PANalyzr SW Install Procedure for Linux

06/11/2021

Table of Contents

PANalyzr Release Notes

Version 0.8.6, released 06/11/2021

New Features

- TBD

Bug Fixes

- TBD

Spanalytics Contact Details

Please be sure to visit our **PANalyzr YouTube channel** at https://www.youtube.com/channel/UCS5XR9Kghwy7HPL9PUEUVvg for the latest install and user instructions

Technical Support: support@panalyzr.com
Technical Support Phone: 804-364-1050, option 6

Sales: sales@panalyzr.com

Other inquiries: support@panalyzr.com

Open-Source Utilities

The PANalyzr Protocol Analyzer software utilizes several open-source solutions to provide additional features to the system, including crackle, Knob, E0 and Wireshark. Spanalytics has modified these utilities, and the modified source code are either included in this installation, or available upon request.

- □ Knob - The original Knob code can be found at https://github.com/francozappa/knob. The source code modifications made are included in this installation (located in the **/opt/panalyzr** directory after the installation completes)
- □ E0 – The original E0 code can be found at https://github.com/adelmas/e0. The source code modifications made for this installation are available upon request
- □ Brackle – The original crackle code can be found at https://github.com/mikeryan/crackle. The source code modifications made for this installation are available upon request
- □ Wireshark – The original Wireshark code can be found at https://www.wireshark.org/download.html. The source code modifications made for this installation are available upon request
- □ KillerZee – The original code can be found at https://github.com/joswr1ght/killerzee. The source code modifications made for this installation are available upon request
- □ Z-Wave Wireshark plugin – The original code can be found at https://github.com/AFITWiSec/EZ-Wave. The source code modifications for this installation are available upon request
- □ libpcap – The original libpcap code can be found at https://www.tcpdump.org/index.html#latest-releases

License Clauses

libpcap

Introduction

This procedure describes the steps required to install and run the latest version of the PANalyzr Protocol Analyzer software on an Ubuntu Linux machine.

System Requirements

The following system settings and software are required:

- Linux Ubuntu (v18.04 or higher)
- 3GB free hard drive space
- Internet access (to download required package dependencies)

Wireshark

PANalyzr requires Wireshark version 3.4.2.

If version 3.4.2 is currently installed, the user will be prompted to allow the installation to perform necessary preferences file updating.

If version 3.4.2 is not currently installed, the user will be prompted to allow an new install, an upgrade or downgrade, as applicable, to version 3.4.2.

Please note that PANalyzr will not run or dissect packet data properly unless Wireshark version 3.4.2 is installed.

Install the PANalyzr Software

- □ Copy the file ***panalyzr_0.8.6.deb*** to the Desktop of the Ubuntu machine
- □ Open a terminal window and type the following commands:
  - □ **cd ~/Desktop**
  - □ **sudo dpkg -i panalyzr_0.8.6.deb**
- □ Enter your user password when prompted
- □ When the installation completes, close the terminal window
- □ Click on the **Show Applications** button (located on the Dock)
- □ In the *Type to search…* field, enter “Panalyzr-Setup”
- □ Click on the **PANalyzr-Setup** app icon.

Wireshark version 3.4.2 not found on the system

The steps below should take approximately 10 minutes to complete, depending on the Linux machine specifications.

Note: The process used to upgrade or downgrade Wireshark on the computer could remove existing Wireshark preferences and configuration files. A backup of these files is strongly recommended before running these commands.

- ☐ In the opened PANalyzr-Setup terminal window, hit the **Enter** button to start the installation at the *“Okay to proceed with installing main prerequisites? Note: PANalyzr will not run correctly without these dependencies [Y/n]:”* prompt
- ☐ (If prompted) Enter your user password
- ☐ At the *“Okay to proceed with setup for Z-Wave packet capturing? [Y/n]:”* prompt, hit the **Enter** button
- ☐ At the *“Okay to proceed with installing Wireshark v3.4.2? (This will overwrite the existing version on the system) [Y/n]:”* prompt, hit the **Enter** button
- ☐ At the *“Press [ENTER] to continue or Ctrl-c to cancel adding it”* prompt, hit the **Enter** button
- ☐ In the first “Configuring wireshark-common” window, select the **Yes** option, then hit the **Enter** button
- ☐ In the second “Configuring wireshark-common” window, select the **Yes** option, then hit the **Enter** button
- ☐ At the *“Okay to proceed with install g++ version 9 and make it the default system compiler? [Y/n]:”* prompt, hit the **Enter** button
- ☐ At the *“Press [ENTER] to continue or Ctrl-c to cancel adding it”* prompt, hit the **Enter** button

PANalyzr-WS is now successfully installed on the system

Wireshark version 3.4.2 found on the system

The steps below should take approximately 2 to 3 minutes to complete, depending on the Linux machine specifications.

- ☐ In the opened PANalyzr-Setup terminal window, hit the **Enter** button to start the installation at the *“Okay to proceed with installing main prerequisites? Note: PANalyzr will not run correctly without these dependencies [Y/n]:”* prompt
- ☐ (If prompted) Enter your user password
- ☐ At the *“Okay to proceed with setup for Z-Wave packet capturing? [Y/n]:”* prompt, hit the **Enter** button
- ☐ At the *“Okay to proceed with install g++ version 9 and make it the default system compiler? [Y/n]:”* prompt, hit the **Enter** button
- ☐ At the *“Press [ENTER] to continue or Ctrl-c to cancel adding it”* prompt, hit the **Enter** button

PANalyzr-WS is now successfully installed on the system

Run PANalyzr

See the PANalyzr User Guide for details on how to utilize the PANalyzr Protocol Analyzer software.

Troubleshooting

Error message during install

If the error message “Error: dpkg frontend is locked by another process” is displayed, this is an indication that a system or package update is already in progress. The user must either wait for this update to complete, or if possible and applicable given any tasks in progress, can restart the computer.

Bad Request Errors during installation on VMWare Workstation virtual machines

PANalyzr requires the installation of several standard Linux packages. If these packages are not installed properly, PANalyzr functionality will be impacted.

When installing PANalyzr on a VMWare Workstation Player virtual machine, it has been noted that errors are encountered when performing the package installation. An indication of this is the error message “*400 Bad Request [IP: 91.189.91.38 80*]” being shown repeatedly.

If this occurs, re-running the PANalyzr-Setup (sometimes two or three times) will resolve the issue.

This issue does not occur when running the PANalyzr installation on Linux computers or laptops

Uninstall PANalyzr

- ☐ Double-click on the panalyzr_0.8.6.deb file on the Desktop
- ☐ In the *panalyzr* window, click the **Remove** button
- ☐ Enter your user password when prompted
- ☐ (Optional, to remove any temp files created) Open a terminal window and type:
    - ☐ sudo rm -rf /opt/panalyzr
    - ☐ rm /tmp/wireshark_output.txt