

PCAPNG

draft-tuexen-opsawg-pcapng-00.txt

Michael Tüxen  
tuexen@wireshark.org

# What is PCAPNG?

- Initially Wireshark used PCAP as the file format for saving capture files.
- PCAP only allows you to save the captured packets and the corresponding capture time.
- PCAPNG was developed to overcome several limitations of PCAP. Work started more than 10 years ago...
- Now Wireshark uses PCAPNG as its default file format for saving capture files.

# Why use PCAPNG?

- Support for
  - capturing from multiple interfaces
  - meta data
  - statistical data
  - packet annotations
  - DNS-related information
- Extensible by using a TLV-based format.

# Why bring PCAPNG to the IETF?

- Having a well specified file format for capture files is important for the network community.
- Experience while improving PCAPNG support for Wireshark showed that the document can be improved.
- Other users of the file format like have additional requirements.
- Wider review improves the specification.

# Is there interest in PCAPNG

- within the IETF?
- within OSPAWG?