Dec 28, 2018, 10:18 PM (https://localhost/post/996) (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 2 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius) (https://localhost/user/nefarius)

While we're already having a working code base for a dedicated Bluetooth host dongle function driver supporting genuine and fake DS3s I wanna also explore the path of a different approach: keeping the default Windows Bluetooth driver stack in place and patching it in a way that it will accept a DS3 connection transparently in parallel to other devices (keyboards, headsets etc.) via filter driver.

Analysis environment

- Windows 7 32-Bit
- Generic Bluetooth Radio (Cambridge Silicon Radio Ltd.)
  - Hardware ID: `USB\VID_0A12&PID_0001`
- Genuine Sony DualShock 3 controller

Tools used

- DebugView
- RequestTrace

Analysis

On Interrupt Pipe (HCI communication) connection seems to work at least until receiving `HCI_Remote_Name_Request_Complete_EV` :

```
121  0.33298123   ** RT_CompletionRoutineUrbSubmit: Irp: 0x856D85F0 - IOCTL_INTERNAL_USB_SUBMIT_URB
122  0.33299682   ** 07 FF 00 AC 19 28 4D 7A  AC 50 4C 41 59 53 54 41  .ÿ.¬.(Mz¬PLAYSTA
123  0.33301127   ** 54 49 4F 4E 28 52 29 33  20 43 6F 6E 74 72 6F 6C  TION(R)3 Control
124  0.33302462   ** 6C 65 72 00 00 00 00 00  00 00 00 00 00 00 00 00  ler.............
125  0.33303764   ** 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/71f8b8f8-b2c4-4c35-a290-10d7cb3db73e-image.png)

This corresponds to this

```
681     #pragma region HCI_Remote_Name_Request_Complete_EV
682
683         case HCI_Remote_Name_Request_Complete_EV:
684
685             TraceEvents(TRACE_LEVEL_INFORMATION,
686                 TRACE_INTERRUPT,
687                 "HCI_Remote_Name_Request_Complete_EV");
688
689             if (buffer[2] == 0x00)
690             {
691                 BD_ADDR_FROM_BUFFER(clientAddr, &buffer[3]);
692
693                 ULONG length;
694
695                 //
696                 // Scan through rest of buffer until null-terminator is found
697                 //
698                 for (length = 1;
699                     buffer[length + 8] != 0x00
700                     && (length + 8) < NumBytesTransferred;
701                     length++);
702
```

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/d908db13-e738-4e5c-81c0-18daef84c852-image.png)

in AirBender/WireShock. The `HCI_Command_Remote_Name_Request` is the last HCI command which has to succeed, which looks like it does. Next is building the L2CAP connection, which seems to get initiated as well a few requests later:

```
186  0.81712651   ** Irp: 0x85B26B20 - IOCTL_INTERNAL_USB_SUBMIT_URB - URB_FUNCTION_BULK_OR_INTERRUPT_TRANSFER. Buffer: 0x88790B78, MDL: 0x0,
187  0.82000822   ** RT_CompletionRoutineUrbSubmit: Irp: 0x854EE008 - IOCTL_INTERNAL_USB_SUBMIT_URB - URB_FUNCTION_BULK_OR_INTERRUPT_TRANSFER
188  0.82002413   ** 42 20 0C 00 08 00 01 00   02 01 04 00 11 00 C0 74   B ............À t
189  0.82003832   ** 42 20 0C 00 08 00 01 00   02 01 04 00 11 00 C0 74   B ............À t
190  0.82006723   ** Irp: 0x854EE008 - IOCTL_INTERNAL_USB_SUBMIT_URB - URB_FUNCTION_BULK_OR_INTERRUPT_TRANSFER. Buffer: 0x856F4000, MDL: 0x0,
191  0.82200235   ** RT_CompletionRoutineUrbSubmit: Irp: 0x854EE5A0 - IOCTL_INTERNAL_USB_SUBMIT_URB - URB_FUNCTION_BULK_OR_INTERRUPT_TRANSFER
```

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/38853936-6843-4d7a-b6ab-8bbec8fd2d78-image.png)

As `buffer[6] == 0x01 && buffer[7] == 0x00` represents the L2CAP control channel. So the L2CAP ping-pong should be looked at in greater detail and find the stage where it starts to break.

Dec 28, 2018, 10:38 PM (https://localhost/post/997)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

L2CAP_Connection_Request

```
00000181        0.82300282      ** RT_CompletionRoutineUrbSubmit: Irp: 0x854DC8B8 - IOCTL_INTERNAL_USB_SUBMI
T_URB - URB_FUNCTION_BULK_OR_INTERRUPT_TRANSFER - Status STATUS_SUCCESS - Buffer: 0x85703000, MDL: 0x887905F
0, Length: 0x10, Pipe:0x85A2137C, Flags: 0x3.
00000182        0.82301444      ** 42 20 0C 00 08 00 01 00  02 01 04 00 11 00 40 7C  B ...........@|
00000183        0.82302463      ** 42 20 0C 00 08 00 01 00  02 01 04 00 11 00 40 7C  B ...........@|
00000184        0.82304817      ** Irp: 0x854DC8B8 - IOCTL_INTERNAL_USB_SUBMIT_URB - URB_FUNCTION_BULK_OR_IN
TERRUPT_TRANSFER. Buffer: 0x878B3000, MDL: 0x0, Length: 0x1000, Pipe:0x85A2137C, Flags: 0x3.
```

This gets repeated over and over again, so either the correct answer is missing in the trace or not sent at all.

Dec 30, 2018, 5:15 PM (https://localhost/post/998)

(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)

This `.INF` section will add driver as a lower class filter driver for the Bluetooth (https://docs.microsoft.com/en-us/windows-hardware/drivers/install/system-defined-device-setup-classes-available-to-vendors) class (GUID: `{e0cbf06c-cd8b-4647-bb8a-263b43f0f974}`) and load it on every `BTHUSB` host device:

```
[Filter_Device.NT.HW]
AddReg = Filter_AddReg

[Filter_AddReg]
HKLM,SYSTEM\CurrentControlSet\Control\Class\{e0cbf06c-cd8b-4647-bb8a-263b43f0f974},LowerFilters,0x00010008,F
ilter
```

Section for uninstallation missing.

EDIT: obsolete, will do this via helper tool instead of INF file.

Dec 30, 2018, 10:34 PM (https://localhost/post/999)

(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)

Gotcha! 👮

```
2018/12/30-22:27:05.535 TRACE_LEVEL_VERBOSE     >> IOCTL_INTERNAL_USB_SUBMIT_URB
2018/12/30-22:27:05.535 TRACE_LEVEL_VERBOSE     >> >> URB_FUNCTION_BULK_OR_INTERRUPT_TRANSFER (PipeHandle: 8
54C164C)
2018/12/30-22:27:05.535 TRACE_LEVEL_VERBOSE     Bulk OUT transfer
2018/12/30-22:27:05.535 TRACE_LEVEL_INFORMATION 3C 00 10 00 0C 00 01 00 03 01 08 00 00 00 40 21 02 00 00 00
2018/12/30-22:27:05.535 TRACE_LEVEL_INFORMATION L2CAP_Connection_Response (Response: 02)
```

Byte 8 is `L2CAP_Connection_Response` from Windows Bluetooth driver, byte 16 is status:

```
/// <summary>
///     Connection refused - PSM not supported.
/// </summary>
L2CAP_ConnectionResponseResult_ConnectionRefusedPsmNotNupported = 0x0002
```

This is kinda nice to know because it's the very first L2CAP connection failing because the PSM (Protocol/Service Multiplexer) the DS3 wants to establish a channel for is forbidden in Windows. Let's patch that and see what happens 😏

Dec 31, 2018, 9:38 AM (https://localhost/post/1002) □
□ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 □
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Why this happens is actually documented (https://docs.microsoft.com/en-us/windows-hardware/drivers/ddi/content/bthddi/ns-bthddi-_brb_psm#members), especially:

> Some PSMs are reserved for use by Windows:
> SDP: 0x01
> RFCOMM: 0x03
> HID Control: 0x11
> HID Data: 0x13
> BNEP: 0x0F

It is well-known (https://github.com/felis/USB_Host_Shield_2.0/wiki/PS3-Information#Bluetooth) that the DS3 establishes communication channels via PSM `0x11` and `0x13`, which works fine on the PS3 (custom Bluetooth stack firmware) and Linux (no such reservations/limitations). On Windows however this is a pretty big deal and *the* showstopper for an out-of-the-box working connection of a DS3 with standard Windows Bluetooth stack.

A pretty neat hack around this limitation was discovered (https://nadavrub.wordpress.com/2015/07/17/simulate-hid-device-with-windows-desktop/) a few years back, but API hooking or binary patches in kernel space are strictly forbidden (mainly for stability and security reasons, even Anti-Virus vendors had to back down from this approach starting with the Vista kernel) so while having this info as a fallback, it's not something we can use in production and therefore a KMDF Bluetooth Profile Driver (https://github.com/Microsoft/Windows-driver-samples/tree/master/bluetooth/bthecho) won't be helpful here.

Will further go down and explore the lower `BTHUSB` filter route 😉

Jan 1, 2019, 12:51 PM (https://localhost/post/1003)
□ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 □
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Hm, even if nothing of this works in the end: I've now accidentally created a Bluetooth sniffer which is nice 😅

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/4a15c70c-bf43-4bcf-bd12-2593eed2be29-image.png)

Jan 1, 2019, 3:13 PM (https://localhost/post/1004)

(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius) (https://localhost/user/nefarius)

I abandoned the Bluetooth Profile Driver idea to soon; let's see what this skeleton can do for me 🤔

2019/01/01-15:12:33.976	BthPS3IndicationCallback	TRACE_LEVEL_VERBOSE	BthPS3IndicationCallback Entry
2019/01/01-15:12:33.976	BthPS3IndicationCallback	TRACE_LEVEL_VERBOSE	BthPS3IndicationCallback Exit
2019/01/01-15:12:33.976	BthPS3UnregisterPSM	TRACE_LEVEL_VERBOSE	BthPS3UnregisterPSM Entry
2019/01/01-15:12:33.976	BthPS3UnregisterPSM	TRACE_LEVEL_VERBOSE	BthPS3UnregisterPSM Exit
2019/01/01-15:12:33.982	BthPS3EvtDriverContextCleanup	TRACE_LEVEL_INFORMATION	BthPS3EvtDriverContextCleanup Entry
2019/01/01-15:12:37.071	DriverEntry	TRACE_LEVEL_INFORMATION	DriverEntry Entry
2019/01/01-15:12:37.071	DriverEntry	TRACE_LEVEL_INFORMATION	DriverEntry Exit
2019/01/01-15:12:37.071	BthPS3EvtDeviceAdd	TRACE_LEVEL_INFORMATION	BthPS3EvtDeviceAdd Entry
2019/01/01-15:12:37.072	BthPS3EvtDeviceAdd	TRACE_LEVEL_INFORMATION	BthPS3EvtDeviceAdd Exit
2019/01/01-15:12:37.072	BthPS3RetrieveLocalInfo	TRACE_LEVEL_VERBOSE	BthPS3RetrieveLocalInfo Entry
2019/01/01-15:12:37.072	BthPS3RetrieveLocalInfo	TRACE_LEVEL_VERBOSE	BthPS3RetrieveLocalInfo Exit
2019/01/01-15:12:37.072	BthPS3RegisterPSM	TRACE_LEVEL_VERBOSE	BthPS3RegisterPSM Entry
2019/01/01-15:12:37.072	BthPS3RegisterPSM	TRACE_LEVEL_INFORMATION	++ Trying to register PSM 20563
2019/01/01-15:12:37.072	BthPS3RegisterPSM	TRACE_LEVEL_INFORMATION	++ Got PSM 20563
2019/01/01-15:12:37.072	BthPS3RegisterPSM	TRACE_LEVEL_VERBOSE	BthPS3RegisterPSM Exit
2019/01/01-15:12:37.072	BthPS3RegisterL2CAPServer	TRACE_LEVEL_VERBOSE	BthPS3RegisterL2CAPServer Entry
2019/01/01-15:12:37.072	BthPS3IndicationCallback	TRACE_LEVEL_VERBOSE	BthPS3IndicationCallback Entry
2019/01/01-15:12:37.072	BthPS3IndicationCallback	TRACE_LEVEL_VERBOSE	BthPS3IndicationCallback Exit
2019/01/01-15:12:37.072	BthPS3RegisterL2CAPServer	TRACE_LEVEL_VERBOSE	BthPS3RegisterL2CAPServer Exit

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/9a0cde3c-1002-4d22-baf5-c52f9f1aba30-image.png)

Jan 1, 2019, 3:35 PM (https://localhost/post/1005)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Oh my! 😲 This actually worked 👀

I've currently set up a `BTHUSB` lower filter driver simply looking for an incoming L2CAP connection request with the dredded PSM `0x11` and patching it to an artificial fixed value (currently `0x5053`)

```
UrbFunctionBulkInTransferCompleted      2019/01/01-15:26:42.733 TRACE_LEVEL_VERBOSE     UrbFunctionBulkInTra
nsferCompleted Entry
UrbFunctionBulkInTransferCompleted      2019/01/01-15:26:42.733 TRACE_LEVEL_INFORMATION >> L2CAP_Connection_
Request
UrbFunctionBulkInTransferCompleted      2019/01/01-15:26:42.733 TRACE_LEVEL_INFORMATION ++ PSM: 0x11
UrbFunctionBulkInTransferCompleted      2019/01/01-15:26:42.733 TRACE_LEVEL_INFORMATION ++ Patching PSM to 0
x5053
```

This grants us a way around `bthport.sys!BthIsSystemPSM` denying the connection right away, so far so good! But that's not enough; how should the Bluetooth stack now know what to do with a non-existent PSM? Well, we need to register a custom Profile Driver for it, of course! 😆

```
2019/01/01-15:26:31.001 TRACE_LEVEL_INFORMATION ++ Trying to register PSM 0x5053
2019/01/01-15:26:31.001 TRACE_LEVEL_INFORMATION ++ Got PSM 0x5053
2019/01/01-15:26:31.001 TRACE_LEVEL_VERBOSE     BthPS3RegisterPSM Exit
2019/01/01-15:26:31.001 TRACE_LEVEL_VERBOSE     BthPS3RegisterL2CAPServer Entry
2019/01/01-15:26:31.001 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Entry
2019/01/01-15:26:31.001 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Exit
2019/01/01-15:26:31.001 TRACE_LEVEL_VERBOSE     BthPS3RegisterL2CAPServer Exit
2019/01/01-15:26:42.763 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Entry
2019/01/01-15:26:42.763 TRACE_LEVEL_INFORMATION BthPS3IndicationCallback ++ IndicationRemoteConnect
2019/01/01-15:26:42.763 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Exit
```

And we actually receive the connection request in our own profile driver now 😳

That is... *very* interesting! Let's see where the road leads me from here on.

Jan 1, 2019, 5:43 PM (https://localhost/post/1006)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

> PSMs shall be odd and the least significant bit of the most significant byte shall be zero, hence the following ranges do not contain valid PSMs: 0x0100-0x01FF, 0x0300-0x03FF, 0x0500-0x05FF, 0x0700-0x07FF, 0x0900-0x09FF, 0x0B00-0x0BFF, 0x0D00-0x0DFF, 0x0F00-0x0FFF. All even values are also not valid as PSMs.

Jan 4, 2019, 4:46 PM (https://localhost/post/1011)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


414n (https://localhost/user/414n)
(https://localhost/user/414n)

Really interesting, keep up the good work!

Am I right in assuming these are research notes for an Airbender successor?

Jan 4, 2019, 5:54 PM (https://localhost/post/1012)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@414n (https://forums.vigem.org/uid/37) not quite, this is already a successor successor 😆

The AirBender successor is code-named WireShock and already exists in the lab, has working support for fake DS3s and doesn't require additional software to function (AirBender needs Shibari to actually function).

However, WireShock is - like AirBender - a USB function driver, which means it needs to *replace* the entire default Windows Bluetooth driver which means your Bluetooth host gets unusable for anything else that is not a DualShock. That's the same technique ScpToolkit used.

This research is my attempt to discover "the holy grail"; a solution which keeps the existing Bluetooth drivers in place so headsets, keyboards etc. keep working but allows transparent co-existence with DualShock/Nav/Move 3 devices.

Jan 5, 2019, 6:25 PM (https://localhost/post/1014)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Right, now that we've gotten so far to send back a connection response, the second channel pops up and requires a "proxy-PSM" as well:

```
UrbFunctionBulkInTransferCompleted      2019/01/05-18:11:16.983 TRACE_LEVEL_INFORMATION >> L2CAP_Connection_
Request
UrbFunctionBulkInTransferCompleted      2019/01/05-18:11:16.983 TRACE_LEVEL_INFORMATION ++ PSM: 0x13
```

May I just add that writing a Bluetooth Profile Driver takes forever even if you can steal big chunks of code from the Windows driver samples (https://github.com/Microsoft/Windows-driver-samples/tree/master/bluetooth/bthecho) 😵

Jan 5, 2019, 9:21 PM (https://localhost/post/1015)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Oh yeah, registering a proxy PSM for `PSM_HID_INTERRUPT` as well shoots us even further forward:

```
UrbFunctionInterruptInTransferCompleted 2019/01/05-21:13:01.717 TRACE_LEVEL_INFORMATION HCI_Connection_Compl
ete_EV
UrbFunctionBulkInTransferCompleted      2019/01/05-21:13:01.742 TRACE_LEVEL_VERBOSE     UrbFunctionBulkInTra
nsferCompleted Entry
UrbFunctionBulkInTransferCompleted      2019/01/05-21:13:01.742 TRACE_LEVEL_INFORMATION >> L2CAP_Connection_
Request
UrbFunctionBulkInTransferCompleted      2019/01/05-21:13:01.742 TRACE_LEVEL_INFORMATION ++ PSM: 0x11
UrbFunctionBulkInTransferCompleted      2019/01/05-21:13:01.742 TRACE_LEVEL_INFORMATION ++ Patching PSM to 0
x5053
UrbFunctionBulkInTransferCompleted      2019/01/05-21:13:01.763 TRACE_LEVEL_VERBOSE     UrbFunctionBulkInTra
nsferCompleted Entry
UrbFunctionBulkInTransferCompleted      2019/01/05-21:13:01.763 TRACE_LEVEL_INFORMATION >> L2CAP_Configurati
on_Request
UrbFunctionBulkInTransferCompleted      2019/01/05-21:13:01.765 TRACE_LEVEL_VERBOSE     UrbFunctionBulkInTra
nsferCompleted Entry
UrbFunctionBulkInTransferCompleted      2019/01/05-21:13:01.765 TRACE_LEVEL_INFORMATION >> L2CAP_Configurati
on_Response
UrbFunctionBulkInTransferCompleted      2019/01/05-21:13:01.771 TRACE_LEVEL_VERBOSE     UrbFunctionBulkInTra
nsferCompleted Entry
UrbFunctionBulkInTransferCompleted      2019/01/05-21:13:01.771 TRACE_LEVEL_INFORMATION >> L2CAP_Connection_
Request
UrbFunctionBulkInTransferCompleted      2019/01/05-21:13:01.771 TRACE_LEVEL_INFORMATION ++ PSM: 0x13
UrbFunctionBulkInTransferCompleted      2019/01/05-21:13:01.771 TRACE_LEVEL_INFORMATION ++ Patching PSM to 0
x5055
UrbFunctionBulkInTransferCompleted      2019/01/05-21:13:01.781 TRACE_LEVEL_VERBOSE     UrbFunctionBulkInTra
nsferCompleted Entry
UrbFunctionBulkInTransferCompleted      2019/01/05-21:13:01.781 TRACE_LEVEL_INFORMATION >> L2CAP_Configurati
on_Request
UrbFunctionBulkInTransferCompleted      2019/01/05-21:13:01.783 TRACE_LEVEL_VERBOSE     UrbFunctionBulkInTra
nsferCompleted Entry
UrbFunctionBulkInTransferCompleted      2019/01/05-21:13:01.783 TRACE_LEVEL_INFORMATION >> L2CAP_Configurati
on_Response
```

Which generates some more noise in the profile driver:

```
2019/01/05-21:13:01.379 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Entry
2019/01/05-21:13:01.379 TRACE_LEVEL_INFORMATION BthPS3IndicationCallback ++ IndicationRemoteConnect
2019/01/05-21:13:01.379 TRACE_LEVEL_VERBOSE     BthPS3SendConnectResponse Entry
2019/01/05-21:13:01.379 TRACE_LEVEL_VERBOSE     BthPS3ConnectionIndicationCallback Entry
2019/01/05-21:13:01.379 TRACE_LEVEL_VERBOSE     BthPS3ConnectionIndicationCallback Exit
2019/01/05-21:13:01.379 TRACE_LEVEL_VERBOSE     BthPS3SendConnectResponse Exit (STATUS_SUCCESS (0x00000000))
2019/01/05-21:13:01.379 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Exit
2019/01/05-21:13:01.389 TRACE_LEVEL_VERBOSE     BthPS3RemoteConnectResponseCompletion Entry
2019/01/05-21:13:01.389 TRACE_LEVEL_INFORMATION Connection completion, status: STATUS_SUCCESS (0x00000000)
2019/01/05-21:13:01.389 TRACE_LEVEL_INFORMATION Connection established with client
2019/01/05-21:13:01.389 TRACE_LEVEL_INFORMATION Connection completed, connection: 0xFFFFFA80089CC0C0
2019/01/05-21:13:01.389 TRACE_LEVEL_VERBOSE     BthPS3RemoteConnectResponseCompletion Exit
2019/01/05-21:13:01.395 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Entry
2019/01/05-21:13:01.395 TRACE_LEVEL_INFORMATION BthPS3IndicationCallback ++ IndicationRemoteConnect
2019/01/05-21:13:01.395 TRACE_LEVEL_VERBOSE     BthPS3SendConnectResponse Entry
2019/01/05-21:13:01.395 TRACE_LEVEL_VERBOSE     BthPS3SendConnectResponse Exit (STATUS_SUCCESS (0x00000000))
2019/01/05-21:13:01.395 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Exit
2019/01/05-21:13:01.395 TRACE_LEVEL_VERBOSE     BthPS3ConnectionIndicationCallback Entry
2019/01/05-21:13:01.395 TRACE_LEVEL_VERBOSE     BthPS3ConnectionIndicationCallback Exit
2019/01/05-21:13:01.413 TRACE_LEVEL_VERBOSE     BthPS3RemoteConnectResponseCompletion Entry
2019/01/05-21:13:01.413 TRACE_LEVEL_INFORMATION Connection completion, status: STATUS_DEVICE_NOT_CONNECTED
(0xC000009D)
2019/01/05-21:13:01.413 TRACE_LEVEL_VERBOSE     BthPS3RemoteConnectResponseCompletion Exit
```

Now ofc. the state machine I ripped off the `bthecho` sample driver goes crazy here and the connection drops but both channels connection requests actually bubble up to our driver, that's good news 🙂

Jan 6, 2019, 2:50 PM (https://localhost/post/1016) □
□ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 □
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Btw. if you attempt to register one of the "forbidden" PSMs within your profile driver like so:

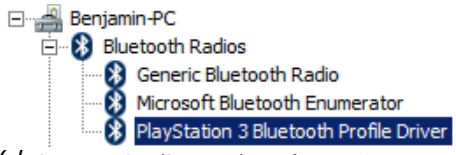
```
DevCtx->Header.ProfileDrvInterface.BthReuseBrb(
        &(DevCtx->RegisterUnregisterBrb),
        BRB_REGISTER_PSM
    );

brb = (struct _BRB_PSM *)
        &(DevCtx->RegisterUnregisterBrb);

brb->Psm = PSM_HID_CONTROL; // LOL, nope

status = BthPS3SendBrbSynchronously(
        DevCtx->Header.IoTarget,
        DevCtx->Header.Request,
        (PBRB)brb,
        sizeof(*brb)
);
```

the system crashes 😆 no NT_STATUS failure code, you'll be sent straight to hell. So, uh, don't do that 🙃

Jan 8, 2019, 6:42 PM (https://localhost/post/1017)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

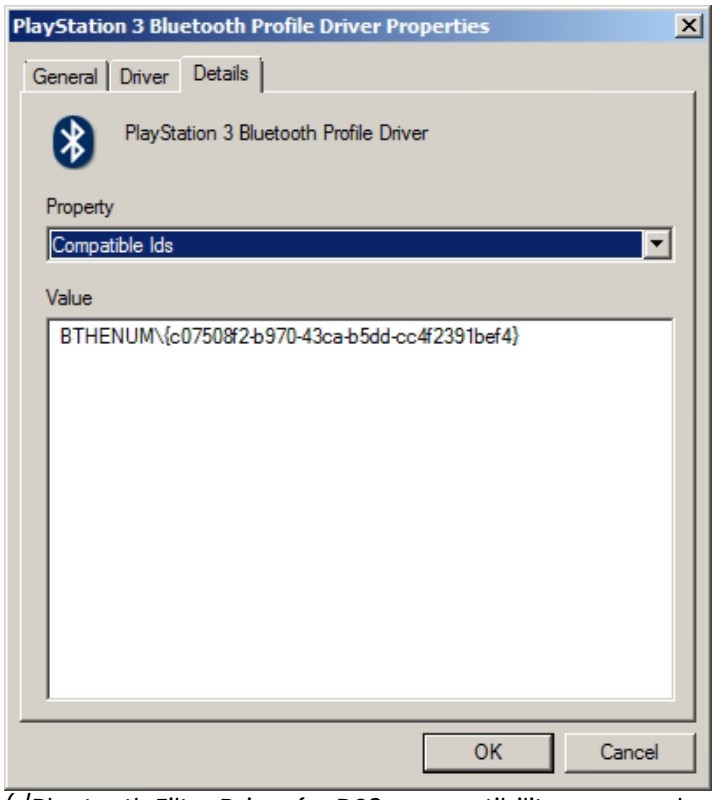
nefarius (https://localhost/user/nefarius) (https://localhost/user/nefarius)

This is how the profile driver could look like, notice the original host driver still being in place:

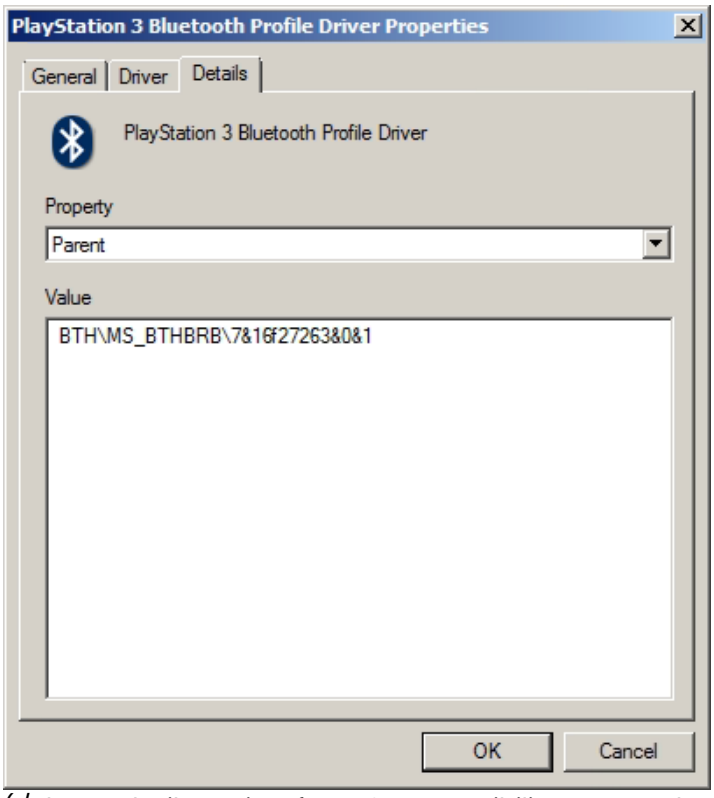


(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/773f36f0-6910-4c26-9450-888fe4875590-image.png)

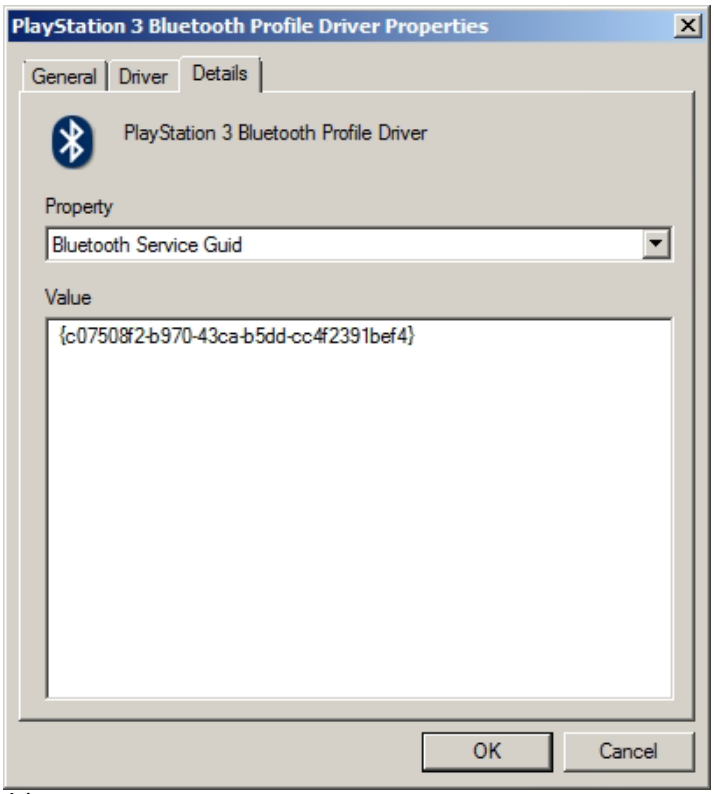
The Hardware ID would be `BTHENUM\{CUSTOM_SERVICE_GUID}` where in my lab example I simply recycled the one `bthecho` uses:



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/a1661077-ee57-467e-af06-1f96fd6e12e1-image.png)



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/ba14d738-13b0-4557-b1ff-52e792f9f6a3-image.png)



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/43c9e941-7715-4309-9141-334c11c140f1-image.png)

The service GUID I registered with a WinAPI call to BluetoothSetLocalServiceInfo (https://msdn.microsoft.com/en-us/library/windows/desktop/bb870603%28v=vs.85%29.aspx):

```
DWORD SetBthServiceInfo(
    BOOLEAN bEnabled
    )
{
    DWORD err = ERROR_SUCCESS;
    BLUETOOTH_LOCAL_SERVICE_INFO SvcInfo = {0};
    SvcInfo.Enabled = bEnabled;

    if (FAILED(StringCbCopyW(SvcInfo.szName, sizeof(SvcInfo.szName), BthEchoSampleSvcName)))
    {
        printf("Copying svc name failed\n");
        goto exit;
    }

    if (ERROR_SUCCESS != (err = BluetoothSetLocalServiceInfo(
        NULL, //callee would select the first found radio
        &BTHECHOSAMPLE_SVC_GUID,
        0,
        &SvcInfo
        )))
    {
        printf("BluetoothSetLocalServiceInfo failed, err = %d\n", err);
        goto exit;
    }
exit:
    return err;
}
```

Again, simply taken from the Microsoft sample. I also noticed, that the `bthsrvinst` project links against `BluetoothApis.lib`, which bombs on Windows 7. Link against `Bthprops.lib` instead and it will work.

> Supported in Windows 8 and later versions of Windows.

Jan 8, 2019, 6:56 PM (https://localhost/post/1018)
□ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 □ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius) (https://localhost/user/nefarius)

😯

```
2019/01/08-18:50:55.893 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Entry
2019/01/08-18:50:55.893 TRACE_LEVEL_INFORMATION New connection for 5053 from AC7A4D2819AC arrived
2019/01/08-18:50:55.893 TRACE_LEVEL_VERBOSE     L2CAP_PS3_SendConnectResponse Entry
2019/01/08-18:50:55.893 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectResponsePendingCompleted Entry
2019/01/08-18:50:55.893 TRACE_LEVEL_INFORMATION Connection PENDING completed with status: STATUS_SUCCESS (0x
00000000)
2019/01/08-18:50:55.893 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectResponsePendingCompleted Exit
2019/01/08-18:50:55.893 TRACE_LEVEL_VERBOSE     BthPS3ConnectionIndicationCallback Entry
2019/01/08-18:50:55.893 TRACE_LEVEL_VERBOSE     BthPS3ConnectionIndicationCallback Exit
2019/01/08-18:50:55.893 TRACE_LEVEL_VERBOSE     L2CAP_PS3_SendConnectResponse Exit (STATUS_SUCCESS (0x000000
00))
2019/01/08-18:50:55.893 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Exit
2019/01/08-18:50:55.904 TRACE_LEVEL_VERBOSE     BthPS3RemoteConnectResponseCompletion Entry
2019/01/08-18:50:55.904 TRACE_LEVEL_INFORMATION Connection completion, status: STATUS_SUCCESS (0x00000000)
2019/01/08-18:50:55.904 TRACE_LEVEL_INFORMATION Connection established with client
2019/01/08-18:50:55.904 TRACE_LEVEL_INFORMATION Connection completed, connection: 0xFFFFFA8009F6C480
2019/01/08-18:50:55.904 TRACE_LEVEL_VERBOSE     BthPS3RemoteConnectResponseCompletion Exit
2019/01/08-18:50:55.911 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Entry
2019/01/08-18:50:55.911 TRACE_LEVEL_INFORMATION New connection for 5055 from AC7A4D2819AC arrived
2019/01/08-18:50:55.911 TRACE_LEVEL_VERBOSE     L2CAP_PS3_SendConnectResponse Entry
2019/01/08-18:50:55.911 TRACE_LEVEL_VERBOSE     L2CAP_PS3_SendConnectResponse Exit (STATUS_SUCCESS (0x000000
00))
2019/01/08-18:50:55.911 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Exit
2019/01/08-18:50:55.911 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectResponsePendingCompleted Entry
2019/01/08-18:50:55.911 TRACE_LEVEL_INFORMATION Connection PENDING completed with status: STATUS_SUCCESS (0x
00000000)
2019/01/08-18:50:55.911 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectResponsePendingCompleted Exit
2019/01/08-18:50:55.911 TRACE_LEVEL_VERBOSE     BthPS3ConnectionIndicationCallback Entry
2019/01/08-18:50:55.911 TRACE_LEVEL_VERBOSE     BthPS3ConnectionIndicationCallback Exit
2019/01/08-18:50:55.927 TRACE_LEVEL_VERBOSE     BthPS3RemoteConnectResponseCompletion Entry
```

Right, so the connection handshake works for both Control and Interrupt channel, now I need to copypasta *a ton* of code to send and respond to the configuration requests. And extend the state machine to handle two channels instead of one like the example code intended. Oh dear 👀

Jan 8, 2019, 7:12 PM (https://localhost/post/1019) □
□ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 □
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Nope, wrong assumption. The profile driver doesn't craft configuration requests, the parent driver does.

Sniff-log from under `BTHUSB`:

```
2019/01/08-19:06:14.202 TRACE_LEVEL_INFORMATION >> L2CAP_Connection_Request
2019/01/08-19:06:14.233 TRACE_LEVEL_INFORMATION << L2CAP_Connection_Response (Response: 01)
2019/01/08-19:06:14.233 TRACE_LEVEL_INFORMATION << L2CAP_Connection_Response (Response: 01)
2019/01/08-19:06:14.233 TRACE_LEVEL_INFORMATION << L2CAP_Connection_Response (Response: 00)
2019/01/08-19:06:14.233 TRACE_LEVEL_INFORMATION << L2CAP_Configuration_Request
2019/01/08-19:06:14.245 TRACE_LEVEL_INFORMATION >> L2CAP_Configuration_Request
2019/01/08-19:06:14.245 TRACE_LEVEL_INFORMATION << L2CAP_Configuration_Response
2019/01/08-19:06:14.247 TRACE_LEVEL_INFORMATION >> L2CAP_Configuration_Response
2019/01/08-19:06:14.253 TRACE_LEVEL_INFORMATION >> L2CAP_Connection_Request
2019/01/08-19:06:14.253 TRACE_LEVEL_INFORMATION << L2CAP_Connection_Response (Response: 01)
2019/01/08-19:06:14.253 TRACE_LEVEL_INFORMATION << L2CAP_Connection_Response (Response: 01)
2019/01/08-19:06:14.253 TRACE_LEVEL_INFORMATION << L2CAP_Connection_Response (Response: 00)
2019/01/08-19:06:14.253 TRACE_LEVEL_INFORMATION << L2CAP_Configuration_Request
2019/01/08-19:06:14.266 TRACE_LEVEL_INFORMATION >> L2CAP_Configuration_Request
2019/01/08-19:06:14.266 TRACE_LEVEL_INFORMATION << L2CAP_Configuration_Response
2019/01/08-19:06:14.267 TRACE_LEVEL_INFORMATION >> L2CAP_Configuration_Response
2019/01/08-19:06:14.275 TRACE_LEVEL_INFORMATION >> L2CAP_Disconnection_Request
2019/01/08-19:06:14.281 TRACE_LEVEL_INFORMATION >> L2CAP_Disconnection_Request
```

That's both cool and frightening; hopefully the host knows what it's doing 😜

Also, why is PENDING sent twice per channel 🤔 did I do that or the host...

EDIT: I did that, no need for it, the parent driver has everything under control 😏

Jan 8, 2019, 8:05 PM (https://localhost/post/1020)
□ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 □ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius) (https://localhost/user/nefarius)

Sniffing intensifies 😏

```
2019/01/08-20:04:06.318 TRACE_LEVEL_INFORMATION >> L2CAP_Connection_Request [Code: 0x02, Identifier: 0x01, L
ength: 4, PSM: 0x5053, SCID: 0x1440]
2019/01/08-20:04:06.349 TRACE_LEVEL_INFORMATION << L2CAP_Connection_Response [Code: 0x03, Identifier: 0x01,
Length: 8, DCID: 0x0000, SCID: 0x1440, Result: 0x0001, Status: 0x0000]
2019/01/08-20:04:06.349 TRACE_LEVEL_INFORMATION << L2CAP_Connection_Response [Code: 0x03, Identifier: 0x01,
Length: 8, DCID: 0x0000, SCID: 0x1440, Result: 0x0001, Status: 0x0000]
2019/01/08-20:04:06.349 TRACE_LEVEL_INFORMATION << L2CAP_Connection_Response [Code: 0x03, Identifier: 0x01,
Length: 8, DCID: 0x0040, SCID: 0x1440, Result: 0x0000, Status: 0x0000]
2019/01/08-20:04:06.349 TRACE_LEVEL_INFORMATION << L2CAP_Configuration_Request [Code: 0x04, Identifier: 0x0
1, Length: 8, DCID: 0x1440, Flags: 0x0000, Options: 0x02A00201]
2019/01/08-20:04:06.360 TRACE_LEVEL_INFORMATION >> L2CAP_Configuration_Request [Code: 0x04, Identifier: 0x0
2, Length: 4, DCID: 0x0040, Flags: 0x0000, Options: 0x00001000]
2019/01/08-20:04:06.361 TRACE_LEVEL_INFORMATION << L2CAP_Configuration_Response [Code: 0x05, Identifier: 0x0
2, Length: 6, SCID: 0x1440, Flags: 0x0000, Result: 0x0000, Options: 0x0000]
2019/01/08-20:04:06.362 TRACE_LEVEL_INFORMATION >> L2CAP_Configuration_Response [Code: 0x05, Identifier: 0x0
1, Length: 6, SCID: 0x0040, Flags: 0x0000, Result: 0x0000, Options: 0x0052]
2019/01/08-20:04:06.369 TRACE_LEVEL_INFORMATION >> L2CAP_Connection_Request [Code: 0x02, Identifier: 0x03, L
ength: 4, PSM: 0x5055, SCID: 0x1481]
2019/01/08-20:04:06.369 TRACE_LEVEL_INFORMATION << L2CAP_Connection_Response [Code: 0x03, Identifier: 0x03,
Length: 8, DCID: 0x0000, SCID: 0x1481, Result: 0x0001, Status: 0x0000]
2019/01/08-20:04:06.369 TRACE_LEVEL_INFORMATION << L2CAP_Connection_Response [Code: 0x03, Identifier: 0x03,
Length: 8, DCID: 0x0000, SCID: 0x1481, Result: 0x0001, Status: 0x0000]
2019/01/08-20:04:06.369 TRACE_LEVEL_INFORMATION << L2CAP_Connection_Response [Code: 0x03, Identifier: 0x03,
Length: 8, DCID: 0x0041, SCID: 0x1481, Result: 0x0000, Status: 0x0000]
2019/01/08-20:04:06.369 TRACE_LEVEL_INFORMATION << L2CAP_Configuration_Request [Code: 0x04, Identifier: 0x0
2, Length: 8, DCID: 0x1481, Flags: 0x0000, Options: 0x02A00201]
2019/01/08-20:04:06.380 TRACE_LEVEL_INFORMATION >> L2CAP_Configuration_Request [Code: 0x04, Identifier: 0x0
4, Length: 28, DCID: 0x0041, Flags: 0x0000, Options: 0x02001603]
2019/01/08-20:04:06.381 TRACE_LEVEL_INFORMATION << L2CAP_Configuration_Response [Code: 0x05, Identifier: 0x0
4, Length: 30, SCID: 0x1481, Flags: 0x0000, Result: 0x0001, Options: 0x1603]
2019/01/08-20:04:06.383 TRACE_LEVEL_INFORMATION >> L2CAP_Configuration_Response [Code: 0x05, Identifier: 0x0
2, Length: 6, SCID: 0x0041, Flags: 0x0000, Result: 0x0000, Options: 0x0052]
2019/01/08-20:04:06.389 TRACE_LEVEL_INFORMATION >> L2CAP_Disconnection_Request [Code: 0x06, Identifier: 0x0
5, Length: 4, DCID: 0x0041, SCID: 0x1481]
2019/01/08-20:04:06.389 TRACE_LEVEL_INFORMATION << L2CAP_Disconnection_Response [Code: 0x07, Identifier: 0x0
5, Length: 4, DCID: 0x0041, SCID: 0x1481]
2019/01/08-20:04:06.399 TRACE_LEVEL_INFORMATION >> L2CAP_Disconnection_Request [Code: 0x06, Identifier: 0x0
6, Length: 4, DCID: 0x0040, SCID: 0x1440]
2019/01/08-20:04:06.399 TRACE_LEVEL_INFORMATION << L2CAP_Disconnection_Response [Code: 0x07, Identifier: 0x0
6, Length: 4, DCID: 0x0040, SCID: 0x1440]
```

L2CAP Channel Configuration

MTU

A successful agreement on MTU value `L2CAP_MAX_MTU` :

```
<< L2CAP_Configuration_Request [Code: 0x04, Identifier: 0x15, Length: 8, DCID: 0x3240, Flags: 0x0000, Option
s: 0xFFFF0201]
>> L2CAP_Configuration_Request [Code: 0x04, Identifier: 0x02, Length: 4, DCID: 0x0040, Flags: 0x0000, Option
s: 0x02010000]
<< L2CAP_Configuration_Response [Code: 0x05, Identifier: 0x02, Length: 6, SCID: 0x3240, Flags: 0x0000, Resul
t: 0x0000, Options: 0x0000]
>> L2CAP_Configuration_Response [Code: 0x05, Identifier: 0x15, Length: 10, SCID: 0x0040, Flags: 0x0000, Resu
lt: 0x0000, Options: 0x0201]
<< L2CAP_Configuration_Request [Code: 0x04, Identifier: 0x16, Length: 8, DCID: 0x3281, Flags: 0x0000, Option
s: 0xFFFF0201]
>> L2CAP_Configuration_Response [Code: 0x05, Identifier: 0x16, Length: 10, SCID: 0x0041, Flags: 0x0000, Resu
lt: 0x0000, Options: 0x0201]
```

QOS

Controller and host currently can't agree on QUALITY OF SERVICE (QOS) OPTION.

Option `0x02001603` is translated to: `0x03` (QoS option type) with length of 22 (`0x16`) and requested option is `0x0200` (`0x02` = *Service Type* as Guaranteed, `L2CAP_FLOW_SERVICE_TYPE_GUARANTEED`)

```
>> L2CAP_Configuration_Request [Code: 0x04, Identifier: 0x04, Length: 28, DCID: 0x0041, Flags: 0x0000, Optio
ns: 0x02001603]
<< L2CAP_Configuration_Response [Code: 0x05, Identifier: 0x04, Length: 30, SCID: 0x3281, Flags: 0x0000, Resu
lt: 0x0001, Options: 0x1603]
```

Jan 8, 2019, 9:09 PM (https://localhost/post/1022)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

> ***Ladies and gentlemen, we got him***

The DS3 is connected to standard Windows Bluetooth Stack 🎉

I must be dreaming 😂 it actually works, my DS3 is connected to an USB Bluetooth dongle running the standard Windows Bluetooth Stack, the filter and the profile driver! `git commit && git push` 😆

Lower filter log

```
2019/01/08-21:02:33.479 >> L2CAP_Connection_Request [Code: 0x02, Identifier: 0x01, Length: 4, PSM: 0x5053, S
CID: 0x42C0]
2019/01/08-21:02:33.491 << L2CAP_Connection_Response [Code: 0x03, Identifier: 0x01, Length: 8, DCID: 0x0000,
SCID: 0x42C0, Result: 0x0001, Status: 0x0000]
2019/01/08-21:02:33.491 << L2CAP_Connection_Response [Code: 0x03, Identifier: 0x01, Length: 8, DCID: 0x0040,
SCID: 0x42C0, Result: 0x0000, Status: 0x0000]
2019/01/08-21:02:33.491 << L2CAP_Configuration_Request [Code: 0x04, Identifier: 0x03, Length: 8, DCID: 0x42C
0, Flags: 0x0000, Options: 0xFFFF0201]
2019/01/08-21:02:33.497 >> L2CAP_Configuration_Request [Code: 0x04, Identifier: 0x02, Length: 4, DCID: 0x004
0, Flags: 0x0000, Options: 0x00010004]
2019/01/08-21:02:33.497 << L2CAP_Configuration_Response [Code: 0x05, Identifier: 0x02, Length: 6, SCID: 0x42
C0, Flags: 0x0000, Result: 0x0000, Options: 0x0000]
2019/01/08-21:02:33.499 >> L2CAP_Configuration_Response [Code: 0x05, Identifier: 0x03, Length: 10, SCID: 0x0
040, Flags: 0x0000, Result: 0x0000, Options: 0x0201]
2019/01/08-21:02:33.507 >> L2CAP_Connection_Request [Code: 0x02, Identifier: 0x03, Length: 4, PSM: 0x5055, S
CID: 0x4301]
2019/01/08-21:02:33.507 << L2CAP_Connection_Response [Code: 0x03, Identifier: 0x03, Length: 8, DCID: 0x0000,
SCID: 0x4301, Result: 0x0001, Status: 0x0000]
2019/01/08-21:02:33.507 << L2CAP_Connection_Response [Code: 0x03, Identifier: 0x03, Length: 8, DCID: 0x0041,
SCID: 0x4301, Result: 0x0000, Status: 0x0000]
2019/01/08-21:02:33.507 << L2CAP_Configuration_Request [Code: 0x04, Identifier: 0x04, Length: 8, DCID: 0x430
1, Flags: 0x0000, Options: 0xFFFF0201]
2019/01/08-21:02:33.516 >> L2CAP_Configuration_Request [Code: 0x04, Identifier: 0x04, Length: 28, DCID: 0x00
41, Flags: 0x0000, Options: 0x02001603]
2019/01/08-21:02:33.516 << L2CAP_Configuration_Response [Code: 0x05, Identifier: 0x04, Length: 6, SCID: 0x43
01, Flags: 0x0000, Result: 0x0000, Options: 0x0000]
2019/01/08-21:02:33.519 >> L2CAP_Configuration_Response [Code: 0x05, Identifier: 0x04, Length: 10, SCID: 0x0
041, Flags: 0x0000, Result: 0x0000, Options: 0x0201]
```

Profile driver log

```
2019/01/08-21:02:33.201 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Entry
2019/01/08-21:02:33.201 TRACE_LEVEL_INFORMATION New connection for PSM 0x5053 from AC7A4D2819AC arrived
2019/01/08-21:02:33.201 TRACE_LEVEL_VERBOSE     L2CAP_PS3_SendConnectResponse Entry
2019/01/08-21:02:33.201 TRACE_LEVEL_VERBOSE     BthPS3ConnectionIndicationCallback Entry
2019/01/08-21:02:33.201 TRACE_LEVEL_VERBOSE     BthPS3ConnectionIndicationCallback Exit
2019/01/08-21:02:33.201 TRACE_LEVEL_VERBOSE     L2CAP_PS3_SendConnectResponse Exit (STATUS_SUCCESS (0x000000
00))
2019/01/08-21:02:33.201 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Exit
2019/01/08-21:02:33.209 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectResponseCompleted Entry
2019/01/08-21:02:33.209 TRACE_LEVEL_INFORMATION Connection completion, status: STATUS_SUCCESS (0x00000000)
2019/01/08-21:02:33.209 TRACE_LEVEL_INFORMATION Connection established with client
2019/01/08-21:02:33.209 TRACE_LEVEL_INFORMATION Connection completed, connection: 0xFFFFFA8009A7A5E0
2019/01/08-21:02:33.209 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectResponseCompleted Exit
2019/01/08-21:02:33.216 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Entry
2019/01/08-21:02:33.216 TRACE_LEVEL_INFORMATION New connection for PSM 0x5055 from AC7A4D2819AC arrived
2019/01/08-21:02:33.216 TRACE_LEVEL_VERBOSE     L2CAP_PS3_SendConnectResponse Entry
2019/01/08-21:02:33.216 TRACE_LEVEL_VERBOSE     L2CAP_PS3_SendConnectResponse Exit (STATUS_SUCCESS (0x000000
00))
2019/01/08-21:02:33.216 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Exit
2019/01/08-21:02:33.216 TRACE_LEVEL_VERBOSE     BthPS3ConnectionIndicationCallback Entry
2019/01/08-21:02:33.216 TRACE_LEVEL_VERBOSE     BthPS3ConnectionIndicationCallback Exit
2019/01/08-21:02:33.225 TRACE_LEVEL_VERBOSE     BthPS3ConnectionIndicationCallback Entry
2019/01/08-21:02:33.225 TRACE_LEVEL_INFORMATION BthPS3ConnectionIndicationCallback ++ IndicationRemoteConfig
Request
2019/01/08-21:02:33.225 TRACE_LEVEL_VERBOSE     BthPS3ConnectionIndicationCallback Exit
2019/01/08-21:02:33.228 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectResponseCompleted Entry
2019/01/08-21:02:33.228 TRACE_LEVEL_INFORMATION Connection completion, status: STATUS_SUCCESS (0x00000000)
2019/01/08-21:02:33.228 TRACE_LEVEL_INFORMATION Connection established with client
2019/01/08-21:02:33.228 TRACE_LEVEL_INFORMATION Connection completed, connection: 0xFFFFFA8009D890C0
2019/01/08-21:02:33.228 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectResponseCompleted Exit
```

Jan 9, 2019, 7:45 PM (https://localhost/post/1025)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

This is the last (still working) Chinese ripoff-DS3 I currently possess and it connects as well 🤠

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/8b7e4079-2500-48e1-a869-73ab9d6f16a8-image-resized.png)

