ACTIVE | COUNTERMEASURES

Network Threat Hunter Training

Level 1

Thanks to our sponsors!

ACTIVE | COUNTERMEASURES

BLACK HILLS
Information Security
• 2008 •

WILD WEST
HACKIN' FEST

More cool stuff

- Wild West Hackin' Fest
  - Oct 12-14
  - $150 virtual ticket

https://wildwesthackinfest.com/deadwood/

- Advanced Network Threat Hunting
  - Oct 11 & 12
  - $725 (includes WWHF ticket)
  - Last run for the year!

https://www.antisyphontraining.com/advanced-network-threat-hunting-w-chris-brenton/

Before we get started

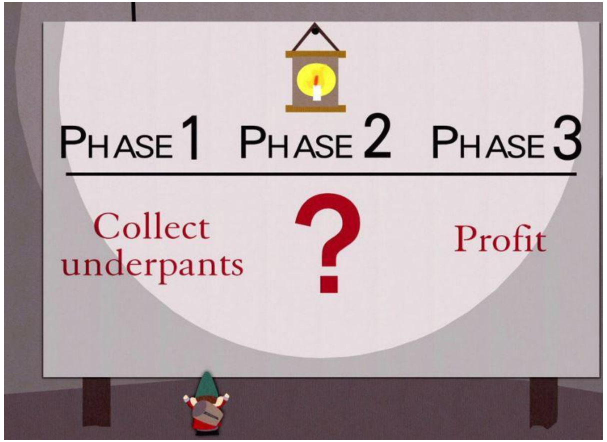
- You'll need the class VM to do the labs
  - **Just updated last week**
- Or run the install script
- Or deploy on DigitalOcean
- Login info:
  - Name: thunt
  - Pass: aybab2u
- This should have been done before class :-)

Logistics

- 10 minute break at top of each hour
- 20 minute break at 3 hour point
- Use the Discord channel for discussion
  - #acm-webcast-chat channel
- The team is monitoring for your questions

In this webcast

- I'm going to question some industry accepted standard practices
  - Because what we are doing is broken
  - And it's not getting any better
  - Will diverge from the norm
- Please keep an open mind
- Prime cognitive bias fodder



How we (try to) catch the bad guys

- Centralized log collection
- Write "signatures" to identify patterns that may indicate an attack
    - Patterns in the log messages
    - Matches against intel feeds
- Alert on signature matches
- Follow up on alerts

Limitations of deployment

- Every device and system?
- Are you sure?
- Are you REALLY sure?
  - I have yet to see an environment that can accurately make this claim
  - Even when you log, adversaries can disable this
- **"Fail open" system**
  - Can access Internet without logging and no alert
  - Can you detect disabled logging?

What are signatures?

- Basically RegEx for logs
- Match known bad patterns
- Because adversaries have stopped innovating and we now know all of the possible bad patterns they can use
- Oh wait...
- Sigs are the 1990's anti-virus model

Are we getting better at detection?

- Interesting nuggets in Mandiant's M-Trends 2022 report
- Dwell time is down to less than 30 days
  - Skewed by Ransomware at 4 days
  - But ***drop shows no correlation to breach impact***
  - This questions if detection is actually improving
- For threats Mandiant investigated:
  - 20% had been in place over 90 - 300 days
  - 8% are 1 year+

https://www.mandiant.com/media/15671

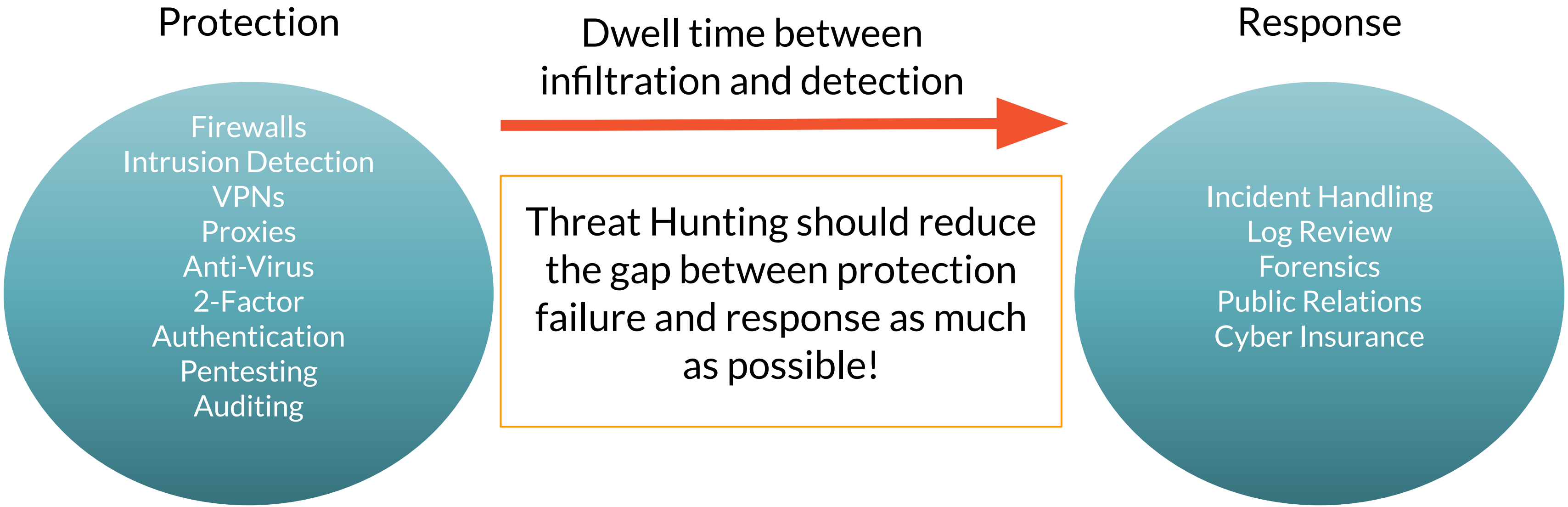
So is log review threat hunting?

- Just to review
  - Protocol can't describe security events
  - It's a fail open system
  - We try to pattern match on old attack patterns
  - False positive rates are extremely high
  - It's old technology
- The data says otherwise
- This process is clearly broken
- We need to assess new ideas and improve

What Threat Hunting should be

- A **proactive** validation of all systems connected to the organization's network
- Needs to include all systems
  - Desktops, laptops, cellphones, tablets
  - Servers, network gear, printers
  - IoT, IIoT, any type of Internet "Thing"
- Execute without making assumptions
- Deliverable is a compromise assessment

The Purpose of Threat Hunting



Protection

Firewalls
Intrusion Detection
VPNs
Proxies
Anti-Virus
2-Factor
Authentication
Pentesting
Auditing

Dwell time between
infiltration and detection

Threat Hunting should reduce the gap between protection failure and response as much as possible!

Response

Incident Handling
Log Review
Forensics
Public Relations
Cyber Insurance

The data clearly shows centralized logging is insufficient for this task

What threat hunting is not

- Managing SOC alerts
- Check logs for suspect activity
- Check dashboards for unusual activity
- Monitor and respond to EDR alerts
- These are all ***reactive*** activities
- Threat hunting is a ***proactive*** process

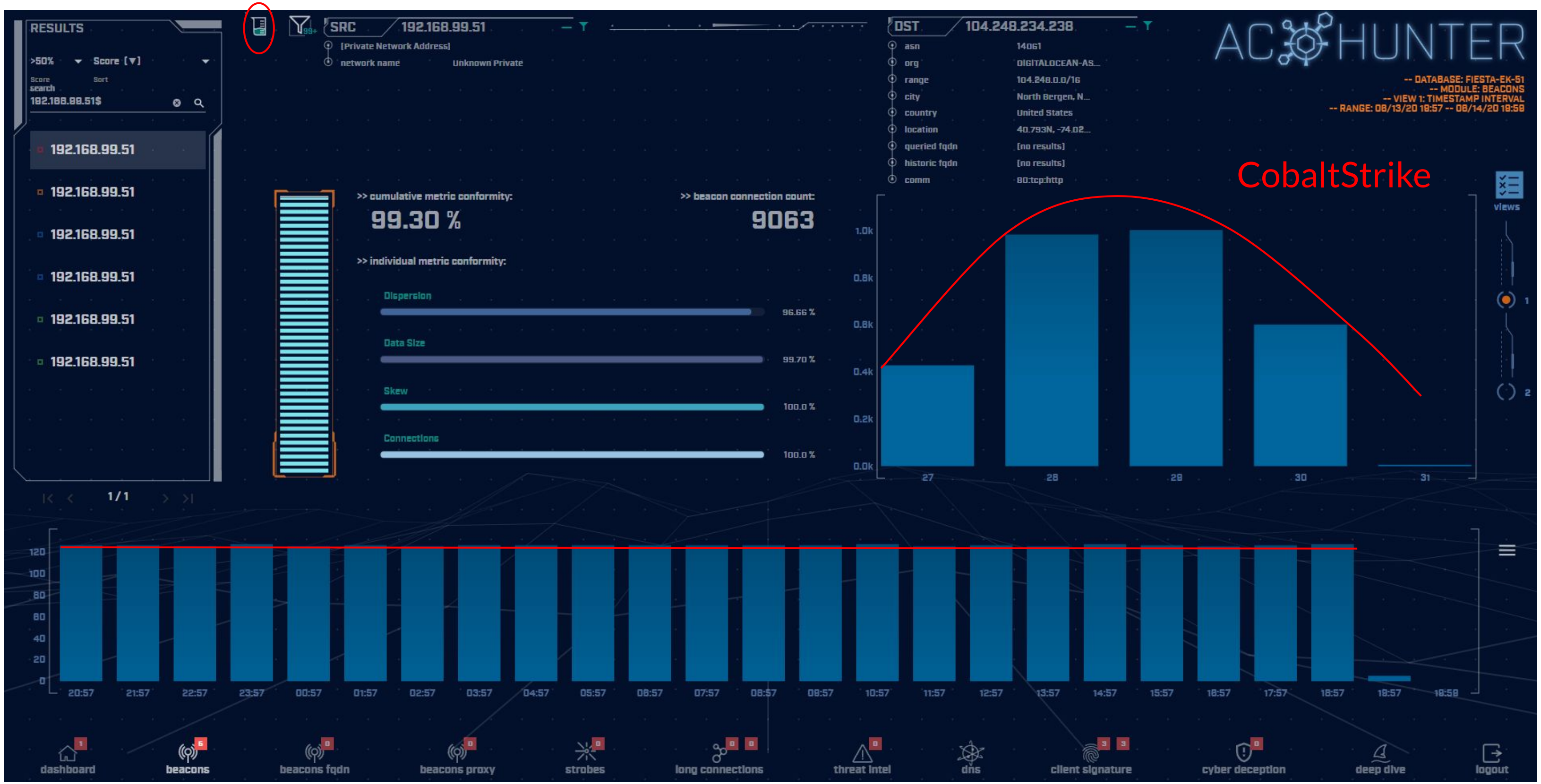
The process of threat hunting

- Review the integrity of every device
  - Desktops, servers, network gear, IoT, IIoT, etc.
- Generate one of 3 dispositions
  - I'm pretty certain the system is safe
  - I'm pretty certain the system is compromised
  - I'm unsure of state so will collect additional info to derive one of the above two results
- Leverage context for host log review

Proposal - Start with the network

- The network is the great equalizer
  - You see everything, regardless of platform
  - High level assessment of the terrain
- You can hide processes but not packets
- Malware is usually controlled
  - Which makes targeting C2 extremely effective
  - Identify compromise when C2 "calls home"
  - Must be frequent enough to be useful
- Wide view so you can target from there

Start on the network



RESULTS

>50% Score [▼]

Score Sort

search 192.168.99.51$

192.168.99.51
192.168.99.51
192.168.99.51
192.168.99.51
192.168.99.51
192.168.99.51

1 / 1

SRC 192.168.99.51

[Private Network Address]

network name Unknown Private

DST 104.248.234.238

asn	14061
org	DIGITALOCEAN-AS...
range	104.248.0.0/16
city	North Bergen, N...
country	United States
location	40.793N, -74.02...
queried fqdn	[no results]
historic fqdn	[no results]
comm	80:tcp:http

-- DATABASE: FIESTA-EK-51
-- MODULE: BEACONS
-- VIEW 1: TIMESTAMP INTERVAL
-- RANGE: 08/13/20 18:57 -- 08/14/20 18:58

>> cumulative metric conformity: 99.30 %

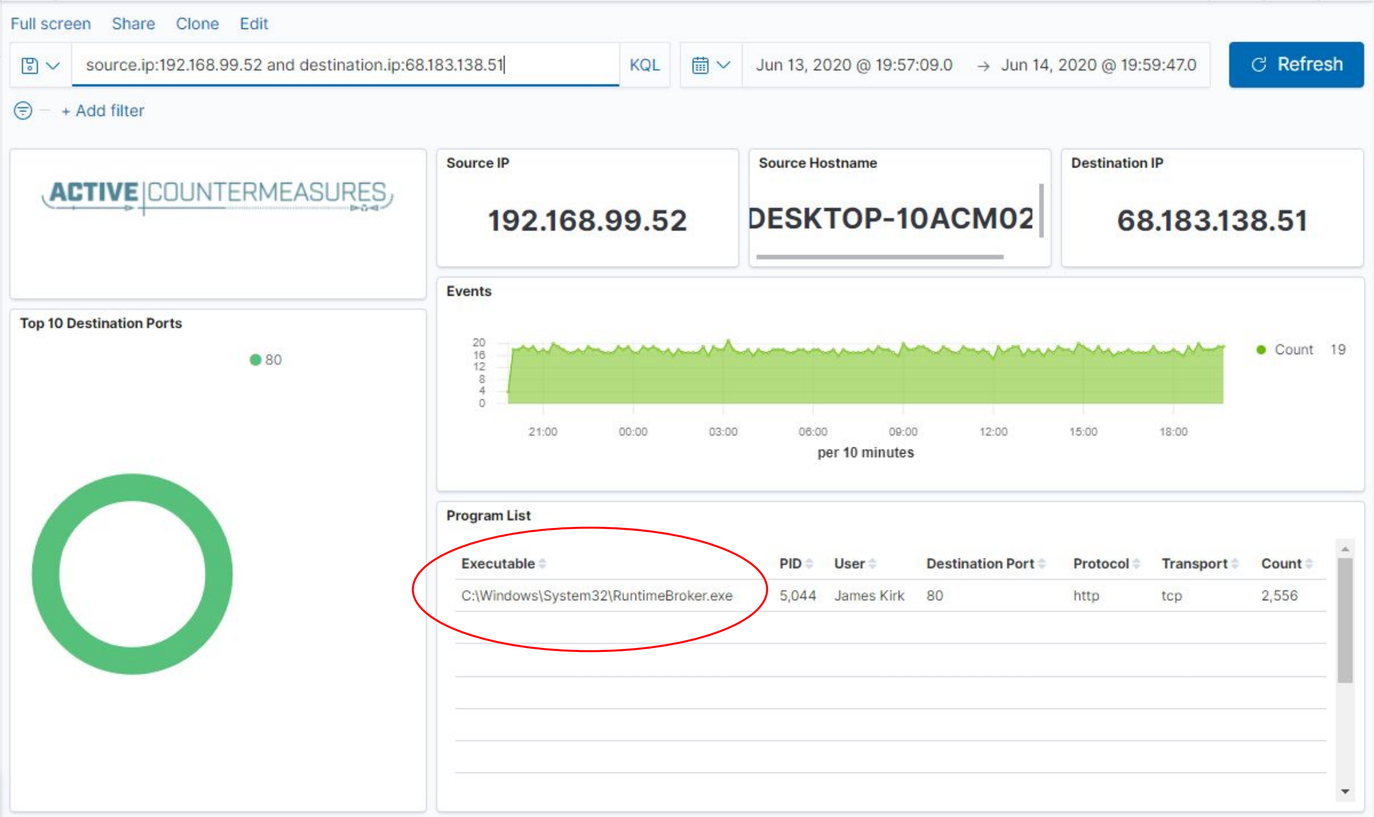
>> beacon connection count: 9063

>> individual metric conformity:

Dispersion	96.66 %
Data Size	99.70 %
Skew	100.0 %
Connections	100.0 %

CobaltStrike

THEN pivot to the system logs



source.ip:192.168.99.52 and destination.ip:68.183.138.51

Jun 13, 2020 @ 19:57:09.0 → Jun 14, 2020 @ 19:59:47.0

Source IP: 192.168.99.52

Source Hostname: DESKTOP-10ACM02

Destination IP: 68.183.138.51

Program List

Executable	PID	User	Destination Port	Protocol	Transport	Count
C:\Windows\System32\RuntimeBroker.exe	5,044	James Kirk	80	http	tcp	2,556

Don't cross "the passive/active line"

- All threat hunting activity should be undetectable to an adversary
- Passive in nature
  - Review packets
  - Review SIEM logs
- If active techniques are required, we must trigger incident response first
  - Example: Isolating the suspect host
  - Example: Running commands on suspect host

ACTIVE COUNTERMEASURES

C2 Detection Techniques

Where to Start

- Traffic to and from the Internet
  - Monitor internal interface of firewall
- Packet captures or Zeek data
- Analyze in large time blocks
  - More data = better fidelity
  - Minimum of 12 hours, 24 is ideal
- Analyze communications in pairs
  - Every outbound session passing the firewall
  - Ignore internal to internal (high false positive)

Threat score system

- Our job is to disposition IPs
- How do you know when to make a choice?
- A numeric system can help guide you
  - Score of 0-50 = system is safe
  - Score of 100+ = system is compromised
- Score modifiers
  - Major - Clue that strongly indicates integrity state
  - Minor - Clue that peripherally indicates integrity state

Threat hunting process order

- Connection persistency
- Business need for connection?
- Abnormal protocol behaviour
- Reputation check of external IP
- Investigation of internal IP
- Disposition
  - No threat detected = add to safelist
  - Compromised = Trigger incident handling

Does targeting C2 have blind spots?

- Attackers motivated by gain
  - Information
  - Control of resources
- Sometimes "gain" does not require C2
  - Just looking to destroy the target
  - Equivalent to dropping a cyber bomb
  - We are talking nation state at this level
- NotPetya
  - Worm with no C2 designed to seek and destroy

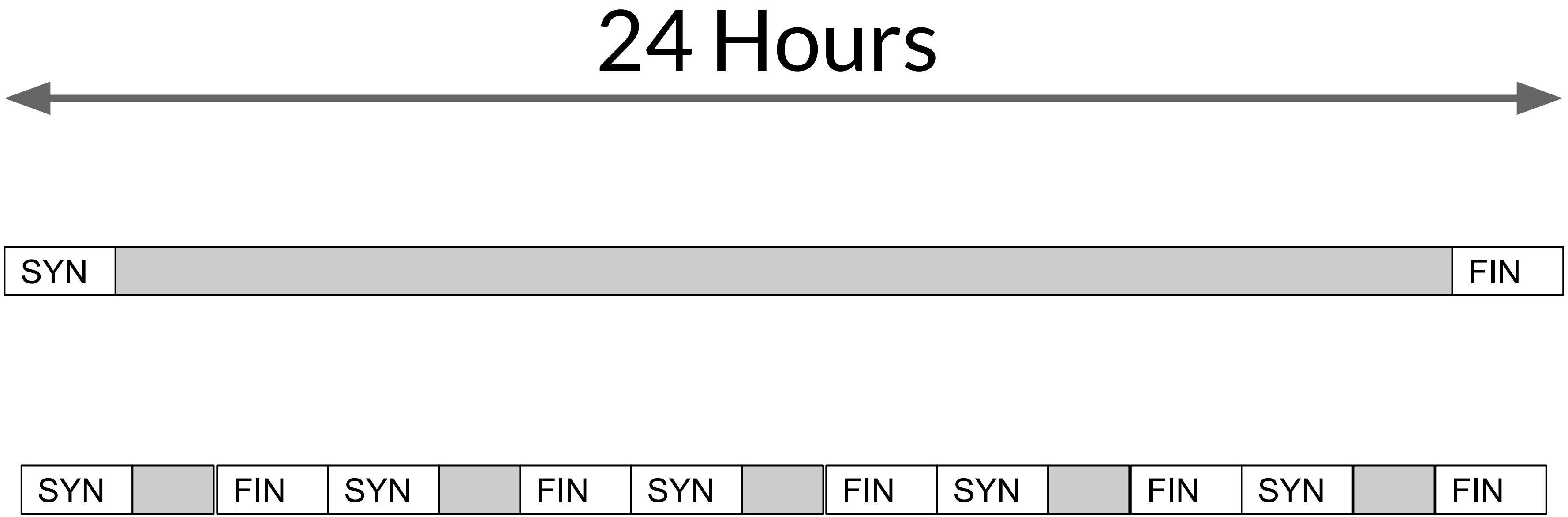
Bad guys Vs. Red Teams

- Bad guys = C2 is part of a business model
- Red team = C2 is why they get paid
- Much harder to detect red team C2 than the real bad guys
    - In the wild, most evil C2 beacons <= 1/minute
    - Red team on long term contract <= 1/week
- Focus will be on the bad guys

Long connections

- You are looking for:
- Total time for each connection
  - Which ones have gone on the longest?
- Cumulative time for all pair connections
  - Total amount of time the pair has been in contact
- Can be useful to ignore ports or protocols
  - C2 can change channels

Long connection examples

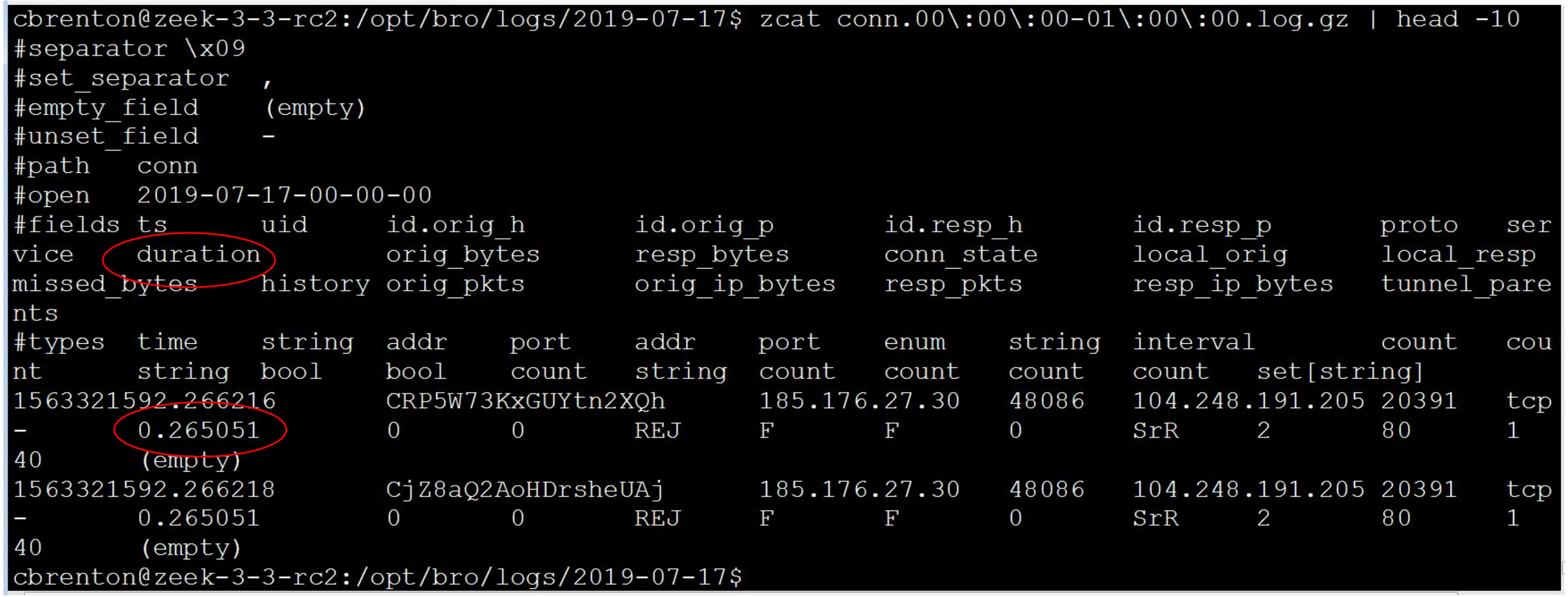


24 Hours

SYN FIN

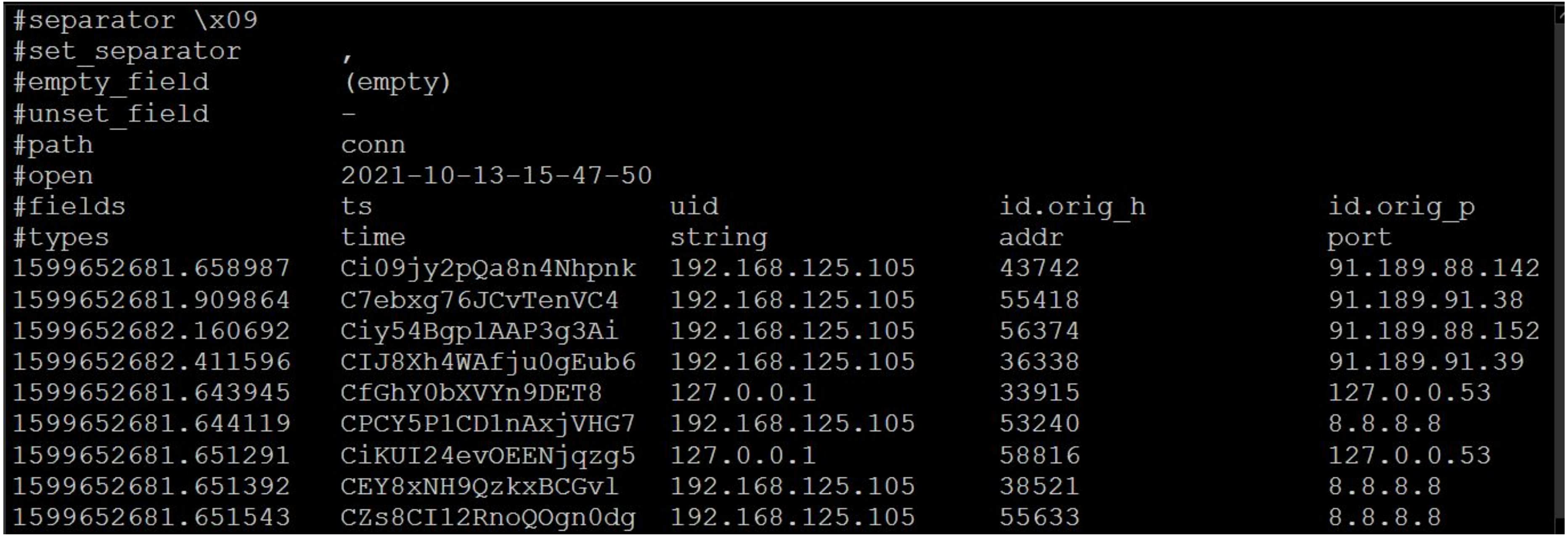
SYN FIN SYN FIN SYN FIN SYN FIN SYN FIN

Connection timing from Zeek



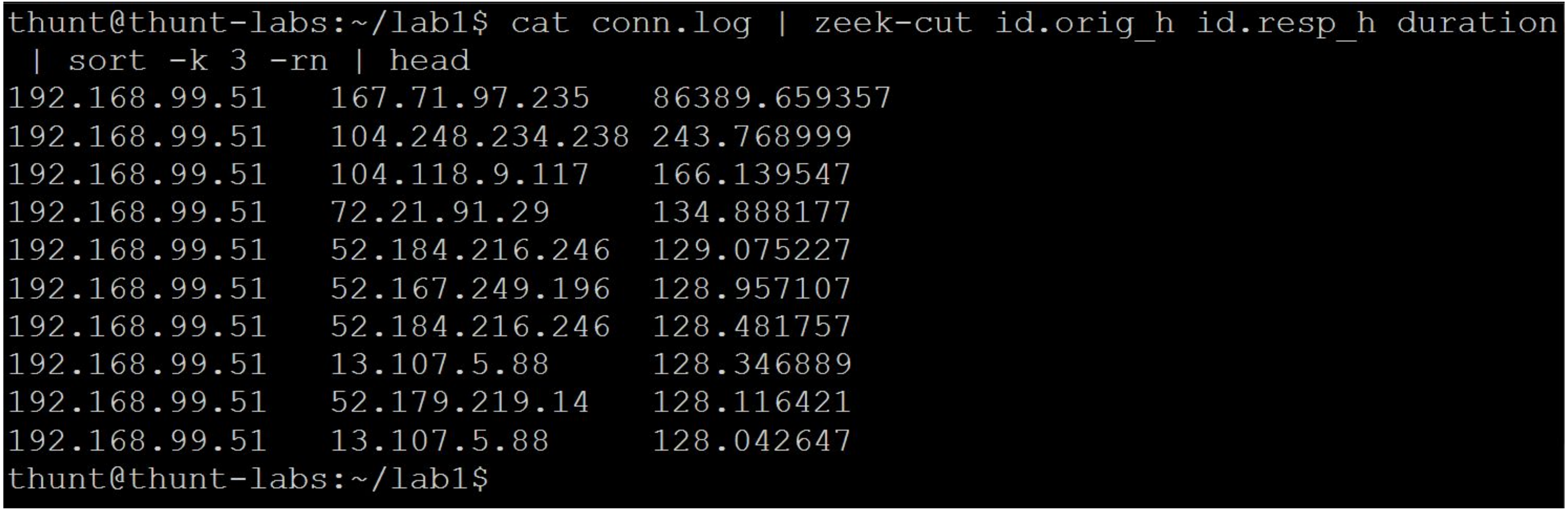
```
cbrenton@zeek-3-3-rc2:/opt/bro/logs/2019-07-17$ zcat conn.00\:00\:00-01\:00\:00.log.gz | head -10
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   conn
#open   2019-07-17-00-00-00
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   ser
vice    duration        orig_bytes      resp_bytes      conn_state      local_orig      local_resp
missed_bytes    history orig_pkts       orig_ip_bytes   resp_pkts       resp_ip_bytes   tunnel_pare
nts
#types  time    string  addr    port    addr    port    enum    string  interval        count   cou
nt      string  bool    bool    count   string  count   count   count   count   set[string]
1563321592.266216       CRP5W73KxGUYtn2XQh      185.176.27.30   48086   104.248.191.205 20391   tcp
-       0.265051        0       0       REJ     F       F       0       SrR     2       80      1
40      (empty)
1563321592.266218       CjZ8aQ2AoHDrsheUAj      185.176.27.30   48086   104.248.191.205 20391   tcp
-       0.265051        0       0       REJ     F       F       0       SrR     2       80      1
40      (empty)
cbrenton@zeek-3-3-rc2:/opt/bro/logs/2019-07-17$
```

less -Sx20 conn.log



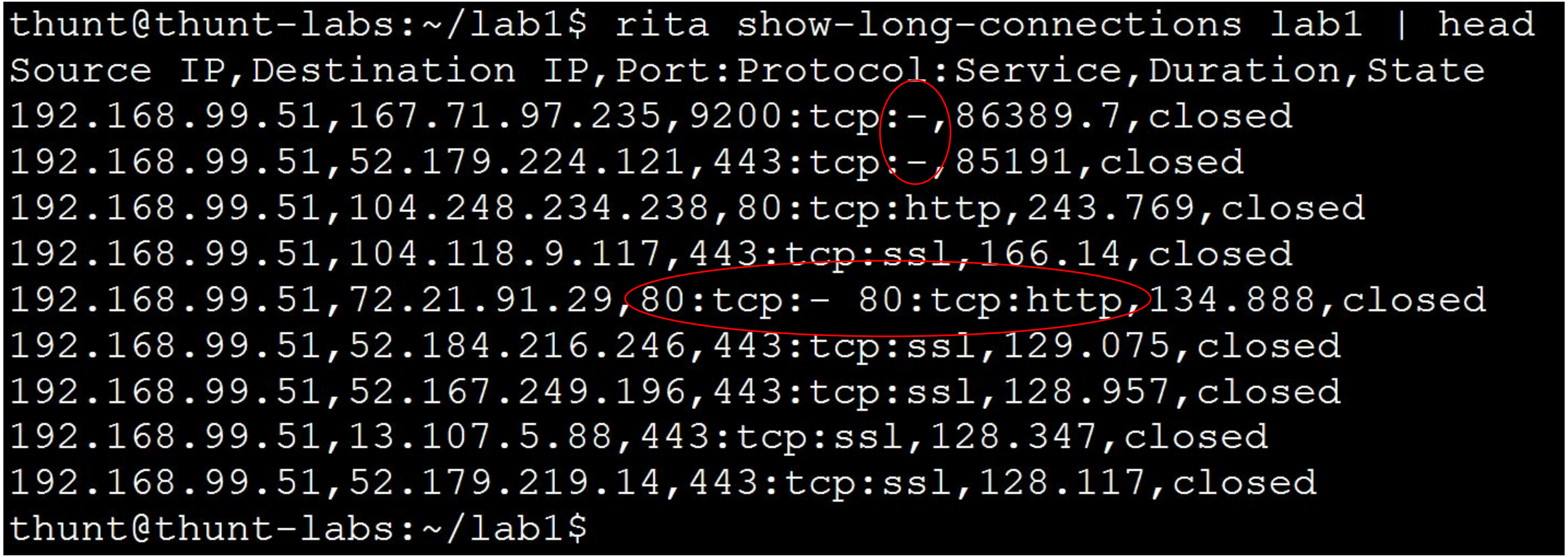
```
#separator \x09
#set_separator      ,
#empty_field        (empty)
#unset_field        -
#path               conn
#open               2021-10-13-15-47-50
#fields             ts                  uid                 id.orig_h           id.orig_p
#types              time                string              addr                port
1599652681.658987   Ci09jy2pQa8n4Nhpnk  192.168.125.105     43742               91.189.88.142
1599652681.909864   C7ebxg76JCvTenVC4   192.168.125.105     55418               91.189.91.38
1599652682.160692   Ciy54Bgp1AAP3g3Ai   192.168.125.105     56374               91.189.88.152
1599652682.411596   CIJ8Xh4WAfju0gEub6  192.168.125.105     36338               91.189.91.39
1599652681.643945   CfGhY0bXVYn9DET8    127.0.0.1           33915               127.0.0.53
1599652681.644119   CPCY5P1CD1nAxjVHG7  192.168.125.105     53240               8.8.8.8
1599652681.651291   CiKUI24evOEENjqzg5  127.0.0.1           58816               127.0.0.53
1599652681.651392   CEY8xNH9QzkxBCGvl   192.168.125.105     38521               8.8.8.8
1599652681.651543   CZs8CI12RnoQOgn0dg  192.168.125.105     55633               8.8.8.8
```

