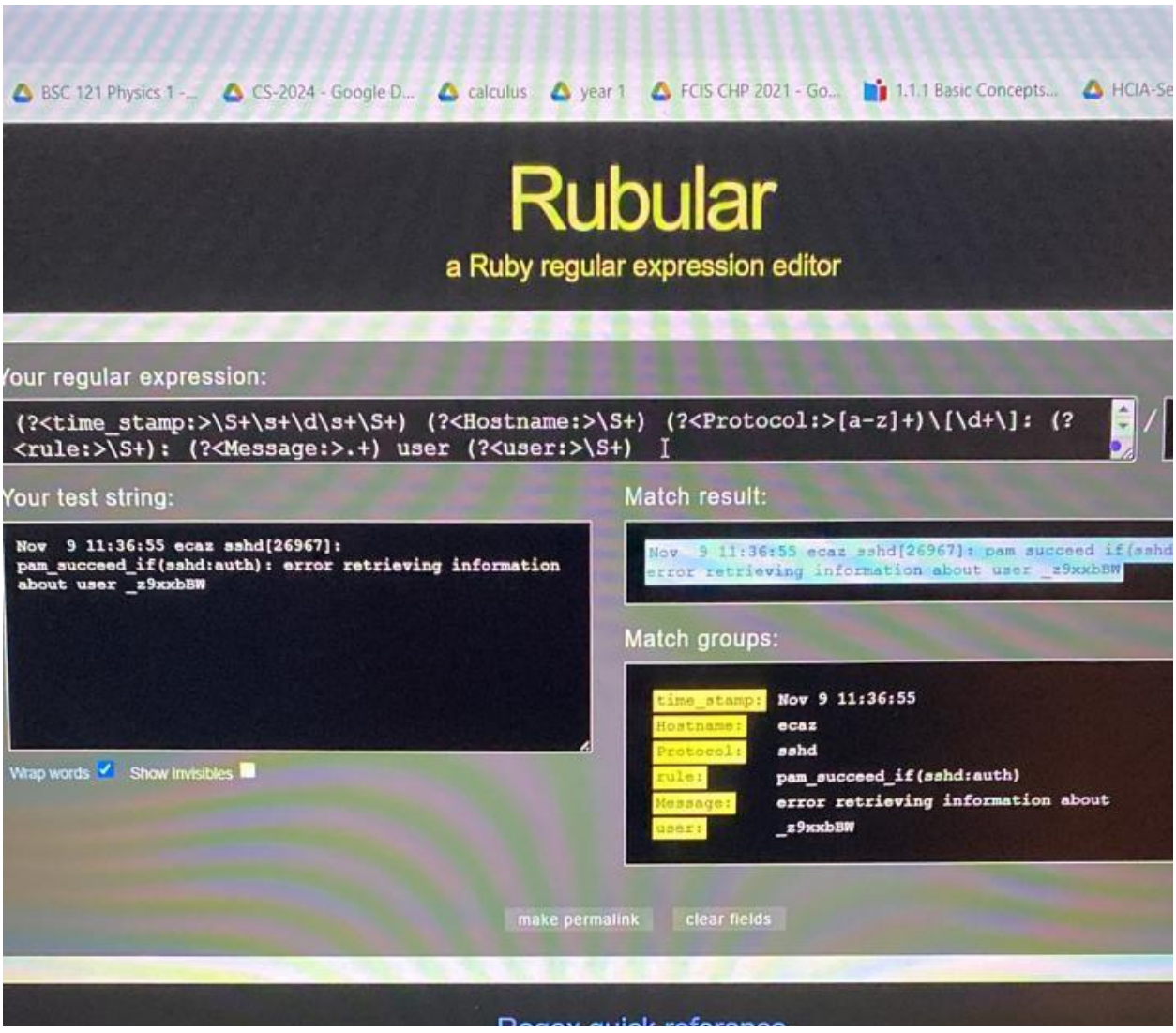
Task 2

Integrating fluent-bit with elasticsearch

