Quick Write Up: Track Layer Cake

FCSC 2024 - Yxène

Layer Cake 1/3 - Énoncé - intro

Description

Un développeur de GoodCorp souhaite publier une nouvelle image Docker. Il utilise une variable d'environnement stockant un flag au moment du build, et vous assure que ce secret n'est pas visible du public. L'image est `anssi/fcsc2024-forensics-layer-cake-1`.

Récupérez ce flag et prouvez-lui le contraire.

Cette épreuve fait partie d'une serie :

- Layer Cake 1/3.
- Layer Cake 2/3.
- Layer Cake 3/3.

Auteur

nop

Docker ?

Qu’est ce que Docker ?

- Outil qui permet de créer, déployer et exécuter des applications dans des conteneurs.
- Permet de standardiser et isoler les environnements d’exécution.
- Plus léger et plus rapide que les machines virtuelles.

Vocabulaire Docker

- **Conteneur** : Environnement léger, isolé, qui contient tout ce qu'il faut pour exécuter une application (code, bibliothèques, dépendances).
- **Image**: Modèle à partir duquel on crée des conteneurs.
- **Dockerfile** : Fichier de configuration pour construire une image. Il décrit étape par étape comment préparer l'environnement.
- **Docker Hub** : Registre d'images Docker (comme GitHub, mais pour images de conteneurs).