Longest duration with Zeek



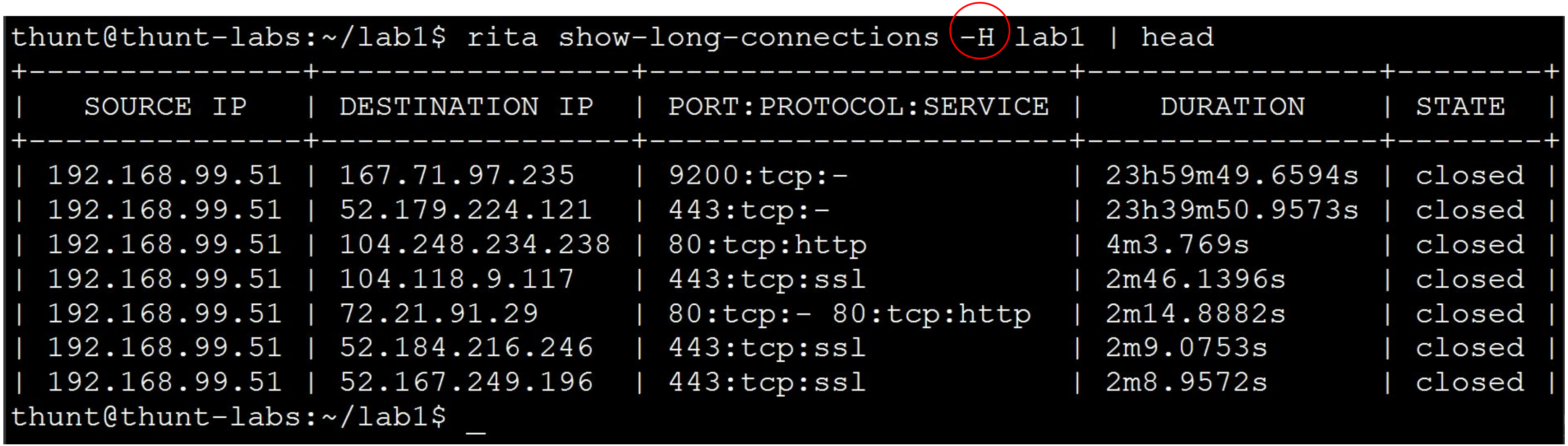
```
thunt@thunt-labs:~/lab1$ cat conn.log | zeek-cut id.orig_h id.resp_h duration
 | sort -k 3 -rn | head
192.168.99.51   167.71.97.235   86389.659357
192.168.99.51   104.248.234.238 243.768999
192.168.99.51   104.118.9.117   166.139547
192.168.99.51   72.21.91.29     134.888177
192.168.99.51   52.184.216.246  129.075227
192.168.99.51   52.167.249.196  128.957107
192.168.99.51   52.184.216.246  128.481757
192.168.99.51   13.107.5.88     128.346889
192.168.99.51   52.179.219.14   128.116421
192.168.99.51   13.107.5.88     128.042647
thunt@thunt-labs:~/lab1$
```

Longest duration with RITA



```
thunt@thunt-labs:~/lab1$ rita show-long-connections lab1 | head
Source IP,Destination IP,Port:Protocol:Service,Duration,State
192.168.99.51,167.71.97.235,9200:tcp:-,86389.7,closed
192.168.99.51,52.179.224.121,443:tcp:-,85191,closed
192.168.99.51,104.248.234.238,80:tcp:http,243.769,closed
192.168.99.51,104.118.9.117,443:tcp:ssl,166.14,closed
192.168.99.51,72.21.91.29,80:tcp:- 80:tcp:http,134.888,closed
192.168.99.51,52.184.216.246,443:tcp:ssl,129.075,closed
192.168.99.51,52.167.249.196,443:tcp:ssl,128.957,closed
192.168.99.51,13.107.5.88,443:tcp:ssl,128.347,closed
192.168.99.51,52.179.219.14,443:tcp:ssl,128.117,closed
thunt@thunt-labs:~/lab1$
```

Cleaner RITA output



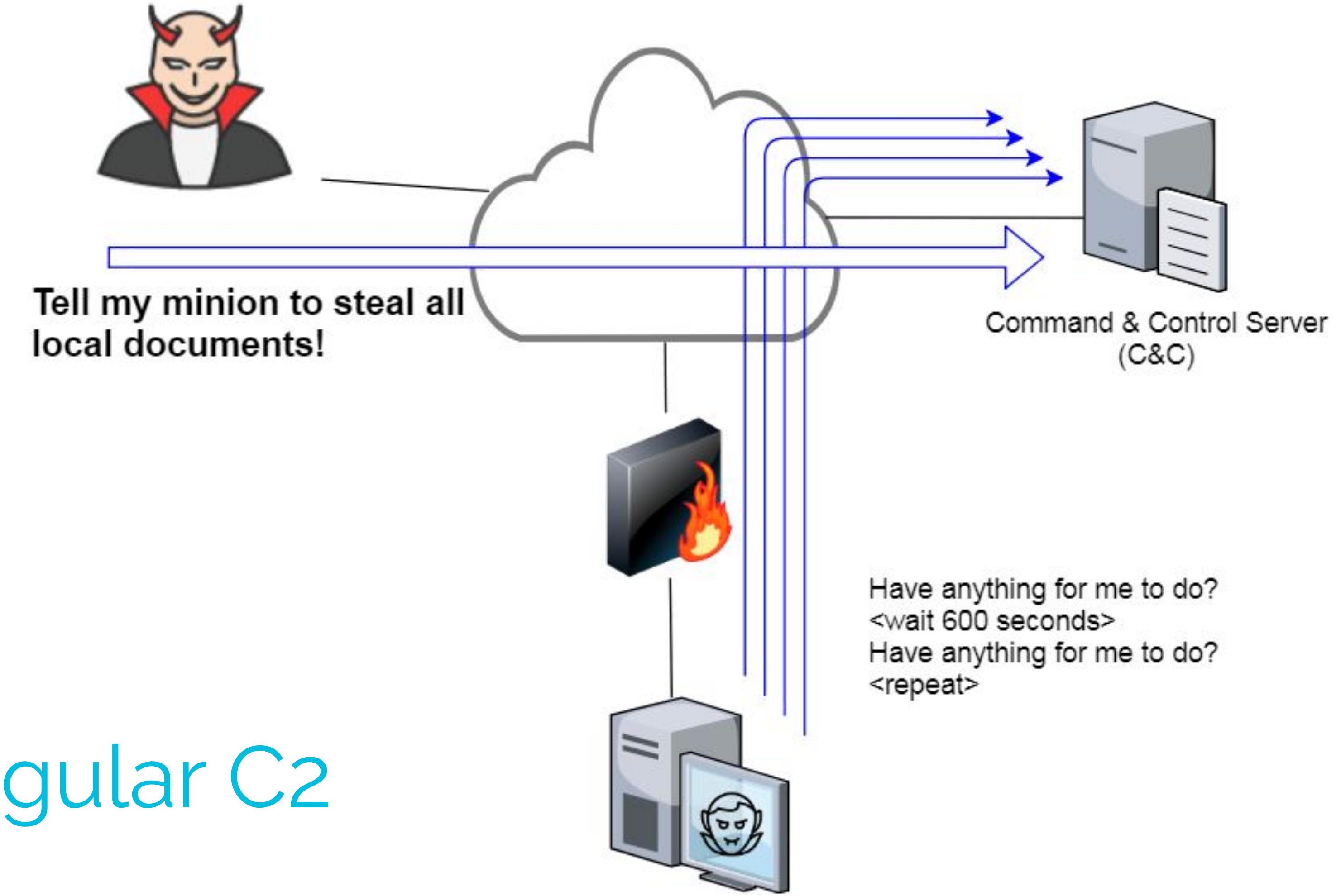
```
thunt@thunt-labs:~/lab1$ rita show-long-connections -H lab1 | head
+----------------+------------------+------------------------+-----------------+--------+
|   SOURCE IP    | DESTINATION IP   | PORT:PROTOCOL:SERVICE  |    DURATION     | STATE  |
+----------------+------------------+------------------------+-----------------+--------+
| 192.168.99.51 | 167.71.97.235    | 9200:tcp:-             | 23h59m49.6594s | closed |
| 192.168.99.51 | 52.179.224.121   | 443:tcp:-              | 23h39m50.9573s | closed |
| 192.168.99.51 | 104.248.234.238 | 80:tcp:http            | 4m3.769s        | closed |
| 192.168.99.51 | 104.118.9.117    | 443:tcp:ssl            | 2m46.1396s      | closed |
| 192.168.99.51 | 72.21.91.29      | 80:tcp:- 80:tcp:http   | 2m14.8882s      | closed |
| 192.168.99.51 | 52.184.216.246   | 443:tcp:ssl            | 2m9.0753s       | closed |
| 192.168.99.51 | 52.167.249.196   | 443:tcp:ssl            | 2m8.9572s       | closed |
thunt@thunt-labs:~/lab1$ _
```

What about firewalls?

- Surprisingly hard to get this info
- "Timing" tends to be TTL, not duration
- BSD
  - pftop - output connection age in seconds
- Junos
  - show security flow session extensive node all
  - Duration in seconds

What is a beacon?

- Repetitive connection establishment between two IP addresses
  - Easiest to detect
- Repetitive connection establishment between internal IP and FQDN
  - Target can be spread across multiple IP's
    - Usually a CDN provider
  - Target IPs also destination for legitimate traffic
  - Far more difficult to detect

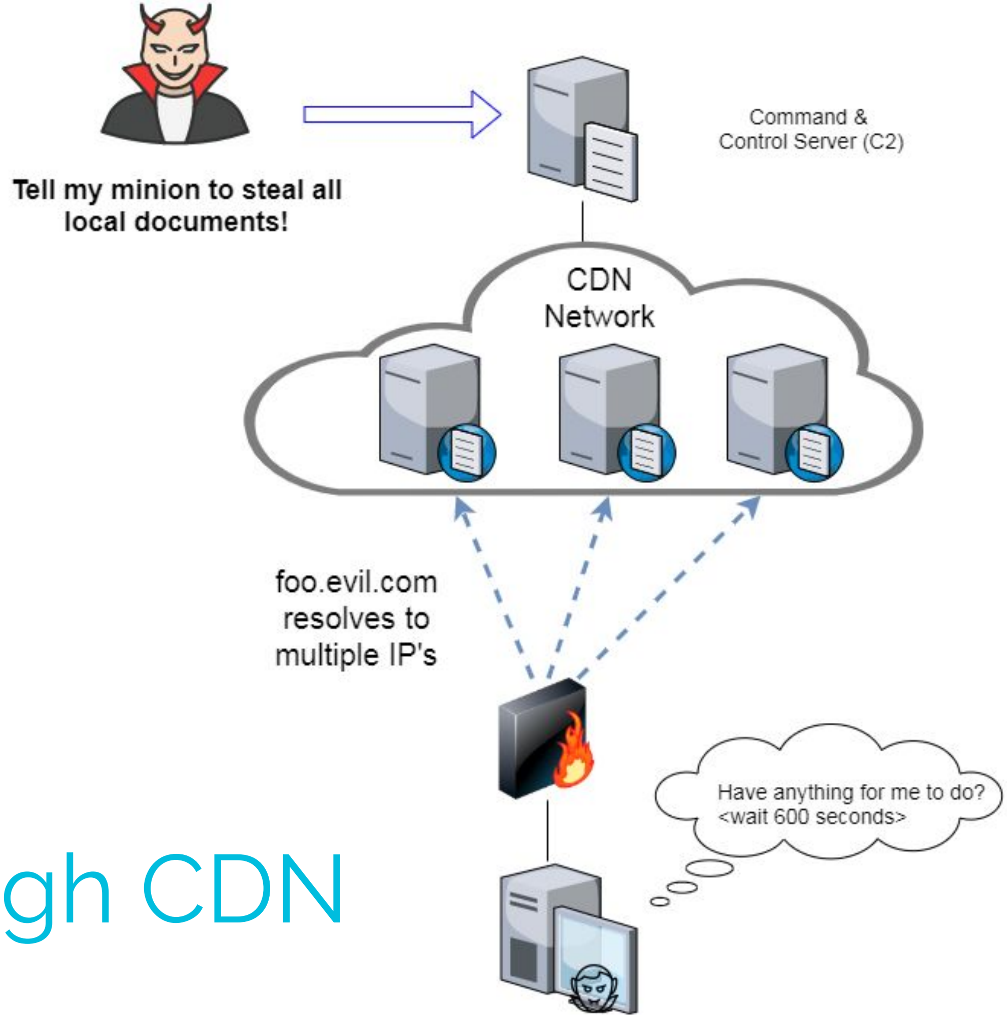


Tell my minion to steal all local documents!

Command & Control Server (C&C)

Have anything for me to do?
<wait 600 seconds>
Have anything for me to do?
<repeat>

Regular C2

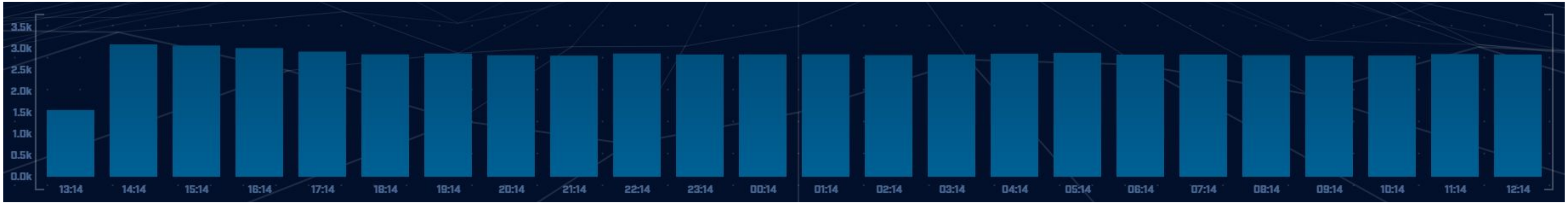

Tell my minion to steal all local documents!
Command & Control Server (C2)
CDN Network
foo.evil.com resolves to multiple IP's
Have anything for me to do?
<wait 600 seconds>

C2 through CDN

Beacon detection based on timing

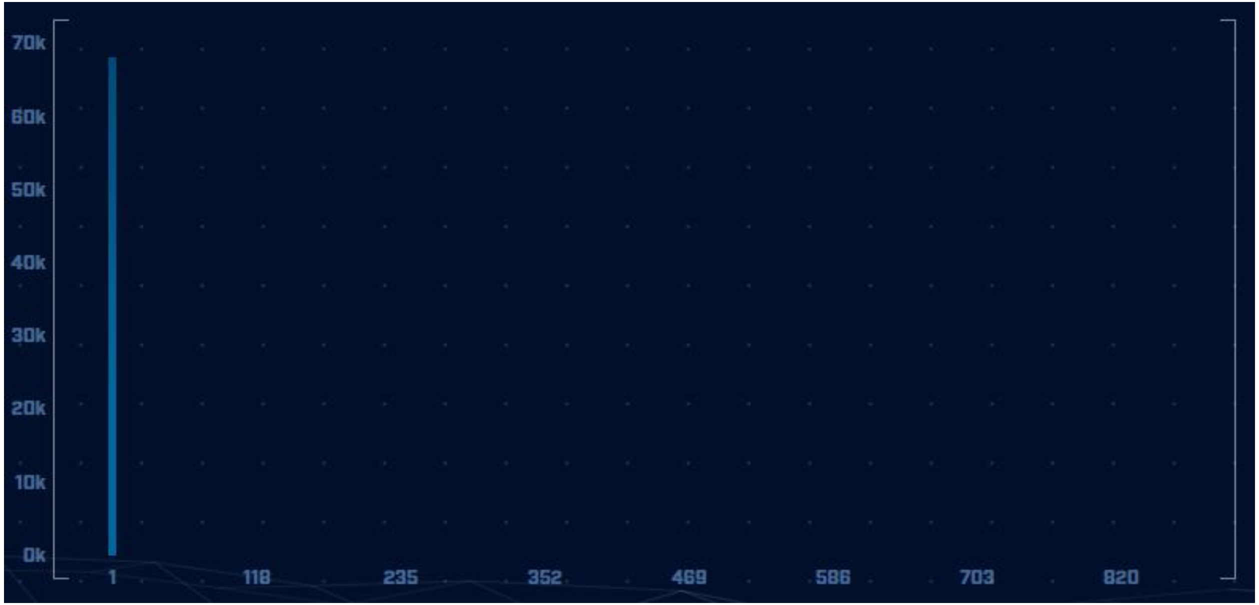
- May follow an exact time interval
  - Technique is less common today
  - Detectable by k-means
  - Potential false positives
- May introduce "jitter"
  - Vary connection sleep delta
  - Avoids k-means detection
  - False positives are extremely rare
- Short enough delta for terminal activities

Connection quantity VS time



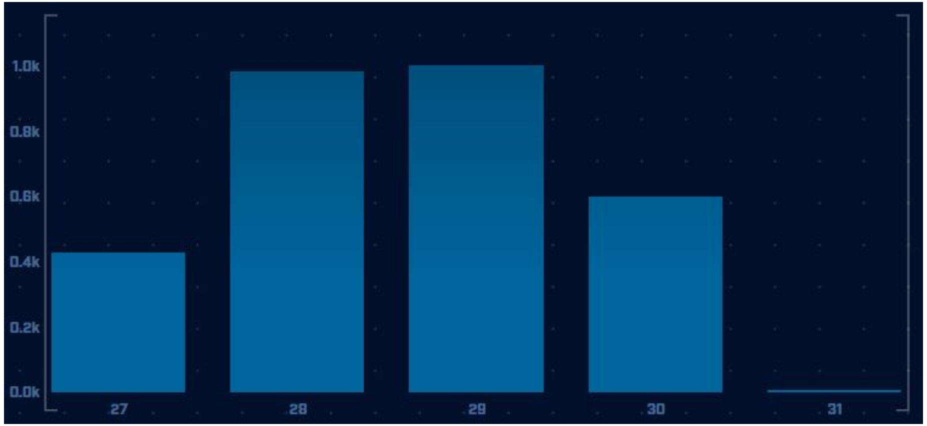
Each bar represents the number of times the source connected to the destination during that one hour time block

Connect time deltas with no jitter



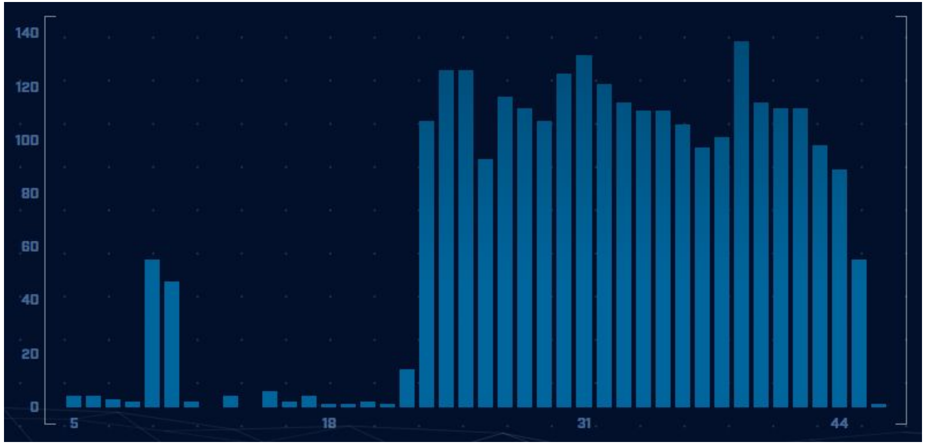
How often a specific time delta was observed

Connection time deltas with jitter



Cobalt Strike will typically produce a bell curve

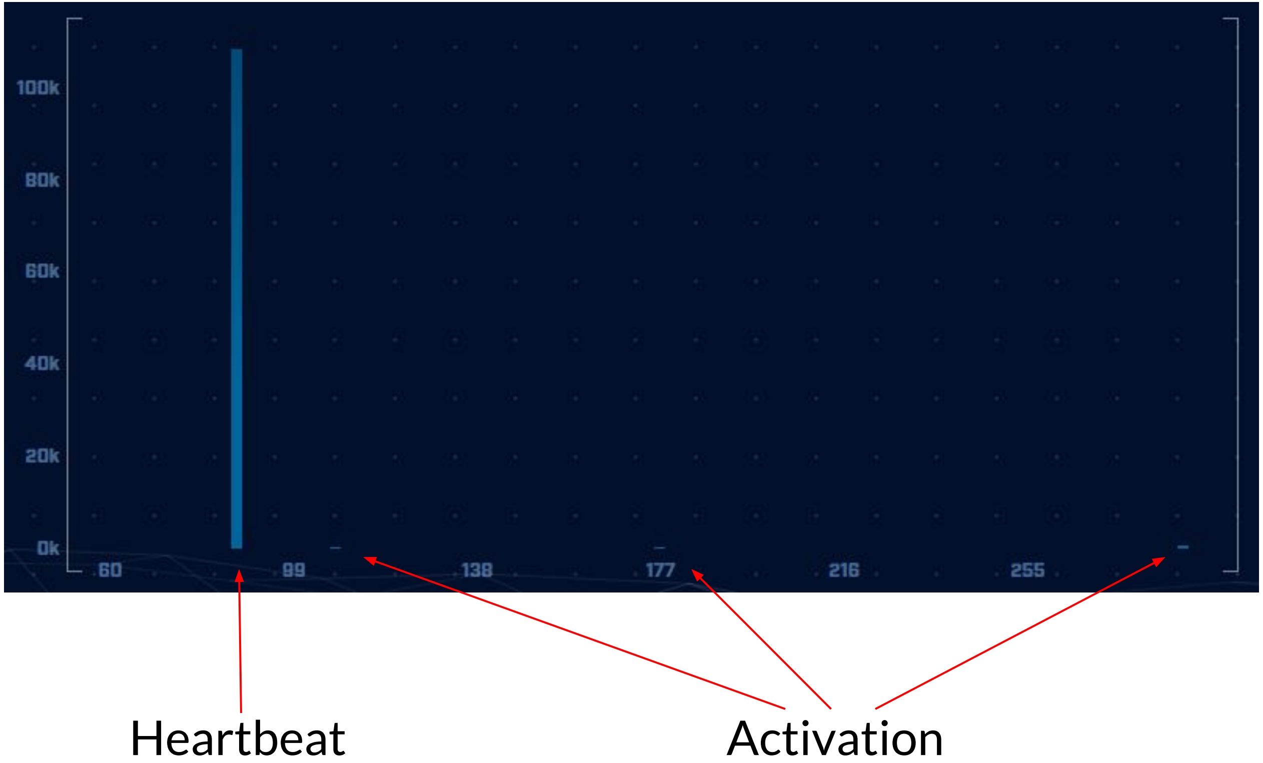
Pretty well randomized but still a small dwell time "window"



Detection based on session size

- Focuses on detection of the heartbeat
  - Useful for C2 over social media
- Variations from the heartbeat indicate activation of C2 channel
- Session size can help reveal info regarding commands being issued
- Possible to randomly pad but this is extremely rare

Session size analysis



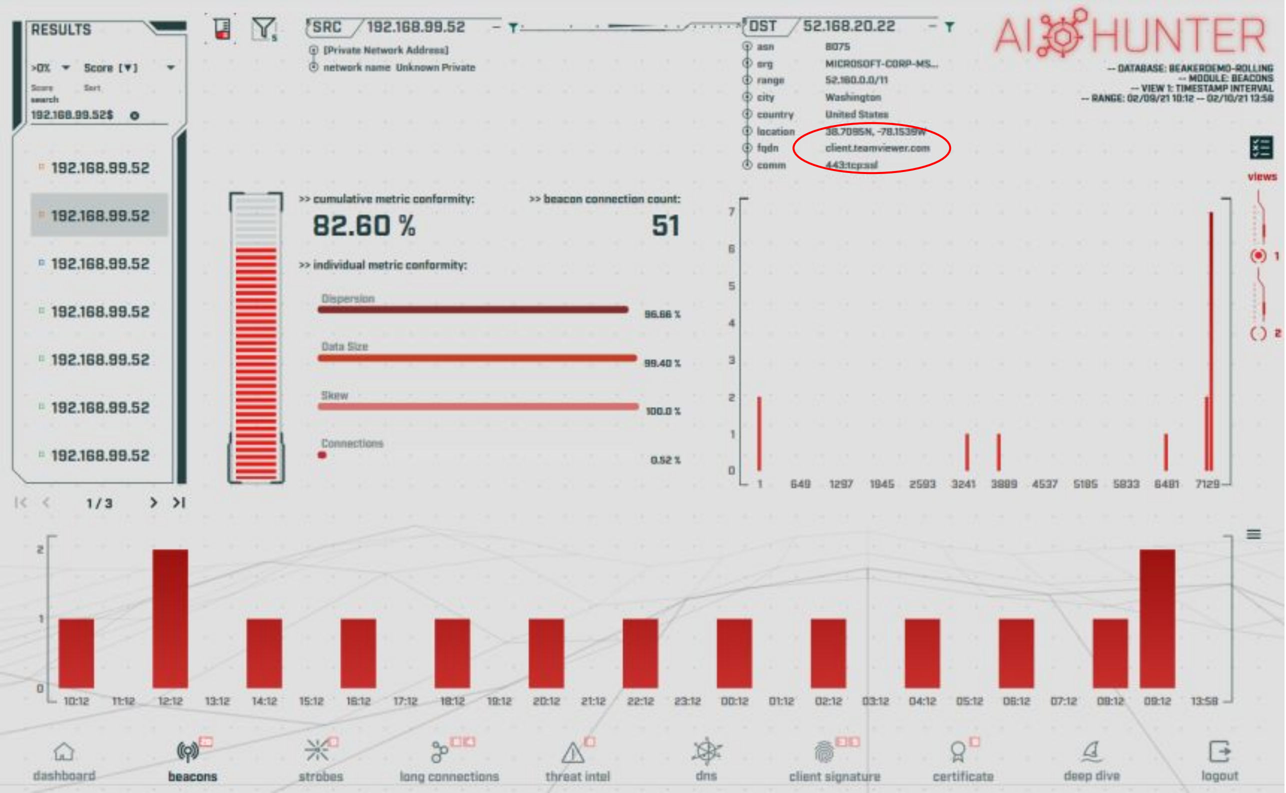
Heartbeat

Activation

Detecting beacons with jitter

- Easier to detect when normalized out over long periods of time
  - Average the time deltas for each hour
  - Plot over 24 hours
- Should make a beacon even more suspect
  - False positives don't obscure their beacon timing
  - High probability of being evil

Is there a business need?



RESULTS

>0% Score [▼]

Score search

Sort

192.168.99.52$

192.168.99.52

192.168.99.52

192.168.99.52

192.168.99.52

192.168.99.52

192.168.99.52

192.168.99.52

1 / 3

SRC 192.168.99.52

[Private Network Address]

network name Unknown Private

DST 52.168.20.22

asn	8075
org	MICROSOFT-CORP-MS...
range	52.160.0.0/11
city	Washington
country	United States
location	38.7095N, -78.1539W
fqdn	client.teamviewer.com
comm	443:tcp:ssl

-- DATABASE: BEAKERDEMO-ROLLING
-- MODULE: BEACONS
-- VIEW 1: TIMESTAMP INTERVAL
-- RANGE: 02/09/21 10:12 -- 02/10/21 13:58

>> cumulative metric conformity:
82.60 %

>> beacon connection count:
51

>> individual metric conformity:

Dispersion	96.66 %
Data Size	99.40 %
Skew	100.0 %
Connections	0.52 %

Can I get false positives?

- Sort of...
- Checking for connection persistency
- Then checking for business need
- It's possible to have persistent connections with a legit business need
    - NTP
    - Windows Notification Services
    - Checking for patches

ACTIVE COUNTERMEASURES

C2 Detection Techniques Part 2

What next?

- You've identified connection persistence
- You can't identify a business need
- Next steps
  - Protocol analysis
  - Reputation check of external target
  - Investigate internal IP address

Unexpected app or port usage

- There should be a business need for all outbound protocols
- Research non-standard or unknown ports
  - TCP/5222 (Chrome remote desktop)
  - TCP/5800 & 590X (VNC)
  - TCP/502 (Modbus)

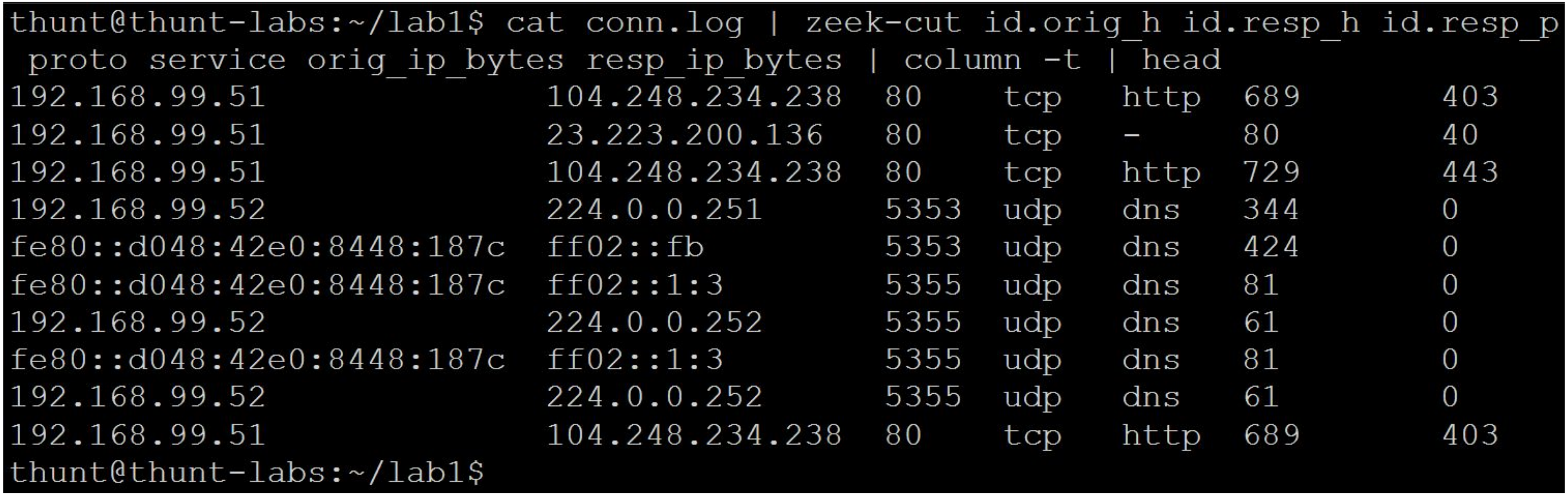
Unknown app on standard port

- C2 wants to tunnel out of environment
  - Pick a port likely to be permitted outbound
  - Does not always worry about protocol compliance
- Check standard ports for unexpected apps
  - Indication of tunneling
- Different than app on non-standard port
  - This is sometimes done as "a feature"
  - Example: SSH listening on TCP/2222

Zeek decodes many apps

- Detect over 50 applications
  - HTTP, DNS, SIP, MYSQL, RDP, NTLM, etc. etc.
- Fairly easy to add new ones
  - Example: HL7 if you are in healthcare
- Checks all analyzers for each port
- Does not assume WKP = application

Zeek example

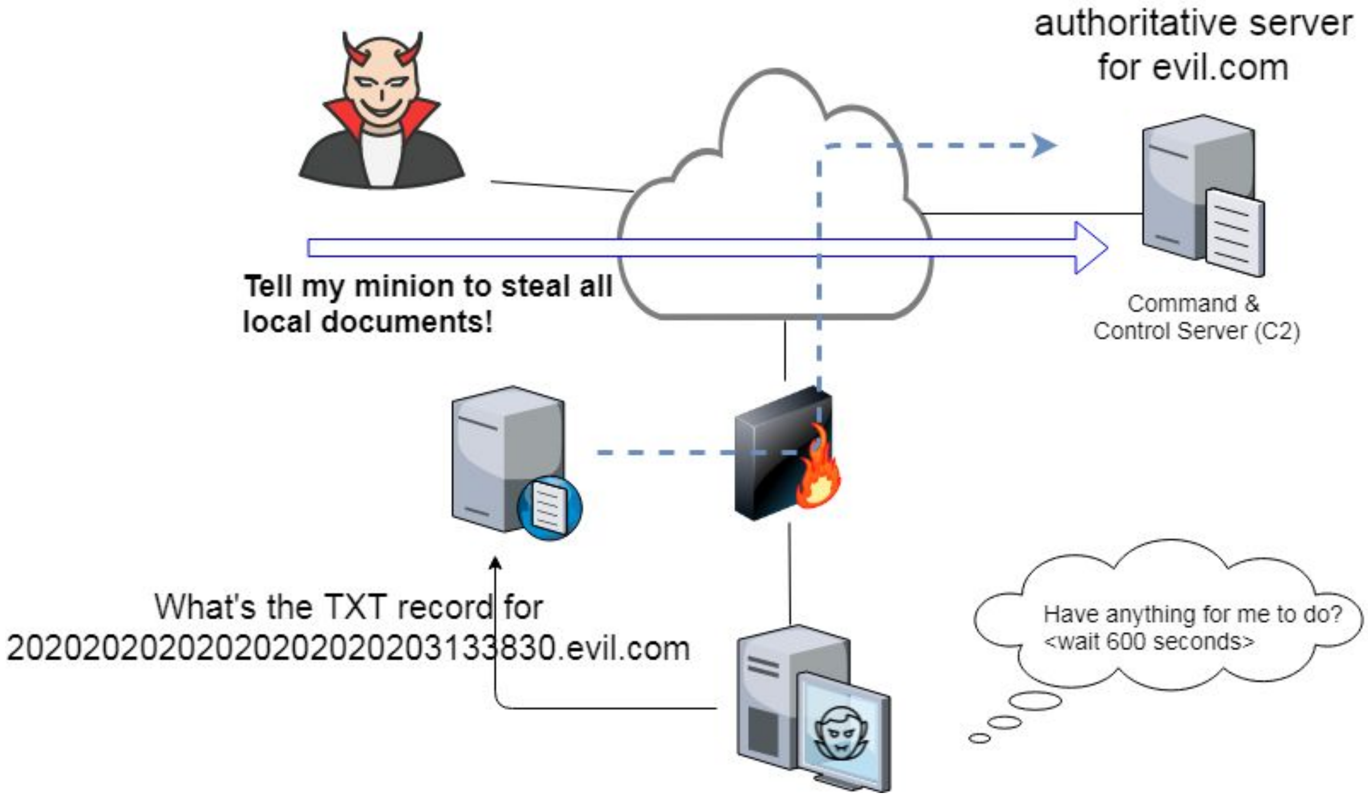


```
thunt@thunt-labs:~/lab1$ cat conn.log | zeek-cut id.orig_h id.resp_h id.resp_p
 proto service orig_ip_bytes resp_ip_bytes | column -t | head
192.168.99.51              104.248.234.238  80    tcp   http  689       403
192.168.99.51              23.223.200.136   80    tcp   -     80        40
192.168.99.51              104.248.234.238  80    tcp   http  729       443
192.168.99.52              224.0.0.251      5353  udp   dns   344       0
fe80::d048:42e0:8448:187c  ff02::fb         5353  udp   dns   424       0
fe80::d048:42e0:8448:187c  ff02::1:3        5355  udp   dns   81        0
192.168.99.52              224.0.0.252      5355  udp   dns   61        0
fe80::d048:42e0:8448:187c  ff02::1:3        5355  udp   dns   81        0
192.168.99.52              224.0.0.252      5355  udp   dns   61        0
192.168.99.51              104.248.234.238  80    tcp   http  689       403
thunt@thunt-labs:~/lab1$
```

