

Lab Exercise 22- Docker Image Vulnerability

Scanning Using Trivy (Windows)

Name:- Vansh Bhatt

SapID:- 500125395

Batch:- DevOps B1

To:- Hitesh Sharma Sir

Objective

By the end of this lab, you will be able to:

- Install and configure **Trivy** on Windows
- Scan **Docker images** for vulnerabilities
- Interpret scan reports and take remediation actions

Prerequisites

- Windows 10/11 (with **Docker Desktop** installed and running)
- Internet access (Trivy downloads vulnerability databases)
- Basic familiarity with Docker CLI commands

Step 1: Verify Docker Setup

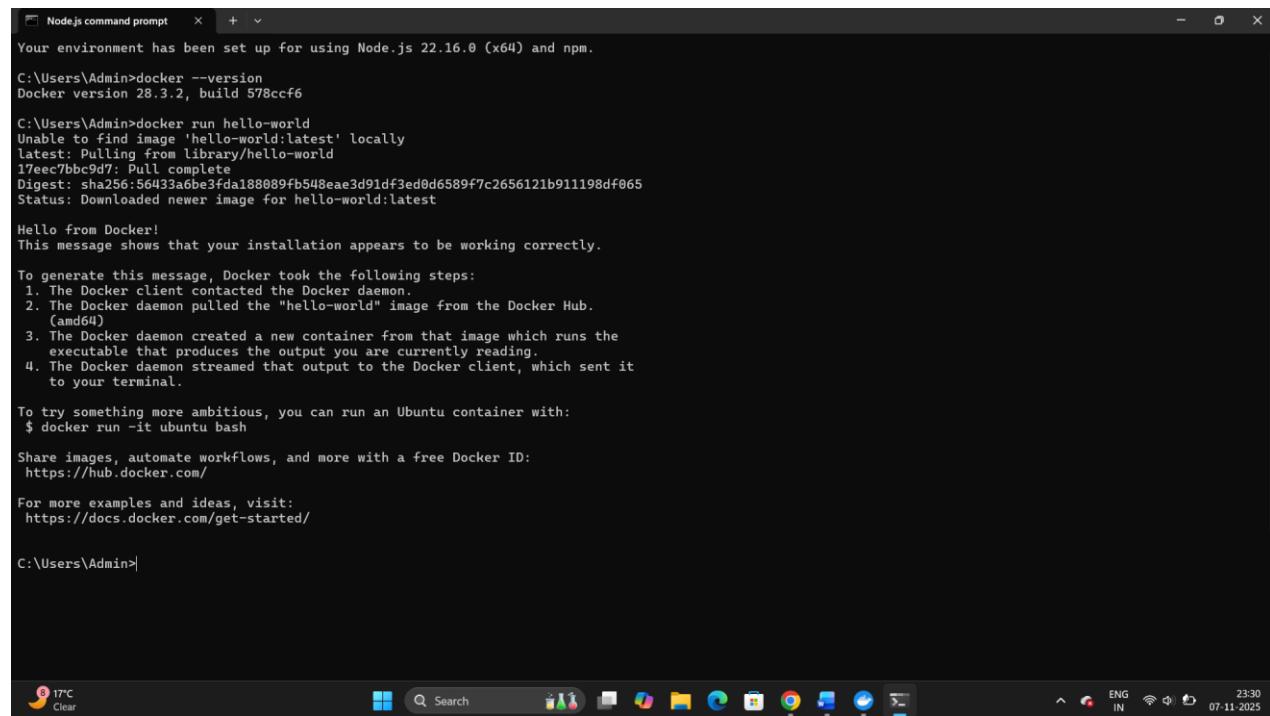
Before using Trivy, make sure Docker is working correctly.

```
docker --version
```

```
docker run hello-world
```

Expected Output:

Docker runs successfully and displays the “Hello from Docker!” message.



```
Node.js command prompt  x  +  ▾
Your environment has been set up for using Node.js 22.16.0 (x64) and npm.

C:\Users\Admin>docker --version
Docker version 28.3.2, build 578ccf6

C:\Users\Admin>docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
17eec7bbc9d7: Pull complete
Digest: sha256:56d433a6be3fd188889fb548eae3d91df3ed0d6589f7c2656121b911198df065
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
    (and64)
 3. The Docker daemon created a new container from that image which runs the
 executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
 to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
 $ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
 https://hub.docker.com/

For more examples and ideas, visit:
 https://docs.docker.com/get-started/

C:\Users\Admin>
```

