Exploratory Data Analysis
MODBUS / TCP

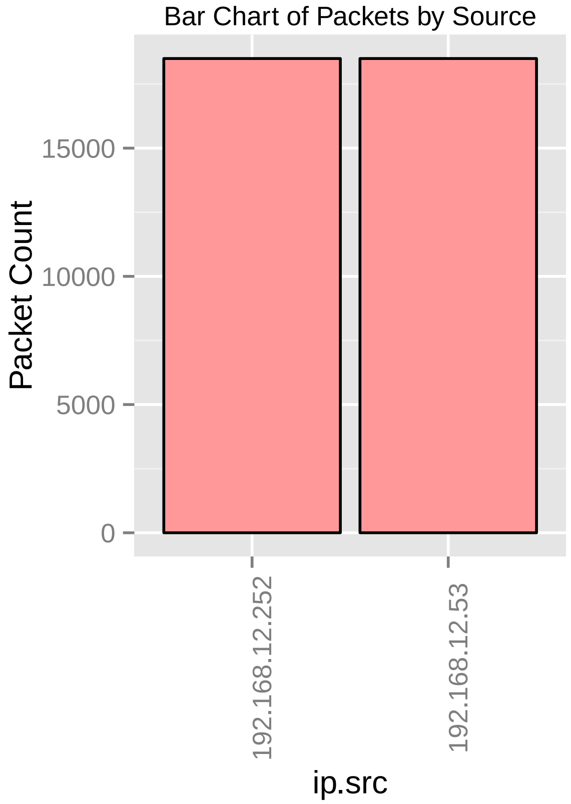
Lisa MALIPHOL

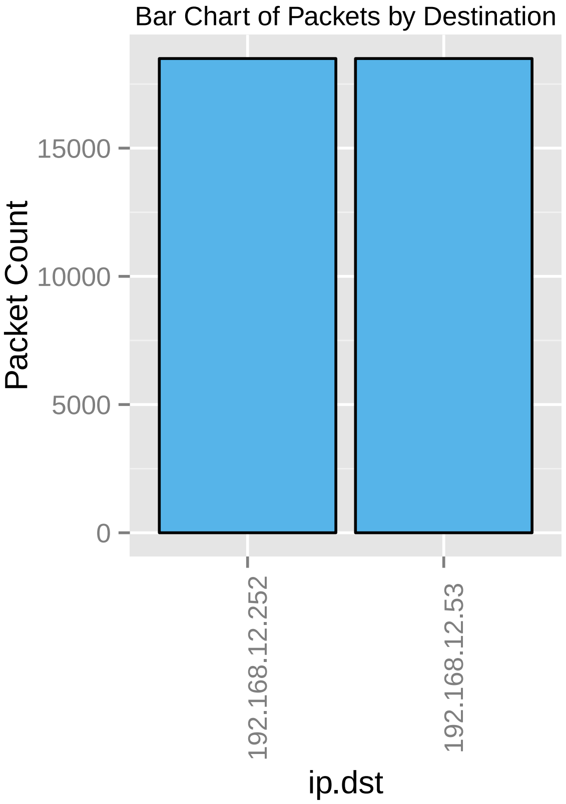
Introduction

The following analysis was done using a pcap file created from a simulation using the new SCADA simulation box under noral conditions (no attacks):

