Accessory Test System User Guide

Version 6

Contents

Contents

Contents

Figures and Tables

1. Introduction

1.1 Purpose of This Specification

This document describes the configuration and use of Apple's Accessory Test System (ATS). ATS consists of:

- A set of real-time tools for diagnosing and debugging the hardware-layer and iAP protocol performance of accessories.
- A set of automated validation tools for ensuring that new accessories more fully comply with the MFi specifications.
- Various hardware components for connecting to various types of MFi accessories.

1.2 Requirements, Recommendations, and Permissions

This specification contains statements that are incorporated by reference into legal agreements between Apple and its licensees. The use of the words *must*, *must not*, *required*, *shall*, *shall not*, *should*, *should not*, *recommended*, *not recommended*, *may*, *optional*, and *deprecated* in a statement have the following meanings:

- *must*, *shall*, or *required* means the statement is an absolute requirement.
- *must not*, *shall not* or *prohibited* means the statement is an absolute prohibition.
- *should* or *recommended* means the full implications must be understood before choosing a different course.
- *should not* or *not recommended* means the full implications must be understood before choosing this course.
- *may* or *optional* means the statement is truly optional, and its presence or absence cannot be assumed.
- *deprecated* means the statement is provided for historical purposes only and is equivalent to 'must not'.

The absence of requirements, recommendations, or permissions for a specific accessory design in this specification must not be interpreted as implied approval of that design. Developers are strongly encouraged to ask Apple for feedback on accessory designs that are not explicitly mentioned in this specification.

1.3 Developer Preview

Content labeled as *developer preview* is not intended for use in the development of Proposed Products or Licensed Products under an MFi License. Although content labeled this way has been reviewed for accuracy, it is not final. Apple is supplying this content to help accessory developers plan for the adoption of the accessory

interface features described herein. This information is subject to change, and accessories implemented according to this content must be tested with final operating system software and final documentation before going through self-certification.

1.4 Manufacturer Preview

Content labeled as *manufacturer preview* is final and may be used in the development of Proposed Products under an MFi License, although associated MFi components (if applicable) may not yet be available to order. Apple is supplying this content to help accessory developers start developing against the accessory interface features described herein.

1.5 Terminology

1.5.1 Device

Device and *iOS device* refer to an iPhone, iPad, or iPod running iOS.

Where appropriate, specific Apple product and operating system references will also be used.

1.5.2 Accessory

Accessory refers to any product that connects to a *device* via the interfaces described in this specification.

2. Overview

ATS is designed to analyze iAP traffic delivered over UART, USB, and Bluetooth transports, CarPlay traffic over USB and Wireless (Bluetooth and Wi-Fi), AirPlay 2 traffic over Wi-Fi, and Lightning Audio traffic.

> **Note:** The 30-pin connector is deprecated for new product plans and support will be removed from ATS in the future along with availability of the ATS 30-pin Box and MFi 30-pin Breakout.

2.1 Equipment List

Before getting started, make sure you have any equipment you may need, as listed below.

Mac computers may be purchased at https://apple.com.

The MFi Portal contains links to Authorized Distributors to purchase the following:

- ATS Lightning Box
- ATS Smart Connector Box
- ATS Lightning Audio Box
- MFi Lightning SI Tester
- MFi Lightning Tester
- MFi USB SI Tester
- MFi USB Breakout
- Total Phase Beagle USB 480 analyzer
- Frontline ComProbe BPA analyzer

A powered USB hub may also be useful to centralize connections for all equipment.

2.2 Supported macOS Versions

ATS will run on any Mac running macOS 10.12 Sierra or later.

> **Note:** Wireless captures with iPhone XR, iPhone XS, and iPhone XS Max can only be taken with a Mac running macOS 10.13 High Sierra or later.

If you do not already have ATS, download it from the MFi Portal (https://mfi.apple.com) or contact your MFi Representative.

2.3 ATS Lightning Box

The ATS Lightning Box is required to use ATS with Lightning accessories. It allows for analysis of data over the Lightning connector, and can also make USB signals available for use with the Beagle USB 480 analyzer (page 12).

Figure 2-1 ATS Lightning Box
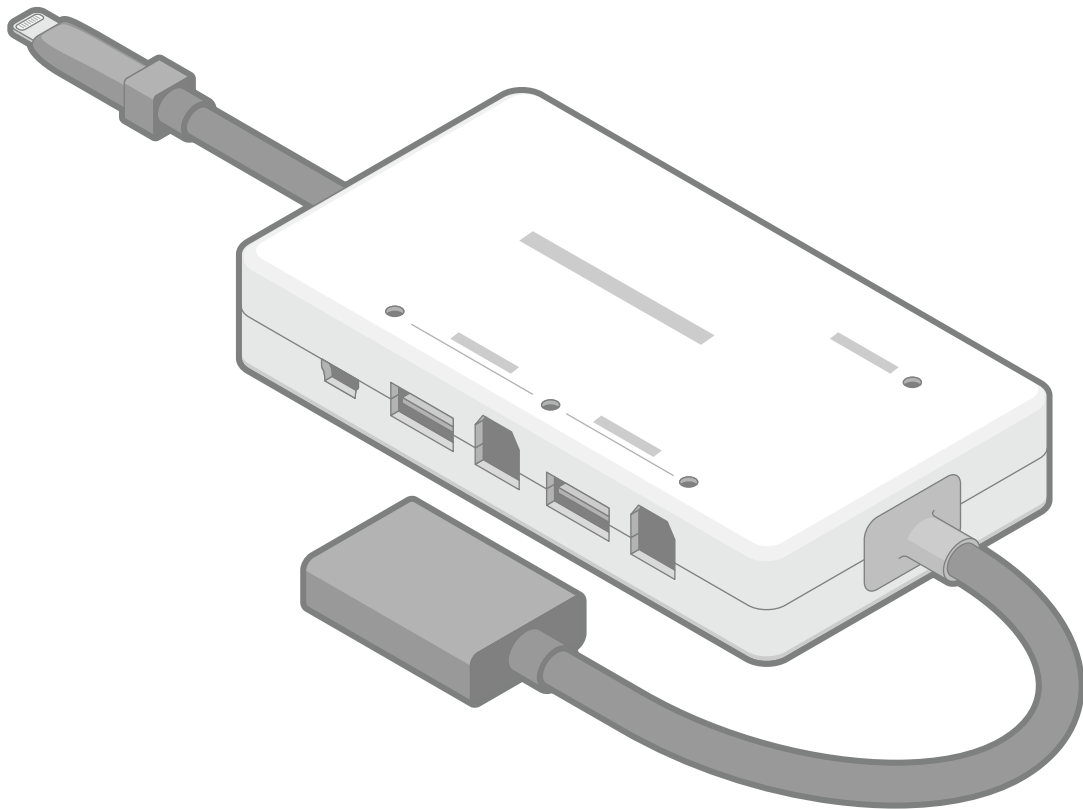
Additional test hardware may be required to complete certification:

- Total Phase Beagle USB 480 analyzer, required to capture iAP2 over USB traffic.
- Frontline ComProbe BPA 100 analyzer or ComProbe BPA 600 analyzer, required to capture iAP2 over Bluetooth traffic.
- Lightning Connector Extension Cable

2.4 ATS Smart Connector Box

The ATS Smart Connector Box is required to use ATS with Smart Connector accessories. It allows for analysis of data over the Smart Connector.

Figure 2-2   ATS Smart Connector Box

Additional test hardware may be required to complete certification:

• MFi Lightning Tester

2.5 ATS Lightning Audio Box

The ATS Lightning Audio Box is required to use ATS with Lightning Audio accessories. It allows for analysis of data over the Lightning Audio transport.

Figure 2-3   ATS Lightning Audio Box
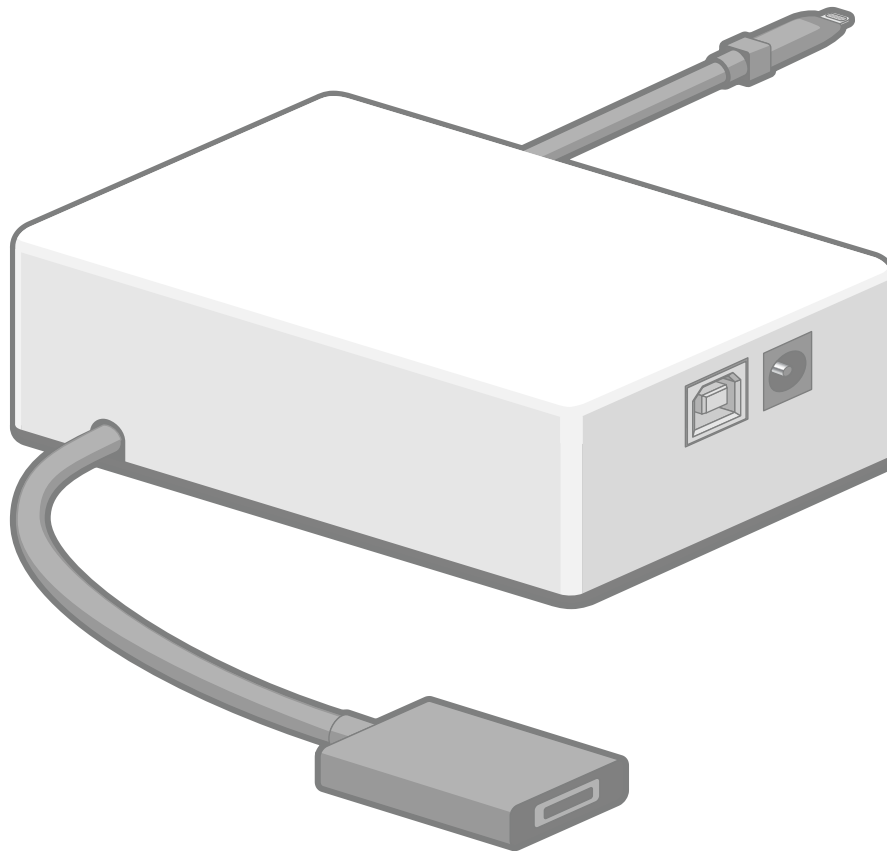
2.6 Beagle USB 480 analyzer

The Total Phase Beagle USB 480 analyzer or Beagle USB 480 Power analyzer is required to use ATS with USB accessories. The Beagle USB 480 analyzer is capable of monitoring of high-/full-/low-speed USB data. With support for real-time class-level decoding of main USB classes, the Beagle USB 480 analyzer is a powerful and versatile tool for USB development.

More information about Total Phase products is available at http://www.totalphase.com.

2.7 ComProbe BPA analyzer

Analyzing Bluetooth traffic requires a Frontline ComProbe BPA 100 analyzer or ComProbe BPA 600 analyzer. Either device will allow for analysis of iAP-over-Bluetooth data captured wirelessly over the air. See ComProbe BPA analyzer Driver (page 14) for firmware installation.

More information about Frontline products is available at http://www.fte.com.

Note: ATS does not provide a comprehensive Bluetooth analysis solution

ATS only provides a solution for capturing and validating iAP-over-Bluetooth. For full visibility into the entire Bluetooth stack, Frontline offers the USB-powered ComProbe BPA 600 analyzer, a tool for the development of robust and interoperable Classic, low energy and dual-mode Bluetooth products. For more information about the ComProbe BPA 600 analyzer, see http://www.fte.com/getbpa600.

2.8 30-pin Hardware

For information about 30-pin hardware, see ATS 30-pin Box (page 77).

3. Installation and Updates

3.1 Software Installation

For Mac system requirements, see Supported macOS Versions (page 9). If needed, use the "Software Update…" command under the Apple menu or check the Mac App Store to get an updated version of macOS.

Download the .zip bundle containing the latest ATS application from the MFi Portal. For more information about connecting to the MFi Portal, contact your MFi Representative. Unzip the bundle then copy the ATS application to your "Applications" folder. Once installed, the ATS app can be launched by double-clicking on ATS in the "Applications" folder.

You will be required to login with your Apple ID and password before updating ATS. You must use an Apple ID that's configured as an ATS user in the MFi Portal.

3.2 Drivers, Firmware Updates, Packages

Various drivers, firmware updates, and packages need to be installed for ATS to capture traffic. The required dependencies depend on the type of capture and all required installations are guided by the app.

3.2.1 ComProbe BPA analyzer Driver

Note: Prior to updating the driver for the ComProbe BPA analyzer, select the following setting in System Preferences > Security & Privacy > General > "Allow apps downloaded from: App Store and identified developers". Also, during the driver installation, select "Allow" (in System Preferences > Security & Privacy > General) next to "System software from developer 'Frontline Test Equipment, inc.' was blocked from loading."

Before connecting the ComProbe BPA analyzer hardware, launch the ATS application. If your Mac requires an updated ComProbe BPA analyzer driver, ATS will notify you, then launch the driver installer. Once installation is complete, you may attach the ComProbe BPA analyzer and begin using it.

3.2.2 Firmware Updates

Updates for the ATS Box firmware, Beagle USB 480 analyzer firmware, and ComProbe BPA analyzer firmware are contained in the ATS application bundle. If an ATS application update includes firmware that is newer than the version on the selected capture hardware, ATS will prompt you to update the firmware.

The firmware on the ATS Lightning Box must be updated.

A separate application will be launched to update the firmware.

OK

ATS Lightning Box Firmware Updater 0.4.0

ATS Lightning Box - ATS

The attached box has firmware version 0.3.5. Click Update to update the firmware to version 0.4.0.

Update

ATS Lightning Box Firmware Updater 0.4.0

ATS Lightning Box - ATS

The box's firmware was successfully updated to version 0.4.0.

Quit

This step should only be necessary once per application / firmware update.

3.3 Reporting Bugs

To report bugs or request enhancements to ATS, file a New Problem at https://bugreport.apple.com. Include "MFi ATS" in the Title field. When reporting bugs, attach an ATS trace file that demonstrates the issue.

4. Starting an ATS Capture

This chapter will instruct you on how to start a capture using ATS with the following steps:

1. Determine your accessory type per What is your accessory's type? (page 17).
2. Setup your capture hardware per Capture Hardware Setup (page 19).
3. Launch the ATS app.
4. Open the "New ATS Capture" window and configure it per Capture Configuration (page 17).
5. Click Start Capture.
6. Initiate the communication between the Apple device and accessory per Hardware Considerations (page 24).

4.1 What is your accessory's type?

There are several ways to connect the above equipment to ATS. You should use the method most appropriate for your accessory:

- If your accessory sends iAP data over the UART transport, it is an iAP-over-UART accessory.
- If your accessory sends iAP data over the USB transport, it is an iAP-over-USB accessory.
- If your accessory sends iAP data over the Bluetooth transport, it is an iAP-over-Bluetooth accessory.
- If your accessory sends iAP data over the Smart Connector transport, it is an iAP-over-Smart Connector accessory.
- If your accessory sends iAP data over the Lightning Audio transport, it is an iAP-over-Lightning Audio accessory.
- If your accessory sends CarPlay (and iAP) data over the USB transport, it is a CarPlay-over-USB accessory.
- If your accessory sends CarPlay (and iAP) data wirelessly, it is a CarPlay-over-Wireless accessory.
- If your accessory sends AirPlay 2 data, it is an AirPlay 2 accessory.
- If your accessory does not send iAP data it is a Non-iAP accessory.

4.2 Capture Configuration

Once you know what accessory type you have, the Capture Configuration Table (page 18) shows what selections need to be made in the "New ATS Capture" window (see Figure 4-1 (page 19)). This is accessible via File > New > Capture…, or the New Capture toolbar icon or the Command-N shortcut.

