Wireshark and USB

John E. Harbold
SVFIG – June 28, 2014

Wireshark is known as a network monitoring tool, but it can also monitor other interfaces such as Bluetooth and USB.

This talk is about Wireshark and USB.

Wireshark

- Website: http://www.wireshark.org/.
- Platforms: Windows, OS-X & Linux.
- Development Libraries: Add Wireshark to your application!
- Dissectors: Decode data packets.

USB

- Website: http://www.usb.org/home.
- Platforms: The name says it, **Universal** Serial Bus.
- Versions & Clock Speeds:
  - V 1.1 - 12.0 MHz
  - V 2.0 - 480.0 MHz
  - V 3.0 - 5.2 GHz
  - V 3.1 - 10.0 GHz

USB

- Interfaces:
  - Hub
  - Device
  - Both: OTG (On-The-Go)

- Protocol
  - Clear Feature
  - Get Configuration
  - Get Descriptor
  - Get Interface
  - Get Status
  - Set Address
  - Set Configuration
  - Set Feature
  - Set Interface
  - Synch Frame

Descriptor Types

- Device
- Configuration
- String
- Interface
- Endpoint
- Device Qualifier
- Other Speed Configuration
- Interface Power

Feature Types

- Device Remote Wake-up
- Endpoint Halt
- Test Mode

Demonstration

- Install Wireshark.
- Start Wireshark (Linux as root).
- Select USB interface.
- Start packet capture.
- Plug USB device into interface.
- Record USB protocol.