USB Protocol Analyzer

User's Guide and User's Reference

Genoa Technology, Inc.
5401 Tech Circle
Moorpark, CA 93021

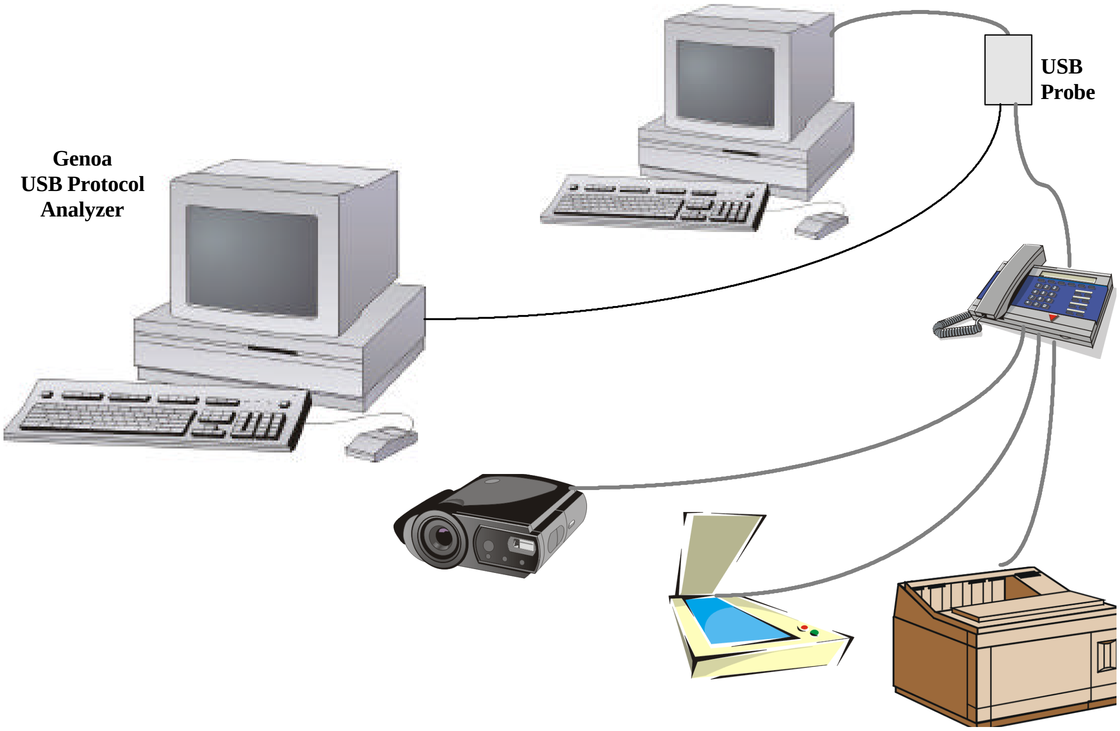
User's Guide 1

User's Guide

General

Genoa Technology's USB Protocol Analyzer was developed to aid in the diagnosis of USB Protocol non-compliances. Using a proprietary USB Probe for bus signal conditioning and a Capture Board for data acquisition, the USB Protocol Analyzer decodes signal-level information into USB events, packets, transactions, frames, and data, while checking for compliance to USB Specification 1.0.

The USB Protocol Analyzer program runs under Windows 95 or Windows NT on a PC hosting the capture board in a full ISA slot.



The following is the list of features the Protocol Analyzer provides:

- ♦ non-intrusive probing of USB bus signals, on any branch of the bus: root, non-root, full speed, low speed
- ♦ programmable capture parameters:
    - capture size 128k .. 32M acquisitions
    - acquisition offset: 0..100%
    - record idle ON/OFF option
    - 22 trigger conditions
- ♦ programmable analysis parameters:
    - max. number of signaling errors: 10..500
    - max. number of packet errors: 10..500

- max. number of transaction errors: 10..500
  - max. number of frame errors: 10..500
  - targets: packets; packets and transactions; packets, transaction and frames
  - statistics ON/OFF
- powerful USB analysis:
  - 11 types of detectable signaling errors
  - 11 types of detectable packet errors
  - 168 types of detectable transaction errors
  - 5 types of detectable frame errors
- USB traffic displayed on three layers: events, transactions, data, with the preservation of the traffic focus when switching between layers
- display options:
  - filters for traffic items, frame range, pipes
  - user assigned colors for traffic items, trigger marker, and reference marker
- timing measurements on Event layer:
  - event duration
  - relative time to trigger
  - relative time to reference (user settable)
  - relative time to start
- decoding of standard requests on Transaction layer
- export traffic commands:
  - in text files for event and transaction traffic
  - in binary files for pipe data
- search commands for:
  - events
  - transactions
  - data
  - frames
- goto commands:
  - trigger
  - event reference
  - event
  - packet
  - transaction
- statistics data for
  - events
  - transaction
  - frames
- context sensitive help
- optional use of HP16555A logic analyzer board to get the waveform of USB bus
- demo traffic files to illustrate the error types, and finding protocol errors

The max. capture size is 32M acquisitions. In trying to convert this into a capture time, there are two extreme situations:

- the minimum capture time is reached when each frame transfers 0s only
- the maximum capture time is reached when the traffic contains SOF tokens only

In the first case, each frame will provide 12000 acquisitions. Therefore 32M acquisitions will represent a capture time of 2.67s.

In the second case, most of the acquisitions are caused by the time stamp overflow, which happens each us. Therefore 32M acquisitions will represent a capture time of 32s.

In reality, for large captures, the number of 0s is close to the number of 1s. Supposing that each acquisition transfers one 0 followed by a 1, for a highly loaded frame that means about 6000 acquisitions or 1500 bytes. Therefore a 32M capture will represent 8M of USB bytes. It is reasonable to assume that in real life, a 32M capture may provide up to 8M of USB bytes and a capture time of about 6s.

Getting Started

List of deliverables

Item	Qty	Type	Description	Cable Labels	Genoa P/N
1	1	Assembly	USB Probe		99001
2	1	Assembly	USB ISA Capture Board		99002
3	1	Cable	Probe Trigger Adapter, 10”		18018
4	1	Cable	USB Probe to Capture Board	Probe to Capture	17180
5	1	Cable	USB Series A, 12”		18020
6	1	Document	User’ Guide and User’s Reference		USB101
7	2	3.5” disk	USB Protocol Analyzer program		USB101

System Requirements

IBM compatible PC
OS: Windows 95 or Windows NT
SVGA 800/600 or better, mouse, 10MB hard disk room, 16MB memory

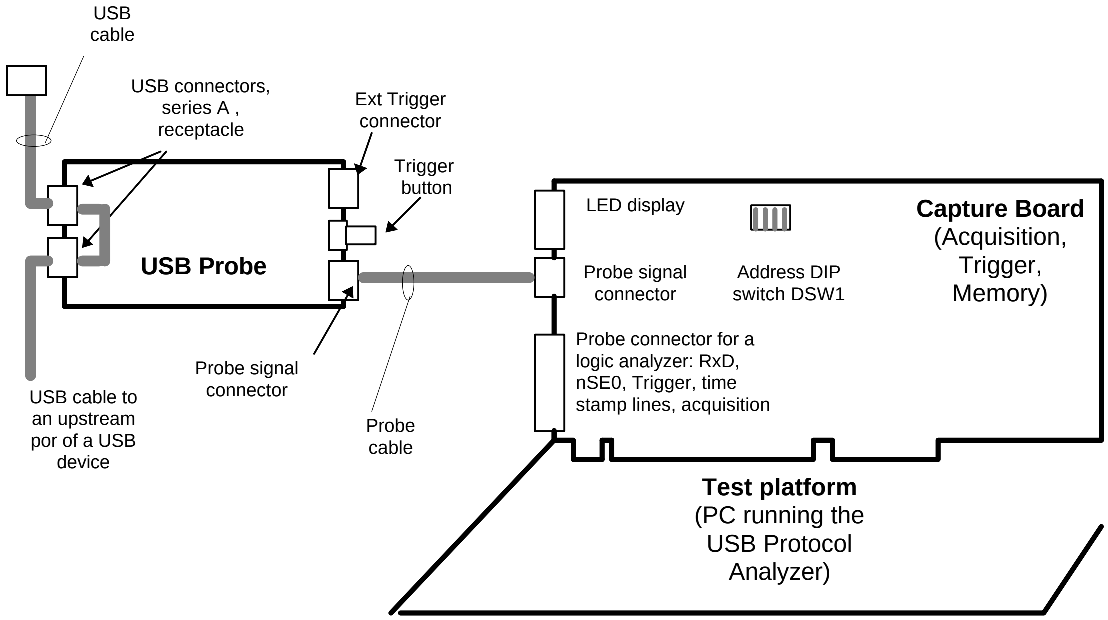
Installation

1. Set the address DIP switch on the address assigned to the USBISA board (default 0x320). Plug in the board and power up the PC (the board does not use interrupts or DMA).
2. If running under Windows95, go in Device Manager and check for any address conflict. If a conflict is shown, try another address for the USBISA board. If running Windows NT skip this check (if there is an address conflict, the board will not work)
3. Insert the installation disk #1, and run “setup.exe” from that disk. Install Shield will perform the application installation (there are two installation disks).
4. Reboot the PC and run USB Protocol Analyzer.
5. Go to Configuration, Capture device and in Configure Options dialog set the Capture Device combo on GENOAUSBISA and the Address combo on the address set by the DIP switch on the USBISA board. Refer to Configure Capture Device for details.
6. Press OK button to close the dialog. At that moment the New command of USB menu is enabled.

Theory of Operation

Overview

The diagram below presents the hardware setup of the USB Protocol Analyzer:


USB cable
USB connectors, series A , receptacle
Ext Trigger connector
Trigger button
USB Probe
LED display
Capture Board (Acquisition, Trigger, Memory)
Probe signal connector
Address DIP switch DSW1
Probe connector for a logic analyzer: RxD, nSE0, Trigger, time stamp lines, acquisition
Probe signal connector
USB cable to an upstream por of a USB device
Probe cable
Test platform (PC running the USB Protocol Analyzer)

A non intrusive USB Probe is inserted on the USB bus under test. This device converts the differential signals *D+* and *D-* into digital signals *RxD* and *nSE0*. The probe presents a trigger button and external trigger connector to add external trigger capabilities to the traffic capture.

RxD line indicates the NRZI signaling, while *nSE0* indicates the occurrence of SE0 state on the bus (active LO). Both signals are sent to the capture board which contains the Acquisition Machine, the Trigger Machine and the Acquisition Memory. The capture board is plugged into a full ISA connector of the PC running the application.

The Acquisition Machine samples *RxD* and *nSE0* signals with 60MHz sampling clock. Each time a change occurs on any of these two lines, the Acquisition Machine stores the new bus state(i.e. the state of *RxD* and *nSE0* lines) and a 6 bit time stamp which indicates the duration of the previous bus state. A new acquisition may be caused as well by the overflow of the time stamp counter. The time stamp resolution is 16.667ns. Each time a new acquisition occurs, the Acquisition Machine provides an acquisition clock pulse for the Acquisition Memory, which is using that pulse to store the bus state and the time stamp. In order to avoid recording long idle times, the Acquisition Machine may be programmed to truncate the durations of recorded idle states.

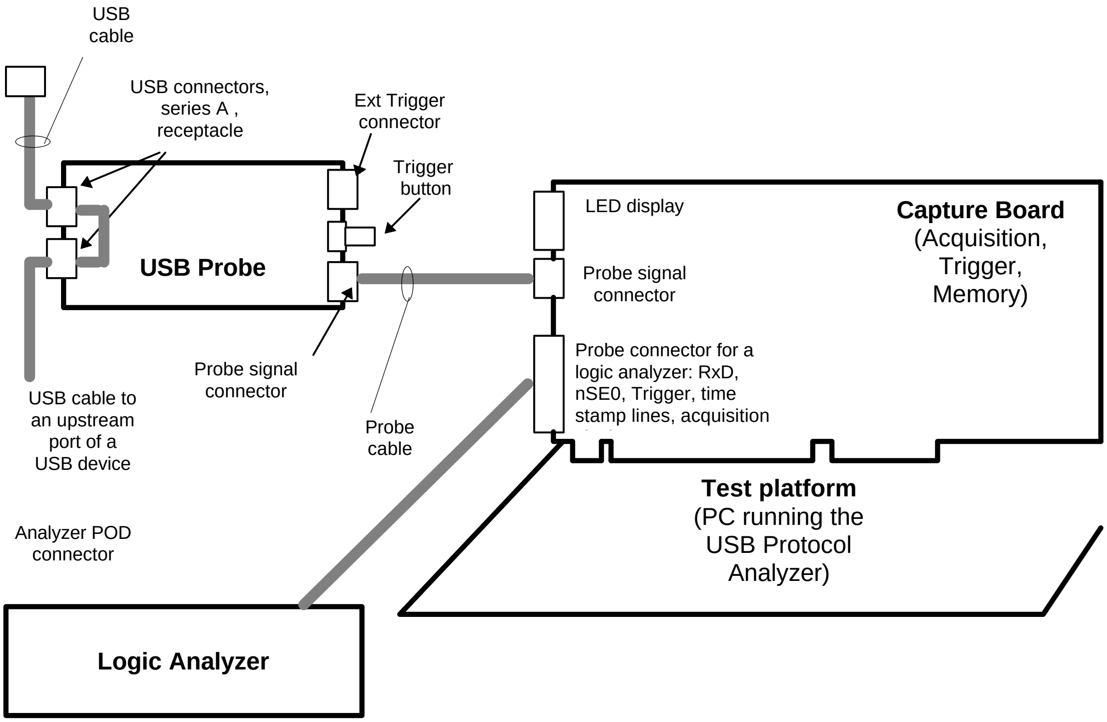
The Trigger Machine may be programmed with the trigger conditions available in this program. The user may also program the size of the Acquisition Memory and the acquisition offset (the percentage of the acquisition memory used to store pre-trigger traffic). When the trigger condition occurs, a trigger line (referred as *triggerOut*) will be set HI to indicate that event.

The Acquisition Memory stores the bus state and time stamp on each acquisition clock provided by the Acquisition Machine. The trigger position (given by the rising edge of *triggerOut* signal) is stored in one of the board registers. The Acquisition Memory stops acquiring new acquisitions in two situations: either it has detected the trigger condition and reaches the end of the programmed post-trigger memory, or it is stopped by the user.

Once the traffic capture is completed, the acquisition data is uploaded to the PC running the USB Protocol Analyzer. At that moment the acquisition data starts to be analyzed in order to re-create the USB traffic in terms of events, packets, transactions, frames, and data. During this process, the traffic is analyzed for compliance to USB specification. Each non-compliance (referred as a protocol error) is logged to be presented in the test reports, statistics, and in the traffic flow.

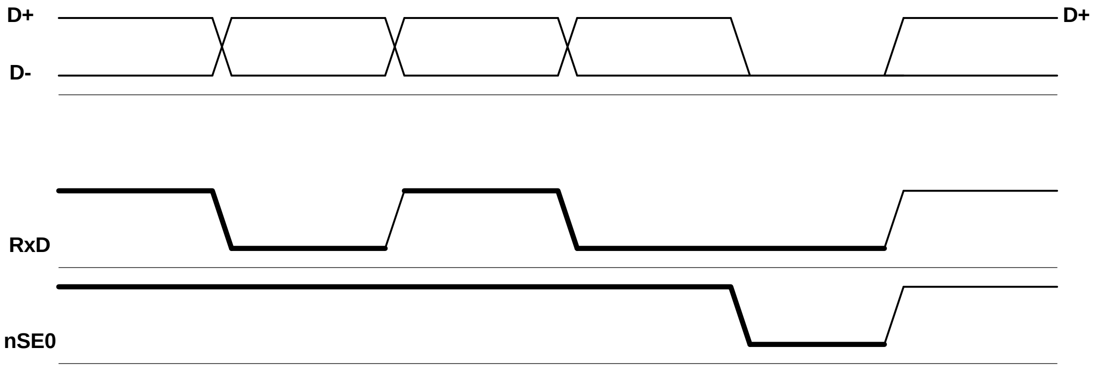
The USB Protocol Analyzer displays the traffic flow on three traffic layers: Event Layer, Transaction Layer, and Data Layer (for each pipe which carried data).

The *RxD*, *nSE0*, *triggerOut*, time stamp signals and the acquisition clock (i.e. the outputs of the Acquisition Machine) are brought to a probe connector to allow the monitoring of the traffic with a logic analyzer. Note that the logic analyzer is not connected in any way to the PC running the program. It may be used to get the waveform for a part of the traffic around the trigger point. The setup involving the logic analyzer is shown in the diagram below:


USB cable
USB connectors, series A , receptacle
Ext Trigger connector
Trigger button
USB Probe
LED display
Capture Board
(Acquisition, Trigger, Memory)
Probe signal connector
Probe connector for a logic analyzer: RxD, nSE0, Trigger, time stamp lines, acquisition
Probe signal connector
USB cable to an upstream port of a USB device
Probe cable
Test platform
(PC running the USB Protocol Analyzer)
Analyzer POD connector
Logic Analyzer

USB Probe

The task of USB Probe is to convert the differential lines *D+* and *D-* of the USB bus into digital signals *RxD* and *nSE0*. The diagram below shows the relationship between *D+*, *D-* and *RxD*, *nSE0*:



Despite the probe is supposed to be non-intrusive, it adds however an extra load on *D+* and *D-* lines. That load is presented in the specification of the PDIUSBP11 transceiver (Philips). If the USB bus is driven by a driver unable to work with two receiver loads, then it is possible to see the USB Probe affecting the USB traffic.

The USB Probe contains as well a trigger button and an external trigger connector. That will allow the user to provide either a manual trigger or an external trigger for the traffic capture.

The pin assignment of the 8 pin trigger connector is presented below:

GND	D0	D1	GND
GND	D2	D3	GND.

The mating connector is at one end of the Trigger Cable. At the other end of this cable there is a DB25 female connector to be used in conjunction with a parallel port cable by an LPT port to provide the external trigger. The external trigger becomes active when on data lines of that LPT is written a byte having zeroes on the last four bits (i.e. 0x00, 0x10, .., 0xf0). The attachment of the Trigger Cable does not require a specific position (the pin assignment is symmetrical) and is provided by Genoa Technology.

The probe receives the power supply from the capture board , and returns *RxD*, *nSE0*, and *nExtTrigger* signals. The *nExtTrigger* signal goes LO when either the trigger button is pressed, or the D0..D3 lines from the trigger connector go LO.

The probe is connected to the capture board via the Probe Cable labeled “Probe to Capture”. This cable is provided by Genoa Technology.

The probe provides two USB series A female connectors. One connector receives a short USB cable referred as USB Cable. This cable is provided by Genoa Technology and has USB series A male connectors at both ends. The other end of the USB Cable goes into the upstream port of the bus branch whose traffic is monitored. The other USB connector on the probe will receive the upstream cable of the device supposed to be attached to the bus branch.

Capture Board

The Capture Board contains the Acquisition Machine, the Trigger Machine, and the Acquisition Memory. The board is plugged into a full ISA connector of the PC running the USB Protocol Analyzer.

The board is connected to the USB Probe via the Probe Cable. That cable provides the power supply for the probe, and brings *RxD*, *nSE0*, and *nExtTrigger* signals.

The Capture Board provides the acquisition data (*RxD*, *nSE0*, and time stamp), trigger signal, and the acquisition clock for the Acquisition Memory or for a logic analyzer (if the user needs to get the waveform of *RxD* and *nSE0* signals).

The acquisition process is presented in the description of the Acquisition Machine.

The Capture Board may be programmed with the following capture parameters:

- trigger condition
- record idle option
- bus type
- the size of the acquisition memory
- the acquisition offset

The options for the trigger condition are presented in Trigger Machine.

Record Idle option allows the user either to record the complete durations of idle times when set ON, or to truncate those durations to 22 FS bit times when set OFF. Having record idle ON allows the Frame Analysis and the detection of transaction time-out errors. If record idle is OFF, the Frame Analysis is skipped and only FS transactions will be checked against time-out errors.

The bus type may be one of the followings:

- full speed root
- full speed non-root
- low speed root
- low speed non-root

A root bus carries both downstream and upstream traffic. A non-root bus carries the whole downstream traffic for the corresponding speed, but only a part of the upstream traffic. That part corresponds to the devices attached downstream with respect to the point where the USB Probe is installed.

The size of the Acquisition Memory may be set to: 128k, 256k, 512k, 1M, 2M, 4M, 8M, 16M, and 32M.

The acquisition offset is the percentage of the acquisition memory used to store acquisitions before the occurrence of the trigger condition.

The Capture Board provides a DIP switch to set the base I/O address of the board. The I/O space used by the board is 0x00..0x20. The tables below show the assignment of the DIP switches and the settings for different addresses:

DSW1 Settings

Switch No	Function	Default
1	LED1 disable	OFF
2	No function	OFF
3	No function	OFF
4	Address bit 5	ON
5	Address bit 6	OFF
6	Address bit 7	OFF
7	Address bit 8	ON
8	Address bit 9	ON

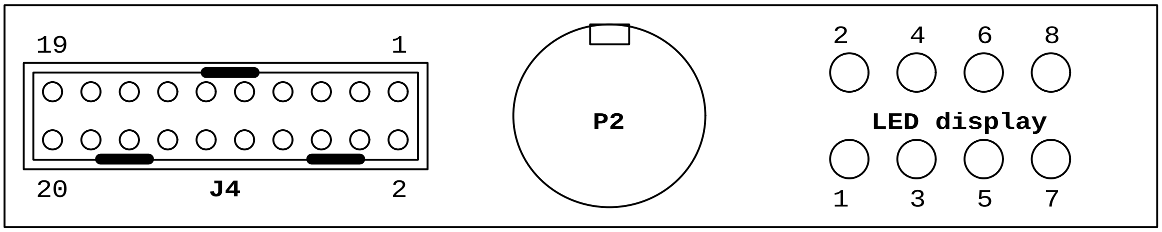
Default address: 0x320.

ISA address	DSW 8	DSW 7	DSW 5	DSW 4	DSW 3
0x240	ON	OFF	OFF	ON	OFF
0x300	ON	ON	OFF	OFF	OFF
0x320	ON	ON	OFF	OFF	ON
0x340	ON	ON	OFF	ON	OFF
0x360	ON	ON	OFF	ON	ON

The base address of the Capture board must be specified in the Address combo of Configure Options dialog (refer to Configure Capture Device for details). Note that Capture Device combo must indicate GENOAUSBISA device.

The Capture Board provides on its bracket:

- the logic analyzer probe connector J4
- the USB Probe connector P2
- the LED display



Pin assignment of logic analyzer probe connector J4

Pin #	Signal name
1	N/C
2	*acqClock* (rising edge, 8.3ns width)
3	*acqClock* (rising edge, 8.3ns width)
4	N/C
5	N/C
6	N/C
7	N/C
8	*triggerOut*
9	*RxD* (from probe)
10	*nSE0* (from probe)
11	*sampleClock* (60MHz)
12	*nSE0* (from acquisition machine)
13	*RxD* (from acquisition machine)
14	*stamp5*
15	*stamp4*
16	*stamp3*
17	*stamp2*
18	*stamp1*
19	*stamp0*
20	GND

NOTE: the signals at the probe connector are active during the capture only.

LED indicators

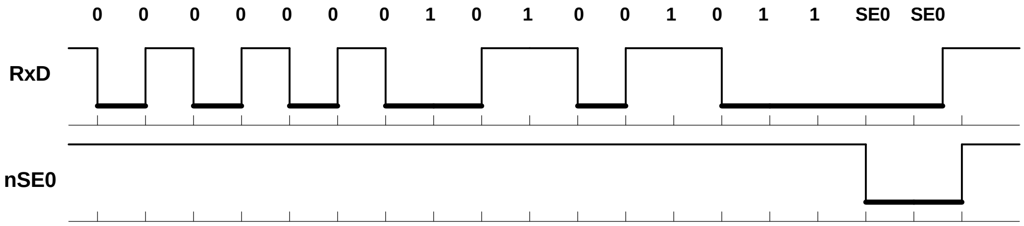
LED #	Function
1	board ready (flash)
2	not used
3	logic analyzer port active
4	trigger detected
5	setup for low speed traffic
6	trigger/acquisition enabled
7	reading capture memory
8	capture status: ON (enabled), OFF (disabled), flash (in progress)

Acquisition Machine

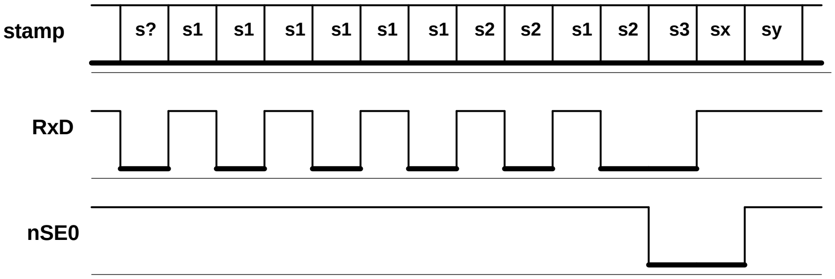
The task of the Acquisition Machine is to feed the Acquisition Memory with acquisition data and acquisition clock, in order to record the USB traffic. *RxD* and *nSE0* lines received from the USB Probe are sampled with 60MHz. Each time the bus state changes, the Acquisition Machine stores the new state and the 6 bit time stamp whose resolution is 16.66ns. The time stamp indicates how long the previous state has stayed on the bus. If the time stamp overflows (i.e. reaches 0x3f = 63), the Acquisition Machine will store a new acquisition as well. However, if Record Idle option was OFF when New USB process the Acquisition Machine will truncate idle times (i.e. the duration of J state following SE0 state) to 22 FS bit times (refer to USB Process for details).

Each time a new acquisition is made - caused by the bus change or time stamp overflow - an acquisition clock pulse is provided. That pulse is used to store in the Acquisition Memory the bus state and the time stamp (referred as acquisition data). The first acquisition has a NULL time stamp.

For example an ACK packet consists of 2 bytes: the sync byte (0x80) and the PID byte (0xd2). The bit stream of this packet will be: 0000000101001011. On a FS bus, the packet will have the following NZRI representation (nSE0 has been added to indicate the end of packet):



The waveform of this packet, presented on the logic analyzer screen (if used) is presented below:



where:
s? is unknown (indicates the duration of the previous state)
s1 is a time stamp corresponding to 1 FS bit time
s2 is a time stamp corresponding to 2 FS bit times
s3 is a time stamp corresponding to 3 FS bit times
sx + sy = s2 (i.e. sx + sy indicates the duration of SE0 state).

Note that the time stamp of the current state is presented by the next acquisition. In the example above, the time stamp of s1 FS bit times of the first K state of ACK packet is presented in the 2nd acquisition of that packet.

The time stamp is given in sampling periods (16.66ns). Theoretically a FS bit time will have a time stamp of 5. The table below presents the relationship between the time stamp presented by the Acquisition Machine and the bit times:

Time stamp conversion for FS bit times (a FS bit cell is 83.33ns):

1 FS bit time	1/2.. 3/2 FS bit cells	3..7 clocks
2 FS bit times	3/2.. 5/2 FS bit cells	8..12 clocks
3 FS bit times	5/2.. 7/2 FS bit cells	13..17 clocks
4 FS bit times	7/2.. 9/2 FS bit cells	18..22 clocks
5 FS bit times	9/2..11/2 FS bit cells	23..27 clocks
6 FS bit times	11/2..13/2 FS bit cells	28..32 clocks
7 FS bit times	13/2..15/2 FS bit cells	33..37 clocks

Time stamp conversion for LS bit times (a LS bit cell is 666.66ns)

1 LS bit time	1/2.. 3/2 LS bit cells	20..59 clocks
2 LS bit times	3/2.. 5/2 LS bit cells	60..99 clocks
3 LS bit times	5/2.. 7/2 LS bit cells	100..139 clocks
4 LS bit times	7/2.. 9/2 LS bit cells	140..179 clocks
5 LS bit times	9/2..11/2 LS bit cells	180..219 clocks
6 LS bit times	11/2..13/2 LS bit cells	220..259 clocks
7 LS bit times	13/2..15/2 LS bit cells	260..299 clocks

By using these time stamp conversion tables, the user may check the packet signaling. Note that the time stamp is one acquisition clock delayed with respect to the bus state which had that duration. That is when looking to a bus state, the duration of that state is indicated in the time stamp of the next acquisition.

Trigger Machine

The Trigger Machine receives the acquisition data and acquisition clock from the Acquisition Machine and provides a trigger signal referred as *triggerOut* active HI. This signal is available at the J4 probe connector. The trigger occurs on the rising edge of *triggerOut*.

The following trigger options are available:

1. **Immediate trigger**: *triggerOut* goes HI on the first acquisition clock received from Acquisition Machine .
2. **No trigger**: *triggerOut* line is held LO. In this way the Acquisition Memory records the last part of the USB traffic, and the capture needs to be stopped by the user.
3. **Program trigger**: the user may trigger the capture from its own application by calling SetProgramTrigger function. The result of that call is the rising of *triggerOut* signal. The prototype of this function is: void SetProgramTrigger(void). The "usbisa.lib" file is provided to let the user application link to "usbisa.dll".
4. **External trigger**: *triggerOut* line goes HI when either the user presses the trigger button on theUSB Probe, or *D0..D3* lines of the trigger connector go LO.
5. **K state trigger**: *triggerOut* line goes HI when the first K state occurs on the bus
6. **SOF trigger**: the user may must set the frame number and occurrence of the frame he wants to trigger the capture. When the Trigger Machine detects the specified occurrence of the specified SOF packet, *triggerOut* signal will go HI.
7. **SETUP trigger**: the user must set the speed, address, endpoint, and occurrence of the SETUP token he wants to trigger the capture. When the Trigger Machine detects the specified occurrence of the specified SETUP token, *triggerOut* signal will go HI.
8. **OUT trigger**: the user must set the speed, address, endpoint, and occurrence of the OUT token he wants to trigger the capture. When the Trigger Machine detects the specified occurrence of the specified OUT token, *triggerOut* signal will go HI.
9. **IN trigger**: the user must set the speed, address, endpoint, and occurrence of the IN token he wants to trigger the capture. When the Trigger Machine detects the specified occurrence of the specified IN token, *triggerOut* signal will go HI.
10. **DATA0 trigger**: the user must set the speed, the first 0..8 data bytes, and occurrence of the DATA0 packet he wants to trigger the capture. When the Trigger Machine detects the specified occurrence of the specified DATA0 packet, *triggerOut* signal will go HI.
11. **DATA1 trigger**: the user must set the speed, the first 0..8 data bytes, and occurrence of the DATA1 packet he wants to trigger the capture. When the Trigger Machine detects the specified occurrence of the specified DATA1 packet, *triggerOut* signal will go HI.
12. **ACK trigger**: the user must set the speed and occurrence of the ACK packet he wants to trigger the capture. When the Trigger Machine detects the specified occurrence of the specified ACK packet, *triggerOut* signal will go HI.
13. **NAK trigger**: the user must set the speed and occurrence of the NAK packet he wants to trigger the capture. When the Trigger Machine detects the specified occurrence of the specified NAK packet, *triggerOut* signal will go HI.
14. **STALL trigger**: the user must set the speed and occurrence of the STALL packet he wants to trigger the capture. When the Trigger Machine detects the specified occurrence of the specified STALL packet, *triggerOut* signal will go HI.

Any of the trigger options mentioned above may be set in the New USB Process dialog (refer to USB Process for details).

Logic Analyzer (Optional)

A general purpose logic analyzer may be used in parallel with the Capture Board to trigger the capture on the *triggerOut* signal provided by the Trigger Machine and to store (a part of) the acquisition data provided by the Acquisition Machine. That data describes the USB traffic both in state - presented on *RxD* and *nSE0* lines - and time - presented on *stamp0..stamp5* lines (that is a 6 bit time stamp). The use of the logic analyzer is indicated when the user needs to get the traffic waveform.

The logic analyzer monitors 9 signal lines brought to the probe connector J4 on the Capture Board. The states of these lines are stored on each acquisition clock pulse brought to J4 as well. These lines are presented below:

Signal line	Logic analyzer label	Description
stamp0..5	STAMP	6 bit time stamp of 16.67ns resolution (60MHz sampling rate)
RxD	RXD	signals NRZI data
nSE0	NSE0	signals SE0 state (active LO)
triggerOut	TRIG	trigger line (active on rising edge)
acqClock		acquisition clock (active on rising edge), width 8.3 ns

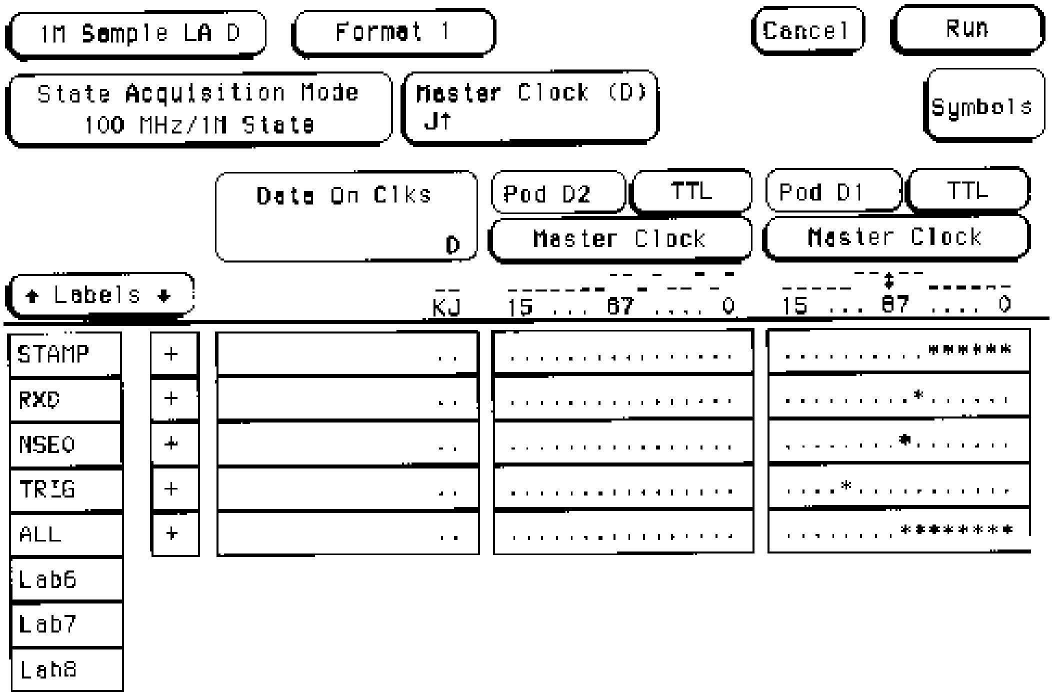
The table below presents the pin assignments of J4 connector:

Pin #	Signal name
1	N/C
2	*acqClock* (rising edge, 8.3ns width)
3	*acqClock* (rising edge, 8.3ns width)
4	N/C
5	N/C
6	N/C
7	N/C
8	*triggerOut*
9	*RxD* (from probe)
10	*nSE0* (from probe)
11	*sampleClock* (60MHz)
12	*nSE0* (from acquisition machine)
13	*RxD* (from acquisition machine)
14	*stamp5*
15	*stamp4*
16	*stamp3*
17	*stamp2*
18	*stamp1*
19	*stamp0*
20	GND

NOTE: the signals at the probe connector are active during the capture only.

The analyzer POD may be installed on the probe connector via a termination adapter (HP 01650-63203). For details on the whole setup refer to Hardware Setup.

The logic analyzer must be configured by the user to work on state mode using an external clock and to trigger on the rising edge of *triggerOut*. The picture below presents the format screen of a HP16555A logic analyzer used to capture up to 1M acquisitions:



State Acquisition Mode 100 MHz/1M State

Master Clock (D) J↑

Data On Clks D

Pod D2 TTL Master Clock

Pod D1 TTL Master Clock

Interpreting the waveform is presented in Viewing Signals.

USB Process

The USB Process consists of the capture and analysis of a part of the USB traffic which occurred on the bus branch where the USB Probe is installed.

During the traffic capture, the Capture Board stores the bus states and time stamps on each acquisition clock provided by the Acquisition Machine. The traffic capture starts when the user clicks Run button of New USB Process dialog (refer to New USB for details). Before starting the capture, the user must set the capture options and analysis options. The traffic capture stops either when the trigger condition is detected and the end of post trigger acquisition memory is reached, or when the user clicks the Stop button of New USB Process dialog.

Once the capture is completed, acquisition data is transferred from the Capture Board to the PC running the application. This data is analyzed in four stages: Event Analysis, Packet Analysis, Transaction Analysis and Frame Analysis. The program releases reports from each stage, presenting the traffic summary and the list of detected protocol errors. For each error is provided the description and the place in the traffic where it occurred. Statistics data is available to create a “global picture” of the traffic which has been captured and analyzed.

The progress of the USB Process is displayed in USB Progress window of New USB Process dialog. The process may be canceled by clicking Cancel button.

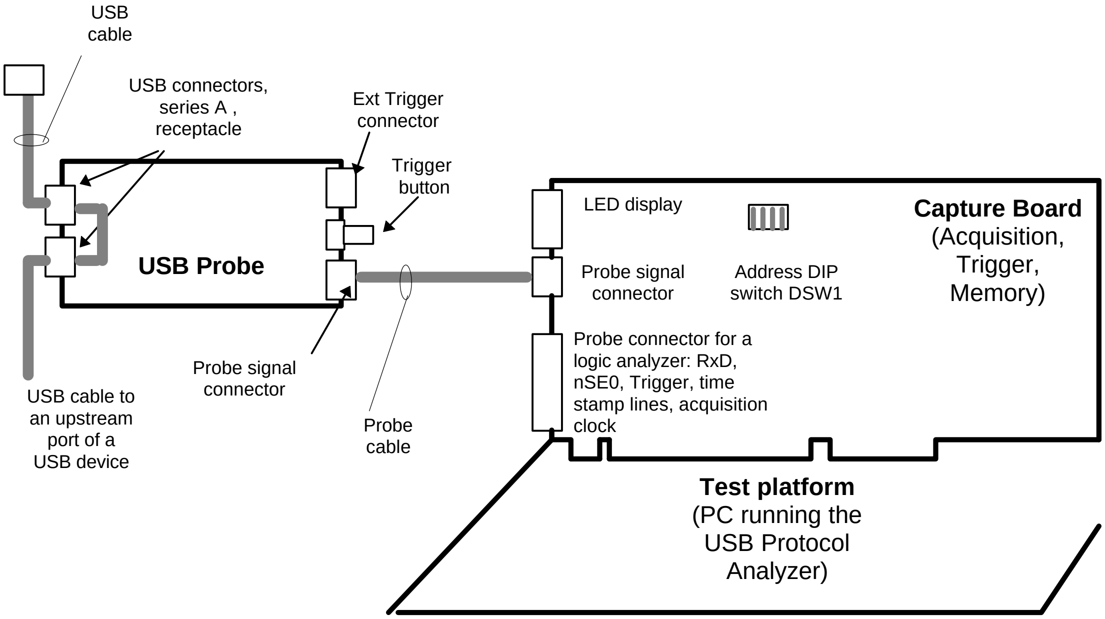
The user may choose to perform only some parts of the USB Process. For example to perform the traffic capture, Event Analysis, and Packet Analysis. Then it may resume the USB Process with other stages. For more information refer to New USB and Resume USB.

Configuring the Protocol Analyzer

Hardware Setup

The hardware setup is presented for two different situations: with and without the logic analyzer.

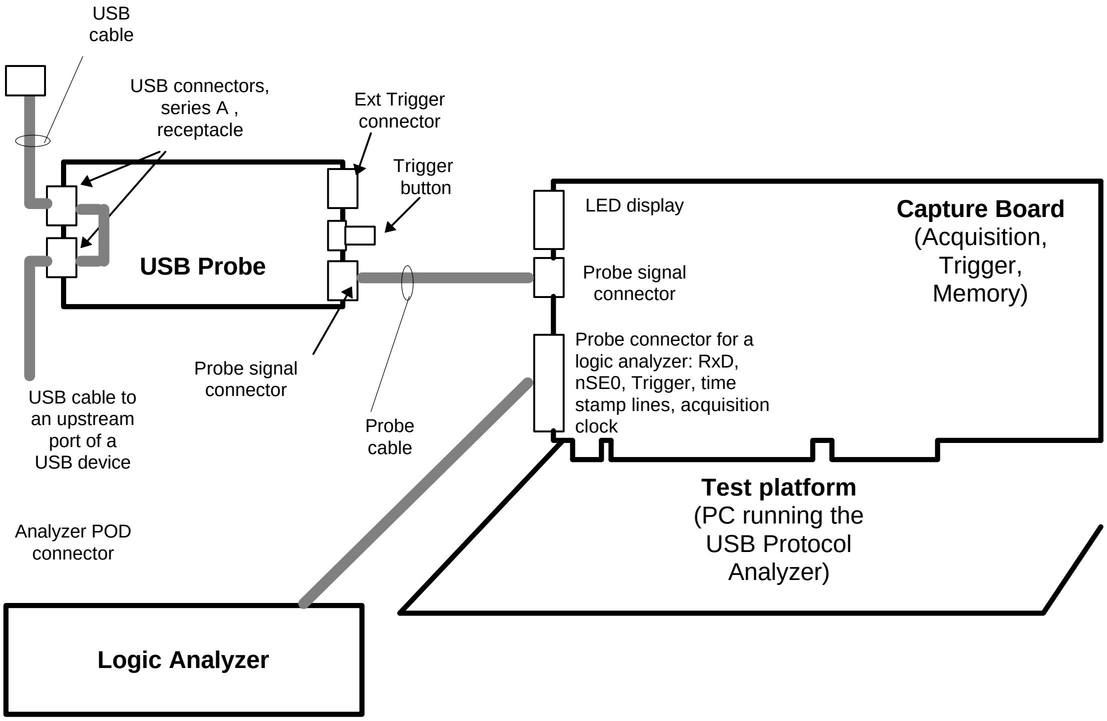
The diagram below illustrates the setup without the logic analyzer:


USB cable
USB connectors, series A , receptacle
Ext Trigger connector
Trigger button
USB Probe
Probe signal connector
USB cable to an upstream port of a USB device
Probe cable
LED display
Probe signal connector
Address DIP switch DSW1
Capture Board (Acquisition, Trigger, Memory)
Probe connector for a logic analyzer: RxD, nSE0, Trigger, time stamp lines, acquisition clock
Test platform (PC running the USB Protocol Analyzer)

In this case the hardware setup comprises the following steps:

1. insert the USB Cable provided by Genoa Technology in one of the USB receptacle connectors on the USB Probe (that is a short USB cable having USB series A connectors at both ends)
2. insert the other end of the USB Cable into the hub downstream port
3. insert the free end of the USB cable coming from the USB device into the other port of the USB Probe
4. connect the USB Probe to the Capture Board via the Probe Cable (labeled "Probe to Capture").
5. set the base address of the Capture Board by using the dip switch DSW1.
6. start the USB Protocol Analyzer application and select Configure item of the bar menu, then choose Capture Device. The program opens the Configure Options dialog. In this dialog, select in Capture Device combo the item GENOAUSBISA, and in Address combo the base address as set on the Capture Board .

If a logic analyzer is added to get (a part of) the traffic waveform, the setup presented below will be used:


USB cable
USB connectors, series A , receptacle
Ext Trigger connector
Trigger button
USB Probe
Probe signal connector
Probe cable
USB cable to an upstream port of a USB device
Analyzer POD connector
LED display
Capture Board (Acquisition, Trigger, Memory)
Probe signal connector
Probe connector for a logic analyzer: RxD, nSE0, Trigger, time stamp lines, acquisition clock
Test platform (PC running the USB Protocol Analyzer)
Logic Analyzer

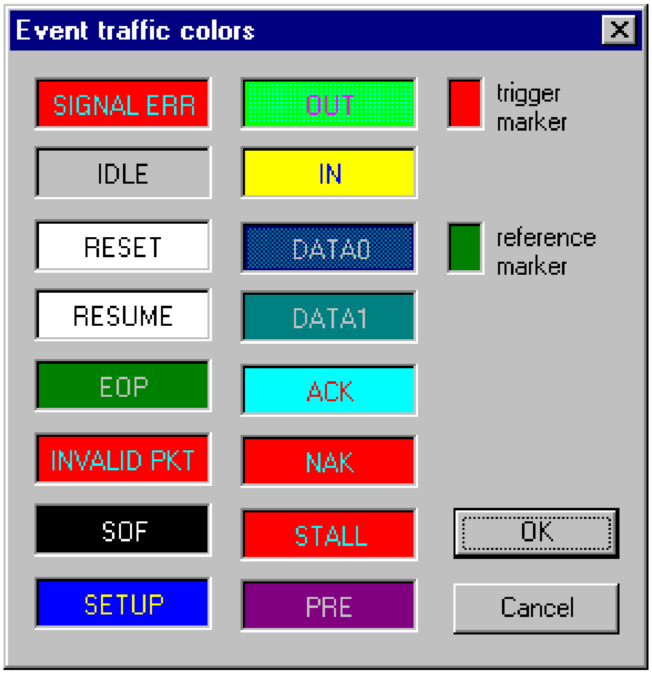
In this case the hardware setup comprises the following steps:

1. insert the USB Cable provided by Genoa Technology in one of the USB receptacle connectors on the USB Probe (that is a short USB cable having USB series A connectors at both ends)
2. insert the other end of the USB Cable into the hub downstream port
3. insert the free end of the USB cable coming from the USB device into the other port of the USB Probe
4. connect the USB Probe to the Capture Board via the Probe Cable
5. install the logic analyzer POD on the probe connector J4 via termination adapter (HP 01650-63203)
6. set the base address of the Capture Board by using the dip switch DSW1.
7. start the USB Protocol Analyzer application and select Configure item of the bar menu, then choose Capture Device. The program opens Configure Options dialog. In this dialog, select in Capture Device combo the item GENOAUSBISA, and in Address combo the base address as set on the Capture Board.

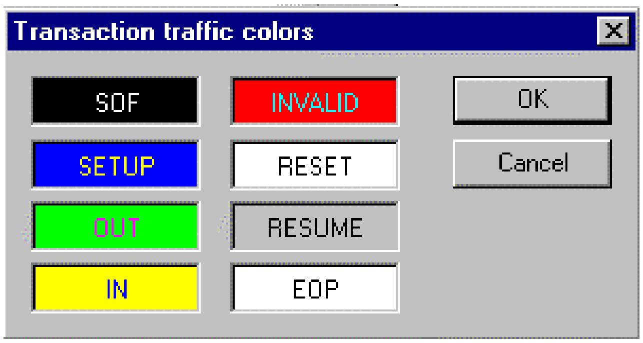
Choosing Traffic Colors

The USB traffic is shown on three layers: Event Layer, Transaction Layer, and Data Layer. On the first two layers, the traffic is presented as a list of traffic items. The user may assign a color for each traffic item by selecting Configure item of the bar menu, then Traffic colors - Events to select colors for the event traffic, or Traffic colors - Transactions to select colors for the transaction traffic.

When Events is selected, the program opens Event traffic colors dialog. The user may specify a color for each event, as well as for the trigger and reference marker. When a control is clicked in this dialog, the program brings a color selection dialog which allows the user to choose the color.



When Transactions is selected, the program opens Transaction traffic colors dialog. The user may specify a color for each transaction item. When a control is clicked in this dialog, the program brings a color selection dialog which allows the user to choose the color.

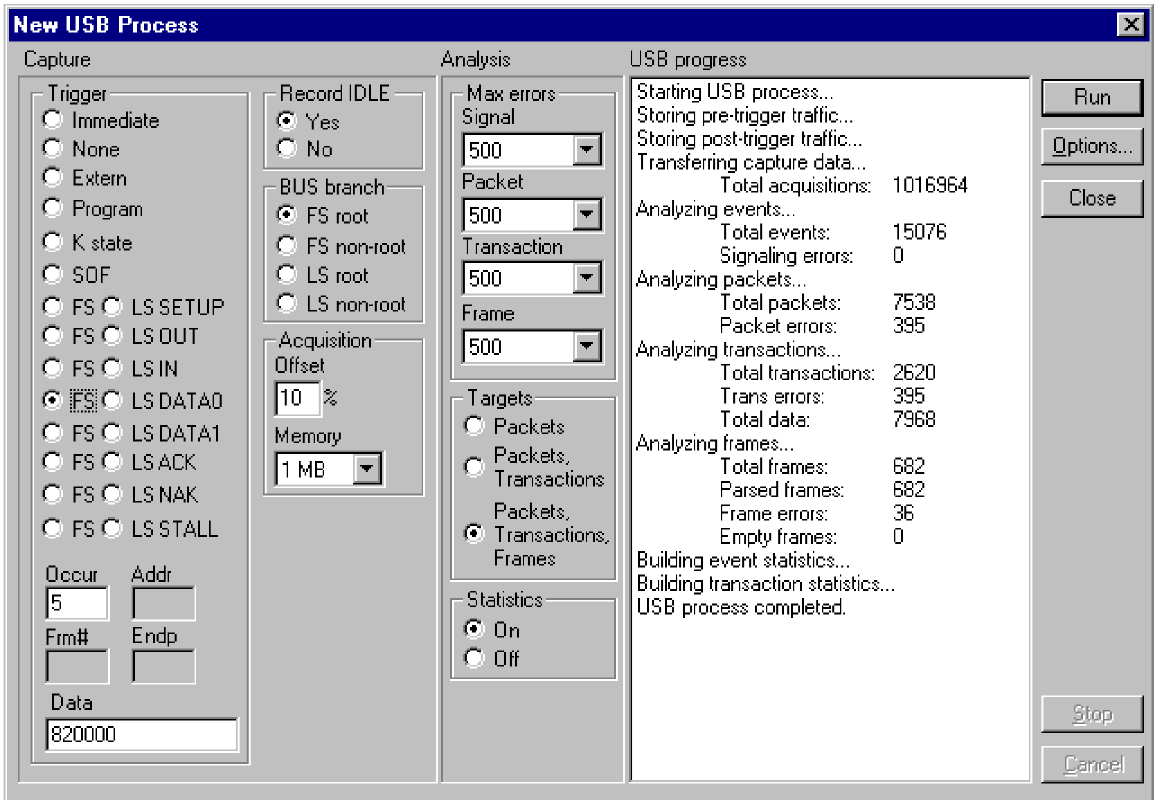


USB Process

New USB

New USB command is available in USB drop menu. When this command is activated, the program will perform one of the followings:

- if an USB traffic is on the screen, the program asks if the current USB traffic should be overwritten or the command should be canceled. If the current traffic shouldn't be overwritten, the user may cancel the command and then save the traffic (refer to save command).
- if no USB traffic is on the screen, or the current USB traffic is saved, or the current traffic may be overwritten, the program opens New USB dialog:



Trigger
○ Immediate
○ None
○ Extern
○ Program
○ K state
○ SOF
○ FS ○ LS SETUP
○ FS ○ LS OUT
○ FS ○ LS IN
● FS ○ LS DATA0
○ FS ○ LS DATA1
○ FS ○ LS ACK
○ FS ○ LS NAK
○ FS ○ LS STALL

Occur: 5
Addr:
Frm#:
Endp:
Data: 820000

Record IDLE
● Yes
○ No

BUS branch
● FS root
○ FS non-root
○ LS root
○ LS non-root

Acquisition
Offset: 10 %
Memory: 1 MB

Max errors
Signal: 500
Packet: 500
Transaction: 500
Frame: 500

Targets
○ Packets
○ Packets, Transactions
● Packets, Transactions, Frames

Statistics
● On
○ Off

```
Starting USB process...
Storing pre-trigger traffic...
Storing post-trigger traffic...
Transferring capture data...
            Total acquisitions:   1016964
Analyzing events...
            Total events:         15076
            Signaling errors:     0
Analyzing packets...
            Total packets:        7538
            Packet errors:        395
Analyzing transactions...
            Total transactions:   2620
            Trans errors:         395
            Total data:           7968
Analyzing frames...
            Total frames:         682
            Parsed frames:        682
            Frame errors:         36
            Empty frames:         0
Building event statistics...
Building transaction statistics...
USB process completed.
```

In this dialog the user may set the followings:

- the capture options: trigger options, acquisition offset, acquisition memory (size) , bus branch option, record idle option
- the analysis options: max. errors for signals, packets, frames, and transactions, analysis targets (i.e. selective analysis), and the statistics option. Having statistics off, it will shorten the USB process.

