PAINT User Guide

Version: Wireshark 1.6.5-PAINT-Beta

Table of Contents

What is PAINT?

PAINT is a tool that works with the popular open-source tool Wireshark by identifying the originating and the consuming executable processes for each TCP/IP network packet. PAINT was a DARPA-sponsored Cyber Fast Track (CFT) project and stands for Process Attribution In Network Traffic.

PAINT works with Wireshark 1.6.5. Newer versions of Wireshark are not yet compatible.

PAINT is provided for free by Digital Operatives for personal and academic use only. All commercial customers must contact Digital Operatives for a license. PAINT comes with no support and no warranty.

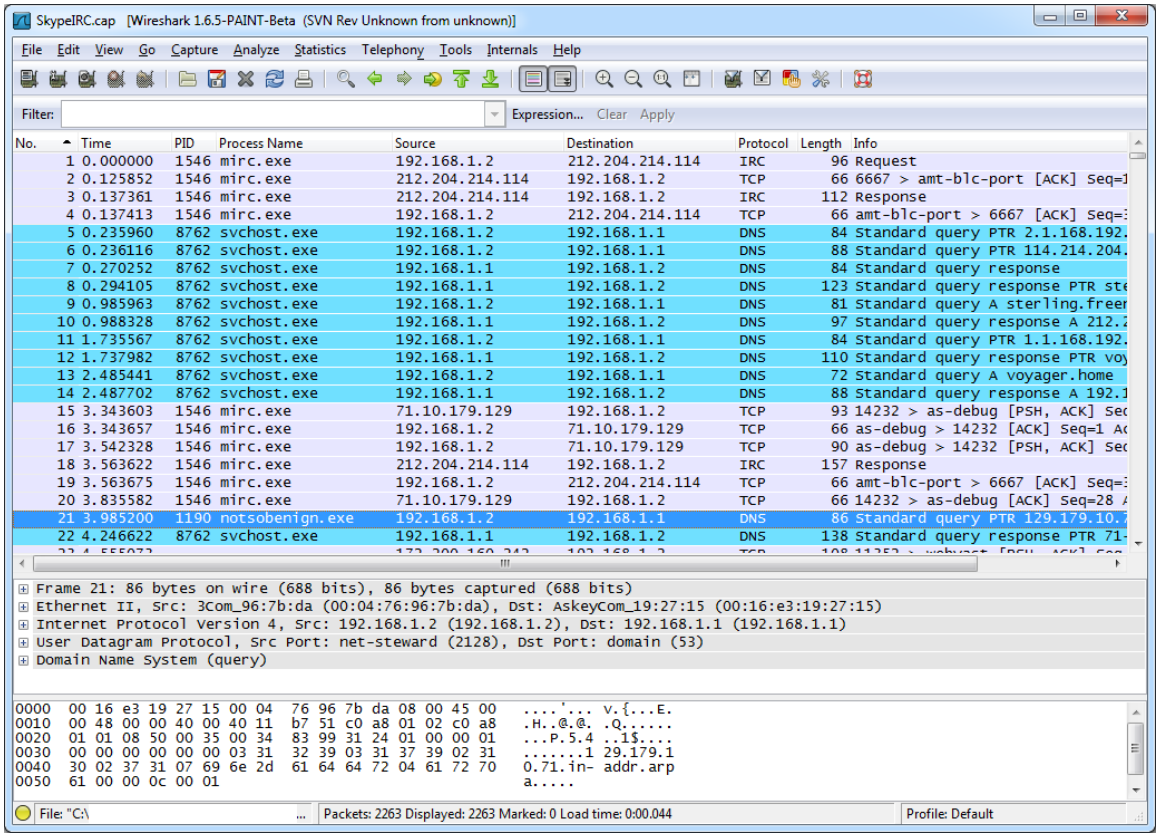

Figure 1: Screen capture of PAINT with Wireshark (Fictitious Traffic and Attribution)

How to Use

1. PAINT currently runs on Windows 7, 32 and 64 bits.
2. Run *wireshark-win32-1.6.5-PAINTmods-Beta.exe* to install. Install as you would install a standard Wireshark installation.
3. Run PAINT-Beta.exe to install PAINT.
4. Run Wireshark as an Administrator.
5. When capturing 802.11 traffic, set "Link-layer header type" to "Force802.11" in Capture Options.

How It Works

PAINT replaces the dumpcap.exe executable that comes with the standard Wireshark installation with our own. The updated new dumpcap.exe captures Event Tracing for Windows (ETW) events provided by Windows to capture TCPIP and NDIS (Network Driver Interface Specification) layer events to ultimately trace each TCPIP packet to the originating and target executable. The PAINT version of Wireshark no longer uses the winpcap driver to capture network packets.

When the network traffic capture is complete, PAINT creates a .process file in addition to the usual .pcap file. This file will be named the same as the pcap file with the additional extension of .process. When the PAINT version of Wireshark loads a pcap file, it will also look for a .process file of the same name. PID and Process Name information will be loaded if the .process file is found. This process is transparent to the end user. However, **if you move or copy the pcap file, you must do the same with the equivalent .process file or Wireshark PAINT will not be able to retrieve the process information.**

The PAINT version of Wireshark 1.6.5 was modified to include two additional columns: PID and Process Name.

