ISP RAS

Подходы к представлению результатов анализа сетевого трафика

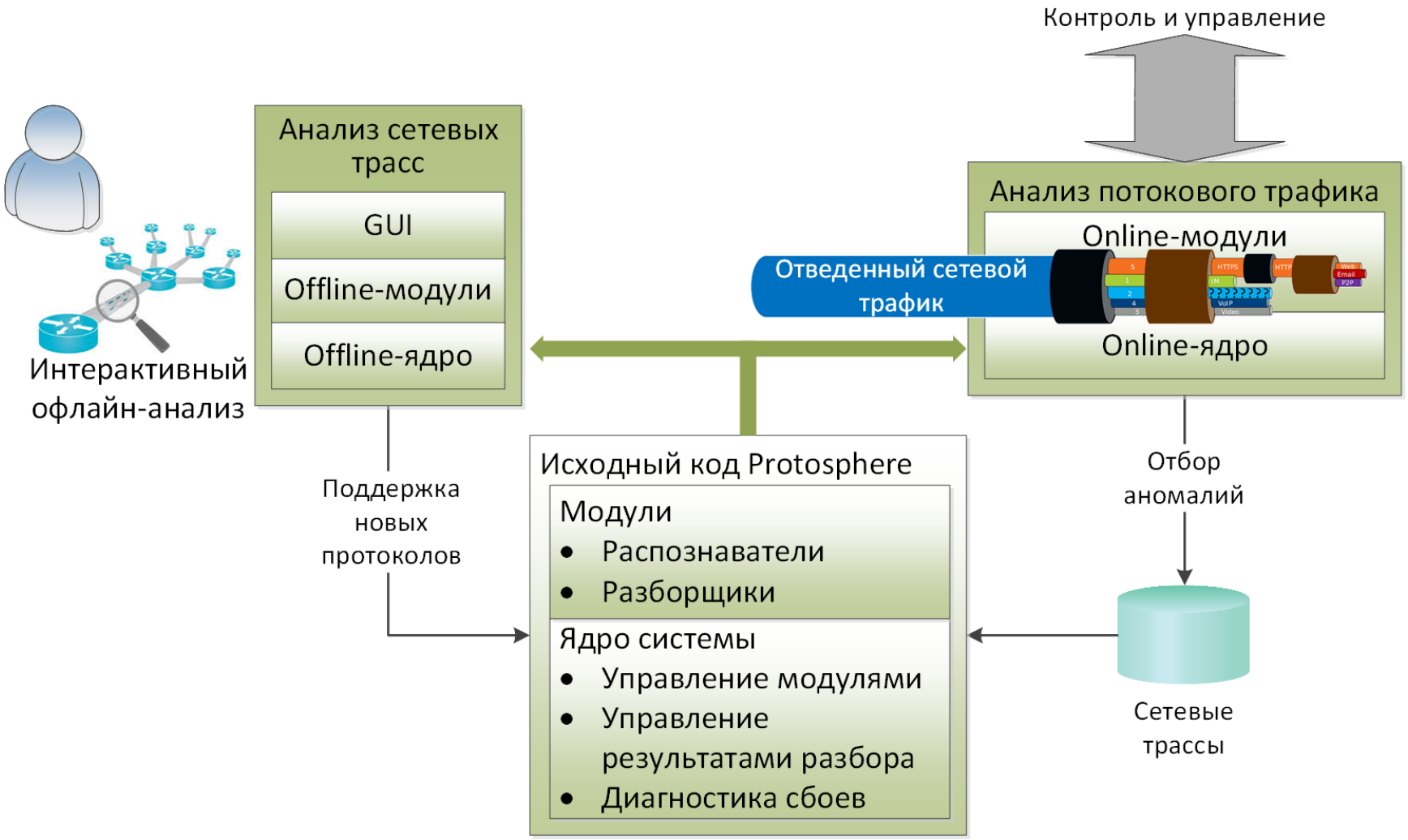
А. И. Гетьман, Ю. В. Маркин, Д. О. Обыденков, В. А. Падарян, А. Ю. Тихонов
{thorin, ustas, obydenkov, vartan, fireboo}@ispras.ru

02.12.2016

Разбор сетевых пакетов

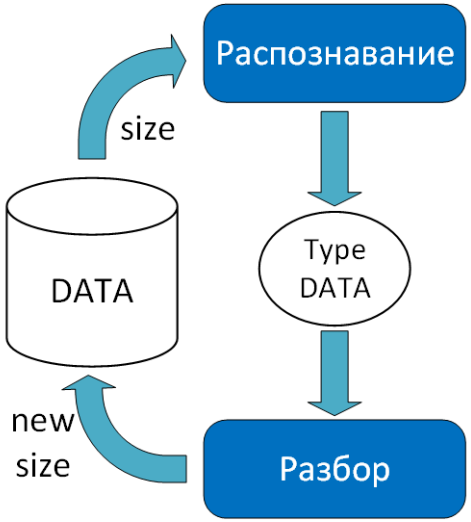
	Online анализ	Offline анализ
Условия анализа	• Ресурсы ограничены • Приоритет – скорость	• Ресурсов достаточно • Приоритет – детализация
Задачи анализа	• Безопасность сети (Firewall, IDS/IPS) • Контроль и обеспечение качества связи (QoS, QoE) • Управление политиками контроля сетевого трафика (PCC, NAC)	• Расследования инцидентов нарушения информационной безопасности • Анализ несоответствий между стандартом протокола и реализацией • Обратная инженерия и отладки сетевых протоколов

