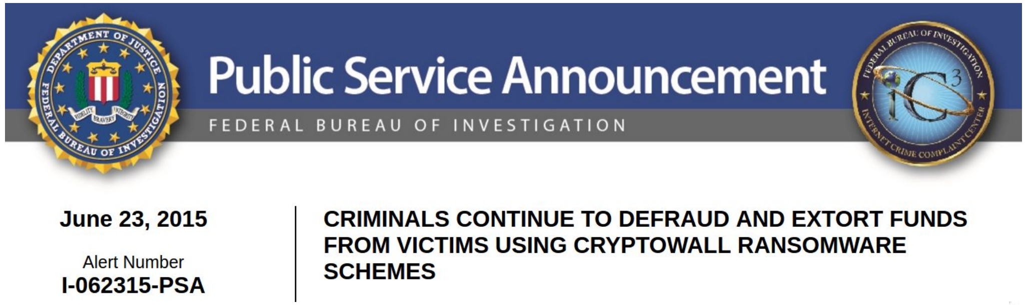


Ransomware Hackers Blackmail U.S. Police Departments

Chris Francescani

Tuesday, 26 Apr 2016 | 10:30 AM ET

NBC NEWS



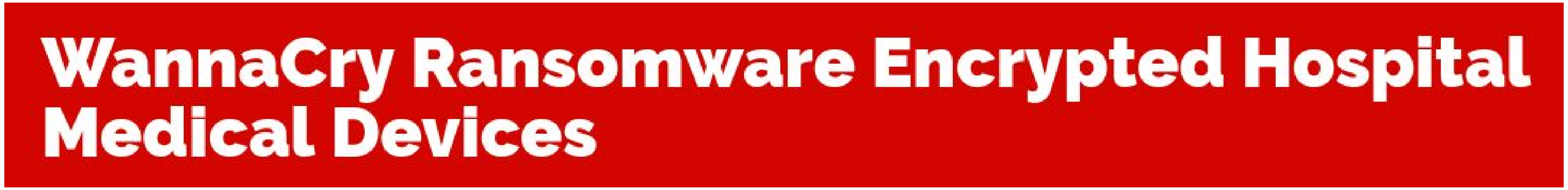
Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

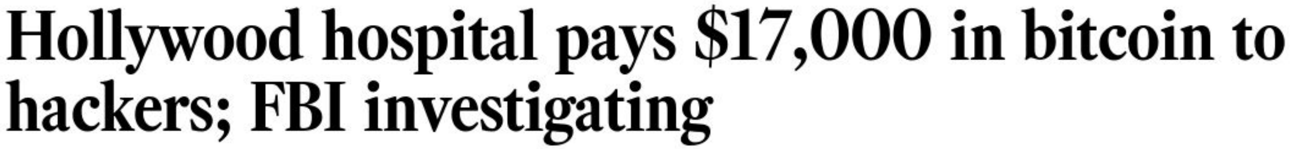
June 23, 2015

Alert Number
I-062315-PSA

CRIMINALS CONTINUE TO DEFRAUD AND EXTORT FUNDS FROM VICTIMS USING CRYPTOWALL RANSOMWARE SCHEMES

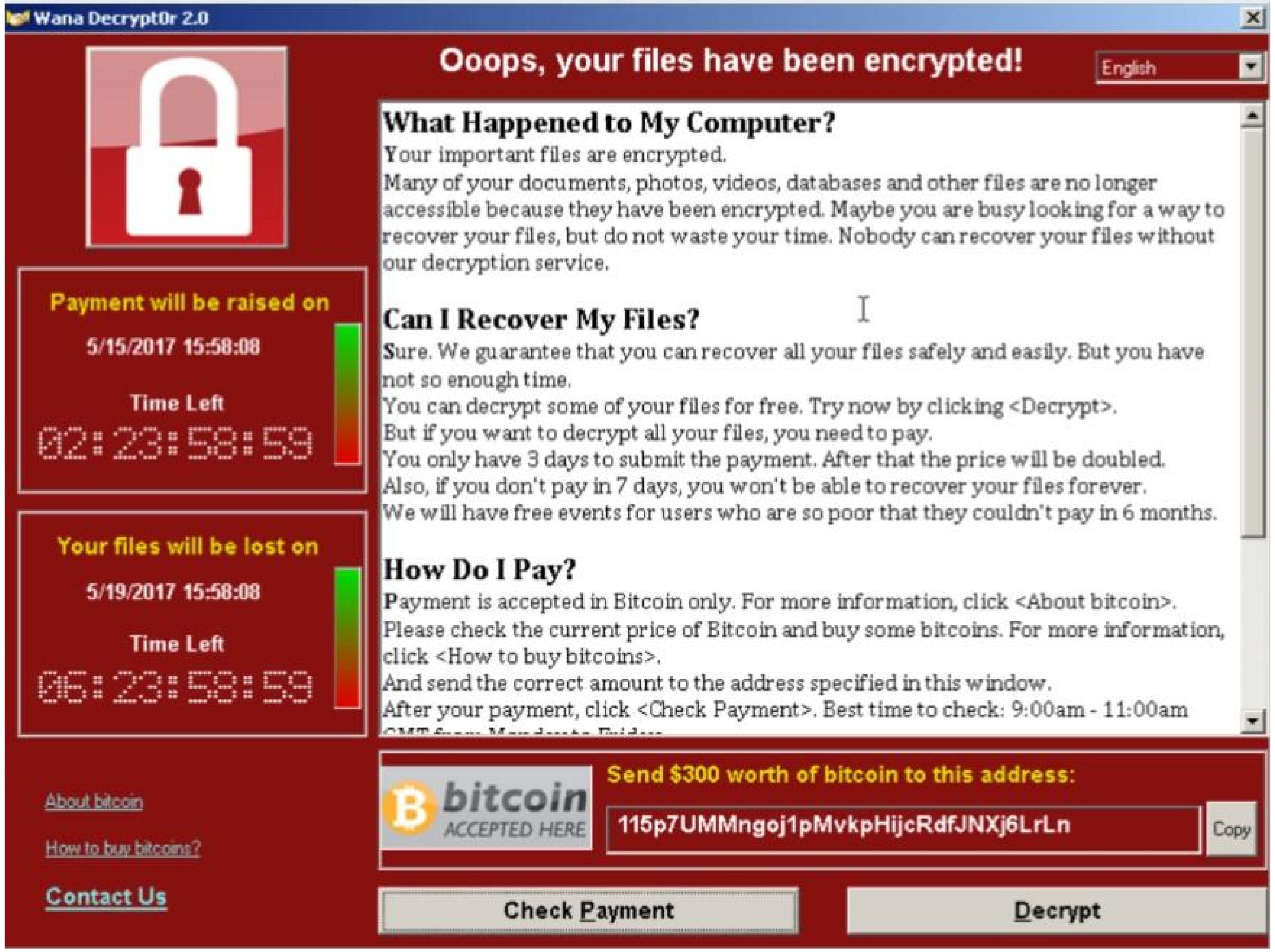


WannaCry Ransomware Encrypted Hospital Medical Devices



Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

Do you WannaCry?



Ooops, your files have been encrypted!

Payment will be raised on

5/15/2017 15:58:08

Time Left

02:23:58:59

Your files will be lost on

5/19/2017 15:58:08

Time Left

06:23:58:59

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Do you WannaCry?

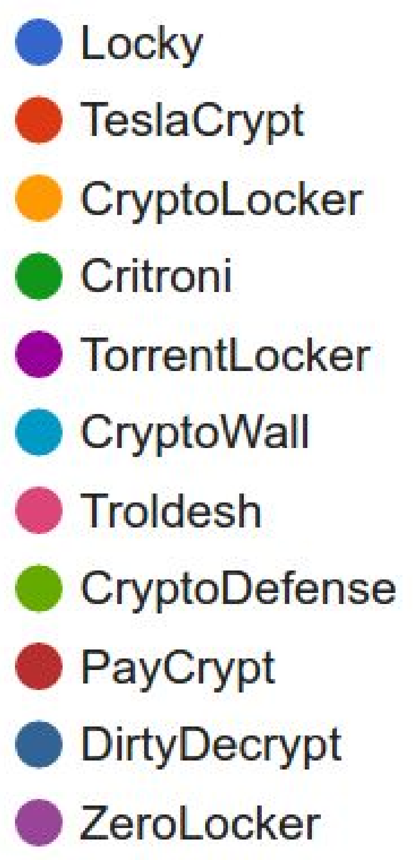
ShieldFS vs WannaCry

ShieldFS **detected** WannaCry

after it encrypted >=200 files

Files lost: **zero**, all were **recovered automatically**

It’s not just WannaCry...



- ● Locky
- ● TeslaCrypt
- ● CryptoLocker
- ● Critroni
- ● TorrentLocker
- ● CryptoWall
- ● Troldesh
- ● CryptoDefense
- ● PayCrypt
- ● DirtyDecrypt
- ● ZeroLocker

➢ Detected: 1436/1483, **96.9%**

➢ Files lost: always **0%**

Why

ShieldFS is different?

ShieldFS: Key Takeaways

The way ransomware interacts with the filesystem is significantly **different** than benign applications

ShieldFS: Key Takeaways

The way ransomware interacts with the filesystem is significantly **different** than benign applications

DETECTION.

Monitor **filesystem activity**

Usage of **crypto** primitives

ShieldFS: Key Takeaways

The way ransomware interacts with the filesystem is significantly **different** than benign applications

DETECTION.

Monitor **filesystem activity**

Usage of **crypto** primitives

PROTECTION. Mere **detection** is **insufficient**

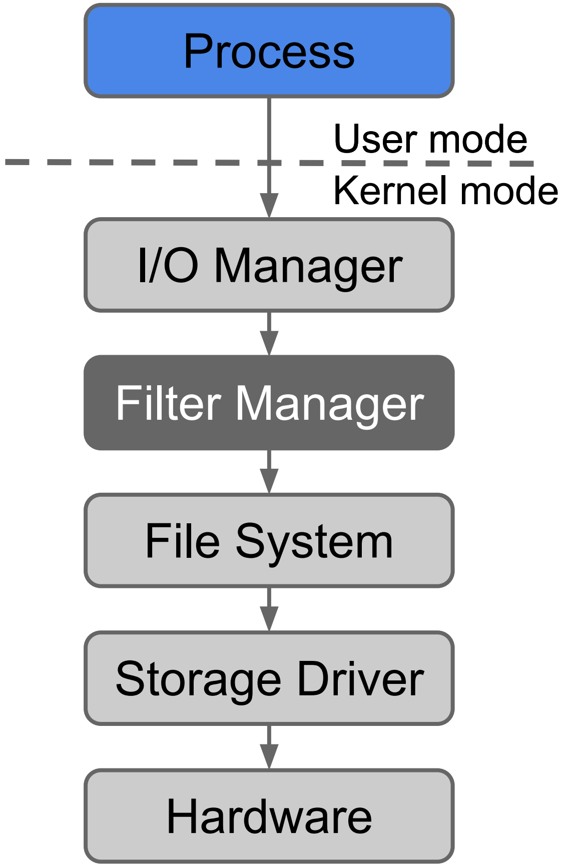
- Stopping a suspicious process may **be too late**
- We need to **protect users' data**, reverting the effects of ransomware attacks.

What

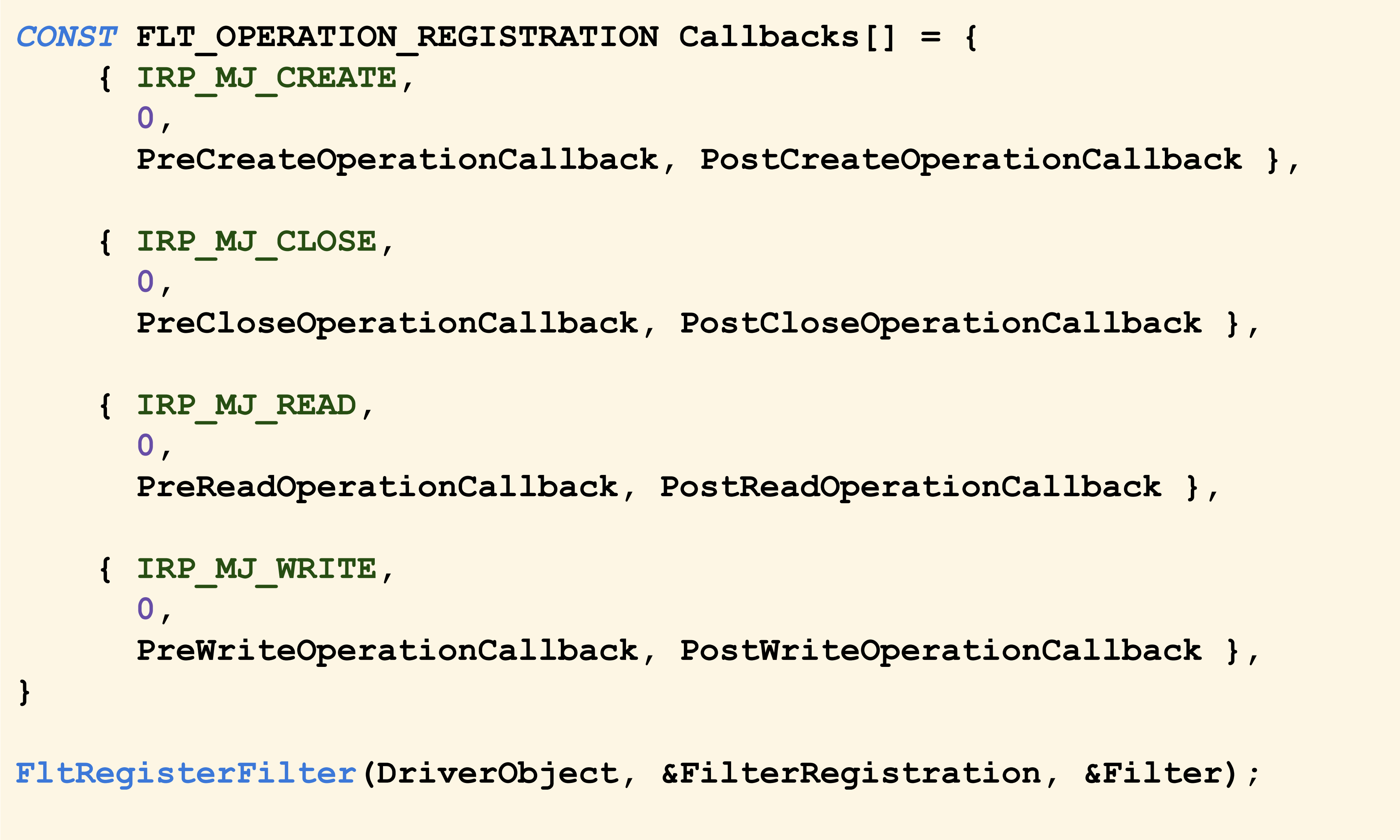
does ShieldFS observe?

FS Activity Monitor

- Windows Kernel module to **monitor** and **log** the file system activity
  - Windows Minifilter Driver
  - Log IRPs (I/O Request Packets)

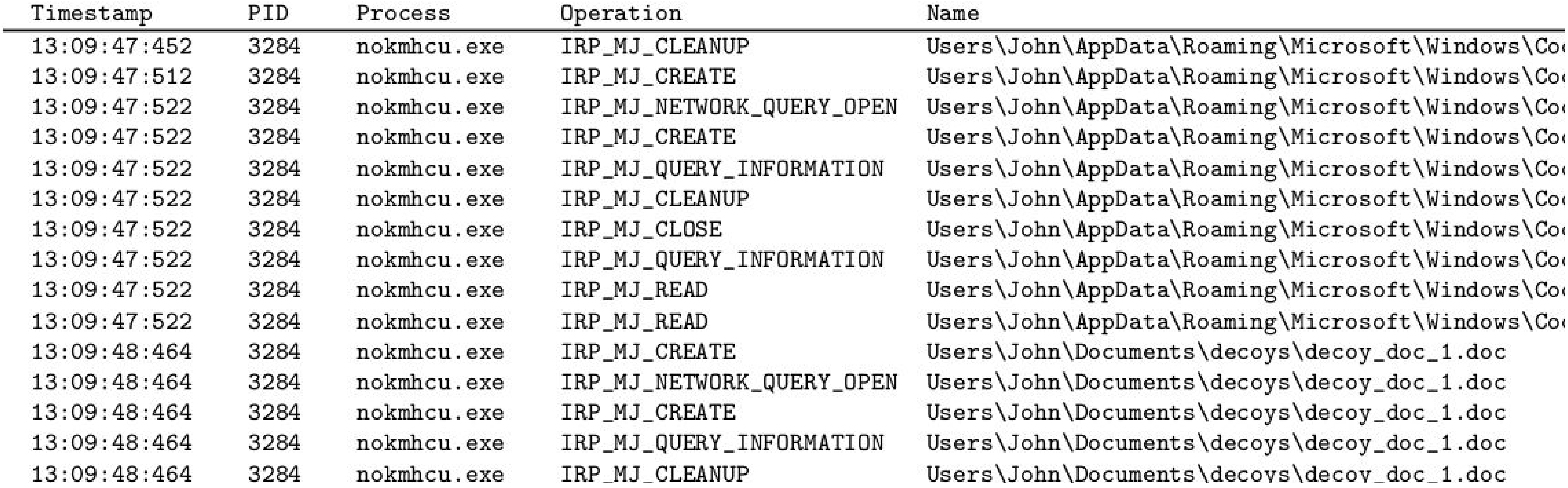


Filter Manager API



```
CONST FLT_OPERATION_REGISTRATION Callbacks[] = {
    { IRP_MJ_CREATE,
      0,
      PreCreateOperationCallback, PostCreateOperationCallback },

    { IRP_MJ_CLOSE,
      0,
      PreCloseOperationCallback, PostCloseOperationCallback },

    { IRP_MJ_READ,
      0,
      PreReadOperationCallback, PostReadOperationCallback },

    { IRP_MJ_WRITE,
      0,
      PreWriteOperationCallback, PostWriteOperationCallback },
}

FltRegisterFilter(DriverObject, &FilterRegistration, &Filter);
```

IRP Log Example



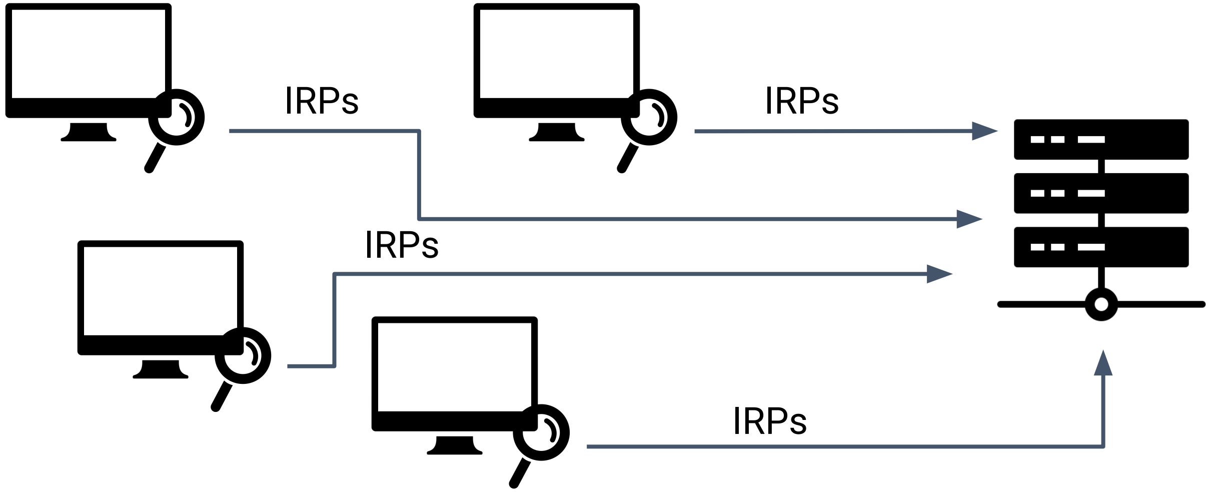
```
Timestamp     PID    Process       Operation                 Name
13:09:47:452  3284   nokmhcu.exe   IRP_MJ_CLEANUP            Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:512  3284   nokmhcu.exe   IRP_MJ_CREATE             Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522  3284   nokmhcu.exe   IRP_MJ_NETWORK_QUERY_OPEN Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522  3284   nokmhcu.exe   IRP_MJ_CREATE             Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522  3284   nokmhcu.exe   IRP_MJ_QUERY_INFORMATION  Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522  3284   nokmhcu.exe   IRP_MJ_CLEANUP            Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522  3284   nokmhcu.exe   IRP_MJ_CLOSE              Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522  3284   nokmhcu.exe   IRP_MJ_QUERY_INFORMATION  Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522  3284   nokmhcu.exe   IRP_MJ_READ               Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522  3284   nokmhcu.exe   IRP_MJ_READ               Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:48:464  3284   nokmhcu.exe   IRP_MJ_CREATE             Users\John\Documents\decoys\decoy_doc_1.doc
13:09:48:464  3284   nokmhcu.exe   IRP_MJ_NETWORK_QUERY_OPEN Users\John\Documents\decoys\decoy_doc_1.doc
13:09:48:464  3284   nokmhcu.exe   IRP_MJ_CREATE             Users\John\Documents\decoys\decoy_doc_1.doc
13:09:48:464  3284   nokmhcu.exe   IRP_MJ_QUERY_INFORMATION  Users\John\Documents\decoys\decoy_doc_1.doc
13:09:48:464  3284   nokmhcu.exe   IRP_MJ_CLEANUP            Users\John\Documents\decoys\decoy_doc_1.doc
```

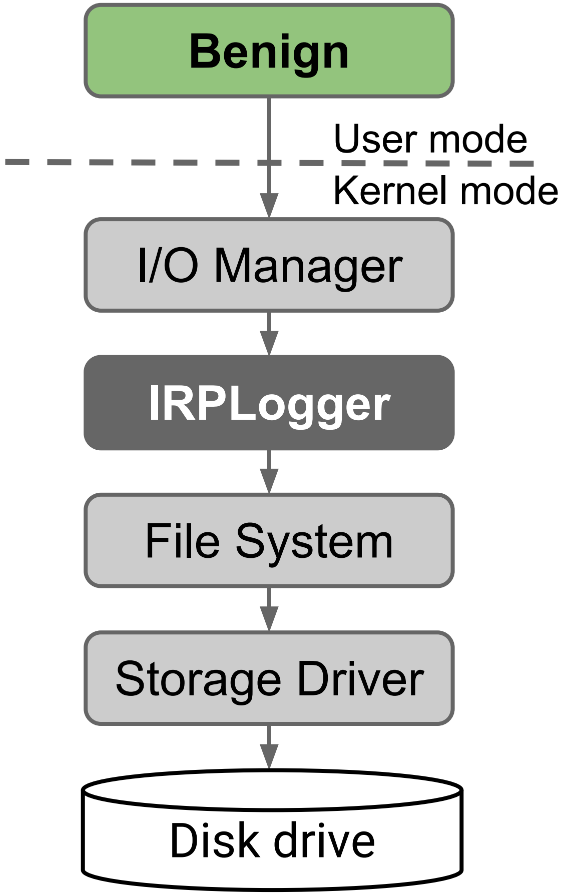
Where

do we start from?

