Manual Collection Techniques – Email Artifacts

In this lesson, we are going to teach you how to retrieve email, web, and file-based artifacts from a malicious email. These are important to gather more information about the attack and to take appropriate defensive measures to protect the business. To collect the email and web artifacts, we will be using an email client and a text editor. To collect file-based artifacts, we will use PowerShell (or a Linux terminal if you're not on Windows OS).

Analysts should never analyze phishing emails on a corporate or personal system. It is good practice to always use a virtual machine or a "dirty" system, such as an old laptop or computer designed specifically for risky security tasks, such as malware analysis or investigating suspicious websites. Organizations will take different approaches to what their security team can and can't do. For these activities, we have ensured everything is safe so you can complete analysis on your host system, but getting into the habit of using a virtual machine isn't a bad idea!

EMAIL ARTIFACTS

The easiest email artifacts to retrieve are:

- **Sending Address**
- **Subject Line**
- **Recipients** (Unless they're in BCC)
- **Date + Time**

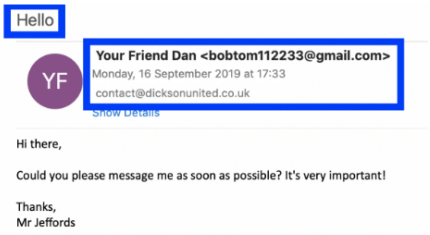
This is because they are immediately available in the email client. Below we will cover how to get these using an email client such as Outlook (or you can use Thunderbird), and also how to retrieve them using a text editor (we'll be using Sublime Text 2).

EMAIL CLIENT EXTRACTION

Want to follow along with this walkthrough? Download the email by clicking on the button to ensure you can find all of the information you need to investigate suspicious emails.

Download "Hello.zip"

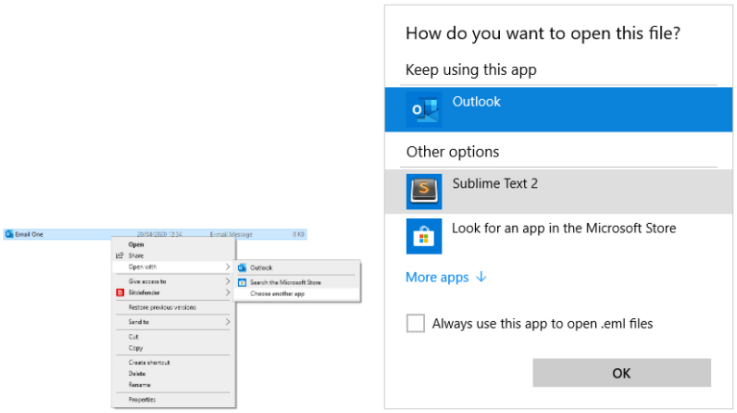
Viewing our example email in Microsoft's Outlook client we can immediately retrieve four artifacts:



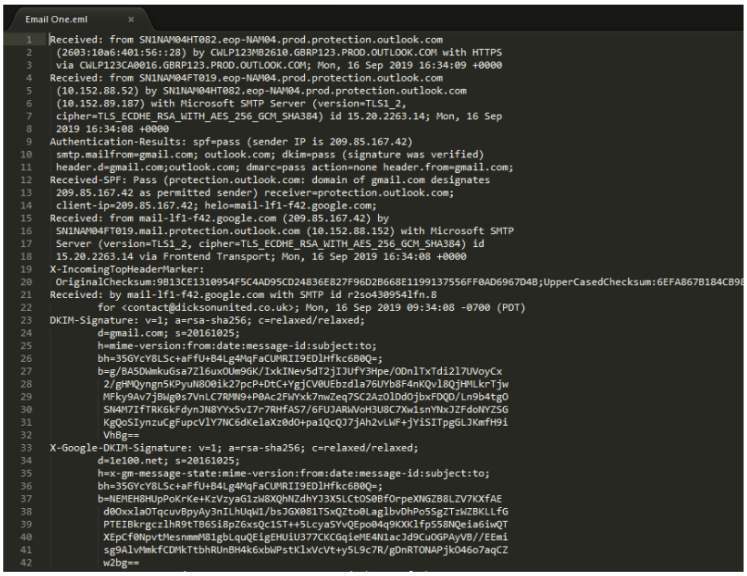
1. **Subject Line** = Hello
2. **Sending Address** = bobtom112233@gmail.com
3. **Date + Time** = Monday 16th September 2019 at 17:33
4. **Recipient(s)** = contact@dicksonunited.co.uk

TEXT EDITOR EXTRACTION

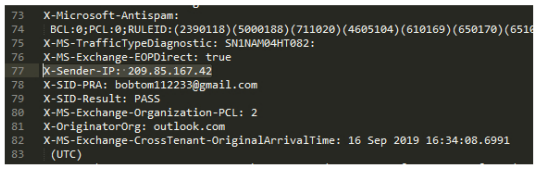
Whilst we can get the majority of the email artifacts we need from a client, there is additional information that we need to collect such as the **Sending Server IP** (which server has sent the email), and the **Reply-To address** (where any replies to the email will be sent – this may not always be the initial sender). These can easily be obtained by downloading the email in either .eml or .msg file format and opening the file with a text editor.



When the email opens in the text editor it'll produce a long document that looks extremely long and complicated – but don't worry, we're only looking for some specific parts, and we can easily get to them using the Find feature (CTRL+F).



The first thing we want to collect is the sending server IP, also referred to as the X-Sender-IP. Press CTRL + F (or your OS equivalent) and search for "IP". The first string that you find should be the X-Sender-IP (if not, keep clicking "Find" or "Find Prev" until you find it).



Now that we have the IP, we need to convert the address into a hostname. We can do this by performing a reverse DNS lookup. We recommend you use the free online service by Domain Tools – http://whois.domaintools.com/. If we input the sending server IP we just received (http://whois.domaintools.com/209.85.167.42) we can retrieve information about the server.

Home > Whois Lookup > 209.85.167.42

IP Information for 209.85.167.42

Quick Stats

IP Location	United States Of America Mountain View Google Llc
ASN	AS15169 (registered Mar 30, 2000)
Resolve Host	mail-lf1-f42.google.com
Whois Server	whois.arin.net
IP Address	209.85.167.42

In the above screenshot, we can see that the host is **mail-lf1-f42.google.com** – a Gmail sending server. Sometimes the sending address domain and sending IP might not match up. If the sender is **bob@gmail.com** but the IP address belongs to **Outlook**, we know that the sending address has been spoofed. We'll cover this in a future lesson.

Next, we need to retrieve the **Reply-To** address. In the below screenshot, using a different example email, we have used the search function within Sublime Text 2 looking for the string "reply". We have now identified the address that would receive any replies to this email.

```
24
25  From: "Amazon.co.uk" <amazonsupp0rt@outlook.com>
26  Reply-to: "no-reply@amazon.co.uk" <no-reply@amazon.co.uk>
27  Date: Monday, 27 May 2019 at 23:15
28  To: "Claire.Shelley@DicksonUnited.co.uk" <Claire.Shelley@DicksonUnited.co.u=
29  k>
30  Subject: Suspicious Amazon Order Alert
31
32  =20
```

CONCLUSION

You should now be able to extract the following artifacts from a suspicious email:

- **Sending Address**
- **Subject Line**
- **Recipient(s)**
- **Date and Time**
- **Sending Server IP**
- **Reverse DNS of Sending Server IP**
- **Reply-To** (if present)

At the end of this section, you'll have a chance to put your artifact retrieval to the test with some example phishing emails! Let's move on to web-based artifacts.