NIRMA UNIVERSITY
INSTITUTE OF TECHNOLOGY
NAAC ACCREDITED 'A' GRADE

Generic IP independent BIOS Signing and Parsing

Gahan Saraiya

Institute of Technology
Nirma University

May 10, 2020

NIRMA UNIVERSITY
INSTITUTE OF TECHNOLOGY
NAAC ACCREDITED 'A' GRADE

Outline

About the Project

In general to generate BIOS image (*.rom file), compilation of XYZ.c (source code) has to be done, this compilation not only involves compilation of DXE driver, PEI driver, EFI Application but also includes pre-processing checks, compression of raw files which takes huge amount of time depending on the system configuration. Implementation of this project aids in reduction of this compilation time.

Motivation: Stakeholders

- BIOS development Team
- Automation Team
- Validation Team
- Other Development Team

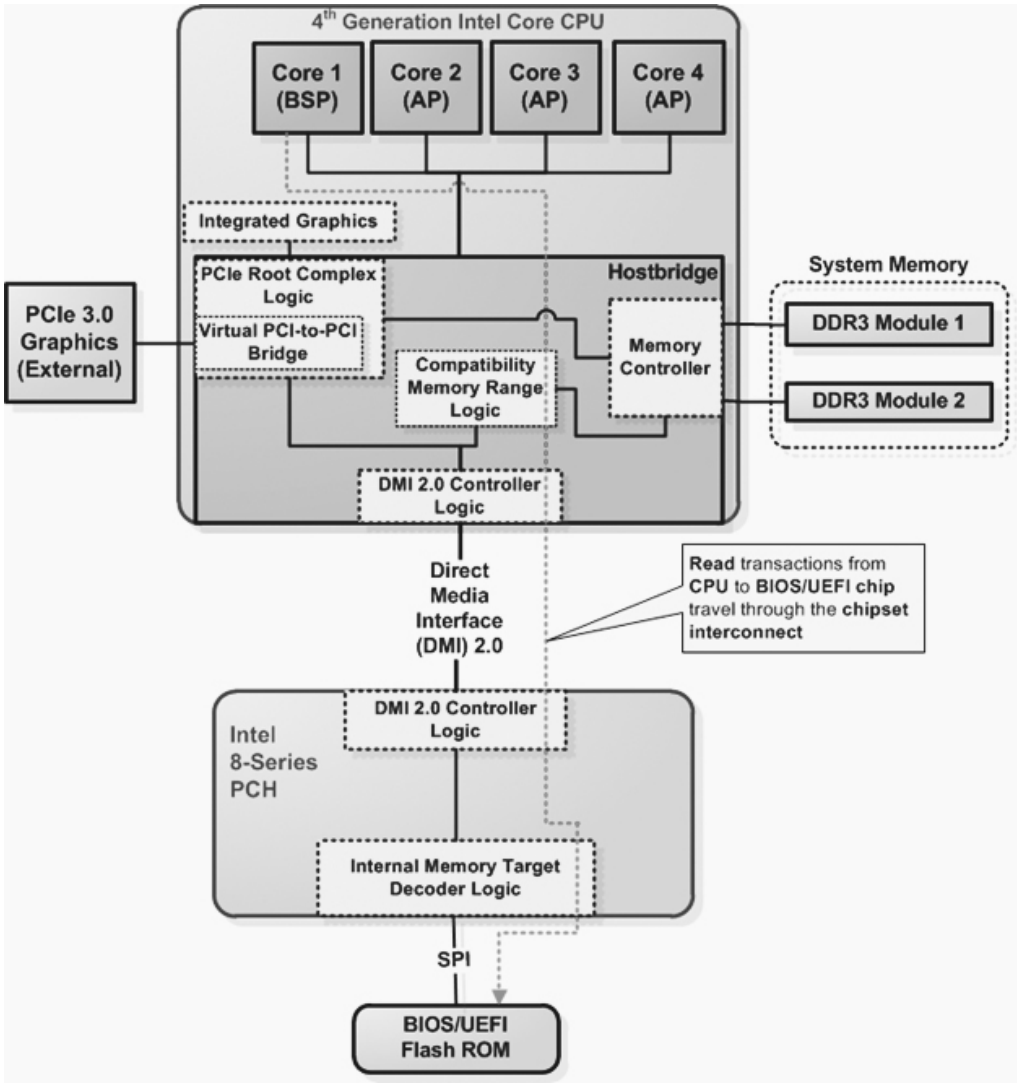
Motivation: Issues/Challenges to the industry (Towards my contribution)

- BIOS image generation: Compilation of whole source code
- More Time complexity: Compilation of source code to generate BIOS image
- Accessing and modifying BIOS Setup Option(s) remotely
- Firmware Flashing of BIOS remotely
- Updating CPU microcode
- Summarizing changes among BIOS image
- Avoiding exposing the source code support
- Avoid setting of BIOS development platform for stake holders
- Runtime BIOS Support for temporary UEFI variable creation

