frontline®

Debug Communications Faster℠

THE RIGHT TOOLS AND SERVICES WILL HELP YOU BRING YOUR *BLUETOOTH* PRODUCTS TO MARKET FASTER

Presenter:
Tomas O' Raghallaigh
Frontline Test Equipment, Inc.
toraghallaigh@fte.com

fte.com Frontline™
Debug Communications Faster℠

Frontline Tools and Services

- Air sniffer (Protocol Analyzers)
- Host Control Interface (HCI) (wired)
- Robustness testing (Black Box Testing, Fuzzing)
- Interoperability Testing (IOT)

Bluetooth Wireless Technology

BPA 500™ Dual Mode *Bluetooth* Protocol Analyzer (*Bluetooth* v4.0 + HS)

- "Classic" (BR/EDR)
- low energy
- 802.11 - High Speed (Option)

fte.com frontline™ Debug Communications Faster℠

Multiple Points of Observation

BPA 500 can sniff:

- Air Traffic
  - “Classic” (BR/EDR)
  - low energy
  - Dual mode – “classic” AND low energy
- HCI Traffic with BPA 500 add-ons
- Virtual Sniffing (software sniffing)
- BTSnoop (Free file format for logging data readable in Frontline viewers)

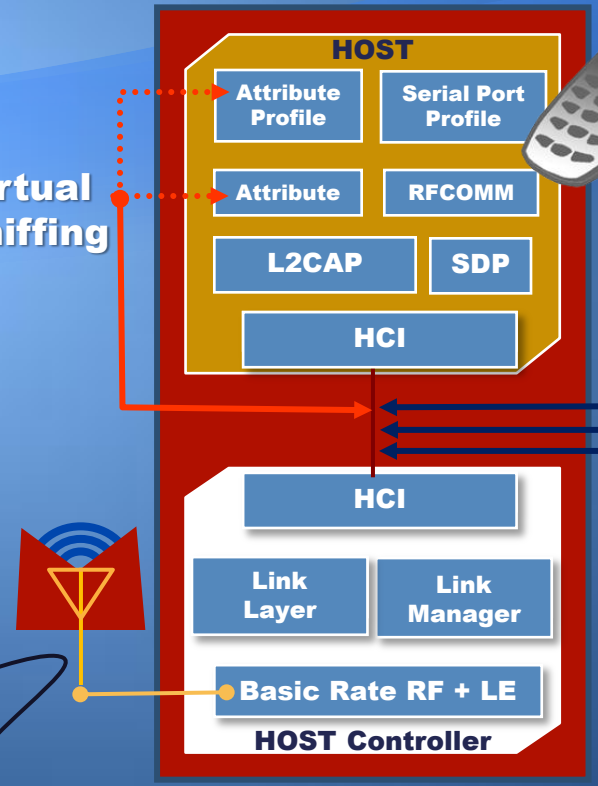
fte.com Frontline™ Debug Communications Faster℠

Points of Observation

Bluetooth low energy

Virtual Sniffing

Bluetooth Dual Mode



HCI Sniffing

USB

SDIO

UART

Bluetooth "Classic"

fte.com frontline™ Debug Communications Faster℠

Sniffs Air – Dual Mode

- Sniffs low energy and "Classic" *Bluetooth* devices

- Displays all packets into a single view

fte.com frontline™ Debug Communications Faster℠

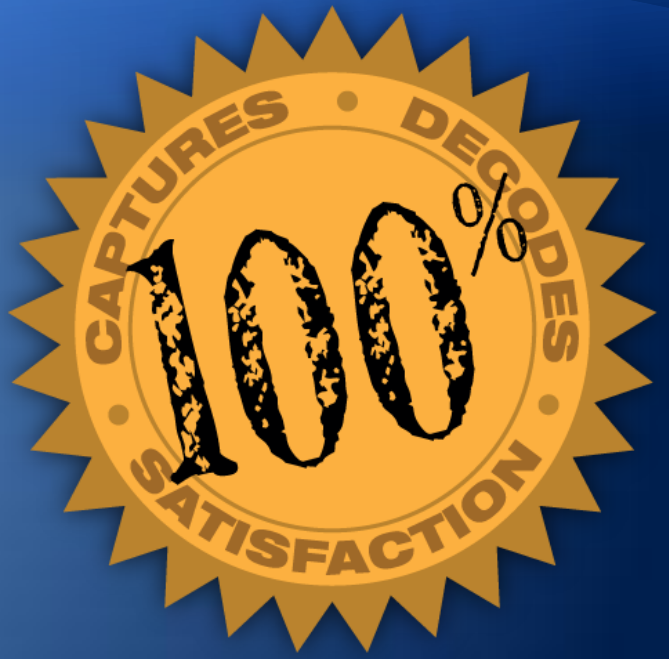
NEW Data Capture Method!