Архитектура системы Protosphere



Возможности ядра системы

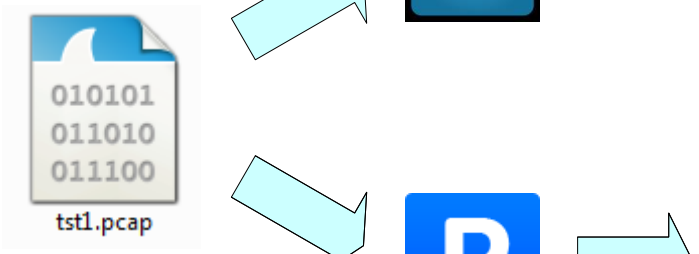
- Сборка сеансов протоколов различного уровня
- Обработка данных, содержащих искажения, потери, перестановки и дублирование пакетов, ассиметричный трафик
- Управление ресурсами для поддержки состояний разбираемых потоков



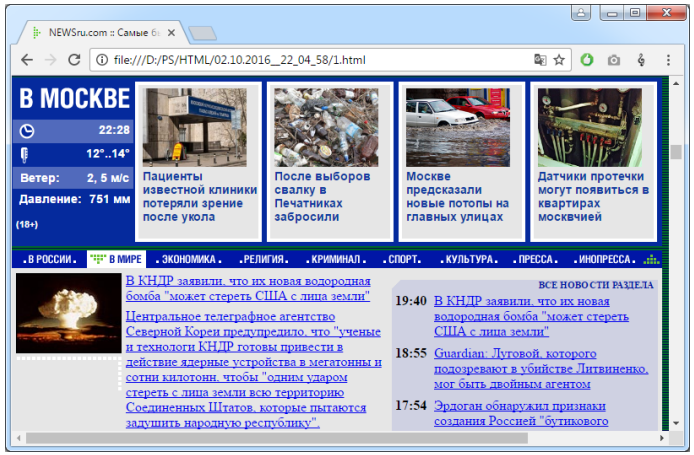
- Поддержка анализа сжатых и шифрованных данных
- Поддержка туннелей произвольной конфигурации
- Извлечение объектов из трафика: видео/аудио потоки, веб-страницы, произвольные файлы и т.д.

Восстановление высокоуровневых данных

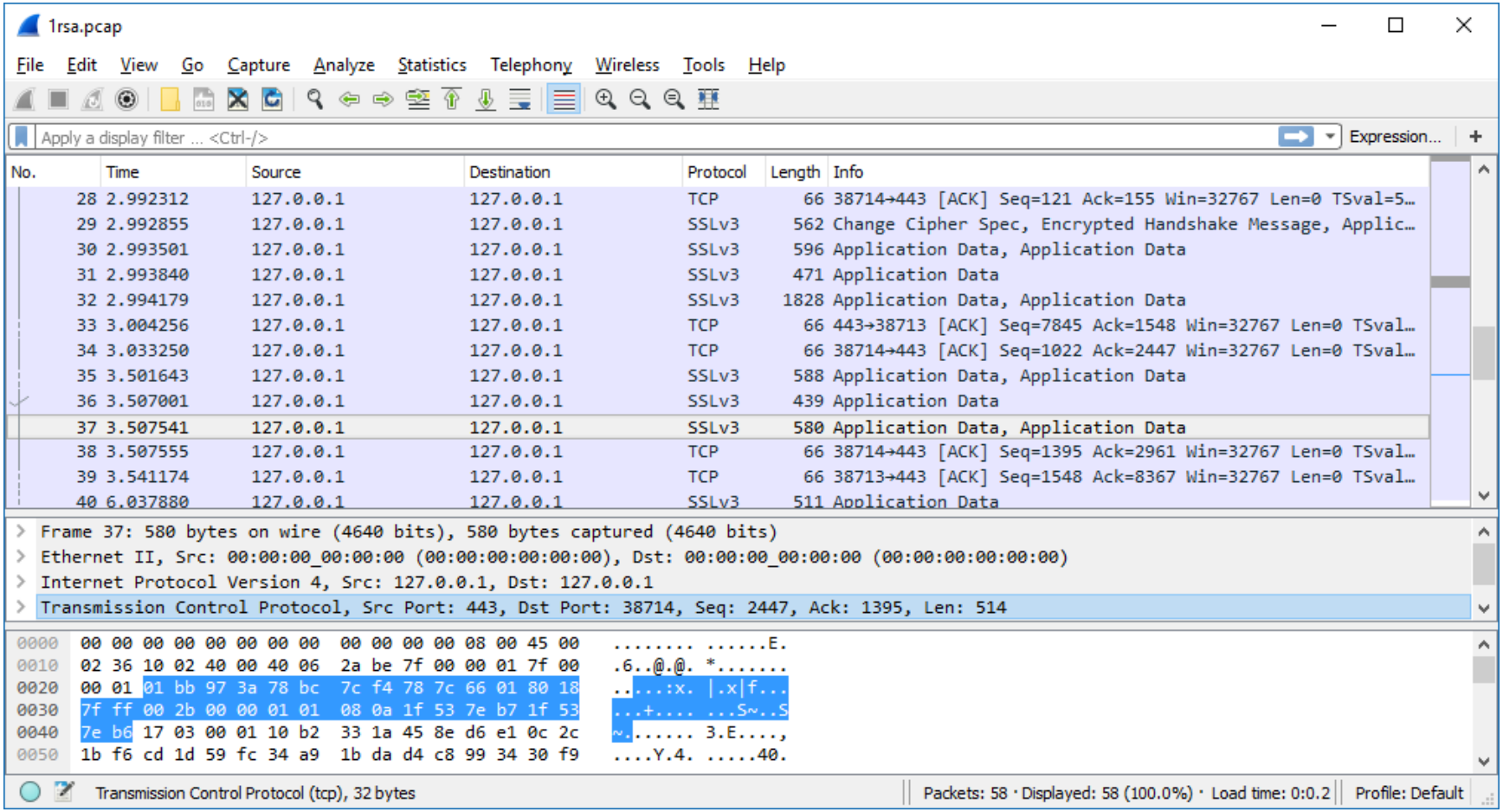
Корректное восстановление TCP-потока при переупорядочивании пакетов