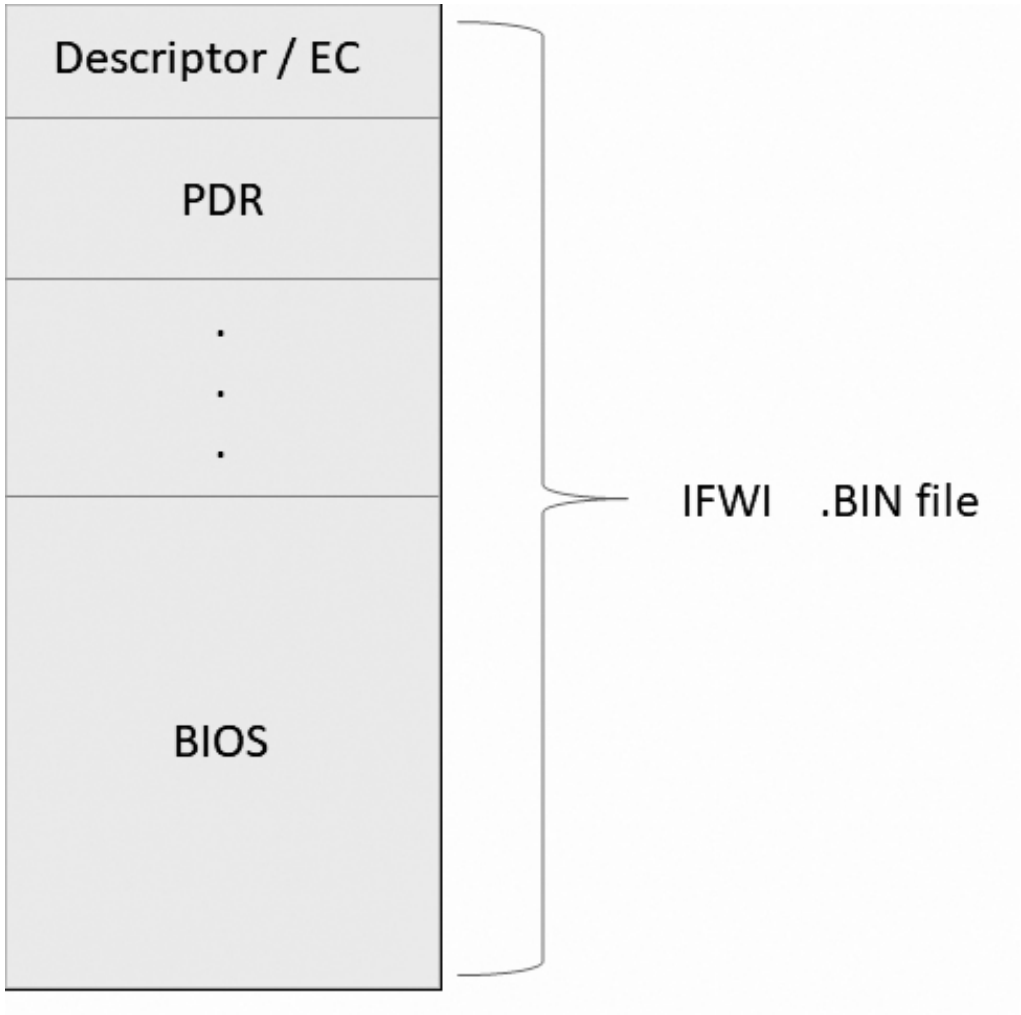
BIOS: Basics

- Set of Software Routines
  - Initialize and test hardware on start
  - Provides the OS with a generic hardware abstraction
- the BIOS must do its job before your computer can load its operating system and applications

BIOS: Architecture



BIOS: Firmware Image

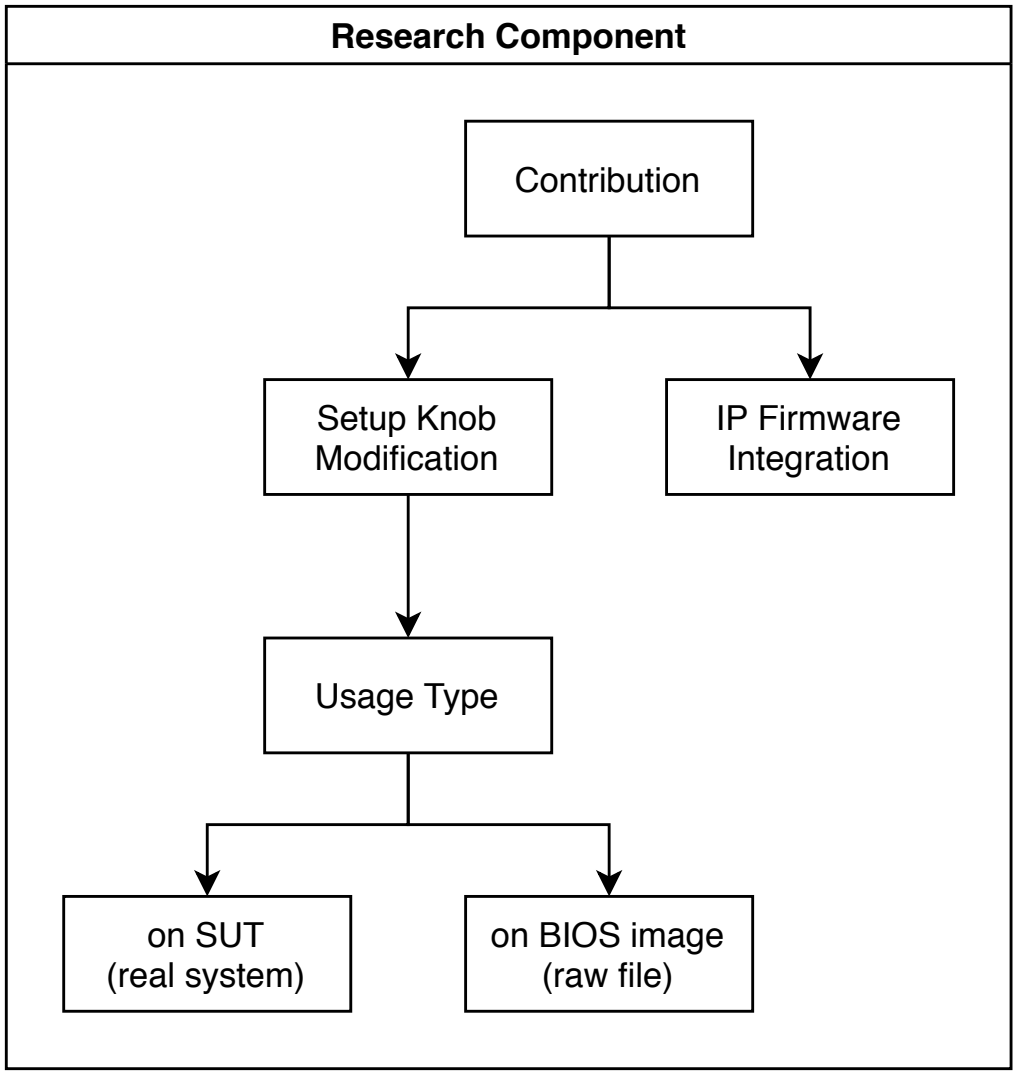


Requirement Specification

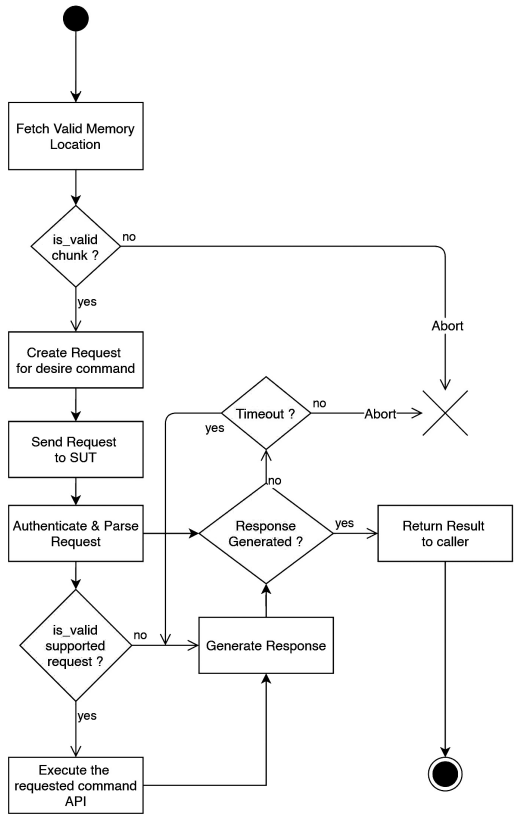
- Visual Studio C/C++ IDE
- Visual Studio Code
- Python 3
- Memory Access Interfaces[1]

[1] itp, itp2, windows, linux, ltb, dci, efi shell, etc.

