

Linux incident response - understanding endianness

Taz Wake | Halkyn Consulting Ltd | Originally published 2023-10-25

Endianness is a concept related to how multibyte data is stored in computer memory. Computers store data in bytes, which are made up of smaller units called bits (usually 8 bits in a byte). When multibyte data types, such as integers and floating-point numbers, are stored in memory, the order in which the bytes are arranged can vary between computer architectures. This order is referred to as the endianness, and there are two main types: little-endian and big-endian.

In little-endian systems, the least significant byte (the smallest unit) of a multibyte data type is stored at the lowest memory address, while the most significant byte (the largest unit) is stored at the highest memory address. In other words, the data is stored in memory from right to left, with the least significant byte at the smallest address and the most significant byte at the largest address.

In contrast, big-endian systems store the most significant byte at the lowest memory address, and the least significant byte at the highest memory address. The data is stored in memory from left to right, with the most significant byte at the smallest address and the least significant byte at the largest address.

For example, take a file containing the hex string 0x12345678.

Reading it with xxd in little-endian format will look like this:

```
78 56 34 12
```

Reading it with xxd in big-endian format will look like this:

```
12 34 56 78
```

The choice of endianness can affect how data is exchanged between different computer systems. For example, if a file containing multibyte data is created on a little-endian system and then transferred to a big-endian system, the bytes need to be rearranged to interpret the data correctly.

Both Linux and Microsoft Windows operating systems support both little-endian and big-endian architectures. However, the x86 and x86-64 architectures, which are commonly used in PCs and servers, are little-endian architectures. This means that most PCs running Linux, macOS or Windows use little-endian byte order. However, there are other architectures, such as some older RISC-based systems, that use big-endian byte order. Operating systems designed to run on these architectures, such as certain versions of Unix and Solaris, handle big-endian byte order natively. In modern computing, little-endian architectures are prevalent due to their widespread use in personal computers and servers. This uniformity simplifies data exchange and interoperability between different systems.

Fun, added, fact? The XFS filesystem (default on RHEL and Amazon Linux), stores filesystem metadata in big-endian format, irrespective of the underlying architecture.

Find out more about Linux filesystems, and how we can manually analyse them on the new FOR577 Linux incident response course from [SANS Institute](#). This course is available both for in-person attendees and live-online students. You can also register now for early access to the on-demand version which will be available in early 2024.

Find out more: <https://sans.org/for577>

#forensics #linux #dfr #threathunting #filesystems #endianess #knowledge #learning

About Halkyn Consulting

Halkyn Consulting Ltd is a UK-based security and risk management consultancy providing 24/7 incident response, digital forensics, threat hunting, virtual security leadership (vCISO) and security compliance support to organisations worldwide. We deliver clear, practical, vendor-independent advice based on real-world threats — no hype, no upsell.

More free security resources are available at www.halkynconsulting.co.uk/security-resources.

Web: www.halkynconsulting.co.uk | **Email:** info@halkynconsulting.co.uk | **Tel:** +44 1244 940858