Nzyme

Information Security Inc.

Contents

- About Nzyme
- How Does It Work?
- Test Setup
- Installing the requirements
- Installing Nzyme
- Configuring and using Nzyme
- References

About Nzyme

- Java-based program that puts wireless network adapters into monitor mode, sniffs management frames from all configured 2.4Ghz or 5Ghz channels and writes them into a Graylog instance for monitoring and analysis
- An open source tool used to detect WiFi attacks or to perform incident response after an attack has happened

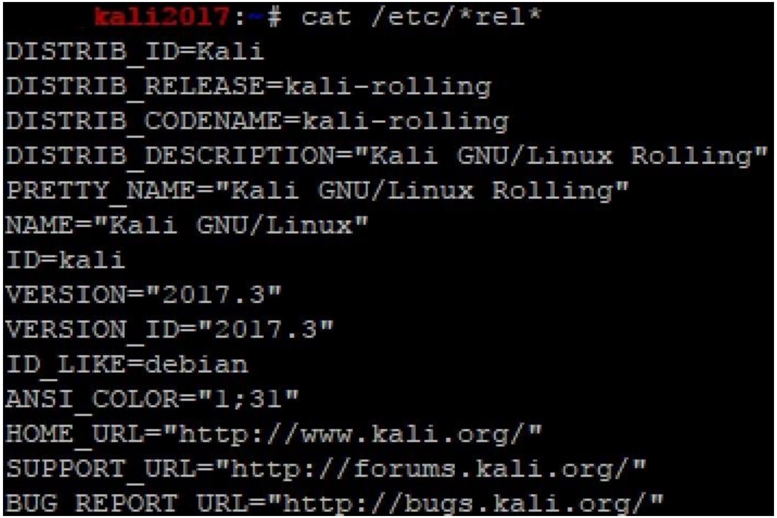
Introducing Nzyme: WiFi Monitoring, Intrusion Detection And Forensics

How Does It Work?

- Nzyme reads 802.11 WiFi frames directly from the air using any WiFi adapter that supports monitor mode
- Then parses the frames and sends them over the network to a Graylog (free and open source log management) setup

Test Setup

- Kali Linux 2017 version 3



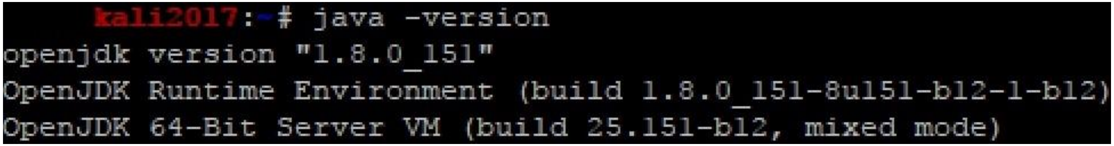
```
     kali2017:~# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2017.3"
VERSION_ID="2017.3"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

Test Setup

- Alpha wireless card => AWUS036NHA

Installing the requirements

- Make sure Java 7 or 8 is installed

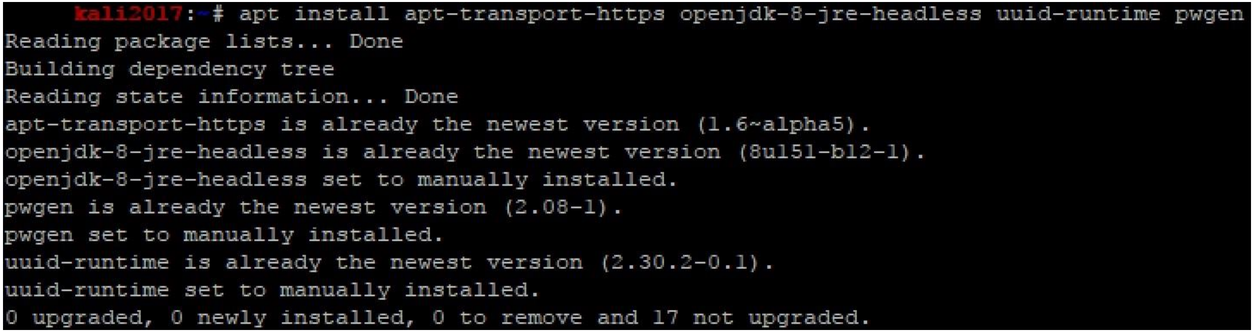


