



# RITA

Real Intelligence Threat Analytics

## CHEAT SHEET

This document is a quick reference guide to commonly used RITA commands and arguments. Additional RITA information and installation files can be found at: <https://github.com/activecm/rita>

### CONFIGURATION

| Command                                      | Description                                |
|--|--|
| <code>sudo nano /etc/rita/config.yaml</code> | RITA configuration file.                   |
| <code>rita test-config</code>                | Check the configuration file for validity. |

### INSTALLATION

| Command   | Description   |
|---|---|
| <code>sudo chmod +x ./install.sh</code>                       | Make the install file executable.   |
| <code>sudo ./install.sh</code>                                | Install RITA as well as supported versions of Zeek and MongoDB.                   |
| <code>sudo ./install.sh --disable-zeek --disable-mongo</code> | Install RITA only, without Zeek or MongoDB. You can use these flags individually. |

### IMPORTING AND ANALYZING DATA

| Command   | Description   |
|---|---|
| <code>mergcap -w outfilename.pcap infilename1.pcap infilename2.pcap</code>        | Merge multiple PCAP files into one PCAP file.                                       |
| <code>zeek -r filename.pcap local "Log::default_rotation_interval = 1 day"</code> | Generate Zeek logs from a PCAP file.  |
| <code>rita import path/to/your/zeek_logs datasetname</code>                       | One-off dataset import.   |
| <code>rita import --rolling /path/to/your/zeek_logs datasetname</code>            | Rolling datasets allow you to progressively analyze log data over a period of time. |
| <code>/opt/zeek/logs/&lt;date&gt;</code>  | Default Zeek logs directory.  |

### EXAMINING DATA

| Command  | Description  |
|--|--|
| <code>rita list</code>   | Print the datasets currently stored.                         |
| <code>rita show-beacons -H datasetname   less -S</code>          | Print hosts which show signs of C2 software.                 |
| <code>rita show-beacons-fqdn -H datasetname   less -S</code>     | Print hosts which show signs of C2 software (FQDN Analysis). |
| <code>rita show-strobes -H datasetname   less -S</code>          | Print strobe (fast beacon) information.                      |
| <code>rita show-long-connections -H datasetname   less -S</code> | Print long connections and relevant information.             |
| <code>rita show-useragents -H datasetname   less -S</code>       | Print user agent information.                                |
| <code>rita show-exploded-dns -H datasetname   less -S</code>     | Print DNS analysis. Exposes covert DNS channels.             |
| <code>rita show-bl-hostnames -H datasetname   less -S</code>     | Print blacklisted hostnames which received connections.      |
| <code>rita show-bl-source-ips -H datasetname   less -S</code>    | Print blacklisted IPs which initiated connections.           |
| <code>rita show-bl-dest-ips -H datasetname   less -S</code>      | Print blacklisted IPs which received connections.            |
| <code>rita html-report datasetname</code>                        | Create an HTML report for an analyzed database.              |
| <code>rita delete datasetname</code>                             | Delete database/dataset.                                     |

### FILTERING RESULTS

| Command   | Description  |
|---|--|
| <code>rita show-beacons datasetname   grep -v -w -F -f exclude-beacons.txt</code>             | Place IP addresses to exclude in this text file, one per line. |
| <code>rita show-strobes datasetname   grep -v -w -F -f exclude-strobes.txt</code>             | Place IP addresses to exclude in this text file, one per line. |
| <code>rita show-long-connections datasetname   grep -v -w -F -f exclude-longconns.txt</code>  | Place IP addresses to exclude in this text file, one per line. |
| <code>rita show-bl-hostnames datasetname   grep -v -w -F -f exclude-bl-hostnames.txt</code>   | Place IP addresses to exclude in this text file, one per line. |
| <code>rita show-bl-source-ips datasetname   grep -v -w -F -f exclude-bl-source-ips.txt</code> | Place IP addresses to exclude in this text file, one per line. |
| <code>rita show-bl-dest-ips datasetname   grep -v -w -F -f exclude-bl-dest-ips.txt</code>     | Place IP addresses to exclude in this text file, one per line. |

