HxD – Freeware Hex Editor and Disk Editor

<https://mh-nexus.de/en/hxd/>

**Meta**

**Prompt**

Test your abilities to extract metadata.

**Walk-Through**

This challenge will give you experience with extracting metadata from an image file. You are given an image with contains metadata and you will need to use a metadata viewer to help answer the questions. You can see the image provided below:

A quick Google search for “metadata viewer” will provide several websites that can be used to view the metadata from the image.

💡

Tip: Make sure you’re using a reputable tool and don’t place too much confidence on a random website you found. You can always compare your results from multiple sources to verify that your answers are correct.

You can then upload your image to the view to get a table containing the metadata information. We’ve used [metadata2go.com](http://metadata2go.com/) in our example here, but other tools or sites will work as well.

We’ve censored some of the fields so you can practice using a metadata viewer

Once you have this table, you will just need to find the corresponding field to get the answer to each question.

**Questions**

**When was the image created? (Round to the nearest minute)**

See the “Create Date” field from the metadata viewer

**What is the image size in pixels? (ex: 800x600)**

See the “Image Size” field from the metadata viewer

**What is the make of the camera that took the picture?**

See the “Make” field from the metadata viewer

**What is the model of the camera that took the picture?**

See the “Model” field from the metadata viewer

**What is the exposure time for the picture? (ex: 1/200)**

See the “Exposure Time” field from the metadata viewer

**Where was the picture taken? Please use only positive numbers with 4 decimal places. (ex: 45.4000N, 75.6667W)**

See the “GPSPosition” field from the metadata viewer

⚠️

Depending on your metadata viewer, you may need to convert the GPS coordinates from DMS (degree, minutes, seconds) format to decimal format. The [FCC has a tool](https://www.fcc.gov/media/radio/dms-decimal) that can to the conversion.

©️ 2022 Cyber Skyline. All Rights Reserved. Unauthorized reproduction or distribution of this copyrighted work is illegal.

**Barcode**

**Prompt**

We intercepted a barcode we think might be hiding a flag. See if you can find it.

**Walk-Through**

This challenge will give you experience conducting lookups on a standard barcode. The challenge provides a .gif of the barcode.

You can solve this challenge by using mobile barcode scanning apps or an online barcode reader. We used <https://online-barcode-reader.inliteresearch.com/> for this example.

We’ve censored the value of the barcode so you can practice using a barcode viewer

**Questions**

**What format does the barcode use?**

You can find the format under the “Type” field.

**What is the flag hidden in the barcode?**

You can find the hidden flag by obtaining the value of the barcode in a barcode viewer.

©️ 2022 Cyber Skyline. All Rights Reserved. Unauthorized reproduction or distribution of this copyrighted work is illegal.

**Stego 1 - Strings**

**Prompt**

The hackers have hidden a message in this image. Find out what it is.

**Walk-Through**

This challenge will give you experience using basic Linux tools to find messages hidden with steganography. An image was altered slightly to embed a hidden flag somewhere in the raw binary of the image.



**Questions**

**What is the hidden flag in the image?**

The hidden flag can be found by using the Linux strings program. The following command will reveal the message:

strings Steg1.jpg | grep SKY

The strings command will search for sequences of ASCII text and the grep command will search those sequences for any that contain “SKY”, which is present in all flags.

©️ 2022 Cyber Skyline. All Rights Reserved. Unauthorized reproduction or distribution of this copyrighted work is illegal.

**Stego 2 - BlindHide**

**Prompt**

The hackers have hidden a message in this image. Find out what it is.

**Walk-Through**

This challenge will give you experience using basic tools to find messages hidden with steganography.



The Digital Invisible Ink Toolkit was used to hide a message using the BlindHide mode. The same tool can be used to reveal the hidden message.

You will need to set the filename of the output file using the “Set Message” option. This can be whatever you would like. In this example, we set it to out.txt.

When attempting to open the decoded file as a text document, you will find that the file appears as gibberish. However, there is a marker “JFIF” which is used to indicate that the decoded file is actually a .jpg image. This can be confirmed by running the Linux file command on the output document.

We’ve censored the flag so you can practice using the Digital Invisible Ink Toolkit

**Questions**

**What is the hidden flag?**

Use the Digital Invisible Ink Toolkit to obtain the hidden image using the “BlindHide” mode.

©️ 2022 Cyber Skyline. All Rights Reserved. Unauthorized reproduction or distribution of this copyrighted work is illegal.

**Stego 3 - BattleSteg**

**Prompt**

The hackers have hidden a message in this image. Find out what it is.

**Walk-Through**

This challenge will give you experience using basic tools to find messages hidden with steganography.



The Digital Invisible Ink Toolkit was used to hide a message using the BattleSteg mode. The same tool can be used to reveal the hidden message.

When the data is extracted from the image, another image is revealed:

This message can be decoded using an [online hieroglyph translator](http://discoveringegypt.com/egyptian-hieroglyphic-writing/hieroglyphic-typewriter/).

**Questions**

**What is the md5 sum of the hidden file?**

The MD5 sum can be found by running the Linux md5sum program on the output file from the Digital Invisible Ink Toolkit.

md5sum file.out

**What is the hidden message?**

Use the Digital Invisible Ink Toolkit to obtain the hidden image using the “BattleSteg” mode and then use the [online hieroglyph translator](http://discoveringegypt.com/egyptian-hieroglyphic-writing/hieroglyphic-typewriter/) to obtain the hidden message.

©️ 2022 Cyber Skyline. All Rights Reserved. Unauthorized reproduction or distribution of this copyrighted work is illegal.

**Stego 4 - HideSeek**

**Prompt**

The hackers have hidden a message in this image. Find out what it is.

**Walk-Through**

This challenge will give you experience using basic tools to find messages hidden with steganography.



The Digital Invisible Ink Toolkit was used to hide a message using the HideSeek mode. The same tool can be used to reveal the hidden message.

When the data is extracted from the image, another image is revealed:

This message can be decoded using the [Futurama Alphabet converter](https://www.gotfuturama.com/Interactive/AlienCodec/).

**Questions**

**What is the md5 sum of the hidden file?**

The MD5 sum can be found by running the Linux md5sum program on the output file from the Digital Invisible Ink Toolkit.

md5sum file.out

**What is the hidden message?**

Use the Digital Invisible Ink Toolkit to obtain the hidden image using the “HideSeek ” mode and then use the [Futurama Alphabet converter](https://www.gotfuturama.com/Interactive/AlienCodec/) to obtain the hidden message.

©️ 2022 Cyber Skyline. All Rights Reserved. Unauthorized reproduction or distribution of this copyrighted work is illegal.