



CONFIDENCE: SECURED

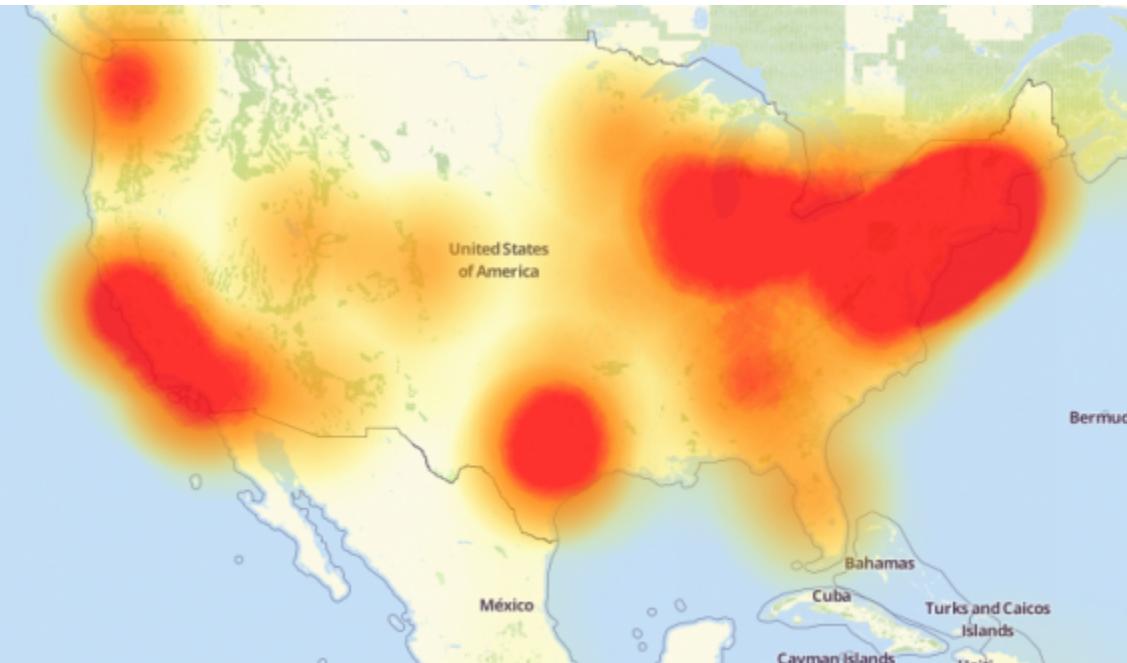
Sweet Security Supercharged

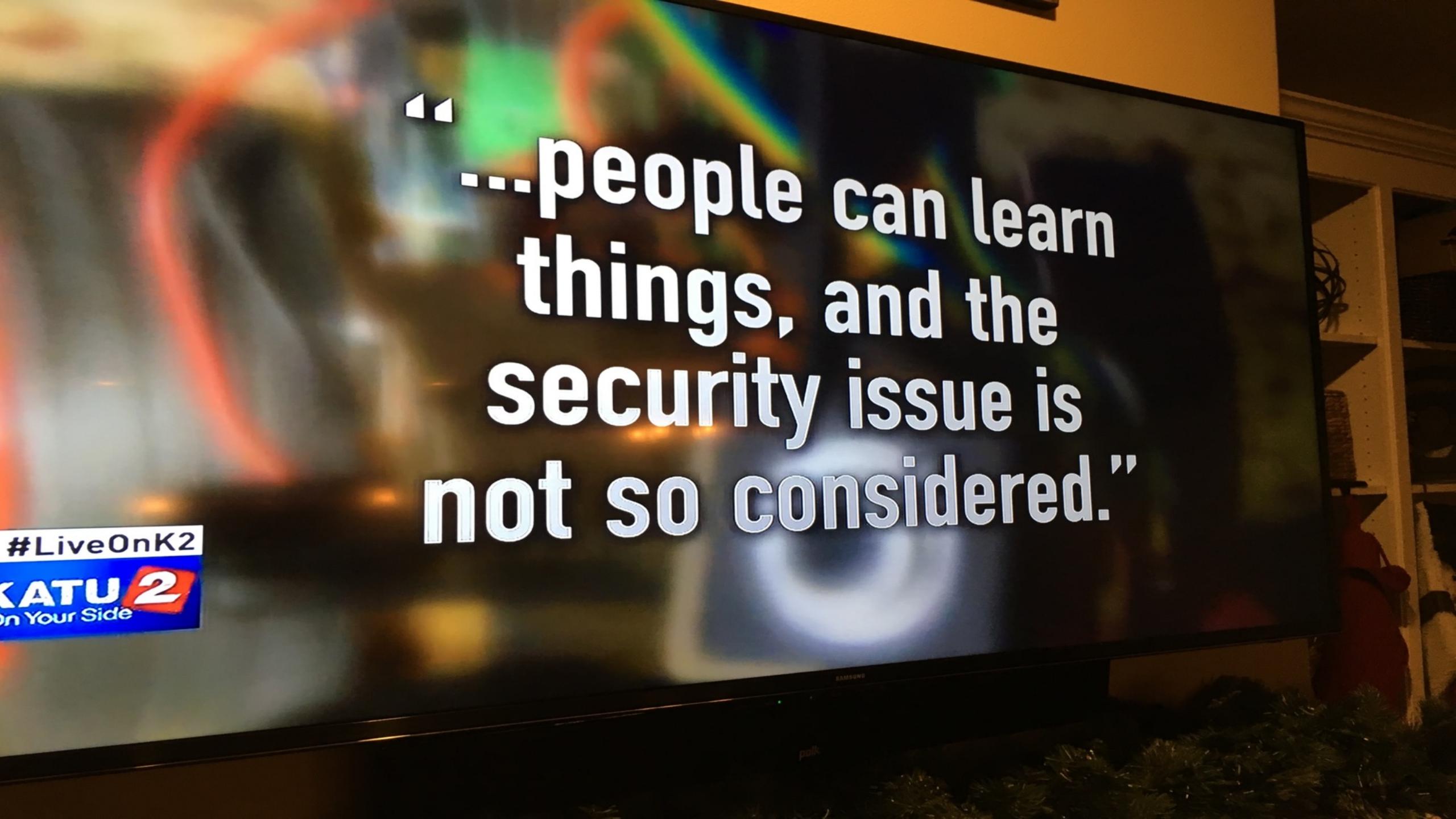
Deploying a Defensive Raspberry Pi (And Beyond)



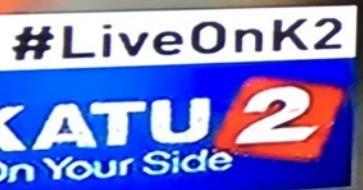
PROTECT THE UNPATCHABLE

The Problem



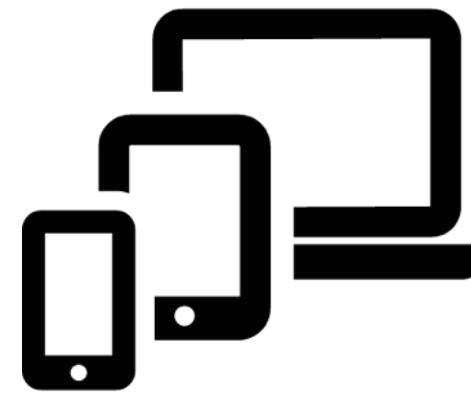
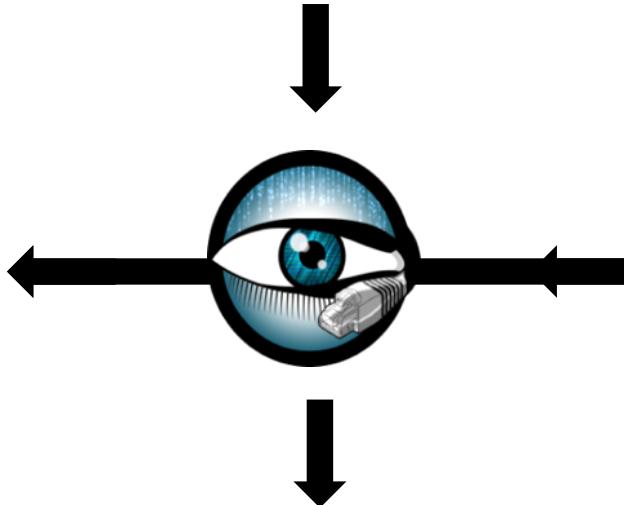


“...people can learn things, and the security issue is not so considered.”



