# SNOW CRASH

*Using QR codes as a means of cyber attack*

Design Manual

2020-12-11

Brendan D. Burke

C00232110@itcarlow.ie

# Contents

## Introduction

The Snow Crash project consists of a collection of attacks utilising QR code technology. This document sets out the main design details of the project and describes how it will be built. It defines the technologies that will be used for each section and how these technologies interact with each other. It will expand upon the use case diagrams featured in the project's functional specifications. It will also attempt to layout a project timeline.

## Technology Stack

### Libqrencode

Libqrencode is a fast and compact library for encoding data in a QR Code, a 2D symbology that can be scanned by handy terminals such as a smartphone. Libqrencode accepts a string or a list of data chunks as input and then encodes this in a QR Code symbol and saves it to a raw bitmap data array. It can then convert the bitmap to other image formats, as necessary (Fukuchi, 2020). Any QR codes generated will be converted to .png format due to it's portability.

### ZBar Bar Code Reader

ZBar Bar Code Reader is an open-source software suite for reading bar codes from various sources, such as video streams, image files and raw intensity sensors. It is very fast (can perform real time scanning from video streams), has a very small memory footprint, and the core scanner and decoder represent under 1K loc. Given that ZBar is the most popular open-source software suite used for reading bar codes it makes sense to use it as the main testing library (Brown, 2011). ZBar comes in two main forms, zbarimg and zbarcam. Both utilize the same library but zbarimg is for command line testing/reading and zbarcam is for reading in QR codes from a camera.

### feh

feh is a lightweight, configurable, and versatile image viewer aimed mostly at console users. It can also be started from graphical file managers. Apart from viewing images, it can compile text and thumbnail listings, show (un)loadable files, set X11 backgrounds, and more. Unlike most other viewers, it does not have a fancy GUI, but simply displays images. It is controlled via command line arguments and configurable key/mouse actions (Friesel, 2020).

### Dialog

Dialog is a Linux tool for creating simple TUI (Text-based User Interface) dialog boxes during shell scripts. These can be helpful for getting input and may be considered more intuitive by a number of users. Dialog can be used to create a number of different TUI forms such as message boxes, forms, calendars, etc. Dialog makes use of the ncurses library bundled with most Linux distros.

### GitHub

GitHub will serve as a remote repository for source code control. In the event something breaks or gets deleted it can be used to rollback to previous, working versions.

### Virtualbox

Any testing of QR codes that are potentially dangerous should be done inside a virtual machine (Android, Windows).

### Kali

The Wireless attack described in Section 2 of the project will be conducted using Kali Linux and a suitable external wireless adapter capable of running in master mode as it will have to act as an access point for the victim to connect to.

### Wifipumpkin3

Wifipumpkin3 is a framework for wireless network attacks. It is not installed with Kali by default. It is written in Python 3 and has a small number of dependencies which can be installed on Kali or any other Debian-based system.

