WIRESHARK DISSECTOR

Wireshark is a popular network traffic analyzer. It allows deep inspection and rich analysis of many network protocols. For a more detailed introduction to Wireshark please see their about page.
In 2014 as a GSOC project, Kevin Cox wrote a Wireshark dissector for the Ceph protocol. This dissector allows Wireshark and related tools to identifyy and understandnd Ceph network traffic.

PRIOR WORK

There had been two past efforts to create a Wireshark dissector for Ceph, however they were not very complete and no longer compile on a modern version Wireshark.
Additionally, both of these dissectors were designed as plugins meaning that they were outside of the Wireshark project. This means that it is hard to keep them up to date as the Wireshark API changes over time. Converting these plugins to internal dissectors was considered however the plugins did not comply with Wireshark coding standards and were unsuitable to be included in Wireshark.

GSOC PROJECT

Before the project started it was decided that the best route forward was to create the new dissector from scratch, using the existing Wireshark plugins as examples. From the start the Ceph dissector was built and tested in the Wireshark source tree following the their coding guidelines to ensure it would work everywhere Wireshark runs and continue to be maintainable into the future.
The aim of the project was centered around creating a dissector which could be easily maintained and extended as both Ceph and Wireshark changed over time. The main points from the proposal - in order of importance - were:

- Create a strong framework, from which the dissector can be built. It is critical that this is easy to understand and use so that new message types can be added in the future.
- Code such that the dissector can be accepted into upstream Wireshark.
- Work with the Wireshark team to get the dissector into Wireshark natively.
- Implement as many message types as possible.

The project was successful and the first patch was accepted into Wireshark on August 4th. For the rest of the summer the work was focused on adding more messages and many of thoses patches were accepted as well.

ANALYSING CEPH TRAFFIC WITH WIRESHARK

While the code has been included in Wireshark it has yet to be released. Until the next release you must build from the latest sources if you want to use the Ceph support. The process is outlined in great detail in the Building and Installing section of the Wireshark Users Guide.
Once you have Wireshark up and running the Ceph dissector will automatically identify and analyze any Ceph traffic. If your traffic isn't getting recognized for some reason there are a few likely reasons.
If you didn't caputre the whole session the dissector won't be able to recognize the protocol, ensure you capture right from the start of the session.
The other likely cause is that another dissector is configured to analyze traffic on the ports your Ceph traffic is using. While the Ceph dissector will recognize traffic on any port other dissectors with the port set explicitly get priority. Try disabling the other protocols or changing the port they analyze.
h3. Contributing to the Ceph Dissector

The process for working with the dissector is documented in the Ceph developer documentation