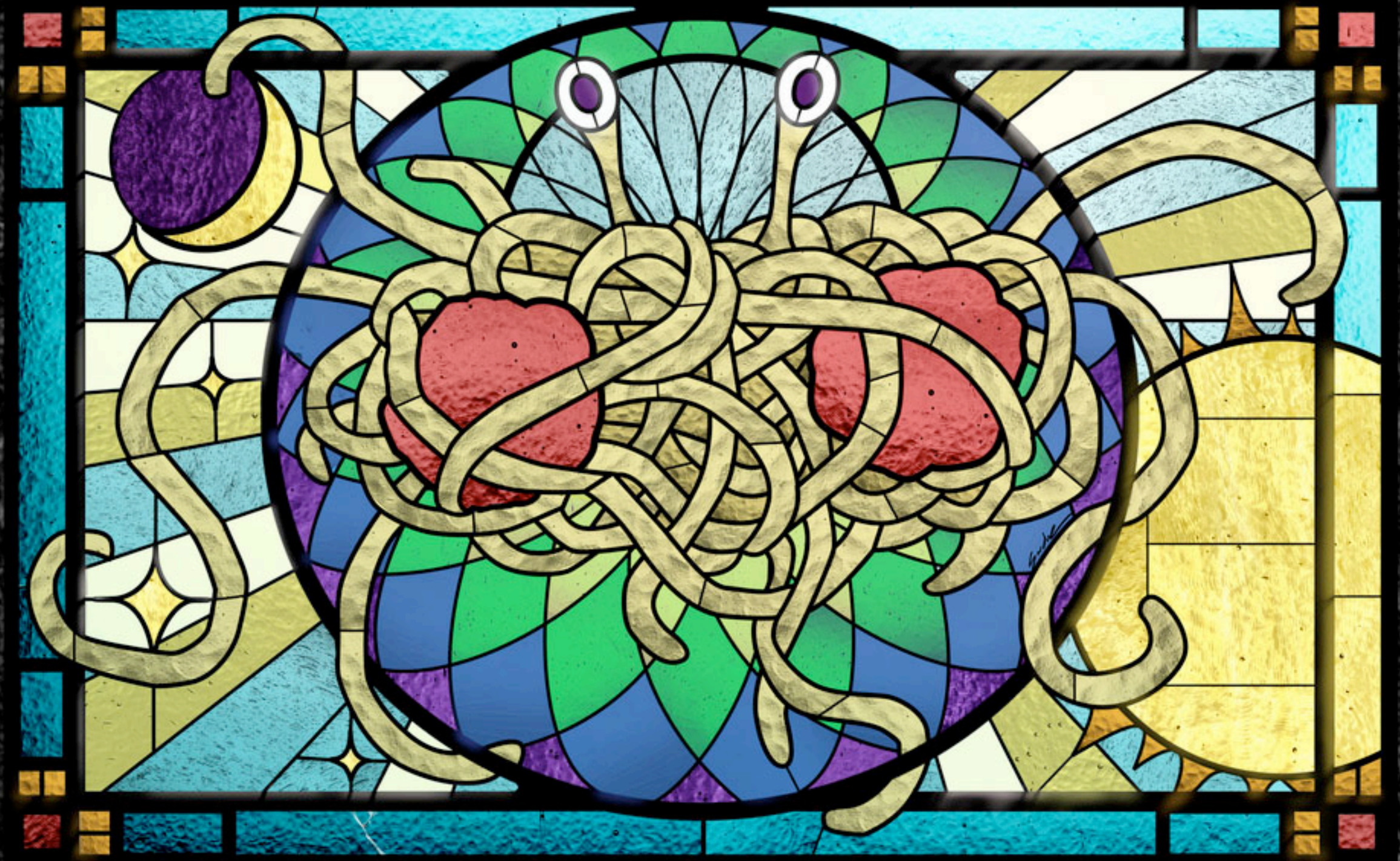
Logs, Damn Logs and Statistics

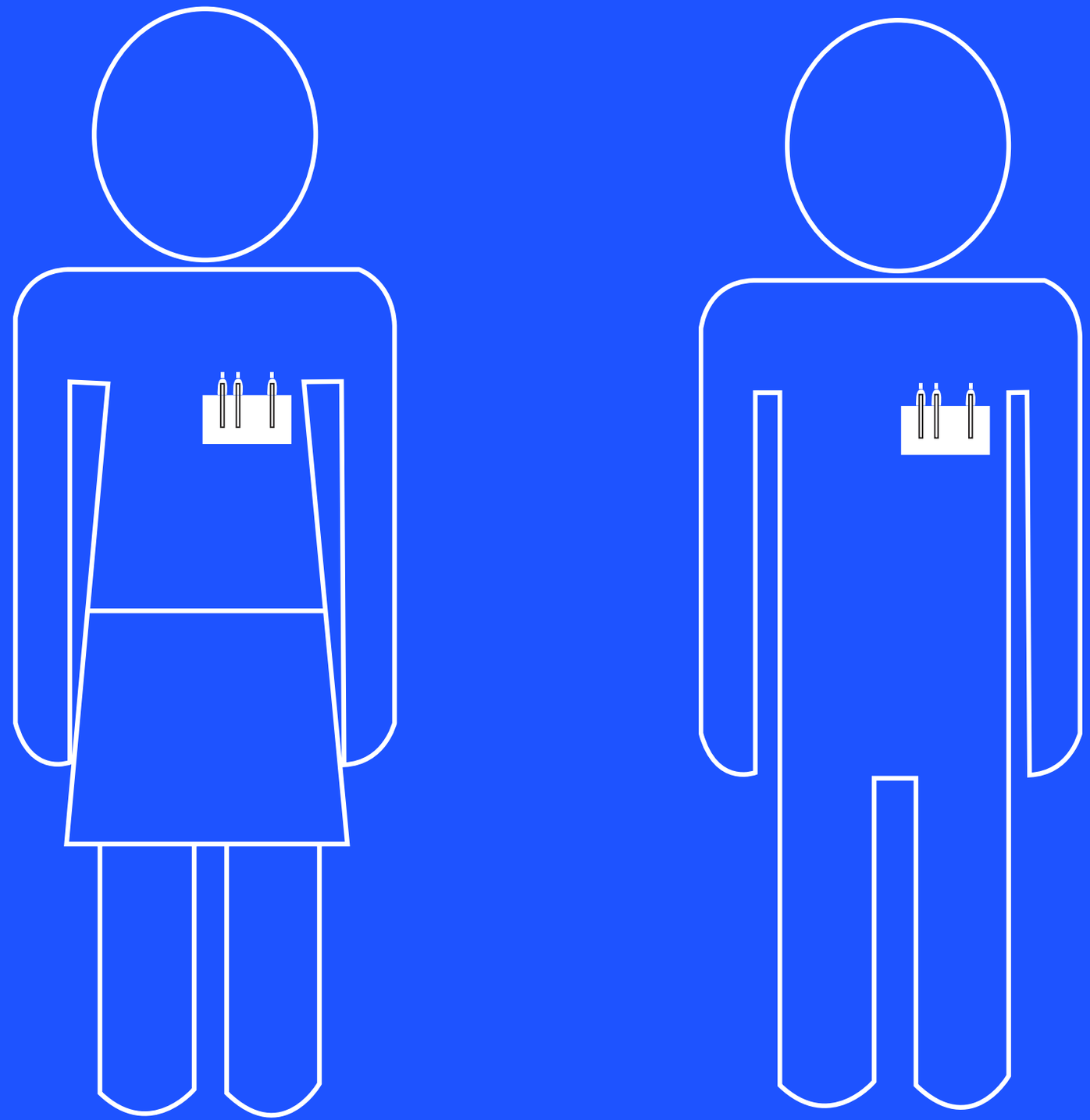
Edward Marczak

marczak@radiotope.com

@marczak

http://radiotope.com/node/172





"I DON'T KNOW HOW TO READ LOGS."

"I'M NOT A TERMINAL PERSON."

“I HATE TEXT.”

Untitled

Helvetica | Regular | 24 | 1.0

This is a text document.

I'm typing in TextEdit.

Yay! \o/

Apr 24 20:51:58 Skara-Brae 1PasswordAgent[173]: [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" UserInfo=0x100356080 {NSLocalizedDescription=Socket closed by remote peer}

Apr 24 20:54:41 Skara-Brae sandboxd[13664] ([13658]): TextEdit(13658) deny file-read-data /Users/marczak/Dropbox/Library/FontCollections

Apr 24 20:54:59 Skara-Brae 1PasswordAgent[173]: [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" UserInfo=0x10181e500 {NSLocalizedDescription=Socket closed by remote peer}

Apr 24 20:56:00 Skara-Brae 1PasswordAgent[173]: [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" UserInfo=0x101a18a0 {NSLocalizedDescription=Socket closed by remote peer}

Apr 24 20:56:56 Skara-Brae Keynote[9399]: kCGErrorIllegalArgument: _CGSFindSharedWindow: WID -1

Apr 24 20:56:56 Skara-Brae Keynote[9399]: kCGErrorFailure: Set a breakpoint @ CGErrorBreakpoint() to catch errors as they are logged.

