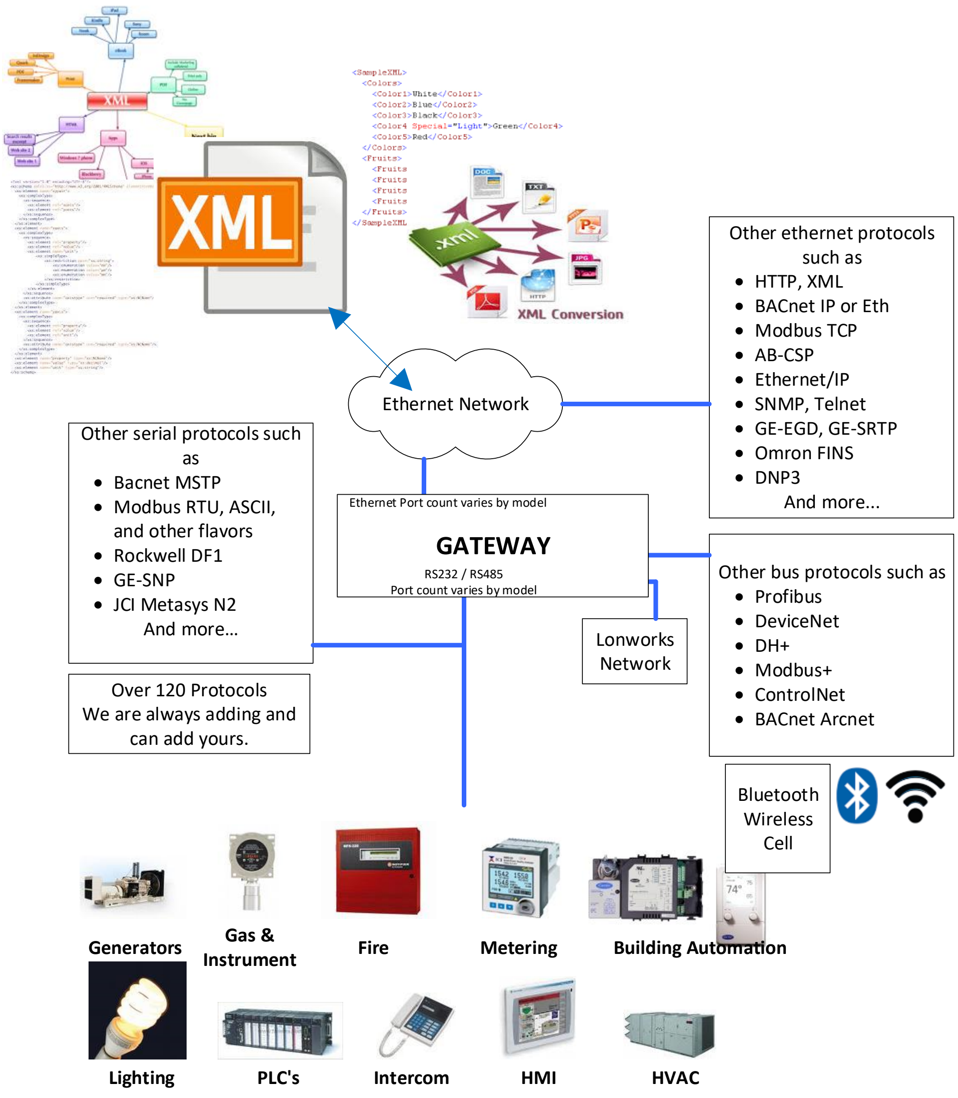
CHIPKIN

Case Study
Using XML over HTTP
to monitor and control
Using QuickServer / FieldServer products



Other ethernet protocols such as

- HTTP, XML
- BACnet IP or Eth
- Modbus TCP
- AB-CSP
- Ethernet/IP
- SNMP, Telnet
- GE-EGD, GE-SRTP
- Omron FINS
- DNP3

And more...

Other serial protocols such as

- Bacnet MSTP
- Modbus RTU, ASCII, and other flavors
- Rockwell DF1
- GE-SNP
- JCI Metasys N2

And more...

Over 120 Protocols
We are always adding and can add yours.