Table 4-1   Capture Configuration

Accessory Type	Tab	Transport	Capture Device	Protocol
iAP-over-UART	Wired	UART	ATS Lightning Box	iAP1 or iAP2
iAP-over-USB	Wired	USB	Beagle USB 480 analyzer	iAP1 or iAP2
			ATS Lightning Box*	
iAP-over-Bluetooth	Wireless	Bluetooth	ComProbe BPA analyzer	iAP1 or iAP2
iAP-over-Smart Connector	Wired	UART	ATS Smart Connector Box	iAP2
iAP-over-Lightning Audio	Wired	Lightning Audio	ATS Lightning Audio Box	iAP1 or iAP2
CarPlay-over-USB	Wired	USB	Beagle USB 480 analyzer	CarPlay over USB
CarPlay-over-Wireless	Wireless	Bluetooth	ComProbe BPA analyzer	iAP2
		Wi-Fi	Apple Device	CarPlay
AirPlay 2	Wireless	Wi-Fi	Apple Device	AirPlay 2

* The ATS Lightning Box is only needed if the accessory has a Lightning connector, or if you are testing in the ATS Certification Assistant.

Figure 4-1 New ATS Capture Window
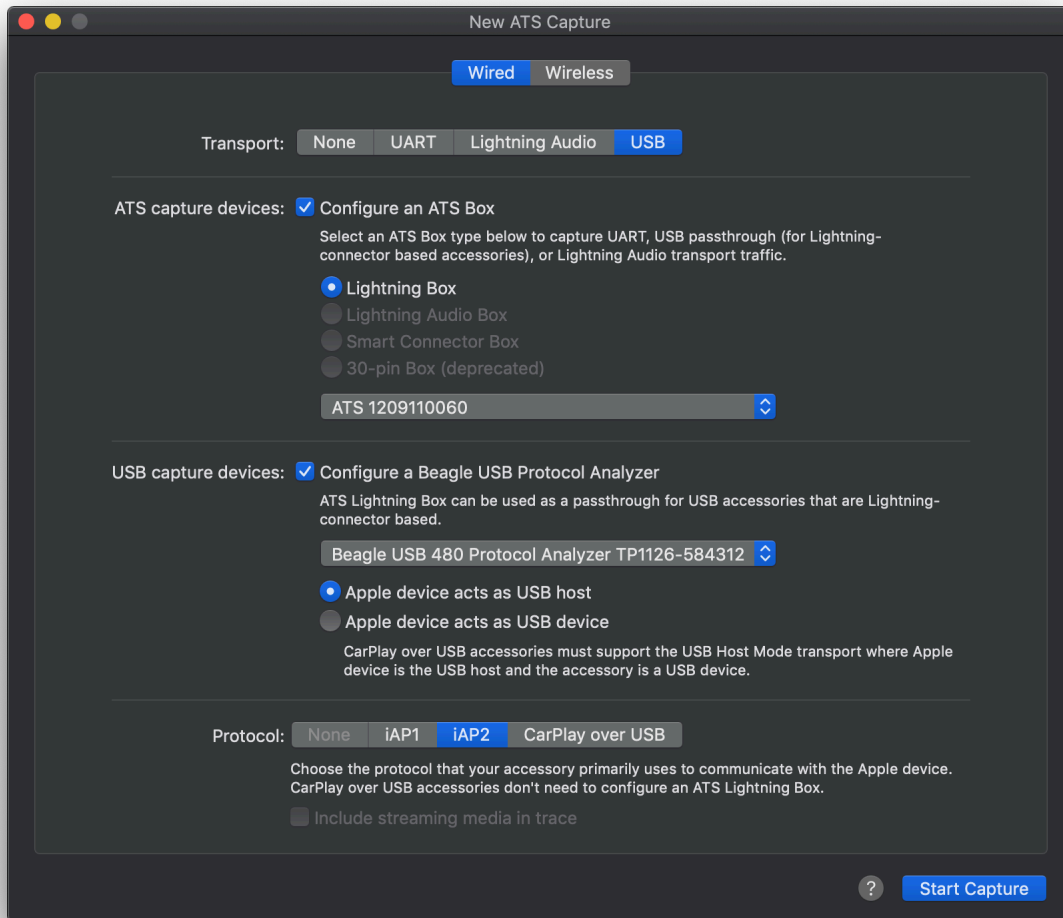
4.3 Capture Hardware Setup

4.3.1 iAP-over-UART, iAP-over-Smart Connector, or Non-iAP

For accessories that do not transmit iAP-over-USB, you only need to connect an ATS Box.

Connect an ATS Box to your Mac as shown. For Lightning accessories, use an ATS Lightning Box. For Smart Connector accessories, use an ATS Smart Connector Box. For 30-pin accessories, use an ATS 30-pin Box.

Figure 4-2 ATS Box Configuration (Non-USB)
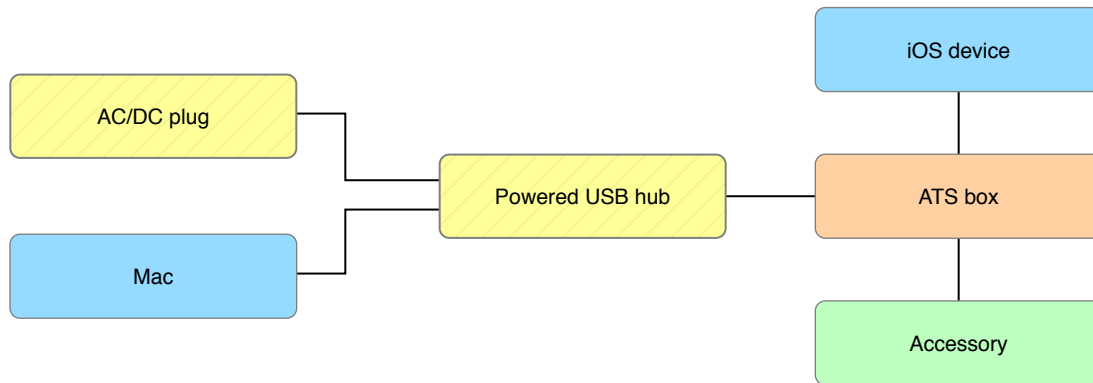
4.3.2 iAP-over-USB (Lightning) or CarPlay-over-USB

For iAP-over-USB accessories which use the Lightning connector, as well as for CarPlay-over-USB accessories, you must connect additional equipment.

Connect the equipment as shown.

Figure 4-3 ATS Lightning Box USB Configuration
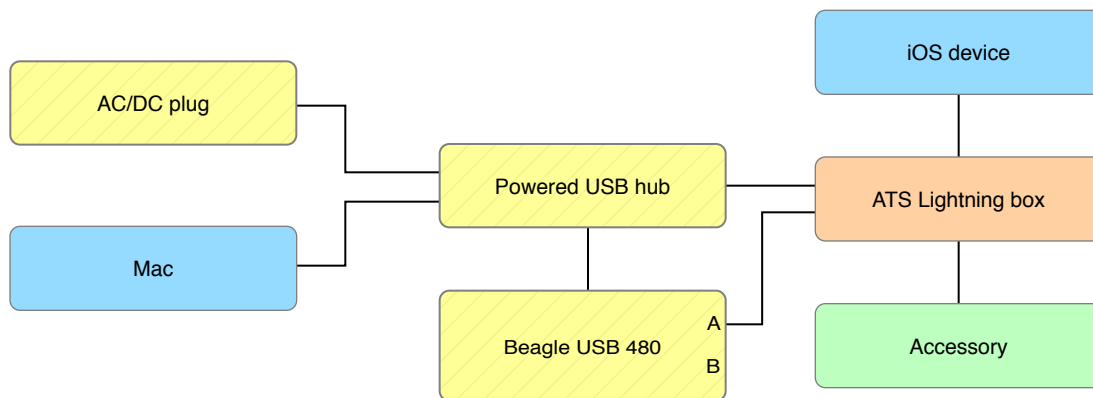
Note: The Beagle USB 480 analyzer must be connected to Port A of the ATS Lightning Box. Port B must remain empty and is reserved for future use.

4.3.3 iAP-over-Bluetooth

Configure the equipment as shown.

Figure 4-4   Bluetooth Configuration
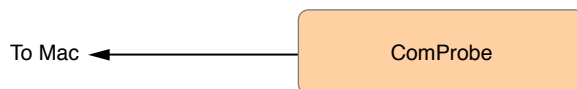
A Bluetooth link key is required to configure the capture, refer to Capturing iAP-over-Bluetooth (page 26) for more information.

4.3.4 iAP-over-Lightning Audio

Connect an ATS Lightning Audio Box to your Mac as shown.

Figure 4-5   ATS Lightning Audio Box Configuration
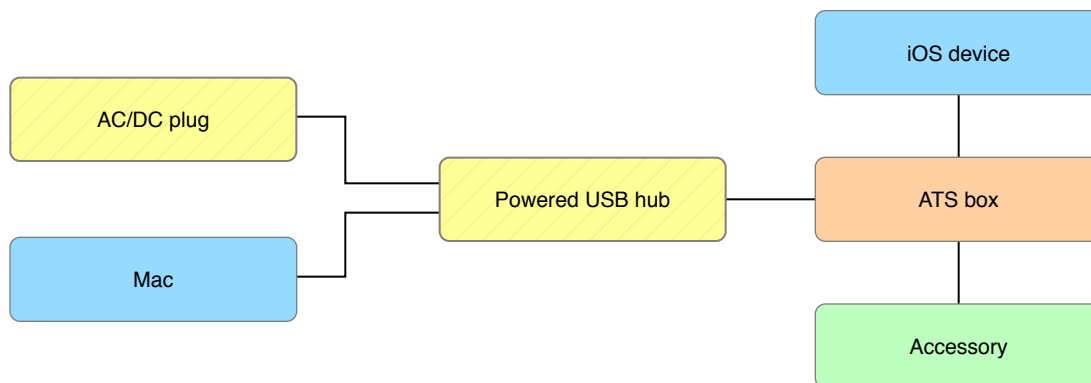
4.3.5 CarPlay and AirPlay 2

4.3.5.1 Enabling Traffic Decryption

CarPlay over USB sessions are encrypted in iOS 8.3 and later for CarPlay accessories that support it. In order for ATS to decrypt the CarPlay session with iOS 8.3 through iOS 9.2, you must use ATS Utility (page 57) to turn on the "Enable CarPlay Traffic Sniffing" switch before the CarPlay session begins. For iOS 9.3.1 and later, use ATS Utility (page 57) to "Enable Traffic Decryption" which will install an AirPlay Diagnostic Mode configuration profile that will remain installed for up to six months.

All wireless CarPlay and AirPlay 2 sessions are encrypted. Use ATS Utility (page 57) to "Enable Traffic Decryption" which will install the AirPlay Diagnostic Mode configuration profile - that will remain installed for up to six months - prior to capturing Wi-Fi traffic in ATS.

4.3.5.2 CarPlay over USB

Note: Capture Requirements

In order to capture an encrypted CarPlay over USB session, you must follow the instructions from Enabling Traffic Decryption (page 21).

ATS can be configured to capture CarPlay over USB using either the Total Phase Beagle USB 480 analyzer alone or with the ATS Lightning Box. To capture with only the Beagle USB 480 analyzer, disable the "Configure an ATS Box" option in the "New ATS Capture" window.

4.3.5.3 CarPlay and AirPlay 2 over Wi-Fi

Note: Wireless Capture Requirements

All wireless sessions are encrypted, so you must follow the instructions from Enabling Traffic Decryption (page 21). Make sure you've chosen to trust the attached computer on the device before starting a capture. ATS will also prompt a package installation when the capture is configured.

Note: Wireless captures with iPhone XR, iPhone XS, and iPhone XS Max can only be taken with a Mac running macOS 10.13 High Sierra or later. On macOS 10.12 Sierra Xcode is required to be installed to perform wireless captures with other devices.

ATS can capture CarPlay or AirPlay 2 traffic over Wi-Fi by connecting the iOS device to the Mac. To begin a Wi-Fi capture, first ensure you meet the requirements described above, then connect the iOS device to the Mac with a Lightning cable.

4.3.6 iAP-over-USB (30-pin)

For iAP-over-USB accessories which utilize the 30-pin connector, you must connect additional equipment.

Connect the equipment as shown.

Figure 4-6   ATS 30-pin Box USB Configuration
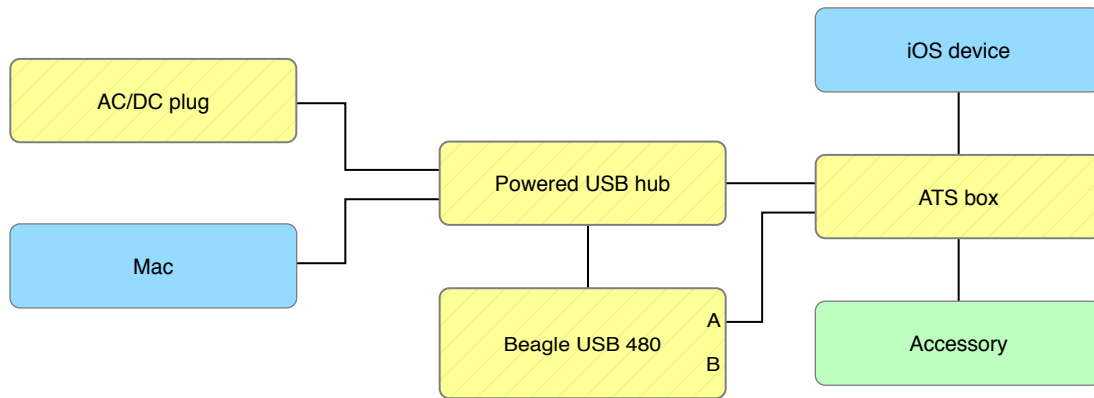
5. Hardware Considerations

There are several things to keep in mind when using ATS to ensure validation occurs correctly.

5.1 Connecting an ATS Smart Connector Box to your Mac

Before connecting an ATS Smart Connector Box to your Mac, make sure the box is not connected to a device or an accessory. Failure to do so prevents the ATS Smart Connector Box from operating correctly. When the ATS Smart Connector Box is in this state, the green PASS light on its enclosure will not turn on. To resolve the issue, disconnect the ATS Smart Connector Box from your Mac and then reconnect it after removing the device or accessory.

5.2 Connector Adapters

30-pin accessories must use the ATS 30-pin Box. Lightning accessories must use the ATS Lightning Box. Accessory developers must not connect a Lightning to 30-pin Adapter to the accessory side of the ATS Lightning Box. If your accessory uses the Lightning to 30-pin Adapter, then the ATS 30-pin Box must be used instead of the ATS Lightning Box. Either variant of the Lightning to 30-pin Adapter may be used (the Lightning to 30-pin Adapter and the Lightning to 30-pin Adapter (0.2 m)). See Figure 5-1 (page 25).

> **Note: 30-pin Accessories Cannot Claim Compatibility with Lightning**
>
> Adapters may only be used in Sniffer mode and are not allowed during certification.

