27.11.24 – add some materials and translations

tags - Reverse engineering, osint, network protocols

**12.11.2024**

E88 Pro

WiFi

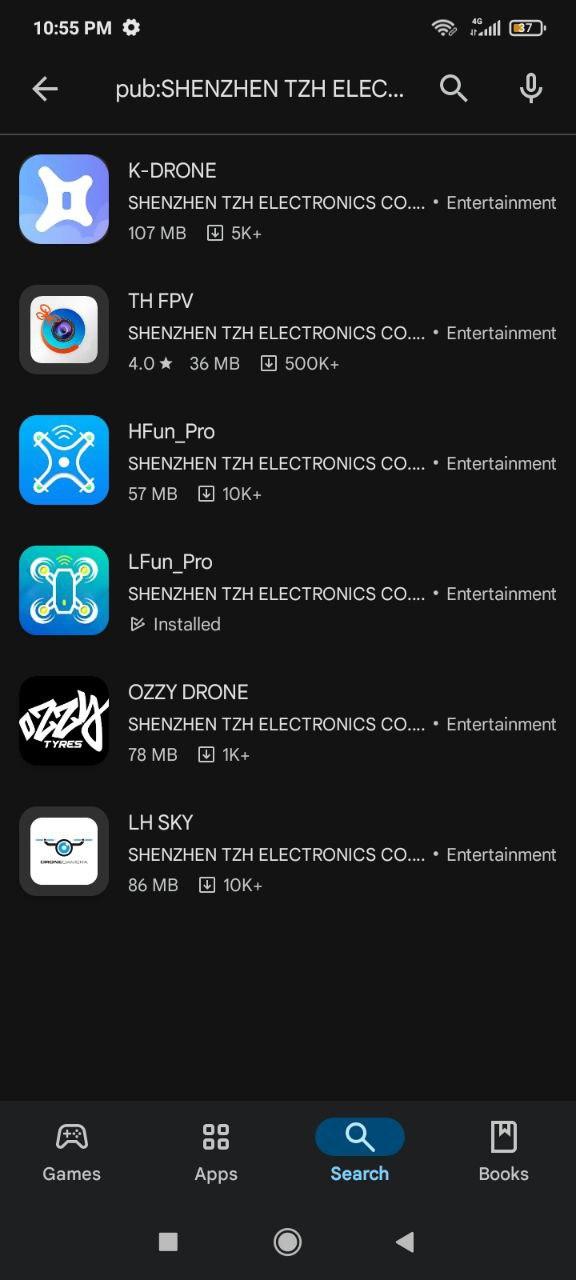
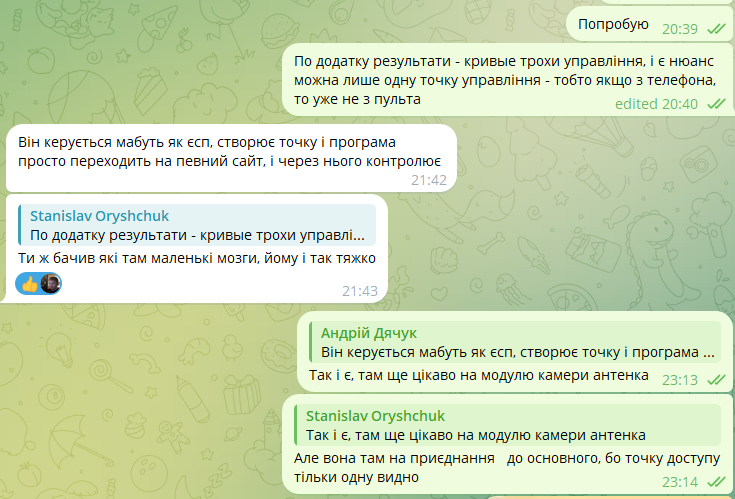
2 cams

<https://github.com/c0nr3f/E88-Pro-Python>

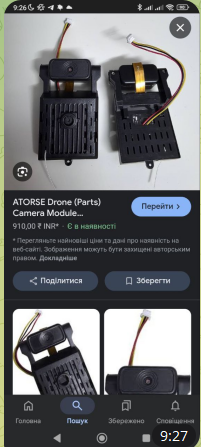
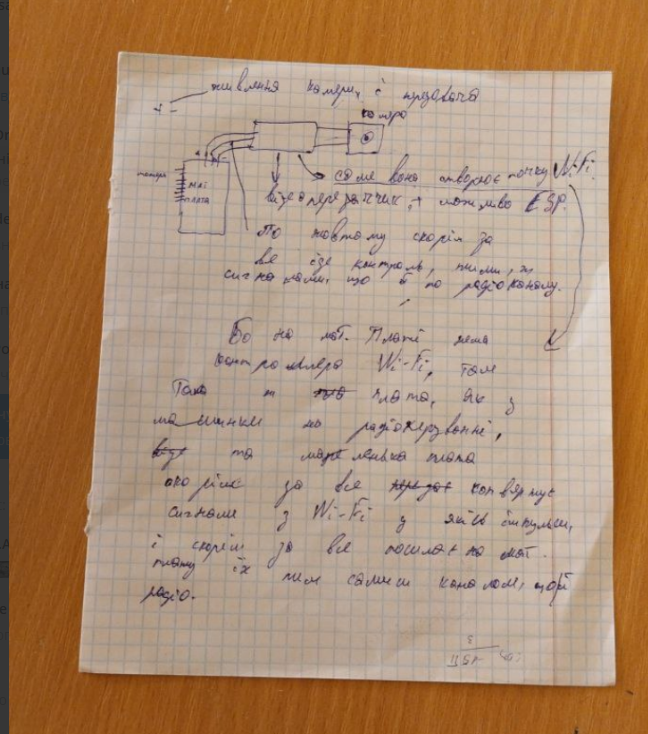
AP WIFI\_8K\_WC4CAF8

