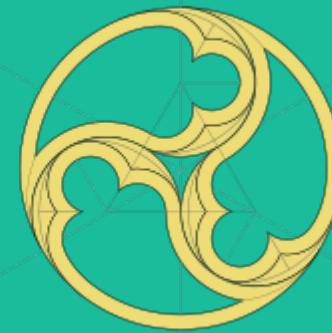


Network Traffic Analysis with

Malcolm



<https://github.com/idaholab/Malcolm>

Malcolm

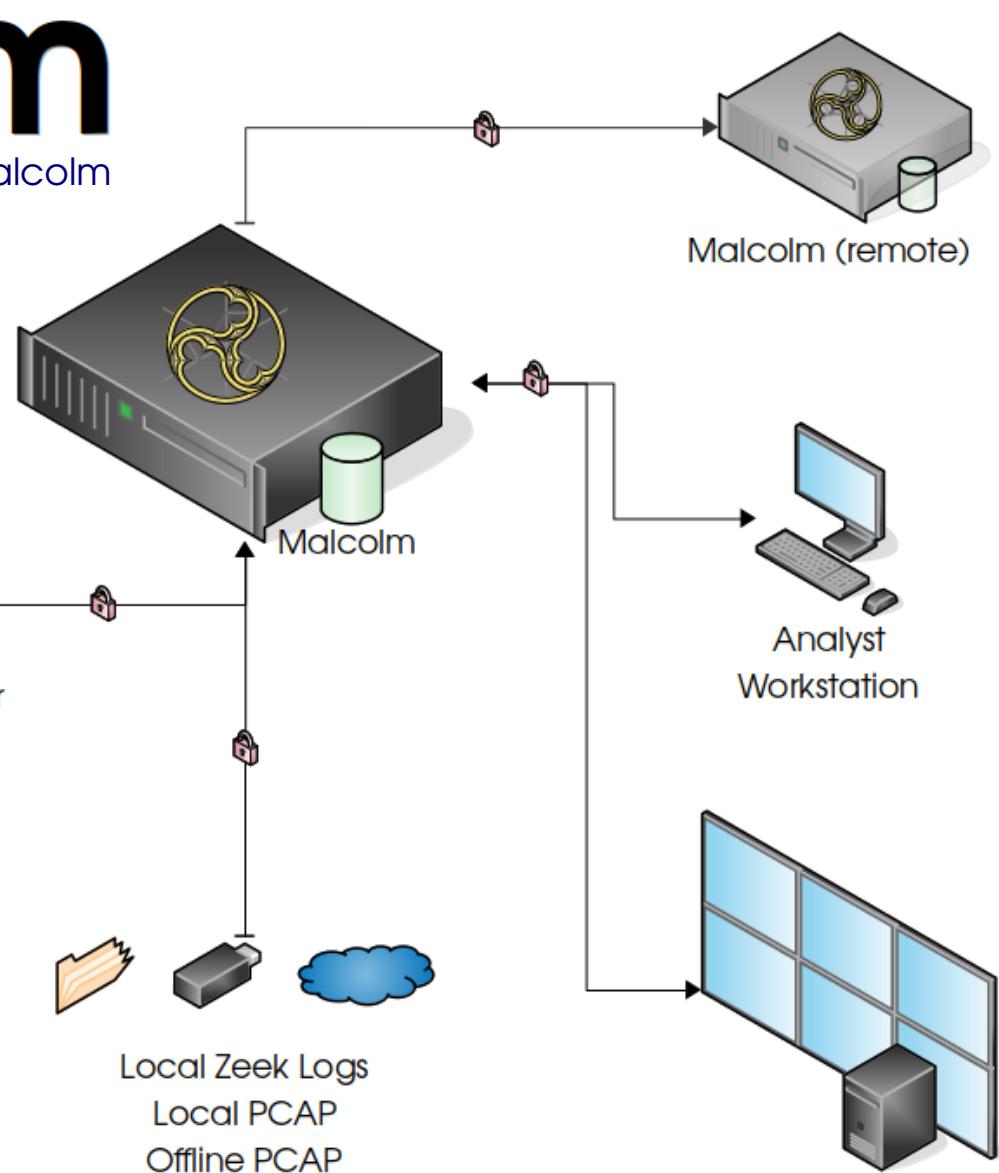
<https://github.com/idaholab/Malcolm>



Switch SPAN Port
or Network TAP



Sensor



Malcolm is a powerful, easily deployable network traffic analysis tool suite for full packet capture artifacts (PCAP files) and Zeek logs.

Malcolm leverages industry-standard open source tools, including:



... and more!

Supported Protocols

Link and Internet Layers

Border Gateway Protocol (BGP)

Building Automation and Control (BACnet)

Distributed Computing Env. / Remote Procedure Calls (DCE/RPC)

Dynamic Host Configuration Protocol (DHCP)

Distributed Network Protocol 3 (DNP3)

Domain Name System (DNS)

EtherNet/IP / Common Industrial Protocol (CIP)

FTP (File Transfer Protocol)

Google Quick UDP Internet Connections (gQUIC)

Hypertext Transfer Protocol (HTTP)

Internet Relay Chat (IRC)

Kerberos

Lightweight Directory Access Protocol (LDAP)

Modbus

MQ Telemetry Transport (MQTT)

MySQL

NT Lan Manager (NTLM)

Network Time Protocol (NTP)

Oracle

PostgreSQL

Process Field Net (PROFINET)

Remote Authentication Dial-In User Service (RADIUS)

Remote Desktop Protocol (RDP)

Remote Framebuffer (RFB)

S7comm / Connection Oriented Transport Protocol (COTP)

Session Initiation Protocol (SIP)

Server Message Block (SMB) / Common Internet File System (CIFS)

Simple Mail Transfer Protocol (SNMP)

Simple Network Management Protocol (SMTP)

SOCKS

Secure Shell (SSH)

Secure Sockets Layer (SSL) / Transport Layer Security (TLS)

Syslog

Tabular Data Stream (TDS)

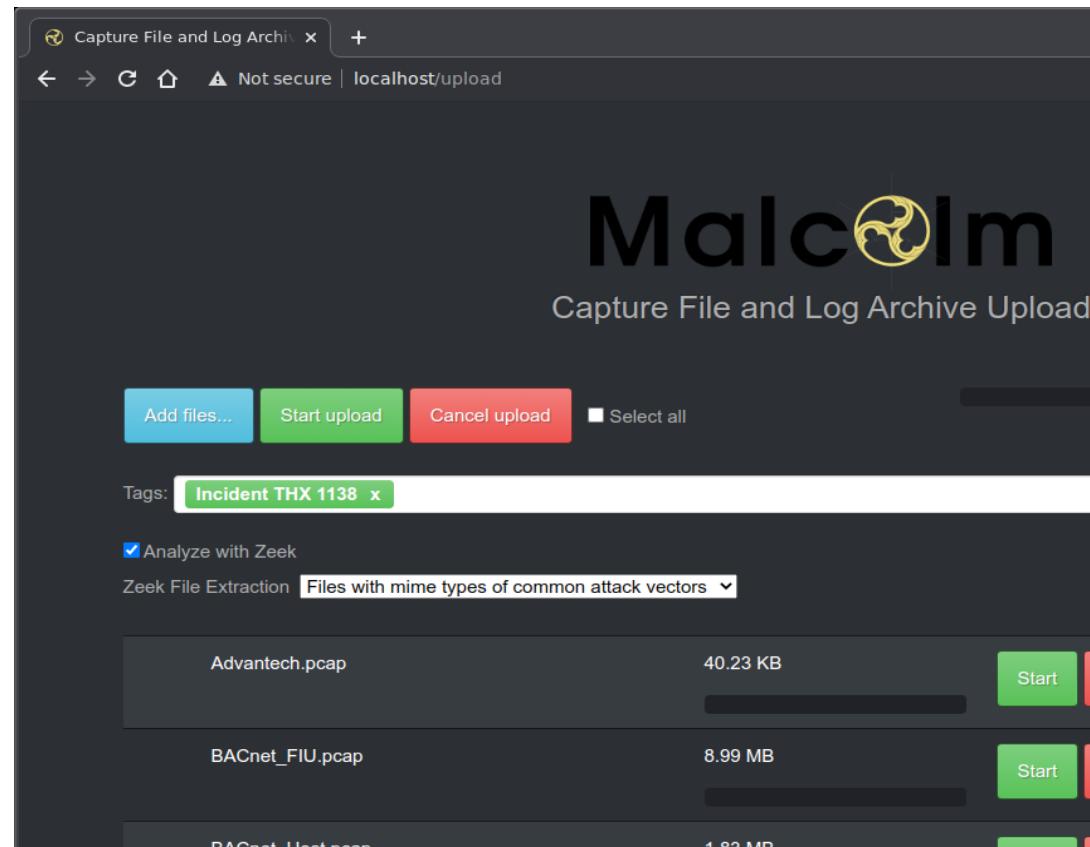
Tunnel protocols (e.g., WireGuard, GTP, GRE, Teredo, AYIYA, IP-in-IP, ...)

