МІНІСТЕРСТВО ОСВІТИ, НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Лабораторна робота 5

Аналіз мережевих комунікацій

Варіант №5

Підготував:

студент 4 курсу

групи ФІ-84

Коломієць Андрій Юрійович

Email:*andkol-ipt22@lll.kpi.ua*

Викладач:

Київ – 2021

Мета роботи

Отримати навички аналізу мережевих комунікацій ШПЗ.

Постановка задачі

Дослідити методи аналізу та протидії аналізу мережевого трафіку на прикладі зразків з лабораторної роботи 4 та відомого ШПЗ.

Варіанти завдань

• Додайте INetSim у Cuckoo Sandbox . Проаналізуйте 3-5 зразків з theZoo .

• Розгорніть OpenVPN за допомогою openvpn-install , робота за протоколом TCP. На стороні клієнта встановіть з’єднання з OpenVPN сервером через HTTP проксі. Проксі можна отримати за допомогою fetch-some-proxies або онлайн сервісів.

• (опційно) Замініть OpenVPN на SoftEther VPN.

• Додайте сертифікат CA mitmproxy у список довірених на клієнті . Проаналізуйте трафік Вашого зразку з лабораторної роботи 4.

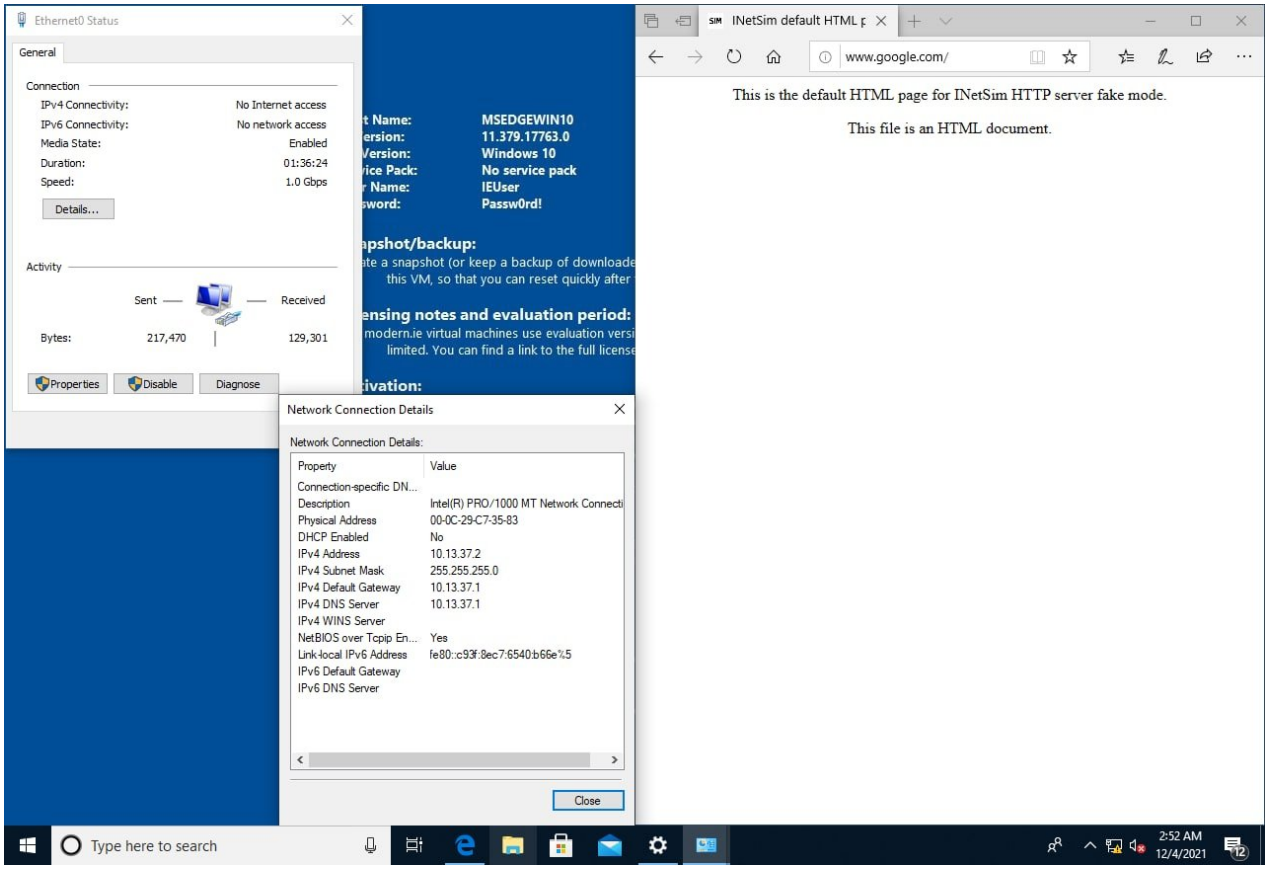
• Перенесіть реалізацію обробника пакетів на Python3 та запустіть на шлюзі . Модифікуйте трафік Вашого зразку з лабораторної роботи 4. Врахуйте можливість фрагментації пакетів .

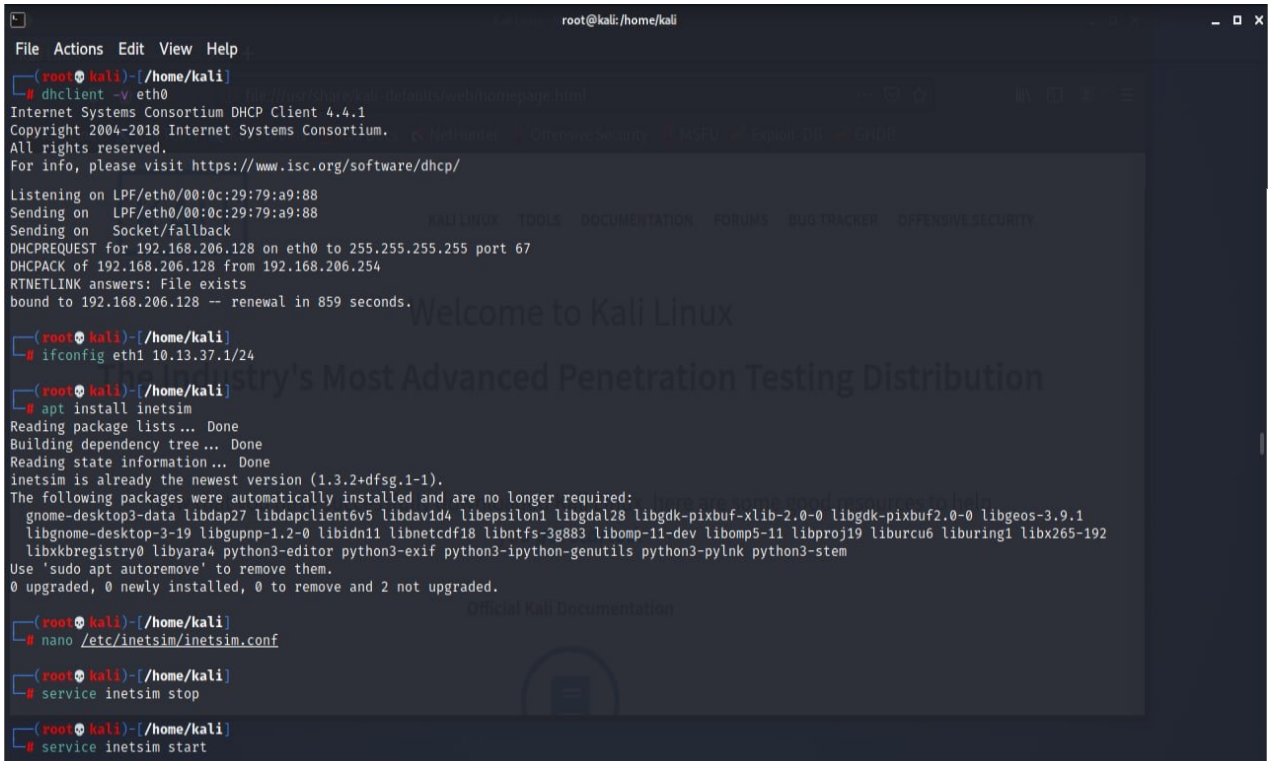
• Розробіть застосунок, що емулює (sinkhole) сервер керування для Вашого зразку з лабораторної роботи 4, – збирає інформацію про клієнта та подає команду самознищення (зразку, не цільової системи). У випадку використання Python та HTTP(S) зверніть увагу на Flask, CherryPy, Tornado та Twisted.

