ATTACK DEFENSE

by PentesterAcademy

Name	Tool: Dive
URL	https://attackdefense.com/challengedetails?cid=1416
Type	DevSecOps : Docker Tools

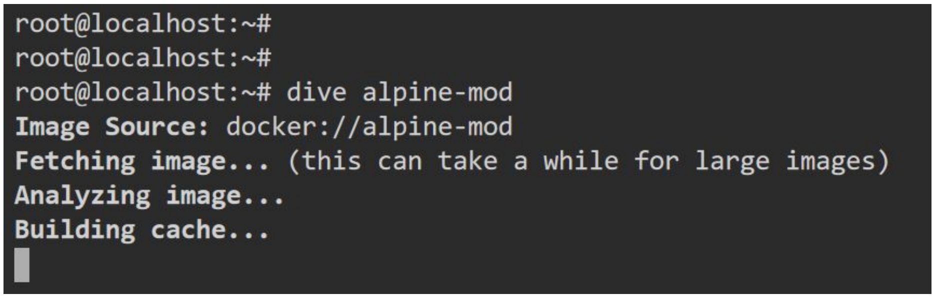
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Analyze the image with dive and retrieve the flag!

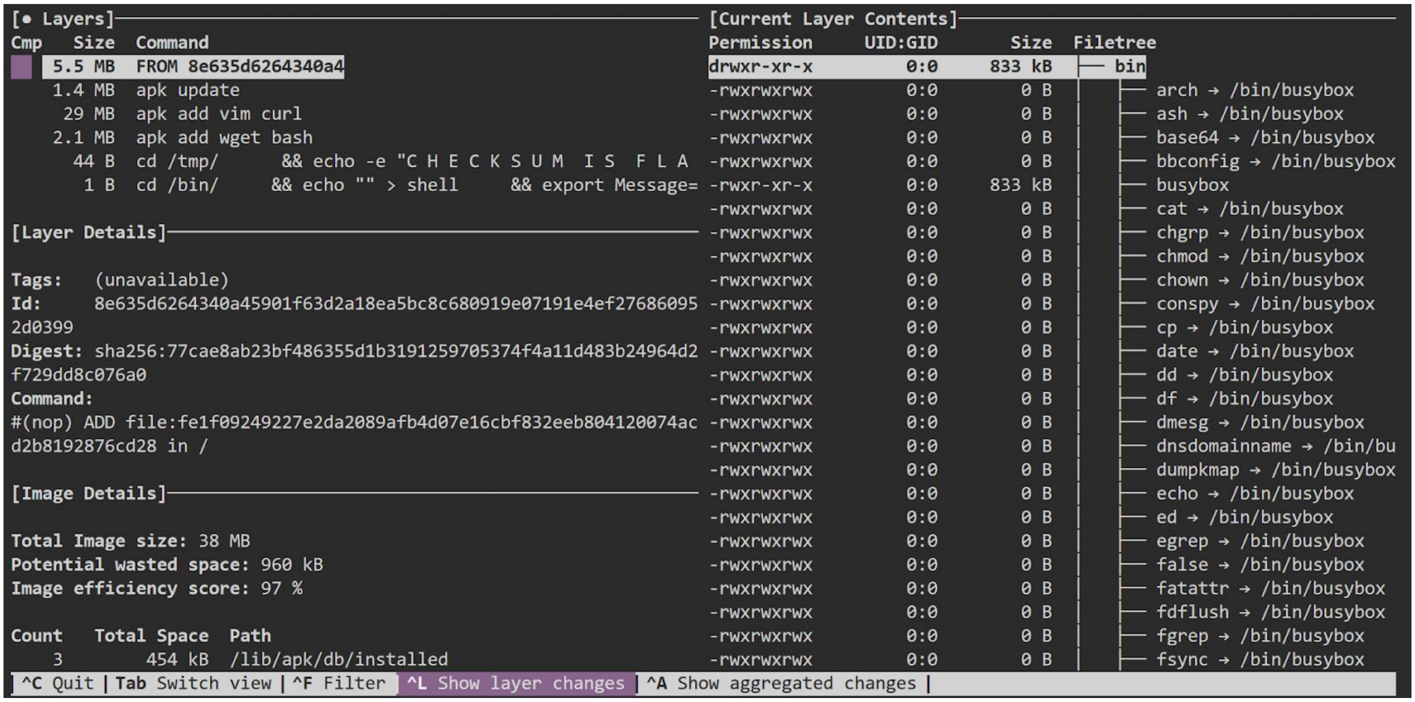
Solution:

Step 1: Analyze the image 'alpine-mod' with dive.