Apr 24 20:56:56 Skara-Brae Keynote[9399]: kCGErrorIllegalArgument: CGSSetWindowShadowAndRimParametersWithStretch: Invalid window 0xffffffff

Apr 24 20:57:00 Skara-Brae 1PasswordAgent[173]: [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" UserInfo=0x101a1ab30 {NSLocalizedDescription=Socket closed by remote peer}

Al Yankovic @alyankovic 22 Apr

Spent the weekend camping in the desert, surrounded by natural beauty. But no Wi-Fi or 3G. #TheHORROR

Al Yankovic @alyankovic 21 Apr

"Life is nothing but a series of tweetable moments" - René Descartes

Al Yankovic @alyankovic 20 Apr

“Hey, what’s a good rhyme for ‘El Paso’? Oh wait, I’ve got it – ‘hassle’!” – Steve Miller Band brainstorming session

Al Yankovic @alyankovic 19 Apr

Have you guys heard about all the amazing coincidences between the lives of president Abraham Lincoln and ‘90s MTV VJ Kennedy? #MindBlown

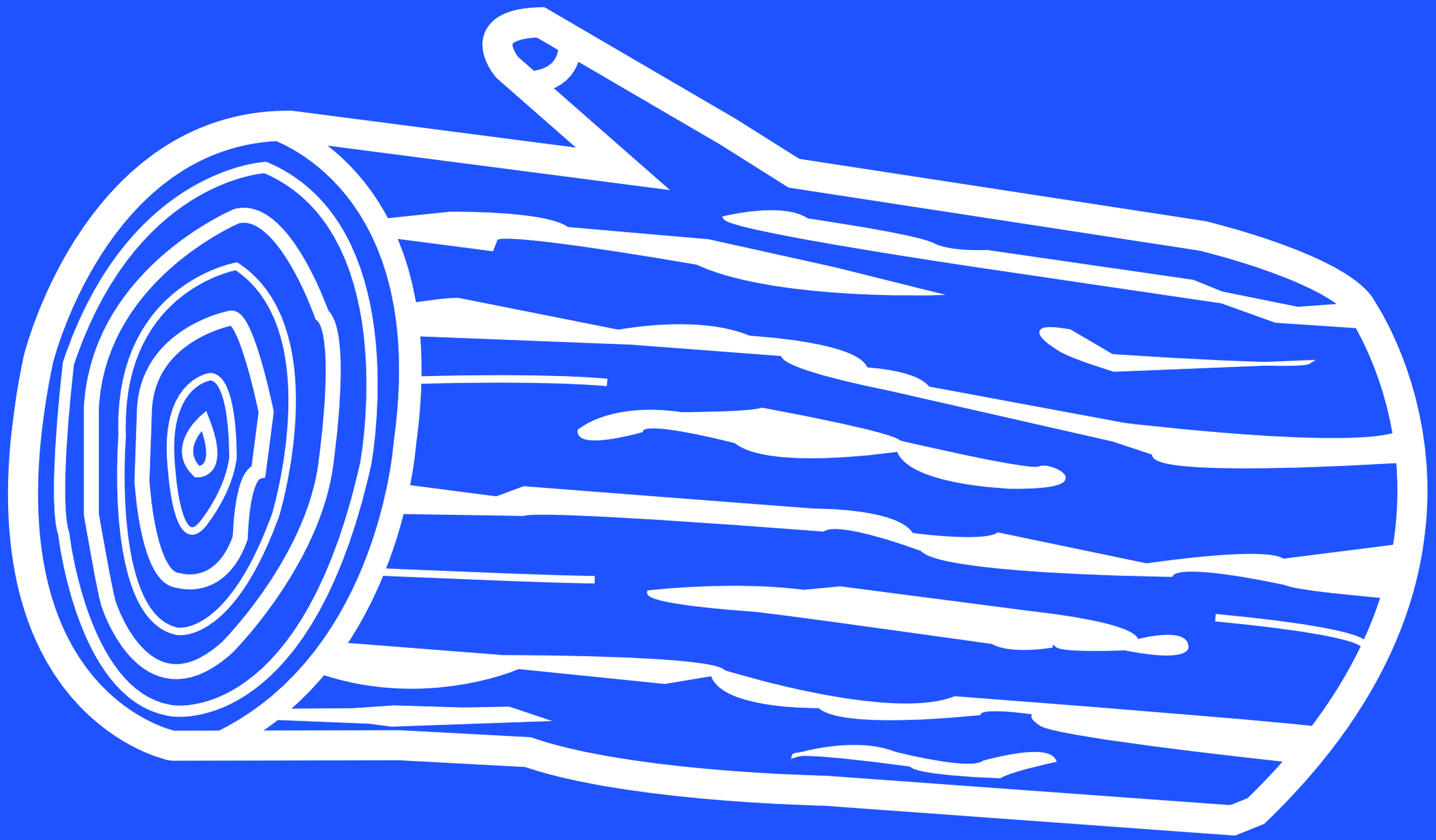
Al Yankovic @alyankovic 18 Apr

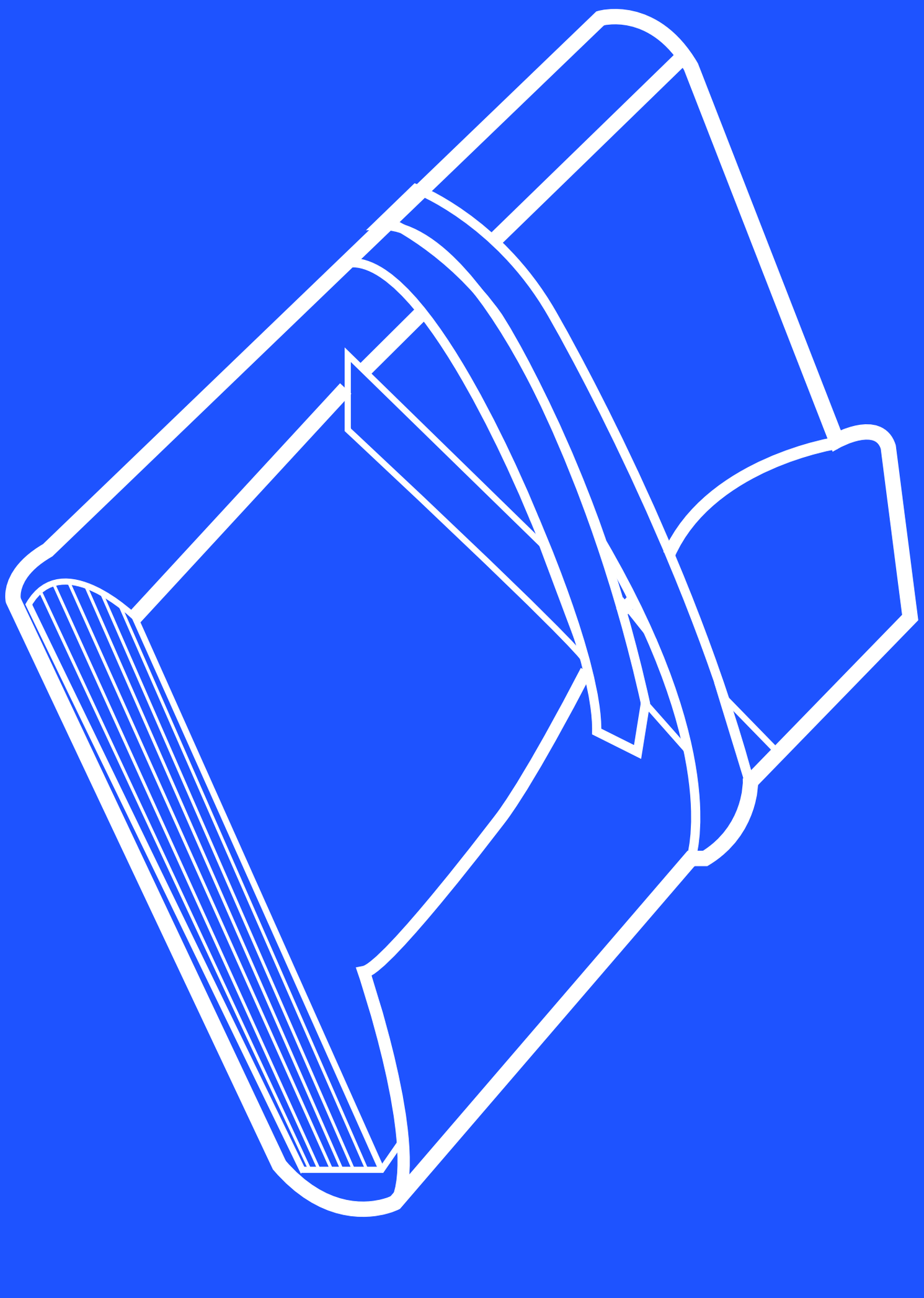
Such sad news. RIP Dick Clark. twitpic.com/9bd5uf