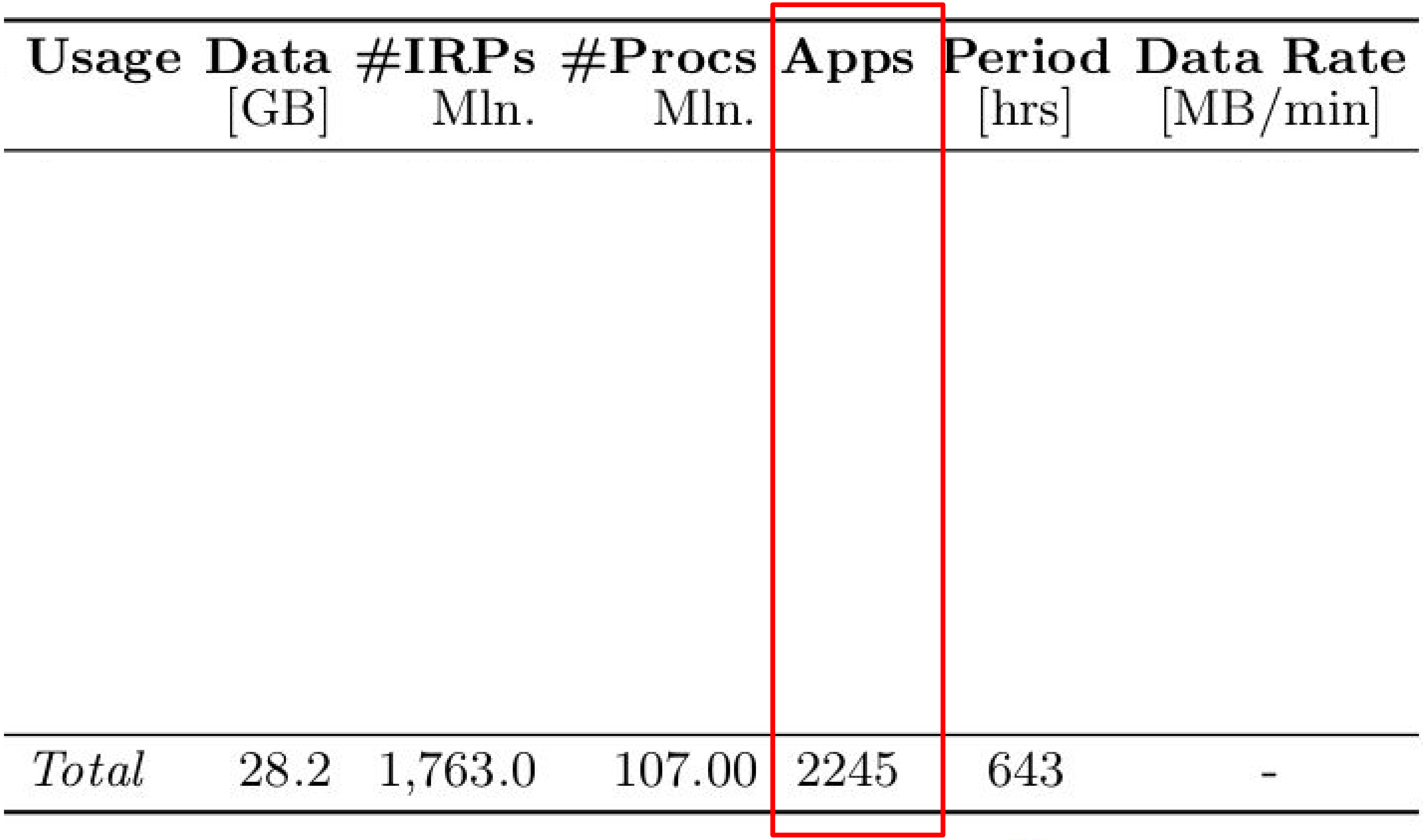
Background/Clean FS Activity

- IRP logger on 11 **clean** machines
- FS activity under "typical" usage
  - ~1 month worth of data



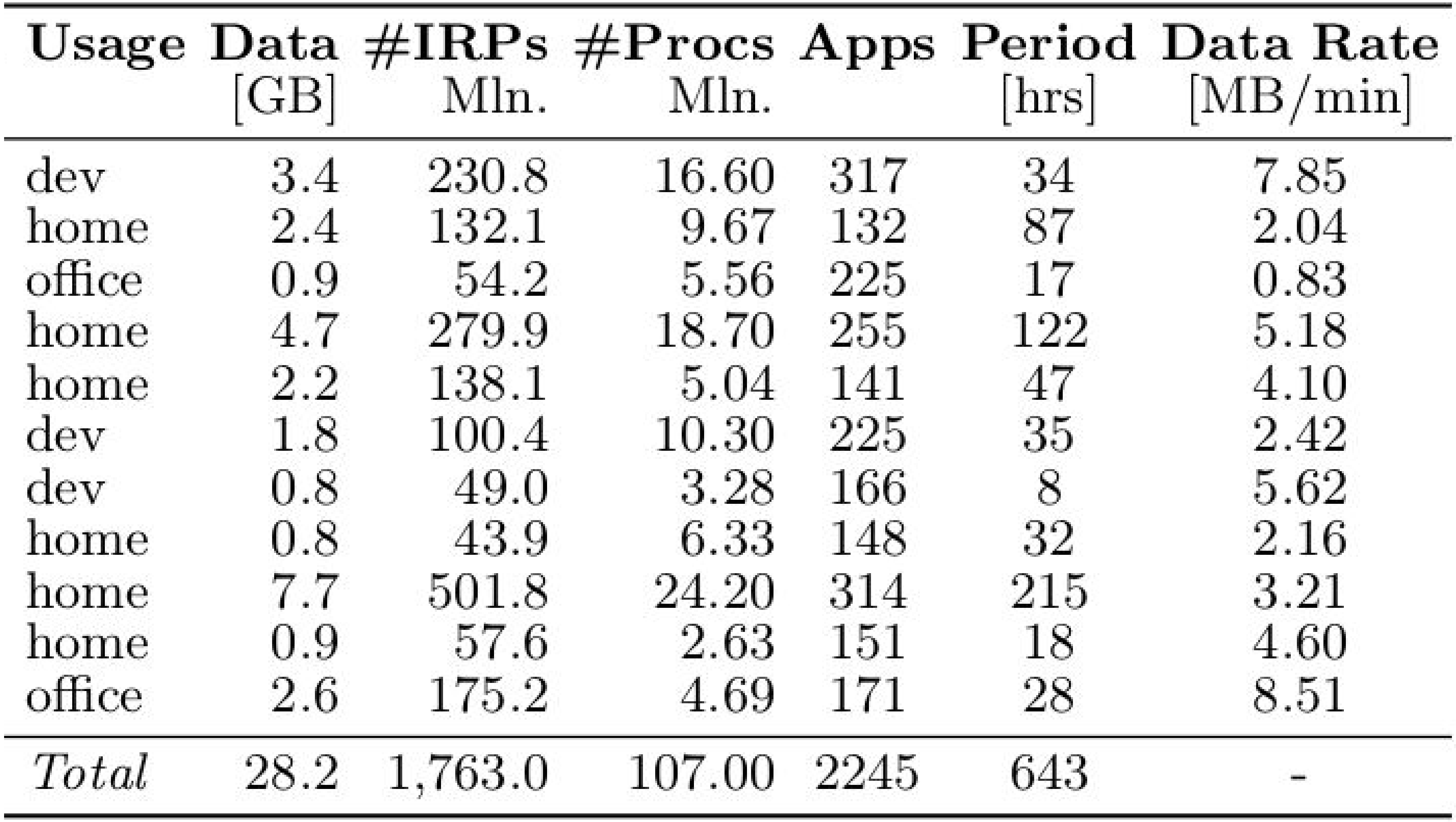


Collected FS Activity



Usage	Data	#IRPs	#Procs	Apps	Period	Data Rate
	[GB]	Mln.	Mln.		[hrs]	[MB/min]
Total	28.2	1,763.0	107.00	2245	643	-

Collected FS Activity

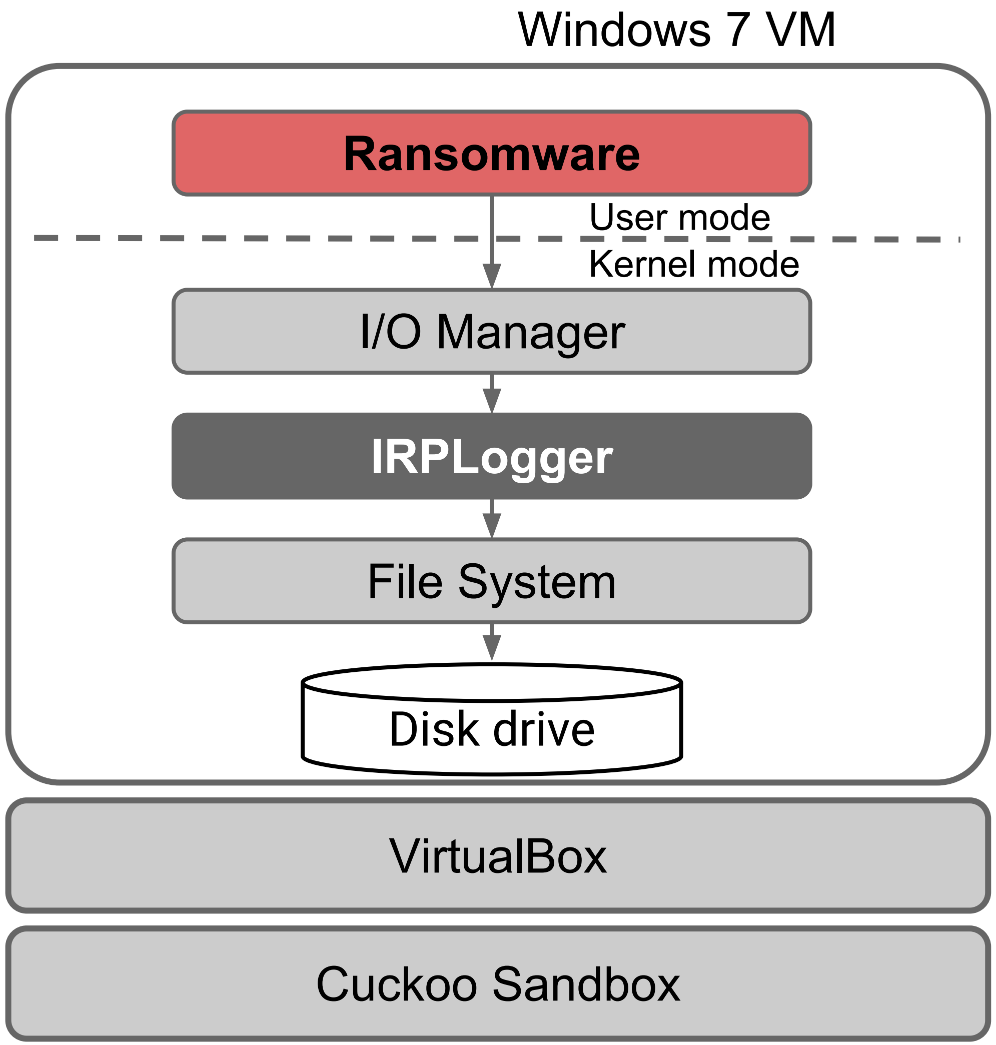


Usage	Data [GB]	#IRPs Mln.	#Procs Mln.	Apps	Period [hrs]	Data Rate [MB/min]
dev	3.4	230.8	16.60	317	34	7.85
home	2.4	132.1	9.67	132	87	2.04
office	0.9	54.2	5.56	225	17	0.83
home	4.7	279.9	18.70	255	122	5.18
home	2.2	138.1	5.04	141	47	4.10
dev	1.8	100.4	10.30	225	35	2.42
dev	0.8	49.0	3.28	166	8	5.62
home	0.8	43.9	6.33	148	32	2.16
home	7.7	501.8	24.20	314	215	3.21
home	0.9	57.6	2.63	151	18	4.60
office	2.6	175.2	4.69	171	28	8.51
Total	28.2	1,763.0	107.00	2245	643	-

Analysis Environment

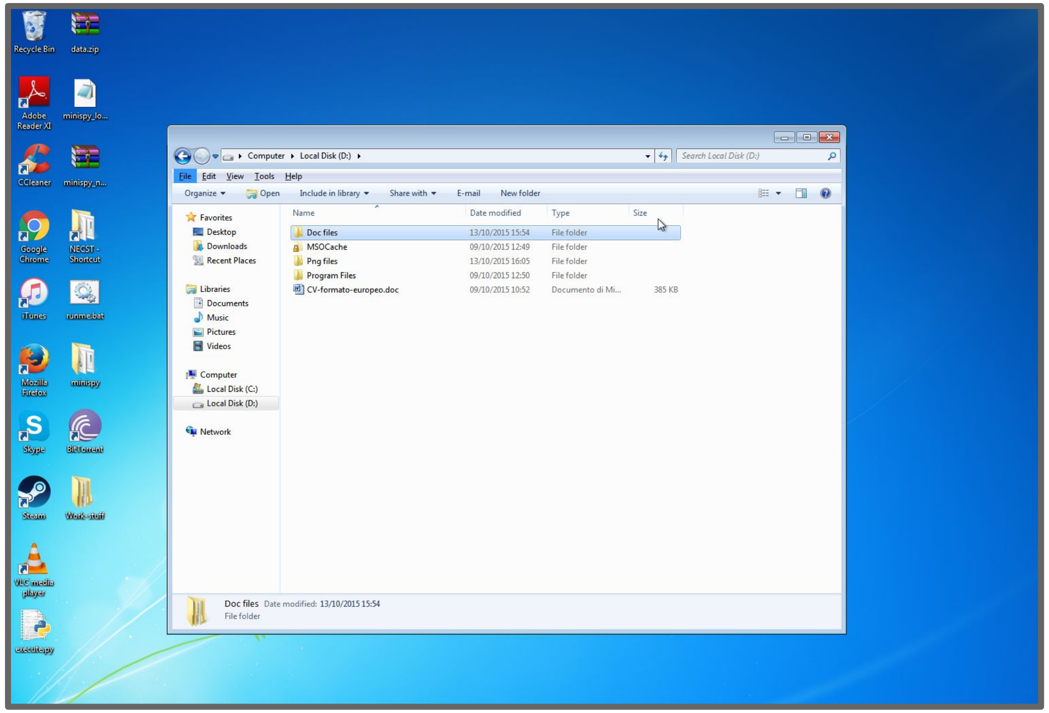
383 samples of 5 distinct families

- ● CryptoWall
- ● Crowti
- ● CryptoDefense
- ● Critroni
- ● TeslaCrypt



Environment Preparation

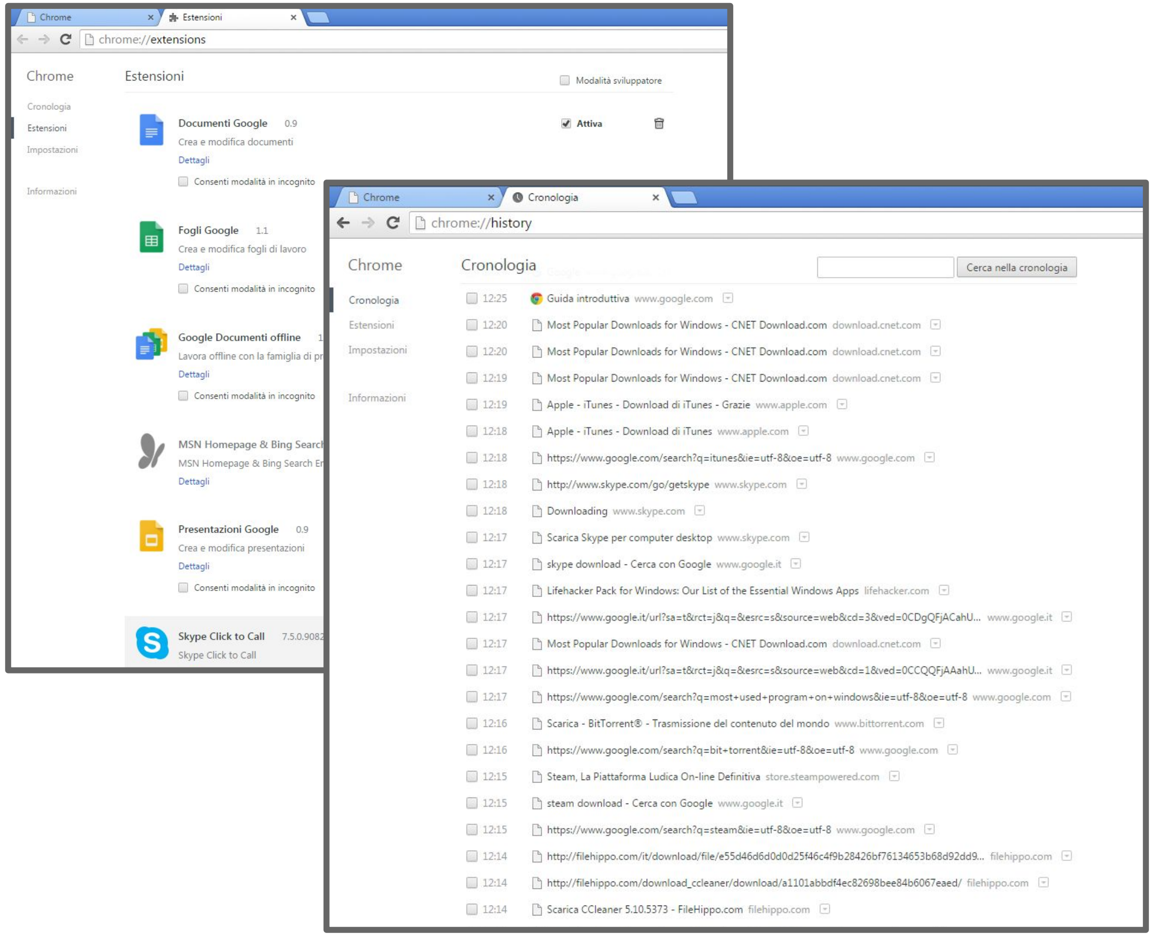
- Trigger ransomware activity
- Avoid anti-sandbox tricks



Computer ▸ Local Disk (D:) ▸

Name	Date modified	Type	Size
Doc files	13/10/2015 15:54	File folder	
MSOCache	09/10/2015 12:49	File folder	
Png files	13/10/2015 16:05	File folder	
Program Files	09/10/2015 12:50	File folder	
CV-formato-europeo.doc	09/10/2015 10:52	Documento di Mi...	385 KB

Doc files Date modified: 13/10/2015 15:54
File folder



chrome://extensions

Estensioni

□ Modalità sviluppatore

Documenti Google 0.9
Crea e modifica documenti
Dettagli
□ Consenti modalità in incognito
☑ Attiva

Fogli Google 1.1
Crea e modifica fogli di lavoro
Dettagli
□ Consenti modalità in incognito

Google Documenti offline 1
Lavora offline con la famiglia di pr
Dettagli
□ Consenti modalità in incognito

MSN Homepage & Bing Search
MSN Homepage & Bing Search En
Dettagli

Presentazioni Google 0.9
Crea e modifica presentazioni
Dettagli
□ Consenti modalità in incognito

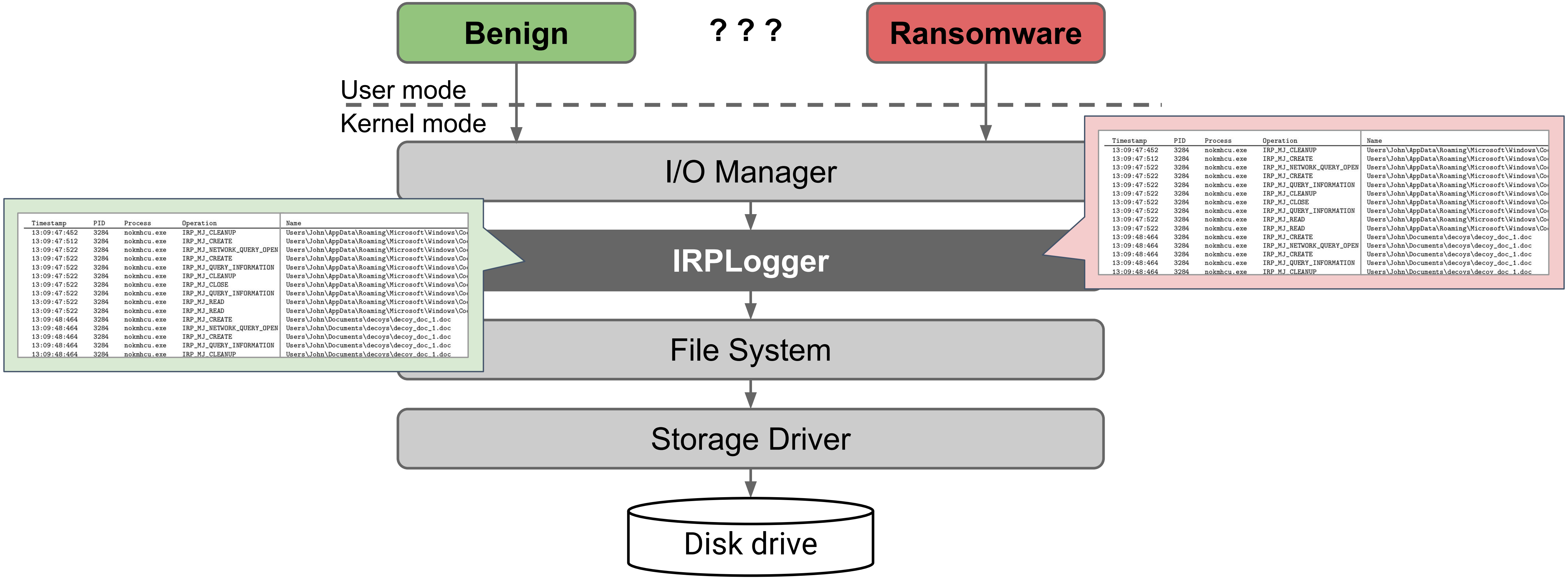
Skype Click to Call 7.5.0.9082
Skype Click to Call

chrome://history

Cronologia

12:25	Guida introduttiva	www.google.com
12:20	Most Popular Downloads for Windows - CNET Download.com	download.cnet.com
12:20	Most Popular Downloads for Windows - CNET Download.com	download.cnet.com
12:19	Most Popular Downloads for Windows - CNET Download.com	download.cnet.com
12:19	Apple - iTunes - Download di iTunes - Grazie	www.apple.com
12:18	Apple - iTunes - Download di iTunes	www.apple.com
12:18	https://www.google.com/search?q=itunes&ie=utf-8&oe=utf-8	www.google.com
12:18	http://www.skype.com/go/getskype	www.skype.com
12:18	Downloading	www.skype.com
12:17	Scarica Skype per computer desktop	www.skype.com
12:17	skype download - Cerca con Google	www.google.it
12:17	Lifehacker Pack for Windows: Our List of the Essential Windows Apps	lifehacker.com
12:17	https://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0CDgQFjACahU...	www.google.it
12:17	Most Popular Downloads for Windows - CNET Download.com	download.cnet.com
12:17	https://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCQQFjAAahU...	www.google.it
12:17	https://www.google.com/search?q=most+used+program+on+windows&ie=utf-8&oe=utf-8	www.google.com
12:16	Scarica - BitTorrent® - Trasmissione del contenuto del mondo	www.bittorrent.com
12:16	https://www.google.com/search?q=bit+torrent&ie=utf-8&oe=utf-8	www.google.com
12:15	Steam, La Piattaforma Ludica On-line Definitiva	store.steampowered.com
12:15	steam download - Cerca con Google	www.google.it
12:15	https://www.google.com/search?q=steam&ie=utf-8&oe=utf-8	www.google.com
12:14	http://filehippo.com/it/download/file/e55d46d6d0d0d25f46c4f9b28426bf76134653b68d92dd9...	filehippo.com
12:14	http://filehippo.com/download_ccleaner/download/a1101abbdf4ec82698bee84b6067eaed/	filehippo.com
12:14	Scarica CCleaner 5.10.5373 - FileHippo.com	filehippo.com

Ransomware vs Benign apps



```
Timestamp      PID    Process       Operation                    Name
13:09:47:452   3284   nokmhcu.exe   IRP_MJ_CLEANUP               Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:512   3284   nokmhcu.exe   IRP_MJ_CREATE                Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522   3284   nokmhcu.exe   IRP_MJ_NETWORK_QUERY_OPEN    Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522   3284   nokmhcu.exe   IRP_MJ_CREATE                Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522   3284   nokmhcu.exe   IRP_MJ_QUERY_INFORMATION     Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522   3284   nokmhcu.exe   IRP_MJ_CLEANUP               Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522   3284   nokmhcu.exe   IRP_MJ_CLOSE                 Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522   3284   nokmhcu.exe   IRP_MJ_QUERY_INFORMATION     Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522   3284   nokmhcu.exe   IRP_MJ_READ                  Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522   3284   nokmhcu.exe   IRP_MJ_READ                  Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:48:464   3284   nokmhcu.exe   IRP_MJ_CREATE                Users\John\Documents\decoys\decoy_doc_1.doc
13:09:48:464   3284   nokmhcu.exe   IRP_MJ_NETWORK_QUERY_OPEN    Users\John\Documents\decoys\decoy_doc_1.doc
13:09:48:464   3284   nokmhcu.exe   IRP_MJ_CREATE                Users\John\Documents\decoys\decoy_doc_1.doc
13:09:48:464   3284   nokmhcu.exe   IRP_MJ_QUERY_INFORMATION     Users\John\Documents\decoys\decoy_doc_1.doc
13:09:48:464   3284   nokmhcu.exe   IRP_MJ_CLEANUP               Users\John\Documents\decoys\decoy_doc_1.doc
```

```
Timestamp      PID    Process       Operation                    Name
13:09:47:452   3284   nokmhcu.exe   IRP_MJ_CLEANUP               Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:512   3284   nokmhcu.exe   IRP_MJ_CREATE                Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522   3284   nokmhcu.exe   IRP_MJ_NETWORK_QUERY_OPEN    Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522   3284   nokmhcu.exe   IRP_MJ_CREATE                Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522   3284   nokmhcu.exe   IRP_MJ_QUERY_INFORMATION     Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522   3284   nokmhcu.exe   IRP_MJ_CLEANUP               Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522   3284   nokmhcu.exe   IRP_MJ_CLOSE                 Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522   3284   nokmhcu.exe   IRP_MJ_QUERY_INFORMATION     Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522   3284   nokmhcu.exe   IRP_MJ_READ                  Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:47:522   3284   nokmhcu.exe   IRP_MJ_READ                  Users\John\AppData\Roaming\Microsoft\Windows\Co
13:09:48:464   3284   nokmhcu.exe   IRP_MJ_CREATE                Users\John\Documents\decoys\decoy_doc_1.doc
13:09:48:464   3284   nokmhcu.exe   IRP_MJ_NETWORK_QUERY_OPEN    Users\John\Documents\decoys\decoy_doc_1.doc
13:09:48:464   3284   nokmhcu.exe   IRP_MJ_CREATE                Users\John\Documents\decoys\decoy_doc_1.doc
13:09:48:464   3284   nokmhcu.exe   IRP_MJ_QUERY_INFORMATION     Users\John\Documents\decoys\decoy_doc_1.doc
13:09:48:464   3284   nokmhcu.exe   IRP_MJ_CLEANUP               Users\John\Documents\decoys\decoy_doc_1.doc
```