My Contribution towards issues/challenges



Setup Knobs Modification: Process Flow I

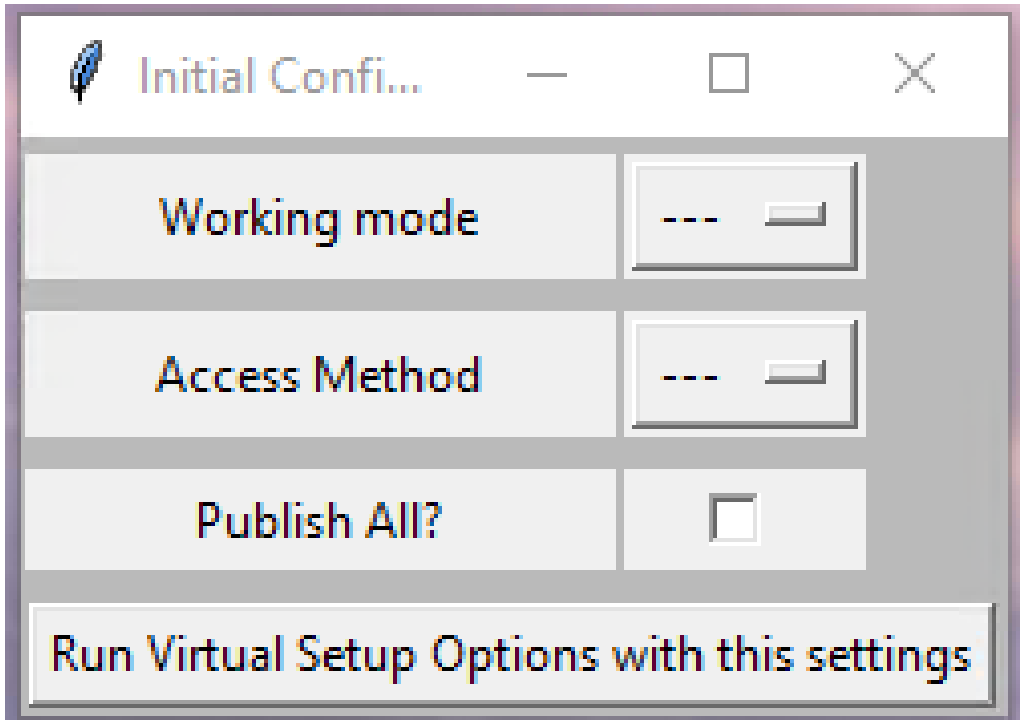


Setup Knobs Modification Flow on SUT

Implementation of Parsing: Additional Tech Stack

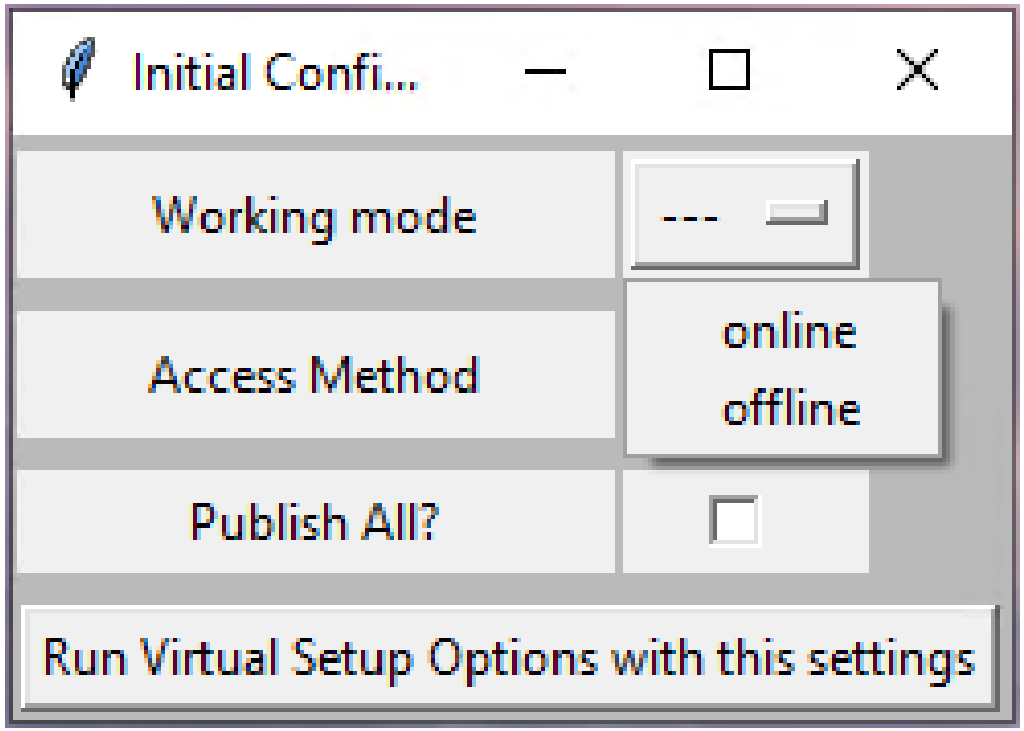
- Tkinter
- XML
- Decompression binaries

Setup Knobs Modification: Implementation Snaps I



Menu to Select initial configuration for work

Setup Knobs Modification: Implementation Snaps II



Available work mode for the system: Online and Offline

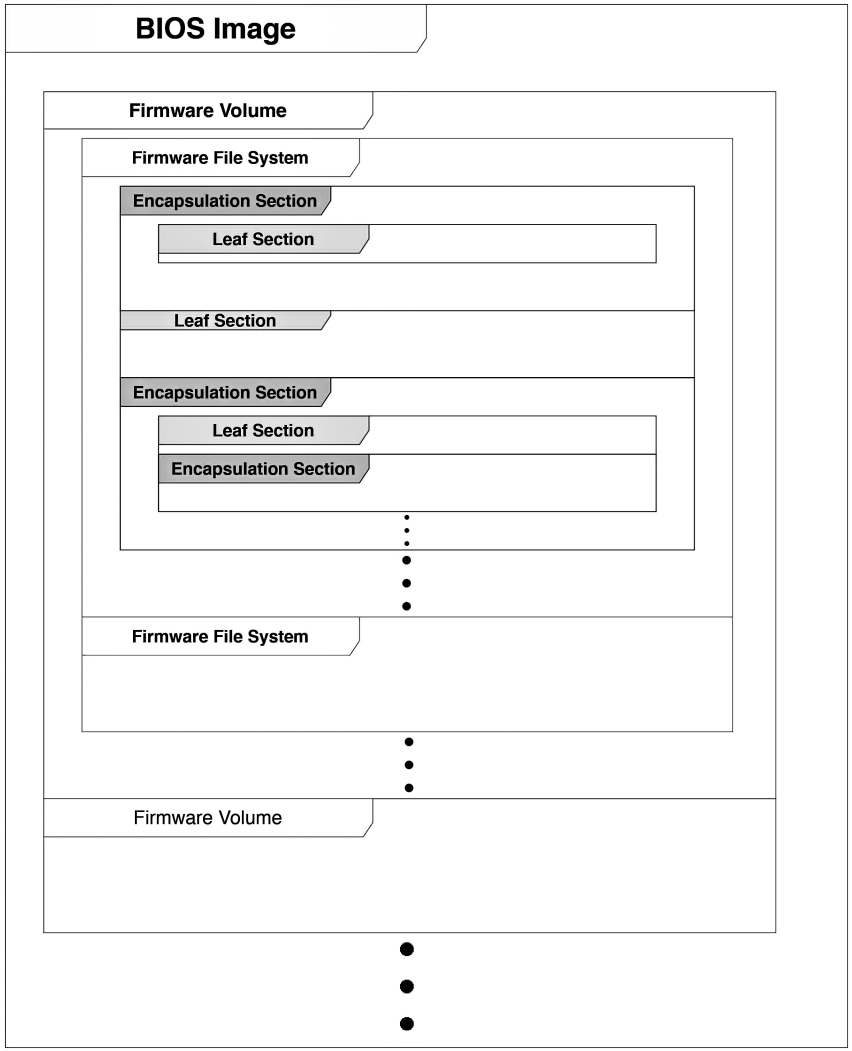
Setup Knobs Modification: Overview of GUI Actions

