 Email header analysis

Some of the pertinent information that we need to collect can be obtained visually from an email client or web client (such as Gmail, Yahoo!, etc.). But some information, such as the sender's IP address and reply-to information, can only be obtained via the email header.

In [Phishing Emails 1](https://tryhackme.com/room/phishingemails1tryoe), we saw how to obtain this information manually by sifting through an email's source code.

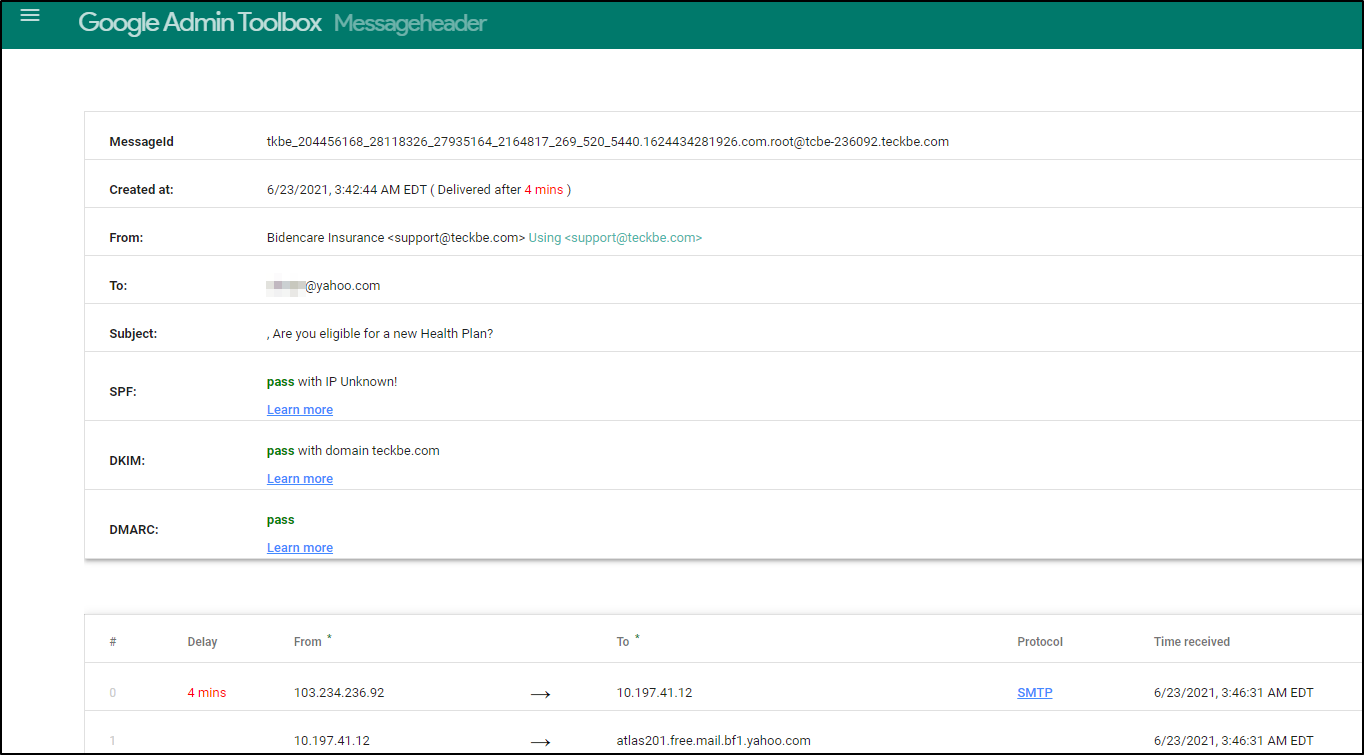
Below we'll look at some tools that will help us retrieve this information.

First up to bat is a tool from Google that can assist us with analyzing email headers called **Messageheader** from the Google Admin Toolbox.

Per the [site](https://toolbox.googleapps.com/apps/main/), "*Messageheader analyzes SMTP message headers, which help identify the root cause of delivery delays. You can detect misconfigured servers and mail-routing problems*".

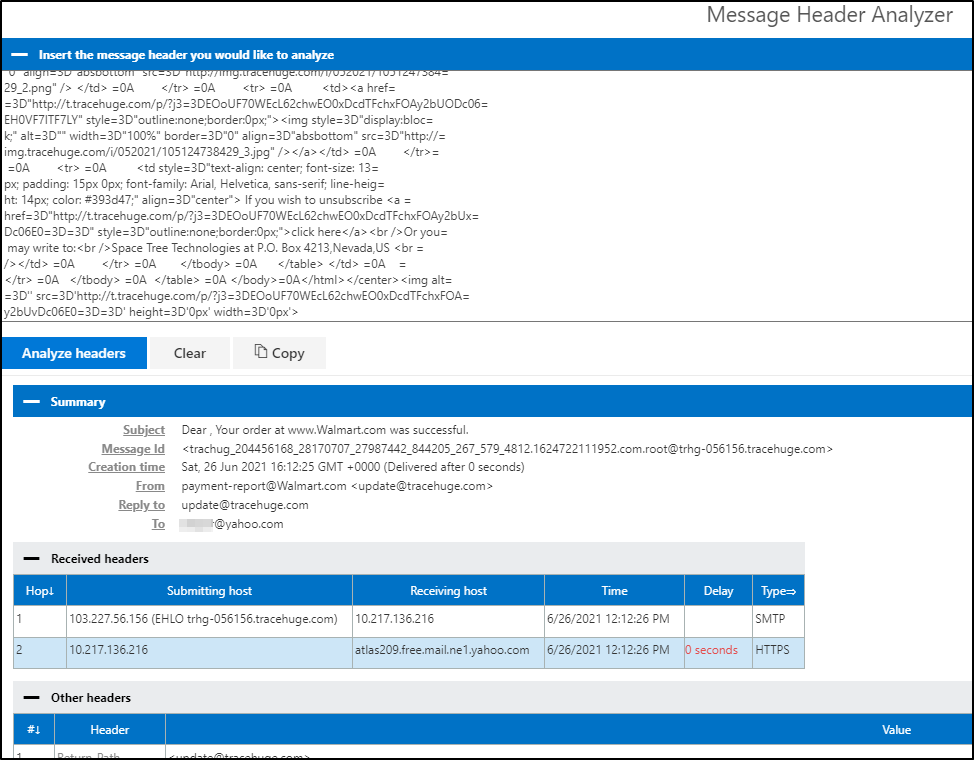
**Usage**: Copy and paste the entire email header and run the analysis tool.

* **Messageheader**: <https://toolbox.googleapps.com/apps/messageheader/analyzeheader>

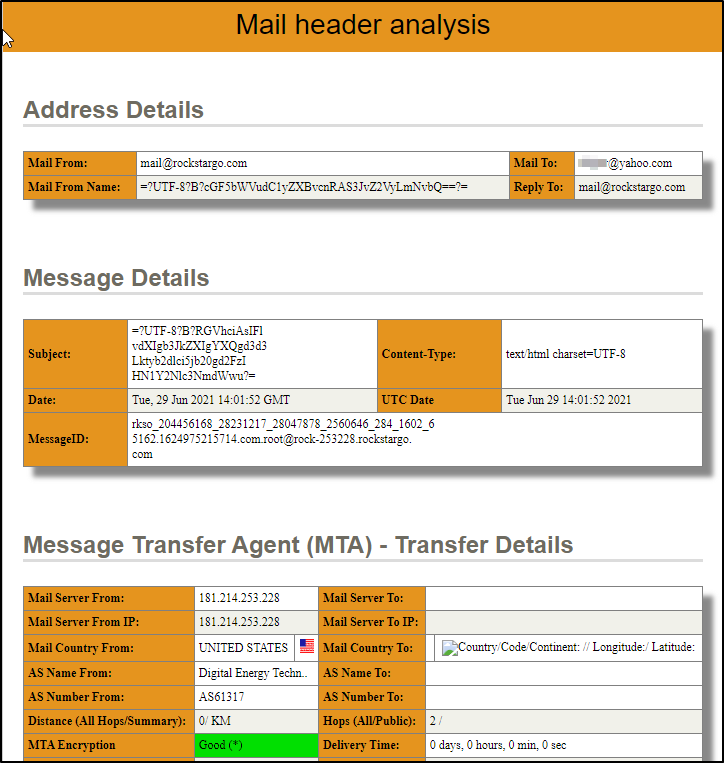


Another tool is called **Message Header Analyzer**.

* **Message Header Analyzer**: <https://mha.azurewebsites.net/>



Lastly, you can also use [mailheader.org](https://mailheader.org/).



