

Projecte USEIT

Grup: chinofarmers

Membre1: Gerard Tersa

Membre2: Enric Zhang

Membre3: Joel Gallart

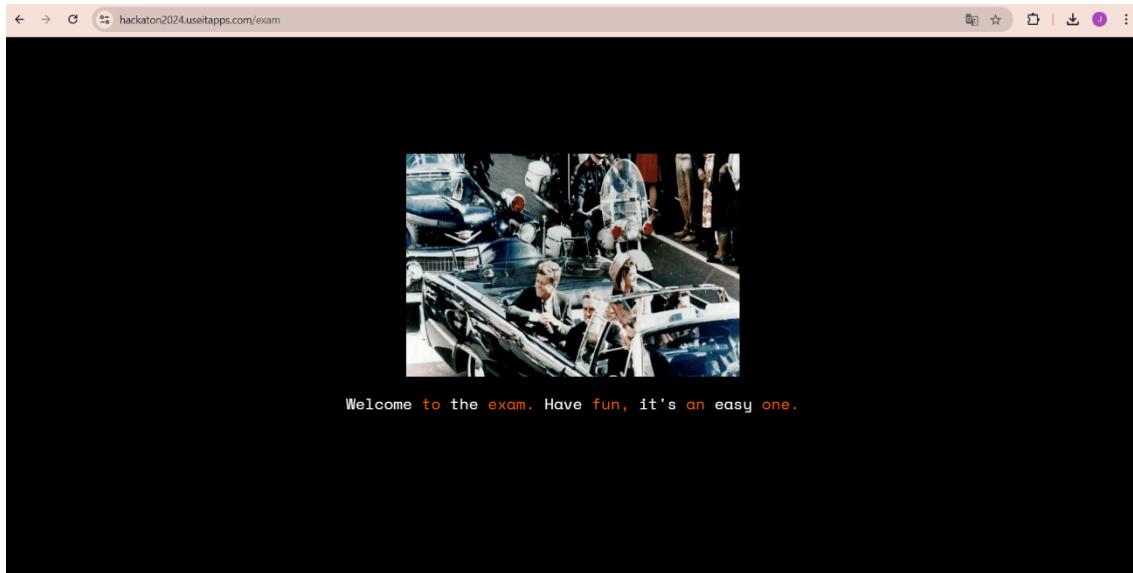
Membre4: Vidal Vidal

Introducció

Per començar hem triat aquest projecte degut a que segons el nostre punt de vista era el que veiem més asequible per als nostres coneixements. Un cop començat, hem vist que hem que fer molta recerca de informació per al nostre grau de experiència. Gràcies a aquest repte hem expandit els nostres coneixements sobre coses com les metadades, els desxifrats o el aws. Concluint així en un projecte on hem disfrutat el procès encara que el grau de dificultat ha acabat sent major del que esperàvem.

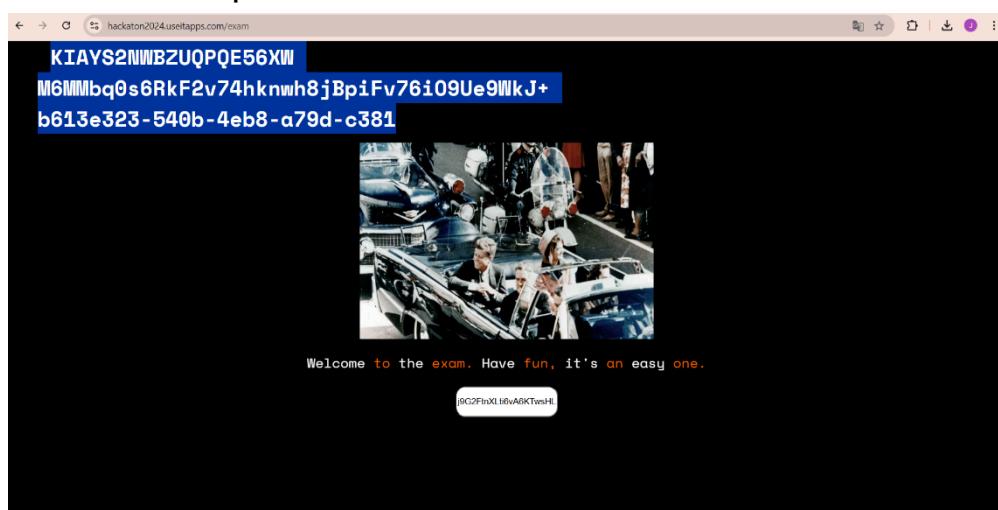
1 nivell:

