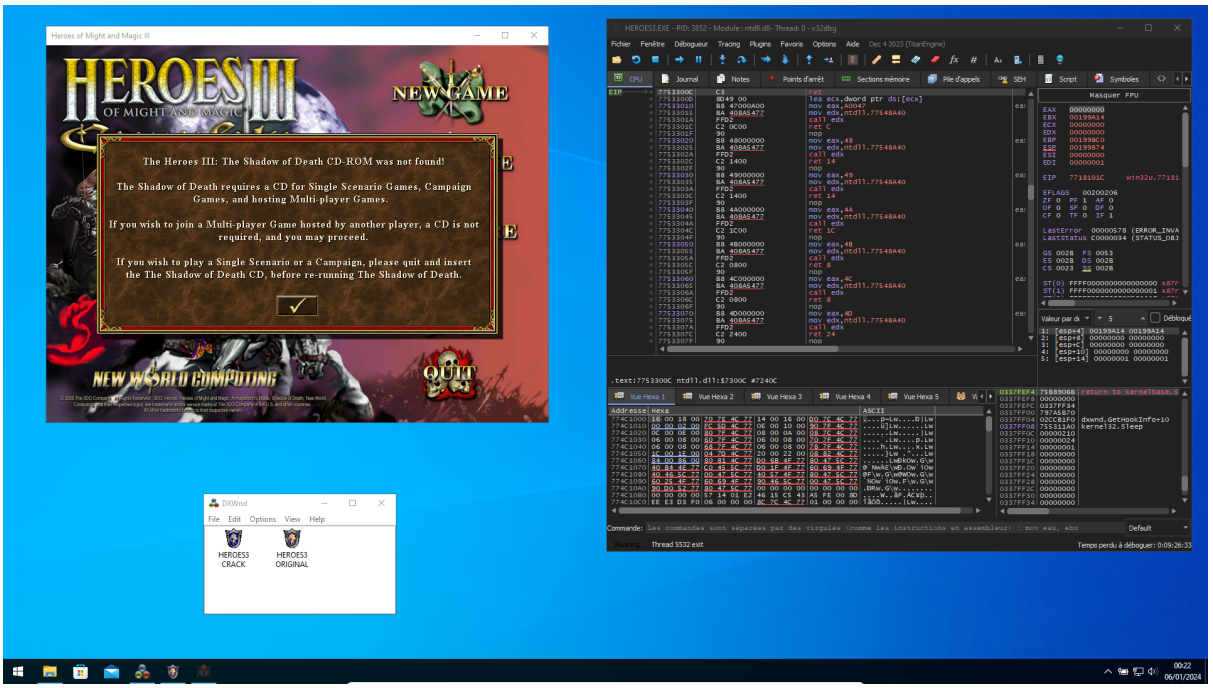
Writeup : Reverse engineering and cracking Heroes of Might and Magic III

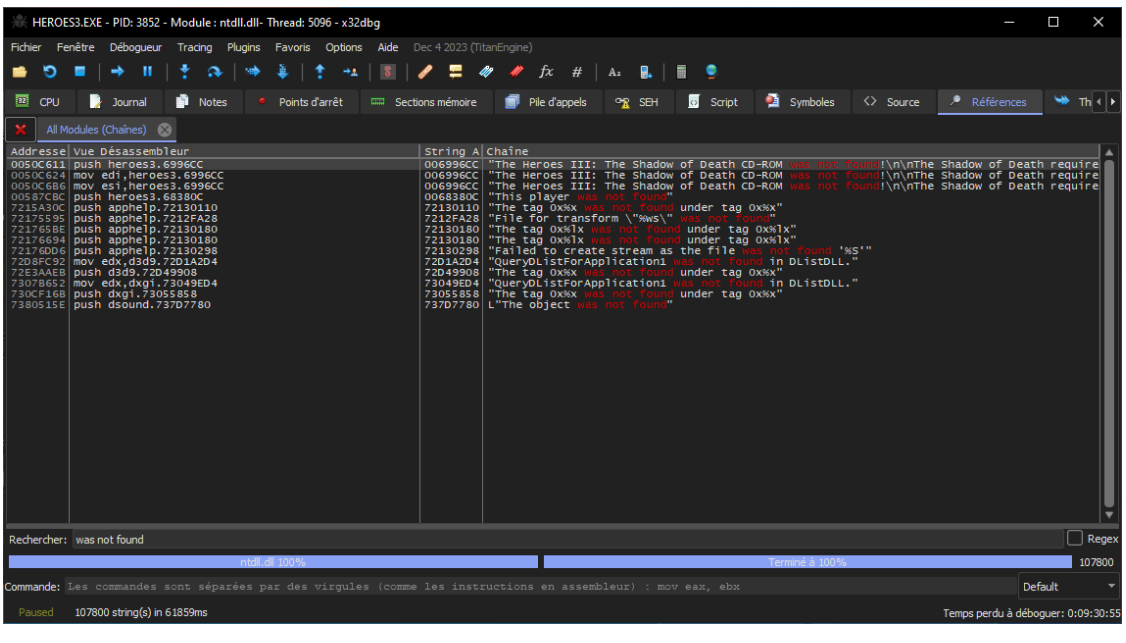
Setup :

- DXWind (pour lancer le jeu en fenêtré afin de pouvoir le déboguer plus facilement)
- x32dbg (Débogueur fait pour windows)



Étape 1 : Bypass CD ROM check pour jouer à la campagne

- Rechercher des références vers des chaînes de caractères présentes dans le message de début concernant la présence du CD.