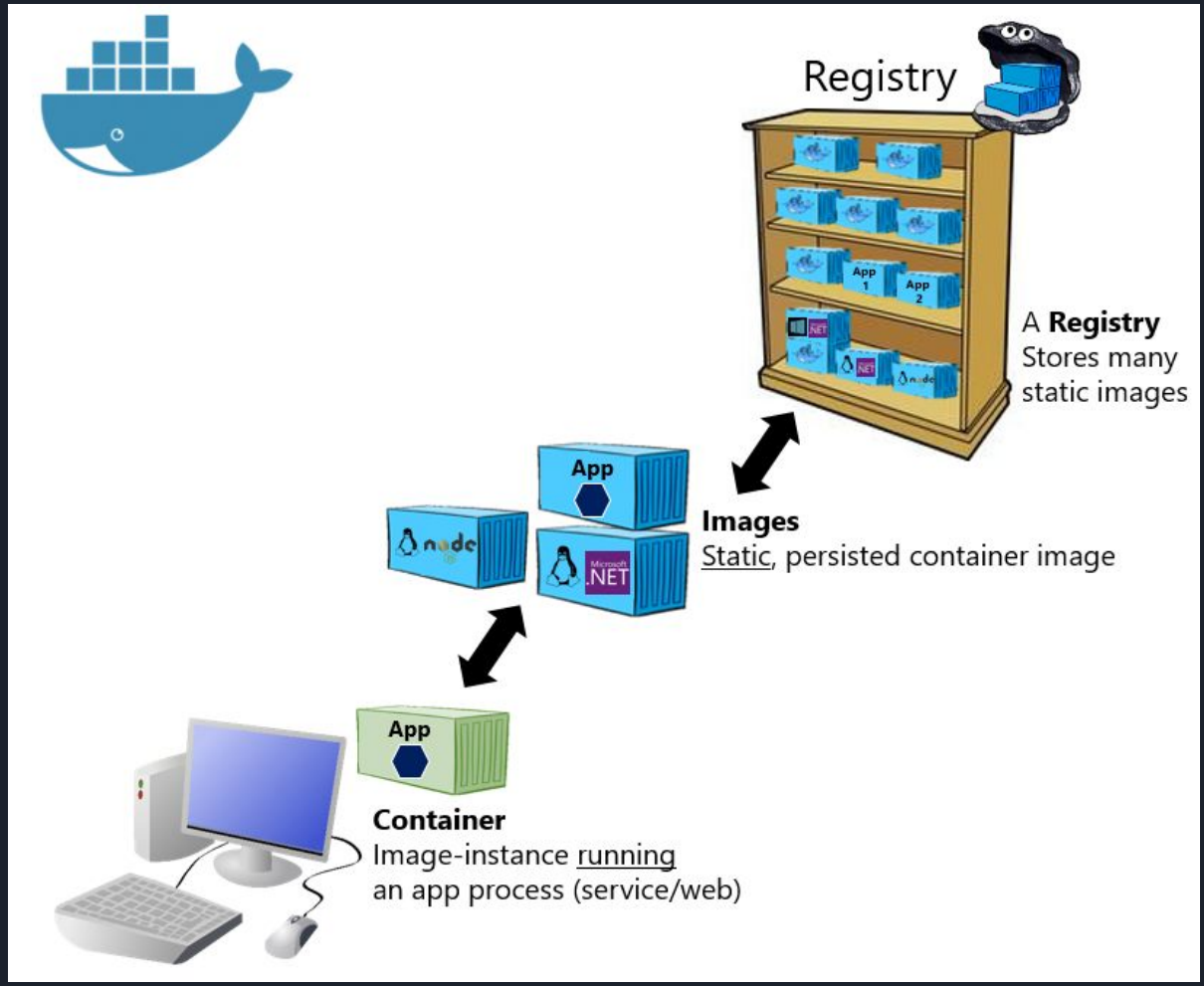


Schéma Docker

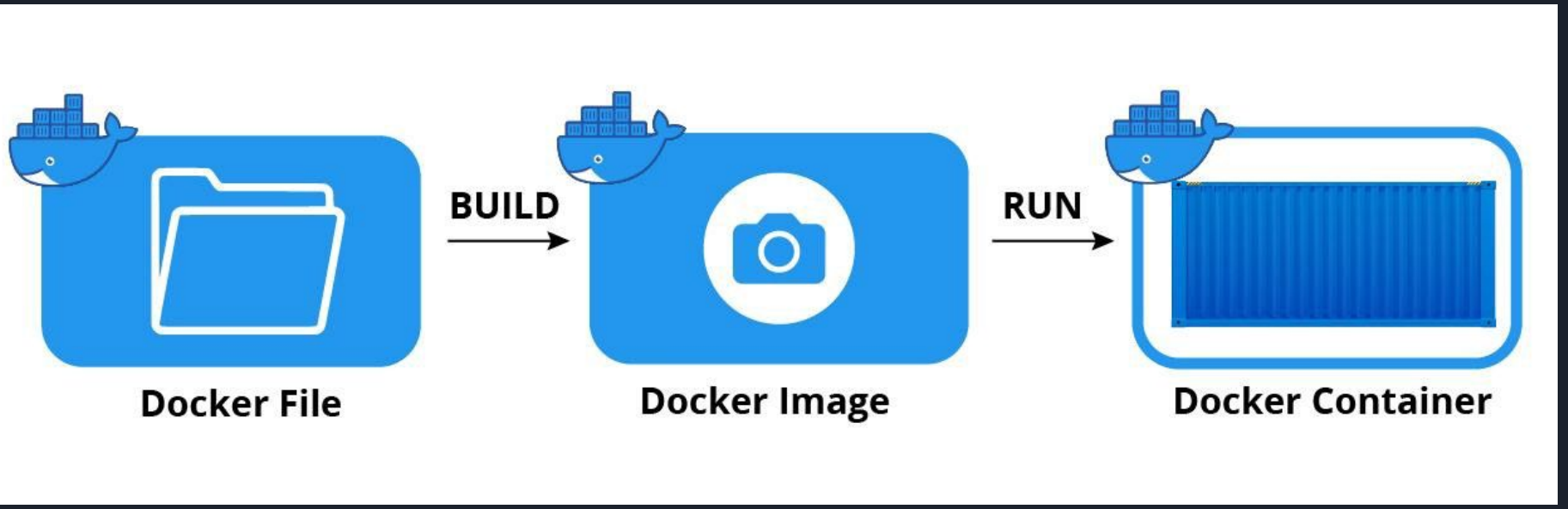
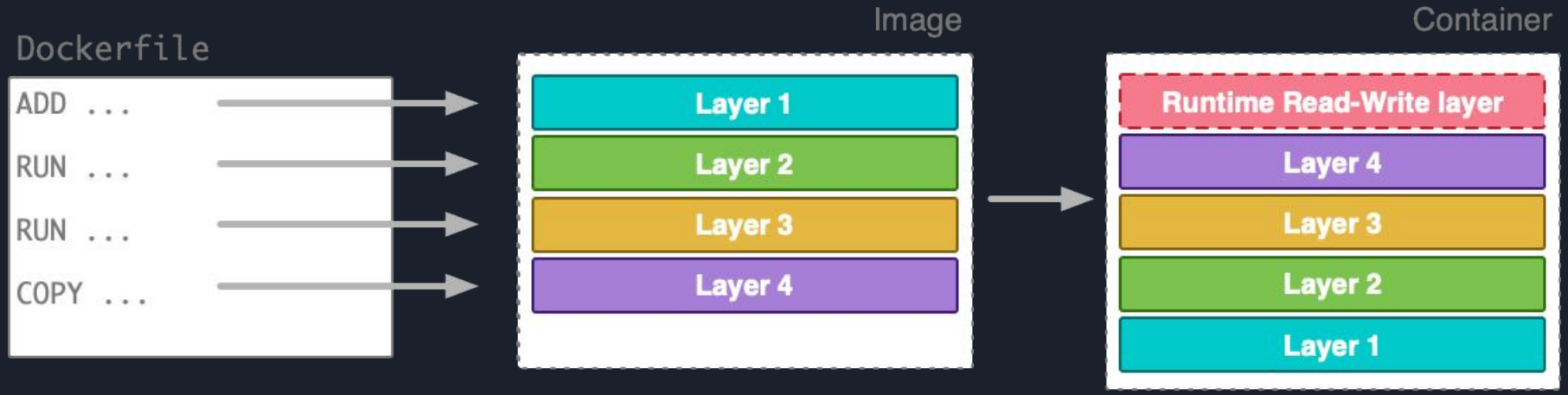


