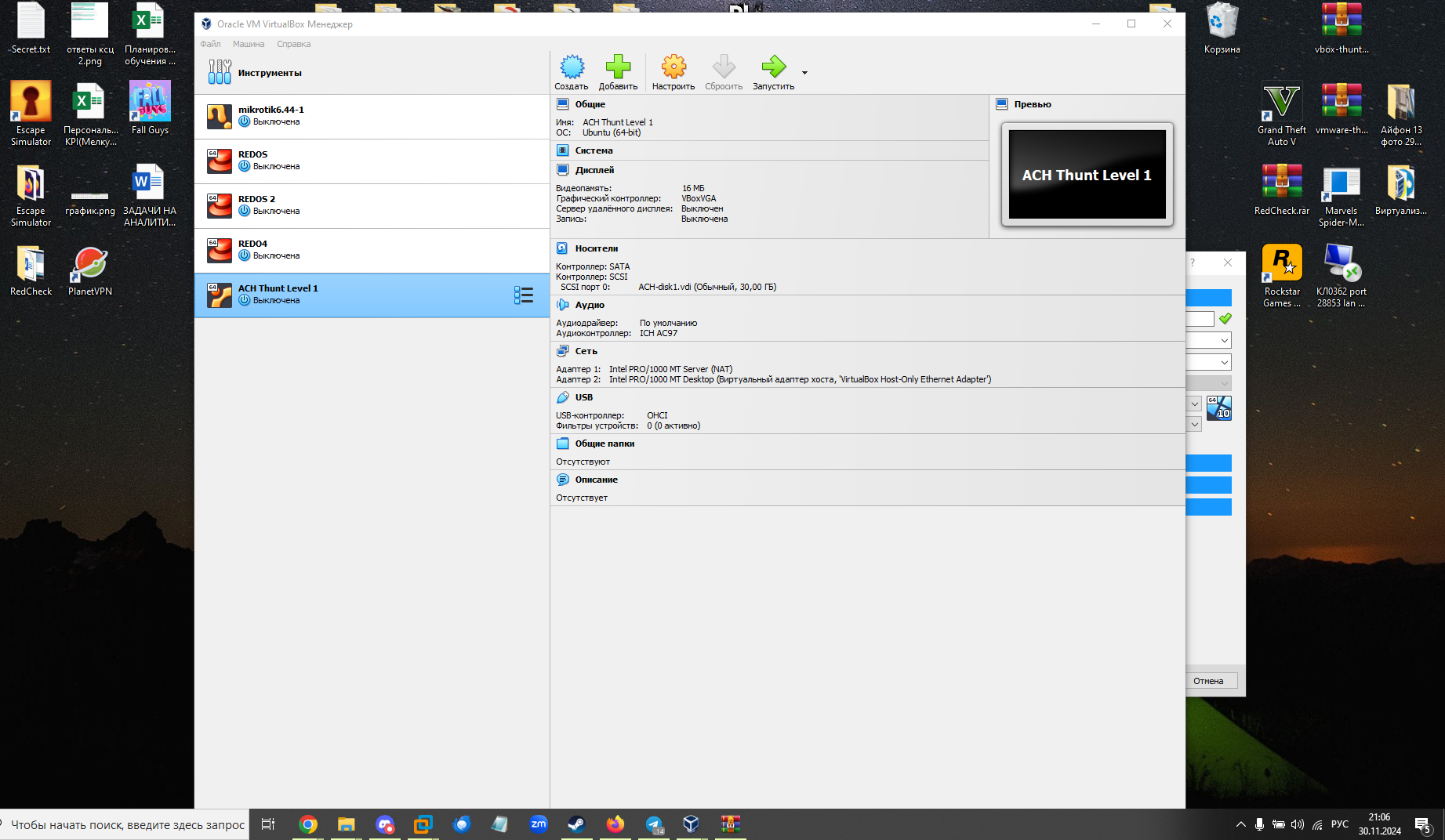
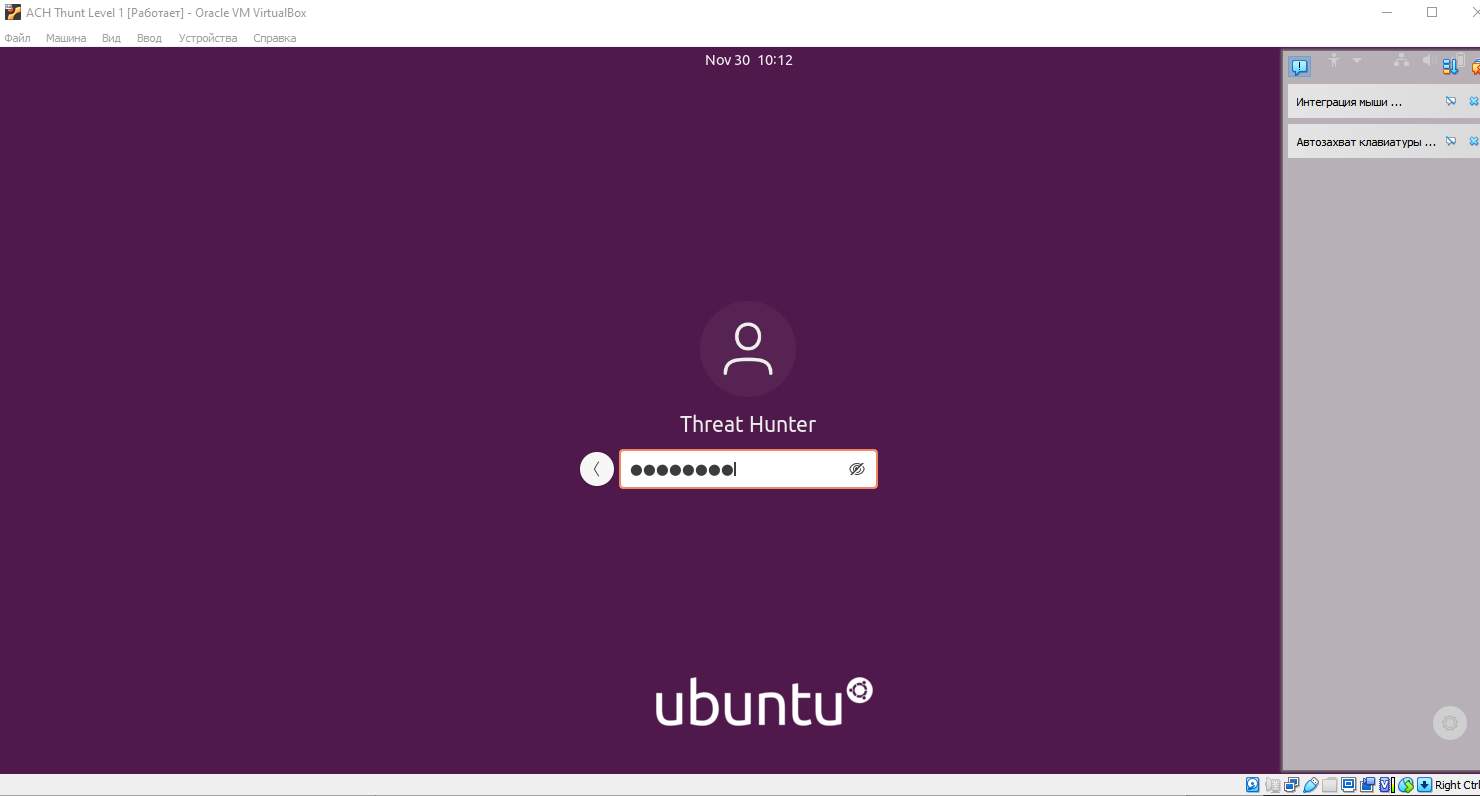