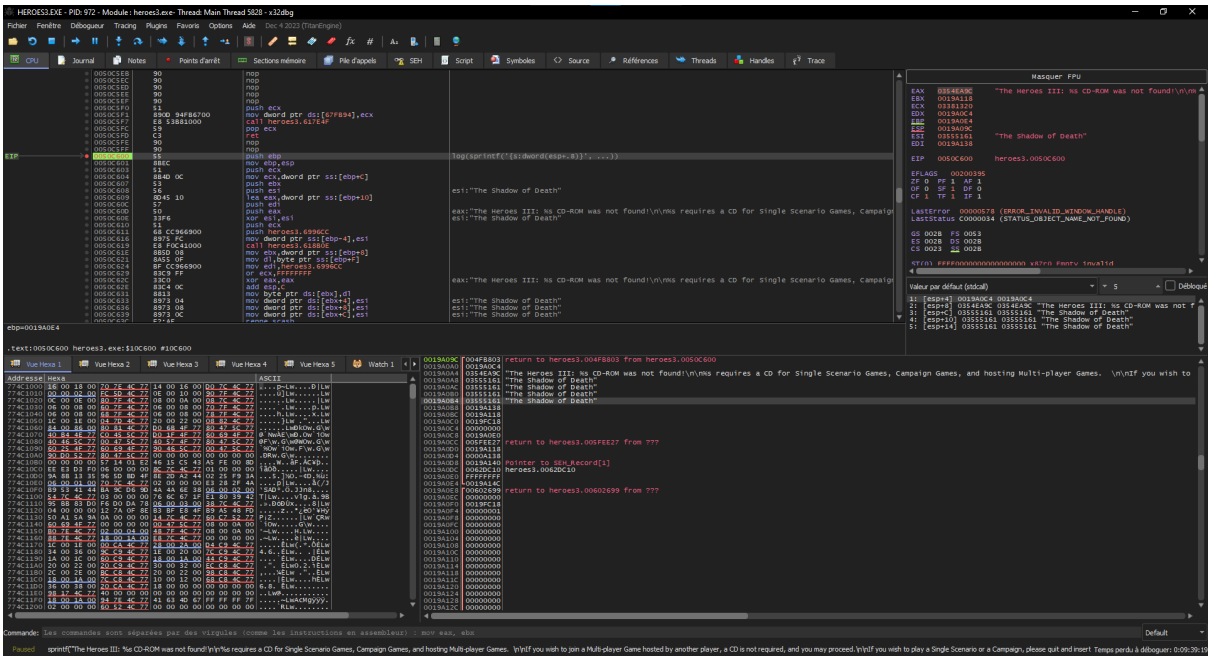


- Poser un breakpoint sur la fonction dans laquelle la chaîne de caractère a été trouvé afin que le programme se mette en pause lorsque cette fonction est appelée.

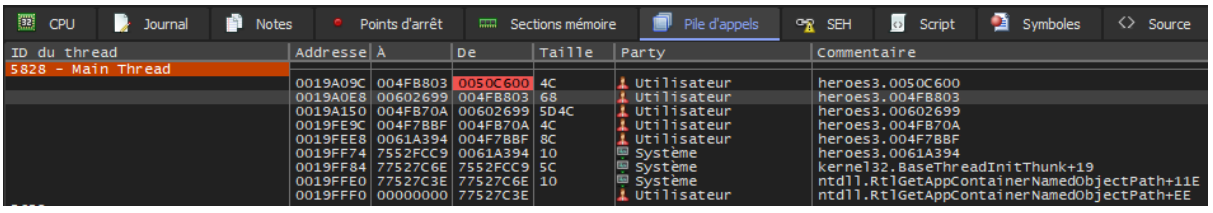
"The Heroes III: The Shadow of Death CD-ROM was not found!\n\nThe Shadow of Death requires a CD for Single Scenario Games, Campaign Games, and hosting Multi-player Games. \n\nIf you wish to join a Multi-player Game hosted by another player, a CD is not required, and you may proceed.\n\nIf you wish to play a Single Scenario or a Campaign, please quit and insert the The Shadow of Death CD, before re-running The Shadow of Death."

- Relancer le jeu, car la fonction n'est appelée qu'une seule fois. Après avoir relancé, nous atteignons le breakpoint avant que le message s'affiche.