Ethernet Network

Ethernet Port count varies by model

GATEWAY

RS232 / RS485
Port count varies by model

Lonworks Network

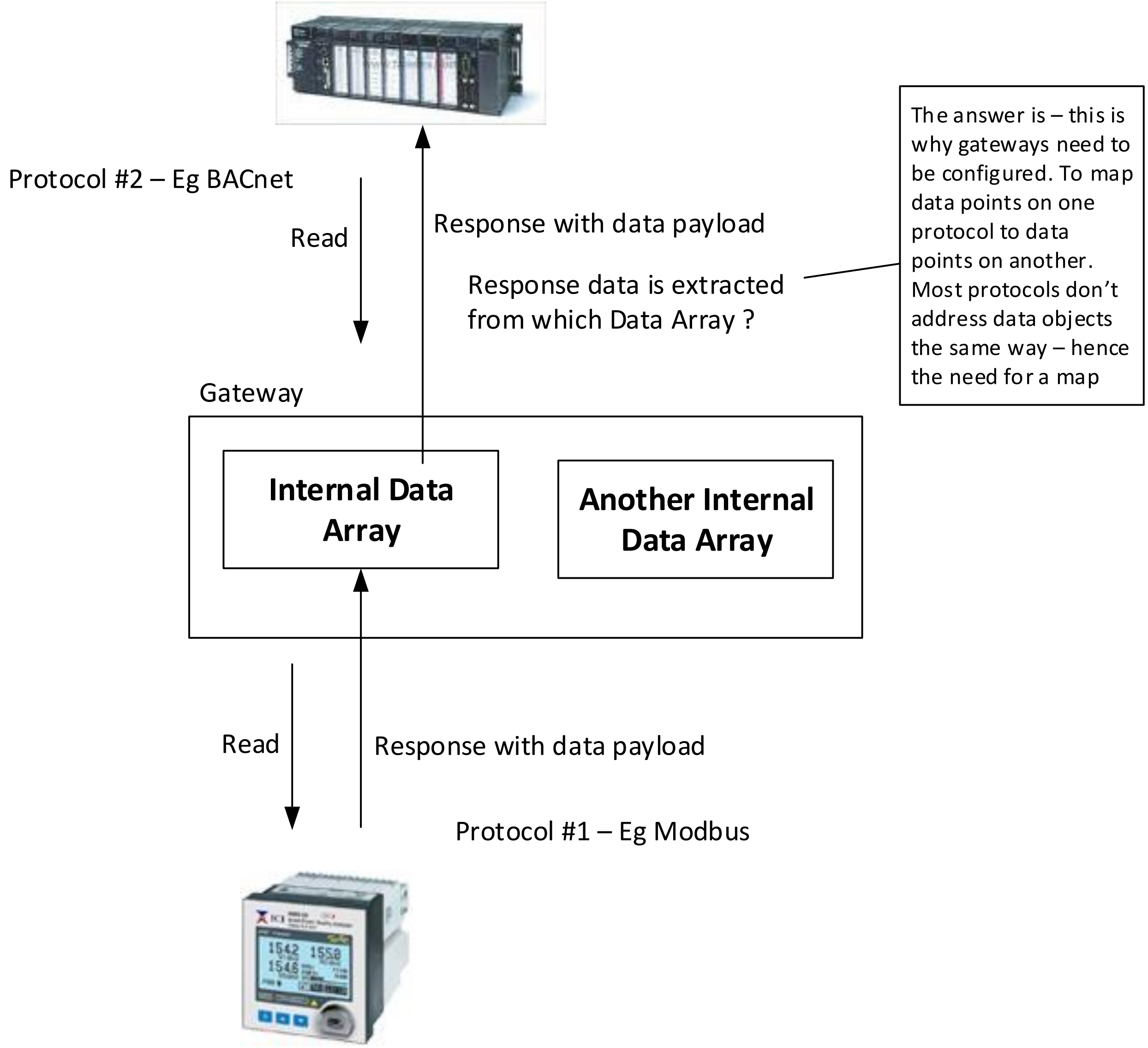
Other bus protocols such as

- Profibus
- DeviceNet
- DH+
- Modbus+
- ControlNet
- BACnet Arcnet

Bluetooth
Wireless
Cell

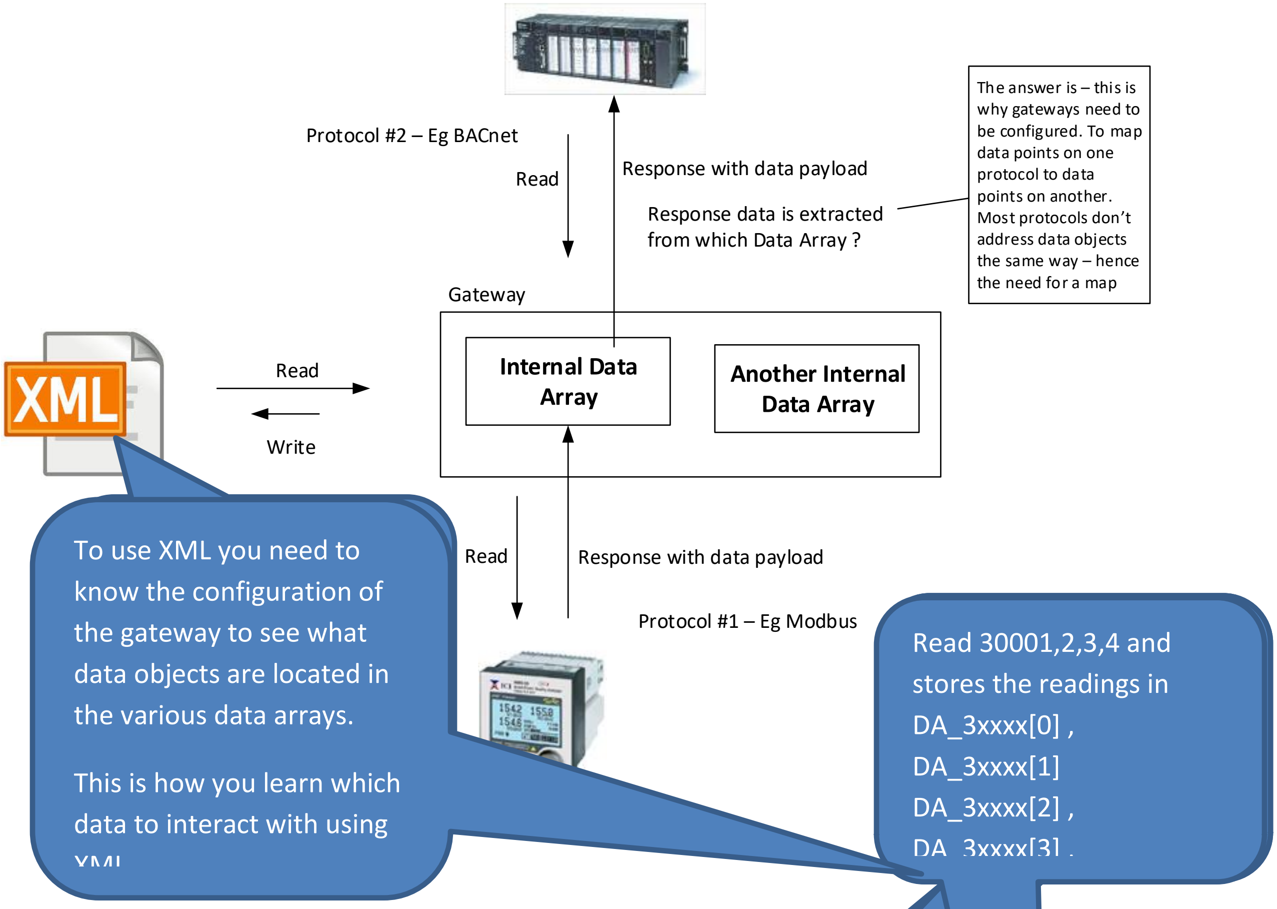
How Gateways Work – Sharing Data Using Internal Data Arrays

Different protocols address data objects differently. That is why you cant take a message from one protocol and automatically convert it to a message in another protocol. Modbus would though up its hands in despair if you asked it for Mutli_State_Input(19001) from Device 389001. BACnet has no idea what a Holding Register is. This is why gateways need configuration – a map – that maps data objects of the one protocol to data objects in another protocol. **It also means that gateways need to cache data (in Data Arrays) and that each item in storage can be identified (in the map) by two addresses – one for each protocol.**


Protocol #2 – Eg BACnet
Read
Response with data payload
Response data is extracted
from which Data Array ?
Gateway
Internal Data Array
Another Internal Data Array
Read
Response with data payload
Protocol #1 – Eg Modbus

The answer is – this is why gateways need to be configured. To map data points on one protocol to data points on another. Most protocols don't address data objects the same way – hence the need for a map

You can use XML to Read and Write this Shared Data



Protocol #2 – Eg BACnet

Read

Response with data payload

Response data is extracted from which Data Array ?

