ITSC 305 – Reverse Engineering of IoT Devices

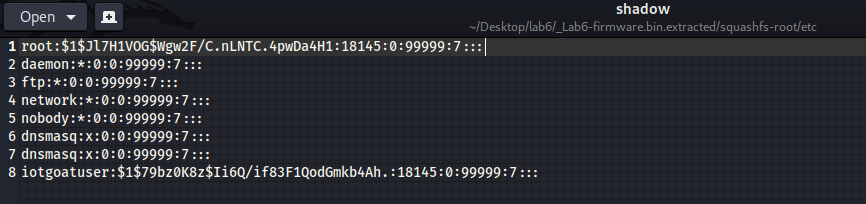
Lab 6

Coleton Sanheim

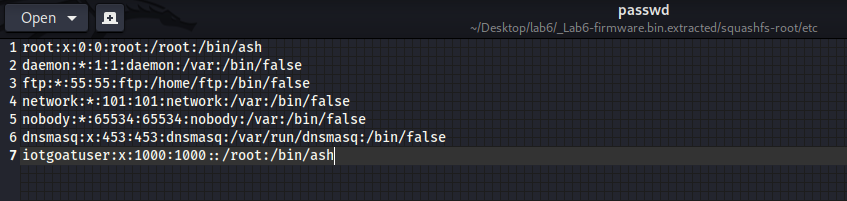
2022-04-24

Part 1:

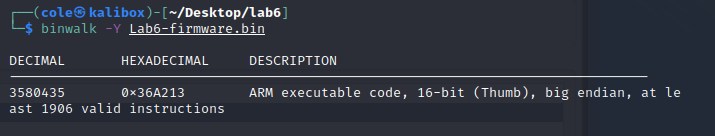
Here is the root password:



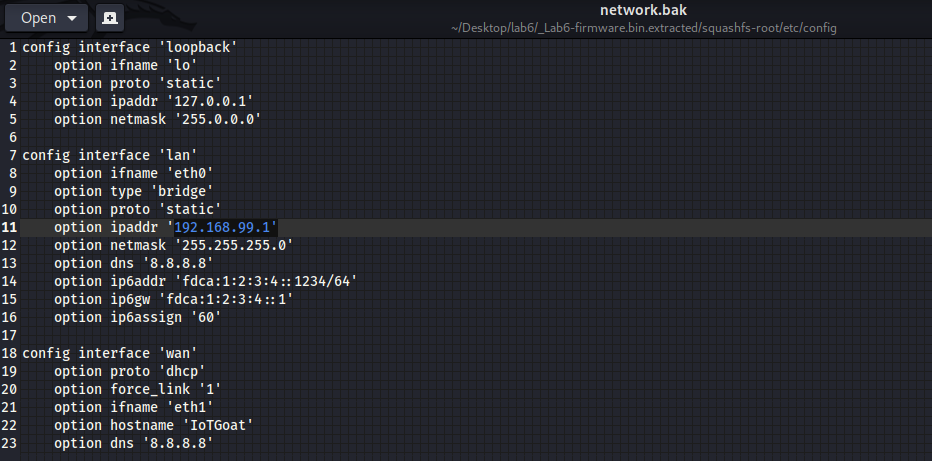
Here is the username of user #1000:



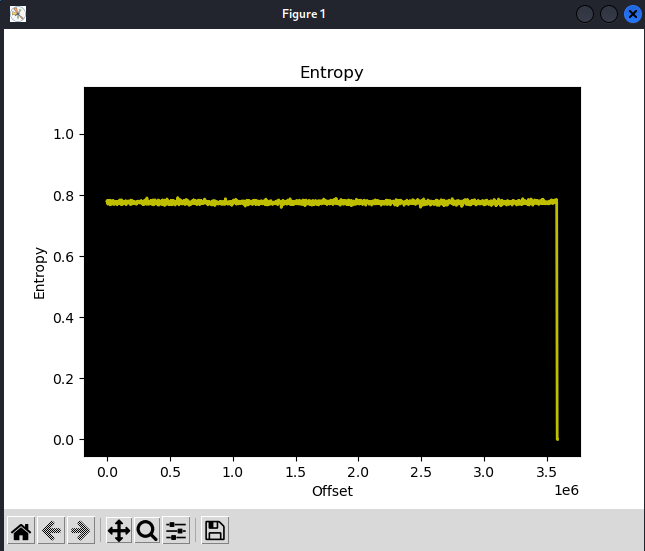
Here is the architecture of the system:



Here is the IP address of LAN

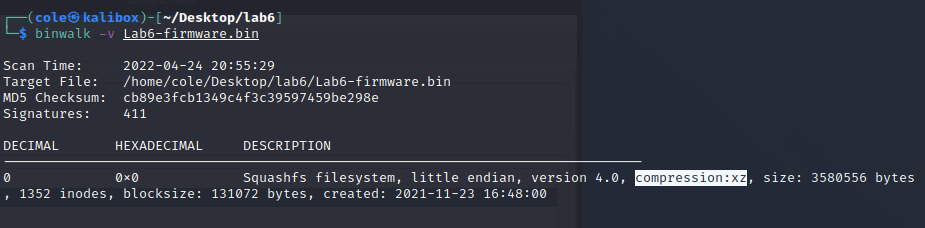


Here is the screenshot of the entropy:



Here you can see that the firmware is compressed, as the entropy doesn’t change at all and then suddenly changes to zero.