Schéma Docker

Images Docker

Architecture en couches *(layers)*



Dock

ADD .

RUN .

RUN .

COPY

ainer

er

Layer Cake 1/3 - Énoncé - intro

Description

Un développeur de GoodCorp souhaite publier une nouvelle image Docker. Il utilise une variable d'environnement stockant un flag au moment du build, et vous assure que ce secret n'est pas visible du public. L'image est `anssi/fcsc2024-forensics-layer-cake-1`.

Récupérez ce flag et prouvez-lui le contraire.

Cette épreuve fait partie d'une serie :

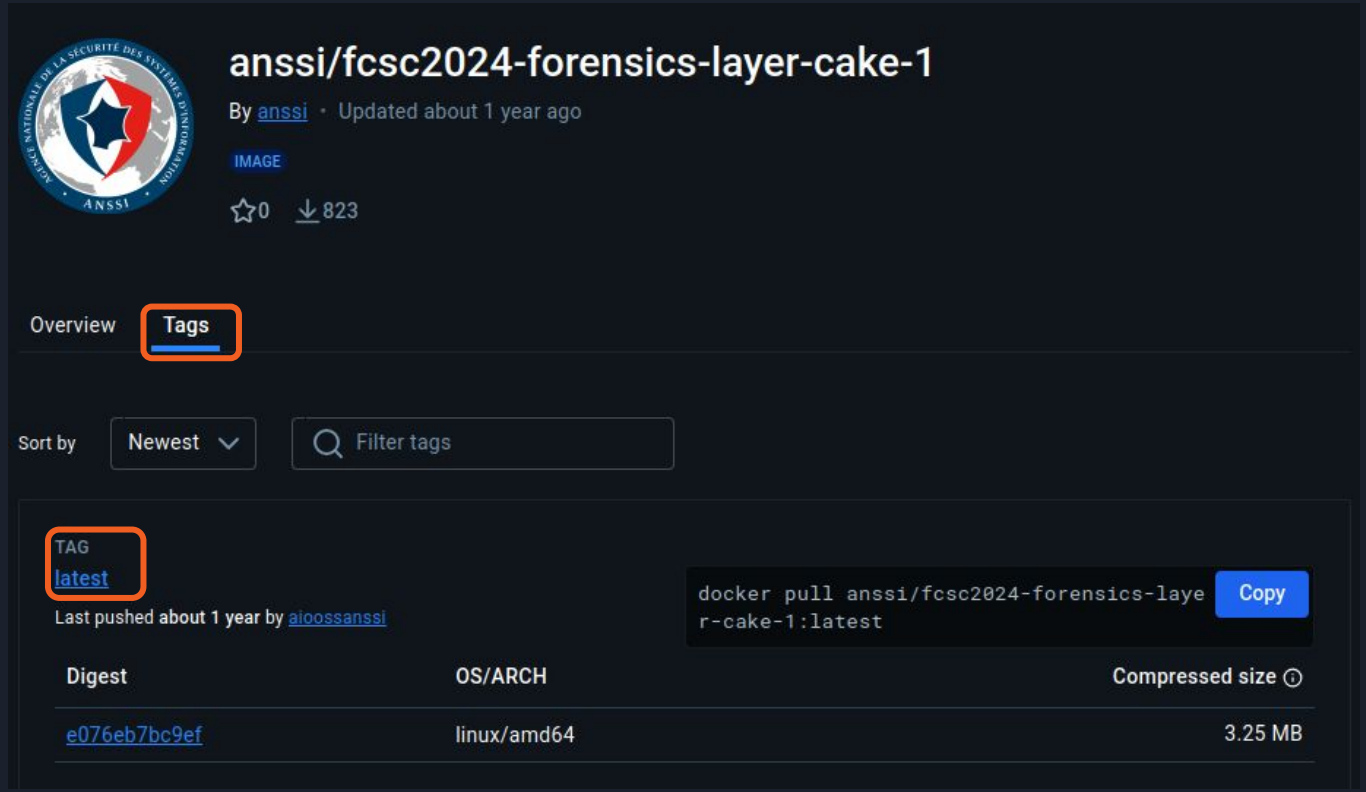
- Layer Cake 1/3.
- Layer Cake 2/3.
- Layer Cake 3/3.

