1 Hash Test Preview

1.1 Rubric:

- The test duration is 80 minutes.
- The test is an individual assessment.
- You must not communicate with anyone else during the test (online or in person).
- The test is open book. You may bring in your own handwritten paper notes but must not share these with anyone else.
- You may not browse the web. The only page permitted in your browser is the Moodle page for the test.
- You must work only in one bash shell. All other windows must be closed.
- You must not disturb other students.
- If you need assistance, raise your hand.

1.2 Context:

You are performing an investigation and have been supplied with the compressed archive `archive.tar.gz`. You have also been supplied with the three hashsets:

- `hashset-earlier` - the hashes of the files in the archive taken at some point in the past.
- `hashset-good` - the hashes of known good system configuration files.
- `hashset-bad` - the hashes of known malware

1.3 Instructions:

You are sitting in pairs: one person on the left, on on the right. There are two tests on Moodle. You take only one of them.

- Choose the Moodle HashTest/LEFT directory if you are sitting on the left.
- Choose the Moodle HashTest/RIGHT directory if you are sitting on the right.

Create the folder `~/Desktop/HashTest/` and use this for all your working.

Open a terminal and set your working directory to `~/Desktop/HashTest/`

Confirm this directory is empty using the command:

```
ls -A
```

From your Moodle (LEFT test or RIGHT test as appropriate), save the three hashsets and the archive to the directory `~/Desktop/HashTest/`

Expand the archive into using the command

```
tar -xzf archive.tar.gz
```

Write your University ID and the date on your answer paper.

If you are taking the LEFT test, write LEFT on your answer paper.

If you are taking the RIGHT test, write RIGHT on your answer paper.

1.4 Questions:

Q1) Explaining your reasoning, identify which cryptographic hashes were used to produce:

Q1.1) `hashset-earlier` (2 marks)

Q1.2) `hashset-bad` (2 marks)

Q1.3) `hashset-good` (2 marks)

Q2) Identify which files are present in the archive but have different content from when `hashset-earlier` was taken. (5 marks)

Q3) Identify which files have been deleted from the archive that were present when the `hashset-earlier` was taken. (4 marks)

Q4) Identify which files in `hashset-earlier` are duplicate copies of other files in `hashset-earlier`. Ensure your answer unambiguously groups together the files that are duplicates of each other. (5 marks)

Q5) Identify which files in the archive have been renamed from the name used in `hashset-earlier` to the name used in the archive. Ensure your answer is unambiguous as to which name is "from" and which name is "to". (5 marks)

Q6) Identify which files in the archive are known malware. (5 marks)

Q7) Identify which files in the archive are neither known good system configuration files, nor known malware. (5 marks)

Q8) Unseen question. (5 marks)