

Защита информации в сети

Формат rsar файла

доц. Нестеренко В.А.

Структура *pcap* файла

| |
|-------------------------------|
| Заголовок файла (PCAPFILEHDR) |
| Заголовок пакета (PCAPPKTHDR) |
| Содержимое пакета (EVENT) |
| Заголовок пакета (PCAPPKTHDR) |
| Содержимое пакета (EVENT) |
| ... |

Материалы по лекции

- *main.h* – основной заголовочный файл
- *dump.h* – структура рсар файла и заголовки протоколов.
- *treat_dump.c* – программа обработки рсар файла.
- *anyfunc.c* – обработка события.

Задания для практической работы

- Реализовать рассмотренную программу
- Подсчитать число пакетов для разных протоколов в файле *class_tcodump.pcap*
- Воспроизвести результаты относительно пакетов *syn* и *syn_ack* в файле *class_tcodump.pcap*