USB Snoopy FAQ

Michel XHAARD

Contents

- Contents
- 1 What is USB Snoopy ?
- 2 Why do you make a Snoopy file ?
- 3 What is the brief history of USB Snoopy ?
- 4 What Snoopy can I use ?
- 5 What are the prerequits to make a snoop ?
- 6 Where can I get Snoopy software ?
- 7 How do I install my Snoopy soft ?
- 8 What can I sniff ?
    - 8.1 Have a look in your package
    - 8.2 Have a look from your snoopy soft:
- 9 When I close Dgbview crashes. What can I do ?
- 10 How can I make good snoops ?
- 11 Where can I see some examples of snoops ?
- 12 Can I remove this package ?
- About this document ...

1 What is USB Snoopy ?

Snoopy is a sort of viewer of USB traffic. Working on a windoze based machine he translate all (we expect) the data sent and received by the original windoze driver in a more human readable form and writes this result in a big ascii file.

2 Why do you make a Snoopy file ?

Unfortunately all manufacturers don't help the free software community. Several of us have tried, at various times, to obtain information on the spca50x chips from SunPlus, but have failed. Therefore we use reverse engineering for the protocols and functionality provided by these greats chips. Snoopy is one of the tools we use. This is free GPL software for windoze platforms.

3 What is the brief history of USB Snoopy ?

The initial release came in July 2000 from Roland and Tom http://www.wingmanteam.com/usbsnoopy or http://home.jps.net/koma with version 0.1 for windoze 98. This team, in 2001 port Snoopy on windoze 2000 version 0.13 . A spin-off project SnoopyPro is hosted on sourceforge.net(in mars 2003 version SnoopyPro-0.22) this version didn't produce a readable file . One developer Benoit Papillault hosted the last release (jan 2003) sniff-bin-1.8.zip working on windoze 98/2000/XP http://benoit.papillault.free.fr.

4 What Snoopy can I use ?

First, a Snoopy capable of doing a readable file .

Second, a Snoopy must be agreed on by the developer team. Why? some developers use PERL scripts filters to preanalyze the file. These filters parse the syntax of the file. We don't need to rewrite these filters for each version of snoopy. Contact the developer team (on IRC: irc.freenode.net channel #spca50x)

5 What are the prerequits to make a snoop ?

A windoze box able to work with USB, the original driver of your cam, the snoopy software, unzip software, some space in your hard drive, and to be ``cool''.

6 Where can I get Snoopy software ?

Download on the Internet:

http://www.wingmanteam.com/usbsnoopy

http://home.jps.net/koma

http://benoit.papillault.free.fr

http://usbsnoop.sourceforge.net

7 How do I install my Snoopy soft ?

First unzip the package where you want in the windoze tree eg: c:\Program Files. There is a README file for each version . Read the install method:

From : http://home.jps.net/koma

USB Snoopy is made in three parts:

- A filter to watch the traffic :usbsnoopy.sys
- A debug viewer: dgbview to catch the output (don't forgot to save the snoopy file)
- A dialogue box interface to install and remove the filter

From: http://benoit.papillault.free.fr

A unique exe file includes the right filter (windoze98 , windoze2000 or windozeXP) and a dialogue box to control the sniffer. The output is directly writen in a file SNOOPY.log readable with your favorite editor.

For the two versions, the filter acts as a driver and is copied in: C:\WINDOWS\SYSTEM32\DRIVERS or C:\WINNT\SYSTEM32\DRIVERS.

Put a symbolic link to the interface (and viewer if necessary) in your Desktop.

That's all.

From my experience, windoze doesn't like a big file in notepad. The best way is to use a Linux editor for that.

It's a bad idea to mix the two versions get the right one for you.

I have not tested the XP version.

8 What can I sniff ?

You have to install your windoze driver first. Please follow the instructions in your driver manual in most cases install first the soft and when the soft is correctly installed, plug your device on the USB bus.

8.1 Have a look in your package

In most cases the driver comes with a lot of soft. we just want to :

- Init the Cam
- Start the stream

- Stop the stream
- Change picture params

Select the more simplest soft and the more simplest way to do that. Because Snoopy catches all the traffic in a file it is not necessary to write all the pictures data .

8.2 Have a look from your snoopy soft:

Run the viewer if necessary, run the sniffer. The first step is to install the filter:

For usbsnoop : select unpack the filter then install.

For sniff-usb : just click OK The soft detects your windoze platform and installs the usbsnoop.sys in the right place.

