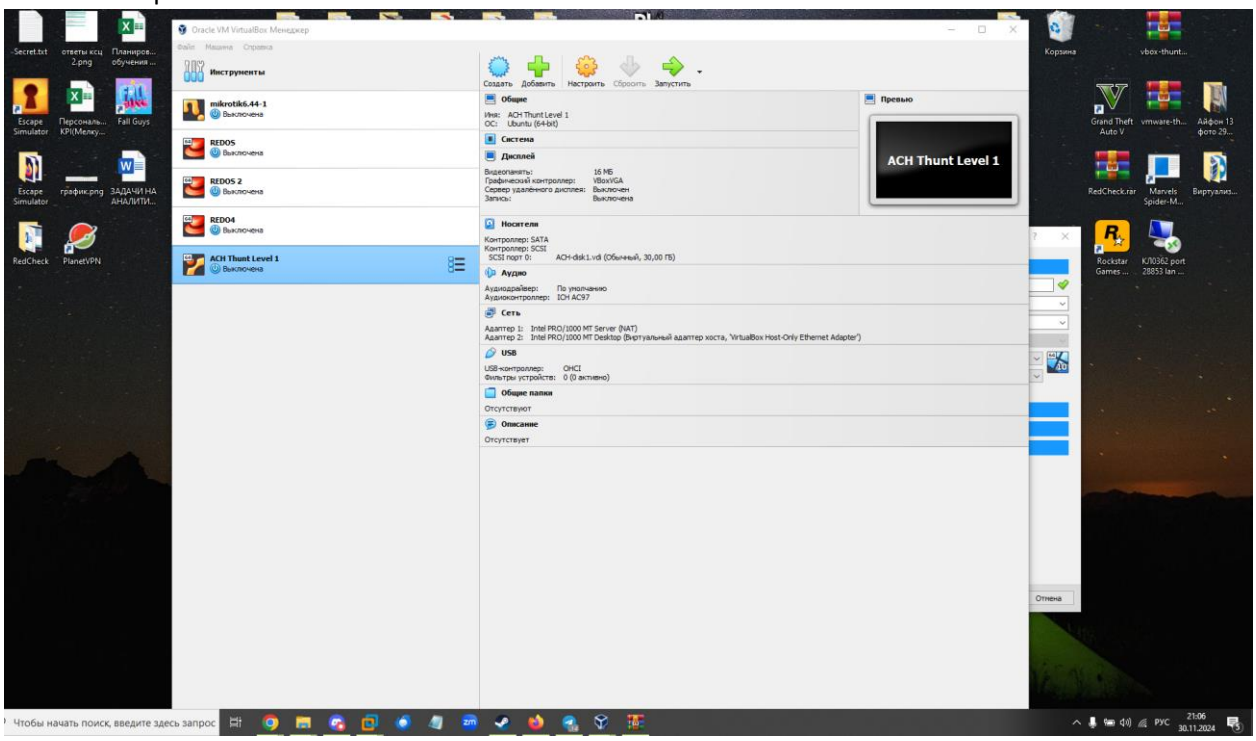
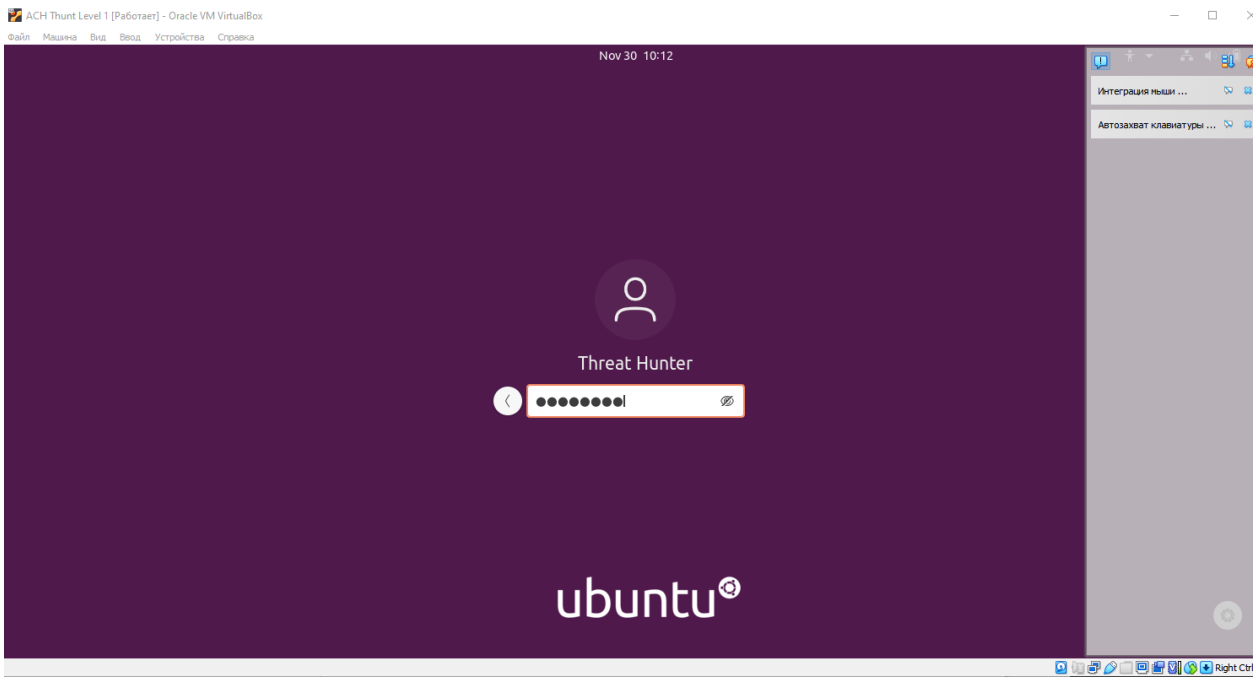
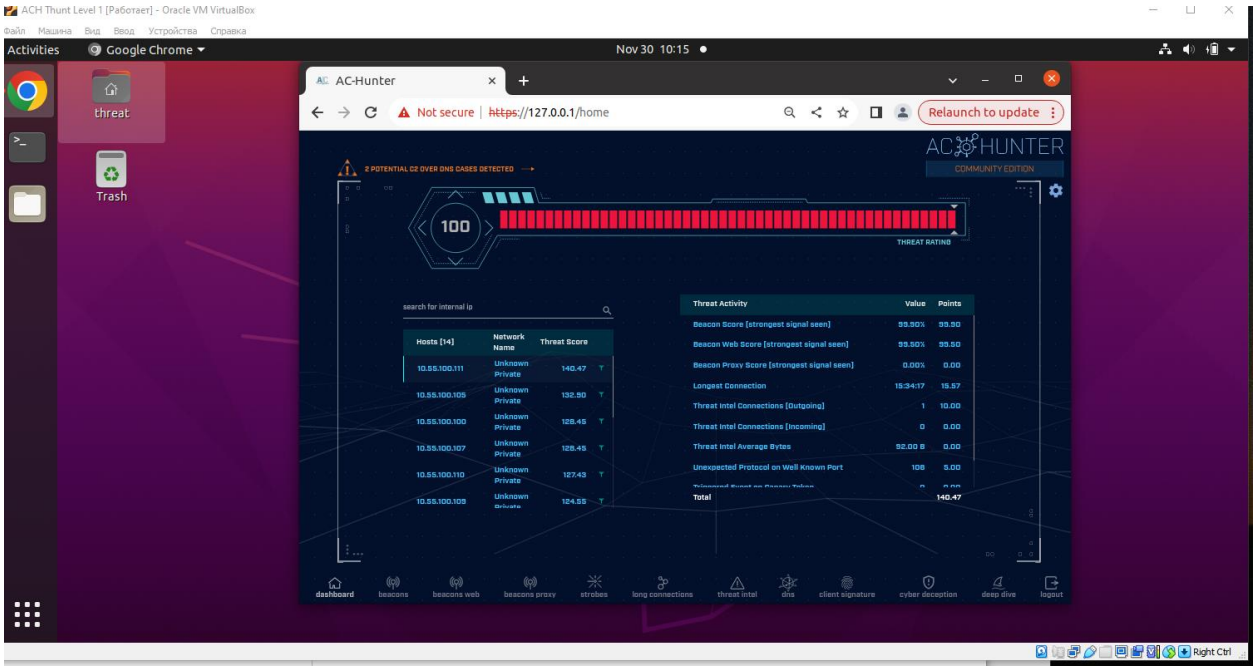
Скачиваем файл