Notes About Processing 802.11 Traffic

Because the NDIS layers works at a lower level than the winpcap driver, it cannot determine whether a network packet is an 802.3 packet or an 802.11 packet. Therefore it is necessary to specify the link-layer by setting "Link-layer header type" to "Force802.11" in Capture Options. It is 802.3 by default. See Figure 2.

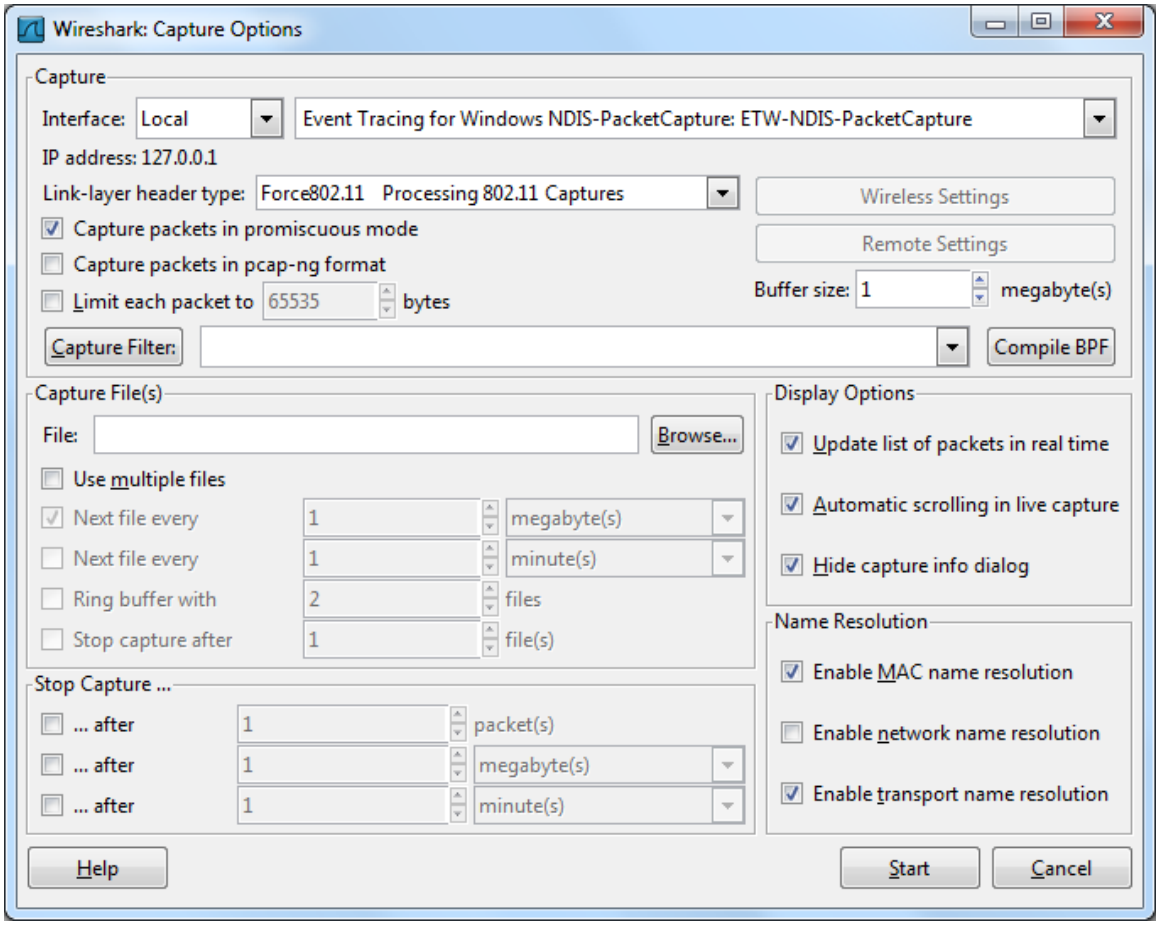

Figure 2: New PAINT version of Wireshark Capture Option: Force802.11

Limitations

PAINT was a research project and is currently in Beta stage. It may contain usability, feature, and performance limitations compared to polished open-source and commercial-of-the-shelf software products.

Some of these limitations are:

- PAINT/dumpcap does not support capture filters. Capture filters are built-in to libpcap and PAINT/dumpcap does not use libpcap.
- Filters in Wireshark, both capture and display, filter by packet content. The process information introduced in PAINT is additional meta information about the packets captured and does not alter the packet content. Therefore, packets are not filterable by the PID or the process name.

- While we are able to retrieve process path, it doesn't fit in the traffic window well. Therefore we omitted the process path from display. If it's desired, it is not difficult to modify PAINT/dumpcap to send the full process path and introduce another column in Wireshark for display.
- PAINT version of Wireshark will process about 100 packets per second on a moderate modern box.

Contact Us

We would love to hear from you on how useful PAINT has been to your research and mission, or how it might be improved. Please get in touch with us at contact@digitaloperatives.com

Also visit our website at www.digitaloperatives.com for future product and research announcements and our blog for latest news: http://digitaloperatives.blogspot.com