

Подходы к представлению результатов анализа сетевых трафика

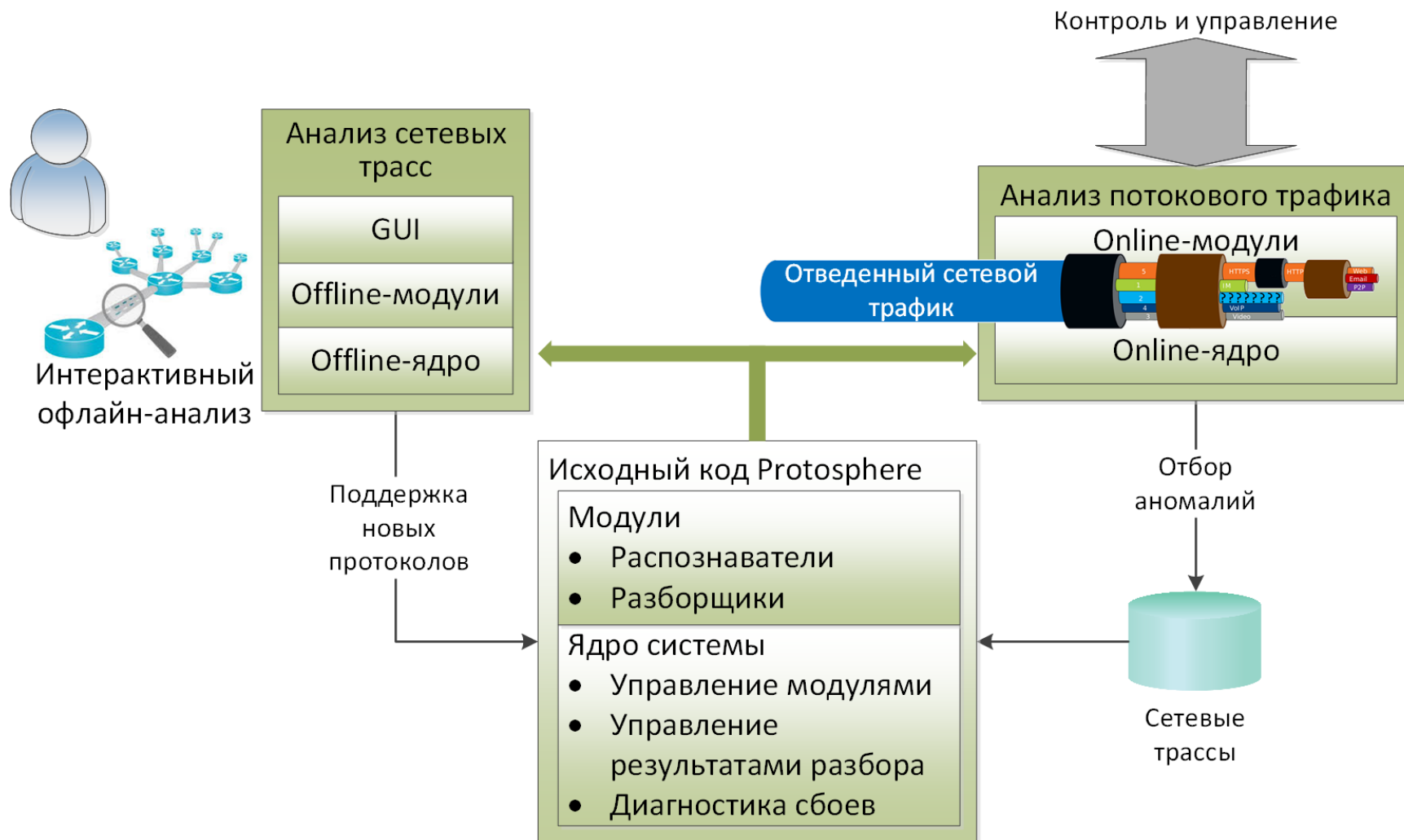
А. И. Гетьман, Ю. В. Маркин, Д. О. Обыденков, В. А. Падарян, А. Ю. Тихонов
{thorin, ustas, obydenkov, vartan, fireboo}@ispras.ru