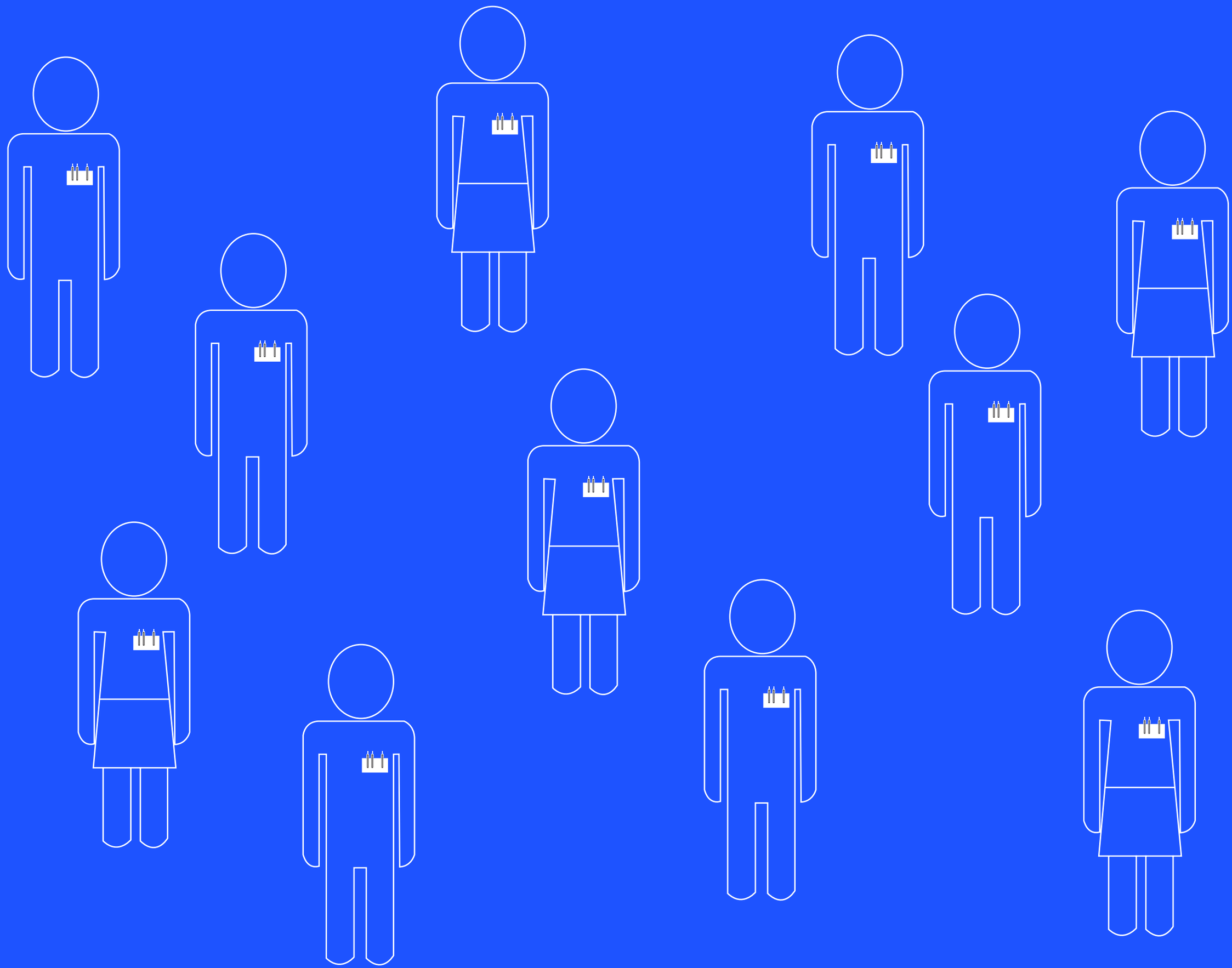
View photo

Al Yankovic @alyankovic 18 Apr

You can't walk through hot lava, even if you're wearing ice cube shoes. #ThingsIveLearnedFromMyKid







Parsing Tools

- grep

- sed

- awk

- any regex

Mar 9 08:32:37 Skara-Brae configd[15]: network configuration changed.

Mar 9 08:32:37 } Timestamp

Skara-Brae } Hostname

configd[15]: } Process

network configuration changed. } Message

Where are Log Files Stored?

Traditionally: /var/log

Apple adds: /Library/Logs
~/Library/Logs

How did I get Here?

- Direct file access
- syslog message

Direct Write

```
echo "Starting application" >> /logs/myapp.log
echo "Something happened" >> /logs/myapp.log
echo "Ending application" >> /logs/myapp.log
```

Direct Write

```
echo "$(date) ${0}: App started" >> /logs/myapp.log

APPNAME=${0}
LOGFILE="/logs/${APPNAME}.log"
```

Direct Write

```
APPNAME=${0}
LOGFILE="logs/${APPNAME}.log"

function log{
  echo "$(date) ${APPNAME}: ${1}" >> ${LOGFILE}
}
```

Syslog

Syslog

```
$ grep syslog /etc/services
syslog          514/udp #
syslog-conn     601/udp     #Reliable Syslog Service
syslog-conn     601/tcp     #Reliable Syslog Service
```

Syslog-Messages

Messages are categorized by:

Facility

Severity

Syslog-Facility

NOTICE

AUTHPRIV

REMOTEAUTH

FTP

INSTALL

INTERNAL

KERN

MAIL

Syslog-Severity

(aka Priority)

Emergency	(level 0)
Alert	(level 1)
Critical	(level 2)
Error	(level 3)
Warning	(level 4)
Notice	(level 5)
Info	(level 6)
Debug	(level 7)

Syslog

Bash: logger

Obj-C: NSLog

Python: logging module

Ruby: syslog module

/ETC/SYSLOG.CONF

Log Routing

```
$ ls -C /var/log/*.log
/var/log/fsck_hfs.log                  /var/log/opendirectoryd.log
/var/log/hdiejectd.log                 /var/log/ppp.log
/var/log/install.log                   /var/log/secure.log
/var/log/ipfw.log                      /var/log/system.log
/var/log/kernel.log                    /var/log/windowserver.log
/var/log/launchd-shutdown.log          /var/log/windowserver_last.log
/var/log/notifyd.log
```

/etc/syslog.conf

```
*.notice;authpriv,remoteauth,ftp,install,internal.none     /var/log/system.log
kern.*                                                     /var/log/kernel.log

# Send messages normally sent to the console also to the serial port.
# To stop messages from being sent out the serial port, comment out this line.
#*.err;kern.*;auth.notice;authpriv,remoteauth.none;mail.crit                /dev/
tty.serial

# The authpriv log file should be restricted access; these
# messages shouldn't go to terminals or publically-readable
# files.
auth.info;authpriv.*;remoteauth.crit                /var/log/secure.log

lpr.info                                            /var/log/lpr.log
```

/etc/syslog.conf

Facility.Priority	/path/to/logfile
ftp.*	/var/log/ftp.log
lpr.info	/var/log/lpr.log
auth.info;authpriv.*	/var/log/secure.log
*.notice;authpriv	/var/log/system.log
.	/var/log/uber.log
install.*	/var/log/install.log
install.*	@127.0.0.1:32376

Syslog-Cleaning Up

/usr/bin/newsyslog

/etc/newsyslog.conf

/var/log/ftp.log	640	5	1000	*	J
/var/log/ahwmond.log	640	5	1000	*	J
/var/log/install.log	640	5	1000	*	J
/var/log/ipfw.log	640	5	1000	*	J

Syslog-Cleaning Up

```
$ ls -l /var/log/kernel.*
/var/log/kernel.log
/var/log/kernel.log.0.bz2
/var/log/kernel.log.1.bz2
```

NEWSYSLOG[2345]: LOGFILE

TURNED OVER DUE TO SIZE>100K

Syslog-Cleaning Up

$ tail /var/log/kernel.log.0.bz2

BZh91AY&SY?? ?~0Z ??????????@A?? 4Q@?@
T?????? ???;&6?({???^?dz;?{?;?/??6w?u?[?^???M?}?>?????? &-?

???Q??p@{???\?*_C????=??>????
?s??????s??????K??????F??/G????

[? ?????3?M????

?????Q?*??{?? ??s????_w??X??@?|?p;?s????7??~??$?|?4?v? T??-W??o?o=@???u??=

??w?>??????????~

?*??(~?6}???/??|M\=Wo????\??(? }H?Q+???? ?A?)%V???Q?

Syslog-Cleaning Up

```
cat /var/log/kernel.log.0.bz2 | bunzip2 | tail -4
```

Syslog-Cleaning Up

```
bzcat /var/log/kern.log.0.bz2 | tail -4
```

Remote Syslog

```
$ grep syslog /etc/services
syslog          514/udp #
```

Remote Syslog

Facility.Priority @syslog.server.address:port

UDP?

ASL

```
defaults write /Library/
Preferences/
com.apple.ApplePushServiced
APSWriteLogs -bool TRUE
```

```
defaults write /Library/
Preferences/
com.apple.ApplePushServiced
APSLogLevel -int 7
```

odutil set log debug

SEARCH

HOW DO I

HOW DO I TAKE PICTURES

HOW DO I LOVE THEE

HOW DO I BEAT SKYRIM

HOW DO I WIN AT CHESS

How Do I ~~Get~~ To Carnegie Hall?

"You will be fooled by a trick if it involves more time, money and practice than you (or any other sane onlookers) would be willing to invest."

-Tellers, Smithsonian Magazine March 2012

http://www.smithsonianmag.com/arts-culture/Teller-Reveals-His-Secrets.html

Preview

```
/dev/rdisk2s2:     Executing fsck_hfs (version
diskdev_cmds-540.1~25).
QUICKCHECK ONLY; FILESYSTEM CLEAN

/dev/rdisk2s2: fsck_hfs run at Wed Apr 25 09:25:23 2012
/dev/rdisk2s2: ** /dev/rdisk2s2 (NO WRITE)
/dev/rdisk2s2:     Executing fsck_hfs (version
diskdev_cmds-540.1~25).
QUICKCHECK ONLY; FILESYSTEM CLEAN

/dev/rdisk2s2: fsck_hfs run at Wed Apr 25 09:25:23 2012
/dev/rdisk2s2: ** /dev/rdisk2s2 (NO WRITE)
/dev/rdisk2s2:     Executing fsck_hfs (version
diskdev_cmds-540.1~25).
QUICKCHECK ONLY; FILESYSTEM CLEAN

/dev/rdisk2s2: fsck_hfs run at Wed Apr 25 21:09:46 2012
/dev/rdisk2s2: ** /dev/rdisk2s2 (NO WRITE)
/dev/rdisk2s2:     Executing fsck_hfs (version
diskdev_cmds-540.1~25).
QUICKCHECK ONLY; FILESYSTEM CLEAN

/dev/rdisk2s2: fsck_hfs run at Wed Apr 25 21:09:57 2012
/dev/rdisk2s2: ** /dev/rdisk2s2 (NO WRITE)
/dev/rdisk2s2:     Executing fsck_hfs (version
diskdev_cmds-540.1~25).
```

Options... Test

Utilities

- cat
- gunzip/bzcat
- tail
- less/more
- syslog (ASL)

All Messages

Hide Log List | Move to Trash | Clear Display | Reload | Ignore Sender | Inspector | Insert Marker | Activity Monitor | Terminal | String Matching | Filter

SYSTEM LOG QUERIES

All Messages

DIAGNOSTIC AND USAGE INFORMATI...