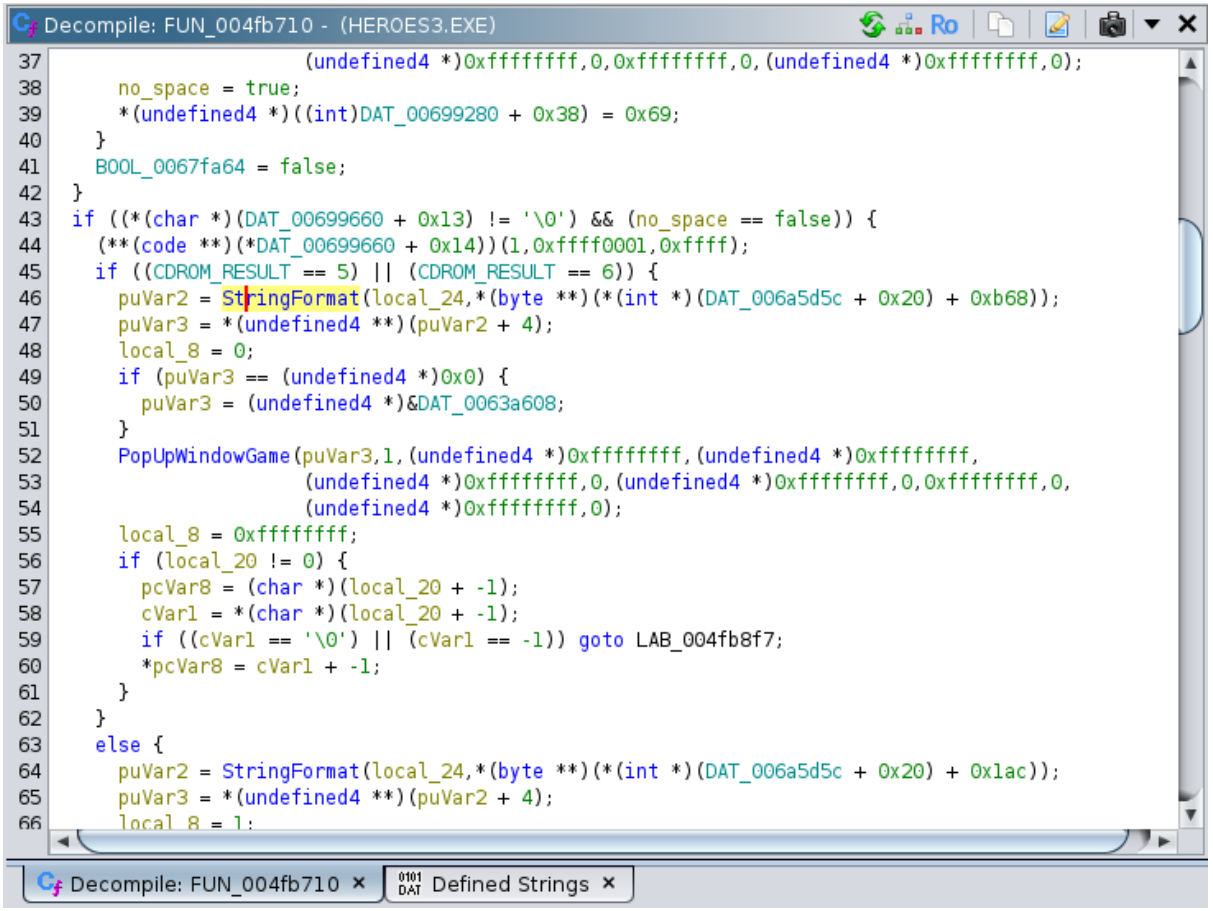
- Quand on regarde les paramètres passés dans cette fonction (dans la stack) on aperçoit que le premier paramètre est une format string et que les paramètres suivants sont les valeurs à formater, ce qui peut nous laisser penser que cette fonction est une fonction de type sprintf / string formatting.



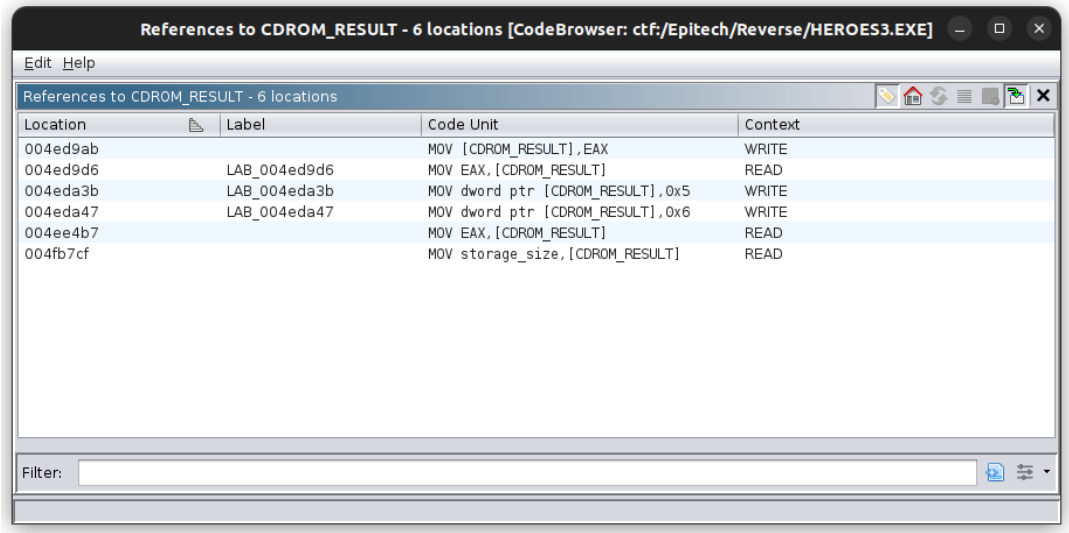
- Ensuite nous regardons la pile d'appels pour voir où est-ce que notre fonction est appelée et nous rendre dans la fonction d'appel.