In the dialog box you can see your USB tree. The first entry are the USB root hub followed by your USB device The vendor product id help you select the right one.

Each device can have a lot of interfaces. The windoze device driver install one driver for each interface. The video interface an audio are in most case an isochronous pipes. bulk pipes are often used to download or upload pictures on the cam . Interrupt pipes are often used as status lines.

To install the filter click on properties of an interface and install. to remove click uninstall, It's easy .

When the filter is installed unplug and plug the device .The sniff begins you see all traffic in the viewer and for the other version the length of the file Snoopy increase. Uninstall the filter save the file on the viewer close the dialog box you have all the prerequits to make good snoops.

9 When I close Dgbview crashes. What can I do ?

In some case in windoze 98 Dgbview crashes Go to the task scheduler and stop the task.

10 How can I make good snoops ?

First what do you want ?

It's a good idea to make a little snoop for each relevant function you need.

Make a plan and test your assumption first.

11 Where can I see some examples of snoops ?

Here:

From usbsnoops:

00000108 20.61817600 UsbSnoop - Entering DriverUnload: DriverObject C146EB28

00000109 76.15237040 UsbSnoop - Entering DriverEntry: DriverObject C146EB28

00000110 76.15238240 UsbSnoop - Running under Windows 98

00000111 76.15240880 UsbSnoop - Entering AddDevice: DriverObject C146EB28, pdo C1470028

00000112 76.15260560 UsbSnoop - IRP_MJ_PNP (IRP_MN_FILTER_RESOURCE_REQUIREMENTS)

00000113 76.15270720 UsbSnoop - IRP_MJ_INTERNAL_DEVICE_CONTROL, IOCTL_INTERNAL_USB_GET_ROOTHUB_PDO

00000114 76.15272320 UsbSnoop - IRP_MJ_PNP (IRP_MN_START_DEVICE)

00000115 76.15304800 UsbSnoop - IRP_MJ_PNP (IRP_MN_QUERY_CAPABILITIES)

00000116 76.15307440 UsbSnoop - IRP_MJ_INTERNAL_DEVICE_CONTROL, IOCTL_INTERNAL_USB_SUBMIT_URB

00000117 76.15308400

00000118 76.15308880 >>>>>>> URB 1 going down...

00000119 76.15309920 - URB_FUNCTION_GET_DESCRIPTOR_FROM_DEVICE:

00000120 76.15310960 TransferBufferLength = 00000012

00000121 76.15311920 TransferBuffer = c1470702

00000122 76.15313200 TransferBufferMDL = 00000000

00000123 76.15314080 Index = 00

00000124 76.15315200 DescriptorType = 01 (USB_DEVICE_DESCRIPTOR_TYPE)

00000125 76.15316080 LanguageId = 0000

00000126 76.15824560

00000127 76.15825040 <<<<<<< URB 1 coming back...

00000128 76.15826240 - URB_FUNCTION_CONTROL_TRANSFER:

00000129 76.15827280 PipeHandle = c146f3ac

00000130 76.15828640 TransferFlags = c2808b1f (USBD_TRANSFER_DIRECTION_IN, USBD_SHORT_TRANSFER_OK)

00000131 76.15829600 TransferBufferLength = 00000012

00000132 76.15830640 TransferBuffer = c1470702

00000133 76.15831920 TransferBufferMDL = c177b300

00000134 76.15832320 0000:

00000135 76.15836480 12 01 00 01 00 00 00 08 fc 04 4b 50 00 01 00 00

00000136 76.15836960 0010:

00000137 76.15838080 00 01

00000138 76.15838960 UrbLink = 00000000

00000139 76.15841360 SetupPacket : 80 06 00 01 00 00 12 00

00000140 76.15846880 UsbSnoop - IRP_MJ_INTERNAL_DEVICE_CONTROL, IOCTL_INTERNAL_USB_SUBMIT_URB

From usb-sniff:

0 ms] UsbSnoop compiled on Jan 13 2003 20:05:44 loading

[0 ms] UsbSnoop - DriverEntry(ee3aabe0) : Windows NT WDM version 1.16

[0 ms] UsbSnoop - AddDevice(ee3aaf20) : DriverObject fa009030, pdo f9c42ab0

[0 ms] fido=f9ffee20 pdx=f9ffeed8

[0 ms] fdo=f9c42ab0 OriginalDriverObject=fa03c3d0 d=f9cab1c8

[1 ms] UsbSnoop - DispatchAny(ee3a8600) : IRP_MJ_PNP (0x00000018)