capture_sew_20150617.pcap
3.0 MB
38,082 packets 10 minutes

Packet Analysis





MODBUS/TCP responses are identified by packets having source port number 502

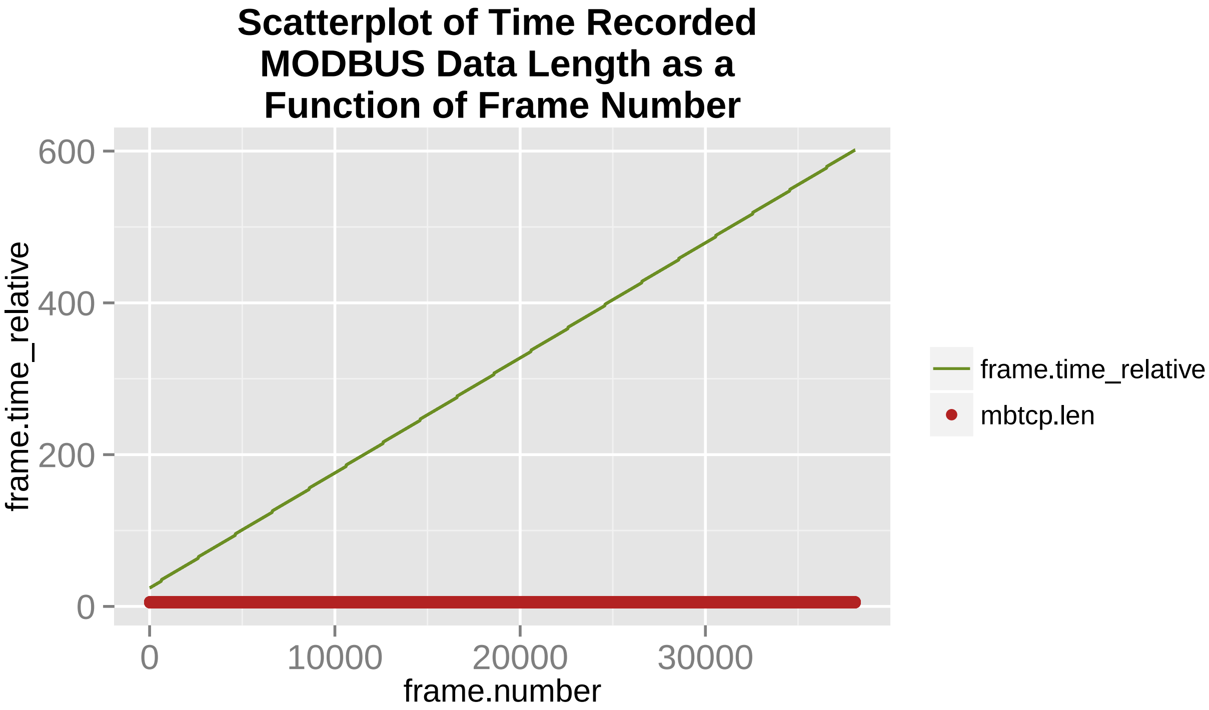
```r
summary(responses)
```

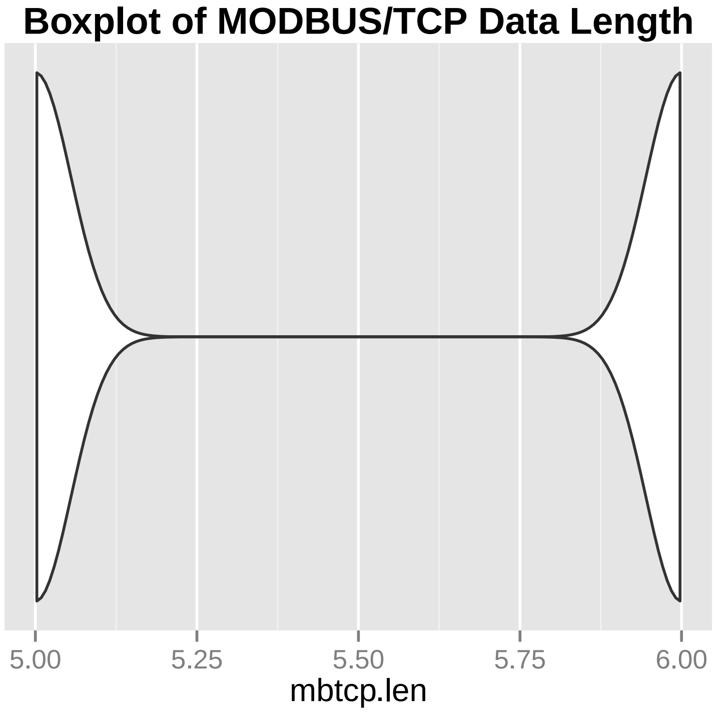
```
##   frame.number   frame.time_relative frame.time_delta_displayed
##  Min.   :    6   Min.   : 24.53      Min.   :0.001583
##  1st Qu.: 9525   1st Qu.:169.16      1st Qu.:0.011678
##  Median :19044   Median :313.81      Median :0.012367
##  Mean   :19044   Mean   :313.35      Mean   :0.011918
##  3rd Qu.:28564   3rd Qu.:457.18      3rd Qu.:0.012762
##  Max.   :38083   Max.   :601.43      Max.   :0.014795
##
##    frame.len  ip.proto  ip.version            ip.src
##  Min.   :67   6:18496   4:18496    192.168.12.252:18496
##  1st Qu.:67                        192.168.12.53 :    0
##  Median :67
##  Mean   :67
##  3rd Qu.:67
##  Max.   :67
##
##            ip.dst      mbtcp.modbus.unit_id tcp.srcport  tcp.dstport
##  192.168.12.252:    0   Min.   :1            1058:    0   1058:18496
##  192.168.12.53 :18496   1st Qu.:1            502 :18496   502 :    0
##                         Median :1
##                         Mean   :1
##                         3rd Qu.:1
##                         Max.   :1
##
##  mbtcp.prot_id mbtcp.trans_id    mbtcp.len mbtcp.modbus.func_code
##   :    0       Min.   :  0.0   Min.   :5    :    0
##  0:18496       1st Qu.: 64.0   1st Qu.:5   4:18496
##                Median :127.0   Median :5
##                Mean   :127.4   Mean   :5
##                3rd Qu.:191.0   3rd Qu.:5
##                Max.   :255.0   Max.   :5
##
##  mbtcp.modbus.reference_num mbtcp.modbus.word_cnt mbtcp.modbus.data
##   :18496                    Min.   : NA           Length:18496
##  0:    0                    1st Qu.: NA           Class :character
##  1:    0                    Median : NA           Mode  :character
##  2:    0                    Mean   :NaN
##  3:    0                    3rd Qu.: NA
##                             Max.   : NA
##                             NA's   :18496
```

