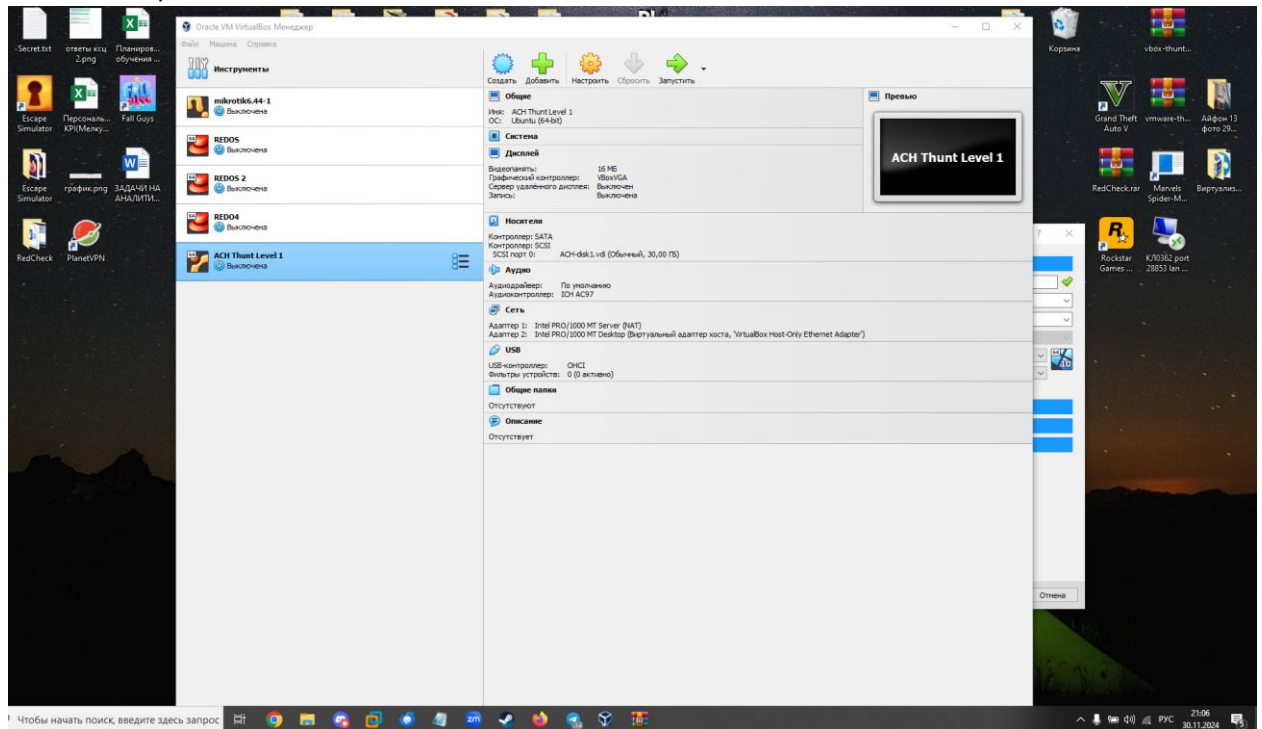
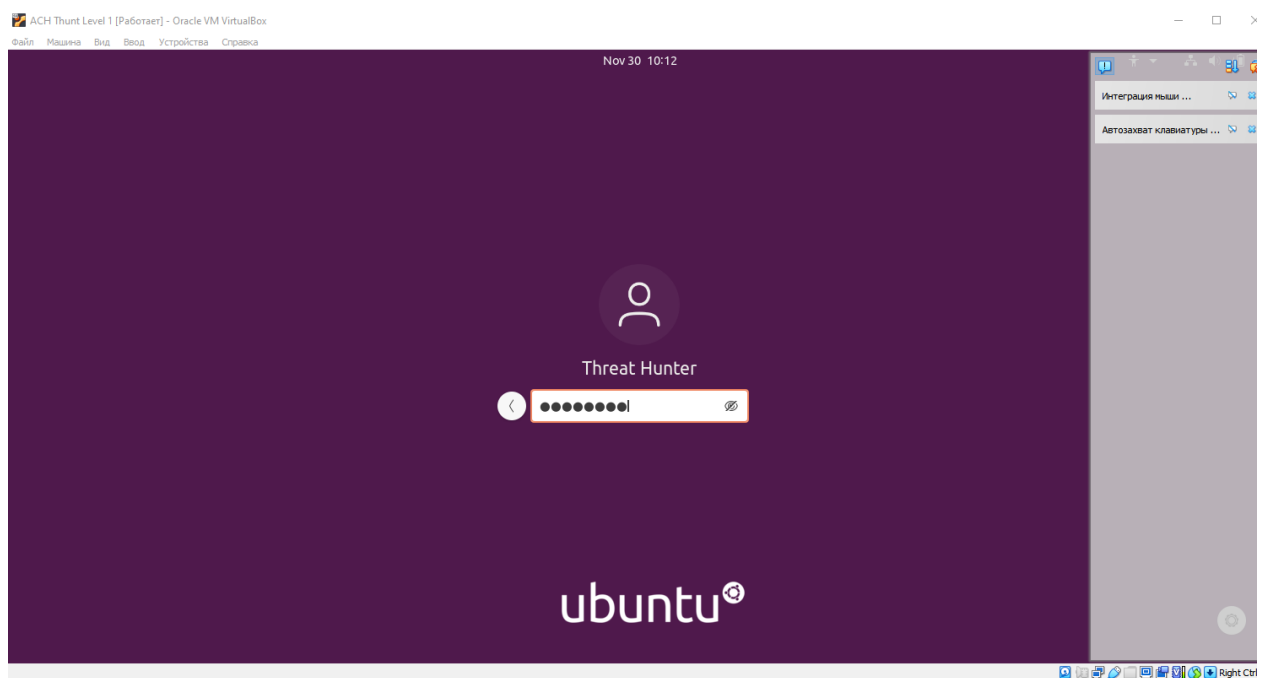