Command: dive alpine-mod



```
root@localhost:~#
root@localhost:~#
root@localhost:~# dive alpine-mod
Image Source: docker://alpine-mod
Fetching image... (this can take a while for large images)
Analyzing image...
Building cache...
```

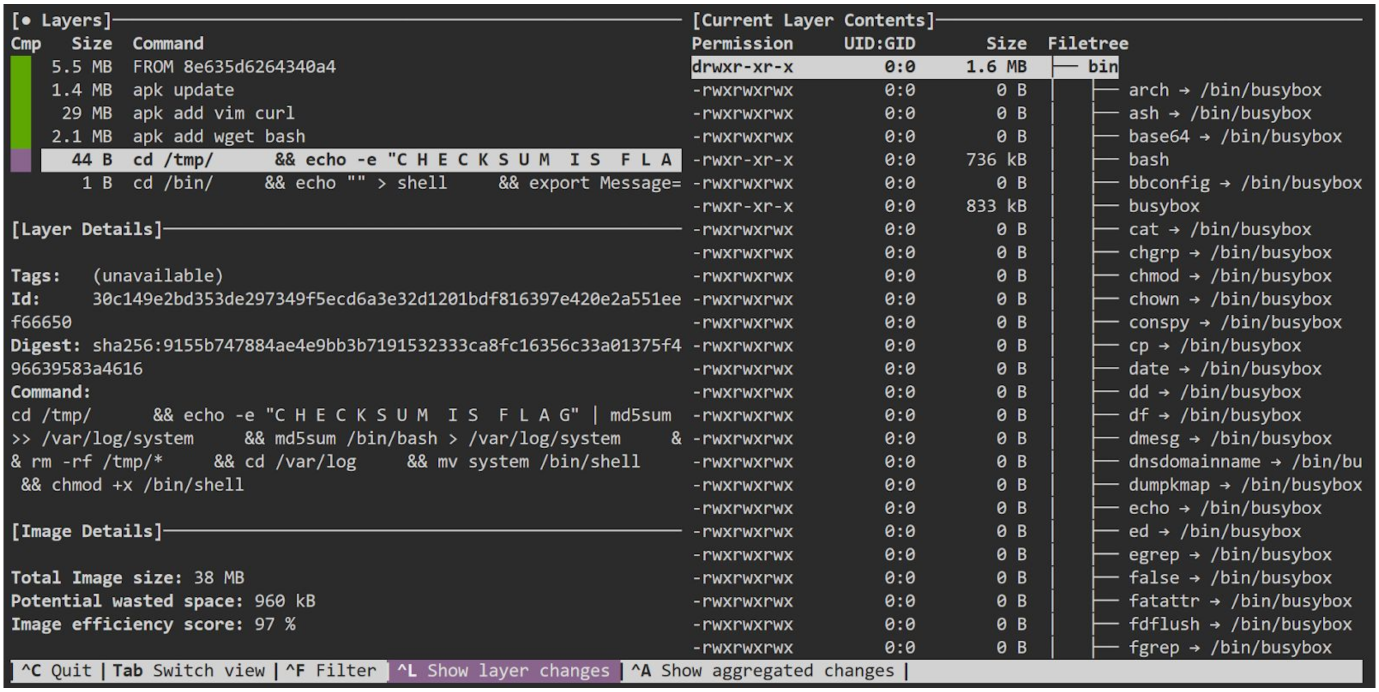


```
[● Layers]──────────────────────────────────────────────────────── [Current Layer Contents]──────────────────────────────────
Cmp   Size  Command                                                Permission     UID:GID       Size  Filetree
■    5.5 MB  FROM 8e635d6264340a4                                  drwxr-xr-x         0:0     833 kB  ├── bin
     1.4 MB  apk update                                            -rwxrwxrwx         0:0        0 B  │       ├── arch → /bin/busybox
      29 MB  apk add vim curl                                      -rwxrwxrwx         0:0        0 B  │       ├── ash → /bin/busybox
     2.1 MB  apk add wget bash                                     -rwxrwxrwx         0:0        0 B  │       ├── base64 → /bin/busybox
       44 B  cd /tmp/      && echo -e "C H E C K S U M  I S  F L A -rwxrwxrwx         0:0        0 B  │       ├── bbconfig → /bin/busybox
        1 B  cd /bin/     && echo "" > shell      && export Message= -rwxr-xr-x         0:0     833 kB  │       ├── busybox
                                                                   -rwxrwxrwx         0:0        0 B  │       ├── cat → /bin/busybox
[Layer Details]─────────────────────────────────────────────────── -rwxrwxrwx         0:0        0 B  │       ├── chgrp → /bin/busybox
                                                                   -rwxrwxrwx         0:0        0 B  │       ├── chmod → /bin/busybox
Tags:   (unavailable)                                              -rwxrwxrwx         0:0        0 B  │       ├── chown → /bin/busybox
Id:     8e635d6264340a45901f63d2a18ea5bc8c680919e07191e4ef27686095 -rwxrwxrwx         0:0        0 B  │       ├── conspy → /bin/busybox
2d0399                                                             -rwxrwxrwx         0:0        0 B  │       ├── cp → /bin/busybox
Digest: sha256:77cae8ab23bf486355d1b3191259705374f4a11d483b24964d2 -rwxrwxrwx         0:0        0 B  │       ├── date → /bin/busybox
f729dd8c076a0                                                      -rwxrwxrwx         0:0        0 B  │       ├── dd → /bin/busybox
Command:                                                           -rwxrwxrwx         0:0        0 B  │       ├── df → /bin/busybox
#(nop) ADD file:fe1f09249227e2da2089afb4d07e16cbf832eeb804120074ac -rwxrwxrwx         0:0        0 B  │       ├── dmesg → /bin/busybox
d2b8192876cd28 in /                                                -rwxrwxrwx         0:0        0 B  │       ├── dnsdomainname → /bin/bu
                                                                   -rwxrwxrwx         0:0        0 B  │       ├── dumpkmap → /bin/busybox
[Image Details]─────────────────────────────────────────────────── -rwxrwxrwx         0:0        0 B  │       ├── echo → /bin/busybox
                                                                   -rwxrwxrwx         0:0        0 B  │       ├── ed → /bin/busybox
Total Image size: 38 MB                                            -rwxrwxrwx         0:0        0 B  │       ├── egrep → /bin/busybox
Potential wasted space: 960 kB                                     -rwxrwxrwx         0:0        0 B  │       ├── false → /bin/busybox
Image efficiency score: 97 %                                       -rwxrwxrwx         0:0        0 B  │       ├── fatattr → /bin/busybox
                                                                   -rwxrwxrwx         0:0        0 B  │       ├── fdflush → /bin/busybox
Count   Total Space  Path                                          -rwxrwxrwx         0:0        0 B  │       ├── fgrep → /bin/busybox
    3        454 kB  /lib/apk/db/installed                         -rwxrwxrwx         0:0        0 B  │       ├── fsync → /bin/busybox
│^C Quit │Tab Switch view │^F Filter │^L Show layer changes │^A Show aggregated changes │
```