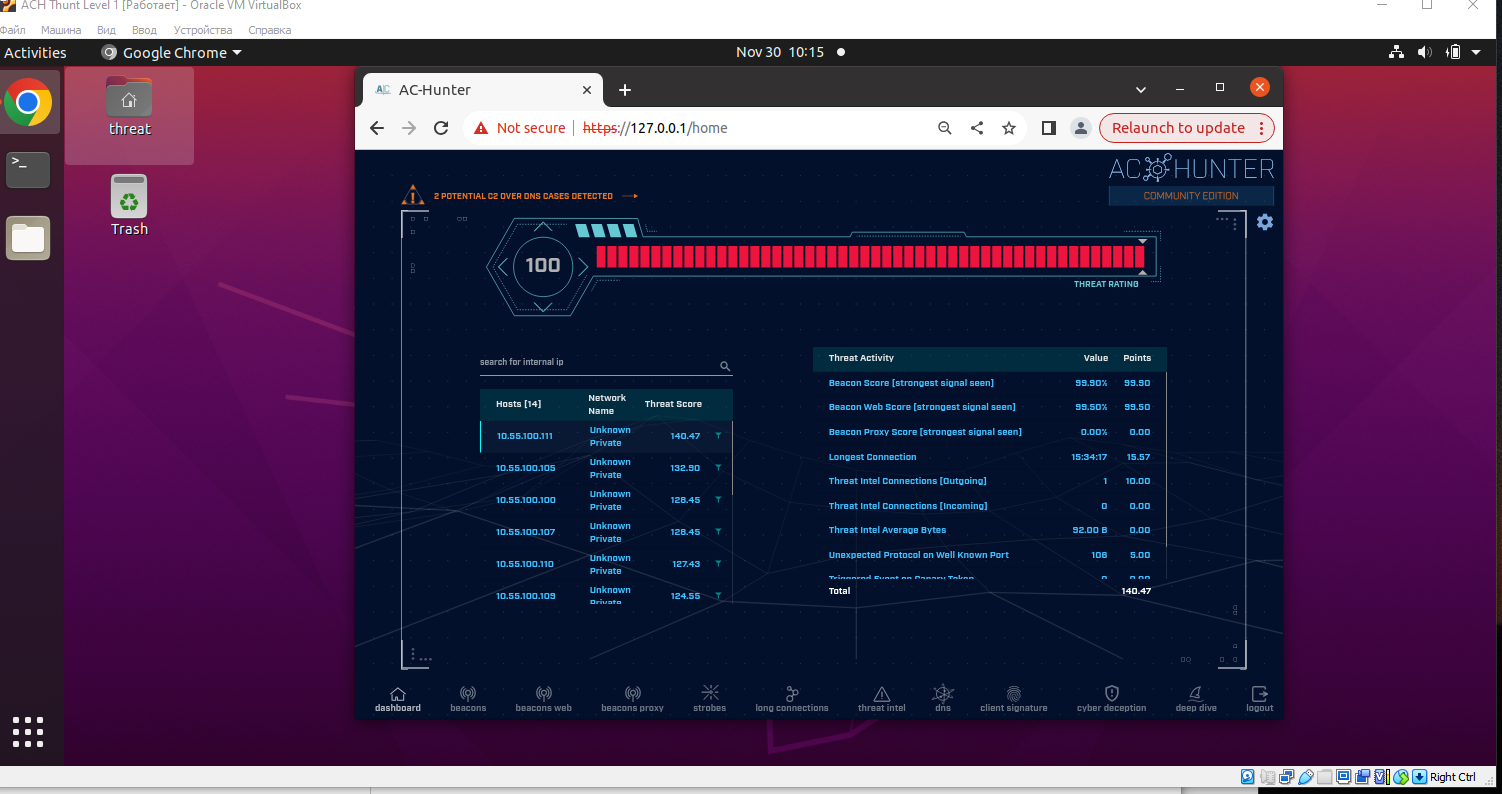
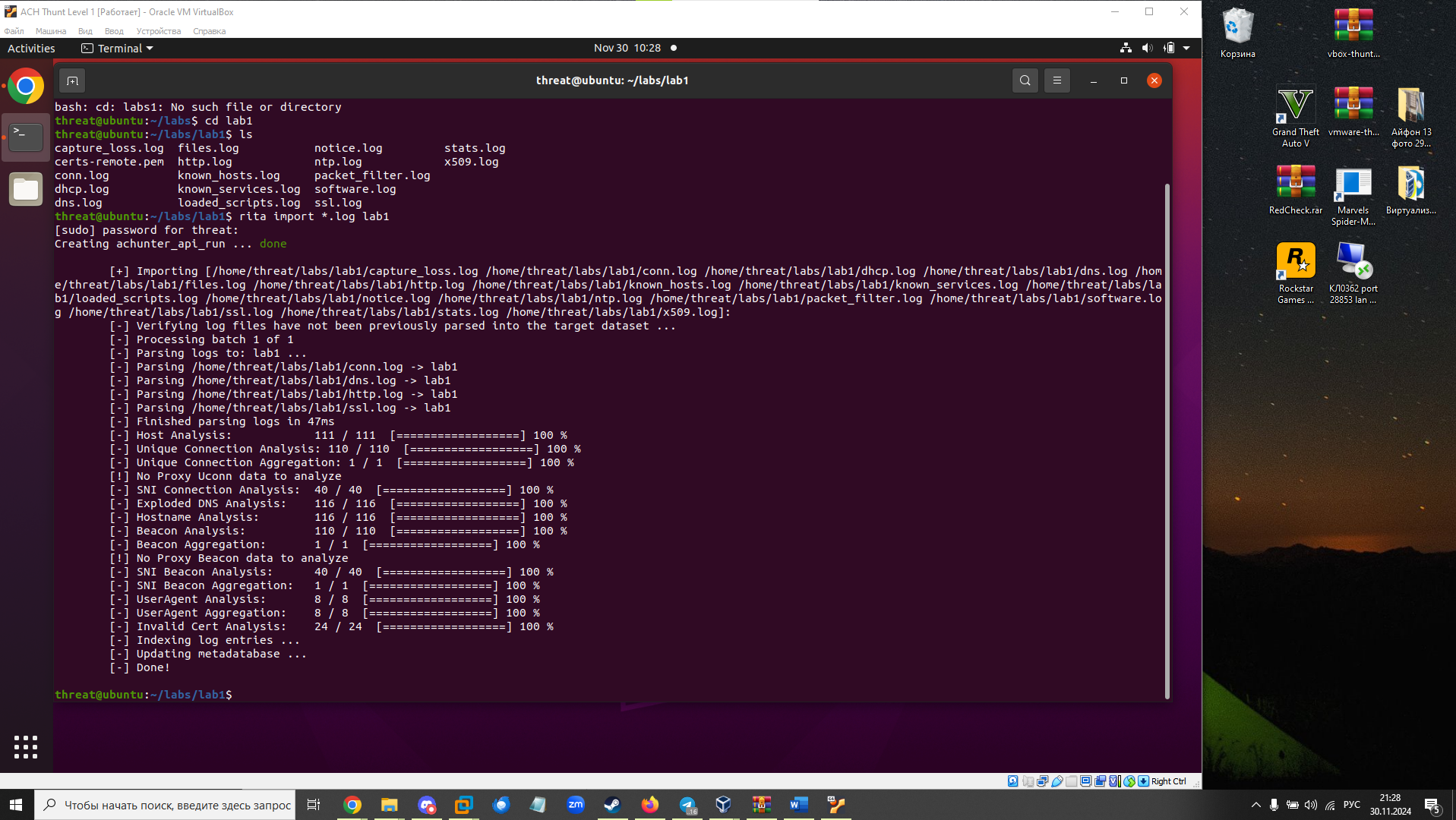
Скачиваем файл   