The trigger option will cause to have the traffic capture triggered on a user defined condition. The following trigger conditions are available:

- immediate trigger: the trigger will occur immediately
- none (no trigger): the capture is overwritten until it is stopped by the user

- external trigger: the trigger will be caused by an external trigger signal or by pressing the trigger button of the USB Probe
- program trigger: the trigger will occur when the user application calls SetProgramTrigger function, while the protocol analyzer is running and Run button has been pressed (i.e. the capture is in progress)
- K state trigger: the trigger will occur on the first K state shown on the bus
- trigger on SOF packet (settings: frame#, occurrence)
- trigger on SETUP token (settings: speed, address, endpoint, occurrence)
- trigger on OUT token (settings: speed, address, endpoint, occurrence)
- trigger on IN token (settings: speed, address, endpoint, occurrence)
- trigger on DATA0 packet (settings: speed, first 0..8 data bytes, occurrence)
- trigger on DATA1 packet (settings: speed, first 0..8 data bytes, occurrence)
- trigger on ACK packet (settings: speed, occurrence)
- trigger on NAK packet (settings: speed, occurrence)
- trigger on STALL packet (settings: speed, occurrence)

For more information on trigger options refer to Trigger Machine.

The acquisition offset indicates the percentage of the acquisition memory that will be assigned for pre-trigger capture.

Acquisition memory (size) indicates the size of the acquisition buffer. The available options are: 128k, 256k, 512k, 1M, 2M, 4M, 8M, 16M, 32M.

Record idle option limits the record of idle times (between packets) to a few bit times, saving in this way acquisition memory for packet transfers. Refer to Record Idle Option for more information on this option.

The bus branch option indicates what kind of USB bus branch will be monitored: full speed root, full speed non-root, low speed root, or low speed non-root. Low speed branches are not supposed to drive full speed traffic. Full speed non-root branches may drive transactions with missing upstream traffic (such transactions involve devices which are not located downstream from the capture place). These transactions, when seen on a FS non-root branch will be referred as alien transactions. Alien transactions are not allowed on root branches. Refer to Alien Transactions for details.

Max. errors options set limits for the number of errors accepted during the USB process: signal errors for Event Analysis, packet errors for Packet Analysis, transaction errors for Transaction Analysis, and frame errors for Frame Analysis.

Analysis target options allow to apply selective USB analysis:

- if packets, only Event Analysis and Packet Analysis will be applied. (Event Analysis is applied for any option)
- if packets, transactions, the program will apply Event Analysis, Packet Analysis, and Transaction Analysis
- if packets, transactions, frames, the program will apply Event Analysis, Packet Analysis, Transaction Analysis, and Frame Analysis (i.e. full USB analysis).

If statistics option is enabled, then statistics information from each applied analysis will be available. Disabling statistics will speed up the analysis process.

Once all options have been set, the user may initiate the USB Process by pressing the Run button. The user may cancel the process by pressing the Cancel button. From that point the user may re-program the options and re-initiate the process by pressing the Run button, or may close the dialog by pressing Close button. If Cancel button has been pressed while the process was in progress, then:

- all layer screens become empty
- Results, Go to, Search, and View drop menus will be disabled
- in File drop menu, the following commands will be disabled: Close, Export, Save, Print.

When Run button is pressed, the USB Process is started. The process contains the following stages:

- the capture device is programmed according to the options set by the user.
- the capture device performs the capture until the stop condition occurs. The user may stop the capture at any time by pressing Stop button.
- the acquisition data is transferred from the capture device to the PC hosting the protocol analyzer
- the acquisition data is processed in order to build the temporary data base which re-creates the USB traffic as specified by analysis target options. In the same time, analysis reports are generated to present all protocol non-compliances. If statistics option was on, then statistics data will be created for the captured traffic.

As the Process is going on, the USB progress window presents a series of messages about this process. Finally, the progress window will present the process summary: how many signaling errors, packet errors, frame errors, transaction errors, how many events, packets, frames, transactions, data, etc. When the process is completed, the user may press the Close button to close dialog.

Once the dialog is closed, the front end displays the Event Layer for the new traffic, having the traffic focus on the event at trigger position and the time information relative to trigger. The user may switch on a different layer, may apply display filters, may search for errors, or look to results.

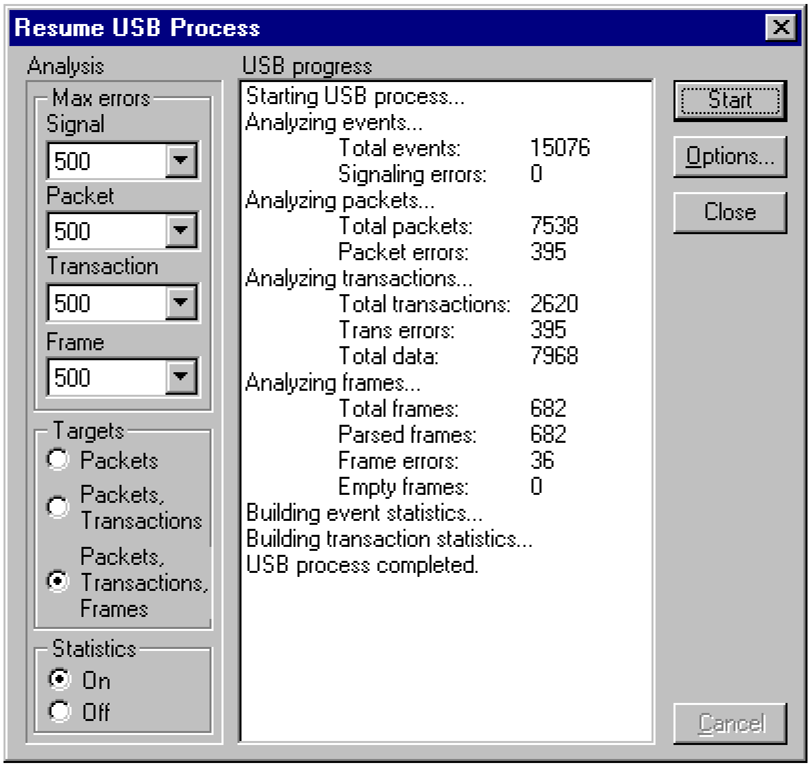
The capture options may be saved in a data base by pressing Options button. The program will ask for the user name and description. Options which have been saved may be loaded, deleted, or overwritten. The program will display the list of saved options by user name, description, and date.

Resume USB

For large captures, a full USB Process may be time consuming. For this reason, the process may be applied in two or more steps to allow getting faster partial results.

Resume USB command is available in USB drop menu. This command allows as well to apply the USB analysis on a capture which has previously imported, or have been submitted to an incomplete USB Process.

When this command is activated, the program opens Resume USB Process dialog:



Max errors
Signal 500
Packet 500
Transaction 500
Frame 500

Targets
○ Packets
○ Packets, Transactions
● Packets, Transactions, Frames

Statistics
● On
○ Off

```
Starting USB process...
Analyzing events...
        Total events:       15076
        Signaling errors:   0
Analyzing packets...
        Total packets:      7538
        Packet errors:      395
Analyzing transactions...
        Total transactions: 2620
        Trans errors:       395
        Total data:         7968
Analyzing frames...
        Total frames:       682
        Parsed frames:      682
        Frame errors:       36
        Empty frames:       0
Building event statistics...
Building transaction statistics...
USB process completed.
```

Options allowed by the controls of this dialog work as presented in New USB.

If an analysis required by the selected target option is already completed, that will be indicated by a message in USB progress window. For example: "Packet analysis already done...".

When Resume USB Process dialog is closed, the front end keeps the layer existing at the moment when resume has been started.

Record Idle Option

This option may be set ON or OFF.

When set ON, the Acquisition Machine will record the real duration of idle states (that is J state following SE0 state). The following are the benefits of recording real values of idle times:

- Transaction Analysis will be able to detect transaction time-out errors for LS transactions included. A time-out error occurs when the time distance between two consecutive packets of a transaction is greater than 16 bit times
- Frame Analysis may be performed in order to detect frame timing errors
- timing information becomes available on Event Layer
- Frame Statistics becomes available in Transaction Statistics dialog

The disadvantage of recording real values of idle times is spending the acquisition memory for times when no traffic activity occurred.

When set OFF, the Acquisition Machine will truncate idle times to 22 FS bit times. That will still allow to detect time-out errors for FS transactions, but all other benefits mentioned above will not be available. However, the advantage of truncating idle times is the ability to record a larger traffic.

Alien Transactions

An alien transaction has the upstream packet replaced by idle states. Such transactions may be "seen" on a FS non-root bus branch if the USB device involved in that transaction is not placed downstream from the point where the USB Probe is installed. Alien transactions may also be seen on LS non-root branches.

On a FS non-root bus it is possible to see the following alien transactions:

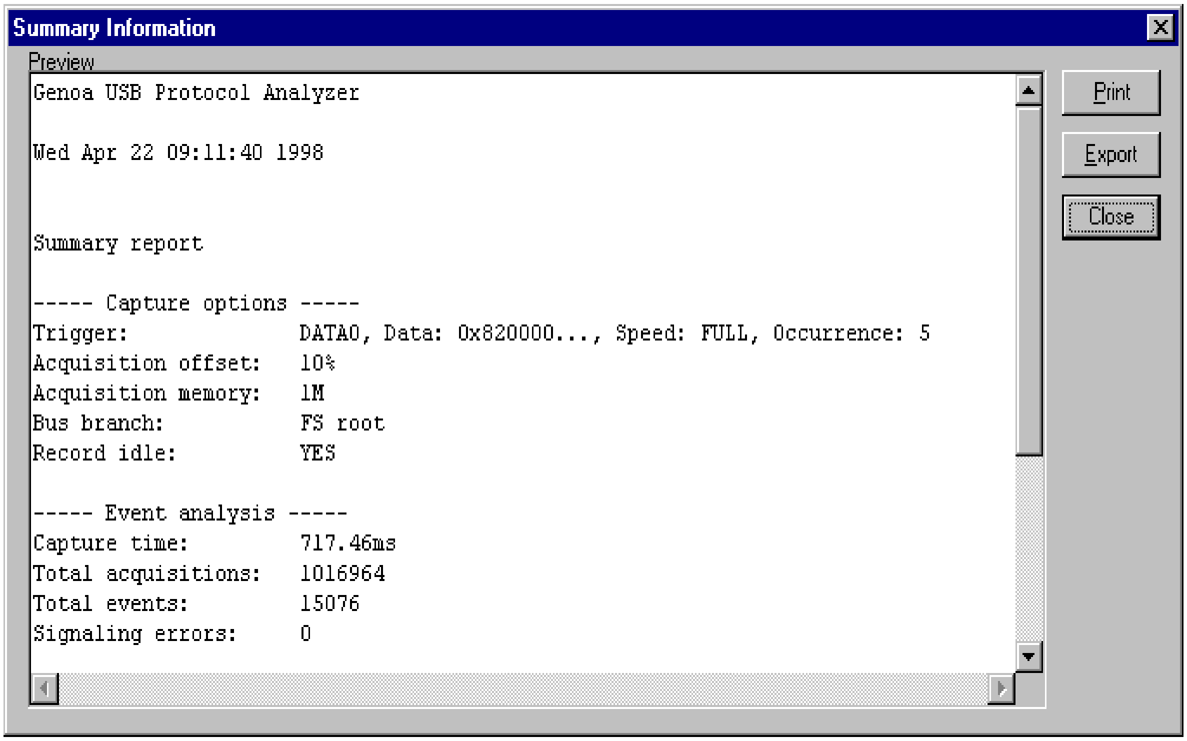
- IN, IDLE (FS alien IN, missing the handshake packet)
- IN, IDLE, ACK (FS alien IN, missing the data packet)
- PRE, IDLE, SETUP, IDLE, PRE, IDLE, DATA0, IDLE (LS alien SETUP, missing the handshake packet)
- PRE, IDLE, OUT, IDLE, PRE, IDLE, DATA0/1, IDLE (LS alien OUT, missing the handshake packet)
- PRE, IDLE, IN, IDLE, PRE, IDLE, ACK (LS alien IN, missing the data packet)
- PRE, IDLE, IN, IDLE (LS alien IN, missing the handshake packet)

On a LS non-root bus it is possible to see the following alien transactions:

- IN, IDLE (LS alien IN, missing the handshake packet)
- IN, IDLE, ACK (LS alien IN, missing the data packet)

Looking at Results

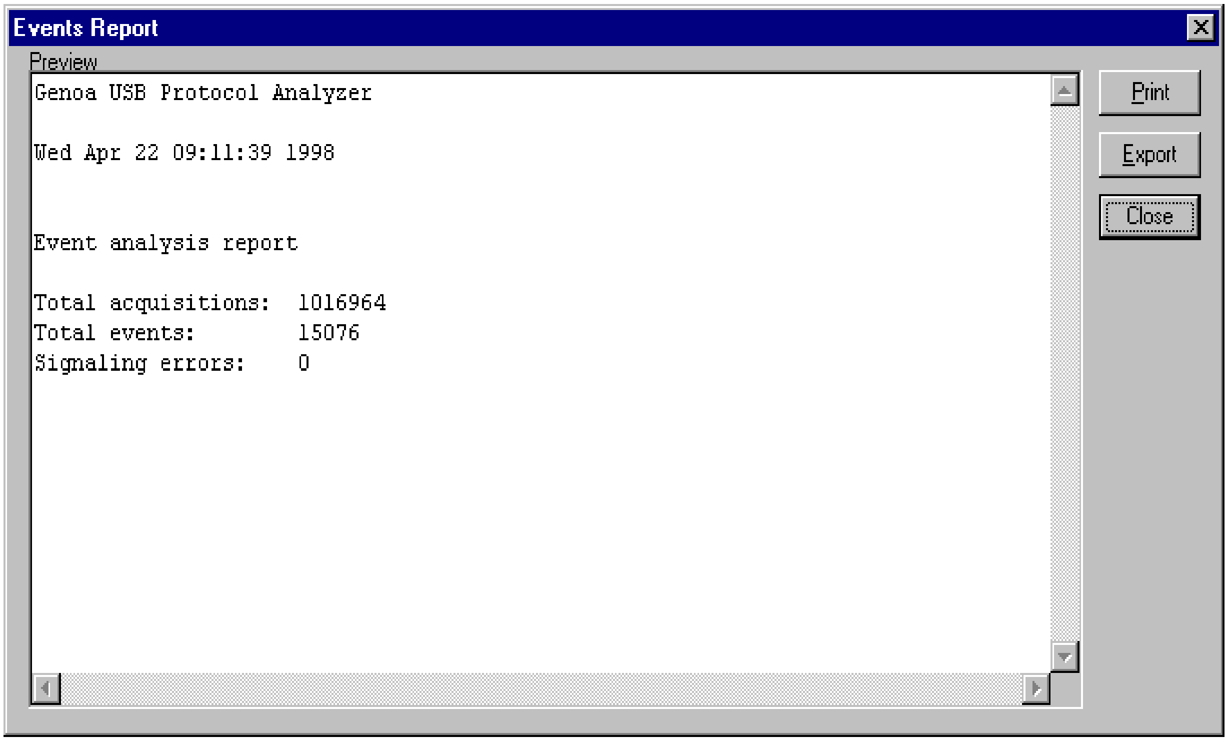
Summary



```
Genoa USB Protocol Analyzer

Wed Apr 22 09:11:40 1998


Summary report

----- Capture options -----
Trigger:               DATA0, Data: 0x820000..., Speed: FULL, Occurrence: 5
Acquisition offset:    10%
Acquisition memory:    1M
Bus branch:            FS root
Record idle:           YES

----- Event analysis -----
Capture time:          717.46ms
Total acquisitions:    1016964
Total events:          15076
Signaling errors:      0
```

The summary of the USB Process may be accessed with Summary command of Results drop menu. The summary briefs the results generated by the last process initiated either with New USB or with Resume USB.

Event Analysis Report



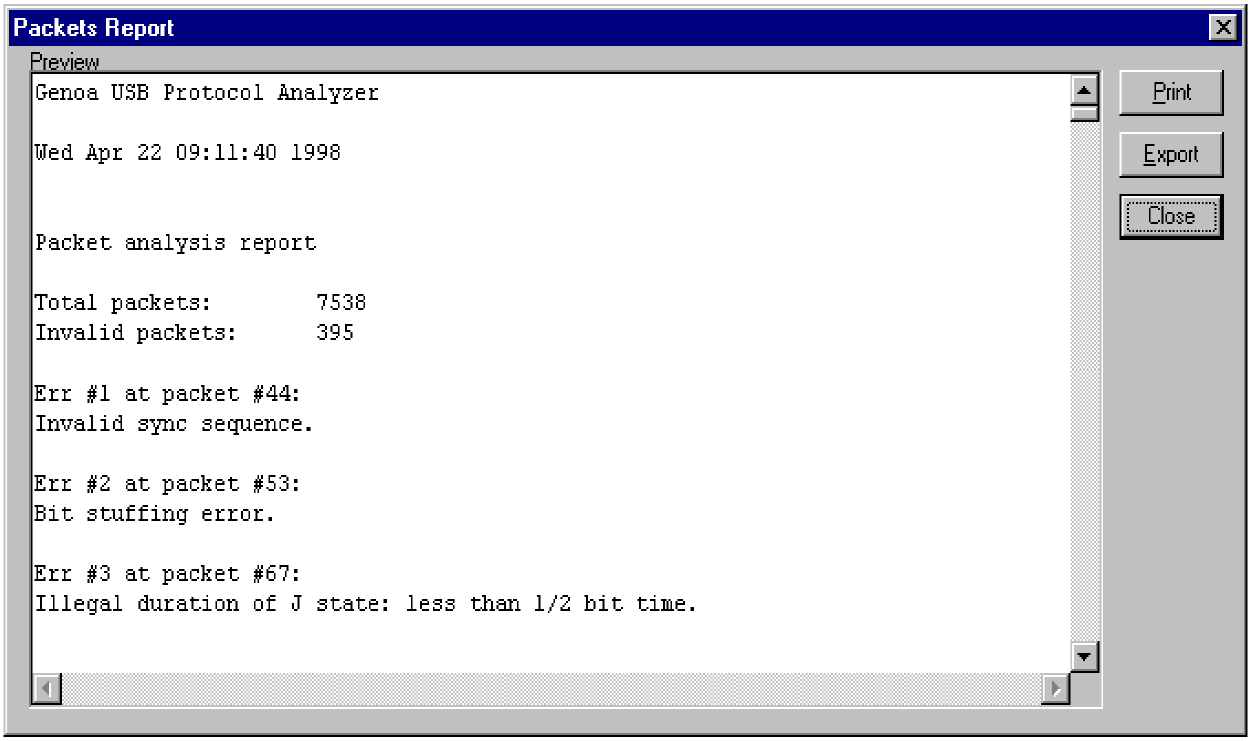
```
Genoa USB Protocol Analyzer

Wed Apr 22 09:11:39 1998


Event analysis report

Total acquisitions:  1016964
Total events:        15076
Signaling errors:    0
```

Event Analysis Report command is available in Results drop menu. The report presents the followings:

- date and time when it has been created
- total number or acquisitions
- total number of events
- total number or signaling errors
- the log of each signaling error: number, the acquisition where it has been detected, and the error description

Refer to Signaling Errors for the list of these errors whose detection is implemented in USB Protocol Analyzer.

Packet Analysis Report



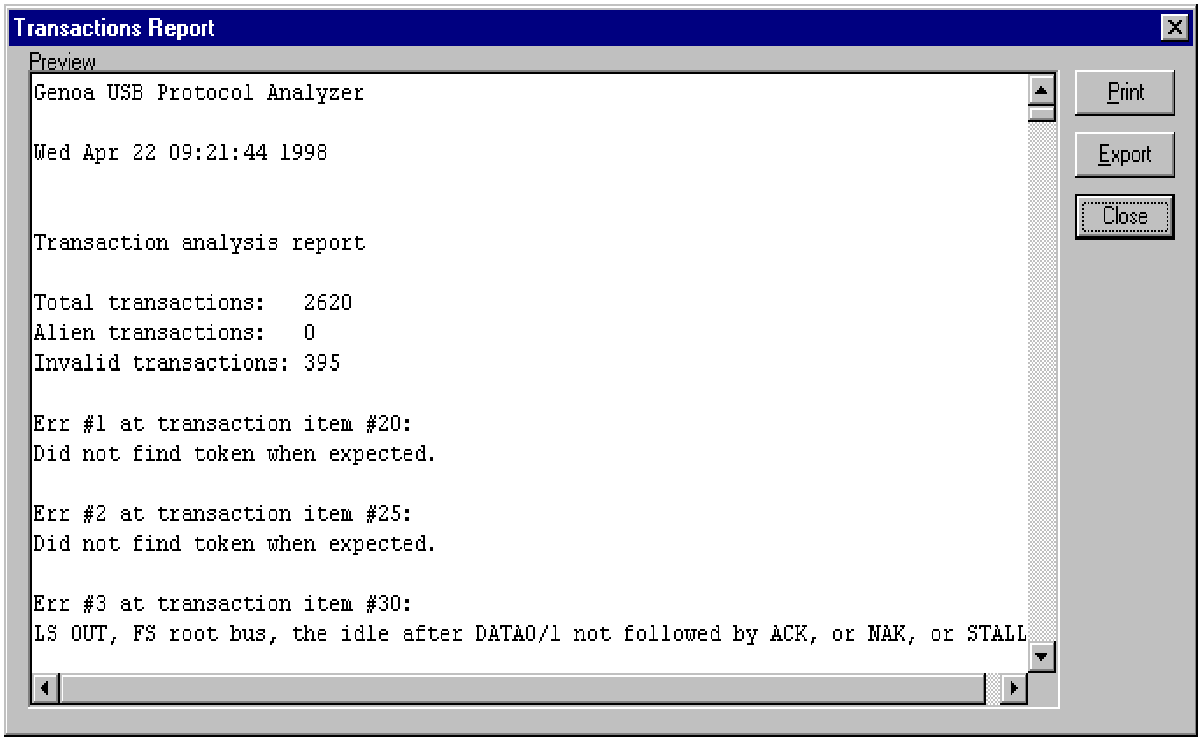
```
Genoa USB Protocol Analyzer

Wed Apr 22 09:11:40 1998


Packet analysis report

Total packets:        7538
Invalid packets:      395

Err #1 at packet #44:
Invalid sync sequence.

Err #2 at packet #53:
Bit stuffing error.

Err #3 at packet #67:
Illegal duration of J state: less than 1/2 bit time.
```

Packet Analysis Report command is available in Results drop menu. The report presents the followings:

- date and time when it has been created
- total number of packets
- the number of invalid packets
- the log of each packet error: error number, packet number, error description

Refer to Packet Errors for the list of these errors whose detection is implemented in USB Protocol Analyzer.

Transaction Analysis Report



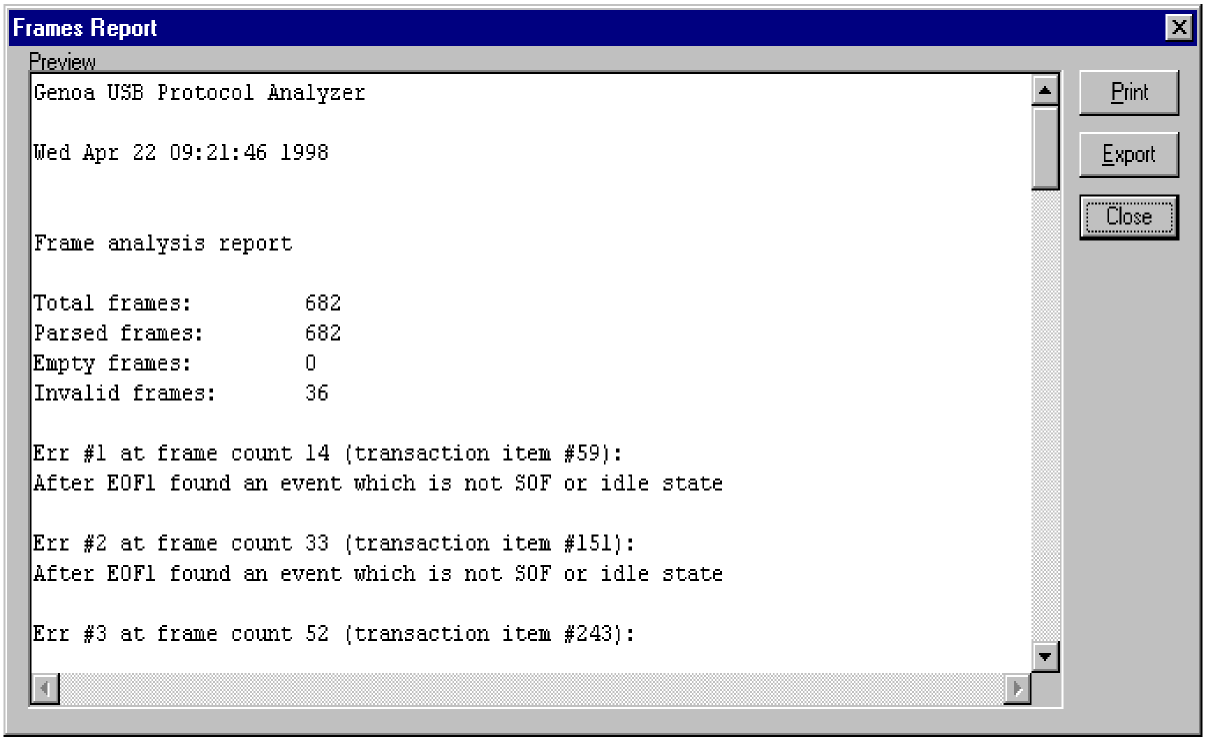
```
Genoa USB Protocol Analyzer

Wed Apr 22 09:21:44 1998


Transaction analysis report

Total transactions:   2620
Alien transactions:   0
Invalid transactions: 395

Err #1 at transaction item #20:
Did not find token when expected.

Err #2 at transaction item #25:
Did not find token when expected.

Err #3 at transaction item #30:
LS OUT, FS root bus, the idle after DATA0/1 not followed by ACK, or NAK, or STALL
```

Transaction Analysis Report command is available in Results drop menu. The report presents the followings:

- date and time when it has been created
- total number of transactions
- the number of alien transactions (refer to Alien Transactions)
- the number of invalid transactions
- the log of each transaction error: error number, transaction item number, error description

Refer to Transaction Errors for the list of these errors whose detection is implemented in USB Protocol Analyzer.

Frame Analysis Report



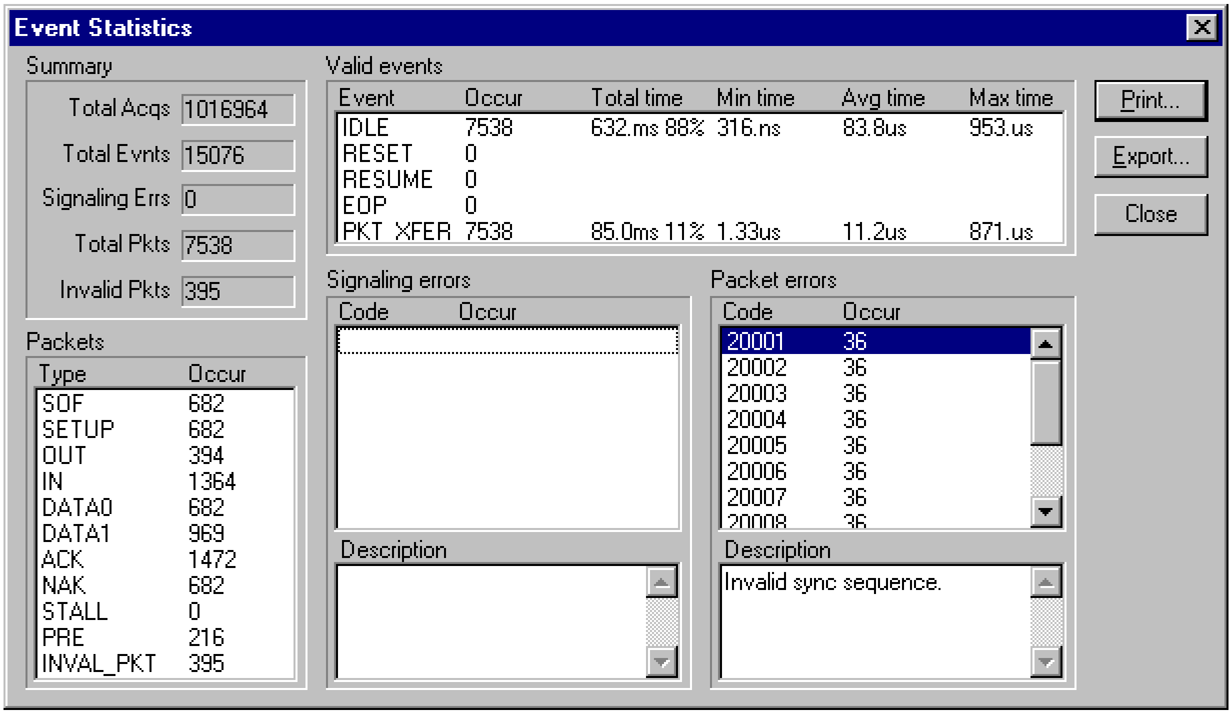
```
Genoa USB Protocol Analyzer

Wed Apr 22 09:21:46 1998


Frame analysis report

Total frames:         682
Parsed frames:        682
Empty frames:         0
Invalid frames:       36

Err #1 at frame count 14 (transaction item #59):
After EOF1 found an event which is not SOF or idle state

Err #2 at frame count 33 (transaction item #151):
After EOF1 found an event which is not SOF or idle state

Err #3 at frame count 52 (transaction item #243):
```

Frame Analysis Report command is available in Results drop menu. The report presents the followings:

- date and time when it has been created
- total number of frames (SOF tokens)
- the number of parsed frames
- the number of empty frames
- the number of invalid frames
- the log of each frame error: error number, frame count, error description

Refer to Frame Errors for the list of these errors whose detection is implemented in USB Protocol Analyzer.

Event Statistics



Summary

Total Acqs 1016964
Total Evnts 15076
Signaling Errs 0
Total Pkts 7538
Invalid Pkts 395

Valid events

Event	Occur	Total time	Min time	Avg time	Max time
IDLE	7538	632.ms 88%	316.ns	83.8us	953.us
RESET	0				
RESUME	0				
EOP	0				
PKT_XFER	7538	85.0ms 11%	1.33us	11.2us	871.us

Packets

Type	Occur
SOF	682
SETUP	682
OUT	394
IN	1364
DATA0	682
DATA1	969
ACK	1472
NAK	682
STALL	0
PRE	216
INVAL_PKT	395

Signaling errors

Code	Occur

Description

Packet errors

Code	Occur
20001	36
20002	36
20003	36
20004	36
20005	36
20006	36
20007	36
20008	36

Description

Invalid sync sequence.

Event Statistics command is available in Results drop menu. This dialog presents statistics data resulted from Event Analysis if statistics were enabled before the start of USB Process.

The dialog contains the following controls:

- Summary group
- Valid Events list
- Packets list
- Signaling Errors group
- Packet Errors group
- Print button
- Export button
- Close button

Summary group indicates the summary of Event Analysis:

- total acquisitions
- total events
- signaling errors
- total packets
- invalid packets

Valid Events list presents global information on the following events:
- IDLE state
- RESET
- RESUME
- EOP (end of packet)
- PKT_XFER (packet transfer)

That global information refers to:
- number of event occurrences
- total time (accumulated, given in time value and percentage)
- min. time (the minimal event duration)
- average time (the average event duration)
- max. time (the maximal event duration)

Packets list presents the number of occurrences of each packet type and PRE (preamble).

Signaling Errors group contains an error list and a description box. The error list presents the number of occurrences of each signaling error which has been detected. The description box displays the description of the error type selected in the error list.

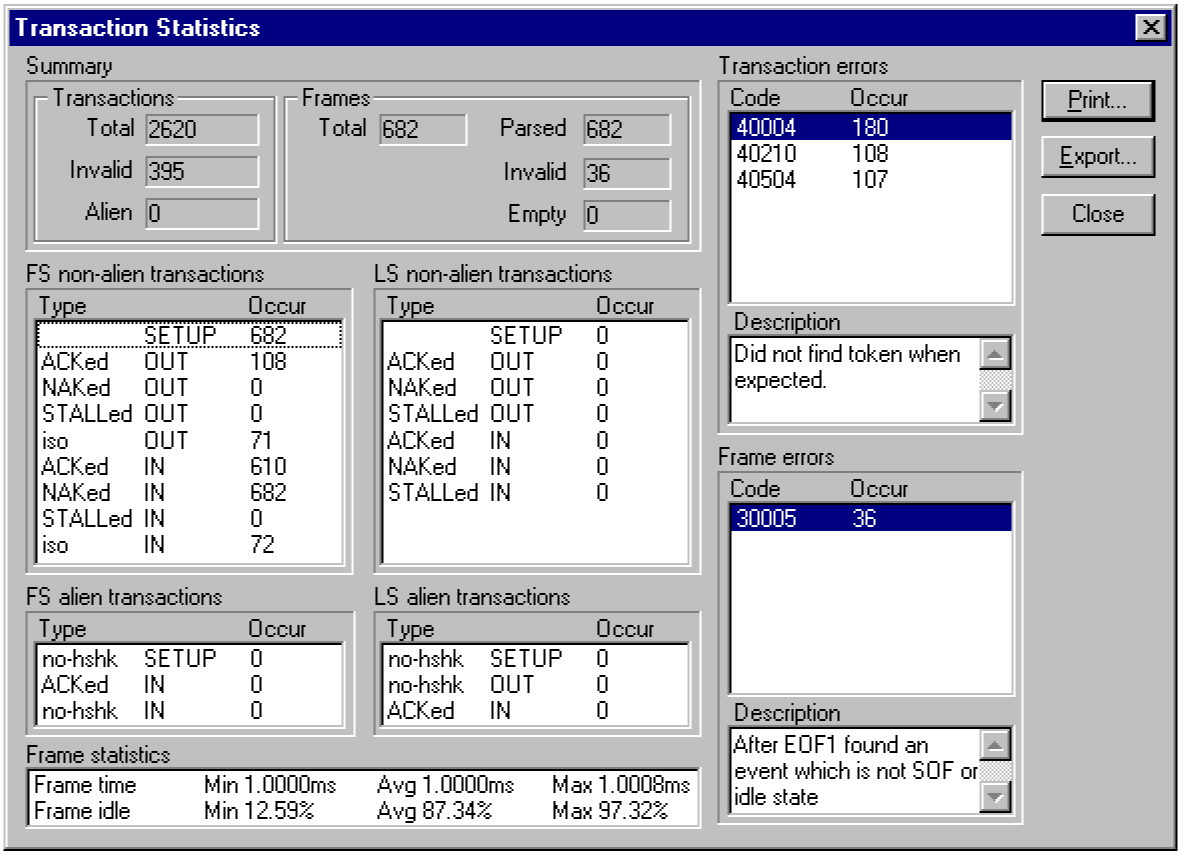
Packet Errors group contains an error list and a description box. The error list presents the number of occurrences of each packet error which has been detected. The description box displays the description of the error type selected in the error list.

Print button brings Print dialog box to allow the user to print Event Statistics.

Export button brings a file selection dialog to allow the user to save Event Statistics in an user defined text file.

Close button is used to close Event Statistics dialog.

Transaction Statistics



Summary

Transactions

Total 2620

Invalid 395

Alien 0

Frames

Total 682

Parsed 682

Invalid 36

Empty 0

FS non-alien transactions

Type		Occur
	SETUP	682
ACKed	OUT	108
NAKed	OUT	0
STALLed	OUT	0
iso	OUT	71
ACKed	IN	610
NAKed	IN	682
STALLed	IN	0
iso	IN	72

LS non-alien transactions

Type		Occur
	SETUP	0
ACKed	OUT	0
NAKed	OUT	0
STALLed	OUT	0
ACKed	IN	0
NAKed	IN	0
STALLed	IN	0

FS alien transactions

Type		Occur
no-hshk	SETUP	0
ACKed	IN	0
no-hshk	IN	0

LS alien transactions

Type		Occur
no-hshk	SETUP	0
no-hshk	OUT	0
ACKed	IN	0

Frame statistics

Frame time	Min 1.0000ms	Avg 1.0000ms	Max 1.0008ms
Frame idle	Min 12.59%	Avg 87.34%	Max 97.32%

Transaction errors

Code	Occur
40004	180
40210	108
40504	107

Description

Did not find token when expected.

Frame errors

Code	Occur
30005	36

Description

After EOF1 found an event which is not SOF or idle state

Transaction Statistics command is available in Results drop menu. This dialog presents statistics data resulted from Transaction Analysis and Frame Analysis if statistics were enabled before the start of USB Process.

The dialog contains the following controls:

- Summary group
- FS non-alien transactions list
- LS non-alien transactions list
- FS alien transactions list
- LS alien transactions list
- Frame statistics box
- Transaction errors group
- Frame errors group
- Print button
- Export button
- Close button

Summary group indicates the summary of Transaction Analysis and Frame Analysis:

- total transactions (SETUP, OUT, IN, INVALID)
- invalid transactions
- alien transactions
- total frames (SOFs)
- parsed frames
- invalid frames
- empty frames

FS non-alien transactions list presents number of occurrences of FS non-alien transactions (for alien attribute refer to Alien Transactions):

- SETUP
- ACKed OUT
- NAKed OUT
- STALLed OUT
- iso OUT (FS OUT transaction without handshake)
- ACKed IN
- NAKed IN
- STALLed IN
- iso IN (FS IN transactions without handshake)

LS non-alien transactions list presents number of occurrences of LS non-alien transactions (for alien attribute refer to Alien Transactions):

- SETUP
- ACKed OUT
- NAKed OUT
- STALLed OUT
- ACKed IN
- NAKed IN
- STALLed IN

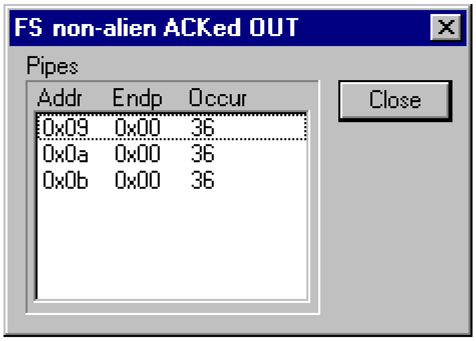
FS alien transactions list presents number of occurrences of FS alien transactions (for alien attribute refer to Alien Transactions):

- SETUP
- ACKed IN
- no-hshk IN (IN transaction without handshake)

LS alien transactions list presents number of occurrences of LS alien transactions (for alien attribute refer to Alien Transactions):

- SETUP
- no-hshk OUT (OUT transaction without handshake)
- ACKed IN

When double click a transaction in any of these lists, the program brings Transaction Details dialog:



Addr	Endp	Occur
0x09	0x00	36
0x0a	0x00	36
0x0b	0x00	36

Frame statistics box displays the followings:

- minimal, average and maximal duration for valid frames
- minimal, average and maximal frame idle duration for valid frames

This information is available only if the capture has been made with Record Idle on during USB Process and Frame Analysis has been completed with statistics set ON.

Transaction Errors group contains an error list and a description box. The error list presents the number of occurrences of each transaction error which has been detected. The description box displays the description of the error type selected in the error list.

Frame Errors group contains an error list and a description box. The error list presents the number of occurrences of each frame error which has been detected. The description box displays the description of the error type selected in the error list.

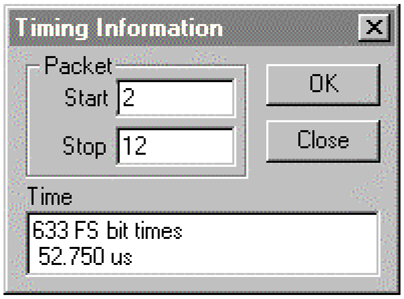
Print button brings Print dialog box to allow the user to print Event Statistics.

Export button brings a file selection dialog to allow the user to save Transaction Statistics in an user defined text file.

Close button is used to close Transaction Statistics dialog.

Timing Info

This command is available in Results drop menu being enabled on Event Layer only . When activated, the program presents Timing Information dialog:



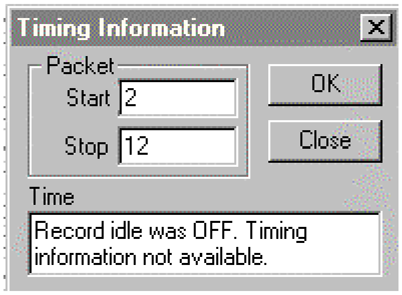
Start 2

Stop 12

Time

633 FS bit times
52.750 us

This dialog presents the time distance between two user defined packets. That information is indicated in time value and FS bit times, being available only if the capture has been made with Record Idle ON during USB Process. Otherwise the program will present the dialog below:



Start 2

Stop 12

Time

Record idle was OFF. Timing information not available.

Isolating Traffic Errors

Finding Traffic Errors

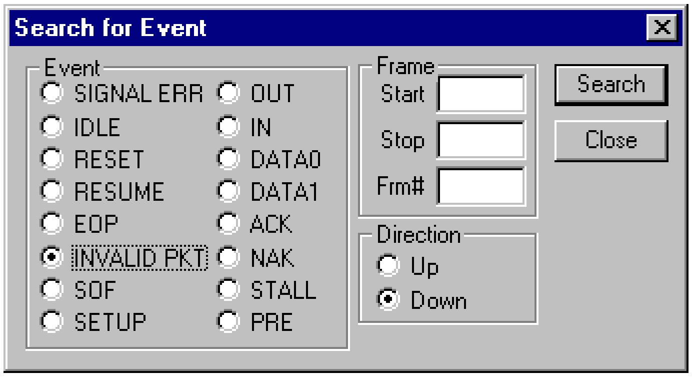
One of the goals of the USB Protocol Analyzer is to detect protocol errors in the traffic which has been captured and analyzed, and to present these errors to the user.

The fastest way to get a global picture of the whole traffic, errors included, is to look at Event Statistics and Transaction Statistics (accessible by using Statistics command from Results drop menu).

Another quick way to get global results is to use Summary, Event Analysis report, Packet Analysis report, and Frame Analysis report.

The Summary presents a briefing of the whole USB Process. The reports present a summary of each analysis stage and the list of specific errors detected during that stage. Those lists may be used in conjunction with Go to commands to reach the point in the traffic where a specific error has been detected.

Search commands may be used as well to get to the traffic errors on the current traffic layer:

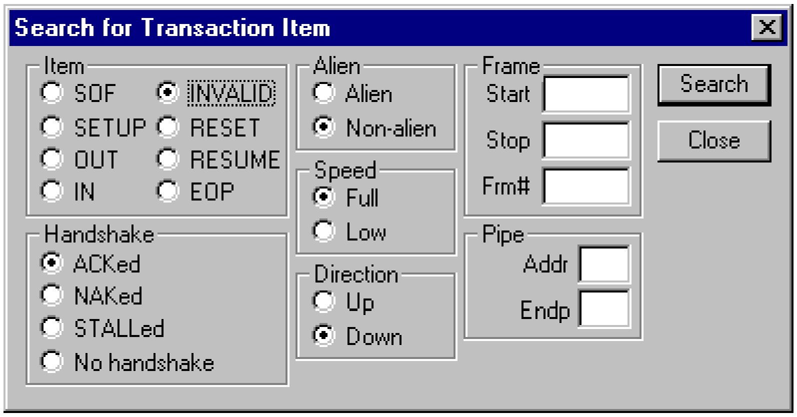


Event
○ SIGNAL ERR ○ OUT
○ IDLE ○ IN
○ RESET ○ DATA0
○ RESUME ○ DATA1
○ EOP ○ ACK
● INVALID PKT ○ NAK
○ SOF ○ STALL
○ SETUP ○ PRE

Frame
Start
Stop
Frm#

Direction
○ Up
● Down

Select SIGNAL_ERR or INVALID_PKT radio button to find a signaling error, respectively a packet error. This command is enabled on Event Layer only.



Item
○ SOF ● INVALID
○ SETUP ○ RESET
○ OUT ○ RESUME
○ IN ○ EOP

Handshake
● ACKed
○ NAKed
○ STALLed
○ No handshake

Alien
○ Alien
● Non-alien

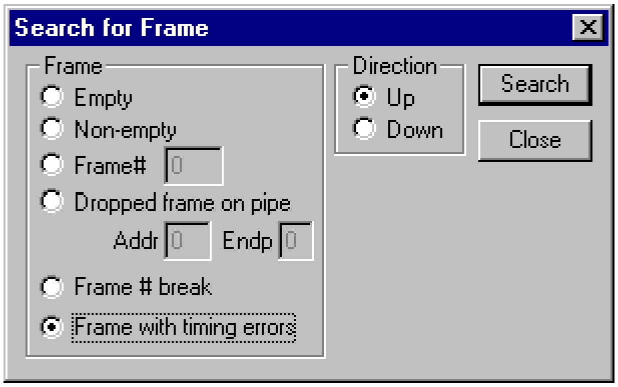
Speed
● Full
○ Low

Direction
○ Up
● Down

Frame
Start
Stop
Frm#

Pipe
Addr
Endp

Select INVALID radio button to find a transaction error. This command is enabled on Transaction Layer only.



Search for Frame

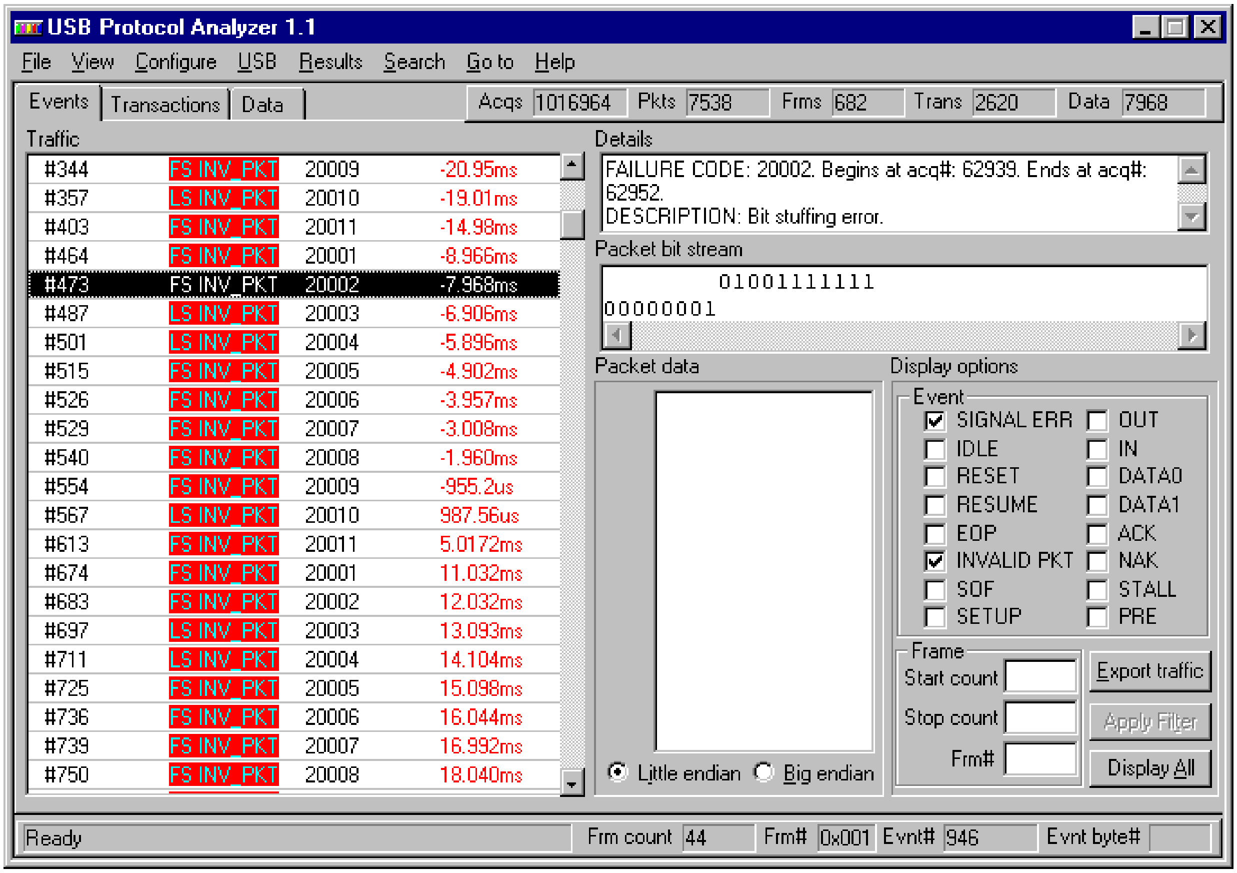
Frame
○ Empty
○ Non-empty
○ Frame# 0
○ Dropped frame on pipe
Addr 0 Endp 0
○ Frame # break
● Frame with timing errors

Direction
● Up
○ Down

Select Frame with timing errors radio button to find the SOF token corresponding to an invalid frame. That frame is prompted in the Traffic window by SOF INV!. This command is enabled on Transaction Layer only.

The best way to view traffic errors is to disable in display options all traffic items but errors. The user may select an error in the traffic and switch between filtered and unfiltered traffic(by pressing Apply Filter, respectively Display All buttons). That will allow to see the error context (i.e. all traffic items around the error occurrence).

The picture below presents the errors display on Event Layer. Note that in display options, only SIGNAL ERR and INVALID PKT traffic items are selected.



Acqs 1016964 Pkts 7538 Frms 682 Trans 2620 Data 7968

Traffic

#344	FS INV_PKT	20009	-20.95ms
#357	LS INV_PKT	20010	-19.01ms
#403	FS INV_PKT	20011	-14.98ms
#464	FS INV_PKT	20001	-8.966ms
#473	FS INV_PKT	20002	-7.968ms
#487	LS INV_PKT	20003	-6.906ms
#501	LS INV_PKT	20004	-5.896ms
#515	FS INV_PKT	20005	-4.902ms
#526	FS INV_PKT	20006	-3.957ms
#529	FS INV_PKT	20007	-3.008ms
#540	FS INV_PKT	20008	-1.960ms
#554	FS INV_PKT	20009	-955.2us
#567	LS INV_PKT	20010	987.56us
#613	FS INV_PKT	20011	5.0172ms
#674	FS INV_PKT	20001	11.032ms
#683	FS INV_PKT	20002	12.032ms
#697	LS INV_PKT	20003	13.093ms
#711	LS INV_PKT	20004	14.104ms
#725	FS INV_PKT	20005	15.098ms
#736	FS INV_PKT	20006	16.044ms
#739	FS INV_PKT	20007	16.992ms
#750	FS INV_PKT	20008	18.040ms

Details

FAILURE CODE: 20002. Begins at acq#: 62939. Ends at acq#: 62952.
DESCRIPTION: Bit stuffing error.

