

```
threat@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9216 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:c7:30:19 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.246.137/24 brd 192.168.246.255 scope global dynamic noprefixroute ens33
        valid_lft 1101sec preferred_lft 1101sec
    inet6 fe80::85d0:f4ab:32d7:6d30/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: br-a1acd2bf679a: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:b4:ec:24:9a brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.1/16 brd 172.18.255.255 scope global br-a1acd2bf679a
        valid_lft forever preferred_lft forever
    inet6 fe80::42:b4ff:feec:249a/64 scope link
        valid_lft forever preferred_lft forever
4: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:54:5f:f9:f6 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
6: veth6872ea7@if5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-a1acd2bf679a state UP group default
    link/ether 2e:3a:0a:d7:f3:1d brd ff:ff:ff:ff:ff:ff link-netnsid 1
    inet6 fe80::2c3a:aff:fed7:f31d/64 scope link
        valid_lft forever preferred_lft forever
8: vethc0a1b6a@if7: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-a1acd2bf679a state UP group default
    link/ether 32:e6:95:9e:88:d1 brd ff:ff:ff:ff:ff:ff link-netnsid 4
    inet6 fe80::30e6:95ff:fe9e:88d1/64 scope link
        valid_lft forever preferred_lft forever
10: vethc07511b@if9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-a1acd2bf679a state UP group default