Открываем его

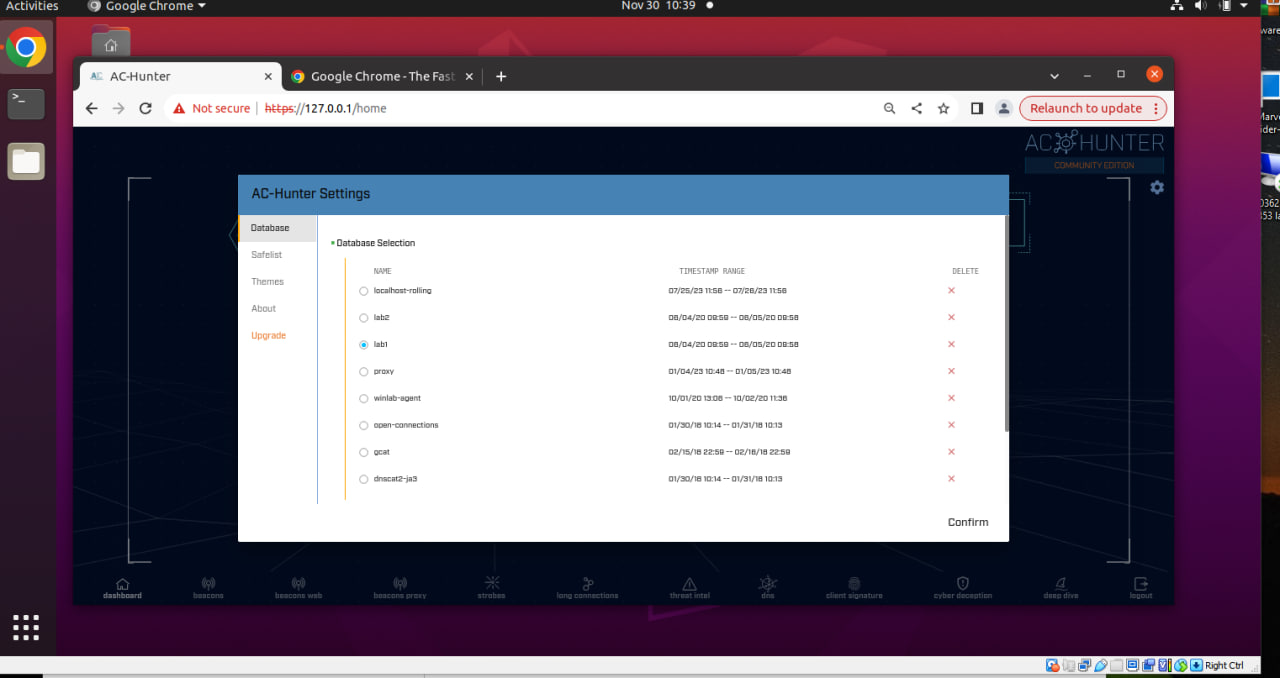


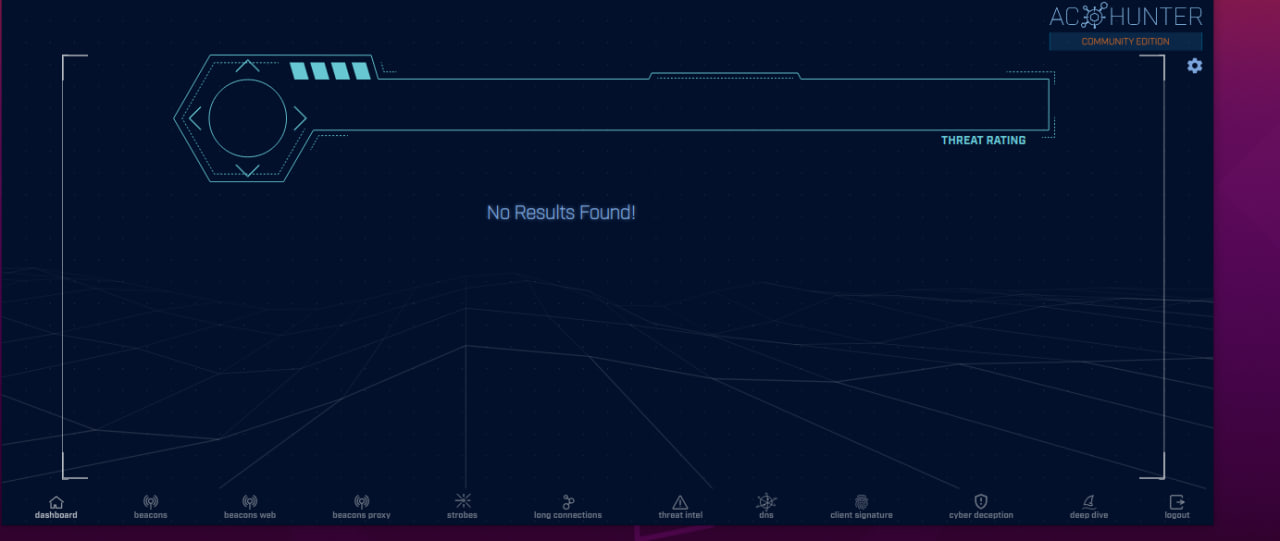


Произвожу импорт логов

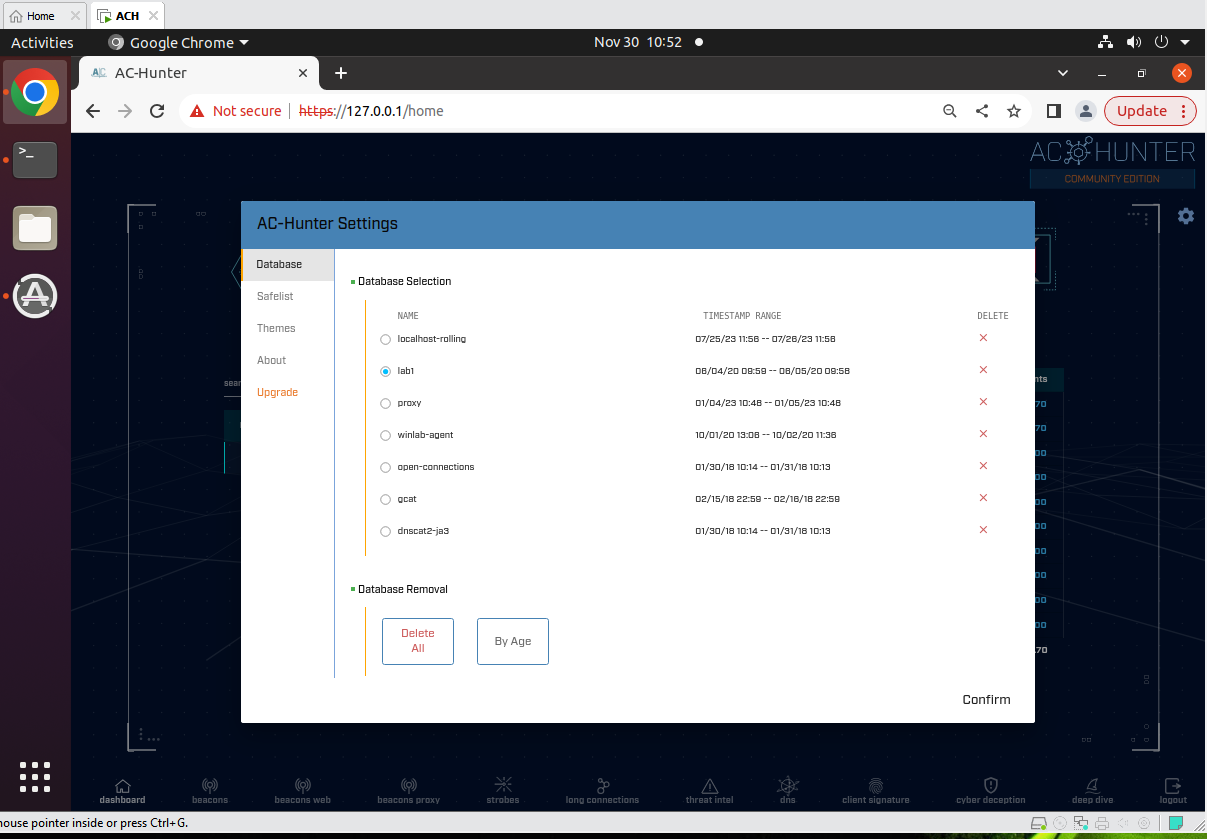


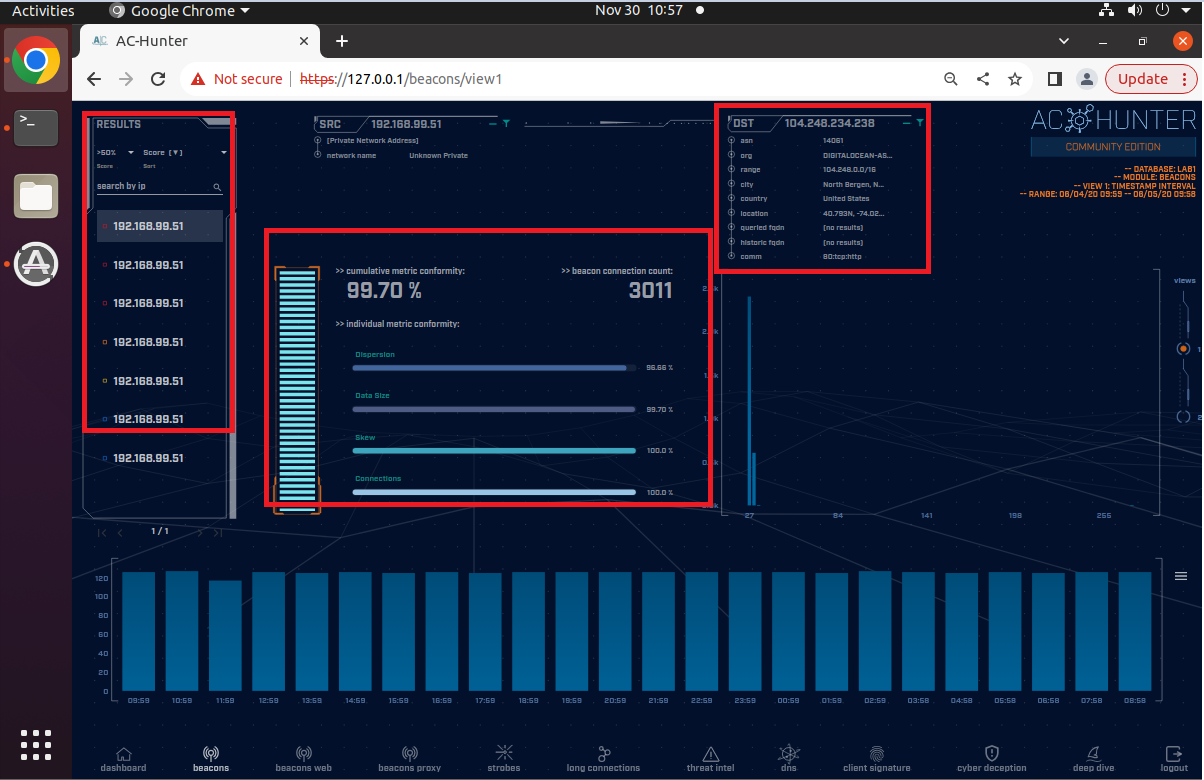
Я переместился в VMARE потому что почему-то в виртуалбоксе у меня пропало всё после того как я выбрал lab1

