Анализ содержимого Ethernet-кадра

Дунайцев Р.А. (СПбГУТ)

roman.dunaytsev@spbgut.ru

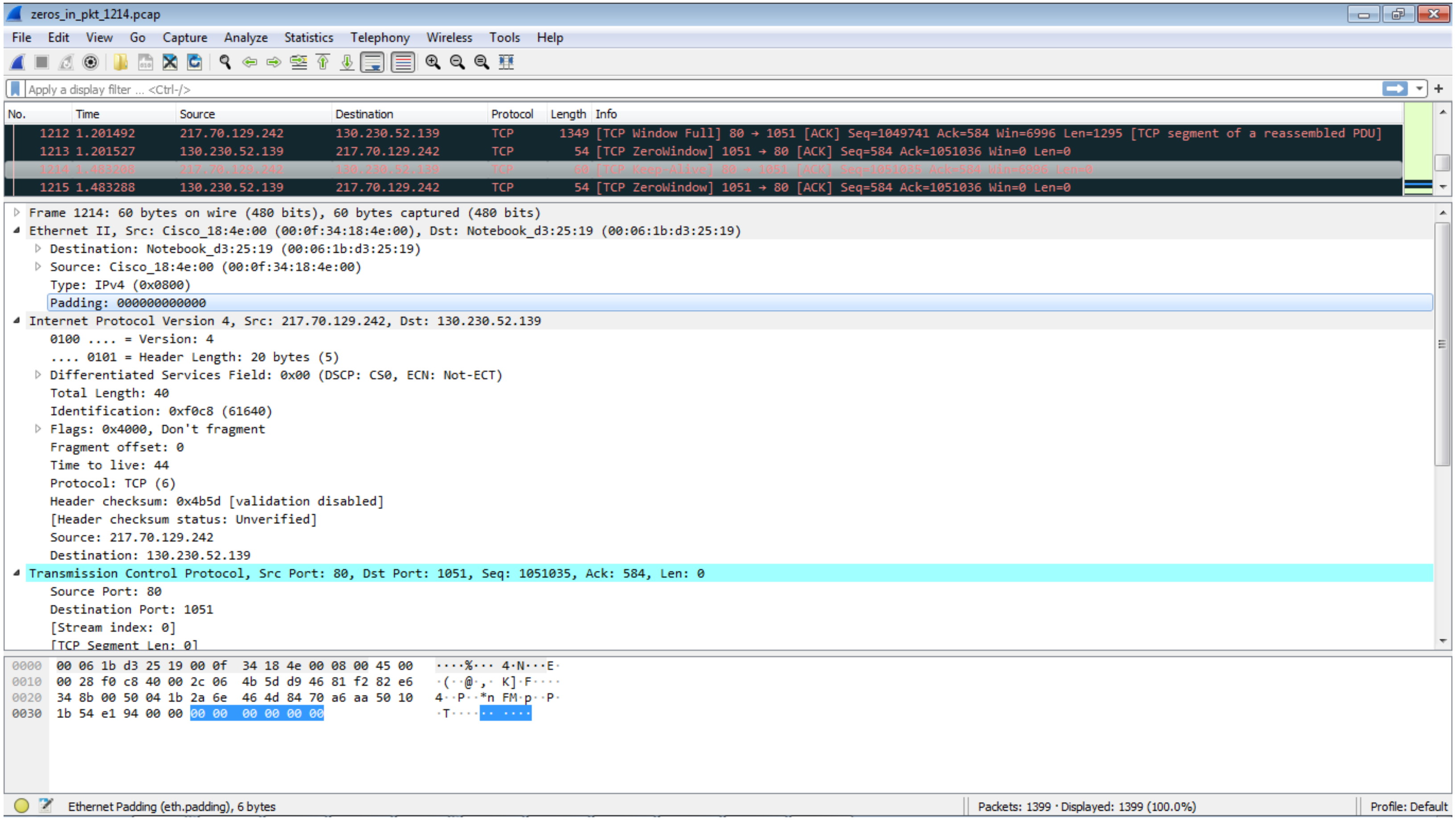
Краткая теоретическая справка

- Откройте файл **zeros_in_pkt_1214.pcap** в Wireshark. Найдите в нем Ethernet-кадр № 1214. В конце этого кадра имеется 6 нулевых байт, которые современные версии Wireshark определяют как Padding, относящийся к Ethernet. Однако так Wireshark эти байты интерпретировал не всегда, да и у других анализаторов трафика мнения по этому поводу расходятся (см. скриншоты далее). Известно, что разные протоколы используют Padding (т.е. заполнение незначащей информацией) с различными целями: для выравнивания по определенной границе, для дополнения до минимального размера и т.п. Кроме того, внутри этого Ethernet-кадра находится пробный TCP-сегмент «Keep-Alive», который также может содержать «one garbage octet» (см. раздел 4.2.3.6):
- https://tools.ietf.org/html/rfc1122
- Так что это за байты и какому протоколу они принадлежат: TCP, IP или Ethernet?

Задание на дом

- Откройте файл **zeros_in_pkt_1214.pcap** в Wireshark. Для Ethernet-кадра № 1214 выполните следующее:
  1) Рассчитайте контрольную сумму TCP, полагая, что 6 нулевых байт в конце принадлежат данному протоколу. Также рассчитайте контрольную сумму TCP, полагая, что 6 нулевых байт в конце НЕ принадлежат ему. Сравните полученные значения с содержимым поля **Checksum**. Какой вариант оказался правильным?
  2) Рассчитайте контрольную сумму заголовка IPv4, полагая, что 6 нулевых байт в конце принадлежат данному протоколу. Также рассчитайте контрольную сумму заголовка IPv4, полагая, что 6 нулевых байт в конце НЕ принадлежат ему. Сравните полученные значения с содержимым поля **Header checksum**. Какой вариант оказался правильным?
  3) Скопируйте содержимое всего кадра как Hex Stream и с помощью сайта https://www.scadacore.com/tools/programming-calculators/online-checksum-calculator/ найдите его **Frame Check Sequence** (см. табл. CRC-32, строка Reversed, столбец Big Endian (ABCD)). Сравните со значением FCS на скриншоте для Omnipeek 11 (FCS: 0xF4DA3A02 Calculated)
- Отчет должен содержать выполненные расчеты, а также выводы о том, какой протокол вставил эти 6 нулевых байт, с какой целью и встречаются ли они в других Ethernet-кадрах этого файла

Wireshark 3.2.3: Padding ☺


zeros_in_pkt_1214.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time      Source          Destination     Protocol Length Info
 1212 1.201492  217.70.129.242  130.230.52.139  TCP      1349 [TCP Window Full] 80 → 1051 [ACK] Seq=1049741 Ack=584 Win=6996 Len=1295 [TCP segment of a reassembled PDU]
 1213 1.201527  130.230.52.139  217.70.129.242  TCP        54 [TCP ZeroWindow] 1051 → 80 [ACK] Seq=584 Ack=1051036 Win=0 Len=0
 1214 1.483208  217.70.129.242  130.230.52.139  TCP        60 [TCP Keep-Alive] 80 → 1051 [ACK] Seq=1051035 Ack=584 Win=6996 Len=0
 1215 1.483288  130.230.52.139  217.70.129.242  TCP        54 [TCP ZeroWindow] 1051 → 80 [ACK] Seq=584 Ack=1051036 Win=0 Len=0
```

