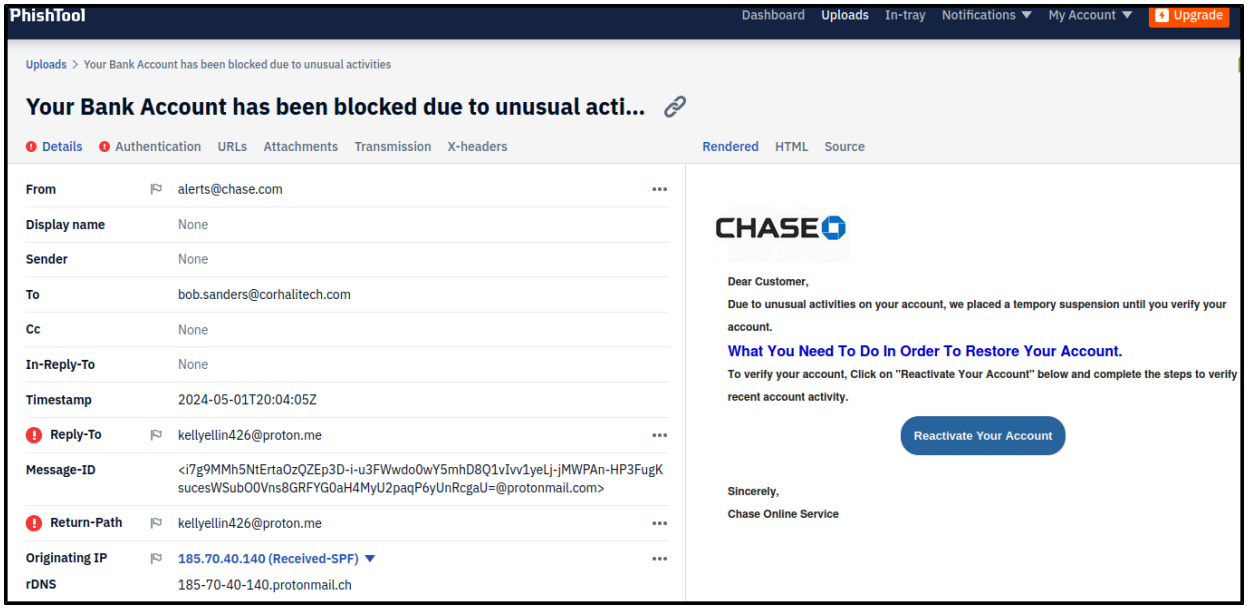
Automated Email Analysis with PhishTool

Manual email analysis, while thorough, can be time-consuming in high-volume environments. Automated analysis tools like PhishTool streamline the investigation process by performing many manual checks simultaneously, extracting key indicators, and providing consolidated reports. These tools integrate multiple analysis techniques covered in previous sections - header analysis, authentication checking, URL extraction, and attachment scanning - into a single platform with automated threat intelligence lookups.

PhishTool

While there is an enterprise edition of Phishtool, there also is a free tool. Note that this will need an account, so you would need to sign up with an email address, even for the free version.