Packet bit stream

```
            01001111111
00000001
```

● Little endian ○ Big endian

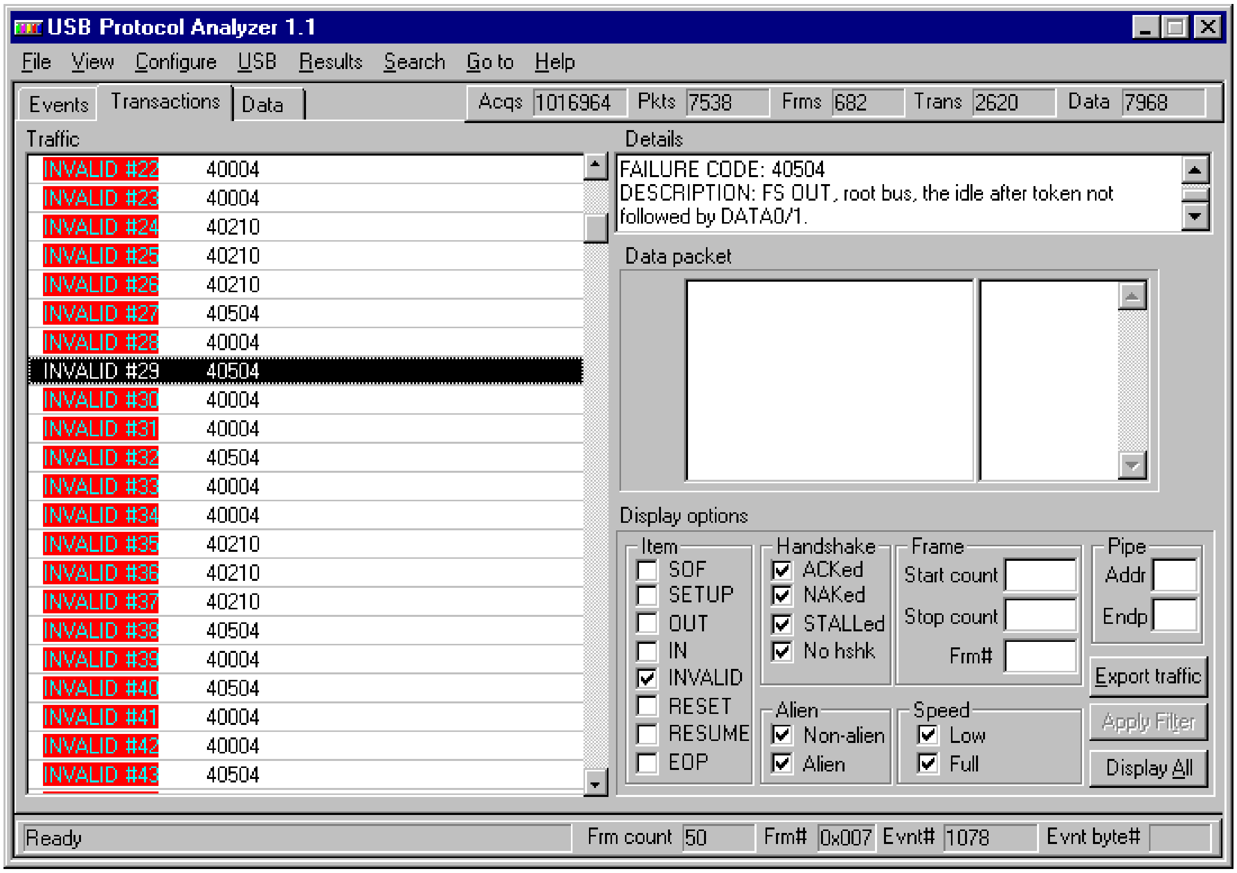
Event

☑ SIGNAL ERR	☐ OUT
☐ IDLE	☐ IN
☐ RESET	☐ DATA0
☐ RESUME	☐ DATA1
☐ EOP	☐ ACK
☑ INVALID PKT	☐ NAK
☐ SOF	☐ STALL
☐ SETUP	☐ PRE

Frame
Start count
Stop count
Frm#

Ready Frm count 44 Frm# 0x001 Evnt# 946 Evnt byte#

The picture below presents the errors display on Transaction Layer. Note that in display options, only INVALID traffic item is selected.



Acqs 1016964 Pkts 7538 Frms 682 Trans 2620 Data 7968

INVALID #22	40004
INVALID #23	40004
INVALID #24	40210
INVALID #25	40210
INVALID #26	40210
INVALID #27	40504
INVALID #28	40004
INVALID #29	40504
INVALID #30	40004
INVALID #31	40004
INVALID #32	40504
INVALID #33	40004
INVALID #34	40004
INVALID #35	40210
INVALID #36	40210
INVALID #37	40210
INVALID #38	40504
INVALID #39	40004
INVALID #40	40504
INVALID #41	40004
INVALID #42	40004
INVALID #43	40504

FAILURE CODE: 40504
DESCRIPTION: FS OUT, root bus, the idle after token not followed by DATA0/1.

Item
☐ SOF
☐ SETUP
☐ OUT
☐ IN
☑ INVALID
☐ RESET
☐ RESUME
☐ EOP

Handshake
☑ ACKed
☑ NAKed
☑ STALLed
☑ No hshk

Alien
☑ Non-alien
☑ Alien

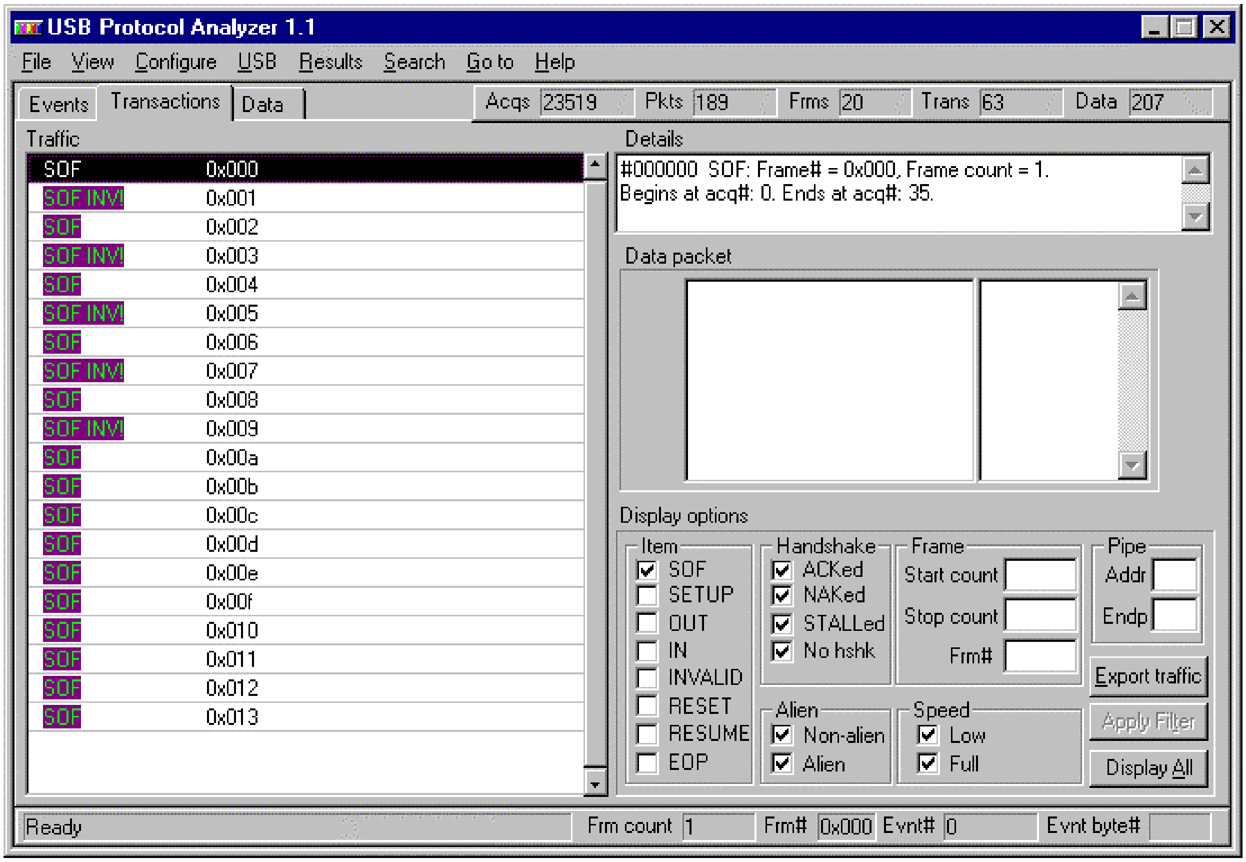
Frame
Start count
Stop count
Frm#

Speed
☑ Low
☑ Full

Pipe
Addr
Endp

Ready Frm count 50 Frm# 0x007 Evnt# 1078 Evnt byte#

The picture below presents the display of frames only. The SOF token of an invalid frame (i.e. a frame with timing errors) is prompted as SOF INV!. Note that in display options, only SOF traffic item is selected.


USB Protocol Analyzer 1.1
File View Configure USB Results Search Go to Help
Events Transactions Data
Export traffic
Apply Filter
Display All

Acqs 23519 Pkts 189 Frms 20 Trans 63 Data 207

Traffic

SOF	0x000
SOF INV!	0x001
SOF	0x002
SOF INV!	0x003
SOF	0x004
SOF INV!	0x005
SOF	0x006
SOF INV!	0x007
SOF	0x008
SOF INV!	0x009
SOF	0x00a
SOF	0x00b
SOF	0x00c
SOF	0x00d
SOF	0x00e
SOF	0x00f
SOF	0x010
SOF	0x011
SOF	0x012
SOF	0x013

Details

#000000 SOF: Frame# = 0x000, Frame count = 1.
Begins at acq#: 0. Ends at acq#: 35.

Data packet

Display options

Item: ☑ SOF ☐ SETUP ☐ OUT ☐ IN ☐ INVALID ☐ RESET ☐ RESUME ☐ EOP

Handshake: ☑ ACKed ☑ NAKed ☑ STALLed ☑ No hshk

Frame: Start count Stop count Frm#

Pipe: Addr Endp

Alien: ☑ Non-alien ☑ Alien

Speed: ☑ Low ☑ Full

Ready Frm count 1 Frm# 0x000 Evnt# 0 Evnt byte#

Note that frame errors may exist even if there are no other errors (signaling errors, packet errors, or transaction errors).

Viewing Signals

In order to view the waveform of a particular traffic item (event, packet, transaction, etc., but especially protocol errors), the user must have on the logic analyzer the capture of the traffic displayed by the USB Protocol Analyzer. It is recommended to save the capture on the logic analyzer to have it available for later use.

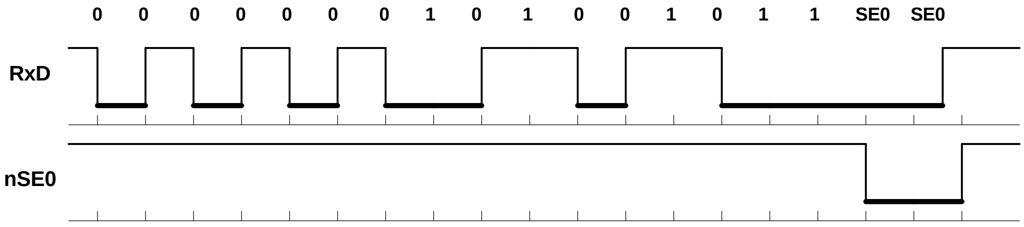
Each traffic item (event or transaction) has an acquisition range. That range is displayed for the current traffic item in Details window on Event Layer or on Transaction Layer. The range is defined by the number of the start acquisition and the number of the stop acquisition. These numbers are relative to the start of the capture. Because the capture stored on the logic analyzer and the capture stored in on the Capture Board have the same trigger, is easy to correlate the acquisition numbers from the logic analyzer with those shown in Details window.

When interpreting the waveform of a traffic item, it is important to remember the following things:

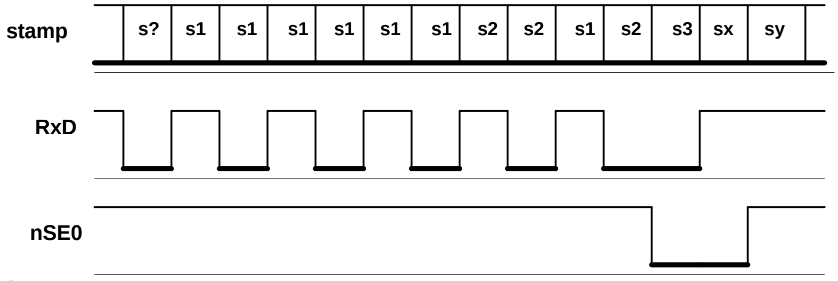
- the bus state is indicated on RXD and NSE0 labels
- the time stamp is indicated on STAMP label (6 channel label), its resolution being 16.66ns (60MHz sampling frequency)
- the duration of the current state is indicated on the next time stamp

The example below shows how to interpret the waveform of an ACK packet.

The ACK packet consists of 2 bytes: the sync byte (0x80) and the PID byte (0xd2). The bit stream of this packet will be: 0000000101001011. On a FS bus, the packet will have the following NZRI representation (nSE0 has been added to indicate the end of packet):



The waveform of this packet, presented on the logic analyzer screen is presented below:



where:
s? is unknown (indicates the duration of the previous state)
s1 is a time stamp corresponding to 1 FS bit time
s2 is a time stamp corresponding to 2 FS bit times
s3 is a time stamp corresponding to 3 FS bit times
sx + sy = s2 (i.e. sx + sy indicates the duration of SE0 state).

Note that the time stamp of the current state is presented by the next acquisition. In the example above, the time stamp of s1 FS bit times of the first K state of ACK packet is presented in the 2nd acquisition of that packet.

The time stamp is given in sampling periods (16.66ns). Theoretically a FS bit time will have a time stamp of 5. The table below presents the relationship between the time stamp presented by the Acquisition Machine and the bit times:

Time stamp conversion for FS bit times (a FS bit cell is 83.33ns):

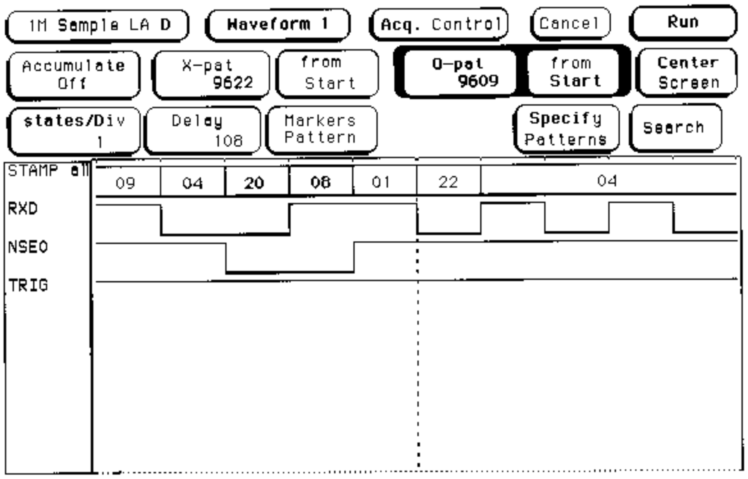
1 FS bit time	1/2.. 3/2 FS bit cells	3..7 clocks
2 FS bit times	3/2.. 5/2 FS bit cells	8..12 clocks
3 FS bit times	5/2.. 7/2 FS bit cells	13..17 clocks
4 FS bit times	7/2.. 9/2 FS bit cells	18..22 clocks
5 FS bit times	9/2..11/2 FS bit cells	23..27 clocks
6 FS bit times	11/2..13/2 FS bit cells	28..32 clocks
7 FS bit times	13/2..15/2 FS bit cells	33..37 clocks

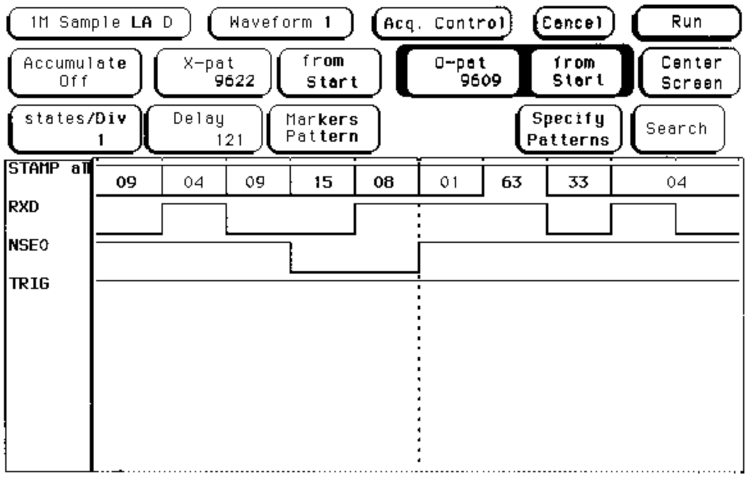
Time stamp conversion for LS bit times (a LS bit cell is 666.66ns)

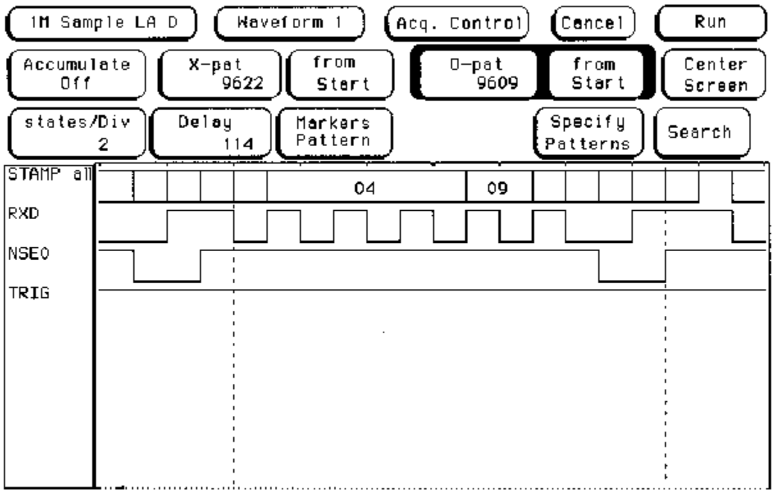
1 LS bit time	1/2.. 3/2 LS bit cells	20..59 clocks
2 LS bit times	3/2.. 5/2 LS bit cells	60..99 clocks
3 LS bit times	5/2.. 7/2 LS bit cells	100..139 clocks
4 LS bit times	7/2.. 9/2 LS bit cells	140..179 clocks
5 LS bit times	9/2..11/2 LS bit cells	180..219 clocks
6 LS bit times	11/2..13/2 LS bit cells	220..259 clocks
7 LS bit times	13/2..15/2 LS bit cells	260..299 clocks

By using these time stamp conversion tables, the user may check the packet signaling. Note that the time stamp is one acquisition clock delayed with respect to the bus state which had that duration. That is when looking to a bus state, the duration of that state is indicated in the time stamp of the next acquisition.

The following pictures illustrate the logic analyzer screens after centering the waveform of an ACK packet on O marker (beginning), X marker (end) , respectively O and X markers (logic analyzer HP16555A):

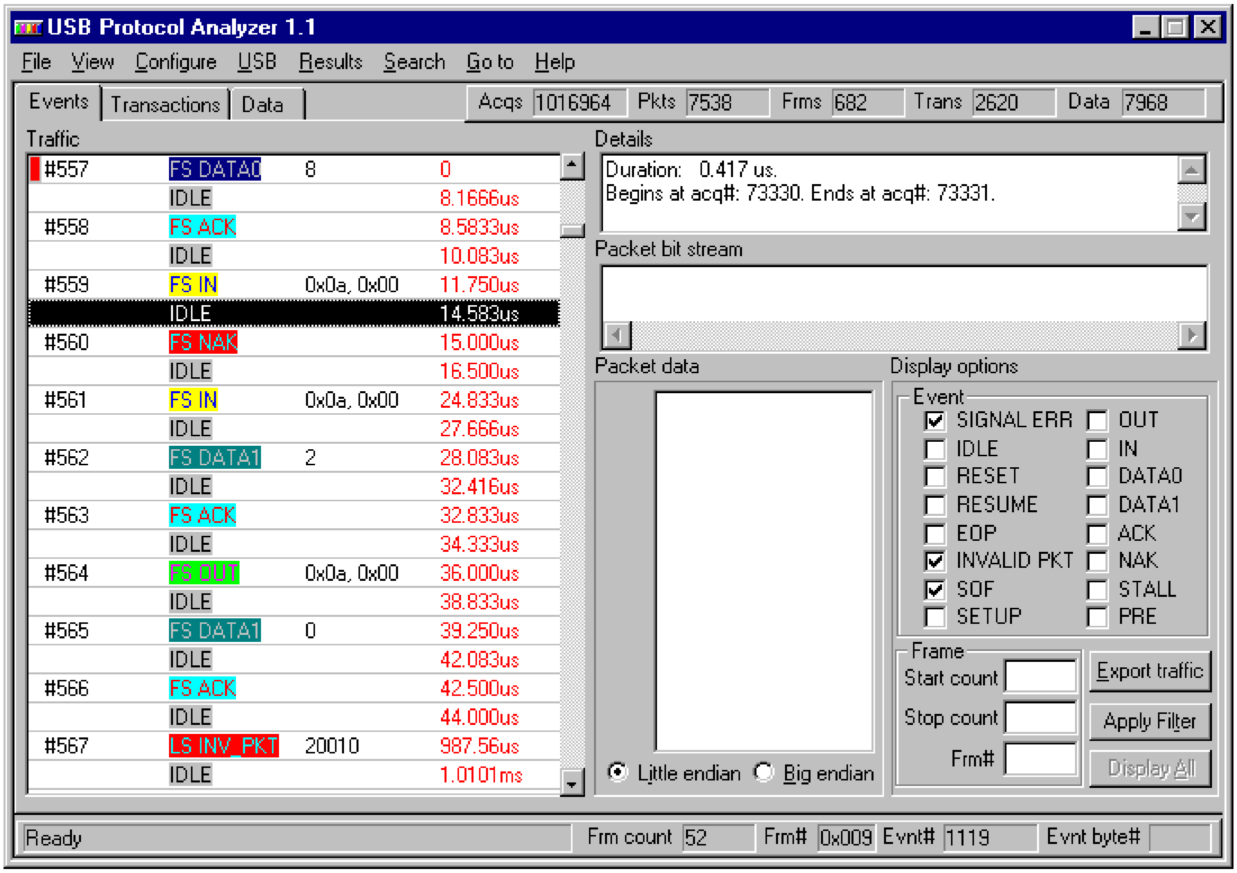

Accumulate Off
X-pat 9622 from Start
O-pat 9609 from Start
states/Div 1
Delay 108


1M Sample LA D
Waveform 1
Acq. Control
Cancel
Run
Accumulate Off
X-pat 9622
from Start
O-pat 9609
from Start
Center Screen
states/Div 1
Delay 121
Markers Pattern
Specify Patterns
Search
STAMP all
09
04
09
15
08
01
63
33
04
RXD
NSEO
TRIG


1M Sample LA D
Waveform 1
Acq. Control
Cancel
Run
Accumulate Off
X-pat 9622
from Start
O-pat 9609
from Start
Center Screen
states/Div 2
Delay 114
Markers Pattern
Specify Patterns
Search
STAMP all
04
09
RXD
NSEO
TRIG

Viewing Event Traffic

Event Layer



Acqs 1016964 Pkts 7538 Frms 682 Trans 2620 Data 7968

#557	FS DATA0	8	0
	IDLE		8.1666us
#558	FS ACK		8.5833us
	IDLE		10.083us
#559	FS IN	0x0a, 0x00	11.750us
	IDLE		14.583us
#560	FS NAK		15.000us
	IDLE		16.500us
#561	FS IN	0x0a, 0x00	24.833us
	IDLE		27.666us
#562	FS DATA1	2	28.083us
	IDLE		32.416us
#563	FS ACK		32.833us
	IDLE		34.333us
#564	FS OUT	0x0a, 0x00	36.000us
	IDLE		38.833us
#565	FS DATA1	0	39.250us
	IDLE		42.083us
#566	FS ACK		42.500us
	IDLE		44.000us
#567	LS INV_PKT	20010	987.56us
	IDLE		1.0101ms

Duration: 0.417 us.
Begins at acq#: 73330. Ends at acq#: 73331.

● Little endian ○ Big endian

☑ SIGNAL ERR ☐ OUT
☐ IDLE ☐ IN
☐ RESET ☐ DATA0
☐ RESUME ☐ DATA1
☐ EOP ☐ ACK
☑ INVALID PKT ☐ NAK
☑ SOF ☐ STALL
☐ SETUP ☐ PRE

Start count
Stop count
Frm#

Ready Frm count 52 Frm# 0x009 Evnt# 1119 Evnt byte#

The Event Layer is accessed by clicking the tab of its folder, or by pressing `F2` key. This layer presents the USB traffic in terms of USB events. It contains the following controls:

- the layer tab which may be clicked to switch on this layer
- the Traffic window
- the Details window
- the Packet Data window
- the Bit Stream window
- the Display Options group

Also the Traffic Information bar and the Status Bar are available as on any other traffic layer.

The event traffic displays the list USB events resulted from Event Analysis and Packet Analysis. The following event types may be shown:

- SIGNAL ERR
- IDLE

- RESET
- EOP
- RESUME
- packet transfer, specified by the packet type: INVALID PKT, SOF, SETUP, IN, OUT, DATA0, DATA1, ACK, NAK, STALL, PRE (the preamble is not a packet but the program will present it as a packet transfer because it contains two bytes: sync and PID).

SIGNAL ERR event is defined as a non-compliance in USB signaling, other than USB packet signaling. Such non-compliances may be: K state follows SE0 state, invalid EOP (too long, too short), invalid RESET (too short), etc. Refer to Signaling Errors for the complete list of these errors whose detection is implemented in the program.

IDLE event is defined as J state, detected in other situations than packet transfer. Example: after EOP, after RESET, after RESUME, etc. J state seen in the middle of a packet transfer is not IDLE event.

RESET event is defined as the SE0 state for at least 10ms.

RESUME event is defined as K state for at least 20ms, followed by LS EOP (low speed end of packet).

EOP event is defined as an end of packet signaling which does not follow a packet transfer. Such EOPs may be seen on a low speed bus (provided by the upstream hub).

INVALID PKT event is a packet presenting a format error: invalid sync, PID error, bit stuff error, CRC error, etc..

SOF event is the start of frame packet. If frame analysis has been performed within the USB Process, then frames with invalid timing are signaled by using SOF INV!.

SETUP event is SETUP token packet.

IN event is IN token packet.

OUT event is OUT token packet.

DATA0 event is DATA0 data packet.

DATA1 event is DATA1 data packet.

ACK event is ACK handshake packet

NAK event is NAK handshake packet

STALL event is STALL handshake packet.

PRE event is PRE (preamble) packet.

For each event which has been detected, the event traffic window presents an event prompt .

If the number of max. errors for Packet Analysis specified in Resume USB Process dialog or New USB Process dialog is reached during the USB Process, then the traffic may end with UNDECODED PKT items.

In Details window the program presents details on the currently selected event in the Traffic window. Those details depend on the event type.

Bit Stream window presents the packet bit stream, when the event cursor selects a invalid packet which has not been decoded. Sync bits and stuffed bits are presented on the lower row of that window, while the data bits are presented on the higher row. If the packet is invalid because has a sync error or a bit stuff error, the bit stream decoding stops at the place where the error is detected.

If the currently selected event in Traffic window is a decoded packet (that means a valid packet or a packet presenting a CRC error), the Bit Stream window stays empty.

The Packet Data window presents the body of a decoded packet, i.e. a packet having correct sync and stuffed bits. Sync, PID, and CRC are included. The packet body indicates the CRC, regardless if CRC is correct or not.

The packet body is represented in binary, hex, and ASCII. The binary representation may use little or big endian order, if Little endian, respectively Big endian radio button is pressed.

The number of the selected byte in this window is indicated in Evnt byte# field. When the first byte is selected (i.e. sync byte), the that field displays zero.

If the packet is not decoded as result of an error detected in sync sequence or in bit stuffing, then packet data window stays empty.

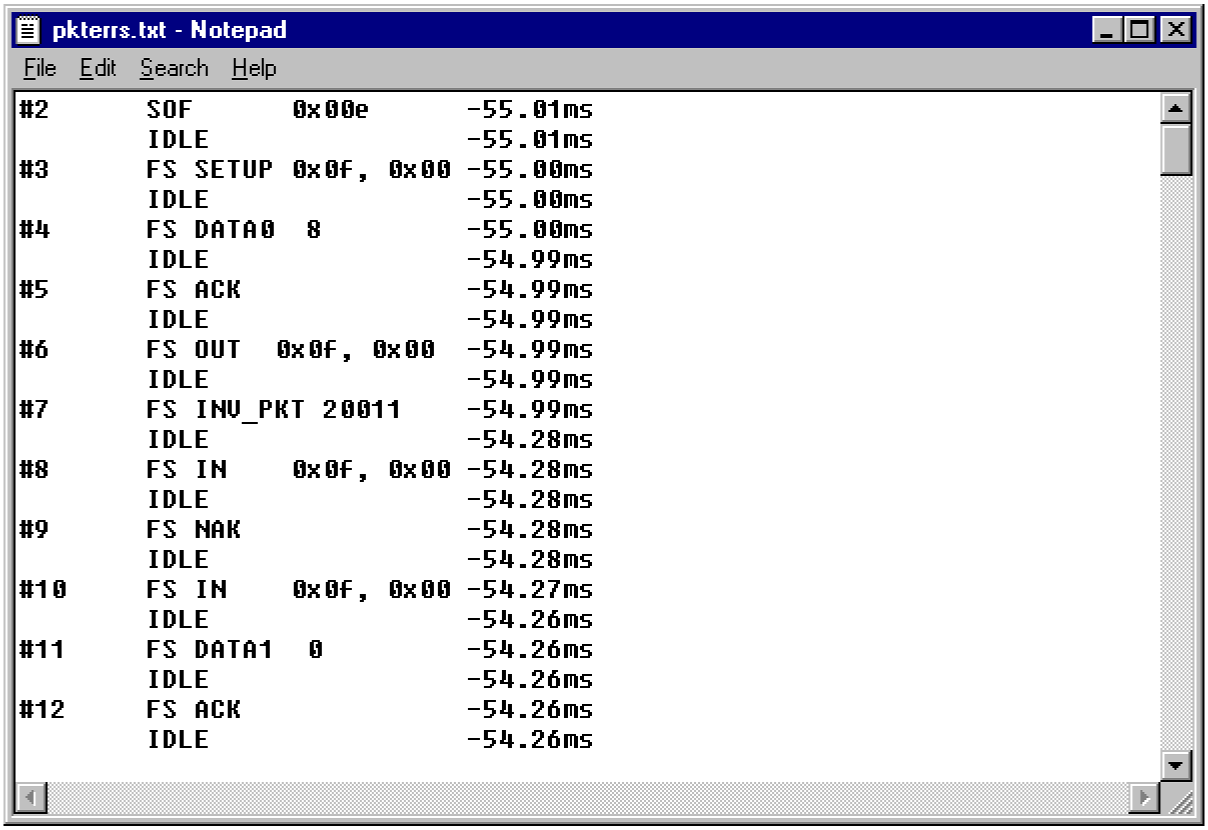
Display options allow the user to specify the events to be displayed in Traffic window.

Event group allows the user to specify the events to be displayed in the filtered traffic. Each event has assigned a check box . Event selection options are ORed. For example if EOP and IDLE check boxes are on, then EOP and IDLE events will be displayed.

Frame group allows the user to specify the frame range for event display.

Display options have available two buttons: Display All, and Apply Filter. When the first button is pressed, the event traffic window will display all events around the event cursor. When Apply Filter button is pressed, the event traffic window will display events selected according to display options. If the current event is enabled by display filter, the traffic focus is preserved after pressing Apply Filter. Otherwise the event cursor will be set on the closest event enabled by display filter.

Export Traffic button allows the user to save the filtered traffic in a user defined text file. The traffic format in that file is similar to the traffic displayed in Traffic window:

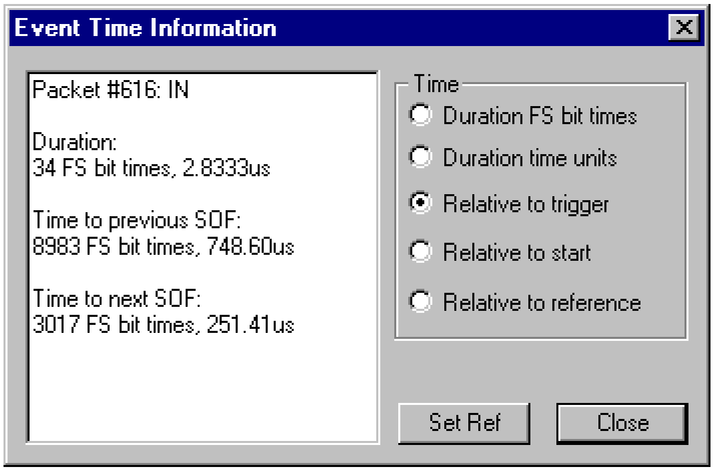


```
#2      SOF       0x00e      -55.01ms
        IDLE                 -55.01ms
#3      FS SETUP  0x0f, 0x00 -55.00ms
        IDLE                 -55.00ms
#4      FS DATA0   8         -55.00ms
        IDLE                 -54.99ms
#5      FS ACK               -54.99ms
        IDLE                 -54.99ms
#6      FS OUT   0x0f, 0x00  -54.99ms
        IDLE                 -54.99ms
#7      FS INV_PKT 20011     -54.99ms
        IDLE                 -54.28ms
#8      FS IN     0x0f, 0x00 -54.28ms
        IDLE                 -54.28ms
#9      FS NAK               -54.28ms
        IDLE                 -54.28ms
#10     FS IN     0x0f, 0x00 -54.27ms
        IDLE                 -54.26ms
#11     FS DATA1   0         -54.26ms
        IDLE                 -54.26ms
#12     FS ACK               -54.26ms
        IDLE                 -54.26ms
```

Up to 1000 traffic items may be exported. This command allows the user to save the filtered traffic in a text file. That file may be loaded, viewed and printed with a text utility (as NotePad for example).

Event Time Information

This command may be activated on the Event Layer only, either by clicking the right mouse button on the desired packet, or by selecting that packet and pressing SPACE bar. At that moment the program opens Event time information dialog :



Packet #616: IN

Duration:
34 FS bit times, 2.8333us

Time to previous SOF:
8983 FS bit times, 748.60us

Time to next SOF:
3017 FS bit times, 251.41us

Time
○ Duration FS bit times
○ Duration time units
● Relative to trigger
○ Relative to start
○ Relative to reference

This dialog indicates the packet duration and its position within the current frame. The packet duration and position are given in FS bit times and real time units. The packet position is available only if the capture has been performed with Record Idle option ON.

The dialog provides as well radio button to choose the time information displayed on the last column of Traffic window:

- event duration in FS bit times, when Duration in FS bit times radio button is pressed
- event duration in time units, when Duration time units radio button is pressed
- event position relative to trigger, when Relative to trigger radio button is pressed
- event position relative to start, when Relative to start radio button is pressed
- event position relative to reference, when Relative to reference radio button is pressed

The event duration is displayed in black on white, between brackets.

The position relative to trigger is displayed in the color chosen for the trigger marker in Event traffic colors dialog.

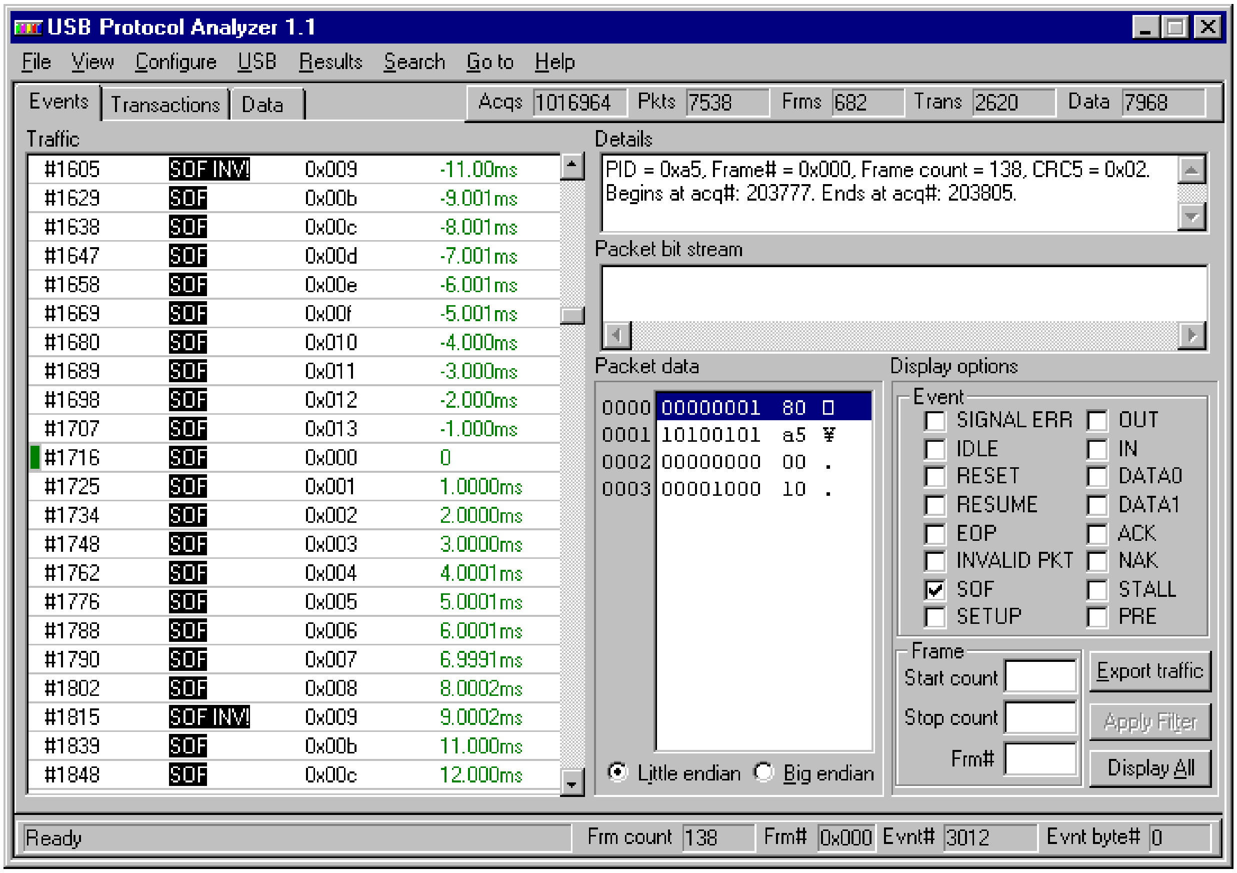
The position relative to start is displayed in black on white.

The position relative to start is displayed in the color chosen for the reference marker in Event traffic colors dialog.

In this dialog the user may set the reference on the event selected with the right mouse button before opening the dialog by pressing Set Ref button.

When Close button is pressed, the Traffic window is redisplayed to reflect the new options.

Frame timing is easy to be viewed by setting the reference frame and by selecting SOF traffic item in display options:



Acqs 1016964 Pkts 7538 Frms 682 Trans 2620 Data 7968

```
#1605   SOF INV!   0x009   -11.00ms
#1629   SOF        0x00b   -9.001ms
#1638   SOF        0x00c   -8.001ms
#1647   SOF        0x00d   -7.001ms
#1658   SOF        0x00e   -6.001ms
#1669   SOF        0x00f   -5.001ms
#1680   SOF        0x010   -4.000ms
#1689   SOF        0x011   -3.000ms
#1698   SOF        0x012   -2.000ms
#1707   SOF        0x013   -1.000ms
#1716   SOF        0x000   0
#1725   SOF        0x001   1.0000ms
#1734   SOF        0x002   2.0000ms
#1748   SOF        0x003   3.0000ms
#1762   SOF        0x004   4.0001ms
#1776   SOF        0x005   5.0001ms
#1788   SOF        0x006   6.0001ms
#1790   SOF        0x007   6.9991ms
#1802   SOF        0x008   8.0002ms
#1815   SOF INV!   0x009   9.0002ms
#1839   SOF        0x00b   11.000ms
#1848   SOF        0x00c   12.000ms
```

PID = 0xa5, Frame# = 0x000, Frame count = 138, CRC5 = 0x02.
Begins at acq#: 203777. Ends at acq#: 203805.

```
0000 00000001  80  □
0001 10100101  a5  ¥
0002 00000000  00  .
0003 00001000  10  .
```

● Little endian ○ Big endian

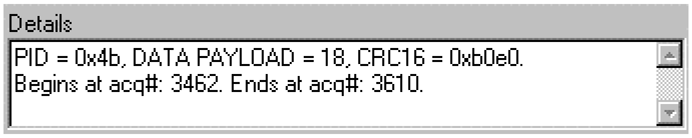
Event

☐ SIGNAL ERR	☐ OUT
☐ IDLE	☐ IN
☐ RESET	☐ DATA0
☐ RESUME	☐ DATA1
☐ EOP	☐ ACK
☐ INVALID PKT	☐ NAK
☑ SOF	☐ STALL
☐ SETUP	☐ PRE

Frame
Start count
Stop count
Frm#

Ready Frm count 138 Frm# 0x000 Evnt# 3012 Evnt byte# 0

Details Window

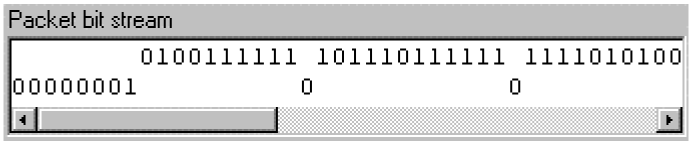


PID = 0x4b, DATA PAYLOAD = 18, CRC16 = 0xb0e0.
Begins at acq#: 3462. Ends at acq#: 3610.

This is a text box displaying details on the event selected in Traffic window. Event details depend on the event type:

- SIGNAL ERR: error code, duration, the number of the first event acquisition, the number of the last event acquisition, error description
- IDLE: duration, the number of the first event acquisition, the number of the last event acquisition. If the USB Process had Record Idle option OFF, the duration of IDLE event is not relevant being indicated by >= (the capture device truncates the duration of idle times to 22 FS bit times).
- RESET: duration, the number of the first event acquisition, the number of the last event acquisition.
- EOP: duration, the number of the first event acquisition, the number of the last event acquisition.
- RESUME: duration, the number of the first event acquisition, the number of the last event acquisition .
- INVALID PKT: error code, the number of the first event acquisition, the number of the last event acquisition, error description
- SOF: PID, frame number, CRC5, the number of the first event acquisition, the number of the last event acquisition. If frame analysis has been performed within the USB Process, then frames with invalid timing are signaled by using SOF INV!. In such a case the Details window presents the description of the frame timing failure.
- SETUP: PID, address, endpoint, CRC5, the number of the first event acquisition, the number of the last event acquisition
- IN: PID, address, endpoint, CRC5, the number of the first event acquisition, the number of the last event acquisition
- OUT: PID, address, endpoint, CRC5, the number of the first event acquisition, the number of the last event acquisition
- DATA0: PID, data payload, CRC16, the number of the first event acquisition, the number of the last event acquisition
- DATA1: PID, data payload, CRC16, the number of the first event acquisition, the number of the last event acquisition
- ACK: PID, the number of the first event acquisition, the number of the last event acquisition
- NAK: PID, the number of the first event acquisition, the number of the last event acquisition
- STALL: PID, the number of the first event acquisition, the number of the last event acquisition
- PRE: PID, the number of the first event acquisition, the number of the last event acquisition

Bit Stream Window



```
         0100111111 101110111111 1111010100
00000001           0            0
```

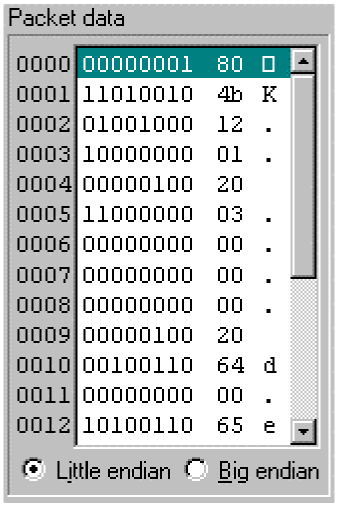
This window presents the packet bit stream, when the event cursor selects a invalid packet which has not been decoded.

Sync bits and stuffed bits are presented on the lower row of that window, while the data bits are presented on the higher row.

If the packet is invalid because has a sync error or a bit stuff error, the bit stream decoding stops at the place where the error is detected.

If the currently selected event in Traffic window is a decoded packet (that means a valid packet or a packet presenting a CRC error), the Bit Stream window stays empty.

Packet Data Window



```
0000 00000001  80  □
0001 11010010  4b  K
0002 01001000  12  .
0003 10000000  01  .
0004 00000100  20
0005 11000000  03  .
0006 00000000  00  .
0007 00000000  00  .
0008 00000000  00  .
0009 00000100  20
0010 00100110  64  d
0011 00000000  00  .
0012 10100110  65  e
```

● Little endian ○ Big endian

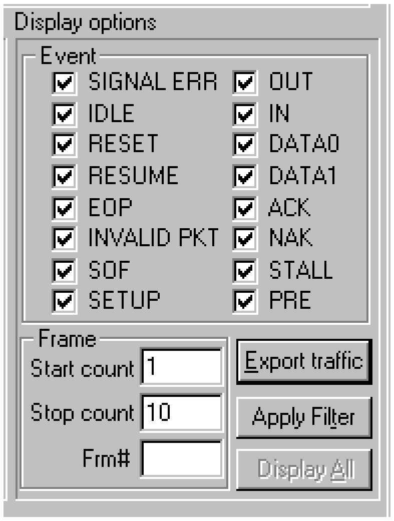
This window presents the body of a decoded packet, i.e. a packet having correct sync and stuffed bits. Sync, PID, and CRC are included. The packet body indicates the CRC, regardless if CRC is correct or not.

The packet body is represented in binary, hex, and ASCII. The binary representation may use little or big endian order, if Little endian, respectively Big endian radio button is pressed.

The packet data window presents a byte cursor. If the packet is decoded, the user may select any byte. The number of that byte will be indicated in Evnt byte# field of Status Bar. When the first byte is selected (i.e. sync byte), that field displays zero.

If the packet is not decoded as result of an error detected in sync sequence or in bit stuffing, then packet data window stays empty, and the bit stream window shows the packet bit stream up to the point where the error has been detected.

Display Options



Display options

Event

☑ SIGNAL ERR ☑ OUT
☑ IDLE ☑ IN
☑ RESET ☑ DATA0
☑ RESUME ☑ DATA1
☑ EOP ☑ ACK
☑ INVALID PKT ☑ NAK
☑ SOF ☑ STALL
☑ SETUP ☑ PRE

Frame

Start count: 1
Stop count: 10
Frm#:

Display options allow the user to specify the events to be displayed in Traffic window. The following controls are available for display options:

- Event group
- Frame group
- Display All button
- Apply Filter button
- Export Traffic button

Event group allows the user to specify the events to be displayed in the filtered traffic. Each event has assigned a check box . Event selection options are ORed. For example if EOP and IDLE check boxes are on, then EOP and IDLE events will be displayed.

Frame group allows the user to specify the frame range for the display of filtered traffic. It presents the following edit controls:

- Start, for specifying the count of the frame to start with. An empty control means that the display will start from the beginning of the traffic. The first SOF token corresponds to a count of 1.
- Stop, for specifying the count of the frame to stop after. An empty control means that the display will stop at the end of the traffic.
- Frm#, to indicate that the program will display traffic of frames having this frame number. An empty control means that the program will display the traffic of all frames between those specified by Start and Stop controls. Valid range for frame number is: 0x000..0x7ff.

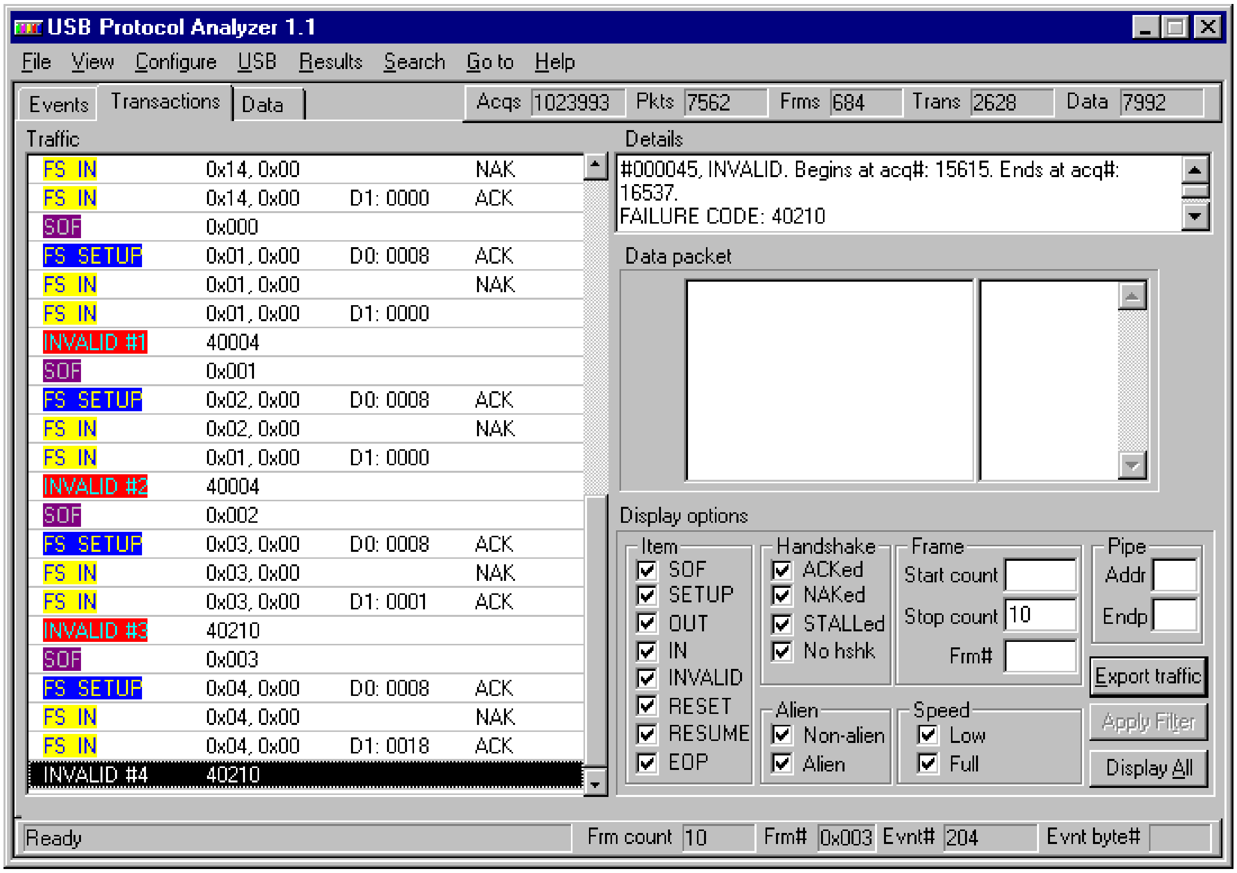
These options are ANDed between them, and ANDed with event selection options and are applicable for the traffic captured on FS bus only.

Display options have available two buttons: Display All, and Apply Filter. When the first button is pressed, the event traffic window will display all events. When Apply Filter button is pressed, the event traffic window will display events selected according to display options. If the current event is enabled by display filter, the traffic focus is preserved after pressing Apply Filter. Otherwise the event cursor will be set on the closest event enabled by display filter.

Export Traffic button allows the user to save the filtered traffic in a user defined text file. The traffic format in that file is similar to the traffic displayed in Traffic window. Up to 1000 traffic items may be exported. This command allows the user to save the filtered traffic in a text file. That file may be loaded, viewed and printed with a text utility (as NotePad for example).

Viewing Transaction Traffic

Transaction Layer



Acqs 1023993 Pkts 7562 Frms 684 Trans 2628 Data 7992

FS IN	0x14, 0x00		NAK
FS IN	0x14, 0x00	D1: 0000	ACK
SOF	0x000		
FS SETUP	0x01, 0x00	D0: 0008	ACK
FS IN	0x01, 0x00		NAK
FS IN	0x01, 0x00	D1: 0000	
INVALID #1	40004		
SOF	0x001		
FS SETUP	0x02, 0x00	D0: 0008	ACK
FS IN	0x02, 0x00		NAK
FS IN	0x01, 0x00	D1: 0000	
INVALID #2	40004		
SOF	0x002		
FS SETUP	0x03, 0x00	D0: 0008	ACK
FS IN	0x03, 0x00		NAK
FS IN	0x03, 0x00	D1: 0001	ACK
INVALID #3	40210		
SOF	0x003		
FS SETUP	0x04, 0x00	D0: 0008	ACK
FS IN	0x04, 0x00		NAK
FS IN	0x04, 0x00	D1: 0018	ACK
INVALID #4	40210		

#000045, INVALID. Begins at acq#: 15615. Ends at acq#: 16537.
FAILURE CODE: 40210

Item: ☑ SOF ☑ SETUP ☑ OUT ☑ IN ☑ INVALID ☑ RESET ☑ RESUME ☑ EOP
Handshake: ☑ ACKed ☑ NAKed ☑ STALLed ☑ No hshk
Frame: Start count, Stop count 10, Frm#
Pipe: Addr, Endp
Alien: ☑ Non-alien ☑ Alien
Speed: ☑ Low ☑ Full

Ready Frm count 10 Frm# 0x003 Evnt# 204 Evnt byte#

The Transaction Layer is accessed by clicking the tab of its folder, or by pressing F3 key. This layer presents the USB traffic in terms of transaction items. It contains the following controls:

- the layer tab which may be clicked to switch on this layer
- the Traffic window
- the Details window
- the Data Packet window
- the Display Options group

Also the Traffic Information bar and the Status Bar are available as on any other traffic layer.
The transaction traffic presents the list of transaction items resulted from Transaction Analysis. The following transaction items may be shown:

- SOF
- SETUP
- OUT
- IN
- RESET
- EOP
- RESUME
- INVALID

SOF is the start of frame token. It is not a transaction, but it is important to present the frame markers in the traffic. If frame analysis has been performed within the USB Process , then frames with invalid timing are signaled by using SOF INV!.

SETUP is the SETUP transaction.
OUT is the OUT transaction.
IN is the IN transaction.

RESET event is defined as the SE0 state for at least 10ms.