Auteur

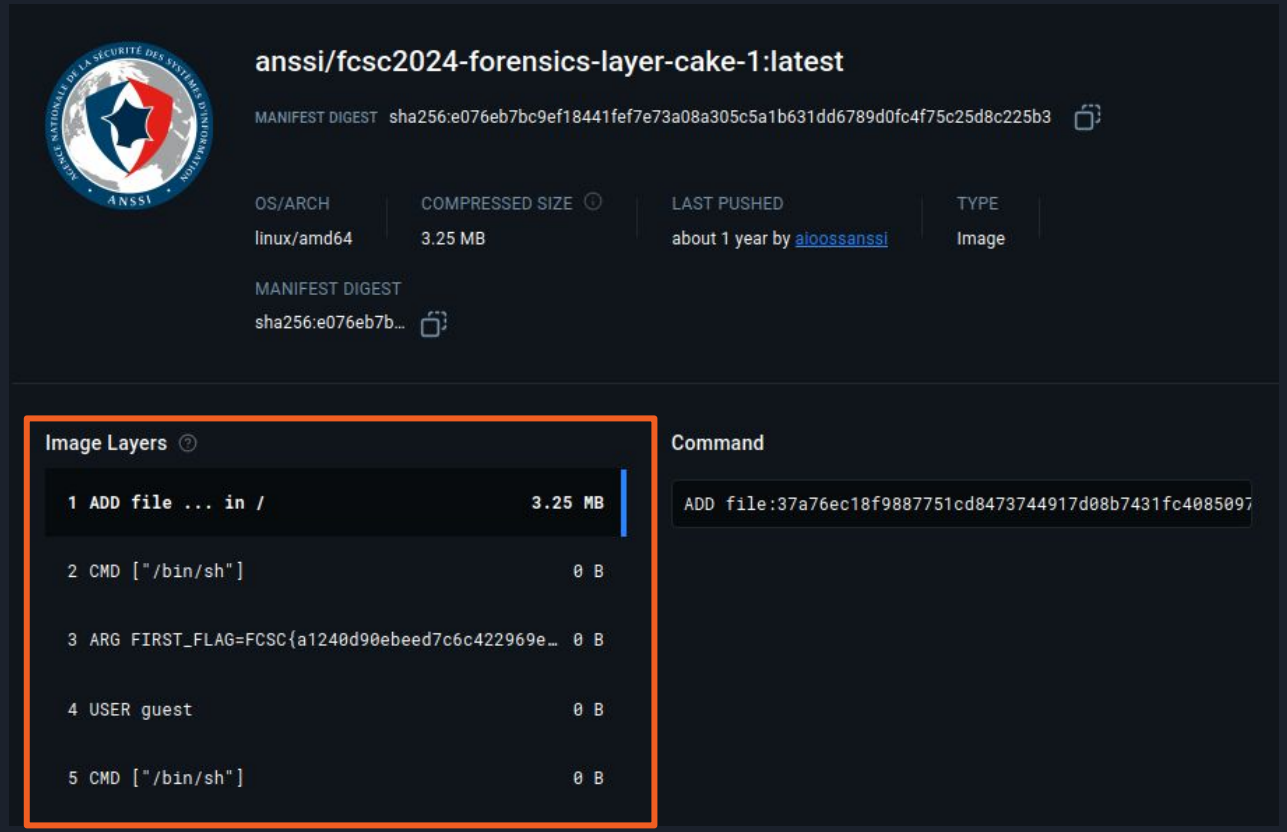
nop

Layer Cake 1/3 - Docker Hub

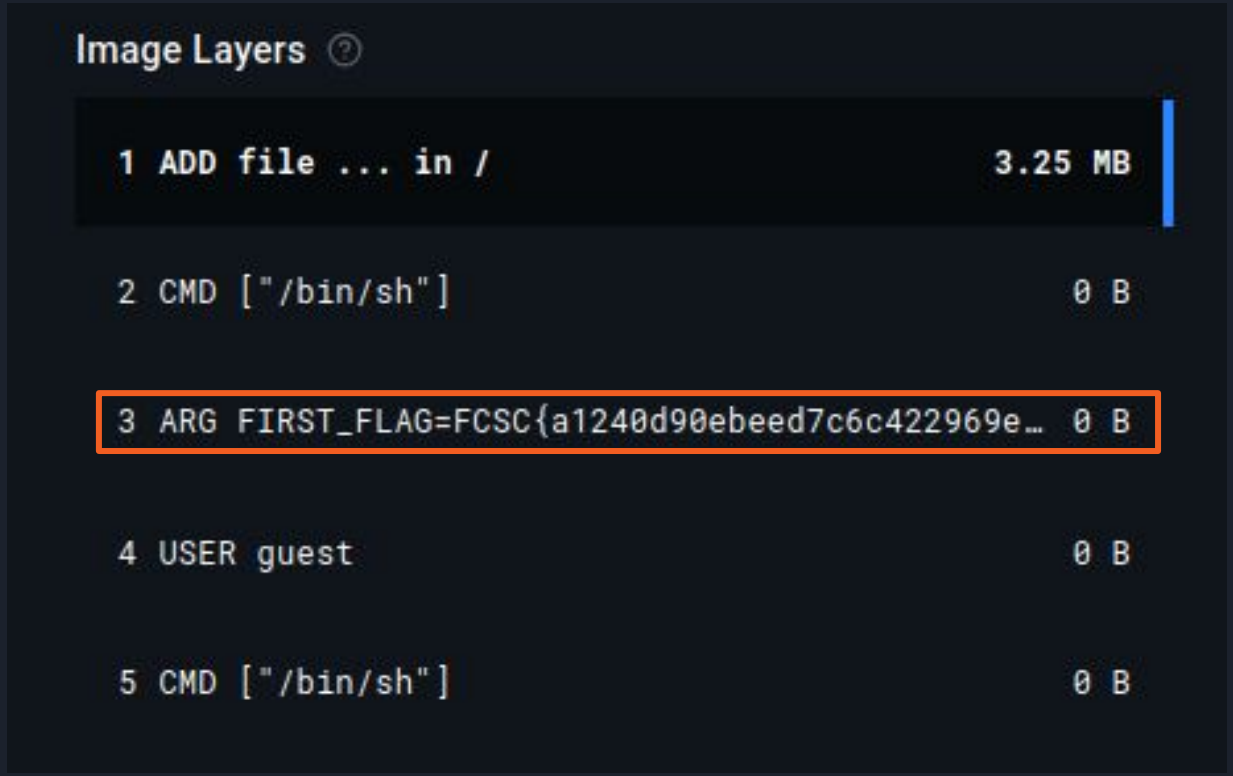
Layer Cake 1/3 - Docker Hub



Layer Cake 1/3 - Docker Hub



Layer Cake 1/3 - Docker Hub



Layer Cake 2/3 - Énoncé - intro

Description

Un développeur de GoodCorp souhaite publier une nouvelle image