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





**Web
Install**

Sweet Security



**Sensor
Install**

**Full
Install**



**Web
Install**

Sensor

Sensor

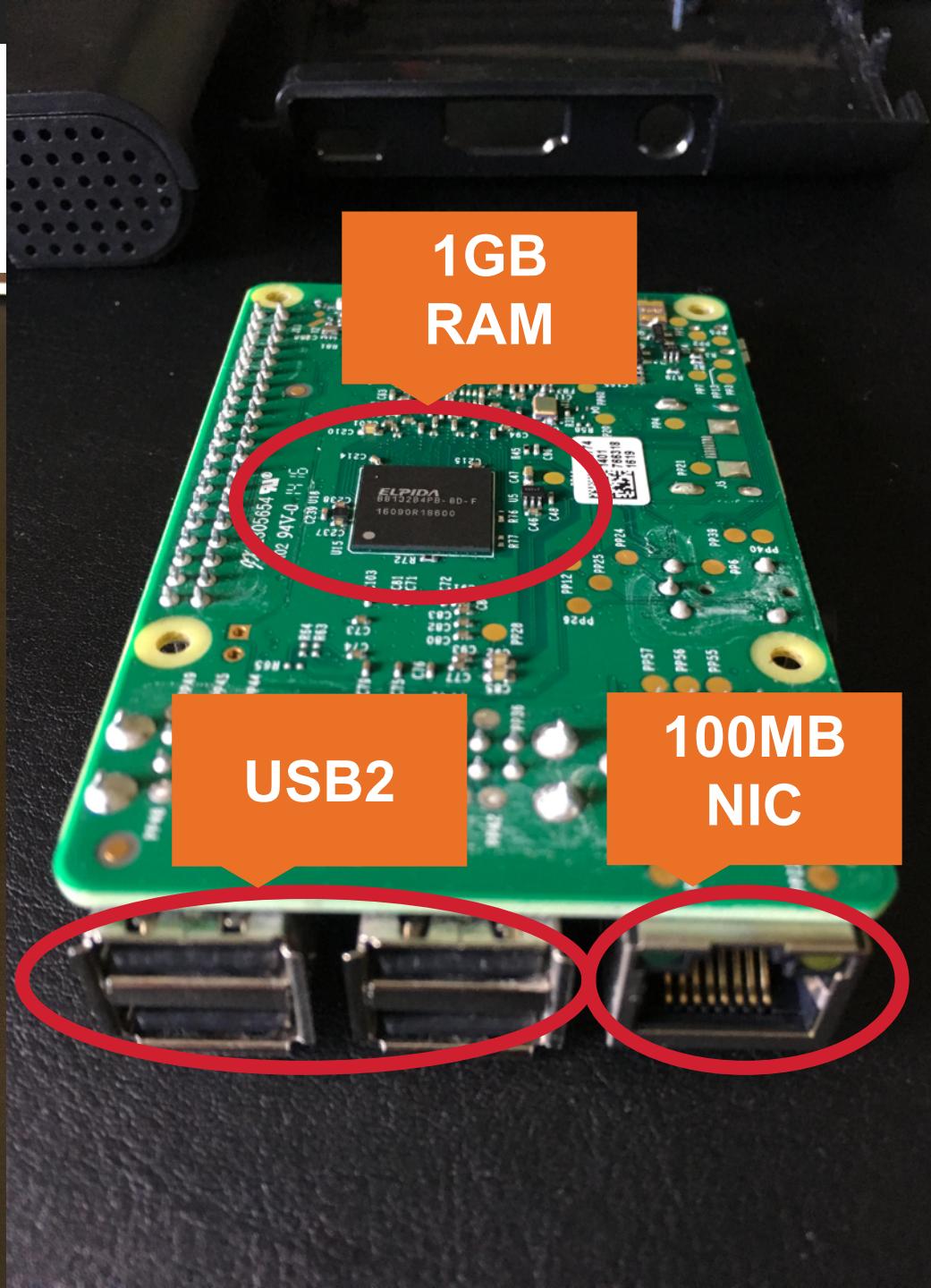
Sensor

Sensor

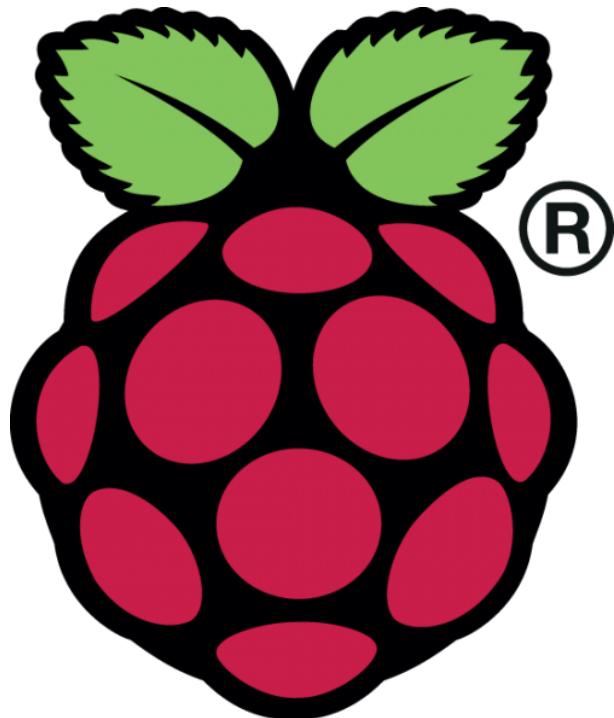
**Sensor
Install**

**Full
Install**

The Pi Problem



Bandwidth Data



Without SweetSecurity

223.22 Mbps



Download

11.85 Mbps



Upload

10.6 ms



Ping

With SweetSecurity

83.47 Mbps



Download

12.16 Mbps



Upload

10.8 ms



Ping

Raspberry Pi w/ USB Gigabit NIC



21.14 Mbps

 Download

12.19 Mbps

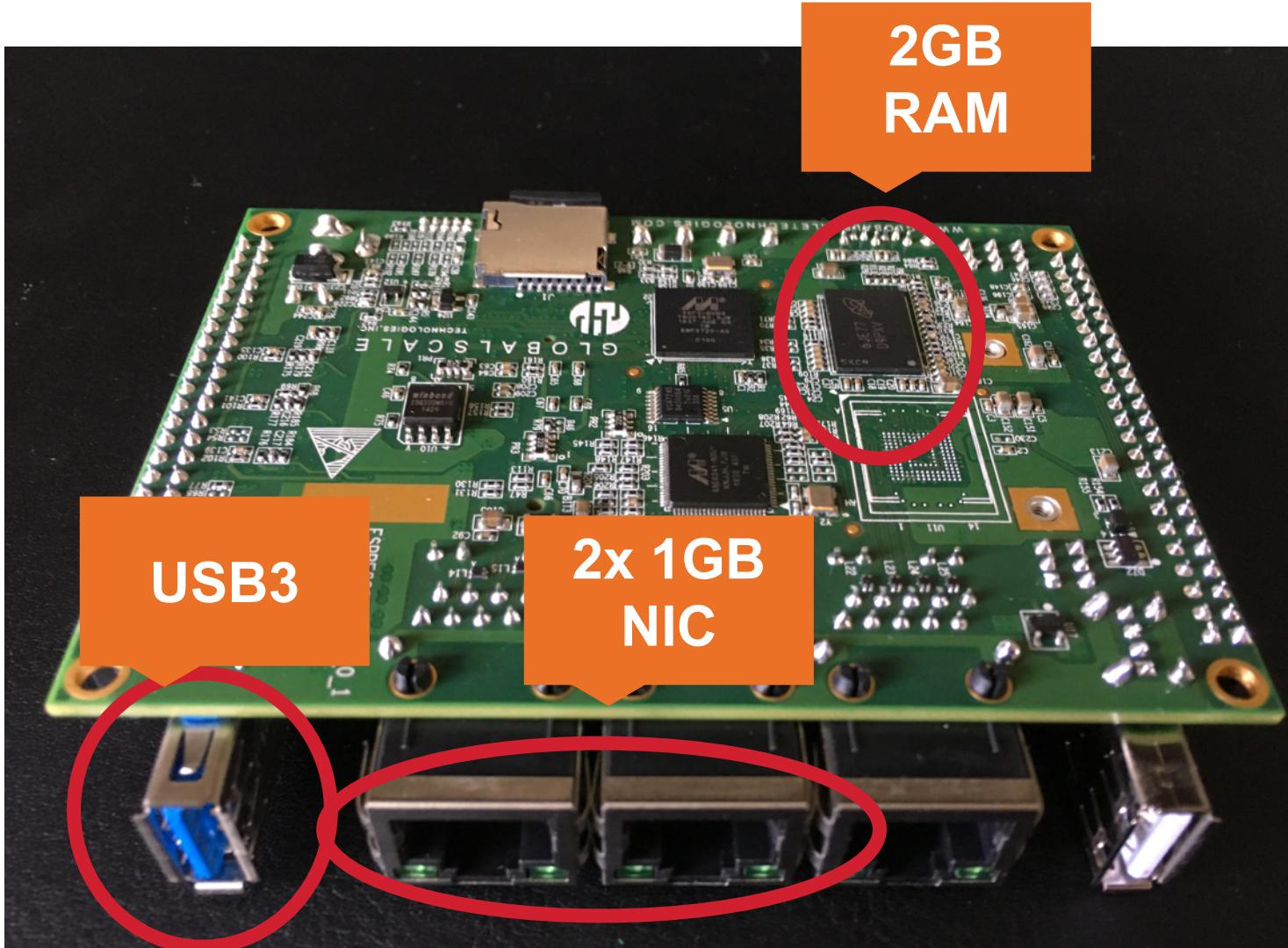
 Upload

11.8 ms

 Ping

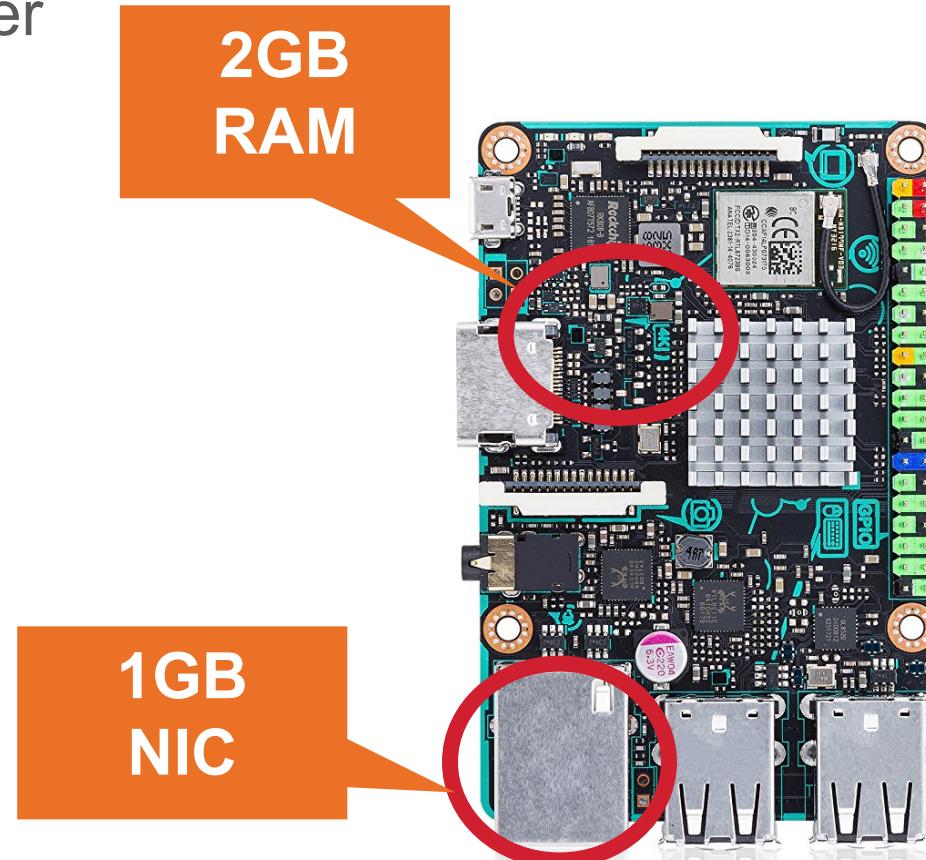
EspressoBIN

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



TinkerBoard

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



Intel NUC

Products Learn & Develop Support



USA (English) Sign In

Products

Features and Benefits

Related Technologies

Related Videos

Related Materials

Support



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



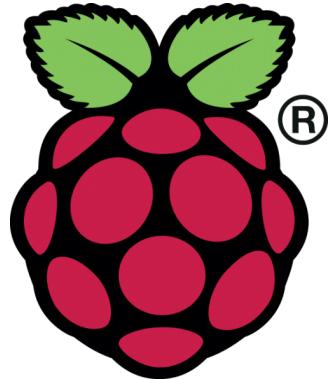
Upload

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



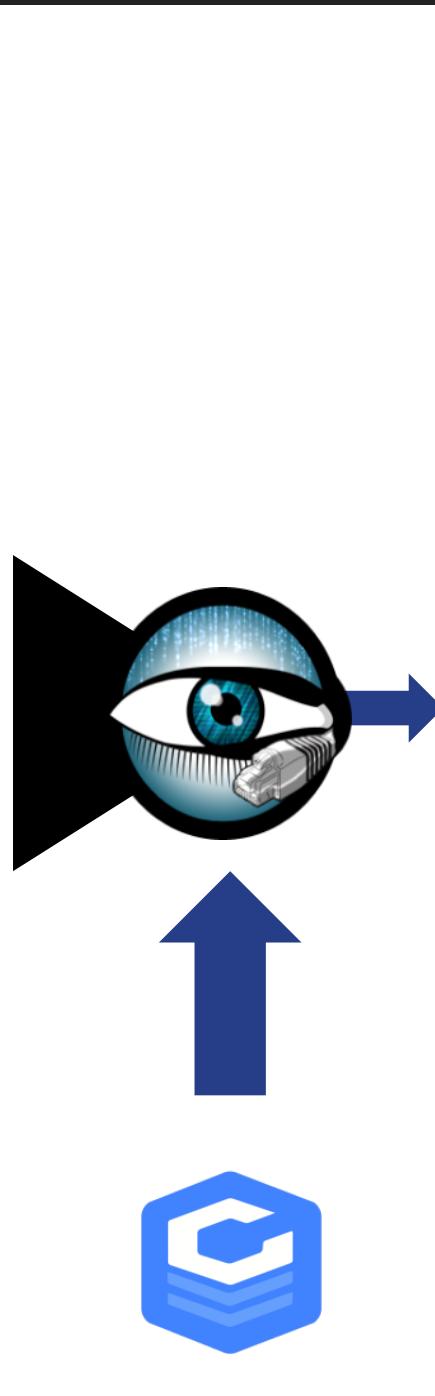
Upload

12.2 ms



Ping

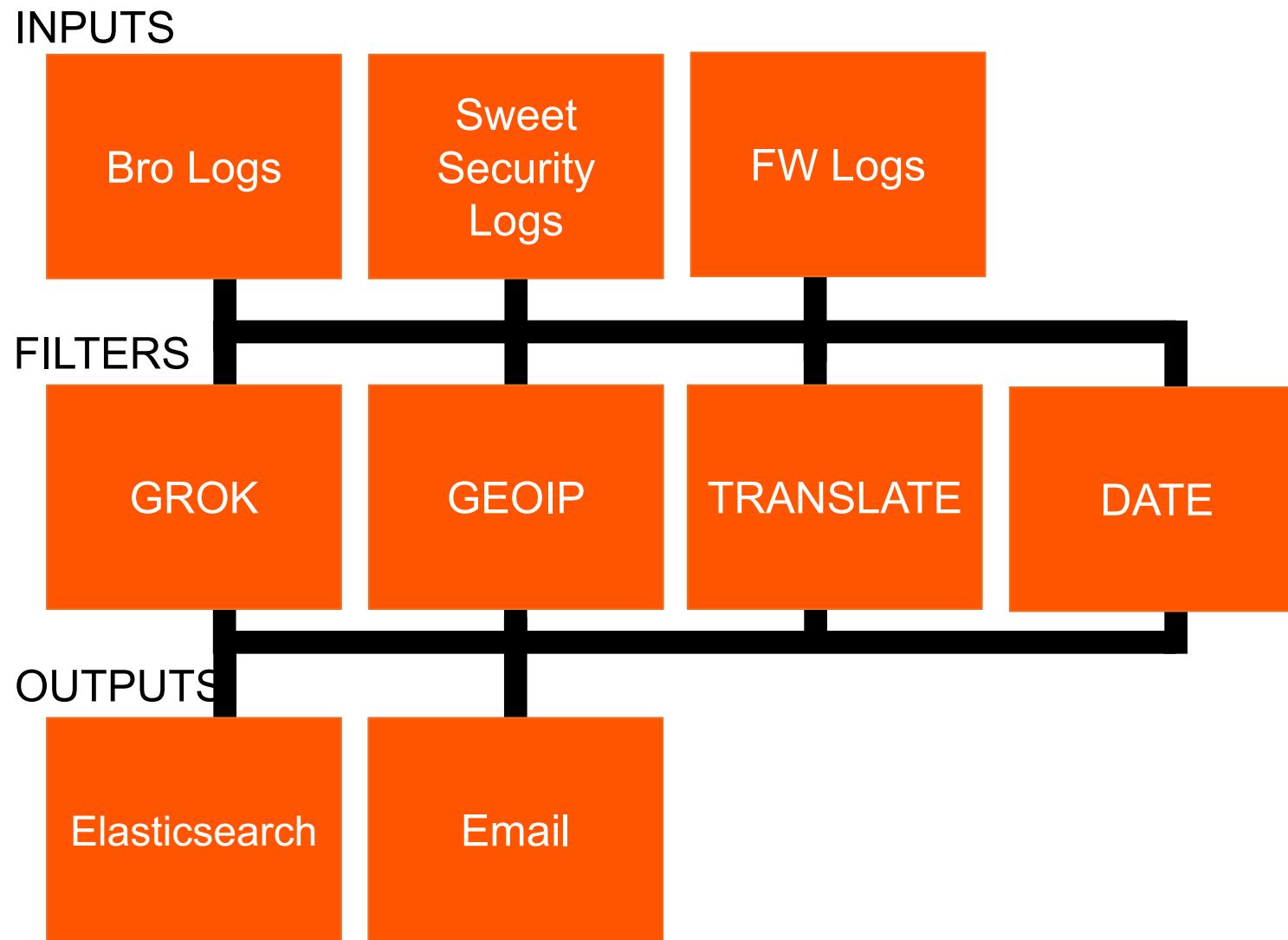
Full Packet Capture



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

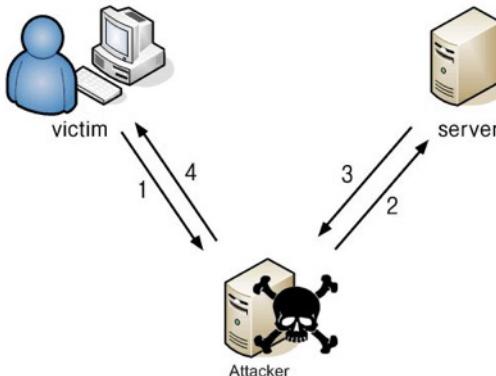
The Details



0:20



0:01



60:00



```
nmap -sn 192.168.1.1/24 -e eth0
```



SweetSecurity.db



```
nmap -sV 192.168.1.2
```

IF ignore==0 AND active==1

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

60:00



MalwareDomainList.com



maliciousIP.yaml

```
"162.247.72.201": "YES"  
"24.187.20.8": "YES"  
"193.34.117.51": "YES"
```



60:00



check.torproject.org/exit-addresses



torIP.yaml

```
"162.247.72.201": "YES"  
"24.187.20.8": "YES"  
"193.34.117.51": "YES"
```