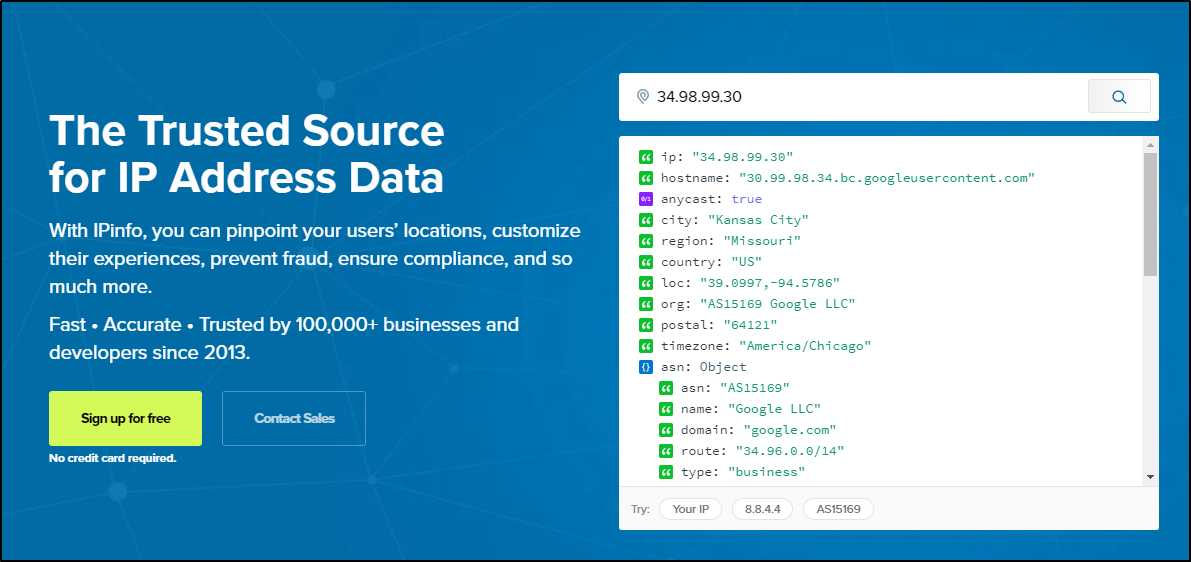
Even though not covered in the previous Phishing rooms, a Message Transfer Agent (MTA) is software that transfers emails between sender and recipient. Read more about MTAs [here](https://csrc.nist.gov/glossary/term/mail_transfer_agent). Since we're on the subject, read about MUAs (Mail User Agent) [here](https://csrc.nist.gov/glossary/term/mail_user_agent).

**Note**: The option on which tool to use rests ultimately on you. It is good to have multiple resources to refer to as each tool might reveal information that another tool may not reveal.

The tools below can help you analyze information about the sender's IP address:

* IPinfo.io: <https://ipinfo.io/>

Per the [site](https://ipinfo.io/), "*With IPinfo, you can pinpoint your users’ locations, customize their experiences, prevent fraud, ensure compliance, and so much more*".



* URLScan.io: <https://urlscan.io/>

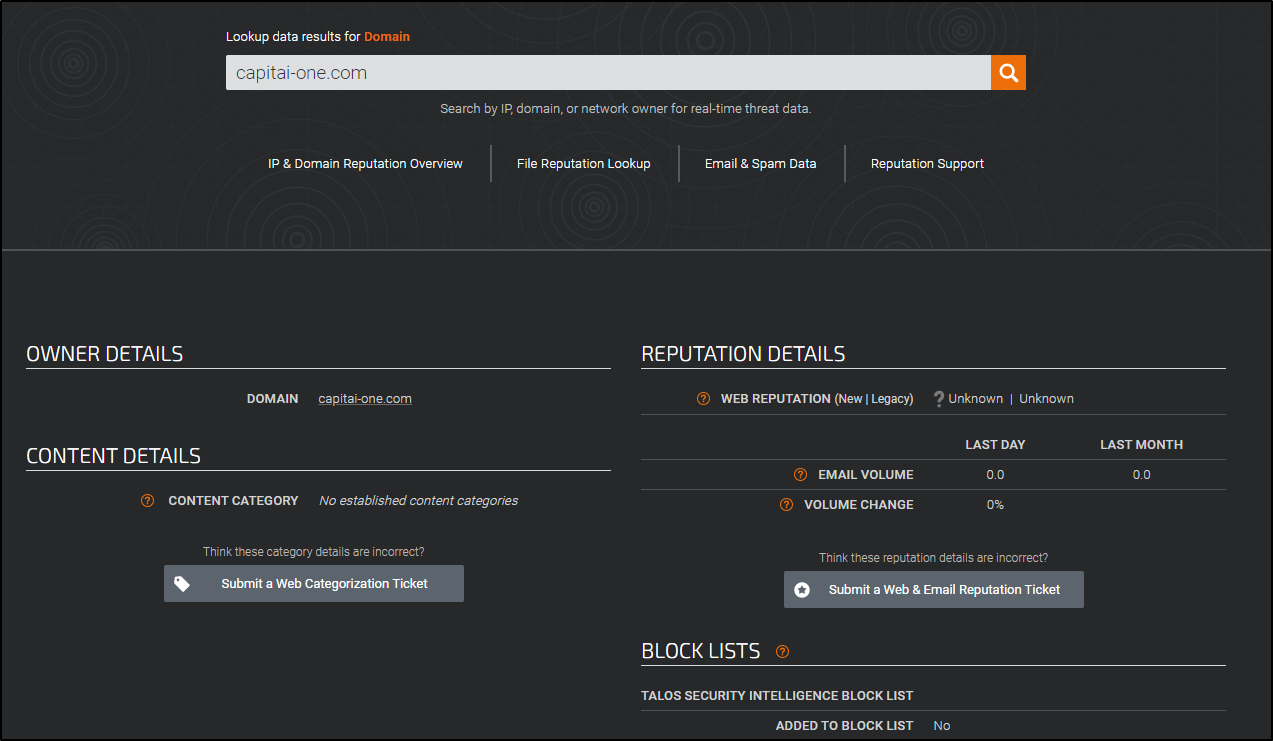
Per the [site](https://urlscan.io/about/), "*urlscan.io is a free service to scan and analyse websites. When a URL is submitted to urlscan.io, an automated process will browse to the URL like a regular user and record the activity that this page navigation creates. This includes the domains and IPs contacted, the resources (JavaScript, CSS, etc) requested from those domains, as well as additional information about the page itself. urlscan.io will take a screenshot of the page, record the DOM content, JavaScript global variables, cookies created by the page, and a myriad of other observations. If the site is targeting the users one of the more than 400 brands tracked by urlscan.io, it will be highlighted as potentially malicious in the scan results*".



Notice that urlscan.io provides a screenshot of the URL. This screenshot is provided, so you don't have to navigate to the URL in question explicitly.

You can use other tools that provide the same functionality and more, such as [URL2PNG](https://www.url2png.com/) and [Wannabrowser](https://www.wannabrowser.net/" \t "_blank).

* Talos Reputation Center: <https://talosintelligence.com/reputation>



***Answer the questions below***

What is the official site name of the bank that capitai-one.com tried to resemble?

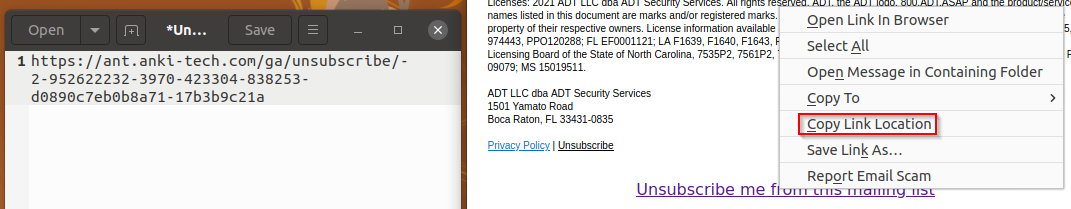


 Email body analysis

Now it's time to direct your focus to the email body. This is where the malicious payload may be delivered to the recipient either as a link or an attachment.

Links can be extracted manually, either directly from an HTML formatted email or by sifting through the raw email header.

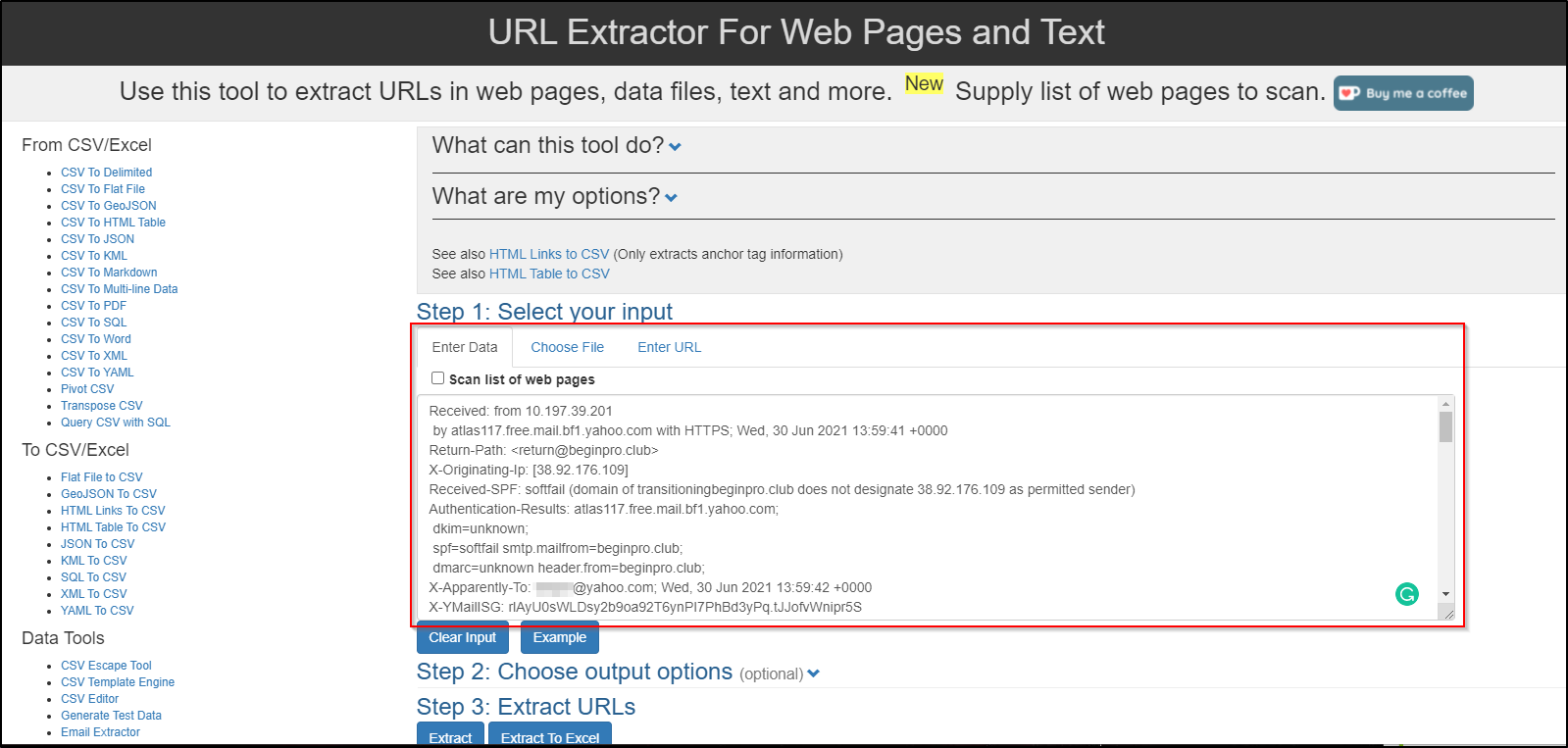
Below is an example of obtaining a link manually from an email by right-clicking the link and choosing **Copy Link Location**.



