SHRESHTA IT

Threat hunting using DNS

@pswapneel

TLP:WHITE

$whoami

- Chief Network Security engineer and CEO @ Shreshta IT - 15+ years in Information Security
- Technical trainer - workshops on Information Security, Network Security Monitoring, DNS/DNSSEC Security, UNIX system administration
- APNIC Community Trainer
- Active participant and speaker in the security community and NOG's in the Asia Pacific region and most recently has presented at 2020 FIRST Virtual Symposium for Latin America and Caribbean, APNIC 50, UKNOF July, APNIC NFH SEA, LKNOG3
- @pswapneel
- swapneel.patnekar@shreshtait.com

Background

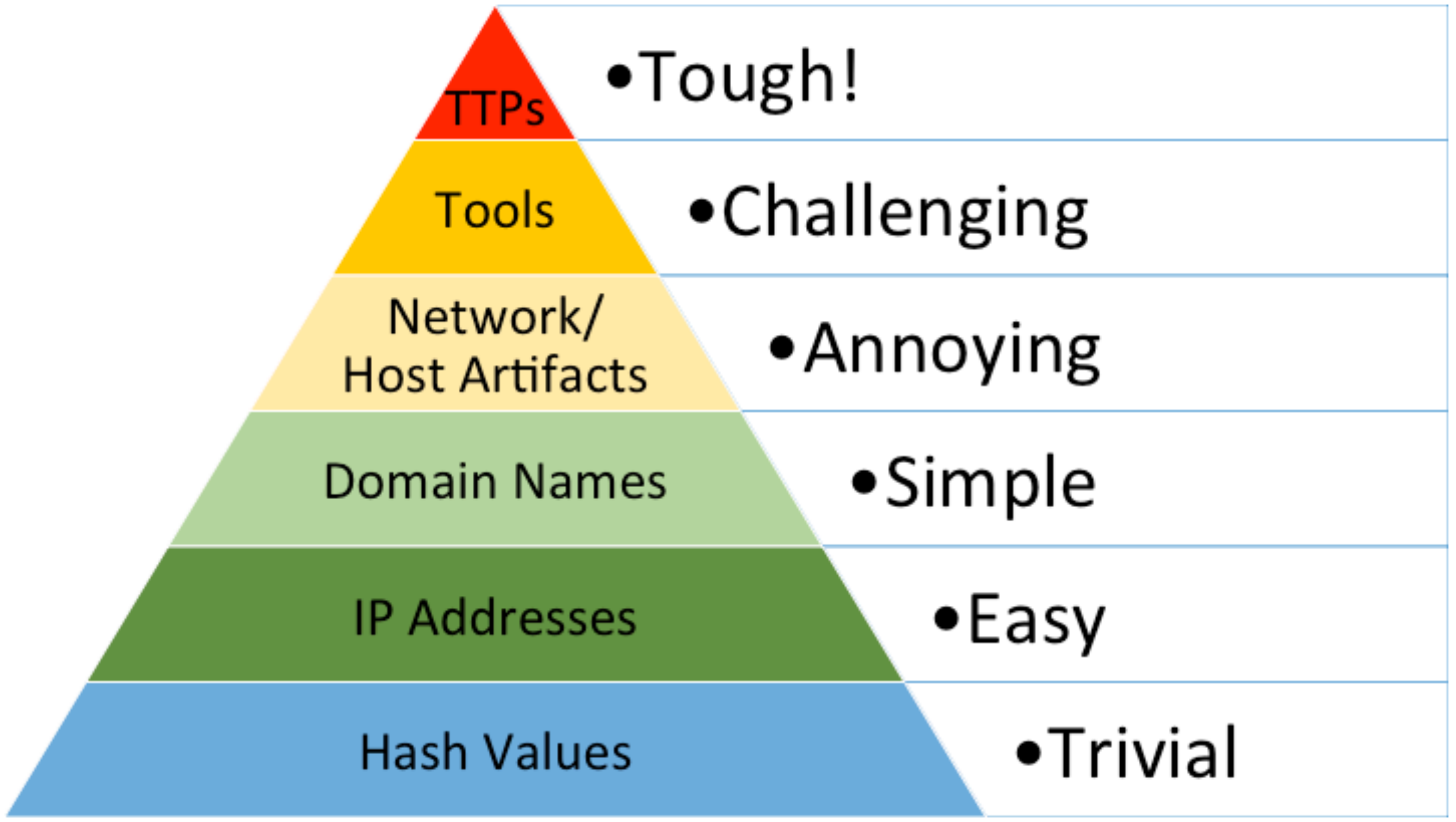
- At $dayjob, we implement Network Security Monitoring(NSM) & DNS Firewalls (Response Policy Zones)
  - 200+ recursive resolvers

