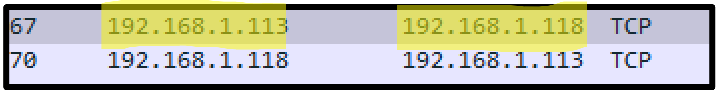
BPR תשובות מרים מאיר 317924835 הכול בגדר ניחוש חוץ משאלה 1

1.

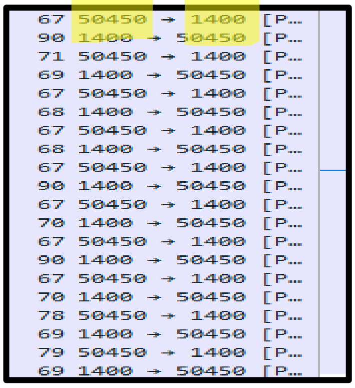
filter: frame contains "BPR"

IP's used: 192.168.1.113 and 192.168.1.118



```
67    192.168.1.113    192.168.1.118    TCP
70    192.168.1.118    192.168.1.113    TCP
```

Ports used: 50450 and 1400

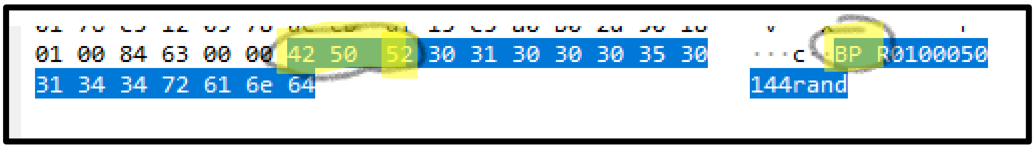


```
67 50450 → 1400 [P…
90 1400 → 50450 [P…
71 50450 → 1400 [P…
69 1400 → 50450 [P…
67 50450 → 1400 [P…
68 1400 → 50450 [P…
67 50450 → 1400 [P…
68 1400 → 50450 [P…
67 50450 → 1400 [P…
90 1400 → 50450 [P…
67 50450 → 1400 [P…
70 1400 → 50450 [P…
67 50450 → 1400 [P…
90 1400 → 50450 [P…
67 50450 → 1400 [P…
70 1400 → 50450 [P…
78 50450 → 1400 [P…
69 1400 → 50450 [P…
79 50450 → 1400 [P…
69 1400 → 50450 [P…
```

2.

First field:

a. BPR
b. The 3 first bytes

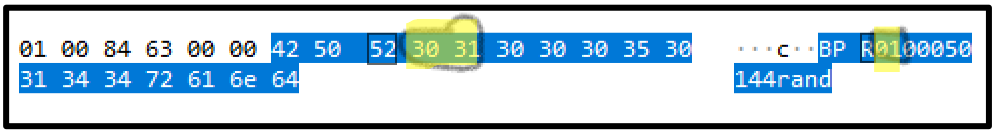


```
01 00 84 63 00 00 42 50 52 30 31 30 30 30 35 30    ···c··BP R0100050
31 34 34 72 61 6e 64                                144rand
```

c. BPR is the only option

Second field:

a. Sequence number of response/requests
b. takes up the next 2 bytes(the response should have the same number as its request)



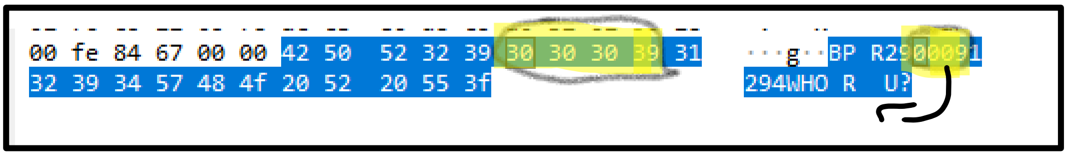
```
01 00 84 63 00 00 42 50 52 30 31 30 30 30 35 30    ···c··BP R0100050
31 34 34 72 61 6e 64                                144rand
```

c. goes up by one each request from 00 to 31 and then restarts to 00 so the options are 00-31

