

---

## **Safe Malware Analysis with VirusTotal**

**(EICAR Test File)**

**Project:** Safe Malware Analysis with VirusTotal

**Author:** Mihira Seru

**Description:** Independent research on detecting safe test files (EICAR) using VirusTotal.

**Date:** November 2025

---

### **Step-by-Step Guide: Safe Malware Analysis Using the EICAR Test File and VirusTotal**

This guide demonstrates how to safely perform a basic malware analysis using the EICAR test file inside a virtual machine (VM).

It walks through setting up a secure environment, uploading the file to VirusTotal, interpreting antivirus detections, and restoring your system to a clean state.

The project helps beginners understand how security analysts verify and analyze potential threats without handling real malware.

---

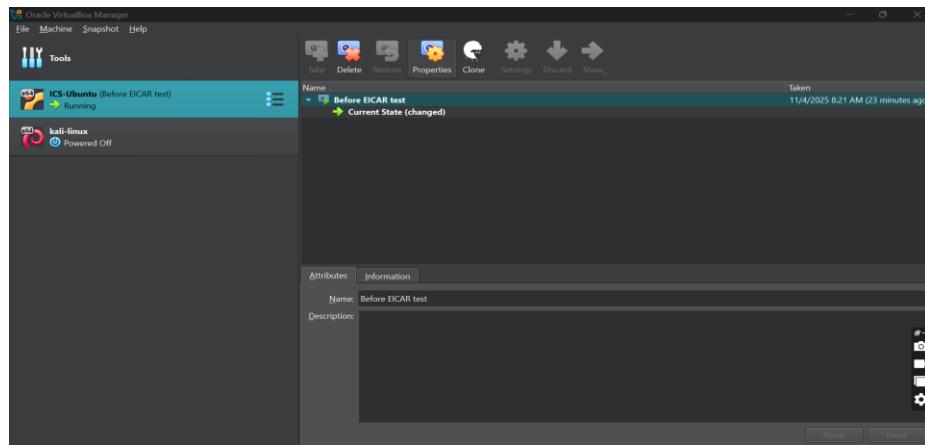
#### **Setting up lab environment for testing**

1. Open ubuntu VM
2. Take a snapshot as **Clean State**  
Machine → Take Snapshot...
  - A dialog appears:
  - Name: **Clean State** (or anything you like)
  - Description (optional): “Before EICAR test.”
  - Click OK
3. Restoring a Snapshot in VirtualBox - **use it only when something goes wrong**

- Restoring removes all changes made after the snapshot — useful for cleaning up experiments, undoing mistakes, or resetting before the next test.

Steps:

- Shut down the VM.
- In VirtualBox, open the **Snapshots** view.
- Select the snapshot you want to return to (e.g., *Clean State*).
- Click **Restore** → confirm.
- The VM will revert to exactly how it was when that snapshot was taken.



## Creating & testing a sample Virus file

1. For this we use a website named [eicar.org](http://eicar.org), to get the standard (trusted) virus files for testing. So that, they don't affect your system.

Steps:

- Open nano editor with filename as : EICAR.org  
**\$nano EICAR.com**
- Enter the string as shown, then press **Ctrl + O** → **Enter** → **Ctrl + X**
- Use **ls** command to verify if the file got saved or not

```
mihira@mihira-VirtualBox: ~
```

GNU nano 6.2 EICAR.com \*

<50!P%@AP[4\PZX54(P^)7CC)7]\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H\*

- Now we have created our sample antivirus file for testing.

2. Open your browser (inside the VM) and go to: <https://www.virustotal.com>



- **VirusTotal** is a free site that scans files with many antivirus engines to check for threats. Uploading our EICAR file shows how antivirus detections work in real time.
  - Uploading [EICAR.com](http://EICAR.com) to VirusTotal

- These are the detections from various antivirus (AV) engines.

**Note:** Do **not** perform this on your host system.  
 The EICAR test file may still trigger alerts even though it's harmless.  
 Always use an isolated VM for safe handling.

## Analysing results on VirusTotal

### 1. Detection Overview:

- The file has **61/68 detections**, meaning 61 antivirus engines identified it as malicious.
- The **Community Score 224** shows that VirusTotal users also recognized it as a known test file.