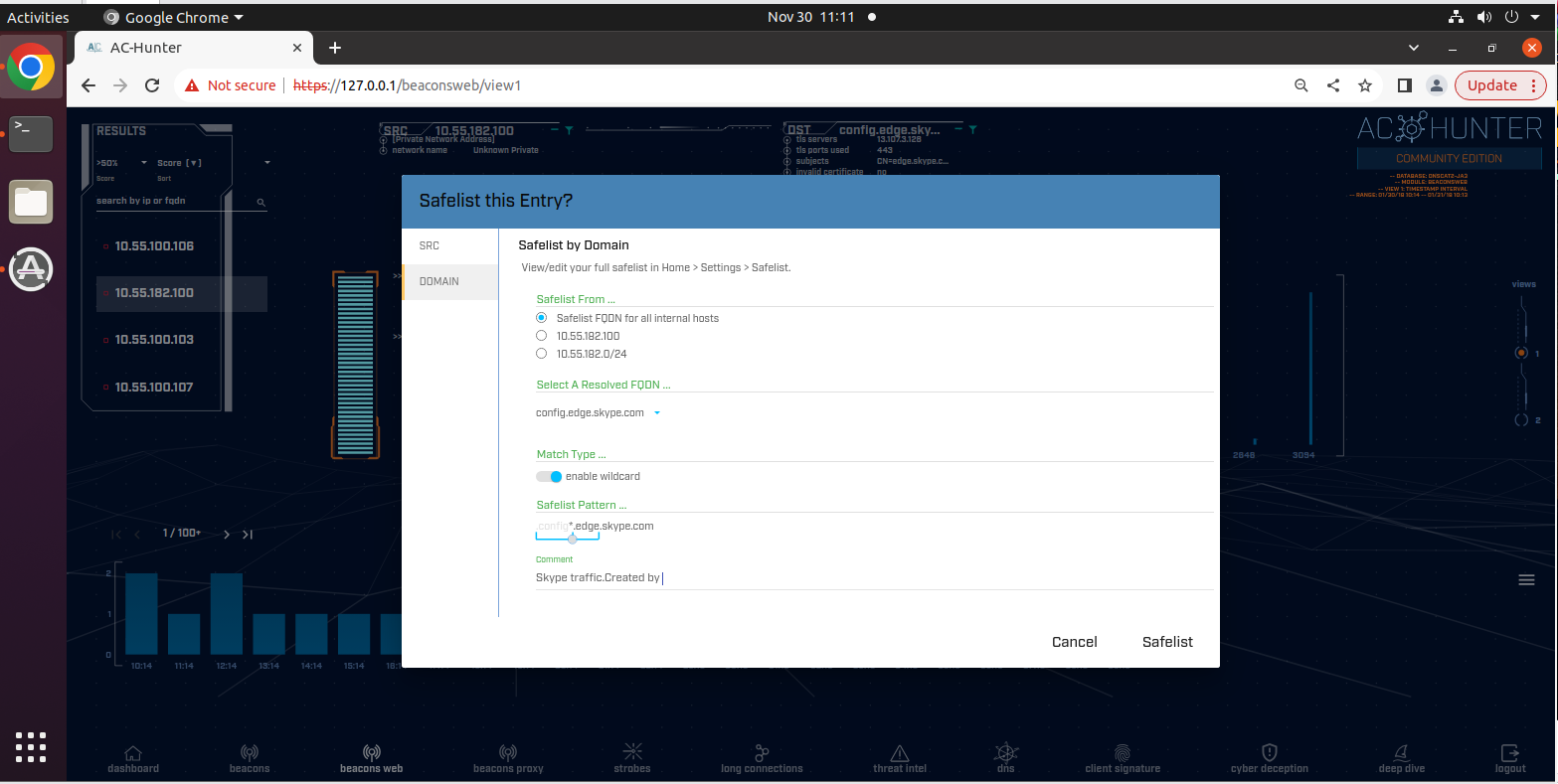
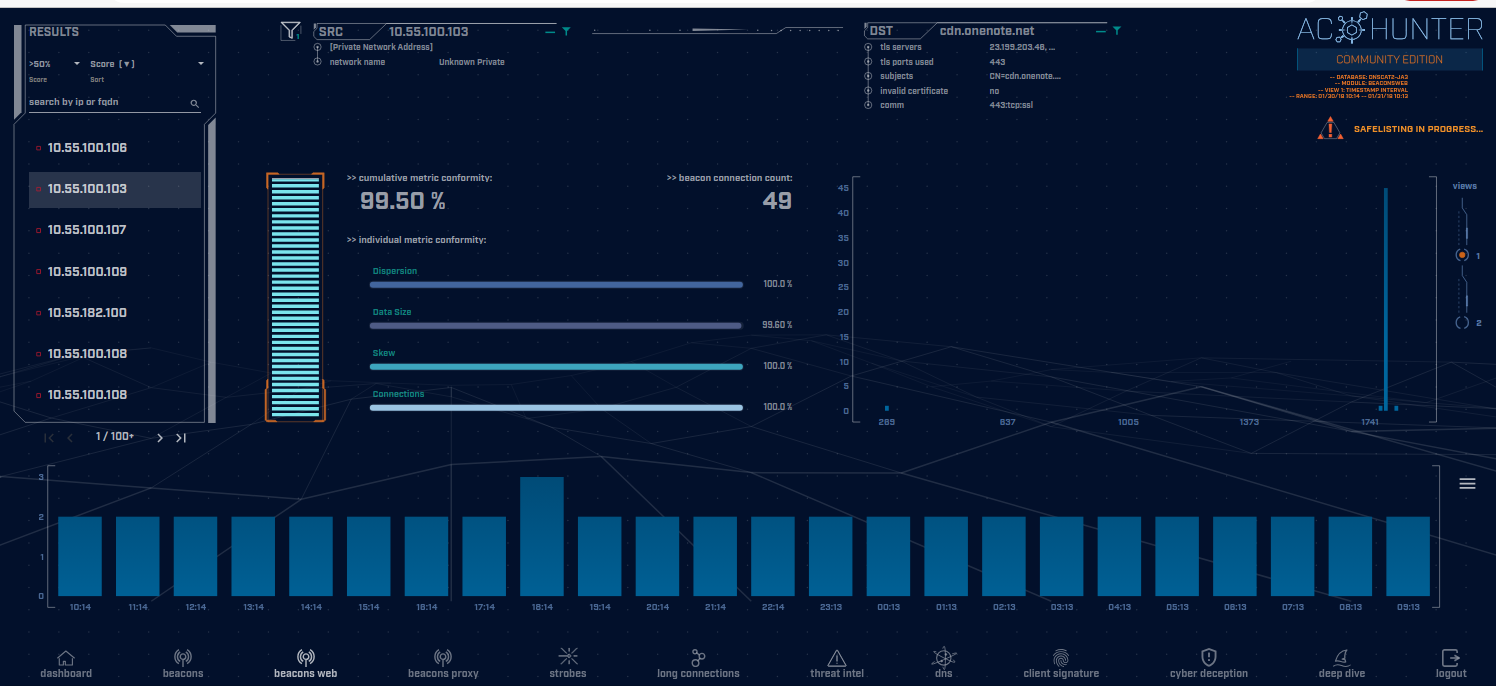