Diagnostic and Usage Messages

User Diagnostic Reports

System Preferences_2012-04-02...
System Preferences_2012-04-02...
System Preferences_2012-04-02...
System Preferences_2012-04-02...
System Preferences_2012-04-02...
System Preferences_2012-04-02...
System Preferences_2012-04-03...
System Preferences_2012-04-03...
System Preferences_2012-04-03...
System Preferences_2012-04-03...
System Preferences_2012-04-03...
vzwwirelessd_2012-04-04-1052...
vzwwirelessd_2012-04-12-0804...
vzwwirelessd_2012-04-12-0806...
vzwwirelessd_2012-04-17-0811...
vzwwirelessd_2012-04-17-2018...

System Diagnostic Reports

FILES

system.log
kernel.log

```
6:08:12 PM CrashPlan menu bar: CPMessageHandler Asked to change 'isConnected' status for GUID 60011405, but I couldn't find any compu
6:08:13 PM kernel: utun_ctl_connect: creating interface utun0
6:08:13 PM configd: en3: DHCP duplicate configured service
6:08:13 PM configd: en3: AUTOMATIC-V6 duplicate configured service
6:08:19 PM CrashPlan menu bar: CPMessageHandler Asked to change 'isConnected' status for GUID 390468735873843458, but I couldn't find
6:08:18 PM SafariDAVClient: ServerNotifications: Setting delegate to APSD
6:08:19 PM SafariDAVClient: Subscription request completed
6:08:21 PM SafariDAVClient: Subscription request completed
6:08:28 PM SafariDAVClient: Subscription request completed
6:08:51 PM 1PasswordAgent: [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" U
6:09:29 PM CrashPlan menu bar: CPMessageHandler Asked to change 'isConnected' status for GUID 60010804, but I couldn't find any compu
6:09:52 PM 1PasswordAgent: [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" U
6:09:59 PM com.smithmicro.vzwwirelessd: Apr 20 18:09:59 Skara-Brae com.smithmicro.vzwwirelessd[4769] <Info>: Shutting down
6:10:52 PM 1PasswordAgent: [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" U
6:11:53 PM 1PasswordAgent: [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" U
6:12:53 PM 1PasswordAgent: [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" U
6:12:58 PM CrashPlan menu bar: CPMessageHandler Asked to change 'isConnected' status for GUID 420604, but I couldn't find any compute
6:13:44 PM CrashPlan menu bar: CPMessageHandler Asked to change 'isConnected' status for GUID 402402, but I couldn't find any compute
6:13:54 PM 1PasswordAgent: [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" U
6:13:59 PM CrashPlan menu bar: CPMessageHandler Asked to change 'isConnected' status for GUID 421202, but I couldn't find any compute
6:14:54 PM 1PasswordAgent: [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" U
6:15:55 PM 1PasswordAgent: [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" U
6:16:55 PM 1PasswordAgent: [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" U
6:17:56 PM 1PasswordAgent: [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" U
6:18:56 PM 1PasswordAgent: [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" U
6:19:43 PM SyncServer: [0x10b616e60] |DataManager|Warning| Client com.apple.DotMacSync image file path /System/Library/PreferencePane
```

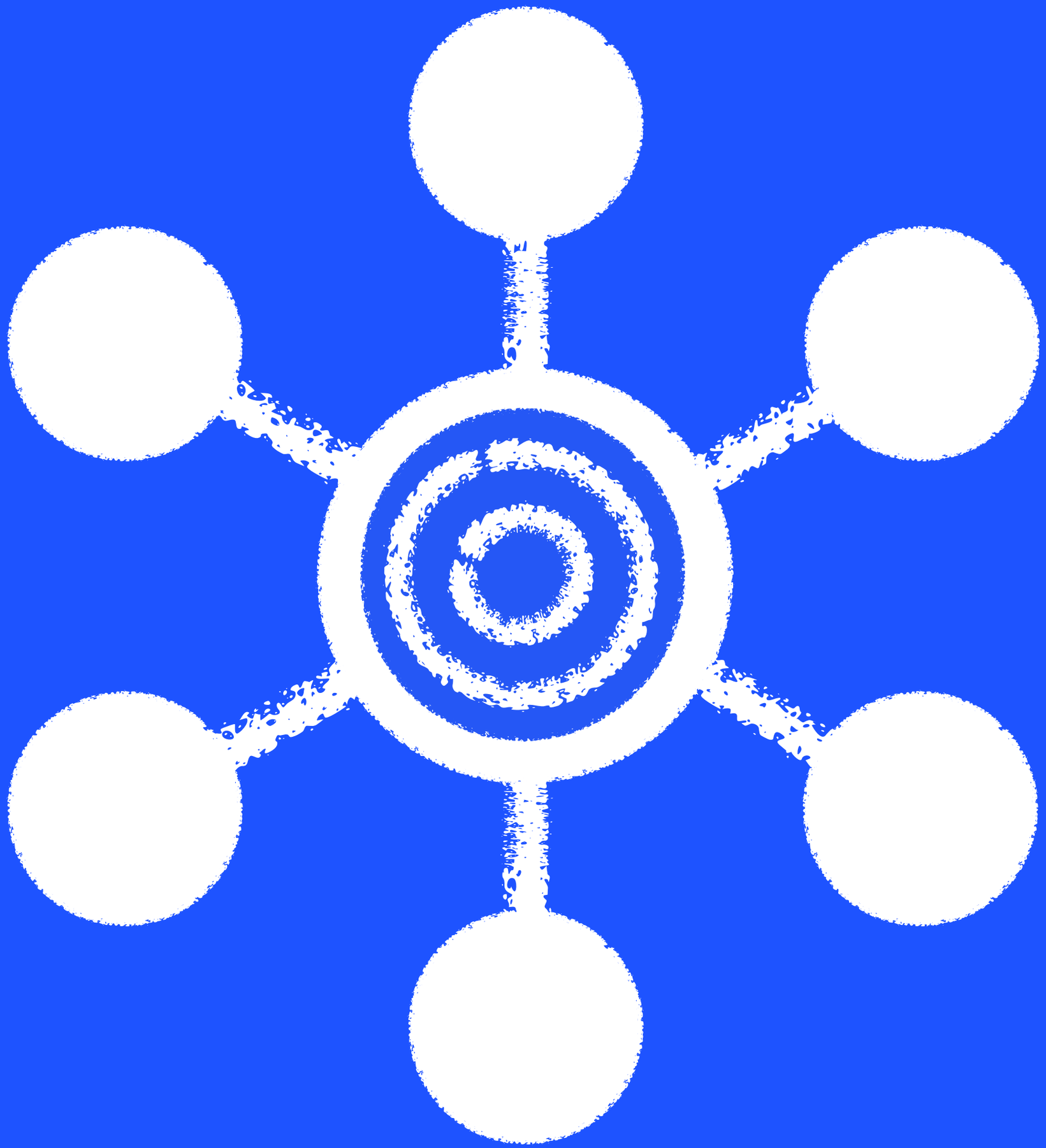
4000 messages from 4/18/12 12:00:36 PM to 4/20/12 6:29:01 PM

Earlier | Later

Console

WHAT HAVE I

DONE?



SPLUNK

search

All time

All indexed data

This lists all of the data you have loaded into your default indexes. Add more data.

Events indexed	Earliest event	Latest event
86,764	Sun Mar 11 18:55:00 2012	Sat Apr 28 17:17:25 2012

Sources (≥ 1)

	source	Count	Last Update
1	udp:514	86,763	Sat Apr 28 17:17:25 2012

Source types (≥ 1)

	sourcetype	Count	Last Update
1	syslog	86,764	Sat Apr 28 17:17:25 2012

Hosts (≥ 10)

	host	Count	Last Update
1	127.0.0.1	29,458	Sat Apr 28 17:17:25 2012
2	192.168.100.219	25,429	Wed Mar 21 23:28:48 2012
3	192.168.100.222	11,801	Wed Mar 28 06:58:18 2012

Add Data to Splunk

Choose a Data Type

A file or directory of files
Syslog
Windows event logs
Windows Registry
Windows performance metrics
Unix/Linux logs and metrics
File integrity monitoring
Configuration files
OPSEC LEA
Cisco device logs
IIS logs
Apache logs
WebSphere logs, metrics and other data
Any other data...

