Detection of Ransomware using Immutable Anomalous Performance Data

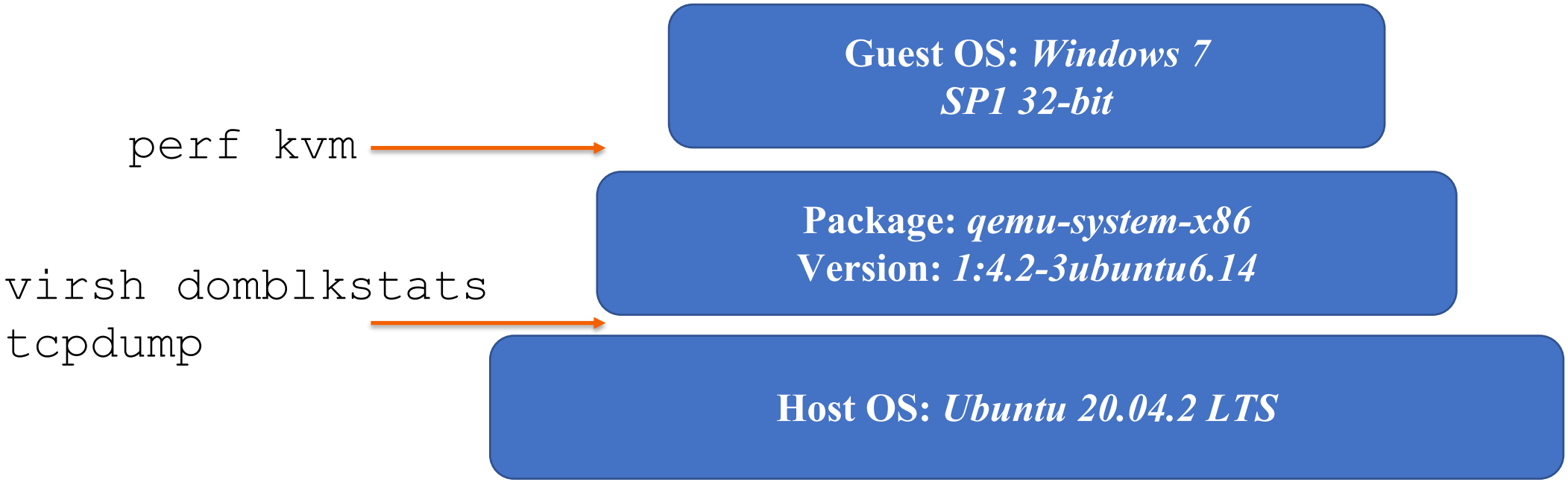
Rajendra Boppana
Kumar Thummapudi (Student)
Palden Lama, Gregory White

[MONITOR ACTIVATES]

Experimental Setup and Data Collection

Experimental Setup

- Chameleon cloud at TACC: a Chameleon node is configured for experiments



perf

- `sudo perf kvm stat -I <interval_in_msecs>`
  `--interval-count <no_of_intervals>`
  `-o <write_output_to_file> --append`
  `-e <list_of_events_comma_separated>`

- Stats were collected for about 1 minute
  - 100 ms sampling interval ⇒ 600 samples
  - 1 ms sampling interval ⇒ 60,000 samples

- Up to four events of interest + instructions

Hardware Performance Counter Events

Events	Events	Events
Cycles	Instructions	Branches
Branch-misses	Mem-stores	L1-dcache-loads
L1-dcache-load-misses	L1-icache-load-misses	LLC-loads
LLC-load-misses	dTLB-loads	dTLB-load-misses
iTLB-loads	iTLB-load-misses	CPU-clock
Context-switches	Page-faults	Mem-loads

perf Raw Data

```
# started on Fri Jan 15 02:25:56 2021

#           time             counts unit events
     0.106274293        318,119,958      instructions
     0.106274293        117,426,826      L1-dcache-loads
     0.106274293          1,921,114      L1-dcache-load-misses     #    1.64% of all L1-dcache hits
     0.106274293                451      context-switches
     0.212214660          1,158,977      instructions
     0.212214660            476,369      L1-dcache-loads
     0.212214660             70,048      L1-dcache-load-misses     #    0.12% of all L1-dcache hits
     0.212214660                253      context-switches
     0.318276587          2,275,197      instructions
     0.318276587            874,941      L1-dcache-loads
     0.318276587             94,930      L1-dcache-load-misses     #    0.24% of all L1-dcache hits
     0.318276587                246      context-switches
     0.424265273          1,013,470      instructions
     0.424265273            423,016      L1-dcache-loads
     0.424265273             63,970      L1-dcache-load-misses     #    0.21% of all L1-dcache hits
     0.424265273                229      context-switches
     0.530226164        237,117,650      instructions
     0.530226164         84,987,565      L1-dcache-loads
```

perf Data Reformatted

```
...4.109.79 | ...s — -bash ... | ...— -bash | ...a — -bash ... | ...— -bash ... | ...a — -bash ... | ...a — -bash ...
instructions,L1-icache-load-misses,dTLB-load-misses,branch-misses,iTLB-load-misses
205940,33951,2307,2525,2031
0,0,0,0,0
721071,20182,3515,3723,3112
129234,19057,1810,2288,1025
0,0,0,0,0
1113885,36209,3855,6103,4484
935598,11827,1281,2613,685
1510712,6680,770,994,280
0,0,0,0,0
1676139,14476,1736,2604,1582
1977447,4086,846,717,412
99678,9259,515,1272,416
1118104,14501,1566,2476,1851
1967547,10765,1420,1968,588
3623577,11653,1933,2315,1844
854466,29191,4295,5384,5232
```

domblkstat

```
for (( j = 1; j <= 3000; j++ ))
   do
      date >> domblkstats
     virsh domblkstat Win7KVM >> domblkstats
     echo >> domblkstats
   done
```