Figure 5-1   Permitted Adapter Configurations
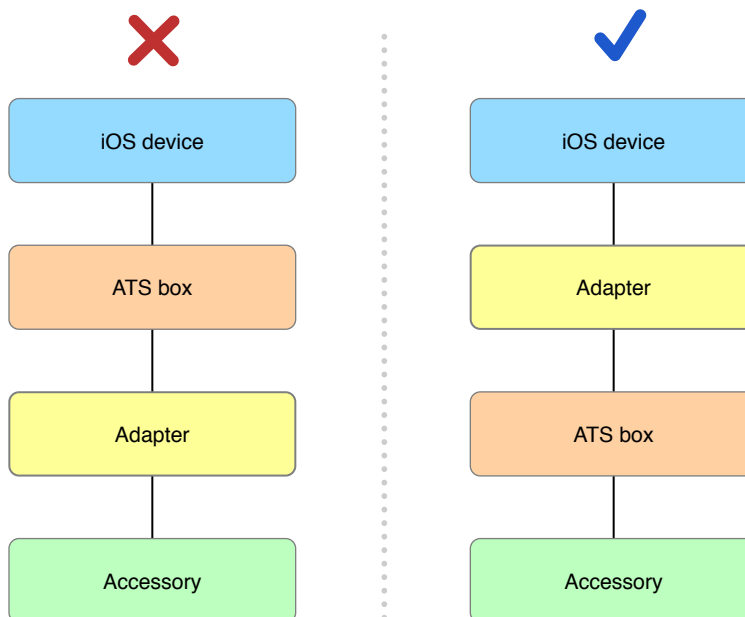
5.3 Connection Order

When attaching devices to the ATS 30-pin Box, the device must always be connected before connecting an accessory. For the ATS Lightning Box, the order is reversed: the accessory must be connected before the device is connected. Neither the accessory nor the device should be connected to the ATS Box when the capture begins.

> **Note: A Warning About the ATS Lightning Box When Connecting**
>
> The ATS Lightning Box Lightning connector must be plugged directly into the device. Once inserted, do not torque the Lightning connector. Improper use may result in the breakage of the ATS Lightning Box or device.

5.4 Accessory Connection Orientation

Although the Lightning connector supports multiple orientations, the ATS Lightning Box requires that the connector be inserted in a specific orientation. When connecting your accessory to the ATS Lightning Box, ensure that the light next to the accessory connector is green and not red. If red, turn the connector over and re-insert.

5.5 ATS Lightning Box without USB Traffic

When configuring a capture with the ATS Lightning Box and with an accessory which does not use USB, the Total Phase Beagle USB 480 analyzer must not be physically connected to the ATS Lightning Box. Connection of a Beagle USB 480 analyzer will prevent accurate voltage measurements of the D+/D- lines and prevent correct operation of brick detection and load testing.

5.6 Capturing iAP-over-Bluetooth

To begin a Bluetooth capture, a link key is required. The ATS Utility app provides link keys See ATS Utility (page 57).

When configuring a capture with a ComProbe BPA analyzer make sure to turn the device's Bluetooth off before starting the capture. Once the capture has begun, turn the device's Bluetooth back on, connect to your accessory, and begin using it.

Due to the inherent nature of capturing data wirelessly, ATS may not be able to always correctly capture the communication between the device and accessory. If there is too much RF interference, or the device and accessory are placed incorrectly with respect to the ComProbe BPA analyzer you may see missing Bluetooth data in the ATS trace. To help alleviate these issues make sure that the ComProbe BPA analyzer, device, and accessory are placed to form an equilateral triangle during capture. You should also make sure that the RF environment is free of noise by turning off other devices or equipment that may use the 2.4 GHz frequency range for features such as Wi-Fi and Bluetooth.

> **Note: Reducing RF Interference with Shielding Cloth**
>
> If excessive RF noise is interfering with ATS's ability to capture iAP traffic, consider using RF shielding cloth to protect your test environment.

> **Note: ATS Only Supports One ComProbe BPA analyzer**
>
> ATS only supports one active ComProbe BPA analyzer capture at a time. Starting a second ComProbe BPA analyzer capture before stopping the first one may result in unexpected behavior.

Note: iAP Detection and SDP

ATS relies on seeing a Service Discovery Protocol (SDP) exchange during the capture in order to determine which RFCOMM channel contains iAP. If SDP is not seen, an info message will be posted when an RFCOMM channel opens informing you that ATS may be ignoring an iAP channel. This is *not* an indication of bad behavior, but rather a technical limitation of the capture environment.

6. ATS User Interface

6.1 Views

6.1.1 Capture Document

The main window of the ATS application consists of a set of buttons, menu items and controls, plus a real-time display of hardware-related messages and iAP traffic.
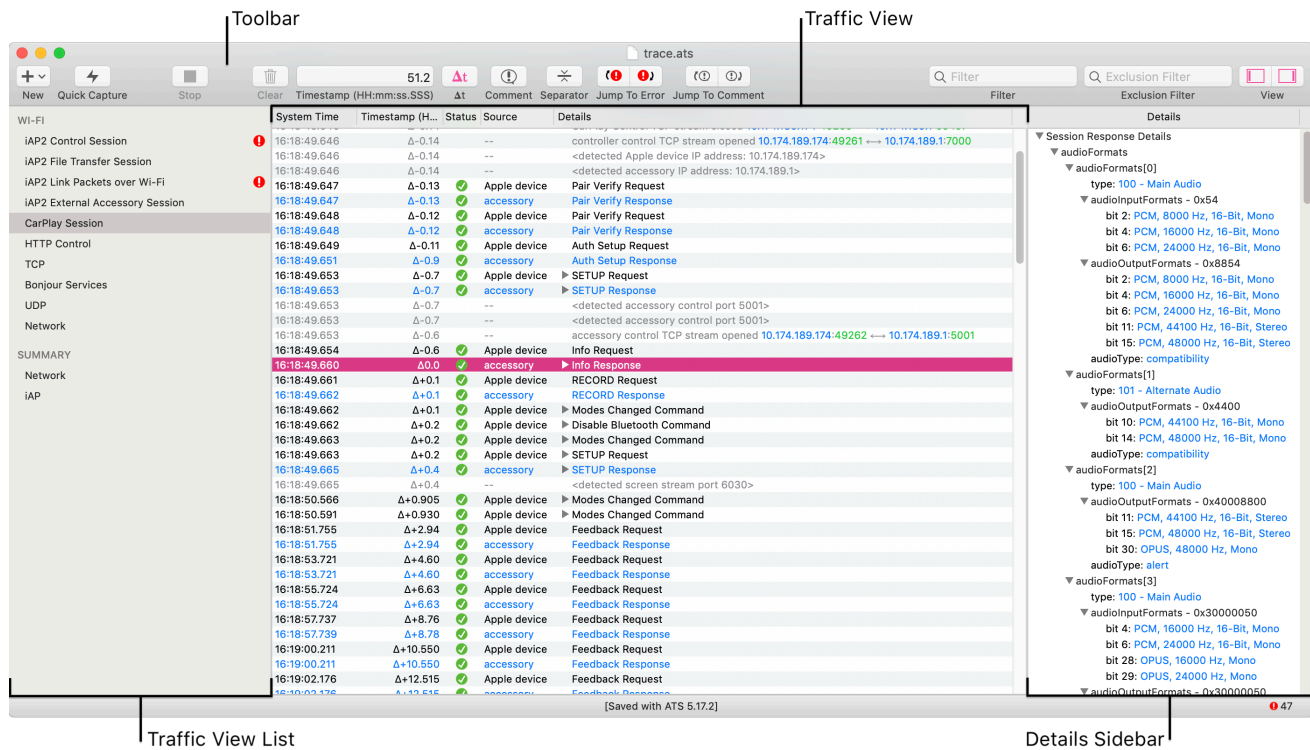
Analysis begins immediately after the document is created through the "New ATS Capture" window; it is invoked via File > New > Capture…, or by pressing Command-N.

Note: Quick Capture

There's a quick and convenient way of starting a capture. Either select click on the Quick Capture toolbar item, or go to File > New > Quick Capture, or press Command-Shift-N. A new Capture Document will be created and automatically connect to the first available capture device(s) using your previous capture settings.

The Capture Document toolbar contains several buttons and fields, outline in Table 6-1 (page 29).

Table 6-1   Toolbar Item Descriptions

Toolbar Item	Description
New	Configure and start a new capture via the "New ATS Capture" window.
Quick Capture	Start a capture immediately using the previous capture configuration.
Stop	Stop the active capture.
Clear	Clear the traffic that is currently shown. Only works during live capture. Does not permanently delete the traffic as it is needed for analysis.
Timestamp	Shows the timestamp of the currently selected row in the Traffic View. Can also be used to type in a timestamp to jump to the nearest matching row.
Δt	Toggles the "delta-timestamp mode" where the timestamp column displays the time difference between the selected row and other rows.
Comment	Inserts a comment annotation below the currently selected row.
Separator	Inserts a separator annotation below the currently selected row.
Jump To Error	Selects the next or previous error in the trace.
Jump To Comment	Selects the next or previous annotation in the trace.
Filter	You can filter for strings that occur in a row. A "match" occurs when all search terms are found in the row text (including child rows); matching search terms is irrespective of their ordering. Input multiple search terms using spaces, group search terms inside of quotes for exact sequential matches. e.g. `The brown fox` will match any rows that include "the" and "brown" and "fox"; searching for `The "brown fox"` will match rows that include "the" and "brown fox".
Exclusion Filter	Behaves the same way as the Filter but excludes the matches from the results.
View	Click on either segment to reveal either the Traffic View List or Details Sidebar.

Note: A Warning About Timestamps

The ATS Box and the Total Phase Beagle USB 480 analyzer have separate, unrelated clocks. ATS does not synchronize timestamps between the ATS Box and the Beagle USB 480 analyzer. Timestamps from any of the ATS Box traffic views cannot be reliably correlated with timestamps from any of the Beagle USB 480 analyzer traffic views. For example, you cannot reliably correlate the arrival of an "Accessory Detect" event in the iAP Packets over UART traffic view with the arrival of an iAP packet in the iAP Packets over USB HID view.

6.1.2 Traffic Views

Once a capture has begun, a list of traffic views will be displayed along the left side of the capture document. These enable you to review the behavior of your accessory in different ways. Some views will only be displayed under certain circumstances. For example, the "iAP Packets over USB HID" traffic view is only available when capturing that type of traffic. Possible traffic views include:

- iAP Packets over UART
- iAP Packets over USB HID
- iAP Packets over USB Bulk Pipe
- iAP Packets over Bluetooth
- iAP2 Control Session
- iAP2 File Transfer Session
- iAP2 External Accessory Session
- iAP2 Link Packets over UART
- UART Native HID
- iAP2 Link Packets over Wi-Fi
- CarPlay Session
- HTTP Control
- PTP Messages
- TCP
- Bonjour Services
- UDP
- Network
- NCM
- iAP2 Link Packets over USB HID
- USB HID Reports for iAP
- USB Transfers
- USB Transactions
- USB Packets
- iAP2 Link Packets over Lightning Audio
- Lightning Audio HID
- Lightning Audio External Accessory Session
- iAP2 Link Packets over Smart Connector
- Smart Connector Native HID
- Smart Connector External Accessory Session
- Measurements
- iAP Summary
- Hardware Summary
- Network Summary

The Traffic View List may be hidden by clicking on the left segment of the "View" button in the toolbar.

6.1.3 iAP Packets and iAP2 Control Session Traffic Views

Four types of iAP Packet traffic views may be available depending upon your configuration:

- iAP Packets over UART
- iAP Packets over USB HID
- iAP Packets over USB Bulk Pipe
- iAP Packets over Bluetooth

When using iAP2 the following traffic views may also be available:

- iAP2 Control Session over UART
- iAP2 Control Session over USB HID
- iAP2 Control Session over USB Bulk Pipe
- iAP2 Control Session over Bluetooth

The primary purpose of these traffic views is to display iAP packets, iAP2 messages, errors and warnings. Depending on your configuration you may see connection information as well. For example, in the iAP Packets over UART traffic view, you may see device or accessory connection information. In iAP Packets over USB, you may see USB reset information.

Note: Missing iAP Packets Over USB?

ATS does not thoroughly validate USB level information. It only captures enough USB information to assemble iAP packets. If you expect to see iAP over the USB transport but see none, check whether ATS displays error messages in any of the USB traffic views. If so, exit ATS and use the Total Phase Data Center application to debug your accessory's USB communication.

6.1.3.1 Fields in iAP2 Control Session Traffic Views

The iAP2 Control Session traffic views include a number of descriptive fields for iAP2 Control Session traffic observed by ATS.

The "Timestamp" field provides an absolute timestamp for each event. (Review the warning about timestamps above.)

The "Status" field can indicate whether a problem occurred with each particular event.

The "Source" field describes the source of the traffic. For iAP2 traffic, this will be either "Apple device" or "accessory" depending on which device sent the packet. For hardware-level notifications, such as those alerting the ATS application that a device has been attached or removed, the source will read "ATS Lightning Box".

The "Name", and "Description" fields provide a human-readable description of the contents of each iAP2 message or hardware-level event.

6.1.3.2 Fields in iAP Packet Traffic Views

The iAP Packet Traffic Views include a number of descriptive fields for iAP traffic observed by ATS.

The "Timestamp" field provides an absolute timestamp for each event. (Review the warning about timestamps above.)

The "Status" field can indicate whether a problem occurred with each particular event.

The "Source" field describes the source of the traffic. For iAP traffic, this will be either "device" or "accessory" depending on which device sent the packet. For hardware-level notifications, such as those alerting the ATS application that a device has been attached or removed, the source will read "ATS".

The "Lingo", "Command", and "Description" fields provide a human-readable description of the contents of each iAP packet or hardware-level event.

Note: groupBy Default, Sync Bytes are not Displayed

By default, any extra-packet 0xFF sync bytes (used to wake the device or otherwise) do not appear in the packet view. You may configure ATS to display these bytes in the ATS preferences.

6.1.4 CarPlay

6.1.5 CarPlay Control Session and Network Traffic Views

The following traffic views are available when capturing CarPlay session:

- CarPlay Session
- HTTP Control
- TCP
- Bonjour Services
- UDP
- Network
- NCM (CarPlay-over-USB only)

6.1.5.1 CarPlay Session and HTTP Control

The CarPlay Session traffic view displays CarPlay messages exchanged between the device and the accessory. The HTTP Control traffic view displays the HTTP requests and responses from which the CarPlay Session data is parsed.

6.1.5.2 TCP, UDP, Bonjour Services, Network, and NCM

The TCP and UDP traffic views display TCP packets and UDP datagrams exchanged during a CarPlay session. The Bonjour Services traffic view displays the Bonjour service instance that the CarPlay accessory is advertising on the network. The Network traffic view displays an even more complete picture of the network traffic by including Bonjour records and ethernet frames not associated with a TCP or UDP stream. The NCM traffic view displays individual NCM transfer blocks. The NCM traffic view is only seen in CarPlay-over-USB captures.

6.1.6 AirPlay 2

6.1.7 AirPlay 2 Network Traffic Views

The following traffic views are available when capturing AirPlay 2 session:

- HTTP Control
- PTP Messages
- TCP
- Bonjour Services
- UDP
- Network

6.1.7.1 HTTP Control

The HTTP Control traffic view displays the HTTP requests and responses exchanged during an AirPlay 2 session.

6.1.7.2 PTP Messages

The PTP Messages (Precision Time Protocol) traffic views displays the Event and General messages exchanged between the device and the accessory to synchronize their clocks during an AirPlay 2 session.

6.1.7.3 TCP, UDP, Bonjour Services, and Network

The TCP and UDP traffic views display TCP packets and UDP datagrams exchanged during an AirPlay 2 session. The Bonjour Services traffic views displays all the Bonjour service instances that all the accessories on the network are advertising. The Network traffic view displays an even more complete picture of the network traffic by including Bonjour records and ethernet frames not associated with a TCP or UDP stream.

6.1.8 iAP2 File Transfer Session Traffic View

The iAP2 File Transfer Session traffic view displays data from the iAP2 File Transfer Session declared during iAP2 link synchronization.

## 6.1.9 iAP2 External Accessory Session Traffic View

The iAP2 External Accessory Session traffic view displays data from the iAP2 EA Session declared during iAP2 link synchronization.

> **Note: External Accessory Native Transport**
>
> ATS does not capture External Accessory Native Transport (USB Host Mode) data, and therefore the External Accessory Session traffic view will remain blank in this configuration. ATS will, however, validate the accessory's configuration with this setup.