```
2019/01/09-19:39:23.848 >> L2CAP_Connection_Request [Code: 0x02, Identifier: 0x01, Length: 4, PSM: 0x5053, S
CID: 0x0040]
2019/01/09-19:39:23.858 << L2CAP_Connection_Response [Code: 0x03, Identifier: 0x01, Length: 8, DCID: 0x0000,
SCID: 0x0040, Result: 0x0001, Status: 0x0000]
2019/01/09-19:39:23.858 << L2CAP_Connection_Response [Code: 0x03, Identifier: 0x01, Length: 8, DCID: 0x0040,
SCID: 0x0040, Result: 0x0000, Status: 0x0000]
2019/01/09-19:39:23.858 << L2CAP_Configuration_Request [Code: 0x04, Identifier: 0x01, Length: 8, DCID: 0x004
0, Flags: 0x0000, Options: 0xFFFF0201]
2019/01/09-19:39:23.871 >> L2CAP_Configuration_Request [Code: 0x04, Identifier: 0x02, Length: 4, DCID: 0x004
0, Flags: 0x0000, Options: 0x00001000]
2019/01/09-19:39:23.871 << L2CAP_Configuration_Response [Code: 0x05, Identifier: 0x02, Length: 6, SCID: 0x00
40, Flags: 0x0000, Result: 0x0000, Options: 0x0000]
2019/01/09-19:39:23.873 >> L2CAP_Configuration_Response [Code: 0x05, Identifier: 0x01, Length: 10, SCID: 0x0
040, Flags: 0x0000, Result: 0x0000, Options: 0x0201]
2019/01/09-19:39:23.880 >> L2CAP_Connection_Request [Code: 0x02, Identifier: 0x03, Length: 4, PSM: 0x5055, S
CID: 0x0041]
2019/01/09-19:39:23.880 << L2CAP_Connection_Response [Code: 0x03, Identifier: 0x03, Length: 8, DCID: 0x0000,
SCID: 0x0041, Result: 0x0001, Status: 0x0000]
2019/01/09-19:39:23.880 << L2CAP_Connection_Response [Code: 0x03, Identifier: 0x03, Length: 8, DCID: 0x0041,
SCID: 0x0041, Result: 0x0000, Status: 0x0000]
2019/01/09-19:39:23.880 << L2CAP_Configuration_Request [Code: 0x04, Identifier: 0x02, Length: 8, DCID: 0x004
1, Flags: 0x0000, Options: 0xFFFF0201]
2019/01/09-19:39:23.893 >> L2CAP_Configuration_Request [Code: 0x04, Identifier: 0x04, Length: 4, DCID: 0x004
1, Flags: 0x0000, Options: 0x00001000]
2019/01/09-19:39:23.893 << L2CAP_Configuration_Response [Code: 0x05, Identifier: 0x04, Length: 6, SCID: 0x00
41, Flags: 0x0000, Result: 0x0000, Options: 0x0000]
2019/01/09-19:39:23.894 >> L2CAP_Configuration_Response [Code: 0x05, Identifier: 0x02, Length: 10, SCID: 0x0
041, Flags: 0x0000, Result: 0x0000, Options: 0x0201]
```

Jan 9, 2019, 9:13 PM (https://localhost/post/1026)

(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

DualShock 4 (Revision 1) connection sequence

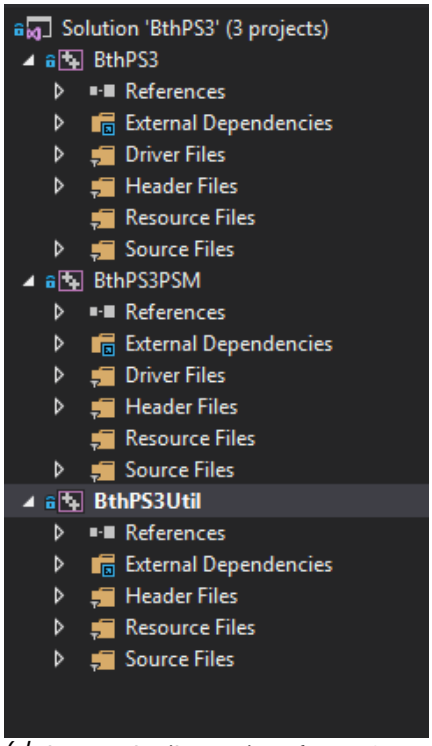
(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/759bd2c1-8fe3-4260-8dc5-5170dcfdb563-image-resized.png)

2019/01/09-21:11:02.588 << L2CAP_Connection_Request [Code: 0x02, Identifier: 0x02, Length: 4, PSM: 0x0001, S
CID: 0x0040]
2019/01/09-21:11:02.597 >> L2CAP_Connection_Response [Code: 0x03, Identifier: 0x02, Length: 8, DCID: 0x0040,
SCID: 0x0040, Result: 0x0001, Status: 0x0002]
2019/01/09-21:11:02.599 >> L2CAP_Connection_Response [Code: 0x03, Identifier: 0x02, Length: 8, DCID: 0x0040,
SCID: 0x0040, Result: 0x0000, Status: 0x0000]
2019/01/09-21:11:02.599 << L2CAP_Configuration_Request [Code: 0x04, Identifier: 0x03, Length: 8, DCID: 0x004
0, Flags: 0x0000, Options: 0x04000201]
2019/01/09-21:11:02.610 >> L2CAP_Configuration_Response [Code: 0x05, Identifier: 0x03, Length: 10, SCID: 0x0
040, Flags: 0x0000, Result: 0x0000, Options: 0x0201]
2019/01/09-21:11:02.612 >> L2CAP_Configuration_Request [Code: 0x04, Identifier: 0x01, Length: 8, DCID: 0x004
0, Flags: 0x0000, Options: 0x04000201]
2019/01/09-21:11:02.612 << L2CAP_Configuration_Response [Code: 0x05, Identifier: 0x01, Length: 6, SCID: 0x00
40, Flags: 0x0000, Result: 0x0000, Options: 0x0000]
2019/01/09-21:11:02.612 << L2CAP_Disconnection_Request [Code: 0x06, Identifier: 0x00, Length: 0, DCID: 0x350
F, SCID: 0x1903]
2019/01/09-21:11:02.623 << L2CAP_Disconnection_Request [Code: 0x06, Identifier: 0x00, Length: 1, DCID: 0x350
F, SCID: 0x1903]
2019/01/09-21:11:04.088 << L2CAP_Disconnection_Request [Code: 0x06, Identifier: 0x00, Length: 2, DCID: 0x350
F, SCID: 0x1903]
2019/01/09-21:11:04.449 << L2CAP_Disconnection_Request [Code: 0x06, Identifier: 0x00, Length: 3, DCID: 0x350
F, SCID: 0x1903]
2019/01/09-21:11:04.513 << L2CAP_Disconnection_Request [Code: 0x06, Identifier: 0x00, Length: 4, DCID: 0x350
F, SCID: 0x1903]
2019/01/09-21:11:04.718 << L2CAP_Disconnection_Request [Code: 0x06, Identifier: 0x00, Length: 5, DCID: 0x350
F, SCID: 0x1903]
2019/01/09-21:11:05.031 << L2CAP_Connection_Request [Code: 0x02, Identifier: 0x04, Length: 4, PSM: 0x0011, S
CID: 0x0041]
2019/01/09-21:11:05.069 >> L2CAP_Connection_Response [Code: 0x03, Identifier: 0x04, Length: 8, DCID: 0x0041,
SCID: 0x0041, Result: 0x0001, Status: 0x0002]
2019/01/09-21:11:05.091 >> L2CAP_Connection_Response [Code: 0x03, Identifier: 0x04, Length: 8, DCID: 0x0041,
SCID: 0x0041, Result: 0x0000, Status: 0x0000]
2019/01/09-21:11:05.091 << L2CAP_Configuration_Request [Code: 0x04, Identifier: 0x05, Length: 8, DCID: 0x004
1, Flags: 0x0000, Options: 0x02A00201]
2019/01/09-21:11:05.135 >> L2CAP_Configuration_Response [Code: 0x05, Identifier: 0x05, Length: 10, SCID: 0x0
041, Flags: 0x0000, Result: 0x0000, Options: 0x0201]
2019/01/09-21:11:05.156 >> L2CAP_Configuration_Request [Code: 0x04, Identifier: 0x02, Length: 8, DCID: 0x004
1, Flags: 0x0000, Options: 0x02A00201]
2019/01/09-21:11:05.156 << L2CAP_Configuration_Response [Code: 0x05, Identifier: 0x02, Length: 6, SCID: 0x00
41, Flags: 0x0000, Result: 0x0000, Options: 0x0000]
2019/01/09-21:11:05.156 << L2CAP_Connection_Request [Code: 0x02, Identifier: 0x06, Length: 4, PSM: 0x0013, S
CID: 0x0042]
2019/01/09-21:11:05.192 >> L2CAP_Connection_Response [Code: 0x03, Identifier: 0x06, Length: 8, DCID: 0x0042,
SCID: 0x0042, Result: 0x0001, Status: 0x0002]
2019/01/09-21:11:05.199 >> L2CAP_Connection_Response [Code: 0x03, Identifier: 0x06, Length: 8, DCID: 0x0042,
SCID: 0x0042, Result: 0x0000, Status: 0x0000]
2019/01/09-21:11:05.199 << L2CAP_Configuration_Request [Code: 0x04, Identifier: 0x07, Length: 8, DCID: 0x004
2, Flags: 0x0000, Options: 0x02A00201]
2019/01/09-21:11:05.209 >> L2CAP_Configuration_Response [Code: 0x05, Identifier: 0x07, Length: 10, SCID: 0x0
042, Flags: 0x0000, Result: 0x0000, Options: 0x0201]
2019/01/09-21:11:05.212 >> L2CAP_Configuration_Request [Code: 0x04, Identifier: 0x03, Length: 8, DCID: 0x004
2, Flags: 0x0000, Options: 0x02A00201]
2019/01/09-21:11:05.212 << L2CAP_Configuration_Response [Code: 0x05, Identifier: 0x03, Length: 6, SCID: 0x00
42, Flags: 0x0000, Result: 0x0000, Options: 0x0000]
2019/01/09-21:11:07.797 << L2CAP_Disconnection_Request [Code: 0x06, Identifier: 0x08, Length: 4, DCID: 0x004
0, SCID: 0x0040]
2019/01/09-21:11:07.801 >> L2CAP_Disconnection_Response [Code: 0x07, Identifier: 0x08, Length: 4, DCID: 0x00
40, SCID: 0x0040]

Jan 12, 2019, 12:31 AM (https://localhost/post/1029)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Oof, code base growing rapidly 😯



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/4e064261-c7a3-4eb8-8a13-c1fcfbd06181-image.png)

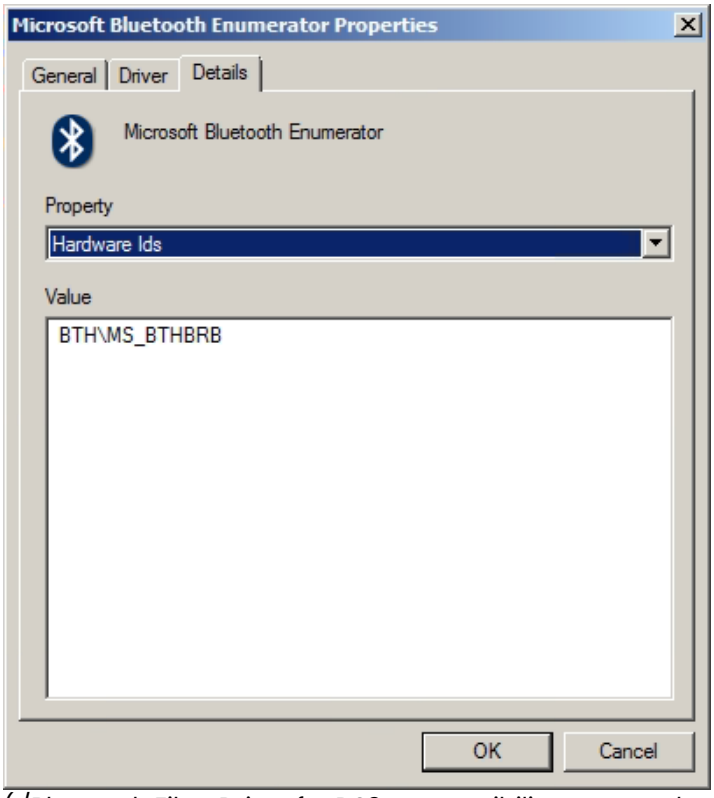
From top to bottom:

- Profile driver
- Filter driver
- Driver installation utility

Jan 12, 2019, 11:38 AM (https://localhost/post/1030)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Enum BTH - Microsoft Bluetooth Enumerator

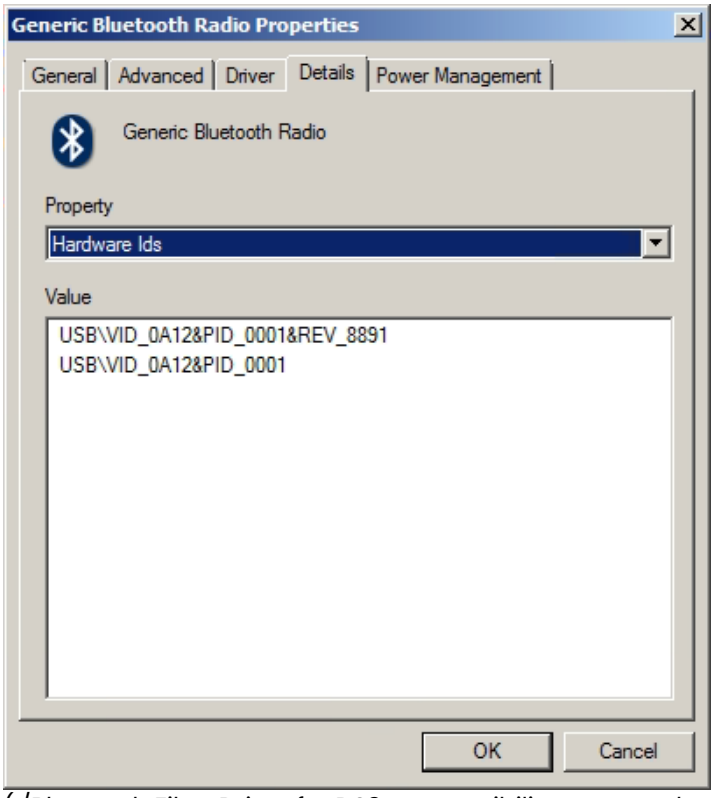


(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/ca5c635d-2be8-4358-b4d9-1849473af9f5-image.png)

(Default)	REG_SZ	(value not set)
Capabilities	REG_DWORD	0x00000080 (128)
Class	REG_SZ	Bluetooth
ClassGUID	REG_SZ	{e0cbf06c-cd8b-4647-bb8a-263b43f0f974}
CompatibleIDs	REG_MULTI_SZ	
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{4c5d34e0-110b-11e9-9a52-480fcf488337}
DeviceDesc	REG_SZ	@bth.inf,%bth\ms_bthbrb.devicedesc%;Microsoft Bluetooth Enumerator
Driver	REG_SZ	{e0cbf06c-cd8b-4647-bb8a-263b43f0f974}\0001
HardwareID	REG_MULTI_SZ	BTH\MS_BTHBRB
Mfg	REG_SZ	@bth.inf,%microsoft%;Microsoft
ParentIdPrefix	REG_SZ	8&be3621&0
Service	REG_SZ	BthEnum
UINumber	REG_DWORD	0x00000000 (0)

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/6ea3077d-93fc-4f16-8ddc-efe543a129cb-image.png)

Enum USB - Generic Bluetooth Radio

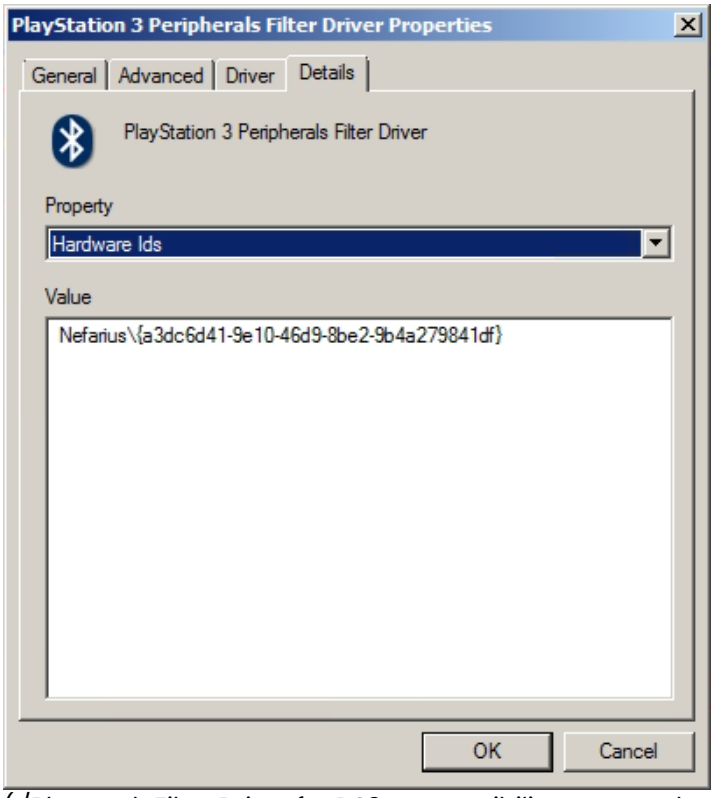


(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/d1de37d7-b6da-4a75-9dae-7595f9a13709-image.png)

(Default)	REG_SZ	(value not set)
Capabilities	REG_DWORD	0x00000084 (132)
Class	REG_SZ	Bluetooth
ClassGUID	REG_SZ	{e0cbf06c-cd8b-4647-bb8a-263b43f0f974}
CompatibleIDs	REG_MULTI_SZ	USB\Class_e0&SubClass_01&Prot_01 USB\Class_e0&SubClass_01 USB\Class_e0
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{4c5d34e0-110b-11e9-9a52-480fcf488337}
DeviceDesc	REG_SZ	Generic Bluetooth Radio
Driver	REG_SZ	{e0cbf06c-cd8b-4647-bb8a-263b43f0f974}\0000
HardwareID	REG_MULTI_SZ	USB\VID_0A12&PID_0001&REV_8891 USB\VID_0A12&PID_0001
LocationInformation	REG_SZ	Port_#0004.Hub_#0002
Mfg	REG_SZ	Cambridge Silicon Radio Ltd.
ParentIdPrefix	REG_SZ	7&16f27263&0
Service	REG_SZ	BTHUSB
UINumber	REG_DWORD	0x00000000 (0)

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/c6667e68-8eb4-4317-b746-8c8c579df759-image.png)

PlayStation 3 Peripherals Filter Driver

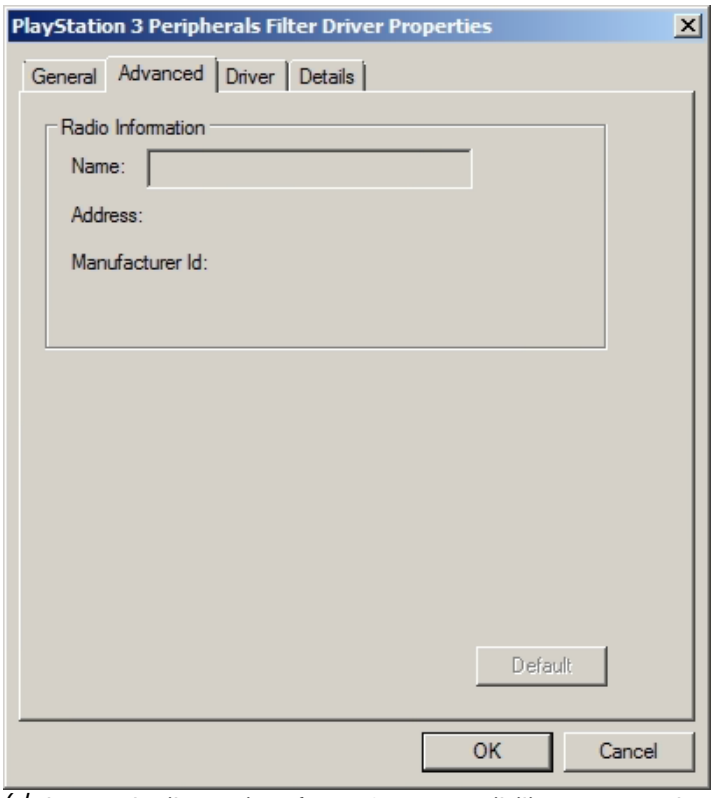


(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/97dc8e2f-53ec-42f6-882b-13a725649c6b-image.png)

(Default)	REG_SZ	(value not set)
Capabilities	REG_DWORD	0x00000000 (0)
Class	REG_SZ	Bluetooth
ClassGUID	REG_SZ	{e0cbf06c-cd8b-4647-bb8a-263b43f0f974}
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{00000000-0000-0000-FFFF-FFFFFFFFFFFF}
DeviceDesc	REG_SZ	@oem0.inf,%bthps3psm.devicedesc%;PlayStation 3 Peripherals Filter Driver
Driver	REG_SZ	{e0cbf06c-cd8b-4647-bb8a-263b43f0f974}\0002
HardwareID	REG_MULTI_SZ	Nefarius\{a3dc6d41-9e10-46d9-8be2-9b4a279841df}
Mfg	REG_SZ	@oem0.inf,%manufacturername%;Nefarius Software Solutions e.U.
Service	REG_SZ	BthPS3PSM

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/82276012-0158-4d9d-a71e-34ca738b432e-image.png)

How the Heck do I get rid of the Advanced tab 🤔



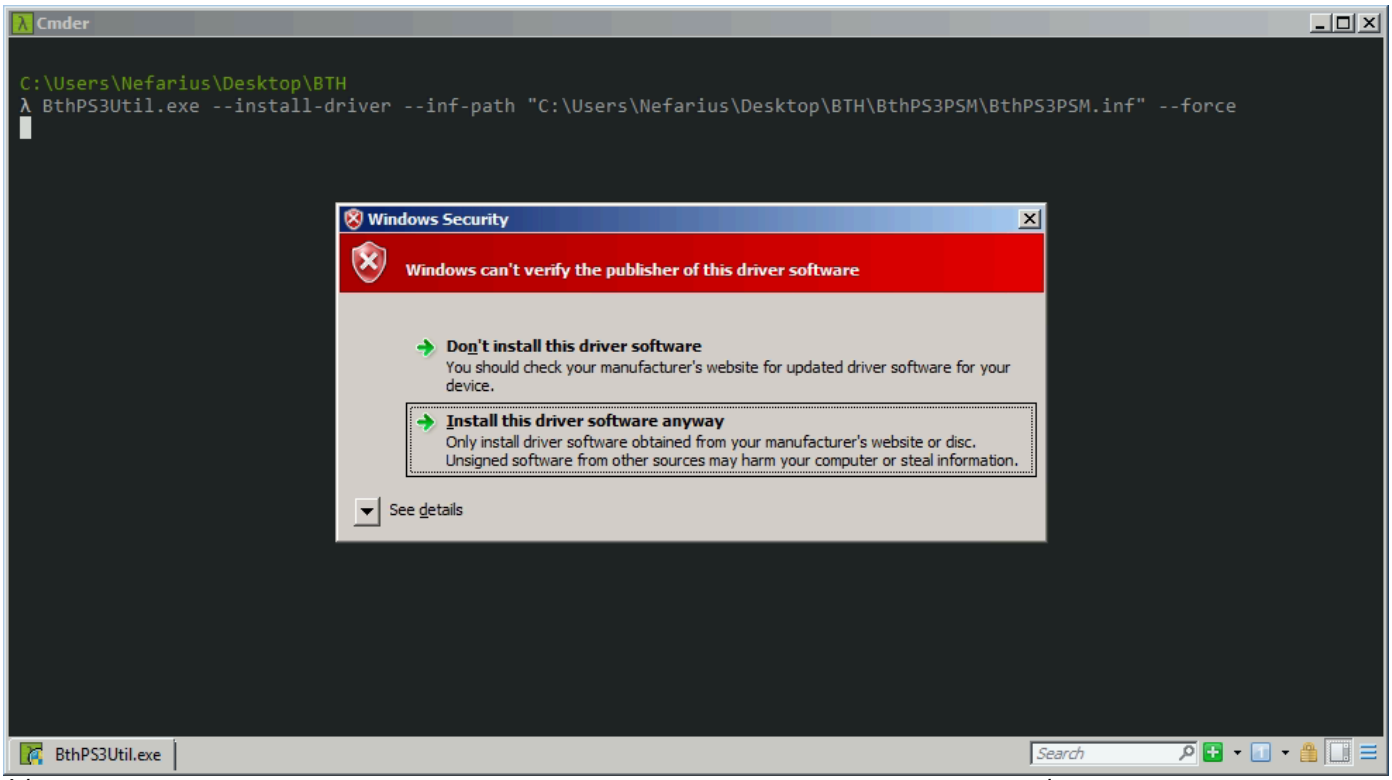
(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/c76cdce4-f691-4fb5-90c8-6cfe38bd12cb-image.png)

Jan 12, 2019, 4:51 PM (https://localhost/post/1031)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Working on BthPS3Util

Creating a small command line utility for abstracting away the mess of creating filter device node, installing filter driver, enabling the filter and registering the service profile.



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/3235ea5f-c436-4f3f-8969-a3b90a480c5c-image.png)

```
C:\Users\Nefarius\Desktop\BTH
λ BthPS3Util.exe --create-filter-device
Device node created successfully
```

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/3fe40c51-c0ad-4bfa-98ae-0863ad41b749-image.png)

```
C:\Users\Nefarius\Desktop\BTH
λ BthPS3Util.exe --install-driver --inf-path "C:\Users\Nefarius\Desktop\BTH\BthPS3PSM\BthPS3PSM.inf" --force
Driver installed successfully

C:\Users\Nefarius\Desktop\BTH
λ
```

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/9b5bed5d-d8cf-4311-8149-26726d846457-image.png)

Jan 14, 2019, 7:55 PM (https://localhost/post/1034)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius) (https://localhost/user/nefarius)

Bloody hell, my mind was *not* prepared to deal with a state machine handling two L2CAP channels with all those async stuff happening and the tons of error handling required. Time for my favorite part in what I call (dramatic music playing 🎶) *poke-in-the-dark-development*:

1. think about the solution
2. code it
3. think about it again
4. realize it's flawed
5. revert changes

6. `goto 1`

🤦

Jan 18, 2019, 4:46 PM (https://localhost/post/1057)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Oddly enough I wasn't able to find an official way to get the remote device name from an incoming connection, just the MAC address. This isn't a showstopper but odd and annoying for device identification. Or am I missing something 🤔

Jan 18, 2019, 5:27 PM (https://localhost/post/1058)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@nefarius (https://forums.vigem.org/uid/1) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1057):

> Oddly enough I wasn't able to find an official way to get the remote device name from an incoming connection, just the MAC address. This isn't a showstopper but odd and annoying for device identification. Or am I missing something

Wait a minute... if I got this right, calling `IOCTL_BTH_GET_DEVICE_INFO` (https://docs.microsoft.com/en-us/windows-hardware/drivers/ddi/content/bthioctl/ni-bthioctl-ioctl_bth_get_device_info) returns a `BTH_DEVICE_INFO_LIST` (https://docs.microsoft.com/en-us/windows-hardware/drivers/ddi/content/bthioctl/ns-bthioctl-_bth_device_info_list) containing `BTH_DEVICE_INFO` (https://docs.microsoft.com/en-ie/windows/desktop/api/bthdef/ns-bthdef-_bth_device_info) which can then be matched against `address` and contains a `name` member:

> Name of the remote Bluetooth device, as reported by the device, encoded in UTF8. The user may have locally provided a display name for the remote Bluetooth device; that name is overridden, and does not appear in this member; it is accessible only with a call to the BluetoothGetDeviceInfo function.

Bingo! The name isn't a 100% safe to rely on in device identification compared to the MAC address, but it's the best shot. It's important to react differently depending on the device type (DualShock 3, Navigation Controller, Motion Controller or DualShock 4 a.k.a. Wireless Controller). This is how it's currently done in WireShock:

```
BD_ADDR_FROM_BUFFER(clientAddr, &buffer[3]);

ULONG length;

//
// Scan through rest of buffer until null-terminator is found
//
for (length = 1;
        buffer[length + 8] != 0x00
        && (length + 8) < NumBytesTransferred;
        length++);

//
// Store remote name in device context
//
WireBusSetChildRemoteName(
        Device,
        &clientAddr,
        &buffer[9],
        length
);

switch (buffer[9])
{
case 'P': // First letter in PLAYSTATION(R)3 Controller ('P')
        WireBusSetChildDeviceType(
                Device,
                &clientAddr,
                DS_DEVICE_TYPE_PS3_DUALSHOCK
        );
        break;
case 'N': // First letter in Navigation Controller ('N')
        WireBusSetChildDeviceType(
                Device,
                &clientAddr,
                DS_DEVICE_TYPE_PS3_NAVIGATION
        );
        break;
case 'M': // First letter in Motion Controller ('M')
        WireBusSetChildDeviceType(
                Device,
                &clientAddr,
                DS_DEVICE_TYPE_PS3_MOTION
        );
        break;
case 'W': // First letter in Wireless Controller ('W')
        WireBusSetChildDeviceType(
                Device,
                &clientAddr,
                DS_DEVICE_TYPE_PS4_DUALSHOCK
        );
        break;
default:
        TraceEvents(TRACE_LEVEL_ERROR,
                TRACE_INTERRUPT,
                "Couldn't determine device type from remote name (%c)",
                buffer[9]
        );
        break;
}
```

I've discovered that a DS4 (Rev1) paired in PC-mode will also try to directly connect with PSM `0x11` and `0x13` in addition to the correct `0x01` and gets denied. It continues to work though; my best guess is that the controller simply tries if the Bluetooth host is a PS4 and changes its behavior accordingly. This is unfortunate for my profile driver, because now I need to know that it is a DS4, not a DS3, and deny the connection request because the filter will rewrite the PSMs as well. This rabbit hole... 😵

Jan 18, 2019, 5:29 PM (https://localhost/post/1059) □
□ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 □
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

Daltz333 (https://localhost/user/daltz333)
(https://localhost/user/daltz333)

Quite interesting research. So putting this into simple terms, the filter driver will pickup the DS4 and will interpret it's requests instead? Which is bad because the DS4 has bluetooth support already.

Jan 18, 2019, 5:34 PM (https://localhost/post/1060)
□ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 □
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@daltz333 (https://forums.vigem.org/uid/6) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1059):

> Quite interesting research. So putting this into simple terms, the filter driver will pickup the DS4 and will interpret it's requests instead? Which is bad because the DS4 has bluetooth support already.

The filter is stupid and has no idea what kind of device is connecting, it looks for Protocol/Service Multiplexer values `0x11` (HID Control) and `0x13` (HID Interrupt) and patches them to artificial values the profile driver listens on. So now the profile driver is in charge of handling the connection requests. The profile driver needs to know what kind of device connects because anything else than the PS3 peripherals could in theory use those PSMs as well. Now we also know that the DS4 tries them as well for whatever reason. It doesn't need to because it has a valid SDP record but I guess it does it to "poke" the Bluetooth host and switches to native PS4 mode if the PSMs get accepted. Who knows what would happen then.

Jan 20, 2019, 4:53 PM (https://localhost/post/1065) □
□ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 □
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Papers, please 👮

```
2019/01/20-16:50:29.960 TRACE_LEVEL_INFORMATION New connection for PSM 0x5053 from AC7A4D2819AC arrived
2019/01/20-16:50:29.960 TRACE_LEVEL_INFORMATION ++ deviceInfoList.numOfDevices: 2
2019/01/20-16:50:29.960 TRACE_LEVEL_INFORMATION ++ Device 0 address ACFD93095C20, name: Wireless Controller
2019/01/20-16:50:29.960 TRACE_LEVEL_INFORMATION ++ Device 1 address AC7A4D2819AC, name: PLAYSTATION(R)3 Cont
roller
2019/01/20-16:50:29.981 TRACE_LEVEL_INFORMATION New connection for PSM 0x5055 from AC7A4D2819AC arrived
2019/01/20-16:50:29.981 TRACE_LEVEL_INFORMATION ++ deviceInfoList.numOfDevices: 2
2019/01/20-16:50:29.981 TRACE_LEVEL_INFORMATION ++ Device 0 address ACFD93095C20, name: Wireless Controller
2019/01/20-16:50:29.981 TRACE_LEVEL_INFORMATION ++ Device 1 address AC7A4D2819AC, name: PLAYSTATION(R)3 Cont
roller
2019/01/20-16:50:29.993 TRACE_LEVEL_INFORMATION L2CAP_PS3_ConnectionIndicationCallback ++ IndicationRemoteCo
nfigRequest
```

We got the name! Delightful 😀

Jan 20, 2019, 6:27 PM (https://localhost/post/1066)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Some more hardening and error handling, that will be all for today 😌

```
2019/01/20-18:11:22.457 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Entry
2019/01/20-18:11:22.457 TRACE_LEVEL_INFORMATION New connection for PSM 0x5053 from AC7A4D2819AC arrived
2019/01/20-18:11:22.457 TRACE_LEVEL_VERBOSE     L2CAP_PS3_SendConnectResponse Entry
2019/01/20-18:11:22.457 TRACE_LEVEL_ERROR       BTHPS3_GET_DEVICE_NAME failed with status STATUS_INVALID_PAR
AMETER (0xC000000D)
2019/01/20-18:11:22.457 TRACE_LEVEL_VERBOSE     L2CAP_PS3_SendConnectResponse Exit (STATUS_SUCCESS (0x000000
00))
2019/01/20-18:11:22.457 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Exit
2019/01/20-18:11:23.072 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Entry
2019/01/20-18:11:23.072 TRACE_LEVEL_INFORMATION New connection for PSM 0x5053 from AC7A4D2819AC arrived
2019/01/20-18:11:23.072 TRACE_LEVEL_VERBOSE     L2CAP_PS3_SendConnectResponse Entry
2019/01/20-18:11:23.072 TRACE_LEVEL_INFORMATION ++ Device AC7A4D2819AC name: PLAYSTATION(R)3 Controller
2019/01/20-18:11:23.072 TRACE_LEVEL_VERBOSE     L2CAP_PS3_SendConnectResponse Exit (STATUS_SUCCESS (0x000000
00))
2019/01/20-18:11:23.072 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Exit
2019/01/20-18:11:23.072 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry
2019/01/20-18:11:23.072 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
2019/01/20-18:11:23.093 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Entry
2019/01/20-18:11:23.093 TRACE_LEVEL_INFORMATION New connection for PSM 0x5055 from AC7A4D2819AC arrived
2019/01/20-18:11:23.093 TRACE_LEVEL_VERBOSE     L2CAP_PS3_SendConnectResponse Entry
2019/01/20-18:11:23.093 TRACE_LEVEL_INFORMATION ++ Device AC7A4D2819AC name: PLAYSTATION(R)3 Controller
2019/01/20-18:11:23.093 TRACE_LEVEL_VERBOSE     L2CAP_PS3_SendConnectResponse Exit (STATUS_SUCCESS (0x000000
00))
2019/01/20-18:11:23.093 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Exit
```

Jan 24, 2019, 8:42 PM (https://localhost/post/1081) (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius) (https://localhost/user/nefarius)

I'm feeling a cold creeping up on me but nevertheless managed to utilize enough brain power to implement resource cleanup on disconnect without a single BSOD! 🤠

```
--- DS3 connecting ---
2019/01/24-20:39:11.096 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Entry
2019/01/24-20:39:11.096 TRACE_LEVEL_INFORMATION New connection for PSM 0x5053 from AC7A4D2819AC arrived
2019/01/24-20:39:11.096 TRACE_LEVEL_VERBOSE     L2CAP_PS3_SendConnectResponse Entry
2019/01/24-20:39:11.096 TRACE_LEVEL_INFORMATION ++ Device AC7A4D2819AC name: PLAYSTATION(R)3 Controller
2019/01/24-20:39:11.096 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
0, Context: 0xFFFFFA8007488780)
2019/01/24-20:39:11.096 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
2019/01/24-20:39:11.096 TRACE_LEVEL_VERBOSE     L2CAP_PS3_SendConnectResponse Exit (STATUS_SUCCESS (0x000000
00))
2019/01/24-20:39:11.096 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Exit
2019/01/24-20:39:11.112 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Entry
2019/01/24-20:39:11.112 TRACE_LEVEL_INFORMATION New connection for PSM 0x5055 from AC7A4D2819AC arrived
2019/01/24-20:39:11.112 TRACE_LEVEL_VERBOSE     L2CAP_PS3_SendConnectResponse Entry
2019/01/24-20:39:11.112 TRACE_LEVEL_INFORMATION ++ Device AC7A4D2819AC name: PLAYSTATION(R)3 Controller
2019/01/24-20:39:11.112 TRACE_LEVEL_VERBOSE     ++ Found desired connection item in connection list
2019/01/24-20:39:11.112 TRACE_LEVEL_VERBOSE     L2CAP_PS3_SendConnectResponse Exit (STATUS_SUCCESS (0x000000
00))
2019/01/24-20:39:11.112 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Exit
2019/01/24-20:39:11.112 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
0, Context: 0xFFFFFA8007488780)
2019/01/24-20:39:11.112 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
2019/01/24-20:39:11.121 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
4, Context: 0xFFFFFA8007488780)
2019/01/24-20:39:11.121 TRACE_LEVEL_INFORMATION L2CAP_PS3_ConnectionIndicationCallback ++ IndicationRemoteCo
nfigRequest
2019/01/24-20:39:11.121 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
--- DS3 connected ---

--- DS3 disconnecting (by holding PS button for 10 seconds) ---
2019/01/24-20:39:35.193 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
3, Context: 0xFFFFFA8007488780)
2019/01/24-20:39:35.193 TRACE_LEVEL_VERBOSE     ++ IndicationRemoteDisconnect [0xFFFFFA80073F9CE0]
2019/01/24-20:39:35.193 TRACE_LEVEL_VERBOSE     ++ HID Interrupt Channel 0xFFFFFA80073F9CE0 disconnected
2019/01/24-20:39:35.193 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
2019/01/24-20:39:35.196 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
3, Context: 0xFFFFFA8007488780)
2019/01/24-20:39:35.196 TRACE_LEVEL_VERBOSE     ++ IndicationRemoteDisconnect [0xFFFFFA800775E170]
2019/01/24-20:39:35.196 TRACE_LEVEL_VERBOSE     ++ HID Control Channel 0xFFFFFA800775E170 disconnected
2019/01/24-20:39:35.196 TRACE_LEVEL_VERBOSE     ClientConnections_RemoveAndDestroy Entry (Context: 0xFFFFFA8
007488780)
2019/01/24-20:39:35.196 TRACE_LEVEL_VERBOSE     ++ Found desired connection item in connection list
2019/01/24-20:39:35.196 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
2019/01/24-20:39:35.196 TRACE_LEVEL_VERBOSE     EvtClientConnectionsDestroyConnection Entry
2019/01/24-20:39:35.619 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
1, Context: 0xFFFFFA8007488780)
2019/01/24-20:39:35.619 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
2019/01/24-20:39:35.619 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
1, Context: 0xFFFFFA8007488780)
2019/01/24-20:39:35.619 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
--- DS3 disconnected ---
```

'till next time 👋

Jan 25, 2019, 6:20 PM (https://localhost/post/1082)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Device identification and connection drop on error/incompatibility implemented and working 😇

```
2019/01/25-18:16:35.587 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Entry
2019/01/25-18:16:35.587 TRACE_LEVEL_INFORMATION New connection for PSM 0x5053 from AC7A4D2819AC arrived
2019/01/25-18:16:35.587 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnect Entry
2019/01/25-18:16:35.588 TRACE_LEVEL_ERROR       BTHPS3_GET_DEVICE_NAME failed with status STATUS_INVALID_PAR
AMETER (0xC000000D), dropping connection
2019/01/25-18:16:35.588 TRACE_LEVEL_VERBOSE     L2CAP_PS3_DenyRemoteConnect Entry
2019/01/25-18:16:35.588 TRACE_LEVEL_VERBOSE     L2CAP_PS3_DenyRemoteConnectCompleted Entry (STATUS_SUCCESS
(0x00000000))
2019/01/25-18:16:35.588 TRACE_LEVEL_VERBOSE     L2CAP_PS3_DenyRemoteConnectCompleted Exit
2019/01/25-18:16:35.588 TRACE_LEVEL_VERBOSE     L2CAP_PS3_DenyRemoteConnect Exit
2019/01/25-18:16:35.588 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Exit
2019/01/25-18:16:36.188 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Entry
2019/01/25-18:16:36.188 TRACE_LEVEL_INFORMATION New connection for PSM 0x5053 from AC7A4D2819AC arrived
2019/01/25-18:16:36.188 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnect Entry
2019/01/25-18:16:36.188 TRACE_LEVEL_INFORMATION ++ Device AC7A4D2819AC name: PLAYSTATION(R)3 Controller
2019/01/25-18:16:36.188 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
0, Context: 0xFFFFFA8008FDB5B0)
2019/01/25-18:16:36.188 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
2019/01/25-18:16:36.188 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnect Exit (STATUS_SUCCESS (0x000000
00))
```

Jan 26, 2019, 9:33 AM (https://localhost/post/1085)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Marvelous terrible quality video demonstrating that DS4 and DS3 can live together in peace on the default Bluetooth host driver:

 Youtube Video (https://www.youtube.com/watch?v=0-Y3sHGmSiQ)

In typical USB-fashion the darn plug didn't want to go into the socket in one go 🤦 and the room didn't have enough light to combat the bright screen causing the camera to adjust exposure so it all went a bit too dark 😅

What's happening in the video:

- Bluetooth host USB dongle gets plugged in, default Window driver, filter and profile driver get loaded
- DS4 gets paired in PC-mode and works as expected
- DS3 gets powered on by tap on PS button and connects (there is no output report sent yet so the LEDs will keep flashing although it has connected successfully)
- DS4 continues to work unimpressed by second device, so no interference
- DS3 gets force-shut-off by holding PS button for around ten seconds
- DS4 continues to work after DS3 has left the building

So far not so shabby! 🎉

Feb 1, 2019, 2:41 AM (https://localhost/post/1092)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

(https://localhost/user/nefarius) nefarius (https://localhost/user/nefarius)

Managed to send it the first output report, now the LEDs stay bright on 😃

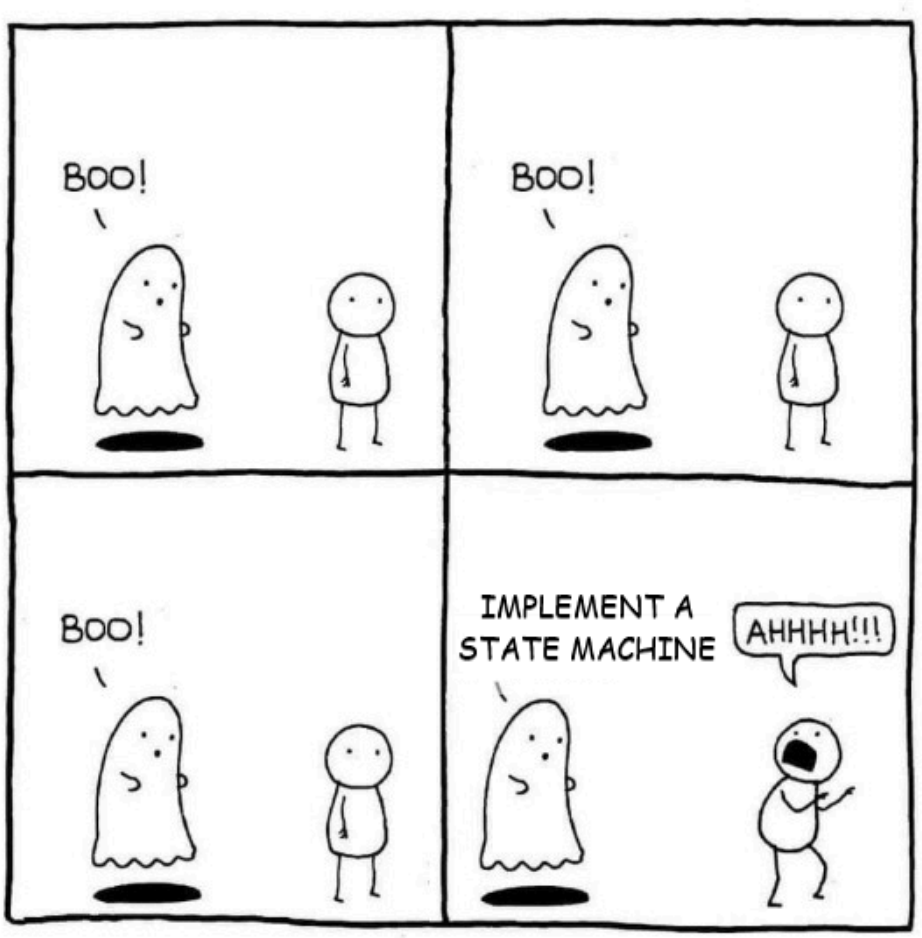
```
2019/02/01-02:39:55.177 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Entry
2019/02/01-02:39:55.177 TRACE_LEVEL_INFORMATION New connection for PSM 0x5053 from AC7A4D2819AC arrived
2019/02/01-02:39:55.177 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnect Entry
2019/02/01-02:39:55.177 TRACE_LEVEL_ERROR       BTHPS3_GET_DEVICE_NAME failed with status STATUS_INVALID_PAR
AMETER (0xC000000D), dropping connection
2019/02/01-02:39:55.177 TRACE_LEVEL_VERBOSE     L2CAP_PS3_DenyRemoteConnect Entry
2019/02/01-02:39:55.177 TRACE_LEVEL_VERBOSE     L2CAP_PS3_DenyRemoteConnectCompleted Entry (STATUS_SUCCESS
(0x00000000))
2019/02/01-02:39:55.177 TRACE_LEVEL_VERBOSE     L2CAP_PS3_DenyRemoteConnectCompleted Exit
2019/02/01-02:39:55.177 TRACE_LEVEL_VERBOSE     L2CAP_PS3_DenyRemoteConnect Exit
2019/02/01-02:39:55.177 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Exit
2019/02/01-02:39:55.757 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Entry
2019/02/01-02:39:55.757 TRACE_LEVEL_INFORMATION New connection for PSM 0x5053 from AC7A4D2819AC arrived
2019/02/01-02:39:55.757 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnect Entry
2019/02/01-02:39:55.757 TRACE_LEVEL_INFORMATION ++ Device AC7A4D2819AC name: PLAYSTATION(R)3 Controller
2019/02/01-02:39:55.757 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
0, Context: 0xFFFFFA8007378CA0)
2019/02/01-02:39:55.757 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
2019/02/01-02:39:55.757 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnect Exit (STATUS_SUCCESS (0x000000
00))
2019/02/01-02:39:55.757 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Exit
2019/02/01-02:39:55.764 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ControlConnectResponseCompleted Entry
2019/02/01-02:39:55.764 TRACE_LEVEL_INFORMATION Connection completion, status: STATUS_SUCCESS (0x00000000)
2019/02/01-02:39:55.764 TRACE_LEVEL_INFORMATION HID Control Channel connection established
2019/02/01-02:39:55.764 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ControlConnectResponseCompleted Exit
2019/02/01-02:39:55.772 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Entry
2019/02/01-02:39:55.772 TRACE_LEVEL_INFORMATION New connection for PSM 0x5055 from AC7A4D2819AC arrived
2019/02/01-02:39:55.772 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnect Entry
2019/02/01-02:39:55.772 TRACE_LEVEL_INFORMATION ++ Device AC7A4D2819AC name: PLAYSTATION(R)3 Controller
2019/02/01-02:39:55.772 TRACE_LEVEL_VERBOSE     ++ Found desired connection item in connection list
2019/02/01-02:39:55.772 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnect Exit (STATUS_SUCCESS (0x000000
00))
2019/02/01-02:39:55.772 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Exit
2019/02/01-02:39:55.772 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
0, Context: 0xFFFFFA8007378CA0)
2019/02/01-02:39:55.772 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
2019/02/01-02:39:55.781 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
4, Context: 0xFFFFFA8007378CA0)
2019/02/01-02:39:55.781 TRACE_LEVEL_INFORMATION L2CAP_PS3_ConnectionIndicationCallback ++ IndicationRemoteCo
nfigRequest
2019/02/01-02:39:55.781 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
2019/02/01-02:39:55.784 TRACE_LEVEL_VERBOSE     L2CAP_PS3_InterruptConnectResponseCompleted Entry
2019/02/01-02:39:55.784 TRACE_LEVEL_INFORMATION Connection completion, status: STATUS_SUCCESS (0x00000000)
2019/02/01-02:39:55.784 TRACE_LEVEL_INFORMATION HID Interrupt Channel connection established
2019/02/01-02:39:55.784 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionStateConnected Entry
2019/02/01-02:39:55.784 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionStateConnected Exit
2019/02/01-02:39:55.784 TRACE_LEVEL_VERBOSE     L2CAP_PS3_InterruptConnectResponseCompleted Exit
2019/02/01-02:39:55.785 TRACE_LEVEL_VERBOSE     Control transfer request completed with status STATUS_SUCCES
S (0x00000000)
```

Feb 1, 2019, 9:52 AM (https://localhost/post/1093)

(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Biggest struggle in this project so far 😆



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/1bd58b96-8320-4453-b860-2170d0b5b56c-image.png)

Feb 3, 2019, 12:02 PM (https://localhost/post/1095)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Couldn't fall asleep last night, implemented bus enumerator instead:

 Youtube Video (https://youtu.be/xSw0GMgxfgU)

What's going on in the video: once the connection of both HID Control and Interrupt channels has been established, the wonderful KMDF bus driver API kicks in and spawns a new PNP device:

```
WDF_CHILD_IDENTIFICATION_DESCRIPTION_HEADER_INIT(
        &pdoDesc.Header,
        sizeof(PDO_IDENTIFICATION_DESCRIPTION)
    );

pdoDesc.RemoteAddress = ClientConnection->RemoteAddress;
pdoDesc.DeviceType = ClientConnection->DeviceType;

//
// Invoke new child creation
//
status = WdfChildListAddOrUpdateChildDescriptionAsPresent(
        WdfFdoGetDefaultChildList(ClientConnection->DevCtxHdr->Device),
        &pdoDesc.Header,
        NULL
);
```

In order to de-clutter the profile/bus driver I decided to outsource the device-specific logic into one or more additional function drivers, introducing IOCTLs to fetch data from and send to the PDOs without having to deal with Bluetooth-specific paradigms at all. I've introduced artificial GUID-based hardware IDs for every distinct device:

- `DS_DEVICE_TYPE_SIXAXIS` - SIXAXIS or DualShock 3 compatible (including 3rd party controllers)
- `DS_DEVICE_TYPE_NAVIGATION` - PlayStation Move Navigation Controller
- `DS_DEVICE_TYPE_MOTION` - PlayStation Move Motion Controller
- `DS_DEVICE_TYPE_WIRELESS` - DualShock 4 Revision 1 or 2 Wireless Controller

On a personal note; I'm quite pleased about the pacing here, implementing the bus logic was done almost entirely from memory and implemented once again without crashing the test host 👏


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

A **lot** of progress was made today. Nothing much to present yet but I've basically started to design and implement the interface that will be used to talk to the exposed PDOs via own function driver. This causes the code base for the profile driver remain encapsulated for Bluetooth related stuff only. Higher level functions (HID mini-driver, LED, Rumble, ...) will then be implemented by one or more individual function drivers latching onto the PDOs.

Cheers

Feb 5, 2019, 9:03 PM (https://localhost/post/1097)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Wrapped all necessary driver (un-)installation tasks in a small self-contained tool and finished proper error handling:

```
C:\Users\Nefarius\Desktop\BTH
λ BthPS3Util.exe --enable-service
Service enabled successfully

C:\Users\Nefarius\Desktop\BTH
λ BthPS3Util.exe --install-driver --inf-path "C:\Users\Nefarius\Desktop\BTH\BthPS3\BthPS3.inf"
Driver installed successfully

C:\Users\Nefarius\Desktop\BTH
λ BthPS3Util.exe --create-filter-service --bin-path "C:\Users\Nefarius\Desktop\BTH\BthPS3PSM\BthPS3PSM.sys"
Service created successfully

C:\Users\Nefarius\Desktop\BTH
λ BthPS3Util.exe --enable-filter
Filter enabled. Reconnect affected devices or reboot system to apply changes!

C:\Users\Nefarius\Desktop\BTH
λ BthPS3Util.exe --enable-filter
Filter already enabled. No changes were made

C:\Users\Nefarius\Desktop\BTH
λ BthPS3Util.exe --create-filter-service --bin-path "C:\Users\Nefarius\Desktop\BTH\BthPS3PSM\BthPS3PSM.sys"
Service creation failed, error: The specified service already exists.