Disk Memory Subsystem Events

Events	Events	Events
rd_req	wr_req	flush_operations
rd_bytes	wr_bytes	
rd_total_times	wr_total_times	flush_total_times

domblkstat Raw Data

```
Fri 15 Jan 2021 02:25:56 AM UTC
Readings before start of 03bb4d5c0179fdceacc5df7645e6e7fa93e931ac9beb1968c7bbe40ba3499194.exe
 rd_req 5631044
 rd_bytes 208307542016
 wr_req 12565984
 wr_bytes 1398550276096
 flush_operations 57891
 rd_total_times 84024961512087
 wr_total_times 217260993681892
 flush_total_times 3056746313763


Fri 15 Jan 2021 02:25:56 AM UTC
 rd_req 5631064
 rd_bytes 208308118528
 wr_req 12565984
 wr_bytes 1398550276096
 flush_operations 57891
 rd_total_times 84024964295807
 wr_total_times 217260993681892
 flush_total_times 3056746313763
```

domblkstat Data Reformatted

...4.109.79 | ...s — -bash ... | ...— -bash | ...a — -bash ... | ...— -bash ... | ...a — -bash ... | ...a — -bash ... | ...s — -bash ... | ...—

```
wr_total_times,wr_req,rd_req,flush_total_times,rd_total_times,rd_bytes,flush_operations,wr_bytes
43230405,60,4,20045227,2874432,20480,2,3573760
18499650,10,0,1373147,0,0,3,53760
0,0,0,0,0,0,0,0
622063648,20,0,3574910,0,0,2,107008
0,0,0,0,0,0,0,0
0,0,0,0,0,0,0,0
0,0,0,0,0,0,0,0
0,0,0,0,0,0,0,0
0,0,0,0,0,0,0,0
0,0,0,0,0,0,0,0
0,0,0,0,0,0,0,0
0,0,0,0,0,0,0,0
0,0,0,0,0,0,0,0
0,0,0,0,0,0,0,0
0,0,0,0,0,0,0,0
0,0,5,0,508748,135168,0,0
0,0,8,0,425161,221184,0,0
0,0,3,0,331244,94208,0,0
0,0,2,0,114098,40960,0,0
0,0,0,0,0,0,0,0
0,0,0,0,0,0,0,0
```

Significant Events

- Identify events that give better prediction accuracy
  - Fisher scoring
  - sklearn feature_selection RFECV

- Significant processor events (hardware limit: 4)
  - L1-icache-load-misses
  - branch-misses
  - dTLB-load-misses
  - iTLB-load-misses

Events Sampled

- Processor events:
  - L1-icache-load-misses
  - branch-misses
  - dTLB-load-misses
  - iTLB-load-misses
  - Instructions (provided by perf)
- All 8 disk stats
- Network traffic

Machine Learning (ML) Models

- Support vector machine (SVM)
- Random forest (RF)
- K-nearest neighbors (KNN)
- Decision tree (DT)

Analysis Modes

- One event at a time
- Combined: all events together
  - Scales: Min-max, Max-abs, **no-scale**

Features

March 2021

- t samples = 1 instance
- k sub-instances
- Mean, std. dev. and freq-domain counter parts for each sub-instance
- $4k$ features per processor event
- $4kn$ if n events are combined

Features (2)

August 2021

- 100 samples = 1 instance
- Mean, standard deviation for each event
- $2n$ features if n events are combined

- Variations:
  mean, fft
  median, fft
  median, semi-interquartile range

Target Machine States

- No background load
- Background load:
  - web browser
  - video player
  - Microsoft Office documents

Benign Applications

- Secure delete (sDel)
- AES encrypt/decrypt (aesCrypt)
- File compression (7zip)
- None (DryR)