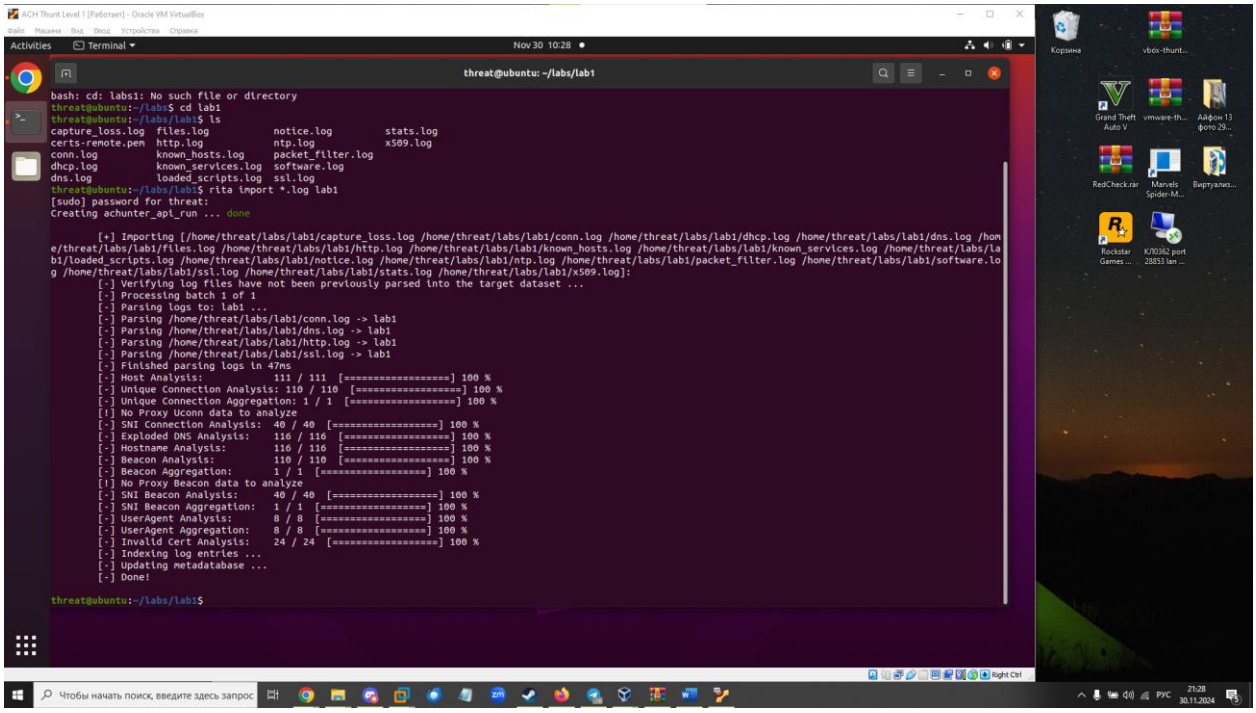


Открываем его

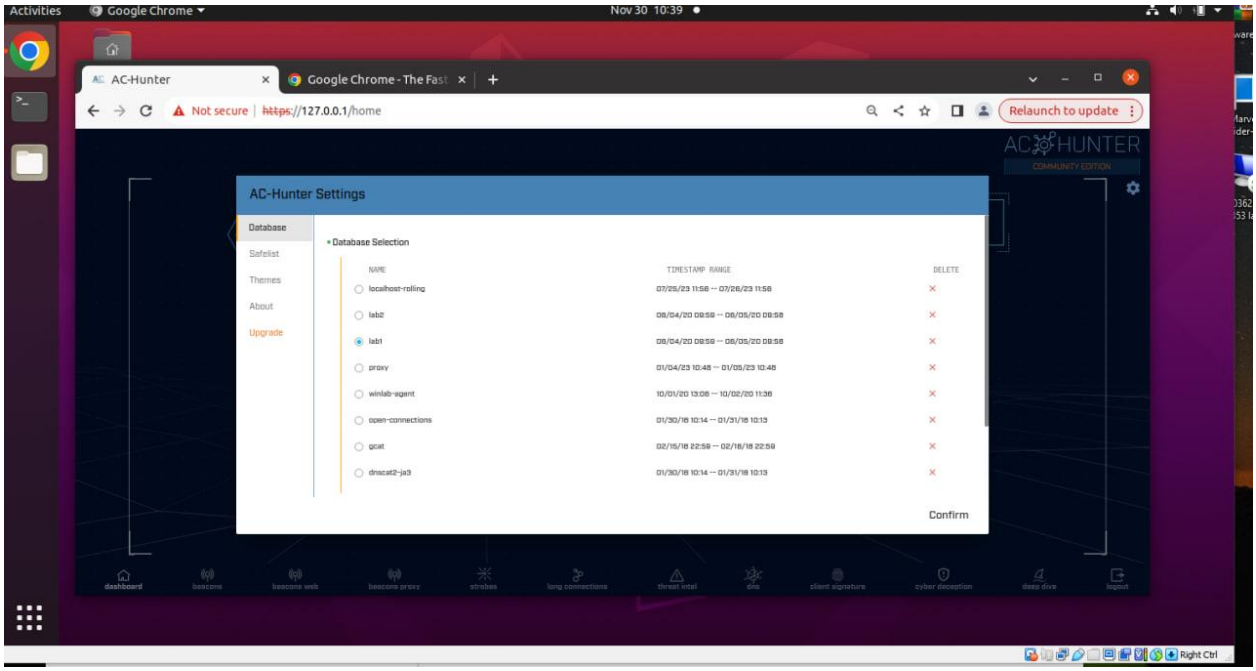




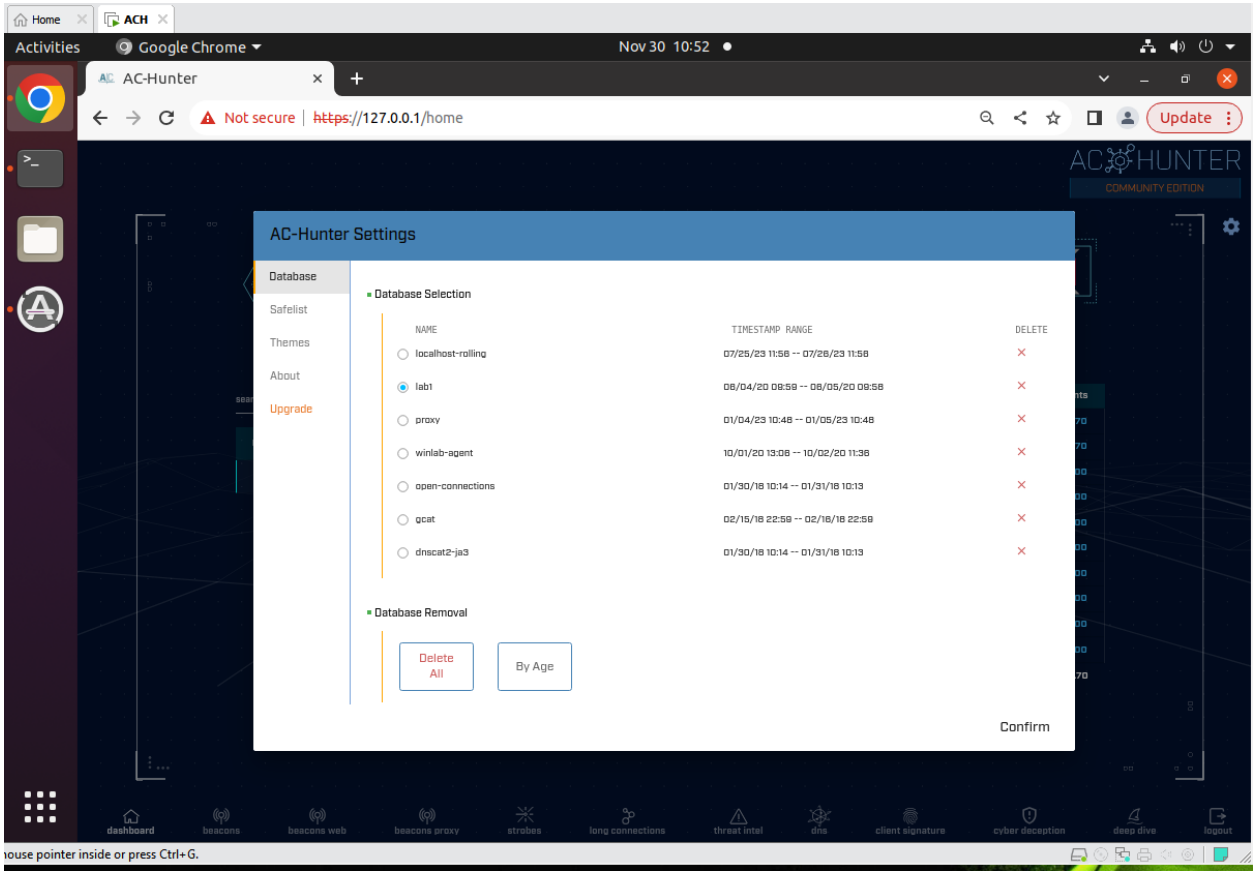
Произвожу импорт логов