02.12.2016

Разбор сетевых пакетов

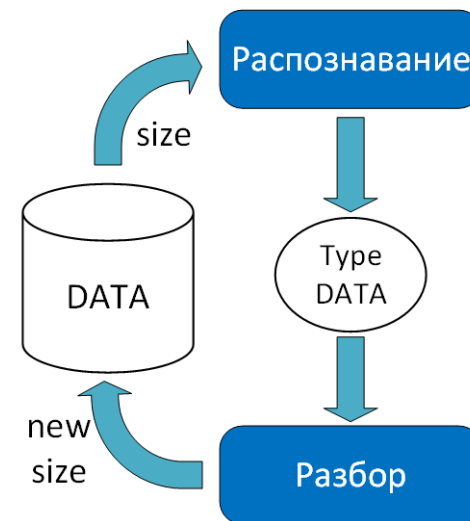
	Online анализ	Offline анализ
Условия анализа	• Ресурсы ограничены • Приоритет – скорость	• Ресурсов достаточно • Приоритет – детализация
Задачи анализа	• Безопасность сети (Firewall, IDS/IPS) • Контроль и обеспечение качества связи (QoS, QoE) • Управление политиками контроля сетевого трафика (PCC, NAC)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

Архитектура системы Protosphere



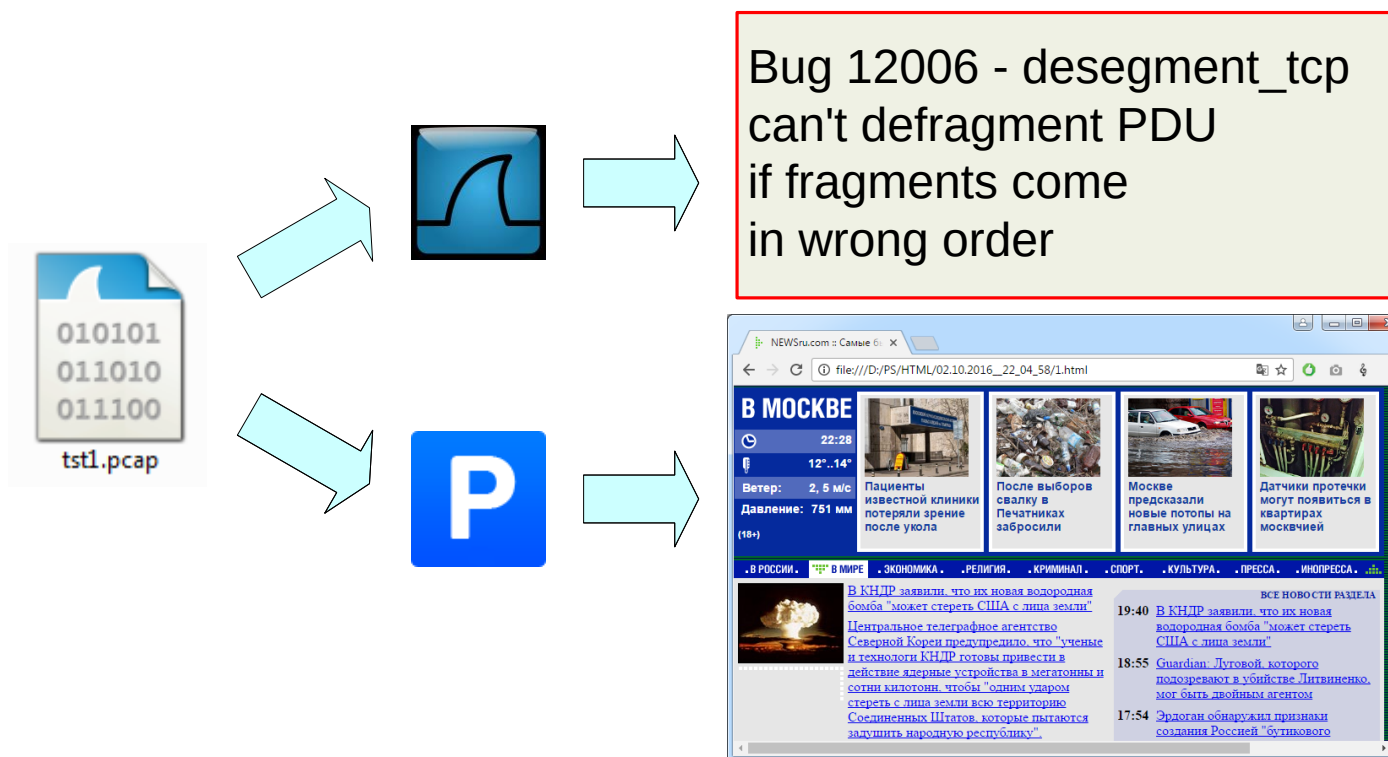
Возможности ядра системы

- Сборка сеансов протоколов различного уровня
- Обработка данных, содержащих искажения, потери, перестановки и дублирование пакетов, асимметричный трафик
- Управление ресурсами для поддержки состояний разбираемых потоков
- Поддержка анализа сжатых и зашифрованных данных
- Поддержка туннелей произвольной конфигурации
- Извлечение объектов из трафика: видео/аудио потоки, веб-страницы, произвольные файлы и т.д.



Восстановление высокоуровневых данных

Корректное восстановление ТСР-потока при переупорядочивании пакетов



Представление списка сетевых пакетов

The image shows the Wireshark network protocol analyzer interface. The main window displays a list of captured packets from a file named '1rsa.pcap'. The packets are filtered by the expression 'Expression...'. The selected packet (No. 37) is a Transmission Control Protocol (TCP) segment, 580 bytes long, sent from 127.0.0.1 to 127.0.0.1. The packet details pane shows the structure of the packet: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
28	2.992312	127.0.0.1	127.0.0.1	TCP	66	38714→443 [ACK] Seq=121 Ack=155 Win=32767 Len=0 TSval=5...