- Networks - Network operators, enterprise networks

- Recursive resolver software - BIND9, Unbound

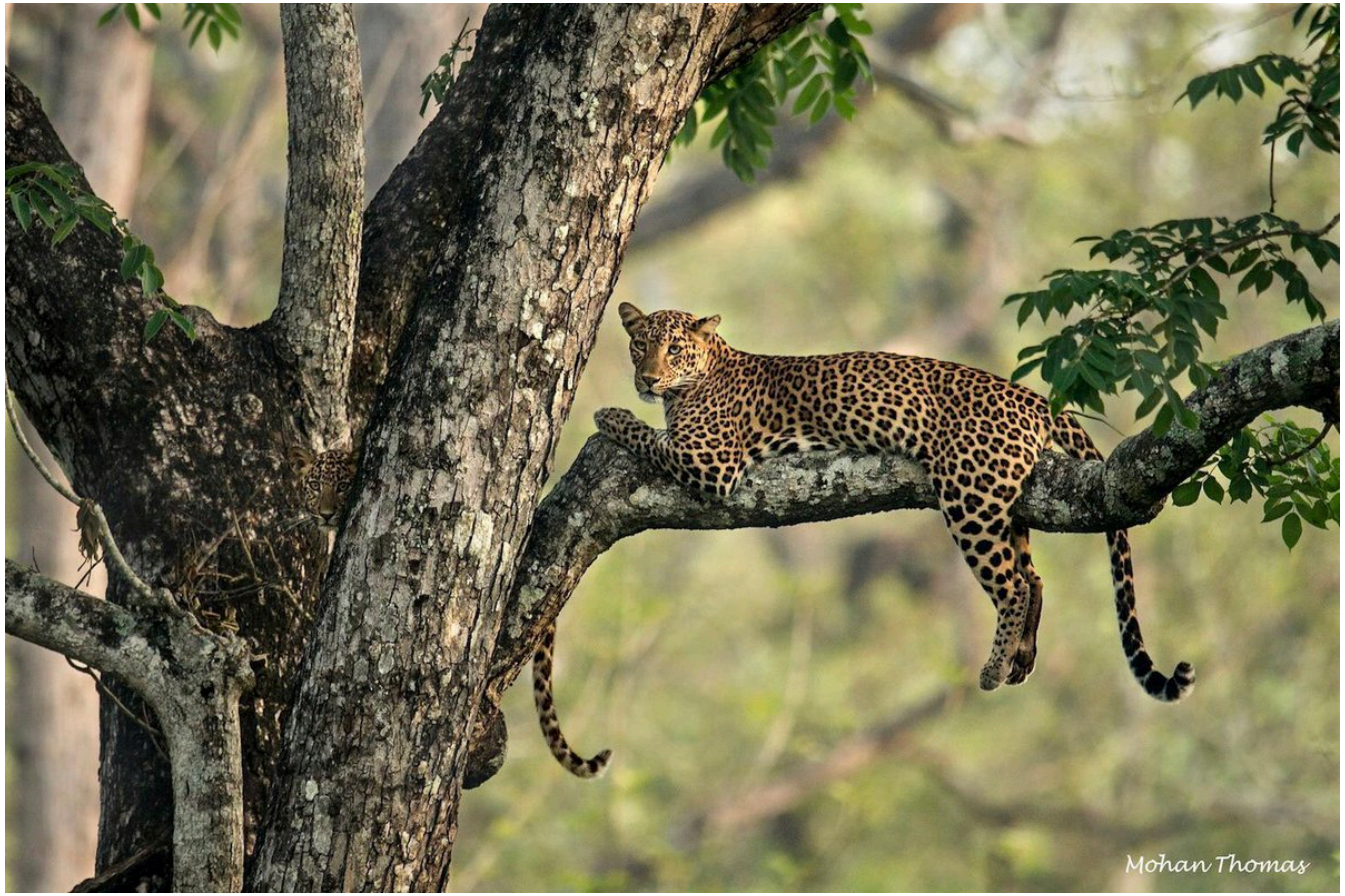
Pyramid of Pain

- Everything on the Internet begins with a DNS query
- Domain names are cheap and used by malware
- Using DNS as layer of defence - Economical layer in a multi-tiered security defense
- Atomic indicators in DNS are a great source for threat hunting!



Source: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Finding anomalies



Source - Mohan Thomas / https://twitter.com/GetMohanThomas/status/1408309926460477441?s=20

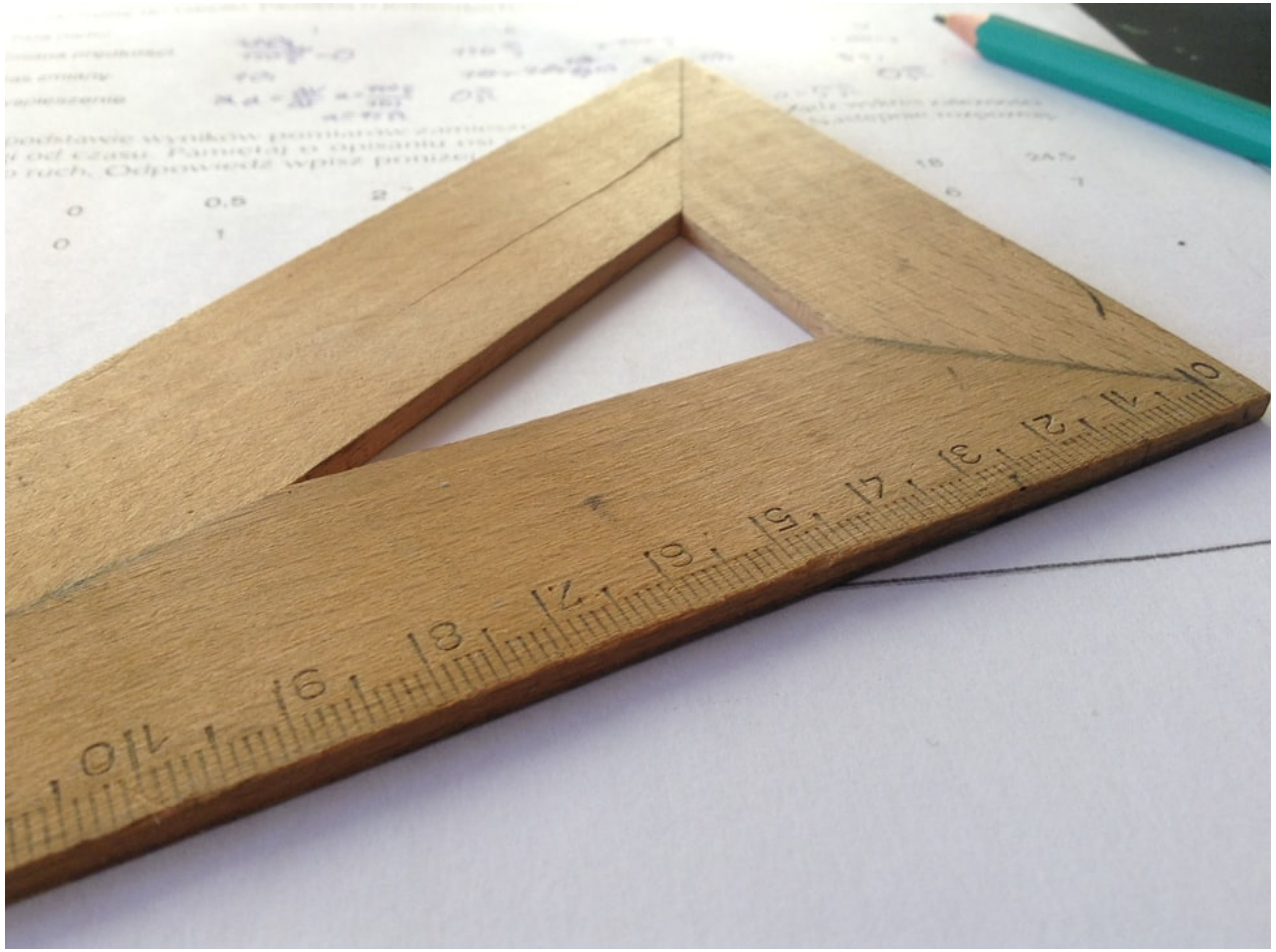
Anomalies

- DGA’s
- Fast flux
- Newly registered domains
- Look alike domains
- Punycode domains

Source: https://www.porterblepeople.com/2015/03/finding-your-material-dropbox-and-devonthink/

Baselining your environment

- On-premise email server in the infrastructure will result in a lot of DNS PTR
- Web browsing will be DNS A, AAAA, CNAME
- What is triggering the NXDOMAIN and NULL responses ?



