

YAHOO!  
FINANCE

TC TechCrunch

YAHOO!  
SPORTS

IHUFFPOSTI

MAKERS

YAHOO!  
NEWS

engadget

YAHOO!  
M&E

YAHOO!  
ENTERTAINMENT

Aol.

BUILD  
0 4 0 0

RYOT

# Welcome to MolochON 2019

verizon  
media



# Meet Us!



**Andy**  
Moloch Creator



**Elyse**  
Moloch Software  
Engineer & UI expert



**Rosalie**  
Technical Open Source  
Community Manager



# Code of Conduct

Assume positive intent  
Respect participants  
Welcome to new members  
Be kind to beginners  
Consider your impact on others  
Use words carefully  
Leave with class

More info on GitHub: [github.com/aol/moloch/blob/master/CODE\\_OF\\_CONDUCT.md](https://github.com/aol/moloch/blob/master/CODE_OF_CONDUCT.md)



# Chatham House Rule

**Participants are free to use the information received, but neither the identity nor the affiliation of the speakers, nor that of any other participant, may be revealed.**

Please refrain from taking photos, recordings, or posting on social media unless given express permission.



# Happy Hour

6pm

**The Oxford**

195 S Murphy Ave

Sponsored By

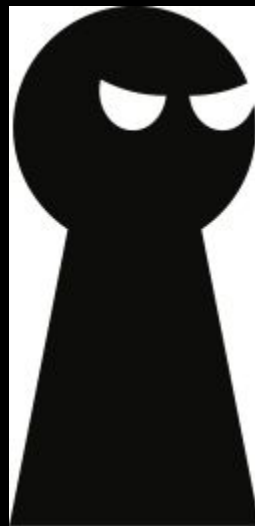
# ARISTA



---

# We're hiring

[theparanoids.com](http://theparanoids.com)



verizon  
media



YAHOO!  
FINANCE

TC TechCrunch

YAHOO!  
SPORTS

IHUFFPOSTI

MAKERS

YAHOO!  
NEWS

engadget

YAHOO!  
M&E

YAHOO!  
ENTERTAINMENT

Aol.

BUILD  
O A O

RYOT

# Recent Changes

verizon  
media



---

# Major Changes

- Moloch 2.0
- Elasticsearch 7 support
- New molo.ch Homepage
- Expression Shortcuts
- Cancel Queries
- Improved documentation





---

# Moloch 2.0

- Requires ES 6.7.x or later
  - 6.8.2+ or 7.3+ recommended
- Variable shortcuts for Moloch search expressions
- Multiple notifiers in Parliament
- Stats improvements
- Many fixes and improvements - Viewer & Capture



---

# New Molo.ch Homepage

- Hosted on github
- Lives at [github.com/aol/molochweb](https://github.com/aol/molochweb)
  - anyone can do PRs
- Github wiki will no longer be updated
- Settings are linkable now



---

# Capture

- Classify/Parse data inside CONNECT method
- New Classify/Parsers: telnet, mpls, dtls, ...
- Can limit disk queue finally!
- Support ES auto generated ids



# Capture

- Fingerprints: communityId, ja3, ja3s, hassh, ...

## SSH

**Versions** ▾ ssh-1.99-openssh\_3.9p1 ssh-2.0-openssh\_5.3

**Hassh** ▾ 21b457a327ce7a2d4fce5ef2c42400bd

**Hassh Server** ▾ f430cd6761697a6a658ee1d45ed22e49

**JA3** ▾ b288289af2999820648eb3ca4d8304c5

**JA3s** ▾ b7bd51222a09f3ad66a340710ae9c01a

**Id** c5ukVm0B2JS8siK3BwMH **Community Id:** 1:eCGZrs2oS78hdxeW5zAzN+gSTUc=

**Time** 2013/12/20 13:45:11 - 2013/12/20 13:45:12



---

# Capture - Rules

- Rules: Added startsWith, contains, endsWith operators

```
- name: "tag some awesome tls sites"  
  when: "fieldSet"  
  fields:  
    protocols: tls  
    host.http: www.aol.com  
    host.http,endsWith: yahoo.com  
  ops:  
    "awesomeSite": "yes"
```



---

# WISE

- Move wiseService directory to top level
- Better redis support (2.1.0)
- Support arrays for JSON formatted data

```
[{
  "ip": ["2001:16d8:ffce:0010:aca8:353c:291d:a9b3", "10.20.30.50"],
  "tag": "ipwise-array", "status": "super-bad"
},{
  "ip": "2001:16d8:ffce:0010:aca8:353c:291d:0002,10.20.30.51",
  "tag": "ipwise-comma", "status": "super-good"
}]
```



---

# Viewer

- Cancel queries
- Hunt improvements
- Search variable shortcuts
- Connections improvements
- Multi Field Intersection
- More!



# Demo





---

# Parliament

- Dark mode
- Help page
- Multiple notifiers
- Improved issues workflow



# Demo



---

# Upcoming Changes - Elasticsearch

- Index Lifecycle Management
- Support version 8
- Easier to reindex/shrink indices (2.1.0)
- Support more db.pl features in UI



---

# Upcoming Changes - Capture

- “Easy” to add new ethernet/ip protocols
- Glib2 upgrade (meson)
- Public Suffix List
- Include sample Rules files with releases
- Latest HTTP/3 (QUIC)



---

# Upcoming Changes - Viewer

- Visualizations - give us ideas!
- Add high/low/average to timeline data
- Optimize more Elasticsearch database updates
- Resolve IPs
- Improve accessibility and keyboard shortcuts
- Improve Multiviewer
- Fix bugs!