The answer is – this is why gateways need to be configured. To map data points on one protocol to data points on another. Most protocols don't address data objects the same way – hence the need for a map

Gateway

Internal Data Array

Another Internal Data Array

Read

Write

Read

Response with data payload

Protocol #1 – Eg Modbus

To use XML you need to know the configuration of the gateway to see what data objects are located in the various data arrays.

This is how you learn which data to interact with using XML

Read 30001,2,3,4 and stores the readings in DA_3xxxx[0] , DA_3xxxx[1] DA_3xxxx[2] , DA_3xxxx[3] ,

```
Connections,

Adapter ,Protocol,

N1      ,Modbus/TCP,



Nodes,

Node_Name      ,Node_ID  ,Protocol    ,Adapter    ,Address     ,Poll_Delay

EnergyMeter     ,1         ,Modbus/TCP ,N1         ,192.168.1.6 ,0.001



Tasks

Task_Name ,Data_Array_Name ,Data_Array_Offset ,Function ,Node_Name       ,Address ,Length,
```

XML Read Request

http://192.168.1.5/data_arrays.xml?name=FIRE1234.0:100

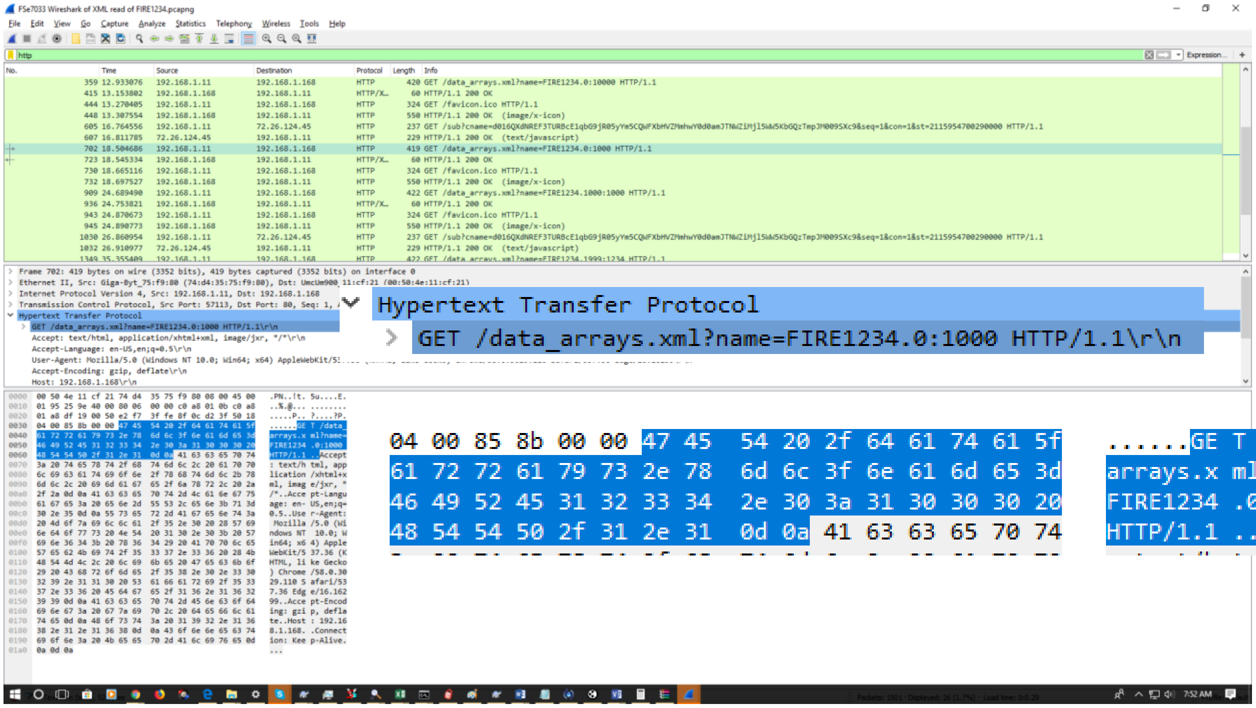
192.168.1.5 = Remote Server IP Address, Configurable from settings file.