In the layer view (section on left), the information regarding the command which was used to create the layer along with other information about the image is listed.

In the file tree view (section on the right), the filesystem tree is displayed, options are available to show/hide added, removed, modified and unmodified files.

Step 2: View the command executed in the fourth layer. The arrow keys can be used to navigate through layers.



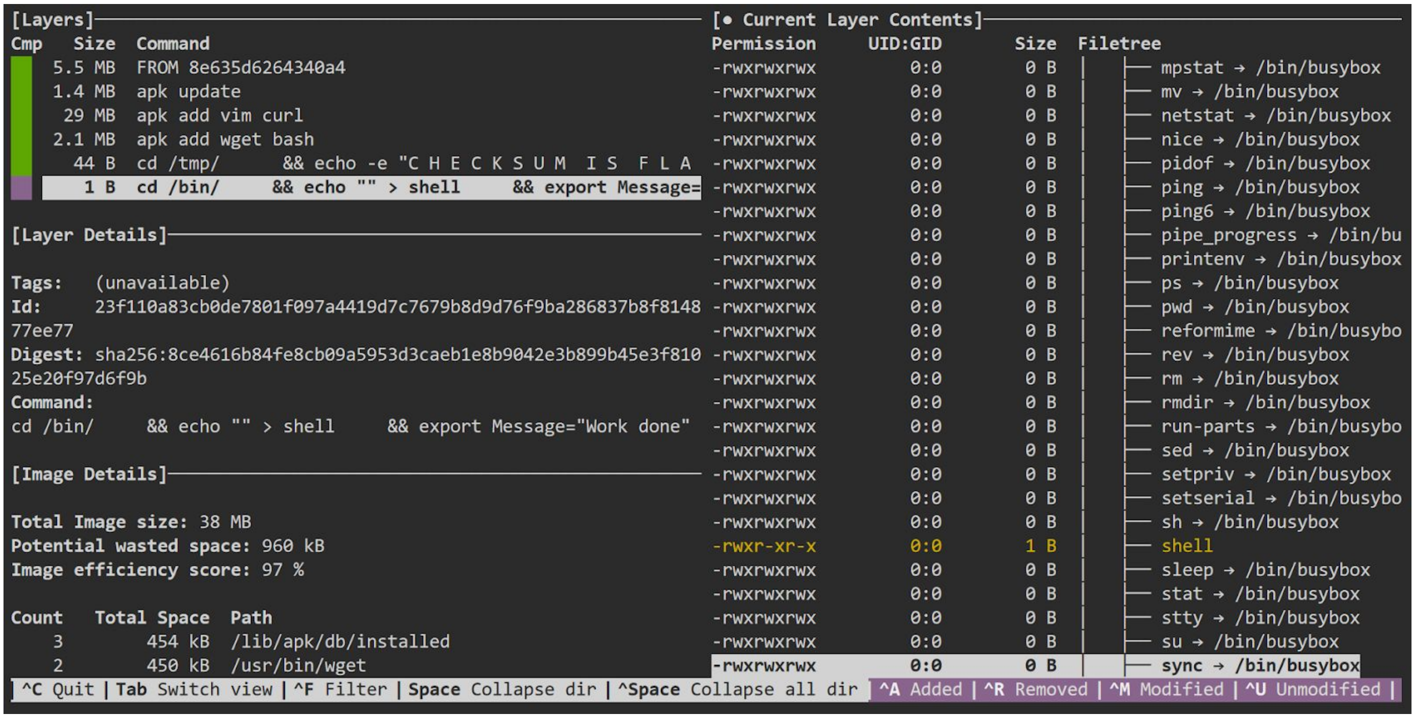
```
[● Layers]──────────────────────────────────────────────────────── [Current Layer Contents]──────────────────────────────────────
Cmp   Size  Command                                                Permission     UID:GID       Size  Filetree
       5.5 MB  FROM 8e635d6264340a4                                drwxr-xr-x         0:0     1.6 MB  ── bin
       1.4 MB  apk update                                          -rwxrwxrwx         0:0        0 B     ├── arch → /bin/busybox
        29 MB  apk add vim curl                                    -rwxrwxrwx         0:0        0 B     ├── ash → /bin/busybox
       2.1 MB  apk add wget bash                                   -rwxrwxrwx         0:0        0 B     ├── base64 → /bin/busybox
        44 B  cd /tmp/       && echo -e "C H E C K S U M  I S  F L A  -rwxr-xr-x         0:0     736 kB     ├── bash
         1 B  cd /bin/       && echo "" > shell      && export Message= -rwxrwxrwx         0:0        0 B     ├── bbconfig → /bin/busybox
                                                                   -rwxr-xr-x         0:0     833 kB     ├── busybox
[Layer Details]─────────────────────────────────────────────────── -rwxrwxrwx         0:0        0 B     ├── cat → /bin/busybox
                                                                   -rwxrwxrwx         0:0        0 B     ├── chgrp → /bin/busybox
Tags:    (unavailable)                                             -rwxrwxrwx         0:0        0 B     ├── chmod → /bin/busybox
Id:      30c149e2bd353de297349f5ecd6a3e32d1201bdf816397e420e2a551ee -rwxrwxrwx         0:0        0 B     ├── chown → /bin/busybox
