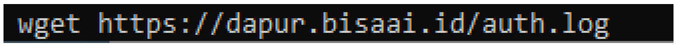
Nama : Tri Hesti Wahyuningsih

ID SIB : 3261839

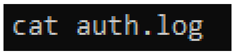
IP Address Log Filtering

1. Download terlebih dahulu file log dengan perintah wget



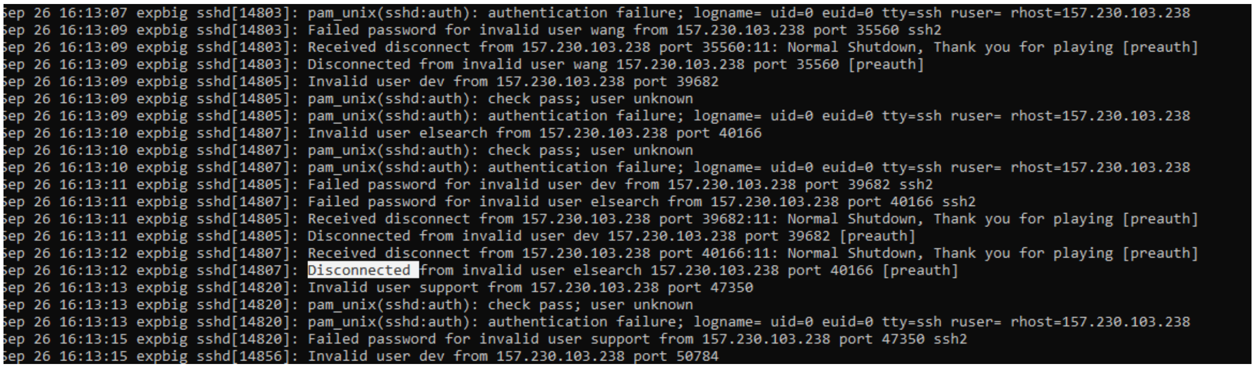
```
wget https://dapur.bisaai.id/auth.log
```

