

02 Walkthrough

Apprenant	Date	Sujet	Nom du CTF
Michel MEIRESONNE	25/01/2023	Cryptographie Résolution	Base-Ball

Résolution

TkhNMkI7SWwgZmF1dCBhdm9pciBkZSBib25uZXMgYmFzZXN9

Déterminer le type de chiffrement

Sur [Dcode](#) on peut identifier rapidement le type.

Rechercher un outil

★ RECHERCHE SUR DCODE PAR MOTS-CLÉS :
TkhNMkI7SWwgZmF1dCBhdm9pciBkZSBib25uZXMgYmFzZXN9

★ PARCOURIR LA LISTE COMPLÈTE DES OUTILS

► **Code Base64** (ymfzzty0)

► **Précision et Rappel** (f1)

⚠ Vous ne trouvez pas ?
► Vous cherchez à déchiffrer un message ? Essayez le [détecteur de chiffrement](#) !
► Parcourez [la liste de tous les outils dCode](#)
► Décrivez vos besoins: [écrivez-nous](#) !

Reconnaitre un Chiffrement

Outil pour identifier/reconnaitre le type de chiffrement/codage appliqué à un message (plus de 200 chiffres/codes sont détectables) afin de le déchiffrer/décoder rapidement.

RECONNAITRE UN CHIFFREMENT
Cryptographie › Reconnaitre un Chiffrement

Real-Time Feedback
Like a spell checker, SonarLint squiggles coding issues and enables you to code better.
Sonar [Open](#)

IDENTIFIER UN MESSAGE CODÉ

★ MESSAGE CHIFFRÉ À RECONNAÎTRE ?
TkhNMkI7SWwgZmF1dCBhdm9pciBkZSBib25uZXMgYmFzZXN9

★ INDICES/MOTS-CLÉS (FACULTATIF)

[► ANALYSER](#)

Voir aussi : [Analyse des Fréquences](#) — [Indice de Coïncidence](#)

IDENTIFIER DES SYMBOLES

Résolution en ligne

Il existe plusieurs sites pour déchiffrer, par exemple

- [Cyberchief](#)
- [Dcode](#)
- [Online-toolz](#)

Ici on le fait avec [Cyberchief](#)

The screenshot shows the Cyberchief application interface. At the top, a green header bar displays 'Version 9.55.0 - Sponsored by DEF24.com', 'Last build: 2 months ago', and links for 'Options', 'About / Support', and a help icon. The main interface is divided into three vertical panels. The leftmost panel, 'Operations', contains a search bar, a 'Favourites' section with a star icon, and a list of operations: 'To Base64', 'From Base64', 'To Hex', 'From Hex', 'To Hexdump', 'From Hexdump', 'URL Decode', 'Regular expression', 'Entropy', 'Fork', and 'Magic'. Below this list are sections for 'Data format' and 'Encryption / Encoding'. The middle panel, 'Recipe', is currently empty. The rightmost panel is split into 'Input' and 'Output' sections. The 'Input' section shows 'length: 0' and 'lines: 1'. The 'Output' section shows 'time: 1ms', 'length: 36', and 'lines: 1'. At the bottom of the 'Recipe' panel, there is a 'STEP' indicator, a green 'BAKE!' button with a chef icon, and an 'Auto Bake' checkbox which is checked.

- **avec Magic**

- Si le type de chiffrement est indéterminer

Dans la partie Opération on chercher Magic, puis la fait glisser vers Recipe.

This screenshot shows the 'Magic' operation selected in the 'Operations' sidebar. The 'Recipe' panel now contains the configuration for the 'Magic' operation. It includes a 'Depth' input field set to '3', an 'Intensive mode' checkbox, an 'Extensive language support' checkbox, and a 'Crib (known plaintext string or regex)' input field. The 'Output' panel shows the result of the operation: 'Nothing of interest could be detected about the input data. Have you tried modifying the operation arguments?'. The 'STEP' indicator, 'BAKE!' button, and 'Auto Bake' checkbox are still visible at the bottom of the 'Recipe' panel.

