

24HIUT - OSINT Writeup

More like an eagle than a turbot 1/3

Enoncé

L'autre jour j'étais pris d'une certaine nostalgie, j'ai donc ressorti un ancien disque dur contenant des photos de vacances. Il contient mon premier voyage sur les traces de mes ancêtres. Regarde cette photo de moi, c'était lors d'un séjour dans la capitale.

Néanmoins ce n'est pas dans cette ville que j'ai passé mon été. Je me souviens vaguement des rues dans lesquelles je me baladais car j'étais encore jeune. Par contre, je n'oublierai jamais mon étonnement quand j'ai croisé ce terrain de foot à plus de 1100 mètres d'altitude ! C'était le bonheur absolu !

Pourrais-tu retrouver le nom de cette ville ?

Fichiers

- *image.jpg*

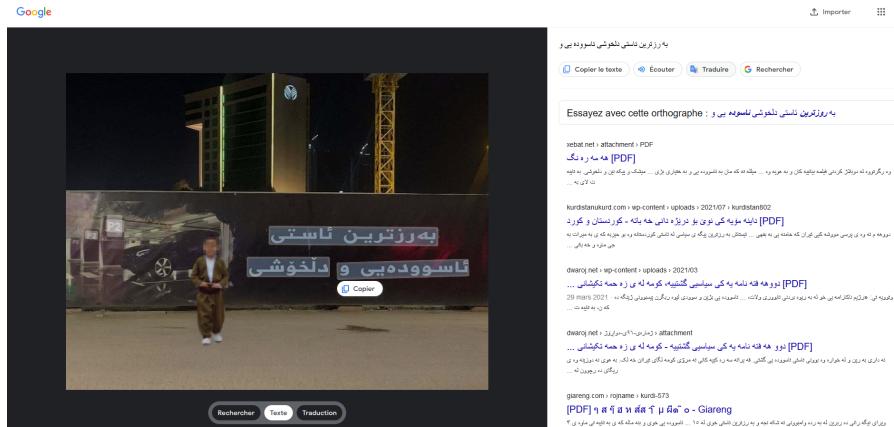


Author : baddhack

Solution

Sur l'image fournie il y a un texte publicitaire qui est censé attirer notre attention. A première vue cela semble être de l'arabe, nous pouvons au moins traduire le texte pour voir s'il peut nous donner des indications.

En uploadant l'image sur Google, nous pouvons extraire le texte qui est automatiquement détecté et même le traduire.



En cliquant sur "Traduire" nous sommes redirigé vers Google Traduction et voici le résultat :

Le texte ne semble pas être utile pour la suite de la recherche. Par contre, ce qu'on pouvait penser être de l'arabe ne l'est finalement pas. La langue détectée par Google Traduction est le **Kurde (Sorani)**.

En cherchant "Sorani" sur Google nous avons une page Wikipédia qui nous donne des explications, voici un extrait de la page :

Le sorani (ou soranî) est un des trois dialectes kurdes. Il est parlé par une grande partie des Kurdes d'Iran et d'Irak, soit environ 30 % des kurdophones. Il s'agit d'une langue indo-européenne du groupe des langues iraniennes.

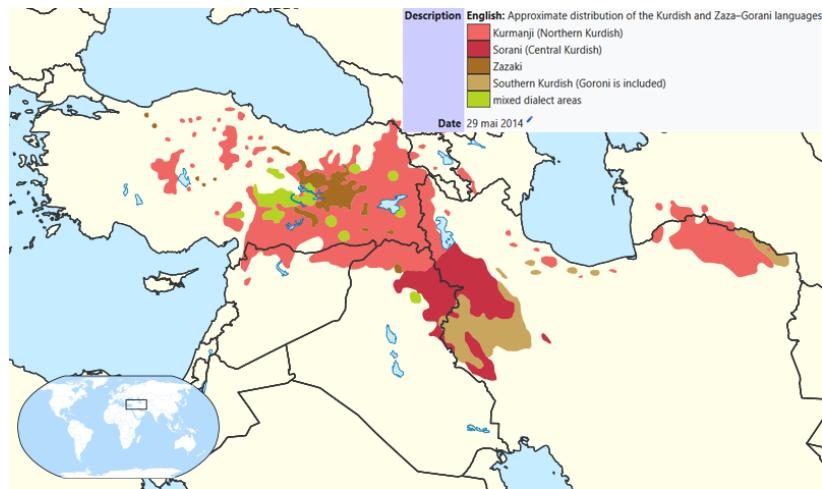
Référence : <https://fr.wikipedia.org/wiki/Sorani>

On apprend donc que le texte au second plan est un dialecte kurde majoritairement parlé en Irak et en Iran. Cela réduit notre zone de recherche. Pour réduire encore plus cette zone, nous pouvons essayer d'en apprendre plus sur la répartition géographique de ce dialecte.