    link/ether ea:53:87:54:36:78 brd ff:ff:ff:ff:ff:ff link-netnsid 3
    inet6 fe80::e853:87ff:fe54:3678/64 scope link
```

Рисунок 1 – демонстрация ip-адреса хоста

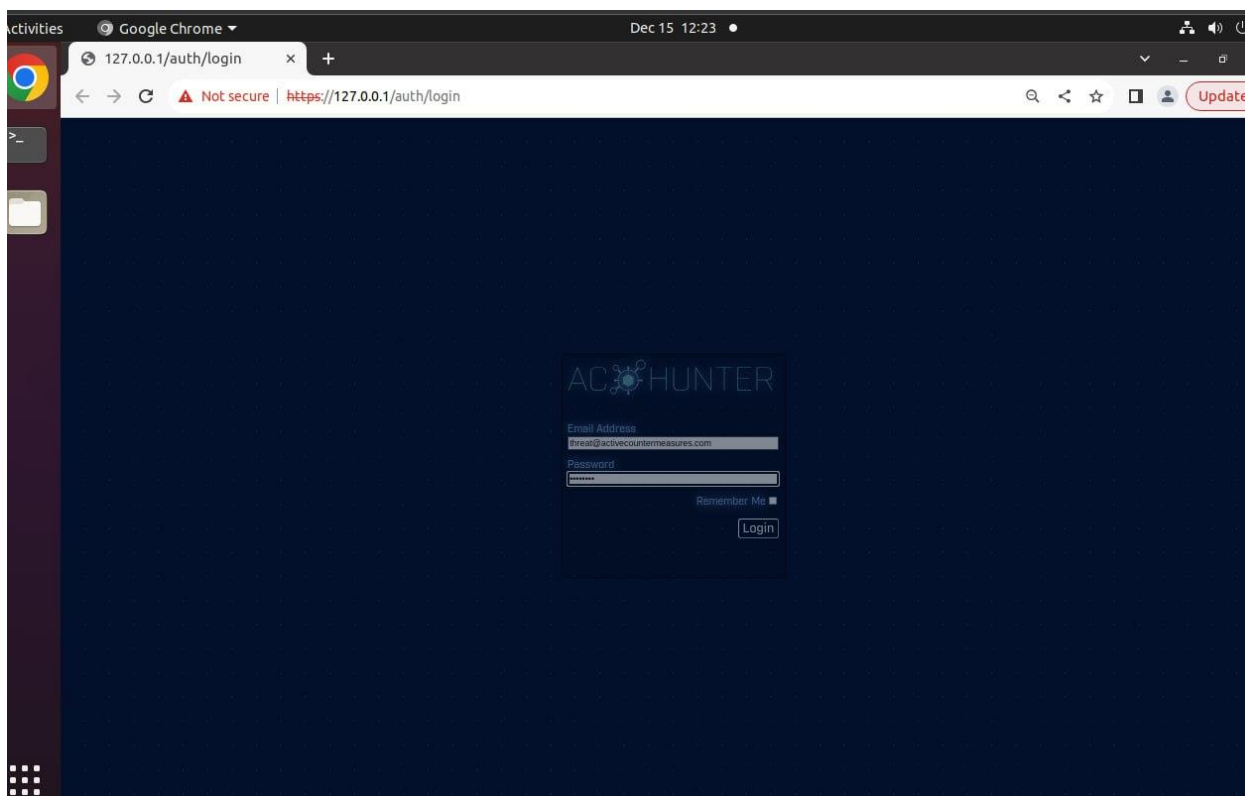


Рисунок 2 – вход в прикладное ПО

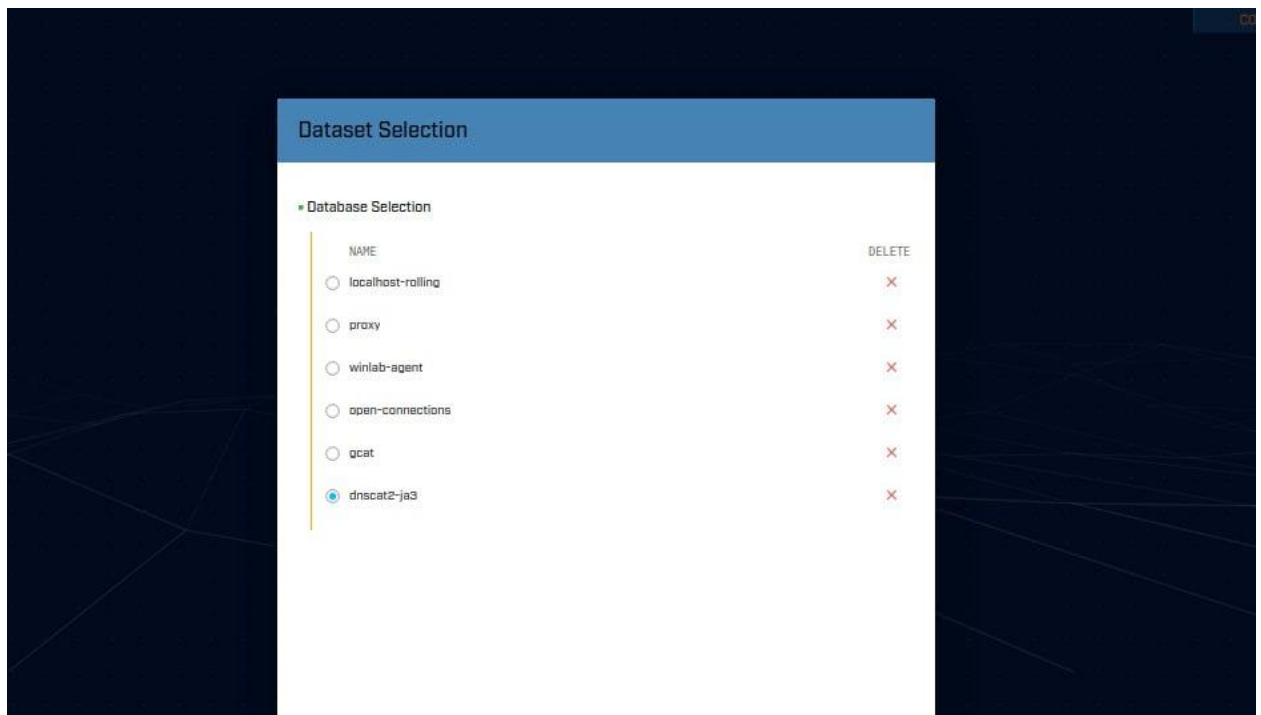


Рисунок 3 – выбор датасета dnscat2-ja3 для дальнейшей работы

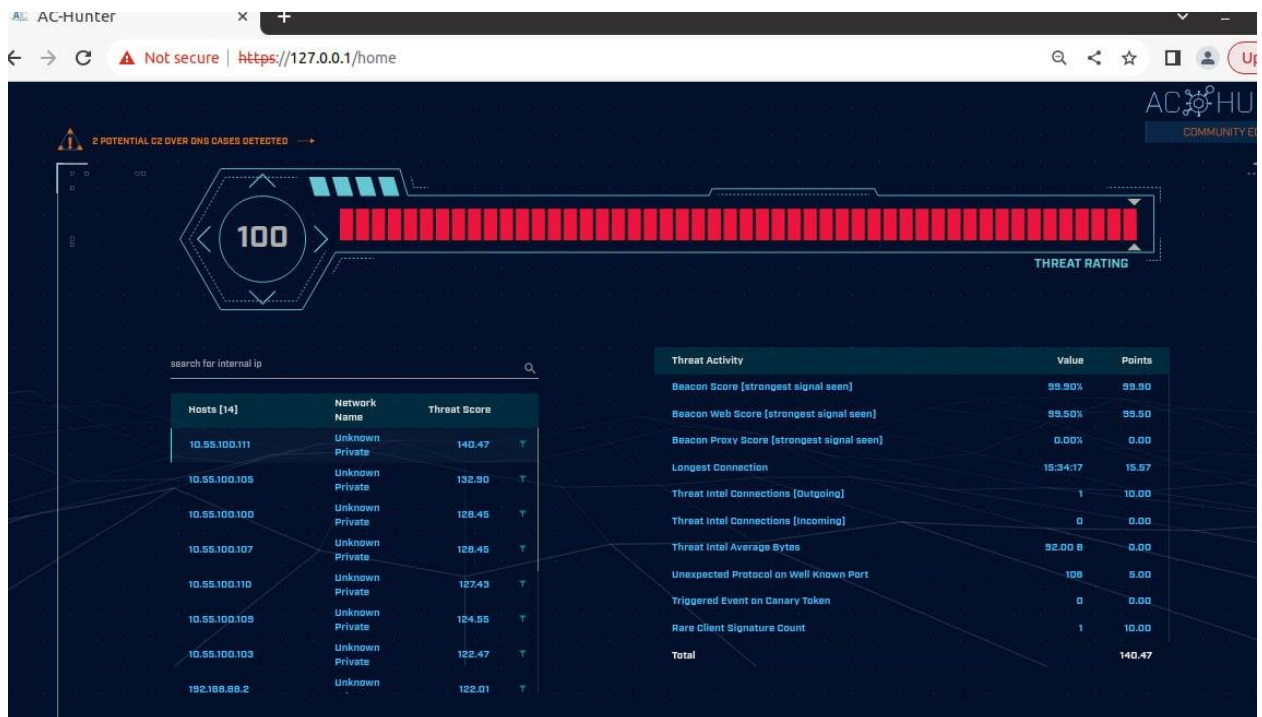


Рисунок 4 – интерфейс AC-Hunter

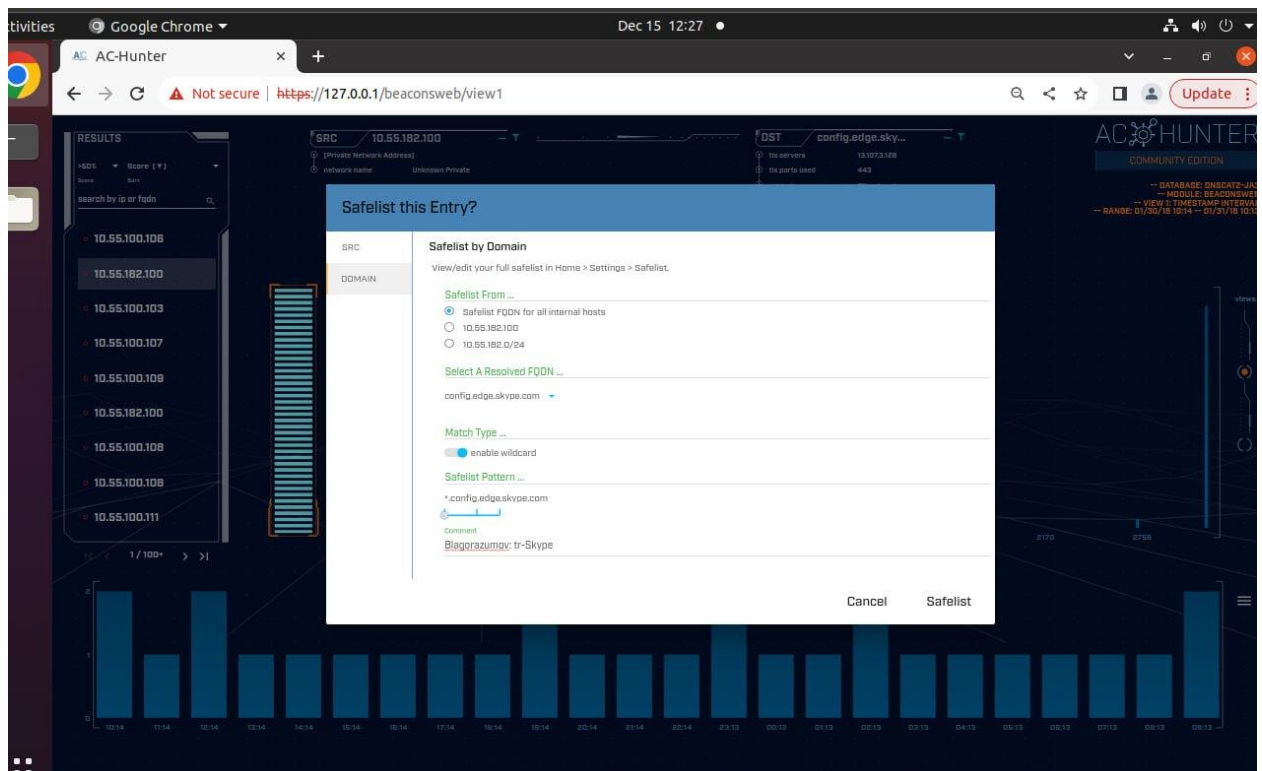


Рисунок 5 – добавляем в safelist легитимное подключение к Skype

```
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.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.log /home/threat/labs/lab1/p.log