Unexpected protocol use

- Attackers may bend but not break rules
- This can result in:
  - Full protocol compliance
  - Abnormal behaviour
- Need to understand "normal"
  - For the protocol
  - For your environment

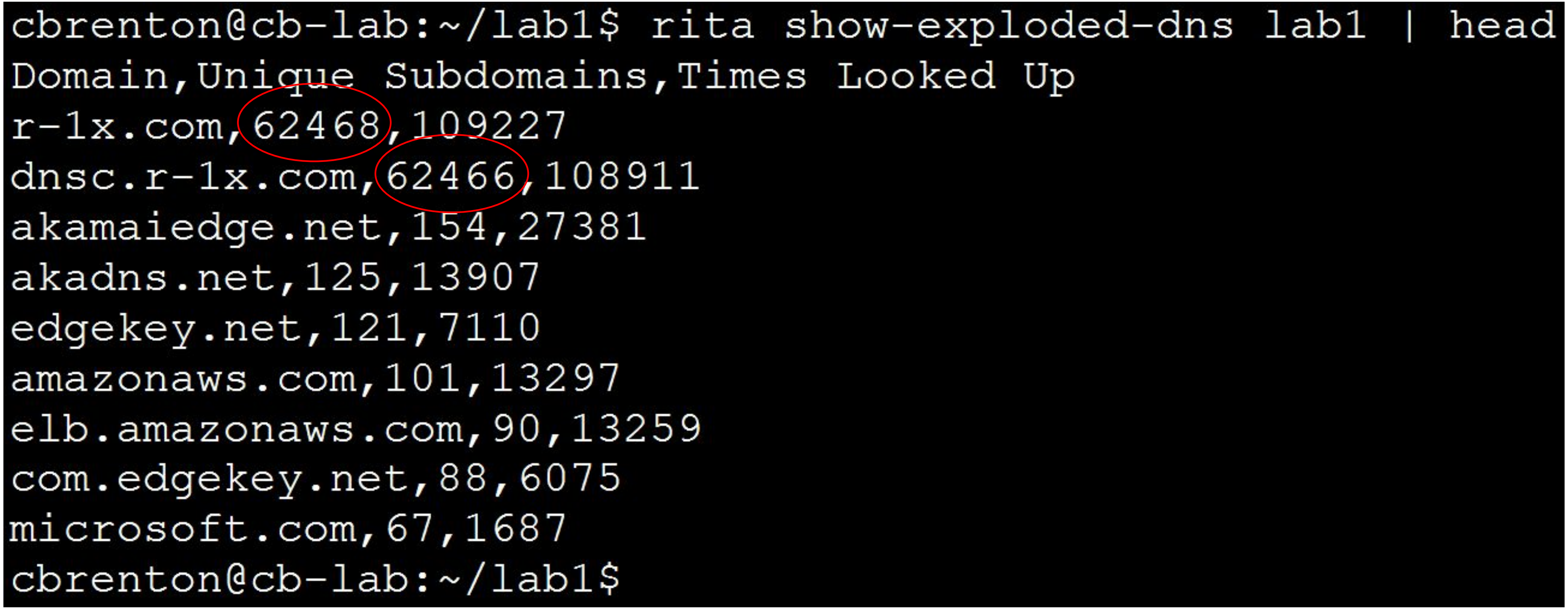
C2 over DNS


authoritative server
for evil.com
Command &
Control Server (C2)
Tell my minion to steal all
local documents!
What's the TXT record for
20202020202020202020203133830.evil.com
Have anything for me to do?
<wait 600 seconds>

Example: Too many FQDNs

- How many FQDNs do domains expose?
  - Most is < 10
  - Recognizable Internet based vendors 200 - 600
    - Microsoft
    - Akamai
    - Google
    - Amazon
- Greater than 1,000 is suspicious
- Could be an indication of C2 traffic

Detecting C2 over DNS with RITA

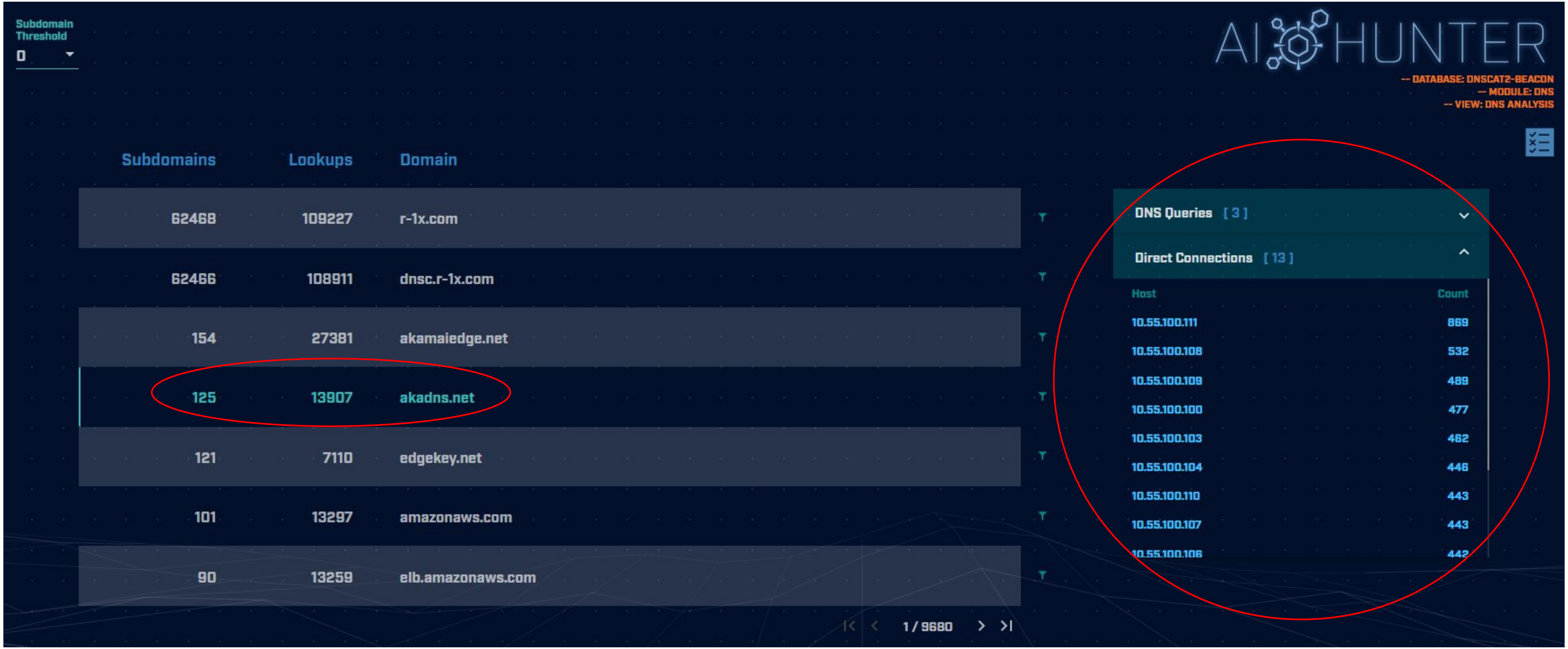


```
cbrenton@cb-lab:~/lab1$ rita show-exploded-dns lab1 | head
Domain,Unique Subdomains,Times Looked Up
r-1x.com,62468,109227
dnsc.r-1x.com,62466,108911
akamaiedge.net,154,27381
akadns.net,125,13907
edgekey.net,121,7110
amazonaws.com,101,13297
elb.amazonaws.com,90,13259
com.edgekey.net,88,6075
microsoft.com,67,1687
cbrenton@cb-lab:~/lab1$
```

Bonus checks on DNS

- Check domains with a lot of FQDNs
- Get a list of the IPs returned
- Compare against traffic patterns
  - Are internal hosts visiting this domain?
  - Is it just your name servers?
- Unique trait of C2 over DNS
  - Lots or FQDN queries
  - But no one ever connects to these systems

Normal DNS query patten



Subdomain Threshold
0

-- DATABASE: DNSCAT2-BEACON
-- MODULE: DNS
-- VIEW: DNS ANALYSIS

Subdomains	Lookups	Domain
62468	109227	r-1x.com
62466	108911	dnsc.r-1x.com
154	27381	akamaiedge.net
125	13907	akadns.net
121	7110	edgekey.net
101	13297	amazonaws.com
90	13259	elb.amazonaws.com

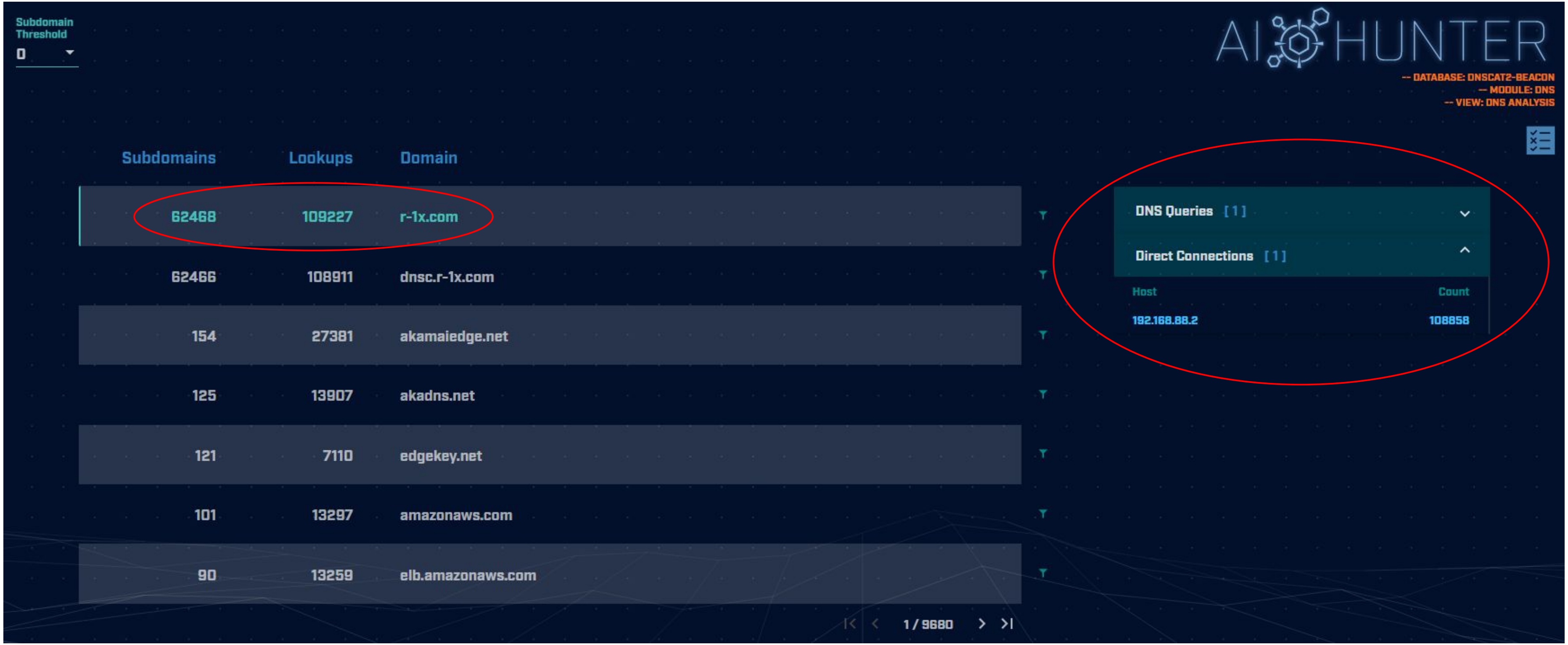
1 / 9680

DNS Queries [3]

Direct Connections [13]

Host	Count
10.55.100.111	869
10.55.100.108	532
10.55.100.109	489
10.55.100.100	477
10.55.100.103	462
10.55.100.104	446
10.55.100.110	443
10.55.100.107	443
10.55.100.106	442

Things that make you go "hummm"



-- DATABASE: DNSCAT2-BEACON
-- MODULE: DNS
-- VIEW: DNS ANALYSIS

Subdomains	Lookups	Domain
62468	109227	r-1x.com
62466	108911	dnsc.r-1x.com
154	27381	akamaiedge.net
125	13907	akadns.net
121	7110	edgekey.net
101	13297	amazonaws.com
90	13259	elb.amazonaws.com

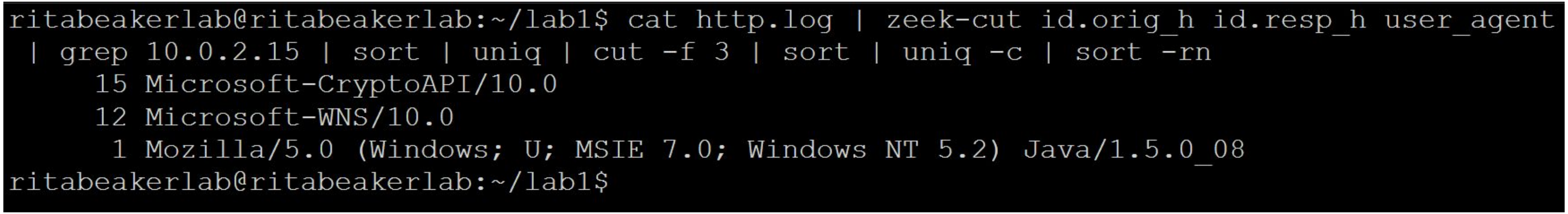
1 / 9680

DNS Queries [1]

Direct Connections [1]

Host	Count
192.168.88.2	108858

Look for odd HTTP user agents

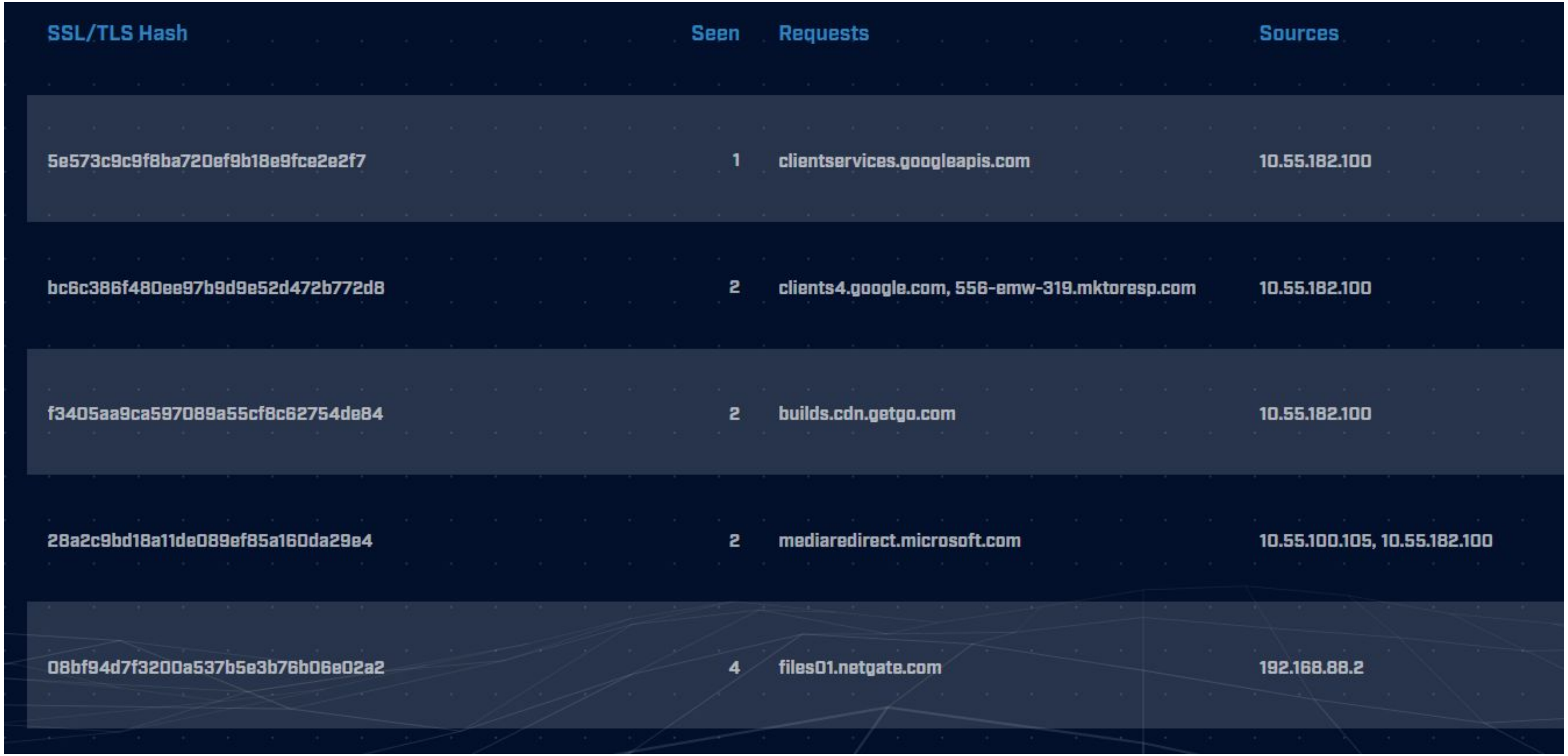


```
ritabeakerlab@ritabeakerlab:~/lab1$ cat http.log | zeek-cut id.orig_h id.resp_h user_agent
 | grep 10.0.2.15 | sort | uniq | cut -f 3 | sort | uniq -c | sort -rn
     15 Microsoft-CryptoAPI/10.0
     12 Microsoft-WNS/10.0
      1 Mozilla/5.0 (Windows; U; MSIE 7.0; Windows NT 5.2) Java/1.5.0_08
ritabeakerlab@ritabeakerlab:~/lab1$
```

10.0.2.15 identifies itself as:

Windows 10 when speaking to 27 different IP's on the Internet
Windows XP when speaking to one specific IP on the Internet

Unique SSL Client Hello: Zeek + JA3



SSL/TLS Hash	Seen	Requests	Sources
5e573c9c9f8ba720ef9b18e9fce2e2f7	1	clientservices.googleapis.com	10.55.182.100
bc6c386f480ee97b9d9e52d472b772d8	2	clients4.google.com, 556-emw-319.mktoresp.com	10.55.182.100
f3405aa9ca597089a55cf8c62754de84	2	builds.cdn.getgo.com	10.55.182.100
28a2c9bd18a11de089ef85a160da29e4	2	mediaredirect.microsoft.com	10.55.100.105, 10.55.182.100
08bf94d7f3200a537b5e3b76b06e02a2	4	files01.netgate.com	192.168.88.2

Check destination IP address

- Start simple
  - Who manages ASN?
  - Geolocation info?
  - IP delegation
  - PTR records
- Do you recognize the target organization?
  - Business partner or field office
  - Current vendor (active status)
- Other internal IP's connecting?

Some helpful links

https://www.abuseipdb.com/check/<IP Address>

https://otx.alienvault.com/indicator/ip/<IP Address>

https://search.censys.io/hosts/<IP Address>

https://dns.google/query?name=<IP Address>

https://www.google.com/search?q=<IP Address>

https://www.onyphe.io/search/?query=<IP Address>

https://securitytrails.com/list/ip/<IP Address>

https://www.shodan.io/host/<IP Address>

https://www.virustotal.com/gui/ip-address/<IP Address>/relations

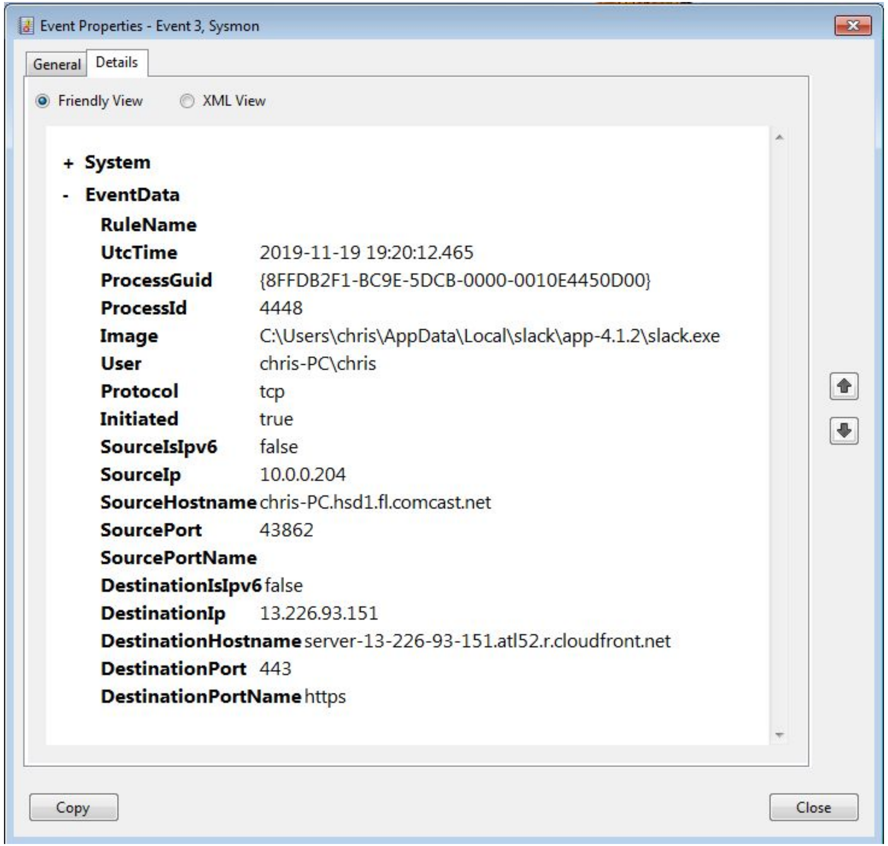
Internal system

- Info available varies greatly between orgs
- Inventory management systems
- Security tools like Carbon Black
- OS projects like BeaKer
- Internal security scans
- DHCP logs
- Login events
- Passive fingerprinting

Leverage internal host logging

- Network shows suspicious traffic patterns
- Use this data to pivot to host logs
- Filter your logs based on:
  - Suspect internal host
  - Timeframe being analyzed
- Anything stand out as unique or odd?

Sysmon Event ID Type 3's

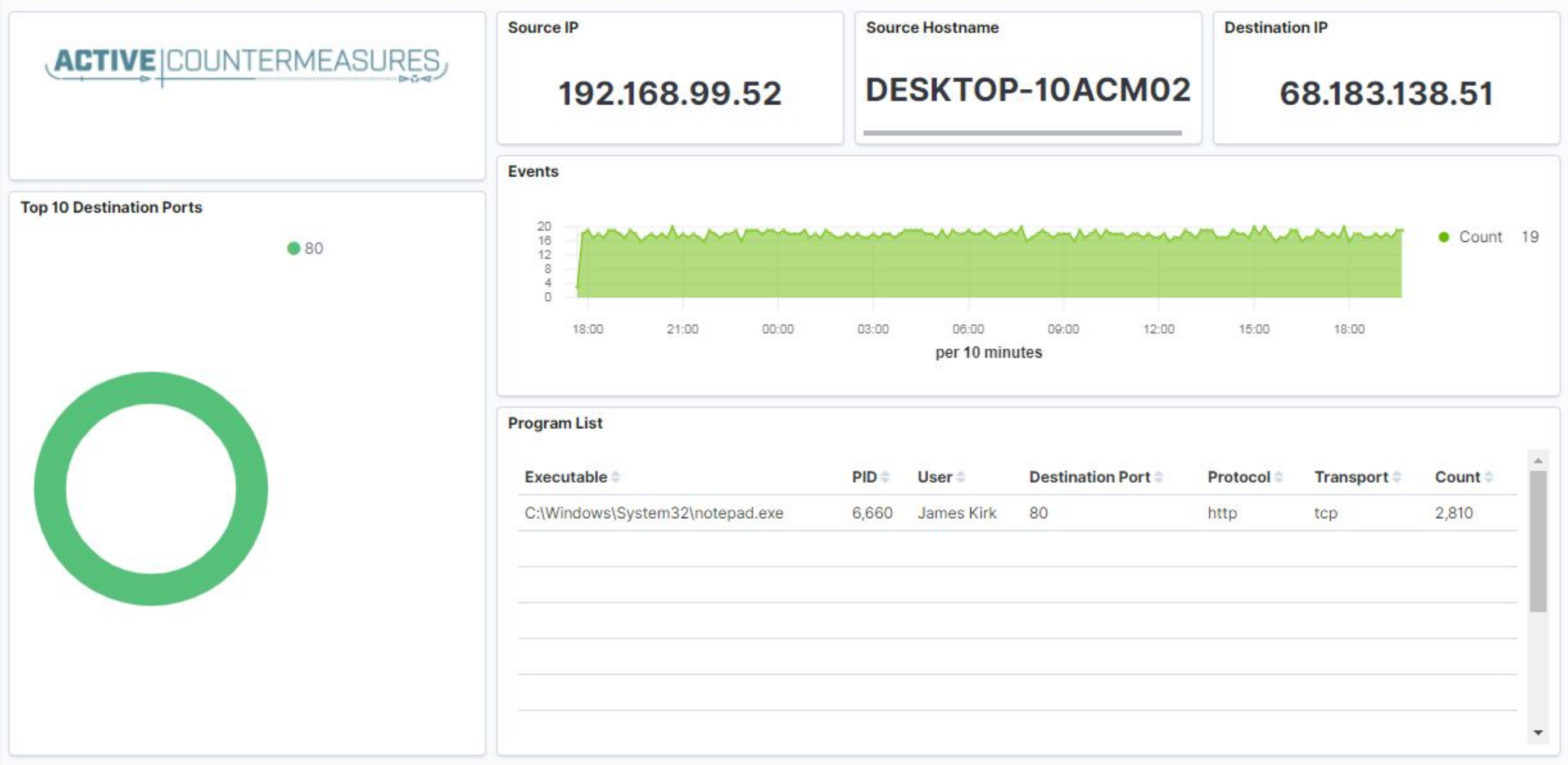


● Friendly View ○ XML View

```
+ System
- EventData
    RuleName
    UtcTime             2019-11-19 19:20:12.465
    ProcessGuid         {8FFDB2F1-BC9E-5DCB-0000-0010E4450D00}
    ProcessId           4448
    Image               C:\Users\chris\AppData\Local\slack\app-4.1.2\slack.exe
    User                chris-PC\chris
    Protocol            tcp
    Initiated           true
    SourceIsIpv6        false
    SourceIp            10.0.0.204
    SourceHostname      chris-PC.hsd1.fl.comcast.net
    SourcePort          43862
    SourcePortName
    DestinationIsIpv6   false
    DestinationIp       13.226.93.151
    DestinationHostname server-13-226-93-151.atl52.r.cloudfront.net
    DestinationPort     443
    DestinationPortName https
```

Map outbound connections to the applications that created them.

Sysmon Type 3 + BeaKer



Source IP

192.168.99.52

Source Hostname

DESKTOP-10ACM02

Destination IP

68.183.138.51

Top 10 Destination Ports

● 80

Events

Program List

Executable	PID	User	Destination Port	Protocol	Transport	Count
C:\Windows\System32\notepad.exe	6,660	James Kirk	80	http	tcp	2,810

But I have no system logs!

- Might be a good time to start collecting them
- Full packet captures from system
- Apply additional network tools to collect more data
- Just remember, nothing detectable until we trigger incident response mode!

What next?

- Disposition session
  - "I think it's safe" = add to safelist
  - "I think we've detected a compromise" = Incident response mode
- Remember to leave no footprints
  - All actions should be undetectable to potential adversaries
  - Passive activities only
- Incident response may include active tasks

ACTIVE COUNTERMEASURES

Network Threat Hunting Tools

tcpdump

- What's it good for?
  - Lightweight packet capturing tool
  - Cross platform support (windump on Windows)
- When to use it
  - Audit trail of all traffic
  - Can also filter to see only specific traffic
  - Can be fully automated
- Where to get it

https://www.tcpdump.org/

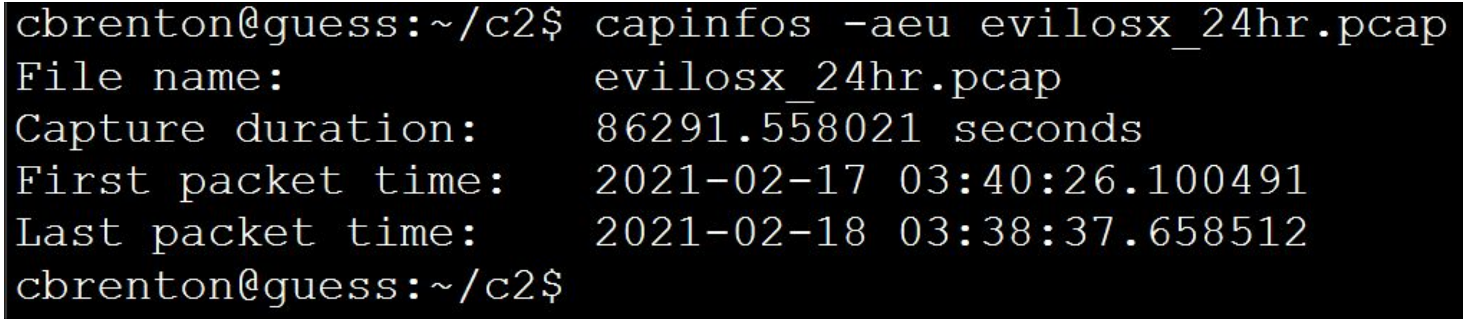
tcpdump example

- Debian/Ubuntu
  - Place the following in /etc/rc.local
- Red Hat/CentOS, Fedora
  - Place the following in /etc/rc.d/rc.local
- Grabs all traffic and rotates every 60 min
  - Date/time stamped and compressed

```
#Place _above_ any "exit" line
mkdir -p /opt/pcaps
screen -S capture -t capture -d -m bash -c "tcpdump -ieth0 -G
3600 -w '/opt/pcaps/`hostname -s`.%Y%m%d%H%M%S.pcap' -z bzip2"
```

capinfos

- Print summary info regarding pcaps
- For a decent hunt you want 12+ hours
- 86,400 seconds = 24 hours



```
cbrenton@guess:~/c2$ capinfos -aeu evilosx_24hr.pcap
File name:           evilosx_24hr.pcap
Capture duration:    86291.558021 seconds
First packet time:   2021-02-17 03:40:26.100491
Last packet time:    2021-02-18 03:38:37.658512
cbrenton@guess:~/c2$
```

tshark

- What's it good for?
  - Extracting interesting fields from packet captures
  - Multiple passes to focus on different attributes
  - Combine with text manipulation tools
  - Can be automated
- When to use it
  - Both major and minor attributes
- Where to get it

https://www.wireshark.org/

Tshark example - DNS queries

```
$ tshark -r thunt-lab.pcapng -T fields -e dns.qry.name
udp.port==53 | head -10

6dde0175375169c68f.dnsc.r-1x.com
6dde0175375169c68f.dnsc.r-1x.com
0b320175375169c68f.dnsc.r-1x.com
0b320175375169c68f.dnsc.r-1x.com
344b0175375169c68f.dnsc.r-1x.com
344b0175375169c68f.dnsc.r-1x.com
0f370175375169c68f.dnsc.r-1x.com
0f370175375169c68f.dnsc.r-1x.com
251e0175375169c68f.dnsc.r-1x.com
251e0175375169c68f.dnsc.r-1x.com
```

Tshark example - user agents

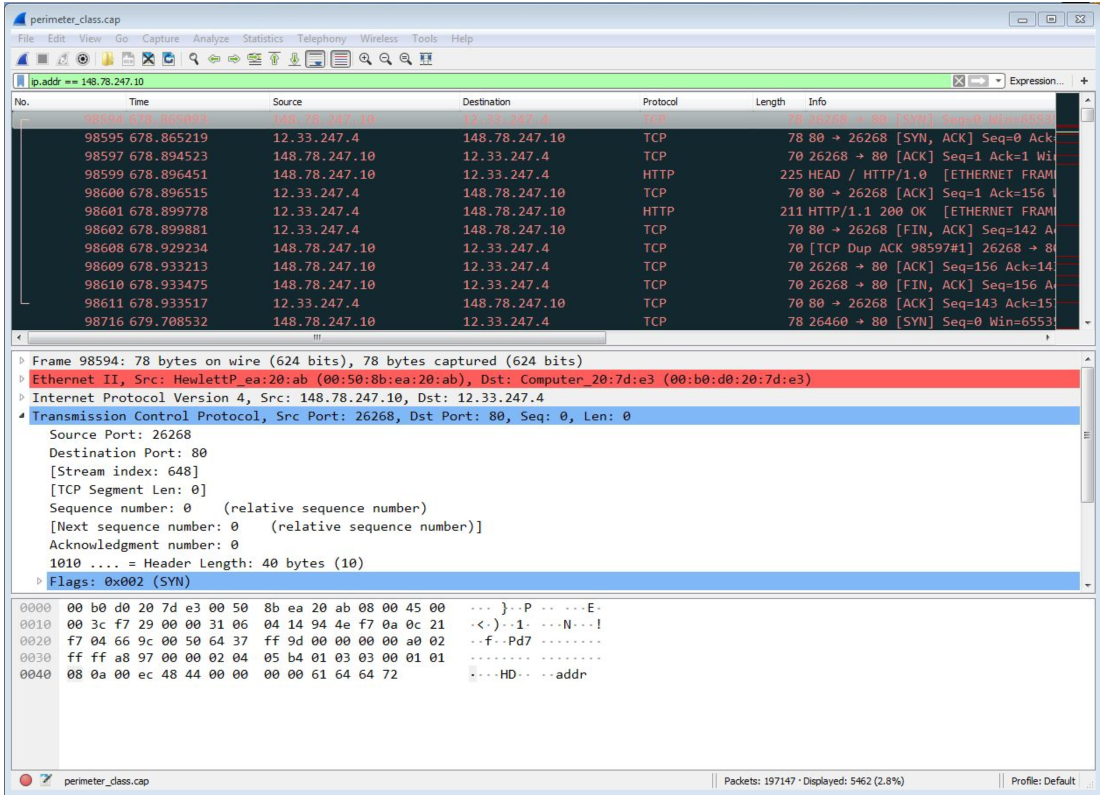
```
$ tshark -r sample.pcap -T fields -e http.user_agent tcp.
dstport==80 | sort | uniq -c | sort -n | head -10
      2 Microsoft Office/16.0
      2 Valve/Steam HTTP Client 1.0 (client;windows;10;1551832902)
      3 Valve/Steam HTTP Client 1.0
     11 Microsoft BITS/7.5
     11 Windows-Update-Agent
     12 Microsoft-CryptoAPI/6.1
    104 PCU
```