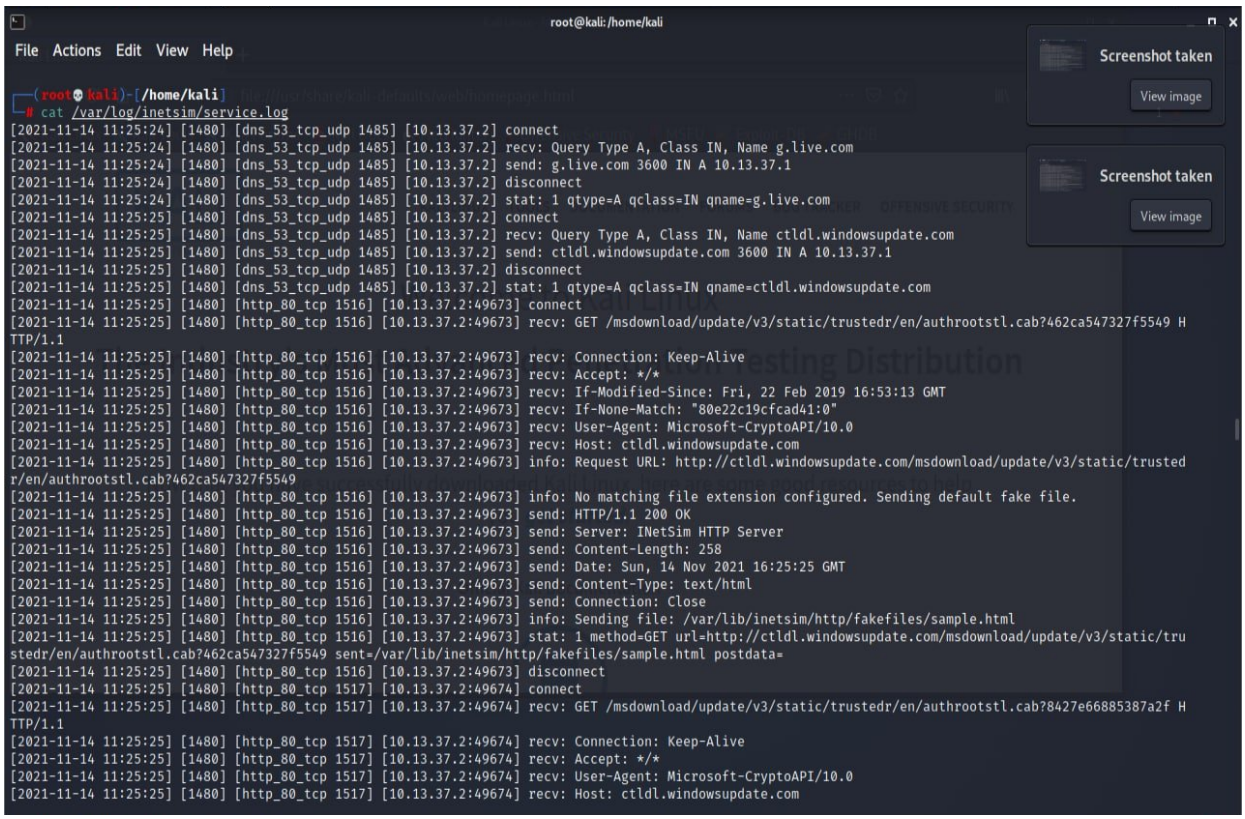
• (підвищеної складності) Розшифруйте трафік за умови доступу до пам’яті openssl під час роботи.

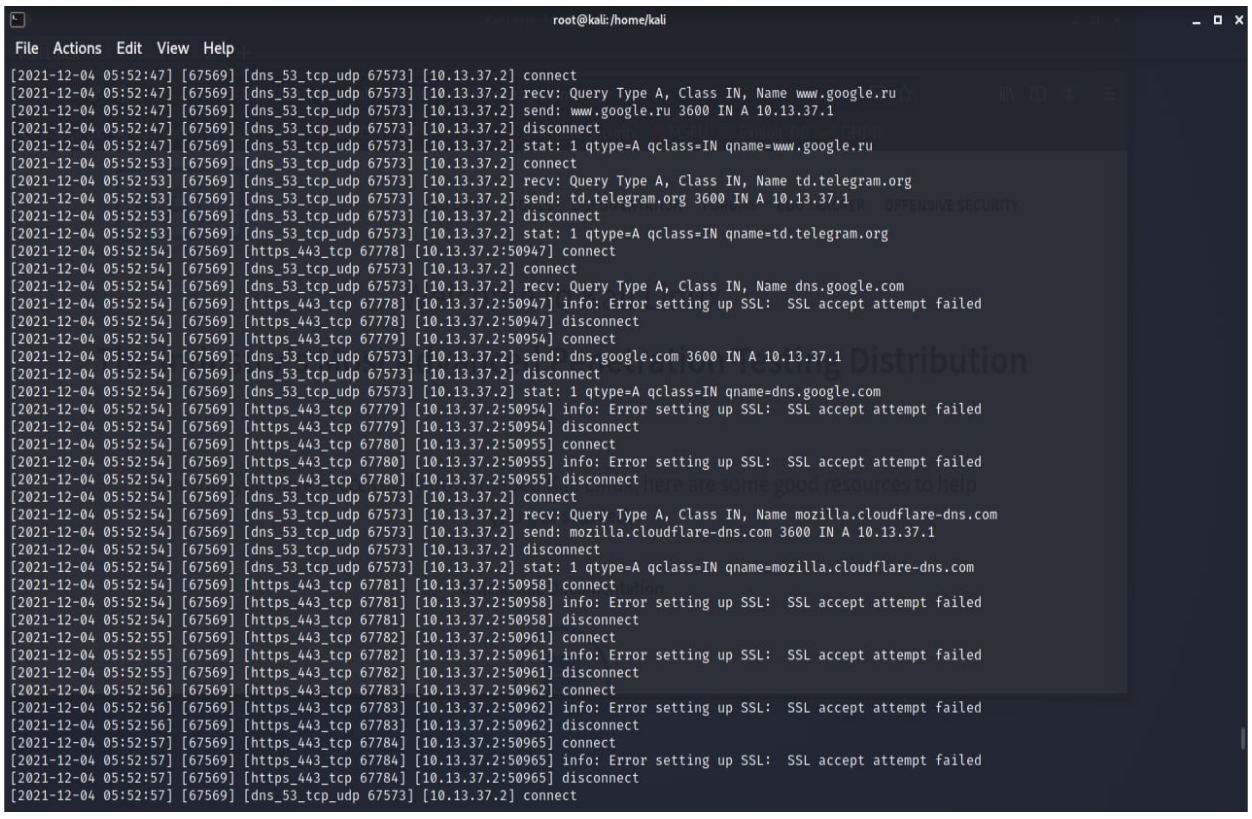
Виконання завдання

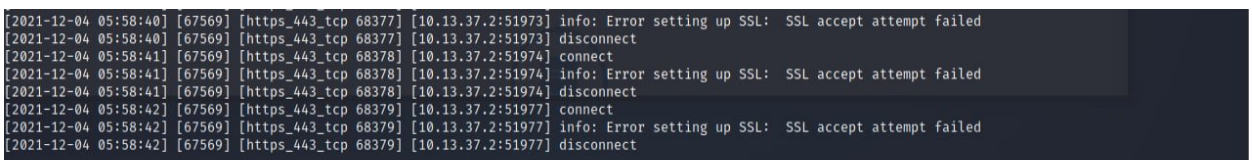
*Додайте **INetSim у Cuckoo Sandbox** . Проаналізуйте **3-5** зразків з **theZoo**.*