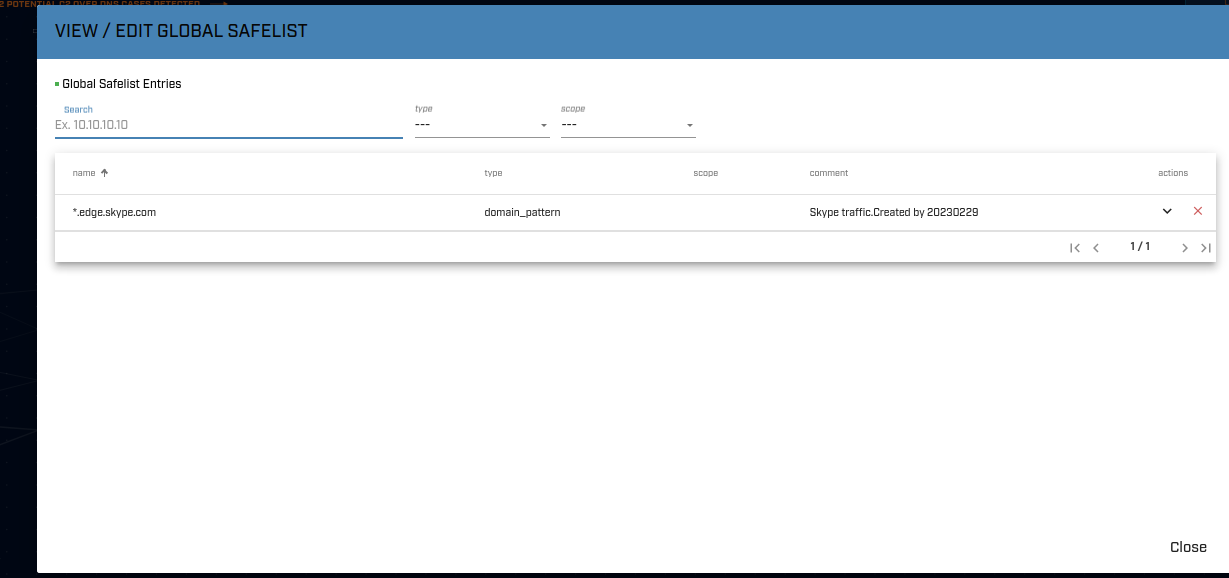
Выбрал снова lab1 и открыл снова



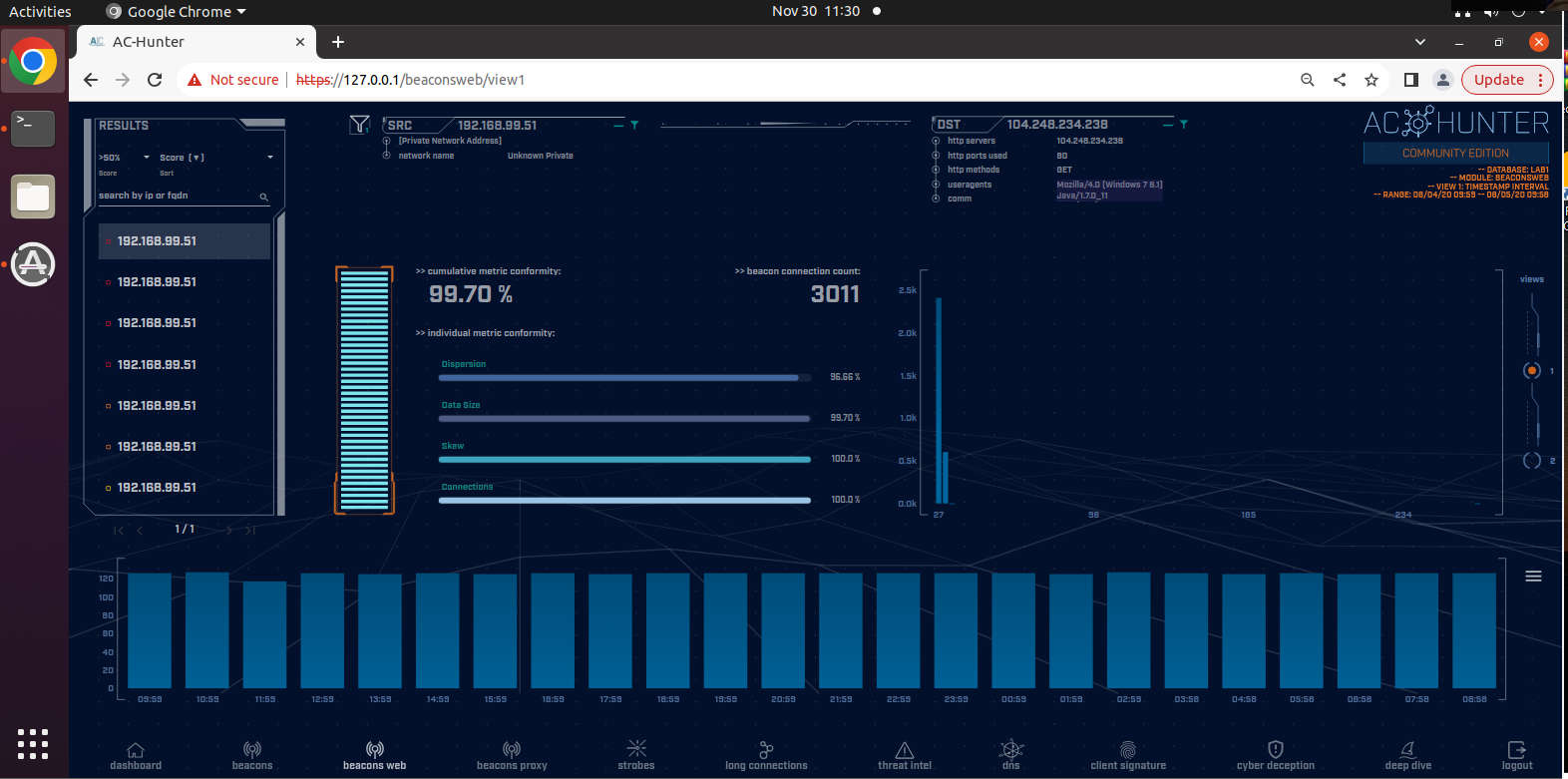


В руководстве сказано добавить скайп в сэйфлист   
 

Проверяем появился ли сэйфлист



