Using 'Big Data' Tools to Understand Your Cyber Environment

(bonus for Incident Response too)

BE Rhodes | November 30th, 2020

Outline

- WHOIS: Brad Rhodes
- Why Are We Here?
- Cyber is Big Data!
- Big Data Tools (Free-*ish* is Good)
- Normalizing Data (Garbage In = Garbage Out)
- Visualizing an Environment (Wireshark, Power BI, Tableau)
- Introducing Pandas Profiling
- **Bonus:** Windows Logs Analysis with Power BI (for IR)
- **Lab Time!**
- Resources for You!
- Questions & Contact Info

Downloads & Install

Time: (allotted) 30 mins, varies depending on your internet connection

- Wireshark: https://www.wireshark.org/download.html
- Microsoft Power BI Desktop (Windows-only): https://powerbi.microsoft.com/en-us/desktop/
  - ✓ Note: this link will open the embedded Microsoft Store application
- Tableau Public (Windows, Mac): https://public.tableau.com/en-us/s/
  - ✓ Note: this download requests an email to download
- MaxMind GeoIP Database (optional): https://dev.maxmind.com/geoip/geoip2/geolite2/
  - ✓ Note: this download requires you establish an account

WHOIS: Brad Rhodes

zvelo

- TLDR:
    - ✓ Head of Cybersecurity at zvelo
    - ✓ LTC, Cyber (17A) Colorado Army National Guard & Cyber Shield Planner
    - ✓ Military Cyber Professionals Association, HammerCon Co-Lead
    - ✓ Speaker, Author, Professor, Instructor, Coach
    - ✓ #toomany Pro-Certs, highlights: CISSP-ISSEP, CISM, PMP, CEH, GMON, GCIH, RHCSA, CCNA Cyber Ops, CySA+

Recordings, presentations and such:
https://github.com/cyberguy514?tab=repositories

Why Are We Here?

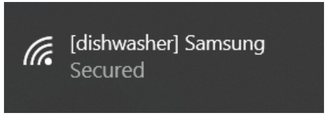
You can put just about EVERYTHING on the Internet today.

- **Traditionals** - Laptops, servers, phones, network hardware, etc.
- **Internet of Things** - Smart speakers, thermostats, fridges, crockpots, and more.
- **Everything Else** - ICS/SCADA, sensors, cars, and others

Do you really know what is in your Cyber Operating Environment?

Are you VULNERABLE (*due to the 'smart' thing your employee BYOD'd*)?

Is your DATA LEAKING right now (*via something you thought you could trust*)?



[dishwasher] Samsung
Secured

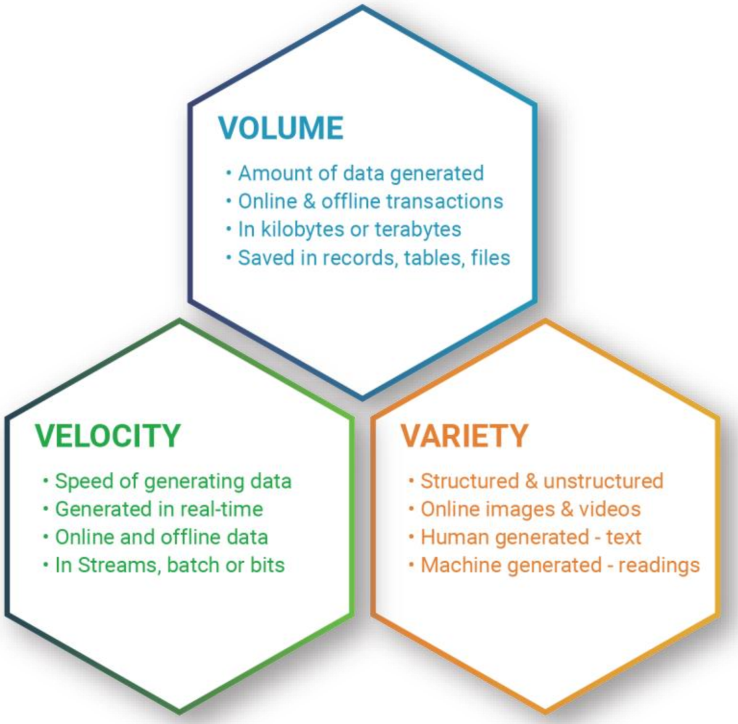
The Numi toilet combines unmatched design and technology to bring you the finest in personal comfort and cleansing. Kohler's most advanced toilet now offers personalized settings that let you fine-tune every option to your exact preferences, from ambient colored lighting to wireless Bluetooth® music sync capability to the heated seat and foot warmer. Play your favorite music and podcasts - simply stream wirelessly with any device enabled with Bluetooth technology, store MP3 files to the SD card, or plug in your device using the auxiliary cable. Other upgrades include Power-Save mode for energy efficiency, emergency flush for power outages, and an intuitive touch-screen remote. From its striking form to its exceptional water efficiency, the Numi toilet marks a new standard of excellence in the bathroom. Read More

If any of these questions keep you up at night, then this talk is for you! Let's explore **'FREE'** (*other than your time*) Big Data tools, tactical techniques, and concepts you can use right now to begin to understand the cyber stuff in your environment! And hopefully sleep a little better!

Cyber is Big Data!

- **VOLUME:** Zettabytes (~1 Billion Terrabytes) of data on the internet (source: Cisco)
- **VOLUME *and* VARIETY:** 5G — support for 1,000,000 devices per km^2 (source: Rogers Communications)
- **VARIETY:** 500 Billion '*things*' on the internet by 2030 (source: Cisco)
- **VOLUME *and* VARIETY:** Small Home Network has 40-50 devices and millions of data points daily
- **VELOCITY:** 1Gbps typical network speeds

THE 3VS OF BIG DATA



VOLUME

- Amount of data generated
- Online & offline transactions
- In kilobytes or terabytes
- Saved in records, tables, files

VELOCITY

- Speed of generating data
- Generated in real-time
- Online and offline data
- In Streams, batch or bits

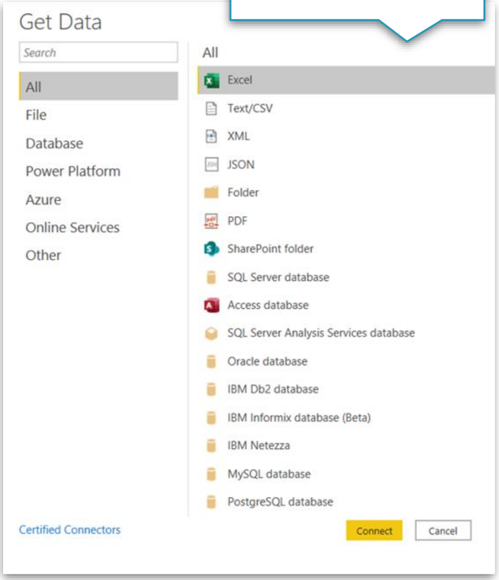
VARIETY

- Structured & unstructured
- Online images & videos
- Human generated - text
- Machine generated - readings

Big Data Tools (Free-ish is Good)

Microsoft Power BI (Desktop): Capabilities & Limitations

70+ Sources!



Get Data

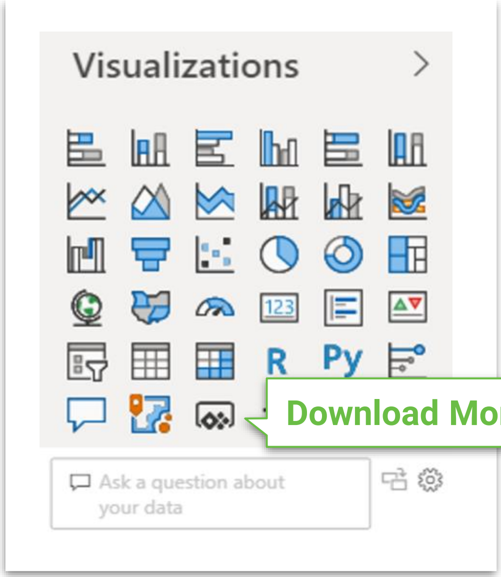
Search

All
File
Database
Power Platform
Azure
Online Services
Other

All
- Excel
- Text/CSV
- XML
- JSON
- Folder
- PDF
- SharePoint folder
- SQL Server database
- Access database
- SQL Server Analysis Services database
- Oracle database
- IBM Db2 database
- IBM Informix database (Beta)
- IBM Netezza
- MySQL database
- PostgreSQL database

Certified Connectors

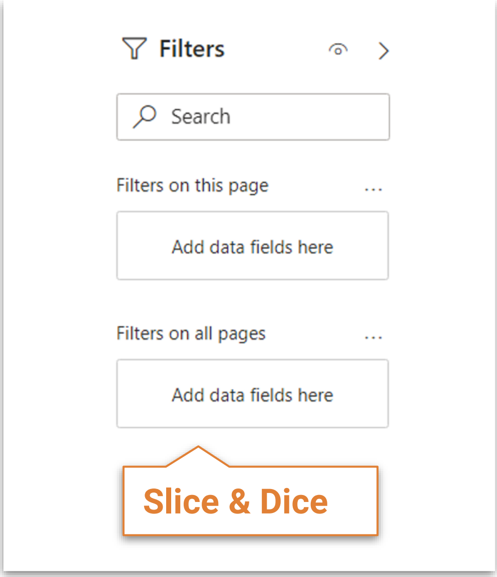
Connect Cancel



Visualizations

Ask a question about your data

Download More!



Filters

Search

Filters on this page ...

Add data fields here

Filters on all pages ...

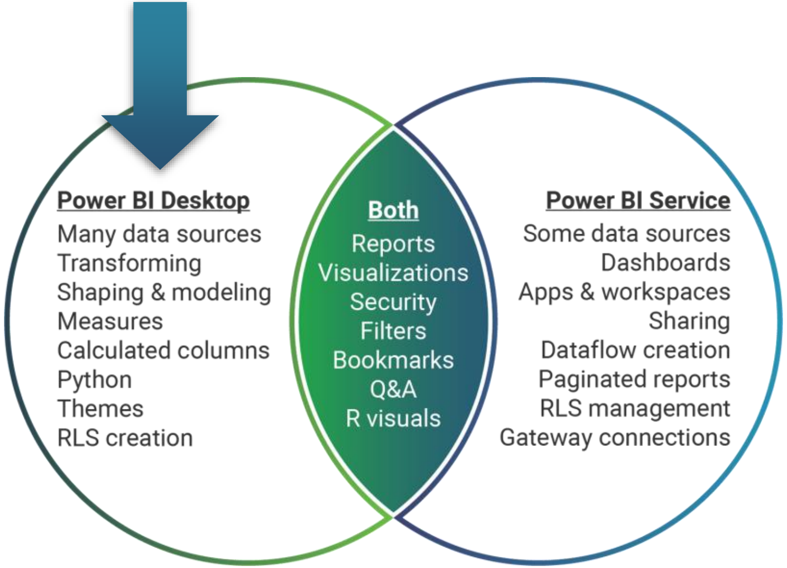
Add data fields here

Slice & Dice

Best Capabilities in Microsoft Power BI Desktop: Ingest, Build, Save, & **REFRESH**!

Big Data Tools (Free-ish is Good)

Microsoft Power BI (Desktop): Capabilities & Limitations

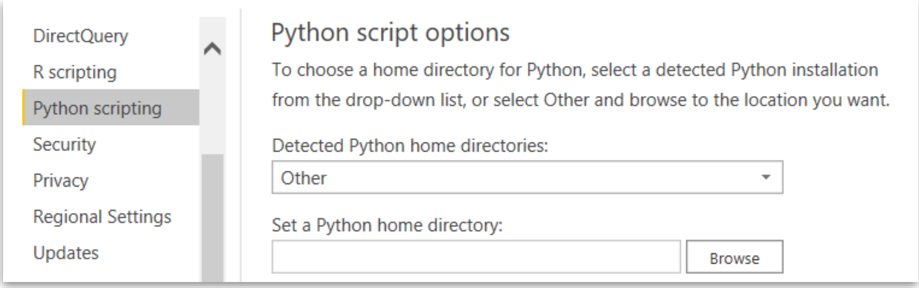


Power BI Desktop
Many data sources
Transforming
Shaping & modeling
Measures
Calculated columns
Python
Themes
RLS creation

Both
Reports
Visualizations
Security
Filters
Bookmarks
Q&A
R visuals

Power BI Service
Some data sources
Dashboards
Apps & workspaces
Sharing
Dataflow creation
Paginated reports
RLS management
Gateway connections

Ref: https://docs.microsoft.com/en-us/power-bi/fundamentals/service-service-vs-desktop



Python script options

To choose a home directory for Python, select a detected Python installation from the drop-down list, or select Other and browse to the location you want.