Wireshark

- What's it good for?
  - Packet analysis with guardrails
  - Stream level summaries
- When to use it
  - As part of a manual analysis
  - When steps cannot be automated
- Where to get it

https://www.wireshark.org/

Useful when I have a target


perimeter_class.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
ip.addr == 148.78.247.10
```

```
No.          Time              Source              Destination         Protocol      Length  Info
      98594 678.865093    148.78.247.10     12.33.247.4         TCP              78 26268 → 80 [SYN] Seq=0 Win=6553
      98595 678.865219    12.33.247.4       148.78.247.10       TCP              78 80 → 26268 [SYN, ACK] Seq=0 Ack
      98597 678.894523    148.78.247.10     12.33.247.4         TCP              70 26268 → 80 [ACK] Seq=1 Ack=1 Wi
      98599 678.896451    148.78.247.10     12.33.247.4         HTTP            225 HEAD / HTTP/1.0  [ETHERNET FRAM
      98600 678.896515    12.33.247.4       148.78.247.10       TCP              70 80 → 26268 [ACK] Seq=1 Ack=156 
      98601 678.899778    12.33.247.4       148.78.247.10       HTTP            211 HTTP/1.1 200 OK  [ETHERNET FRAM
      98602 678.899881    12.33.247.4       148.78.247.10       TCP              70 80 → 26268 [FIN, ACK] Seq=142 A
      98608 678.929234    148.78.247.10     12.33.247.4         TCP              70 [TCP Dup ACK 98597#1] 26268 → 8
      98609 678.933213    148.78.247.10     12.33.247.4         TCP              70 26268 → 80 [ACK] Seq=156 Ack=14
      98610 678.933475    148.78.247.10     12.33.247.4         TCP              70 26268 → 80 [FIN, ACK] Seq=156 A
      98611 678.933517    12.33.247.4       148.78.247.10       TCP              70 80 → 26268 [ACK] Seq=143 Ack=15
      98716 679.708532    148.78.247.10     12.33.247.4         TCP              78 26460 → 80 [SYN] Seq=0 Win=6553
```

```
▷ Frame 98594: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
▷ Ethernet II, Src: HewlettP_ea:20:ab (00:50:8b:ea:20:ab), Dst: Computer_20:7d:e3 (00:b0:d0:20:7d:e3)
▷ Internet Protocol Version 4, Src: 148.78.247.10, Dst: 12.33.247.4
◢ Transmission Control Protocol, Src Port: 26268, Dst Port: 80, Seq: 0, Len: 0
     Source Port: 26268
     Destination Port: 80
     [Stream index: 648]
     [TCP Segment Len: 0]
     Sequence number: 0    (relative sequence number)
     [Next sequence number: 0    (relative sequence number)]
     Acknowledgment number: 0
     1010 .... = Header Length: 40 bytes (10)
   ▷ Flags: 0x002 (SYN)
```

```
0000  00 b0 d0 20 7d e3 00 50  8b ea 20 ab 08 00 45 00   ··· }··P ·· ···E·
0010  00 3c f7 29 00 00 31 06  04 14 94 4e f7 0a 0c 21   ·<·)··1· ···N···!
0020  f7 04 66 9c 00 50 64 37  ff 9d 00 00 00 00 a0 02   ··f··Pd7 ········
0030  ff ff a8 97 00 00 02 04  05 b4 01 03 03 00 01 01   ········ ········
0040  08 0a 00 ec 48 44 00 00  00 00 61 64 64 72         ····HD·· ··addr
```

perimeter_class.cap | Packets: 197147 · Displayed: 5462 (2.8%) | Profile: Default

Zeek

- Old name = Bro   New name = Zeek
- What's it good for?
  - Near real time analysis (1+ hour latency)
  - More storage friendly than pcaps
- When to use it
  - When you need to scale
  - When you know what attributes to review
- Where to get it

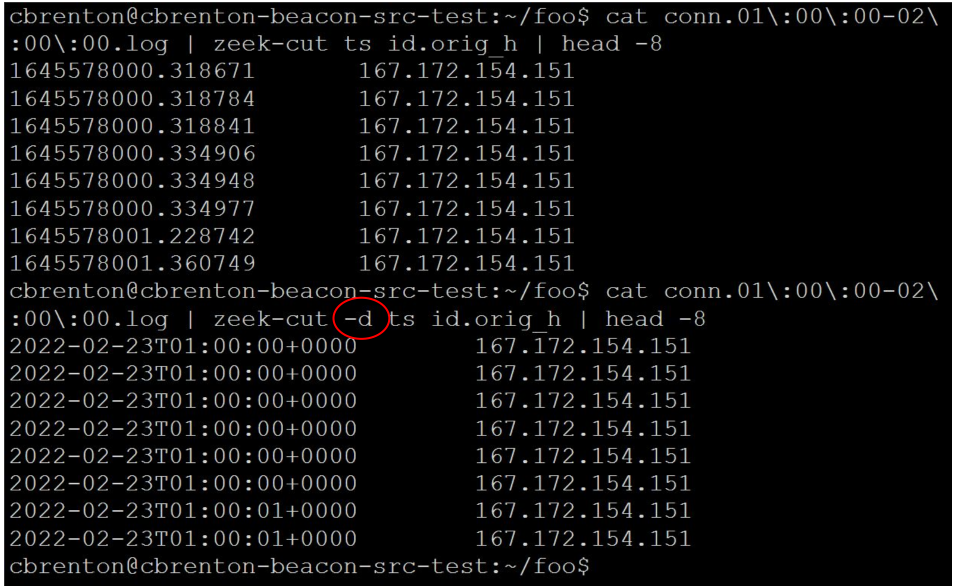
https://www.zeek.org/
sudo apt -y install zeek

Zeek example - cert check

```
$ cat ssl* | zeek-cut id.orig_h id.resp_h id.resp_p
validation_status | grep 'self signed' | sort | uniq
122.228.10.51   192.168.88.2    9943    self signed certificate in
certificate chain
24.111.1.134    192.168.88.2    9943    self signed certificate in
certificate chain
71.6.167.142    192.168.88.2    9943    self signed certificate in
certificate chain
```

-d for human readable times

- Zeek-cut prints epoch time by default
- "-d" converts to human readable



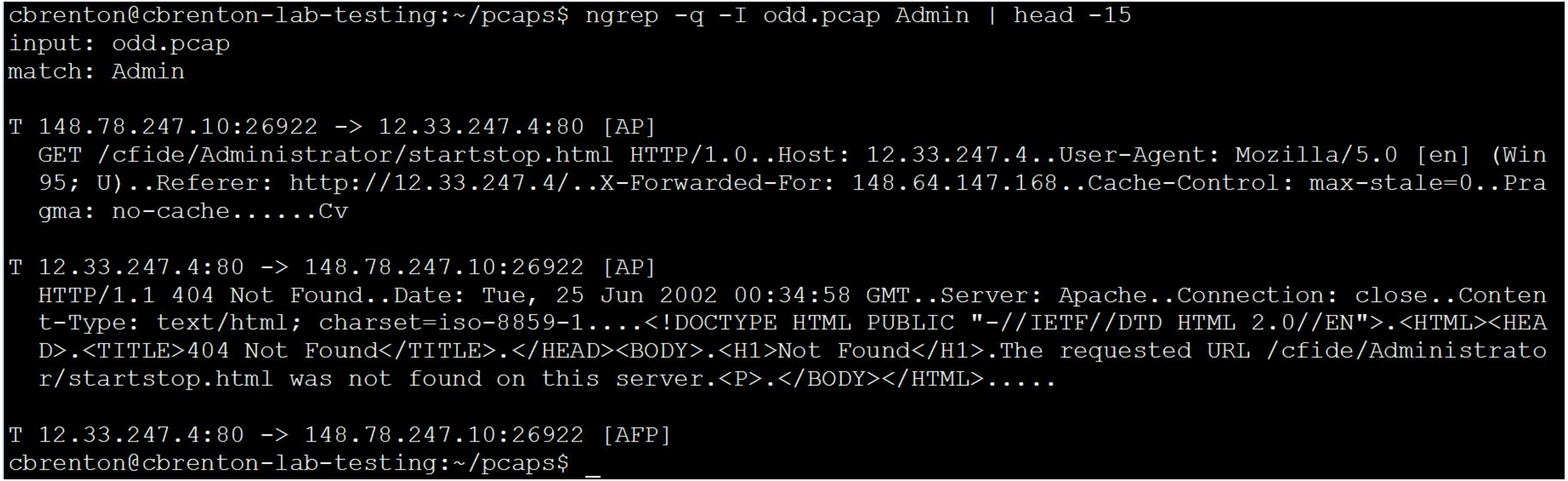
```
cbrenton@cbrenton-beacon-src-test:~/foo$ cat conn.01\:00\:00-02\
:00\:00.log | zeek-cut ts id.orig_h | head -8
1645578000.318671       167.172.154.151
1645578000.318784       167.172.154.151
1645578000.318841       167.172.154.151
1645578000.334906       167.172.154.151
1645578000.334948       167.172.154.151
1645578000.334977       167.172.154.151
1645578001.228742       167.172.154.151
1645578001.360749       167.172.154.151
cbrenton@cbrenton-beacon-src-test:~/foo$ cat conn.01\:00\:00-02\
:00\:00.log | zeek-cut -d ts id.orig_h | head -8
2022-02-23T01:00:00+0000        167.172.154.151
2022-02-23T01:00:00+0000        167.172.154.151
2022-02-23T01:00:00+0000        167.172.154.151
2022-02-23T01:00:00+0000        167.172.154.151
2022-02-23T01:00:00+0000        167.172.154.151
2022-02-23T01:00:00+0000        167.172.154.151
2022-02-23T01:00:01+0000        167.172.154.151
2022-02-23T01:00:01+0000        167.172.154.151
cbrenton@cbrenton-beacon-src-test:~/foo$
```

ngrep

- Pattern match on passing packets
- Like "grep" for network traffic
- Useful for quick checks
    - NIDS with signature better choice for long term
- Useful switches
    - "-q" = Don't print "#" for non-matches
    - "-I" = Read a pcap file

https://github.com/jpr5/ngrep
sudo apt install ngrep

ngrep example



```
cbrenton@cbrenton-lab-testing:~/pcaps$ ngrep -q -I odd.pcap Admin | head -15
input: odd.pcap
match: Admin

T 148.78.247.10:26922 -> 12.33.247.4:80 [AP]
  GET /cfide/Administrator/startstop.html HTTP/1.0..Host: 12.33.247.4..User-Agent: Mozilla/5.0 [en] (Win
  95; U)..Referer: http://12.33.247.4/..X-Forwarded-For: 148.64.147.168..Cache-Control: max-stale=0..Pra
  gma: no-cache......Cv

T 12.33.247.4:80 -> 148.78.247.10:26922 [AP]
  HTTP/1.1 404 Not Found..Date: Tue, 25 Jun 2002 00:34:58 GMT..Server: Apache..Connection: close..Conten
  t-Type: text/html; charset=iso-8859-1....<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<HTML><HEA
  D>.<TITLE>404 Not Found</TITLE>.</HEAD><BODY>.<H1>Not Found</H1>.The requested URL /cfide/Administrato
  r/startstop.html was not found on this server.<P>.</BODY></HTML>.....

T 12.33.247.4:80 -> 148.78.247.10:26922 [AFP]
cbrenton@cbrenton-lab-testing:~/pcaps$ _
```

Datamash

- What's it good for?
  - Similar to the R-base tools, but more extensive
  - Performing simple calculation on data
- When to use it
  - Performing calculations on multiple lines
  - Statistical analysis
- Where to get it

https://www.gnu.org/software/datamash/
sudo apt install datamash

Datamash example

```
cbrenton@cbrenton-lab-testing:~/lab3$ cat conn.log | zeek-cut
id.orig_h id.resp_h duration | sort -k3 -rn | head -5
192.168.1.105   143.166.11.10   328.754946
192.168.1.104   63.245.221.11   41.884228
192.168.1.104   63.245.221.11   31.428539
192.168.1.105   143.166.11.10   27.606923
192.168.1.102   192.168.1.1     4.190865

cbrenton@cbrenton-lab-testing:~/lab3$ cat conn.log | zeek-cut
id.orig_h id.resp_h duration | grep -v -e '^$' | grep -v '-' | sort |
datamash -g 1,2 sum 3| sort -k3 -rn | head -5
192.168.1.105   143.166.11.10   356.361869
192.168.1.104   63.245.221.11   73.312767
192.168.1.102   192.168.1.1     5.464553
192.168.1.103   192.168.1.1     4.956918
192.168.1.105   192.168.1.1     1.99374
```

Duplicate IPs

RITA

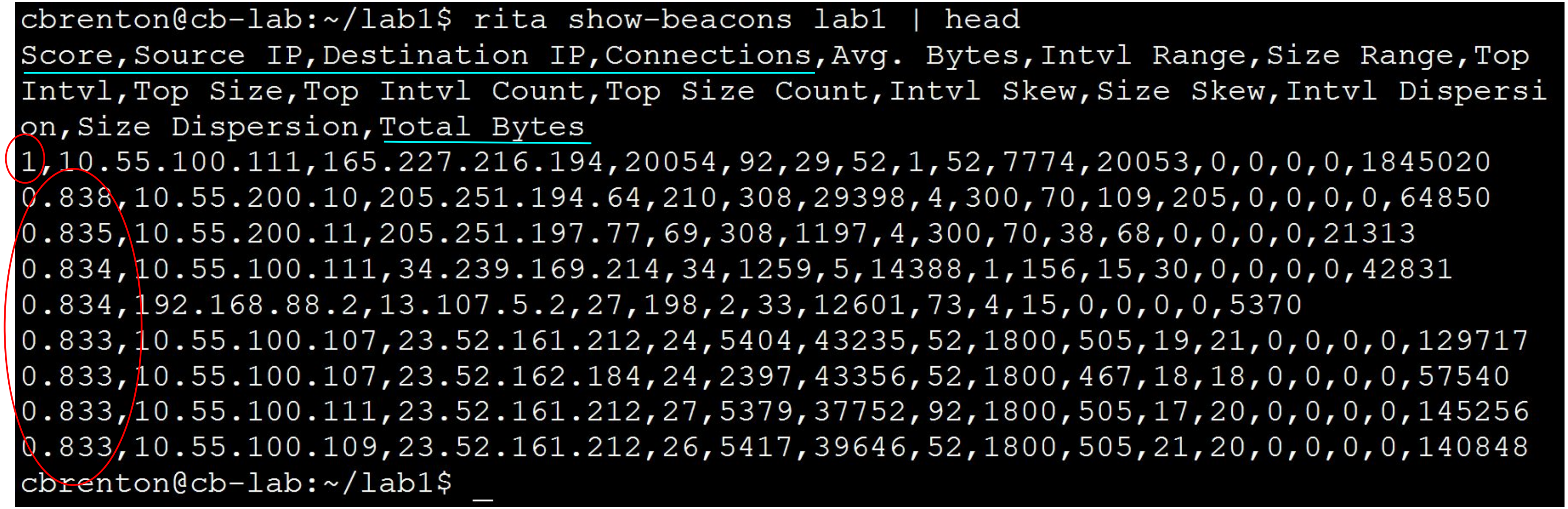
- What's it good for?
  - Beacon & long conn at scale
  - Some secondary attributes
- When to use it
  - Can better organize Zeek data
  - Good when you are comfortable scripting
  - Will scale but can be time consuming
- Where to get it

  https://github.com/activecm/rita

RITA syntax examples

```
rita <command to use> <db to check>

rita show-long-connections lab1
rita show-long-connections lab1 | head -10

rita list
```

RITA example - beacons



```
cbrenton@cb-lab:~/lab1$ rita show-beacons lab1 | head
Score,Source IP,Destination IP,Connections,Avg. Bytes,Intvl Range,Size Range,Top
Intvl,Top Size,Top Intvl Count,Top Size Count,Intvl Skew,Size Skew,Intvl Dispersi
on,Size Dispersion,Total Bytes
1,10.55.100.111,165.227.216.194,20054,92,29,52,1,52,7774,20053,0,0,0,0,1845020
0.838,10.55.200.10,205.251.194.64,210,308,29398,4,300,70,109,205,0,0,0,0,64850
0.835,10.55.200.11,205.251.197.77,69,308,1197,4,300,70,38,68,0,0,0,0,21313
0.834,10.55.100.111,34.239.169.214,34,1259,5,14388,1,156,15,30,0,0,0,0,42831
0.834,192.168.88.2,13.107.5.2,27,198,2,33,12601,73,4,15,0,0,0,0,5370
0.833,10.55.100.107,23.52.161.212,24,5404,43235,52,1800,505,19,21,0,0,0,0,129717
0.833,10.55.100.107,23.52.162.184,24,2397,43356,52,1800,467,18,18,0,0,0,0,57540
0.833,10.55.100.111,23.52.161.212,27,5379,37752,92,1800,505,17,20,0,0,0,0,145256
0.833,10.55.100.109,23.52.161.212,26,5417,39646,52,1800,505,21,20,0,0,0,0,140848
cbrenton@cb-lab:~/lab1$ _
```

Scale is 0 - 1 with 1.0 being a perfect beacon score

RITA can also check

- ▷ Beacons based on HTTP/host or TLS/SNI
- ▷ Beacons based on FQDN
- ▷ Beacons through SOCKS server
- ▷ Long connections
- ▷ Still open (not yet logged) connections
- ▷ C2 over DNS
- ▷ Matches against your threat intel list

Passer

```
TC,172.1.199.23,TCP_43,open,
TC,172.16.199.23,TCP_55443,open,
UC,172.16.199.23,UDP_626,open,serialnumberd/clientscanner likely nmap
scan Warnings:scan
UC,172.16.199.23,UDP_1194,open,openvpn/client Warnings:tunnel
UC,172.16.199.23,UDP_3386,open,udp3386/client
UC,172.16.199.23,UDP_5632,open,pcanywherestat/clientscanner
Warnings:scan
UC,172.16.199.23,UDP_64738,open,shodan_host/clientscanner abcdefgh
Unlisted host Warnings:scan
DN,2001:db8:1001:0000:0000:0000:0000:0015,AAAA,ns3.markmonitor.com.,
DN,fe80:0000:0000:0000:189f:545b:7d4c:eeb8,PTR,Apple
TV._device-info._tcp.local.,model=J105aA
```

Beacon/Threat Simulator

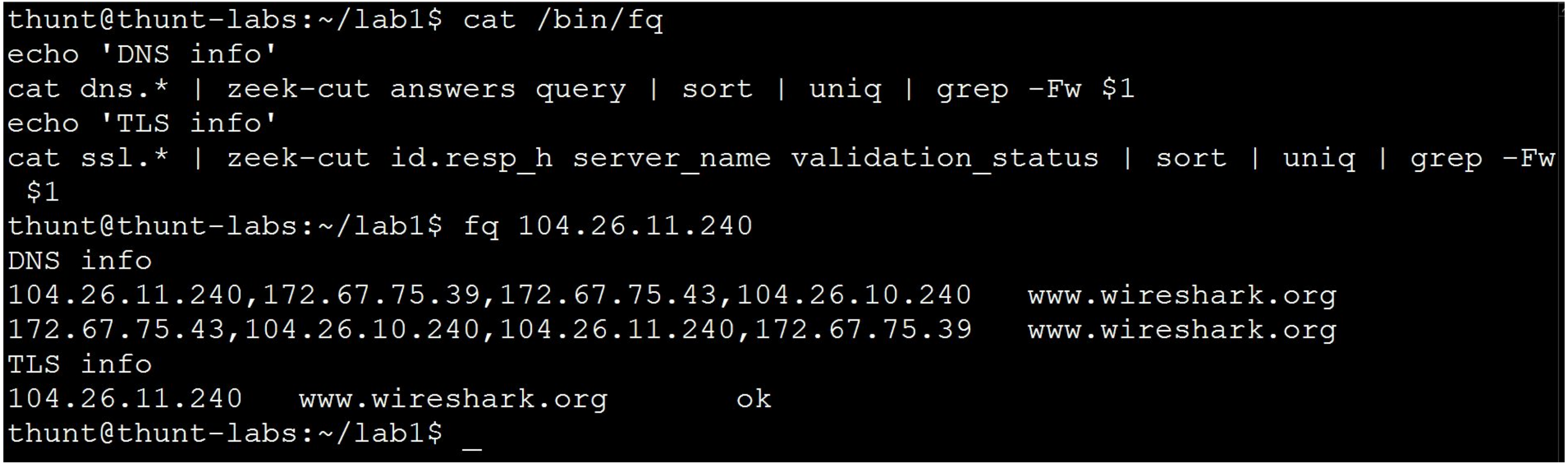
- Permits you to test your C2 detection setup
- Target any TCP or UDP port
- Can jitter timing
- Can jitter payload size
- Not designed to exfiltrate data!

```
beacon-simulator.sh <target IP> 80 300 10 tcp 5000
```

Connect to TCP/80 on target IP every 300 seconds, +/-10 seconds, vary payload between 0-5,000 bytes

https://github.com/activecm/threat-tools

Create your own scripts!



```
thunt@thunt-labs:~/lab1$ cat /bin/fq
echo 'DNS info'
cat dns.* | zeek-cut answers query | sort | uniq | grep -Fw $1
echo 'TLS info'
cat ssl.* | zeek-cut id.resp_h server_name validation_status | sort | uniq | grep -Fw
 $1
thunt@thunt-labs:~/lab1$ fq 104.26.11.240
DNS info
104.26.11.240,172.67.75.39,172.67.75.43,104.26.10.240   www.wireshark.org
172.67.75.43,104.26.10.240,104.26.11.240,172.67.75.39   www.wireshark.org
TLS info
104.26.11.240   www.wireshark.org       ok
thunt@thunt-labs:~/lab1$ _
```

Example script you can create to make life easier
"fq" check dns.log and ssl.log in the local directory
Returns info on specified IP address

ACTIVE COUNTERMEASURES

C2 Labs

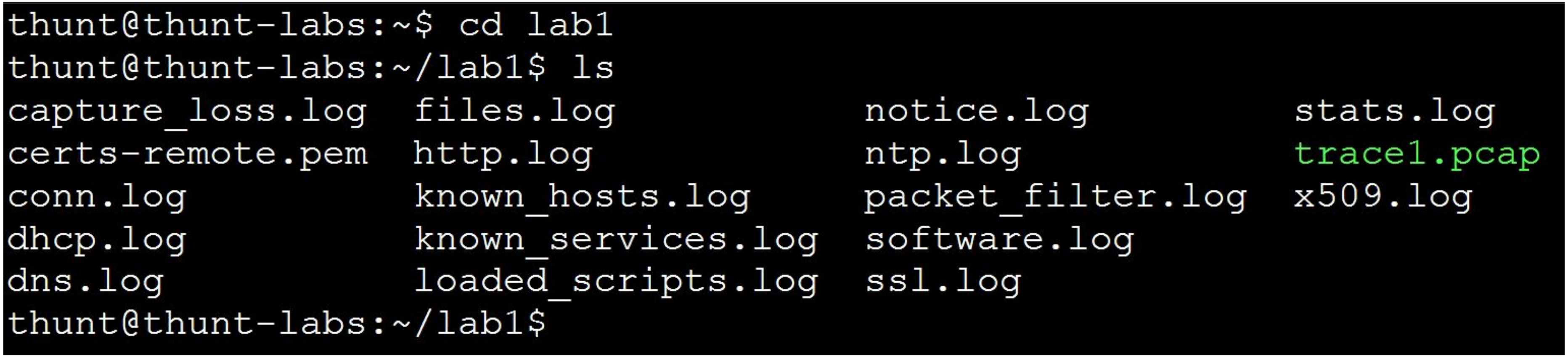
What We Will Cover

- This section is mostly hands on labs
- Implement what you have learned
- Lab format:
  - Given a problem
    - Use earlier content to help solve
  - Given hints
    - If you don't know where to start, try the hints
  - Given the exact commands
  - Solution
    - Complete walk through of the solution

Reminder

- All lab files are on the VM
  - No network access needed
  - Unless you want to do third party research
  - Can also be done from your host system browser
- Login info
  - Name = thunt
  - Password = aybab2u
- Labs are in /home/thunt/lab*

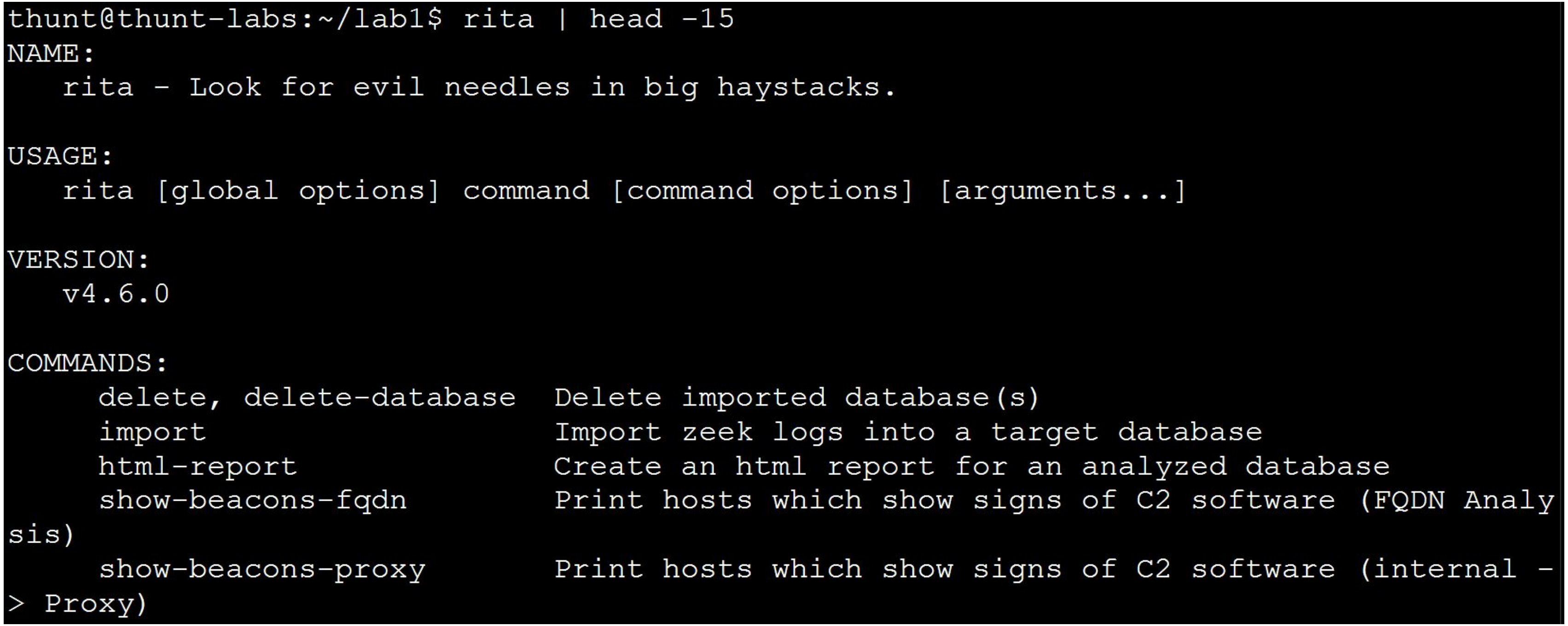
Some commands to get you started



```
thunt@thunt-labs:~$ cd lab1
thunt@thunt-labs:~/lab1$ ls
capture_loss.log  files.log           notice.log         stats.log
certs-remote.pem  http.log            ntp.log            trace1.pcap
conn.log          known_hosts.log     packet_filter.log  x509.log
dhcp.log          known_services.log  software.log
dns.log           loaded_scripts.log  ssl.log
thunt@thunt-labs:~/lab1$
```

"cd" to change to a new directory
"ls" will list all files
".log" files are Zeek log files
".pcap" or ".pcapng" files are pcap traffic captures
I've already created the Zeek logs from the pcap for you

RITA commands



```
thunt@thunt-labs:~/lab1$ rita | head -15
NAME:
   rita - Look for evil needles in big haystacks.

USAGE:
   rita [global options] command [command options] [arguments...]

VERSION:
   v4.6.0

COMMANDS:
     delete, delete-database  Delete imported database(s)
     import                   Import zeek logs into a target database
     html-report              Create an html report for an analyzed database
     show-beacons-fqdn        Print hosts which show signs of C2 software (FQDN Analy
sis)
     show-beacons-proxy       Print hosts which show signs of C2 software (internal -
> Proxy)
```

Type "rita" or "rita | less" to see a list of commands

Find long connections

- Files located in /home/thunt/lab1
- Easiest to work with RITA
- Record any IPs you consider suspect
    - We will further investigate them later

Find long conns - Hints

- Long connections is a relative term. You need to know the length of time being audited.
- pcap - "capinfos" can help
- Zeek - Difference between highest and lowest timestamp (ts) in conn.log
  - Not necessarily first and last

Useful commands to try

```
capinfos -aeu trace1.pcap
cat conn.log | zeek-cut ts | datamash range 1


rita show-long-connections lab1 | head
```

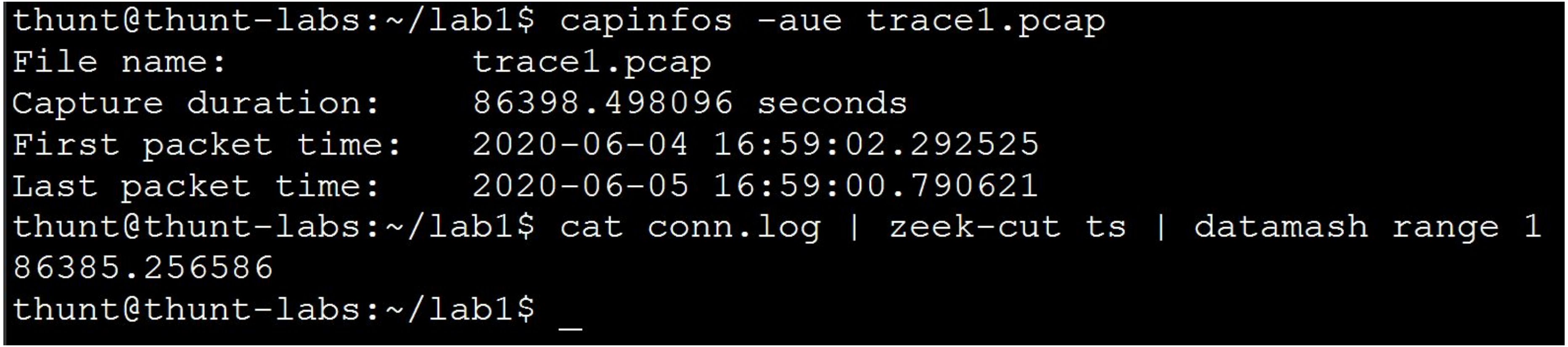
Long conns - Answers

- Capinfos to check capture duration
  - 86,398 seconds
  - 86,400 = 24 hours
  - Look for connections lasting 20,000+
  - Or about 5.5 hours

- What if I only have Zeek logs?

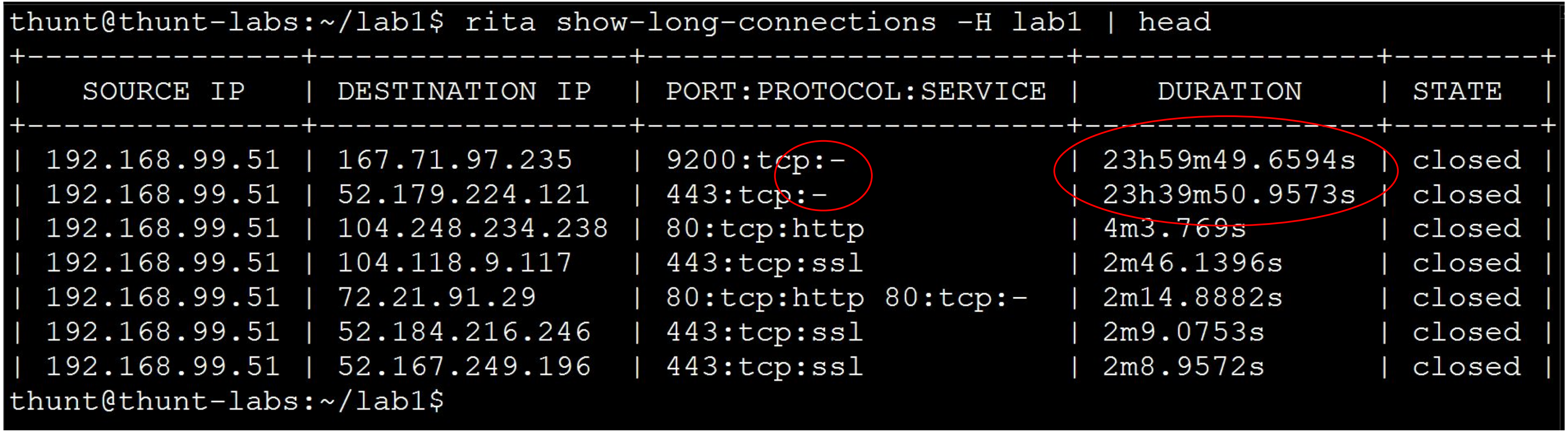
```
cat conn.log | zeek-cut ts | datamash range 1
```

About a day's worth of data



```
thunt@thunt-labs:~/lab1$ capinfos -aue trace1.pcap
File name:           trace1.pcap
Capture duration:    86398.498096 seconds
First packet time:   2020-06-04 16:59:02.292525
Last packet time:    2020-06-05 16:59:00.790621
thunt@thunt-labs:~/lab1$ cat conn.log | zeek-cut ts | datamash range 1
86385.256586
thunt@thunt-labs:~/lab1$ _
```

RITA output