Bug 12006 - desegment_tcp can't defragment PDU if fragments come in wrong order

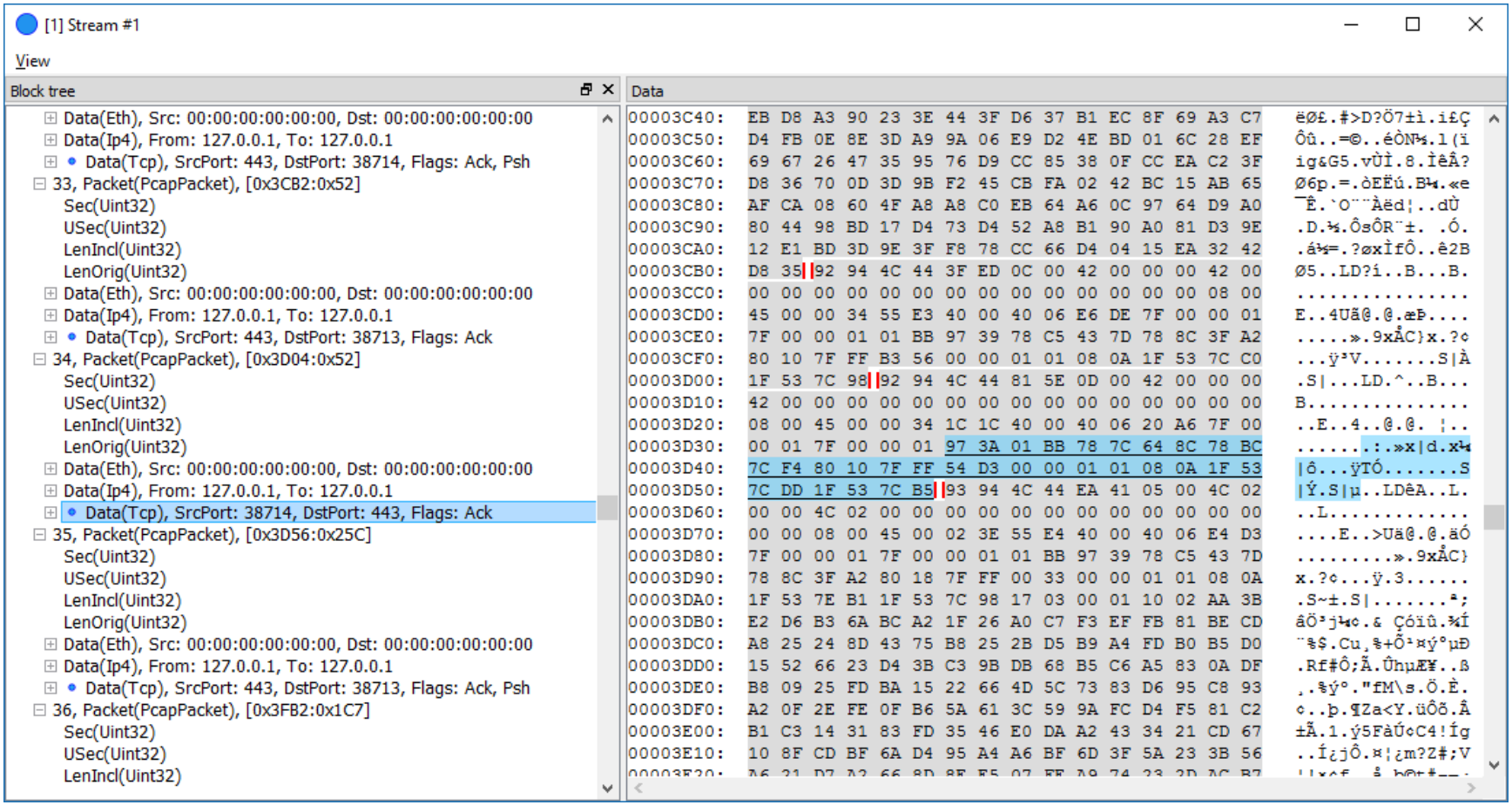


Представление списка сетевых пакетов

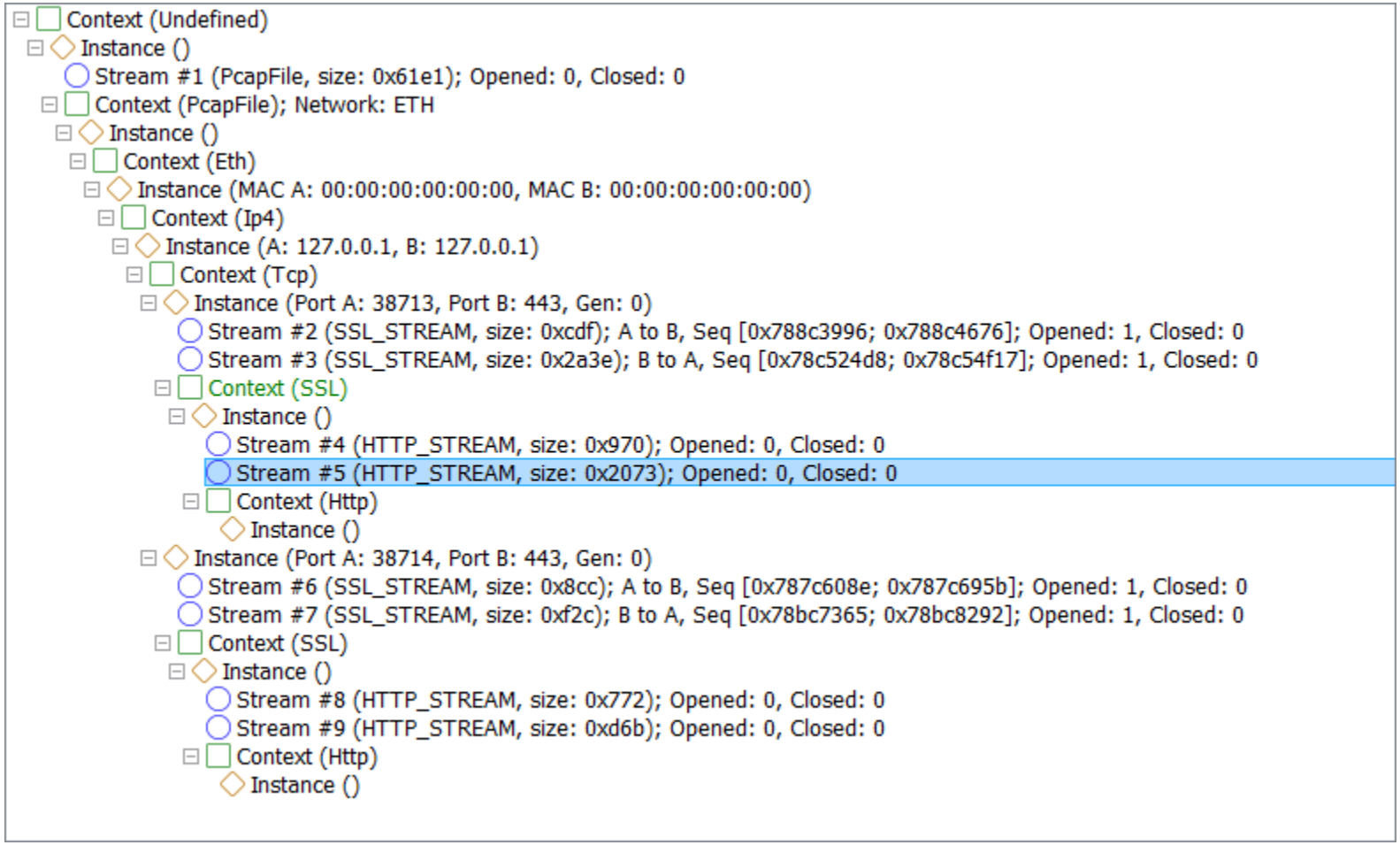