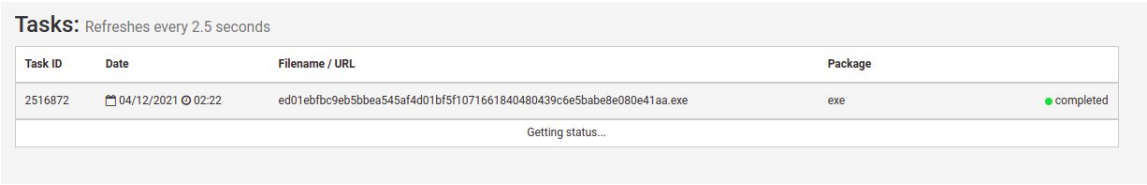



root@kali: /home/kali
File Actions Edit View Help
Screenshot taken
View image
Screenshot taken
View image
┌──(root💀kali)-[/home/kali]
└─# cat /var/log/inetsim/service.log
[2021-11-14 11:25:24] [1480] [dns_53_tcp_udp 1485] [10.13.37.2] connect
[2021-11-14 11:25:24] [1480] [dns_53_tcp_udp 1485] [10.13.37.2] recv: Query Type A, Class IN, Name g.live.com
[2021-11-14 11:25:24] [1480] [dns_53_tcp_udp 1485] [10.13.37.2] send: g.live.com 3600 IN A 10.13.37.1
[2021-11-14 11:25:24] [1480] [dns_53_tcp_udp 1485] [10.13.37.2] disconnect
[2021-11-14 11:25:24] [1480] [dns_53_tcp_udp 1485] [10.13.37.2] stat: 1 qtype=A qclass=IN qname=g.live.com
[2021-11-14 11:25:25] [1480] [dns_53_tcp_udp 1485] [10.13.37.2] connect
[2021-11-14 11:25:25] [1480] [dns_53_tcp_udp 1485] [10.13.37.2] recv: Query Type A, Class IN, Name ctldl.windowsupdate.com
[2021-11-14 11:25:25] [1480] [dns_53_tcp_udp 1485] [10.13.37.2] send: ctldl.windowsupdate.com 3600 IN A 10.13.37.1
[2021-11-14 11:25:25] [1480] [dns_53_tcp_udp 1485] [10.13.37.2] disconnect
[2021-11-14 11:25:25] [1480] [dns_53_tcp_udp 1485] [10.13.37.2] stat: 1 qtype=A qclass=IN qname=ctldl.windowsupdate.com
[2021-11-14 11:25:25] [1480] [http_80_tcp 1516] [10.13.37.2:49673] connect
[2021-11-14 11:25:25] [1480] [http_80_tcp 1516] [10.13.37.2:49673] recv: GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?462ca547327f5549 H
TTP/1.1
[2021-11-14 11:25:25] [1480] [http_80_tcp 1516] [10.13.37.2:49673] recv: Connection: Keep-Alive
[2021-11-14 11:25:25] [1480] [http_80_tcp 1516] [10.13.37.2:49673] recv: Accept: */*
[2021-11-14 11:25:25] [1480] [http_80_tcp 1516] [10.13.37.2:49673] recv: If-Modified-Since: Fri, 22 Feb 2019 16:53:13 GMT
[2021-11-14 11:25:25] [1480] [http_80_tcp 1516] [10.13.37.2:49673] recv: If-None-Match: "80e22c19cfcad41:0"
[2021-11-14 11:25:25] [1480] [http_80_tcp 1516] [10.13.37.2:49673] recv: User-Agent: Microsoft-CryptoAPI/10.0
[2021-11-14 11:25:25] [1480] [http_80_tcp 1516] [10.13.37.2:49673] recv: Host: ctldl.windowsupdate.com
[2021-11-14 11:25:25] [1480] [http_80_tcp 1516] [10.13.37.2:49673] info: Request URL: http://ctldl.windowsupdate.com/msdownload/update/v3/static/trusted
r/en/authrootstl.cab?462ca547327f5549
[2021-11-14 11:25:25] [1480] [http_80_tcp 1516] [10.13.37.2:49673] info: No matching file extension configured. Sending default fake file.
[2021-11-14 11:25:25] [1480] [http_80_tcp 1516] [10.13.37.2:49673] send: HTTP/1.1 200 OK
[2021-11-14 11:25:25] [1480] [http_80_tcp 1516] [10.13.37.2:49673] send: Server: INetSim HTTP Server
[2021-11-14 11:25:25] [1480] [http_80_tcp 1516] [10.13.37.2:49673] send: Content-Length: 258
[2021-11-14 11:25:25] [1480] [http_80_tcp 1516] [10.13.37.2:49673] send: Date: Sun, 14 Nov 2021 16:25:25 GMT
[2021-11-14 11:25:25] [1480] [http_80_tcp 1516] [10.13.37.2:49673] send: Content-Type: text/html
[2021-11-14 11:25:25] [1480] [http_80_tcp 1516] [10.13.37.2:49673] send: Connection: Close
[2021-11-14 11:25:25] [1480] [http_80_tcp 1516] [10.13.37.2:49673] info: Sending file: /var/lib/inetsim/http/fakefiles/sample.html
[2021-11-14 11:25:25] [1480] [http_80_tcp 1516] [10.13.37.2:49673] stat: 1 method=GET url=http://ctldl.windowsupdate.com/msdownload/update/v3/static/tru
stedr/en/authrootstl.cab?462ca547327f5549 sent=/var/lib/inetsim/http/fakefiles/sample.html postdata=
[2021-11-14 11:25:25] [1480] [http_80_tcp 1516] [10.13.37.2:49673] disconnect
[2021-11-14 11:25:25] [1480] [http_80_tcp 1517] [10.13.37.2:49674] connect
[2021-11-14 11:25:25] [1480] [http_80_tcp 1517] [10.13.37.2:49674] recv: GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?8427e66885387a2f H
TTP/1.1
[2021-11-14 11:25:25] [1480] [http_80_tcp 1517] [10.13.37.2:49674] recv: Connection: Keep-Alive
[2021-11-14 11:25:25] [1480] [http_80_tcp 1517] [10.13.37.2:49674] recv: Accept: */*
[2021-11-14 11:25:25] [1480] [http_80_tcp 1517] [10.13.37.2:49674] recv: User-Agent: Microsoft-CryptoAPI/10.0
[2021-11-14 11:25:25] [1480] [http_80_tcp 1517] [10.13.37.2:49674] recv: Host: ctldl.windowsupdate.com


root@kali: /home/kali
File Actions Edit View Help
[2021-12-04 05:52:47] [67569] [dns_53_tcp_udp 67573] [10.13.37.2] connect
[2021-12-04 05:52:47] [67569] [dns_53_tcp_udp 67573] [10.13.37.2] recv: Query Type A, Class IN, Name www.google.ru
[2021-12-04 05:52:47] [67569] [dns_53_tcp_udp 67573] [10.13.37.2] send: www.google.ru 3600 IN A 10.13.37.1
[2021-12-04 05:52:47] [67569] [dns_53_tcp_udp 67573] [10.13.37.2] disconnect
[2021-12-04 05:52:47] [67569] [dns_53_tcp_udp 67573] [10.13.37.2] stat: 1 qtype=A qclass=IN qname=www.google.ru
[2021-12-04 05:52:53] [67569] [dns_53_tcp_udp 67573] [10.13.37.2] connect
[2021-12-04 05:52:53] [67569] [dns_53_tcp_udp 67573] [10.13.37.2] recv: Query Type A, Class IN, Name td.telegram.org
[2021-12-04 05:52:53] [67569] [dns_53_tcp_udp 67573] [10.13.37.2] send: td.telegram.org 3600 IN A 10.13.37.1
[2021-12-04 05:52:53] [67569] [dns_53_tcp_udp 67573] [10.13.37.2] disconnect
[2021-12-04 05:52:53] [67569] [dns_53_tcp_udp 67573] [10.13.37.2] stat: 1 qtype=A qclass=IN qname=td.telegram.org
[2021-12-04 05:52:54] [67569] [https_443_tcp 67778] [10.13.37.2:50947] connect
[2021-12-04 05:52:54] [67569] [dns_53_tcp_udp 67573] [10.13.37.2] connect
[2021-12-04 05:52:54] [67569] [dns_53_tcp_udp 67573] [10.13.37.2] recv: Query Type A, Class IN, Name dns.google.com
[2021-12-04 05:52:54] [67569] [https_443_tcp 67778] [10.13.37.2:50947] info: Error setting up SSL: SSL accept attempt failed
[2021-12-04 05:52:54] [67569] [https_443_tcp 67778] [10.13.37.2:50947] disconnect
[2021-12-04 05:52:54] [67569] [https_443_tcp 67779] [10.13.37.2:50954] connect
[2021-12-04 05:52:54] [67569] [dns_53_tcp_udp 67573] [10.13.37.2] send: dns.google.com 3600 IN A 10.13.37.1
[2021-12-04 05:52:54] [67569] [dns_53_tcp_udp 67573] [10.13.37.2] disconnect
[2021-12-04 05:52:54] [67569] [dns_53_tcp_udp 67573] [10.13.37.2] stat: 1 qtype=A qclass=IN qname=dns.google.com
[2021-12-04 05:52:54] [67569] [https_443_tcp 67779] [10.13.37.2:50954] info: Error setting up SSL: SSL accept attempt failed
[2021-12-04 05:52:54] [67569] [https_443_tcp 67779] [10.13.37.2:50954] disconnect
[2021-12-04 05:52:54] [67569] [https_443_tcp 67780] [10.13.37.2:50955] connect
[2021-12-04 05:52:54] [67569] [https_443_tcp 67780] [10.13.37.2:50955] info: Error setting up SSL: SSL accept attempt failed
[2021-12-04 05:52:54] [67569] [https_443_tcp 67780] [10.13.37.2:50955] disconnect
[2021-12-04 05:52:54] [67569] [dns_53_tcp_udp 67573] [10.13.37.2] connect
[2021-12-04 05:52:54] [67569] [dns_53_tcp_udp 67573] [10.13.37.2] recv: Query Type A, Class IN, Name mozilla.cloudflare-dns.com
[2021-12-04 05:52:54] [67569] [dns_53_tcp_udp 67573] [10.13.37.2] send: mozilla.cloudflare-dns.com 3600 IN A 10.13.37.1
[2021-12-04 05:52:54] [67569] [dns_53_tcp_udp 67573] [10.13.37.2] disconnect
[2021-12-04 05:52:54] [67569] [dns_53_tcp_udp 67573] [10.13.37.2] stat: 1 qtype=A qclass=IN qname=mozilla.cloudflare-dns.com
[2021-12-04 05:52:54] [67569] [https_443_tcp 67781] [10.13.37.2:50958] connect
[2021-12-04 05:52:54] [67569] [https_443_tcp 67781] [10.13.37.2:50958] info: Error setting up SSL: SSL accept attempt failed
[2021-12-04 05:52:54] [67569] [https_443_tcp 67781] [10.13.37.2:50958] disconnect
[2021-12-04 05:52:55] [67569] [https_443_tcp 67782] [10.13.37.2:50961] connect
[2021-12-04 05:52:55] [67569] [https_443_tcp 67782] [10.13.37.2:50961] info: Error setting up SSL: SSL accept attempt failed
[2021-12-04 05:52:55] [67569] [https_443_tcp 67782] [10.13.37.2:50961] disconnect
[2021-12-04 05:52:56] [67569] [https_443_tcp 67783] [10.13.37.2:50962] connect
[2021-12-04 05:52:56] [67569] [https_443_tcp 67783] [10.13.37.2:50962] info: Error setting up SSL: SSL accept attempt failed
[2021-12-04 05:52:56] [67569] [https_443_tcp 67783] [10.13.37.2:50962] disconnect
[2021-12-04 05:52:57] [67569] [https_443_tcp 67784] [10.13.37.2:50965] connect
[2021-12-04 05:52:57] [67569] [https_443_tcp 67784] [10.13.37.2:50965] info: Error setting up SSL: SSL accept attempt failed
[2021-12-04 05:52:57] [67569] [https_443_tcp 67784] [10.13.37.2:50965] disconnect
[2021-12-04 05:52:57] [67569] [dns_53_tcp_udp 67573] [10.13.37.2] connect