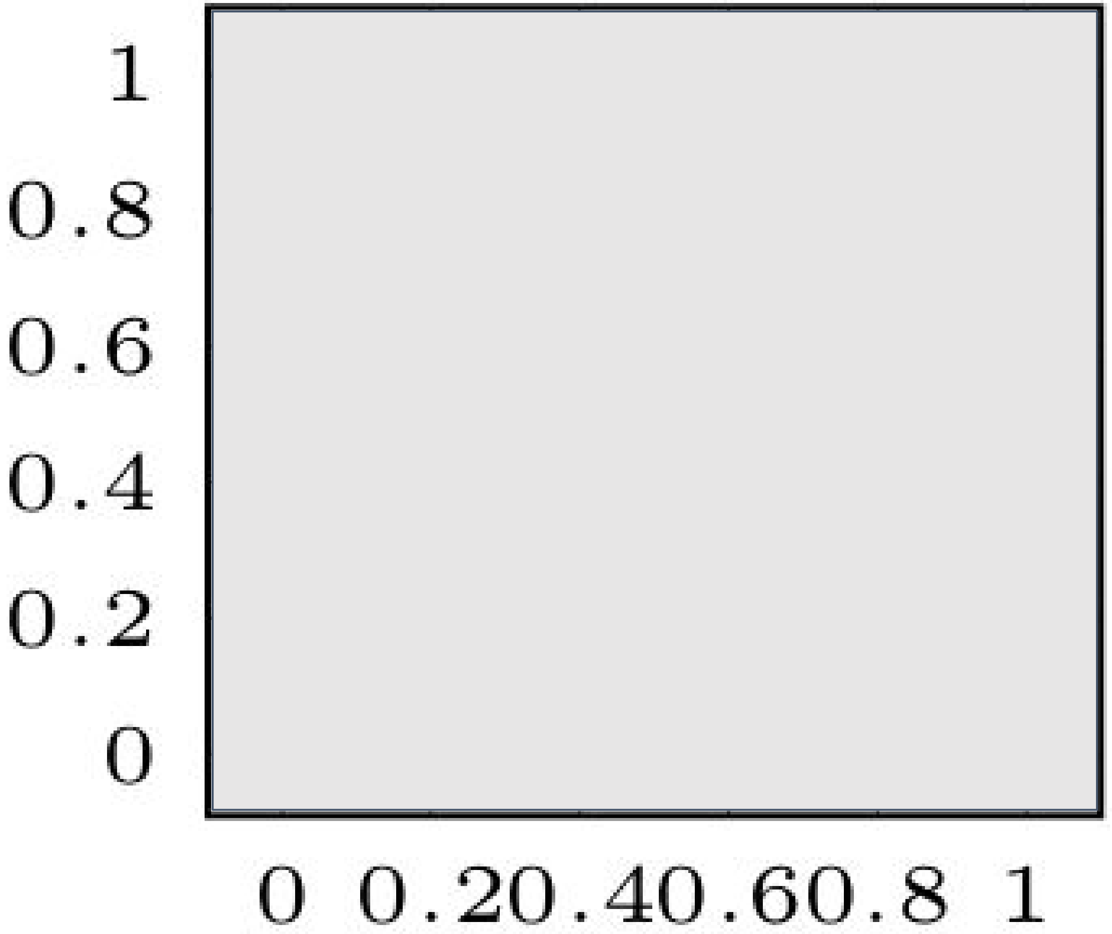
ShieldFS

Self-healing

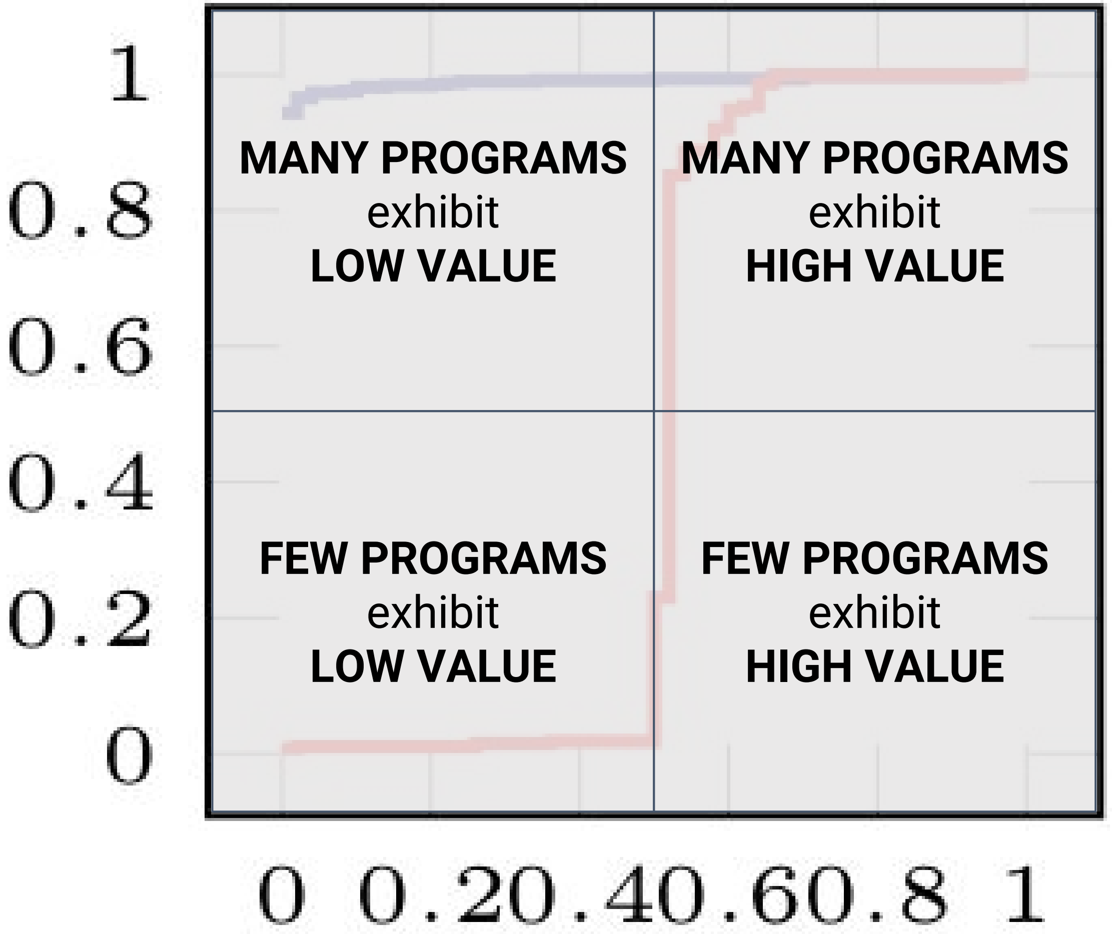
→ Ransomware-aware

Filesystem

Ransomware vs Benign apps



Ransomware vs Benign apps



MANY PROGRAMS
exhibit
LOW VALUE

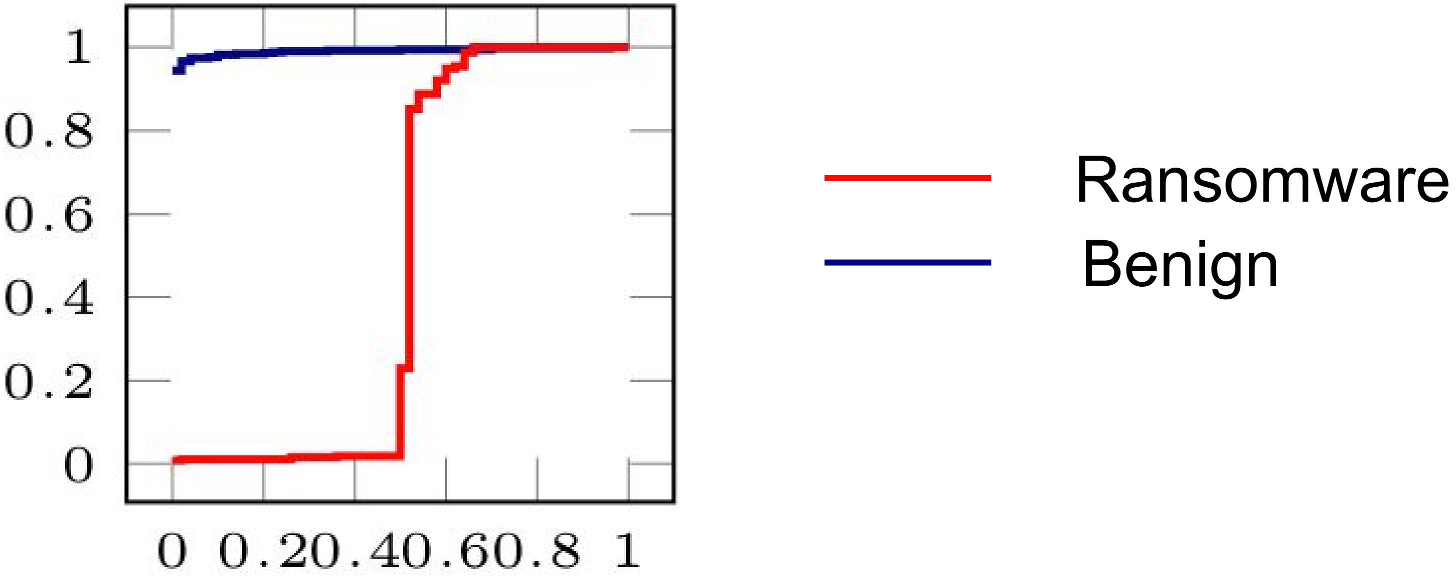
MANY PROGRAMS
exhibit
HIGH VALUE

FEW PROGRAMS
exhibit
LOW VALUE

FEW PROGRAMS
exhibit
HIGH VALUE

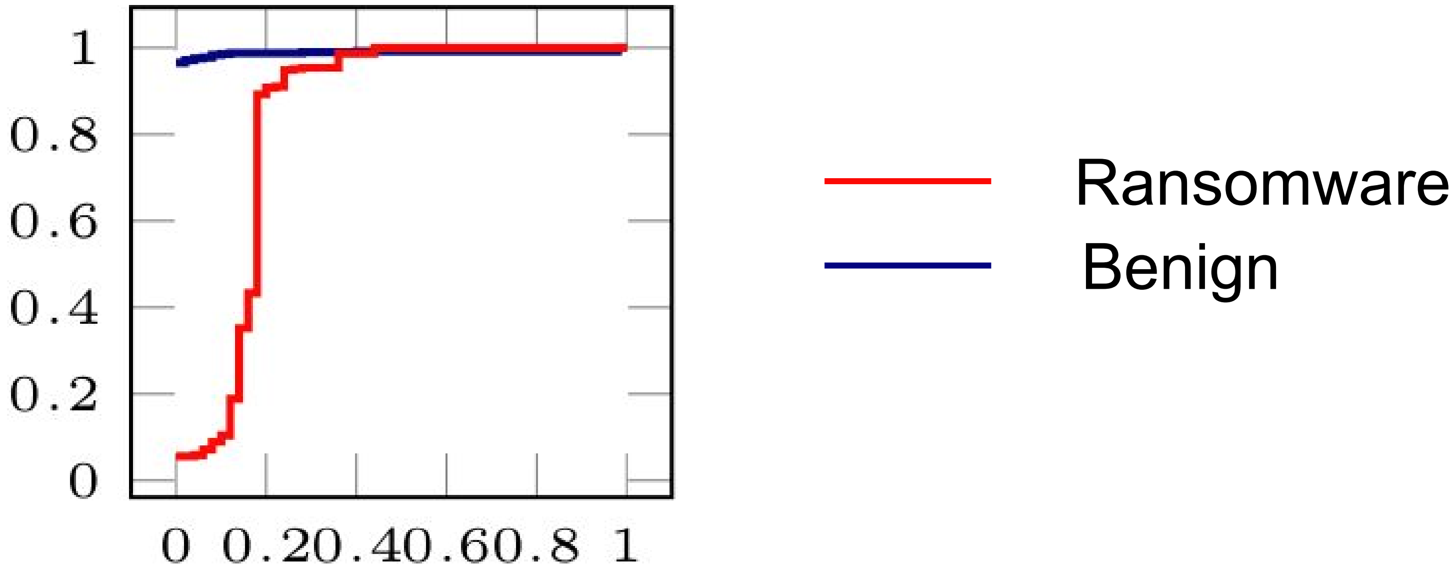
Ransomware vs Benign apps

(1) #Folder-listing



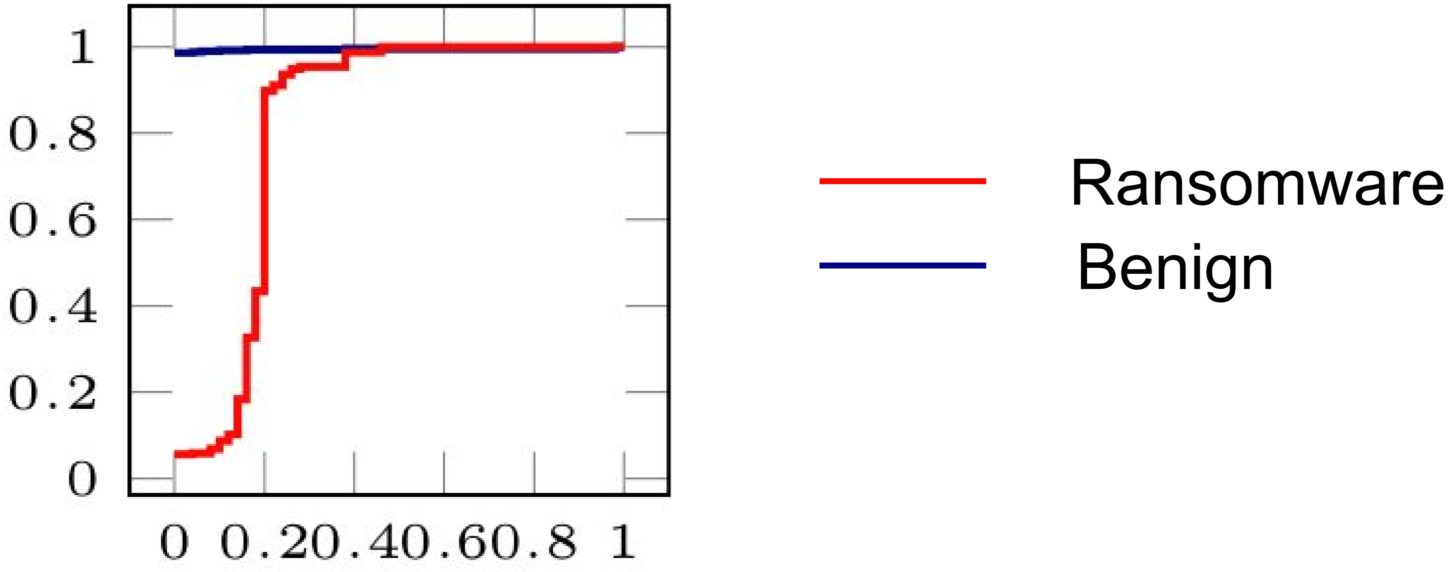
Ransomware vs Benign apps

(2) #Files-Read

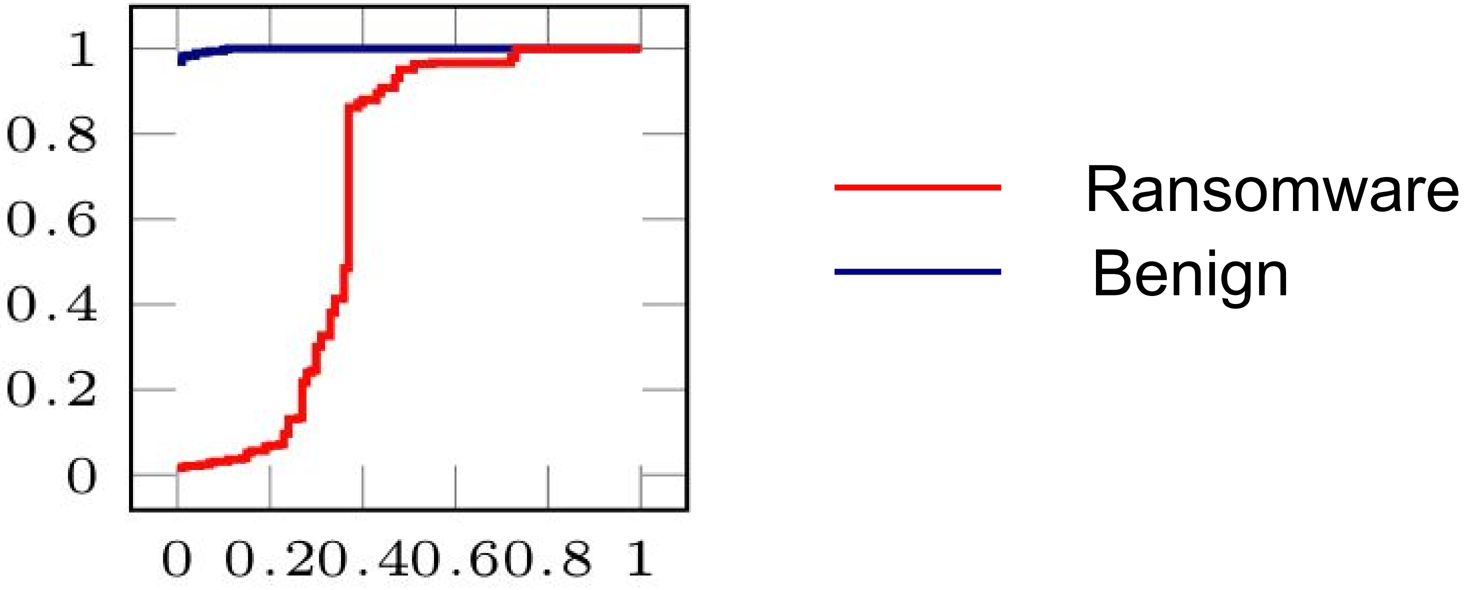


Ransomware vs Benign apps

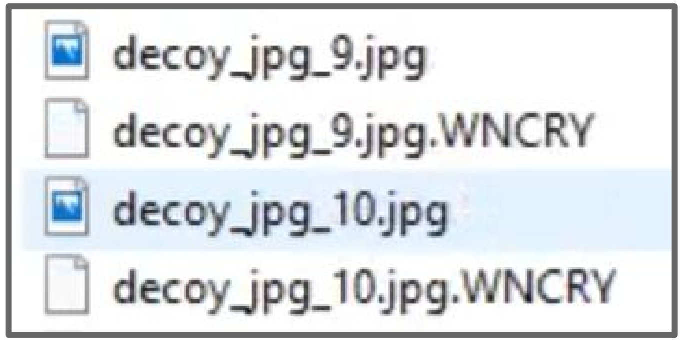
(3) #Files-Written



Ransomware vs Benign apps



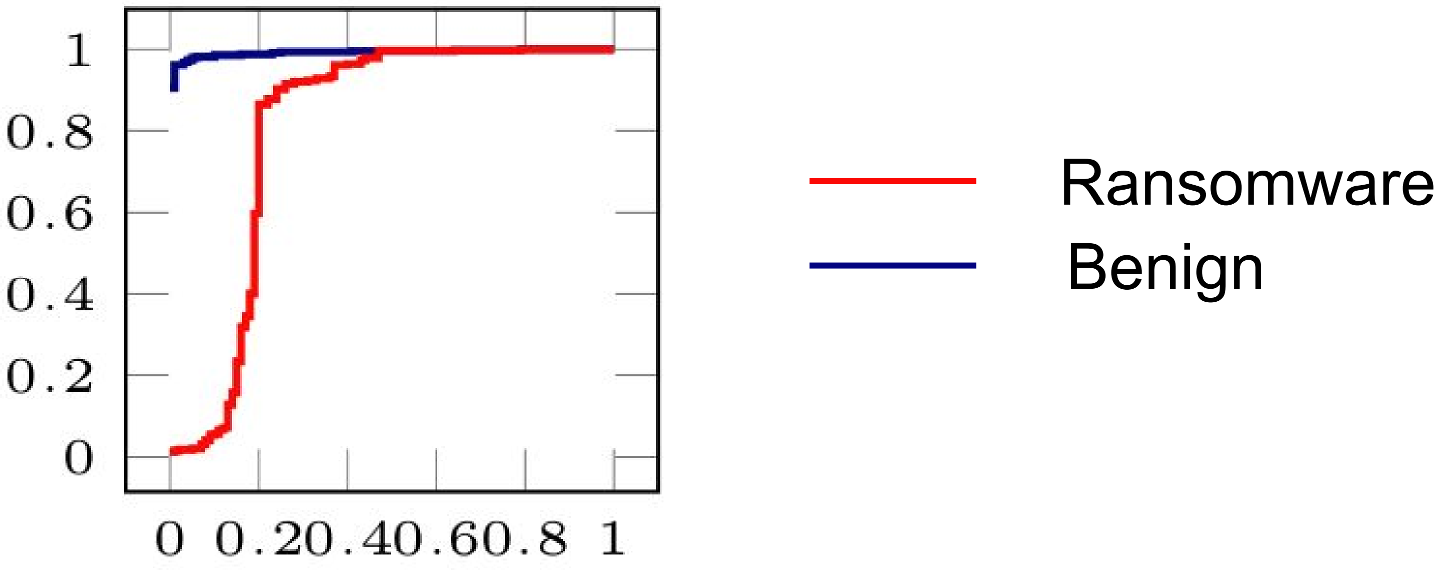
(4) #Files-Renamed



decoy_jpg_9.jpg
decoy_jpg_9.jpg.WNCRY
decoy_jpg_10.jpg
decoy_jpg_10.jpg.WNCRY

Ransomware vs Benign apps

PDF JPG DOC

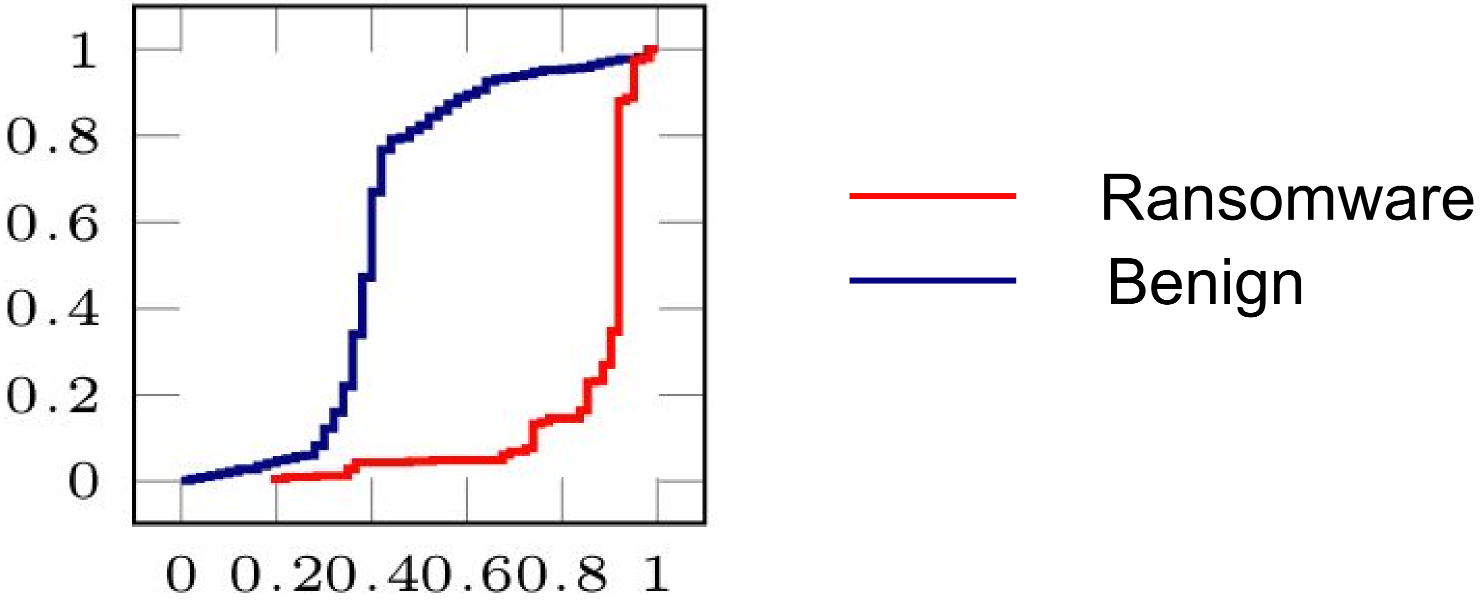


(5) File type coverage

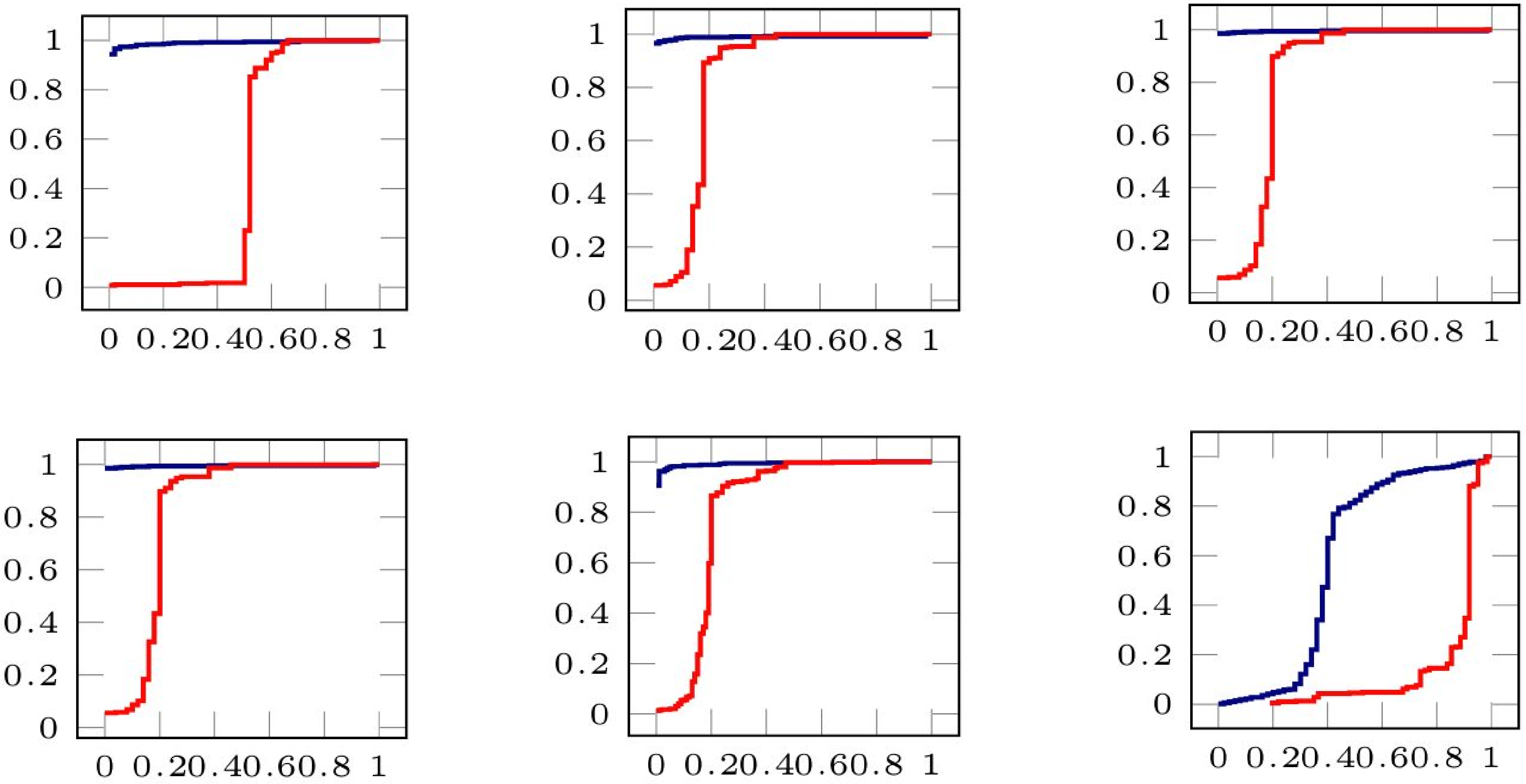