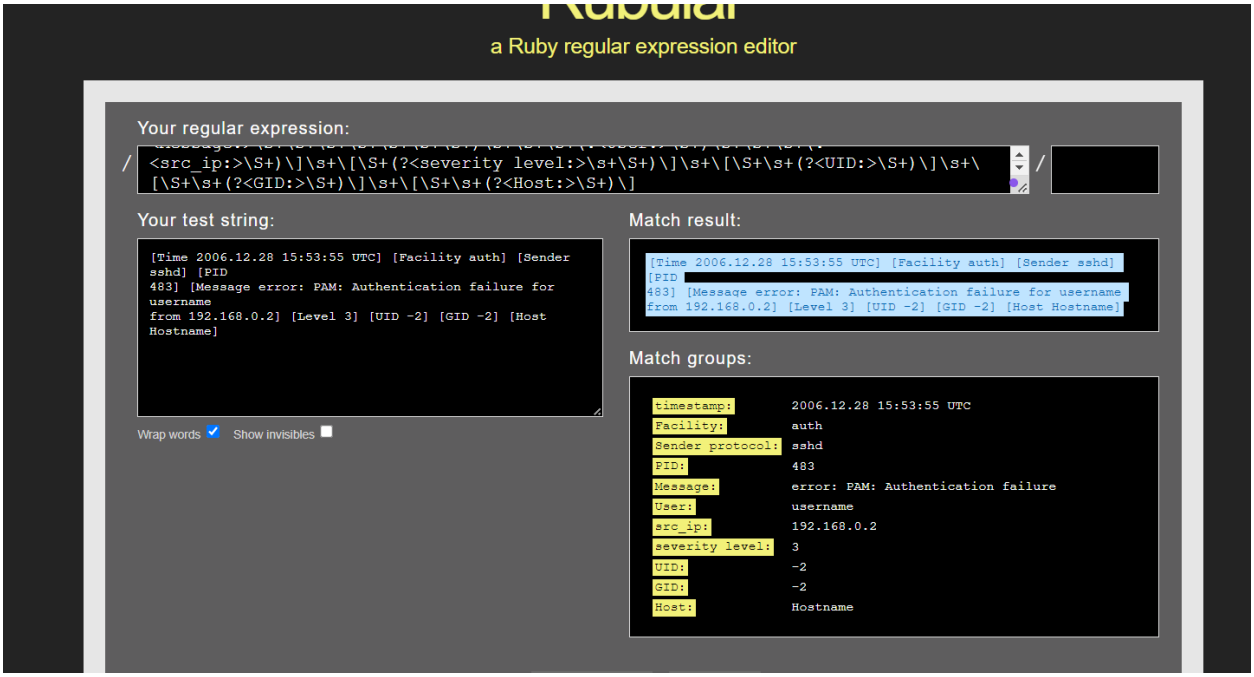
First: Using regex to parse the logs in rebular