Button	Interpretation
Push Changes	Apply changes to system if online mode else apply changes to 'bin' file
View Changes	View saved changes in new window
Exit	Exit the GUI
Reload	Reload the GUI
Discard Changes	Discard any change made, any value if modified are restored to current value
Load Defaults	Restore to default values and revert any changes made

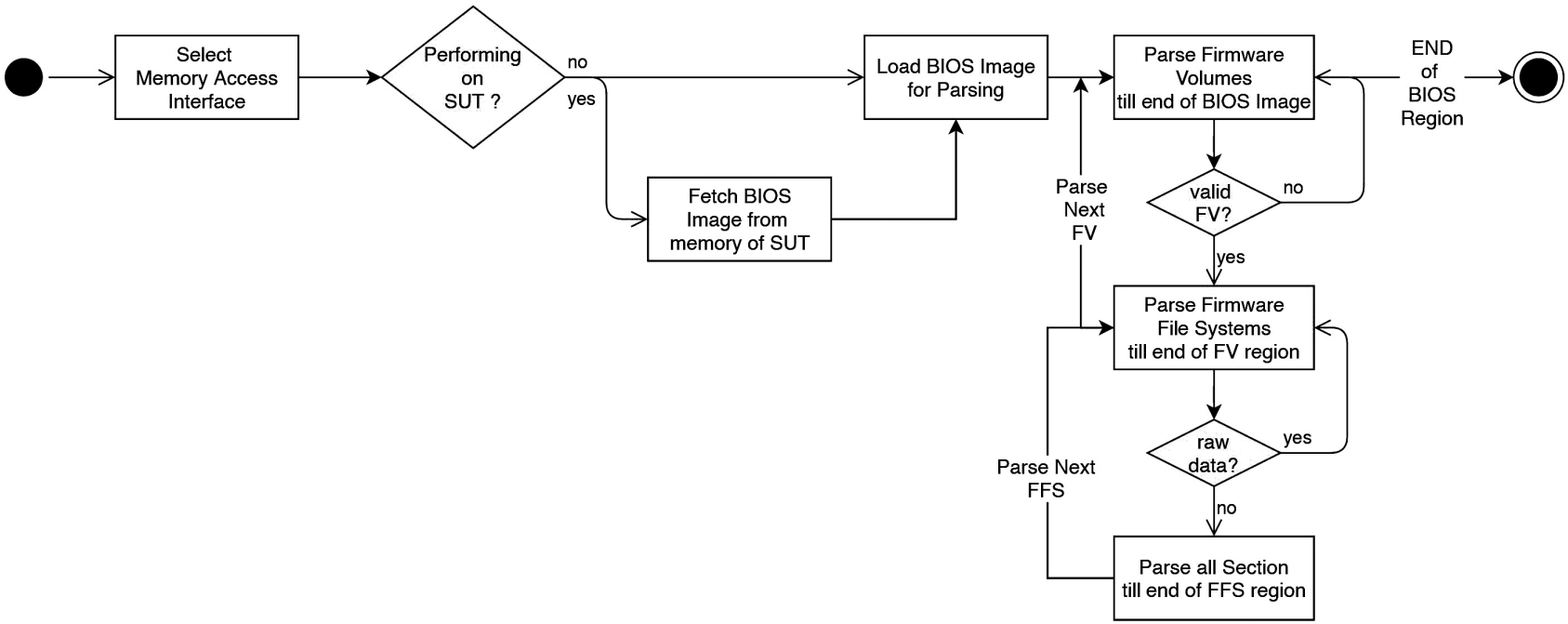
Setup Knobs Modification: Outcome

- Cross platform usage
- API as a driver in BIOS Firmware
- Generic solution for usage types - on **SUT**, on **BIOS image**
- Information parsing and simulation
- Realtime sync for simulation changes
- Seamless Integration

Implementation of Parsing: Format of BIOS Image



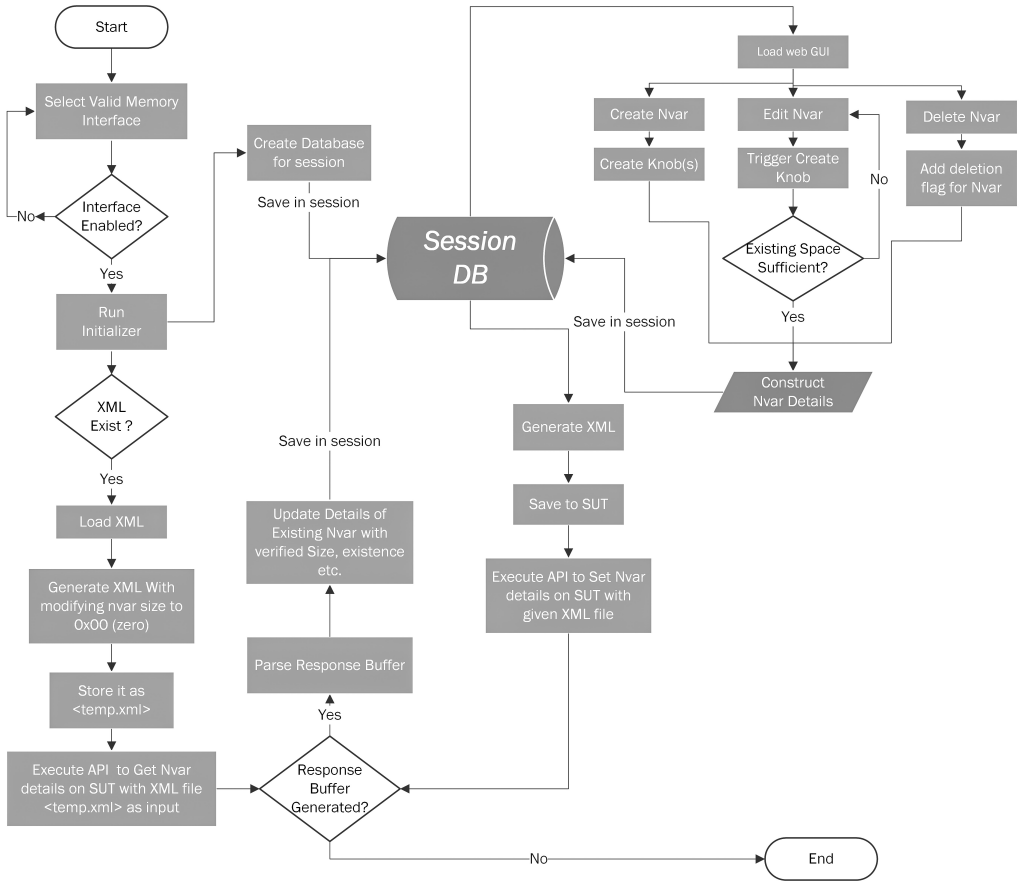
Implementation of Parsing: Work Flow



Outcome

- Human Readable interpretation of BIOS Image
- GUIDs Lookup
- Verification of existence of module by GUID
- Storing the image file system content by GUID
- Summarizing changes of two BIOS image