22 Ransomwares (source: virusshare.com)

File Name	Family (MalwareBytes)	Family (Microsoft)
03bb4d5c0179fdceacc5df7645e6e7fa93e931ac9beb1968c7bbe40ba3499194	Ransom.Phobos	Ransom:Win32/Phobos.SW!MSR
0a937d4fe8aa6cb947b95841c490d73e452a3cafcd92645afc353006786aba76	Ransom.LockBit	Ransom:Win32/LockBit.PA!MTB
133bf8be0cf7003b83b03579970997d408a930e58ec2726715140520900c06de	Ransom.Sodinokibi	Ransom:Win32/Revil.SI!MTB
17d153a225ea04a229862875795eeec0adb8c3e2769ba0e05073baaf86850467	Ransom.Sodinokibi	Ransom:Win32/Revil.SI!MTB
3cff33197edc918d47d08f44d6ddbdda157337f0ad58288d15746cf72c0e4c57	Ransom.Sodinokibi	Ransom:Win32/Revil.SI!MTB
3fdad99a17a6766fe396081f82394f5e2da0142651427da64a5b6e28c9df2fd4	Ransom.Sodinokibi	Ransom:Win32/Sodinokibi.C
42c28feb23c992a350673d63413bf11bc816d00a079462ab524934219d46430d	Ransom.Sodinokibi	Ransom:Win32/Sodinokibi.DSB!MTB
4e2554b448424859b508433e6c4a043718343febc7894a849f446dd197b47d1e	Ransom.Maze	Ransom:Win32/Maze.PA!MTB
4f7bdda79e389d6660fca8e2a90a175307a7f615fa7673b10ee820d9300b5c60	Ransom.NetWalker	Ransom:Win32/Filecoder.DD!MTB
57cf4470348e3b5da0fa3152be84a81a5e2ce5d794976387be290f528fa419fd	Ransom.NetWalker	Ransom:Win32/NetWalker!MSR
5cba3e44271279e747a67dd312d4dca18832b5a850ea6b85a460846ef0101fb6	Ransom.Sodinokibi	Undetected
5d9b75e2cb84333c6b56604ce47af75b11f80bf9079054f6619251b68357d87c	Ransom.Sodinokibi	Trojan:Win32/Occamy.C
6628de7ffbbe168a4fa9ff0a1a29b54e88a32e5963db0dd1aea4b80102c8ce01	Ransom.Sodinokibi	Ransom:Win32/Revil.SI!MTB
7c2dbad516d18d2c1c21ecc5792bc232f7b34dadc1bc19e967190d79174131d1	Ransom.DeathRansom	Undetected
7d98972d5c78e1d4969da76856d6818942b606c267efa67fd31d39ae77497e9c	Ransom.Rapid	Ransom:Win32/Robinhood.AR!MTB
7faeb64c50cd15d036ca259a047d6c62ed491fff3729433fefba0b02c059d5ed	Ransom.Ryuk	Ransom:Win32/Sodinokibi.AD!MTB
81689f1be92c8fb7e94fe241441c7eb43cfb77c6d23592b0248566bd709ff2ed	---	Ransom:Win32/Revil.SI!MTB
d6b7b27e13700aaa7f108bf9e76473717a7a1665198e9aafcc2d2227ca11bba9	Ransom.Ryuk	Ransom:Win32/Ruyk.A!ibt
e8a091a84dd2ea7ee429135ff48e9f48f7787637ccb79f6c3eb42f34588bc684	Malware.AI.4262356839	Ransom:Win32/Maze
ecfb5c95d0f3d112650ef4047936e8fa5244c21c921f6c7a6963e92abab4949d	Ransom.FileCryptor	Ransom:MSIL/Kelnoc.A
f2c9ae3735430b930a81148c0bb470fcb733e456a2a942f859a1b59c4a7b2150	Malware.AI.2057448532	Ransom:Win32/Locky.A
fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44	Ransom.Povlsomware	Ransom:MSIL/RnToad.SL!MTB

Benign App Experiments

- Each benign app
  - 65 rounds without background load
  - 65 rounds with background load
  - Each round: 60,000 samples of 5 hardware counter events

$$65 \times 2 \times 4 = 520 \quad \text{rounds}$$

Ransomware Experiments

- Each ransomware (RW)
  - 25 rounds without background load
  - 25 rounds with background load
  - Each round: 60,000 samples of 5 hardware counter events

$$25 \times 2 \times 22 = 1100 \text{ rounds}$$

Analysis

- Benign: 500 rounds out of 520 at random
- RW: 500 rounds out of 1100 at random

- 30,000 samples per round
- 200 samples/instance
- 80:20 training-testing split

- Random forest model
- 51 repetitions

Case I: Train with 11 RW, Test with 11 other RW

03bb4d5c0179fdceacc5df7645e6e7fa93e931ac9beb1968c7bbe40ba3499194	Ransom.Phobos
0a937d4fe8aa6cb947b95841c490d73e452a3cafcd92645afc353006786aba76	Ransom.LockBit
133bf8be0cf7003b83b03579970997d408a930e58ec2726715140520900c06de	Ransom.Sodinokibi
17d153a225ea04a229862875795eeec0adb8c3e2769ba0e05073baaf86850467	
3cff33197edc918d47d08f44d6ddbdda157337f0ad58288d15746cf72c0e4c57	
3fdad99a17a6766fe396081f82394f5e2da0142651427da64a5b6e28c9df2fd4	
42c28feb23c992a350673d63413bf11bc816d00a079462ab524934219d46430d	
5cba3e44271279e747a67dd312d4dca18832b5a850ea6b85a460846ef0101fb6	
5d9b75e2cb84333c6b56604ce47af75b11f80bf9079054f6619251b68357d87c	
6628de7ffbbe168a4fa9ff0a1a29b54e88a32e5963db0dd1aea4b80102c8ce01	
4e2554b448424859b508433e6c4a043718343febc7894a849f446dd197b47d1e	Ransom.Maze
4f7bdda79e389d6660fca8e2a90a175307a7f615fa7673b10ee820d9300b5c60	Ransom.NetWalker
57cf4470348e3b5da0fa3152be84a81a5e2ce5d794976387be290f528fa419fd	
7c2dbad516d18d2c1c21ecc5792bc232f7b34dadc1bc19e967190d79174131d1	Ransom.DeathRansom
7d98972d5c78e1d4969da76856d6818942b606c267efa67fd31d39ae77497e9c	Ransom.Rapid
7faeb64c50cd15d036ca259a047d6c62ed491fff3729433fe1ba0b02c059d5ed	Ransom.Ryuk
d6b7b27e13700aaa7f108bf9e76473717a7a1665198e9aafcc2d2227ca11bba9	
e8a091a84dd2ea7ee429135ff48e9f48f7787637ccb79f6c3eb42f34588bc684	Malware.AI.4262356839
f2c9ae3735430b930a81148c0bb470fcb733e456a2a942f859a1b59c4a7b2150	Malware.AI.2057448532
ecfb5c95d0f3d112650ef4047936e8fa5244c21c921f6c7a6963e92abab4949d	Ransom.FileCryptor
fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44	Ransom.Povlsomware
81689f1be92c8fb7e94fe241441c7eb43cfb77c6d23592b0248566bd709ff2ed	---