- Nous analysons donc cette fonction dans Ghidra et nous nous rendons compte qu'après notre fonction de formatage de chaîne de caractères, une autre fonction est appelée (PopUpWindowGame dans notre screen, renommé ici pour plus de clarté) qui est la fonction qui fait apparaître la fenêtre qui nous dit que le jeu solo est accessible uniquement avec le CD ROM.
- Dans ce même screen nous pouvons apercevoir que l'apparition de la popup dépend d'une condition sur une variable globale (ici renommée CDROM_RESULT). Après avoir récupéré l'adresse de cette variable globale nous regardons les références qui lui sont faites dans Ghidra.



- Il y a donc 3 accès à cette variable globale en écriture dans le code du jeu que nous allons patcher avec des instructions NOP (instruction qui ne fait rien),



- Après avoir patch le code du jeu et relancé le programme nous pouvons voir que la popup n'apparaît plus et que nous avons accès à toutes les fonctionnalités du jeu en solo.

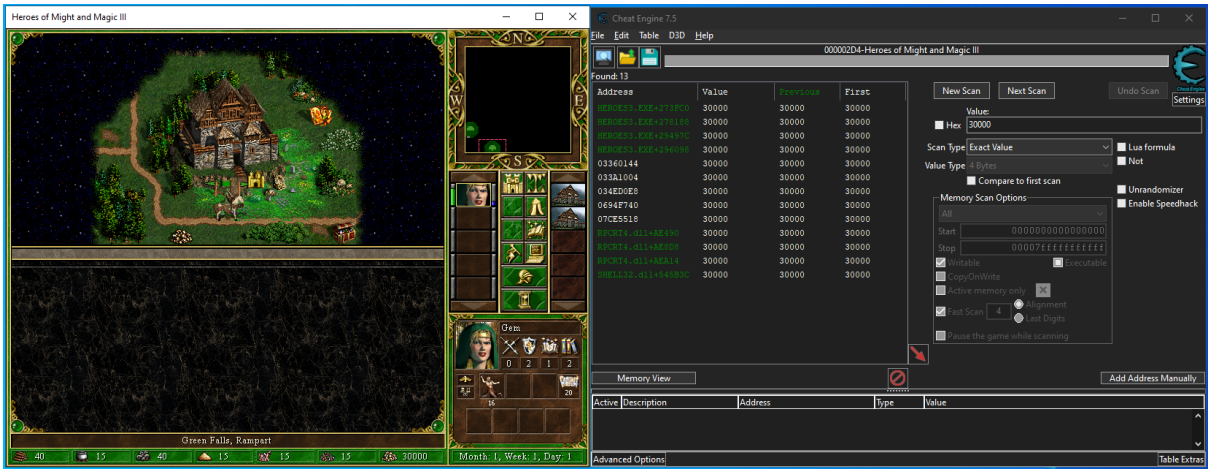
Nous allons maintenant passer à l’étape 2 qui consiste à tricher sur le jeu.

Étape 2 : Trichons avec Cheat Engine.

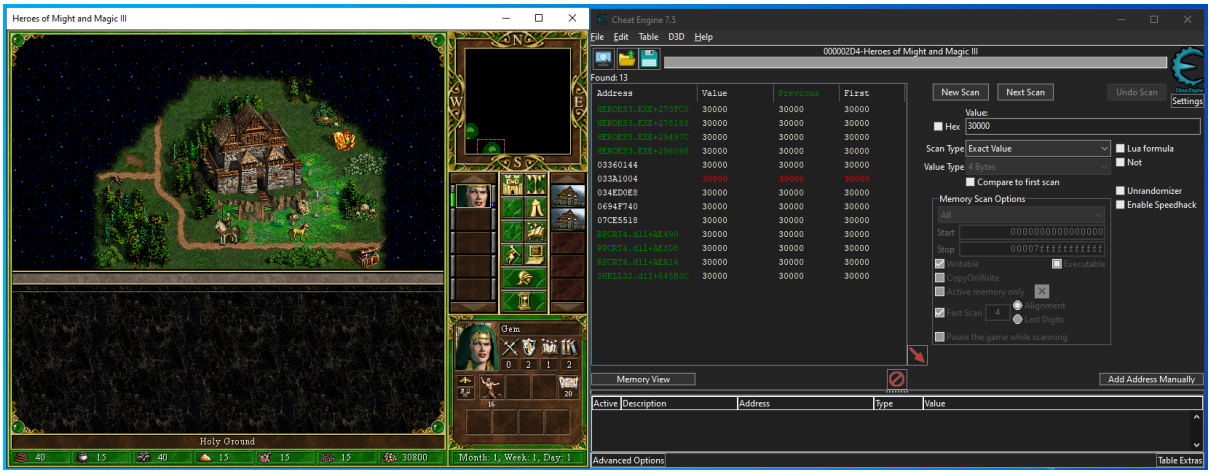
- Pour le début de cette étape nous téléchargeons donc Cheat Engine qui nous permettra de scanner et modifier la mémoire du programme en temps réel.

