**Problem 1).**

**1.**The first issue I see is the location of the server room. Having it in the janitor’s closet is dangerous because normally janitor closets always have chemicals if one of these chemicals spill it could be a disaster for the system. In addition to this anyone can access the servers.

**1a**.The Control for this would be to make an actual server room where no chemicals or easy access can happen.

**2**. Three off these server’s work under one network if this were to shut down you would lose practically 50% of your servers. The other four are with the same network switch this in turn can create the same problem with having them under one network card.

**2a**.The Control for this would for each computer to have its own Network Interface Card and each server should have its own switch as well to prevent the likelihood of all servers failing under one switch.

**3**. Many research professors house their own servers in their offices. This is dangerous if the professors don’t know how to encrypt and save information properly because everything could be easily compromised. Easy for hackers to invade.

**3a**.A control for this would be to install a dedicated server with a secure shell protocol implemented.

**3b**.Another Control for this would Virtual machines so all the information that is worked on is instanced.

**4**.Destop Support Techs use the same admin password to access all workstations. The issue with this one is that everyone has the same level authority in the system. Someone that does the wrong thing with or without intent of the destroying the server can be an issue, everything can be potentially wiped out.

**4a.**A Control or remedy for this would be to simply give different authorization to different groups. Meaning an Admin should get its own User and Password and regular employees should get a different kind of username and password with different kind of access.

**Problem2)**

CVE-2022-20701- The current description of this is in Cisco Small Business RV160, 260,340, and RV345 Series Routers could allow an attacker to any of the following: Executing arbitrary code to Elevate privileges Execute arbitrary commands , Bypass authentication and authorization protections, Fetch and run unsigned software.

Its base score on NVD is a 7.8 and with Cisco Systems Inc. it is a 10.0 CRITICAL

Sources: <https://nvd.nist.gov/vuln/detail/CVE-2022-20701>

**Problem 3)**

Data Breach 1. Ubisoft Cybersecurity incident disrupts operations and forces company-wide password reset. Lapsus$ group believe to be responsible for the temporary disruption of some its games, systems, and services.

**Answer:** If the company had to do a company wide password reset due to this breach. Its sounds like Ubisoft had problems with authentication protocols they have installed with the servers or to get in. The Lapsus$ gang seems to target companies in the ransoming aspect. Lapsus$ has information the company finds very important, and the company is willing to pay the information or else it will get leaked. The process for Lapsus$ to get into Ubisoft’s servers was probably just skimming through passwords that the company was using and finally got access into the system after a certain amount of tries. Maybe the password wasn’t strong enough. Passwords should be changed regularly to avoid this.

