**Team Name:** Noble Team

**Current Leader:** Viren Kumar

**Members:** Melanie Brown, Marwan Elashry, Viren Kumar, Tanya Malik, Emily Nolan, and Lucas Scharf

**Melanie Brown:** Test that Cortana’s wake word is still “Hey Cortana”. “Cortana” alone works as well. Tested on my personal computer. Windows 10 VM Cortana would not recognize voice. My laptop’s microphone worked in the VM, but not with waking Cortana.

**Marwan Elashry:** Tested Cortana’s wake word and found out that both “Hey Cortana” and “Cortana” work. It worked only when I tested it on my windows laptop, but not my mac laptop.

**Viren Kumar:** Recreated file structure findings from last year including, Cortana’s primary directory, Cortana’s local saved data for an individual user, SQLite database files with plain text of chat history. Recreated code analysis findings from last year including, disassembling in Ghidra revealing the number of functions. Recreated network communication finding of encrypted traffic sent via TLS. Attempted to decrypt TLS traffic using these sources:

<https://resources.infosecinstitute.com/topic/decrypting-ssl-tls-traffic-with-wireshark/>

<https://www.youtube.com/watch?v=5qecyZHL-GU&t=310s&ab_channel=ChrisGreer>

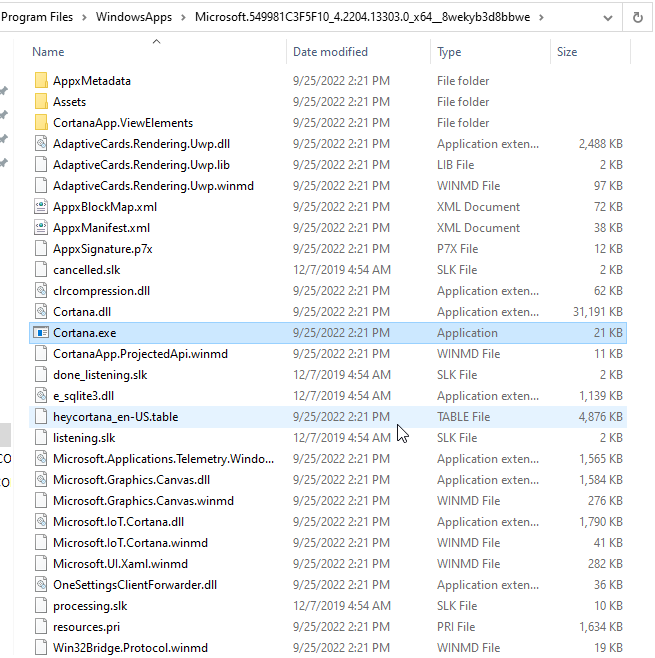
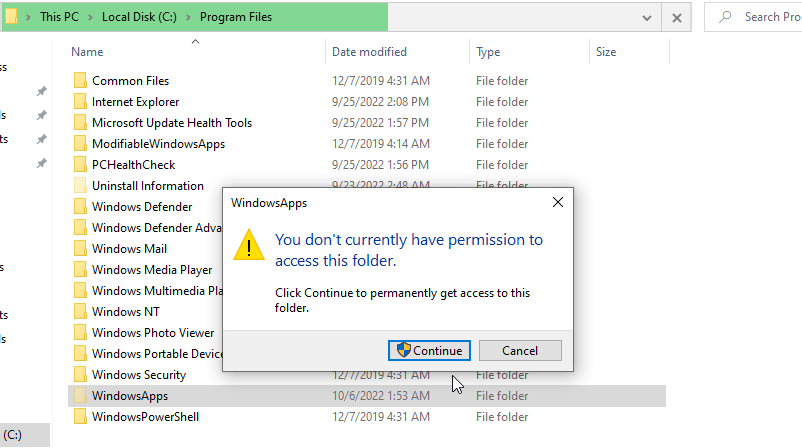
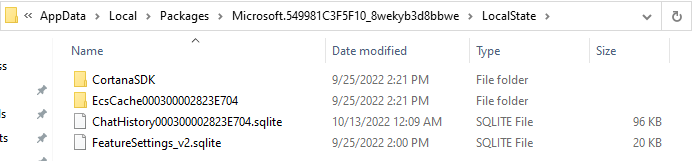
Tested Cortana’s wake word’s (“Hey Cortana” and “Cortana”), worked on my VM.