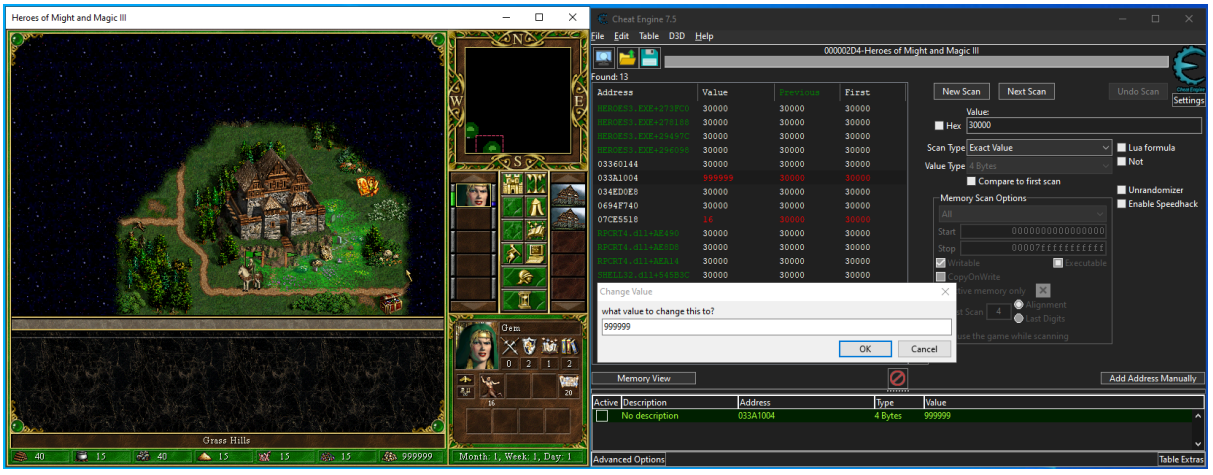
1. Known initial values cheat.

    - On peut s’apercevoir au lancement de la campagne “Shadow of Death” en difficulté la plus simple que nous avons 30000 golds pour commencer. Nous faisons donc une recherche de valeur sur Cheat Engine avec ce fameux 30000. Nous en avons plusieurs.



- Pour déterminer laquelle de ces valeurs est à modifier nous allons looter des golds dans le jeu afin de voir laquelle des ces valeurs change. Et nous pouvons voir qu'une seule valeur change. Nous pouvons donc conclure que cette valeur représente bien nos golds. Et après modification de cette valeur nous avons donc le montant de golds en jeu qui a bien été changé.