```
▷ Frame 1214: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
◢ Ethernet II, Src: Cisco_18:4e:00 (00:0f:34:18:4e:00), Dst: Notebook_d3:25:19 (00:06:1b:d3:25:19)
   ▷ Destination: Notebook_d3:25:19 (00:06:1b:d3:25:19)
   ▷ Source: Cisco_18:4e:00 (00:0f:34:18:4e:00)
     Type: IPv4 (0x0800)
     Padding: 000000000000
◢ Internet Protocol Version 4, Src: 217.70.129.242, Dst: 130.230.52.139
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   ▷ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 40
     Identification: 0xf0c8 (61640)
   ▷ Flags: 0x4000, Don't fragment
     Fragment offset: 0
     Time to live: 44
     Protocol: TCP (6)
     Header checksum: 0x4b5d [validation disabled]
     [Header checksum status: Unverified]
     Source: 217.70.129.242
     Destination: 130.230.52.139
◢ Transmission Control Protocol, Src Port: 80, Dst Port: 1051, Seq: 1051035, Ack: 584, Len: 0
     Source Port: 80
     Destination Port: 1051
     [Stream index: 0]
     [TCP Segment Len: 0]
```

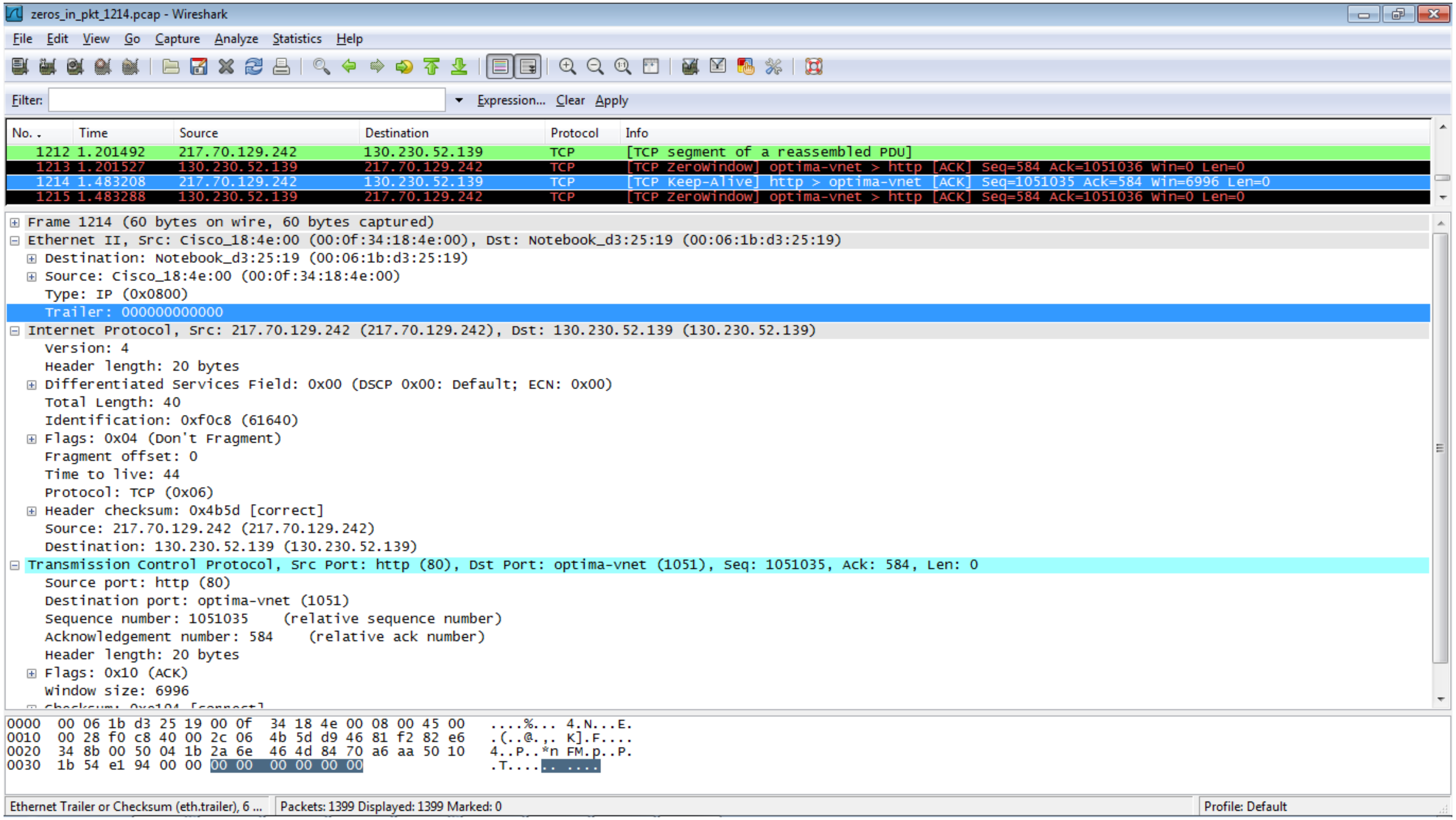
```
0000  00 06 1b d3 25 19 00 0f  34 18 4e 00 08 00 45 00   ····%··· 4·N···E·
0010  00 28 f0 c8 40 00 2c 06  4b 5d d9 46 81 f2 82 e6   ·(··@·,· K]·F····
0020  34 8b 00 50 04 1b 2a 6e  46 4d 84 70 a6 aa 50 10   4··P··*n FM·p··P·
0030  1b 54 e1 94 00 00 00 00  00 00 00 00               ·T······ ····
```

Ethernet Padding (eth.padding), 6 bytes

Packets: 1399 · Displayed: 1399 (100.0%)

Profile: Default

Wireshark 0.99.8: Trailer ☹


zeros_in_pkt_1214.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

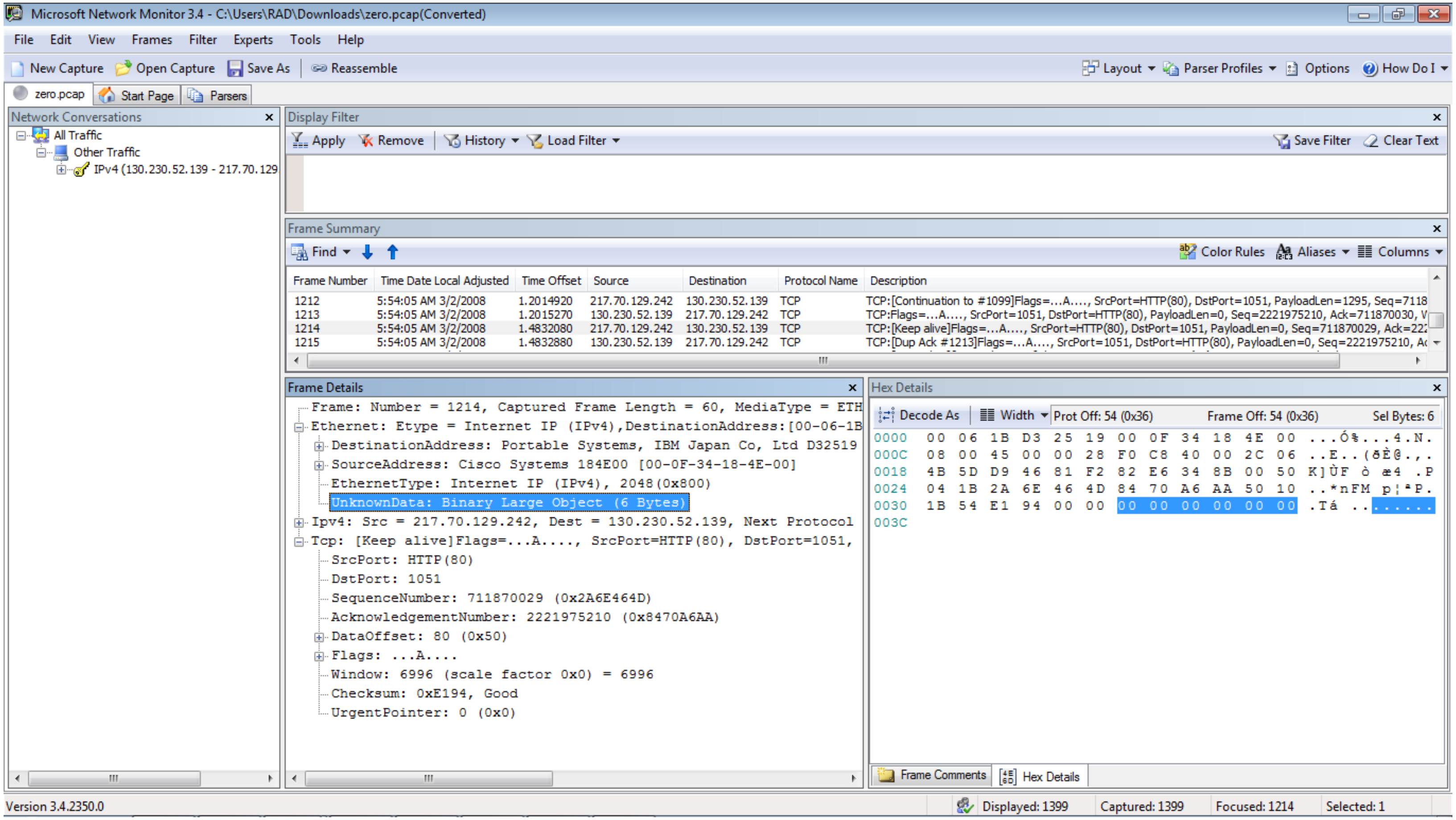
```
No. .   Time      Source           Destination      Protocol  Info
 1212 1.201492   217.70.129.242   130.230.52.139   TCP       [TCP segment of a reassembled PDU]
 1213 1.201527   130.230.52.139   217.70.129.242   TCP       [TCP ZeroWindow] optima-vnet > http [ACK] Seq=584 Ack=1051036 Win=0 Len=0
 1214 1.483208   217.70.129.242   130.230.52.139   TCP       [TCP Keep-Alive] http > optima-vnet [ACK] Seq=1051035 Ack=584 Win=6996 Len=0
 1215 1.483288   130.230.52.139   217.70.129.242   TCP       [TCP ZeroWindow] optima-vnet > http [ACK] Seq=584 Ack=1051036 Win=0 Len=0
```

```
⊞ Frame 1214 (60 bytes on wire, 60 bytes captured)
⊟ Ethernet II, Src: Cisco_18:4e:00 (00:0f:34:18:4e:00), Dst: Notebook_d3:25:19 (00:06:1b:d3:25:19)
  ⊞ Destination: Notebook_d3:25:19 (00:06:1b:d3:25:19)
  ⊞ Source: Cisco_18:4e:00 (00:0f:34:18:4e:00)
    Type: IP (0x0800)
    Trailer: 000000000000
⊟ Internet Protocol, Src: 217.70.129.242 (217.70.129.242), Dst: 130.230.52.139 (130.230.52.139)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 40
    Identification: 0xf0c8 (61640)
  ⊞ Flags: 0x04 (Don't Fragment)
    Fragment offset: 0
    Time to live: 44
    Protocol: TCP (0x06)
  ⊞ Header checksum: 0x4b5d [correct]
    Source: 217.70.129.242 (217.70.129.242)
    Destination: 130.230.52.139 (130.230.52.139)
⊟ Transmission Control Protocol, Src Port: http (80), Dst Port: optima-vnet (1051), Seq: 1051035, Ack: 584, Len: 0
    Source port: http (80)
    Destination port: optima-vnet (1051)
    Sequence number: 1051035    (relative sequence number)
    Acknowledgement number: 584    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x10 (ACK)
    Window size: 6996
  ⊞ Checksum: 0xe104 [correct]
```

```
0000  00 06 1b d3 25 19 00 0f  34 18 4e 00 08 00 45 00   ....%... 4.N...E.
0010  00 28 f0 c8 40 00 2c 06  4b 5d d9 46 81 f2 82 e6   .(..@.,. K].F....
0020  34 8b 00 50 04 1b 2a 6e  46 4d 84 70 a6 aa 50 10   4..P..*n FM.p..P.
0030  1b 54 e1 94 00 00 00 00  00 00 00 00               .T...... ....
```

Ethernet Trailer or Checksum (eth.trailer), 6 ... | Packets: 1399 Displayed: 1399 Marked: 0 | Profile: Default

Network Monitor 3.4: Unknown



Frame Number	Time Date Local Adjusted	Time Offset	Source	Destination	Protocol Name	Description
1212	5:54:05 AM 3/2/2008	1.2014920	217.70.129.242	130.230.52.139	TCP	TCP:[Continuation to #1099]Flags=...A...., SrcPort=HTTP(80), DstPort=1051, PayloadLen=1295, Seq=7118
1213	5:54:05 AM 3/2/2008	1.2015270	130.230.52.139	217.70.129.242	TCP	TCP:Flags=...A...., SrcPort=1051, DstPort=HTTP(80), PayloadLen=0, Seq=2221975210, Ack=711870030, V
1214	5:54:05 AM 3/2/2008	1.4832080	217.70.129.242	130.230.52.139	TCP	TCP:[Keep alive]Flags=...A...., SrcPort=HTTP(80), DstPort=1051, PayloadLen=0, Seq=711870029, Ack=222
1215	5:54:05 AM 3/2/2008	1.4832880	130.230.52.139	217.70.129.242	TCP	TCP:[Dup Ack #1213]Flags=...A...., SrcPort=1051, DstPort=HTTP(80), PayloadLen=0, Seq=2221975210, Ac

Frame Details

```
Frame: Number = 1214, Captured Frame Length = 60, MediaType = ETH
Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[00-06-1B
  DestinationAddress: Portable Systems, IBM Japan Co, Ltd D32519
  SourceAddress: Cisco Systems 184E00 [00-0F-34-18-4E-00]
  EthernetType: Internet IP (IPv4), 2048(0x800)
  UnknownData: Binary Large Object (6 Bytes)
Ipv4: Src = 217.70.129.242, Dest = 130.230.52.139, Next Protocol
Tcp: [Keep alive]Flags=...A...., SrcPort=HTTP(80), DstPort=1051,
  SrcPort: HTTP(80)
  DstPort: 1051
  SequenceNumber: 711870029 (0x2A6E464D)
  AcknowledgementNumber: 2221975210 (0x8470A6AA)
  DataOffset: 80 (0x50)
  Flags: ...A....
  Window: 6996 (scale factor 0x0) = 6996
  Checksum: 0xE194, Good
  UrgentPointer: 0 (0x0)
```

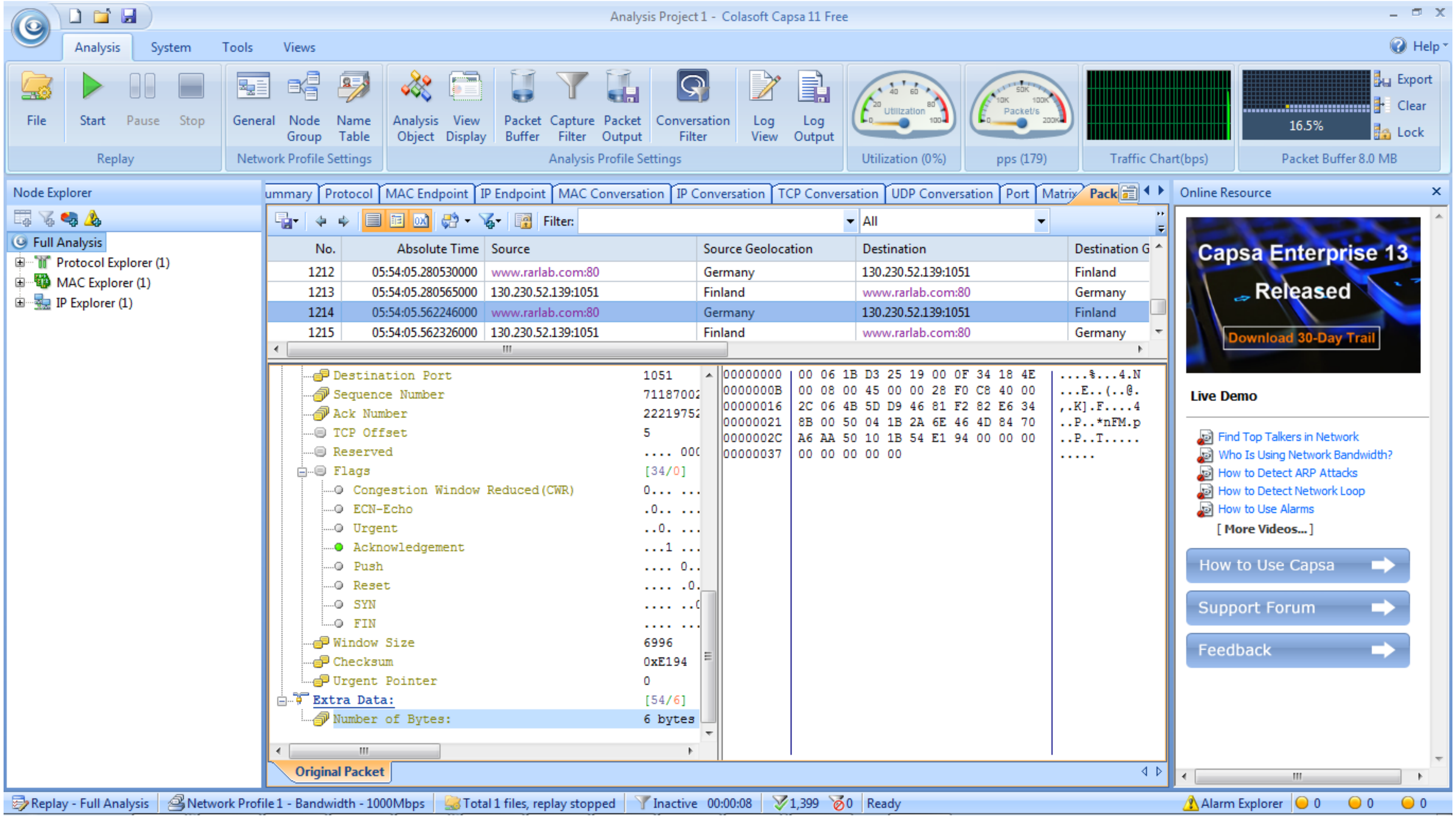
Hex Details

Prot Off: 54 (0x36) Frame Off: 54 (0x36) Sel Bytes: 6

