## Data Collection Work Instruction

| **Windows registry, Trace log and UccApiLog collection from Volume Shadow Copy** | |
| --- | --- |
| 1. | Requirements:  Download and extract the md5deep software package (<https://github.com/jessek/hashdeep/releases>). Add the extract location to the system’s path variable  Download and extract the SysinternalsSuite (<https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite> and add the SysInternalsSuite utils path to your environment PATH settings because the scripts make use of the Psexec and strings utils.  Make sure you run the script below from a command line with the appropriate privileges on the target client.  Volume Shadow Copies should be active on the Windows target client |
| 2. | Run the script “SfB\_DataColl\SfB\_data\_collection.bat” |
| 3. | Insert the required information. Once the scripts asks to “[Copy the Shadow Copy Volume value from the log file:]”, copy the appropriate Shadow Copy Volume value from the log file. |
| 4. | The script collects the files with Skype for Business artefacts from the client to the “username” folder.  A log of the collection activities and an overview of the collected files’ sha256 hashes will be stored in the “log” folder. |

## Extraction to report instruction

| **NTUSER.dat collection from VSC** | |
| --- | --- |
| 1. | Requirements:  Install the GitBash only from the Git for Windows (<https://git-for-windows.github.io/>) package.  Download and install the application RegFileExport (http://www.nirsoft.net/) to extract information from registry.  The tracerpt program which is Microsoft Windows 10 built-in (https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/tracerpt\_1) |
| 2 | Run the script “Extract2Report\SfB\_extract\_artefacts.sh” |
| 3. | Insert the required information, please be aware that the folder/file paths should be inserted as the \*nix structure and are case sensitive. |
| 4. | The script stores the report files in the “report” folder.   * In the file 01.<username>.SfB\_Artefacts\_Report.rpt the complete artefacts report is stored. * Keep in mind that the file “<username>.etl\_output.csv” is large in file size. This csv file contains the extracted information from the Trace log files |