|  |  |  |  |
| --- | --- | --- | --- |
|  | Analysis Notes - | |  |
| Suspect Details | | Exhibit numbers, Computer details, HDD’s / Partitions / OS etc. | |
|  | |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| Client |  | Reference |  |
| OIC (plus contact details) |  | Bailed to Return Date |  |
| Seize Date |  | Case Type |  |
| Examiner |  | Exam commenced |  |
| Other relevant information |  | Software used, versions and licensing |  |

| Action | Done? | Date | Time | Notes | Initial |
| --- | --- | --- | --- | --- | --- |
| Load case & verify in EnCase |  |  |  |  |  |
| Load case into FTK Imager |  |  |  |  |  |
| Dual verification of key evidence items. |  |  |  |  |  |
| Recover lost folders (FAT16 & 32). |  |  |  |  |  |
| Mount archives; zip, thumbs.db, etc |  |  |  |  |  |
| File signature analysis, compute hash values |  |  |  |  |  |
| Run filefinder |  |  |  |  |  |
| Initialise Case script |  |  |  |  |  |
| Timeline analysis, date of last activity |  |  |  |  |  |
| Log-on passwords –  use SAMInside |  |  |  |  |  |
| Registry protected area  (Secret explorer) |  |  |  |  |  |
| Internet History, favourites. Other browsers?  Netanalysis |  |  |  |  |  |
| Run relevant keyword searches |  |  |  |  |  |
| Emails, local & web-based. |  |  |  |  |  |
| IM clients |  |  |  |  |  |
| Export doc / office & exe files; look at Meta data if required |  |  |  |  |  |
| Clean-up utilities. Check log files |  |  |  |  |  |
| Encryption, Steg , use FTK |  |  |  |  |  |
| Link files |  |  |  |  |  |
| Print artefacts |  |  |  |  |  |
| CD/DVD burning apps; check log files |  |  |  |  |  |
| Email OIC with results |  |  |  |  |  |

|  |
| --- |
| Additional Notes |
|  |