MODBUS/TCP requests are identified by packets having destination port number 502

```r
summary(requests)
```

```
##   frame.number   frame.time_relative frame.time_delta_displayed
##  Min.   :    5   Min.   : 24.52      Min.   :0.000162
##  1st Qu.: 9524   1st Qu.:169.16      1st Qu.:0.000261
##  Median :19044   Median :313.80      Median :0.000303
##  Mean   :19044   Mean   :313.33      Mean   :0.009683
##  3rd Qu.:28563   3rd Qu.:457.17      3rd Qu.:0.000355
##  Max.   :38082   Max.   :601.41      Max.   :1.893315
##    frame.len  ip.proto  ip.version            ip.src
##  Min.   :68   6:18496   4:18496    192.168.12.252:    0
##  1st Qu.:68                        192.168.12.53 :18496
##  Median :68
##  Mean   :68
##  3rd Qu.:68
##  Max.   :68
##             ip.dst      mbtcp.modbus.unit_id tcp.srcport  tcp.dstport
##  192.168.12.252:18496   Min.   :1            1058:18496   1058:    0
##  192.168.12.53 :    0   1st Qu.:1            502 :    0   502 :18496
##                         Median :1
##                         Mean   :1
##                         3rd Qu.:1
##                         Max.   :1
##  mbtcp.prot_id mbtcp.trans_id    mbtcp.len mbtcp.modbus.func_code
##   :    0       Min.   :  0.0   Min.   :6    :    0
##  0:18496       1st Qu.: 64.0   1st Qu.:6   4:18496
##                Median :127.0   Median :6
##                Mean   :127.4   Mean   :6
##                3rd Qu.:191.0   3rd Qu.:6
##                Max.   :255.0   Max.   :6
##  mbtcp.modbus.reference_num mbtcp.modbus.word_cnt mbtcp.modbus.data
##   :   0                    Min.   :1             Length:18496
##  0:7616                    1st Qu.:1             Class :character
##  1:8704                    Median :1             Mode  :character
##  2:1088                    Mean   :1
##  3:1088                    3rd Qu.:1
##                            Max.   :1
```





Conversation End Points:

```
##             ip.src         ip.dst mbtcp.modbus.unit_id count
## 1:  192.168.12.53 192.168.12.252                    1 18496
## 2: 192.168.12.252  192.168.12.53                    1 18496
```