The compression is xz



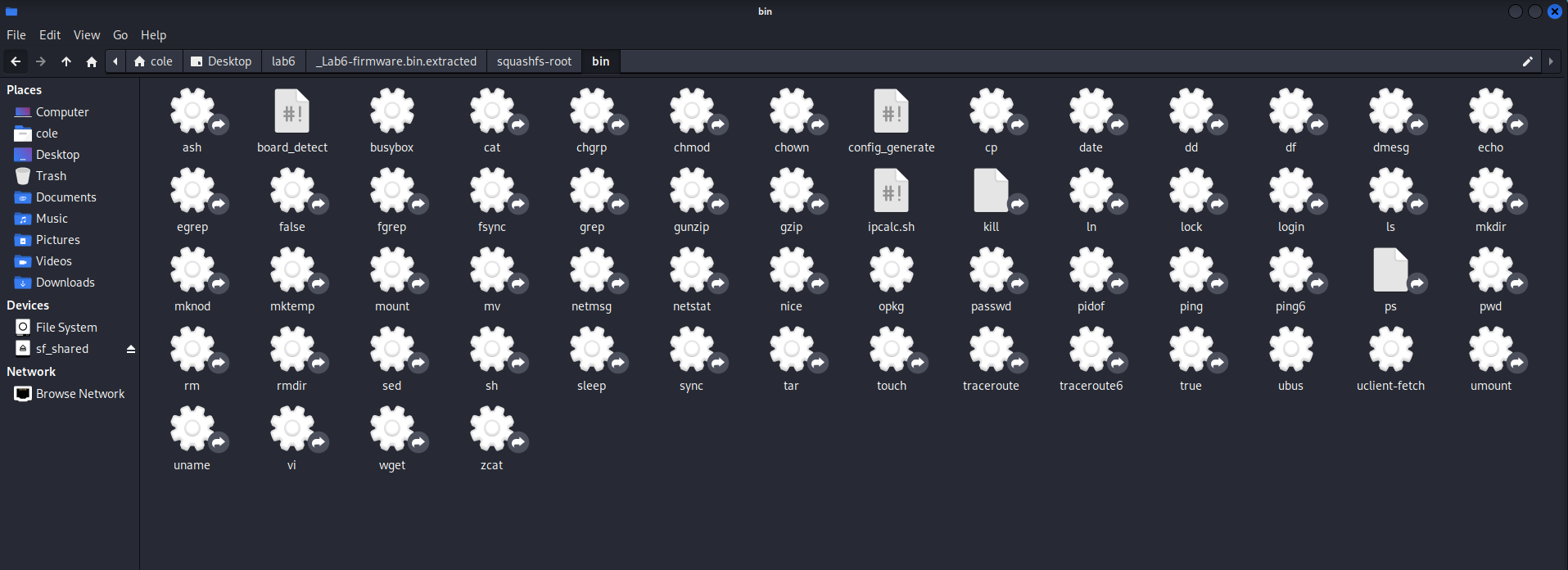
I would guess this is meant for general computing systems as the entropy is higher than what you would expect for an embedded system.

Here are two interesting things I found in the file structure:

A picture containing graphical user interface

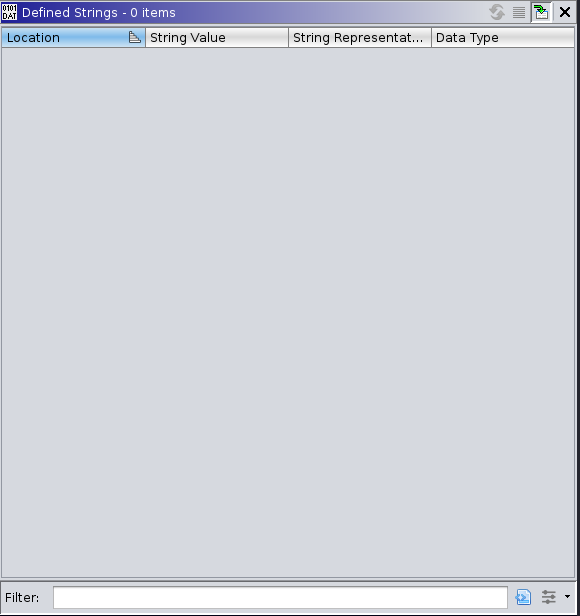
Description automatically generated

This is a screenshot I took in the www directory. After some research this appears to be a set up application for a router? Which seems weird to be present in this system.

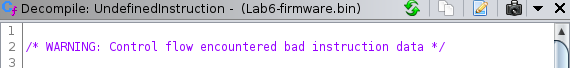


This is a screenshot I took of the bin directory. Here you can see commands that you can use when interacting with the system, however this is interesting to see as when compared with an actual systems commands, there is a fraction of the commands present, which seems strangely limited.

Here are two interesting things I found using Ghidra:



Ghidra was unable to define any strings in the file, which is interesting as this is the first time analyzing a file that didn’t have any defined strings.



Every function that was assembled in Ghidra was prefaced by this warning, which leads me to believe something about this file is unreabable to Ghidra.

Critical Reflection:

This was a very interesting thing to examine, however I was mostly lost when it came to examining this data. While examining the file structure I noticed lots of bash shell scripts and the like which seem to do with system processes. I also noticed that there was no saved data, (IE no user made files) which now that I think about it makes sense as this is a copy of a firmware and did not necessarily copy over any saved data. The Ghidra analysis was hard to understand, there was lots of data and I do not have the knowledge to fully understand what was being presented. However the main thing I noticed was that there was much less data to analyze here then there would be for other files I have looked at, (primarily malware samples). I do not know why this is the case and I couldn’t find a suitable answer when researching.