```
     kali2017:~# java -version
openjdk version "1.8.0_151"
OpenJDK Runtime Environment (build 1.8.0_151-8u151-b12-1-b12)
OpenJDK 64-Bit Server VM (build 25.151-b12, mixed mode)
```

Installing the requirements

- Graylog (open source log management platform) => installation (http://docs.graylog.org/en/2.3/pages/installation/operating_system_packages.html); (http://docs.graylog.org/en/2.3/pages/installation/os/debian.html)

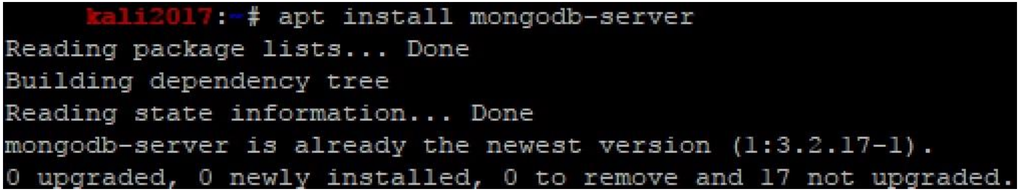
- Installing the required packages



```
     kali2017:~# apt install apt-transport-https openjdk-8-jre-headless uuid-runtime pwgen
Reading package lists... Done
Building dependency tree
Reading state information... Done
apt-transport-https is already the newest version (1.6~alpha5).
openjdk-8-jre-headless is already the newest version (8u151-b12-1).
openjdk-8-jre-headless set to manually installed.
pwgen is already the newest version (2.08-1).
pwgen set to manually installed.
uuid-runtime is already the newest version (2.30.2-0.1).
uuid-runtime set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 17 not upgraded.
```

Installing the requirements

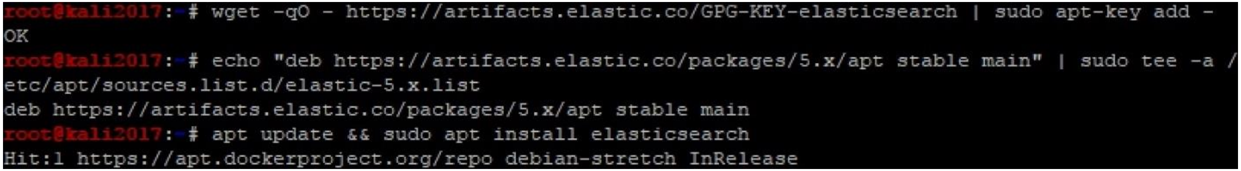
- Installing mongodb



```
     kali2017:~# apt install mongodb-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
mongodb-server is already the newest version (1:3.2.17-1).
0 upgraded, 0 newly installed, 0 to remove and 17 not upgraded.
```

Installing the requirements

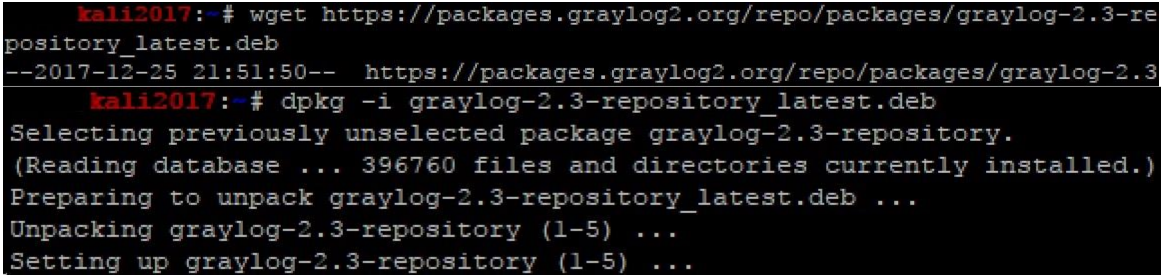
- Installing Elasticsearch



