1 Test

NAME_YOUR_TEST_CASE

file name	md5	file size
alist.of	3451c9e7de48d53248b536e12b01938d	123 B
files.that	b2c4c8e1c7da08143ec21ba088b3ac53	456 B
belong.to	7ad3cb46812e14c1ba9571def9134f1a	13 B
the.case	e314e89d4e3ea2806be9a179f3161045	16 B

Description:
Please describe the test case with a few words. What is created and in what way does it contain any anti-forensic techniques.
Do not(!) describe the expected behaviour of the software in here.
To be used on:
What kind of forensic tool can be tested with this test case?
(e.g., image analysis software, hardware writeblocker, ...)

Obligatory behaviour:
What MUST the tool show/do?
For example, software must show that an animated gif contains multiple pictures.

Ideal behaviour:
What SHOULD the tool show/do? This is generally an improved version of the obligatory feedback. For example, a software could not only show the animated gif sequentially, but instead show every single frame in an extra view.

Alternatively allowed behaviour:
If the obligatory part cannot be achieved, what MUST be done alternatively?
For example, if the software is unable to show animated graphic files, it MUST instead state that the file is animated and advise the user to view it in a different program.

Bad behaviour:
At the moment there are two types of bad behaviour.
[p]otentially critical behaviour: A test case results in a wrong error message or in an unresponsive tool. This is not critical per se but can mislead the investigator in a false direction.
[c]ritical behaviour: Everything that results in misinformation of the investigator. Critical behaviour ranges from a crashing tool (potential exploitation possibility) to altering the evidence data itself, thus making it useless.