Wireshark

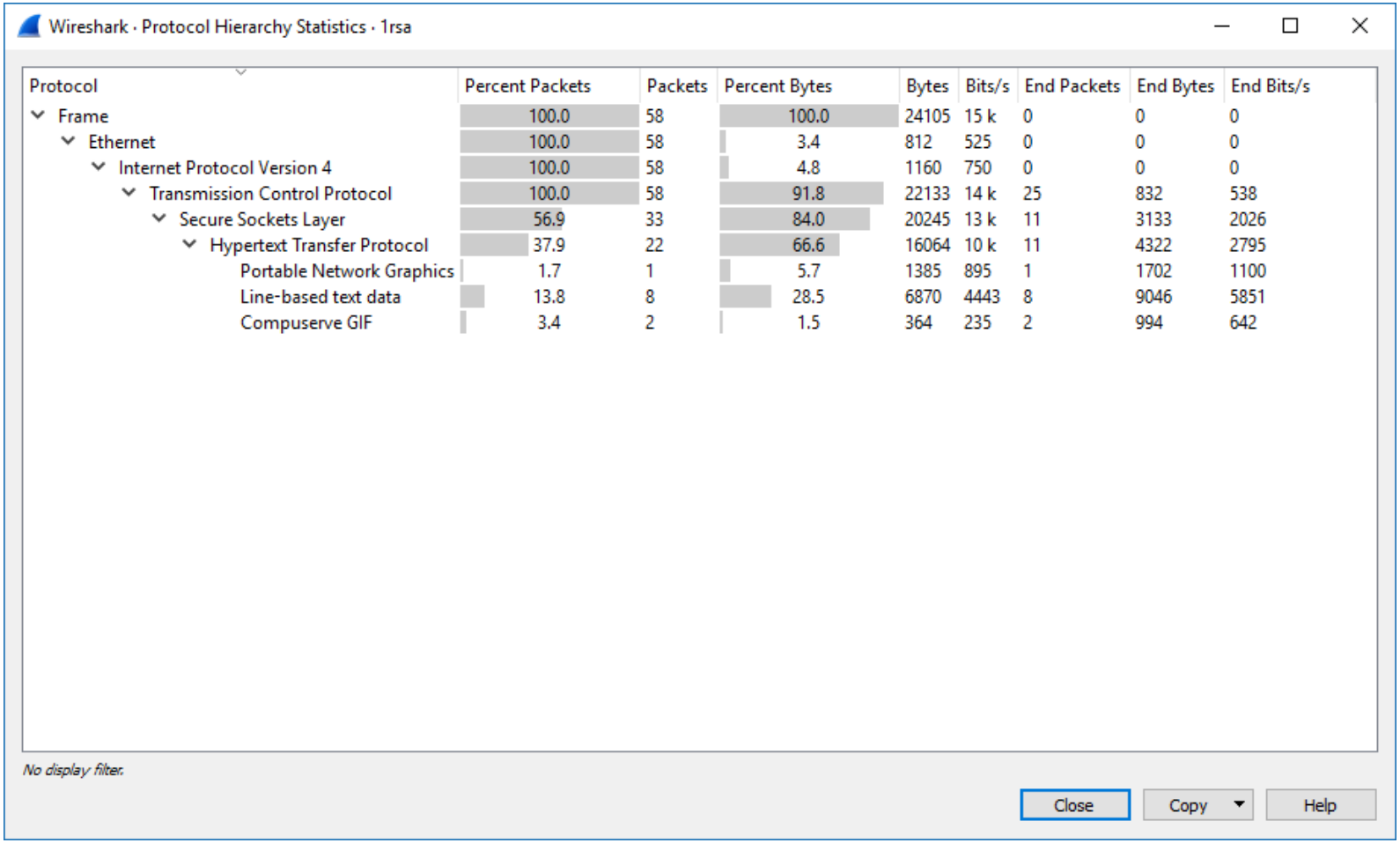
Представление списка сетевых пакетов



Дерево потоков сетевых взаимодействий



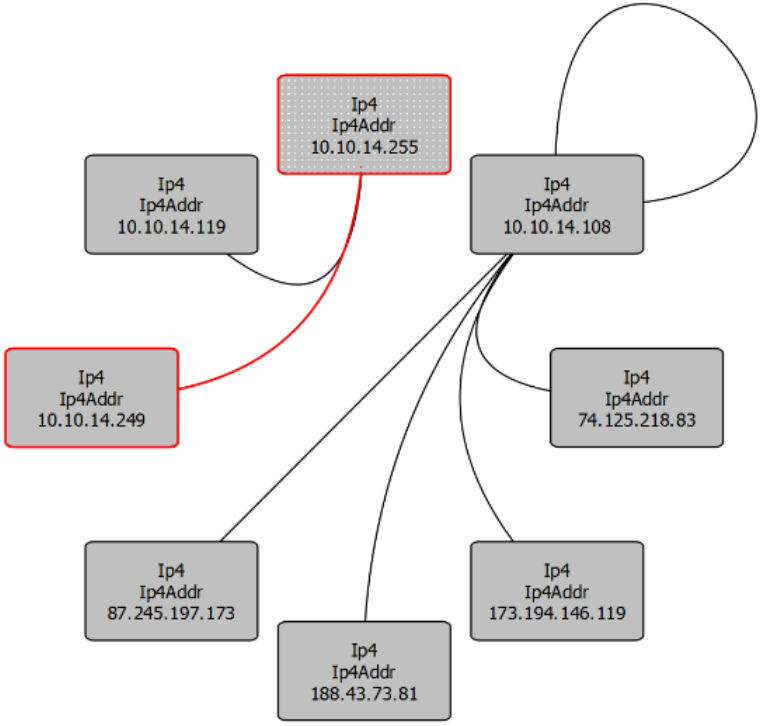
Дерево потоков сетевых взаимодействий



