Ajuntament de Lleida

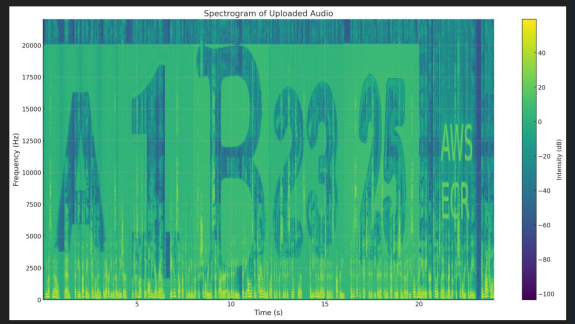
HackEPS 2024

Step 1

La imagen contenia metadata “ASCII: password=j9G2FtnXLti6vA6KTwsHL3ttzrFju6NYx8:code_delivered” la cual nos permitia construir la contraseña junto con el codigo proporcionado por la organización. Una vez puesta la password aparecia un H1 secreto con credenciales de AWS y el path del siguiente paso.

Step 2

Solución: En Application -> Storage había un link a un audio. Analizando las frecuencias nos aparece un texto. Ese texto nos lleva a AWS ECR para descargar una imagen de Docker.

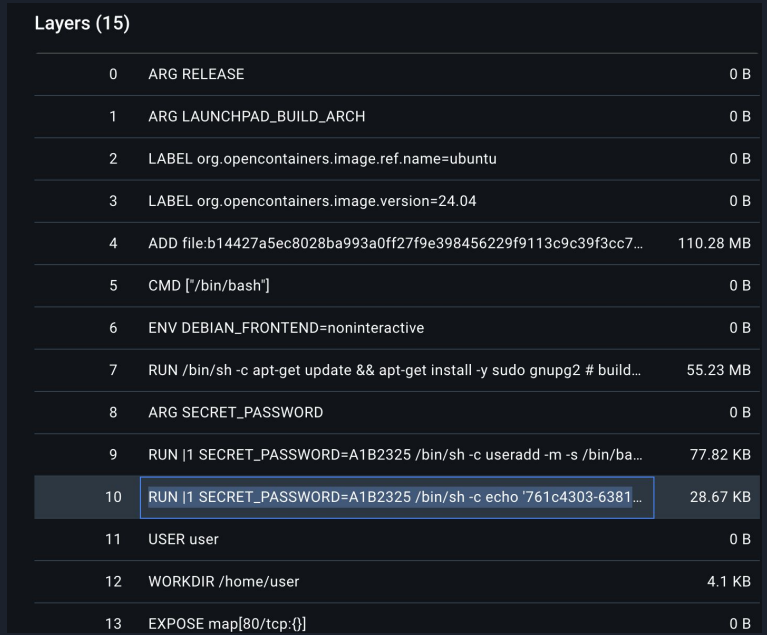



```
~ $ aws ecr describe-repositories
{
    "repositories": [
        {
            "repositoryArn": "arn:aws:ecr:us-west-2:590184058473:repository/hackeps2024",
            "registryId": "590184058473",
            "repositoryName": "hackeps2024",
            "repositoryUri": "590184058473.dkr.ecr.us-west-2.amazonaws.com/hackeps2024",
            "createdAt": "2024-10-16T09:22:18.732000+02:00",
            "imageTagMutability": "MUTABLE",
            "imageScanningConfiguration": {
                "scanOnPush": false
            },
            "encryptionConfiguration": {
                "encryptionType": "AES256"
            }
        }
    ]
}
```

Step 2

Una vez descargada la imagen había dos posibles rutas para encontrar el patch al siguiente step.

1. Coger el UUID de las capas de Docker
2. Entrar en la imagen y analizar el archivo secret_uuid.gpg
   (gpg --batch --yes --passphrase "A1B2325" -o secret_uuid.txt -d secret_uuid.gpg)