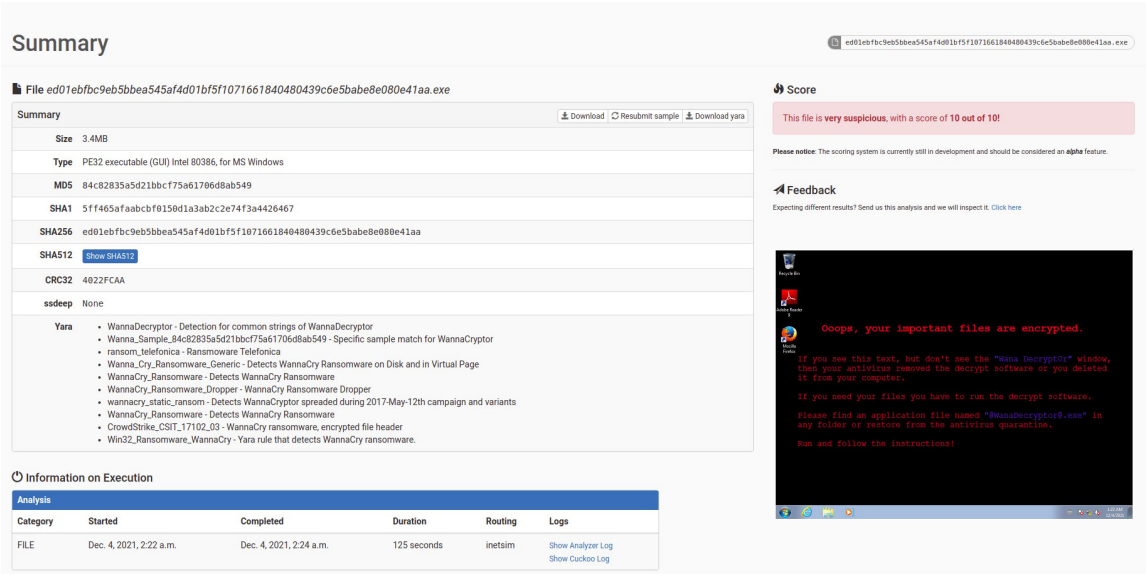

[2021-12-04 05:58:40] [67569] [https_443_tcp 68377] [10.13.37.2:51973] info: Error setting up SSL: SSL accept attempt failed
[2021-12-04 05:58:40] [67569] [https_443_tcp 68377] [10.13.37.2:51973] disconnect
[2021-12-04 05:58:41] [67569] [https_443_tcp 68378] [10.13.37.2:51974] connect
[2021-12-04 05:58:41] [67569] [https_443_tcp 68378] [10.13.37.2:51974] info: Error setting up SSL: SSL accept attempt failed
[2021-12-04 05:58:41] [67569] [https_443_tcp 68378] [10.13.37.2:51974] disconnect
[2021-12-04 05:58:42] [67569] [https_443_tcp 68379] [10.13.37.2:51977] connect
[2021-12-04 05:58:42] [67569] [https_443_tcp 68379] [10.13.37.2:51977] info: Error setting up SSL: SSL accept attempt failed
[2021-12-04 05:58:42] [67569] [https_443_tcp 68379] [10.13.37.2:51977] disconnect

Wanna Cry



Tasks: Refreshes every 2.5 seconds

Task ID	Date	Filename / URL	Package	
2516872	04/12/2021 02:22	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe	exe	completed
Getting status...				



Summary

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

File *ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe*

Summary — Download | Resubmit sample | Download yara

Size	3.4MB
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	84c82835a5d21bbcf75a61706d8ab549
SHA1	5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
SHA256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
SHA512	Show SHA512
CRC32	4022FCAA
ssdeep	None

Yara

- WannaDecryptor - Detection for common strings of WannaDecryptor
- Wanna_Sample_84c82835a5d21bbcf75a61706d8ab549 - Specific sample match for WannaCryptor
- ransom_telefonica - Ransmoware Telefonica
- Wanna_Cry_Ransomware_Generic - Detects WannaCry Ransomware on Disk and in Virtual Page
- WannaCry_Ransomware - Detects WannaCry Ransomware
- WannaCry_Ransomware_Dropper - WannaCry Ransomware Dropper
- wannacry_static_ransom - Detects WannaCryptor spreaded during 2017-May-12th campaign and variants
- WannaCry_Ransomware - Detects WannaCry Ransomware
- CrowdStrike_CSIT_17102_03 - WannaCry ransomware, encrypted file header
- Win32_Ransomware_WannaCry - Yara rule that detects WannaCry ransomware.

Information on Execution

Analysis

Category	Started	Completed	Duration	Routing	Logs
FILE	Dec. 4, 2021, 2:22 a.m.	Dec. 4, 2021, 2:24 a.m.	125 seconds	inetsim	Show Analyzer Log Show Cuckoo Log

Score

This file is **very suspicious**, with a score of **10 out of 10!**

Please notice: The scoring system is currently still in development and should be considered an **alpha** feature.

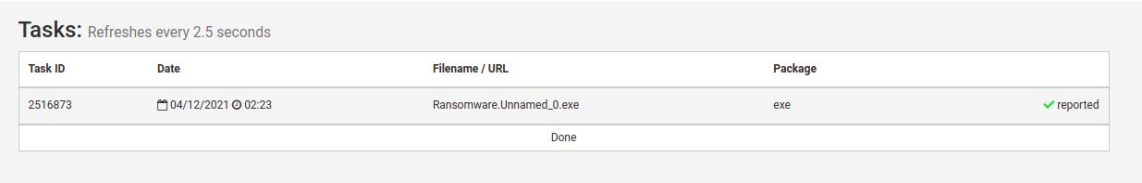
Feedback

Expecting different results? Send us this analysis and we will inspect it. Click here

Посилання на Cuckoo Sandbox report:

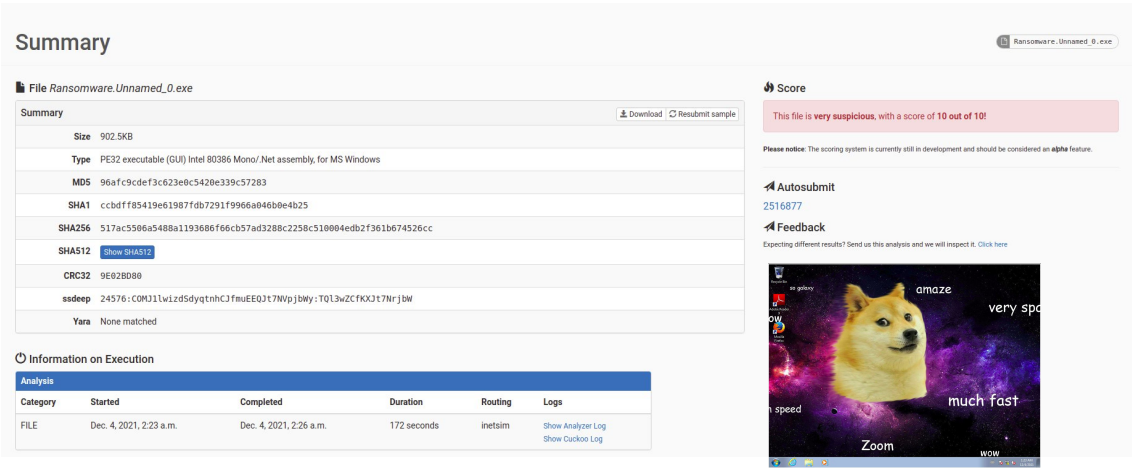
https://cuckoo.cert.ee/analysis/2516872/summary/

Ransomware.Unnamed_0



Tasks: Refreshes every 2.5 seconds

Task ID	Date	Filename / URL	Package	
2516873	04/12/2021 02:23	Ransomware.Unnamed_0.exe	exe	reported
Done				



Summary

Ransomware.Unnamed_0.exe

File *Ransomware.Unnamed_0.exe*

Summary	Download / Resubmit sample
Size	902.5KB
Type	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5	96afc9cdef3c623e0c5420e339c57283
SHA1	ccbdff85419e61987fdb7291f9966a046b0e4b25
SHA256	517ac5506a5488a1193686f66cb57ad3288c2258c510004edb2f361b674526cc
SHA512	Show SHA512
CRC32	9E02BD80
ssdeep	24576:COMJ1lwizdSdyqtnhCJfmuEEQJt7NVpjbWy:TQl3wZCfKXJt7NrjbW
Yara	None matched

Information on Execution

Analysis					
Category	Started	Completed	Duration	Routing	Logs
FILE	Dec. 4, 2021, 2:23 a.m.	Dec. 4, 2021, 2:26 a.m.	172 seconds	inetsim	Show Analyzer Log Show Cuckoo Log

Score

This file is **very suspicious**, with a score of **10 out of 10!**

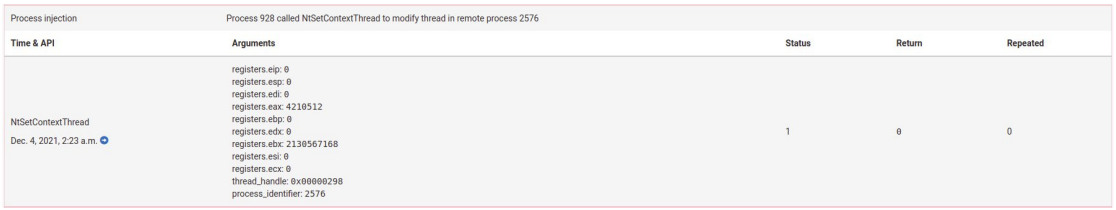
Please notice: The scoring system is currently still in development and should be considered an **alpha** feature.