```
root@kali2017:~# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
OK
root@kali2017:~# echo "deb https://artifacts.elastic.co/packages/5.x/apt stable main" | sudo tee -a /
etc/apt/sources.list.d/elastic-5.x.list
deb https://artifacts.elastic.co/packages/5.x/apt stable main
root@kali2017:~# apt update && sudo apt install elasticsearch
Hit:1 https://apt.dockerproject.org/repo debian-stretch InRelease
```

Installing the requirements

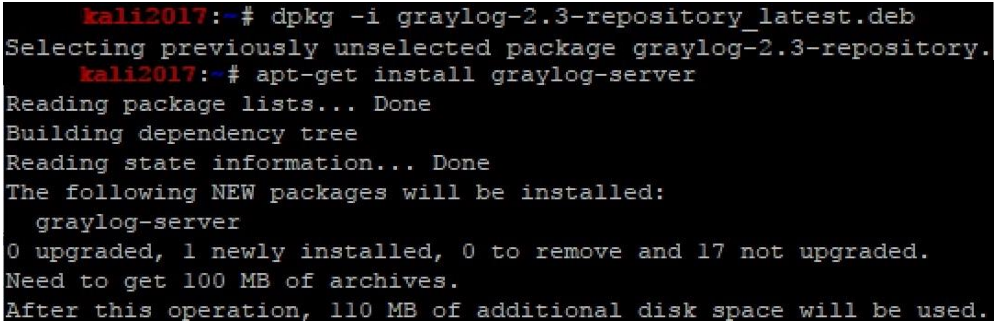
- Downloading and installing Graylog server



```
     kali2017:~# wget https://packages.graylog2.org/repo/packages/graylog-2.3-re
pository_latest.deb
--2017-12-25 21:51:50--  https://packages.graylog2.org/repo/packages/graylog-2.3
     kali2017:~# dpkg -i graylog-2.3-repository_latest.deb
Selecting previously unselected package graylog-2.3-repository.
(Reading database ... 396760 files and directories currently installed.)
Preparing to unpack graylog-2.3-repository_latest.deb ...
Unpacking graylog-2.3-repository (1-5) ...
Setting up graylog-2.3-repository (1-5) ...
```

Installing the requirements

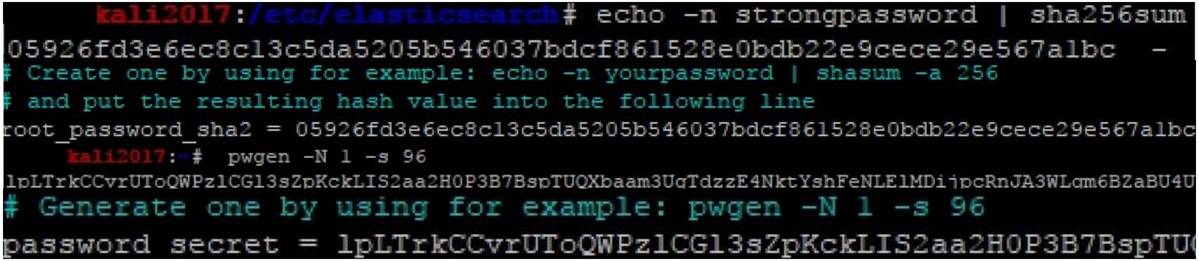
- Downloading and installing Graylog server



```
     kali2017:~# dpkg -i graylog-2.3-repository_latest.deb
Selecting previously unselected package graylog-2.3-repository.
     kali2017:~# apt-get install graylog-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  graylog-server
0 upgraded, 1 newly installed, 0 to remove and 17 not upgraded.
Need to get 100 MB of archives.
After this operation, 110 MB of additional disk space will be used.
```

Installing the requirements

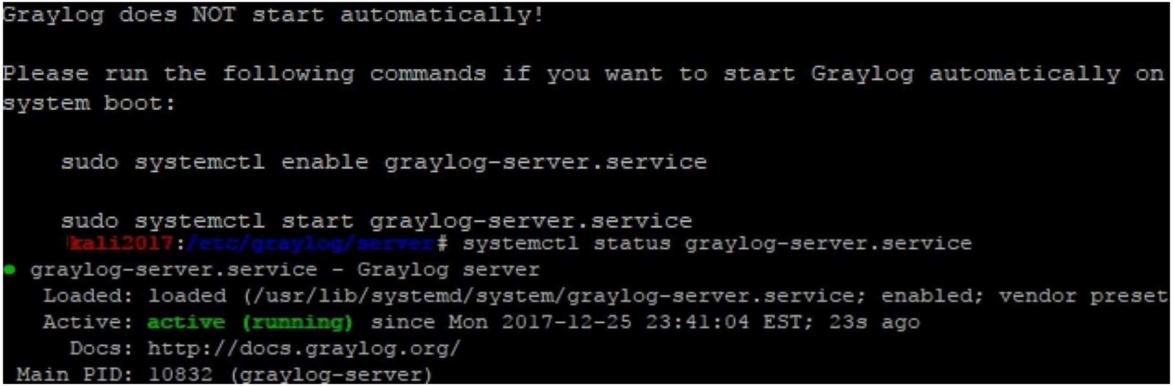
- Adding the required passwords



