tripwire®

CONFIDENCE: SECURED

Sweet Security Supercharged

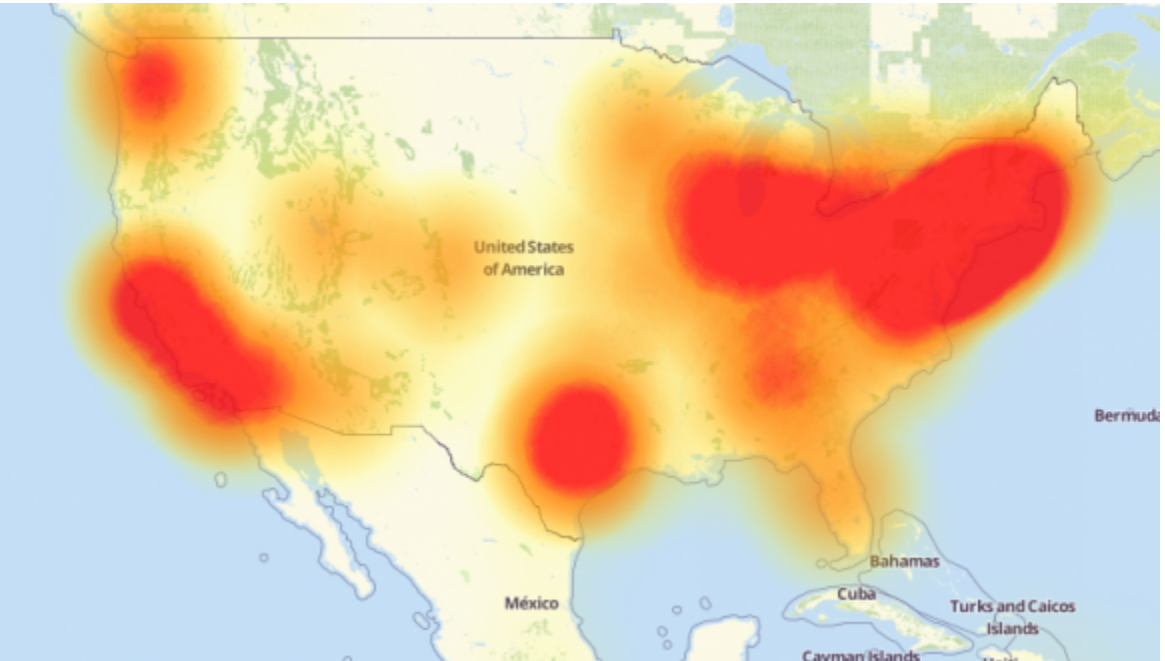
Deploying a Defensive Raspberry Pi (And Beyond)

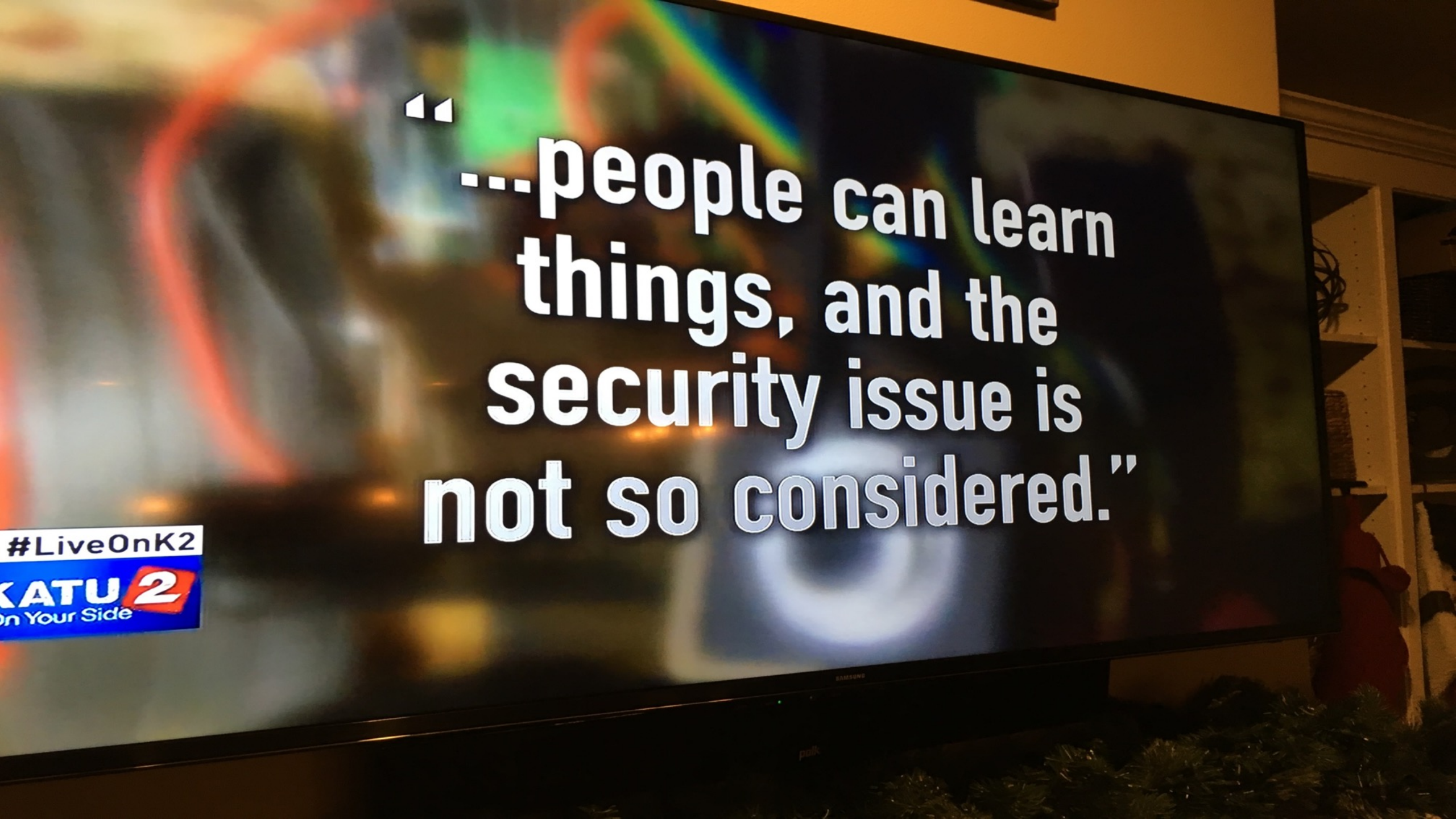
PROTECT THE UNPATCHABLE

The Problem


CENTRAL INTELLIGENCE AGENCY
INFORMATION OPERATIONS CENTER
KNOWLEDGE
STEALTH
INNOVATION


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

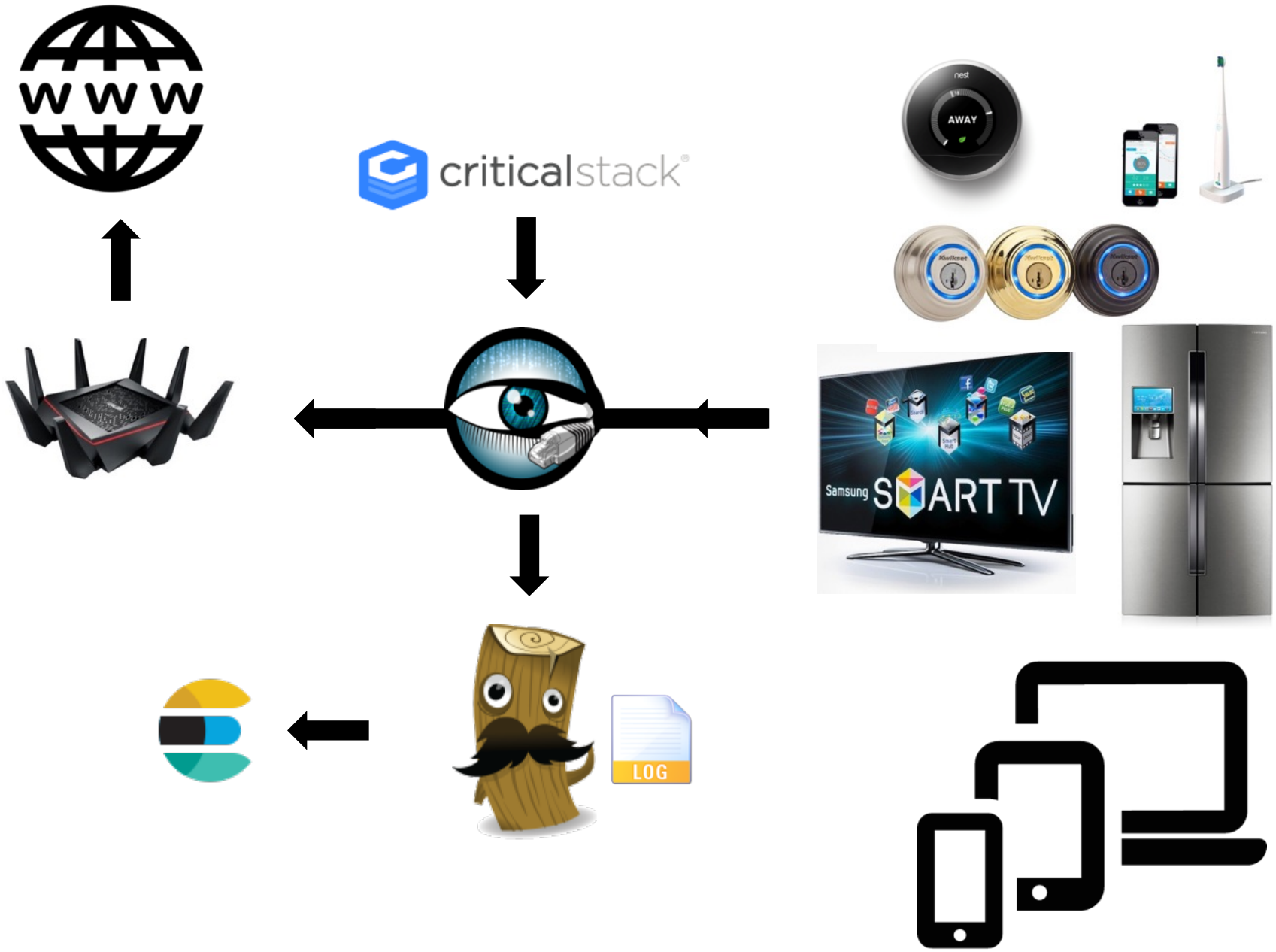

United States of America
Bermuda
Bahamas
Cuba
México
Turks and Caicos Islands
Cayman Islands


"...people can learn things, and the security issue is not so considered."
#LiveOnK2
KATU 2
On Your Side

Securing Your Home

Beginner	Advanced*
Change Default Passwords	Upgrade Firmware
Change Default SSID	Disable Remote Management
Logout of Router	Turn Off Network
Use WPA2	Limit WLAN Signal Emissions
	Monitor for Unknown Devices
	Disable WPS
	Disable UPnP

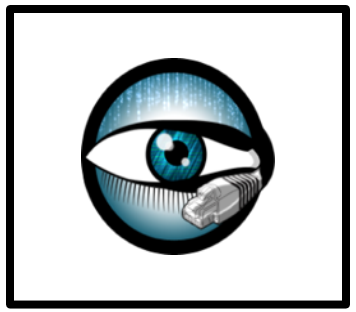
https://www.us-cert.gov/ncas/tips/ST15-002