D'après Wikipédia :

Le sorani est parlé dans le nord du Kurdistan iranien et au Kurdistan irakien, où le Grand Zab le sépare des parlers kurmandji.

En cherchant "Sorani Map" sur Google Image, nous avons plein cartes qui donnent une idée de la zone géographique où le dialecte est utilisé.



Référence : https://fr.m.wikipedia.org/wiki/Fichier:Kurdish_languages_map.svg

Wikipédia encore une fois, nous donne une approximation de la répartition des différents dialectes kurdes. Nous avons donc une idée plus précise de où chercher et cela élimine une bonne partie de l'Irak et de l'Iran.

Si on reprend notre énoncé pour ne pas se détourner de notre objectif principal, la photo a été prise dans une capitale mais ce n'est pas la ville que nous cherchons. Celle que nous souhaitons retrouver possède un terrain de foot situé à plus de 1100 mètres d'altitude.

Nous pourrions à présent trouver une carte des reliefs afin de relever des villes qui seraient à haute altitude mais cela risque d'être un peu long. La solution la plus simple est de dégainer notre meilleur ami [Overpass Turbo](#) ! Cet outil est basé sur Open Street Map et offre de nombreuses possibilités de requête pour trouver des objets ou des lieux.

Dans notre cas, nous pouvons simplement nous placer au dessus de la zone que nous venons d'identifier de manière assez large et effectuer une requête qui nous permettrait de trouver une ville ou directement un terrain de foot situé à plus de 1100m d'altitude.

Voici la requête à prévue pour la résolution du challenge :

```
///"playground and ele=1000"
[out:json][timeout:50];
// gather results
(
// query part for: "playground and ele=1000"
way["leisure"="pitch"]["sport"="soccer"](if:t["ele"]>1100)({{bbox}});
);
// print results
out body;
>;
out skel qt;
```

Explication requête :

Si on suit la documentation présente ici : <https://wiki.openstreetmap.org/wiki/Elements>

Notre terrain de foot devrait correspondre à l'élément "way" car c'est une aire ou surface. Dans le doute, on pourrait répéter la même ligne avec "node" pour être sûr de ne rien louper. Nous indiquons ensuite le type d'objet que l'on recherche, c'est un terrain de jeu (pitch) et le sport associé est le football (soccer). Enfin, il est possible de préciser l'altitude avec le paramètre "ele" (pour elevation). Référence :

<https://wiki.openstreetmap.org/wiki/Key:ele>

Les requêtes OverPass Turbo ne sont pas simple à réaliser au début, mais il y a un assistant de requête qui peut vous aider à créer vos premières requêtes et avoir une idée de la syntaxe.

The screenshot shows the OverPass Turbo web application. At the top, there are buttons for 'Exécuter' (Execute), 'Partager' (Share), 'Exporter' (Export), 'Assistant' (Assistant), 'Enregistrer' (Save), 'Charger' (Load), 'Paramètres' (Settings), and 'Aide' (Help). The title bar says 'overpass turbo'. Below the title is a search bar and a map of Turkey with various place names in multiple languages. On the left, the query code is displayed:

