|  |
| --- |
| **Pro Forma 3** |
| **System Information:** |
| $CarvedFiles(5)  $Unalloc(4)  System Volume Information (4) File Types By Extension   * Images(2) * Audio(2) * Office(3) * Plain Text(5)   By MIME Type   * Octet-stream(2) * X-ms-wma(2) * X-ms-bmp(2) * Plain(5)   Deleted Files   * File Systems(6) * All(11) |
| **Image Analysis:** |
| When looking inside the Audio files and extracting the “f0001344.wma” we hear a man saying that the password to get the recipe from the image is “frootL00p”.  Once we had the password, inside the Images folder we extract the “f0000096.bmp” image and open it up inside the Steganography tool. When right clicked and the password entered the software extracts a text file called “Recipe no secrets included” inside we find the real recipe.  MD5 Hash of Image file - fecfb69be3daecf19a8f64894c31ecca |
| **Internet Analysis:** |
| From loading the 2 Wireshark network capture files into Network Miner I can see in the Files section an image file called “drink.bmp”. When checking this files MD5 hash we get: fecfb69be3daecf19a8f64894c31ecca  Another audio file called “drink.wma” is found whose MD5 hash is 6af5ec92c88f70cdb4acf5d9553a8fec  Further in the files section we can find 7 message files from someone nicknamed “esbestikk” saying:  1.” Hi J Jo”  2.” Yes i put image and sound file on server”  3.“ frenergy”  4.” 192.168.0.9”  5.” frenergy/b005sterFru1t”  6.” disks will be wiped”  7.” out”  At packet number 283,284,285,286 we can see a user esbettik logging in using password 5uperju1ce  Inside Wireshark when we open the frenergy1 file and filter only FTP protocols at No.1396, No.1397, No.1474, No.1476, No1986 we can see the file “drink.bmp” being transferred from source=”192.168.0.9” to destination=”192.168.0.15”  At No.343, No.344, No.351, No.543 we can see the file “drink.wma” being  transferred from source=”192.168.0.9” to destination=”192.168.0.15” |
| **Notes:** |
| In autopsy I opened the USB stick image to try and find any carved files. Inside I found the image and an audio file saying the password to open the image using the Steganography tool and get the recipe.  Took hash of image with recipe  In the internet files I found a message conversation between 2 users talking about files being uploaded to server  Furthermore I can see the 2 files being transferred over network |