29	2.992855	127.0.0.1	127.0.0.1	SSLv3	562	Change Cipher Spec, Encrypted Handshake Message, Applic...
30	2.993501	127.0.0.1	127.0.0.1	SSLv3	596	Application Data, Application Data
31	2.993840	127.0.0.1	127.0.0.1	SSLv3	471	Application Data
32	2.994179	127.0.0.1	127.0.0.1	SSLv3	1828	Application Data, Application Data
33	3.004256	127.0.0.1	127.0.0.1	TCP	66	443→38713 [ACK] Seq=7845 Ack=1548 Win=32767 Len=0 TSval...
34	3.033250	127.0.0.1	127.0.0.1	TCP	66	38714→443 [ACK] Seq=1022 Ack=2447 Win=32767 Len=0 TSval...
35	3.501643	127.0.0.1	127.0.0.1	SSLv3	588	Application Data, Application Data
36	3.507001	127.0.0.1	127.0.0.1	SSLv3	439	Application Data
37	3.507541	127.0.0.1	127.0.0.1	SSLv3	580	Application Data, Application Data
38	3.507555	127.0.0.1	127.0.0.1	TCP	66	38714→443 [ACK] Seq=1395 Ack=2961 Win=32767 Len=0 TSval...
39	3.541174	127.0.0.1	127.0.0.1	TCP	66	38713→443 [ACK] Seq=1548 Ack=8367 Win=32767 Len=0 TSval...
40	6.037880	127.0.0.1	127.0.0.1	SSLv3	511	Application Data

> Frame 37: 580 bytes on wire (4640 bits), 580 bytes captured (4640 bits)

> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)

> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

> Transmission Control Protocol, Src Port: 443, Dst Port: 38714, Seq: 2447, Ack: 1395, Len: 514

```

0000  00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00  .....E.
0010  02 36 10 02 40 00 40 06 2a be 7f 00 00 01 7f 00  .6..@. *.
0020  00 01 01 bb 97 3a 78 bc 7c f4 78 7c 66 01 80 18  ...:x. |.x|f...
0030  7f ff 00 2b 00 00 01 01 08 0a 1f 53 7e b7 1f 53  ...+.....S~..S
0040  7e b6 17 03 00 01 10 b2 33 1a 45 8e d6 e1 0c 2c  ~.....3.E....,
0050  1b f6 cd 1d 59 fc 34 a9 1b da d4 c8 99 34 30 f9  ....Y.4. ....40.
  