Autosubmit

2516877

Feedback

Expecting different results? Send us this analysis and we will inspect it. Click here

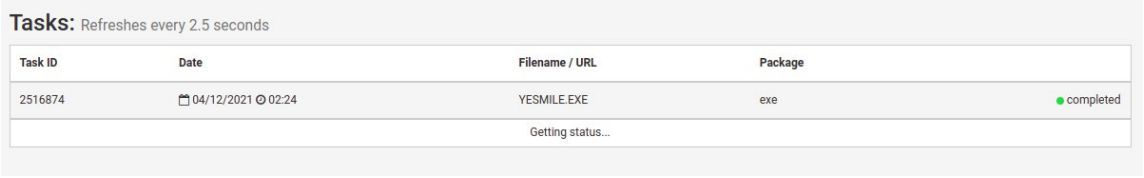


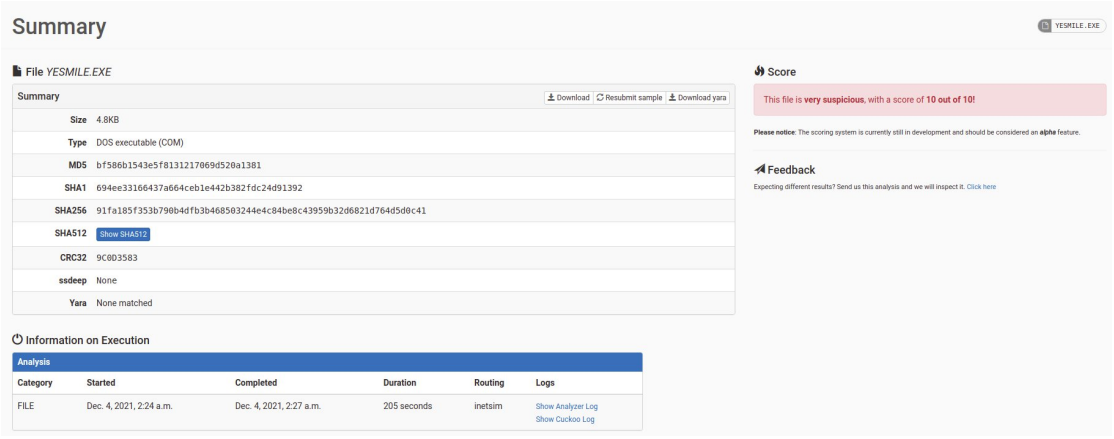
Process injection	Process 928 called NtSetContextThread to modify thread in remote process 2576			
Time & API	**Arguments**	**Status**	**Return**	**Repeated**
NtSetContextThread Dec. 4, 2021, 2:23 a.m.	registers.eip: 0 registers.esp: 0 registers.edi: 0 registers.eax: 4210512 registers.ebp: 0 registers.edx: 0 registers.ebx: 2130567168 registers.esi: 0 registers.ecx: 0 thread_handle: 0x00000298 process_identifier: 2576	1	0	0

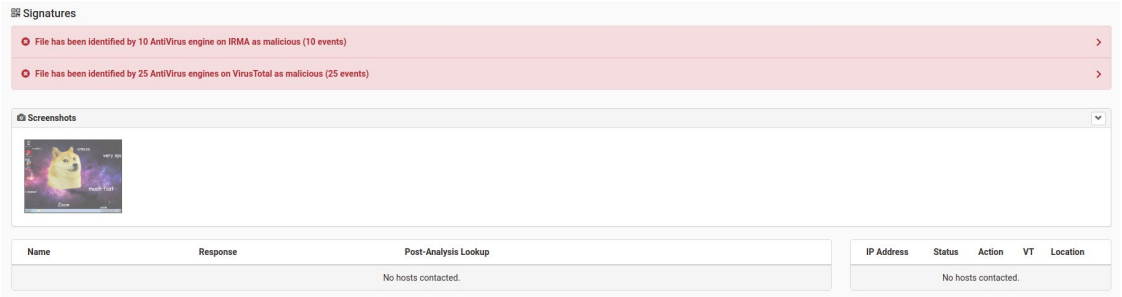
Посилання на Cuckoo Sandbox report:

https://cuckoo.cert.ee/analysis/2516873/summary/

YESMILE







Посилання на Cuckoo Sandbox report:

https://cuckoo.cert.ee/analysis/2516874/summary/

*Розгорніть **OpenVPN** за допомогою **openvpn-install**, робота за протоколом **TCP**. На стороні клієнта встановіть з'єднання з **OpenVPN** сервером через **HTTP** проксі. Проксі можна отримати за допомогою **fetch-some-proxies** або онлайн сервісів.*

Отримуємо проксі.

```
┌──(kali㉿kali)-[~/Downloads/fetch-some-proxies-master]
└─$ python fetch.py --help
+-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-+
|f||e||t||c||h||-||s||o||m||e||-||p||r||o||x||i||e||s| ← v3.2.3
+-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-+

Usage: fetch.py [options]

Options:
  --version           Show program's version number and exit
  -h, --help          Show this help message and exit
  --anonymity=ANON..  Regex for filtering anonymity (e.g. "anonymous|elite")
  --country=COUNTRY   Regex for filtering country (e.g. "china|brazil")
  --max-latency=MA..  Maximum (tolerable) latency in seconds (default 10)
  --no-https          Disable HTTPS checking (not recommended)
  --output=OUTPUTF..  Store resulting proxies to output file
  --port=PORT         List of ports for filtering (e.g. "1080,8000")
  --raw               Display only results (minimal verbosity)
  --threads=THREADS   Number of scanning threads (default 20)
  --timeout=TIMEOUT   Request timeout in seconds (default 10)
  --type=TYPE         Regex for filtering proxy type (e.g. "http")


┌──(kali㉿kali)-[~/Downloads/fetch-some-proxies-master]
└─$ python fetch.py
+-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-+
|f||e||t||c||h||-||s||o||m||e||-||p||r||o||x||i||e||s| ← v3.2.3
+-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-+

[i] initial testing...
[i] retrieving list of proxies...
[i] testing 1768 proxies (20 threads)...

http://131.255.239.38:3128       # latency: 3.24 sec; country: Brazil; anony
mity: elite (high)
http://120.196.112.6:3128        # latency: 3.13 sec; country: China; anonym
ity: elite (high)
```

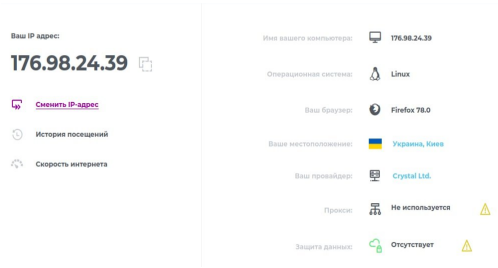
На стороні клієнта встановимо з'єднання з OpenVPN сервером через HTTP проксі.

З'єднання

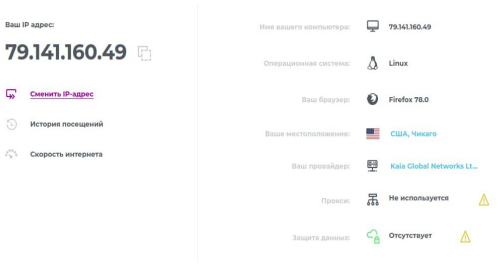
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo openvpn --config USA freeopenvpn tcp.ovpn --http-proxy 131.255.239.
38 3128
2021-12-04 08:06:56 DEPRECATED OPTION: --max-routes option ignored.The numbe
r of routes is unlimited as of OpenVPN 2.4. This option will be removed in a
 future version, please remove it from your configuration.
2021-12-04 08:06:56 DEPRECATED OPTION: --cipher set to 'AES-128-CBC' but mis
sing in --data-ciphers (AES-256-GCM:AES-128-GCM). Future OpenVPN version wil
l ignore --cipher for cipher negotiations. Add 'AES-128-CBC' to --data-ciphe
rs or change --cipher 'AES-128-CBC' to --data-ciphers-fallback 'AES-128-CBC'
 to silence this warning.
2021-12-04 08:06:56 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO]
[LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021
2021-12-04 08:06:56 library versions: OpenSSL 1.1.1l  24 Aug 2021, LZO 2.10
Enter Auth Username: freeopenvpn
🔐 Enter Auth Password: *********
2021-12-04 08:07:36 Outgoing Control Channel Authentication: Using 160 bit m
essage hash 'SHA1' for HMAC authentication
2021-12-04 08:07:36 Incoming Control Channel Authentication: Using 160 bit m
essage hash 'SHA1' for HMAC authentication
2021-12-04 08:07:36 TCP/UDP: Preserving recently used remote address: [AF_IN
ET]131.255.239.38:3128
2021-12-04 08:07:36 Attempting to establish TCP connection with [AF_INET]131
.255.239.38:3128 [nonblock]
2021-12-04 08:07:41 TCP: connect to [AF_INET]131.255.239.38:3128 failed: Con
nection timed out
2021-12-04 08:07:41 SIGUSR1[connection failed(soft),init_instance] received,
 process restarting
2021-12-04 08:07:46 Outgoing Control Channel Authentication: Using 160 bit m
essage hash 'SHA1' for HMAC authentication
2021-12-04 08:07:46 Incoming Control Channel Authentication: Using 160 bit m
essage hash 'SHA1' for HMAC authentication
2021-12-04 08:07:46 TCP/UDP: Preserving recently used remote address: [AF_IN
ET]131.255.239.38:3128
2021-12-04 08:07:46 Attempting to establish TCP connection with [AF_INET]131
.255.239.38:3128 [nonblock]
2021-12-04 08:07:46 TCP connection established with [AF_INET]131.255.239.38:
3128
2021-12-04 08:07:46 Send to HTTP proxy: 'CONNECT us1.freeopenvpn.org:443 HTT
P/1.0'
```