Norootfirewall - firewall, help watch app’s traffic

WiFi Cam

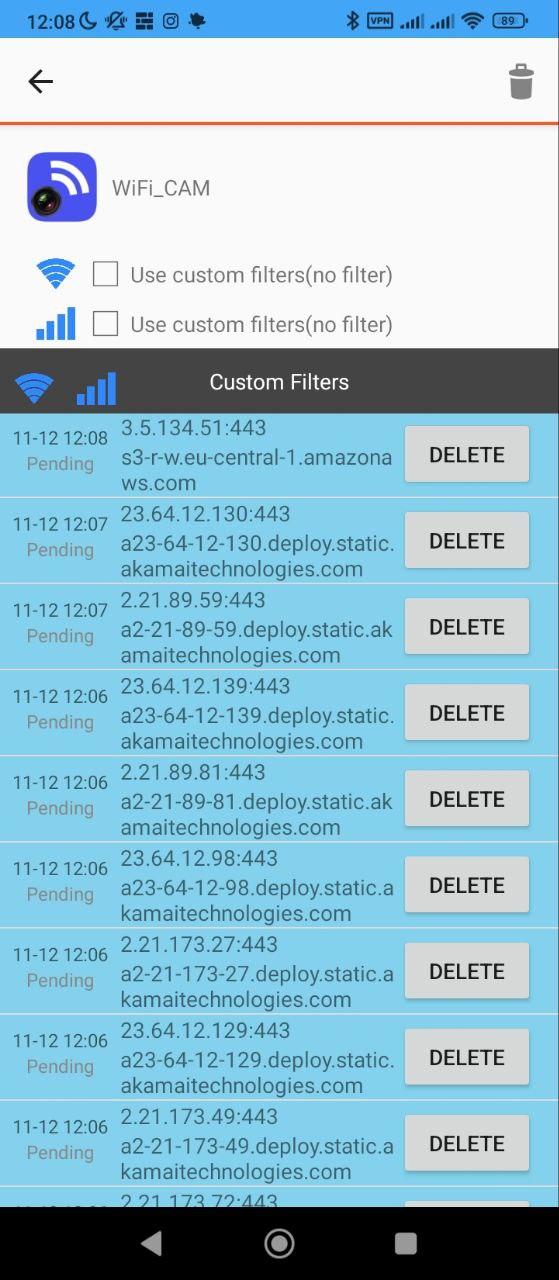
] LFun\_Pro

According to the application, the results are slightly crooked control, and there is a nuance that you can only control one point - that is, if from the phone, then not from the remote control

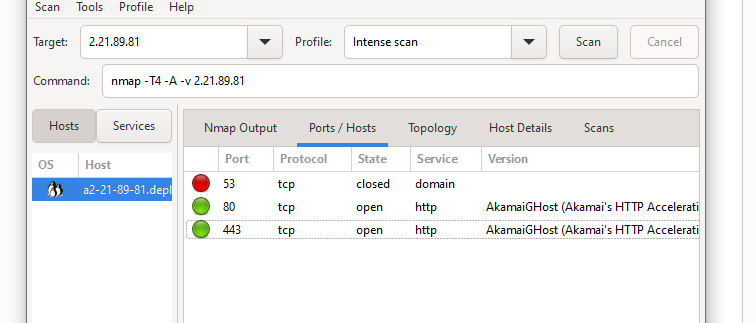
 Scheme by Andriy

Andriy Dyachuk, [11/11/2024 9:29 AM] You can try to control the drone in a straight line by reading the signals using an oscilloscope, they can even be sent by an Arduino board //translated, probably first motivation of this project

