

**Hispa**sec]



# DOCUMENTACIÓN

**Writeup UAM**

OSINT  
Julio 2023

Informe técnico

---

# Cláusula legal

La información contenida en este documento es de carácter confidencial y va dirigida de manera exclusiva a su destinatario, quedando sujeta al secreto profesional. Queda prohibida por Ley la distribución, divulgación, copia o reproducción del contenido de este documento sin la correspondiente autorización por parte de su autor.

# Documentación

## Informe técnico

### Índice

<b>1. Datos del reto.</b>	<b>3</b>
1.1. Especificaciones técnicas.	3
<b>2. Proceso de resolución del reto.</b>	<b>4</b>
2.1. Siguiendo las pistas (Flag 1)	4
2.1.1. Enumeración de los usuarios en las redes sociales	4
2.1.2. Enumeración de la cuenta de twitter	5
2.1.3. Acceso al servidor de discord	6
2.2. Siguiendo las pistas (Flag 2)	8
2.2.1. Localizador de vuelo	8
2.2.2. Localizador de MAC	10

# 1. Datos del reto.

## 1.1. Especificaciones técnicas.

A continuación se detalla el alcance y el conjunto de especificaciones del reto, así como las normativas de aplicación.

Alcance	
Activo/s:	OSINT
Categoría:	OSINT
Fecha de inicio:	30/06/2023.
Fecha de fin:	14/07/2023.
Cumplimiento normativo:	Las contraseñas y otra información sobre los usuarios no son almacenadas en cumplimiento con la ley de protección de datos (Reglamento General de Protección de Datos, RGPD). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

## 2. Proceso de resolución del reto.

A continuación se detalla la manera intencionada en la que se espera que el usuario resuelva el reto. Cada entrada viene encabezada por la descripción detallada del punto en concreto, acompañado de los pasos a seguir para reproducirlo.

### 2.1. Siguiendo las pistas (Flag 1)

Buenas a todos los que me estén leyendo, soy , investigador privado; si habéis conseguido leer este mensaje es porque sois bastante buenos investigadores y necesito vuestra ayuda, llevo bastante tiempo detrás de un ciberdelincuente que se hace llamar "Definitif Juacker", se rumorea por la deep web que su contacto más fiable se hace llamar "Disimulated\_Men" pero no lo encontré; buena suerte!!

Flag: UAM{md5}

#### 2.1.1. Enumeración de los usuarios en las redes sociales

##### Descripción

Se buscan los usuarios en diferentes redes sociales para sacar más información sobre ellos.

##### Evidencias

Se comprueba que en **Twitter** existe la cuenta de **Disimulated\_Men** la cual tiene muchos tweets pero nada relevante aparentemente.



## 2.1.2. Enumeración de la cuenta de twitter

### Descripción

Enumerar totalmente la cuenta de **Twitter** localizada para sacar más información de la que aparentemente hay.

### Evidencias

En las publicaciones, likes, etc no hay nada; al buscar su nombre en **Twitter** sin acceder al perfil encontraremos un perfil que cuadra bastante con uno de los *nicks* mencionados en la descripción del reto.



Además de esta, hay otra forma de encontrarle y es mirar los seguidores del perfil de **Disimulated Men**.



### 2.1.3. Acceso al servidor de discord

#### Descripción

Enumerar totalmente la cuenta de twitter localizada para conseguir entrar a un servidor de discord.

#### Evidencias

Al entrar en el nuevo perfil encontrado, podemos ver un enlace a un **pastebin**, lo abrimos y nos damos cuenta de que parece algo en arte **ASCII**; al verlo en **RAW**, veremos que es un link de invitación de discord.




A screenshot of a Pastebin page. At the top, it says "Nothing important" in a large, bold font. Below this, there's a header bar with social media links (Facebook, Twitter), a date "JUN 1ST, 2023 (EDITED)", a view count "58", and a comment count "0". There's also a "NEVER" button and an "ADD COMMENT" button. The main content area shows a message: "Not a member of Pastebin yet? [Sign Up](#). it unlocks many cool features!". Below this, there's a text editor interface with a toolbar showing "text", "1.08 KB", "None", and "0" comments. The text area contains a large block of ASCII art, which is a complex drawing made of characters like underscores, pipes, and slashes, forming a landscape or abstract shape. The ASCII art is displayed on a grid with line numbers 1 through 8 visible on the left.