/home/threat/labs/lab1/packet_filter.log /home/threat/labs/lab1/software.log /home/threat/labs/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: 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 %

[-] Explored DNS Analysis: 116 / 116 [=====] 100 %

[-] Hostname Analysis: 116 / 116 [=====] 100 %
```

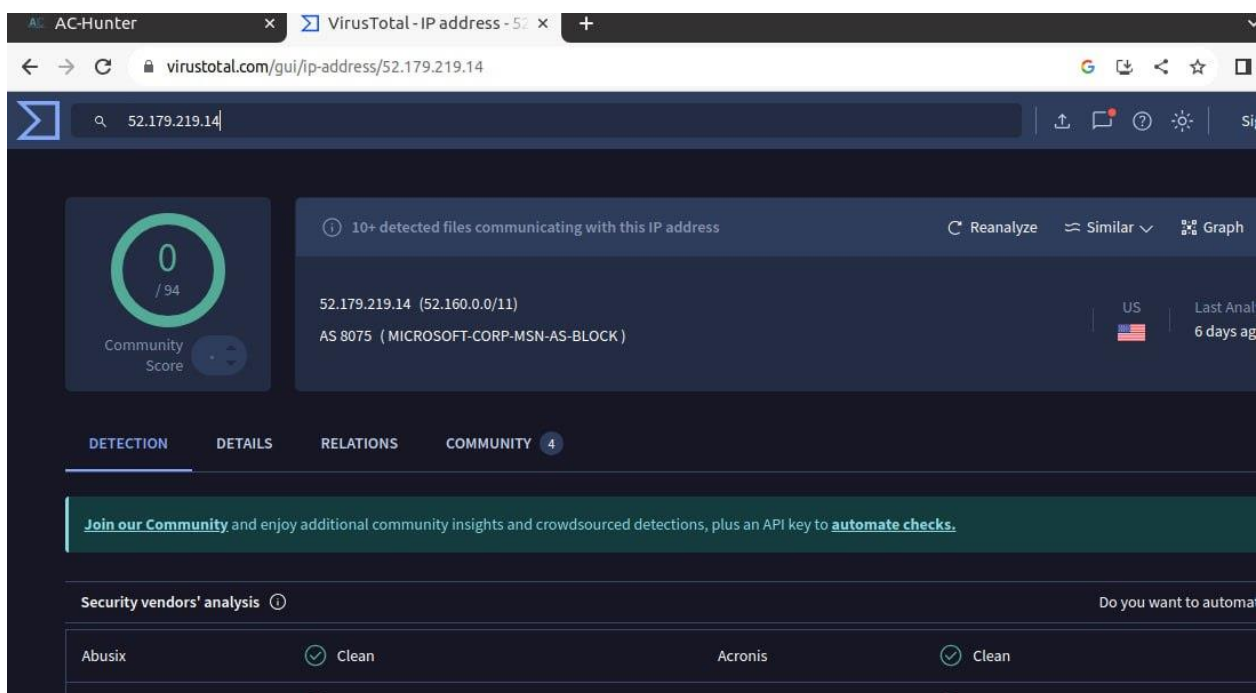
Рисунок 6 – импорт логов для 1 части лабораторной работы



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/eghmbblnphlaefbmnoenohhncmcepaperfijekpleokhjfmnmijghedkienliddbcmgdjldbegpeemiboacnfcnpbnn
hlnjbpcejfpecdioiddklfegefcbjbcnagjclnoijpajlpkkegakmpddojnlphegeehaacomfggdfkagpbighfkndllaamndepdanhnogedkaodhgakiigoheninoalnoabditio
kpebgahpnghbebkpiffooljden;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=C98EA5B0842DBB94058BF071E1DA76512D21
FE36&FORM=Threshold Microsoft-WNS/10.0
