Scenario 1: A normal JPEG file is downloaded:

In this scenario, the user downloads a valid JPEG file from the following website.

Step 1:
The user starts ZAP by clicking on the menu **Extension FileTester** -> **Activate/Deactivate Extension** button.

A popup appears, informing the user that the extension has been activated.

Step 2:
The user starts his browser and goes to the following link, to download the JPEG image file.

The browser/download manager starts downloading the file and ZAP checks starts capturing the responses.

The FileTester extension starts scanning the file that is being downloaded.

The extension checks whether the downloading file is of the types, **JPEG**, **PNG**, **ZIP** or **EXE.** Once that is valid, it starts checking whether the JPEG file has valid image data.

Once the extension has confirmed the validity of the JPEG file, it then starts to scan and extract the EXIF metadata from the file.

Step 3:
The user can view the report of the scans anytime by clicking on **Extension FileTester** -> **Get Report of Scans** button. Once the user clicks on the Get Report of Scans button, a text file is

generated on the main zaproxy directory and it contains the results of all the scans that’s been performed on the file. The user can open the file using a simple text editor to view the report of scans.

The user can click on the **Extension FileTester** -> **Activate/Deactivate Extension** button again to deactivate the FileTester extension.

Scenario 2: A RAR file is downloaded

In this scenario, the user downloads a file type (RAR) that the extension does not support.

<u>Step 1:</u>

The user starts ZAP by clicking on the menu **Extension FileTester** -> **Activate/Deactivate Extension** button.

A popup appears, informing the user that the extension has been activated.

<u>Step 2:</u>

The user starts his browser and goes to the following link, to download the RAR image file.

The browser/download manager starts downloading the file and ZAP checks starts capturing the responses.

The FileTester extension starts scanning the file that is being downloaded.

The extension checks whether the downloading file is of the types, **JPEG**, **PNG**, **ZIP** or **EXE.** Once the extension recognizes that the file is not a part of the supported file types, it stops processing the file.

The user can click on the **Extension FileTester** -> **Activate/Deactivate Extension** button again to deactivate the FileTester extension.

Scenario 3: An invalid JPEG file is downloaded

In this scenario, the user downloads an invalid JPEG file from the following website.

Step 1:

The user starts ZAP by clicking on the menu **Extension FileTester** -> **Activate/Deactivate Extension** button.

A popup appears, informing the user that the extension has been activated.

Step 2:

The user starts his browser and goes to the following link, to download the JPEG image file.

The browser/download manager starts downloading the file and ZAP checks starts capturing the responses.

The FileTester extension starts scanning the file that is being downloaded.

The extension checks whether the downloading file is of the types, **JPEG**, **PNG**, **ZIP** or **EXE.** Once the file extension is valid, it starts checking whether the JPEG file has valid image data.

Once the extension has confirmed the JPEG file is invalid, it throws an alert popup box, informing the user that the file is invalid and suspicious.

In this scenario, the extension does not proceed to scan and extract the EXIF metadata from the file.

Step 3:

The user can view the report of the scans anytime by clicking on **Extension FileTester** -> **Get Report of Scans** button. Once the user clicks on the Get Report of Scans button, a text file is generated on the main zaproxy directory and it contains the results of all the scans that's been performed on the file. The user can open the file using a simple text editor to view the report of scans.

The user can click on the **Extension FileTester** -> **Activate/Deactivate Extension** button again to deactivate the FileTester extension.

Scenario 4: A Zipbomb file is downloaded

In this scenario, the user downloads a ZIP file from the following website that is unfortunately a malicious Zip Bomb.

Step 1:

The user starts ZAP by clicking on the menu **Extension FileTester** -> **Activate/Deactivate Extension** button.

A popup appears, informing the user that the extension has been activated.

Step 2:

The user starts his browser and goes to the following link, to download the Zip file.

The browser/download manager starts downloading the file and ZAP checks starts capturing the responses.

The FileTester extension starts scanning the file that is being downloaded.

The extension checks whether the downloading file is of the types, **JPEG**, **PNG**, **ZIP** or **EXE.** Once that is valid, it starts checking whether the ZIP file is password-protected.

Then the Zip file is checked for the presence of any ZIP bombs. Once the extension identifies the file as a Zip bomb, it throws an alert pop-up, informing the user that the file is an invalid/suspicious file.

Step 3:

The user can view the report of the scans anytime by clicking on **Extension FileTester** -> **Get Report of Scans** button. Once the user clicks on the Get Report of Scans button, a text file is generated on the main zaproxy directory and it contains the results of all the scans that’s been performed on the file. The user can open the file using a simple text editor to view the report of scans.

The user can click on the **Extension FileTester** -> **Activate/Deactivate Extension** button again to deactivate the FileTester extension.

Scenario 5: A malicious Exe file is downloaded

In this scenario, the user downloads an exe file from the following website that unfortunately contains a malicious virus.

<u>Step 1:</u>
The user starts ZAP by clicking on the menu **Extension FileTester** -> **Activate/Deactivate Extension** button.

A popup appears, informing the user that the extension has been activated.

<u>Step 2:</u>
The user starts his browser and goes to the following link, to download the exe file.

The browser/download manager starts downloading the file and ZAP checks starts capturing the responses.

The FileTester extension starts scanning the file that is being downloaded.

The extension checks whether the downloading file is of the types, **JPEG**, **PNG**, **ZIP** or **EXE.** Once the file is identified as an exe, the extension sends the exe file to VirusTotal via an api, for scanning for viruses.

<u>Note:</u> The VirusTotal server takes a few minutes to complete the scan on the exe file. So, the user has to wait a while before getting the results of the virus scan.

<u>Step 3:</u>

The user can view the report of the scans anytime by clicking on **Extension FileTester** -> **Get Report of Scans** button. Once the user clicks on the Get Report of Scans button, a text file is generated on the main zaproxy directory and it contains the results of all the scans that's been performed on the file.

If the exe file is still being scanned, the user would be informed in the report text file that the exe file is still being scanned by VirusTotal. Every time the **Get Report of Scans** button is clicked, a call is made to the VirusTotal API to check whether the scanning is completed.

Once the file has been scanned successfully, the user would be informed of the results of the scan in the report text file.

The user can open the file using a simple text editor and check whether the exe file is identified as a virus or a safe file.

The user can click on the **Extension FileTester** -> **Activate/Deactivate Extension** button again to deactivate the FileTester extension.