```
0000  00 06 1B D3 25 19 00 0F 34 18 4E 00  ...Ó%...4.N.
000C  08 00 45 00 00 28 F0 C8 40 00 2C 06  ..E..(ðÈ@.,.
0018  4B 5D D9 46 81 F2 82 E6 34 8B 00 50  K]ÙF ò æ4 .P
0024  04 1B 2A 6E 46 4D 84 70 A6 AA 50 10  ..*nFM p¦ªP.
0030  1B 54 E1 94 00 00 00 00 00 00 00 00  .Tá ........
003C
```

Version 3.4.2350.0 Displayed: 1399 Captured: 1399 Focused: 1214 Selected: 1

Colasoft Capsa Free 11.1.2: Extra

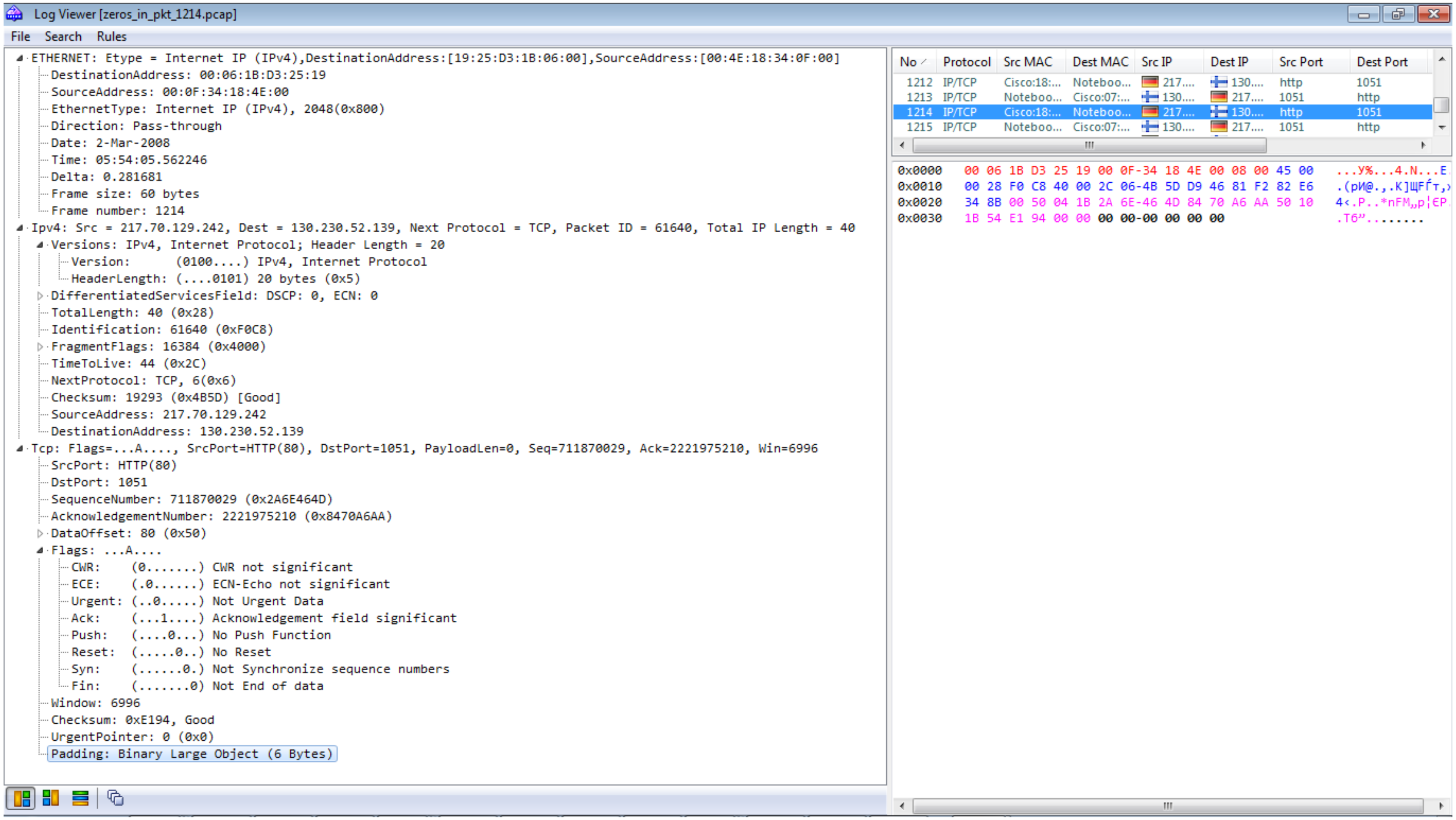


No.	Absolute Time	Source	Source Geolocation	Destination	Destination G
1212	05:54:05.280530000	www.rarlab.com:80	Germany	130.230.52.139:1051	Finland
1213	05:54:05.280565000	130.230.52.139:1051	Finland	www.rarlab.com:80	Germany
1214	05:54:05.562246000	www.rarlab.com:80	Germany	130.230.52.139:1051	Finland
1215	05:54:05.562326000	130.230.52.139:1051	Finland	www.rarlab.com:80	Germany

```
    Destination Port                       1051
    Sequence Number                        71187002
    Ack Number                             22219752
    TCP Offset                             5
    Reserved                               .... 000
  ⊟ Flags                                  [34/0]
      Congestion Window Reduced(CWR)       0... ...
      ECN-Echo                             .0.. ...
      Urgent                               ..0. ...
      Acknowledgement                      ...1 ...
      Push                                 .... 0..
      Reset                                .... .0.
      SYN                                  .... ..0
      FIN                                  .... ...
    Window Size                            6996
    Checksum                               0xE194
    Urgent Pointer                         0
⊟ Extra Data:                              [54/6]
    Number of Bytes:                       6 bytes
```

```
00000000 | 00 06 1B D3 25 19 00 0F 34 18 4E | ....%...4.N
0000000B | 00 08 00 45 00 00 28 F0 C8 40 00 | ...E..(..@.
00000016 | 2C 06 4B 5D D9 46 81 F2 82 E6 34 | ,.K].F....4
00000021 | 8B 00 50 04 1B 2A 6E 46 4D 84 70 | ..P..*nFM.p
0000002C | A6 AA 50 10 1B 54 E1 94 00 00 00 | ..P..T.....
00000037 | 00 00 00 00 00                   | .....
```

TamoSoft CommView 6.5: Padding

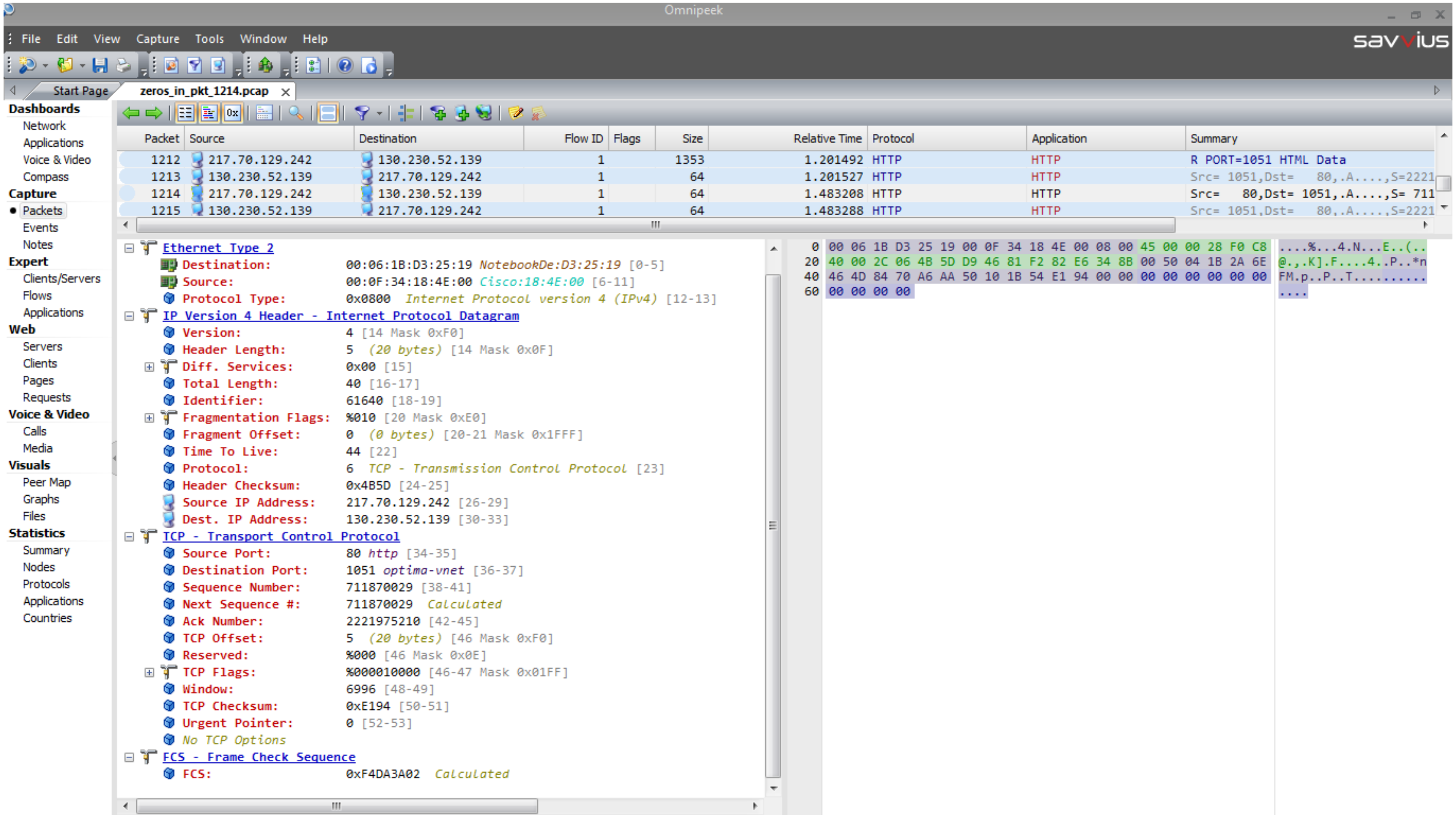