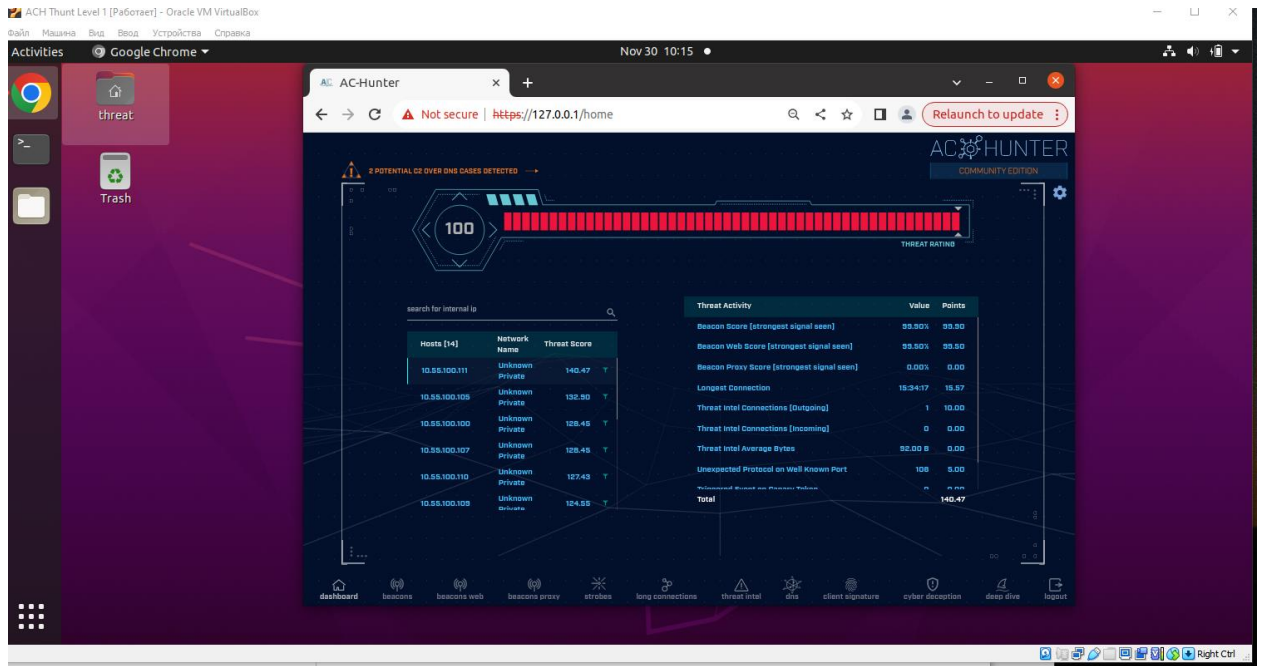


