GNU/Linux Administration - Support #938

Monitor USB Data With Wireshark on Arch Linux

06/19/2018 10:11 AM - Daniel Curtis

Status:	Closed	**Start date:**	06/19/2018
Priority:	Normal	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	100%
Category:	Workstation	**Estimated time:**	1.00 hour
Target version:	Arch Linux	**Spent time:**	1.50 hour

Description

This is a guide on sniffing USB data using Wireshark on Arch Linux.

Prepare the Environment

- Make sure the system is up to date:

```
sudo pacman -Syu
```

Setup usbmon

- Load the usbmon kernel module:

```
sudo modprobe usbmon
```

- Give regular users privileges to access the usbmon interfaces:

```
sudo setfacl -m u:$USER:r /dev/usbmon*
sudo chmod +r /dev/usbmon*
```

Install Wireshark

- Install wireshark:

```
sudo pacman -S wireshark-gtk
```

- Add a regular user to the wireshark group:

```
sudo usermod -aG wireshark $USER
```

  - **NOTE**: Log out and log back in to make the new group membership take effect.

- Change the group ownership of the usbmon interfaces

```
sudo chgrp wireshark /dev/usbmon*
```

NOTE: Using the regular application launcher from the menu did not let me see the usbmon interfaces. To work around this, I opened up a terminal and launched wireshark from there:

```
wireshark-gtk &
```

Resources

- https://wiki.wireshark.org/CaptureSetup/USB

History

#1 - 06/19/2018 10:35 AM - Daniel Curtis

- Description updated

#2 - 06/21/2018 05:02 PM - Daniel Curtis

- Description updated

- Status changed from New to Resolved

- % Done changed from 0 to 100

#3 - 06/10/2019 02:34 PM - Daniel Curtis

- Status changed from Resolved to Closed