Ransomware vs Benign apps

101001
010101
001101

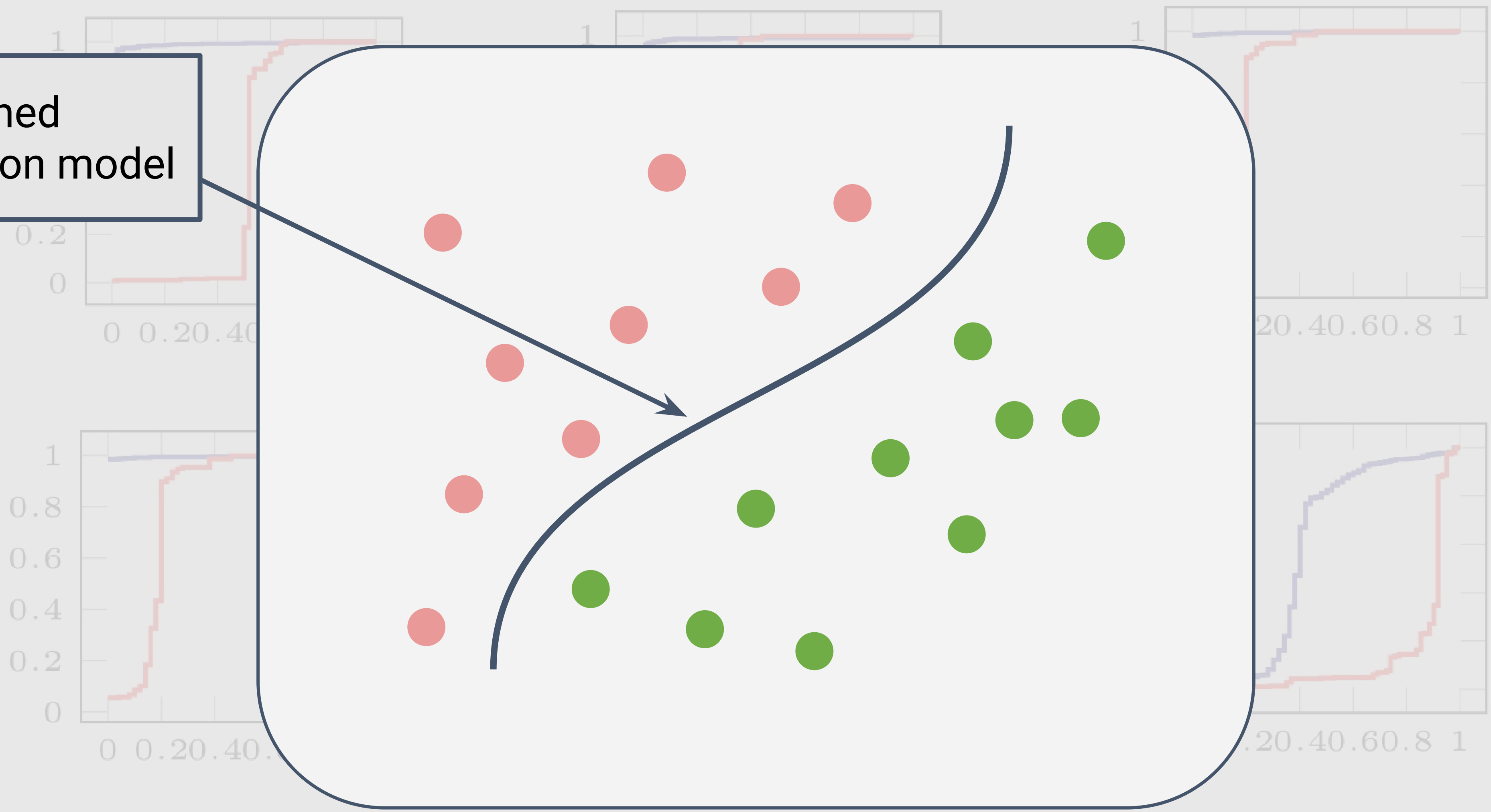
(6) Write-Entropy



Ransomware vs Benign apps



Machine Learning



Learned classification model

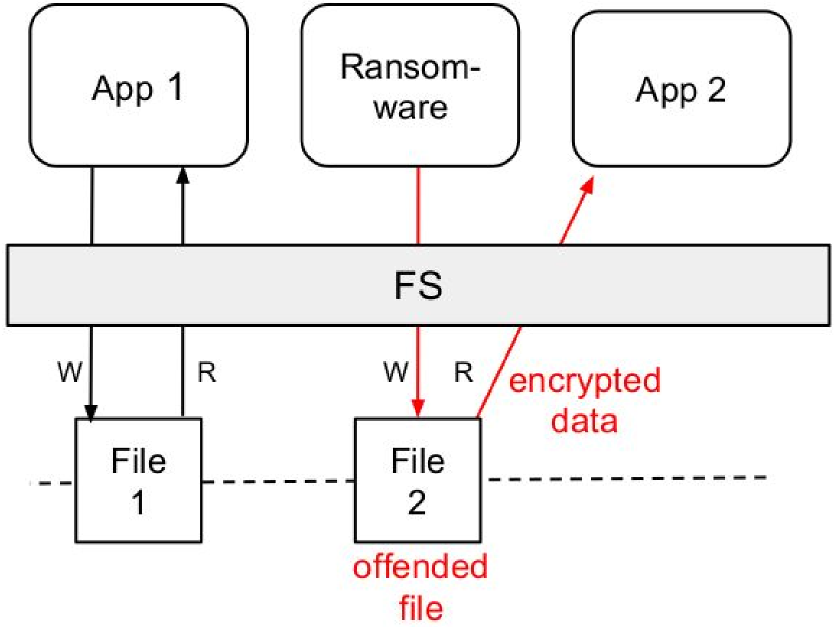
ShieldFS

→ <u>Self-healing</u>

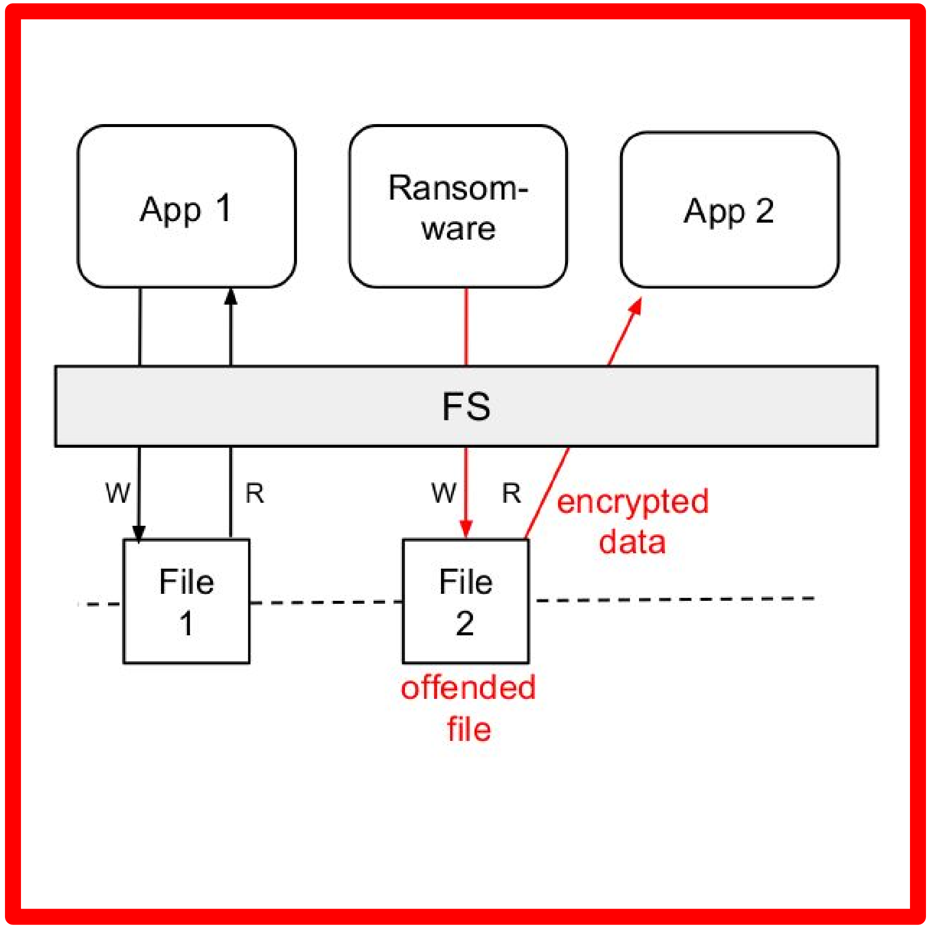
Ransomware-aware

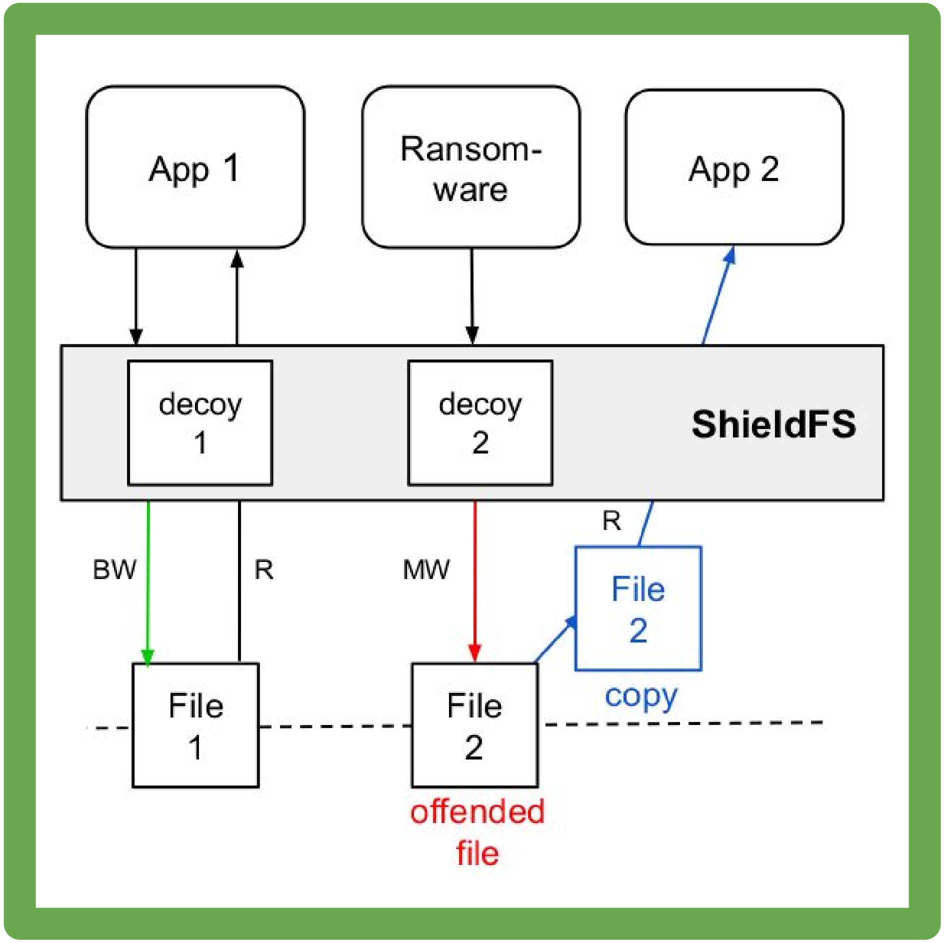
Filesystem

ShieldFS: Healing Approach



ShieldFS: Healing Approach

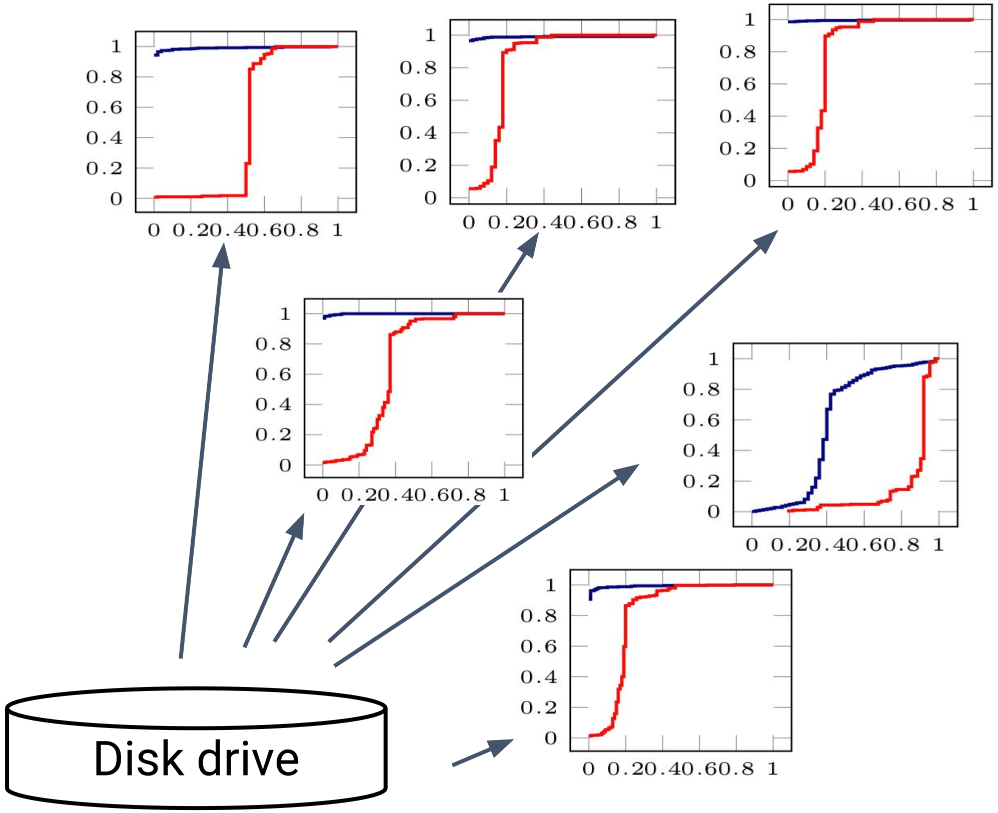


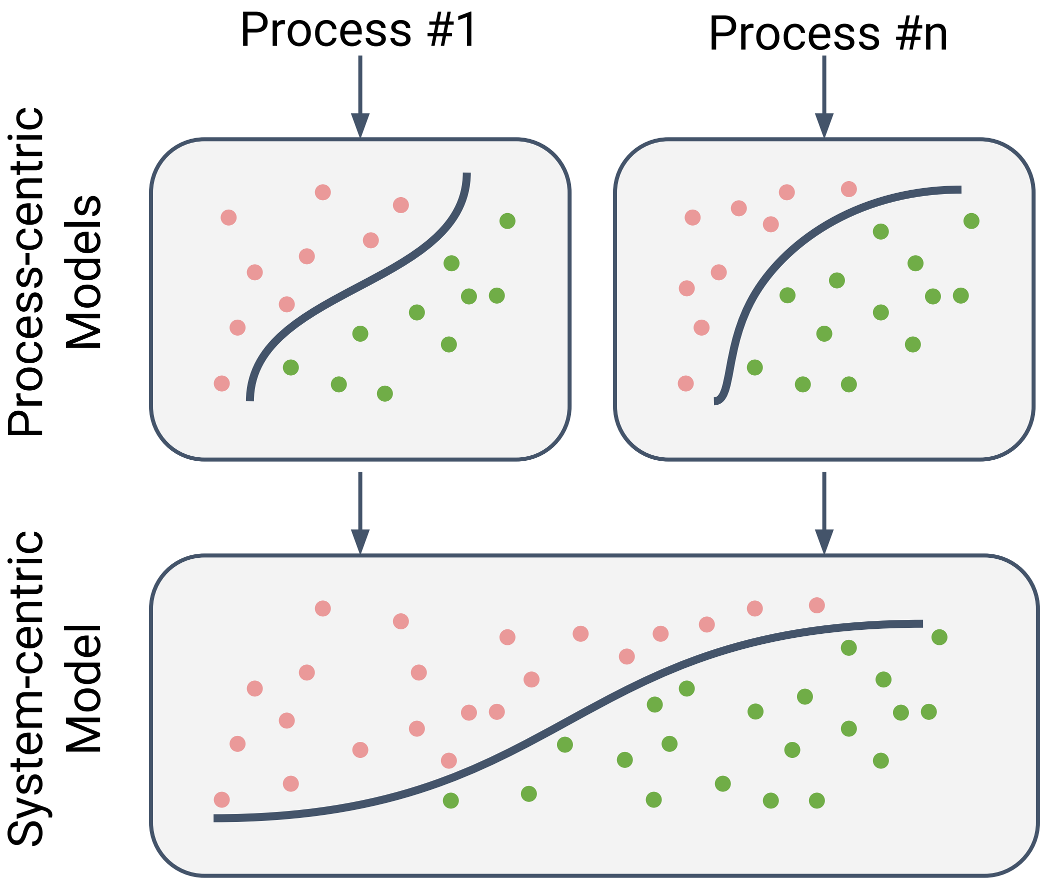


THIS SLIDE IS TO PROVE THAT WE CAN CREATE COMPLEX ANIMATION FLOWS

THIS SLIDE IS TO PROVE THAT WE CAN CREATE COMPLEX ANIMATION FLOWS

Detection Models


Disk drive

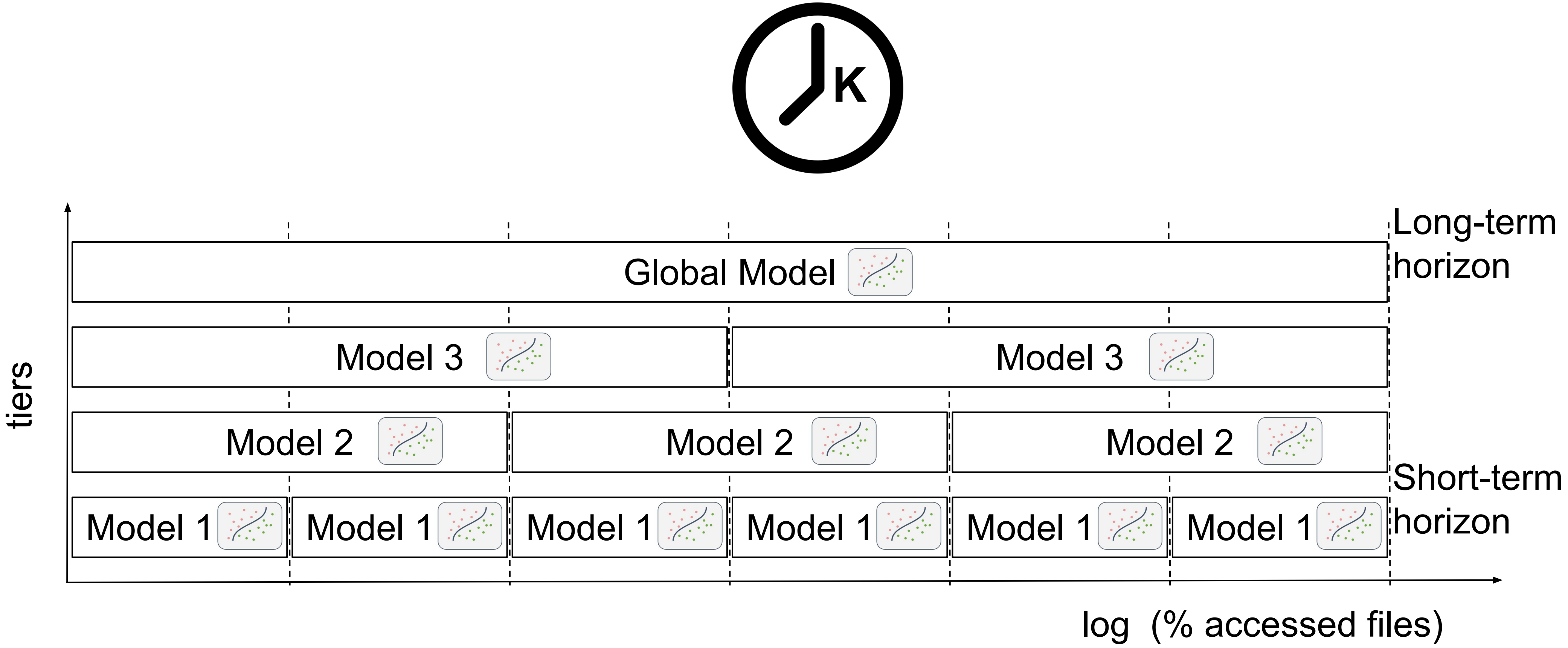

Process #1

Process #n

Process-centric Models

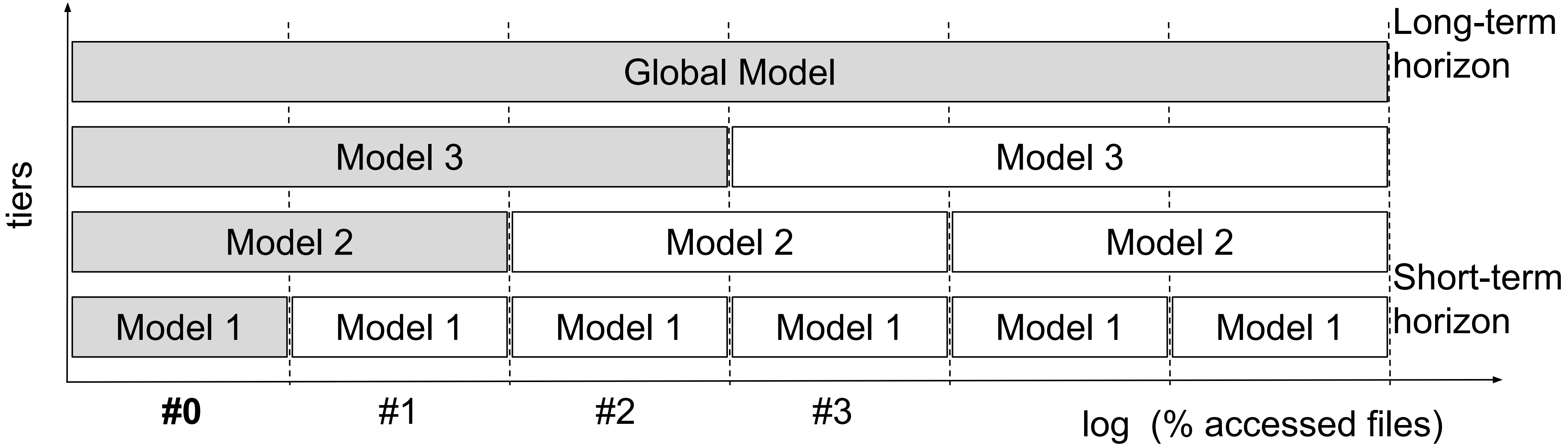
System-centric Model

Multi-tier Incremental Models



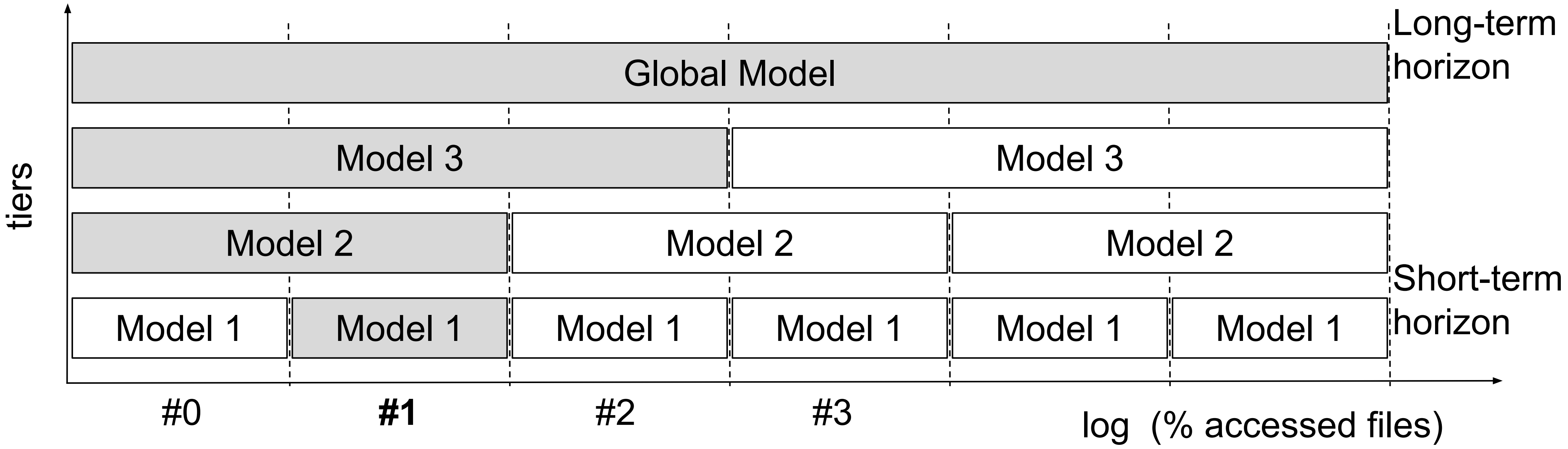
Multi-tier Incremental Models

tick #0



