

- O TI2) Threat Actors & APTs
  - 6 Topics | 2 Quizzes
- TI3) Operational Threat Intelligence
  - 7 Topics | 1 Quiz

## **Artifact Analysis With PhishTool**

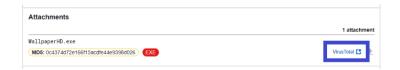
**Phishing Analysis ARTIFACT ANALYSIS, PHISHTOOL** 

Blue Team Level 1 Certification (Standard) > PA5) Analysing URLs, Attachments, and Artifacts > Ar... COMPLETE

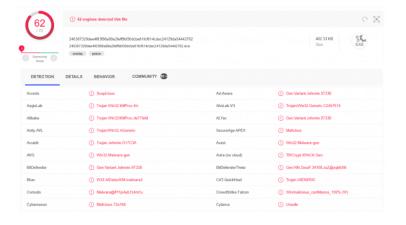
This lesson is going to show how you can analyze artifacts from the PhishTool analysis console, including; WHOIS checks, VirusTotal reputation checks for MD5 hashes and URLs, URL visualization, Doing all of this within PhishTool keeps investigations streamlined and allows you to get the information you need in one place.

## **FILE ARTIFACT ANALYSIS**

PhishTool will automatically retrieve the file name and MD5 hash from any email attachments, and the console has a button that allows us to search for the hash value in VirusTotal straight from the console. If the submitted email contains an attachment, click the following button on the right-hand side to submit it for a reputation check.



This will automatically generate a VirusTotal search query for the MD5 file hash, and open it in a new browser window.



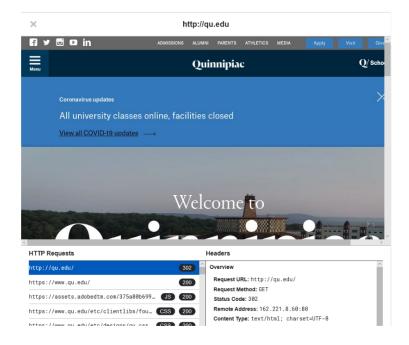
## **WEB ARTIFACT ANALYSIS**

Similarly to how we use URL2PNG to visualize what is at the end of a URL, PhishTool has the ability to generate a live screenshot of a URL. If an email is submitted to PhishTool that includes any URLs, whether malicious or not, a web capture can be viewed by clicking on the URL, and selecting Web Capture.

114) lactical Threat Intelligence
7 Topics   1 Quiz
TI5) Strategic Threat Intelligence
5 Topics   1 Quiz
Tl6) Malware and Global Campaigns
6 Topics   1 Quiz
DIGITAL FORENSICS DOMAIN
DF1) Introduction to Digital Forensics
• 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
O DF6) Volatility
3 Topics   1 Quiz
O 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
BTL1 EXAM
Exam Preparation
Using RDP and SSH
How to Start Your Exam



This feature also kindly provides us with the HTTP requests made, and headers from the site.



Another analysis activity we can perform from within the PhishTool console is a WHOIS lookup, providing us with information about the domain such as where it's hosted, who owns the domain, how long it has been alive for, and contact information. Let's try a WHOIS search on a different URL from another phishing email.



Below is the sidebar that will come from the right-hand side of the analysis console, and provides us with valuable WHOIS data. From this we can see that the domain has been alive for 2643 days, the domain name was registered with Domain.com LLC, and we have some contact email addresses.



Name servers

ns3.a2hosting.com

ns4.a2hosting.com

Emails

compliance@domain-inc.net
support@ipage-inc.com

< Previous Topic

-----, ---

Back to Lesson

Next Topic >



Privacy & Cookies Policy