```
ETHERNET: Etype = Internet IP (IPv4),DestinationAddress:[19:25:D3:1B:06:00],SourceAddress:[00:4E:18:34:0F:00]
  DestinationAddress: 00:06:1B:D3:25:19
  SourceAddress: 00:0F:34:18:4E:00
  EthernetType: Internet IP (IPv4), 2048(0x800)
  Direction: Pass-through
  Date: 2-Mar-2008
  Time: 05:54:05.562246
  Delta: 0.281681
  Frame size: 60 bytes
  Frame number: 1214
Ipv4: Src = 217.70.129.242, Dest = 130.230.52.139, Next Protocol = TCP, Packet ID = 61640, Total IP Length = 40
  Versions: IPv4, Internet Protocol; Header Length = 20
    Version:      (0100....) IPv4, Internet Protocol
    HeaderLength: (....0101) 20 bytes (0x5)
  DifferentiatedServicesField: DSCP: 0, ECN: 0
  TotalLength: 40 (0x28)
  Identification: 61640 (0xF0C8)
  FragmentFlags: 16384 (0x4000)
  TimeToLive: 44 (0x2C)
  NextProtocol: TCP, 6(0x6)
  Checksum: 19293 (0x4B5D) [Good]
  SourceAddress: 217.70.129.242
  DestinationAddress: 130.230.52.139
Tcp: Flags=...A...., SrcPort=HTTP(80), DstPort=1051, PayloadLen=0, Seq=711870029, Ack=2221975210, Win=6996
  SrcPort: HTTP(80)
  DstPort: 1051
  SequenceNumber: 711870029 (0x2A6E464D)
  AcknowledgementNumber: 2221975210 (0x8470A6AA)
  DataOffset: 80 (0x50)
  Flags: ...A....
    CWR:    (0.......) CWR not significant
    ECE:    (.0......) ECN-Echo not significant
    Urgent: (..0.....) Not Urgent Data
    Ack:    (...1....) Acknowledgement field significant
    Push:   (....0...) No Push Function
    Reset:  (.....0..) No Reset
    Syn:    (......0.) Not Synchronize sequence numbers
    Fin:    (.......0) Not End of data
  Window: 6996
  Checksum: 0xE194, Good
  UrgentPointer: 0 (0x0)
  Padding: Binary Large Object (6 Bytes)
```

No	Protocol	Src MAC	Dest MAC	Src IP	Dest IP	Src Port	Dest Port
1212	IP/TCP	Cisco:18:...	Noteboo...	217....	130....	http	1051
1213	IP/TCP	Noteboo...	Cisco:07:...	130....	217....	1051	http
1214	IP/TCP	Cisco:18:...	Noteboo...	217....	130....	http	1051
1215	IP/TCP	Noteboo...	Cisco:07:...	130....	217....	1051	http

```
0x0000   00 06 1B D3 25 19 00 0F-34 18 4E 00 08 00 45 00   ...У%...4.N...E.
0x0010   00 28 F0 C8 40 00 2C 06-4B 5D D9 46 81 F2 82 E6   .(рИ@.,.K]ЩFЃт,х
0x0020   34 8B 00 50 04 1B 2A 6E-46 4D 84 70 A6 AA 50 10   4‹.P..*nFM„p¦ЄP.
0x0030   1B 54 E1 94 00 00 00 00-00 00 00 00               .Tб”........
```

Omnipeek 11: уже 10 ‘0’ байт???



Packet	Source	Destination	Flow ID	Flags	Size	Relative Time	Protocol	Application	Summary
1212	217.70.129.242	130.230.52.139	1		1353	1.201492	HTTP	HTTP	R PORT=1051 HTML Data
1213	130.230.52.139	217.70.129.242	1		64	1.201527	HTTP	HTTP	Src= 1051,Dst= 80,.A....,S=2221
1214	217.70.129.242	130.230.52.139	1		64	1.483208	HTTP	HTTP	Src= 80,Dst= 1051,.A....,S= 711
1215	130.230.52.139	217.70.129.242	1		64	1.483288	HTTP	HTTP	Src= 1051,Dst= 80,.A....,S=2221

```
⊟ Ethernet Type 2
    Destination:          00:06:1B:D3:25:19 NotebookDe:D3:25:19 [0-5]
    Source:               00:0F:34:18:4E:00 Cisco:18:4E:00 [6-11]
    Protocol Type:        0x0800  Internet Protocol version 4 (IPv4) [12-13]
⊟ IP Version 4 Header - Internet Protocol Datagram
    Version:              4 [14 Mask 0xF0]
    Header Length:        5  (20 bytes) [14 Mask 0x0F]
  ⊞ Diff. Services:       0x00 [15]
    Total Length:         40 [16-17]
    Identifier:           61640 [18-19]
  ⊞ Fragmentation Flags:  %010 [20 Mask 0xE0]
    Fragment Offset:      0  (0 bytes) [20-21 Mask 0x1FFF]
    Time To Live:         44 [22]
    Protocol:             6  TCP - Transmission Control Protocol [23]
    Header Checksum:      0x4B5D [24-25]
    Source IP Address:    217.70.129.242 [26-29]
    Dest. IP Address:     130.230.52.139 [30-33]
⊟ TCP - Transport Control Protocol
    Source Port:          80 http [34-35]
    Destination Port:     1051 optima-vnet [36-37]
    Sequence Number:      711870029 [38-41]
    Next Sequence #:      711870029  Calculated
    Ack Number:           2221975210 [42-45]
    TCP Offset:           5  (20 bytes) [46 Mask 0xF0]
    Reserved:             %000 [46 Mask 0x0E]
  ⊞ TCP Flags:            %000010000 [46-47 Mask 0x01FF]
    Window:               6996 [48-49]
    TCP Checksum:         0xE194 [50-51]
    Urgent Pointer:       0 [52-53]
    No TCP Options
⊟ FCS - Frame Check Sequence
    FCS:                  0xF4DA3A02  Calculated
```