- We have developed a brand new capture method for the BPA 500 that delivers rock-solid data captures with less user interaction than ever before…

fte.com frontline™
Debug Communications Faster℠

Frontline's Guarantee

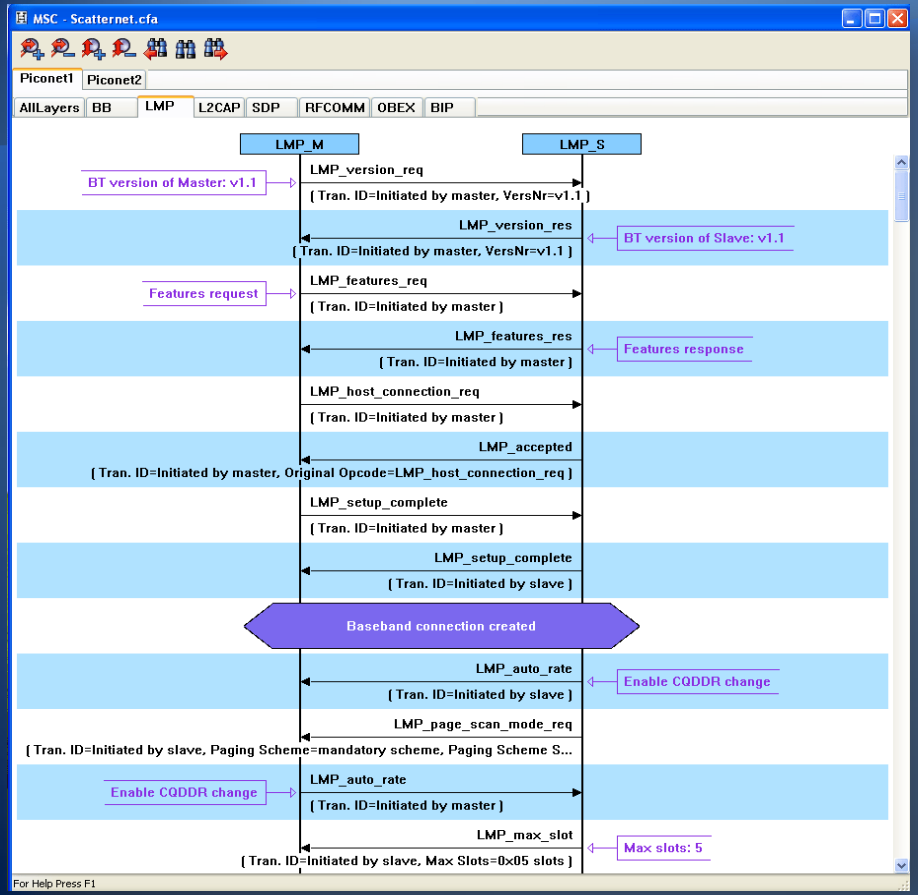
We're so confident about our new data capture method, we guarantee:



100% Quality Data Captures
100% Data Decodes
100% Satisfaction Guaranteed

fte.com frontline™
Debug Communications Faster℠

MSC – Message Sequencing Chart



- All in simple, easy-to-understand terms
- MCS makes it easy to see
  - Physical link activities
  - Logical links activities
  - Protocol level activities
  - Profile level activities

BPA 500 Add-ons

802.11 ComProbe Add-on

802.11 ComProbe and antennas to monitor *Bluetooth* packets across a Wi-Fi transport

USB ComProbe Add-on

USB HCI sniffer hardware using the USB ComProbe II

SDIO ComProbe Add-on

SDIO sniffer hardware using the SDIO ComProbe

High Speed UART Add-on

UART HCI sniffer hardware

fte.com frontline™
Debug Communications Faster℠

HCI Sniffing Add-ons Summary

Rx
Tx
Gnd
TT Level

Bluetooth Host

USB HCI (External)

Bluetooth Host Controller

ComProbe Software

USB ComProbe Add-on (USB-CP-OPT)