Detected Python home directories: Other

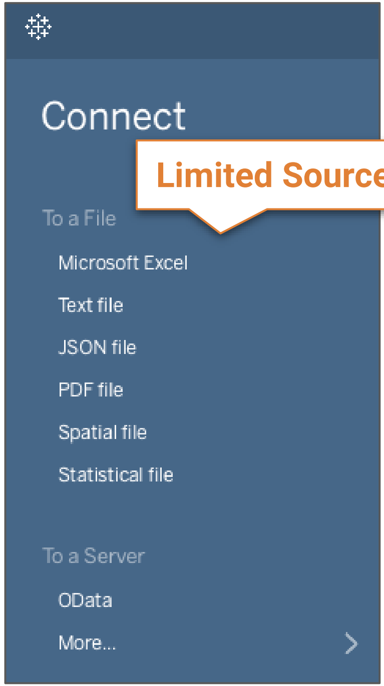
Set a Python home directory:

Power BI Key Limitations:

- 1GB data ingest
- Records/rows limits depend on data source size
- Cannot save visualization directly (but you export as PDF!)
- Sharing visualizations requires receiver to have Power BI

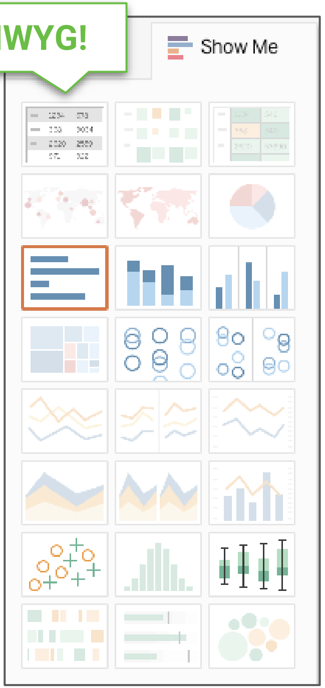
Big Data Tools (Free-ish is Good)

Tableau Public (Desktop & Online): Capabilities and Limitations

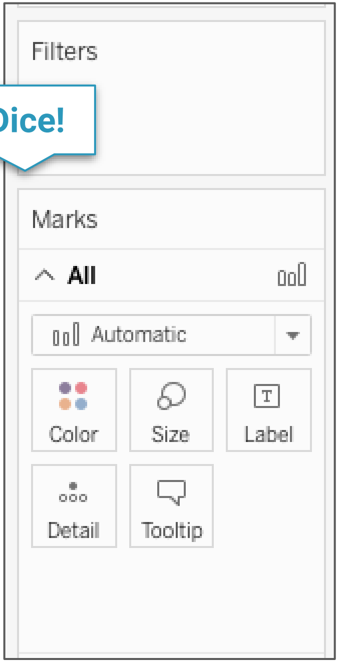


Limited Sources!

WYSIWYG!



Slice & Dice!



Best Capabilities in Tableau Public Desktop: JSON file handling & Sharing*

Big Data Tools (Free-ish is Good)

Tableau Public (Desktop & Online): Capabilities and Limitations

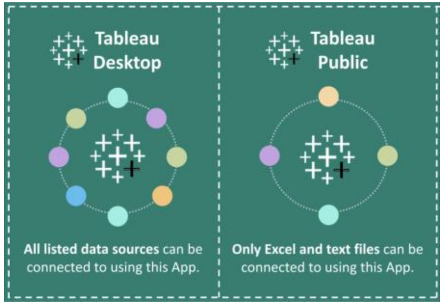


Tableau Desktop
Tableau Public
All listed data sources can be connected to using this App.
Only Excel and text files can be connected to using this App.

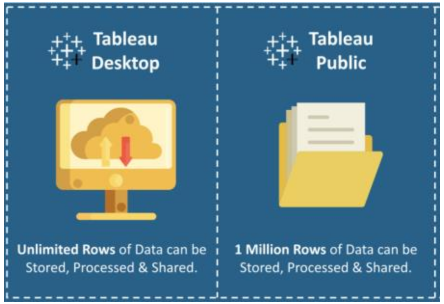


Tableau Desktop
Tableau Public
Unlimited Rows of Data can be Stored, Processed & Shared.
1 Million Rows of Data can be Stored, Processed & Shared.

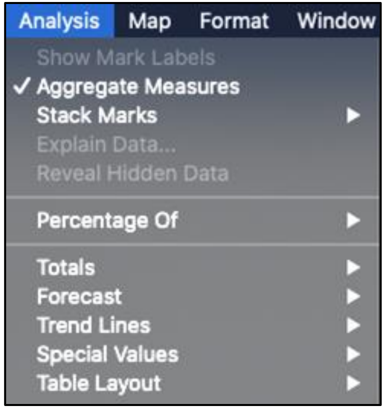


Tableau Desktop
Tableau Public
Nobody can see your reports unless provided with an access.
All the Reports are public once they're published.

Ref: https://www.edureka.co/blog/tableau-desktop-vs-tableau-public-vs-tableau-reader/

Tableau Public Key Limitations:

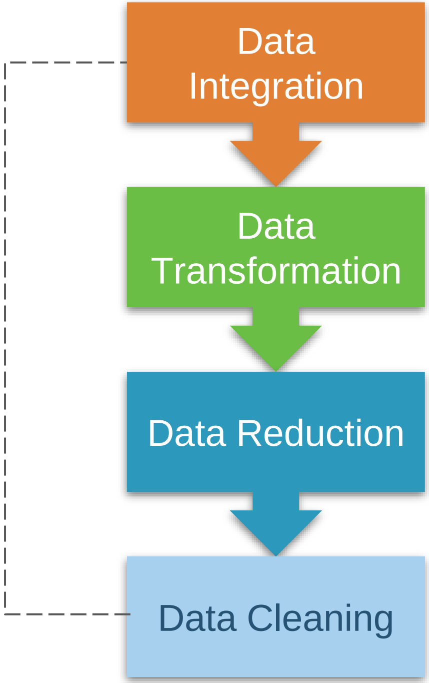
- 1M records/rows limits
- Limited data sources
- *** RISK:** To save your visualizations, they are saved to the Tableau Public Cloud (you can restrict access).

Big Data Tools (Free-ish is Good)

Security
Onion

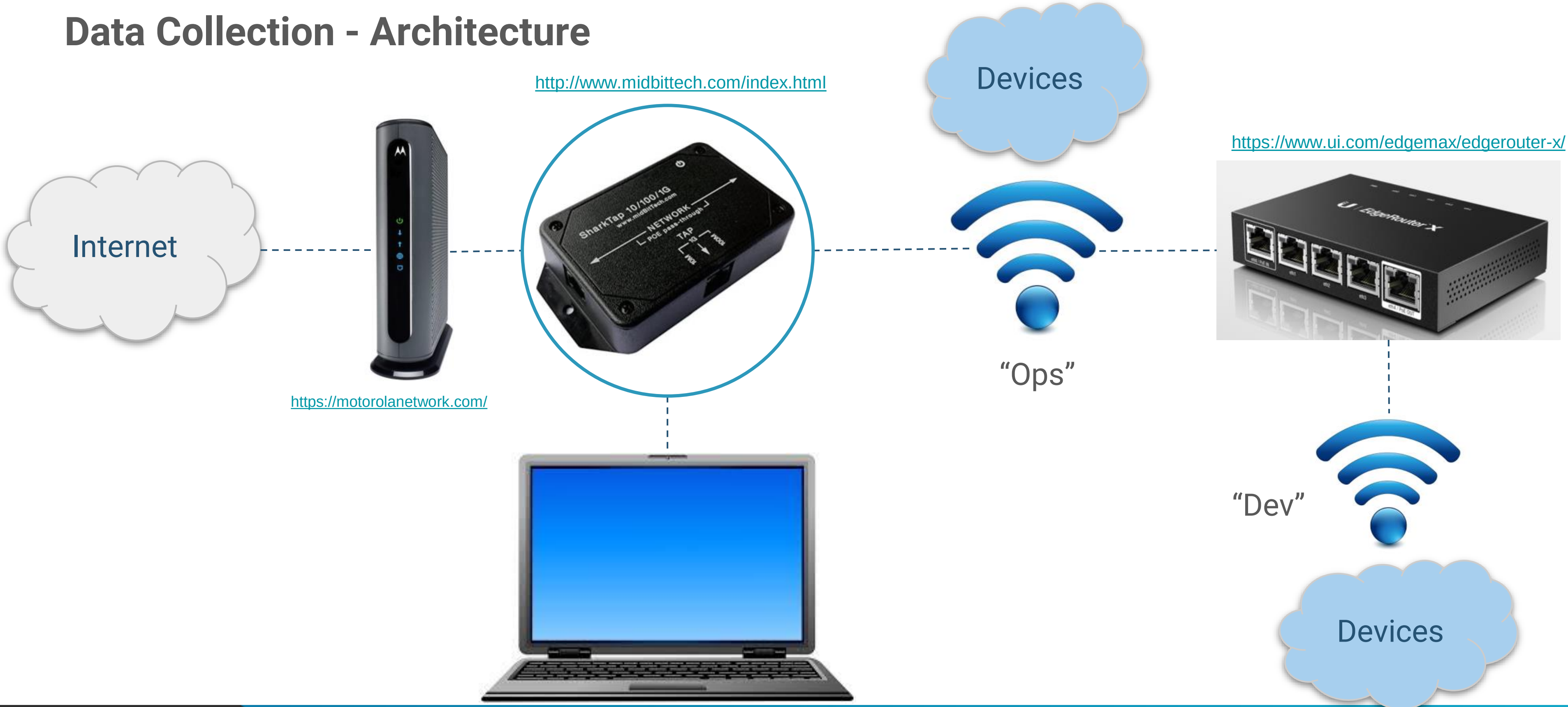
Normalizing Data (Garbage In = Garbage Out)

- What are your sources?
- Are there common fields in your sources?
- If there are common fields, is the data format the same?
- Are there logical pivot points?
- Are there duplicates in the data? How do you dedupe?
- **Goal: Extract, Transform, Load (ETL)**



Visualizing an Environment (Wireshark and Power BI)

Data Collection - Architecture



http://www.midbittech.com/index.html

Devices

https://www.ui.com/edgemax/edgerouter-x/

Internet

“Ops”

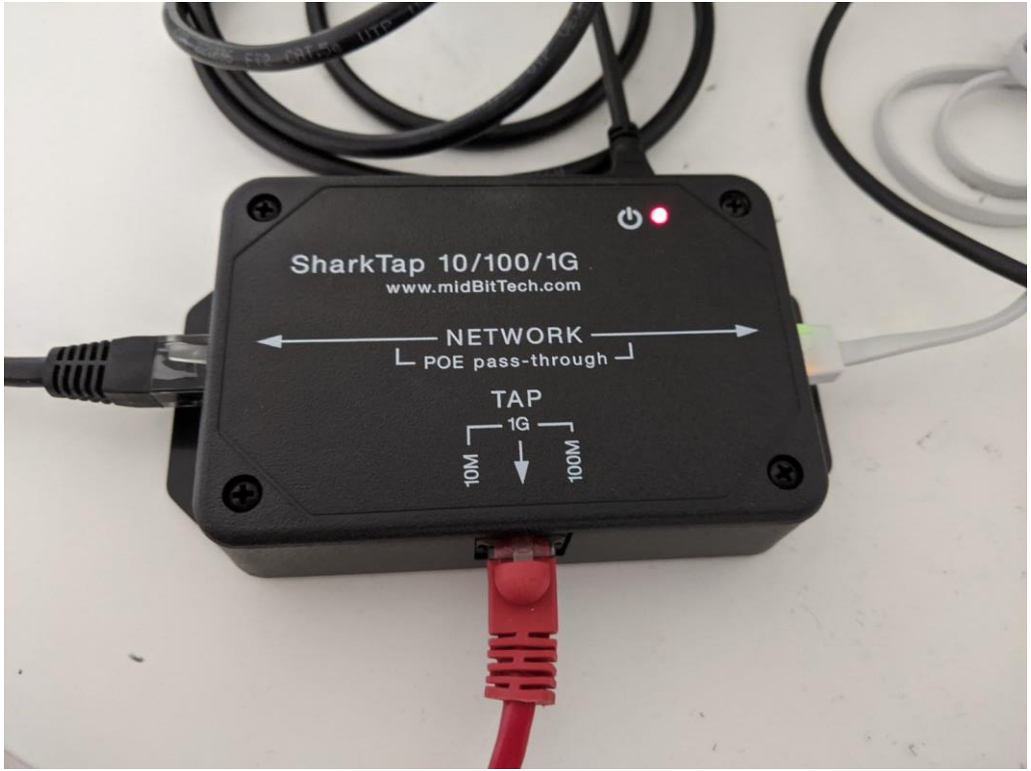
https://motorolanetwork.com/

“Dev”

Devices

Visualizing an Environment (Wireshark and Power BI)

“Sensors” - the Tap!