```

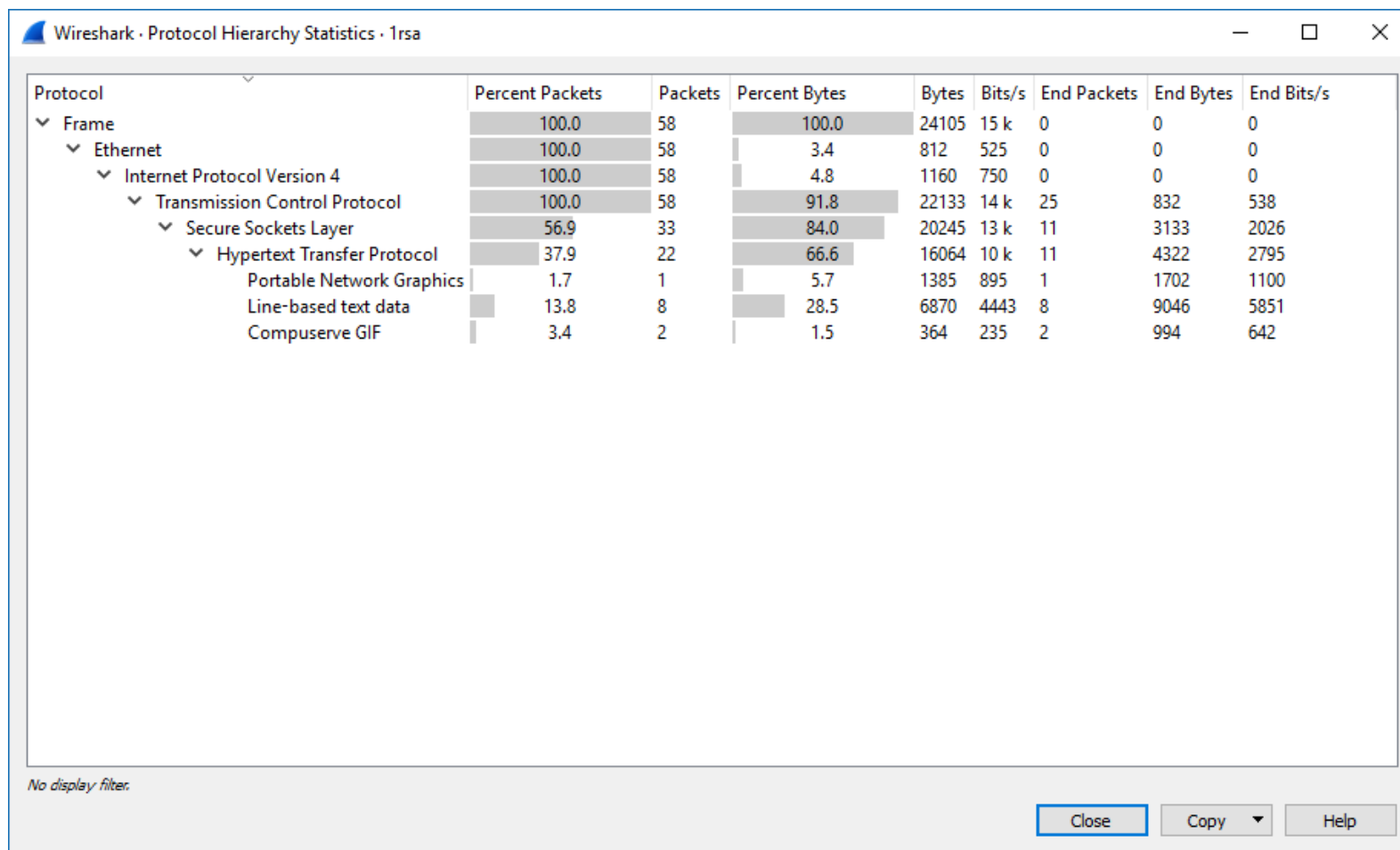
Transmission Control Protocol (tcp), 32 bytes