Case II: Train and Test all 22 RW

File Name	Family (MalwareBytes)
03bb4d5c0179fdceacc5df7645e6e7fa93e931ac9beb1968c7bbe40ba3499194	Ransom.Phobos
0a937d4fe8aa6cb947b95841c490d73e452a3cafcd92645afc353006786aba76	Ransom.LockBit
133bf8be0cf7003b83b03579970997d408a930e58ec2726715140520900c06de	Ransom.Sodinokibi
17d153a225ea04a229862875795eeec0adb8c3e2769ba0e05073baaf86850467	Ransom.Sodinokibi
3cff33197edc918d47d08f44d6ddbdda157337f0ad58288d15746cf72c0e4c57	Ransom.Sodinokibi
3fdad99a17a6766fe396081f82394f5e2da0142651427da64a5b6e28c9df2fd4	Ransom.Sodinokibi
42c28feb23c992a350673d63413bf11bc816d00a079462ab524934219d46430d	Ransom.Sodinokibi
4e2554b448424859b508433e6c4a043718343febc7894a849f446dd197b47d1e	Ransom.Maze
4f7bdda79e389d6660fca8e2a90a175307a7f615fa7673b10ee820d9300b5c60	Ransom.NetWalker
57cf4470348e3b5da0fa3152be84a81a5e2ce5d794976387be290f528fa419fd	Ransom.NetWalker
5cba3e44271279e747a67dd312d4dca18832b5a850ea6b85a460846ef0101fb6	Ransom.Sodinokibi
5d9b75e2cb84333c6b56604ce47af75b11f80bf9079054f6619251b68357d87c	Ransom.Sodinokibi
6628de7ffbbe168a4fa9ff0a1a29b54e88a32e5963db0dd1aea4b80102c8ce01	Ransom.Sodinokibi
7c2dbad516d18d2c1c21ecc5792bc232f7b34dadc1bc19e967190d79174131d1	Ransom.DeathRansom
7d98972d5c78e1d4969da76856d6818942b606c267efa67fd31d39ae77497e9c	Ransom.Rapid
7faeb64c50cd15d036ca259a047d6c62ed491fff3729433fefba0b02c059d5ed	Ransom.Ryuk
81689f1be92c8fb7e94fe241441c7eb43cfb77c6d23592b0248566bd709ff2ed	---
d6b7b27e13700aaa7f108bf9e76473717a7a1665198e9aafcc2d2227ca11bba9	Ransom.Ryuk
e8a091a84dd2ea7ee429135ff48e9f48f7787637ccb79f6c3eb42f34588bc684	Malware.AI.4262356839
ecfb5c95d0f3d112650ef4047936e8fa5244c21c921f6c7a6963e92abab4949d	Ransom.FileCryptor
f2c9ae3735430b930a81148c0bb470fcb733e456a2a942f859a1b59c4a7b2150	Malware.AI.2057448532
fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44	Ransom.Povlsomware