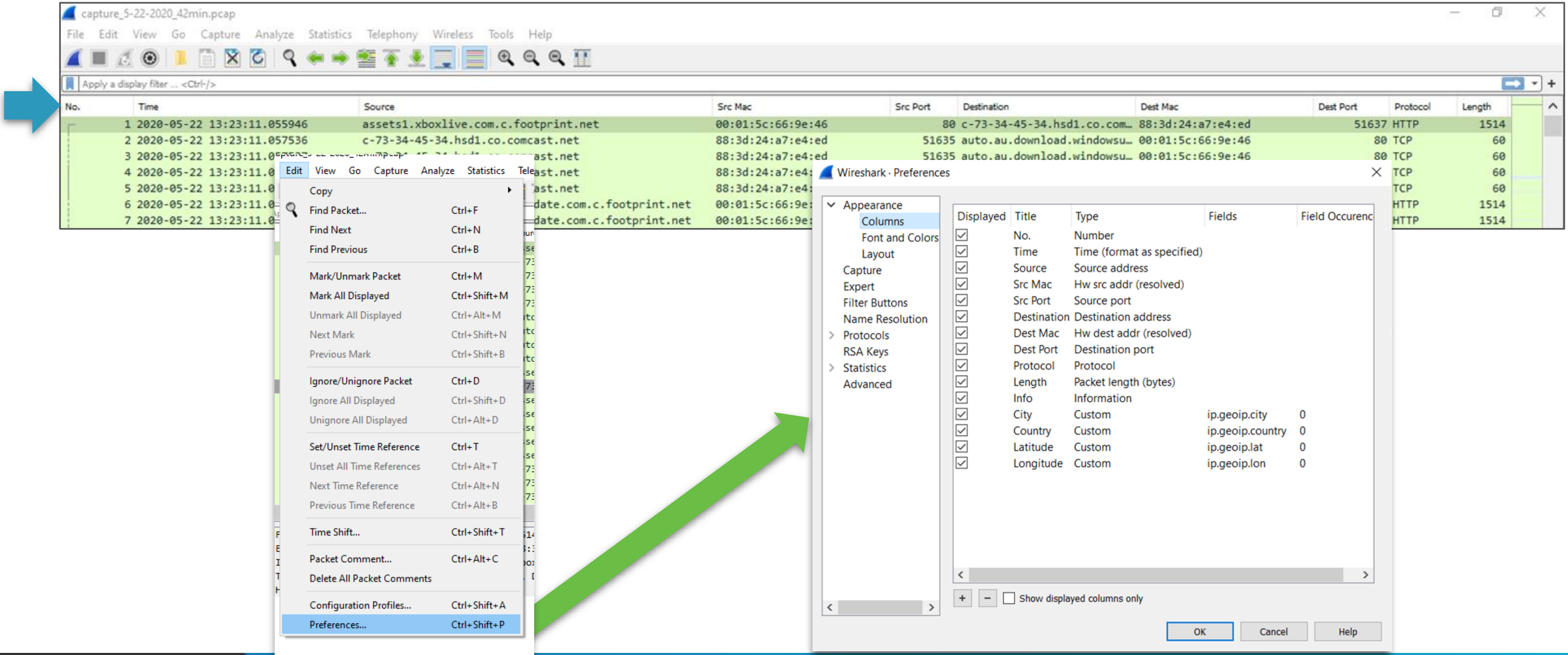
Easy!

Passive!

1G Bandwidth!

Visualizing an Environment (Wireshark)

Wireshark View - WYSIWYG



capture_5-22-2020_42min.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Src Mac	Src Port	Destination	Dest Mac	Dest Port	Protocol	Length
1	2020-05-22 13:23:11.055946	assets1.xboxlive.com.c.footprint.net	00:01:5c:66:9e:46	80	c-73-34-45-34.hsd1.co.com…	88:3d:24:a7:e4:ed	51637	HTTP	1514
2	2020-05-22 13:23:11.057536	c-73-34-45-34.hsd1.co.comcast.net	88:3d:24:a7:e4:ed	51635	auto.au.download.windowsu…	00:01:5c:66:9e:46	80	TCP	60
3	2020-05-22 13:23:11.0	ast.net	88:3d:24:a7:e4:ed	51635	auto.au.download.windowsu…	00:01:5c:66:9e:46	80	TCP	60
4	2020-05-22 13:23:11.0	ast.net	88:3d:24:a7:e4:					TCP	60
5	2020-05-22 13:23:11.0	ast.net	88:3d:24:a7:e4:					TCP	60
6	2020-05-22 13:23:11.0	date.com.c.footprint.net	00:01:5c:66:9e:					HTTP	1514
7	2020-05-22 13:23:11.0	date.com.c.footprint.net	00:01:5c:66:9e:					HTTP	1514

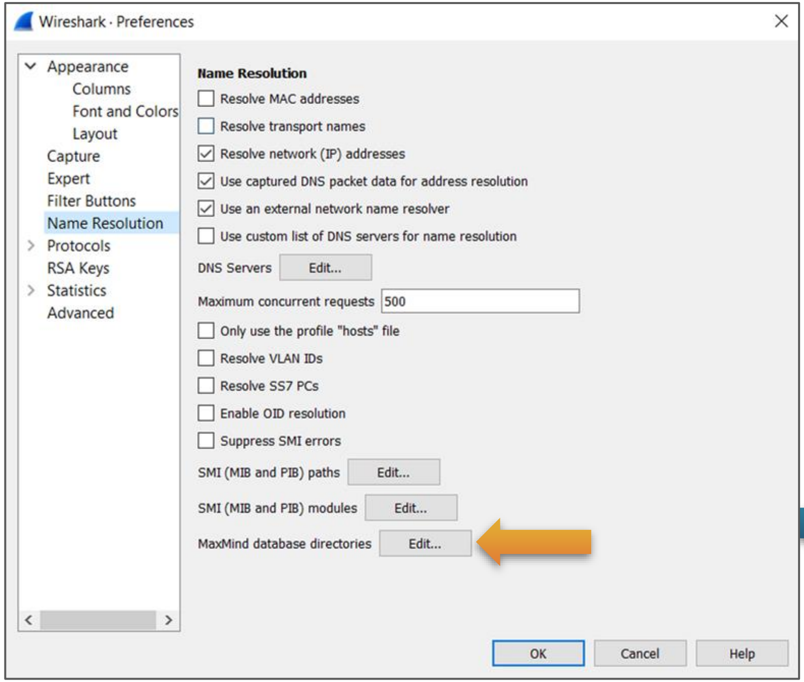
Edit View Go Capture Analyze Statistics Tele
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Packet Ctrl+M
Mark All Displayed Ctrl+Shift+M
Unmark All Displayed Ctrl+Alt+M
Next Mark Ctrl+Shift+N
Previous Mark Ctrl+Shift+B
Ignore/Unignore Packet Ctrl+D
Ignore All Displayed Ctrl+Shift+D
Unignore All Displayed Ctrl+Alt+D
Set/Unset Time Reference Ctrl+T
Unset All Time References Ctrl+Alt+T
Next Time Reference Ctrl+Alt+N
Previous Time Reference Ctrl+Alt+B
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Delete All Packet Comments
Configuration Profiles... Ctrl+Shift+A
Preferences... Ctrl+Shift+P
Wireshark · Preferences
Appearance
Columns
Font and Colors
Layout
Capture
Expert
Filter Buttons
Name Resolution
Protocols
RSA Keys
Statistics
Advanced
+ −
OK
Cancel
Help

Displayed	Title	Type	Fields	Field Occurenc
☑	No.	Number		
☑	Time	Time (format as specified)		
☑	Source	Source address		
☑	Src Mac	Hw src addr (resolved)		
☑	Src Port	Source port		
☑	Destination	Destination address		
☑	Dest Mac	Hw dest addr (resolved)		
☑	Dest Port	Destination port		
☑	Protocol	Protocol		
☑	Length	Packet length (bytes)		
☑	Info	Information		
☑	City	Custom	ip.geoip.city	0
☑	Country	Custom	ip.geoip.country	0
☑	Latitude	Custom	ip.geoip.lat	0
☑	Longitude	Custom	ip.geoip.lon	0

□ Show displayed columns only

Visualizing an Environment (Wireshark and Power BI)

Wireshark Settings / GeoIP



Wireshark · Preferences

- Appearance
  - Columns
  - Font and Colors
  - Layout
- Capture
- Expert
- Filter Buttons
- Name Resolution
- Protocols
- RSA Keys
- Statistics
- Advanced

Name Resolution

- □ Resolve MAC addresses
- □ Resolve transport names
- ☑ Resolve network (IP) addresses
- ☑ Use captured DNS packet data for address resolution
- ☑ Use an external network name resolver
- □ Use custom list of DNS servers for name resolution

DNS Servers [Edit...]

Maximum concurrent requests: 500

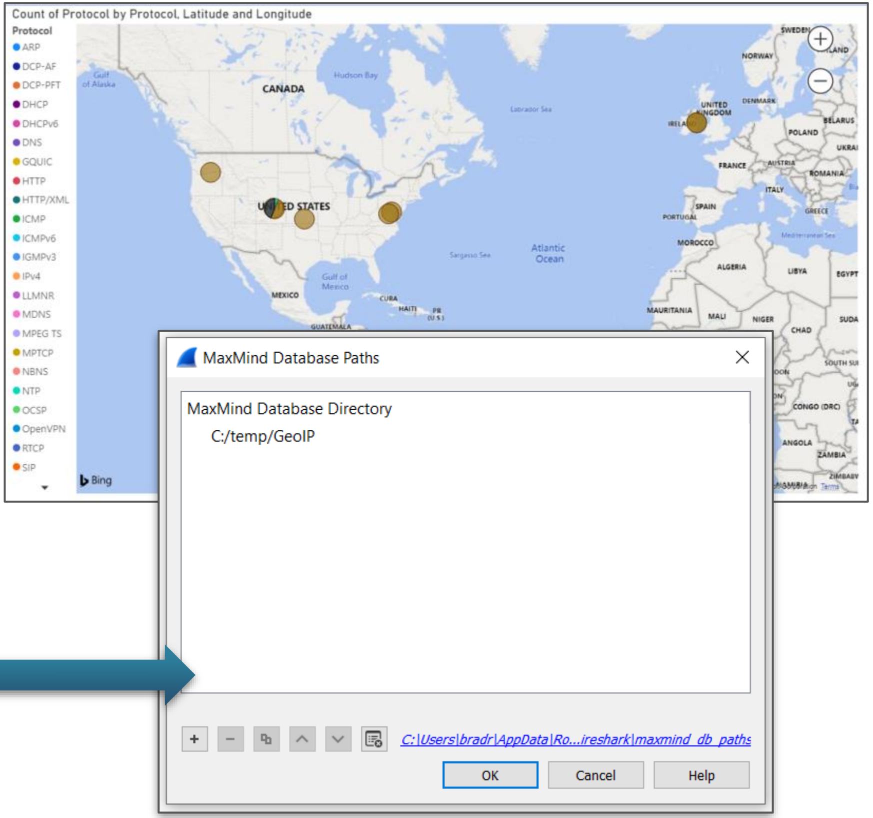
- □ Only use the profile "hosts" file
- □ Resolve VLAN IDs
- □ Resolve SS7 PCs
- □ Enable OID resolution
- □ Suppress SMI errors

SMI (MIB and PIB) paths [Edit...]

SMI (MIB and PIB) modules [Edit...]

MaxMind database directories [Edit...]