Packets: 58 · Displayed: 58 (100.0%) · Load time: 0:0.2 | Profile: Default

Wireshark



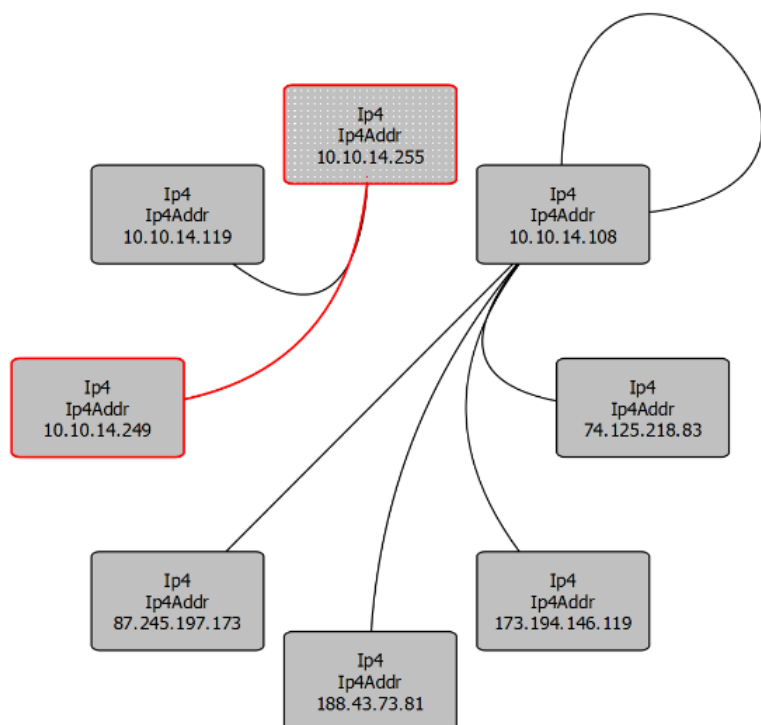
Дерево потоков сетевых взаимодействий



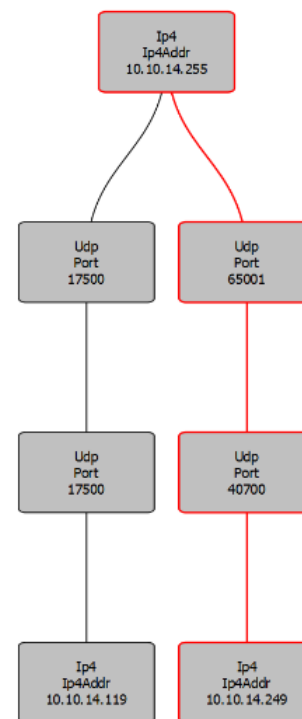
Wireshark

Локализация

Взаимодействия всех сетевых узлов



Отдельное сетевое соединение



Детализация

◆ [1] A: Tcp Port 3179, B: Tcp Port 80

Settings

SrcPort: 3179, DstPort: 80 Src: 10.1.1.101, Dst: 209.225.11.237	00000394 73 3E 0D 0A 3C 63 6F 6E 74 65 6E 74 20 6C 6F 63 s>..<content loc
SrcPort: 80, DstPort: 3179 Src: 209.225.11.237, Dst: 10.1.1.101	000003A4 61 74 69 6F 6E 3D 22 74 6F 70 22 20 65 78 70 6F ation="top" expo
SrcPort: 3179, DstPort: 80 Src: 10.1.1.101, Dst: 209.225.11.237	000003B4 73 75 72 65 73 3D 22 33 30 22 2F 3E 0D 0A 3C 2F sures="30"/>..</
SrcPort: 3179, DstPort: 80 Src: 10.1.1.101, Dst: 209.225.11.237	000003C4 6E 65 65 64 73 3E 0D 0A 3C 61 76 6F 69 64 3E 0D needs>..<avoid>.
SrcPort: 80, DstPort: 3179 Src: 209.225.11.237, Dst: 10.1.1.101	000003D4 0A 3C 2F 61 76 6F 69 64 3E 0D 0A 3C 70 72 6F 66 .</avoid>..<prof
SrcPort: 3179, DstPort: 80 Src: 10.1.1.101, Dst: 209.225.11.237	000003E4 69 6C 65 3E 0D 0A 3C 70 72 6F 70 65 72 74 79 20 ile>..<property
SrcPort: 80, DstPort: 3179 Src: 209.225.11.237, Dst: 10.1.1.101	000003F4 6E 61 6D 65 3D 22 4C 61 6E 67 75 61 67 65 22 20 name="Language"
SrcPort: 3179, DstPort: 80 Src: 10.1.1.101, Dst: 209.225.11.237	00000404 76 61 6C 3D 22 65 6E 22 2F 3E 0D 0A 3C 2F 70 72 val="en"/>..</pr
SrcPort: 80, DstPort: 3179 Src: 209.225.11.237, Dst: 10.1.1.101	00000414 6F 66 69 6C 65 3E 0D 0A 3C 2F 63 6F 6E 74 65 6E ofile>..</conten
SrcPort: 3179, DstPort: 80 Src: 10.1.1.101, Dst: 209.225.11.237	00000424 74 5F 72 65 71 75 65 73 74 3E 0D 0A 3C 2F 78 61 t_request>..</xa
SrcPort: 80, DstPort: 3179 Src: 209.225.11.237, Dst: 10.1.1.101	00000434 63 70 3E 0D 0A cp>..