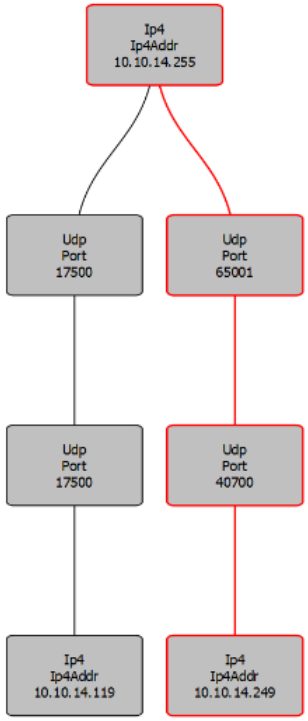
Wireshark

Локализация

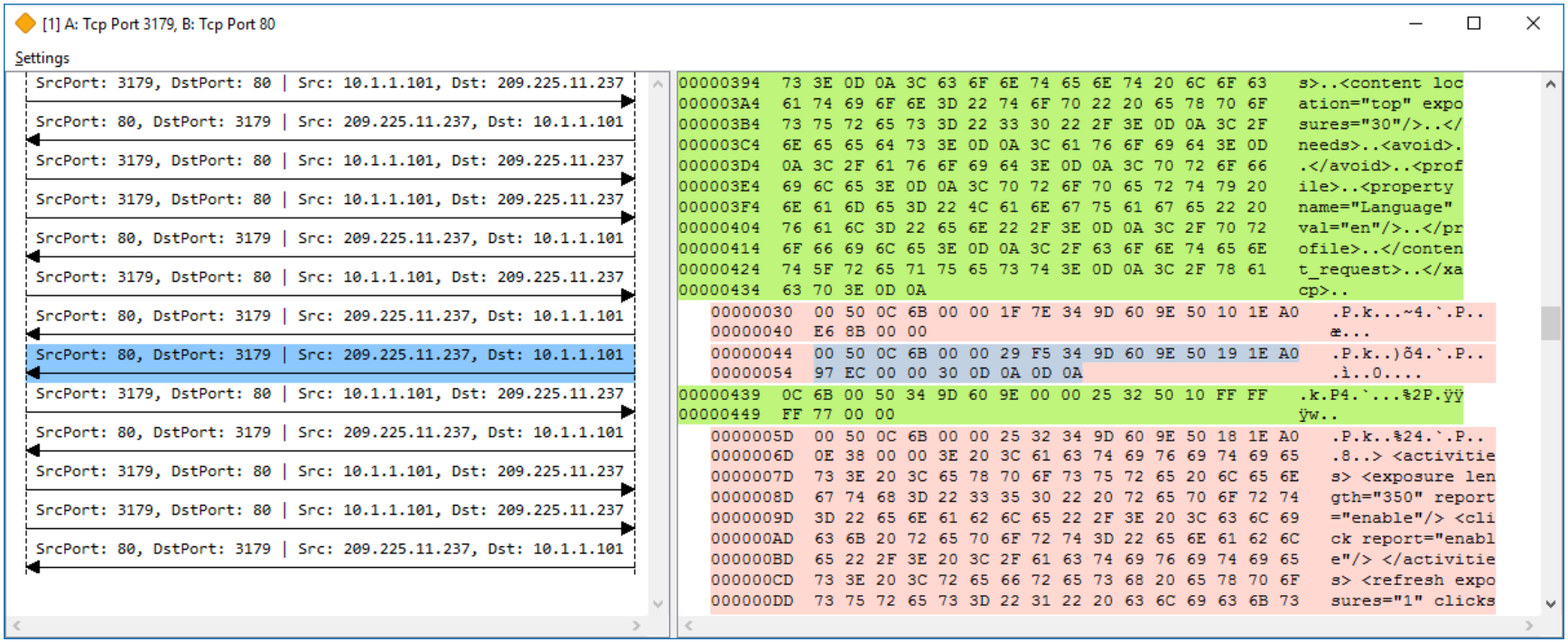
Взаимодействия всех сетевых узлов



Отдельное сетевое соединение