```
thunt@thunt-labs:~/lab1$ rita show-long-connections -H lab1 | head
+---------------+-----------------+-------------------------+----------------+--------+
|   SOURCE IP   | DESTINATION IP  | PORT:PROTOCOL:SERVICE |    DURATION    | STATE  |
+---------------+-----------------+-------------------------+----------------+--------+
| 192.168.99.51 | 167.71.97.235   | 9200:tcp:-            | 23h59m49.6594s | closed |
| 192.168.99.51 | 52.179.224.121  | 443:tcp:-             | 23h39m50.9573s | closed |
| 192.168.99.51 | 104.248.234.238 | 80:tcp:http           | 4m3.769s       | closed |
| 192.168.99.51 | 104.118.9.117   | 443:tcp:ssl           | 2m46.1396s     | closed |
| 192.168.99.51 | 72.21.91.29     | 80:tcp:http 80:tcp:-  | 2m14.8882s     | closed |
| 192.168.99.51 | 52.184.216.246  | 443:tcp:ssl           | 2m9.0753s      | closed |
| 192.168.99.51 | 52.167.249.196  | 443:tcp:ssl           | 2m8.9572s      | closed |
thunt@thunt-labs:~/lab1$
```

No service info is common with long connections
Usually means connection started before data capture was launched

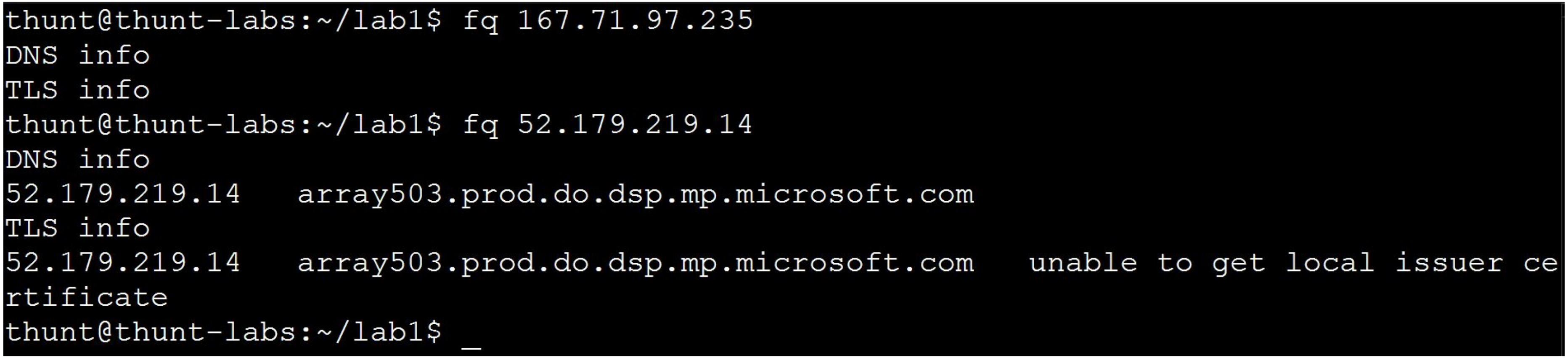
Next lab!

- Let's investigate the external IP of the two longest session
  - 167.71.97.235
  - 52.179.219.14
- We'll use three common research methods
  - "fq" command (checks dns.log and ssl.log)
  - AbuseIPDB
    - https://www.abuseipdb.com/check/<IP address>
  - AlienVault
    - https://otx.alienvault.com/indicator/ip/<IP address>

Investigate - hints

- You were given the two IP addresses to research
- fq <IP address>
- Use a browser to connect to the two research Websites and enter each IP

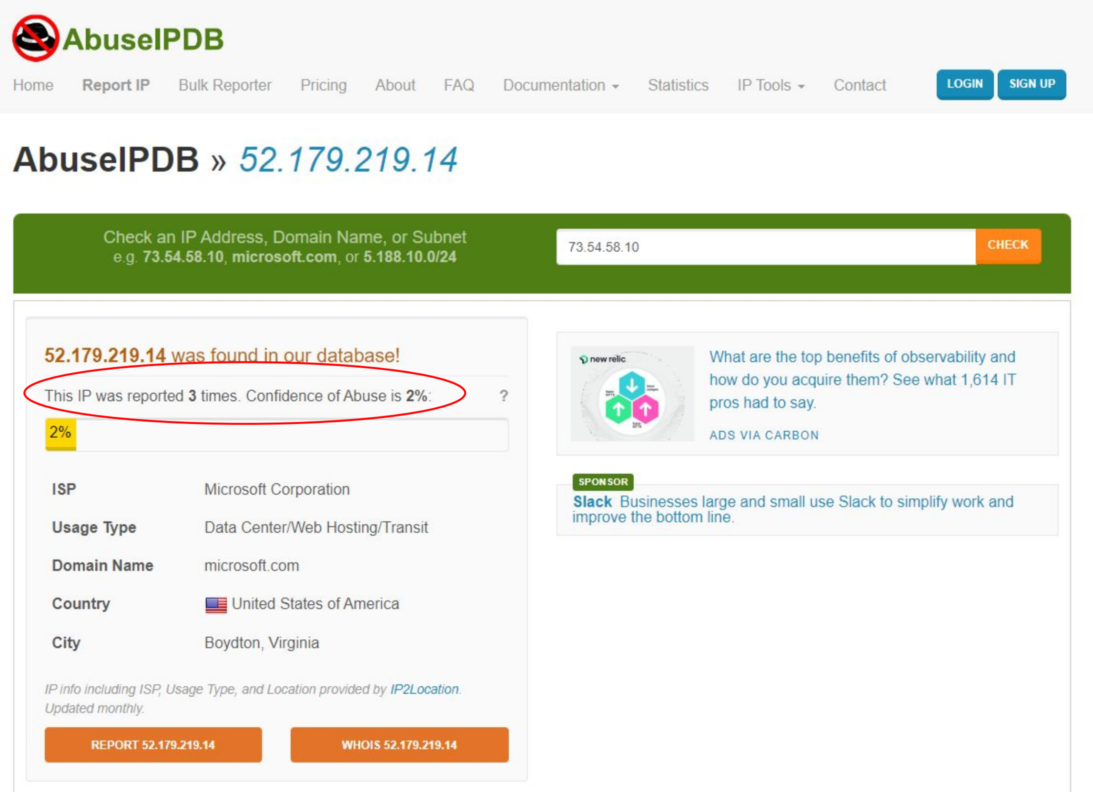
One out of two is not bad



```
thunt@thunt-labs:~/lab1$ fq 167.71.97.235
DNS info
TLS info
thunt@thunt-labs:~/lab1$ fq 52.179.219.14
DNS info
52.179.219.14   array503.prod.do.dsp.mp.microsoft.com
TLS info
52.179.219.14   array503.prod.do.dsp.mp.microsoft.com   unable to get local issuer ce
rtificate
thunt@thunt-labs:~/lab1$ _
```

Second IP was contacted because system was trying to reach a microsoft.com host.
MS includes a cert for this system in Windows

AbuseIPDB info on MS system



AbuseIPDB
Home Report IP Bulk Reporter Pricing About FAQ Documentation IP Tools Contact LOGIN SIGN UP

AbuseIPDB » 52.179.219.14

Check an IP Address, Domain Name, or Subnet
e.g. **73.54.58.10**, **microsoft.com**, or **5.188.10.0/24**

73.54.58.10 CHECK

52.179.219.14 was found in our database!

This IP was reported **3** times. Confidence of Abuse is **2%**: ?

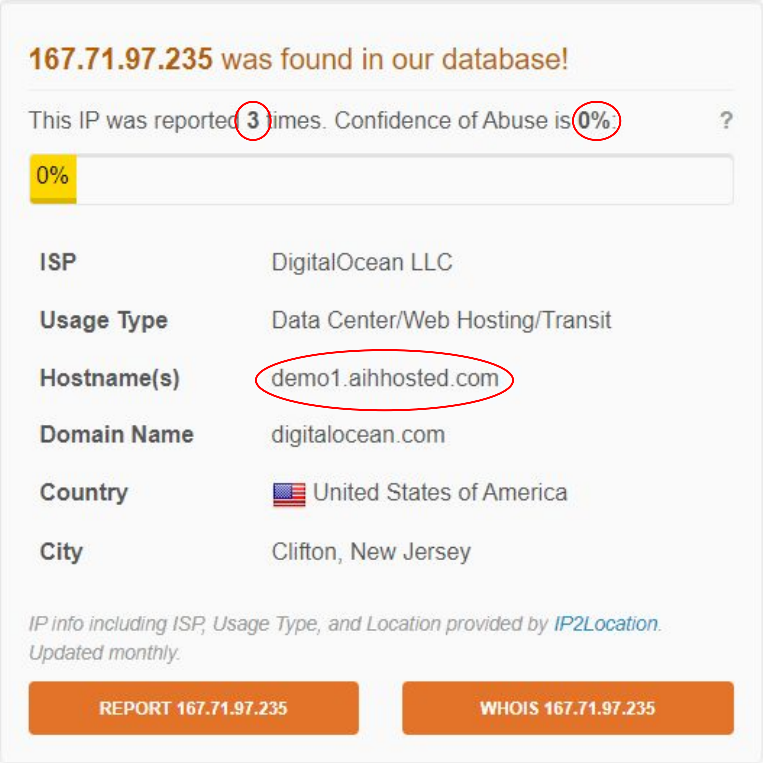
2%

ISP	Microsoft Corporation
Usage Type	Data Center/Web Hosting/Transit
Domain Name	microsoft.com
Country	🇺🇸 United States of America
City	Boydton, Virginia

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

REPORT 52.179.219.14 WHOIS 52.179.219.14

AbuseIPDB on first IP



167.71.97.235 was found in our database!

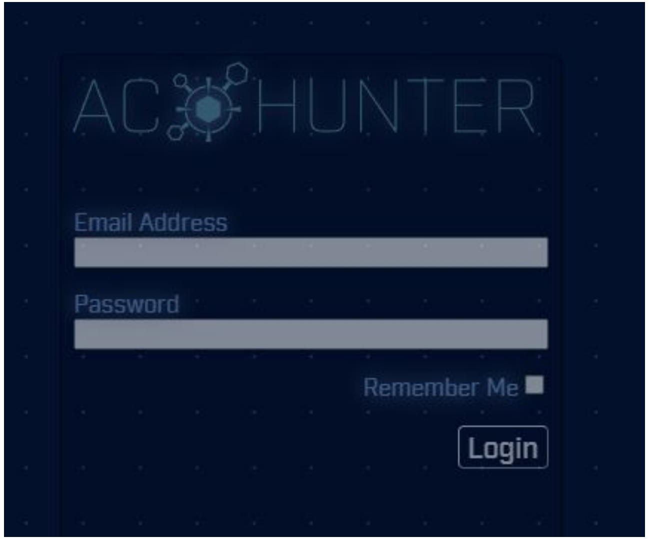
This IP was reported 3 times. Confidence of Abuse is 0%: ?

0%

ISP	DigitalOcean LLC
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	demo1.aihhosted.com
Domain Name	digitalocean.com
Country	United States of America
City	Clifton, New Jersey

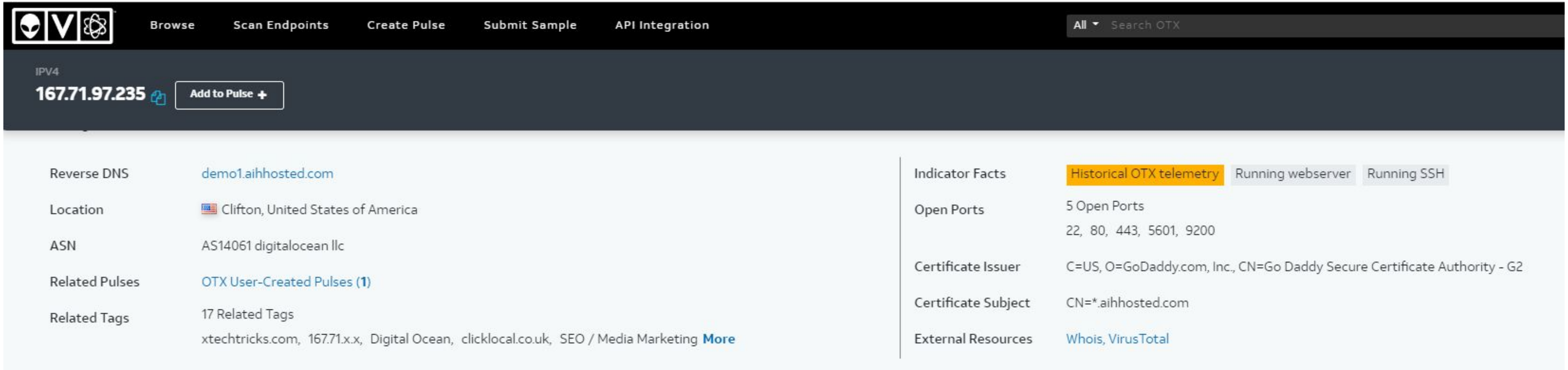
IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

Connecting to demo1 via browser



Should only be done with a source IP with no association with your org!
Trying www.aihhosted.com would be another option

AlienVault useful data



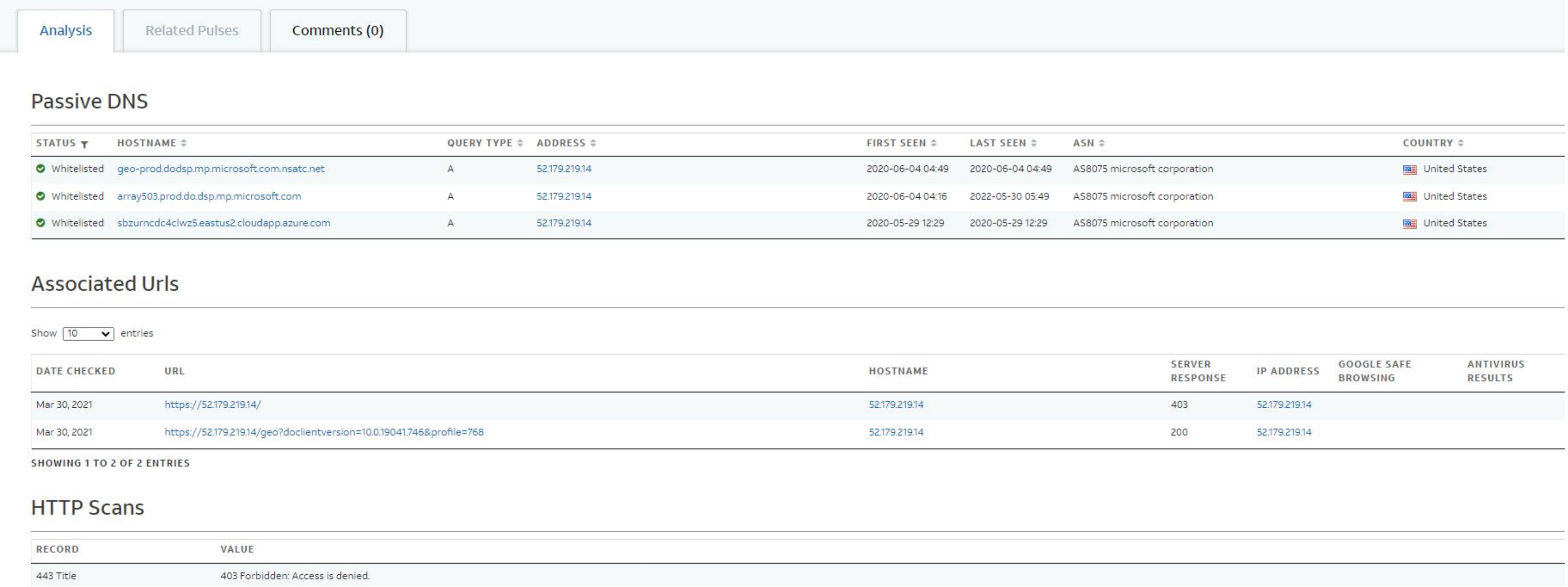
IPV4

167.71.97.235

Reverse DNS	demo1.aihhosted.com
Location	Clifton, United States of America
ASN	AS14061 digitalocean llc
Related Pulses	OTX User-Created Pulses (1)
Related Tags	17 Related Tags xtechtricks.com, 167.71.x.x, Digital Ocean, clicklocal.co.uk, SEO / Media Marketing **More**

Indicator Facts	Historical OTX telemetry Running webserver Running SSH
Open Ports	5 Open Ports 22, 80, 443, 5601, 9200
Certificate Issuer	C=US, O=GoDaddy.com, Inc., CN=Go Daddy Secure Certificate Authority - G2
Certificate Subject	CN=*.aihhosted.com
External Resources	Whois, VirusTotal

AlienVault analysis



Passive DNS

STATUS	HOSTNAME	QUERY TYPE	ADDRESS	FIRST SEEN	LAST SEEN	ASN	COUNTRY
✓ Whitelisted	geo-prod.dodsp.mp.microsoft.com.nsatc.net	A	52.179.219.14	2020-06-04 04:49	2020-06-04 04:49	AS8075 microsoft corporation	United States
✓ Whitelisted	array503.prod.do.dsp.mp.microsoft.com	A	52.179.219.14	2020-06-04 04:16	2022-05-30 05:49	AS8075 microsoft corporation	United States
✓ Whitelisted	sbzurncdc4clwz5.eastus2.cloudapp.azure.com	A	52.179.219.14	2020-05-29 12:29	2020-05-29 12:29	AS8075 microsoft corporation	United States

Associated Urls

Show 10 entries

DATE CHECKED	URL	HOSTNAME	SERVER RESPONSE	IP ADDRESS	GOOGLE SAFE BROWSING	ANTIVIRUS RESULTS
Mar 30, 2021	https://52.179.219.14/	52.179.219.14	403	52.179.219.14		
Mar 30, 2021	https://52.179.219.14/geo?doclientversion=10.0.19041.746&profile=768	52.179.219.14	200	52.179.219.14		

SHOWING 1 TO 2 OF 2 ENTRIES

HTTP Scans

RECORD	VALUE
443 Title	403 Forbidden: Access is denied.

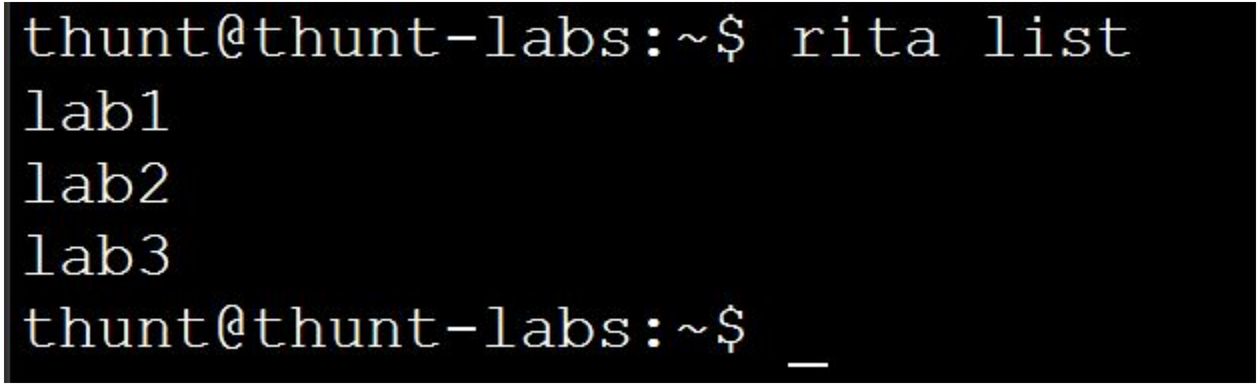
Answers

- Longest connection appears to be business partner related
- Second longest is is used in keeping Windows 10 updated
- Neither appear to be malware related

Let's look for beacons

- Beacons are hard to detect!
- Neither pcaps or Zeek logs record dwell time between connections
- Using connect quantity misses low & slow
- Using session size also problematic
- RITA to the rescue!
- We've already imported data into RITA

"list" imported data



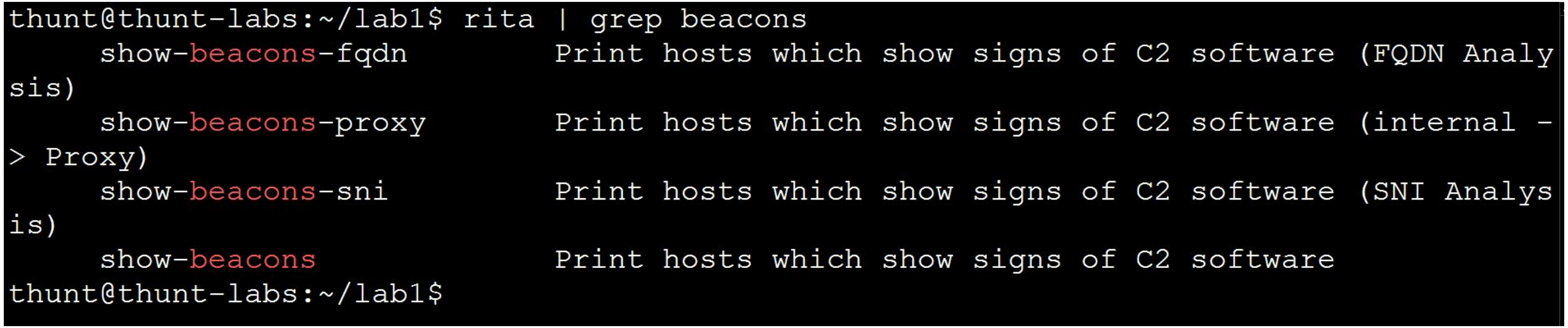
```
thunt@thunt-labs:~$ rita list
lab1
lab2
lab3
thunt@thunt-labs:~$ _
```

Lab time!

- Using RITA, identify potential beacons
- We are still working with "lab1"
- Consider any session scoring .8 or higher worthy of deeper analysis

Hints

- RITA is the best tool for beacon detection
- Remember the syntax:
  - rita <command> <database>
- Finding RITA's beacon commands



```
thunt@thunt-labs:~/lab1$ rita | grep beacons
     show-beacons-fqdn        Print hosts which show signs of C2 software (FQDN Analy
sis)
     show-beacons-proxy       Print hosts which show signs of C2 software (internal -
> Proxy)
     show-beacons-sni         Print hosts which show signs of C2 software (SNI Analys
is)
     show-beacons             Print hosts which show signs of C2 software
thunt@thunt-labs:~/lab1$
```

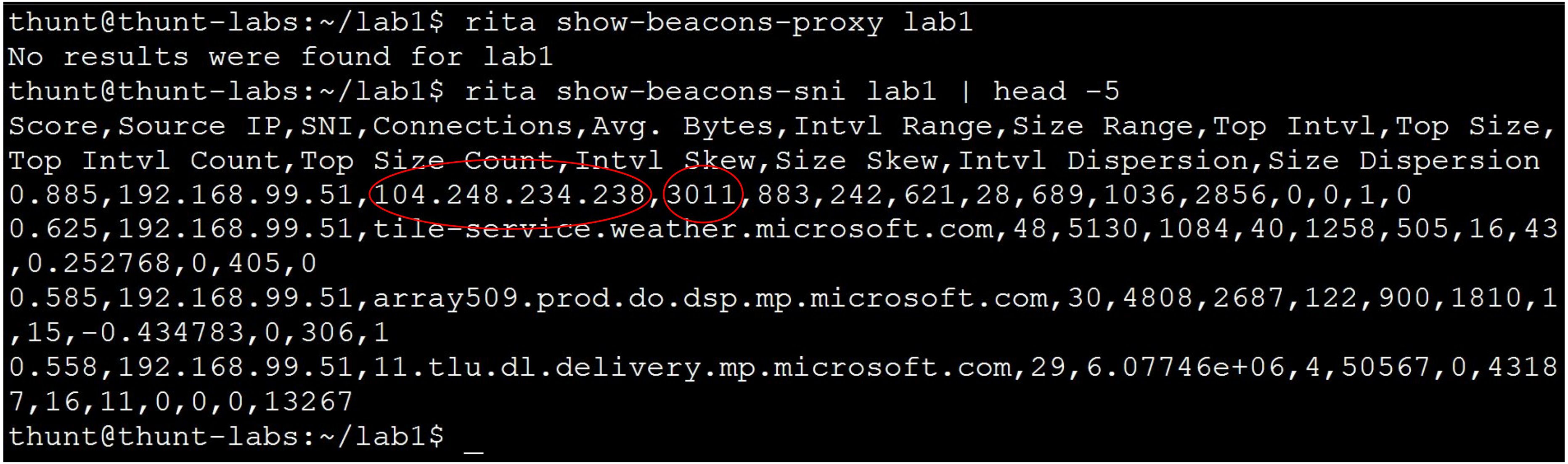
Commands

```
rita show-beacons-proxy lab1
rita show-beacons-sni lab1
rita show-beacons-fqdn lab1
rita show-beacons lab1
```

Answers - Beacon check order

- beacon-proxy
  - Only option if outbound SOCKS proxy is in use
- beacon-sni
  - Will check HTTP and HTTPS to all ports
  - Best way to catch C2 through CDN networks
- beacon-fqdn
  - Only useful for non HTTP/HTTPS to multiple IPs
- beacon
  - IP to IP check (no DNS being used)

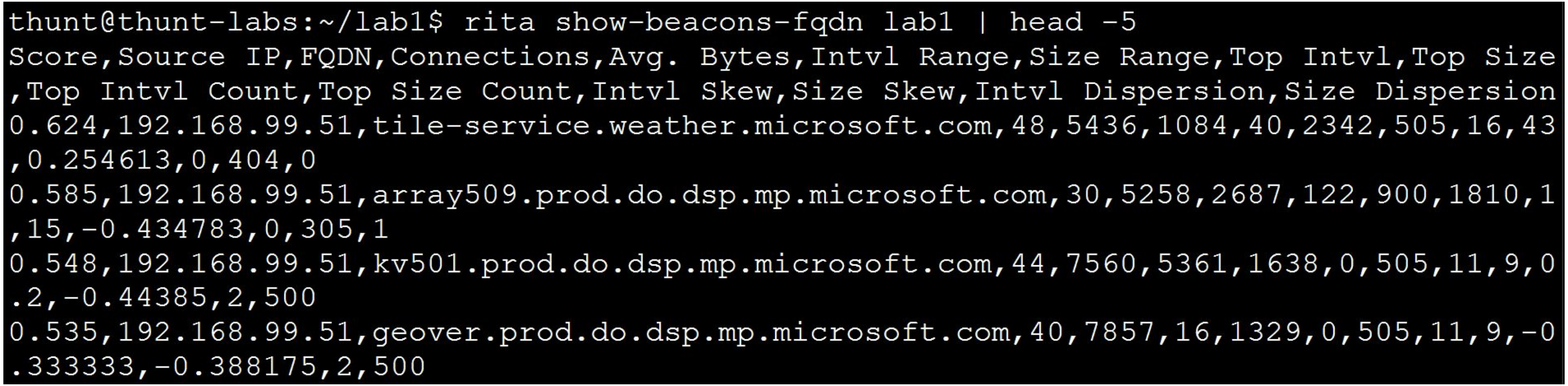
Answers - proxy & SNI



```
thunt@thunt-labs:~/lab1$ rita show-beacons-proxy lab1
No results were found for lab1
thunt@thunt-labs:~/lab1$ rita show-beacons-sni lab1 | head -5
Score,Source IP,SNI,Connections,Avg. Bytes,Intvl Range,Size Range,Top Intvl,Top Size,
Top Intvl Count,Top Size Count,Intvl Skew,Size Skew,Intvl Dispersion,Size Dispersion
0.885,192.168.99.51,104.248.234.238,3011,883,242,621,28,689,1036,2856,0,0,1,0
0.625,192.168.99.51,tile-service.weather.microsoft.com,48,5130,1084,40,1258,505,16,43
,0.252768,0,405,0
0.585,192.168.99.51,array509.prod.do.dsp.mp.microsoft.com,30,4808,2687,122,900,1810,1
,15,-0.434783,0,306,1
0.558,192.168.99.51,11.tlu.dl.delivery.mp.microsoft.com,29,6.07746e+06,4,50567,0,4318
7,16,11,0,0,0,13267
thunt@thunt-labs:~/lab1$ _
```

Server name is the IP address, that's very very odd
3,011 connections is really odd
We'll need to run this one down

Beacon FQDN

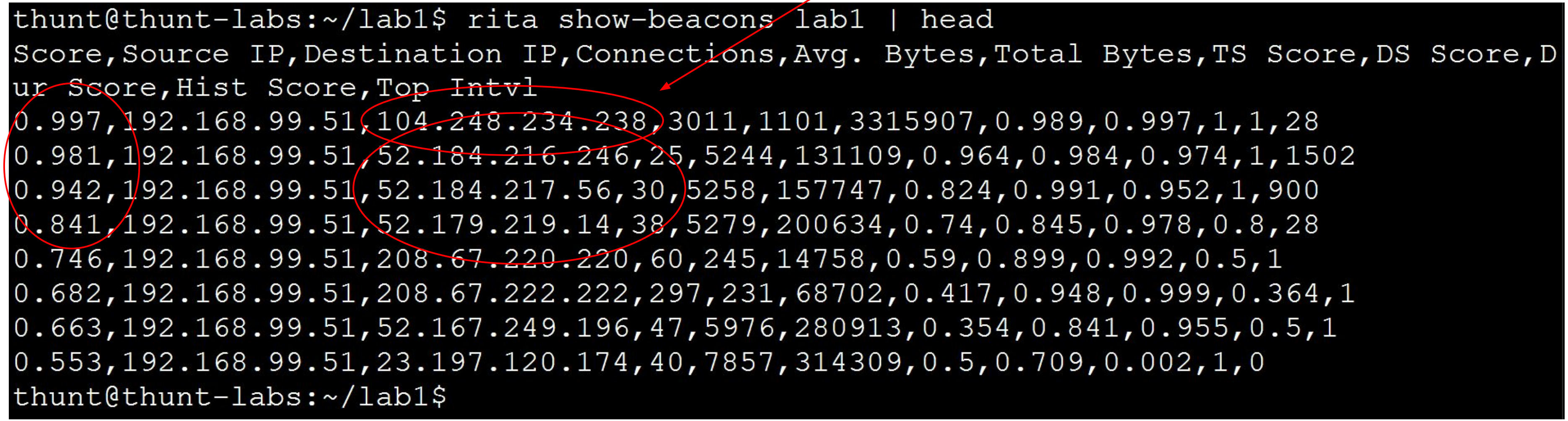


```
thunt@thunt-labs:~/lab1$ rita show-beacons-fqdn lab1 | head -5
Score,Source IP,FQDN,Connections,Avg. Bytes,Intvl Range,Size Range,Top Intvl,Top Size
,Top Intvl Count,Top Size Count,Intvl Skew,Size Skew,Intvl Dispersion,Size Dispersion
0.624,192.168.99.51,tile-service.weather.microsoft.com,48,5436,1084,40,2342,505,16,43
,0.254613,0,404,0
0.585,192.168.99.51,array509.prod.do.dsp.mp.microsoft.com,30,5258,2687,122,900,1810,1
,15,-0.434783,0,305,1
0.548,192.168.99.51,kv501.prod.do.dsp.mp.microsoft.com,44,7560,5361,1638,0,505,11,9,0
.2,-0.44385,2,500
0.535,192.168.99.51,geover.prod.do.dsp.mp.microsoft.com,40,7857,16,1329,0,505,11,9,-0
.333333,-0.388175,2,500
```

No results of note

IP to IP beacons

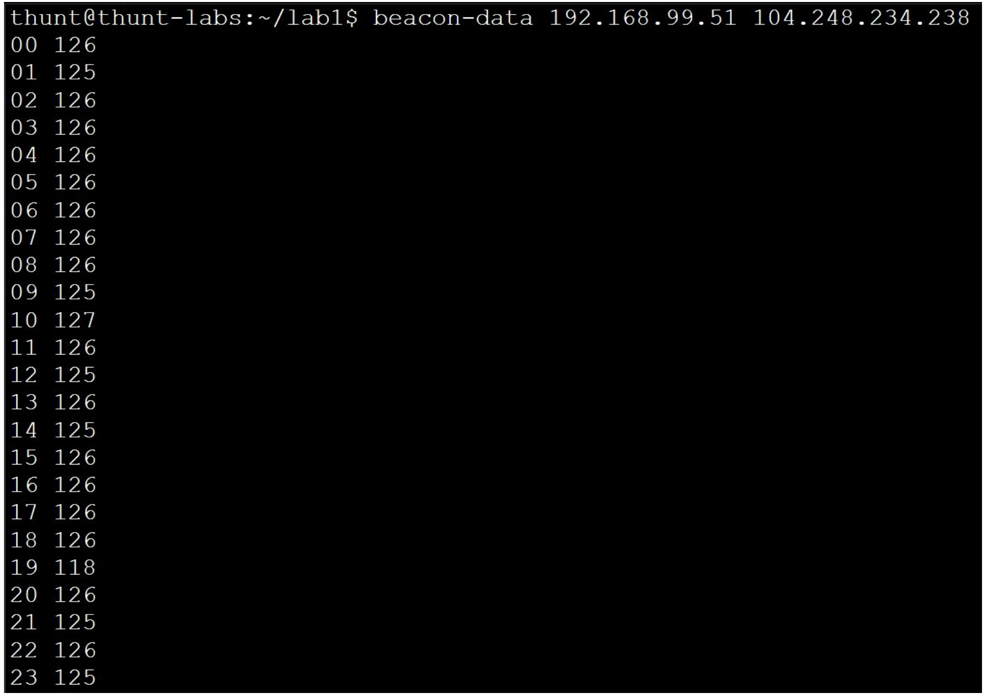
Detected via SNI



```
thunt@thunt-labs:~/lab1$ rita show-beacons lab1 | head
Score,Source IP,Destination IP,Connections,Avg. Bytes,Total Bytes,TS Score,DS Score,D
ur Score,Hist Score,Top Intvl
0.997,192.168.99.51,104.248.234.238,3011,1101,3315907,0.989,0.997,1,1,28
0.981,192.168.99.51,52.184.216.246,25,5244,131109,0.964,0.984,0.974,1,1502
0.942,192.168.99.51,52.184.217.56,30,5258,157747,0.824,0.991,0.952,1,900
0.841,192.168.99.51,52.179.219.14,38,5279,200634,0.74,0.845,0.978,0.8,28
0.746,192.168.99.51,208.67.220.220,60,245,14758,0.59,0.899,0.992,0.5,1
0.682,192.168.99.51,208.67.222.222,297,231,68702,0.417,0.948,0.999,0.364,1
0.663,192.168.99.51,52.167.249.196,47,5976,280913,0.354,0.841,0.955,0.5,1
0.553,192.168.99.51,23.197.120.174,40,7857,314309,0.5,0.709,0.002,1,0
thunt@thunt-labs:~/lab1$
```

Three additional IPs detected (four total)

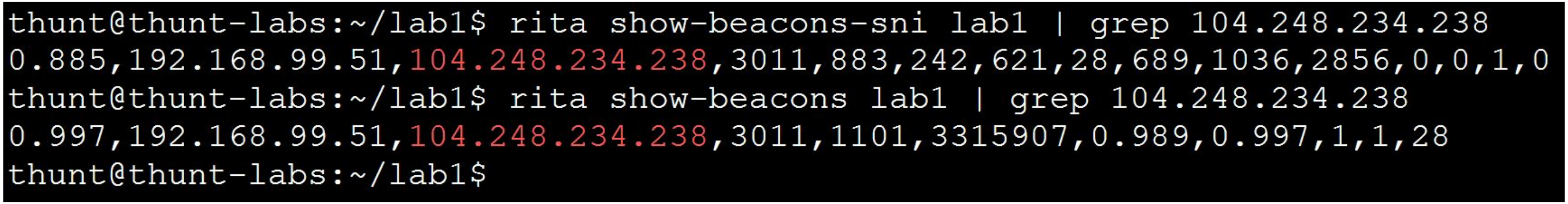
Is there a way to visualize beacons?



```
thunt@thunt-labs:~/lab1$ beacon-data 192.168.99.51 104.248.234.238
00 126
01 125
02 126
03 126
04 126
05 126
06 126
07 126
08 126
09 125
10 127
11 126
12 125
13 126
14 125
15 126
16 126
17 126
18 126
19 118
20 126
21 125
22 126
23 125
```

We cover these types of techniques in the Advanced Threat Hunting class

Wait, why is the SNI score lower?