Sensor Management / Health

00:05



<http://webPortal/getConfig>



05:00

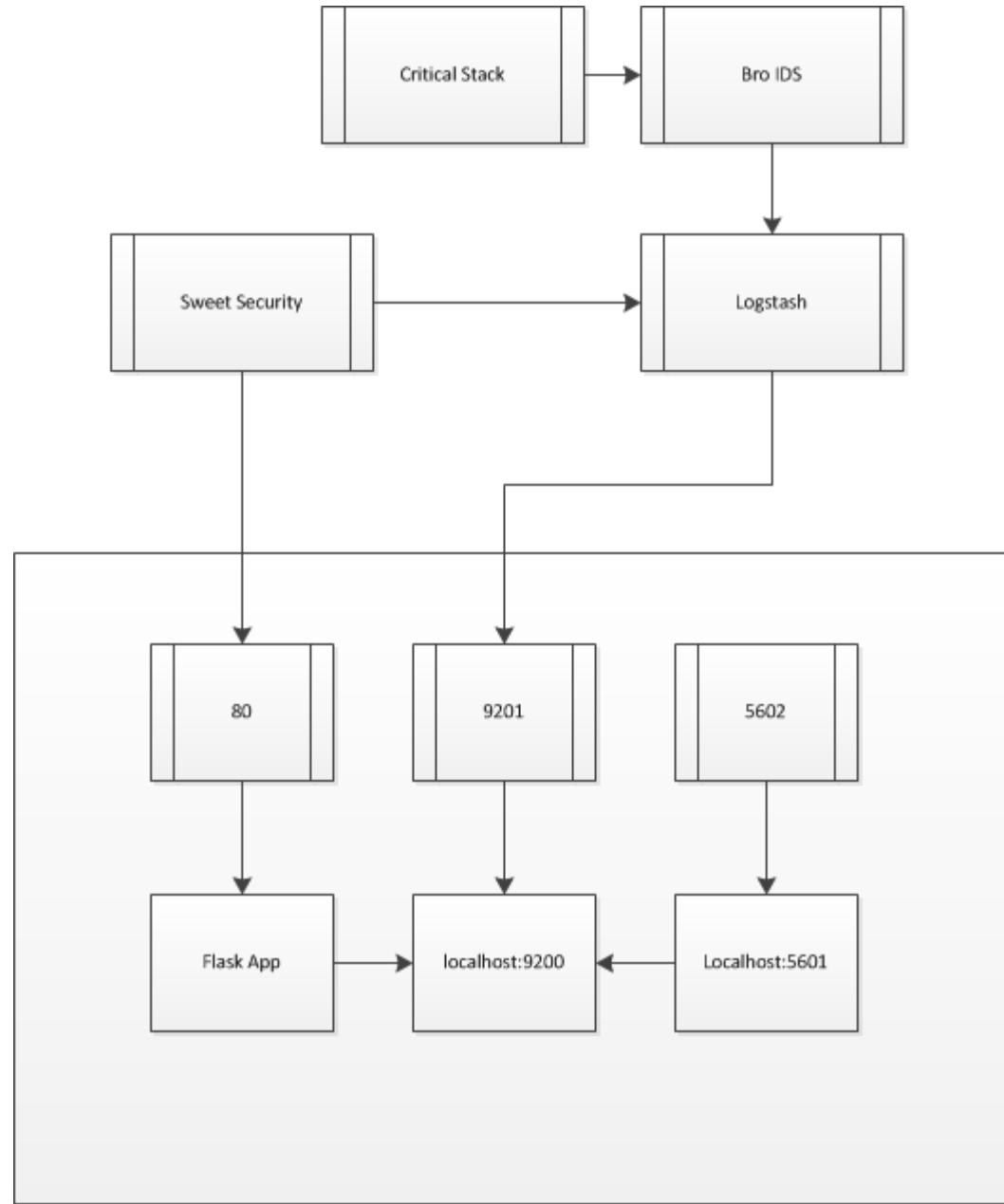


<http://webPortal/healthCheck>

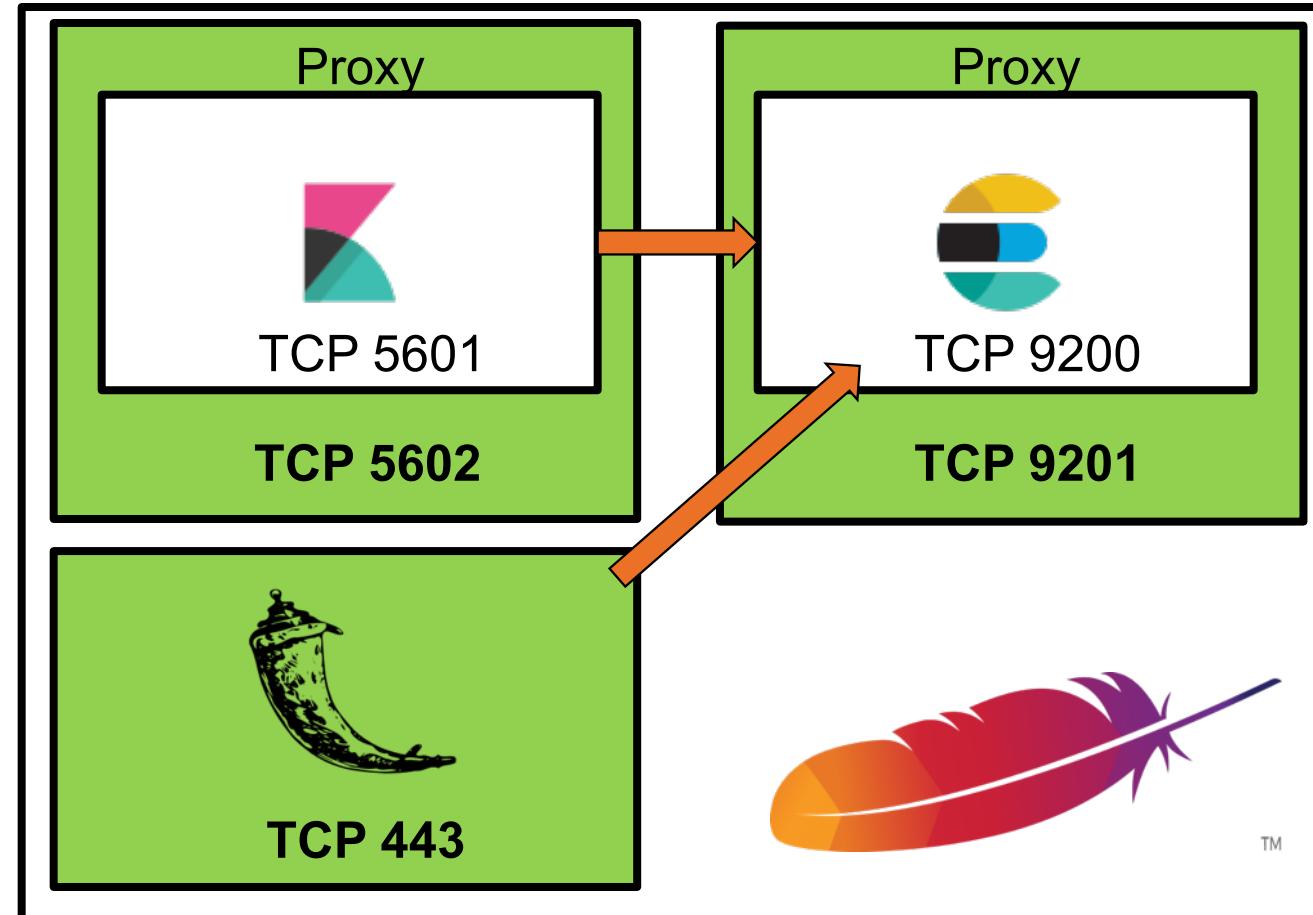


hostname	nickname	ip4	mac	vendor	ignore	active
iPhone.lan	iPhone	192.168.1.2	00:11:22:33:44:55:66	Apple	0	0
therm.lan	Thermostat	192.168.1.3	aa:bb:cc:dd:ee:ff	Google	0	1
mac.lan	Macbook	192.168.1.4	01:23:45:67:89:0a	Apple	1	1
tstr9412.lan	Toaster	192.168.1.5	no:ta:re:al:ma:c!	KitchenAid	0	1

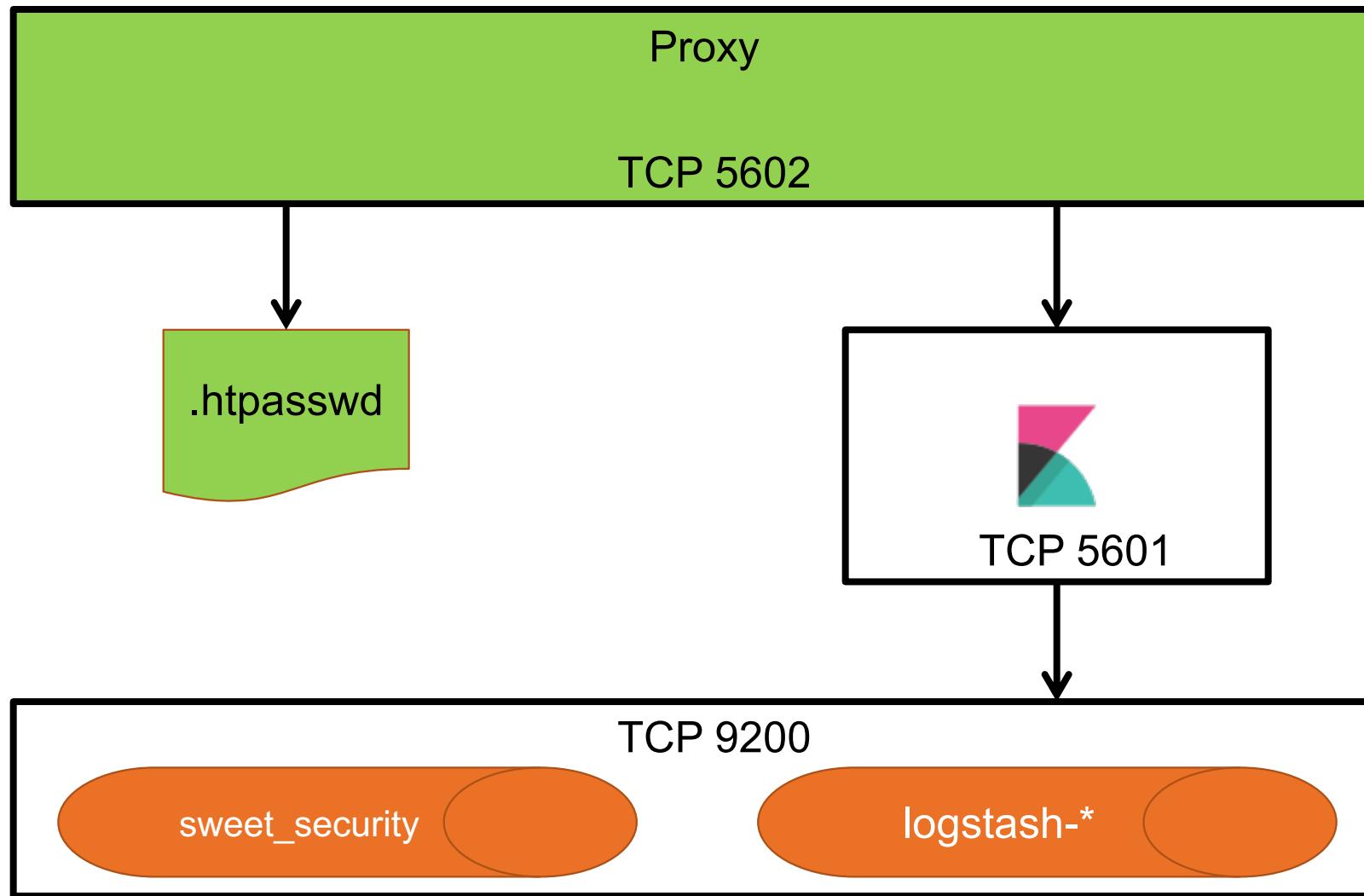




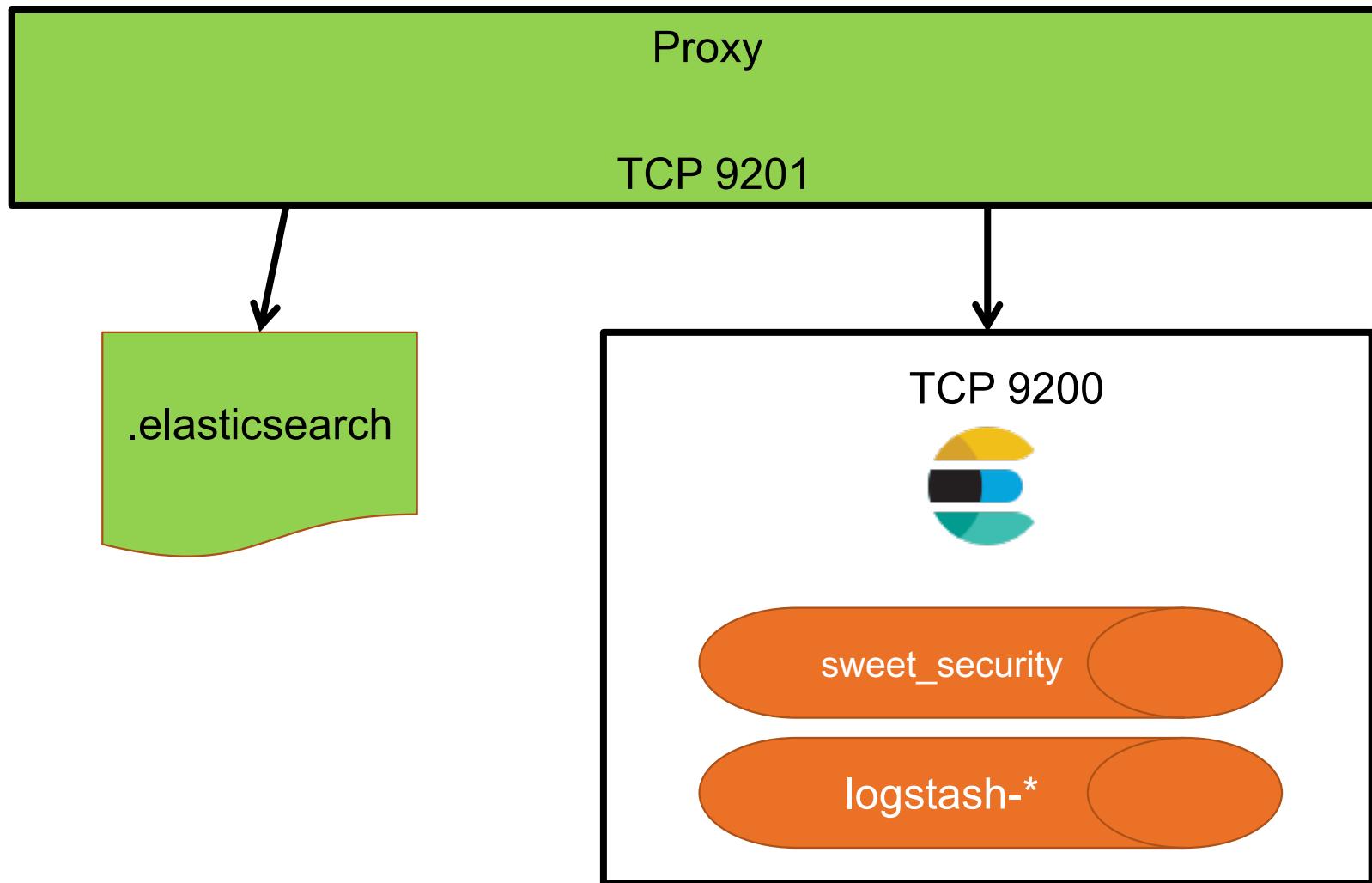
Web Portal Communication



Kibana Architecture



Elasticsearch Architecture



Web Portal Home Page

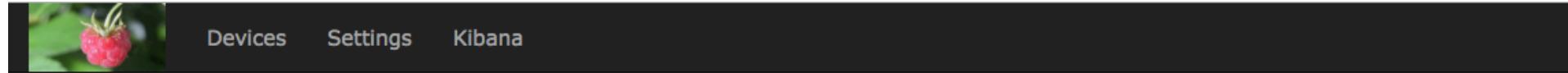


Devices Settings Kibana

Welcome to Sweet Security

There have been no devices discovered yet. Head over to settings tab to make sure everything is running properly.