Andriy: "These are all the addresses to which it breaks after connecting to a point with a name similar to a drone"



nmap 2.21.89.81

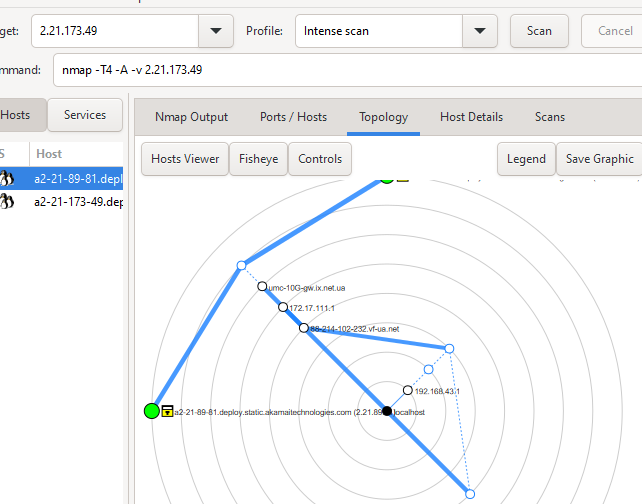
****

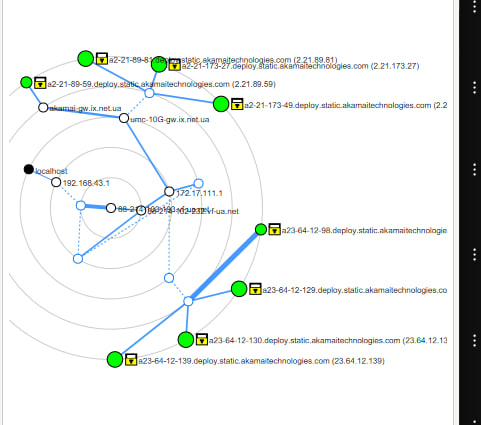
**Stanislav Oryshchuk, [12.11.2024 13:04]**

**гугл - Akamai Technologies, Inc. — американська компанія, яка спеціалізується на наданні послуг cloud-сервісів. це мабуть сервери на яких сам додаток хоститься**

**(**google - Akamai Technologies, Inc. — an American company that specializes in providing cloud services. these are probably the servers on which the application itself is hosted