Скачиваем файл

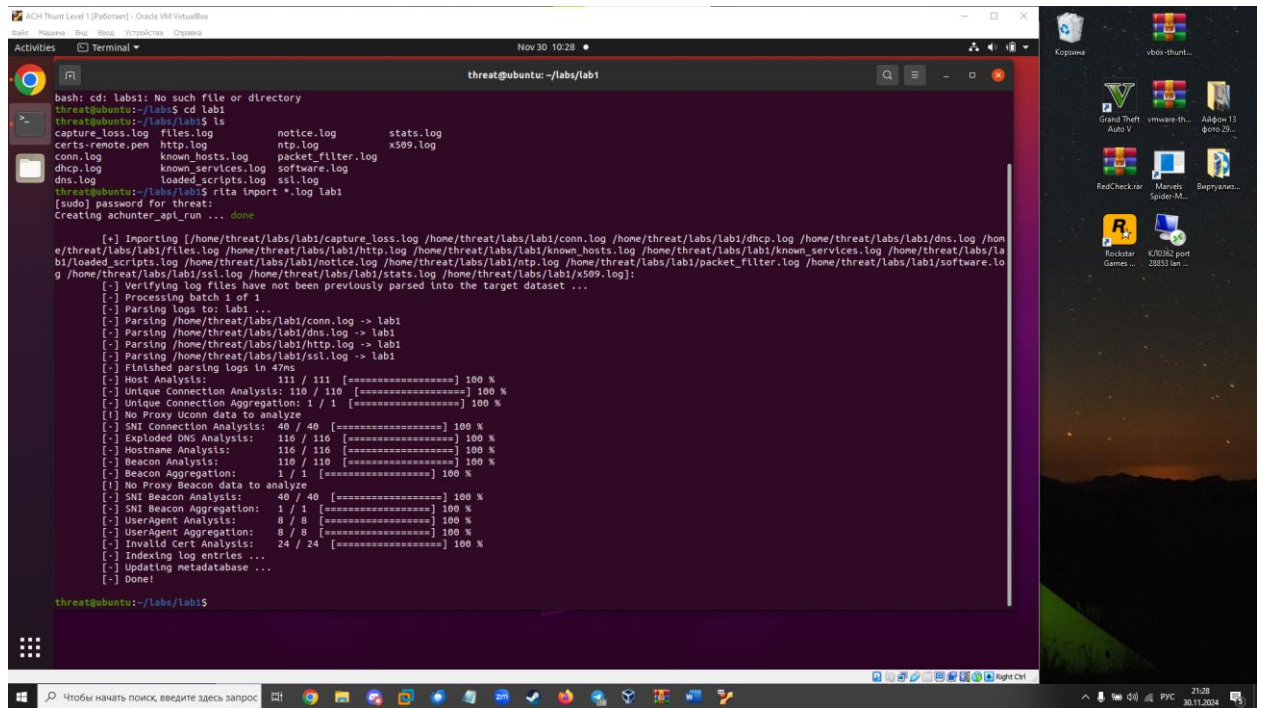


Открываем его

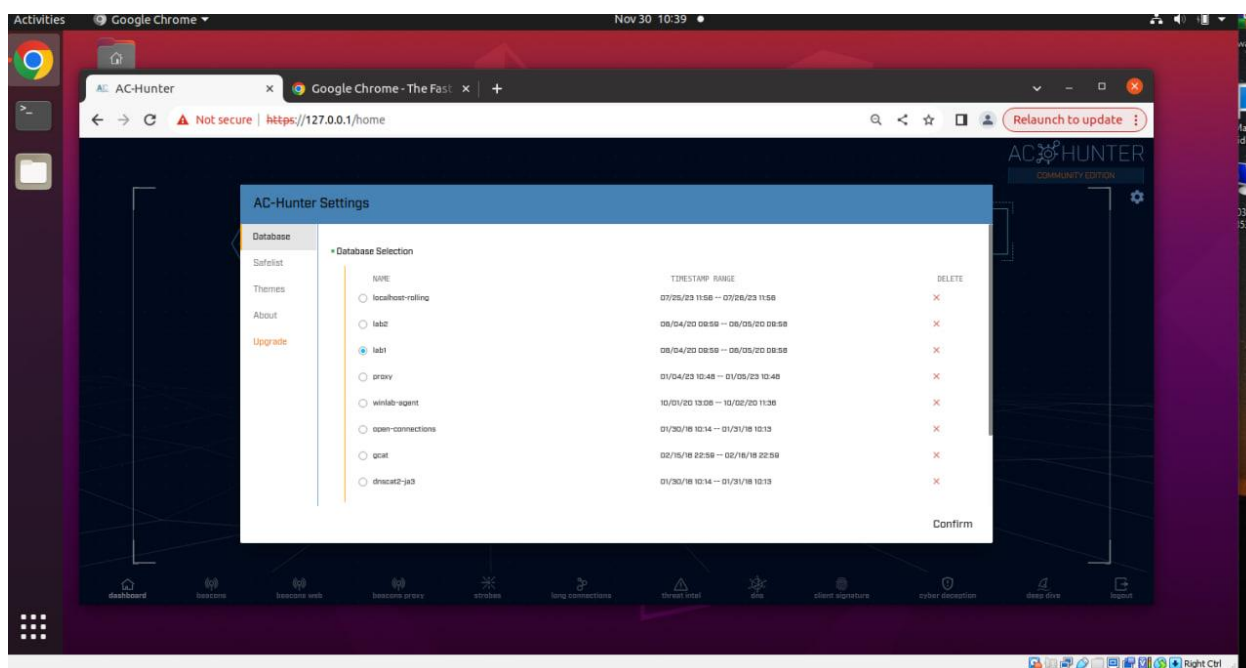




Произвожу импорт логов



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



Home ACH

Activities Google Chrome Nov 30 10:52

AC-Hunter x +

Not secure | https://127.0.0.1/home

Update

AC-HUNTER

COMMUNITY EDITION

AC-Hunter Settings

Database

Safelist

Themes

About

Upgrade

Database Selection

NAME	TIMESTAMP RANGE	DELETE
<input type="radio"/> localhost-rolling	07/25/23 11:58 -- 07/26/23 11:58	X
<input checked="" type="radio"/> lab1	08/04/20 08:58 -- 08/05/20 08:58	X
<input type="radio"/> proxy	01/04/23 10:48 -- 01/05/23 10:48	X
<input type="radio"/> winlab-agent	10/01/20 13:08 -- 10/02/20 11:38	X
<input type="radio"/> open-connections	01/30/18 10:14 -- 01/31/18 10:13	X
<input type="radio"/> gcac	02/15/18 22:58 -- 02/16/18 22:58	X
<input type="radio"/> dnscat2-jas	01/30/18 10:14 -- 01/31/18 10:13	X

