# Manual Collection Techniques – Web Artifacts

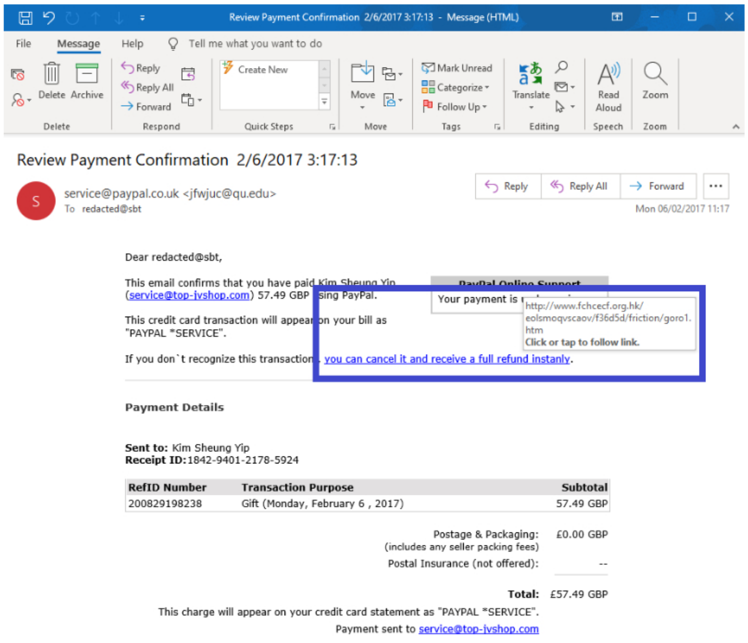
The term "web artifact" is used to describe a hyperlink in an email which will redirect the recipient to a domain, an IP address, or a specific URL. These can be used to host fake login portals that steal any entered credentials or pages that host malware which is downloaded when the site is visited. Collecting these artifacts is extremely straight forward and can be done in just a few clicks. We are looking to retrieve:

- **The full URL** (the complete web address as it is sent in the email)
- **The root domain** (only the domain name, not including specific pages)

Below we'll show you how to do it within an email client such as Outlook or Thunderbird, and how to do it from a text editor.

## EMAIL CLIENT EXTRACTION

In this phishing email, we can see that this section of text is hyperlink, and the user is told to click on it. By hovering the mouse over this text we can see the URL, which definitely doesn't belong to PayPal.



Review Payment Confirmation 2/6/2017 3:17:13

service@paypal.co.uk <jfwjuc@qu.edu>
To redacted@sbt
Mon 06/02/2017 11:17

Dear redacted@sbt,

This email confirms that you have paid Kim Sheung Yip (service@top-jvshop.com) 57.49 GBP using PayPal.

This credit card transaction will appear on your bill as "PAYPAL *SERVICE".

If you don`t recognize this transaction, you can cancel it and receive a full refund instanly.

PayPal Online Support
Your payment is

http://www.fchcecf.org.hk/eolsmoqvscaov/f36d5d/friction/goro1.htm
Click or tap to follow link.

Payment Details

**Sent to:** Kim Sheung Yip
**Receipt ID:**1842-9401-2178-5924

| RefID Number | Transaction Purpose | Subtotal |
|---|---|---|
| 200829198238 | Gift (Monday, February 6 , 2017) | 57.49 GBP |

| | |
|---|---|
| Postage & Packaging:<br>(includes any seller packing fees) | £0.00 GBP |
| Postal Insurance (not offered): | -- |
| **Total:** | £57.49 GBP |

This charge will appear on your credit card statement as "PAYPAL *SERVICE".
Payment sent to service@top-jvshop.com

We can right-click the URL and select "Copy Hyperlink" to send the URL to our clipboard, which we can post elsewhere.