En el primer nivell se'ns proporcionava una Web (hackaton2024.useitapps.com/exam) i un paper amb una contrasenya. En primer moment se veia això:



Però si passaves el cursor per abaix del text veies que es ficava amb mode escriptura. Després si anaves a inspeccionar ho podies fer mostrar. Després vam estar provant diferents possibles contrasenyes, fins que vam indagar mes i vam mirar les metadades de la imatge i vam trobar una contrasenya de la qual vam tindre que afegir la que ens van proporcionar a nosaltres. I va quedar aquesta j9G2FtnXLti6vA6KTwsHL3ttzrFju6NYx8:fcwTUTIXDdhDHVHSVmrtoVDcfIrlSh

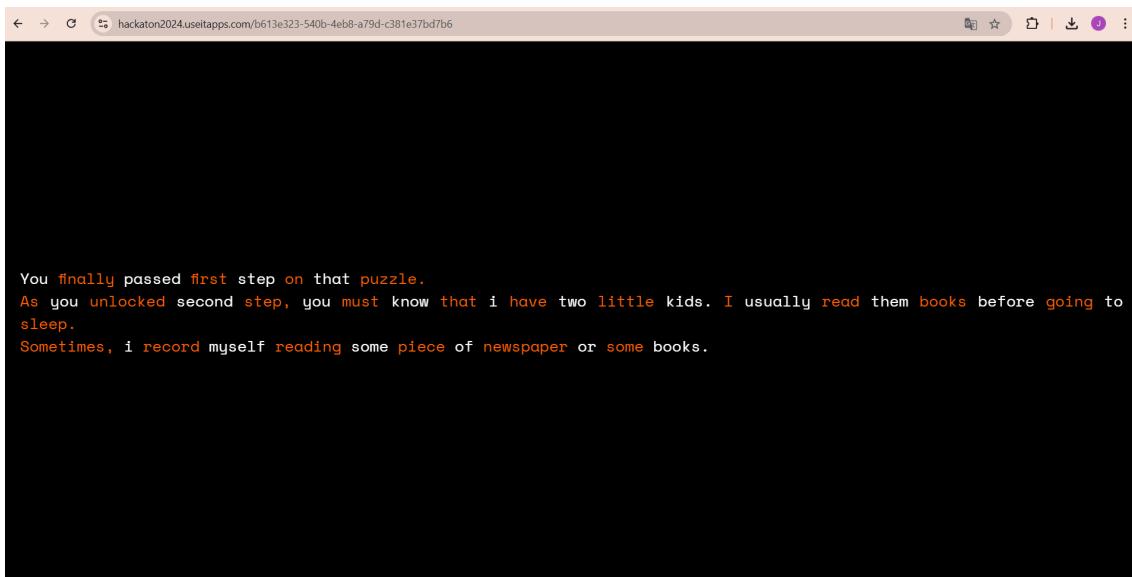
I si la ficaves apareixia això ocult a dalt:



2 nivell:

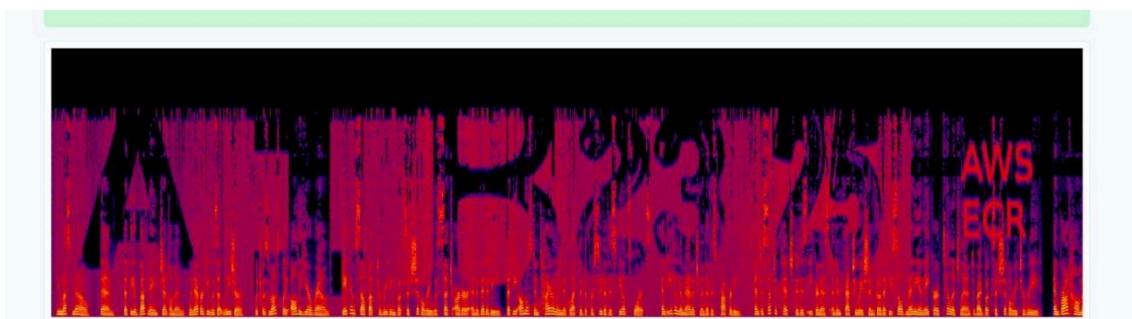
A partir del codi anterior passem al següent nivell

(<https://hackaton2024.useitapps.com/b613e323-540b-4eb8-a79d-c381e37bd7b6>)



En aquesta pagina si la inspeccionava te ficava que hi havia un àudio a la direcció audio/audio.wav, aquesta la fiquem al buscador (<https://hackaton2024.useitapps.com/audio/audio.wav>) i tenim una àudio.