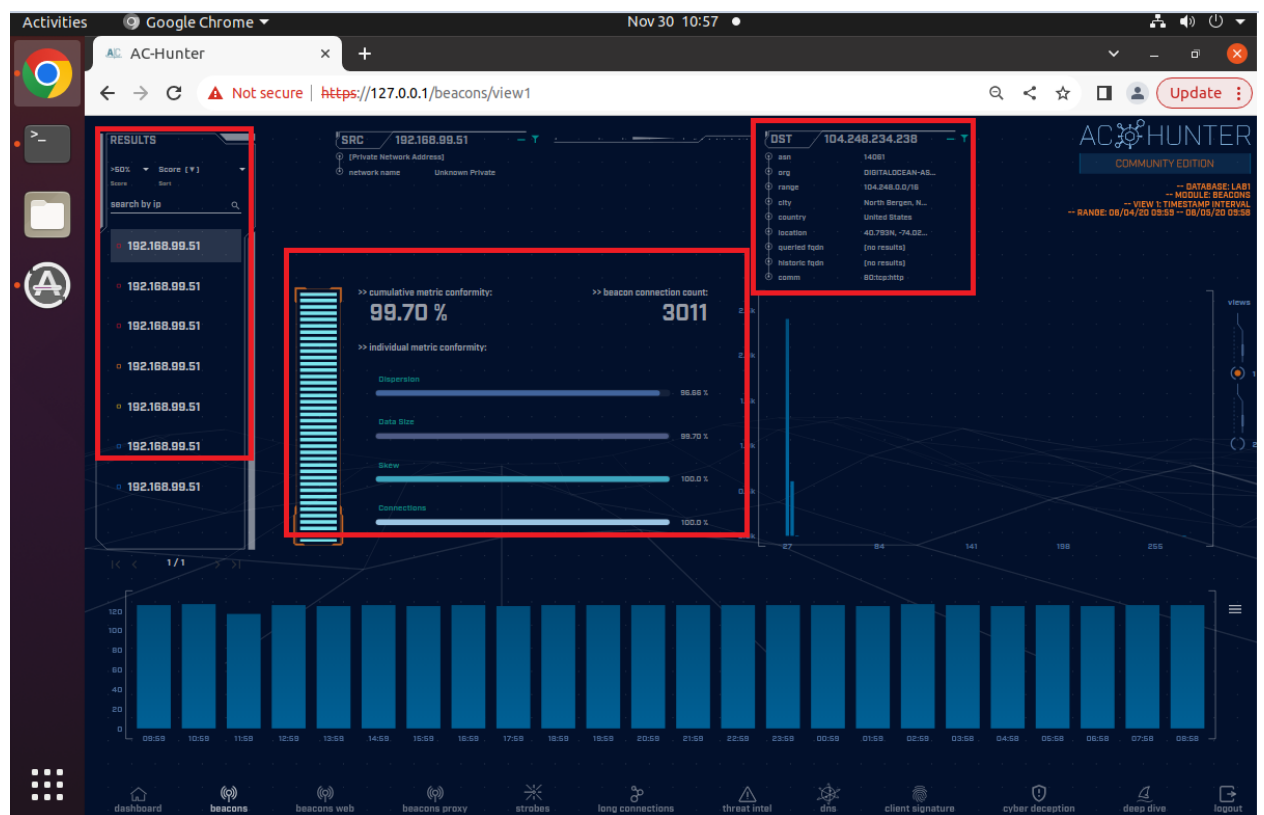
Database Removal

Delete All By Age

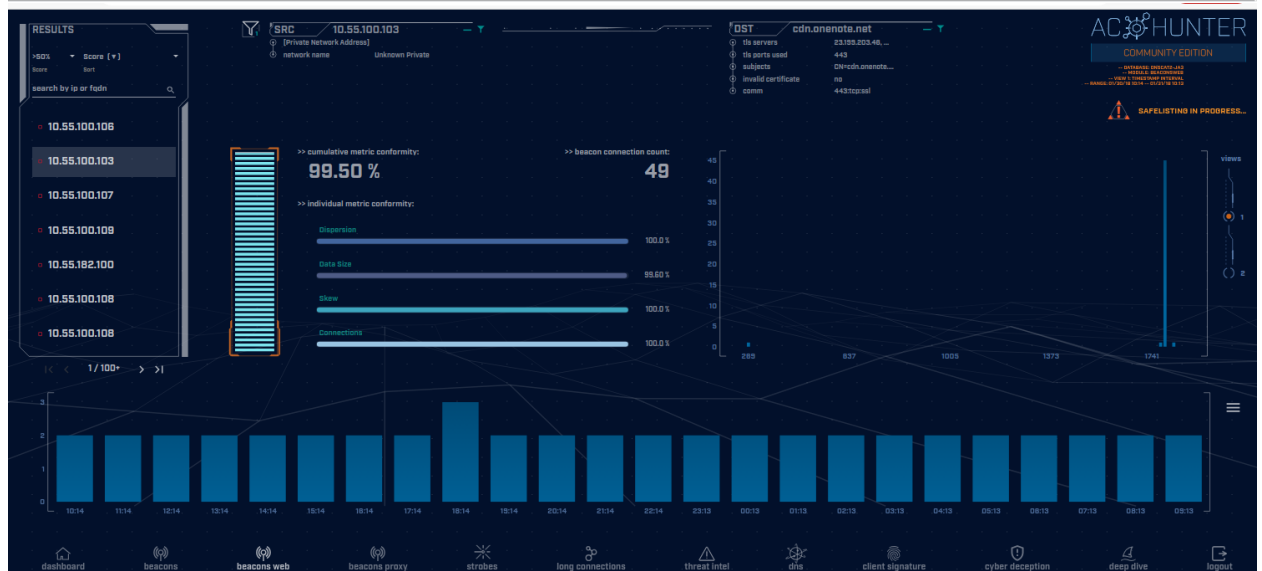
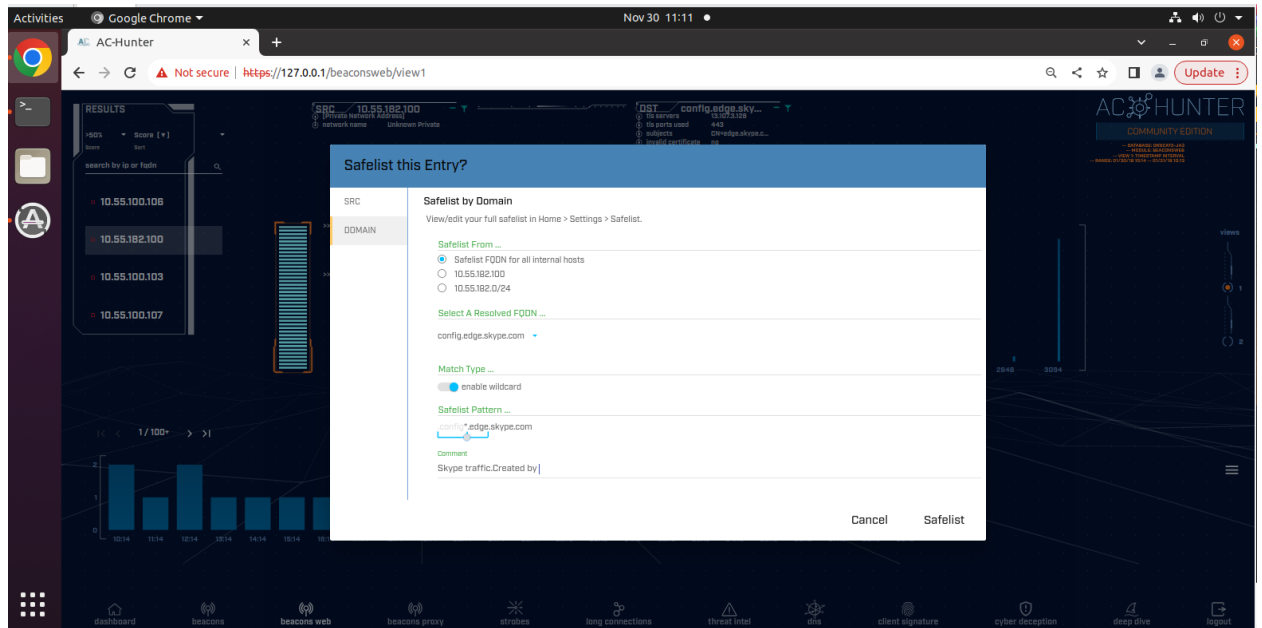
Confirm

dashboard beacons beacons web beacons proxy stratos long connections threat intel dns client signature cyber deception deep dive layout