Source: @djmalecki / Unsplash

Malware 🔗🛸

Domain Generation Algorithm (DGA)

- Malware connects to a single/few domains - Defence implies blocking the malicious domains
- DGA - On the fly generation of new domain names for the malware to connect to (C2C)
- Detection becomes more work for network defenders

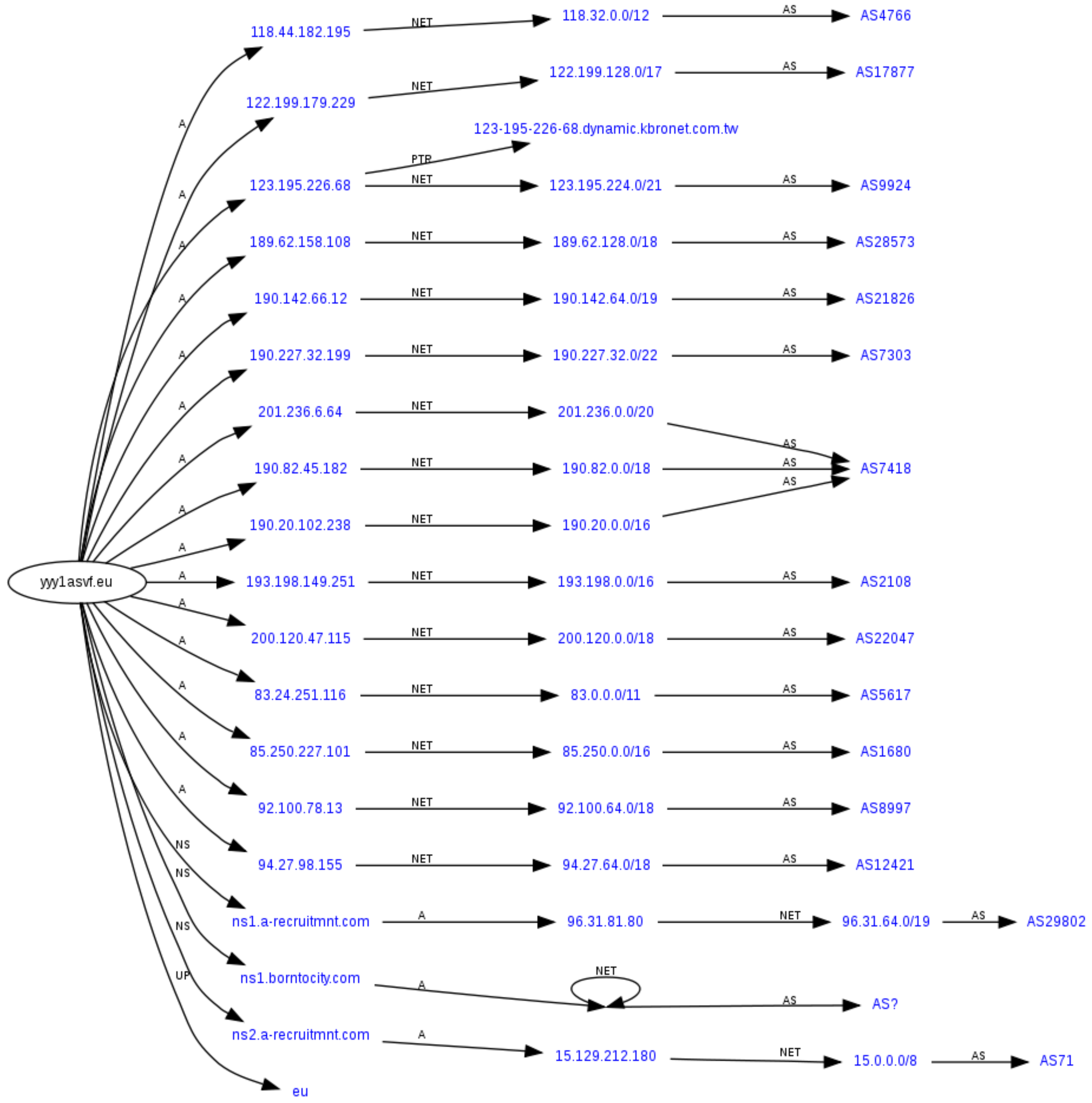
PC @nasa / Unsplash

Fast flux

- Domain name points to rapid changing IP address where the IP addresses are swapped in and out with extremely high frequency

- The real attacker network sits behind compromised hosts which are used as proxy

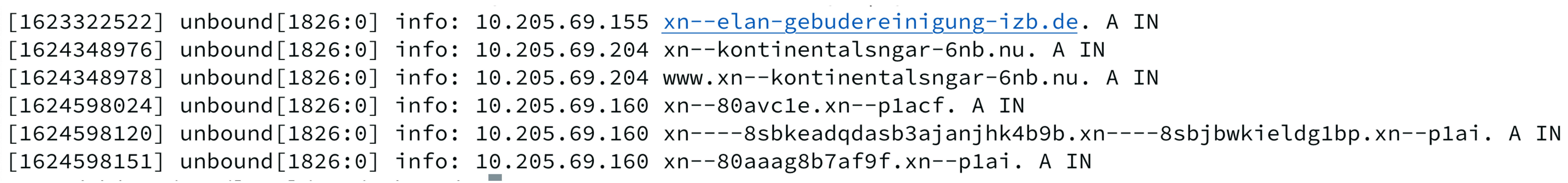
- Mitigation is by blocking the domain but detection is key