[OK] [Cancel] [Help]



Count of Protocol by Protocol, Latitude and Longitude

Protocol: ● ARP ● DCP-AF ● DCP-PFT ● DHCP ● DHCPv6 ● DNS ● GQUIC ● HTTP ● HTTP/XML ● ICMP ● ICMPv6 ● IGMPv3 ● IPv4 ● LLMNR ● MDNS ● MPEG TS ● MPTCP ● NBNS ● NTP ● OCSP ● OpenVPN ● RTCP ● SIP

MaxMind Database Paths

MaxMind Database Directory

C:/temp/GeoIP

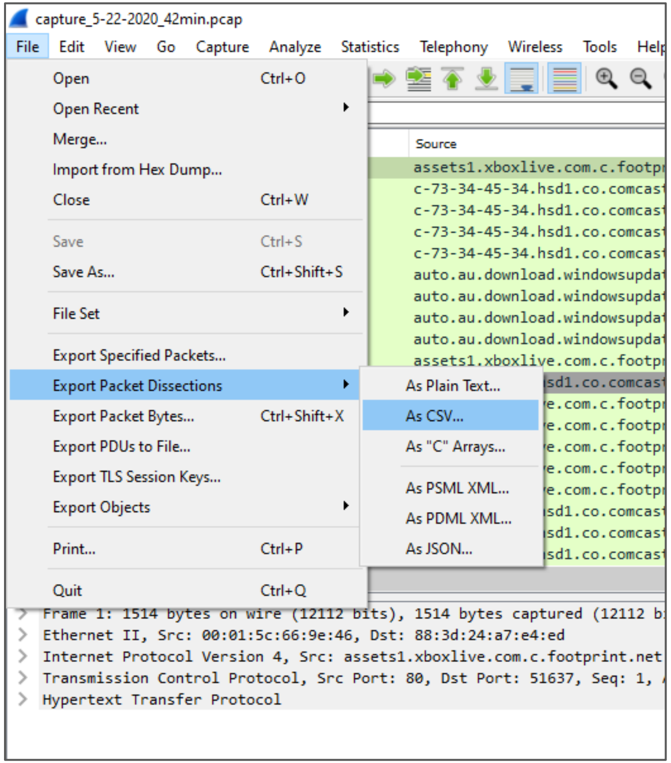
C:\Users\bradr\AppData\Ro...ireshark\maxmind_db_paths

[OK] [Cancel] [Help]

https://www.maxmind.com/en/home

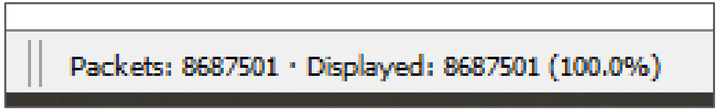
Visualizing an Environment (Wireshark)

Export to CSV

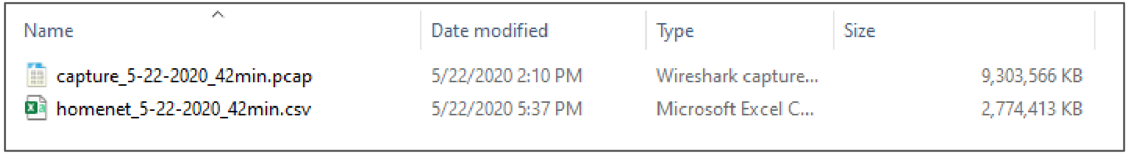


```
assets1.xboxlive.com.c.footpr
c-73-34-45-34.hsd1.co.comcast
c-73-34-45-34.hsd1.co.comcast
c-73-34-45-34.hsd1.co.comcast
c-73-34-45-34.hsd1.co.comcast
auto.au.download.windowsupdat
auto.au.download.windowsupdat
auto.au.download.windowsupdat
auto.au.download.windowsupdat
assets1.xboxlive.com.c.footpr
sd1.co.comcast
e.com.c.footpr
e.com.c.footpr
e.com.c.footpr
e.com.c.footpr
e.com.c.footpr
sd1.co.comcast
sd1.co.comcast
sd1.co.comcast
```

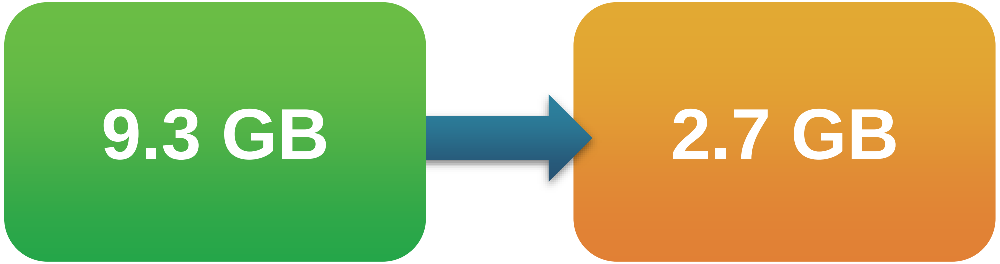
```
> Frame 1: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 b
> Ethernet II, Src: 00:01:5c:66:9e:46, Dst: 88:3d:24:a7:e4:ed
> Internet Protocol Version 4, Src: assets1.xboxlive.com.c.footprint.net
> Transmission Control Protocol, Src Port: 80, Dst Port: 51637, Seq: 1, A
> Hypertext Transfer Protocol
```



```
Packets: 8687501 · Displayed: 8687501 (100.0%)
```



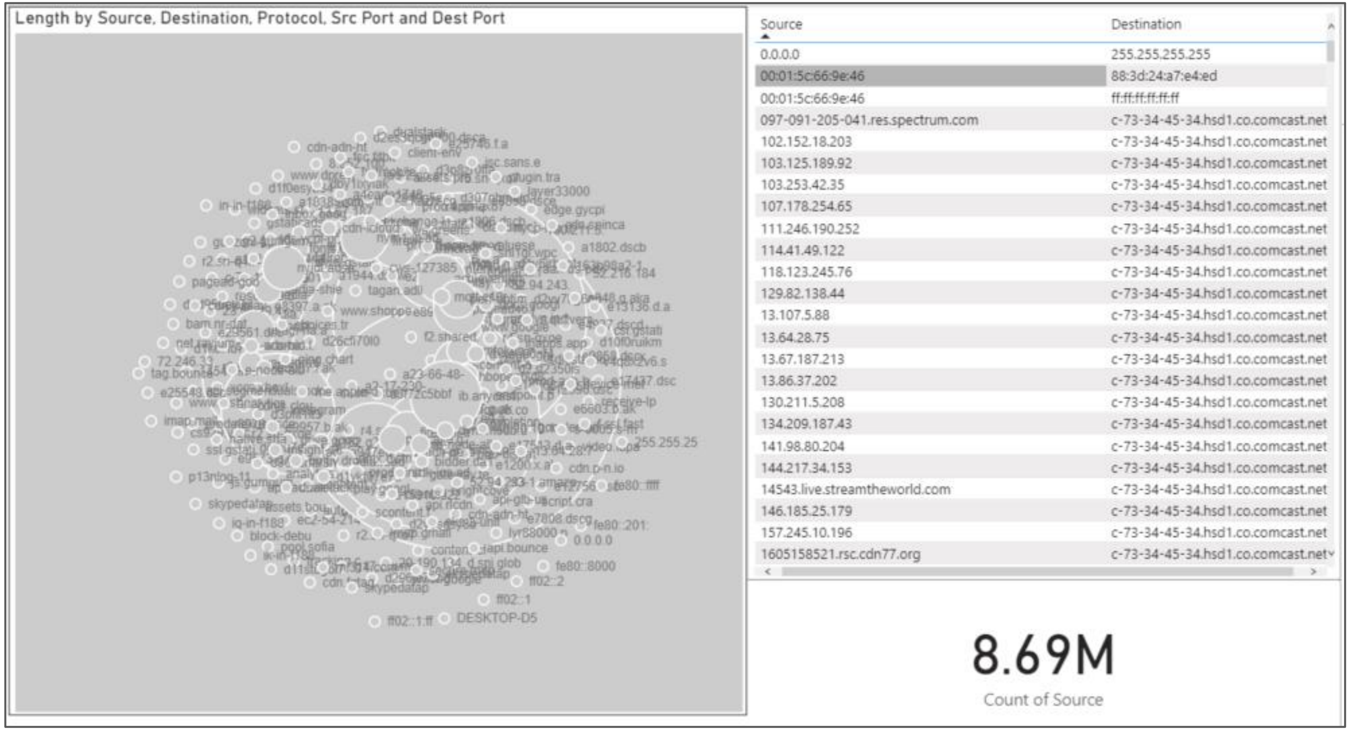
Name	Date modified	Type	Size
capture_5-22-2020_42min.pcap	5/22/2020 2:10 PM	Wireshark capture...	9,303,566 KB
homenet_5-22-2020_42min.csv	5/22/2020 5:37 PM	Microsoft Excel C...	2,774,413 KB



9.3 GB → 2.7 GB

Visualizing an Environment (Power BI)

Network Visualization in Power BI - Why?



Length by Source, Destination, Protocol, Src Port and Dest Port

Source	Destination
0.0.0.0	255.255.255.255
00:01:5c:66:9e:46	88:3d:24:a7:e4:ed
00:01:5c:66:9e:46	ff:ff:ff:ff:ff:ff
097-091-205-041.res.spectrum.com	c-73-34-45-34.hsd1.co.comcast.net
102.152.18.203	c-73-34-45-34.hsd1.co.comcast.net
103.125.189.92	c-73-34-45-34.hsd1.co.comcast.net
103.253.42.35	c-73-34-45-34.hsd1.co.comcast.net
107.178.254.65	c-73-34-45-34.hsd1.co.comcast.net
111.246.190.252	c-73-34-45-34.hsd1.co.comcast.net
114.41.49.122	c-73-34-45-34.hsd1.co.comcast.net
118.123.245.76	c-73-34-45-34.hsd1.co.comcast.net
129.82.138.44	c-73-34-45-34.hsd1.co.comcast.net
13.107.5.88	c-73-34-45-34.hsd1.co.comcast.net
13.64.28.75	c-73-34-45-34.hsd1.co.comcast.net
13.67.187.213	c-73-34-45-34.hsd1.co.comcast.net
13.86.37.202	c-73-34-45-34.hsd1.co.comcast.net
130.211.5.208	c-73-34-45-34.hsd1.co.comcast.net
134.209.187.43	c-73-34-45-34.hsd1.co.comcast.net
141.98.80.204	c-73-34-45-34.hsd1.co.comcast.net
144.217.34.153	c-73-34-45-34.hsd1.co.comcast.net
14543.live.streamtheworld.com	c-73-34-45-34.hsd1.co.comcast.net
146.185.25.179	c-73-34-45-34.hsd1.co.comcast.net
157.245.10.196	c-73-34-45-34.hsd1.co.comcast.net
1605158521.rsc.cdn77.org	c-73-34-45-34.hsd1.co.comcast.net

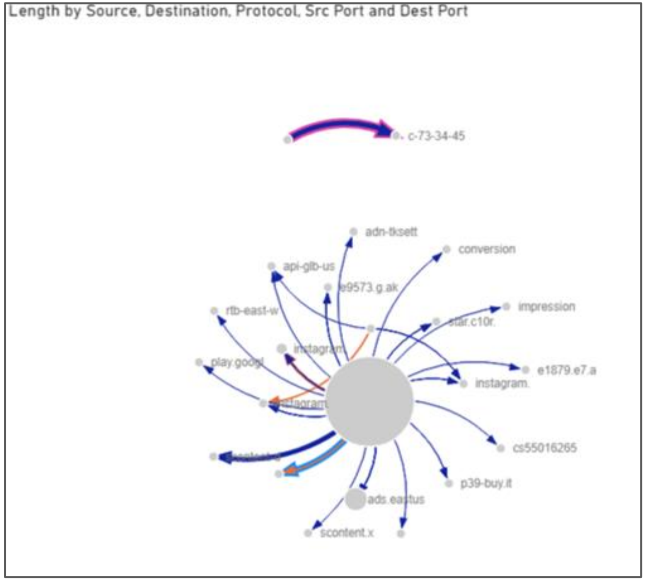
8.69M

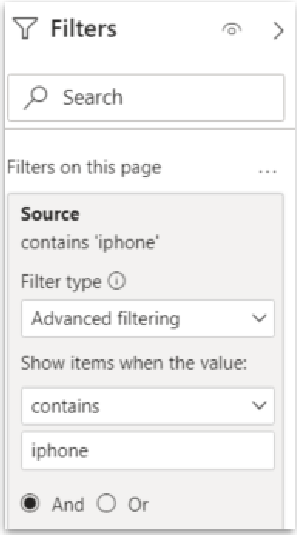
Count of Source

Visualizing an Environment (Power BI)

Network Visualization in Power BI - Why?

- Quickly filter/sort to focus your investigations!




Filters

Search

Filters on this page ...