CN(C)C(=O)OC(=O)c1ccc(cc1)C(=O)OC(=O)CN(C)C

Al acceder al servidor nos hablará un bot el cuál nos dará la primera flag y unas indicaciones:

4 de julio de 2023

 **Agenda personal de Juacker** BOT hoy a las 9:58  
UAN [REDACTED]

Bienvenido al servidor, puede que seas definitif juacker desde otro lugar; para realizar tu verificación introduce 1verify



## 2.2. Siguiendo las pistas (Flag 2)

¡Increíble! Tienes que tener un gran coeficiente intelectual, si no fuera autónomo te contrataría; ahora tengo que hacer varias cosas para otra investigación así que tendrás que arreglárselas solo... jaja... cuando encuentres algo me avisas, chao.

Flag: UAM{md5}

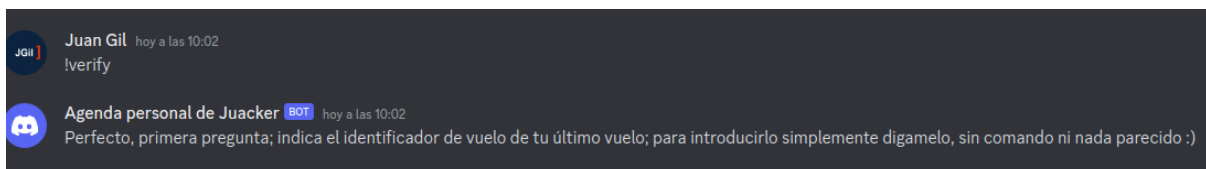
### 2.2.1. Localizador de vuelo

#### Descripción

Al introducir el comando que el bot nos dice nos pedirá un identificador de vuelo, para conseguirlo hay que volver a **Twitter** para saber hacia donde es el vuelo además de usar una herramienta para encontrarlo.

#### Evidencias

El bot de discord nos muestra lo siguiente al introducir el comando:



Al buscar en el **Twitter** de **Hacker\_Definitivo\_Real** encontramos un **Tweet** que habla de irse a *Lyon*, además de que en su biografía aparece que es de *Málaga*.

### Hacker\_Definitivo\_Real

@Real\_Juacker

[pastebin.com/fSDHAFn6](https://pastebin.com/fSDHAFn6)

📍 La red de Málaga city 📅 Joined May 2023

1 Following 0 Followers

#### Tweets

#### Replies

#### Highlights

#### Media

#### Likes



**Hacker\_Definitivo\_Real** @Real\_Juacker · May 30

...

Esta noche me voy para Francia, a la zona de Lyon; espero que me vaya gucci y poder hacer maldades jejeje