Web Portal Home Page



Macbook



IP: 192.168.1.4

Vendor: Apple

Firewall: ACCEPT

Open Ports: 0

Monitored: No

[More Info...](#)

Toaster



IP: 192.168.1.5

Vendor: KitchenAid

Firewall: ACCEPT

Open Ports: 0

Monitored: Yes

[More Info...](#)

iPhone



IP: 192.168.1.2

Vendor: Apple

Firewall: ACCEPT

Open Ports: 0

Monitored: Yes

[More Info...](#)

Thermostat



IP: 192.168.1.3

Vendor: Google

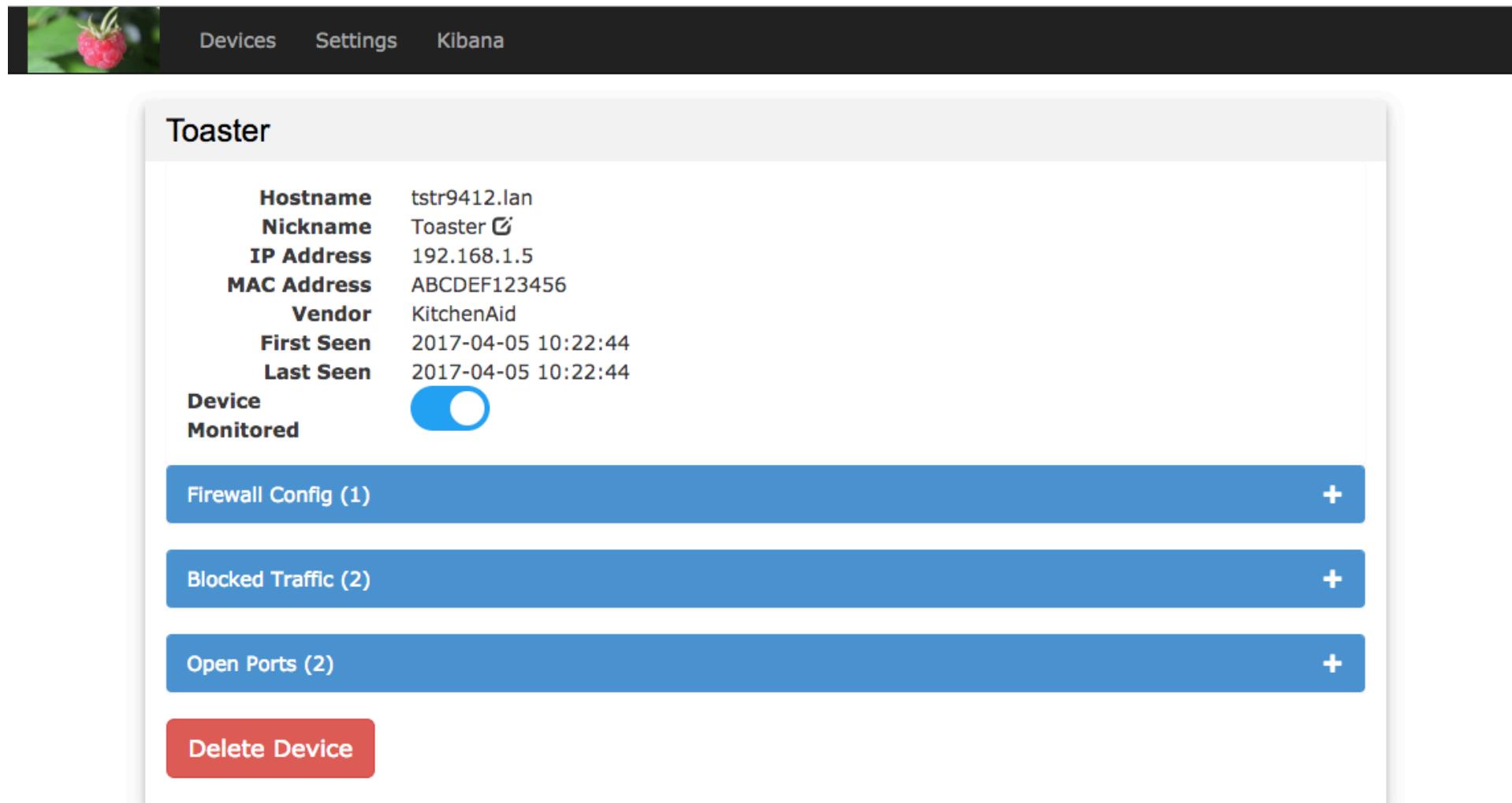
Firewall: ACCEPT

Open Ports: 0

Monitored: Yes

[More Info...](#)

Device Details Page



The screenshot shows a device details page for a "Toaster". The top navigation bar includes a logo, "Devices", "Settings", and "Kibana". The main content area displays the device's name "Toaster" and its configuration:

Hostname	tstr9412.lan
Nickname	Toaster 
IP Address	192.168.1.5
MAC Address	ABCDEF123456
Vendor	KitchenAid
First Seen	2017-04-05 10:22:44
Last Seen	2017-04-05 10:22:44

A toggle switch labeled "Device Monitored" is turned on. Below the configuration, there are three expandable sections:

- Firewall Config (1)** 
- Blocked Traffic (2)** 
- Open Ports (2)** 

A red "Delete Device" button is located at the bottom left.

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

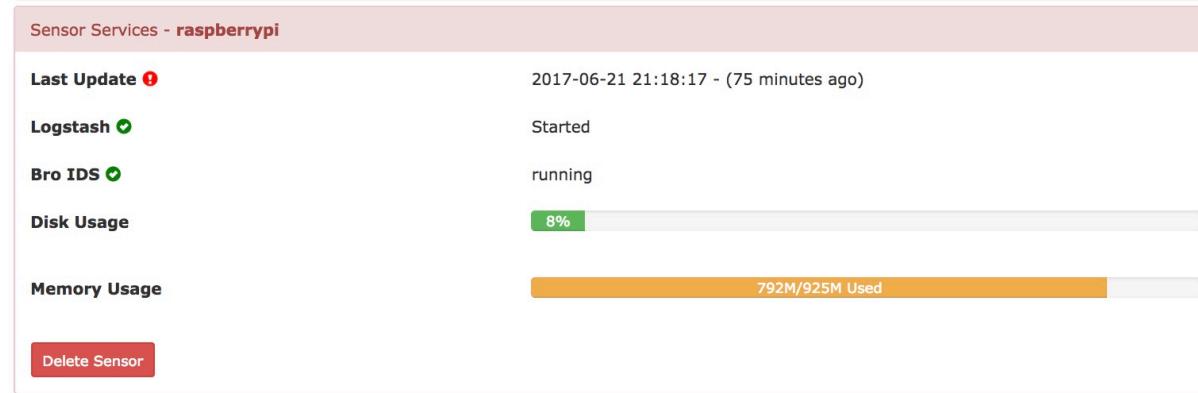
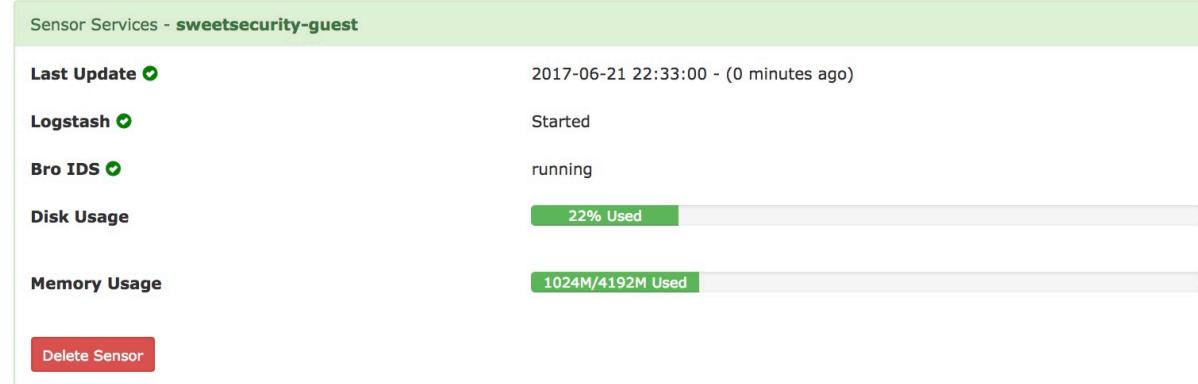
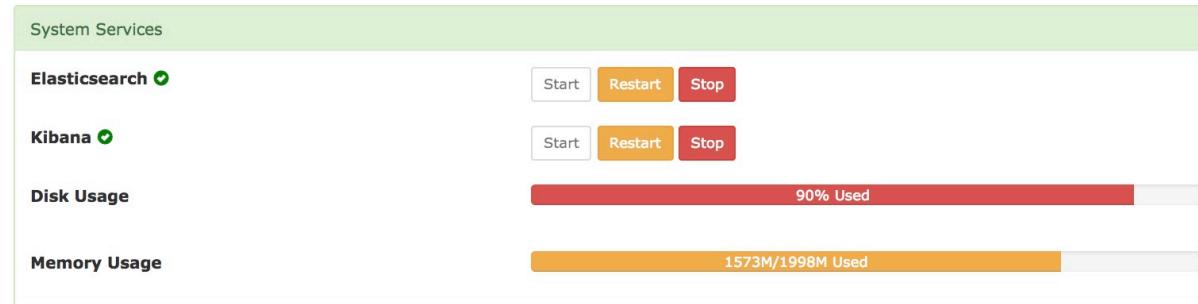
Firewall Configuration

Firewall Config (2)		
Destination	Action	
4.3.2.1	ACCEPT	<button>Delete</button>
kitchenaid.com	ACCEPT	<button>Delete</button>
All	DROP	<button>Edit</button>

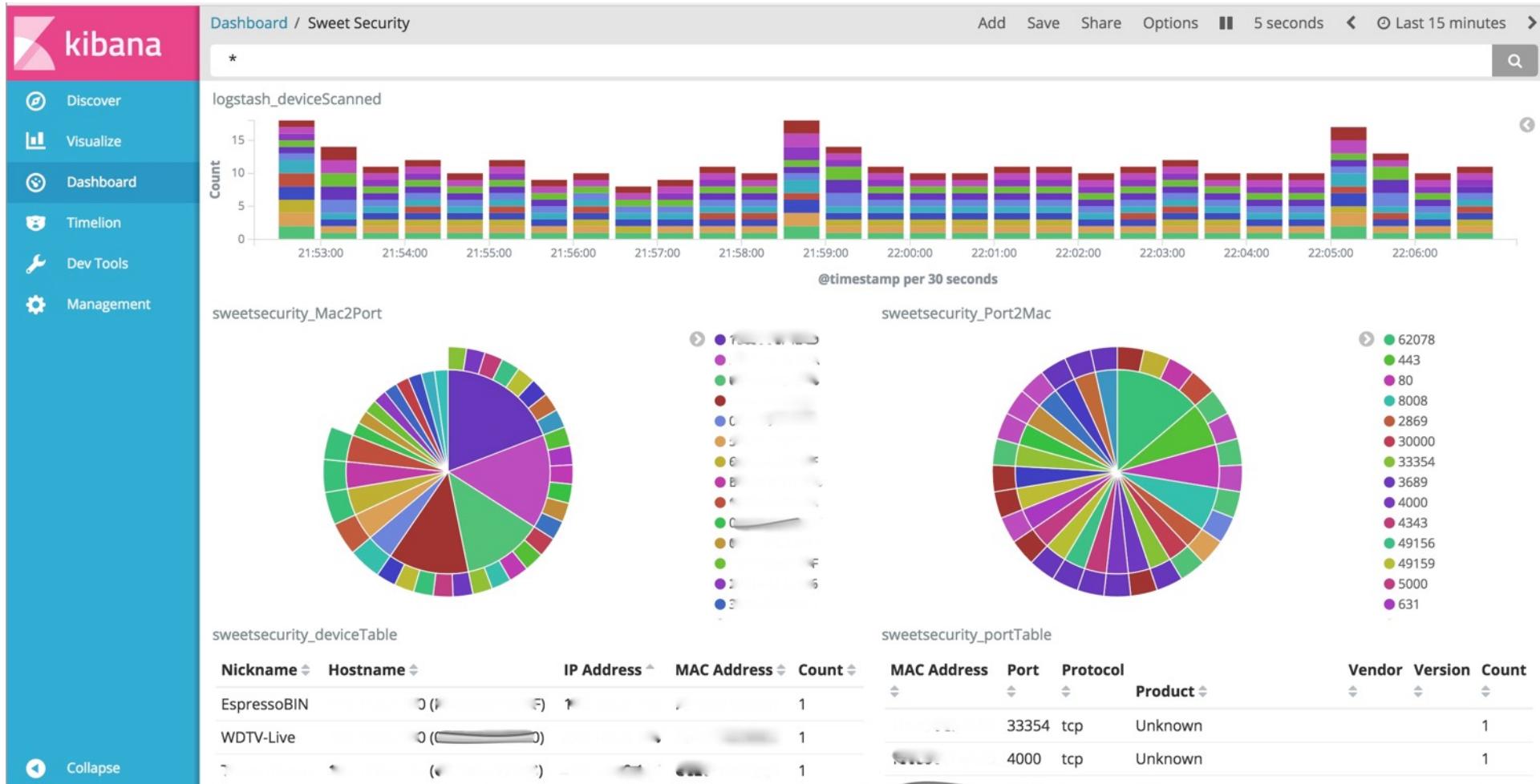
[Add Firewall Entry](#)

Blocked Traffic (2)	
IP Address	Known URLs
1.2.3.4	haxordurl.ru
4.3.2.1	toasterrecipes.com

System Health

[Devices](#) [Settings](#) [Kibana](#)

Device Insights



Device Insights

kibana

- Discover
- Visualize
- Dashboard**
- Timelion
- Dev Tools
- Management

logstash_deviceScanned

sweetsecurity_Mac2Port

sweetsecurity_Port2Mac

sweetsecurity_deviceTable

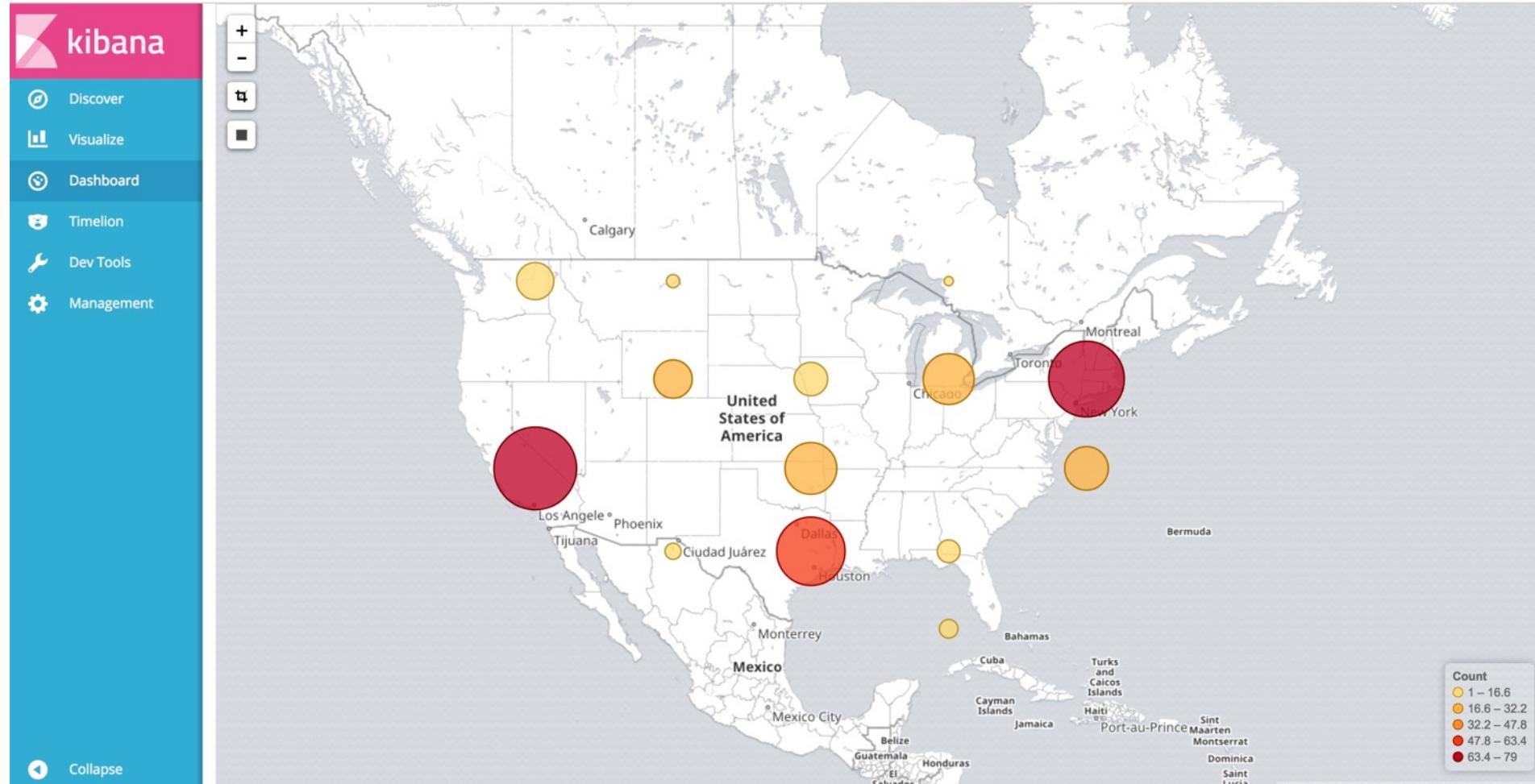
Nickname	Hostname	IP Address	MAC Address	Count
HP Printer	192.168.1.6 (JST-1000A)	192.168.1.6	00:0c:29:00:00:01	1

sweetsecurity_portTable

MAC Address	Port	Protocol	Product	Vendor	Version	Count
00:0c:29:00:00:01	443	tcp	HP HTTP Server; HP Officejet 6950 - P4C84A; Serial Number: TNSCM200LX; Built:Thu	HP		1
00:0c:29:00:00:01	631	tcp	HP HTTP Server; HP Officejet 6950 - P4C84A-	HP		1