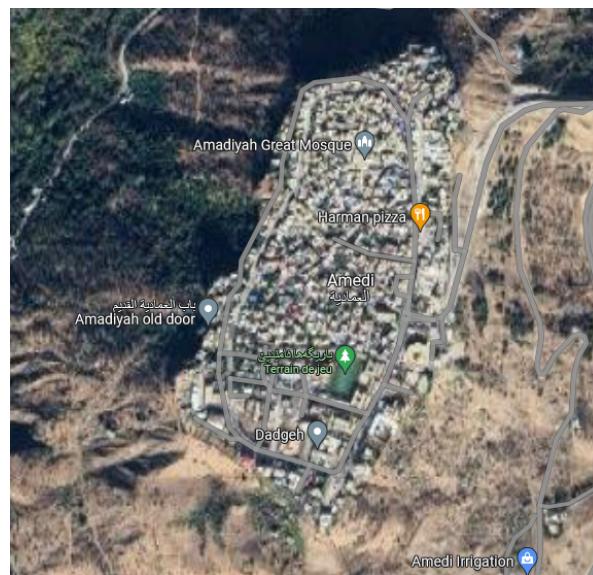
```
1 // "playground and ele=1000"
2 [out:json][timeout:5];
3 // gather results
4
5 // query part 1 - playground and ele=1000
6 node["leisure=pitch"]["sport=soccer"][(if:t["ele"]>1000)((bbox));
7 way["leisure=pitch"]["sport=soccer"][(if:t["ele"]>1000)((bbox));
8 relation["leisure=pitch"]["sport=soccer"][(if:t["ele"]>1000)((bbox));
9
10 // print results
11 out body;
12
13 out skele qt;
```

At the bottom of the interface, there is a URL: <https://overpass-turbo.eu/>.



En se plaçant donc sur la région définie au début et en exécutant la requête, nous avons 1 seul résultat qui est retourné.

En vue satellitaire sur Maps, nous retrouvons bien notre terrain de foot ainsi que le nom de la ville :



Flag : `24HIUT{Amedi}`

Bonus

Dans ce challenge 2 indices étaient fournis dans le titre : [plus proche de l'aigle que du turbot](#)

Indice Aigle :

En faisant plus de recherche sur la région du Kurdistan, il était possible de réduire encore plus la zone de recherche. Au départ nous avions 2 pays qui ressortaient le plus dans nos recherches, l'Iran et l'Irak. En cherchant "Kurdistan Irakien" sur google, une page Wikipédia vous donne l'indication suivante :

Kurdistan irakien

Article Discussion Lire Modifier Modifier le code Voir l'historique Outils

Pour les articles homonymes, voir [Kurdistan \(homonymie\)](#).

Le Kurdistan irakien ou [Kurdistan du Sud](#), ou plus officiellement [région du Kurdistan](#), est une entité politique autonome du Nord de l'Irak, reconnue par la [constitution irakienne](#), adoptée le 15 octobre 2005 par un référendum populaire.

Cette région est bordée par l'Iran à l'est, la Turquie au nord et la Syrie à l'ouest, en étant incluse dans la région du Kurdistan. La capitale du gouvernement kurde est Erbil.

Étymologie et nom officiel [modifier | modifier le code]

Le mot Kurdistan signifie littéralement « pays des Kurdes ». La région du Kurdistan est connue par plusieurs termes apparentés au mot « Kurde » au cours de l'[Antiquité](#). Les Sumériens l'appelaient « KUR.A », « Tritum » ou « pays de Karda », les Elamites « Kurdasu », les Akkadiens « Kurtei », les Assyriens « Kurti », les Babyloniens « Qardu », les Grecs « Καρδούχοι » (Kardoúchoi) et les Romains « Corduene ».

Concernant le nom officiel, la nouvelle [Constitution irakienne](#) parle de « région du Kurdistan » (*Kurdistan Region* en anglais)³. Le gouvernement régional parle de « Kurdistan-Iraq » (en anglais : *Kurdistan Region*) ; « Kurdistan-Iraq » ou « région du Kurdistan » en français⁵. Le nom du gouvernement est le « gouvernement régional du Kurdistan » ou KRG (en kurde : *Hikûmetî Herêmî Kurdistan*).

Les Kurdes appellent aussi leur région « Kurdistan du Sud » (en kurde : *Kurdîstan Başûr*) ou « Sud du Kurdistan » (en kurde : *Başûrî Kurdistan*) en référence à la localisation géographique de la région autonome au sein du [Kurdistan](#) dans son ensemble.

Région du Kurdistan
Hêremê Kurdistanê (ku)
Başûrî Kurdistan (ku)

Emblème Drapeau

Territoire officiel de la région du Kurdistan irakien

Territoire conquis par le Kurdistan irakien pendant la seconde guerre civile irakienne

Autre territoire revendiqué par le Kurdistan irakien

Reste du territoire de l'Irak

Référence : https://fr.wikipedia.org/wiki/Kurdistan_irakien

L'aigle représente l'emblème de la région du Kurdistan irakien. Cela aurait permis d'éliminer l'Iran de nos recherches et nous pouvions ensuite nous concentrer uniquement sur le nord de l'Irak.

