

Conception_CTF_ "Doko-Doko?"-Alex

Titre du défi : [Doko, doko?]

Conception de l'épreuve de Capture The Flag (CTF) - "Doko, doko?"

Introduction

"Doko, doko?" est une épreuve de CTF basée sur l'Open Source Intelligence (OSINT), et plus spécifiquement sur la géolocalisation (GéoINT).

Description du Défi

Le challenge invite les participants à télécharger une image depuis la plateforme CTFd et à chercher des indices pour identifier un lieu précis. Le joueur découvre des éléments de texte écrits dans une langue avec idéogrammes, ainsi qu'un dessin de biche, qui sont les indices clefs pour résoudre le défi.

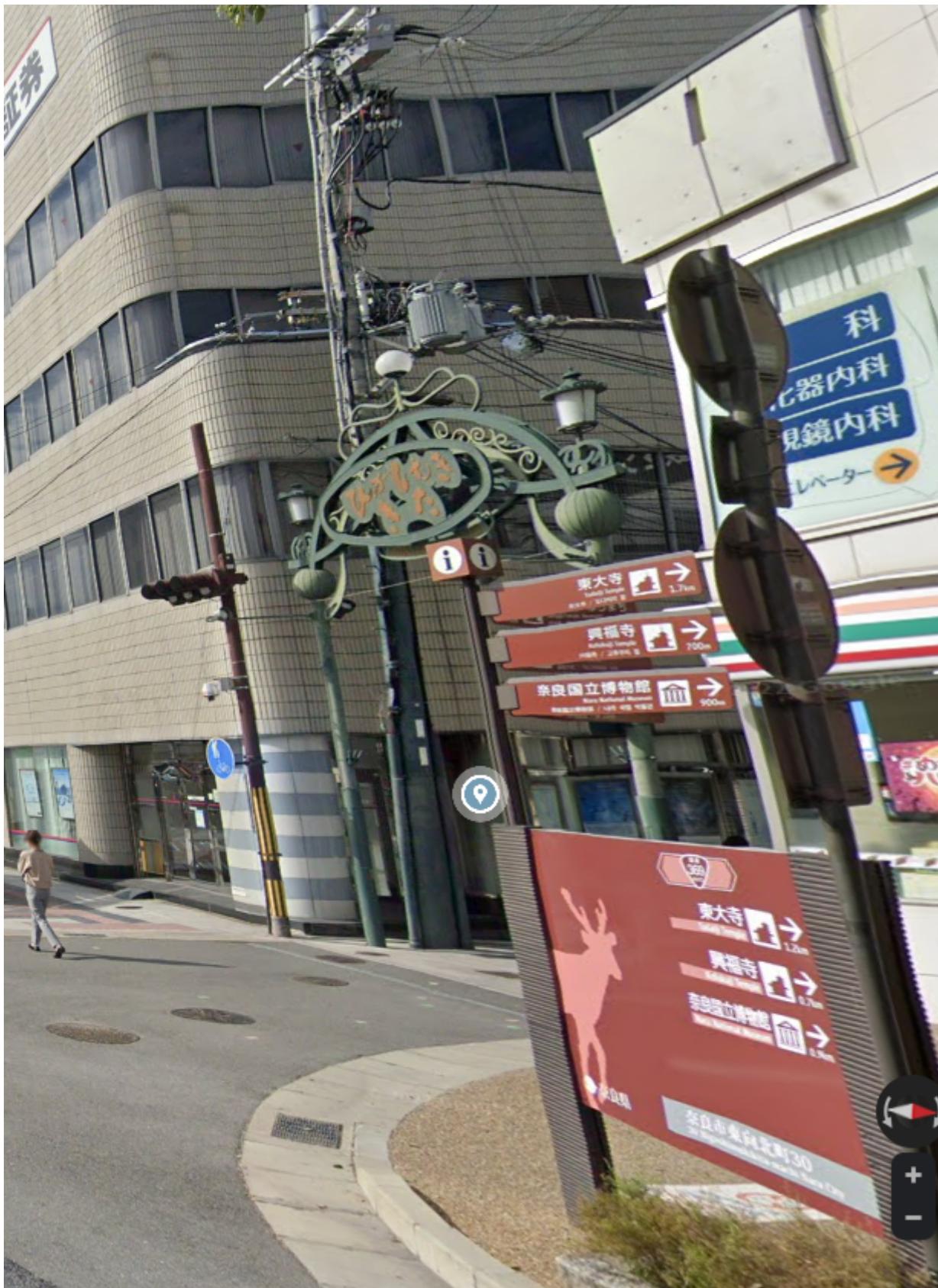
Déroulement du Défi

Étape 1

La première étape consiste à télécharger l'image fournie.

Pour la préparation de l'épreuve, l'image avait été trouvée sur Google Map.

<https://www.google.com/maps/@34.6844694,135.8289151,3a,75y,269.25h,95.88t/data=!3m6!1e1!3m4!1spnU8ZSFUUHi8biBO06noQ!2e0!7i16384!8i8192>



Étape 2

La seconde étape consiste à chercher des indices dans l'image. Les éléments suivants peuvent être utiles :

- L'écriture en idéogrammes suggère un lieu où l'usage de cette forme d'écriture est la norme, a priori en Asie : la Chine, le Japon, Taiwan, Singapour, Hong Kong, Macao, etc.

b) Le dessin de la biche est un indice fort. Il est le symbole de la ville et peut donc aider à identifier le flag.

Étape 3

La troisième étape consiste à utiliser Google Lens pour effectuer une recherche textuelle sur l'image. Cela permettra aux participants de déchiffrer les idéogrammes.

Étape 4

La quatrième étape consiste à effectuer une recherche textuelle sur le panneau avec des flèches dans l'image, par déduction logique on comprend que ce sont des lieux avec leurs directions. Cette recherche devrait renvoyer à des lieux précis que l'on peut vérifier sur Google pour avoir une idée précise sur le lieu, et donc le **flag**. Il s'agit de la ville de Nara, au Japon.

Flag

Le flag pour ce défi est [NHM2I{Nara}].

Conclusion

"Doko, doko?" est un défi de GéoINT qui invite les joueurs à utiliser Google Lens de manière plus pertinente et à ne pas se laisser impressionner par une langue qu'ils ne maîtrisent peut-être pas. Ce défi illustre comment les outils d'OSINT peuvent être utilisés pour déchiffrer des indices et résoudre des énigmes, même dans des langues étrangères. De la même manière, il était possible de résoudre l'éénigme via une simple recherche Google "ville+Asie+biche", qui amenait vers des informations sur la ville de Nara.

A l'origine l'idée était de demander au joueur les coordonnées GPS associées au lieu de cette photo, mais les outils d'OSINT ont tellement progressé que le challenge pouvait être résolu en quelques secondes et le défi perdait de son intérêt... L'image a dû être cropée, mais la difficulté abaissée en ne demandant plus que le nom de la ville.