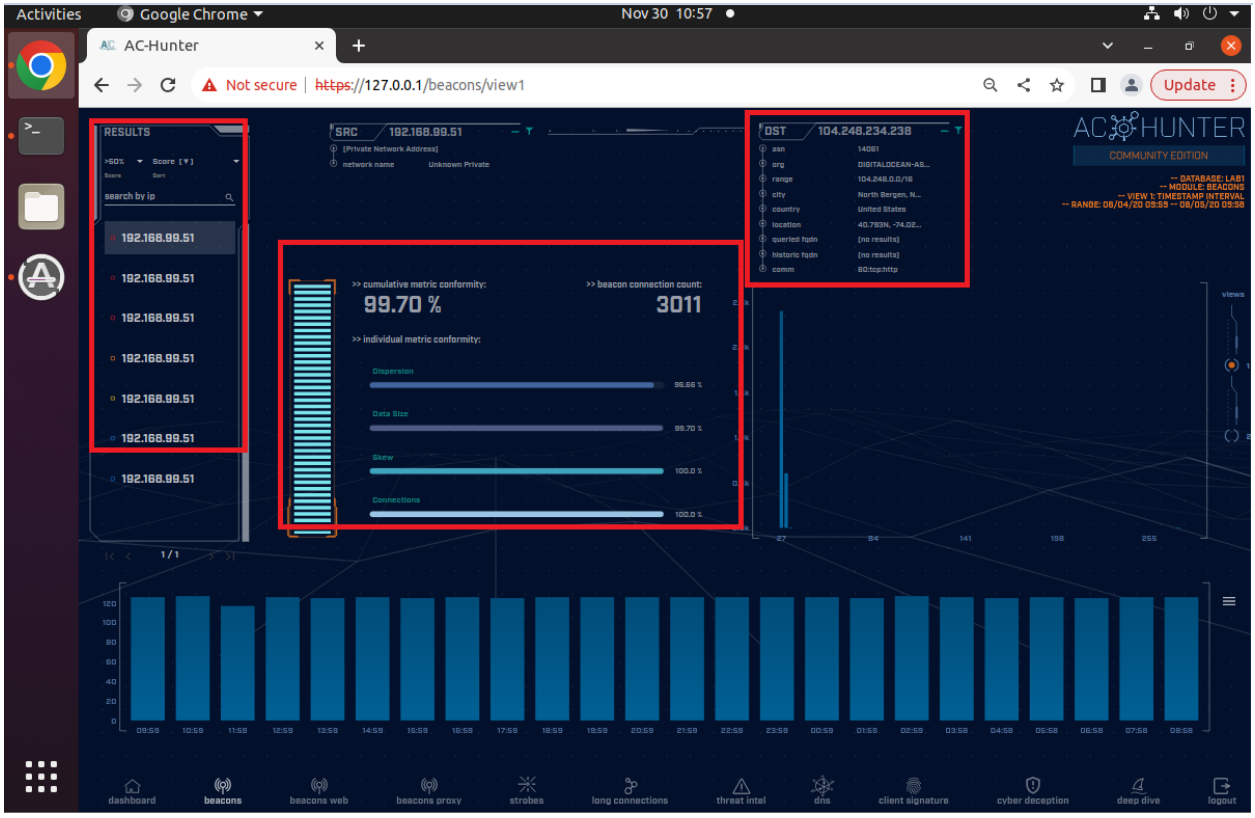


Я переместился в VMARE потому что почему-то в виртуалбоксе у меня пропало всё после того как я выбрал lab1

