FORENSICS: SHARK ON THE WATCH BY Monhal

EASY

Scenario:

Branko, a senior security researcher in your team, has decided to retire and pursue his hobby of bird-watching worldwide. Branko had an impressive collection of security-related books and articles that he collected over time. Rather than taking those with him, he chose to entrust the books to whoever will find the secret that he left on one of his thumb drives. Knowing Branko, you decided to focus on one specific thumb drive that you are sure has a hidden secret.

Objectives:

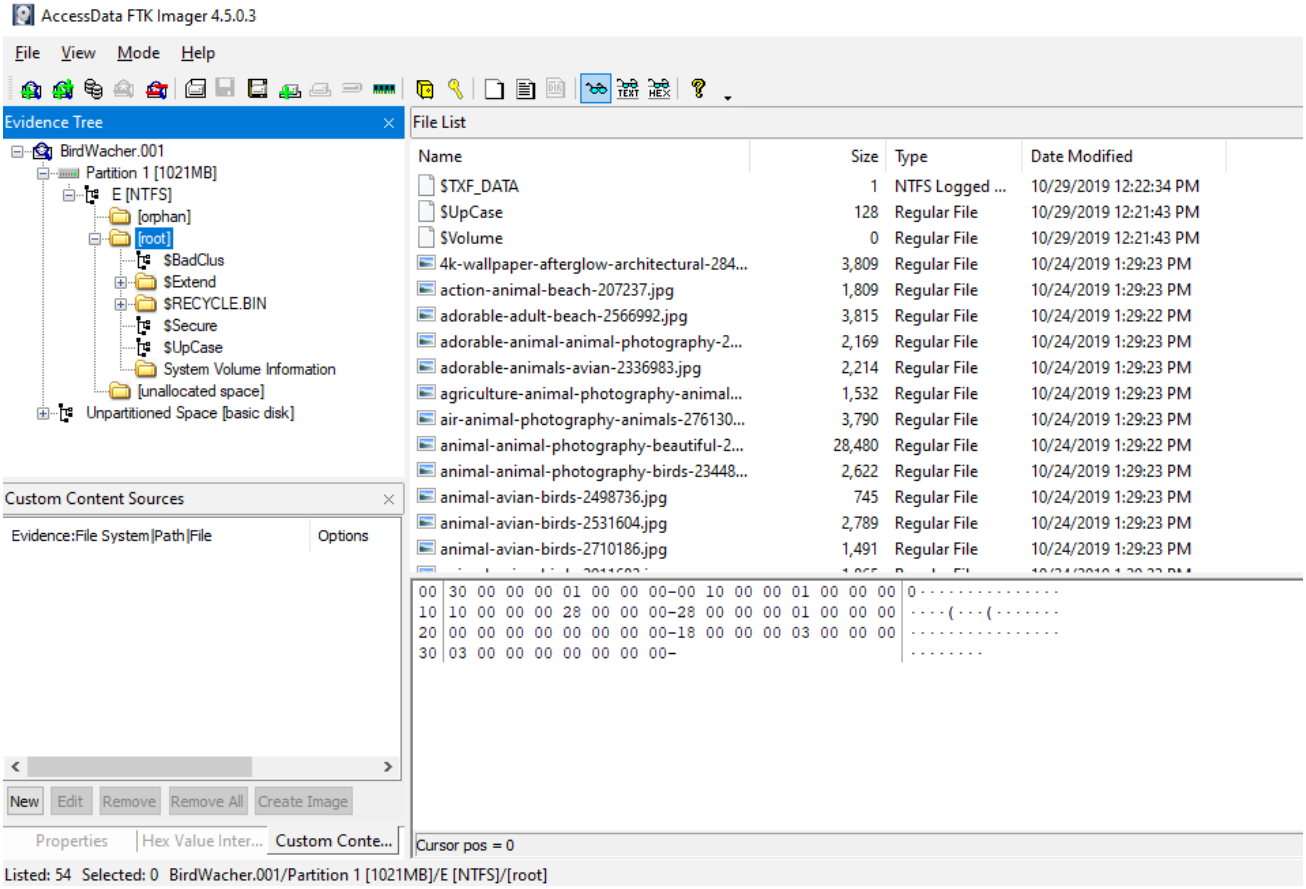
- Identify how Branko hid the secret on the thumb drive.
- Extract the secret (python might come in handy).

Used tools:

FTK Imager
HxD

First, extracting the .zip file in the downloaded ZIP.
Loading the file 'Birdwatcher.001' in FTK Imager and navigating to BirdWatcher.001 > Partition 1 > E [NTFS] > root directory. There it is possible to see all the images hidden in that directory.