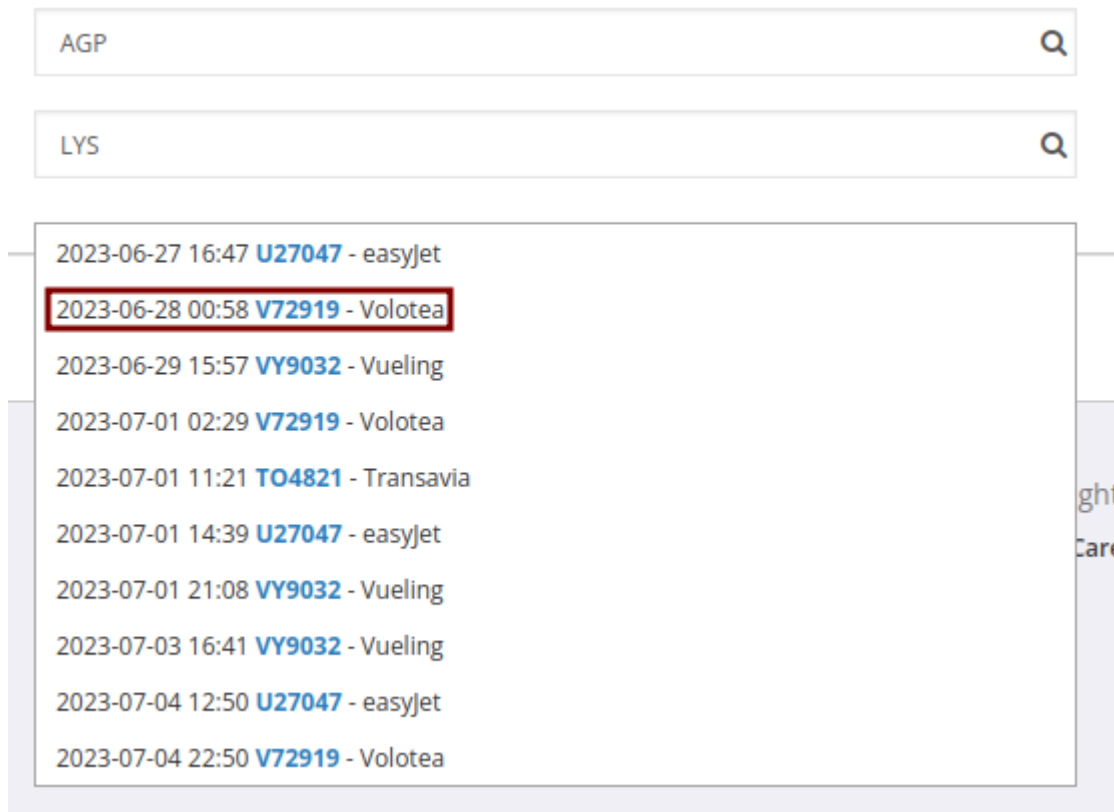


84



Utilizando una herramienta como **flight radar** podemos encontrar el vuelo, hay que introducir los aeropuertos y tenemos que tener en cuenta que el vuelo debe ser por la noche por lo que dice el **Tweet**:

<https://www.flightradar24.com/data>

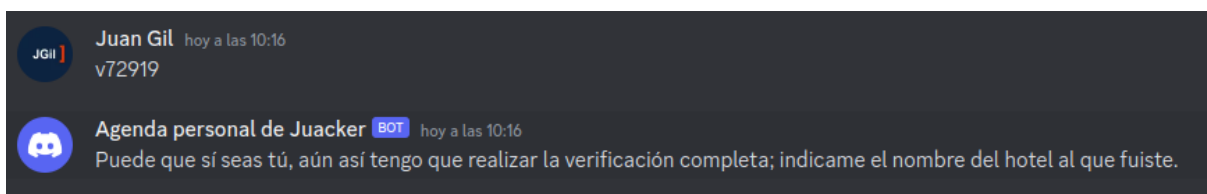


AGP

LYS

2023-06-27 16:47	U27047	- easyjet
2023-06-28 00:58	V72919	- Volotea
2023-06-29 15:57	VY9032	- Vueling
2023-07-01 02:29	V72919	- Volotea
2023-07-01 11:21	TO4821	- Transavia
2023-07-01 14:39	U27047	- easyjet
2023-07-01 21:08	VY9032	- Vueling
2023-07-03 16:41	VY9032	- Vueling
2023-07-04 12:50	U27047	- easyjet
2023-07-04 22:50	V72919	- Volotea

Al decirle ese localizador al bot nos dará el siguiente paso:



Juan Gil hoy a las 10:16  
v72919

Agenda personal de Juacker BOT hoy a las 10:16  
Puede que sí seas tú, aún así tengo que realizar la verificación completa; indicame el nombre del hotel al que fuiste.