```
 0  00 06 1B D3 25 19 00 0F 34 18 4E 00 08 00 45 00 00 28 F0 C8  ....%...4.N...E..(..
20  40 00 2C 06 4B 5D D9 46 81 F2 82 E6 34 8B 00 50 04 1B 2A 6E  @.,.K].F....4..P..*n
40  46 4D 84 70 A6 AA 50 10 1B 54 E1 94 00 00 00 00 00 00 00 00  FM.p..P..T..........
60  00 00 00 00                                                  ....
```

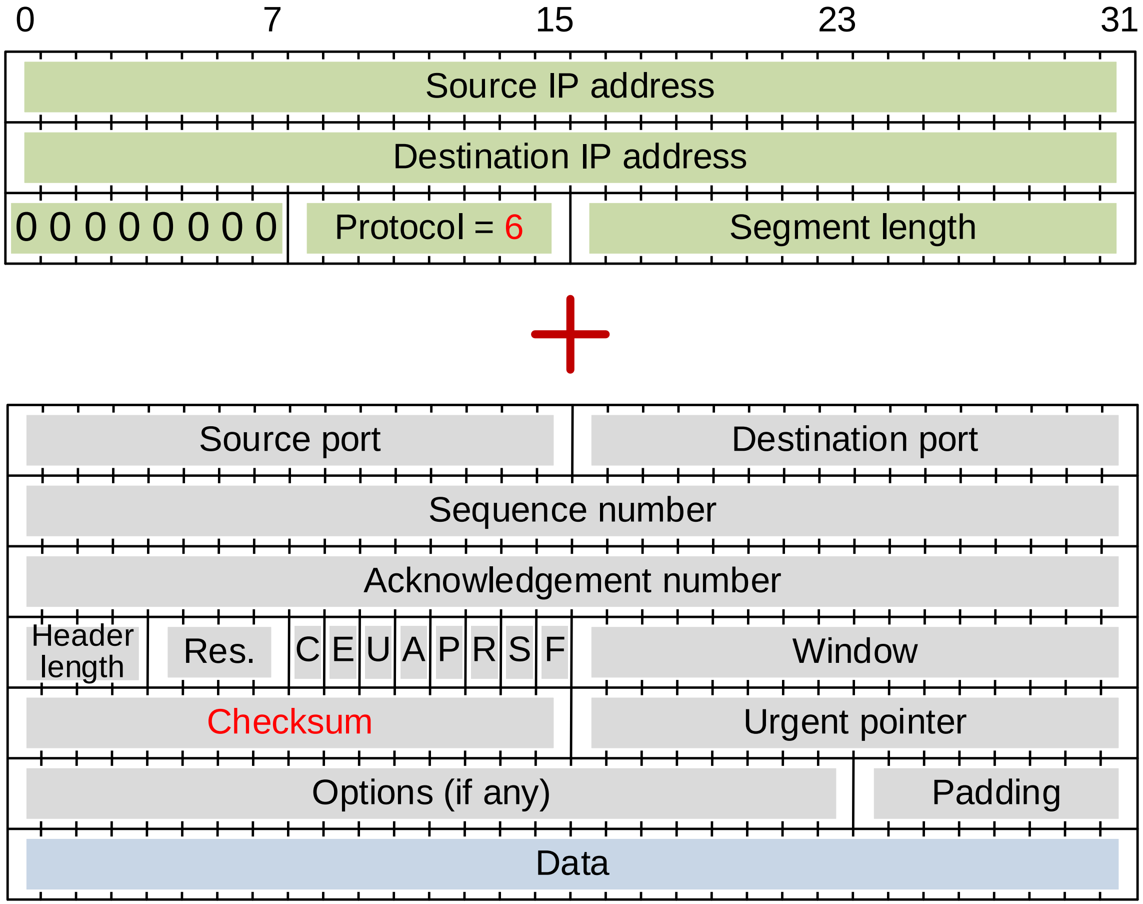
Алгоритм Internet Checksum

- Алгоритм расчета контрольной суммы Интернет (Internet Checksum), используемый в IPv4, UDP и TCP, описан в
  - https://tools.ietf.org/html/rfc1071

- Обратите внимание, что в отличие от контрольной суммы заголовка протокола IPv4, в UDP и TCP при расчете контрольной суммы учитывается (но сам не передается) **псевдозаголовок** (pseudo header)

- В ОС Microsoft Windows для расчета контрольных сумм можно воспользоваться стандартным калькулятором, переключившись в режим «Программист»:
  - View > Programmer > Hex

Контрольная сумма TCP

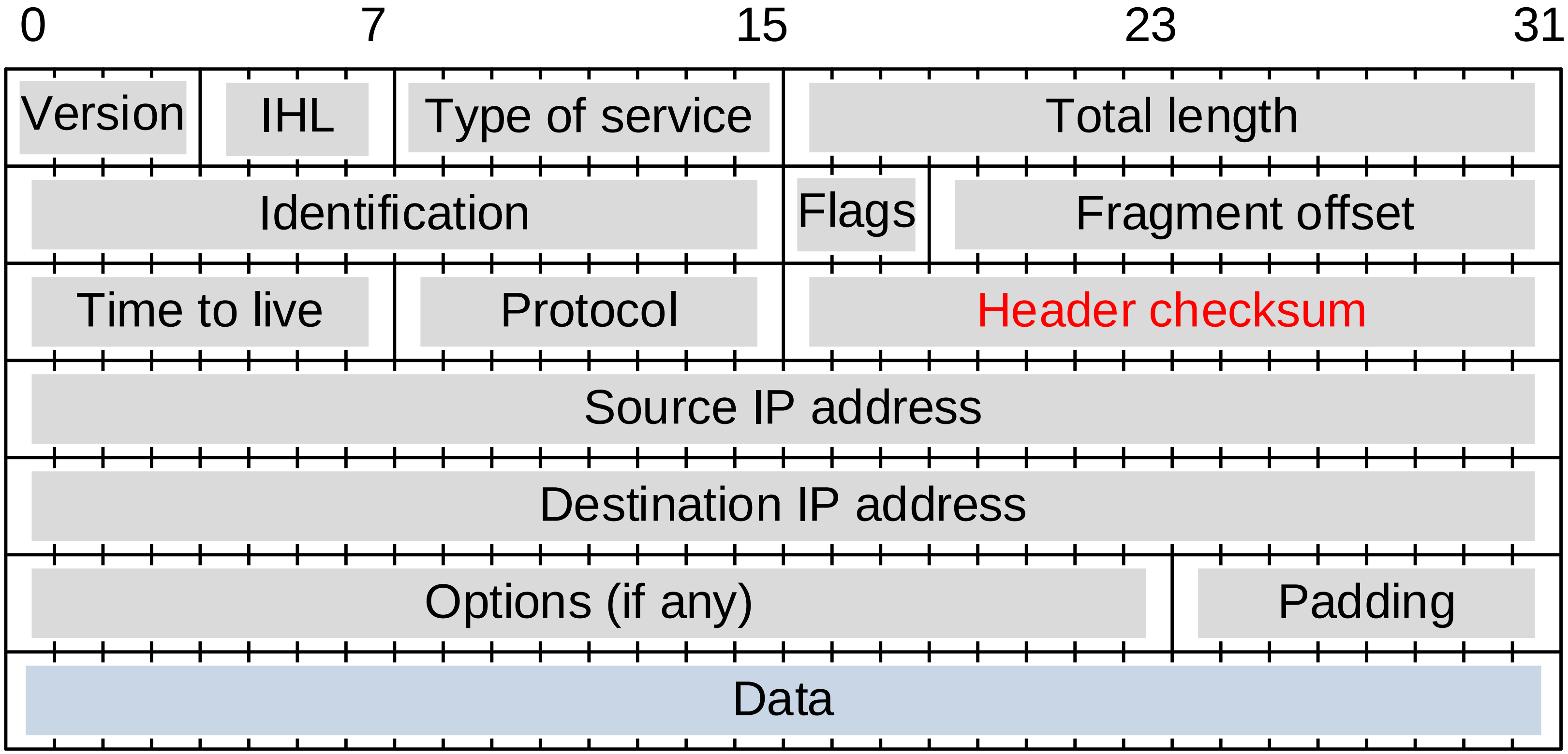


0	7	15	23	31
Source IP address				
Destination IP address				
0 0 0 0 0 0 0 0	Protocol = 6	Segment length		

+

Source port										Destination port
Sequence number										
Acknowledgement number										
Header length	Res.	C	E	U	A	P	R	S	F	Window
Checksum										Urgent pointer
Options (if any)										Padding
Data										

Контрольная сумма IPv4



0 7 15 23 31

Version IHL Type of service Total length

Identification Flags Fragment offset

Time to live Protocol Header checksum

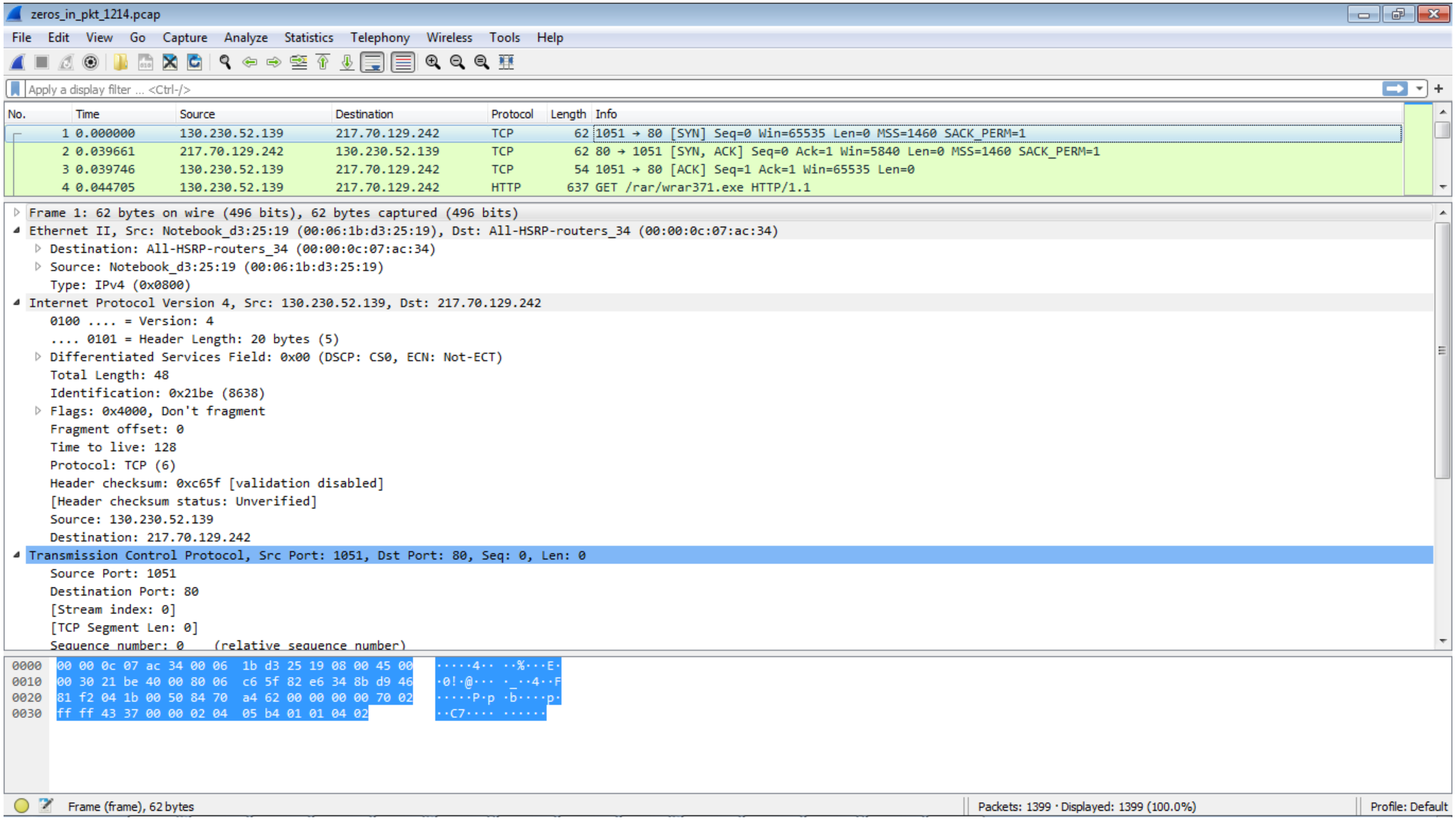
Source IP address

Destination IP address

Options (if any) Padding

Data

Пример расчета для кадра № 1


zeros_in_pkt_1214.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

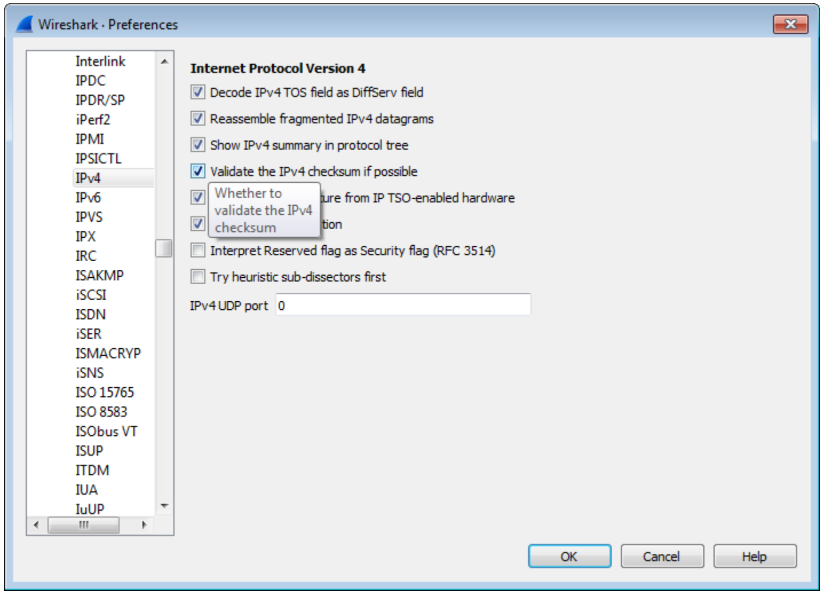
```
No.  Time       Source          Destination     Protocol Length Info
   1 0.000000   130.230.52.139  217.70.129.242  TCP       62 1051 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
   2 0.039661   217.70.129.242  130.230.52.139  TCP       62 80 → 1051 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
   3 0.039746   130.230.52.139  217.70.129.242  TCP       54 1051 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   4 0.044705   130.230.52.139  217.70.129.242  HTTP     637 GET /rar/wrar371.exe HTTP/1.1
```

```
Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
Ethernet II, Src: Notebook_d3:25:19 (00:06:1b:d3:25:19), Dst: All-HSRP-routers_34 (00:00:0c:07:ac:34)
   Destination: All-HSRP-routers_34 (00:00:0c:07:ac:34)
   Source: Notebook_d3:25:19 (00:06:1b:d3:25:19)
   Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 130.230.52.139, Dst: 217.70.129.242
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
   Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 48
   Identification: 0x21be (8638)
   Flags: 0x4000, Don't fragment
   Fragment offset: 0
   Time to live: 128
   Protocol: TCP (6)
   Header checksum: 0xc65f [validation disabled]
   [Header checksum status: Unverified]
   Source: 130.230.52.139
   Destination: 217.70.129.242
Transmission Control Protocol, Src Port: 1051, Dst Port: 80, Seq: 0, Len: 0
   Source Port: 1051
   Destination Port: 80
   [Stream index: 0]
   [TCP Segment Len: 0]
   Sequence number: 0    (relative sequence number)
```