www
criticalstack
nest
AWAY
Samsung SMART TV
LOG

Web
Install

Full
Install

Sweet Security



Sensor
Install

Web Install

Full Install

Sensor

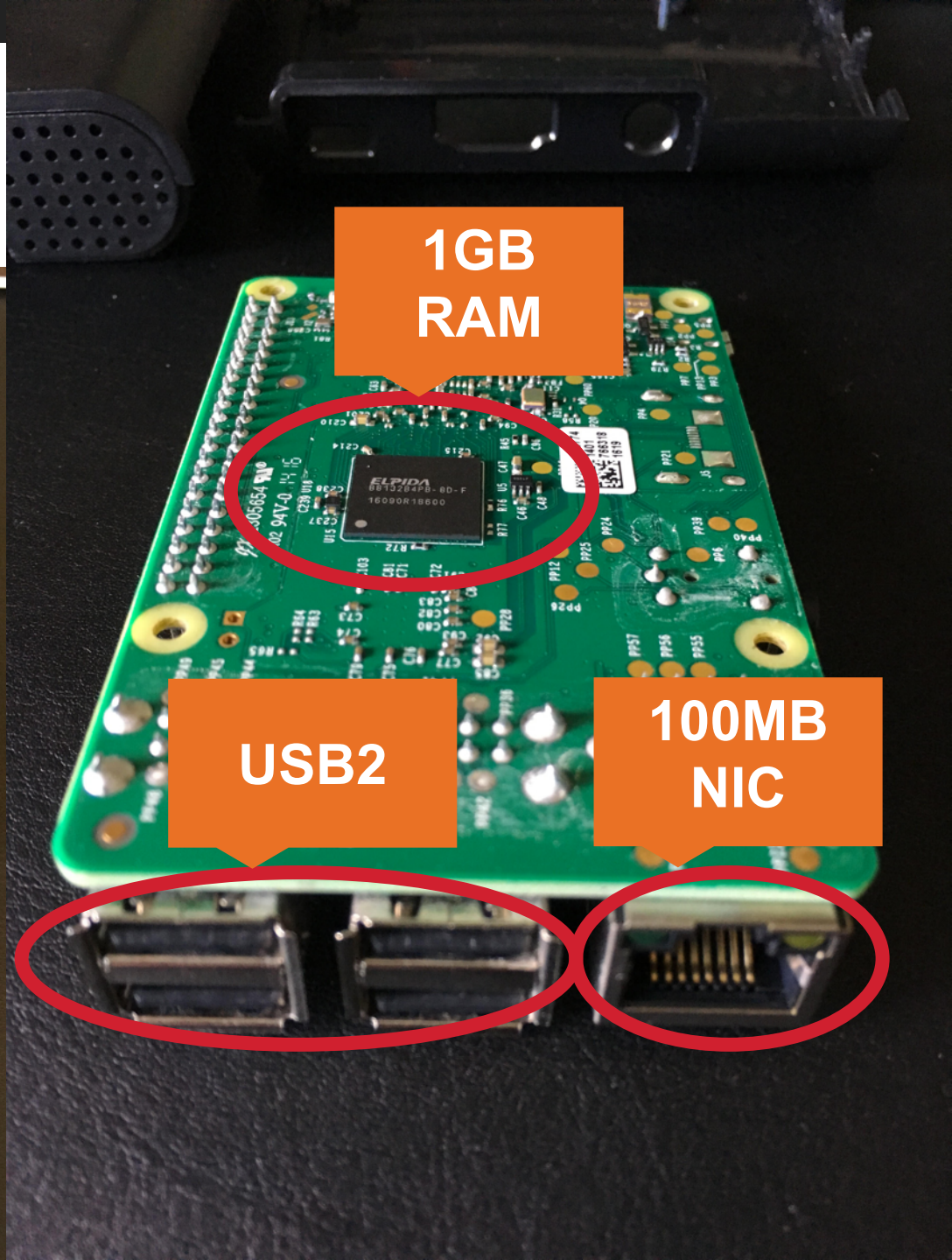
Sensor

Sensor

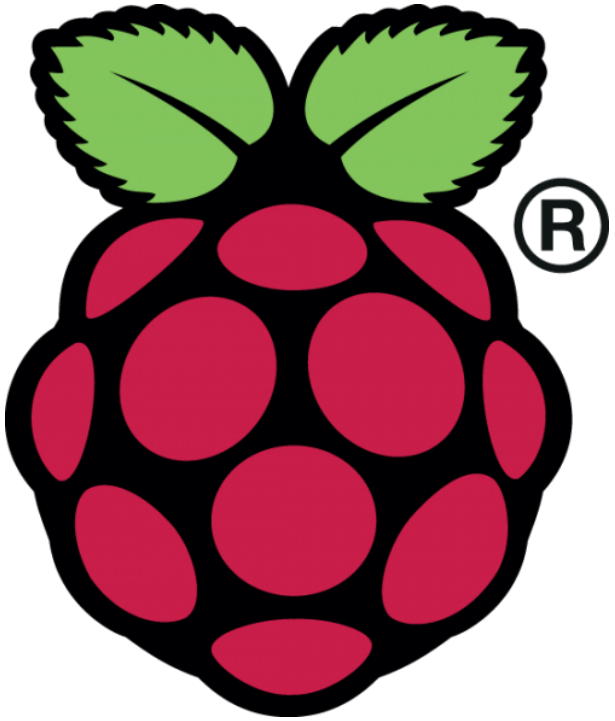
Sensor

Sensor Install

The Pi Problem



Bandwidth Data



Without SweetSecurity

223.22 Mbps	11.85 Mbps	10.6 ms
Download	Upload	Ping

With SweetSecurity

83.47 Mbps	12.16 Mbps	10.8 ms
Download	Upload	Ping

Raspberry Pi w/ USB Gigabit NIC

21.14 Mbps

Download

12.19 Mbps

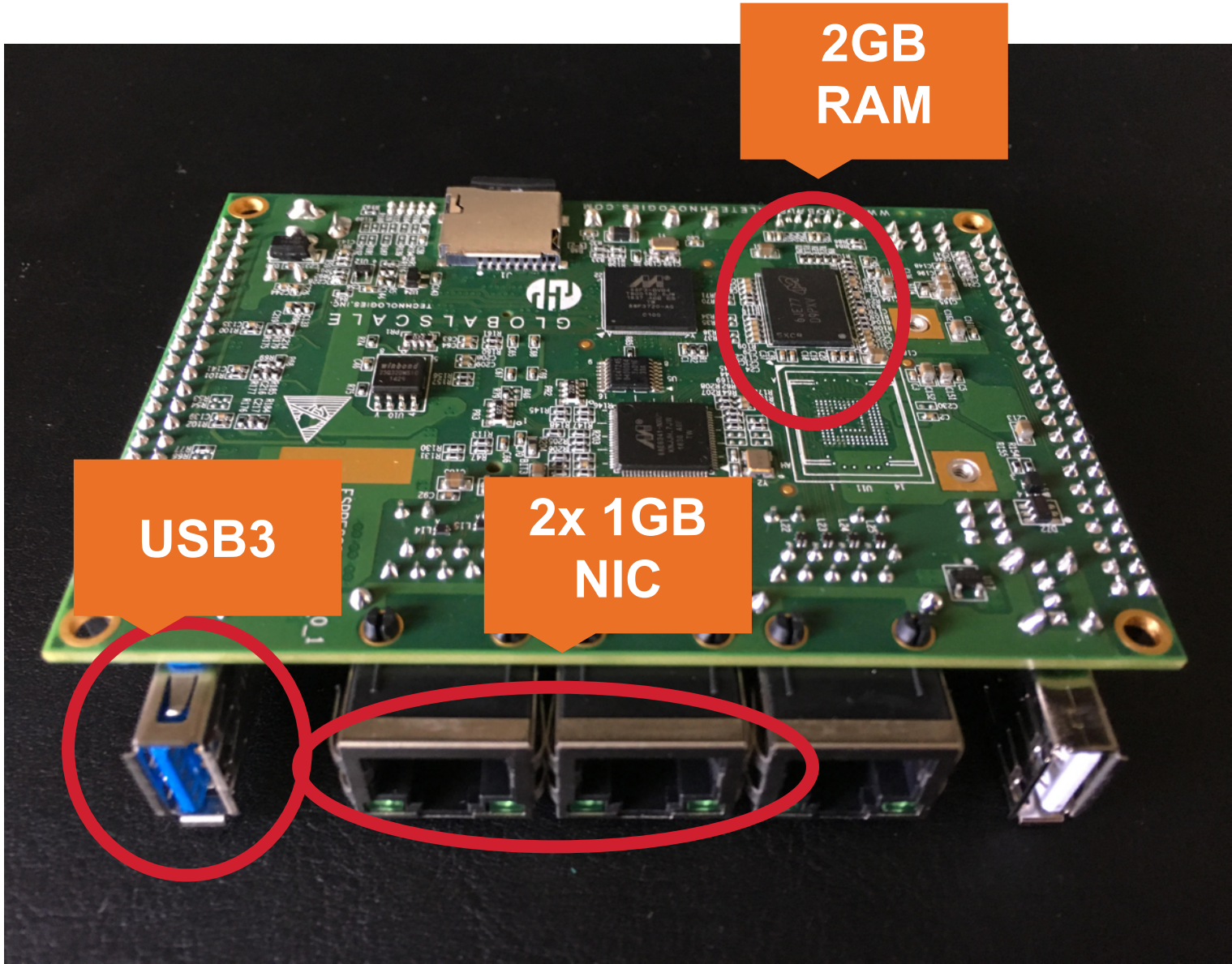
Upload

11.8ms

Ping

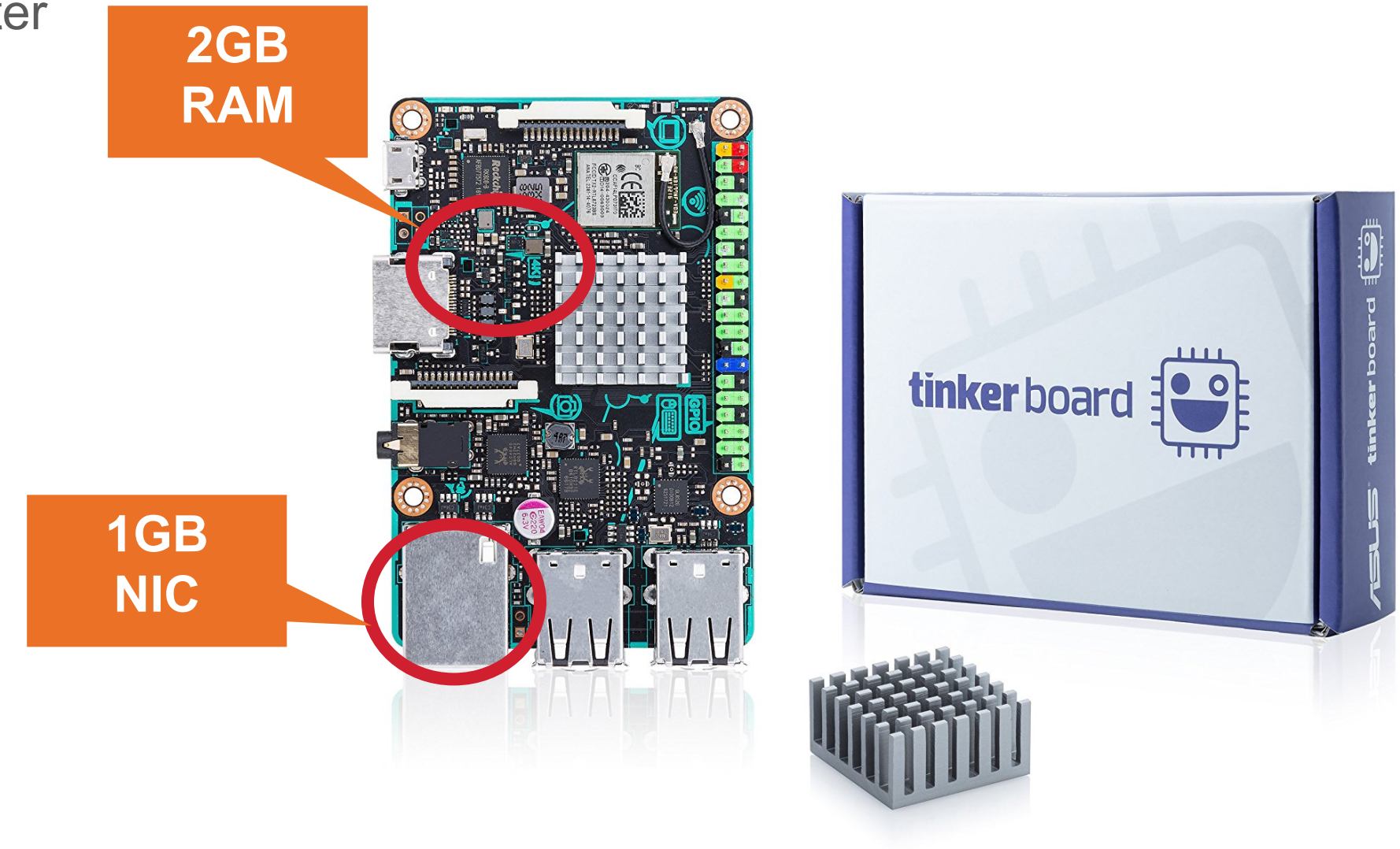
EspressoBIN

- Single Board Computer
- Kickstarter Campaign
- $49 (1GB)
- ~$79 (2GB)
- SATA Connection
- *Issues with Architecture



TinkerBoard

- Single Board Computer
- $59
- Quad Code CPU
- 2GB DDR3 RAM
- 1GB NIC
- *TinkerOS?
- *Armbian?



Intel NUC

Intel® NUC Board NUC5i5MYBE

- Intel® Core™ i5-5300U Processor (3M Cache, up to 2.90 GHz) Processor Included
- M.2 and 2.5" Drive Internal Drive Form Factor
- 2x mDP, 1x eDP Graphics Output

Add to Compare

From $513.04

Intel® NUC Board NUC5i3MYBE

- Intel® Core™ i3-5010U Processor (3M Cache, 2.10 GHz) Processor Included
- M.2 and 2.5" Drive Internal Drive Form Factor
- 2x mDP, 1x eDP Graphics Output

Add to Compare

From $350.00

Intel® NUC Board DE3815TYBE

- Intel Atom® Processor E3815 (512K Cache, 1.46 GHz) Processor Included
- 2.5" Drive Internal Drive Form Factor
- HDMI, VGA Header, eDP Graphics Output

Add to Compare

From $124.00

Old Computers?

- Code is CPU architecture agnostic
  - ARM
  - x86
  - x86_64

Bandwidth Data

Without SweetSecurity

230.02 Mbps Download

12.18 Mbps Upload

11.6 ms Ping

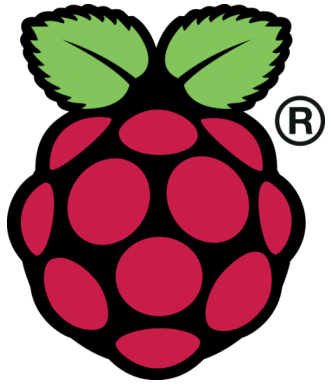
With SweetSecurity

230.21 Mbps Download

12.23 Mbps Upload

12.2 ms Ping

Bandwidth Data



Raspberry Pi 3

83.47 Mbps Download

12.16 Mbps Upload

10.8 ms Ping

Dell Server (1gb NIC)

