Experts in network security monitoring and network forensics

NETRESEC

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 written in C# using the .NET framework 2.0. Make sure you have that installed before running SplitCap. Most versions of MS Windows do luckily have the .NET framework installed per default.

```
Usage: SplitCap [OPTIONS]...

OPTIONS:
-r <input_file> : Set the pcap file to read from
-o <output_directory> : Manually specify output directory
-d : Delete previous output data
-p <nr_parallel_sessions> : Set the number of parallel sessions to keep in memory (default = 10000).
More sessions might be needed to split pcap files from busy links such as an Internet backbone link,
this will however require more memory
-b <file_buffer_bytes> : Set the number of bytes to buffer for each session/output file (default =
10000). Larger buffers will speed up the process due to fewer disk write operations, but will occupy
more memory.
-s <GROUP> : Split traffic and group packets to pcap files based on <GROUP>. Possible values for
<GROUP> are:
  flow : Each flow, i.e. unidirectional traffic for a 5-tuple, is grouped
  host : Traffic grouped to one file per host. Most packets will end up in two files.
  hostpair : Traffic grouped based on host-pairs communicating
  nosplit : Do not split traffic. Only create ONE output pcap.
  (default) session : Packets for each session (bi-directional flow) are grouped
-ip <IP address to filter on>
-port <port number to filter on>
-y <FILETYPE> : Output file type for extracted data. Possible values for <FILETYPE> are:
  L7 : Only store application layer data
  (default) pcap : Store complete pcap frames

Example 1: SplitCap -r dumpfile.pcap
Example 2: SplitCap -r dumpfile.pcap -o session_directory
Example 3: SplitCap -r dumpfile.pcap -s hostpair
Example 4: SplitCap -r dumpfile.pcap -s flow -y L7
Example 5: SplitCap -r dumpfile.pcap -ip 1.2.3.4 -port 80 -port 443 -s nosplit
```

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

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 pcaps with GUI application

Do you need to filter large pcap files based on flows / sessions? Then please have a look at our CapLoader 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: http://www.netresec.com/?page=CapLoader

Links

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