Step 2: Install Trivy on Windows

Manual Installation

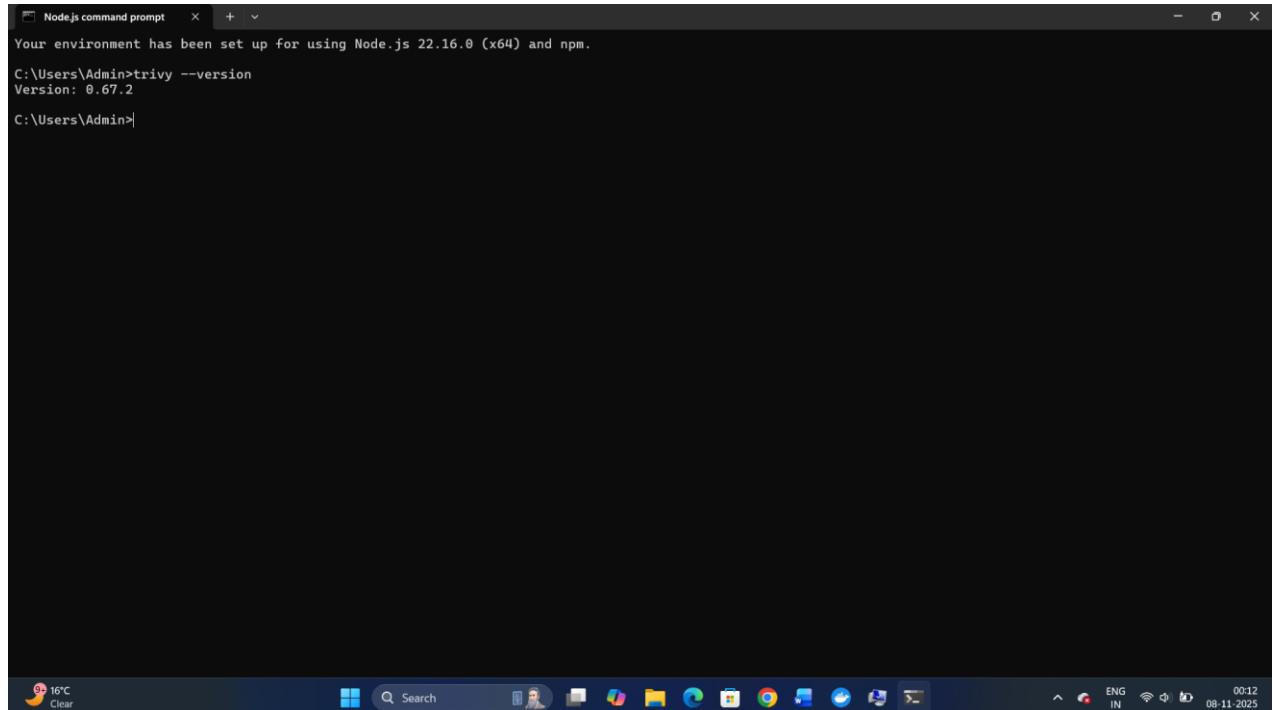
1. Go to the official GitHub releases page:
<https://github.com/aquasecurity/trivy/releases>
2. Download the Windows ZIP file (trivy_x.x.x_windows_amd64.zip)
3. Extract it (e.g., to C:\trivy)
4. Add that folder to your **System PATH** environment variable

Verify Installation

Open **PowerShell** and run:

```
trivy --version
```

Expected Output: Trivy version and build information.



```
Node.js command prompt  x  +  v
Your environment has been set up for using Node.js 22.16.0 (x64) and npm.
C:\Users\Admin>trivy --version
Version: 0.67.2
C:\Users\Admin>
```

The screenshot shows a Windows command prompt window titled "Node.js command prompt". The title bar also includes a weather icon showing 16°C and a "Clear" button. The window displays the command "trivy --version" being run in the directory "C:\Users\Admin". The output shows the Trivy version as "Version: 0.67.2". The taskbar at the bottom of the screen shows various pinned icons, including the Start button, a search bar, and icons for File Explorer, Edge, and other system utilities. The system tray in the bottom right corner shows battery status, network connectivity, and the date and time (08-11-2025).

