

Blue Team Level 1 Certification  
(Standard)

## Introduction to BTL1

Welcome to Blue Team Level 1

4 Topics

Lab and Forum Access

## SECURITY FUNDAMENTALS DOMAIN

Introduction to Security Fundamentals

1 Topic

Soft Skills

7 Topics

Security Controls

5 Topics 1 Quiz

Networking

6 Topics 1 Quiz

Management Principles

4 Topics 1 Quiz

## PHISHING ANALYSIS DOMAIN

PA1) Introduction to Emails and Phishing

7 Topics 1 Quiz

PA2) Types of Phishing Emails

10 Topics 2 Quizzes

PA3) Tactics and Techniques Used

12 Topics 2 Quizzes

PA4) Investigating a Phishing Email

8 Topics 2 Quizzes

PA5) Analysing URLs, Attachments, and Artifacts

8 Topics 1 Quiz

Section Introduction: Analysing Artifacts

Visualization Tools

URL Reputation Tools

File Reputation Tools

Malware Sandboxing

[Video] Manual Artifact Analysis

Artifact Analysis With PhishTool

[Video] Artifact Analysis with PhishTool

Activity: End-of-Section Review: Analysing Artifacts

PA6) Taking Defensive Actions

12 Topics 1 Quiz

PA7) Report Writing

7 Topics 1 Quiz

PA8) Phishing Response Challenge

3 Topics 1 Quiz

## THREAT INTELLIGENCE DOMAIN

T11) Introduction to Threat Intelligence

7 Topics

T12) Threat Actors &amp; APTs

6 Topics 2 Quizzes

T13) Operational Threat Intelligence

7 Topics 1 Quiz

## Artifact Analysis With PhishTool

Blue Team Level 1 Certification (Standard) &gt; PA5) Analysing URLs, Attachments, and Artifacts &gt; Ar...

COMPLETE

Phishing Analysis  
ARTIFACT ANALYSIS, PHISHTOOL

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.

**Attachments**

1 attachment

WallpaperHD.exe

MD5: 0c4374d72e166f15acdfc44e9398d026 EXE

VirusTotal

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

62 / 73

62 engines detected this file

240387329dee4033f8ba95a2ef89430dcbaf161614cdac241296d54442762

402.33 KB

Size

EXE

File Type

File Name

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
Acronis	Suspicious	Ad-Aware	Gen Variant:Johanna.97338
AvastLab	Trojan.Win32.KillProc.41c	AlertLab-V3	Trojan.Win32.Generic.C2.657519
Alibaba	Trojan.Win32.KillProc.d077a6d	ALYac	Gen Variant:Johanna.97338
Antiy-AVL	Trojan.Win32.AG.Generic	SecureAge APEX	Malicious
Arcabit	Trojan.Johanna.D17C3A	Avast	Win32.Malware.gen
AVG	Win32.Malware.gen	Akra (no cloud)	TR/Crypt.XPACK.Gen
BitDefender	Gen Variant:Johanna.97338	BitDefender Theta	Gen:NN.Zenaf.34188.zu2@sig698
Bitav	W32.AIDetectVM.malware.2	CAT-QuickHeal	Trojan.IGENERIC
Comodo	Malware@8119a4b724m1u	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.72a166	Cylance	Unsafe

## 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.

☐ I14) Tactical Threat Intelligence

7 Topics 1 Quiz

☐ TI5) Strategic Threat Intelligence

5 Topics 1 Quiz

☐ TI6) 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

☐ 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

**BTL1 EXAM**

☐ Exam Preparation

☐ Using RDP and SSH

☐ How to Start Your Exam

URLs

5 URLs

From domain: http://qu.edu

 Web capture

 WHOIS

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

The screenshot shows the Quinnipiac University homepage. The URL bar indicates a 302 redirect from the original URL to a new one. The page content includes a navigation bar with links like 'Admissions', 'Alumni', 'Parents', 'Athletics', 'Media', and buttons for 'Apply' and 'Visit'. The main header features the university's name and a 'Q/ School' link. Below this, a blue banner contains the text 'Coronavirus updates' and 'All university classes online, facilities closed', with a link to 'View all COVID-19 updates'. The background of the page shows a large image of the university's campus with the text 'Welcome to' overlaid.

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.

A screenshot of a web browser's developer console, specifically the 'URLs' tab. The console shows a list of network requests. The first request is from 'http://hotmail.com'. The second request is 'https://i.abb.com/qjNPt1v/logo.png'. The third request is 'https://www.alphabioticsboston.org/rfvb/dcvf77.html'. Below the list are two buttons: 'Web capture' and 'WHOIS'.

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.

WHOIS	Source WHOIS record
<h2>WHOIS</h2> <h3>alphabioticsboston.org</h3> <hr/> <h4>Registrant</h4> <p><b>Organisation:</b> REDACTED FOR PRIVACY</p> <p><b>Name:</b> REDACTED FOR PRIVACY</p> <p><b>Country:</b> US</p> <hr/> <h4>Dates</h4> <p><b>Created:</b> 15/02/13</p> <p><b>Expires:</b> 15/02/21</p> <p><b>Age:</b> 2643 days old</p> <hr/> <h4>Registrar</h4> <p>Domain.com, LLC</p>	

---

**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](#)