The same can be accomplished with the assistance of a tool. One tool that can aid us with this task is URL Extractor.

* URL Extractor: <https://www.convertcsv.com/url-extractor.htm>

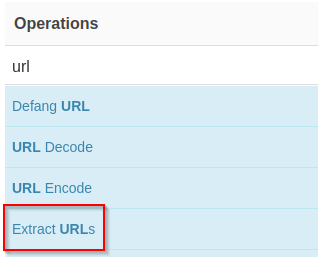
You can copy and paste the raw header into the text box for **Step 1: Select your input**.



The extracted URLs are visible in **Step 3**.



You may also use [CyberChef](https://gchq.github.io/CyberChef/" \t "_blank) to extract URLs with the Extract URLs recipe.



**Tip**: It's important to note the root domain for the extracted URLs. You will need to perform an analysis on the root domain as well.

After extracting the URLs, the next step is to check the reputation of the URLs and root domain. You can use any of the tools mentioned in the previous task to aid you with this.

If the email has an attachment, you'll need to obtain the attachment safely. Accomplishing this is easy in Thunderbird by using the Save button.

https://assets.tryhackme.com/additional/phishing2/save-attachment.png

After you have obtained the attachment, you can then get its hash. You can check the file's reputation with the hash to see if it's a known malicious document.

Obtain the file's SHA256 hash

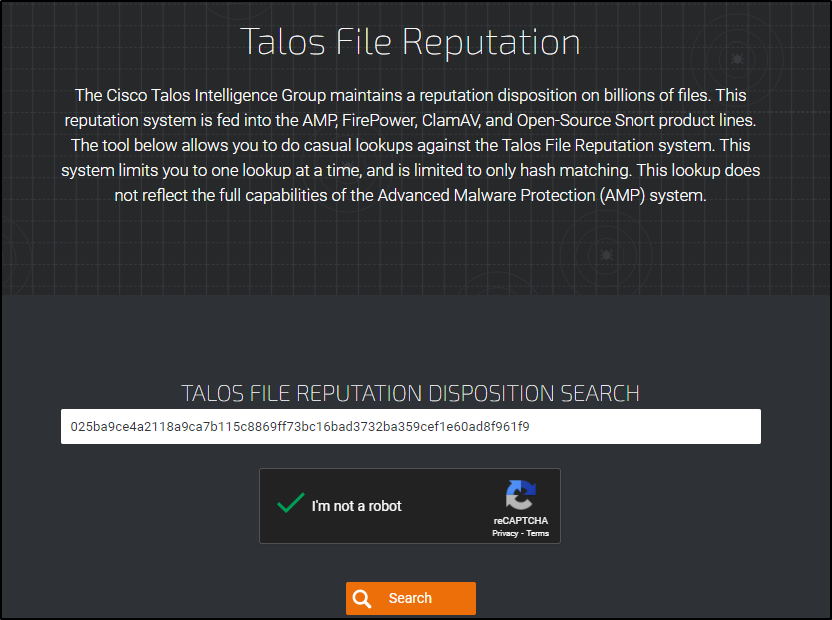
user@machine**$** sha256sum Double\ Jackpot\ Slots\ Las\ Vegas.dot

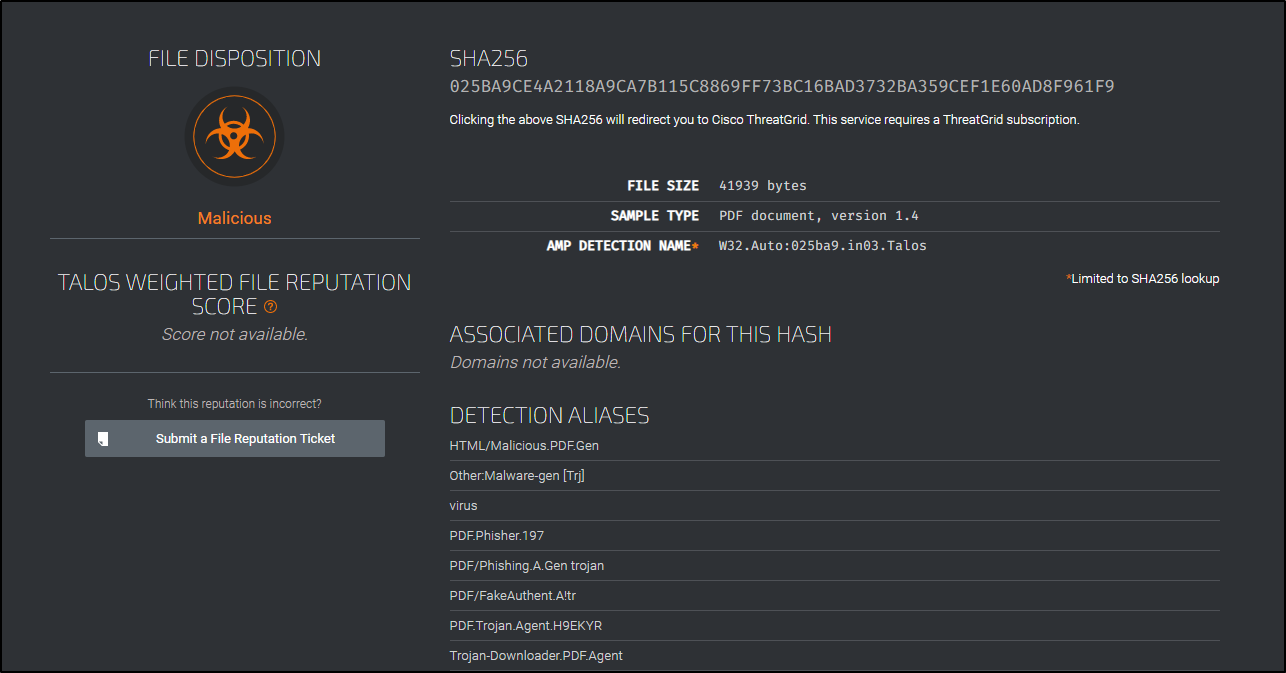
c650f397a9193db6a2e1a273577d8d84c5668d03c06ba99b17e4f6617af4ee83 Double Jackpot Slots Las Vegas.dot

There are many tools available to help us with this, but we'll focus on two primarily; they are listed below:

* Talos File Reputation: <https://talosintelligence.com/talos_file_reputation>

Per the[site](https://talosintelligence.com/talos_file_reputation), "*The Cisco Talos Intelligence Group maintains a reputation disposition on billions of files. This reputation system is fed into the AMP, FirePower, ClamAV, and Open-Source Snort product lines. The tool below allows you to do casual lookups against the Talos File Reputation system. This system limits you to one lookup at a time, and is limited to only hash matching. This lookup does not reflect the full capabilities of the Advanced Malware Protection (AMP) system*".