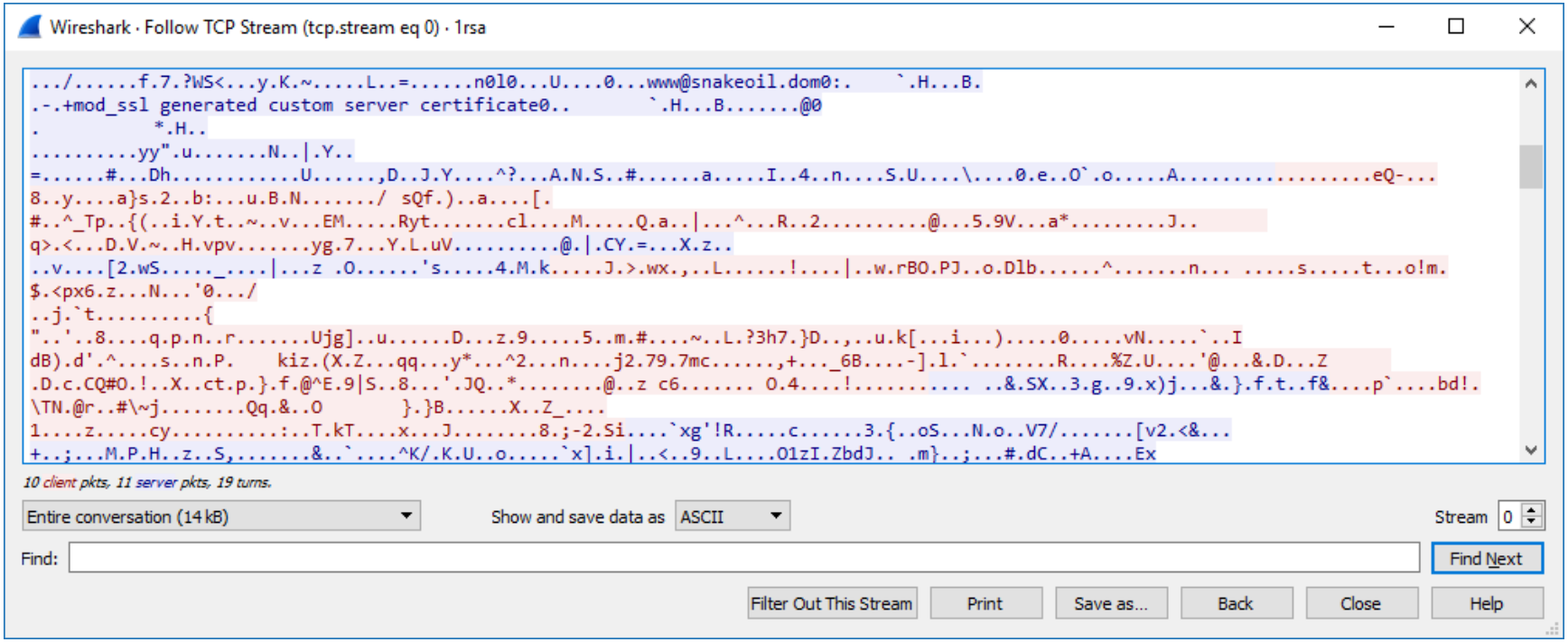


Детализация



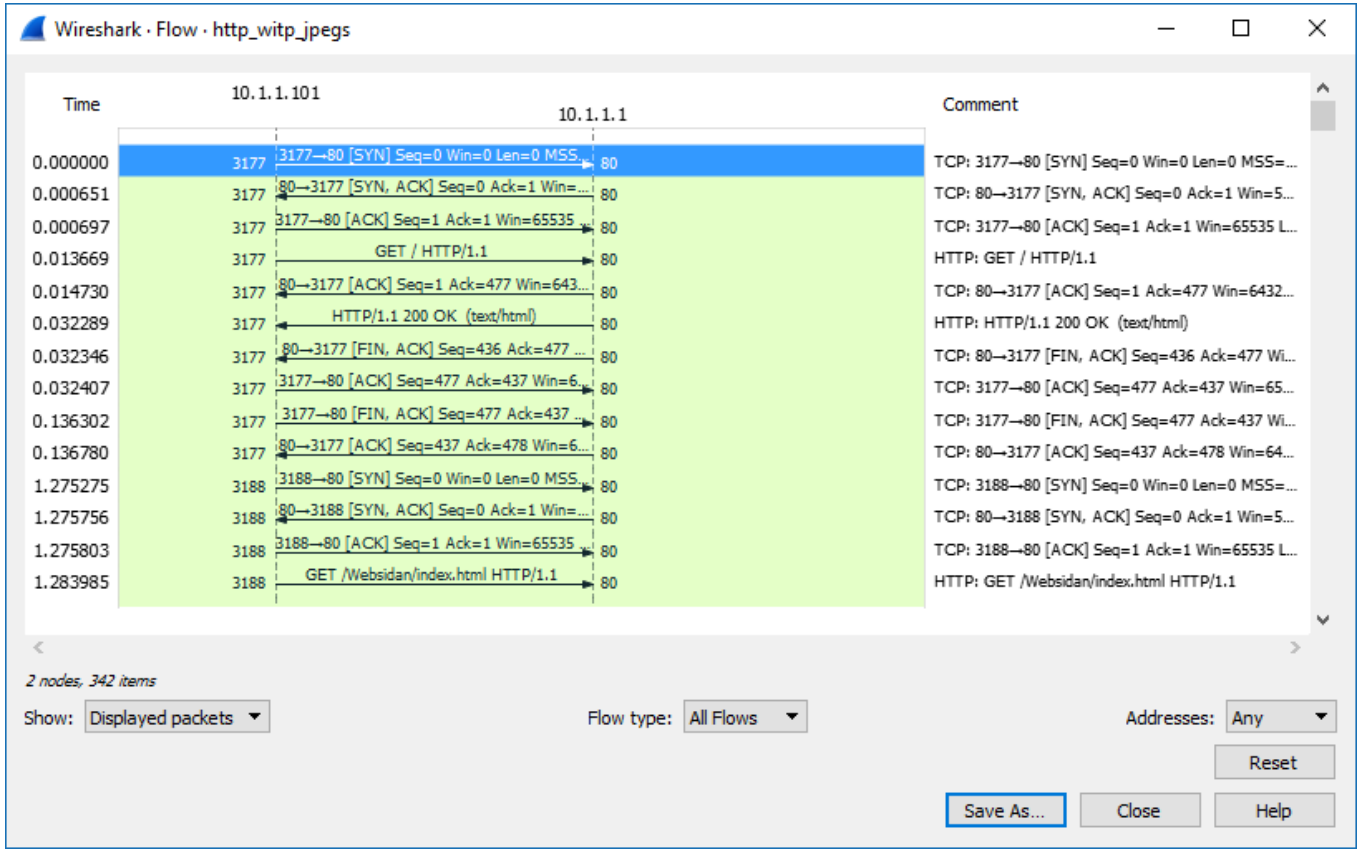
- Последовательность обмена пакетами в рамках отдельного потока протокола произвольного уровня или группы потоков