Figure 1 - the images in the root directory



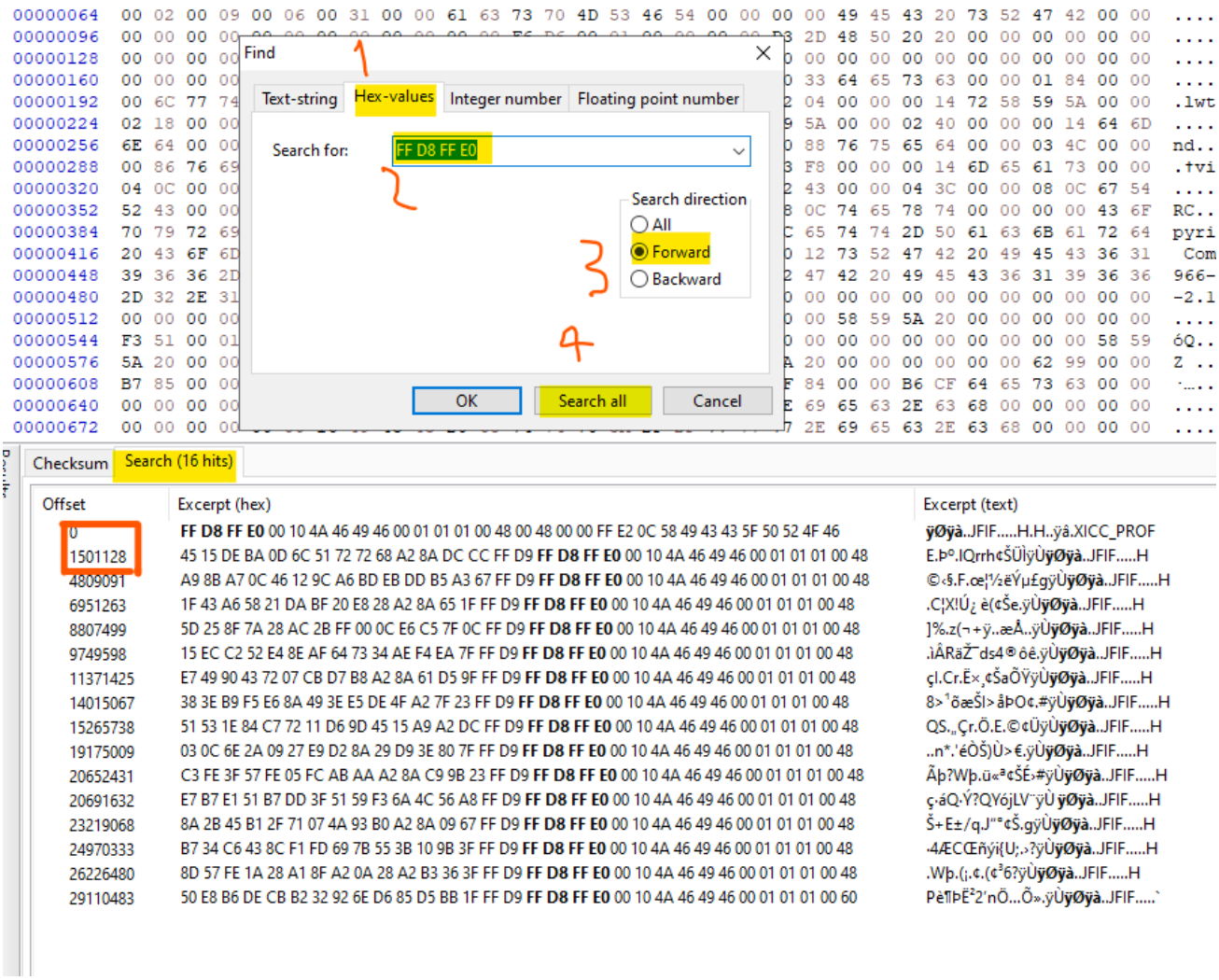
As the challenge scenario there are hidden data in those images, and the logic says that the image with the biggest size will be the targetted image.

Exporting the largest image to Desktop and oppening it in HxD
Now, in order to work properly. We need to investigate the given image. (surf investigating):

- the image is .jpg
- jpg header = FF D8 FF E0
- jpg footer = FF D9

In order to detect the embedded .jpgs in the given image. We need to seach for the headers. The headers number will be equal to the .jpgs number in the file .

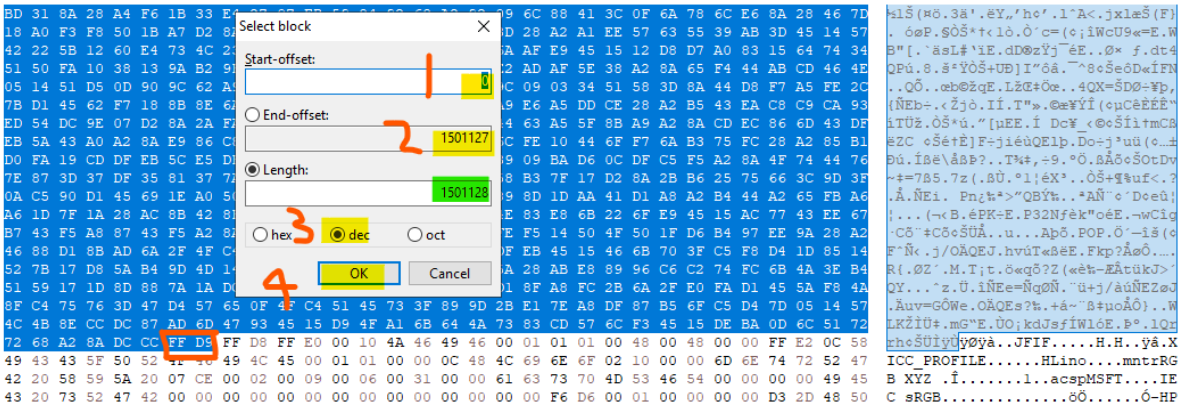
Figure 2 - presents the search &the files. (Ex: file 1: header 0, footer 1501127 | file 2: header 1501128, footer 4809090)