---

# Writing Good GitHub Issues



- Make sure bug has not already been reported
  - If it has, provide more details or give it a thumbs up
- Provide a clear and descriptive title
- Describe the exact steps to reproduce the bug, or describe the feature request in as much detail as possible
- Explain the expected behavior, or why the current behavior is not sufficient
- Fill out the issue template completely

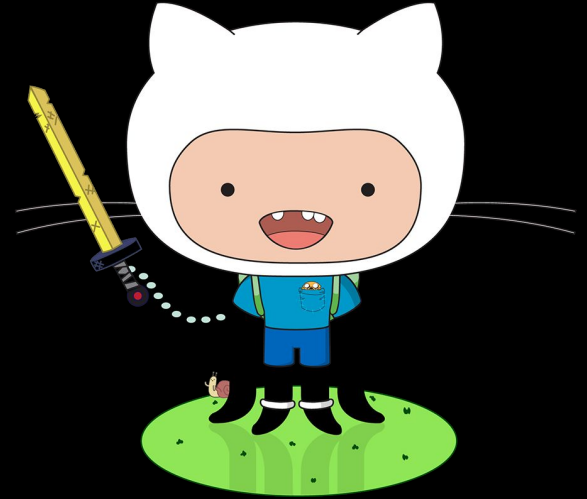
More information in our Moloch **CONTRIBUTING** file



---

# How YOU can help

- Add documentation
- Submit bugs
- Request features
- Submit pull requests
- Talk to the community on Slack



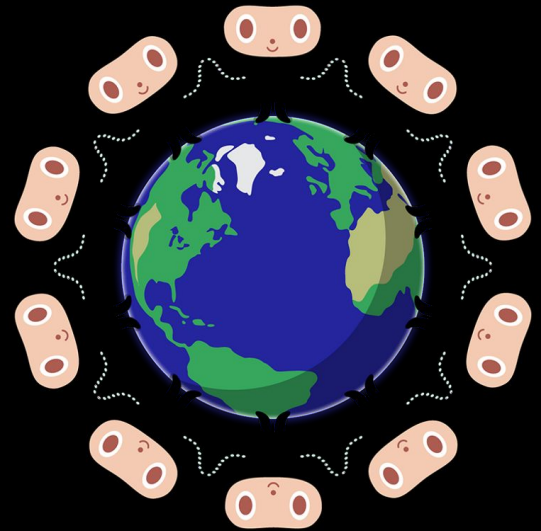
More information in our Moloch **CONTRIBUTING** file



---

# How YOU can help - Specifics

- Look through issues - good first issue tag
- Contribute sample rules
- Provide anonymized sample PCAPs
- Looking for someone who enjoys packaging!




More information in our Moloch **CONTRIBUTING** file







# Slack Community

- **Very active Slack community**
  - 728 ➔ 1052 users
  - ~80 ➔ ~100 weekly active users
  - 1k-1.5k messages sent weekly
- **Discuss bugs and feature requests**
- **Help users with questions**


 **andywick** 🍷 11:18 AM  
We now have a Moloch Video Playlist on youtube  
<https://www.youtube.com/playlist?list=PLXXo-3b5ZQ1jk2wk9lyoxoGyqZq5cT6Hq> Elyse has made lots of feature demos, and I have one Architecture video. Thanks to @Rosalie for the motivation and getting them published. Welcome feedback. (edited)


👍 5 🐼 2 🐼 3 🐼 4 🐼 3 🐼 2 🐼 2 🐼 3


 **Esben** 4:07 PM  
thanks


 **ben mcdowall** 2:55 PM  
Thanks :)



 **John Lim** 11:39 AM  
Thank you, it works


 **remco** 4:04 AM  
that solved it, thanks.


 **PRChiou** 9:53 PM  
thank you andy!


 **DW** 1:14 PM  
ah nice thanks

 **gradius** 6:14 PM  
Moloch is utilized as more of a "We really need PCAPs" to put a timeline together in great detail or "we want to confirm what we're seeing from other tools"  
Which by the way, it does wonderfully, so thank you everyone who works on it ❤️

 **art** 🐼 3:09 PM  
 **tlacuache** 3:10 PM  
ah yeah that's perfect  
schweet  
very cool. that'll be in like 1.7.1 or something?

 **elyse** 🐼 3:13 PM  
yup

 **tlacuache** 3:14 PM  
**amazing**  
Posted using /giphy | GIF by chescaleigh (1 MB) ▾



^ 1

---

# Open Source Community

- Improved documentation
- People are having their own Moloch meetups
- More PRs and people interested in contributing
- More feature requests and bug reports
- More STARS
  - 2880 ➔ 3406 in the past year
- Want another contributor besides just us



---

# Moloch Principles - WIP

<b>Full Packet Capture</b>	Provide full packet capture of IP packets with fast metadata searching and easy retrieval of packets (supporting non IP packets in progress) - Moloch is not an IDS/NIDS/NSM
<b>Large Scale</b>	Support 100Gbps+ deployments easily
<b>Sessions</b>	Group packets into sessions when appropriate, allowing for less data to be stored in ES and faster searches
<b>Useful Metadata</b>	Not fully decoding every packet or every protocol - not replacing wireshark or other tools
<b>Open</b>	Remain open source - will only require open source Elasticsearch features, will be transparent on features/issues/bugs



---

# Questions?