Indice turbot :

Le turbot est un poisson, d'où la comparaison entre 2 animaux dans le titre. Avec cette indication, je souhaitais pousser les joueurs à utiliser l'outil OverPass Turbo pour résoudre le challenge.

Solution simple :

J'ai trouvé cette solution après avoir conçu le challenge, et celle-ci pourrait le faire basculer en [easy](#) au lieu de [medium](#).

Google kurdistan city 1000m altitude

Tous Images Actualités Shopping Vidéos Plus Outils

Environ 209 000 résultats (0,41 secondes)

Images correspondant à kurdistan city 1000m altitude

Je pense que l'image parle d'elle même

Drôle de plongeoir 2/3

Enoncé

Parfois le week-end nous allions nous baigner à une dizaine de minutes de la ville. Je n'ai plus le nom du lieu mais j'ai le souvenir que mes parents me laissaient sauter dans cette piscine qui était remplie grâce à une source naturelle. Pendant ce temps ils étaient assis dans un restaurant juste à côté et je me souviens encore de cette odeur de viande grillée.

Comment s'appelle ce restaurant déjà ?

Author : baddhack

Solution

Dans ce challenge, le titre donnait aussi une indication. L'objectif est de trouver un lieu où l'on peut se baigner avec un plongeoir différent de ce que l'on peut retrouver dans une piscine municipale.

D'après l'énoncé, le lieu est situé à une dizaine de minutes de la ville précédemment trouvée. Lors des tests de ce challenge, une personne a trouvé le bon lieu uniquement en se promenant sur Maps et en repérant les points possibles situés à une dizaine de minutes en voiture.

Je vais uniquement détailler la solution attendue. Ici, suite à la découverte de l'outil Overpass Turbo, je souhaitais encourager son utilisation. L'énoncé mentionne une source d'eau naturelle qui serait utilisée pour remplir la piscine. Sur Overpass Turbo, cette source pourrait être identifiée avec l'objet "waterway".

(Référence : <https://wiki.openstreetmap.org/wiki/Key:waterway>)

Key	Value	Element	Comment	Carto rendering	Photo
Natural watercourses					
waterway	river	<input checked="" type="checkbox"/>	A river is a wide, natural watercourse that flows from a source to an ocean, sea, lake or another river. For narrow naturally-formed waterways, see waterway=stream .		
waterway	riverbank	<input checked="" type="checkbox"/>	Use of these tags is discouraged. See water=river + natural=water instead.		
waterway	stream	<input checked="" type="checkbox"/>	A naturally-formed waterway that is too narrow to be classed as a river. An active, able-bodied person should be able to jump over it.		
waterway	tidal_channel	<input checked="" type="checkbox"/>	A natural tidal waterway within the coastal marine environment with bi-directional flow of salty water which depends on the tides.		

La documentation pour la clé "waterway" donnent plusieurs valeurs possibles pour les sources d'eau naturelles. En regardant les 4, celle qui semble la plus convenir pour alimenter une piscine est la rivière "stream".

En effectuant une simple recherche `waterway=stream` avec l'assistant de recherche d'Overpass Turbo on obtient le résultat suivant :

The screenshot shows the Overpass Turbo interface with a map of a river system. The map includes several roads labeled with numbers like 33 and 178, and various geographical features. A legend at the bottom right indicates the following statistics: Champs - nœuds: 559472, chemins: 188484, relations: 0. Attaché - points d'intérêt - POIs: 60, lignes: 10869, polygones: 0.