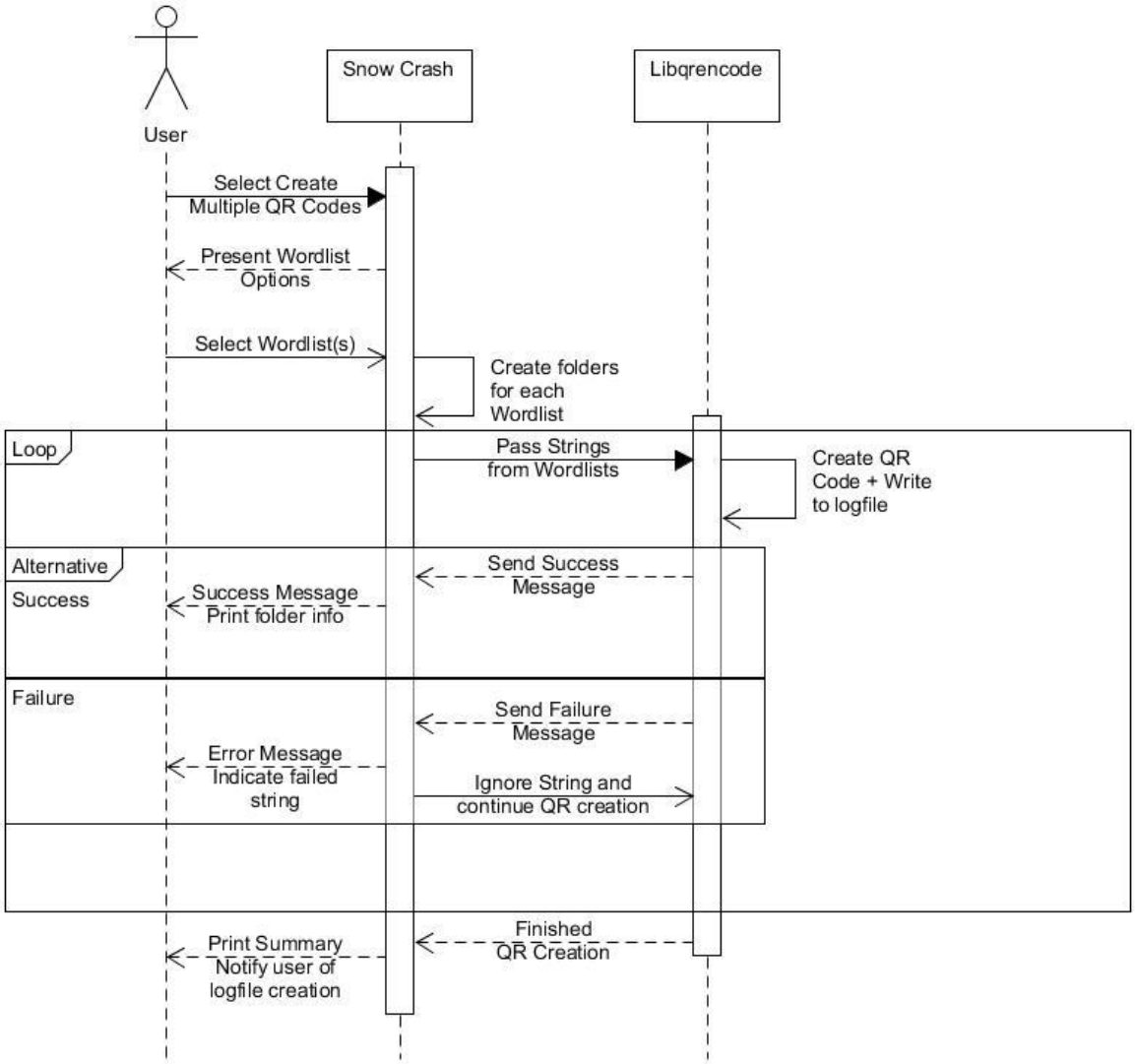
### Android Studio

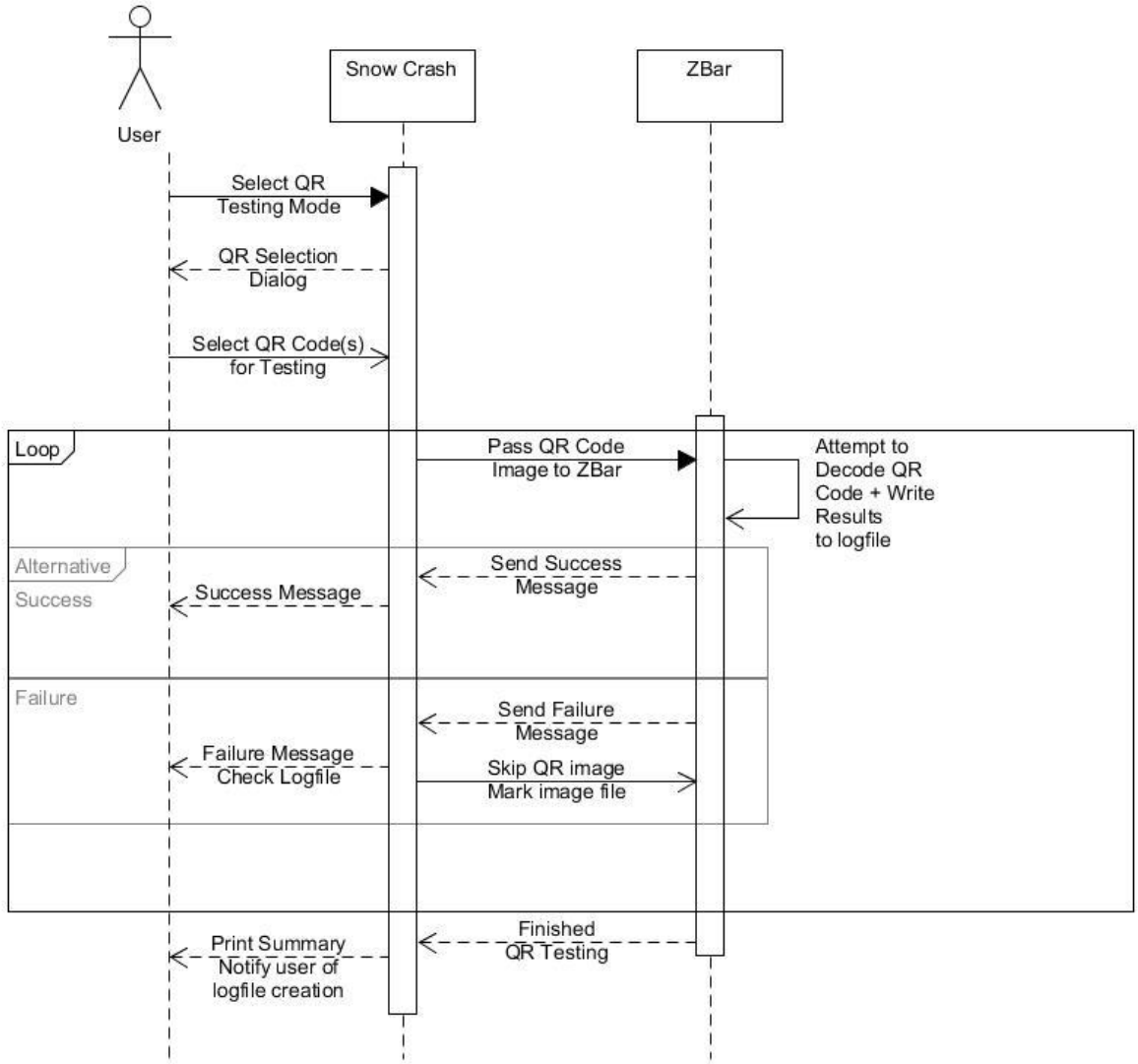
Android Studio is the de facto IDE for developing, testing, and debugging Android apps. It also contains an emulator for testing apps; however, this emulator is not sandboxed and should not be used for testing malware.

