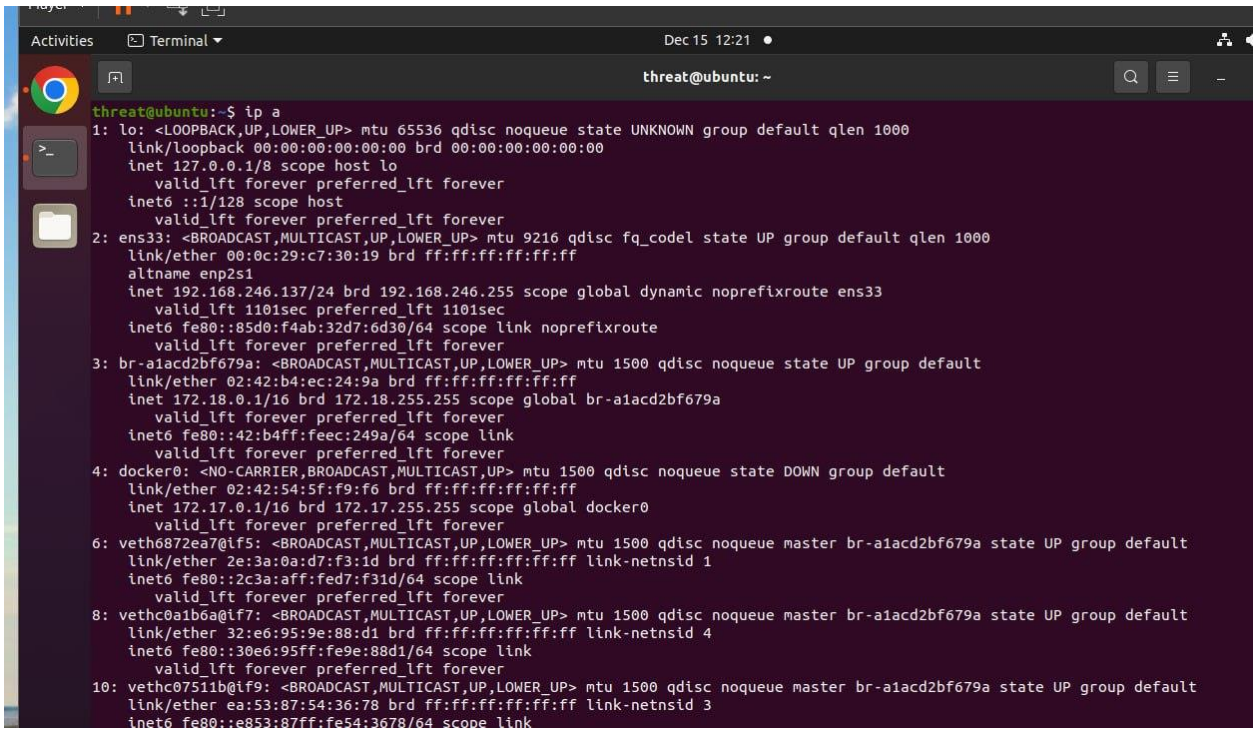


Рисунок 1 – демонстрация ip-адреса хоста

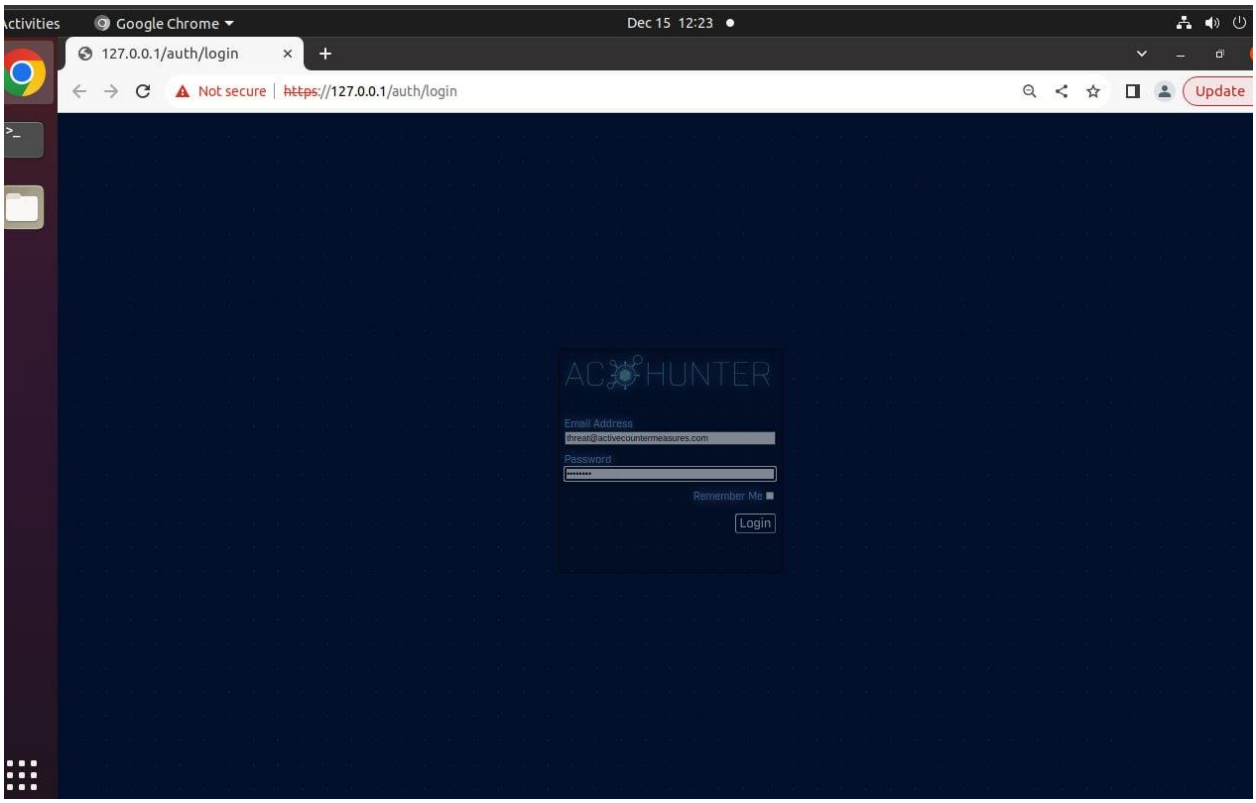


Рисунок 2 – вход в прикладное ПО

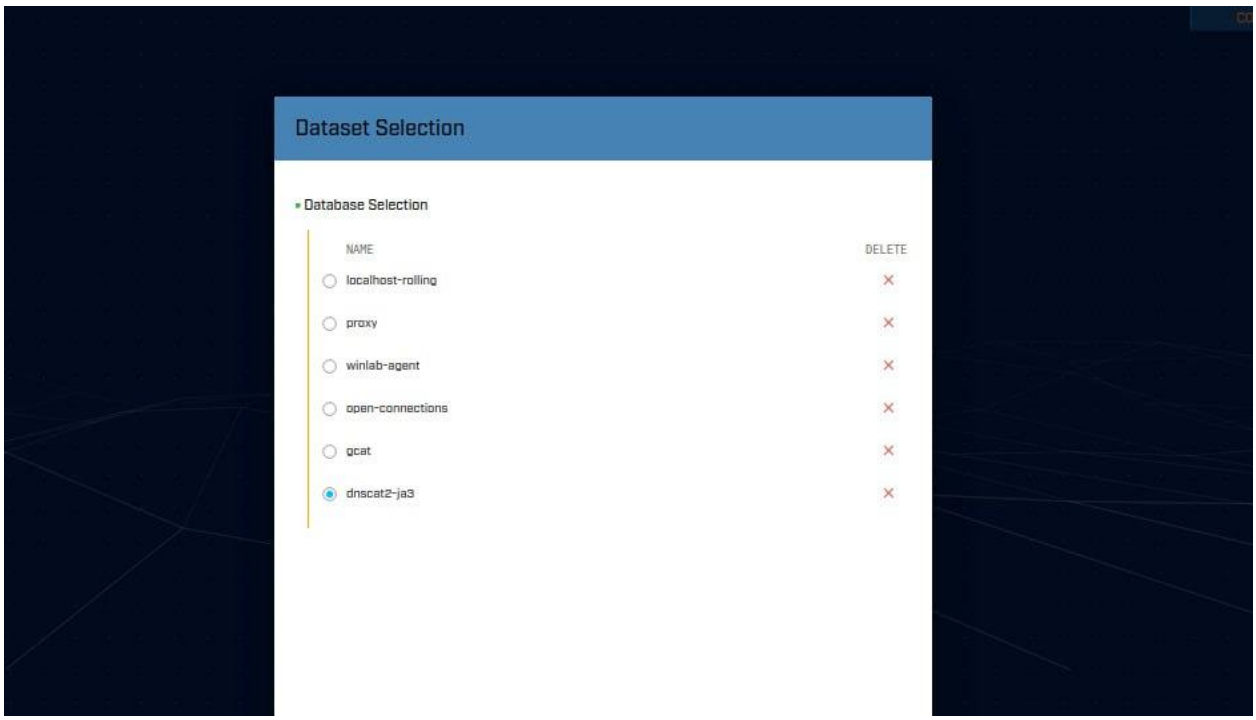


Рисунок 3 – выбор датасета dnscat2-ja3 для дальнейшей работы

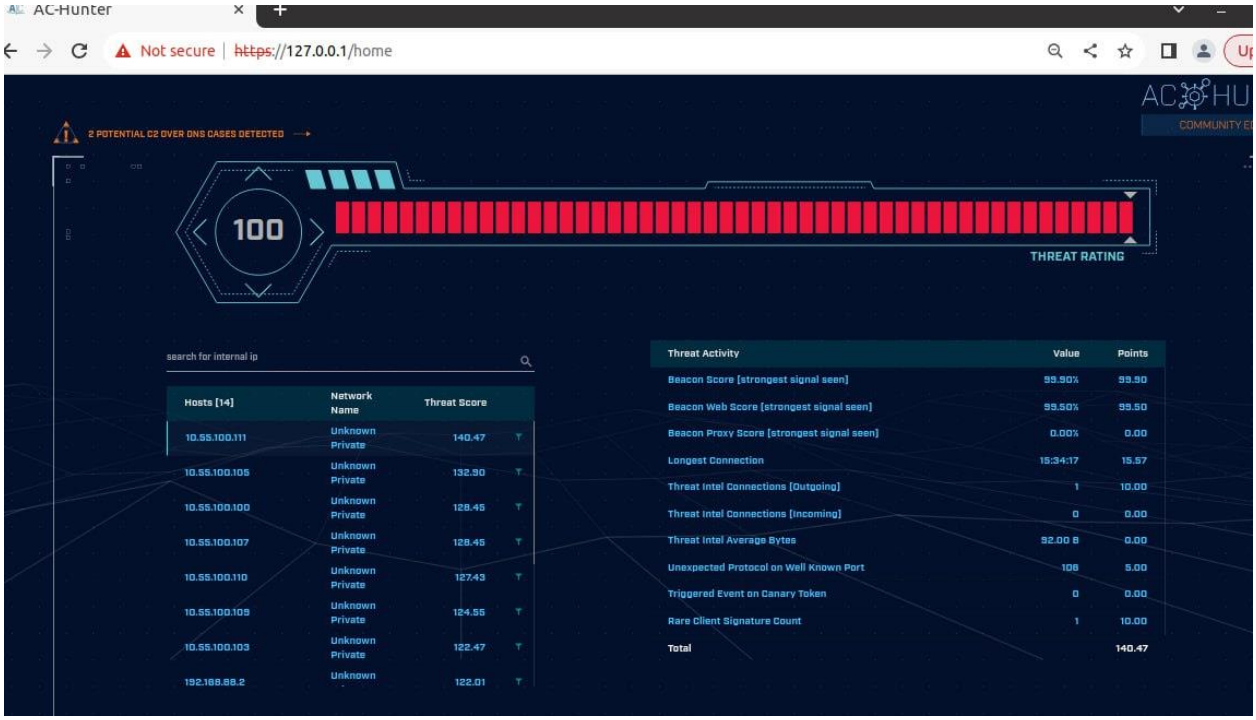


Рисунок 4 – интерфейс AC-Hunter

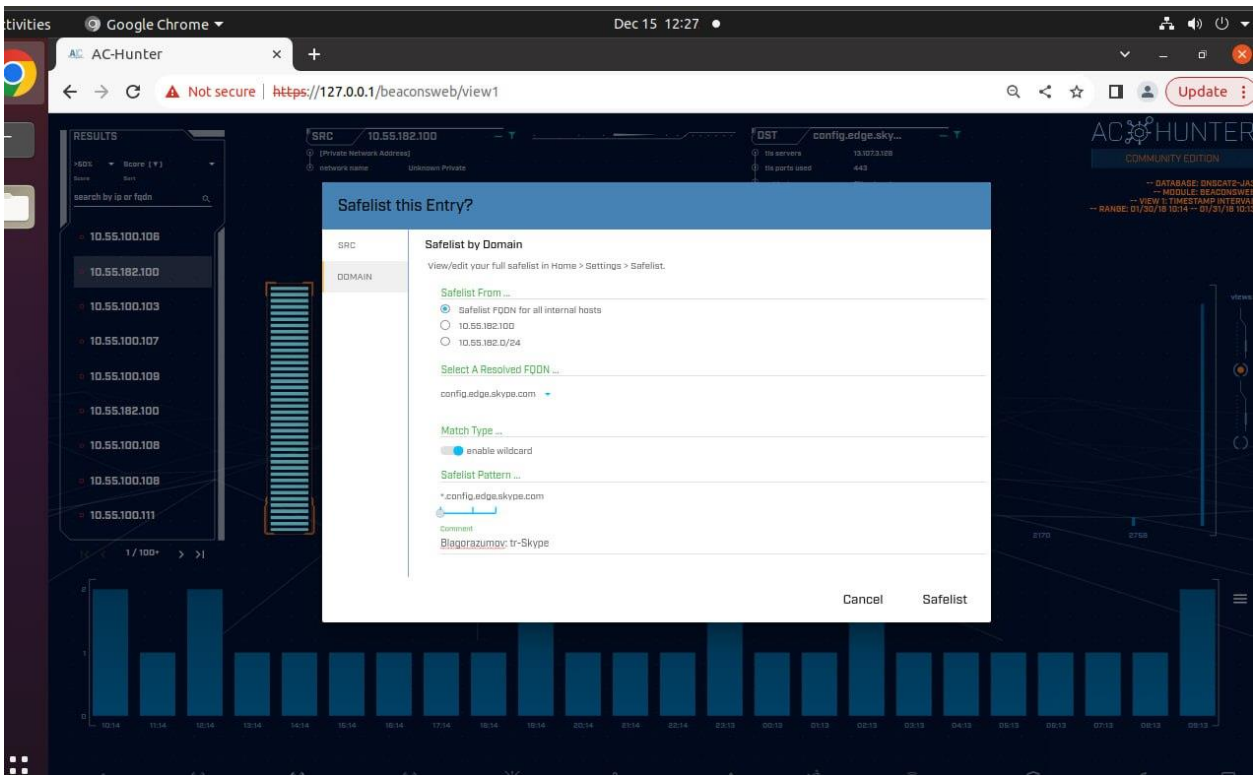


Рисунок 5 – добавляем в safelist легитимное подключение к Skype

```
threat@ubuntu:~/labs/lab1$ rita import *.log blago_lab1
Creating achunter_api_run ... done



        [+] Importing [/home/threat/labs/lab1/capture_loss.log /home/threat/labs/lab1/conn.log /home/threat/labs/lab1/dhcp.lo
reat/labs/lab1/dns.log /home/threat/labs/lab1/files.log /home/threat/labs/lab1/http.log /home/threat/labs/lab1/known_hosts.lo
reat/labs/lab1/known_services.log /home/threat/labs/lab1/loaded_scripts.log /home/threat/labs/lab1/notice.log /home/threat/la
p.log /home/threat/labs/lab1/packet_filter.log /home/threat/labs/lab1/software.log /home/threat/labs/lab1/ssl.log /home/threa
1/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: blago_lab1 ...
        [-] Parsing /home/threat/labs/lab1/ssl.log -> blago_lab1
        [-] Parsing /home/threat/labs/lab1/conn.log -> blago_lab1
        [-] Parsing /home/threat/labs/lab1/dns.log -> blago_lab1
        [-] Parsing /home/threat/labs/lab1/http.log -> blago_lab1
        [-] Finished parsing logs in 463ms
        [-] 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 %
```