RESUME event is defined as K state for at least 20ms, followed by LS EOP (low speed end of packet).

EOP event is defined as an end of packet signaling which does not follow a packet transfer. Such EOPs may be seen on a low speed bus (provided by the upstream hub).

INVALID is an invalid transaction. (refer to

Transaction Errors).

RESET, RESUME, EOP are not transactions, but may affect the transaction flow, and for this reason the display of these traffic items is allowed in the Traffic window of Transaction Layer.

For each transaction item which has been detected, the Traffic window presents a transaction prompt.

Details window provides details on the current transaction item. Those details depend on the transaction item type.

Data Packet window presents the body of the data packet (sync, PID, and CRC16 included), of a valid transaction (if applicable). If the transaction is not valid, or it does not contain a data packet, this window stays empty. If the user wants to see the event traffic around an invalid transaction, it may switch on Event Layer. For example if the transaction is given invalid because its data packet is not valid, the invalid packet may be seen on the Event Layer. Bytes of the data packet are displayed both in hex and ASCII.

Display options allow the user to specify the traffic items to be displayed in Traffic window.

Item group allows the user to specify the transaction items to be displayed in filtered traffic. Transaction items mean not only transactions (SETUP, OUT, IN, INVALID), but SOF tokens, RESET, RESUME, and standalone EOP whose display in Traffic window may be desired. Item selection options are ORed. For example if SOF and INVALID check boxes are on, then SOF and INVALID items will be displayed.

Handshake group allows the user to specify the type of the handshake packet for OUT or IN transactions.

Alien group allows the user to specify the alien attribute for SETUP, OUT or IN transactions. (refer to Alien Transactions). This is applicable for traffic captured on non-root bus only.

Speed group allows the user to specify the speed for SETUP, OUT or IN transactions, as well as for EOPs. This is applicable for traffic captured on FS bus only.

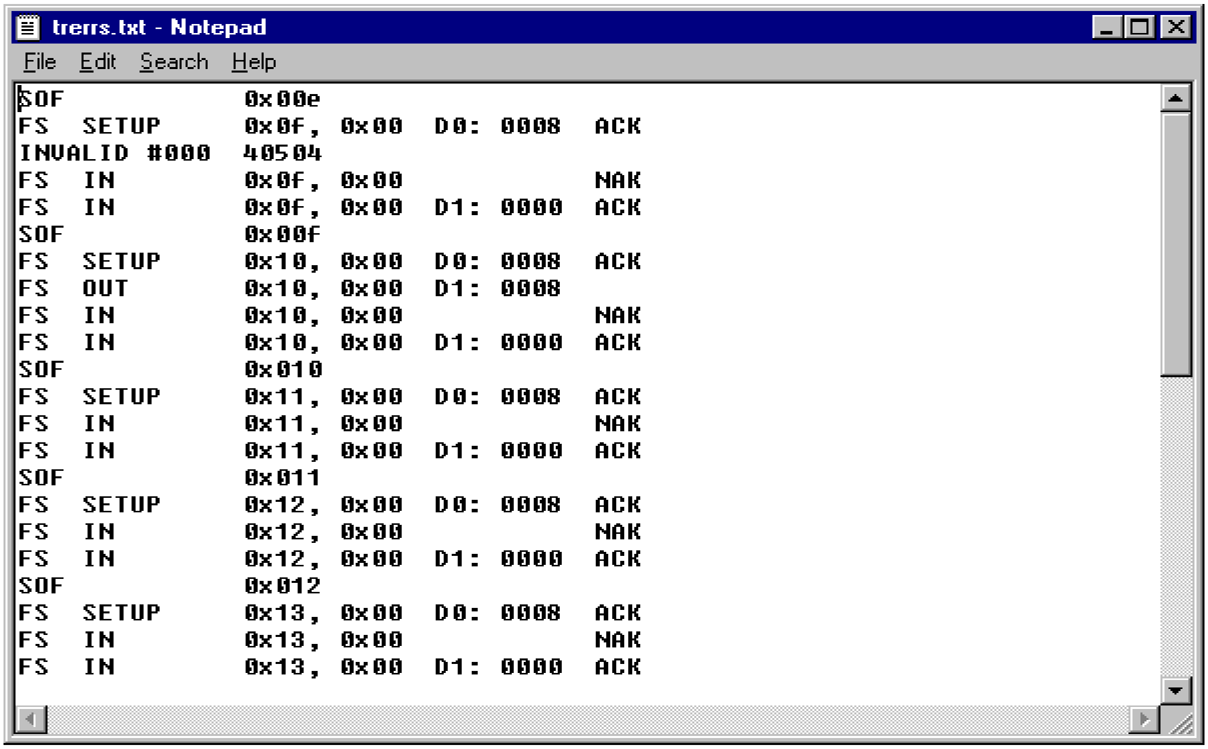
Pipe group allows the user to specify the pipe address and endpoint for SETUP, OUT or IN transactions. The pipe is specified in Addr and Endp edit controls. The valid range for pipe address is: 0x00..0x7f. The valid range for the pipe endpoint is: x00..0x0f. An empty control is a wild card for that parameter. For example and empty Endp edit control will not restrict the display to a specific endpoint.

Frame group allows the user to specify the frame range for the display operation.

Options of all groups are ANDed between them.

Display options have available two buttons: Display All, and Apply Filter. When the first button is pressed, the traffic will display all transaction items. When Apply Filter button is pressed, the traffic will display items selected according to display options, i.e. filtered traffic. If the current item is enabled by display filter, the traffic focus is preserved after pressing Apply Filter. Otherwise the traffic cursor will be set on the closest item enabled by display filter.

Export Traffic button allows the user to save the filtered traffic in a user defined text file. The traffic format in that file is similar to the traffic displayed in Traffic window:



```
SOF            0x00e
FS   SETUP     0x0f, 0x00   D0: 0008   ACK
INVALID #000   40504
FS   IN        0x0f, 0x00              NAK
FS   IN        0x0f, 0x00   D1: 0000   ACK
SOF            0x00f
FS   SETUP     0x10, 0x00   D0: 0008   ACK
FS   OUT       0x10, 0x00   D1: 0008
FS   IN        0x10, 0x00              NAK
FS   IN        0x10, 0x00   D1: 0000   ACK
SOF            0x010
FS   SETUP     0x11, 0x00   D0: 0008   ACK
FS   IN        0x11, 0x00              NAK
FS   IN        0x11, 0x00   D1: 0000   ACK
SOF            0x011
FS   SETUP     0x12, 0x00   D0: 0008   ACK
FS   IN        0x12, 0x00              NAK
FS   IN        0x12, 0x00   D1: 0000   ACK
SOF            0x012
FS   SETUP     0x13, 0x00   D0: 0008   ACK
FS   IN        0x13, 0x00              NAK
FS   IN        0x13, 0x00   D1: 0000   ACK
```

Up to 1000 traffic items may be exported. This command allows the user to save the filtered traffic in a text file. That file may be loaded, viewed and printed with a text utility (as NotePad for example).

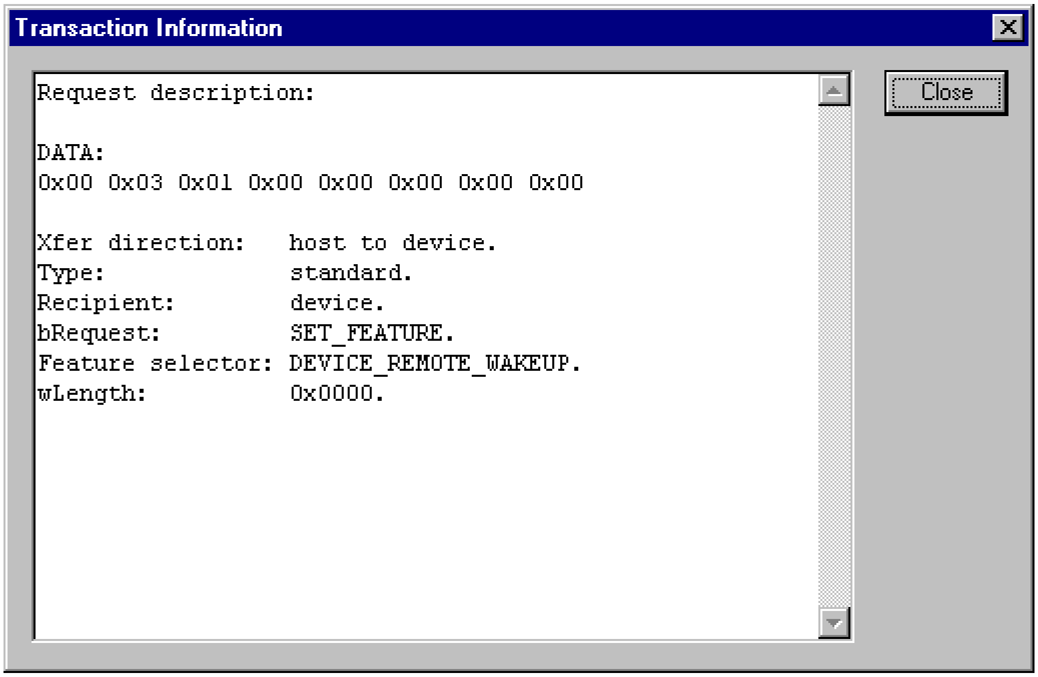
Decoding Standard Requests

Besides the information shown in the Traffic window or in Details window, some additional information may be available for some transaction items. This version of the program provides additional information for SETUP transactions which perform standard requests.

Decoding a standard request is available on Transaction Layer and may be activated in one of the following ways:

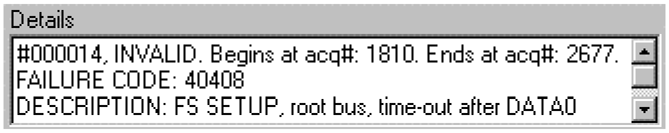
- by clicking with the right mouse button the SETUP transaction
- by selecting the SETUP transaction and pressing SPACE bar

At that moment the program opens Transaction information dialog:



```
Request description:

DATA:
0x00 0x03 0x01 0x00 0x00 0x00 0x00 0x00

Xfer direction:   host to device.
Type:             standard.
Recipient:        device.
bRequest:         SET_FEATURE.
Feature selector: DEVICE_REMOTE_WAKEUP.
wLength:          0x0000.
```

Details Window

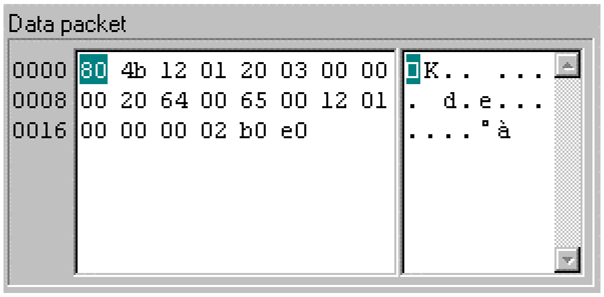


```
#000014, INVALID. Begins at acq#: 1810. Ends at acq#: 2677.
FAILURE CODE: 40408
DESCRIPTION: FS SETUP, root bus, time-out after DATA0
```

This window provides details on the current transaction item. Those details depend on the transaction item type:

- SOF: transaction item#, name, frame#, the number of the acquisition the transaction item starts with, the number of the acquisition the transaction item ends with. If frame analysis has been performed within the USB Process, then frames with invalid timing are signaled by using SOF INV!. In such a case the Details window presents the description of the frame timing failure.
- SETUP, OUT, IN: transaction item#, speed, alien attribute (refer to Alien Transactions); the number of the acquisition the transaction item starts with, the number of the acquisition the transaction item ends with; name, details on token: address, endpoint; idle time after token; details on data packet (if applicable): type, data payload; idle time after data packet (if applicable); handshake packet: (if applicable).
- INVAL: transaction item#, error code, name; the number of the acquisition the transaction item starts with, the number of the acquisition the transaction item ends with; error code, error description
- RESET: duration, the number of the acquisition the transaction item starts with, the number of the acquisition the transaction item ends with
- EOP: duration, the number of the acquisition the transaction item starts with, the number of the acquisition the transaction item ends with
- RESUME: duration, the number of the acquisition the transaction item starts with, the number of the acquisition the transaction item ends with

Data Packet Window

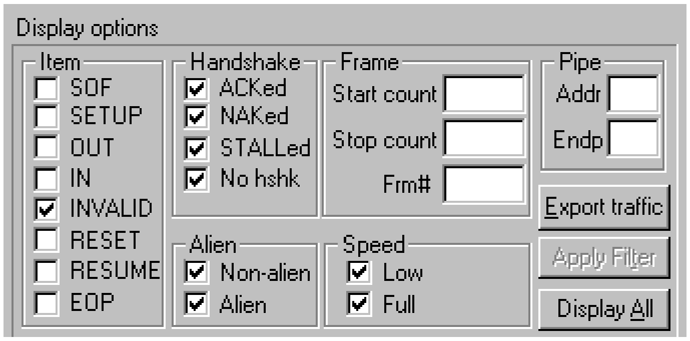


```
0000 80 4b 12 01 20 03 00 00  □K..  ...
0008 00 20 64 00 65 00 12 01  .  d.e...
0016 00 00 00 02 b0 e0        ....°à
```

This window presents the body of the data packet (sync, PID, and CRC16 included), of a valid transaction (if applicable). If the transaction is not valid, or it does not contain a data packet, this window stays empty. If the user wants to see the event traffic around an invalid transaction, it may switch on Event Layer. For example if the transaction is given invalid because its data packet is not valid, the invalid packet may be seen on the Event Layer.

Bytes of the data packet are displayed both in hex and ASCII.

Display Options



Item
☐ SOF
☐ SETUP
☐ OUT
☐ IN
☑ INVALID
☐ RESET
☐ RESUME
☐ EOP

Handshake
☑ ACKed
☑ NAKed
☑ STALLed
☑ No hshk

Frame
Start count
Stop count
Frm#

Pipe
Addr
Endp

Alien
☑ Non-alien
☑ Alien

Speed
☑ Low
☑ Full

Display options allow the user to specify the traffic items to be displayed in Traffic window. The following controls are available for these options:

- Item group
- Handshake group
- Alien group
- Speed group
- Pipe group
- Frame group
- Apply Filter button
- Display All button
- Export Traffic button

Item group allows the user to specify the transaction items to be displayed in filtered traffic. Transaction items mean not only transactions (SETUP, OUT, IN, INVALID), but SOF tokens, RESET, RESUME, and standalone EOP whose display in Traffic window may be desired. Item selection options are ORed. For example if SOF and INVALID check boxes are on, then SOF and INVALID items will be displayed.

Handshake group allows the user to specify the type of the handshake packet for OUT or IN transactions.

Alien group allows the user to specify the alien attribute for SETUP, OUT or IN transactions. (refer to Alien Transactions). This is applicable for traffic captured on non-root bus only.

Speed group allows the user to specify the speed when for SETUP, OUT or IN transactions, as well as for EOPs. This is applicable for traffic captured on FS bus only.

Pipe group allows the user to specify the pipe address and endpoint for SETUP, OUT or IN transactions. The pipe is specified in Addr and Endp edit controls. The valid range for pipe address is: 0x00..0x7f. The valid range for the pipe endpoint is: x00..0x0f. An empty control is a wild card for that parameter. For example and empty Endp edit control will not restrict the display to a specific endpoint.

Frame group allows the user to specify the frame range for the display operation. It presents the following edit controls:

- Start, for specifying the count of the frame to start with. An empty control means that the display will start from the beginning of the traffic. The first SOF token corresponds to a count of 1.

- **Stop**, for specifying the count of the frame to stop after. An empty control means that the display will stop at the end of the traffic.
- **Frm#**, to indicate that the program will display traffic of frames having this frame number. An empty control means that the program will display traffic in all frames between those specified by **Start** and **Stop** controls. Valid range for frame number is: 0x000..0x7ff.

Frame options are ANDed between them, and ANDed with the other selection options and are applicable for the traffic captured on FS bus only.

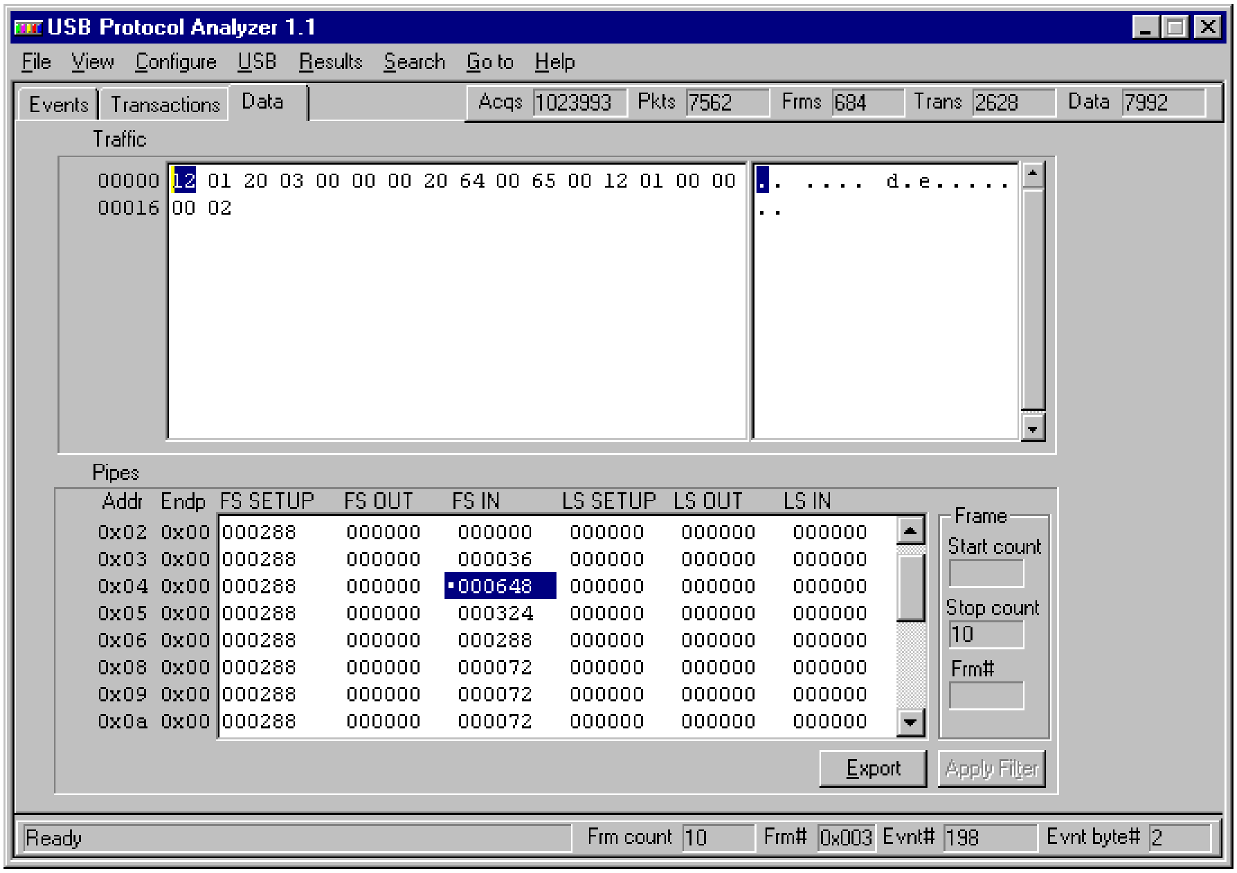
Options of all groups are ANDed between them.

Display options have available two buttons: **Display All**, and **Apply Filter**. When the first button is pressed, the traffic will display all transaction items. When **Apply Filter** button is pressed, the traffic will display items selected according to display options, i.e. filtered traffic. If the current item is enabled by display filter, the traffic focus is preserved after pressing **Apply Filter**. Otherwise the traffic cursor will be set on the closest item enabled by display filter.

Export Traffic button allows the user to save the filtered traffic in a user defined text file. The traffic format in that file is similar to the traffic displayed in Traffic window. Up to 1000 traffic items may be exported. This command allows the user to save the filtered traffic in a text file. That file may be loaded, viewed and printed with a text utility (as NotePad for example).

Viewing Data Traffic

Data Layer



Acqs 1023993 Pkts 7562 Frms 684 Trans 2628 Data 7992

```
00000 12 01 20 03 00 00 00 20 64 00 65 00 12 01 00 00   ..  ....  d.e.....
00016 00 02                                              ..
```

Addr	Endp	FS SETUP	FS OUT	FS IN	LS SETUP	LS OUT	LS IN
0x02	0x00	000288	000000	000000	000000	000000	000000
0x03	0x00	000288	000000	000036	000000	000000	000000
0x04	0x00	000288	000000	000648	000000	000000	000000
0x05	0x00	000288	000000	000324	000000	000000	000000
0x06	0x00	000288	000000	000288	000000	000000	000000
0x08	0x00	000288	000000	000072	000000	000000	000000
0x09	0x00	000288	000000	000072	000000	000000	000000
0x0a	0x00	000288	000000	000072	000000	000000	000000

Start count
Stop count 10
Frm#

Ready Frm count 10 Frm# 0x003 Evnt# 198 Evnt byte# 2

The Data Layer is accessed by clicking the tab of its folder, or by pressing F4 key. This layer presents the data traffic over an user specified pipe and transaction type. That data has been transferred in non-alien transactions which have not been NAKed or STALLed. The sync, PID and CRC bytes are not displayed. Data Layer contains the following controls:

- the layer tab which may be clicked to switch on this layer
- the Traffic window
- Display options group

Also the Traffic Information bar and the Status bar are available as on any other traffic layer.

If the transaction is alien (refer to Alien Transactions), it means that the pipe does not go through the bus branch where the USB Probe is installed. If the transaction has been NAKed or STALLed it means the data did no go through, therefore should not be presented as being transferred.

Display options allow the user to specify the pipe and transaction type for which data traffic must be displayed within the frame range indicated on the screen.

Pipes table presents the number of data bytes transferred in transactions occurred over each pipe which has been used in the traffic that was captured and analyzed. The pipe is specified by address and endpoint. A cell in this table corresponds to a specific pipe and to one of the non-alien transaction types mentioned below, which were not NAKed or STALLed:

- FS SETUP
- FS OUT
- FS IN
- LS SETUP
- LS OUT
- LS IN

A pipe is mentioned in the table only if it transferred data at least in one transaction type. The cell corresponding to that transaction type will show non-zero bytes. Transaction types of that pipe which did not transfer data will show zero bytes.

If a pipe did not transfer data in any of transaction types, that pipe is not mentioned in the table.

The cell whose data is presented in the Traffic window and is marked with a '*'.

Frame group presents read only controls as set on the previous traffic layer.

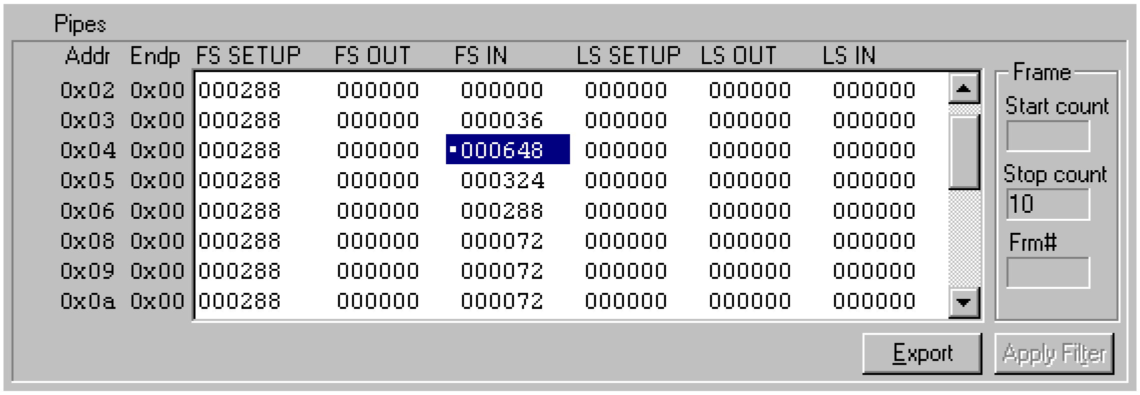
Apply Filter button allows the user to switch on another pipe and transaction type (in fact on another cell of **Pipes** table), and to present the data for that new option. This may be achieved in any of the following ways:

- double click a cell in **Pipes** table
- select a cell in **Pipes** table and press Apply Filter button

If the new cell did not provide any data transfer (i.e. displays zero bytes), the program does not update the content of Traffic window.

Export button allows the user to save in an user defined binary file the data presented in Traffic window.

Display Options



Pipes

Addr	Endp	FS SETUP	FS OUT	FS IN	LS SETUP	LS OUT	LS IN
0x02	0x00	000288	000000	000000	000000	000000	000000
0x03	0x00	000288	000000	000036	000000	000000	000000
0x04	0x00	000288	000000	▪000648	000000	000000	000000
0x05	0x00	000288	000000	000324	000000	000000	000000
0x06	0x00	000288	000000	000288	000000	000000	000000
0x08	0x00	000288	000000	000072	000000	000000	000000
0x09	0x00	000288	000000	000072	000000	000000	000000
0x0a	0x00	000288	000000	000072	000000	000000	000000

Frame
Start count
Stop count: 10
Frm#

Display options presents the following controls:

- **Pipes** table
- **Frame** group
- **Apply Filter** button

Pipes table presents the number of bytes transferred on each transaction type occurred over each pipe which has been used in the traffic that was captured and analyzed. The pipe is specified by address and endpoint. A cell in this table corresponds to a specific pipe and to one of the non-alien transaction types mentioned below, which was not NAKed, or STALLed:

- FS SETUP
- FS OUT
- FS IN
- LS SETUP
- LS OUT
- LS IN

A pipe is mentioned in the table only if it transferred data at least in one transaction type. The cell corresponding to that transaction type will show non-zero bytes. Transaction types of that pipe which did not transfer data will show zero bytes.

If a pipe did not transfer data in any of transaction types, that pipe is not mentioned in the table.

The data is presented for the currently selected cell which is highlighted and is marked with a '*'.

Normally there should be only one transaction type over a specified pipe (if not bi-directional). However, if the captured traffic contains RESET events, it will be possible to see that the same pipe has been assigned for different period of times to different transaction types.

Frame group presents read only controls as set on the Transaction Layer.

Apply Filter button allows the user to switch on another pipe and transaction type (in fact on another cell of **Pipes** table), and to present the data for that new option. This may be achieved in any of the following ways:

- double click a cell in **Pipes** table
- select a cell in **Pipes** table and press Apply Filter button

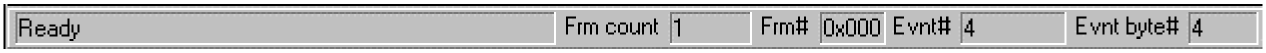
If the new cell did not provide any data transfer (i.e. displays zero bytes), the program does not update the content of Traffic window .

Switching between Traffic Layers

Traffic Focus

When switching between filtered and unfiltered traffic, or when switching between traffic layers, it is essential to preserve the traffic focus. That means the currently selected traffic item indicates the same point in the traffic.

The traffic focus is indicated on the Status bar:



Ready | Frm count 1 | Frm# 0x000 | Evnt# 4 | Evnt byte# 4

Frm count indicates the count of the frame containing the current traffic item. The first frame has a count of 1. If the traffic has been captured on a low speed bus, or it is not preceded by any SOF, that control stays empty.

Frm# indicates the number of the frame containing the current traffic item. If the traffic has been captured on a low speed bus, or it is not preceded by any SOF, that control stays empty.

Evnt# indicates the number of the event the traffic focus is selecting. On Event Layer this control indicates the number of the selected event. On Transaction Layer this control indicates an event depending on the type of the selected transaction item (refer to Traffic Focus on Transaction Layer). On Data Layer the control indicates the data packet of the transaction which provided the byte selected in the Traffic window.

Evnt byte# indicates the number of the byte transferred in the event indicated by Evnt# control. If no data bytes have been transferred in that event, this control stays empty.

The traffic focus information helps the user to check that it stays in the same place of the traffic when switching between filtered and unfiltered traffic, or switching between traffic layers.

When switching between filtered and unfiltered traffic, the traffic focus does not change (i.e. the fields mentioned above preserve their contents). When switching from a higher to a lower layer, the traffic focus does not change as well. When switching from a lower to a higher layer the traffic focus may slightly change.

Switching from Events to Transactions

Switching from events to transactions may be performed in any of the following ways:

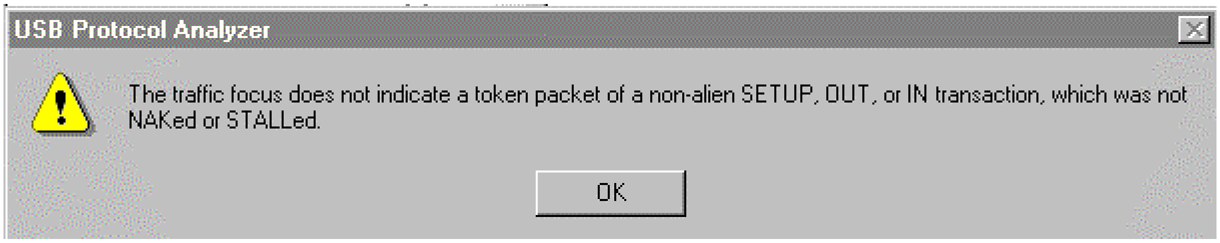
- click the tab of Transaction Layer
- press `F3`
- press `CTRL+TAB`

At that moment the screen will present Transaction Layer. The traffic focus is preserved if the currently selected event was a data packet. Otherwise the traffic focus is slightly changed in order to indicate the data packet of the currently selected transaction.

Note that when entering the Transaction Layer, the program presents unfiltered traffic.

Switching from Events to Data

Switching from events to data is possible only if the currently selected event in Traffic window is part of a SETUP, OUT, or IN non-alien transaction which was not NAKed or STALLed. Otherwise the program displays the message presented below:



The traffic focus does not indicate a token packet of a non-alien SETUP, OUT, or IN transaction, which was not NAKed or STALLed.

The reason for this restriction is the program needs to know the pipe whose data traffic must be presented. If the transaction is alien (refer to Alien Transactions), it means that the pipe does not go through the bus branch where the USB Probe is installed. If the transaction has been NAKed or STALLed it means the data did no go through, therefore should not be presented as being transferred.

Switching from events to data may be performed in any of the following ways:

- click the tab of Data Layer
- press `F4`
- press `CTRL+SHIFT+TAB`

Switching from Transactions to Events

Switching from transactions to events may be performed in any of the following ways:

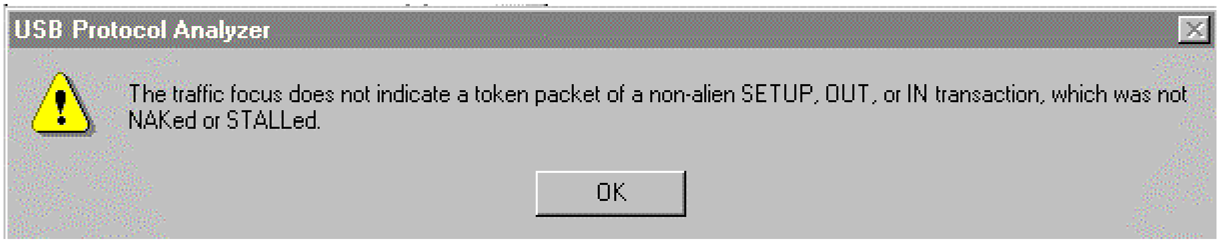
- click the tab of Event Layer
- press `F2`
- press `CTRL+SHIFT+TAB`

At that moment the screen will present Event Layer. The traffic focus is preserved (i.e. the information presented on Status bar does not change).

Note that when entering the Event Layer, the program presents unfiltered traffic.

Switching from Transactions to Data

Switching from transactions to data is possible only if the currently selected item in Traffic window is a SETUP, OUT, or IN transaction, non-alien, which was not NAKed or STALLed. Otherwise the program displays the message presented below:



The traffic focus does not indicate a token packet of a non-alien SETUP, OUT, or IN transaction, which was not NAKed or STALLed.

The reason for this restriction is the program needs to know the pipe whose data traffic must be presented. If the transaction is alien (refer to Alien Transactions), it means that the pipe does not go through the bus branch where the USB Probe is installed. If the transaction has been NAKed or STALLed it means the data did no go through, therefore should not be presented as being transferred.

Switching from transactions to data may be performed in any of the following ways:
- click the tab of Data Layer
- press `F4`
- press `CTRL+TAB`

Switching from Data to Events

Switching from data to events may be performed in any of the following ways:
- click the tab of Event Layer
- press `F2`
- press `CTRL+TAB`

At that moment the screen will present Event Layer. The traffic focus is preserved (i.e. the information presented on Status bar does not change).

Note that when entering the Event Layer, the program presents unfiltered traffic.

Switching from Data to Transactions

Switching from data to transactions may be performed in any of the following ways:
- click the tab of Transaction Layer
- press `F3`
- press `CTRL+SHIFT+TAB`

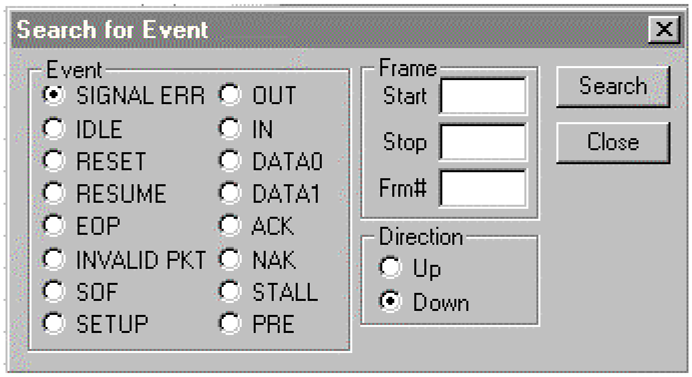
At that moment the screen will present Transaction Layer. The traffic focus is preserved (i.e. the information presented on Status bar does not change).

Note that when entering the Transaction Layer, the program presents unfiltered traffic.

Searching in USB Traffic

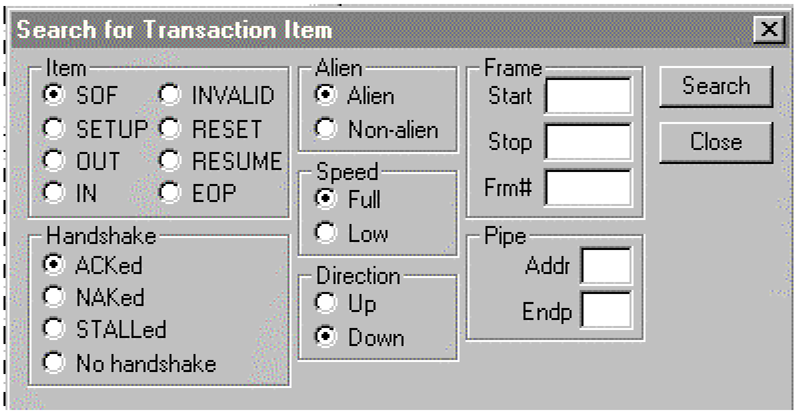
Search for Events

This command is available in Search drop menu on Event Layer. When activated, the program opens Search Event dialog:



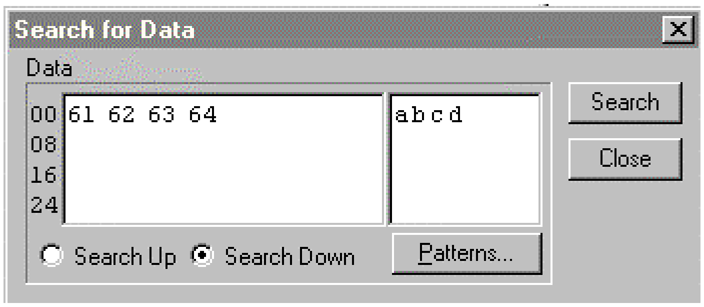
Search for Transactions

This command is available in Search drop menu on Transaction Layer. When activated, the program opens Search Transaction dialog:



Search for Data

This command is available in Search drop menu on Data Layer. When activated, the program opens Search Data dialog:

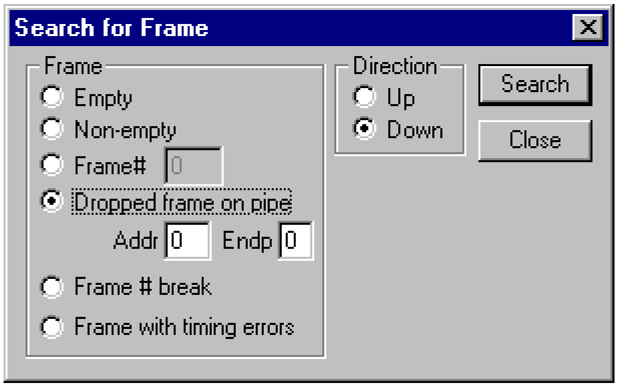


00 61 62 63 64 abcd
08
16
24

○ Search Up ● Search Down

Search for Frames

This command is available in Search drop menu on Transaction Layer. When activated, the program opens Search Frame dialog:



○ Empty
○ Non-empty
○ Frame# 0
● Dropped frame on pipe
Addr 0 Endp 0
○ Frame # break
○ Frame with timing errors

○ Up
● Down

Goto Commands

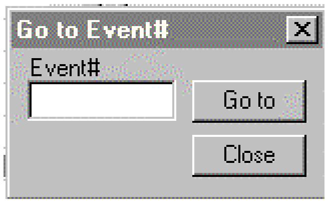
Goto Trigger

This command is available in Go to drop menu and it is enabled on Event Layer only. When activated, the program sets the event cursor in Traffic window on the event where the trigger occurred.

Note that after the execution of a go to command, the program displays unfiltered traffic.

Goto Event

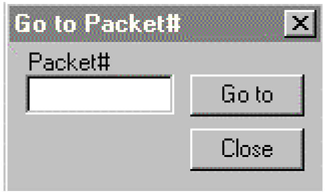
This command is available in Go to drop menu and it is enabled on Event Layer only. When activated, the program opens Goto Event dialog:



This command may be used to get to the events mentioned in Event Analysis report.
Note that after the execution of a go to command, the program displays unfiltered traffic.

Goto Packet

This command is available in Go to drop menu and it is enabled on Event Layer only. When activated, the program opens Goto Packet dialog:



This command may be used to get to the events mentioned in Packet Analysis report.
Note that after the execution of a go to command, the program displays unfiltered traffic.

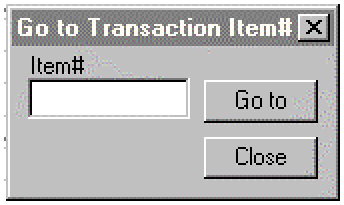
Goto Reference

This command is available in Go to drop menu and it is enabled on Event Layer only. When activated, the program sets the event cursor in Traffic window on the event where the event reference has been set (refer to Event Time Information for setting an event reference).

Note that after the execution of a go to command, the program displays unfiltered traffic.

Goto Transaction Item

This command is available in Go to drop menu and it is enabled on Transaction Layer only. When activated, the program opens Goto Transaction Item dialog:

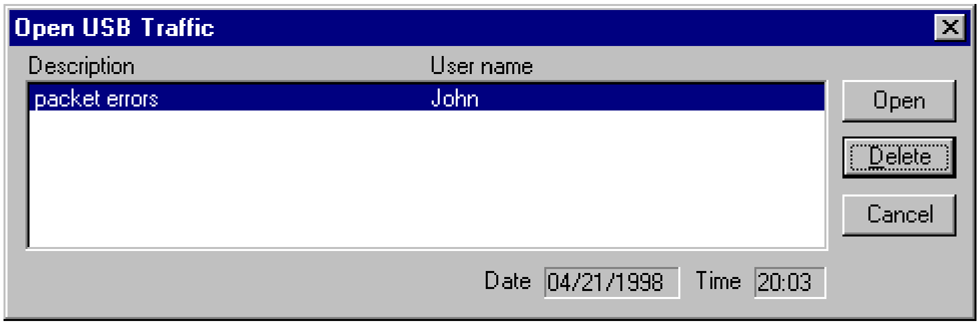


This command may be used to get to the events mentioned in Transaction Analysis report or Frame Analysis Report. Note that after the execution of a go to command, the program displays unfiltered traffic.

File Commands

Open Traffic File

This command is available in File drop menu. When activated, the program opens Open USB Traffic dialog:



Description: packet errors
User name: John
Date 04/21/1998
Time 20:03

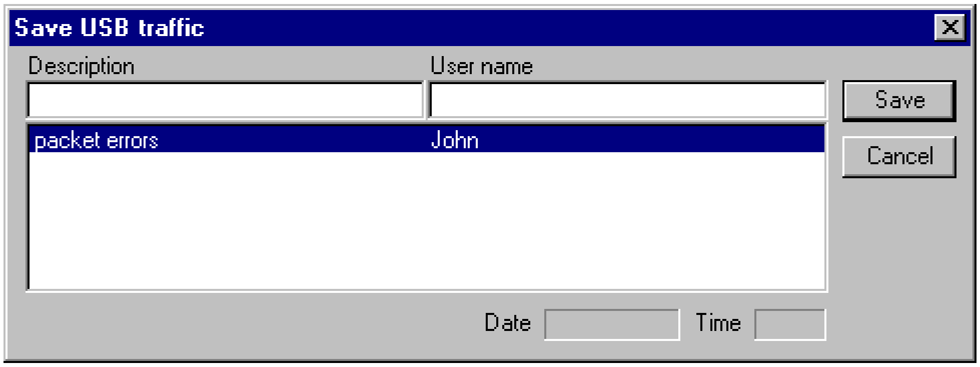
The user may load or delete a traffic file which was previously saved.

Close

This command is available in File drop menu. When activated, the program asks if the current traffic should be saved (if not already). After the execution of this command, all traffic folders are closed.

Save

This command is available in File drop menu. When activated, the program opens Save USB Traffic dialog:



Description: packet errors
User name: John

This dialog allows the user to save the traffic in compressed format. Traffic files are held in a data base operated by open and save commands.

Export USB

This command is available in File drop menu. When activated, the program opens a file selection dialog to allow the user to save the traffic in a user defined file having the extension ".usb". Such a file may be loaded by using Import USB command from File drop menu.

Traffic files having user defined names may be used to share between multiple users the information created by the protocol analyzer (note that Open and Save commands operate on a data base).

Export Capture

This command is available in File drop menu. When activated, the program opens a file selection dialog to allow the user to save the capture file in a user defined file having the extension ".cpt". Such a file may be loaded by using Import Capture command from File drop menu.

The capture file contains the capture options and the capture information received from the capture device. Such a file may be used to help technical support (the information stored in a capture file is not submitted to the USB analysis).

Import USB

This command is available in File drop menu. When activated, the program opens a file selection dialog to allow the user to load the traffic from a file having the extension ".usb". Such a file is supposed to be created by using Export USB command from File drop menu (note that Open and Save commands operate on a data base).

Traffic files having user defined names may be used to share between multiple users the information created by the protocol analyzer (note that Open and Save commands operate on a data base).

Import Capture

This command is available in File drop menu. When activated, the program opens a file selection dialog to allow the user to load a capture file having the extension ".cpt". Such a file is supposed to be created by using Export Capture command from File drop menu.

The capture file contains the capture options and the capture information received from capture device . Such a file may be used to help technical support (the information stored in a capture file is not submitted to the USB analysis).

After the capture is imported, the program opens Resume USB Process dialog (refer to Resume USB).

Print Setup

This command is available in File drop menu. When activated, the program opens Print Setup dialog to allow the user to specify print settings.

Print

This command is available in File drop menu. When activated, the program opens a Print dialog to allow the user to print the screen of the current traffic layer.

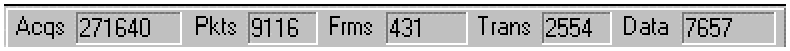
The user export a part of the traffic shown on Event Layer or on Transaction Layer, by using Export Traffic button. Up to 1000 traffic items may be exported. This command allows the user to save the filtered traffic in a text file (by using the same traffic item prompts as in traffic windows). That file may be loaded, viewed and printed with a text utility (as NotePad for example).

Exit

This command is available in File drop menu. When activated, the program asks if the current traffic should be saved (if not already). Upon the execution of this command the USB Protocol Analyzer application is closed.

User's Reference

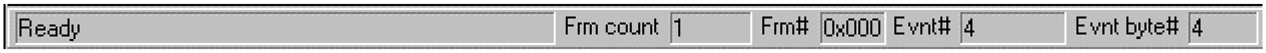
Traffic Information Bar


Acqs 271640
Pkts 9116
Frms 431
Trans 2554
Data 7657

This bar indicates the traffic summary resulted from the last ISB Process. It contains the following read only controls:

- Acqs which indicates total of acquisitions of the captured traffic
- Pkts which indicates the total of packets found in the traffic
- Frms which indicates the total of SOF tokens found in the traffic
- Trans which indicates the total of transactions (SETUP, OUT, IN) found in the traffic
- Data which indicates the total of data bytes found in the traffic (sync, PID, CRC included)

Status Bar


Ready
Frm count 1
Frm# 0x000
Evnt# 4
Evnt byte# 4

The purpose of the status bar is to present status messages and indicate the traffic focus.

Example of status messages are: "Packing data…" while a traffic file is saved, or "Unpacking data…" while a traffic file is loaded.

The traffic focus is indicated by the following read only controls:

- Frm count
- Frm#
- Evnt#
- Evnt byte#

Frm count indicates the count of the frame containing the current traffic item. The first frame has a count of 1. If the traffic has been captured on a low speed bus, or it is not preceded by any SOF, that control stays empty.

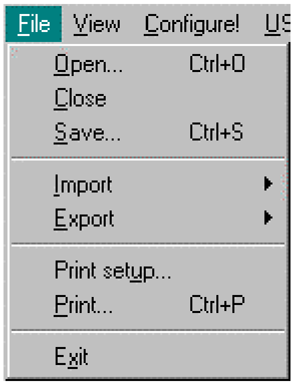
Frm# indicates the number of the frame containing the current traffic item. If the traffic has been captured on a low speed bus, or it is not preceded by any SOF, that control stays empty.

Evnt# indicates the number of the event the traffic focus is selecting. On Event Layer this control indicates the number of the selected event. On Transaction Layer this control indicates an event depending on the type of the selected transaction item (refer to Traffic Focus on Transaction Layer). On Data Layer the control indicates the data packet of the transaction which provided the byte selected in the Traffic window.

Evnt byte# indicates the number of the byte transferred in the event indicated in Evnt# control. If no data bytes have been transferred in that event, this control stays empty.

The traffic focus information helps the user to check that it stays in the same place of the traffic when switching between filtered and unfiltered traffic, or when switching between traffic layers.

File Menu

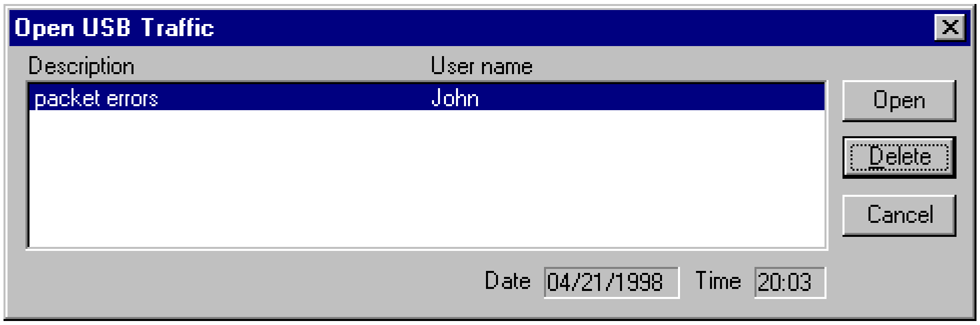


Open

Open command may be activated in any of the following ways:

- by typing CTRL+O
- by typing ALT+F, then ALT+O
- by clicking File menu item, then Open command

When activated, this command brings Open USB Traffic dialog:



Description	User name
packet errors	John

Date 04/21/1998 Time 20:03

If the program displays USB traffic which has not been saved, the user is first asked if that traffic can be overwritten. The user may choose either to cancel the Open command, or to overwrite the existing traffic.

Close

Close command may be activated in any of the following ways:

- by typing ALT+F, then ALT+C
- by clicking File menu item, then Close command

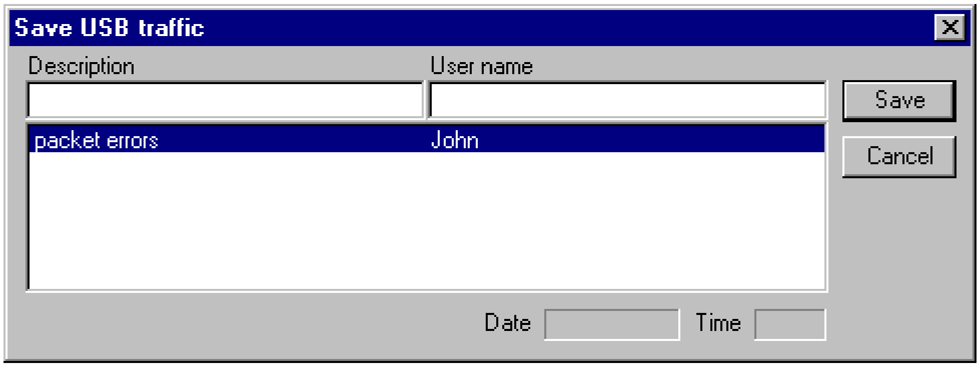
If the program displays USB traffic which has not been saved, the user is asked if that traffic should be saved. The user may choose to cancel the Close command, or to close the traffic, or to save the existing traffic.

Save

Save command may be activated in any of the following ways:

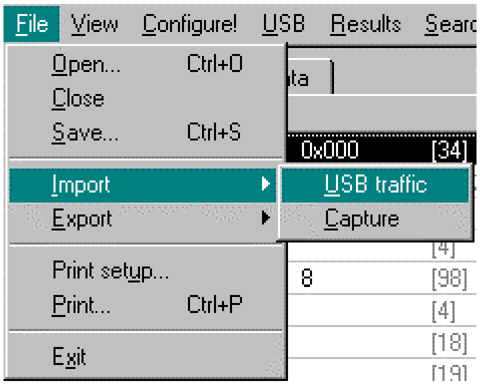
- by typing `CTRL+S`
- by typing `ALT+F`, then `ALT+S`
- by clicking File menu item, then Save command

When activated, this command brings Save USB Traffic dialog:



Description	User name
packet errors	John

Import USB

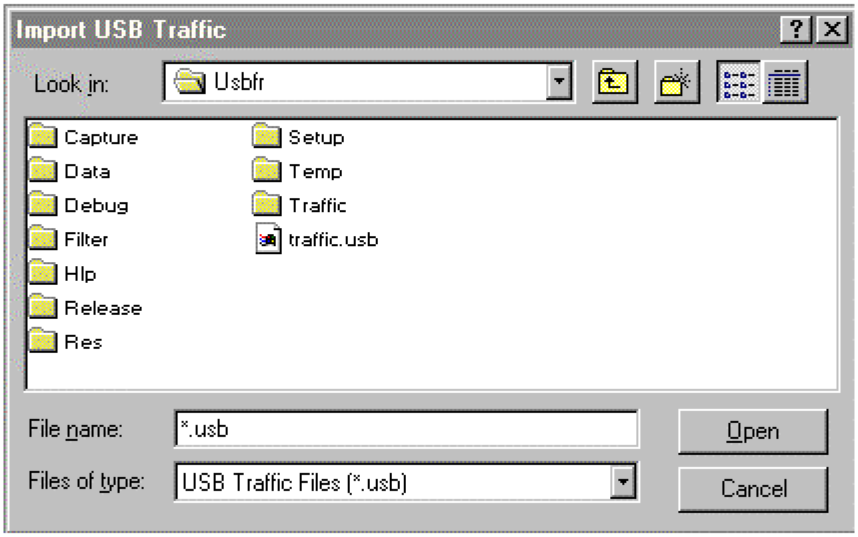


Import USB command may be activated in any of the following ways:

- by typing `ALT+F`, then `ALT+I`, then `ALT+U`
- by clicking File menu item, then Import command, then USB traffic command.

If the program displays USB traffic which has not been saved, the user is first asked if that traffic can be overwritten. The user may choose either to cancel the Import USB command, or to overwrite the existing traffic.

When activated, this command brings a file selection dialog presented below:



File name: *.usb

Files of type: USB Traffic Files (*.usb)

Once the traffic file is selected it may be loaded by clicking Open button. USB traffic files are saved in user defined files having extension ".usb", by using Export USB command of File menu.