f66650                                                             -rwxrwxrwx         0:0        0 B     ├── conspy → /bin/busybox
Digest: sha256:9155b747884ae4e9bb3b7191532333ca8fc16356c33a01375f4 -rwxrwxrwx         0:0        0 B     ├── cp → /bin/busybox
96639583a4616                                                      -rwxrwxrwx         0:0        0 B     ├── date → /bin/busybox
Command:                                                           -rwxrwxrwx         0:0        0 B     ├── dd → /bin/busybox
cd /tmp/      && echo -e "C H E C K S U M  I S  F L A G" | md5sum  -rwxrwxrwx         0:0        0 B     ├── df → /bin/busybox
>> /var/log/system      && md5sum /bin/bash > /var/log/system     & -rwxrwxrwx         0:0        0 B     ├── dmesg → /bin/busybox
& rm -rf /tmp/*      && cd /var/log      && mv system /bin/shell   -rwxrwxrwx         0:0        0 B     ├── dnsdomainname → /bin/bu
 && chmod +x /bin/shell                                            -rwxrwxrwx         0:0        0 B     ├── dumpkmap → /bin/busybox
                                                                   -rwxrwxrwx         0:0        0 B     ├── echo → /bin/busybox
[Image Details]─────────────────────────────────────────────────── -rwxrwxrwx         0:0        0 B     ├── ed → /bin/busybox
                                                                   -rwxrwxrwx         0:0        0 B     ├── egrep → /bin/busybox
Total Image size: 38 MB                                            -rwxrwxrwx         0:0        0 B     ├── false → /bin/busybox
Potential wasted space: 960 kB                                     -rwxrwxrwx         0:0        0 B     ├── fatattr → /bin/busybox
Image efficiency score: 97 %                                       -rwxrwxrwx         0:0        0 B     ├── fdflush → /bin/busybox
                                                                   -rwxrwxrwx         0:0        0 B     ├── fgrep → /bin/busybox
| ^C Quit | Tab Switch view | ^F Filter | ^L Show layer changes | ^A Show aggregated changes |
```