Installation and configuration

- Runs on any OS with Docker (Linux, macOS, Windows)
- Alternately, Linux-based Malcolm OS can be installed on hardware or in a virtual machine
- Minimum requirements: 12+ GB RAM, 4+ CPU cores, 8 GB storage + “enough” storage for traffic and logs
- Read
 - <https://github.com/idaholab/Malcolm#QuickStart>
- Watch
 - Malcolm Network Traffic Analysis Tool Suite 

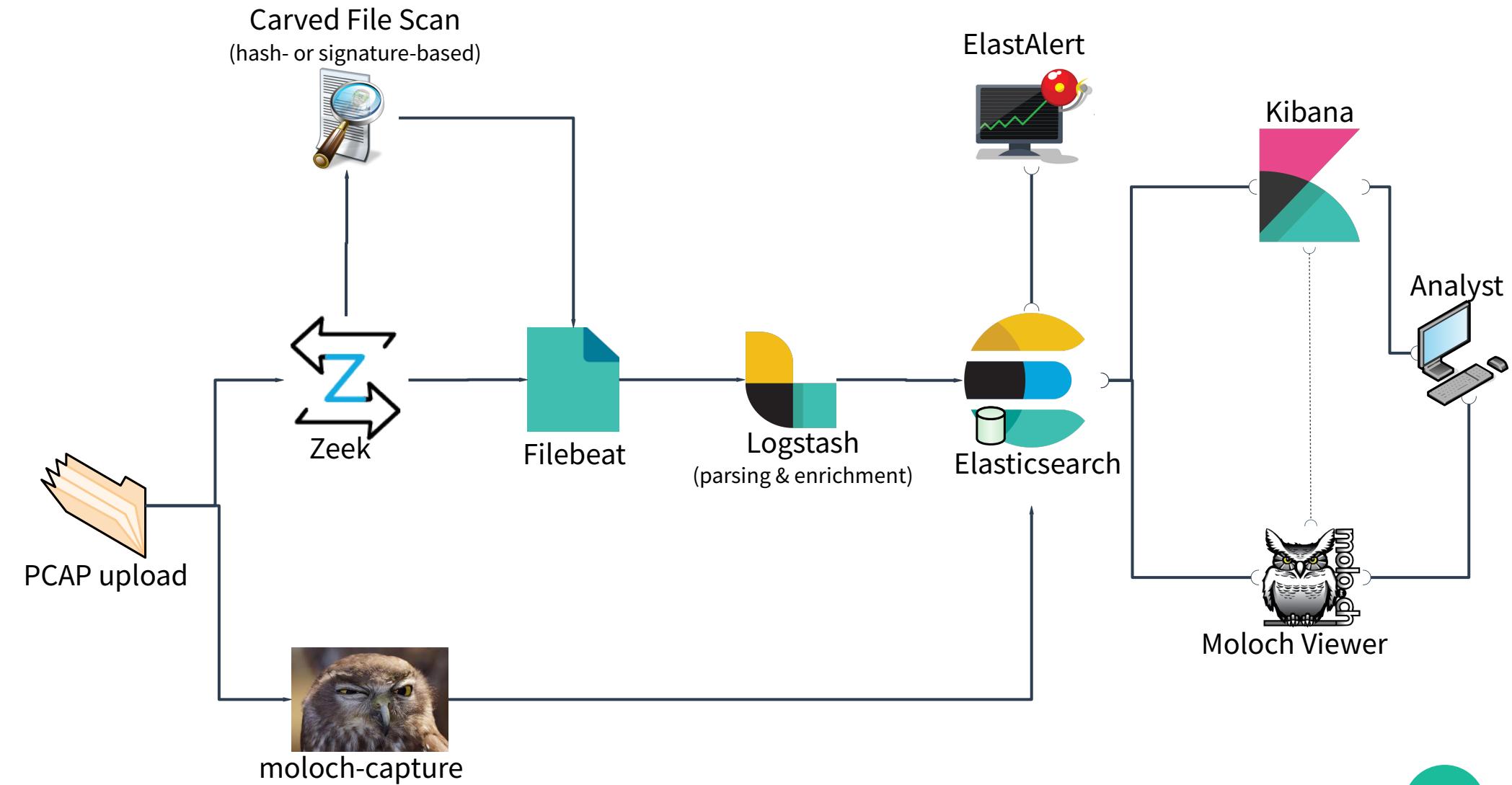
Artifact upload

- **https://localhost/upload once Malcolm is running***
- Apply searchable tags
- Enable Zeek analysis and **file extraction**
 - Can also be enabled in global defaults
- Upload PCAP files or archived Zeek logs
 - pcapng not supported yet



*Links and examples assume Malcolm is accessible on localhost, YMMV depending configuration

Malcolm PCAP processing pipeline



Log enrichment

- Logstash enriches Zeek log data
 - MAC addresses to hardware vendor
 - GeolP and ASN lookups
 - Internal/external traffic based on IP ranges
 - Reverse DNS lookups
 - DNS query and hostname entropy analysis
 - Connection fingerprinting (JA3 for TLS, HASSH for SSH, Community ID for flows)

Custom host and subnet name assignment

- <https://localhost/name-map-ui>

- Assign custom names to network hosts and segments



Host and Network Segment Name Mapping

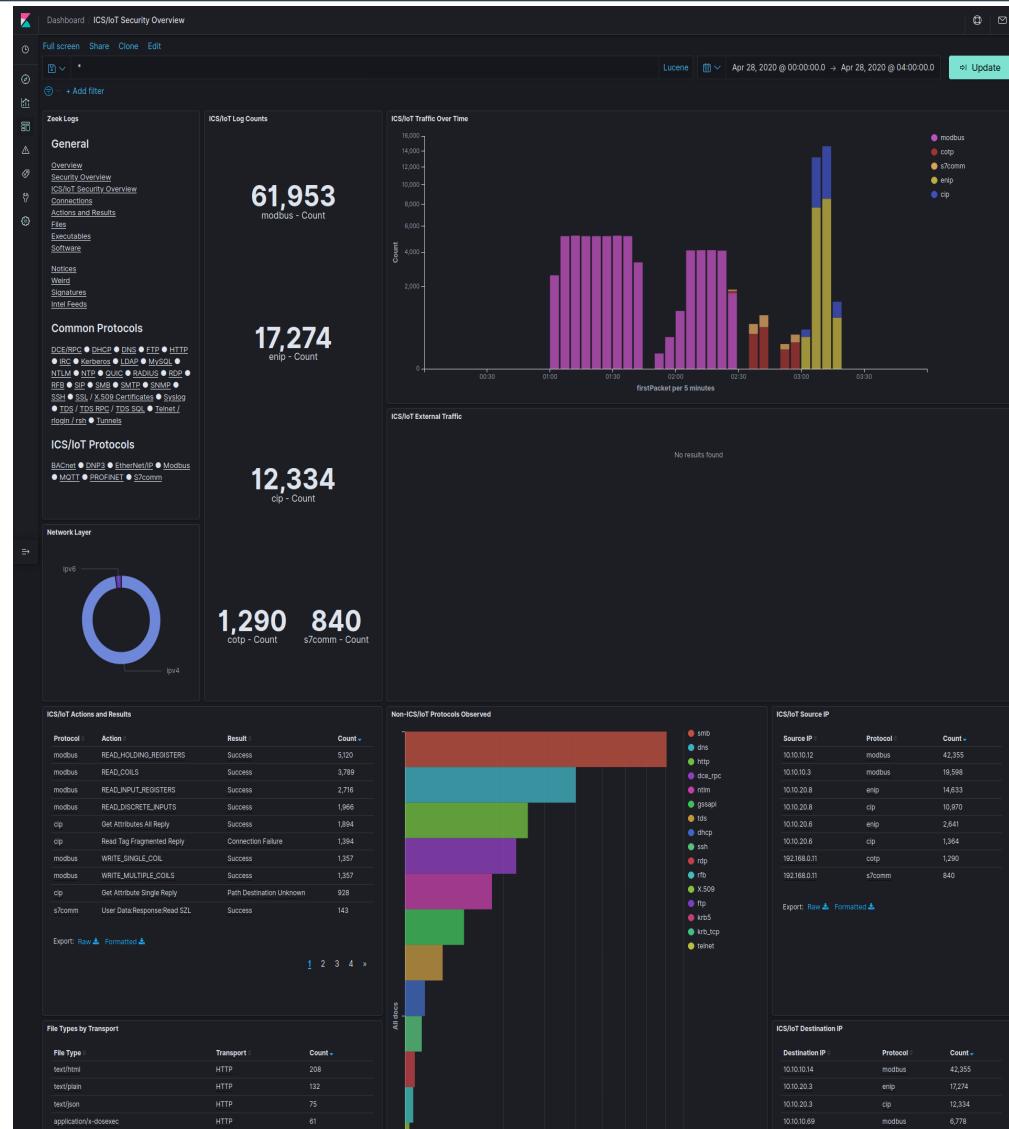
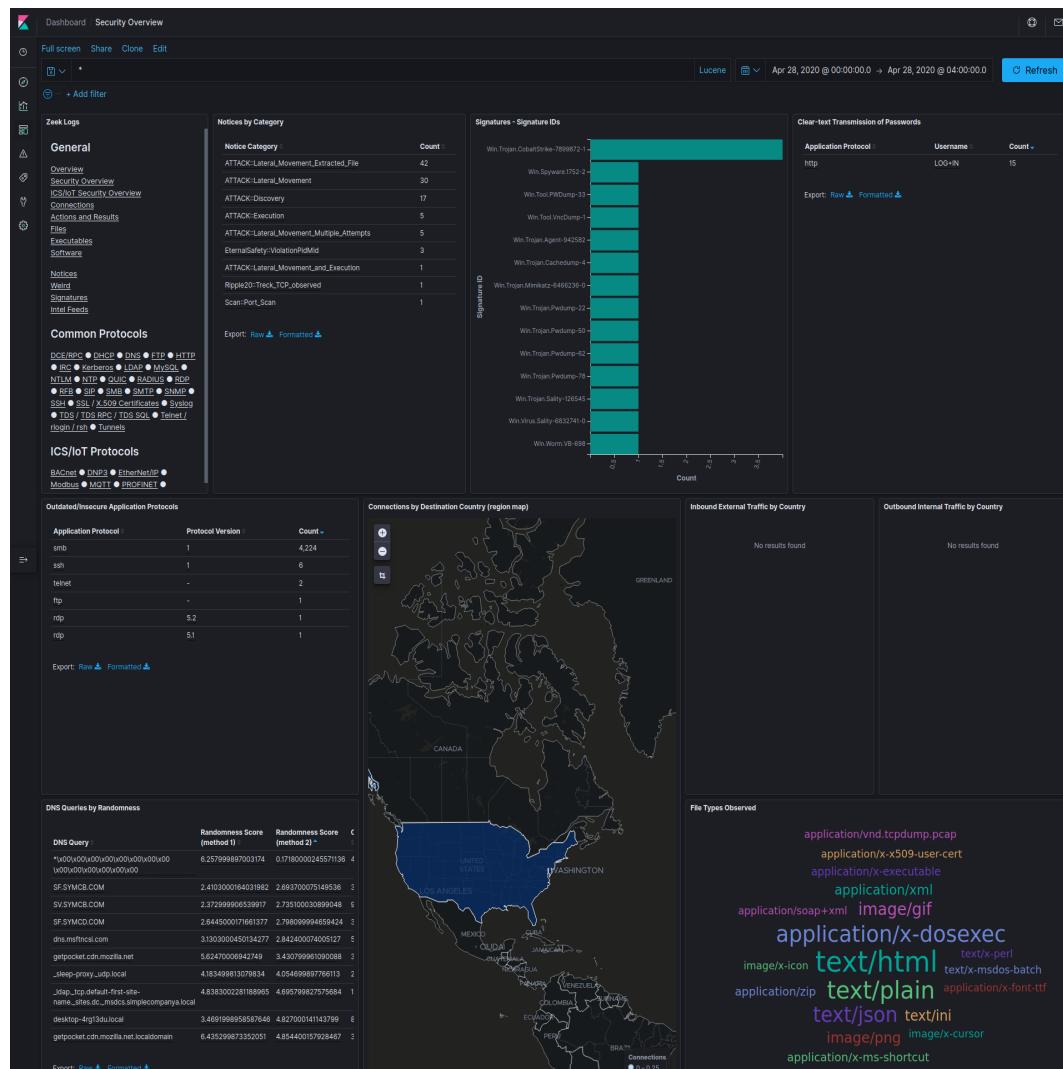
Type	Address	Name	Tag	Search mappings
segment	10.0.0.0/24	Site Office Network	Cyberville	 
segment	10.10.10.0/24	Battery Network	Cyberville	 
host	10.10.10.3	Schneider Battery HMI	Cyberville	 
host	10.10.10.5,10.10.20.5,10.10.30.5,192.168.0.5,10.10.100.5,10.0.0.5	Historian	Cyberville	 
host	10.10.10.11	Cellular Modem	Cyberville	 
host	10.10.10.14,10.10.10.15,10.10.10.16,10.10.10.17,10.10.10.18	Schneider Modbus Slave	Cyberville	 
segment	10.10.20.0/24	Combined Cycle BOP	Cyberville	 
segment	10.10.30.0/24	Wind Turbine Network	Cyberville	 
segment	10.10.100.0/24	Substation Network	Cyberville	 
segment	192.168.0.0/24	Solar Panel Network	Cyberville	 