26 3.tlu.d.delivery.mp.microsoft.com /filestreamingservice/files/62023f49-c795-4f2c-b1ad-691785434443?P1=1591295946&
P2=402&P3=2&P4=NT59YouPqG4KLxd/4KmhTLEQdz6EKxsXlaLRGmYkfJ/oAVAnmgIZx2TXpHocIv5Fj1Ghc2FXZzoPXeI8/8GXW== Microsoft-Delivery-Optimization
/10.0
threat@ubuntu:~/labs/lab1$
```

Рисунок 10 – анализ логов подозрительного подключения



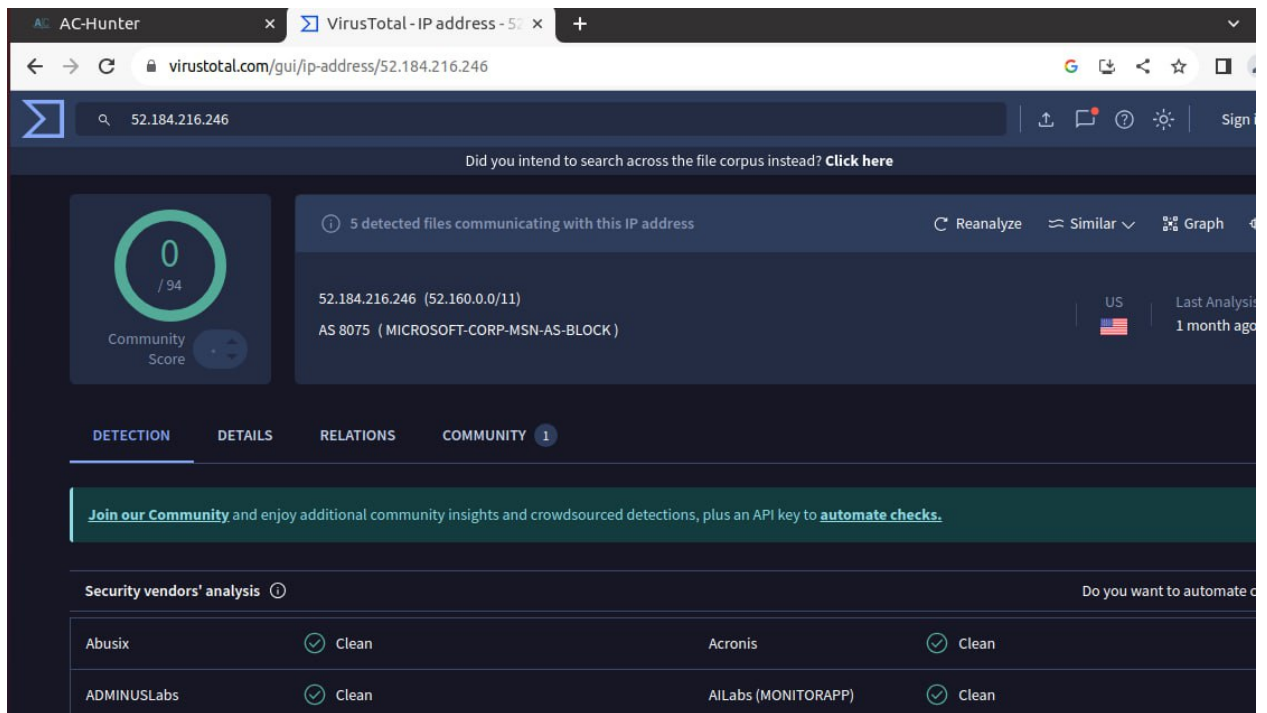


Рисунок 11-12 – проверка на VirusTotal ip-адресов остальных записей (чистых)

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

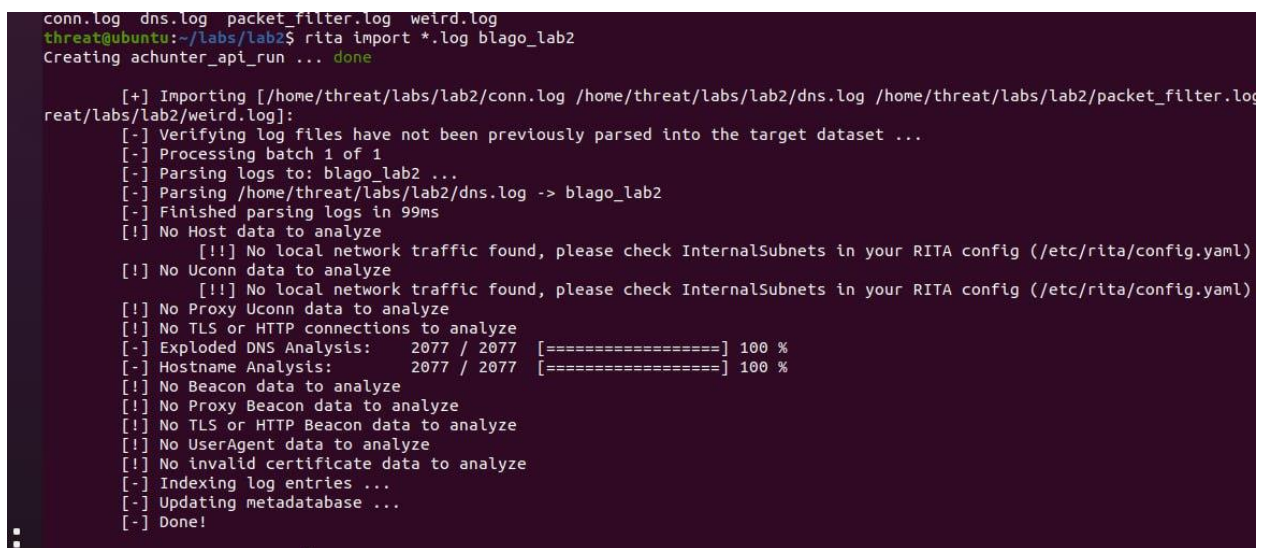


Рисунок 13 – загрузка логов для 2 части практической работы

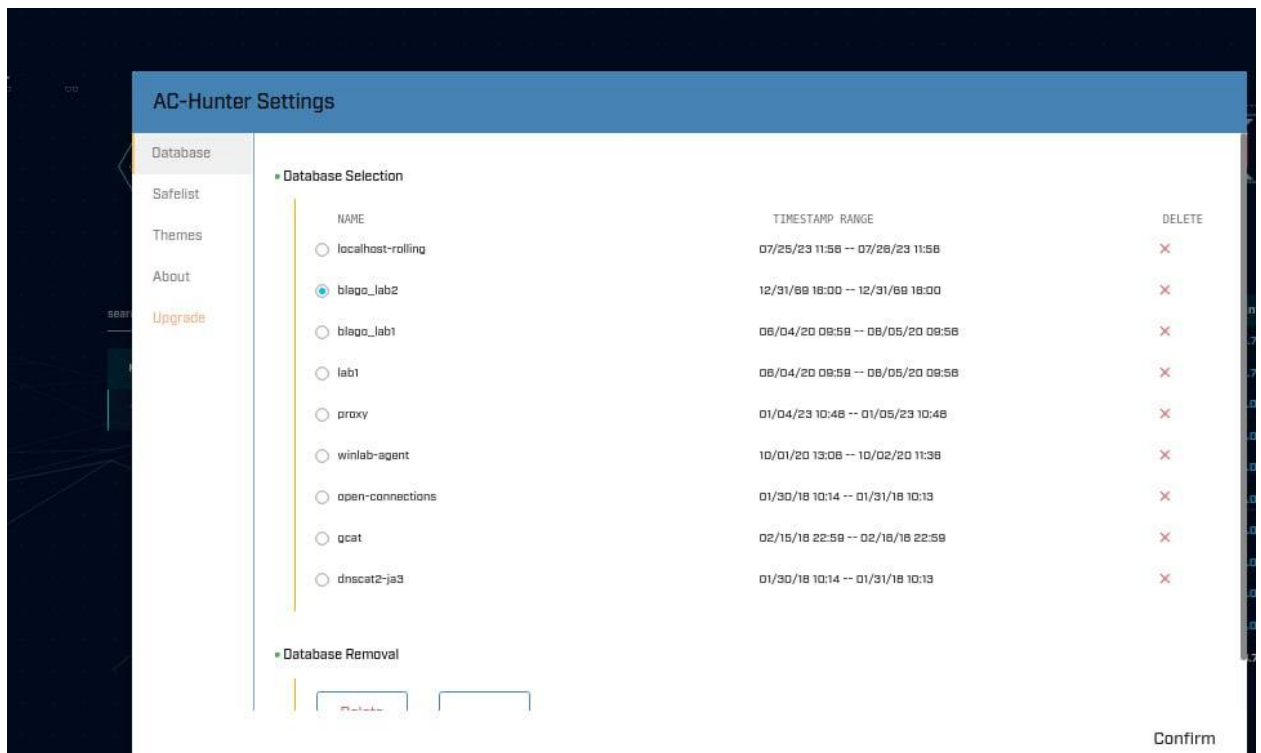
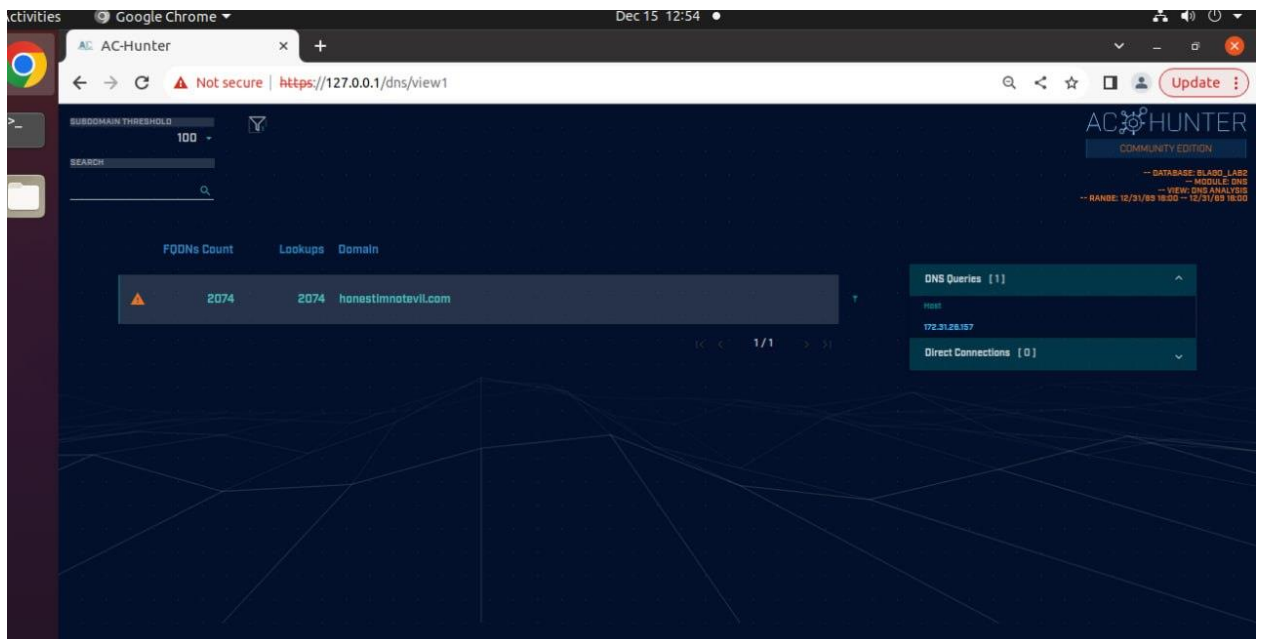


Рисунок 14 – загрузка логов для анализа в AC Hunter