```
2021-12-04 08:07:41 SIGUSR1[connection failed(soft),init_instance] received,
 process restarting
2021-12-04 08:07:46 Outgoing Control Channel Authentication: Using 160 bit m
essage hash 'SHA1' for HMAC authentication
2021-12-04 08:07:46 Incoming Control Channel Authentication: Using 160 bit m
essage hash 'SHA1' for HMAC authentication
2021-12-04 08:07:46 TCP/UDP: Preserving recently used remote address: [AF_IN
ET]131.255.239.38:3128
2021-12-04 08:07:46 Attempting to establish TCP connection with [AF_INET]131
.255.239.38:3128 [nonblock]
2021-12-04 08:07:46 TCP connection established with [AF_INET]131.255.239.38:
3128
2021-12-04 08:07:46 Send to HTTP proxy: 'CONNECT us1.freeopenvpn.org:443 HTT
P/1.0'
2021-12-04 08:07:46 Send to HTTP proxy: 'Host: us1.freeopenvpn.org'
2021-12-04 08:07:48 HTTP proxy returned: 'HTTP/1.1 200 Connection establishe
d'
2021-12-04 08:07:50 TCP_CLIENT link local: (not bound)
2021-12-04 08:07:50 TCP_CLIENT link remote: [AF_INET]131.255.239.38:3128
2021-12-04 08:07:51 VERIFY OK: depth=1, O=5fa2b89021f9231b1afdb036, CN=5fa2b
89021f9231b1afdb043
2021-12-04 08:07:51 VERIFY KU OK
2021-12-04 08:07:51 Validating certificate extended key usage
2021-12-04 08:07:51 NOTE: --mute triggered...
2021-12-04 08:07:53 4 variation(s) on previous 3 message(s) suppressed by --
mute
2021-12-04 08:07:53 [5fa2b89521f9231b1afdb048] Peer Connection Initiated wit
h [AF_INET]131.255.239.38:3128
2021-12-04 08:07:55 Data Channel: using negotiated cipher 'AES-128-GCM'
2021-12-04 08:07:55 Outgoing Data Channel: Cipher 'AES-128-GCM' initialized
with 128 bit key
2021-12-04 08:07:55 Incoming Data Channel: Cipher 'AES-128-GCM' initialized
with 128 bit key
2021-12-04 08:07:55 TUN/TAP device tun1 opened
2021-12-04 08:07:55 net_iface_mtu_set: mtu 1500 for tun1
2021-12-04 08:07:55 net_iface_up: set tun1 up
2021-12-04 08:07:55 net_addr_v4_add: 192.168.231.2/24 dev tun1
2021-12-04 08:07:55 WARNING: this configuration may cache passwords in memor
y -- use the auth-nocache option to prevent this
2021-12-04 08:07:55 Initialization Sequence Completed
```

IP addrese before



IP addrese after



*Додайте сертифікат **CA mitmproxy** у список довірених на клієнті.*

Проаналізуйте трафік .

Приблизні кроки згідно документації сайту для встановлення CA mitmproxy такі

Встановлення кореневого/сертифікату ЦС

Маючи файл сертифіката ЦС `foo.crt`, виконайте такі дії, щоб встановити його в Ubuntu:

1. Створіть каталог для додаткових сертифікатів ЦС в `/usr/local/share/ca-certificates`:

   ```
   sudo mkdir /usr/local/share/ca-certificates/extra
   ```

2. Скопіюйте `.crt` файл CA в цей каталог:

   ```
   sudo cp foo.crt /usr/local/share/ca-certificates/extra/foo.crt
   ```

3. Нехай Ubuntu додати в `.crt` шлях файлу щодо `/usr/local/share/ca-certificates` до `/etc/ca-certificates.conf`:

   ```
   sudo dpkg-reconfigure ca-certificates
   ```

Щоб зробити це неінтерактивно, запустіть:

```
sudo update-ca-certificates
```

У випадку `.pem` файлу в Ubuntu, його потрібно спочатку конвертувати у `.crt` файл:

```
openssl x509 -in foo.pem -inform PEM -out foo.crt
```

Або `.cer` файл можна конвертувати у `.crt` файл:

```
openssl x509 -inform DER -in foo.cer -out foo.crt
```

Завантажуємо сертифікат з сайту вказаному на сторінці:

https://docs.mitmproxy.org/stable/concepts-certificates/

Додаємо сертифікат

https://manuals.gfi.com/en/kerio/connect/content/server-configuration/ssl-certificates/adding-trusted-root-certificates-to-the-server-1605.html

```
sudo cp ~/.mitmproxy/mitmproxy-ca-cert.cer /usr/local/share/ca-certificates/extra/mitmproxy-ca-cert.crt
```

```
andrew@asus-X505BP:~/Downloads$ sudo update-ca-certificates
Updating certificates in /etc/ssl/certs...
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...

Adding debian:mitmproxy-ca-cert.pem
done.
done.
```

Перевіряємо зміни, дійсно в папці ~/ .mitmproxy/ находиться сертифікат

```
andrew@asus-X505BP:~/Downloads$ ll ~/.mitmproxy/
total 32
drwxrwxr-x  2 andrew andrew 4096 грд  4 17:17 ./
drwxr-xr-x 31 andrew andrew 4096 грд 11 01:52 ../
-rw-rw-r--  1 andrew andrew 1318 грд  4 17:17 mitmproxy-ca-cert.cer
-rw-rw-r--  1 andrew andrew 1140 грд  4 17:17 mitmproxy-ca-cert.p12
-rw-rw-r--  1 andrew andrew 1318 грд  4 17:17 mitmproxy-ca-cert.pem
-rw-rw-r--  1 andrew andrew 2529 грд  4 17:17 mitmproxy-ca.p12
-rw-rw-r--  1 andrew andrew 3026 грд  4 17:17 mitmproxy-ca.pem
-rw-rw-r--  1 andrew andrew  770 грд  4 17:17 mitmproxy-dhparam.pem
```

Оновлюємо сертифікати

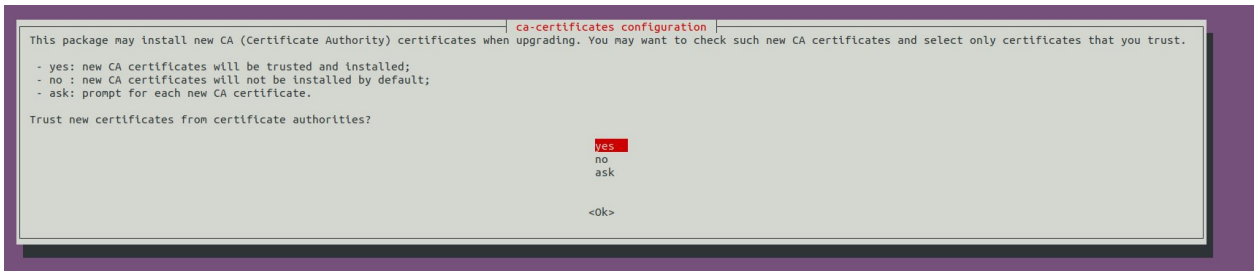
```
andrew@asus-X505BP:~/Desktop$  sudo update-ca-certificates --fresh
[sudo] password for andrew:
Sorry, try again.
[sudo] password for andrew:
Clearing symlinks in /etc/ssl/certs...
done.
Updating certificates in /etc/ssl/certs...
129 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...