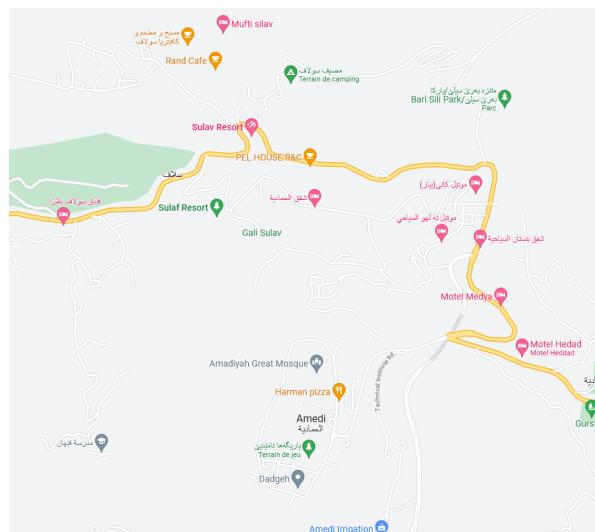
```

1 /*
2 This has been generated by the overpass-turbo wizard.
3 The original search was:
4 [timeout:25];
5 // "waterway=stream"
6 out:json[timeout:25];
7 // gather results
8 (
9   // query part for: "waterway=stream"
10   way["waterway"="stream"]((bbox));
11 );
12 // print results
13 out body;
14 };
15 out skel qt;

```

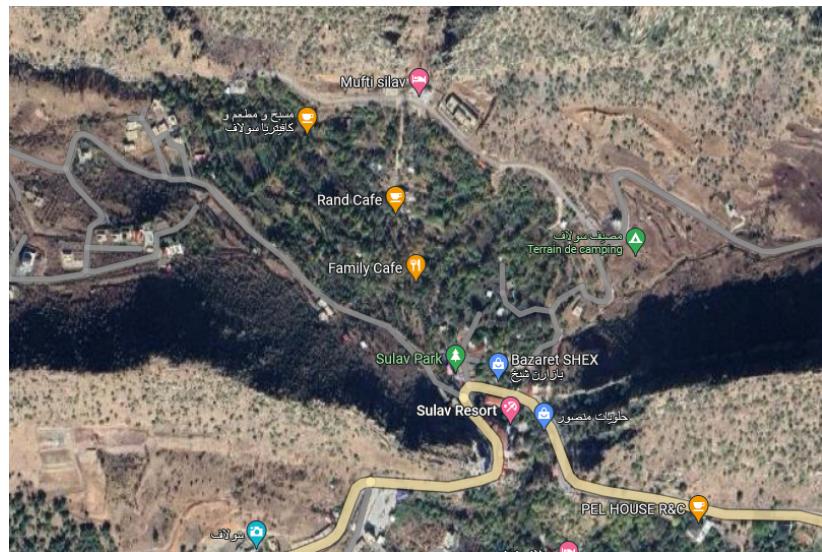
Il n'y a pas énormément de zones à une dizaine de minutes à traiter, en parcourant Maps nous pouvons essayer de regarder si les sources alimentent une quelconque piscine ou quelques chose de similaire en fin de course.

Sur Maps on peut voir pour la zone au nord "Sulav Resort"