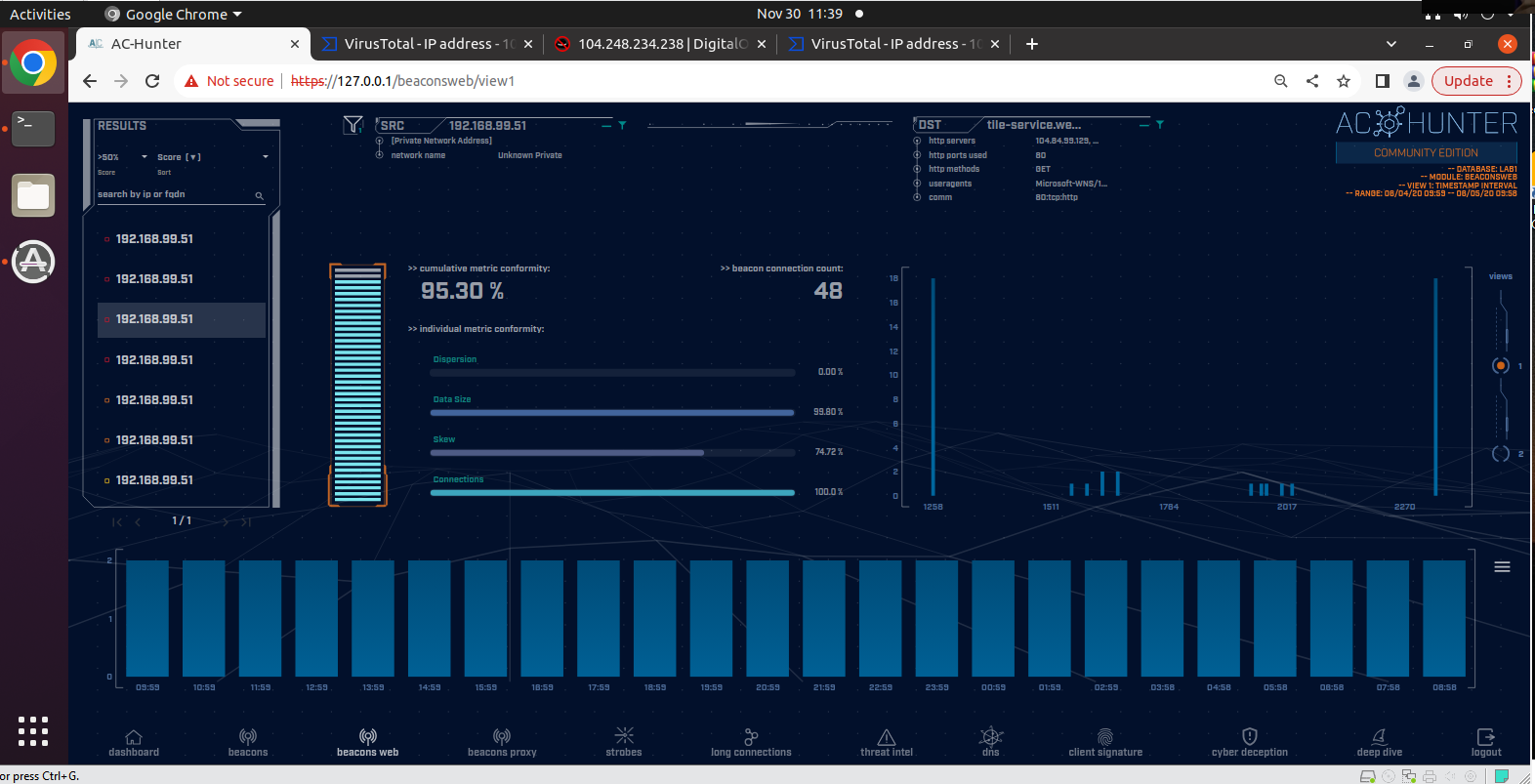
Начинается анализ событий из lab1



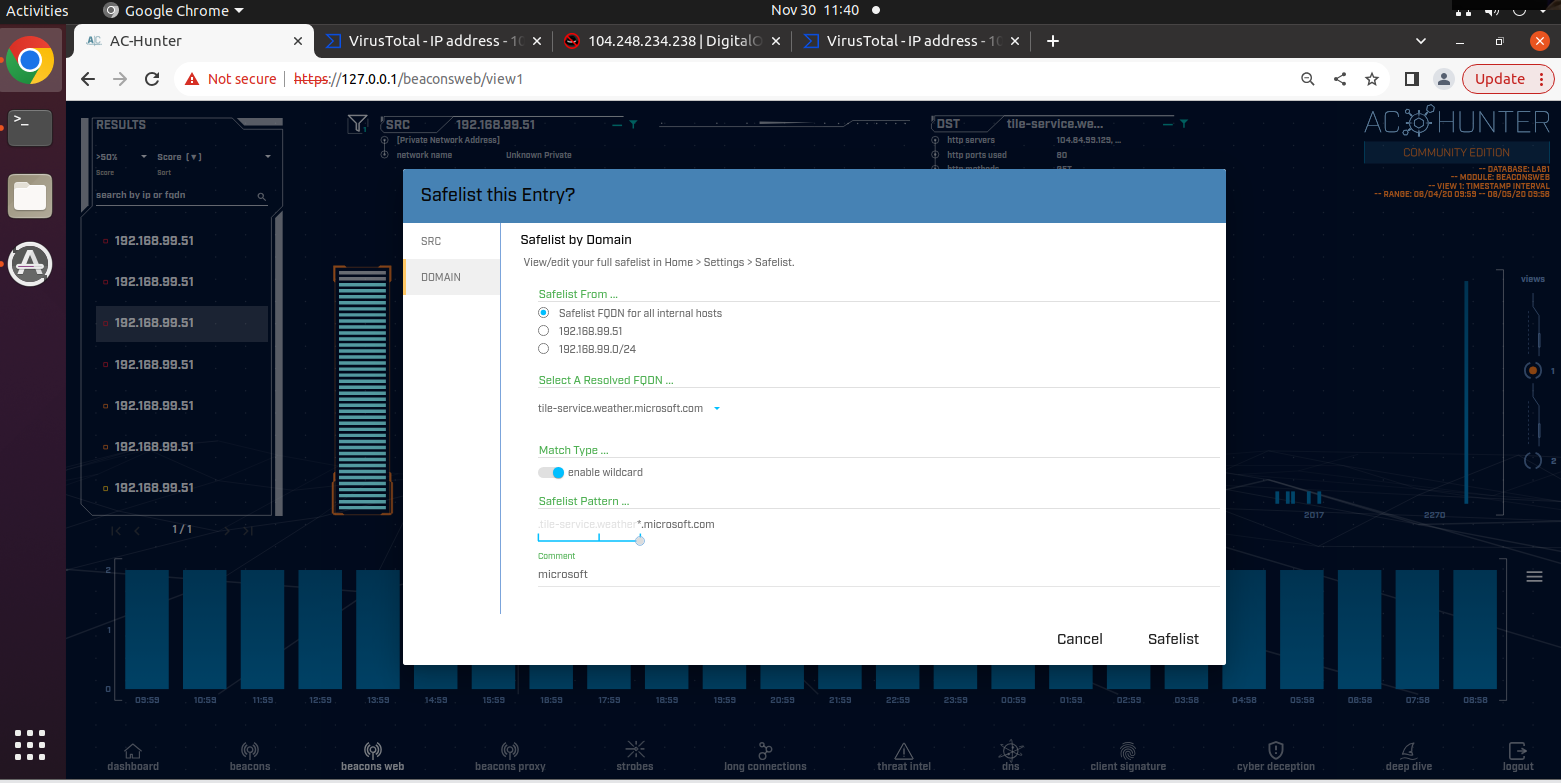
Большое количество подключений за последние 24 часа (3 011).

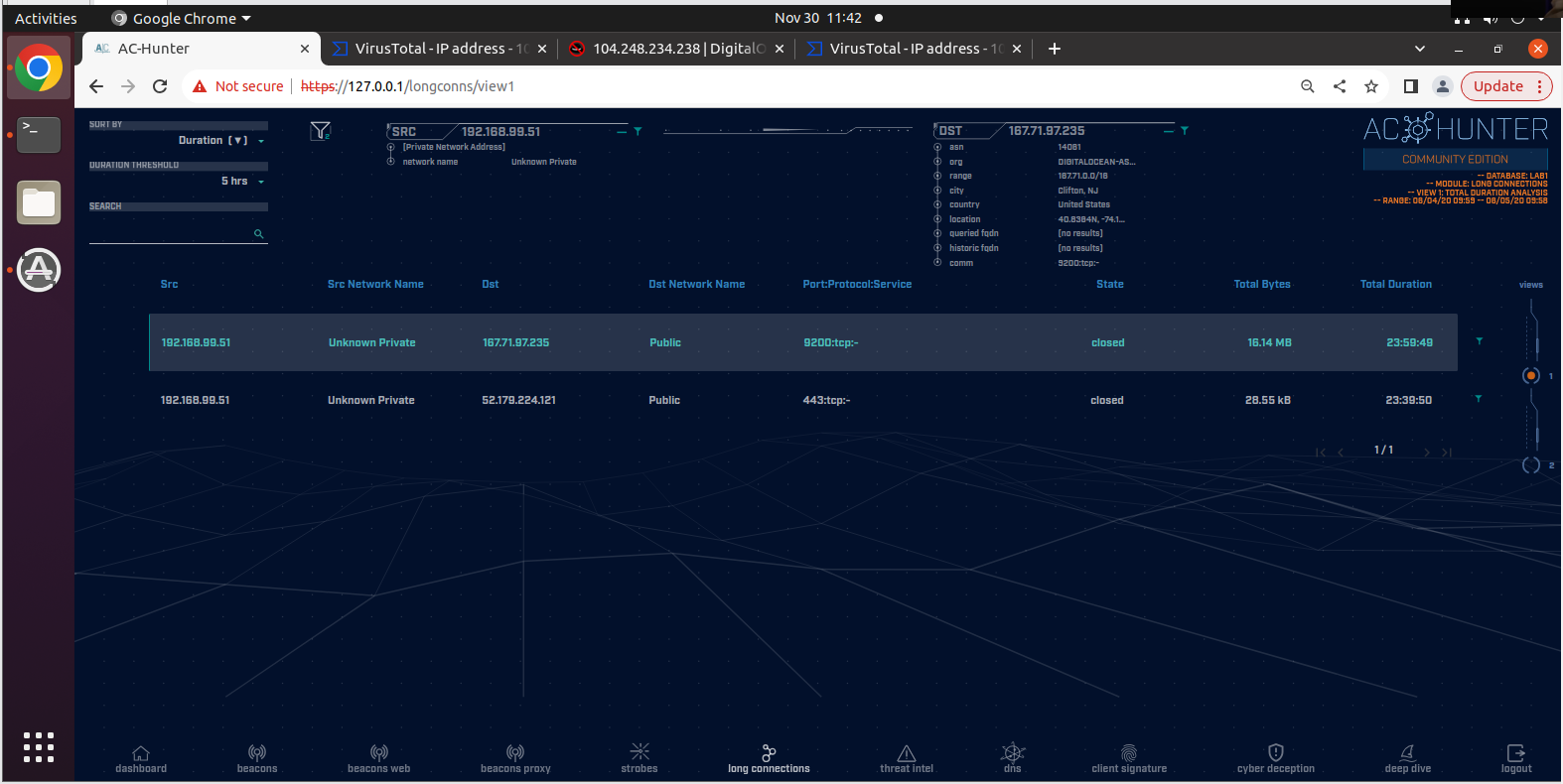
Гистограмма ровная.