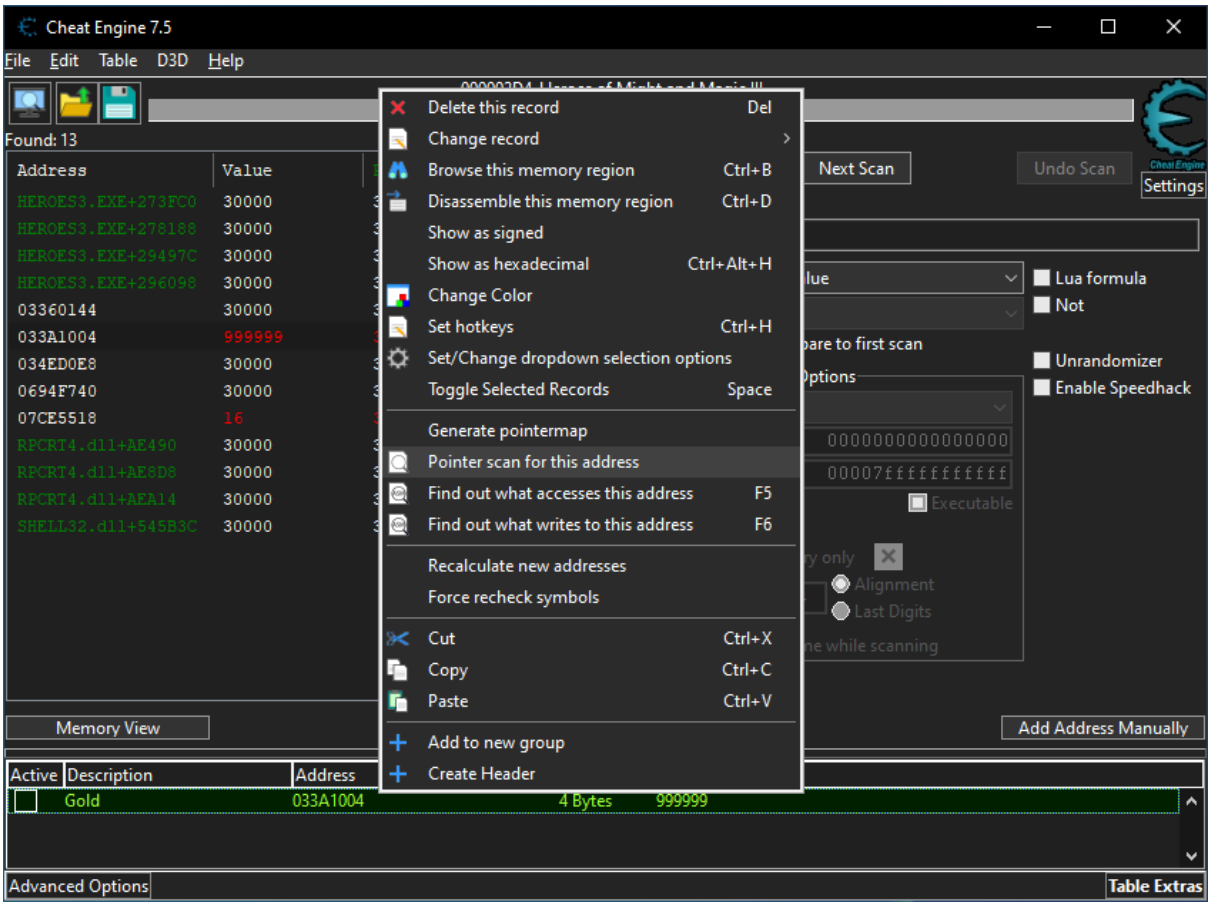




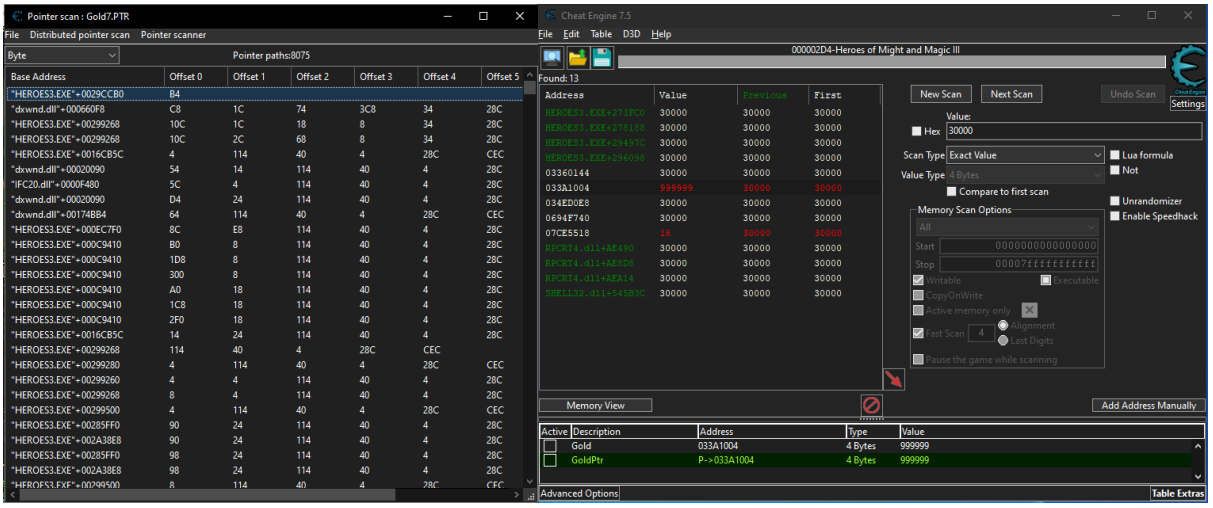
- Nous utilisons donc cette méthode pour trouver toutes nos variables connues. (bois, mercure, minerai, sulfure, cristal, gemmes et pour finir les golds).

2. Rendre le cheat persistant.

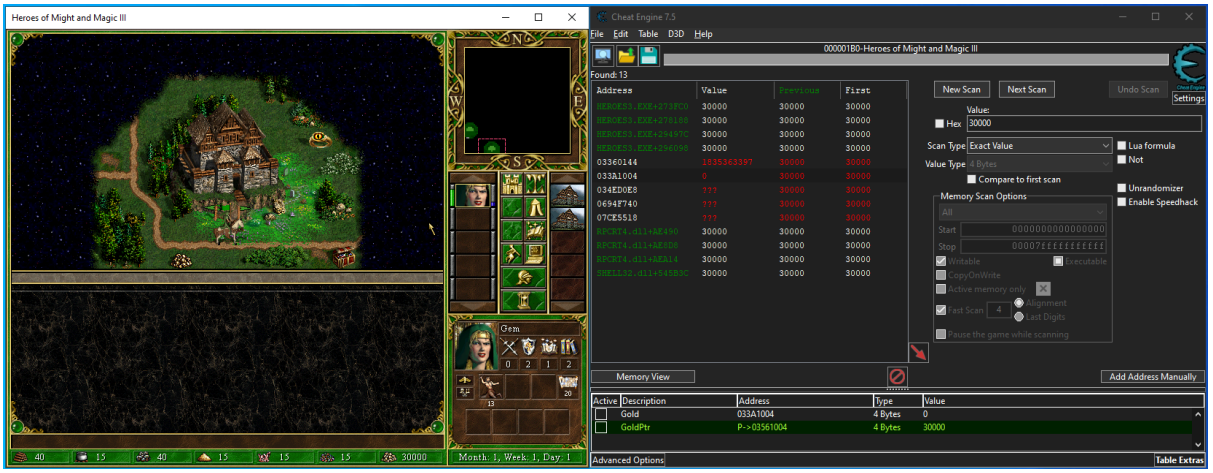
- Ensuite nous devons trouver un pointeur (qui ne change jamais) sur ces variables afin que nous puissions modifier ces valeurs même lors du redémarrage du jeu, car actuellement nos adresses mémoires sont des adresses qui changent à chaque redémarrage du programme. et pour faire ceci nous allons donc faire un scan de pointeur pour cette adresse (l'adresse des golds pour notre exemple).



