|  |
| --- |
| **Pro Forma 2:** |
| **Chain of Custody Process:** |
| Once on the scene I secured the USB stick with me for analysis. From 10am till 11am I had the USB with me while I inspected the scene for any further evidence. At 11 I passed it on to my supervisor who sent it to the main headquarters for holding, it stayed there till 1pm. When I returned from the scene I took the usb out of the cabinet and plugged it into my work station. I took a copy of the USB image to be put through autopsy and look for any clues there.  Once I was finished taking the image I returned the USB into the holding cabinet in the storage room. |
| **Forensic Tools:** |
| ForensicImager – software used to make a bit for bit copy of the usb image  Autopsy – image files are imported to be “opened up” and inspected for any deleted o hidden files.  Wireshark – used to capture and filter network packets sent across networks  Networkminer – Wireshark files were imported for further in-depth analysis  WinMD5 – computes MD5 hash for a file and can optionally compare hashes for match |
| **Forensic Acquisition:** |
| First I secured a copy of the USB image by using forensicimager.  Before inserting the USB I used a write blocker to stop any data getting back onto the USB and corrupting it.  I opened the software up and clicked the “image acquisition” button. This allowed me to select a plugged in storage and make a copy of its image.  I selected the USB2 (drive G) and waited for around 20 minutes for the process to be over.  See images in appendix “Taking USB Image”.  Once complete the copy of the USB image was saved to my personal usb stick for use in autopsy later. |
| **Notes:** |
| First step I took is to secure the image of the USB stick, with that I could use the autopsy software to try and find any hidden or deleted files.  I loaded both of the Wireshark files provided by the company in networkminer to see who was logged in and what were they doing.  When I opened the image in autopsy I got a lot of carved and deleted files back. |