Module 1 Analyze Photos Lab

Description: In this lab, we will put on our digital forensics hats to analyze two photos for visual differences. We will then perform hashing on the photos and see the results that we will get. Finally, we will open them in a hex editor and discuss the results.

Requirement for lab: This lab is done in a Windows environment. Note: It is recommended that you run this lab in a virtual Windows machine.

Part 1 (Installing Tools)

Step 1: Login into your Windows machine

Step 2: Open a Web browser

Step 3: Do a search for **HashCalc**

Step 4: Click on the website URL (https://www.slavasoft.com/hashcalc)

Step 5: Click on Downloads at the top

Step 6: Scroll down the page, until you reach the "Free Software Downloads" section. You will see HashCalc 2.02

Step 7: Click the Download link

Step 8: This will download the HashCalc zip file

Step 9: Select the Show in Folder option

Step 10: Right-click and Extract the files

Step 11: You will then see the hashcalc folder

Step 12: Double-click on the folder

Step 13: Inside the folder, you will see setup.exe

Step 14: Double-click on setup.exe

Step 15: A UAC (User Account Control) prompt will open, select Yes

Step 16: The HashCalc Setup Wizard will launch

Step 17: Click Next and then Accept the license agreement

Step 18: Leave all the Default settings and click Next, then Install

Step 19: Uncheck the "View the README file" and "Launch HashCalc" checkboxes, then select Finish

Step 20: Go back to your browser search box and search for "**HxD Hex Editor**"

Step 21: Click on this URL in the search results: https://mh-nexus.de/en/hxd

Step 22: Scroll down the page, until you come to the latest version release for Windows (at the time of filming this video, the latest release was 2.1)

Step 23: Click the "Download Page" link

Step 24: Click the "Download per HTTPS" link for English

Note: You will see that we are given the SHA-1 hash calculation for the downloadable file. We will compare hashes in just a moment.

Step 25: The zip file will download

Step 26: On your Desktop, double-click HashCalc to open the application

Step 27: We are going to compare the hash of the HxD zip file

Step 28: Click the three little dots at the top-right of the HashCalc screen to browse for a file

Step 29: Locate the HxDSetup.zip file, select the file, and click Open

Step 30: Leave the default hash calculation types alone and click the Calculate button at the bottom

Step 31: Compare the hash for SHA-1 that you calculated with the hash on the website.

Question 1: Do the hashes match? _____

Step 32: Close the HashCalc application

Step 33: Open the Downloads folder where the HxDSetup.zip file is.

Step 34: Right-click on the file and Extract the files to the location of your choosing (I'm Extracting to the Desktop)

Step 35: Double-click on HxDSetup.exe to launch the installer

Step 36: A UAC (User Account Control) window will open, select Yes

Step 37: Choose English for the language and select OK

Step 38: Click Next and then Accept the license agreement

Step 39: Keep all the Default options and click Next

Step 40: Under the "Select Additional tasks" window, check the box to create a Desktop shortcut

Step 41: Click Install

Step 42: Uncheck the “View readme.txt” and the “Launch HxD Hex Editor” checkboxes

Step 43: Click Finish

Step 44: Close your browser window

Part 2 (Photo Setup)

Step 1: Login into your Windows machine

Step 2: Open a Web browser

Step 3: Search for any photo (I prefer a .jpg one) that you want and save it to your computer

Step 4: Double-click the **HxD Editor**

Step 5: The Editor launches

Step 6: Select File, then Open and navigate to the photo you just saved

Step 7: Select the photo and click the Open button

Step 8: You will see the Hex in the editor

Step 9: If you used a .jpg file, you will notice the Hex: FF D8 FF which is indicative of a .jpg file.

Step 10: Scroll to the very bottom of the HxD page and click in the text area

Step 11: Type in a short word. In this example, I just type the word test

Step 12: At the top, click File and Save As

Step 13: Name the file and save it

Step 14: We will analyze the file in Part 3

Part 3 (Analyzing Photos)

Step 1: Login into your Windows machine

Step 2: Open the folder with the original photo you had saved as well as the edited one

Step 3: Double-click on the HashCalc application and the HxD application to launch them

Step 4: Open both photos and see if you notice any visual differences

Question 1: Are there any visual differences in the photos? _____

Step 5: Next, Right-click on each photo to check the file size

Question 2: Are the files the same size? _____

Step 6: Next, we will check the Hash calculation of the files

Step 7: Select the three little dots on the top-right side of HashCalc to select a file

Step 8: Select the original photo you saved first

Step 9: Deselect all Hash options, except MD5

Step 10: Click Calculate

Step 11: Make a note of the hash

Step 12: Select the three little dots on the top-right side of HashCalc to select a file

Step 13: Choose the second photo you had altered and saved

Question 3: Are the file hashes the same? _____

Step 14: Switch over to HxD editor

Step 15: Select File, then Open

Step 16: Select the original photo you had saved and then select Open

Step 17: The file opens in the Hex editor

Step 18: Scroll down to the very bottom of the page

Question 4: Do you notice any secret information typed there? _____

Step 19: Select File, then Open

Step 20: Now choose the second file that you had altered and select Open

Step 21: Scroll to the bottom of the page

Question 5: Is there any secret information type there? _____