```
      kali2017:/etc/elasticsearch# echo -n strongpassword | sha256sum
05926fd3e6ec8c13c5da5205b546037bdcf861528e0bdb22e9cece29e567a1bc  -
# Create one by using for example: echo -n yourpassword | shasum -a 256
# and put the resulting hash value into the following line
root_password_sha2 = 05926fd3e6ec8c13c5da5205b546037bdcf861528e0bdb22e9cece29e567a1bc
     kali2017:~#  pwgen -N 1 -s 96
1pLTrkCCvrUToQWPz1CG13sZpKckLIS2aa2H0P3B7BspTUQXbaam3UgTdzzE4NktYshFeNLE1MDijpcRnJA3WLqm6BZaBU4U
# Generate one by using for example: pwgen -N 1 -s 96
password secret = 1pLTrkCCvrUToQWPz1CG13sZpKckLIS2aa2H0P3B7BspTU
```

Installing the requirements

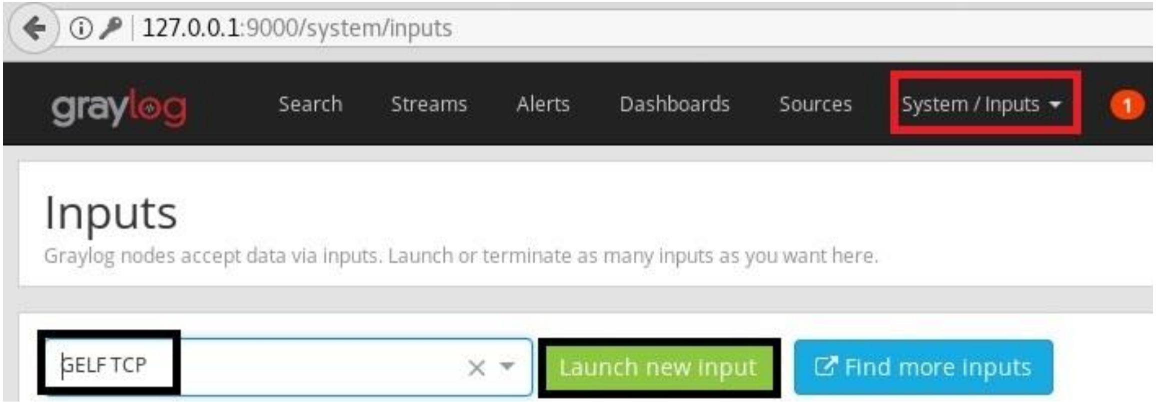
- Starting Graylog server



```
Graylog does NOT start automatically!

Please run the following commands if you want to start Graylog automatically on
system boot:

    sudo systemctl enable graylog-server.service

    sudo systemctl start graylog-server.service
     kali2017:/etc/graylog/server# systemctl status graylog-server.service
● graylog-server.service - Graylog server
   Loaded: loaded (/usr/lib/systemd/system/graylog-server.service; enabled; vendor preset
   Active: active (running) since Mon 2017-12-25 23:41:04 EST; 23s ago
     Docs: http://docs.graylog.org/
 Main PID: 10832 (graylog-server)
```

Installing the requirements

- Setting up GELF TCP input



127.0.0.1:9000/system/inputs

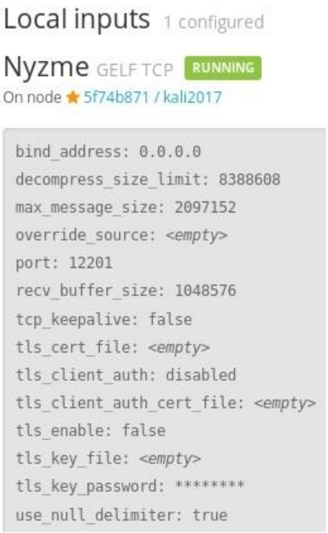
Inputs

Graylog nodes accept data via inputs. Launch or terminate as many inputs as you want here.

GELF TCP

Installing the requirements

- Setting up GELF TCP input



Local inputs 1 configured

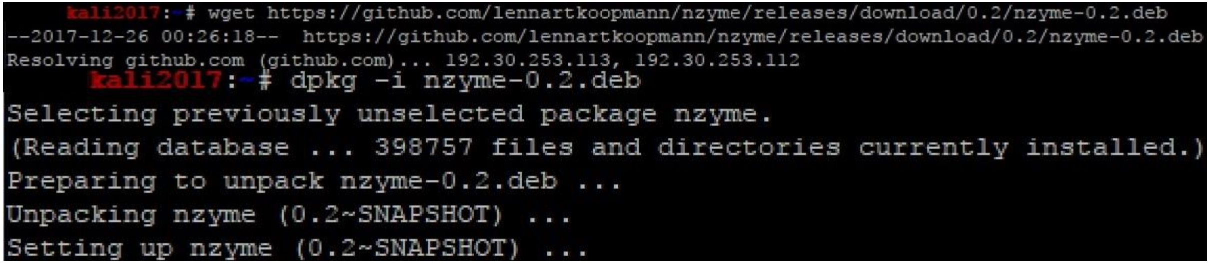
Nyzme GELF TCP RUNNING

On node ★ 5f74b871 / kali2017

```
bind_address: 0.0.0.0
decompress_size_limit: 8388608
max_message_size: 2097152
override_source: <empty>
port: 12201
recv_buffer_size: 1048576
tcp_keepalive: false
tls_cert_file: <empty>
tls_client_auth: disabled
tls_client_auth_cert_file: <empty>
tls_enable: false
tls_key_file: <empty>
tls_key_password: ********
use_null_delimiter: true
```

Installing Nzyme

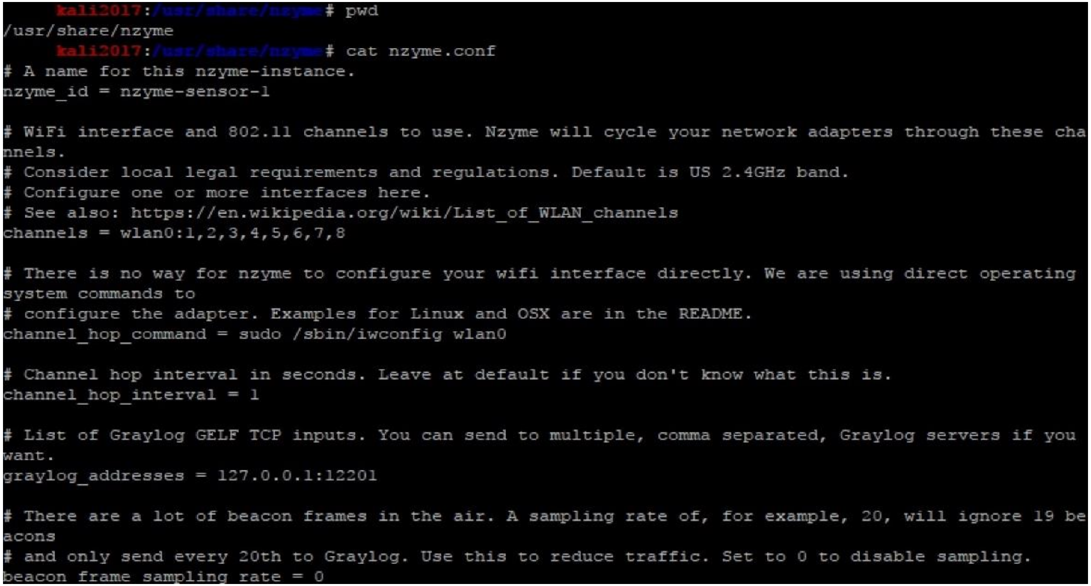
- Downloading and installing the latest release