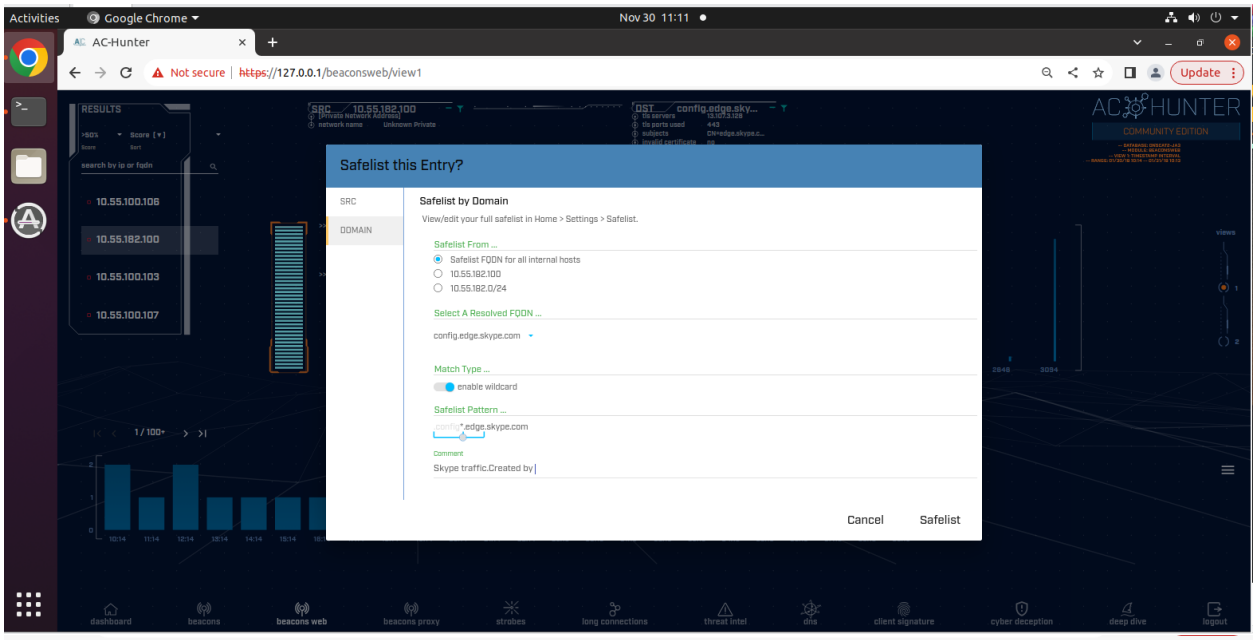


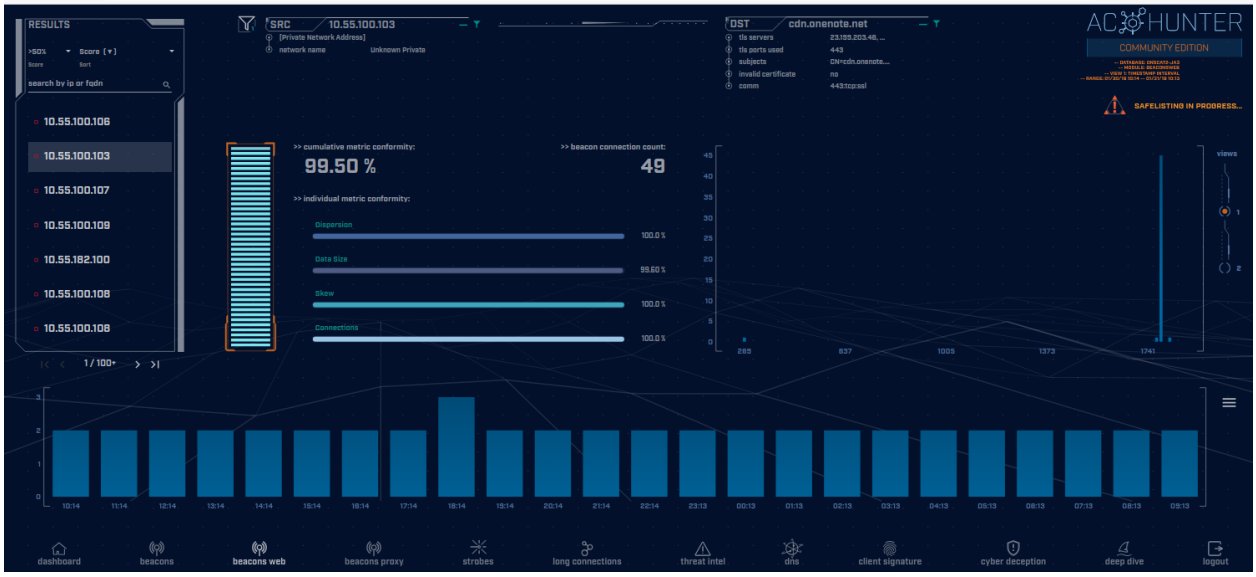
Выбрал снова lab1 и открыл снова



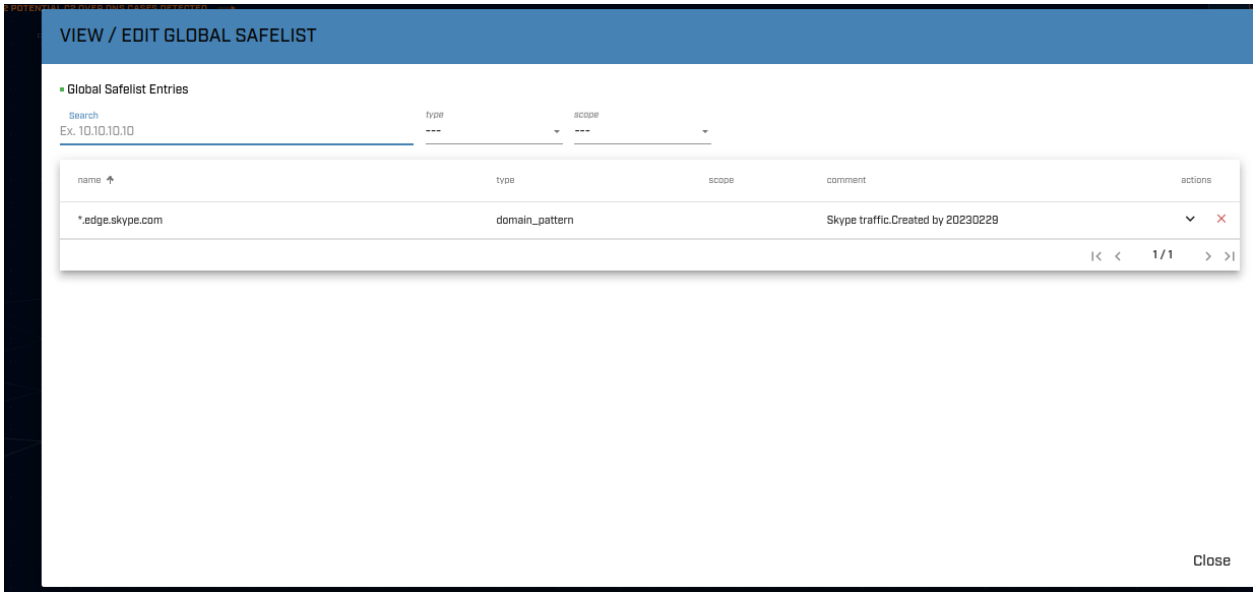


В руководстве сказано добавить скайп в сэйфлист