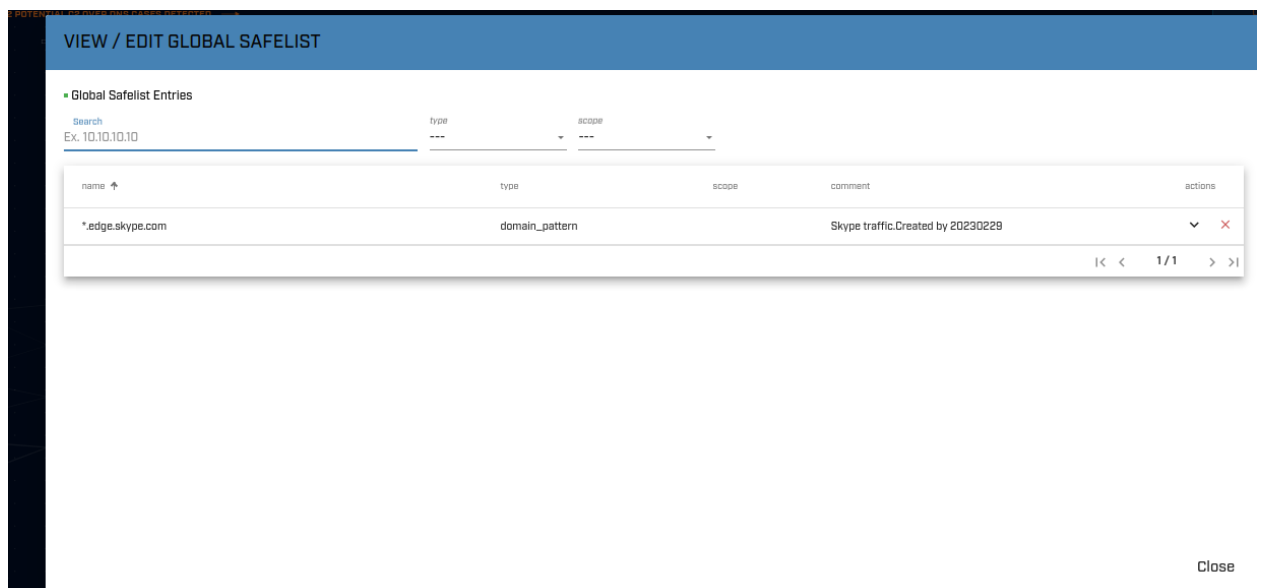
mouse pointer inside or press Ctrl+G.



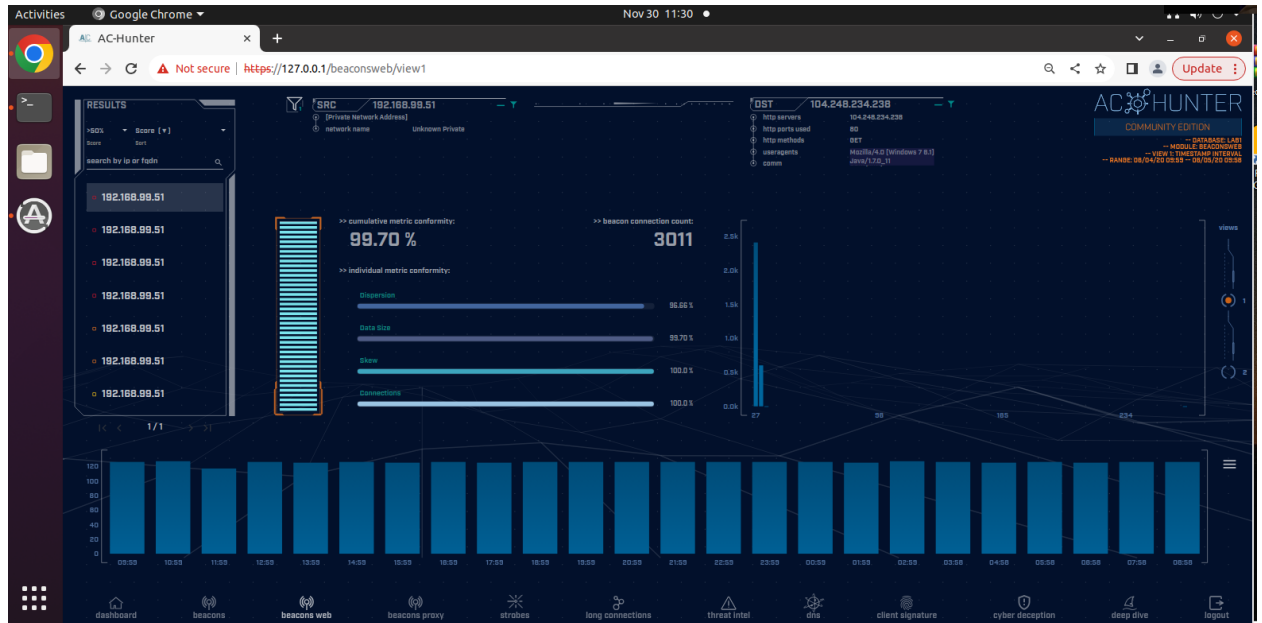
В руководстве сказано добавить скайп в сэйфлист