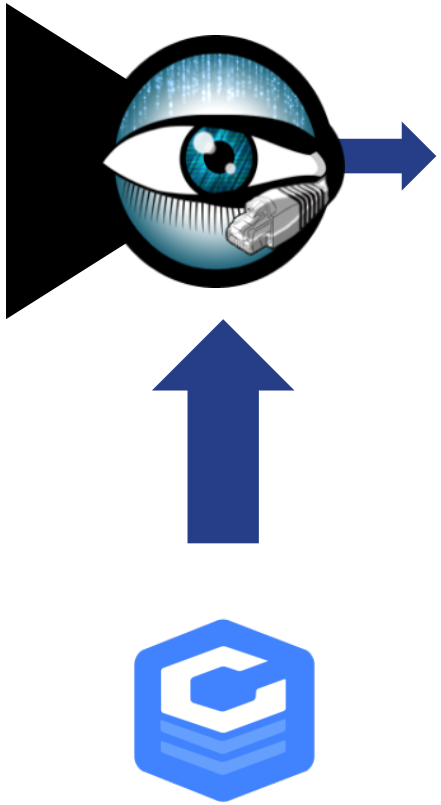
230.21 Mbps Download

12.23 Mbps Upload

12.2 ms Ping

Full Packet Capture

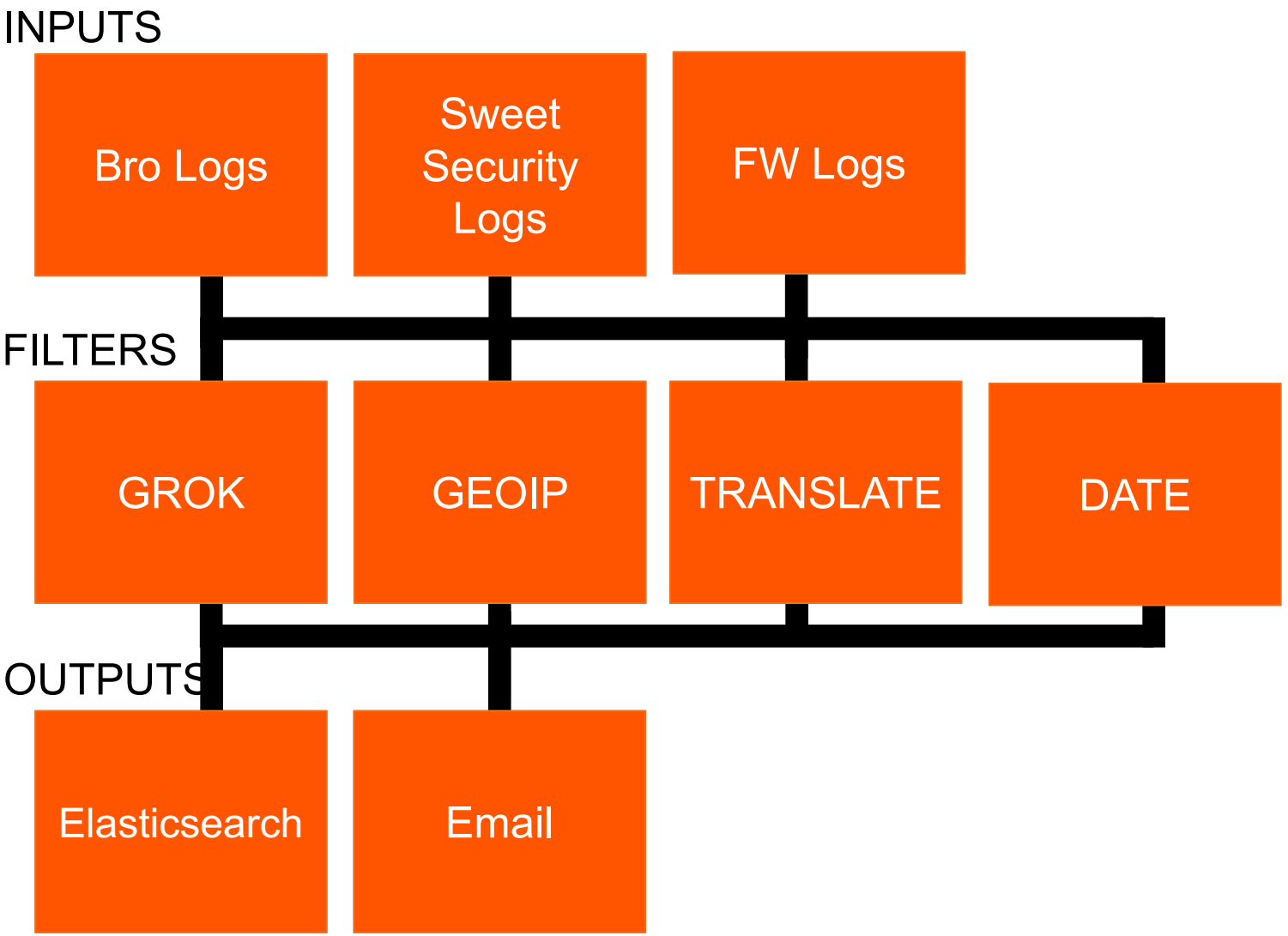
```
73 65 72 20 72 6F 6F 74 20 62 79 20 28 75 69 64 ser root by (uid
3D 30 29 89 70 94 50 E4 ED 0A 00 99 00 00 00 99 =0).p.P.........
00 00 00 52 54 00 DA 2C 4C 52 54 00 DA 98 99 08 ...RT..,LRT.....
00 45 00 00 8B 00 00 40 00 40 11 43 37          .E.....@.@.C7...
               A4 DF 02 02 00 77 79 82 3C 37 38 ,.........wy.<78
3E 4E 6F 76 20 20 33 20 31 32 3A 31 37 3A 30 31 >Nov  3 12:17:01
20 64 61 74 61 62 61 73 65 20 2F 55 53 52 2F 53  database /USR/S
42 49 4E 2F 43 52 4F 4E 5B 31 38 31 33 35 5D 3A BIN/CRON[18135]:
20 28 72 6F 6F 74 29 20 43 4D 44 20 28 20 20 20  (root) CMD (
63 64 20 2F 20 26 26 20 72 75 6E 2D 70 61 72 74 cd / && run-part
73 20 2D 2D 72 65 70 6F 72 74 20 2F 65 74 63 2F s --report /etc/
63 72 6F 6E 2E 68 6F 75 72 6C 79 29 89 70 94 50 cron.hourly).p.P
13 04 0B 00 88 00 00 00 88 00 00 00 52 54 00 DA ............RT..
2C 4C 52 54 00 DA 98 99 08 00 45 00 00 7A 00 00 ,LRT......E..z..
40 00 40 11 43 48                   A4 DF @.@.CH.....
02 02 00 66 AD DD 3C 38 36 3E 4E 6F 76 20 20 33 ...f..<86>Nov  3
20 31 32 3A 31 37 3A 30 31 20 64 61 74 61 62 61  12:17:01 databa
73 65 20 43 52 4F 4E 5B 31 38 31 33 34 5D 3A 20 se CRON[18134]:
70 61 6D 5F 75 6E 69 78 28 63 72 6F 6E 3A 73 65 pam_unix(cron:se
73 73 69 6F 6E 29 3A 20 73 65 73 73 69 6F 6E 20 ssion): session
63 6C 6F 73 65 64 20 66 6F 72 20 75 73 65 72 20 closed for user
72 6F 6F 74 42 71 94 50 62 6E 05 00 3C 00 00 00 rootBq.Pbn..<...