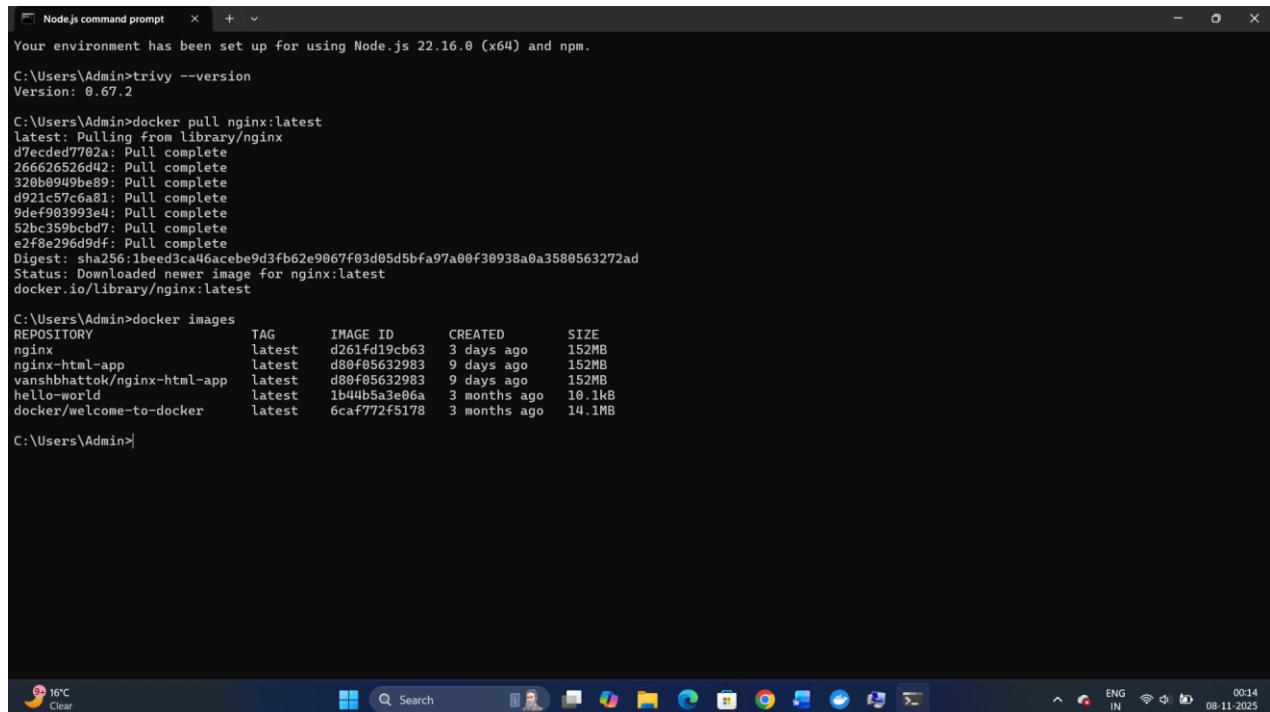
Step 3: Pull a Docker Image

Let's pull an image that we'll scan:

```
docker pull nginx:latest
```

Check it's downloaded:

```
docker images
```



```
Node.js command prompt
Your environment has been set up for using Node.js 22.16.0 (x64) and npm.
C:\Users\Admin>trivy --version
Version: 0.67.2
C:\Users\Admin>docker pull nginx:latest
latest: Pulling from library/nginx
d7ebed7702a: Pull complete
266626526d42: Pull complete
320b0949be89: Pull complete
d921c57c6a81: Pull complete
9def903993e4: Pull complete
52bc359bcfd7: Pull complete
e2f8e296d9df: Pull complete
Digest: sha256:1beed3ca46acebe9d3fb62e9067f03d05d5bfa97a00f30938a0a3580563272ad
Status: Downloaded newer image for nginx:latest
docker.io/library/nginx:latest

C:\Users\Admin>docker images
REPOSITORY          TAG      IMAGE ID      CREATED       SIZE
nginx              latest   d261fd19cb63  3 days ago   152MB
nginx-html-app     latest   d80f05632983  9 days ago   152MB
vanshahattok/nginx-html-app latest   d80f05632983  9 days ago   152MB
hello-world        latest   1b44b5a3e06a  3 months ago  10.1kB
docker/welcome-to-docker latest   6caf772f5178  3 months ago  14.1MB

C:\Users\Admin>
```