host Name Tag (optional)

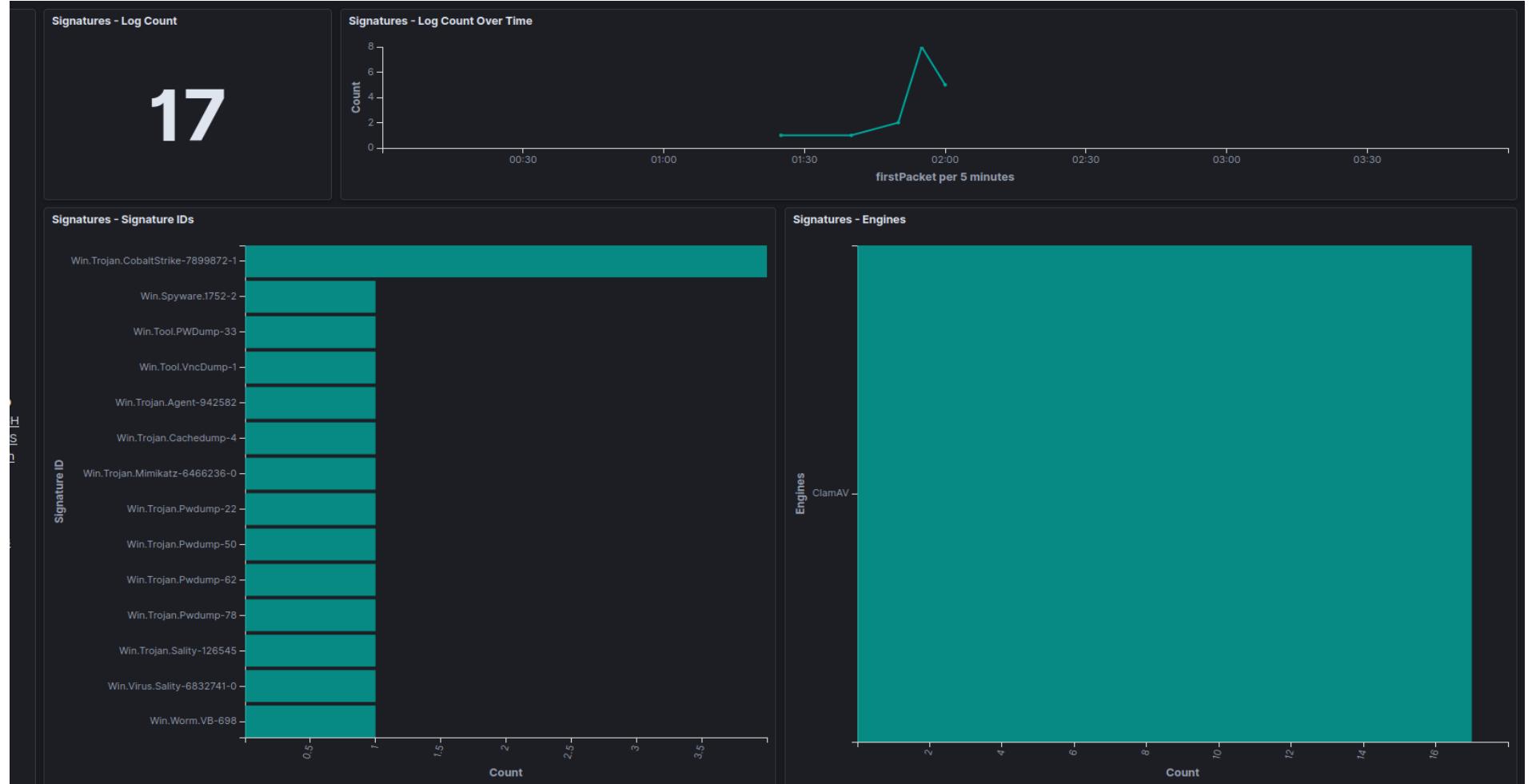
Kibana

- <https://localhost/kibana>
- Front end for enriched Zeek logs
- Search with Kibana Query Language or Lucene Query Syntax
- Dashboards
 - Overviews: Overview, Security Overview, ICS/IoT Security Overview, Connections, Actions and Results, Files, Executables, Software, Notices, Weird and Signatures
 - Protocol-specific: prebuilt for all protocols Malcolm understands
 - WYSIWYG editors to create custom visualizations and dashboards
 - Great for drilling down from high-level trends of network traffic to specific items of interest

Kibana: Security & ICS/IoT Security Overview

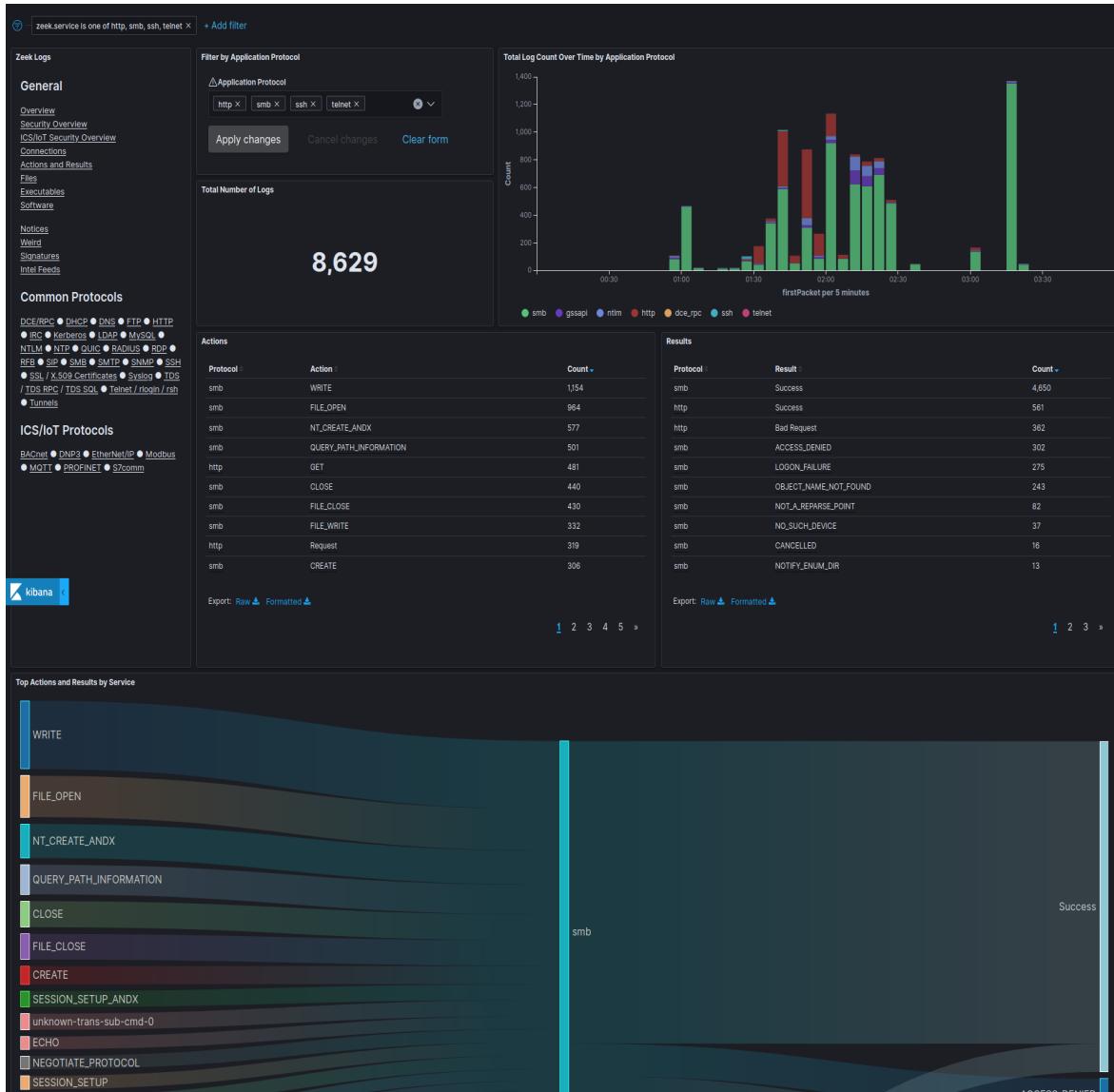


Kibana: Signatures



- Reports hits from file scanning engines (e.g., ClamAV) against files carved from network traffic