3C 00 00 00 52 54 00 0D 5E C5 52 54 00 DA 2C 4C <...RT..^.RT..,L
08 06 00 01 08 00 06 04 00 01 52 54 00 DA 2C 4C ..........RT..,L
               00 00 00 00 00 00    00 00 ..............+..
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```



Network Traffic Metadata

conn.log
dhcp.log
dns.log
ftp.log
http.log
irc.log
known_services.log
smtp.log
snmp.log
ssh.log
ssl.log
syslog.log
tunnel.log
intel.log
notice.log

The Details

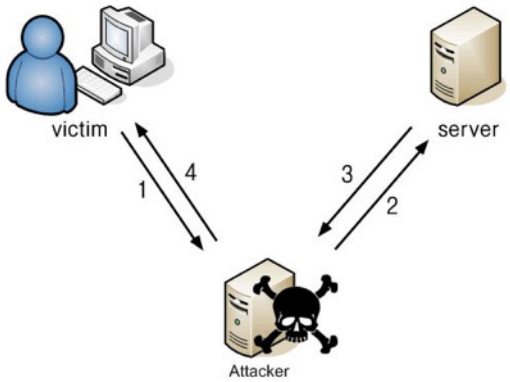

INPUTS
Bro Logs
Sweet Security Logs
FW Logs
FILTERS
GROK
GEOIP
TRANSLATE
DATE
OUTPUTS
Elasticsearch
Email

0:20

nmap -sn 192.168.1.1/24 -e eth0

SweetSecurity.db

0:01



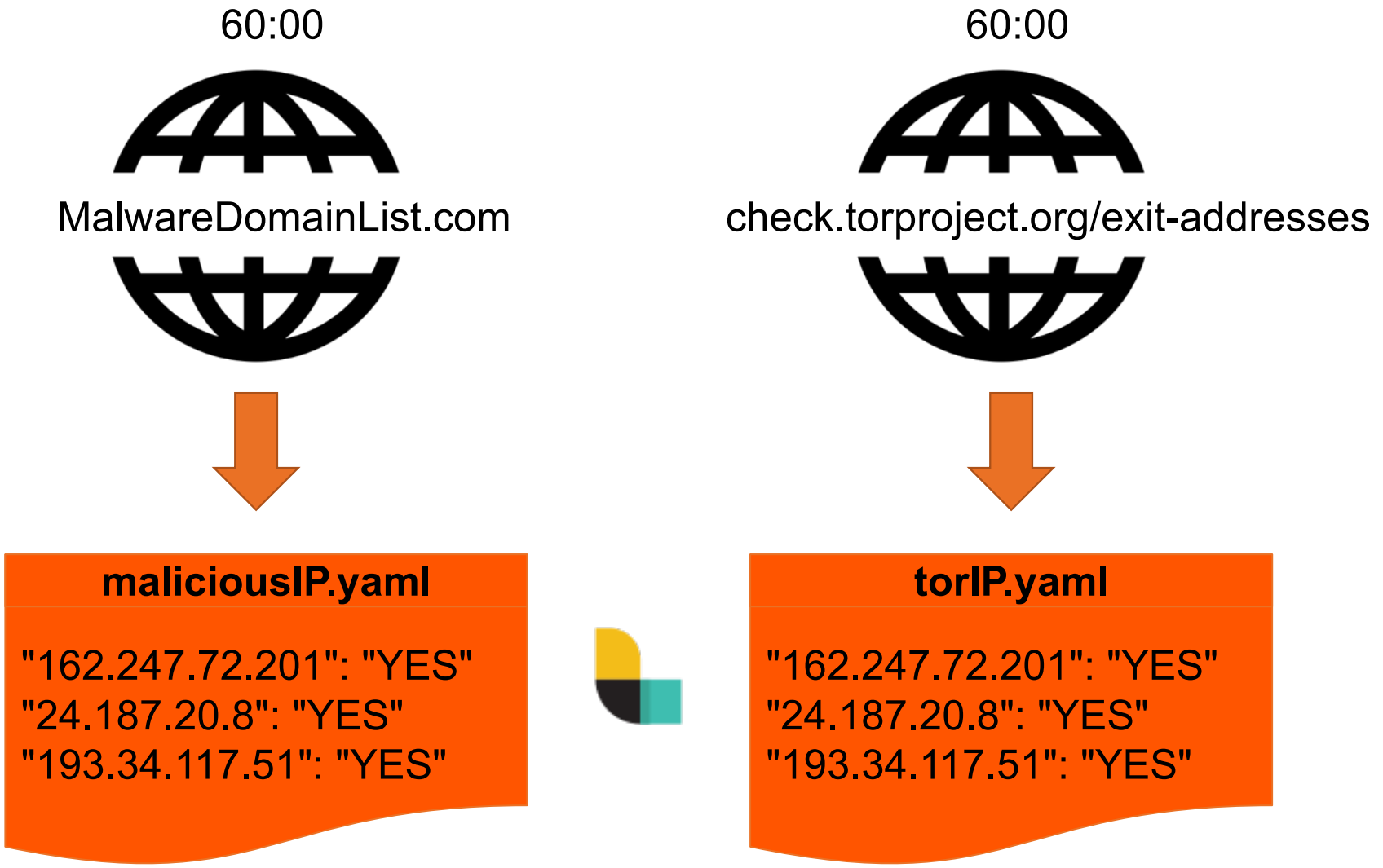
IF ignore==0 **AND** active==1

60:00

nmap -sV 192.168.1.2

hostname	nickname	ip4	mac	vendor	ignore	active
iPhone.lan	iPhone	192.168.1.2	00:11:22:33:44:55	Apple	0	0
therm.lan	**Thermostat**	**192.168.1.3**	**aa:bb:cc:dd:ee:ff**	**Google**	**0**	**1**
mac.lan	Macbook	192.168.1.4	01:23:45:67:89:0a	Apple	1	1
tstr9412.lan	**Toaster**	**192.168.1.5**	**ab:cd:ef:12:34:56**	**KitchenAid**	**0**	**1**

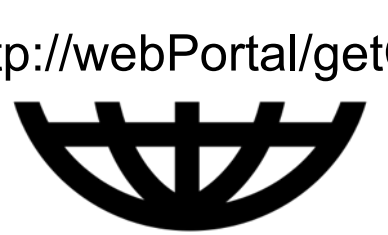
Logstash IOC Matching



Sensor Management / Health

00:05

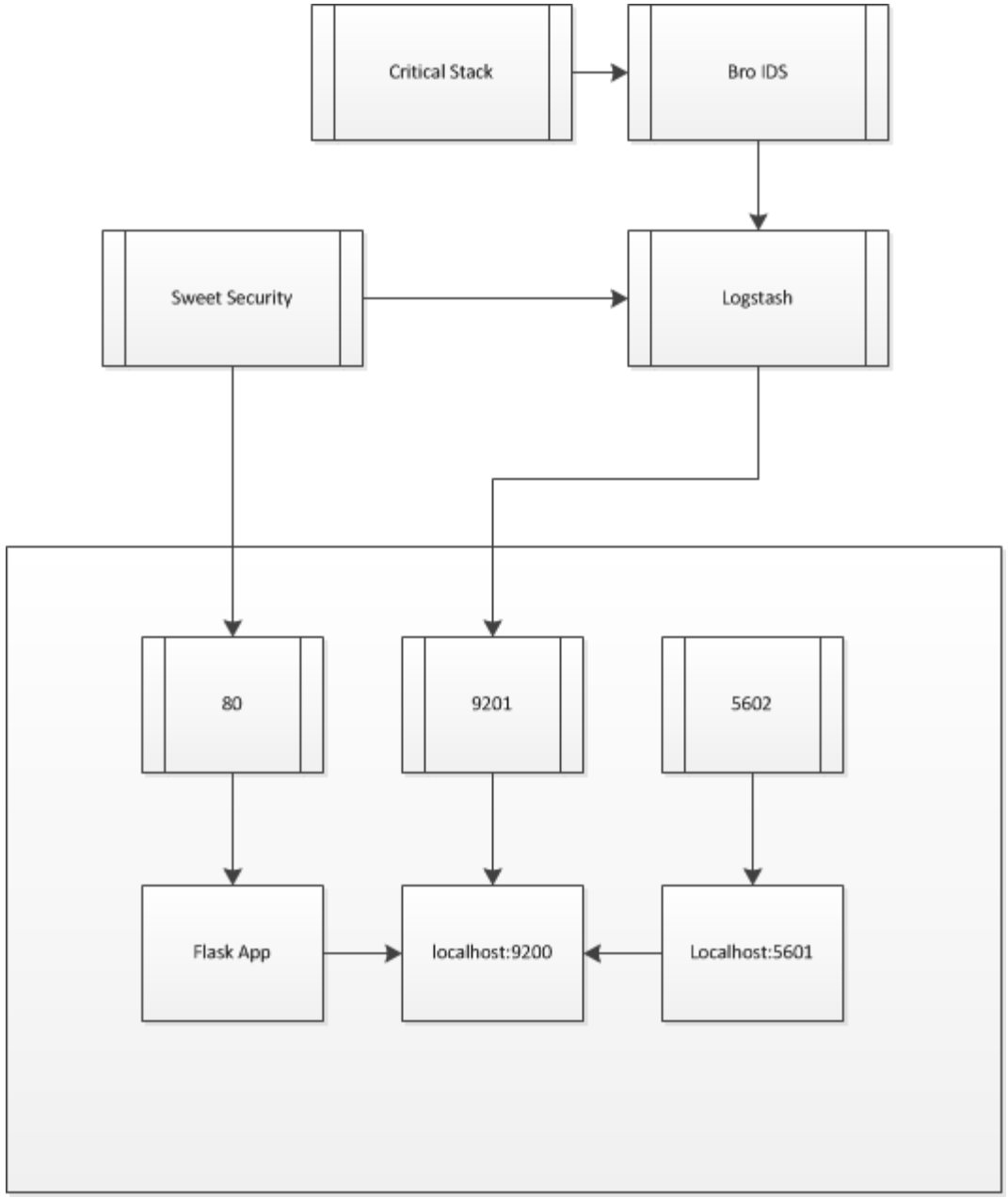
http://webPortal/getConfig



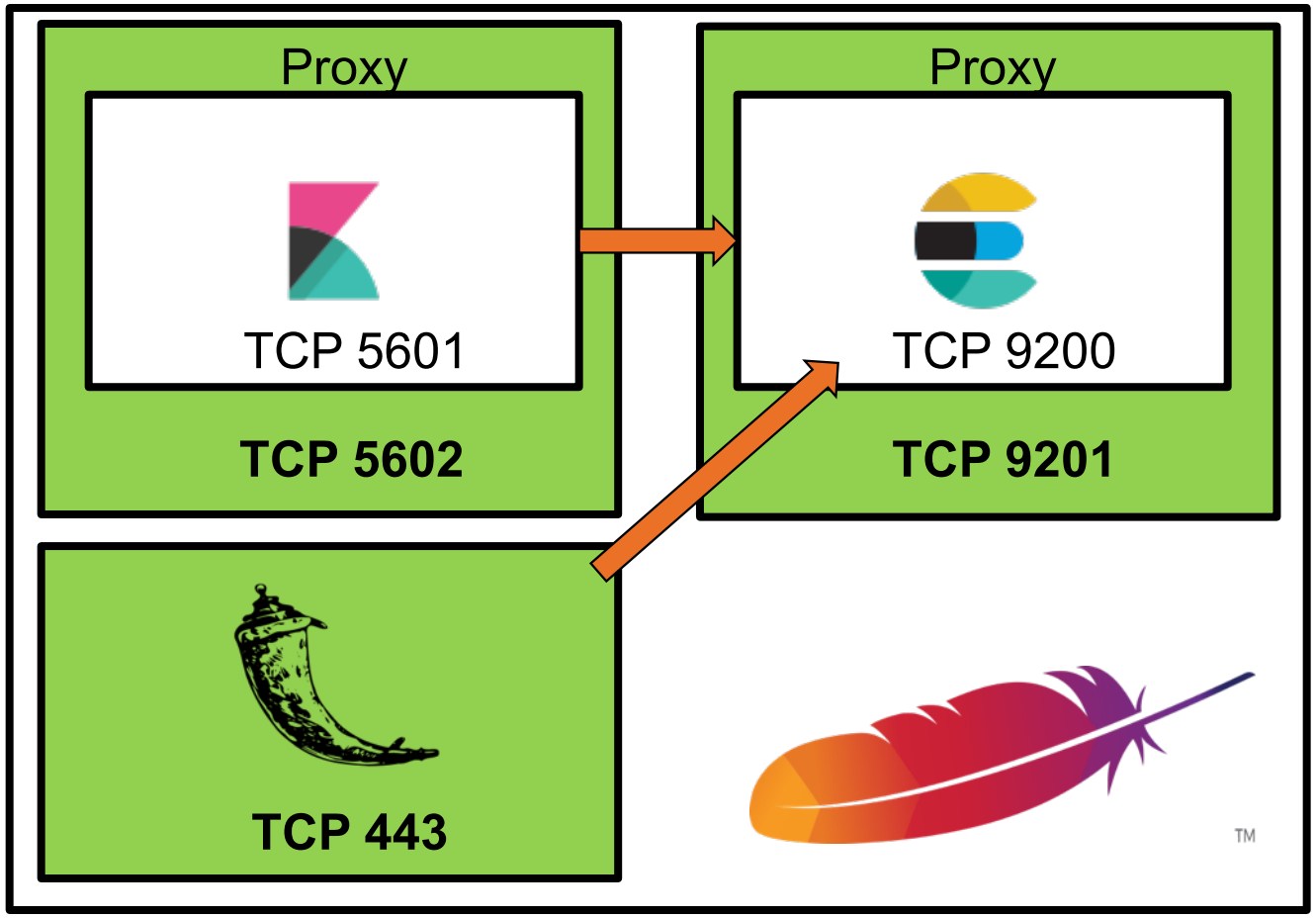
05:00

http://webPortal/healthCheck

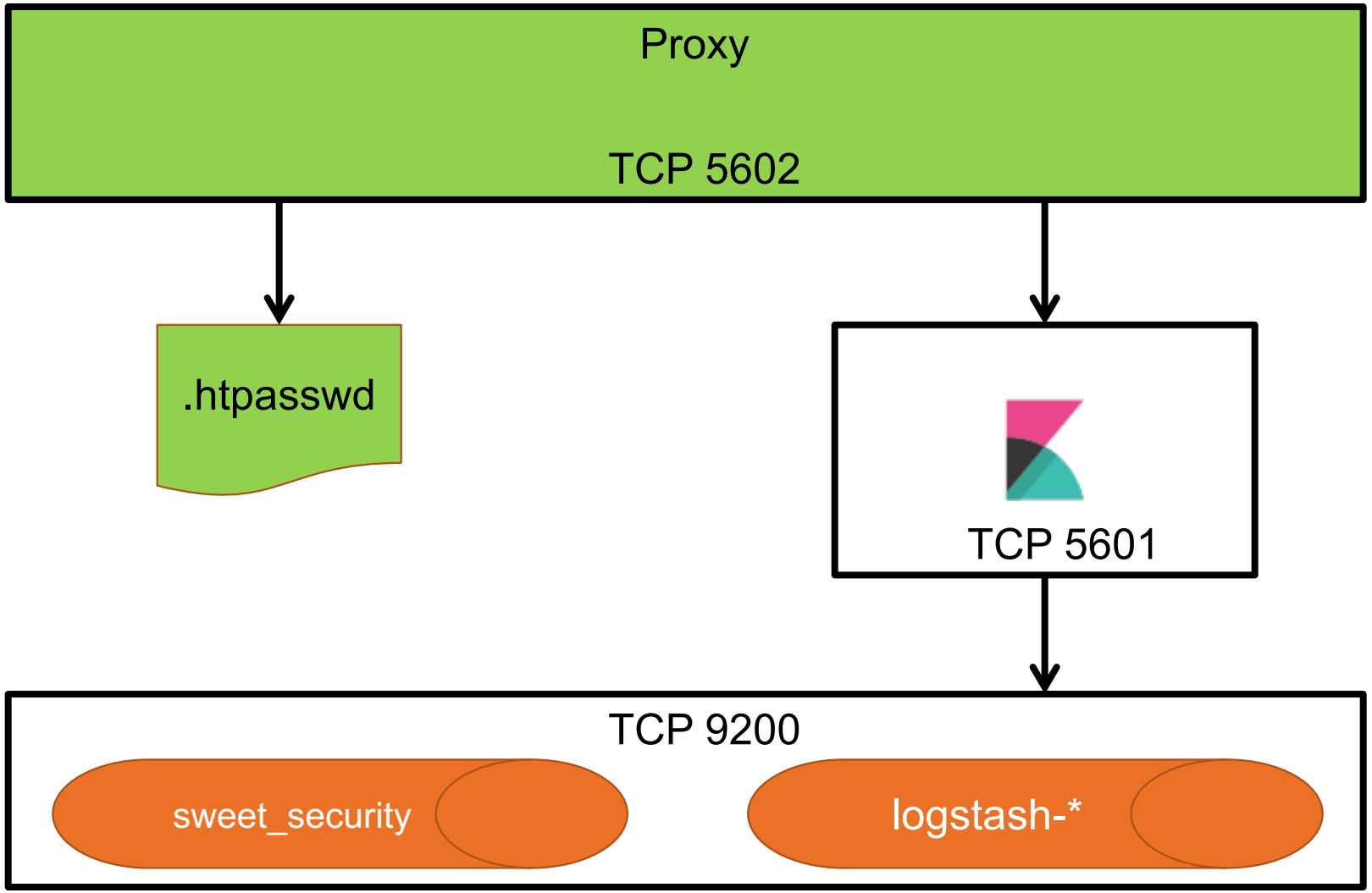
hostname	nickname	ip4	mac	vendor	ignore	active
iPhone.lan	iPhone	192.168.1.2	00:11:22:33:44:55:66	Apple	0	0
therm.lan	Thermostat	192.168.1.3	aa:bb:cc:dd:ee:ff	Google	0	1
mac.lan	Macbook	192.168.1.4	01:23:45:67:89:0a	Apple	1	1