Review Payment Confirmation 2/6/2017 3:17:13

service@paypal.co.uk <jfwjuc@qu.edu>

5 Topics

○ DF2) Forensics Fundamentals

10 Topics | 5 Quizzes

○ DF3) Digital Evidence Collection

8 Topics | 1 Quiz

○ DF4) Windows Investigations

3 Topics | 3 Quizzes

○ DF5) Linux Investigations

4 Topics | 2 Quizzes

○ DF6) Volatility

3 Topics | 1 Quiz

○ DF7) Autopsy

4 Topics | 1 Quiz

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

○ SI1) Introduction to SIEM

7 Topics | 1 Quiz

○ SI2) Logging

6 Topics | 2 Quizzes

○ SI3) Aggregation

2 Topics | 1 Quiz

○ SI4) Correlation

6 Topics | 1 Quiz

○ SI5) Using Splunk

5 Topics | 2 Quizzes

INCIDENT RESPONSE DOMAIN

○ IR1) Introduction to Incident Response

8 Topics | 1 Quiz

○ IR2) Preparation Phase

10 Topics | 2 Quizzes

○ IR3) Detection and Analysis Phase

7 Topics | 4 Quizzes

○ IR4) Containment, Eradication, and Recovery Phase

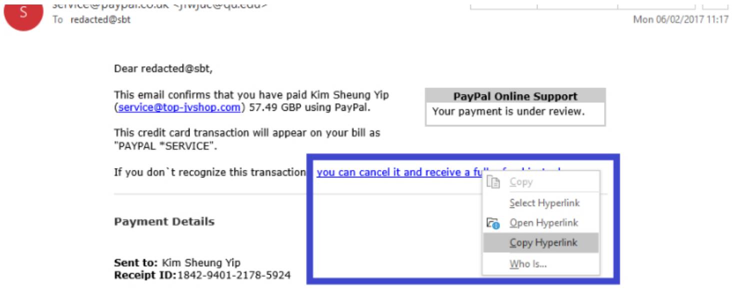
5 Topics | 1 Quiz

○ IR5) Lessons Learned and Reporting

7 Topics

○ IR6) MITRE ATT&CK

13 Topics | 2 Quizzes



service@paypal.co.uk <jrwjdc@qu.edu>
To redacted@sbt
Mon 06/02/2017 11:17

Dear redacted@sbt,

This email confirms that you have paid Kim Sheung Yip (service@top-jvshop.com) 57.49 GBP using PayPal.

This credit card transaction will appear on your bill as "PAYPAL *SERVICE".

If you don`t recognize this transaction you can cancel it and receive a fu...

**PayPal Online Support**
Your payment is under review.

**Payment Details**

**Sent to:** Kim Sheung Yip
**Receipt ID:**1842-9401-2178-5924

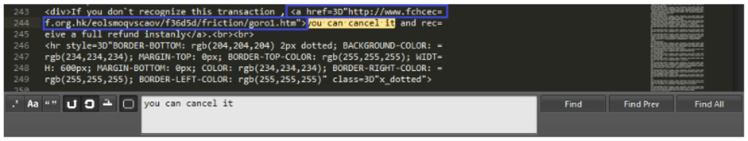
Although this method is much faster than using a text editor, there is always the risk that you could accidentally click on the malicious URL and end up visiting the page. Be careful when right-clicking and selecting Copy Hyperlink to avoid this mistake, and remember to always analyze phishing emails inside a virtual machine or on a dirty system!

# TEXT EDITOR EXTRACTION

In a text editor, we can use the CTRL+F keyboard shortcut to enable the "Find" feature. There are three quick ways to find the URL(s) we want:

- **Search for "http" as this will identify any http or https addresses being mentioned within the email.**
- **Search for anchor HTML tags <a> which are used to perform hyperlinking.**
- **Search for the text from the email body that is a hyperlink, in this example, we could search for "you can cancel it".**

We're going to use the last method.



```
<div>If you don`t recognize this transaction , <a href=3D"http://www.fchcec=
f.org.hk/eolsmoqvscaov/f36d5d/friction/goro1.htm">you can cancel it and rec=
eive a full refund instanly</a>.<br><br>
<hr style=3D"BORDER-BOTTOM: rgb(204,204,204) 2px dotted; BACKGROUND-COLOR: =
rgb(234,234,234); MARGIN-TOP: 0px; BORDER-TOP-COLOR: rgb(255,255,255); WIDT=
H: 600px; MARGIN-BOTTOM: 0px; COLOR: rgb(234,234,234); BORDER-RIGHT-COLOR: =
rgb(255,255,255); BORDER-LEFT-COLOR: rgb(255,255,255)" class=3D"x_dotted">
```

you can cancel it

And there we have it, we can see the URL within the **<a>** HTML tags, and can copy it without fear of accidentally clicking on the link and being taken to a potentially malicious site.

‹ Previous Topic

Back to Lesson

Next Topic ›