Section Introduction, Investigating Emails

This section of the Phishing Analysis domain will cover how phishing investigations take place once an email has been reported as suspicious by the security team or the recipient. This includes retrieving email, web, and file-based artifacts using manual and automated methods so that they can be analyzed at the next stage of the investigation.

LEARNING OBJECTIVES

By the end of this section you will have achieved the following objectives:

- Explain the key email artifacts we need to retrieve from suspect emails, and why we need to record them.
- Retrieve key email artifacts from a reported phishing email using manual techniques via an email client and a text editor.
- Retrieve key artifacts from a reported phishing email using automated techniques using the PhishTool analysis workbench.
- Retrieve and understand why web-based and file-based artifacts are important during investigations where they are present in a phishing email.