An USB traffic file contains the whole information with regards to that traffic (capture options, signals, events, packets, transactions, frames, reports, statistics, etc.), and is held in compressed format.

Traffic files having user defined names may be used to share between multiple users the information created by the protocol analyzer (note that Open and Save commands operate on a data base).

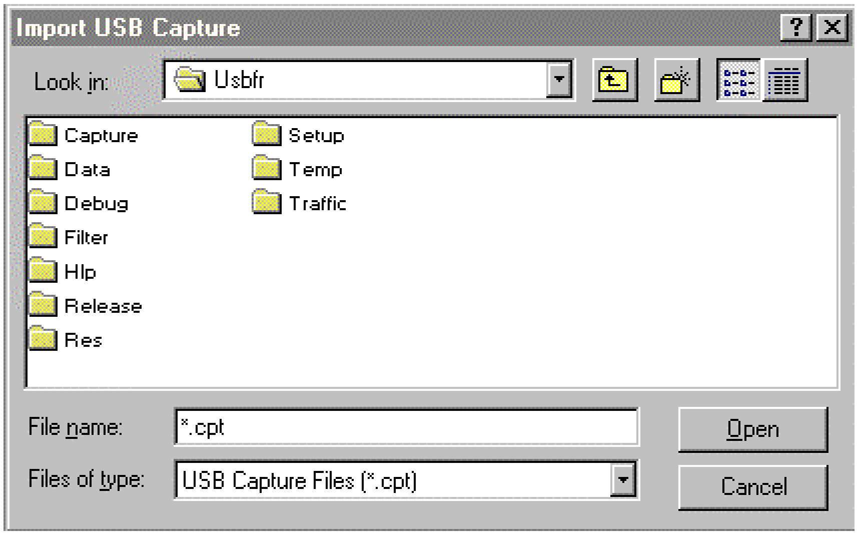
Import Capture

Import Capture command may be activated in any of the following ways:

- by typing `ALT+F`, then `ALT+I`, then `ALT+C`
- by clicking File menu item, then Import command, then Capture command.

If the program displays USB traffic which has not been saved, the user is first asked if that traffic can be overwritten. The user may choose either to cancel the Import Capture command, or to overwrite the existing traffic.

When activated, this command brings a file selection dialog presented below:



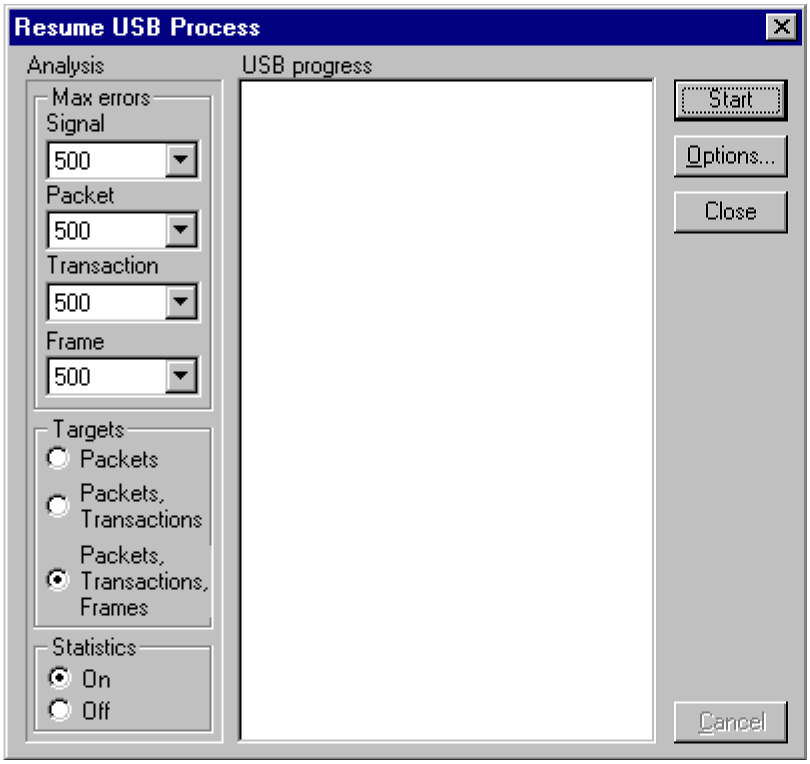
Look in: Usbfr

File name: *.cpt

Files of type: USB Capture Files (*.cpt)

Once the capture file is selected it may be loaded by clicking Open button. Capture files are saved in user defined files having extension ".cpt", by using Export Capture command of File menu.

The capture file contains information on signals and capture options only. After it is loaded, the program brings Resume USB Process dialog to allow the user to resume the USB Process:



Max errors

Signal: 500

Packet: 500

Transaction: 500

Frame: 500

Targets

○ Packets

○ Packets, Transactions

● Packets, Transactions, Frames

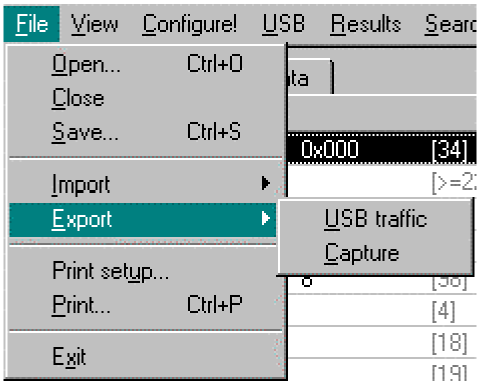
Statistics

● On

○ Off

Such a file may be used to help technical support (the information stored in a capture file is not submitted to the USB analysis).

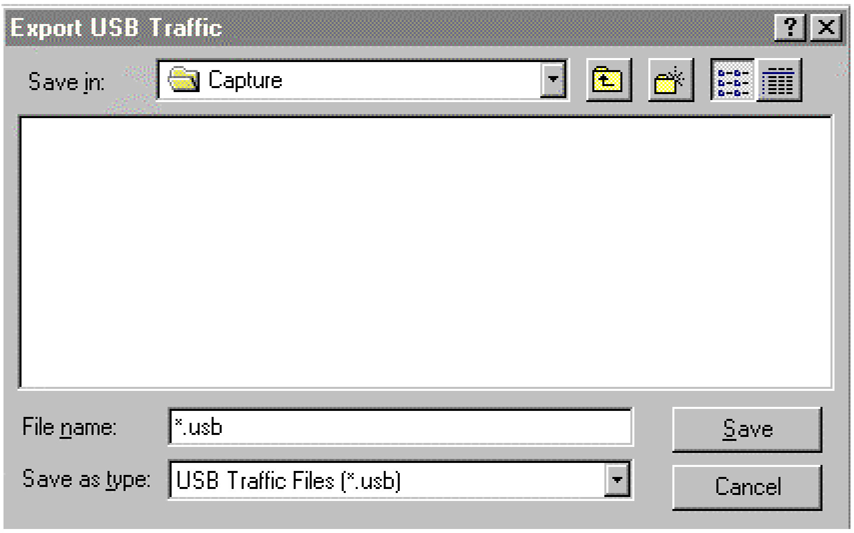
Export USB



Export USB command may be activated in any of the following ways:

- by typing ALT+F, then ALT+E, then ALT+U
- by clicking File menu item, then Export command, then USB traffic command.

When activated, this command brings a file selection dialog presented below:



Save in: Capture

File name: *.usb

Save as type: USB Traffic Files (*.usb)

The USB traffic file is saved in the file presented in File Name control when Save button is pressed.

An USB traffic file contains the whole information with regards to that traffic (capture options, signals, events, packets, transactions, frames, reports, statistics, etc.), and is held in compressed format.

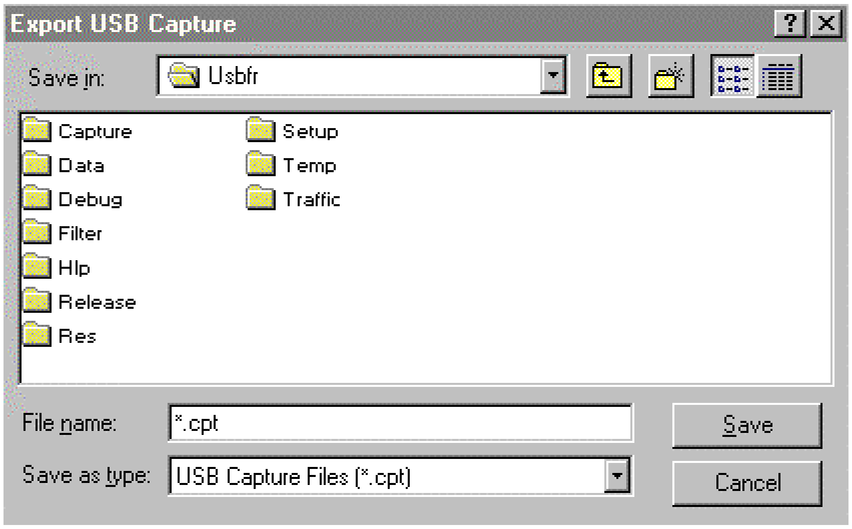
Traffic files having user defined names may be used to share between multiple users the information created by the protocol analyzer (note that Open and Save commands operate on a data base).

Export Capture

Export Capture command may be activated in any of the following ways:

- by typing ALT+F, then ALT+E, then ALT+C
- by clicking File menu item, then Export command, then Capture command.

When activated, this command brings a file selection dialog presented below:



Save in: Usbfr

File name: *.cpt

Save as type: USB Capture Files (*.cpt)

The capture file has the extension ".cpt" and contains information on signals and capture options only. Such a file may be used to help technical support (the information stored in a capture file is not submitted to the USB analysis).

Print Setup

Print Setup command may be activated in any of the following ways:

- by typing ALT+F, then ALT+U
- by clicking File menu item, then Print Setup command.

When activated, this command brings Print Setup dialog (as in other Windows applications).

Print

Print command may be activated in any of the following ways:

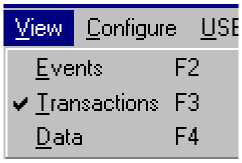
- by typing ALT+F, then ALT+P
- by clicking File menu item, then Print command.

When activated, this command brings Print dialog (as in other Windows applications).

Exit

This command is available in File drop menu. When activated, the program asks if the current traffic should be saved (if not already). Upon the execution of this command the USB Protocol Analyzer application is closed.

View Menu

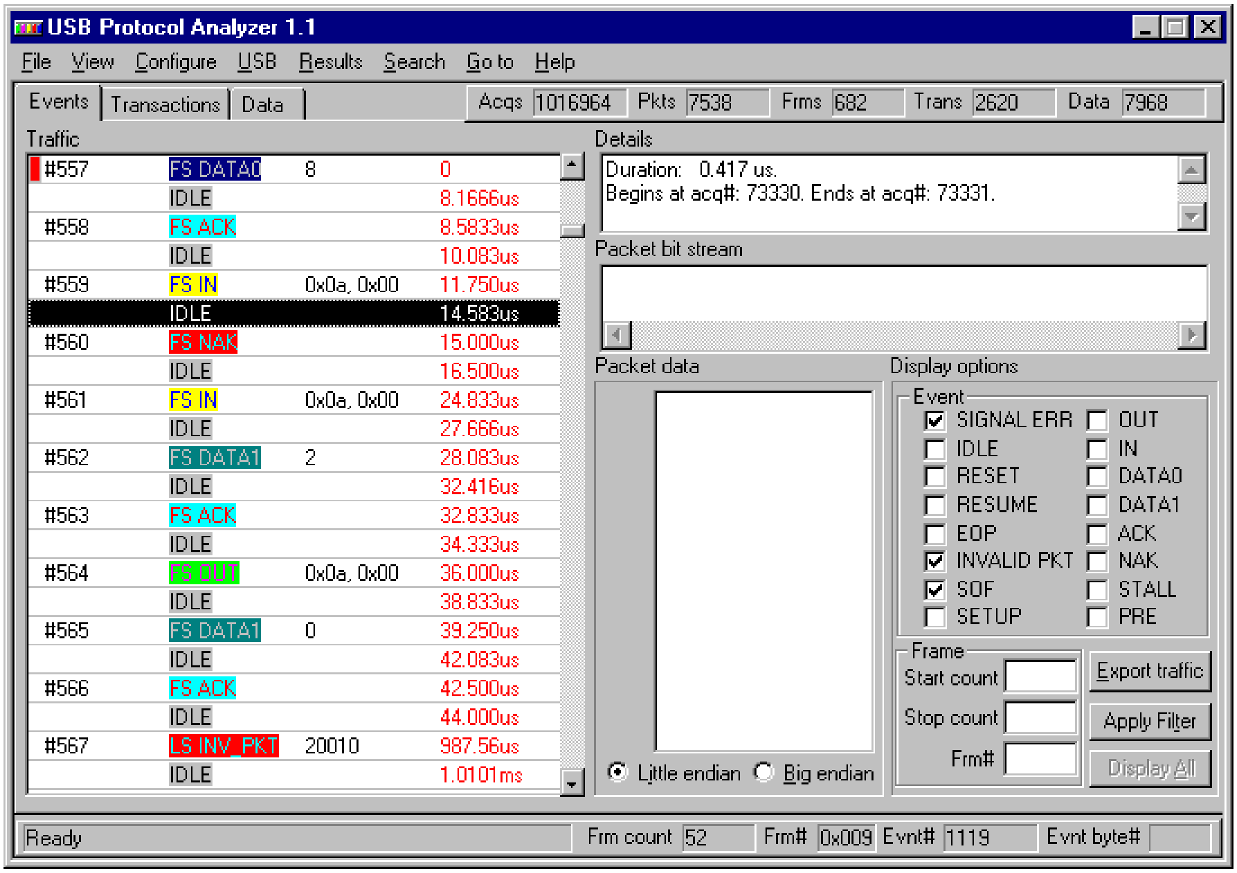


Events

View Events command may be activated in any of the following ways:

- by typing ALT+V, then ALT+E
- by typing F2
- by clicking View menu item, then Events command.
- by clicking the tab of Event Layer

When this command is activated, the program presents Event Layer:



Acqs 1016964 Pkts 7538 Frms 682 Trans 2620 Data 7968

#557	FS DATA0	8	0
	IDLE		8.1666us
#558	FS ACK		8.5833us
	IDLE		10.083us
#559	FS IN	0x0a, 0x00	11.750us
	IDLE		14.583us
#560	FS NAK		15.000us
	IDLE		16.500us
#561	FS IN	0x0a, 0x00	24.833us
	IDLE		27.666us
#562	FS DATA1	2	28.083us
	IDLE		32.416us
#563	FS ACK		32.833us
	IDLE		34.333us
#564	FS OUT	0x0a, 0x00	36.000us
	IDLE		38.833us
#565	FS DATA1	0	39.250us
	IDLE		42.083us
#566	FS ACK		42.500us
	IDLE		44.000us
#567	LS INV_PKT	20010	987.56us
	IDLE		1.0101ms

Duration: 0.417 us.
Begins at acq#: 73330. Ends at acq#: 73331.

● Little endian ○ Big endian

Event
☑ SIGNAL ERR ☐ OUT
☐ IDLE ☐ IN
☐ RESET ☐ DATA0
☐ RESUME ☐ DATA1
☐ EOP ☐ ACK
☑ INVALID PKT ☐ NAK
☑ SOF ☐ STALL
☐ SETUP ☐ PRE

Frame
Start count
Stop count
Frm#

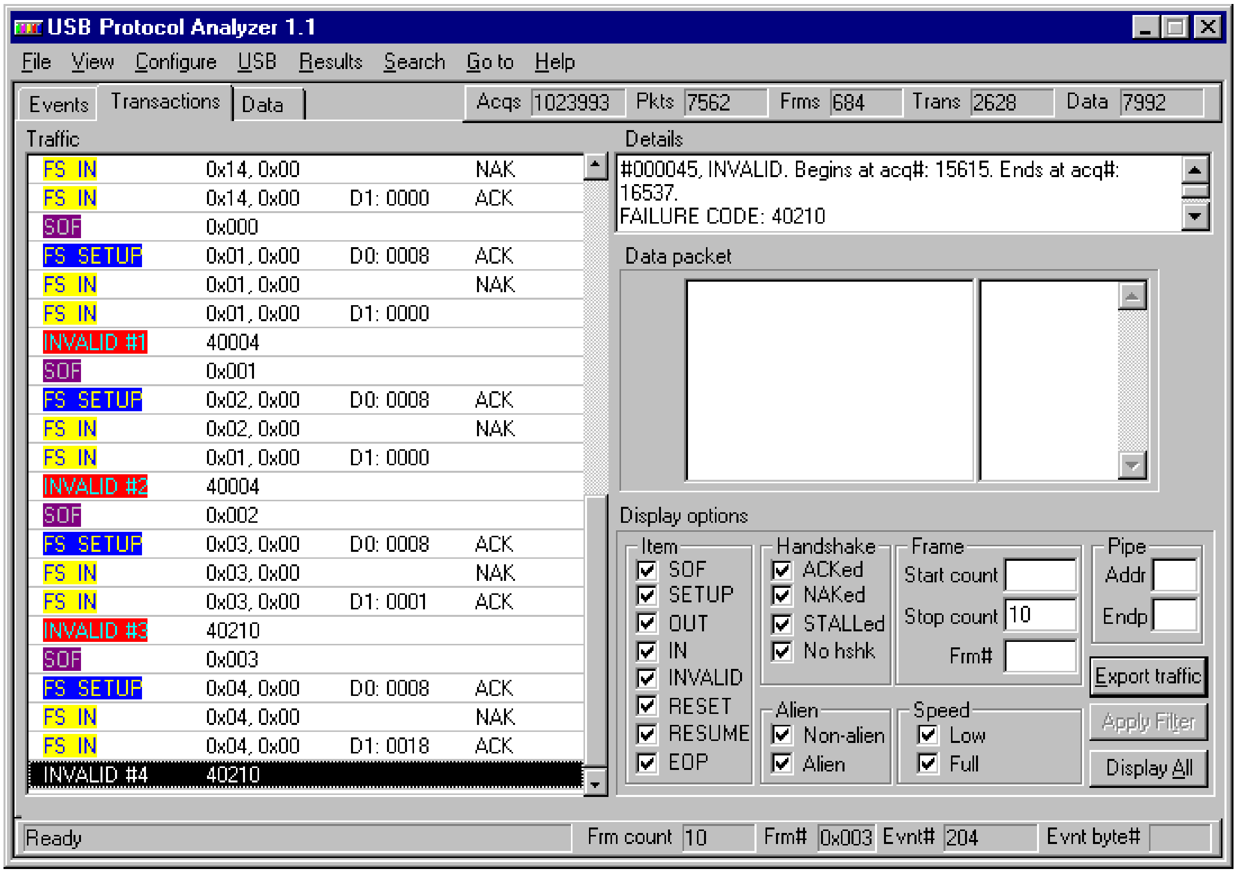
Ready Frm count 52 Frm# 0x009 Evnt# 1119 Evnt byte#

Transactions

View Transactions command may be activated in any of the following ways:

- by typing ALT+V, then ALT+T
- by typing F3
- by clicking View menu item, then Transactions command.
- by clicking the tab of Transaction Layer

When this command is activated, the program presents Transaction Layer:



Acqs 1023993 Pkts 7562 Frms 684 Trans 2628 Data 7992

FS IN	0x14, 0x00		NAK
FS IN	0x14, 0x00	D1: 0000	ACK
SOF	0x000		
FS SETUP	0x01, 0x00	D0: 0008	ACK
FS IN	0x01, 0x00		NAK
FS IN	0x01, 0x00	D1: 0000	
INVALID #1	40004		
SOF	0x001		
FS SETUP	0x02, 0x00	D0: 0008	ACK
FS IN	0x02, 0x00		NAK
FS IN	0x01, 0x00	D1: 0000	
INVALID #2	40004		
SOF	0x002		
FS SETUP	0x03, 0x00	D0: 0008	ACK
FS IN	0x03, 0x00		NAK
FS IN	0x03, 0x00	D1: 0001	ACK
INVALID #3	40210		
SOF	0x003		
FS SETUP	0x04, 0x00	D0: 0008	ACK
FS IN	0x04, 0x00		NAK
FS IN	0x04, 0x00	D1: 0018	ACK
INVALID #4	40210		

#000045, INVALID. Begins at acq#: 15615. Ends at acq#: 16537.
FAILURE CODE: 40210

Item
☑ SOF
☑ SETUP
☑ OUT
☑ IN
☑ INVALID
☑ RESET
☑ RESUME
☑ EOP

Handshake
☑ ACKed
☑ NAKed
☑ STALLed
☑ No hshk

Frame
Start count
Stop count 10
Frm#

Pipe
Addr
Endp

Alien
☑ Non-alien
☑ Alien

Speed
☑ Low
☑ Full

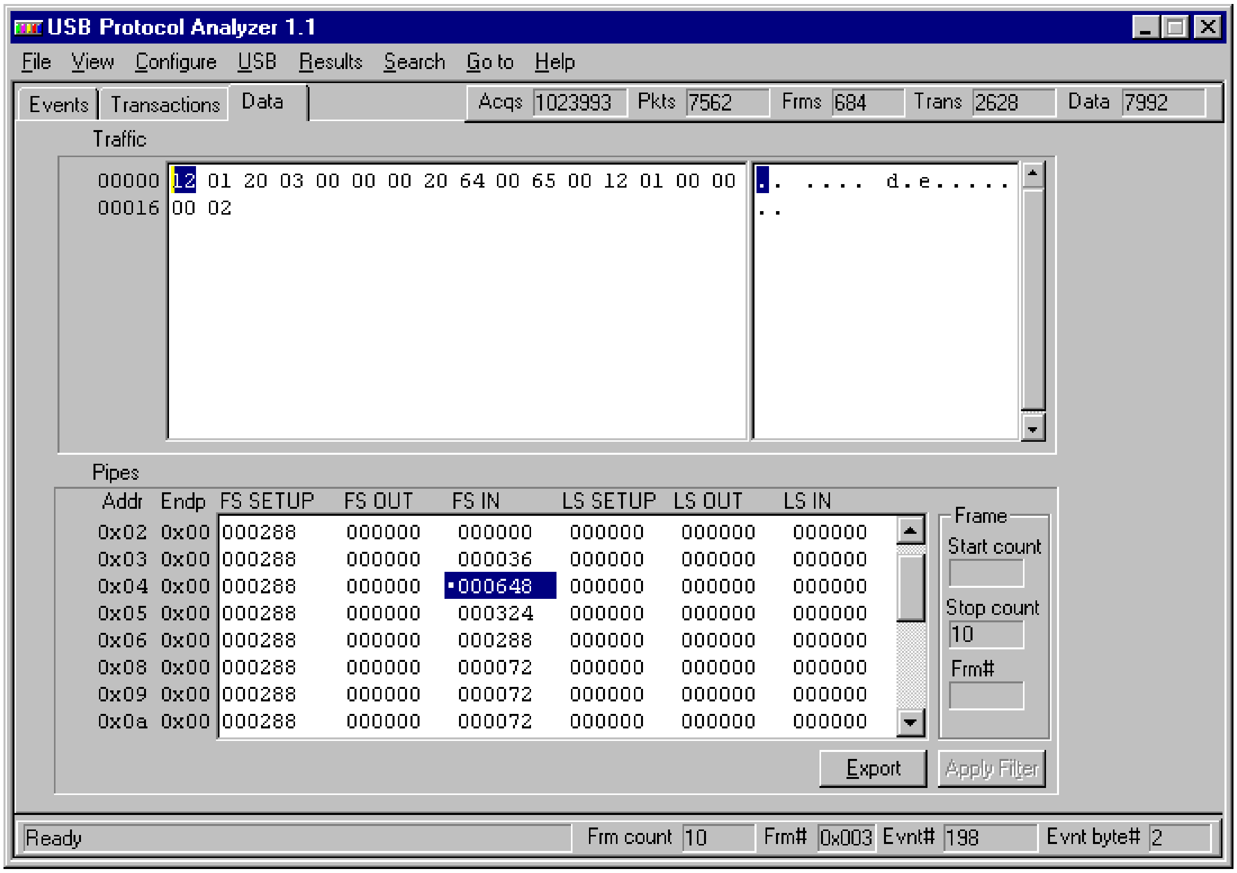
Ready Frm count 10 Frm# 0x003 Evnt# 204 Evnt byte#

Data

View Data command may be activated in any of the following ways:

- by typing ALT+V, then ALT+D
- by typing F4
- by clicking View menu item, then Data command.
- by clicking the tab of Data Layer

When this command is activated, the program presents Data Layer:



Acqs 1023993 Pkts 7562 Frms 684 Trans 2628 Data 7992

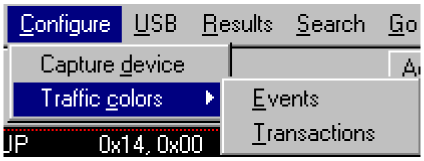
```
00000 12 01 20 03 00 00 00 20 64 00 65 00 12 01 00 00   .. .... d.e.....
00016 00 02                                              ..
```

Addr	Endp	FS SETUP	FS OUT	FS IN	LS SETUP	LS OUT	LS IN
0x02	0x00	000288	000000	000000	000000	000000	000000
0x03	0x00	000288	000000	000036	000000	000000	000000
0x04	0x00	000288	000000	000648	000000	000000	000000
0x05	0x00	000288	000000	000324	000000	000000	000000
0x06	0x00	000288	000000	000288	000000	000000	000000
0x08	0x00	000288	000000	000072	000000	000000	000000
0x09	0x00	000288	000000	000072	000000	000000	000000
0x0a	0x00	000288	000000	000072	000000	000000	000000

Start count
Stop count 10
Frm#

Ready Frm count 10 Frm# 0x003 Evnt# 198 Evnt byte# 2

Configure Menu

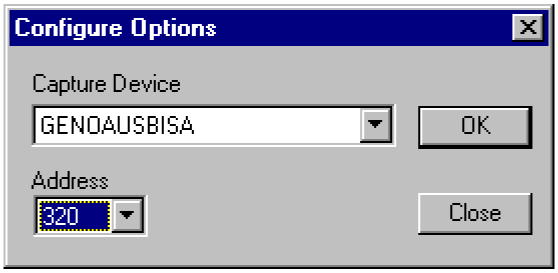


Configure Capture Device

Configure Capture Device command may be activated in any of the following ways:

- by clicking Configure menu item of bar menu, then selecting Capture Device command
- by typing `ALT+C,` then `ALT+D`

When activated, this command brings Configure Options dialog:



Capture Device: GENOAUSBISA

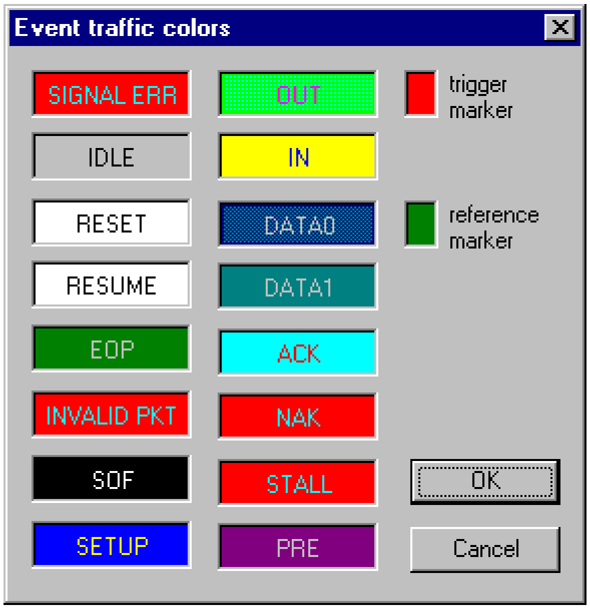
Address: 320

Configure Event Traffic Colors

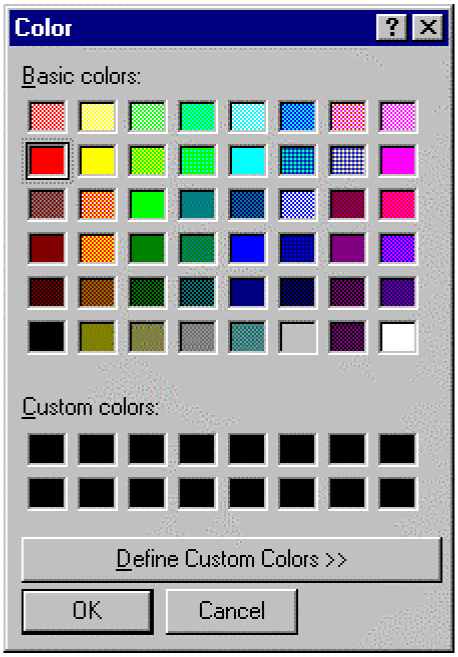
Configure Capture Device command may be activated in any of the following ways:

- by clicking Configure menu item of bar menu, then selecting Traffic Colors, Events command
- by typing `ALT+C,` then `ALT+C` and `ALT+E`

When activated, this command brings Event traffic colors dialog:



The user may specify a color for each event, as well as for the trigger and reference marker. When a control is clicked in this dialog, the program brings a color selection dialog which allows the user to choose the color:

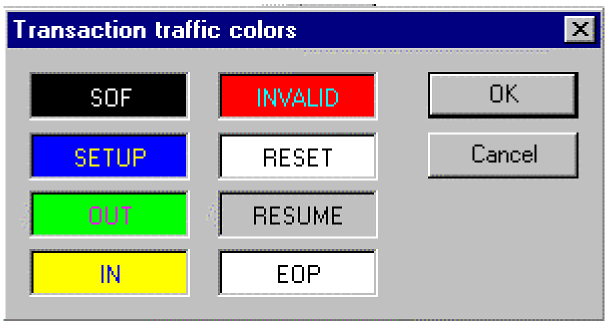


Configure Transaction Traffic Colors

Configure Capture Device command may be activated in any of the following ways:

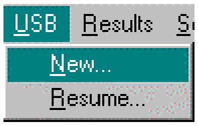
- by clicking Configure menu item of bar menu, then selecting Traffic Colors, Transactions command
- by typing `ALT+C`, then `ALT+C` and `ALT+T`

When activated, this command brings Transaction traffic colors dialog:



The user may specify a color for each transaction item. When a control is clicked in this dialog, the program brings a color selection dialog which allows the user to choose the color.

USB Menu

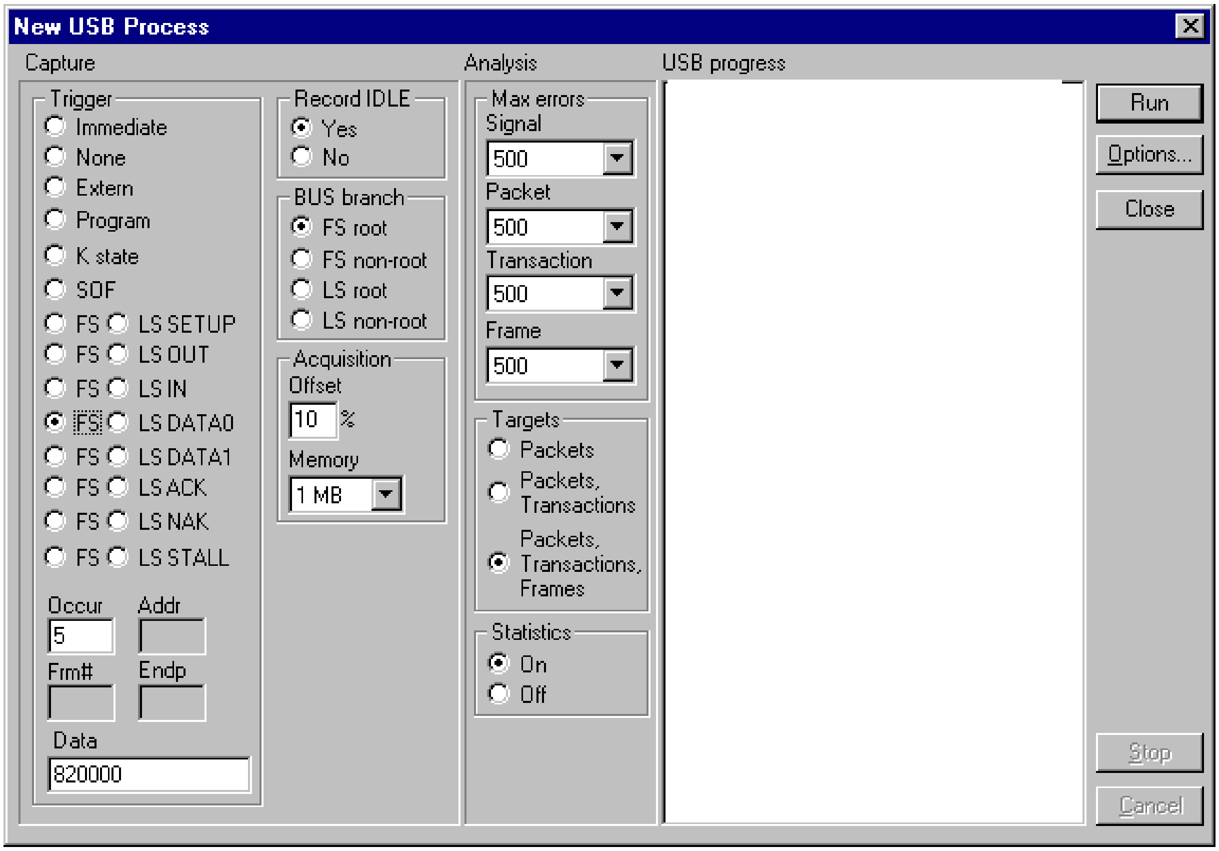


New USB

New USB command may be activated in any of the following ways:

- by typing ALT+U, then ALT+N
- by clicking USB menu item, then New command.

When this command is activated, the program presents New USB Process dialog:



Trigger
○ Immediate
○ None
○ Extern
○ Program
○ K state
○ SOF
○ FS ○ LS SETUP
○ FS ○ LS OUT
○ FS ○ LS IN
● FS ○ LS DATA0
○ FS ○ LS DATA1
○ FS ○ LS ACK
○ FS ○ LS NAK
○ FS ○ LS STALL

Occur: 5
Addr:
Frm#:
Endp:
Data: 820000

Record IDLE
● Yes
○ No

BUS branch
● FS root
○ FS non-root
○ LS root
○ LS non-root

Acquisition
Offset: 10 %
Memory: 1 MB

Max errors
Signal: 500
Packet: 500
Transaction: 500
Frame: 500

Targets
○ Packets
○ Packets, Transactions
● Packets, Transactions, Frames

Statistics
● On
○ Off

If the program displays already USB traffic which has not been saved, the user will be asked if that traffic may be overwritten. The user may choose to overwrite the current traffic or to cancel New USB command.

This dialog provides options for the traffic capture and for the traffic analysis. It contains the following controls:

- **Trigger** group
- **Record Idle** group
- **Bus Branch** group
- **Acquisition** group
- **Max. Errors** group
- **Targets** group
- **Statistics** group
- **USB Progress** window
- **Run** button
- **Options** button
- **Close** button
- **Stop** button
- **Cancel** button

Trigger group allows the user to choose one of the available trigger options (refer to Trigger Machine for details).

Record Idle group allows the user to specify Record Idle option (refer to Record Idle Option for details).

Bus Branch group allows the user to specify the type of the bus branch where the USB Probe is inserted. Available options are: FS root, FS non-root, LS root, LS non-root.

Acquisition group allows the user to specify the size of the acquisition memory used to capture the USB traffic, and the acquisition offset. The memory size provides the following options: 128k, 256k, 512k, 1M, 2M, 4M, 8M, 16M, 32M. The acquisition offset indicates the percentage of the acquisition memory used to store traffic occurred before the trigger.

Max. Errors group allows the user to specify the max. number of errors of each traffic analysis stage: signaling errors for Event Analysis, packet errors for Packet Analysis, transaction errors for Transaction Analysis, frame errors for Frame Analysis. Available options are: 10, 50, 500.

Targets group allows the user to specify the targets of USB Process:

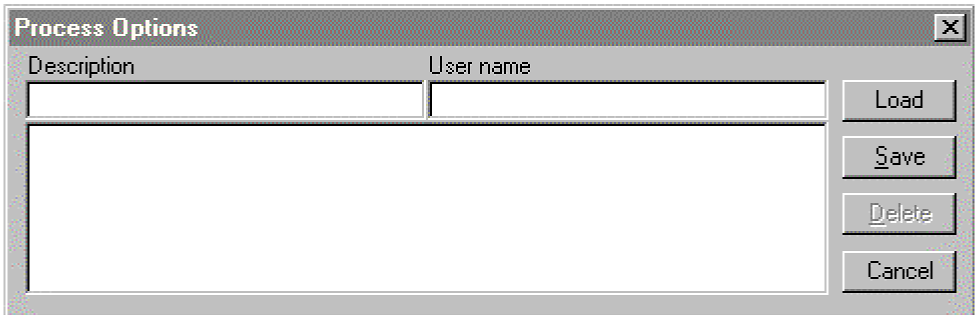
- events and packets when **Packets** radio button is selected
- events, packets, and transactions when **Packets, Transactions** radio button is selected
- events, packets, transactions, frames when **Packets, Transactions, Frames** radio button is selected (that is a complete USB Process)

If the user choose an incomplete USB Process, it may resume the process with the stages which were not done (refer to Resume USB).

Statistics group allows the user to enable or disable building the statistics for the traffic which is captured and analyzed.

USB Progress window presents the progress of the USB Process. When a stage of the process is terminated, the program displays a summary of that stage. That summary will be also written in the Summary report.

Pressing Run button will start the USB Process with the current options. These options may be saved before starting the process by pressing Options button. At that moment the program opens Process Options dialog:



This dialog contains the following controls:

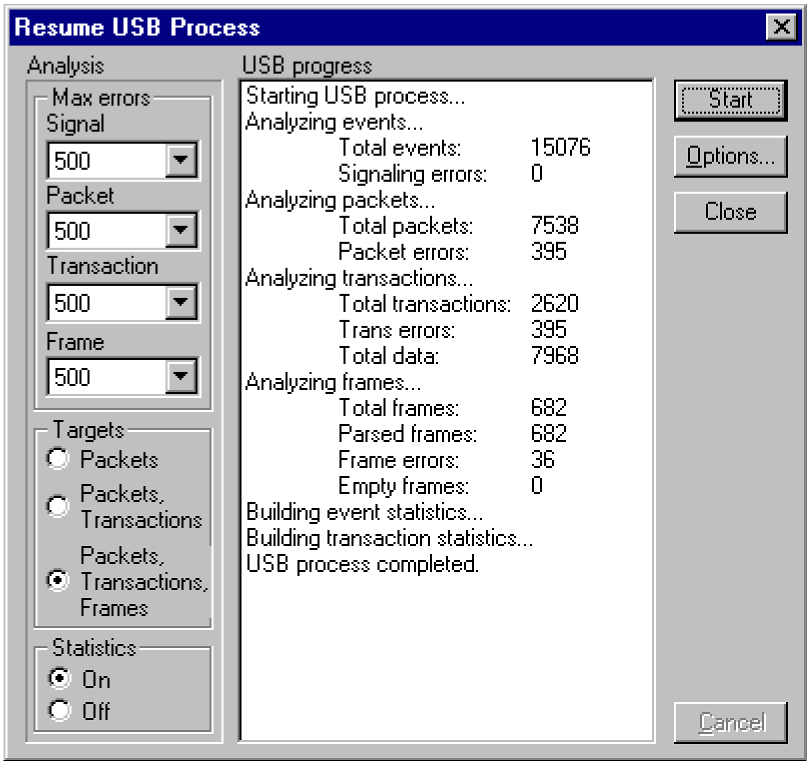
- Load button to allow the user to load selected options
- Save button to allow the user to save current options
- Delete button to allow the user to delete selected options
- Cancel button to cancel the operation

Resume USB

Resume USB command may be activated in any of the following ways:

- by typing ALT+U, then ALT+R
- by clicking USB menu item, then Resume command.

When this command is activated, the program presents Resume USB Process dialog:



Signal: 500
Packet: 500
Transaction: 500
Frame: 500

Targets:
○ Packets
○ Packets, Transactions
● Packets, Transactions, Frames

Statistics:
● On
○ Off

```
Starting USB process...
Analyzing events...
            Total events:        15076
            Signaling errors:    0
Analyzing packets...
            Total packets:       7538
            Packet errors:       395
Analyzing transactions...
            Total transactions:  2620
            Trans errors:        395
            Total data:          7968
Analyzing frames...
            Total frames:        682
            Parsed frames:       682
            Frame errors:        36
            Empty frames:        0
Building event statistics...
Building transaction statistics...
USB process completed.
```

This dialog provides options for the traffic capture and for the traffic analysis:

- **Max. Errors** group
- **Targets** group
- **Statistics** group
- **USB Progress** window
- **Run** button
- **Options** button
- **Close** button
- **Stop** button
- **Cancel** button

Max. Errors group allows the user to specify the max. number of errors of each traffic analysis stage: signaling errors for Event Analysis, packet errors for Packet Analysis, transaction errors for Transaction Analysis, frame errors for Frame Analysis. Available options are: 10, 50, 500.

Targets group allows the user to specify the targets of USB Process:

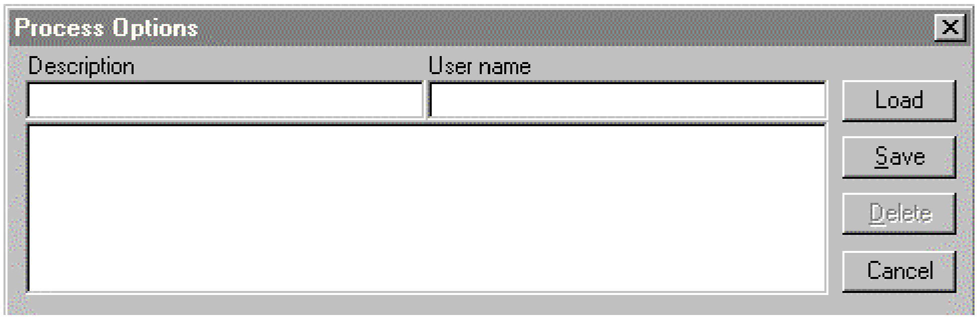
- events and packets when **Packets** radio button is selected
- events, packets, and transactions when **Packets, Transactions** radio button is selected
- events, packets, transactions, frames when **Packets, Transactions, Frames** radio button is selected (that is a complete USB Process)

If the user choose an incomplete USB Process, it may resume the process with the stages which were not done.

Statistics group allows the user to enable or disable building the statistics for the traffic which is captured and analyzed.

USB Progress window presents the progress of the USB Process. When a stage of the process is terminated, the program displays a summary of that stage.

Pressing **Run** button will start the USB Process with the current options. These options may be saved before starting the process by pressing **Options** button. At that moment the program opens Process Options dialog:

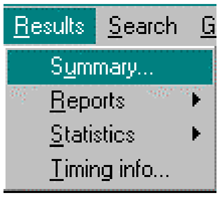


This dialog contains the following controls:

- **Load** button to allow the user to load selected options
- **Save** button to allow the user to save current options
- **Delete** button to allow the user to delete selected options
- **Cancel** button to cancel the operation

Results Menu

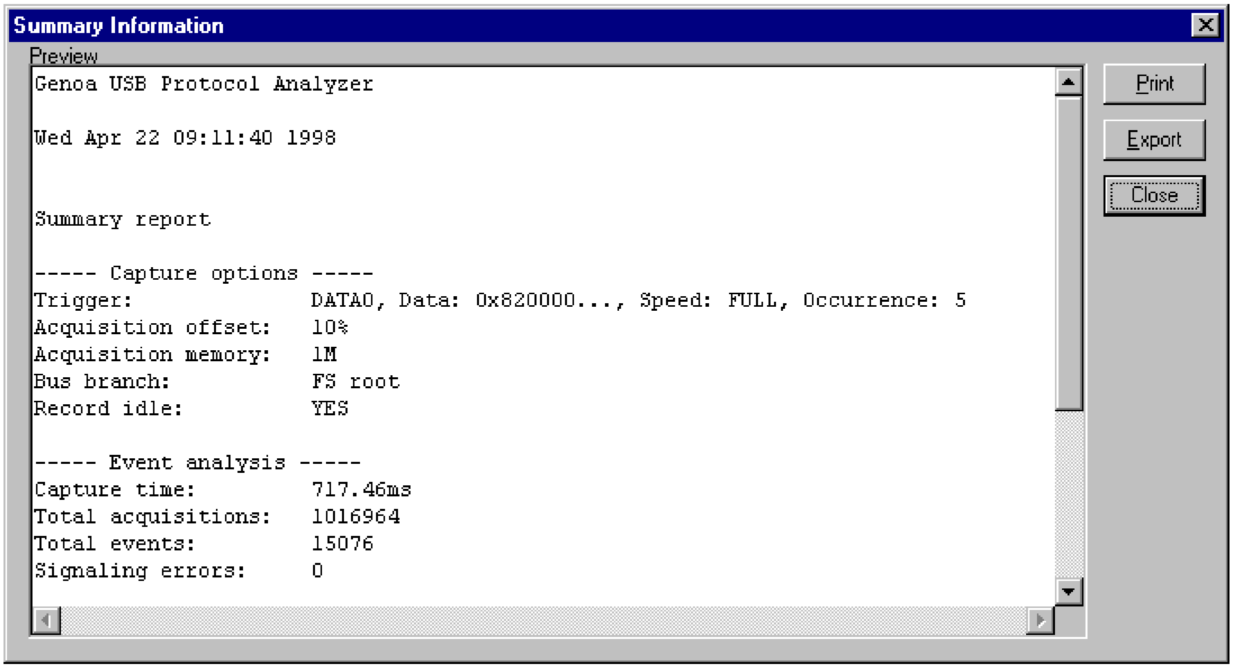
Summary



Summary command may be activated in any of the following ways:

- by typing ALT+R, then ALT+U
- by clicking Results menu item, then Summary command.

When this command is activated, the program presents a Report dialog containing a summary of the last USB Process:

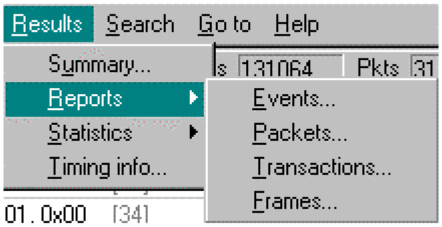


```
Genoa USB Protocol Analyzer

Wed Apr 22 09:11:40 1998


Summary report

----- Capture options -----
Trigger:             DATA0, Data: 0x820000..., Speed: FULL, Occurrence: 5
Acquisition offset:  10%
Acquisition memory:  1M
Bus branch:          FS root
Record idle:         YES

----- Event analysis -----
Capture time:        717.46ms
Total acquisitions:  1016964
Total events:        15076
Signaling errors:    0
```

The dialog contains the following controls:

- the text window with its vertical scroll bar
- the Print button which brings Print dialog to allow the user to print the text
- the Export button which brings a file selection window to allow the user to save the text in a user defined file
- the Close button which closes the Report dialog

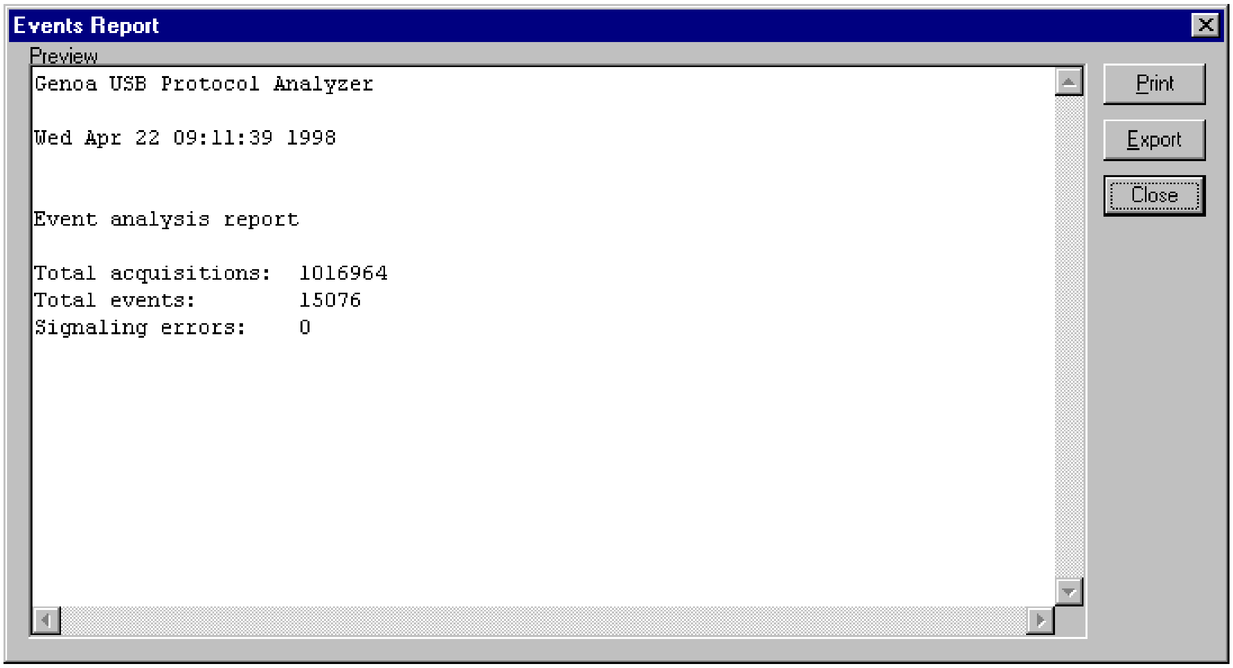
Event Analysis Report



Event Analysis Report command may be activated in any of the following ways:

- by typing ALT+R, then ALT+R, then ALT+E
- by clicking Results menu item, then Reports command, then Events command.

When this command is activated, the program presents Report dialog containing the Event Analysis report of the last USB Process:



```
Genoa USB Protocol Analyzer

Wed Apr 22 09:11:39 1998


Event analysis report

Total acquisitions:  1016964
Total events:        15076
Signaling errors:    0
```

The dialog contains the following controls:

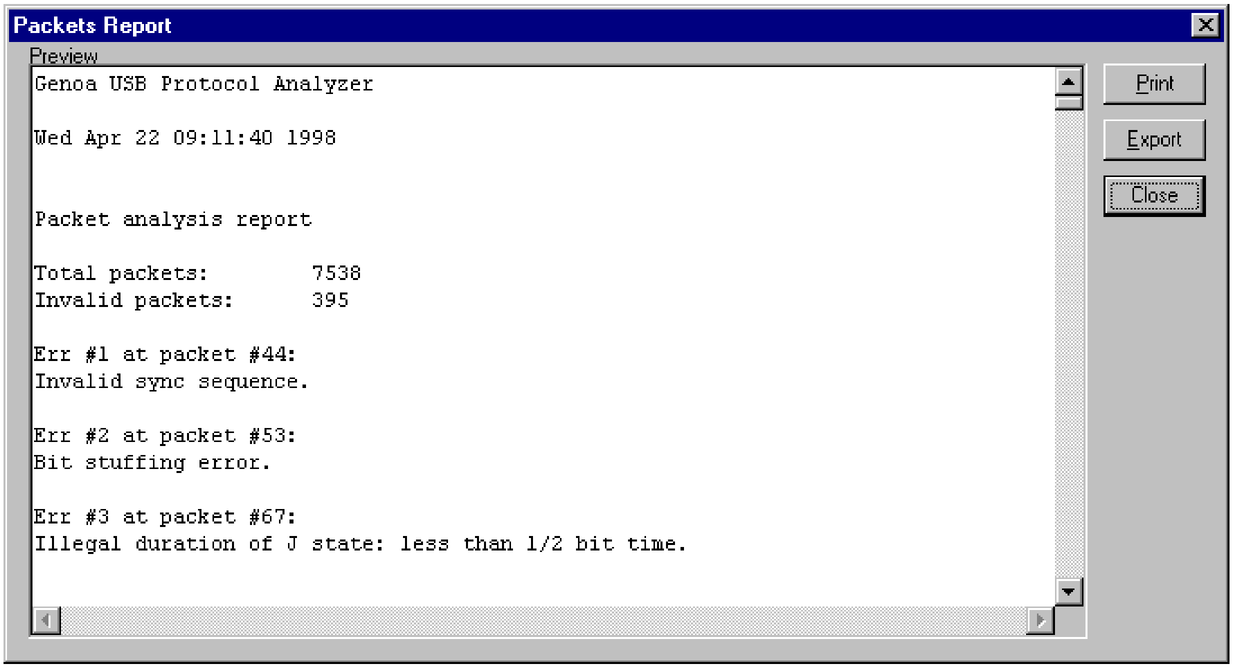
- the text window with its vertical scroll bar
- the Print button which brings Print dialog to allow the user to print the text
- the Export button which brings a file selection window to allow the user to save the text in a user defined file
- the Close button which closes the Report dialog

Packet Analysis Report

Packet Analysis Report command may be activated in any of the following ways:

- by typing ALT+R, then ALT+R, then ALT+P
- by clicking Results menu item, then Reports command, then Packets command.

