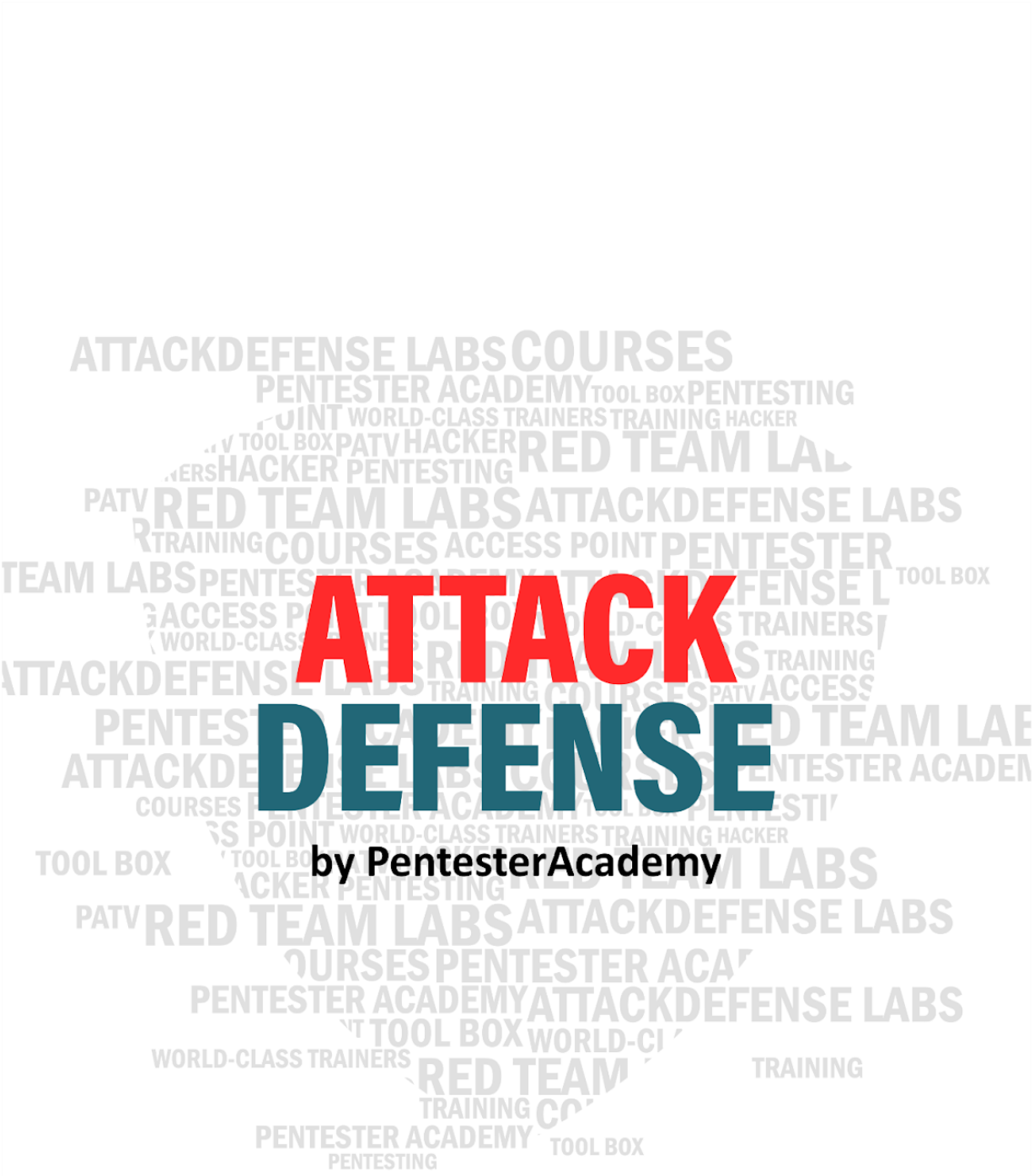

ATTACK
DEFENSE
by PentesterAcademy

Name	File Carving (Foremost)
URL	https://www.attackdefense.com/challengedetails?cid=1791
Type	Forensics: Disk Forensics

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.

In this lab, a disk image file “evidence.img” is provided in the home directory of the root user (/root/). One of the JPEG files present on the disk contains the flag.

Objective: Extract files from the given image using Foremost and retrieve the flag!

Solution:

Step 1: Use the foremost tool to process the disk image file and extract files.