2. Setelah itu kita gunakan fungsi cat



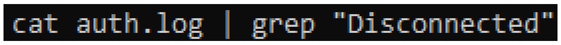
```
cat auth.log
```

Dibawah merupakan isi dari file log



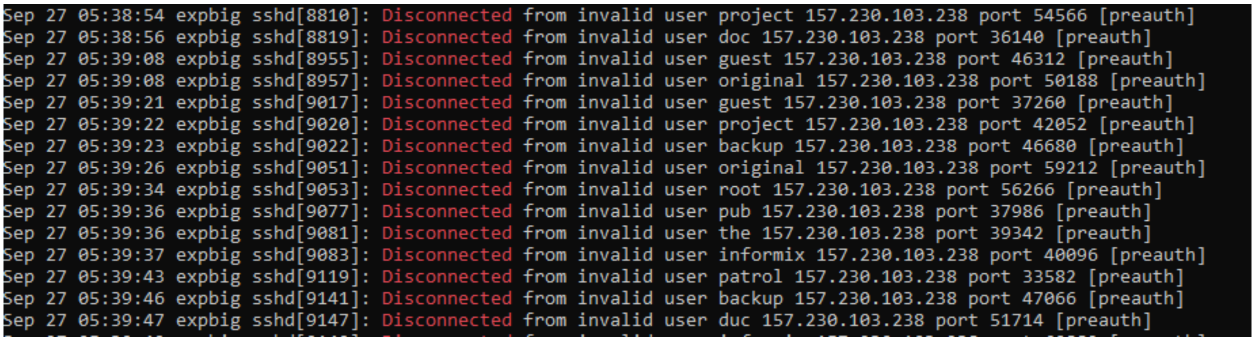
```
Sep 26 16:13:07 expbig sshd[14803]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=157.230.103.238
Sep 26 16:13:09 expbig sshd[14803]: Failed password for invalid user wang from 157.230.103.238 port 35560 ssh2
Sep 26 16:13:09 expbig sshd[14803]: Received disconnect from 157.230.103.238 port 35560:11: Normal Shutdown, Thank you for playing [preauth]
Sep 26 16:13:09 expbig sshd[14803]: Disconnected from invalid user wang 157.230.103.238 port 35560 [preauth]
Sep 26 16:13:09 expbig sshd[14805]: Invalid user dev from 157.230.103.238 port 39682
Sep 26 16:13:09 expbig sshd[14805]: pam_unix(sshd:auth): check pass; user unknown
Sep 26 16:13:09 expbig sshd[14805]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=157.230.103.238
Sep 26 16:13:10 expbig sshd[14807]: Invalid user elsearch from 157.230.103.238 port 40166
Sep 26 16:13:10 expbig sshd[14807]: pam_unix(sshd:auth): check pass; user unknown
Sep 26 16:13:10 expbig sshd[14807]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=157.230.103.238
Sep 26 16:13:11 expbig sshd[14805]: Failed password for invalid user dev from 157.230.103.238 port 39682 ssh2
Sep 26 16:13:11 expbig sshd[14807]: Failed password for invalid user elsearch from 157.230.103.238 port 40166 ssh2
Sep 26 16:13:11 expbig sshd[14805]: Received disconnect from 157.230.103.238 port 39682:11: Normal Shutdown, Thank you for playing [preauth]
Sep 26 16:13:11 expbig sshd[14805]: Disconnected from invalid user dev 157.230.103.238 port 39682 [preauth]
Sep 26 16:13:12 expbig sshd[14807]: Received disconnect from 157.230.103.238 port 40166:11: Normal Shutdown, Thank you for playing [preauth]
Sep 26 16:13:12 expbig sshd[14807]: Disconnected from invalid user elsearch 157.230.103.238 port 40166 [preauth]
Sep 26 16:13:13 expbig sshd[14820]: Invalid user support from 157.230.103.238 port 47350
Sep 26 16:13:13 expbig sshd[14820]: pam_unix(sshd:auth): check pass; user unknown
Sep 26 16:13:13 expbig sshd[14820]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=157.230.103.238
Sep 26 16:13:15 expbig sshd[14820]: Failed password for invalid user support from 157.230.103.238 port 47350 ssh2
Sep 26 16:13:15 expbig sshd[14856]: Invalid user dev from 157.230.103.238 port 50784
```

3. Kita filter log yang disconnect menggunakan fungsi grep berikut



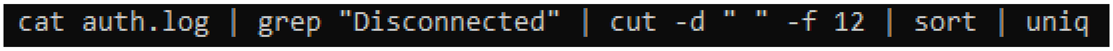
```
cat auth.log | grep "Disconnected"
```