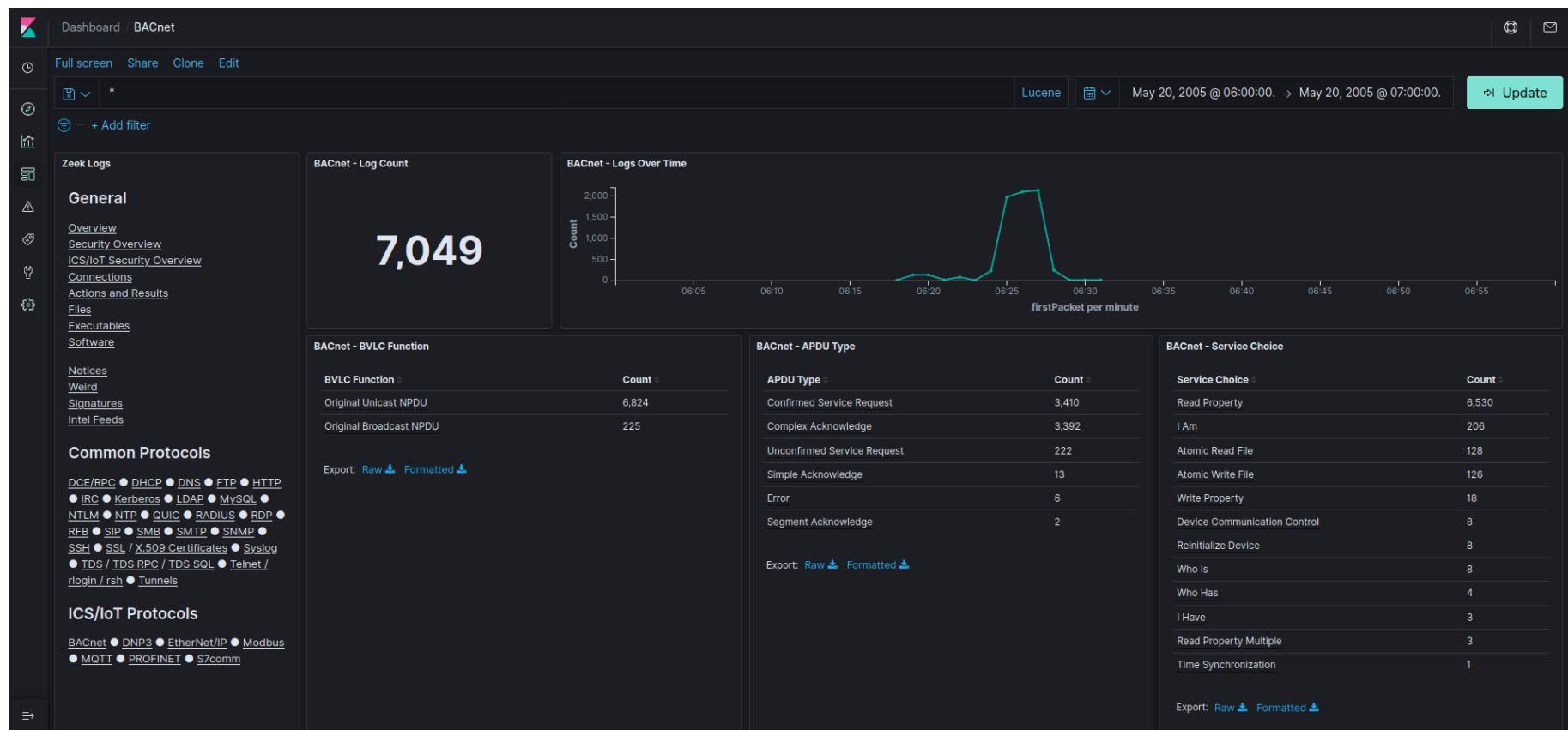
Kibana: Actions and Results



- Malcolm normalizes “action” (e.g., write, read, create file, logon, logoff, etc.) and “result” (e.g., success, failure, access denied, not found) across protocols