tstr9412.lan	Toaster	192.168.1.5	no:ta:re:al:ma:c!	KitchenAid	0	1


Critical Stack
Bro IDS
Sweet Security
Logstash
80
9201
5602
Flask App
localhost:9200
Localhost:5601

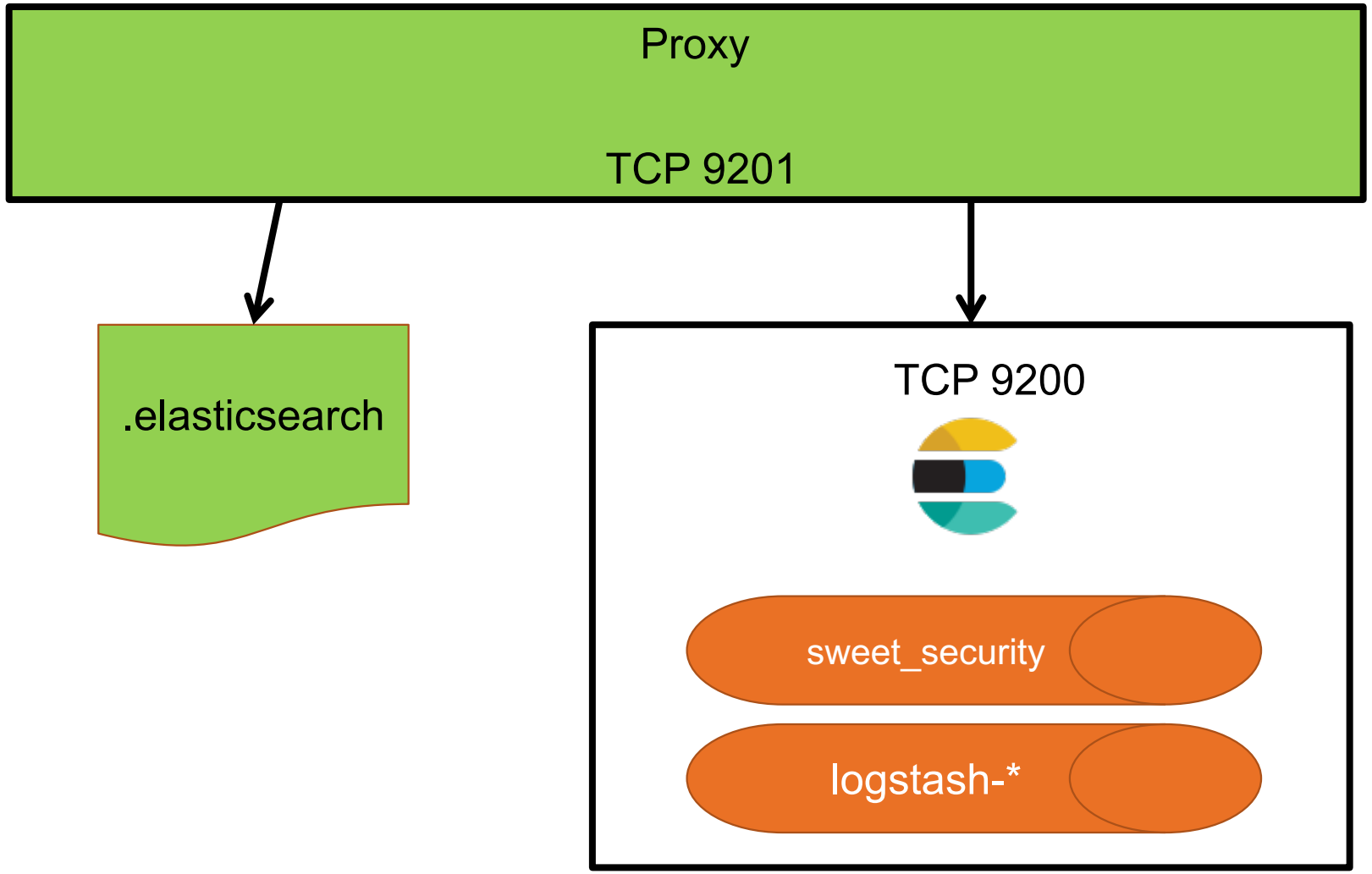
Web Portal Communication



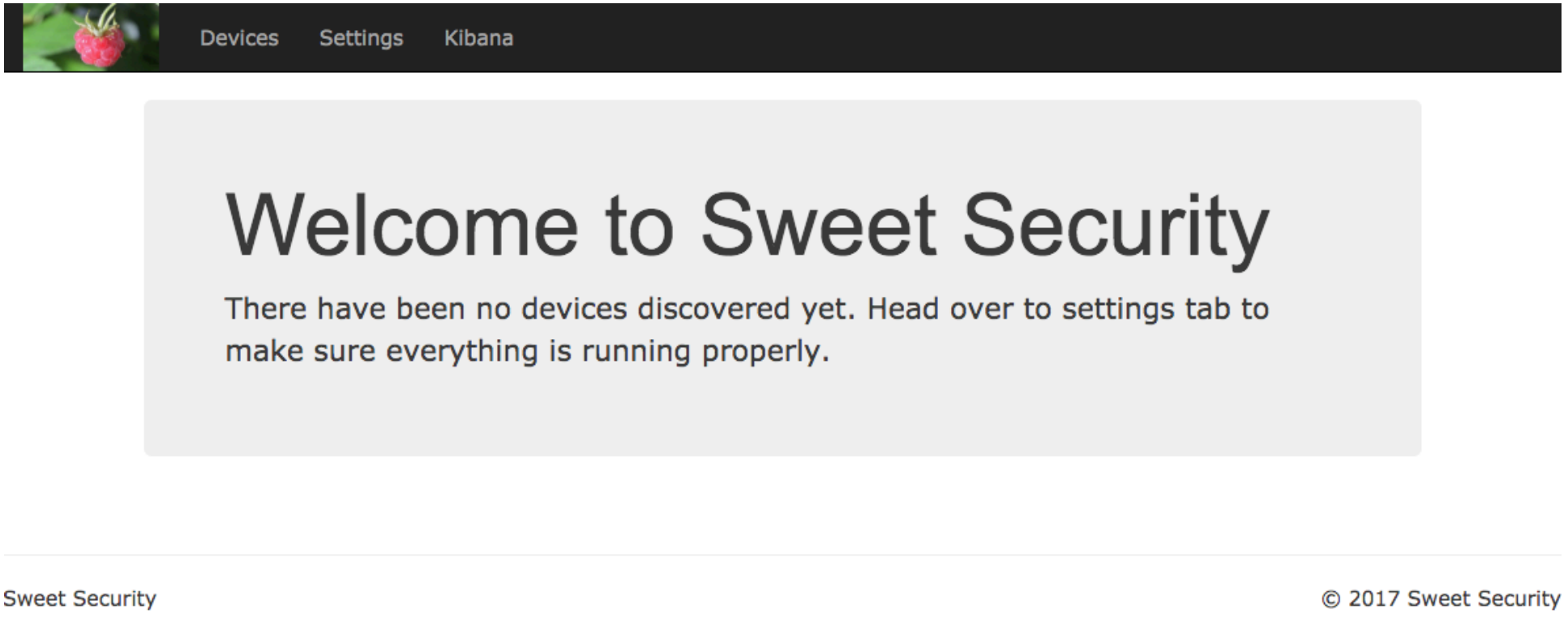
Kibana Architecture



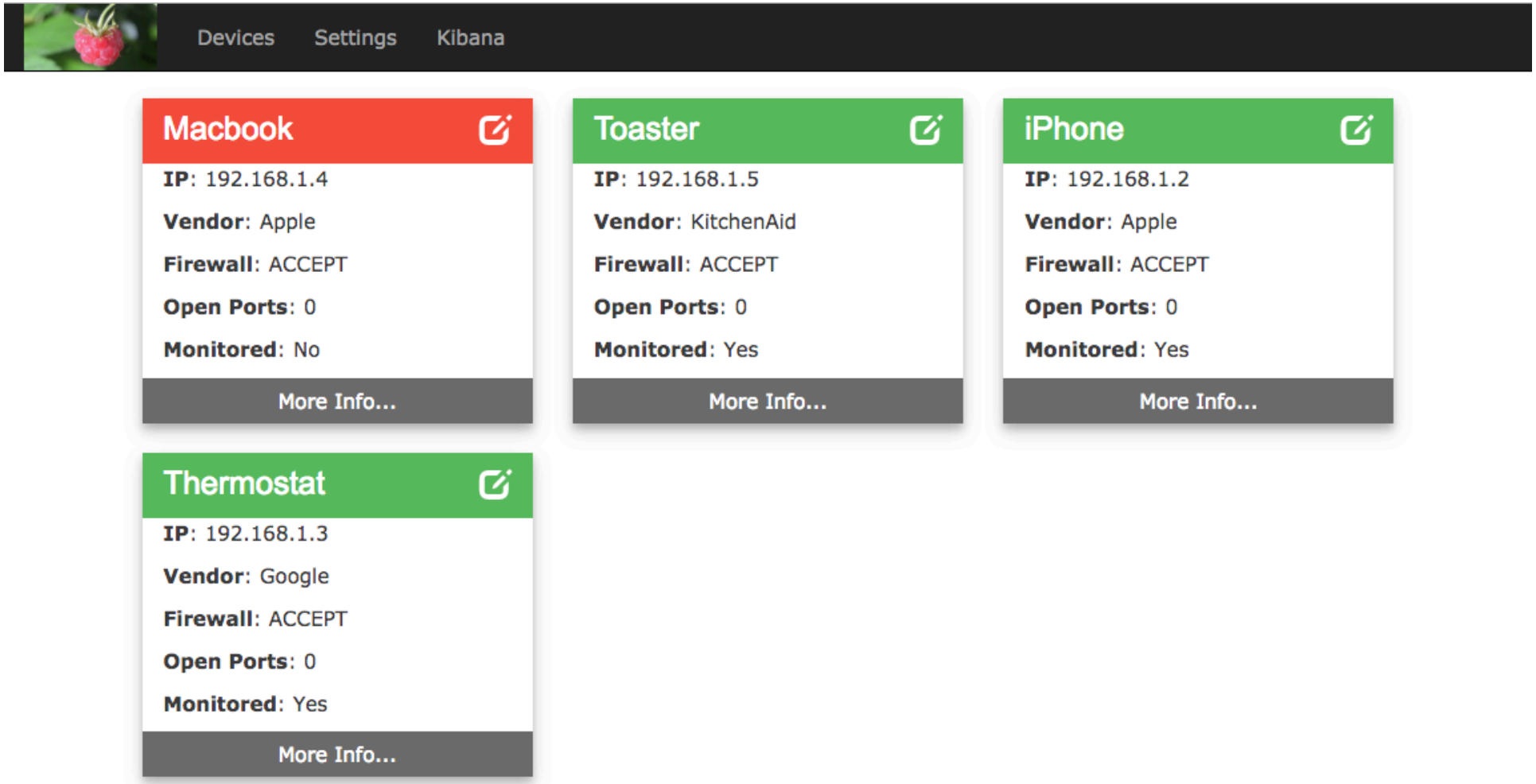
Elasticsearch Architecture



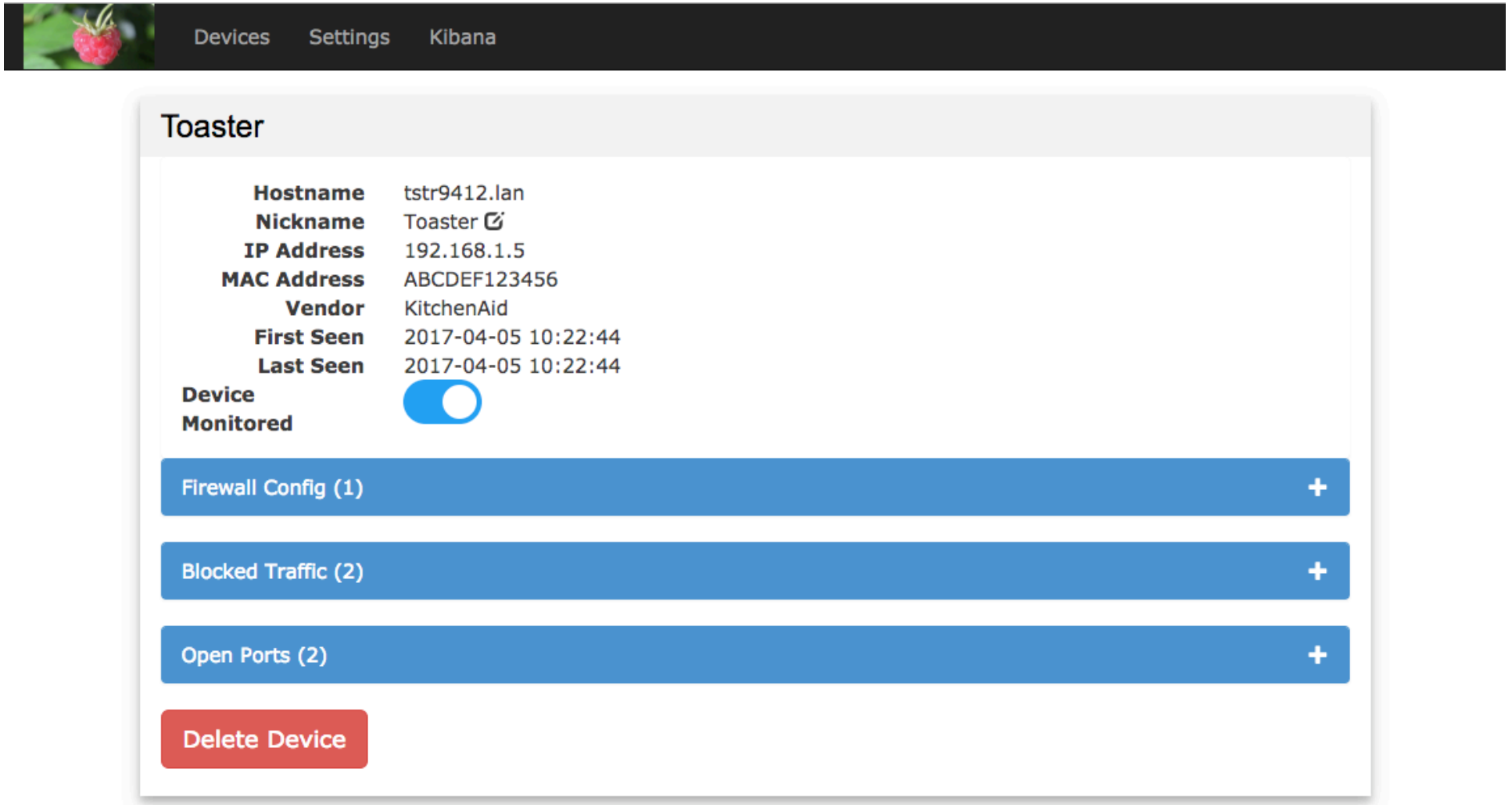
Web Portal Home Page



Web Portal Home Page



Device Details Page



Device Open Port Info

Open Ports (2) +

Last Port Scan: 2017-04-05 10:31

Port	Protocol	Name	Product	Version	Last Seen
23	tcp	telnet	Linux telnetd	Unknown	2017-04-05 10:31
80	tcp	http	Apache httpd	2.4.10	2017-04-05 10:31

Firewall Configuration

Firewall Config (2)

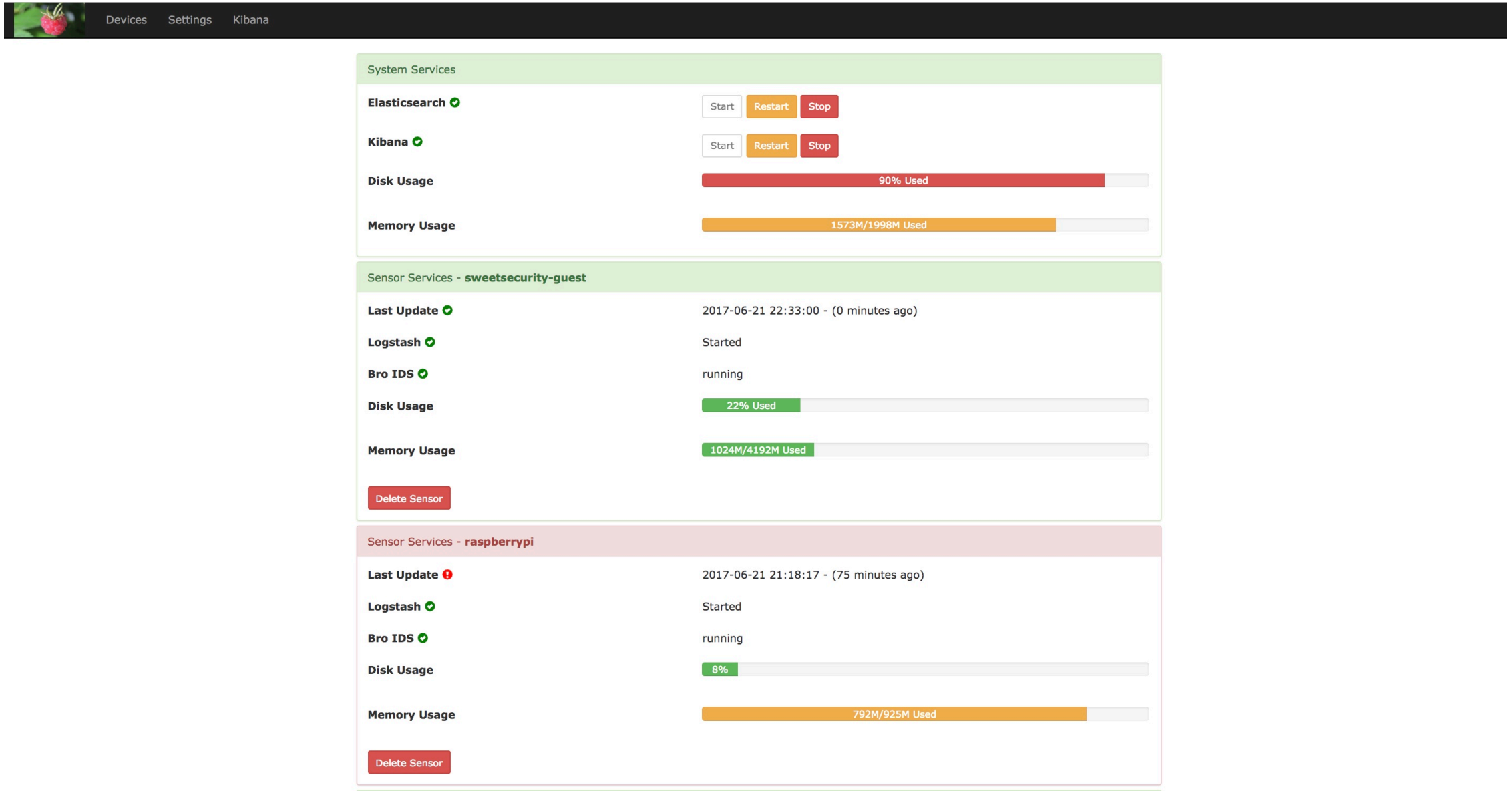
Destination	Action	
4.3.2.1	ACCEPT	Delete
kitchenaid.com	ACCEPT	Delete
All	DROP	Edit

Add Firewall Entry

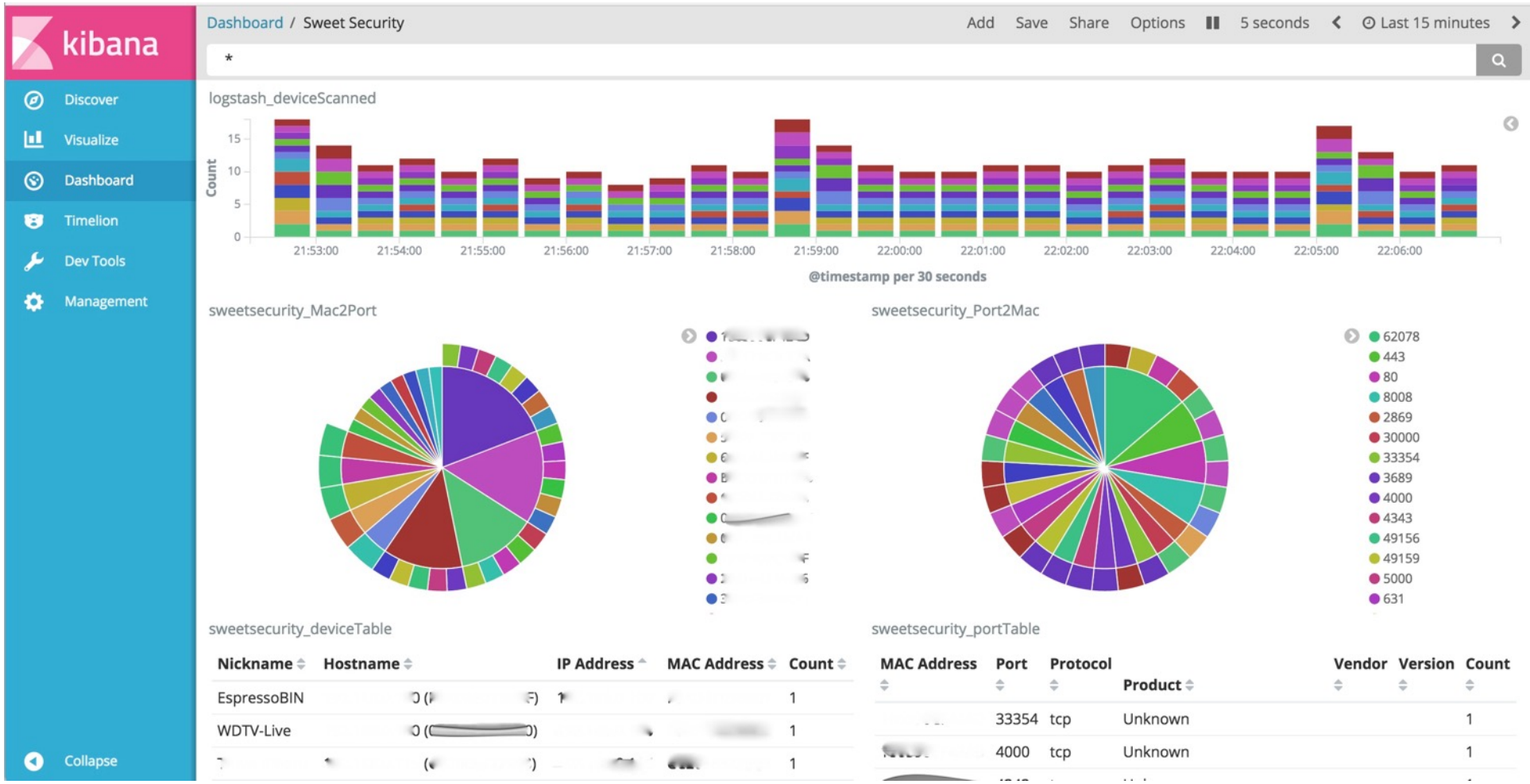
Blocked Traffic (2)

IP Address	Known URLs
1.2.3.4	haxordurl.ru
4.3.2.1	toasterrecipes.com

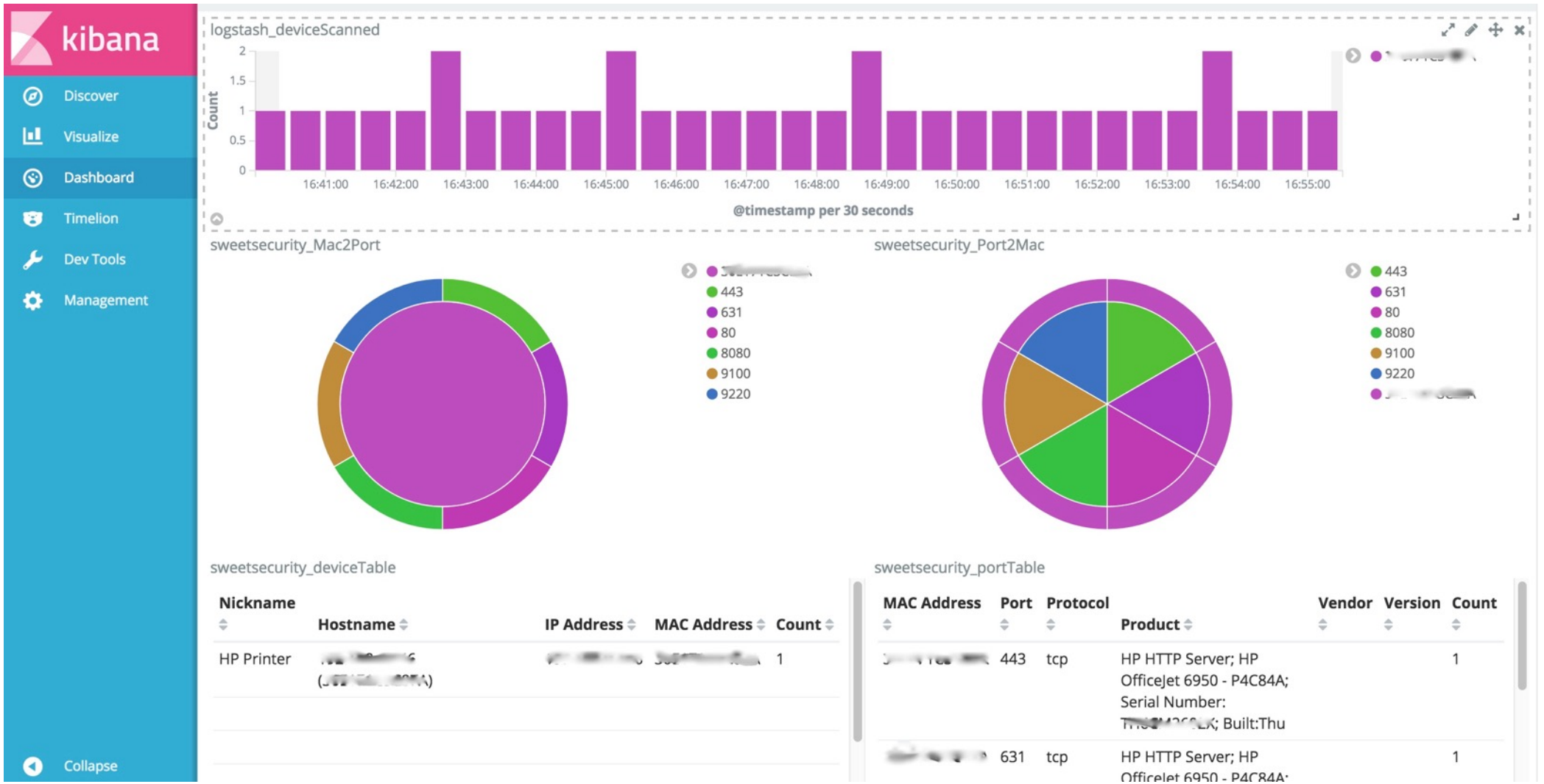
System Health



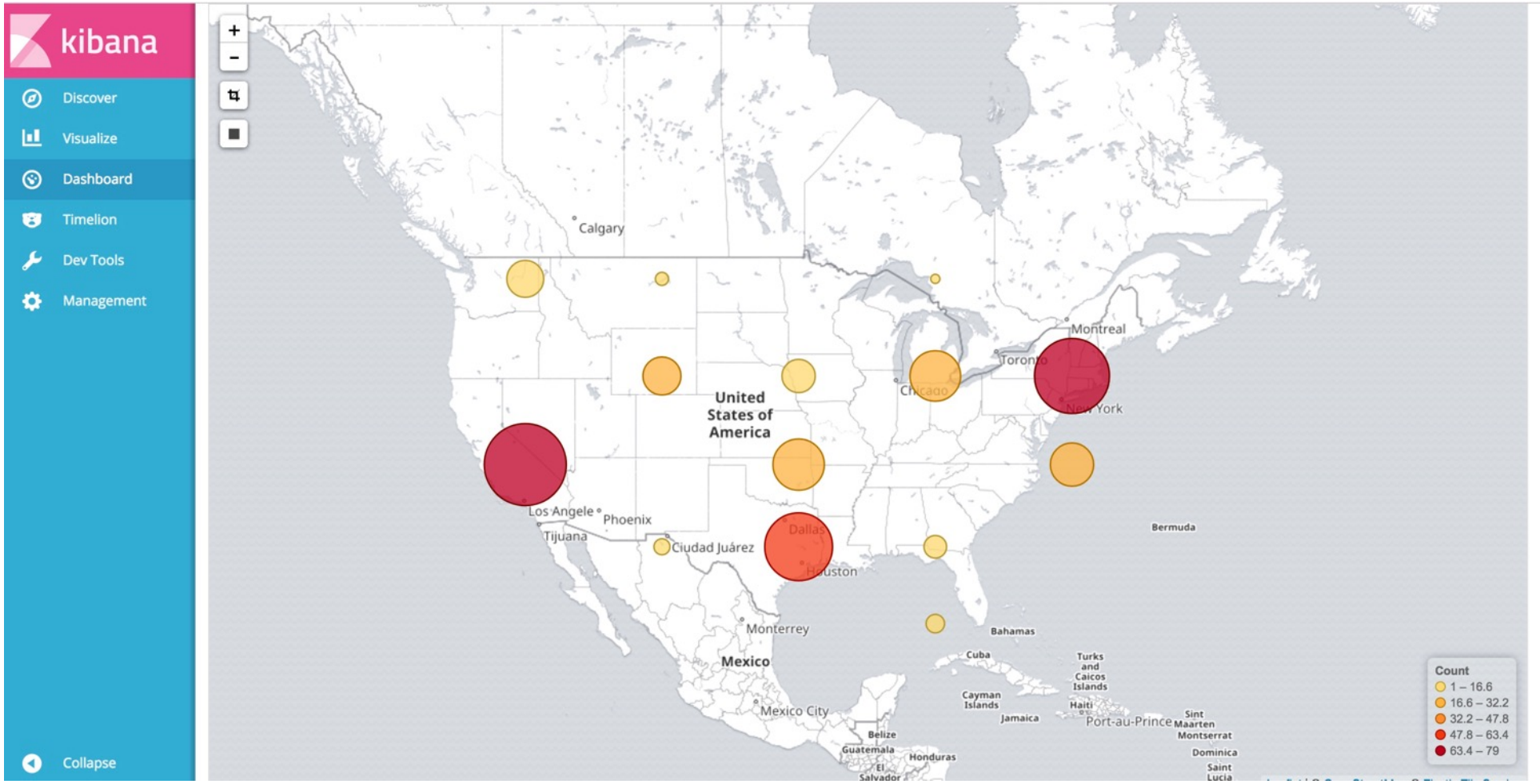
Device Insights



Device Insights

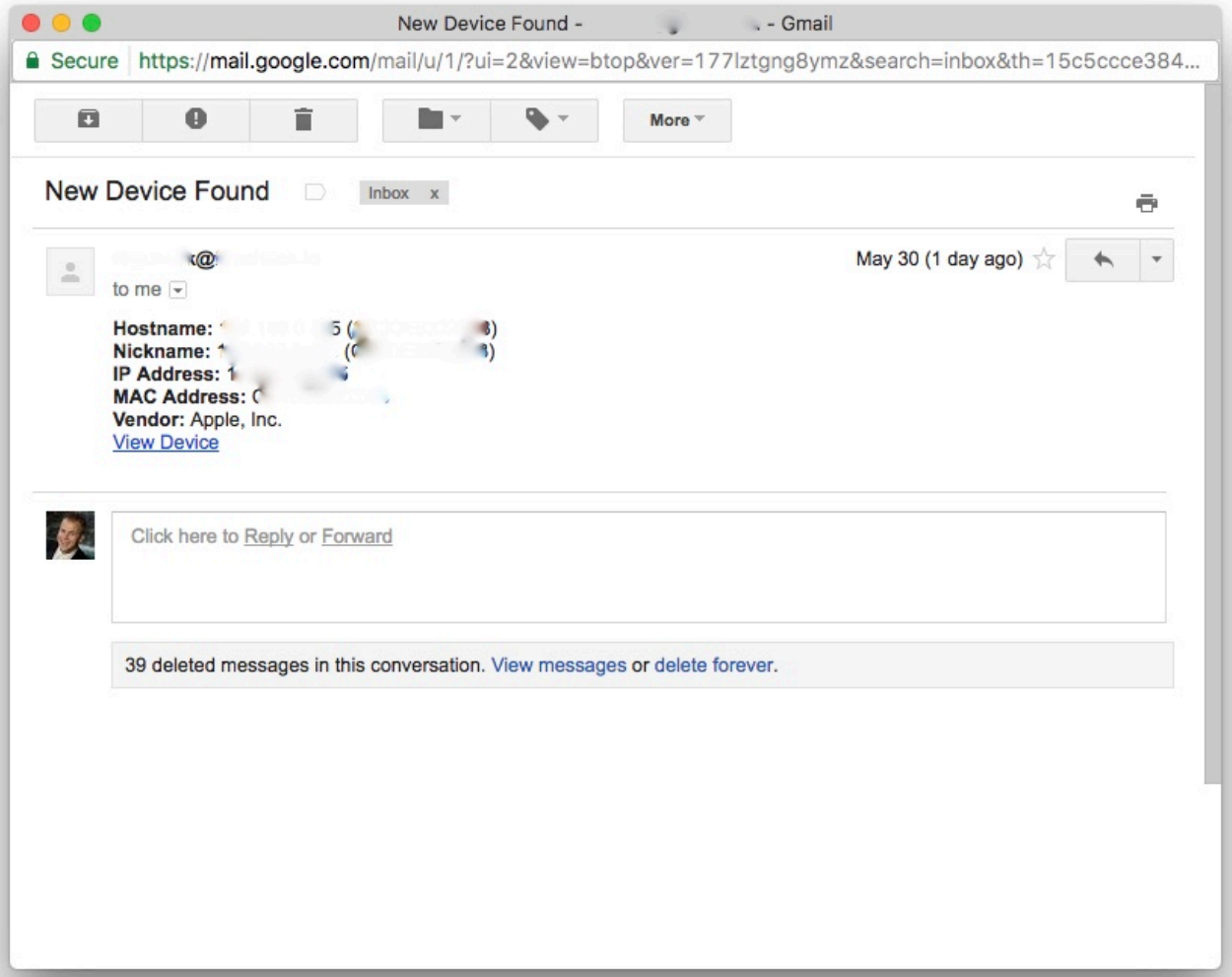


GeoIP Location



Threat Hunting w/ Sweet Security

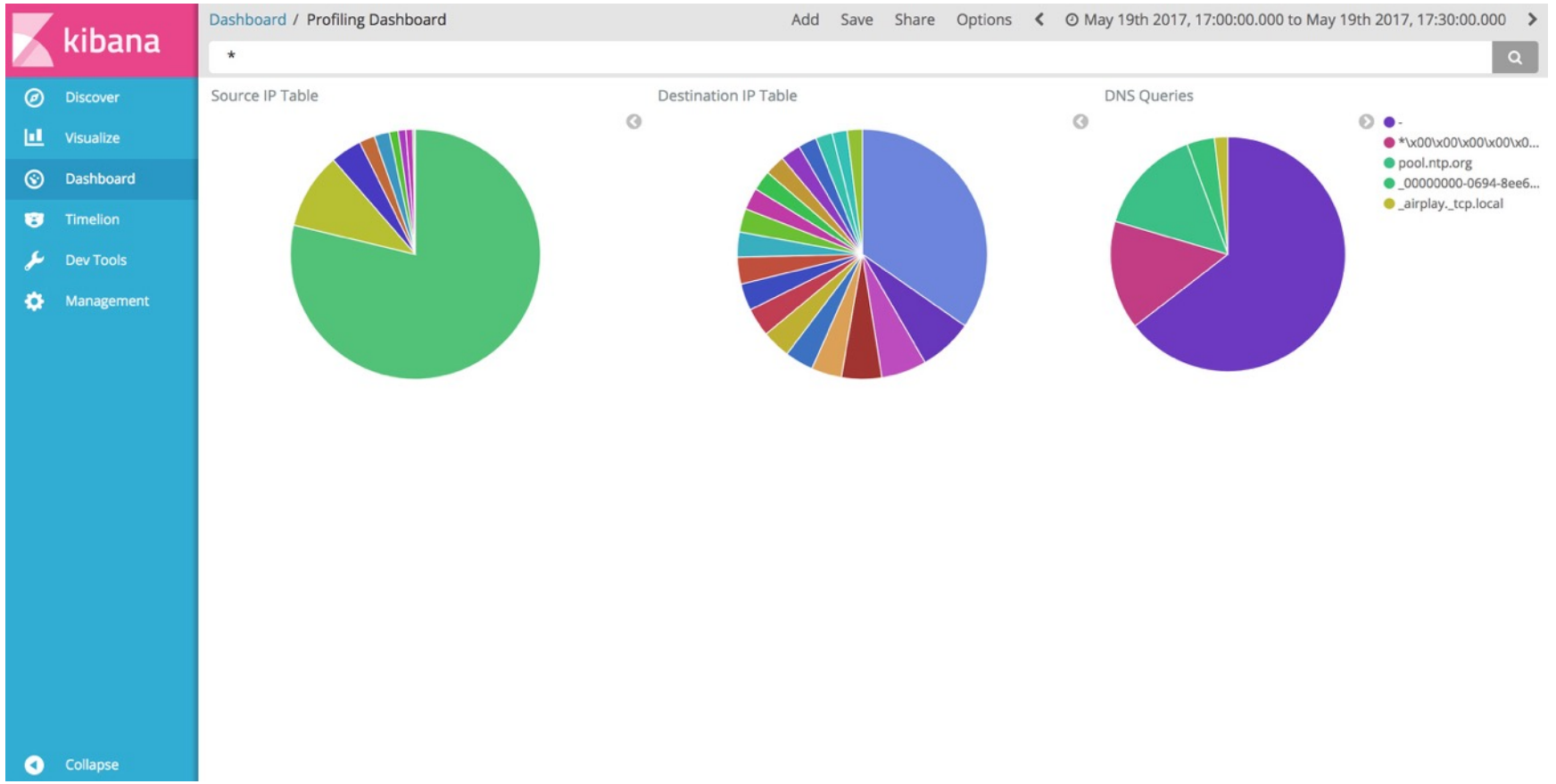
Threat Hunting: Rogue Devices



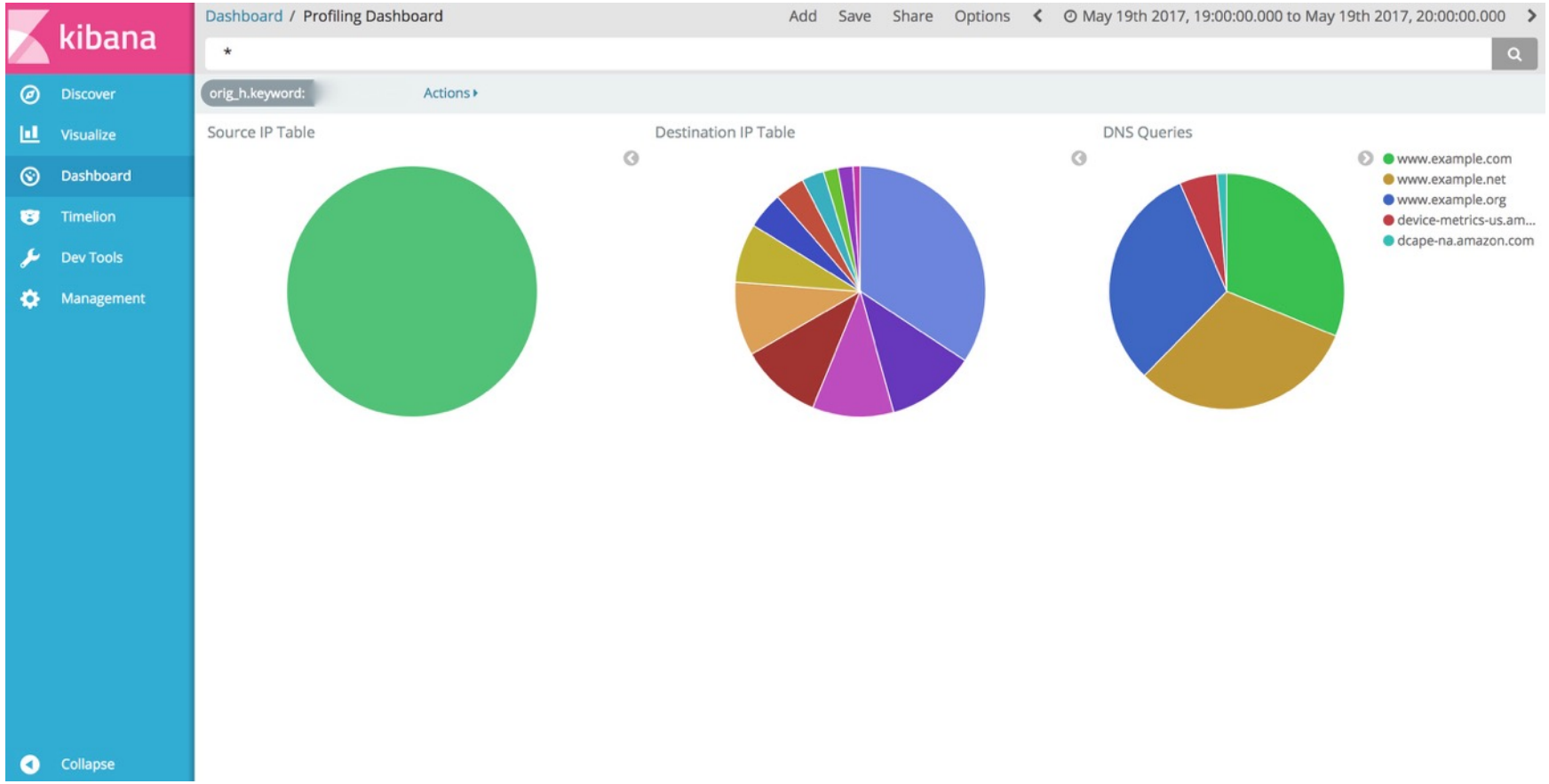
Threat Hunting: Amazon Echo

- Detecting activity to ”interesting” domains

Threat Hunting: Amazon Echo

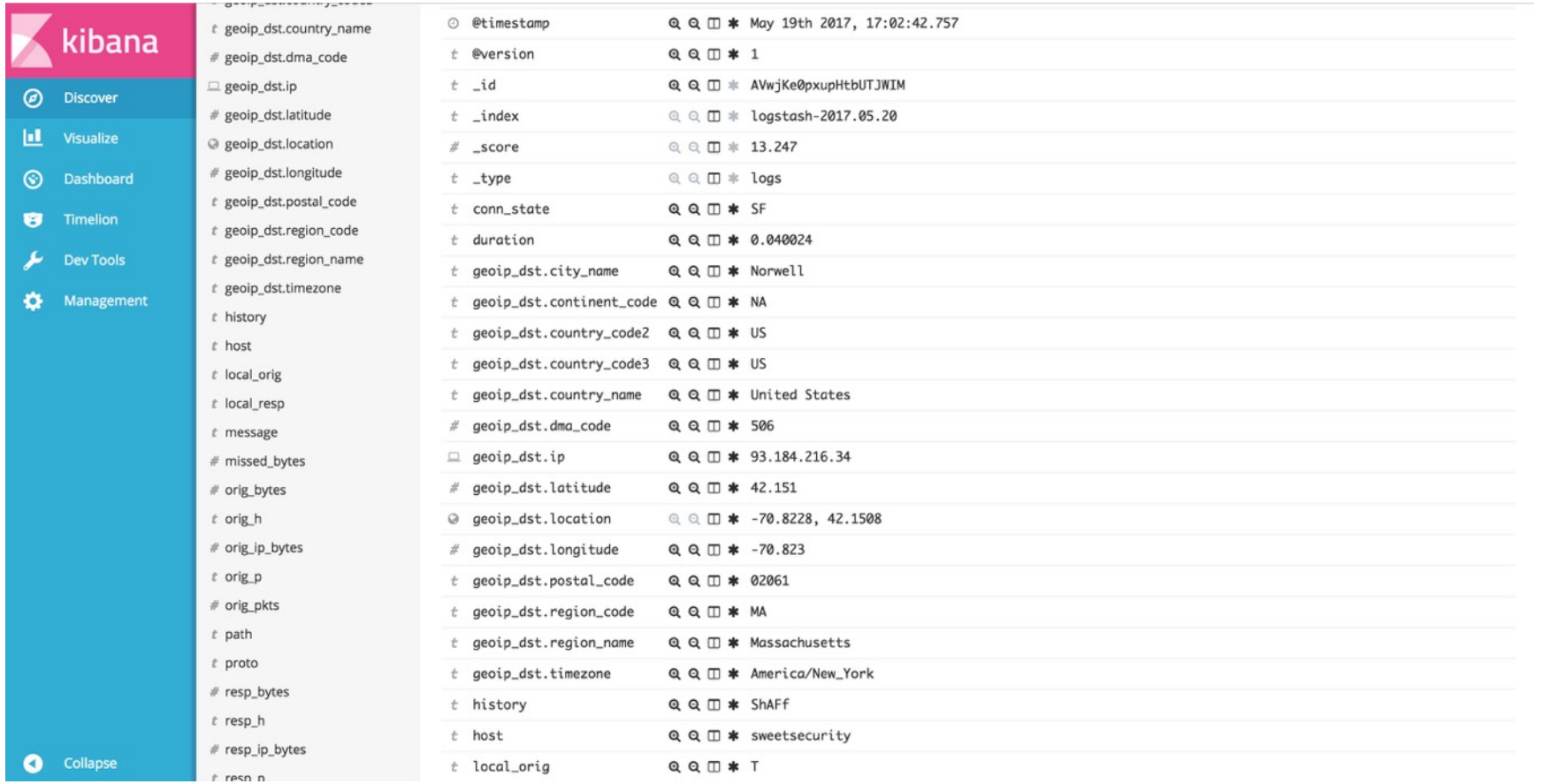


Threat Hunting: Amazon Alexa

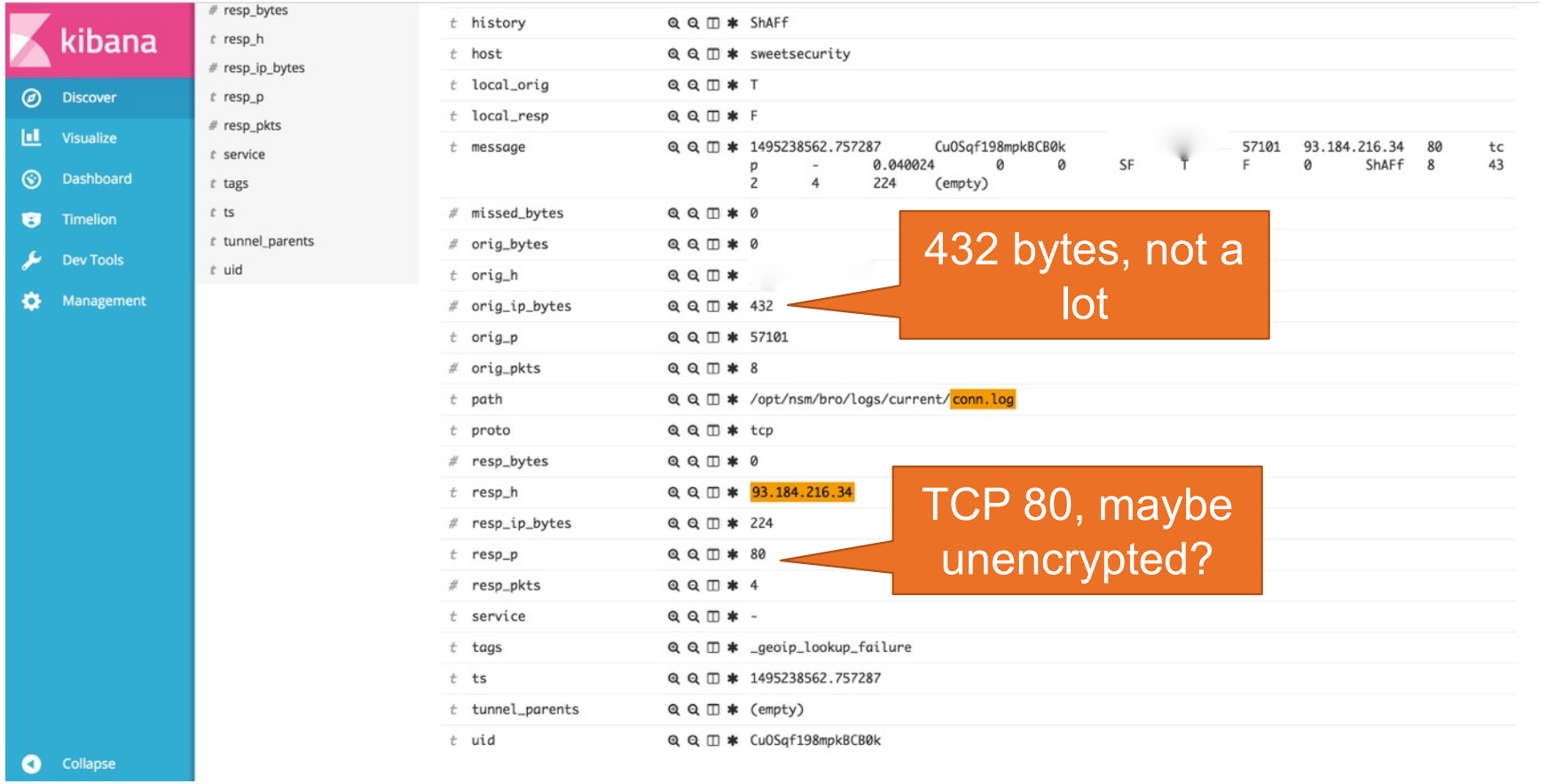