Sehingga yang ditampilkan hanya log histori disconnected



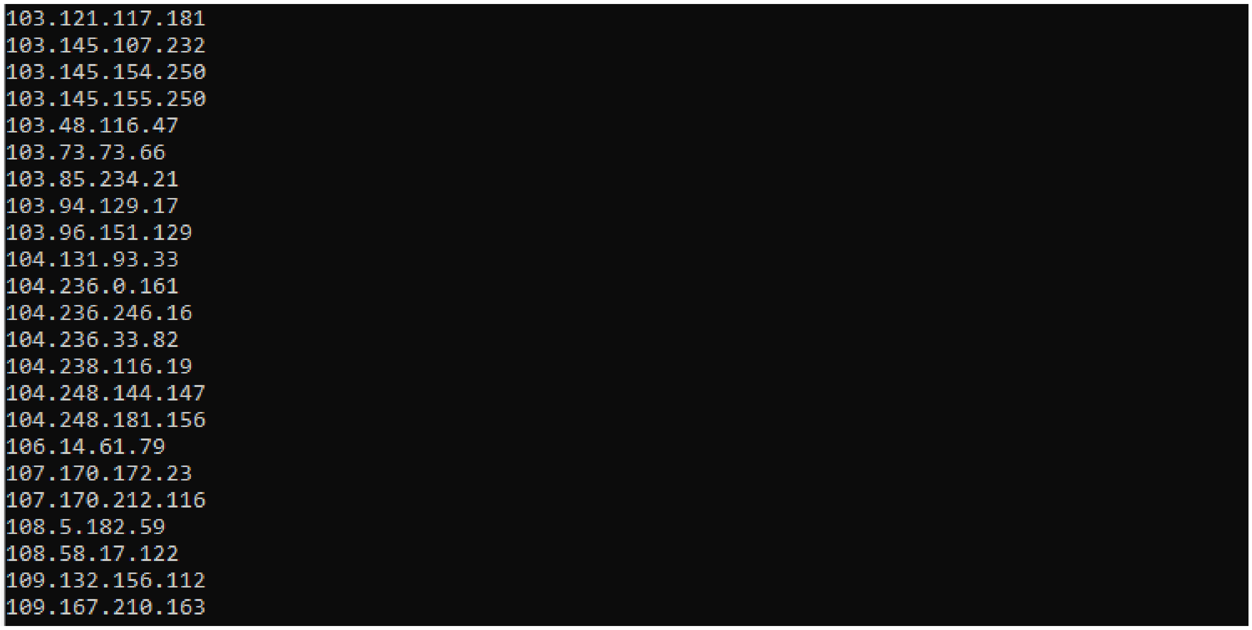
```
Sep 27 05:38:54 expbig sshd[8810]: Disconnected from invalid user project 157.230.103.238 port 54566 [preauth]
Sep 27 05:38:56 expbig sshd[8819]: Disconnected from invalid user doc 157.230.103.238 port 36140 [preauth]
Sep 27 05:39:08 expbig sshd[8955]: Disconnected from invalid user guest 157.230.103.238 port 46312 [preauth]
Sep 27 05:39:08 expbig sshd[8957]: Disconnected from invalid user original 157.230.103.238 port 50188 [preauth]
Sep 27 05:39:21 expbig sshd[9017]: Disconnected from invalid user guest 157.230.103.238 port 37260 [preauth]
Sep 27 05:39:22 expbig sshd[9020]: Disconnected from invalid user project 157.230.103.238 port 42052 [preauth]
Sep 27 05:39:23 expbig sshd[9022]: Disconnected from invalid user backup 157.230.103.238 port 46680 [preauth]
Sep 27 05:39:26 expbig sshd[9051]: Disconnected from invalid user original 157.230.103.238 port 59212 [preauth]
Sep 27 05:39:34 expbig sshd[9053]: Disconnected from invalid user root 157.230.103.238 port 56266 [preauth]
Sep 27 05:39:36 expbig sshd[9077]: Disconnected from invalid user pub 157.230.103.238 port 37986 [preauth]
Sep 27 05:39:36 expbig sshd[9081]: Disconnected from invalid user the 157.230.103.238 port 39342 [preauth]
Sep 27 05:39:37 expbig sshd[9083]: Disconnected from invalid user informix 157.230.103.238 port 40096 [preauth]
Sep 27 05:39:43 expbig sshd[9119]: Disconnected from invalid user patrol 157.230.103.238 port 33582 [preauth]
Sep 27 05:39:46 expbig sshd[9141]: Disconnected from invalid user backup 157.230.103.238 port 47066 [preauth]
Sep 27 05:39:47 expbig sshd[9147]: Disconnected from invalid user duc 157.230.103.238 port 51714 [preauth]
```