Рисунок 6 – импорт логов для 1 части лабораторной работы

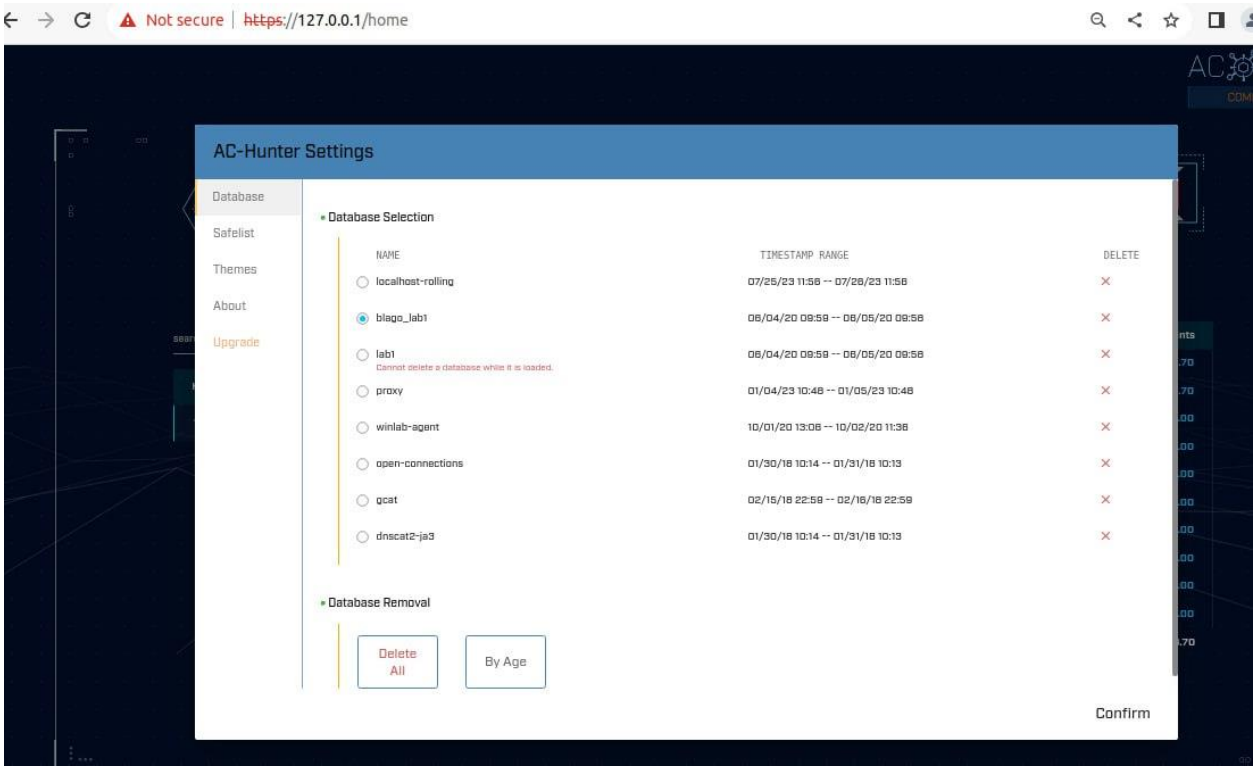


Рисунок 7 – выбор логов для считывания ПО

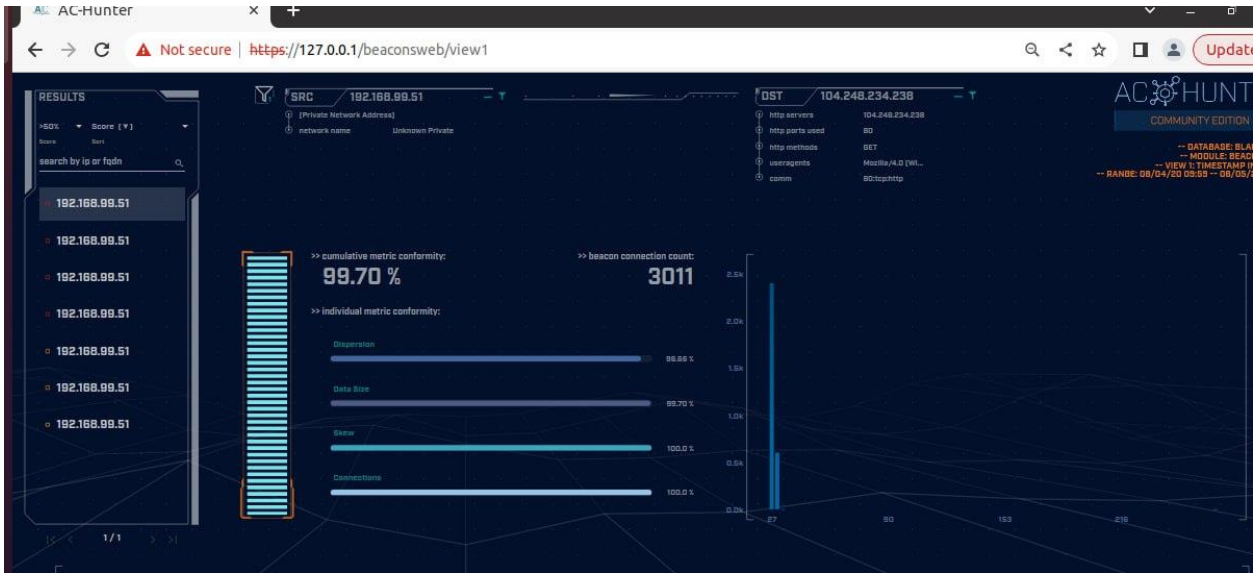
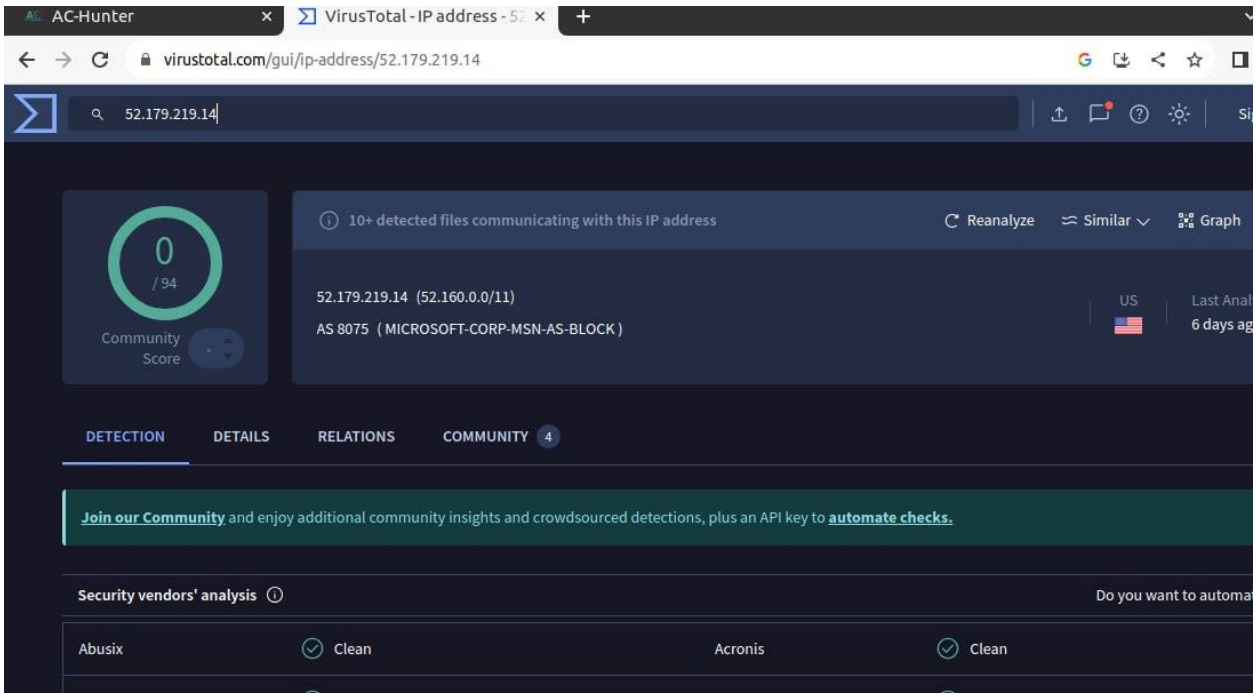