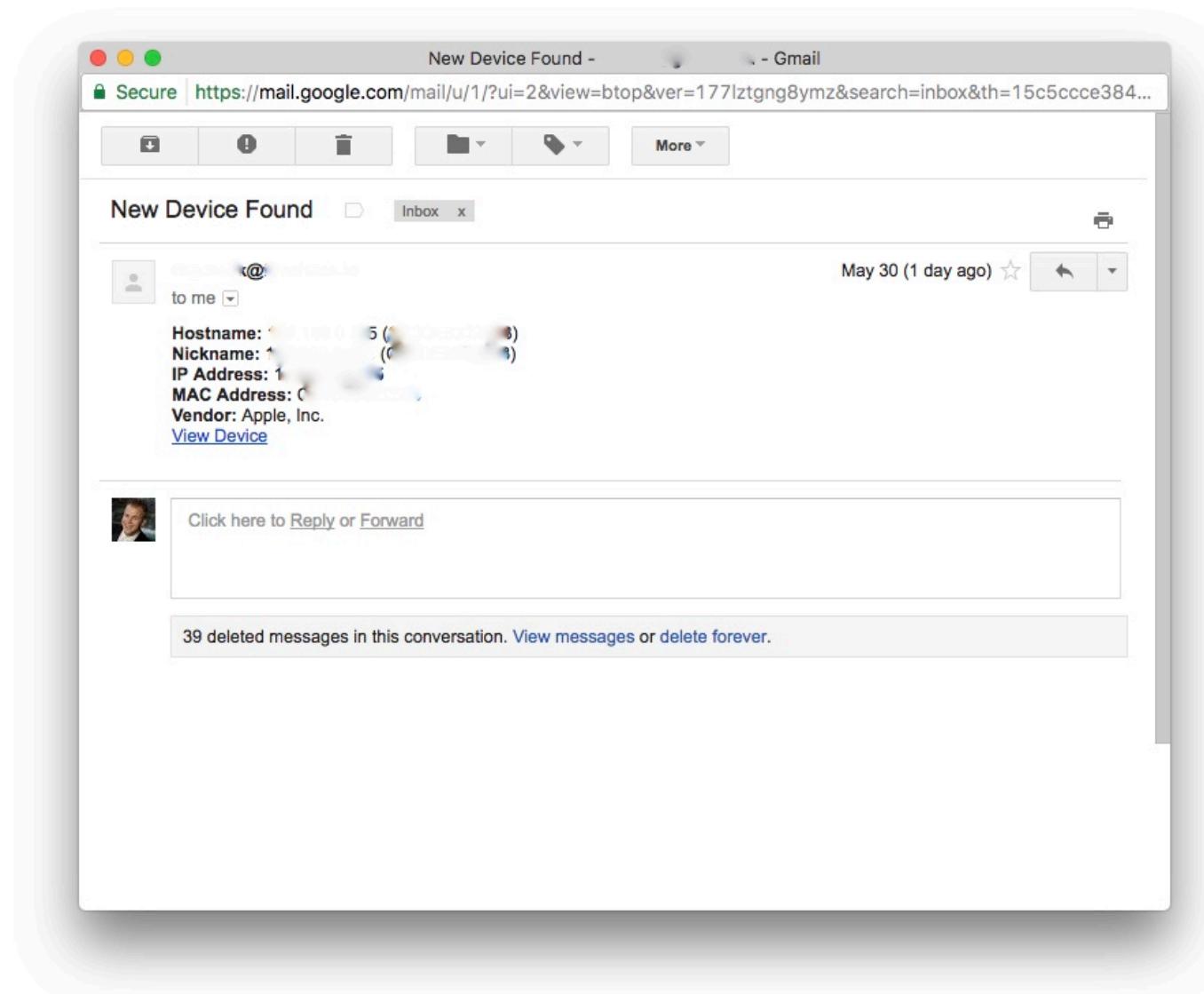
Collapse

GeolP Location



Threat Hunting w/ Sweet Security

Threat Hunting: Rogue Devices

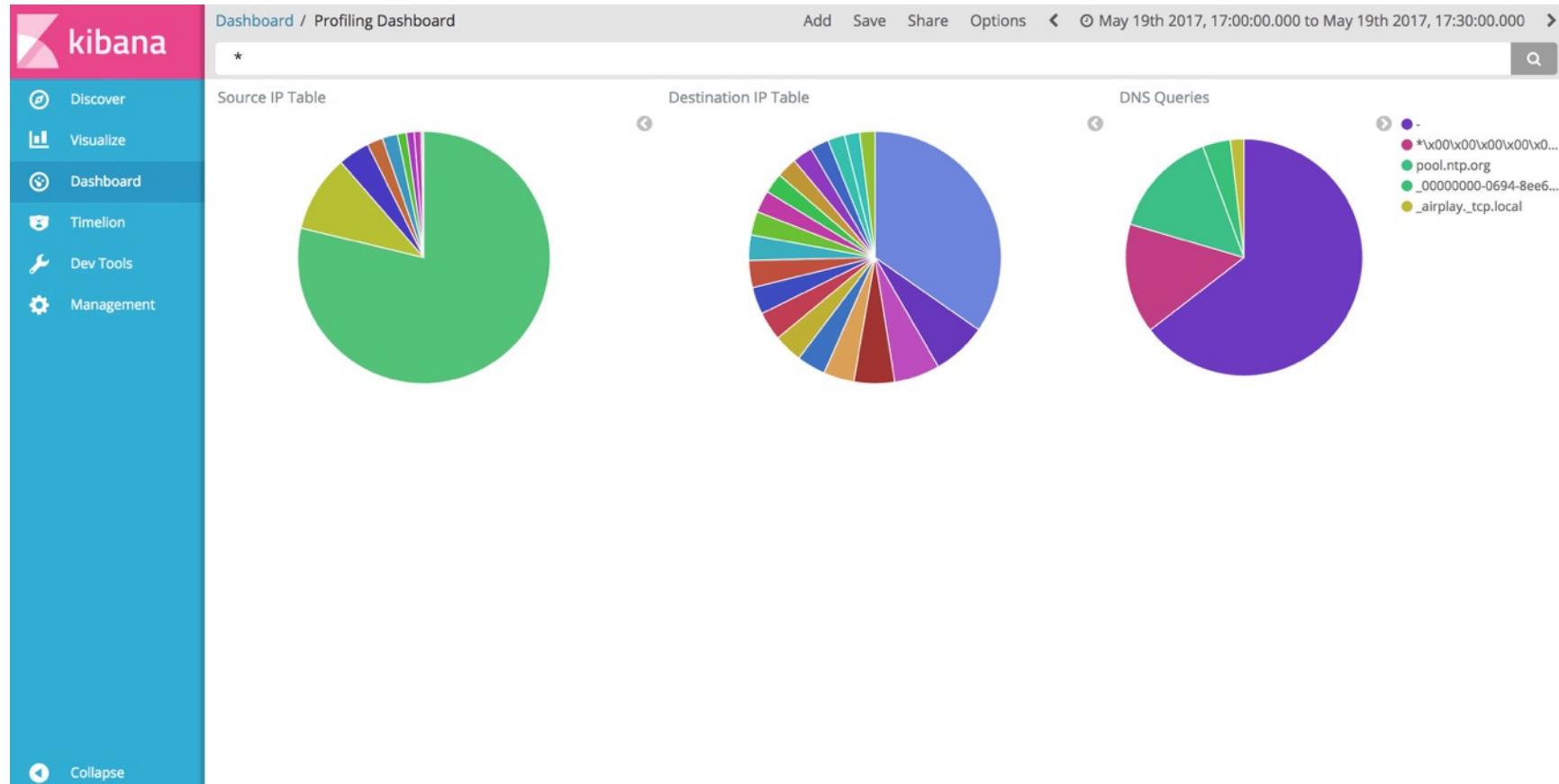


Threat Hunting: Amazon Echo

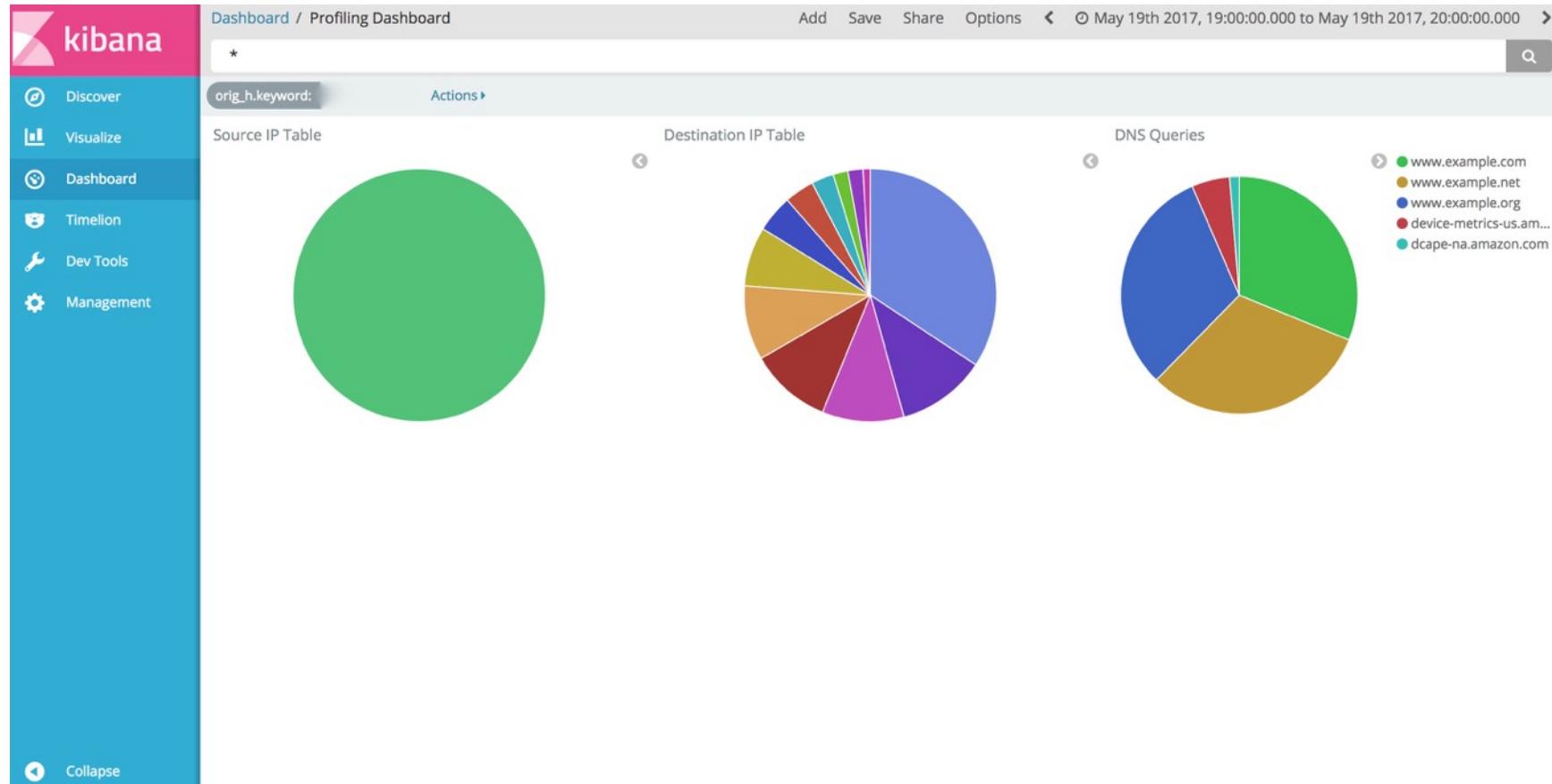
- ◆ Detecting activity to "interesting" domains