```
0000  00 00 0c 07 ac 34 00 06  1b d3 25 19 08 00 45 00   ·····4·· ··%···E·
0010  00 30 21 be 40 00 80 06  c6 5f 82 e6 34 8b d9 46   ·0!·@··· ·_··4··F
0020  81 f2 04 1b 00 50 84 70  a4 62 00 00 00 00 70 02   ·····P·p ·b····p·
0030  ff ff 43 37 00 00 02 04  05 b4 01 01 04 02         ··C7···· ······
```

Frame (frame), 62 bytes   Packets: 1399 · Displayed: 1399 (100.0%)   Profile: Default

Edit > Preferences > Protocols > …



Internet Protocol Version 4

☑ Decode IPv4 TOS field as DiffServ field

☑ Reassemble fragmented IPv4 datagrams

☑ Show IPv4 summary in protocol tree

☑ Validate the IPv4 checksum if possible

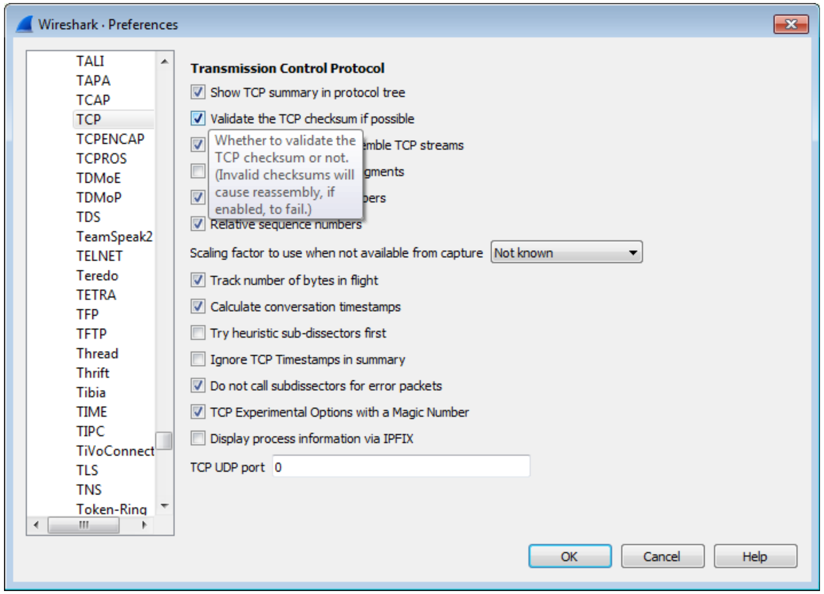
☑ Whether to validate the IPv4 checksum ure from IP TSO-enabled hardware

☑ tion

☐ Interpret Reserved flag as Security flag (RFC 3514)

☐ Try heuristic sub-dissectors first

IPv4 UDP port 0



Transmission Control Protocol

☑ Show TCP summary in protocol tree

☑ Validate the TCP checksum if possible

☑ Whether to validate the TCP checksum or not. (Invalid checksums will cause reassembly, if enabled, to fail.) mble TCP streams

☐ gments

☑ bers

☑ Relative sequence numbers

Scaling factor to use when not available from capture Not known

☑ Track number of bytes in flight

☑ Calculate conversation timestamps

☐ Try heuristic sub-dissectors first

☐ Ignore TCP Timestamps in summary

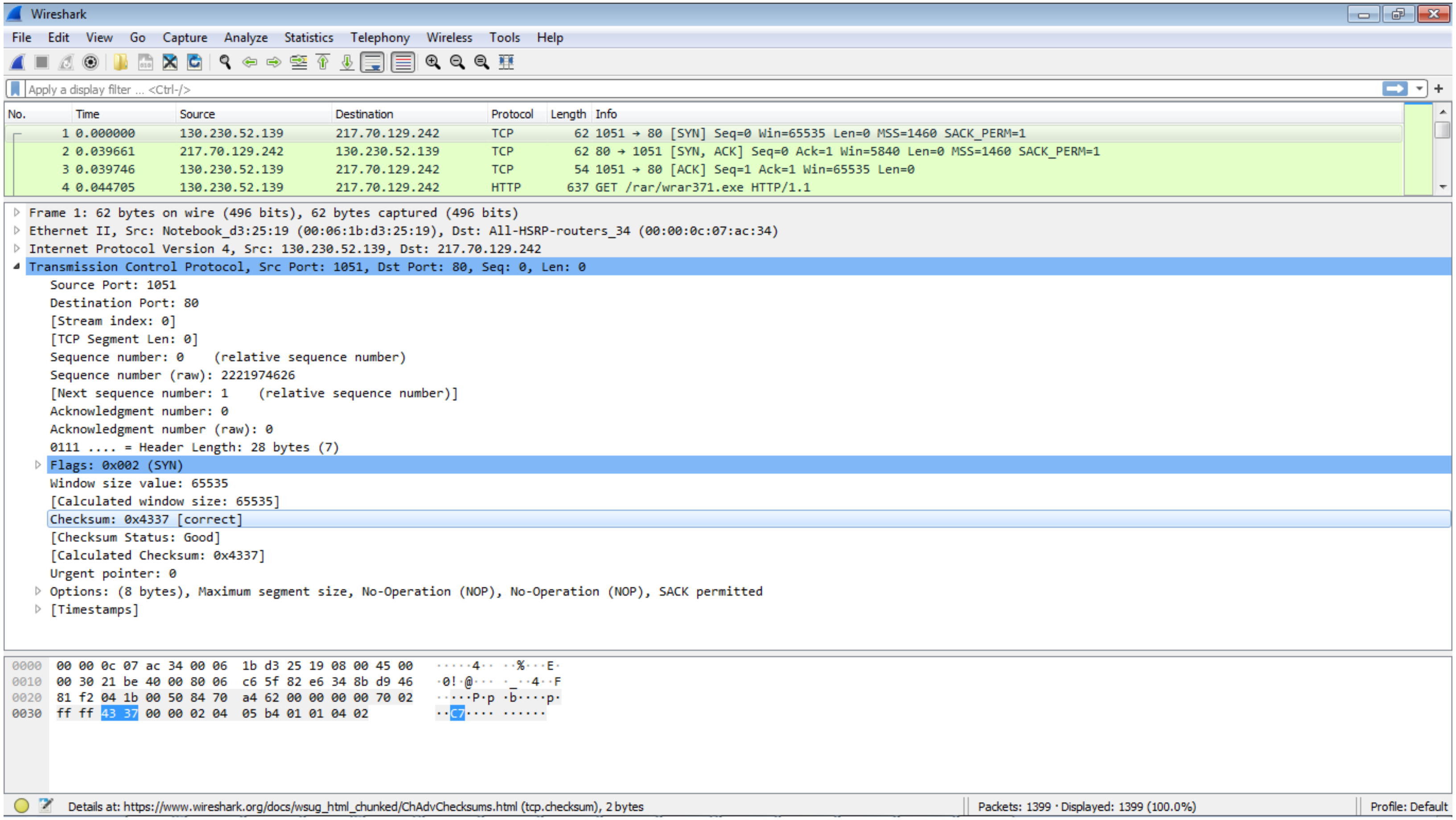
☑ Do not call subdissectors for error packets

☑ TCP Experimental Options with a Magic Number

☐ Display process information via IPFIX

TCP UDP port 0

Контрольная сумма TCP: 4337


Wireshark
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  130.230.52.139  217.70.129.242  TCP        62 1051 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
   2 0.039661  217.70.129.242  130.230.52.139  TCP        62 80 → 1051 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
   3 0.039746  130.230.52.139  217.70.129.242  TCP        54 1051 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   4 0.044705  130.230.52.139  217.70.129.242  HTTP      637 GET /rar/wrar371.exe HTTP/1.1
```

```
▷ Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
▷ Ethernet II, Src: Notebook_d3:25:19 (00:06:1b:d3:25:19), Dst: All-HSRP-routers_34 (00:00:0c:07:ac:34)
▷ Internet Protocol Version 4, Src: 130.230.52.139, Dst: 217.70.129.242
◢ Transmission Control Protocol, Src Port: 1051, Dst Port: 80, Seq: 0, Len: 0
     Source Port: 1051
     Destination Port: 80
     [Stream index: 0]
     [TCP Segment Len: 0]
     Sequence number: 0    (relative sequence number)
     Sequence number (raw): 2221974626
     [Next sequence number: 1    (relative sequence number)]
     Acknowledgment number: 0
     Acknowledgment number (raw): 0
     0111 .... = Header Length: 28 bytes (7)
   ▷ Flags: 0x002 (SYN)
     Window size value: 65535
     [Calculated window size: 65535]
     Checksum: 0x4337 [correct]
     [Checksum Status: Good]
     [Calculated Checksum: 0x4337]
     Urgent pointer: 0
   ▷ Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted
   ▷ [Timestamps]
```

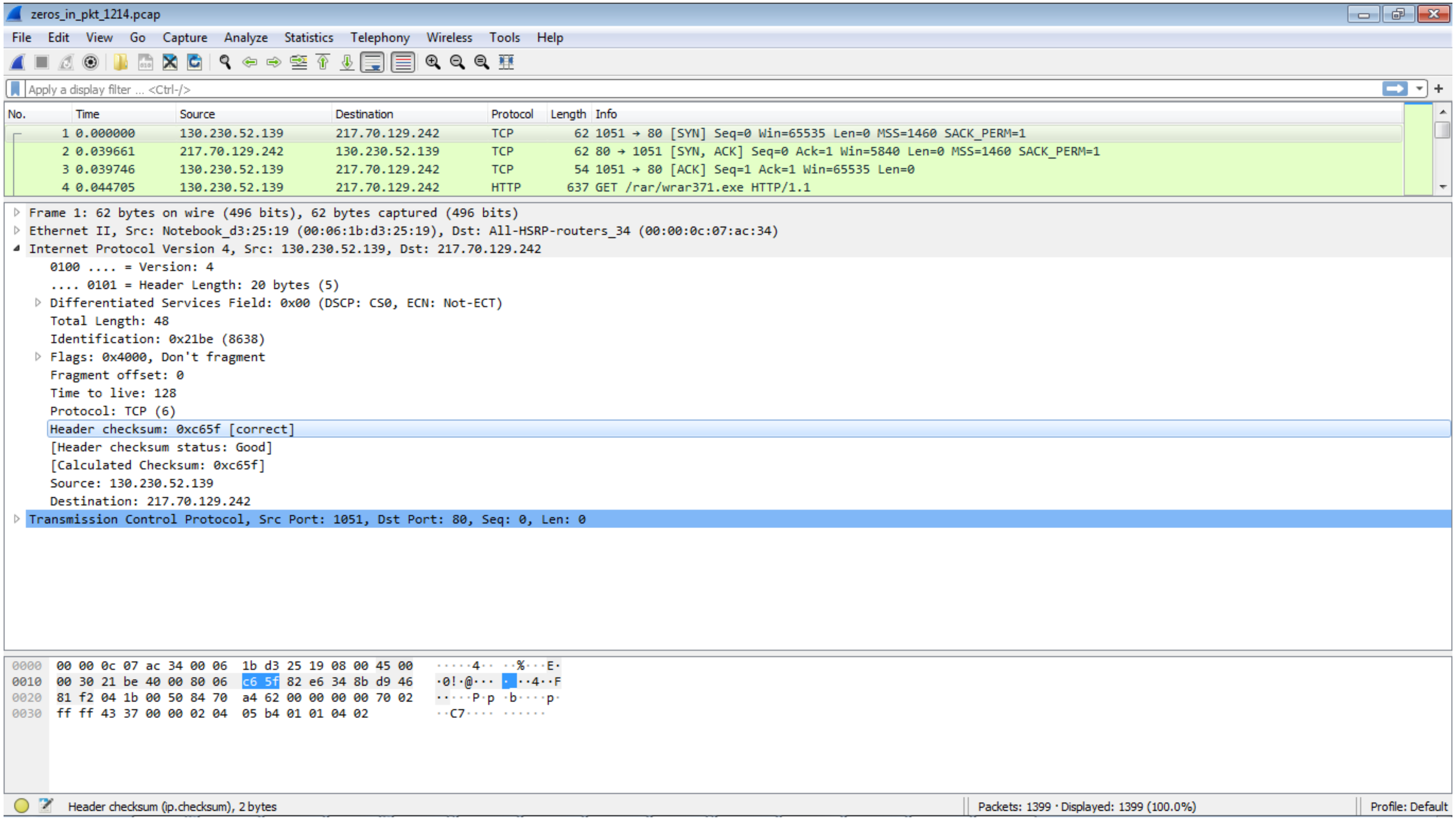
```
0000  00 00 0c 07 ac 34 00 06  1b d3 25 19 08 00 45 00   ·····4·· ··%···E·
0010  00 30 21 be 40 00 80 06  c6 5f 82 e6 34 8b d9 46   ·0!·@··· ·_··4··F
0020  81 f2 04 1b 00 50 84 70  a4 62 00 00 00 00 70 02   ·····P·p ·b····p·
0030  ff ff 43 37 00 00 02 04  05 b4 01 01 04 02         ··C7···· ······
```

Details at: https://www.wireshark.org/docs/wsug_html_chunked/ChAdvChecksums.html (tcp.checksum), 2 bytes | Packets: 1399 · Displayed: 1399 (100.0%) | Profile: Default

Расчет контрольной суммы TCP

82e6 + 348b	b771	112aa > 12ab	1738	b00d	bcc8 > NOT > 4337
d946 + 81f2	15b38 > 5b39				
0006 + 001c	0022	048d			
041b + 0050	046b				
8470 + a462	128d2 > 28d3	28d3	98d5		
0000 + 0000	0000				
7002 + ffff	17001 > 7002	7002			
0000 + 0000	0000				
0204 + 05b4	07b8	0cbb	0cbb	0cbb	
0101 + 0402	0503				

Контрольная сумма IPv4: c65f


zeros_in_pkt_1214.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.     Time        Source           Destination      Protocol Length Info
      1 0.000000    130.230.52.139   217.70.129.242   TCP        62 1051 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
      2 0.039661    217.70.129.242   130.230.52.139   TCP        62 80 → 1051 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
      3 0.039746    130.230.52.139   217.70.129.242   TCP        54 1051 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
      4 0.044705    130.230.52.139   217.70.129.242   HTTP      637 GET /rar/wrar371.exe HTTP/1.1
```