FIRE1234 = DataArray name in gateway

0:100 = x:y

X = Offset into DataArray

y = Number of Items to read from DataArray



FSe7033 Wireshark of XML read of FIRE1234.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…

```
No.      Time         Source          Destination     Protocol  Length Info
     359 12.933076    192.168.1.11    192.168.1.168   HTTP      420 GET /data_arrays.xml?name=FIRE1234.0:10000 HTTP/1.1
     415 13.153802    192.168.1.168   192.168.1.11    HTTP/X…    60 HTTP/1.1 200 OK
     444 13.270405    192.168.1.11    192.168.1.168   HTTP      324 GET /favicon.ico HTTP/1.1
     448 13.307554    192.168.1.168   192.168.1.11    HTTP      550 HTTP/1.1 200 OK  (image/x-icon)
     605 16.764556    192.168.1.11    72.26.124.45    HTTP      237 GET /sub?cname=d016QXdNREF3TURBcE1qbG9jR05yYm5CQWFXbHVZMmhwY0d0amJTNWZiMjl5WW5KbGQzTmpJM009SXc9&seq=1&con=1&st=211595470029000 HTTP/1.1
     607 16.811785    72.26.124.45    192.168.1.11    HTTP      229 HTTP/1.1 200 OK  (text/javascript)
     702 18.504686    192.168.1.11    192.168.1.168   HTTP      419 GET /data_arrays.xml?name=FIRE1234.0:1000 HTTP/1.1
     723 18.545334    192.168.1.168   192.168.1.11    HTTP/X…    60 HTTP/1.1 200 OK
     730 18.665116    192.168.1.11    192.168.1.168   HTTP      324 GET /favicon.ico HTTP/1.1
     732 18.697527    192.168.1.168   192.168.1.11    HTTP      550 HTTP/1.1 200 OK  (image/x-icon)
     909 24.689490    192.168.1.11    192.168.1.168   HTTP      422 GET /data_arrays.xml?name=FIRE1234.1000:1000 HTTP/1.1
     936 24.753821    192.168.1.168   192.168.1.11    HTTP/X…    60 HTTP/1.1 200 OK
     943 24.870673    192.168.1.11    192.168.1.168   HTTP      324 GET /favicon.ico HTTP/1.1
     945 24.890773    192.168.1.168   192.168.1.11    HTTP      550 HTTP/1.1 200 OK  (image/x-icon)
    1030 26.860954    192.168.1.11    72.26.124.45    HTTP      237 GET /sub?cname=d016QXdNREF3TURBcE1qbG9jR05yYm5CQWFXbHVZMmhwY0d0amJTNWZiMjl5WW5KbGQzTmpJM009SXc9&seq=1&con=1&st=211595470029000 HTTP/1.1
    1032 26.910977    72.26.124.45    192.168.1.11    HTTP      229 HTTP/1.1 200 OK  (text/javascript)
    1349 35.355409    192.168.1.11    192.168.1.168   HTTP      422 GET /data_arrays.xml?name=FIRE1234.1999:1234 HTTP/1.1
```

```
> Frame 702: 419 bytes on wire (3352 bits), 419 bytes captured (3352 bits) on interface 0
> Ethernet II, Src: Giga-Byt_75:f9:80 (74:d4:35:75:f9:80), Dst: UmcUm900_11:cf:21 (00:50:4e:11:cf:21)
> Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.1.168
> Transmission Control Protocol, Src Port: 57113, Dst Port: 80, Seq: 1, A
v Hypertext Transfer Protocol
  > GET /data_arrays.xml?name=FIRE1234.0:1000 HTTP/1.1\r\n
    Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/53
    Accept-Encoding: gzip, deflate\r\n
    Host: 192.168.1.168\r\n
```

```
0000  00 50 4e 11 cf 21 74 d4  35 75 f9 80 08 00 45 00   .PN..!t. 5u....E.
0010  01 95 25 9e 40 00 80 06  00 00 c0 a8 01 0b c0 a8   ..%.@... ........
0020  01 a8 df 19 00 50 e2 f7  3f fe 8f 0c d2 3f 50 18   .....P.. ?....?P.
0030  04 00 85 8b 00 00 47 45  54 20 2f 64 61 74 61 5f   ......GE T /data_
0040  61 72 72 61 79 73 2e 78  6d 6c 3f 6e 61 6d 65 3d   arrays.x ml?name=
0050  46 49 52 45 31 32 33 34  2e 30 3a 31 30 30 30 20   FIRE1234 .0:1000 
0060  48 54 54 50 2f 31 2e 31  0d 0a 41 63 63 65 70 74   HTTP/1.1 ..Accept
0070  3a 20 74 65 78 74 2f 68  74 6d 6c 2c 20 61 70 70   : text/h tml, app
0080  6c 69 63 61 74 69 6f 6e  2f 78 68 74 6d 6c 2b 78   lication /xhtml+x
0090  6d 6c 2c 20 69 6d 61 67  65 2f 6a 78 72 2c 20 2a   ml, imag e/jxr, *
00a0  2f 2a 0d 0a 41 63 63 65  70 74 2d 4c 61 6e 67 75   /*..Acce pt-Langu
00b0  61 67 65 3a 20 65 6e 2d  55 53 2c 65 6e 3b 71 3d   age: en- US,en;q=
00c0  30 2e 35 0d 0a 55 73 65  72 2d 41 67 65 6e 74 3a   0.5..Use r-Agent:
00d0  20 4d 6f 7a 69 6c 6c 61  2f 35 2e 30 20 28 57 69    Mozilla /5.0 (Wi
00e0  6e 64 6f 77 73 20 4e 54  20 31 30 2e 30 3b 20 57   ndows NT  10.0; W
00f0  69 6e 36 34 3b 20 78 36  34 29 20 41 70 70 6c 65   in64; x6 4) Apple
0100  57 65 62 4b 69 74 2f 35  33 37 2e 33 36 20 28 4b   WebKit/5 37.36 (K
0110  48 54 4d 4c 2c 20 6c 69  6b 65 20 47 65 63 6b 6f   HTML, li ke Gecko
0120  29 20 43 68 72 6f 6d 65  2f 35 38 2e 30 2e 33 30   ) Chrome /58.0.30
0130  32 39 2e 31 31 30 20 53  61 66 61 72 69 2f 35 33   29.110 S afari/53
0140  37 2e 33 36 20 45 64 67  65 2f 31 36 2e 31 36 32   7.36 Edg e/16.162
0150  39 39 0d 0a 41 63 63 65  70 74 2d 45 6e 63 6f 64   99..Acce pt-Encod
0160  69 6e 67 3a 20 67 7a 69  70 2c 20 64 65 66 6c 61   ing: gzi p, defla
0170  74 65 0d 0a 48 6f 73 74  3a 20 31 39 32 2e 31 36   te..Host : 192.16
0180  38 2e 31 2e 31 36 38 0d  0a 43 6f 6e 6e 65 63 74   8.1.168. .Connect
0190  69 6f 6e 3a 20 4b 65 65  70 2d 41 6c 69 76 65 0d   ion: Kee p-Alive.
01a0  0a 0d 0a                                          ...
```