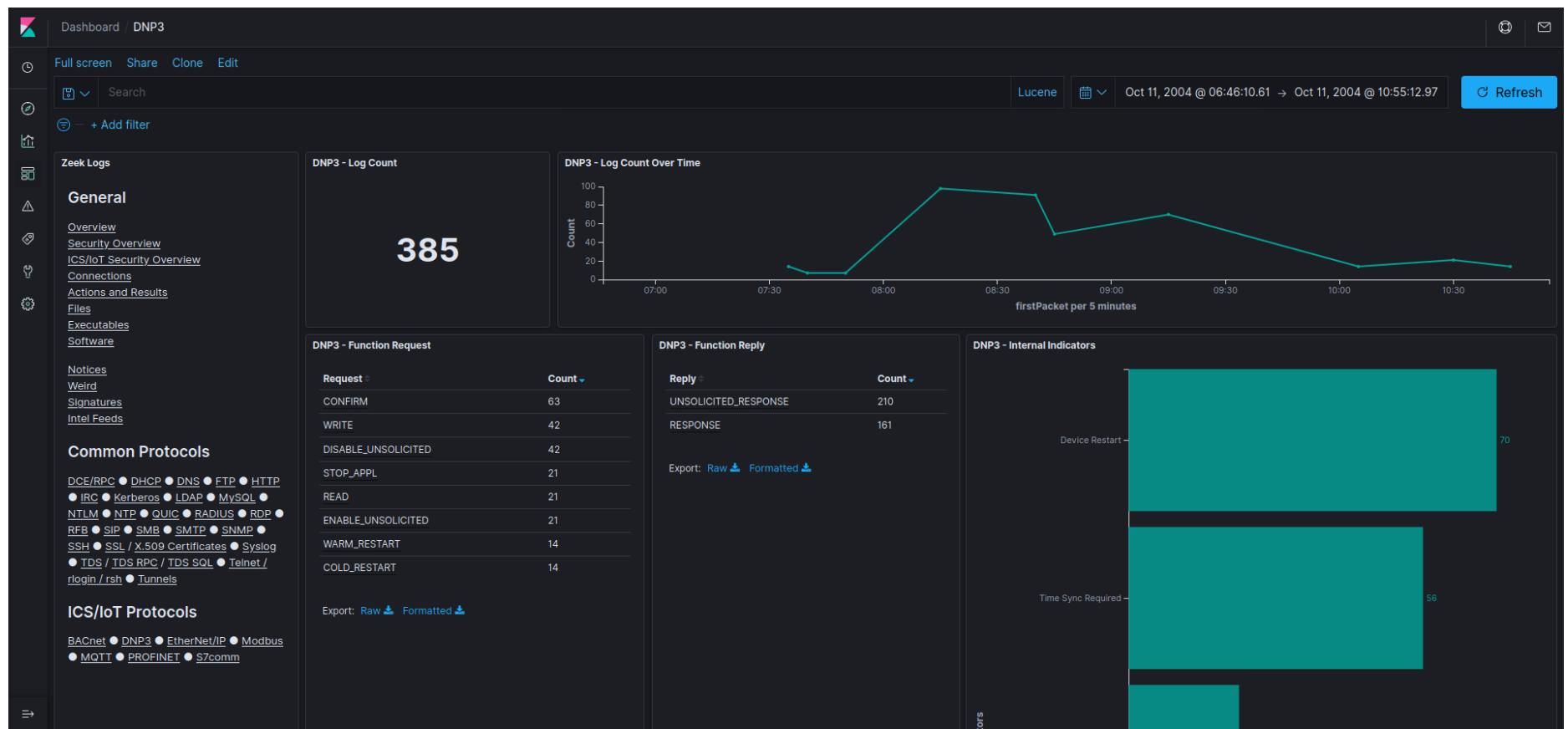
Kibana: ICS protocol dashboards

BACnet



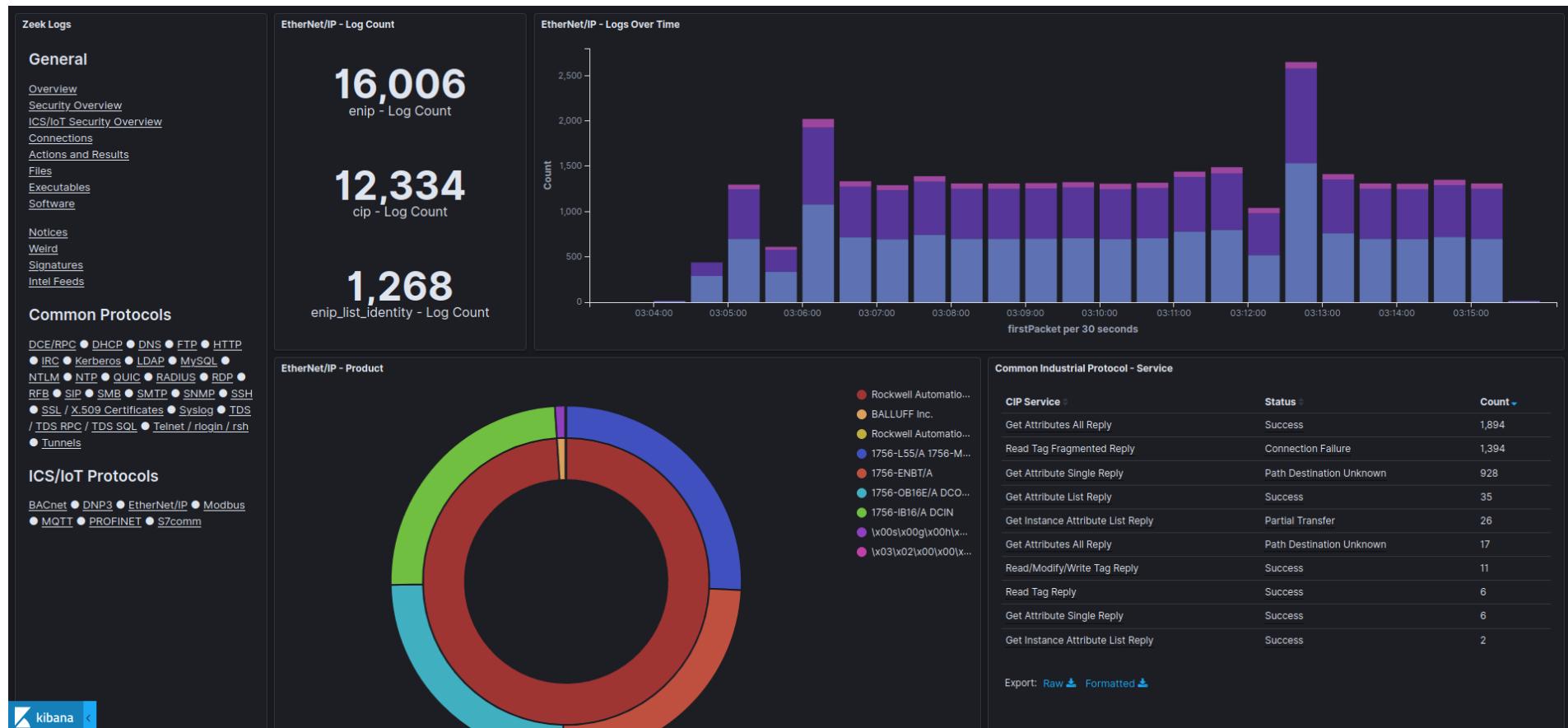
Kibana: ICS protocol dashboards

DNP3

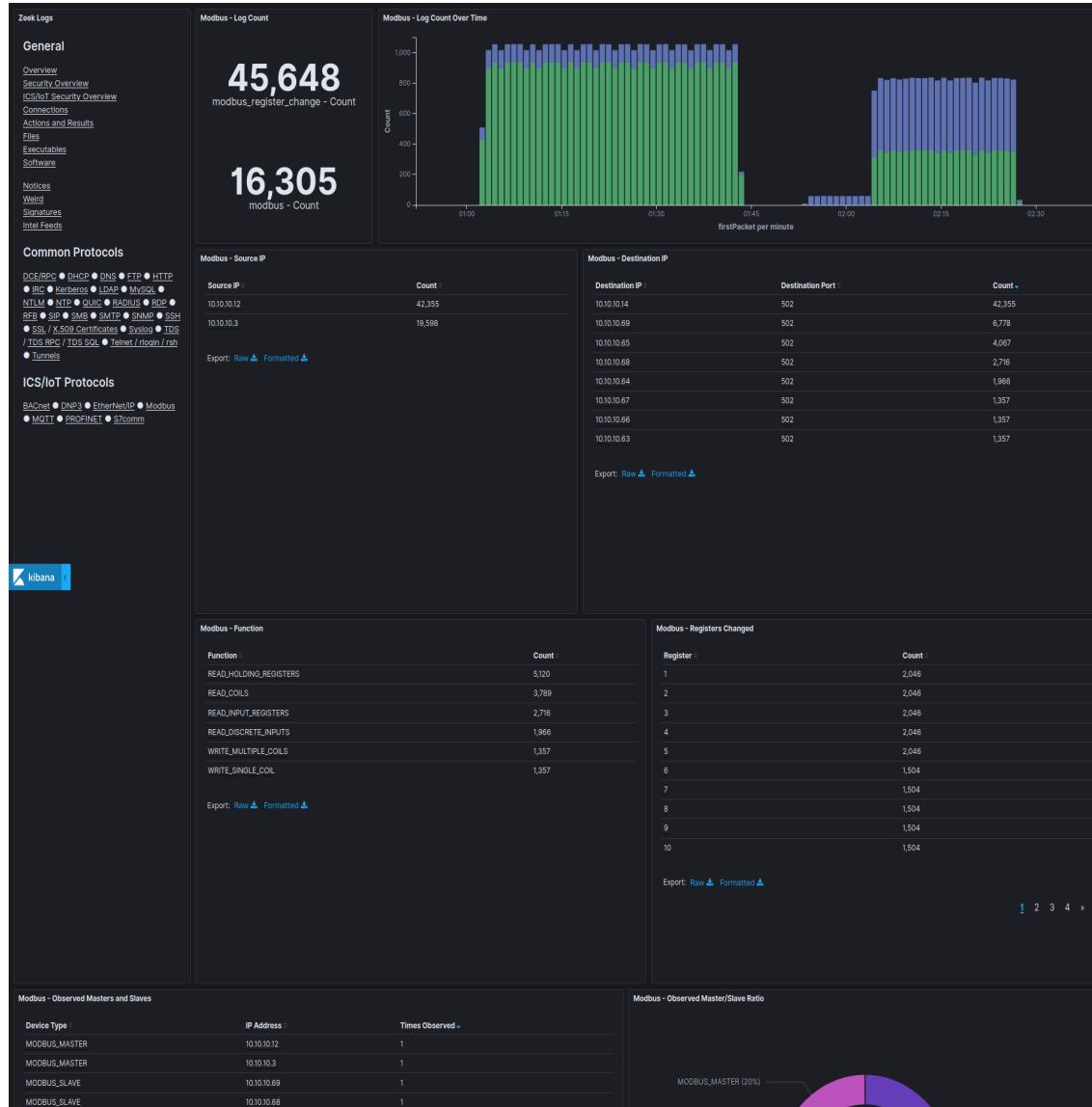


Kibana: ICS protocol dashboards

EtherNet/IP

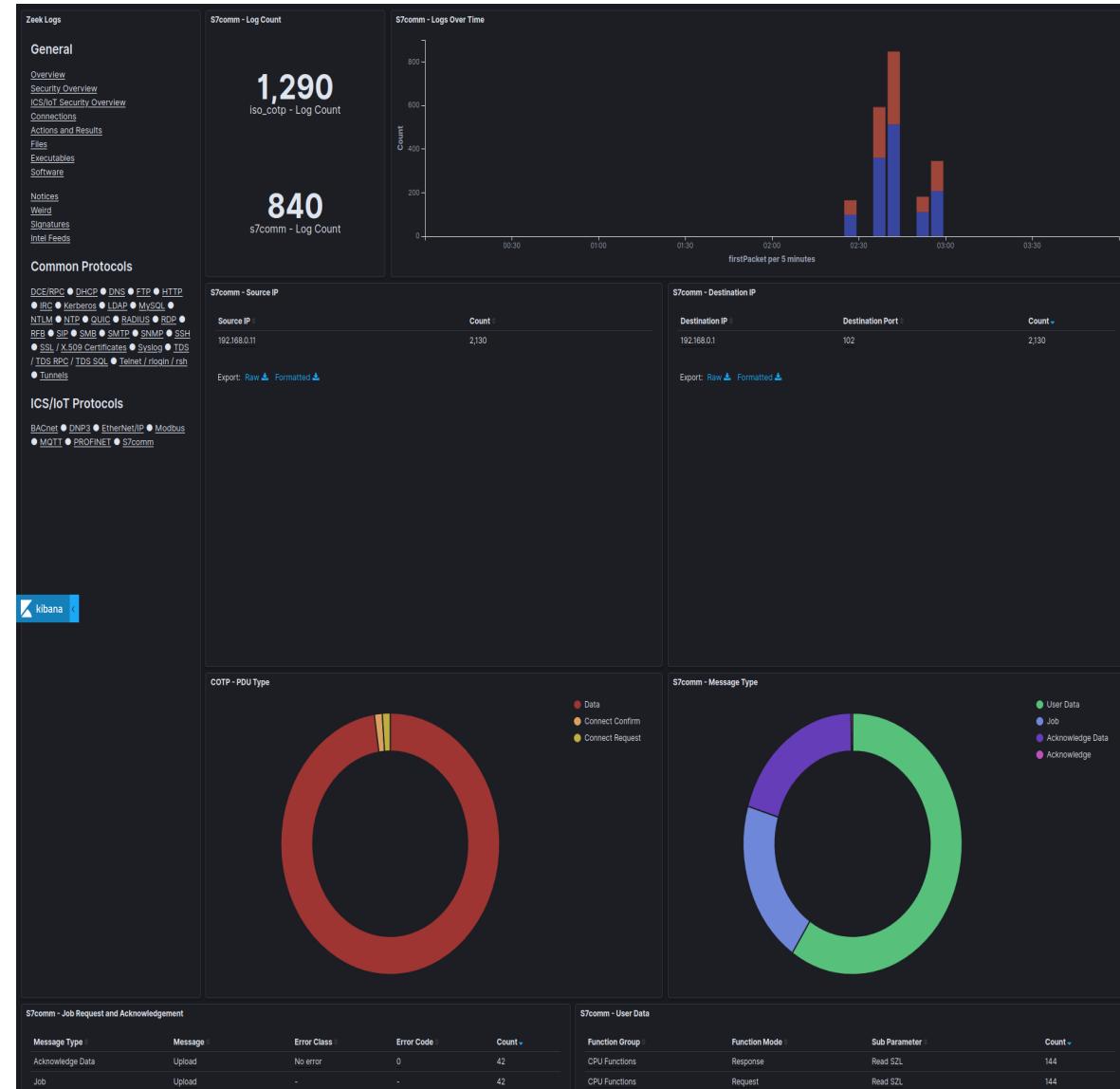


Kibana: ICS protocol dashboards



Modbus

Kibana: ICS protocol dashboards

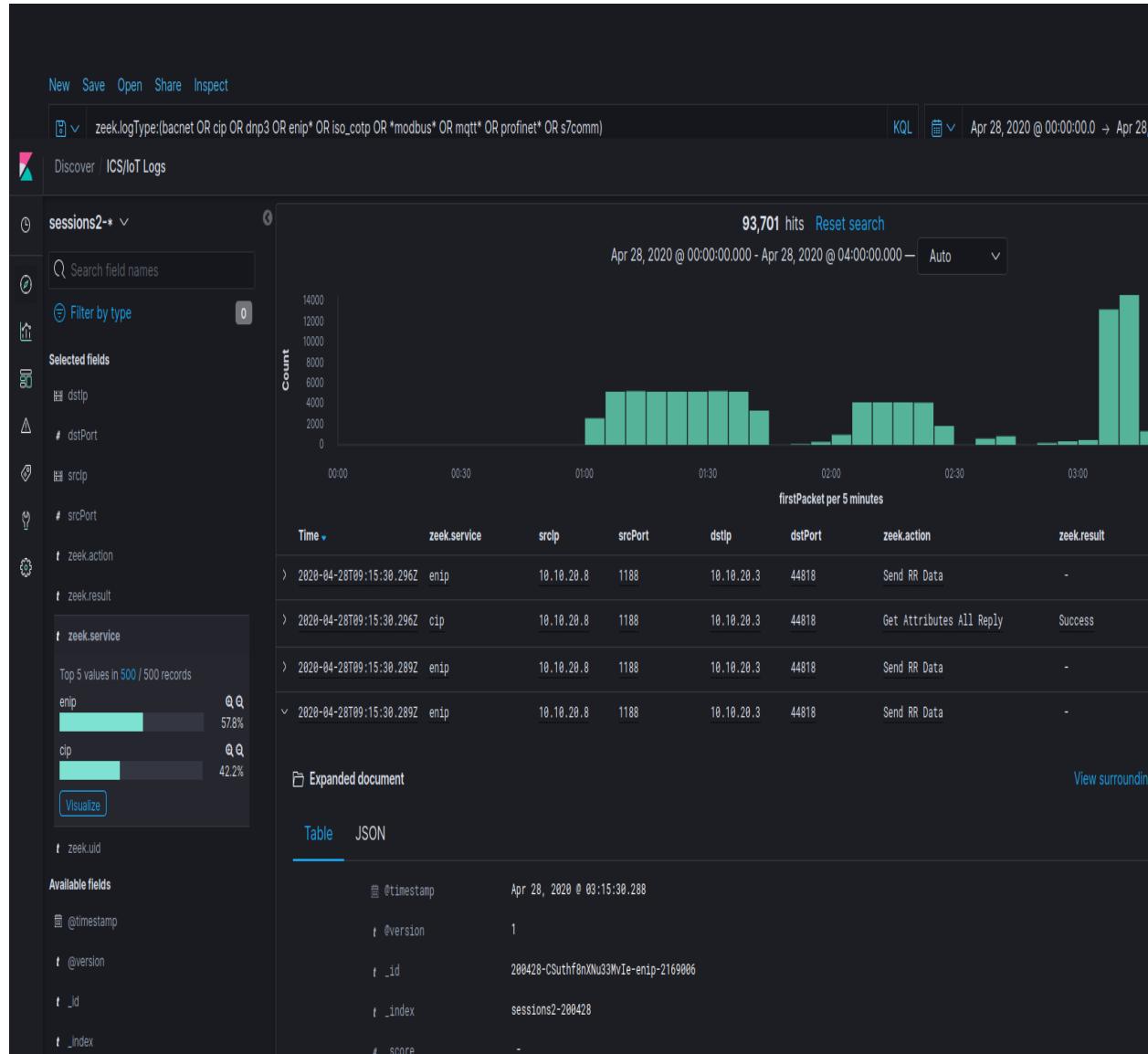


S7comm

Kibana

- ## Discover

- Field-level details of logs matching filter criteria
- Create and view saved searches
- View other events just before and after an event



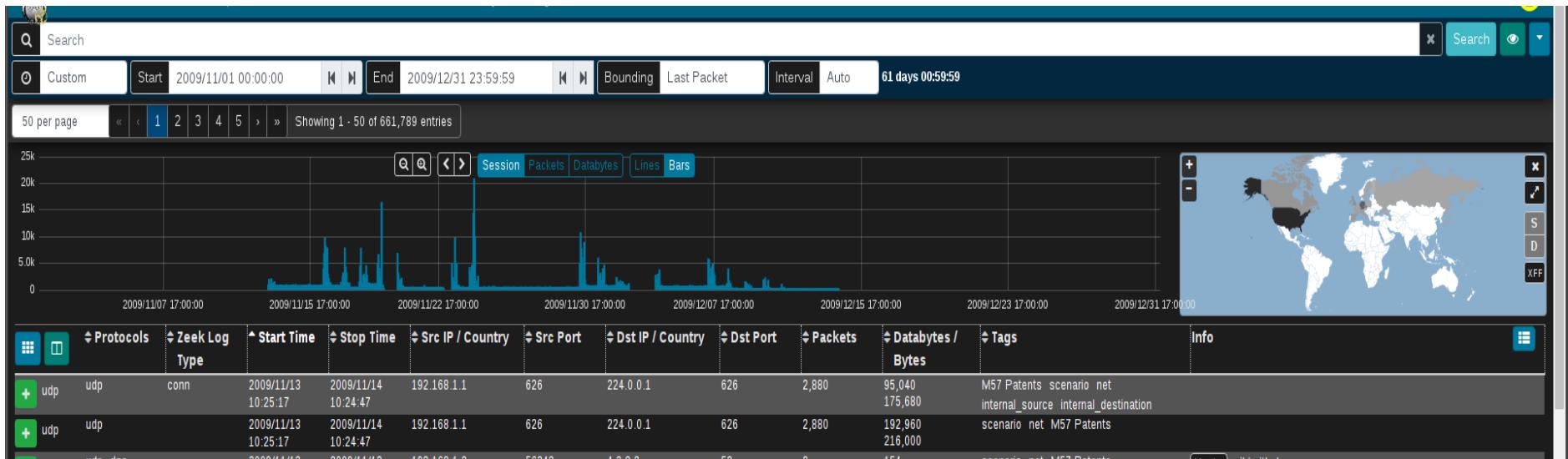
Moloch

- <https://localhost/>
- Front end for **both** enriched Zeek logs and Moloch sessions
- Filter by Zeek logs or Moloch sessions; or, view both data sources together
- “Wireshark at scale”: full PCAP availability for viewing packet payloads, exporting filtered and joined PCAP sessions and running deep-packet searches



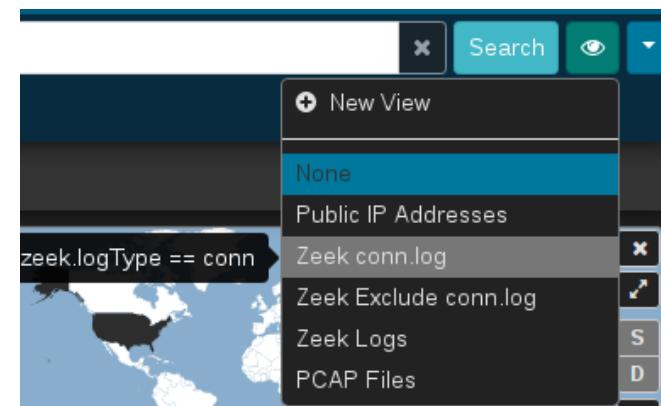
Moloch: Sessions

- Field-level details of sessions/logs matching filters



- Views: overlay saved filters on current search

- E.g., show Moloch sessions vs. Zeek logs



Moloch: Packet payloads

- Displayed for Moloch sessions with full PCAP
- File carving on the fly
- Download session PCAP
- Examine payload with CyberChef

The screenshot shows the Moloch web interface. At the top, there is a search bar with the query "ip.src == 10.10.10.3 && protocols == http && bytes > 10000". Below the search bar are various filters and controls: "Custom", "Start" (2020/04/28 00:00:00), "End" (2020/04/28 04:00:00), "Bounding", "Last Packet", "Interval" (Auto), and a timestamp "04:00:00". The main area displays a table of 83 entries, with the first few rows shown below:

Packets	Src	Dst	Timestamp	Length	Source	Destination
200	10.10.10.3	10.10.10.11	2020/04/28 01:59:42	57557	HTTP/1.1 200 OK	PCAnyPass.exe
			2020/04/28 01:59:42	57628	Server: SimpleHTTP/0.6 Python/2.7.17	
			2020/04/28 02:01:50	57474	Date: Fri, 17 Apr 2020 19:21:32 GMT	
			2020/04/28 01:57:06	57485	Content-type: application/x-msdos-program	
			2020/04/28 01:57:24		Content-Length: 49152	
					Last-Modified: Fri, 16 Apr 2010 19:09:50 GMT	

On the right side of the interface, there is a "File Bytes" section showing a hex dump of the file content. The bottom right corner features a "CyberChef" button.

Moloch: PCAP Export

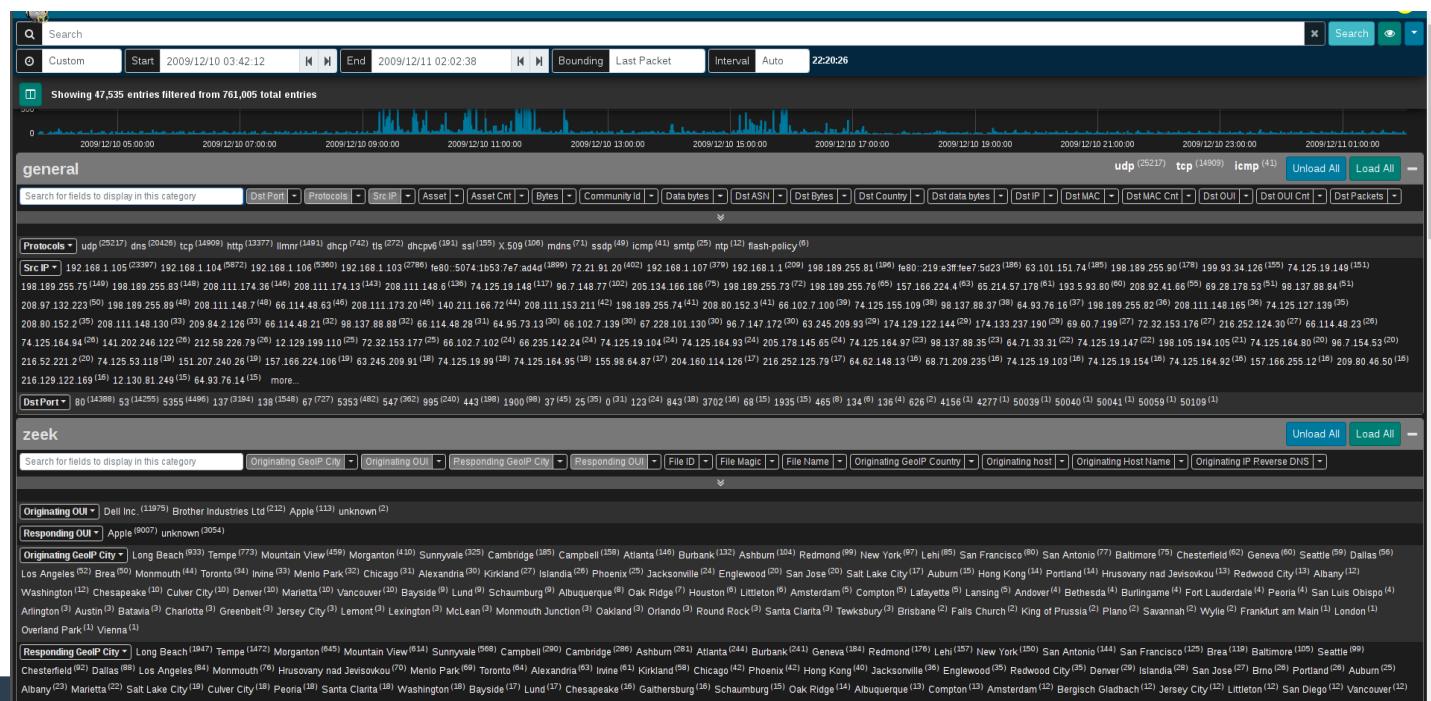
- Creates a new PCAP file from filtered sessions
- Include open, visible or all matching sessions
- Apply “PCAP Files” view to sessions first
- Narrow as much as possible prior to exporting (huge PCAP files are a pain)

The screenshot shows the Moloch web interface version 1.8.0. At the top, there's a search bar with the query "country == US && protocols == http". Below it, a button says "Custom" and "Apply action to 7075 query matching sessions". The timeline at the bottom shows traffic from November 23 to November 25, 2009. A world map is on the right. The main area displays a table of sessions with columns for Protocols, Zeek Log Type, Start Time, Stop Time, Src IP / Country, Src Port, Dst IP / Country, Dst Port, Packets, Bytes, and Info. The table lists several http/tcp sessions between 192.168.1.103 and 198.189.255.75, mostly port 80, with various byte counts and tags like "M57 Patents". An "Export PCAP" button is visible at the top right.