**)**

****

****

**Stanislav Oryshchuk, [14.11.2024 13:56]**

**Трохи апдейтів:**

**- з відключеною камерою точки немає, тобто дійсно точка роздається там**

**- робив сканування Wireshark при підключенні до точки**

**Stanislav Oryshchuk, [14.11.2024 13:58]**

**По іп в сновному фігурують 192.168.4.101**

**192.168.4.153.**

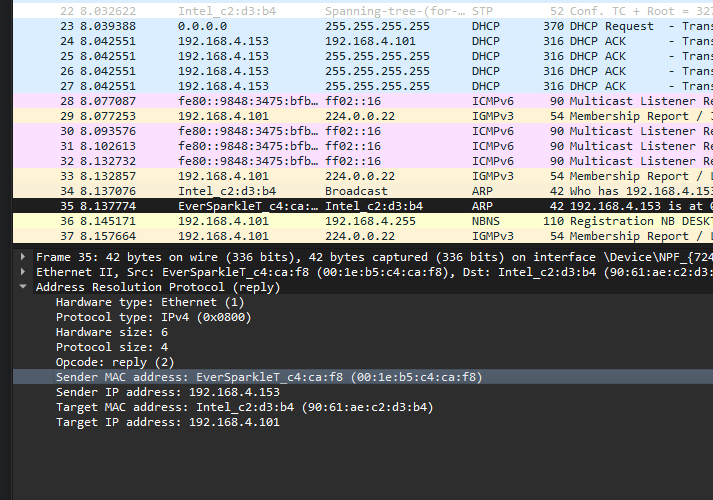
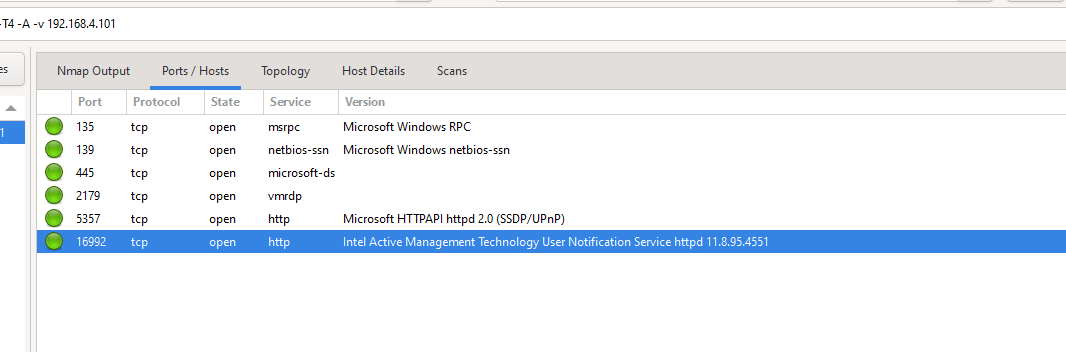