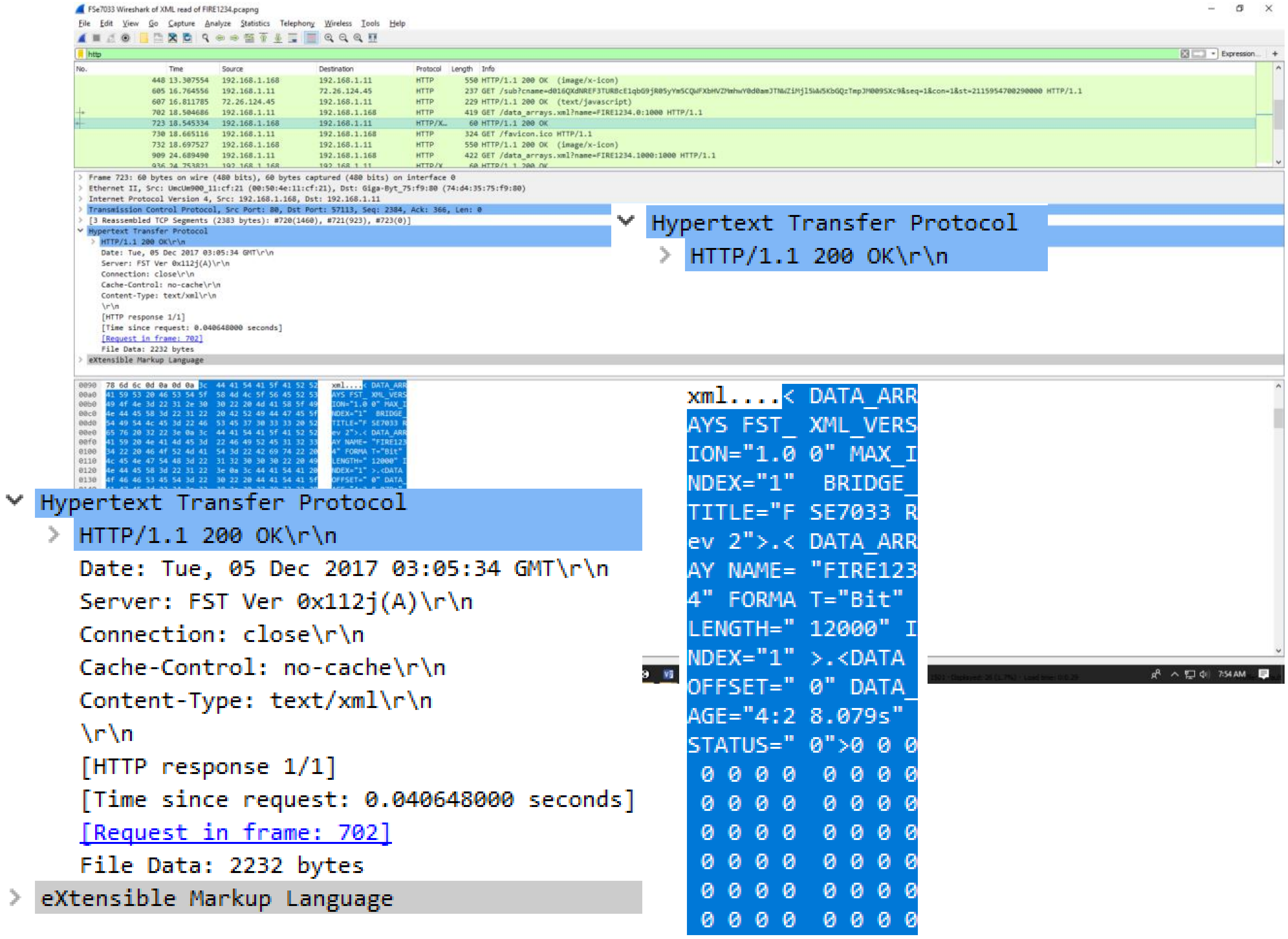
```
v Hypertext Transfer Protocol
  > GET /data_arrays.xml?name=FIRE1234.0:1000 HTTP/1.1\r\n
```

```
04 00 85 8b 00 00 47 45  54 20 2f 64 61 74 61 5f   ......GE T /data_
61 72 72 61 79 73 2e 78  6d 6c 3f 6e 61 6d 65 3d   arrays.x ml?name=
46 49 52 45 31 32 33 34  2e 30 3a 31 30 30 30 20   FIRE1234 .0:1000
48 54 54 50 2f 31 2e 31  0d 0a 41 63 63 65 70 74   HTTP/1.1 ..Accept
```