MODBUS/TCP Data[1] Analysis

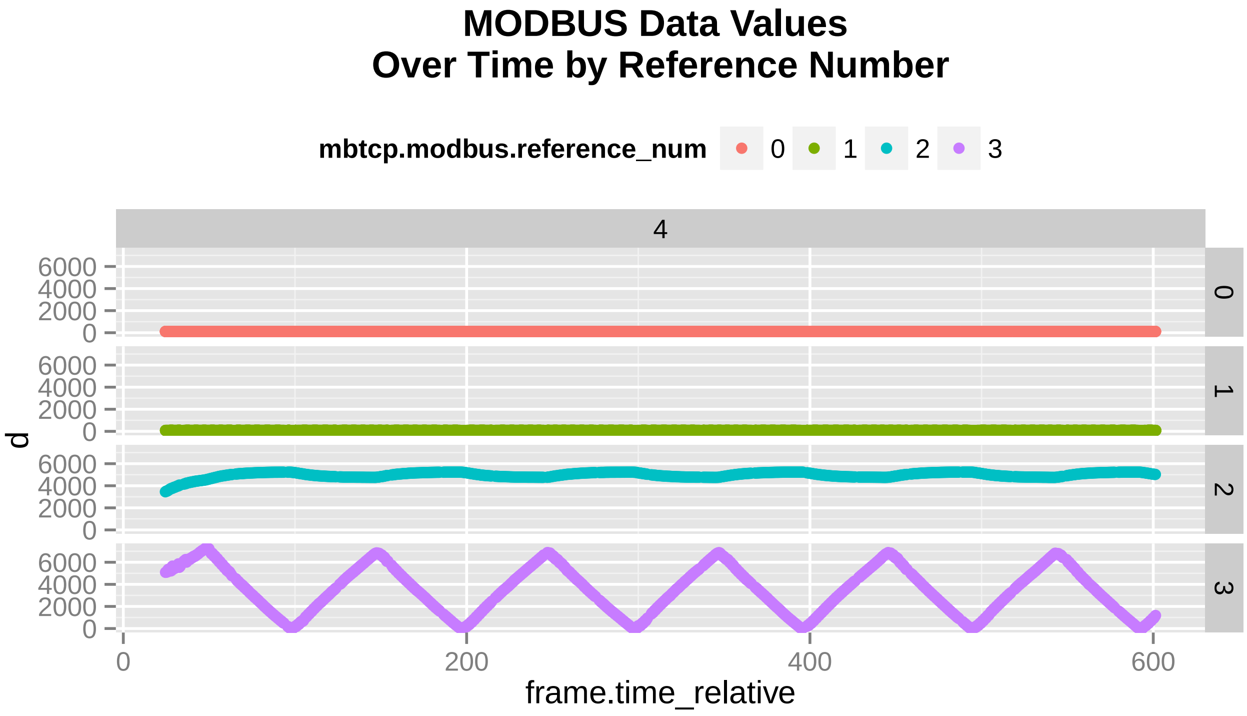
The following analysis was done over the dataset of the previous that have been merged to include the request and response of the same transaction in the same record. An additional field was created to transform **resp.data** as a numeric value.