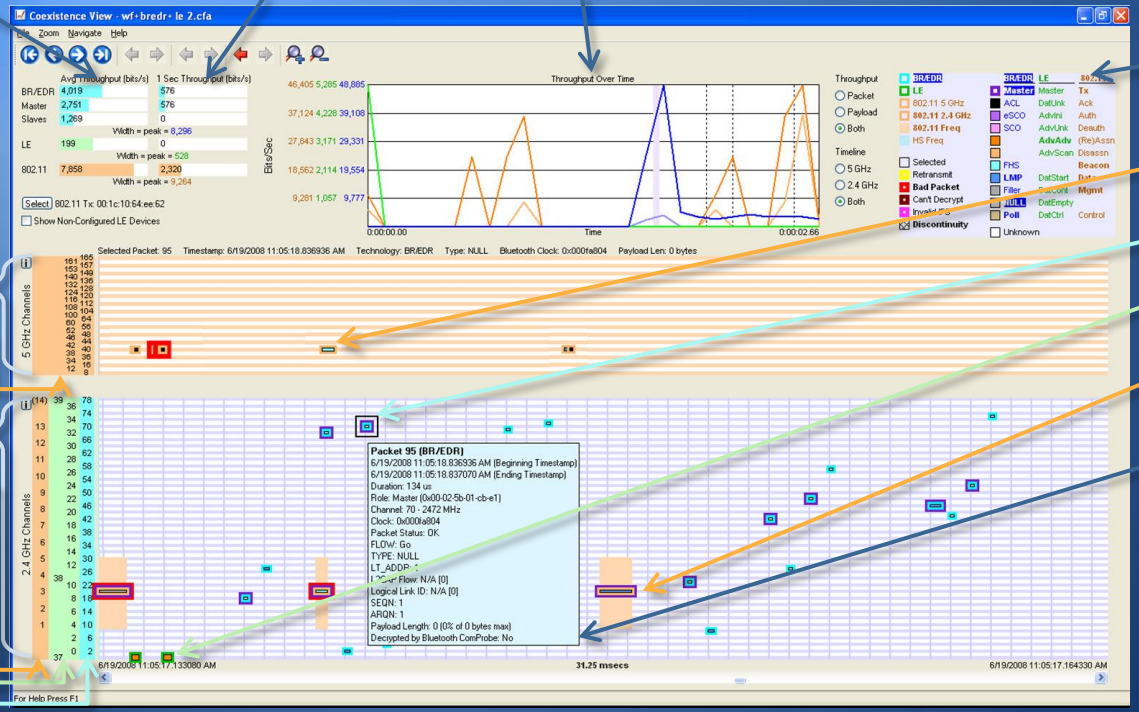
fte.com frontline™
Debug Communications Faster℠

802.11 Sniffing Add-on

- *Bluetooth* specification 3.0/4.0 +HS
- Combined *Bluetooth* and Wi-Fi throughput graph
- Numeric Data throughput readout for Average and Live (1 second window) payload
- Wi-Fi and *Bluetooth* channels identified on a single display
- Combined *Bluetooth* /Wi-Fi capture log
- Full, stand-alone Wi-Fi decoding and protocol analysis
- Detachable antenna to enable conductive capture of Wi-Fi data

fte.com frontline™
Debug Communications Faster℠

Bluetooth Classic, 802.11, LE Coexistence Timeline



5GHz Channels

802.11 (only)

2.4GHz Channels

802.11

Low energy

Classic (BR/EDR)

Legend –
Highlighted (selected packet)
Bold (At least one packet seen)

802.11 Packet – 5 GHz range

Classic Packet

Low energy Packet

802.11 Packet – 2.4 GHz range

Tooltip – Detailed Information about packet on mouse over

fte.com frontline™
Debug Communications Faster℠

Frontline Customers

CSR (Cambridge Silicon Radio)
Qualcomm
Broadcom
Motorola
Infineon
Intel
Texas Instruments
Siemens
Atheros
Marvell
Alps
MSI
Apple
ISSC
Sony