Step 4: Scan Docker Image with Trivy

Now, run a vulnerability scan on the image:

```
trivy image nginx:latest
```

```
C:\Users\Admin>trivy image nginx:latest
2025-11-08T00:15:16+05:30    INFO  [vulndb] Need to update DB
2025-11-08T00:15:16+05:30    INFO  [vulndb] Downloading vulnerability DB...
2025-11-08T00:15:16+05:30    INFO  [vulndb] Downloading artifact...      repo="mirror.gcr.io/aquasec/trivy-db:2"
74.36 MiB / 74.36 MiB [=====] 100.00% 4.23 MiB p/s 18s
2025-11-08T00:15:36+05:30    INFO  [vulndb] Artifact successfully downloaded      repo="mirror.gcr.io/aquasec/trivy-db:2"
2025-11-08T00:15:36+05:30    INFO  [vuln] Vulnerability scanning is enabled
2025-11-08T00:15:36+05:30    INFO  [secret] Secret scanning is enabled
2025-11-08T00:15:36+05:30    INFO  [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-11-08T00:15:36+05:30    INFO  [secret] Please see https://trivy.dev/v0.67/docs/scanner/secret#recommendation for faster secret detection
2025-11-08T00:16:00+05:30    INFO  [javadb] Downloading Java DB...
2025-11-08T00:16:00+05:30    INFO  [javadb] Downloading artifact...      repo="mirror.gcr.io/aquasec/trivy-java-db:1"
794.89 MiB / 794.89 MiB [=====] 100.00% 12.86 MiB p/s 1m2s
2025-11-08T00:17:04+05:30    INFO  [javadb] Artifact successfully downloaded      repo="mirror.gcr.io/aquasec/trivy-java-db:1"
2025-11-08T00:17:04+05:30    INFO  [javadb] Java DB is cached for 3 days. If you want to update the database more frequently, "trivy clean --java-db" command clears the DB cache.
2025-11-08T00:17:04+05:30    INFO  Detected OS   family="debian" version="13.1"
2025-11-08T00:17:04+05:30    INFO  [debian] Detecting vulnerabilities... os_version="13" pkg_num=150
2025-11-08T00:17:04+05:30    INFO  Number of language-specific files num=0
2025-11-08T00:17:04+05:30    WARN  Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/v0.67/docs/scanner/vulnerabilit
y#severity-selection for details.

Report Summary



| Target                     | Type   | Vulnerabilities | Secrets |
|----------------------------|--------|-----------------|---------|
| nginx:latest (debian 13.1) | debian | 97              | -       |



Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)

nginx:latest (debian 13.1)
=====
Total: 97 (UNKNOWN: 0, LOW: 84, MEDIUM: 12, HIGH: 1, CRITICAL: 0)
```

Explanation:

Trivy will:

- Fetch the latest vulnerability database
- Analyze all OS packages and libraries inside the image
- Display severity levels (LOW, MEDIUM, HIGH, CRITICAL)

Sample Output

nginx:latest (debian 12.2)

=====

Total: 12 (LOW: 2, MEDIUM: 4, HIGH: 5, CRITICAL: 1)