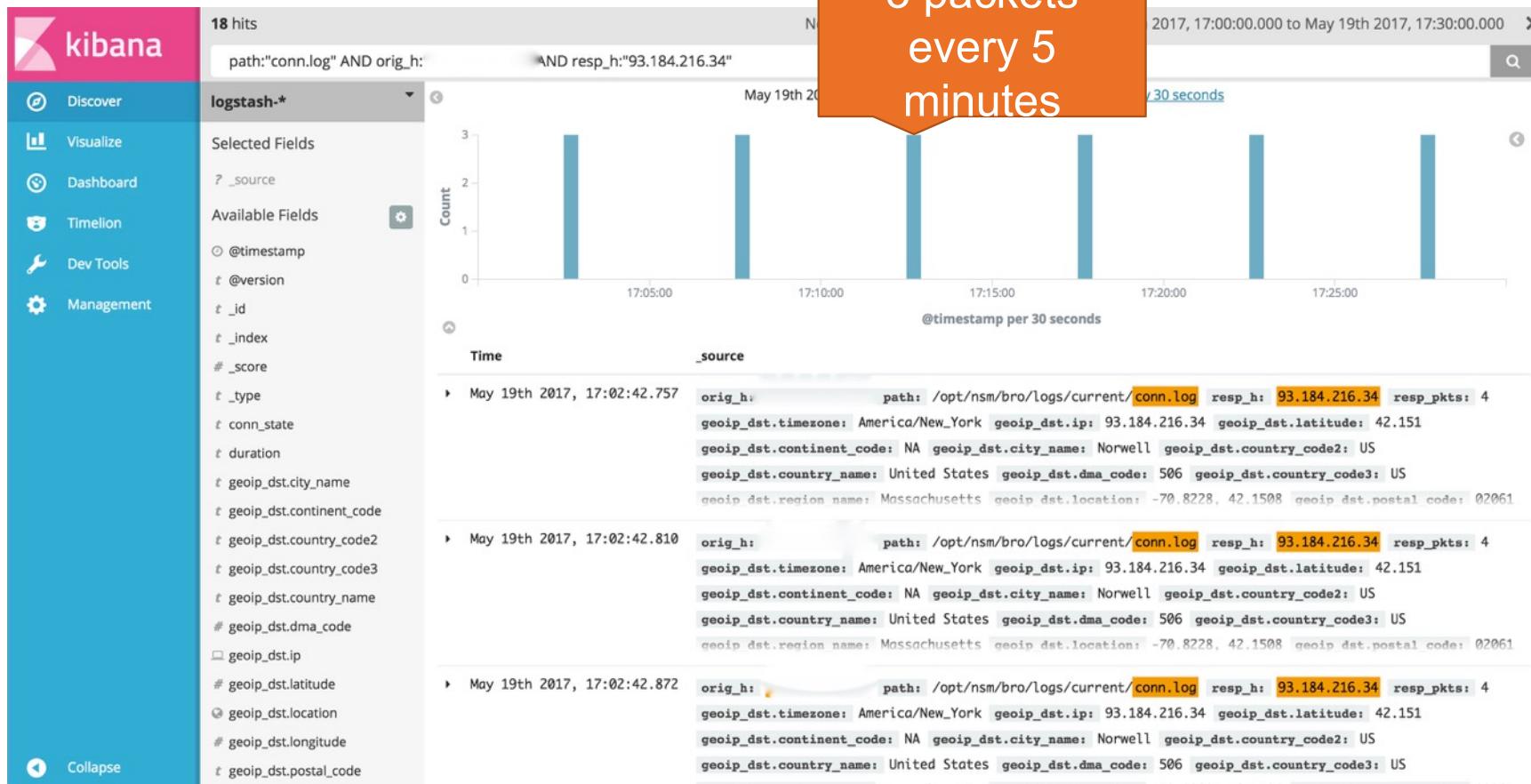
Threat Hunting: Amazon Echo



Threat Hunting: Amazon Alexa



Threat Hunting: Amazon Alexa

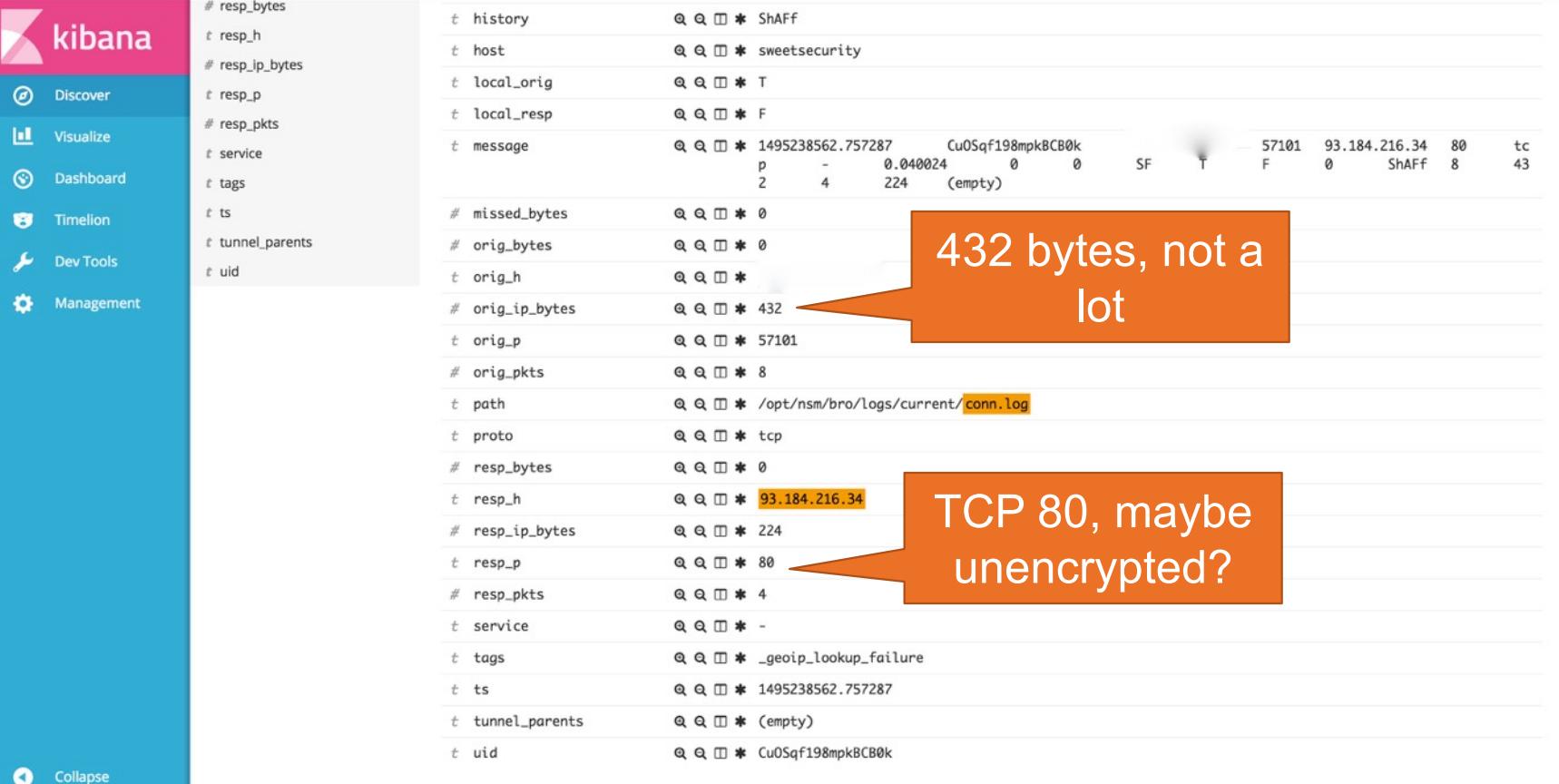


Threat Hunting: Amazon Alexa

The screenshot shows the Kibana Discover interface with a sidebar on the left containing navigation links: Discover, Visualize, Dashboard, Timeline, Dev Tools, and Management. A 'Collapse' button is at the bottom of the sidebar. The main area displays a list of log entries from the 'logstash-2017.05.20' index. Each entry includes a timestamp, version, ID, index, score, type, and various geoip and host fields. The geoip fields include country_name, dma_code, ip, latitude, longitude, postal_code, region_code, region_name, timezone, continent_code, country_code2, country_code3, and country_name. The host fields include history, host, local_orig, local_resp, message, missed_bytes, orig_bytes, orig_h, orig_ip_bytes, orig_p, orig_pkts, path, proto, resp_bytes, resp_h, resp_ip_bytes, and resp_n.

Field	Value
@timestamp	May 19th 2017, 17:02:42.757
@version	1
_id	AVwjKe0pxupHtbUTJWIM
_index	logstash-2017.05.20
_score	13.247
_type	logs
conn_state	SF
duration	0.040024
geoip_dst.city_name	Norwell
geoip_dst.continent_code	NA
geoip_dst.country_code2	US
geoip_dst.country_code3	US
geoip_dst.country_name	United States
geoip_dst.dma_code	506
geoip_dst.ip	93.184.216.34
geoip_dst.latitude	42.151
geoip_dst.location	-70.8228, 42.1508
geoip_dst.longitude	-70.823
geoip_dst.postal_code	02061
geoip_dst.region_code	MA
geoip_dst.region_name	Massachusetts
geoip_dst.timezone	America/New_York
history	ShAFF
host	sweetsecurity
local_orig	T

Threat Hunting: Amazon Alexa



The screenshot shows the Kibana Discover interface with a sidebar containing navigation links: Discover, Visualize, Dashboard, Timelion, Dev Tools, and Management. The main area displays a table of network log fields and their values. An orange callout highlights the 'orig_ip_bytes' field with the value '432'. Another orange callout highlights the 'resp_h' field with the value '93.184.216.34'.

Field	Value
# resp_bytes	
t resp_h	Q Q D * ShAFF
# resp_ip_bytes	
t resp_p	Q Q D * sweetsecurity
# resp_pkts	
t service	Q Q D * T
t tags	Q Q D * F
t ts	Q Q D * 1495238562.757287
t tunnel_parents	p - 0.040024 Cu0Sqf198mpkBCB0k
t uid	2 4 224 (empty) SF T 57101 F 93.184.216.34 80 tc 43
# missed_bytes	Q Q D * 0
# orig_bytes	Q Q D * 0
t orig_h	Q Q D *
# orig_ip_bytes	Q Q D * 432
t orig_p	Q Q D * 57101
# orig_pkts	Q Q D * 8
t path	Q Q D * /opt/nsm/bro/logs/current/conn.log
t proto	Q Q D * tcp
# resp_bytes	Q Q D * 0
t resp_h	Q Q D * 93.184.216.34
# resp_ip_bytes	Q Q D * 224
t resp_p	Q Q D * 80
# resp_pkts	Q Q D * 4
t service	Q Q D * -
t tags	Q Q D * _geoip_lookup_failure
t ts	Q Q D * 1495238562.757287
t tunnel_parents	Q Q D * (empty)
t uid	Q Q D * Cu0Sqf198mpkBCB0k

Threat Hunting: Amazon Alexa

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

Not actually
HTTP, bummer.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	93.184.216.34	93.184.216.34	TCP	74	54564 → 80 [SYN] Seq=0 Win=4380 Len=0 MSS=1460 SACK_PERM=1 TSval=128182269 TSecr=0 WS=16
2	0.002242	93.184.216.34	93.184.216.34	TCP	74	[TCP Out-Of-Order] 54564 → 80 [SYN] Seq=0 Win=4380 Len=0 MSS=1460 SACK_PERM=1 TSval=128182269 TSecr=0 ..
3	0.022370	93.184.216.34	93.184.216.34	TCP	66	54564 → 80 [ACK] Seq=1 Ack=1 Win=4384 Len=0 TSval=128182275 TSecr=468041848
4	0.025239	93.184.216.34	93.184.216.34	TCP	66	[TCP Dup ACK 3#1] 54564 → 80 [ACK] Seq=1 Ack=1 Win=4384 Len=0 TSval=128182275 TSecr=468041848
5	0.025266	93.184.216.34	93.184.216.34	TCP	66	54564 → 80 [FIN, ACK] Seq=1 Ack=1 Win=4384 Len=0 TSval=128182275 TSecr=468041848
6	0.028455	93.184.216.34	93.184.216.34	TCP	66	[TCP Out-Of-Order] 54564 → 80 [FIN, ACK] Seq=1 Ack=1 Win=4384 Len=0 TSval=128182275 TSecr=468041848
7	0.053535	93.184.216.34	93.184.216.34	TCP	66	54564 → 80 [ACK] Seq=2 Ack=2 Win=4384 Len=0 TSval=128182283 TSecr=468041855
8	0.055823	93.184.216.34	93.184.216.34	TCP	66	[TCP Dup ACK 7#1] 54564 → 80 [ACK] Seq=2 Ack=2 Win=4384 Len=0 TSval=128182283 TSecr=468041855
9	0.069205	93.184.216.34	93.184.216.34	TCP	74	54565 → 80 [SYN] Seq=0 Win=4380 Len=0 MSS=1460 SACK_PERM=1 TSval=128182287 TSecr=0 WS=16
10	0.070587	93.184.216.34	93.184.216.34	TCP	74	[TCP Out-Of-Order] 54565 → 80 [SYN] Seq=0 Win=4380 Len=0 MSS=1460 SACK_PERM=1 TSval=128182287 TSecr=0 ..
11	0.092892	93.184.216.34	93.184.216.34	TCP	66	54565 → 80 [ACK] Seq=1 Ack=1 Win=4384 Len=0 TSval=128182293 TSecr=952985750
12	0.094754	93.184.216.34	93.184.216.34	TCP	66	[TCP Dup ACK 11#1] 54565 → 80 [ACK] Seq=1 Ack=1 Win=4384 Len=0 TSval=128182293 TSecr=952985750
13	0.095805	93.184.216.34	93.184.216.34	TCP	66	54565 → 80 [FIN, ACK] Seq=1 Ack=1 Win=4384 Len=0 TSval=128182293 TSecr=952985750
14	0.097437	93.184.216.34	93.184.216.34	TCP	66	[TCP Out-Of-Order] 54565 → 80 [FIN, ACK] Seq=1 Ack=1 Win=4384 Len=0 TSval=128182293 TSecr=952985750
15	0.119897	93.184.216.34	93.184.216.34	TCP	66	54565 → 80 [ACK] Seq=2 Ack=2 Win=4384 Len=0 TSval=128182300 TSecr=952985757
16	0.121825	93.184.216.34	93.184.216.34	TCP	66	[TCP Dup ACK 15#1] 54565 → 80 [ACK] Seq=2 Ack=2 Win=4384 Len=0 TSval=128182300 TSecr=952985757
17	0.133045	93.184.216.34	93.184.216.34	TCP	74	54566 → 80 [SYN] Seq=0 Win=4380 Len=0 MSS=1460 SACK_PERM=1 TSval=128182303 TSecr=0 WS=16
18	0.134719	93.184.216.34	93.184.216.34	TCP	74	[TCP Out-Of-Order] 54566 → 80 [SYN] Seq=0 Win=4380 Len=0 MSS=1460 SACK_PERM=1 TSval=128182303 TSecr=0 ..
19	0.158894	93.184.216.34	93.184.216.34	TCP	66	54566 → 80 [ACK] Seq=1 Ack=1 Win=4384 Len=0 TSval=128182310 TSecr=962396928
20	0.160256	93.184.216.34	93.184.216.34	TCP	66	[TCP Dup ACK 19#1] 54566 → 80 [ACK] Seq=1 Ack=1 Win=4384 Len=0 TSval=128182310 TSecr=962396928
21	0.160269	93.184.216.34	93.184.216.34	TCP	66	54566 → 80 [FIN, ACK] Seq=1 Ack=1 Win=4384 Len=0 TSval=128182310 TSecr=962396928
22	0.161823	93.184.216.34	93.184.216.34	TCP	66	[TCP Out-Of-Order] 54566 → 80 [FIN, ACK] Seq=1 Ack=1 Win=4384 Len=0 TSval=128182310 TSecr=962396928
23	0.194163	93.184.216.34	93.184.216.34	TCP	66	54566 → 80 [ACK] Seq=2 Ack=2 Win=4384 Len=0 TSval=128182319 TSecr=962396936
24	0.196008	93.184.216.34	93.184.216.34	TCP	66	[TCP Dup ACK 23#1] 54566 → 80 [ACK] Seq=2 Ack=2 Win=4384 Len=0 TSval=128182319 TSecr=962396936

Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Acknowledgment number: 0
Header Length: 40 bytes

▶ Flags: 0x002 (SYN)
Window size value: 4380
[Calculated window size: 4380]
Checksum: 0x8bc3 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0