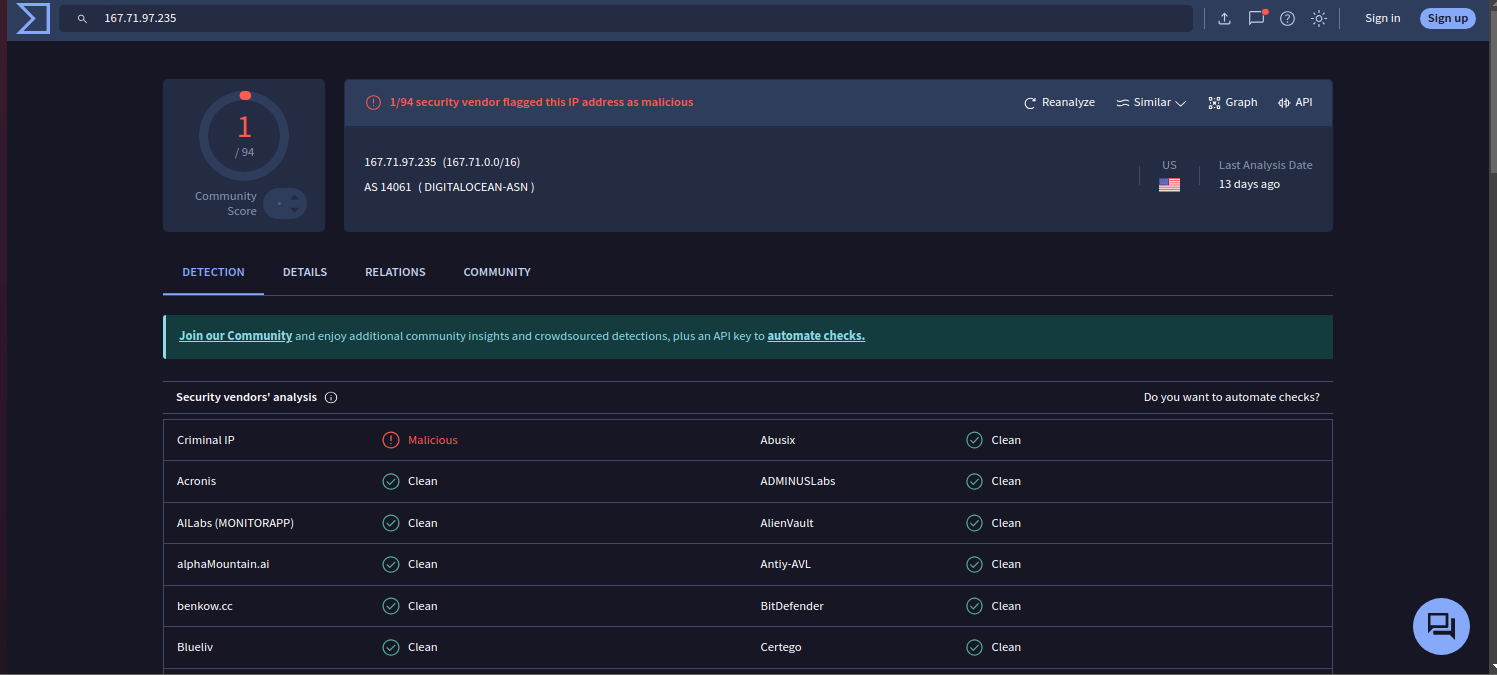
Отсутствует строка хостинга. полное доменное имя веб-сервера?

Проверим каждое соединение  


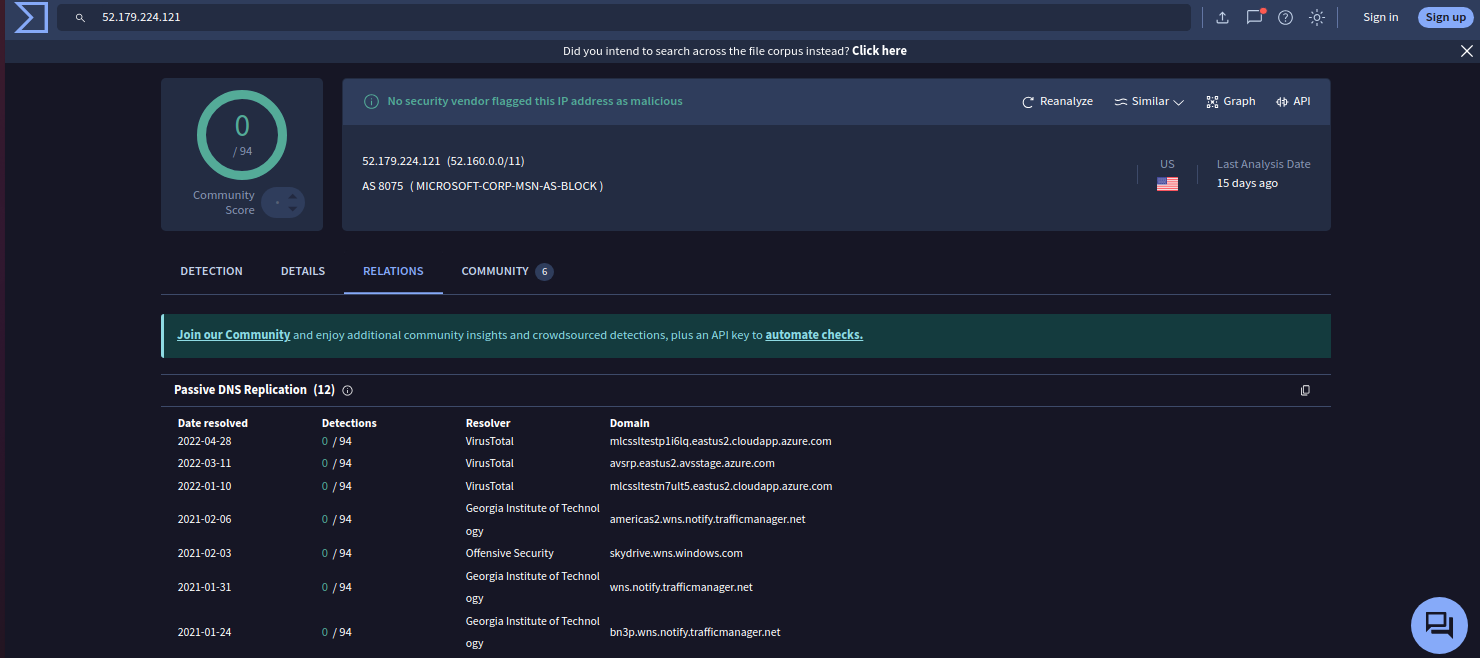
Убрал несколько адресов в safelist дабы убрать false positive срабатывания.