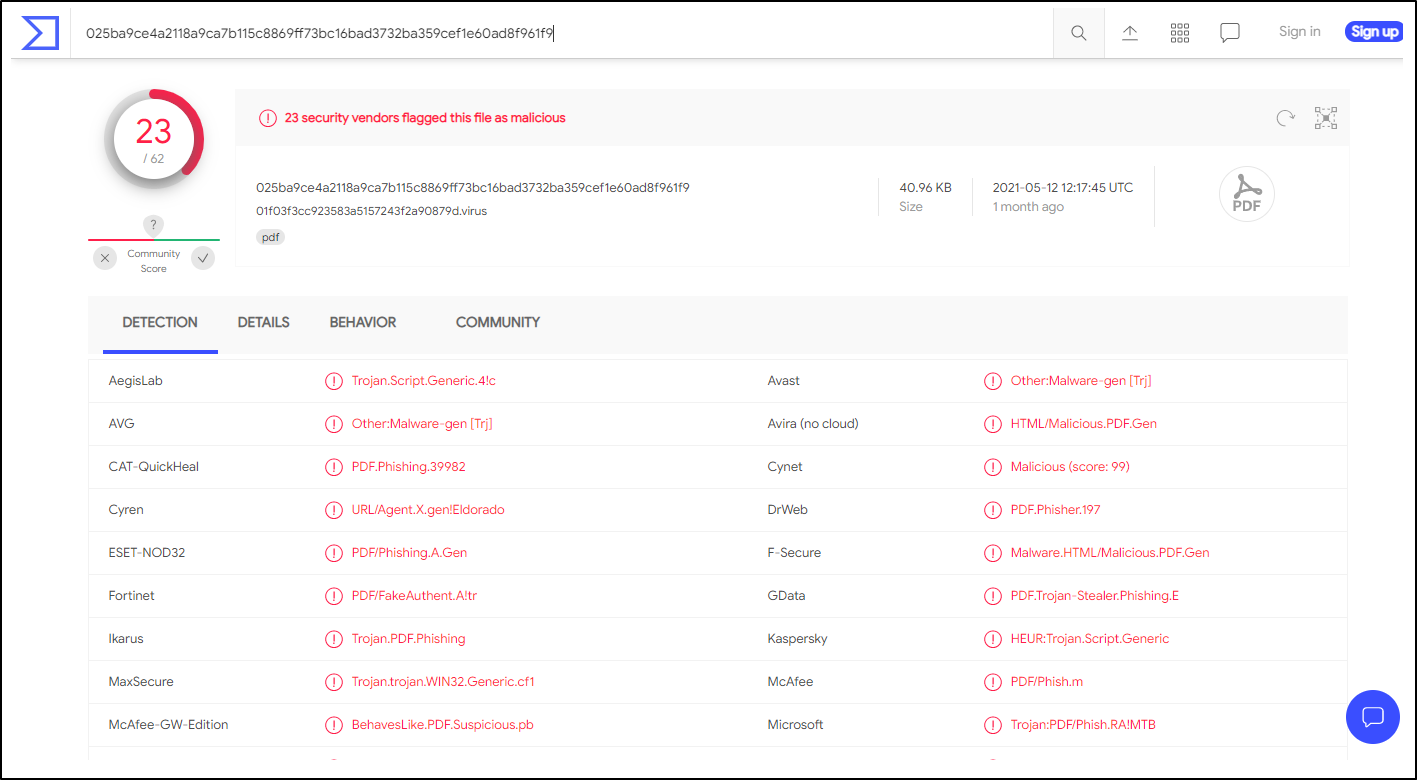




* VirusTotal: <https://www.virustotal.com/gui/>

Per the [site](https://www.virustotal.com/gui/), "Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community."





Another tool/company worth mentioning is [Reversing Labs](https://www.reversinglabs.com/), which also has a [file reputation service](https://register.reversinglabs.com/file_reputation).

***Answer the questions below***

How can you manually get the location of a hyperlink?

 Malware Sandbox

Luckily as Defenders, we don't need to have malware analysis skills to dissect and reverse engineer a malicious attachment to understand the malware better.

There are online tools and services where malicious files can be uploaded and analyzed to better understand what the malware was programmed to do. These services are known as malware sandboxes.

For instance, we can upload an attachment we obtained from a potentially malicious email and see what URLs it attempts to communicate with, what additional payloads are downloaded to the endpoint, persistence mechanisms, Indicators of Compromise (IOCs), etc.

Some of these online malware sandboxes are listed below.

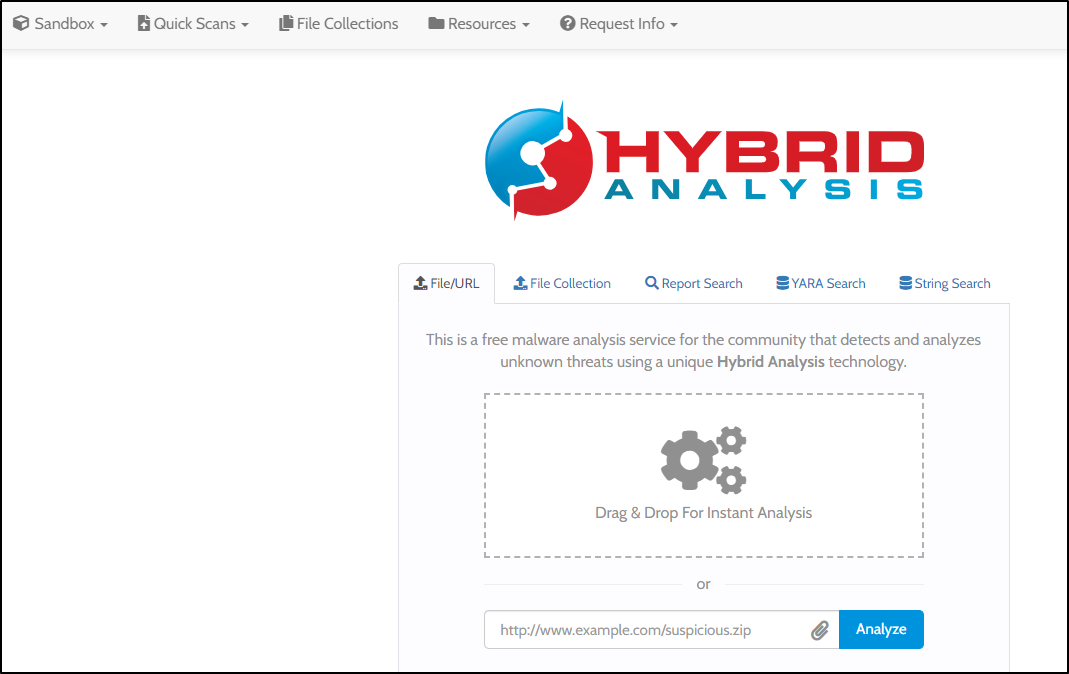
* Any.Run: <https://app.any.run/>

Per the [site](https://app.any.run/), "*Analyze a network, file, module, and the registry activity. Interact with the OS directly from a browser. See the feedback from your actions immediately*".



* Hybrid Analysis: <https://www.hybrid-analysis.com/>

Per the site, *"This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique Hybrid Analysis technology*."



* <https://www.joesecurity.org/>

Per the site, "*Joe Sandbox empowers analysts with a large spectrum of product features. Among them: Live Interaction, URL Analysis & AI based Phishing Detection, Yara and Sigma rules support, MITRE ATT&CK matrix, AI based malware detection, Mail Monitor, Threat Hunting & Intelligence, Automated User Behavior, Dynamic VBA/JS/JAR instrumentation, Execution Graphs, Localized Internet Anonymization and many more*".



We will interact with these services in the upcoming Phishing cases.

hishTool

A tool that will help with automated phishing analysis is [PhishTool](https://www.phishtool.com/" \t "_blank).

Yes, I saved this for last! What is PhishTool?

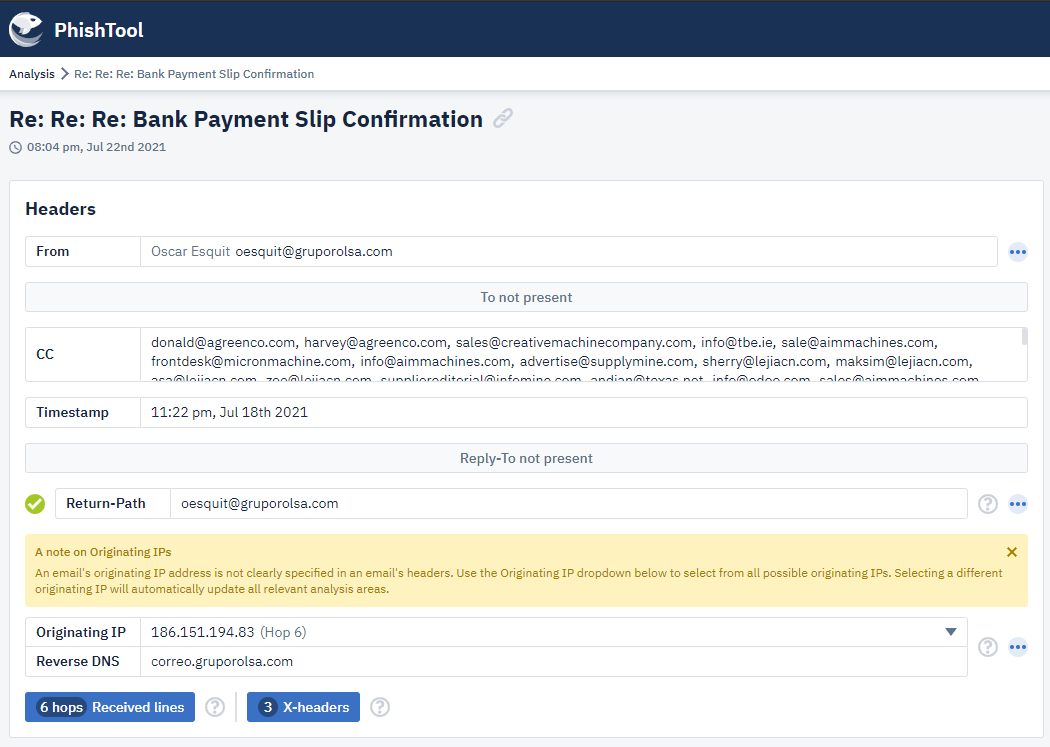
Per the site, "*Be you a security researcher investigating a new phish-kit, a SOC analyst responding to user reported phishing, a threat intelligence analyst collecting phishing IoCs or an investigator dealing with email-born fraud.*

*PhishTool combines threat intelligence, OSINT, email metadata and battle tested auto-analysis pathways into one powerful phishing response platform. Making you and your organisation a formidable adversary - immune to phishing campaigns that those with lesser email security capabilities fall victim to.*"

**Note**: There is a free community edition you can download and use. :)

I uploaded a malicious email to PhishTool and connected VirusTotal to my account using my community edition API key.

