

Intrepid icscap Plugin

Free Wireshark Plugin for Automotive Network Tools from Intrepid Control Systems

Intrepid icscap Plugin is a free plugin for Wireshark that empowers engineers to monitor and analyze in-vehicle network traffic using Intrepid hardware. Supporting Automotive Ethernet, CAN, CAN FD, LIN, and FlexRay networks, icscap delivers real-time packet-level visibility to Wireshark.

When paired with Vehicle Spy, icscap evolves into a complete development and validation suite. Engineers can go beyond packet analysis to decode signals, simulate and transmit traffic using Tx Panel in VSpy, analyze stateful protocols such as SOME/IP and DoIP, perform diagnostics and calibration, and even automate testing and fuzzing using existing databases. Together, icscap and Vehicle Spy give full visibility into both packet-level and system-level network activity, accelerating development, troubleshooting, and compliance testing.

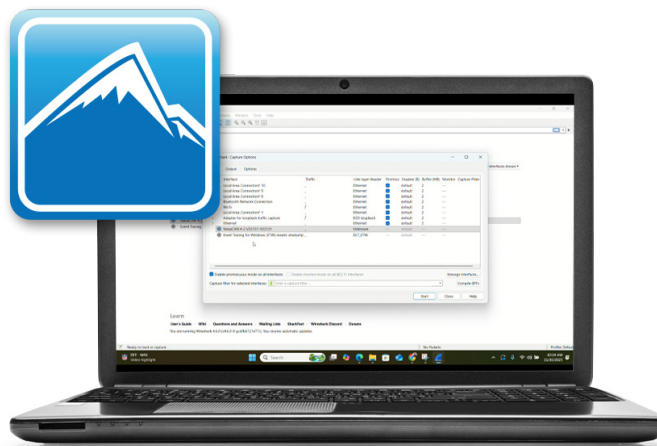
Intrepid icscap Plugin Features & Benefits:

- Capture and analyze Automotive Ethernet, CAN, CAN FD, LIN, and FlexRay traffic for debugging, validation, and compliance testing.
- Use a familiar interface to inspect raw packets and diagnose communication issues efficiently.
- Extend Wireshark with Lua scripts to interpret proprietary messages or complex traffic patterns (Protobuf, SOME/IP, etc).

Ordering Information

Part Number	Description
ICSCAP	Free Wireshark Plugin for Automotive Network Tools from Intrepid Control Systems

Specifications subject to change; please contact Intrepid for the latest information. All trademarks are the property of their respective owners.



- Capture traffic for offline analysis, regression testing, replay, or teaching purposes.
- Easy installation with Intrepid interfaces, minimizing setup time and downtime.

Intrepid icscap Plugin + Vehicle Spy

- Track SOME/IP, DoIP, UDS, and other multi-frame protocols, understanding sequence and system-level interactions.
- Inject messages or replay traffic to validate ECU responses and simulate complex network scenarios.
- Perform CCP, XCP, and UDS operations for ECU testing and system tuning.
- Measure latency, jitter, and throughput across multiple networks.
- Build test sequences, automate validations, and stress-test ECUs with malformed or randomized messages based on databases.
- Native interpretation of DBC, ARXML, FIBEX files to correlate packets with meaningful signals.



INTREPID
CONTROL SYSTEMS
www.intrepidcs.com

1850 Research Drive
Troy, MI 48083 USA
Ph: +1 (586) 731-7950

Rev. 20251113