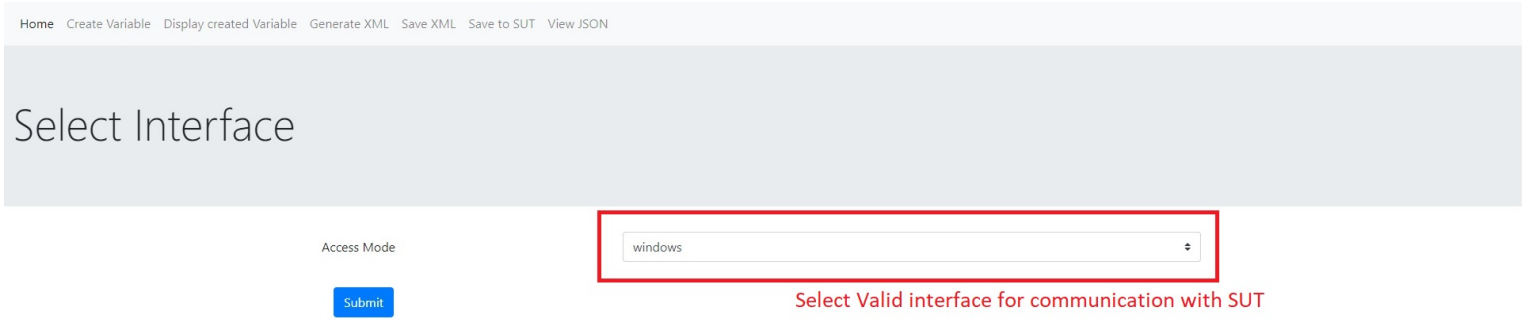
Runtime UEFI Variable Creation: Work Flow



Runtime UEFI Variable Creation: Additional Tech Stack

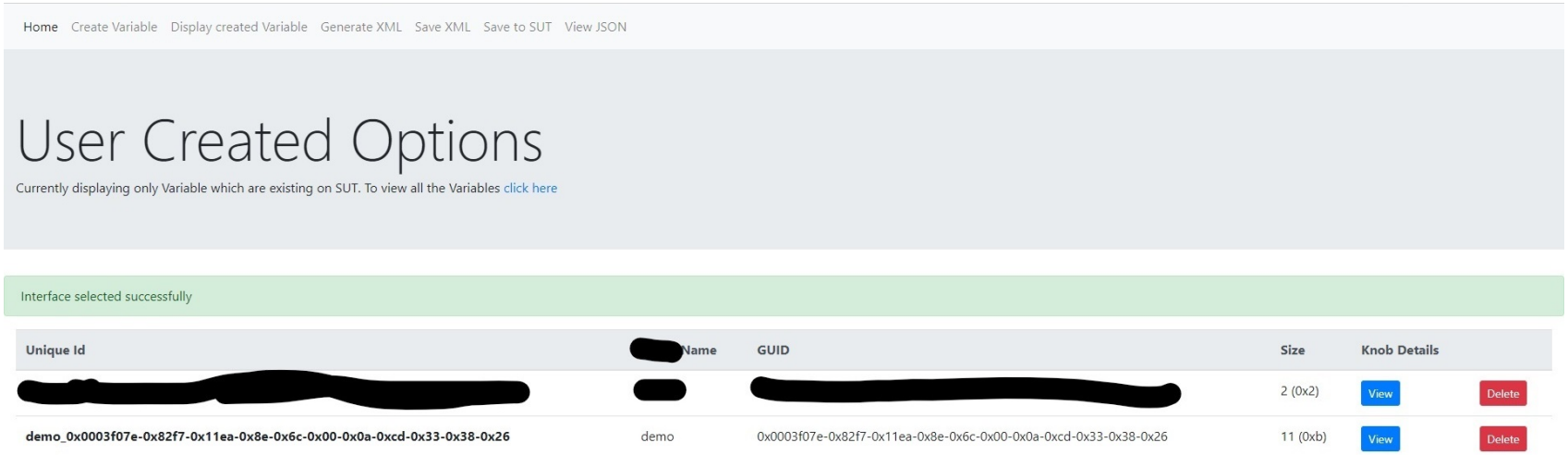
- Flask
- Ajax
- jQuery
- Javascript
- HTML/CSS
- XML
- JSON