Or Choose a Data Source

From files and directories
From a TCP port
From a UDP port
Run and collect the output of a script

Is your data on another machine, besides this Splunk server? Install Splunk's universal forwarder on that machine and tell it to send the data to this Splunk server.

splunk> Search

Administrator | App | Manager | Alerts | Jobs | Logout

Summary | Search | Status | Dashboards & Views | Searches & Reports | Help | About

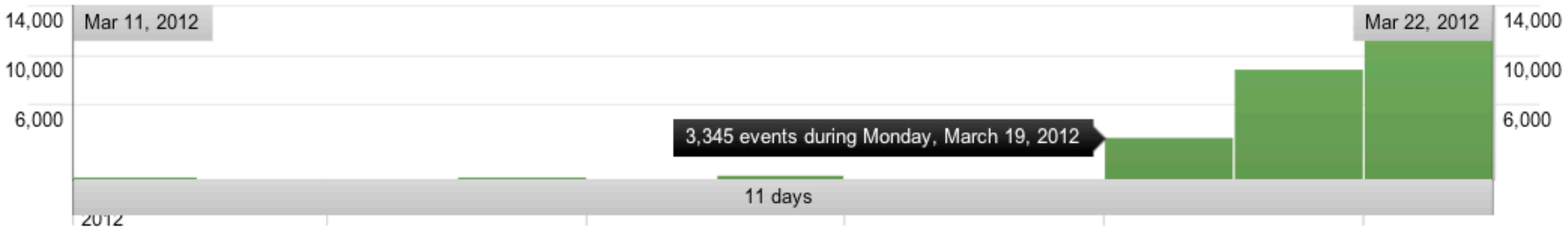
Search

host="192.168.100.219" All time

25,429 matching events

Save | Create

Hide | Zoom out | Zoom to selection | Deselect | Linear scale



Field discovery is: On

Hide

3 selected fields Edit

host (1)

source (1)

sourcetype (1)

25,429 events over all time

Export | « prev 1 2 3 4 5 6 7 8 9 10 next » | 10 per page

Options

1 3/21/12 11:28:48.000 PM Mar 21 23:28:48 192.168.100.219 Mar 21 23:29:03 Paws racoon[132]: [132] INFO: fe80::1%lo0[4500] used as isakmp port (fd=21)

Field discovery is: On

Hide

3 selected fields Edit

- a host (2)
- a source (1)
- a sourcetype (1)

8 interesting fields

- a index (1)
- # linecount (1)
- # pid (3)
- a process (3)
- a punct (6)
- a splunk_server (1)
- # timeendpos (1)
- # timestartpos (1)

View all 23 fields

1,081 events in the last day (since 5:19:48 PM April 27, 2012)

Export « prev 1 2 3 4 5 6 7 8 9 10 next » 10 per page

Options

1 4/28/12 5:19:18.000 PM
Apr 28 17:19:18 192.168.100.218 Apr 28 17:19:18 Skara-Brae 1PasswordAgent[173]: [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" UserInfo=0x101a42eb0 {NSLocalizedDescription=Socket closed by remote peer}
host=192.168.100.218 | sourcetype=syslog | source=udp:514

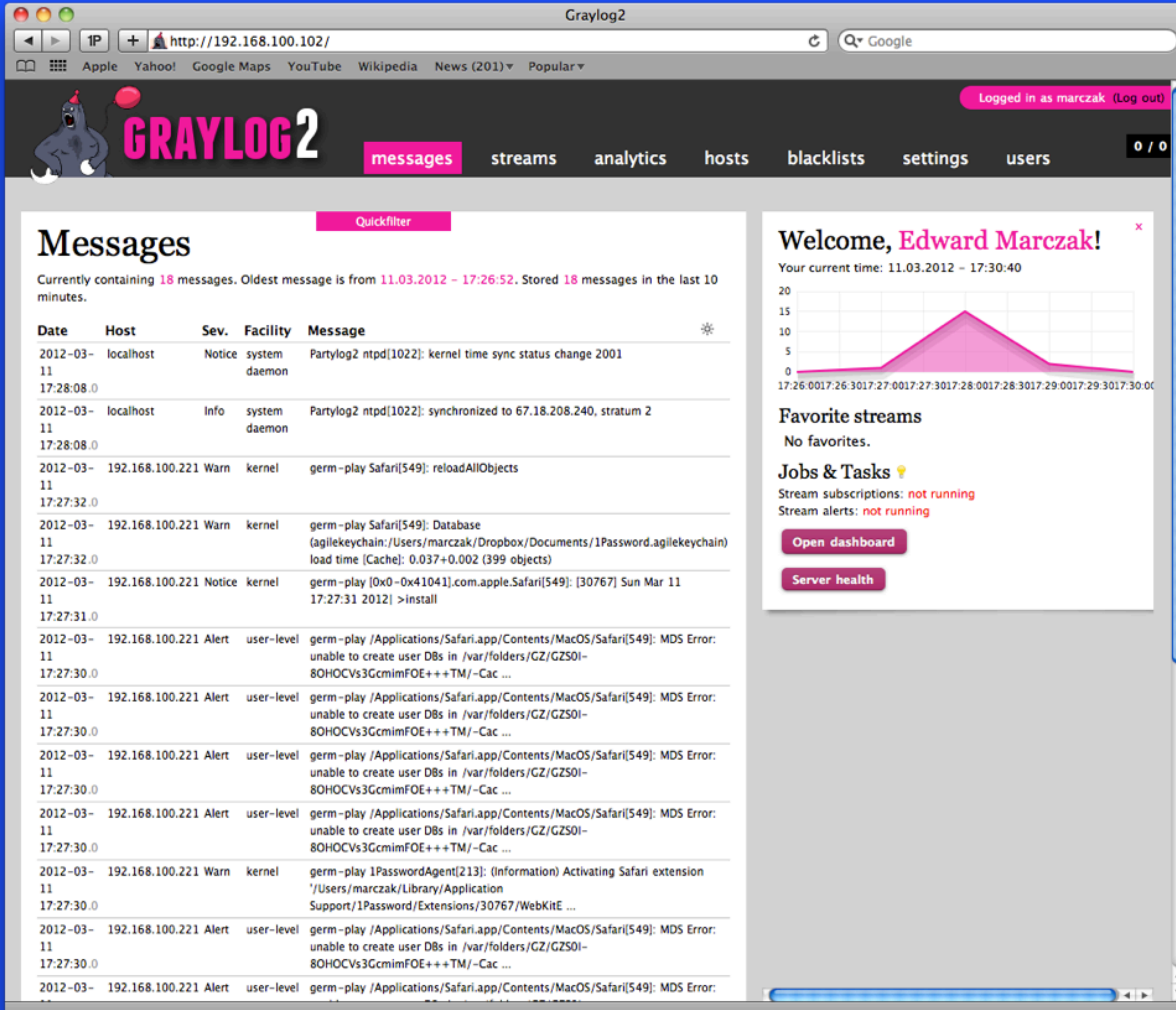
2 4/28/12 5:18:19.000 PM
Apr 28 17:18:19 127.0.0.1 Apr 28 17:18:19 Marczak-Familys-Mac-mini com.apple.usbmuxd[53]: HandleUSBMuxConnect Client 0x101c79d20-iTunes/com.apple.iTunes requesting attach to 0x361:62078 failed, no such device
host=127.0.0.1 | sourcetype=syslog | source=udp:514

3 4/28/12 5:18:19.000 PM
Apr 28 17:18:19 127.0.0.1 Apr 28 17:18:19 Marczak-Familys-Mac-mini AppleMobileDeviceHelper[2497]: 2497:2904531648|AppleMobileDeviceHelper.m:_getDisabledDataClassNamesFromLockdo ERROR: Could not find a device with the target identifier d56d4bc548bd7e996d2927731f22f7c20fc27662. Assuming there are no disabled data
host=127.0.0.1 | sourcetype=syslog | source=udp:514

4 4/28/12 5:18:17.000 PM
Apr 28 17:18:17 192.168.100.218 Apr 28 17:18:17 Skara-Brae 1PasswordAgent[173]: [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" UserInfo=0x101b06610 {NSLocalizedDescription=Socket closed by remote peer}

```
error OR failed OR severe OR ( sourcetype=access_* ( 404 OR 500 OR 503 ) )
```

GRAYLOG



Graylog2
http://192.168.100.102/
Google
Apple Yahoo! Google Maps YouTube Wikipedia News (201) Popular
GRAYLOG2
Logged in as marczak (Log out)
messages streams analytics hosts blacklists settings users
0 / 0
Quickfilter
Messages
Currently containing 18 messages. Oldest message is from 11.03.2012 - 17:26:52. Stored 18 messages in the last 10 minutes.
Date Host Sev. Facility Message
2012-03-11 17:28:08.0 localhost Notice system daemon Partylog2 ntpd[1022]: kernel time sync status change 2001
2012-03-11 17:28:08.0 localhost Info system daemon Partylog2 ntpd[1022]: synchronized to 67.18.208.240, stratum 2
2012-03-11 17:27:32.0 192.168.100.221 Warn kernel germ-play Safari[549]: reloadAllObjects
2012-03-11 17:27:32.0 192.168.100.221 Warn kernel germ-play Safari[549]: Database (agilekeychain:/Users/marczak/Dropbox/Documents/1Password.agilekeychain) load time [Cache]: 0.037+0.002 (399 objects)
2012-03-11 17:27:31.0 192.168.100.221 Notice kernel germ-play [0x0-0x41041].com.apple.Safari[549]: [30767] Sun Mar 11 17:27:31 2012| >install
2012-03-11 17:27:30.0 192.168.100.221 Alert user-level germ-play /Applications/Safari.app/Contents/MacOS/Safari[549]: MDS Error: unable to create user DBs in /var/folders/GZ/GZSOI-8OHOCVs3GcmimFOE+++TM/-Cac ...
2012-03-11 17:27:30.0 192.168.100.221 Alert user-level germ-play /Applications/Safari.app/Contents/MacOS/Safari[549]: MDS Error: unable to create user DBs in /var/folders/GZ/GZSOI-8OHOCVs3GcmimFOE+++TM/-Cac ...
2012-03-11 17:27:30.0 192.168.100.221 Alert user-level germ-play /Applications/Safari.app/Contents/MacOS/Safari[549]: MDS Error: unable to create user DBs in /var/folders/GZ/GZSOI-8OHOCVs3GcmimFOE+++TM/-Cac ...
2012-03-11 17:27:30.0 192.168.100.221 Alert user-level germ-play /Applications/Safari.app/Contents/MacOS/Safari[549]: MDS Error: unable to create user DBs in /var/folders/GZ/GZSOI-8OHOCVs3GcmimFOE+++TM/-Cac ...
2012-03-11 17:27:30.0 192.168.100.221 Warn kernel germ-play 1PasswordAgent[213]: (Information) Activating Safari extension '/Users/marczak/Library/Application Support/1Password/Extensions/30767/WebKitE ...
2012-03-11 17:27:30.0 192.168.100.221 Alert user-level germ-play /Applications/Safari.app/Contents/MacOS/Safari[549]: MDS Error: unable to create user DBs in /var/folders/GZ/GZSOI-8OHOCVs3GcmimFOE+++TM/-Cac ...
2012-03- 192.168.100.221 Alert user-level germ-play /Applications/Safari.app/Contents/MacOS/Safari[549]: MDS Error:
Welcome, Edward Marczak!
Your current time: 11.03.2012 - 17:30:40
20
15
10
5
0
Favorite streams
No favorites.
Jobs & Tasks
Stream subscriptions: not running
Stream alerts: not running
Open dashboard
Server health

