



# Merging Data

# Merging Data

» Using mergecap (command line)

» Merging features

- Prepend
- Chronologically
- Append

» Same for command line?

- Yes, you need to use the appropriate switches...

# Merging Data

```
root@kali:~/Desktop# mergecap -h
Mergcap 1.10.2 (SVN Rev 51934 from /trunk-1.10)
Merge two or more capture files into one.
See http://www.wireshark.org for more information.

Usage: mergcap [options] -w <outfile>|- <infile> [<infile> ...]

Output:
  -a                concatenate rather than merge files.
                   default is to merge based on frame timestamps.
  -s <snaplen>      truncate packets to <snaplen> bytes of data.
  -w <outfile>|-    set the output filename to <outfile> or '-' for stdout.
  -F <capture type> set the output file type; default is pcapng.
                   an empty "-F" option will list the file types.
  -T <encap type>   set the output file encapsulation type;
                   default is the same as the first input file.
                   an empty "-T" option will list the encapsulation types.

Miscellaneous:
  -h                display this help and exit.
  -v                verbose output.

root@kali:~/Desktop#
```

# Questions?