Source: https://en.wikipedia.org/wiki/Fast_flux

Punycode domains

- Punycode is a special encoding used to convert Unicode characters to ASCII

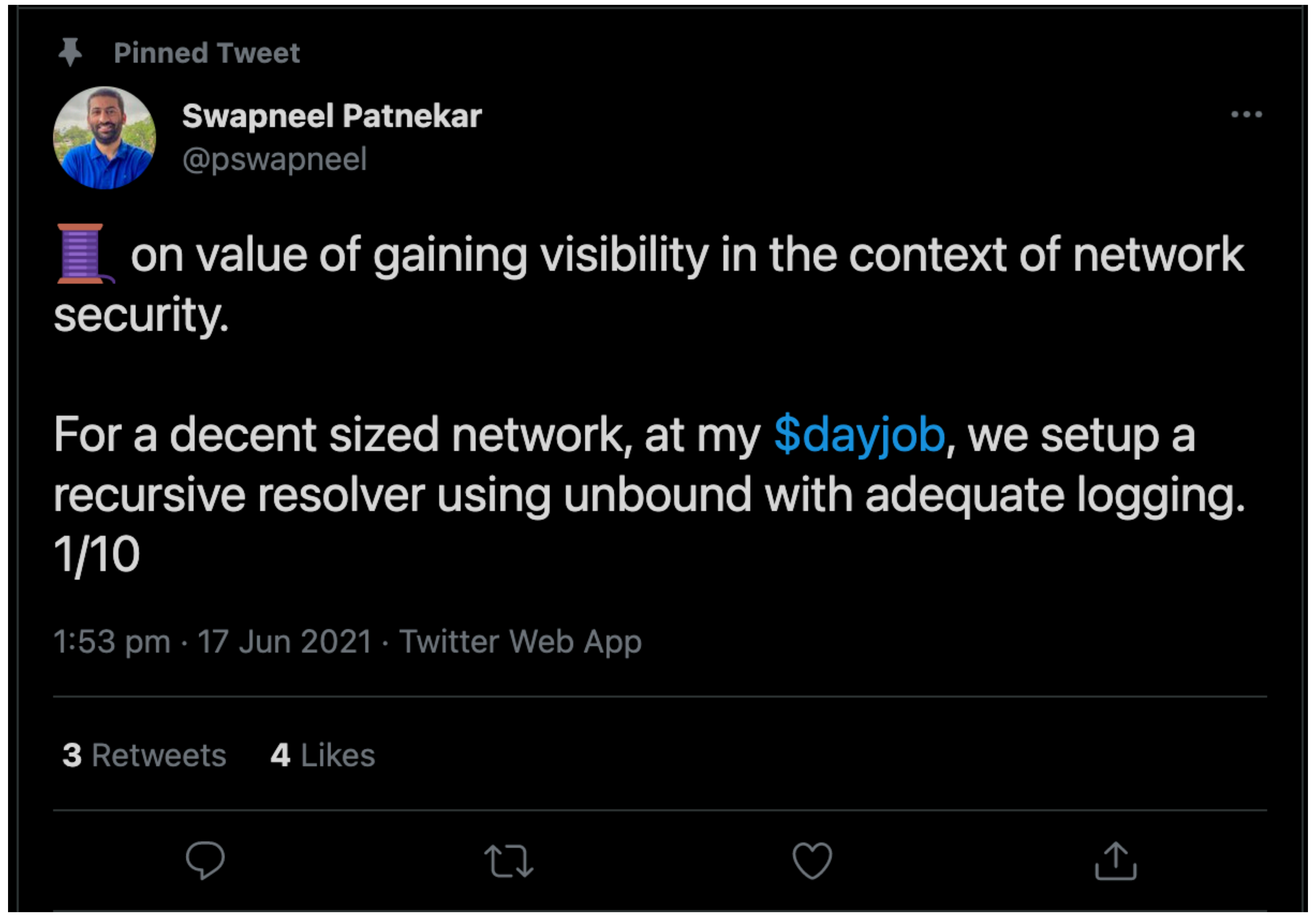


```
[1623322522] unbound[1826:0] info: 10.205.69.155 xn--elan-gebudereinigung-izb.de. A IN
[1624348976] unbound[1826:0] info: 10.205.69.204 xn--kontinentalsngar-6nb.nu. A IN
[1624348978] unbound[1826:0] info: 10.205.69.204 www.xn--kontinentalsngar-6nb.nu. A IN
[1624598024] unbound[1826:0] info: 10.205.69.160 xn--80avc1e.xn--p1acf. A IN
[1624598120] unbound[1826:0] info: 10.205.69.160 xn----8sbkeadqdasb3ajanjhk4b9b.xn----8sbjbwkieldg1bp.xn--p1ai. A IN
[1624598151] unbound[1826:0] info: 10.205.69.160 xn--80aaag8b7af9f.xn--p1ai. A IN
```

www.xn--kontinentalsngar-6nb.nu ————-> www.kontinentalsängar.nu.

The Hunt

- Network operator - 5000 systems
  Internal network



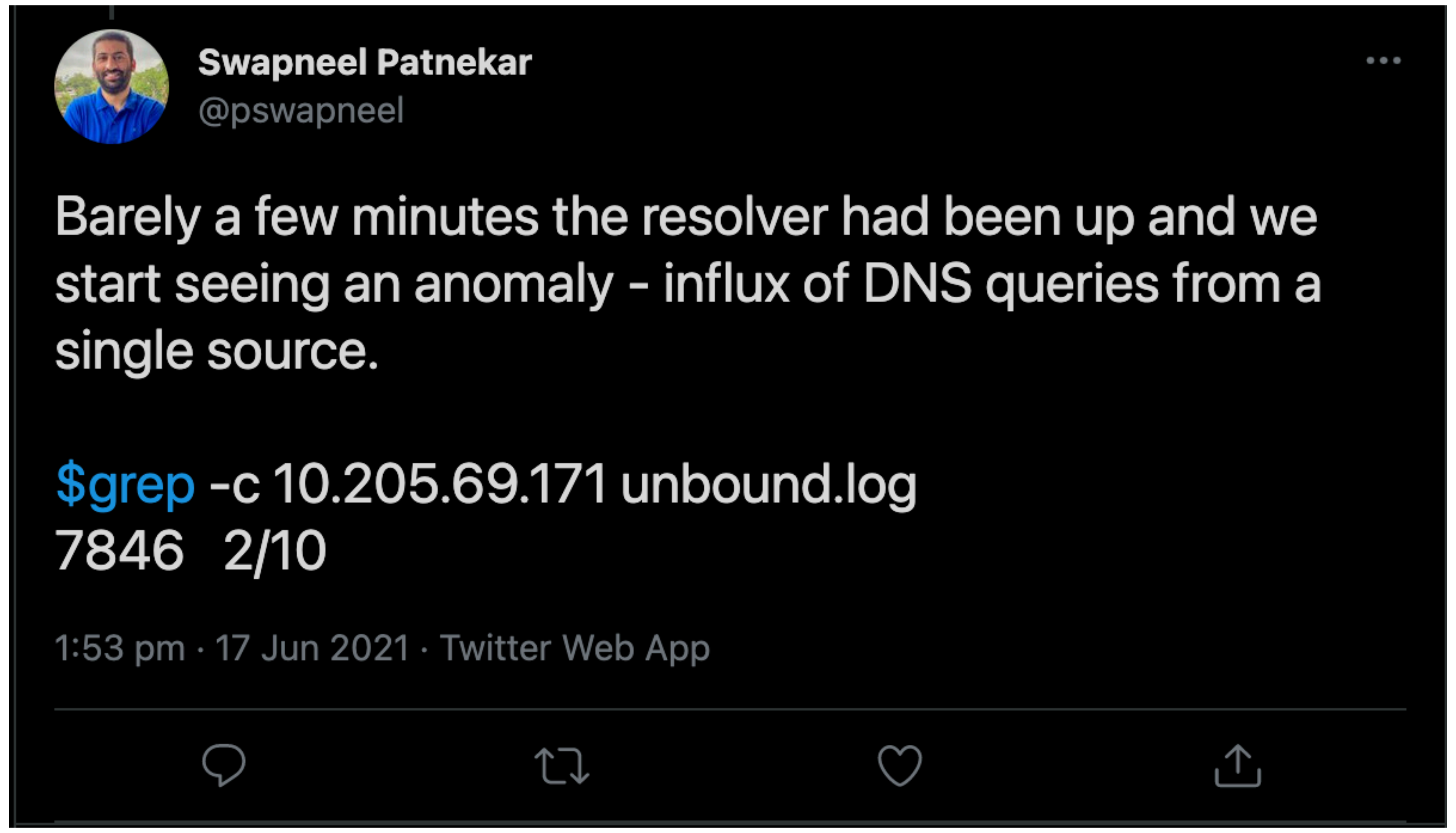
Swapneel Patnekar
@pswapneel

🧵 on value of gaining visibility in the context of network security.