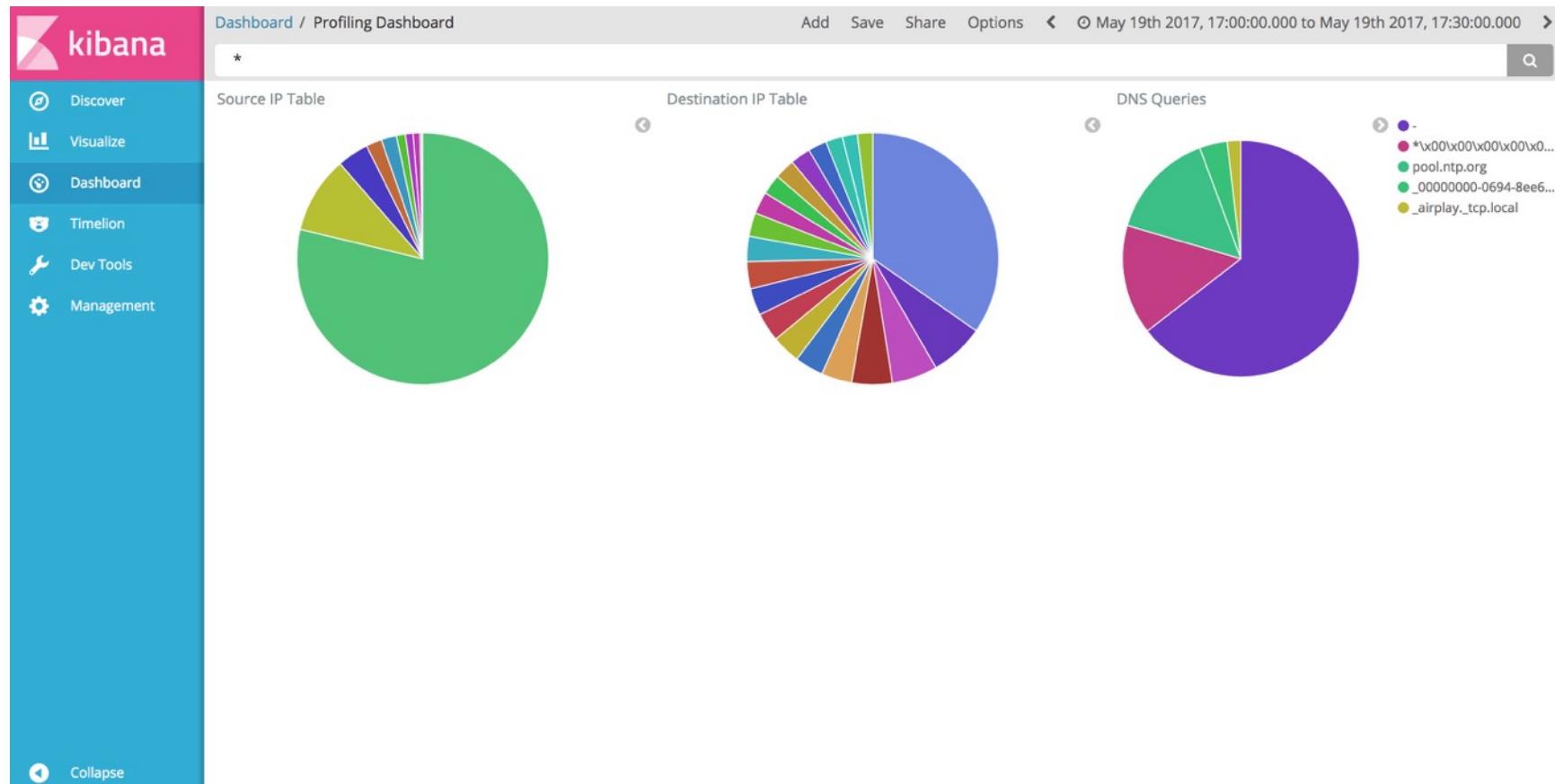
▼ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
▶ Maximum segment size: 1460 bytes