1-



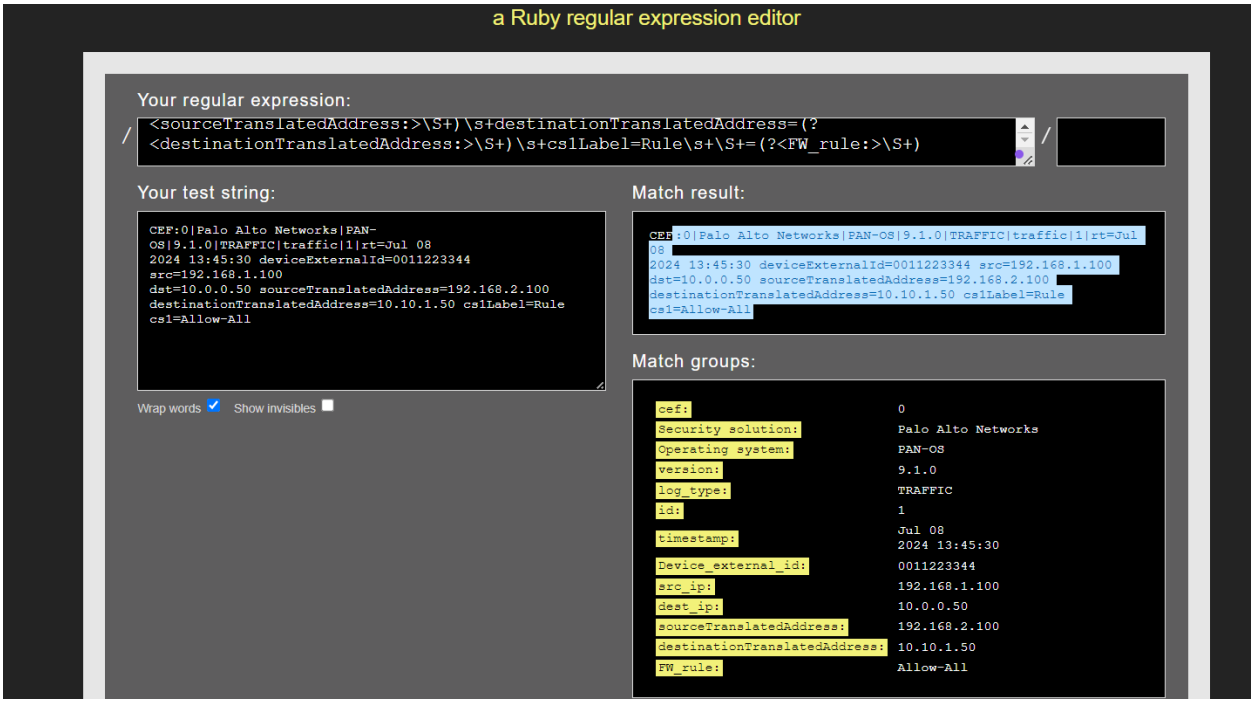
2-

```
\[Time\s+(?<timestamp:>\S+\s+\S+\s+\S+)\]\s+\[Facility\s+(?<Facility:>\S+)\]\s+\[Sender\s+(?<Sender protocol:>\S+)]
\s+\[PID\s+(?<PID:>\d+)\]\s+\[Message\s+(?<Message:>\S+\s+\S+\s+\S+\s+\S+)\s+\S+\s+(?<User:>\S+)\s+\S+\s+(?<src_ip:>\S+)\]
\s+\[\S+(?<severity level:>\s+\S+)\]\s+\[\S+\s+(?<UID:>\S+)\]\s+\[\S+\s+(?<GID:>\S+)\]\s+\[\S+\s+(?<Host:>\S+)\]
```



3-

```
:(?<cef:>\d+)\|(?<Security solution:>\S+\s+\S+\s+[a-zA-Z]+)\|(?<Operating system:>[a-zA-Z]+-[a-zA-Z]+)\|(?<version:>\d+\.\d+\.\d+)\|
(?<log_type:>[a-zA-Z]+)\|[a-zA-Z]+\|(?<id:>\d+)\|rt=(?<timestamp:>\S+\s+\S+\s+\S+\s+\S+)\s+deviceExternalId=(?<Device_external_id:>\S+)
\s+src=(?<src_ip:>\S+)\s+dst=(?<dest_ip:>\S+)\s+sourceTranslatedAddress=(?<sourceTranslatedAddress:>\S+)\s+destinationTranslatedAddress=
(?<destinationTranslatedAddress:>\S+)\s+cs1Label=Rule\s+\S+=(?<FW_rule:>\S+)
```



Second:

Integrating fluent-bit with elasticsearch

1-Adding our server GPG key to your keyring

```
root@abdelrahman-1-2:/home/abdelrahman/Downloads# curl https://packages.fluentbit.io/fluentbit.key | gpg --dearmor > /u
sr/share/keyrings/fluentbit-keyring.pgp
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  3175  100  3175    0     0   3829      0 --:--:-- --:--:-- --:--:--  3829
```

