What is an IP-address?

And how it is used for the identification of child sexual abuse offenders online

FACTS

IP stands for Internet Protocol.

It is a technical language that allows two devices to communicate with each other over the Internet.

IP addresses can either be 'static' [never changing] or 'dynamic' [temporary].
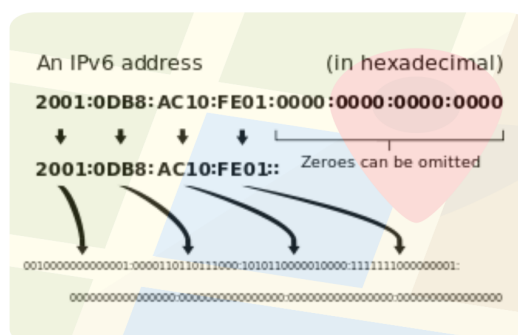
How does it work?

An IP-address is the identifier or unique signature of a device, which allows the device to be identified, pinpointed and differentiated from other devices that are connected to the Internet. Every device comes with its own IP-address whether it is a computer, TV, gaming console or other device.

IP-addresses allow for communication between devices. In the same way that a person needs a post address to be able to send a letter, a remote computer needs the IP-address of a device to be able to communicate with it. IP-addresses thus enable users to send and retrieve data and ensure that communication and data reach the correct destination. It reveals information such as where the device is located and which Internet Service Providers is servicing it. This protocol is universal and works the same for every device or location.

IP-Address format

An IP-address consists of a set of numbers and dots. The number of available IP addresses is beginning to expand as a new version of the IP protocol - IP version 6 or IPv6 - becomes more widely used.

An IPv6 address   (in hexadecimal)

2001:0DB8:AC10:FE01:0000:0000:0000:0000

2001:0DB8:AC10:FE01::   Zeroes can be omitted

0010000000000001:0000110110110111000:1010110000010000:1111111000000001:

0000000000000000:0000000000000000:0000000000000000:0000000000000000

The use of IP-addresses for identification purposes

When child sexual abuse offenders connect to the Internet they use devices which have IP-addresses. These IP-addresses leave a trail of Internet activity. This can provide the authorities with an opportunity to track down the device and often will enable them to tell when and where the device was used. This in turn means the individual who was using the device to commit a crime often can be identified.

The authorities can also cooperate with Internet Service Providers (ISPs) to access (temporary) IP-address logs and activities on their servers for the purpose of user identification.

Unfortunately, offenders can take measures to hide their IP-address. One method is by using Proxy Servers. Rather than accessing a website directly, the user's request will be redirected through the proxy server that does not record the IP address of the device making the request. This offers a degree of anonymity. Another example is the use of IP-spoofers to mask the real IP-address and wrongfully present a different IP-address as the source of illegal conduct.

There are also other tools and Internet services available which can make finding an individual's IP address very difficult and time-consuming.

ECPAT