When this command is activated, the program presents a Report dialog containing the Packet Analysis report of the last USB Process:



```
Genoa USB Protocol Analyzer

Wed Apr 22 09:11:40 1998


Packet analysis report

Total packets:        7538
Invalid packets:      395

Err #1 at packet #44:
Invalid sync sequence.

Err #2 at packet #53:
Bit stuffing error.

Err #3 at packet #67:
Illegal duration of J state: less than 1/2 bit time.
```

The dialog contains the following controls:

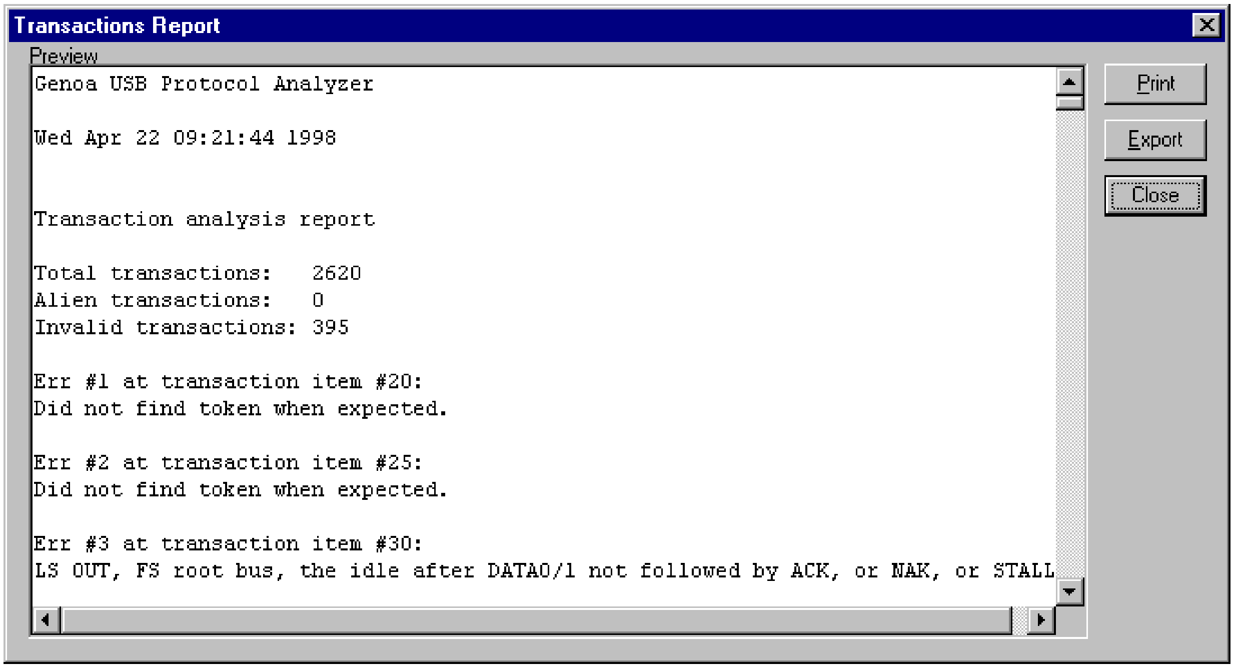
- the text window with its vertical scroll bar
- the Print button which brings Print dialog to allow the user to print the text
- the Export button which brings a file selection window to allow the user to save the text in a user defined file
- the Close button which closes the Report dialog

Transaction Analysis Report

Transaction Analysis Report command may be activated in any of the following ways:

- by typing ALT+R, then ALT+R, then ALT+T
- by clicking Results menu item, then Reports command, then Transactions command.

When this command is activated, the program presents a Report dialog containing the Transaction Analysis report of the last USB Process:



```
Genoa USB Protocol Analyzer

Wed Apr 22 09:21:44 1998


Transaction analysis report

Total transactions:   2620
Alien transactions:   0
Invalid transactions: 395

Err #1 at transaction item #20:
Did not find token when expected.

Err #2 at transaction item #25:
Did not find token when expected.

Err #3 at transaction item #30:
LS OUT, FS root bus, the idle after DATA0/1 not followed by ACK, or NAK, or STALL
```

The dialog contains the following controls:

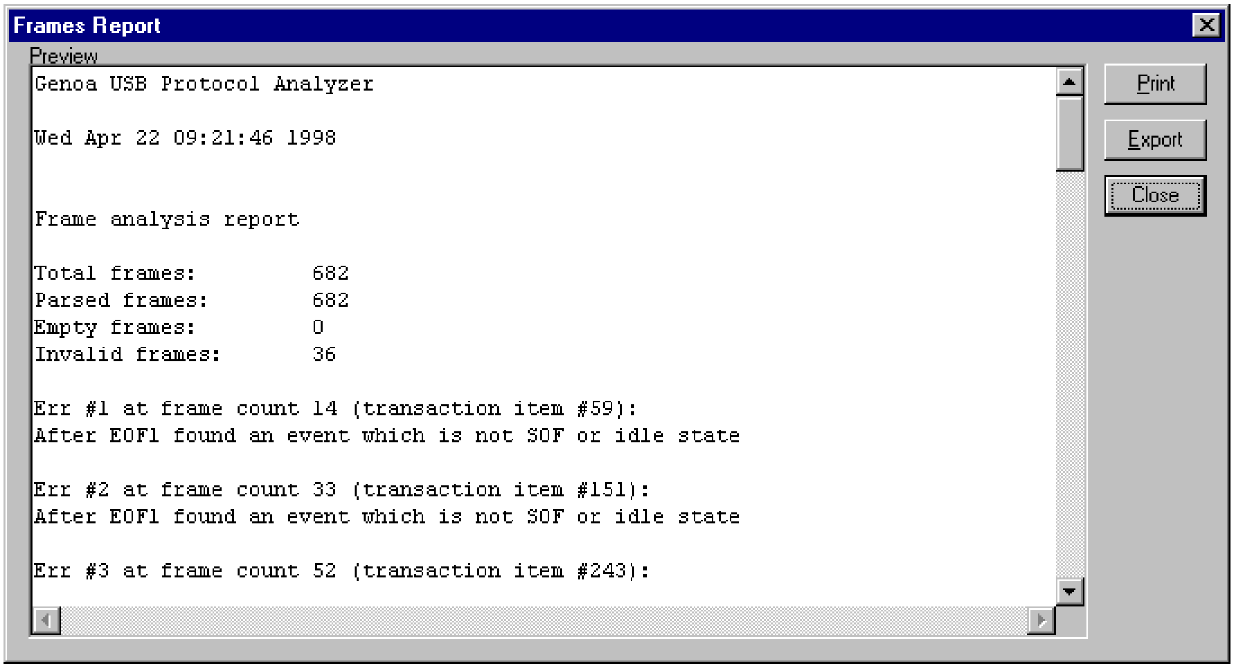
- the text window with its vertical scroll bar
- the Print button which brings Print dialog to allow the user to print the text
- the Export button which brings a file selection window to allow the user to save the text in a user defined file
- the Close button which closes the Report dialog

Frame Analysis Report

Frame Analysis Report command may be activated in any of the following ways:

- by typing ALT+R, then ALT+R, then ALT+F
- by clicking Results menu item, then Reports command, then Frames command.

When this command is activated, the program presents a Report dialog containing the Frame Analysis report of the last USB Process:

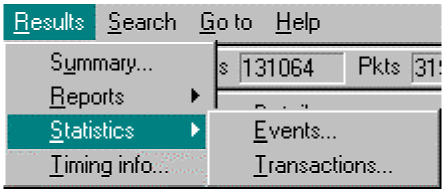


```
Genoa USB Protocol Analyzer

Wed Apr 22 09:21:46 1998


Frame analysis report

Total frames:          682
Parsed frames:         682
Empty frames:          0
Invalid frames:        36

Err #1 at frame count 14 (transaction item #59):
After EOF1 found an event which is not SOF or idle state

Err #2 at frame count 33 (transaction item #151):
After EOF1 found an event which is not SOF or idle state

Err #3 at frame count 52 (transaction item #243):
```

The dialog contains the following controls:

- the text window with its vertical scroll bar
- the Print button which brings Print dialog to allow the user to print the text
- the Export button which brings a file selection window to allow the user to save the text in a user defined file
- the Close button which closes the Report dialog

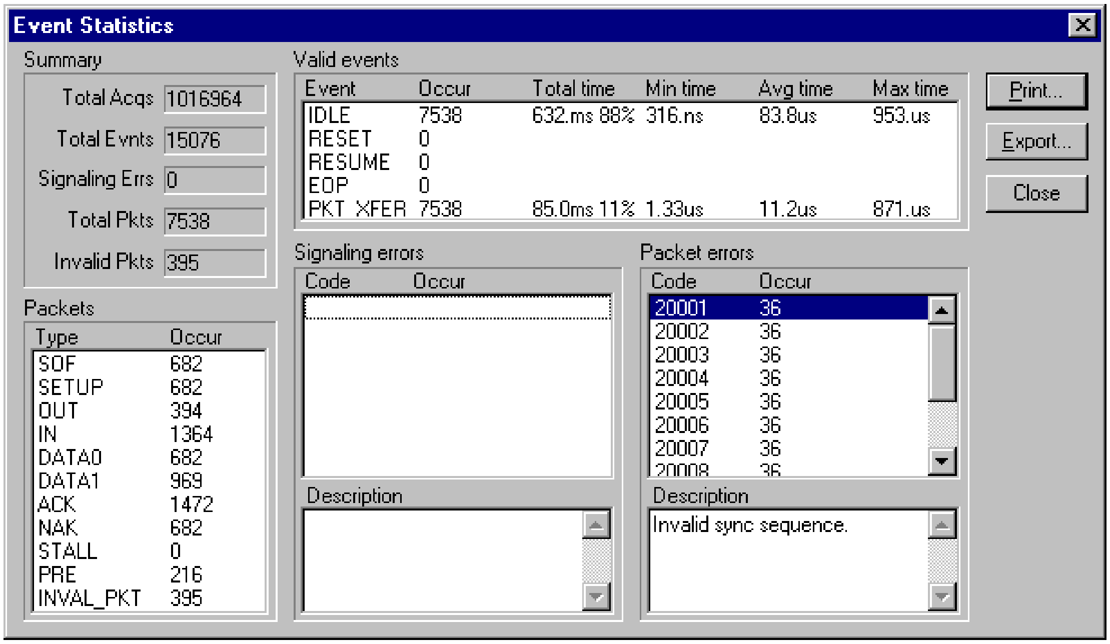
Event Statistics



Event Statistics command may be activated in any of the following ways:

- by typing ALT+R, then ALT+S, then ALT+E
- by clicking **Results** menu item, then **Statistics** command, then **Events** command.

When this command is activated, the program presents Event Statistics dialog containing the statistics data resulted from the Event Analysis of the last USB Process:



Summary

Total Acqs 1016964
Total Evnts 15076
Signaling Errs 0
Total Pkts 7538
Invalid Pkts 395

Valid events

Event	Occur	Total time	Min time	Avg time	Max time
IDLE	7538	632.ms 88%	316.ns	83.8us	953.us
RESET	0				
RESUME	0				
EOP	0				
PKT_XFER	7538	85.0ms 11%	1.33us	11.2us	871.us

Packets

Type	Occur
SOF	682
SETUP	682
OUT	394
IN	1364
DATA0	682
DATA1	969
ACK	1472
NAK	682
STALL	0
PRE	216
INVAL_PKT	395

Signaling errors

Code	Occur

Description

Packet errors

Code	Occur
20001	36
20002	36
20003	36
20004	36
20005	36
20006	36
20007	36
20008	36

Description

Invalid sync sequence.

This dialog presents statistics data resulted from Event Analysis if statistics were enabled before the start of USB Process.

The dialog contains the following controls:

- Summary group
- Valid Events list
- Packets list
- Signaling Errors group
- Packet Errors group
- Print button
- Export button
- Close button

Summary group indicates the summary of Event Analysis:
- total acquisitions
- total events
- signaling errors
- total packets
- invalid packets

Valid Events list presents global information on the following events:
- IDLE state
- RESET
- RESUME
- EOP (end of packet)
- PKT_XFER (packet transfer)

That global information refers to:
- number of event occurrences
- total time (accumulated, given in time value and percentage)
- min. time (the minimal event duration)
- average time (the average event duration)
- max. time (the maximal event duration)

Packets list presents the number of occurrences of each packet type and PRE (preamble).

Signaling Errors group contains an error list and a description box. The error list presents the number of occurrences of each signaling error which has been detected. The description box displays the description of the error type selected in the error list.

Packet Errors group contains an error list and a description box. The error list presents the number of occurrences of each packet error which has been detected. The description box displays the description of the error type selected in the error list.

Print button brings Print dialog box to allow the user to print Event Statistics.

Export button brings a file selection dialog to allow the user to save Event Statistics in an user defined file.

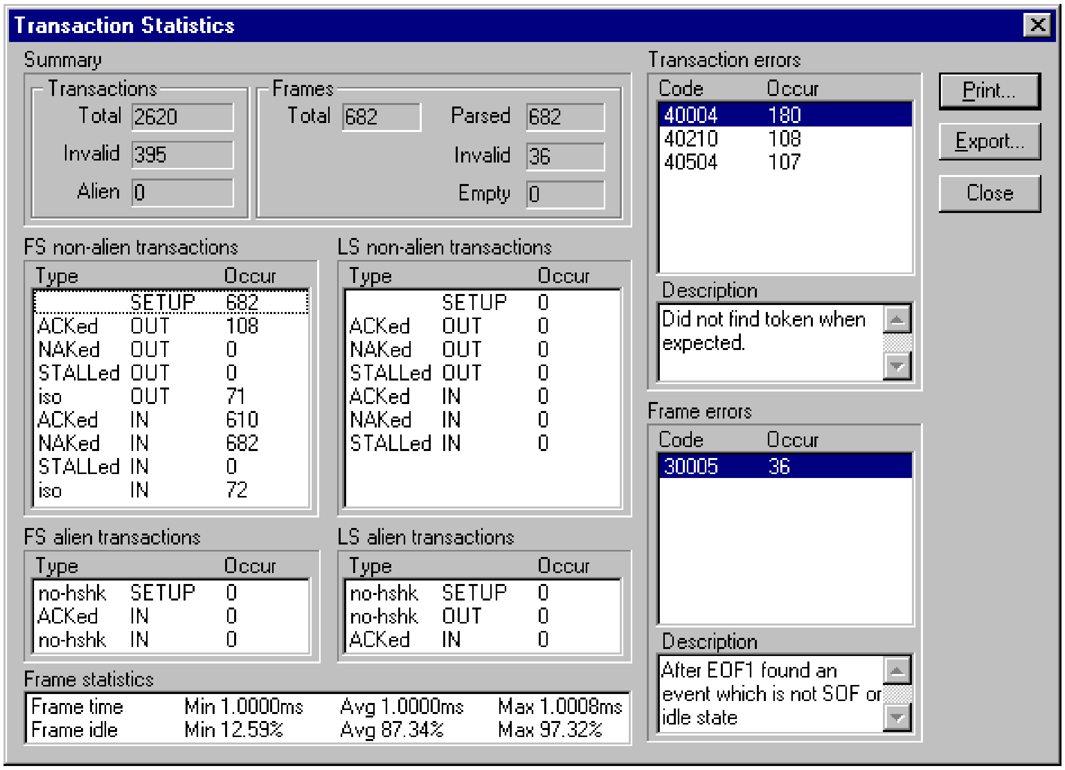
Close button is used to close Event Statistics dialog.

Transaction Statistics

Transaction Statistics command may be activated in any of the following ways:

- by typing ALT+R, then ALT+S, then ALT+T
- by clicking Results menu item, then Statistics command, then Events command.

When this command is activated, the program presents Transaction Statistics dialog containing the statistics data resulted from the Transaction Event Analysis of the last USB Process:



Summary

Transactions

Total	2620
Invalid	395
Alien	0

Frames

Total	682	Parsed	682
		Invalid	36
		Empty	0

FS non-alien transactions

Type		Occur
	SETUP	682
ACKed	OUT	108
NAKed	OUT	0
STALLed	OUT	0
iso	OUT	71
ACKed	IN	610
NAKed	IN	682
STALLed	IN	0
iso	IN	72

LS non-alien transactions

Type		Occur
	SETUP	0
ACKed	OUT	0
NAKed	OUT	0
STALLed	OUT	0
ACKed	IN	0
NAKed	IN	0
STALLed	IN	0

FS alien transactions

Type		Occur
no-hshk	SETUP	0
ACKed	IN	0
no-hshk	IN	0

LS alien transactions

Type		Occur
no-hshk	SETUP	0
no-hshk	OUT	0
ACKed	IN	0

Frame statistics

Frame time	Min 1.0000ms	Avg 1.0000ms	Max 1.0008ms
Frame idle	Min 12.59%	Avg 87.34%	Max 97.32%

Transaction errors

Code	Occur
40004	180
40210	108
40504	107

Description: Did not find token when expected.

Frame errors

Code	Occur
30005	36

Description: After EOF1 found an event which is not SOF or idle state

The dialog contains the following controls:

- Summary group
- FS non-alien transactions list
- LS non-alien transactions list
- FS alien transactions list
- LS alien transactions list
- Frame statistics box
- Transaction errors group
- Frame errors group
- Print button
- Export button
- Close button

Summary group indicates the summary of Transaction Analysis and Frame Analysis:

- total transactions (SETUP, OUT, IN, INVALID)
- invalid transactions
- alien transactions
- total frames (SOFs)
- parsed frames
- invalid frames
- empty frames

FS non-alien transactions list presents number of occurrences of FS non-alien transactions (for alien attribute refer to Alien Transactions):

- SETUP
- ACKed OUT
- NAKed OUT
- STALLed OUT
- iso OUT (FS OUT transaction without handshake)
- ACKed IN
- NAKed IN
- STALLed IN
- iso IN (FS IN transactions without handshake)

LS non-alien transactions list presents number of occurrences of LS non-alien transactions (for alien attribute refer to Alien Transactions):

- SETUP
- ACKed OUT
- NAKed OUT
- STALLed OUT
- ACKed IN
- NAKed IN
- STALLed IN

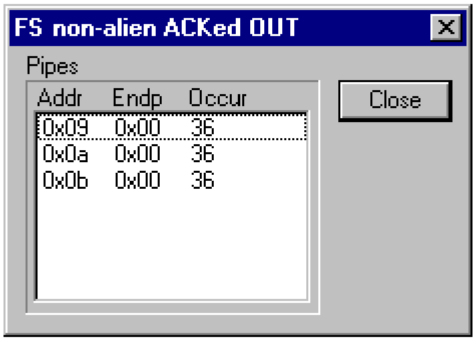
FS alien transactions list presents number of occurrences of FS alien transactions (for alien attribute refer to Alien Transactions):

- SETUP
- ACKed IN
- no-hshk IN (IN transaction without handshake)

LS alien transactions list presents number of occurrences of LS alien transactions (for alien attribute refer to Alien Transactions):

- SETUP
- no-hshk OUT (OUT transaction without handshake)
- ACKed IN

When double click a transaction in any of these lists, the program brings Transaction Statistics Details dialog:



FS non-alien ACKed OUT

Pipes

Addr	Endp	Occur
0x09	0x00	36
0x0a	0x00	36
0x0b	0x00	36

Frame statistics box displays the followings:

- minimal, average and maximal duration for valid frames
- minimal, average and maximal frame idle duration for valid frames

This information is available only if the capture has been made with Record Idle option ON during USB Process and Frame Analysis has been completed with statistics set ON.

Transaction Errors group contains an error list and a description box. The error list presents the number of occurrences of each transaction error which has been detected. The description box displays the description of the error type selected in the error list.

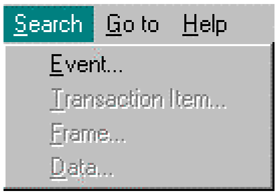
Frame errors group contains an error list and a description box. The error list presents the number of occurrences of each frame error which has been detected. The description box displays the description of the error type selected in the error list.

Print button brings Print dialog box to allow the user to print Event Statistics.

Export button brings a file selection dialog to allow the user to save Transaction Statistics in an user defined text file.

Close button is used to close Transaction Statistics dialog.

Search Menu



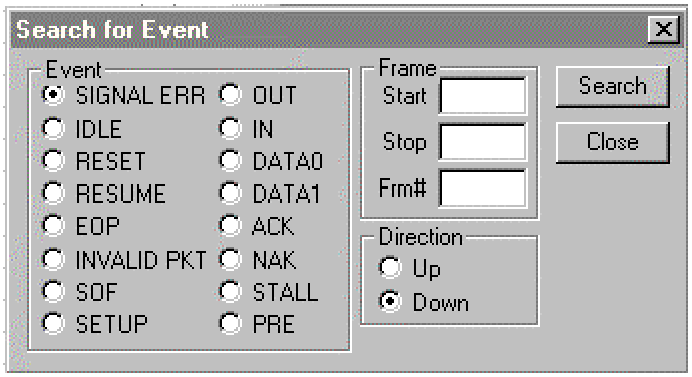
Event

Search Event command may be activated in any of the following ways:

- by typing ALT+S, then ALT+E
- by clicking Search menu item, then Event command.

The command is enabled on Event Layer only.

When this command is activated, the program presents Search Event dialog:



This dialog allows the user to specify the event to search for on Event Layer. It contains the following controls:

- Event group
- Frame group
- Direction group
- Search button
- Close button

Event group provides radio buttons for each event type to search for.

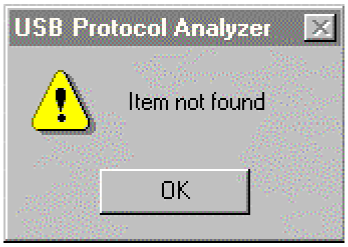
Frame group allows the user to specify the frame range for the search operation. It presents the following edit controls:

- Start, for specifying the count of the frame to start with. An empty control means that the search will start from the beginning of the traffic. The first SOF token corresponds to a count of 1.
- Stop, for specifying the count of the frame to stop after. An empty control means that the search will stop at the end of the traffic.

- Frm#, to indicate that the search will occur only in frames having this frame number. An empty control means that the search will occur in all frames specified by Start and Stop controls. Valid range for frame number is: 0x000..0x7ff.

Direction group allows the user to specify the search direction.

Search button starts the search. If the search is successful, the event cursor in Traffic window will be set on the event which has been found. Note that unfiltered traffic is displayed. If the search fails, the program displays the dialog presented below:



Item not found

Close button is used to close this dialog.

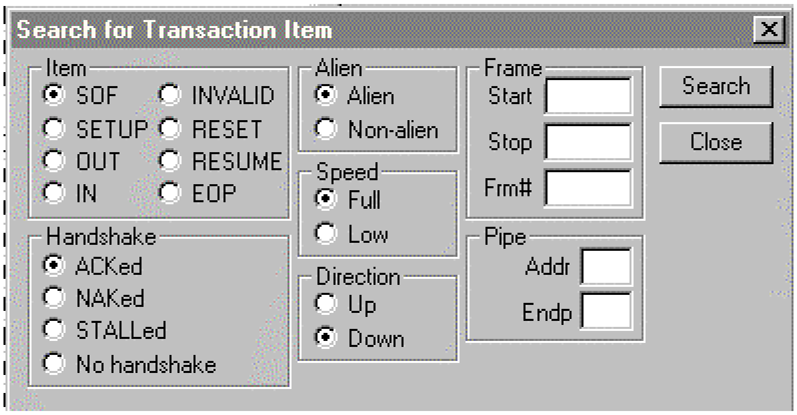
Transaction Item

Search Transaction Item command may be activated in any of the following ways:

- by typing ALT+S, then ALT+T
- by clicking Search menu item, then Transaction Item command.

The command is enabled on Transaction Layer only.

When this command is activated, the program presents Search Transaction Item dialog:



Item
● SOF ○ INVALID
○ SETUP ○ RESET
○ OUT ○ RESUME
○ IN ○ EOP

Handshake
● ACKed
○ NAKed
○ STALLed
○ No handshake

Alien
● Alien
○ Non-alien

Speed
● Full
○ Low

Direction
○ Up
● Down

Frame
Start
Stop
Frm#

Pipe
Addr
Endp

This dialog allows the user to specify the transaction to search for on Transaction Layer. It contains the following controls:

- Item group
- Handshake group
- Alien group
- Speed group
- Pipe group
- Frame group
- Direction group

- **Search** button
- **Close** button

Item group allows the user to specify the transaction item to search for. Transaction items mean not only transactions (SETUP, OUT, IN, INVALID), but SOF tokens, RESET, RESUME, and standalone EOP whose display in Traffic window may be desired.

Handshake group allows the user to specify the type of the handshake packet when the item to search for indicates an OUT or IN transaction.

Alien group allows the user to specify the alien attribute (refer to Alien Transactions). That is applicable when the item to search for indicates a SETUP, OUT or IN transaction, and on non-root bus only.

Speed group allows the user to specify the transaction speed when the item to search for indicates a SETUP, OUT or IN transaction This is applicable for traffic captured on FS bus only.

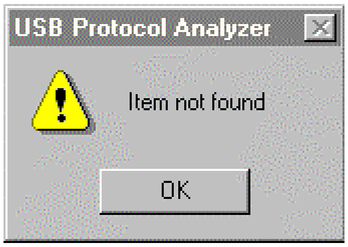
Pipe group allows the user to specify the pipe address and endpoint when the item to search for indicates a SETUP, OUT or IN transaction. The pipe is specified in **Addr** and **Endp** edit controls. The valid range for pipe address is: 0x00..0x7f. The valid range for the pipe endpoint is: x00..0x0f. An empty control is a wild card for that parameter. For example and empty **Endp** edit control will not restrict the search to for a specific endpoint.

Frame group allows the user to specify the frame range for the search operation. It presents the following edit controls:

- **Start**, for specifying the count of the frame to start with. An empty control means that the search will start from the beginning of the traffic. The first SOF token corresponds to a count of 1.
- **Stop**, for specifying the count of the frame to stop after. An empty control means that the search will stop at the end of the traffic.
- **Frm#**, to indicate that the search will occur only in frames having this frame number. An empty control means that the search will occur in all frames specified by **Start** and **Stop** controls. Valid range for frame number is: 0x000..0x7ff.

Direction group allows the user to specify the search direction.

Search button starts the search. If the search is successful, the transaction cursor in Traffic window will be set on the transaction item which has been found. Otherwise the program displays the dialog presented below:



Item not found

Close button is used to close this dialog.

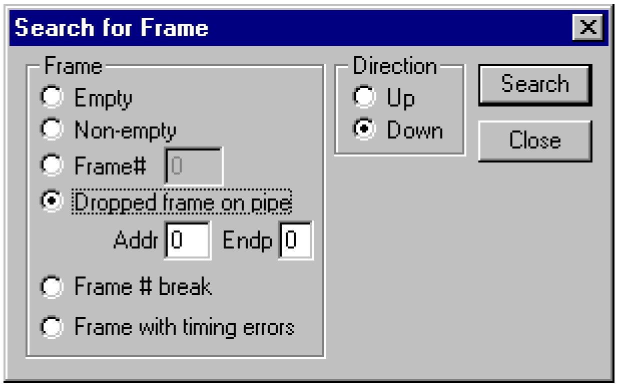
Frame

Search Frame command may be activated in any of the following ways:

- by typing ALT+S, then ALT+F
- by clicking Search menu item, then Frame command.

The command is enabled on Transaction Layer only.

When this command is activated, the program presents Search Frame dialog:



Search for Frame

Frame
○ Empty
○ Non-empty
○ Frame# 0
● Dropped frame on pipe
Addr 0 Endp 0
○ Frame # break
○ Frame with timing errors

Direction
○ Up
● Down

This dialog allows the user to specify the frame to search for on Transaction Layer. It contains the following controls:

- Frame group
- Direction group
- Search button
- Close button

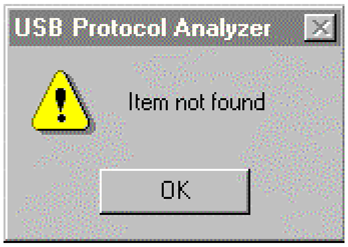
Frame group allows the user to specify the type of the frame to search for. It presents the following edit controls:

- Empty radio button, for specifying the search for an empty frame. That means that the SOF token of that frame is followed by idle state, then the SOF token of the next frame
- Non-empty, for specifying the search for a non-empty frame.
- Frame# radio button and edit control, for specifying the number of the frame to search for. Valid range for frame number is: 0x000..0x7ff.
- Dropped frame on pipe radio button, with Addr and Endp edit controls. This option allows the user to specify the search for a frame which does not provide a transfer on the pipe specified in Addr and Endp edit controls. If the frame traffic is broken by RESET or RESUME the search will place the transaction cursor on that item. The valid range for pipe address is: 0x00..0x7f. The valid range for the pipe endpoint is: x00..0x0f.
- Frame # break radio button, for specifying the search for a frame presenting a break in the frame #. That means one of the following situations: either the previous frame has a frame # within the range 0x000..0x7fe, and the frame # of the current frame is not the frame # of the previous frame plus one, or the previous frame has a frame # of 0x7ff and the frame # of the current frame is not 0x000
- Frame with timing errors radio button, for specifying the search for a frame with invalid timing (refer to

Frame Errors)

Direction group allows the user to specify the search direction.

Search button starts the search. If the search is successful, the transaction cursor in Traffic window will be set on the transaction item which has been found. Note that unfiltered traffic is displayed. If the search fails, the program displays the dialog presented below:



Item not found

Close button is used to close this dialog.

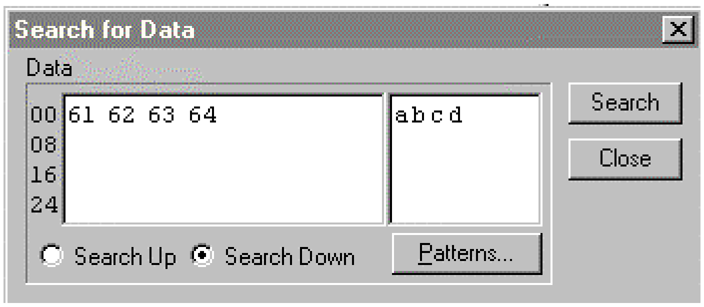
Data

Search Data command may be activated in any of the following ways:

- by typing ALT+S, then ALT+D
- by clicking Search menu item, then Data command.

The command is enabled on Data Layer only.

When this command is activated, the program presents Search Data dialog:



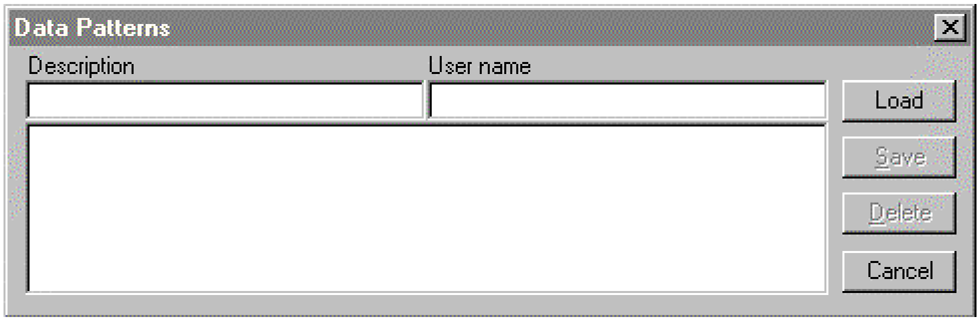
61 62 63 64

abcd

This dialog allows the user to enter binary string to search for in the data presented on Data Layer. That string is limited to 32 bytes. The dialog has the following controls:

- the box of the hex representation
- the box of the ASCII representation
- Search Up radio button, pressed for searching up
- Search Down radio button, pressed for searching down
- Patterns button, to bring Data Patterns dialog
- Search button, to start the search
- Close button, to close this dialog

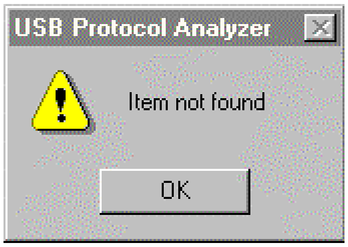
Data Patterns dialog is presented below:



This dialog contains the following controls:

- Load button to allow the user to load a previously saved binary string
- Save button to allow the user to save the binary string presented in the dialog
- Delete button to allow the user to delete a previously saved binary string
- Cancel button to cancel the operation

If the search is successful, the byte cursor is placed on the first byte in the string which has been found. Otherwise the program displays the dialog presented below:

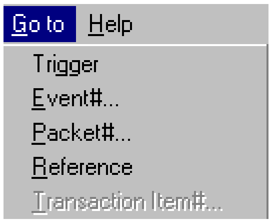


Item not found

Close button is used to close this dialog.

Goto Menu

Goto commands may be used to get to traffic items referred in analysis reports.



Goto Trigger

Go to Trigger command may be activated in any of the following ways:

- by typing ALT+G, then ALT+G
- by clicking Go to menu item, then Trigger command.

The command is enabled on Event Layer only.

When this command is activated, the program places the event cursor on the event the capture has triggered on.

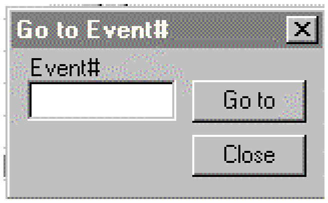
Goto Event

Go to Event command may be activated in any of the following ways:

- by typing ALT+G, then ALT+E
- by clicking Go to menu item, then Event command.

The command is enabled on Event Layer only and allows to get to the events referred in Event Analysis report.

When this command is activated, the program presents Goto Event dialog:



The user has to enter the event number in Event# control and press Goto button. As result, the event cursor will be placed on that event. Note that after the execution of a goto command, the program presents unfiltered traffic.

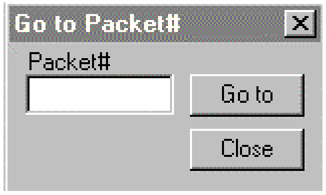
Goto Packet

Go to Packet command may be activated in any of the following ways:

- by typing ALT+G, then ALT+P
- by clicking Go to menu item, then Packet command.

The command is enabled on Event Layer only and allows to get to the packets referred in Packet Analysis report.

When this command is activated, the program presents Goto Packet dialog:



The user has to enter the packet number in Packet# control and press Goto button. As result, the event cursor will be placed on that packet. Note that after the execution of a goto command, the program presents unfiltered traffic.

Goto Reference

Go to Reference command may be activated in any of the following ways:

- by typing ALT+G, then ALT+R
- by clicking Go to menu item, then Reference command.

The command is enabled on Event Layer only.

When this command is activated, the program places the event cursor on the event set for reference. Refer to Event Time Information for setting an event reference.

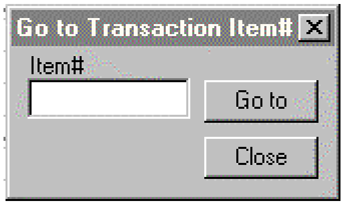
Goto Transaction Item

Go to Transaction command may be activated in any of the following ways:

- by typing ALT+G, then ALT+T
- by clicking Go to menu item, then Transaction command.

The command is enabled on Transaction Layer only and allows to get to the transaction items referred in Transaction Analysis report or Frame Analysis report.

When this command is activated, the program presents



The user has to enter the transaction item number in Item# control and press Goto button. As result, the transaction cursor will be placed on that transaction item. Note that after the execution of a goto command, the program presents unfiltered traffic.

Event Traffic

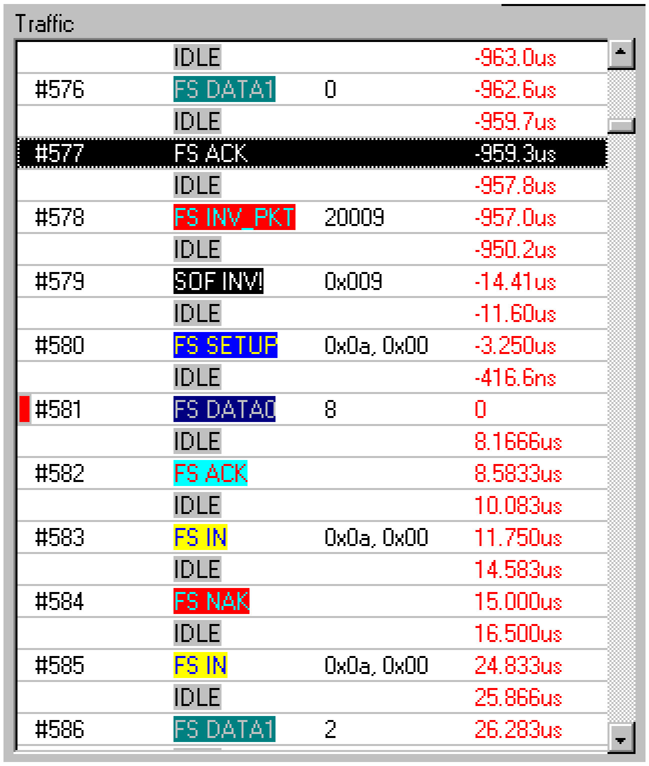
Event Layer

This layer presents the USB traffic in terms of USB events. It contains the following controls:

- the layer tab which may be clicked to switch on this layer
- Traffic window
- Details window
- Bit Stream window
- Display options group

Also the Traffic Information bar and the Status bar are available as on any other traffic layer.

Traffic Window



	IDLE		-963.0us
#576	FS DATA1	0	-962.6us
	IDLE		-959.7us
#577	FS ACK		-959.3us
	IDLE		-957.8us
#578	FS INV_PKT	20009	-957.0us
	IDLE		-950.2us
#579	SOF INV!	0x009	-14.41us
	IDLE		-11.60us
#580	FS SETUP	0x0a, 0x00	-3.250us
	IDLE		-416.6ns
#581	FS DATA0	8	0
	IDLE		8.1666us
#582	FS ACK		8.5833us
	IDLE		10.083us
#583	FS IN	0x0a, 0x00	11.750us
	IDLE		14.583us
#584	FS NAK		15.000us
	IDLE		16.500us
#585	FS IN	0x0a, 0x00	24.833us
	IDLE		25.866us
#586	FS DATA1	2	26.283us

This window presents a list of event prompts corresponding to a part of the USB traffic. The following USB events may be shown:

- SIGNAL ERR
- IDLE
- RESET
- EOP
- RESUME
- packet transfer, specified by the packet type: INVALID PKT, SOF, SETUP, IN, OUT, DATA0, DATA1, ACK, NAK, STALL, PRE.

SIGNAL ERR event is defined as a non-compliance in USB signaling, other than USB packet signaling. Such non-compliances may be: K state follows SE0 state, invalid EOP (too long, too short), invalid RESET (too short), etc. Refer to Signaling Errors for the complete list of these errors whose detection is implemented in the program.

IDLE event is defined as J state, detected in other situations than packet transfer. Example: after EOP, after RESET, after RESUME, etc. J state seen in the middle of a packet transfer is not IDLE event.

RESET event is defined as the SE0 state for at least 10ms.

RESUME event is defined as K state for at least 20ms, followed by LS EOP (low speed end of packet).

EOP event is defined as an end of packet signaling which does not follow a packet transfer. Such EOPs may be seen on a low speed bus (provided by the upstream hub).

INVALID PKT event is a packet presenting a format error: invalid sync, bit stuff error, CRC error, etc..

SOF event is the start of frame packet. If frame analysis has been performed within the USB Process, then frames with invalid timing are signaled by using SOF INV!.

SETUP event is SETUP token packet.

IN event is IN token packet.

OUT event is OUT token packet.

DATA0 event is DATA0 data packet.

DATA1 event is DATA1 data packet.

ACK event is ACK handshake packet

NAK event is NAK handshake packet

STALL event is STALL handshake packet.

PRE event is PRE (preamble) packet.

For each event which has been detected, the event traffic window presents an event prompt (refer to Event Prompts.

If the number of max. errors for Packet Analysis specified in Resume USB Process dialog or New USB Process dialog is reached during the USB Process, then the traffic may end with UNDECODED PKT items.

Event Prompts

The event prompt depends on the event type:

- SIGNAL ERR: name, error code
- IDLE: name, duration in FS bit times. If the USB Process had record idle option OFF, the duration of IDLE event is not relevant being indicated by: >=22 (the capture device truncates the duration of idle times to 22 FS bit times).
- RESET: name, duration in FS bit times.
- EOP: name, duration in FS bit times.
- RESUME: name, duration in FS bit times.
- INVALID PKT: name, error code and duration in FS bit times.
- SOF: packet#, name, frame number, duration in FS bit times. If frame analysis has been performed within the USB Process, then frames with invalid timing are signaled by using SOF INV! prompt.
- SETUP: packet#, speed, name, address, endpoint, duration in FS bit times
- IN: packet#, speed, name, address, endpoint, duration in FS bit times
- OUT: packet#, speed, name, address, endpoint, duration in FS bit times

- DATA0: packet#, name, speed, data payload, duration in FS bit times
- DATA1: packet#, name, speed, data payload, duration in FS bit times
- ACK: packet#, name, speed, duration in FS bit times
- NAK: packet#, name, speed, duration in FS bit times
- STALL: packet#, name, speed, duration in FS bit times
- PRE: packet#, name, speed, duration in FS bit times (despite PRE is not a packet it has assigned packet#)

The event speed (when applicable) is specified by FS (full speed) or LS (low speed).

The event prompt displays on the last position the timing information as chosen in Event time information dialog:
- event duration in FS bit times,
- event duration in time units
- event position relative to trigger
- event position relative to start
- event position relative to reference

The event duration is displayed in black on white, between brackets.

The position relative to trigger is displayed in the color chosen for the trigger marker in Event traffic colors dialog.

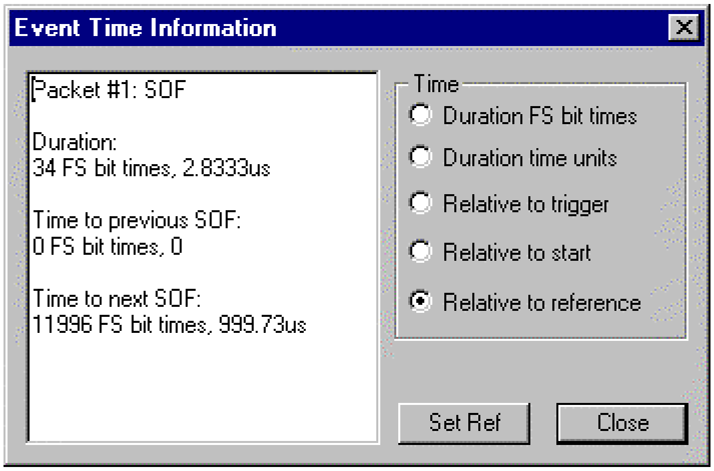
The position relative to start is displayed in black on white.

The position relative to start is displayed in the color chosen for the reference marker in Event traffic colors dialog.

The event traffic may be submitted to the traffic filter as indicated in Display options on Event Layer.

Event Time Information

Time information is available for each item of event traffic. That information may be brought either by clicking the desired item with the right mouse button, or by selecting the item with the arrow keys and then pressing the SPACE bar. At that moment the program opens Event Time Information dialog:



Packet #1: SOF

Duration:
34 FS bit times, 2.8333us

Time to previous SOF:
0 FS bit times, 0

Time to next SOF:
11996 FS bit times, 999.73us

Time
○ Duration FS bit times
○ Duration time units
○ Relative to trigger
○ Relative to start
● Relative to reference

This dialog allows the user to perform the followings:

- get the event position with respect to the previous and the next SOF token.
- choose the timing information which is displayed on the last column of the Traffic window of the Event Layer
- set the reference on the event which has been selected with the right mouse button before getting this dialog

The event position is presented in FS bit times and real time units.

The timing information may be:

- event duration in FS bit times, when Duration FS bit times radio button is pressed
- event duration in real time units, when Duration time units radio button is pressed
- the position of the selected event with respect to the trigger event, when Relative to trigger radio button is pressed
- the position of the selected event with respect to the first event, when Relative to start radio button is pressed
- the position of the selected event with respect to the event reference , when Relative to reference radio button is pressed

The event duration is displayed in black on white, between brackets.

The position relative to trigger is displayed in the color chosen for the trigger marker in Event traffic colors dialog.

The position relative to start is displayed in black on white.

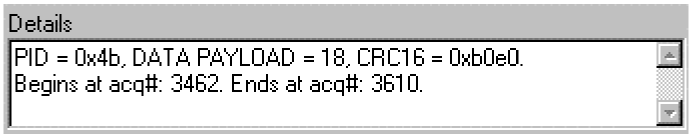
The position relative to start is displayed in the color chosen for the reference marker in Event traffic colors dialog.

In this dialog the user may set the reference on the event selected with the right mouse button before opening the dialog by pressing Set Ref button.

When Close button is pressed, the Traffic window is redisplayed to reflect the new options.

The timing information is available only if the capture has been performed with Record Idle option ON. Otherwise only event duration is presented for events other than IDLE.

Details Window

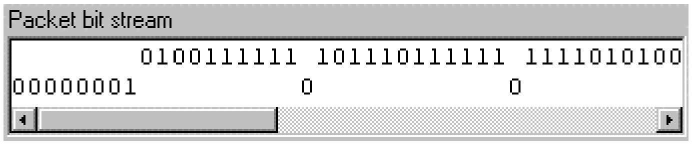


PID = 0x4b, DATA PAYLOAD = 18, CRC16 = 0xb0e0.
Begins at acq#: 3462. Ends at acq#: 3610.

This is a text box displaying details on the event selected in Traffic window. Event details depend on the event type:

- SIGNAL ERR: error code, duration, the number of the first event acquisition, the number of the last event acquisition, error description
- IDLE: duration, the number of the first event acquisition, the number of the last event acquisition. If the USB Process had record idle option OFF, the duration of IDLE event is not relevant being indicated by >= (the capture device truncates the duration of idle times to 22 FS bit times).
- RESET: duration, the number of the first event acquisition, the number of the last event acquisition.
- EOP: duration, the number of the first event acquisition, the number of the last event acquisition.
- RESUME: duration, the number of the first event acquisition, the number of the last event acquisition .
- INVALID PKT: error code, the number of the first event acquisition, the number of the last event acquisition, error description
- SOF: PID, frame number, CRC5, the number of the first event acquisition, the number of the last event acquisition. If frame analysis has been performed within the USB Process , then frames with invalid timing are signaled by using SOF INV!. In such a case the Details window presents the description of the frame timing failure.
- SETUP: PID, address, endpoint, CRC5, the number of the first event acquisition, the number of the last event acquisition
- IN: PID, address, endpoint, CRC5, the number of the first event acquisition, the number of the last event acquisition
- OUT: PID, address, endpoint, CRC5, the number of the first event acquisition, the number of the last event acquisition
- DATA0: PID, data payload, CRC16, the number of the first event acquisition, the number of the last event acquisition
- DATA1: PID, data payload, CRC16, the number of the first event acquisition, the number of the last event acquisition
- ACK: PID, the number of the first event acquisition, the number of the last event acquisition
- NAK: PID, the number of the first event acquisition, the number of the last event acquisition
- STALL: PID, the number of the first event acquisition, the number of the last event acquisition
- PRE: PID, the number of the first event acquisition, the number of the last event acquisition

Bit Stream Window


Packet bit stream

```
         0100111111 101110111111 1111010100
00000001            0            0
```

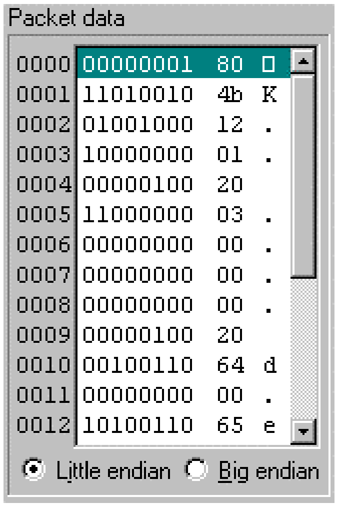
This window presents the packet bit stream, when the event cursor selects a invalid packet which has not been decoded.

Sync bits and stuffed bits are presented on the lower row of that window, while the data bits are presented on the higher row.

If the packet is invalid because has a sync error or a bit stuff error, the bit stream decoding stops at the place where the error is detected.

If the currently selected event in Traffic window is a decoded packet (that means a valid packet or a packet presenting a CRC error), the Bit Stream window stays empty.

Packet Data Window


Packet data

```
0000 00000001  80  □
0001 11010010  4b  K
0002 01001000  12  .
0003 10000000  01  .
0004 00000100  20
0005 11000000  03  .
0006 00000000  00  .
0007 00000000  00  .
0008 00000000  00  .
0009 00000100  20
0010 00100110  64  d
0011 00000000  00  .
0012 10100110  65  e
```

● Little endian ○ Big endian

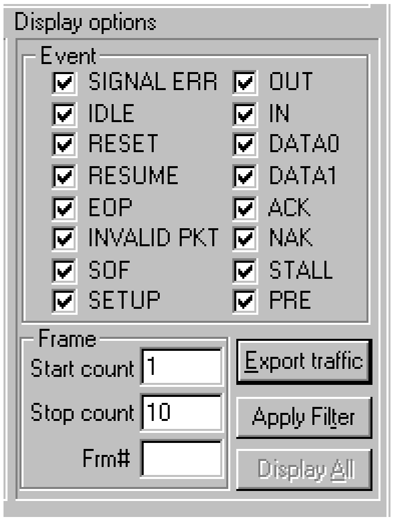
This window presents the body of a decoded packet, i.e. a packet having correct sync and stuffed bits. Sync, PID, and CRC are included. The packet body indicates the CRC, regardless if CRC is correct or not.

The packet body is represented in binary, hex, and ASCII. The binary representation may use little or big endian order, if Little endian, respectively Big endian radio button is pressed.

The packet data window presents a byte cursor. If the packet is decoded, the user may select any byte. The number of that byte will be indicated in Evnt byte# field of the Status bar. When the first byte is selected, the that field displays zero.

If the packet is not decoded as result of an error detected in sync sequence or in bit stuffing, then packet data window stays empty, and the bit stream window shows the packet bit stream up to the point where the error has been detected.

Display Options



Display options

Event

☑ SIGNAL ERR ☑ OUT
☑ IDLE ☑ IN
☑ RESET ☑ DATA0
☑ RESUME ☑ DATA1
☑ EOP ☑ ACK
☑ INVALID PKT ☑ NAK
☑ SOF ☑ STALL
☑ SETUP ☑ PRE

Frame

Start count: 1
Stop count: 10
Frm#:

Display options allow the user to specify the events to be displayed in Traffic window. The following controls are available for display options:

- Event group
- Frame group
- Display All button
- Apply Filter button
- Export Traffic button

Event group allows the user to specify the events to be displayed in the filtered traffic. Each event has assigned a check box . Event selection options are ORed. For example if EOP and IDLE check boxes are on, then EOP and IDLE events will be displayed.