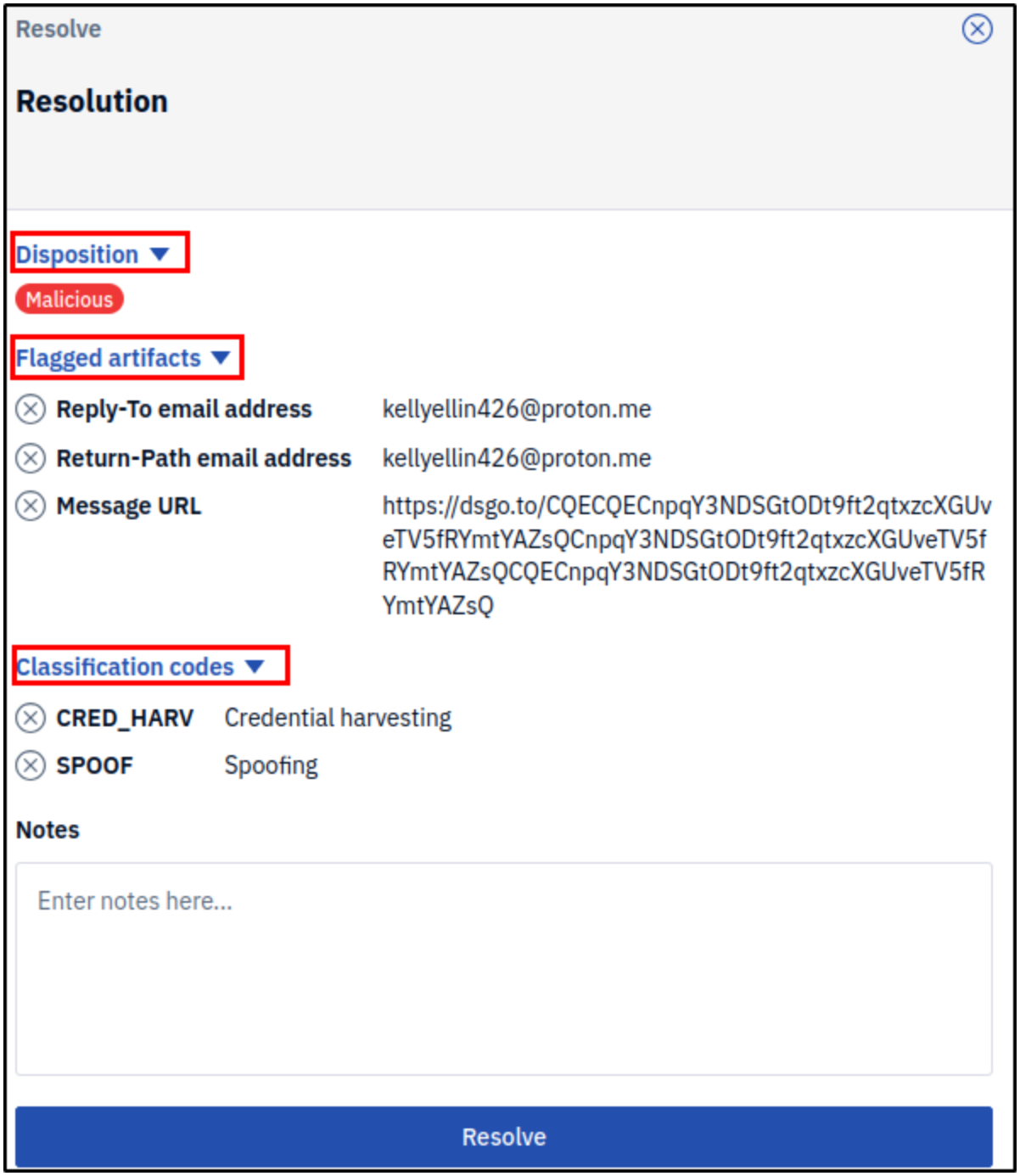
When you upload an eml file to PhishTool, it displays the email for you with options for Rendered, HTML and Source. On the left, it provides Header information, with a number of alerts if anything suspicious is found. In the below screenshot it gives alerts for the Reply-To and Return-Path being different to the From: header. There also is an Alert about the DMARC check failing under the Authentication tab.



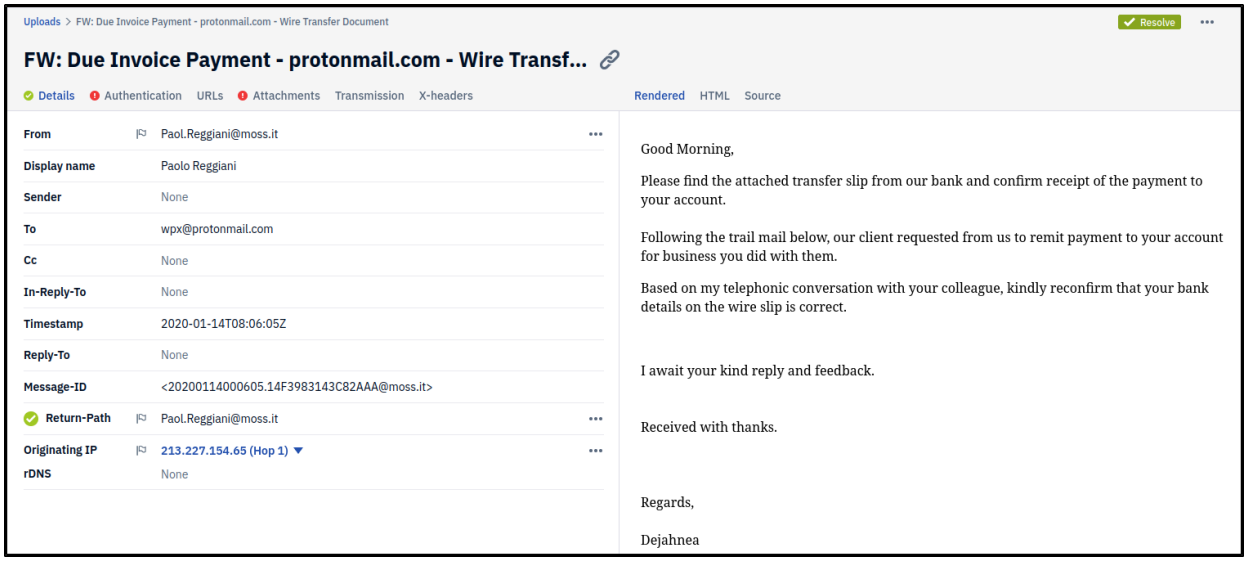
Additionally, it extracts URLs, Attachments, Transmissions and X-headers. The Transmissions tab shows the Received-chain.