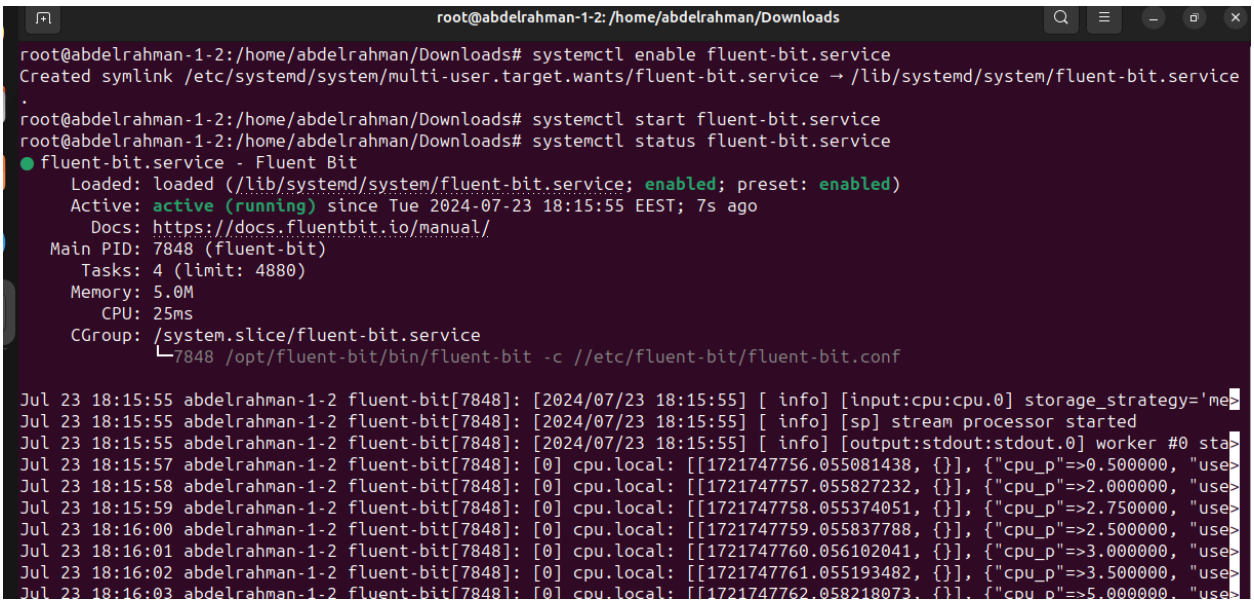
2-Adding its APT server entry to sources lists and updating apt-get

```
root@abdelrahman-1-2:/home/abdelrahman/Downloads# echo "deb [signed-by=/usr/share/keyrings/fluentbit-keyring.gpg] https
://packages.fluentbit.io/debian/bookworm bookworm main" | sudo tee /etc/apt/sources.list.d/fluent-bit.x.list
deb [signed-by=/usr/share/keyrings/fluentbit-keyring.gpg] https://packages.fluentbit.io/debian/bookworm bookworm main
```

3-Installing Fluent-Bit.

```
root@abdelrahman-1-2:/home/abdelrahman/Downloads# apt-get update
Hit:1 http://security.ubuntu.com/ubuntu mantic-security InRelease
Hit:2 http://eg.archive.ubuntu.com/ubuntu mantic InRelease
Hit:3 http://eg.archive.ubuntu.com/ubuntu mantic-updates InRelease
Hit:4 http://eg.archive.ubuntu.com/ubuntu mantic-backports InRelease
Get:5 https://packages.fluentbit.io/debian/bookworm bookworm InRelease [7,577 B]
Get:6 https://packages.fluentbit.io/debian/bookworm bookworm/main amd64 Packages [16.6 kB]
Fetched 24.2 kB in 2s (13.5 kB/s)
Reading package lists... Done
root@abdelrahman-1-2:/home/abdelrahman/Downloads# apt-get install fluent-bit
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libpq5
The following NEW packages will be installed:
  fluent-bit libpq5
0 upgraded, 2 newly installed, 0 to remove and 19 not upgraded.
1 not fully installed or removed.
Need to get 42.4 MB of archives.
After this operation, 97.7 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://eg.archive.ubuntu.com/ubuntu mantic-updates/main amd64 libpq5 amd64 15.7-0ubuntu0.23.10.1 [143 kB]
Get:2 https://packages.fluentbit.io/debian/bookworm bookworm/main amd64 fluent-bit amd64 3.1.3 [42.3 MB]
Fetched 42.4 MB in 22s (1,930 kB/s)
Selecting previously unselected package libpq5:amd64.
(Reading database ... 240290 files and directories currently installed.)
Preparing to unpack .../libpq5_15.7-0ubuntu0.23.10.1_amd64.deb ...
```

4-Enabling the service



5- Configuring fluent-bit to send logs to elasticsearch server

```
[INPUT]
    name tail
    tag  linux
    path  /var/log/auth.log

    # Read interval (sec) Default: 1
    interval_sec 1

[OUTPUT]
    name             es
    match            *
    Host             192.168.1.9
    Port             9200
    HTTP_User        elastic
    HTTP_Passwd      u=hNzUobNkVUtM2j5Qv5
    tls              on
    tls.verify       off
    Index            Task2
    Type             Log
    Suppress_Type_Name  ON

[OUTPUT]
    name  stdout
    match *
```

And the logs has successfully been sent to elasticsearch