Threat Hunting: Amazon Alexa

Threat Hunting: Amazon Alexa

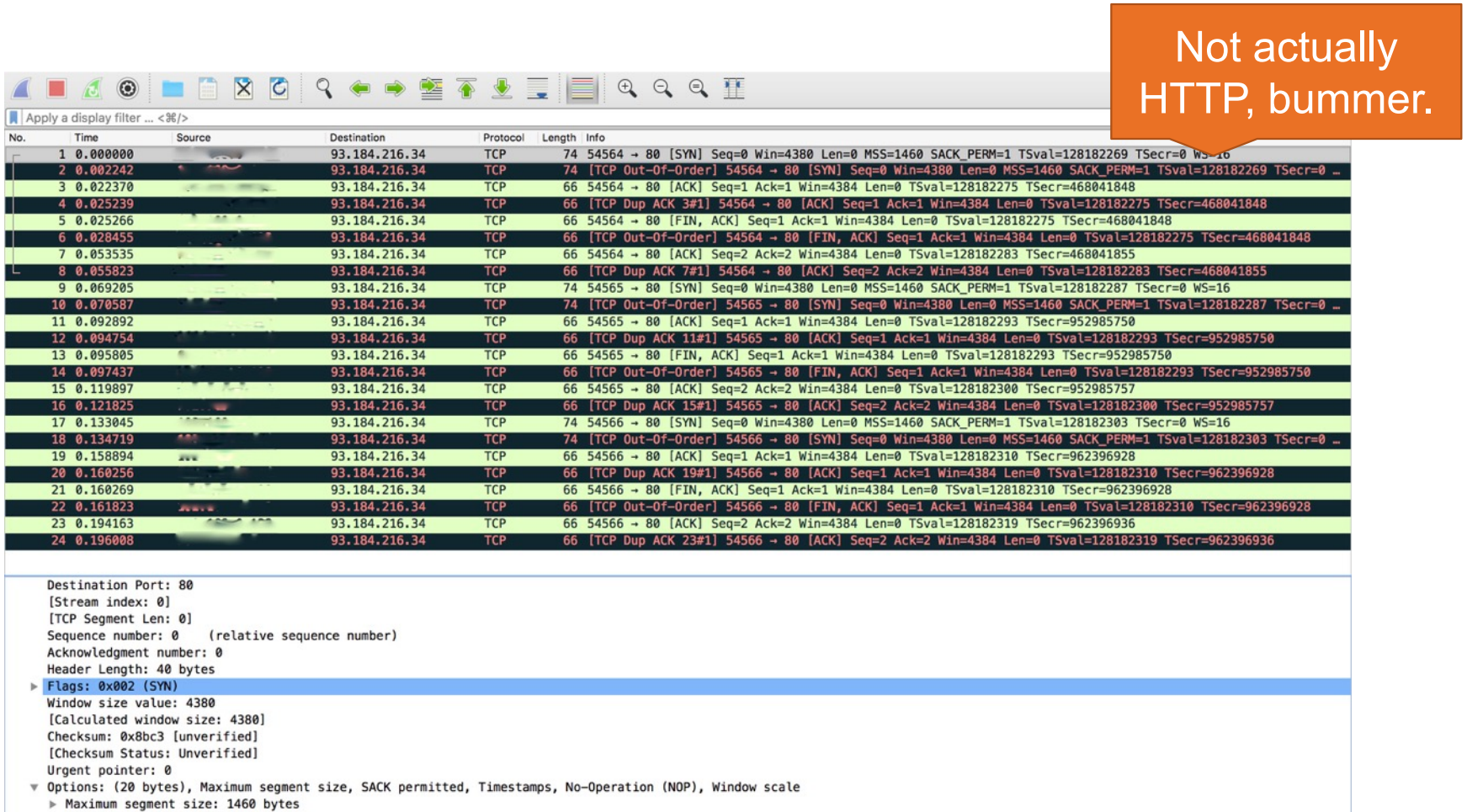


Threat Hunting: Amazon Alexa



Threat Hunting: Amazon Alexa

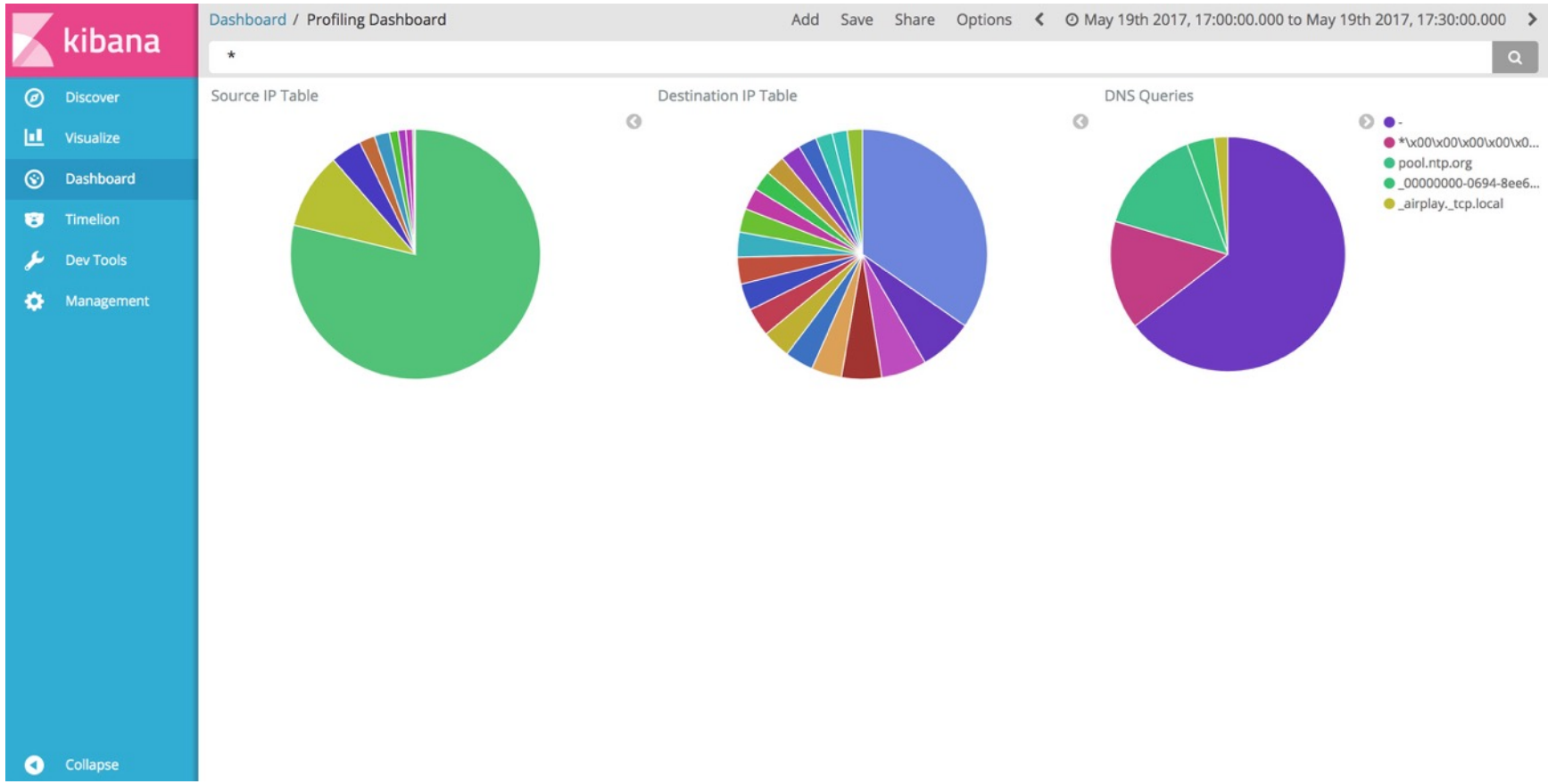
- **tcpdump** -i enp0s25 -A -XX dst 93.184.216.34 -w example.com.pcap



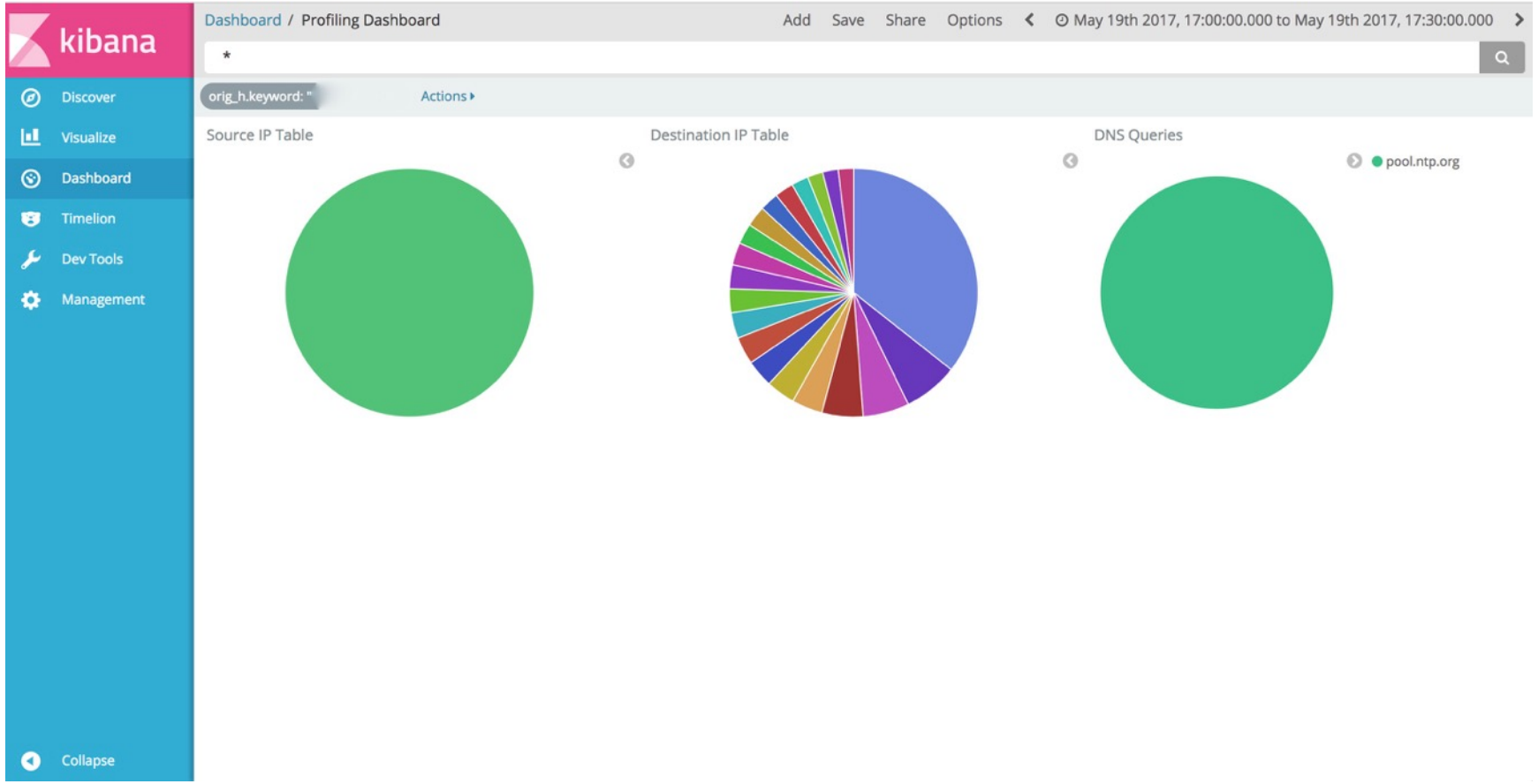
Threat Hunting: WDTVLive

- Massive amounts of NTP traffic

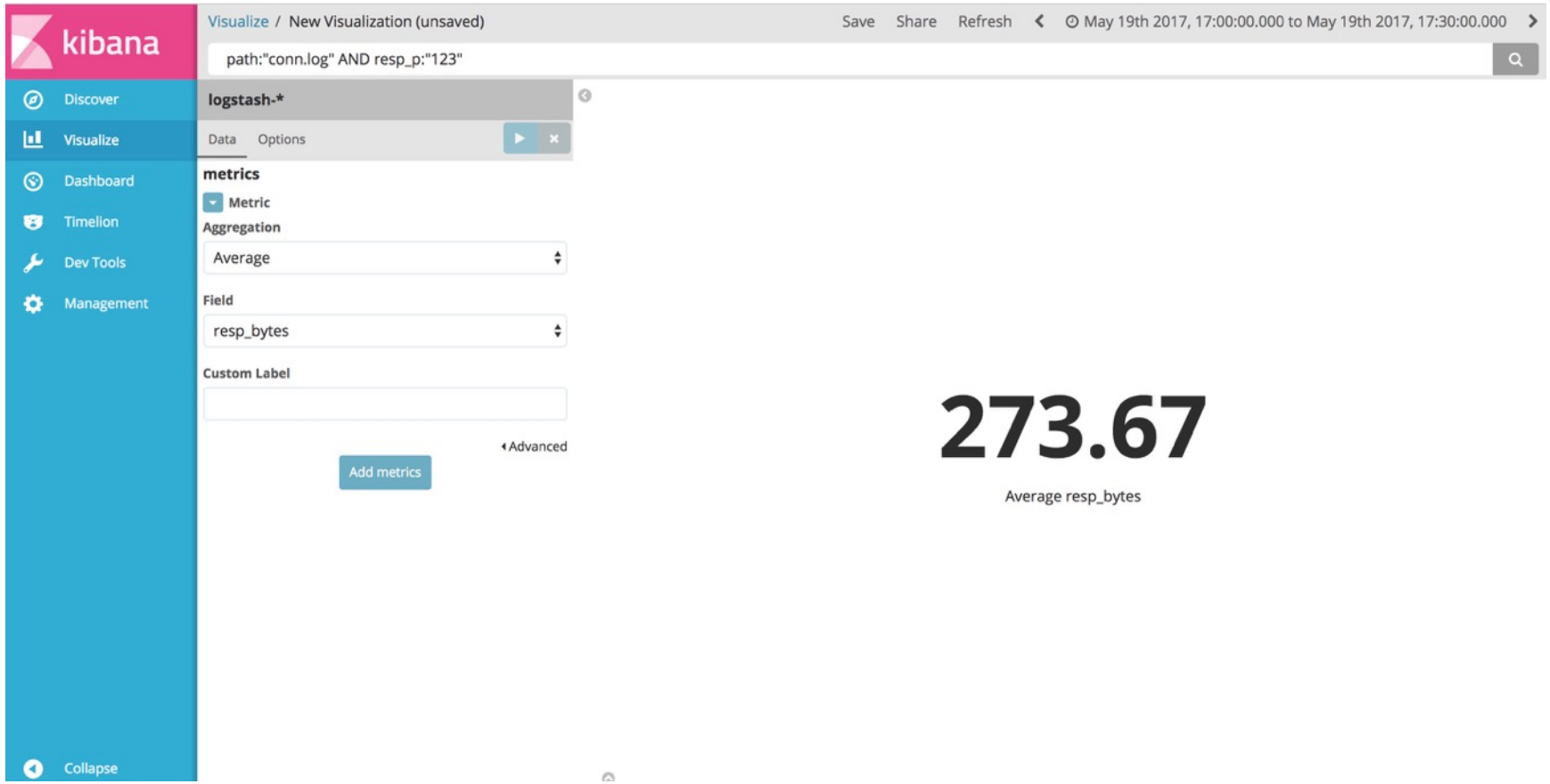
Threat Hunting: WDTVLive



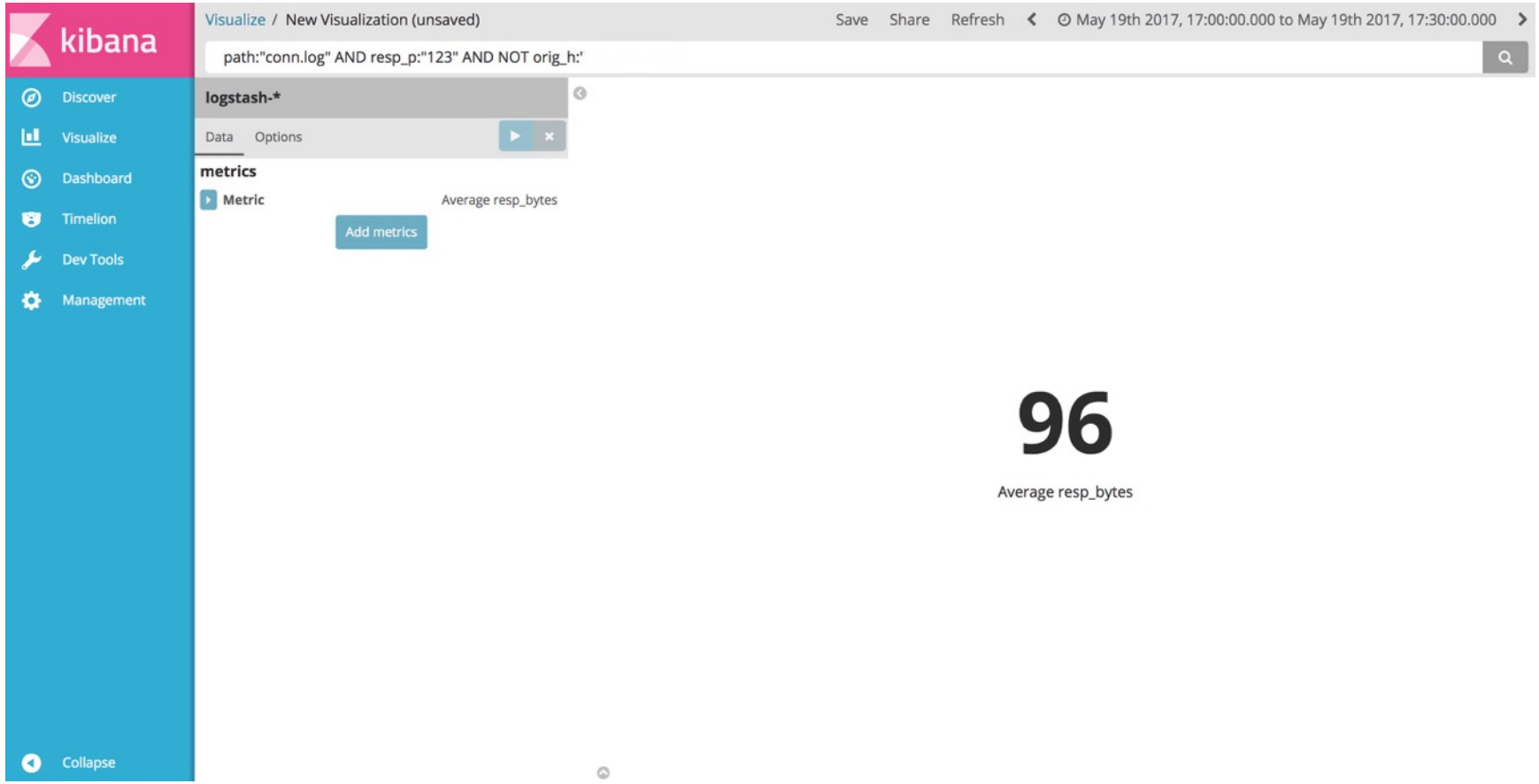
Threat Hunting: WDTVLive



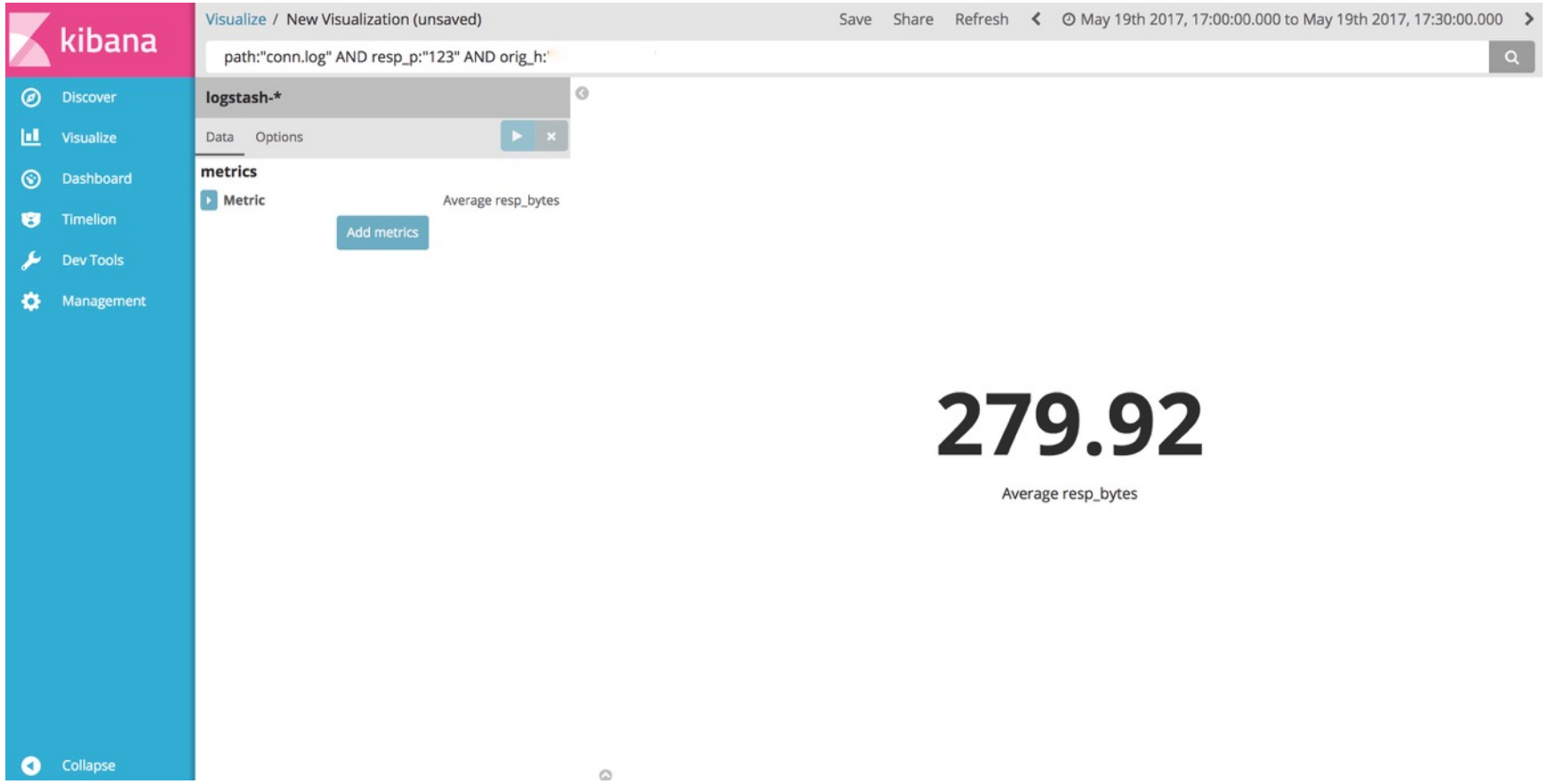
Threat Hunting: WDTVLive



Threat Hunting: WDTVLive

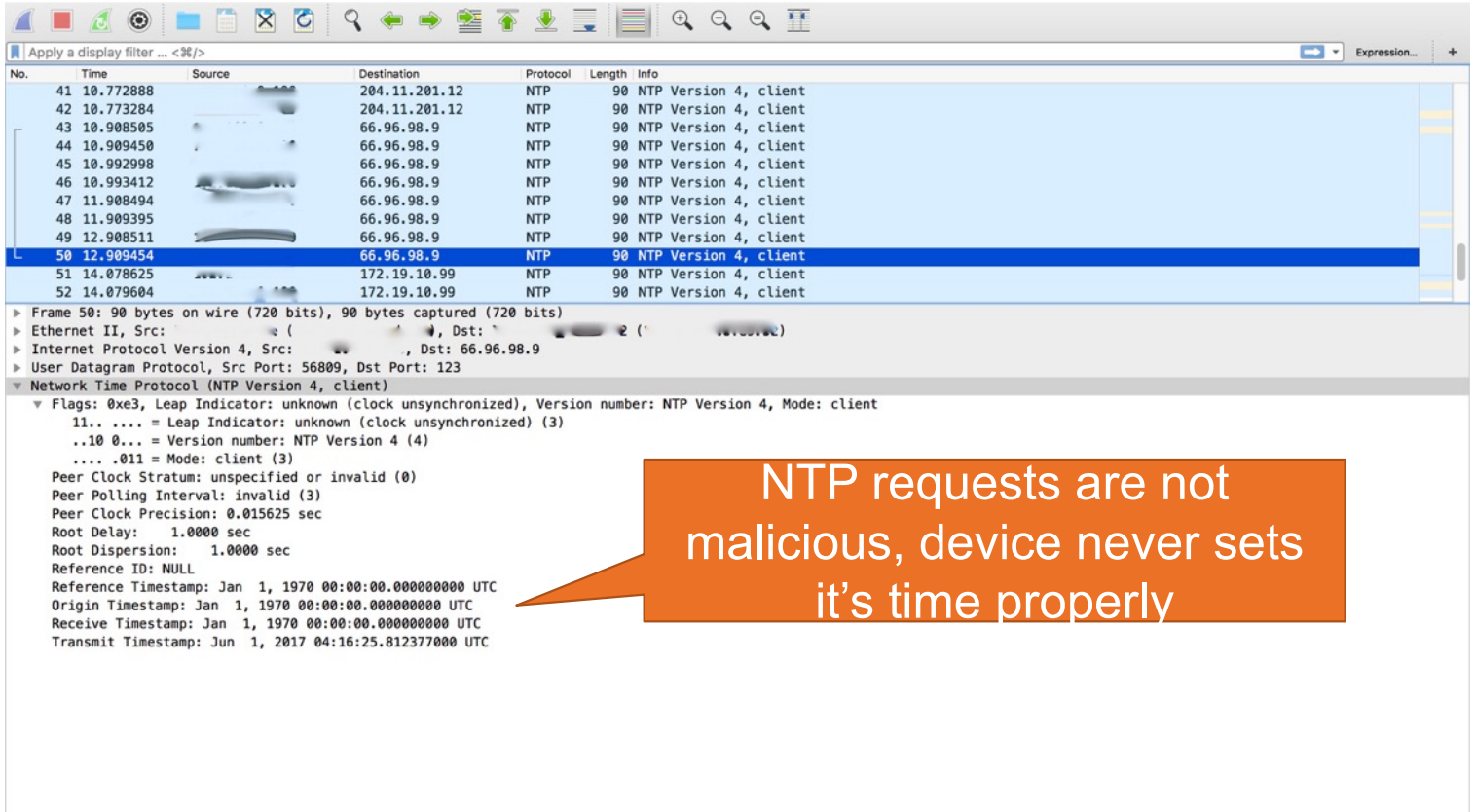


Threat Hunting: WDTVLive



Threat Hunting: WDTVLive

- **tcpdump** -i enp0s25 -A -XX src _WDTVLIVEIP_ -w wdtv.pcap



Threat Hunting: Baselines

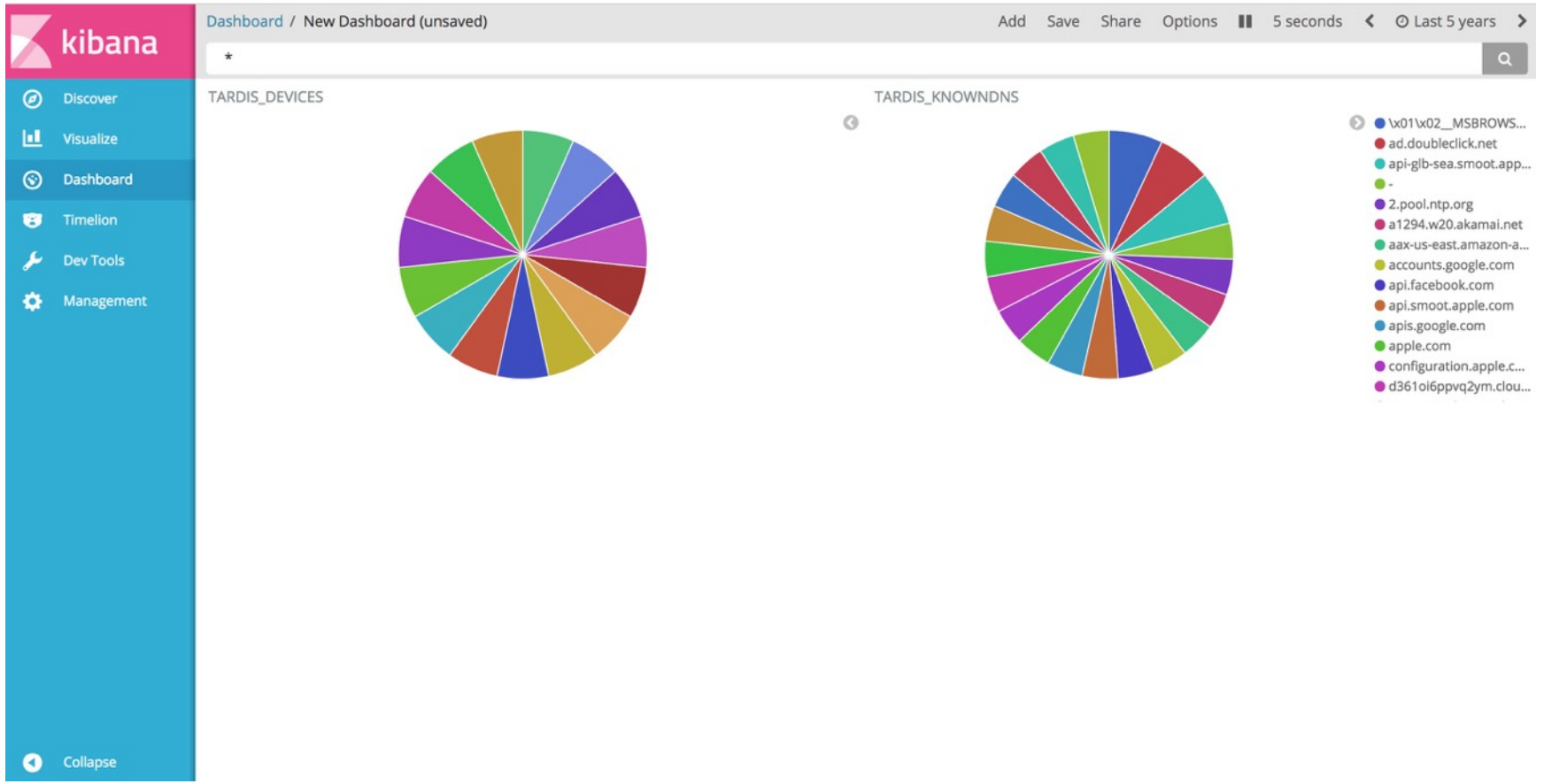
- Learning Mode
  - resp_h
  - resp_h:resp_p
  - query
  - server_name
- Alerting Mode
  - Lock whitelist, alert when something is outside baseline
- Blocking Mode
  - Lock whitelist, block when something is outside baseline

Threat Hunting: Baselines

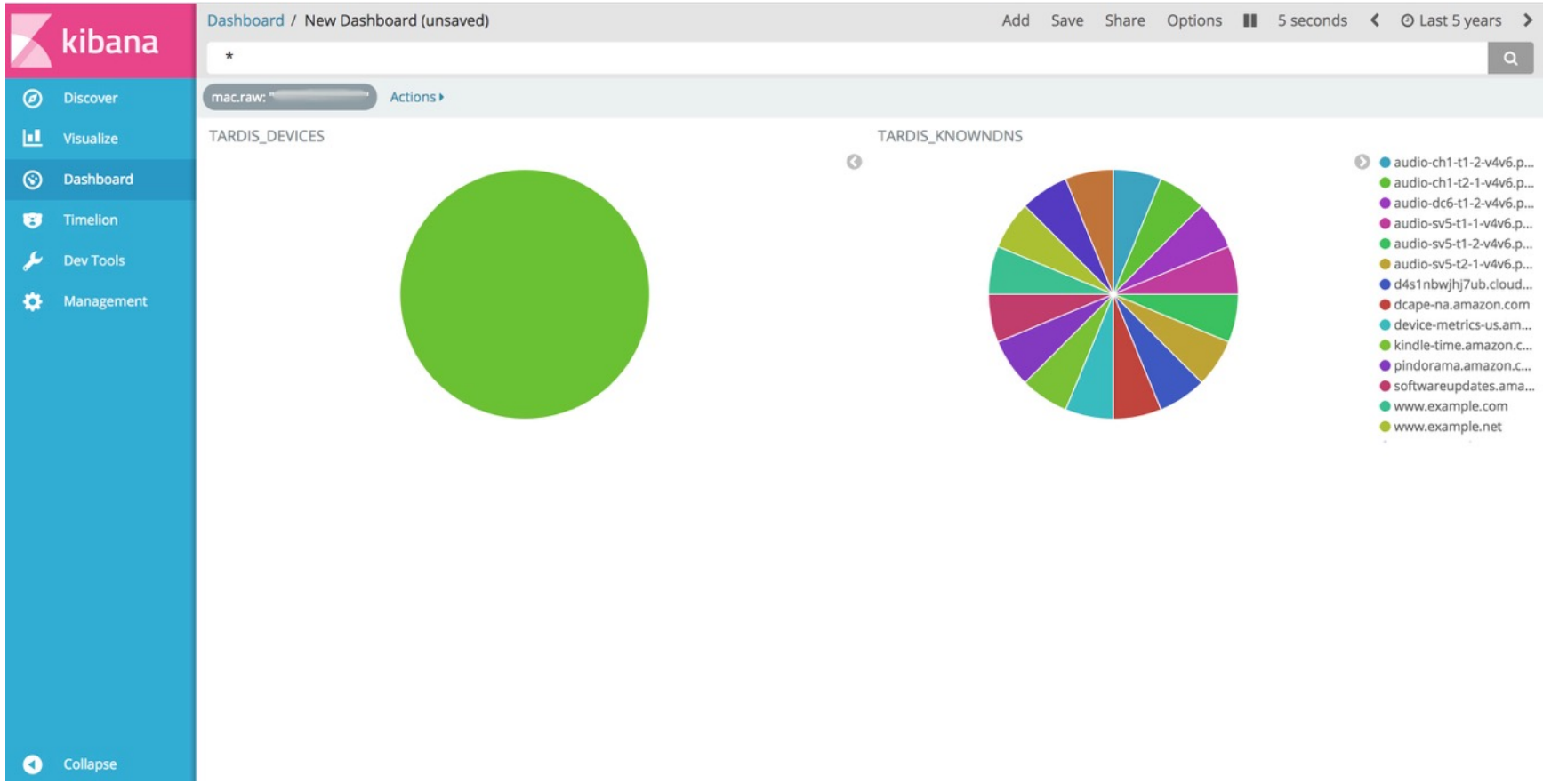
```
KNOWN WEBSITES
  {u'date': u'1492468890547', u'mac': u'AC63BE92121F', u'server_name': u'd4s1nbwjhj7ub.cloudfront.net'}
  {u'date': u'1492813688867', u'mac': u'AC63BE92121F', u'server_name': u'softwareupdates.amazon.com'}
  {u'date': u'1492468890539', u'mac': u'AC63BE92121F', u'server_name': u'device-metrics-us.amazon.com'}
  {u'date': u'1492468890543', u'mac': u'AC63BE92121F', u'server_name': u'dcape-na.amazon.com'}