Docker. Il copie au moment du build un fichier contenant un flag, puis le supprime. Il vous assure que ce secret n'est pas visible du public. L'image est `anssi/fcsc2024-forensics-layer-cake-2`.

Récupérez ce flag et prouvez-lui le contraire.

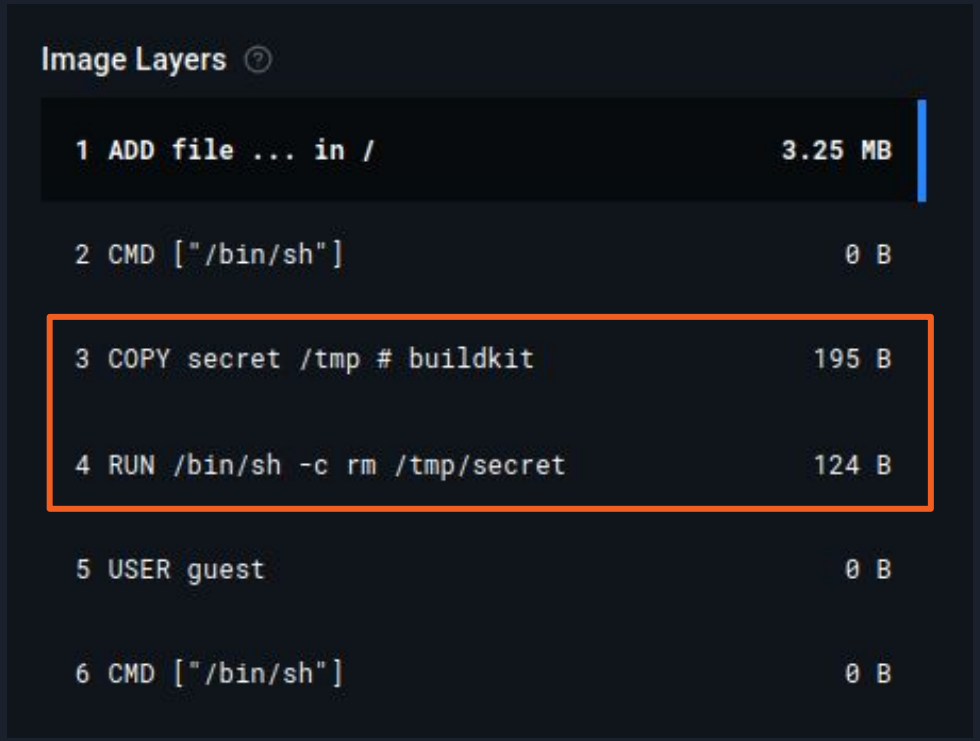
Cette épreuve fait partie d'une serie :