Рисунок 8 – первая запись – 104.248.234.238

Рисунок 9 – вторая запись, служба\сервис от Windows

```
threat@ubuntu:~/labs/lab1$ cat dns.log | zeek-cut query answers | grep 104.248.234.238
threat@ubuntu:~/labs/lab1$ cat http.log | zeek-cut id.orig_hid.resp_h host uri user_agent | sort | uniq -c | sort -rn | head -3
   3011        104.248.234.238 /rmvk30g/eghmbblnphlaefbmmnoenohhoncmcepapefjjekpleokhjfjmnmijghedkienplidbbcmgdjldbegpeemiboacnfcpnbnn
hlmjbpcejfpecdioiddklfegefcjbcnagjclnoijpajlpkkegakmpdddojnlphegeehaacmofggdfkagpbighfkndllaamndepdanhnogedkaodhgakiigoheminoolnaobdiio
kpebghapnghbebkepiffooljden;1;4;1       Mozilla/4.0 (Windows 7 6.1) Java/1.7.0_11
     48         tile-service.weather.microsoft.com      /en-US/livetile/preinstall?region=US&appid=C98EA5B0842DBB9405BBF071E1DA76512D21
FE36&FORM=Threshold     Microsoft-WNS/10.0
     26         3.tlu.dl.delivery.mp.microsoft.com      /filestreamingservice/files/62023f49-c795-4f2c-b1ad-691785434443?P1=1591295946&
P2=402&P3=2&P4=NT59YouPqG4KlXd/4KmhtlEQdz6EKxjsXlalRGmYkfJ/oAVAnmgIZx2TXpHocIv5Fj1Ghc2FXZZoPXeI8/8GXw== Microsoft-Delivery-Optimization
/10.0
threat@ubuntu:~/labs/lab1$
```

Рисунок 10 – анализ логов подозрительного подключения



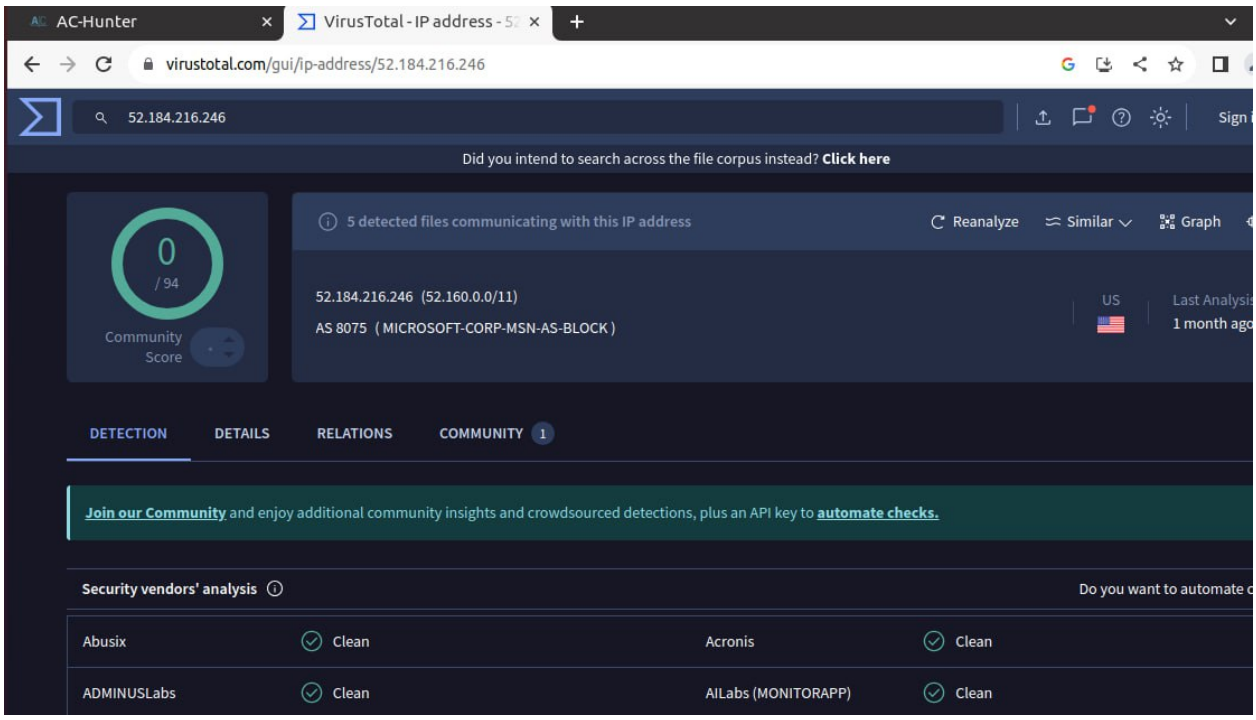


Рисунок 11-12 – проверка на VirusTotal ip-адресов остальных записей (чистых)

Выводы:

1) Была заменена строка агента пользователя
2) Отсутствует поле "host" в HTTP-заголовке
3) Большое количество соединений (3011) за короткий срок
4) Остальные подключения осуществляются к службам Microsoft, поэтому можем добавить в safelist