C:\Users\Nefarius\Desktop\BTH
λ
```

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/cd8e8aa4-2962-427e-903a-a514d6ce6085-image.png)

This tool can then assist a setup in automating the installation and also making test installations more bearable 😉

What happens in the picture for each line:

- `BluetoothSetLocalServiceInfo` (https://msdn.microsoft.com/en-us/library/windows/desktop/bb870603%28v=vs.85%29.aspx?f=255&MSPPError=-2147217396) is invoked which causes `bthenum` to spawn a PDO for the profile driver to latch onto
- Bluetooth profile driver gets installed in driver store and device driver installation for newly spawned PDO gets kicked off
- `bthusb` lower filter driver service (`BthPS3PSM`) gets created

- `BthPS3PSM` gets added as lower filter driver for `GUID_DEVCLASS_BLUETOOTH` device class
- Same action is invoked again, leading to a different response
- Service creation is invoked again, failing because it's already registered

That'll be all for today, folks! 🤠

Feb 6, 2019, 5:52 PM (https://localhost/post/1098)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

It's communicating! 😄

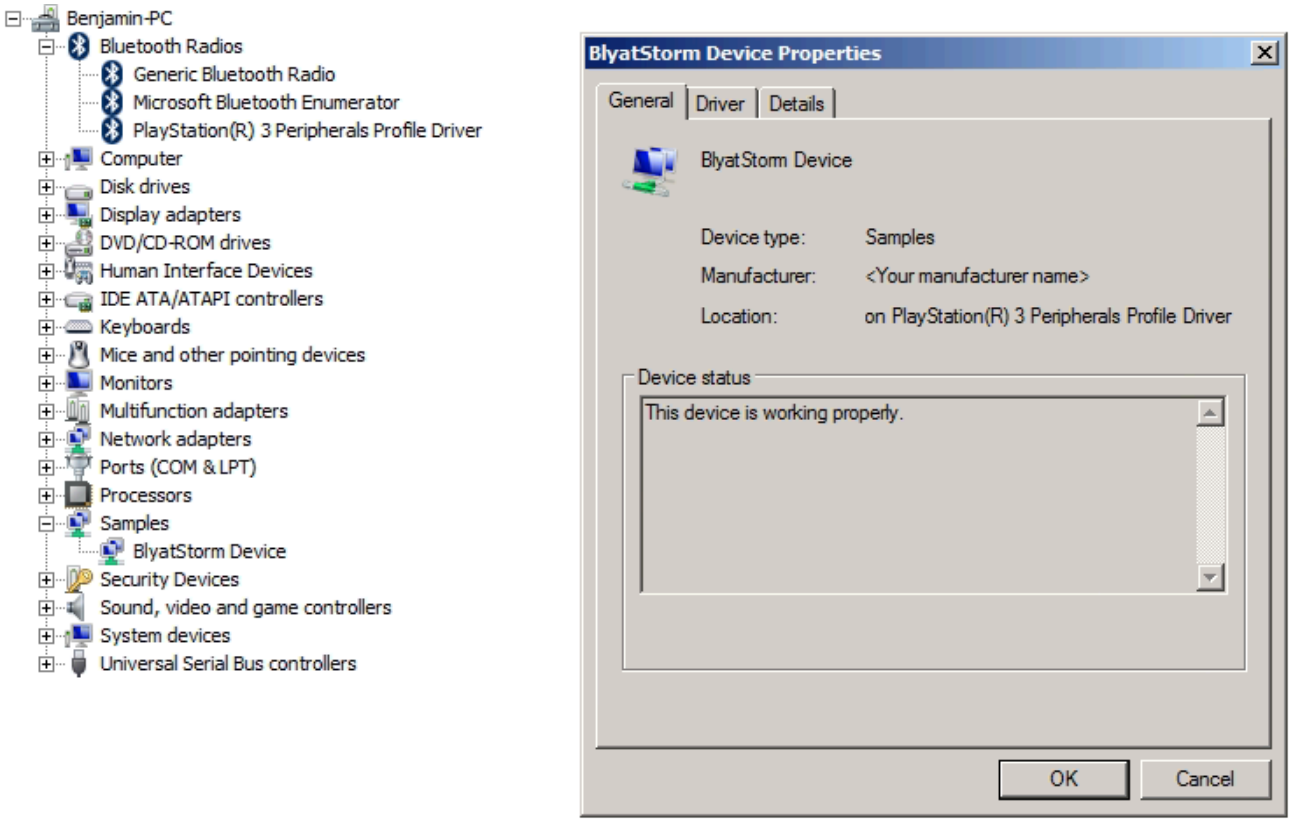
(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/ezgif.com-gif-maker.gif)

I've managed to quickly hack together an ugly demo function driver for the SIXAXIS PDO in under an hour and test it with only two crashes 😇

```
_Use_decl_annotations_
VOID
OutputReport_EvtTimerFunc(
    WDFTIMER  Timer
)
{
    WDFDEVICE device = WdfTimerGetParentObject(Timer);
    WDFIOTARGET ioTarget = WdfDeviceGetIoTarget(device);
    PDEVICE_CONTEXT devCtx = DeviceGetContext(device);

    TraceEvents(TRACE_LEVEL_INFORMATION, TRACE_DEVICE, "%!FUNC! Entry");

    static UCHAR G_Ds3HidOutputReport[] = {
    0x52, 0x01, 0x00, 0xFF, 0x00, 0xFF, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x1E, 0xFF, 0x27, 0x10, 0x00,
    0x32, 0xFF, 0x27, 0x10, 0x00, 0x32, 0xFF, 0x27,
    0x10, 0x00, 0x32, 0xFF, 0x27, 0x10, 0x00, 0x32,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00
    };

    static BOOLEAN toggle = FALSE;

    toggle = !toggle;
    G_Ds3HidOutputReport[11] = (toggle) ? 0x02 : 0x04;

    PBTHPS3_HID_CONTROL_WRITE controlWrite;
    NTSTATUS status;

    WDF_MEMORY_DESCRIPTOR  MemoryDescriptor;
    WDFMEMORY  MemoryHandle = NULL;
    status = WdfMemoryCreate(NULL,
        NonPagedPool,
        'aylB',
        sizeof(BTHPS3_HID_CONTROL_WRITE),
        &MemoryHandle,
        &controlWrite);

    BTHPS3_HID_CONTROL_WRITE_INIT(controlWrite);

    controlWrite->BufferLength = 0x32;
    controlWrite->Buffer = ExAllocatePoolWithTag(
        NonPagedPoolNx,
        0x32,
        'aylB'
    );
    RtlCopyMemory(controlWrite->Buffer, G_Ds3HidOutputReport, 0x32);

    WDF_MEMORY_DESCRIPTOR_INIT_HANDLE(&MemoryDescriptor,
        MemoryHandle,
        NULL);

    status = WdfIoTargetSendInternalIoctlSynchronously(
        ioTarget,
        NULL,
        IOCTL_BTHPS3_HID_CONTROL_WRITE,
        &MemoryDescriptor,
        NULL,
        NULL,
        NULL
    );

    ExFreePoolWithTag(controlWrite->Buffer, 'aylB');
```

```
    if (!NT_SUCCESS(status)) {
        TraceEvents(TRACE_LEVEL_ERROR,
            TRACE_DEVICE,
            "WdfIoTargetSendInternalIoctlSynchronously failed with status %!STATUS!",
            status
        );
        return;
    }

    WdfTimerStart(devCtx->OutputReportTimer, WDF_REL_TIMEOUT_IN_MS(0x01F4));

    TraceEvents(TRACE_LEVEL_INFORMATION, TRACE_DEVICE, "%!FUNC! Exit");
}
```

This is a timer callback function getting called around every 500 ms and cycling through LED 1 and 2 by submitting an output report to the HID Control endpoint via `IOCTL_BTHPS3_HID_CONTROL_WRITE`. The driver is very minimal, inefficient with memory handling and horribly named but for a demonstration just perfect 😆



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/4c2d7745-b075-4ec9-8c92-64719155effa-image.png)

Next I'm gonna try to read from it 💥

Feb 10, 2019, 10:29 AM (https://localhost/post/1099)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Turns out reading from the HID interrupt channel *the right way* is a bit more challenging than I expected. Unfortunately there's no Bluetooth equivalent of the continuous reader (https://docs.microsoft.com/en-us/windows-hardware/drivers/usbcon/how-to-use-the-continous-reader-for-getting-data-from-a-usb-endpoint--umdf-) for USB pipes in WDF so you've to implement that thing yourself. There are reference implementations (https://github.com/Microsoft/Windows-driver-samples/blob/6c1981b8504329521343ad00f32daa847fa6083a/bluetooth/bthecho/common/lib/connection.c#L121) available but they're so "ripped apart" and all over the place I'll instead try to write it from scratch to better understand what's happening. Maybe I get somewhere today, we'll see 🎖️

Feb 10, 2019, 6:01 PM (https://localhost/post/1100)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

There we go 😎

```
2019/02/10-17:52:51.880 TRACE_LEVEL_VERBOSE     BthPS3_PDO_EvtWdfIoQueueIoInternalDeviceControl Entry
2019/02/10-17:52:51.880 TRACE_LEVEL_VERBOSE     BthPS3_EvtWdfIoQueueIoInternalDeviceControl Entry
2019/02/10-17:52:51.880 TRACE_LEVEL_VERBOSE     bufferLength: 50
2019/02/10-17:52:51.885 TRACE_LEVEL_VERBOSE     brb->BufferSize: 50, brb->RemainingBufferSize: 0
2019/02/10-17:52:51.885 TRACE_LEVEL_INFORMATION A1 01 00 00 00 00 00 7A 81 80 7D 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 03 05 16 FF CD 00 01 33 00 77 00 40 01 FA 01 ED 01 91 00 05
2019/02/10-17:52:51.885 TRACE_LEVEL_VERBOSE     BthPS3_PDO_EvtWdfIoQueueIoInternalDeviceControl Exit
```

What threw me off for quite a few hours was the weird behavior of the `RemainingBufferSize` member of the _BRB_L2CA_ACL_TRANSFER structure (https://docs.microsoft.com/en-us/windows-hardware/drivers/ddi/content/bthddi/ns-bthddi-_brb_l2ca_acl_transfer#members), which was increasing fast to values way higher than the buffer I supplied could hold. Turns out this field is *not* talking about the `Buffer` member the caller supplies but the internal buffer of the Bluetooth host which tells you how many bytes have already come in from the remote device and are available to be read by further calls with that same BRB. I don't think the reference code I had a peek at did take that into account as this value was subtracted from `BufferSize` which could lead to a negative value resulting in 💥

Now that that's sorted out off to cleaning up this mess and looking for leaking memory 😇

Feb 10, 2019, 6:37 PM (https://localhost/post/1101)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

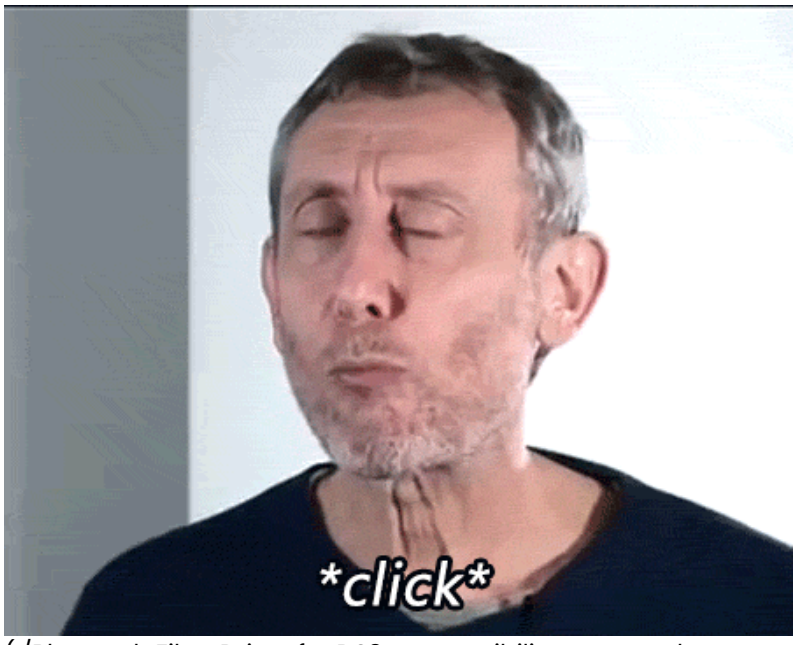
 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Going the extra mile today: testing the PS Move Navigation controller 😈 Connection established:

```
2019/02/10-18:32:19.445 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Entry
2019/02/10-18:32:19.445 TRACE_LEVEL_INFORMATION New connection for PSM 0x5053 from 70401E341 arrived
2019/02/10-18:32:19.445 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnect Entry
2019/02/10-18:32:19.446 TRACE_LEVEL_ERROR       BTHPS3_GET_DEVICE_NAME failed with status STATUS_INVALID_PAR
AMETER (0xC000000D), dropping connection
2019/02/10-18:32:19.446 TRACE_LEVEL_VERBOSE     L2CAP_PS3_DenyRemoteConnect Entry
2019/02/10-18:32:19.446 TRACE_LEVEL_VERBOSE     L2CAP_PS3_DenyRemoteConnectCompleted Entry (STATUS_SUCCESS
(0x00000000))
2019/02/10-18:32:19.446 TRACE_LEVEL_VERBOSE     L2CAP_PS3_DenyRemoteConnectCompleted Exit
2019/02/10-18:32:19.446 TRACE_LEVEL_VERBOSE     L2CAP_PS3_DenyRemoteConnect Exit
2019/02/10-18:32:19.446 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Exit
2019/02/10-18:32:20.247 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Entry
2019/02/10-18:32:20.247 TRACE_LEVEL_INFORMATION New connection for PSM 0x5053 from 70401E341 arrived
2019/02/10-18:32:20.247 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnect Entry
2019/02/10-18:32:20.247 TRACE_LEVEL_INFORMATION ++ Device 70401E341 name: Navigation Controller
2019/02/10-18:32:20.247 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnect Exit (STATUS_SUCCESS (0x000000
00))
2019/02/10-18:32:20.247 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Exit
2019/02/10-18:32:20.247 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
0, Context: 0xFFFFFA80074DE0C0)
2019/02/10-18:32:20.247 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
2019/02/10-18:32:20.497 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ControlConnectResponseCompleted Entry
2019/02/10-18:32:20.497 TRACE_LEVEL_INFORMATION Connection completion, status: STATUS_SUCCESS (0x00000000)
2019/02/10-18:32:20.497 TRACE_LEVEL_INFORMATION HID Control Channel connection established
2019/02/10-18:32:20.497 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ControlConnectResponseCompleted Exit
2019/02/10-18:32:20.689 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Entry
2019/02/10-18:32:20.689 TRACE_LEVEL_INFORMATION New connection for PSM 0x5055 from 70401E341 arrived
2019/02/10-18:32:20.689 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnect Entry
2019/02/10-18:32:20.689 TRACE_LEVEL_INFORMATION ++ Device 70401E341 name: Navigation Controller
2019/02/10-18:32:20.689 TRACE_LEVEL_VERBOSE     ++ Found desired connection item in connection list
2019/02/10-18:32:20.689 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnect Exit (STATUS_SUCCESS (0x000000
00))
2019/02/10-18:32:20.689 TRACE_LEVEL_VERBOSE     BthPS3IndicationCallback Exit
2019/02/10-18:32:20.689 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
0, Context: 0xFFFFFA80074DE0C0)
2019/02/10-18:32:20.689 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
2019/02/10-18:32:20.783 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
4, Context: 0xFFFFFA80074DE0C0)
2019/02/10-18:32:20.783 TRACE_LEVEL_INFORMATION L2CAP_PS3_ConnectionIndicationCallback ++ IndicationRemoteCo
nfigRequest
2019/02/10-18:32:20.783 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
2019/02/10-18:32:20.824 TRACE_LEVEL_VERBOSE     L2CAP_PS3_InterruptConnectResponseCompleted Entry
2019/02/10-18:32:20.824 TRACE_LEVEL_INFORMATION Connection completion, status: STATUS_SUCCESS (0x00000000)
2019/02/10-18:32:20.824 TRACE_LEVEL_INFORMATION HID Interrupt Channel connection established
2019/02/10-18:32:20.824 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionStateConnected Entry
2019/02/10-18:32:20.824 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionStateConnected Exit
2019/02/10-18:32:20.824 TRACE_LEVEL_VERBOSE     L2CAP_PS3_InterruptConnectResponseCompleted Exit
2019/02/10-18:32:20.824 TRACE_LEVEL_VERBOSE     BthPS3_EvtWdfChildListCreateDevice Entry
2019/02/10-18:32:20.824 TRACE_LEVEL_VERBOSE     BthPS3_EvtWdfChildListCreateDevice Exit
```

And there we have the HID Input Report in the function driver 🎉

```
2019/02/10-18:34:23.749 TRACE_LEVEL_INFORMATION InputReport_EvtTimerFunc Entry
2019/02/10-18:34:23.757 TRACE_LEVEL_INFORMATION A1 01 00 00 00 00 00 80 80 7D 85 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 03 03 14 FF C2 00 00 23 D6 77 00 40 02 00 02 04 01 A3 01 FF
2019/02/10-18:34:23.757 TRACE_LEVEL_INFORMATION InputReport_EvtTimerFunc Exit
```



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/giphy.gif)

Feb 15, 2019, 2:47 PM (https://localhost/post/1107)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Alright, time to properly polish and fix power management.

I've implemented dropping all connections in case of `bthenum` surprise removal (unplugging the USB Bluetooth dongle without warning), freeing memory and instructing child device (PDO) removal. This works well and allows unloading the driver, so no dangling objects here. But as soon as the function driver attaches, everything stalls on surprise removal. I haven't yet had the time to debug/implement it but I can document a few assumptions to help me later when I pick it up again.

- `EvtWdfIoQueueIoInternalDeviceControl` sends BRBs *synchronously* out of convenience, this probably isn't the brightest idea, will adjust that to asynchronous
- PDO might be missing PNP/Power capabilities
- Queue I/O stop callback isn't invoked
- Maybe implement self-managed I/O flush callback?

I bet it's an easy fix and I'm just overthinking the issue. Will pick up development again in a few days 👋

Feb 17, 2019, 10:16 PM (https://localhost/post/1109)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Surprise removal power-down sequence fixed!

Two things had to be done (properly):

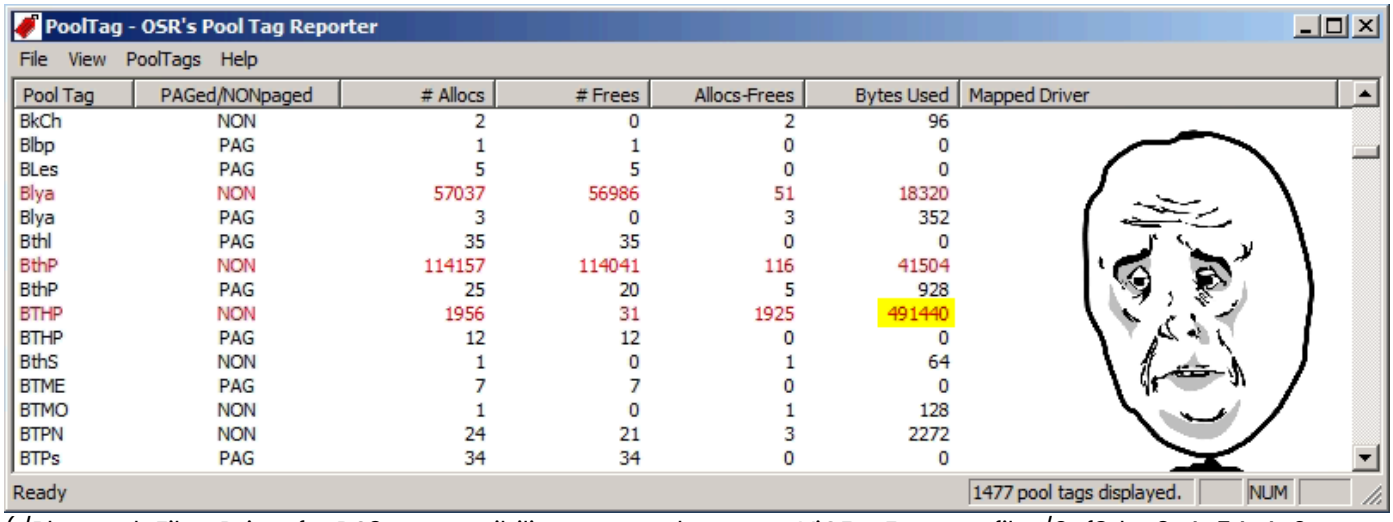
- In EVT_WDF_IO_QUEUE_IO_INTERNAL_DEVICE_CONTROL (https://docs.microsoft.com/en-us/windows-hardware/drivers/ddi/content/wdfio/nc-wdfio-evt_wdf_io_queue_io_internal_device_control) I've converted every BRB submission to asynchronous I/O (https://docs.microsoft.com/en-us/windows-hardware/drivers/wdf/sending-i-o-requests-asynchronously) which avoids clogging up the queue dispatch callback and also slightly improved performance and resource usage (memory for request and payload buffer)
- EVT_WDF_IO_QUEUE_IO_STOP (https://docs.microsoft.com/en-us/windows-hardware/drivers/ddi/content/wdfio/nc-wdfio-evt_wdf_io_queue_io_stop) calls WdfRequestCancelSentRequest (https://docs.microsoft.com/en-us/windows-hardware/drivers/ddi/content/wdfrequest/nf-wdfrequest-wdfrequestcancelsentrequest) to complete pending requests sent to the I/O target (in this case our Bluetooth parent FDO)

Another step closer to finishing and hardening the profile/bus driver 🎉

Feb 18, 2019, 9:13 PM (https://localhost/post/1114)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

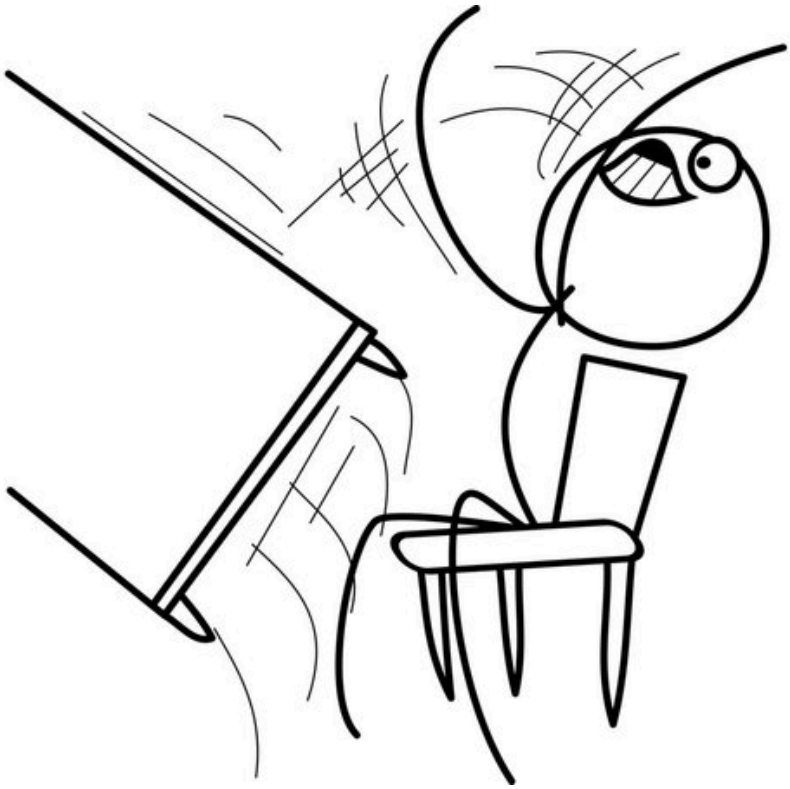
nefarius (https://localhost/user/nefarius) (https://localhost/user/nefarius)

Goddammit, I managed to make `bthport.sys` leak memory ☠️



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/0af8dce9-4a54-4a2c-8997-00b4302f7df7-image.png)

Time for code review! 🤦



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/f8f42c18-eff8-4356-821d-9242840c5764-image.png)

zzZ

Feb 19, 2019, 5:54 PM (https://localhost/post/1115)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

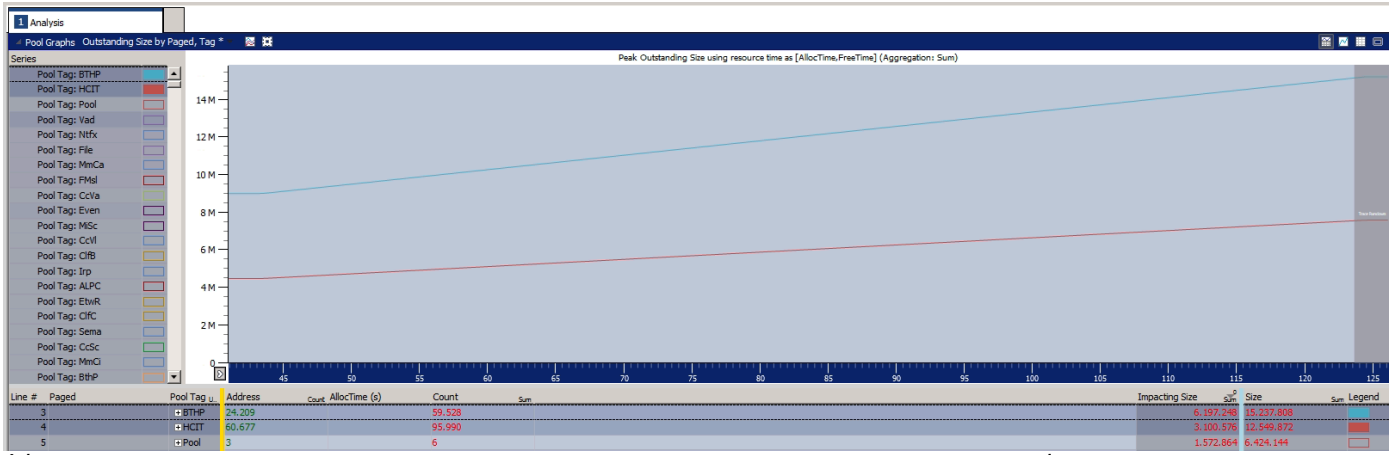
nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Aha! It only happens when I send data to the HID Control Channel, how interesting 🤔 We'll see about that... 🕵️

Feb 21, 2019, 7:51 PM (https://localhost/post/1116)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Seriously, how did I do that 😦



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/fb2e64d0-a643-4c1f-bbeb-1258dc7c6827-image.png)

Pool tag details:

```
BTHP - bthport.sys  - Bluetooth port driver (generic)
HCIT - bthport.sys  - Bluetooth port driver (HCI)
```

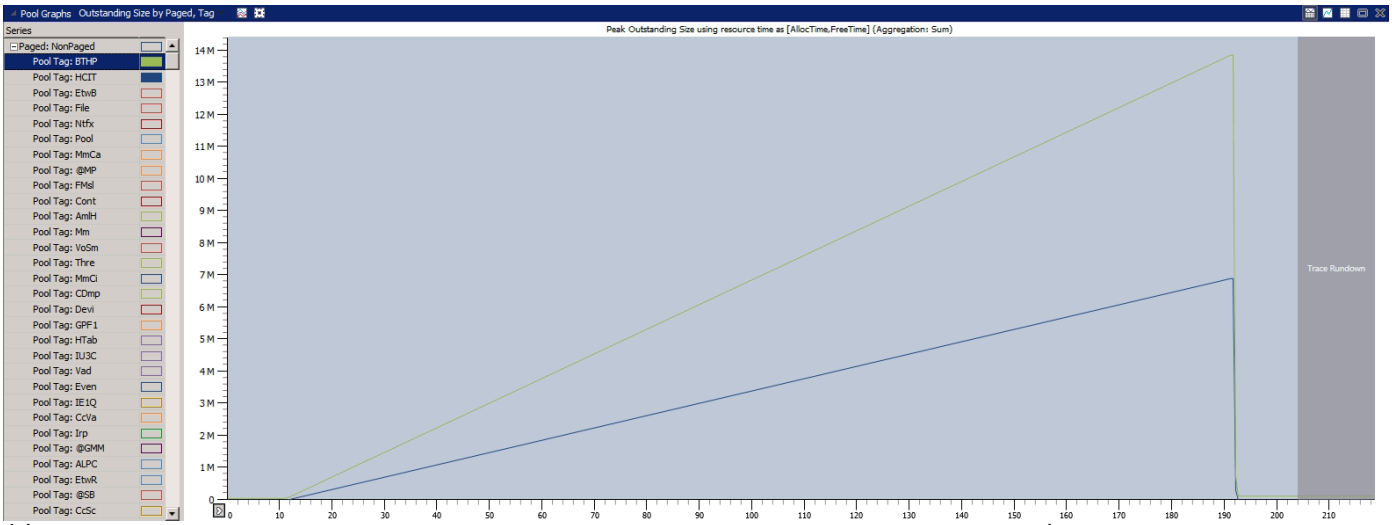
Now if the symbols could download faster than over 56k I could actually see more zzz

---

Feb 23, 2019, 8:36 PM (https://localhost/post/1124)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Better graph, still no clue 🙄

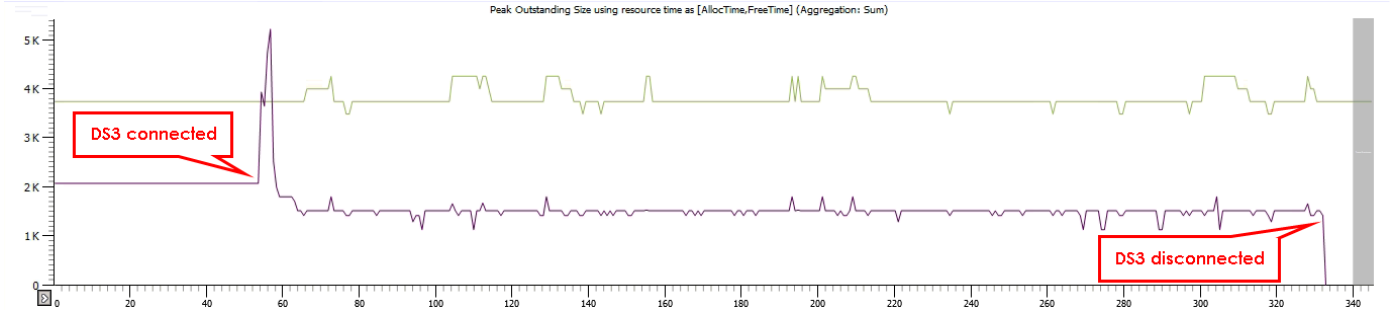


(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/672e2330-8588-48a9-bc71-85b0e9cf4b0a-image.png)

Feb 24, 2019, 2:12 PM (https://localhost/post/1128)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Ha, found it! 🎉 Now that's more like it:



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/a2b0a76d-1234-4c8b-9645-8a20ec4334ce-image.png)

Purple is non-paged memory from HCI-specific pool now only slightly jittering up and down as expected. Green is the BTHP pool which is now steady as well. The uneven bumps are probably owed to timing in the driver and probably latency on the radio link.

So what was the issue? Well, previously I was only writing to the HID Control Channel (periodically) because that's how the HID Output Report travels to the remote device. Now since I couldn't find any issues with my memory handling in my own drivers I was starting to experiment and implemented **reading** from the control channel (where there shouldn't be any data coming back because the DS3 sends data over the HID Interrupt Channel) as well and look at that: with every packet I send out there's **one byte** of "response" available to read as well! The content is always a solid `0x00` but still, this was allocating and holding memory in the lower sections of `bthport.sys` and the reason for the rise in non-paged memory usage. I'm now also periodically reading and therefore "emptying" the control channel and now it's not growing anymore. Nice!

Time for a break ☀️

Mar 2, 2019, 7:10 PM (https://localhost/post/1133)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

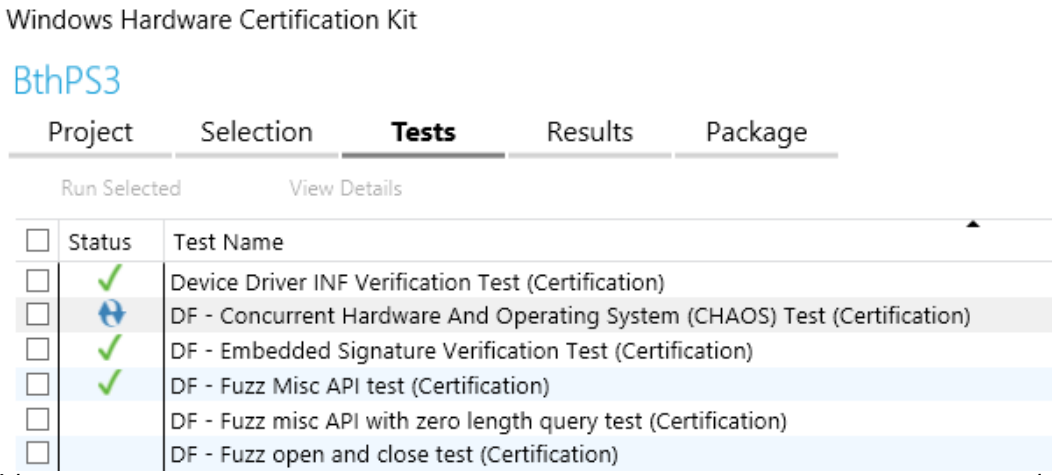
Guess some sort of Writer's Block got me, but for coding. No worries though, will do something else then until the spirits are up for it again 😄

Cheers 🥂

Mar 7, 2019, 10:03 PM (https://localhost/post/1136)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

I've currently "interrupted" further coding with building my WHQL lab. The progress on it gets its own thread here but since my Windows 7 test boxes are ready I'll throw the current revision of the profile driver into it and see what happens 😈



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/bdd6f230-7bd5-4489-9d1e-ff9982140566-image.png)

Mar 7, 2019, 10:54 PM (https://localhost/post/1137)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

E epikvigem (https://localhost/user/epikvigem)
(https://localhost/user/epikvigem)

Can't wait to connect my Ps3 controller via bluetooth to pc without installing malicious software 😄 (it's this project all about this right?, if yes, when it will be released? 😇)

Mar 8, 2019, 7:43 AM (https://localhost/post/1138)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@epikvigem (https://forums.vigem.org/uid/155) pretty much sums it up, yeah 😛 This set of drivers will allow you to use the popular PS3 peripherals (DualShock 3, Navigation & Move Controllers) transparently with little overhead on Windows 7 up to 10.

As for the estimated release schedule... If the current pace stays where it is I aim for early or mid May?

Cheers

Mar 8, 2019, 7:45 AM (https://localhost/post/1139)

 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

HCK had its run over night on the profile driver and look how happy it is 😅

Windows Hardware Certification Kit

BthPS3

Project | Selection | **Tests** | Results | Package

Run Selected | View Details | View By: Certification

Status	Test Name	Type	Length	Target	Machine(s)
✓	Device Driver INF Verification Test (Certification)		05m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - Concurrent Hardware And Operating System (CHAOS) Test (Certification)		01h 15m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - Embedded Signature Verification Test (Certification)		01m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - Fuzz Misc API test (Certification)		15m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - Fuzz misc API with zero length query test (Certification)		15m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - Fuzz open and close test (Certification)		15m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - Fuzz Query and Set File Information Test (Certification)		15m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - Fuzz Query and Set Security Test (Certification)		15m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - Fuzz random FSCTL test (Certification)		15m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - Fuzz random IOCTL test (Certification)		15m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - Fuzz sub-opens test (Certification)		15m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - Fuzz sub-opens with streams test (Certification)		15m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - Fuzz zero length buffer FSCTL test (Certification)		15m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - Fuzz zero length buffer IOCTL test (Certification)		15m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - PNP Cancel Remove Device Test (Certification)		08m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - PNP Cancel Stop Device Test (Certification)		08m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - PNP DIF Remove Device Test (Certification)		08m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - PNP Disable And Enable Device Test (Certification)		08m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - PNP Rebalance Fail Restart Device Test (Certification)		08m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - PNP Rebalance Request New Resources Device Test (Certification)		08m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - PNP Remove Device Test (Certification)		08m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - PNP Stop (Rebalance) Device Test (Certification)		08m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - PNP Surprise Remove Device Test (Certification)		08m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - Reinstall with IO Before and After (Certification)		01h 30m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	DF - Sleep and PNP (disable and enable) with IO Before and After (Certification)		45m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	Wdf - Check Kmdf Coinstaller Version Test		02m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	Wdf - Check Kmdf Function Table Test		01m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	Wdf - Kmdf Fault Injection Test		12m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1
✓	Wdf - Verify Driver Load Order Group is not WdfLoadGroup		02m	PlayStation(R) 3 Peripherals Profile Driver	LABW7X64-1

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/76f129b3-e1ce-46f2-bbaf-8504840ef178-image.png)

Next I have to polish and test the filter driver and extend it with a few management features (like turning it on or off from user-land).

Mar 8, 2019, 9:22 AM (https://localhost/post/1140)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

L

Locksmith (https://localhost/user/locksmith)
(https://localhost/user/locksmith)

@nefarius (https://forums.vigem.org/uid/1) this looks awesome! Really looking forward to seeing this in production! Is there anything we as a community can do or provide to assist your work? Beta testing, experiment with various BT dongles/pads, or just show interest in your product? 🙂 What kind of licensing are you thinking about once this is ready? Propriety paid/free, open source and all its variations, dual - community version open source (without binaries) VS paid WHQL certified?

Mar 8, 2019, 8:59 PM (https://localhost/post/1141)

(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius) (https://localhost/user/nefarius)

@Locksmith (https://forums.vigem.org/uid/138) pardon the delay, I wanted to answer this in detail as it contains a lot of interesting and valid questions.

Community involvement

I will be getting to a stage where the full stack can be tested and I would greatly appreciate it if I get a few owners of those obviously "fake" and aftermarket DualShock "PANHAI" controllers since I can't order them in my country and back in SCP-days a rather large demographic was interested in getting them to work as they typically only cost around 10$. I'm not a fan of those personally but if they work on the stack with ease, be my guest 😉 As I own the genuine Sony hardware I can guarantee a 100% compatibility for those obviously. Just a heads-up: I won't give out production-signed binaries to beta testers anymore though as that's irresponsible. So anybody interested would be required to put his or her machine into test mode (https://docs.microsoft.com/en-us/windows-hardware/drivers/install/the-testsigning-boot-configuration-option). Usually not a big deal but I've heard that a few anti-cheat and DRM solutions out there won't let you launch certain games anymore until reverted.

Dongle compatibility shouldn't be much of an issue anymore as the vendor software stack is kept in place and isn't touched anymore (unlike SCP) so e.g. Intel Wireless cards will keep operating with the Intel vendor driver. Tests welcome though nonetheless.

Last but not least I ofc. welcome interest in my post-~~apocalyptic~~SCP shenanigans 😉 I've launched into this mess out of personal motivation; getting comfortable with yet another kernel-mode driver, the Windows Bluetooth Driver Interface, WHQL-fun and maybe finally getting a finished plug-and-play solution so I can visit my couch again and play Castlevania 😆 A lot of what's happening here currently is straight out research and development. As a lot of people are apparently not understanding (or accepting) what "work in progress" means I keep "advertising" for the forum etc. to a minimum as long as there's not enough resources for me to research, develop, give support, regularly update news etc. This doesn't mean I want to stay in my own bubble here, I welcome anybody interested but in return I expect acceptance if things don't quite go according to plan.

Licensing

Despite a few "hiccups" I've had with larger corporations ~~taking my stuff~~ being a bit clumsy in the past I'm still a big advocate and believer in open-source. First and foremost because I'd probably not be in this "business" of dealing with gaming peripherals if the mad lad creating SCP hadn't open-sourced his or her work plus all of the other fabulous projects and samples I profited of by studying the sources. This also includes non-Windows sources like bits and pieces in the Linux kernel or Arduino projects. So I'll definitely open-source this stack as well once I tag it production-ready.

Now one might ask why this time I didn't go for GitHub from the very beginning but use a private Git repository instead. It makes developing the back-doors so much easier! 😆 Jokes aside, once again this is another measure I had to take to protect myself from idiocy. What I've noticed over the years is that non-developers who find something interesting on GitHub usually ignore the README and other helpful resources completely, get confused because there is no "download EXE here now" button and then come haunt and annoy me and my team with questions that could've been avoided from the very start. I have no problem with answering questions but if I get used as a search engine replacement I take that as a personal offense as you clearly show me that you don't value my time. Phew, that went sour fast 😅

Back to licensing. With upcoming releases I'm gonna include an EULA to both protect myself (you know, warranty, haha) and probably place some restrictions on it regarding commercial use. Maybe dual-licensing it. Again, there are reasonable motivations behind it. To private individuals I wanna ensure all the freedom and openness as possible as that's the target demographic. Corporations though are dumb. What do I mean by that? Well, just forking a driver, re-branding and releasing it (not that this has happened before, huehuehue) is a horrible practice. Drivers need maintenance and the knowledge on how to maintain them properly. If they cause an issue on an end-users machine it needs to be diagnosed and addressed. Can they provide that? No, they'll conveniently send them to me who's expected to give free support and fix everything. Nope, get fucked, GPL and other restrictions it will be for you then. I haven't settled on the best solution there yet but I'm working on ideas that benefit all sides as much as possible.

Regarding WHQL... Binaries without it aren't really worth it nowadays so it's either just the sources and have fun or a properly signed binary. Could I sell it? Eh. Would it sell? Eh. Would I take a few Schekels if offered? Oh, absolutely, the bills haven't stopped 🤣 I need to figure this out. Bring back donations? Eh. Maybe they'll flourish again if a finished attractive product is released? So many questions, so little time. We'll figure it out 😀

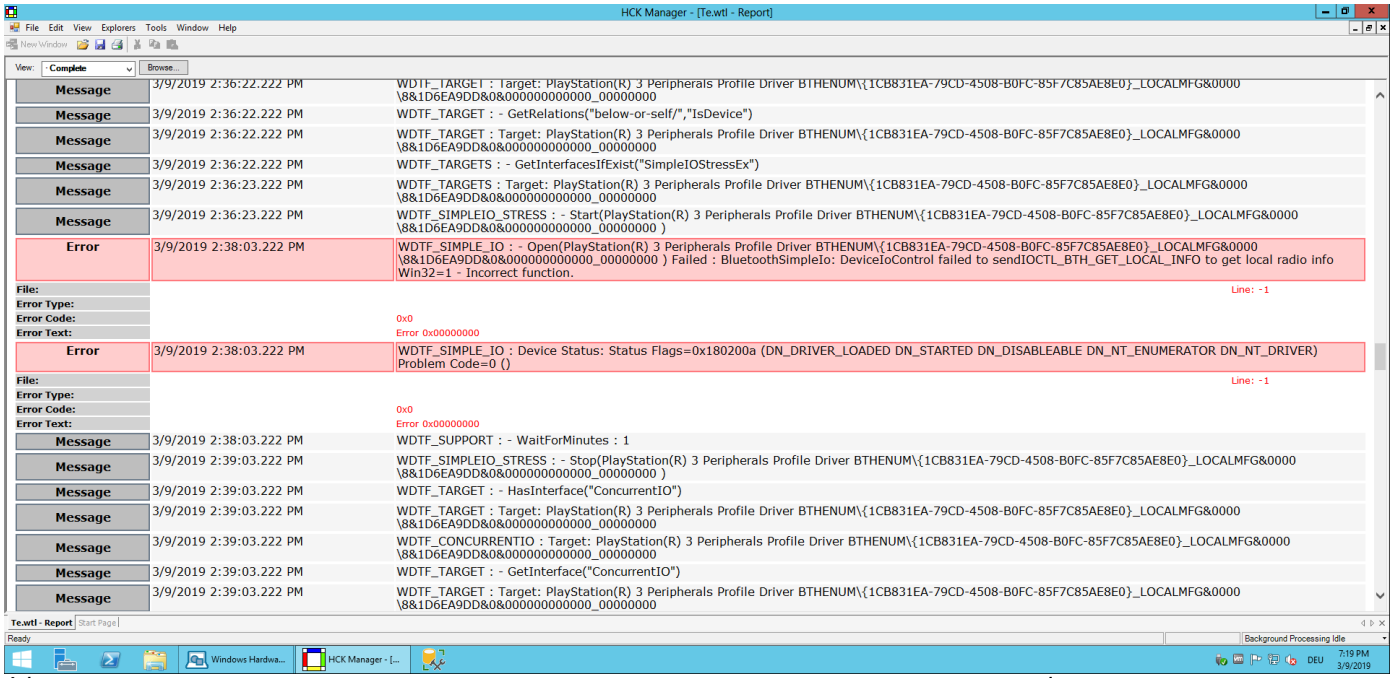
I think I've got everything out I wanted to address, pardon the wall of text 😅

Cheers

Mar 9, 2019, 7:23 PM (https://localhost/post/1142)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

(https://localhost/user/nefarius) nefarius (https://localhost/user/nefarius)

Meh, HCK tests on Windows 8.1 do a bit more in-depth Bluetooth testing it seems and it's complaining that I've left out some I/O handlers I thought I don't need. Well, can't argue against *the machine* so back to hacking and fixing 💀

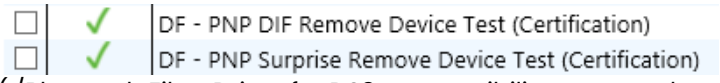


(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/34182df1-4525-4f2f-9bdc-9941ffabf32f-image.png)

Mar 9, 2019, 7:53 PM (https://localhost/post/1143)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

There we go! 😃

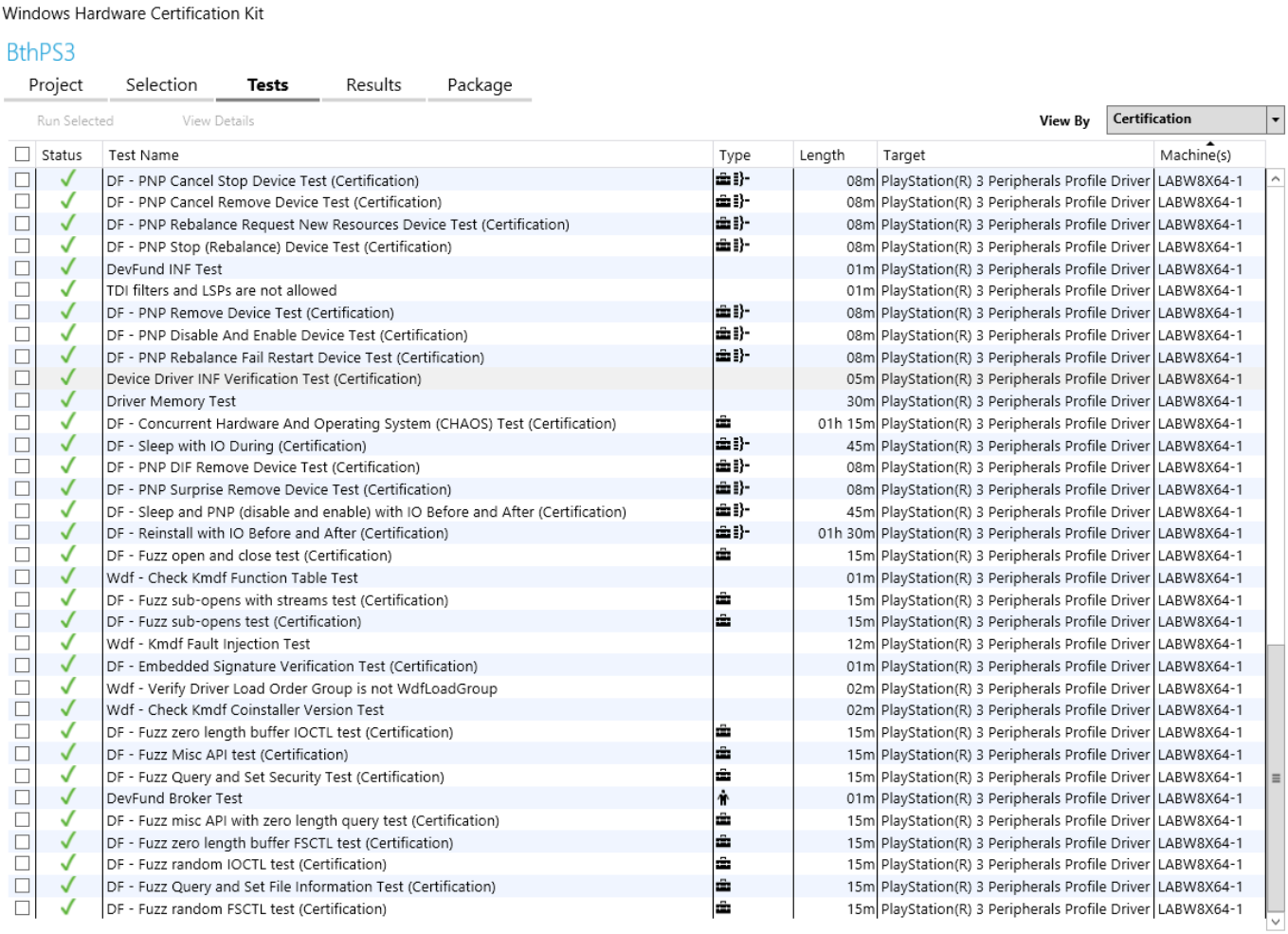


(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/e8e9995d-4abf-45e6-b82d-94e61c28e311-image.png)

Mar 10, 2019, 9:00 AM (https://localhost/post/1144)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Another night of wasting electricity done but the results at least are satisfying 😁



Status	Test Name	Type	Length	Target	Machine(s)
✓	DF - PNP Cancel Stop Device Test (Certification)		08m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - PNP Cancel Remove Device Test (Certification)		08m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - PNP Rebalance Request New Resources Device Test (Certification)		08m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - PNP Stop (Rebalance) Device Test (Certification)		08m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DevFund INF Test		01m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	TDI filters and LSPs are not allowed		01m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - PNP Remove Device Test (Certification)		08m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - PNP Disable And Enable Device Test (Certification)		08m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - PNP Rebalance Fail Restart Device Test (Certification)		08m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	Device Driver INF Verification Test (Certification)		05m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	Driver Memory Test		30m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - Concurrent Hardware And Operating System (CHAOS) Test (Certification)		01h 15m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - Sleep with IO During (Certification)		45m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - PNP DIF Remove Device Test (Certification)		08m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - PNP Surprise Remove Device Test (Certification)		08m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - Sleep and PNP (disable and enable) with IO Before and After (Certification)		45m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - Reinstall with IO Before and After (Certification)		01h 30m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - Fuzz open and close test (Certification)		15m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	Wdf - Check Kmdf Function Table Test		01m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - Fuzz sub-opens with streams test (Certification)		15m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - Fuzz sub-opens test (Certification)		15m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	Wdf - Kmdf Fault Injection Test		12m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - Embedded Signature Verification Test (Certification)		01m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	Wdf - Verify Driver Load Order Group is not WdfLoadGroup		02m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	Wdf - Check Kmdf Coinstaller Version Test		02m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - Fuzz zero length buffer IOCTL test (Certification)		15m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - Fuzz Misc API test (Certification)		15m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - Fuzz Query and Set Security Test (Certification)		15m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DevFund Broker Test		01m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - Fuzz misc API with zero length query test (Certification)		15m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - Fuzz zero length buffer FSCTL test (Certification)		15m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - Fuzz random IOCTL test (Certification)		15m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - Fuzz Query and Set File Information Test (Certification)		15m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1
✓	DF - Fuzz random FSCTL test (Certification)		15m	PlayStation(R) 3 Peripherals Profile Driver	LABW8X64-1

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/e4024742-8380-48fd-8cba-dad69cfe6a90-image.png)

Next I'll test with children connected. Not sure how it'll react since the power and sleep tests will most certainly disconnect them from the Bluetooth host but we'll see!

Mar 10, 2019, 11:23 AM (https://localhost/post/1145) (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius) (https://localhost/user/nefarius)

I was bitching a lot about the Hardware Lab Kit and debugging utilities in general in the past but to perfectly honest; the more I become familiar with them and overcome their quirks the more I appreciate the feedback they provide.

Like for example; I've tried to connect a DS3 while the profile driver is running under Driver Verifier (which in short means that a strong rule-set applies triggering bugs that might have gone under) on Windows 8.1 and it crashed with:

```
KMODE_EXCEPTION_NOT_HANDLED (1e)
This is a very common bugcheck.  Usually the exception address pinpoints
the driver/function that caused the problem.  Always note this address
as well as the link date of the driver/image that contains this address.
Arguments:
Arg1: ffffffff80000003, The exception code that was not handled
Arg2: fffff801f61cd3c0, The address that the exception occurred at
Arg3: 0000000000000000, Parameter 0 of the exception
Arg4: 7efefefefeff3252, Parameter 1 of the exception
```

Once in WinDbg with the symbols loaded we get a nice "stack trace":

```
STACK_TEXT:
... : nt!KeBugCheckEx
... : nt!KiFatalExceptionHandler+0x22
... : nt!RtlpExecuteHandlerForException+0xd
... : nt!RtlDispatchException+0x1a5
... : nt!KiDispatchException+0x18d
... : nt!KiExceptionDispatch+0xc2
... : nt!KiBreakpointTrap+0x2dc
... : nt!DbgBreakPoint+0x1
... : Wdf01000!FxIoTargetSendIoctl+0x282da
... : Wdf01000!imp_WdfIoTargetSendIoctlSynchronously+0x48
... : BthPS3!L2CAP_PS3_HandleRemoteConnect+0x16a [e:\development\gogs\bthps3\bthps3\l2cap.c @ 49]
... : BthPS3!BthPS3_IndicationCallback+0x9c [e:\development\gogs\bthps3\bthps3\bluetooth.c @ 552]
... : bthport!L2CapInt_ProcessL2capConnectReq+0x40b
... : bthport!L2CapInt_ProcessSignallingPacket+0x45f
... : bthport!L2CapInt_ProcessReadBip+0x13a
... : bthport!HCI_ProcessAclReadBip+0x661
... : bthport!HCI_ProcessAclRead+0x2a8
... : bthport!HCI_ProcessMpBip+0x92
... : bthport!BTHPORT_RecvMpBip+0x41
... : BTHUSB!BthUsb_ReadTransferComplete+0x18d
... : BTHUSB!UsbWrapWorkRoutine+0x18d
... : BTHUSB!UsbWrapInterruptReadComplete+0x1d3
... : nt!IovpLocalCompletionRoutine+0x174
... : nt!IopfCompleteRequest+0x2ee
... : nt!IovCompleteRequest+0x1d7
... : Wdf01000!FxRequest::CompleteInternal+0x23c
... : Wdf01000!imp_WdfRequestComplete+0x8c
... : BthPS3PSM!UrbFunctionBulkInTransferCompleted+0x107 [e:\development\gogs\bthps3\bthps3psm\filter.c @ 23
3]
... : Wdf01000!FxRequestBase::CompleteSubmitted+0x459
... : Wdf01000!FxIoTarget::_RequestCompletionRoutine+0x162
... : nt!IopUnloadSafeCompletion+0x49
... : nt!IovpLocalCompletionRoutine+0x174
... : nt!IopfCompleteRequest+0x2ee
... : nt!IovCompleteRequest+0x1d7
... : USBPORT!USBPORT_Core_iCompleteDoneTransfer+0xa02
... : USBPORT!USBPORT_Core_iIrpCsqCompleteDoneTransfer+0x21c
... : USBPORT!USBPORT_Core_UsbIocDpc_Worker+0x238
... : USBPORT!USBPORT_Xdpc_Worker_IocDpc+0x1fe
... : nt!KiExecuteAllDpcs+0x1b0
... : nt!KiRetireDpcList+0xd7
... : nt!KiIdleLoop+0x5a
```

Alrighty, so line 49 in the function `L2CAP_PS3_HandleRemoteConnect` in `l2cap.c` of the driver `BthPS3` is triggering the fault. Let's see what's there:

```
46      //
47      // Request remote name from radio for device identification
48      //
49      status = BTHPS3_GET_DEVICE_NAME(
50          DevCtx->Header.IoTarget,
51          ConnectParams->BtAddress,
52          remoteName
53      );
```

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/aa26ddef-fe79-44b6-86a7-b926f86433be-image.png)

Ah, an inline function! What does it contain that might bomb? I have a suspicion (mostly because it's hinted in the stack trace 😉)...

