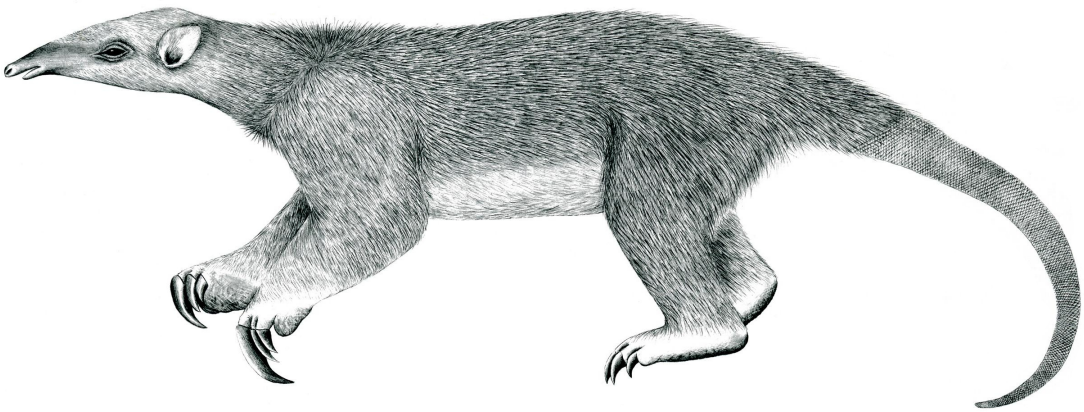
Tranalyzer2

modbus

Modbus



Tranalyzer Development Team

Contents

1 modbus

1.1 Description

The modbus plugin analyzes Modbus traffic.

1.2 Configuration Flags

The following flags can be used to control the output of the plugin:

Name	Default	Description
MB_DEBUG	0	Activate debug output
MB_FE_FRMT	0	Function/Exception codes representation: 0: hex, 1: int
MB_NUM_FUNC	0	Number of function codes to store (0 to hide modbusFC)
MB_UNIQ_FUNC	0	Aggregate multiply defined function codes
MB_NUM_FEX	0	Number of function codes causing exceptions to store (0 to hide modbusFEx)
MB_UNIQ_FEX	0	Aggregate multiply defined function codes causing exceptions
MB_NUM_EX	0	Number of exception codes to store (0 to hide modbusExC)
MB_UNIQ_EX	0	Aggregate multiply defined exception codes

1.3 Flow File Output

The modbus plugin outputs the following columns:

Column	Type	Description	Flags
modbusStat	H16	Status	
modbusUID	U8	Unit identifier	
modbusNPkts	U32	Number of Modbus packets	
modbusNumEx	U16	Number of exceptions	
modbusFCBF	H64	Aggregated function codes	
modbusFC	RH8	List of function codes	MB_NUM_FUNC>0
modbusFExBF	H64	Aggregated function codes which caused exceptions	
modbusFEx	RH8	List of function codes which caused exceptions	MB_NUM_FEX>0
modbusExCBF	H16	Aggregated exception codes	
modbusExC	RH8	List of exception codes	MB_NUM_EX>0

1.3.1 modbusStat

The `modbusStat` column is to be interpreted as follows:

modbusStat	Description
0x0001	Flow is Modbus
0x0002	Non-modbus protocol identifier
0x0004	Unknown function code
0x0008	Unknown exception code
0x0010	Multiple unit identifiers
0x0020	—
0x0040	—
0x0080	—
0x0100	List of function codes truncated... increase `MB_NUM_FUNC`
0x0200	List of function codes which caused exceptions truncated... increase `MB_NUM_FEX`
0x0400	List of exception codes truncated... increase `MB_NUM_EX`
0x0800	—
0x1000	—
0x2000	—
0x4000	Snapped packet
0x8000	Malformed packet

1.3.2 modbusFC and modbusFCBF

The `modbusFC` and `modbusFCBF` columns are to be interpreted as follows:

modbusFC	modbusFCBF	Description
1 = 0x01	0x0000 0000 0000 0002	Read Coils
2 = 0x02	0x0000 0000 0000 0004	Read Discrete Inputs
3 = 0x03	0x0000 0000 0000 0008	Read Multiple Holding Registers
4 = 0x04	0x0000 0000 0000 0010	Read Input Registers
5 = 0x05	0x0000 0000 0000 0020	Write Single Coil
6 = 0x06	0x0000 0000 0000 0040	Write Single Holding Register
7 = 0x07	0x0000 0000 0000 0080	Read Exception Status
8 = 0x08	0x0000 0000 0000 0100	Diagnostic
11 = 0x0b	0x0000 0000 0000 0800	Get Com Event Counter
12 = 0x0c	0x0000 0000 0000 1000	Get Com Event Log
15 = 0x0f	0x0000 0000 0000 8000	Write Multiple Coils
16 = 0x10	0x0000 0000 0001 0000	Write Multiple Holding Registers
17 = 0x11	0x0000 0000 0002 0000	Report Slave ID

modbusFC	modbusFCBF	Description
20 = 0x14	0x0000 0000 0010 0000	Read File Record
21 = 0x15	0x0000 0000 0020 0000	Write File Record
22 = 0x16	0x0000 0000 0040 0000	Mask Write Register
23 = 0x17	0x0000 0000 0080 0000	Read/Write Multiple Registers
24 = 0x18	0x0000 0000 0100 0000	Read FIFO Queue
43 = 0x2b	0x0000 0800 0000 0000	Read Decide Identification

1.3.3 modbusFEx and modbusFExBF

The modbusFEx and modbusFExBF columns are to be interpreted as modbusFC and modbusFCBF, respectively.

1.3.4 modbusExC and modbusExCBF

The modbusExC and modbusExCBF column are to be interpreted as follows:

modbusExC	modbusExCBF	Description
1 = 0x01	0x0002	Illegal function code
2 = 0x02	0x0004	Illegal data address
3 = 0x03	0x0008	Illegal data value
4 = 0x04	0x0010	Slave device failure
5 = 0x05	0x0020	Acknowledge
6 = 0x06	0x0040	Slave device busy
7 = 0x07	0x0080	Negative acknowledge
8 = 0x08	0x0100	Memory parity error
10 = 0x0a	0x0400	Gateway path unavailable
11 = 0x0b	0x0800	Gateway target device failed to respond

1.4 Packet File Output

In packet mode (-s option), the modbus plugin outputs the following columns:

Column	Type	Description	Flags
mbTranId	U16	Transaction Identifier	
mbProtId	U16	Protocol Identifier	
mbLen	U16	Length	
mbUnitId	U8	Unit identifier	
mbFuncCode	H8	Function code	MB_FE_FRMT=0
mbFuncCode	U8	Function code	MB_FE_FRMT=1

1.4.1 mbFuncCode

If `mbFuncCode` column is to be interpreted as follows:

mbFuncCode	Description
< 128 `(=0x80)`	refer to modbusFC and modbusFCBF
≥ 128 `(=0x80)`	subtract 128 (=`0x80`) and refer to modbusFEx and modbusFExBF

1.5 Monitoring Output

In monitoring mode, the modbus plugin outputs the following columns:

Column	Type	Description	Flags
`modbusNPkts`	U64	Number of Modbus packets	
`modbusStat`	H16	Status	

1.6 Plugin Report Output

The following information is reported:

- Aggregated `modbusStat`
- Number of Modbus packets