Digital Forensics

Assignment 5 – Data Carving and Virtual Machine Forensics

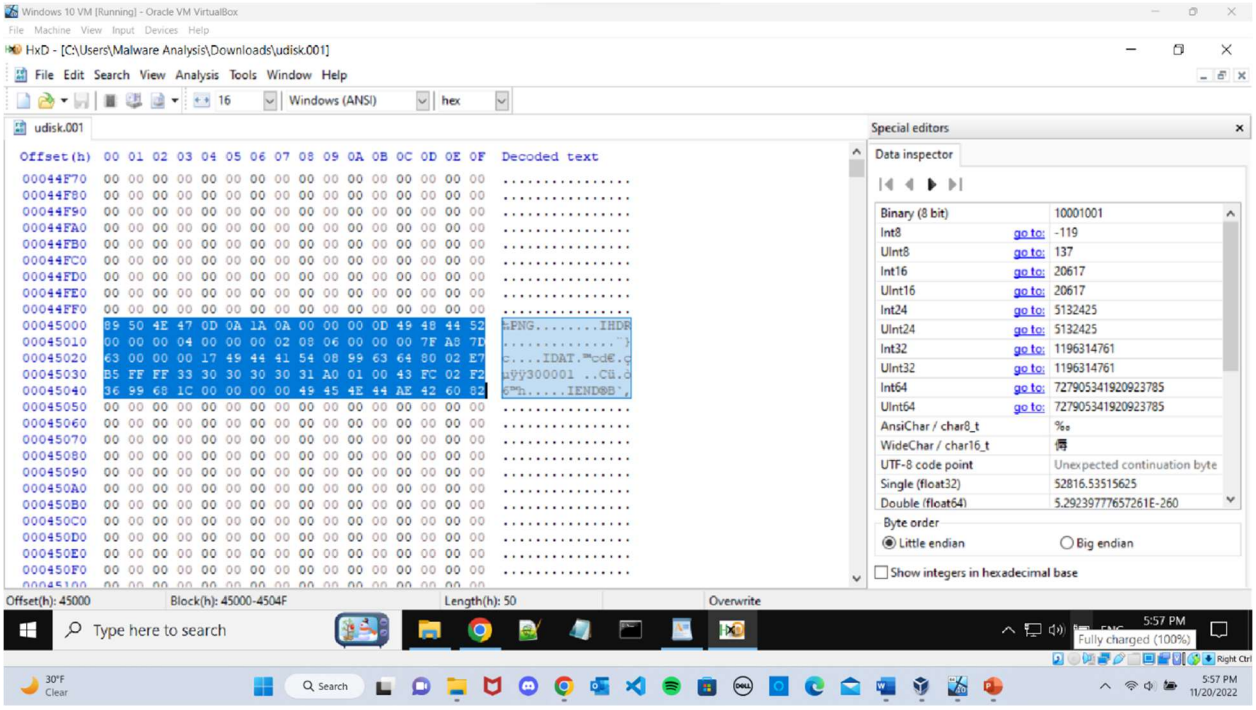
10 points

Kush Patel

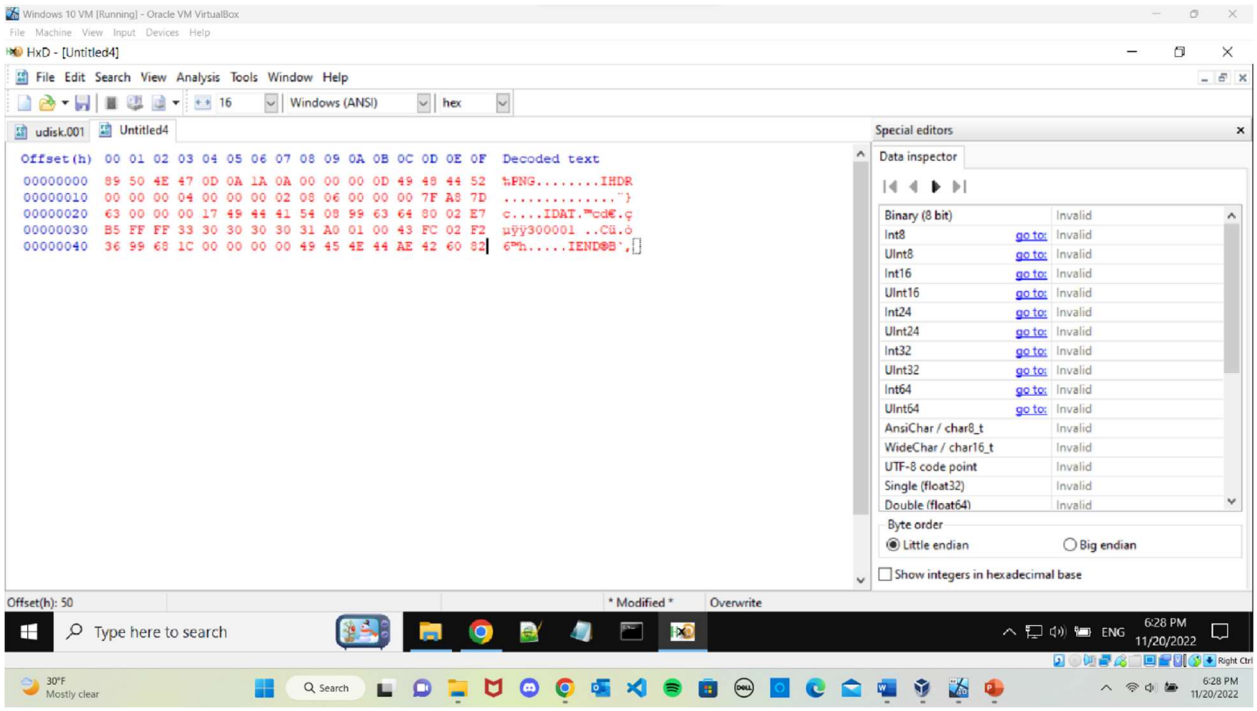
QUESTIONS

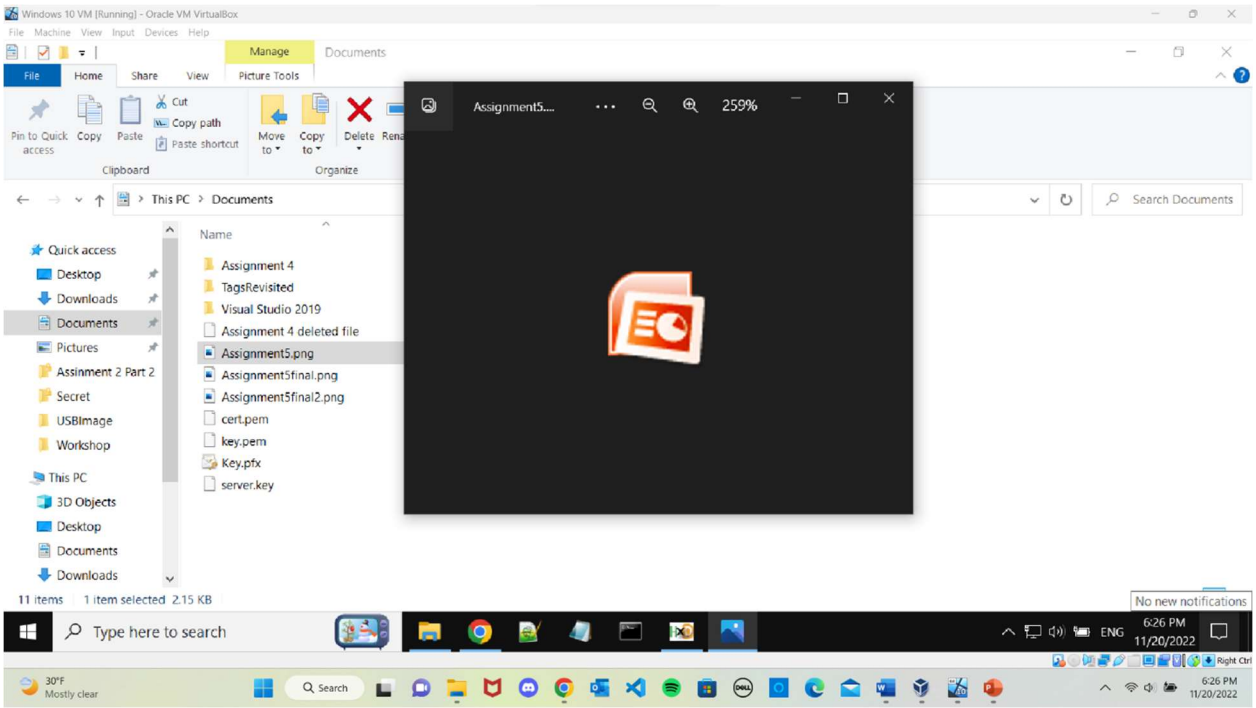
Please use the USB drive image udsik.001 (a raw image without compression) at https://www.dropbox.com/sh/ib0hn2229qb6dlc/AAC31n8e3yKV8-hU69kxFYsYa?dl=0. The image is also available at https://www.cs.uml.edu/~xinwenfu/forenisics/.

1. Please use HxD to carve an image of any type from udsik.001. Data carving has been discussed in class (CCI_10_Guide_Ch06-Tools.pptx).
    a. Provide a screenshot of the highlighted image **data** within HxD. (5 points)



b. Save the carved image data into a file with an appropriate extension using HxD. Provide a screenshot of the displayed image. (5 points)





OPTIONAL. If you have disk space, perform the following lab optionally and get 2 bonus points.

We can use Autopsy on the Windows VM to load a VM file for analysis.

c. Download Metasploitable -disk001.vhd at https://www.dropbox.com/sh/s74x9rnfj2i4brt/AABUJWTgfprM-juGYHUwUZxFa?dl=0 to the Windows VM. The VM file is also available at https://www.cs.uml.edu/~xinwenfu/forenisics/.

d. Start Autopsy for Windows, and click the **Create New Case** button. In the New Case Information window, enter today's date in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, create a subfolder if needed, and then click Select.

e. In the Additional Information window, type today's date in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

f. In the Select Data Source window, click the **Browse** button next to the "Browse for an image file" text box, Navigate to where Metasploitable -disk001.vhd is stored, click the file, and then click Open.

g. Autopsy should recognize the file type. Take a screenshot of the content of Metasploitable -disk001.vhd within Autopsy. (2 points)