PACKAGE	VULNERABILITY ID	SEVERITY	INSTALLED VERSION	FIXED VERSION
openssl	CVE-2023-0464	HIGH	3.0.9-1	3.0.9-2
zlib	CVE-2022-37434	MEDIUM	1.2.11-5	1.2.12

```

Node.js command prompt x + v
y#severity-selection for details.

Report Summary



| Target                     | Type   | Vulnerabilities | Secrets |
|----------------------------|--------|-----------------|---------|
| nginx:latest (debian 13.1) | debian | 97              | -       |



Legend:
- '-' Not scanned
- '0': Clean (no security findings detected)

nginx:latest (debian 13.1)
=====
Total: 97 (UNKNOWN: 0, LOW: 84, MEDIUM: 12, HIGH: 1, CRITICAL: 0)



| Library                      | Vulnerability       | Severity | Status   | Installed Version | Fixed Version | Title                                         |
|------------------------------|---------------------|----------|----------|-------------------|---------------|-----------------------------------------------|
| apt all versions, do not     | CVE-2011-3374       | LOW      | affected | 3.0.3             |               | It was found that apt-key in apt correctly... |
| 2011-3374                    |                     |          |          |                   |               | https://avd.aquasec.com/nvd/cve-              |
| bash o other user than root] | TEMP-0841856-B18BAF |          |          | 5.2.37-2+b5       |               | [Privilege escalation possible t              |
| org/tracker/TEMP-0841856-B1- |                     |          |          |                   |               | https://security-tracker.debian.              |
|                              |                     |          |          |                   |               | 8BAF                                          |
| bsdutils                     | CVE-2022-0563       |          |          | 1:2.41-5          |               | util-linux: partial disclosure o              |


```

```

Node.js command prompt x + v
2011-4116
| sysinit-utils | TEMP-0517018-A83CE6 |
|  ert installer exposes |
| w|
| org/tracker/TEMP-0517018-A8-|
| |
| tar | CVE-2005-2541 |
| user when extracting setuid |
| |
2005-2541
| |
| TEMP-0290435-0B57B5 |
| sired side effects|
| org/tracker/TEMP-0290435-0B-|
| |
| util-linux | CVE-2022-0563 |
| arbitrary files in chfn |
| |
2022-0563
| |
C:\Users\Admin>



```

Step 5: Save Report to a File

You can export the results in different formats.

Save as a text file:

```
trivy image nginx:latest > nginx_scan.txt
```

```

trivy image nginx:latest > nginx_scan.txt
2025-11-08T00:19:50+05:30 INFO  [vuln] Vulnerability scanning is enabled
2025-11-08T00:19:50+05:30 INFO  [secret] Secret scanning is enabled
2025-11-08T00:19:50+05:30 INFO  [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-11-08T00:19:50+05:30 INFO  [secret] Please see https://trivy.dev/v0.67/docs/scanner/secret#recommendation for faster secret detection
2025-11-08T00:19:50+05:30 INFO  Detected OS    family="debian" version="13.1"
2025-11-08T00:19:50+05:30 INFO  [debian] Detecting vulnerabilities...  os_version="13" pkg_num=150
2025-11-08T00:19:50+05:30 INFO  Number of language-specific files  num=0
2025-11-08T00:19:50+05:30 WARN  Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/v0.67/docs/scanner/vulnerabilit
y#severity-selection for details.
C:\Users\Admin>



```

Save as a JSON report:

```
trivy image --format json -o nginx.json nginx:latest
```

```
C:\Users\Admin>trivy image --format json -o nginx_scan.json nginx:latest
2025-11-08T00:21:19+05:30    INFO  [vuln] Vulnerability scanning is enabled
2025-11-08T00:21:19+05:30    INFO  [secret] Secret scanning is enabled
2025-11-08T00:21:19+05:30    INFO  [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-11-08T00:21:19+05:30    INFO  [secret] Please see https://trivy.dev/v0.67/docs/scanner/secret#recommendation for faster secret detection
2025-11-08T00:21:20+05:30    INFO  Detected OS   family="debian" version="13.1"
2025-11-08T00:21:20+05:30    INFO  [debian] Detecting vulnerabilities... os_version="13" pkg_num=150
2025-11-08T00:21:20+05:30    INFO  Number of language-specific files      num=0
2025-11-08T00:21:20+05:30    WARN   Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/v0.67/docs/scanner/vulnerabilit
y#severity-selection for details.

C:\Users\Admin>
```

Tip: JSON format is useful for automation or CI/CD integration.