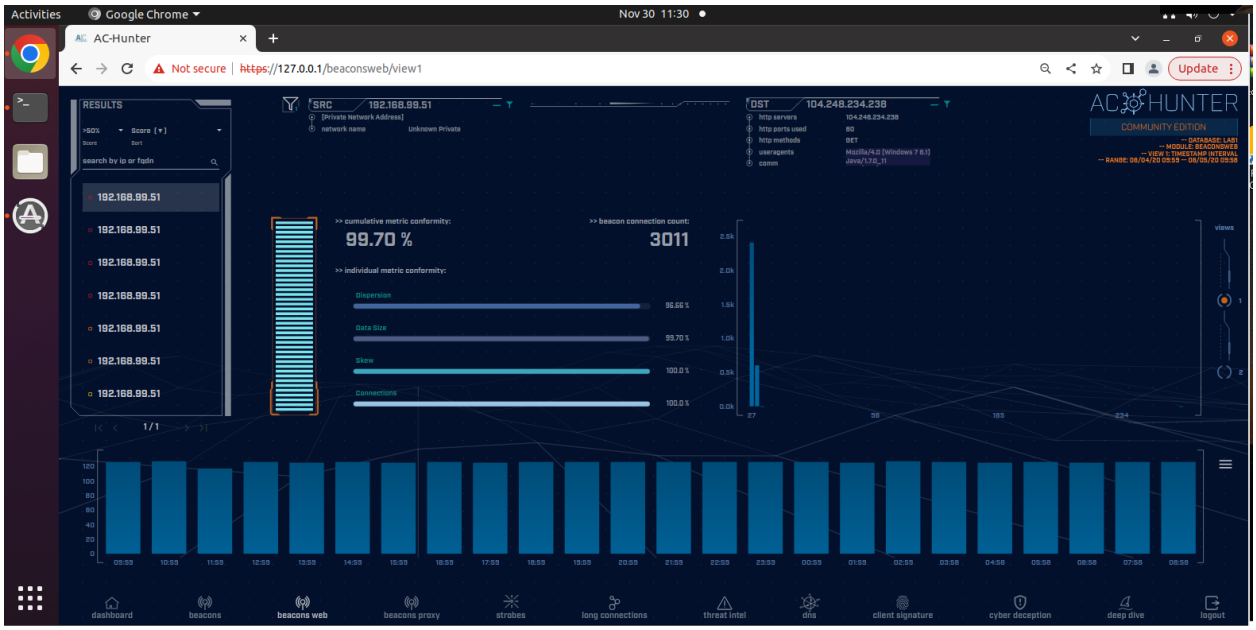




Проверяем появился ли сэйфлист



Начинается анализ событий из lab1

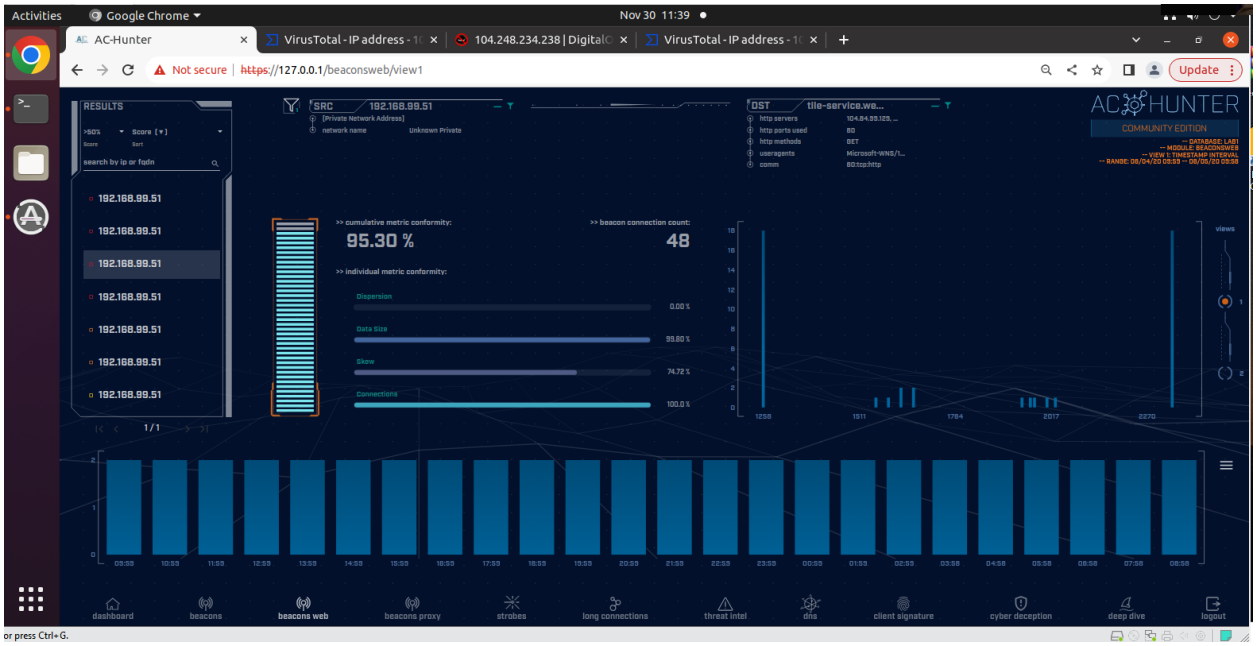


Большое количество подключений за последние 24 часа (3 011).

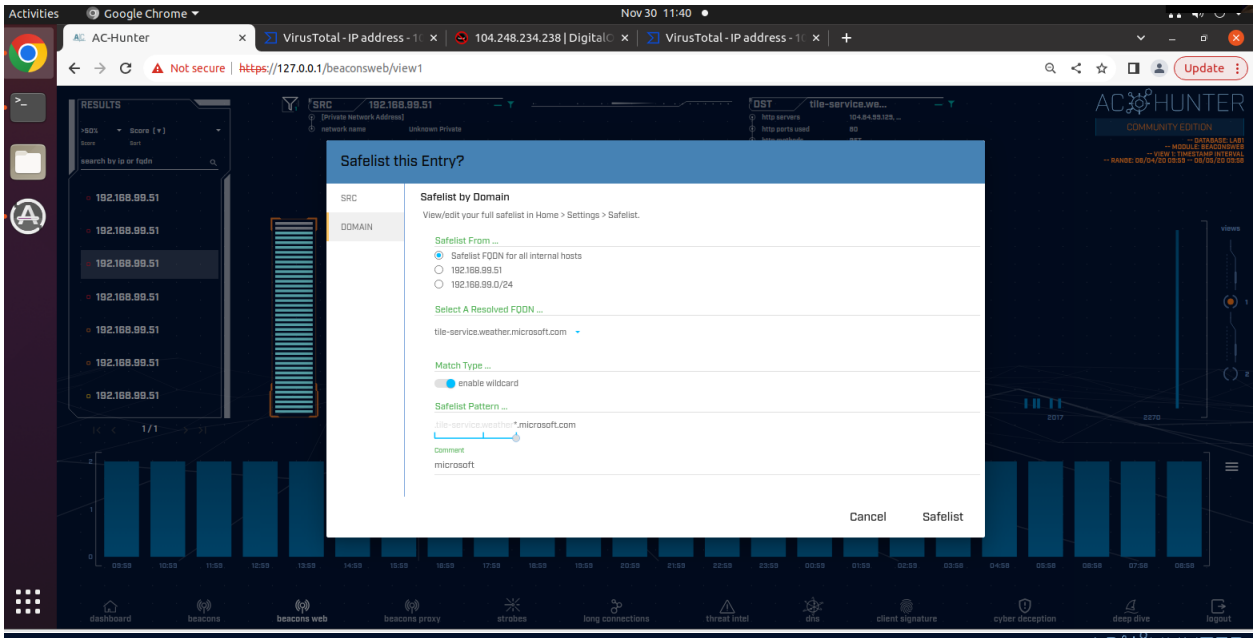
Гистограмма ровная.

Отсутствует строка хостинга. полное доменное имя веб-сервера?

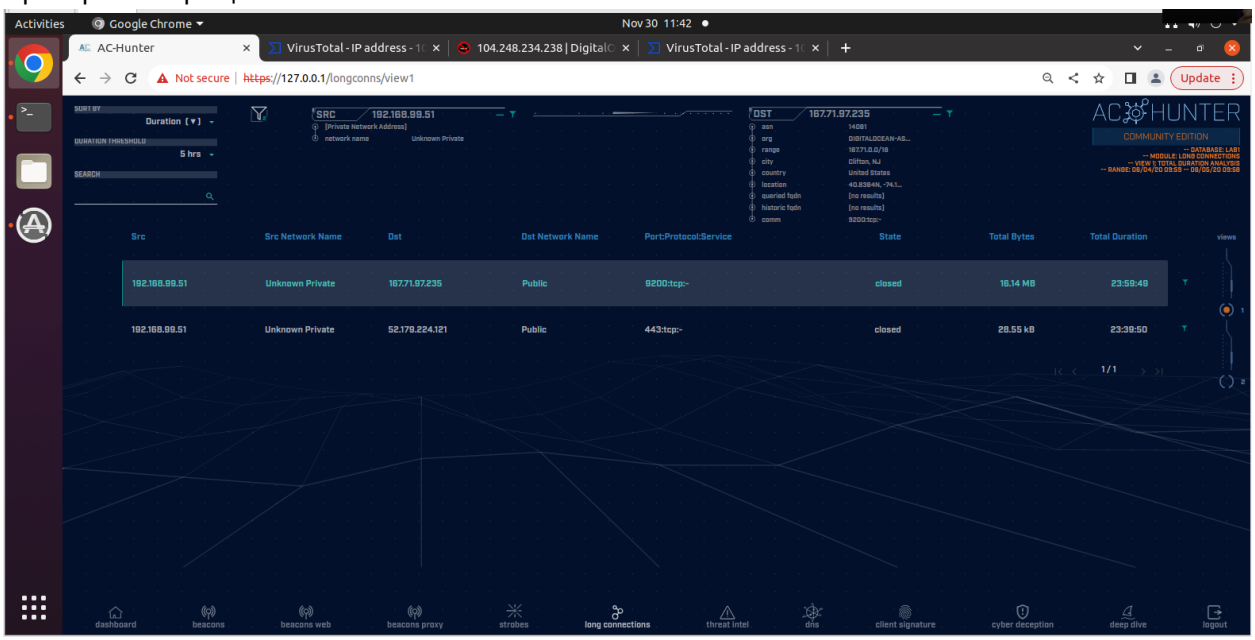
Проверим каждое соединение

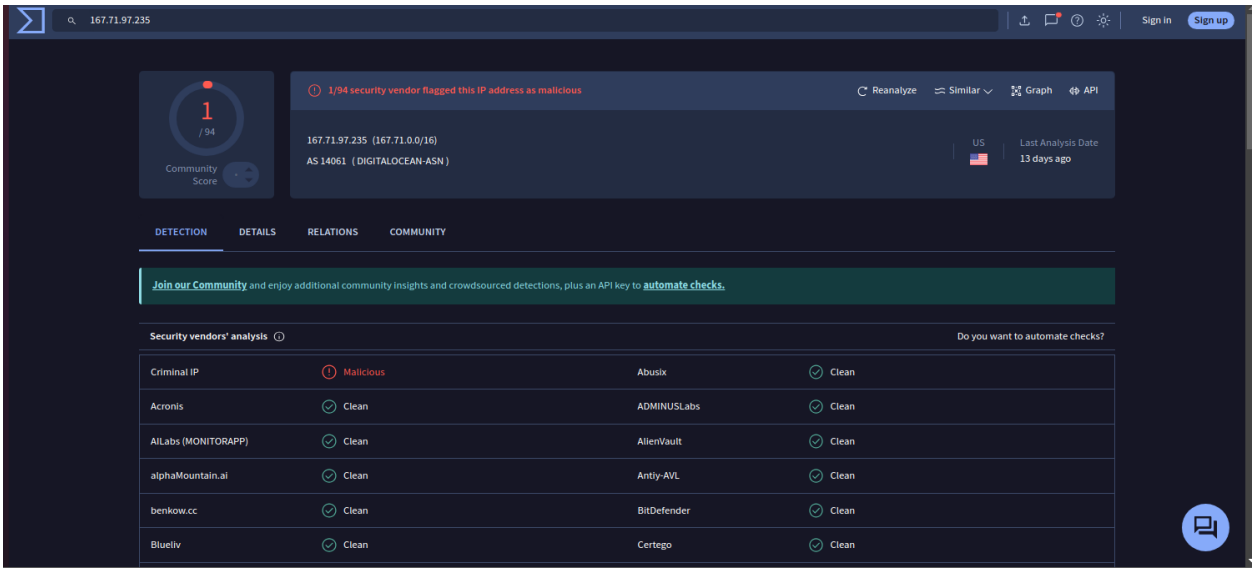


Убрал несколько адресов в safelist дабы убрать false positive срабатывания.