Case I Results: Average of 51 Repetitions

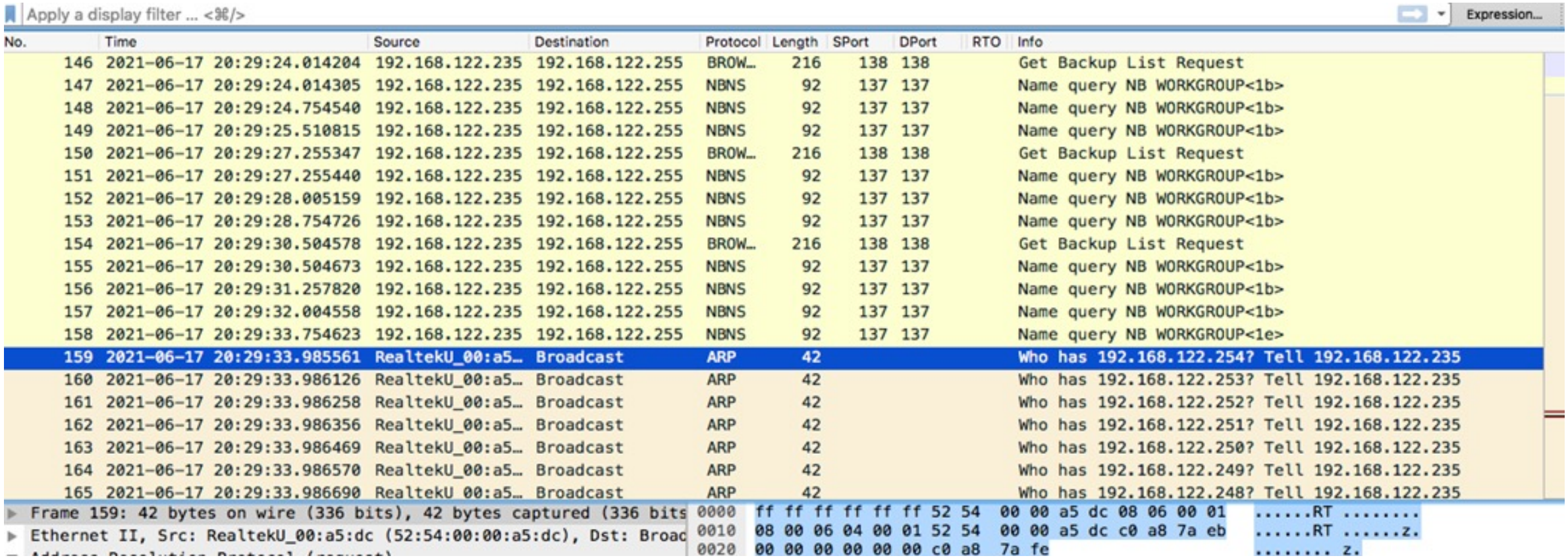
	Acc	fpr	fnr
L1-icache-load-misses	0.729392	0.203824	0.337412
branch-misses	0.704353	0.241176	0.350098
dTLB-load-misses	0.703235	0.247961	0.345608
iTLB-load-misses	0.754373	0.198157	0.293216
instructions	0.721529	0.180588	0.376314
combined-noscale	0.875784	0.0292157	0.219235

Case II Results: Average of 51 Repetitions

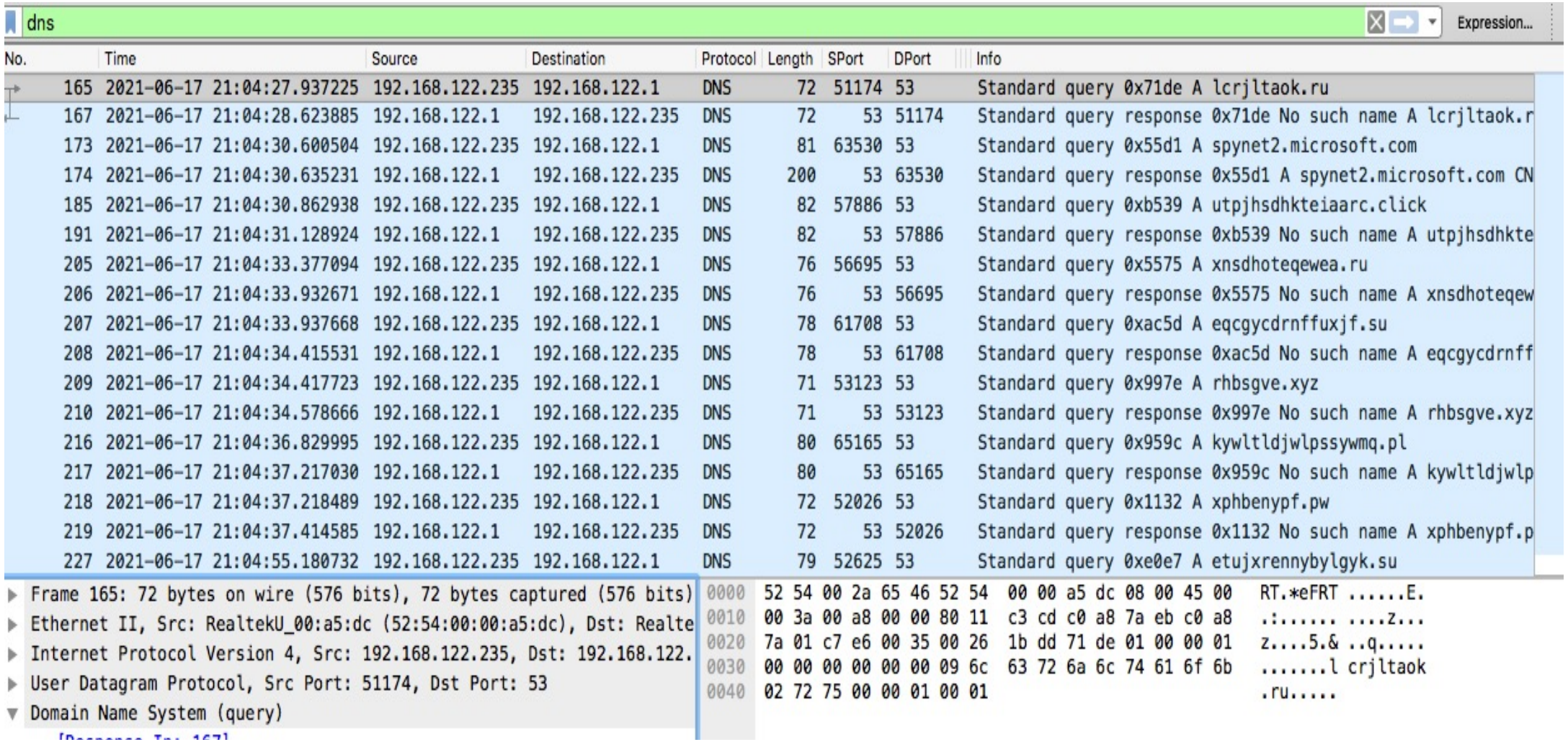
	Acc	fpr	fnr
L1-icache-load-misses	0.757627	0.228137	0.256569
branch-misses	0.748294	0.255392	0.24798
dTLB-load-misses	0.727549	0.263412	0.281392
iTLB-load-misses	0.774824	0.212686	0.237569
instructions	0.783627	0.207235	0.225529
combined-noscale	0.946431	0.043098	0.0638824