Graylog2

http://192.168.100.102/analytics

Apple Yahoo! Google Maps YouTube Wikipedia News (322) Popular

GRAYLOG2

messages streams analytics hosts blacklists settings users

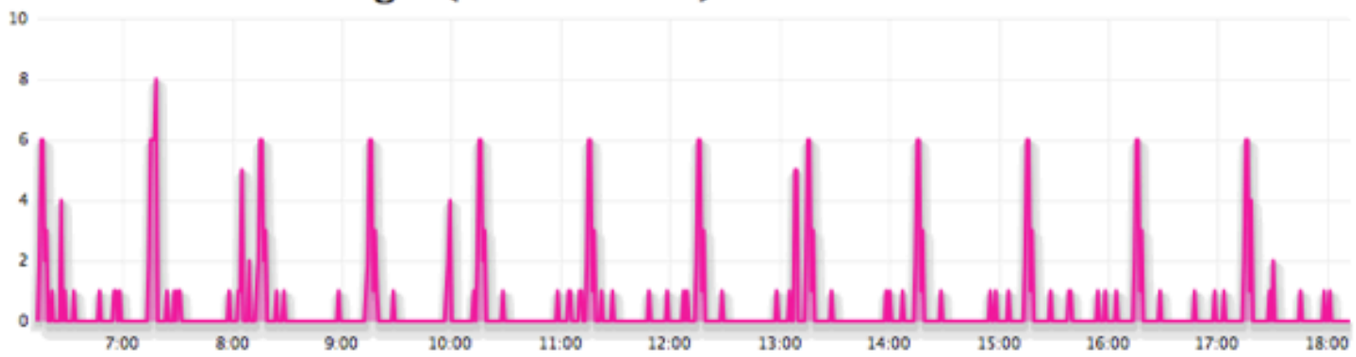
Logged in as marczak (Log out)

0 / 0

marczak #

Analytics

Count of new messages (last 12 hours.)



Count of number of messages from all hosts. Select a range with your mouse and click the button to see all messages in the selected range.

12 Hours Days Weeks Update graph

The analytics shell

This shell allows you to query all messages in a structured and dynamic way. The complete syntax description and examples are documented in the Graylog2 wiki.

Selectors
- all
- stream([stream_id])
- streams([stream_id], [stream_id], ...)

Operators
- find
- count
- distribution

Conditional operators
- < >
- <= >=
- = !=

Data types
- String: "something"
- Integer: 9001

Additional fields must be prefixed with an underscore. Find queries are limited to 500 results. Use the quickfiltering if you need more and pagination.

The stream() and streams() selectors also take stream shortnames as parameters.

The fields **message and full_message** are broken to terms. This means that searches on them do not mean *equals [search term]* but *contains [search term]*.

Examples:
- all.find()
- all.count(host = "example.org", _http_response_code = 204)
- all.distribution([host], _http_response_code > 500)
- stream(some_stream).distribution([_processed_controller], :_http_response_code = 500)

Hosts

Quick jump to host: Go!

Monitoring 6 hosts.

Quickfilter

Messages

Currently containing 35.719 messages. Oldest message is from 25.04.2012 - 12:54:15. Stored 13 messages in the last 10 minutes.

Message: ?rror or ?arn

Timeframe:

Facility:

Severity: or higher

Host:

Add additional field | Run filter

Quickfilter hit 83 messages.

Date	Host	Sev.	Facility	Message
2012-04-29 14:40:07.0	192.168.100.222	Notice	user-level	ladmins-MacBook-Pro mdworker[1820]: zip importer encountered an error (2) scanning "/Users/emily/Music/iTunes/Mobile Applications/com.newtoyinc.WordsWi ...
2012-04-29 14:39:49.0	192.168.100.222	Notice	user-level	ladmins-MacBook-Pro mdworker[1820]: zip importer encountered an error (2) scanning "/Users/emily/Music/iTunes/Mobile Applications/com.younggam.LockScre ...
2012-04-29 14:38:37.0	192.168.100.222	Notice	user-level	ladmins-MacBook-Pro mdworker[1820]: zip importer encountered an error (2) scanning "/Users/emily/Music/iTunes/Mobile Applications/com.fabiociotoli.twee ...
2012-04-29 14:38:08.0	192.168.100.222	Notice	user-level	ladmins-MacBook-Pro mdworker[1820]: zip importer encountered an error (2) scanning "/Users/emily/Music/iTunes/Mobile Applications/com.google.Translate. ...

x

Message
w5B2HI_gSkaJ_BUCpF7BQw

```
Partylog2 CRON[17154]: (root) CMD ( cd / && run-
parts --report /etc/cron.hourly)
```

In which terms was this message broken to?

From: localhost

Date: 2012-04-29 14:17:01 -0400

Severity: Info

Facility: clock

Full message:

```
<78>Apr 29 14:17:01 Partylog2 CRON[17154]: (root)
CMD ( cd / && run-parts --report
/etc/cron.hourly)
```

Permalink

DIY

Language of choice

+ Web service

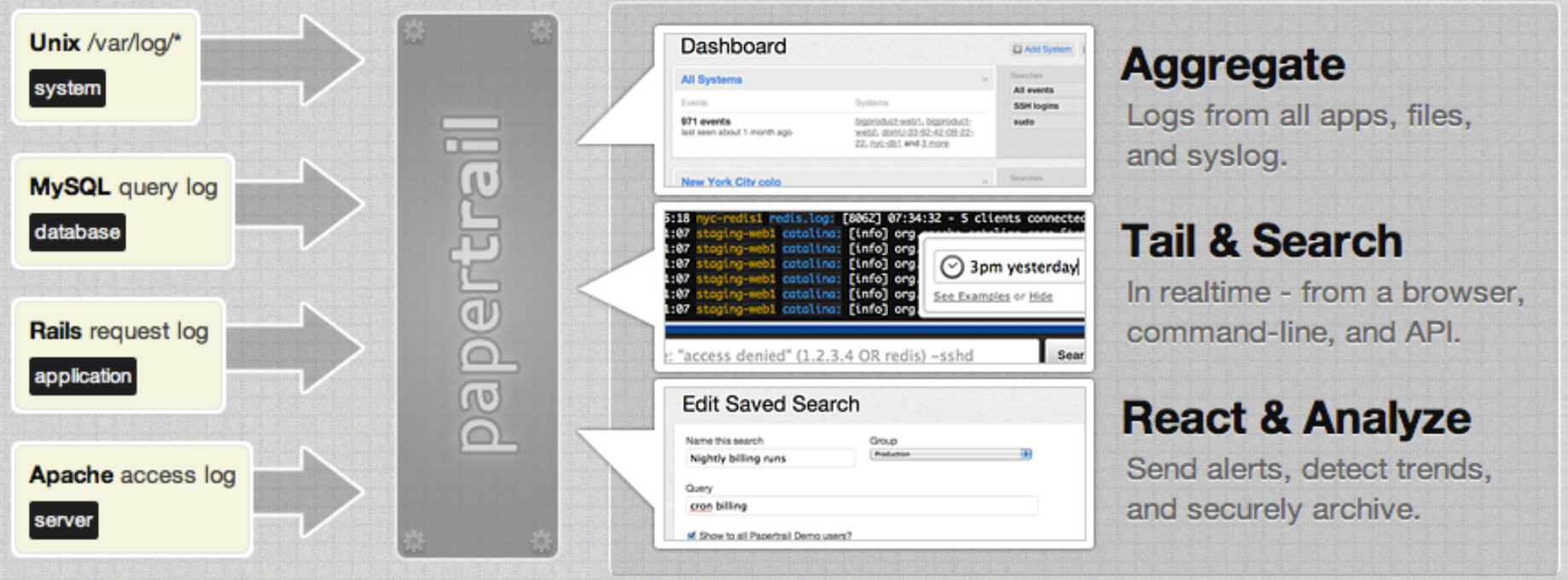
+ Database

+ Graphing library

HOSTED

papertrail

Tour Pricing & Sign Up Twitter Blog Sign In



Hosted log management for servers, apps, and cloud services.

Instantly manage logs from 2 servers—or 2,000.

Start Logging!
Free. No expiration.
No credit card.

Papertrail helps **detect, resolve, and avoid infrastructure problems** using log messages. Papertrail's practicality comes from **our own experience** as sysadmins and developers, and entrepreneurs. Take the tour or sign up.

Take a Tour

Pricing & Sign Up

Starts at **$0**. Setup takes one minute.