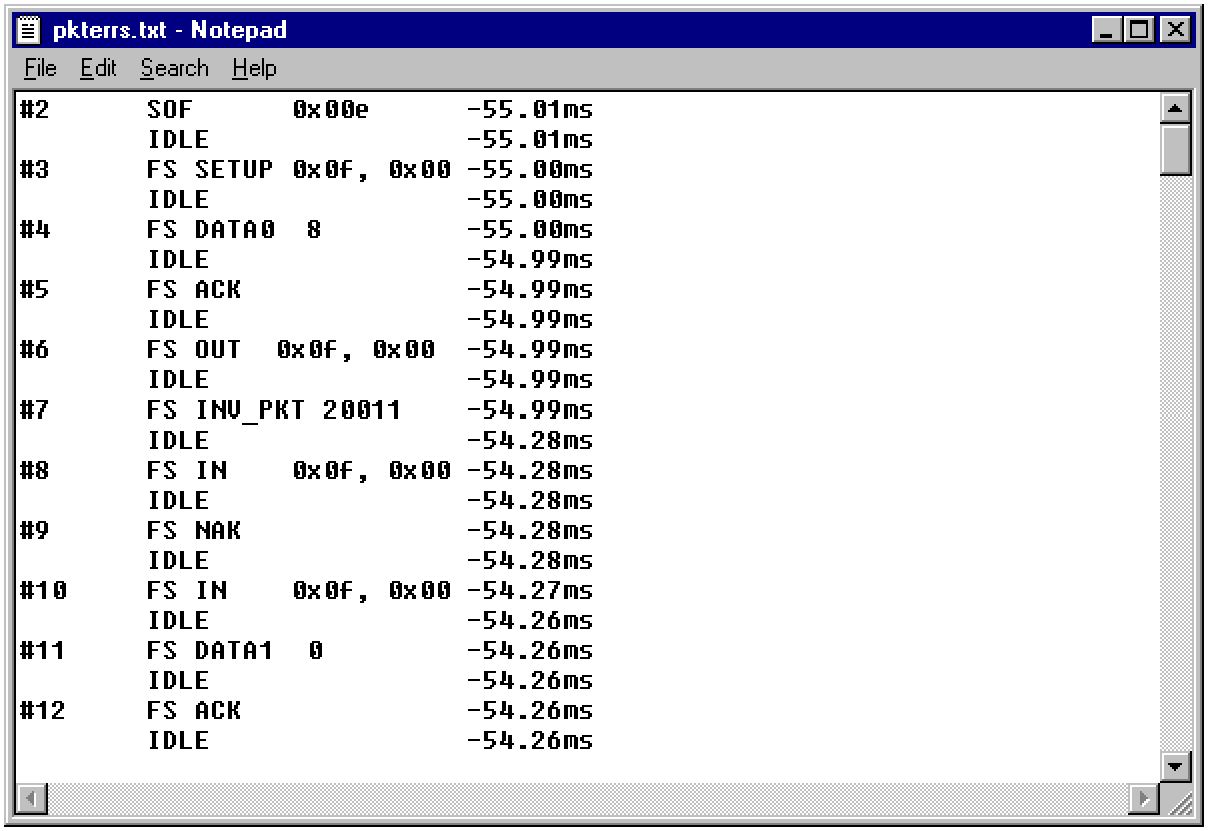
Frame group allows the user to specify the frame range for event display. It presents the following edit controls:

- Start, for specifying the count of the frame to start with. An empty control means that the display will start from the beginning of the traffic. The first SOF token corresponds to a count of 1.
- Stop, for specifying the count of the frame to stop after. An empty control means that the display will stop at the end of the traffic.
- Frm#, to indicate that the program will display traffic of frames having this frame number. An empty control means that the program will display traffic of all frames between those specified by Start and Stop controls. Valid range for frame number is: 0x000..0x7ff.

These options are ANDed between them, and ANDed with event selection options. For example if start count is 500, and stop count is 900, and frame# is 0x10a, then the event traffic will present events detected in a frame having frame# of 0x10a and being somewhere between frame 500 and frame 900 (in the same capture there may be different frames having the same frame#, if the captured traffic contains more than 2000 frames). If one field of the frame selection is empty, that is considered wild card. For example if frame# is empty, the event traffic will present events detected in all frames between 500 and 900 which are enabled by other display options. Frame selection options are applicable for the traffic captured on FS bus only

Display options have available two buttons: Display All, and Apply Filter. When the first button is pressed, the event traffic window will display all events around the event cursor. When Apply Filter button is pressed, the event traffic window will display events selected according to display options. If the current event is enabled by display filter, the traffic focus is preserved after pressing Apply Filter. Otherwise the event cursor will be set on the closest event enabled by display filter.

Export Traffic button allows the user to save the filtered traffic in a user defined text file. The traffic format in that file is similar to the traffic displayed in Traffic window:



```
#2       SOF       0x00e      -55.01ms
         IDLE                 -55.01ms
#3       FS SETUP  0x0f, 0x00 -55.00ms
         IDLE                 -55.00ms
#4       FS DATA0   8         -55.00ms
         IDLE                 -54.99ms
#5       FS ACK               -54.99ms
         IDLE                 -54.99ms
#6       FS OUT   0x0f, 0x00  -54.99ms
         IDLE                 -54.99ms
#7       FS INV_PKT 20011     -54.99ms
         IDLE                 -54.28ms
#8       FS IN     0x0f, 0x00 -54.28ms
         IDLE                 -54.28ms
#9       FS NAK               -54.28ms
         IDLE                 -54.28ms
#10      FS IN     0x0f, 0x00 -54.27ms
         IDLE                 -54.26ms
#11      FS DATA1   0         -54.26ms
         IDLE                 -54.26ms
#12      FS ACK               -54.26ms
         IDLE                 -54.26ms
```

Up to 1000 traffic items may be exported. This command allows the user to save the filtered traffic in a text file. That file may be loaded, viewed and printed with a text utility (as NotePad for example). If the traffic has not been filtered yet, the program will prompt a warning:

The picture below presents the filtered event traffic when SIGNAL ERR and INVALID PKT have been checked:

Traffic Focus on Event Layer

The traffic focus is indicated by the following read only controls provided by Status bar:

- Frm count
- Frm#
- Evnt#
- Evnt byte#

Frm count indicates the count of the frame containing the current traffic item. The first frame has a count of 1. If the traffic has been captured on a low speed bus, or it is not preceded by any SOF, that control stays empty.

Frm# indicates the number of the frame containing the current traffic item. If the traffic has been captured on a low speed bus, or it is not preceded by any SOF, that control stays empty.

Evnt# indicates the number of the event the traffic focus is selecting. On Event Layer this control indicates the number of the selected event.

Evnt byte# indicates the number of the byte transferred in the event indicated in Evnt# control. The first byte in the packet (the sync byte) has a # of zero. If no data bytes have been transferred in that event, this control stays empty. That means the current event is not a packet transfer, or it is an undecoded packet (it presents a wrong sync byte, or bit stuffing error, or it is a truncated packet).

The traffic focus information helps the user to check that it stays in the same place of the traffic when filtering or switching between traffic layers.

Switching on Transaction Layer

Switching from events to transactions is possible regardless of the currently selected event. It may be performed in any of the following ways:

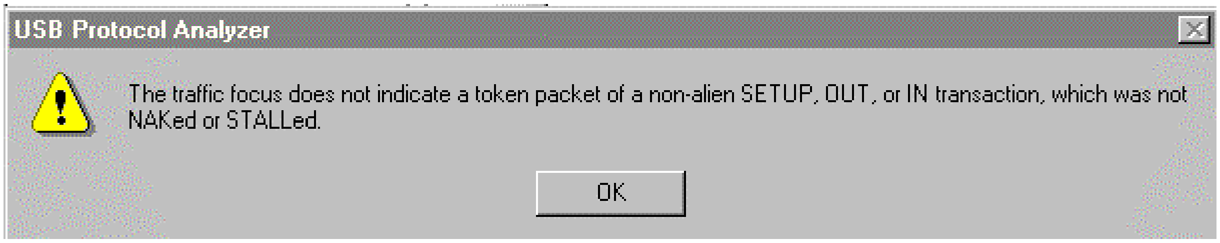
- click the tab of Transaction Layer
- press `F3`
- press `CTRL+TAB`

At that moment the screen will present the Transaction Layer. The traffic focus is preserved if the currently selected event was a data packet. Otherwise the traffic focus is slightly changed in order to indicate the data packet of the currently selected transaction.

Note that when entering the Transaction Layer, the program presents unfiltered traffic.

Switching on Data Layer

Switching from events to data is possible only if the currently selected event in Traffic window is an event which is part of a SETUP, OUT, or IN non-alien transaction, alien transaction which was not NAKed or STALLed. Otherwise the program displays the message presented below:



The traffic focus does not indicate a token packet of a non-alien SETUP, OUT, or IN transaction, which was not NAKed or STALLed.

The reason for this restriction is the program needs to know the pipe whose data traffic must be presented. If the transaction is alien (refer to Alien Transactions), it means that the pipe does not go through the bus branch where the USB Probe is installed. If the transaction has been NAKed or STALLed it means the data did no go through, therefore should not be presented as being transferred.

Switching from events to data may be performed in any of the following ways:

- click the tab of Data Layer
- press `F4`
- press `CTRL+SHIFT+TAB`

Transaction Traffic

Transaction Layer

This layer presents the USB traffic in terms of transaction items. It contains the following controls:

- the layer tab which may be clicked to switch on this layer
- Traffic window
- Details window
- Data Packet window
- Display options group

Also the Traffic Information bar and the Status bar are available as on any other traffic layer.

Traffic Window

This window presents a list of transaction item prompts corresponding to a part of the USB traffic. The following transaction items may be shown:

- SOF
- SETUP
- OUT
- IN
- RESET
- EOP
- RESUME
- INVALID

SOF is the start of frame token. It is not a transaction, but it is important to present the frame markers in the traffic. If frame analysis has been performed within the USB Process, then frames with invalid timing are signaled by using SOF INV!.

SETUP is the SETUP transaction.
OUT is the OUT transaction.
IN is the IN transaction.

RESET event is defined as the SE0 state for at least 10ms.

RESUME event is defined as K state for at least 20ms, followed by LS EOP (low speed end of packet).

EOP event is defined as an end of packet signaling which does not follow a packet transfer. Such EOPs may be seen on a low speed bus (provided by the upstream hub).

INVALID is an invalid transaction. (refer to

Transaction Errors).

RESET, RESUME, EOP are not transactions, but may affect the transaction flow, and for this reason the display of these traffic items is allowed in the Traffic window of Transaction Layer.

For each transaction item which has been detected, the Traffic window presents a transaction prompt (refer to Transaction Prompts).

Transaction Prompts

The prompt of the transaction item depends of the item type:

- SOF: transaction item#, name, frame number. If frame analysis has been performed within the USB Process, then frames with invalid timing are signaled by using SOF INV!.
- SETUP: speed, alien attribute (refer to Alien Transactions), name, address, endpoint, type of data packet, handshake packet
- OUT: speed, alien attribute (refer to Alien Transactions), name, address, endpoint, type of data packet, handshake packet
- IN: speed, alien attribute (refer to Alien Transactions), name, address, endpoint, type of data packet, handshake packet
- RESET: name
- EOP: speed, name
- RESUME: name
- INVALID: error code

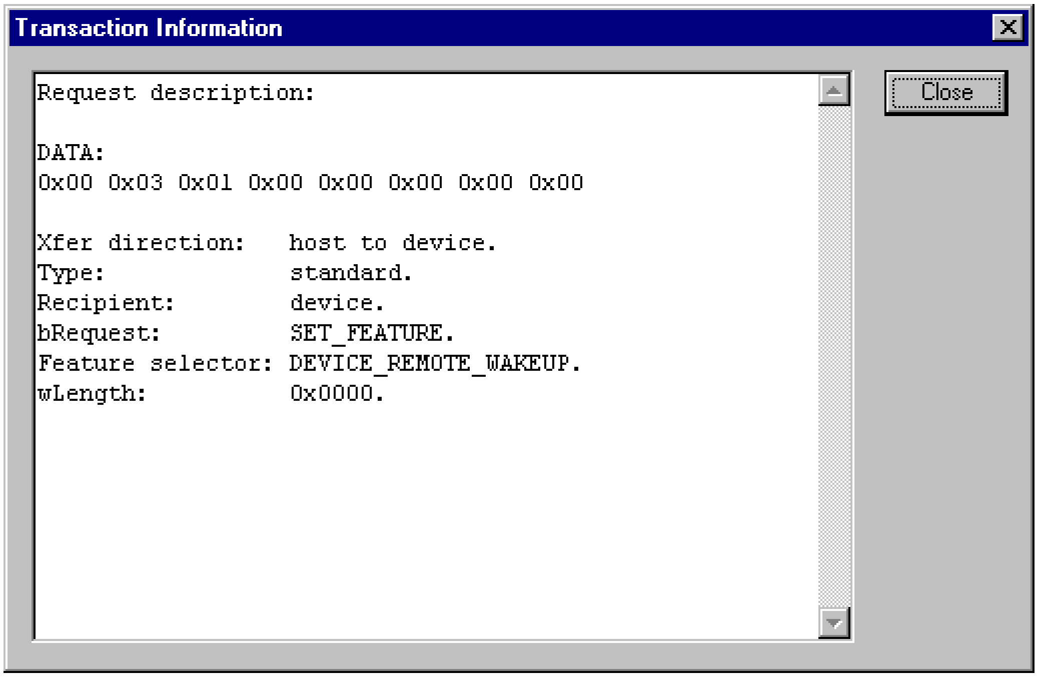
For SETUP, OUT and IN transactions, the speed and alien attribute are presented in a single prefix: FS stands for “full speed non alien”, FSA stands for “full speed alien”, LS stands for “low speed non alien”, LSA stands for “low speed alien”.

Decoding Standard Requests

To decode standard requests on Transaction Layer, the user may proceed in any of the following two ways:

- click the SETUP transaction with the right mouse button
- select that transaction and press SPACE bar

At that moment the program will bring Transaction Information dialog:

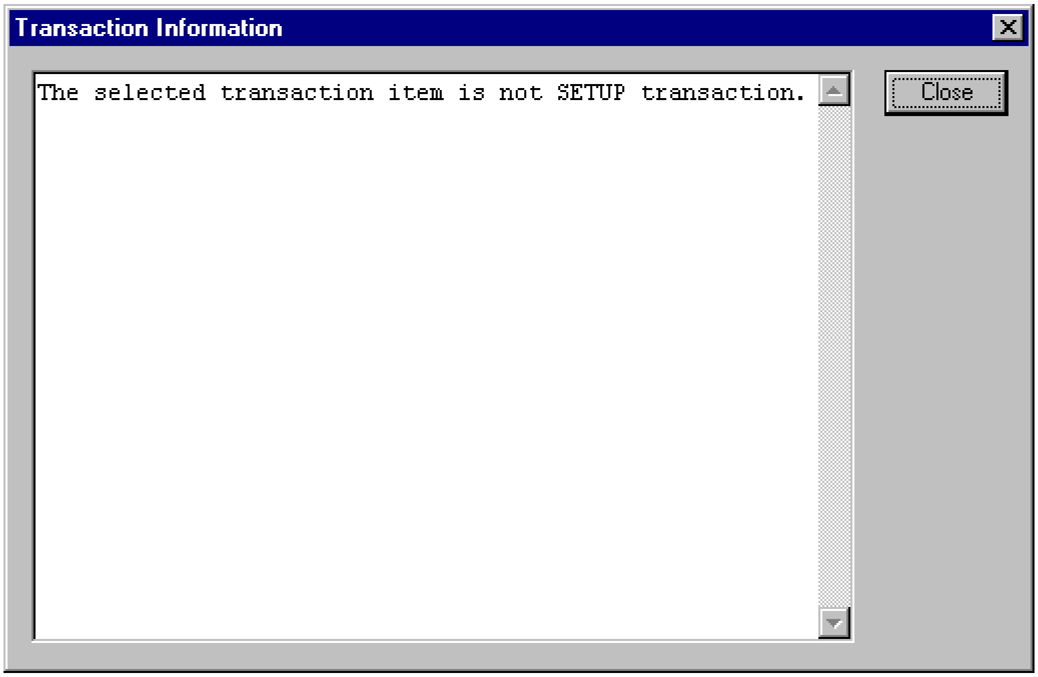


```
Request description:

DATA:
0x00 0x03 0x01 0x00 0x00 0x00 0x00 0x00

Xfer direction:   host to device.
Type:             standard.
Recipient:        device.
bRequest:         SET_FEATURE.
Feature selector: DEVICE_REMOTE_WAKEUP.
wLength:          0x0000.
```

This dialog presents additional information for some transaction traffic items. This version of the program provides additional transaction information for SETUP transactions which perform standard requests.

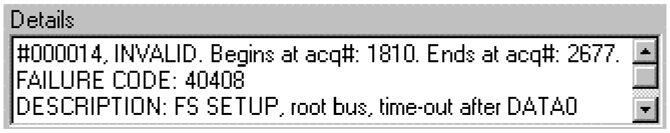
The request made by the USB Host and is presented as a string of bytes. The program maps the request bytes on the format indicated in the USB Specification. If the a standard request generates input transfers (for example descriptors), the program will present that input data both in hex and in the format indicated in USB Specification.

For transaction items which are not a SETUP transactions, the dialog will display no additional information:



The selected transaction item is not SETUP transaction.

Details Window

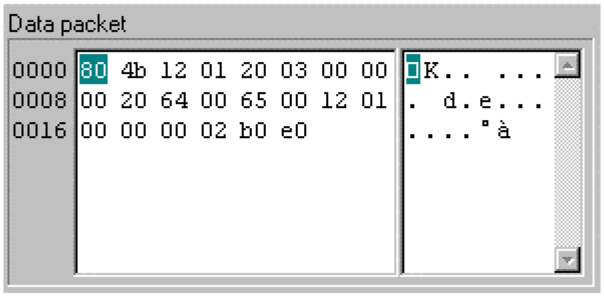


#000014, INVALID. Begins at acq#: 1810. Ends at acq#: 2677.
FAILURE CODE: 40408
DESCRIPTION: FS SETUP, root bus, time-out after DATA0

This window provides details on the current transaction item. Those details depend on the transaction item type:

- SOF: transaction item#, name, frame#, the number of the acquisition the transaction item starts with, the number of the acquisition the transaction item ends with. If frame analysis has been performed within the USB Process, then frames with invalid timing are signaled by using SOF INV!. In such a case the Details window presents the description of the frame timing failure.
- SETUP, OUT, IN: transaction item#, speed, alien attribute (refer to Alien Transactions); the number of the acquisition the transaction item starts with, the number of the acquisition the transaction item ends with; name, details on token: address, endpoint; idle time after token; details on data packet (if applicable): type, data payload; idle time after data packet (if applicable); handshake packet: (if applicable).
- INVAL: transaction item#, error code, name; the number of the acquisition the transaction item starts with, the number of the acquisition the transaction item ends with; error code, error description,
- RESET: duration, the number of the acquisition the transaction item starts with, the number of the acquisition the transaction item ends with;
- EOP: duration, the number of the acquisition the transaction item starts with, the number of the acquisition the transaction item ends with
- RESUME: duration, the number of the acquisition the transaction item starts with, the number of the acquisition the transaction item ends with

Data Packet Window

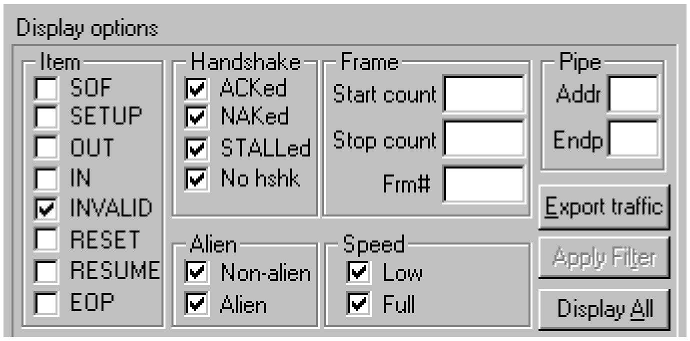


```
0000 80 4b 12 01 20 03 00 00   K..  ...
0008 00 20 64 00 65 00 12 01  .  d.e...
0016 00 00 00 02 b0 e0        ....°à
```

This window presents the body of the data packet (sync, PID, and CRC16 included), of a valid transaction (if applicable). If the transaction is not valid, or it does not contain a data packet, this window stays empty. If the user wants to see the event traffic around an invalid transaction, it may switch on Event Layer. For example if the transaction is given invalid because its data packet is not valid, the invalid packet may be seen on the Event Layer.

Bytes of the data packet are displayed both in hex and ASCII.

Display Options



Item: ☐ SOF ☐ SETUP ☐ OUT ☐ IN ☑ INVALID ☐ RESET ☐ RESUME ☐ EOP

Handshake: ☑ ACKed ☑ NAKed ☑ STALLed ☑ No hshk

Frame: Start count ☐ Stop count ☐ Frm# ☐

Pipe: Addr ☐ Endp ☐

Alien: ☑ Non-alien ☑ Alien

Speed: ☑ Low ☑ Full

Display options allow the user to specify the traffic items to be displayed in Traffic window. These options provide the following controls:

- Item group
- Handshake group
- Alien group
- Speed group
- Pipe group
- Frame group
- Apply Filter button
- Display All button

Item group allows the user to specify the transaction items to be displayed in filtered traffic. Transaction items mean not only transactions (SETUP, OUT, IN, INVALID), but SOF tokens, RESET, RESUME, and standalone EOP whose display in Traffic window may be desired. Item selection options are ORed. For example if SOF and INVALID check boxes are on, then SOF and INVALID items will be displayed.

Handshake group allows the user to specify the type of the handshake packet for OUT or IN transactions.

Alien group allows the user to specify the alien attribute for SETUP, OUT or IN transactions. (refer to Alien Transactions). This is applicable for traffic captured on non-root bus only.

Speed group allows the user to specify the speed when for SETUP, OUT or IN transactions, as well as for EOPs. This is applicable for traffic captured on FS bus only.

Pipe group allows the user to specify the pipe address and endpoint for SETUP, OUT or IN transactions. The pipe is specified in Addr and Endp edit controls. The valid range for pipe address is: 0x00..0x7f. The valid range for the pipe endpoint is: x00..0x0f. An empty control is a wild card for that parameter. For example and empty Endp edit control will not restrict the display to a specific endpoint.

Frame group allows the user to specify the frame range for the display operation. It presents the following edit controls:

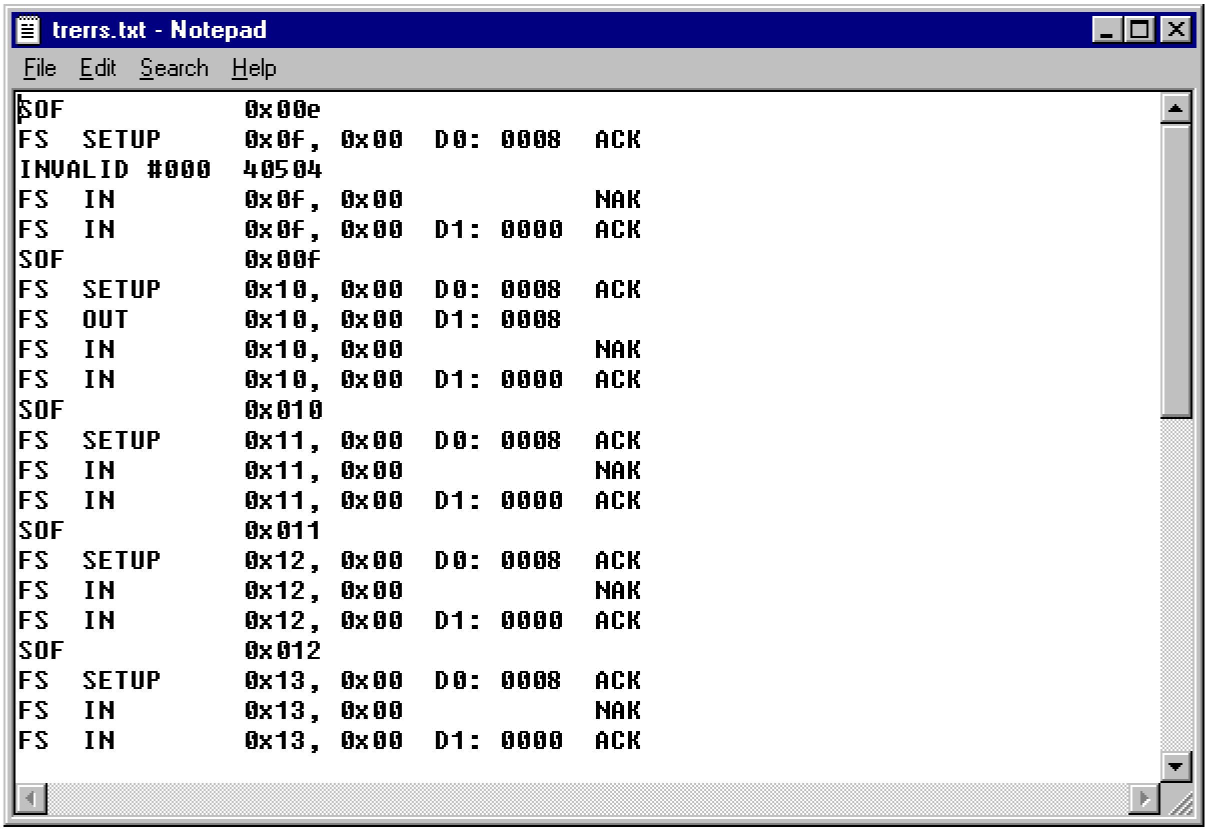
- Start, for specifying the count of the frame to start with. An empty control means that the display will start from the beginning of the traffic. The first SOF token corresponds to a count of 1.
- Stop, for specifying the count of the frame to stop after. An empty control means that the display will stop at the end of the traffic.
- Frm#, to indicate that the program will display traffic of frames having this frame number. An empty control means that the program will display traffic in all frames between those specified by Start and Stop controls. Valid range for frame number is: 0x000..0x7ff.

Frame options are ANDed between them, and ANDed with the other selection options. For example if start count is 500, and stop count is 900, and frame# is 0x10a, then the event traffic will present traffic items detected in a frame having frame# of 0x10a and being somewhere between frame 500 and frame 900 (in the same capture there may be different frames having the same frame#, if the captured traffic contains more than 2000 frames). If one field of the frame selection is empty, that is considered wild card. For example if frame# is empty, the traffic will present items detected in all frames between 500 and 900 which are enabled by other display options. Frame selection options are applicable for the traffic captured on FS bus only.

Options of all groups are ANDed between them.

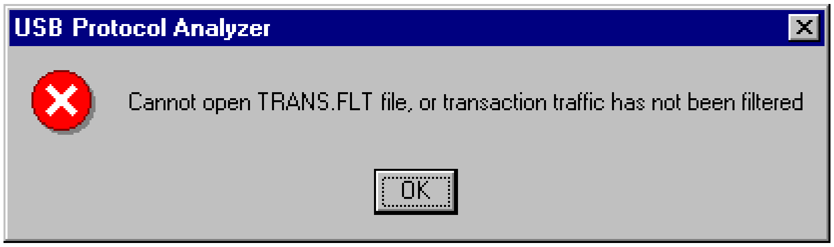
Display options have available two buttons: Display All, and Apply Filter. When the first button is pressed, the traffic will display all items around the current item. When Apply Filter button is pressed, the traffic will display items selected according to display options, i.e. filtered traffic. If the current item is enabled by display filter, the traffic focus is preserved after pressing Apply Filter. Otherwise the traffic cursor will be set on the closest item enabled by display filter.

Export Traffic button allows the user to save the filtered traffic in a user defined text file. The traffic format in that file is similar to the traffic displayed in Traffic window:



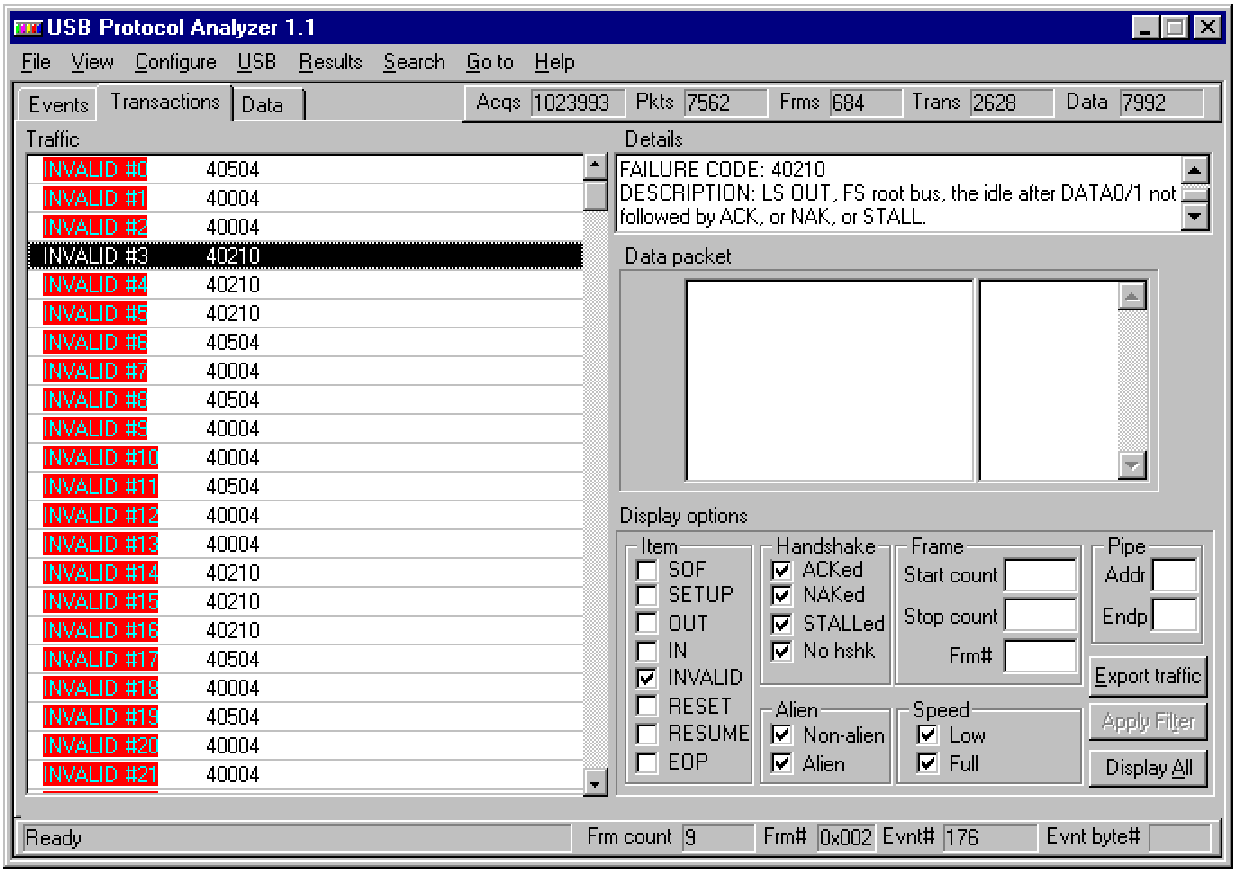
```
SOF             0x00e
FS   SETUP      0x0f, 0x00  D0: 0008  ACK
INVALID #000    40504
FS   IN         0x0f, 0x00            NAK
FS   IN         0x0f, 0x00  D1: 0000  ACK
SOF             0x00f
FS   SETUP      0x10, 0x00  D0: 0008  ACK
FS   OUT        0x10, 0x00  D1: 0008
FS   IN         0x10, 0x00            NAK
FS   IN         0x10, 0x00  D1: 0000  ACK
SOF             0x010
FS   SETUP      0x11, 0x00  D0: 0008  ACK
FS   IN         0x11, 0x00            NAK
FS   IN         0x11, 0x00  D1: 0000  ACK
SOF             0x011
FS   SETUP      0x12, 0x00  D0: 0008  ACK
FS   IN         0x12, 0x00            NAK
FS   IN         0x12, 0x00  D1: 0000  ACK
SOF             0x012
FS   SETUP      0x13, 0x00  D0: 0008  ACK
FS   IN         0x13, 0x00            NAK
FS   IN         0x13, 0x00  D1: 0000  ACK
```

Up to 1000 traffic items may be exported. This command allows the user to save the filtered traffic in a text file. That file may be loaded, viewed and printed with a text utility (as NotePad for example). If the traffic has not been filtered yet, the program will prompt a warning:



Cannot open TRANS.FLT file, or transaction traffic has not been filtered

The picture below presents the filtered transaction traffic when INVALID item has been selected:



Acqs 1023993 Pkts 7562 Frms 684 Trans 2628 Data 7992

INVALID #0	40504
INVALID #1	40004
INVALID #2	40004
INVALID #3	40210
INVALID #4	40210
INVALID #5	40210
INVALID #6	40504
INVALID #7	40004
INVALID #8	40504
INVALID #9	40004
INVALID #10	40004
INVALID #11	40504
INVALID #12	40004
INVALID #13	40004
INVALID #14	40210
INVALID #15	40210
INVALID #16	40210
INVALID #17	40504
INVALID #18	40004
INVALID #19	40504
INVALID #20	40004
INVALID #21	40004

FAILURE CODE: 40210
DESCRIPTION: LS OUT, FS root bus, the idle after DATA0/1 not followed by ACK, or NAK, or STALL.

Item: ☐ SOF ☐ SETUP ☐ OUT ☐ IN ☑ INVALID ☐ RESET ☐ RESUME ☐ EOP

Handshake: ☑ ACKed ☑ NAKed ☑ STALLed ☑ No hshk

Frame: Start count Stop count Frm#

Pipe: Addr Endp

Alien: ☑ Non-alien ☑ Alien

Speed: ☑ Low ☑ Full

Ready Frm count 9 Frm# 0x002 Evnt# 176 Evnt byte#

Traffic Focus on Transaction Layer

The traffic focus is indicated by the following read only controls provided by Status bar:

- Frm count
- Frm#
- Evnt#
- Evnt byte#

Frm count indicates the count of the frame containing the current traffic item. The first frame has a count of 1. If the traffic has been captured on a low speed bus, or it is not preceded by any SOF, that control stays empty.

Frm# indicates the number of the frame containing the current traffic item. If the traffic has been captured on a low speed bus, or it is not preceded by any SOF, that control stays empty.

Evnt# indicates the number of an event depending on the type of the current transaction item:

- for SOF, RESET, RESUME, EOP it is indicated the number of that event
- for INVALID it is indicated the number of an event which is part of the invalid transaction
- for SETUP, OUT, IN transactions, it is indicated the number of the data packet event (if the transaction contains such a packet), or the number of the token packet event

Evnt byte# indicates the number of the byte transferred in the event indicated in Evnt# control, when that event is a data packet of a transaction. The first byte in the packet (the sync byte) has a #

of zero. If the current transaction item is not a transaction, or it is but it does not have a data packet, this control stays empty.

The traffic focus information helps the user to check that it stays in the same place of the traffic when switching between filtered and unfiltered traffic, or when switching between traffic layers.

Switching on Event Layer

Switching from transactions to events is possible regardless of the currently selected transaction item. It may be performed in any of the following ways:

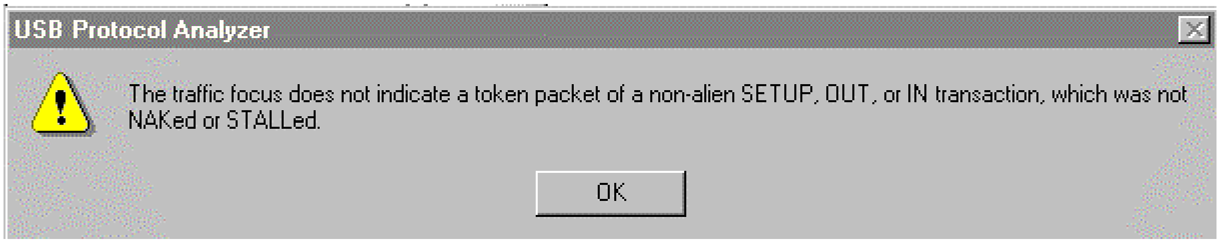
- click the tab of Event Layer
- press `F2`
- press `CTRL+SHIFT+TAB`

At that moment the screen will present Event Layer. The traffic focus is preserved (i.e. the information presented on Status bar not change).

Note that when entering the Event Layer, the program presents unfiltered traffic.

Switching on Data Layer

Switching from transactions to data is possible only if the currently selected item in Traffic window is a SETUP, OUT, or IN transaction, non-alien, which was not NAKed or STALLed. Otherwise the program displays the message presented below:


USB Protocol Analyzer

The traffic focus does not indicate a token packet of a non-alien SETUP, OUT, or IN transaction, which was not NAKed or STALLed.

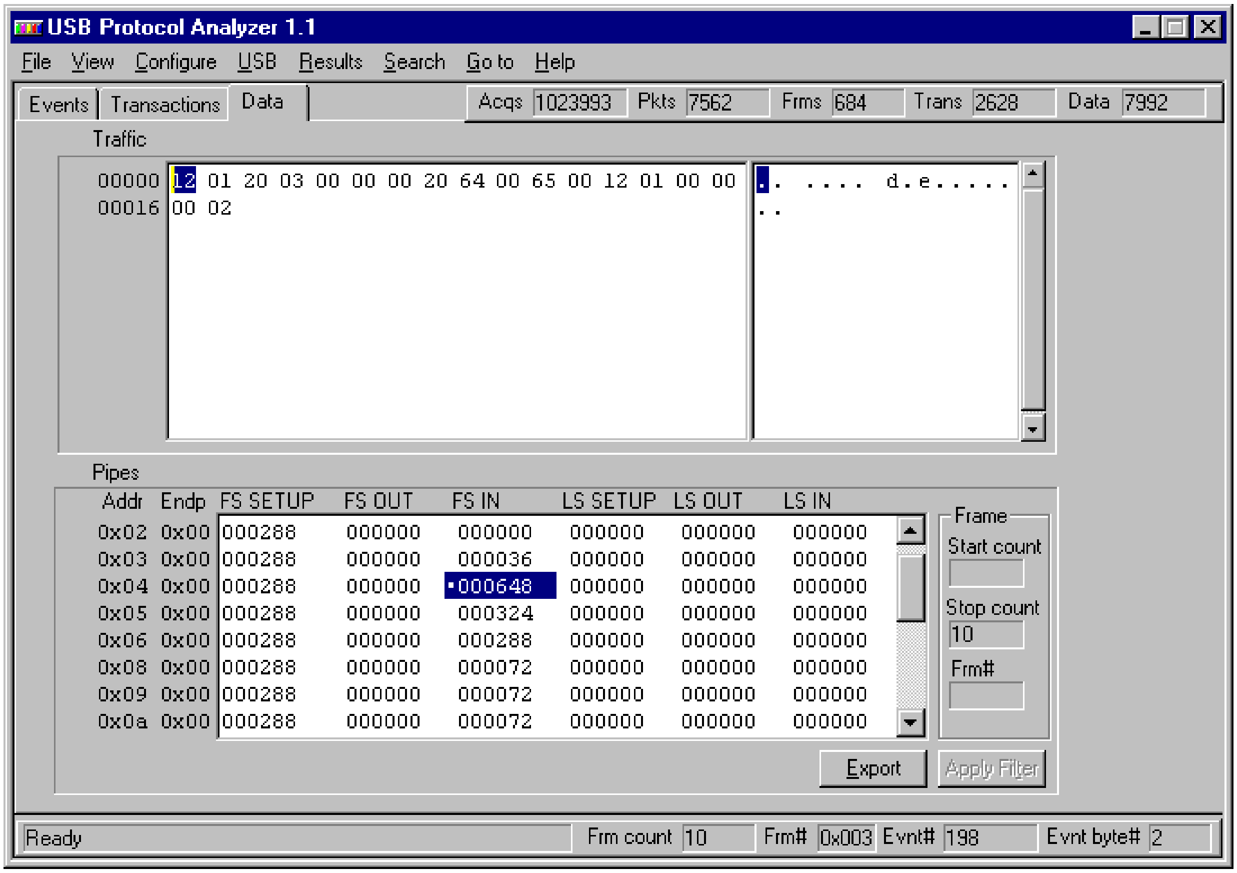
The reason for this restriction is the program needs to know the pipe whose data traffic must be presented. If the transaction is alien (refer to Alien Transactions), it means that the pipe does not go through the bus branch where the USB Probe is installed. If the transaction has been NAKed or STALLed it means the data did no go through, therefore should not be presented as being transferred.

Switching from transactions to data may be performed in any of the following ways:

- click the tab of Data Layer
- press `F4`
- press `CTRL+TAB`

Data Traffic

Data Layer



Acqs 1023993 Pkts 7562 Frms 684 Trans 2628 Data 7992

```
00000 12 01 20 03 00 00 00 20 64 00 65 00 12 01 00 00   .. ....  d.e......
00016 00 02                                              ..
```

Addr	Endp	FS SETUP	FS OUT	FS IN	LS SETUP	LS OUT	LS IN
0x02	0x00	000288	000000	000000	000000	000000	000000
0x03	0x00	000288	000000	000036	000000	000000	000000
0x04	0x00	000288	000000	▪000648	000000	000000	000000
0x05	0x00	000288	000000	000324	000000	000000	000000
0x06	0x00	000288	000000	000288	000000	000000	000000
0x08	0x00	000288	000000	000072	000000	000000	000000
0x09	0x00	000288	000000	000072	000000	000000	000000
0x0a	0x00	000288	000000	000072	000000	000000	000000

Start count

Stop count 10

Frm#

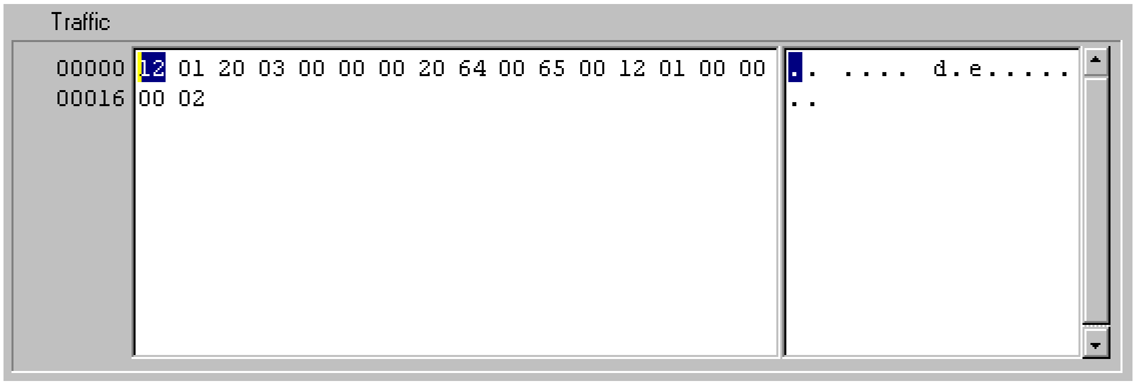
Ready Frm count 10 Frm# 0x003 Evnt# 198 Evnt byte# 2

This layer presents the data traffic over an user specified pipe. That data has been transferred in transactions which have not been NAKed or STALLed. The sync, PID and CRC bytes are not displayed. Data Layer contains the following controls:

- the layer tab which may be clicked to switch on this layer
- Traffic window
- Display options group

Also the Traffic Information bar and the Status bar are available as on any other traffic layer.

Traffic Window



```
00000 12 01 20 03 00 00 00 20 64 00 65 00 12 01 00 00   ..  ....  d.e.....
00016 00 02                                             ..
```

This window displays data bytes transferred over the pipe and transaction type currently selected in Pipes Table. Both hex and ASCII representation are available. The highlighted byte is referred as current byte (i.e. the byte cursor indicates that byte).

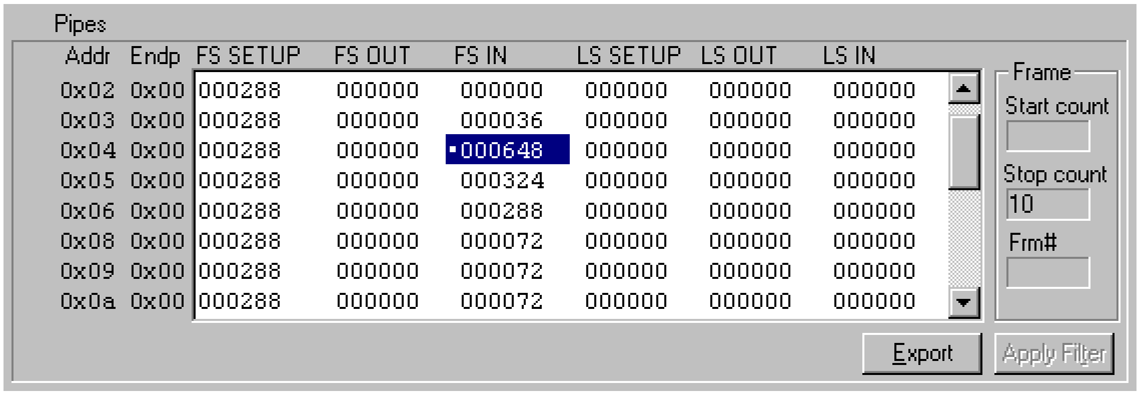
Bytes shown on the Traffic window are provided in the data packets by one of the following non-alien transaction types over the selected pipe:

- SETUP transactions
- OUT transactions which have not been NAKed or STALLed
- IN transactions which have not been NAKed or STALLed

If the transaction is alien (refer to Alien Transactions), it means that the pipe does not go through the bus branch where the USB Probe is installed. If the transaction has been NAKed or STALLed it means the data did no go through, therefore should not be presented as being transferred.

Note that sync byte, PID, and CRC16 bytes are not presented.

Display Options



Addr	Endp	FS SETUP	FS OUT	FS IN	LS SETUP	LS OUT	LS IN
0x02	0x00	000288	000000	000000	000000	000000	000000
0x03	0x00	000288	000000	000036	000000	000000	000000
0x04	0x00	000288	000000	000648	000000	000000	000000
0x05	0x00	000288	000000	000324	000000	000000	000000
0x06	0x00	000288	000000	000288	000000	000000	000000
0x08	0x00	000288	000000	000072	000000	000000	000000
0x09	0x00	000288	000000	000072	000000	000000	000000
0x0a	0x00	000288	000000	000072	000000	000000	000000

Start count:
Stop count: 10
Frm#:

Display options presents the following controls:

- Pipes table
- Frame group
- Apply Filter button

Pipes table presents the number of bytes transferred on each transaction type occurred over each pipe which has been used in the traffic that was captured and analyzed. The pipe is specified by address and endpoint. A cell in this table corresponds to a specific pipe and to one of the non-alien transaction types mentioned below (which was not NAKed, or STALLed):

- FS SETUP
- FS OUT
- FS IN
- LS SETUP
- LS OUT
- LS IN

A pipe is mentioned in the table only if it transferred data at least in one transaction type. The cell corresponding to that transaction type will show non-zero bytes. Transaction types of that pipe which did not transfer data will show zero bytes.

If a pipe did not transfer data in any of transaction types, that pipe is not mentioned in the table.

The data is presented for the currently selected cell which is highlighted and is marked with a '*'.

Normally there should be only one transaction type over a specified pipe (if not bi-directional). However, if the captured traffic contains RESET events, it will be possible to see that the same pipe has been assigned for different period of times to different transaction types.

Frame group presents read only controls as set on the Transaction Layer.

Apply Filter button allows the user to switch on another pipe and transaction type (in fact on another cell of Pipes table), and to present the data for that new option. This may be achieved in any of the following ways:

- double click a cell in Pipes table
- select a cell in Pipes table and press Apply Filter button

If the new cell did not provide any data transfer (i.e. displays zero bytes), the program does not update the content of Traffic window.

Traffic Focus on Data Layer

The traffic focus is indicated by the following read only controls provided by Status bar:

- Frm count
- Frm#
- Evnt#
- Evnt byte#

Frm count indicates the count of the frame containing the data packet which provides the current byte. The first frame has a count of 1. If the traffic has been captured on a low speed bus, or it is not preceded by any SOF, that control stays empty.

Frm# indicates the number of the frame containing the data packet which provides the current byte. If the traffic has been captured on a low speed bus, or it is not preceded by any SOF, that control stays empty.

Evnt# indicates the data packet which provides the current byte.

Evnt byte# indicates the number of the current byte. Because sync and PID bytes are stripped of, this control will no indicate values of 0 or 1.

The traffic focus information helps the user to check that it stays in the same place of the traffic when filtering or switching between traffic layers.

Switching on Event Layer

Switching from data to events is possible regardless of the currently selected byte or pipe. It may be performed in any of the following ways:

- click the tab of Event Layer
- press `F2`
- press `CTRL+TAB`

At that moment the screen will present Event Layer. The traffic focus is preserved (i.e. the information presented on Status Bar does not change).

Note that when entering the Event Layer, the program presents unfiltered traffic.

Switching on Transaction Layer

Switching from data to transactions is possible regardless of the currently selected byte or pipe. It may be performed in any of the following ways:

- click the tab of Transaction Layer
- press `F3`
- press `CTRL+SHIFT+TAB`

At that moment the screen will present Transaction Layer. The traffic focus is preserved (i.e. the information presented on Status bar does not change).

Note that when entering the Transaction Layer , the program presents unfiltered traffic.

APPENDIX A - Protocol Errors

Protocol errors whose occurrences are detected by the USB Protocol Analyzer are divided in four categories:

- signaling errors, detectable by Event Analysis
- packet errors, detectable by Packet Analysis
- transaction errors, detectable by Transaction Analysis
- frame errors, detectable by Frame Analysis

Each error has assigned an error code and an error description. This section presents the protocol errors. The error codes have the prefix “PV” (standing for protocol violation), while the error descriptions are presented between double quotes.

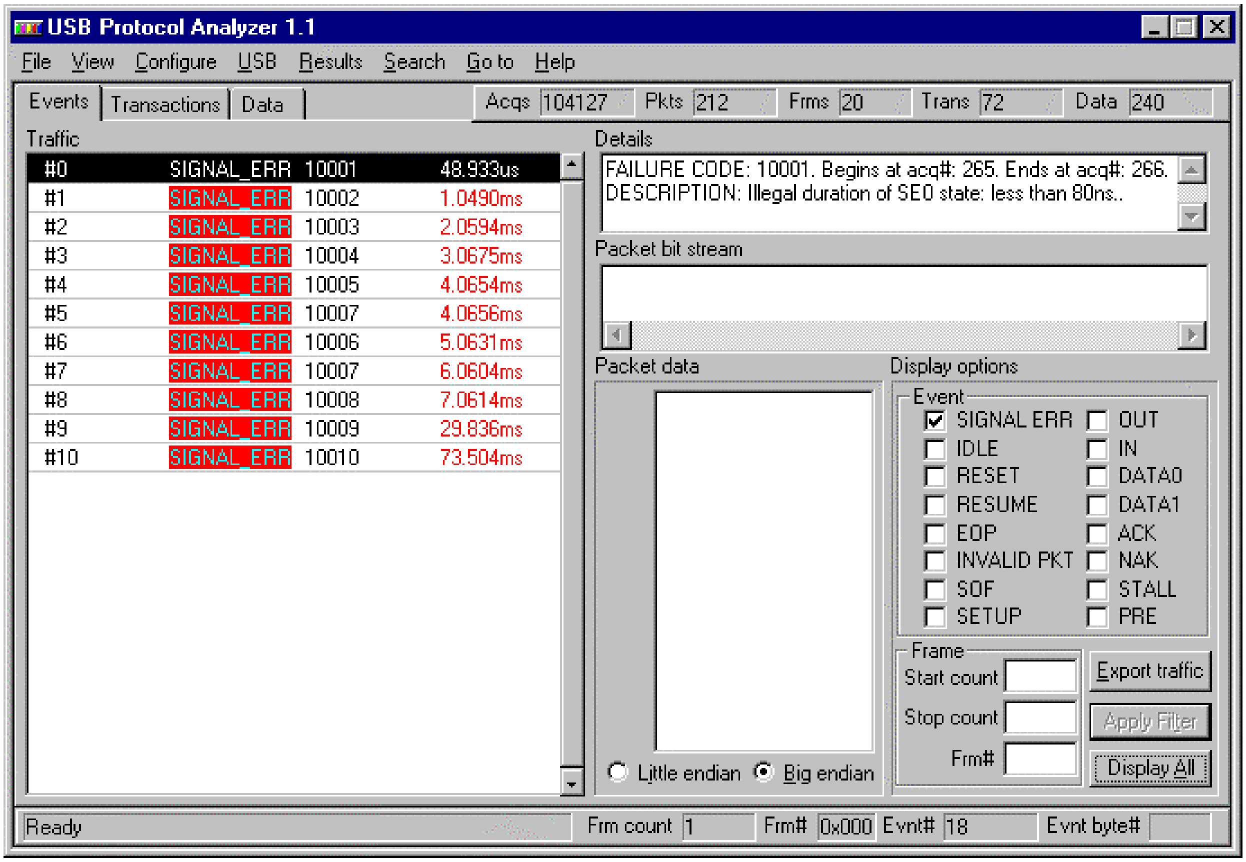
Signaling Errors

The following is the list of signaling errors whose detection is implemented in the Protocol Analyzer:

PV010001 = "Illegal duration of SE0 state: less than 80ns.";
PV010002 = "Illegal duration of SE0 state: between 5/2 FS bit times and 1 LS bit time.";
PV010003 = "Illegal duration of SE0 state: between 5/2 LS bit times and 10ms.";
PV010004 = "Illegal duration of EOP: more than 5/2 LS bit times.";
PV010005 = "K state following SE0 state.";
PV010006 = "Illegal duration of J state: less than 1/2 bit time.";
PV010007 = "K state duration too short for RESUME signaling: less than 20ms.";
PV010008 = "Illegal duration of K state: less than 1/2 bit time.";
PV010009 = "Illegal duration of LS EOP at the end of resume: less than 1 LS bit time.";
PV010010 = "Illegal duration of LS EOP at the end of resume: more than 5/2 LS bit times.";
PV010011 = "Found FS EOP on a low speed bus.";

Signaling errors detected during the Event Analysis are logged in Event Analysis report and in Event Statistics. For each error, the program indicates the description and the code. The report also indicates the number of the event where the error has been detected. Using goto commands, the user may access quickly the points in the traffic where the errors have been detected. Other ways to find the signaling errors use search commands, or Display options on Event Layer.