Protocols	Zeek Log Type	Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Bytes	Info
tcp	http tcp	2009/11/25 06:15:38 MST	2009/11/25 06:15:38 MST	192.168.1.103 US	1263	198.189.255.89 US	80	33	28,482 30,358	scenario net M57 Patents aa.avg.com/softw/90/update/u7iaw2525u252475.bin
tcp	http tcp	2009/11/25 06:15:37 MST	2009/11/25 06:15:37 MST	192.168.1.103 US	1261	198.189.255.89 US	80	106	106,451 112,439	scenario net M57 Patents aa.avg.com/softw/90/update/u7avi1787u170575.bin
tcp	http tcp	2009/11/25 06:02:51 MST	2009/11/25 06:02:51 MST	192.168.1.106 US	1252	198.189.255.89 US	80	33	28,487 30,363	scenario net M57 Patents aa.avg.com/softw/90/update/u7iaw2525u252475.bin
tcp	http tcp	2009/11/25 06:02:51 MST	2009/11/25 06:02:51 MST	192.168.1.106 US	1250	198.189.255.89 US	80	104	106,456 112,316	scenario net M57 Patents aa.avg.com/softw/90/update/u7avi1787u170575.bin
tcp	http tcp	2009/11/25 04:36:23 MST	2009/11/25 04:36:23 MST	192.168.1.104 US	1072	198.189.255.75 US	80	34	28,487 30,427	scenario net M57 Patents aa.avg.com/softw/90/update/u7iaw2525u252475.bin
tcp	http tcp	2009/11/25 04:36:22 MST	2009/11/25 04:36:23 MST	192.168.1.104 US	1070	198.189.255.75 US	80	106	106,456 112,456	scenario net M57 Patents aa.avg.com/softw/90/update/u7avi1787u170575.bin
tcp	http tcp	2009/11/25	2009/11/25	192.168.1.104 US	1058	198.189.255.75 US	80	11	3,605	scenario net M57 Patents aaawl-ssd.sun.com/update/1.6.0/man-1.6.0.xml

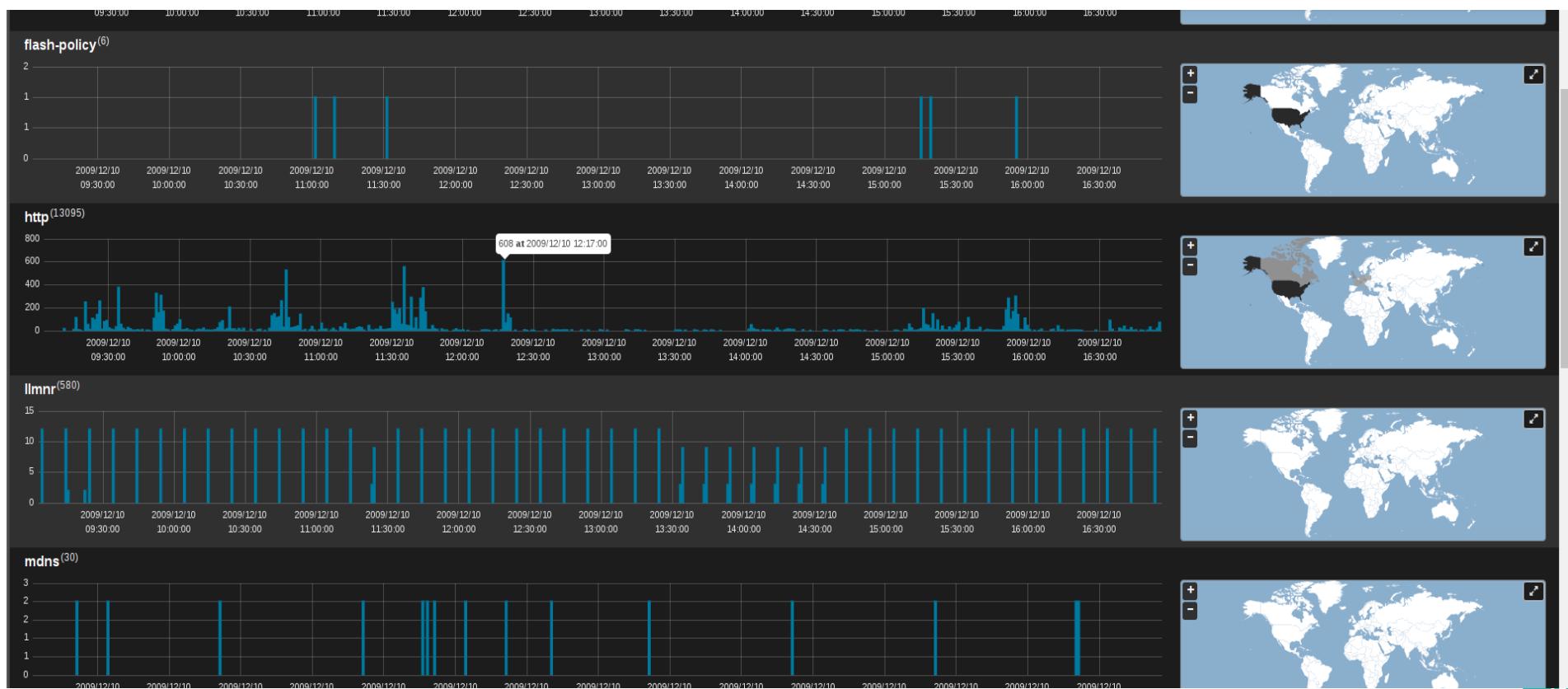
Moloch: SPIView

- Explore “top n ” and field cardinality for all fields of both Moloch sessions and Zeek logs
- Apply filters or pivot to Sessions or SPIGraph view for field values of interest
- Limit search to ≤ 1 week before using as it runs many queries



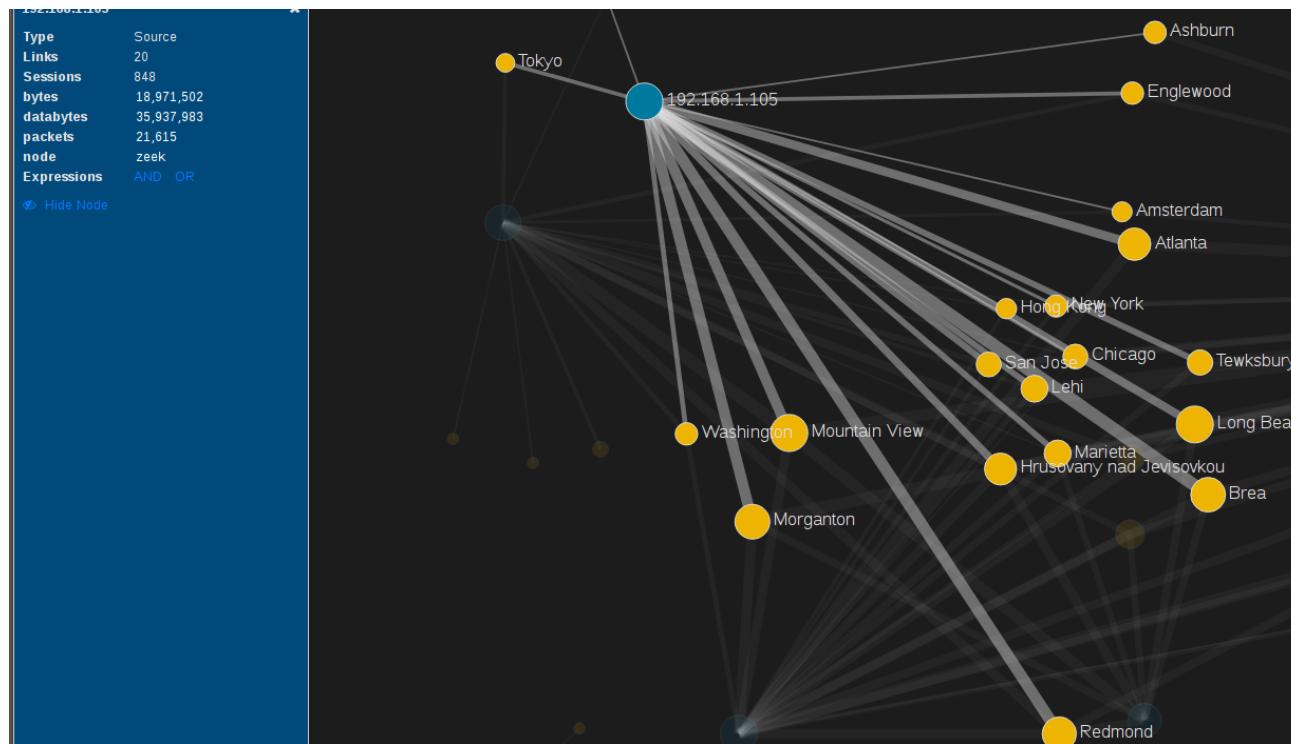
Moloch: SPIGraph

- View “top n ” field values chronologically and geographically
- Identify trends and patterns in network traffic