6.1.10 Measurements View

The Measurements view provides a way of visualizing the behavior of the device and your accessory over time. This view is only available when using the ATS 30-pin Box.
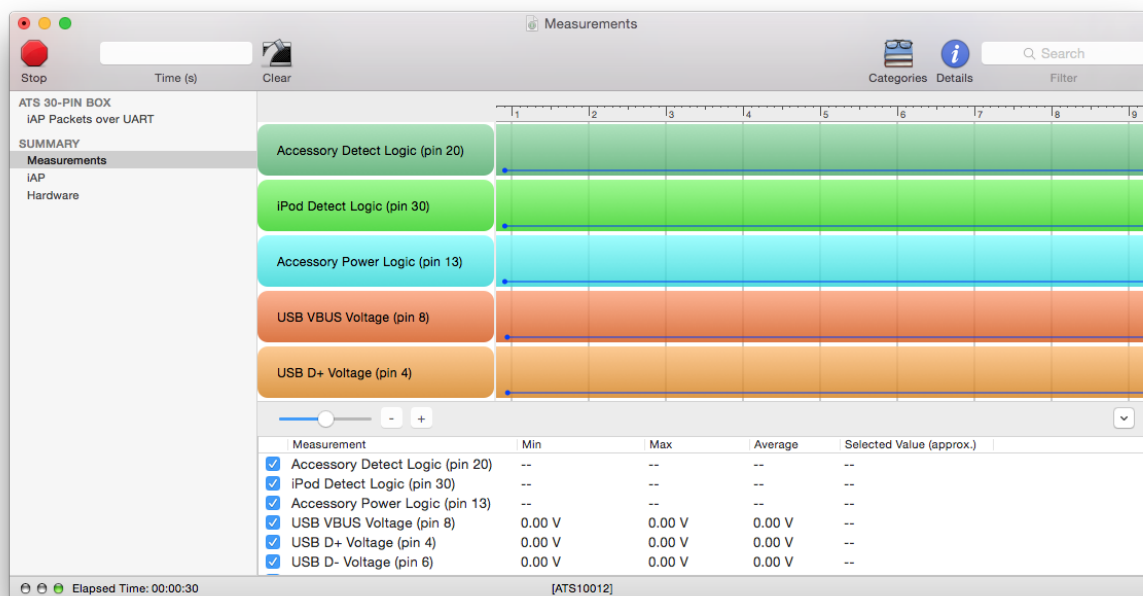
The Measurements view provides a graphical area that shows various pin states over time. Below the graphical area is a summary of each pin state, their minimum, maximum and average values. The value of each pin at a particular time can be shown by clicking any point within the graphical area.

The "Clear" button affects the Measurements view in the same manner as the traffic views.

Note: High Impedance

High impedance is displayed in the Measurements view as "inf kΩ," an abbreviation for "infinite kilo-ohms."

6.1.11 Hardware View

The Hardware view provides a real time summary of various hardware related information observed during the capture.

6.1.11.1 Electrical (ATS Lightning Box)

The "Electrical" section of the Hardware view contains observations about the electrical behavior of the accessory. It contains the following information:

Electrical

Power to Accessory		
Voltage	0.00 V	
Current	0 mA	
Power	0.0 W	

USB Power Brick Detection

USB Vbus	5.09 V	
USB D+ (220kΩ shunt to ground)	2.48 V	
USB D+ (220kΩ shunt to vcc)	2.79 V	
USB D- (220kΩ shunt to ground)	1.80 V	
USB D- (220kΩ shunt to vcc)	2.19 V	
Brick Detect:	2.1 A USB power brick	

Power to Apple device

Voltage	5.07 V
Current	22 mA
Power	0.1 W

Lightning Module

Functional Variant B - USB Device Mode
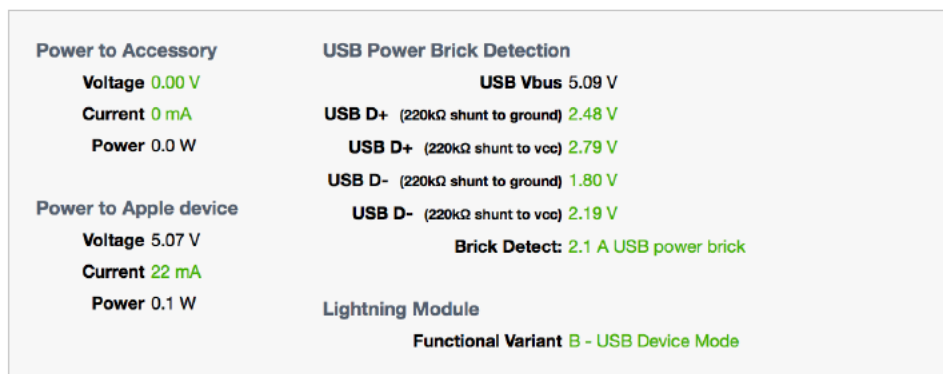
6.1.11.2 Electrical (ATS 30-pin Box)

The "Electrical" section of the Hardware view contains observations about the electrical behavior of the accessory. It contains the following information:

Electrical

Accessory detect (pin 20)		Pin Voltages	
State floating		**FW (pins 11/12)** 0.00 V	
Ground count 0		**USB Vbus (pin 8)** 0.00 V	
Float count 0		**USB D+ (pin 4)** 0.00 V	
		USB D- (pin 6) 0.00 V	
ID resistor (pin 10)		**Tx-to-iPod (pin 18)** 0.00 V	
State floating		**Reserved (pin 14)** floating	
		Reserved (pin 17) floating	
Accessory Power (pin 13)			
Current 0.00 mA (1 sec average)			

The "accessory detect" section counts the number of rising and falling edges on pin 20 of the 30-pin connector. This information may help detect failures or inconsistencies in how an accessory drives this pin, which should typically be grounded.

The "ID resistor" section reports the accessory ID resistor value on pin 10 measured by the ATS 30-pin Box, and also displays how close the value is to the nominal value for a given accessory type. Due to measurement resolution, the exact numerical value that is displayed may differ slightly from what is in the circuit.

The "accessory power" section shows the average accessory current consumption during the most recent one second. Individual current samples are taken at a rate of approximately 500 Hz.

The "pin voltages" section reports the voltages present on the FireWire, USB Vbus, USB D+ and USB D- pins. Non-zero FireWire voltages are displayed in red as a reminder that FireWire-based charging is no longer allowed for new accessory designs. If the three USB voltages are all within specification for a 500 mA, 1 A, or 2.1 A charging accessory, this fact will be noted below the voltages. For USB D+ and D- voltage measurements to be made, no device may be connected. This ensures that if an iAP-over-USB accessory happens to be connected to the ATS 30-pin Box, it will not have its USB signal integrity affected by attempts by the ATS 30-pin Box to measure its USB D+ and D- voltages as though it were a USB charging accessory.

The "Tx-to-iPod (pin 18)" field reports the voltage on the accessory UART transmit pin. Voltages outside of the legal range for the marking-high/idle state will be shown in red.
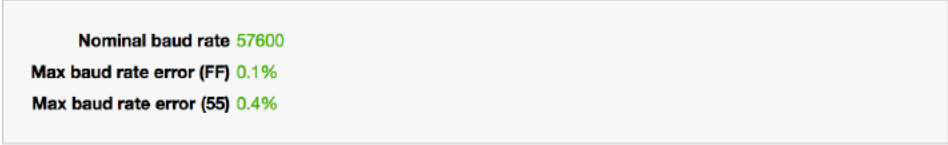
The "Reserved (pin 14)" and "Reserved (pin 17)" fields report whether the accessory incorrectly drives or correctly leaves as floating the two 30-pin connector pins marked as reserved for future use.

The "Nominal baud rate" field is determined by looking for standard baud rates in the vicinity of the actual baud rates measured for iAP traffic from the accessory. Only 19200 bps and 57600 bps are allowed for new accessory designs, so rates other than these will be shown in red.

6.1.11.3 UART Transport

The "Serial Transport" section of the Hardware view contains statistics about the quality of the UART data transmitted by the accessory. It includes the following information:

Serial Transport

Nominal baud rate	57600
Max baud rate error (FF)	0.1%
Max baud rate error (55)	0.4%

The two "Max baud rate error" fields latch the highest observed deviations from the nominal baud rate, according to both the 0xFF (start-bit) and 0x55 methods. A worst-case deviation between 2% and 3% is shown in yellow. A worst-case deviation beyond 3% is shown in red. Significant deviation of these values from nominal typically indicates firmware and/or hardware problems with an accessory.

6.1.12 Summary View

The Summary view displays sections which provide real time accessory information as a high level overview of the events seen.

All fields in the Summary view sections can be reset with the "Clear" toolbar button.

6.1.12.1 iAP Section

The iAP view provides real time information about the state of iAP.

6.1.12.2 Identification (iAP2) Section

The "Identification" section of the iAP view summarizes accessory identification information, providing useful excerpts from the latest information available. This includes the following:

6.1.12.3 Identification (iAP1) Section

The "Identification" section of the iAP view summarizes both device and accessory identification settings, preferences, and other information. It includes the following information:

The "Lingoes used" field provides a bit-field summarizing all lingoes for which the accessory has sent at least one packet.

The "Lingoes ACK'd" field provides a bit field summarizing all lingoes for which the device has sent a positive (successful) acknowledgement back to the accessory. Because not all lingoes include ACK commands, these two fields will not, in general, be the same. (Each offers a particular kind of iAP traffic summary, which may or may not be relevant to the problem at hand.)

The "iPod SW" field shows the version information sent by the device in response to GetiPodSoftwareVersion.

The "Bundle Seed ID" field shows the application ID provided by the accessory.

The "EA protocol" shows the reverse domain name protocol name representing the External Accessory framework protocol that the accessory supports.

The transaction ID state represents whether ATS expects to see transaction IDs.

The "Accessory info" fields provide human-readable description of all information returned by the accessory via RetAccessoryInfo iAP packets.

The Lingo usage table indicates whether each lingo has been identified for and its version information sent by the device in response to RequestLingoProtocolVersion.

6.1.12.4 Authentication Section

The "Authentication" fields of the iAP view provide the total elapsed time taken to complete authentication (for iAP only), as well as the level of authentication used and (in the case of level 2 authentication) the serial number and class of the authentication coprocessor IC. The total elapsed time is defined to start with the accessory's IdentifyDeviceLingoes packet and to end with the device's successful acknowledgement of authentication via a RetDevAuthenticationStatus packet.

Authentication

Version	--
Certificate Serial	--
Certificate Description	--
Elapsed Time	--

6.2 Copying Trace Data

Information from the traffic window may be copied and pasted into other applications. The Copy action can be invoked via either Edit > Copy, the contextual menu (right-click) or via the Command-C shortcut. Selected rows in the traffic view will be turned into text and copied into the pasteboard. This is a convenient way to reference test results in email.

6.3 Error Reporting

As ATS detects accessory errors, it adds feedback in the main traffic window. A more detailed view of each message is available in the "Details" pane of each traffic view.

The bottom right corner of the Capture Document will also provide a count of all the errors and warnings in the trace (not limited to the errors in the currently selected traffic view).
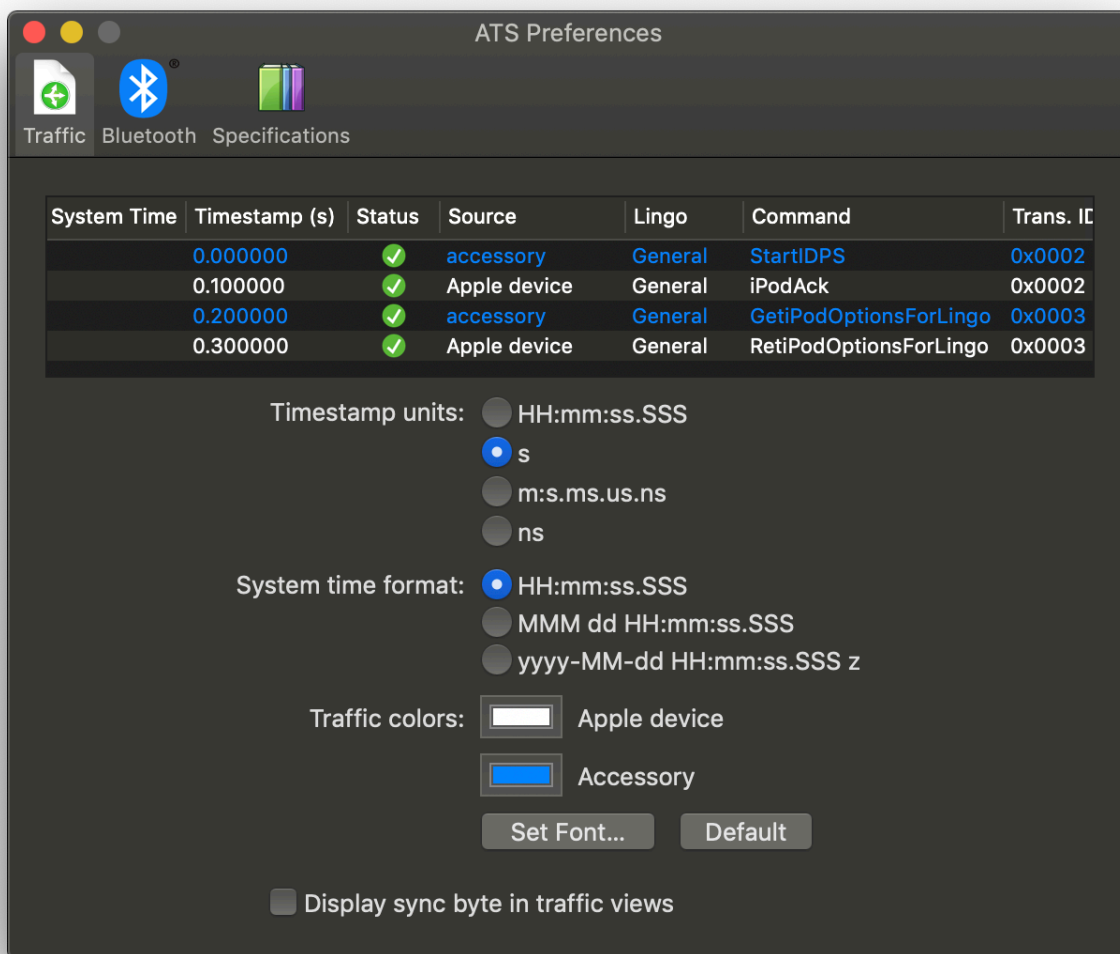

6.4 Preferences

The ATS preferences pane provides the ability to customize ATS's behavior. The preferences are accessible under the ATS menu.

6.4.1 Traffic Preferences

The "Timestamp units" setting gives you the ability to change the format of the timestamps shown in any of the traffic views. The available options are:

Table 6-2   Timestamp units options

Option	Description
HH:mm:ss.SSS	(default) display the time expressed in hours : minutes : seconds . milliseconds
s	display the time expressed in number of seconds
m:s.ms.us.ns	display the time in units separated into minutes : seconds . milliseconds . microseconds . nanoseconds
ns	display the time expressed in number of nanoseconds

The "System time format" preference allows you to change the format of the System Time column in all of the traffic views. The available options are:

Table 6-3   System time format options

Option	Description
HH:mm:ss.SSS	display the system time
MMM dd HH:mm:ss.SSS	display the system date and time
yyyy-MM-dd HH:mm:ss.SSS z	display the system date and time in GMT timezone format

The "Traffic Colors" preference allows you to change the color of iAP and CarPlay packets shown in any of the traffic views based upon their source.

The "Set Font…" button allows you to change the font, size and styling of the text used in the traffic views. The Default button reverts this setting back to its original state.

