

Bytes and Strings Rear Their Ugly Heads Again

The pickle protocol has been around for many years, and it has matured as Python itself has matured. There are now [four different versions](#) of the pickle protocol.

- Python 1.x had two pickle protocols, a text-based format (“version 0”) and a binary format (“version 1”).
- Python 2.3 introduced a new pickle protocol (“version 2”) to handle new functionality in Python class objects. It is a binary format.
- Python 3.0 introduced another pickle protocol (“version 3”) with explicit support for bytes objects and byte arrays. It is a binary format.

Oh look, [the difference between bytes and strings](#) rears its ugly head again. (If you’re surprised, you haven’t been paying attention.) What this means in practice is that, while Python 3 can read data pickled with protocol version 2, Python 2 can not read data pickled with protocol version 3.