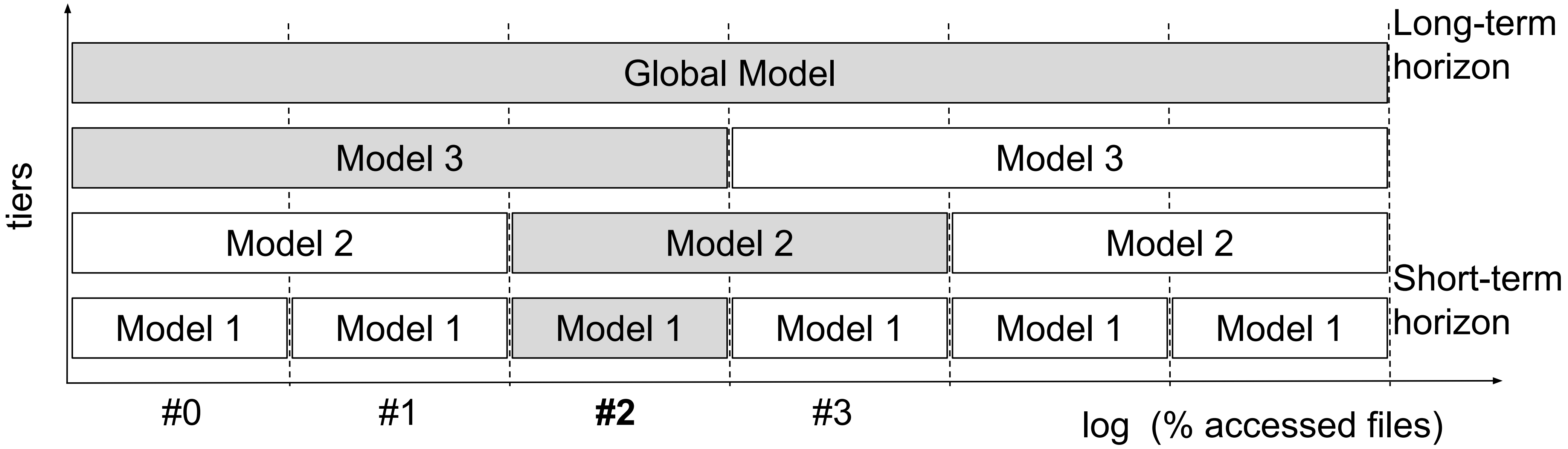
Multi-tier Incremental Models

tick #1



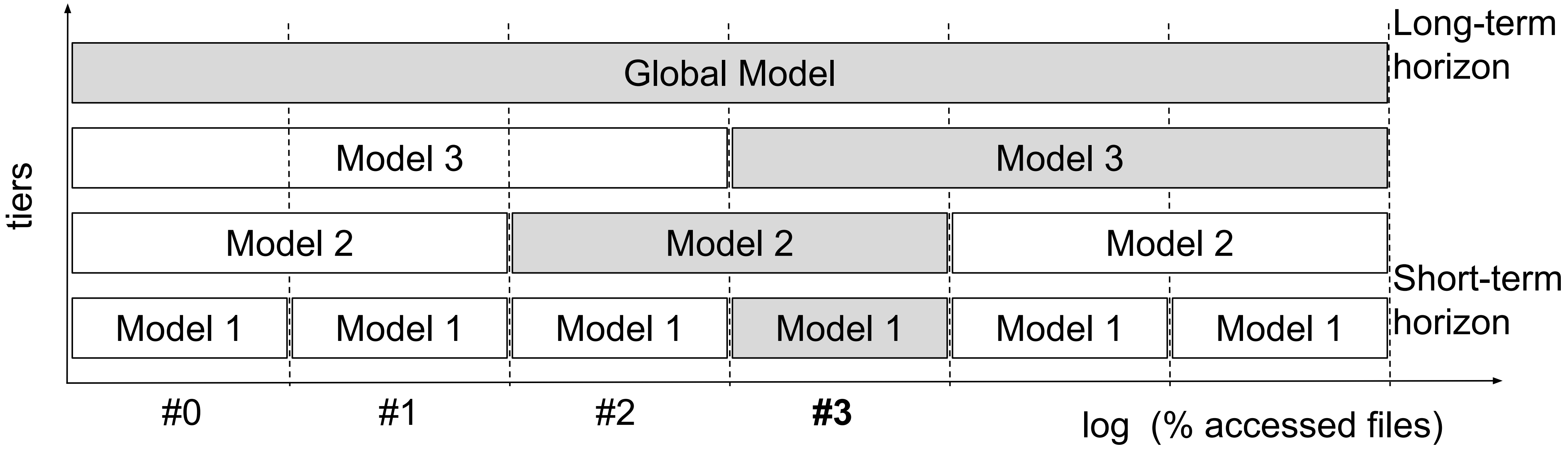
Multi-tier Incremental Models

tick #2



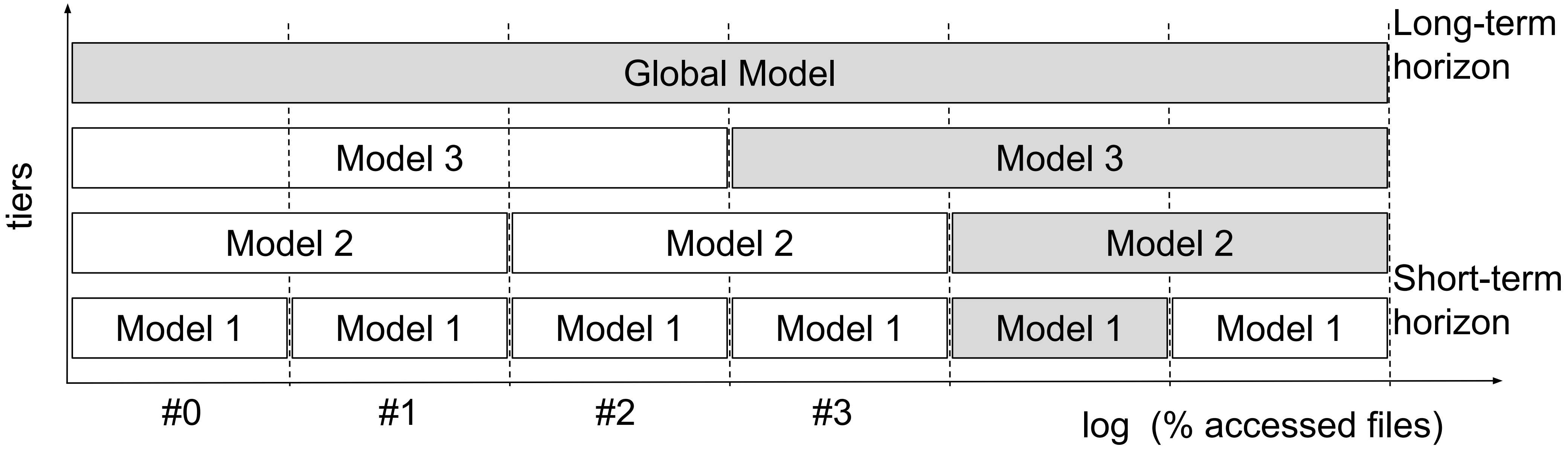
Multi-tier Incremental Models

tick #3



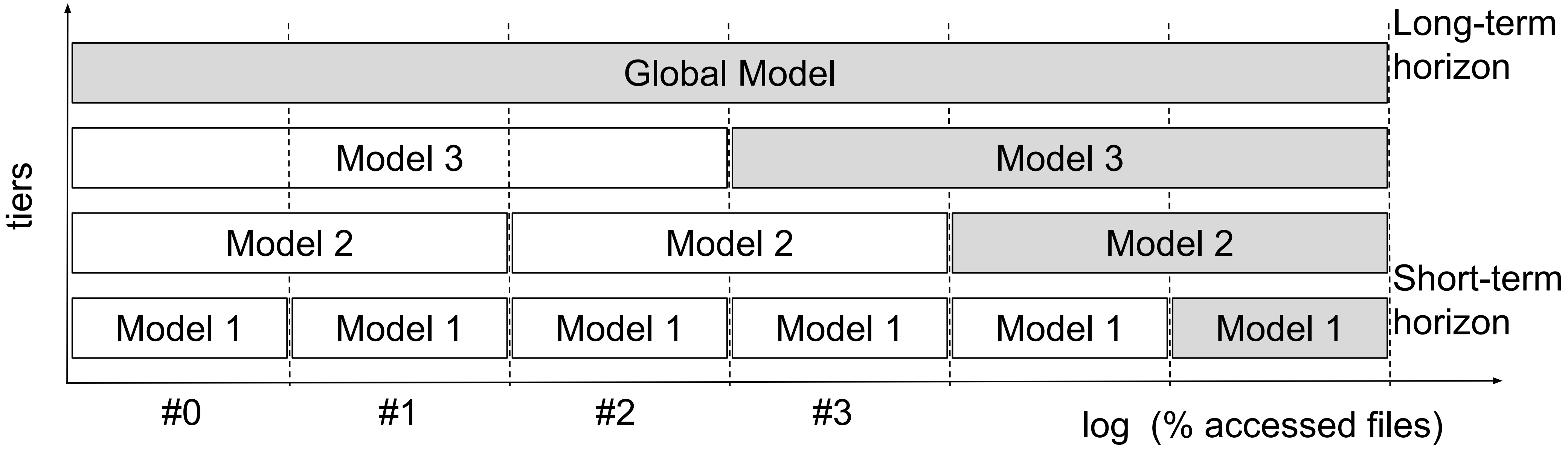
Multi-tier Incremental Models

tick #4

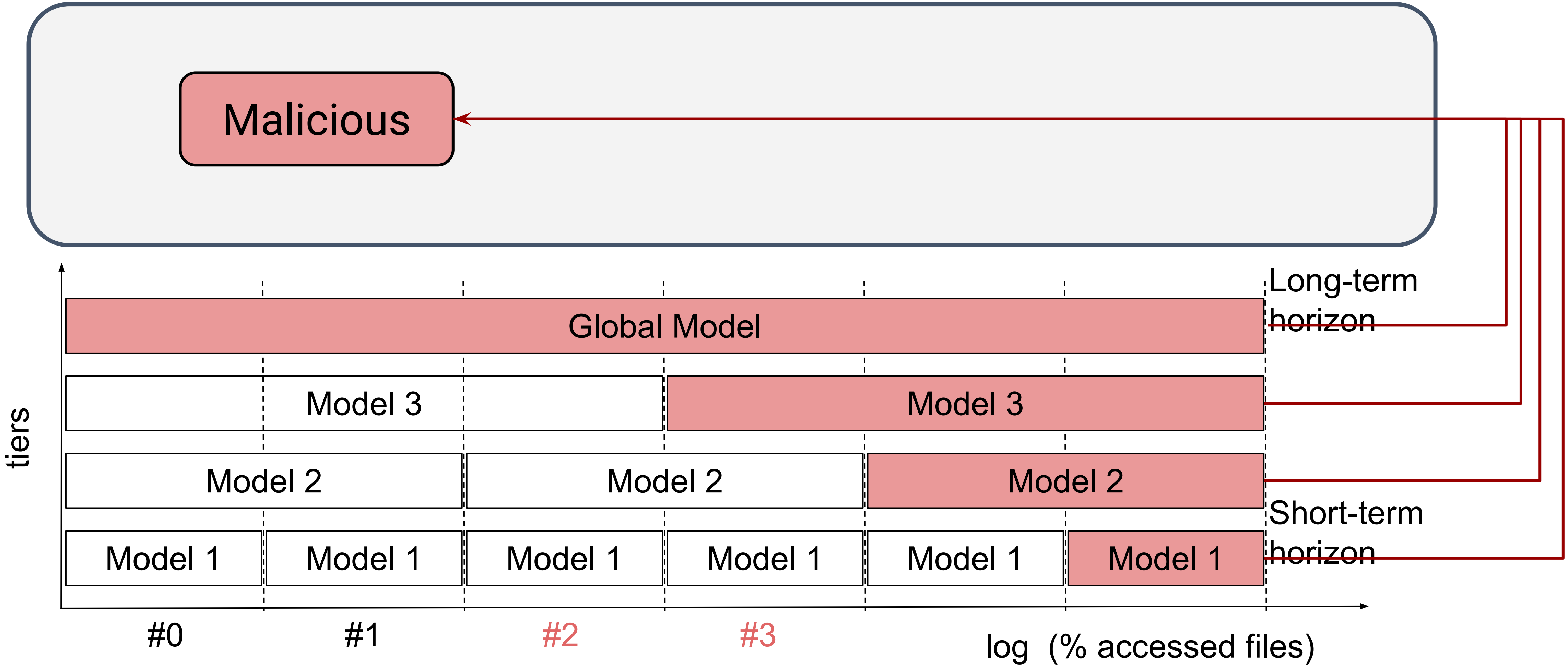


Multi-tier Incremental Models

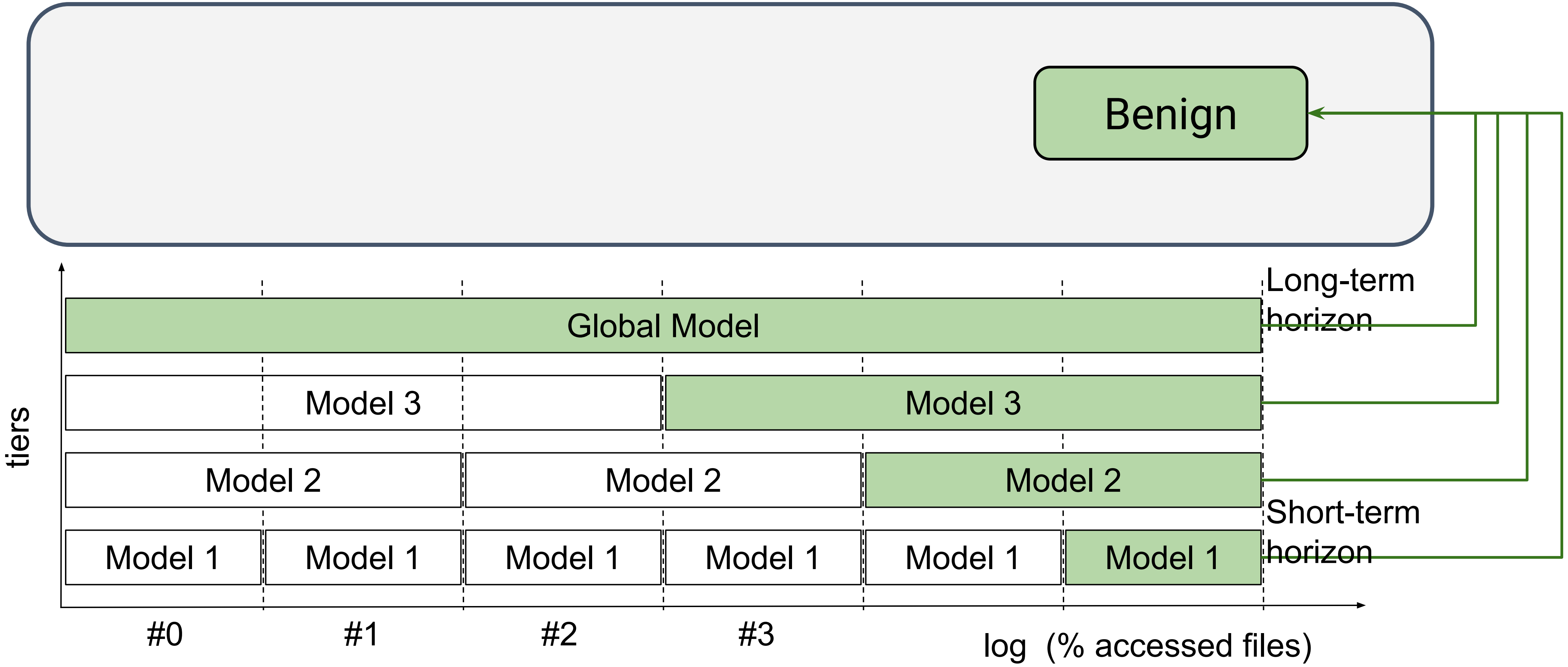
tick #5



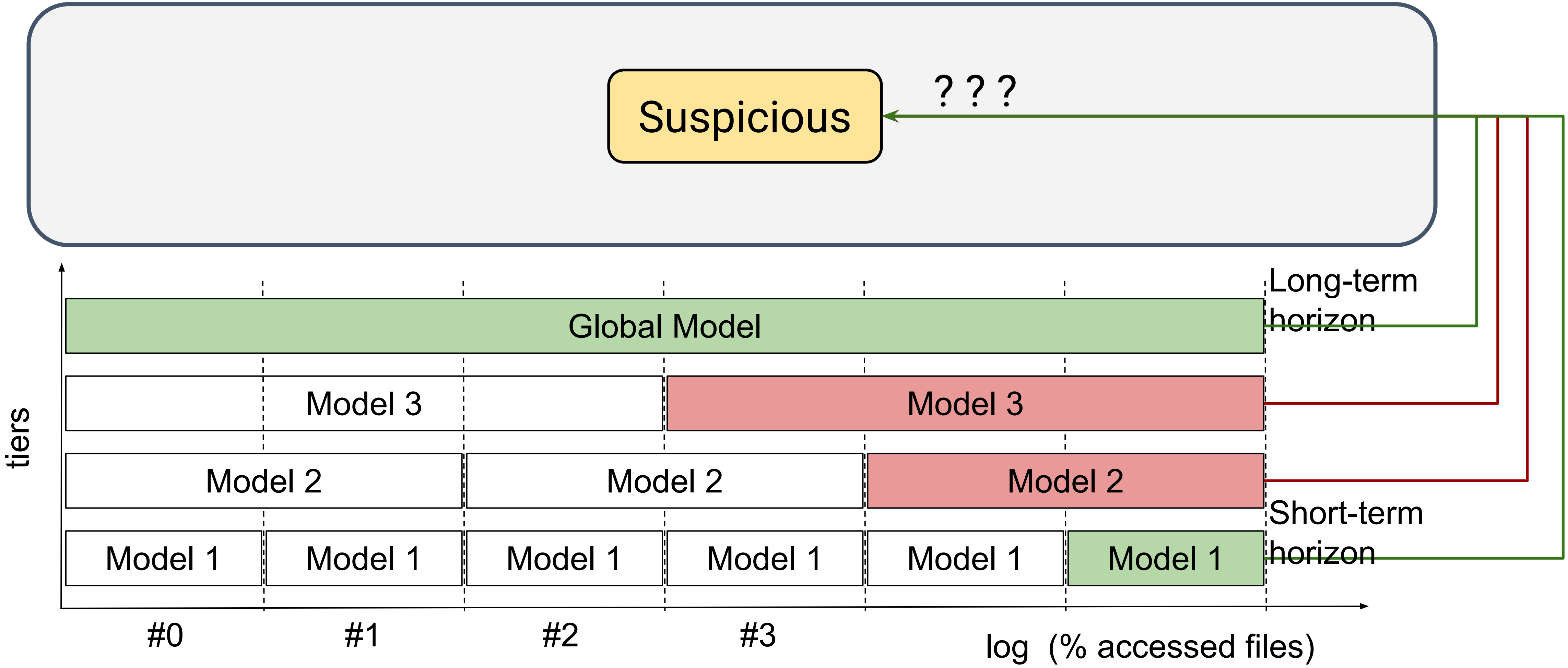
Multi-tier Incremental Models



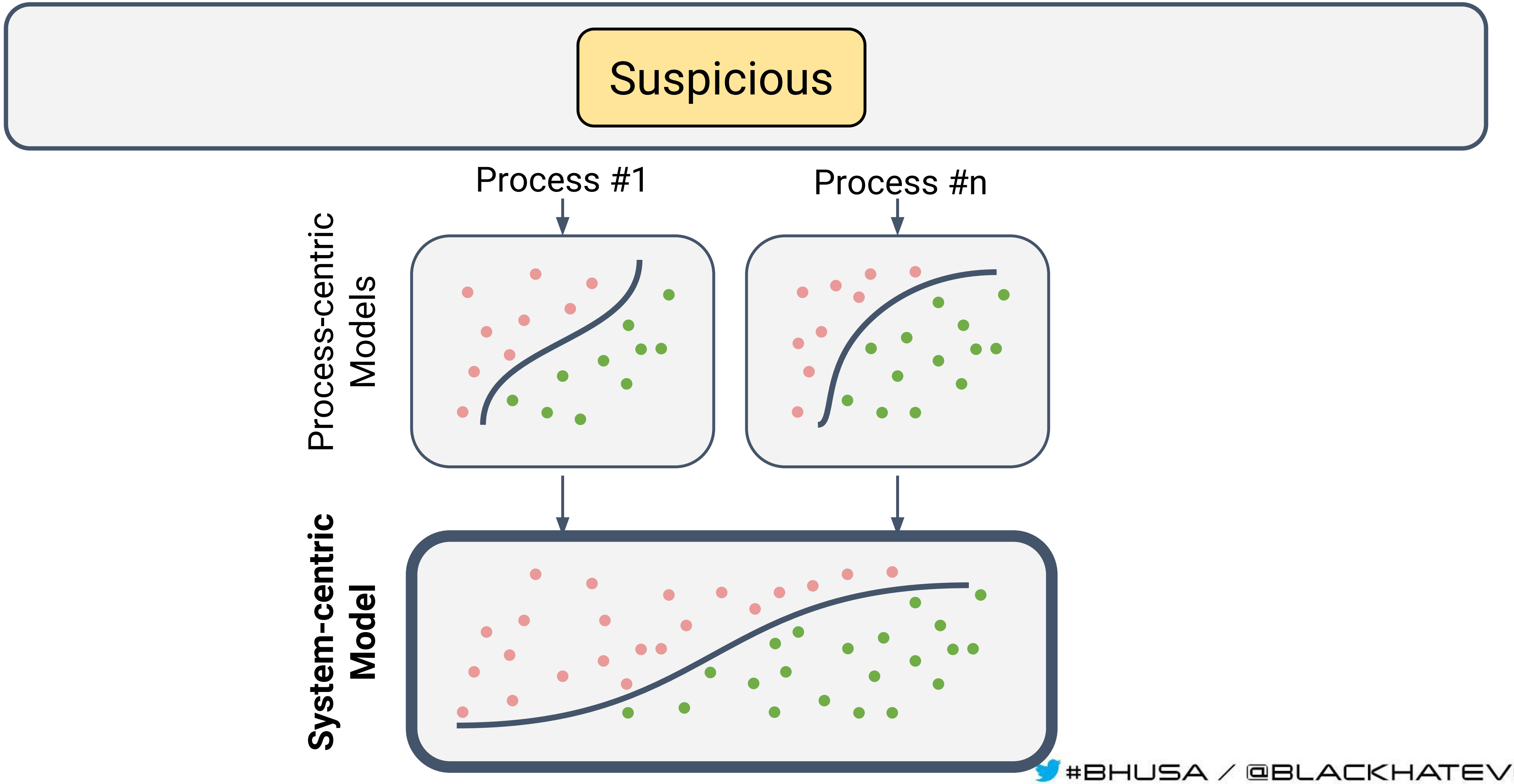
Multi-tier Incremental Models



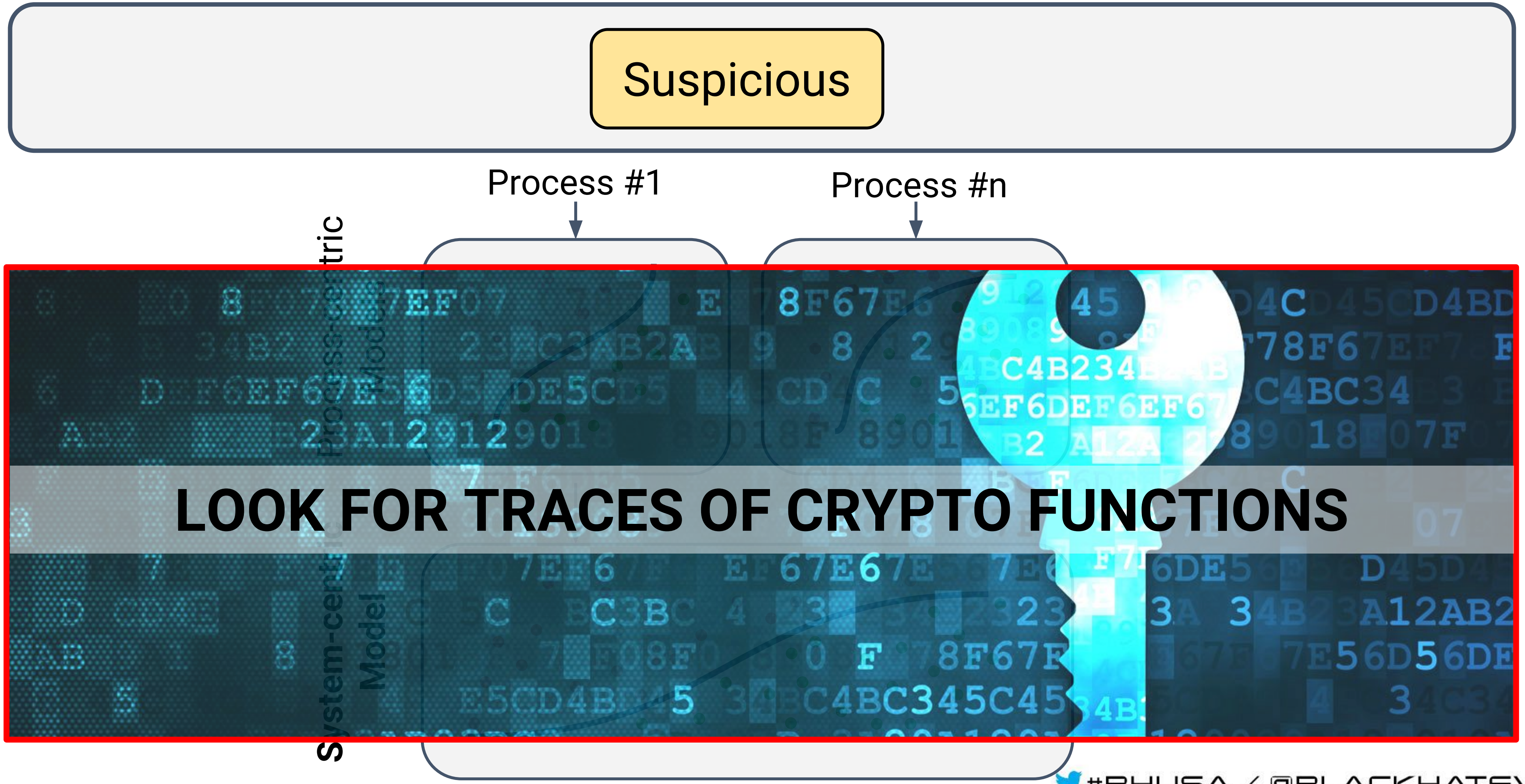
Multi-tier Incremental Models



I’m Confused..

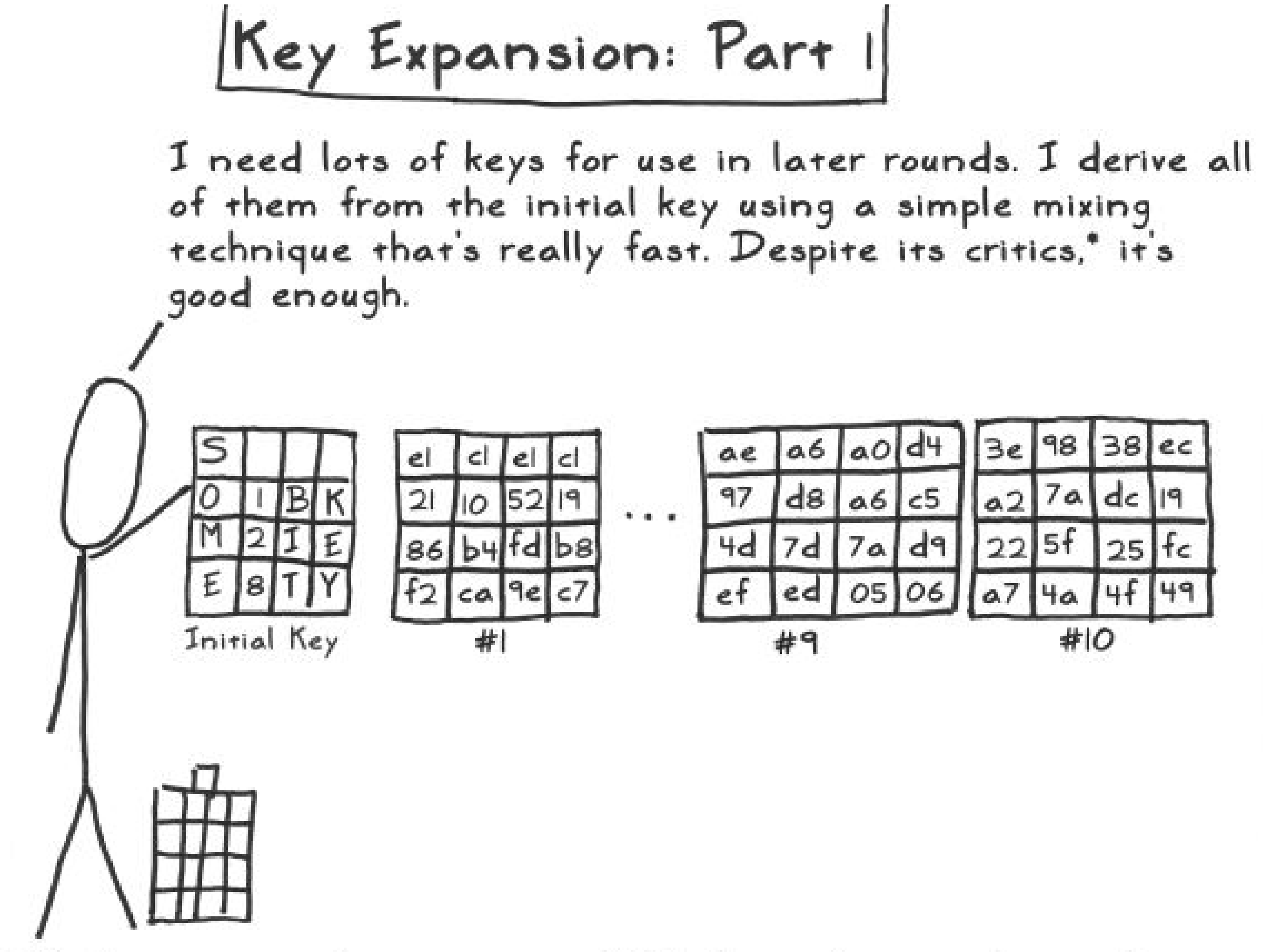

Suspicious
Process #1
Process #n
Process-centric Models
System-centric Model

I’m Confused..



LOOK FOR TRACES OF CRYPTO FUNCTIONS

Block Ciphers: Key Schedule


Key Expansion: Part 1