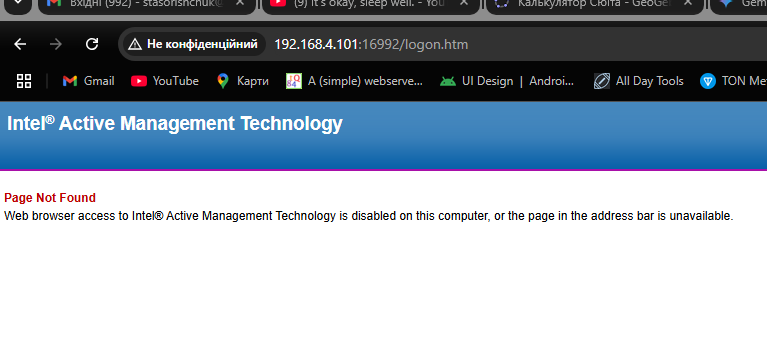
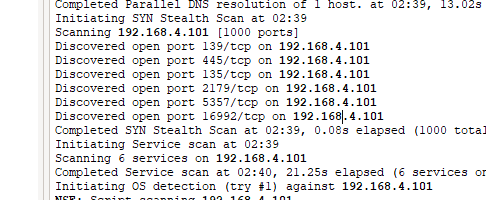
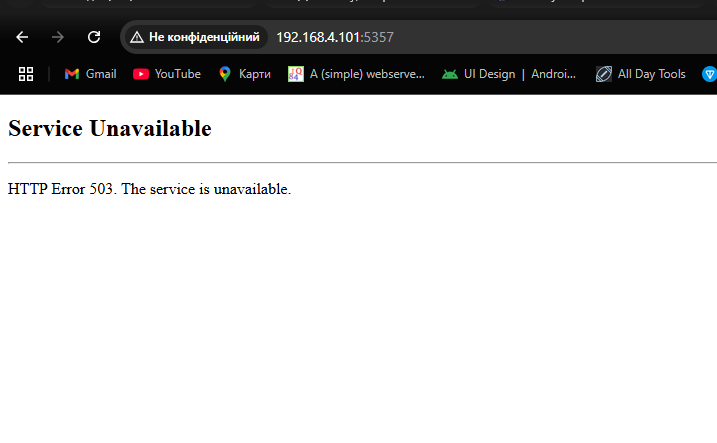
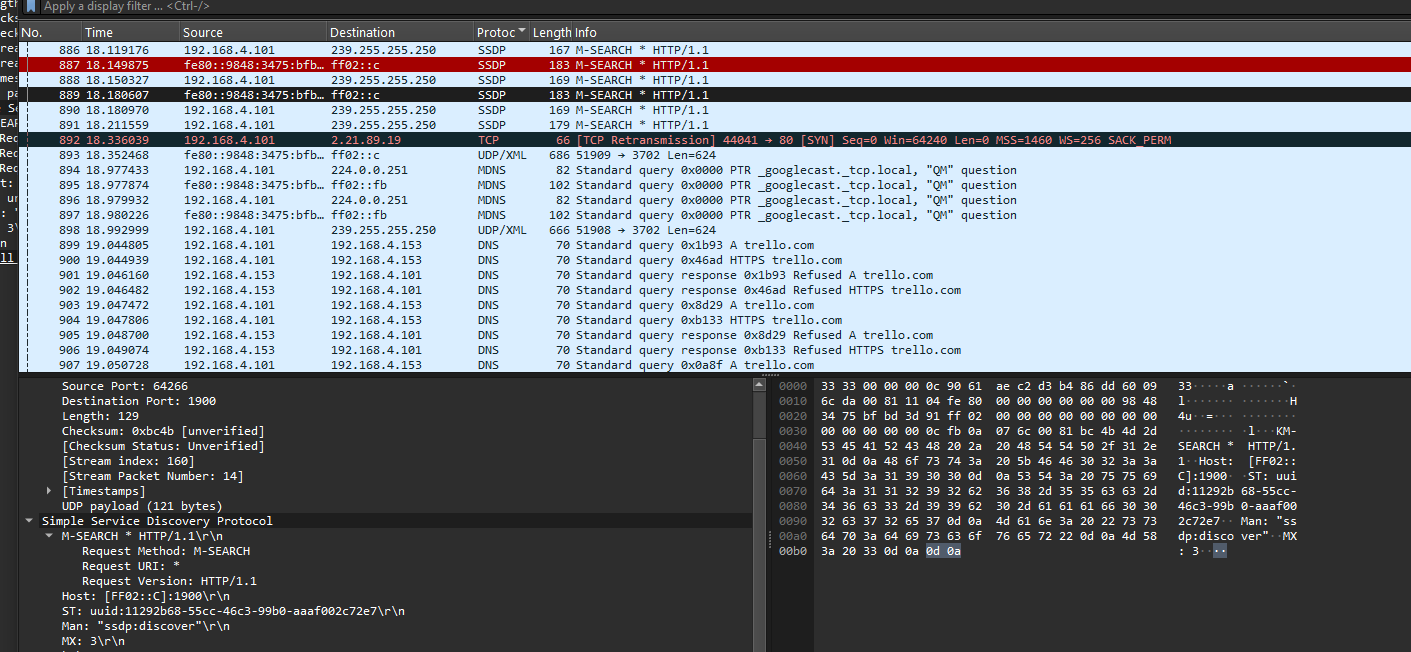
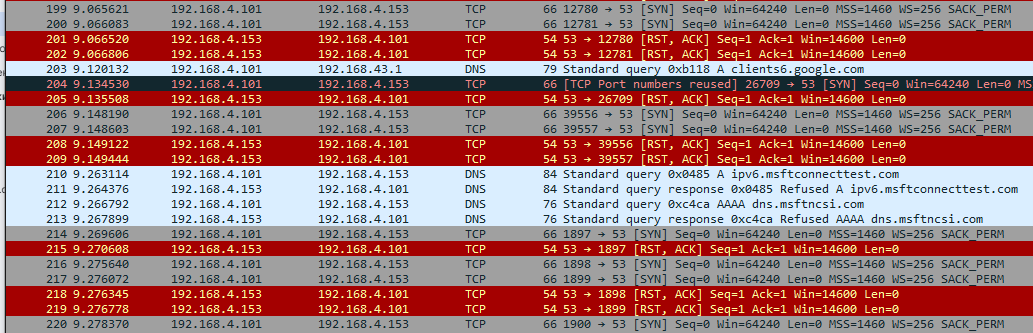
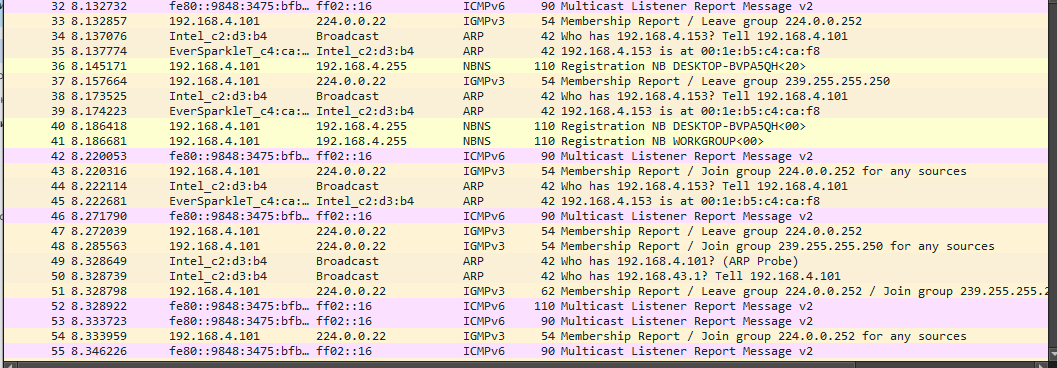
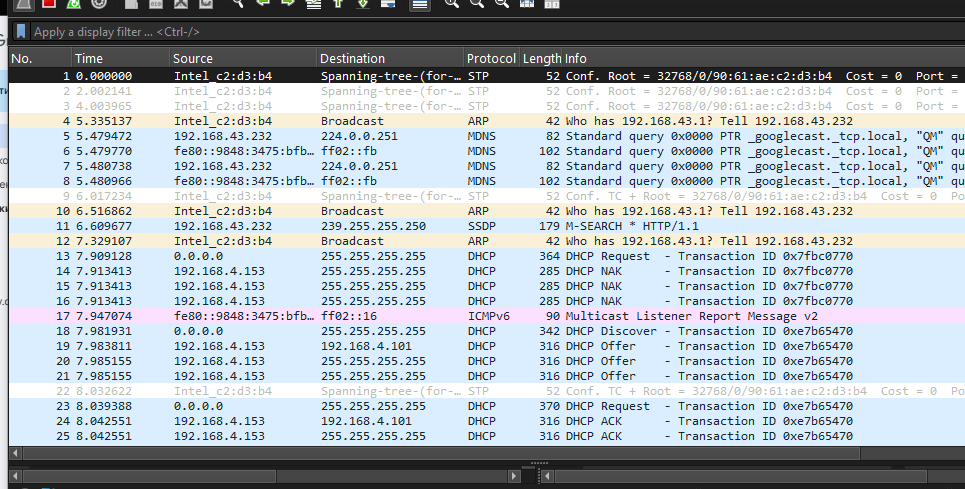
**Але якщо вводити їх в браузері, трохи перебираючи порти - нічого немає. І це походу просто локальна адреса ноута і самої точки**