For a decent sized network, at my $dayjob, we setup a recursive resolver using unbound with adequate logging. 1/10

1:53 pm · 17 Jun 2021 · Twitter Web App

3 Retweets 4 Likes

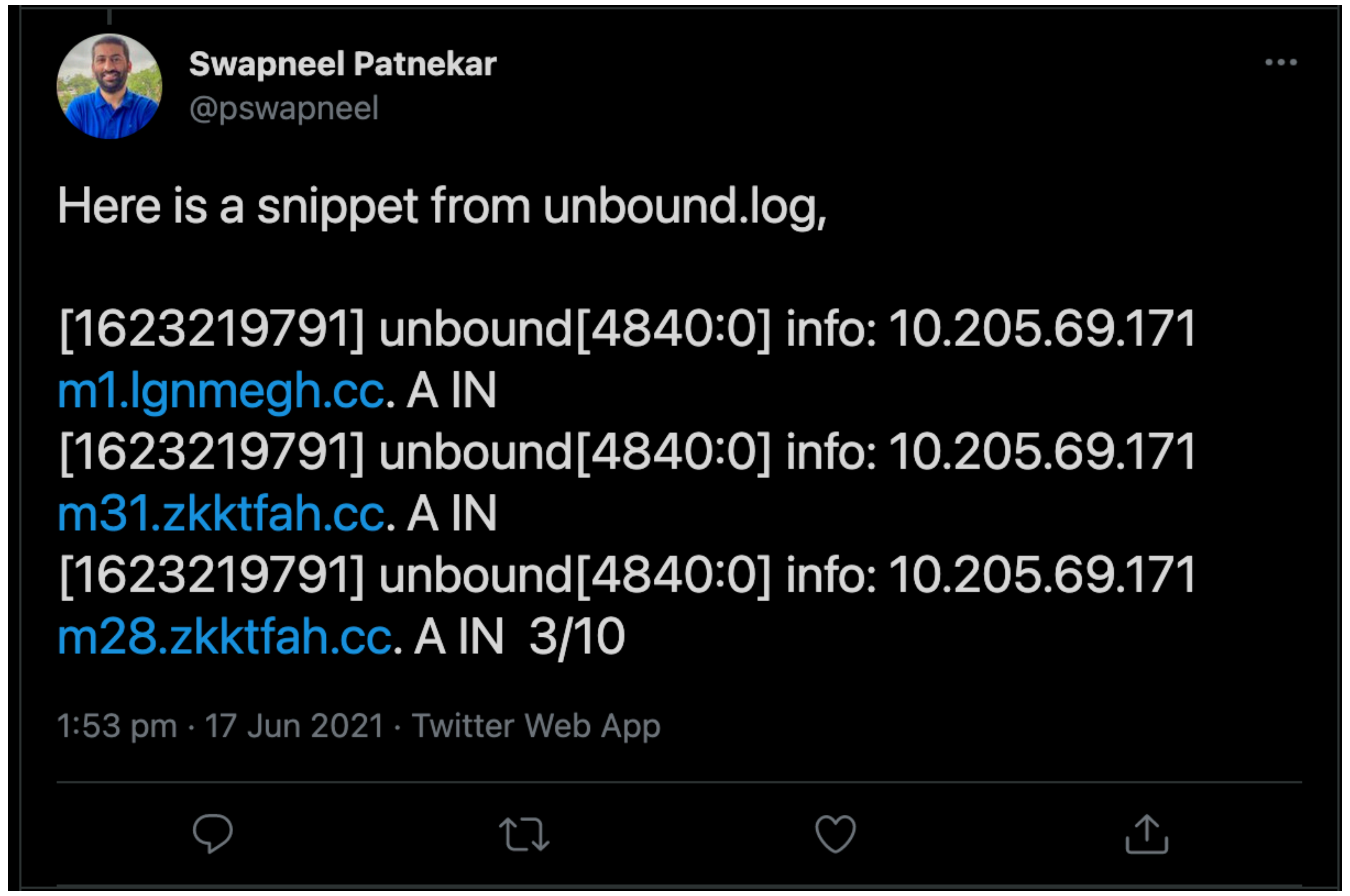


Swapneel Patnekar
@pswapneel

Barely a few minutes the resolver had been up and we start seeing an anomaly - influx of DNS queries from a single source.

```
$grep -c 10.205.69.171 unbound.log
7846   2/10
```

1:53 pm · 17 Jun 2021 · Twitter Web App



Swapneel Patnekar
@pswapneel

Here is a snippet from unbound.log,

```
[1623219791] unbound[4840:0] info: 10.205.69.171
m1.lgnmegh.cc. A IN
[1623219791] unbound[4840:0] info: 10.205.69.171
m31.zkktfah.cc. A IN
[1623219791] unbound[4840:0] info: 10.205.69.171
m28.zkktfah.cc. A IN  3/10
```

1:53 pm · 17 Jun 2021 · Twitter Web App

Source: https://twitter.com/pswapneel/status/1405441027746324482?s=20

DNS logging

- DNS query logging doesn’t log responses by default
- Logging responses impacts the operational performance of the DNS resolver
- DNS query logging - bare minimum - something is better than nothing!