Source
contains 'iphone'

Filter type ⓘ

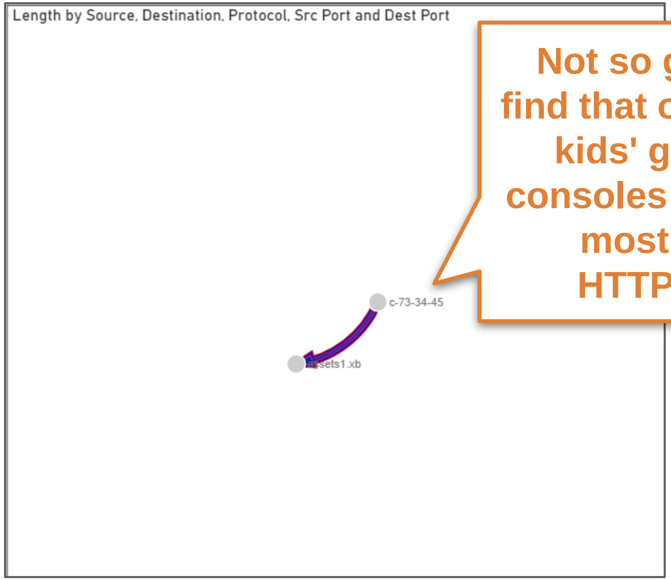
Advanced filtering

Show items when the value:

contains

iphone

● And ○ Or

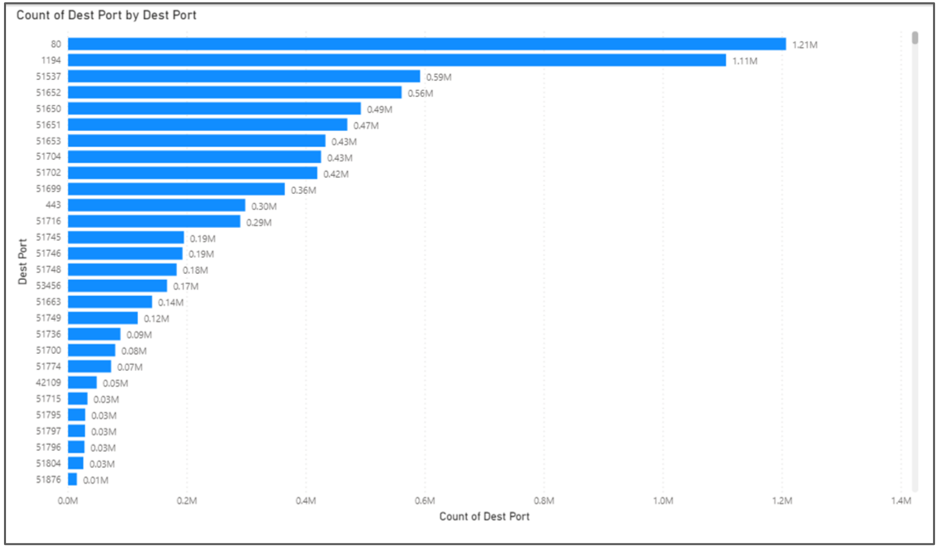

Length by Source, Destination, Protocol, Src Port and Dest Port
c-73-34-45
assets1.xb

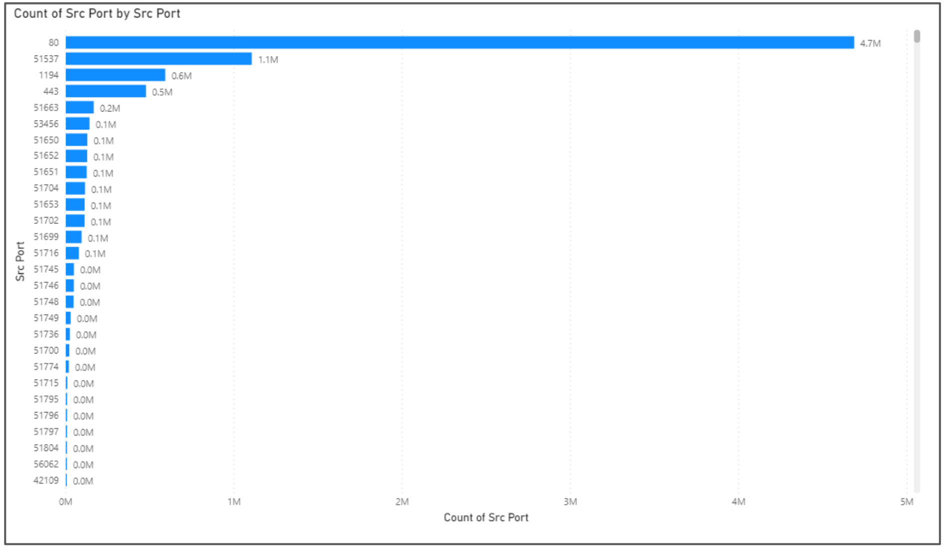
Not so great to find that one of the kids' gaming consoles talks out mostly on HTTP/80...

Visualizing an Environment (Power BI)

Network Visualization in Power BI - why?

- Quickly conduct long tail analysis!





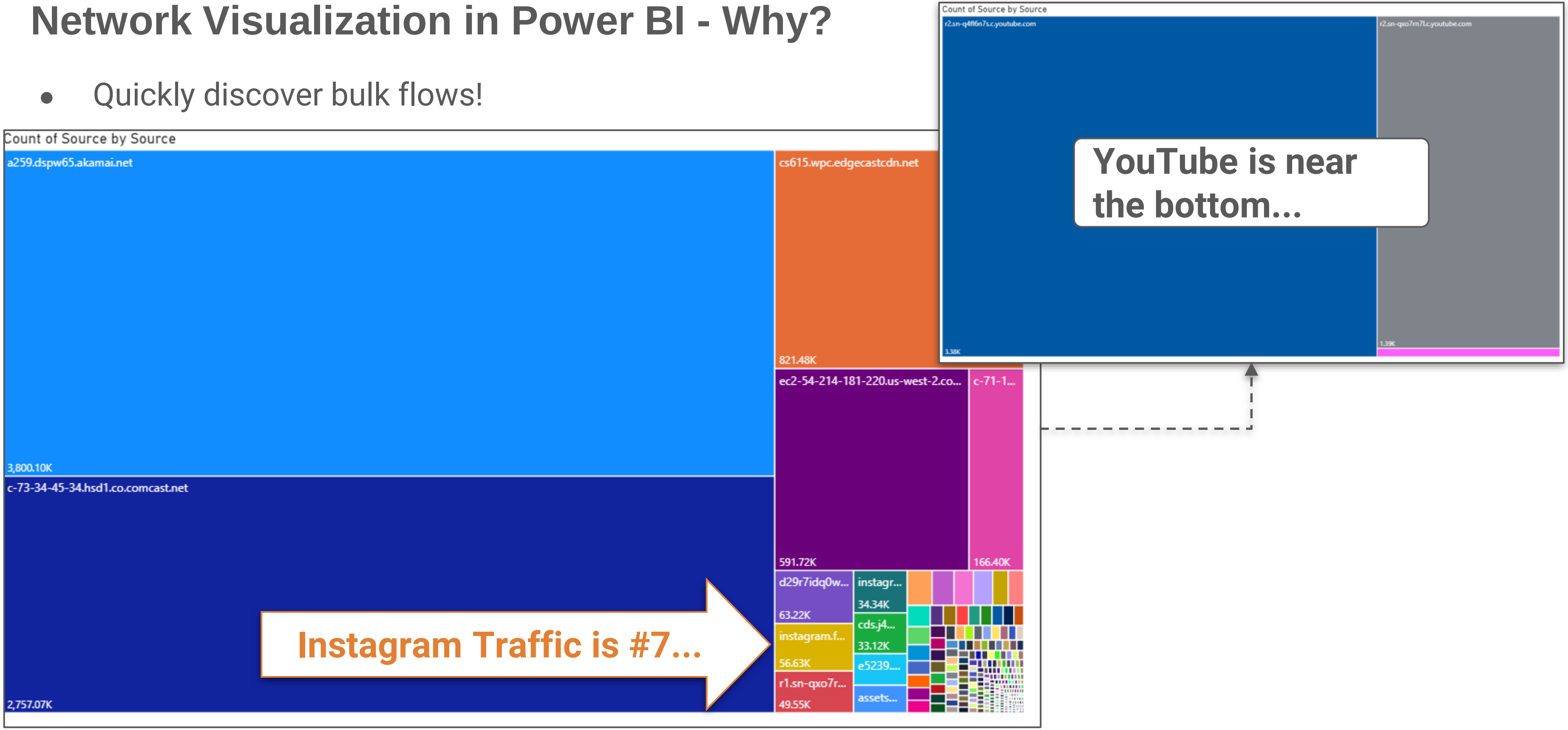
Destination Port

Source Port

Visualizing an Environment (Power BI)

Network Visualization in Power BI - Why?

- Quickly discover bulk flows!


Count of Source by Source
a259.dspw65.akamai.net
3,800.10K
c-73-34-45-34.hsd1.co.comcast.net
2,757.07K
cs615.wpc.edgecastcdn.net
821.48K
ec2-54-214-181-220.us-west-2.co...
591.72K
c-71-1...
166.40K
d29r7idq0w...
63.22K
instagr...
34.34K
cds.j4...
33.12K
instagram.f...
56.63K
e5239....
r1.sn-qxo7r...
49.55K
assets...
Count of Source by Source
r2.sn-q4fl6n7s.c.youtube.com
3.38K
r2.sn-qxo7rn7l.c.youtube.com
1.39K

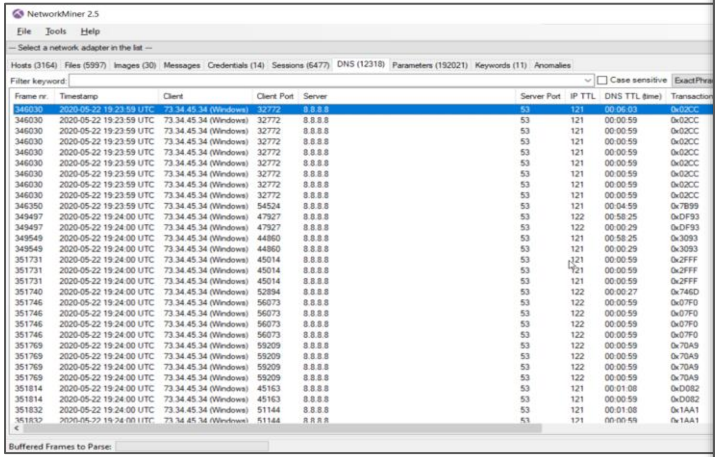
Instagram Traffic is #7...

YouTube is near the bottom...

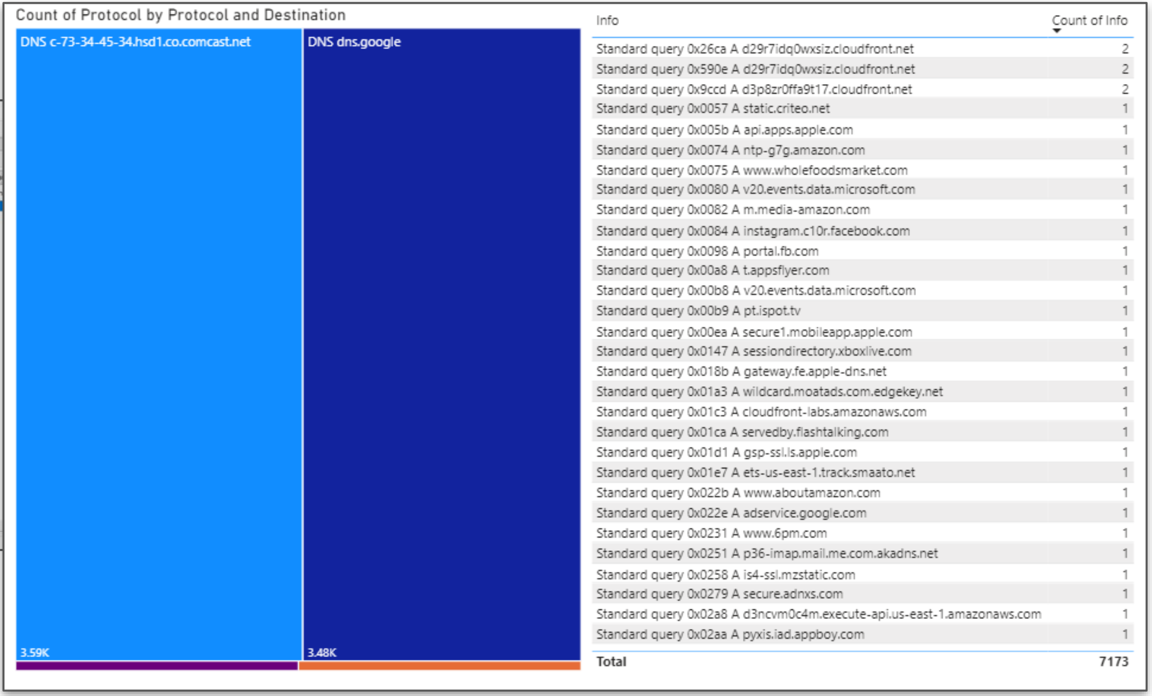
Visualizing an Environment (Power BI)

Network Visualization in Power BI - Why?