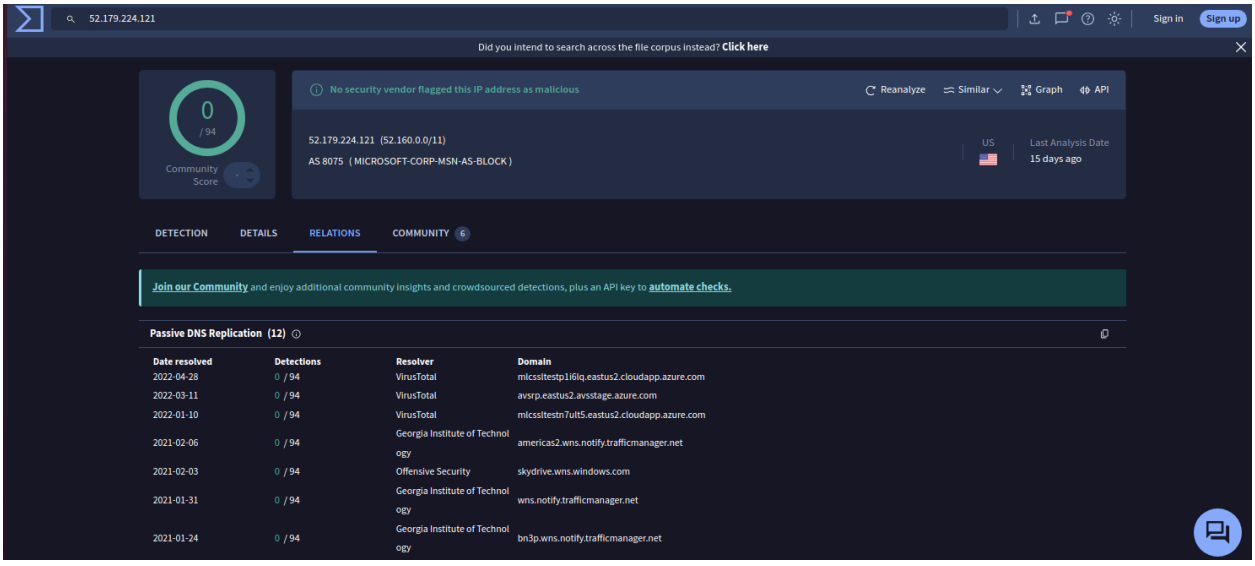
Проверяем обращения





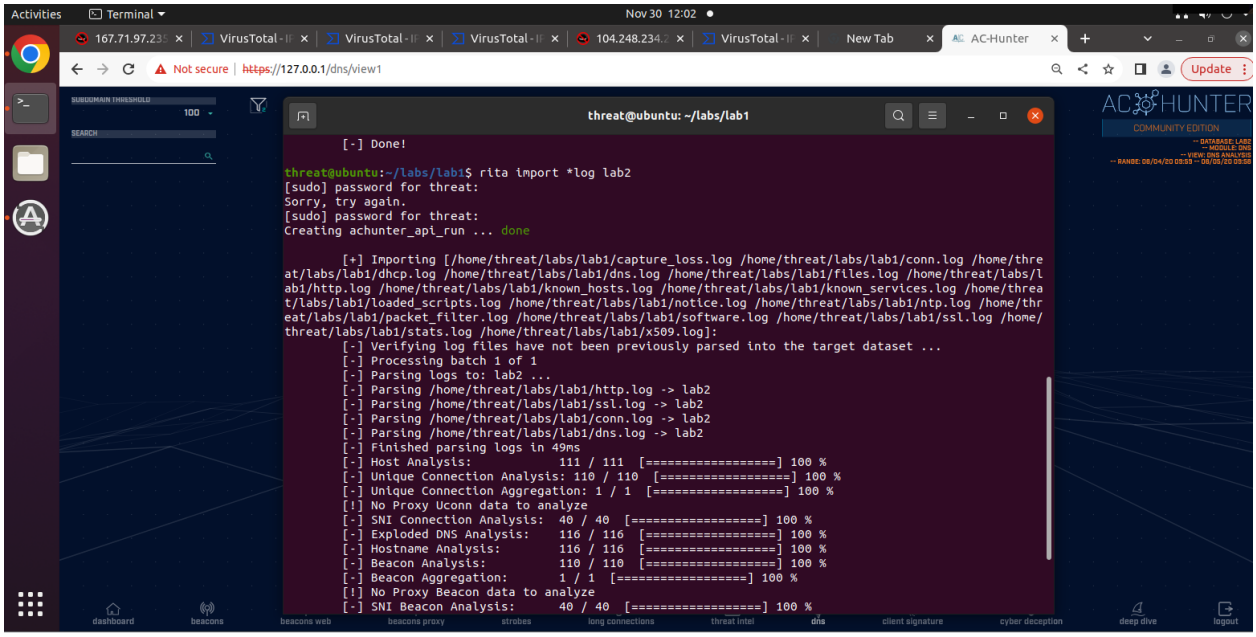
1 на него сильно поругался,не знаю считать ли это чем-то сильно нелегитимным…