FQDNs Count	Lookups	Domain
2074	2074	honestimnotevil.com
21	21	5da0b7f90908be408ac43eb80a.honestimnotevil.com
21	21	...c751246282ec22b36bb5761c2762.5da0b7f90908be408ac43eb80a.honestimnotevil.com
7	7	...c5843efe182166d82ecf895312d7.60a5291b4324545e080e62a0ea.honestimnotevil.com
7	7	60a5291b4324545e080e62a0ea.honestimnotevil.com
4	4	...48d806a1b09b25b0bbdba6a4d018.a62e1536e8f6f362509c462faa.honestimnotevil.com
4	4	...8aed61cea42db89d05185f96cb2cc0.c3d37e9c6fc2384d2378f9f16.honestimnotevil.com
4	4	a62e1536e8f6f362509c462faa.honestimnotevil.com

DNS Queries [1]
 Host
 172.31.28.157

Direct Connections [0]

Рисунок 15-16 – большое количество DNS-запросов

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

```

threat@ubuntu:~/labs/lab2$ cd
threat@ubuntu:~$ cd labs/lab3
threat@ubuntu:~/labs/lab3$ rita import *.log blago_lab3
Creating achunter_api_run ... done

[+] Importing [/home/threat/labs/lab3/capture_loss.log /home/threat/labs/lab3/conn.log /home/threat/labs/lab3/dhcp.log /home/
reat/labs/lab3/dns.log /home/threat/labs/lab3/files.log /home/threat/labs/lab3/http.log /home/threat/labs/lab3/known_hosts.log /home/
reat/labs/lab3/known_services.log /home/threat/labs/lab3/loaded_scripts.log /home/threat/labs/lab3/notice.log /home/threat/labs/lab3/
p.log /home/threat/labs/lab3/packet_filter.log /home/threat/labs/lab3/software.log /home/threat/labs/lab3/ssl.log /home/threat/labs/l
3/stats.log /home/threat/labs/lab3/x509.log]:
[-] Verifying log files have not been previously parsed into the target dataset ...