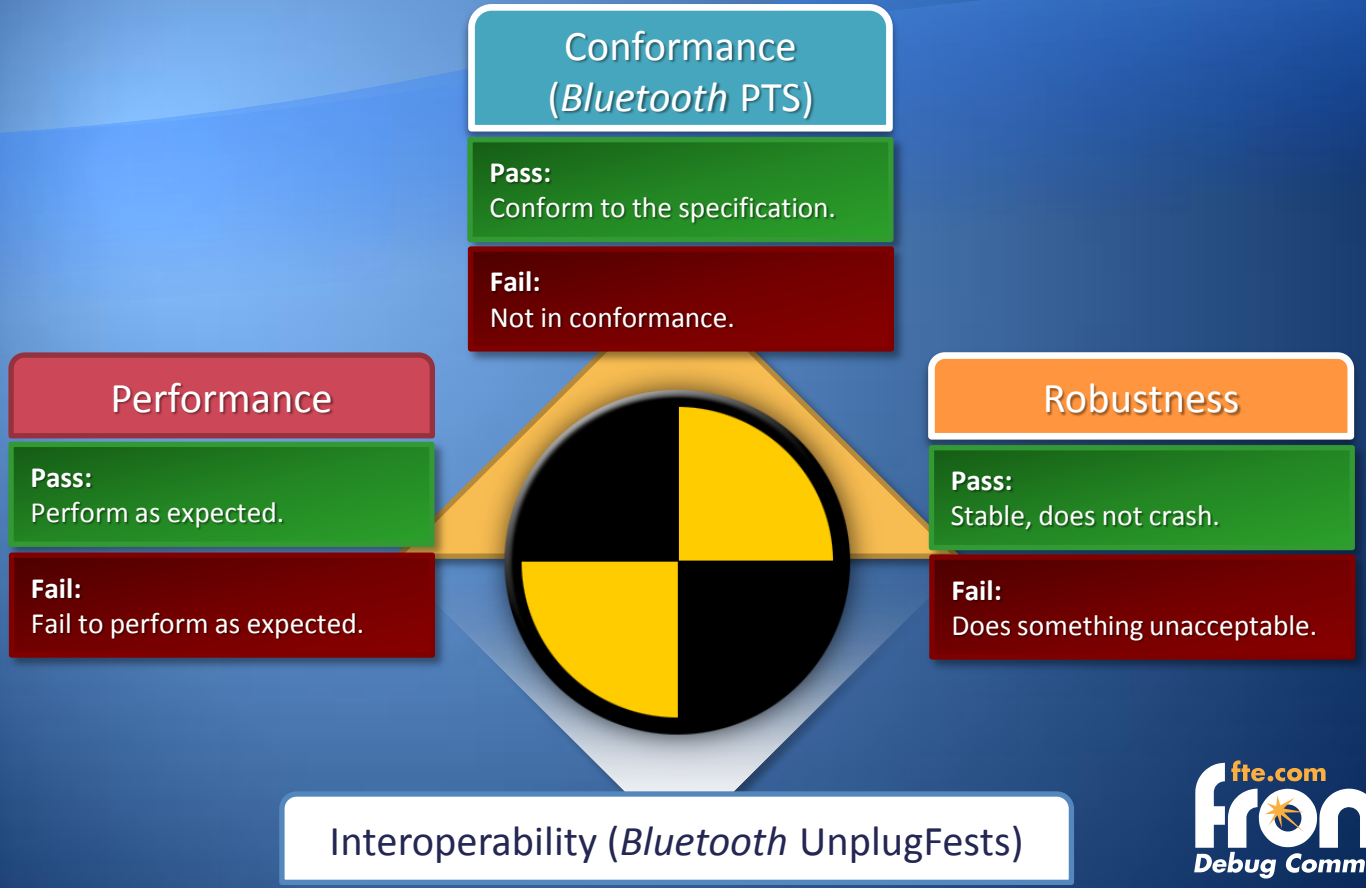
Sony Ericcson
Kyocera
VW
Ford
Audi
Microsoft
Panasonic
Hitachi
Symbol Technology
NXP
Continental
Plantronics
BenQ
MiTek
Sybase

Sybase
Cisco
Visteon
BMW
Daimler Chrysler
Delphi
Nissan
Johnson Controls
US Government
Toyota
IVT
Samsung
LG
MP

Bluetooth Robustness Tester

- Black box testing
- Fuzzing (crash testing)
- Test cases to highlight unusual behavior
- Test cases target profile and protocol levels
- Based on sending systematically broken (rarely random) inputs to a device in order to crash it

Black Box Testing Categories



EARLY RESULTS – UPF39

TEST RUNS AT UPF 39
30

TESTRUNS FAILED AT UPF39
21 (70%)

SCORING ANOMALY TYPES:

Underflows
Invalid length fields
Invalid type fields

TEST RUNS	TEST RUNS FAILED	PROTOCOLS / PROFILESAVAILABLE FOR TEST: 20
4	3	A2DP
4	3	AVRCP
--	--	BNEP (NAP/PAN)
--	--	BIP
--	--	BPP
2	0	DUN
--	--	FAX
1	1	FTP
--	--	HCRP
--	--	HDP
6	5	HFP
1	1	HSP
--	--	HID
--	--	Irmc-Sync
6	4	L2CAP
1	1	OPP
2	1	PBAP
1	1	RFCOMM
2	1	SDP
--	--	SIM Access