Now we can specify every image in this file according to the blocks (see the red square in figure 2).

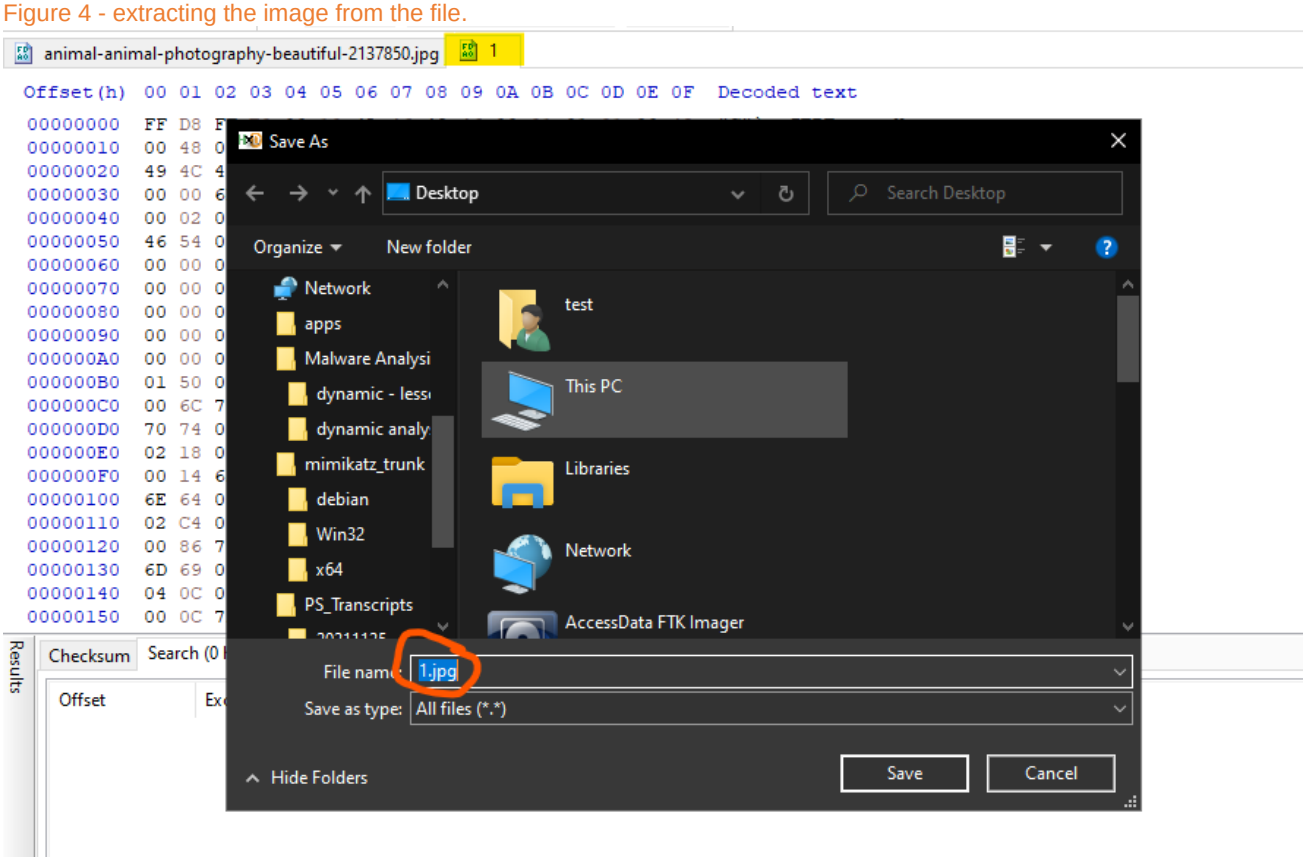
In order to select the block, Right Click > Select Block / Ctrl + E.

Figure 3 - Block selecting. *Notice the footer.



After selecting the block. The image need to be extracted. It is possible to copy the selected block and to paste it in a new HxD file. (make sure to check the header and footer after pasting). Then saving the image as .jpg!

Figure 4 - extracting the image from the file.



Repeating this step over all the 16 blocks found in the file.
<u>One of the pictures will contain the flag.</u>

CHALLENGE PWNED!

Please feel free to contact me on: **Monhalsarbouch@gmail.com**