6.4.2 Bluetooth Preferences
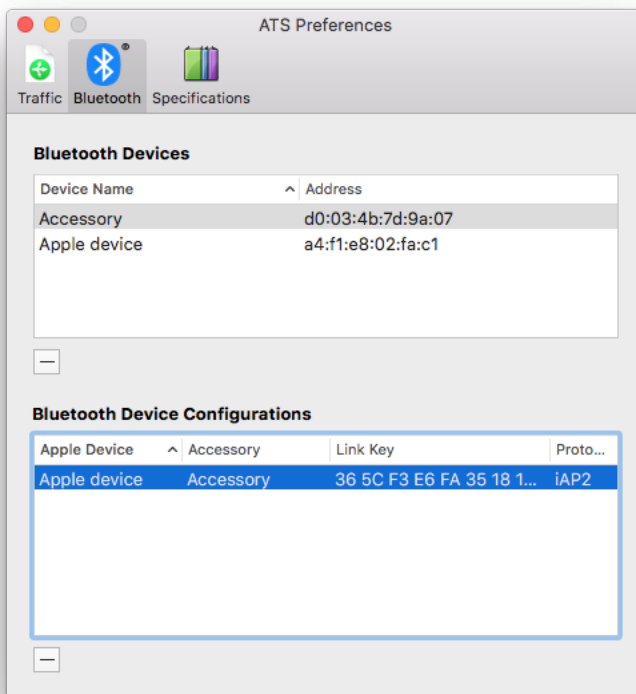
The "Bluetooth Devices" table displays all of the stored Bluetooth devices that have been seen during device inquiry. You can delete unwanted Bluetooth devices by selecting them in the table and clicking the "-" button below the table.

The "Bluetooth Devices Configuration" table displays all of the stored Bluetooth capture configurations. You can delete unwanted configurations by selecting them in the table and clicking the "-" button below the table.

The Link Key cell can be edited in this table. This is useful when the link key changes during a new pairing.

6.4.3 Specification Support

When an error is detected in an ATS capture, you can view the *Accessory Interface Specification* from within the ATS capture window to quickly look up the referenced topic.

The specification can be loaded in ATS by selecting an error in the ATS capture, or by clicking the "+" button in the ATS preferences pane, see Preferences (page 40). Similarly, the specification can be removed by clicking the "-" button below the table.

At this time this feature can be used to look up references for only iAP2 and CarPlay specification violations.

To load a specification from within an ATS capture window:

1. In an ATS capture, double-click on a row of traffic that contains an error. This will reveal the Details sidebar.
2. In the Details sidebar, locate section "Spec Reference". If you have not yet loaded a specification, you will see the text "You have not loaded any specs yet". Click the "Import specs…" link.
3. ATS Preferences will open. Click the "+" button at the bottom of the window.
4. Use the resulting Finder window to select your PDF copy of *Accessory Interface Specification*.
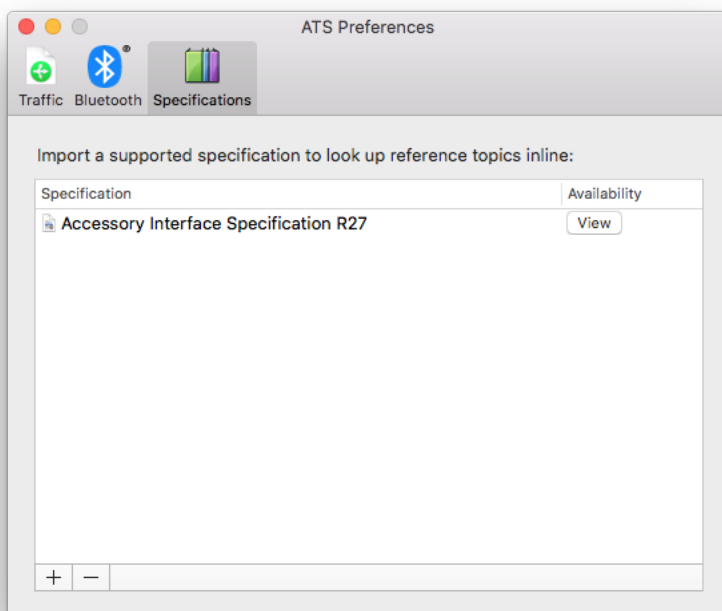
To view a specification reference from within an ATS capture window:

1. Return to the ATS capture window and double-click on a row of traffic that contains an error. This will reveal the Details sidebar.
2. In the Details sidebar, you will now see links to sections of the specification. Clicking links will open the relevant specification reference in new ATS window.

7. USB Vbus Load Test

For 500 mA, 1 A, 2.1 A, and 2.4 A Vbus charging accessories, you may invoke a test of your accessory's power supply by selecting "Run USB Vbus Load Test" under the "Capture" menu. This test will only run for accessories that present appropriate D+/D- resistors. Accessories that charge the device but do not present appropriate D+/D- resistors will not be able to use the USB Vbus Load Test. Additionally when using the ATS 30-pin Box, only a maximum of 1 A load will be applied during the test. For accessories capable of handling loads greater than 1 A, be sure to conduct additional load testing outside of ATS. Disconnect any device before running this test.
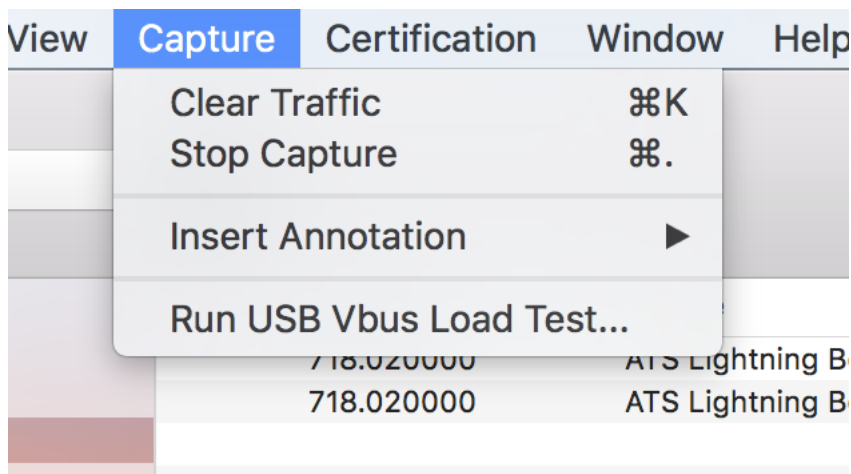
The USB Vbus Load Test is run inside of an existing Capture Document. After the test has completed, check the trace for any errors that were thrown during the test. When using the ATS Lightning Box, a voltage summary will be displayed when the test completes.
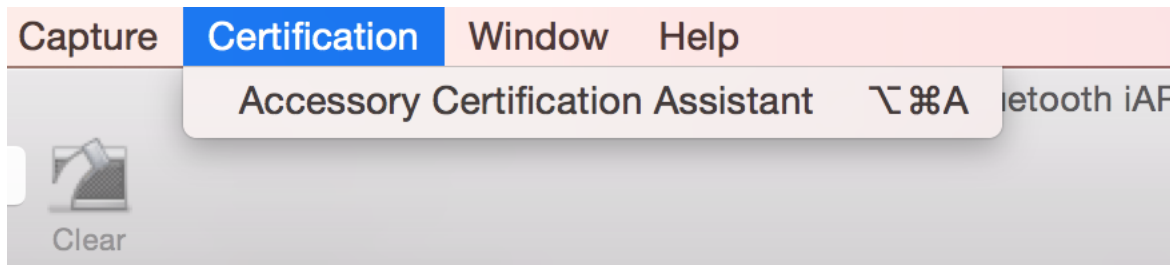
8. Accessory Certification Assistant

ATS allows you to run MFi self-certification tests and submit the results to Apple. To use the Accessory Certification Assistant, you must have an Apple ID and password that is registered with the MFi program. For help registering your Apple ID, contact your MFi Representative.

Note: Disclaimer

ATS is not a comprehensive certification solution. It is ultimately the accessory developer's responsibility to ensure the accessory complies fully with all specifications required for each product. If no errors are generated during the test procedure, it is neither guaranteed nor implied that the accessory has met all certification requirements.

The Accessory Certification Assistant is your guide for running MFi self-certification tests. You can access it via the Accessory Certification Assistant menu item in the Certification menu. Before running the assistant, make sure your computer is connected to the Internet.

The assistant will guide you through the process of configuring and running certification tests for your accessory. The first step is authentication.

You must be connected to the Internet to use the Certification Assistant. If you are not connected to the Internet, you will not be able to run any tests. The Certification Assistant connects to the ATS server over an SSL-encrypted secure connection. Make sure your firewall settings allow you to access the ATS server at:

- Domain: bogart.apple.com, selfcert.apple.com
- Port: 443

Note that ATS is not compatible with SSL proxies or virus scan systems that intercept the secure communication between ATS and ATS's backend systems.

Use your Apple ID credentials that were registered with the MFi program to access the Certification Assistant. For help registering your Apple ID, contact your MFi Representative.

Once you have logged in, you can create a new certificaton configuration, resume an existing one, or view the results from a past submission.

Note: Submission History Prior to ATS 5.7

If you have previously submitted self-certification test results with ATS 5.6 or earlier, those submissions will not be visible in ATS 5.7 or later.

8.1 Creating a New Certification Configuration

To create a new accessory certification configuration, choose "Create a new certification configuration" and click Continue. ATS will present you with a list of product plans that are ready for self-certification. If you just want to test your accessory in the Accessory Certification Assistant and don't want to submit your results, choose the "Test Mode" accessory.
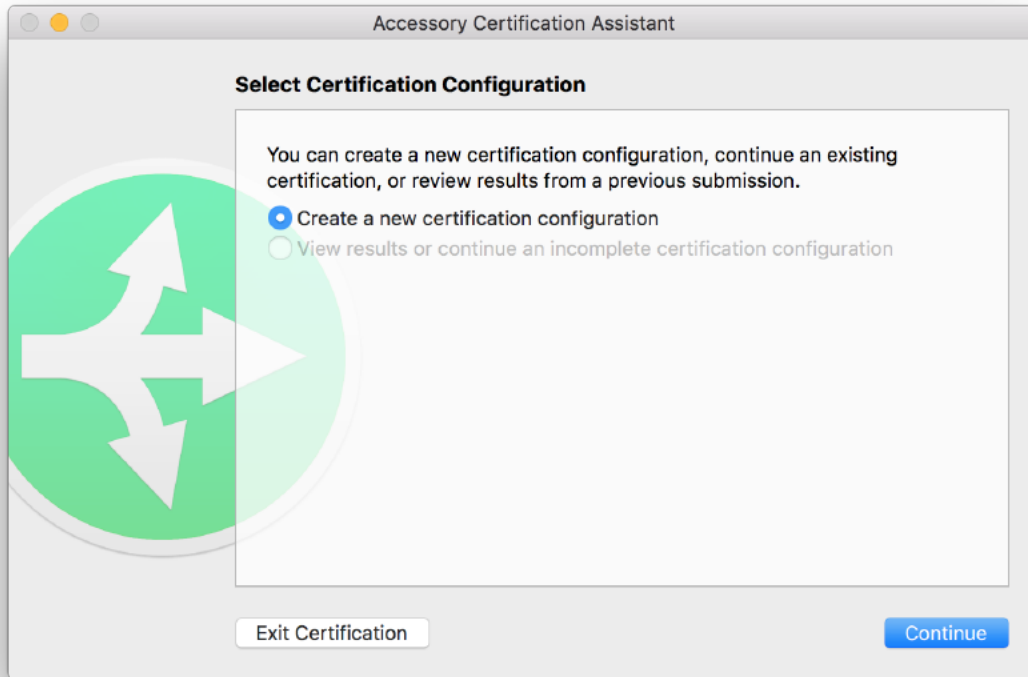
In order to validate the behavior of your accessory, ATS needs to know how it connects to devices and what features it uses or supports. ATS will ask you to specify all of the accessory's connectors.
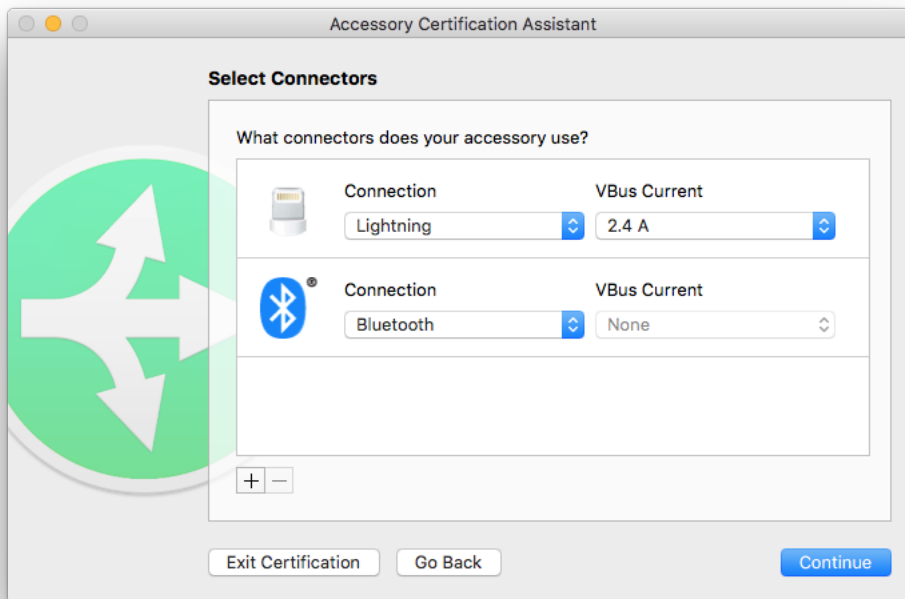
When ATS has collected all of the information it needs, it will present you with a review screen showing all of the details you specified. If you need to change any of the details, click "Go Back" one or more times to get to the configuration that you need to change. When everything is correct, click Continue to save your configuration and start testing.
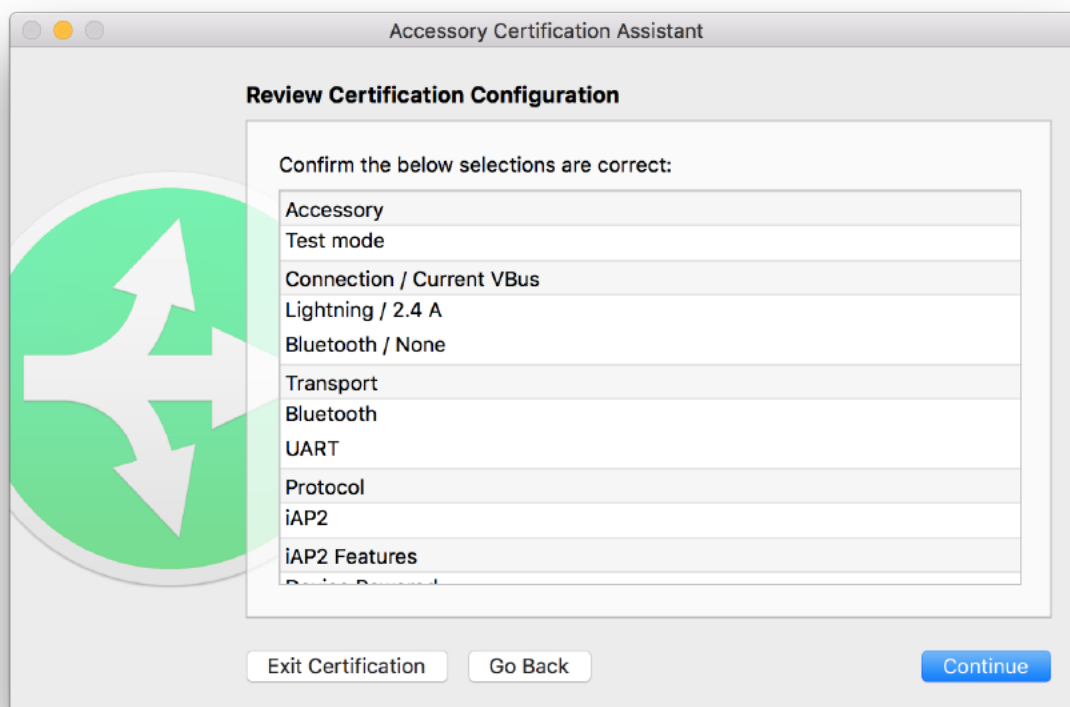
8.2 Testing Your Accessory and Submitting Results

The first screen you see when you begin testing is the Test Center. This screen presents a list of tests you will need to perform with your accessory and summarizes any test results that you have generated so far. You can perform the tests in any order, and you can repeat them as many times as you like. Only the most recent test results will be included when you submit your test data to Apple.