- Возможность выбора уровня протокола, узлов обмена, выводимых над «стрелками» данных

Детализация



Wireshark
(TCP Stream)

Детализация

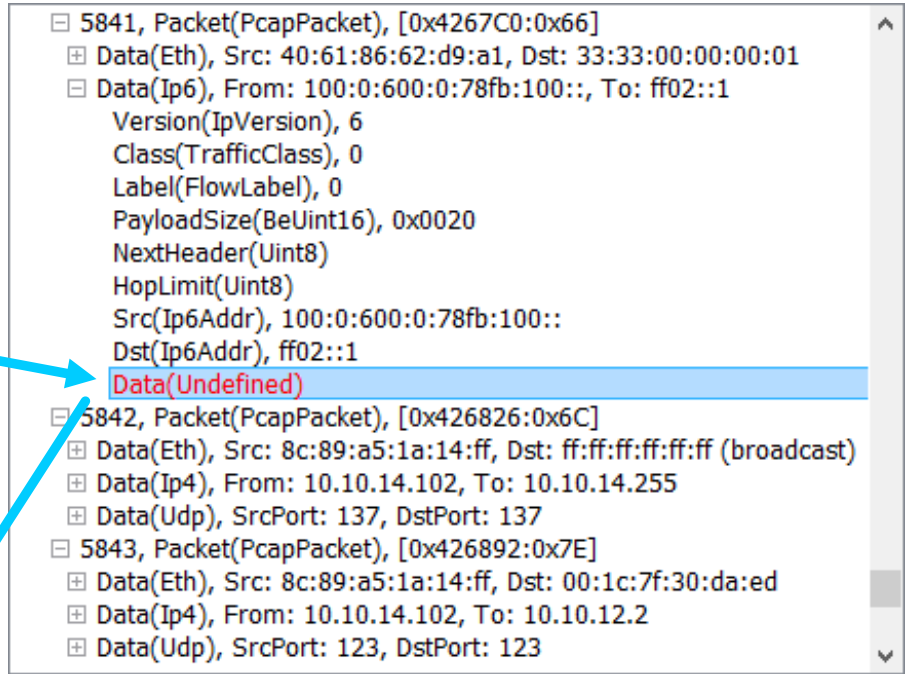


Wireshark
(Flow graph)