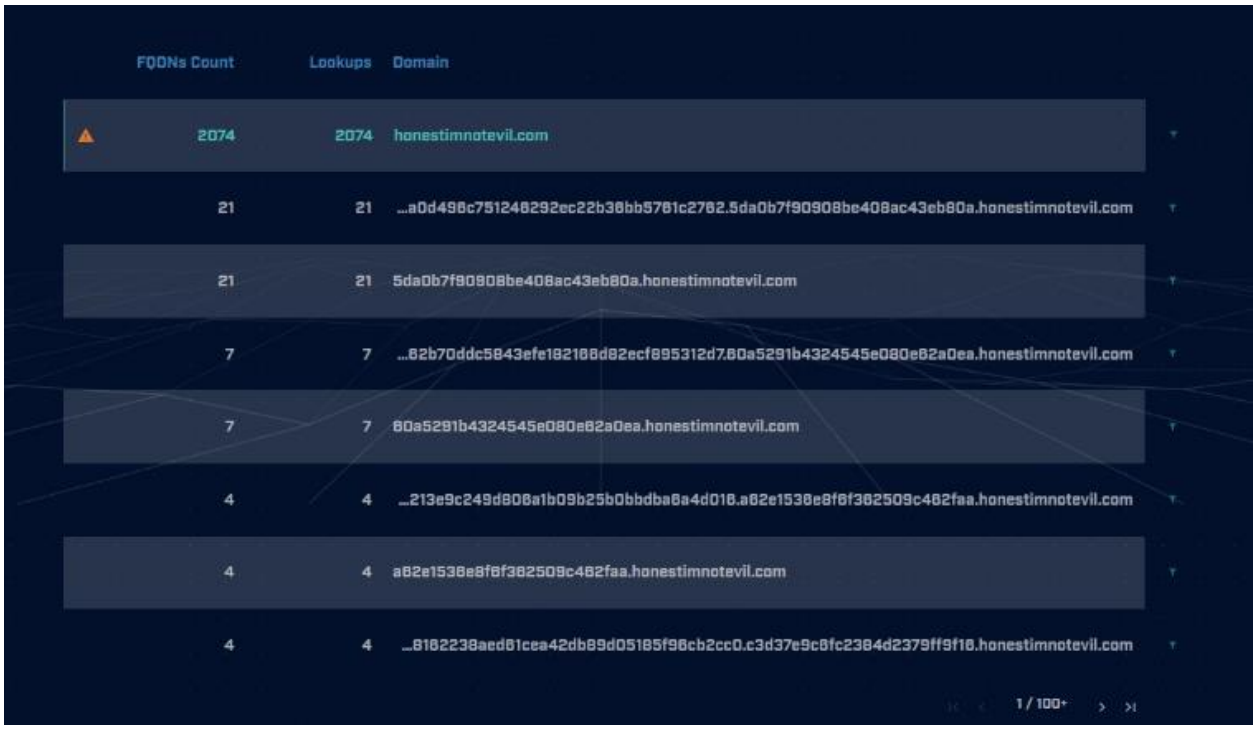
Второй адрес



Как итог,мне не нарвистя как я и указал ранее про 3000 соединений с высоким beacon score,много строк пропущено,мне не нравится FQDN,хоста в заголовке HTTP

Перехожу к lab2





Тут всё очень быстро, огромное обращение к днс

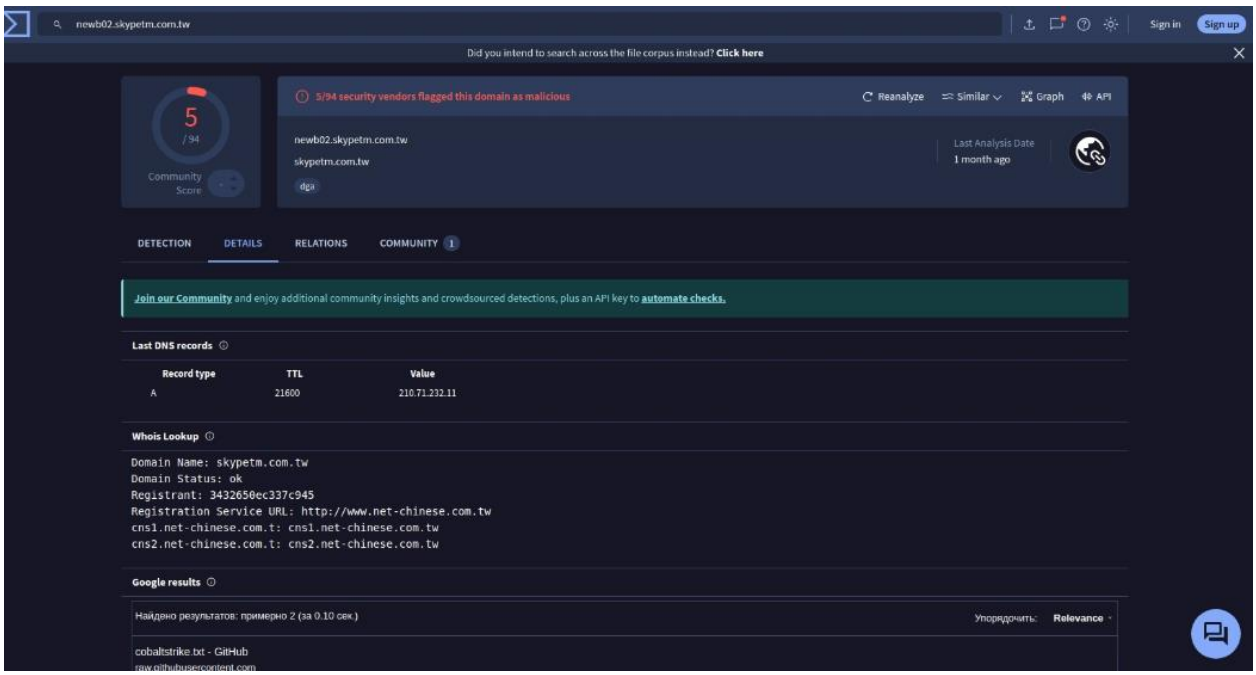
Переходим к lab3

```
threat@ubuntu:~/labs/lab1$ rita import *log lab3
Creating achunter_api_run ... done

       [+] Importing [/home/threat/labs/lab1/capture_loss.log /home/threat/labs/lab1/conn.log /home/threat/labs/lab1/dhcp.log
 /home/threat/labs/lab1/dns.log /home/threat/labs/lab1/files.log /home/threat/labs/lab1/http.log /home/threat/labs/lab1/known_
hosts.log /home/threat/labs/lab1/known_services.log /home/threat/labs/lab1/loaded_scripts.log /home/threat/labs/lab1/notice.lo
g /home/threat/labs/lab1/ntp.log /home/threat/labs/lab1/packet_filter.log /home/threat/labs/lab1/software.log /home/threat/lab
s/lab1/ssl.log /home/threat/labs/lab1/stats.log /home/threat/labs/lab1/x509.log]:
       [-] Verifying log files have not been previously parsed into the target dataset ...
       [-] Processing batch 1 of 1
       [-] Parsing logs to: lab3 ...
       [-] Parsing /home/threat/labs/lab1/conn.log -> lab3
       [-] Parsing /home/threat/labs/lab1/dns.log -> lab3
       [-] Parsing /home/threat/labs/lab1/http.log -> lab3
       [-] Parsing /home/threat/labs/lab1/ssl.log -> lab3
       [-] Finished parsing logs in 89ms
       [-] Host Analysis:            111 / 111  [==================] 100 %
       [-] Unique Connection Analysis: 110 / 110  [==================] 100 %
       [-] Unique Connection Aggregation: 1 / 1  [==================] 100 %
       [!] No Proxy Uconn data to analyze
       [-] SNI Connection Analysis:  40 / 40  [==================] 100 %
       [-] Exploded DNS Analysis:    116 / 116  [==================] 100 %
       [-] Hostname Analysis:        116 / 116  [==================] 100 %
       [-] Beacon Analysis:          110 / 110  [==================] 100 %
       [-] Beacon Aggregation:       1 / 1  [==================] 100 %
       [!] No Proxy Beacon data to analyze
       [-] SNI Beacon Analysis:      40 / 40  [==================] 100 %
       [-] SNI Beacon Aggregation:   1 / 1  [==================] 100 %
       [-] UserAgent Analysis:       8 / 8  [==================] 100 %
       [-] UserAgent Aggregation:    8 / 8  [==================] 100 %
       [-] Invalid Cert Analysis:    24 / 24  [==================] 100 %
       [-] Indexing log entries ...
       [-] Updating metadatabase ...
       [-] Done!

threat@ubuntu:~/labs/lab1$
```

Благодаря safe листам потенциальные FP события убраны и остаётся всего два,осталось узнать оба ли они опасны?(а может и ни один)



Проверяю и уже вижу что-то неладное,
гистограмма плоская, FQDN странный
Второй ip связан с Microsoft, добавляем в safelist

Собственно,на этом всё,данный ip нелегитимен