- Layer Cake 1/3.
- Layer Cake 2/3.
- Layer Cake 3/3.

Auteur

nop

Layer Cake 2/3 - Docker Hub



Téléchargement de l’image Docker

```
docker pull anssi/fcsc2024-forensics-layer-cake-2
```

Conversion de l’image en archive tar

```
docker save anssi/fcsc2024-forensics-layer-cake-2 -o layercake2.tar.gz
```

Contenu de l’archive

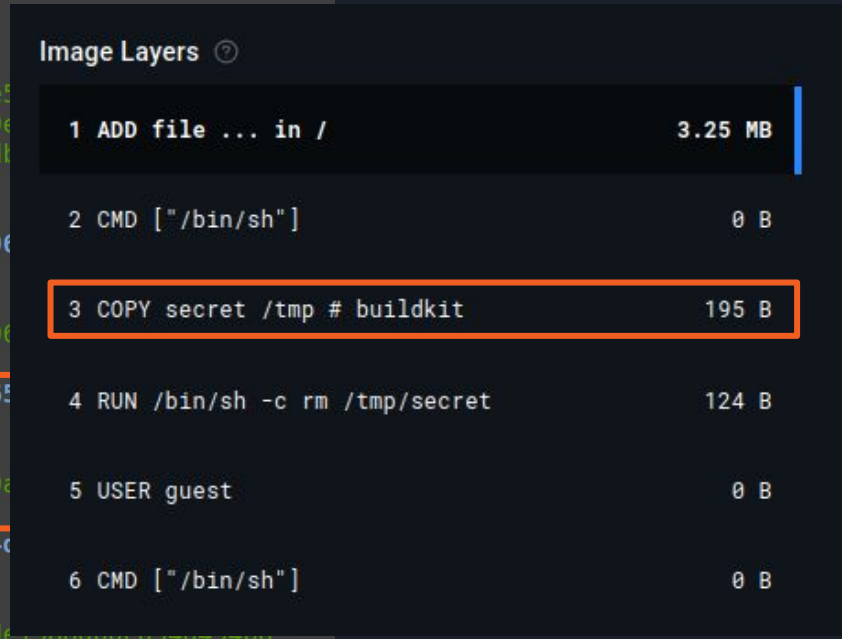
```
layercake2:
blobs  index.json  manifest.json  oci-layout  repositories

layercake2/blobs:
sha256

layercake2/blobs/sha256:
03014d9fc4801b1810b112fd53e05e35ea127e55c82d1304b5622cfe257c0ad8
aa6a5e1de1984008d10132de21845c0fa3c4e07be027ce81fa90e0763dae188c
faa3fc90c95f81da62416cc55e178d89a69f69e15d2d946fc332b6fb5f6f903e
7cf5cccfa50aed470d1c6857ba3e20bc2f337d5549e5801b2e93c3fabef03959
d4fc045c9e3a848011de66f34b81f052d4f2c15a17bb196d637e526349601820
fe62c480fd0c4bba858571806e7474fa5aa061ce78292de1988db0cd54d494b6
a1fadde3873bbcd604a1526f9e3cea2c974c13c2a1dbb8832102c89f4d4eafc5
eebed19322aaa0082058596cc4cff6c33253f1ce4327e9ae4399edb2f657242e
```

