Conclusion/Recommendation

I was tasked in finding out if there is any evidence of the frenergy company executive sharing the top secret drink recipe with its rival company. For this I was given 2 wireshark network files and found a USB on the scene which was allegedly the suspects property. When loading up the USB file we can find an image file called “f0000096.bmp”. This image has a file hidden inside it which I can only access with a password, this password is found in the audio file “f0001344.wma” also on the USB stick. This tells is the password is “frootL00p” which when placed inside the Steganography produces the full secret recipe. This images hash is “fecfb69be3daecf19a8f64894c31ecca” we now would have to find out where was this file sent from and who sent it.

Inside the wireshark files we can see messages were sent which talk about putting files up on the server with IP 192.168.0.9 with credentials frenergy/b005sterFri1t. This is where the files must have been uploaded to.

When using the network miner with the 2 Wireshark files we can see that the same image file with the hash “fecfb69be3daecf19a8f64894c31ecca” and the same audio file with the hash “6af5ec92c88f70cdb4acf5d9553a8fec” have been transferred from server IP 192.168.0.9 to destination 192.168.0.15.

GDPR

Computer Misuse act