Проверяем появился ли сэйфлист



Начинается анализ событий из lab1

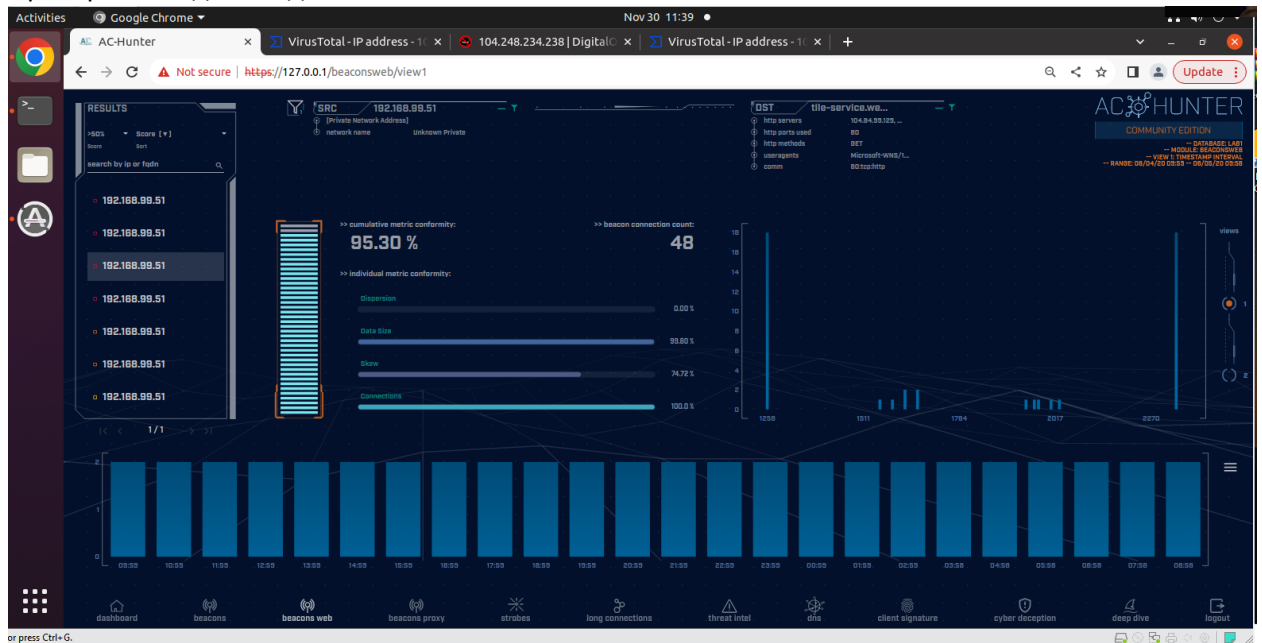


Большое количество подключений за последние 24 часа (3 011).

Гистограмма ровная.

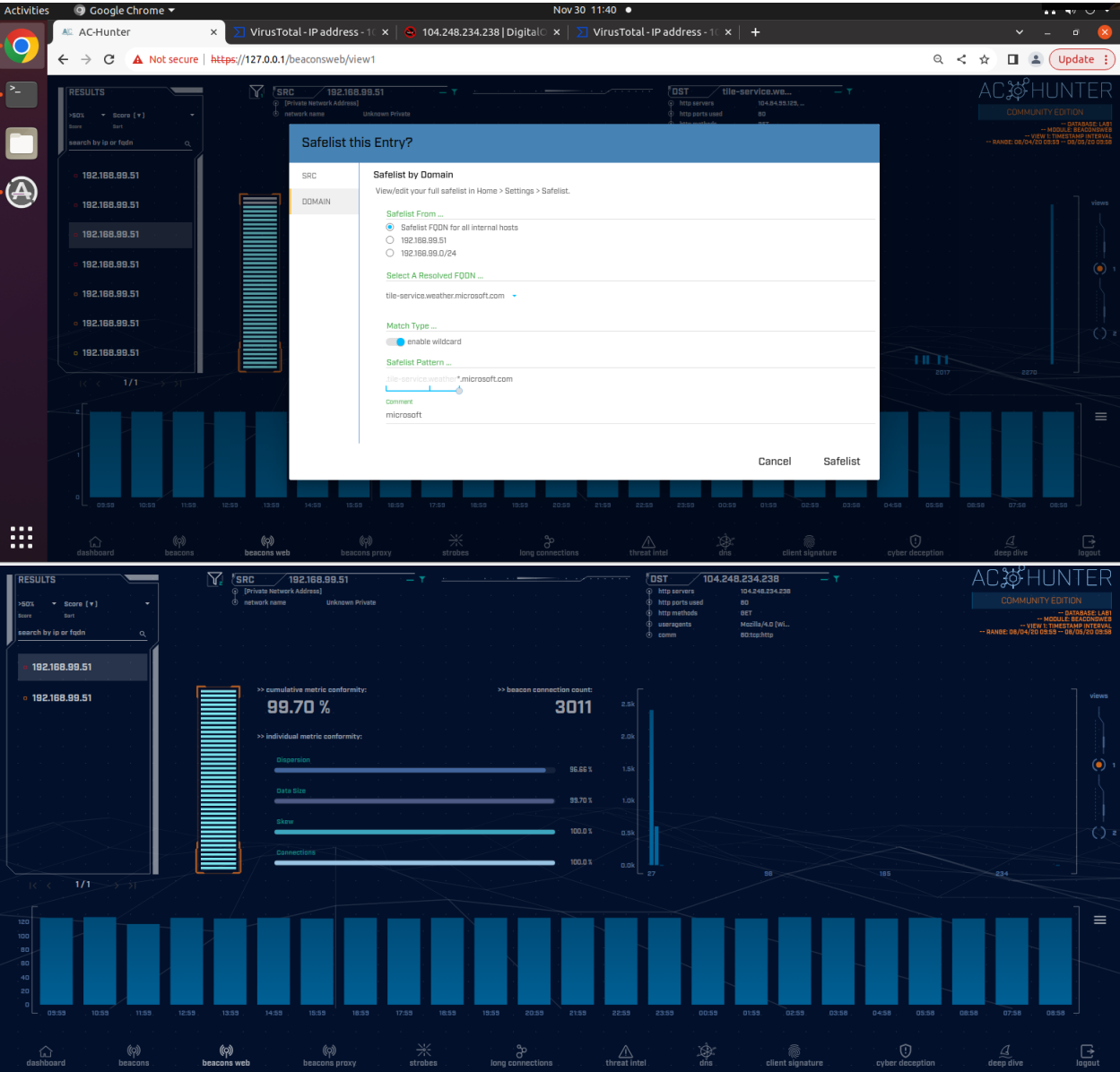
Отсутствует строка хостинга. полное доменное имя веб-сервера?