SrcPort: 3179, DstPort: 80 Src: 10.1.1.101, Dst: 209.225.11.237	00000030 00 50 0C 6B 00 00 1F 7E 34 9D 60 9E 50 10 1E A0 .P.k...~4.`.P..
SrcPort: 80, DstPort: 3179 Src: 209.225.11.237, Dst: 10.1.1.101	00000040 E6 8B 00 00 #...
SrcPort: 3179, DstPort: 80 Src: 10.1.1.101, Dst: 209.225.11.237	00000044 00 50 0C 6B 00 00 29 F5 34 9D 60 9E 50 19 1E A0 .P.k..)ô4.`.P..
SrcPort: 80, DstPort: 3179 Src: 209.225.11.237, Dst: 10.1.1.101	00000054 97 EC 00 00 30 0D 0A 0D 0A .i..0....
SrcPort: 3179, DstPort: 80 Src: 10.1.1.101, Dst: 209.225.11.237	00000439 0C 6B 00 50 34 9D 60 9E 00 00 25 32 50 10 FF FF .k.P4.`...%2P.ÿÿ
SrcPort: 80, DstPort: 3179 Src: 209.225.11.237, Dst: 10.1.1.101	00000449 FF 77 00 00 ýw..
SrcPort: 3179, DstPort: 80 Src: 10.1.1.101, Dst: 209.225.11.237	0000005D 00 50 0C 6B 00 00 25 32 34 9D 60 9E 50 18 1E A0 .P.k...%24.`.P..
SrcPort: 80, DstPort: 3179 Src: 209.225.11.237, Dst: 10.1.1.101	0000006D 0E 38 00 00 3E 20 3C 61 63 74 69 76 69 74 69 65 .8..> <activitie
SrcPort: 3179, DstPort: 80 Src: 10.1.1.101, Dst: 209.225.11.237	0000007D 73 3E 20 3C 65 78 70 6F 73 75 72 65 20 6C 65 6E s> <exposure len
SrcPort: 80, DstPort: 3179 Src: 209.225.11.237, Dst: 10.1.1.101	0000008D 67 74 68 3D 22 33 35 30 22 20 72 65 70 6F 72 74 gth="350" report
SrcPort: 3179, DstPort: 80 Src: 10.1.1.101, Dst: 209.225.11.237	0000009D 3D 22 65 6E 61 62 6C 65 22 2F 3E 20 3C 63 6C 69 ="enable"/> <cli
SrcPort: 80, DstPort: 3179 Src: 209.225.11.237, Dst: 10.1.1.101	000000AD 63 6B 20 72 65 70 6F 72 74 3D 22 65 6E 61 62 6C ck report="enabl
SrcPort: 3179, DstPort: 80 Src: 10.1.1.101, Dst: 209.225.11.237	000000BD 65 22 2F 3E 20 3C 2F 61 63 74 69 76 69 74 69 65 e"/> </activitie
SrcPort: 80, DstPort: 3179 Src: 209.225.11.237, Dst: 10.1.1.101	000000CD 73 3E 20 3C 72 65 66 72 65 73 68 20 65 78 70 6F s> <refresh expo
SrcPort: 3179, DstPort: 80 Src: 10.1.1.101, Dst: 209.225.11.237	000000DD 73 75 72 65 73 3D 22 31 22 20 63 6C 69 63 6B 73 sures="1" clicks