### Android-x86

Android-x86 is an open-source project that allows you to run the Android operating system in a virtual machine. It allows for multiple versions of Android (6.0, 7.1, 8.1, LineageOS roms, etc.) to be installed. These ports are fully featured and can perform many of the functions a real mobile device can including access Google Play.

## Sequence Diagrams


User
Snow Crash
Libqrencode
Select Create Multiple QR Codes
Present Wordlist Options
Select Wordlist(s)
Create folders for each Wordlist
Loop
Pass Strings from Wordlists
Create QR Code + Write to logfile
Alternative
Success
Send Success Message
Success Message Print folder info
Failure
Send Failure Message
Error Message Indicate failed string
Ignore String and continue QR creation
Finished QR Creation
Print Summary Notify user of logfile creation




## Project Timeline

| Week | Due Date | Deliverable |
|---|---|---|
| 1 | 25/12/2020 | Xmas Break. |
| 2 | 01/01/2021 | Start compiling wordlists. Create basic Bash/ZSH script that creates QR codes using said wordlists. Review documentation to date. |
| 3 | 08/01/2021 | Continue with basic script. Review documentation to date. |
| 4 | 15/01/2021 | Start integrating TUI elements using Dialog. |
| 5 | 22/01/2021 | Introduce ZBar testing library and work on logging. |
| 6 | 29/01/2021 | Add feh and work on slideshow feature. |
| 7 | 05/02/2021 | Add error-checking, crash-recovery, and clean up code. |
| 8 | 12/02/2021 | Add error-checking, crash-recovery, and clean up code. |

| | | |
|---|---|---|
| 9 | 19/02/2021 | Section 2, Attack 1. Perform, video, document, etc. |
| 10 | 26/02/2021 | Section 2, Attack 1. Perform, video, document, etc. |
| 11 | 05/03/2021 | Section 2, Attack 2. Perform, video, document, etc. |
| 12 | 12/03/2021 | Section 2, Attack 2. Perform, video, document, etc. |
| 13 | 19/03/2021 | Section 2, Attack 3. Perform, video, document, etc. |
| 14 | 26/03/2021 | Section 2, Attack 3. Perform, video, document, etc. |
| 15 | 02/04/2021 | Section 3 QR code Malware, work on final documentation and demo. |
| 16 | 09/04/2021 | Section 3 QR code Malware. If Android apk version does not work by this week swap to Windows implementation and write malicious exe. |
| 17 | 16/04/2021 | Section 3 QR code Malware, work on final documentation and demo. |
| 18 | 23/04/2021 | Section 3 QR code Malware, work on final documentation and demo. |
| 19 | 30/04/2021 | Final week, get everything together and submit. |

## Bibliography

Brown, J., 2011. *ZBar bar code reader.* [Online]
Available at: http://zbar.sourceforge.net/
[Accessed 10 December 2020].

Friesel, D., 2020. *Feh – Image viewer and Cataloguer.* [Online]
Available at: https://github.com/derf/feh
[Accessed 10 December 2020].

Fukuchi, K., 2020. *Libqrencode.* [Online]
Available at: https://fukuchi.org/works/qrencode/
[Accessed 10 December 2020].