Проверим каждое соединение

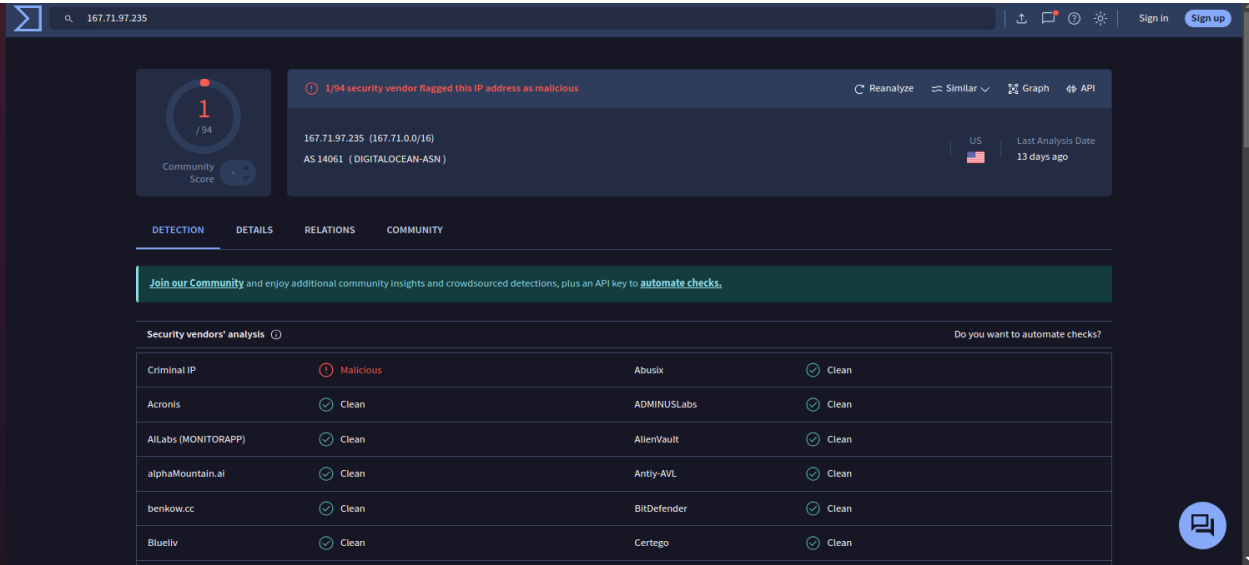
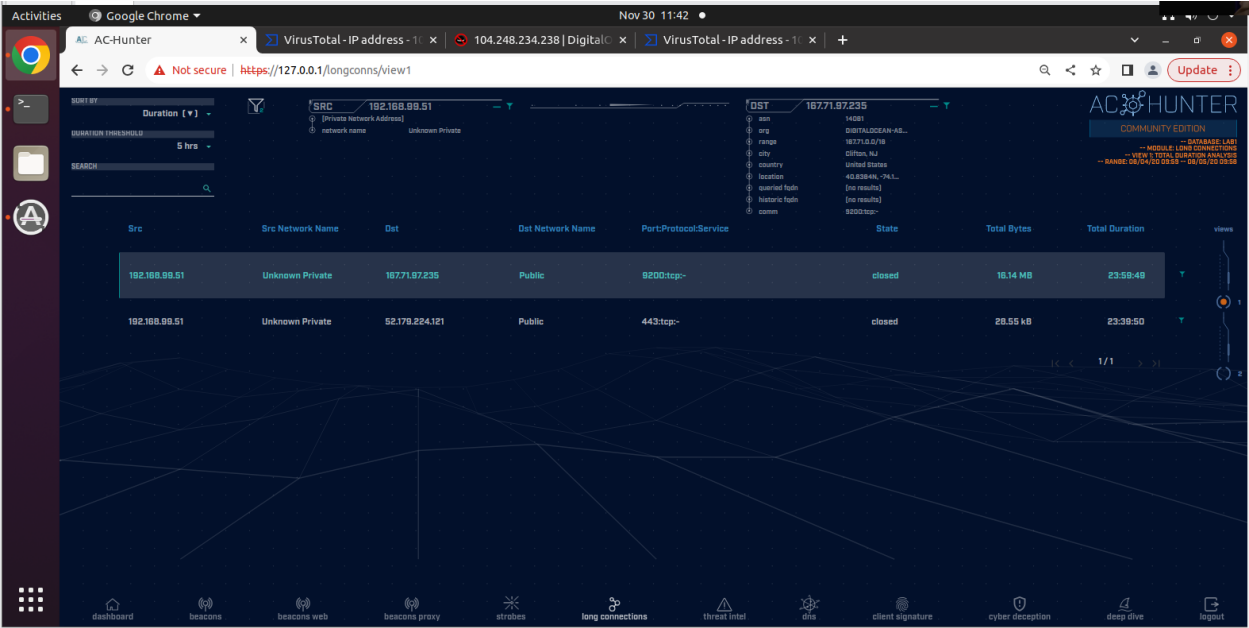


or press Ctrl+G.

Убрал несколько адресов в safelist дабы убрать false positive срабатывания.

