

Part 1: Observing Virus Detection

Step 0: Antivirus check!

Make sure that you have some form of antivirus installed on your machine. (If you don't have one, you can install any free antivirus (except Malwarebytes, it doesn't work for this lab) – Just make sure you're downloading from an official website and not a third-party link.)

Windows: ESET

Mac: BitDefender Virus Scanner

For optimization reasons, popular antivirus tool Malwarebytes has chosen to opt-out of detecting EICAR's testfiles. Malwarebytes is still an excellent antivirus, but if it's what you use, you'll want to download an alternative option for this lab.

Step 1: Observe (harmless) virus files

Okay, let's get some (fake) viruses! Fortunately, the European Institute for Computer Antivirus Research (EICAR) has us covered with their Anti Malware Testfile website.

Be sure to read the text on the download page thoroughly, as it contains important information!

Now it's time to get started:

Download each of the 4 harmless antivirus test files to your own computer (not Azure Labs).

There are 4 files for download to facilitate various scenarios:

[eicar.com](https://www.eicar.com)

eicar.com.txt (The same file as [eicar.com](https://www.eicar.com), but named differently)

eicar_com.zip (A zip containing [eicar.com](https://www.eicar.com))

eicarcom2.zip (A zip containing a zip containing [eicar.com](https://www.eicar.com))

🤔 Why do you think EICAR distributes the same file in four different ways?

Click here for an answer!

After you've downloaded the virus files, your antivirus might react automatically.

If nothing pops up, open your antivirus program and run an antivirus scan.

How did your computer respond to the viruses? Compare with others in the lab!

Was it the same or different?

🤔 How do you think your antivirus is able to detect the EICAR files as "dangerous"?

🔗 Checkpoint 1: You should have downloaded the four EICAR files and seen your antivirus detect them.

Step 2: Upload these files to Virus Total

In this next step, we'll upload the files to a virus monitoring website to get more information on how they're detected.

Go to VirusTotal web page.

Upload the files that you have created or downloaded from EICAR.

VirusTotal will analyze the file if it's suspicious. It will also automatically share the results with the security community. You can do this any time you have a file you're unsure of!

💡 TIP: If you can't upload the EICAR file, here's a screenshot of our results: Feel free to play with VirusTotal. Try uploading some other files and see what their results show up as. What happens if you modify the existing file?

🔗 Checkpoint 2: VirusTotal lets you see whether an uploaded file is marked as malware by a particular anti-virus scanner once you upload it.

🎉 You've completed Part 1 of this lab! 🎉 With whatever time you have left, try to go as far as you can with Part 2!

Part 2: Looking Under the Hood

APIs provide a powerful way to access remote data from within a terminal, script, or other computer program. For this lab's stretch features, we'll learn how to use the VirusTotal API to check out a file on our Ubuntu box through the terminal. Along the way, we'll also learn a little more about how files are recognized using file signatures.

Step 3: Get your API key for Virus Total.

In this step, you will obtain your API key from VirusTotal site. Take note of your API key for this will be used in the following steps.

⚠️ Keep your API key secure at all times! Treat it like a password!

Go to the VirusTotal website.

Either sign in or create a free account.

Once signed in, go to the VirusTotal API key page to access your key.

💡 HINT: The screenshot below shows what your VirusTotal API Key page should look like!

An alternative location of your VirusTotal API key can also be found in your account user menu!

🔗 Checkpoint 3: You should have a 🔑 to VirusTotal's API.

Step 4: Configure vt-cli tool with your API key

Great news – you already should have the vt-cli installed on your Azure Labs machine.

Configure the vt-cli tool with your API key:

Sign into your Ubuntu machine

Run the following command:

`vt init`

Paste in your api key when prompted

VirusTotal will save your key for future use. If you're curious, you can find this config in your home directory (~) in a file called `.vt.toml`.

Help, I'm getting a command not found error for vt!

💡 HINT: Click [here](#) for an example of vt-cli configuration!