Replacing debian:ACCVRAIZ1.pem
Replacing debian:AC_RAIZ_FNMT-RCM.pem
Replacing debian:Actalis_Authentication_Root_CA.pem
Replacing debian:AffirmTrust_Commercial.pem
Replacing debian:AffirmTrust_Networking.pem
Replacing debian:AffirmTrust_Premium.pem
Replacing debian:AffirmTrust_Premium_ECC.pem
Replacing debian:Amazon_Root_CA_1.pem
Replacing debian:Amazon_Root_CA_2.pem
Replacing debian:Amazon_Root_CA_3.pem
Replacing debian:Amazon_Root_CA_4.pem
Replacing debian:Atos_TrustedRoot_2011.pem
Replacing debian:Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.pem
Replacing debian:Baltimore_CyberTrust_Root.pem
Replacing debian:Buypass_Class_2_Root_CA.pem
Replacing debian:Buypass_Class_3_Root_CA.pem
Replacing debian:CA_Disig_Root_R2.pem
Replacing debian:CFCA_EV_ROOT.pem
Replacing debian:COMODO_Certification_Authority.pem
Replacing debian:COMODO_ECC_Certification_Authority.pem
Replacing debian:COMODO_RSA_Certification_Authority.pem
Replacing debian:Certigna.pem
Replacing debian:Certum_Trusted_Network_CA.pem
Replacing debian:Certum_Trusted_Network_CA_2.pem
Replacing debian:Chambers_of_Commerce_Root_-_2008.pem
Replacing debian:Comodo_AAA_Services_root.pem
Replacing debian:Cybertrust_Global_Root.pem
Replacing debian:D-TRUST_Root_Class_3_CA_2_2009.pem
Replacing debian:D-TRUST_Root_Class_3_CA_2_EV_2009.pem
Replacing debian:DigiCert_Assured_ID_Root_CA.pem
Replacing debian:DigiCert_Assured_ID_Root_G2.pem
Replacing debian:DigiCert_Assured_ID_Root_G3.pem
Replacing debian:DigiCert_Global_Root_CA.pem
Replacing debian:DigiCert_Global_Root_G2.pem
Replacing debian:DigiCert_Global_Root_G3.pem
Replacing debian:DigiCert_High_Assurance_EV_Root_CA.pem
Replacing debian:DigiCert_Trusted_Root_G4.pem
Replacing debian:E-Tugra_Certification_Authority.pem
Replacing debian:EC-ACC.pem
Replacing debian:Entrust.net_Premium_2048_Secure_Server_CA.pem
Replacing debian:Entrust_Root_Certification_Authority.pem
Replacing debian:Entrust.net_Premium_2048_Secure_Server_CA.pem
Replacing debian:Entrust_Root_Certification_Authority.pem
Replacing debian:Entrust_Root_Certification_Authority_-_EC1.pem
Replacing debian:Entrust_Root_Certification_Authority_-_G2.pem
Replacing debian:GDCA_TrustAUTH_R5_ROOT.pem
Replacing debian:GeoTrust_Primary_Certification_Authority_-_G2.pem
Replacing debian:GlobalSign_ECC_Root_CA_-_R4.pem
Replacing debian:GlobalSign_ECC_Root_CA_-_R5.pem
Replacing debian:GlobalSign_Root_CA.pem
Replacing debian:GlobalSign_Root_CA_-_R2.pem
Replacing debian:GlobalSign_Root_CA_-_R3.pem
Replacing debian:GlobalSign_Root_CA_-_R6.pem
Replacing debian:Global_Chambersign_Root_-_2008.pem
Replacing debian:Go_Daddy_Class_2_CA.pem
Replacing debian:Go_Daddy_Root_Certificate_Authority_-_G2.pem
Replacing debian:Hellenic_Academic_and_Research_Institutions_ECC_RootCA_2015.pem
Replacing debian:Hellenic_Academic_and_Research_Institutions_RootCA_2011.pem
Replacing debian:Hellenic_Academic_and_Research_Institutions_RootCA_2015.pem
Replacing debian:Hongkong_Post_Root_CA_1.pem
Replacing debian:ISRG_Root_X1.pem
Replacing debian:IdenTrust_Commercial_Root_CA_1.pem
Replacing debian:IdenTrust_Public_Sector_Root_CA_1.pem
Replacing debian:Izenpe.com.pem
Replacing debian:Microsec_e-Szigno_Root_CA_2009.pem
Replacing debian:NetLock_Arany_=Class_Gold=_Főtanúsítvány.pem
Replacing debian:Network_Solutions_Certificate_Authority.pem
Replacing debian:OISTE_WISeKey_Global_Root_GB_CA.pem
Replacing debian:OISTE_WISeKey_Global_Root_GC_CA.pem
Replacing debian:QuoVadis_Root_CA.pem
Replacing debian:QuoVadis_Root_CA_1_G3.pem
Replacing debian:QuoVadis_Root_CA_2.pem
Replacing debian:QuoVadis_Root_CA_2_G3.pem
Replacing debian:QuoVadis_Root_CA_3.pem
Replacing debian:QuoVadis_Root_CA_3_G3.pem
Replacing debian:SSL.com_EV_Root_Certification_Authority_ECC.pem
Replacing debian:SSL.com_EV_Root_Certification_Authority_RSA_R2.pem
Replacing debian:SSL.com_Root_Certification_Authority_ECC.pem
Replacing debian:SSL.com_Root_Certification_Authority_RSA.pem
Replacing debian:SZAFIR_ROOT_CA2.pem
Replacing debian:SecureSign_RootCA11.pem
Replacing debian:SecureTrust_CA.pem
Replacing debian:Secure_Global_CA.pem
Replacing debian:Security_Communication_RootCA2.pem
Replacing debian:Security_Communication_Root_CA.pem
Replacing debian:Sonera_Class_2_Root_CA.pem
Replacing debian:Staat_der_Nederlanden_EV_Root_CA.pem
Replacing debian:Staat_der_Nederlanden_Root_CA_-_G3.pem
Replacing debian:Starfield_Class_2_CA.pem
Replacing debian:Starfield_Root_Certificate_Authority_-_G2.pem
Replacing debian:Starfield_Services_Root_Certificate_Authority_-_G2.pem
Replacing debian:SwissSign_Gold_CA_-_G2.pem
```

```
Replacing debian:Starfield_Services_Root_Certificate_Authority_-_G2.pem
Replacing debian:SwissSign_Gold_CA_-_G2.pem
Replacing debian:SwissSign_Silver_CA_-_G2.pem
Replacing debian:T-TeleSec_GlobalRoot_Class_2.pem
Replacing debian:T-TeleSec_GlobalRoot_Class_3.pem
Replacing debian:TUBITAK_Kamu_SM_SSL_Kok_Sertifikasi_-_Surum_1.pem
Replacing debian:TWCA_Global_Root_CA.pem
Replacing debian:TWCA_Root_Certification_Authority.pem
Replacing debian:TeliaSonera_Root_CA_v1.pem
Replacing debian:TrustCor_ECA-1.pem
Replacing debian:TrustCor_RootCert_CA-1.pem
Replacing debian:TrustCor_RootCert_CA-2.pem
Replacing debian:Trustis_FPS_Root_CA.pem
Replacing debian:USERTrust_ECC_Certification_Authority.pem
Replacing debian:USERTrust_RSA_Certification_Authority.pem
Replacing debian:VeriSign_Universal_Root_Certification_Authority.pem
Replacing debian:XRamp_Global_CA_Root.pem
Replacing debian:certSIGN_ROOT_CA.pem
Replacing debian:ePKI_Root_Certification_Authority.pem
Replacing debian:Certigna_Root_CA.pem
Replacing debian:Entrust_Root_Certification_Authority_-_G4.pem
Replacing debian:GTS_Root_R1.pem
Replacing debian:GTS_Root_R2.pem
Replacing debian:GTS_Root_R3.pem
Replacing debian:GTS_Root_R4.pem
Replacing debian:Hongkong_Post_Root_CA_3.pem
Replacing debian:Microsoft_ECC_Root_Certificate_Authority_2017.pem
Replacing debian:Microsoft_RSA_Root_Certificate_Authority_2017.pem
Replacing debian:NAVER_Global_Root_Certification_Authority.pem
Replacing debian:Trustwave_Global_Certification_Authority.pem
Replacing debian:Trustwave_Global_ECC_P256_Certification_Authority.pem
Replacing debian:Trustwave_Global_ECC_P384_Certification_Authority.pem
Replacing debian:UCA_Extended_Validation_Root.pem
Replacing debian:UCA_Global_G2_Root.pem
Replacing debian:certSIGN_Root_CA_G2.pem
Replacing debian:e-Szigno_Root_CA_2017.pem
Replacing debian:emSign_ECC_Root_CA_-_C3.pem
Replacing debian:emSign_ECC_Root_CA_-_G3.pem
Replacing debian:emSign_Root_CA_-_C1.pem
Replacing debian:emSign_Root_CA_-_G1.pem
Replacing debian:mitmproxy-ca-cert.pem
done.
done.
```

```
andrew@asus-X505BP:/usr/local/share/ca-certificates/extra$ sudo dpkg-reconfigure ca-certificates
[sudo] password for andrew:
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Processing triggers for ca-certificates (20210119~20.04.2) ...
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...