Проверяем обращения   


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

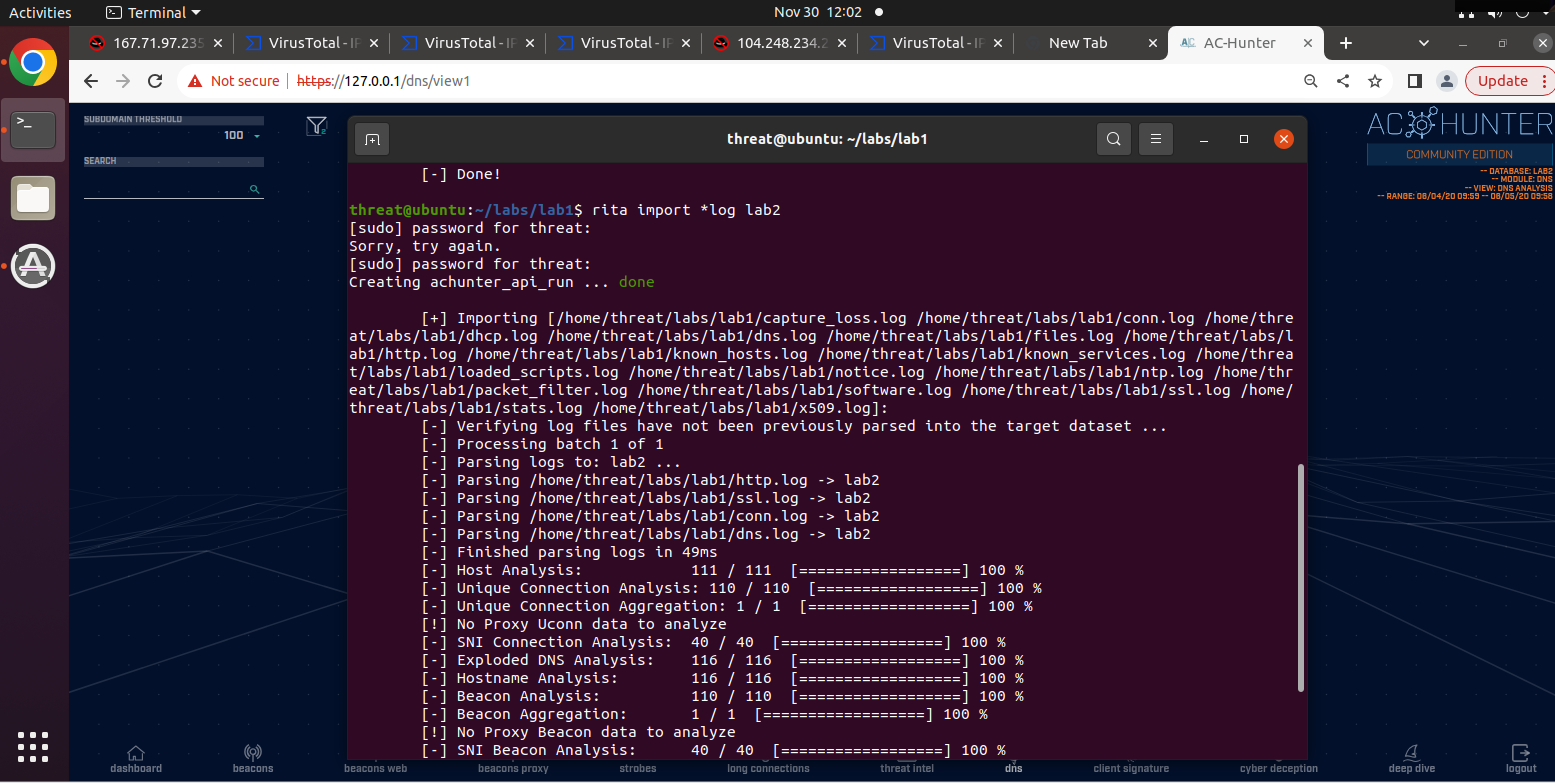
Второй адрес

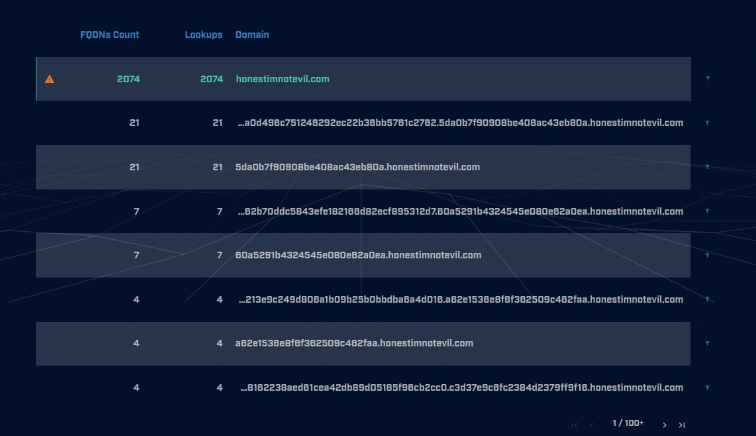


Как итог,мне не нарвистя как я и указал ранее про 3000 соединений с высоким beacon score,много строк пропущено,мне не нравится FQDN,хоста в зaголовке HTTP



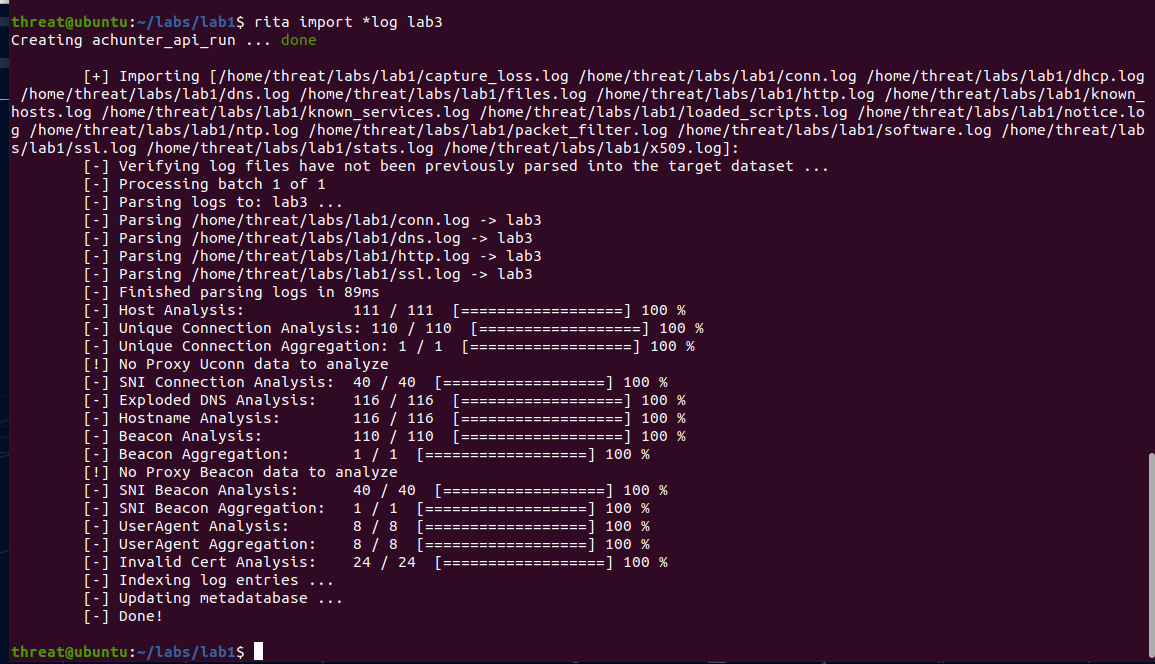
Перехожу к lab2





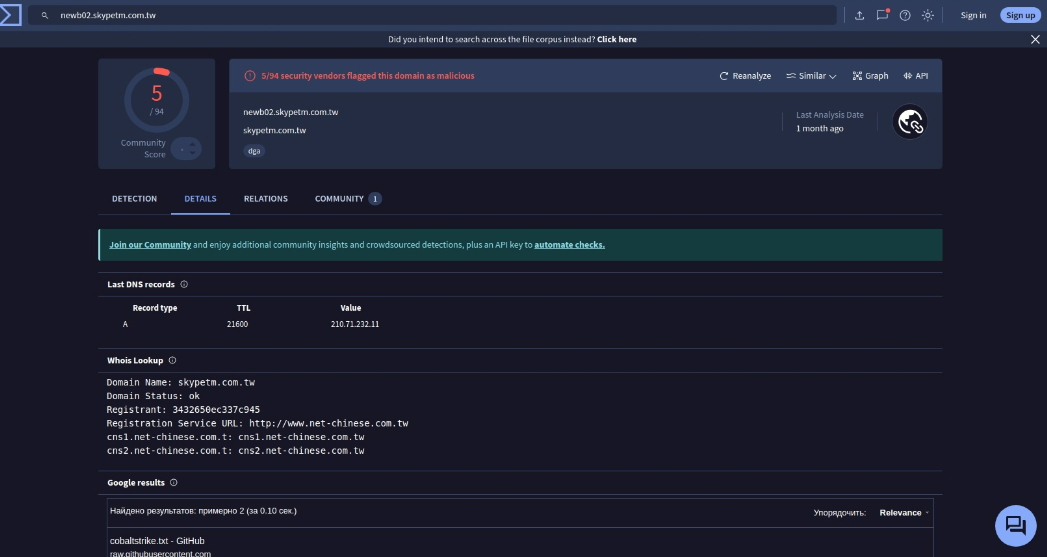
Тут всё очень быстро, огромное обращение к днс

Переходим к lab3





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