

NETRESEC | Products | Resources | Blog | About Netresec |

NETRESEC > Products > SplitCap

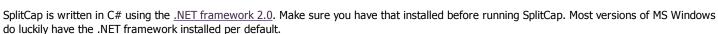
## SplitCap

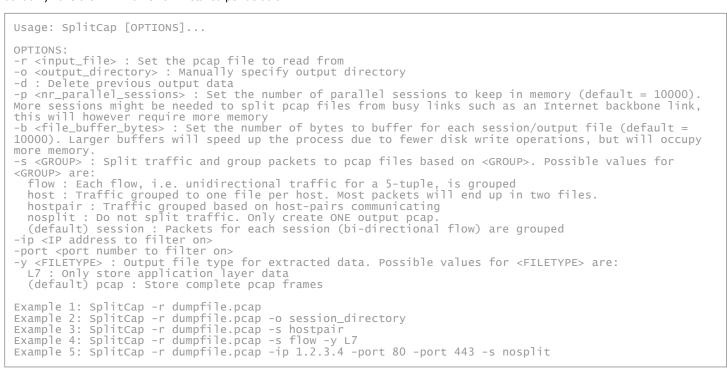
SplitCap is a free (as in beer) open source pcap file splitter. SplitCap splits one big pcap file into multiple files based on TCP and UDP sessions, one pcap file per session. SplitCap can also be used to split a pcap file into one pcap file per host-pair instead of session.

One of the best features of SplitCap is that is is REALLY fast!

>> Download the latest version of Splitcap <<

The TCP and UDP session concept in SplitCap is defined as bi-directional flows, i.e. all frames / packets with the same 5-touple (source host, destination host, source port, destination port, transport protocol) regardless of packet direction are considered part of the same session.





SplitCap is created as part of the <u>Statistical Protocol IDentification</u> research project carried out by Erik Hjelmvik with fundings from <u>.SE (The Swedish Internet Infrastructure Foundation)</u>.

SplitCap can since version 1.5 also be used in order to efficiently filter a large PCAP file based on one or several IP addresses or TCP/UDP port numbers. Simply use the "-s nosplit" option together with one or several "-port" or "-ip" switches to specify what traffic to keep from the large pcap file. SplitCap performs this type of filtering much faster and with way less memory usage compared to tshark.

Warning: When extracting application layer data (L7) by using "-y L7" SplitCap does not perform any proper TCP session reassembly. This means that TCP retransmissions and overlapping segments will cause the same data to be written twice. Out-of-order TCP packets will also cause the application layer data to be stored in an out of order sequence.

Applications that can do proper TCP session reassembly are NetworkMiner and Wireshark.

You can read more about how to use SplitCap in our blog post "Split or filter your PCAP files with SplitCap".

## Splitting large peaps with GUI application

Do you need to filter large pcap files based on flows / sessions? Then please have a look at our <u>CapLoader</u> tool instead. CapLoader can be used to efficiently extract full content data for a single or multiple flows from big pcap files. Please visit our CapLoader page for more information: <a href="http://www.netresec.com/?page=CapLoader">http://www.netresec.com/?page=CapLoader</a>

## Links

- SplitCap project page on SourceForge
- Statistical Protocol IDentification SPID
- NetworkMiner
- .SE The Swedish Internet Infrastructure Foundation
- NETRESEC Network Security Blog

## sourceforge

© 2010-2013 NETRESEC AB | Contact Us | Privacy | RSS