Обратная инженерия протоколов
Журнал ошибок

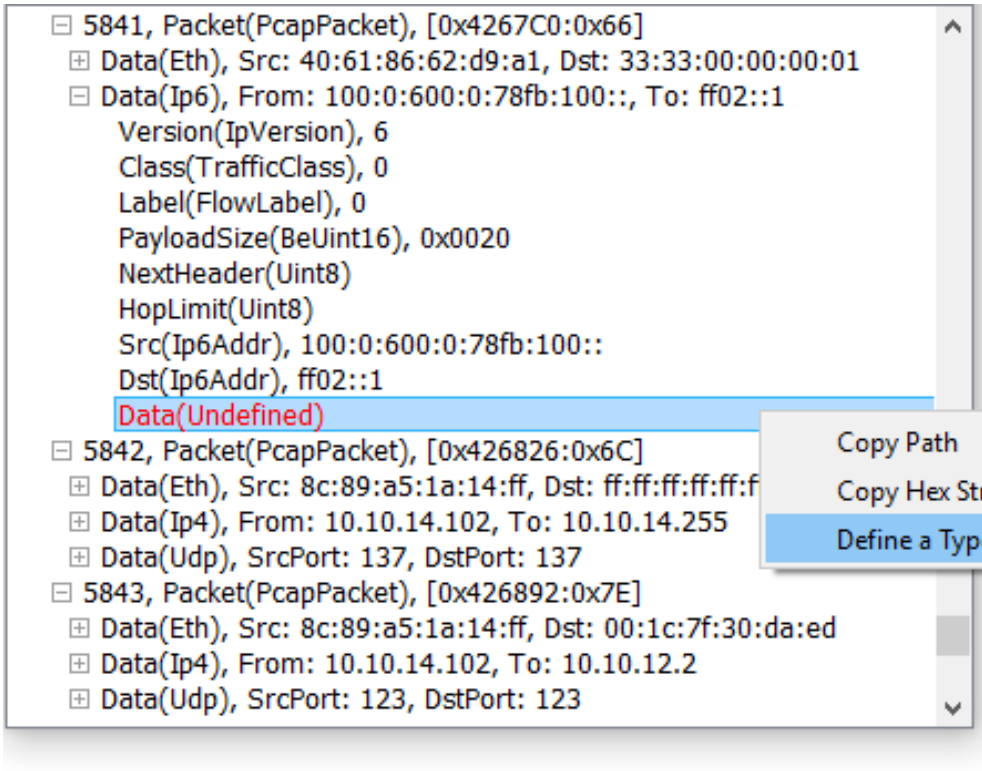
Журнал

Timestamp	Topic	Content
13:29:10.100	HTTP	Found HTTP-client.
13:29:10.100	HTTP	Found HTTP-server.
13:29:10.111	HTTP	Gif file found.
13:29:10.122	EthLog	Can't recognize parse type.
13:29:10.123	IPv4	Can't recognize parse type.
13:29:10.123	IPv6	Unsupported IPv6 next header
13:29:10.123	IPv6	Can't recognize parse type.
13:29:10.149	EthLog	Can't recognize parse type.
13:29:10.382	SSL	Can't decrypt data from server
13:29:10.386	SSL	Can't decrypt data from server

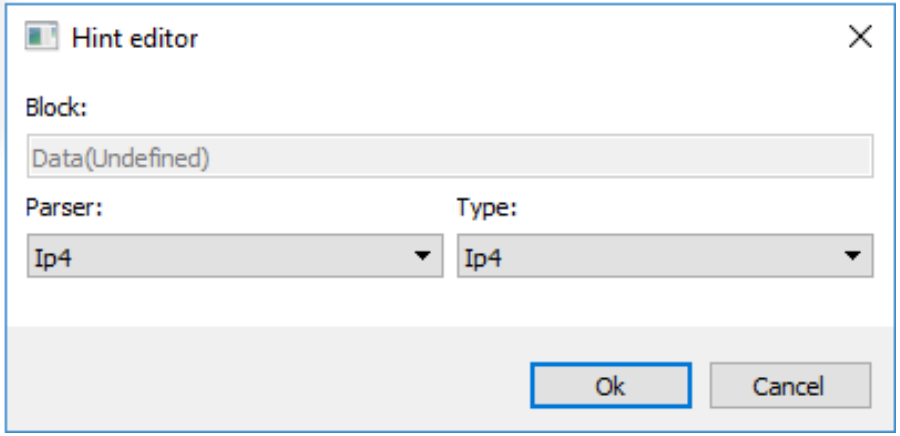



```
004267F0:  01 00 00 00 00 00 FF 02 00 00 00 00 00 00 00 00
00426800:  00 00 00 00 00 01 3A 00 05 02 00 00 00 00 82 00
00426810:  F9 C5 03 E8 00 00 00 00 00 00 00 00 00 00 00 00
00426820:  00 00 00 00 00 00 78 24 D0 50 13 33 0E 00 5C 00
00426830:  00 00 5C 00 00 00 FF FF FF FF FF FF 8C 89 A5 1A
00426840:  14 FF 08 00 45 00 00 4E 22 F4 00 00 80 11 E6 32
00426850:  0A 0A 0E 66 0A 0A 0E FF 00 89 00 89 00 3A F0 86
00426860:  9A FA 01 10 00 01 00 00 00 00 00 00 20 46 48 46
```

Обратная инженерия протоколов
Интерактивный разбор



Система не смогла определить тип разбора



Спасибо за внимание

Буду рад ответить на ваши вопросы