**Stanislav Oryshchuk, [14.11.2024 13:59]**

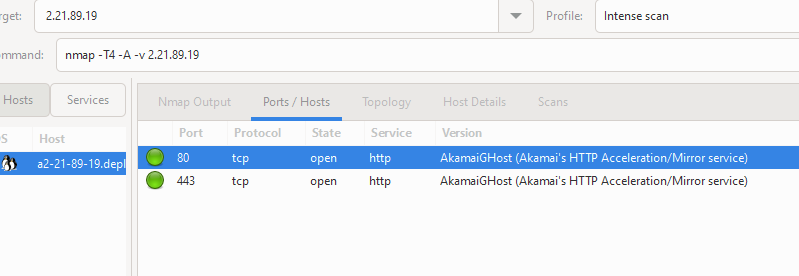
**В деяких пакетах як відправник значиться EverSparkleT\_c4:ca:f8, а то назва китайської компанії, ймовірно виробник модуля**

**Stanislav Oryshchuk, [14.11.2024 14:00]**

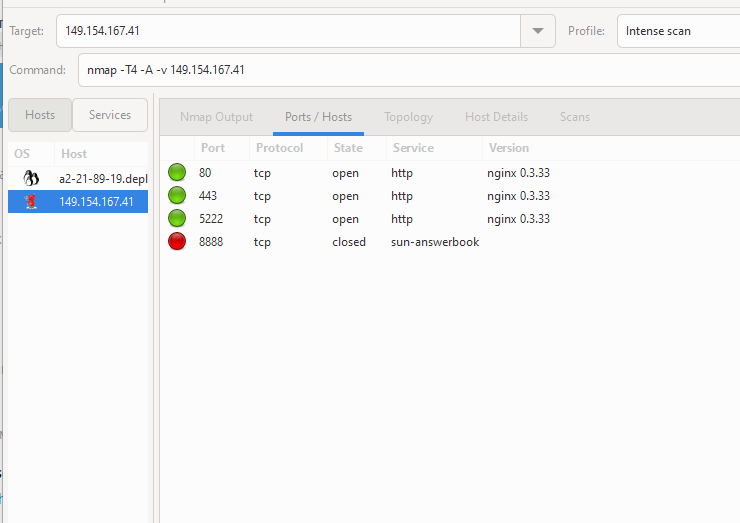
**Там ще були інші, але то також і ті що просто в той час у мене були відкриті вкладки**

****

**уже тільки зараз скидаючи скрін побачив TCP на 2.21.89.19 - подібні зустрічалися раніше через файрвол**

****

****

****

## Sun Answerbook server, or more commonly an alternative [HTTP](https://whatportis.com/ports/80_hypertext-transfer-protocol-http) port

**Sun AnswerBook Protocol is a Sun Microsystems proprietary protocol used to access Sun's online technical support database, known as AnswerBook.**

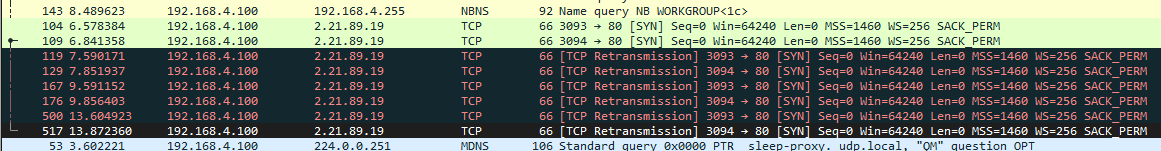
**AnswerBook was first introduced in 1989 as a way for Sun customers to access technical support information online. The original AnswerBook was a text-based system, and was later replaced with a graphical interface.**

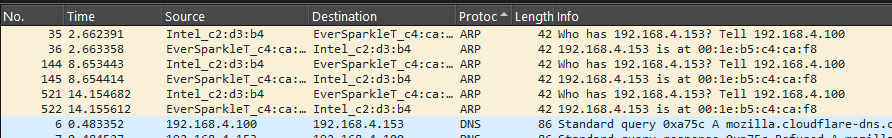
**AnswerBook**

[**https://whatportis.com/ports/8888\_sun-answerbook-dwhttpd-server-deprecated-by-docssuncom**](https://whatportis.com/ports/8888_sun-answerbook-dwhttpd-server-deprecated-by-docssuncom)

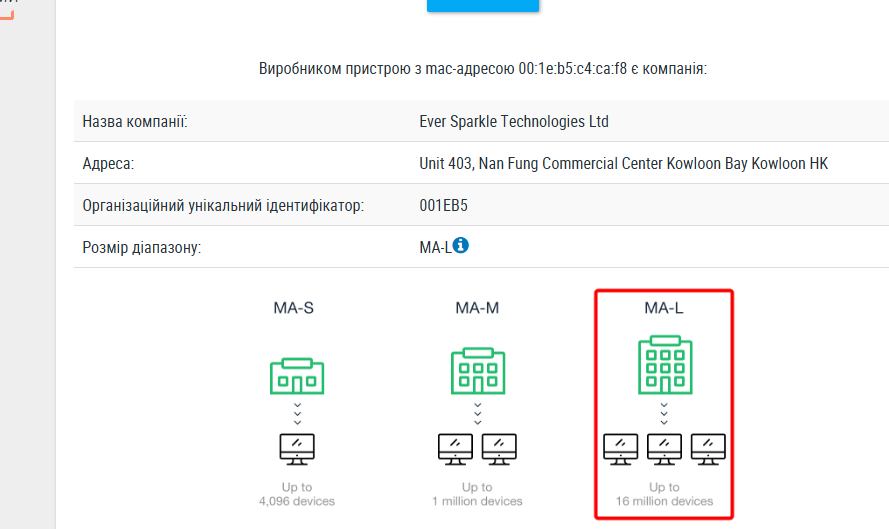
[**https://whatportis.com/ports**](https://whatportis.com/ports) **+++ collection of tools**