- **avec From base64**

- Si il a trouver que c'est du base64

Dans la partie Opération on chercher From Base64, puis la fait glisser vers Recipe.

Operations

base64

To Base64

From Base64

Show Base64 offsets

Fork

From Base32

From Base58

From Base85

Parse SSH Host Key

To Base32

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars ☐ Strict mode

STEP

BAKE!

Auto Bake

Input

length: 0
lines: 1

Output

time: 7ms
length: 2
lines: 1

Puis on colle le chiffré

```
TkhNMkl7SWwgZmF1dCBhdm9pciBkZSBib25uZXMGYmFzZXN9
```

dans Input.

Le message déchiffré s'affiche dans Output

NHM2I{Il faut avoir de bonnes bases}

avec From base64

Version 9.55.0 - Sponsored by DEF24.comLast build: 2 months agoOptionsAbout / Support

Operations

base64

To Base64

From Base64

Show Base64 offsets

Fork

From Base32

From Base58

From Base85

Parse SSH Host Key

To Base32

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars ☐ Strict mode

STEP

BAKE!

Auto Bake

Input

start: 0
end: 48
length: 48

length: 48
lines: 1

TkhNMkl7SWwgZmF1dCBhdm9pciBkZSBib25uZXMGYmFzZXN9

Output

start: 0
end: 36
length: 36

time: 2ms
length: 36
lines: 1

NHM2I{Il faut avoir de bonnes bases}

avec Magic

Operations

magic

Magic

Image Brightness / Contrast

Detect File Type

Scan for Embedded Files

Favourites

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Recipe

Magic

Depth
3

☐ Intensive mode

☐ Extensive language support

Crib (known plaintext string or regex)

STEP

BAKE!

Auto Bake

Input

length: 48
lines: 1

TkhNMkl7SWwgZmF1dCBhdm9pciBkZSBib25uZXMGYmFzZXN9

Output

time: 37ms
length: 38822
lines: 1439

Recipe (click to load)	Result snippet	Properties
From Base64('A-Za-z0-9+/=',true,false)	NHM2I{Il faut avoir de bonnes bases}	Valid UTF8 Entropy: 4.23
From Base64('A-Za-z0-9_',true,false)	NHM2I{Il faut avoir de bonnes bases}	Valid UTF8 Entropy: 4.23
From Base64('A-Za-z0-9+\\.',true,false)	NHM2I{Il faut avoir de bonnes bases}	Valid UTF8 Entropy: 4.23

Le déchiffrement en lignes de commande

On utilise la commande

```
echo -ne TkhNMkl7SWwgZmF1dCBhdm9pciBkZSBib25uZXMGYmFzZXN9|base64  
# Flag{drapeau d'initiation}
```

Bonus

Source: <https://www.dcode.fr/code-base-64>

Qu'est-ce que l'encodage Base64 ?

Base64 est un codage informatique utilisant 64 caractères pour encoder n'importe quelle chaîne binaire avec du texte (il est notamment utilisé pour les emails).

Pourquoi utiliser la Base64 ?

Un message codé en Base64 contiendra uniquement des caractères ASCII imprimables
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=

Cette propriété permet de transmettre n'importe quelles données sur des systèmes originellement prévue pour ne transmettre que du texte (sans avoir à se soucier de l'encodage initial ni de la manière dont les caractères apparaîtront sur l'écran du destinataire du message)

Qu'est-ce que Base64URL ?

Base64URL est une variante de Base64 adaptée aux URL (http). Les caractères 62 + et 63 / peuvent poser des problèmes dans les URL, les remplacer alors par respectivement - et _. De plus, le = est quant à lui supprimé.

Quand Base64 a-t-il été inventé ?

La Norme RFC 2045 qui officialise Base64 date de 1996