### 2. Popular Threat Label:

Popular threat label ⓘ virus.eicar/test

Threat categories virus

Family labels eicar test file

- It's labeled as **virus.eicar/test**, which means this is the **EICAR test file**, a *non-malicious* file used to check antivirus detection.
- Many AVs tag it as "Test File" or "EICAR-Test-NOT Virus," confirming it's safe.

### 3. Vendor Analysis Table:

Security vendors' analysis ⓘ		Do you want to automate checks?	
AhnLab-V3	ⓘ Virus/EICAR_Test_File	Alibaba	ⓘ Virus:Win32/EICAR.A
AliCloud	ⓘ Engtest:Multi/Eicar	ALYac	ⓘ Misc.Eicar-Test-File
Arcabit	ⓘ EICAR-Test-File (not A Virus)	Avast	ⓘ EICAR Test-NOT Virus!!!
Avast-Mobile	ⓘ Eicar	AVG	ⓘ EICAR Test-NOT Virus!!!
Avira (no cloud)	ⓘ Eicar-Test-Signature	Baidu	ⓘ Win32.Test.Eicar.a
BitDefender	ⓘ EICAR-Test-File (not A Virus)	ClamAV	ⓘ Eicar-Signature
CTX	ⓘ Txt.virus.eicar	Cynet	ⓘ Malicious (score: 99)
DrWeb	ⓘ EICAR Test File (NOT A Virus!)	Elastic	ⓘ Eicar
Emsisoft	ⓘ EICAR-Test-File (not A Virus) (B)	eScan	ⓘ EICAR-Test-File
ESET-NOD32	ⓘ Eicar Test File	Fortinet	ⓘ EICAR_TEST_FILE
GData	ⓘ EICAR_TEST_FILE	Google	ⓘ Detected
Huorong	ⓘ TEST/AEngTestFile EICAR	Ikarus	ⓘ EICAR-Test-File



- Each antivirus engine's result is listed.
- For example, **Avast** → **"EICAR Test-NOT Virus!!!"** and **Arcabit** → **"EICAR-Test-File (not A Virus)"** clearly indicate it's not real malware.

Field	Description
<b>Security Vendor</b>	<b>Name of the antivirus engine</b> (e.g., Avast, Kaspersky).
<b>Detection Name / Result</b>	<b>What the engine labeled the file as</b> (e.g., <i>EICAR-Test-File</i> , <i>Trojan.Win32</i> ).
<b>Severity Icon</b>	<b>Shows if the file is malicious</b> ⓘ or clean ⓘ.
<b>Category / Family Label</b>	<b>Type or family of threat</b> (e.g., <i>EICAR</i> , <i>Trojan</i> , <i>Worm</i> ).
<b>Community Tags</b>	<b>Keywords describing file behavior or context</b> (e.g., <i>powershell</i> , <i>attachment</i> ).

### 4. Details tab

The screenshot shows the 'DETAILS' tab of a VirusShare file analysis page. It includes sections for 'Basic properties', 'History', and 'Names'. The 'Basic properties' section lists various file characteristics like MD5, SHA-1, SHA-256, SSDeep, TLSH, File type, Magic, TrID, Magika, and File size. The 'History' section shows submission and analysis dates. The 'Names' section lists the file's name and source.

Property	Value
MD5	69630e4574ec6798239b091cda43dca0
SHA-1	c9bd99fdff007f5adf4cc2be48005cea317c62
SHA-256	131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbd8267
SSDeep	3:a+JraNvsgzsVqSwHqNtJuOgzsky
TLSH	T1E6A022003B0EEE2BA20B00200032E8B00808020F2CE00A3820A020BBC83308803EC228
File type	Powershell <a href="#">source</a> <a href="#">powershell</a> <a href="#">ps</a> <a href="#">ps1</a>
Magic	EICAR virus test files
TrID	EICAR antivirus test file (100%)
Magika	POWERSHELL
File size	69 B (69 bytes)

Date	Event
First Seen In The Wild	2020-02-18 13:15:46 UTC
First Submission	2006-05-23 17:26:21 UTC
Last Submission	2025-11-04 03:52:46 UTC
Last Analysis	2025-11-04 03:33:55 UTC

Name	Source
eicar.txt	
EICAR.com	

- File info like hash values (MD5, SHA-1, SHA-256), size, file type, creation time, and signatures. Used to verify integrity and identify file type.