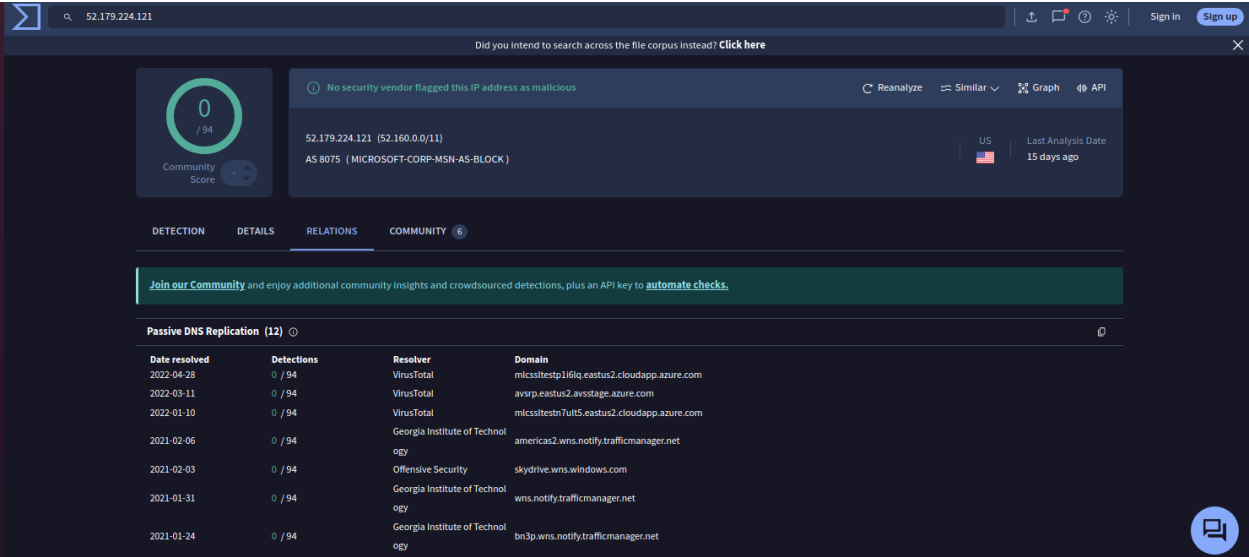


Проверяем обращения



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

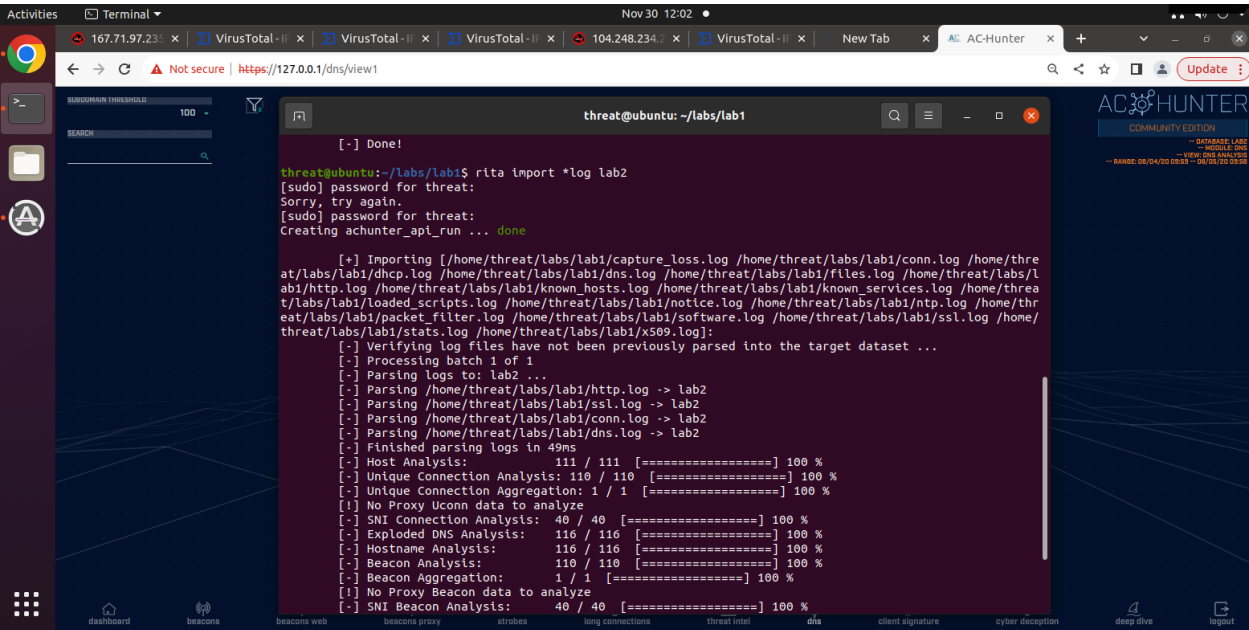
Второй адрес



Как итог,мне не нравистя 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



FQDNs Count	Lookups	Domain
2074	2074	honestimnotevil.com
21	21	...a0d498c751248292ec22b38bb5781c2782.5da0b7f90908be408ac43eb80a.honestimnotevil.com
21	21	5da0b7f90908be408ac43eb80a.honestimnotevil.com
7	7	...82b70ddc5843efe182188d82ecf895312d7.80a5291b4324545e080e02a0ea.honestimnotevil.com
7	7	80a5291b4324545e080e02a0ea.honestimnotevil.com
4	4	...213e9c249d808a1b09b25b0bbdba8a4d018.a82e1538e8f8f362509c482faa.honestimnotevil.com
4	4	a82e1538e8f8f362509c482faa.honestimnotevil.com
4	4	...8182238aed81cea42db89d05185f96cb2cc0.c3d37e9c8fc2384d2379ff9f10.honestimnotevil.com

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)

newb02.skypetm.com.tw

Did you intend to search across the file corpus instead? [Click here](#)

5 / 94
Community Score

5/94 security vendors flagged this domain as malicious

newb02.skypetm.com.tw
skypetm.com.tw
dga

Last Analysis Date
1 month ago

Reanalyze Similar Graph API

DETECTION DETAILS RELATIONS COMMUNITY 1

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Last DNS records

Record type	TTL	Value
A	21600	210.71.232.11

Whois Lookup

Domain Name: skypetm.com.tw
Domain Status: ok
Registrant: 3432650ec337c945
Registration Service URL: <http://www.net-chinese.com.tw>
cns1.net-chinese.com.tw: cns1.net-chinese.com.tw
cns2.net-chinese.com.tw: cns2.net-chinese.com.tw

Google results

Найдено результатов: примерно 2 (за 0.10 сек.)

Упорядочить: Relevance

cobaltstrike.txt - GitHub
raw.githubusercontent.com

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