```
291         status = WdfIoTargetSendIoctlSynchronously(
292             IoTarget,
293             NULL,
294             IOCTL_BTH_GET_DEVICE_INFO,
295             InputBuffer:&MemoryDescriptor,
296             OutputBuffer:&MemoryDescriptor,
297             NULL,
298             NULL
299         );
```

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/1fb3a003-67bc-40b5-b66e-d24d26a82546-image.png)

Let's have a look at the docs of `WdfIoTargetSendIoctlSynchronously` and check out the requirements section (https://docs.microsoft.com/en-us/windows-hardware/drivers/ddi/content/wdfiotarget/nf-wdfiotarget-wdfiotargetsendioctlsynchronously#requirements):

> IRQL PASSIVE_LEVEL

Hm, but our L2CAP callback is invoked at `PASSIVE_LEVEL`, right? Let's throw in some tracing and have another run:

```
2019/03/10-10:46:19.023 TRACE_LEVEL_VERBOSE     BthPS3_IndicationCallback Entry (Low (0x00))
2019/03/10-10:46:19.023 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnect Entry (Low (0x00))
2019/03/10-10:46:19.038 TRACE_LEVEL_VERBOSE     BthPS3_IndicationCallback Entry (DPC (0x02))
2019/03/10-10:46:19.038 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnect Entry (DPC (0x02))
```

Hey! 😠 The second call isn't at `PASSIVE_LEVEL`, that's `DISPATCH_LEVEL`! How dare you! Oh wait, the docs, check the docs (https://docs.microsoft.com/en-us/windows-hardware/drivers/ddi/content/bthddi/nc-bthddi-pfnbthport_indication_callback#requirements):

> IRQL Developers should code this function to operate at either IRQL = DISPATCH_LEVEL (if the callback function does not access paged memory), or IRQL = PASSIVE_LEVEL (if the callback function must access paged memory)

Ouch! How evil! 😅 So that can totally happen and `!wdfkd.wdflogdump` gives clear insights:

```
1: kd> !wdfkd.wdflogdump BthPS3
...
37: FxVerifierCheckIrqlLevel - Called at wrong IRQL; at level 2, should be at level 0
---- end of log ----
```

Right, so this would've fallen under the radar if it didn't bomb in the lab. Thanks, WHQL 😝 Onward with the fixes!

Mar 10, 2019, 6:10 PM (https://localhost/post/1146)
□ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 □ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

kirian (https://localhost/user/kirian) (https://localhost/user/kirian)

How future proof is this filter solution? Do you think it is possible for Windows to make such a change in a update that could break it or you think that is unlikely or just straight up impossible unless windows change in a fundamental way?

Sorry if this is no place to ask or if my question does not make much sense. I am no developer/coder in any meaningful way, but I know just enough about coding to understand your posts here and I find it really interesting to know how this actually works. I would really appreciate to hear your thoughts on this with some insight on why and how windows could or couldn't break this in the near future.
Also, thanks for your work on the ScpToolKit and on maintaining this posts on the development! I find myself refreshing this page many times a day just to see your explanations on how you are making your way through this.

Mar 10, 2019, 8:40 PM (https://localhost/post/1147)
□ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1 □ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius) (https://localhost/user/nefarius)

@kirian (https://forums.vigem.org/uid/158) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1146):

> How future proof is this filter solution? Do you think it is possible for Windows to make such a change in a update that could break it or you think that is unlikely or just straight up impossible unless windows change in a fundamental way?

Heya! This is actually the most future-proof you can get. Apart from the filter driver which proxies the *forbidden* PSMs the profile/bus driver uses a standard DDI (Device Driver Interface) provided by Microsoft which exists since (at least) Windows XP and is documented fairly well (see here (https://docs.microsoft.com/en-us/windows-hardware/drivers/bluetooth/using-the-bluetooth-driver-stack) and here (https://github.com/Microsoft/Windows-driver-samples/tree/master/bluetooth)). Microsoft is the grand master of backwards compatibility so I expect this to last quite a fair bit without the need of updates once it's deemed stable.

@kirian (https://forums.vigem.org/uid/158) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1146):

> Sorry if this is no place to ask or if my question does not make much sense. I am no developer/coder in any meaningful way, but I know just enough about coding to understand your posts here and I find it really interesting to know how this actually works. I would really appreciate to hear your thoughts on this with some insight on why and how windows could or couldn't break this in the near future.

Perfectly fine to ask here, this thread isn't meant to be only fed by myself, it's just my chaotic attempt of Rubber Duck Debugging and leaving a trail of insights on this "black magic" in kernel land 😉 Research and development as I like to call it.

I mean as far as the profile driver goes since it's a common practice to write profile drivers (well, probably not anymore because literally any standard device has one already) and the API is "official" and not some binary patching nonsense I'm pretty confident that this will outlive at least SCP 😝

As for the PSM proxy... That's a bit of a *risky* move because I'm shipping around a function that was probably designed with a meaningful goal in mind and here I walz in and build a bridge across the forbidden river 😉 We will see, I guess 😇

Also this method is far more likely to pass WHQL as I don't have to run the whole test battery directly against the USB device itself since the original driver is kept in place. With AirBender/WireShock I'd probably get a few dirty looks when I submit an INF file with a couple of dozen Hardware IDs which aren't mine to the Microsoft Portal 😉 Plus the user gets to keep all of their other Bluetooth devices connected, isn't that lovely 👍

@kirian (https://forums.vigem.org/uid/158) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1146):

> Also, thanks for your work on the ScpToolKit and on maintaining this posts on the development! I find myself refreshing this page many times a day just to see your explanations on how you are making your way through this.

Glad to hear I'm not only feeding my echo chamber 😆 Yeah, SCP's kind of my Dark Ages, it changed me in a lot of ways. Thanks for sticking around and showing interest 😃

Cheers

Mar 14, 2019, 4:34 PM (https://localhost/post/1152) □ □ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 □ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

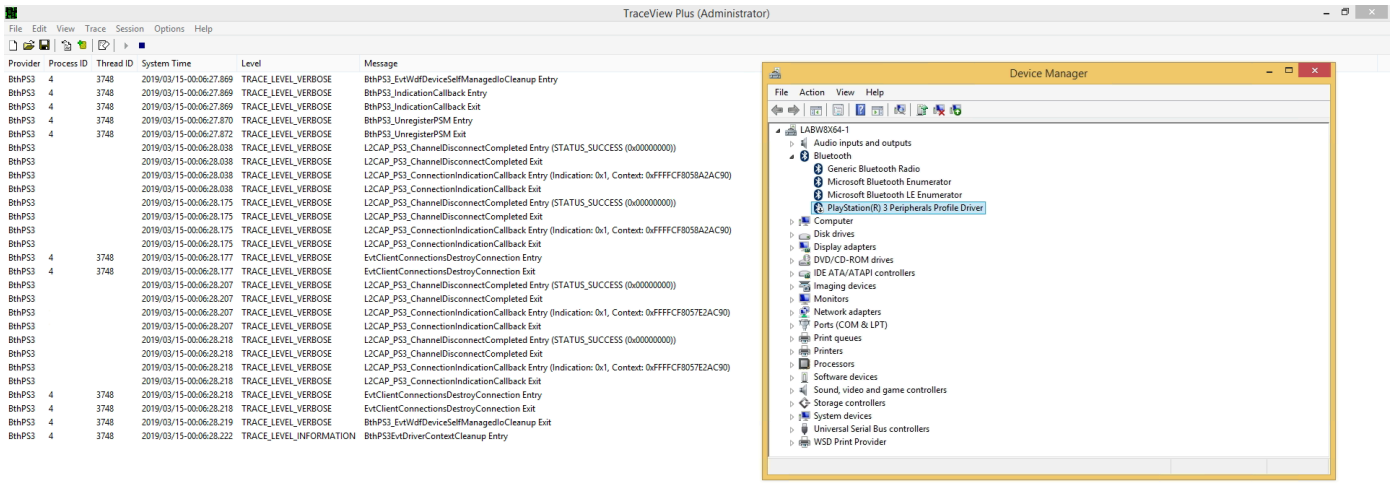
 nefarius (https://localhost/user/nefarius) (https://localhost/user/nefarius)

Hm, disabling/shutting down the profile device causes crashes due to referencing freed memory. Next challenge is to trace along the whole connection/disconnection state machine and identify race conditions and whatnot 😪

Mar 15, 2019, 12:11 AM (https://localhost/post/1153) □ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1 □ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius) (https://localhost/user/nefarius)

Let's welcome this new week by finishing a major bug fix: properly hardening the shutdown sequence to disconnect remote devices and free resources afterwards 🤠



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/972d30ca-3706-4250-832d-f6d3d84ad145-image.png)

Now entering hibernation zzZ

Mar 15, 2019, 7:26 PM (https://localhost/post/1154)

(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

P (https://localhost/user/pnkiller78) pnkiller78 (https://localhost/user/pnkiller78)

@nefarius (https://forums.vigem.org/uid/1) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1153):

> Now entering hibernation zzZ

I really liked that one 😂 I registered to the forum just to reply to this...

Now getting serious, I've been following this topic, let me tell you that is awesome. I was a programmer myself when I was young, like 20 years ago, nothing like this, mostly enterprise application, databases and stuff, so I have a fair idea of the whole development process thing. This thread has been very interesting to follow, I didn't know how many things got involved in developing drivers and stuff related to hardware, very interesting.
Also, your previous post about hunting the bug related to the crash when device got disabled, it got me thinking in other things that could happen that could be related...

What happens when

1. The controller is moved out of range of the bluetooth receiver
2. The bluetooth receiver is disabled in the Device Manager (eg. if the receiver is embedded in a wifi card like the Intel ones on laptops)
3. The bluetooth receiver is disconnected from the host (eg. the receiver it's a USB dongle type)
4. If the controller get connected to host via USB cable while operating/connected via Bluetooth protocol, do it still operates or got it disconnected???
5. Does the controller start to charge its internal battery when is connected to host via USB cable?

I'm sure you already considered this scenarios, but I got curious about the answer to this events.
Anyway, let thank your for your effort in this, I really appreciate it.
It's really amazing to see that somebody got the time, knowledge and motivation to write this. In other OS like linux, this works out-of-the-box, also on NVidia Shield TV, but on windows it's disappointing to have to resort to third-party solutions to be able use our gamepads properly.

Also, what is the HARDWARE id that get reported to OS when the PS3 controllers are connected via this driver?

Mar 15, 2019, 8:26 PM (https://localhost/post/1155)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@pnkiller78 (https://forums.vigem.org/uid/171) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1154):

> Now getting serious, I've been following this topic, let me tell you that is awesome. I was a programmer myself when I was young, like 20 years ago, nothing like this, mostly enterprise application, databases and stuff, so I have a fair idea of the whole development process thing. This thread has been very interesting to follow, I didn't know how many things got involved in developing drivers and stuff related to hardware, very interesting.

Welcome, mate 🙂 I've been trying to steer my career towards programming as a full-time profession but so far that hasn't really worked so I went back to doing everything the way I like and devote time to device driver development. Not my loss so far 😝 I struggled a lot in the past while developing the other projects and found this style of "blogging" to be a good way to both reflect on what I've been doing and as a reference and timeline for myself and other people interested. Sounds like it's a good strategy.

@pnkiller78 (https://forums.vigem.org/uid/171) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1154):

> Also, your previous post about hunting the bug related to the crash when device got disabled, it got me thinking in other things that could happen that could be related... What happens when

Thanks for participating, let's go through the points one by one:

@pnkiller78 (https://forums.vigem.org/uid/171) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1154):

> The controller is moved out of range of the bluetooth receiver

Then after a certain timeout the host driver (the one which controls the Bluetooth host device, a.k.a. "stock driver") will initiate a disconnect sequence and notifies the profile driver that the device is gone and now my clean-up code takes over. So far this case is handled properly. Should test it though 🤔

@pnkiller78 (https://forums.vigem.org/uid/171) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1154):

> The bluetooth receiver is disabled in the Device Manager (eg. if the receiver is embedded in a wifi card like the Intel ones on laptops)

That's a typical power down event and since the profile driver is a child of the `bthport.sys` which then gets unloaded it receives shutdown indication as well and needs to dispose all connections and free memory before unloading the profile driver. So far this is handled already.

@pnkiller78 (https://forums.vigem.org/uid/171) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1154):

> The bluetooth receiver is disconnected from the host (eg. the receiver it's a USB dongle type)

This case is called "surprise removal" and is also handled. When the parent is gone, the whole stack gets demolished. The profile children (PDOs) get removed, the profile driver enters clean-up and unloads, then the stock drivers unload. This is also implemented and tested.

@pnkiller78 (https://forums.vigem.org/uid/171) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1154):

> If the controller get connected to host via USB cable while operating/connected via Bluetooth protocol, do it still operates or got it disconnected???

This is in fact an absurd case because the SIXAXIS/DS3 does *not* disconnect from Bluetooth when connected to USB while also connected wireless. That's a scenario I haven't tackled yet ❗

@pnkiller78 (https://forums.vigem.org/uid/171) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1154):

> Does the controller start to charge its internal battery when is connected to host via USB cable?

Yes, despite all the BS and false information you find on the web there is no special driver required for the controller to charge via a standard 500 mA USB outlet. It also charges with a simple mobile phone charger, if it doesn't it has a hardware issue, not a software one. It does *report* battery charge level via software though on both USB and Bluetooth.

@pnkiller78 (https://forums.vigem.org/uid/171) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1154):

> I'm sure you already considered this scenarios, but I got curious about the answer to this events.

I try to think of all aspects, especially because I wanna get this through WHQL so the quality and robustness has to be stellar 😉

@pnkiller78 (https://forums.vigem.org/uid/171) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1154):

> Anyway, let thank your for your effort in this, I really appreciate it.
> It's really amazing to see that somebody got the time, knowledge and motivation to write this. In other OS like linux, this works out-of-the-box, also on NVidia Shield TV, but on windows it's disappointing to have to resort to third-party solutions to be able use our gamepads properly.

Thanks, I might have just slipped into insanity without noticing 😆 Seriously though, it's been quite the challenge getting this and real-life obstacles handled in one go but as I'm adapting my life to support this stuff I might be able to keep this rodeo going until production-ready 😅 Linux has the advantage of the open kernel and

contributors have added the Sony-specific customization a long time ago. On Windows you need to play after the rules of Microsoft. And dance with the devil in kernel-land where the forbidden fruits grow and magic can be found even to this day!

@pnkiller78 (https://forums.vigem.org/uid/171) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1154):

> Also, what is the HARDWARE id that get reported to OS when the PS3 controllers are connected via this driver?

I created some custom, GUID-based Hardware IDs the function drivers will use in the future.

Hope I got everything, cheers!

Mar 15, 2019, 9:13 PM (https://localhost/post/1156)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

P pnkiller78 (https://localhost/user/pnkiller78)
(https://localhost/user/pnkiller78)

@nefarius (https://forums.vigem.org/uid/1) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1155):

> Hope I got everything, cheers!

Wow, I'm really impressed... I'm pretty sure that I'm going to use this driver when it get released intro production. I only regret having bought a Mayflash Wireless Adapter like 3-4 months ago to use my SIXAXIS/DS3 wireless without having to sacrifice the bluetooth receiver on a PC that I use to play retro games. 😅 I needed to use a wireless headphones to play at night, so that's why I needed the bluetooth device on the host working with standard drivers (not dedicated to just the controller), to be able to connect the headphones... you know, I didn't want the wife to be mad at me for being playing games at night.... 😒

I forgot to ask... how is going to be the process to pair the controller with the host receiver? I don't remember exactly, but in the old days of ScpToolkit and Motioninjoy there was a small utility to set the host's bluetooth mac to which the controller should connect when the user pressed the PS button... please correct me if I'm wrong... how is going to be now?

Mar 15, 2019, 10:11 PM (https://localhost/post/1157)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@pnkiller78 (https://forums.vigem.org/uid/171) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1156):

> I forgot to ask... how is going to be the process to pair the controller with the host receiver? I don't remember exactly, but in the old days of ScpToolkit and Motioninjoy there was a small utility to set the host's bluetooth mac to which the controller should connect when the user pressed the PS button... please correct me if I'm wrong... how is going to be now?

That's still the same; you send a single request to the device via USB updating the host MAC address it shall connect to. This can be done via SCP, FireShock or even WinUSB and a bit of custom code. No biggie.

I'll provide a tool for that.

Mar 16, 2019, 11:58 AM (https://localhost/post/1158)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Ugh, I'm on a hunt. A bug hunt. And it's always issues I've introduced myself 😆

```
2: kd> !analyze -v
*******************************************************************************
*                                                                             *
*                        Bugcheck Analysis                                    *
*                                                                             *
*******************************************************************************

DRIVER_IRQL_NOT_LESS_OR_EQUAL (d1)
An attempt was made to access a pageable (or completely invalid) address at an
interrupt request level (IRQL) that is too high.  This is usually
caused by drivers using improper addresses.
If kernel debugger is available get stack backtrace.
Arguments:
Arg1: ffffe000c63b0dd4, memory referenced
Arg2: 0000000000000002, IRQL
Arg3: 0000000000000000, value 0 = read operation, 1 = write operation
Arg4: fffff800ccac6434, address which referenced memory
```

`DRIVER_IRQL_NOT_LESS_OR_EQUAL` is the most misleading bugcheck there is because the IRQL has little to do with this particular case, it's just me accessing freed memory:

```
FAULTING_SOURCE_CODE:
  1257:         brb->RemainingBufferSize
  1258:     );
  1259:
  1260:     deviceCtxHdr->ProfileDrvInterface.BthFreeBrb((PBRB)brb);
> 1261:     WdfRequestCompleteWithInformation(
  1262:         Request,
  1263:         Params->IoStatus.Status,
  1264:         brb->BufferSize
  1265:     );
  1266: }
```

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/ca8ee713-3e75-4251-8632-5c2c9e29e881-image.png)

A classic 😁

Mar 18, 2019, 2:11 PM (https://localhost/post/1165)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

D da2ce7 (https://localhost/user/da2ce7)
(https://localhost/user/da2ce7)

Hello @nefarius (https://forums.vigem.org/uid/1),
What wonderful work you have been doing!

If you could put the code on github, (possibly just your “src” ans “include” directories {and licence of course}, so that noobs won’t compile and break their system.). It would allow some of us to have a more in-depth read-through of your code.

Otherwise, keep up the amazing work; I look forward to seeing the code in person.

Cam.

Mar 18, 2019, 2:55 PM (https://localhost/post/1166)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@da2ce7 (https://forums.vigem.org/uid/172) Greetings. The plan is indeed to move to GitHub once the project is mature and stable enough. Right now it will stay private 😄

Mar 23, 2019, 9:35 PM (https://localhost/post/1171)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Pop the champagne, another milestone reached 🍾

SIXAXIS/DualShock 3 and Navigation controller playable through Shibari

 Youtube Video (https://youtu.be/4U62laA5zpw)

After all this time of tinkering and watching byte streams I wanted to experience some results so I've modded Shibari (https://github.com/ViGEm/Shibari) to support the exposed children of the `BthPS3` bus and look at them go 😄

Now I can enter some serious testing and do benchmarks without having to write the function driver. In this example the bus children are in Raw PDO mode meaning that the PNP-Manager will bring them up without a function driver required and exposes them to user-land applications which then can talk to them via classic Win32-API `CreateFile` (https://docs.microsoft.com/en-us/windows/desktop/api/fileapi/nf-fileapi-createfilea) and `DeviceIoControl` (https://docs.microsoft.com/en-us/windows/desktop/api/ioapiset/nf-ioapiset-deviceiocontrol).

This is of course only an "intermediate stage", I'll still provide HID-minifilter drivers so no additional software will be required to expose the controllers via HID/DI and (probably) XInput.

Stay tuned!

Mar 26, 2019, 8:31 PM (https://localhost/post/1174)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 2
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Castlevania Chronicles Pro-Gameplay by Gordon Freeman

 Youtube Video (https://youtu.be/oFWnXQjG2jg)

Pardon the shit quality, recorded this on my HTPC for authenticity and the i3 wasn't really happy 😅

---

9 DAYS LATER

Apr 4, 2019, 3:50 PM (https://localhost/post/1185)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

L Locksmith (https://localhost/user/locksmith)
(https://localhost/user/locksmith)

@nefarius (https://forums.vigem.org/uid/1) Looking good there! Almost like it's ready for beta testers? 😄 It's been over a week without updates on my favorite tech blog! 😉

!ERAU QSSI DLRO WEHT

Apr 4, 2019, 8:48 PM (https://localhost/post/1186)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@Locksmith (https://forums.vigem.org/uid/138) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1185):

> @nefarius (https://forums.vigem.org/uid/1) Looking good there! Almost like it's ready for beta testers? 😄 It's been over a week without updates on my favorite tech blog! 😉

Hey,

no worries, I'm still here, had to take a bit of a break, need to wipe my development PC and reinstall all the fun. Plus I've quit my day job and had to organize a few things and regain a proper sleep schedule 😅

There'll be more updates soon.

Cheers

Apr 9, 2019, 7:01 PM (https://localhost/post/1188)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

L Luke76bg (https://localhost/user/luke76bg)
(https://localhost/user/luke76bg)

Hi Nefarious, i'm actually using your scp toolkit driver for windows, even if incomplete it works well, i have both a ds3 and a ds4, and i really hope that when this project will be finished, both pads will be supported! Congratulations for all the latest progress you made! ^^

Apr 9, 2019, 9:21 PM (https://localhost/post/1190)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@Luke76bg (https://forums.vigem.org/uid/219) I hope for the same, mate 😆 glad it brings you joy, we're getting very close, just stay with me 😅

Apr 10, 2019, 5:39 PM (https://localhost/post/1194)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

L Luke76bg (https://localhost/user/luke76bg)
(https://localhost/user/luke76bg)

@nefarius (https://forums.vigem.org/uid/1) I'm not going anywhere! I can't wait! ^___^

17 DAYS LATER

Apr 27, 2019, 4:00 PM (https://localhost/post/1220)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

E enricorov (https://localhost/user/enricorov)
(https://localhost/user/enricorov)

Thank you very much for the effort you're putting into this project. I can't wait for the beta to be released and being able to use both bluetooth audio and my trusty ~~Vault 13 canteen~~ DS3 controller. Should you need testers, please count me in.

8 DAYS LATER

May 5, 2019, 11:52 PM (https://localhost/post/1225)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

E epikvigem (https://localhost/user/epikvigem)
(https://localhost/user/epikvigem)

@nefarius (https://forums.vigem.org/uid/1) any news? 🙂

May 6, 2019, 6:44 PM (https://localhost/post/1228)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Dear me, it's been a month! Time to see if the sources still compile 😬

8 DAYS LATER

May 14, 2019, 8:27 PM (https://localhost/post/1238)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 5
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius) (https://localhost/user/nefarius)

Alright, until the next demo is ready I shall at least write down a little To-Do kind of list of open topics 😬

Profile driver

Auto-disconnect on buffer overrun threshold

I've seen that the Bluetooth sub-system keeps all input reports buffered if they're not "consumed" by the profile or function driver which could lead to non-pageable memory exhaustion in case of a bug where the function driver stops consuming and inherently emptying the buffer. I plan on realizing that with a buffer size threshold value of a few kilobytes which, when exceeded, will drop the connection of the controller as there is no "stop sending input reports" command to my knowledge. This protection mechanism should be part of the profile/bus driver as it is the last bastion to system stability 😉

Same for the control endpoint if the "OK bytes" are forgotten to be consumed. Running out of precious non-pageable memory has to be avoided at all costs 👀

Harden (dis-)connect state machine

The state machine is almost a 100% finished, I didn't cover a few edge-cases I can't test because I would need to introduce radio connection errors which I can't without the proper equipment, although should implement fallback paths so the driver won't end up in an unknown state and cause hangs or orphaned objects. Again, no open paths allowed in kernel land. They *will* bite back one day ☠️

Filter driver

This little fella basically works well but needs attention.

Add sideband channel

A filter can't be directly accessed to e.g. send it configuration changes. Therefore a sideband channel or control device object has to be introduced. This is a very good template to base it upon (https://github.com/microsoft/Windows-driver-samples/tree/master/general/toaster/toastDrv/kmdf/filter/sideband). The control object will be protected by ACLs only allowing administrative users access to protect against abuse. `SDDL_DEVOBJ_SYS_ALL_ADM_ALL` sounds right for this purpose (context (https://docs.microsoft.com/en-us/windows-hardware/drivers/kernel/sddl-for-device-objects)).

Add support for multiple radios

The current assumption is that there's only one radio to work with. In a real world scenario this may be false since multiple "filter-able" Bluetooth host radio devices may be present. Therefore the filter should - in conjunction with the sideband mechanism - keep a reference to every device it's attached to and provide some sort of identification (bus serial, name, etc.). This will also impact the way the filter can be configured.

User-land configuration

It should be convenient for the end-user to enable or disable the drivers patching capabilities during runtime without the need of unloading the filter or having to re-plug or re-enable any devices. Some simple IOCTLs should be introduced for the sideband channel which can then be sent by a simple GUI tool. The driver should then store the state change in the according registry sections it can access (Hardware key (https://docs.microsoft.com/en-us/windows-hardware/drivers/wdf/introduction-to-registry-keys-for-drivers) sounds like the right place).

User-land tool for control

I plan on providing a simple C#-based tool which displays the available filtered radios with some basic information and some toggle switches to enable or disable PSM patching on the fly and other possible useful information which might come up (host radio MAC address for easy pairing access for example or entirely integrate PS3 pairing).

Setup tools

The recent discoveries of the ViGEm.Setup (https://github.com/ViGEm/ViGEm.Setup) toolset may certainly benefit this project as well. Maybe portions of `BthPS3Util` should/could be ported to WiX custom action 🤔

Shibari/Function driver

Not entirely sure if I should continue/publish my Shibari hack which already makes this stack usable. Proper function drivers should be the end goal but those will once again eat quite a bit of time as well. We'll see about that.

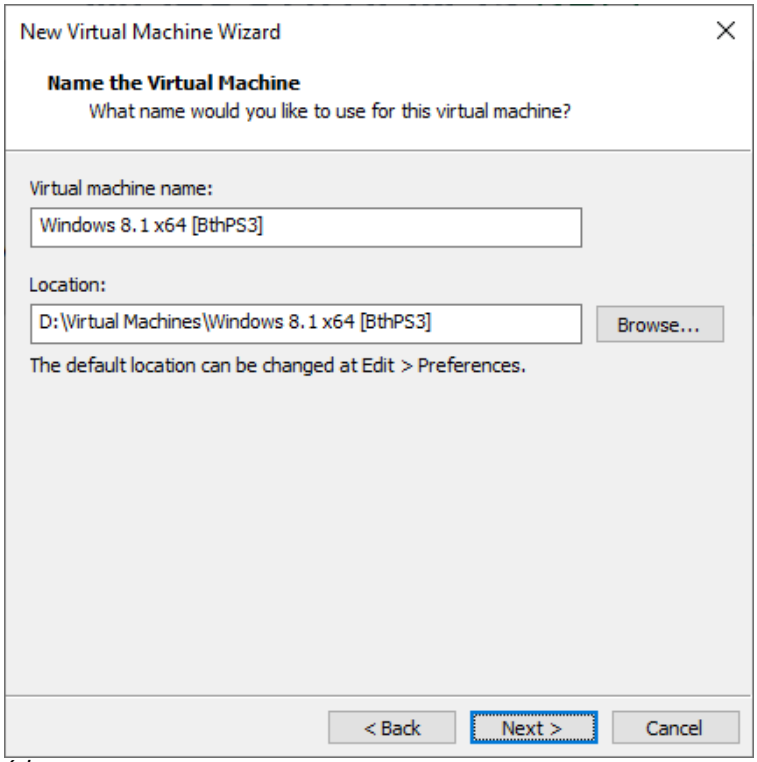
So far so good, will ramp up the pace again soon.

Cheers

May 17, 2019, 9:35 PM (https://localhost/post/1252) □
□ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 □
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

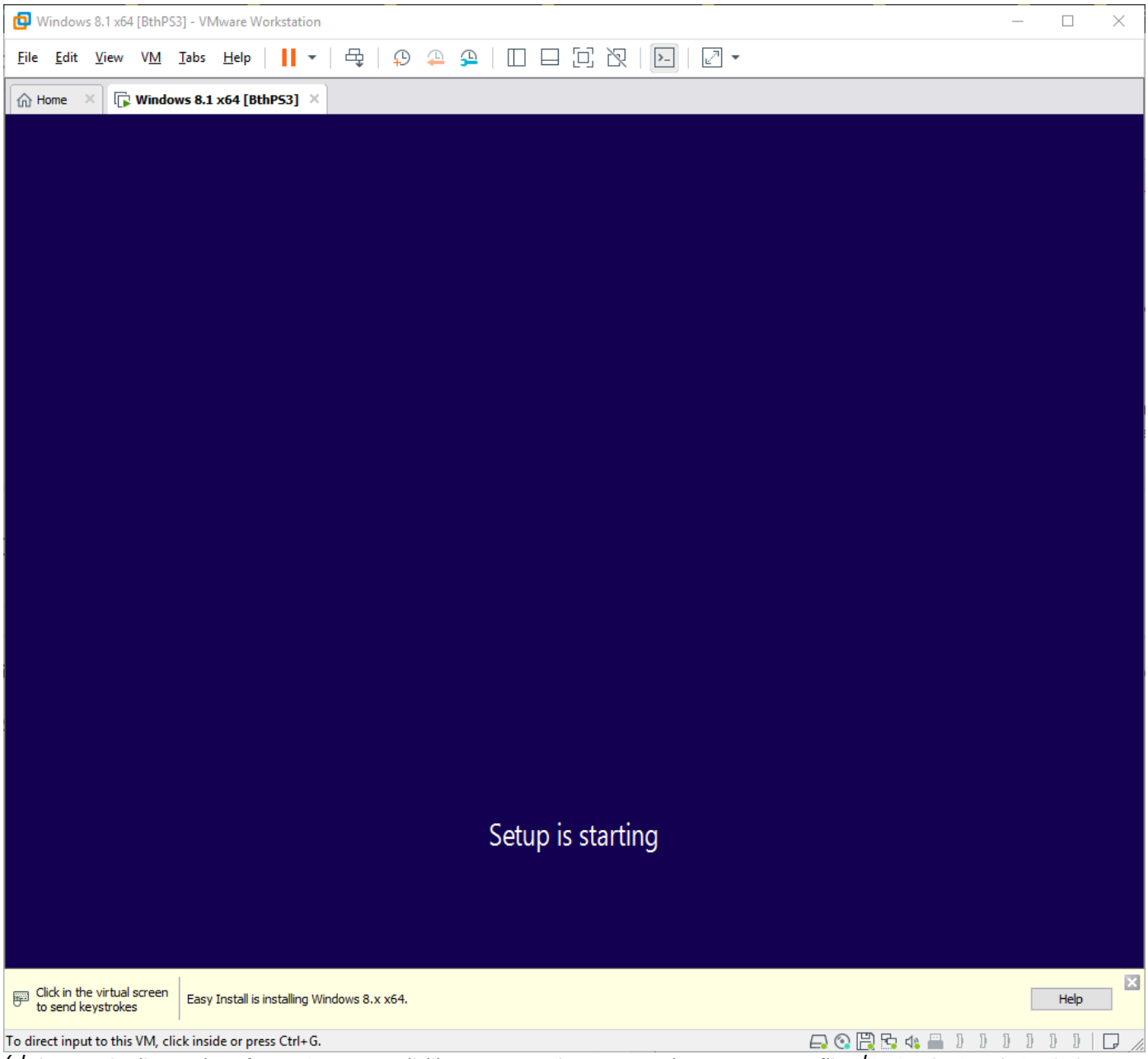
nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

About to test the latest filter modifications (added sideband code), here we go again 😅



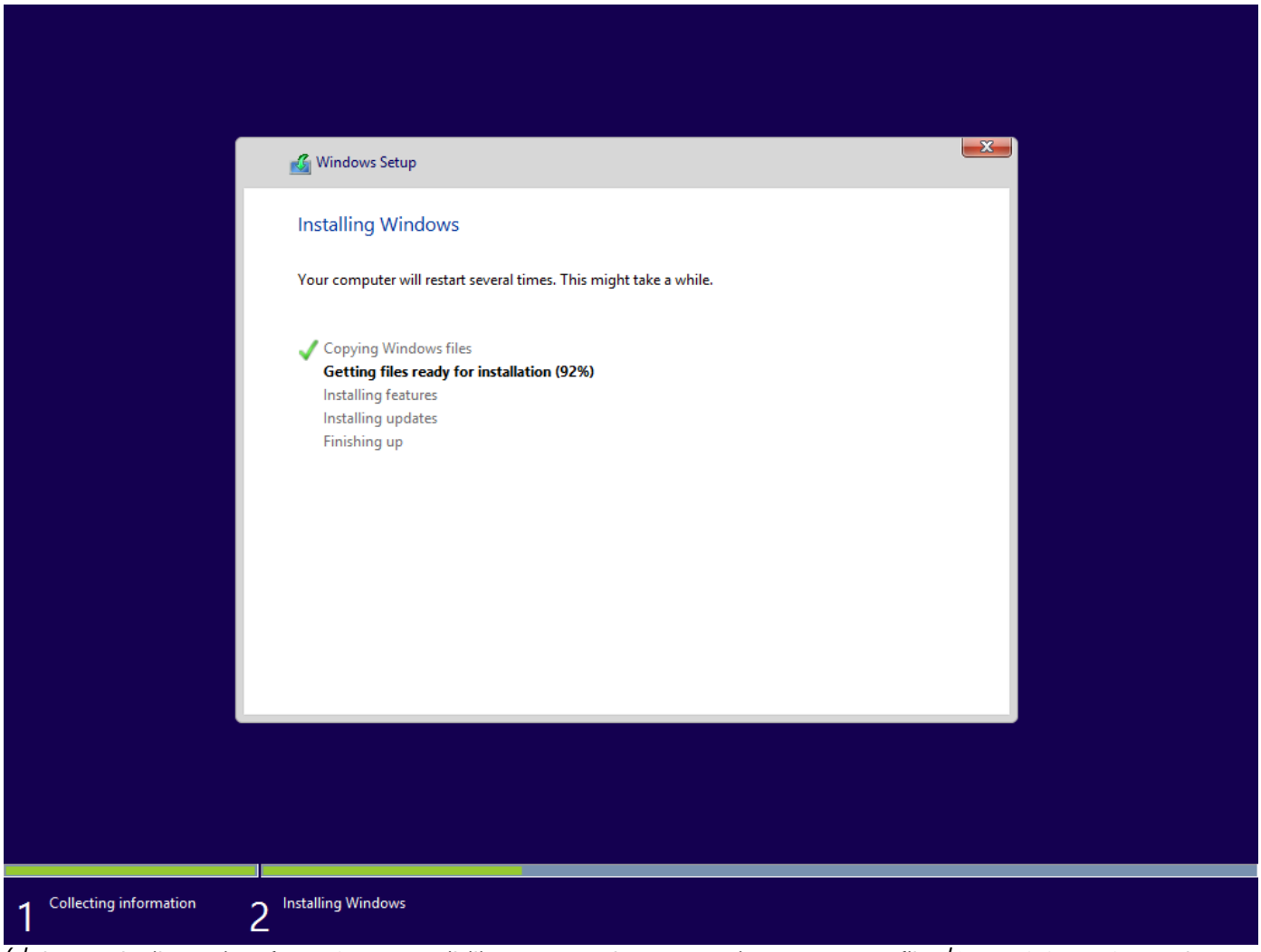
(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/7056b9f7-0e38-41ca-a873-b4ada6ca4028-image.png)

Bless you, VMware 😃



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/9a354b73-cd02-4bd7-a572-b2836b41e2ab-image.png)

That's quite quick, RAM-cached hard disk provides quite the I/O 😆

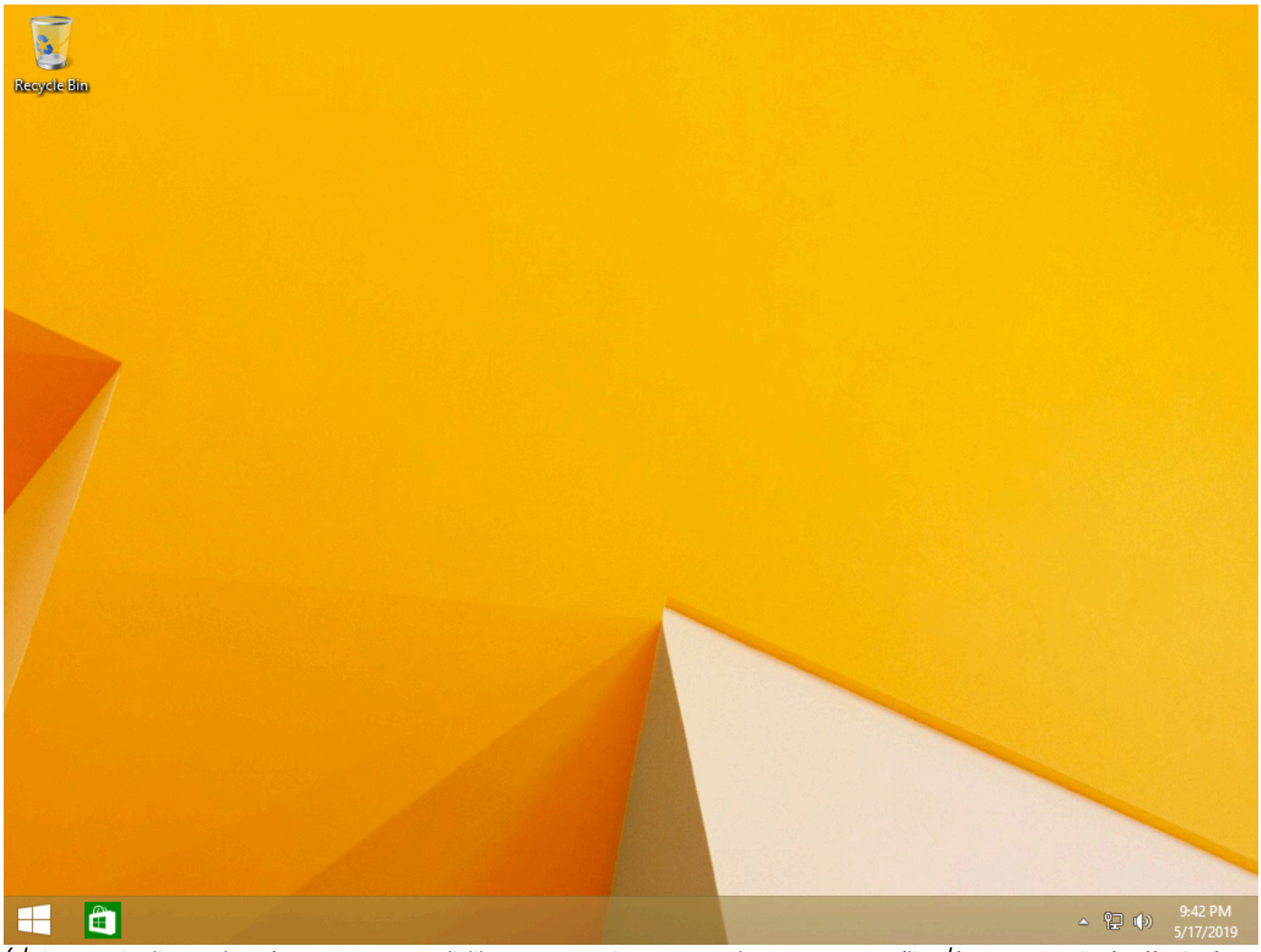


(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/2ac88313-e079-4eed-9595-a22d537b1c6c-image.png)

May 17, 2019, 9:42 PM (https://localhost/post/1253)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

And we have a Desktop, that install only took 5 minutes 😯



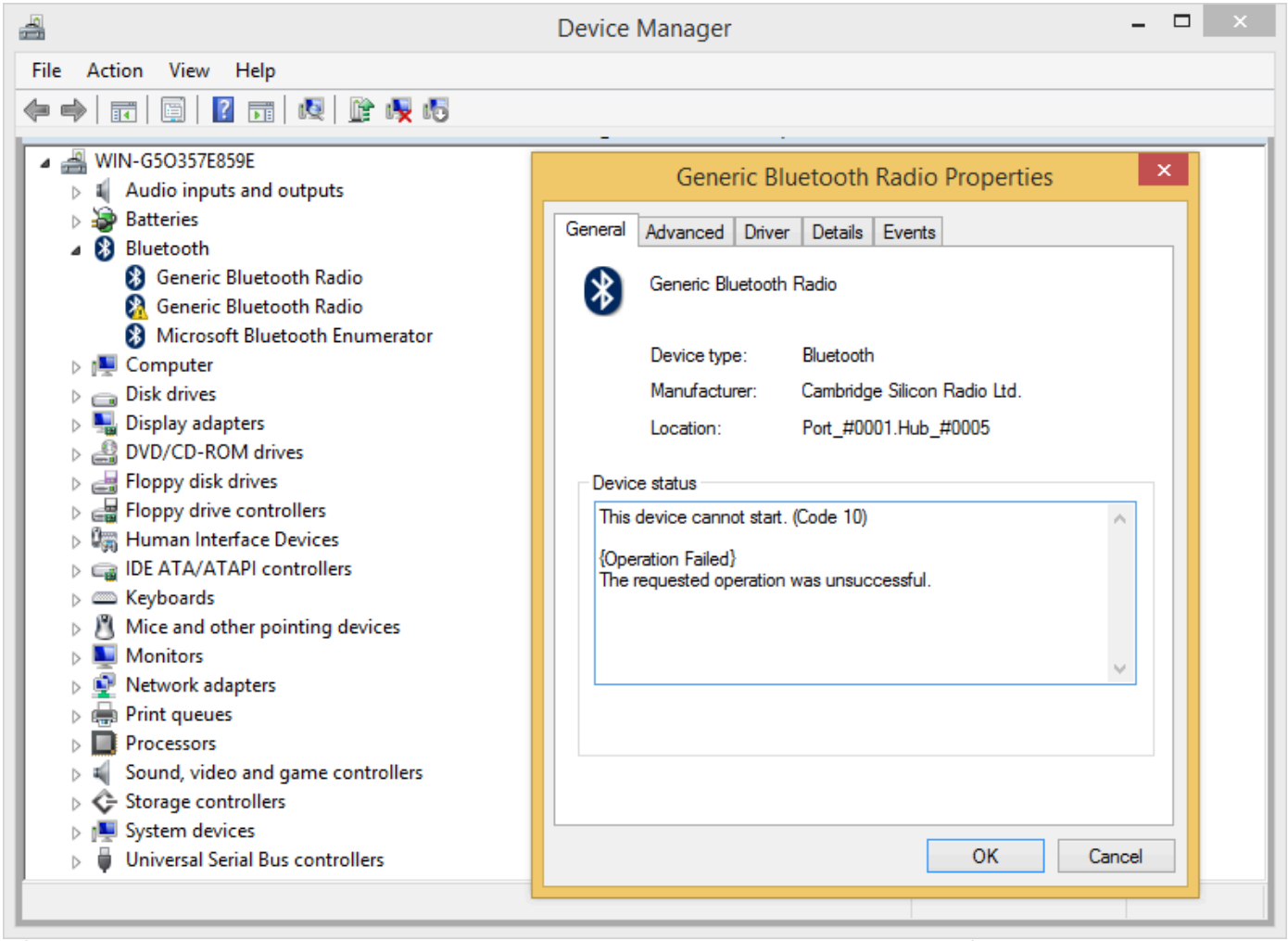
(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/fac015a6-abcf-4ff2-b8f0-ef8b22573701-image.png)

May 17, 2019, 9:57 PM (https://localhost/post/1254)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

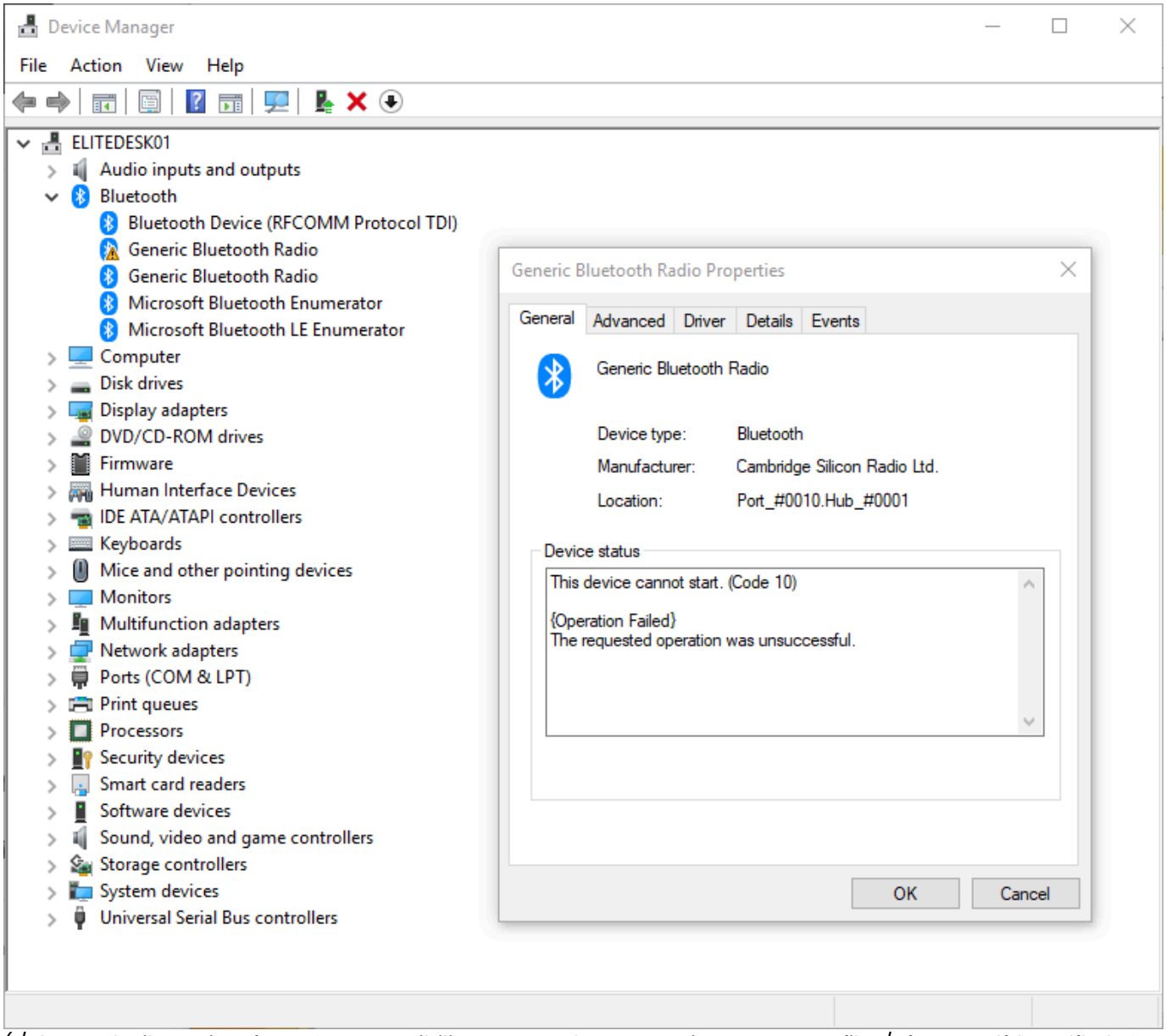
Oh, this if funny, I thought I've checked this already but apparently not; it's not possible to have two (or more) USB Bluetooth host dongles active at the same time 🤔

Windows 8.1



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/e382d185-2c19-4f0e-9fda-8e3d2787c3f8-image.png)

Windows 10



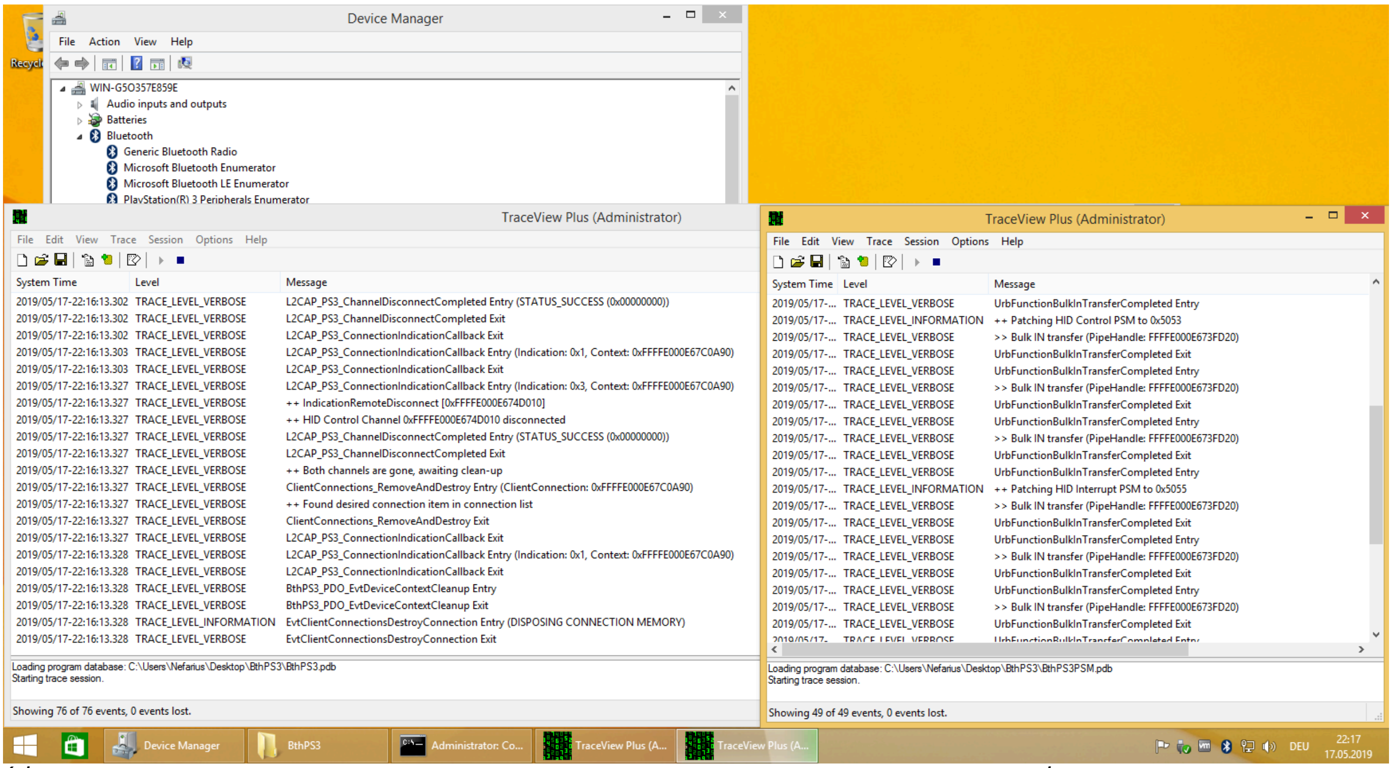
(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/0f571c51-dfd0-4dfb-b13c-fb727bba3898-image.png)

Well, that's good to know but hasn't interfered with anything I've implemented today because I wanted to have the capability of storing device-specific settings through a control device anyway. So I guess this is true (https://superuser.com/a/1349429) 😅

May 17, 2019, 10:18 PM (https://localhost/post/1256)
□ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 □ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius) (https://localhost/user/nefarius)

Phew, everything still works after my mayhem 😅 And on a completely fresh machine as well!



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/4b0bf8ce-7834-44e5-a7f7-d36bf04da985-image.png)

Time for a game and/or slumber 💤

May 18, 2019, 11:31 AM (https://localhost/post/1259)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Alright, breakfast is done, back to work 😋 Looks like disabling the patching is working as expected:

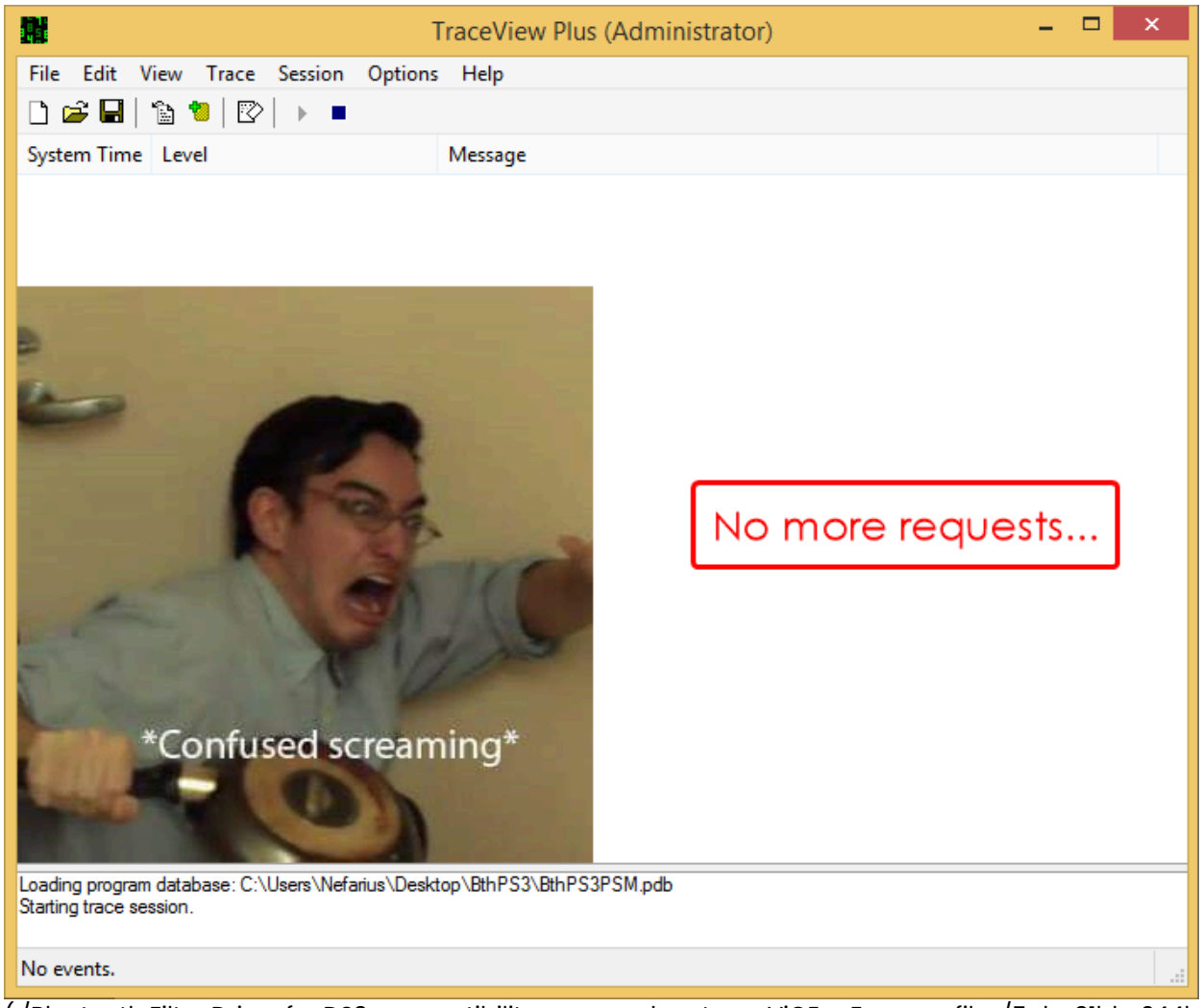
```
2019/05/18-11:29:22.504 TRACE_LEVEL_VERBOSE     UrbFunctionBulkInTransferCompleted Entry
2019/05/18-11:29:22.504 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-11:29:22.504 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
2019/05/18-11:29:22.504 TRACE_LEVEL_VERBOSE     >> Bulk IN transfer (PipeHandle: FFFFE000E7133D20)
2019/05/18-11:29:22.504 TRACE_LEVEL_VERBOSE     UrbFunctionBulkInTransferCompleted Exit
2019/05/18-11:29:23.355 TRACE_LEVEL_VERBOSE     UrbFunctionBulkInTransferCompleted Entry
2019/05/18-11:29:23.355 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-11:29:23.355 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
2019/05/18-11:29:23.356 TRACE_LEVEL_VERBOSE     >> Bulk IN transfer (PipeHandle: FFFFE000E7133D20)
2019/05/18-11:29:23.356 TRACE_LEVEL_VERBOSE     UrbFunctionBulkInTransferCompleted Exit
```

Now onto making it dynamically changeable and storing it in the registry to make it survive device power cycling.

May 18, 2019, 11:53 AM (https://localhost/post/1260)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Wait a minute... 🤔 After the first few denied connection requests when the controller shuts off and I retry to connect it there are no more requests flowing through the filter 😕



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/5aba31bb-244b-471e-b36a-ae98aa075e12-image.png)

Is this due to VMware? I don't think so... Hm, that sure is surprising me, I thought the host controller driver always has to be contacted in case of a new connection request but apparently it's cached in the actual chip somehow. Well, there goes my fabulous plan of making it dynamically configurable 😞

I'll do a bit more testing and if I can't get it to work I'll simply rip out the control device again (was a good practice anyway) and introduce two `Parameters` registry values to globally control the patching. Taking a few steps back and not over-complicating things. There's other stuff in the pipeline 🙂

May 18, 2019, 12:34 PM (https://localhost/post/1261)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Hm, somehow VMware is not happy at all with what I'm doing, I'll now switch over to a physical machine and see how it's going there.

May 18, 2019, 12:55 PM (https://localhost/post/1262) □
□ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 □
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Aha! Deception! It actually *was* VMware! 😯 On a physical Windows 10 machine it works flawlessly like expected even with a 5 meter USB repeater:

Test with Nav Controller