- Quickly sort protocols - e.g. DNS!


NetworkMiner 2.5
File Tools Help
— Select a network adapter in the list —
Hosts (3164) Files (5997) Images (30) Messages Credentials (14) Sessions (6477) DNS (12318) Parameters (192021) Keywords (11) Anomalies
Filter keyword:
☐ Case sensitive
ExactPhra
Buffered Frames to Parse:

Frame nr.	Timestamp	Client	Client Port	Server	Server Port	IP TTL	DNS TTL (time)	Transaction
346030	2020-05-22 19:23:59 UTC	73.34.45.34 (Windows)	32772	8.8.8.8	53	121	00:06:03	0x02CC
346030	2020-05-22 19:23:59 UTC	73.34.45.34 (Windows)	32772	8.8.8.8	53	121	00:00:59	0x02CC
346030	2020-05-22 19:23:59 UTC	73.34.45.34 (Windows)	32772	8.8.8.8	53	121	00:00:59	0x02CC
346030	2020-05-22 19:23:59 UTC	73.34.45.34 (Windows)	32772	8.8.8.8	53	121	00:00:59	0x02CC
346030	2020-05-22 19:23:59 UTC	73.34.45.34 (Windows)	32772	8.8.8.8	53	121	00:00:59	0x02CC
346030	2020-05-22 19:23:59 UTC	73.34.45.34 (Windows)	32772	8.8.8.8	53	121	00:00:59	0x02CC
346030	2020-05-22 19:23:59 UTC	73.34.45.34 (Windows)	32772	8.8.8.8	53	121	00:00:59	0x02CC
346030	2020-05-22 19:23:59 UTC	73.34.45.34 (Windows)	32772	8.8.8.8	53	121	00:00:59	0x02CC
346030	2020-05-22 19:23:59 UTC	73.34.45.34 (Windows)	32772	8.8.8.8	53	121	00:00:59	0x02CC
346350	2020-05-22 19:23:59 UTC	73.34.45.34 (Windows)	54524	8.8.8.8	53	121	00:04:59	0x7B99
349497	2020-05-22 19:24:00 UTC	73.34.45.34 (Windows)	47927	8.8.8.8	53	122	00:58:25	0xDF93
349497	2020-05-22 19:24:00 UTC	73.34.45.34 (Windows)	47927	8.8.8.8	53	122	00:00:29	0xDF93
349549	2020-05-22 19:24:00 UTC	73.34.45.34 (Windows)	44860	8.8.8.8	53	121	00:58:25	0x3093
349549	2020-05-22 19:24:00 UTC	73.34.45.34 (Windows)	44860	8.8.8.8	53	121	00:00:29	0x3093
351731	2020-05-22 19:24:00 UTC	73.34.45.34 (Windows)	45014	8.8.8.8	53	121	00:00:59	0x2FFF
351731	2020-05-22 19:24:00 UTC	73.34.45.34 (Windows)	45014	8.8.8.8	53	121	00:00:59	0x2FFF
351731	2020-05-22 19:24:00 UTC	73.34.45.34 (Windows)	45014	8.8.8.8	53	121	00:00:59	0x2FFF
351740	2020-05-22 19:24:00 UTC	73.34.45.34 (Windows)	52894	8.8.8.8	53	122	00:00:27	0x746D
351746	2020-05-22 19:24:00 UTC	73.34.45.34 (Windows)	56073	8.8.8.8	53	122	00:00:59	0x07F0
351746	2020-05-22 19:24:00 UTC	73.34.45.34 (Windows)	56073	8.8.8.8	53	122	00:00:59	0x07F0
351746	2020-05-22 19:24:00 UTC	73.34.45.34 (Windows)	56073	8.8.8.8	53	122	00:00:59	0x07F0
351746	2020-05-22 19:24:00 UTC	73.34.45.34 (Windows)	56073	8.8.8.8	53	122	00:00:59	0x07F0
351769	2020-05-22 19:24:00 UTC	73.34.45.34 (Windows)	59209	8.8.8.8	53	122	00:00:59	0x70A9
351769	2020-05-22 19:24:00 UTC	73.34.45.34 (Windows)	59209	8.8.8.8	53	122	00:00:59	0x70A9
351769	2020-05-22 19:24:00 UTC	73.34.45.34 (Windows)	59209	8.8.8.8	53	122	00:00:59	0x70A9
351769	2020-05-22 19:24:00 UTC	73.34.45.34 (Windows)	59209	8.8.8.8	53	122	00:00:59	0x70A9
351814	2020-05-22 19:24:00 UTC	73.34.45.34 (Windows)	45163	8.8.8.8	53	121	00:01:08	0xD082
351814	2020-05-22 19:24:00 UTC	73.34.45.34 (Windows)	45163	8.8.8.8	53	121	00:00:59	0xD082
351832	2020-05-22 19:24:00 UTC	73.34.45.34 (Windows)	51144	8.8.8.8	53	121	00:01:08	0x1AA1
351832	2020-05-22 19:24:00 UTC	73.34.45.34 (Windows)	51144	8.8.8.8	53	121	00:00:59	0x1AA1


Count of Protocol by Protocol and Destination
DNS c-73-34-45-34.hsd1.co.comcast.net
DNS dns.google
3.59K
3.48K

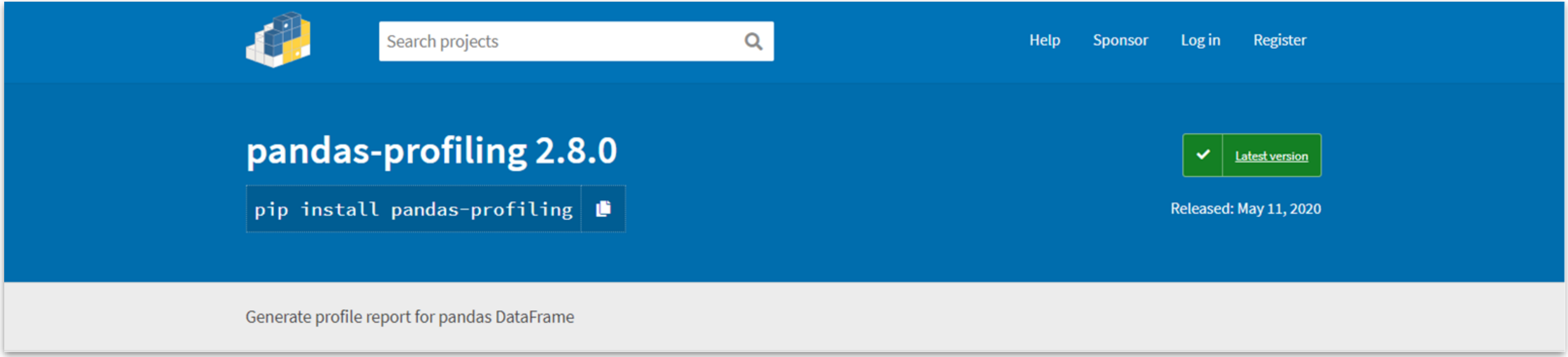
Info	Count of Info
Standard query 0x26ca A d29r7idq0wxsiz.cloudfront.net	2
Standard query 0x590e A d29r7idq0wxsiz.cloudfront.net	2
Standard query 0x9ccd A d3p8zr0ffa9t17.cloudfront.net	2
Standard query 0x0057 A static.criteo.net	1
Standard query 0x005b A api.apps.apple.com	1
Standard query 0x0074 A ntp-g7g.amazon.com	1
Standard query 0x0075 A www.wholefoodsmarket.com	1
Standard query 0x0080 A v20.events.data.microsoft.com	1
Standard query 0x0082 A m.media-amazon.com	1
Standard query 0x0084 A instagram.c10r.facebook.com	1
Standard query 0x0098 A portal.fb.com	1
Standard query 0x00a8 A t.appsflyer.com	1
Standard query 0x00b8 A v20.events.data.microsoft.com	1
Standard query 0x00b9 A pt.ispot.tv	1
Standard query 0x00ea A secure1.mobileapp.apple.com	1
Standard query 0x0147 A sessiondirectory.xboxlive.com	1
Standard query 0x018b A gateway.fe.apple-dns.net	1
Standard query 0x01a3 A wildcard.moatads.com.edgekey.net	1
Standard query 0x01c3 A cloudfront-labs.amazonaws.com	1
Standard query 0x01ca A servedby.flashtalking.com	1
Standard query 0x01d1 A gsp-ssl.ls.apple.com	1
Standard query 0x01e7 A ets-us-east-1.track.smaato.net	1
Standard query 0x022b A www.aboutamazon.com	1
Standard query 0x022e A adservice.google.com	1
Standard query 0x0231 A www.6pm.com	1
Standard query 0x0251 A p36-imap.mail.me.com.akadns.net	1
Standard query 0x0258 A is4-ssl.mzstatic.com	1
Standard query 0x0279 A secure.adnxs.com	1
Standard query 0x02a8 A d3ncvm0c4m.execute-api.us-east-1.amazonaws.com	1
Standard query 0x02aa A pyxis.iad.appboy.com	1
Total	**7173**

Let’s see it live...

A “PCAP” of badness (what do we find) using Power BI & Tableau Public

Introducing Pandas Profiling

- Automated & quick data analysis using Pandas!
- https://github.com/pandas-profiling/pandas-profiling
- https://pypi.org/project/pandas-profiling/



pandas-profiling 2.8.0

```
pip install pandas-profiling
```

Released: May 11, 2020

Generate profile report for pandas DataFrame

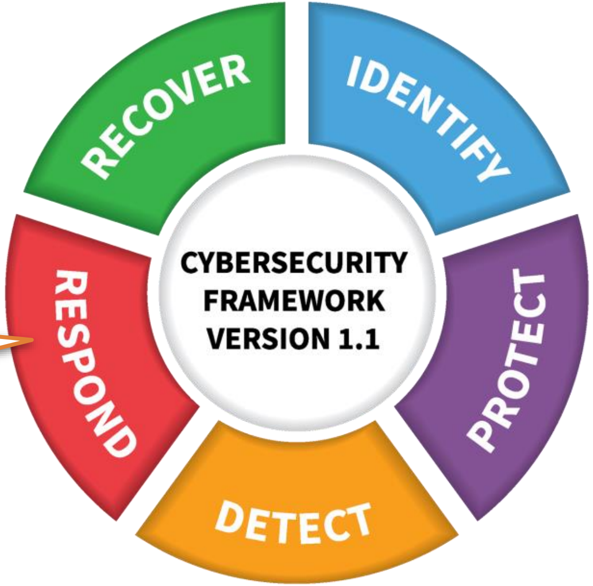
Let’s see it live...

A “PCAP” of badness (what do we quickly find) using Pandas Profiling

Windows Logs Analysis with Power BI (for IR)

- Process...
  - Ingest the Windows Log
  - Export CSV
  - Ingest into Power BI
  - Given a LOG with evil — Where is it?
  - But first...

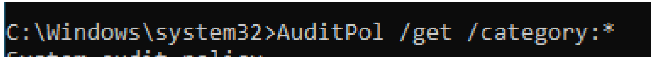
We Are HERE!