done.
done.
```

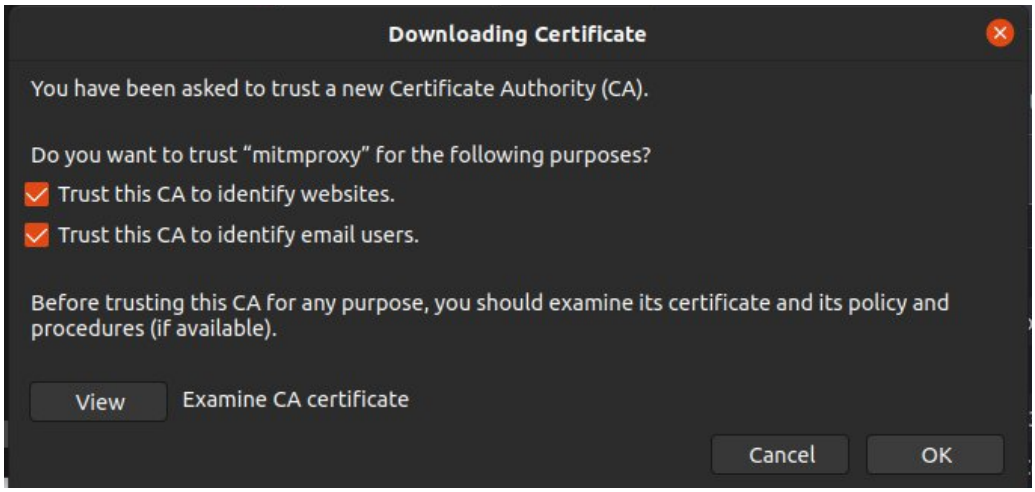


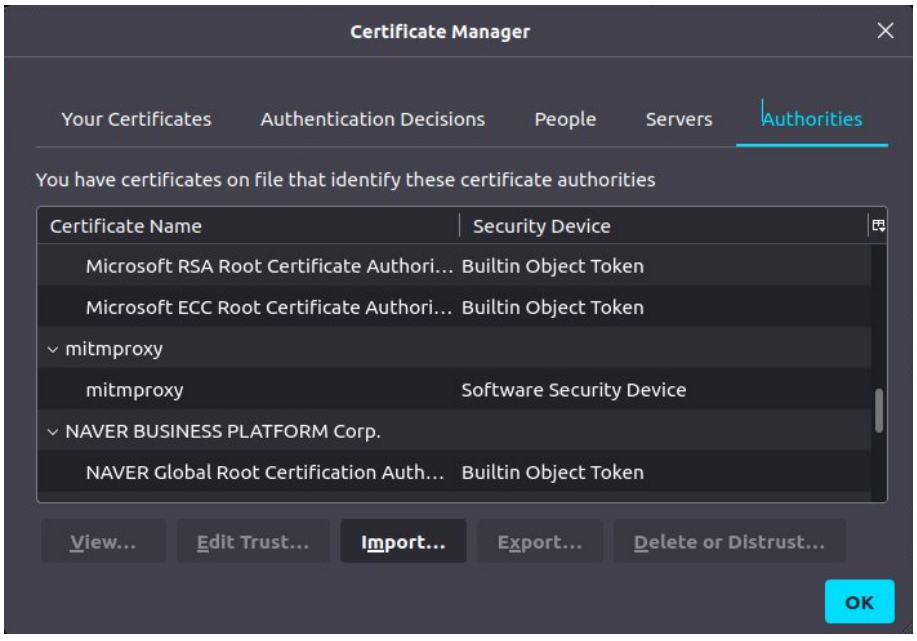
```
andrew@asus-X505BP:/usr/local/share/ca-certificates/extra$ cat /etc/ca-certificates.conf
# This file lists certificates that you wish to use or to ignore to be
# installed in /etc/ssl/certs.
# update-ca-certificates(8) will update /etc/ssl/certs by reading this file.
#
# This is autogenerated by dpkg-reconfigure ca-certificates.
# Certificates should be installed under /usr/share/ca-certificates
# and files with extension '.crt' is recognized as available certs.
#
# line begins with # is comment.
# line begins with ! is certificate filename to be deselected.
#
mozilla/ACCVRAIZ1.crt
mozilla/AC_RAIZ_FNMT-RCM.crt
mozilla/Actalis_Authentication_Root_CA.crt
!mozilla/AddTrust_External_Root.crt
mozilla/AffirmTrust_Commercial.crt
mozilla/AffirmTrust_Networking.crt
mozilla/AffirmTrust_Premium.crt
mozilla/AffirmTrust_Premium_ECC.crt
mozilla/Amazon_Root_CA_1.crt
mozilla/Amazon_Root_CA_2.crt
mozilla/Amazon_Root_CA_3.crt
mozilla/Amazon_Root_CA_4.crt
mozilla/Atos_TrustedRoot_2011.crt
```

Все виконувалося згідно інструкцій офіційного сайту, котрий зсилався на інший сайт:

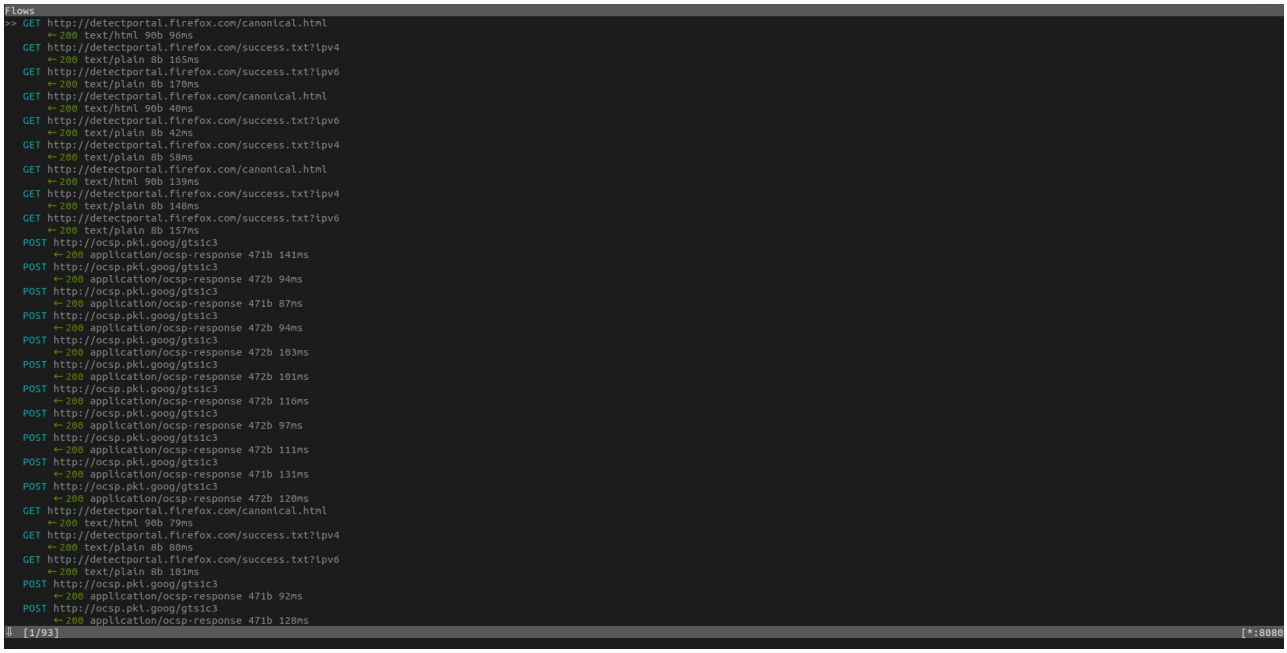
https://askubuntu.com/questions/73287/how-do-i-install-a-root-certificate/94861#94861

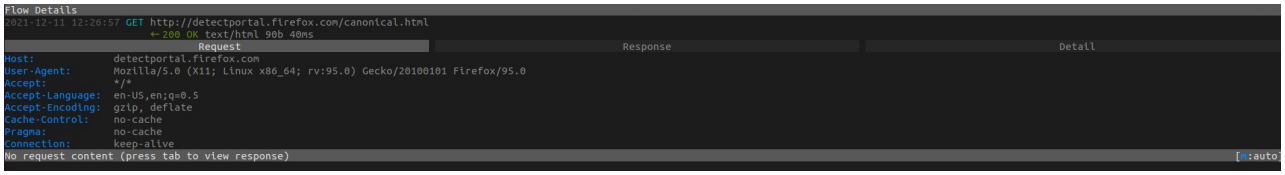
Додаємо сертифікат mitmproxy в Muzilla Firefox

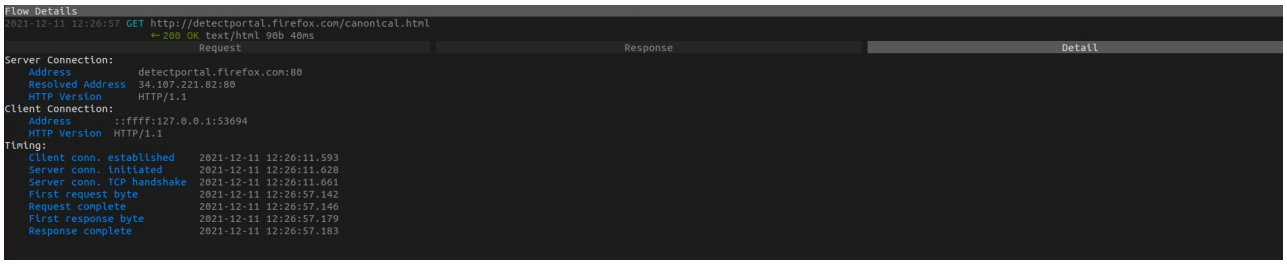




Тепер весь трафік проходить через mitproxy і ми можемо аналізувати перехоплені пакети







Якщо перейти по HTTP посиланню mitmproxy, або вводити IP адрес довільний в лінії пошуку теж запит надсилається: