# VRC High School - Reverse Engineering Online Challenge

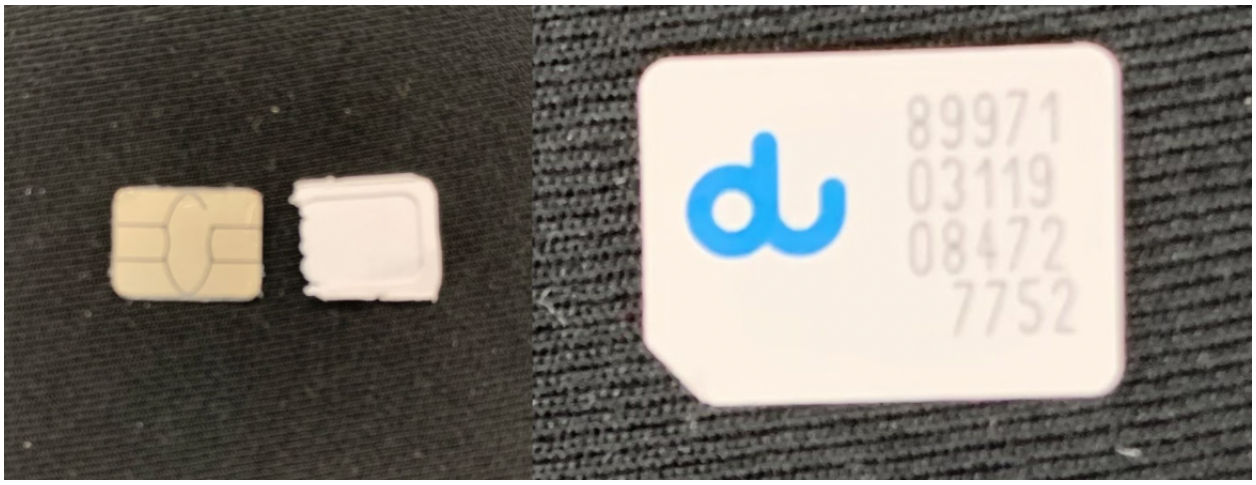
By: Max Buffetta, Alex Buffetta, and Arjun Verma

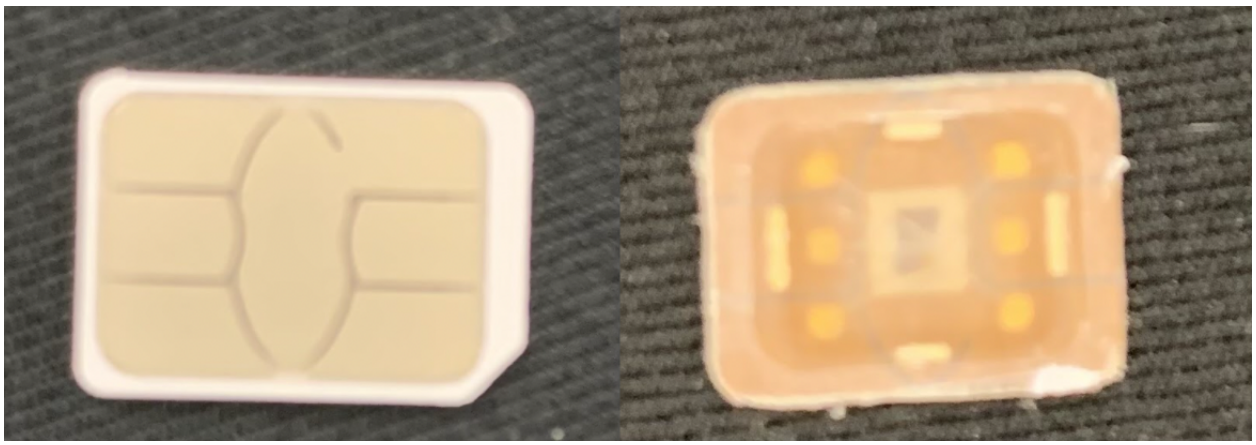
421C

Indian Hill High School, 6865 Drake Rd, Cincinnati, Ohio, USA 45243

**Introduction**

The electronic device our team chose to reverse engineer is a SIM card: a chip that goes into phones and computers to hold information, carrying an identification number unique to the owner, and preventing operation if removed. We selected this device because, while it may be small, it is a very intricate and unique piece of technology that can hold a lot of information. A SIM card contains a unique serial number (ICCID), international mobile subscriber identity (IMSI), security authentication, and much more. SIM cards come in different sizes starting from full SIM then mini-SIM, micro-SIM, nano-SIM, and embedded SIM. Different phones and computers use different size SIM cards for adaptability. You receive a SIM card from the phone or computer carrier that you subscribe to. For example, if you have a Verizon phone, you would need to ask Verizon for a SIM card.

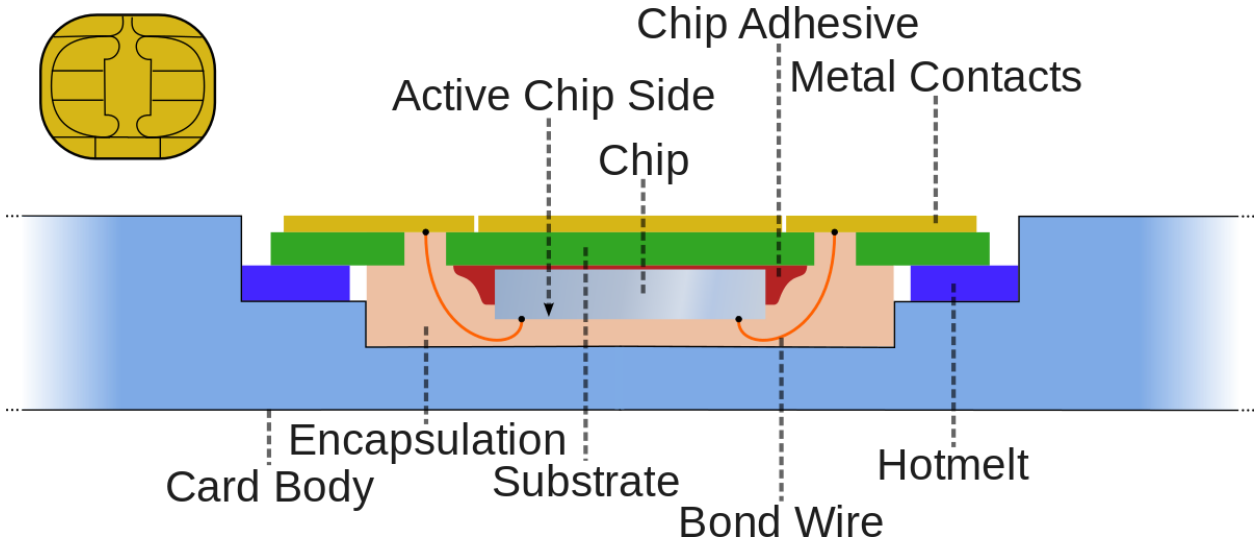


The images above show the SIM card our team took apart.

**Parts List**

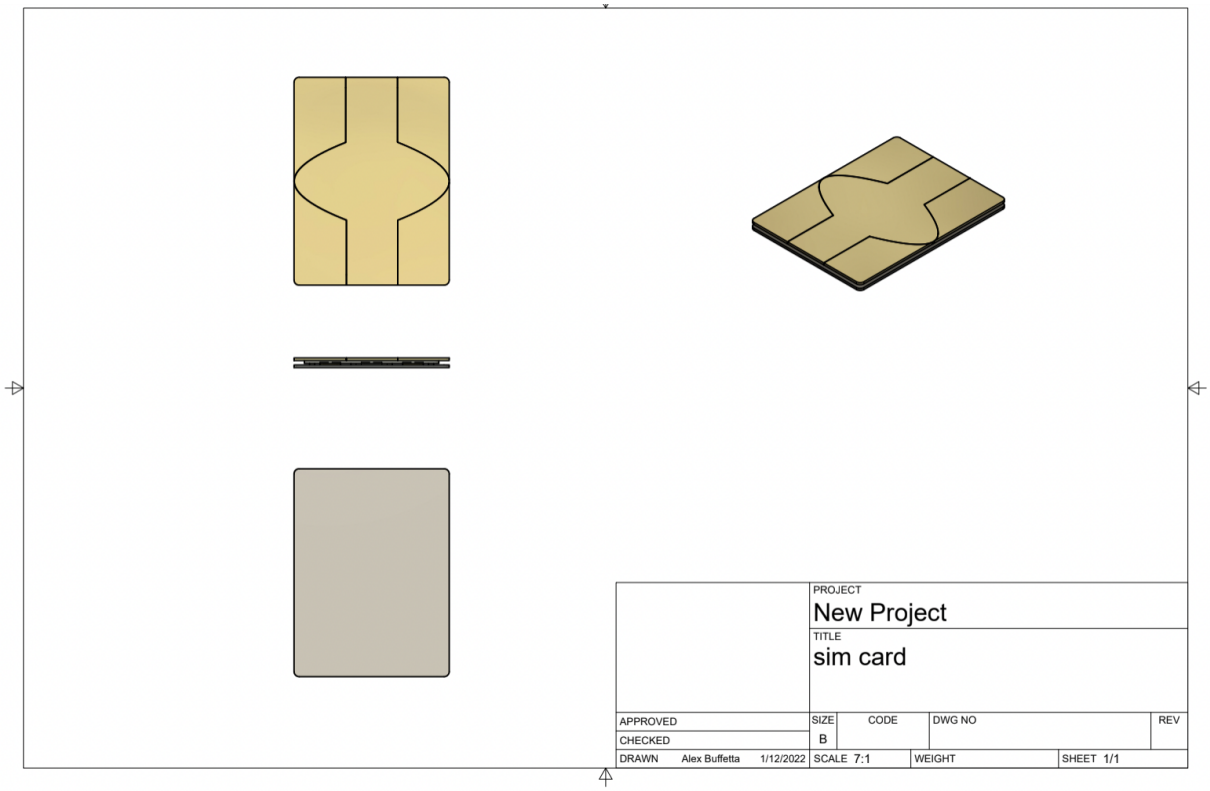
Components found inside a SIM card include: metal contacts, chip adhesive, substrate, chip, active chip side, hotmelt, bound wire, encapsulation, and the card body. The most important part of the SIM card is the chip. The chip is what stores all the information and what allows you to connect to your network. Components like the chip adhesive and the encapsulation are like a protective shield that protects the data and prevents the data from being damaged. The shiny copper pieces on the SIM card are the metal contacts that conduct electricity. The bound wire connects the chip to the metal contacts allowing the electricity to flow. The substrate is the layer that all the components are assembled upon. The hotmelt is just glue that also aids in holding the card together. The card body encases the chip and protects it from getting damaged. These components come together and form the SIM card which can then store large amounts of data.

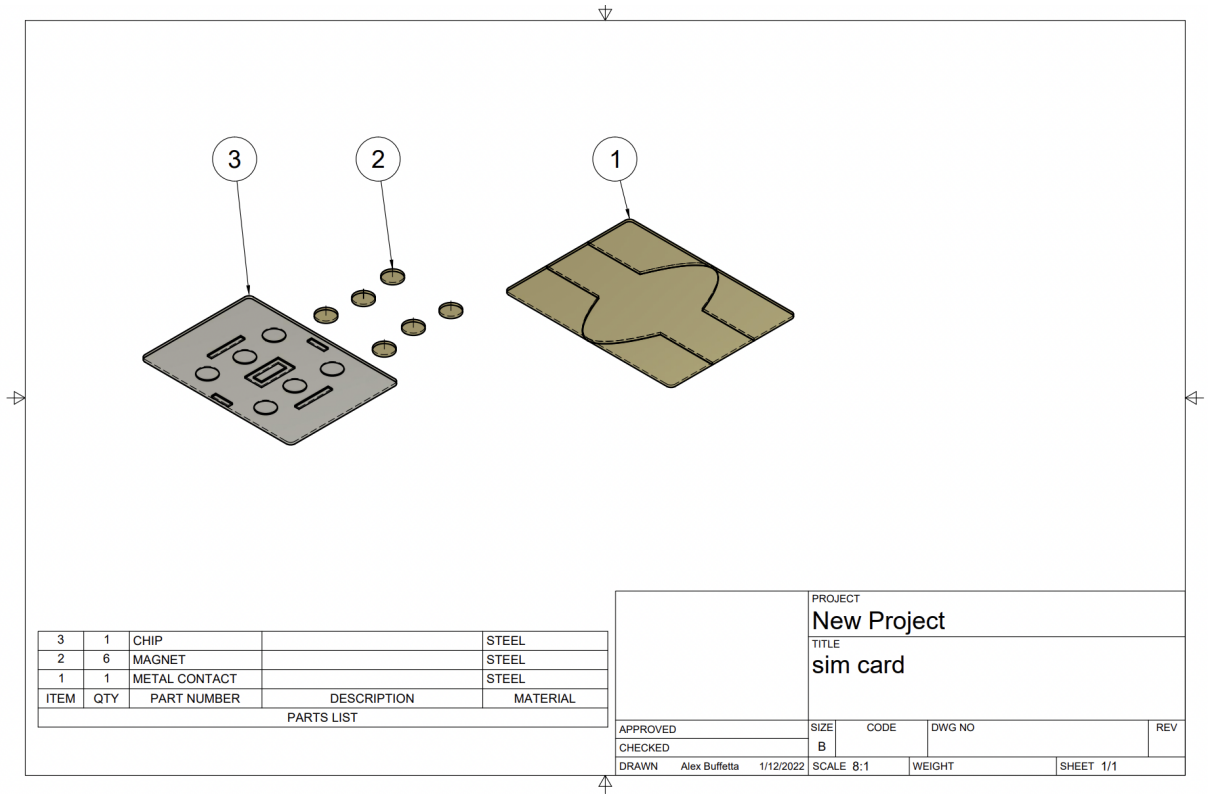



Above is an image containing all the components of a SIM card.

## Reconstruction

Below are two 3D models of the SIM card made in Autodesk Fusion 360.



## Conclusion

The lesson that we learned from this project is that SIM cards are more complex than they look. A SIM card has several intricate parts that allow it to become an extremely efficient, yet compact device for storing specific pieces of data. While the direct most application of SIM cards comes from use in mobile devices, recent devices utilize SIM cards as near field communicators (NFC). As we have seen with the components of the SIM card, its unique design and security will allow it to have a multitude of new applications, with an emphasis on user privacy. Overall, our deep dive into a relatively “simple” electronic device was quite complex and showed us the true ingenuity of a piece of technology the size of your fingernail.

# Works Cited

Anthony, Sebastian. “The Humble SIM Card Has Finally Been Hacked: Billions of Phones at Risk of Data Theft, Premium Rate Scams - ExtremeTech.” *ExtremeTech*, 22 July 2013

Andersson, Jonas. “SIM Cards – the New Frontier for Biometrics.” *Card technology today* 21.4 (2009): 10–11. Web.

“SIM Card Forensics: An Introduction - Infosec Resources.” *Infosec Resources*, 12 June 2021, resources.infosecinstitute.com/topic/sim-card-forensics-introduction/.