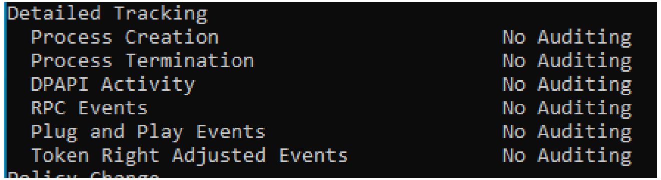
https://www.nist.gov/cyberframework

Windows Logs Analysis with Power BI (for IR)

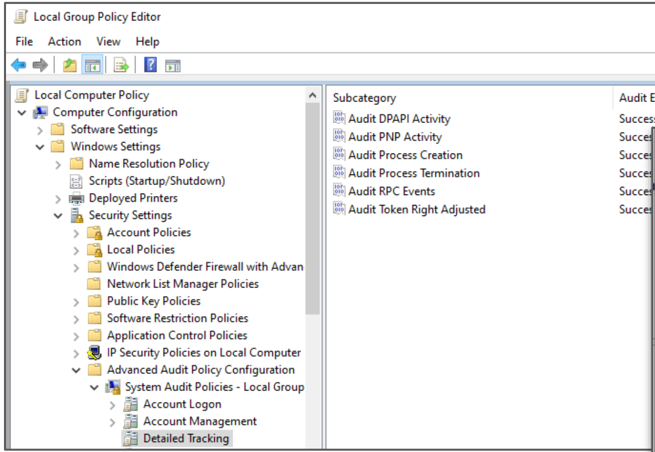
- Hopefully, you’re doing good Windows Logging!?
- At a minimum, turn on detailed tracking...
- And command line logging via GPO!



```
C:\Windows\system32>AuditPol /get /category:*
System audit policy
```

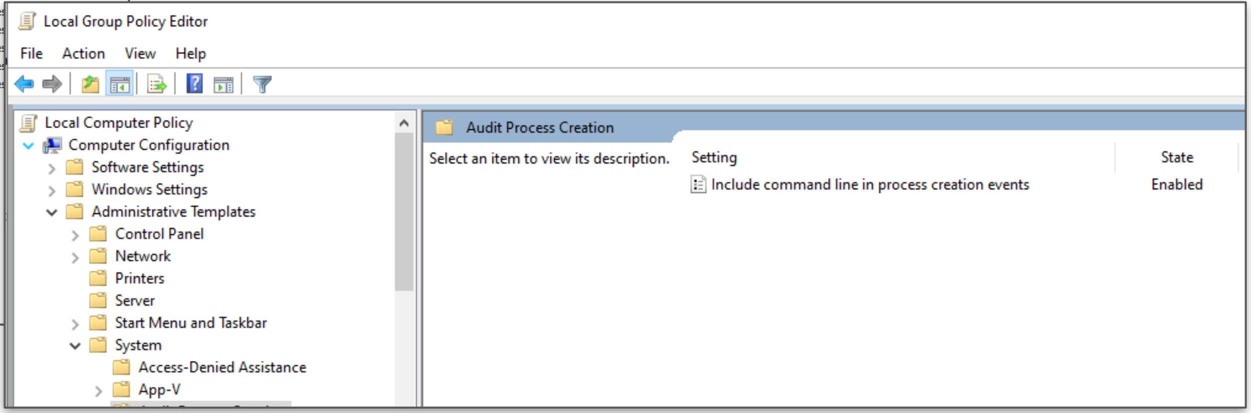


```
Detailed Tracking
  Process Creation                          No Auditing
  Process Termination                       No Auditing
  DPAPI Activity                            No Auditing
  RPC Events                                No Auditing
  Plug and Play Events                      No Auditing
  Token Right Adjusted Events               No Auditing
Policy Change
```



- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
        - Windows Defender Firewall with Advan
        - Network List Manager Policies
        - Public Key Policies
        - Software Restriction Policies
        - Application Control Policies
        - IP Security Policies on Local Computer
        - Advanced Audit Policy Configuration
          - System Audit Policies - Local Group
            - Account Logon
            - Account Management
            - Detailed Tracking

Subcategory	Audit Events
Audit DPAPI Activity	Success and Failure
Audit PNP Activity	Succes
Audit Process Creation	Succes
Audit Process Termination	Succes
Audit RPC Events	Succes
Audit Token Right Adjusted	Succes



- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Control Panel
      - Network
      - Printers
      - Server
      - Start Menu and Taskbar
      - System
        - Access-Denied Assistance
        - App-V

Audit Process Creation

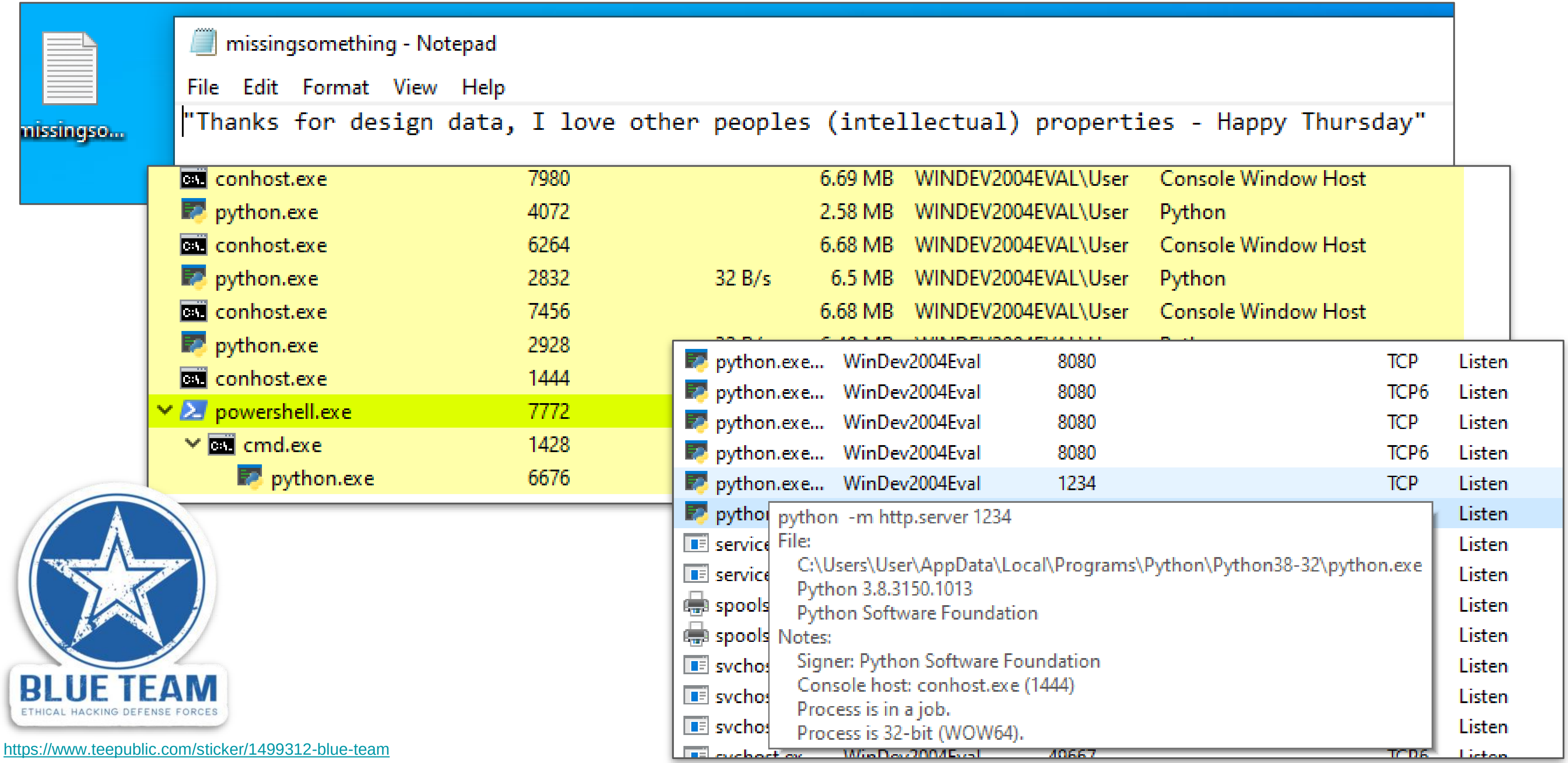
Select an item to view its description.

Setting	State
Include command line in process creation events	Enabled

https://www.itprotoday.com/strategy/understanding-and-enabling-command-line-auditing

https://www.malwarearchaeology.com/cheat-sheets

Windows Logs Analysis with Power BI (for IR)



missingso...

missingsomething - Notepad

```
"Thanks for design data, I love other peoples (intellectual) properties - Happy Thursday"
```

```
conhost.exe        7980              6.69 MB  WINDEV2004EVAL\User  Console Window Host
python.exe         4072              2.58 MB  WINDEV2004EVAL\User  Python
conhost.exe        6264              6.68 MB  WINDEV2004EVAL\User  Console Window Host
python.exe         2832   32 B/s     6.5 MB   WINDEV2004EVAL\User  Python
conhost.exe        7456              6.68 MB  WINDEV2004EVAL\User  Console Window Host
python.exe         2928
conhost.exe        1444
powershell.exe     7772
  cmd.exe          1428
    python.exe     6676
```

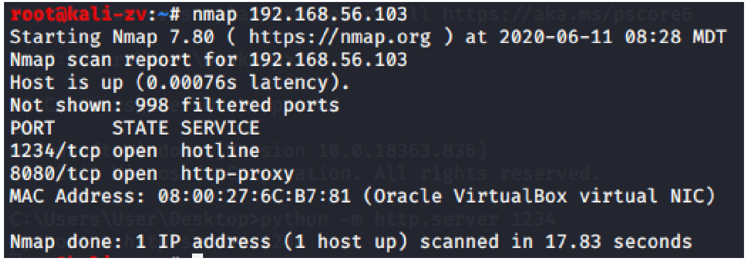
```
python.exe...  WinDev2004Eval  8080   TCP   Listen
python.exe...  WinDev2004Eval  8080   TCP6  Listen
python.exe...  WinDev2004Eval  8080   TCP   Listen
python.exe...  WinDev2004Eval  8080   TCP6  Listen
python.exe...  WinDev2004Eval  1234   TCP   Listen
pytho                                       Listen
service                                     Listen
service                                     Listen
spools                                      Listen
spools                                      Listen
svcho                                       Listen
svcho                                       Listen
svcho                                       Listen
svchost.ex...  WinDev2004Eval  49667  TCP6  Listen
```

```
python  -m http.server 1234
File:
   C:\Users\User\AppData\Local\Programs\Python\Python38-32\python.exe
   Python 3.8.3150.1013
   Python Software Foundation
Notes:
   Signer: Python Software Foundation
   Console host: conhost.exe (1444)
   Process is in a job.
   Process is 32-bit (WOW64).
```

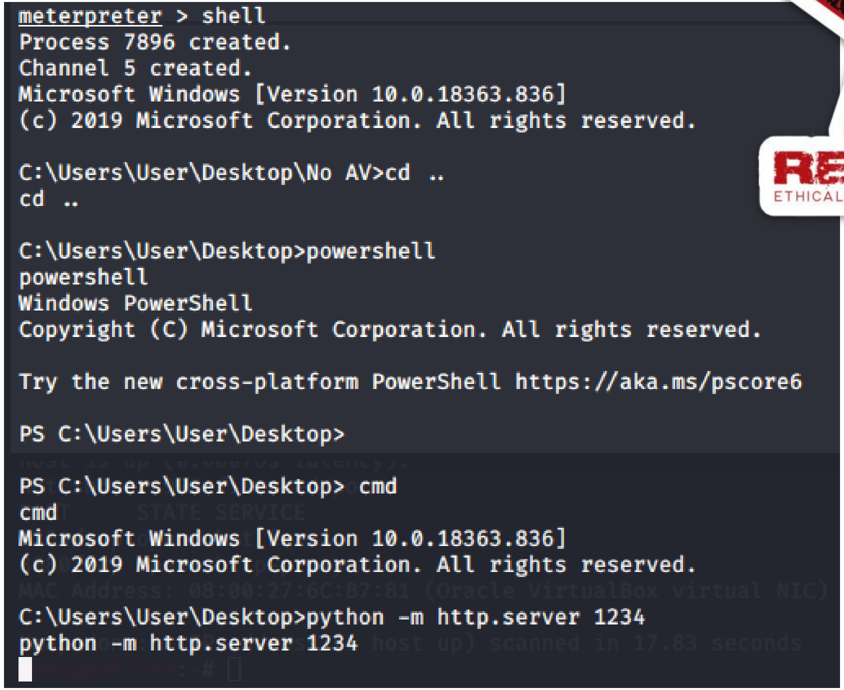
BLUE TEAM
ETHICAL HACKING DEFENSE FORCES

https://www.teepublic.com/sticker/1499312-blue-team

Windows Logs Analysis with Power BI (for IR)