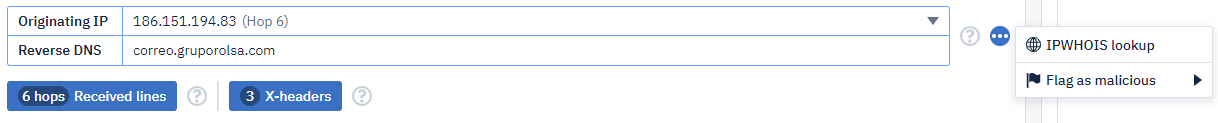
Below are a few screenshots of the malicious email and the PhishTool interface.



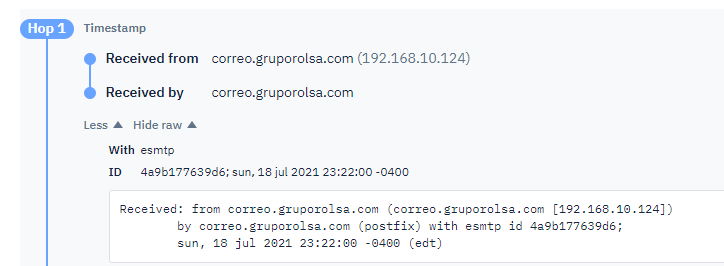
From the image above, you can see the PhishTool conveniently grabs all the pertinent information we'll need regarding the email.

* Email sender
* Email recipient (in this case, a long list of CCed email addresses)
* Timestamp
* Originating IP and Reverse DNS lookup

We can obtain information about the SMTP relays, specific X-header information, and IP info information.



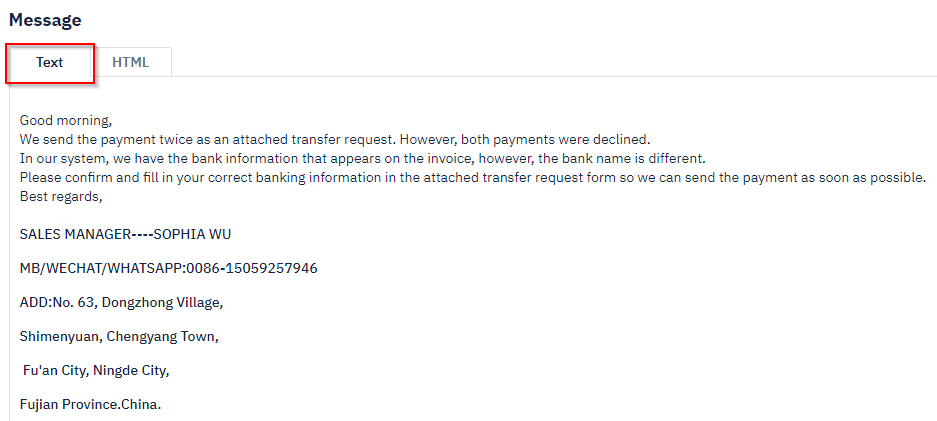
Below is a snippet of Hop 1 of 6 (SMTP relays).



Notice that the tool notifies us that '**Reply-To no present**' although it provides the alternative header information, **Return-Path**.

To the right of the PhishTool dashboard, we can see the email body. There are two tabs across the top that we can toggle to view the email in text format or its HTML source code.

Text view:

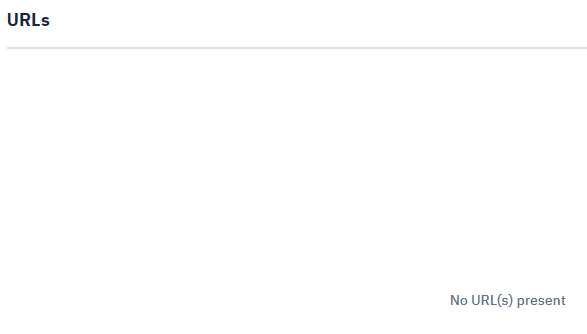


HTML view:

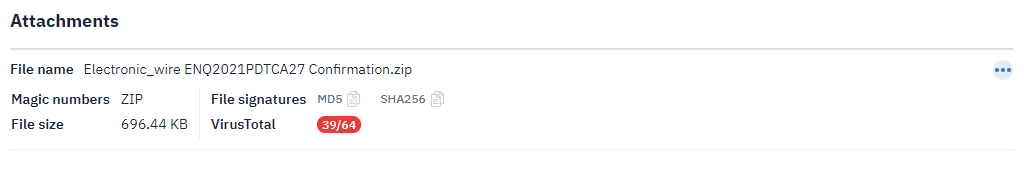


The bottom two panes will display information about attachments and URLs.

The right pane will show if any URLs were found in the email. In this case, no emails were found.



The left pane will show information about the attachment. This particular malicious email has a zip file.

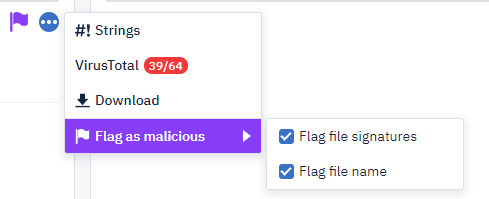


We can automatically get feedback from VirusTotal since our community edition API key is connected.

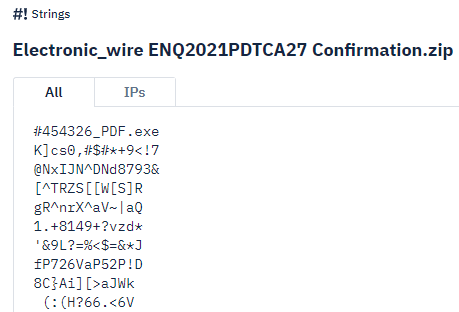
Here we can grab the zip file name and its hashes without manually interacting with the malicious email.

 There is an ellipsis at the far right of the above image. If that is clicked, we are provided additional actions that we can perform with the attachment.

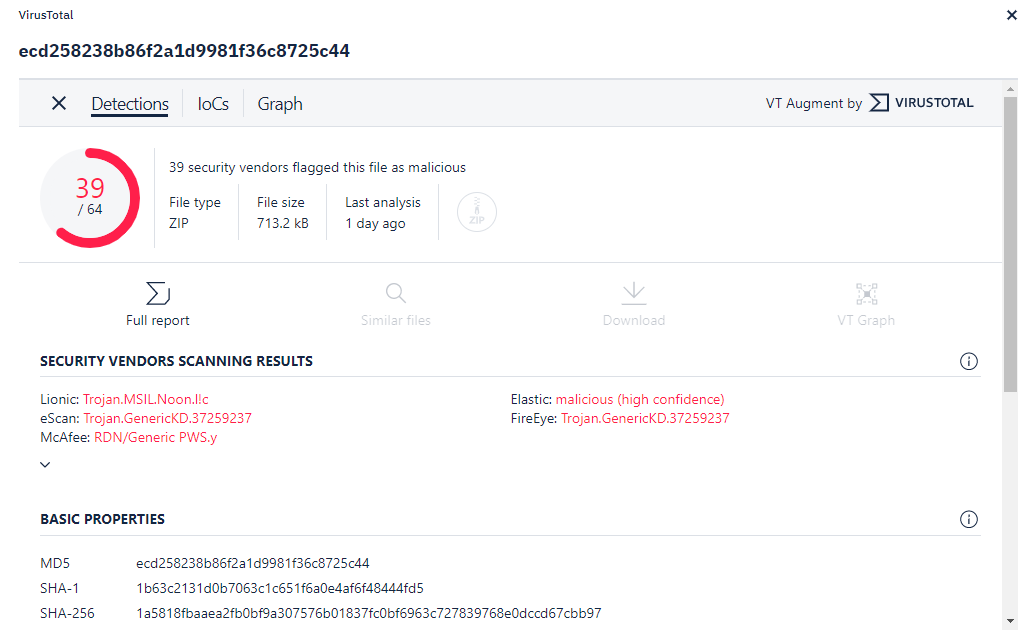
Below is a screenshot of the additional options sub-menu.



Let's look at the Strings output.

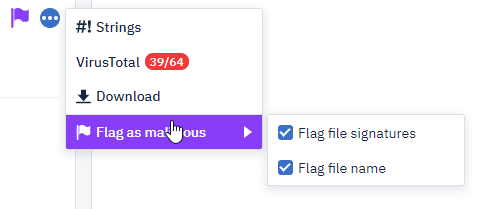


Next, let's look at the information from VirusTotal.

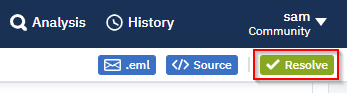


Since the VirusTotal API key is the free community edition, an analyst can manually navigate to VirusTotal and do a file hash search to view more information about this attachment.

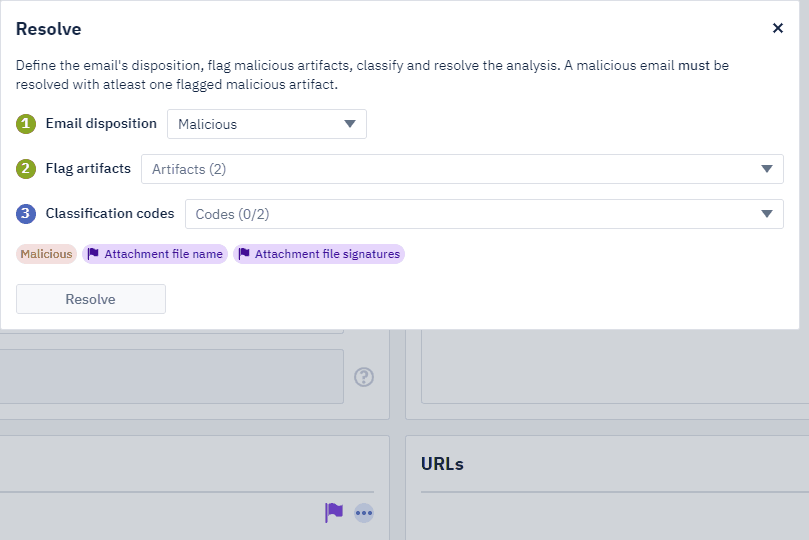
Lastly, any submissions you upload to PhishTool, you can flag as malicious and resolve with notes. Similar to how you would if you were a SOC Analyst.