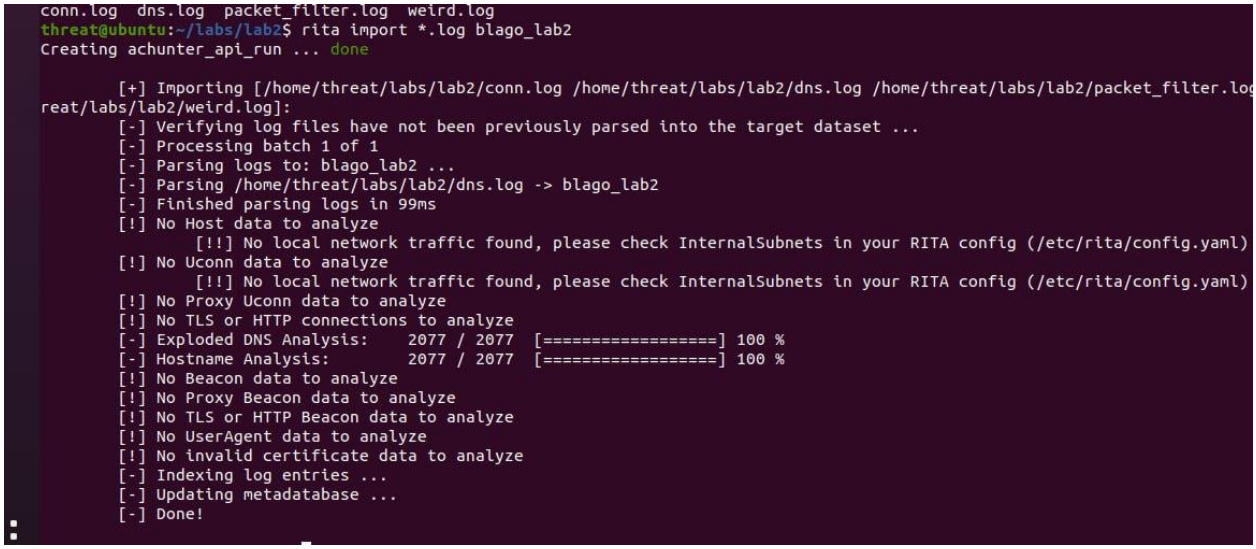


Рисунок 13 – загрузка логов для 2 части практической работы

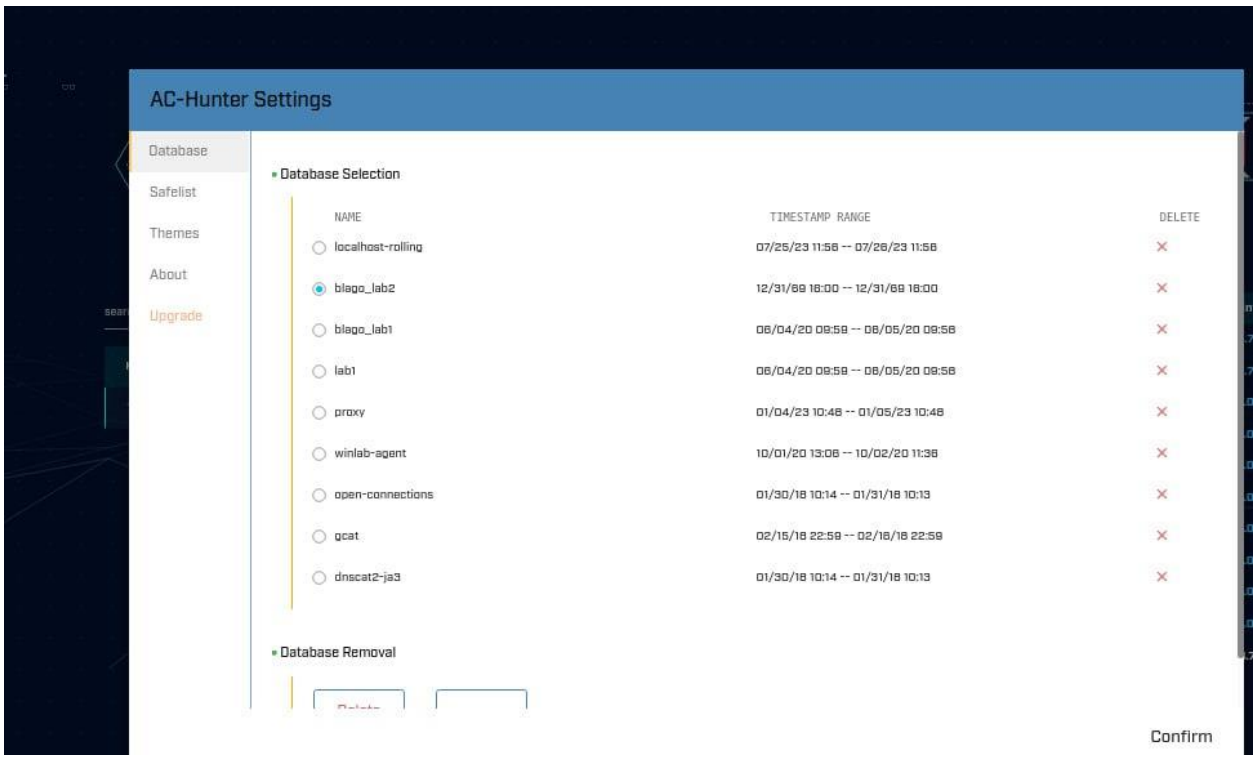
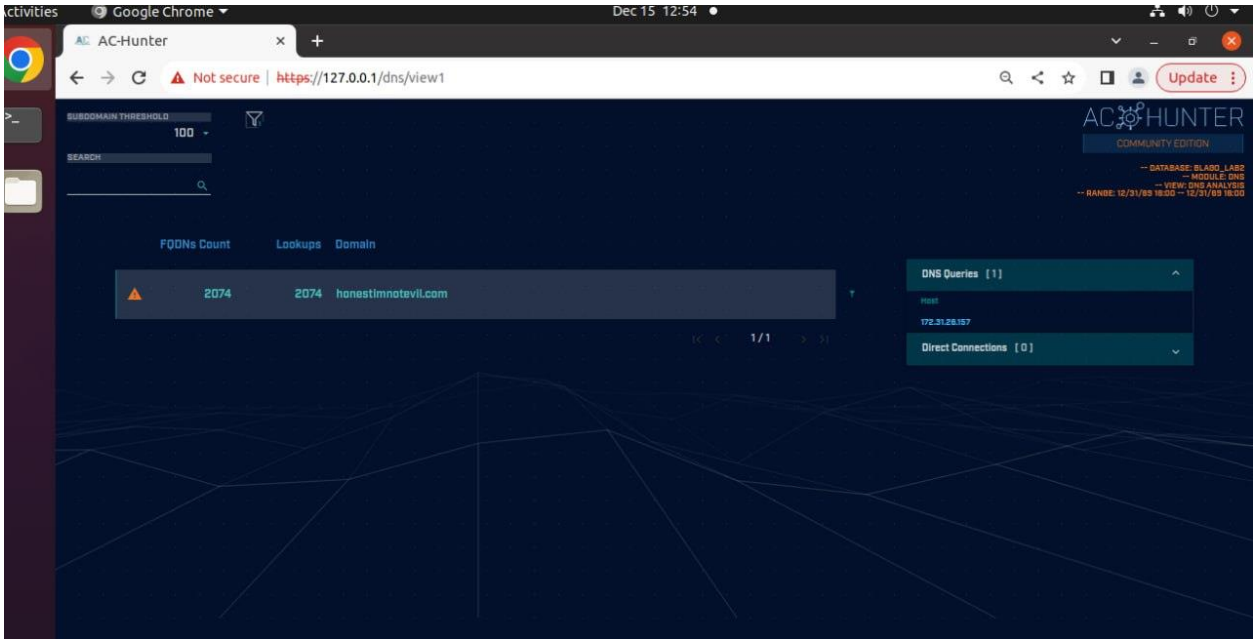