In the fourth layer, a file named /var/log/system is created which is later moved to /bin/shell.

Step 3: Switch to the file tree view by pressing the TAB key and identify the added file.

The shell file appears in green color which represents that the file was added in this layer.

Step 4: Navigate to the last layer and identify the modified file.



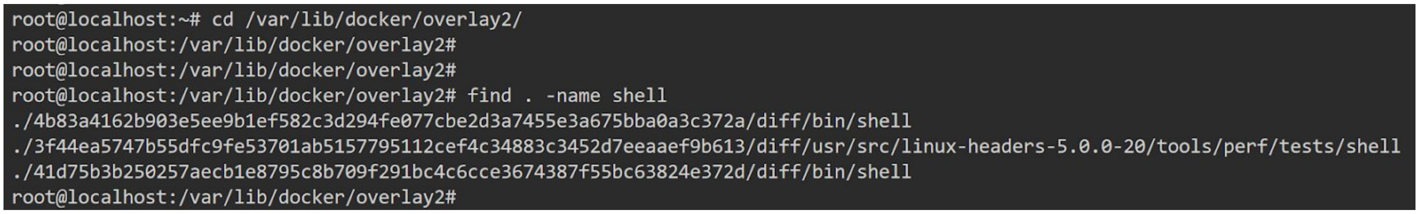
```
[Layers]──────────────────────────────────────────────────────────── [● Current Layer Contents]──────────────────────────────────────────
Cmp   Size  Command                                                  Permission     UID:GID       Size  Filetree
     5.5 MB  FROM 8e635d6264340a4                                    -rwxrwxrwx         0:0        0 B  │   ├── mpstat → /bin/busybox
     1.4 MB  apk update                                              -rwxrwxrwx         0:0        0 B  │   ├── mv → /bin/busybox
      29 MB  apk add vim curl                                        -rwxrwxrwx         0:0        0 B  │   ├── netstat → /bin/busybox
     2.1 MB  apk add wget bash                                       -rwxrwxrwx         0:0        0 B  │   ├── nice → /bin/busybox
       44 B  cd /tmp/       && echo -e "C H E C K S U M  I S  F L A  -rwxrwxrwx         0:0        0 B  │   ├── pidof → /bin/busybox
        1 B  cd /bin/      && echo "" > shell      && export Message= -rwxrwxrwx         0:0        0 B  │   ├── ping → /bin/busybox
                                                                     -rwxrwxrwx         0:0        0 B  │   ├── ping6 → /bin/busybox
[Layer Details]───────────────────────────────────────────────────── -rwxrwxrwx         0:0        0 B  │   ├── pipe_progress → /bin/bu
                                                                     -rwxrwxrwx         0:0        0 B  │   ├── printenv → /bin/busybox
Tags:   (unavailable)                                                -rwxrwxrwx         0:0        0 B  │   ├── ps → /bin/busybox
Id:     23f110a83cb0de7801f097a4419d7c7679b8d9d76f9ba286837b8f8148   -rwxrwxrwx         0:0        0 B  │   ├── pwd → /bin/busybox
77ee77                                                               -rwxrwxrwx         0:0        0 B  │   ├── reformime → /bin/busybo
Digest: sha256:8ce4616b84fe8cb09a5953d3caeb1e8b9042e3b899b45e3f810   -rwxrwxrwx         0:0        0 B  │   ├── rev → /bin/busybox
25e20f97d6f9b                                                        -rwxrwxrwx         0:0        0 B  │   ├── rm → /bin/busybox
Command:                                                             -rwxrwxrwx         0:0        0 B  │   ├── rmdir → /bin/busybox
cd /bin/     && echo "" > shell     && export Message="Work done"    -rwxrwxrwx         0:0        0 B  │   ├── run-parts → /bin/busybo
                                                                     -rwxrwxrwx         0:0        0 B  │   ├── sed → /bin/busybox
[Image Details]───────────────────────────────────────────────────── -rwxrwxrwx         0:0        0 B  │   ├── setpriv → /bin/busybox
                                                                     -rwxrwxrwx         0:0        0 B  │   ├── setserial → /bin/busybo
Total Image size: 38 MB                                              -rwxrwxrwx         0:0        0 B  │   ├── sh → /bin/busybox
Potential wasted space: 960 kB                                       -rwxr-xr-x         0:0        1 B  │   ├── shell
Image efficiency score: 97 %                                         -rwxrwxrwx         0:0        0 B  │   ├── sleep → /bin/busybox
                                                                     -rwxrwxrwx         0:0        0 B  │   ├── stat → /bin/busybox
Count   Total Space  Path                                            -rwxrwxrwx         0:0        0 B  │   ├── stty → /bin/busybox
    3        454 kB  /lib/apk/db/installed                           -rwxrwxrwx         0:0        0 B  │   ├── su → /bin/busybox
    2        450 kB  /usr/bin/wget                                   -rwxrwxrwx         0:0        0 B  │   ├── sync → /bin/busybox
| ^C Quit | Tab Switch view | ^F Filter | Space Collapse dir | ^Space Collapse all dir | ^A Added | ^R Removed | ^M Modified | ^U Unmodified |
```