Network Traffic Analysis

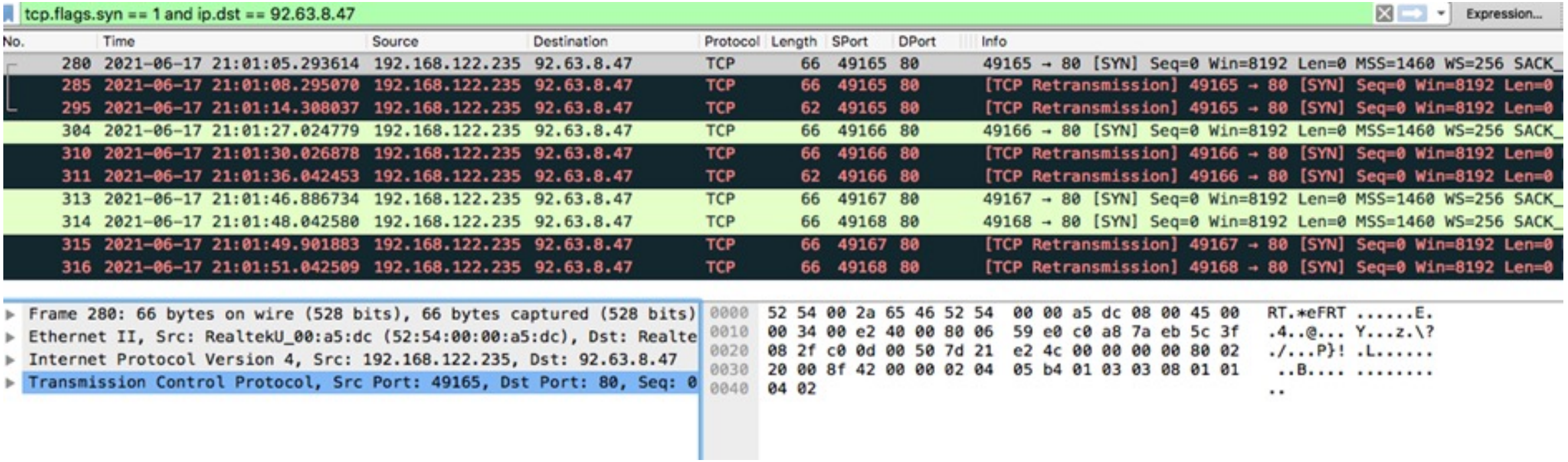
Network Traffic: SMB, NBNS, ARP Activity



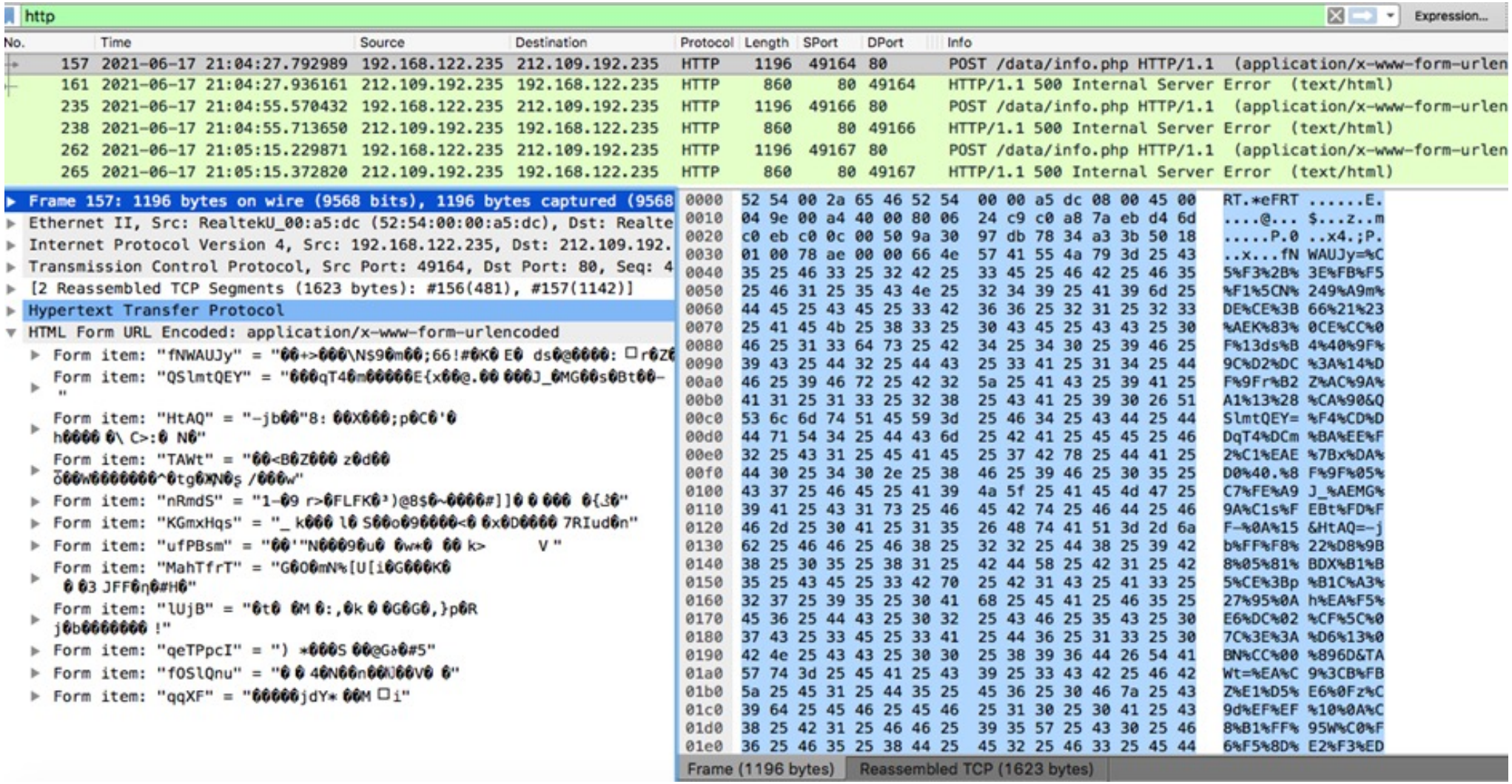
Network Traffic: DNS Queries for Odd Domain Names