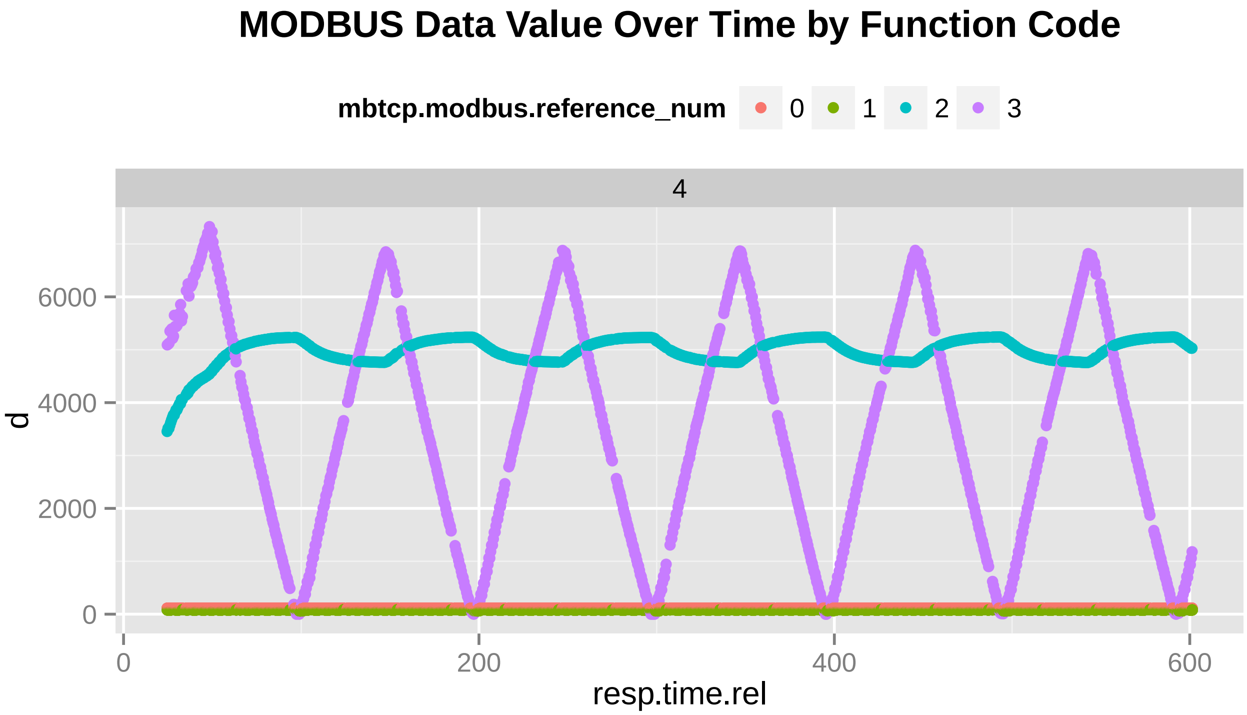
```r
summary(mergedSewDT)
```

```
##   frame.number   frame.time_relative frame.time_delta_displayed
##  Min.   :    5   Min.   : 24.52      Min.   :0.000162          
##  1st Qu.: 9524   1st Qu.:169.16      1st Qu.:0.000261          
##  Median :19044   Median :313.80      Median :0.000303          
##  Mean   :19044   Mean   :313.33      Mean   :0.009683          
##  3rd Qu.:28563   3rd Qu.:457.17      3rd Qu.:0.000355          
##  Max.   :38082   Max.   :601.41      Max.   :1.893315          
##                                                                
##    frame.len            ip.src                  ip.dst     
##  Min.   :68   192.168.12.53:18496   192.168.12.252:18496  
##  1st Qu.:68                                               
##  Median :68                                               
##  Mean   :68                                               
##  3rd Qu.:68                                               
##  Max.   :68                                               
##                                                           
##  mbtcp.modbus.unit_id tcp.srcport  tcp.dstport mbtcp.prot_id
##  1:18496              1058:18496   502:18496   0:18496      
##                                                             
##                                                             
##                                                             
##                                                             
##                                                             
##                                                             
##  mbtcp.trans_id    mbtcp.len mbtcp.modbus.func_code mbtcp.modbus.word_cnt
##  Min.   :  0.0   Min.   :6   4:18496                Min.   :1            
##  1st Qu.: 64.0   1st Qu.:6                          1st Qu.:1            
##  Median :127.0   Median :6                          Median :1            
##  Mean   :127.4   Mean   :6                          Mean   :1            
##  3rd Qu.:191.0   3rd Qu.:6                          3rd Qu.:1            
##  Max.   :255.0   Max.   :6                          Max.   :1            
##                                                                          
##  mbtcp.modbus.reference_num resp.fr.number  resp.time.rel
##  0:7616                     Min.   :    6   Min.   : 24.53
##  1:8704                     1st Qu.: 9525   1st Qu.:169.16
##  2:1088                     Median :19044   Median :313.81
##  3:1088                     Mean   :19044   Mean   :313.35
##                             3rd Qu.:28564   3rd Qu.:457.18
##                             Max.   :38083   Max.   :601.43
##                                                           
##  resp.time.delta       resp.len             resp.src    
##  Min.   :0.001583   Min.   :67   192.168.12.252:18496  
##  1st Qu.:0.011678   1st Qu.:67                         
##  Median :0.012367   Median :67                         
```