```
▷ Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
▷ Ethernet II, Src: Notebook_d3:25:19 (00:06:1b:d3:25:19), Dst: All-HSRP-routers_34 (00:00:0c:07:ac:34)
◢ Internet Protocol Version 4, Src: 130.230.52.139, Dst: 217.70.129.242
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▷ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 48
    Identification: 0x21be (8638)
  ▷ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xc65f [correct]
    [Header checksum status: Good]
    [Calculated Checksum: 0xc65f]
    Source: 130.230.52.139
    Destination: 217.70.129.242
▷ Transmission Control Protocol, Src Port: 1051, Dst Port: 80, Seq: 0, Len: 0
```

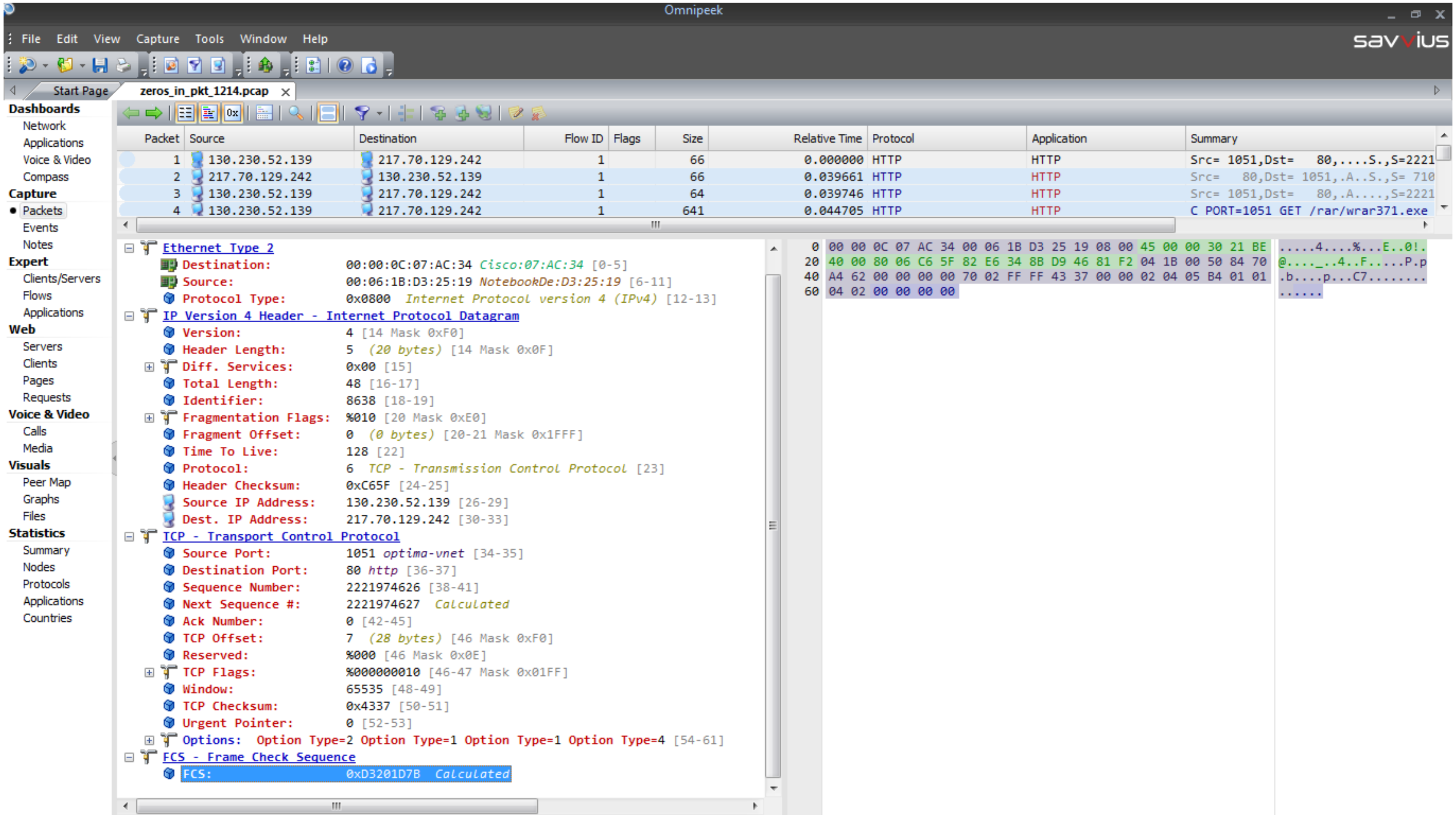
```
0000  00 00 0c 07 ac 34 00 06  1b d3 25 19 08 00 45 00   ·····4·· ··%···E·
0010  00 30 21 be 40 00 80 06  c6 5f 82 e6 34 8b d9 46   ·0!·@··· ···4··F
0020  81 f2 04 1b 00 50 84 70  a4 62 00 00 00 00 70 02   ·····P·p ·b····p·
0030  ff ff 43 37 00 00 02 04  05 b4 01 01 04 02         ··C7···· ······
```

Header checksum (ip.checksum), 2 bytes | Packets: 1399 · Displayed: 1399 (100.0%) | Profile: Default

Расчет контрольной суммы IPv4

4500 + 0030	**4530**	**a6ee**	**de66**	**1399f > 39a0 > NOT > c65f**
21be + 4000	61be			
8006 + 0000	8006	13777 > 3778		
82e6 + 348b	b771			
d946 + 81f2	15b38 > 5b39	5b39	5b39	

Значение FCS Ethernet: d3201d7b

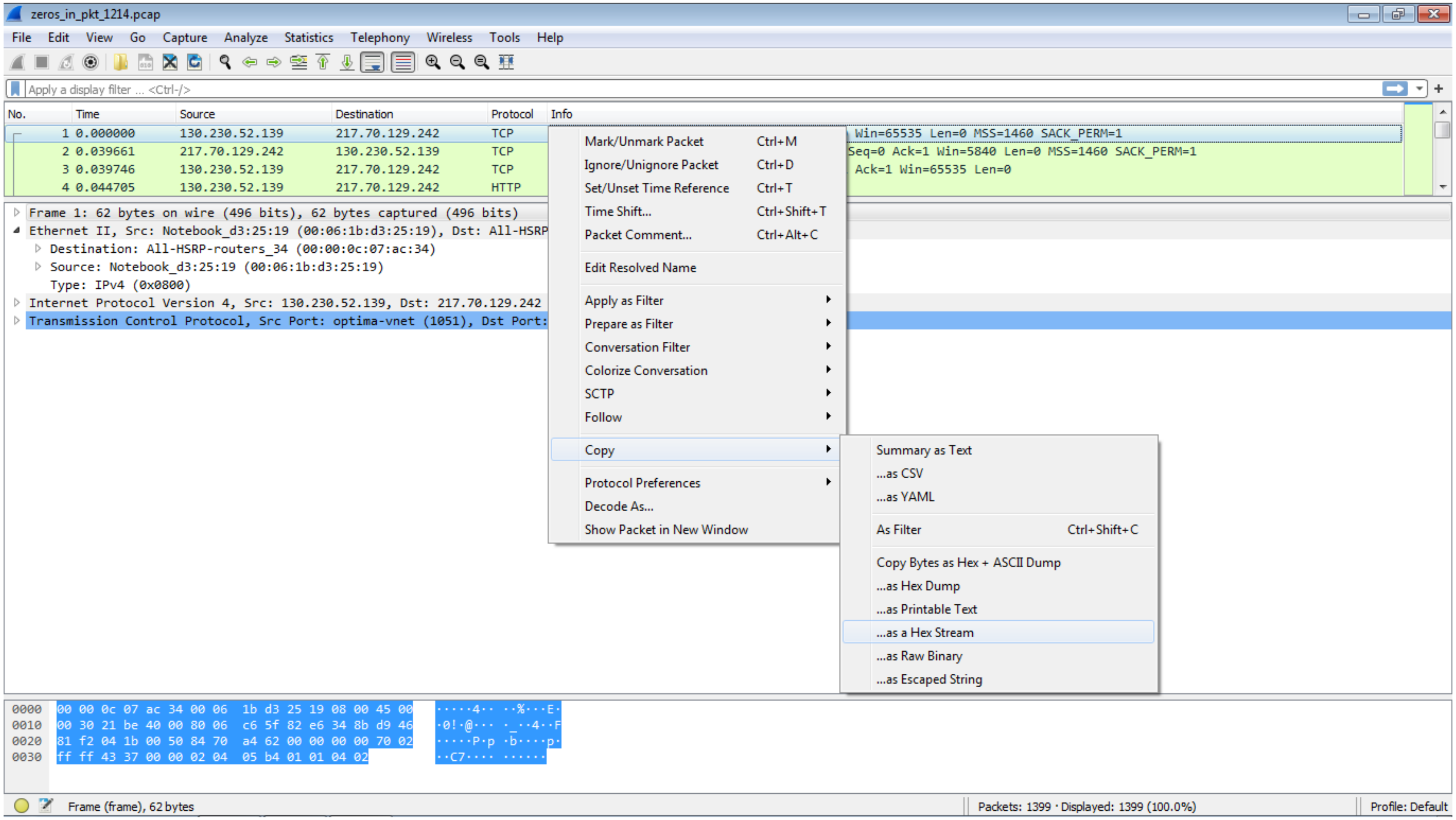


Packet	Source	Destination	Flow ID	Flags	Size	Relative Time	Protocol	Application	Summary
1	130.230.52.139	217.70.129.242	1		66	0.000000	HTTP	HTTP	Src= 1051,Dst= 80,....S.,S=2221
2	217.70.129.242	130.230.52.139	1		66	0.039661	HTTP	HTTP	Src= 80,Dst= 1051,.A..S.,S= 710
3	130.230.52.139	217.70.129.242	1		64	0.039746	HTTP	HTTP	Src= 1051,Dst= 80,.A....,S=2221
4	130.230.52.139	217.70.129.242	1		641	0.044705	HTTP	HTTP	C PORT=1051 GET /rar/wrar371.exe

```
⊟ Ethernet Type 2
    Destination:          00:00:0C:07:AC:34 Cisco:07:AC:34 [0-5]
    Source:               00:06:1B:D3:25:19 NotebookDe:D3:25:19 [6-11]
    Protocol Type:        0x0800  Internet Protocol version 4 (IPv4) [12-13]
⊟ IP Version 4 Header - Internet Protocol Datagram
    Version:              4 [14 Mask 0xF0]
    Header Length:        5  (20 bytes) [14 Mask 0x0F]
  ⊞ Diff. Services:       0x00 [15]
    Total Length:         48 [16-17]
    Identifier:           8638 [18-19]
  ⊞ Fragmentation Flags:  %010 [20 Mask 0xE0]
    Fragment Offset:      0  (0 bytes) [20-21 Mask 0x1FFF]
    Time To Live:         128 [22]
    Protocol:             6  TCP - Transmission Control Protocol [23]
    Header Checksum:      0xC65F [24-25]
    Source IP Address:    130.230.52.139 [26-29]
    Dest. IP Address:     217.70.129.242 [30-33]
⊟ TCP - Transport Control Protocol
    Source Port:          1051 optima-vnet [34-35]
    Destination Port:     80 http [36-37]
    Sequence Number:      2221974626 [38-41]
    Next Sequence #:      2221974627  Calculated
    Ack Number:           0 [42-45]
    TCP Offset:           7  (28 bytes) [46 Mask 0xF0]
    Reserved:             %000 [46 Mask 0x0E]
  ⊞ TCP Flags:            %000000010 [46-47 Mask 0x01FF]
    Window:               65535 [48-49]
    TCP Checksum:         0x4337 [50-51]
    Urgent Pointer:       0 [52-53]
  ⊞ Options:  Option Type=2 Option Type=1 Option Type=1 Option Type=4 [54-61]
⊟ FCS - Frame Check Sequence
    FCS:                  0xD3201D7B  Calculated
```

