

Big picture

Worksheets

PCAP file



An investigation/exploration needs a starting point. In this case, Bro identifies a suspicious connection; the analyst drags a PCAP file into the worksheet. OPUS uses this to find the 4-tuple of the relevant connection in the causality graph.