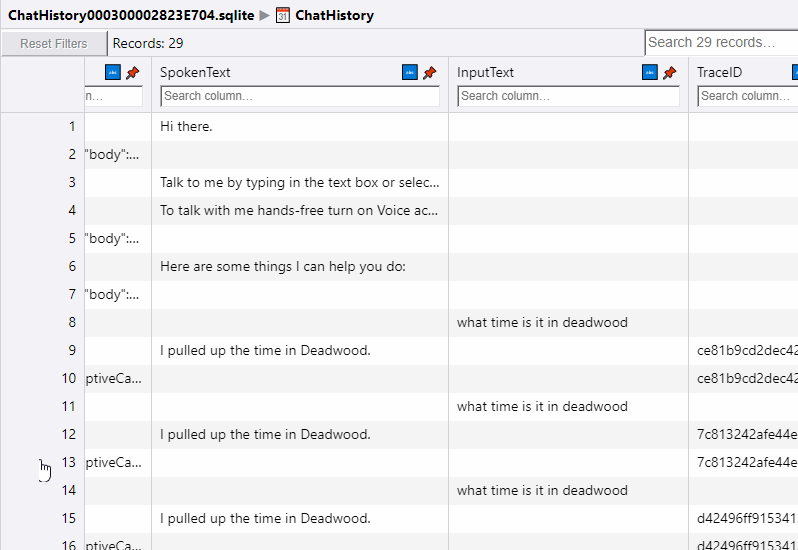
**Tanya Malik:** Edited two letters in the work log.

**Emily Nolan:** Tested Cortana's wake word response and tested false response with continuous conversation/ voices by playing audio for several hours to see if she would wake up and try to answer. She wasn't responding on the VM, but when I logged onto my desktop, she worked, so I tested it there. Also attempted to disassemble dll files.

**Lucas Scharf:**

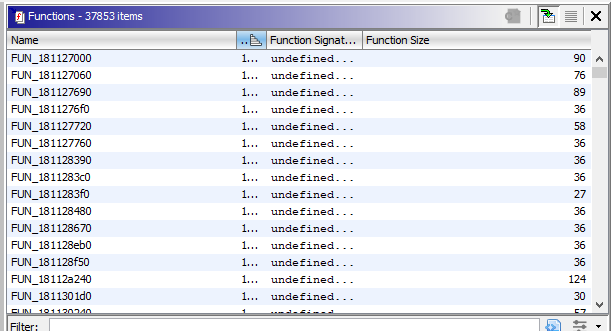
I worked on verifying last year's results listed below. Decrypting audio data is still an ongoing process.

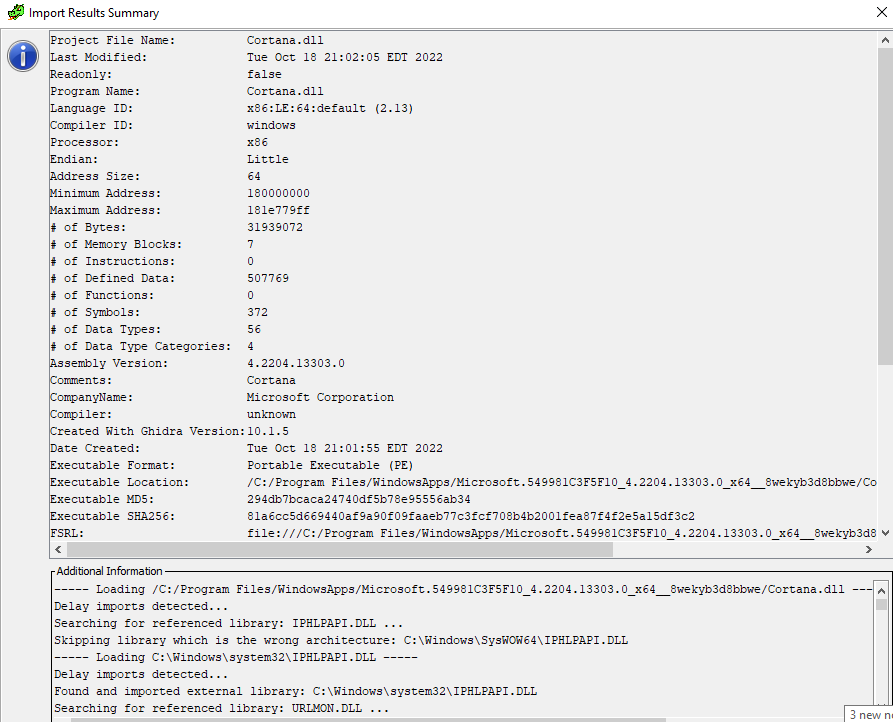
1. **File Structure:** 
   1. It was discovered that the primary directory of the Cortana program could be found in a subdirectory under Program Files, which contained the Cortana application, various dynamically-linked libraries (DLLs), and other files which are required for functionality. These are administrator locked.
      1. 
   2. A subdirectory found in a user’s AppData folder appeared to contain Cortana’s local data for an individual user.
      1. 
      2. This directory was largely unremarkable, aside from one ChatHistory file located in the LocalState directory, which contained a record of all Cortana exchanges stored as an SQLite database.
      3. It was able to be read with any simple program that supports SQLite files.