The attachment file name and file hashes will be marked as malicious. Next, click on **Resolve**.



In the next screen, an analyst can mark the email based on dropdown selections. Refer to the GIF below.



**Note**: I didn't perform further analysis on the domain name or the IP address. Neither did I perform any research regarding the root domain the email originated from. The attachment can further be analyzed by uploading it to a malware sandbox to see what exactly it's doing, which I did not do. Hence the reason why additional Flag artifacts and Classifications codes weren't selected for this malicious email. :)

To expand on classification codes briefly, not all phishing emails can be categorized as the same. A classification code allows us to tag a case with a specific code, such as Whaling (high-value target). Not all phishing emails will target a high-value target, such as a Chief Financial Officer (CFO).

***Answer the questions below***

Look at the Strings output. What is the name of the EXE file?

 Phishing Case 1

 Start Machine

**Scenario**: You are a Level 1 SOC Analyst. Several suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email for your team to implement the appropriate rules to prevent colleagues from receiving additional spam/phishing emails.

**Task**: Use the tools discussed throughout this room (or use your own resources) to help you analyze each email header and email body.

Deploy the machine attached to this task; it will be visible in the **split-screen** view once it is ready.

If you don't see a virtual machine load then click the **Show Split View** button.



***Answer the questions below***

***https://mha.azurewebsites.net/***

What brand was this email tailored to impersonate?



 Submit

What is the From email address?



 Submit

What is the originating IP? Defang the IP address.



 Submit

 Hint

From what you can gather, what do you think will be a domain of interest? Defang the domain.



 Submit

 Hint

What is the shortened URL? Defang the URL.



 Phishing Case 2

**Scenario**: You are a Level 1 SOC Analyst. Several suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email for your team to implement the appropriate rules to prevent colleagues from receiving additional spam/phishing emails.

A malicious attachment from a phishing email inspected in the previous Phishing Room was uploaded to Any Run for analysis.

**Task**: Investigate the analysis and answer the questions below. 

**Link**: <https://app.any.run/tasks/8bfd4c58-ec0d-4371-bfeb-52a334b69f59>

***Answer the questions below***

What does AnyRun classify this email as?



Correct Answer

What is the name of the PDF file?



Correct Answer

What is the SHA 256 hash for the PDF file?



Correct Answer

What two IP addresses are classified as malicious? Defang the IP addresses. (answer: **IP\_ADDR,IP\_ADDR**)



 Submit

 Hint

What Windows process was flagged as **Potentially Bad Traffic**?



 Submit

**Scenario**: You are a Level 1 SOC Analyst. Several suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email for your team to implement the appropriate rules to prevent colleagues from receiving additional spam/phishing emails.

A malicious attachment from a phishing email inspected in the previous Phishing Room was uploaded to Any Run for analysis.

**Task**: Investigate the analysis and answer the questions below. 

**Link**: <https://app.any.run/tasks/82d8adc9-38a0-4f0e-a160-48a5e09a6e83>

***Answer the questions below***

What is this analysis classified as?



 Submit

What is the name of the Excel file?



 Submit

What is the SHA 256 hash for the file?



 Submit

What domains are listed as malicious? Defang the URLs & submit answers in alphabetical order. (answer: **URL1,URL2,URL3**)



 Submit

 Hint

What IP addresses are listed as malicious? Defang the IP addresses & submit answers from lowest to highest. (answer: **IP1,IP2,IP3**)



 Submit

 Hint

What vulnerability does this malicious attachment attempt to exploit?

Phishing 4

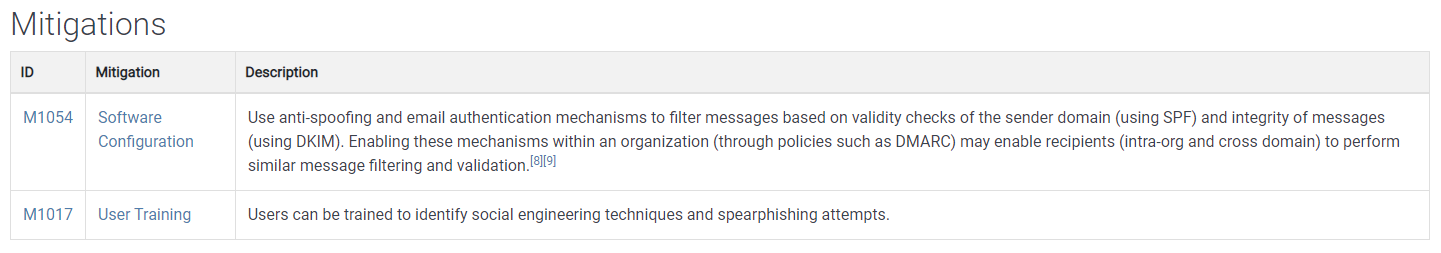
There are various actions a defender can take to help protect the users from falling victim to a malicious email.

Some examples of these actions are listed below:

* Email Security (SPF, DKIM, DMARC)
* SPAM Filters (flags or blocks incoming emails based on reputation)
* Email Labels (alert users that an incoming email is from an outside source)
* Email Address/Domain/URL Blocking (based on reputation or explicit denylist)
* Attachment Blocking (based on the extension of the attachment)
* Attachment Sandboxing (detonating email attachments in a sandbox environment to detect malicious activity)
* Security Awareness Training (internal phishing campaigns)

Per **MITRE ATT&CK** **Framework**, [Phishing](https://attack.mitre.org/techniques/T1598/) is classified as **Technique ID 1598** (**T1598**), and it contains three sub-techniques.

Visit the above link, look at the **Mitigation** section under **Software Configuration**.



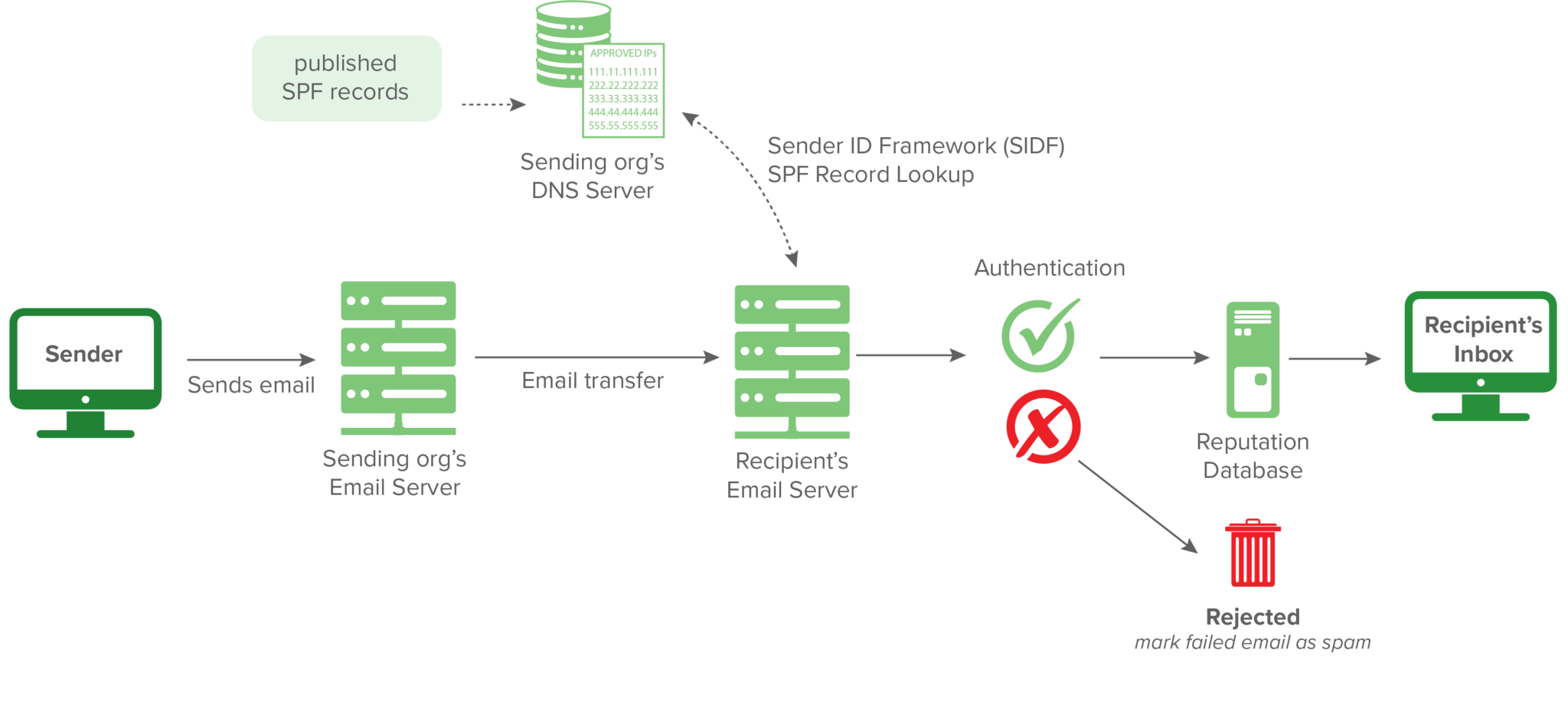
In this room, we will focus specifically on Email Security (SPF, DKIM, DMARC) from the actions noted above.

