Artifact

Inquiry Lesson - The Mighty Notepad!
Created by Anthony Pieper on Oct 5, 2016 7:10 AM

According to the West Virginia Department of Education (n.d.), "[s]tudents actively participate in inquiry learning experiences by developing questions and investigating to find solutions" (para. 1), so relating this to computer science, the first question that I could see used to facilitate an inquiry-based lesson is "what files can you open in Notepad?"

For those of you who don't know, Notepad is the basic text editor that comes with every version of Windows (with a comparable application also loaded on Mac and Linux). Microsoft Word is the big brother of Notepad, and although MS Word can open up any document Notepad can, it doesn't work the other way around. What's nice about Notepad is that it doesn't do any formatting whatsoever, so it can be really good for looking at hidden things within certain types of files (like webpages). My vision for how this lesson would go is that I would show the students the same text passage in Notepad, MS Word, and Adobe Acrobat, and then ask them if they think it will look the same if they opened up all the files in Notepad. Once the lesson is going, I would also encourage the students to try opening different files on their computer to see the results.

Why this is important is that it introduces the concept of the two main file types, binary and text, which is an essential element of computer science. Notepad will open both, but it will only properly display text files. This can also lead into a discussion on encoding and compression, and why even though a plaintext file, a Word document, and a PDF file may all have the same content when viewed in their respective applications, when you view each in Notepad, you'll see dramatically different content. Lastly, this can be expanded into a broader discussion on encryption, which seems to continuously be appearing in news stories regarding hackers and breaches of large organizations. The biggest takeaway with this lesson is that if the sensitive information is stored incorrectly (i.e. in a plaintext file on the server), it's a relatively easy matter for the hacker to get the data (once he hacks the system).

- Tony

Reference:

West Virginia Department of Education. (n.d.). *Inquiry-based lesson plans.* Retrieved from https://wvde.state.wv.us/teach21/Inquiry-BasedLessonPlans.html