Network Traffic: Spurious SYNs



Network Traffic: HTTP Posts with Error Response



Network Traffic

- No suspicious activity by some ransomwares

Category	Ransomwares
SMB Traffic; NBNS Traffic	0a93,03bb,3cff,3fda,4e25,5cba,5d9b,7c2d, 7fae, 17dl, 42c2, 133b, 6628, e8a0, F2c9
SMB and/or NBNS along with ARP	0a93, 7fae
DNS Traffic	F2c9,
HTTP Traffic	F2c9
Spurious SYNs	E8a0, 4e25
Other (DHCP) (May or may not be suspicious)	03bb, 4e25, 4f7b, 7c2d, 7d98, 57cf, 8168, e8a0, ecfb, f2c9, fd32
No suspicious activity	d6b7

Analyzed by Vasudha Vedula, Doctoral Student, UTSA

RATAFIA: Ransomware Analysis using Time And Frequency Informed Autoencoders [IEEE HOST, 2019]

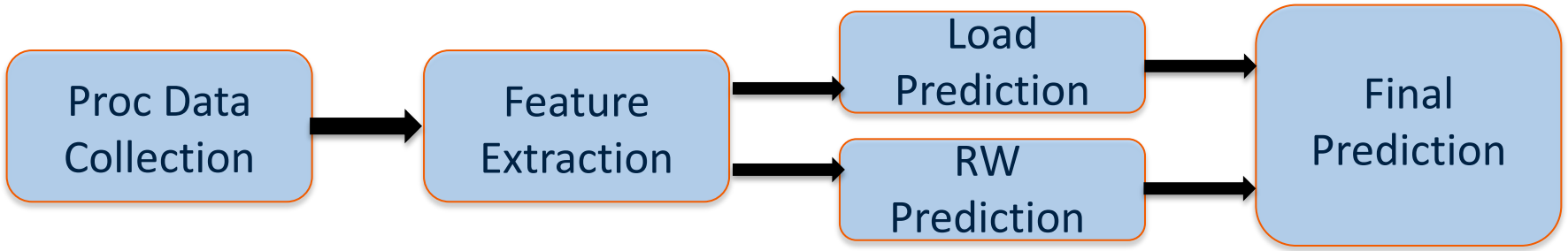
- *perf* to collect processor events
  - 10 ms sampling interval
  - 4-5 ransomwares without loads
- LSTM-based autoencoder
- Detection time: 1 second or more

RanStop: A Hardware-assisted Runtime Crypto-Ransomware Detection Technique [arXiv, 2020]