[1] https://www.wireshark.org/docs/dfref/m/mbtcp.html

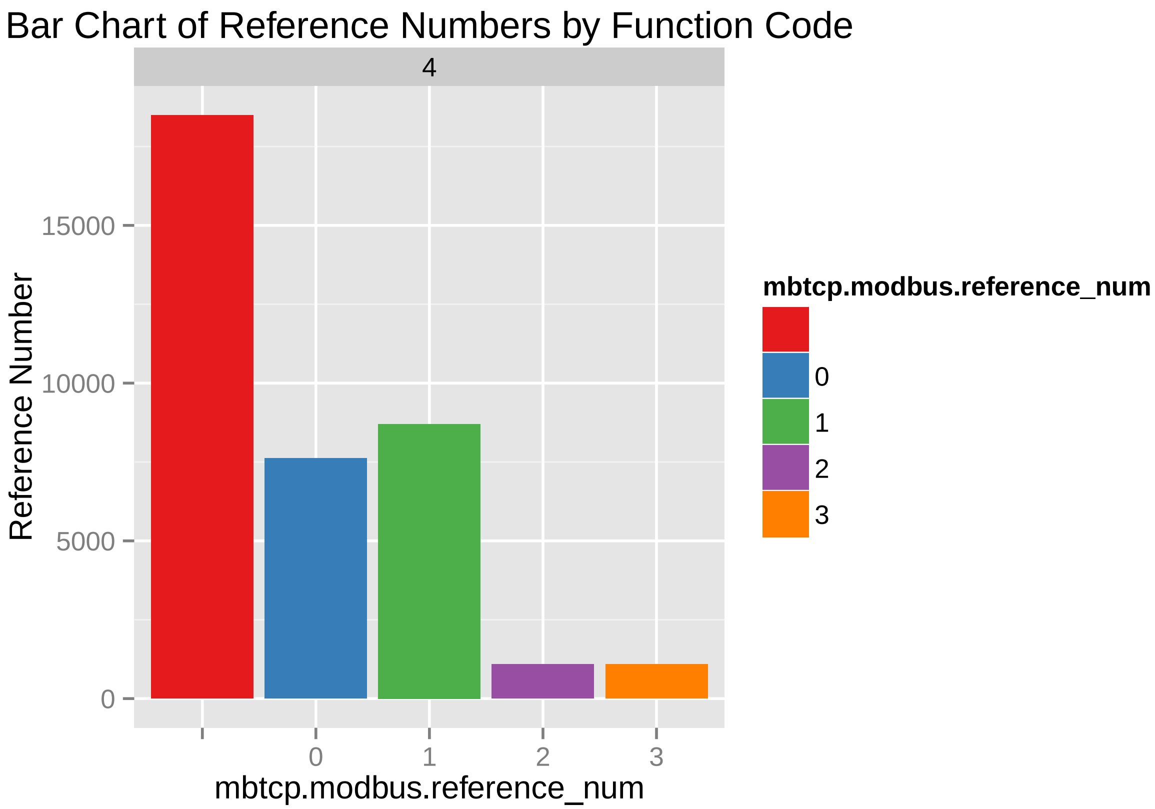
```
##  Mean   :0.011918   Mean   :67
##  3rd Qu.:0.012762   3rd Qu.:67
##  Max.   :0.014795   Max.   :67
##
##          resp.dest     resp.srcport resp.dstport resp.prot_id
##  192.168.12.53:18496   502:18496    1058:18496   0:18496
##
##
##
##
##
##
##  resp.trans_id   resp.mbcp.len resp.func.code   resp.data
##  Min.   :  0.0   Min.   :5     4:18496         00:70  :7616
##  1st Qu.: 64.0   1st Qu.:5                     00:50  :4212
##  Median :127.0   Median :5                     00:54  :4162
##  Mean   :127.4   Mean   :5                     00:40  : 331
##  3rd Qu.:191.0   3rd Qu.:5                     14:74  :  21
##  Max.   :255.0   Max.   :5                     14:70  :  15
##                                                (Other):2139
##        d
##  Min.   :   0.0
##  1st Qu.:  84.0
##  Median : 112.0
##  Mean   : 580.9
##  3rd Qu.: 112.0
##  Max.   :7327.0
##
```