Рисунок 14 – загрузка логов для анализа в AC Hunter



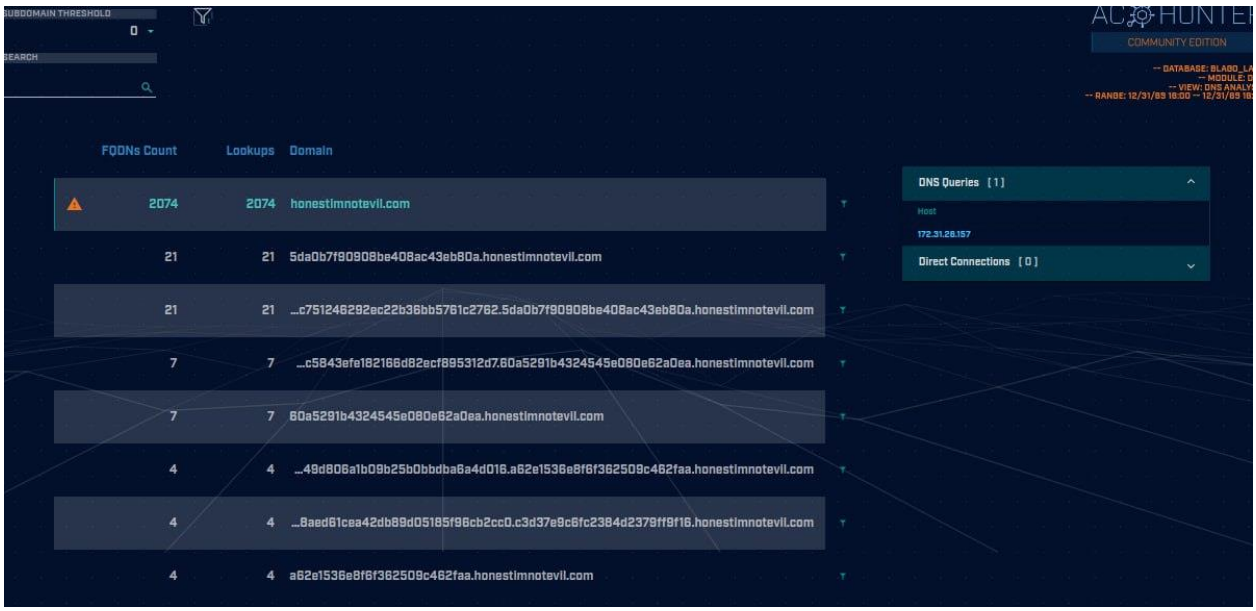


Рисунок 15-16 – большое количество DNS-запросов

Выводы: Большое количество DNS-запросов к различным поддоменам, очень похоже на осуществление атаки C2 через DNS