Tools of the trade

Security Onion

https://securityonionsolutions.com/

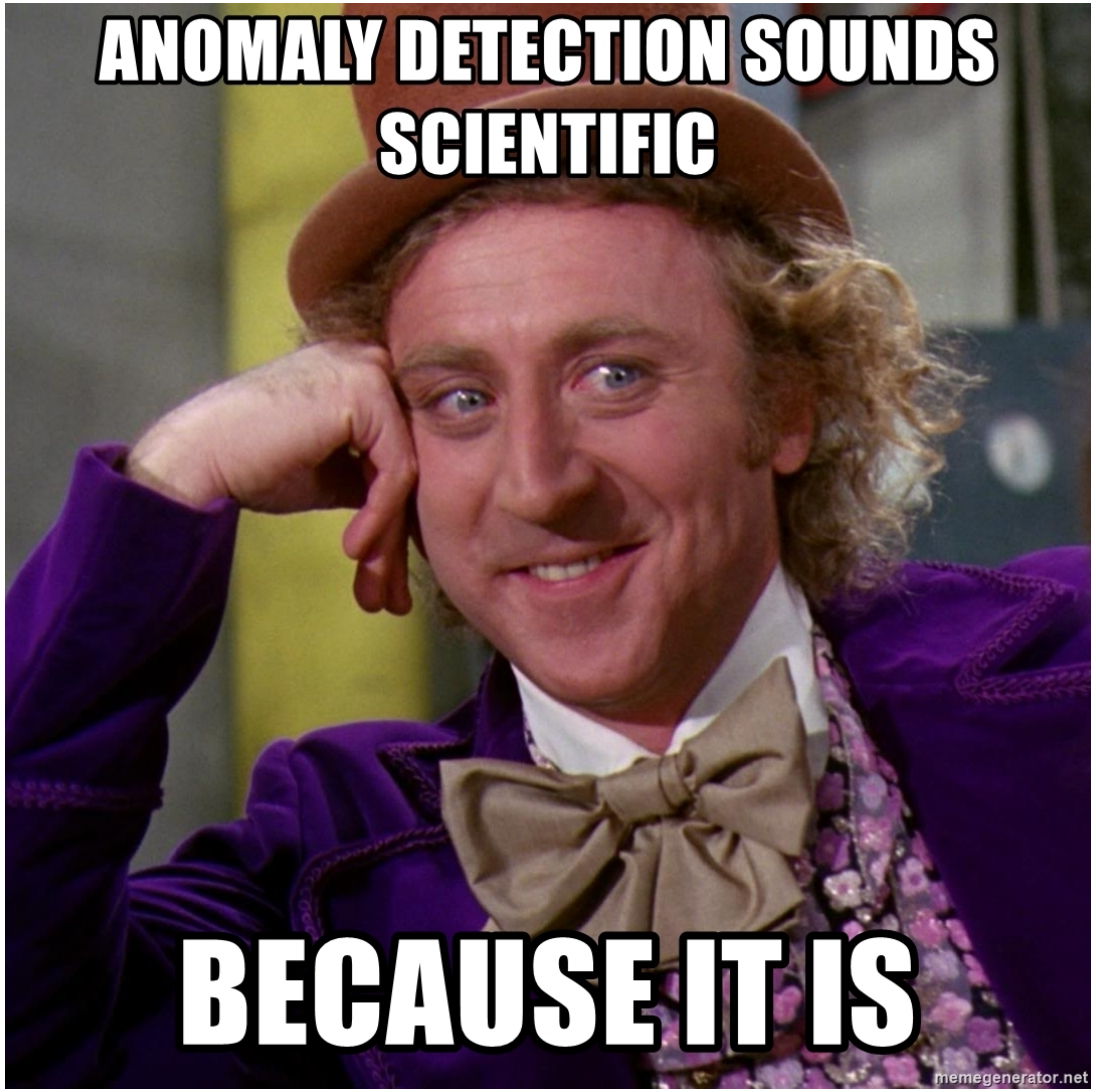
zeek

https://zeek.org/

Source: https://memegenerator.net/img/instances/61457871/open-source-open-source-open-source-open-source.jpg

domain_stats2

- A log enrichment utility written by Mark Baggett
- Domains that were recently registered
- Domains that no one in your organization has ever visited before
- Domains with hostnames that appear to be random characters



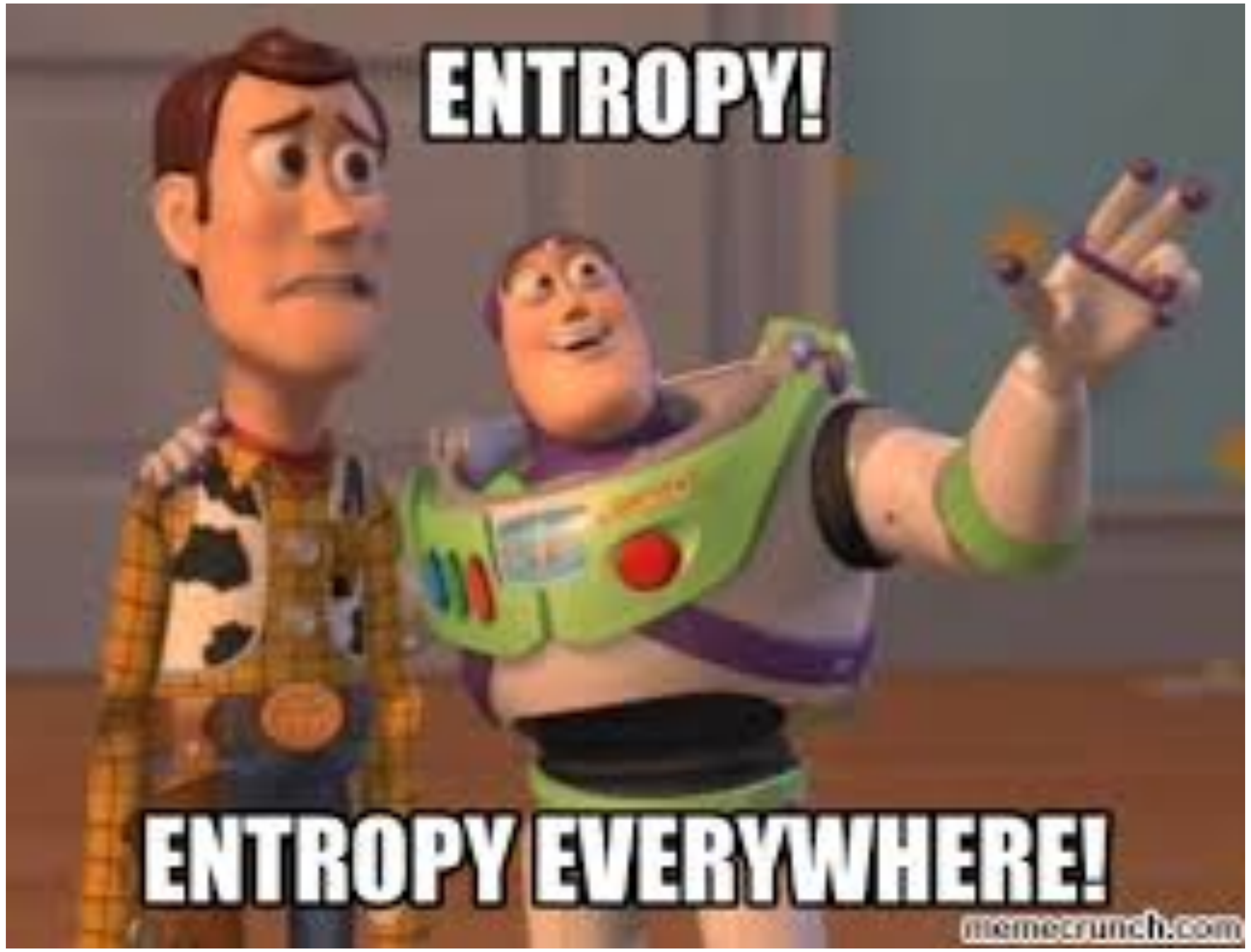
Source : https://memegenerator.net/instance/60078448/willy-wonka-anomaly-detection-sounds-scientific-because-it-is

freq.py

- freq.py and freq_server.py - Tool for detecting DGA written by Mark Baggett

- Web interface which can integrate with a SIEM

- It’s available in Security Onion



Source - https://memecrunch.com/meme/364YE/entropy-everywhere

Passive DNS Monitoring

- Talk I gave ‘Uncovering badness using Passive DNS’ - APNIC 50 FIRST Security 1
- Free and Commercial providers - CIRCL, Farsight Security, Spamhaus Technology
- But they don’t provide the context and correlation within my baseline
- passivedns tool by Edward Bjarte Fjellskål
- Incident handling, Network Security Monitoring, network forensics
- Uses libpcap and parses DNS traffic over TCP and UDP