```
thunt@thunt-labs:~/lab1$ rita show-beacons-sni lab1 | grep 104.248.234.238
0.885,192.168.99.51,104.248.234.238,3011,883,242,621,28,689,1036,2856,0,0,1,0
thunt@thunt-labs:~/lab1$ rita show-beacons lab1 | grep 104.248.234.238
0.997,192.168.99.51,104.248.234.238,3011,1101,3315907,0.989,0.997,1,1,28
thunt@thunt-labs:~/lab1$
```

The beacon-sni detection is a new feature.
We will deprioritize the score until it can prove itself. :-)

Next lab

- We found 4 beacons worth investigating
  - 104.248.234.238
  - 52.184.216.246
  - 52.184.217.56
  - 52.179.219.14
- Let's investigate using the "fq" command
- Potential business need with any of these?

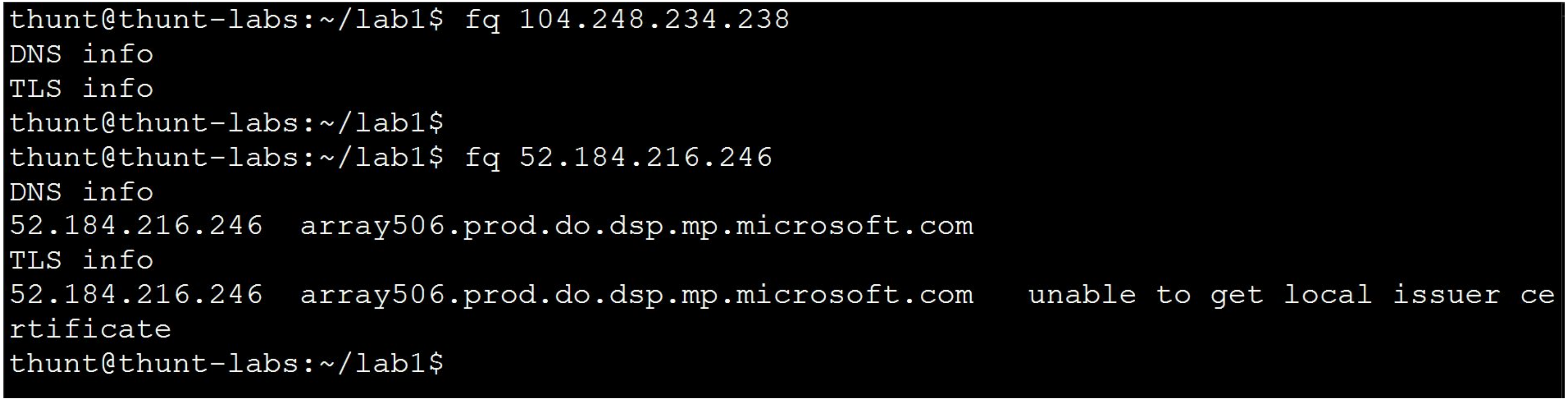
Hints

- Run the "fq" command followed by the IP address you wish to investigate
- Do this for each of the four one at a time
- Note that you must be in the "lab1" directory for this to work

Commands

```
fq 104.248.234.238
fq 52.184.216.246
fq 52.184.217.56
fq 52.179.219.14
```

Answers



```
thunt@thunt-labs:~/lab1$ fq 104.248.234.238
DNS info
TLS info
thunt@thunt-labs:~/lab1$
thunt@thunt-labs:~/lab1$ fq 52.184.216.246
DNS info
52.184.216.246  array506.prod.do.dsp.mp.microsoft.com
TLS info
52.184.216.246  array506.prod.do.dsp.mp.microsoft.com   unable to get local issuer ce
rtificate
thunt@thunt-labs:~/lab1$
```

The first returns no data
The remaining three point to a microsoft patching server

What's up with the digital cert?

- Microsoft signed their own cert
- Did not use a well known authority
- They can get away with this by installing the cert on Windows systems
  - These will verify the cert
  - All other systems are out of luck
  - Good thing everyone uses Windows for everything ;-p
- We could install cert on Linux to fix

Answers - and then there was one

- If we assume the MS certs are valid, those systems check out
- That just leaves us with one suspect IP
  - 104.248.234.238

Next lab- Using ngrep

- We found a suspicious IP pair
  - 192.168.99.51 to 104.248.234.238
- Let's analyze the payloads in these sessions
- Multiple tools can help here
  - But ngrep easily focuses on payload
- Use "host" parameter to focus in on the above IPs

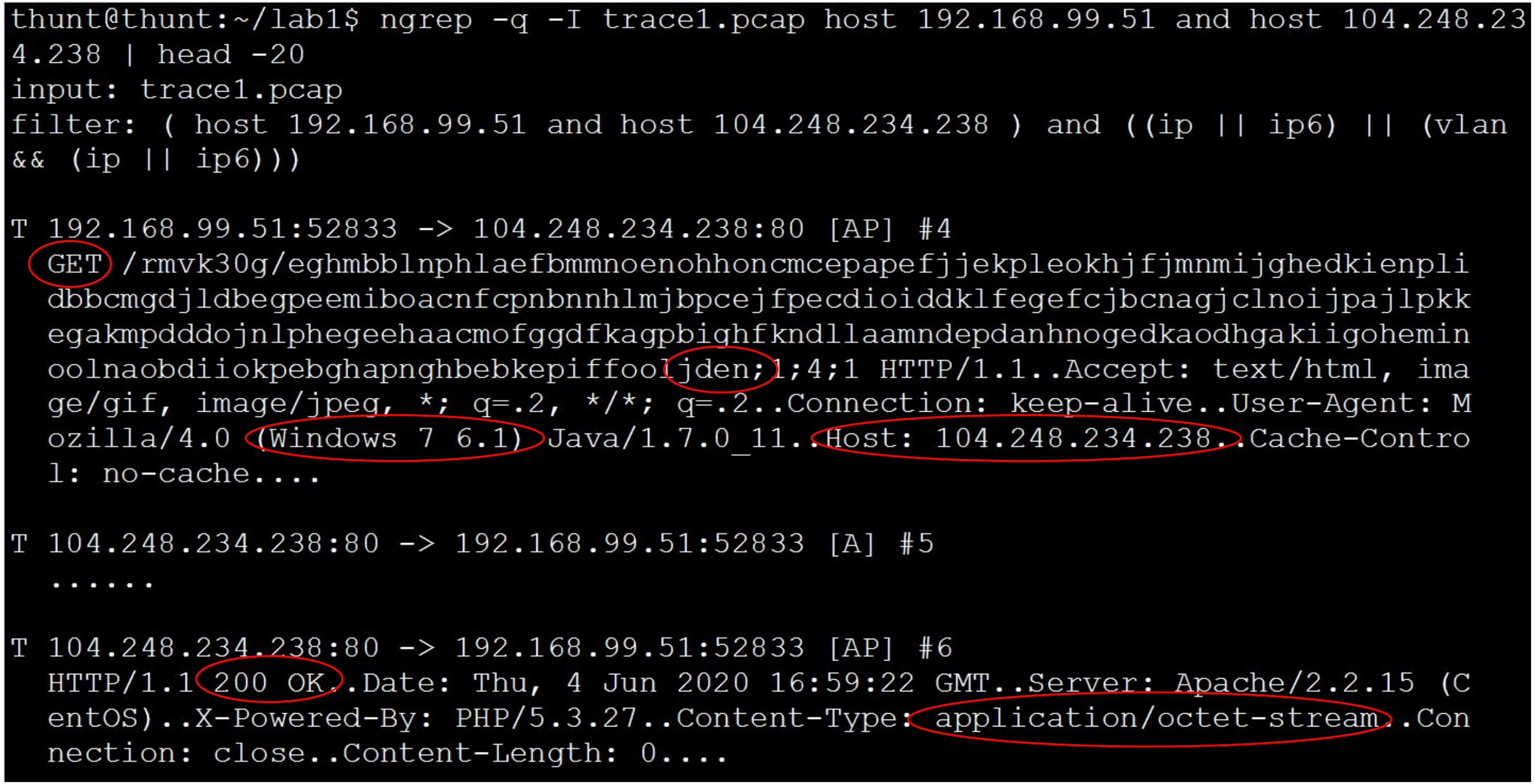
Payload analysis - hints

- Ngrep is normally used to search for patterns within the payload of all packets
- You can use BP filters to:
  - Focus on specific IP addresses
  - Focus on specific ports
  - "host" focuses on specific IP addresses
- Helpful switches
  - "-q" = Don't print "#" for packets that don't match
  - "-I" (capital letter i) = Read from pcap file

Useful commands to try

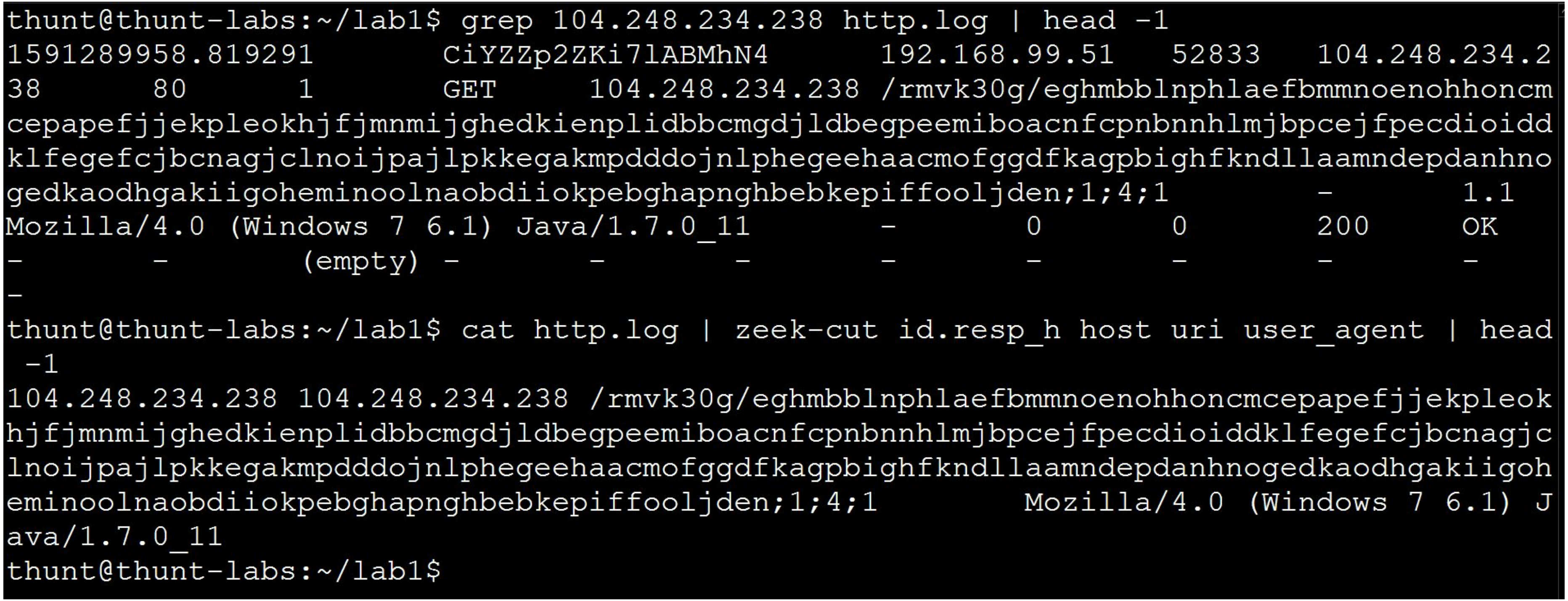
```
ngrep -q -I trace1.pcap host 192.168.99.51 and host
104.248.234.238 | less
```

Things that make you go "humm"



```
thunt@thunt:~/lab1$ ngrep -q -I trace1.pcap host 192.168.99.51 and host 104.248.23
4.238 | head -20
input: trace1.pcap
filter: ( host 192.168.99.51 and host 104.248.234.238 ) and ((ip || ip6) || (vlan
&& (ip || ip6)))

T 192.168.99.51:52833 -> 104.248.234.238:80 [AP] #4
  GET /rmvk30g/eghmbblnphlaefbmmnoenohhoncmcepapefjjekpleokhjfjmnmijghedkienpli
  dbbcmgdjldbegpeemiboacnfcpnbnnhlmjbpcejfpecdioiddklfegefcjbcnagjclnoijpajlpkk
  egakmpdddojnlphegeehaacmofggdfkagpbighfkndllaamndepdanhnogedkaodhgakiigohemin
  oolnaobdiiokpebghapnghbebkepiffooljden;1;4;1 HTTP/1.1..Accept: text/html, ima
  ge/gif, image/jpeg, *; q=.2, */*; q=.2..Connection: keep-alive..User-Agent: M
  ozilla/4.0 (Windows 7 6.1) Java/1.7.0_11..Host: 104.248.234.238..Cache-Contro
  l: no-cache....

T 104.248.234.238:80 -> 192.168.99.51:52833 [A] #5
  ......

T 104.248.234.238:80 -> 192.168.99.51:52833 [AP] #6
  HTTP/1.1 200 OK..Date: Thu, 4 Jun 2020 16:59:22 GMT..Server: Apache/2.2.15 (C
  entOS)..X-Powered-By: PHP/5.3.27..Content-Type: application/octet-stream..Con
  nection: close..Content-Length: 0....
```

Can Zeek give us the same info?



```
thunt@thunt-labs:~/lab1$ grep 104.248.234.238 http.log | head -1
1591289958.819291       CiYZZp2ZKi7lABMhN4      192.168.99.51   52833   104.248.234.2
38      80      1       GET     104.248.234.238 /rmvk30g/eghmbblnphlaefbmmnoenohhoncm
cepapefjjekpleokhjfjmnmijghedkienplidbbcmgdjldbegpeemiboacnfcpnbnnhlmjbpcejfpecdioidd
klfegefcjbcnagjclnoijpajlpkkegakmpdddojnlphegeehaacmofggdfkagpbighfkndllaamndepdanhno
gedkaodhgakiigoheminoolnaobdiiokpebghapnghbebkepiffooljden;1;4;1        -       1.1
Mozilla/4.0 (Windows 7 6.1) Java/1.7.0_11       -       0       0       200     OK
-       -       (empty) -       -       -       -       -       -       -       -
-
thunt@thunt-labs:~/lab1$ cat http.log | zeek-cut id.resp_h host uri user_agent | head
 -1
104.248.234.238 104.248.234.238 /rmvk30g/eghmbblnphlaefbmmnoenohhoncmcepapefjjekpleok
hjfjmnmijghedkienplidbbcmgdjldbegpeemiboacnfcpnbnnhlmjbpcejfpecdioiddklfegefcjbcnagjc
lnoijpajlpkkegakmpdddojnlphegeehaacmofggdfkagpbighfkndllaamndepdanhnogedkaodhgakiigoh
eminoolnaobdiiokpebghapnghbebkepiffooljden;1;4;1        Mozilla/4.0 (Windows 7 6.1) J
ava/1.7.0_11
thunt@thunt-labs:~/lab1$
```

User agent string analysis

- Is it normal for the source IP to ID as a Windows 7 system?
- Let's find out together
- Run this command:

```
cat http.log | zeek-cut id.orig_h id.resp_h user_agent | grep
192.168.99.51 | sort | uniq | cut -f 3 | sort | uniq -c | sort -rn
```

Breaking down the command

Extract IPs and user agent string

```
cat http.log | zeek-cut id.orig_h id.resp_h user_agent |
grep 192.168.99.51 |
sort | uniq |
cut -f 3 |
sort | uniq -c |
sort -rn
```

Filter out all data not associated with this internal IP

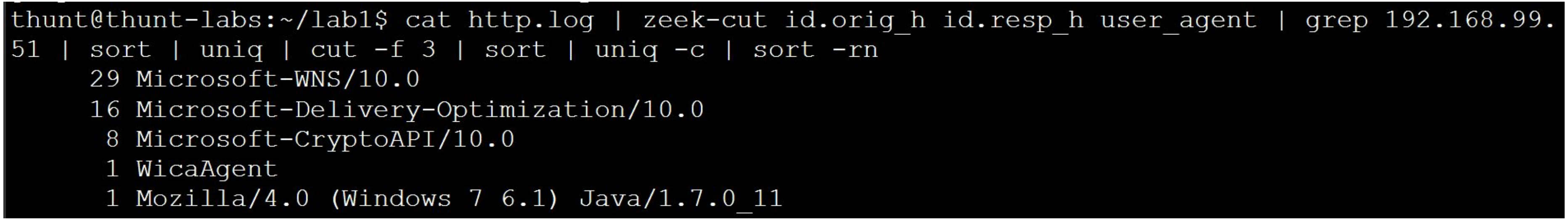
Keep only when copy when the source IP, dest IP and user agent all match

Remove dst IP from each line

Count the number of times each user agent string was used with each unique dst IP

Print data highest to lowest

What you should see



```
thunt@thunt-labs:~/lab1$ cat http.log | zeek-cut id.orig_h id.resp_h user_agent | grep 192.168.99.
51 | sort | uniq | cut -f 3 | sort | uniq -c | sort -rn
     29 Microsoft-WNS/10.0
     16 Microsoft-Delivery-Optimization/10.0
      8 Microsoft-CryptoAPI/10.0
      1 WicaAgent
      1 Mozilla/4.0 (Windows 7 6.1) Java/1.7.0_11
```

Source IP identified itself as Windows 10 during 54 unique IP/sessions
Beacon traffic is the only time it claims to be Windows 7 system

Most likely a Windows 10 system
Use of Windows 7 user agent string highly suspect

Lab - What data are we sending?

- Is the URI in the ngrep output sent consistently?
- We could eyeball it, but...
- Zeek stores this type of data
  - It's in the http.log file
- Let's use this log to identify all of the URI's requested from this external host

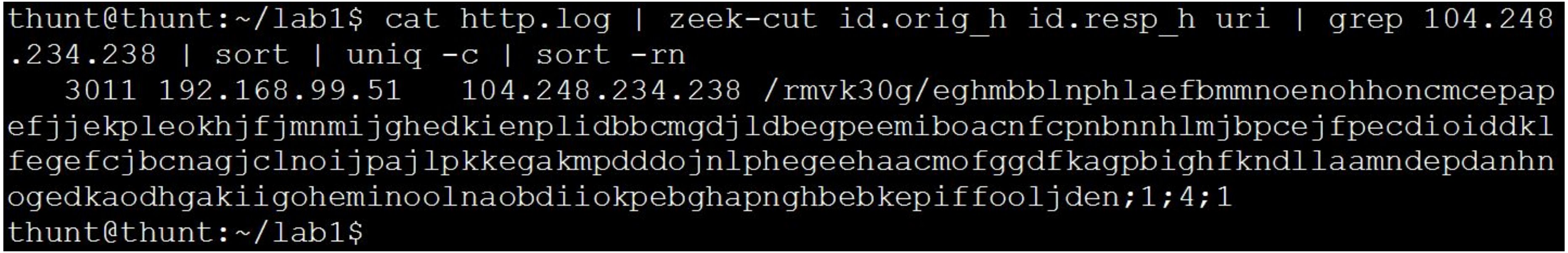
URI request - hints

- Zeek-cut is your friend
- We should extract
    - Source IP
    - Destination IP
    - The "uri" string
- Grep can focus on the traffic we care about
- Remember the threat hunter's mantra
    - sort | uniq | sort

Useful commands to try

```
cat http.log | zeek-cut id.orig_h id.resp_h uri |
grep 104.248.234.238 | sort | uniq -c | sort -rn
```

Answer - Single minded request



```
thunt@thunt:~/lab1$ cat http.log | zeek-cut id.orig_h id.resp_h uri | grep 104.248
.234.238 | sort | uniq -c | sort -rn
   3011 192.168.99.51   104.248.234.238 /rmvk30g/eghmbblnphlaefbmmnoenohhoncmcepap
efjjekpleokhjfjmnmijghedkienplidbbcmgdjldbegpeemiboacnfcpnbnnhlmjbpcejfpecdioiddkl
fegefcjbcnagjclnoijpajlpkkegakmpdddojnlphegeehaacmofggdfkagpbighfkndllaamndepdanhn
ogedkaodhgakiigoheminoolnaobdiiokpebghapnghbebkepiffooljden;1;4;1
thunt@thunt:~/lab1$
```

Answers

- 3,011 connections to external host
- Always sending the same odd "GET" request
- HTTP header data looks forged
- This really looks like a C2 channel
- Google search for "rmvk30g"
  - Looks like Fiesta EK malware

https://www.malware-traffic-analysis.net/2014/04/05/index.html

Lab - Look for C2 over DNS

- Check to see if C2 over DNS is in play
- Note we are still in the "lab1" directory
- Consider any domain with more than 1,000 FQDNs in it suspect
  - Not interested in total quantity of queries
  - Interest in quantities of unique FQDNs

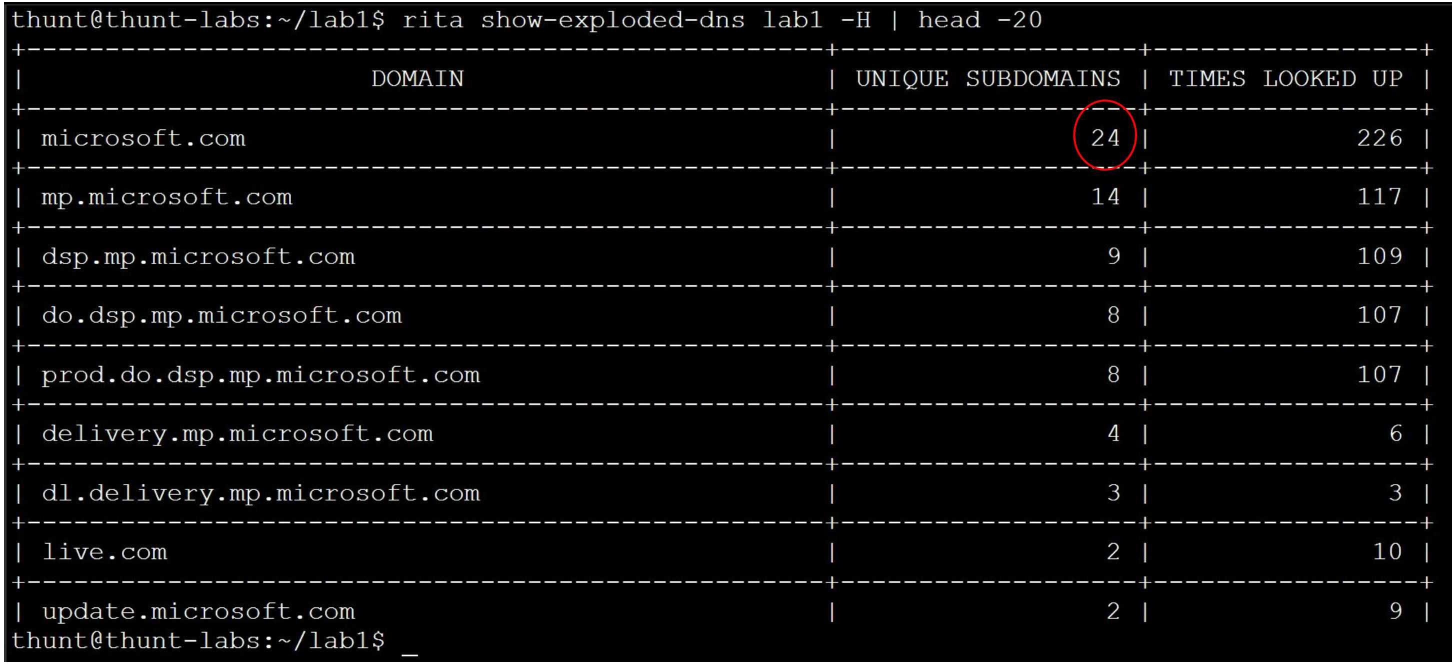
Hints

- Type "rita" to show a list of commands
- Look for any that seem "dns" related
- RITA labels "unique queries" as "Unique Subdomains"

Commands

```
rita show-exploded-dns lab1 -H | head -20
```

Answers

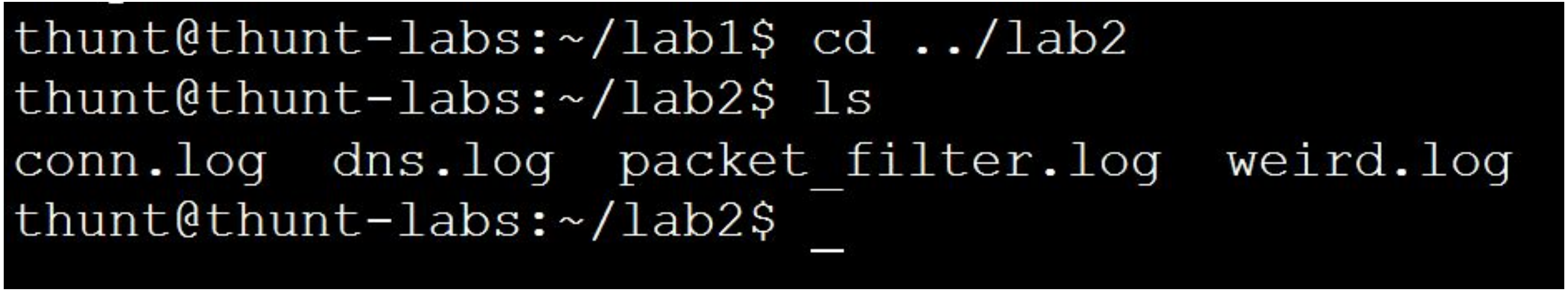


```
thunt@thunt-labs:~/lab1$ rita show-exploded-dns lab1 -H | head -20
+----------------------------------------------------+-------------------+------------------+
|                       DOMAIN                       | UNIQUE SUBDOMAINS | TIMES LOOKED UP  |
+----------------------------------------------------+-------------------+------------------+
| microsoft.com                                      |                24 |              226 |
+----------------------------------------------------+-------------------+------------------+
| mp.microsoft.com                                   |                14 |              117 |
+----------------------------------------------------+-------------------+------------------+
| dsp.mp.microsoft.com                               |                 9 |              109 |
+----------------------------------------------------+-------------------+------------------+
| do.dsp.mp.microsoft.com                            |                 8 |              107 |
+----------------------------------------------------+-------------------+------------------+
| prod.do.dsp.mp.microsoft.com                       |                 8 |              107 |
+----------------------------------------------------+-------------------+------------------+
| delivery.mp.microsoft.com                          |                 4 |                6 |
+----------------------------------------------------+-------------------+------------------+
| dl.delivery.mp.microsoft.com                       |                 3 |                3 |
+----------------------------------------------------+-------------------+------------------+
| live.com                                           |                 2 |               10 |
+----------------------------------------------------+-------------------+------------------+
| update.microsoft.com                               |                 2 |                9 |
thunt@thunt-labs:~/lab1$ _
```

Nothing of note
Unique queries are well under 1,000

Let's move to lab2

- Let's check the data in the lab2 directory
- Ww will also use "lab2" database in RITA



```
thunt@thunt-labs:~/lab1$ cd ../lab2
thunt@thunt-labs:~/lab2$ ls
conn.log  dns.log  packet_filter.log  weird.log
thunt@thunt-labs:~/lab2$ _
```

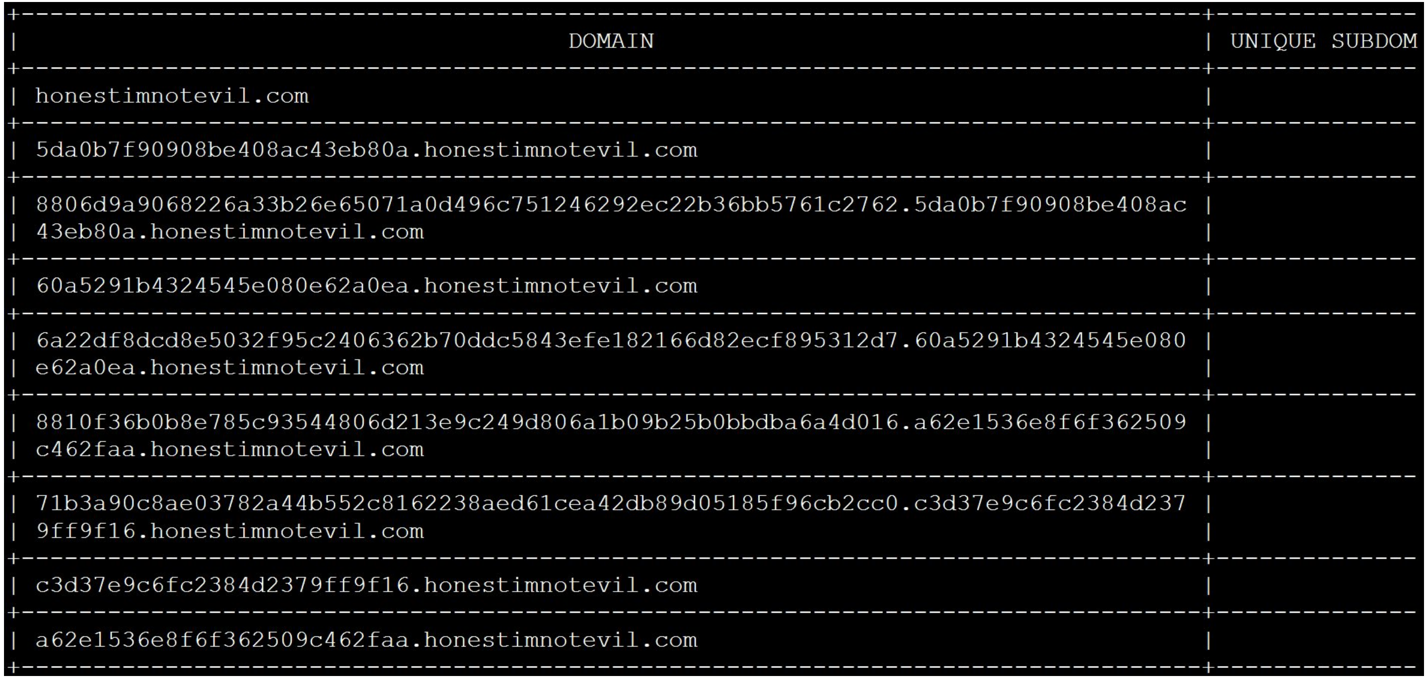
Next lab

- Working with data in the lab2 directory
- Let's repeat our check for C2 over DNS
- Rerun last RITA command changing "lab1" to be "lab2"
- Pipe through "less -S" instead of "head" if lines of data are really long

Commands

```
rita show-exploded-dns lab2 -H | less -S
```

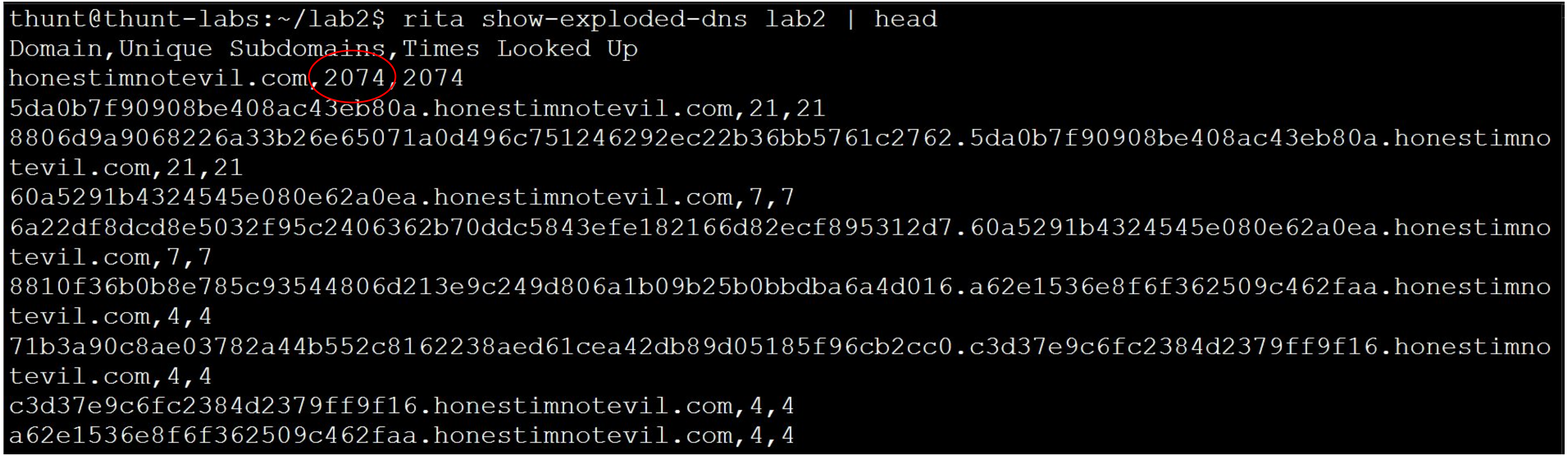
Answers - You should see



```
+----------------------------------------------------------------------------------+--------------
|                                      DOMAIN                                      | UNIQUE SUBDOM
+----------------------------------------------------------------------------------+--------------
| honestimnotevil.com                                                              |
+----------------------------------------------------------------------------------+--------------
| 5da0b7f90908be408ac43eb80a.honestimnotevil.com                                   |
+----------------------------------------------------------------------------------+--------------
| 8806d9a9068226a33b26e65071a0d496c751246292ec22b36bb5761c2762.5da0b7f90908be408ac |
| 43eb80a.honestimnotevil.com                                                      |
+----------------------------------------------------------------------------------+--------------
| 60a5291b4324545e080e62a0ea.honestimnotevil.com                                   |
+----------------------------------------------------------------------------------+--------------
| 6a22df8dcd8e5032f95c2406362b70ddc5843efe182166d82ecf895312d7.60a5291b4324545e080 |
| e62a0ea.honestimnotevil.com                                                      |
+----------------------------------------------------------------------------------+--------------
| 8810f36b0b8e785c93544806d213e9c249d806a1b09b25b0bbdba6a4d016.a62e1536e8f6f362509 |
| c462faa.honestimnotevil.com                                                      |
+----------------------------------------------------------------------------------+--------------
| 71b3a90c8ae03782a44b552c8162238aed61cea42db89d05185f96cb2cc0.c3d37e9c6fc2384d237 |
| 9ff9f16.honestimnotevil.com                                                      |
+----------------------------------------------------------------------------------+--------------
| c3d37e9c6fc2384d2379ff9f16.honestimnotevil.com                                   |
+----------------------------------------------------------------------------------+--------------
| a62e1536e8f6f362509c462faa.honestimnotevil.com                                   |
+----------------------------------------------------------------------------------+--------------
```

Navigate up/down/left/right using arrow keys

Answers - data output



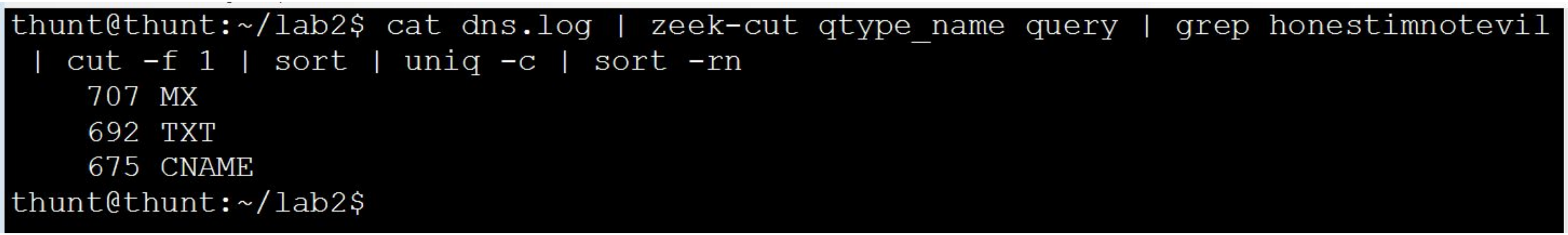
```
thunt@thunt-labs:~/lab2$ rita show-exploded-dns lab2 | head
Domain,Unique Subdomains,Times Looked Up
honestimnotevil.com,2074,2074
5da0b7f90908be408ac43eb80a.honestimnotevil.com,21,21
8806d9a9068226a33b26e65071a0d496c751246292ec22b36bb5761c2762.5da0b7f90908be408ac43eb80a.honestimno
tevil.com,21,21
60a5291b4324545e080e62a0ea.honestimnotevil.com,7,7
6a22df8dcd8e5032f95c2406362b70ddc5843efe182166d82ecf895312d7.60a5291b4324545e080e62a0ea.honestimno
tevil.com,7,7
8810f36b0b8e785c93544806d213e9c249d806a1b09b25b0bbdba6a4d016.a62e1536e8f6f362509c462faa.honestimno
tevil.com,4,4
71b3a90c8ae03782a44b552c8162238aed61cea42db89d05185f96cb2cc0.c3d37e9c6fc2384d2379ff9f16.honestimno
tevil.com,4,4
c3d37e9c6fc2384d2379ff9f16.honestimnotevil.com,4,4
a62e1536e8f6f362509c462faa.honestimnotevil.com,4,4
```

Greater than 1,000 unique queries!

Answers

- We looked up 2,074 FQDNs within honestimnoteveil.com
- This extremely high for a domain we do not recognize
- Could very well indicate C2 over DNS

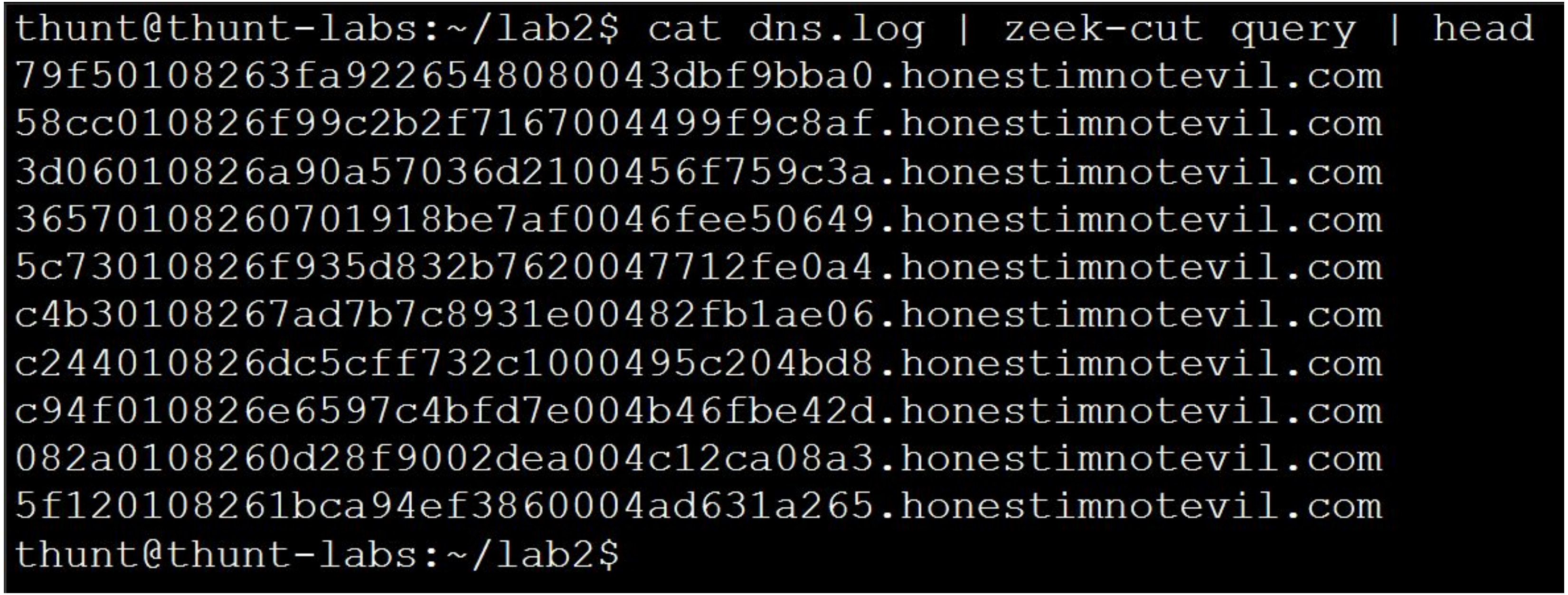
C2 over DNS only w/TXT queries?