The shell file appears in orange color, ie. the shell file was modified in this layer.

Step 5: Since the filename which gets modified is known, search for the file in the directory where docker stores the files of layers. The default directory used by docker daemon is /var/lib/docker. The files of the layers are stored in the overlay2 directory.

Commands:

cd /var/lib/docker/overlay2
find . -name shell

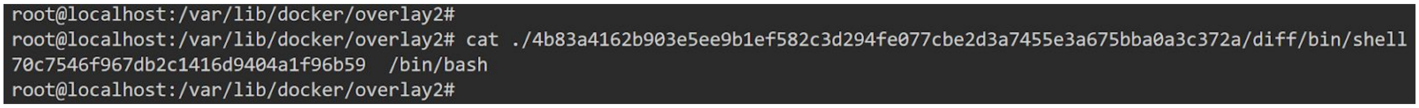


```
root@localhost:~# cd /var/lib/docker/overlay2/
root@localhost:/var/lib/docker/overlay2#
root@localhost:/var/lib/docker/overlay2#
root@localhost:/var/lib/docker/overlay2# find . -name shell
./4b83a4162b903e5ee9b1ef582c3d294fe077cbe2d3a7455e3a675bba0a3c372a/diff/bin/shell
./3f44ea5747b55dfc9fe53701ab5157795112cef4c34883c3452d7eeaaef9b613/diff/usr/src/linux-headers-5.0.0-20/tools/perf/tests/shell
./41d75b3b250257aecb1e8795c8b709f291bc4c6cce3674387f55bc63824e372d/diff/bin/shell
root@localhost:/var/lib/docker/overlay2#
```

shell file is present in /bin directory in two of the layers. One of the layers contains the modified shell file and the other layer contains the flag.

Step 6: Retrieve the flag.

Command: cat ./4b83a4162b903e5ee9b1ef582c3d294fe077cbe2d3a7455e3a675bba0a3c372a/diff/bin/shell



```
root@localhost:/var/lib/docker/overlay2#
root@localhost:/var/lib/docker/overlay2# cat ./4b83a4162b903e5ee9b1ef582c3d294fe077cbe2d3a7455e3a675bba0a3c372a/diff/bin/shell
70c7546f967db2c1416d9404a1f96b59  /bin/bash
root@localhost:/var/lib/docker/overlay2#
```

Flag: 70c7546f967db2c1416d9404a1f96b59

References:

1. Docker (https://www.docker.com/)
2. dive (https://github.com/wagoodman/dive)