[-] Processing batch 1 of 1
[-] Parsing logs to: blago_lab3 ...
[-] Parsing /home/threat/labs/lab3/ssl.log -> blago_lab3
[-] Parsing /home/threat/labs/lab3/conn.log -> blago_lab3
[-] Parsing /home/threat/labs/lab3/dns.log -> blago_lab3
[-] Parsing /home/threat/labs/lab3/http.log -> blago_lab3
[-] Finished parsing logs in 418ms
[-] Host Analysis: 88 / 88 [=====] 100 %
[-] Unique Connection Analysis: 87 / 87 [=====] 100 %
[-] Unique Connection Aggregation: 1 / 1 [=====] 100 %
[!] No Proxy Uconn data to analyze
[-] SNI Connection Analysis: 31 / 31 [=====] 100 %
[-] Exploded DNS Analysis: 107 / 107 [=====] 100 %
[-] Hostname Analysis: 107 / 107 [=====] 100 %
[-] Beacon Analysis: 87 / 87 [=====] 100 %
[-] Beacon Aggregation: 1 / 1 [=====] 100 %
[!] No Proxy Beacon data to analyze
[-] SNI Beacon Analysis: 31 / 31 [=====] 100 %
[-] SNI Beacon Aggregation: 1 / 1 [=====] 100 %
[-] UserAgent Analysis: 8 / 8 [=====] 100 %
[-] UserAgent Aggregation: 8 / 8 [=====] 100 %
[-] Invalid Cert Analysis: 18 / 18 [=====] 100 %
[-] Indexing log entries ...
  
```

Рисунок 17 – загрузка логов для 3 части практической работы

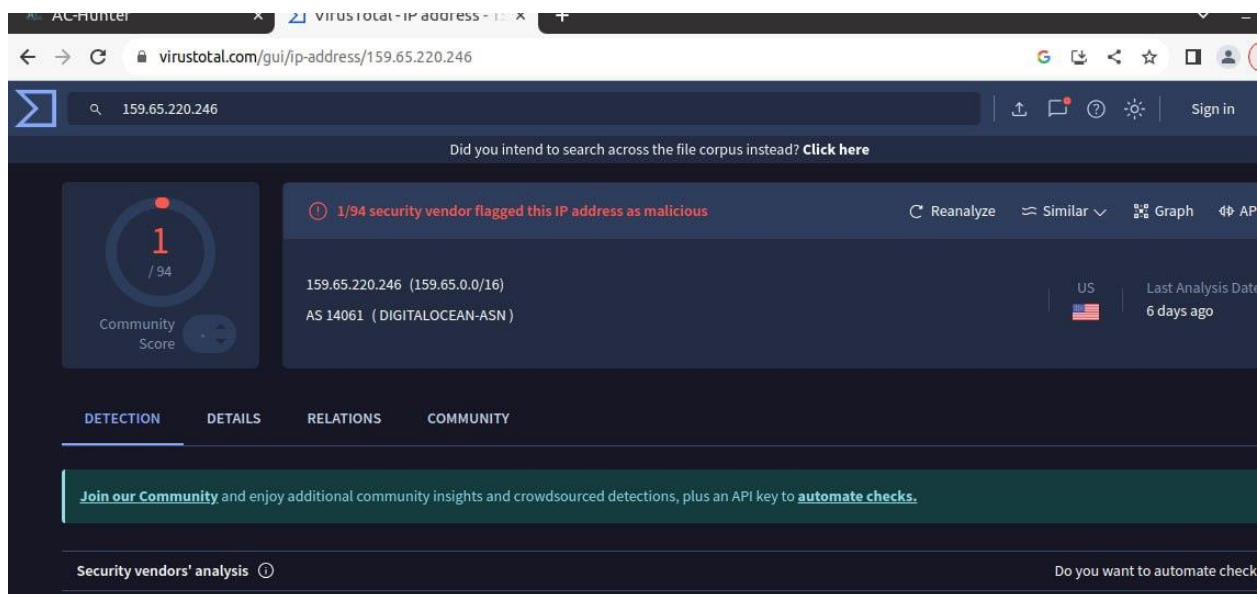


Рисунок 20 – Virustotal показал плохие результаты по сомнительному адресу

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