```
thunt@thunt:~/lab2$ cat dns.log | zeek-cut qtype_name query | grep honestimnotevil
 | cut -f 1 | sort | uniq -c | sort -rn
    707 MX
    692 TXT
    675 CNAME
thunt@thunt:~/lab2$
```

707 + 692 + 675 = 2,074 (same as number of FQDNs found in first lab)

What's with the odd FQDNs?



```
thunt@thunt-labs:~/lab2$ cat dns.log | zeek-cut query | head
79f50108263fa92265480800043dbf9bba0.honestimnotevil.com
58cc010826f99c2b2f716700449 9f9c8af.honestimnotevil.com
3d06010826a90a57036d2100456f759c3a.honestimnotevil.com
3657010826070191 8be7af0046fee50649.honestimnotevil.com
5c73010826f935d832b76200477 12fe0a4.honestimnotevil.com
c4b30108267ad7b7c8931e00482fb1ae06.honestimnotevil.com
c244010826dc5cff732c1000495c204bd8.honestimnotevil.com
c94f010826e6597c4bfd7e004b46fbe42d.honestimnotevil.com
082a0108260d28f9002dea004c12ca08a3.honestimnotevil.com
5f120108261bca94ef3860004ad631a265.honestimnotevil.com
thunt@thunt-labs:~/lab2$
```

We cover decoding this type of C2 channel in the advanced class

Next lab!

- Working with the lab2 data, check for:
  - Beacons
  - Long connections
- Anything of note?

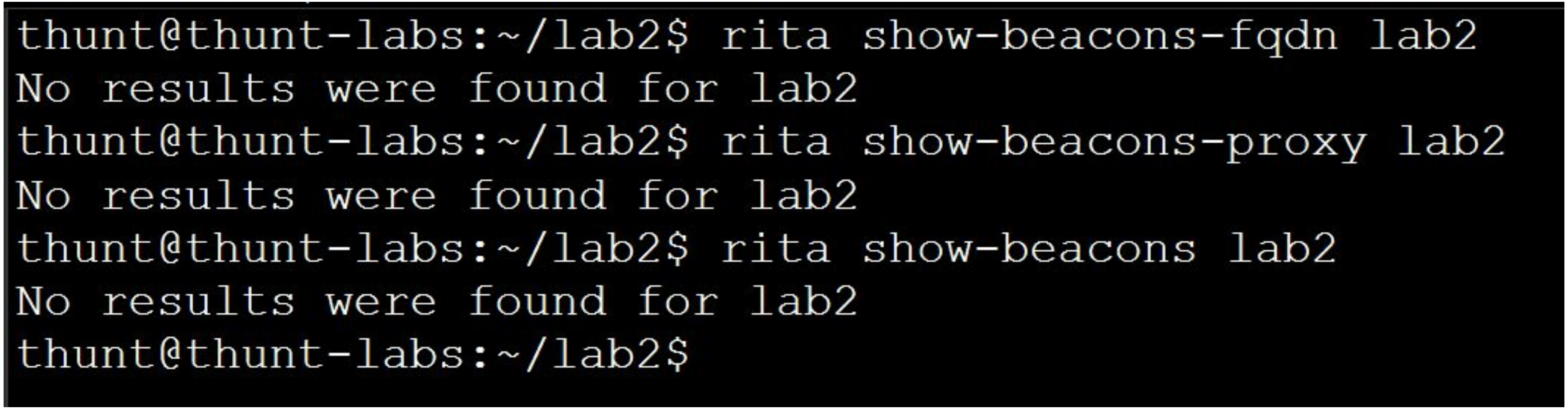
Hints

- Each of these was covered when investigating the lab1 data
- Refer back and repeat the commands as needed to investigate each

Commands

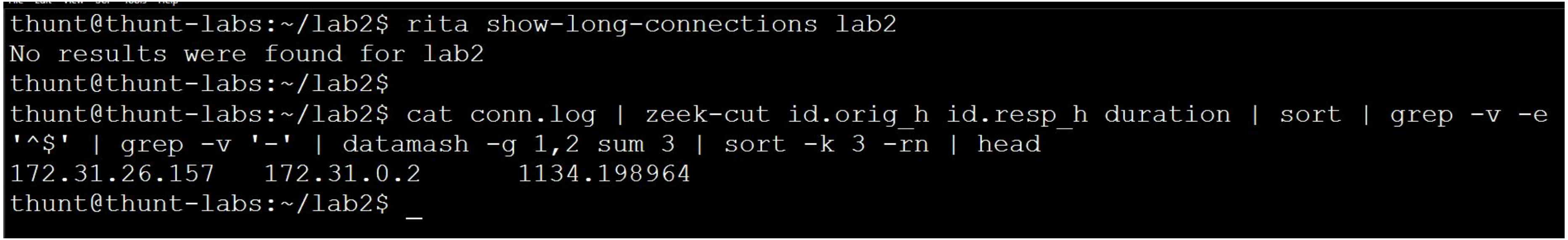
```
rita show-long-connections lab2

rita show-beacons-sni lab2
rita show-beacons-fqdn lab2
rita show-beacons-proxy lab2
rita show-beacons lab2
```

Answers - No beacons found



```
thunt@thunt-labs:~/lab2$ rita show-beacons-fqdn lab2
No results were found for lab2
thunt@thunt-labs:~/lab2$ rita show-beacons-proxy lab2
No results were found for lab2
thunt@thunt-labs:~/lab2$ rita show-beacons lab2
No results were found for lab2
thunt@thunt-labs:~/lab2$
```

Answers - No long conns of note



```
thunt@thunt-labs:~/lab2$ rita show-long-connections lab2
No results were found for lab2
thunt@thunt-labs:~/lab2$
thunt@thunt-labs:~/lab2$ cat conn.log | zeek-cut id.orig_h id.resp_h duration | sort | grep -v -e
'^$' | grep -v '-' | datamash -g 1,2 sum 3 | sort -k 3 -rn | head
172.31.26.157   172.31.0.2      1134.198964
thunt@thunt-labs:~/lab2$ _
```

Answers - Final

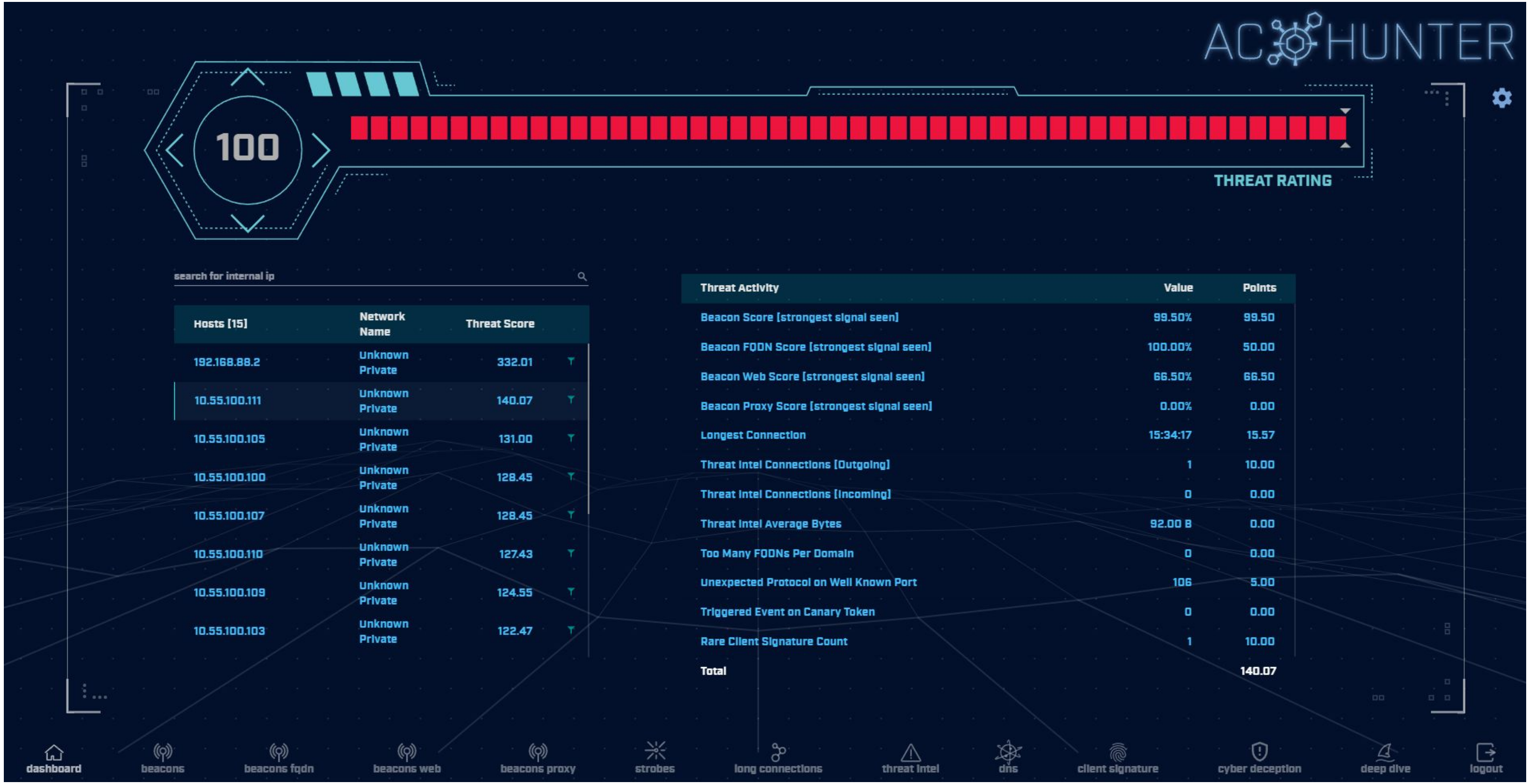
- Lab1 data has a C2 beacon
- Lab2 data has C2 over DNS
- All other data looks clear

What have we learned?

- RITA provides a consistent interface for identifying C2
- Screens pull in additional helpful info
- Even very slow beacons can be detected
- Investigation can be scripted
- Open source, so anyone can use it for free

Quick demo

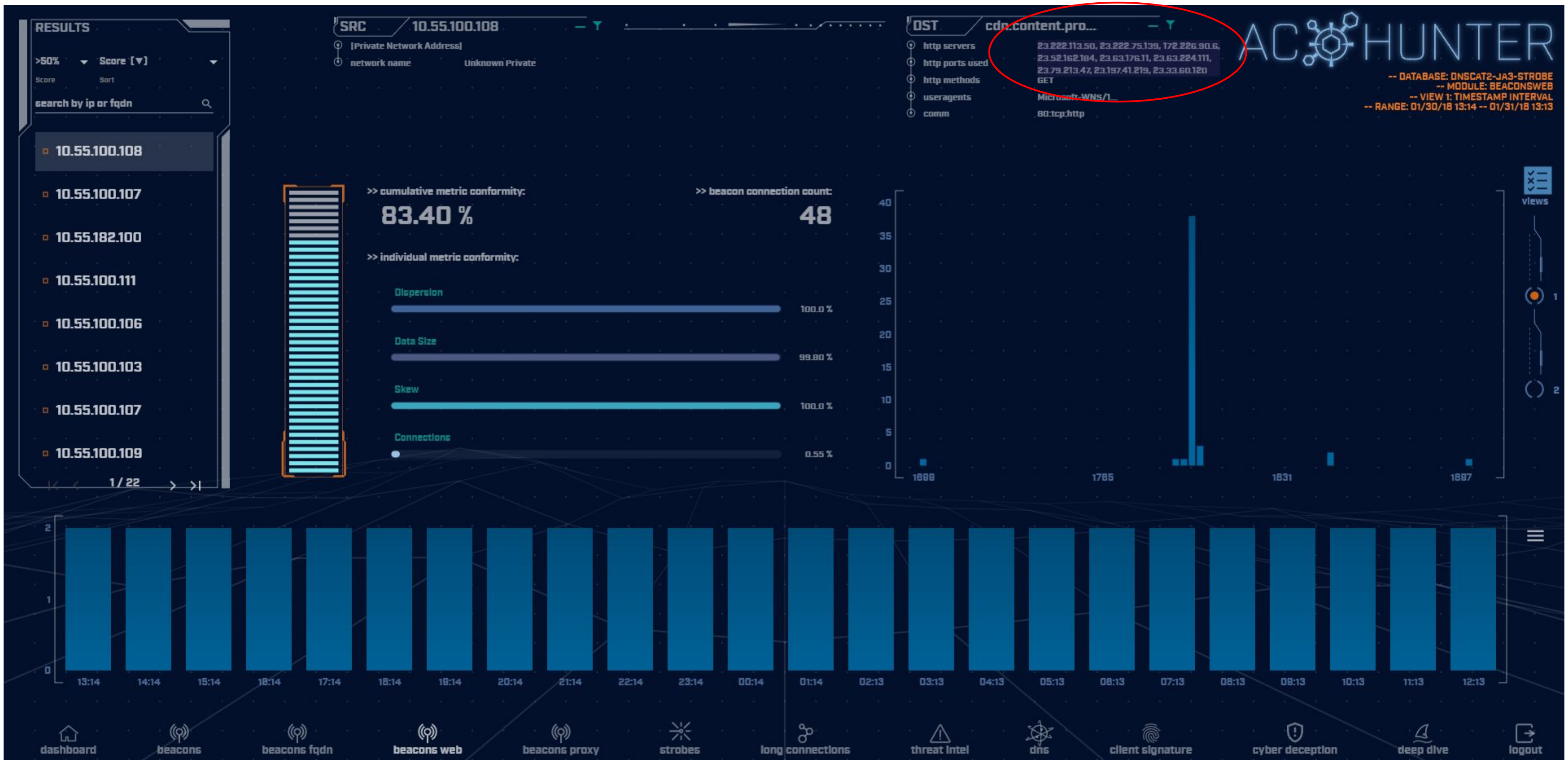
- Similar data, seen through AI-Hunter
- Inexpensive commercial solution
- Automates much of the hunting process



Hosts [15]	Network Name	Threat Score
192.168.88.2	Unknown Private	332.01
10.55.100.111	Unknown Private	140.07
10.55.100.105	Unknown Private	131.00
10.55.100.100	Unknown Private	128.45
10.55.100.107	Unknown Private	128.45
10.55.100.110	Unknown Private	127.43
10.55.100.109	Unknown Private	124.55
10.55.100.103	Unknown Private	122.47

Threat Activity	Value	Points
Beacon Score [strongest signal seen]	99.50%	99.50
Beacon FQDN Score [strongest signal seen]	100.00%	50.00
Beacon Web Score [strongest signal seen]	66.50%	66.50
Beacon Proxy Score [strongest signal seen]	0.00%	0.00
Longest Connection	15:34:17	15.57
Threat Intel Connections [Outgoing]	1	10.00
Threat Intel Connections [Incoming]	0	0.00
Threat Intel Average Bytes	92.00 B	0.00
Too Many FQDNs Per Domain	0	0.00
Unexpected Protocol on Well Known Port	106	5.00
Triggered Event on Canary Token	0	0.00
Rare Client Signature Count	1	10.00
Total		140.07

24 active hunts of 24-hours of data every single day
Top results scored, alerts sent to SIEM



RESULTS

>50% Score

Score [▼] Sort

search by ip or fqdn

10.55.100.108
10.55.100.107
10.55.182.100
10.55.100.111
10.55.100.106
10.55.100.103
10.55.100.107
10.55.100.109

1 / 22

SRC 10.55.100.108

[Private Network Address]

network name Unknown Private

DST cdn.content.pro...

http servers 23.222.113.50, 23.222.75.139, 172.226.90.6, 23.52.162.184, 23.63.176.11, 23.63.224.111, 23.79.213.47, 23.197.41.219, 23.33.60.120

http ports used

http methods GET

useragents Microsoft-WNS/1...

comm 80:tcp:http

AC HUNTER

-- DATABASE: DNSCAT2-JA3-STROBE
-- MODULE: BEACONSWEB
-- VIEW 1: TIMESTAMP INTERVAL
-- RANGE: 01/30/18 13:14 -- 01/31/18 13:13

>> cumulative metric conformity:
83.40 %

>> beacon connection count:
48

>> individual metric conformity:

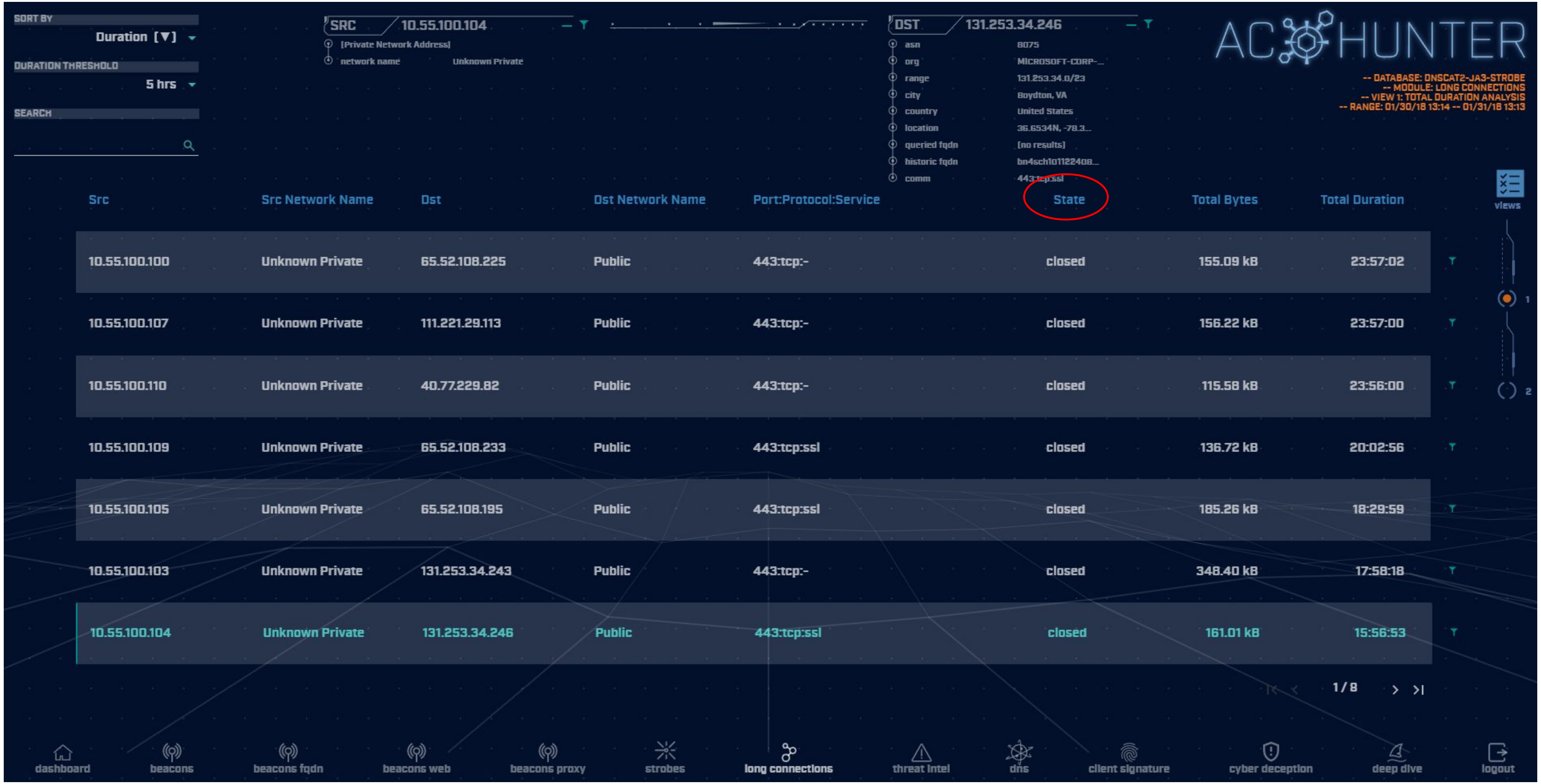
Dispersion 100.0 %

Data Size 99.80 %

Skew 100.0 %

Connections 0.55 %

Track beacons across multiple CDNs
with both timing and session size analysis



SORT BY

Duration [▼]

DURATION THRESHOLD

5 hrs

SEARCH

SRC 10.55.100.104

[Private Network Address]

network name Unknown Private

DST 131.253.34.246

asn	8075
org	MICROSOFT-CORP-...
range	131.253.34.0/23
city	Boydton, VA
country	United States
location	36.6534N, -78.3...
queried fqdn	[no results]
historic fqdn	bn4sch101122408...
comm	443:tcp:ssl

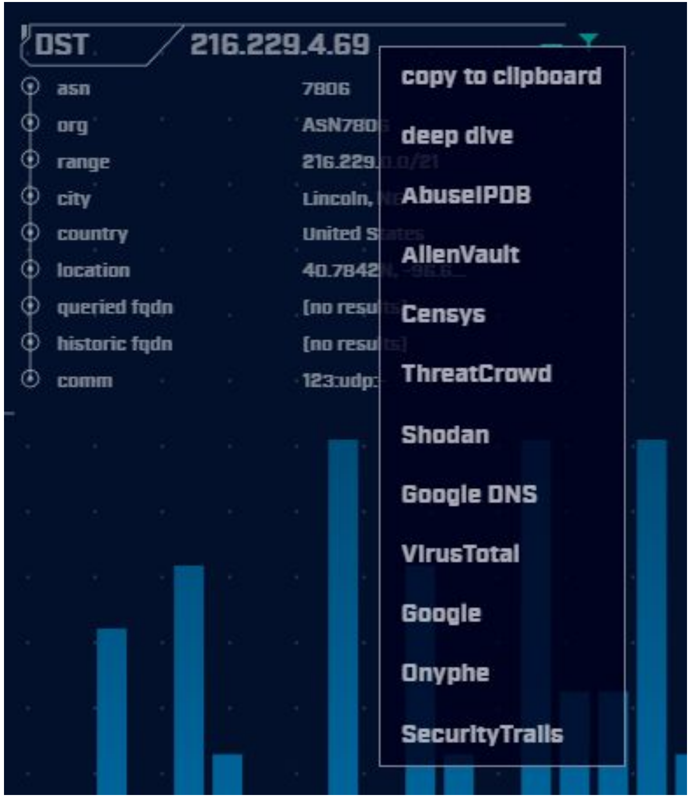
-- DATABASE: DNSCAT2-JA3-STROBE
-- MODULE: LONG CONNECTIONS
-- VIEW 1: TOTAL DURATION ANALYSIS
-- RANGE: 01/30/18 13:14 -- 01/31/18 13:13

Src	Src Network Name	Dst	Dst Network Name	Port:Protocol:Service	State	Total Bytes	Total Duration
10.55.100.100	Unknown Private	65.52.108.225	Public	443:tcp:-	closed	155.09 kB	23:57:02
10.55.100.107	Unknown Private	111.221.29.113	Public	443:tcp:-	closed	156.22 kB	23:57:00
10.55.100.110	Unknown Private	40.77.229.82	Public	443:tcp:-	closed	115.58 kB	23:56:00
10.55.100.109	Unknown Private	65.52.108.233	Public	443:tcp:ssl	closed	136.72 kB	20:02:56
10.55.100.105	Unknown Private	65.52.108.195	Public	443:tcp:ssl	closed	185.26 kB	18:29:59
10.55.100.103	Unknown Private	131.253.34.243	Public	443:tcp:-	closed	348.40 kB	17:58:18
10.55.100.104	Unknown Private	131.253.34.246	Public	443:tcp:ssl	closed	161.01 kB	15:56:53

1 / 8

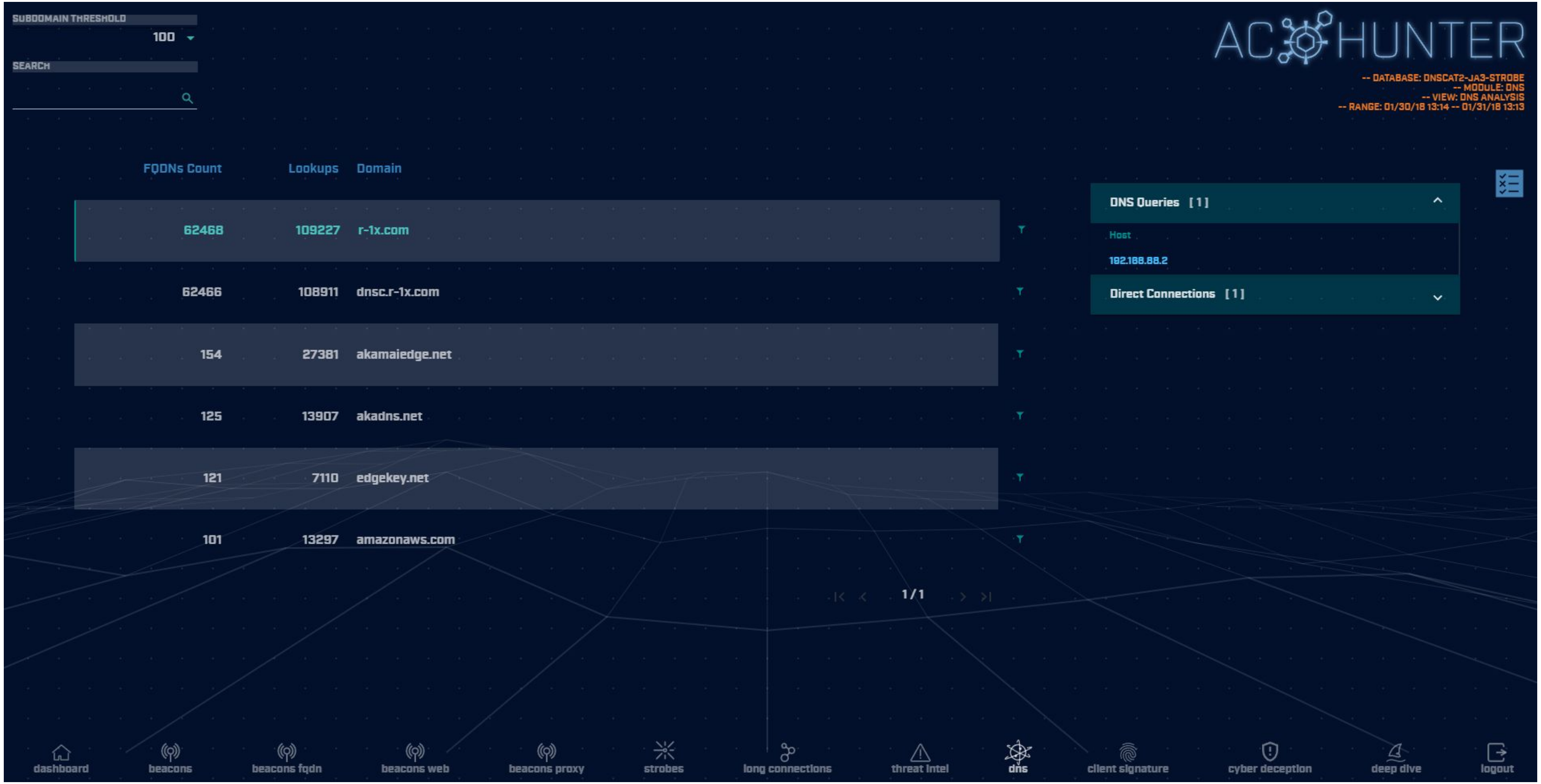
Long connections with lots of intel
View both individual and cumulative

Resources to dig deeper



DST 216.229.4.69