Every time you complete a test, ATS will return you to the Test Center. When you have completed all tests, the Test Center will present a button allowing you to submit your results to Apple.
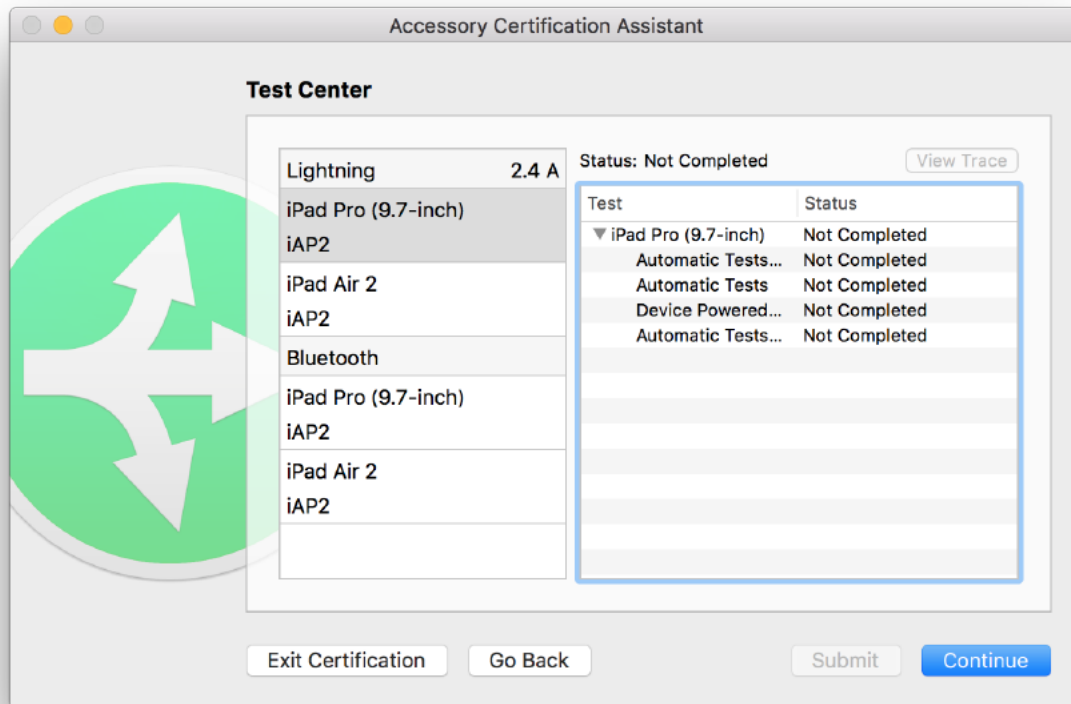
8.3 Reviewing Past Submissions

Test data submitted with ATS 5.7 or later can be viewed: select the submission in the Select Certification Configuration screen and click Results.
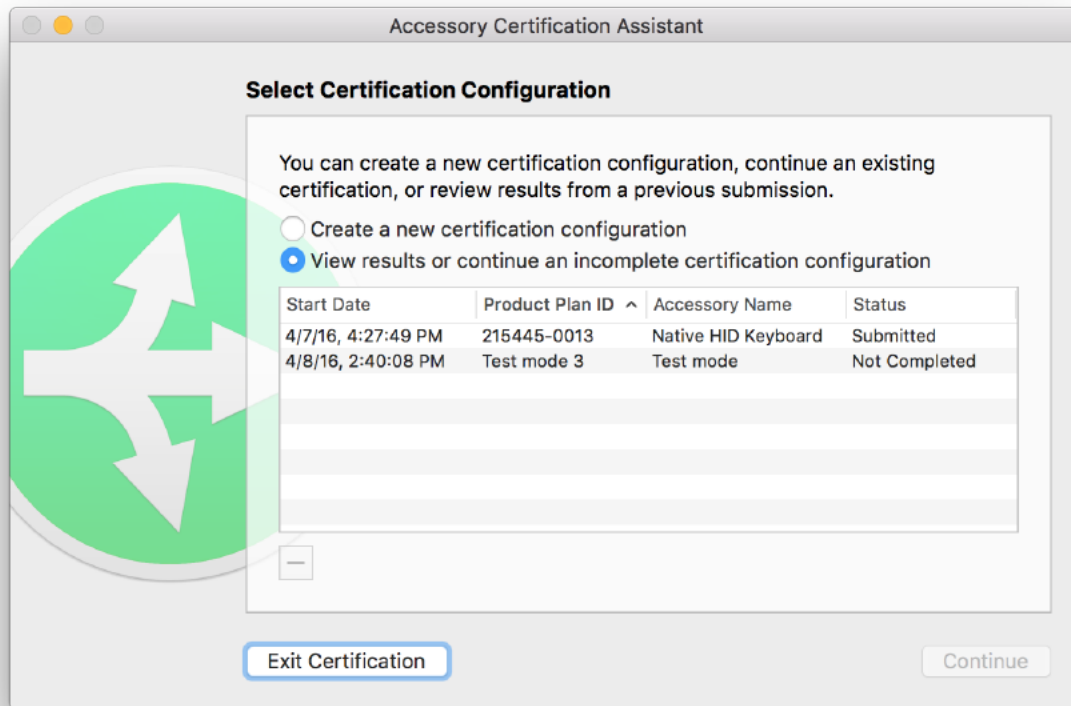
ATS will present a Submission Test Results window summarizing the contents of the submission. You can see individual test results in more detail by clicking on one of the View Trace buttons.

56

Certification Test Results

Product Plan ID: 106601-0158   Start Date: 6/20/16, 4:08:02 PM

Accessory Name: Bluetooth printer iAP2 t...   Status: Submitted

Accessory SKU: 7321

Test	Status	Trace
▼ Overall	Submitted	
▼ Power-only Lightning Configuration	Completed	
▼ iPhone 6s	Completed	View Trace
Automatic Tests (accessory only)	Completed	
Automatic Tests	Completed	
Automatic Tests (Apple Device only)	Completed	
▼ iPhone 6	Completed	View Trace
Automatic Tests (accessory only)	Completed	
Automatic Tests	Completed	
Automatic Tests (Apple Device only)	Completed	
▼ iPhone 5	Completed	View Trace
Automatic Tests (accessory only)	Completed	
Automatic Tests	Completed	
Automatic Tests (Apple Device only)	Completed	
▼ iPod nano 7G	Completed	View Trace
Automatic Tests (accessory only)	Completed	
Automatic Tests	Completed	
Automatic Tests (Apple Device only)	Completed	

9. ATS Utility

ATS Utility is an iOS application that runs on the device to facilitate various features in the ATS app. ATS Utility provides support for retrieving Bluetooth link keys created during Bluetooth pairing, enables sniffing CarPlay over Wireless traffic for iOS 9.2 or later, and performs network performance tests used for CarPlay certification. To use ATS Utility, you must use an Apple ID that's registered as an ATS user in the MFi Portal.

9.1 Software Installation

ATS Utility requires a device running iOS 9.2 or later. If needed, open the Settings app and choose General > Software Update to get the latest version of iOS. The latest version of ATS Utility is available for download from the MFi Portal.

To install ATS Utility on your device, follow these steps:

- On iTunes 12.6 or earlier:
    1. Uninstall any existing installation of the app.
    2. Download the "ATS Utility.zip" file from https://mfi.apple.com.
    3. Unzip the file.
    4. Drag "ATS Utility.ipa" into your iTunes app library.
    5. Sync "ATS Utility.ipa" to your device using iTunes.
    6. Trust the "Apple Inc. - Bluetooth Test Tool" enterprise distribution profile. On iOS 9.2 or later, open the Settings app and go to "General" > "Profile & Device Management" > "Apple Inc. - Bluetooth Test Tool" and tap "Trust".
- On iTunes 12.7 or later:
    1. Uninstall any existing installation of the app.
    2. Connect your device to your computer.
    3. Open iTunes. Locate your device in the left sidebar.
    4. Download the "ATS Utility.zip" file from https://mfi.apple.com.
    5. Unzip the file.
    6. On your computer, locate the "ATS Utility.ipa" that you want to install to your device.
    7. Drag "ATS Utility.ipa" from your computer to your device in the left sidebar of iTunes.
    8. Trust the "Apple Inc. - Bluetooth Test Tool" enterprise distribution profile. On iOS 9.2 or later, open the Settings app and go to "General" > "Profile & Device Management" > "Apple Inc. - Bluetooth Test Tool" and tap "Trust".

If you see an "Untrusted Enterprise App" alert, verify that you've followed the procedure described above to trust the provisioning profile.

9.2 Bluetooth Link Keys
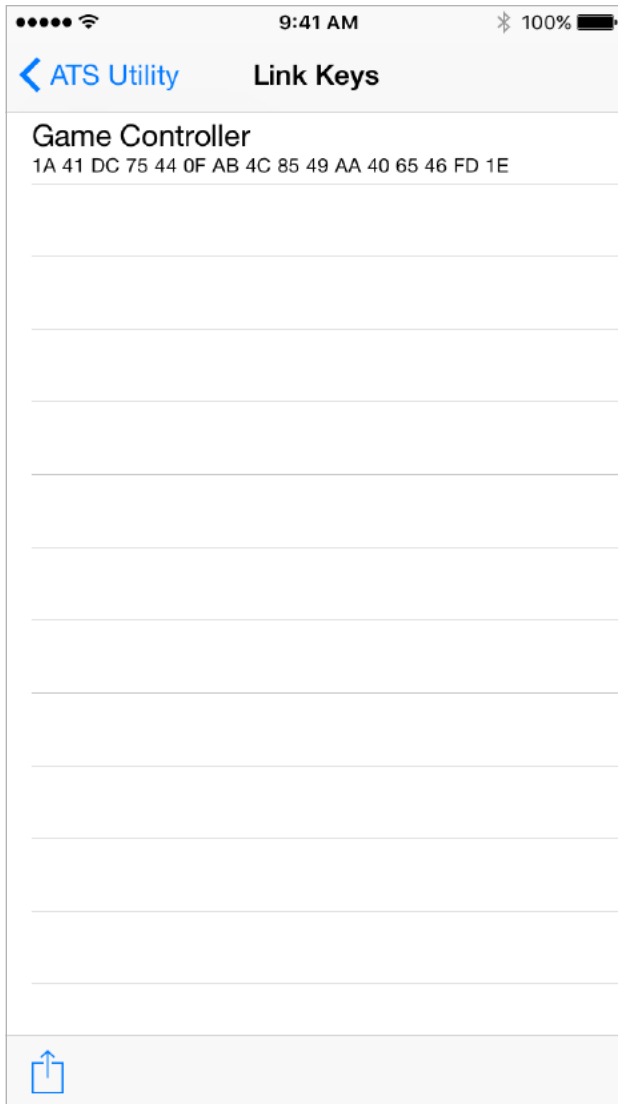
ATS Utility provides a table of Bluetooth accessories that the device has been paired with. The accessory's name is shown at the top of the row and the link key associated with that accessory is shown at the bottom. The table will only show accessories that advertise support for iAP (accessory includes the Service Class UUID for the iAP protocol in its Extended Inquiry Response packet). Double tapping on a row will bring up the accessory's MAC address.

Use this functionality of ATS Utility in ATS's "New ATS Capture" window when you are prompted to enter the Bluetooth link key.

9.3 CarPlay Performance Tests

CarPlay accessories must meet minimum network throughput and latency requirements in order to pass self-certification. ATS Utility includes an implementation of the Iperf network performance analysis tool that CarPlay accessory developers can use to verify that their accessory meets the minimum requirements. ATS Utility supports performance tests for CarPlay via USB and CarPlay via Wi-Fi.

Note: CarPlay Accessory Iperf Requirements

In order to support performance tests, the CarPlay accessory must have **Iperf 2.0.5** installed locally, and it must be capable of invoking Iperf in the manner described in the following sections.
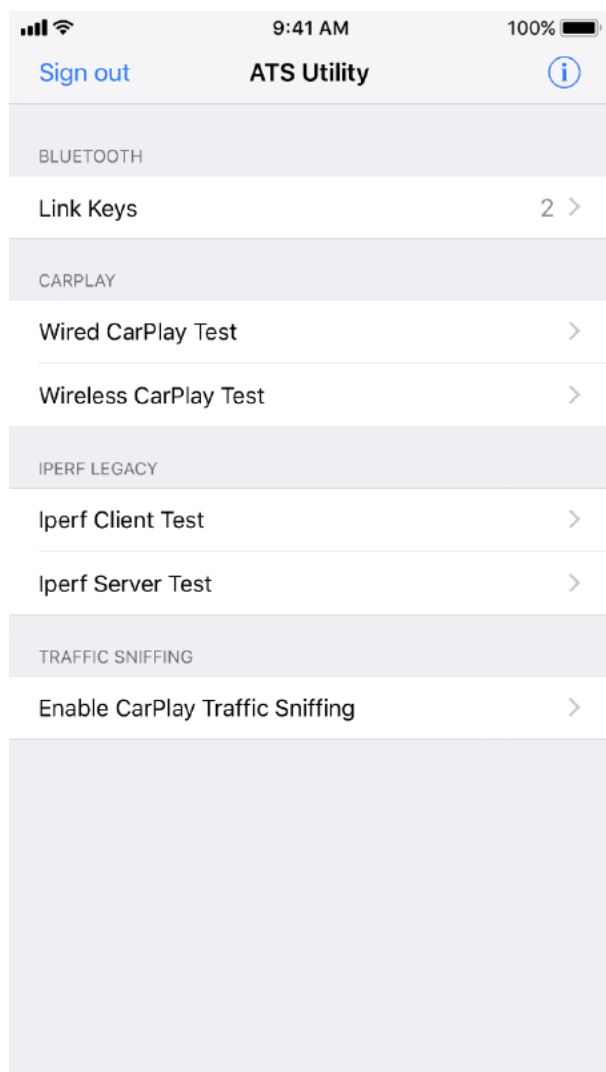
9.3.1 Wired Test