**2**

****

****

**00:1e:b5:c4:ca:f8**

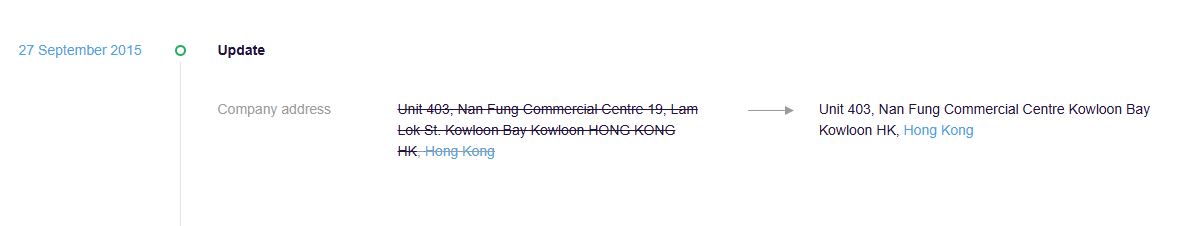
****

**OUI 00:1E:B5**

#### **What is an Organizationally Unique Identifier (OUI)?**

**An OUI is a 24-bit globally unique assigned number. An OUI is assigned with a MA-L identifier block and is referenced by various standards. It can be used to identify an organization or company**

****

****

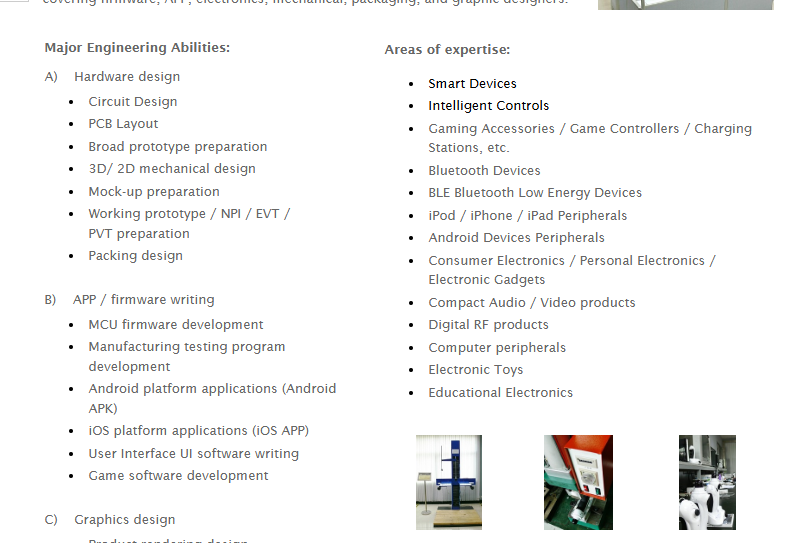
**Nan Fung Commercial Centre 南豐商業中心**

**Address: 19 Lam Lok Street, Kowloon Bay, Kwun Tong District, Kowloon**

[**https://www.ev-sparkle.com/**](https://www.ev-sparkle.com/)

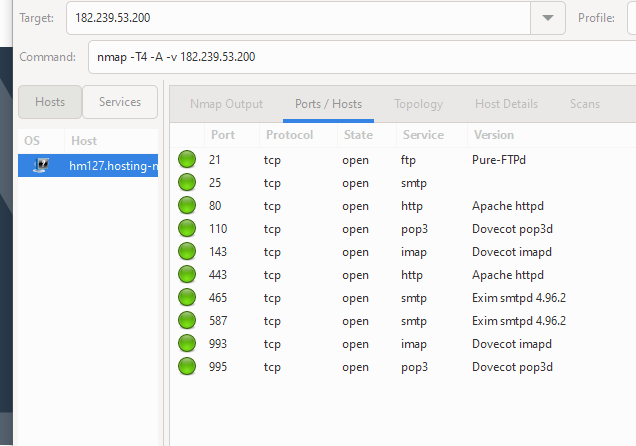
* **Surface Mount Technology (SMT) & Ball Grid Array (BGA)**
* **Through Hole Assembly**
* **Coating and Potting**
* **Box Build Assembly / Complete Unit Assembly**
* **In-circuit Testing, Functional Testing, and System Testing**

