

Blue Team Level 1 Certification  
(Standard)

✓ Networking-101

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

TI1) Introduction to Threat Intelligence

7 Topics

TI2) Threat Actors &amp; APTs

6 Topics 2 Quizzes

TI3) Operational Threat Intelligence

7 Topics 1 Quiz

TI4) 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

## Visualization Tools

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

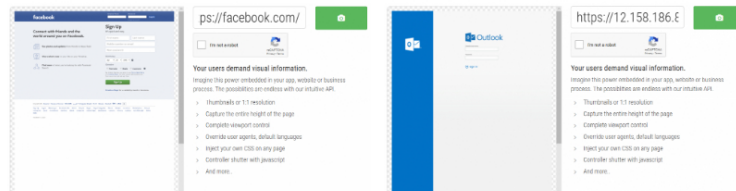
COMPLETE

Phishing Analysis  
VISUALIZATION TOOLS

This lesson will cover tools we can use to visualize a malicious URL without actually having to visit the site, as it could be highly malicious. The tools we're going to cover are URL2PNG, and URLScan. By the end of this lesson, you will feel comfortable with visualizing hyperlinks to assess what is on the other side.

## URL2PNG

URL2PNG is my go-to tool for visualization. You simply enter in a URL, hit go, and it'll provide you with a screenshot of what the webpage looks like. Let's go through a couple of examples. The screenshot on the left shows me entering the following URL into URL2PNG: <https://facebook.com/>. The screenshot on the right shows me entering a malicious URL for a real-world Outlook Web Access credential harvester into the tool:



## URLSCAN

URLScan, amongst other information this tool gathers on a searched URL, has the ability to provide a screenshot. In this example, you can see a screenshot has been taken on the right-hand side, allowing us to see what the destination web page looks like. In this case, it is an Outlook Web App credential harvester.

## firebasestorage.googleapis.com

2a00:1450:4001:81d::200a Malicious Activity!

URL: <https://firebasestorage.googleapis.com/v0/t/ouy0334242.appspot.com/b/AZWEE.htm?alt=media&token=d989cb4d-067c-4468-918e-b88c4542c2ff>

Submission: On April 21 via manual (April 21st 2020, 9:57:31 am) from GB

Summary HTTP Behaviour IDS Similar DNS DCM Content API

## Summary

This website contacted 7 IPs in 4 countries across 5 domains to perform 10 HTTP transactions. The main IP is 2a00:1450:4001:81d::200a, located in Frankfurt am Main, Germany and belongs to GOOGLE, US. The main domain is [firebasestorage.googleapis.com](https://firebasestorage.googleapis.com). TLS certificate: Issued by GTS CA 101 on April 1st 2020. Valid for: 3 months.

The main domain was scanned 10288 times on urlscan.io

Show Scans 10288

17951 structurally similar pages on different IPs, domains and ASNs found

Show Scans 17951

Verdict: Malicious (Score: 100/100)

Show Details

urlscan - Score: 100 phishing

Phishing against Outlook Web Access (Online)

Google Safe Browsing: Clean (Current Classification)

## Additional live information

Current DNS A record: 172.217.22.74 (AS15169 - GOOGLE, US)  
Domain created: January 25th 2005, 17:52:26 (UTC)  
Domain registrar: MarkMonitor Inc.

## Domain &amp; IP information

Q Lookup Go To Report Rescan

## Screenshot

Use screenshot Full Image



## Detected technologies

Bootstrap (Web Frameworks) Website  
Font Awesome (Font Scripts) Website

## Stats

10 Requests 0 Ad-blocked 0 Malicious 100% HTTPS 100% IPv6

DF3) Digital Evidence Collection

8 Topics1 Quiz

DF4) Windows Investigations

3 Topics3 Quizzes

DF5) Linux Investigations

4 Topics2 Quizzes

DF6) Volatility

3 Topics1 Quiz

DF7) Autopsy

4 Topics1 Quiz

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

SI1) Introduction to SIEM

7 Topics1 Quiz

SI2) Logging

6 Topics2 Quizzes

SI3) Aggregation

2 Topics1 Quiz

IP/ASNs	IP Detail	Sub(Domains)	Domain Tree	Links	Certificates	5 Domains	6 Subdomains	7 IPs	4 Countries	203kB Transfer
	IP Address		AS Autonomous System			506kB Size	0 Cookies			
1	2a00:1450:4001:81d::200a		15169 (GOOGLE)							
2	2001:44c0:ac19::1:177a		214244 (BULGARIANPOST)							

# CONCLUSION

Visualization tools are key to allowing analysts to identify what is on the other end of a hyperlink without having to visit the page directly. Whilst it is not necessary to include a screenshot of the destination in your investigation report, it's something I like to do!

< Previous Topic

Back to Lesson

Next Topic >