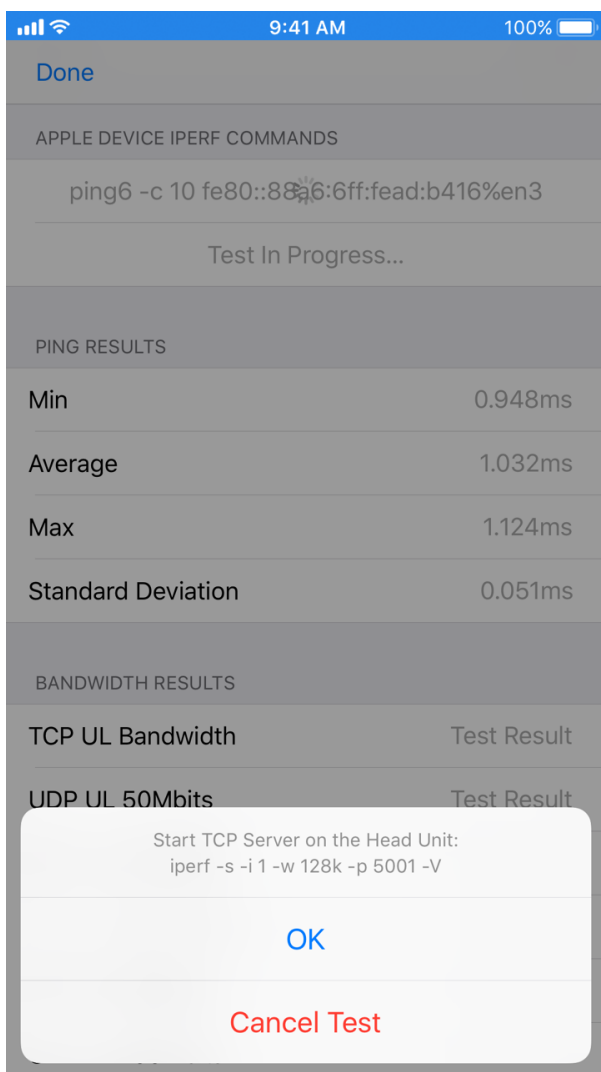### 9.3.1.1 Network Configuration

Tap on 'Wired CarPlay Test' to begin configuring an Iperf test in which the device acts as an Iperf client and connects to an Iperf server running on the CarPlay accessory. ATS Utility automatically populates the accessory IP address field with the appropriate address. Iperf client tests use IPv6 when connected to the CarPlay accessory via USB.
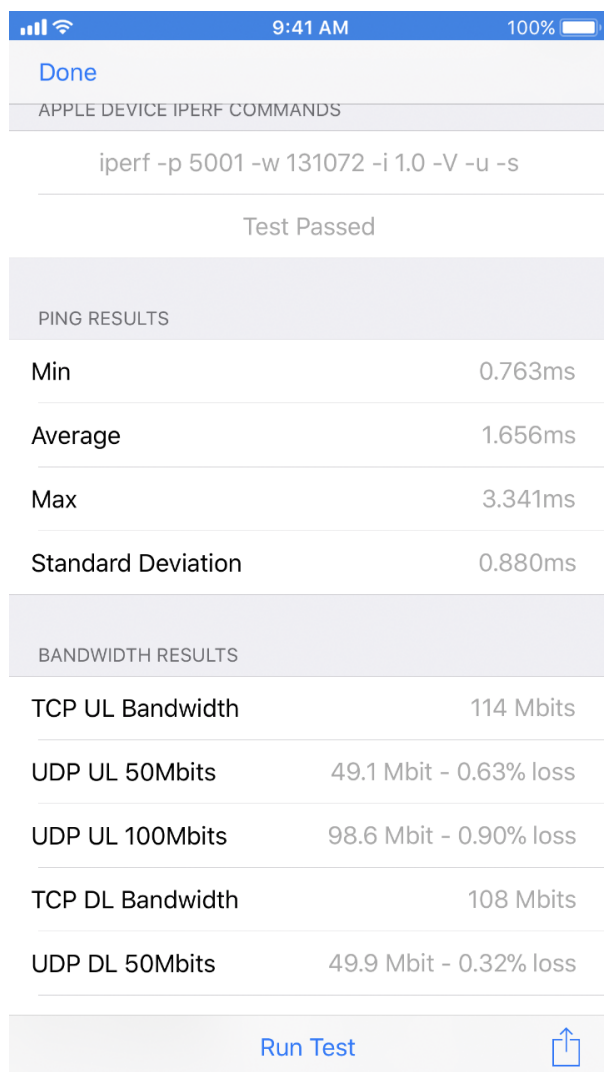
9.3.1.2 Running Wired CarPlay Test

ATS Utility will guide you step by step through the test. Follow displayed instructions to complete the test.

Note: Running IPv6 client on CarPlay Accessory

When running IPv6 client, make sure to replace network interface with CarPlay IPv6 interface after '%' sign in Iperf client command.


Upon succeessful test completion 'Test Passed' will be presented on the device. Use the share option to share the results, and upload 'WiredTestSummary.txt' and 'WiredTestSummary.sig' files for verification.

⠔ᯤ	9:41 AM	100% ▭

Done

APPLE DEVICE IPERF COMMANDS

iperf –p 5001 –w 131072 –i 1.0 –V –u –s

Test Passed

PING RESULTS

Min	0.763ms
Average	1.656ms
Max	3.341ms
Standard Deviation	0.880ms

BANDWIDTH RESULTS

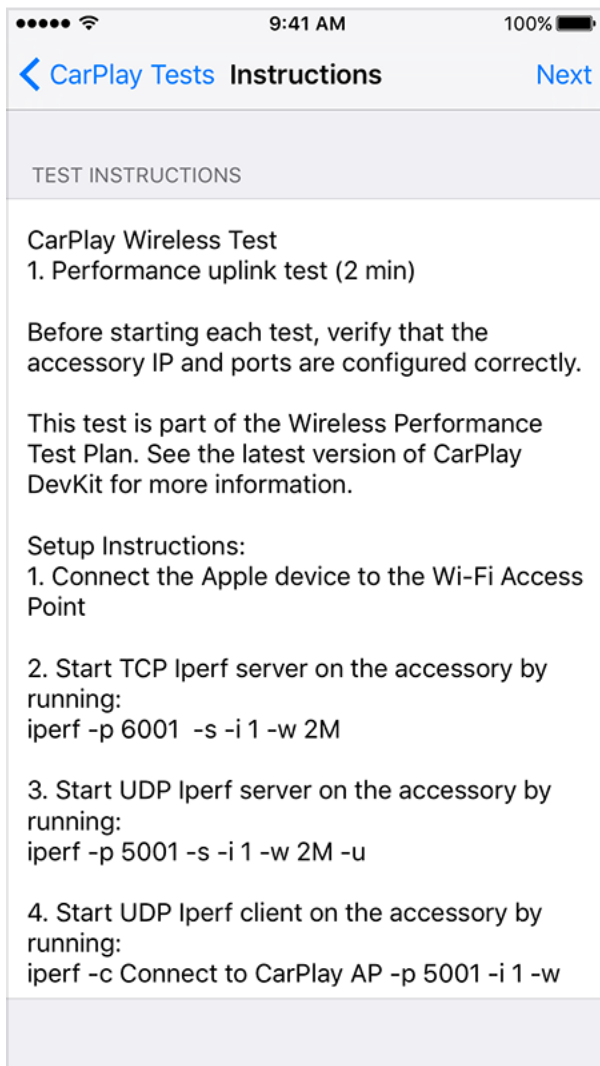| TCP UL Bandwidth	114 Mbits
UDP UL 50Mbits	49.1 Mbit - 0.63% loss
UDP UL 100Mbits	98.6 Mbit - 0.90% loss
TCP DL Bandwidth	108 Mbits
UDP DL 50Mbits	49.9 Mbit - 0.32% loss

Run Test ⬆

9.3.2 Wireless Tests

Tap on 'Wireless CarPlay Test' to begin configuring an Iperf test in which the device acts as both an Iperf client and an Iperf server. The device will connect to an Iperf server running on the CarPlay accessory and will simultaneously listen to Iperf client connections from the CarPlay accessory.
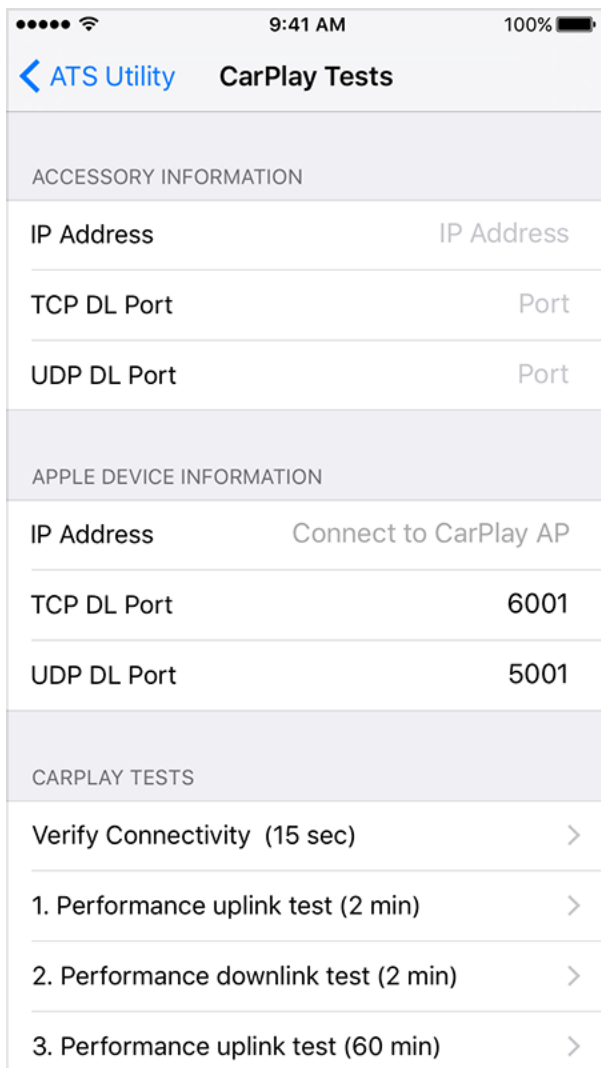
Use the CarPlay Tests screen to enter the details of the Iperf servers running on the CarPlay accessory (such as IP Address, TCP DL Port, and UDP DL Port). When connected to a CarPlay accessory, ATS Utility automatically populates the details of the Iperf servers running on the device (such as IP Address, TCP DL Port, and UDP DL Port). Wireless CarPlay tests use IPv4 when connected to the CarPlay accessory via Wi-Fi.

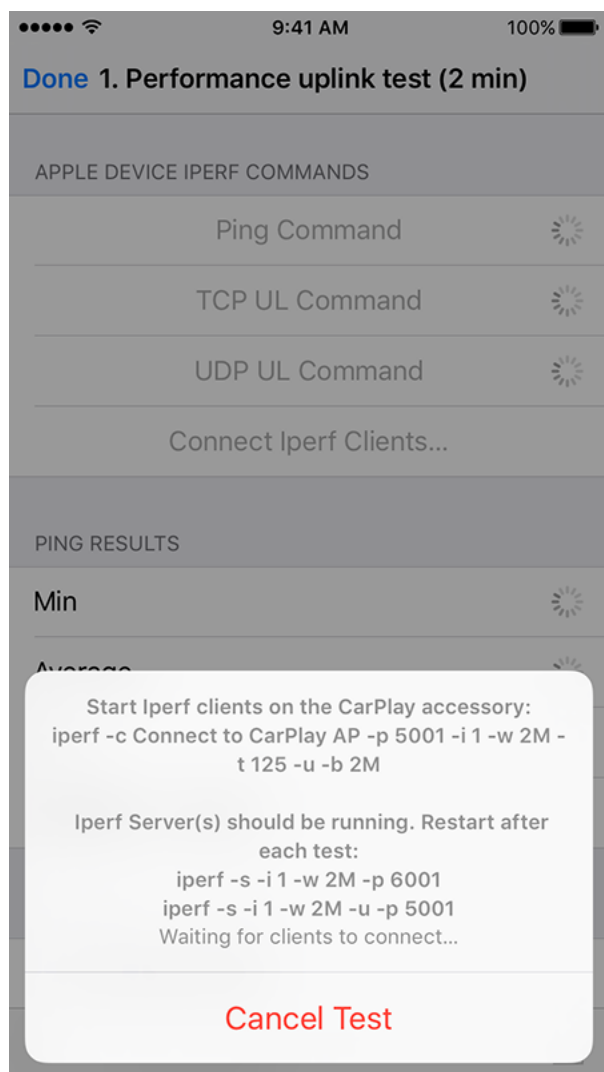Tap on one of the CarPlay tests to start a performance test.

●●●●● 📶   9:41 AM   100%

‹ CarPlay Tests **Instructions**   Next

TEST INSTRUCTIONS

CarPlay Wireless Test
1. Performance uplink test (2 min)

Before starting each test, verify that the
accessory IP and ports are configured correctly.

This test is part of the Wireless Performance
Test Plan. See the latest version of CarPlay
DevKit for more information.

Setup Instructions:
1. Connect the Apple device to the Wi-Fi Access
Point

2. Start TCP Iperf server on the accessory by
running:
iperf -p 6001 -s -i 1 -w 2M

3. Start UDP Iperf server on the accessory by
running:
iperf -p 5001 -s -i 1 -w 2M -u

4. Start UDP Iperf client on the accessory by
running:
iperf -c Connect to CarPlay AP -p 5001 -i 1 -w

Follow the instructions carefully to successfully complete the test.

Enter the test environment parameters that will be included along with the test results.

Tap on 'Run Test' to start the performance test. Each test will guide you through the required steps and show the Iperf client and server commands that should be invoked on the CarPlay accessory.

Note: Starting an Iperf Client and Server on the CarPlay Accessory

For the wireless tests to work, Iperf clients and servers must be running on the CarPlay accessory. The Iperf commands to be invoked on the CarPlay accessory will be presented on-screen during the test.

The following Iperf client flags are supported by ATS Utility for wireless tests:

Table 9-1   TCP Client Flags

Option	Value
-i, --interval	1
-w, --window	2M
-t, --time	<varies per test, in seconds>
-p, --port	<configurable>

Table 9-2   UDP Client Flags

Option	Value
-i, --interval	1
-w, --window	2M
-t, --time	<varies per test, in seconds>
-p, --port	<configurable>
-b, --bandwidth	<varies per test>
-d, --dualtest	<bidirectional test run simultaneously>

The following Iperf server flags are supported by ATS Utility for wireless tests:

Table 9-3   TCP Server Flags

Option	Value
-i, --interval	1
-w, --window	2M
-p, --port	<configurable>

Table 9-4   UDP Server Flags

| Option	Value
-i, --interval	1
-w, --window	2M
-p, --port	<configurable>

Note: Verifying the Connectivity

Tap on 'Verify Connectivity' to verify that the CarPlay accessory IP address and ports are configured correctly. Follow the test instructions carefully to be able to confirm a valid test setup and for assistance in troubleshooting configuration issues.

9.3.3 Legacy Tests

9.3.3.1 Client Configuration

Tap on 'Iperf Client Test' to begin configuring an Iperf test in which the device acts as an Iperf client and connects to an Iperf server running on the CarPlay accessory.
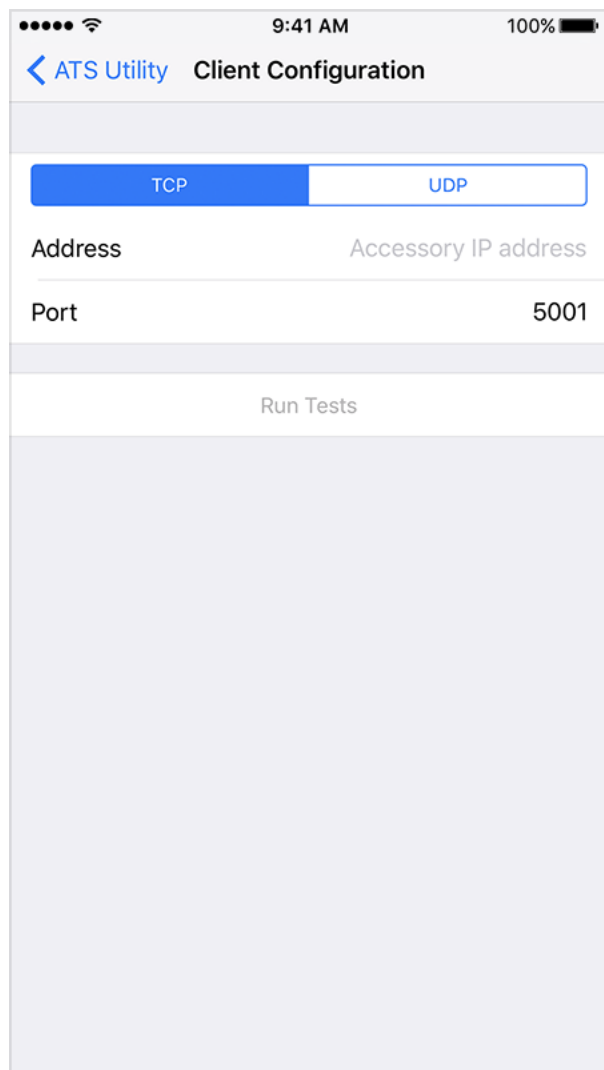
Use the Client Configuration screen to enter the IP address and port of an Iperf server running on the CarPlay accessory. When connected to a CarPlay accessory, ATS Utility automatically populates the accessory IP address field with the appropriate address. Wired Iperf client tests use IPv6 when connected to the CarPlay accessory via USB.

