Solution to Module 2 Hands-on Lab2 Exercise

1. Place the 2 files in a USB drive
2. Delete the Trans.xlsx file in the USB drive.
3. From this point onwards, create a video to show the complete solution to the hands-on lab.
4. Recover the deleted file using Recuva
5. Inside the Trans.xlsx file is the password (secret) to reveal the data in the Bulldozer.bmp. Save those files. Make sure they have the correct file extensions.
6. Use Autopsy and Sleuthkit
7. Open the TreasuryMemo.docx. Copy the Windings font part of the document and paste it in a textbox of a PowerPoint presentation. You will find in there the password "opensesame" that will be used to reveal the steg data in the StegInfo.bmp file.
8. The StegInfo.bmp has the IP address that is of interest. The IPTracker.txt contains the URL of the IPTracker website. Search for the IP address to find out the physical location of the attack.