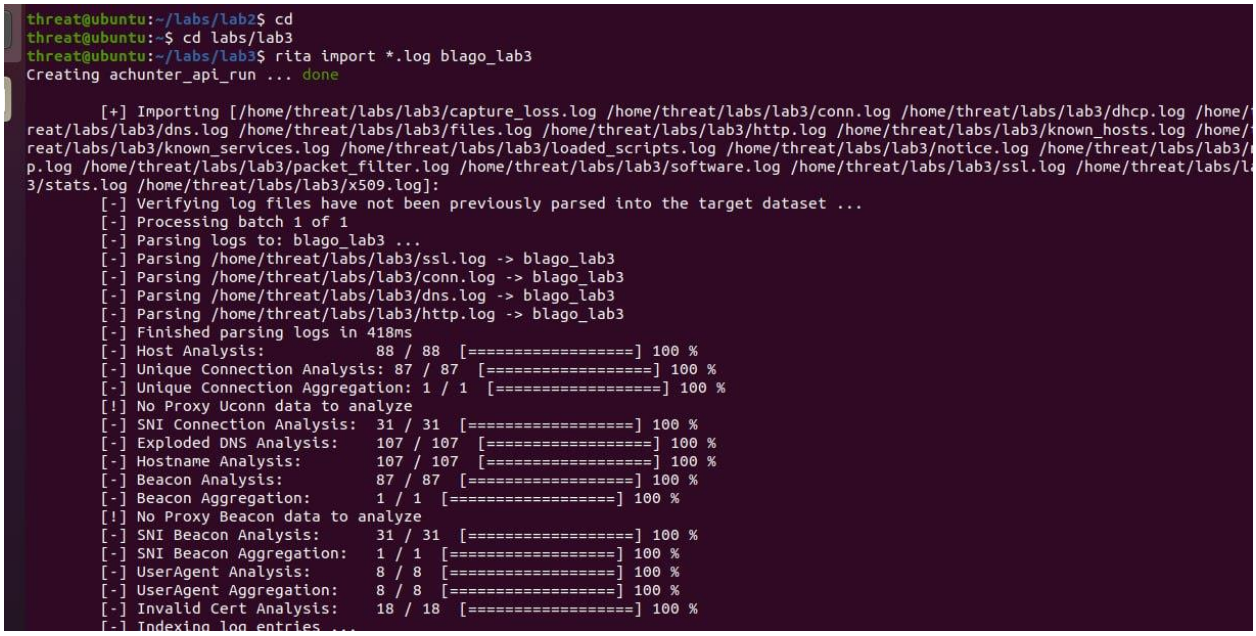


Рисунок 17 – загрузка логов для 3 части практической работы

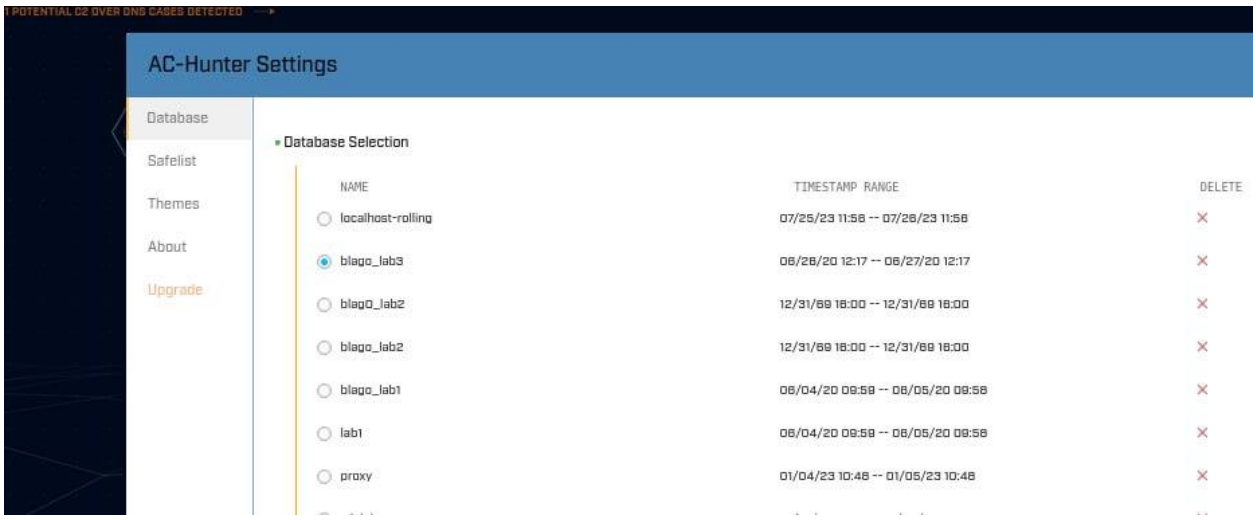


Рисунок 18 – загрузка логов для анализа в AC Hunter

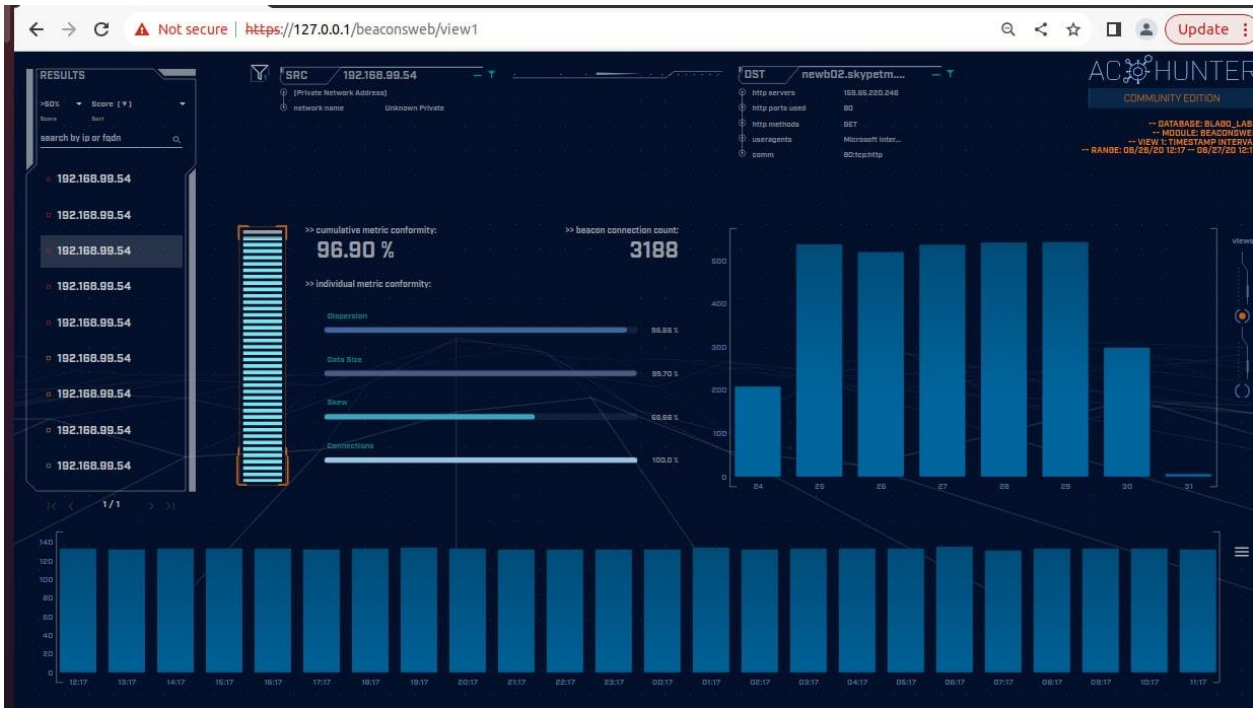


Рисунок 19 – анализ одной из записей – странное имя skype