🔗 Checkpoint 4: If you run the vt version `-v` command, you should see the following:

```
(kali@kali)-[~/vt-cli]
$ vt version -v
* Config file: /home/kali/.vt.toml
* API key: a4fa[REDACTED]42b2
* API host: www.virustotal.com
vt-cli
```

Step 5: Get your file's signature

It's time to reveal the trick that most antivirus software uses to recognize viruses... file signatures. File signatures work using a cryptographic hashing function, which is a fancy piece of math that assigns every input a distinct but predictable output – usually called a hash.

What does that mean?

Distinct means that no two different files will produce the same hash.

Predictable means the same file will always produce the same hash.

We can try it out with a command in Ubuntu: `sha1sum`.

Try using `ls` to list the files in your current directory, then use

`sha1sum <filename>` to see the SHA1 hash for that given file.

If you want, try creating some different text files and calculating their hash.

Changing even one letter will change the result!

Okay, so now let's get the signature for the EICAR testfiles.

Using the wget command, download the EICAR testfiles to Ubuntu:

```
cd ~ (Go back to your home directory)
```

```
wget https://secure.eicar.org/eicar.com
```

```
wget https://secure.eicar.org/eicar.com.txt
```

```
wget https://secure.eicar.org/eicar\_com.zip
```

```
wget https://secure.eicar.org/eicarcom2.zip
```

(If these commands don't work correctly, you can always RDP and open a web browser, then download from the EICAR website as you did in Part 1 – but it's often easier to just use wget for quick file downloads!)

Next, use sha1sum to get the hash of each file.

Which ones are the same? Which are different?



Checkpoint 5: You should be able to see the hashes for each of the four EICAR testfiles.



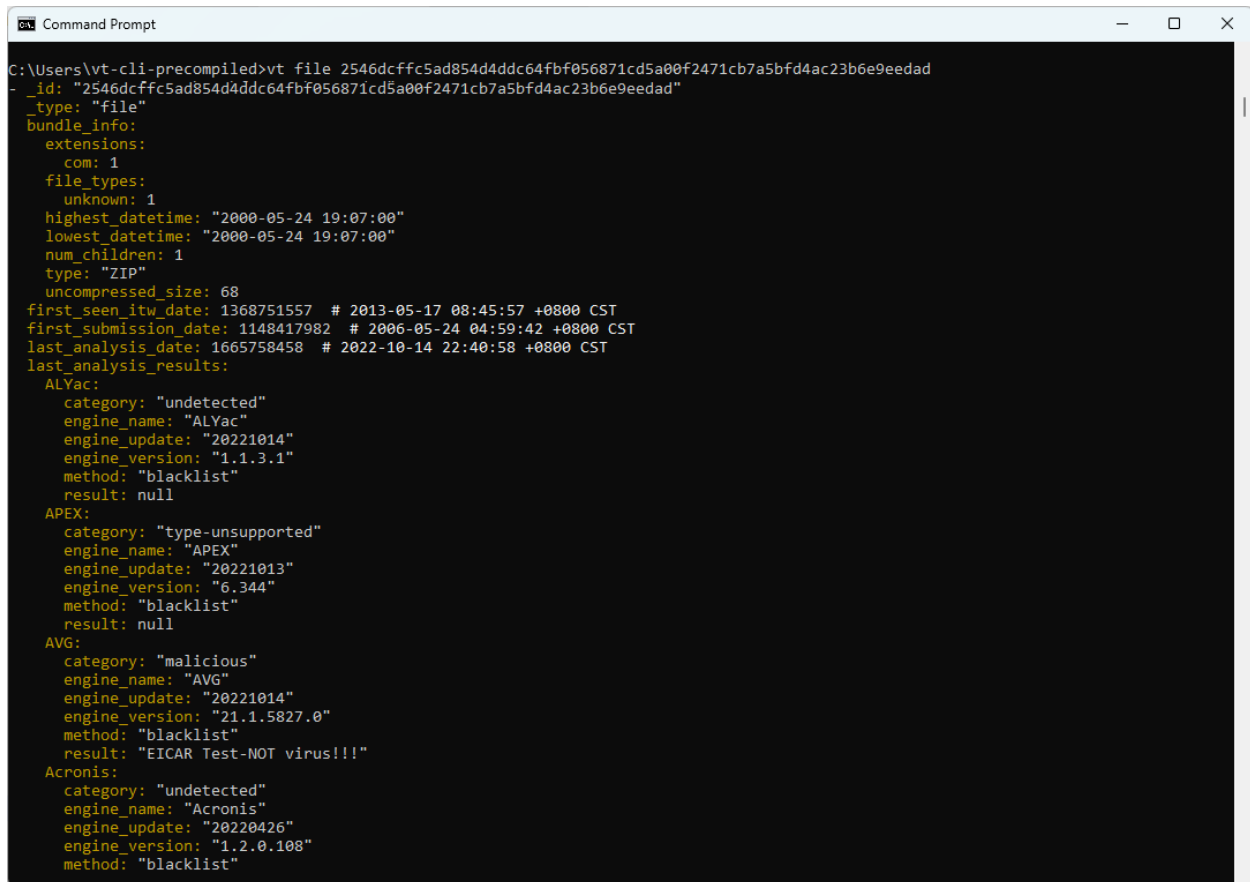
HINT: Stuck? Click [here](#) to see an example of using sha1sum to get hashes!