SPF (Sender Policy Framework)

What is the **Sender Policy Framework** (**SPF**)?

Per [dmarcian](https://dmarcian.com/what-is-spf/" \t "_blank), "*Sender Policy Framework (SPF) is used to authenticate the sender of an email. With an SPF record in place, Internet Service Providers can verify that a mail server is authorized to send email for a specific domain. An SPF record is a DNS TXT record containing a list of the IP addresses that are allowed to send email on behalf of your domain.*"

Below is a visual workflow for SPF.



**Note:** Credit to dmarcian for the above image.

How does a basic SPF record look like?

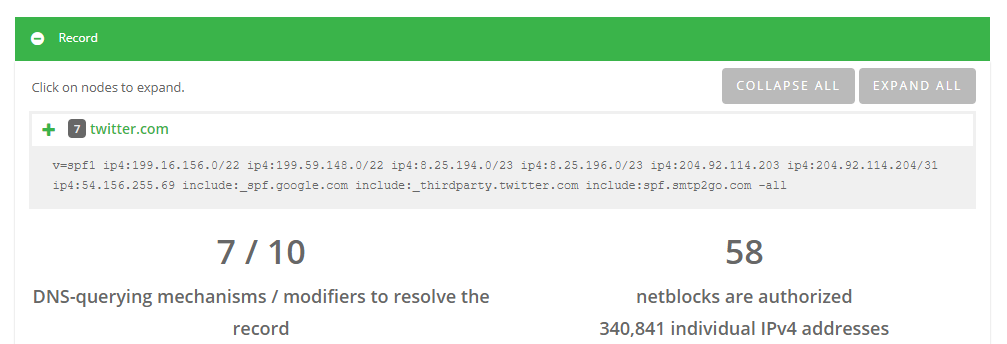
v=spf1 ip4:127.0.0.1 include:\_spf.google.com -all

An explanation for the above record:

* v=spf1 -> This is the start of the SPF record
* ip4:127.0.0.1 -> This specifies which IP (in this case version IP4 & not IP6) can send mail
* include:\_spf.google.com -> This specifies which domain can send mail
* -all -> non-authorized emails will be rejected

Refer to the SPF Record Syntax on dmarcian [here](https://dmarcian.com/spf-syntax-table/) and [here](https://dmarcian.com/what-is-the-difference-between-spf-all-and-all/).

Let's look at Twitter's SPF record using dmarcian's SPF Surveyor [tool](https://dmarcian.com/spf-survey/).



Refer to this resource on [dmarcian](https://dmarcian.com/create-spf-record/" \t "_blank) on how to create your own SPF records.

Let's look at another sample.

The image below is from [Google Admin Toolbox Messageheader](https://toolbox.googleapps.com/apps/messageheader/), which was used to analyze a malicious email.



The above image shows the status of an SPF record check. It reports back as **softfail**.

**Note**: Even though this task uses [dmarcian](https://dmarcian.com/" \t "_blank) for SPF-related information and online checks, many other companies do the same.

***Answer the questions below***

What is the SPF rule to use if you wish to ensure an operator rejects emails without potentially discarding a legitimate email?



 Submit

 Hint

What is the meaning of the **-all** tag?

Fail

DKIM (DomainKeys Identified Mail)

What is **DKIM**?

Per [dmarcian](https://dmarcian.com/what-is-dkim/" \t "_blank), "*DKIM stands for DomainKeys Identified Mail and is used for the authentication of an email that’s being sent. Like SPF, DKIM is an open standard for email authentication that is used for DMARC alignment. A DKIM record exists in the DNS, but it is a bit more complicated than SPF. DKIM’s advantage is that it can survive forwarding, which makes it superior to SPF and a foundation for securing your email.*"

How does a DKIM record look like?

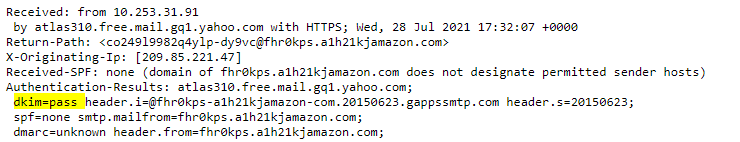
v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxTQIC7vZAHHZ7WVv/5x/qH1RAgMQI+y6Xtsn73rWOgeBQjHKbmIEIlgrebyWWFCXjmzIP0NYJrGehenmPWK5bF/TRDstbM8uVQCUWpoRAHzuhIxPSYW6k/w2+HdCECF2gnGmmw1cT6nHjfCyKGsM0On0HDvxP8I5YQIIlzNigP32n1hVnQP+UuInj0wLIdOBIWkHdnFewzGK2+qjF2wmEjx+vqHDnxdUTay5DfTGaqgA9AKjgXNjLEbKlEWvy0tj7UzQRHd24a5+2x/R4Pc7PF/y6OxAwYBZnEPO0sJwio4uqL9CYZcvaHGCLOIMwQmNTPMKGC9nt3PSjujfHUBX3wIDAQAB

An explanation of the above record:

* v=DKIM1-> This is the version of the DKIM record. This is optional.
* k=rsa -> This is the key type. The default value is RSA. RSA is an encryption algorithm (cryptosystem).
* p= -> This is the public key that will be matched to the private key, which was created during the DKIM setup process.

Refer to the DKIM resource [here](https://dmarcian.com/dkim-selectors/) and [here](https://help.returnpath.com/hc/en-us/articles/222481088-DKIM-DNS-record-overview) for additional information.

The below image is a snippet of an email header for an email flagged as spam that contained a potentially malicious attachment.



***Answer the questions below***

Which email header shows the status of whether DKIM passed or failed?

Authentication-Results

What is **DMARC**?

Per [dmarcian](https://dmarcian.com/start-dmarc/" \t "_blank), "*DMARC, (Domain-based  Message Authentication Reporting, & Conformance) an open source standard, uses a concept called alignment to tie the result of two other open source standards, SPF (a published list of servers that are authorized to send email on behalf of a domain) and DKIM (a tamper-evident domain seal associated with a piece of email), to the content of an email. If not already deployed, putting a DMARC record into place for your domain will give you feedback that will allow you to troubleshoot your SPF and DKIM configurations if needed.*"

How does a basic DMARC record look like?

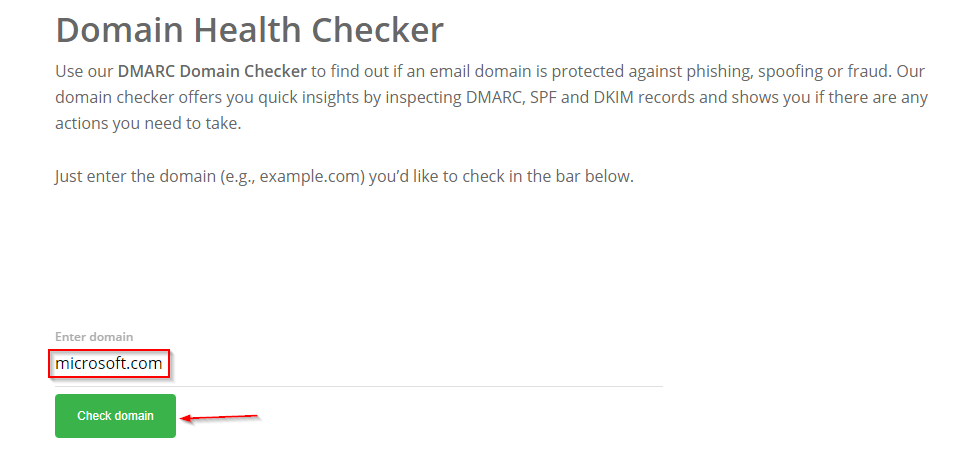
v=DMARC1; p=quarantine; rua=mailto:postmaster@website.com

An explanation of the above record:

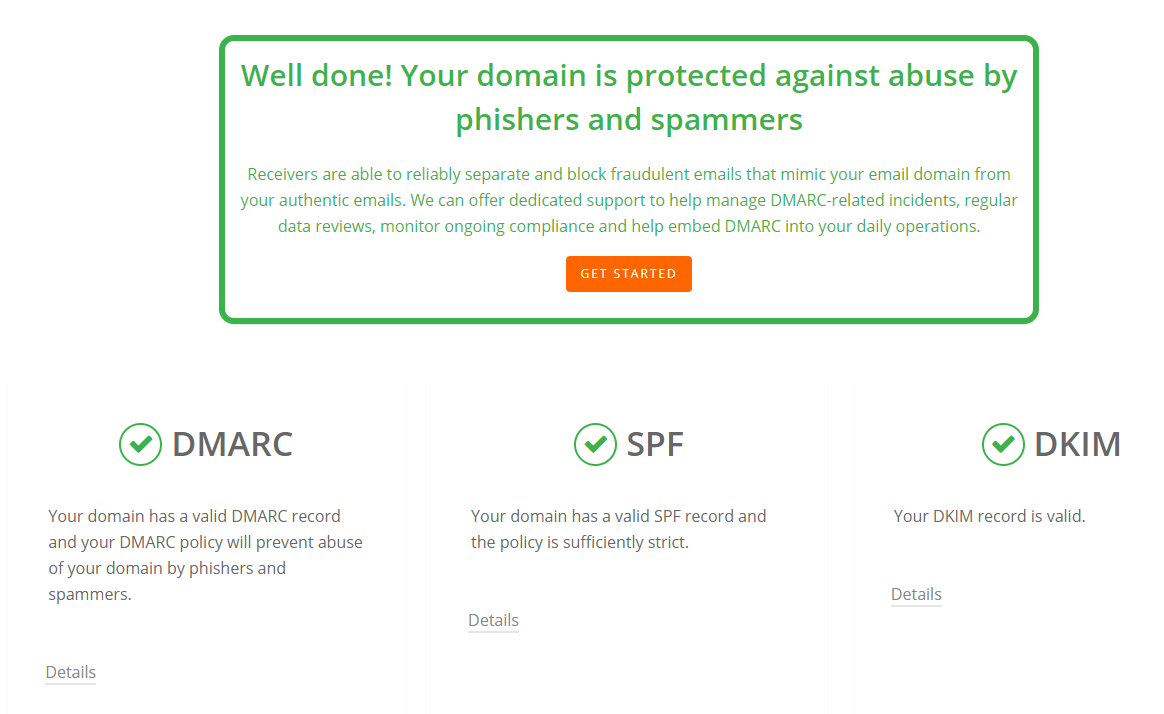
* v=DMARC1 -> Must be in all caps, and it's not optional
* p=quarantine -> If a check fails, then an email will be sent to the spam folder (DMARC Policy)
* rua=mailto:postmaster@website.com -> Aggregate reports will be sent to this email address

Refer to the DMARC resources [here](https://dmarcian.com/dmarc-record/) and [here](https://dmarc.org/overview/) for additional information on DMARC tags. Review the following resource about DMARC [Alignment](https://dmarcian.com/alignment/).

