A report was received by the Northern Police Service regarding a suspected insurance fraud involving Fred Smith and Daphney Smith.  The report was instigated by their business partner Barney Gumble who has stated that due to a failing business, he believes Fred Smith has faked his own death to claim insurance money and is no longer in the country.

An arrest was made of Daphney Smith as she was making arrangements to leave for Spain.  Information was passed onto Spanish authorities who identified and arrested Fred Smith.  Forensic Images were made of the a computer taken from the home of the Smiths, now referred to as Image 1.  These image is now submitted for Forensic Analysis to identify the following:

* Evidence to support the planning or execution of insurance fraud
* Evidence of who had knowledge of the suspected crime
* Evidence of a motive to commit insurance fraud
* We are particularly interested in confirming who did what and when.
* Where evidence of files or data is found we would like to confirm a users awareness of this data.

According to Barney Gumble, both Fred and Daphney Smith are highly computer literate.  It is, therefore, requested that review is made for any potential encrypted or hidden files.

For record the timezone is Europe/London.

There are two aspects to the submission:

* [**Contemporaneous Notes**](https://docs.google.com/document/d/15Fhk5JKk4Zst0njkEqYheyTwPvk-Ai87l_POlBQo52E/edit?usp=sharing):
  + Detailed actions should be recorded
  + Highlight of the significance of findings
  + Justification of the reasons for conducting a certain action
  + Chronological order
  + Detailed enough to allow replication, but not an essay
  + Use of screenshots and tables
  + Clear identification of tools, with justification
  + Clear identification of the data under examination
  + Integrity confirmation of the exhibit
* [**Briefing Statement**](https://docs.google.com/document/d/1NFijqiItlOjEImgUFiihRVUjHCx7BhMcWOCzvC4EuoU/edit?usp=sharing):
  + Focus on summarising existing evidence/leads and promoting further lines of enquiry.
  + Consider the format, tone and structure of what you write – this is intended for a professional audience, there should be few grammatical and spelling errors
  + Accuracy is the key, your results should be accurate, justified and relevant
  + Explain technical terms
  + Ensure you have a balanced perspective on what is there

**Toolsets**:

* You may use any tool introduced during the course, in earlier courses or identified through your own research
* Your “main” tool must be capable of opening an E01 file
* You will need to:
  + Identify hash’s
  + Look for keywords
  + Review images
  + Export and report on data
  + Review dates and times
  + Look at the Registry
  + Look at Windows artefacts
  + Access restore points
  + Identify cloud-based accounts
  + Identify and analyse web history

The password to extract the E03 is: iamsecure

Make sure you extract the E03 into the same folder as the E01 and E02