```
---------------------------         Pressed PS button         ---------------------------
2019/05/18-12:40:54.722 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-12:40:54.722 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
2019/05/18-12:41:13.495 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-12:41:13.495 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
2019/05/18-12:41:32.280 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-12:41:32.280 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
2019/05/18-12:41:51.049 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-12:41:51.049 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
---------------------------         Pressed PS button         ---------------------------
2019/05/18-12:42:55.355 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-12:42:55.355 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
2019/05/18-12:43:14.135 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-12:43:14.135 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
2019/05/18-12:43:32.912 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-12:43:32.912 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
2019/05/18-12:43:51.675 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-12:43:51.675 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
```

Test with DS3 Controller

```
--------------------------         Pressed PS button         --------------------------
2019/05/18-12:46:10.193 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-12:46:10.193 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
2019/05/18-12:46:28.964 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-12:46:28.964 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
2019/05/18-12:46:47.736 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-12:46:47.736 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
2019/05/18-12:47:06.502 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-12:47:06.502 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
--------------------------         Pressed PS button         --------------------------
2019/05/18-12:48:06.959 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-12:48:06.959 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
2019/05/18-12:48:25.733 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-12:48:25.733 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
2019/05/18-12:48:44.510 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-12:48:44.510 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
2019/05/18-12:49:03.293 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-12:49:03.293 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
--------------------------         Pressed PS button         --------------------------
2019/05/18-12:50:40.865 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-12:50:40.865 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
2019/05/18-12:50:59.650 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-12:50:59.650 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
2019/05/18-12:51:18.423 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-12:51:18.423 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
2019/05/18-12:51:37.183 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-12:51:37.183 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
```

As you can see the controller tries for a total of 4 times to connect to the host its programmed to before giving up and shutting off. When I press the PS button again to wake it up within the same session the requests arrive again (and get blocked because patching is disabled in this example) as expected. Good stuff!

Now that I know I'm not entirely bonkers it's time to define some IOCTLs for the control channel. And some coffee ☕

May 18, 2019, 2:32 PM (https://localhost/post/1263)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

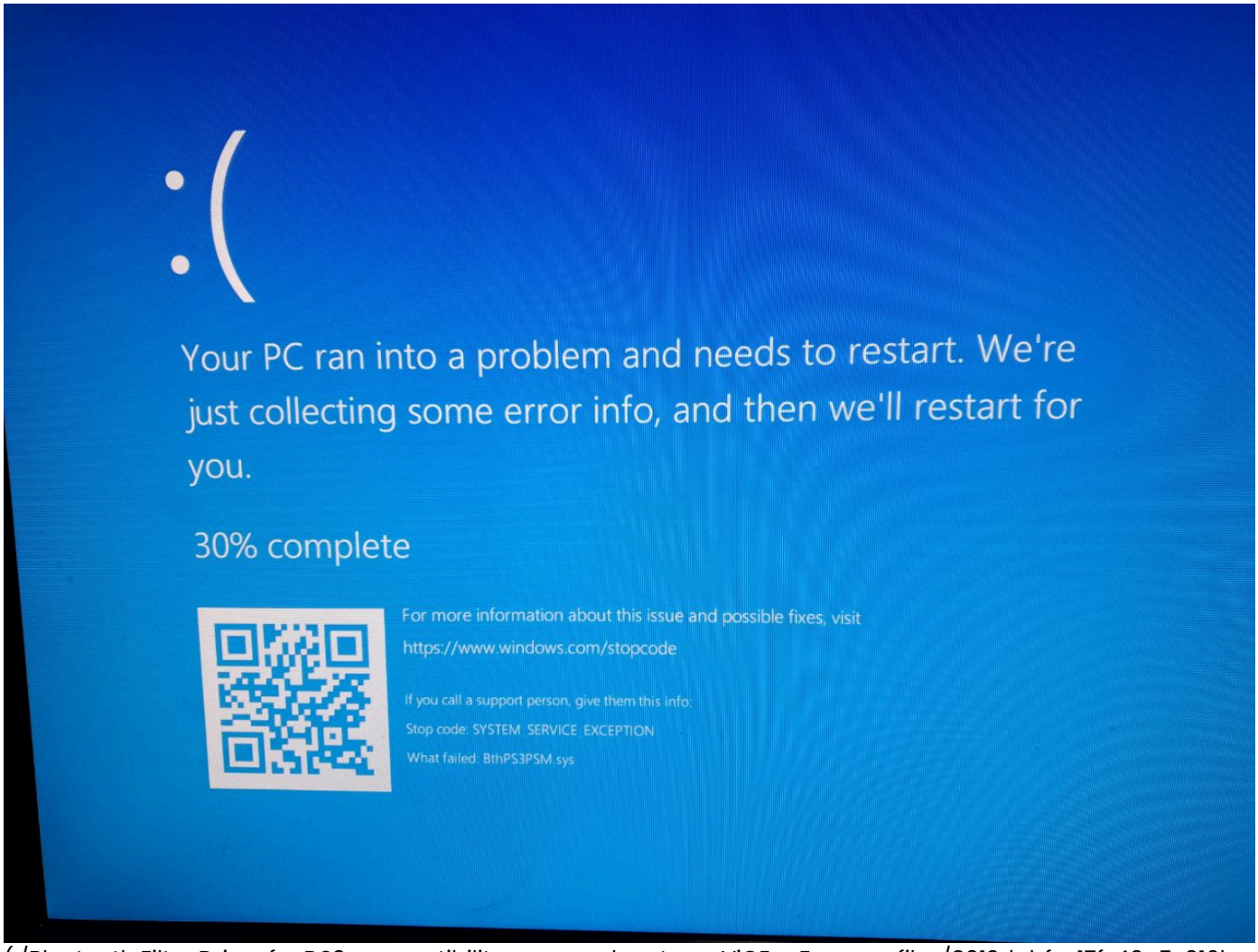
nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Good progress so far 😎 Time for a break and go for a little cycling tour 🚴 while the weather is this nice ☀️

May 18, 2019, 7:03 PM (https://localhost/post/1264)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Oooopsie... 😅



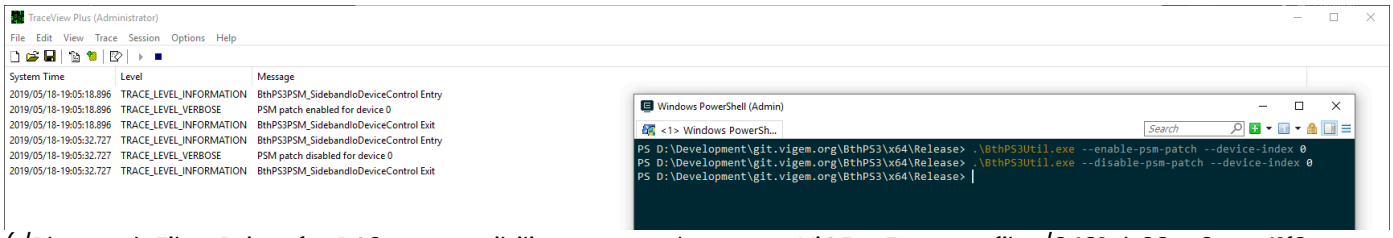
(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/8913dabf-c17f-49a5-916b-94cbdb1616cb-image.png)

Mistake identified, copypasted a variable which in this case isn't initialized, argh!

May 18, 2019, 7:11 PM (https://localhost/post/1265)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Ha, there we go!



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/3491ab69-e9aa-41f9-ad84-a8ab7a2f1d83-image.png)

Let's go for a test:

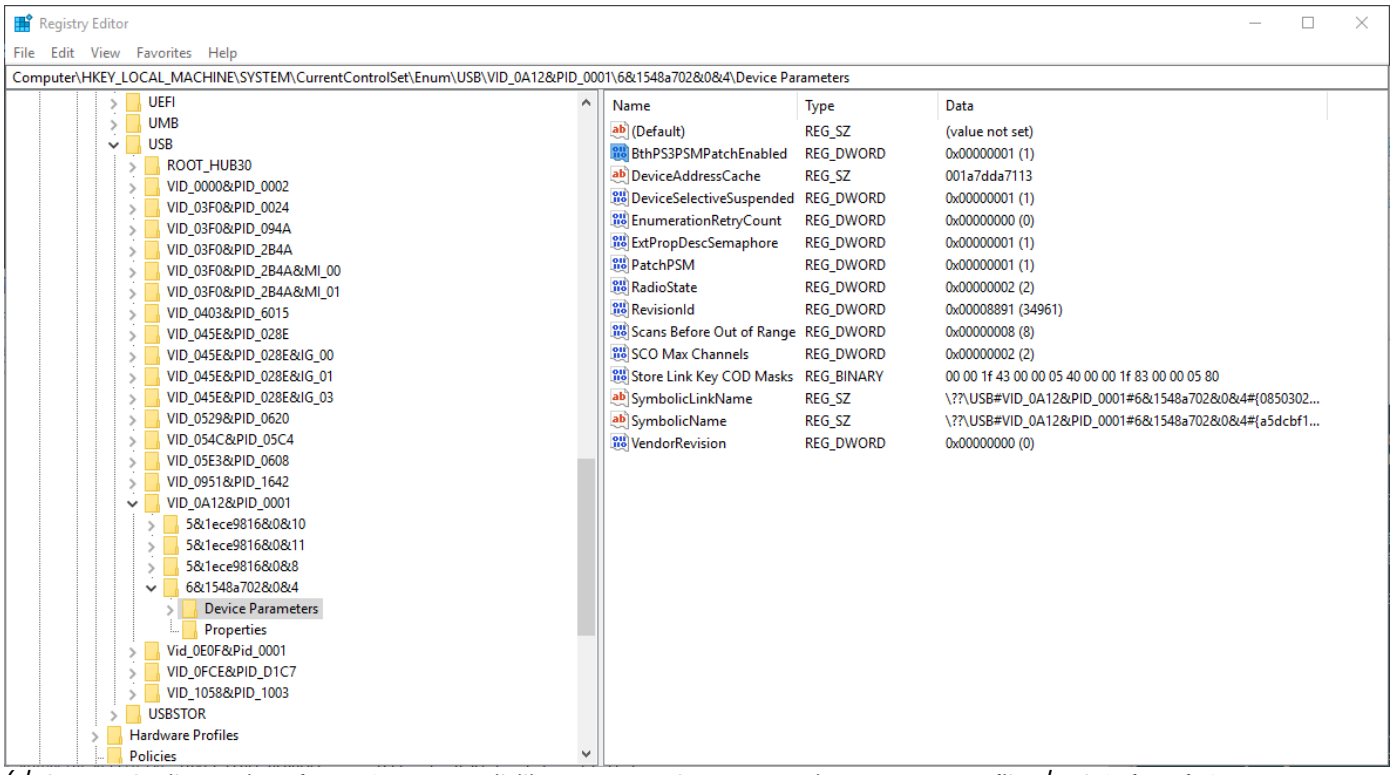
```
2019/05/18-19:09:31.570 TRACE_LEVEL_INFORMATION BthPS3PSM_SidebandIoDeviceControl Entry
2019/05/18-19:09:31.570 TRACE_LEVEL_VERBOSE     PSM patch disabled for device 0
2019/05/18-19:09:31.570 TRACE_LEVEL_INFORMATION BthPS3PSM_SidebandIoDeviceControl Exit
2019/05/18-19:09:36.919 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-19:09:36.919 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
2019/05/18-19:09:55.703 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-19:09:55.703 TRACE_LEVEL_VERBOSE     -- NOT Patching HID Control PSM
2019/05/18-19:09:57.801 TRACE_LEVEL_INFORMATION BthPS3PSM_SidebandIoDeviceControl Entry
2019/05/18-19:09:57.801 TRACE_LEVEL_VERBOSE     PSM patch enabled for device 0
2019/05/18-19:09:57.801 TRACE_LEVEL_INFORMATION BthPS3PSM_SidebandIoDeviceControl Exit
2019/05/18-19:10:14.487 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/05/18-19:10:14.487 TRACE_LEVEL_INFORMATION ++ Patching HID Control PSM to 0x5053
2019/05/18-19:10:14.877 TRACE_LEVEL_VERBOSE     >> Connection request for HID Interrupt PSM 0x0013 arrived
2019/05/18-19:10:14.877 TRACE_LEVEL_INFORMATION ++ Patching HID Interrupt PSM to 0x5055
```

Splendid! 😎

May 18, 2019, 8:19 PM (https://localhost/post/1266)
□ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 □ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius) (https://localhost/user/nefarius)

Storing and loading settings implemented, that will be all for today 😄



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/c8b97fa5-f265-42e4-9ab3-9a4f1a18a272-image.png)

May 18, 2019, 10:59 PM (https://localhost/post/1267)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


(https://localhost/user/nefarius) nefarius (https://localhost/user/nefarius)

One more command 😄

```
PS D:\Development\git.vigem.org\BthPS3\x64\Release> .\BthPS3Util.exe --get-psm-patch --device-index 0
PSM Patching is enabled for this device
PS D:\Development\git.vigem.org\BthPS3\x64\Release> .\BthPS3Util.exe --disable-psm-patch --device-index 0
PS D:\Development\git.vigem.org\BthPS3\x64\Release> .\BthPS3Util.exe --get-psm-patch --device-index 0
PSM Patching is disabled for this device
PS D:\Development\git.vigem.org\BthPS3\x64\Release> .\BthPS3Util.exe --enable-psm-patch --device-index 0
PS D:\Development\git.vigem.org\BthPS3\x64\Release> .\BthPS3Util.exe --get-psm-patch --device-index 0
PSM Patching is enabled for this device
PS D:\Development\git.vigem.org\BthPS3\x64\Release>
```

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/a766efac-567c-4098-83e1-a112d53bc586-image.png)

Now off to important things zzZ

May 19, 2019, 11:41 AM (https://localhost/post/1268)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 3
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

BthPS3 + Shibari Demo with Nav and DS3 Controller [19.05.2019]

It's time for another video 😃 I wanted to see if everything still works after the latest rework and so far everything's looking fine, also performance is stellar, even through Shibari which has to go from kernel to user to kernel context many times per second I notice no input lag whatsoever.

 Youtube Video (https://youtu.be/w6r7J20S8S8)

Next I'll implement the buffer overrun protection.

May 19, 2019, 1:00 PM (https://localhost/post/1269)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

enricorov (https://localhost/user/enricorov)
(https://localhost/user/enricorov)

@nefarius (https://forums.vigem.org/uid/1) It looks great! I'm looking forward to testing this myself, keep up the good work!

May 19, 2019, 1:11 PM (https://localhost/post/1270)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@enricorov (https://forums.vigem.org/uid/236) I still need a strategy on how to involve testers without unfinished binaries spreading...

May 19, 2019, 3:29 PM (https://localhost/post/1271)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

E

enricorov (https://localhost/user/enricorov)
(https://localhost/user/enricorov)

@nefarius (https://forums.vigem.org/uid/1) I suppose that's something hand in hand with invoving other people. You could have the software work only until a certain date, say a month from the beginning of beta, which would prevent people from using the beta binaries indefinitely.

May 19, 2019, 4:00 PM (https://localhost/post/1272)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@enricorov (https://forums.vigem.org/uid/236) hm, a time bomb you mean? 🤔 Well, I'll figure something out, another issue that's more important to me and would need assistance with would be how to properly organize such a circle of testers, having feedback arriving in a nice ordered fashion etc.

May 19, 2019, 5:58 PM (https://localhost/post/1273)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Auto-disconnect on I/O idle implemented

Alright, this challenge was easier to resolve than I initially thought (and without a single crash I might add!) thanks to the frameworks idle power-down (https://docs.microsoft.com/en-us/windows-hardware/drivers/wdf/supporting-idle-power-down) capabilities:

```
-------------------------- Nav connecting --------------------------
2019/05/19-17:48:09.682 TRACE_LEVEL_VERBOSE     BthPS3_IndicationCallback Entry
2019/05/19-17:48:09.682 TRACE_LEVEL_INFORMATION New connection for PSM 0x5053 from 00070401E341 arrived
2019/05/19-17:48:09.682 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnect Entry
2019/05/19-17:48:09.682 TRACE_LEVEL_VERBOSE     ClientConnections_RetrieveByBthAddr Entry
2019/05/19-17:48:09.682 TRACE_LEVEL_VERBOSE     ClientConnections_RetrieveByBthAddr Exit (STATUS_NOT_FOUND
(0xC0000225))
2019/05/19-17:48:09.682 TRACE_LEVEL_ERROR       BTHPS3_GET_DEVICE_NAME failed with status STATUS_INVALID_PAR
AMETER (0xC000000D), dropping connection
2019/05/19-17:48:09.682 TRACE_LEVEL_VERBOSE     L2CAP_PS3_DenyRemoteConnect Entry
2019/05/19-17:48:09.682 TRACE_LEVEL_VERBOSE     L2CAP_PS3_DenyRemoteConnectCompleted Entry (STATUS_SUCCESS
(0x00000000))
2019/05/19-17:48:09.682 TRACE_LEVEL_VERBOSE     L2CAP_PS3_DenyRemoteConnectCompleted Exit
2019/05/19-17:48:09.682 TRACE_LEVEL_VERBOSE     L2CAP_PS3_DenyRemoteConnect Exit
2019/05/19-17:48:09.682 TRACE_LEVEL_VERBOSE     BthPS3_IndicationCallback Exit
2019/05/19-17:48:10.488 TRACE_LEVEL_VERBOSE     BthPS3_IndicationCallback Entry
2019/05/19-17:48:10.488 TRACE_LEVEL_INFORMATION New connection for PSM 0x5053 from 00070401E341 arrived
2019/05/19-17:48:10.488 TRACE_LEVEL_VERBOSE     IRQL DPC (0x02) too high, preparing async call
2019/05/19-17:48:10.488 TRACE_LEVEL_VERBOSE     BthPS3_IndicationCallback Exit
2019/05/19-17:48:10.488 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnectAsync Entry
2019/05/19-17:48:10.488 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnect Entry
2019/05/19-17:48:10.488 TRACE_LEVEL_VERBOSE     ClientConnections_RetrieveByBthAddr Entry
2019/05/19-17:48:10.488 TRACE_LEVEL_VERBOSE     ClientConnections_RetrieveByBthAddr Exit (STATUS_NOT_FOUND
(0xC0000225))
2019/05/19-17:48:10.488 TRACE_LEVEL_INFORMATION ++ Device 00070401E341 name: Navigation Controller
2019/05/19-17:48:10.488 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
0, Context: 0xFFFF858FE830A0D0)
2019/05/19-17:48:10.488 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
2019/05/19-17:48:10.488 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnect Exit (STATUS_SUCCESS (0x000000
00))
2019/05/19-17:48:10.488 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnectAsync Exit
2019/05/19-17:48:10.703 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ControlConnectResponseCompleted Entry
2019/05/19-17:48:10.703 TRACE_LEVEL_INFORMATION Connection completion, status: STATUS_SUCCESS (0x00000000)
2019/05/19-17:48:10.703 TRACE_LEVEL_INFORMATION HID Control Channel connection established
2019/05/19-17:48:10.703 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ControlConnectResponseCompleted Exit
2019/05/19-17:48:10.897 TRACE_LEVEL_VERBOSE     BthPS3_IndicationCallback Entry
2019/05/19-17:48:10.897 TRACE_LEVEL_INFORMATION New connection for PSM 0x5055 from 00070401E341 arrived
2019/05/19-17:48:10.897 TRACE_LEVEL_VERBOSE     IRQL DPC (0x02) too high, preparing async call
2019/05/19-17:48:10.897 TRACE_LEVEL_VERBOSE     BthPS3_IndicationCallback Exit
2019/05/19-17:48:10.897 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnectAsync Entry
2019/05/19-17:48:10.897 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnect Entry
2019/05/19-17:48:10.897 TRACE_LEVEL_VERBOSE     ClientConnections_RetrieveByBthAddr Entry
2019/05/19-17:48:10.897 TRACE_LEVEL_VERBOSE     ++ Found desired connection item in connection list
2019/05/19-17:48:10.897 TRACE_LEVEL_VERBOSE     ClientConnections_RetrieveByBthAddr Exit (STATUS_SUCCESS (0x
00000000))
2019/05/19-17:48:10.897 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
0, Context: 0xFFFF858FE830A0D0)
2019/05/19-17:48:10.897 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
2019/05/19-17:48:10.897 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnect Exit (STATUS_SUCCESS (0x000000
00))
2019/05/19-17:48:10.897 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnectAsync Exit
2019/05/19-17:48:10.969 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
4, Context: 0xFFFF858FE830A0D0)
2019/05/19-17:48:10.969 TRACE_LEVEL_INFORMATION L2CAP_PS3_ConnectionIndicationCallback ++ IndicationRemoteCo
nfigRequest
2019/05/19-17:48:10.969 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
2019/05/19-17:48:11.092 TRACE_LEVEL_VERBOSE     L2CAP_PS3_InterruptConnectResponseCompleted Entry
2019/05/19-17:48:11.092 TRACE_LEVEL_INFORMATION Connection completion, status: STATUS_SUCCESS (0x00000000)
2019/05/19-17:48:11.092 TRACE_LEVEL_INFORMATION HID Interrupt Channel connection established
2019/05/19-17:48:11.092 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionStateConnected Entry
2019/05/19-17:48:11.092 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionStateConnected Exit
2019/05/19-17:48:11.092 TRACE_LEVEL_VERBOSE     L2CAP_PS3_InterruptConnectResponseCompleted Exit
2019/05/19-17:48:11.092 TRACE_LEVEL_VERBOSE     BthPS3_EvtWdfChildListCreateDevice Entry
2019/05/19-17:48:11.093 TRACE_LEVEL_VERBOSE     BthPS3_EvtWdfChildListCreateDevice Exit
                        Device connected, but no I/O, 10 seconds idle timeout
```

```
-------------------------- Device connected, but no I/O, 10 seconds idle timeout --------------------------
-
2019/05/19-17:48:21.094 TRACE_LEVEL_VERBOSE     BthPS3_PDO_EvtWdfDeviceD0Exit Entry
2019/05/19-17:48:21.094 TRACE_LEVEL_INFORMATION Requesting device disconnect
2019/05/19-17:48:21.094 TRACE_LEVEL_VERBOSE     BthPS3_PDO_EvtWdfDeviceD0Exit Exit
2019/05/19-17:48:21.237 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
3, Context: 0xFFFF858FE830A0D0)
2019/05/19-17:48:21.237 TRACE_LEVEL_VERBOSE     ++ IndicationRemoteDisconnect [0xFFFF858FEFFB1B20]
2019/05/19-17:48:21.237 TRACE_LEVEL_VERBOSE     ++ HID Control Channel 0xFFFF858FEFFB1B20 disconnected
2019/05/19-17:48:21.237 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ChannelDisconnectCompleted Entry (STATUS_SUCCESS
(0x00000000))
2019/05/19-17:48:21.237 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ChannelDisconnectCompleted Exit
2019/05/19-17:48:21.237 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
2019/05/19-17:48:21.237 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
1, Context: 0xFFFF858FE830A0D0)
2019/05/19-17:48:21.237 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
2019/05/19-17:48:21.237 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
3, Context: 0xFFFF858FE830A0D0)
2019/05/19-17:48:21.237 TRACE_LEVEL_VERBOSE     ++ IndicationRemoteDisconnect [0xFFFF858FEEE2CB20]
2019/05/19-17:48:21.237 TRACE_LEVEL_VERBOSE     ++ HID Interrupt Channel 0xFFFF858FEEE2CB20 disconnected
2019/05/19-17:48:21.237 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ChannelDisconnectCompleted Entry (STATUS_SUCCESS
(0x00000000))
2019/05/19-17:48:21.237 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ChannelDisconnectCompleted Exit
2019/05/19-17:48:21.237 TRACE_LEVEL_VERBOSE     ++ Both channels are gone, awaiting clean-up
2019/05/19-17:48:21.237 TRACE_LEVEL_VERBOSE     ClientConnections_RemoveAndDestroy Entry (ClientConnection:
0xFFFF858FE830A0D0)
2019/05/19-17:48:21.237 TRACE_LEVEL_VERBOSE     ++ Found desired connection item in connection list
2019/05/19-17:48:21.237 TRACE_LEVEL_VERBOSE     ClientConnections_RemoveAndDestroy Exit
2019/05/19-17:48:21.237 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
2019/05/19-17:48:21.237 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
1, Context: 0xFFFF858FE830A0D0)
2019/05/19-17:48:21.237 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
2019/05/19-17:48:21.237 TRACE_LEVEL_INFORMATION EvtClientConnectionsDestroyConnection Entry (DISPOSING CONNE
CTION MEMORY)
2019/05/19-17:48:21.237 TRACE_LEVEL_VERBOSE     EvtClientConnectionsDestroyConnection Exit
2019/05/19-17:48:21.238 TRACE_LEVEL_VERBOSE     BthPS3_PDO_EvtDeviceContextCleanup Entry
2019/05/19-17:48:21.238 TRACE_LEVEL_VERBOSE     BthPS3_PDO_EvtDeviceContextCleanup Exit
-------------------------- Device connection dropped by profile driver --------------------------
```

Now when something happens to the I/O dispatching (like a process crash or a bug in the function driver), the idle timeout will kick in preventing the buffers from filling up uncontrolled and dropping the connection:

```
-------------------------- Shibari active, dispatching I/O --------------------------
2019/05/19-17:54:15.514 TRACE_LEVEL_VERBOSE     BthPS3_PDO_EvtWdfIoQueueIoDeviceControl Entry
2019/05/19-17:54:15.514 TRACE_LEVEL_VERBOSE     >> IOCTL_BTHPS3_HID_INTERRUPT_READ
2019/05/19-17:54:15.514 TRACE_LEVEL_VERBOSE     bufferLength: 50
2019/05/19-17:54:15.514 TRACE_LEVEL_VERBOSE     BthPS3_PDO_EvtWdfIoQueueIoDeviceControl Exit (status: STATUS
_PENDING (0x00000103))
2019/05/19-17:54:15.544 TRACE_LEVEL_VERBOSE     Interrupt read transfer request completed with status STATUS
_SUCCESS (0x00000000) (remaining: 0)
2019/05/19-17:54:15.544 TRACE_LEVEL_VERBOSE     BthPS3_PDO_EvtWdfIoQueueIoDeviceControl Entry
2019/05/19-17:54:15.544 TRACE_LEVEL_VERBOSE     >> IOCTL_BTHPS3_HID_INTERRUPT_READ
2019/05/19-17:54:15.544 TRACE_LEVEL_VERBOSE     bufferLength: 50
2019/05/19-17:54:15.544 TRACE_LEVEL_VERBOSE     BthPS3_PDO_EvtWdfIoQueueIoDeviceControl Exit (status: STATUS
_PENDING (0x00000103))
2019/05/19-17:54:15.546 TRACE_LEVEL_VERBOSE     Interrupt read transfer request completed with status STATUS
_SUCCESS (0x00000000) (remaining: 0)
2019/05/19-17:54:15.547 TRACE_LEVEL_VERBOSE     BthPS3_PDO_EvtWdfIoQueueIoDeviceControl Entry
2019/05/19-17:54:15.547 TRACE_LEVEL_VERBOSE     >> IOCTL_BTHPS3_HID_INTERRUPT_READ
2019/05/19-17:54:15.547 TRACE_LEVEL_VERBOSE     bufferLength: 50
2019/05/19-17:54:15.547 TRACE_LEVEL_VERBOSE     BthPS3_PDO_EvtWdfIoQueueIoDeviceControl Exit (status: STATUS
_PENDING (0x00000103))
-------------------------- Shibari killed by Task Manager so device is orphaned now ----------------------
----
2019/05/19-17:54:15.558 TRACE_LEVEL_VERBOSE     Control read transfer request completed with status STATUS_C
ANCELLED (0xC0000120)
2019/05/19-17:54:15.558 TRACE_LEVEL_VERBOSE     Control read transfer request completed with status STATUS_C
ANCELLED (0xC0000120)
2019/05/19-17:54:15.558 TRACE_LEVEL_VERBOSE     Interrupt read transfer request completed with status STATUS
_CANCELLED (0xC0000120) (remaining: 0)
2019/05/19-17:54:15.558 TRACE_LEVEL_VERBOSE     Interrupt read transfer request completed with status STATUS
_CANCELLED (0xC0000120) (remaining: 0)
-------------------------- Idle timeout kicked in, dropping device --------------------------
2019/05/19-17:54:25.558 TRACE_LEVEL_VERBOSE     BthPS3_PDO_EvtWdfDeviceD0Exit Entry
2019/05/19-17:54:25.558 TRACE_LEVEL_INFORMATION Requesting device disconnect
2019/05/19-17:54:25.559 TRACE_LEVEL_VERBOSE     BthPS3_PDO_EvtWdfDeviceD0Exit Exit
2019/05/19-17:54:25.648 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
3, Context: 0xFFFF858FE8E610D0)
2019/05/19-17:54:25.648 TRACE_LEVEL_VERBOSE     ++ IndicationRemoteDisconnect [0xFFFF858FEEA47B20]
2019/05/19-17:54:25.648 TRACE_LEVEL_VERBOSE     ++ HID Control Channel 0xFFFF858FEEA47B20 disconnected
2019/05/19-17:54:25.648 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ChannelDisconnectCompleted Entry (STATUS_SUCCESS
(0x00000000))
2019/05/19-17:54:25.648 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ChannelDisconnectCompleted Exit
2019/05/19-17:54:25.648 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
2019/05/19-17:54:25.648 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
1, Context: 0xFFFF858FE8E610D0)
2019/05/19-17:54:25.648 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
2019/05/19-17:54:25.648 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
3, Context: 0xFFFF858FE8E610D0)
2019/05/19-17:54:25.648 TRACE_LEVEL_VERBOSE     ++ IndicationRemoteDisconnect [0xFFFF858FF3EDCB20]
2019/05/19-17:54:25.648 TRACE_LEVEL_VERBOSE     ++ HID Interrupt Channel 0xFFFF858FF3EDCB20 disconnected
2019/05/19-17:54:25.648 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ChannelDisconnectCompleted Entry (STATUS_SUCCESS
(0x00000000))
2019/05/19-17:54:25.648 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ChannelDisconnectCompleted Exit
2019/05/19-17:54:25.648 TRACE_LEVEL_VERBOSE     ++ Both channels are gone, awaiting clean-up
2019/05/19-17:54:25.648 TRACE_LEVEL_VERBOSE     ClientConnections_RemoveAndDestroy Entry (ClientConnection:
0xFFFF858FE8E610D0)
2019/05/19-17:54:25.648 TRACE_LEVEL_VERBOSE     ++ Found desired connection item in connection list
2019/05/19-17:54:25.648 TRACE_LEVEL_VERBOSE     ClientConnections_RemoveAndDestroy Exit
2019/05/19-17:54:25.648 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
2019/05/19-17:54:25.648 TRACE_LEVEL_INFORMATION EvtClientConnectionsDestroyConnection Entry (DISPOSING CONNE
CTION MEMORY)
2019/05/19-17:54:25.648 TRACE_LEVEL_VERBOSE     EvtClientConnectionsDestroyConnection Exit
2019/05/19-17:54:25.648 TRACE_LEVEL_VERBOSE     BthPS3_PDO_EvtDeviceContextCleanup Entry
2019/05/19-17:54:25.648 TRACE_LEVEL_VERBOSE     BthPS3_PDO_EvtDeviceContextCleanup Exit
2019/05/19-17:54:25.649 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Entry (Indication: 0x
1, Context: 0xFFFF858FE8E610D0)
```

```
1, Context: 0xFFFF858FE8E61DD0)
2019/05/19-17:54:25.649 TRACE_LEVEL_VERBOSE     L2CAP_PS3_ConnectionIndicationCallback Exit
--------------------------- Device connection dropped, all memory freed ---------------------------
```

Nice, the list is getting shorter 😄

May 19, 2019, 7:50 PM (https://localhost/post/1274)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

M molitar (https://localhost/user/molitar)
(https://localhost/user/molitar)

@nefarius (https://forums.vigem.org/uid/1) I am really glad to see progress and maybe soon a future where I will not have to use SCPToolkit in Windows 10 with my PS3 controller. I still prefer PS3 controller over the PS4 controller.

I have VMWare setup also with Windows 7 and 10 as well and if you need a beta tester I am more then willing. I use to do some software development for Database applications like Invoicing, Inventory, and Time software in Borland Delphi so I do know a bit about what to look for in bugs and how to report them.

May 19, 2019, 11:56 PM (https://localhost/post/1275)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

L Locksmith (https://localhost/user/locksmith)
(https://localhost/user/locksmith)

Wow, that's an intense weekend @nefarius (https://forums.vigem.org/uid/1)! I guess you'll have to swear the beta testers to secrecy with some blood oath and haunt them through the night if they do not report in! 😉 Great work, and it's really fun and interesting to follow the progress you post. Keep it up! 🙂

!ERAU QSSI DLRO WEHT

May 21, 2019, 6:44 PM (https://localhost/post/1277)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@molitar (https://forums.vigem.org/uid/278) @Locksmith (https://forums.vigem.org/uid/138) have a glimpse on the main page, should be a new category visible 😉

May 22, 2019, 8:47 PM (https://localhost/post/1282)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

M molitar (https://localhost/user/molitar)
(https://localhost/user/molitar)

@nefarius (https://forums.vigem.org/uid/1) Ok great I am doing an image backup of my system right now and will be removing SCP and testing within the hour 😉

May 24, 2019, 1:36 PM (https://localhost/post/1283)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Note to self: add `WdfDeviceInitSetExclusive` (https://docs.microsoft.com/en-us/windows-hardware/drivers/ddi/content/wdfdevice/nf-wdfdevice-wdfdeviceinitsetexclusive) to PDO to prevent multiple handles.

May 25, 2019, 6:39 AM (https://localhost/post/1284)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

R RDP (https://localhost/user/rdp)
(https://localhost/user/rdp)

Ok, finally had do register just to say I too have been following this story for months, and I don't know why (I'm not a programmer, unless you count some rudimentary VBA for Excel...), but coming to check in every few days is better than anything I find on Netflix; what an adventure! I do want to try this out once it is ready (I can only see source code on the main page, I still cant test it yet, right?), and will say goodbye to SCP then!

May 25, 2019, 3:42 PM (https://localhost/post/1285)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@RDP (https://forums.vigem.org/uid/290) be my guest (https://forums.vigem.org/topic/301/bthps3-installation-instructions-beta), I've updated your permissions.

May 25, 2019, 5:50 PM (https://localhost/post/1286)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

S seiif (https://localhost/user/seiif)
(https://localhost/user/seiif)

finally,the long awaited progress is here
i hale thy for doing what everybody couldn't
but seriously i am a follower since day one
i think no one can deny the progress made in this month
i hope i am not asking for much but if it's possible i wish i too can be a part of making a legendary milestone 🙂

May 25, 2019, 6:14 PM (https://localhost/post/1287)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@seiif (https://forums.vigem.org/uid/295) you've been added to the flock. Enjoy the ride.

May 26, 2019, 7:35 AM (https://localhost/post/1294)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

T thePalindrome (https://localhost/user/thepalindrome)
(https://localhost/user/thepalindrome)

pali, reporting for duty with only a *hint* of snark 😛

May 27, 2019, 4:15 AM (https://localhost/post/1298)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

C chaoticyeshua (https://localhost/user/chaoticyeshua)
(https://localhost/user/chaoticyeshua)

Good luck with the testing! I've been following this for a while and can't wait to finally have a true replacement for SCP. I'm very excited with the progress you've posted. Thank you so much for your work on this.

May 27, 2019, 5:54 PM (https://localhost/post/1300)

(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius) (https://localhost/user/nefarius)

The testing so far has been overwhelmingly good apart from some legacy SCP shenanigans ruining our fun with Shibari but that's a different topic and solvable.

May 30, 2019, 1:52 PM (https://localhost/post/1305)

(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

T

teeedubb (https://localhost/user/teeedubb) (https://localhost/user/teeedubb)

Hi nefarius,

I too have been reading your posts on a regular basis and have been getting much enjoyment out of them (even if some of it is so technical it may as well be Chinese to me 😊).
While I'm not a hardcore coder, I love tinkering and would love to help out with testing. My machine is win 10 x64, soon to be 1903, with a Intel 9260 Bluetooth card, which hast had SCP installed on it. Currently have a Xbox 1 and ds4 controller paired to it and have two real ds3's to test with. Oh, and I also have a couple of no name bt adapters that I used to use with SCP that I could also use.

May 31, 2019, 5:41 AM (https://localhost/post/1306)

(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

C

chaoticyeshua (https://localhost/user/chaoticyeshua) (https://localhost/user/chaoticyeshua)

I wouldn't mind testing either if you're still looking for more people to help. I have access to two different Bluetooth adapters (this (https://www.amazon.com/gp/product/B008BC1U4O/ref=ppx_yo_dt_b_search_asin_title?ie=UTF8&psc=1) and this (https://www.amazon.com/gp/product/B071X46MT2/ref=ppx_yo_dt_b_search_asin_title?ie=UTF8&psc=1)), an original DS4 controller, 2x original DS3 controllers, and 2x Xbox One controllers, as well as multiple computers I could use for testing (all Windows 10 1809 currently).

I do desktop and server support for a living, so I'm comfortable modifying the registry and adding/removing drivers and all that. Not sure what all might be needed in this scenario, but I'll do whatever you may need. Just let me know.

May 31, 2019, 1:55 PM (https://localhost/post/1308)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@teeedubb (https://forums.vigem.org/uid/143) @chaoticyeshua (https://forums.vigem.org/uid/270) welcome to the flock then, I've adapted your permissions, have fun 😄

Jun 4, 2019, 10:31 PM (https://localhost/post/1323)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

E

ekze (https://localhost/user/ekze)
(https://localhost/user/ekze)

I'd like to test as well, here's my setup: original Sixaxis and DS3 with a Chinese clone. Bluetooth V4.0+EDR adapter (CSR8510). Had no success with AirBender. photo (https://i.imgur.com/fITSDht.jpg)

Jun 6, 2019, 5:37 AM (https://localhost/post/1329)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

K

Kue (https://localhost/user/kue)
(https://localhost/user/kue)

If you are looking for any more beta testers please include me. I have 2 chinese DS3 controllers. and 2 bluetooth usb dongles (both bluetooth 4.0) and one bluetooth card built in to the laptop (bluetooth 4.2). I would love to help in anyway I can.

Jun 6, 2019, 3:28 PM (https://localhost/post/1331)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@ekze (https://forums.vigem.org/uid/323) @Kue (https://forums.vigem.org/uid/243) welcome aboard! 🚌

Jun 6, 2019, 6:37 PM (https://localhost/post/1333)

 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

T (https://localhost/user/tulio150) tulio150 (https://localhost/user/tulio150)

Hello, i have interest in beta testing too. I currently have two original DS3s that i use for playing with FireShock 1.3.1.0 via USB. Aditionally, i have a Bluetooth CSR2.1 USB adapter (VID_0A12&PID_0001). I've been reading this thread for a while and it's amazing the work you have been doing.

---

10 DAYS LATER

Jun 16, 2019, 7:16 AM (https://localhost/post/1364)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

R (https://localhost/user/ryantburke) ryantburke (https://localhost/user/ryantburke)

Hi! I am also interested in beta testing. I have a two real DS3s. This work is super exciting, I would love to hop on board!

Jun 16, 2019, 11:48 AM (https://localhost/post/1366)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

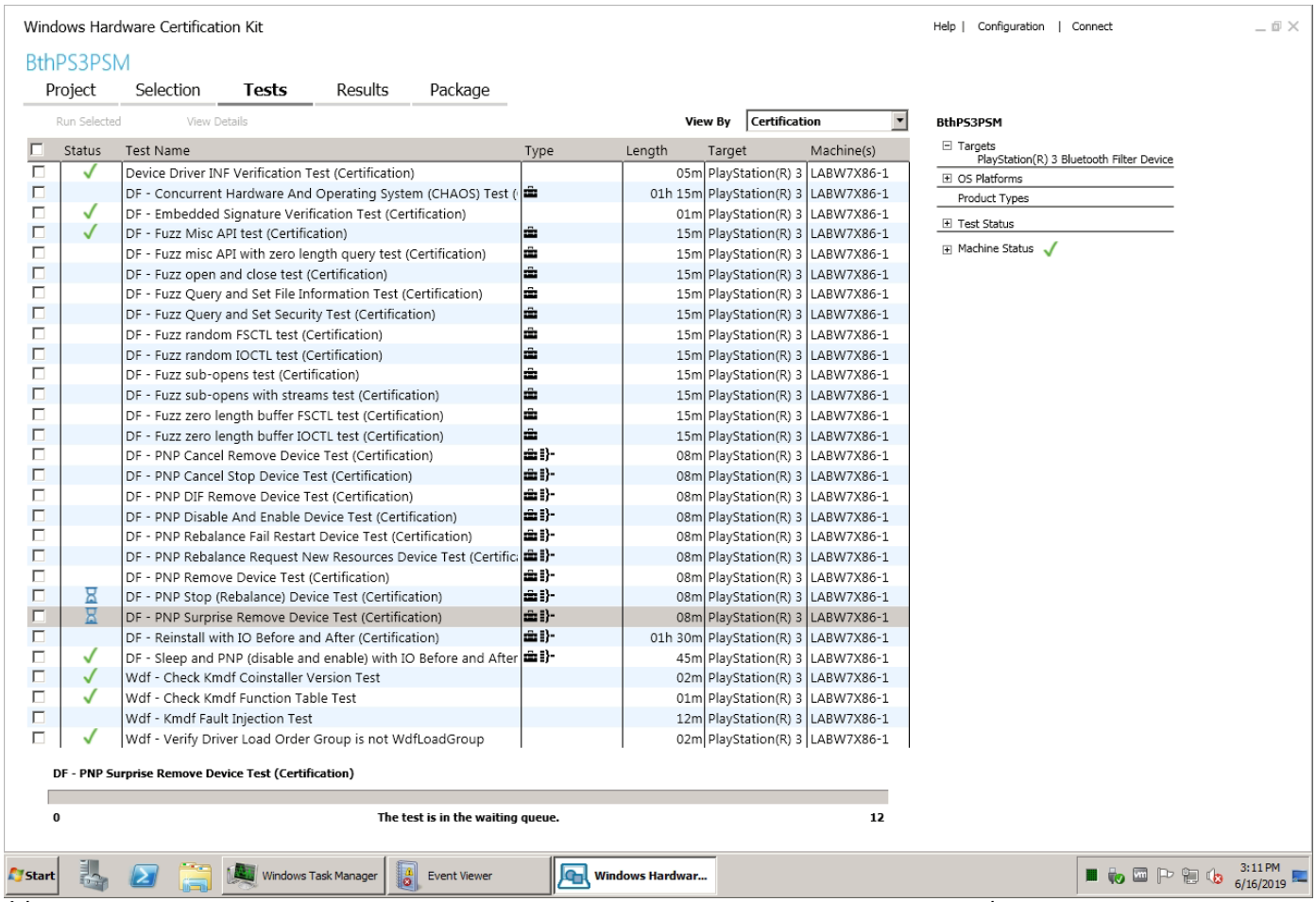
 (https://localhost/user/nefarius) nefarius (https://localhost/user/nefarius)

Since test feedback has been very pleasing so far I'll cut back on recruitment today and implement the missing bits and pieces in the drivers and then throw them into the WHQL test bench. Will keep you updated.

Jun 16, 2019, 3:13 PM (https://localhost/post/1367)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 (https://localhost/user/nefarius) nefarius (https://localhost/user/nefarius)

Jo, it's WHQL-o-clock 😅



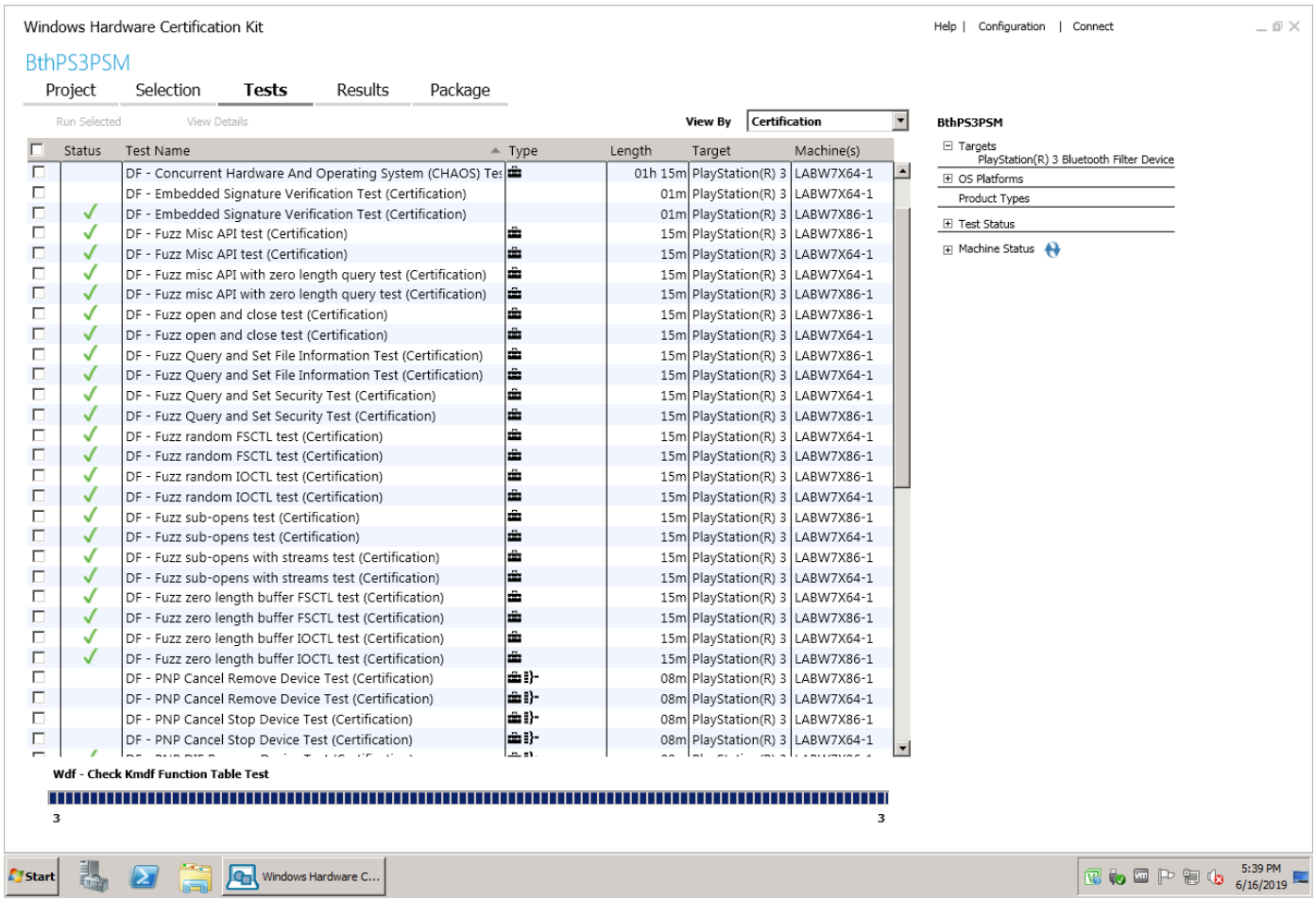
(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/586b0df3-e046-49ff-8470-fe347dae078d-image.png)

This time the filter is my primary test subject. Fingers crossed! ☠️

Jun 16, 2019, 5:41 PM (https://localhost/post/1370)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Oh yes, give me more green! All the green tick marks! 😎



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/vmware_8niffzysxj.png)

Jun 16, 2019, 7:16 PM (https://localhost/post/1371)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@tulio150 (https://forums.vigem.org/uid/326) @ryantburke (https://forums.vigem.org/uid/348) done, welcome!

Jun 16, 2019, 7:27 PM (https://localhost/post/1372)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

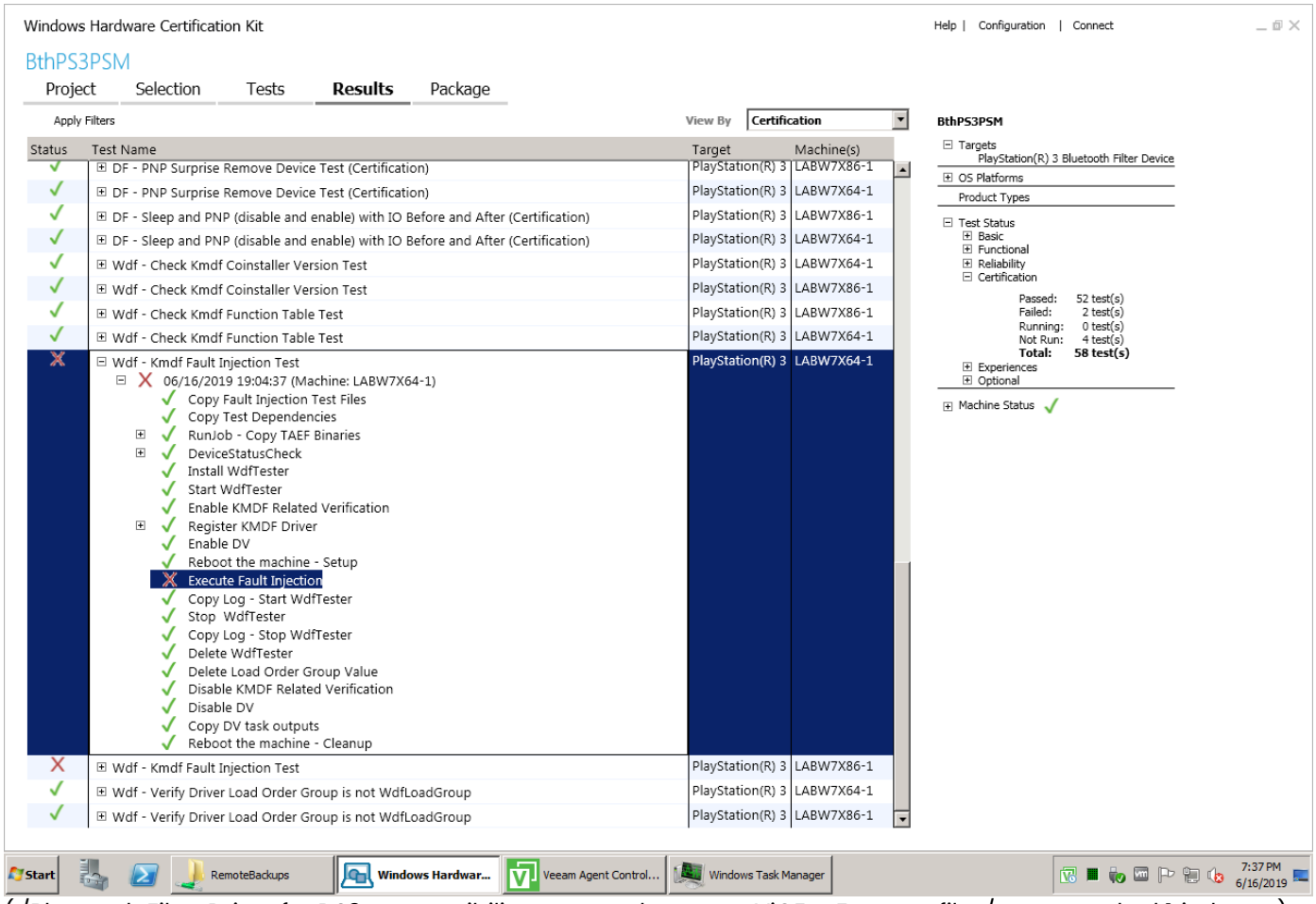

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@Poosaurus you too 😛

Jun 16, 2019, 7:47 PM (https://localhost/post/1373)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Dammit, almost... 👀



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/vmware_zktak1rimb.png)

What's going on here....