manifest.json


```
[
  {
    "Config": "blobs/sha256/03014d9fc4801b1810b112fd53e05e35ea127e55c82d1304b5622cfe257c0ad8",
    "RepoTags": [
      "anssi/fcsc2024-forensics-layer-cake-2:latest"
    ],
    "Layers": [
      "blobs/sha256/d4fc045c9e3a848011de66f34b81f052d4f2c15a17bb196d637e526349601820",
      "blobs/sha256/eebed19322aaa0082058596cc4cff6c33253f1ce4327e9ae4399edb2f657242e",
      "blobs/sha256/fe62c480fd0c4bba858571806e7474fa5aa061ce78292de1988db0cd54d494b6"
    ],
    "LayerSources": {
      "sha256:d4fc045c9e3a848011de66f34b81f052d4f2c15a17bb196d637e526349601820": {
        "mediaType": "application/vnd.oci.image.layer.v1.tar",
        "size": 7667200,
        "digest": "sha256:d4fc045c9e3a848011de66f34b81f052d4f2c15a17bb196d637e526349601820"
      },
      "sha256:eebed19322aaa0082058596cc4cff6c33253f1ce4327e9ae4399edb2f657242e": {
        "mediaType": "application/vnd.oci.image.layer.v1.tar",
        "size": 2560,
        "digest": "sha256:eebed19322aaa0082058596cc4cff6c33253f1ce4327e9ae4399edb2f657242e"
      },
      "sha256:fe62c480fd0c4bba858571806e7474fa5aa061ce78292de1988db0cd54d494b6": {
        "mediaType": "application/vnd.oci.image.layer.v1.tar",
        "size": 2048,
        "digest": "sha256:fe62c480fd0c4bba858571806e7474fa5aa061ce78292de1988db0cd54d494b6"
      }
    }
  }
]
```

manifest.json


```
[
  {
    "Config": "blobs/sha256/03014d9fc4801b1810b112fd53e05e35ea127e55c82d1304b5622cfe257c0ad8",
    "RepoTags": [
      "anssi/fcsc2024-forensics-layer-cake-2:latest"
    ],
    "Layers": [
      "blobs/sha256/d4fc045c9e3a848011de66f34b81f052d4f2c15a17bb196d637e5
      "blobs/sha256/eebed19322aaa0082058596cc4cff6c33253f1ce4327e9ae4399e
      "blobs/sha256/fe62c480fd0c4bba858571806e7474fa5aa061ce78292de1988db
    ],
    "LayerSources": {
      "sha256:d4fc045c9e3a848011de66f34b81f052d4f2c15a17bb196d637e526349
        "mediaType": "application/vnd.oci.image.layer.v1.tar",
        "size": 7667200,
        "digest": "sha256:d4fc045c9e3a848011de66f34b81f052d4f2c15a17bb19
      },
      "sha256:eebed19322aaa0082058596cc4cff6c33253f1ce4327e9ae4399edb2f5
        "mediaType": "application/vnd.oci.image.layer.v1.tar",
        "size": 2560,
        "digest": "sha256:eebed19322aaa0082058596cc4cff6c33253f1ce4327e9a
      },
      "sha256:fe62c480fd0c4bba858571806e7474fa5aa061ce78292de1988db0cd54c
        "mediaType": "application/vnd.oci.image.layer.v1.tar",
        "size": 2048,
        "digest": "sha256:fe62c480fd0c4bba858571806e7474fa5aa061ce78292de1988db0cd54d454b0
      }
    }
  }
]
```

manifest.json


```
[
  {
    "Config": "blobs/sha256/03014d9fc4801b1810b112fd53e05e35ea127e55c82d1304b5622cfe257c0ad8",
    "RepoTags": [
      "anssi/fcsc2024-forensics-layer-cake-2:latest"
    ],
    "Layers": [
      "blobs/sha256/d4fc045c9e3a848011de66f34b81f052d4f2c15a17bb196d637e526349601820",
      "blobs/sha256/eebed19322aaa0082058596cc4cff6c33253f1ce4327e9ae4399edb2f657242e",
      "blobs/sha256/fe62c480fd0c4bba858571806e7474fa5aa061ce78292de1988db0cd54d494b6"
    ],
    "LayerSources": {
      "sha256:d4fc045c9e3a848011de66f34b81f052d4f2c15a17bb196d637e526349601820": {
        "mediaType": "application/vnd.oci.image.layer.v1.tar",
        "size": 7667200,
        "digest": "sha256:d4fc045c9e3a848011de66f34b81f052d4f2c15a17bb196d637e526349601820"
      },
      "sha256:eebed19322aaa0082058596cc4cff6c33253f1ce4327e9ae4399edb2f657242e": {
        "mediaType": "application/vnd.oci.image.layer.v1.tar",
        "size": 2560,
        "digest": "sha256:eebed19322aaa0082058596cc4cff6c33253f1ce4327e9ae4399edb2f657242e"
      },
      "sha256:fe62c480fd0c4bba858571806e7474fa5aa061ce78292de1988db0cd54d494b6": {
        "mediaType": "application/vnd.oci.image.layer.v1.tar",
        "size": 2048,
        "digest": "sha256:fe62c480fd0c4bba858571806e7474fa5aa061ce78292de1988db0cd54d494b6"
      }
    }
  }
]
```