Command: foremost -v -i evidence.img -o output

```
root@attackdefense:~# foremost -v -i evidence.img -o output
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Tue Feb 11 09:34:42 2020
Invocation: foremost -v -i evidence.img -o output
Output directory: /root/output
Configuration file: /etc/foremost.conf
Processing: evidence.img
|------------------------------------------------------------------
File: evidence.img
Start: Tue Feb 11 09:34:42 2020
Length: 1023 MB (1072693248 bytes)
```

```
Num      Name (bs=512)         Size      File Offset     Comment

*0:     00263184.jpg           6 KB       134750208
**********
Finish: Tue Feb 11 09:35:14 2020

1 FILES EXTRACTED

jpg:= 1
------------------------------------------------------------------

Foremost finished at Tue Feb 11 09:35:14 2020
root@attackdefense:~#
```

The carved files are stored in the “output” directory.

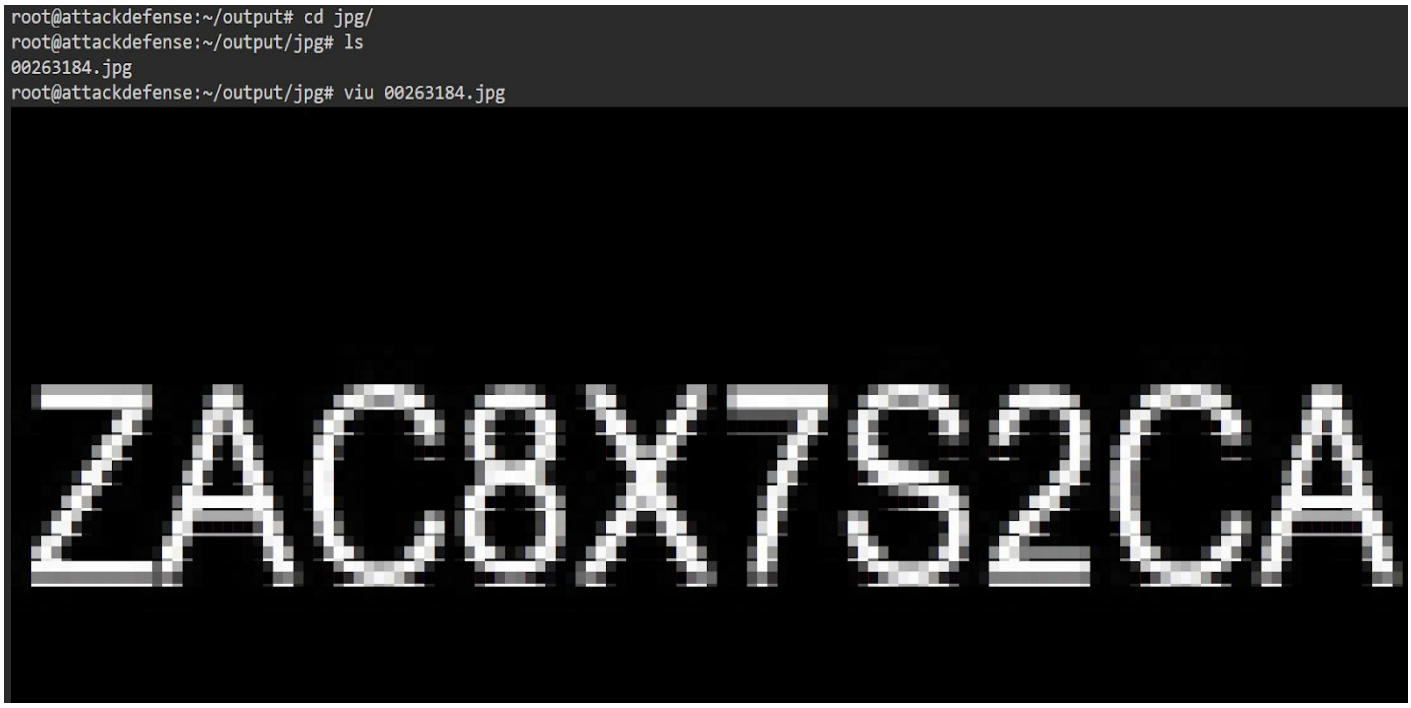
Step 2: Navigate to the output directory and inspect the carved files.

```
root@attackdefense:~/output# ls -lha
total 16K
drwxr-xr-- 3 root root 4.0K Feb 11 09:35 .
drwx------ 1 root root 4.0K Feb 11 09:34 ..
-rw-r--r-- 1 root root  680 Feb 11 09:35 audit.txt
drwxr-xr-- 2 root root 4.0K Feb 11 09:34 jpg
root@attackdefense:~/output#
```

Step 3: change to “jpg” directory and list its contents. Open the JPEG file using the viu tool and retrieve the flag.

Commands:
cd jpg
ls
viu 00263184.jpg

```
root@attackdefense:~/output# cd jpg/
root@attackdefense:~/output/jpg# ls
00263184.jpg
root@attackdefense:~/output/jpg# viu 00263184.jpg
```



Flag: ZAC8X7S2CA

References:

1. Foremost (http://foremost.sourceforge.net/)