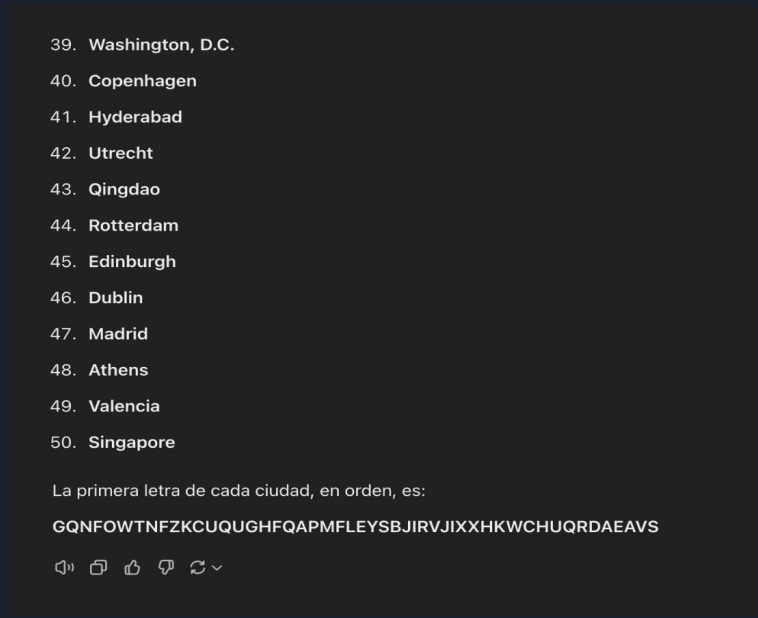


Layers (15)

0	ARG RELEASE	0 B
1	ARG LAUNCHPAD_BUILD_ARCH	0 B
2	LABEL org.opencontainers.image.ref.name=ubuntu	0 B
3	LABEL org.opencontainers.image.version=24.04	0 B
4	ADD file:b14427a5ec8028ba993a0ff27f9e398456229f9113c9c39f3cc7...	110.28 MB
5	CMD ["/bin/bash"]	0 B
6	ENV DEBIAN_FRONTEND=noninteractive	0 B
7	RUN /bin/sh -c apt-get update && apt-get install -y sudo gnupg2 # build...	55.23 MB
8	ARG SECRET_PASSWORD	0 B
9	RUN |1 SECRET_PASSWORD=A1B2325 /bin/sh -c useradd -m -s /bin/ba...	77.82 KB
10	RUN |1 SECRET_PASSWORD=A1B2325 /bin/sh -c echo '761c4303-6381...	28.67 KB
11	USER user	0 B
12	WORKDIR /home/user	4.1 KB
13	EXPOSE map[80/tcp:{}]	0 B

Step 3

1. Hemos visto que dando click a “Travelling” nos descargaba un zip.
2. Analizando las sonatas hemos visto que había una ciudades que con las primeras letras concatenadas obtenemos el path al siguiente paso. Las sonatas han sido analizadas automáticamente por ChatGPT.