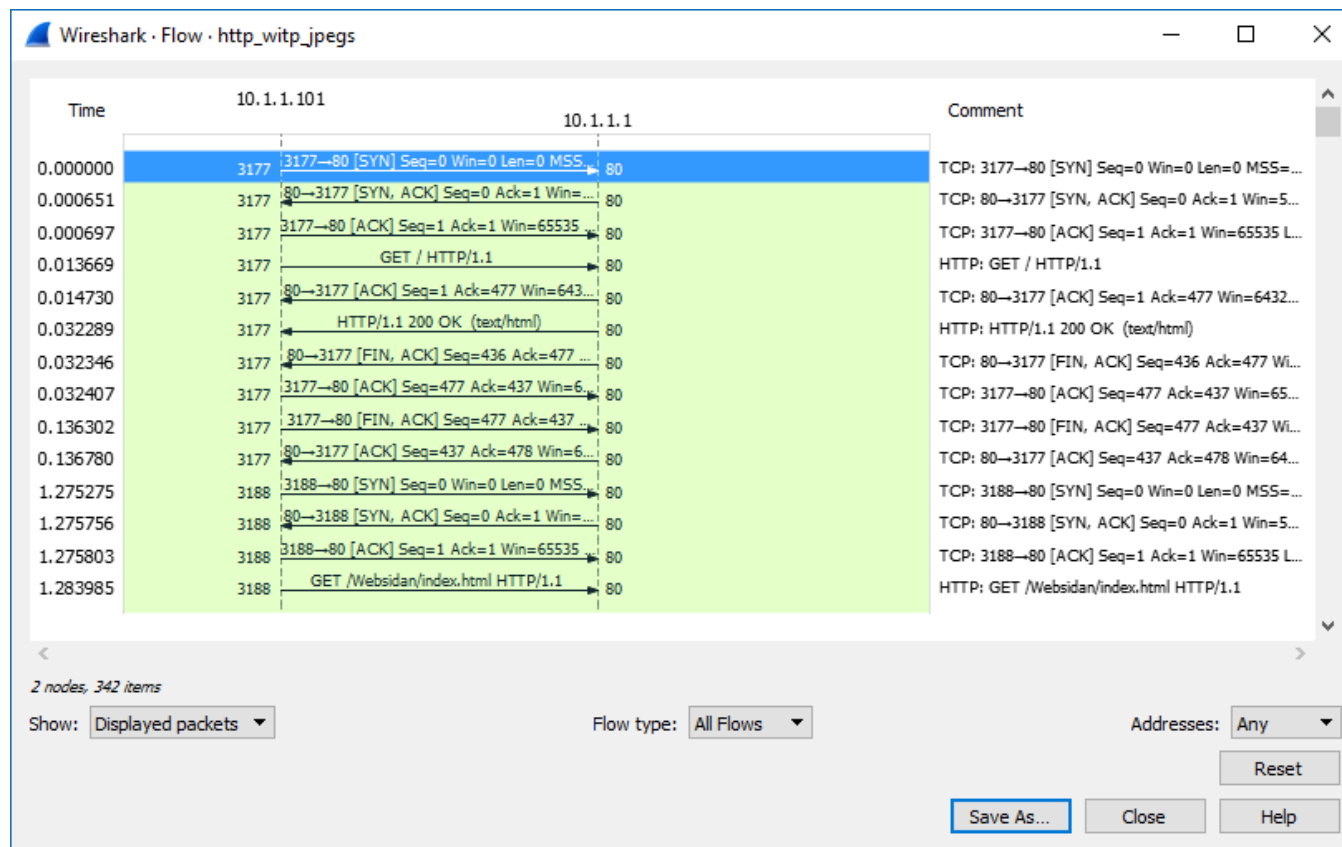
- Последовательность обмена пакетами в рамках отдельного потока протокола произвольного уровня или группы потоков
- Возможность выбора уровня протокола, узлов обмена, выводимых над «стрелками» данных