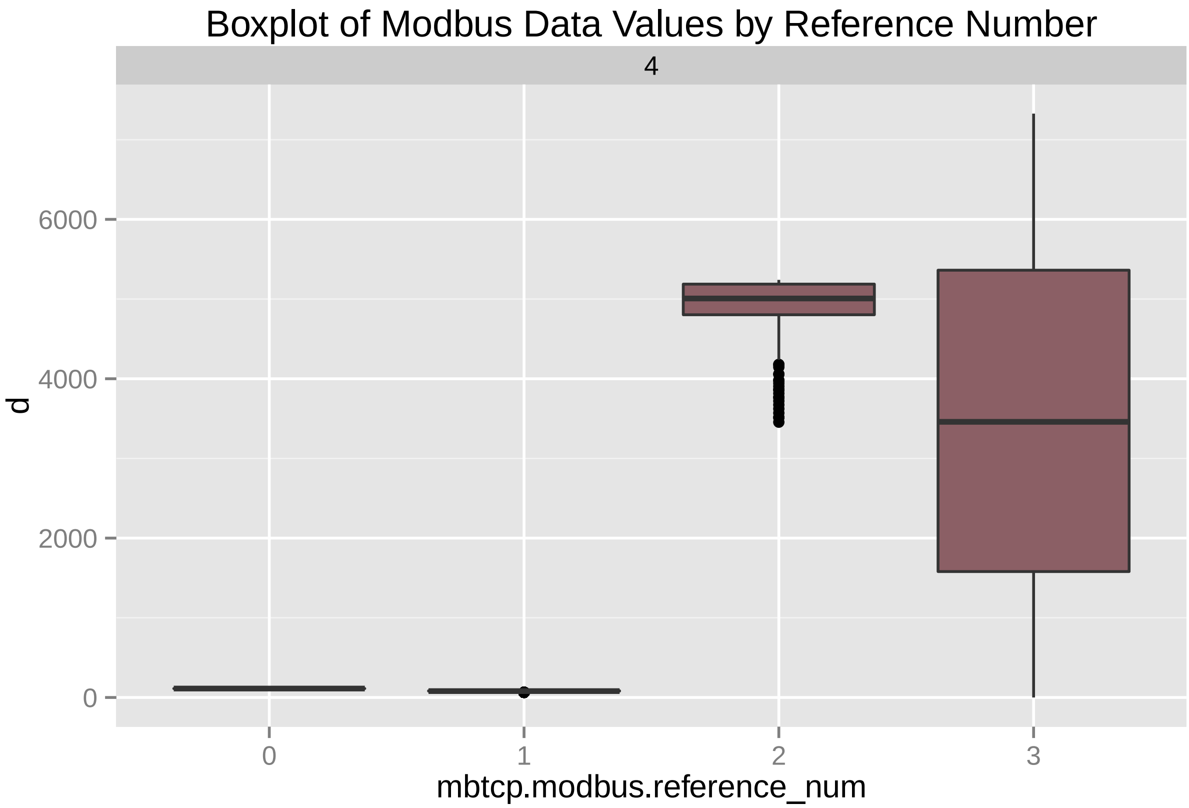


MODBUS Data Value Statistics

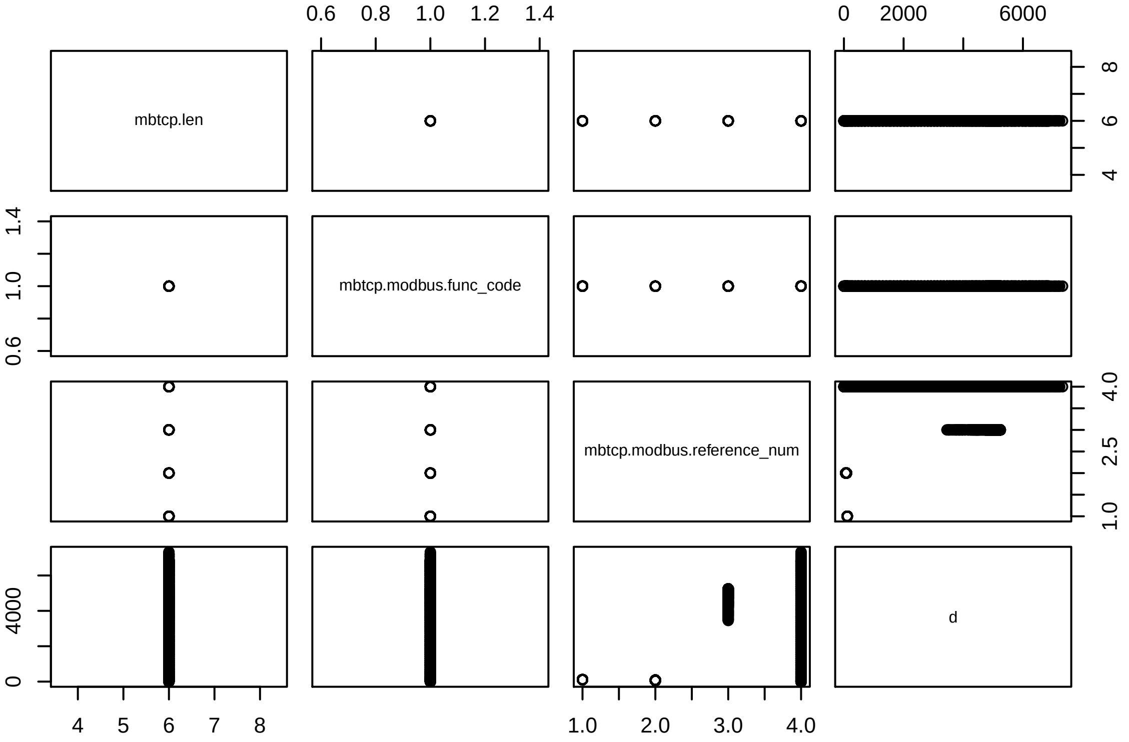
```
##    resp.func.code mbtcp.modbus.reference_num count d.min     d.mean d.max
## 1:              4                          0  7616   112  112.00000   112
## 2:              4                          1  8704    64   81.30423    84
## 3:              4                          2  1088  3455 4972.96140  5241
## 4:              4                          3  1088     0 3467.62592  7327
##           d.sd