Note: Starting an Iperf Server on the CarPlay Accessory

For the Iperf client test to work, an Iperf server must be running on the CarPlay accessory. The server should be invoked as follows:

TCP: IPv6 Server: iperf -s -i 1 -w 128k -p 5001 -V

UDP: IPv6 Server: iperf -s -u -i 1 -w 128k -l 1448 -p 5001 -V

The following Iperf client flags are supported by ATS Utility for wired tests:

Table 9-5   TCP Client Flags

Option	Value
-i, --interval	1
-w, --window	128k
-t, --time	10
-p, --port	\<configurable\>
-V, --ipv6_domain	\<IPv6 domain\>

Table 9-6   UDP Client Flags

Option	Value
-i, --interval	1
-w, --window	128k
-t, --time	10
-l, --len	1448
-p, --port	\<configurable\>
-V, --ipv6_domain	\<IPv6 domain\>
-b, --bandwidth	\<varies per test\>

9.3.3.2 Server Details

Tap on 'Iperf Sever Test' to get to the Server Details screen where you will find all the information you need to configure an Iperf test in which the device acts as an Iperf server and listens to the Iperf client connections from the accessory.

ATS Utility automatically starts the Iperf IPv6 & IPv4 servers on the device when you navigate to the Server Details screen, and it keeps the servers running until you tap the Back button. Server Details screen will display the addresses when connected to the accessory that can assign device IP.

Note: Starting an Iperf Client on the CarPlay Accessory

For the Iperf server test to work, an Iperf client must be running on the CarPlay accessory. The client should be invoked as follows:

TCP: IPv6 Client: iperf –c fe80::123:12:12a2:a12b%en0 -i 1 –w 128k –t 10 –p 5001 –V

UDP: IPv6 Client: iperf –u –c fe80::123:12:12a2:a12b%en0 -i 1 –w 128k –l 1448 –t 10 –p 5001 –V

The following Iperf server flags are supported by ATS Utility for wired tests:

Table 9-7   TCP Server Flags

Option	Value
-i, --interval	1
-w, --window	128k
-p, --port	5001
-V, --ipv6_domain	\<IPv6 domain\>

Table 9-8   UDP Server Flags

Option	Value
-i, --interval	1
-w, --window	128k
-l, --len	1448
-p, --port	5001
-V, --ipv6_domain	\<IPv6 domain\>

10. Known Issues

There are several known issues in ATS, they are organized into sections below. To report bugs or request enhancements to ATS, file a New Problem at https://bugreport.apple.com. Include "MFi ATS" in the Title field. When reporting bugs, attach an ATS trace file that demonstrates the issue.

10.1 UART Accessories

When running ATS with an accessory that transmits iAP-over-UART at baud rates other than 57600, the first accessory byte immediately after power-cycling the ATS hardware box may be preceded by a report of a single phantom unrecognized byte.

For accessories that transmit iAP-over-UART, if sync (0xFF) bytes are not transmitted with iAP packets, then the ATS autobauder may fail to lock to the UART traffic successfully. In such a case, the likely outcome is a series of unrecognized bytes in the iAP Packets over UART traffic view.

10.2 Wi-Fi Captures

Wireless captures with iPhone XR, iPhone XS, and iPhone XS Max can only be taken with a Mac running macOS 10.13 High Sierra or later.

10.3 ATS Box

When connecting a device to the ATS Box, the device may display a message that states, "This accessory is not made to work with iPhone." This is caused by the fact that the ATS Box itself is not an accessory. When using ATS, this message may be ignored. However, you should make sure your accessory does not trigger this message when connected directly to the device without an ATS Box.

10.4 ComProbe BPA analyzer

If a ComProbe BPA analyzer is attached before the Frontline driver is installed, the Mac's internal Bluetooth module may become disabled. If this happens, disconnect the ComProbe BPA analyzer from the Mac, install the Frontline driver, and reboot the Mac. You may connect the ComProbe BPA analyzer after the Mac has rebooted.

The ComProbe BPA 100 analyzer is unable to capture Bluetooth traffic from accessories that use Secure Connection and claim compatibility with Apple devices running iOS 11.0 or later.

10.5 Certification Assistant

The Certification Assistant detects connections and disconnections of the accessory. Both physical and programmatic disconnections are handled in the same way. If your accessory emulates a physical disconnection by manipulating pin states, it should only do so when the Certification Assistant instructs to disconnect the accessory. An emulated disconnection at any other time may prematurely terminate the test and cause an error.

10.6 Vbus Load Test

For USB D+ and D- voltage measurements to be made, no device may be connected. This ensures that if an iAP-over-USB accessory happens to be connected to the ATS Box, it will not have its USB signal integrity affected by attempts by the ATS Box to measure its USB D+ and D- voltages as though it were a USB charging accessory.

For USB D+ and D- voltage measurements to be made using an ATS Lightning Box, no Total Phase Beagle USB 480 analyzer may be attached. USB Brick Detect will fail if a Beagle USB 480 analyzer is connected even when it is not configured in ATS.

The ATS autobauder is bounds-checked to a maximum possible reported baud rate. A very narrow glitch in the UART signal (immediately after accessory start-up, for example) may cause a series of unrecognized bytes in the iAP traffic view as the autobauder attempts to lock to the UART traffic.

The USB Vbus connection in the 30-pin extender cable has a DC resistance in the range of 200 mΩ to 250 mΩ. If the extender cable is placed between the accessory under test and the ATS hardware unit, the reported USB Vbus measurement may be artificially low, especially when the accessory is supplying a full 1 A or 2.1 A of charging current to device.

In certain situations, the thresholds of Vbus and device power warnings and errors may change. This is due to the fact that ATS cannot positively identify the accessory's charging capabilities at all times. For example, ATS is unable to positively identify the accessory's charging capabilities whenever a device is connected to the ATS box. These thresholds may change at any time without prior notice. You must satisfy whichever threshold is described in the MFi specifications for your accessory.

10.7 30-pin Accessories

For the 30-pin connector, if an accessory happens to use only one of the five available DGND pins, and this pin happens to be pin 30, then a number of side effects may be caused by the introduction of ATS into the system. For example, ATS will not properly measure the ID resistor for such an accessory. Because pin 30 is the recommended pin by which the accessory can detect the presence of a device, the ATS 30-pin Box treats this signal as more than just a basic DGND, so an accessory that relies exclusively on pin 30 for its DGND connection may behave in unexpected ways. However, an accessory should be designed to use all available DGND pins as possible.

For the 30-pin connector, ATS keeps Pin 30 grounded at all times, regardless of whether a device is attached. For this reason you must always connect a device before connecting your accessory. If you do not, your accessory may attempt to interact with ATS even though no device is connected.

For the 30-pin connector, accessories that selectively ground pin 20 based on the state of pin 13 may fail to be detected during the setup phase of the Certification Assistant tests. Additionally, the accessory is in violation of the MFi Accessories hardware specification and should be corrected.

For the 30-pin connector, while running the Certification Assistant, if the device bounces Accessory Power (pin 13), the Certification Assistant may misinterpret that as a disconnection of the accessory. If this occurs, you should disconnect your accessory from ATS, dismiss the Certification Assistant's disconnection dialog, then reattach your accessory. You should then be able to complete the test successfully. If the problem persists, contact your MFi Representative for additional support.

11. Technical Notes

11.1 About iAP-Over-UART Baud Rates

A device determines the UART speed of a connected UART accessory by "autobauding" to its Tx signal on a packet-by-packet basis. This is accomplished by measuring the width of the start bit for each start-of-packet 0xFF byte. This measurement can be distorted by the quality of the accessory's Tx signal, especially if it exhibits slow rising-edge or falling-edge transitions.

For example, the following two oscilloscope traces show the start bit for an accessory operating at the deprecated legacy rate of 38400 bps. The vertical cursors have been set to mark the start and the end of a start-of-packet 0xFF bit, and the display format has been inverted to use units of Hertz instead of seconds.

The first trace shows that the actual transmitted bit rate is approximately 38800 bps. This is a deviation of only 1.0% from nominal and is entirely acceptable.
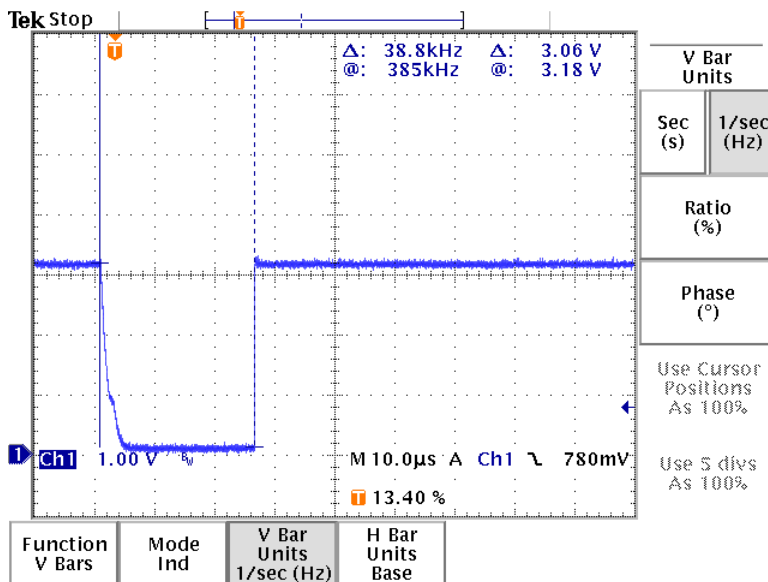
Because the device's UART receiver expects digital signals, however, it will not actually register a falling-edge transition until the accessory's UART TX signal drops below a particular voltage threshold. (The value of this threshold will depend on the generation of device hardware and other factors.)

The following scope trace shows what may occur as a result. Because the falling edge of the accessory's UART TX signal is relatively slow, the measured low-time of the start bit by device may correspond to 41700 bps instead of 38800 bps. Such an 8.5% deviation from the nominal rate is unacceptable.
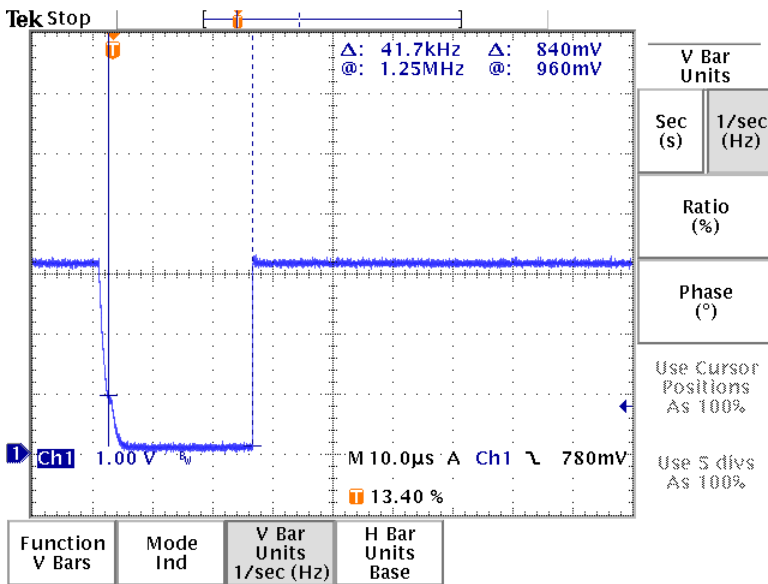
In addition to reporting the results of 0xFF start-bit autobauding, ATS also measures the bit time implied by the time taken for the accessory to transmit the eight data bits of the 0x55 byte that follows each start-of-packet 0xFF byte. It is possible for this alternate measurement method to be affected by the same rise-time and fall-time problems that affect the start-bit method, but the bit-time error should be reduced by a factor of roughly eight, given the measurement of eight bits instead of one.

Even though the device does not do 0x55-based autobauding, ATS reports the results from both measurement methods because large differences between the two are generally indicative of hardware errors, firmware errors, or both. If the rate from 0x55-based autobauding closely matches the intended rate, then the accessory firmware is probably using the right crystal and UART clock divisor. If the rate from 0xFF start-bit-based autobauding shows large errors, however, potential problems with the accessory's UART TX signal should be investigated further via an oscilloscope.

12. ATS 30-pin Box

The ATS 30-pin Box (Figure 12-1 (page 77)) is required to use ATS with 30-pin accessories. Accessories utilizing USB will also require a Beagle USB 480 analyzer (page 12) and MFi 30-pin Breakout (Figure 12-2 (page 78)). The MFi 30-pin Breakout board is a component that allows a USB protocol analyzer to be connected to the USB pins of the 30-pin connector.

Figure 12-1   ATS 30-pin Box
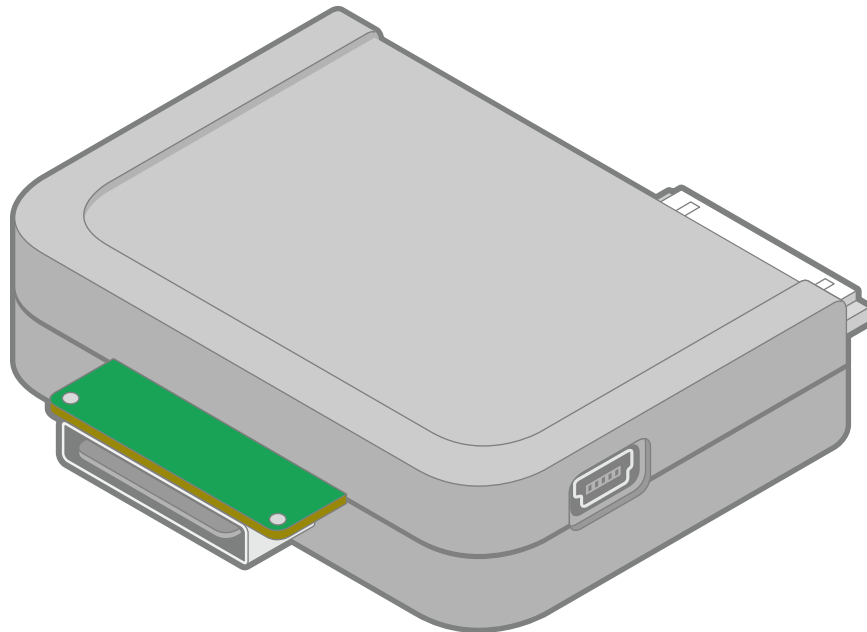
Figure 12-2   MFi 30-pin Breakout (ATS0201)