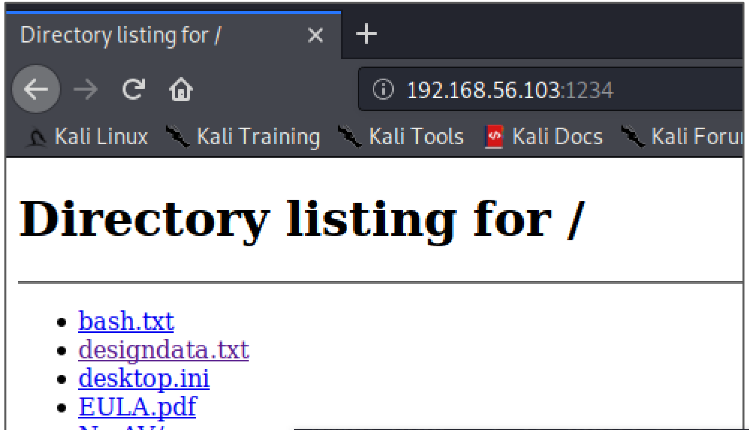


```
root@kali-zv:~# nmap 192.168.56.103
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-11 08:28 MDT
Nmap scan report for 192.168.56.103
Host is up (0.00076s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
1234/tcp open  hotline
8080/tcp open  http-proxy
MAC Address: 08:00:27:6C:B7:81 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 17.83 seconds
```



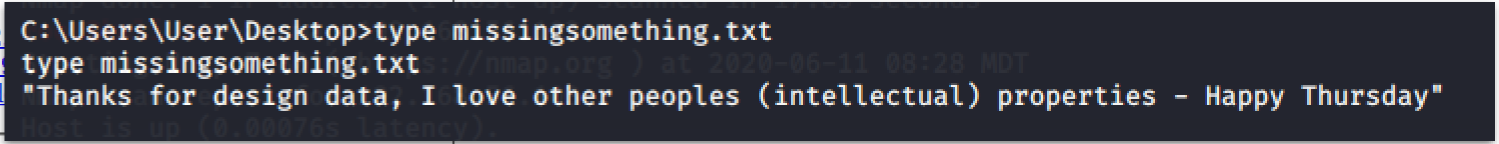
```
meterpreter > shell
Process 7896 created.
Channel 5 created.
Microsoft Windows [Version 10.0.18363.836]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\User\Desktop\No AV>cd ..
cd ..

C:\Users\User\Desktop>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\User\Desktop>

PS C:\Users\User\Desktop> cmd
cmd
Microsoft Windows [Version 10.0.18363.836]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\User\Desktop>python -m http.server 1234
python -m http.server 1234
```

https://www.teepublic.com/sticker/1499286-red-team



Directory listing for /

- bash.txt
- designdata.txt
- desktop.ini
- EULA.pdf
- No AV/
- Process Hacker 2
- Visual Studio 201
- Visual Studio Cod



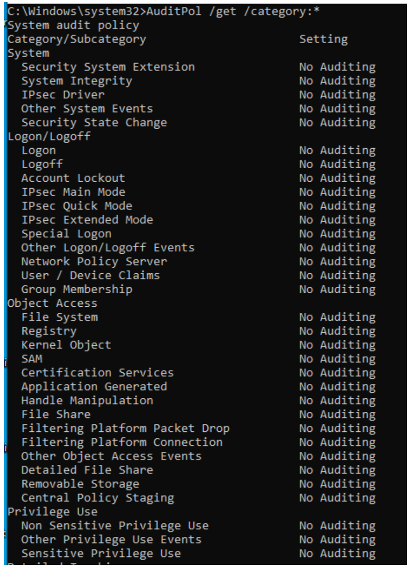
```
C:\Users\User\Desktop>type missingsomething.txt
type missingsomething.txt
"Thanks for design data, I love other peoples (intellectual) properties - Happy Thursday"
```

Let’s see it live...

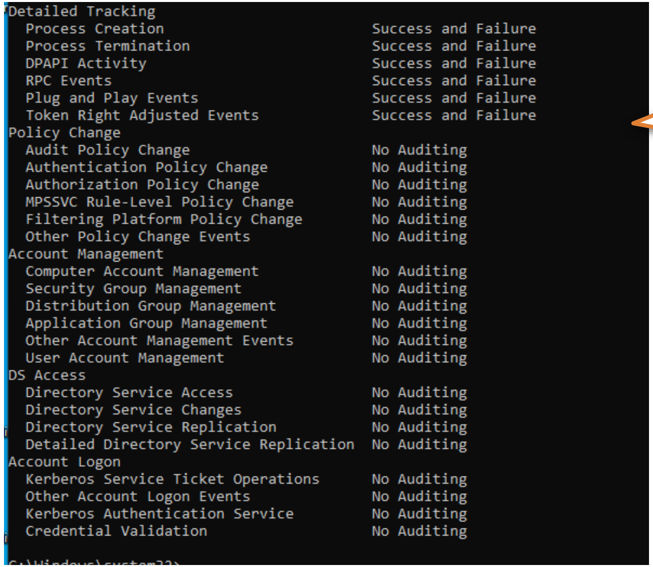
Quick Windows Log Analysis in Power BI

Windows Logs Analysis with Power BI (for IR)

- Windows Security Events you should **always** care about:
    - 4688 - Process Creation
    - 4689 - Process Exit
- Know your networks, systems, data, users!



```
C:\Windows\system32>AuditPol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        No Auditing
  IPsec Driver                            No Auditing
  Other System Events                     No Auditing
  Security State Change                   No Auditing
Logon/Logoff
  Logon                                   No Auditing
  Logoff                                  No Auditing
  Account Lockout                         No Auditing
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
  Special Logon                           No Auditing
  Other Logon/Logoff Events               No Auditing
  Network Policy Server                   No Auditing
  User / Device Claims                    No Auditing
  Group Membership                        No Auditing
Object Access
  File System                             No Auditing
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
  Removable Storage                       No Auditing
  Central Policy Staging                  No Auditing
Privilege Use
  Non Sensitive Privilege Use             No Auditing
  Other Privilege Use Events              No Auditing
  Sensitive Privilege Use                 No Auditing
Detailed Tracking
```



```
Detailed Tracking
  Process Creation                        Success and Failure
  Process Termination                     Success and Failure
  DPAPI Activity                          Success and Failure
  RPC Events                              Success and Failure
  Plug and Play Events                    Success and Failure
  Token Right Adjusted Events             Success and Failure
Policy Change
  Audit Policy Change                     No Auditing
  Authentication Policy Change            No Auditing
  Authorization Policy Change             No Auditing
  MPSSVC Rule-Level Policy Change         No Auditing
  Filtering Platform Policy Change        No Auditing
  Other Policy Change Events              No Auditing
Account Management
  Computer Account Management             No Auditing
  Security Group Management               No Auditing
  Distribution Group Management           No Auditing
  Application Group Management            No Auditing
  Other Account Management Events         No Auditing
  User Account Management                 No Auditing
DS Access
  Directory Service Access                No Auditing
  Directory Service Changes               No Auditing
  Directory Service Replication           No Auditing
  Detailed Directory Service Replication  No Auditing
Account Logon
  Kerberos Service Ticket Operations      No Auditing
  Other Account Logon Events              No Auditing
  Kerberos Authentication Service         No Auditing
  Credential Validation                   No Auditing

C:\Windows\system32>
```

Turn on more logging...or you'll miss stuff!

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/

Lab Time

BIG
DATA
ALSO
TOOLS
DISK
TARGET
CONNECTOMICS
ORGANIZATIONS
SET
USE
RELATIONAL
LARGER
CONTINUES
SOCIAL
INDEXING
TENS
COMPLEX
CITATION
ANALYTICS
USED
CREATED
NOW
BIOLOGICAL
PROCESSING
UBIQUITOUS
CAPACITY
BURIED
WORLD'S
HUNDREDS
DESKTOP
NETWORKS
DATABASES
RECORDS
SEARCH
SOLID
TYPES
CURRENTLY
GARTNER
WORKING
AMOUNT
OPPORTUNITIES
EVERY
EXAMPLES
APPLIED
SENSOR
SHARED
DEFINITION
CURRENT
MAY
MOVING
WIRELESS
MANAGE
RECONSIDER
WITHIN
ARCHIVES
BIOGEOCHEMICAL
ZETTABYTES
PRACTITIONERS
CAPTURE
THOUGHT
TECHNOLOGIES
USING
INTERNET
DISTRIBUTED
BUSINESS
SETS
GENOMICS
COMPLEXITY
DESCRIBING
RADIO-FREQUENCY
NEEDED
REQUIRING
TIME
INFORMATION
ONE
LARGE
MANAGEMENT
TERABYTES
CASE
ABILITY
SOFTWARE
PROCESS
PETABYTES
INCLUDE
IT
PERFORMANCE
PRESENTATIONS
STORE
ELAPSED
SYSTEMS
TOLERABLE
SIZE
RESEARCH
COMBAT
FORMS
STORAGE
MPP
LOGS
COST
SIGNIFICANT
DEFINING
RELATED
COMPUTING
SAN
QUALITIES
SINCE
PARALLEL
MASSIVELY
GROW
DIFFICULTY

Downloads & Install

Time: (allotted) 30 mins, varies depending on your internet connection

- Wireshark: https://www.wireshark.org/download.html
- Microsoft Power BI Desktop (Windows-only): https://powerbi.microsoft.com/en-us/desktop/
  - ✓ Note: this link will open the embedded Microsoft Store application
- Tableau Public (Windows, Mac): https://public.tableau.com/en-us/s/
  - ✓ Note: this download requests an email to download
- MaxMind GeoIP Database (optional): https://dev.maxmind.com/geoip/geoip2/geolite2/
  - ✓ Note: this download requires you establish an account

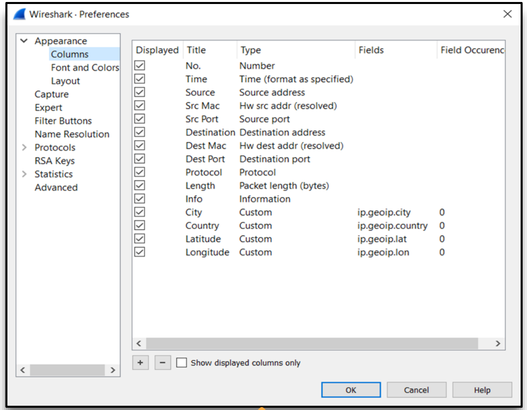
Collection, Formatting, Export

Time: (allotted) 20 mins

WIRESHARK

Run as Admin!
Why?
Promiscuous Mode

Open your fav browser! Spin up ~20 tabs!



Displayed	Title	Type	Fields	Field Occurenc
☑	No.	Number		
☑	Time	Time (format as specified)		
☑	Source	Source address		
☑	Src Mac	Hw src addr (resolved)		
☑	Src Port	Source port		
☑	Destination	Destination address		
☑	Dest Mac	Hw dest addr (resolved)		
☑	Dest Port	Destination port		
☑	Protocol	Protocol		
☑	Length	Packet length (bytes)		
☑	Info	Information		
☑	City	Custom	ip.geoip.city	0
☑	Country	Custom	ip.geoip.country	0
☑	Latitude	Custom	ip.geoip.lat	0
☑	Longitude	Custom	ip.geoip.lon	0

□ Show displayed columns only

Collect using Wireshark for ~10 mins
Add additional columns!

CSV

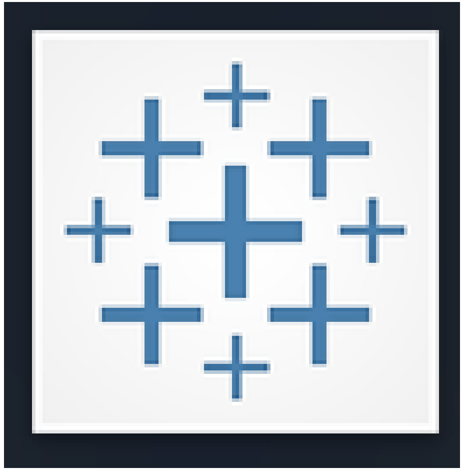
Export to CSV!

Analysis

Time: (allotted) 30 mins

Link for more visuals (assumes you have a Microsoft account): https://appsource.microsoft.com/en-us/marketplace/apps?product=power-bi-visuals

OR



Discovery Ops!

Discovery Ops!

Share?

Time: (allotted) 20 mins

Thank you AvengerCon for this opportunity to present!!

Questions?

Contact Details:

Civilian: brhodes@zvelo.com

Military: brad.e.rhodes.mil@mail.mil

MCPA: brad.rhodes@milcyber.org

LinkedIn: https://www.linkedin.com/in/brad-rhodes-1951ba7/

GitHub: https://github.com/cyberguy514?tab=repositories

Twitter: @cyber514