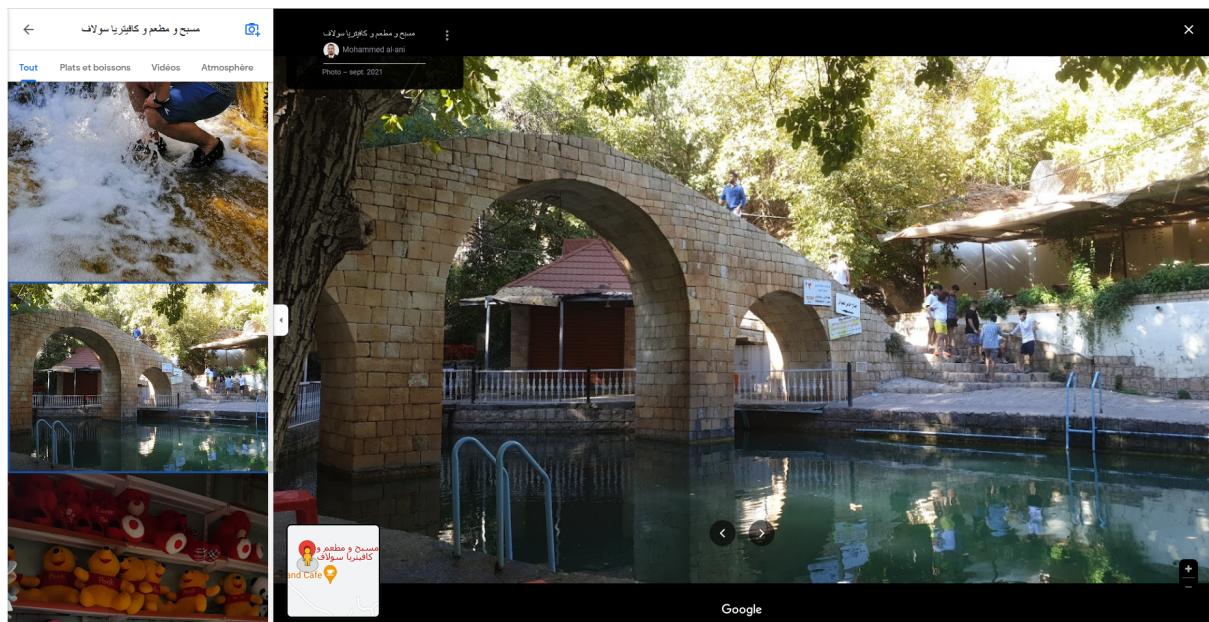


Si l'on traduit cela, c'est une station balnéaire (pas comme celles qu'on connaît je vous l'accorde).

Voici la vue satellitaire, avec quelques restaurants ou cafés qui sont recensés :



Nous cherchons un restaurant qui serait à côté d'une piscine. Etant donné que nous n'avons pas de Street View dans cette zone, il faut regarder les photos que les gens ont postés pour les différents restaurants. Il se trouve que sur le point le plus au nord, nous avons de nombreuses photos comme celle-ci qui sont partagées



Nous avons même un point photo sur le pont avec le restaurant à côté !



Nous retrouvons notre drôle de plongeoir qui est en fait un pont qui surplombe la piscine. Plus qu'à traduire le nom du restaurant et le flag donne : [24HIUT{Restaurant et cafeteria Sulaf}](#)

Grazie mille 3/3

Enoncé

Merci d'avoir retrouvé ce restaurant ! Cela me rappelle de bons souvenirs ! Je suis vraiment fier de ma région.

Vous ai-je dis que j'étais aussi passionné d'histoire ? Lorsque nous nous rendions à la capitale, j'adorais me balader autour de ce site mondialement reconnu.

Sais-tu qui a découvert les premières sources historiques mentionnant ce lieu ?

Solution

La difficulté de ce challenge repose sur la confusion qu'il peut y avoir sur les capitales. En effet, le Kurdistan n'étant pas un pays mais une région autonome, elle s'étend sur différents pays qui possèdent chacun leurs capitales. Mais chaque région du Kurdistan possède aussi sa capitale comme on peut le voir ci-dessous :

Capitale	Diyarbakır (Turquie) Erbil (Irak) Kermanshah (Iran) Hassaké (Syrie)
----------	--

Référence : <https://fr.wikipedia.org/wiki/Kurdistan>

Dans cette série de challenge, nous nous situons au nord de l'Irak depuis le début, c'est donc la capitale du Kurdistan Irakien qu'il faut choisir (Erbil) et non pas la capitale de l'Irak (Bagdad).

A partir de là, la solution se trouve assez facilement à l'aide de Google et Wikipédia 😊

site connu erbil



Tous Images Actualités Vidéos Livres Plus Outils

Environ 422 000 résultats (0,51 secondes)

Wikipedia https://fr.wikipedia.org/wiki/Citadelle_d'Erbil



Citadelle d'Erbil

La citadelle d'Erbil (en kurde: قەلای ھەولێر Qelây Hewlêr) est un tell ancennement fortifié, centre historique de la ville actuelle d'Erbil, dans la région du Kurdistan d'Irak.

Le site de la citadelle peut avoir été occupé dès le Néolithique.

Termes manquants : connu | Doit inclure : connu

On tombe sur la Citadelle d'Erbil qui est un site classé au patrimoine mondial de l'UNESCO.

Citadelle d'Erbil

28 langues

Article Discussion

Lire Modifier Modifier le code Voir l'historique Outils

36° 11' 28" nord, 44° 00' 33" est

Cet article est une ébauche concernant la liste du patrimoine mondial et l'Irak.



Vous pouvez partager vos connaissances en l'améliorant (comment ?) selon les recommandations des projets correspondants.

Consultez la liste des tâches à accomplir en page de discussion.