```
     kali2017:~# wget https://github.com/lennartkoopmann/nzyme/releases/download/0.2/nzyme-0.2.deb
--2017-12-26 00:26:18--  https://github.com/lennartkoopmann/nzyme/releases/download/0.2/nzyme-0.2.deb
Resolving github.com (github.com)... 192.30.253.113, 192.30.253.112
     kali2017:~# dpkg -i nzyme-0.2.deb
Selecting previously unselected package nzyme.
(Reading database ... 398757 files and directories currently installed.)
Preparing to unpack nzyme-0.2.deb ...
Unpacking nzyme (0.2~SNAPSHOT) ...
Setting up nzyme (0.2~SNAPSHOT) ...
```

Configuring and using Nzyme

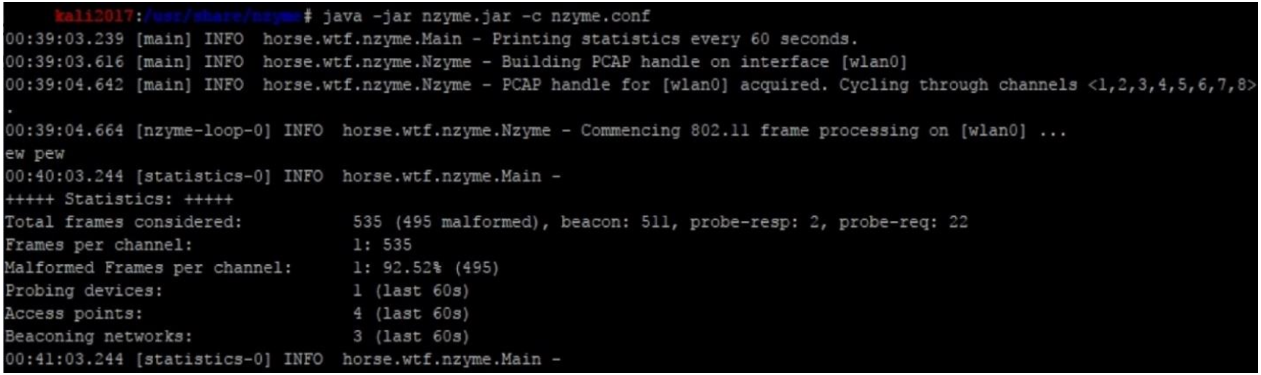
- Create a new file called nzyme.conf in the same folder as your nzyme.jar file



```
     kali2017:/usr/share/nzyme# pwd
/usr/share/nzyme
     kali2017:/usr/share/nzyme# cat nzyme.conf
# A name for this nzyme-instance.
nzyme_id = nzyme-sensor-1

# WiFi interface and 802.11 channels to use. Nzyme will cycle your network adapters through these cha
nnels.
# Consider local legal requirements and regulations. Default is US 2.4GHz band.
# Configure one or more interfaces here.
# See also: https://en.wikipedia.org/wiki/List_of_WLAN_channels
channels = wlan0:1,2,3,4,5,6,7,8

# There is no way for nzyme to configure your wifi interface directly. We are using direct operating
system commands to
# configure the adapter. Examples for Linux and OSX are in the README.
channel_hop_command = sudo /sbin/iwconfig wlan0

# Channel hop interval in seconds. Leave at default if you don't know what this is.
channel_hop_interval = 1

# List of Graylog GELF TCP inputs. You can send to multiple, comma separated, Graylog servers if you
want.
graylog_addresses = 127.0.0.1:12201