Step 6: Scan a Local Image

If you've built your own Docker image:

```
docker build -t myapp:1.0 .
```

```
trivy image myapp:1.0
```

```
C:\Users\Admin>trivy image vanshbhattok/nginx-html-app:latest
2025-11-08T00:25:00+05:30    INFO  [vuln] Vulnerability scanning is enabled
2025-11-08T00:25:00+05:30    INFO  [secret] Secret scanning is enabled
2025-11-08T00:25:00+05:30    INFO  [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-11-08T00:25:00+05:30    INFO  [secret] Please see https://trivy.dev/v0.67/docs/scanner/secret#recommendation for faster secret detection
2025-11-08T00:25:00+05:30    INFO  Detected OS   family="debian" version="13.1"
2025-11-08T00:25:00+05:30    INFO  [debian] Detecting vulnerabilities... os_version="13" pkg_num=150
2025-11-08T00:25:00+05:30    INFO  Number of language-specific files      num=0
2025-11-08T00:25:00+05:30    WARN   Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/v0.67/docs/scanner/vulnerabilit
y#severity-selection for details.

Report Summary
```

Target	Type	Vulnerabilities	Secrets
vanshbhattok/nginx-html-app:latest (debian 13.1)	debian	97	-

```
Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)

vanshbhattok/nginx-html-app:latest (debian 13.1)
=====
Total: 97 (UNKNOWN: 0, LOW: 84, MEDIUM: 12, HIGH: 1, CRITICAL: 0)

|-----|
| Library | Vulnerability | Severity | Status | Installed Version | Fixed Version | Title |
|-----|
| apt     | CVE-2011-3374  | LOW      | affected | 3.0.3          |              | It was found that apt-key in apt |
| all versions, do not | | | | | | correctly... |
|-----|
| 2011-3374 | | | | | | https://avd.aquasec.com/nvd/cve- |
|-----|
```

Step 7: Update Vulnerability Database

Keep Trivy's database up-to-date:

```
trivy image --download-db-only
```

```
C:\Users\Admin>trivy image --download-db-only
C:\Users\Admin>docker rmi nginx:latest
Untagged: nginx:latest
Untagged: nginx@sha256:1beed3ca46acebe9d3fb62e9067f03d05d5bfa97a00f30938a0a3580563272ad
Deleted: sha256:d261fd19cb63238535ab80d4e1be1d9ef7fc8b5a28a20188968dd3e6f06072d
Deleted: sha256:534fa102b912db29b236581b36d96b3961fab8a8e2f87170de3a97440975889e
Deleted: sha256:f356d7e216ceca7946179c3ac20a975853d782fe5f914fd76275ba1949ae7e5b
Deleted: sha256:f8d71bebdd1664ec5c412cc511bde3a5a93df38254ac3e59431da4e9830b3ffa
Deleted: sha256:d65f0afc2c55c237e5a861e22de0c6ff8b24c171b89902f0e980675d50eccc0aa
Deleted: sha256:8edab3f21d7fc317fse932991903851ddf379ab6c58cf806675a63cd91d21
Deleted: sha256:813c6bf1f7312b3773f41f7bee85244570fed62c2aa5e7ba45d83d7fc16106e2c
Deleted: sha256:36d06fe0cbc654e5f67d58c968ed33e53127e4a3288d8ce6f6a60a9c311794d4
```

```
C:\Users\Admin>
```



Step 8: Clean Up

Remove images (optional):

```
docker rmi nginx:latest
```

```
C:\Users\Admin>trivy image --download-db-only
C:\Users\Admin>docker rmi nginx:latest
Untagged: nginx@sha256:1beed3ca46acebe9d3fb62e9067f03d05d5bfa97a00f30938a0a3580563272ad
Deleted: sha256:d261fd19cb63238535ab80d4e1be1d9ef7fc8b5a28a20188968dd3e6f06072d
Deleted: sha256:534fa102b912db29b236581b36d96b3961fab8a8e2f87170de3a97440975889e
Deleted: sha256:f356d7e216ceca7946179c3ac20a975853d782fe5f914fd76275ba1949ae7e5b
Deleted: sha256:f8d71bebdd1664ec5c412cc511bde3a5a93df38254ac3e59431da4e9830b3ffa
Deleted: sha256:d65f0afc2c55c237e5a861e22de0c6ff8b24c171b89902f0e980675d50eccc0aa
Deleted: sha256:8edab3f21d7fc317fse932991903851ddf379ab6c58cf806675a63cd91d21
Deleted: sha256:813c6bf1f7312b3773f41f7bee85244570fed62c2aa5e7ba45d83d7fc16106e2c
Deleted: sha256:36d06fe0cbc654e5f67d58c968ed33e53127e4a3288d8ce6f6a60a9c311794d4
```

```
C:\Users\Admin>
```



Thank You