```
asn             7806
org             ASN780
range           216.229.0.0/21
city            Lincoln, Ne
country         United States
location        40.7842N, -96.6...
queried fqdn    [no results]
historic fqdn   [no results]
comm            123:udp:
```



SUBDOMAIN THRESHOLD
100

SEARCH

-- DATABASE: DNSCAT2-JA3-STROBE
-- MODULE: DNS
-- VIEW: DNS ANALYSIS
-- RANGE: 01/30/18 13:14 -- 01/31/18 13:13

FQDNs Count	Lookups	Domain
62468	109227	r-1x.com
62466	108911	dnsc.r-1x.com
154	27381	akamaiedge.net
125	13907	akadns.net
121	7110	edgekey.net
101	13297	amazonaws.com

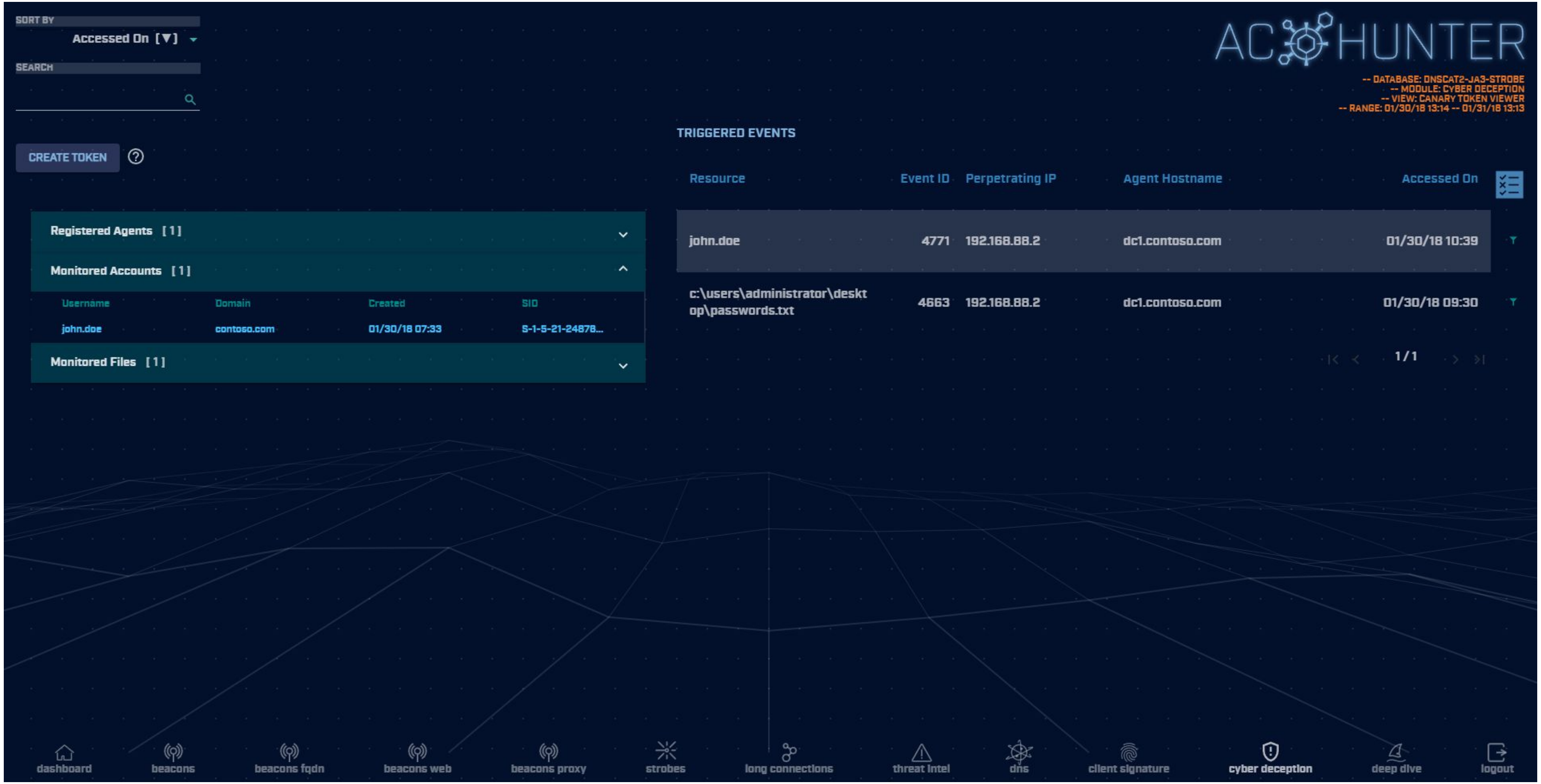
1 / 1

DNS Queries [1]

Host
192.168.88.2

Direct Connections [1]

C2 over DNS analysis



SORT BY: Accessed On [▼]

SEARCH

-- DATABASE: DNSCAT2-JA3-STROBE
-- MODULE: CYBER DECEPTION
-- VIEW: CANARY TOKEN VIEWER
-- RANGE: 01/30/18 13:14 -- 01/31/18 13:13

Registered Agents [1]

Monitored Accounts [1]

Username	Domain	Created	SID
john.doe	contoso.com	01/30/18 07:33	S-1-5-21-24878...

Monitored Files [1]

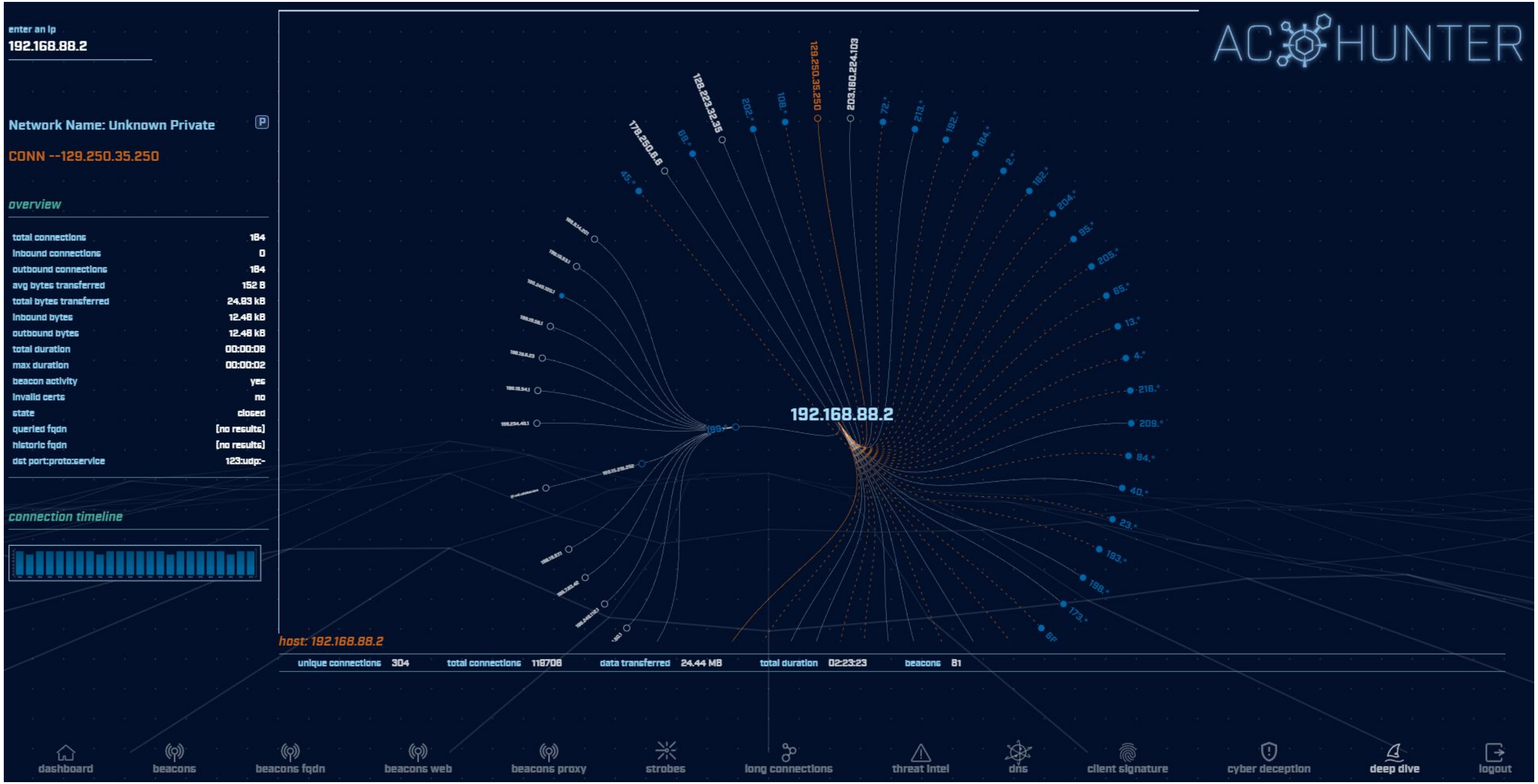
TRIGGERED EVENTS

Resource	Event ID	Perpetrating IP	Agent Hostname	Accessed On
john.doe	4771	192.168.88.2	dc1.contoso.com	01/30/18 10:39
c:\users\administrator\desktop\passwords.txt	4663	192.168.88.2	dc1.contoso.com	01/30/18 09:30

1 / 1

Cyber Deception/Honey Tokens

Lateral movement detection with very low false positive rate


enter an ip
192.168.88.2

Network Name: Unknown Private

CONN --129.250.35.250

overview

total connections	184
inbound connections	0
outbound connections	184
avg bytes transferred	152 B
total bytes transferred	24.83 kB
inbound bytes	12.48 kB
outbound bytes	12.48 kB
total duration	00:00:09
max duration	00:00:02
beacon activity	yes
invalid certs	no
state	closed
queried fqdn	[no results]
historic fqdn	[no results]
dst port:proto:service	123:udp:-

connection timeline

host: 192.168.88.2

unique connections 304 total connections 118708 data transferred 24.44 MB total duration 02:23:23 beacons 81

Deep dive analysis

Take home lab

- This is a bonus lab to do on your own
  - Wait at least a week
  - Will help identify what training "stuck"
- Move to the "lab3" directory
- Check for C2/DNS, long conns & beacons
- Investigate any suspect external IP's
- Do you see anything of concern?
- Hints and answers after "Wrap Up" slide

Keep honing your skills

- Check out our blog
- "Malware of the day"
  - Skip to the bottom
  - Grab the pcap
  - Find the C2 channel
  - Go back and read the blog to check your work
- Subscribe to get notifications

https://www.activecountermeasures.com/subscribe/

More cool stuff

- Wild West Hackin' Fest
  - Oct 12-14
  - $150 virtual ticket

https://wildwesthackinfest.com/deadwood/

- Advanced Network Threat Hunting
  - Oct 11 & 12
  - $725 (includes WWHF ticket)
  - Last run for the year!

https://www.antisyphontraining.com/advanced-network-threat-hunting-w-chris-brenton/

Wrap Up

- Thanks for attending!
- Very special thank you to the folks behind the scenes
  - They give up their free time to help us all out
- Content feedback?
  - Please email: chris@activecountermeasures.com

Take home lab

- Move to the "lab3" directory
- Check for:
  - Beacons (all types)
  - Long connections
  - C2 over DNS
- Investigate any suspect external IP's
- Do you see anything of concern?

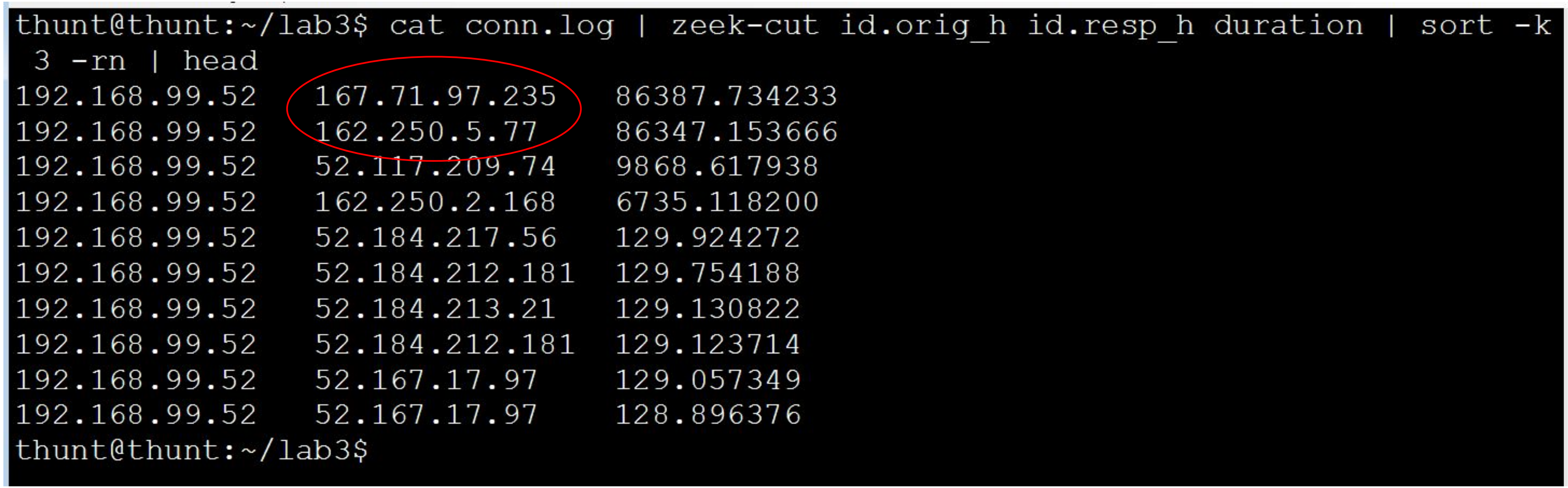
Hints for the take home lab

- Repeat what we did with lab1 & lab2
- Us "up arrow" key to scroll through command buffer to see commands you ran previously
- You've got this! :-)

Useful commands to try

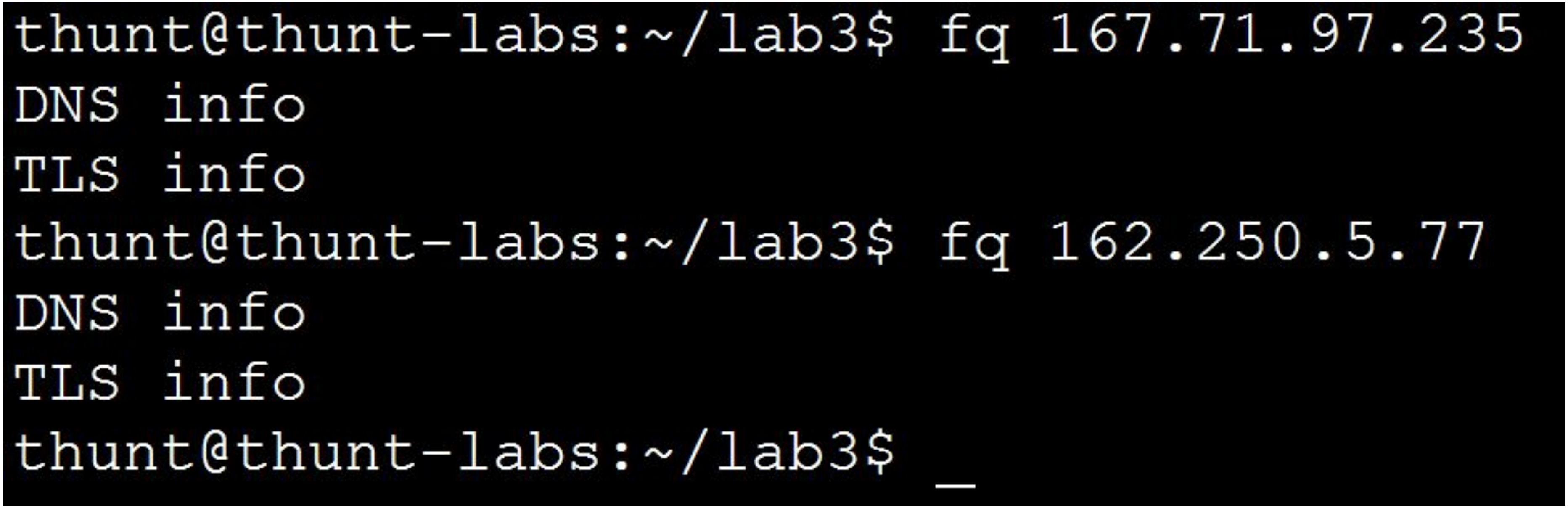
```
rita show-long-connections lab3

rita show-beacons-sni lab3
rita show-beacons-fqdn lab3
rita show-beacons-proxy lab3
rita show-beacons lab3

Rita show-exploded-dns lab3

fq <IP address>
```

Answers - Long connections



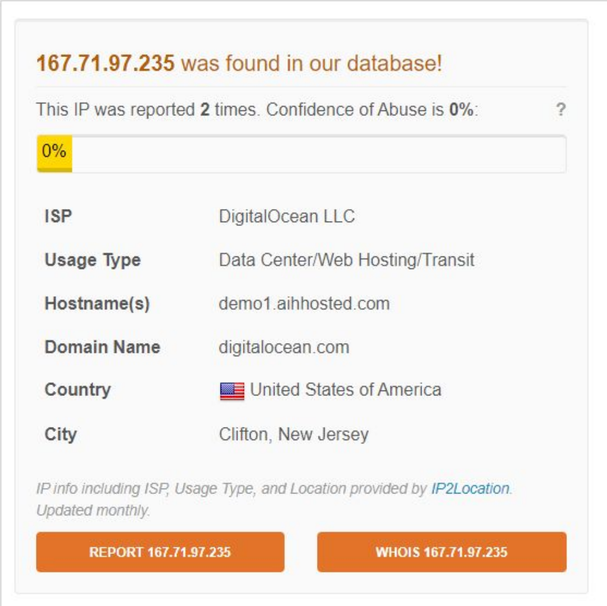
```
thunt@thunt:~/lab3$ cat conn.log | zeek-cut id.orig_h id.resp_h duration | sort -k
 3 -rn | head
192.168.99.52   167.71.97.235   86387.734233
192.168.99.52   162.250.5.77    86347.153666
192.168.99.52   52.117.209.74   9868.617938
192.168.99.52   162.250.2.168   6735.118200
192.168.99.52   52.184.217.56   129.924272
192.168.99.52   52.184.212.181  129.754188
192.168.99.52   52.184.213.21   129.130822
192.168.99.52   52.184.212.181  129.123714
192.168.99.52   52.167.17.97    129.057349
192.168.99.52   52.167.17.97    128.896376
thunt@thunt:~/lab3$
```

fq research



```
thunt@thunt-labs:~/lab3$ fq 167.71.97.235
DNS info
TLS info
thunt@thunt-labs:~/lab3$ fq 162.250.5.77
DNS info
TLS info
thunt@thunt-labs:~/lab3$ _
```

We've seen the 1st before



167.71.97.235 was found in our database!

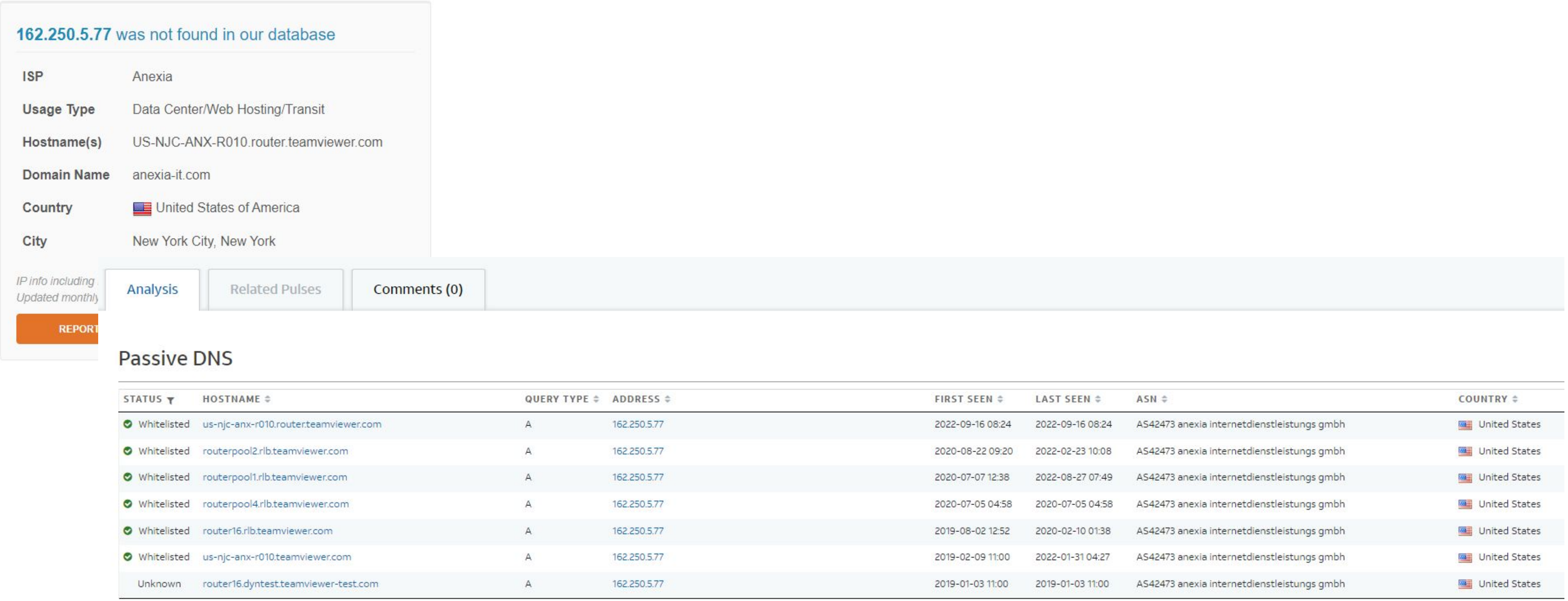
This IP was reported **2** times. Confidence of Abuse is **0%**: ?

ISP	DigitalOcean LLC
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	demo1.aihhosted.com
Domain Name	digitalocean.com
Country	United States of America
City	Clifton, New Jersey

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

In lab1 we said to assume this was business related

Is TeamViewer OK from this system?



162.250.5.77 was not found in our database

ISP	Anexia
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	US-NJC-ANX-R010.router.teamviewer.com
Domain Name	anexia-it.com
Country	United States of America
City	New York City, New York

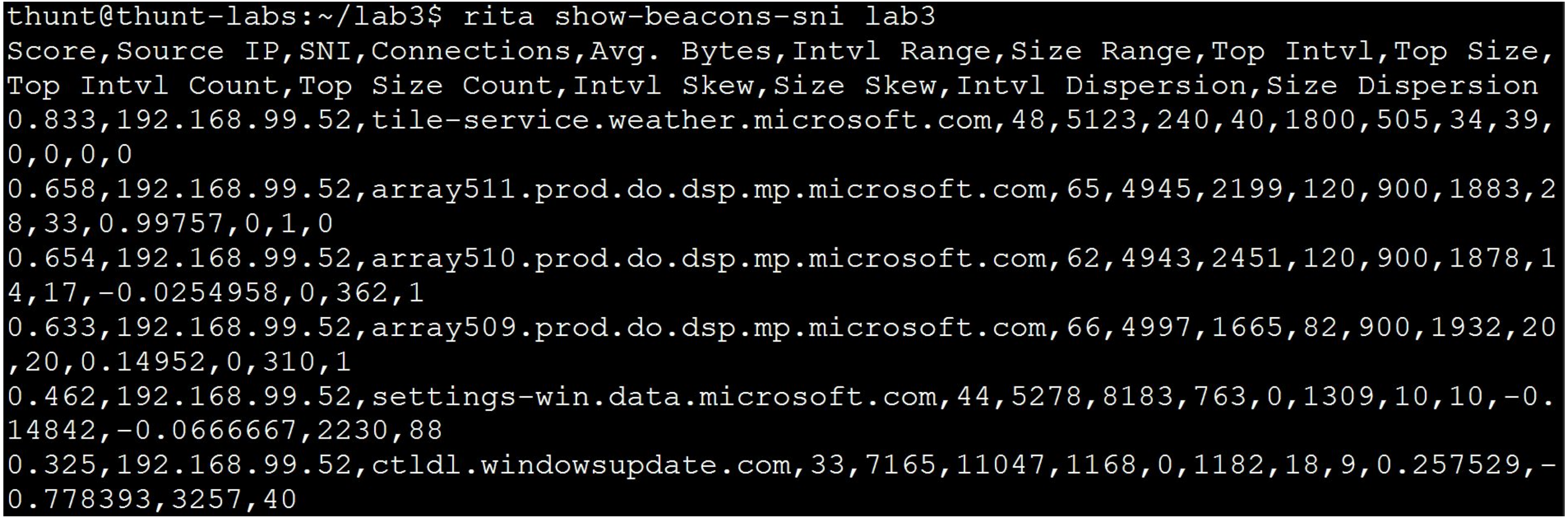
IP info including
Updated monthly

Passive DNS

STATUS	HOSTNAME	QUERY TYPE	ADDRESS	FIRST SEEN	LAST SEEN	ASN	COUNTRY
✓ Whitelisted	us-njc-anx-r010.router.teamviewer.com	A	162.250.5.77	2022-09-16 08:24	2022-09-16 08:24	AS42473 anexia internetdienstleistungs gmbh	United States
✓ Whitelisted	routerpool2.rlb.teamviewer.com	A	162.250.5.77	2020-08-22 09:20	2022-02-23 10:08	AS42473 anexia internetdienstleistungs gmbh	United States
✓ Whitelisted	routerpool1.rlb.teamviewer.com	A	162.250.5.77	2020-07-07 12:38	2022-08-27 07:49	AS42473 anexia internetdienstleistungs gmbh	United States
✓ Whitelisted	routerpool4.rlb.teamviewer.com	A	162.250.5.77	2020-07-05 04:58	2020-07-05 04:58	AS42473 anexia internetdienstleistungs gmbh	United States
✓ Whitelisted	router16.rlb.teamviewer.com	A	162.250.5.77	2019-08-02 12:52	2020-02-10 01:38	AS42473 anexia internetdienstleistungs gmbh	United States
✓ Whitelisted	us-njc-anx-r010.teamviewer.com	A	162.250.5.77	2019-02-09 11:00	2022-01-31 04:27	AS42473 anexia internetdienstleistungs gmbh	United States
Unknown	router16.dyntest.teamviewer-test.com	A	162.250.5.77	2019-01-03 11:00	2019-01-03 11:00	AS42473 anexia internetdienstleistungs gmbh	United States

We would need to verify whether this connectivity is approved

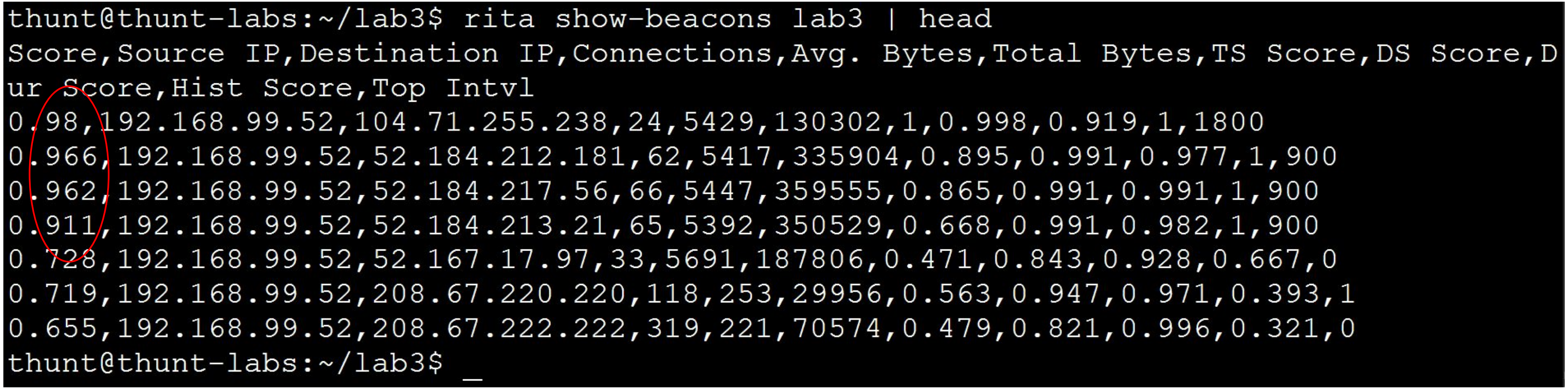
beacon-sni



```
thunt@thunt-labs:~/lab3$ rita show-beacons-sni lab3
Score,Source IP,SNI,Connections,Avg. Bytes,Intvl Range,Size Range,Top Intvl,Top Size,
Top Intvl Count,Top Size Count,Intvl Skew,Size Skew,Intvl Dispersion,Size Dispersion
0.833,192.168.99.52,tile-service.weather.microsoft.com,48,5123,240,40,1800,505,34,39,
0,0,0,0
0.658,192.168.99.52,array511.prod.do.dsp.mp.microsoft.com,65,4945,2199,120,900,1883,2
8,33,0.99757,0,1,0
0.654,192.168.99.52,array510.prod.do.dsp.mp.microsoft.com,62,4943,2451,120,900,1878,1
4,17,-0.0254958,0,362,1
0.633,192.168.99.52,array509.prod.do.dsp.mp.microsoft.com,66,4997,1665,82,900,1932,20
,20,0.14952,0,310,1
0.462,192.168.99.52,settings-win.data.microsoft.com,44,5278,8183,763,0,1309,10,10,-0.
14842,-0.0666667,2230,88
0.325,192.168.99.52,ctldl.windowsupdate.com,33,7165,11047,1168,0,1182,18,9,0.257529,-
0.778393,3257,40
```

1 connection of note and it's Windows tile service

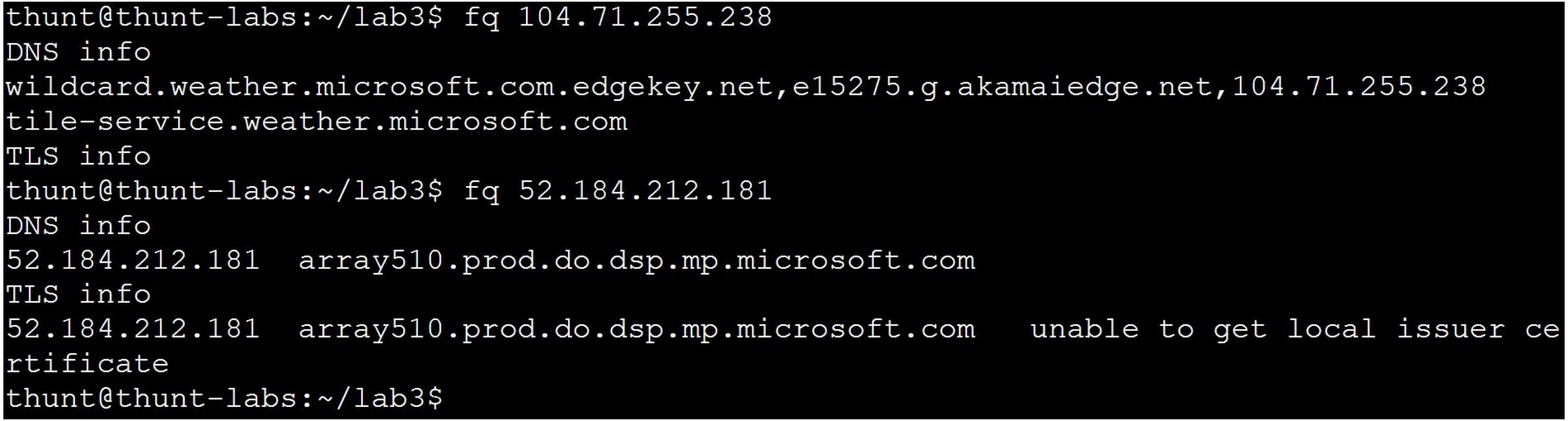
A few IP beacons of note



```
thunt@thunt-labs:~/lab3$ rita show-beacons lab3 | head
Score,Source IP,Destination IP,Connections,Avg. Bytes,Total Bytes,TS Score,DS Score,D
ur Score,Hist Score,Top Intvl
0.98,192.168.99.52,104.71.255.238,24,5429,130302,1,0.998,0.919,1,1800
0.966,192.168.99.52,52.184.212.181,62,5417,335904,0.895,0.991,0.977,1,900
0.962,192.168.99.52,52.184.217.56,66,5447,359555,0.865,0.991,0.991,1,900
0.911,192.168.99.52,52.184.213.21,65,5392,350529,0.668,0.991,0.982,1,900
0.728,192.168.99.52,52.167.17.97,33,5691,187806,0.471,0.843,0.928,0.667,0
0.719,192.168.99.52,208.67.220.220,118,253,29956,0.563,0.947,0.971,0.393,1
0.655,192.168.99.52,208.67.222.222,319,221,70574,0.479,0.821,0.996,0.321,0
thunt@thunt-labs:~/lab3$ _
```

We can check these IPs with the "fq" command

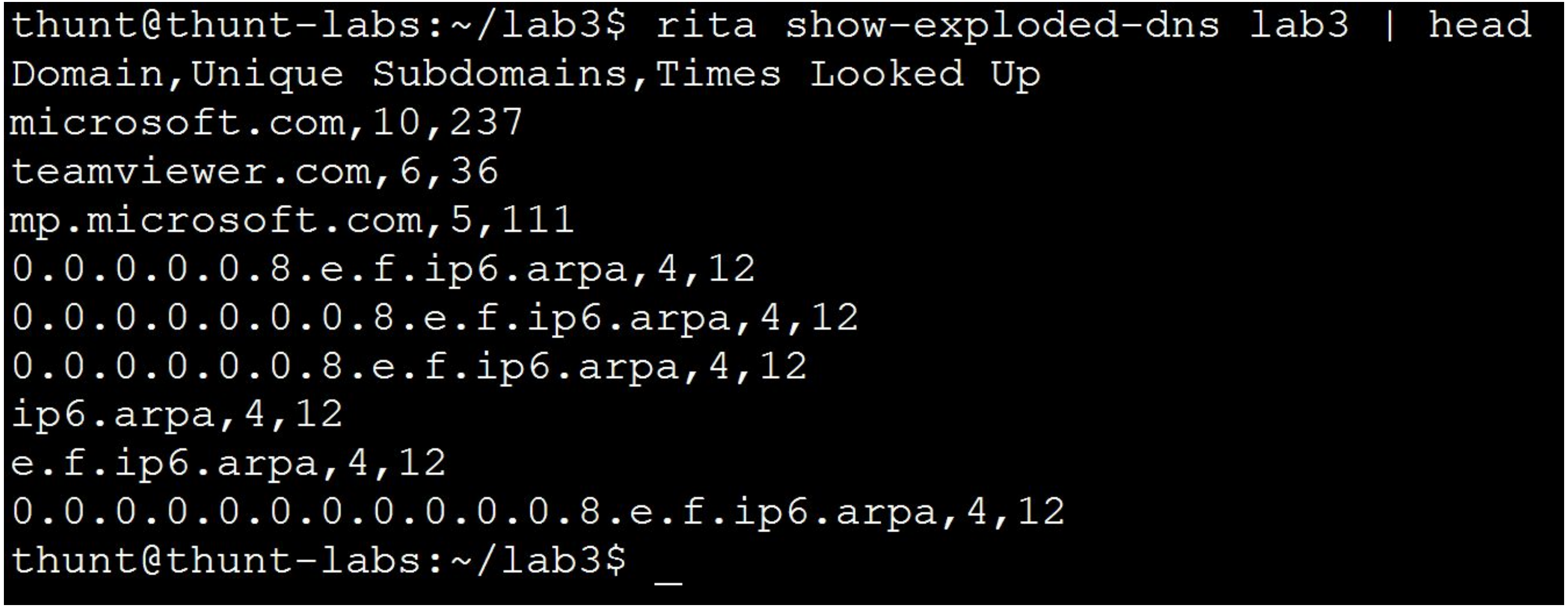
More MS traffic



```
thunt@thunt-labs:~/lab3$ fq 104.71.255.238
DNS info
wildcard.weather.microsoft.com.edgekey.net,e15275.g.akamaiedge.net,104.71.255.238
tile-service.weather.microsoft.com
TLS info
thunt@thunt-labs:~/lab3$ fq 52.184.212.181
DNS info
52.184.212.181  array510.prod.do.dsp.mp.microsoft.com
TLS info
52.184.212.181  array510.prod.do.dsp.mp.microsoft.com   unable to get local issuer ce
rtificate
thunt@thunt-labs:~/lab3$
```

All beacons are Microsoft traffic associated with normal Windows op

C2 over DNS check



```
thunt@thunt-labs:~/lab3$ rita show-exploded-dns lab3 | head
Domain,Unique Subdomains,Times Looked Up
microsoft.com,10,237
teamviewer.com,6,36
mp.microsoft.com,5,111
0.0.0.0.0.8.e.f.ip6.arpa,4,12
0.0.0.0.0.0.0.8.e.f.ip6.arpa,4,12
0.0.0.0.0.0.8.e.f.ip6.arpa,4,12
ip6.arpa,4,12
e.f.ip6.arpa,4,12
0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa,4,12
thunt@thunt-labs:~/lab3$ _
```

No results of note

Answers - Final

- We found:
  - 2 long connections
  - 4 beacons
- Only 1 connection of concern
  - System connecting to TeamViewer
  - Long connection
  - Need to verify if there is a business need for TeamViewer running on this system