Statistical

Analysis

R

RStudio

hhh2011 | Scrape_access_log.R | x

Source on Save | Run | Source

```
1  x <- scan("~/src/Jay/access_log", what="", sep="\n")
2  x[1]
3  length(x)
4
5  # Get starting and ending position of date/time stamps
6  # using vectorized regular expressions:
7  start <- regexpr("[", x, fixed=TRUE)
8  end <- regexpr("]", x, fixed=TRUE)
9  x[1]
10 start[1]
11 end[1]
12
13 # Poke around a bit
14 table(start)
15 table(end)
16 table(end-start)
17
```

1:1 (Top Level) R Script

Workspace | History

Load | Save | Import Dataset | Clear All

Data	
hfh5k2011	351 obs. of 8 variables
hhh2011	1239 obs. of 12 variables
x	1708 obs. of 1 variables
y	591x1 integer matrix
Values	
start	character[8]

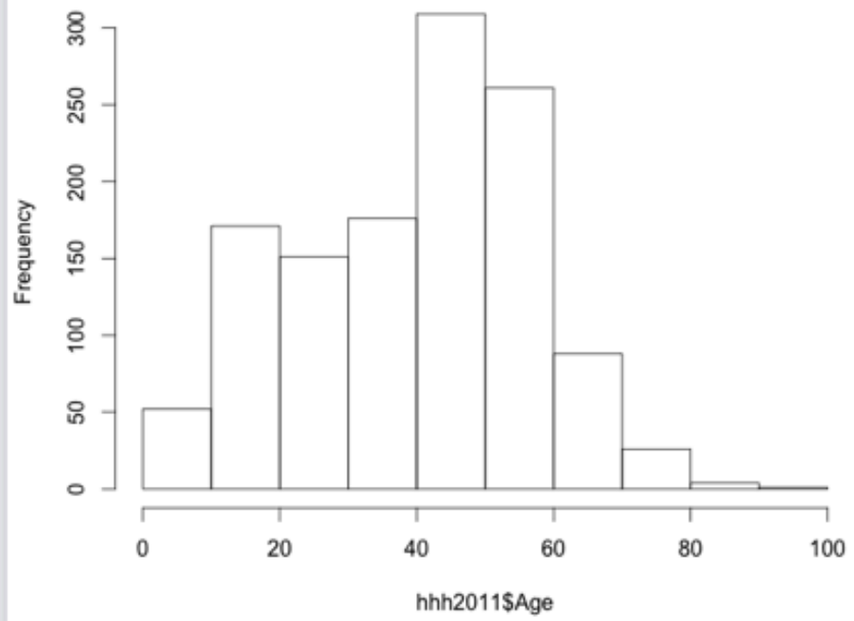
Console ~/

```
3: In max(x) : no non-missing arguments to max; returning -Inf
4: In xy.coords(x, y, xlabel, ylabel, log) : NAs introduced by coercion
> as.matrix(summary(x))

message
 SierraSWoCMon(0x4d)(0xac5ed2c0): +++
:  47
 [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 Socket closed by remote peer UserInfo=0x101854670
{NSLocalizedDescription=Socket closed by remote peer}:  30
 [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 Socket closed by remote peer UserInfo=0x100352a70
{NSLocalizedDescription=Socket closed by remote peer}:  27
 kCGErrorIllegalArgument: CGSSetWindowTransformAtPlacement: Failed
:  27
 kCGErrorIllegalArgument: CGSSetWindowTransformsAtPlacement: Failed
:  27
 [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 Socket closed by remote peer UserInfo=0x101a3a8b0
{NSLocalizedDescription=Socket closed by remote peer}:  25
 (Other)
:1525
> as.matrix(summary(x))[1,1]
[1] "SierraSWoCMon(0x4d)(0xac5ed2c0): +++
:  47  "
> as.matrix(summary(x))[1,2]
Error: subscript out of bounds
> as.matrix(summary(x))[1,0]
character(0)
> as.matrix(summary(x))[2,1]
[1] "[HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 Socket closed by remote peer UserInfo=0x101854670
{NSLocalizedDescription=Socket closed by remote peer}:  30  "
> hfh5k2011 <- read.csv("~/Dropbox/hfh5k2011.csv")
> hhh2011 <- read.csv("~/Downloads/hohoho5k2011 - Sheet 1.csv")
> hist(hhh2011$Age)
>
```

Files | Plots | Packages | Help

Zoom | Export | Clear All



APPLICATIONS OF R IN BUSINESS COMPETITION

Revolution Analytics is proud to announce the winners of the inaugural Applications of R in Business competition, which offered a total of $20,000 in cash prizes to the best examples of applying the R statistics language to real-world business problems.

The top prizes were selected by a panel of independent judges: Edd Dumbill, Chair of O'Reilly's Strata Conference and writer for O'Reilly Media; David Menninger, VP and Research Director at Ventana Research; Steve Miller, technology writer and co-founder of OpenBI LLC; David White, Senior Research Analyst at Aberdeen Group; and Hadley Wickham, R package author and professor at Rice University. Based on the judges' aggregate scores, the winners are:

Grand Prize - $10,000

Shannon Terry and Ben Ogorek, Nationwide Insurance (USA)
A Direct Marketing In-flight Forecasting System

Runner Up Prize - $5,000

Jeffrey Breen, Atmosphere Research Group (USA)
Mining Twitter for Airline Consumer Sentiment

The following entries were selected for Honorable Mention prizes by Revolution Analytics:

Honorable Mention - $1,000

Hakan Koç and Bengt Maas, Salzgitter Mannesmann Forschung GmbH (Germany)
Towards an ideal steel plant - Online liquid steel temperature prediction using R

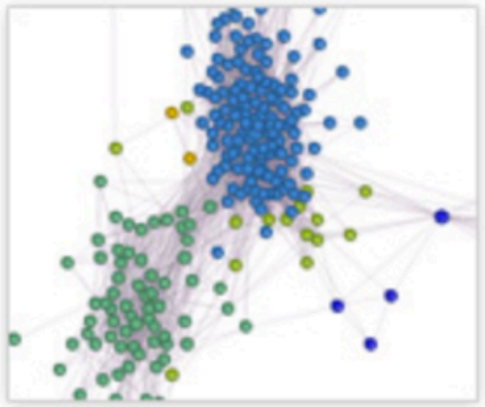
Honorable Mention - $1,000


123.4
123.4

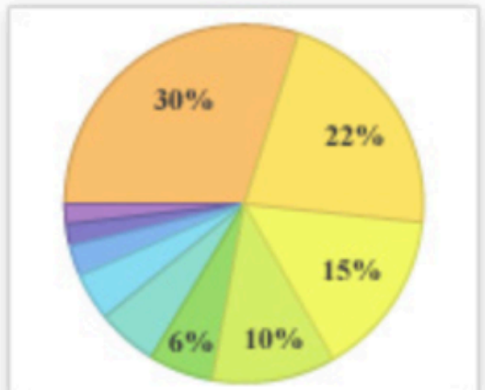
WolframAlpha computational knowledge engine

facebook report

Examples Random



Friend community network



Friend statistics

statuses | posted links | uploaded videos
check-ins
(based on previous 1677 wall posts)

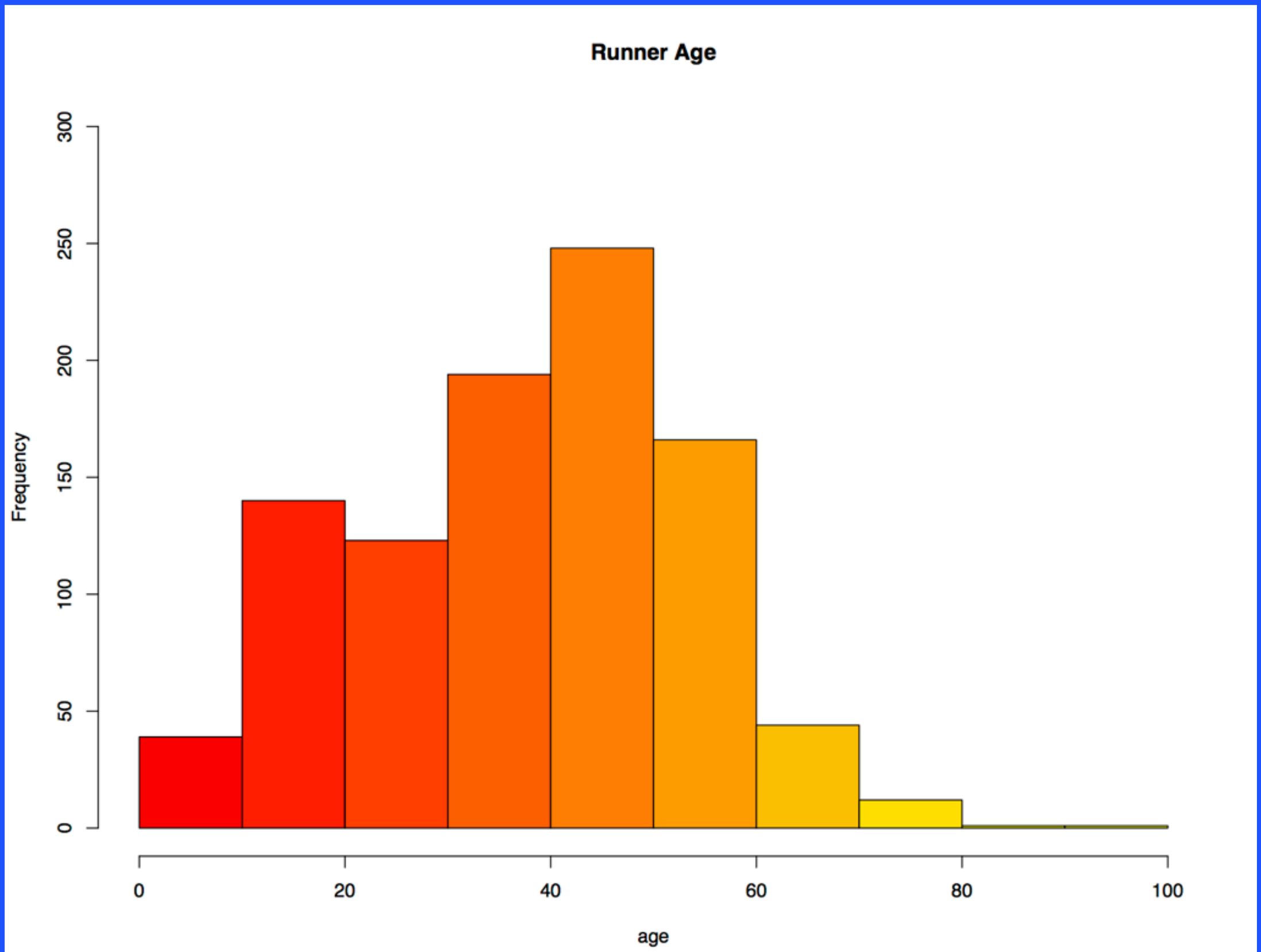
Posting types:

type	count	ratio
uploaded photos	1176	
posted links	384	
statuses	100	
uploaded videos	14	
check-ins	3	