La citadelle d'Erbil (en kurde: قەلای ھەولێر Qelây Hewlêr) est un tell ancennement fortifié, centre historique de la ville actuelle d'Erbil, dans la région du Kurdistan d'Irak.

La citadelle est inscrite sur la liste du patrimoine mondial depuis le 21 juin 2014¹.

Les plus anciennes traces d'occupation du tell remontent au 5^e millénaire avant J.-C. et peut-être plus tôt. La citadelle apparaît pour la première fois dans les sources historiques des tablettes d'Ebla vers 2300 av. J.-C. et revêt une importance particulière pendant la période néo-assyrienne. Pendant la période sassanide et le califat abbasside, Erbil était un centre important pour le christianisme. Après la capture de la citadelle par les Mongols en 1258, l'importance d'Erbil a diminué. Au cours du xx^e siècle, la structure urbaine a été considérablement modifiée, cause de la destruction de nombreuses maisons et bâtiments publics. En 2007 a été créé un Haut Commissariat à la revitalisation de la citadelle d'Erbil (HCECR), chargé de superviser la restauration du centre historique. La même année, les habitants ont été expulsés de la citadelle dans le cadre d'un vaste projet de restauration. Depuis lors, des travaux de recherche et de restauration archéologiques ont été réalisés à l'intérieur du tell et aux alentours du bâtiment par des équipes internationales, en coopération avec des spécialistes locaux. Le gouvernement envisage que 50 familles puissent vivre dans la citadelle quand elle aura été rénovée.

Les bâtiments situés sur le monticule s'étaient sur une zone ovale couvrant approximativement de 430 × 340 mètres pour une superficie de 102 000 mètres carrés. La seule structure religieuse qui survit actuellement est la mosquée Mulla Afandi. Le monticule s'élève entre 25 et 32 mètres au-dessus de la plaine environnante. Quand elle était entièrement occupée, la citadelle était divisée en trois districts ou mahallas : d'est en ouest, le Serai, le Takyâ et le Topkhana. Le Serai était occupé par des familles notables, le district de Takyâ a été nommé d'après les maisons de servitudes appelées takyas, et le district de Topkhana abritait des artisans et des agriculteurs.



Citadelle d'Erbil (Hewlêr) *

Patrimoine mondial de l'UNESCO



Coordonnées 36° 11' 28" nord, 44° 00' 33" est

Pays Irak

Subdivision Kurdistan

Type Culturel

Critères (iv)

Numéro d'identification 1437

Zone géographique Kurdistan **

Année d'inscription 2014 (38e session)

Référence : https://fr.wikipedia.org/wiki/Citadelle_d'Erbil

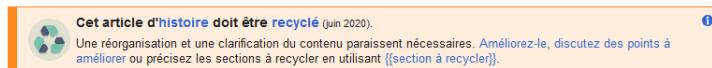
En lisant la page Wikipédia on trouve la mention des tablettes d'Ebla qui seraient la première source mentionnant la citadelle. Sur la page Wikipédia des tablettes d'Ebla on trouve directement la solution :

Tablettes d'Ebla

⋮ 16 langues

Article Discussion

Lire ModifierModifier le code Voir l'historique Outils



Les tablettes d'Ebla désignent plusieurs milliers de tablettes et de fragments mis au jour dans le palais de la ville antique d'Ebla, en Syrie actuelle. Les tablettes ont été découvertes par l'archéologue italien Paolo Matthiae et son équipe en 1974-1975¹ au cours de leurs fouilles dans la ville antique de Tell Mardikh². Les tablettes, qui ont été trouvées *in situ* sur des étagères effondrées, ont conservé nombre de leurs étiquettes contemporaines en argile utilisées pour faciliter leur référencement. Elles datent toutes de la période entre ca. 2500 AEC³ et la destruction de la ville ca. 2250 AEC⁴. Aujourd'hui, les tablettes sont conservées dans des musées des villes syriennes d'Alep, de Damas et d'Idlib.

Référence : https://fr.wikipedia.org/wiki/Tablettes_d'Ebla

Flag : 24HIUT{Paolo Matthiae}

Et c'est ici que s'achève cette série !

J'espère que vous avez apprécié les challenges, et que vous avez découvert au moins une nouvelle technique d'OSINT. Merci pour votre participation 😊