Threat Hunting: WDTVLive

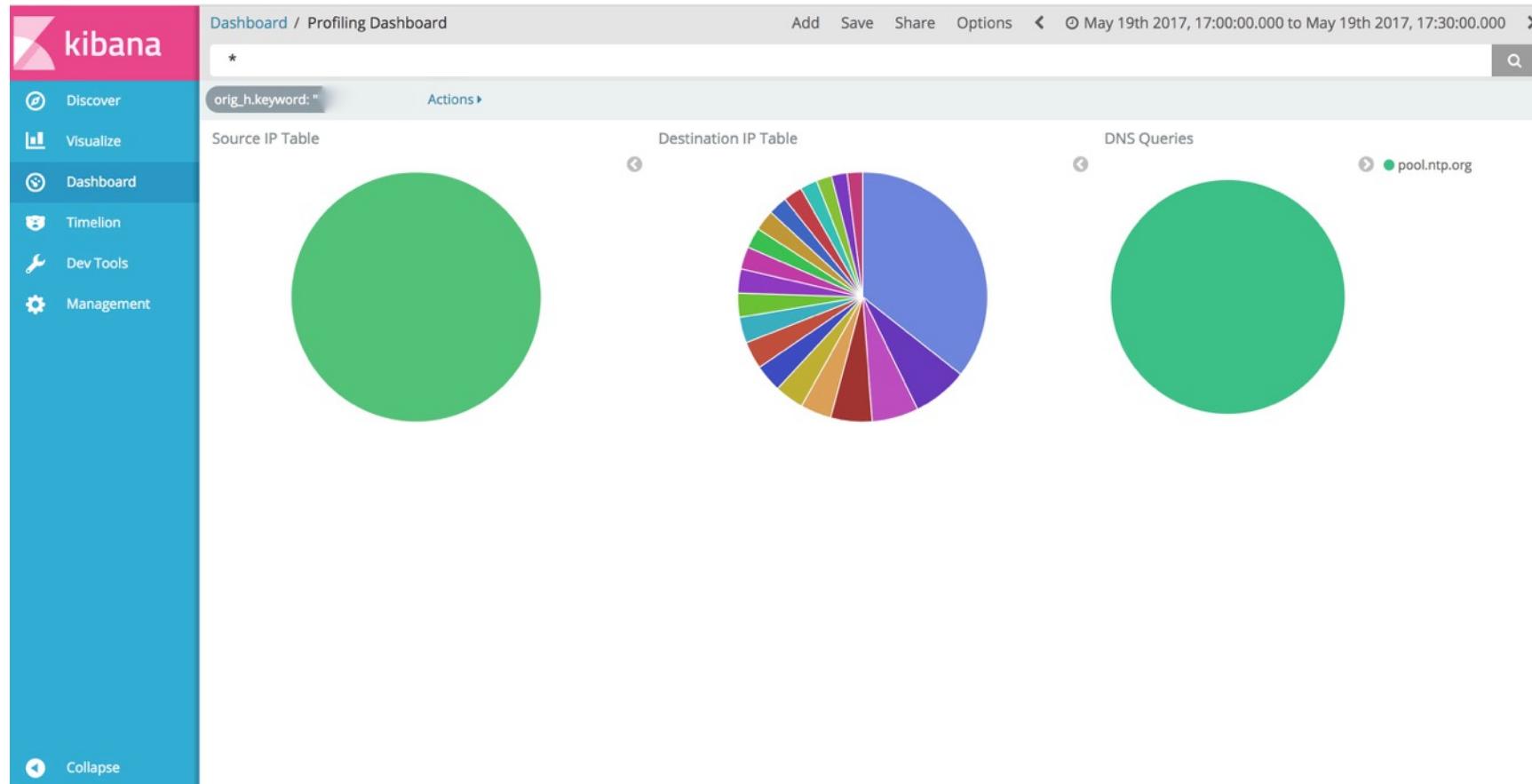
- ◆ Massive amounts of NTP traffic



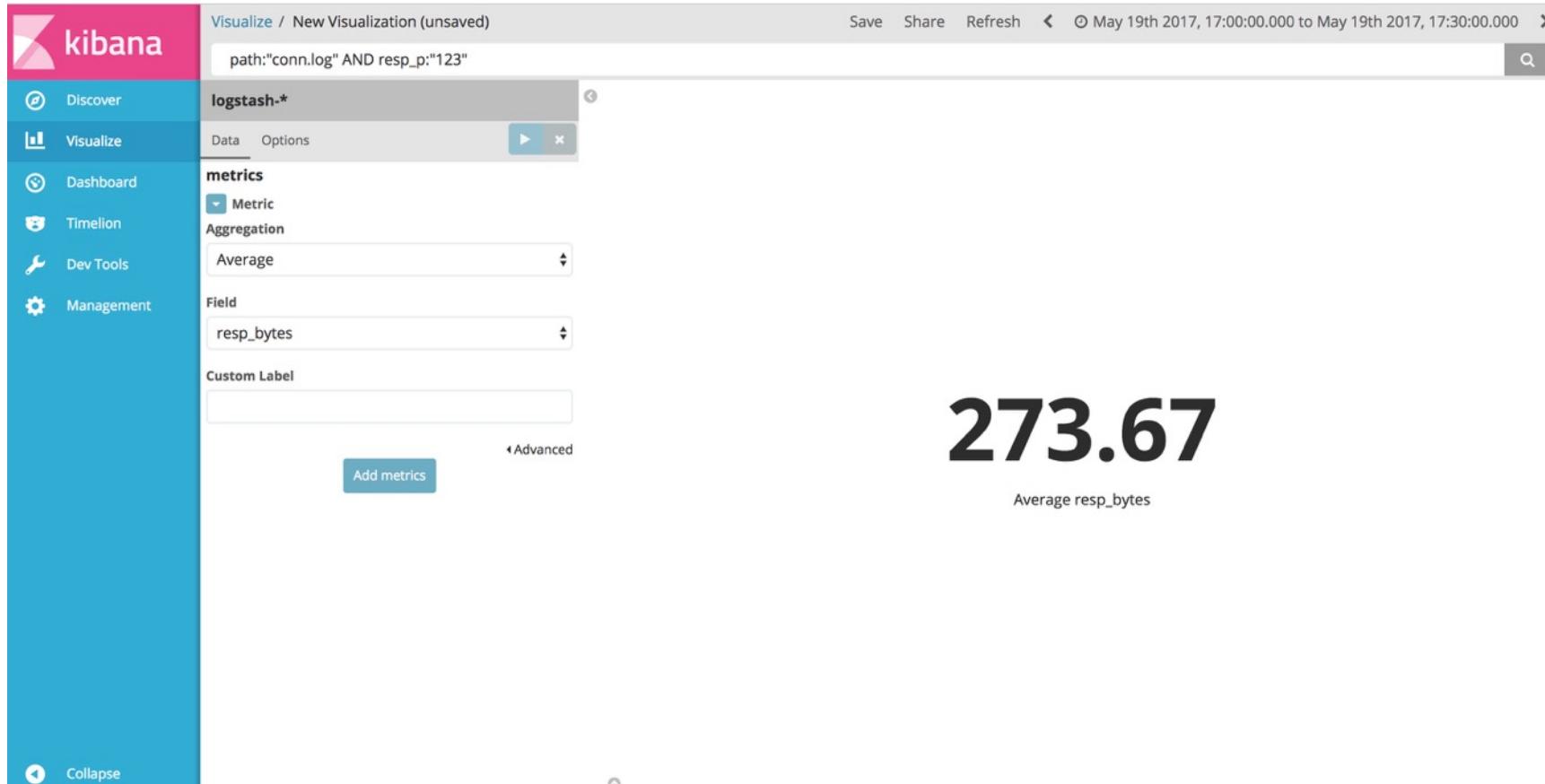
Threat Hunting: WDTVLive



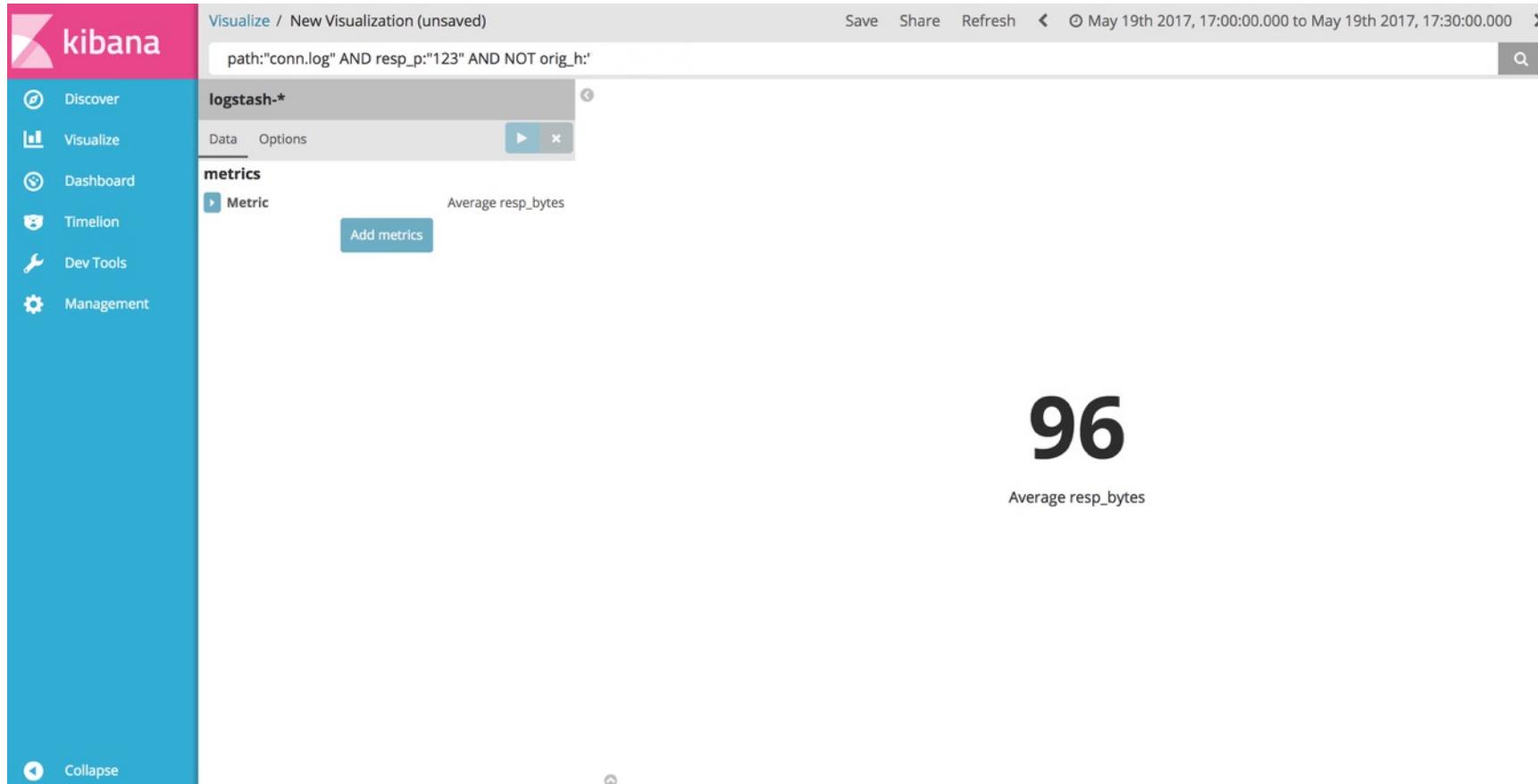
Threat Hunting: WDTVLive



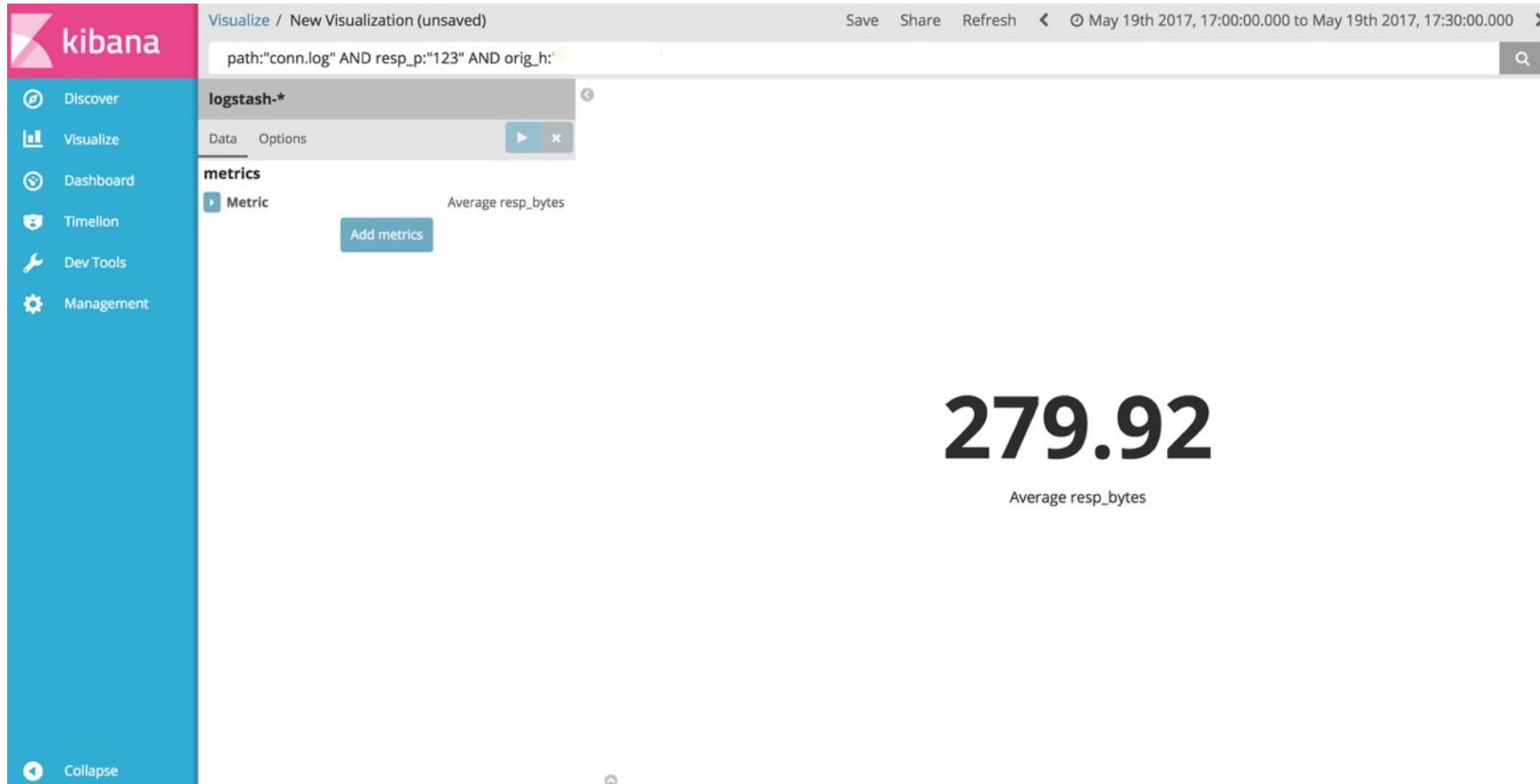
Threat Hunting: WDTVLive



Threat Hunting: WDTVLive



Threat Hunting: WDTVLive



Threat Hunting: WDTVLive

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

No.	Time	Source	Destination	Protocol	Length	Info
41	10.772888	[REDACTED]	204.11.201.12	NTP	90	NTP Version 4, client
42	10.773284	[REDACTED]	204.11.201.12	NTP	90	NTP Version 4, client
43	10.908505	[REDACTED]	66.96.98.9	NTP	90	NTP Version 4, client
44	10.909450	[REDACTED]	66.96.98.9	NTP	90	NTP Version 4, client
45	10.992998	[REDACTED]	66.96.98.9	NTP	90	NTP Version 4, client
46	10.993412	[REDACTED]	66.96.98.9	NTP	90	NTP Version 4, client
47	11.908494	[REDACTED]	66.96.98.9	NTP	90	NTP Version 4, client
48	11.909395	[REDACTED]	66.96.98.9	NTP	90	NTP Version 4, client
49	12.908511	[REDACTED]	66.96.98.9	NTP	90	NTP Version 4, client
50	12.909454	[REDACTED]	66.96.98.9	NTP	90	NTP Version 4, client
51	14.878625	[REDACTED]	172.19.10.99	NTP	90	NTP Version 4, client
52	14.879604	[REDACTED]	172.19.10.99	NTP	90	NTP Version 4, client

► Frame 50: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
► Ethernet II, Src: [REDACTED] ([REDACTED]), Dst: [REDACTED] ([REDACTED])
► Internet Protocol Version 4, Src: [REDACTED], Dst: 66.96.98.9
► User Datagram Protocol, Src Port: 56809, Dst Port: 123
▼ Network Time Protocol (NTP Version 4, client)
 ▼ Flags: 0xe3, Leap Indicator: unknown (clock unsynchronized), Version number: NTP Version 4, Mode: client
 11.. = Leap Indicator: unknown (clock unsynchronized) (3)
 ..10 0... = Version number: NTP Version 4 (4)
 011 = Mode: client (3)
 Peer Clock Stratum: unspecified or invalid (0)
 Peer Polling Interval: invalid (3)
 Peer Clock Precision: 0.015625 sec
 Root Delay: 1.0000 sec
 Root Dispersion: 1.0000 sec
 Reference ID: NULL
 Reference Timestamp: Jan 1, 1970 00:00:00.000000000 UTC
 Origin Timestamp: Jan 1, 1970 00:00:00.000000000 UTC
 Receive Timestamp: Jan 1, 1970 00:00:00.000000000 UTC
 Transmit Timestamp: Jun 1, 2017 04:16:25.812377000 UTC

NTP requests are not
malicious, device never sets
it's time properly

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

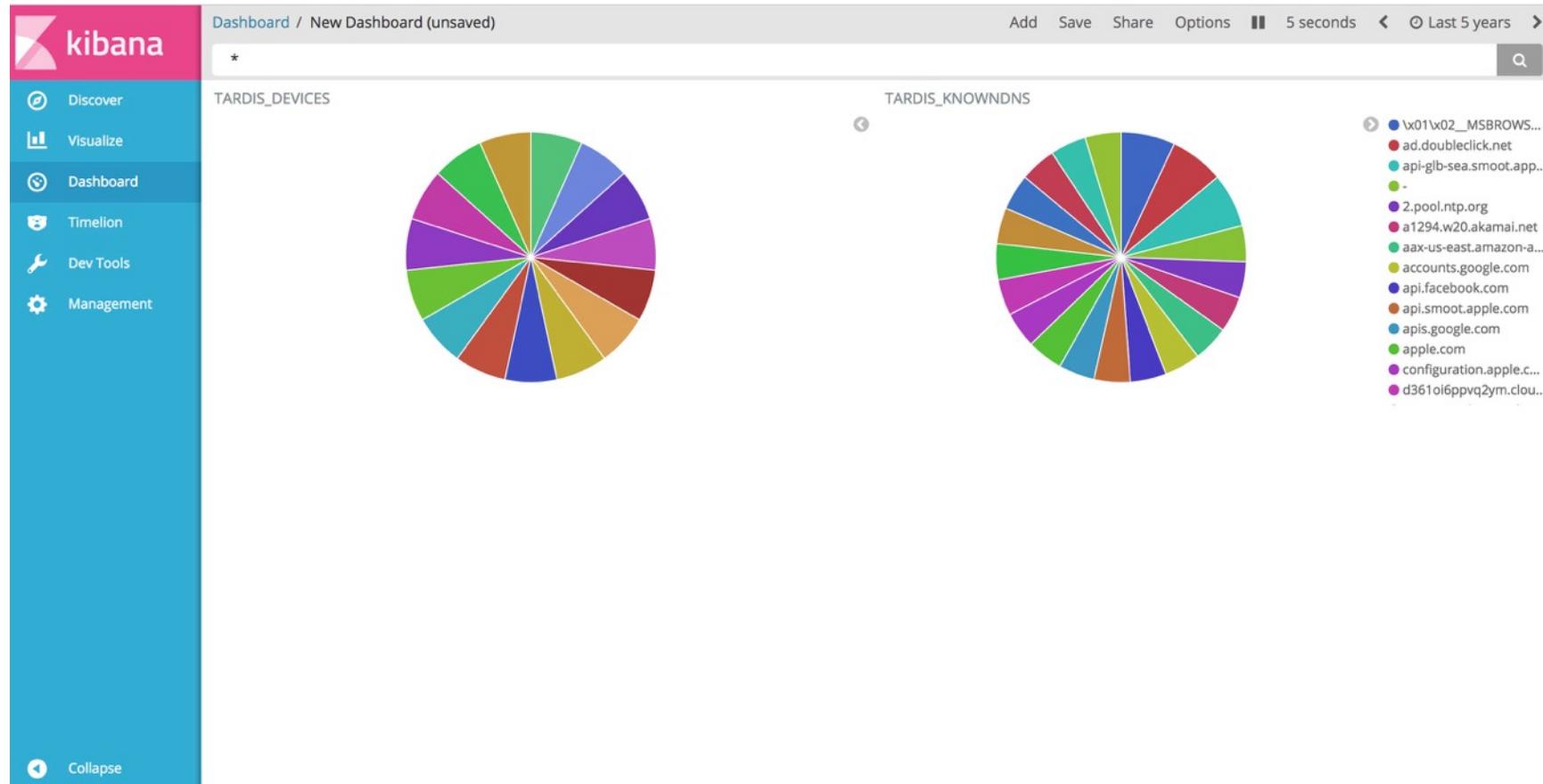
audio-ch1-t1-1-v4v6.pandora.com

t1-2.p-cdn.com

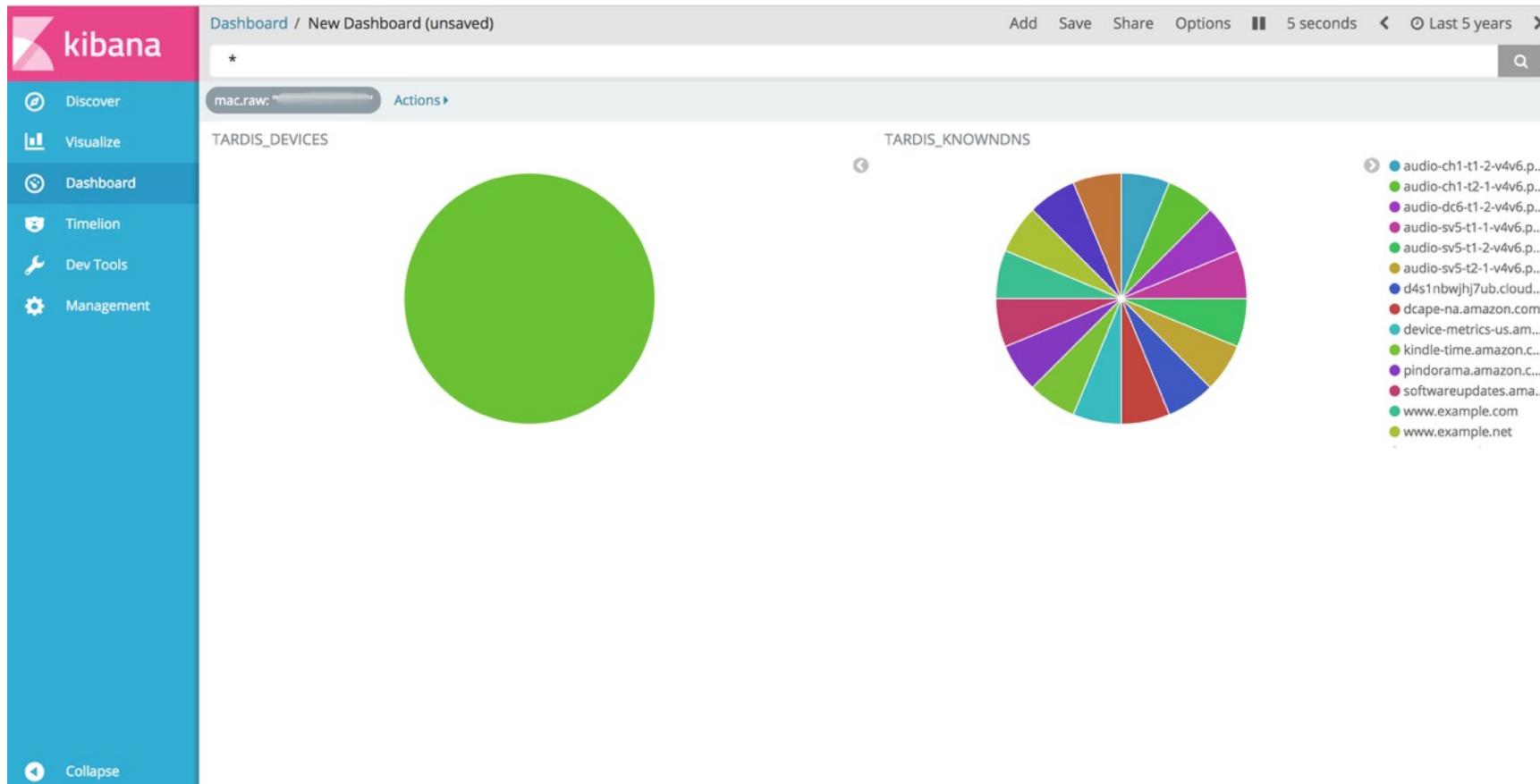
audio-dc6-t2-2-v4v6.pandora.com

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

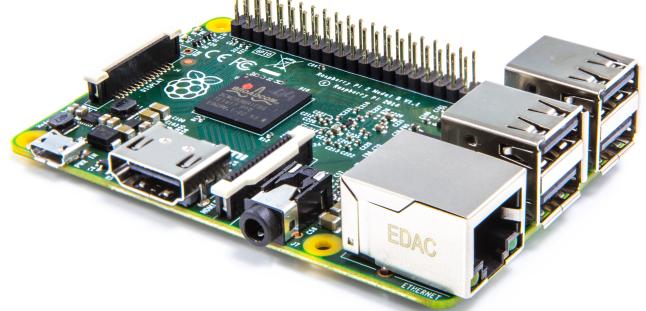
- ◆ Known Bad Lookups
- ◆ Check unknown IP's/URLS
 - ◆ WHOIS
 - ◆ Nslookup
 - ◆ GeolP (mostly for fun)
- ◆ Tor Exit Node IP Search

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>



CONFIDENCE: SECURED

Travis Smith
@MrTrav
tsmith@tripwire.com

THANK YOU