4. Setelah itu kita filter IP saja dan menghilangkan teks lainnya dengan fungsi di bawah ini



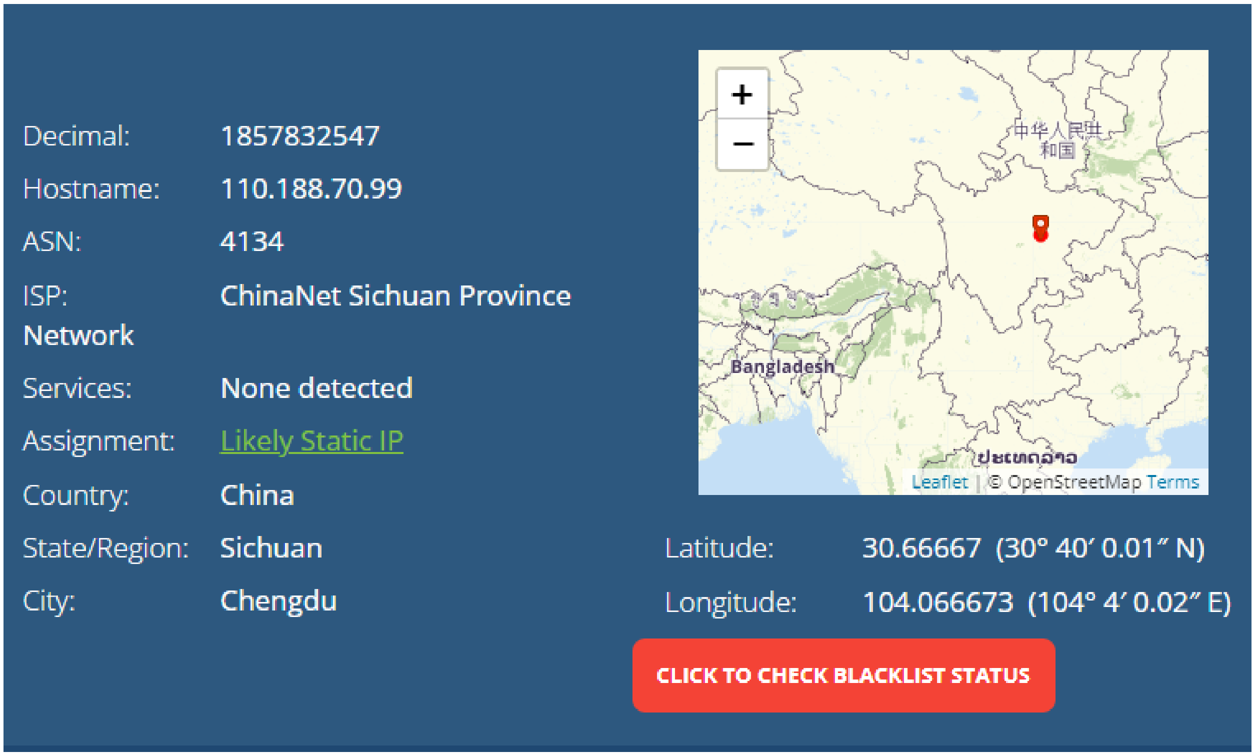
```
cat auth.log | grep "Disconnected" | cut -d " " -f 12 | sort | uniq
```

Menggunakan fungsi sort dan uniq agar tidak terjadi duplikat IP yang sama.



```
103.121.117.181
103.145.107.232
103.145.154.250
103.145.155.250
103.48.116.47
103.73.73.66
103.85.234.21
103.94.129.17
103.96.151.129
104.131.93.33
104.236.0.161
104.236.246.16
104.236.33.82
104.238.116.19
104.248.144.147
104.248.181.156
106.14.61.79
107.170.172.23
107.170.212.116
108.5.182.59
108.58.17.122
109.132.156.112
109.167.210.163
```

5. Track salah satu IP menggunakan situs https://whatismyipaddress.com/



Decimal: 1857832547

Hostname: 110.188.70.99

ASN: 4134

ISP: ChinaNet Sichuan Province

Network

Services: None detected

Assignment: Likely Static IP

Country: China

State/Region: Sichuan

City: Chengdu

Latitude: 30.66667 (30° 40′ 0.01″ N)

Longitude: 104.066673 (104° 4′ 0.02″ E)

+
−
中华人民共和国
Bangladesh
ປະເທດລາວ
Leaflet | © OpenStreetMap Terms
CLICK TO CHECK BLACKLIST STATUS

terdeteksi IP tersebut berasal dari negara China