```
STACK_TEXT:
nt!DbgBreakPoint
Wdf01000!imp_WdfCollectionRemove+0x2d1 [d:\win8_ldr\minkernel\wdf\framework\kmdf\src\support\fxcollectionapi.cpp @ 270]
wdftester!wdftester_WdfCollectionRemove+0xfe
BthPS3PSM!BthPS3PSM_EvtDeviceContextCleanup+0x103 [d:\development\git.vigem.org\bthps3\bthps3psm\device.c @ 372]
Wdf01000!FxObject::DisposeChildrenWorker+0x2fa [d:\win8_ldr\minkernel\wdf\framework\shared\object\fxobjectstatemachine.cpp @ 1188]
Wdf01000!FxObject::PerformDisposingDisposeChildrenLocked+0xbc [d:\win8_ldr\minkernel\wdf\framework\shared\object\fxobjectstatemachine.cpp @ 814]
Wdf01000!FxObject::PerformEarlyDisposeWorkerAndUnlock+0xfb [d:\win8_ldr\minkernel\wdf\framework\shared\object\fxobjectstatemachine.cpp @ 894]
Wdf01000!FxObject::EarlyDispose+0x117 [d:\win8_ldr\minkernel\wdf\framework\shared\object\fxobjectstatemachine.cpp @ 460]
Wdf01000!FxPkgPnp::PnpEventRemovedCommonCode+0x1e2 [d:\win8_ldr\minkernel\wdf\framework\shared\irphandlers\pnp\pnpstatemachine.cpp @ 2047]
Wdf01000!FxPkgFdo::PnpEventFdoRemovedOverload+0x9 [d:\win8_ldr\minkernel\wdf\framework\shared\irphandlers\pnp\fxpkgfdo.cpp @ 1244]
Wdf01000!FxPkgPnp::PnpEnterNewState+0x1a1 [d:\win8_ldr\minkernel\wdf\framework\shared\irphandlers\pnp\pnpstatemachine.cpp @ 1231]
Wdf01000!FxPkgPnp::PnpProcessEventInner+0x122 [d:\win8_ldr\minkernel\wdf\framework\shared\irphandlers\pnp\pnpstatemachine.cpp @ 1147]
Wdf01000!FxPkgPnp::PnpProcessEvent+0x18d [d:\win8_ldr\minkernel\wdf\framework\shared\irphandlers\pnp\pnpstatemachine.cpp @ 933]
Wdf01000!FxDevice::DeleteDeviceFromFailedCreateNoDelete+0x13e [d:\win8_ldr\minkernel\wdf\framework\kmdf\src\core\fxdevice.cpp @ 530]
Wdf01000!FxDriver::AddDevice+0x158 [d:\win8_ldr\minkernel\wdf\framework\kmdf\src\core\fxdriver.cpp @ 550]
nt!PpvUtilCallAddDevice+0x45
nt!PnpCallAddDevice+0xd5
nt!PipCallDriverAddDevice+0x661
nt!PipProcessDevNodeTree+0x2b2
nt!PiRestartDevice+0xc7
nt!PnpDeviceActionWorker+0x313
nt!ExpWorkerThread+0x111
nt!PspSystemThreadStartup+0x194
nt!KiStartSystemThread+0x16
```

Alright, what went wrong there on device disposal...

```
--- start of log ---
1: FxIFRStart - FxIFR logging started
2: LockVerifierSection - Increment Lock counter (2) for Verifier Paged Memory from  \REGISTRY\MACHINE\SYSTEM
\ControlSet001\services\BthPS3PSM from driver globals FFFFFA8009A2B970
3: FxVerifierLock::InitializeLockOrder - Object Type 0x1036 does not have a lock order defined in fx\inc\FxV
erifierLock.hpp
4: FxVerifierLock::InitializeLockOrder - Object Type 0x1036 does not have a lock order defined in fx\inc\FxV
erifierLock.hpp
5: FxPkgPnp::PnpEnterNewState - WDFDEVICE 0x0000057FF58B94E8 !devobj 0xFFFFFA800AD37C20 entering PnP State W
dfDevStatePnpInit from WdfDevStatePnpObjectCreated
6: FxDevice::DeleteDeviceFromFailedCreateNoDelete - WDFDEVICE 0000057FF58B94E8 !devobj FFFFFA800AD37C20 crea
ted, but EvtDriverDeviceAdd returned status 0xc0000001(STATUS_UNSUCCESSFUL) or failure in creation
7: FxDevice::DeleteDeviceFromFailedCreateNoDelete - WDFDEVICE 0000057FF58B94E8, !devobj FFFFFA800AD37C20 is
a filter, converting 0xc0000001(STATUS_UNSUCCESSFUL) to STATUS_SUCCESS
8: FxPkgPnp::PnpEnterNewState - WDFDEVICE 0x0000057FF58B94E8 !devobj 0xFFFFFA800AD37C20 entering PnP State W
dfDevStatePnpRemoved from WdfDevStatePnpInit
9: FxChildList::NotifyDeviceRemove - WDFCHILDLIST 0000057FF597F388:  removing children
10: FxPkgPnp::PnpEnterNewState - WDFDEVICE 0x0000057FF58B94E8 !devobj 0xFFFFFA800AD37C20 entering PnP State
WdfDevStatePnpRemovedChildrenRemoved from WdfDevStatePnpRemoved
11: FxPkgPnp::PnpEnterNewState - WDFDEVICE 0x0000057FF58B94E8 !devobj 0xFFFFFA800AD37C20 entering PnP State
WdfDevStatePnpFdoRemoved from WdfDevStatePnpRemovedChildrenRemoved
12: FxPkgIo::StopProcessingForPower - Perform FxIoStopProcessingForPowerPurgeNonManaged for all queues of WD
FDEVICE 0x0000057FF58B94E8
13: FxIoTarget::WaitForDisposeEvent - WDFIOTARGET 0000057FF59F0368, Waiting on Dispose event FFFFF880031B0AD
0
14: imp_WdfCollectionRemove - WDFOBJECT 0000057FF58B94E8 not in WDFCOLLECTION 0000057FF57BAF78, 0xc0000225(S
TATUS_NOT_FOUND)
---- end of log ----
```

Oh 😐 How did I manage to provoke that. Well, back to fixing stuff 😅

Jun 18, 2019, 3:42 PM (https://localhost/post/1377)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

K (https://localhost/user/krimpsok) krimpsok (https://localhost/user/krimpsok)

Very impressive work, would be interested in beta testing with an original Sixaxis DS3 and Bluetooth 4.0 adapter.

Jun 18, 2019, 7:08 PM (https://localhost/post/1378)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 (https://localhost/user/nefarius) nefarius (https://localhost/user/nefarius)

In my previous test run the filter crashed at the test `Wdf - Kmdf Fault Injection Test`

This test is actually amazing! (https://docs.microsoft.com/en-us/windows-hardware/drivers/devtest/wdffitester-overview) 😲 Summary:

> For each DDI that has been configured for fault injection, the WdfFiTester tool returns an NTSTATUS code of STATUS_UNSUCCESSFUL. The driver is expected to handle the failure.

That is really cool! It means, that it uncovers continued code execution where a faulty return code of a WDF function call isn't caught properly, which may lead to a crash (as demonstrated in my last run). I think I've nailed down the issue in my code and just started another run. Fingers crossed 🤞

Jun 19, 2019, 2:34 PM (https://localhost/post/1379)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

K (https://localhost/user/keefey) keefey (https://localhost/user/keefey)

Beyond impressed with this. I've been wanting to use the PS3 Navi remote for my HTPC for years, but I didn't have the willpower to dig into it like you have. Also, thanks so much for the PS4 remote drivers. They worked flawlessly. Now able to use the Nvidia shield without having to pair/unpair its remote (next step is to run Steam Link on the Pi and then use it directly on that in a different room).

Also happy to beta test, although it looks like you have plenty - I have a plethora of Windows machines, Pi's and Android TVs and tablets (also, as an aside, I'm also happy to give advice on career paths into coding if it will help - I manage teams of coders, previously at Atlassian, now about to join a startup. Was surprised to read it's been difficult).

Looking forward to the final commit! 🎮

Jun 20, 2019, 8:19 PM (https://localhost/post/1380)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 (https://localhost/user/chileanhugdealer)
ChileanHugDealer (https://localhost/user/chileanhugdealer)

Man i've been reading your notes for a while now, it has been one interesting adventure even when i know very little about software coding. i'll be looking forward to send you a tip or buying the final version once its done! (idk if im mistaken or not but i remember you have a patreon going by nefarious soft solutions... right?).

On a side note im using a genuine Sixaxis DS3 so i don't know if thats useful for beta testing (considering how many already got enroled) also im using a Wifi-Bth combo card (Qualcomm atheros) with scp.
Cheers!

---

10 DAYS LATER

Jun 30, 2019, 2:02 PM (https://localhost/post/1394)

 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

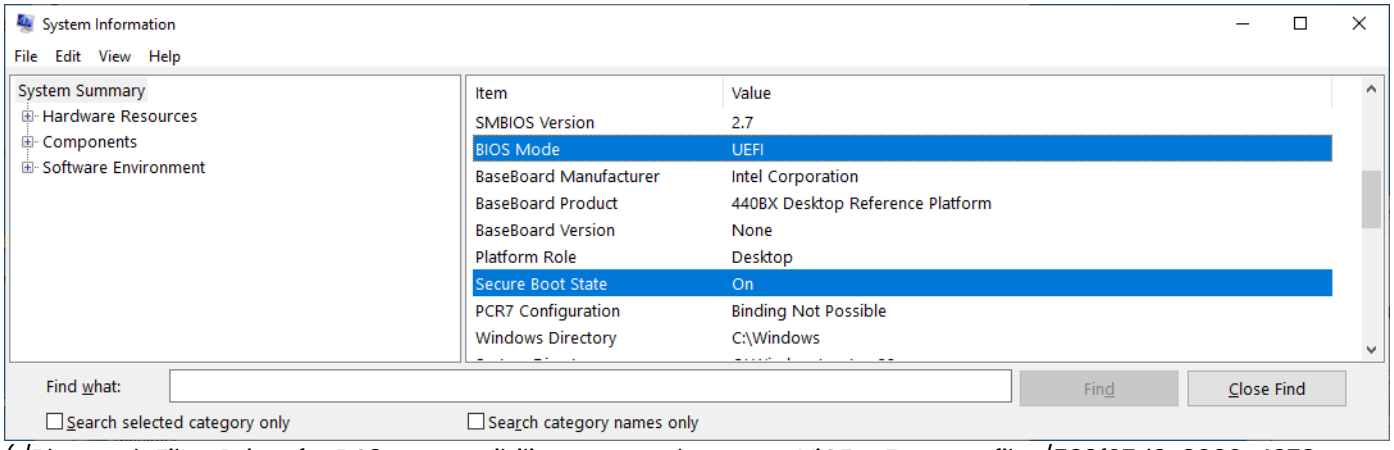
Why WHQL though...

Why am I wasting so much time and resources on WHQL testing? Well, quick real-life demonstration on why cross-signing (misleadingly referred to as self-signing) kernel-mode code with an EV certificate alone in Windows 10 (UEFI, SecureBoot) doesn't work 🙂

Installation attempt of filter driver

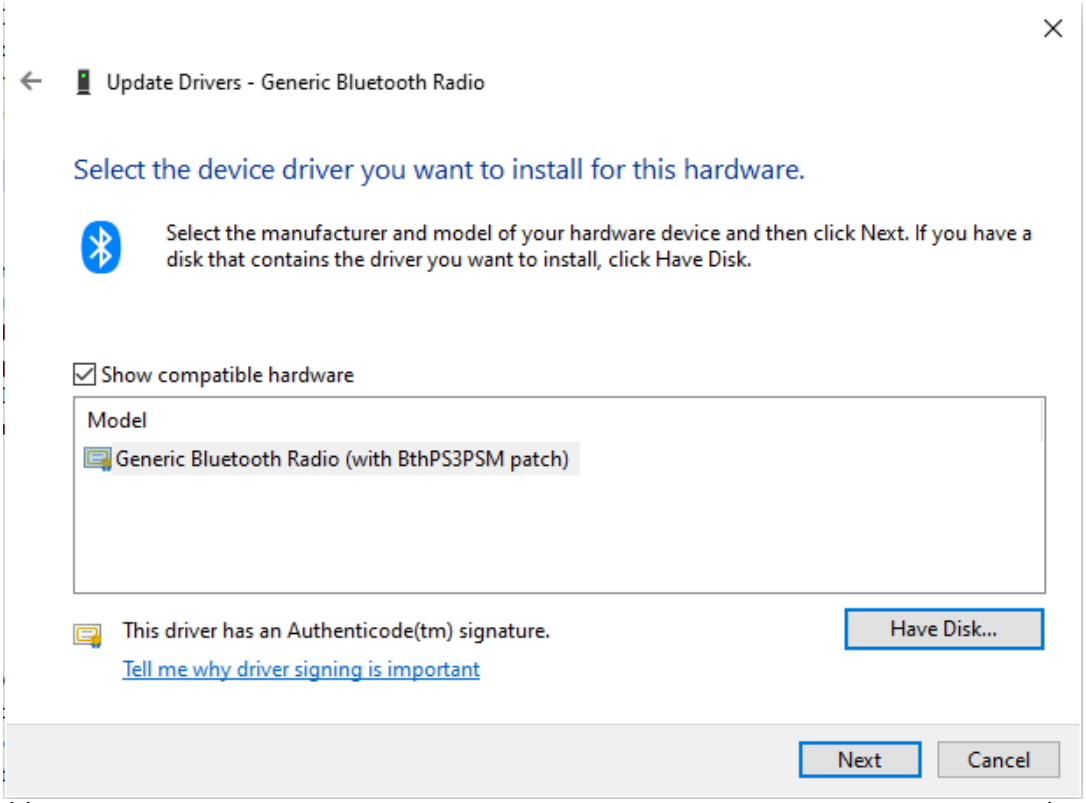
Environment details

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/61ca88c2-51ac-4e61-a910-4716fbb63e61-image.png)



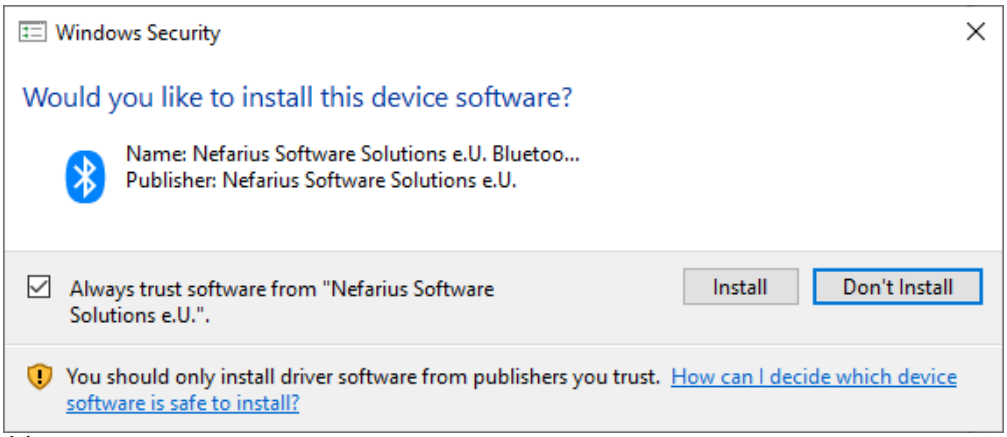
(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/539f07d9-9060-4878-82ed-cb46447f9d85-image.png)

INF (CAT) signed and happily offered



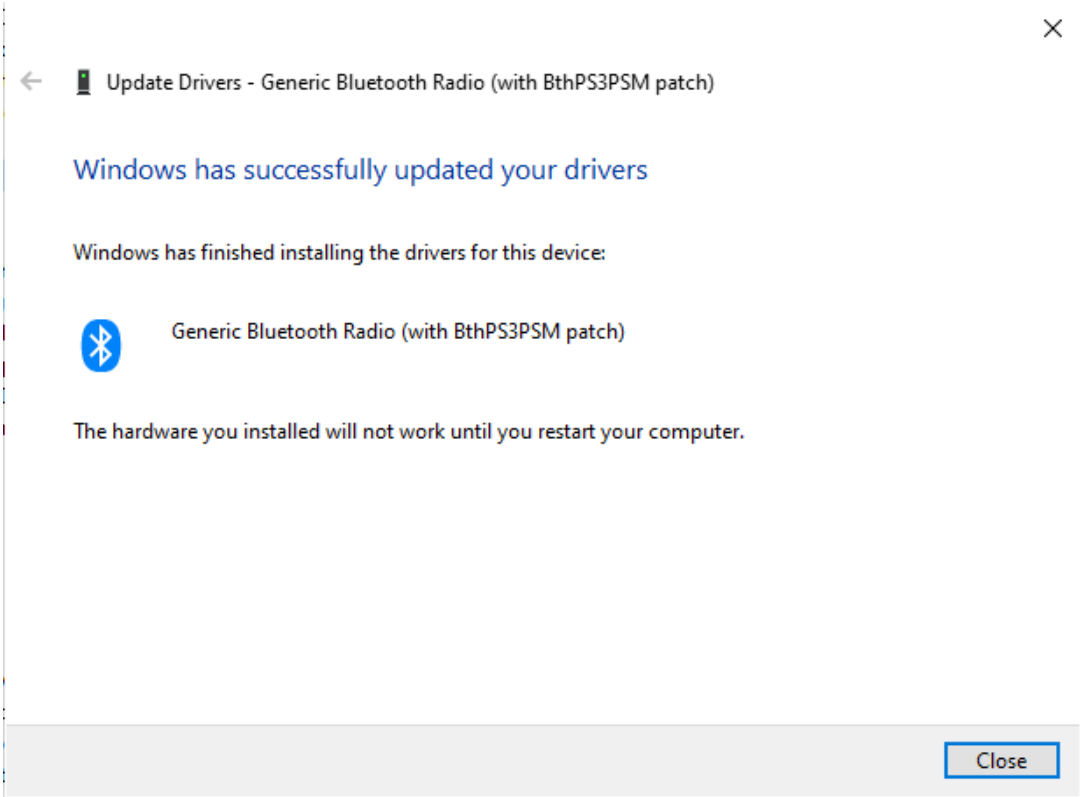
(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/ac968c22-7fad-43c4-8d29-595932771751-image.png)

So far so good...



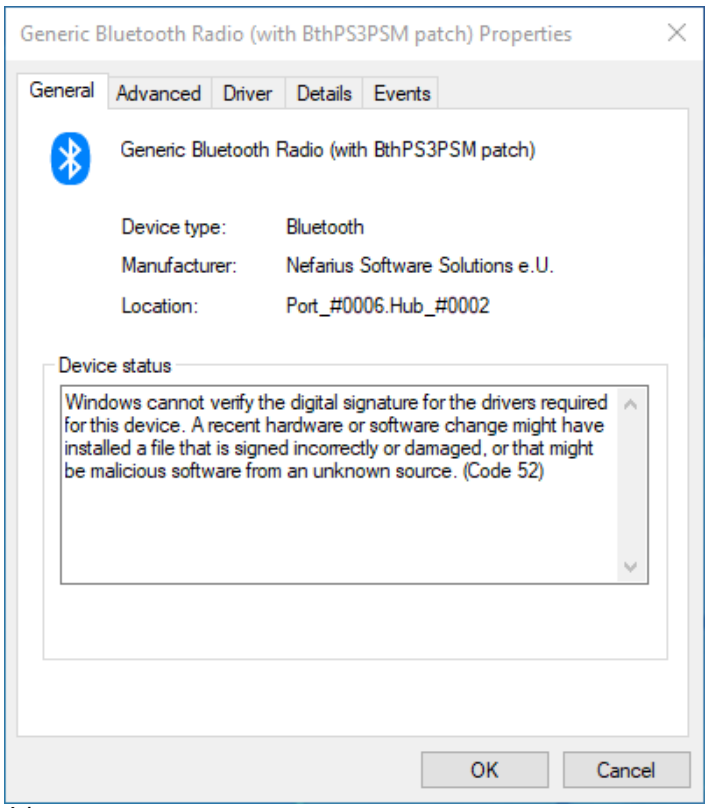
(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/1db1ca3e-5e94-4215-bcdb-34203570dffa-image.png)

Uh oh, restart required, not promising...



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/7eb497fc-f875-4666-a086-05ce95eef758-image.png)

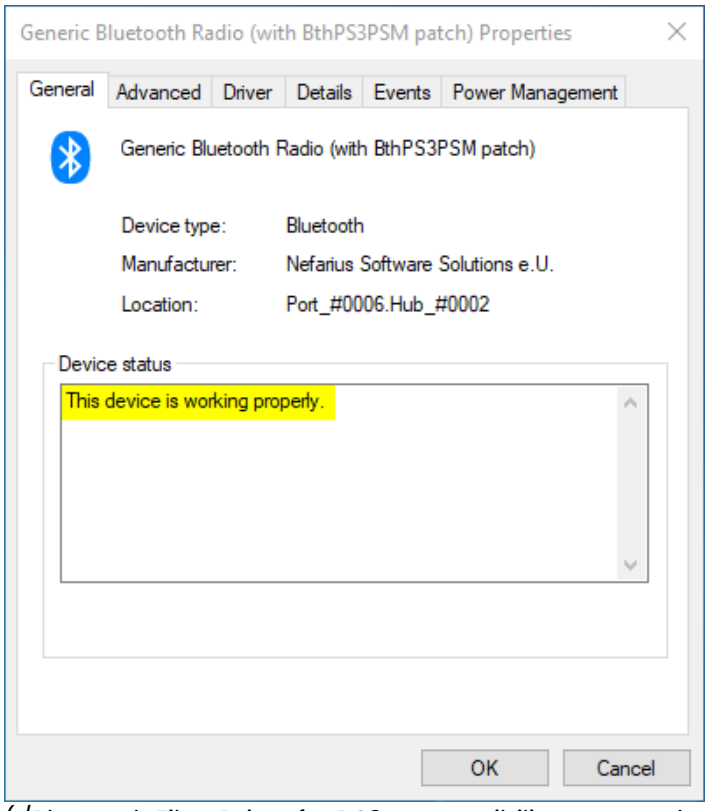
And there we have it ☹️



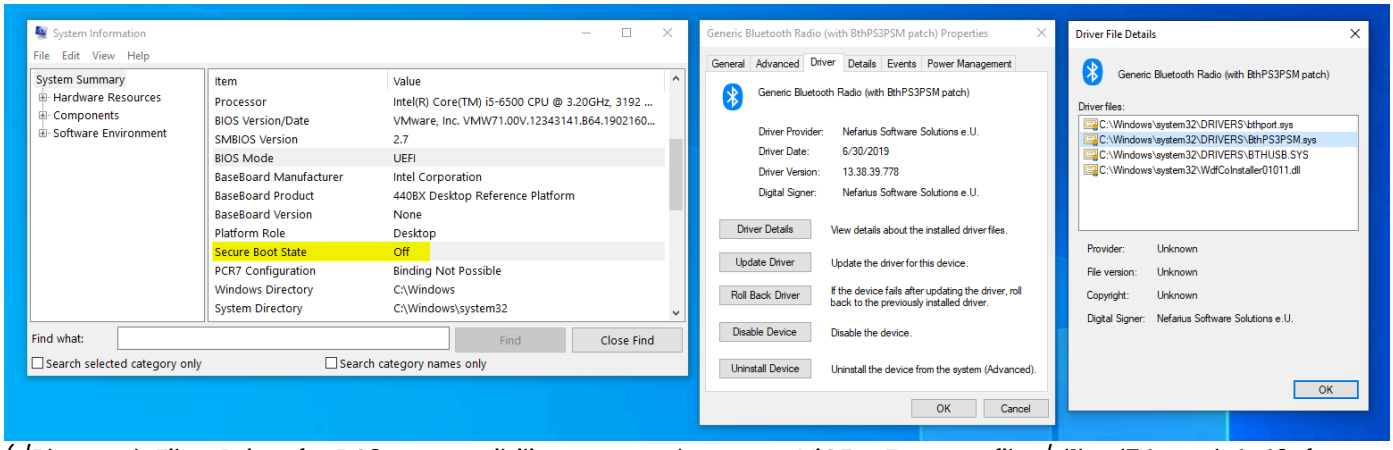
(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/2f25da8e-fd86-4a7a-a295-89f54f98414b-image.png)

Now with "Secure"Boot off

SecureBoot directly influences Code Integrity settings applying to the kernel with a rather drastic impact:



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/065ccc7e-ecc7-4f12-b904-b3fe66168e2b-image.png)



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/d1bed74e-eeb4-43cf-a8e3-a373ad6ef6c5-image.png)

So this would be production-ready. Except the cross-signed binary will not load when the rather common SecureBoot is enabled in UEFI. The Server Edition should be even more restrictive and not load cross-signed drivers anymore even without SecureBoot starting from Server 2016 IIRC. Yay...

Jun 30, 2019, 9:11 PM (https://localhost/post/1395)
□ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 □ (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius) (https://localhost/user/nefarius)

@keefey (https://forums.vigem.org/uid/355) hi! Well, currently it appears to be working fine, the whole self-employed coder thingy 😅 just need to clone myself hehe. Yeah my "mainstream" coding career never took off so here I am being my own boss 😛

@ChileanHugDealer (https://forums.vigem.org/uid/229) heya! Thanks for the encouragement, I do have a Patreon (https://forums.vigem.org/topic/291/shameless-beggar-post) and currently got enough testers and so far I'm pleased with the overall results and now need to focus on getting this stack production-ready.

Cheers

Jul 1, 2019, 4:01 PM (https://localhost/post/1396)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 3
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Status update

We're almost feature-complete on both profile/bus and filter driver.

A very good suggestion I still have to fully implement. The downside of the filter being active is interference with other common devices like the DS4 in "PC mode" and apparently also some branches of Xbox One compatible controllers? I currently only own an Xbox One Elite pad and that requires its own 5 GHz wireless adapter which isn't Bluetooth anyway 🤔

So since the filter sits too low (USB/URB level) to know anything about the HCI/L2CAP state machine, it relies on some outside factors to decide if it should patch or not. So we thought about this flow:

- Filter is active, PS3 peripherals can connect to profile driver
- DS4 in "PC mode" connects, gets redirected to profile driver because PSM got patched
- Profile driver denies connection with `CONNECT_RSP_RESULT_PSM_NEG` and instructs filter to disable itself for like 10 seconds
- User presses PS button on DS4 to retry connection
- Connection now successful due to filter being temporarily disabled
- Timer enables filter again on its own to minimize required user interaction

I haven't found a way to reject a connection attempt without the DS4 giving up so the only remaining inconvenience would be the user having to connect the controller twice if the filter is active. Other than that I think we thought off every possibility to minimize the negative impact on user experience.

What do you think?

Jul 2, 2019, 10:41 AM (https://localhost/post/1397)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

E epikvigem (https://localhost/user/epikvigem)
(https://localhost/user/epikvigem)

@nefarius (https://forums.vigem.org/uid/1) i think that you are breathtaking. 😏

Anyway it's a good solution if there aren't other methods.

Jul 2, 2019, 11:43 AM (https://localhost/post/1398)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

A AnyHoLiC (https://localhost/user/anyholic)
(https://localhost/user/anyholic)

@nefarius (https://forums.vigem.org/uid/1) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1396):

> - Profile driver denies connection with `CONNECT_RSP_RESULT_PSM_NEG` and instructs filter to disable itself for like 10 seconds
> - User presses PS button on DS4 to retry connection
> - Connection now successful due to filter being temporarily disabled
> - Timer enables filter again on its own to minimize required user interaction
>
> I haven't found a way to reject a connection attempt without the DS4 giving up so the only remaining inconvenience would be the user having to connect the controller twice if the filter is active. Other than that I think we thought off every possibility to minimize the negative impact on user experience.
>
> What do you think?

Great job! Thank you for the efforts you put in this along with the team.

I'm not so into technical stuff, but I'll try my best here.

The whole "reconnect" concept reminds of InputMapper 1.6. On the other hand, DS4Windows 1.7.5+ reestablishes the connection without the user initiating it manually. Just a reminder, both of these programs use ViGEm drivers.

How does one (DS4W) achieves it while the other doesn't?

Jul 2, 2019, 2:43 PM (https://localhost/post/1399)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@AnyHoLiC (https://forums.vigem.org/uid/297) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1398):

> How does one (DS4W) achieves it while the other doesn't?

They don't. They don't/can't interfere with the Bluetooth connection process as that's completely abstracted away from them. They can send regular disconnect requests which works fine as long as the connection sequence isn't manipulated and the DS4 remains in "PC mode". The DS4 is a bit of a bastard child in this regards; even when once successfully paired to a Windows machine, once it has been turned off and turned on again it sneakily tries to connect in "PS4 mode" (a.k.a. directly establish HID Control and HID Interrupt L2CAP channels) which usually gets immediately rejected by the Windows Bluetooth stack and it tries again in "PC mode". Now with my filter patch active, the connection is - unexpectedly - routed through and the side effect I described happens. So this listing is my proposed solution/workaround until a better solution surfaces.

Cheers

Jul 2, 2019, 4:23 PM (https://localhost/post/1400)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

A AnyHoLiC (https://localhost/user/anyholic)
(https://localhost/user/anyholic)

@nefarius (https://forums.vigem.org/uid/1) Thanks for the explanation.

So far the only issues I have while connecting DS4 to Windows (Windows 10, specifically) are the most common ones, while using IM and DS4W, which are:

1. It takes longer to establish a connection compared to connecting to a PS4.
2. Latency.
3. Using it with Uplay (Ubisoft's) is basically unusable, which continuously switches back and forth between X360 and DS4 modes.

I have yet to install ViGEm directly using PowerShell without using any extra programs.

You don't have to reply to this.

Thanks again for your insight.

Jul 3, 2019, 6:12 PM (https://localhost/post/1402)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@AnyHoLiC (https://forums.vigem.org/uid/297) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1400):

> I have yet to install ViGEm directly using PowerShell without using any extra programs.

PowerShell ain't no more mate 😛 see the news (https://forums.vigem.org/topic/288/vigem-bus-driver-v1-16-112-released)

Jul 4, 2019, 9:53 AM (https://localhost/post/1406)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

L Luke76bg (https://localhost/user/luke76bg) (https://localhost/user/luke76bg)

@nefarius (https://forums.vigem.org/uid/1) Funny, i have to connect my ds4 to scptoolkit twice too, to get it recognized! I can't wait to try it, i need autofire for bloodstained and joytokey auto repeat doesn't work...However twice or not, your work is amazing!!!

Jul 5, 2019, 10:16 AM (https://localhost/post/1411)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius) (https://localhost/user/nefarius)

Survey: Desired Windows OS compatibility

Ladies and gents, it's getting serious! 😅 I need community feedback on where to go from here with the singing fun for the production release. I've crafted a poll with the first answer being the most convenient and fast but most exclusive route and the last one being the most annoying but also most inclusive. Hop on, your voice matters! 🎉

👉 BthPS3 - Desired Windows OS compatibility 👈 (https://www.strawpoll.me/18273429)

Cheers

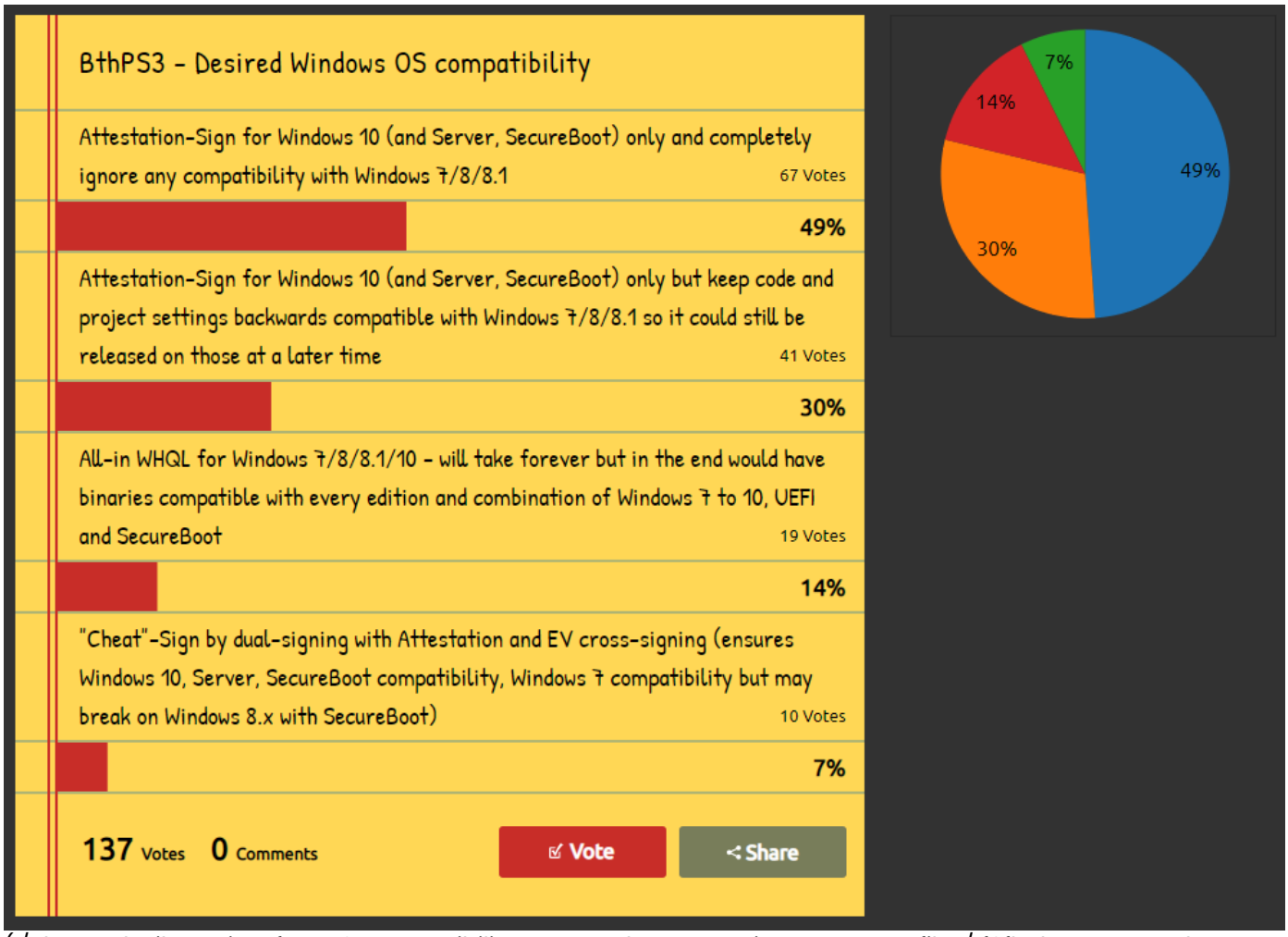
---

9 DAYS LATER

Jul 14, 2019, 1:23 PM (https://localhost/post/1415)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 3 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius) (https://localhost/user/nefarius)

Quick intermediate survey result summary after being up slightly over a week:



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/1f6fb8bc-4477-40dc-a400-791668ba0ddb-image.png)

Well, lots of Windows 10 fans it seems 😄

By the way, another advantage of going with the "ditch legacy OS support completely" option will be: I can develop the function driver (HID-miniport driver, for DI/Unity/PCSX2/... compatibility, pressure exposure etc.) with the User-Mode Driver Framework (https://docs.microsoft.com/en-us/windows-hardware/drivers/wdf/overview-of-the-umdf) which would have loads of advantages (dev speed, debugging, stability, quick release cycles, ...) so that would be another step up in motivation for me.

More news to come!

Jul 14, 2019, 3:43 PM (https://localhost/post/1416)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

A (https://localhost/user/anontsuki) anontsuki (https://localhost/user/anontsuki)

Speaking of which, I was curious about how much information the filter driver would support for the DualShock 3. I was thinking that because it has basically "native" support when patched, everything would work, but do you have to program functions in so that pressure sensitivity and other DS3 related controller functions passed that information along to Windows?

Jul 16, 2019, 3:51 PM (https://localhost/post/1418)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@anontsuki (https://forums.vigem.org/uid/395) that's the job of the function driver which still has to be written, but that's "easy" compared to what was achieved 'till now. So in the ultimate end result Shibari as a proxy application won't be necessary anymore at all.

Jul 17, 2019, 3:38 AM (https://localhost/post/1419)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

A

anontsuki (https://localhost/user/anontsuki)
(https://localhost/user/anontsuki)

Very cool. I look forward to the entire thing being complete, whenever that time comes =).

---

10 DAYS LATER

Jul 26, 2019, 7:28 PM (https://localhost/post/1429)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

L

Luke76bg (https://localhost/user/luke76bg)
(https://localhost/user/luke76bg)

When the first release is scheduled ? 🙂

Jul 26, 2019, 8:00 PM (https://localhost/post/1430)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@Luke76bg (https://forums.vigem.org/uid/219) am still unsure if I should do a "requires Shibari" release or go all in. The latter would definitely take even more time and I gotta balance it with my current workload. Other than that, maybe September?

Jul 26, 2019, 8:15 PM (https://localhost/post/1431)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

kirian (https://localhost/user/kirian)
(https://localhost/user/kirian)

@nefarius (https://forums.vigem.org/uid/1) Shibari was crashing when disconnecting a controller by bluetooth or when an connected controller by bluetooth was connected then by USB, I remember it spawned 2 controllers in this situation or something like that.
Unless these issues can be really easily fixed in a day or two, I'd vote for you to focus on the release with no companion app, even if it takes longer.
Good luck, Nefarius, and have a nice day!

Jul 26, 2019, 8:50 PM (https://localhost/post/1432)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@kirian (https://forums.vigem.org/uid/158) everything that's a pure Shibari issue can be fixed with ease. I just don't put much effort into hardening it because of time budget. Drivers need to be rock solid, that's number one.

Jul 26, 2019, 10:15 PM (https://localhost/post/1433)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

L

Luke76bg (https://localhost/user/luke76bg)
(https://localhost/user/luke76bg)

@nefarius (https://forums.vigem.org/uid/1) Thanks for the answer Nefarious, i'm sure it will be an amazing piece of software! I can't wait! ^^

Jul 26, 2019, 10:22 PM (https://localhost/post/1434)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

E

epikvigem (https://localhost/user/epikvigem)
(https://localhost/user/epikvigem)

@nefarius (https://forums.vigem.org/uid/1) i can't wait too. 🙂

For the release schedule you said "early may" u.u (i'm here following your news since march X'D)

But i'd always think that it's better to wait more for a better "product", thanks for your work :).

Jul 29, 2019, 2:30 AM (https://localhost/post/1435)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@epikvigem (https://forums.vigem.org/uid/155) there's a few topics who threw off the schedule:

- Windows 10 1903 changes apparently breaking kernel drivers left and right. Did quite a bit of research on that to break through all the misinformation on the web.
- WHQL lab advances. This took the most time, setting up the lab and running a lot of tests. Tedious and costly.
- Working on paid commissions. Ever since I've started the business I'm also doing contracted work. That wins ofc. over this hobby-ish fun topic as this stuff doesn't pay the bills as long as the Patreon and other sources of income are low 😉 That's just how life is. More funds, more speed. Simple formula.

Cheers

Aug 3, 2019, 2:17 PM (https://localhost/post/1436)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

K

kempol (https://localhost/user/kempol)
(https://localhost/user/kempol)

since airbender doesnt work, it's safe to uninstall it right?

Aug 3, 2019, 5:10 PM (https://localhost/post/1437)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@kempol (https://forums.vigem.org/uid/421) sure! Can be removed anytime!

---

12 DAYS LATER

Aug 15, 2019, 9:28 AM (https://localhost/post/1447)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Posted on PCSX2 forums

Related thread, for the record (https://forums.pcsx2.net/Thread-Native-Windows-Bluetooth-drivers-for-PlayStation-3-Peripherals-WIP). Might or might not go somewhere. Time will tell.

Aug 15, 2019, 9:13 PM (https://localhost/post/1448)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

P

pnkiller78 (https://localhost/user/pnkiller78)
(https://localhost/user/pnkiller78)

@nefarius (https://forums.vigem.org/uid/1) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1447):

> # Posted on PCSX2 forums
>
> Related thread, for the record (https://forums.pcsx2.net/Thread-Native-Windows-Bluetooth-drivers-for-PlayStation-3-Peripherals-WIP). Might or might not go somewhere. Time will tell.

What happened? I though that this project was going well.... 😞

Aug 15, 2019, 9:43 PM (https://localhost/post/1449)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@pnkiller78 (https://forums.vigem.org/uid/171) Pardon, it appears like I should've been more specific in my wording. I meant let's see if the thread over there grabs some attention which it currently doesn't appear to do. Meanwhile I'll continue my shenanigans over here as usual 🦄

Aug 19, 2019, 2:24 AM (https://localhost/post/1450)

 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

P pnkiller78 (https://localhost/user/pnkiller78)
(https://localhost/user/pnkiller78)

@nefarius (https://forums.vigem.org/uid/1) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1449):

> @pnkiller78 (https://forums.vigem.org/uid/171) Pardon, it appears like I should've been more specific in my wording. I meant let's see if the thread over there grabs some attention which it currently doesn't appear to do. Meanwhile I'll continue my shenanigans over here as usual 🦄

Oh, I see, I was worried that something might have cause you to lost interest.... 😅
I'm waiting with great anticipation for this project to become official... I think it's pretty cool what you have done here.👍

Aug 21, 2019, 10:10 AM (https://localhost/post/1451)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 3
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Note to self: do a release soon before losing your mind ✨

Aug 22, 2019, 7:38 PM (https://localhost/post/1452)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 2
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Dammit, I hate leaving empty functions behind to pick up later, what did I originally plan to do in here 😅