Demo - Threat hunting in DNS*

*Note to PC - This is a placeholder slide

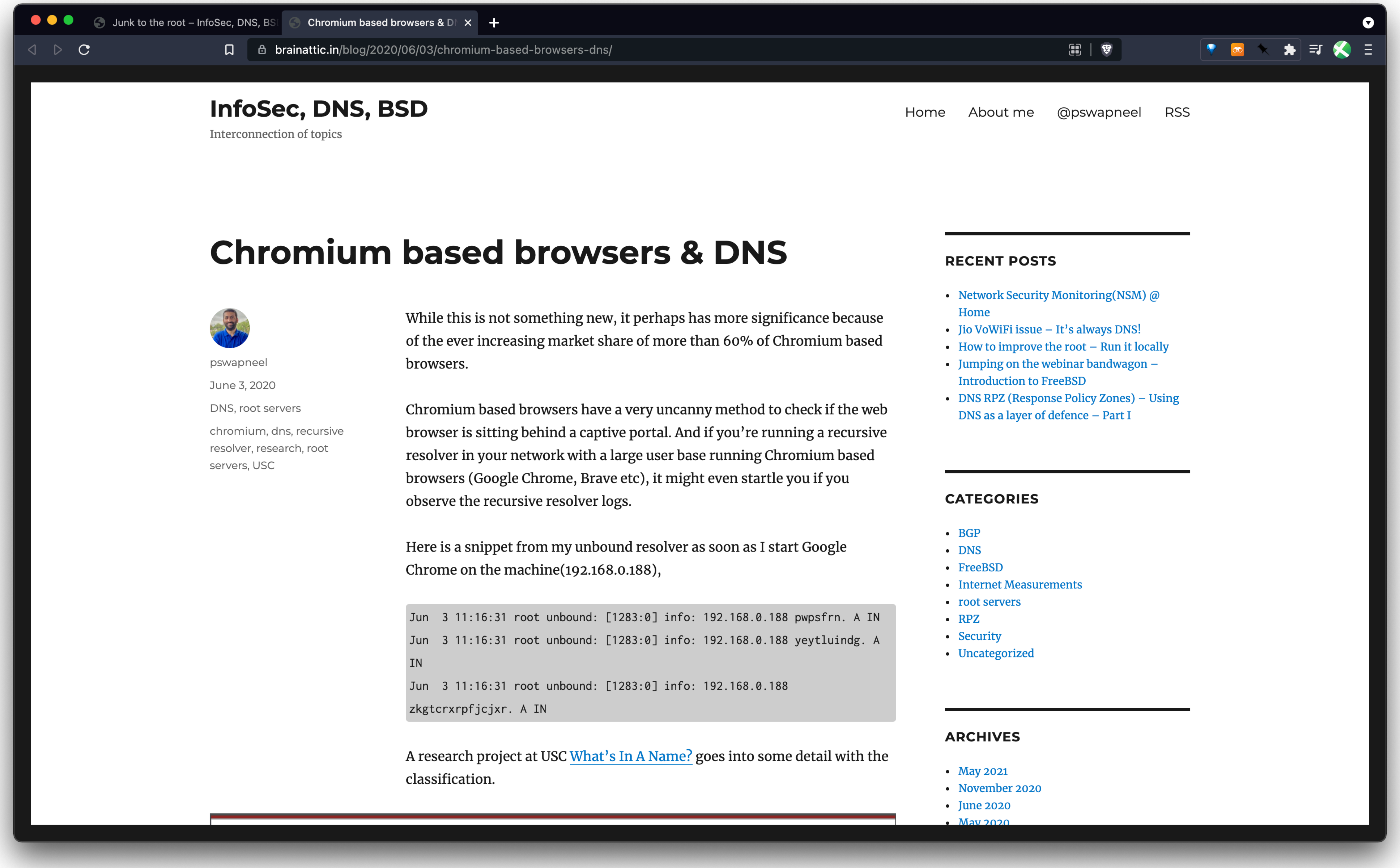
- In this demo, I will be demonstrating how we do threat hunting in DNS by putting all the pieces together

- I will also be showing some interesting things we've been able to uncover
  - How DNS NXDOMAIN and NULL responses led us to a threat hunting rabbit hole
  - Knowing the unknown - We found a DGA, registry had the domains sinkholed. Tracing back to identify the malware is harder than we thought

- Total time for the demo will be within 5 minutes

False Positives

- Chromium browsers - junk queries to the root. Fixed in Chromium 87
- Certain applications send DNS queries which appear to be DGA



Junk to the root – InfoSec, DNS, BS
Chromium based browsers & D
brainattic.in/blog/2020/06/03/chromium-based-browsers-dns/

InfoSec, DNS, BSD

Interconnection of topics

Home
About me
@pswapneel
RSS

Chromium based browsers & DNS

pswapneel

June 3, 2020

DNS, root servers

chromium, dns, recursive resolver, research, root servers, USC

While this is not something new, it perhaps has more significance because of the ever increasing market share of more than 60% of Chromium based browsers.

Chromium based browsers have a very uncanny method to check if the web browser is sitting behind a captive portal. And if you're running a recursive resolver in your network with a large user base running Chromium based browsers (Google Chrome, Brave etc), it might even startle you if you observe the recursive resolver logs.

Here is a snippet from my unbound resolver as soon as I start Google Chrome on the machine(192.168.0.188),

```
Jun  3 11:16:31 root unbound: [1283:0] info: 192.168.0.188 pwpsfrn. A IN
Jun  3 11:16:31 root unbound: [1283:0] info: 192.168.0.188 yeytluindg. A
IN
Jun  3 11:16:31 root unbound: [1283:0] info: 192.168.0.188
zkgtcrxrpfjcjxr. A IN
```

A research project at USC What's In A Name? goes into some detail with the classification.

RECENT POSTS

- Network Security Monitoring(NSM) @ Home
- Jio VoWiFi issue – It's always DNS!
- How to improve the root – Run it locally
- Jumping on the webinar bandwagon – Introduction to FreeBSD
- DNS RPZ (Response Policy Zones) – Using DNS as a layer of defence – Part I

CATEGORIES

- BGP
- DNS
- FreeBSD
- Internet Measurements
- root servers
- RPZ
- Security
- Uncategorized