Runtime UEFI Variable Creation: Implementation Snaps I



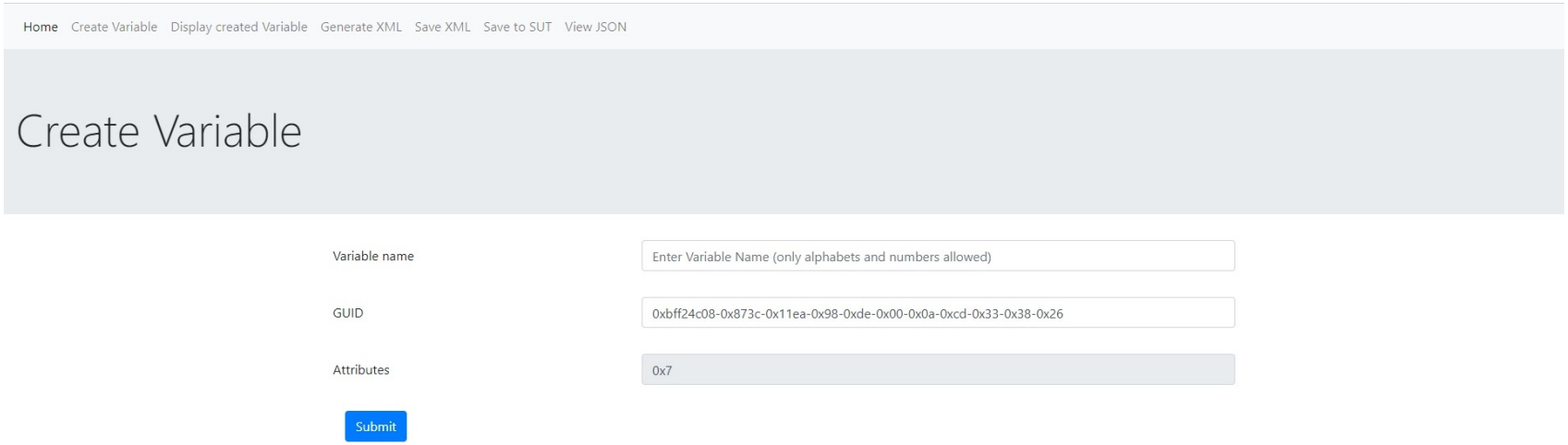
Home Page to Create UEFI Variable

Runtime UEFI Variable Creation: Implementation Snaps II



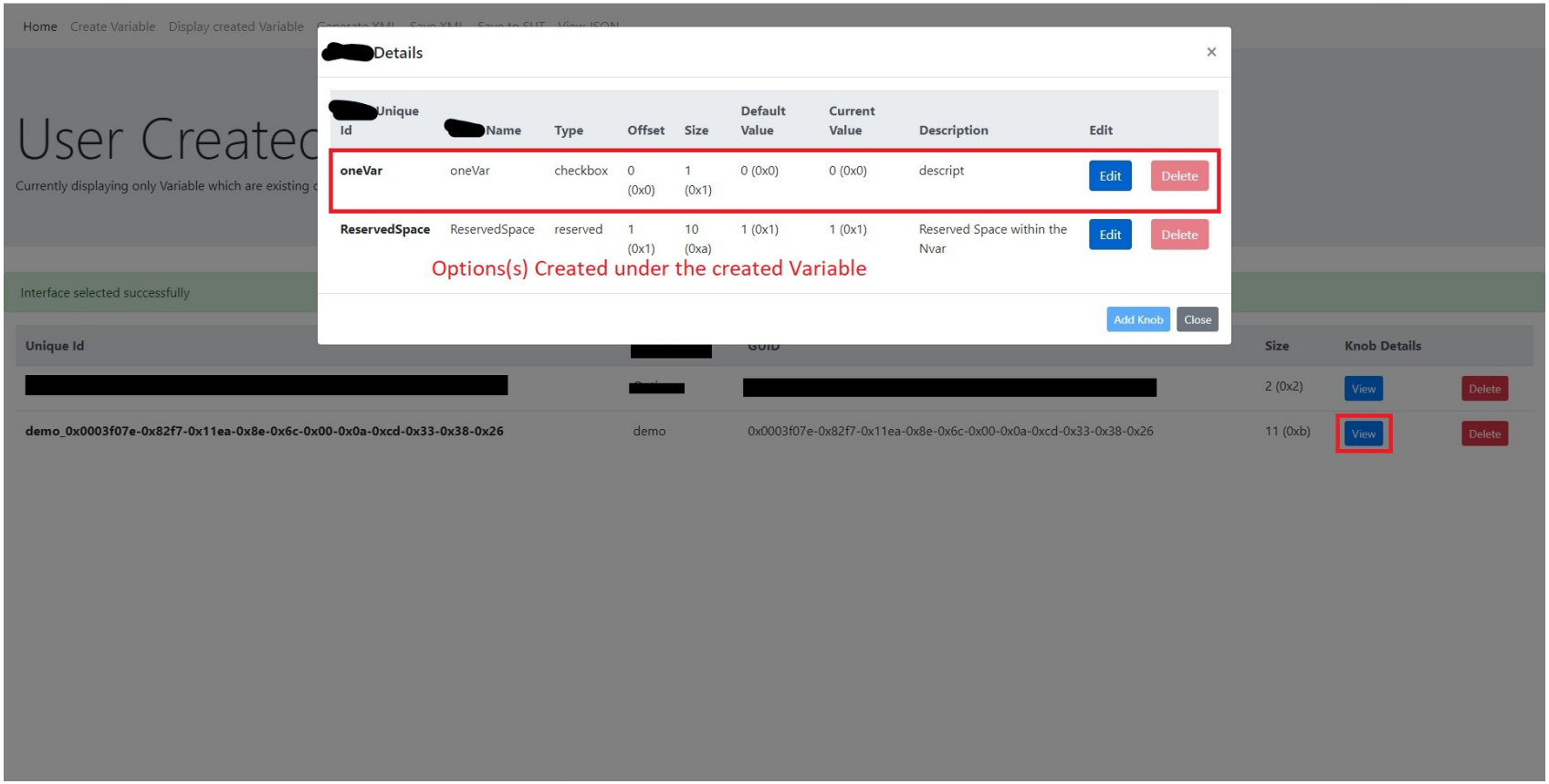
Variables created or exists on SUT

Runtime UEFI Variable Creation: Implementation Snaps III