Third field:

a. length

b. takes up the next 4 bytes

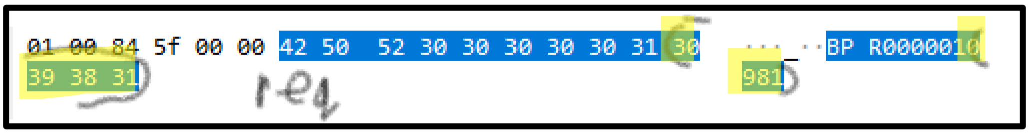


```
00 fe 84 67 00 00 42 50  52 32 39 30 30 30 39 31   ···g··BP R2900091
32 39 34 57 48 4f 20 52  20 55 3f                  294WHO R  U?
```

c. length of message that comes after command so anywhere between 0000 to 9999

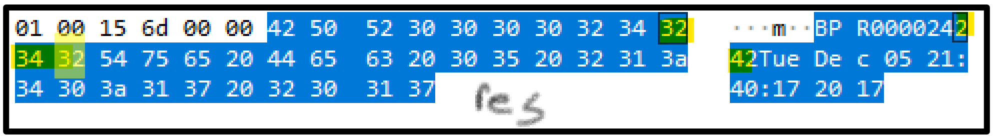
Forth field:

a. Command code
b. Takes up 4 bytes if it's a request or 3 if it's a response



```
01 00 84 5f 00 00 42 50  52 30 30 30 30 30 31 30   ···_··BP R0000010
39 38 31                                           981
```

req



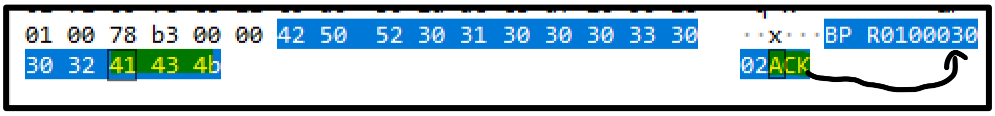
```
01 00 15 6d 00 00 42 50  52 30 30 30 30 32 34 32   ···m··BP R0000242
34 32 54 75 65 20 44 65  63 20 30 35 20 32 31 3a   42Tue De c 05 21:
34 30 3a 31 37 20 32 30  31 37                     40:17 20 17
```

res

c. the command is sent to the server to get the correct response
examples of the codes: 0981, 0992, 1003, ***4, 0970, 232, 002, 1**, 2**

Fifth field:

a. Message
b. The number of bytes set are by the length (third field)



```
01 00 78 b3 00 00 42 50  52 30 31 30 30 30 33 30   ··x···BP R0100030
30 32 41 43 4b                                     02ACK
```

c. could be no message, a random one, an ack that confirms you got the message, a response message based on the requests command like the date or a pong.

3.

Command code	How it functions?
0970	request to end it does not get a response
0981	Asks for the current date and gets 1** "current date"
0992	Asks for Random number from 10 to 99 and gets 2** "random 2-digit num"
1003	Asks for pong and gets 232 pong
*****4 "message"**	Sends message and gets back 002 ACK

4.

First field

No calculation needed just BPR.

Second field

A sequence number that goes up by one every time a new request is made till 31 then restarts.

Third field

Is calculated by the length of the fifth field- message. It uses 4 bytes so in the format of **** signifying the length.

Forth field

Couldn’t figure out the reason for the command codes they're the same when it's the same message and command and different when it's not. (I think each number is also a command but also has a message associated with the code could be no message)

Examples when its different:

The one that’s sends a message is different according to the message just ends with ***4

The response code to 0981 sends back a date with a different code each time that start with 2**

The response code to 0992 that sends back a random number with a different code each time that starts with 1**

Fifth field

A message that is the length of the third field and decided by the command code.

How I split it:

Request-example	**Response-example**
BPR 00 0001 0981	**BPR 00 0024 242 Tue Dec 05 21:40:17 2017**
BPR 02 0001 0992	**BPR 02 0002 158 39**
BPR 05 0001 1003	**BPR 05 0004 232 pong**
BPR 08 0012 1794 HELLO WORLD	**BPR 08 0003 002 ACK**
BPR 04 0001 0970	

לכבוד הבודק תודה לבדיקה! בגלל האופי המחקרי של תרגיל זה. אין לי דרך לדעת אם אני צודקת.
אחרי 6 שעות של להסתכל על התוכן לא ידעתי אם אני ממציאה מדמיינת או שאין שום קשר בכלל.

בהצלחה בבדיקות הבאות!