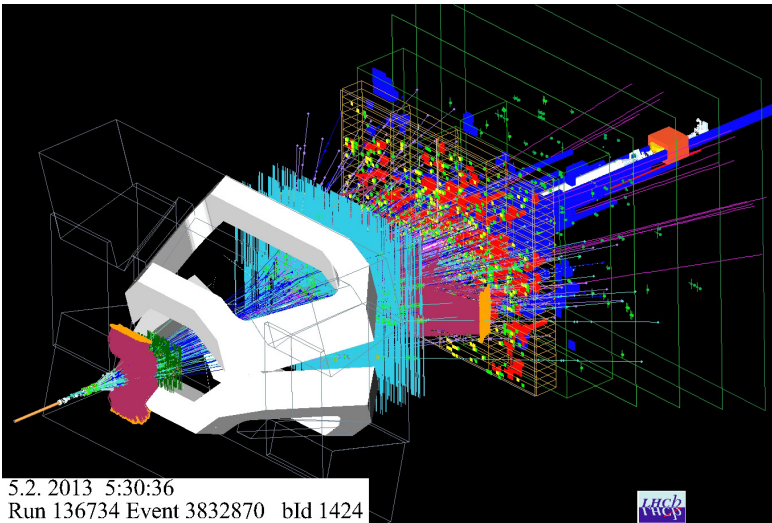


# A Wireshark based verification tool for the new LHCb common detector read-out board Wireshark dissectors for dummies

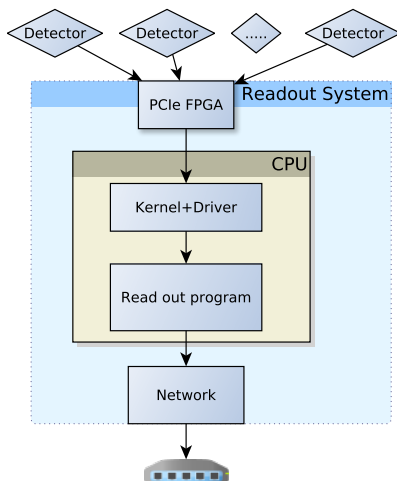
Christina Quast

**LHCb**

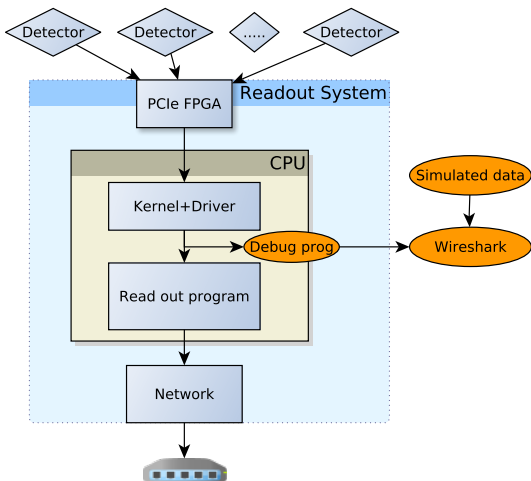
Openlab Summer Student Lightning talks 2015  
Supervisor: Rainer Schwemmer



# Read out board



# Openlab Summer project tasks



# Wireshark dissecting HTTP

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ip.src == 62.146.26.38 && http` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
82	6.7000120	62.146.26.38	128.141.187.149	TCP	74	80->36010 [SYN, ACK] Seq=
85	6.8000150	62.146.26.38	128.141.187.149	TCP	66	80->36010 [ACK] Seq=1 Ack
86	6.8000550	62.146.26.38	128.141.187.149	HTTP	450	HTTP/1.1 304 Not Modified
119	9.6000010	62.146.26.38	128.141.187.149	HTTP/XML	649	HTTP/1.1 200 OK
125	9.9000540	62.146.26.38	128.141.187.149	TCP	2962	[TCP segment of a reass

▶ Ethernet II, Src: Hewlett-d7:81:00 (00:18:71:d7:81:00), Dst: IntelCor\_06:e3:18 (00:1e:64:06:e3:18)

▶ Internet Protocol Version 4, Src: 62.146.26.38 (62.146.26.38), Dst: 128.141.187.149 (128.141.187.149)

▼ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 36010 (36010), Seq: 385, Ack: 1060, Len: 583

Source Port: 80 (80)

Destination Port: 36010 (36010)

[Stream index: 2]

[TCP Segment Len: 583]

Sequence number: 385 (relative sequence number)

[Next sequence number: 968 (relative sequence number)]