Bluetooth™ SPECIAL INTEREST GROUP

fte.com frontline™ Debug Communications Faster℠

EARLY RESULTS – UPF39

TESTRUNS AT UPF 39
30

TESTRUNS FAILED AT UPF39
21 (70%)

SCORING ANOMALY TYPES:

Underflows
Invalid length fields
Invalid type fields

TEST RUNS	TEST RUNS FAILED	PROTOCOLS / PROFILES AVAILABLE FOR TEST: 20
4	3	A2DP
4	3	AVRCP
–	–	BNEP (NAP/PAN)
–	–	BIP
–	–	BPP
2	0	DUN
–	–	FAX
1	1	FTP
–	–	HCRP
–	–	HDP
6	5	HFP
1	1	HSP
–	–	HID
–	–	Irmc-Sync
6	4	L2CAP
1	1	OPP
2	1	PBAP
1	1	RFCOMM
2	1	SDP
–	–	SIM Access

How does the tool work?

- The tool contains thousands of messages in the form of “Test Cases” (anomalies)
- Tests use standard interfaces
  - No source code is needed
  - Any standard-compliant implementation can be tested
- Negative testing – the test cases try to make the implementation stop responding reset or exhibit other faults
  - Also called PROTOS / robustness / security / vulnerability / fuzz(ing) / rapid testing, etc.

What really happens!

Bluetooth Robustness Tester

Valid Message

Reply – OK

Anomaly #1

Reply Ignored

Valid Message #1

Reply - OK?

Anomaly #2

Device Under Test

fte.com frontline™ Debug Communications Faster℠

What is my exposure?

- Product recalls are costly and cause lasting damage
- Proactive robustness schedules can reduce risk and exposure to security issues
- SW Security = SW Quality
  - Security problems are created during development
  - Testing prevents security problems in software
- 99.99% reliable = 100% vulnerable

Bluetooth Interoperability

- 1000+ Devices
  - Biggest device library in industry
- Lots of OEMs, cars
- 10 years of *Bluetooth* experience, instantly in your QA team
- International supply of *Bluetooth* devices
  - China, Japan, Brazil, Europe and North American

fte.com frontline™
Debug Communications Faster℠

TEST RUNS AT UPF 39
30

TESTRUNS FAILED AT UPF39
21 (70%)

SCORING ANOMALY TYPES:

Underflows
Invalid length fields
Invalid type fields

TEST RUNS	TEST RUNS FAILED	PROTOCOLS / PROFILESAVAILABLE FOR TEST: 20
4	3	A2DP
4	3	AVRCP
--	--	BNEP (NAP/PAN)
--	--	BIP
--	--	BPP
2	0	DUN
--	--	FAX
1	1	FTP
--	--	HCRP
--	--	HDP
6	5	HFP
1	1	HSP
--	--	HID
--	--	Irmc-Sync
6	4	L2CAP
1	1	OPP
2	1	PBAP
1	1	RFCOMM
2	1	SDP
--	--	SIM Access

Why use Frontline?

- You need to know your device will work with other devices

  We have a comprehensive, current, and ever-expanding device library in-house. You can have confidence that your devices will work seamlessly with other key components in the ecosystem.

- You need to know your devices will work in North America

  Our testing facility is located in Charlottesville, VA, where we test using North American mobile networks

- You want to leverage Frontline as an extension of your QA department

  We have experience and expertise in-house and have pre-existing relationship with all of the key chip manufacturers, phone companies and peripherals companies.
  If there is a problem, we'll help you solve it.

fte.com Frontline™
Debug Communications Faster℠

Why use Frontline?

- You want to improve your “out-of-the-box” experience

  We use pre-defined and customized test plans that will thoroughly test your devices so you can be sure they will work for your customers the first time and every time.

- You need to test your products in automotive environments

  Frontline is building a comprehensive library of *Bluetooth* car kits used in mass production vehicles. When we can’t get the car kit, we buy the car!

- You want to reduce the costs incurred by testing

  No more sending your employees around the world to test specific networks or devices. We’ve got everything you need right here in our labs!

fte.com Frontline™
Debug Communications Faster℠

Frontline Test Equipment

- 25 years of protocol analysis expertise
- 84 of the Fortune 100 companies use our protocol analyzers
- Involved with *Bluetooth* wireless technology initiatives from the beginning (~10 years)
- Work closely with the *Bluetooth* SIG – specifications, working groups, technology committees
- Frontline products support every *Bluetooth* specification, profile, and protocol

fte.com frontline™
Debug Communications Faster℠

Thank you!

frontline®
Debug Communications Faster℠

fte.com frontline™
Debug Communications Faster℠