## 5. Relations tab

The screenshot shows the 'RELATIONS' tab of a VirusShare file analysis page. It includes sections for 'Contacted Domains', 'Execution Parents', and 'Dropped Files'. The 'Contacted Domains' section shows one domain: ctld.windowsupdate.com. The 'Execution Parents' section shows multiple entries with dates, detection counts, types, and names. The 'Dropped Files' section shows 10 items.

Domain	Detections	Created	Registrar
ctld.windowsupdate.com	0 / 95	1997-07-22	CSC Corporate Domains, Inc.

Scanned	Detections	Type	Name
2025-10-28	57 / 72	Win32 EXE	0020c5419a3e578707fa67d365b8de1cbc40c526edc967d026552d1929c3e1e8
2025-10-16	49 / 72	Win32 EXE	m9m1jutt.exe
2025-11-04	15 / 38	ZIP	awslabs_service-workbench-on-aws.zip
2025-10-28	55 / 72	Win32 EXE	fsa_downloader_98a91c.exe
2025-10-28	56 / 72	Win32 EXE	9f9bc9150a86d8c833fa52e12755ad77.virus
2024-10-23	53 / 68	ZIP	ThundralImageLinkExtractor.zip
2023-10-02	56 / 72	Win32 EXE	00533a84a3cc5442762c8402652408b86cc8ff2fecb18aae4f906a00c64de029
2025-04-22	55 / 72	Win32 EXE	0.49391562435309044
2025-10-28	47 / 68	ZIP	JensWalter_jens.dev.zip
2025-10-28	56 / 72	Win32 EXE	227227944

File	Count
...	...
Dropped Files (10)	10

- Shows links between this file and other items (e.g., URLs or IPs it contacted).

## 6. Behaviour tab

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Display grouped sandbox reports

Sandbox	Detections	Actions
CAPE Linux	△ 0 M 1 W 1 S 0 E 0 P 0	<input checked="" type="checkbox"/> CAPE Sandbox
Lastline	△ 2 M 0 W 0 S 0 E 0 P 0	<input checked="" type="checkbox"/> VirusTotal Jujubox
VirusTotal Observer	△ 0 M 0 W 0 S 0 E 0 P 0	<input checked="" type="checkbox"/> Zenbox

Activity Summary

Download Artifacts ▾ Full Reports ▾ Help ▾

Category	Count	Details
△ Detections	2	2 MALWARE, 2 TROJAN
Mitre Signatures	4 MEDIUM, 10 LOW, 8 INFO	
IDS Rules	1 LOW	
Sigma Rules	NOT FOUND	
Dropped Files	8 OTHER, 1 TEXT, 1 PE_EXE	TEXT
Network comms	NOT FOUND	

Behavior Tags ○

- Shows what the file *does* when executed in VirusTotal's sandbox (e.g., creates files, modifies registry, connects to IPs). For EICAR, this will be empty since it's harmless.

## 7. Community tab

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Contained in Graphs (28) ○

User	Comment	Timestamp
NC_1	Copy of Process Hacker Lookup	2025-08-14 15:14:34
miniuuser	Cyber_Folks S.A. entrance gate s3[.]tld[.]pl to Canada via SQLi Dumper.exe	2025-06-21 19:52:04
Marla.Naples	delete app	2025-06-13 18:00:20
bigosys	Telco Related	2025-04-27 04:27:03
jwanihad	Evidence of ongoing #DataBreach at the University of Alberta - #UAlberta #UAlbertaHacked #youralberta - 04.17....	2025-04-17 22:05:25
Silver9x9x	gentlent.com	2025-04-16 04:56:05
miniuuser	Copy of Still Not Fixed - 04.08.25>>SPREADER 0072ba59a039602494a7a40139142d0b0379c1c36f3a71b25d8426f9...	2025-04-15 18:49:47
miniuuser	stolen credentials by karanPC dot com	2025-02-22 15:58:24
jwanihad	Copy of basic principle of valid certs & a nice business plan with leaked credentials	2025-02-18 22:55:27
miniuuser	basic principle of valid certs & a nice business plan with leaked credentials	2025-02-17 21:05:35

- Comments and votes from other analysts about the file.

## After the Test

1. **Delete** the [EICAR.com](#) file from your VM (optional, since it's harmless).
  2. **Restore your snapshot** to return the VM to a clean state — this removes all test activity and keeps your analysis environment safe for future labs.
- 

## Key Takeaways

- Learned how antivirus engines identify known signatures
- Understood VirusTotal's behaviour and metadata analysis tabs
- Practiced safe malware handling inside an isolated VM