Moloch: Connections

- Visualize logical relationship between hosts
- Use any combination of fields for source and dest. nodes
- Compare current vs. baseline traffic



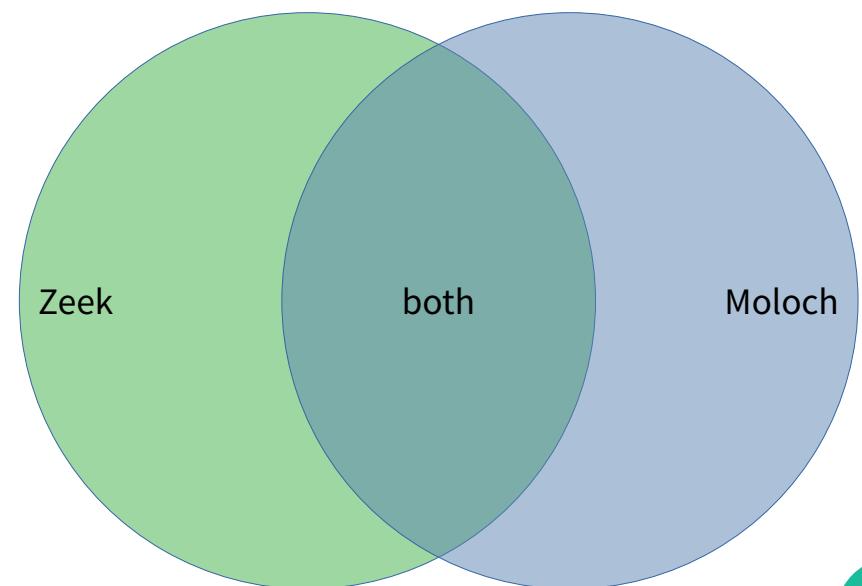
Moloch: Hunt

- Deep-packet search (“PCAP grep”) of session payloads
- Search for ASCII, hex codes or regular expression matches
- Apply “PCAP Files” view to sessions first

The screenshot shows the Moloch Hunt interface. At the top, there's a navigation bar with links: Sessions, SPIView, SPIGraph, Connections, Hunt, Files, Stats, History, Settings, and Users. Below the navigation bar is a search bar containing the query "protocols == http". Underneath the search bar are buttons for "All (careful)", "Start" (set to 1969/12/31 17:00:00), "End" (set to 2019/05/28 09:19:44), and "Bounding" and "Last Packet" buttons. A status message indicates "Creating a new packet search job will search the packets of 43,818 sessions." Below this is a table titled "Hunt Job Queue" with columns: Status, Matches, Name, User, Search text, Notify, Created, and ID. One row is shown: "Running" (62.3%), 297 matches, "HTTP with password" name, "analyst" user, "password (ascii)" search text, "2019/05/28 09:20:28" created, and ID "vRgH_2oB-8T3HMe4R6WA". At the bottom of the interface, several informational messages are displayed: "This hunt is running", "This hunt was last updated at: 2019/05/28 09:21:06", "Examining 50 raw source and destination packets per session", "Found 297 of 27,299 searched sessions out of 43818 total sessions to search", "The sessions query expression was: protocols == http", and "The sessions query time range was from 1969/12/31 17:00:00 to 2019/05/28 09:19:44".

Using Moloch and Kibana together in Malcolm

- Search syntax is different between Moloch and Kibana (and in some cases, so are field names): see [Malcolm documentation](#) for examples and [Moloch help](#)
- Despite considerable overlap, there are differences in **protocol parser support** between Zeek and Moloch
 - Learning the strengths of each will help you more effectively find the good stuff



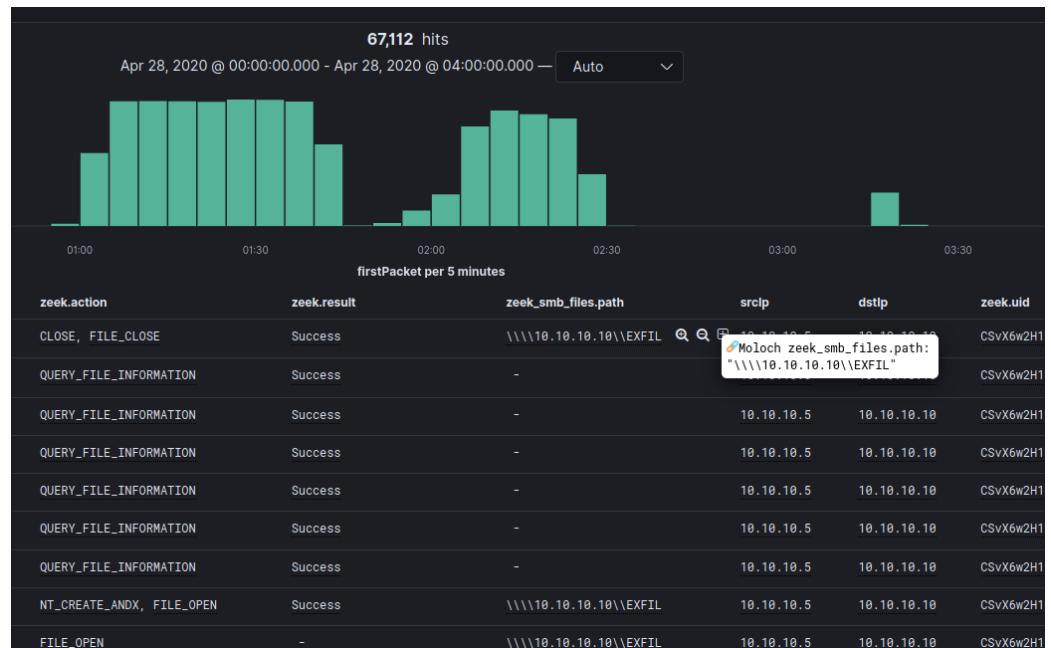
Pivots: Moloch → Kibana

- Moloch → Kibana

The screenshot shows the Moloch interface. At the top, there's a navigation bar with links for Sessions, SPIView, SPIGraph, Connections, Hunt, Files, Stats, History, and Settings. Below the navigation bar is a search bar with a custom date range from 2020/04/28 00:00:00 to 2020/04/28 04:00:00. The main content area displays SMB activity for host 10.10.10.10, showing shares EXFIL and file \\alarms.png. Below this, the "Zeek Common Fields" section lists various fields such as Zeek Connection ID (CSvX6w2H1DADdrC3k8), Zeek Log Type (smb_cmd smb_files), Zeek Node (filebeat), Originating Host (10.10.10.5), Originating Host Name (Historian), Originating Network Se... (Battery Network), Responding Host (10.10.10.10), Responding Network S... (Battery Network), and so on. A dropdown menu for the "Result" field shows options like Success, New Sessions Tab, and Copy value.

Kibana

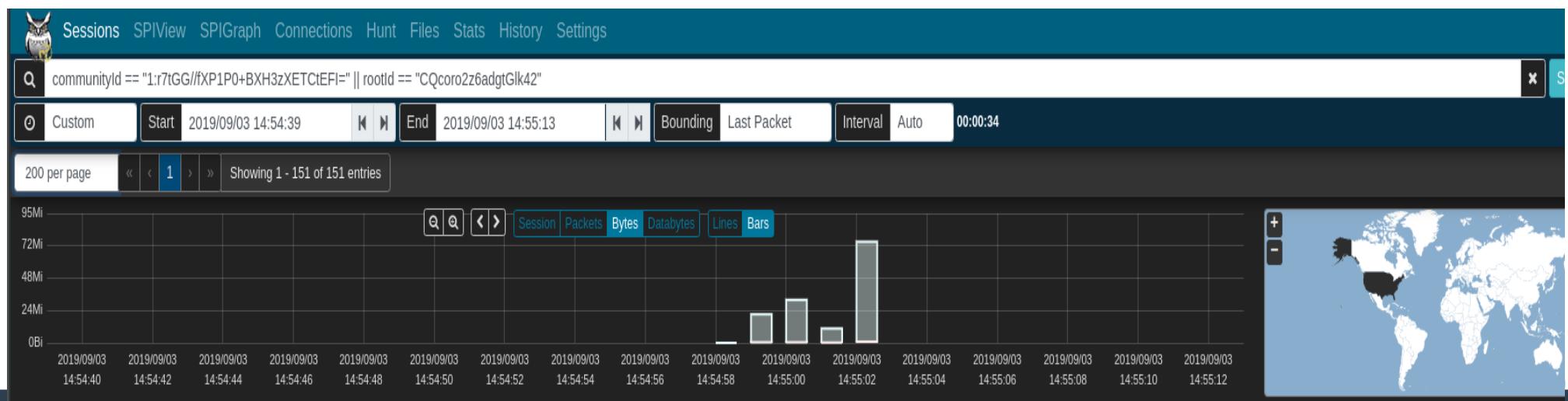
- Kibana → Moloch



Check query search time frame after pivot:
sometimes it gets lost in translation.

Correlating Moloch sessions and Zeek logs

- Correlate Zeek logs and Moloch sessions using common fields
 - communityId fingerprints flows in both and can bridge the two
 - zeek.uid/rootId filters Zeek logs for the same session
 - Filter community ID OR'ed with zeek UID to see all Moloch sessions and Zeek logs for the same traffic
 - `communityId == "1:r7tGG//fXP1P0+BXH3zXETCtEFI=" || rootId == "CQcoro2z6adgtGlk42"`



Search tips

- Always check your search time frame
- “Zoom in” (apply filters) for a particular field value, pivot to another field then “zoom out” (remove filters)
- Most UI controls can work with any data field (1000+)
- Filter on zeek . logType (e.g., conn to see conn.log)
- Filter on protocol or both Moloch and Zeek regardless of data source (e.g., protocol:http in Kibana and protocols == http in Moloch)
- tags field
 - Populated for both Moloch sessions and Zeek logs with tags provided on upload and words extracted from filenames
 - internal_source, internal_destination, external_source, external_destination, cross_segment

Thanks! Visit [Malcolm on GitHub](#)
to read the docs, make
suggestions, report issues and
star to show your support!



Malcolm is Copyright © 2020 Battelle Energy Alliance, LLC, and is developed and released through the cooperation of the Cybersecurity and Infrastructure Security Agency of the US Department of Homeland Security.