Daily posting activity

Analyze My Facebook Data

Learn more about Wolfram|Alpha Personal Analytics »


Runner Age
Frequency
0
50
100
150
200
250
300
0
20
40
60
80
100
age

SierraSWOCMon(0x40)(0xAC5ED2C0): +++ : 47

[HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" UserInfo=0x101854670 {NSLocalizedDescription=Socket closed by remote peer}: 30

[HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" UserInfo=0x100351A70 {NSLocalizedDescription=Socket closed by remote peer}: 27

kCGErrorIllegalArgument: CGSSetWindowTransformAtPlacement: Failed : 27

kCGErrorIllegalArgument: CGSSetWindowTransformsAtPlacement: Failed : 27

[HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" UserInfo=0x101A3A8B0 {NSLocalizedDescription=Socket closed by remote peer}: 25

SierraSWOCMon(0x40)(0xAC5ED2C0): +++ : 47

[HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" UserInfo=0x101854670 {NSLocalizedDescription=Socket closed by remote peer}: 30

[HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" UserInfo=0x100351A70 {NSLocalizedDescription=Socket closed by remote peer}: 27

kCGErrorIllegalArgument: CGSSetWindowTransformAtPlacement: Failed : 27

kCGErrorIllegalArgument: CGSSetWindowTransformsAtPlacement: Failed : 27

[HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" UserInfo=0x101A3A8B0 {NSLocalizedDescription=Socket closed by remote peer}: 25

SierraSWOCMon(0x40)(0xAC5ED2C0): +++ : 47

[HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" UserInfo=0x101854670 {NSLocalizedDescription=Socket closed by remote peer}: 30

[HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" UserInfo=0x100351A70 {NSLocalizedDescription=Socket closed by remote peer}: 27

kCGErrorIllegalArgument: CGSSetWindowTransformAtPlacement: Failed : 27

kCGErrorIllegalArgument: CGSSetWindowTransformsAtPlacement: Failed : 27

[HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" UserInfo=0x101A3A8B0 {NSLocalizedDescription=Socket closed by remote peer}: 25

SierraSWOCMon(0x40)(0xAC5ED2C0): +++ : 47

[HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" UserInfo=0x101854670 {NSLocalizedDescription=Socket closed by remote peer}: 30

[HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" UserInfo=0x100351A70 {NSLocalizedDescription=Socket closed by remote peer}: 27

kCGErrorIllegalArgument: CGSSetWindowTransformAtPlacement:
Failed : 27

kCGErrorIllegalArgument: CGSSetWindowTransformsAtPlacement:
Failed : 27

[HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" UserInfo=0x101A3A8B0 {NSLocalizedDescription=Socket closed by remote peer}: 25

(OTHER)

:1498

Column 1 change

61 choices Sort by: **name** count Cluster

externalIP = "0.0.0.0"; 2

externalIP = "68.194.171.81"; 2

secondsSinceStartOfEpoch = 117440512; 2

secondsSinceStartOfEpoch = 251658240; 2

senderAddress = "192.168.100.1"; 4

} 4

The domain/default pair of (/Applications/Google Chrome Canary.app/Contents/Info, KSBrandID) does not exist 2

- continuousScroll is deprecated for

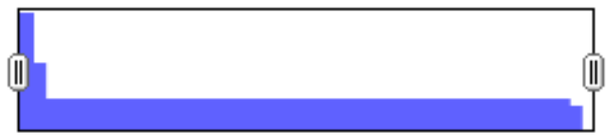
Cluster & Edit column "Column 1"

This feature helps you find groups of different cell values that might be alternative representations of the same thing. For example, the two strings "New York" and "new york" are very likely to refer to the same concept and just have capitalization differences, and "Gödel" and "Godel" probably refer to the same person. Find out more ...

Method nearest neighbor | Distance Function PPM | Radius 1.0 | Block Chars 6 | **496** clusters found

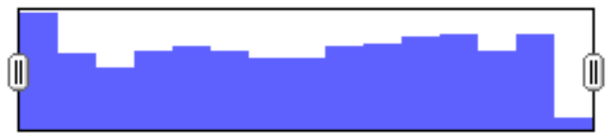
Cluster Size	Row Count	Values in Cluster	Merge?	New Cell Value
452	1383	• [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" UserInfo=0x101854670 {NSLocalizedDescription=Socket closed by remote peer} (30 rows) • [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" UserInfo=0x100352a70 {NSLocalizedDescription=Socket closed by remote peer} (27 rows) • [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" UserInfo=0x101a3a8b0 {NSLocalizedDescription=Socket closed by remote peer} (25 rows) • [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" UserInfo=0x101829d90 {NSLocalizedDescription=Socket closed by remote peer} (24 rows) • [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed by remote peer" UserInfo=0x101b08470 {NSLocalizedDescription=Socket closed by remote peer} (23 rows) • [HYBI] socketDidDisconnect: Error Domain=GCDAsyncSocketErrorDomain Code=7 "Socket closed	☐	[HYBI] socketDidDisconnec

 # Choices in Cluster



0 — 460

 # Rows in Cluster



0 — 1400

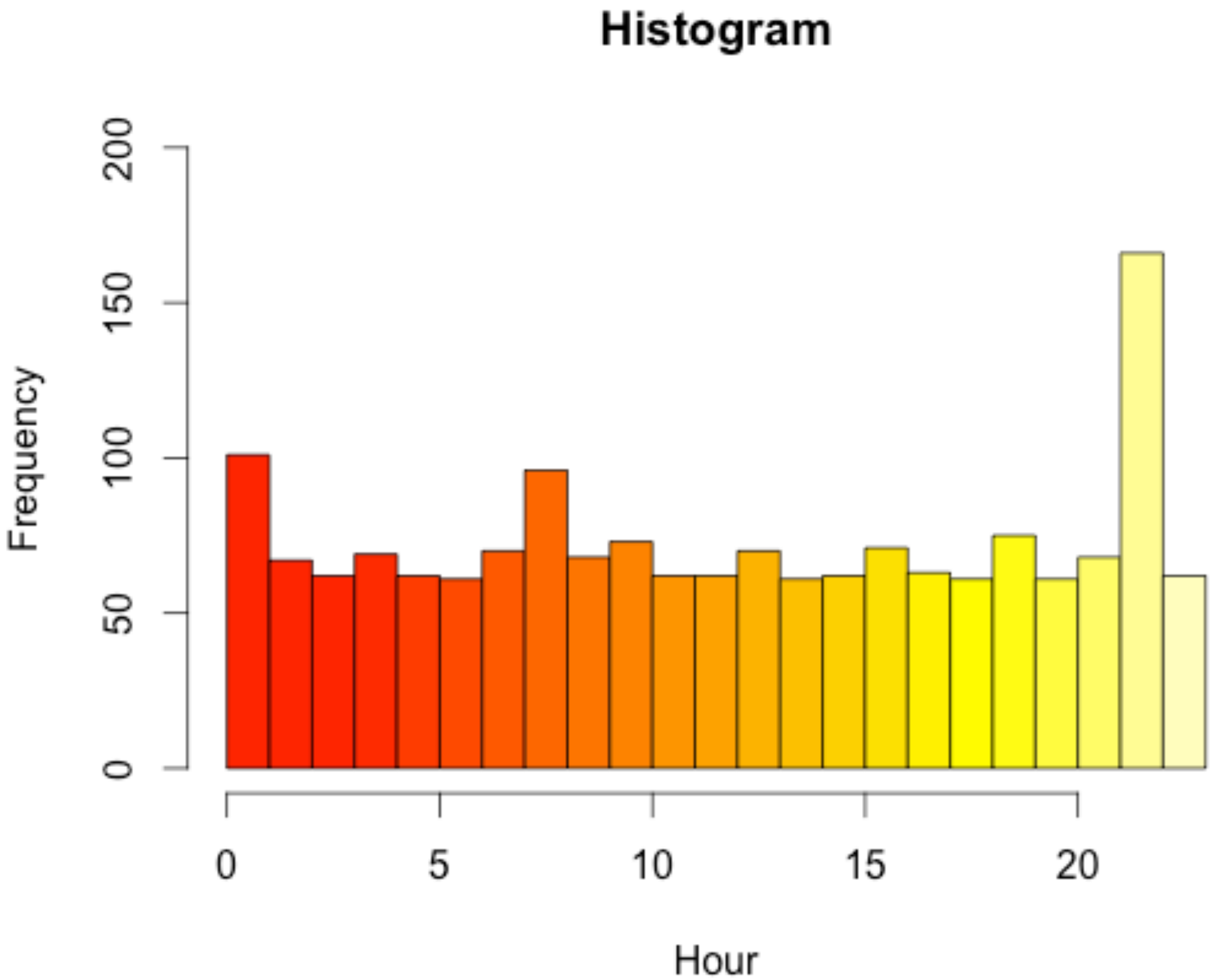
Average Length of Choices

20 — 270

Length Variance of Choices

0 — 5

Select All | Deselect All | **Merge Selected & Re-Cluster** | Merge Selected & Close | Close


Histogram
Frequency
0
50
100
150
200
0
5
10
15
20
Hour

Logs, Damn Logs and Statistics

Thank you!

Edward Marczak

marczak@radiotope.com

@marczak