Step 6: Check if file is malicious using vt-cli

All right, so now let's see if EICAR recognizes these files. To poll the EICAR database, we have to give it a way to look up the file... You guessed it, it's the file's hash.

Use the vt file <File Hash Value> command to check each of your files!

Screenshot on vt-cli results



```
C:\Users\vt-cli-precompiled>vt file 2546dcffc5ad854d4ddc64fbf056871cd5a00f2471cb7a5bfd4ac23b6e9eedad
{
  "_id": "2546dcffc5ad854d4ddc64fbf056871cd5a00f2471cb7a5bfd4ac23b6e9eedad",
  "_type": "file",
  "bundle_info": {
    "extensions": {
      "com": 1
    },
    "file_types": {
      "unknown": 1
    },
    "highest_datetime": "2000-05-24 19:07:00",
    "lowest_datetime": "2000-05-24 19:07:00",
    "num_children": 1,
    "type": "ZIP",
    "uncompressed_size": 68
  },
  "first_seen_itw_date": 1368751557 # 2013-05-17 08:45:57 +0800 CST
  "first_submission_date": 1148417982 # 2006-05-24 04:59:42 +0800 CST
  "last_analysis_date": 1665758458 # 2022-10-14 22:40:58 +0800 CST
  "last_analysis_results": {
    "ALYac": {
      "category": "undetected",
      "engine_name": "ALYac",
      "engine_update": "20221014",
      "engine_version": "1.1.3.1",
      "method": "blacklist",
      "result": null
    },
    "APEX": {
      "category": "type-unsupported",
      "engine_name": "APEX",
      "engine_update": "20221013",
      "engine_version": "6.344",
      "method": "blacklist",
      "result": null
    },
    "AVG": {
      "category": "malicious",
      "engine_name": "AVG",
      "engine_update": "20221014",
      "engine_version": "21.1.5827.0",
      "method": "blacklist",
      "result": "EICAR Test-NOT virus!!!"
    },
    "Acronis": {
      "category": "undetected",
      "engine_name": "Acronis",
      "engine_update": "20220426",
      "engine_version": "1.2.0.108",
      "method": "blacklist"
    }
  }
}
```

Now the picture is coming together... VirusTotal doesn't store actual malware files (that would be a bad idea), but instead it stores the hashes of malware files. That allows users to check if their file is a virus by comparing its hash with those in the database. In the future, if you download something you're uncertain of, consider using VirusTotal to check it out!

[Expand all](#)[Back to top](#)[Go to bottom](#)

Select a repo

Edit Note Details

Change note title, set tags, cover photos, and other metadata here.

SkipNext