- Après ce scan nous trouvons donc le pointeur et nous double cliquons dessus pour l'ajouter dans la liste des adresses.

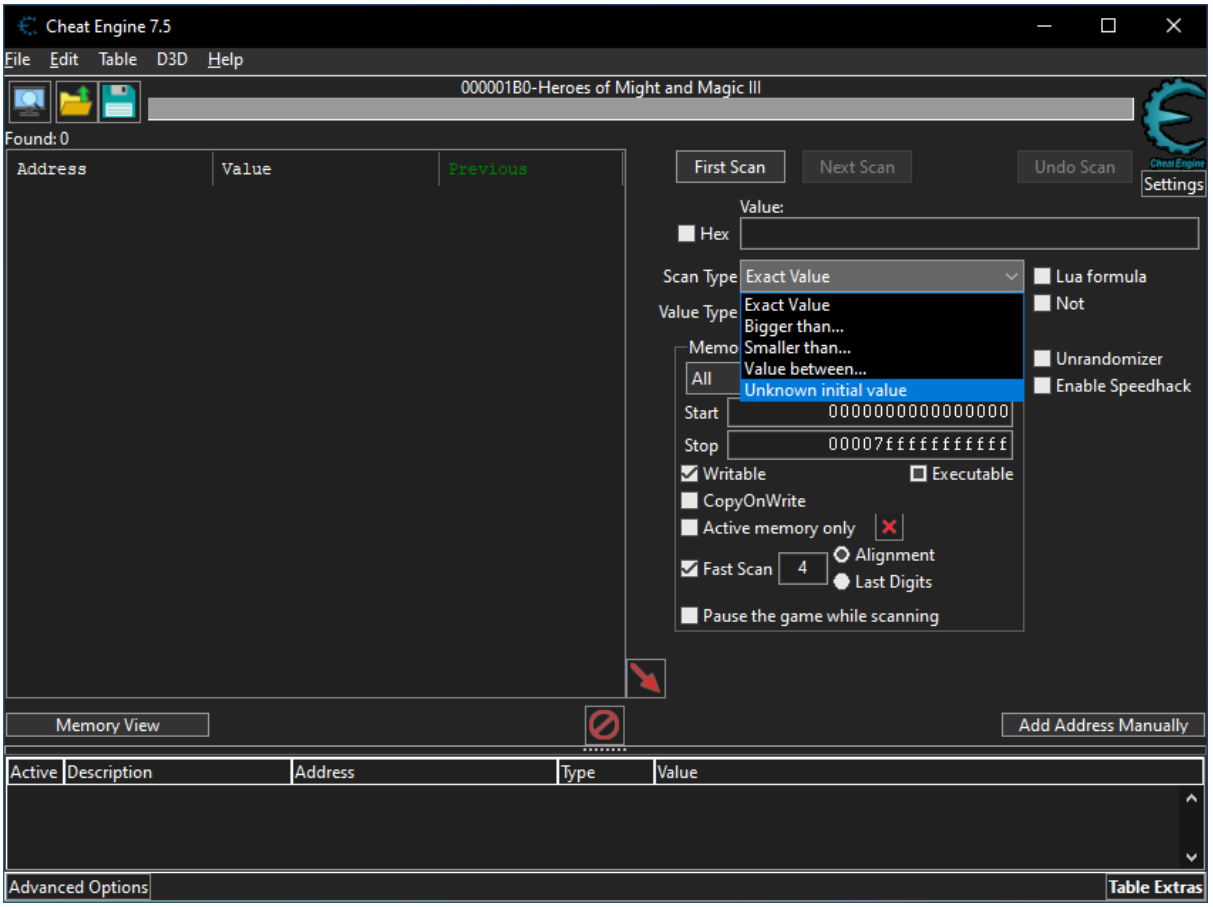


- Pour vérifier, nous redémarrons le jeu et constatons que l'ancienne adresse des golds n'affiche plus la bonne valeur tandis que le pointeur vers les golds et la valeur des golds restent inchangés. Nous appliquons donc cette étape à toutes les valeurs que nous avons récupérées auparavant.