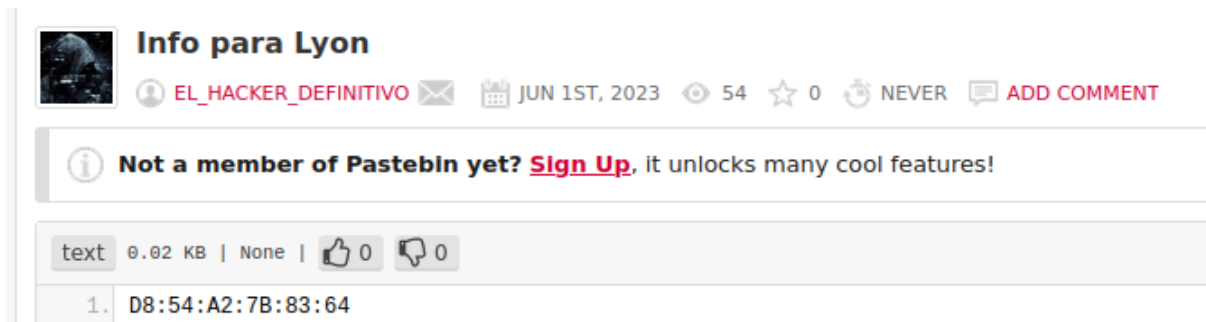
## 2.2.2. Localizador de MAC

### Descripción

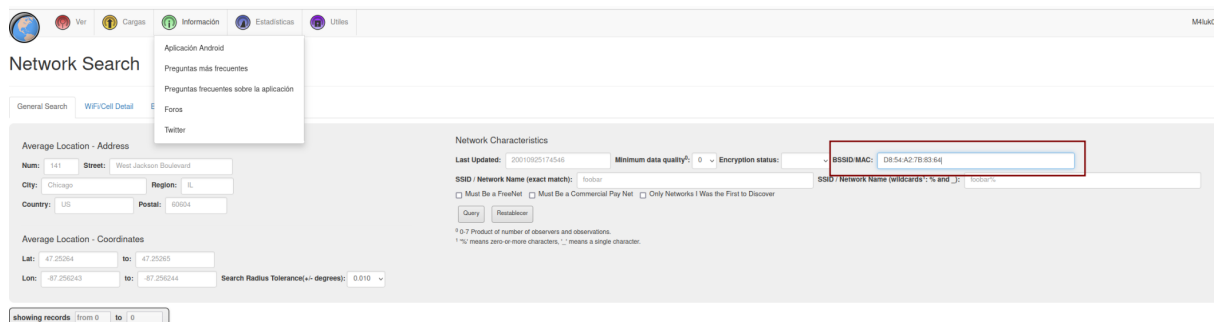
Ahora tenemos que localizar el hotel, para ello, miraremos **pastebin** para encontrar una **MAC** que al pasarla por *wigle* por ejemplo, nos sacará un wifi que se encuentra en el hotel.

### Evidencias


En pastebin encontramos otro post llamado "info para lyon" con una MAC dentro:




Utilizando la búsqueda avanzada de *Wigle*, podemos encontrar a qué wifi pertenece esa **MAC**:

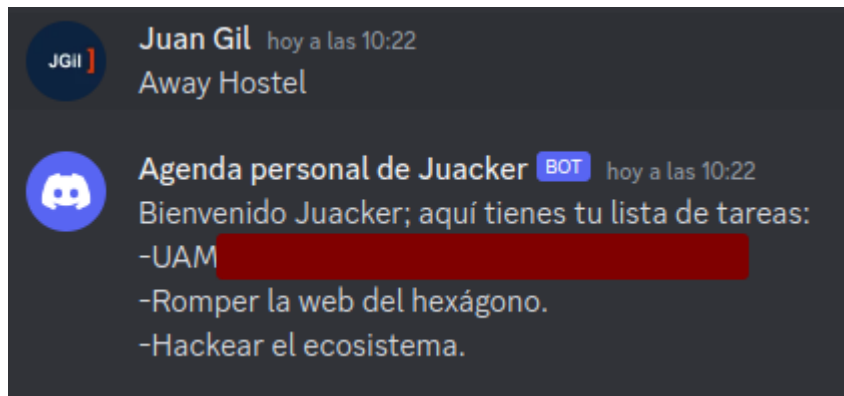


## Computed Network Properties

Network ID	D8:54:A2:7B:83:64
Network Name	
Type	infra
Encryption	
Channel	165
Beacon Interval	
SSID	*Away Guest* (PWD)
Est. Latitude	45.77074051
Est. Longitude	4.83695316
First Seen	2017-07-05T01:22:34.000Z
Most Recently Seen	2023-04-28T16:39:01.000Z
comment	



Nos sale el nombre del hotel, al decírselo al bot, nos dará la segunda flag:



The background of the slide is a dark blue gradient. On the left side, there is a large, abstract pattern of overlapping, semi-transparent squares and rectangles in a lighter blue color, creating a complex, geometric texture. A prominent diagonal line in a bright orange color runs from the top-left towards the bottom-right, intersecting the geometric pattern. In the top-right corner, the company name 'Hispacec]' is displayed in a large, bold, sans-serif font. The 'Hispacec' part is white, and the closing bracket ']' is a vibrant orange, matching the diagonal line.

# Hispacec]

**Hispacec Sistemas S.L.**

C/ Severo Ochoa, 10 - 29590, Málaga

Telf: (+34) 952 020 494

[info@hispacec.com](mailto:info@hispacec.com)