I need lots of keys for use in later rounds. I derive all of them from the initial key using a simple mixing technique that's really fast. Despite its critics,* it's good enough.
Initial Key
#1
...
#9
#10

Initial Key

S			
O	1	B	K
M	2	I	E
E	8	T	Y

#1

e1	c1	e1	c1
21	10	52	19
86	b4	fd	b8
f2	ca	9e	c7

#9

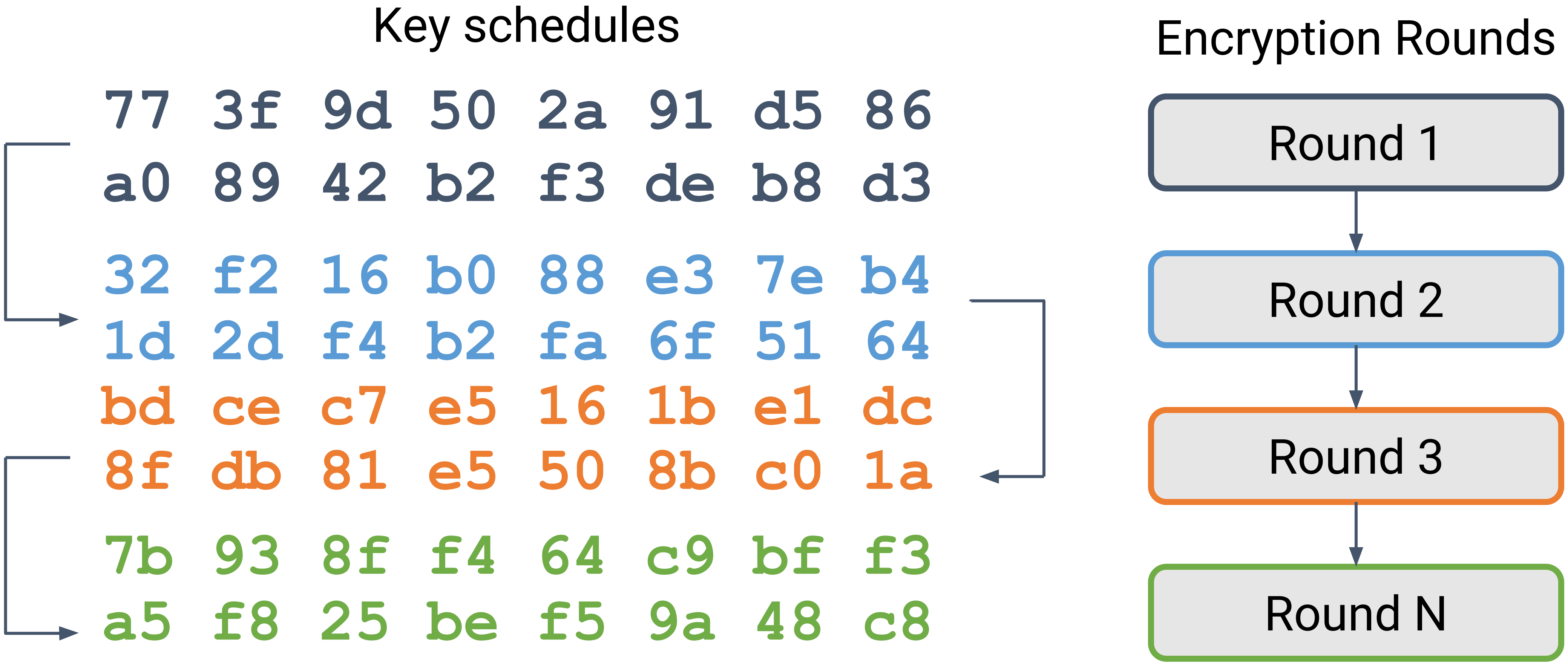
ae	a6	a0	d4
97	d8	a6	c5
4d	7d	7a	d9
ef	ed	05	06

#10

3e	98	38	ec
a2	7a	dc	19
22	5f	25	fc
a7	4a	4f	49

* By far, most complaints against AES's design focus on this simplicity.

Traces of Crypto Primitives



Key schedules

```
77 3f 9d 50 2a 91 d5 86
a0 89 42 b2 f3 de b8 d3

32 f2 16 b0 88 e3 7e b4
1d 2d f4 b2 fa 6f 51 64
bd ce c7 e5 16 1b e1 dc
8f db 81 e5 50 8b c0 1a

7b 93 8f f4 64 c9 bf f3
a5 f8 25 be f5 9a 48 c8
```

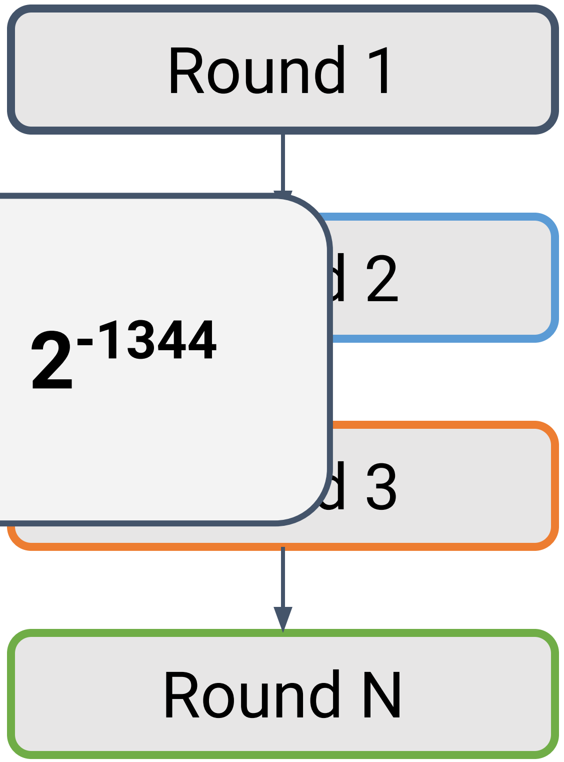
Encryption Rounds

Traces of Crypto Primitives

Key schedules

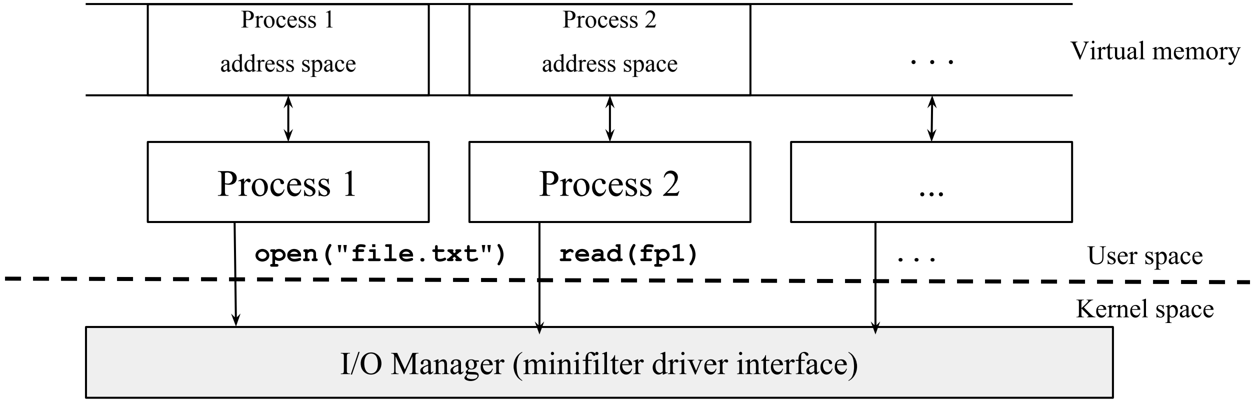
```
77 3f 9d 50 2a 91 d5 86
a0 89 42 b2 f3 de b8 d3

32 f2 16
1d 2d f4
bd ce c7
8f db 81

7b 93 8f f4 64 c9 bf f3
a5 f8 25 be f5 9a 48 c8
```