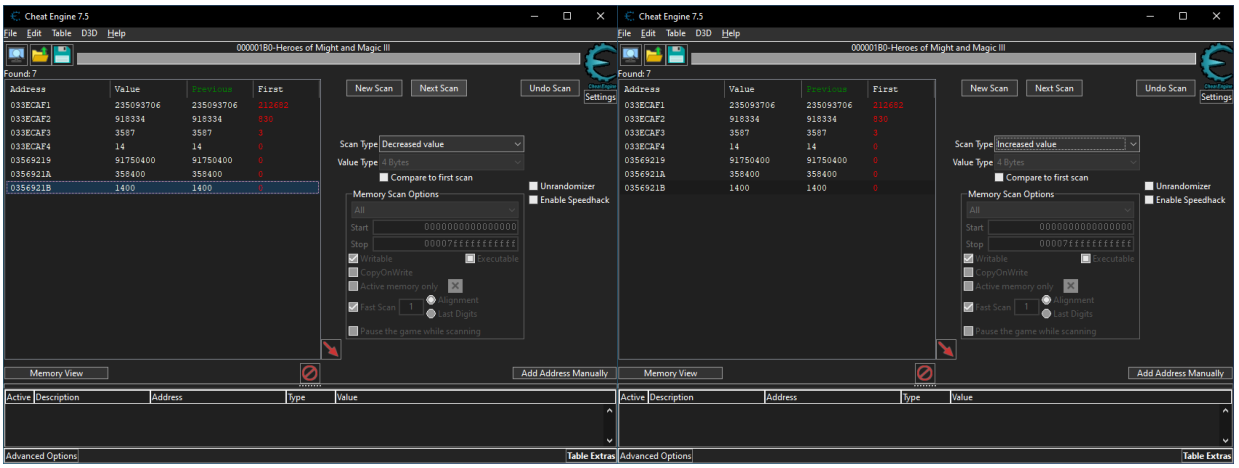


3. Unknown value cheat

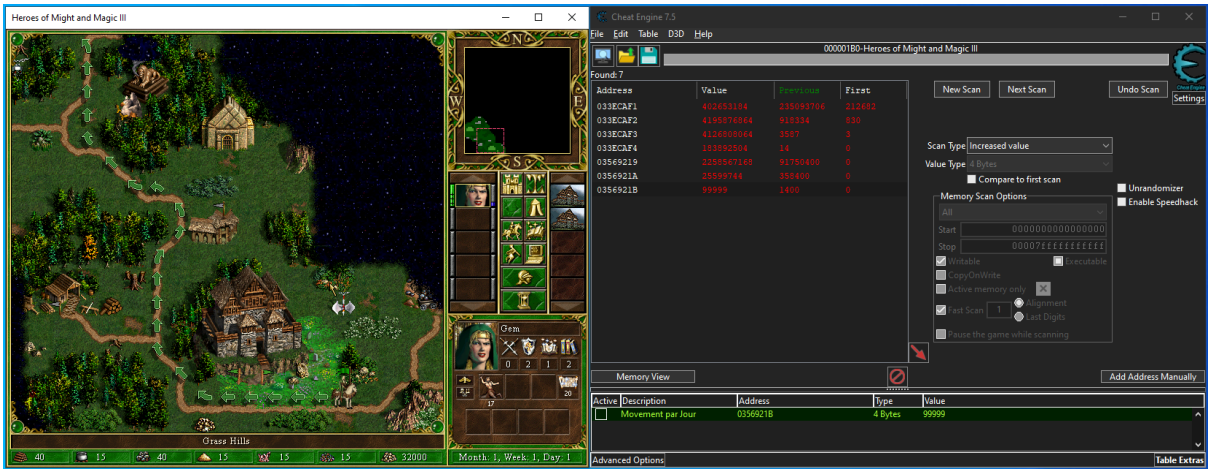
- Pour ceci nous allons donc tenter de changer la valeur des mouvements possibles par jour. Pour ceci, nous supposons que cette valeur décrémente à chaque mouvement de notre joueur et revient à la valeur initiale lorsque nous changeons de jour.
- Pour le premier scan nous cherchons donc une unknown initial value.



- Après le scan initial nous avons déplacé notre joueur d'une case et filtré toutes les valeurs ayant décrémentées. Nous épuisons les mouvements du joueur petit à petit tout en relançant des scans pour filtrer le maximum de valeurs possibles. Ensuite lorsque nous changeons de jour nous filtrons celles qui ont incrémentées, car lors du changement de jour la valeur des mouvements remonte.



- Pour finir nous tombons sur 7 valeurs que nous ne pouvons plus filtrer. Nous les changeons une par une jusqu'à tomber sur la bonne valeur à changer pour avoir nos mouvements illimités !



Étape 3 : Frida

- Pour cette étape, nous allons importer tous les pointeurs sur nos valeurs trouvés durant l'étape 2 et nous allons l'utiliser pour récupérer les différentes ressources dans le jeu en temps réel.

Bonus : Cheat interactif avec Frida