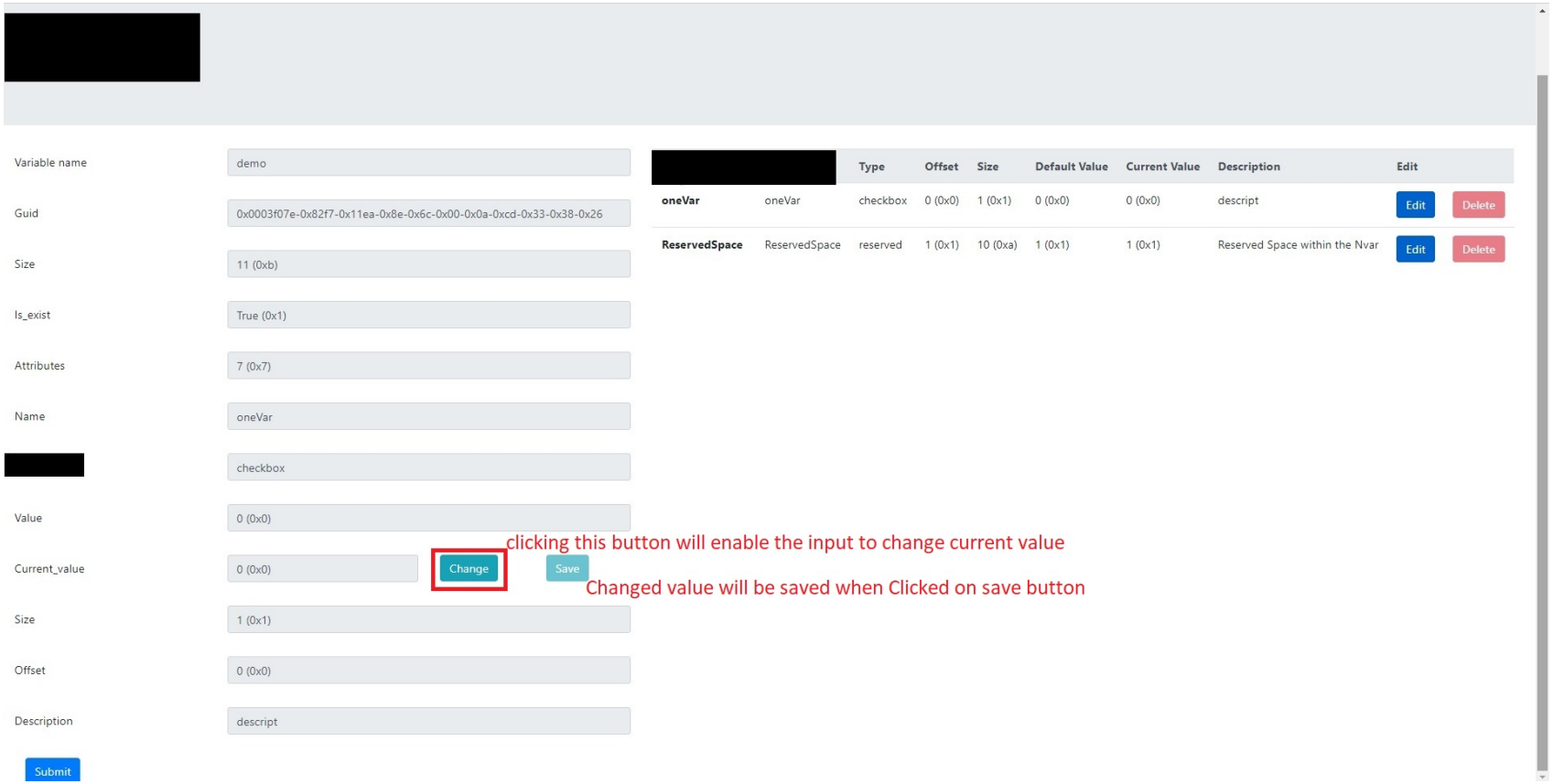
Create new UEFI Variable on SUT

Runtime UEFI Variable Creation: Implementation Snaps IV



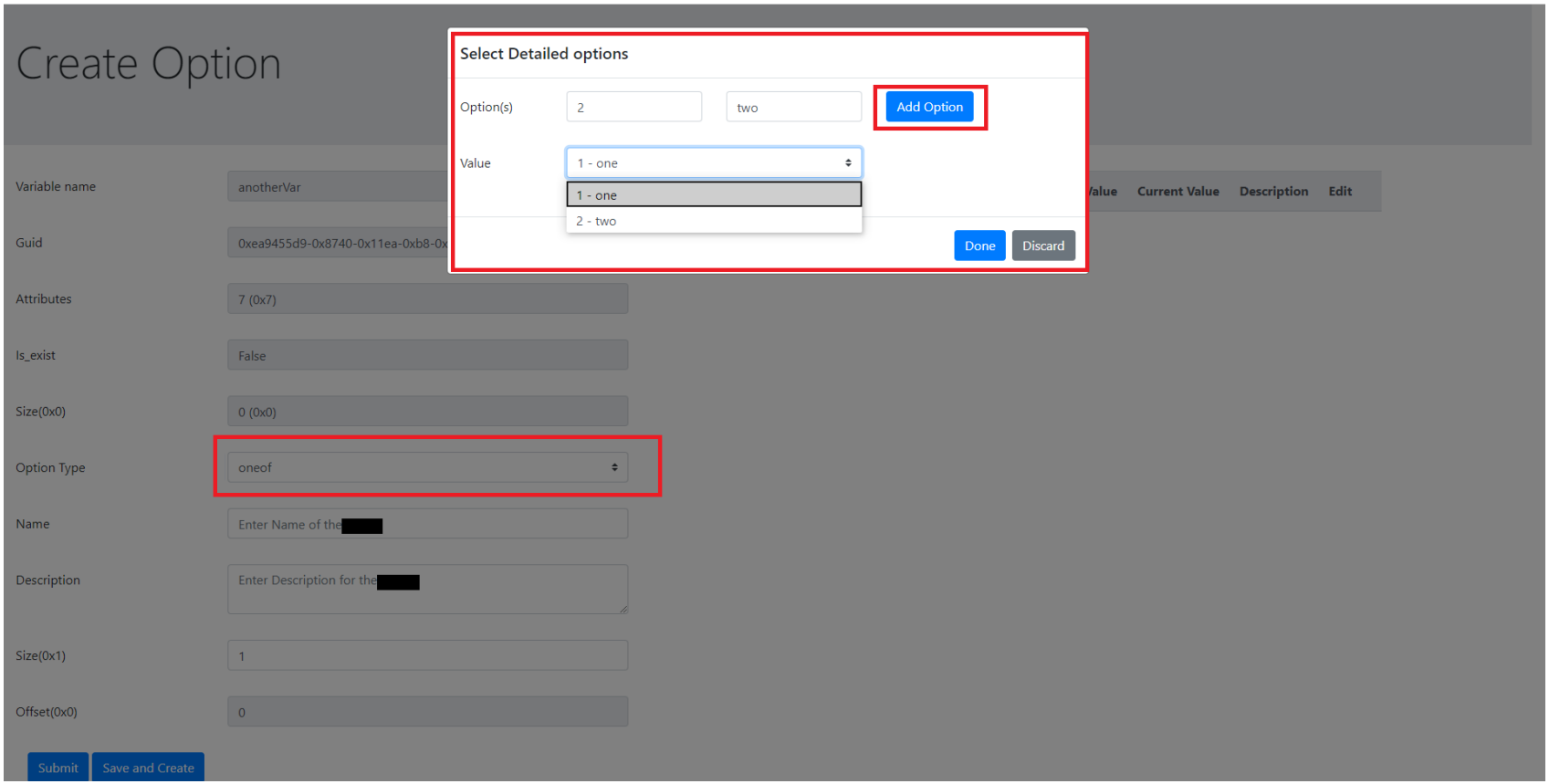
Options listed under Variable

Runtime UEFI Variable Creation: Implementation Snaps V



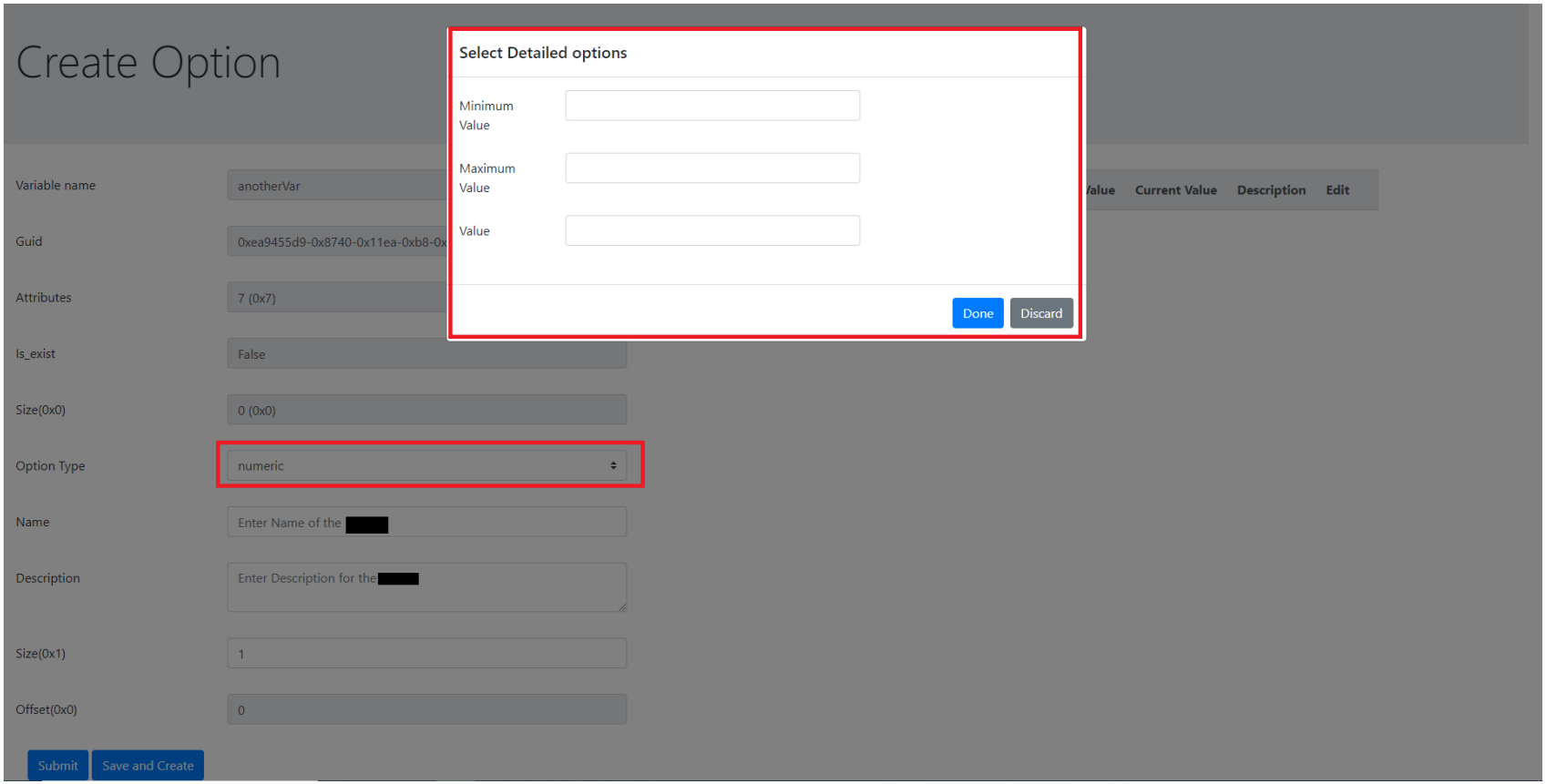
Edit the Existing Option Created under Variable SUT