```
 0 00 00 0C 07 AC 34 00 06 1B D3 25 19 08 00 45 00 00 30 21 BE  .....4....%...E..0!.
20 40 00 80 06 C6 5F 82 E6 34 8B D9 46 81 F2 04 1B 00 50 84 70  @...._..4..F....P.p
40 A4 62 00 00 00 00 70 02 FF FF 43 37 00 00 02 04 05 B4 01 01  .b....p...C7........
60 04 02 00 00 00 00                                            ......
```

Кликаем правой кнопкой и Copy



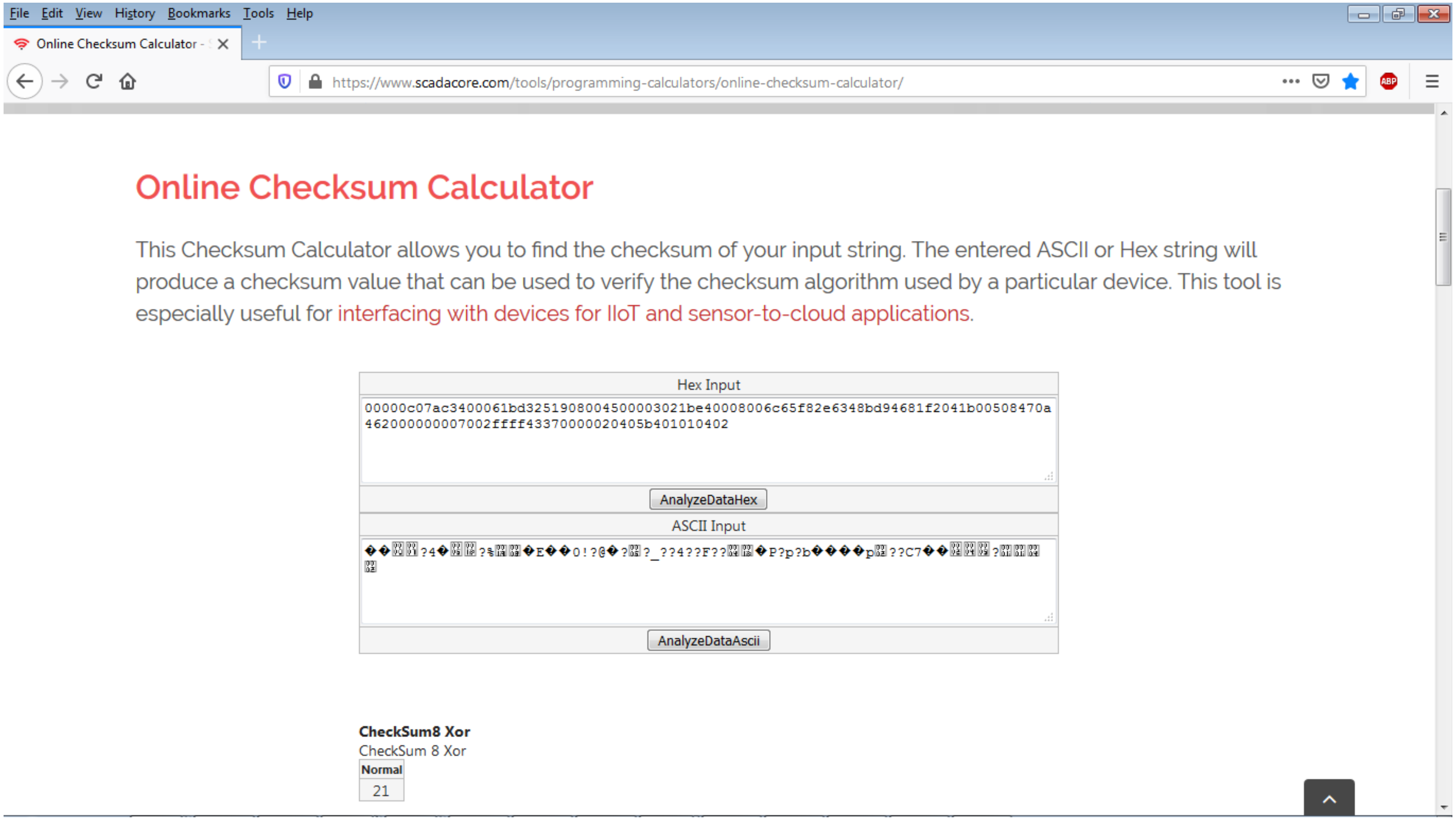
```
No.  Time       Source          Destination     Protocol  Info
   1 0.000000   130.230.52.139  217.70.129.242  TCP       Win=65535 Len=0 MSS=1460 SACK_PERM=1
   2 0.039661   217.70.129.242  130.230.52.139  TCP       Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
   3 0.039746   130.230.52.139  217.70.129.242  TCP       Ack=1 Win=65535 Len=0
   4 0.044705   130.230.52.139  217.70.129.242  HTTP
```

```
▷ Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
◢ Ethernet II, Src: Notebook_d3:25:19 (00:06:1b:d3:25:19), Dst: All-HSRP
  ▷ Destination: All-HSRP-routers_34 (00:00:0c:07:ac:34)
  ▷ Source: Notebook_d3:25:19 (00:06:1b:d3:25:19)
    Type: IPv4 (0x0800)
▷ Internet Protocol Version 4, Src: 130.230.52.139, Dst: 217.70.129.242
▷ Transmission Control Protocol, Src Port: optima-vnet (1051), Dst Port:
```

```
0000  00 00 0c 07 ac 34 00 06  1b d3 25 19 08 00 45 00   ·····4·· ··%···E·
0010  00 30 21 be 40 00 80 06  c6 5f 82 e6 34 8b d9 46   ·0!·@··· ·_··4··F
0020  81 f2 04 1b 00 50 84 70  a4 62 00 00 00 00 70 02   ·····P·p ·b····p·
0030  ff ff 43 37 00 00 02 04  05 b4 01 01 04 02         ··C7···· ······
```

Frame (frame), 62 bytes | Packets: 1399 · Displayed: 1399 (100.0%) | Profile: Default

Вставляем и жмем AnalyzeDataHex


File Edit View History Bookmarks Tools Help
Online Checksum Calculator -
https://www.scadacore.com/tools/programming-calculators/online-checksum-calculator/

Online Checksum Calculator

This Checksum Calculator allows you to find the checksum of your input string. The entered ASCII or Hex string will produce a checksum value that can be used to verify the checksum algorithm used by a particular device. This tool is especially useful for interfacing with devices for IIoT and sensor-to-cloud applications.

Hex Input

```
00000c07ac3400061bd32519080045000003021be40008006c65f82e6348bd94681f2041b00508470a
46200000000007002ffff43370000020405b401010402
```

ASCII Input

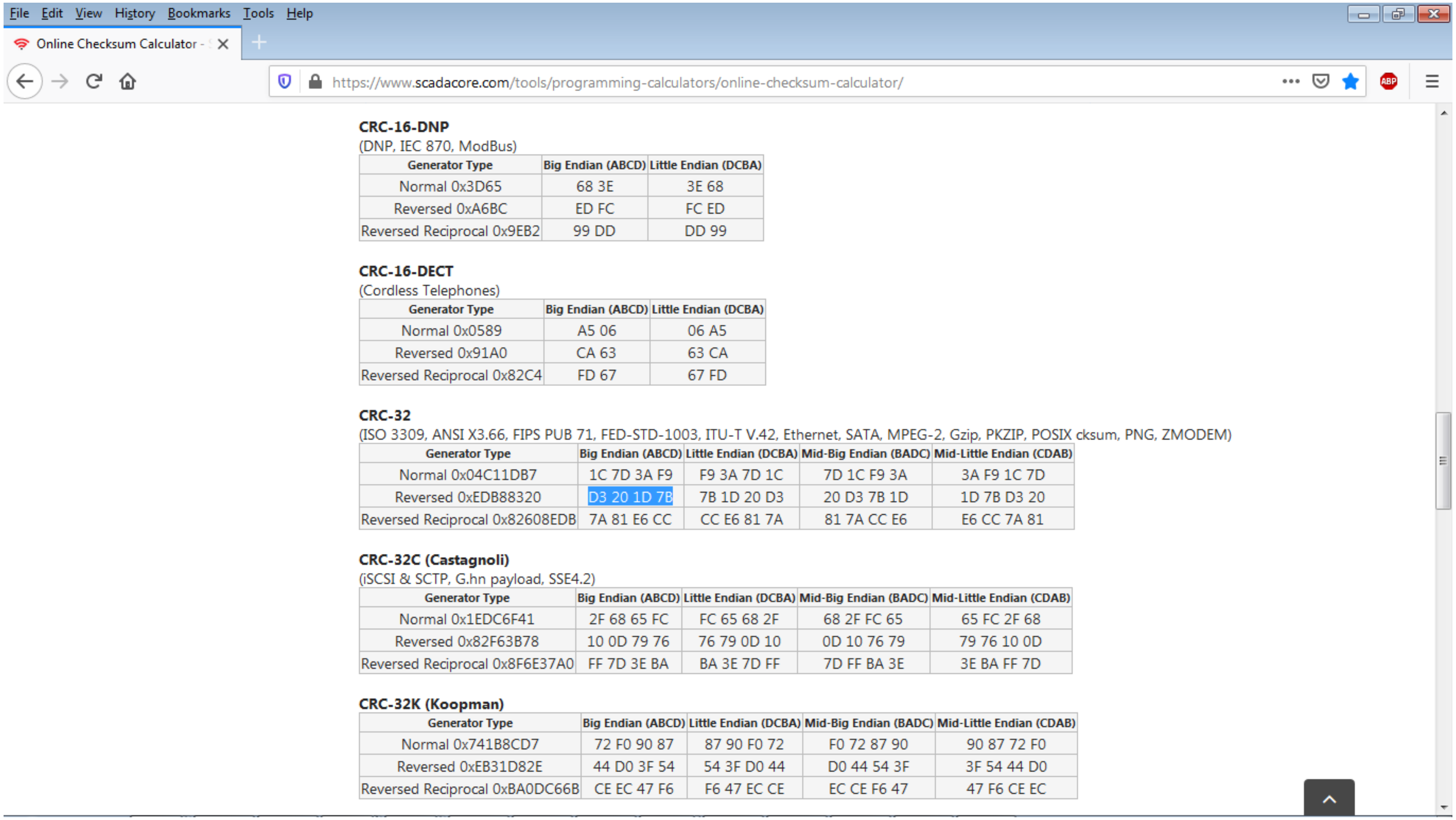
```
��▯▯?4�▯▯?%▯▯�E��0!?@�?▯?_??4??F??▯▯�P?p?b����p▯??C7��▯▯▯?▯▯▯
▯
```

CheckSum8 Xor

CheckSum 8 Xor

Normal
21

CRC-32: Reversed и Big Endian


File Edit View History Bookmarks Tools Help
Online Checksum Calculator -
https://www.scadacore.com/tools/programming-calculators/online-checksum-calculator/
ABP

CRC-16-DNP
(DNP, IEC 870, ModBus)

Generator Type	Big Endian (ABCD)	Little Endian (DCBA)
Normal 0x3D65	68 3E	3E 68
Reversed 0xA6BC	ED FC	FC ED
Reversed Reciprocal 0x9EB2	99 DD	DD 99

CRC-16-DECT
(Cordless Telephones)

Generator Type	Big Endian (ABCD)	Little Endian (DCBA)
Normal 0x0589	A5 06	06 A5
Reversed 0x91A0	CA 63	63 CA
Reversed Reciprocal 0x82C4	FD 67	67 FD

CRC-32
(ISO 3309, ANSI X3.66, FIPS PUB 71, FED-STD-1003, ITU-T V.42, Ethernet, SATA, MPEG-2, Gzip, PKZIP, POSIX cksum, PNG, ZMODEM)

Generator Type	Big Endian (ABCD)	Little Endian (DCBA)	Mid-Big Endian (BADC)	Mid-Little Endian (CDAB)
Normal 0x04C11DB7	1C 7D 3A F9	F9 3A 7D 1C	7D 1C F9 3A	3A F9 1C 7D
Reversed 0xEDB88320	D3 20 1D 7B	7B 1D 20 D3	20 D3 7B 1D	1D 7B D3 20
Reversed Reciprocal 0x82608EDB	7A 81 E6 CC	CC E6 81 7A	81 7A CC E6	E6 CC 7A 81

CRC-32C (Castagnoli)
(iSCSI & SCTP, G.hn payload, SSE4.2)

Generator Type	Big Endian (ABCD)	Little Endian (DCBA)	Mid-Big Endian (BADC)	Mid-Little Endian (CDAB)
Normal 0x1EDC6F41	2F 68 65 FC	FC 65 68 2F	68 2F FC 65	65 FC 2F 68
Reversed 0x82F63B78	10 0D 79 76	76 79 0D 10	0D 10 76 79	79 76 10 0D
Reversed Reciprocal 0x8F6E37A0	FF 7D 3E BA	BA 3E 7D FF	7D FF BA 3E	3E BA FF 7D

CRC-32K (Koopman)

Generator Type	Big Endian (ABCD)	Little Endian (DCBA)	Mid-Big Endian (BADC)	Mid-Little Endian (CDAB)
Normal 0x741B8CD7	72 F0 90 87	87 90 F0 72	F0 72 87 90	90 87 72 F0
Reversed 0xEB31D82E	44 D0 3F 54	54 3F D0 44	D0 44 54 3F	3F 54 44 D0
Reversed Reciprocal 0xBA0DC66B	CE EC 47 F6	F6 47 EC CE	EC CE F6 47	47 F6 CE EC