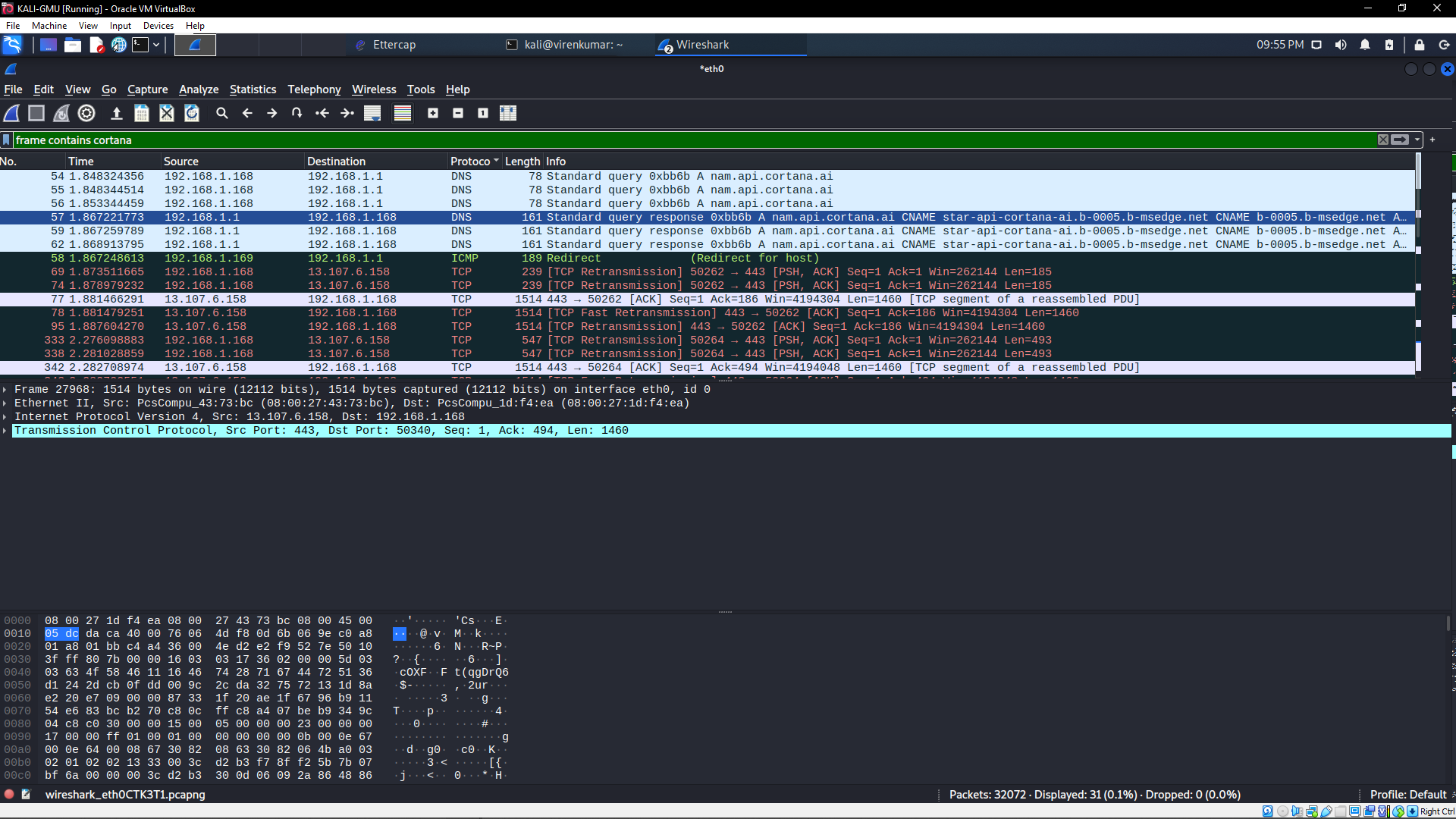
* + 1. The database was found to contain the following information for each request and response: message type (request or response); timestamp; globally unique identifier (GUID); JSON command data (for responses only); plain text of request or response; and additional identifier information (for responses only).

1. **Code Analysis**
   1. Last years group disassembling in Ghidra revealed that this file contained 31,322 functions, suggesting that this module was responsible for the majority of Cortana’s functionality. Now this dll contains 37,853 functions.





1. **Cortana Network Communications**
   1. Cortana was determined to communicate to a specific Microsoft domain, nam.api.cortana.ai, in nearly every instance other than for remote diagnostics; 



Viren and I found a few different domains that Cortana was reaching out to. This is ongoing with our plan to decrypt audio data. We have the CA certificate installed but we are unsure how it works. Still researching.