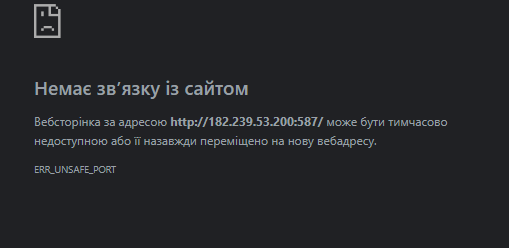
****

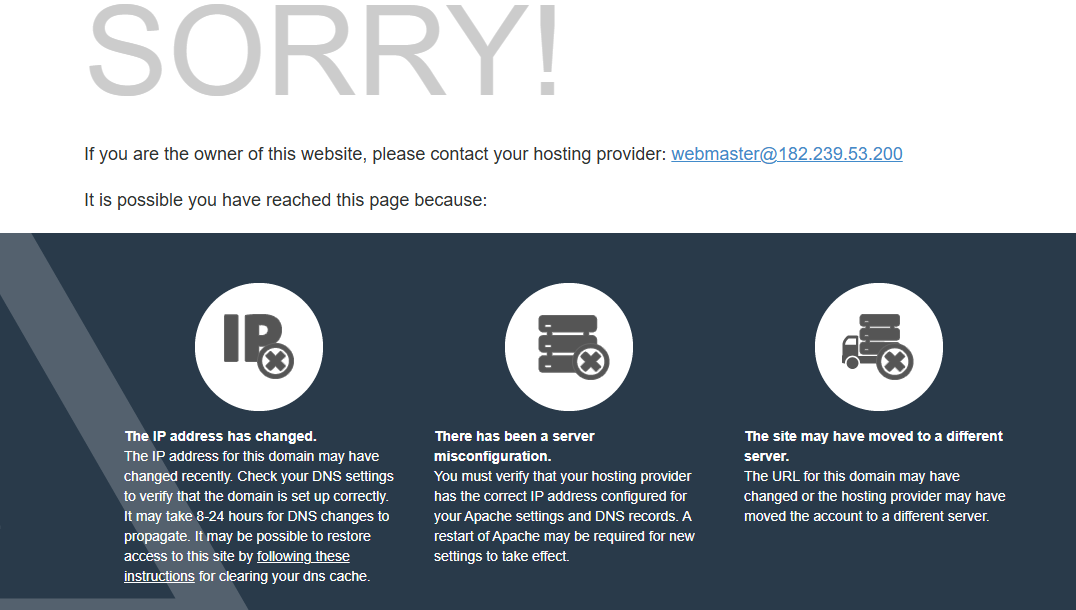
****

**//co work ++++++++++**

**IP address for** [**https://www.ev-sparkle.com/**](https://www.ev-sparkle.com/) **is 182.239.53.200 hosted by Access Solutions Limited HK - noth -**

****

**on almost all**

**on 80**

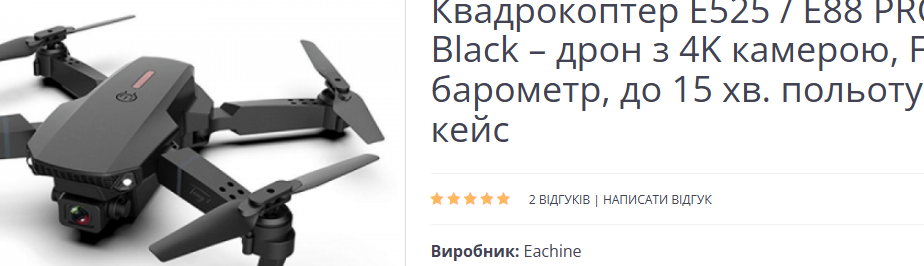
**Dovecot is an open source IMAP and POP3 email server for Linux/UNIX-like systems** [**https://doc.dovecot.org/2.3/**](https://doc.dovecot.org/2.3/)

[**https://www.exploit-db.com/exploits/5257**](https://www.exploit-db.com/exploits/5257)

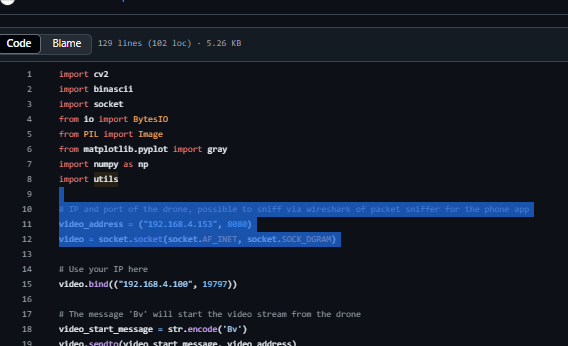
[**https://www.ev-sparkle.com/products.html**](https://www.ev-sparkle.com/products.html)

****

**…………….**

****

[**https://www.eachine.com/**](https://www.eachine.com/)

****

**waiming so**

**Senior Engineering Manager at Ever Sparkle Technologies Ltd.**

**The University of Hong Kong Ever Sparkle Technologies Ltd.**