min.resp.time.rel min.resp.time.rel
## 1:    0.000000          24.53739          601.3492
## 2:    3.960659          24.58845          601.4262
## 3:  256.073630          24.52703          601.2214
## 4: 2125.525453          24.61349          601.3094
```



Bar Chart of Reference Numbers by Function Code

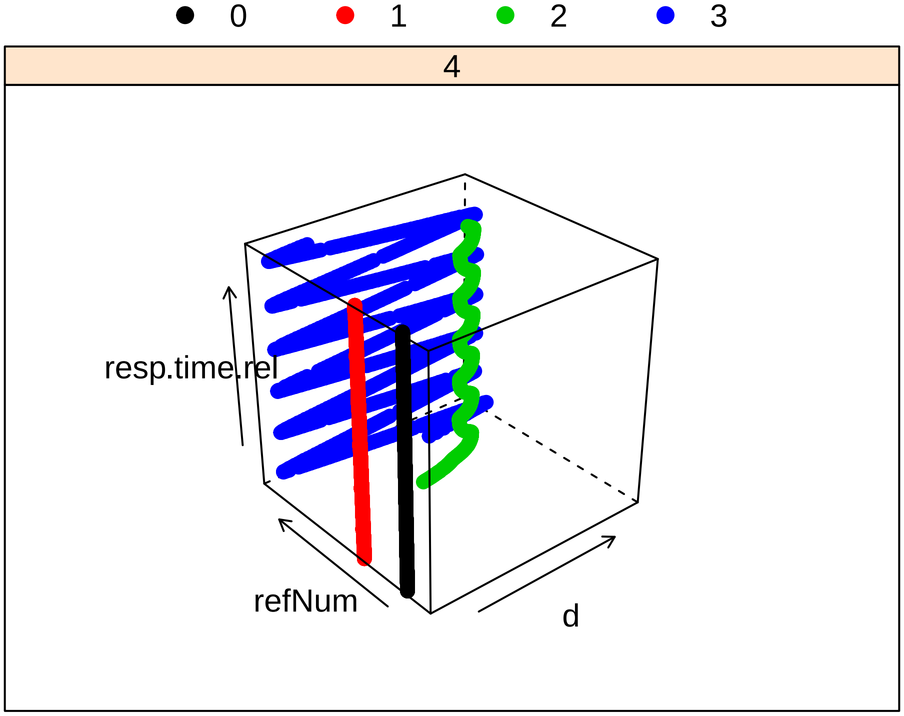


Boxplot of Modbus Data Values by Reference Number



3D Scatterplot

Reference Number, Data Value Over Time for Function Code 4


● 0
● 1
● 2
● 3
resp.time.rel
refNum
d