Acknowledgment number: 1060 (relative ack number)

Header Length: 32 bytes

0020	bb 95 00 50 8c aa ab f0 84 5e 23 de d5 97 80 18	...P....^#.....
0030	00 82 39 16 00 00 01 01 08 0a 05 c9 62 7a 03 db	..9.....bz..
0040	62 dc 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f	b.HTTP/1.1 200 O
0050	4b 0d 0a 53 65 72 76 65 72 3a 20 6e 67 69 6e 78	K..Server: nginx
0060	0d 0a 44 61 74 65 3a 20 4d 6f 6e 2c 20 32 34 20	..Date: Mon, 24
0070	41 75 67 20 32 30 31 35 20 31 35 3a 35 30 3a 30	Aug 2015 15:50:0
0080	31 20 47 4d 54 0d 0a 43 6f 6e 74 65 74 2d 54	1 GMT Content-T

Frame (649 bytes) De-chunked entity body (211 bytes)

# Without MEP dissector

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter:  Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	UDP	61	Source port: 42142 Desti
3	0.000119	127.0.0.1	127.0.0.1	UDP	71	Source port: 34129 Desti

▶ Frame 3: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0

▶ 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 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)

▶ User Datagram Protocol, Src Port: 34129 (34129), Dst Port: 1235 (1235)

▼ Data (29 bytes)

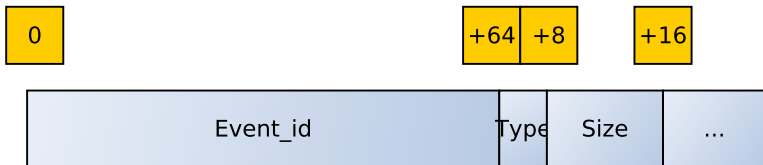
Data: 0900000000000000002000900000242420005424242424200...

[Length: 29]

```

0000 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00  ....E.
0010 00 39 53 ba 40 00 40 11 e8 f7 7f 00 00 01 7f 00  .9S.@. ....
0020 00 01 85 51 04 d3 00 25 fe 38 09 00 00 00 00 00  ...Q...% .8.....
0030 00 00 02 00 09 00 00 02 42 42 00 05 42 42 42 42  ....BB..BBBB
0040 42 00 01 42 00 01 42  ....B..B
  
```

# Protocol



## A basic wireshark dissector

```

static void dissect_mep(tvbuff_t *tvb, packet_info *pinfo,
    proto_tree *tree) {
    gint offset = 0;
    ...
    proto_tree *data_tree = proto_item_add_subtree(data_root,
        ett_data);
    proto_tree_add_item(data_tree, hf_data_evid, tvb, offset,
        8, ENC_BIG_ENDIAN); // 64bit = 8 byte
    offset += 8;
    proto_tree_add_item(data_tree, hf_data_type, tvb, offset,
        1, ENC_BIG_ENDIAN);
    offset += 1;
    proto_tree_add_item(data_tree, hf_data_size, tvb, offset,
        2, ENC_BIG_ENDIAN);
    offset += 2;
    ...
}
}

```





## Wireshark Dissector

## With MEP dissector

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter:  Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	MEP2 meta	61	Num. events: 0
3	0.000118	127.0.0.1	127.0.0.1	MEP Data	65	Event size: 9

▶ Frame 3: 65 bytes on wire (520 bits), 65 bytes captured (520 bits) on interface 0  
 ▶ 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 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)  
 ▶ User Datagram Protocol, Src Port: 50102 (50102), Dst Port: 1235 (1235)  
 ▼ MEP2 Protocol  
   ▼ MEP2 Data  
     MEP2 data: Event ID: 360287970189639680  
     MEP data: Type: Type 2 (2)  
     MEP data: Size: 9  
     ▶ MEP2 Data Payload

```

0000  00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00  .....E.
0010  00 33 6e 35 40 00 40 11 ce 82 7f 00 00 01 7f 00  .3n5@.@. ....
0020  00 01 c3 b6 04 d3 00 1f fe 32 05 00 00 00 00 00  .....2.....
0030  00 00 02 00 09 00 00 09 42 42 42 42 42 42 42 42  .....BBBBBBBB
0040  42
  
```

# Happy Supervisor



## Accomplished tasks

- Github repository with Wireshark dissector for MEP
- Wikipage for future reference
- Python test code
- C program as link between kernel driver and wireshark

## Plans for the (near) future

- Dissector for payload
- Bugfree software