  {u'date': u'1492468890554', u'mac': u'AC63BE92121F', u'server_name': u'www.meethue.com'}
KNOWN DNS QUERIES
  {u'date': u'1492468890559', u'query': u'www.example.com', u'mac': u'AC63BE92121F'}
  {u'date': u'1492468890574', u'query': u'www.meethue.com', u'mac': u'AC63BE92121F'}
  {u'date': u'1492468890567', u'query': u'www.example.net', u'mac': u'AC63BE92121F'}
  {u'date': u'1492468890570', u'query': u'www.example.org', u'mac': u'AC63BE92121F'}
  {u'date': u'1492813688888', u'query': u'softwareupdates.amazon.com', u'mac': u'AC63BE92121F'}
  {u'date': u'1492468890563', u'query': u'dcape-na.amazon.com', u'mac': u'AC63BE92121F'}
  {u'date': u'1492468890598', u'query': u'audio-sv5-t1-2-v4v6.pandora.com', u'mac': u'AC63BE92121F'}
  {u'date': u'1492813688884', u'query': u'd4s1nbwjhj7ub.cloudfront.net', u'mac': u'AC63BE92121F'}
  {u'date': u'1493066752265', u'query': u'audio-ch1-t1-2-v4v6.pandora.com', u'mac': u'AC63BE92121F'}
  {u'date': u'1492468890606', u'query': u'pindorama.amazon.com', u'mac': u'AC63BE92121F'}
  {u'date': u'1493053526778', u'query': u'kindle-time.amazon.com', u'mac': u'AC63BE92121F'}
  {u'date': u'1493053526803', u'query': u'audio-dc6-t1-2-v4v6.pandora.com', u'mac': u'AC63BE92121F'}
  {u'date': u'1493053526811', u'query': u'audio-ch1-t2-1-v4v6.pandora.com', u'mac': u'AC63BE92121F'}
  {u'date': u'1492468890593', u'query': u'device-metrics-us.amazon.com', u'mac': u'AC63BE92121F'}
  {u'date': u'1492468890602', u'query': u'audio-sv5-t1-1-v4v6.pandora.com', u'mac': u'AC63BE92121F'}
  {u'date': u'1493053526807', u'query': u'audio-sv5-t2-1-v4v6.pandora.com', u'mac': u'AC63BE92121F'}
```