```
210 //
211 // Timed auto-reset of filter driver
212 //
213 void BthPS3_EnablePatchEvtWdfTimer(
214     WDFTIMER Timer
215 )
216 {
217     UNREFERENCED_PARAMETER(Timer);
218
219     TraceEvents(TRACE_LEVEL_VERBOSE, TRACE_DEVICE,
220         "IRQL %!irql! too high, preparing async call",
221         KeGetCurrentIrql()
222     );
223 }
224
225 void BthPS3_FilterRequestCompletionRoutine(
226     WDFREQUEST Request,
227     WDFIOTARGET Target,
228     PWDF_REQUEST_COMPLETION_PARAMS Params,
229     WDFCONTEXT Context
230 )
231 {
232
233 }
234
```

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/d6bf245a-254c-4038-ad27-3df3de67685e-image.png)

---

24 DAYS LATER

Sep 15, 2019, 11:24 PM (https://localhost/post/1482)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 2
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

I am still here. Have almost figured out literally everything, stay with me ☺️

Sep 19, 2019, 12:29 PM (https://localhost/post/1483)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

A

Areasis (https://localhost/user/areasis)
(https://localhost/user/areasis)

Exiting keep up the good work 😄👍

Sep 20, 2019, 1:52 AM (https://localhost/post/1484)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

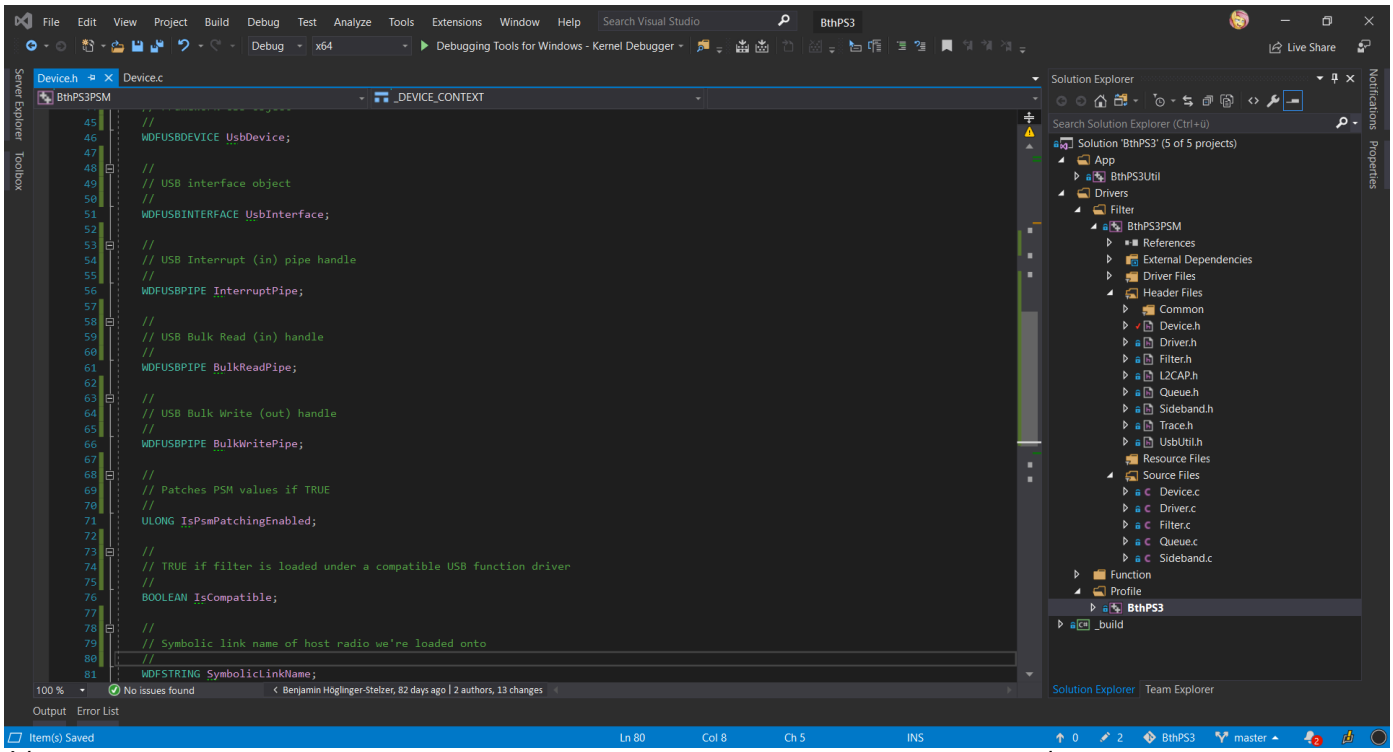
L Luke76bg (https://localhost/user/luke76bg)
(https://localhost/user/luke76bg)

I can't wait!!!! O_O

Sep 20, 2019, 12:14 PM (https://localhost/post/1485)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 2
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Back in business, warming up with some documentation. Also moved to GitHub since in the meantime they allow free private repositories 😃



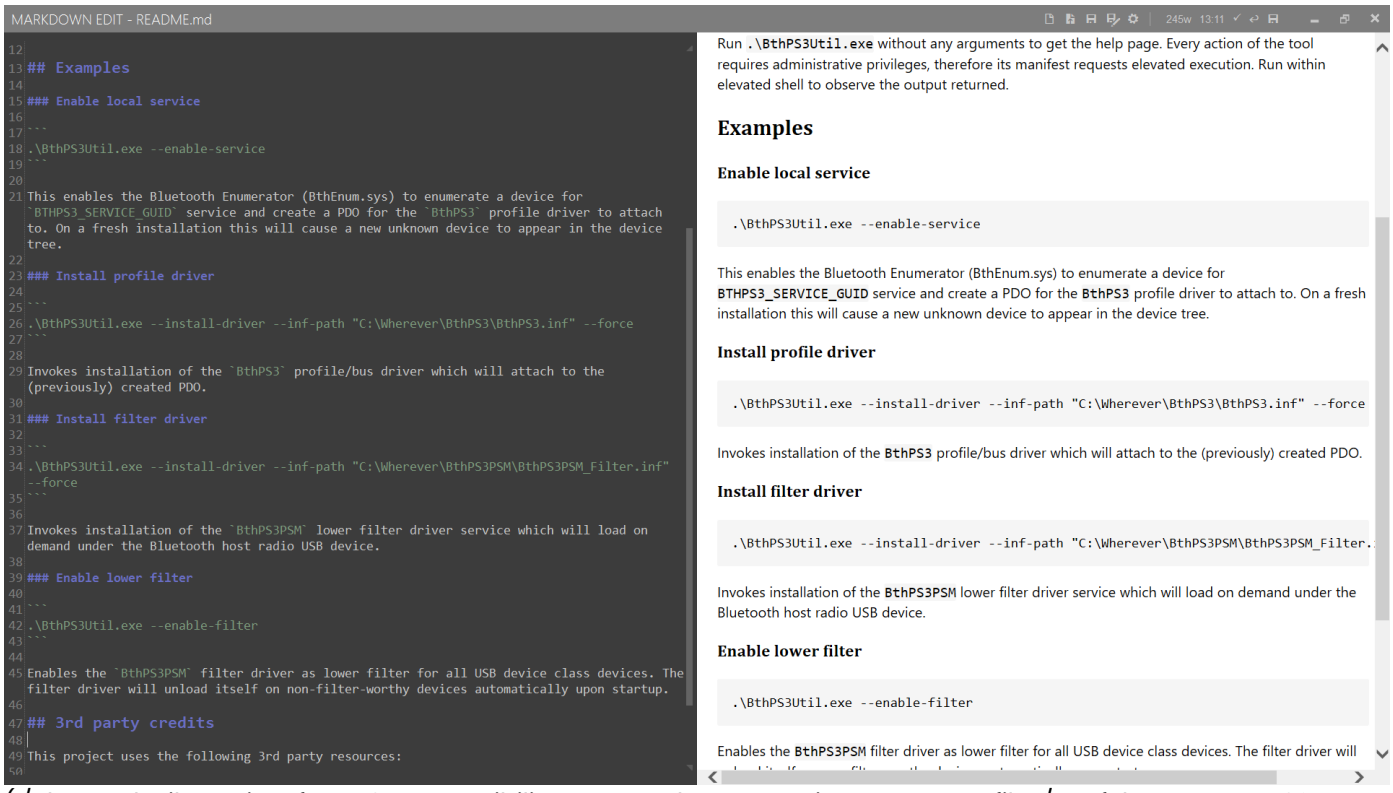
(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/3fcb055c-ca72-47a0-9005-0fcbc8c1fe3f-image.png)

Also upgraded to Visual Studio 2019 and WDK 10 1903, no biggie, but it's mature enough to use now in my taste 😉

Sep 20, 2019, 1:12 PM (https://localhost/post/1486)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Documentation has become equally important, this project got **huge** fast! 😲



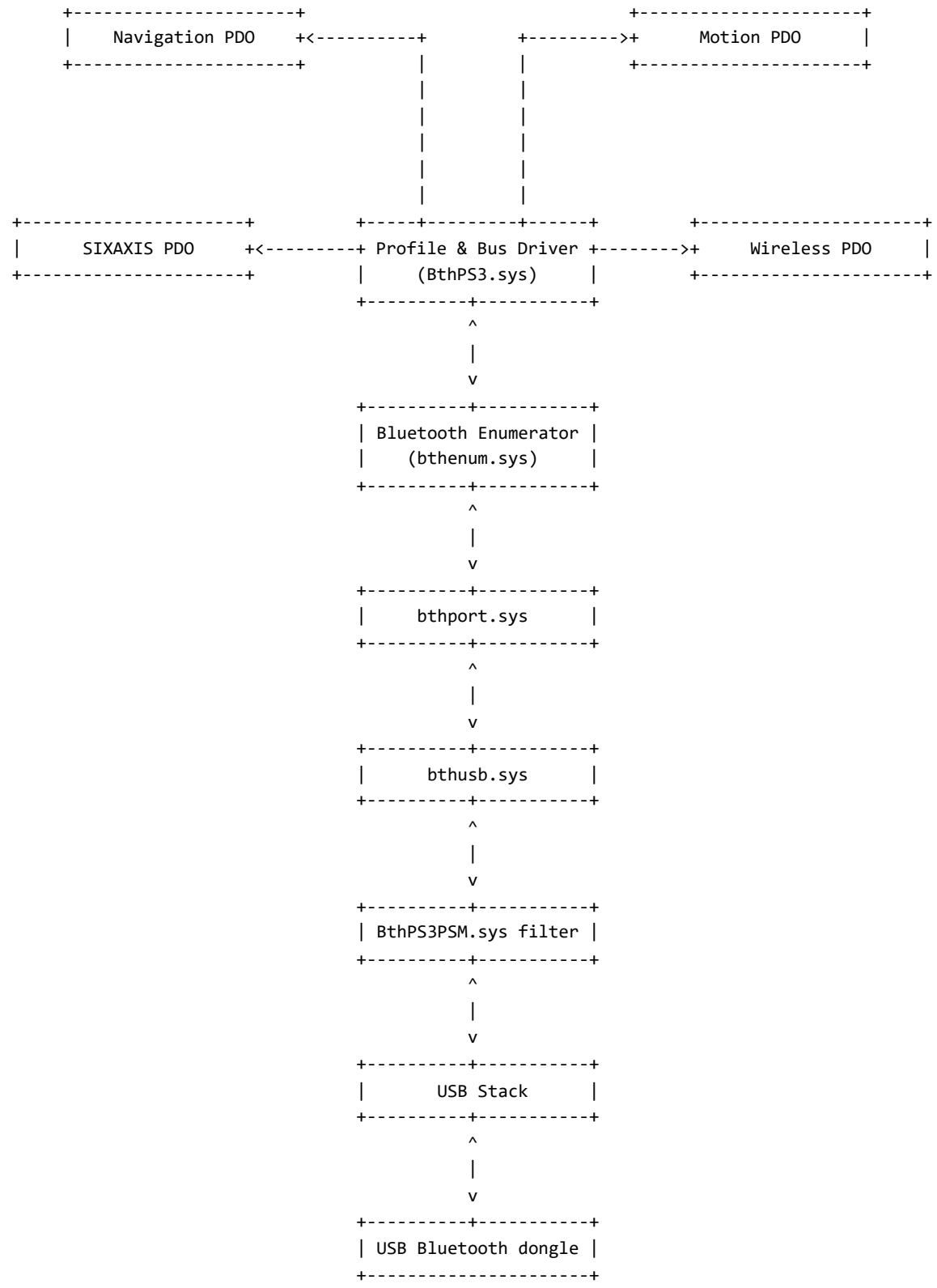
(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/c54fcbee-8140-4892-bfd2-3a349fe66c81-image.png)

Sep 20, 2019, 1:31 PM (https://localhost/post/1487)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 2
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Speaking of complexity; a bit of ASCII art I've come up with for this fun 😅

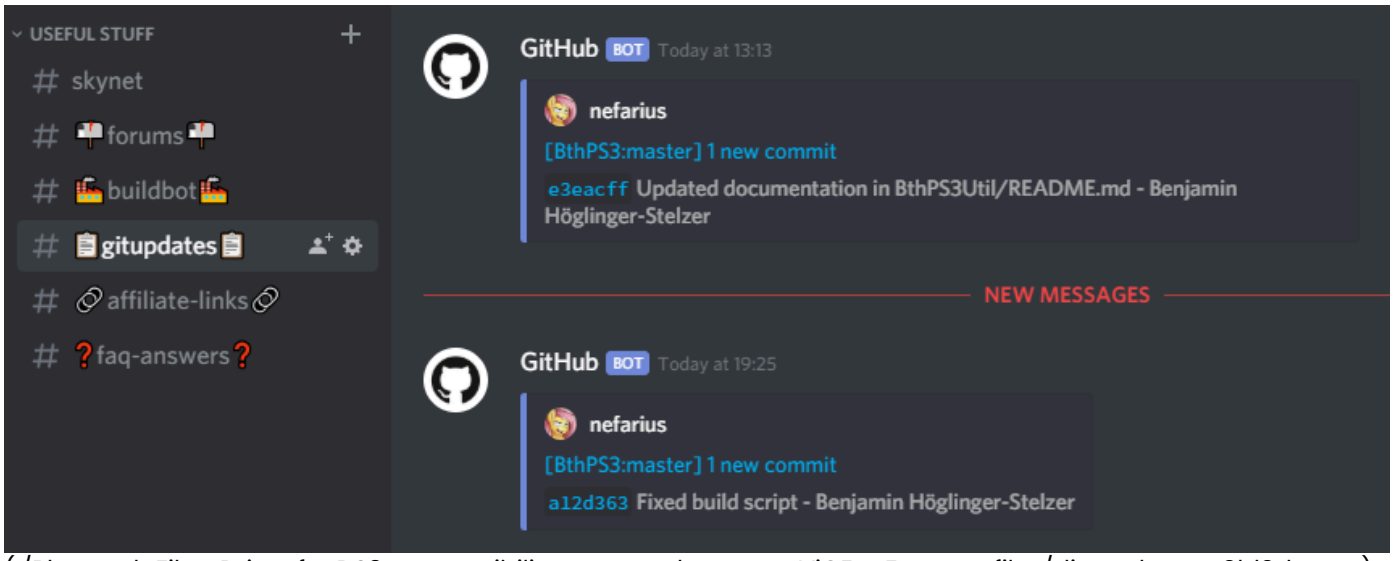
Device tree



Sep 20, 2019, 7:28 PM (https://localhost/post/1488)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 2 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

On the Discord server I've added a push notification for this projects repository, in case you wanna stalk my progression even more 😉

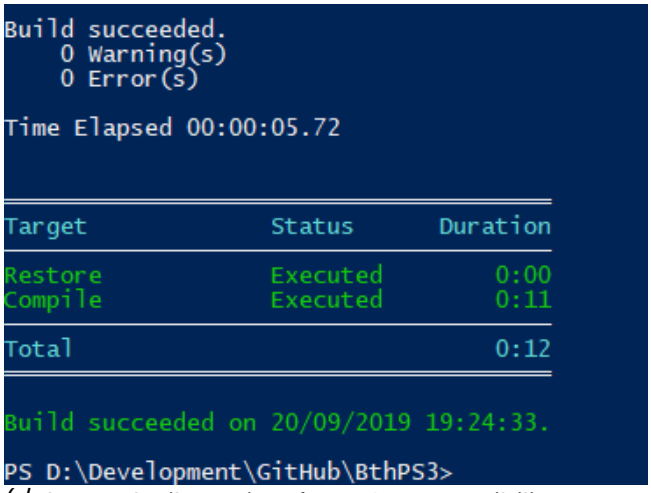


(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/discord_argp0ld0do.png)

Sep 20, 2019, 7:30 PM (https://localhost/post/1489)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Build script for future CI/CD fixed as well:



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/1be41d18-9697-4231-a582-aeef6a4d8e80-image.png)

Sep 21, 2019, 7:47 AM (https://localhost/post/1490)

 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

E epikvigem (https://localhost/user/epikvigem)
(https://localhost/user/epikvigem)

@nefarius (https://forums.vigem.org/uid/1) How can we join the Discord server?

Sep 21, 2019, 10:17 AM (https://localhost/post/1491)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

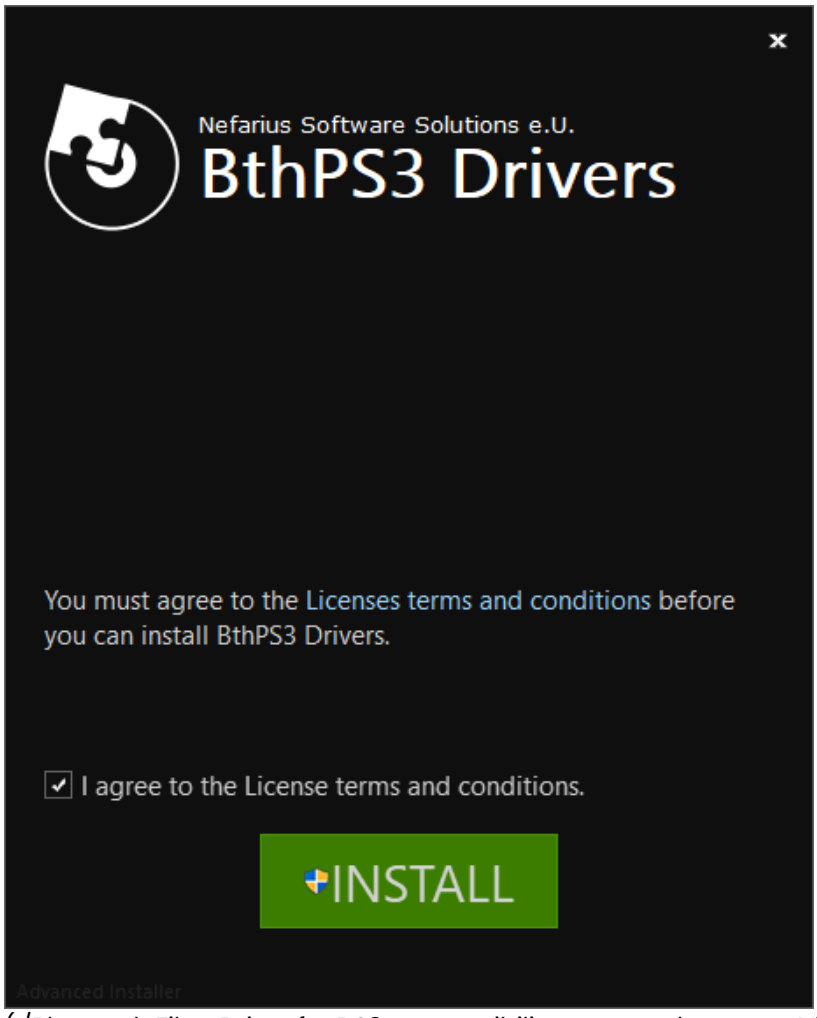
 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@epikvigem (https://forums.vigem.org/uid/155) it's that speech bubble symbol on top of the forums menu bar
🙂

Sep 21, 2019, 11:40 AM (https://localhost/post/1492)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Time to think about taking care of end-user convenience 😉

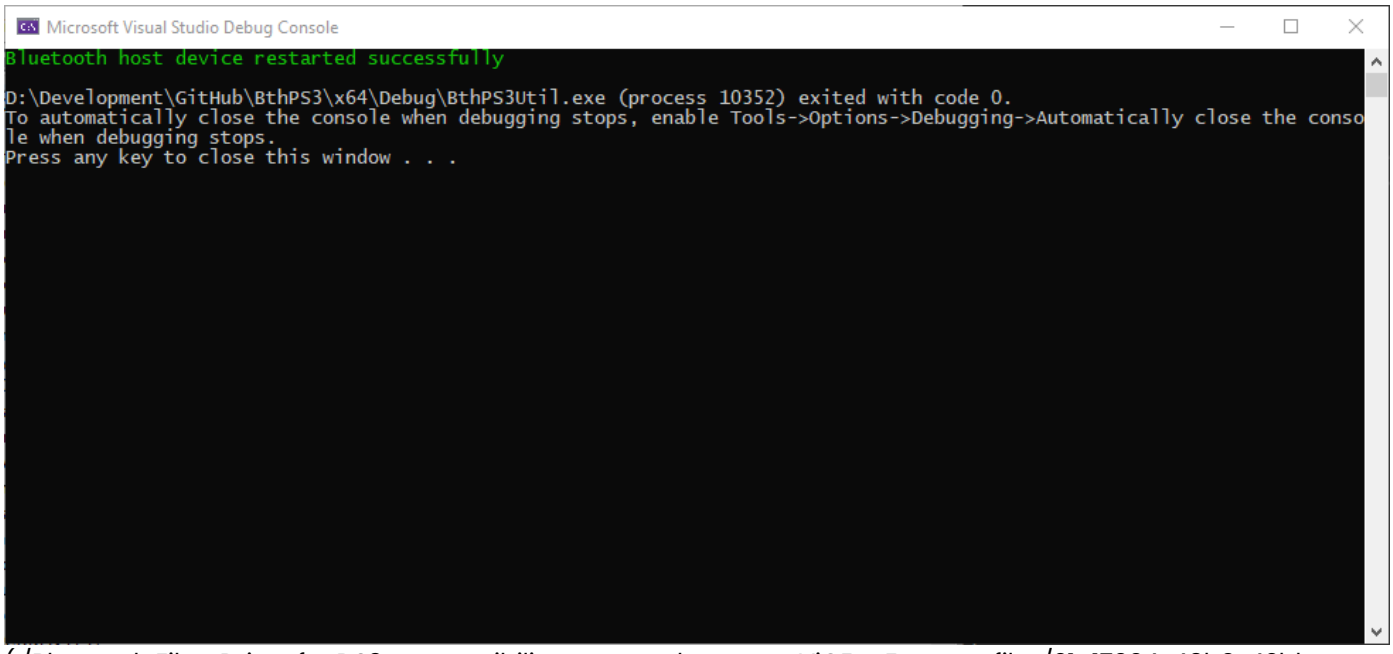


(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/e215108a-f016-4bd8-9280-ea071dc931e7-image.png)

Sep 22, 2019, 4:22 PM (https://localhost/post/1493)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

New feature of the utility I wanted for a long time: restarting the Bluetooth host without user interaction required 🙂

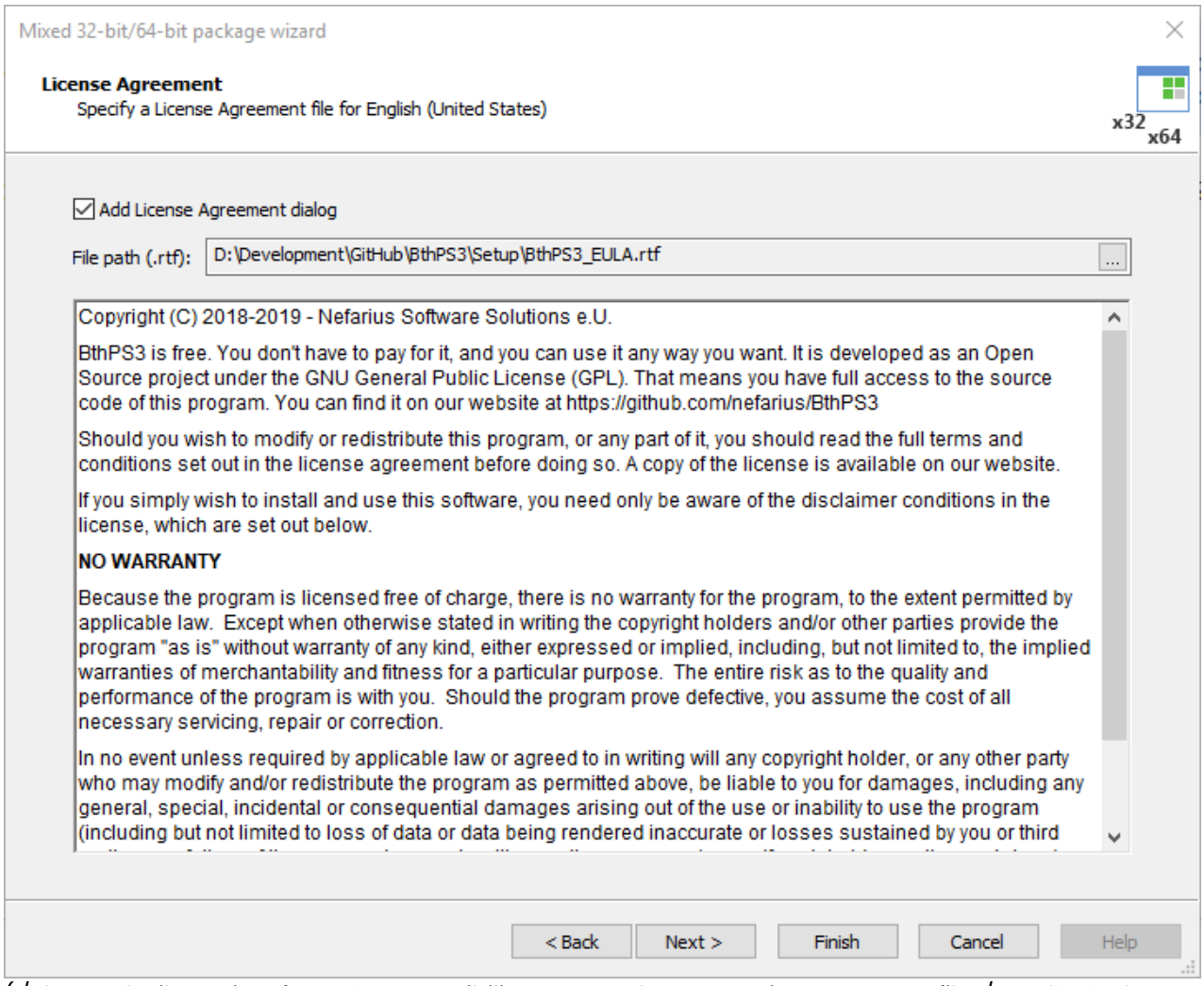


(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/21a17004-49b0-42bb-9f56-c0f64a19071d-image.png)

Sep 24, 2019, 4:14 PM (https://localhost/post/1494)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

I'm re-creating the setup, first design ate way too much time, need to simplify and script a bit. Still love Advanced Installer, best setup maker on the market 💕

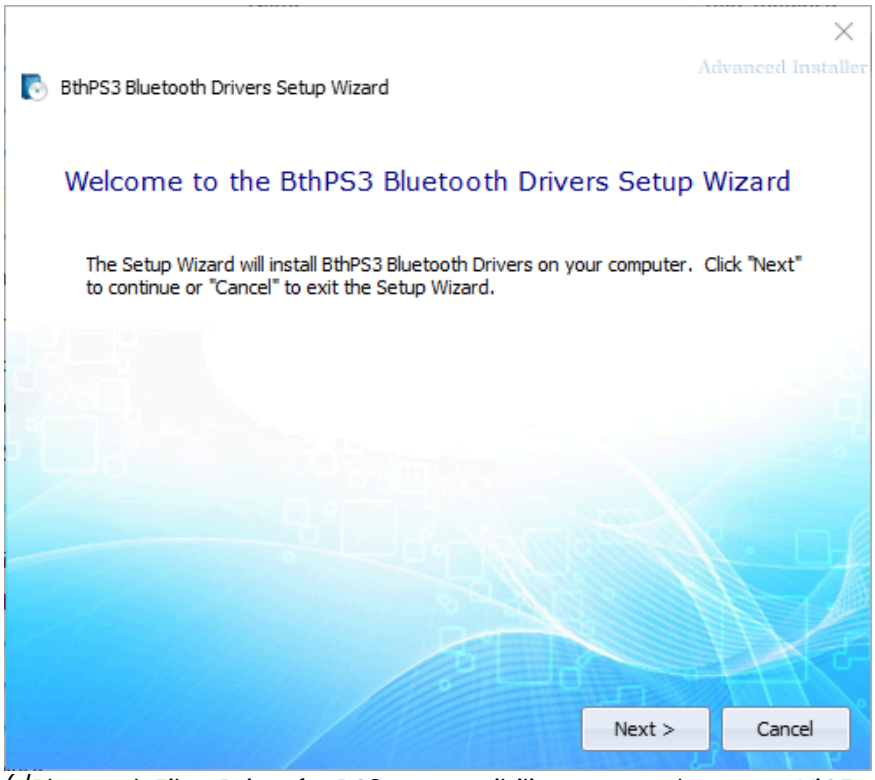


(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/a50d6c6c-bcae-4e0c-a5cf-8057cda3140f-image.png)

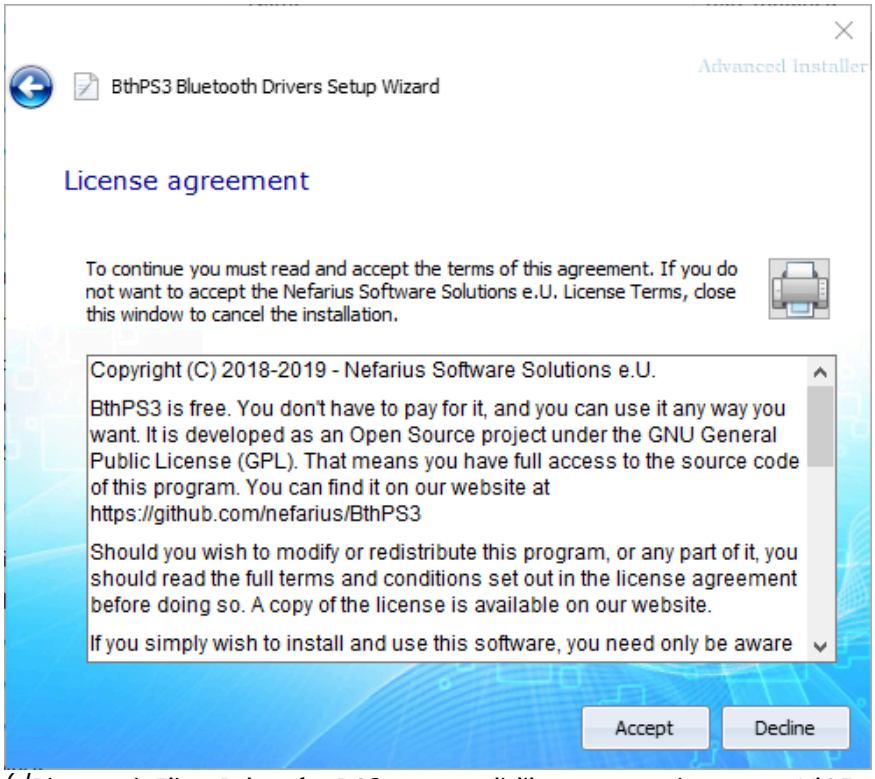
Sep 24, 2019, 4:22 PM (https://localhost/post/1495)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

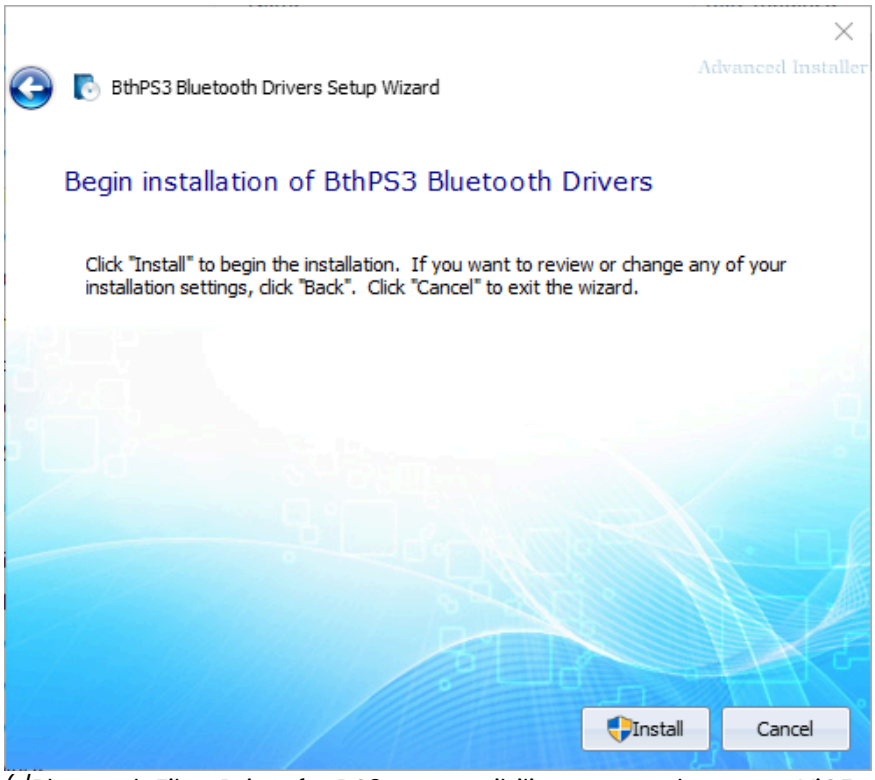
Shiny ✨



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/1caa527f-cab1-4609-ac1f-ebc69242fc34-image.png)



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/2ee1c4aa-2ddc-44c5-9908-576a787c10ea-image.png)

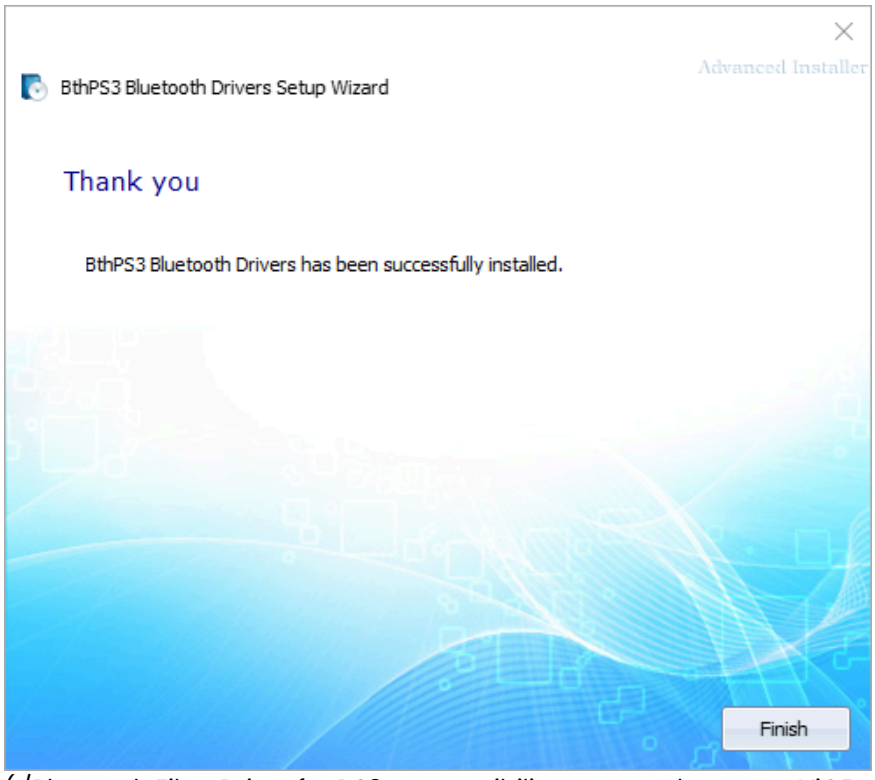


(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/f781b721-f722-4a53-9f43-48882aaf9fb7-image.png)

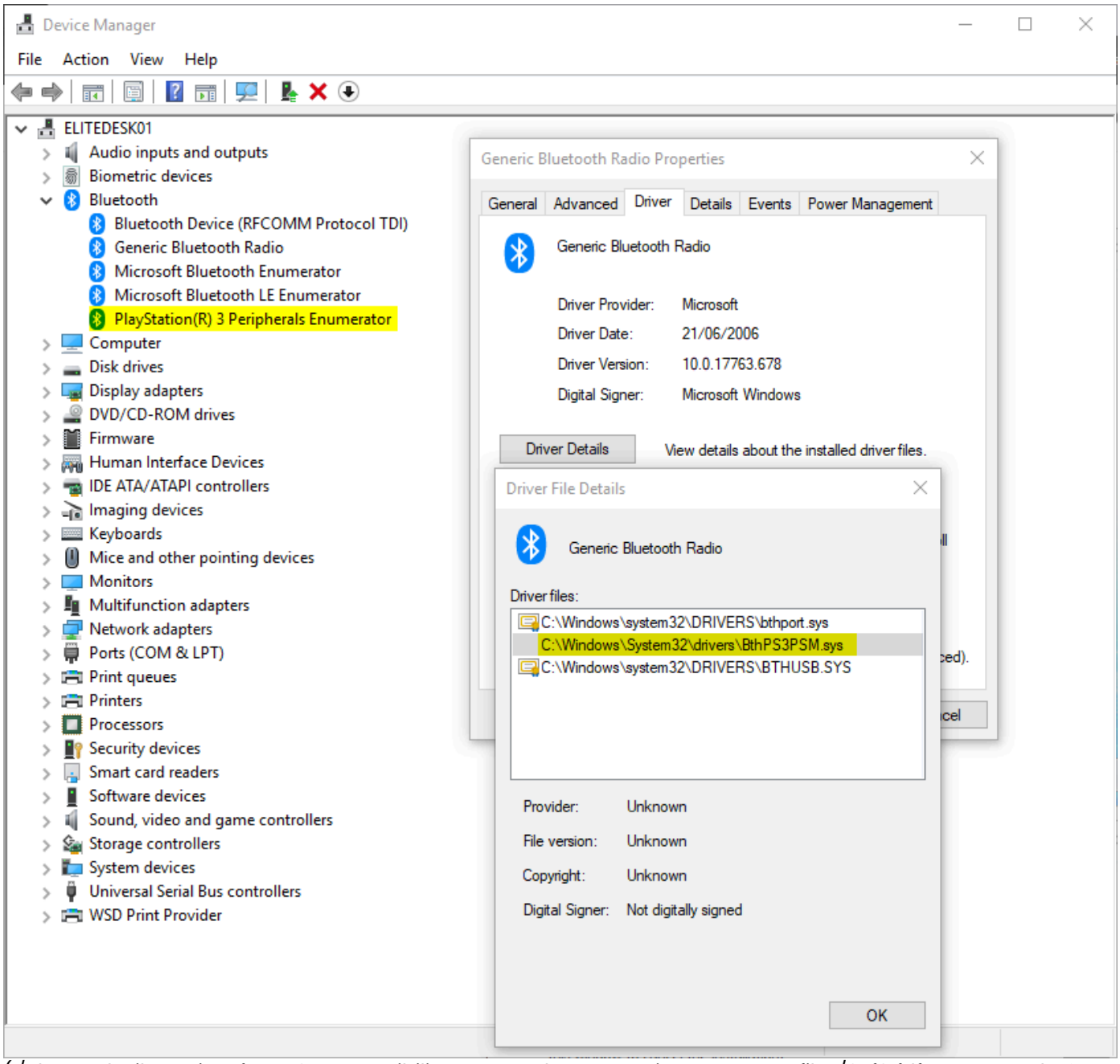
Sep 24, 2019, 4:24 PM (https://localhost/post/1496)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 3 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius) (https://localhost/user/nefarius)

Holy... and it did as promised! 😲



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/27469999-b9a0-4043-bf39-11b079a824e0-image.png)



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/3cf61fdf-ae11-47ce-be2c-210f36d22acf-image.png)

Big step!

Sep 26, 2019, 2:31 AM (https://localhost/post/1497)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

L Luke76bg (https://localhost/user/luke76bg)
(https://localhost/user/luke76bg)

@nefarius (https://forums.vigem.org/uid/1) Can i ask why it says DS3 ? It will support DS4 out of the box, right ?

(i can't access to your discord channel, it says "invalid invitation" 😞

Sep 26, 2019, 12:55 PM (https://localhost/post/1498)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

T techana (https://localhost/user/techana)
(https://localhost/user/techana)

Wow, what an adventure. You've done pretty well 👍 I'm looking forward to install your driver to my son's pc 🙂

Sep 26, 2019, 7:30 PM (https://localhost/post/1499)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@Luke76bg (https://forums.vigem.org/uid/219) because the whole project's main purpose is getting the PS3 peripherals to work. The different DS4 models already work out of the box in various ways wired and wireless on Windows and don't need any of this. Yes, I included compatibility nonetheless as an additional feature but it's not necessary so why include it in the name. Plus naming drivers sucks 😛

Edit: just tested the link, works fine on my end... (https://discord.vigem.org/) 🤔

Sep 28, 2019, 1:42 AM (https://localhost/post/1502)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

L Luke76bg (https://localhost/user/luke76bg)
(https://localhost/user/luke76bg)

@nefarius (https://forums.vigem.org/uid/1) Well i'm using your old scpi toolkit because the other solutions i couldn't get them to work if i have to be honest, your old driver works really good except for some bugs (i have to connect two times my ds4 because the first time it's not really connected, i have to shut it off, and then when i press again the central button, it's connected to the dongle! However your old driver don't have a button mapping tool, autofire, and touchpad and central button can't be used in games, so that's why i'm waiting your solution so badly! Thanks for your answer, i'm so glad you added ds4 compatibility!!! ^^

I'm in your discord now, yesterday wasn't working, i don't know why!

Wait...your driver is not released yet, right ?

Sep 28, 2019, 7:49 AM (https://localhost/post/1503)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@Luke76bg (https://forums.vigem.org/uid/219) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1502):

> Wait...your driver is not released yet, right ?

That is correct. And button mapping and other stuff you mentioned isn't part of this, this covers the age old issue of having to replace the vanilla stock drivers for Bluetooth like under SCP. Controller data manipulation is a whole different topic. Achievable, yes, but not part of this thread 🙂

Sep 28, 2019, 3:38 PM (https://localhost/post/1504)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

G
GregM (https://localhost/user/gregm)
(https://localhost/user/gregm)

@nefarius (https://forums.vigem.org/uid/1) There is Hori Onyx PS4 controller, that work with PS4 by BT only, without support for Windows (not detect as HID device after BT pairing, no drivers). Is there a chance, that will be worked with BthPS3?

Sep 28, 2019, 3:48 PM (https://localhost/post/1505)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

A
Atreides (https://localhost/user/atreides)
(https://localhost/user/atreides)

Do you intend to release it soon ? If not, why don't you release beta version to public ?

Sep 28, 2019, 9:20 PM (https://localhost/post/1506)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@GregM (https://forums.vigem.org/uid/590) no idea, don't know said device, subject to experimentation 😛

May work though if protocol compliant.

Sep 28, 2019, 9:22 PM (https://localhost/post/1507)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@Atreides (https://forums.vigem.org/uid/550) I release it when I feel like it's stable and production ready. Since my name and reputation will be attached to it I won't release some beta garbage potentially crashing your machine. When and why? When it's done 😛 guess I'll still make it in the upcoming month but I have other priorities as well.

Sep 28, 2019, 10:37 PM (https://localhost/post/1508)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

G

GregM (https://localhost/user/gregm)
(https://localhost/user/gregm)

@nefarius (https://forums.vigem.org/uid/1) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1506):

> @GregM (https://forums.vigem.org/uid/590) no idea, don't know said device, subject to experimentation 😛
>
> May work though if protocol compliant.

The driver will work for every device with protocol compliant, or for specific device IDs?

Sep 28, 2019, 10:46 PM (https://localhost/post/1509)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@GregM (https://forums.vigem.org/uid/590) for every device mimicking the classic remote names used by Sony in the firmware and using the same protocol as the PS3/4.

Sep 29, 2019, 10:59 AM (https://localhost/post/1510)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

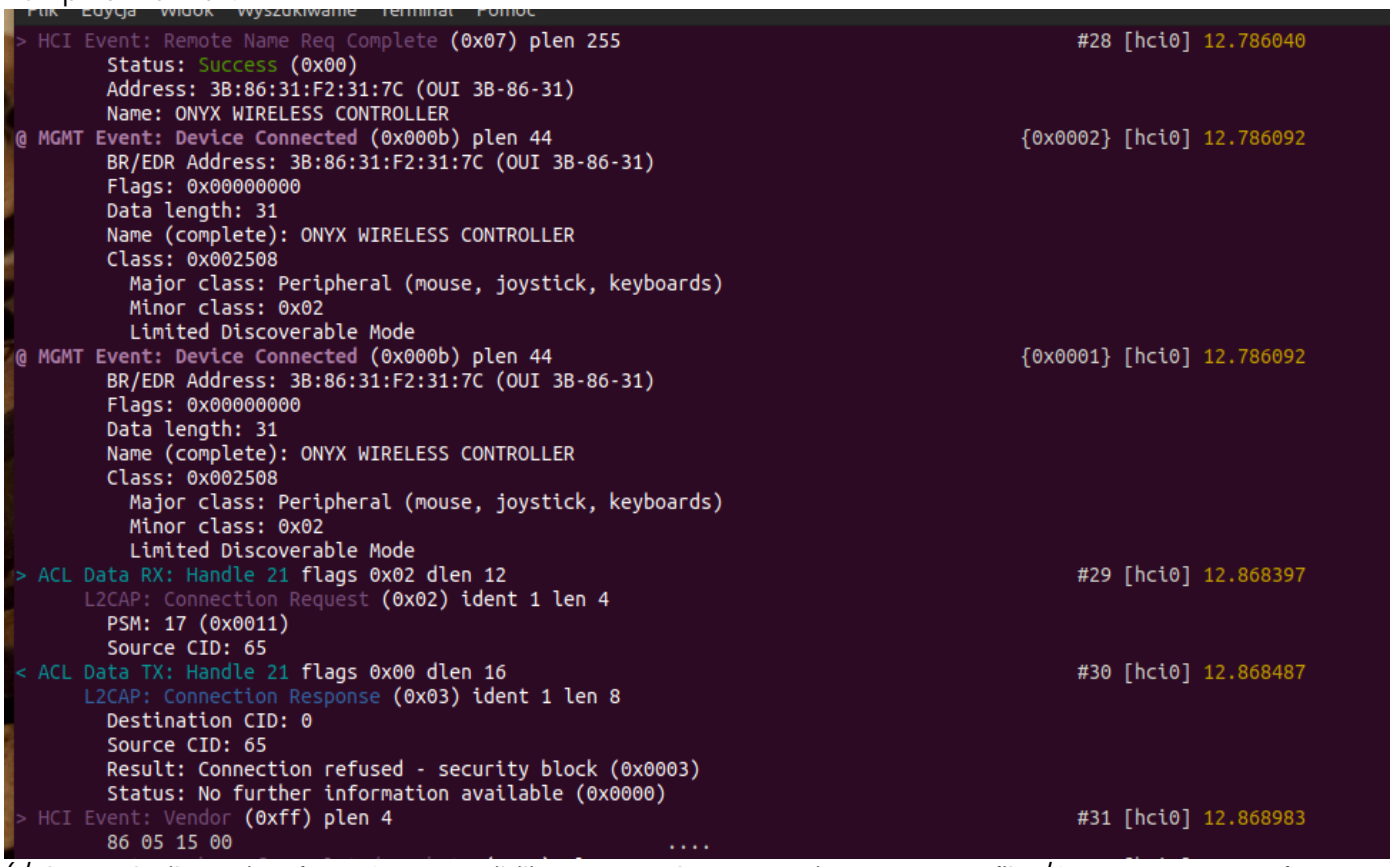
GregM (https://localhost/user/gregm)
(https://localhost/user/gregm)

@nefarius (https://forums.vigem.org/uid/1) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1509):

> @GregM (https://forums.vigem.org/uid/590) for every device mimicking the classic remote names used by Sony in the firmware and using the same protocol as the PS3/4.

The name is ONYX WIRELESS CONTROLLER, followed by PSM 0x11. So, if this name will be ok for the filter, then may work.

Dump from btmon:



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/9c2e7872-5eca-41fe-ac6c-22071e9b1172-obraz.png)

Sep 29, 2019, 11:38 AM (https://localhost/post/1511)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@GregM (https://forums.vigem.org/uid/590) you just raised a feature request: configurable name match 😆
you delayed release, congraz 😄

Sep 29, 2019, 11:49 AM (https://localhost/post/1512)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

GregM (https://localhost/user/gregm)
(https://localhost/user/gregm)

@nefarius (https://forums.vigem.org/uid/1) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1511):

> @GregM (https://forums.vigem.org/uid/590) you just raised a feature request: configurable name match 😆 you delayed release, congraz 😁

Oh, no 🙂

The configurable name match is very good idea (better than static name set) 👍

Sep 29, 2019, 12:01 PM (https://localhost/post/1513)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@GregM (https://forums.vigem.org/uid/590) yep, I'm convinced. That's a good idea and contributes to the flexibility to cover such cases as yours. Shouldn't take too much code to implement.

Sep 29, 2019, 3:15 PM (https://localhost/post/1518)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

GregM (https://localhost/user/gregm)
(https://localhost/user/gregm)

@nefarius (https://forums.vigem.org/uid/1) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1513):

> @GregM (https://forums.vigem.org/uid/590) yep, I'm convinced. That's a good idea and contributes to the flexibility to cover such cases as yours. Shouldn't take too much code to implement.

I can test beta with this feature implemented on Onyx PS4.

Sep 29, 2019, 5:31 PM (https://localhost/post/1519)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@GregM (https://forums.vigem.org/uid/590) that would be fabulous, I recommend hopping on our Discord for more responsive exchanges.

Sep 29, 2019, 7:44 PM (https://localhost/post/1520)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

G

GregM (https://localhost/user/gregm)
(https://localhost/user/gregm)

@nefarius (https://forums.vigem.org/uid/1) said in Bluetooth Filter Driver for DS3-compatibility - research notes (https://localhost/post/1519):

> @GregM (https://forums.vigem.org/uid/590) that would be fabulous, I recommend hopping on our Discord for more responsive exchanges.

Ok, I'm in 🙂

Oct 4, 2019, 6:34 AM (https://localhost/post/1530)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

L

Luke76bg (https://localhost/user/luke76bg)
(https://localhost/user/luke76bg)

@nefarius (https://forums.vigem.org/uid/1) ok i get it ,no problem at all, i just hope that the touch pad will be usable as a button in ds4!

Oct 5, 2019, 3:49 PM (https://localhost/post/1531)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 2
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Auto-reset filter implemented

And there we have it 🎉 it's now configurable if the DualShock **4** should be supported in PS4 mode and if turned off, the filter will be automatically disabled for a certain amount of seconds which allows the DS4 to re-connect in PC mode and then the filter patch will be enabled again automatically 😇

Profile log

```
2019/10/05-15:41:46.795 TRACE_LEVEL_VERBOSE     BthPS3_IndicationCallback Entry
2019/10/05-15:41:46.795 TRACE_LEVEL_INFORMATION New connection for PSM 0x5053 from ACFD93095C20 arrived
2019/10/05-15:41:46.795 TRACE_LEVEL_VERBOSE     IRQL DPC (0x02) too high, preparing async call
2019/10/05-15:41:46.795 TRACE_LEVEL_VERBOSE     BthPS3_IndicationCallback Exit
2019/10/05-15:41:46.795 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnectAsync Entry
2019/10/05-15:41:46.795 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnect Entry
2019/10/05-15:41:46.795 TRACE_LEVEL_VERBOSE     ClientConnections_RetrieveByBthAddr Entry
2019/10/05-15:41:46.795 TRACE_LEVEL_VERBOSE     ClientConnections_RetrieveByBthAddr Exit (STATUS_NOT_FOUND
(0xC0000225))
2019/10/05-15:41:46.795 TRACE_LEVEL_INFORMATION ++ Device ACFD93095C20 name: Wireless Controller
2019/10/05-15:41:46.795 TRACE_LEVEL_INFORMATION Filter disabled, re-enabling in 10 seconds
2019/10/05-15:41:46.795 TRACE_LEVEL_VERBOSE     L2CAP_PS3_DenyRemoteConnect Entry
2019/10/05-15:41:46.796 TRACE_LEVEL_VERBOSE     L2CAP_PS3_DenyRemoteConnectCompleted Entry (STATUS_SUCCESS
(0x00000000))
2019/10/05-15:41:46.796 TRACE_LEVEL_VERBOSE     L2CAP_PS3_DenyRemoteConnectCompleted Exit
2019/10/05-15:41:46.796 TRACE_LEVEL_VERBOSE     L2CAP_PS3_DenyRemoteConnect Exit
2019/10/05-15:41:46.796 TRACE_LEVEL_VERBOSE     L2CAP_PS3_HandleRemoteConnectAsync Exit
2019/10/05-15:41:56.796 TRACE_LEVEL_VERBOSE     BthPS3_EnablePatchEvtWdfTimer called, requesting filter to e
nable patch
2019/10/05-15:41:56.796 TRACE_LEVEL_ERROR       PSM Filter enable request finished with status STATUS_SUCCES
S (0x00000000)
```

Filter log

```
2019/10/05-15:41:46.795 TRACE_LEVEL_VERBOSE     >> Connection request for HID Control PSM 0x0011 arrived
2019/10/05-15:41:46.795 TRACE_LEVEL_INFORMATION ++ Patching HID Control PSM to 0x5053
2019/10/05-15:41:46.795 TRACE_LEVEL_VERBOSE     >> Bulk IN transfer (PipeHandle: FFFF9A0572BD6320)
2019/10/05-15:41:46.795 TRACE_LEVEL_VERBOSE     UrbFunctionBulkInTransferCompleted Exit
2019/10/05-15:41:46.795 TRACE_LEVEL_INFORMATION BthPS3PSM_SidebandIoDeviceControl Entry
2019/10/05-15:41:46.795 TRACE_LEVEL_VERBOSE     PSM patch disabled for device 0
2019/10/05-15:41:46.795 TRACE_LEVEL_INFORMATION BthPS3PSM_SidebandIoDeviceControl Exit
2019/10/05-15:41:49.079 TRACE_LEVEL_VERBOSE     UrbFunctionBulkInTransferCompleted Entry
2019/10/05-15:41:49.079 TRACE_LEVEL_VERBOSE     UrbFunctionBulkInTransferCompleted Exit
2019/10/05-15:41:49.080 TRACE_LEVEL_VERBOSE     UrbFunctionBulkInTransferCompleted Entry
2019/10/05-15:41:49.080 TRACE_LEVEL_VERBOSE     UrbFunctionBulkInTransferCompleted Exit
2019/10/05-15:41:49.080 TRACE_LEVEL_VERBOSE     UrbFunctionBulkInTransferCompleted Entry
2019/10/05-15:41:49.080 TRACE_LEVEL_VERBOSE     UrbFunctionBulkInTransferCompleted Exit
2019/10/05-15:41:56.796 TRACE_LEVEL_INFORMATION BthPS3PSM_SidebandIoDeviceControl Entry
2019/10/05-15:41:56.796 TRACE_LEVEL_VERBOSE     PSM patch enabled for device 0
2019/10/05-15:41:56.796 TRACE_LEVEL_INFORMATION BthPS3PSM_SidebandIoDeviceControl Exit
```

Next step: reading supported device names from registry as well.

Oct 5, 2019, 11:33 PM (https://localhost/post/1532)

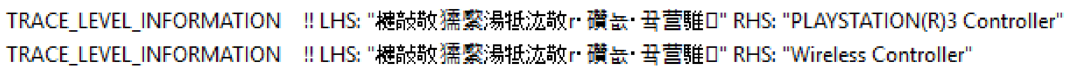
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


(https://localhost/user/nefarius) nefarius (https://localhost/user/nefarius)

Ugh, I feel so dirty. Let's see if this works nonetheless though...

