

Blue Team Level 1 Certification  
(Standard)

✓ 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

✓ Section Introduction: Investigating Emails

✓ Artifacts We Need to Collect

✓ Manual Collection Techniques – Email Artifacts

✓ Manual Collection Techniques – Web Artifacts

✓ Manual Collection Techniques – File Artifacts

✓ [Video] Collecting Artifacts – Manual Methods

✓ Automated Collection With PhishTool

✓ [Video] Collecting Artifacts – Automated Methods

Lab) Manual Artifact Extraction

Activity) End of Section Review: Investigating Emails

✓ PA5) Analysing URLs, Attachments, and Artifacts

8 Topics 1 Quiz

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

# Manual Collection Techniques – File Artifacts

Blue Team Level 1 Certification (Standard) &gt; PA4) Investigating a Phishing Email &gt; Manual Collecti...

COMPLETE



We need to collect file hashes of malicious attachments to perform reputation checks and implement defensive measures. Hashes are the output of a hashing algorithm, such as MD5 (Message Digest 5) or SHA (Secure Hash Algorithm). These algorithms will produce a unique string that is used to represent the file. If there is a single change to the file, such as editing a text file and changing one character, the hash will be completely different. You can read more about hashes [here](#).

## HASHES VIA POWERSHELL

It's most likely that security analysts will be using the Windows OS for day-to-day work. File hashes can be retrieved using PowerShell with the `get-filehash` command. By default, this will generate a SHA256 hash.

```
Windows PowerShell
PS C:\Users\JBeam\Desktop\Malware> get-filehash .\wallpaperHD.exe

Directory: C:\Users\JBeam\Desktop\Malware

Mode                LastWriteTime         Length Name
----                -
-a-----         05/02/2020    07:20      411982 wallpaperHD.exe

PS C:\Users\JBeam\Desktop\Malware> get-filehash .\wallpaperHD.exe

Algorithm Hash Path
-----
SHA256 240387329DEE4F03F98A89A2FEFF9BF30DCBA61FCF614CDAC24129DA54442762 C:\Users\JBeam\Desktop\Malware...
```

We can also retrieve MD5 and SHA1 hashes using the `get-filehash` command with the `-Algorithm` switch.

```
Windows PowerShell
PS C:\Users\JBeam\Desktop\Malware> get-filehash .\wallpaperHD.exe

Algorithm Hash Path
-----
SHA256 240387329DEE4F03F98A89A2FEFF9BF30DCBA61FCF614CDAC24129DA54442762 C:\Users\JBeam\Desktop\Malware...

PS C:\Users\JBeam\Desktop\Malware> get-filehash -algorithm md5 .\wallpaperHD.exe

Algorithm Hash Path
-----
MD5 0C4374D72E166F15ACDFE44E9398D026 C:\Users\JBeam\Desktop\Malware...

PS C:\Users\JBeam\Desktop\Malware> get-filehash -algorithm sha1 .\wallpaperHD.exe

Algorithm Hash Path
-----
SHA1 FBAC123C604137654759F2FBC4C5957D5881D3D1 C:\Users\JBeam\Desktop\Malware...
```

To make it easier, we can chain PowerShell commands using the `;` character and retrieve all three hash values at once.

```
Windows PowerShell
PS C:\Users\JBeam\Desktop\Malware> get-filehash .\wallpaperHD.exe ; get-filehash -algorithm md5 .\wallpaperHD.exe ; get-filehash -algorithm sha1 .\wallpaperHD.exe

Algorithm Hash Path
-----
SHA256 240387329DEE4F03F98A89A2FEFF9BF30DCBA61FCF614CDAC24129DA54442762 C:\Users\JBeam\Desktop\Malware...
MD5 0C4374D72E166F15ACDFE44E9398D026 C:\Users\JBeam\Desktop\Malware...
SHA1 FBAC123C604137654759F2FBC4C5957D5881D3D1 C:\Users\JBeam\Desktop\Malware...
```

## HASHES VIA LINUX CLI

10 Topics5 Quizzes

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

SI4) Correlation

6 Topics1 Quiz

SI5) Using Splunk

5 Topics2 Quizzes

INCIDENT RESPONSE DOMAIN

IR1) Introduction to Incident Response

8 Topics1 Quiz

File hashes can be easily retrieved using the Linux command-line. The three commands we would use are;

- sha256sum <file>
- sha1sum <file>
- md5sum <file>

```
root@SBTLab2: ~/Desktop
root@SBTLab2: ~/Desktop
root@SBTLab2:~/Desktop# sha256sum wallpaperHD.exe
240387329dee4f03f98a89a2feff9bf30dcba61fcf614cdac24129da54442762  wallpaperHD.exe
root@SBTLab2:~/Desktop#
root@SBTLab2:~/Desktop#
root@SBTLab2:~/Desktop# md5sum wallpaperHD.exe
0c4374d72e166f15acdfe44e9398d026  wallpaperHD.exe
root@SBTLab2:~/Desktop#
root@SBTLab2:~/Desktop#
root@SBTLab2:~/Desktop# sha1sum wallpaperHD.exe
f8ac123e004137654759f2fbc4c5957d5881d3d1  wallpaperHD.exe
root@SBTLab2:~/Desktop#
root@SBTLab2:~/Desktop#
```

# CONCLUSION

Whilst typically generating MD5 and SHA1 hashes are enough to perform reputation searches online and taking defensive measures within endpoint detection and response (EDR) platforms, some services such as Talos File Reputation require SHA256 hashes to perform checks against their databases. It's useful to know how to generate all three both in Windows and Linux.

< Previous Topic

Back to Lesson

Next Topic >