Encryption Rounds

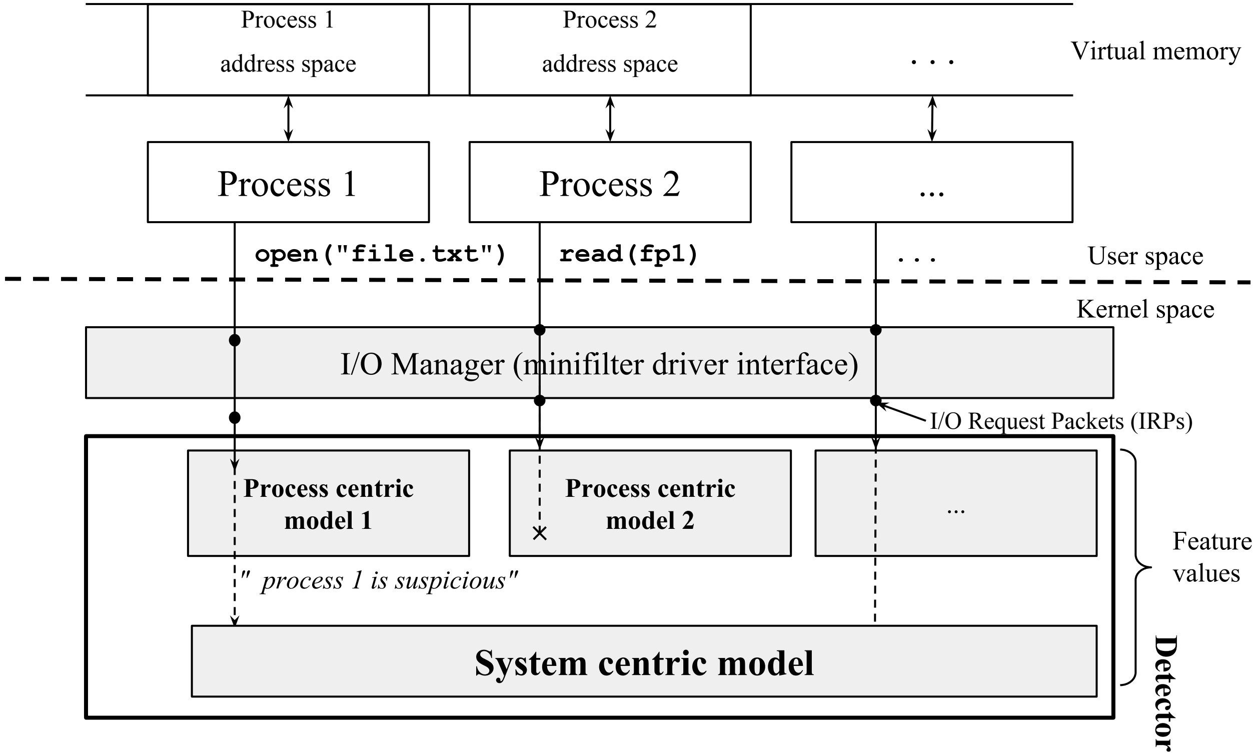


False Positives for AES: $\mathbf{2^{-1344}}$

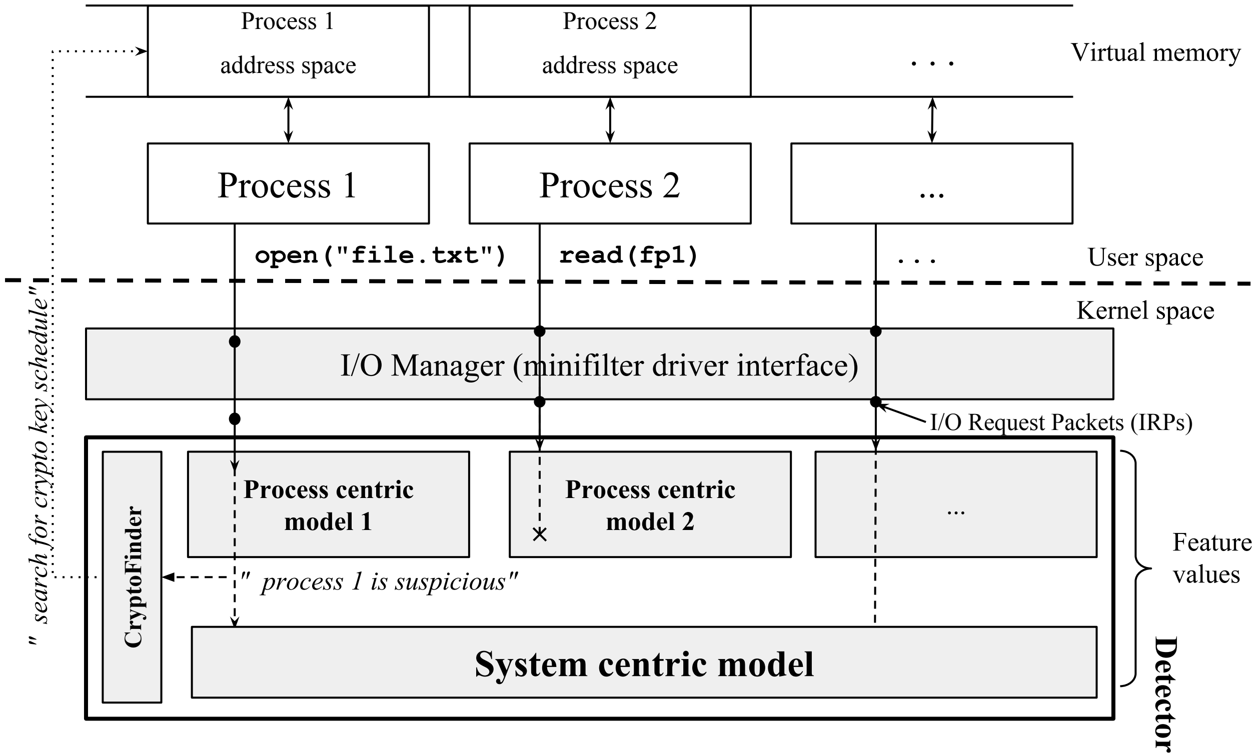
ShieldFS: Architecture



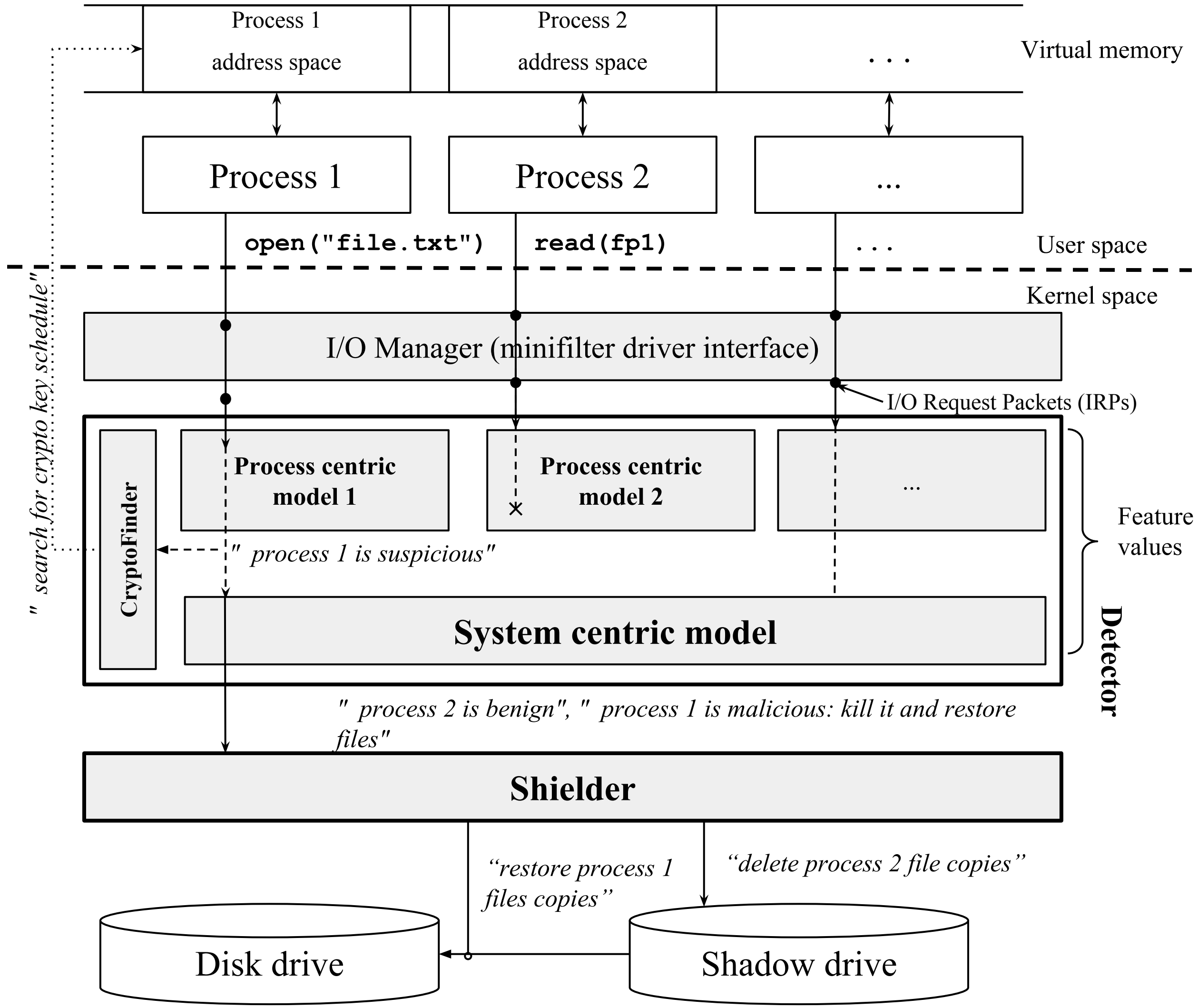
ShieldFS: Architecture



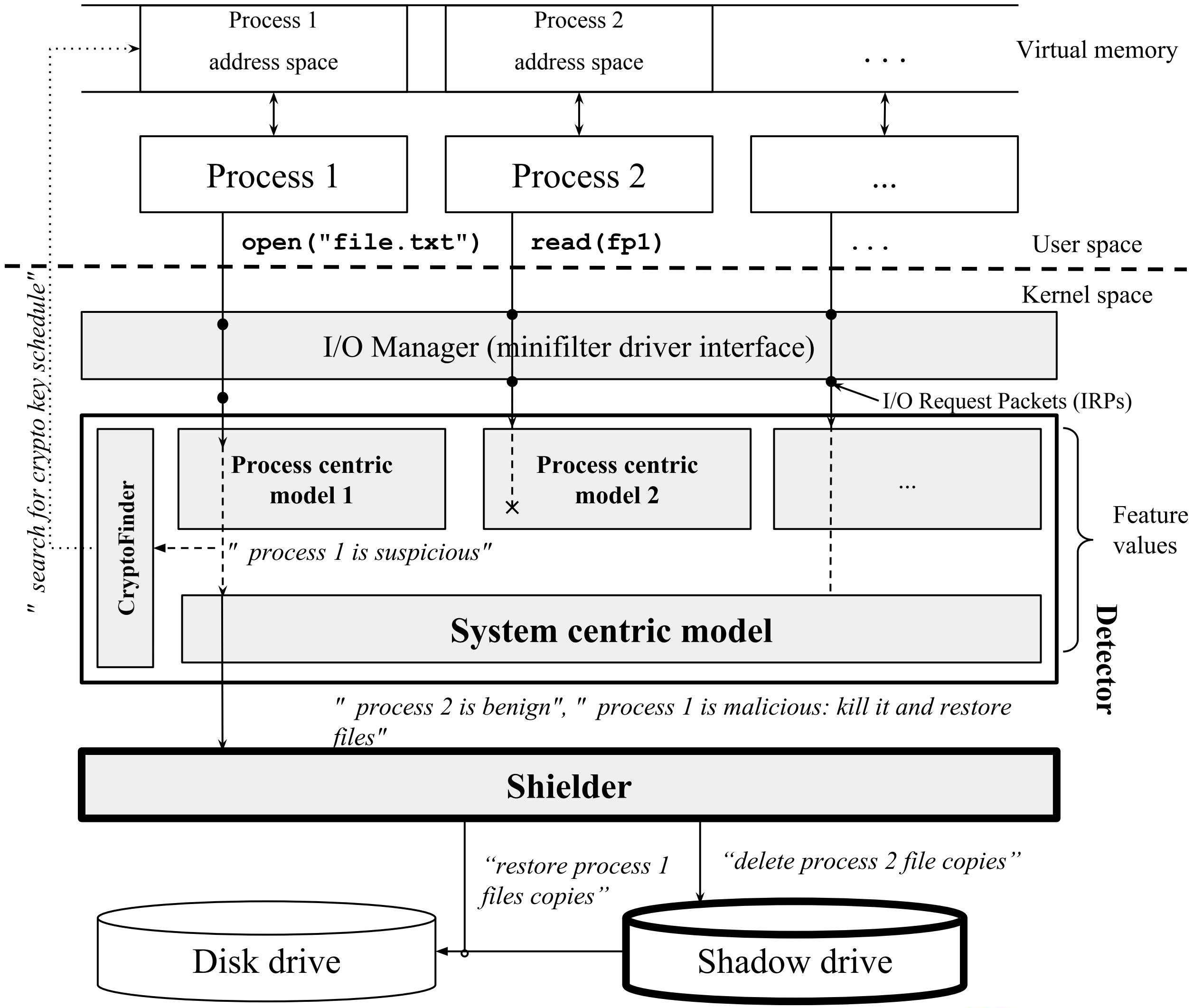
ShieldFS: Architecture



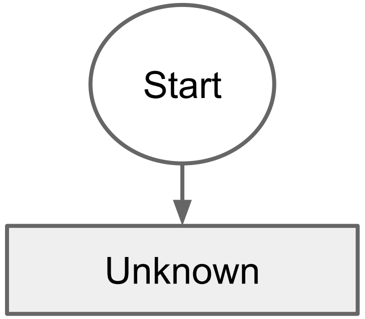
ShieldFS: Architecture



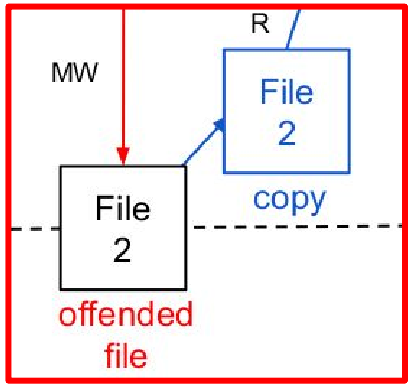
ShieldFS: Architecture

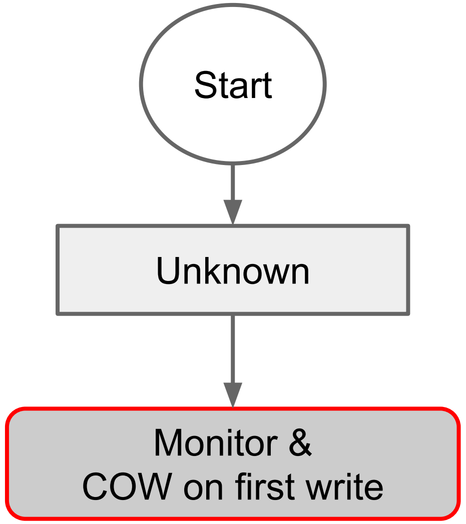


File Recovery Workflow



File Recovery Workflow



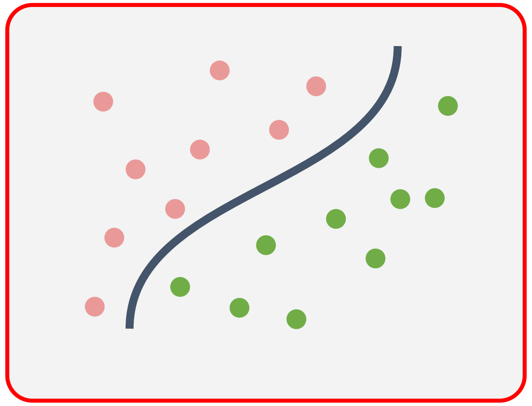


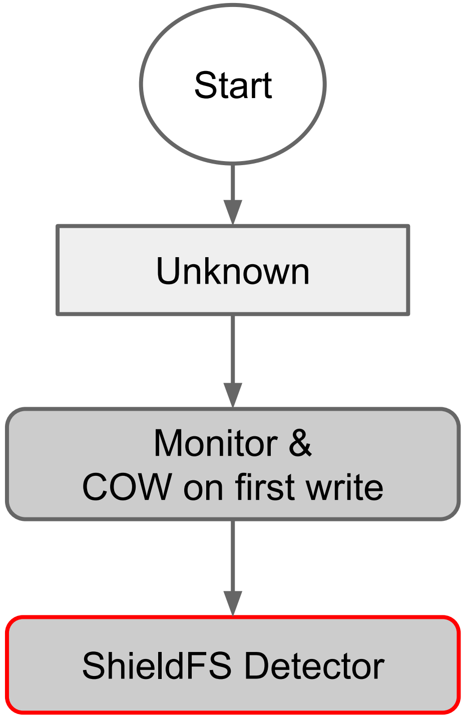
Start

Unknown

Monitor & COW on first write

File Recovery Workflow





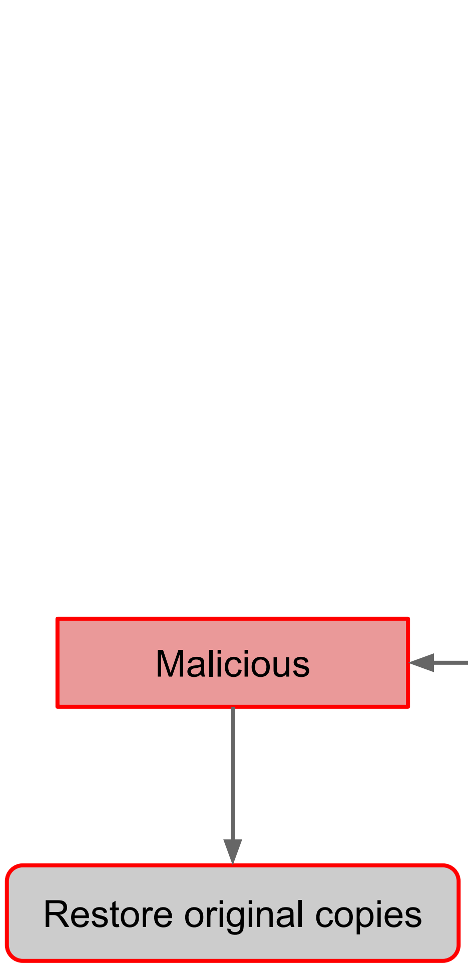
Start

Unknown

Monitor &
COW on first write

ShieldFS Detector

File Recovery Workflow



Start

Unknown

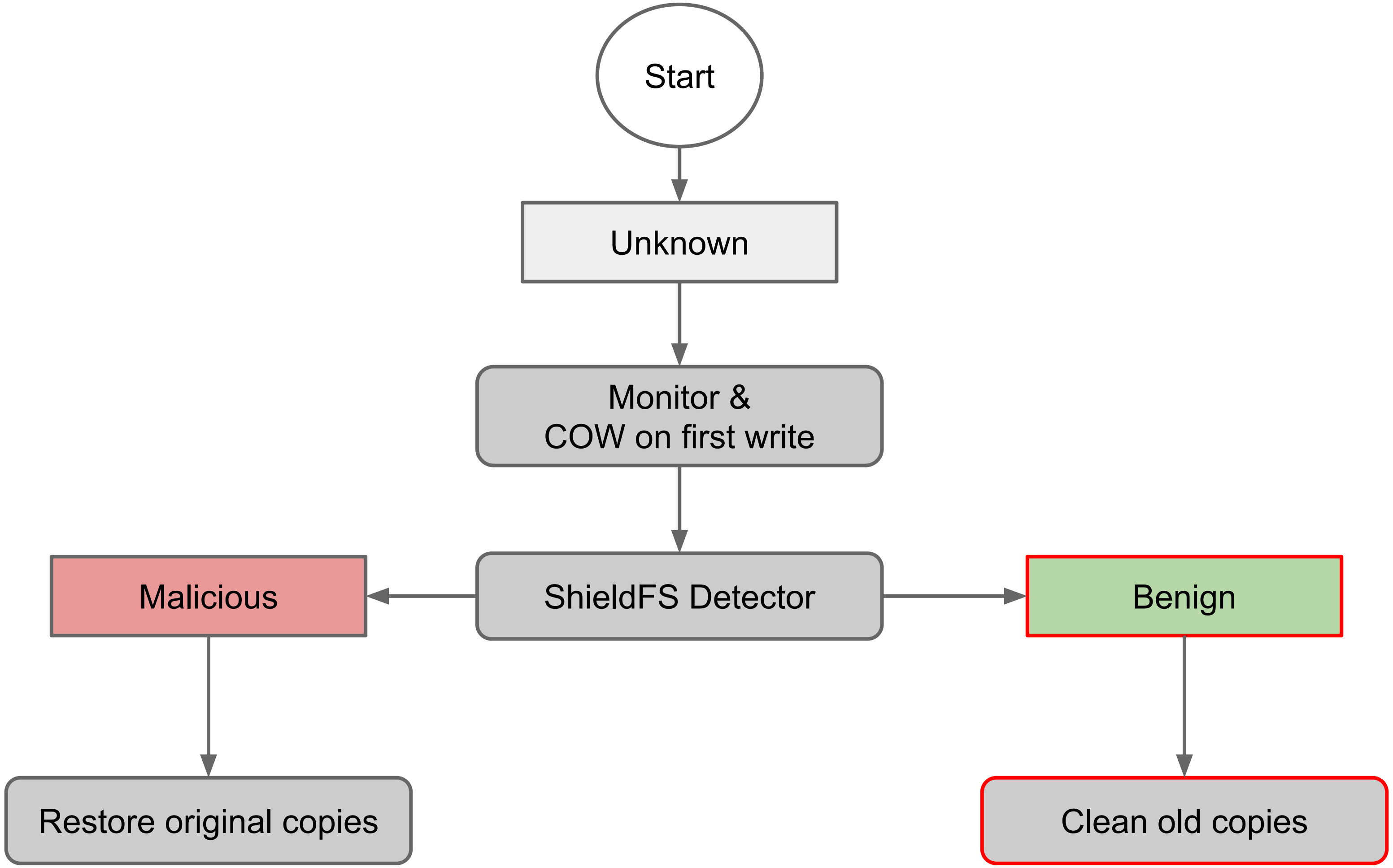
Monitor &
COW on first write

ShieldFS Detector

Malicious

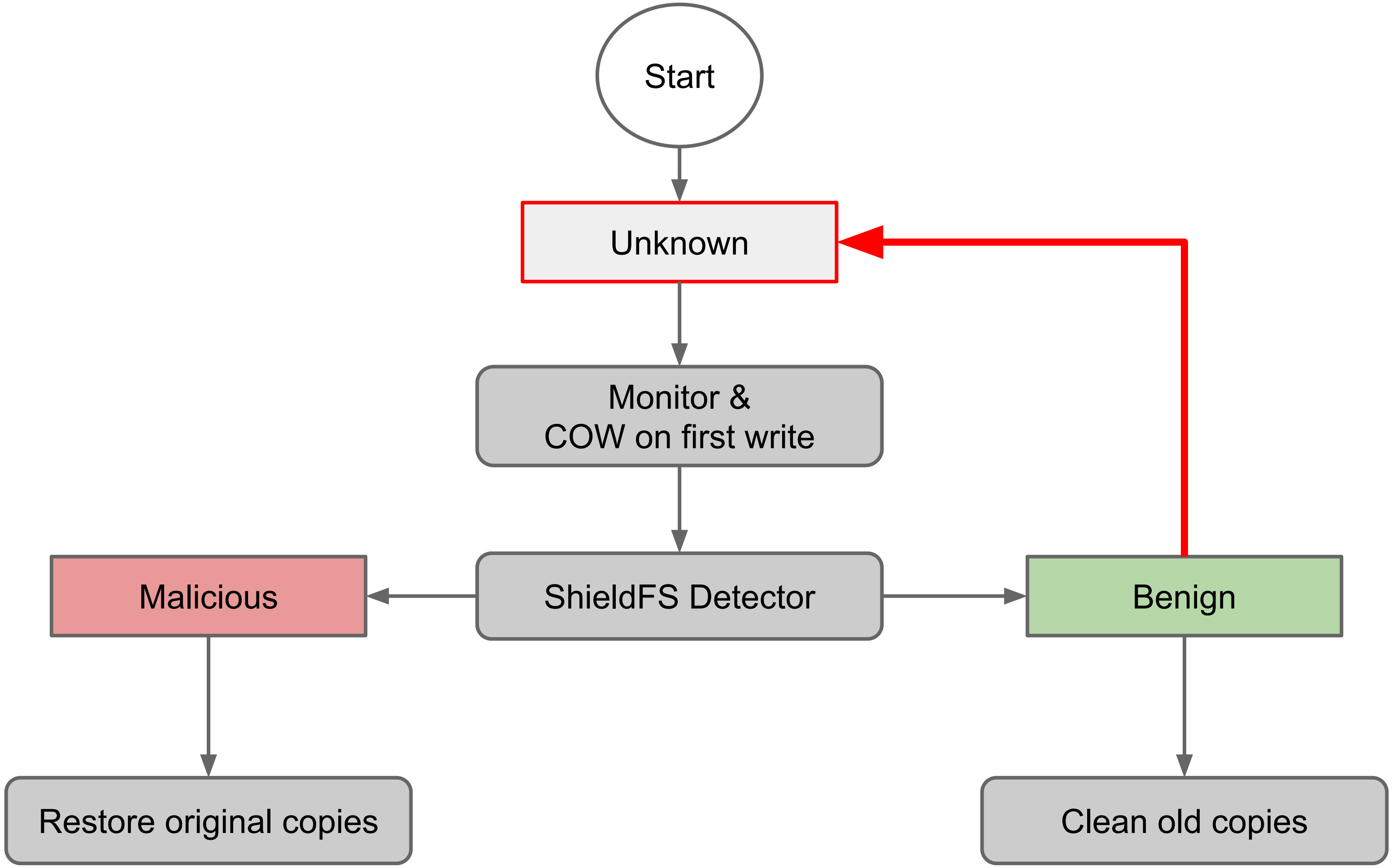
Restore original copies

File Recovery Workflow

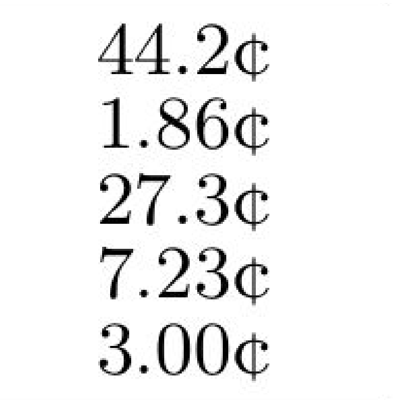


black hat USA 2017

File Recovery Workflow

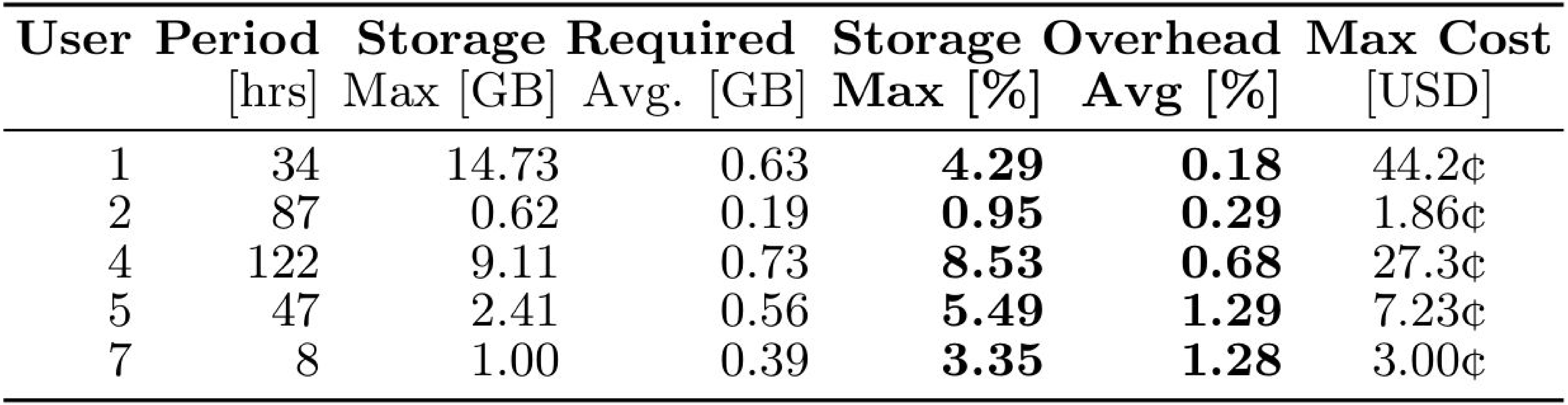


Storage Overhead



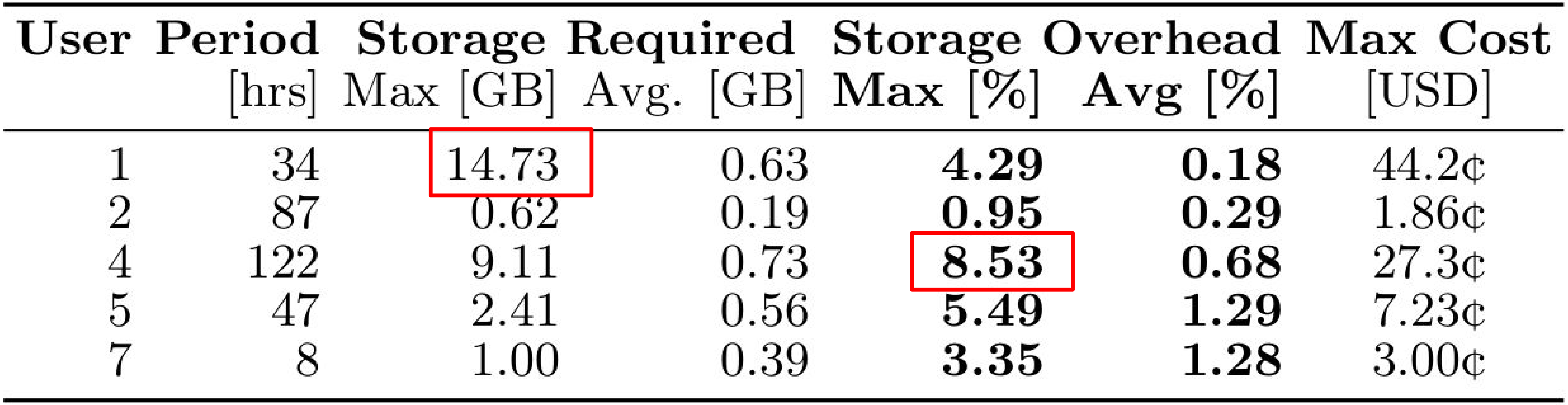
44.2¢
1.86¢
27.3¢
7.23¢
3.00¢

Storage Overhead



User	Period	Storage Required		Storage Overhead		Max Cost
	[hrs]	Max [GB]	Avg. [GB]	**Max [%]**	**Avg [%]**	[USD]
1	34	14.73	0.63	**4.29**	**0.18**	44.2¢
2	87	0.62	0.19	**0.95**	**0.29**	1.86¢
4	122	9.11	0.73	**8.53**	**0.68**	27.3¢
5	47	2.41	0.56	**5.49**	**1.29**	7.23¢
7	8	1.00	0.39	**3.35**	**1.28**	3.00¢

Storage Overhead



User	Period	Storage Required		Storage Overhead		Max Cost
	[hrs]	Max [GB]	Avg. [GB]	**Max [%]**	**Avg [%]**	[USD]
1	34	14.73	0.63	**4.29**	**0.18**	44.2¢
2	87	0.62	0.19	**0.95**	**0.29**	1.86¢
4	122	9.11	0.73	**8.53**	**0.68**	27.3¢
5	47	2.41	0.56	**5.49**	**1.29**	7.23¢
7	8	1.00	0.39	**3.35**	**1.28**	3.00¢

More Numbers?