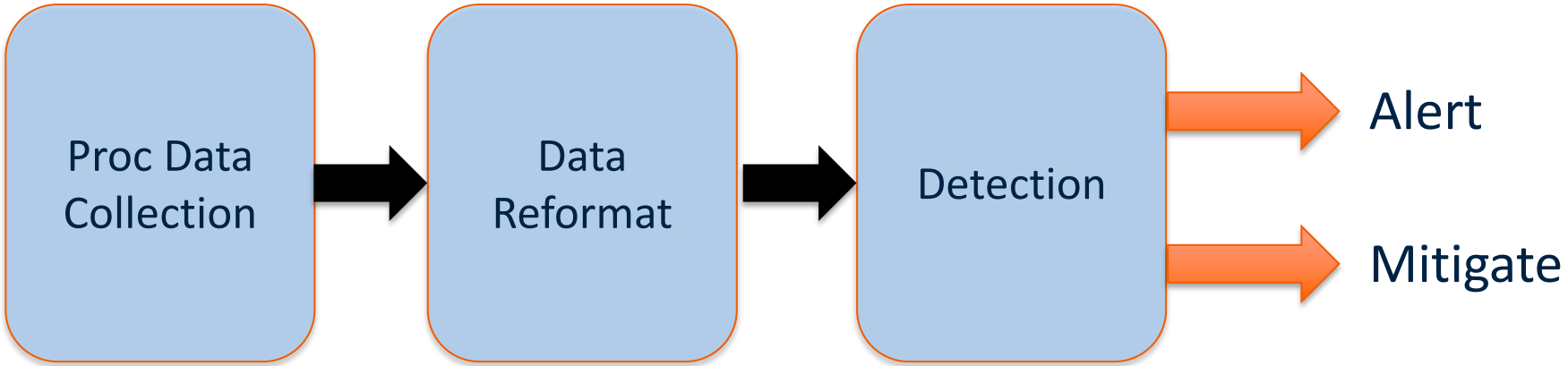
- *likwid* tool to collect processor events
  - 100µs sampling interval
  - Sampled first 2 ms only
  - No load case only
- LSTM model
- Detection time is 2 ms
- Ransomware with delayed action are not detected

Ongoing Work: Fine-tuning FPR and FNR

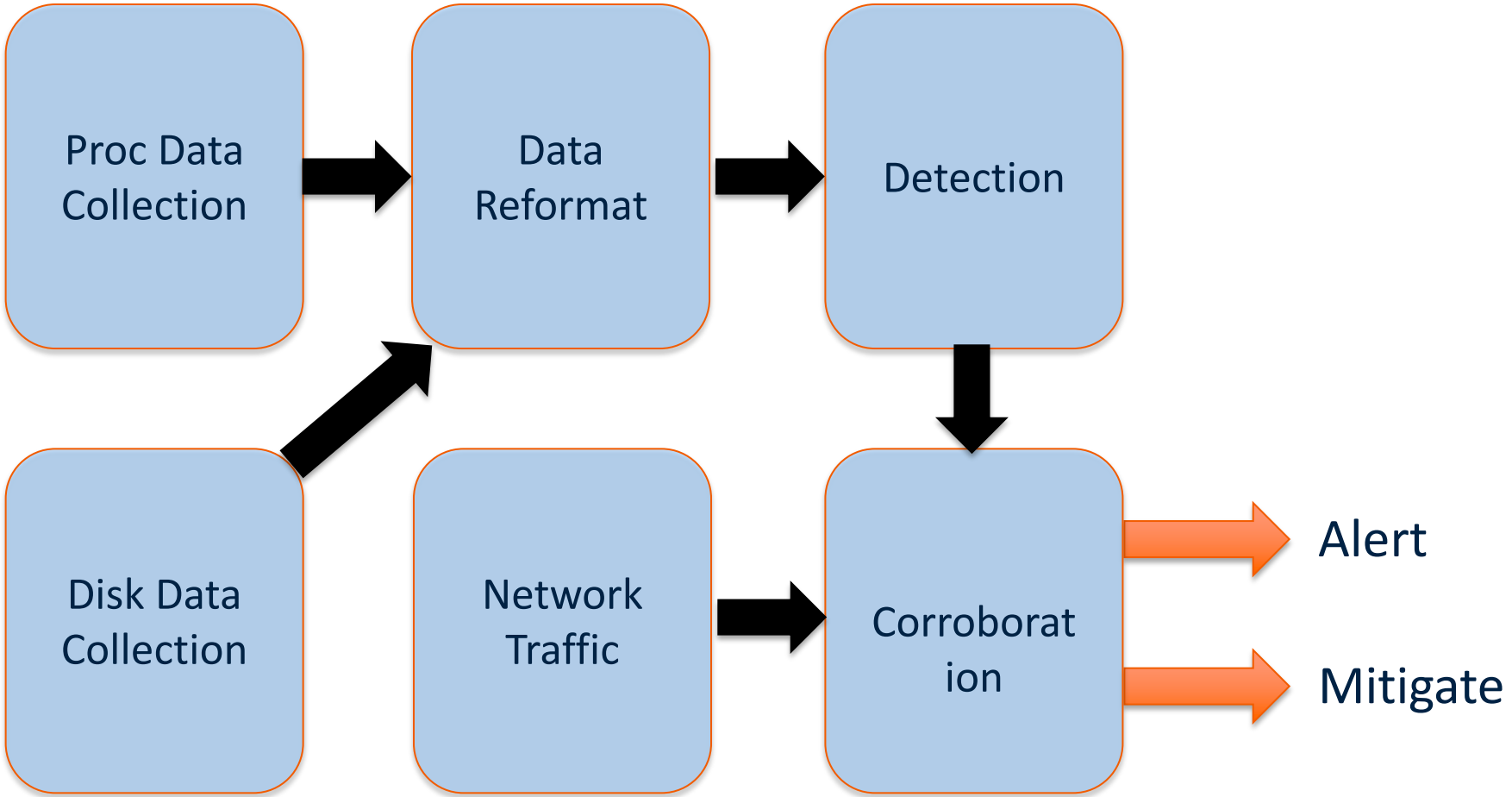
- Different probability thresholds for positive and negative predictions



Ongoing Work: Live Detection



Combine with Disk and Network Traffic Analysis



Questions?

Rajendra.Boppana@utsa.edu