It is even possible to get automatic VirusTotal results for the URLs and attachments if you configure your PhishTool account with a VirusTotal API key.

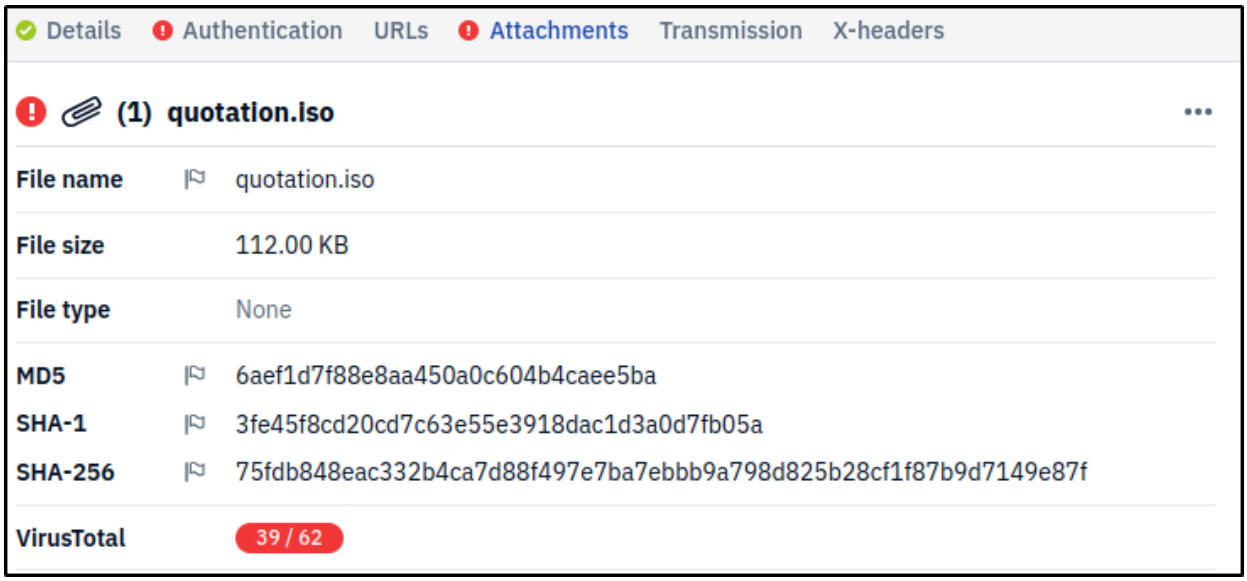
Once you have made a conclusion, you can click on Resolve in the upper right, and fill in whether the email was safe or malicious under Disposition, as well as add Flagged artifacts and Classification codes.



We can take a look at another eml file, this time one with an attachment. This is the same email examined in the Attachment Analysis section.



The alerts show that there is an issue with Authentication (both SPF and DMARC failed) and an alert for an Attachment:



Just like was determined in the Attachment Analysis section, quotation.iso was deemed malicious by PhishTool.

While not all organizations use this particular tool, it is clear that PhishTool, and other tools like this save a lot of time.

Summary

PhishTool demonstrates how automated email analysis platforms can significantly reduce investigation time while maintaining analysis quality. The tool performs comprehensive checks including header analysis, authentication verification, URL and attachment extraction, and automatic VirusTotal integration through API keys. It provides structured reporting with

disposition tracking and artifact flagging, making it suitable for organizational incident response workflows. While automation tools are valuable for efficiency and consistency, they complement rather than replace manual analysis skills, as complex threats may require deeper investigation beyond automated capabilities.