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

5841, Packet(PcapPacket), [0x4267C0:0x66]
Data(Eth), Src: 40:61:86:62:d9:a1, Dst: 33:33:00:00:00:01
Data(Ip6), From: 100:0:600:0:78fb:100::, To: ff02::1
Version(IpVersion), 6
Class(TrafficClass), 0
Label(FlowLabel), 0
PayloadSize(BeUint16), 0x0020
NextHeader(Uint8)
HopLimit(Uint8)
Src(Ip6Addr), 100:0:600:0:78fb:100::
Dst(Ip6Addr), ff02::1
Data(Undefined)
5842, Packet(PcapPacket), [0x426826:0x6C]
Data(Eth), Src: 8c:89:a5:1a:14:ff, Dst: ff:ff:ff:ff:ff:ff (broadcast)
Data(Ip4), From: 10.10.14.102, To: 10.10.14.255
Data(Udp), SrcPort: 137, DstPort: 137
5843, Packet(PcapPacket), [0x426892:0x7E]
Data(Eth), Src: 8c:89:a5:1a:14:ff, Dst: 00:1c:7f:30:da:ed
Data(Ip4), From: 10.10.14.102, To: 10.10.12.2
Data(Udp), SrcPort: 123, DstPort: 123

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

[-] 5841, Packet(PcapPacket), [0x4267C0:0x66]
[+] Data(Eth), Src: 40:61:86:62:d9:a1, Dst: 33:33:00:00:00:01
[-] Data(Ip6), From: 100:0:600:0:78fb:100::, To: ff02::1
 Version(IpVersion), 6
 Class(TrafficClass), 0
 Label(FlowLabel), 0
 PayloadSize(BeUInt16), 0x0020
 NextHeader(UInt8)
 HopLimit(UInt8)
 Src(Ip6Addr), 100:0:600:0:78fb:100::
 Dst(Ip6Addr), ff02::1
 Data(Undefined)
[-] 5842, Packet(PcapPacket), [0x426826:0x6C]
[+] Data(Eth), Src: 8c:89:a5:1a:14:ff, Dst: ff:ff:ff:ff:ff:f
[+] Data(Ip4), From: 10.10.14.102, To: 10.10.14.255
[+] Data(Udp), SrcPort: 137, DstPort: 137
[-] 5843, Packet(PcapPacket), [0x426892:0x7E]
[+] Data(Eth), Src: 8c:89:a5:1a:14:ff, Dst: 00:1c:7f:30:da:ed
[+] Data(Ip4), From: 10.10.14.102, To: 10.10.12.2
[+] Data(Udp), SrcPort: 123, DstPort: 123

Copy Path
Copy Hex String
Define a Type...

Система не смогла
определить тип
разбора

Hint editor

Block:
Data(Undefined)

Parser: Type:
Ip4 Ip4

Ok Cancel

Спасибо за внимание

Буду рад ответить на ваши вопросы