```
Found 2 new Websites
  det-ta-g7g.amazon.com
  todo-ta-g7g.amazon.com
Found 11 new DNS Queries
  det-ta-g7g.amazon.com
  ntp-g7g.amazon.com
  0.north-america.pool.ntp.org
  1.north-america.pool.ntp.org
  3.north-america.pool.ntp.org
  todo-ta-g7g.amazon.com
  2.north-america.pool.ntp.org
  audio-dc6-t1-1-v4v6.pandora.com
  audio-ch1-t1-1-v4v6.pandora.com
  t1-2.p-cdn.com
  audio-dc6-t2-2-v4v6.pandora.com
Found 0 new Listening Ports
```

Threat Hunting: Baselines



Threat Hunting: Baselines



Threat Hunting: Domain Entropy

- google.com
  - 2.646439
- 7cacf3444269af1f6ad07c89f496a02d.org
  - 3.884795
- audio-dc6-t1-2-v4v6.pandora.com
  - 3.977917
- sbfb3c.y21w.za8b4fb8v.76c5.7548l.m79.l6ex.sf5bv.dc7m.v2da8e4kt.drovemeetings.in
  - 4.625840985278011

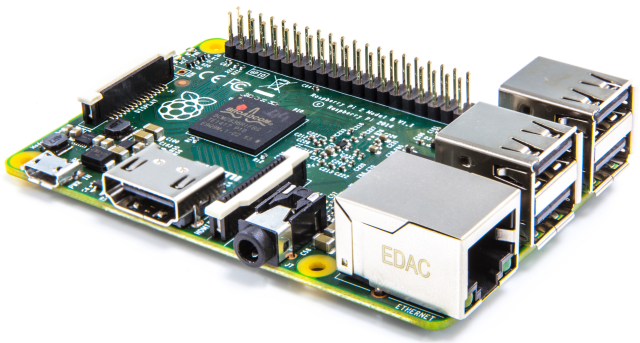
Threat Hunting: General

- Known Bad Lookups
- Check unknown IP's/URLS
  - WHOIS
  - Nslookup
  - GeoIP (mostly for fun)
- Tor Exit Node IP Search

My Setup

Home Network

Guest network



Internal Network

What's New

- ARP Spoofing
- Full Bro Log Support
- Kibana Dashboards
- Architecture Independent
- Service Scripts
- Updated NMAP Prefixes
- Web Administration
- Multi Sensor Support
- Integrated Firewall

GitHub Repo

https://github.com/travisfsmith/sweetsecurity

tripwire
CONFIDENCE: SECURED

Travis Smith
@MrTrav
tsmith@tripwire.com

THANK YOU