# There are a lot of beacon frames in the air. A sampling rate of, for example, 20, will ignore 19 be
acons
# and only send every 20th to Graylog. Use this to reduce traffic. Set to 0 to disable sampling.
beacon_frame_sampling_rate = 0
```

Configuring and using Nzyme

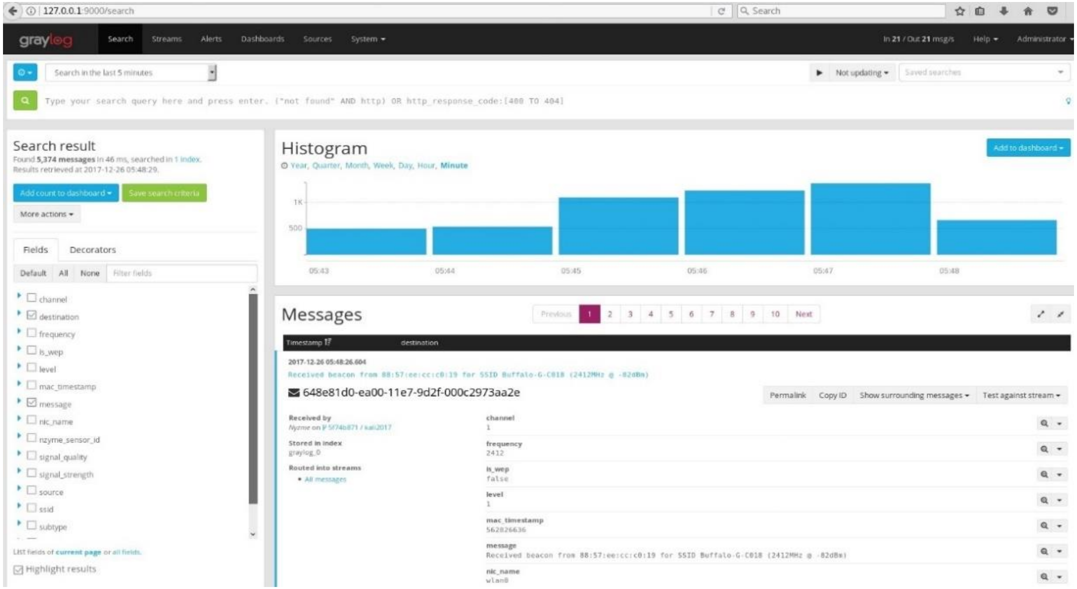
- Running Nzyme



```
     kali2017:/usr/share/nzyme# java -jar nzyme.jar -c nzyme.conf
00:39:03.239 [main] INFO  horse.wtf.nzyme.Main - Printing statistics every 60 seconds.
00:39:03.616 [main] INFO  horse.wtf.nzyme.Nzyme - Building PCAP handle on interface [wlan0]
00:39:04.642 [main] INFO  horse.wtf.nzyme.Nzyme - PCAP handle for [wlan0] acquired. Cycling through channels <1,2,3,4,5,6,7,8>
.
00:39:04.664 [nzyme-loop-0] INFO  horse.wtf.nzyme.Nzyme - Commencing 802.11 frame processing on [wlan0] ...
ew pew
00:40:03.244 [statistics-0] INFO  horse.wtf.nzyme.Main -
+++++ Statistics: +++++
Total frames considered:           535 (495 malformed), beacon: 511, probe-resp: 2, probe-req: 22
Frames per channel:                1: 535
Malformed Frames per channel:      1: 92.52% (495)
Probing devices:                   1 (last 60s)
Access points:                     4 (last 60s)
Beaconing networks:                3 (last 60s)
00:41:03.244 [statistics-0] INFO  horse.wtf.nzyme.Main -
```

Configuring and using Nzyme

- Checking Graylog messages injected by Nyzme



Search result

Found 5,374 messages in 46 ms, searched in 1 index.
Results retrieved at 2017-12-26 05:48:29.

- □ channel
- ☑ destination
- □ frequency
- □ is_wep
- □ level
- □ mac_timestamp
- ☑ message
- □ nic_name
- □ nzyme_sensor_id
- □ signal_quality
- □ signal_strength
- □ source
- □ ssid
- □ subtype

2017-12-26 05:48:26.604

```
Received beacon from 88:57:ee:cc:c0:19 for SSID Buffalo-G-C018 (2412MHz @ -82dBm)
```

648e81d0-ea00-11e7-9d2f-000c2973aa2e

Received by
Nyzme on 5f74b871 / kali2017

Stored in index
graylog_0

Routed into streams
- All messages

channel	1
frequency	2412
is_wep	false
level	1
mac_timestamp	562826636
message	Received beacon from 88:57:ee:cc:c0:19 for SSID Buffalo-G-C018 (2412MHz @ -82dBm)
nic_name	wlan0

References

- Nzyme

https://github.com/lennartkoopmann/nzyme

- Introducing Nzyme

https://wtf.horse/2017/10/02/introducing-nzyme-wifi-802-11-frame-recording-and-forensics/

- Graylog

https://github.com/Graylog2/graylog2-server