[1 ms] UsbSnoop - MyDispatchPNP(ee3aaea0) : IRP_MJ_PNP (0x00000018)

[1 ms] fido=f9ffee20

[1 ms] pdx=f9ffeed8

[1 ms] UsbSnoop - DispatchAny(ee3a8600) : IRP_MJ_PNP (IRP_MN_QUERY_RESOURCE_REQUIREMENTS)

[1 ms] UsbSnoop - MyDispatchPNP(ee3aaea0) : IRP_MJ_PNP (IRP_MN_QUERY_RESOURCE_REQUIREMENTS)

[1 ms] fido=f9ffee20

[1 ms] pdx=f9ffeed8

[1 ms] UsbSnoop - DispatchAny(ee3a8600) : IRP_MJ_PNP (IRP_MN_FILTER_RESOURCE_REQUIREMENTS)

[1 ms] UsbSnoop - MyDispatchPNP(ee3aaea0) : IRP_MJ_PNP (IRP_MN_FILTER_RESOURCE_REQUIREMENTS)

[1 ms] fido=f9ffee20

[1 ms] pdx=f9ffeed8

[1 ms] UsbSnoop - DispatchAny(ee3a8600) : IRP_MJ_INTERNAL_DEVICE_CONTROL

[1 ms] UsbSnoop - MyDispatchInternalIOCTL(ee3a9e70) : fdo=f9c42ab0, Irp=f9c43908, IRQL=0

[1 ms] UsbSnoop - DispatchAny(ee3a8600) : IRP_MJ_PNP (IRP_MN_START_DEVICE)

[1 ms] UsbSnoop - MyDispatchPNP(ee3aaea0) : IRP_MJ_PNP (IRP_MN_START_DEVICE)

[1 ms] fido=f9ffee20

[1 ms] pdx=f9ffeed8

[1 ms] UsbSnoop - DispatchAny(ee3a8600) : IRP_MJ_PNP (IRP_MN_QUERY_CAPABILITIES)

[1 ms] UsbSnoop - MyDispatchPNP(ee3aaea0) : IRP_MJ_PNP (IRP_MN_QUERY_CAPABILITIES)

[1 ms] fido=f9ffee20

[1 ms] pdx=f9ffeed8

[1 ms] UsbSnoop - DispatchAny(ee3a8600) : IRP_MJ_INTERNAL_DEVICE_CONTROL

[1 ms] UsbSnoop - MyDispatchInternalIOCTL(ee3a9e70) : fdo=f9c42ab0, Irp=f9c43908, IRQL=0

[1 ms] >>> URB 1 going down >>>

- URB_FUNCTION_GET_DESCRIPTOR_FROM_DEVICE:

TransferBufferLength = 00000012

TransferBuffer = f9ffe930

TransferBufferMDL = 00000000

Index = 00000000

DescriptorType = 00000001 (USB_DEVICE_DESCRIPTOR_TYPE)

LanguageId = 00000000

[7 ms] UsbSnoop - MyInternalIOCTLCompletion(ee3a9da0) : fido=00000000, Irp=f9c43908, Context=f9cd4a28, IRQL=2

[7 ms] <<< URB 1 coming back <<<

- URB_FUNCTION_CONTROL_TRANSFER:

PipeHandle = f9bb2594

TransferFlags = 005c0077 (USBD_TRANSFER_DIRECTION_IN, USBD_SHORT_TRANSFER_OK)

TransferBufferLength = 00000012

TransferBuffer = f9ffe930

TransferBufferMDL = f9cc6b88

00000000: 12 01 00 01 00 00 00 08 fc 04 4b 50 00 01 00 00

00000010: 00 01

UrbLink = 00000000

SetupPacket =

00000000: 80 06 00 01 00 00 12 00

12 Can I remove this package ?

When all is done, it's a good idea to remove the filter. Go to the relevant directory and delete usbsnoop.sys[1]

About this document ...

USB Snoopy FAQ

This document was generated using the **LaTeX**2HTML translator Version 99.2beta8 (1.43)

The command line arguments were:
latex2html `-no_subdir -split 0 -show_section_numbers /tmp/lyx_tmpdir3219i0gzwJ/lyx_tmpbuf3219yyyt5v/snoopy.tex`

The translation was initiated by mxhaard xhaard on 2003-03-14

Footnotes

... usbsnoop.sys[1]
With the help of Jane Oliver (English Teacher)

---

mxhaard xhaard 2003-03-14