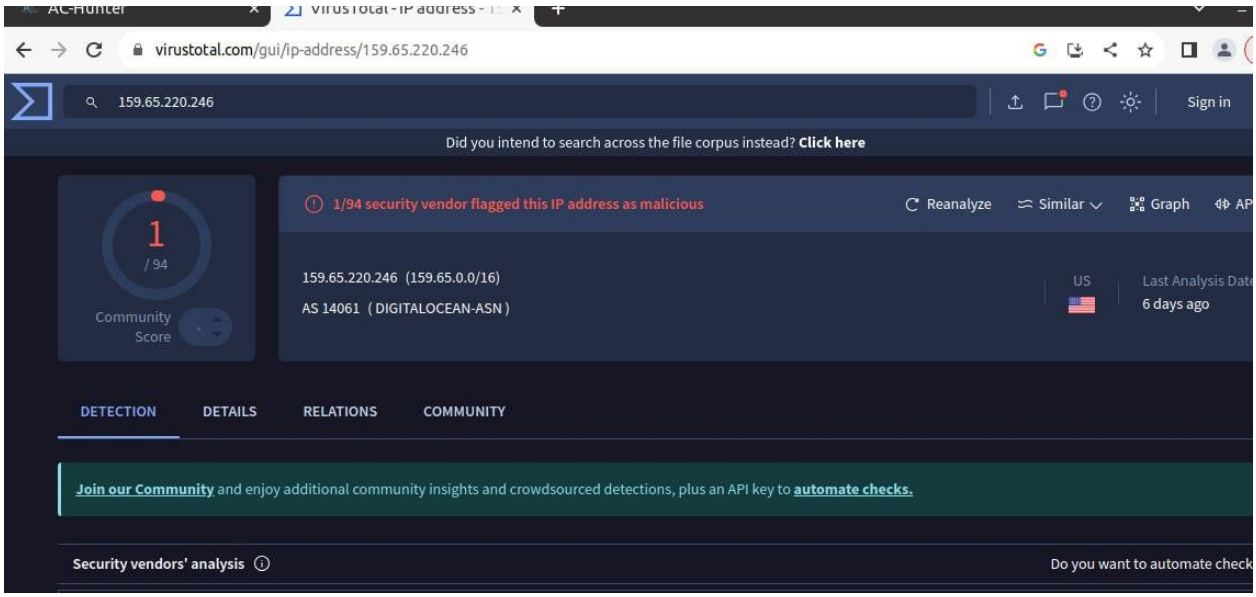


Рисунок 20 – Virustotal показал плохие результаты по сомнительному адресу

Выводы: Проанализировав результаты: графиков (гистограмм) – плоские столбцы; рейтинг на Virustotal и учитывая недопустимое имя для skype можно с уверенностью сказать, что здесь зафиксирован http-beacon.