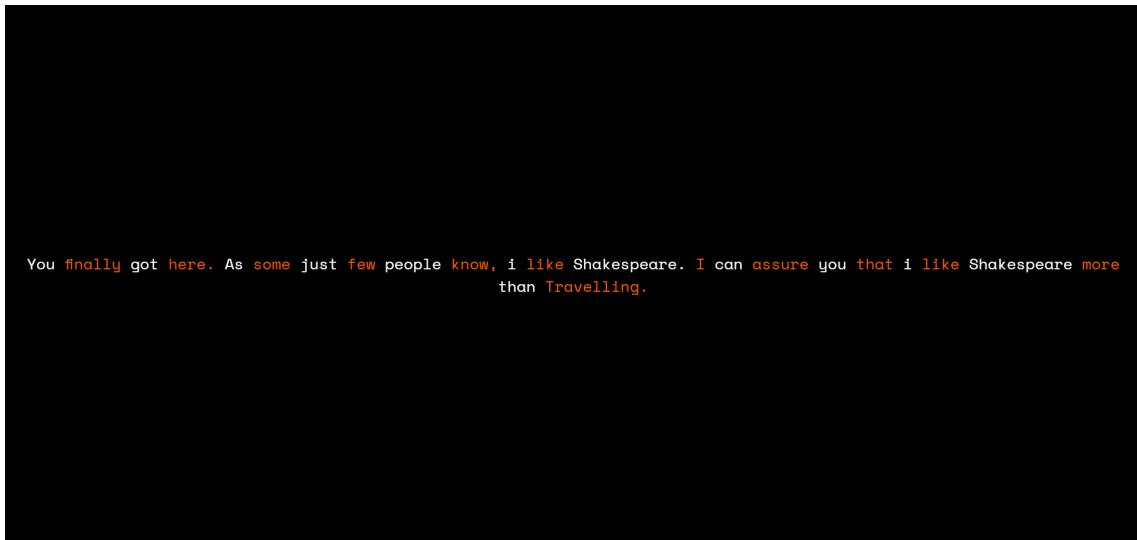
En aquest àudio notem que hi ha certes vibracions i busquem per internet i trobem que existeix una manera per encriptar imatges en àudios. En una pagina Web al ficar el àudio ens va donar aquesta imatge:



Després d'aquesta imatge trobem que tenim que utilitzar aws vam ficar la clau publica AKIAYS2NWBZUQPQE56XW , la clau privada M6MMBq0s6RkF2v74hknwh8jBpiFv76iO9Ue9WkJ+ i la ubicació us-west-2 així busquem a ECR amb el A1B2325 llavors vam fer un push i ens va donar un contenidor i vam fer el run això ens va donar la nova URL.

Nivell 3:

Amb aquesta URL tenim aquesta imatge

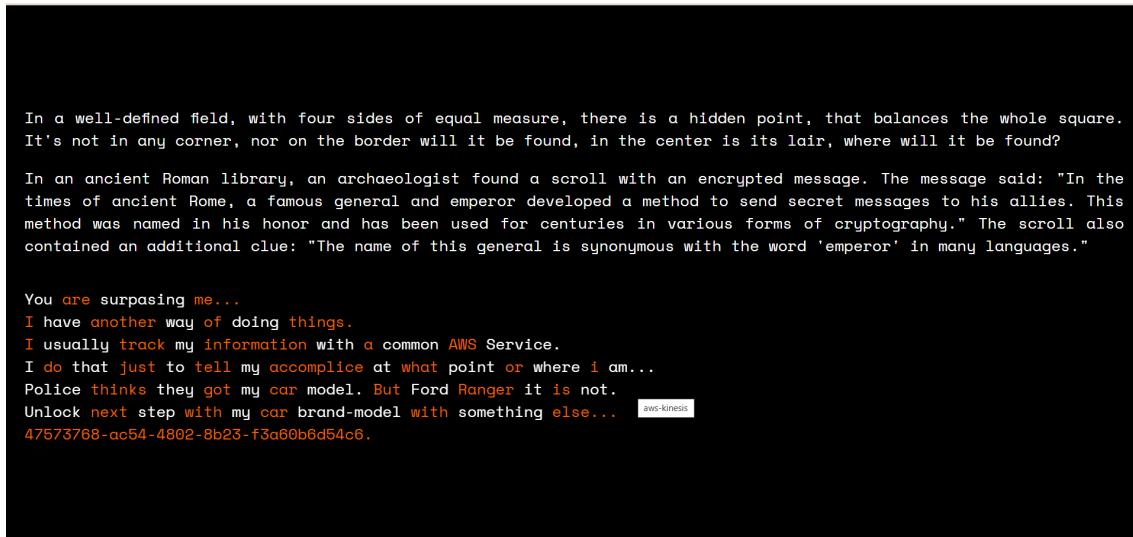


Ens donem compte que si cliquem en tràveling sens descargen un zip que contenen uns sonets de Shakespeare. Rebisem aquests sonets i veiem que a cada sonet hi ha noms de ciutat que no pertany al sonet. Llavors agafem la primera lletra de cada ciutat i obtenim una nova URL.

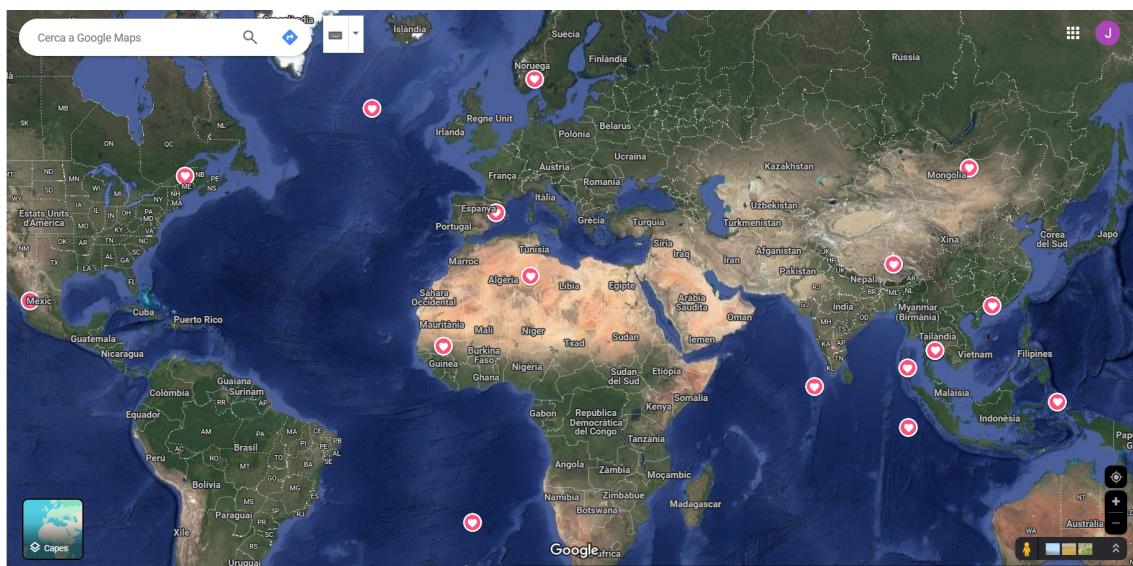
Nivell 4:

Obtenim la següent URL:

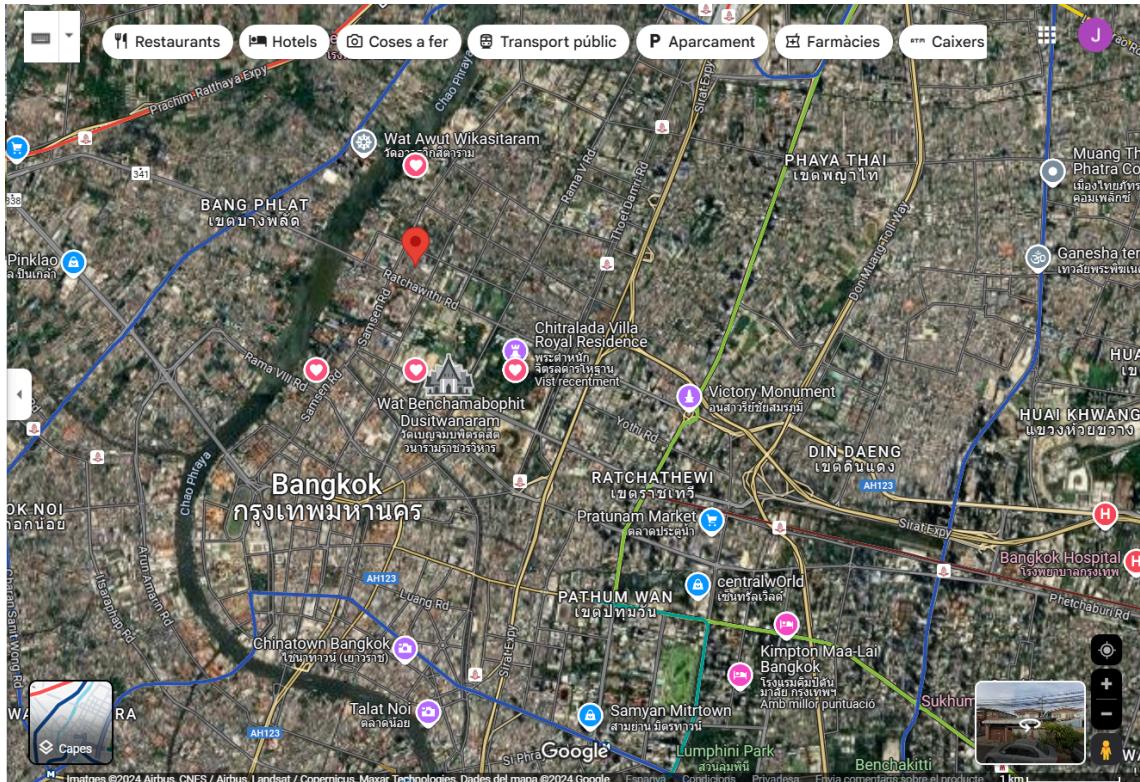
<https://hackaton2024.useitapps.com/GQNFOWTNFZKCQUGHFQA PMFLESBYJROVVJIXXHKWCHUQRQEDMAVS>



Ara tenim aquesta pagina. Mirem que ens donen pistes per a que utilitzem aws kiness llavors el utilitzem junt al codi que tenim abaix per pantalla i ens retorna uns 70 dates que aquestes estan encriptades i utilitzant base 64 les desencriptem i ens donenunes coordenades . Aquestes coordenades les fiquem a un mapa i ens donem compte que hi ha 4 que formen un quadrat en Bangkok



En el mitg del quadrat/triangle tenim aquesta ubicació (235 Soi Suan oi 2)



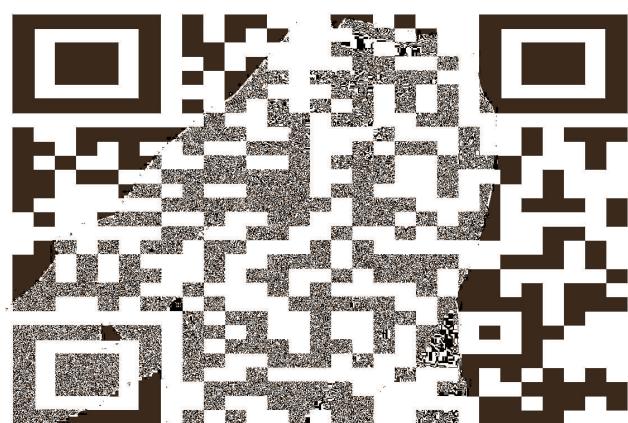
Si fiquem el Street View veiem que hi ha un Honda-Civic amb un portal que fique de 235. Llavors amb el xifrat Ceaser i amb desplaçament 235 hem trobat la següent pàgina
<https://hackaton2024.useitapps.com/lpoeb-Djwjd>

Nivell 5:

En aquest nivell ens en trobat la següent pàgina.



