Documenting my (Nearly Successful) Attempt to Location Spoof in Ingress

by Kaitlin O’Brien

This past week, I have tried to extend beyond my academic comfort zone to explore new concepts and I feel like nothing showcases this as much as my final blog post. I decided that after my exploration of hacking concepts, exploitation in Ingress and location spoofing, I would try my hand at following a few threads and testing out their instructions to ascertain overall feasibility and to learn the degree of accessibility these location spoofing instructions have. After all, I don’t claim to be overtly tech-savvy but I am open to putting my best foot forward to have my avatar in Ingress show up geographically half a world away.

Going into this venture, I wanted to establish what I was and was not comfortable doing with my technology in order to location spoof. I consider myself a novice when it comes to tinkering with technology, and because of this coupled with the fear that I would negatively impact my device or get banned consequently from Pokémon Go for tampering with Ingress settings, I decided that I was uncomfortable with jail breaking my phone, I would not delete my operating system or tamper at great length with overlaying another one on top of my existing one, I would not download suspicious files and I would ask for help in accomplishing my desired result if I was experiencing difficulties. Through various Google searches I returned results that led me to in turn download the following applications to my mobile device:

- The Droid4x which is described here. Verdict: unsuccessful.

- The Change Gps Location application. Verdict: unsuccessful.
- The Fake-A-Location Free application. Verdict: unsuccessful.
- The MAPic- Geotag & Location Editor application. Verdict: unsuccessful.

I read several Subreddit threads related to Pokemon Go Dev, but found that in a lot of cases, I was uncomfortable with the degree of technology knowledge necessary for me to execute my task.

My friend is a recent graduate from the University of Waterloo with a Computer Science degree so I figured he would be a good person to enlist the help of to location spoof on Ingress. From my friend's knowledge background, he noted that it would be easier to spoof an Android than an iPhone because, as this article also corroborates "While Apple's apps must all be vetted by the company to run on its phones, Google allows users to run unapproved apps as well. Apps not purchased from Google's own app store can contain malicious code that could allow an outsider to access the phone" (Weis & Baig, "Apple, Android, Blackberry Phones, What Can't Be Hacked?").

Because of the aforementioned details, my friend suggested I download an Android Emulator on my laptop because he also suspected it would be difficult to download directly to my laptop. To do this, I enlisted the help of Nic Watson, who recommended that I download Android Studio. Once it was downloaded, Nic and I decided to continue to try and work toward location spoofing on our own.

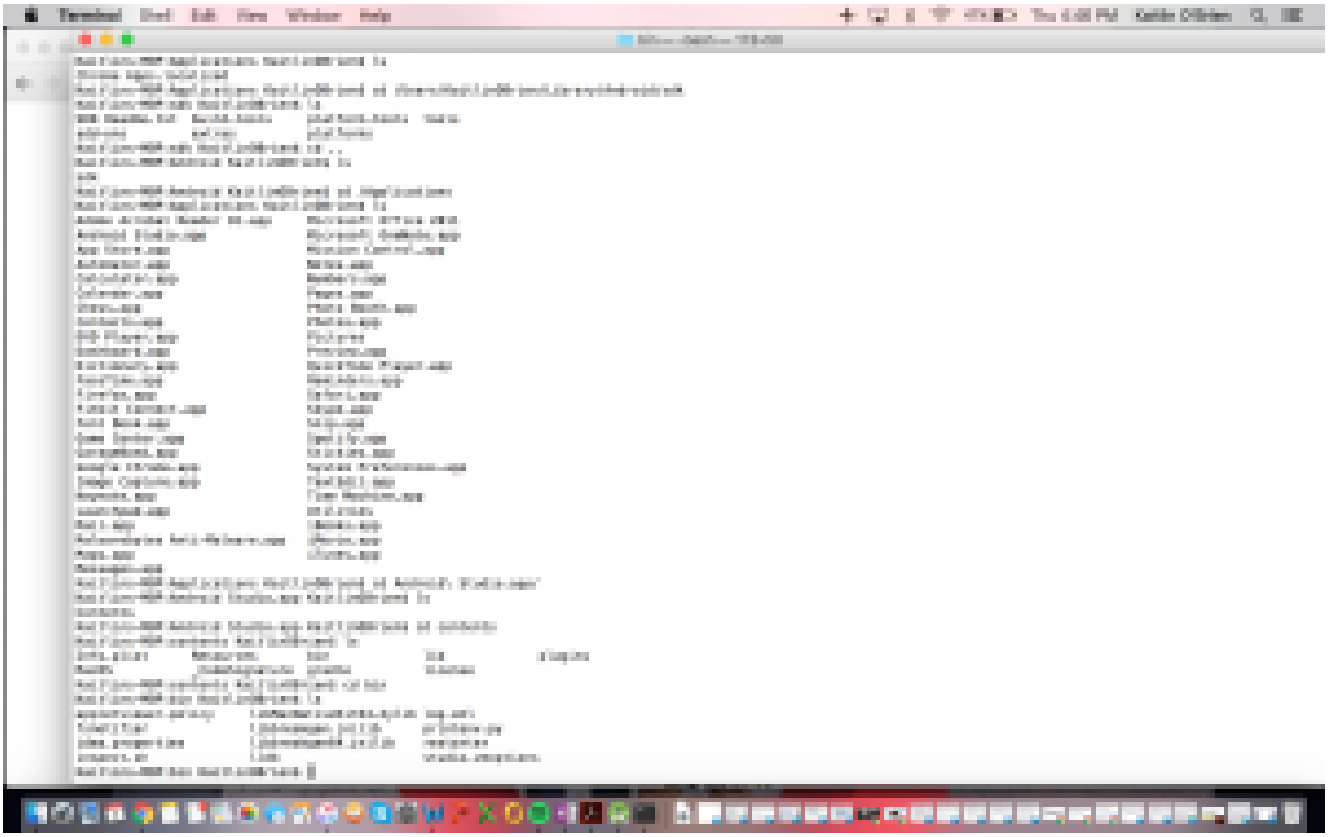
We used the following links to further our motives, but they were to no avail:

http://smallbusiness.chron.com/getting-android-emulator-running-os-x-38684.html.

http://stackoverflow.com/questions/16271242/launch-android-sdk

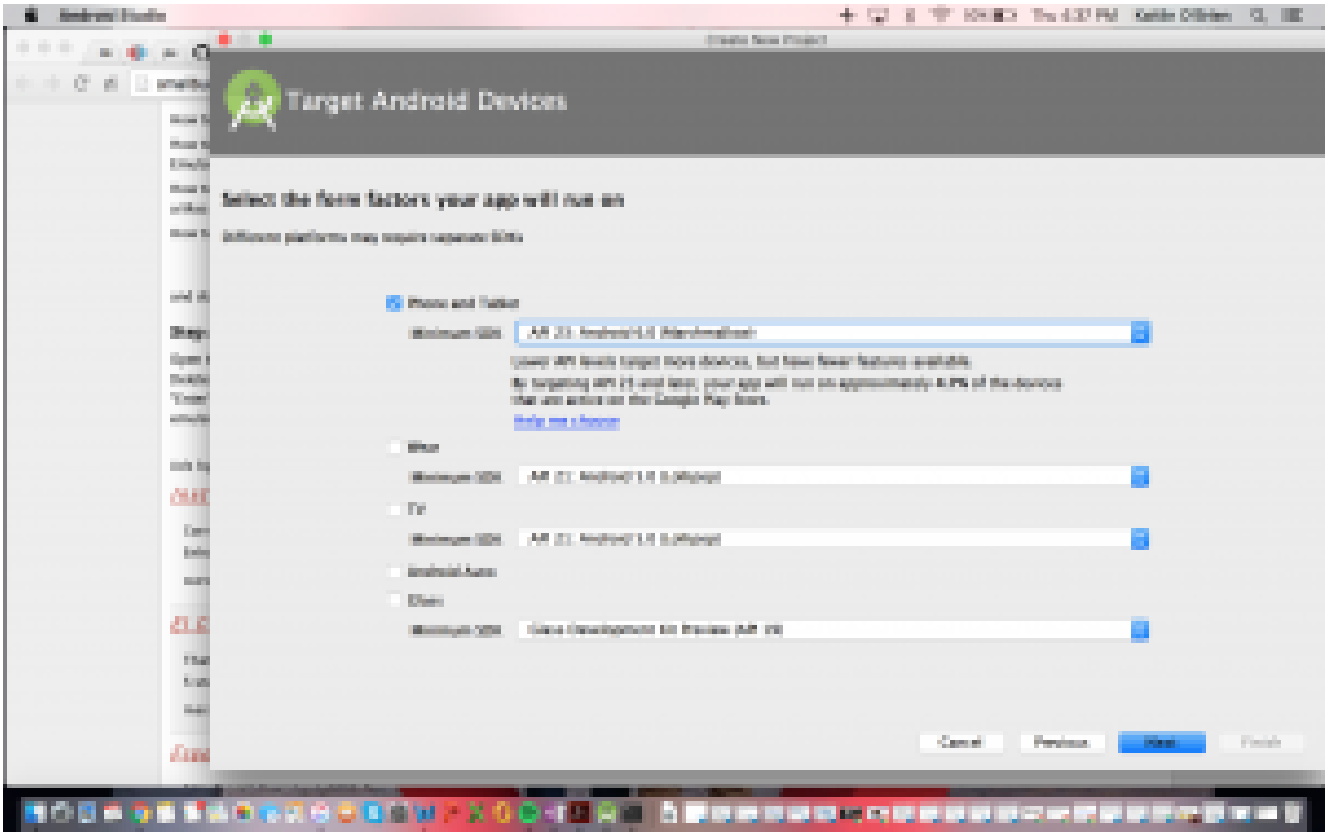
-manager-tools-directory-doesnt-exist-mac

At one point, we were trying to perform some code to reveal some of the contents of the Android Studio folder:



After that link didn’t work, I decided to reach out to my computer science friend again. We troubleshooted during our Skype discussion, and here’s a summary of what we did:

From the Android Studio, I attempted to run an Android Emulator within the developer tools and then installed Ingress on that emulator.



I came across a “Must not use mock locations” message right away, which requires the user to disable developer tools, which I learned was a group of super-settings that allow a user to change aspects of the emulator that normally wouldn’t be seen in Android devices. I was pleased to have gotten this far so that essentially my efforts had been recognized as an attempt to location spoof. Realistically, if I had attempted to perform this task a year or two ago, there is a chance that this effort would have worked because at that point Niantic may not have established a barrier to thwart my efforts.

The removal of developer tools took away my ability to set my location by hand, ruling this method ineffective. The second method is using an android emulator called BlueStacks and I essentially ran into the same problem of disabling location services. I know BlueStacks uses OSX location services that I was unable to emulate due to the technical detail required (I would have to write lots of code). My friend and I assumed that since this spoofing protection on Android exists, it probably exists on IOS. Further investigation of how people cheat in Ingress on Android revealed that people use a different operating system, which may cause irreparable damage to one’s device and the same thing on IOS (a jailbroken system of the operating system voids the warranty). My most recent version of iPhone doesn’t have a jailbroken version available online, so I wouldn’t be able to do that anyway.

If I wanted to investigate this further and over a longer time span, I could write software in order to spoof my MAC address such that I could predictably match my MAC address to the location I want to go, but due to the speed detection in Ingress (users are flagged by Ingress and issued a warning in the game if their speed exceeds 40 km/h), I would have to do

it in a way that creates a believable movement path throughout the world, and all of that would take a significant amount of development effort.

Yesterday's class placed a heavy emphasis on textual communities, which are defined in Carolyn Marvin's W*hen Old Technologies Were New: Thinking About Electric Communication in the Late Nineteenth Century* as, "groups that rally around authoritative texts and their designated interpreters" (Marvin 12). In the context of Ingress, location spoofers are themselves a group of people that are connected because of their shared practice, and that makes them their own textual community. Regarding location spoofers in the context of textual communities helped me to see these game players not as individuals with malicious intent but instead as people who want to push affordances in the game that could allow them to test the limits of the game play relating to their particular character.

Works Cited

Marvin, Carolyn. "Introduction" and "Inventing the Expert." W*hen Old Technologies Were New: Thinking Aaout Electric Communication in the Late Nineteenth Century*. New York/Oxford: Oxford University Press, 1988. 3-62.

Weise, Elizabeth, and Edward Baig. "Apple, Android, Blackberry Phones, What Can't Be Hacked?" *USA Today* 29 Feb. 2016.