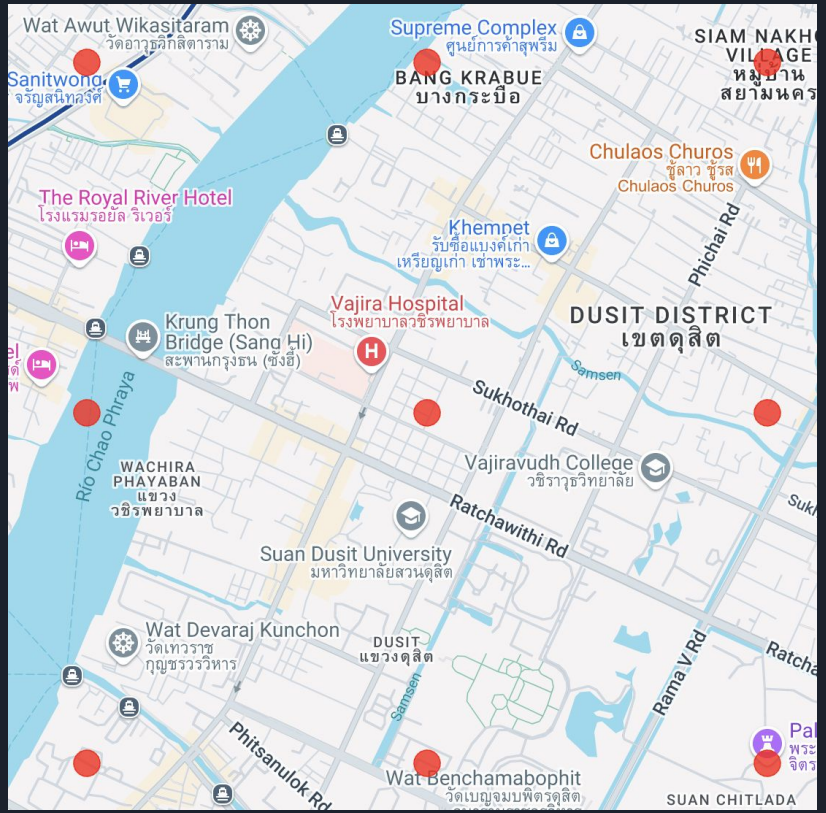
Step 4

Utilizando AWS Kinesis hemos detectado un stream de datos que se iba emitiendo en bucle. Gracias al data["type"] hemos visto que el patrón de repetición era con el símbolo <.

Con las coordenadas hemos descubierto el punto central de un cuadrado en Bangkok.

Mirando en detalle podemos encontrar la marca y modelo del coche.

Aplicando cifrado César 235 con el marca-modelo del coche vamos el siguiente paso



Step 5

Aplicando cambios de contraste el un teléfono móvil hemos descubierto que se trataba de un QR oculto. Buscando la imagen original se consigue restar para obtener el QR legible

Al leer el QR nos permite descargar unos datos de AWS S3. Uno de los zips contenía un listado de nombres, con el buscador de Mac hemos descubierto un fichero llamado “name”. Ese nos ha permitido encontrar a Ibra y pasar al siguiente step.

Step 6

En el HTML hemos descubierto un CSV oculto que hemos descargado.

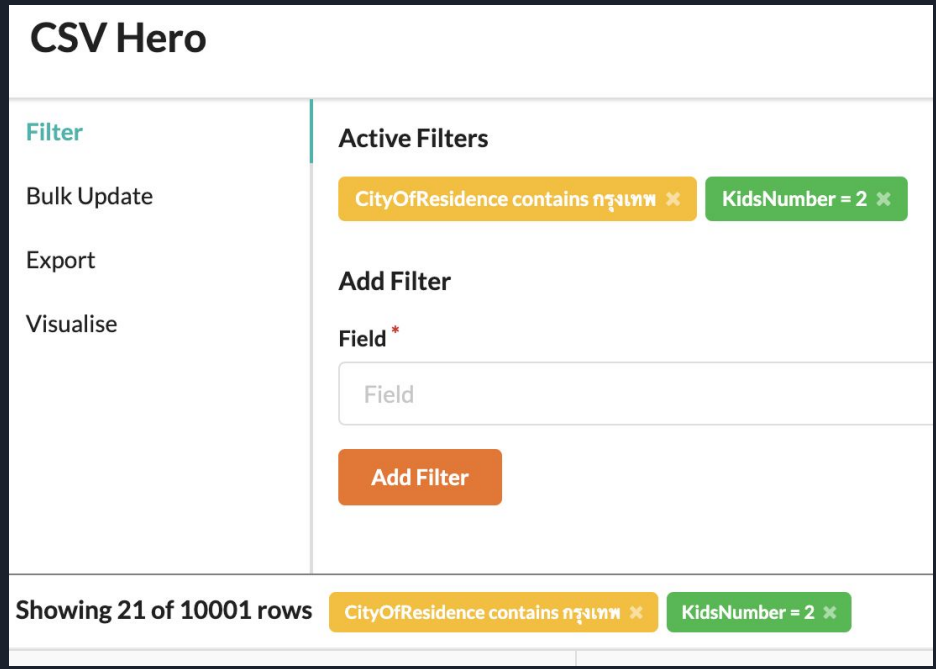
Filtrando por menores de edad sólo había un resultado bien raro. Nos daba el UUID al siguiente paso, fácil verdad? Claramente ha sido suerte!

Final Step

Teniendo en cuenta toda la información recabada en los pasos anteriores hemos hecho un filtrado más exhaustivo al CSV que teníamos.

Con los 21 resultados de 10001 nos dimos cuenta que los números de las filas eran en realidad paths a información extra.

Hicimos una lista y con un script generamos las 21 URLs.



Final Step - Step 2

En las diferentes URL ordenadas por número de fila se encontraba que había unos números sospechosos.

Aplicando el Polybius Square Cipher hemos sacando un conjunto de letras.

Gracias a la organización hemos podido acabar sacando el nombre del asesino

Te pillamos Heriberto-Seda!!!!