XML Write Response

This is the response for the above request example

```
<DATA_ARRAYS FST_XML_VERSION=”1.00” MAX_INDEX=”1” BRIDGE_TITLE=”SBT FSI SERVER”>

        <DATA_ARRAY NAME=”FIRE1234” FORMAT=”BIT” LENGTH=”100” INDEX=”1”>

                <DATA OFFSET=”0” DATA_AGE=”3:00:39.36.123s” STATUS=”0” >

0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 </DATA>

        </DATA_ARRAY>

<DATA_ARRAYS>
```



FSe7033 Wireshark of XML read of FIRE1234.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…

```
http

No.   Time        Source          Destination     Protocol  Length Info
  448 13.307554   192.168.1.168   192.168.1.11    HTTP       550 HTTP/1.1 200 OK  (image/x-icon)
  605 16.764556   192.168.1.11    72.26.124.45    HTTP       237 GET /sub?cname=d016QXdNREF3TURBcE1qbG9jR05yYm5CQWFXbHVZMmhwY0d0amJTNWZiMjl5WW5KbGQzTmpJM009SXc9&seq=1&con=1&st=2115954700290000 HTTP/1.1
  607 16.811785   72.26.124.45    192.168.1.11    HTTP       229 HTTP/1.1 200 OK  (text/javascript)
  702 18.504686   192.168.1.11    192.168.1.168   HTTP       419 GET /data_arrays.xml?name=FIRE1234.0:1000 HTTP/1.1
  723 18.545334   192.168.1.168   192.168.1.11    HTTP/X…     60 HTTP/1.1 200 OK
  730 18.665116   192.168.1.11    192.168.1.168   HTTP       324 GET /favicon.ico HTTP/1.1
  732 18.697527   192.168.1.168   192.168.1.11    HTTP       550 HTTP/1.1 200 OK  (image/x-icon)
  909 24.689490   192.168.1.11    192.168.1.168   HTTP       422 GET /data_arrays.xml?name=FIRE1234.1000:1000 HTTP/1.1
  936 24.753821   192.168.1.168   192.168.1.11    HTTP/X      60 HTTP/1.1 200 OK

> Frame 723: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: UmcUm900_11:cf:21 (00:50:4e:11:cf:21), Dst: Giga-Byt_75:f9:80 (74:d4:35:75:f9:80)
> Internet Protocol Version 4, Src: 192.168.1.168, Dst: 192.168.1.11
> Transmission Control Protocol, Src Port: 80, Dst Port: 57113, Seq: 2384, Ack: 366, Len: 0
> [3 Reassembled TCP Segments (2383 bytes): #720(1460), #721(923), #723(0)]
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Tue, 05 Dec 2017 03:05:34 GMT\r\n
    Server: FST Ver 0x112j(A)\r\n
    Connection: close\r\n
    Cache-Control: no-cache\r\n
    Content-Type: text/xml\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.040648000 seconds]
    [Request in frame: 702]
    File Data: 2232 bytes
> eXtensible Markup Language

0090  78 6d 6c 0d 0a 0d 0a 3c  44 41 54 41 5f 41 52 52   xml....< DATA_ARR
00a0  41 59 53 20 46 53 54 5f  58 4d 4c 5f 56 45 52 53   AYS FST_ XML_VERS
00b0  49 4f 4e 3d 22 31 2e 30  30 22 20 4d 41 58 5f 49   ION="1.0 0" MAX_I
00c0  4e 44 45 58 3d 22 31 22  20 42 52 49 44 47 45 5f   NDEX="1"  BRIDGE_
00d0  54 49 54 4c 45 3d 22 46  53 45 37 30 33 33 20 52   TITLE="F SE7033 R
00e0  65 76 20 32 22 3e 0a 3c  44 41 54 41 5f 41 52 52   ev 2">.< DATA_ARR
00f0  41 59 20 4e 41 4d 45 3d  22 46 49 52 45 31 32 33   AY NAME= "FIRE123
0100  34 22 20 46 4f 52 4d 41  54 3d 22 42 69 74 22 20   4" FORMA T="Bit"
0110  4c 45 4e 47 54 48 3d 22  31 32 30 30 30 22 20 49   LENGTH=" 12000" I
0120  4e 44 45 58 3d 22 31 22  3e 0a 3c 44 41 54 41 20   NDEX="1" >.<DATA
0130  4f 46 46 53 45 54 3d 22  30 22 20 44 41 54 41 5f   OFFSET=" 0" DATA_
```

```
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n

v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Tue, 05 Dec 2017 03:05:34 GMT\r\n
    Server: FST Ver 0x112j(A)\r\n
    Connection: close\r\n
    Cache-Control: no-cache\r\n
    Content-Type: text/xml\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.040648000 seconds]
    [Request in frame: 702]
    File Data: 2232 bytes
> eXtensible Markup Language

xml....< DATA_ARR
AYS FST_ XML_VERS
ION="1.0 0" MAX_I
NDEX="1"  BRIDGE_
TITLE="F SE7033 R
ev 2">.< DATA_ARR
AY NAME= "FIRE123
4" FORMA T="Bit"
LENGTH=" 12000" I
NDEX="1" >.<DATA
OFFSET=" 0" DATA_
AGE="4:2 8.079s"
STATUS=" 0">0 0 0
 0 0 0 0  0 0 0 0
 0 0 0 0  0 0 0 0
 0 0 0 0  0 0 0 0
 0 0 0 0  0 0 0 0
 0 0 0 0  0 0 0 0
 0 0 0 0  0 0 0 0
```