```
#include <ntstrsafe.h>

BOOLEAN
StringUtil_BthNameIsEqual(
    CHAR Lhs,
    WDFSTRING Rhs
)
{
    UNICODE_STRING usRhs;
    DECLARE_UNICODE_STRING_SIZE(usLhs, BTH_MAX_NAME_SIZE);

    //
    // WDFSTRING to UNICODE_STRING
    //
    WdfStringGetUnicodeString(
        Rhs,
        &usRhs
    );

    //
    // CHAR to UNICODE_STRING
    //
    RtlUnicodeStringPrintf(&usLhs, L"%s", Lhs);

    //
    // Compare case-insensitive
    //
    return RtlEqualUnicodeString(&usLhs, &usRhs, TRUE);
}
```

EDIT: nope, not that easy 🤣


TRACE_LEVEL_INFORMATION !! LHS: "楗敲敬獳䌠湯牴汯敬r· [illegible]" RHS: "PLAYSTATION(R)3 Controller"
TRACE_LEVEL_INFORMATION !! LHS: "楗敲敬獳䌠湯牴汯敬r· [illegible]" RHS: "Wireless Controller"

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/2f7dfbb1-2b4e-4284-b75c-c6f157d7c4a3-image.png)

Oct 6, 2019, 1:22 PM (https://localhost/post/1533)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


(https://localhost/user/nefarius) nefarius (https://localhost/user/nefarius)

Welp, fixed... `%s` ain't `%hs` 😖

```
BOOLEAN
StringUtil_BthNameIsEqual(
    PCHAR Lhs,
    WDFSTRING Rhs
)
{
    NTSTATUS status;
    UNICODE_STRING usRhs;
    DECLARE_UNICODE_STRING_SIZE(usLhs, BTH_MAX_NAME_SIZE);

    //
    // WDFSTRING to UNICODE_STRING
    //
    WdfStringGetUnicodeString(
        Rhs,
        &usRhs
    );

    //
    // CHAR to UNICODE_STRING
    //
    status = RtlUnicodeStringPrintf(&usLhs, L"%hs", Lhs);
    if (!NT_SUCCESS(status)) {
        TraceEvents(TRACE_LEVEL_INFORMATION,
            TRACE_UTIL,
            "RtlUnicodeStringPrintf failed with status %!STATUS!",
            status
        );
    }

    TraceEvents(TRACE_LEVEL_INFORMATION,
        TRACE_UTIL,
        "!! LHS: \"%wZ\" RHS: \"%wZ\"",
        &usLhs, &usRhs
    );

    //
    // Compare case-insensitive
    //
    return RtlEqualUnicodeString(&usLhs, &usRhs, TRUE);
}
```

Result:

```
2019/10/06-13:20:31.438 TRACE_LEVEL_INFORMATION !! LHS: "Wireless Controller" RHS: "PLAYSTATION(R)3 Controll
er"
2019/10/06-13:20:31.438 TRACE_LEVEL_INFORMATION !! LHS: "Wireless Controller" RHS: "Wireless Controller1"
2019/10/06-13:20:31.438 TRACE_LEVEL_WARNING     !! Device ACFD93095C20 not identified or denied, dropping co
nnection
```

Oct 7, 2019, 3:57 PM (https://localhost/post/1534)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 2
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

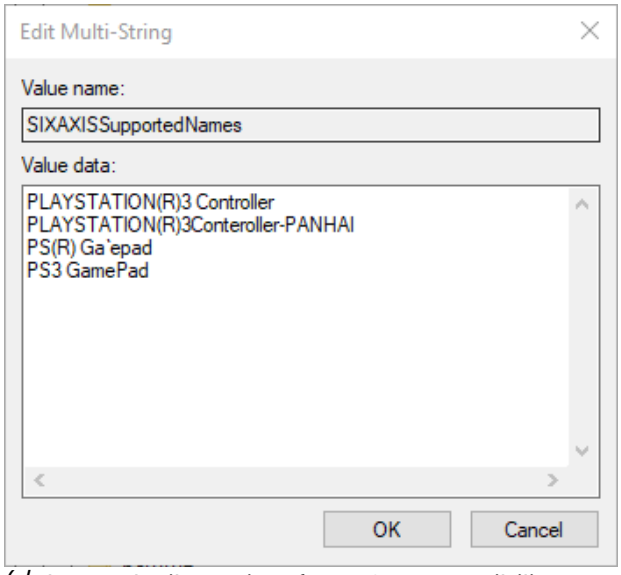
nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

All features implemented, the closed beta team is currently testing the latest changes 🙂

Oct 7, 2019, 8:06 PM (https://localhost/post/1535)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 2
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Aftermarket compatibility established 😄



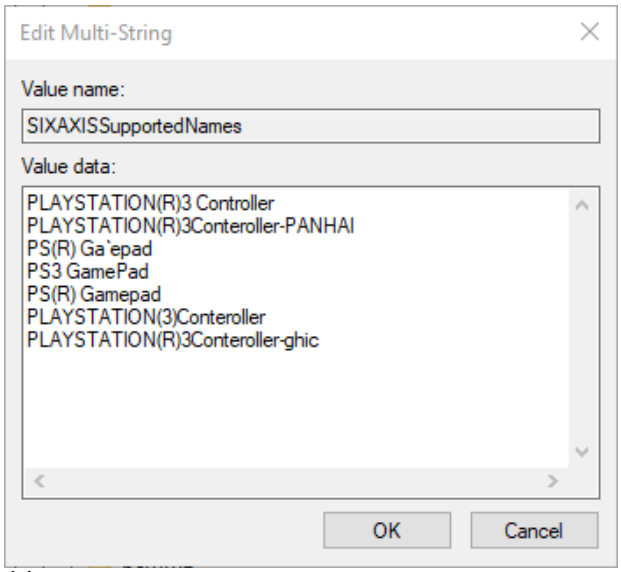
(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/08beadda-ab3e-489c-a86d-ed963b8c319e-image.png)

```
2019/10/07-20:04:47.624 TRACE_LEVEL_INFORMATION ++ Device 00F570996325 name: PLAYSTATION(R)3Conteroller-PANH
AI
2019/10/07-20:04:47.624 TRACE_LEVEL_VERBOSE     StringUtil_BthNameIsEqual LHS: "PLAYSTATION(R)3Conteroller-P
ANHAI" RHS: "PLAYSTATION(R)3 Controller"
2019/10/07-20:04:47.624 TRACE_LEVEL_VERBOSE     StringUtil_BthNameIsEqual LHS: "PLAYSTATION(R)3Conteroller-P
ANHAI" RHS: "PLAYSTATION(R)3Conteroller-PANHAI"
2019/10/07-20:04:47.624 TRACE_LEVEL_INFORMATION ++ Device 00F570996325 identified as SIXAXIS compatible
```

Oct 7, 2019, 8:16 PM (https://localhost/post/1536)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

I dug up more, thanks to the archive of ScpToolkit issues 🤣



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/af3fc049-7c31-443e-813f-c18795738a3a-image.png)

Oct 7, 2019, 8:33 PM (https://localhost/post/1537)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 2
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Navigation and Motion controllers connect as well. But mine are low on battery, so let's let them plugged in over night 😅

Oct 10, 2019, 4:57 AM (https://localhost/post/1538)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

L Luke76bg (https://localhost/user/luke76bg)
(https://localhost/user/luke76bg)

Amazing progress! i can't wait!!!

---

8 DAYS LATER

Oct 18, 2019, 12:18 AM (https://localhost/post/1542)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Pairing devices to BthPS3

Useful link collection for later 😃

- How to find Bluetooth MAC Address in Windows (https://macaddresschanger.com/how-to-find-bluetooth-mac-address-windows)
- SIXAXISPAIRTOOL (http://dancingpixelstudios.com/sixaxis-controller/sixaxispairtool/)

Far more comfortable than SCP or going through FireShock 😇

Oct 19, 2019, 3:15 AM (https://localhost/post/1544)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

L
Luke76bg (https://localhost/user/luke76bg)
(https://localhost/user/luke76bg)

@nefarius (https://forums.vigem.org/uid/1) I have only one dual shock pad for my pc, already paired, this tool it's useful for pairing new pads ?

Oct 19, 2019, 6:03 PM (https://localhost/post/1545)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 2
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@Luke76bg (https://forums.vigem.org/uid/219) yep. Once paired it ain't needed anymore but it's easier to use (IMHO) than what you need to go through with Shibari and PowerShell. The tool is unfortunately closed source but has a wide audience (Android users) so I'd assume it's just freeware doing what it promises. I don't have the resources currently to provide something of similar value.

Oct 21, 2019, 9:57 PM (https://localhost/post/1546)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 2
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

A
anontsuki (https://localhost/user/anontsuki)
(https://localhost/user/anontsuki)

Hopefully that close beta testing is going well, can't wait to finally put SCP away and use this alongside other peripherals! ^_^

Oct 26, 2019, 7:47 PM (https://localhost/post/1552)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@anontsuki (https://forums.vigem.org/uid/395) It's going very well. Unfortunately due to work and health-related issues I need to shift down a few gears and take it easy for the rest of October. So stable production release expected in November I'd say 😑

Oct 27, 2019, 6:40 AM (https://localhost/post/1553)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

A

anontsuki (https://localhost/user/anontsuki)
(https://localhost/user/anontsuki)

@nefarius (https://forums.vigem.org/uid/1) That's okies! You keep it up and keep yourself all in good order! 😃

November isn't far at all.

Oct 29, 2019, 9:08 PM (https://localhost/post/1562)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Trying to sign currently... 💣

Product Name	Submission Status	Submission Created Date ↓
BthPS3	Ready	10/29/2019
BthPS3	Processing	10/29/2019
BthPS3	Processing	10/29/2019
BthPS3	Failed	10/29/2019

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/88e9b45e-2a96-4c00-

9550-fa60360247cf-image.png)

So far every submission has been rejected because the CAB format wasn't correct... FML 💢

Oct 30, 2019, 3:22 PM (https://localhost/post/1567)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

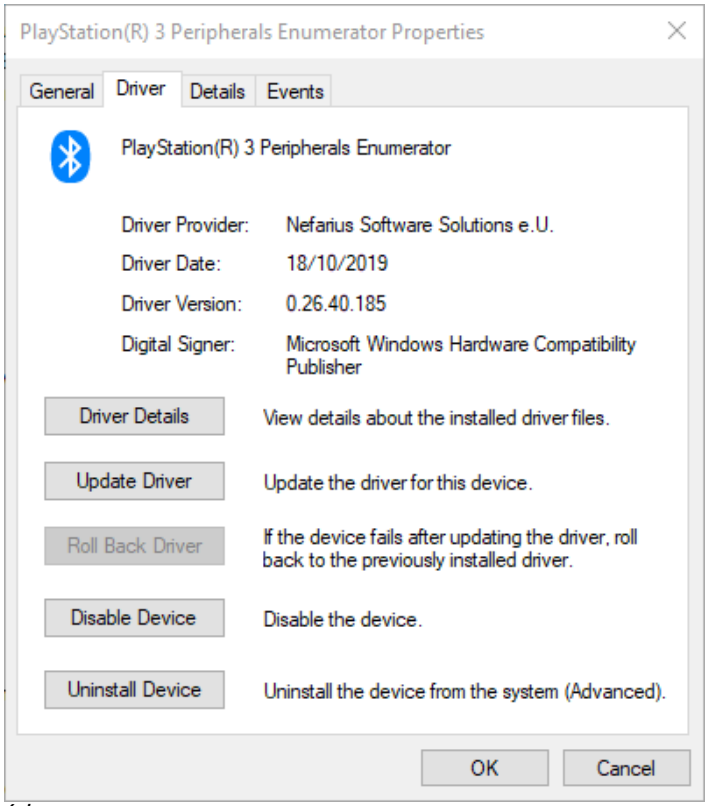
A (https://localhost/user/anontsuki) anontsuki (https://localhost/user/anontsuki)

@nefarius (https://forums.vigem.org/uid/1) 😯 Something special it needs to be?

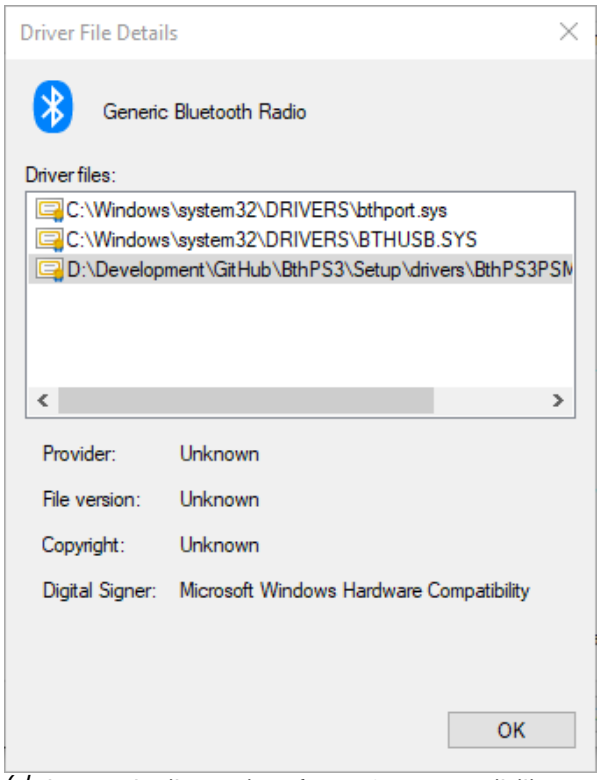
Oct 30, 2019, 4:20 PM (https://localhost/post/1568)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 3
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 (https://localhost/user/nefarius) nefarius (https://localhost/user/nefarius)

Ha! Gotcha!



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/9ea09b9b-922c-4543-b3aa-360fe78bd31f-image.png)



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/4be904d9-1fa3-40f0-9f8c-822274612aad-image.png)

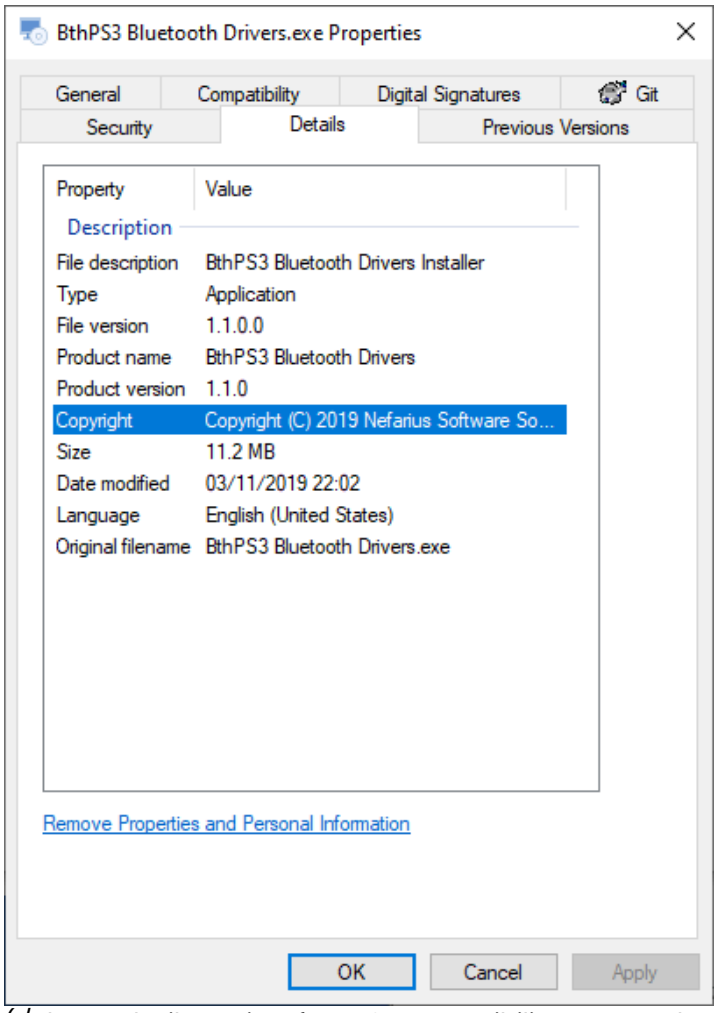
Building those submission CAB files feels like ancient magic once you haven't done it for a couple of months but I got it

---

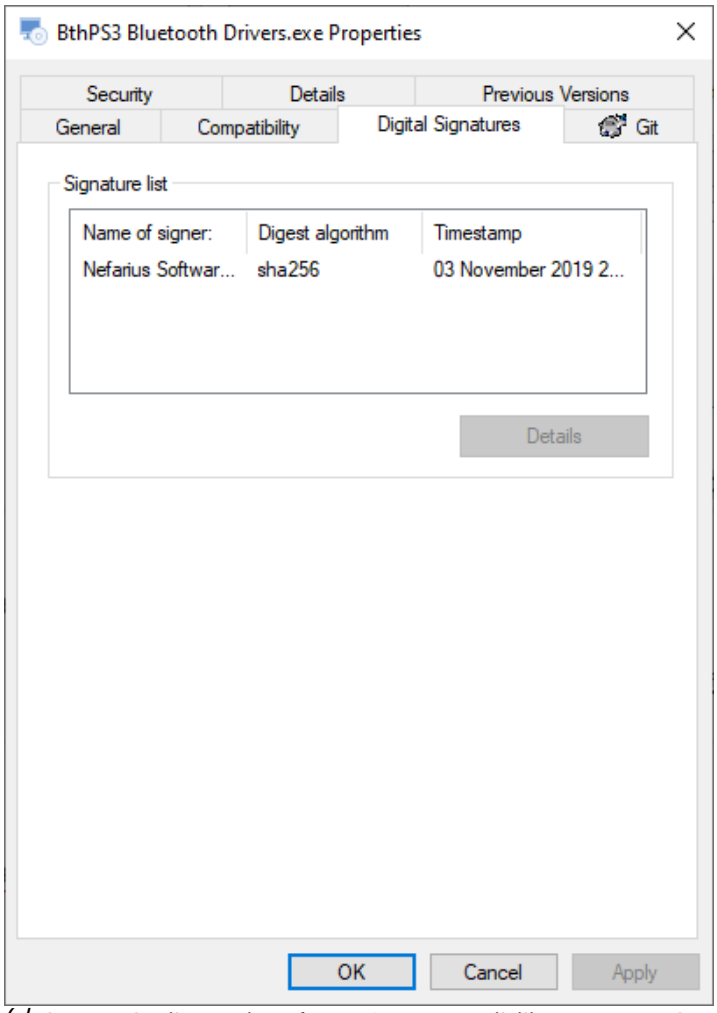
Nov 3, 2019, 10:03 PM (https://localhost/post/1574)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 3
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Almost there



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/7a2e5587-2624-44fa-94a6-392764c15786-image.png)



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/b2c015b7-3fba-4e07-9397-79d8d6a618d7-image.png)

Nov 4, 2019, 8:36 PM (https://localhost/post/1580)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 3 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius) (https://localhost/user/nefarius)

Hehehe 😇

Name	Publisher	Installed On	Size	Version
Microsoft Visual C++ 2008 Redistributable - x64 9.0.3...	Microsoft Corporation	15/10/2019	13.2 MB	9.0.30729
Microsoft System CLR Types for SQL Server 2019 CTP...	Microsoft Corporation	16/10/2019	6.26 MB	15.0.1200.24
Microsoft Visual C++ 2008 Redistributable - x86 9.0.3...	Microsoft Corporation	15/10/2019	10.2 MB	9.0.30729
Microsoft SQL Server 2012 Express LocalDB	Microsoft Corporation	15/10/2019	162 MB	11.4.7001.0
Microsoft .NET Core SDK 3.0.100 (x64) from Visual Stu...	Microsoft Corporation	16/10/2019	164 KB	3.0.100.014277
Microsoft System CLR Types for SQL Server 2012 (x64)	Microsoft Corporation	15/10/2019	3.31 MB	11.4.7001.0
Microsoft Visual C++ 2010 x86 Redistributable - 10.0....	Microsoft Corporation	16/10/2019	11.1 MB	10.0.40219
Markdown Edit	Mike Ward	16/10/2019	188 MB	1.35.0
ViGEm Bus Driver	Nefarius Software Solutions e.U.	19/10/2019	4.35 MB	1.16.115
BthPS3 Bluetooth Drivers	Nefarius Software Solutions e.U.	04/11/2019	5.00 MB	1.1.1
Notepad++ (64-bit x64)	Notepad++ Team	16/10/2019	9.36 MB	7.7.1
NVIDIA Graphics Driver 441.08	NVIDIA Corporation	29/10/2019		441.08
NVIDIA GeForce Experience 3.20.0.118	NVIDIA Corporation	15/10/2019		3.20.0.118
NVIDIA PhysX System Software 9.19.0218	NVIDIA Corporation	15/10/2019		9.19.0218
NVIDIA HD Audio Driver 1.3.38.21	NVIDIA Corporation	29/10/2019		1.3.38.21
OBS Studio	OBS Project	16/10/2019		24.0.3
Macrium Reflect Home Edition	Paramount Software (UK) Ltd.	21/10/2019		7.2
Parsec	Parsec Cloud Inc.	15/10/2019		
AnyDesk	philandro Software GmbH	15/10/2019	2.00 MB	ad 5.3.3

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/c0f3e07b-e998-44d3-af38-a3b44d5bef53-image.png)

Nov 5, 2019, 12:05 AM (https://localhost/post/1581)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

A anontsuki (https://localhost/user/anontsuki)
(https://localhost/user/anontsuki)

Things are getting verrryyyy exciting! Yay 😃

Nov 8, 2019, 6:40 AM (https://localhost/post/1582)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 mbc07 (https://localhost/user/mbc07)
(https://localhost/user/mbc07)

Hey @nefarius (https://forums.vigem.org/uid/1) firstly I would like to thank you for all your hard work all over those years, as I can't ever recall for how long I've been using tools/drivers you've developed, mostly SCP Toolkit and ViGEm Bus Driver.

I just discovered this thread (and read it entirely) and knowing that a solution that allows communicating wirelessly with DualShock 3 controllers on Windows without needing to "sacrifice" an entire BT Adapter is already a possibility indeed is awesome! Your earlier posts, however, made me raise a question not entirely related to BthPS3, but I need to ask anyway.

I don't know if that behavior is exclusive to newer DualShock 4 controllers (CUH-ZCT2U) but if you connect them through USB Cable (or Bluetooth through Sony's Wireless USB Adapter), Windows will see the regular HID Input device and also an Audio device, which allow using whatever is attached to the DualShock 4 headphone jack out of the box, without any 3rd party drivers or apps, including the mic in case of a headset.

However, if you connect the DualShock 4 through Bluetooth, then only the HID Input device appears. Earlier on this thread, you said DualShock 4 controllers also try to communicate through PSMs 0x11 and 0x13 before being denied and settling on PSM 0x01. It's clearly out of the scope of BthPS3 driver but do you think that perhaps it would be possible to send/receive audio to/from the headphone jack and maybe to the internal controller speaker by communicating with the DualShock 4 through those reserved PSMs instead of the default "PC Mode" the controller falls back?

Audio obviously can work wirelessly as the PS4 itself does that and it also works on Windows if you're using Sony's Wireless USB Adapter, but I find curious how PS4 is nearing its end of life and DualShock 4 audio transmission through Bluetooth seems to remain unknown territory even after all those years...

---

16 DAYS LATER

Nov 23, 2019, 11:10 PM (https://localhost/post/1595)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

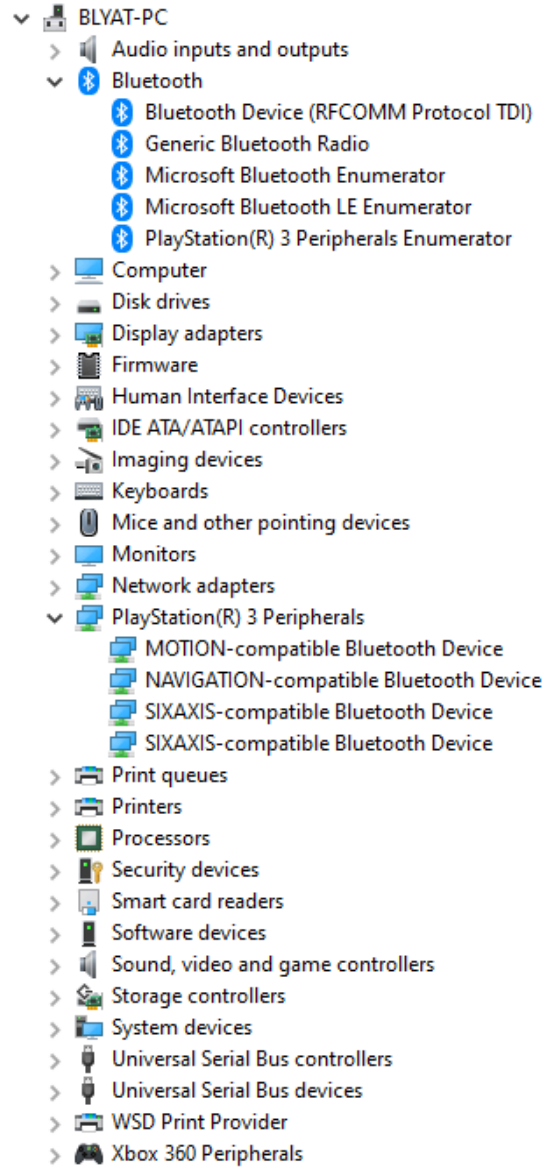
nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@mbc07 (https://forums.vigem.org/uid/704) pardon the delay, I've read your post. In short: I neither have the knowledge nor the capacity/equipment to tackle any audio-related topics regarding the DS4. The driver is modular enough though so future shenanigans may be added.

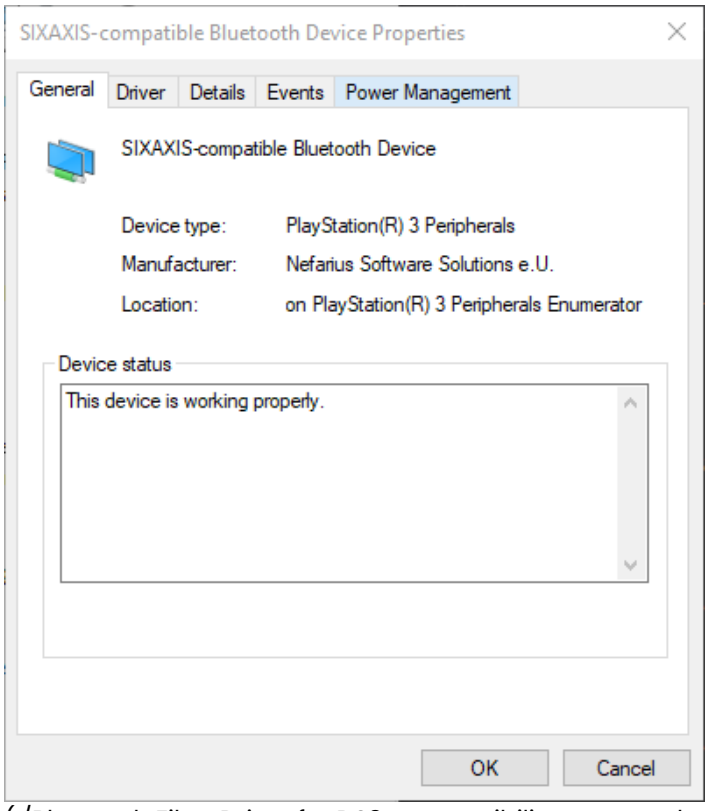
Nov 23, 2019, 11:14 PM (https://localhost/post/1596)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 2
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

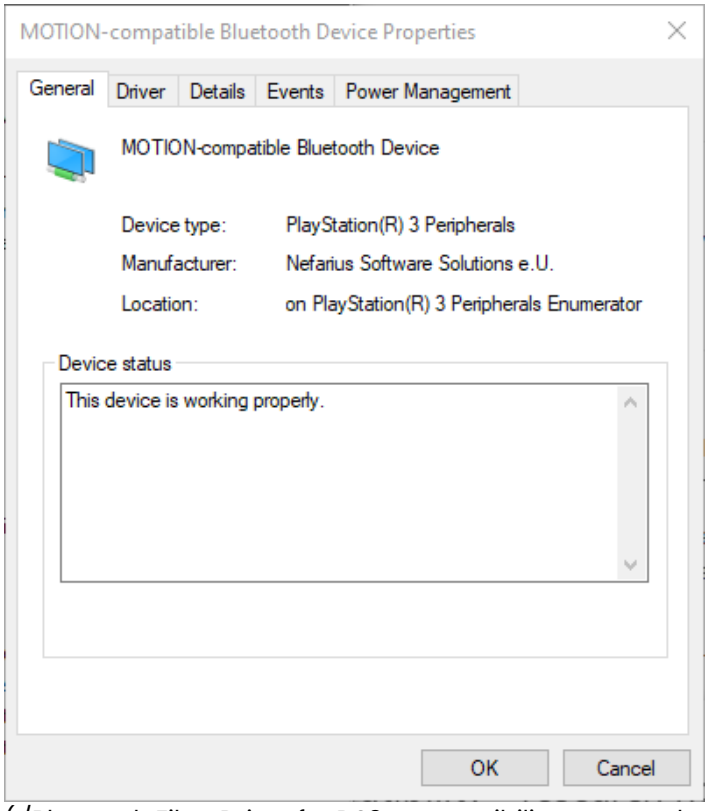
Some cosmetic improvements 😃 Created a NULL driver INF for the child devices:



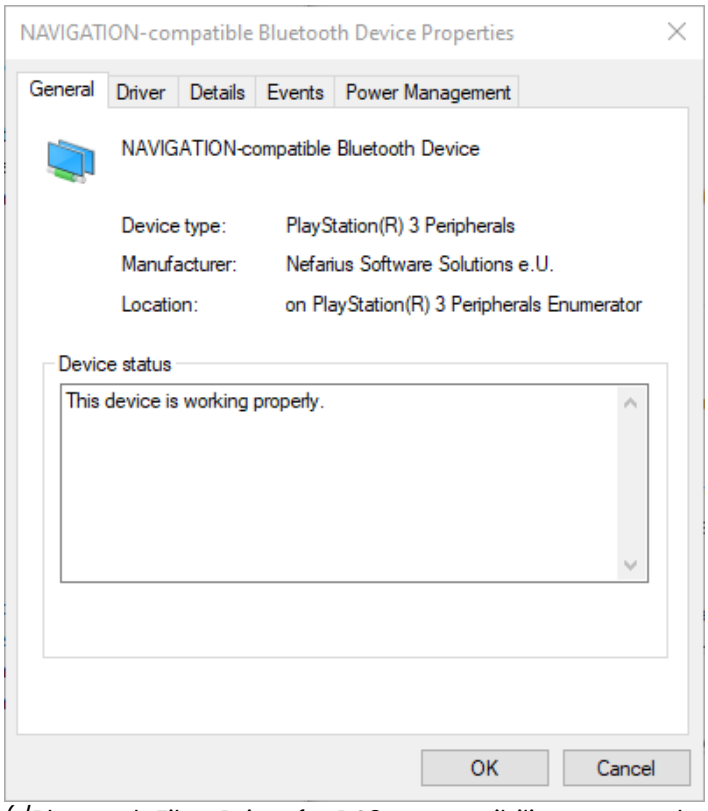
(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/3172fbb2-6842-4e74-a0d4-7cbefcaee198-image.png)



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/0a53b3c4-5e75-4183-98f1-164ce60252bb-image.png)



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/d7be0894-7e77-4524-a47f-3e91af494a4c-image.png)



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/eb4d519b-6085-4e12-b0e6-c215e0512e64-image.png)

Quite slick if I may say so 😏

I'm still polishing the release and haven't died yet, so no worries! 😜

Cheers

Nov 26, 2019, 8:45 PM (https://localhost/post/1600)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

We're pretty much feature-complete at this point 😇

BthPS3 x64 v1.1.0.0 26.11.2019

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/722b20ac-15c7-4ddc-b27f-68e98e57ff16-image.png)

BthPS3 x86 v1.1.0.0 26.11.2019

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/6c081594-92c9-4331-9ce9-8c2b8a3df467-image.png)

Setup works great, now need to prepare website and installation documentation. Stay tuned 📻

Nov 27, 2019, 9:16 AM (https://localhost/post/1601)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

L (https://localhost/user/locksmith) Locksmith (https://localhost/user/locksmith)

🎶 All I want for Christmas, is BthPS3 🎶😇😄

!ERAU QSSI DLRO WEHT

Nov 27, 2019, 12:33 PM (https://localhost/post/1604)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 (https://localhost/user/nefarius) nefarius (https://localhost/user/nefarius)

I've received a valid concern that the use of trademarked names like "PlayStation(R) 3" could raise unnecessary conflict so I decided to push yet another update removing those and put emphasis in the "not by Sony"-nature of the project 😉 Not my intention to step on anybody's feet and am not skilled enough in trademark laws and exceptions to take the risk.

Cheers

Nov 28, 2019, 7:44 PM (https://localhost/post/1605)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 (https://localhost/user/nefarius) nefarius (https://localhost/user/nefarius)

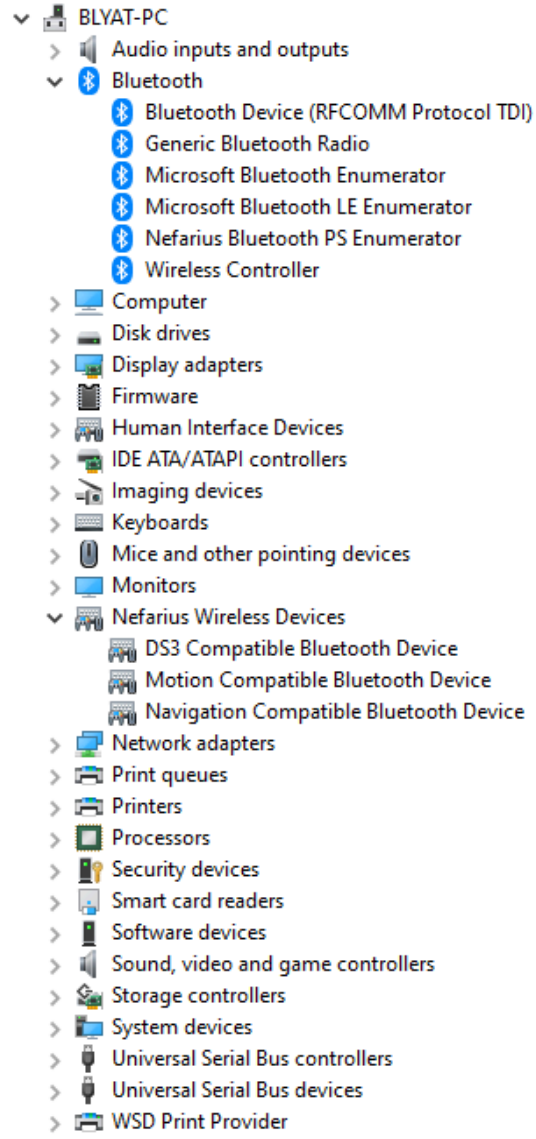
Stay tuned 😉


(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/65ffc789b05211faf1585083e2382c0b.gif)

Nov 28, 2019, 8:02 PM (https://localhost/post/1606)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 2
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

And here, ladies and gentlemen, we have all four device classes living together in harmony at last! 🎉



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/8c7abaf9-9d9a-4ba9-810b-d77cfab2419f-image.png)

(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/67914101-2540-4d8d-b52a-7e02ab61f054-image.png)

😁

Nov 29, 2019, 6:47 PM (https://localhost/post/1607)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

A (https://localhost/user/anontsuki) anontsuki (https://localhost/user/anontsuki)

@nefarius (https://forums.vigem.org/uid/1) Wohooo, I'm so excited! I just can't hide it! ^_^

This is great stuff!

Question, although you've changed the use of trademarked names, do the controllers still get picked up as a "PlayStation(R) 3" controller by whatever program and stuff or will they be seen as something else? (This doesn't matter, just curious).

Release imminent?

Nov 29, 2019, 6:54 PM (https://localhost/post/1608)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 3
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@anontsuki (https://forums.vigem.org/uid/395) for now it will either appear as an emulated X360 or DS4 controller, the name reported by the device - in this case - is totally artificial and up to how I as the driver respond.

Pretty close, like Christmas 😉

Nov 29, 2019, 10:06 PM (https://localhost/post/1609)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

A
anontsuki (https://localhost/user/anontsuki)
(https://localhost/user/anontsuki)

@nefarius (https://forums.vigem.org/uid/1) Oh okay, that's rather normal.

Dec 3, 2019, 12:04 PM (https://localhost/post/1611)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

C
capibov (https://localhost/user/capibov)
(https://localhost/user/capibov)

@nefarius (https://forums.vigem.org/uid/1) amazing work! I was wondering, is this the solution for using ds3 controllers with a cable as well or is SCP still the way to go?

Keep on rocking 🙂

Dec 3, 2019, 2:57 PM (https://localhost/post/1612)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@capibov (https://forums.vigem.org/uid/778) thanks! 😘 This project is a 100% focused on Bluetooth only, USB I might pick up again in the future if life allows it.

Cheers

Dec 3, 2019, 11:27 PM (https://localhost/post/1613)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

W weab-chan (https://localhost/user/weab-chan)
(https://localhost/user/weab-chan)

wait how do you pair the controller with the right bluetooth mac address then!?
I guess using shibari and fireshock?

Dec 4, 2019, 10:05 AM (https://localhost/post/1614)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

L Locksmith (https://localhost/user/locksmith)
(https://localhost/user/locksmith)

@weab-chan (https://forums.vigem.org/uid/417) having followed this thread, I believe the goal is for BthPS3 is to be self-contained and not need other tools.
@capibov (https://forums.vigem.org/uid/778) Shibari (https://forums.vigem.org/topic/259/shibari-installation-instructions) works fine with USB-connected controller. 🙂

!ERAU QSSI DLRO WEHT

Dec 4, 2019, 9:44 PM (https://localhost/post/1620)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

W weab-chan (https://localhost/user/weab-chan)
(https://localhost/user/weab-chan)

@Locksmith (https://forums.vigem.org/uid/138) shibari works fine without fireshock?! or i guess you still need fireshock

---

Dec 5, 2019, 9:16 AM (https://localhost/post/1621)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

L Locksmith (https://localhost/user/locksmith)
(https://localhost/user/locksmith)

@weab-chan (https://forums.vigem.org/uid/417) yeah I guess that's needed too... ^_^

!ERAU QSSI DLRO WEHT

Dec 6, 2019, 1:30 AM (https://localhost/post/1623)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

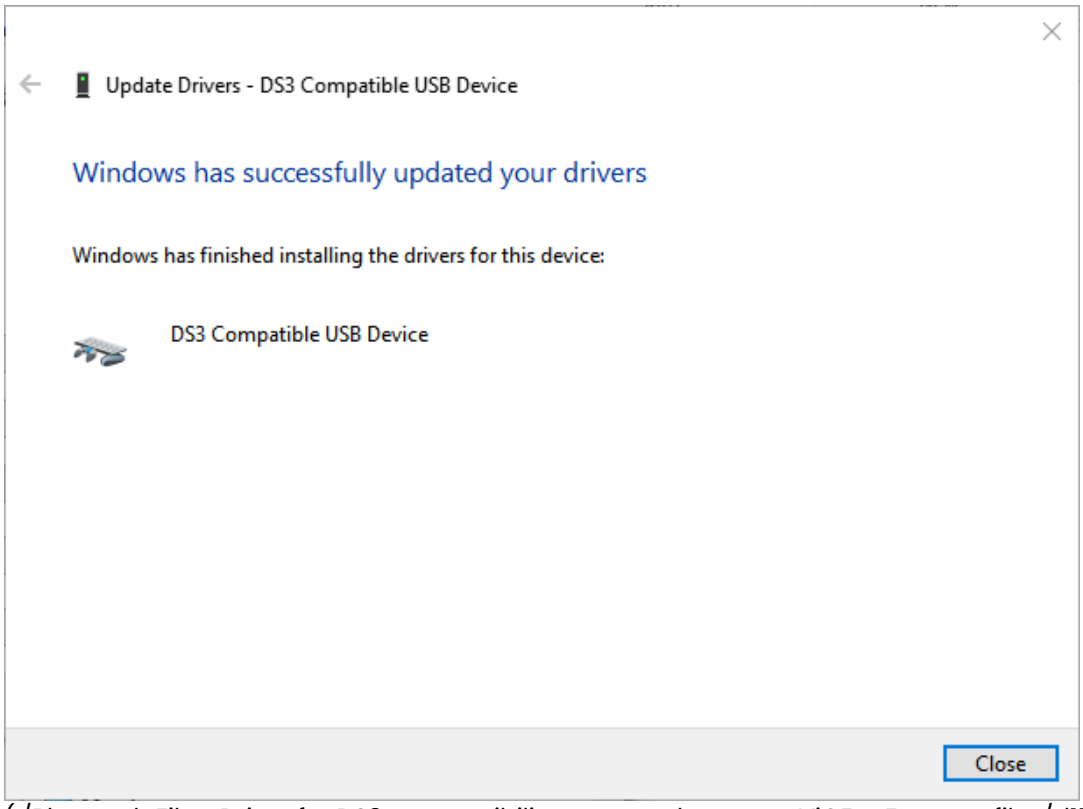
 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@weab-chan (https://forums.vigem.org/uid/417) that will be covered in the release documentation, please refrain from detouring this thread, thanks.

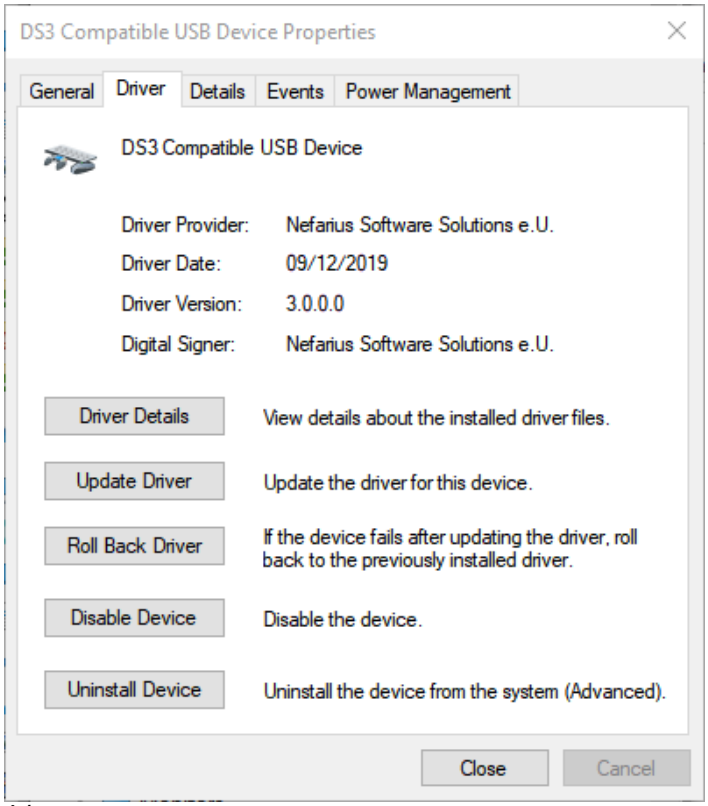
Dec 9, 2019, 7:12 PM (https://localhost/post/1638)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

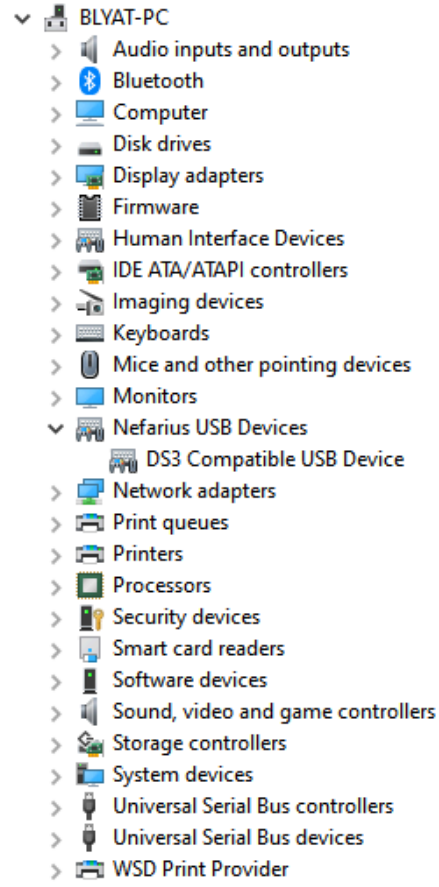
Well, I couldn't help myself, I had to touch, update and refine the USB side of things as well, because literally all available pairing tools (on Windows) are utter garbage 😅



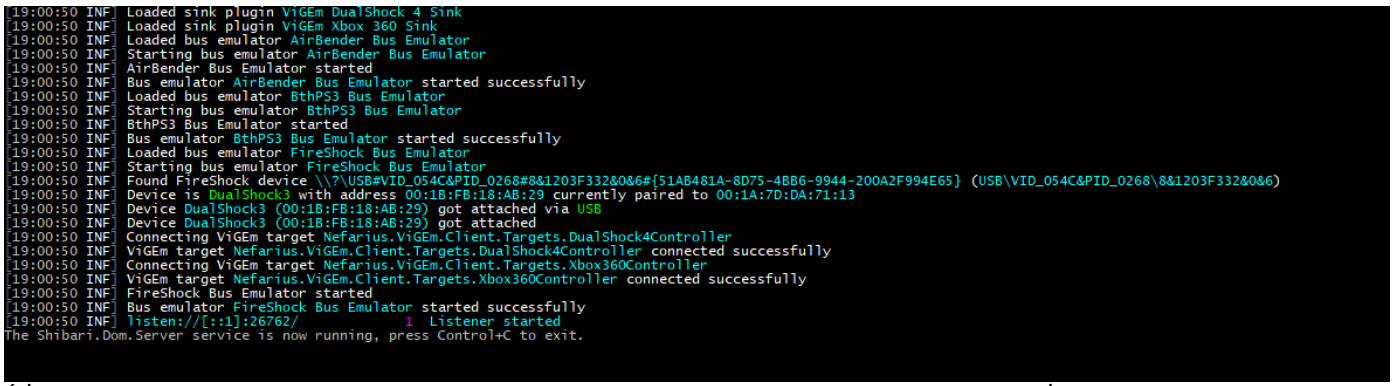
(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/d155dcf3-cc8d-467b-8cb1-80b3f048cba4-image.png)



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/47817ea0-291c-4fd1-8ffd-1c94570ded00-image.png)



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/7942df65-d458-405a-ba8b-75a8ef1b382a-image.png)



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/aac51b13-df37-4b0c-b5ca-4eb355872b47-image.png)

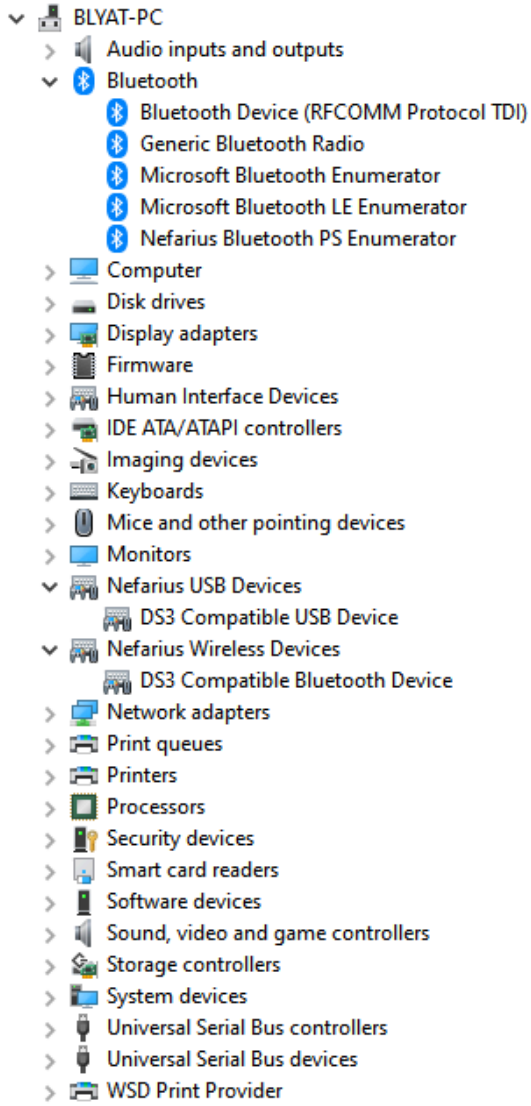
We're getting there...

Dec 9, 2019, 10:52 PM (https://localhost/post/1639)

(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Insane compilation noises



(./Bluetooth Filter Driver for DS3-compatibility - research notes _ ViGEm Forums_files/ca360c9e-33ec-4bbc-a2a8-6533a572b202-image.png)

Dec 9, 2019, 10:59 PM (https://localhost/post/1640)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

mbc07 (https://localhost/user/mbc07)
(https://localhost/user/mbc07)

Um, everything looks so good but... Is there any particular reason for "DS3 Compatible USB Device" and "DS3 Compatible Bluetooth Device" being on their own, separate categories on Device Manager? Why not just show them under the existing "Human Interface Devices" and call it a day?

Dec 9, 2019, 11:04 PM (https://localhost/post/1641)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@mbc07 (https://forums.vigem.org/uid/704) because they are not HID-compliant, therefore would just add to confusion 😎

Dec 10, 2019, 6:01 AM (https://localhost/post/1642)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

P

pnkiller78 (https://localhost/user/pnkiller78)
(https://localhost/user/pnkiller78)

Wow man... thanks a lot... BthPS3 is a dream come true...
I will make a small contribution to show my respect and support.
Thanks for this.

Dec 10, 2019, 11:07 AM (https://localhost/post/1643)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Release has gone live! Merry Whatever you celebrate!

I did a thingy, enjoy! (https://forums.vigem.org/projects/bthps3) 😄 Thanks to anybody following my journey and already donating, hugs and kisses 😘

I'll now vanish into winter vacation, cheers!

Dec 10, 2019, 5:04 PM (https://localhost/post/1646)
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

Don't clutter this thread with support requests

Start a new topic please, thank you 😘

Dec 10, 2019, 8:22 PM (https://localhost/post/1647)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

K
Kip (https://localhost/user/kip)
(https://localhost/user/kip)

Congratulations on the release and thank you! Having removed Scp (which has served me well at the cost of other Bluetooth devices) I can confirm my Bluetooth headphones working along with my Sixaxis controller being picked up by Windows. Hopefully everything will work fine in games too, time to go test.

Scp has been great and mostly trouble free, I just missed having Bluetooth for other stuff and decided to see if there was a newer solution available. I had literally only stumbled across this project a few days ago and couldn't believe my luck when I saw it was almost due for release. I think the biggest things from Scp I will miss is the state of battery charge function via the controller lights and having to launch Shibari every time I was to use a controller since it doesn't hide in the tray.

Thanks again and good luck for the future, I enjoyed reading this thread.

Dec 10, 2019, 9:37 PM (https://localhost/post/1648)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 2
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)


nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@Kip (https://forums.vigem.org/uid/799) thank you kindly, those missing features mentioned are peanuts compared to the whole stack, that's "easy" to add but for now my 2019 is done, see you guys 'n' gals in 2020 🤘

Dec 11, 2019, 11:06 AM (https://localhost/post/1651)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

L
Locksmith (https://localhost/user/locksmith)
(https://localhost/user/locksmith)

Really looking forward to try this out during the holidays (can't find the time before 😵). Is the source also coming out now, or will you keep that for now?

!ERAU QSSI DLRO WEHT

Dec 11, 2019, 6:02 PM (https://localhost/post/1652)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@Locksmith (https://forums.vigem.org/uid/138) read the FAQ 😉

Dec 14, 2019, 4:14 AM (https://localhost/post/1678)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

L Luke76bg (https://localhost/user/luke76bg)
(https://localhost/user/luke76bg)

It's ready ? For real ? So i can remove scp toolkit driver, install this, and i can pair my dual shock 4 and i will have the same functionality that i have now ? Touchpad i guess it's not usable, right ?

Dec 14, 2019, 7:05 AM (https://localhost/post/1680)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius)
(https://localhost/user/nefarius)

@Luke76bg (https://forums.vigem.org/uid/219) it is ☺️ but like mentioned many many times before, DS4 isn't the primary focus of this solution and TouchPad functionality is out of the scope of this 😘

---

12 DAYS LATER

Dec 26, 2019, 5:03 PM (https://localhost/post/1734)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0
(https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

L Luke76bg (https://localhost/user/luke76bg) (https://localhost/user/luke76bg)

@nefarius (https://forums.vigem.org/uid/1) So it's basically like the scp driver right now ? Touch pad doesn't work eve on that! But scp driver has a nasty problem, i have to pair two times the pad to get it working, i mean i click the central button, the light on the pad become light blue, i have to keep pressed the button for some seconds to shutdown the pad and then, when i press the button again, the pad is recognized by the software and the light become dark blue. This is the standard default behavior. With your new software it's enough one time press button ? Please tell me yes 🐶

Dec 26, 2019, 5:09 PM (https://localhost/post/1735)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 1 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

 nefarius (https://localhost/user/nefarius) (https://localhost/user/nefarius)

@Luke76bg (https://forums.vigem.org/uid/219) I already answered many times how the DS4 behaves with this and again, the DS4 compatibility is just a side effect, an extra, it's not my primary concern since the DS4 needs no special drivers to function on Windows...

Dec 27, 2019, 1:09 AM (https://localhost/post/1738)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

L Luke76bg (https://localhost/user/luke76bg) (https://localhost/user/luke76bg)

@nefarius (https://forums.vigem.org/uid/1) Oh sorry i guess i missed these posts maybe, so it's a standard behavior that can't be fixed, not a problem at all, don't worry! ^^

ABOUT A MONTH LATER

Feb 5, 2020, 9:38 AM (https://localhost/post/1802)
 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#) 0 (https://localhost/topic/242/bluetooth-filter-driver-for-ds3-compatibility-research-notes#)

B belam62928 (https://localhost/user/belam62928) (https://localhost/user/belam62928)

@nefarius (https://forums.vigem.org/uid/1)
I know this is late but wanted to note for anyone following along that wanted source code to filter on these events,
you can use the code from github usbsnoop project

(https://github.com/SnoopWare/usbsnoop/blob/master/USBSnoop/DriverEntry.cpp (https://github.com/SnoopWare/usbsnoop/blob/master/USBSnoop/DriverEntry.cpp))
Also the IOCTL lookups can be found here (http://www.ioctls.net/ (http://www.ioctls.net/))
Additionally there is this discussion (https://community.osr.com/discussion/262813/question-regarding-bluetooth-bthusb-filter-driver (https://community.osr.com/discussion/262813/question-regarding-bluetooth-bthusb-filter-driver))
on how to use the windows driver samples - general toaster driver (https://github.com/microsoft/Windows-driver-samples/tree/master/general/toaster/toastDrv (https://github.com/microsoft/Windows-driver-samples/tree/master/general/toaster/toastDrv))
to create a filter driver.