Runtime UEFI Variable Creation: Implementation Snaps VI



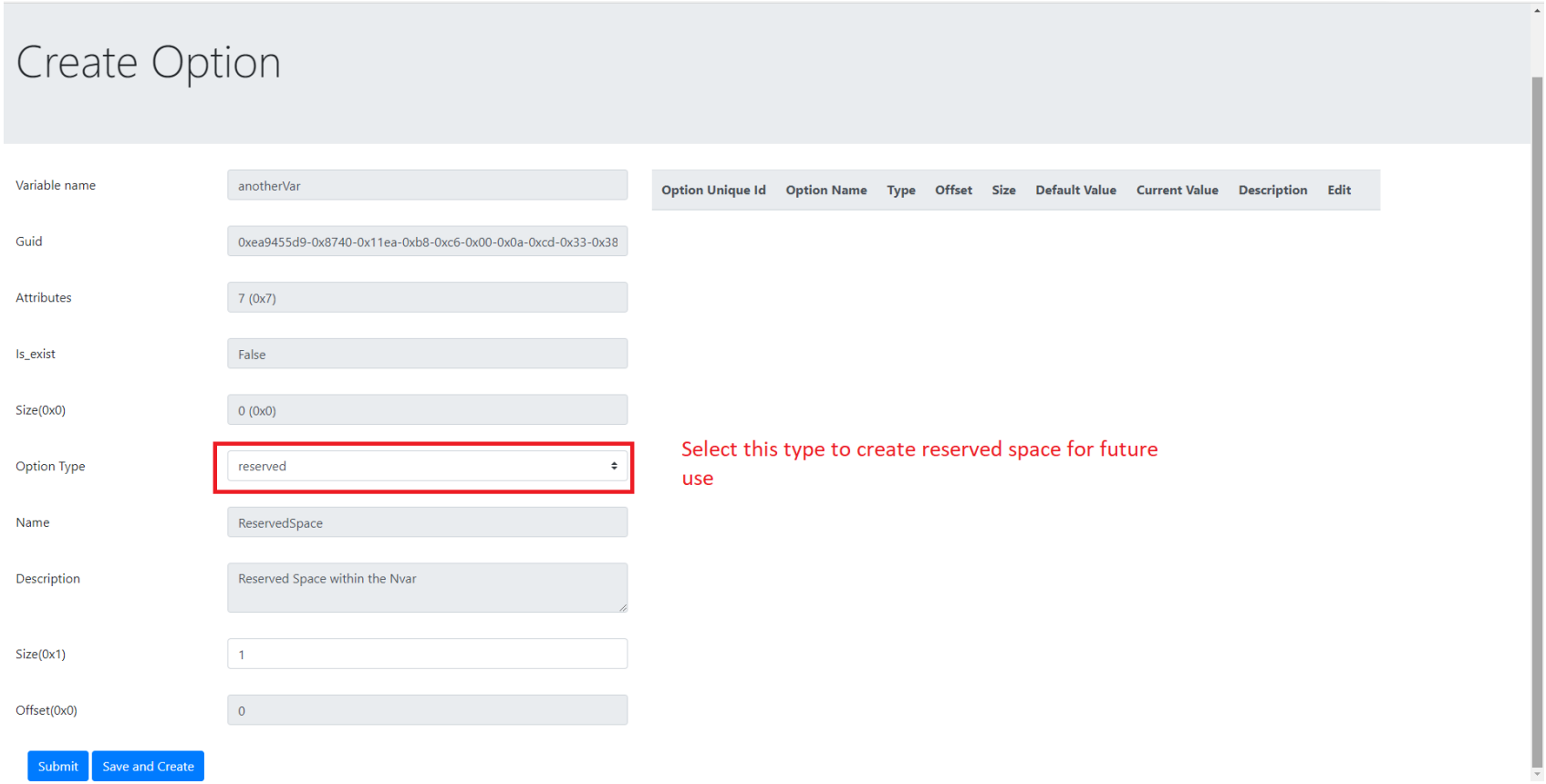
Create New Option(s) under Variable - Oneof Type

Runtime UEFI Variable Creation: Implementation Snaps VII



Create New Option(s) under Variable - Numeric Type

Runtime UEFI Variable Creation: Implementation Snaps VIII



Create Reserved Space for future use under Variable

Runtime UEFI Variable Creation: Implementation Snaps IX

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<SYSTEM>
   <!-- Generated by [redacted] -->
  ▼<Nvar name="Option" Guid="0xbff24c08-0x873c-0x11ea-0x98-0xde-0x00-0x0a-0xcd-0x33-0x38-0x26" Atributes="0x7" Size="0x2">
     <knob name="revision" setupType="numeric" default="0x1" CurrentVal="0x7" size="0x1" offset="0x0" description="Revision number" min="0x0" max="0xff"/>
    ▼<knob name="SubOption" setupType="oneof" default="0x4" CurrentVal="0x4" size="0x1" offset="0x1" description="option descriptions...">
      ▼<options>
         <option text="option 1" value="0x0"/>
         <option text="option 2" value="0x1"/>
         <option text="option 3" value="0x2"/>
         <option text="option 4" value="0x3"/>
         <option text="option 5" value="0x4"/>
       </options>
     </knob>
   </Nvar>
  ▼<Nvar name="demo" Guid="0x0003f07e-0x82f7-0x11ea-0x8e-0x6c-0x00-0x0a-0xcd-0x33-0x38-0x26" Atributes="0x7" Size="0xb">
     <knob name="oneVar" setupType="checkbox" default="0x0" CurrentVal="0x0" size="0x1" offset="0x0" description="descript"/>
     <knob name="ReservedSpace" setupType="reserved" default="0x1" CurrentVal="0x1" size="0xa" offset="0x1" description="Reserved Space within the Nvar"/>
   </Nvar>
 </SYSTEM>
```

Generate XML SUT

Runtime UEFI Variable Creation: Overview of GUI Actions

Button	Interpretation
Create Variable	Opens a form to create new Variable
Display Created Variable	lists out created variable
Generate XML	Generate XML from the stored session database
Save XML	Saves the generated XML on the storage device
Save to SUT	Applies the Pending changes action (Create/Delete/Modify) to SUT
View JSON	View the stored session database in the json format

Future Scope

- Development and testing of individual driver component rather than building the whole BIOS image
- AI powered Search Engine to enhance the findings of FAQs for relevant existing queries and articles
- Automating the initial BIOS Environment Setup
- Platform independent easy installation setup for the framework

NIRMA UNIVERSITY
INSTITUTE OF TECHNOLOGY

Thank You