Let's use the **Domain Health Checker** from [dmarcian.com](https://dmarcian.com/domain-checker/) and check the DMARC status of **microsoft.com**.

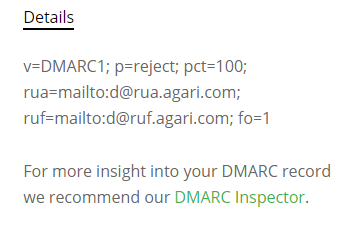


And the results are...



Microsoft passed all checks. We can drill down into **DMARC**, **SPF**, or **DKIM** to get more details.

**DMARC**:



In the details above, we can see that all emails that fail the DMARC check will be rejected.

***Answer the questions below***

Which DMARC policy would you use not to accept an email if the message fails the DMARC check?

p=reject

 S/MIME (Secure/Multipurpose Internet Mail Extensions)

What is [**S/MIME**](https://docs.microsoft.com/en-us/exchange/security-and-compliance/smime-exo/smime-exo)?

Per Microsoft, "*S/MIME (Secure/Multipurpose internet Mail Extensions) is a widely accepted protocol for sending digitally signed and encrypted messages*."

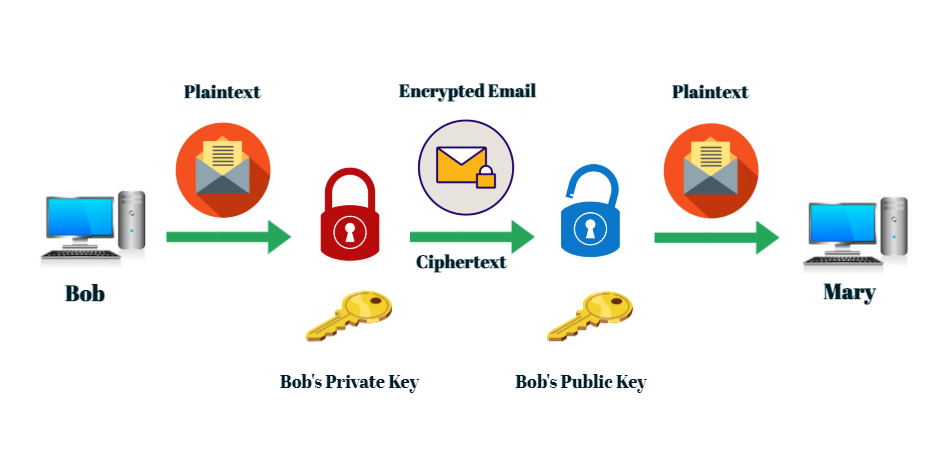
As you can tell from the definition above, the 2 main ingredients for S/MIME are:

1. **Digital Signatures**
2. **Encryption**

Using [Public Key Cryptography](https://www.ibm.com/docs/en/ztpf/1.1.0.14?topic=concepts-public-key-cryptography), S/MIME guarantees data integrity and nonrepudiation.

* If Bob wishes to use S/MIME, then he'll need a digital certificate. This digital certificate will contain his public key.
* With this digital certificate, Bob can "sign" the email message with his private key.
* Mary can then decrypt Bob's message with Bob's public key.
* Mary will do the same (send her certificate to Bob) when she replies to his email, and Bob complete the same process on his end.
* Both will now have each other's certificates for future correspondence.

The illustration below will help you understand how public key cryptography works.



Refer to this Microsoft documentation [here](https://docs.microsoft.com/en-us/exchange/security-and-compliance/smime-exo/smime-exo) for more information on S/MIME and steps on how to configure Office 365 to send/receive S/MIME emails.

***Answer the questions below***

What is nonrepudiation? (The answer is a full sentence, including the ".")

In this task, you'll examine a PCAP file with SMTP traffic. You'll only focus on SMTP codes in this task.

You must be familiar with [Wireshark](https://tryhackme.com/room/wireshark) and packet analysis to answer the questions below.

Here are two resources to assist you with this task:

* <https://www.wireshark.org/docs/dfref/s/smtp.html>
* <https://www.mailersend.com/blog/smtp-codes>

***Answer the questions below***

What Wireshark filter can you use to narrow down the packet output using SMTP status codes?



 Submit

Per the network traffic, what was the message for status code 220? (Do not include the status code (220) in the answer)



 Submit

One packet shows a response that an email was blocked using spamhaus.org. What were the packet number and status code? (no spaces in your answer)



 Submit

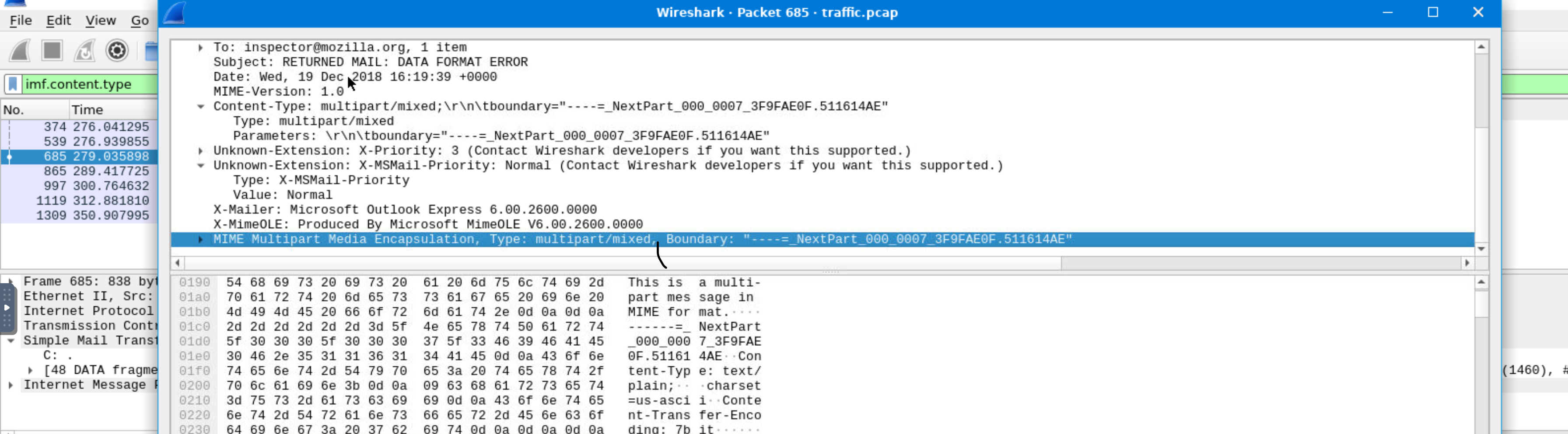
Based on the packet from the previous question, what was the message regarding the mailbox?



 Submit

 Hint

What is the status code that will typically precede a SMTP DATA command?



 SMTP and C&C Communication

Now we'll take a look at how SMTP has been abused by adversaries for C2 (Command and Control) communications.

**MITRE ATT&CK**:

* **Techinique 1071 > Sub-Technique 3**: <https://attack.mitre.org/techniques/T1071/003/>

Per MITRE, "*Adversaries may communicate using application layer protocols associated with electronic mail delivery to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.*"

Several notable groups, such as **APT 28**, **APT 32**, and **Turla**, to name a few, have used this technique.

**Recommended mitigation (per MITRE)**:

"*Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level.*"

**Detection opportunity (per MITRE)**:

"*Analyze packet contents to detect application layer protocols that do not follow the expected protocol standards regarding syntax, structure, or any other variable adversaries could leverage to conceal data.*"

**Note**: We will cover Network Intrusion Prevention and Detection in future rooms.

***Answer the questions below***

Per MITRE ATT&CK, which software is associated with using SMTP and POP3 for C2 communications?



 Submit

We'll wrap up this room by sharing a phishing incident response playbook. This playbook will give you an idea of what steps should be considered and executed given this scenario.

A **playbook** is a defined process that should be followed in a specific situation, in this case, a phishing incident.

Phishing IR Playbook:

* <https://www.incidentresponse.com/playbooks/phishing>

Lastly, the PCAP file used in this room was from **Malware Traffic Analysis**. You can explore more details about this PCAP or other samples.

SMTP PCAP Credit:

* <https://www.malware-traffic-analysis.net/2018/12/19/index.html>

***Answer the questions below***

Per the playbook, what framework was used for the IR process?

NIST