Detection & Recovery Capabilities

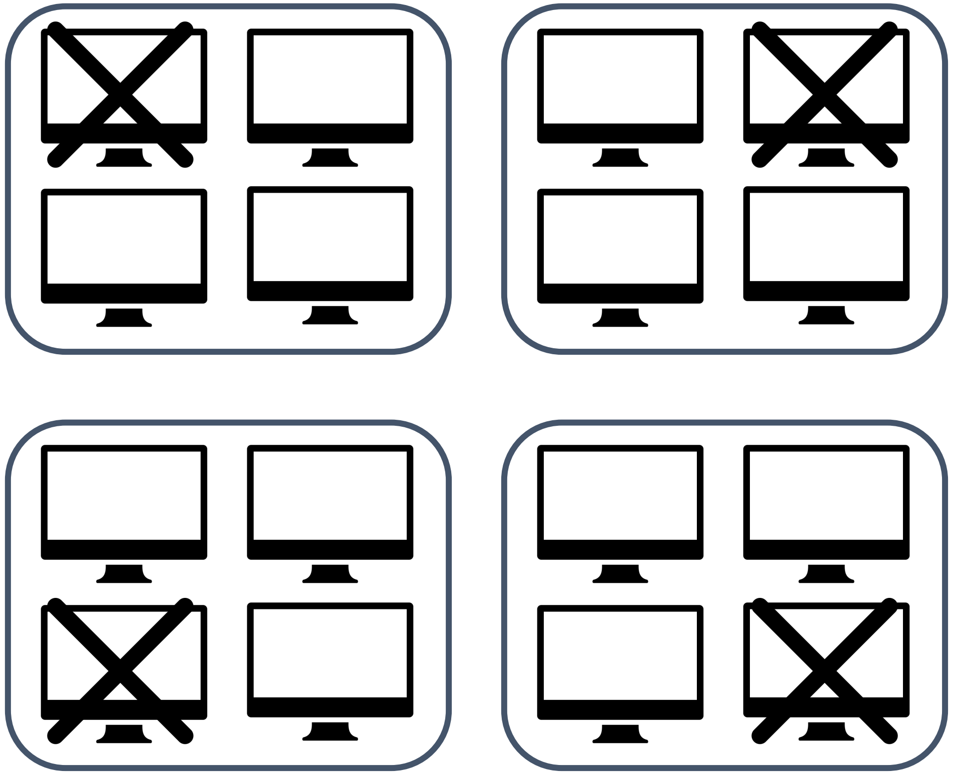
- 1483 unseen samples (from VT + Trend)
  - Locky, TeslaCrypt, CryptoLocker, Critroni, TorrentLocker, CryptoWall, Troldesh, CryptoDefense, PayCrypt, DirtyDecrypt, ZeroLocker, Cerber, WannaCry
- Files protected: always **100%**
  - Even in case of missed detection
- Detection rate: 1436/1483, **96.9%**

Detection & Recovery Capabilities

- 1483 unseen samples (from VT + Trend)
  - Locky, TeslaCrypt, CryptoLocker, Critroni, TorrentLocker, CryptoWall, Troldesh, CryptoDefense, PayCrypt, DirtyDecrypt, ZeroLocker, Cerber, WannaCry

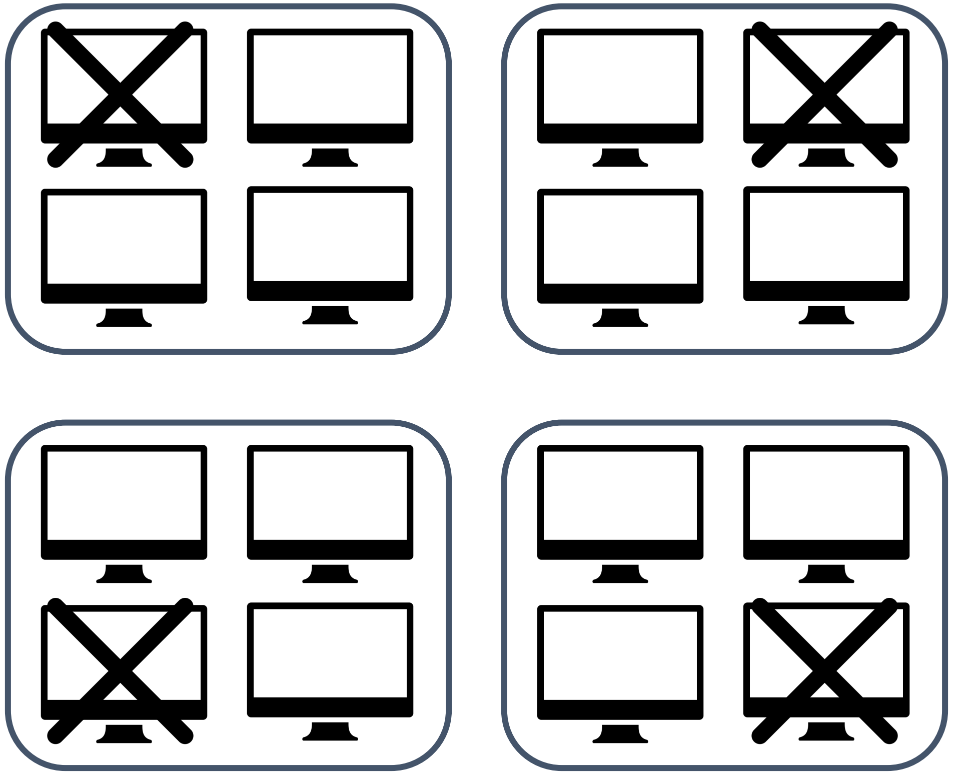
- Files protected: always **100%**
  - Even in case of missed detection
- Detection rate: 1436/1483, **96.9%**

False Positive Evaluation



FPR with One-machine-off Cross Validation

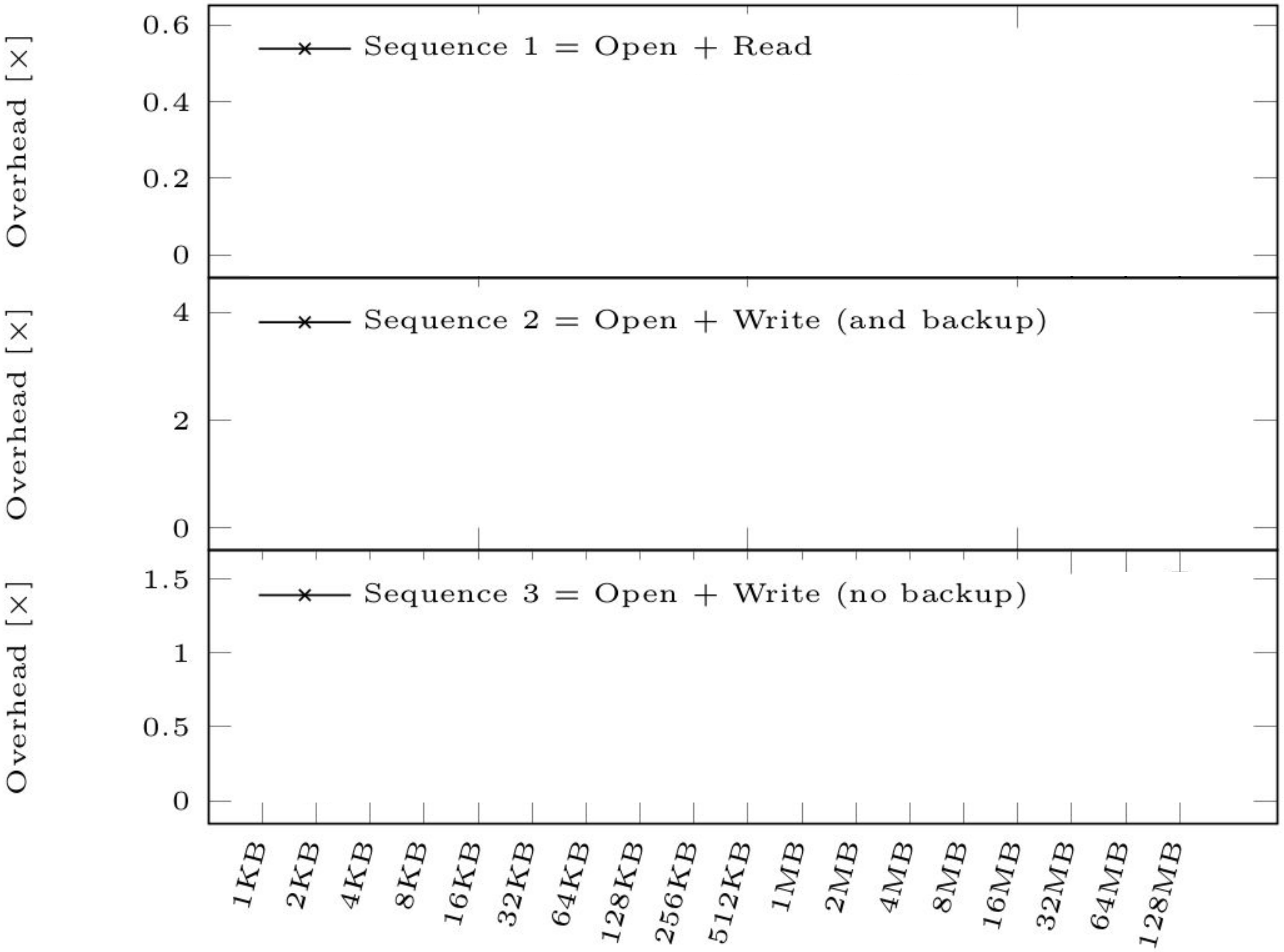
False Positive Evaluation



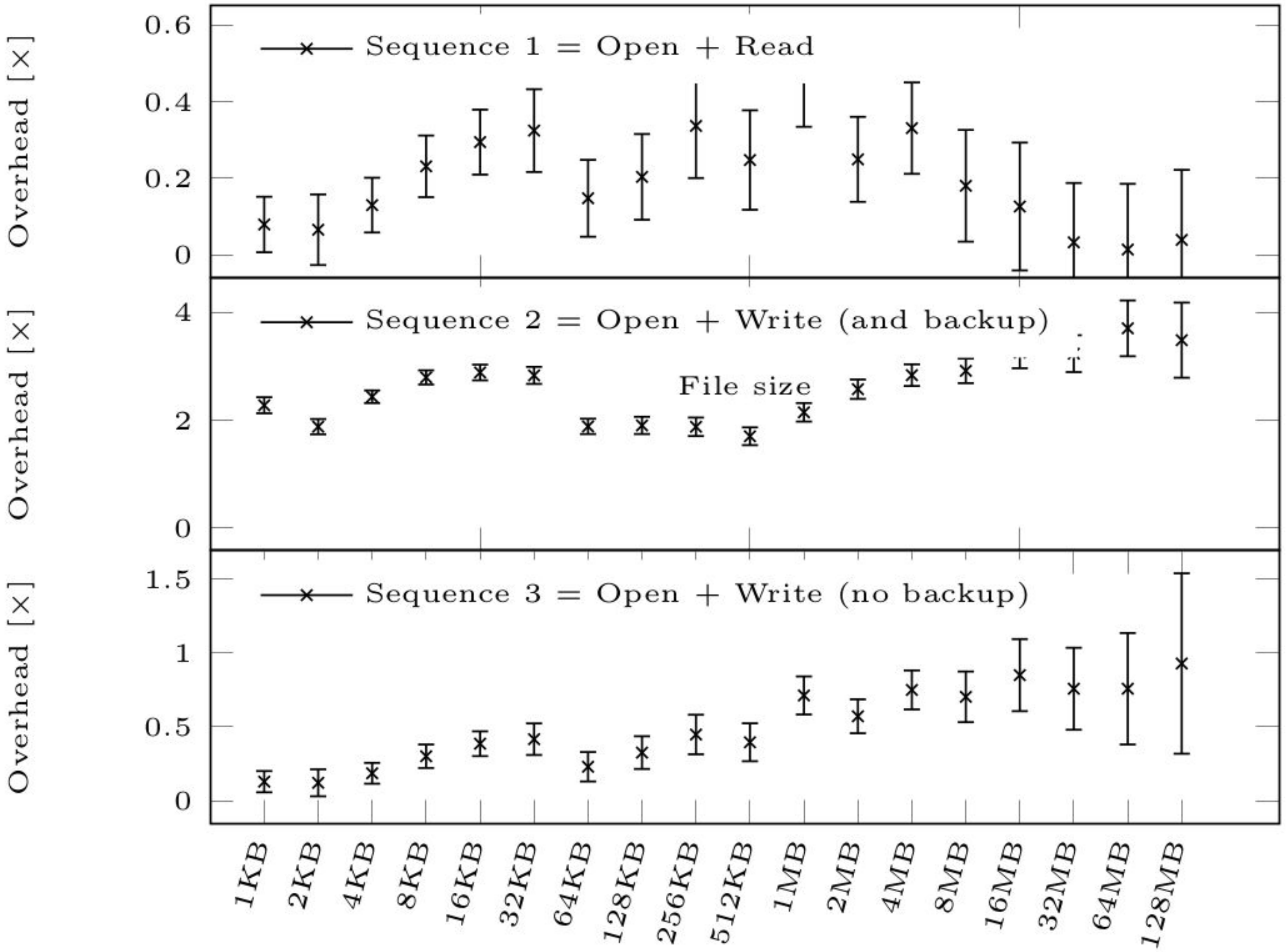
User	False positive rate [%]		
Machine	Process	System	Outcome
1	0.53	23.26	**0.27**
2	0.00	0.00	**0.00**
3	0.00	0.00	**0.00**
4	0.00	1.20	**0.00**
5	0.22	45.45	**0.15**
6	0.00	4.76	**0.00**
7	0.00	88.89	**0.00**
8	0.00	0.00	**0.00**
9	0.00	0.00	**0.00**
10	0.00	0.00	**0.00**
11	0.00	0.00	**0.00**

FPR with One-machine-off Cross Validation

Overhead: Micro-benchmark

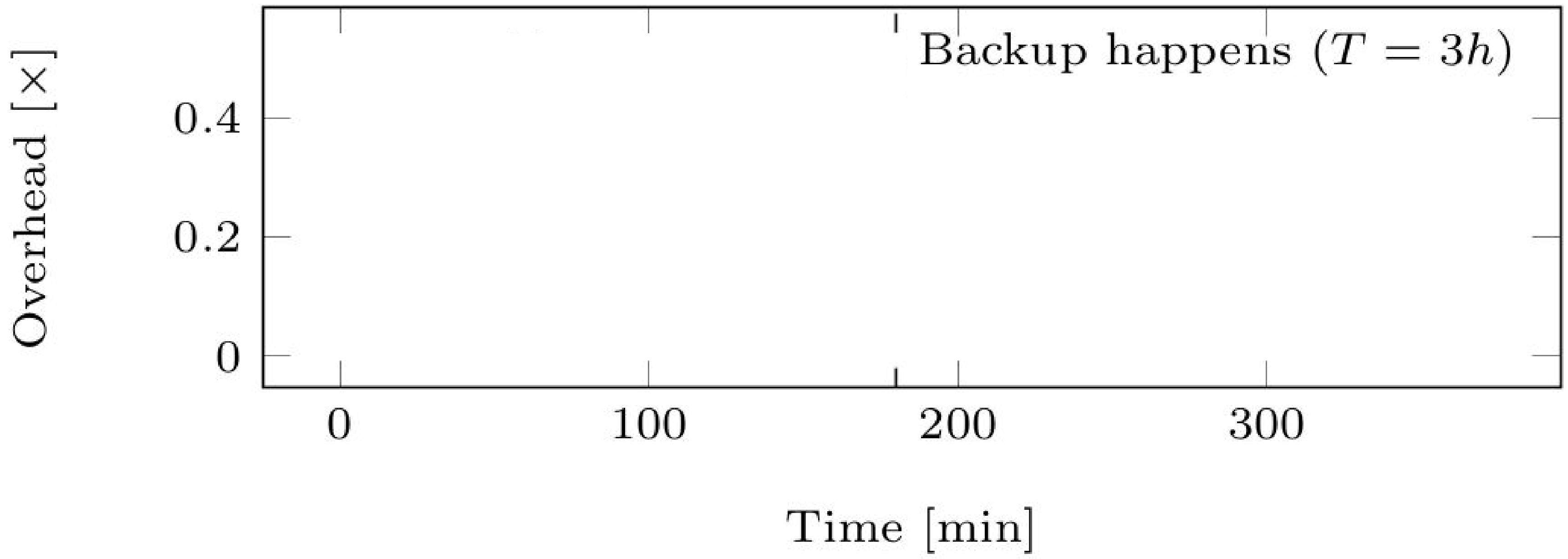


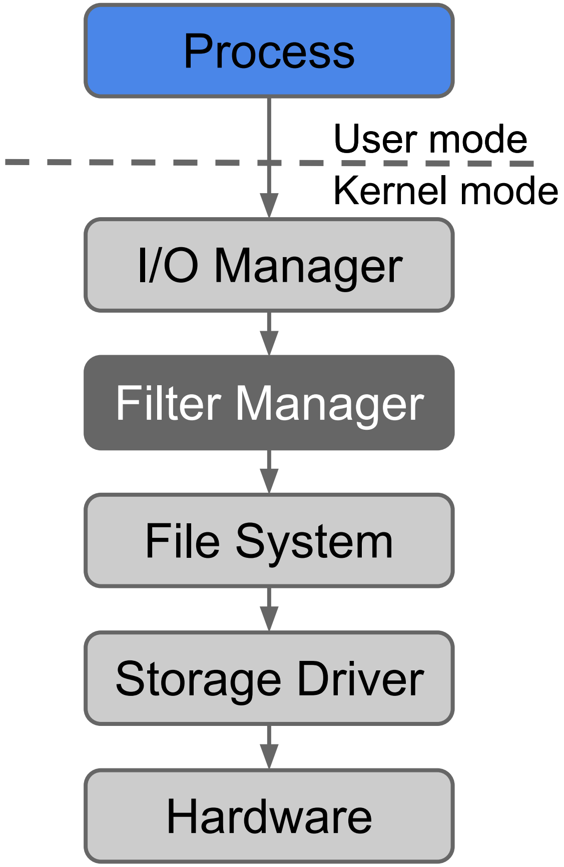
Overhead: Micro-benchmark



...however...

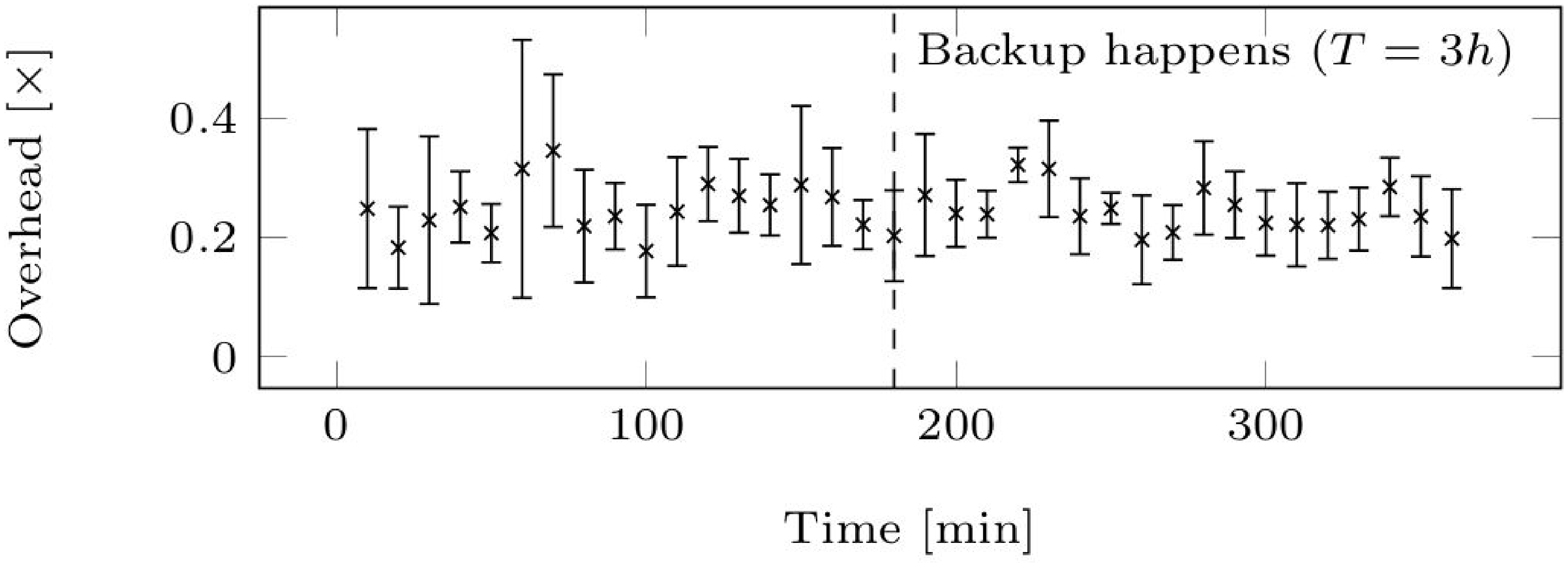
User-Perceived Overhead

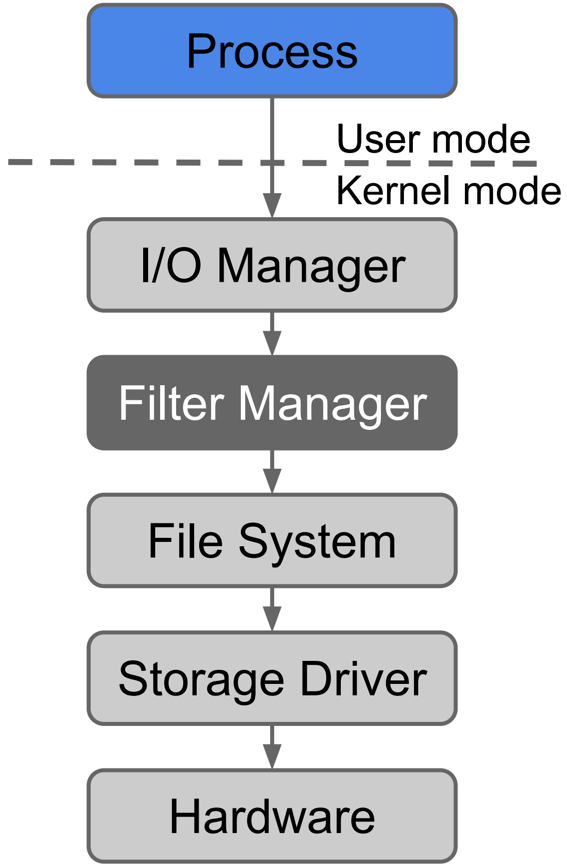




Average estimated overhead = 0.26×

User-Perceived Overhead





Average estimated overhead = 0.26×

Demo Time! 🤞

WannaCry Sample: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

Conclusions

Ransomware **significantly differs** from benign software from the filesystem's viewpoint

DETECTION. **Generic** ML models to identify ransomware

- Filesystem activity
- Use of symmetric crypto primitives

PROTECTION. Pure **detection** is **not enough**

- Self-healing virtual FS
- **Transparently revert the effects** of ransomware

Questions?

Andrea Continella
andrea.continella@polimi.it
@_conand

Federico Maggi
federico_maggi@trendmicro.com
@phretor

http://shieldfs.necst.it

* This work is subject to a US patent (pending) no. 27019

ShieldFS: A Self-healing, Ransomware-aware Filesystem

Andrea Continella
andrea.continella@polimi.it

Alessandro Guagnelli
alessandro.guagnelli@polimi.it

Giovanni Zingaro
giovanni.zingaro@polimi.it

Giulio De Pasquale
giulio.depasquale@polimi.it

Alessandro Barenghi
alessandro.barenghi@polimi.it

Stefano Zanero
stefano.zanero@polimi.it

Federico Maggi
federico.maggi@polimi.it

DEIB, Politecnico di Milano, Milan, Italy

ABSTRACT

Preventive and reactive security measures can only partially mitigate the damage caused by modern ransomware attacks.

1 INTRODUCTION

Ransomware [20] is a class of malware that encrypts valuable files found on the victim's machine and asks for a ransom to

black hat USA 2017

JULY 22-27, 2017
MANDALAY BAY / LAS VEGAS

POLITECNICO MILANO 1863
DIPARTIMENTO DI ELETTRONICA INFORMAZIONE E BIOINGEGNERIA

TREND MICRO

ShieldFS: The Last Word in Ransomware Resilient Filesystems

Andrea Continella, Alessandro Guagnelli, Giovanni Zingaro, Giulio De Pasquale,
Alessandro Barenghi, Stefano Zanero, **Federico Maggi**