ARCHIVES

- May 2021
- November 2020
- June 2020
- May 2020

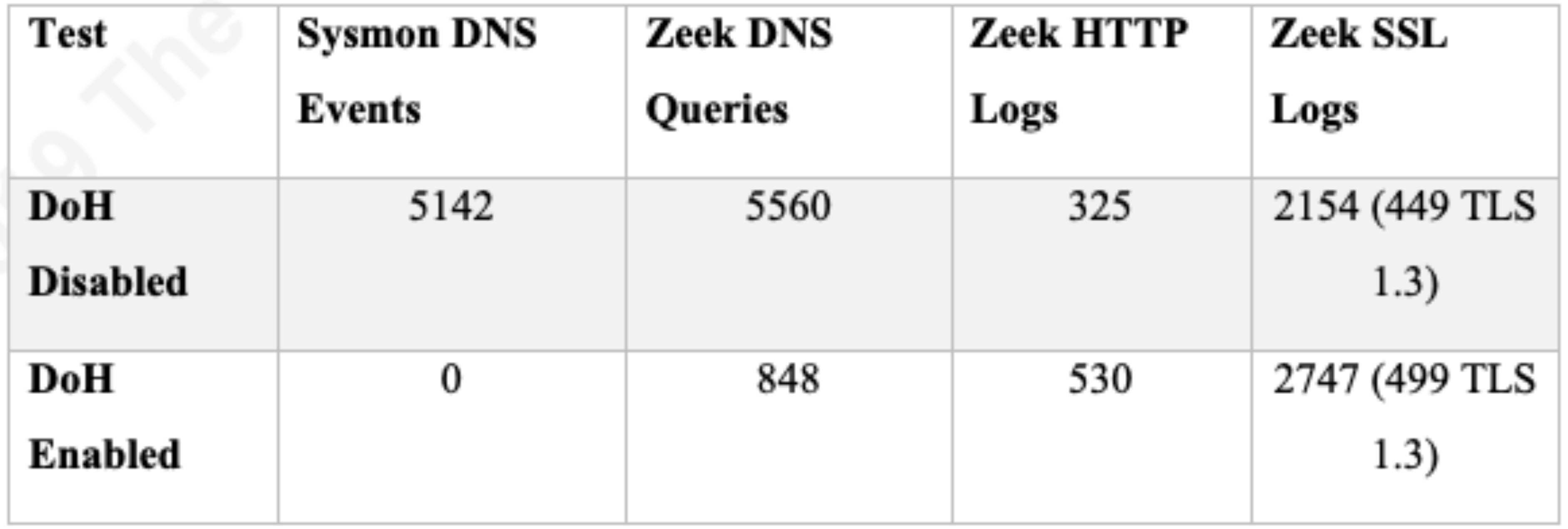
Source: https://brainattic.in/blog/2020/06/03/chromium-based-browsers-dns/

Challenges

Do53

- Plain text query response protocol - It *is* an ideal friend of the network defender

- Visibility - getting insight into a threat hunt starts with DNS



Test	Sysmon DNS Events	Zeek DNS Queries	Zeek HTTP Logs	Zeek SSL Logs
DoH Disabled	5142	5560	325	2154 (449 TLS 1.3)
DoH Enabled	0	848	530	2747 (499 TLS 1.3)

Table 1: DNS over HTTPS Baseline Test

Source: https://www.sans.org/reading-room/whitepapers/dns/paper/39160

DNS over HTTPS (DoH)

- RFC 8484

- Control plane and data plane is the same

- Hides the existence of DNS traffic !

- Identification is a problem - Which session contains DNS traffic and which contains web browsing activity ?

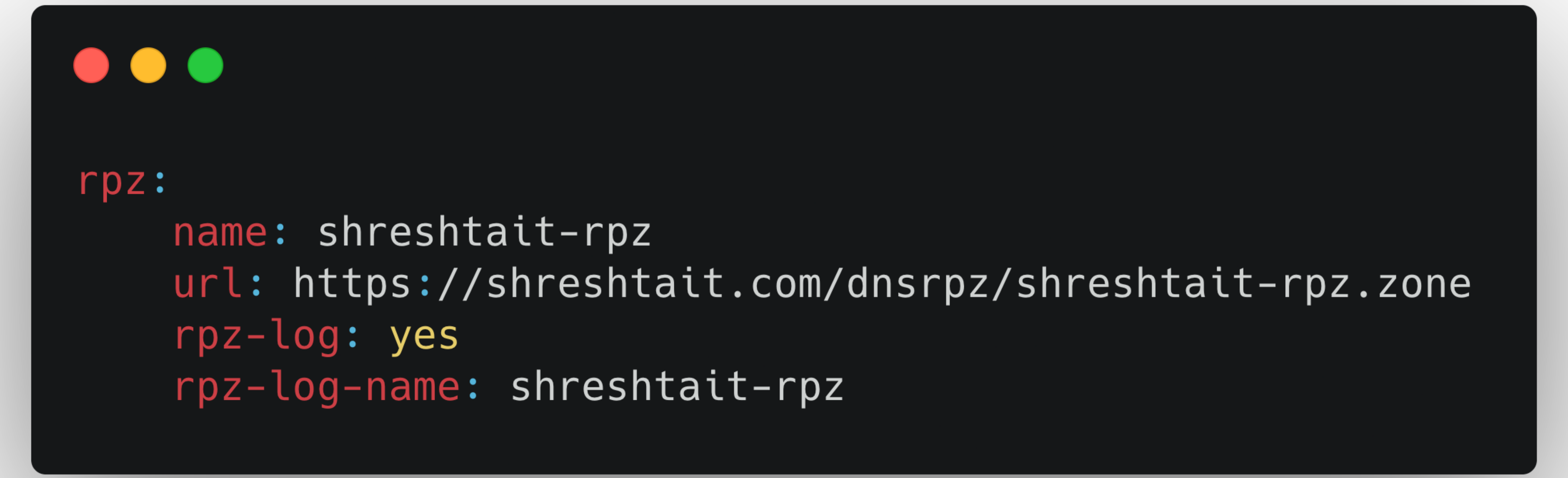
Detecting DoH

- No magic bullets
- TLS Inspection - TLS 1.3 / Certificate Pinning ?
- TLS Fingerprinting - JA3 and JA3S
- Manual heuristics

Source: https://giphy.com/gifs/gifporn-MVUyVpyjakkRW

Community resources

- DNS RPZ zone file - We publish a DNS zone file



```
rpz:
    name: shreshtait-rpz
    url: https://shreshtait.com/dnsrpz/shreshtait-rpz.zone
    rpz-log: yes
    rpz-log-name: shreshtait-rpz
```

- MISP - Currently running a private instance, by end of July 2021, plan is to share with other MISP communities we are already part of CIRCL etc

Hat tip

NLNETLABS

BIND 9

POWERDNS

KNOT DNS

Security Onion

zeek

Resources

- Pyramid of Pain
  https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
- Using DNS as a layer of defence
  https://blog.apnic.net/2020/07/02/dns-rpz-using-the-dns-as-a-layer-of-defence/
- Chromium based browsers and DNS
  https://brainattic.in/blog/2020/06/03/chromium-based-browsers-dns/
- domain_stats2
  https://github.com/MarkBaggett/domain_stats
- APNIC 50 - Uncovering badness using Passive DNS
  https://youtu.be/WKJzVOkMbc0?t=2462
- passivedns - https://github.com/gamelinux/passivedns
- A New Needle and Haystack: Detecting DNS over HTTPS Usage
  https://www.sans.org/reading-room/whitepapers/dns/needle-haystack-detecting-dns-https-usage-39160

Contact

- @pswapneel
- swapneel.patnekar@shreshtait.com