

EXTRACTING FIRMWARE USING JTAG BASED ON HOL/SCALA/LMS/JIKESRVM/JVM INFORMATICS FRAMEWORK – AN INSIGHT INTO FORENSIC IMAGING OF EMBEDDED SYSTEMS IN THE CONTEXT OF SMART DEVICES & IoT.

Nirmal Tej Kumar

Current Member : ante Inst,UTD,Dallas,TX,USA.

Independent Consultant : Informatics/Photonics/Nanotechnology

R&D Collaborator : USA/Israel/BRICS Group of Nations.

email id : tejdnk@gmail.com

Abstract :

In this technical note the author is interested in exploiting the advantages of Higher Order Logic(HOL),Scala,JVM,JikesRVM & LMS in the IoT scenario.The title is highly self explanatory hence detailed explanation is skipped.

index words: IoT/JVM/Scala/HOL/LMS(Lightweight Modular Staging)/Forensic Imaging/Firmware/JTAG.

Introduction & Inspiration :

[i] “JTAG Explained (finally!): Why "IoT", Software Security Engineers, and Manufacturers Should Care “ -

Source : <http://blog.senr.io/blog/jtag-explained>

[ii] Forensic imaging of embedded systems using JTAG (boundary-scan) -

<https://doi.org/10.1016/j.diin.2006.01.003>

[iii] Scala Based FPGA Design Flow (Abstract Only) -

<https://doi.org/10.1145/3020078.3021762>

Informatics Framework Implementation :

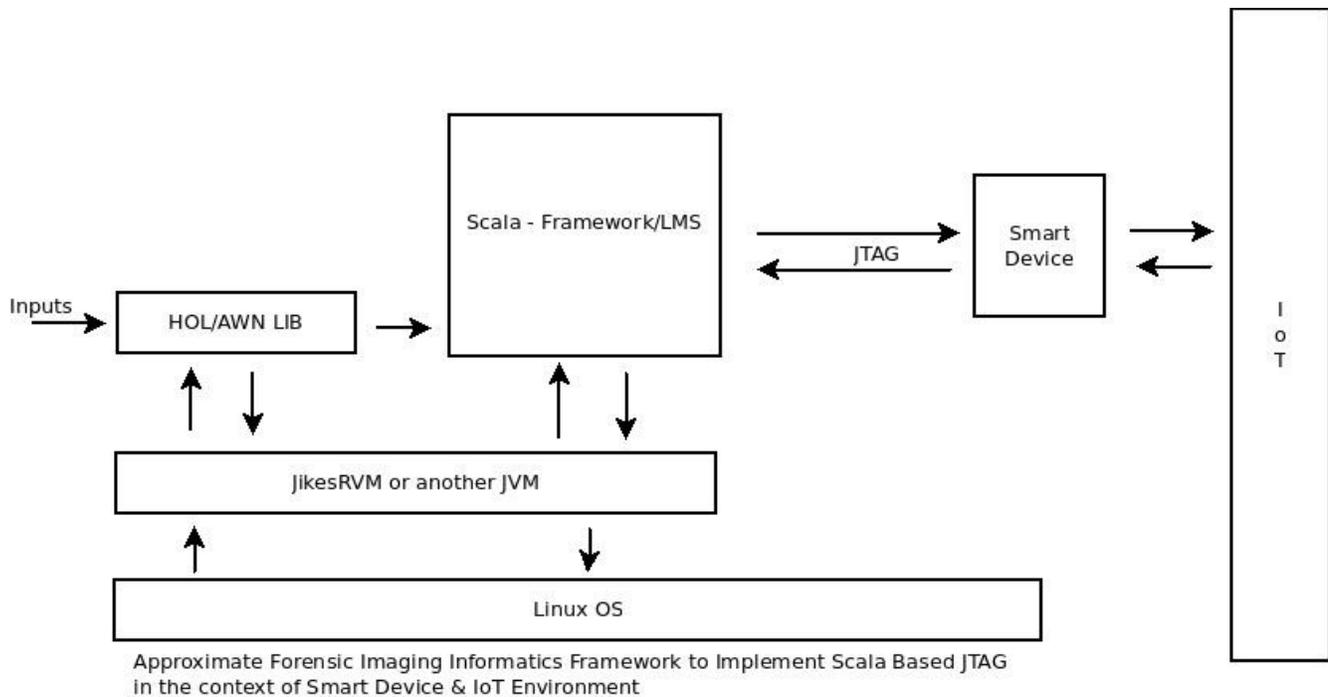


Figure I – Approximate Informatics Framework – HOL/Scala/JTAG/JikesRVM/LMS/IoT
**** Readers please note “the actual implementation might vary to some extent”.**

Analysis of the Informatics Framework:

Informatics framework was explored based on HOL/Scala/JTAG/JVM/IoT to perform forensic imaging of embedded systems in the context of Smart Devices.[Refs from 1 to 9 are used].Figure I illustrates the main idea to help those who are interested in this interesting domain of embedded systems.

Conclusion/s with future perspectives :

A simple HOL/Scala/LMS/JVM/IoT based “Informatics Framework” was designed and presented in this technical note.It is sincerely hoped that many new comers in this promising area will explore this challenging domain of “Forensic Imaging of Embedded Systems” using JTAG.

Additional Information on Software Used :

- [a] <https://isabelle.in.tum.de/> - HOL
- [b] <https://www.isa-afp.org/entries/AWN.html> - HOL based Wireless Library
- [c] <http://www.scala-lang.org/> - Scala Programming Language.
- [d] <http://scala-lms.github.io/> - Lightweight Modular Staging (LMS) is a runtime code generation approach.
- [e] <http://www.spiral.net/software/spiral-scala.html> - Spiral for DSP based in Scala.
- [f] <http://www.jikesrvm.org/> - Java Virtual Machine.
- [g] <https://xdk.bosch-connectivity.com/> - IoT Environment.
- [h] <https://wilsonmar.github.io/intel-iot-setup/> - IoT Environment.

Acknowledgements :

No competing financial interest/s is/are declared in preparing this manuscript. This manuscript is meant to inspire others to develop more advanced Hardware/Firmware/Software verification and its applications in the demanding area of using novel smart devices in IoT Environment. Special thanks to all who made this happen.

References :

- [1] http://www.forensicswiki.org/wiki/JTAG_Forensics
- [2] <https://github.com/ucb-art/chisel-jtag>
- [3] <https://github.com/freechipsproject/rocket-chip/blob/master/src/main/scala/jtag/JtagStateMachine.scala>
- [4] <https://www.xjtag.com/about-jtag/in-system-programming-isp/>
- [5] <http://vixra.org/abs/1710.0320>
- [6] <http://vixra.org/abs/1710.0210>
- [7] <http://vixra.org/abs/1710.0128>
- [8] <http://usbjtag.com/>
- [9] <https://en.wikipedia.org/wiki/JTAG>