Signaling errors are presented in a demo file which may be loaded with Open command from File menu. When only SIGNAL_ERR traffic item is allowed by the Display options of Event Layer, the filtered traffic will look like in the picture below:



Acqs 104127 Pkts 212 Frms 20 Trans 72 Data 240

#0	SIGNAL_ERR	10001	48.933us
#1	SIGNAL_ERR	10002	1.0490ms
#2	SIGNAL_ERR	10003	2.0594ms
#3	SIGNAL_ERR	10004	3.0675ms
#4	SIGNAL_ERR	10005	4.0654ms
#5	SIGNAL_ERR	10007	4.0656ms
#6	SIGNAL_ERR	10006	5.0631ms
#7	SIGNAL_ERR	10007	6.0604ms
#8	SIGNAL_ERR	10008	7.0614ms
#9	SIGNAL_ERR	10009	29.836ms
#10	SIGNAL_ERR	10010	73.504ms

FAILURE CODE: 10001. Begins at acq#: 265. Ends at acq#: 266.
DESCRIPTION: Illegal duration of SE0 state: less than 80ns..

☑ SIGNAL ERR ☐ OUT
☐ IDLE ☐ IN
☐ RESET ☐ DATA0
☐ RESUME ☐ DATA1
☐ EOP ☐ ACK
☐ INVALID PKT ☐ NAK
☐ SOF ☐ STALL
☐ SETUP ☐ PRE

Start count
Stop count
Frm#

○ Little endian ● Big endian

Ready Frm count 1 Frm# 0x000 Evnt# 18 Evnt byte#

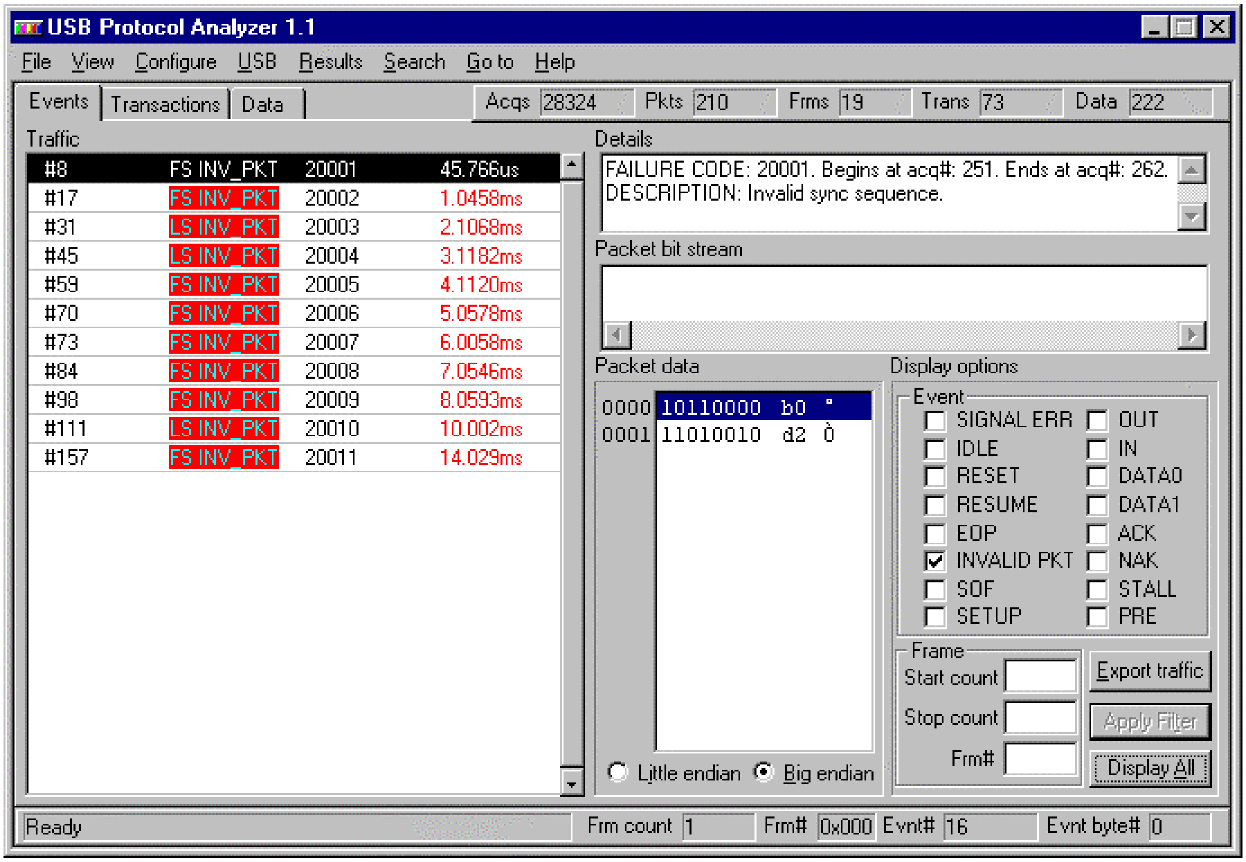
Packet Errors

The following is the list of packet errors whose detection is implemented in the Protocol Analyzer:

PV020001 = "Invalid sync sequence.";
PV020002 = "Bit stuffing error.";
PV020003 = "Illegal duration of J state: less than 1/2 bit time.";
PV020004 = "Illegal duration of K state: less than 1/2 bit time.";
PV020005 = "CRC5 error.";
PV020006 = "CRC16 error.";
PV020007 = "Babble error: more than 10000 bits in the packet.";
PV020008 = "PID error.";
PV020009 = "Truncated packet.";
PV020010 = "SOF PID at low speed.";
PV020011 = "Packet size too big: above 1027 bytes.";

Packet errors detected during the Packet Analysis are logged in Packet Analysis report and in Event Statistics. For each error, the program indicates the description and the code. The report also indicates the number of the packet where the error has been detected. Using goto commands, the user may access quickly the points in the traffic where the errors have been detected. Other ways to find the packet errors use search commands, or Display options on Event Layer.

Packet errors are presented in a demo file which may be loaded with Open command of File menu. When only INVALID_PKT traffic item is allowed by the Display options on Event Layer , the filtered traffic will look like in the picture below:



Acqs 28324 Pkts 210 Frms 19 Trans 73 Data 222

#8	FS INV_PKT	20001	45.766us
#17	FS INV_PKT	20002	1.0458ms
#31	LS INV_PKT	20003	2.1068ms
#45	LS INV_PKT	20004	3.1182ms
#59	FS INV_PKT	20005	4.1120ms
#70	FS INV_PKT	20006	5.0578ms
#73	FS INV_PKT	20007	6.0058ms
#84	FS INV_PKT	20008	7.0546ms
#98	FS INV_PKT	20009	8.0593ms
#111	LS INV_PKT	20010	10.002ms
#157	FS INV_PKT	20011	14.029ms

FAILURE CODE: 20001. Begins at acq#: 251. Ends at acq#: 262.
DESCRIPTION: Invalid sync sequence.

```
0000 10110000  b0  °
0001 11010010  d2  Ò
```

○ Little endian ● Big endian

Event

☐ SIGNAL ERR	☐ OUT
☐ IDLE	☐ IN
☐ RESET	☐ DATA0
☐ RESUME	☐ DATA1
☐ EOP	☐ ACK
☑ INVALID PKT	☐ NAK
☐ SOF	☐ STALL
☐ SETUP	☐ PRE

Frame
Start count
Stop count
Frm#

Ready Frm count 1 Frm# 0x000 Evnt# 16 Evnt byte# 0

Transaction Errors

The following transaction errors are hub related (except the last one):

PV040001 = "PRE not followed by valid idle state.";
PV040002 = "Hub setup time out of range: 4..18 FS bit times.";
PV040003 = "Hub setup time not followed by token when expected.";
PV040004 = "Did not find token when expected.";

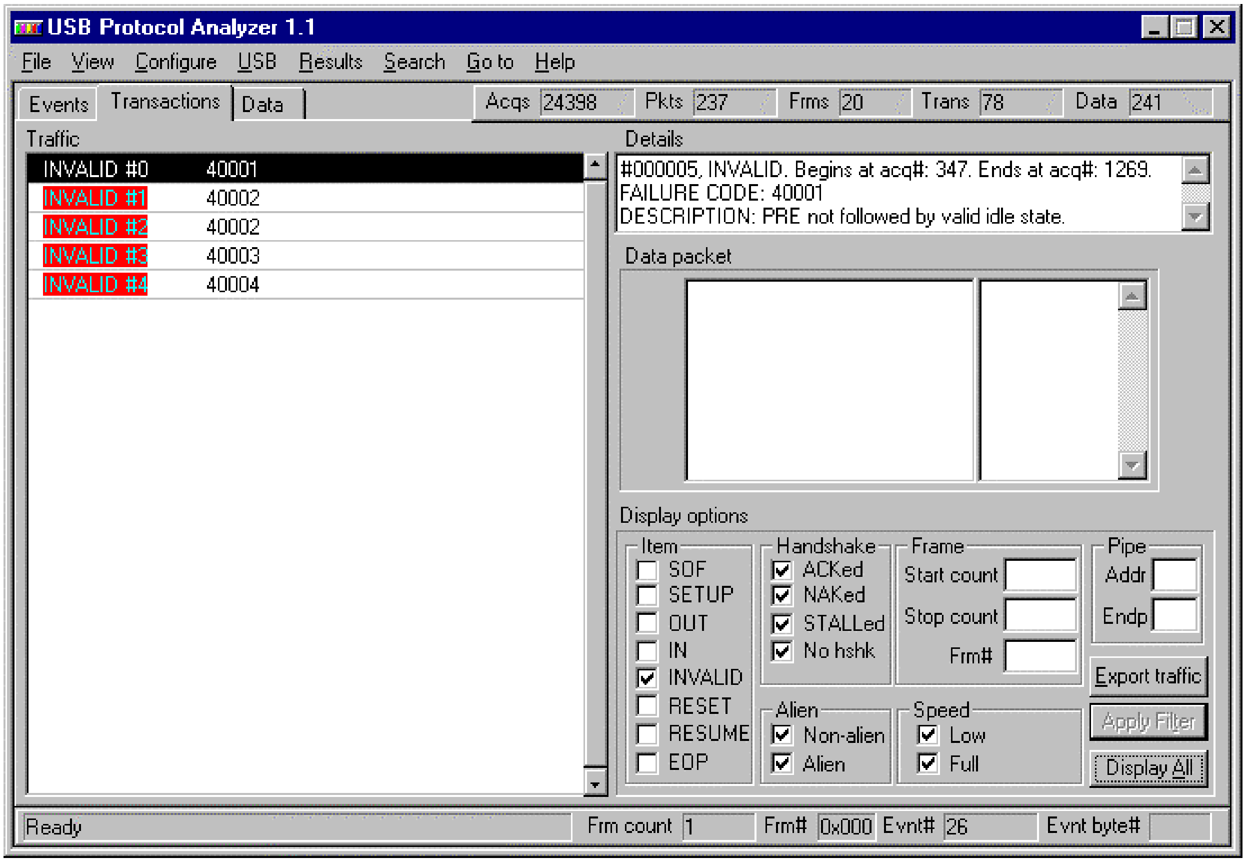
The rest of transaction errors are presented in the following categories:

Errors in LS SETUP on FS root branch
Errors in LS OUT on FS root branch
Errors in LS IN on FS root branch
Errors in FS SETUP on FS root branch
Errors in FS OUT on FS root branch
Errors in FS IN on FS root branch
Errors in LS SETUP on FS non-root branch
Errors in LS OUT on FS non-root branch
Errors in LS IN on FS non-root branch
Errors in FS SETUP on FS non-root branch
Errors in FS OUT on FS non-root branch
Errors in FS IN on FS non-root branch
Errors in LS SETUP on LS root branch
Errors in LS OUT on LS root branch
Errors in LS IN on LS root branch
Errors in LS SETUP on LS non-root branch
Errors in LS OUT on LS non-root branch
Errors in LS IN on LS non-root branch

Transaction errors detected during the Transaction Analysis are logged in Transaction Analysis report and in Event Statistics. For each error, the program indicates the description and the code. The report also indicates the number of the transaction item where the error has been detected. Using goto commands, the user may access quickly the points in the traffic where the errors have been detected. Other ways to find the transaction errors use search commands, or Display options on Transaction Layer.

There are 5 demo files for transaction errors. Each of them may be loaded with Open command from File menu. When only INVALID traffic item is allowed by the Display options of Transaction Layer , the filtered traffic will look like in the pictures below:

For hub related errors:



Acqs 24398 Pkts 237 Frms 20 Trans 78 Data 241

INVALID #0	40001
INVALID #1	40002
INVALID #2	40002
INVALID #3	40003
INVALID #4	40004

#000005, INVALID. Begins at acq#: 347. Ends at acq#: 1269.
FAILURE CODE: 40001
DESCRIPTION: PRE not followed by valid idle state.

Item
- ☐ SOF
- ☐ SETUP
- ☐ OUT
- ☐ IN
- ☑ INVALID
- ☐ RESET
- ☐ RESUME
- ☐ EOP

Handshake
- ☑ ACKed
- ☑ NAKed
- ☑ STALLed
- ☑ No hshk

Frame
Start count
Stop count
Frm#

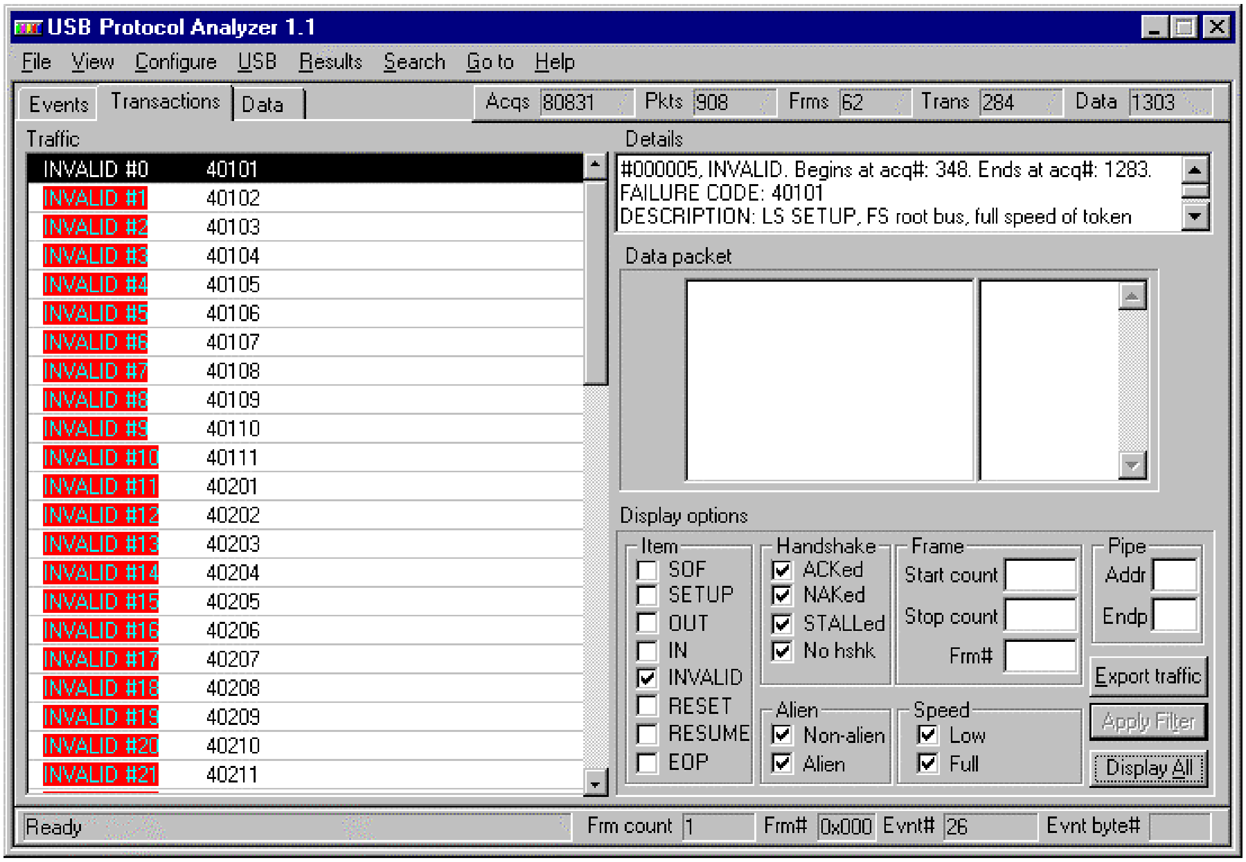
Pipe
Addr
Endp

Alien
- ☑ Non-alien
- ☑ Alien

Speed
- ☑ Low
- ☑ Full

Ready Frm count 1 Frm# 0x000 Evnt# 26 Evnt byte#

For transaction errors on a full speed root bus:



Acqs 80831 Pkts 908 Frms 62 Trans 284 Data 1303

INVALID #0	40101
INVALID #1	40102
INVALID #2	40103
INVALID #3	40104
INVALID #4	40105
INVALID #5	40106
INVALID #6	40107
INVALID #7	40108
INVALID #8	40109
INVALID #9	40110
INVALID #10	40111
INVALID #11	40201
INVALID #12	40202
INVALID #13	40203
INVALID #14	40204
INVALID #15	40205
INVALID #16	40206
INVALID #17	40207
INVALID #18	40208
INVALID #19	40209
INVALID #20	40210
INVALID #21	40211

#000005, INVALID. Begins at acq#: 348. Ends at acq#: 1283.
FAILURE CODE: 40101
DESCRIPTION: LS SETUP, FS root bus, full speed of token

Item: ☐ SOF ☐ SETUP ☐ OUT ☐ IN ☑ INVALID ☐ RESET ☐ RESUME ☐ EOP

Handshake: ☑ ACKed ☑ NAKed ☑ STALLed ☑ No hshk

Frame: Start count Stop count Frm#

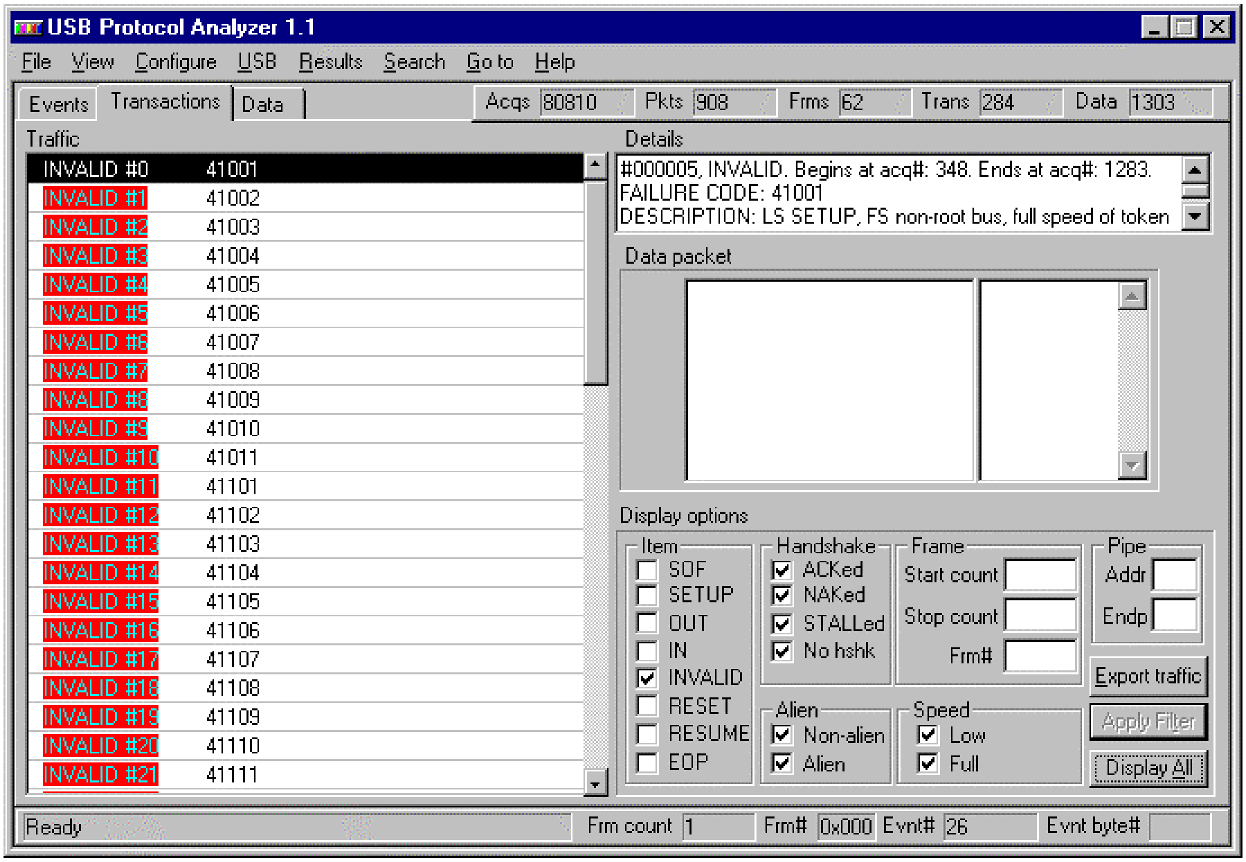
Pipe: Addr Endp

Alien: ☑ Non-alien ☑ Alien

Speed: ☑ Low ☑ Full

Ready Frm count 1 Frm# 0x000 Evnt# 26 Evnt byte#

For transaction errors on a full speed non-root bus:



Acqs 80810 Pkts 908 Frms 62 Trans 284 Data 1303

INVALID #0	41001
INVALID #1	41002
INVALID #2	41003
INVALID #3	41004
INVALID #4	41005
INVALID #5	41006
INVALID #6	41007
INVALID #7	41008
INVALID #8	41009
INVALID #9	41010
INVALID #10	41011
INVALID #11	41101
INVALID #12	41102
INVALID #13	41103
INVALID #14	41104
INVALID #15	41105
INVALID #16	41106
INVALID #17	41107
INVALID #18	41108
INVALID #19	41109
INVALID #20	41110
INVALID #21	41111

#000005, INVALID. Begins at acq#: 348. Ends at acq#: 1283.
FAILURE CODE: 41001
DESCRIPTION: LS SETUP, FS non-root bus, full speed of token

Item
☐ SOF
☐ SETUP
☐ OUT
☐ IN
☑ INVALID
☐ RESET
☐ RESUME
☐ EOP

Handshake
☑ ACKed
☑ NAKed
☑ STALLed
☑ No hshk

Frame
Start count
Stop count
Frm#

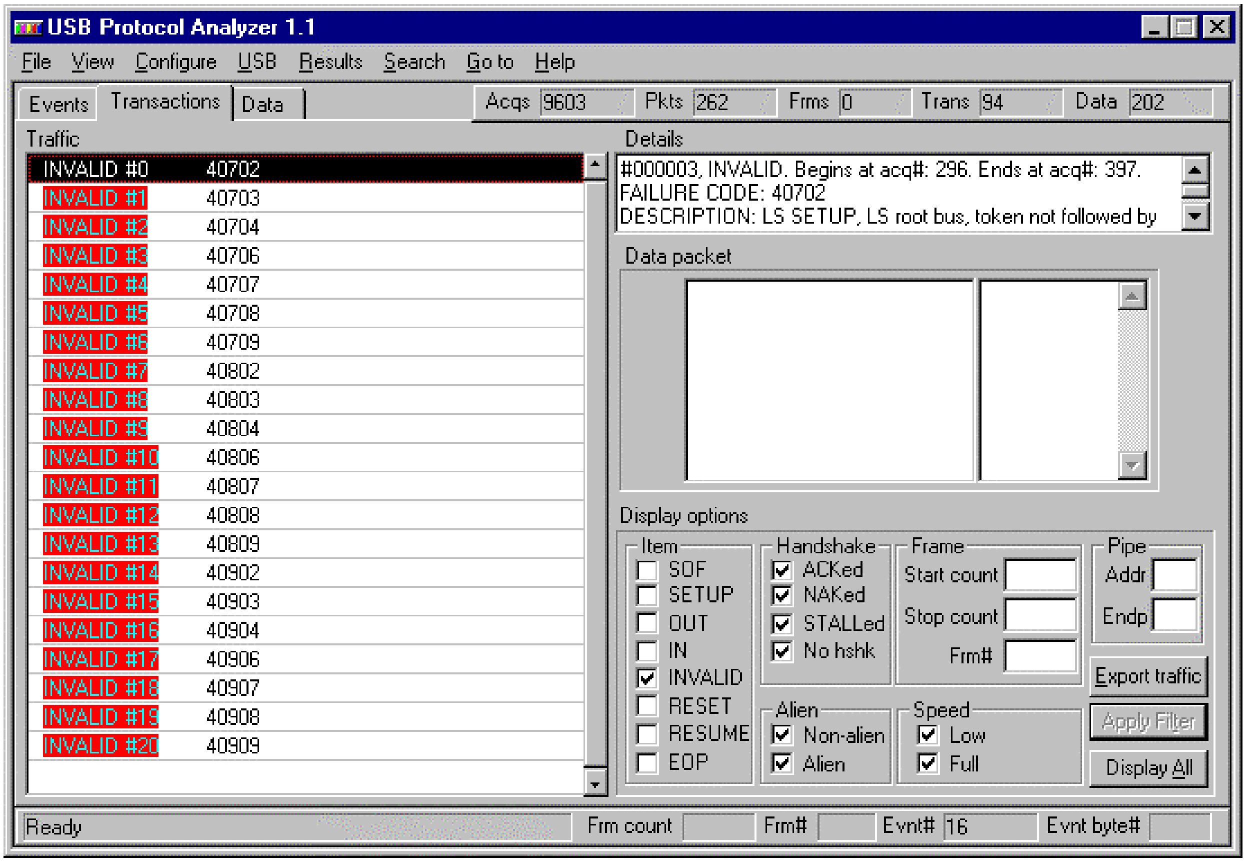
Pipe
Addr
Endp

Alien
☑ Non-alien
☑ Alien

Speed
☑ Low
☑ Full

Ready Frm count 1 Frm# 0x000 Evnt# 26 Evnt byte#

For transaction errors on a low speed root bus:


USB Protocol Analyzer 1.1
File View Configure USB Results Search Go to Help
Events Transactions Data
Export traffic
Apply Filter
Display All

Acqs 9603 Pkts 262 Frms 0 Trans 94 Data 202

Traffic

INVALID #0	40702
INVALID #1	40703
INVALID #2	40704
INVALID #3	40706
INVALID #4	40707
INVALID #5	40708
INVALID #6	40709
INVALID #7	40802
INVALID #8	40803
INVALID #9	40804
INVALID #10	40806
INVALID #11	40807
INVALID #12	40808
INVALID #13	40809
INVALID #14	40902
INVALID #15	40903
INVALID #16	40904
INVALID #17	40906
INVALID #18	40907
INVALID #19	40908
INVALID #20	40909

Details

#000003, INVALID. Begins at acq#: 296. Ends at acq#: 397.
FAILURE CODE: 40702
DESCRIPTION: LS SETUP, LS root bus, token not followed by

Data packet

Display options

Item: ☐ SOF ☐ SETUP ☐ OUT ☐ IN ☑ INVALID ☐ RESET ☐ RESUME ☐ EOP

Handshake: ☑ ACKed ☑ NAKed ☑ STALLed ☑ No hshk

Frame: Start count Stop count Frm#

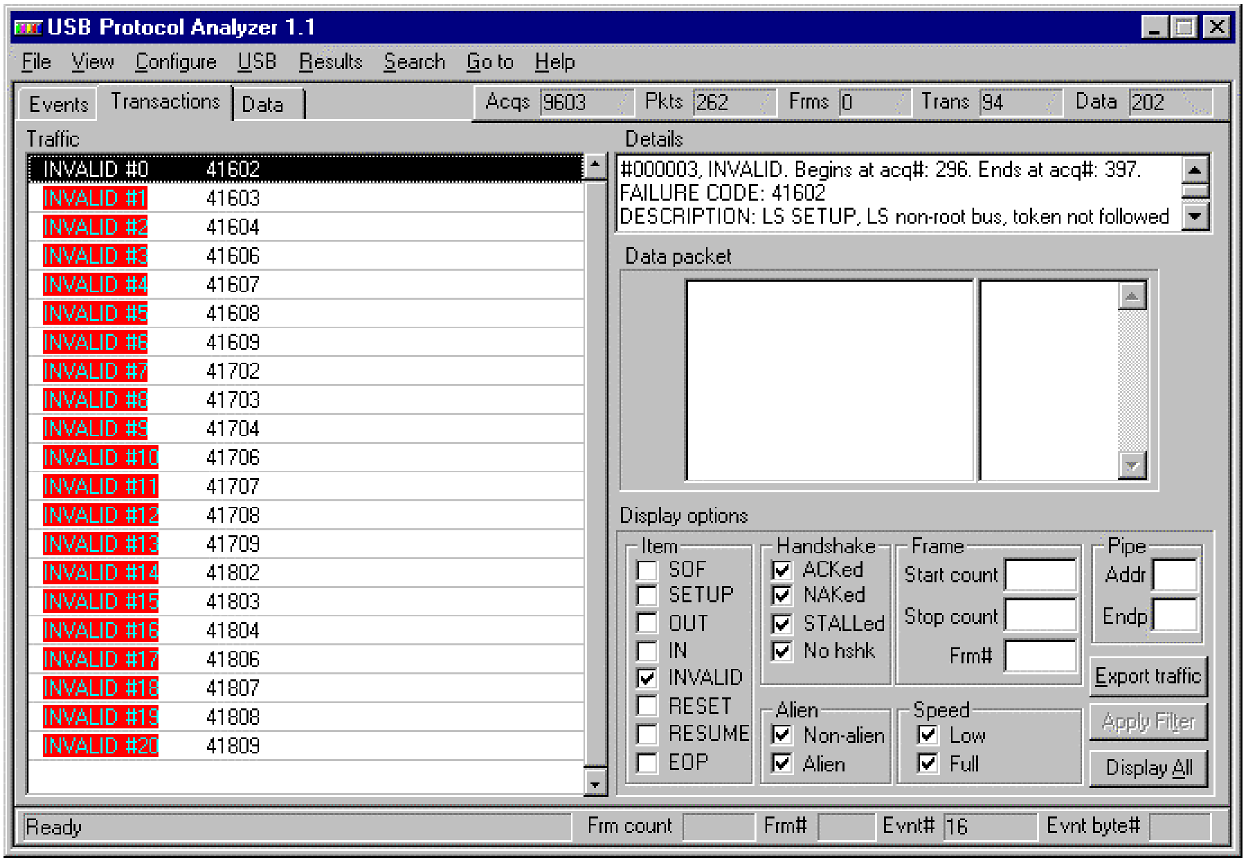
Pipe: Addr Endp

Alien: ☑ Non-alien ☑ Alien

Speed: ☑ Low ☑ Full

Ready Frm count Frm# Evnt# 16 Evnt byte#

For transaction errors on a low speed non-root bus:



Acqs 9603 Pkts 262 Frms 0 Trans 94 Data 202

Traffic	
INVALID #0	41602
INVALID #1	41603
INVALID #2	41604
INVALID #3	41606
INVALID #4	41607
INVALID #5	41608
INVALID #6	41609
INVALID #7	41702
INVALID #8	41703
INVALID #9	41704
INVALID #10	41706
INVALID #11	41707
INVALID #12	41708
INVALID #13	41709
INVALID #14	41802
INVALID #15	41803
INVALID #16	41804
INVALID #17	41806
INVALID #18	41807
INVALID #19	41808
INVALID #20	41809

#000003, INVALID. Begins at acq#: 296. Ends at acq#: 397.
FAILURE CODE: 41602
DESCRIPTION: LS SETUP, LS non-root bus, token not followed

Item: ☐ SOF ☐ SETUP ☐ OUT ☐ IN ☑ INVALID ☐ RESET ☐ RESUME ☐ EOP
Handshake: ☑ ACKed ☑ NAKed ☑ STALLed ☑ No hshk
Frame: Start count Stop count Frm#
Pipe: Addr Endp
Alien: ☑ Non-alien ☑ Alien
Speed: ☑ Low ☑ Full

Ready Frm count Frm# Evnt# 16 Evnt byte#

Errors in LS SETUP on FS root branch

PV040101 = "LS SETUP, FS root bus, full speed of token packet.";
PV040102 = "LS SETUP, FS root bus, token not followed by valid idle state.";
PV040103 = "LS SETUP, FS root bus, time-out after token packet.";
PV040104 = "LS SETUP, FS root bus, the idle after token not followed by PRE.";
PV040105 = "LS SETUP, FS root bus, hub setup time not followed by DATA0 when expected.";
PV040106 = "LS SETUP, FS root bus, full speed of DATA0 packet.";
PV040107 = "LS SETUP, FS root bus, data payload greater than 8 bytes.";
PV040108 = "LS SETUP, FS root bus, DATA0 not followed by valid idle state.";
PV040109 = "LS SETUP, FS root bus, time-out after DATA0 packet.";
PV040110 = "LS SETUP, FS root bus, the idle after DATA0 not followed by ACK.";
PV040111 = "LS SETUP, FS root bus, full speed of ACK packet.";

Errors in LS OUT on FS root branch

PV040201 = "LS OUT, FS root bus, full speed of token packet.";
PV040202 = "LS OUT, FS root bus, token not followed by valid idle state.";
PV040203 = "LS OUT, FS root bus, time-out after token packet.";
PV040204 = "LS OUT, FS root bus, the idle after token not followed by PRE.";
PV040205 = "LS OUT, FS root bus, hub setup time not followed by DATA0/1 when expected.";
PV040206 = "LS OUT, FS root bus, full speed of DATA0/1 packet.";
PV040207 = "LS OUT, FS root bus, data payload greater than 8 bytes.";
PV040208 = "LS OUT, FS root bus, DATA0/1 not followed by valid idle state.";
PV040209 = "LS OUT, FS root bus, time-out after DATA0/1 packet.";
PV040210 = "LS OUT, FS root bus, the idle after DATA0/1 not followed by ACK, or NAK, or STALL.";
PV040211 = "LS OUT, FS root bus, full speed of handshake packet.";

Errors in LS IN on FS root branch

PV040301 = "LS IN, FS root bus, full speed of token packet.";
PV040302 = "LS IN, FS root bus, token not followed by valid idle state.";
PV040303 = "LS IN, FS root bus, time-out after token.";
PV040304 = "LS IN, FS root bus, the idle after token not followed by DATA0/1, or NAK, or STALL.";
PV040305 = "LS IN, FS root bus, full speed of DATA0/1 packet.";
PV040306 = "LS IN, FS root bus, data payload greater than 8 bytes.";
PV040307 = "LS IN, FS root bus, DATA0/1 not followed by valid idle state.";
PV040308 = "LS IN, FS root bus, time-out after DATA0/1 packet.";
PV040309 = "LS IN, FS root bus, the idle after DATA0/1 not followed by PRE.";
PV040310 = "LS IN, FS root bus, the hub setup time not followed by ACK when expected.";
PV040311 = "LS IN, FS root bus, full speed of handshake packet.";

Errors in FS SETUP on FS root branch

PV040401 = "FS SETUP, root bus, low speed of token packet.";
PV040402 = "FS SETUP, root bus, token not followed by valid idle state.";
PV040403 = "FS SETUP, root bus, time-out after token packet.";
PV040404 = "FS SETUP, root bus, the idle after token not followed by DATA0.";
PV040405 = "FS SETUP, root bus, low speed of DATA0 packet.";
PV040406 = "FS SETUP, root bus, data payload greater than 64 bytes.";
PV040407 = "FS SETUP, root bus, DATA0 not followed by valid idle state.";
PV040408 = "FS SETUP, root bus, time-out after DATA0 packet.";
PV040409 = "FS SETUP, root bus, the idle after DATA0 not followed by ACK.";
PV040410 = "FS SETUP, root bus, low speed of ACK packet.";

Errors in FS OUT on FS root branch

PV040501 = "FS OUT, root bus, low speed of token packet.";
PV040502 = "FS OUT, root bus, token not followed by valid idle state.";
PV040503 = "FS OUT, root bus, time-out after token packet.";
PV040504 = "FS OUT, root bus, the idle after token not followed by DATA0/1.";
PV040505 = "FS OUT, root bus, low speed of DATA0/1 packet.";
PV040506 = "FS OUT non-isochronous, root bus, data payload greater than 64 bytes.";
PV040507 = "FS OUT, root bus, DATA0/1 not followed by valid idle state.";
PV040508 = "FS OUT non-isochronous, root bus, time-out after DATA0/1 packet.";
PV040510 = "FS OUT, root bus, low speed of handshake packet.";

Errors in FS IN on FS root branch

PV040601 = "FS IN, root bus, low speed of token packet.";
PV040602 = "FS IN, root bus, token packet not followed by valid idle state.";
PV040603 = "FS IN, root bus, time-out after token packet.";
PV040604 = "FS IN, root bus, the idle after token not followed by DATA0/1, or NAK, or STALL.";
PV040605 = "FS IN, root bus, low speed of DATA0/1 packet.";
PV040606 = "FS IN non-isochronous, root bus, data payload greater than 64 bytes.";
PV040607 = "FS IN, root bus, DATA0/1 not followed by valid idle state.";
PV040608 = "FS IN non-isochronous, root bus, time-out after DATA0/1.";
PV040610 = "FS IN, root bus, low speed of handshake packet.";

Errors in LS SETUP on FS non-root branch

PV041001 = "LS SETUP, FS non-root bus, full speed of token packet.";
PV041002 = "LS SETUP, FS non-root bus, token not followed by valid idle state.";
PV041003 = "LS SETUP, FS non-root bus, time-out after token packet.";
PV041004 = "LS SETUP, FS non-root bus, the idle after token not followed by PRE.";
PV041005 = "LS SETUP, FS non-root bus, hub setup time not followed by DATA0 when expected.";
PV041006 = "LS SETUP, FS non-root bus, full speed of DATA0 packet.";
PV041007 = "LS SETUP, FS non-root bus, data payload greater than 8 bytes.";
PV041008 = "LS SETUP, FS non-root bus, DATA0 not followed by valid idle state.";
PV041009 = "LS SETUP, FS non-root bus, time-out after DATA0 packet.";
PV041010 = "LS SETUP, FS non-root bus, the idle after DATA0 not followed by ACK when expected.";
PV041011 = "LS SETUP, FS non-root bus, full speed of ACK packet.";

Errors in LS OUT on FS non-root branch

PV041101 = "LS OUT, FS non-root bus, full speed of token packet.";
PV041102 = "LS OUT, FS non-root bus, token not followed by valid idle state.";
PV041103 = "LS OUT, FS non-root bus, time-out after token packet.";
PV041104 = "LS OUT, FS non-root bus, the idle after token not followed by PRE.";
PV041105 = "LS OUT, FS non-root bus, hub setup time not followed by DATA0/1 when expected.";
PV041106 = "LS OUT, FS non-root bus, full speed of DATA0/1 packet.";
PV041107 = "LS OUT, FS non-root bus, data payload greater than 8 bytes.";
PV041108 = "LS OUT, FS non-root bus, DATA0/1 not followed by valid idle state.";
PV041109 = "LS OUT, FS non-root bus, time-out after DATA0/1 packet.";
PV041110 = "LS OUT, FS non-root bus, the idle after DATA0/1 not followed by ACK, or NAK, or STALL when expected.";
PV041111 = "LS OUT, FS non-root bus, full speed of handshake packet.";

Errors in LS IN on FS non-root branch

PV041201 = "LS IN, FS non-root bus, full speed of token packet.";
PV041202 = "LS IN, FS non-root bus, token not followed by valid idle state.";
PV041203 = "LS IN, FS non-root bus, time-out after token.";
PV041204 = "LS IN, FS non-root bus, the idle after token not followed by DATA0/1, or NAK, or STALL.";
PV041205 = "LS IN, FS non-root bus, full speed of DATA0/1 packet.";
PV041206 = "LS IN, FS non-root bus, data payload greater than 8 bytes.";
PV041207 = "LS IN, FS non-root bus, DATA0/1 not followed by valid idle state.";
PV041208 = "LS IN, FS non-root bus, time-out after DATA0/1 packet.";
PV041209 = "LS IN, FS non-root bus, the idle after DATA0/1 not followed by PRE.";
PV041210 = "LS IN, FS non-root bus, the hub setup time not followed by ACK when expected.";
PV041211 = "LS IN, FS non-root bus, full speed of handshake packet.";

Errors in FS SETUP on FS non-root branch

PV041301 = "FS SETUP, non-root bus, low speed of token packet.";
PV041302 = "FS SETUP, non-root bus, token not followed by valid idle state.";
PV041303 = "FS SETUP, non-root bus, time-out after token packet.";
PV041304 = "FS SETUP, non-root bus, the idle after token not followed by DATA0.";
PV041305 = "FS SETUP, non-root bus, low speed of DATA0 packet.";
PV041306 = "FS SETUP, non-root bus, data payload greater than 64 bytes.";
PV041307 = "FS SETUP, non-root bus, DATA0 not followed by valid idle state.";
PV041308 = "FS SETUP, non-root bus, time-out after DATA0 packet.";
PV041309 = "FS SETUP, non-root bus, the idle after DATA0 not followed by ACK.";
PV041310 = "FS SETUP, non-root bus, low speed of ACK packet.";

Errors in FS OUT on FS non-root branch

PV041401 = "FS OUT, non-root bus, low speed of token packet.";
PV041402 = "FS OUT, non-root bus, token not followed by valid idle state.";
PV041403 = "FS OUT, non-root bus, time-out after token packet.";
PV041404 = "FS OUT, non-root bus, the idle after token not followed by DATA0/1.";
PV041405 = "FS OUT, non-root bus, low speed of DATA0/1 packet.";
PV041406 = "FS OUT non-isochronous, non-root bus, data payload greater than 64 bytes.";
PV041407 = "FS OUT, non-root bus, DATA0/1 not followed by valid idle state.";
PV041408 = "FS OUT non-isochronous, non-root bus, time-out after DATA0/1 packet.";
PV041410 = "FS OUT, non-root bus, low speed of handshake packet.";

Errors in FS IN on FS non-root branch

PV041501 = "FS IN, non-root bus, low speed of token packet.";
PV041502 = "FS IN, non-root bus, token packet not followed by valid idle state.";
PV041503 = "FS IN, non-root bus, time-out after token packet.";
PV041504 = "FS IN, non-root bus, the idle after token not followed by DATA0/1, or NAK, or STALL.";
PV041505 = "FS IN, non-root bus, low speed of DATA0/1 packet.";
PV041506 = "FS IN non-isochronous, non-root bus, data payload greater than 64 bytes.";
PV041507 = "FS IN, non-root bus, DATA0/1 not followed by valid idle state.";
PV041508 = "FS IN non-isochronous, non-root bus, time-out after DATA0/1.";
PV041510 = "FS IN, non-root bus, low speed of handshake packet.";

Errors in LS SETUP on LS root branch

PV040702 = "LS SETUP, LS root bus, token not followed by valid idle state.";
PV040703 = "LS SETUP, LS root bus, time-out after token packet.";
PV040704 = "LS SETUP, LS root bus, the idle after token not followed by DATA0.";
PV040706 = "LS SETUP, LS root bus, data payload greater than 8 bytes.";
PV040707 = "LS SETUP, LS root bus, DATA0 not followed by valid idle state.";
PV040708 = "LS SETUP, LS root bus, time-out after DATA0 packet.";
PV040709 = "LS SETUP, LS root bus, the idle after DATA0 not followed by ACK.";

Errors in LS OUT on LS root branch

PV040802 = "LS OUT, LS root bus, token packet not followed by valid idle state.";
PV040803 = "LS OUT, LS root bus, time-out after token packet.";
PV040804 = "LS OUT, LS root bus, the idle after token not followed by DATA0/1.";
PV040806 = "LS OUT, LS root bus, data payload greater than 8 bytes.";
PV040807 = "LS OUT, LS root bus, DATA0/1 not followed by valid idle state.";
PV040808 = "LS OUT, LS root bus, time-out after DATA0/1 packet.";
PV040809 = "LS OUT, LS root bus, the idle after DATA0/1 not followed by ACK, or NAK, or STALL.";

Errors in LS IN on LS root branch

PV040902 = "LS IN, LS root bus, token packet not followed by valid idle state.";
PV040903 = "LS IN, LS root bus, time-out after token packet.";
PV040904 = "LS IN, LS root bus, the idle after token not followed by DATA0/1, or NAK, or STALL.";
PV040906 = "LS IN, LS root bus, data payload greater than 8 bytes.";
PV040907 = "LS IN, LS root bus, DATA0/1 not followed by valid idle state.";
PV040908 = "LS IN, LS root bus, time-out after DATA0/1.";
PV040909 = "LS IN, LS root bus, the idle after DATA0/1 not followed by ACK packet";

Errors in LS SETUP on LS non-root branch

PV041602 = "LS SETUP, LS non-root bus, token not followed by valid idle state.";
PV041603 = "LS SETUP, LS non-root bus, time-out after token packet.";
PV041604 = "LS SETUP, LS non-root bus, the idle after token not followed by DATA0.";
PV041606 = "LS SETUP, LS non-root bus, data payload greater than 8 bytes.";
PV041607 = "LS SETUP, LS non-root bus, DATA0 not followed by valid idle state.";
PV041608 = "LS SETUP, LS non-root bus, time-out after DATA0 packet.";
PV041609 = "LS SETUP, LS non-root bus, the idle after DATA0 not followed by ACK.";

Errors in LS OUT on LS non-root branch

PV041702 = "LS OUT, LS non-root bus, token packet not followed by valid idle state.";
PV041703 = "LS OUT, LS non-root bus, time-out after token packet.";
PV041704 = "LS OUT, LS non-root bus, the idle after token not followed by DATA0/1.";
PV041706 = "LS OUT, LS non-root bus, data payload greater than 8 bytes.";
PV041707 = "LS OUT, LS non-root bus, DATA0/1 not followed by valid idle state.";
PV041708 = "LS OUT, LS non-root bus, time-out after DATA0/1 packet.";
PV041709 = "LS OUT, LS non-root bus, the idle after DATA0/1 not followed by ACK, or NAK, or STALL.";

Errors in LS IN on LS non-root branch

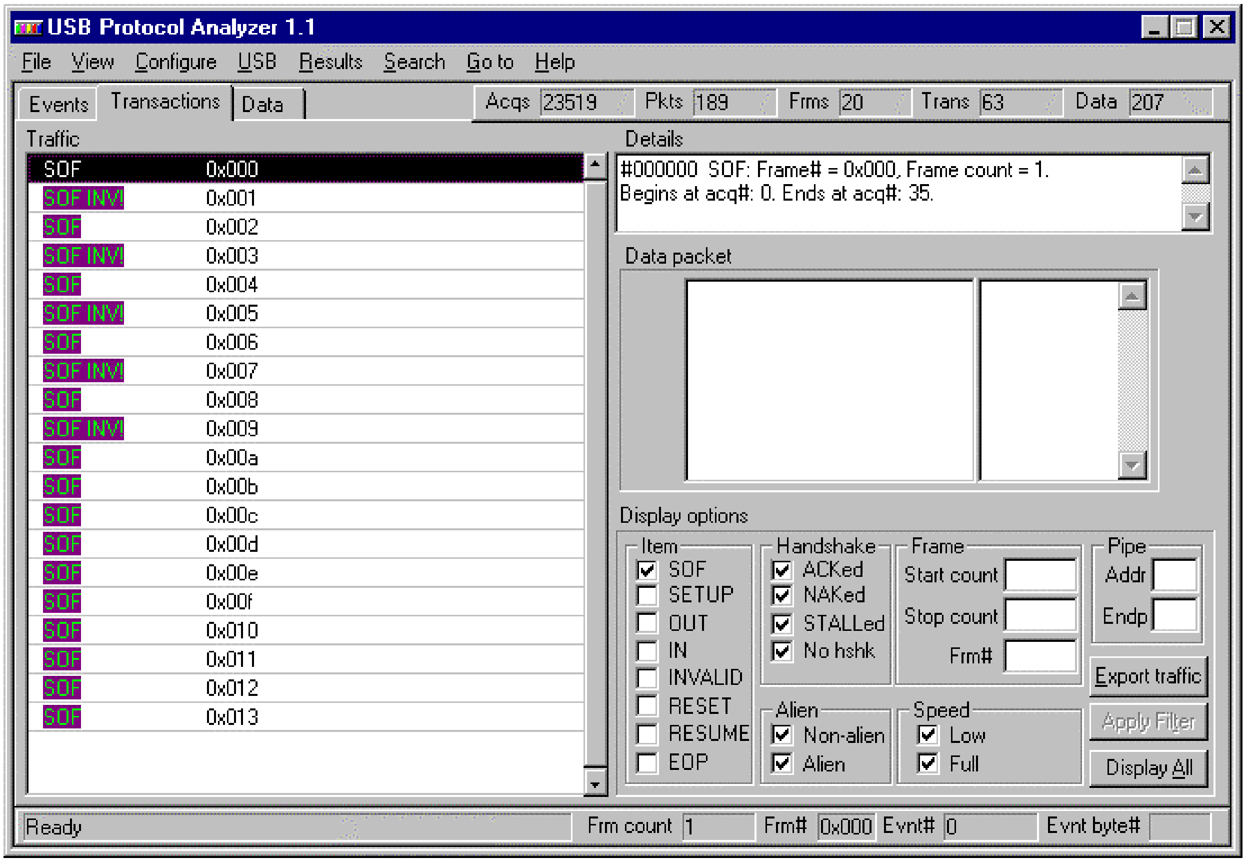
PV041802 = "LS IN, LS non-root bus, token packet not followed by valid idle state.";
PV041803 = "LS IN, LS non-root bus, time-out after token packet.";
PV041804 = "LS IN, LS non-root bus, the idle after token not followed by DATA0/1, or NAK, or STALL.";
PV041806 = "LS IN, LS non-root bus, data payload greater than 8 bytes.";
PV041807 = "LS IN, LS non-root bus, DATA0/1 not followed by valid idle state.";
PV041808 = "LS IN, LS non-root bus, time-out after DATA0/1.";
PV041809 = "LS IN, LS non-root bus, DATA0 not followed by ACK packet";

Frame Errors

PV030001 = "Invalid frame time: less than 12000 - 21 FS bit times.";
PV030002 = "Invalid frame time: more than 12000 + 21 FS bit times.";
PV030003 = "Invalid EOF1: less than 32 FS bit times.";
PV030004 = "At EOF1 found an event which is not idle state.";
PV030005 = "After EOF1 found an event which is not SOF or idle state";

Frame errors detected during the Frame Analysis are logged in Frame Analysis report and in Transaction Statistics. For each error, the program indicates the description and the code. The report also indicates the number of the transaction item corresponding to the SOF token of the invalid frame. Using goto commands, the user may access quickly the points in the traffic where the errors have been detected. Other ways to find the frame errors use search commands, or Display options on Transaction Layer.

Frame errors are presented in a demo file which may be loaded with Open command of File menu. When only SOF traffic item is allowed by the Display options of Transaction Layer, the filtered traffic will look like in the picture below:



Acqs 23519 Pkts 189 Frms 20 Trans 63 Data 207

```
SOF        0x000
SOF INV!   0x001
SOF        0x002
SOF INV!   0x003
SOF        0x004
SOF INV!   0x005
SOF        0x006
SOF INV!   0x007
SOF        0x008
SOF INV!   0x009
SOF        0x00a
SOF        0x00b
SOF        0x00c
SOF        0x00d
SOF        0x00e
SOF        0x00f
SOF        0x010
SOF        0x011
SOF        0x012
SOF        0x013
```

#000000 SOF: Frame# = 0x000, Frame count = 1.
Begins at acq#: 0. Ends at acq#: 35.

Item: ☑ SOF ☐ SETUP ☐ OUT ☐ IN ☐ INVALID ☐ RESET ☐ RESUME ☐ EOP
Handshake: ☑ ACKed ☑ NAKed ☑ STALLed ☑ No hshk
Frame: Start count ☐ Stop count ☐ Frm# ☐
Pipe: Addr ☐ Endp ☐
Alien: ☑ Non-alien ☑ Alien
Speed: ☑ Low ☑ Full

Ready Frm count 1 Frm# 0x000 Evnt# 0 Evnt byte#