Extraction de la couche souhaitée

```
tar xvf
layercake2/blobs/sha256/eebed19322aaa0082058596cc4cff6c33
253f1ce4327e9ae4399edb2f657242
```

```
tmp/
tmp/secret
```

Deuxième flag

```
cat tmp/secret
```

```
FCSC{b38095916b2b578109cbf35b8be713b04a64b2b2df6d73259…}
```

Layer Cake 3/3 - Énoncé - intro

Description

Un développeur de GoodCorp souhaite publier une nouvelle image Docker. Suite à ses mésaventures avec les Dockerfile, il décide d'utiliser Nix pour construire son image. En utilisant Nix, il donne un flag en argument à un service. Il vous assure que ce secret n'est pas visible du public. L'image est `anssi/fcsc2024-forensics-layer-cake-3`.

Récupérez ce flag et prouvez-lui le contraire.

Cette épreuve fait partie d'une serie :

- Layer Cake 1/3.
- Layer Cake 2/3.
- Layer Cake 3/3.

Auteurs

nop

erdnaxe

Layer Cake 3/3 - Docker Hub

Image Docker → archive

```
docker pull anssi/fcsc2024-forensics-layer-cake-3
docker save anssi/fcsc2024-forensics-layer-cake-3 -o layercake3.tar.gz
```

manifest.json


```
[
  {
    "Config": "blobs/sha256/269cd0c184df7781e86c030d8270e686b3f07ef203f56f209370ac0ad674ef35",
    "RepoTags": [
      "anssi/fcsc2024-forensics-layer-cake-3:latest"
    ],
    "Layers": [
      "blobs/sha256/8ea6eb4812d48d7aee7de57a65ba99e4d3c3958fee6eb973419cf7aace4c7fec"
    ],
    "LayerSources": {
      "sha256:8ea6eb4812d48d7aee7de57a65ba99e4d3c3958fee6eb973419cf7aace4c7fec": {
        "mediaType": "application/vnd.oci.image.layer.v1.tar",
        "size": 35153920,
        "digest": "sha256:8ea6eb4812d48d7aee7de57a65ba99e4d3c3958fee6eb973419cf7aace4c7fec"
      }
    }
  }
]
```

Config - 269c...f35


```
{
  "architecture": "amd64",
  "config": {
    "Cmd": [
      "/nix/store/m8ww0n3iqndg8zaiwbsnij6rvmpmjbry-hello/bin/hello"
    ],
    "Env": []
  },
  "created": "1970-01-01T00:00:01Z",
  "os": "linux",
  "preferLocalBuild": true,
  "rootfs": {
    "diff_ids": [
      "sha256:8ea6eb4812d48d7aee7de57a65ba99e4d3c3958fee6eb973419cf7aace4c7fec"
    ],
    "type": "layers"
  },
  "history": [
    {
      "created": "1970-01-01T00:00:01Z"
    }
  ]
}
```

Contenu de la layer

```
./nix:
store

./nix/store:
1rm6sr6ixxzipv5358x0cmaw8rs84g2j-glibc-2.38-44
3sxwxqzkkrgpgaibkm27ggb9kjbzdy31-xgcc-13.2.0-libgcc
5lr5n3qa4day8l1ivbwlcby2nknczqkq-bash-5.2p26
77yhmwrwism02371kzyda4d127kdwdnf-libunistring-1.1
m8ww0n3iqndg8zaiwbsnij6rvmpmjbry-hello
n9sq1bvghs9z0qg6cmwg27y4jmszwgqi-libidn2-2.3.7
rnxji3jf6fb0nx2v0svdqpj9ml53gyqh-hello-2.12.1
```

Dernier flag

```
cat nix/store/m8ww0n3iqndg8zaiwbsnij6rvmpmjbry-hello/bin/hello
```

```
#!/nix/store/5lr5n3qa4day8l1ivbwlcby2nknczqkq-bash-5.2p26/bin/bash
exec /nix/store/rnxji3jf6fb0nx2v0svdqpj9ml53gyqh-hello-2.12.1/bin/hello
-g "FCSC{c12d9a48f1635354fe9c32b216f144ac66f7b8466a5ac82a35aa385…}" -t
```


ANY QUESTIONS?
Layer Cake
imgflip.com