You finally found where i usually reside. You also found my car model and brand. You are really close of completing that.



I si el escanegem ens dóna el seguent:
arn:aws:s3:::accomplicencenames

Amb això ens donem compte que és tracta d'un ARN (Amazon Resource Name) que es refereix a un bucket d'Amazon S3, anomenat **accomplicencenames**. Els ARNs són identificadors únics per a recursos AWS i, en aquest cas, aquest ARN esta indicant un bucket S3.

En aquest bucket hi han una serie d'archius, que per poder-hi accedir i veure'ls hem utilitzat la comanda en el terminal de linux

```
aws s3 ls s3://accompliancenames
```

Amb això és llisten tots els archius dins del bucket, on podem observar que son tot archius .zip amb la comanda.

```
aws s3 cp s3://accompliancenames/<archiu> ./ruta/local
```

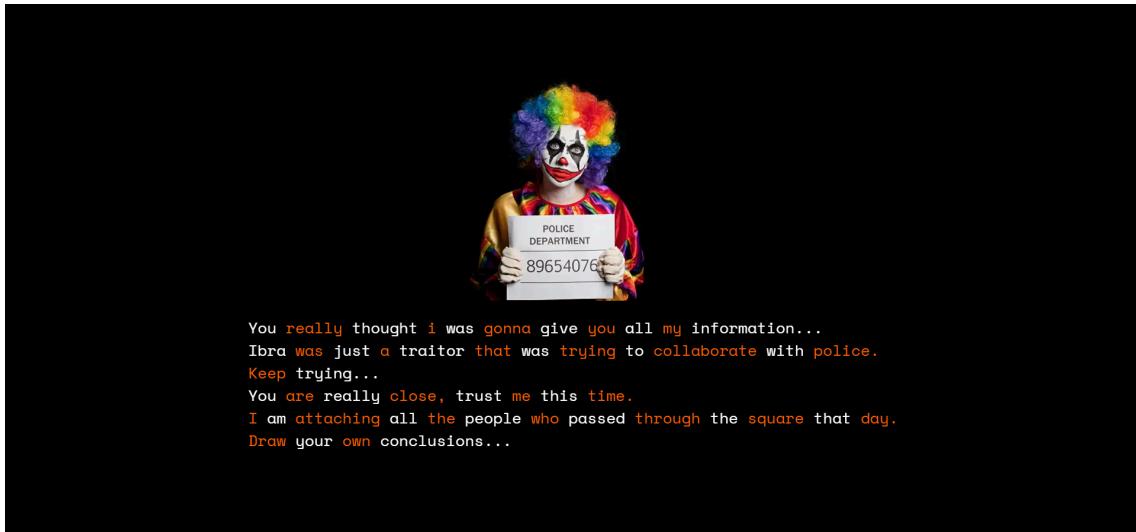
On archiu és el nom de l'archiu en qüestió que volem descarregar.

Tots tenen una característica en comú menys 1, on abans del nom de l'archiu hi ha un número, en la majoria és 22, menys en 1 que es un altre número amb això ens donem compte que aquest restant és el que conté la informació important, així que el descarguem, l'estreiem i veiem que conte una carpeta anonemana *names*.

En aquesta carpeta hi han un nombre molt elevat de carpetes, si accedim a les propietats de la carpeta *names* veiem que conte 87.092 archius, i si entrem dins la carpeta veiem que cada carpeta té 10 elements, per tant lògicament hi ha d'haver alguna carpeta amb menys elements que la resta, una irregularitat, filtrem per tamany en la biblioteca i observem que hi ha una carpeta amb 5 archius, entrem i observem que conte una serie d'archius, entre ells un document de text amb el nou path per la següent pàgina web.

Nivell 6:

<https://hackaton2024.useitapps.com/f081ced9-2c7b-4505-973a-630>



979eb8100

En aquesta pàgina web, observem un pallasso inquietant amb un cartell, si inspeccionem la pàgina web ens donem conté que hi ha un archiu .csv, el qual es un excel, l'obrim en linux i ens dona unes columnes, les quals son el nom, els anys, el nombre de fills, ciutat de residencia, nombre de ciutats visitades en l'últim any. Si ordenem ascendentment ens trobem que en la columna del nom, el primer nom es una path la qual farem servir per anar a la nova pàqina web

Nivel 7: