Brim / Zeek Commands

Show all Zeek streams - *Counts all records by the Zeek streams and sorts them, highest to lowest*

```
count() by _path | sort -r
```

Show all DNS queries

```
_path=dns | count() by query | sort -r
```

Showing only SMB and DCE/RPC activity

```
_path=dce_rpc OR _path=smb_mapping OR _path=smb_files
```

Displays the DCE/RPC, smb_mapping or smb_files Zeek streams.

```
_path=~smb* OR _path=dce_rpc
```

Showing all files seen on the network

```
filename!=null
```

Showing all http requests

```
_path=http | count() by uri | sort -r
```

Show the unique IP address pairings in conn.log.

```
cut id.orig_h, id.resp_h | sort | uniq
```

Show the count of all unique connection pairings between hosts

```
_path=conn | cut id.orig_h, id.resp_h | sort id.orig_h, id.resp_h | uniq -c | sort -r
```

Show a count of all network connections including associated destination port and service protocol

```
_path=conn | cut id.orig_h, id.resp_h, id.resp_p, service | sort id.resp_p | uniq -c | sort -r
```

Show the Top 10 connections between hosts, by data received

```
_path=conn | put total_bytes = orig_bytes + resp_bytes | sort -r total_bytes | head 10 | cut uid, id, orig_bytes, resp_bytes, total_bytes
```