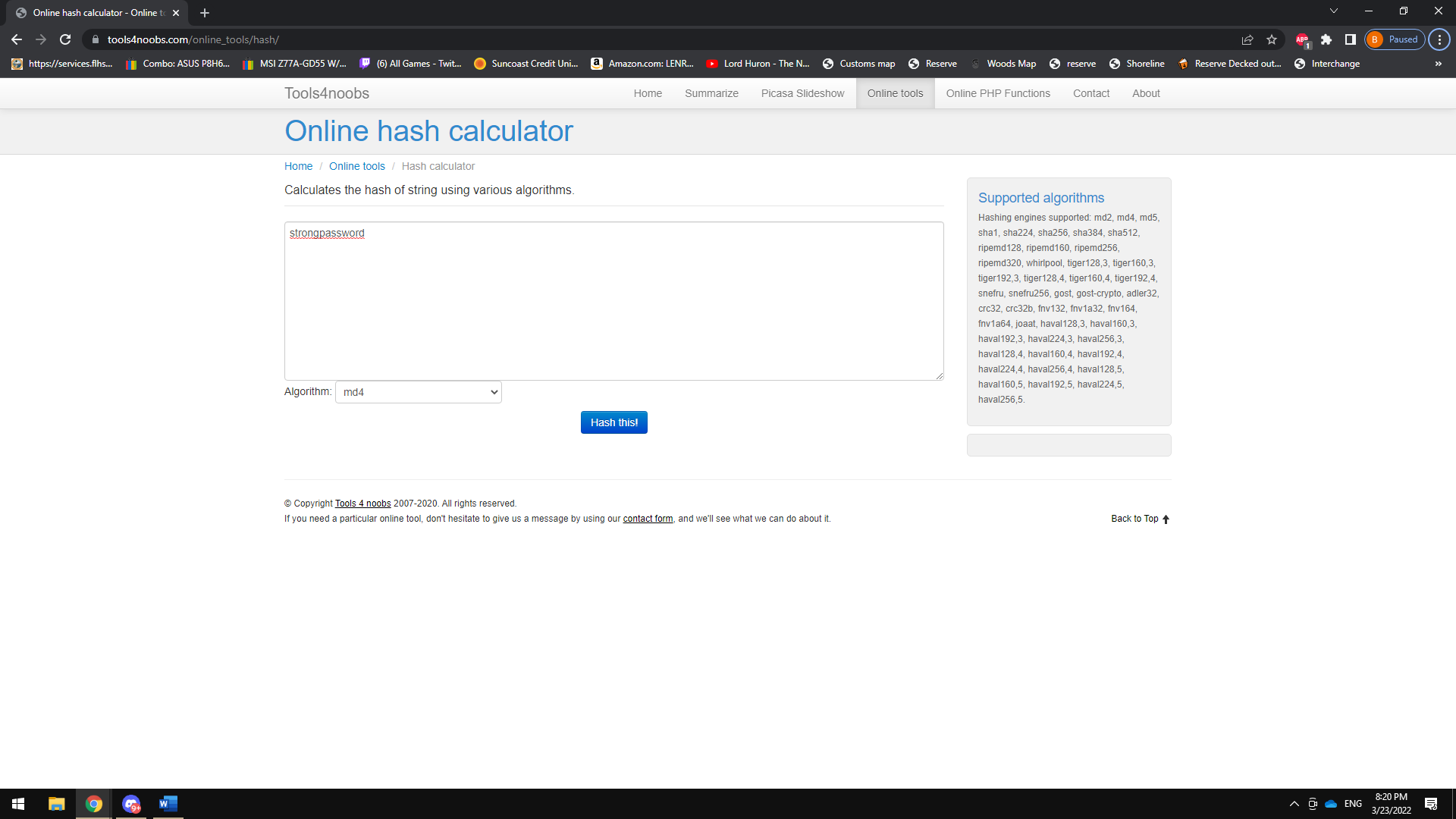
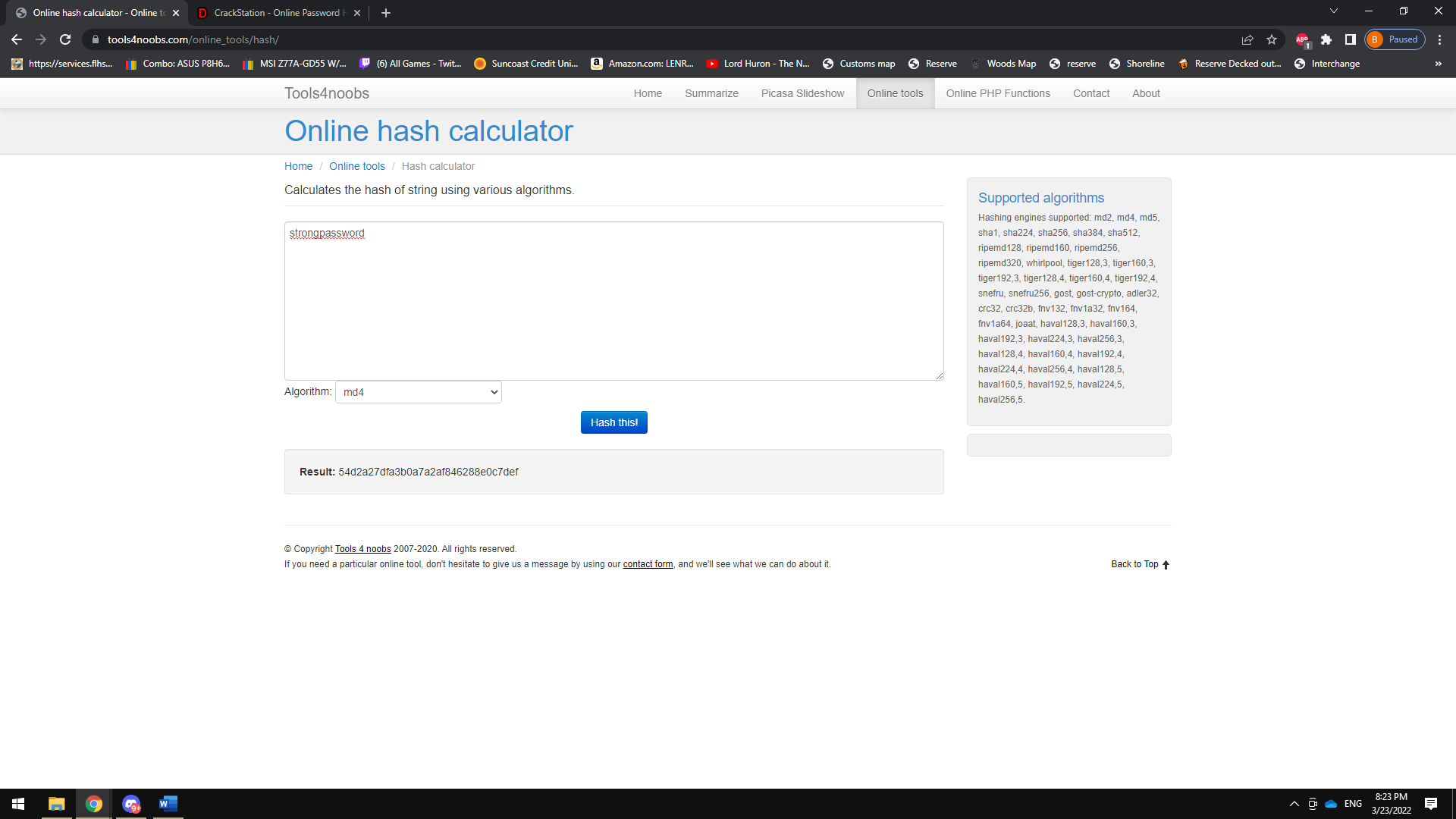
**Source**: <https://portswigger.net/daily-swig/cybersecurity-incident-at-ubisoft-disrupts-operations-forces-company-wide-password-reset>

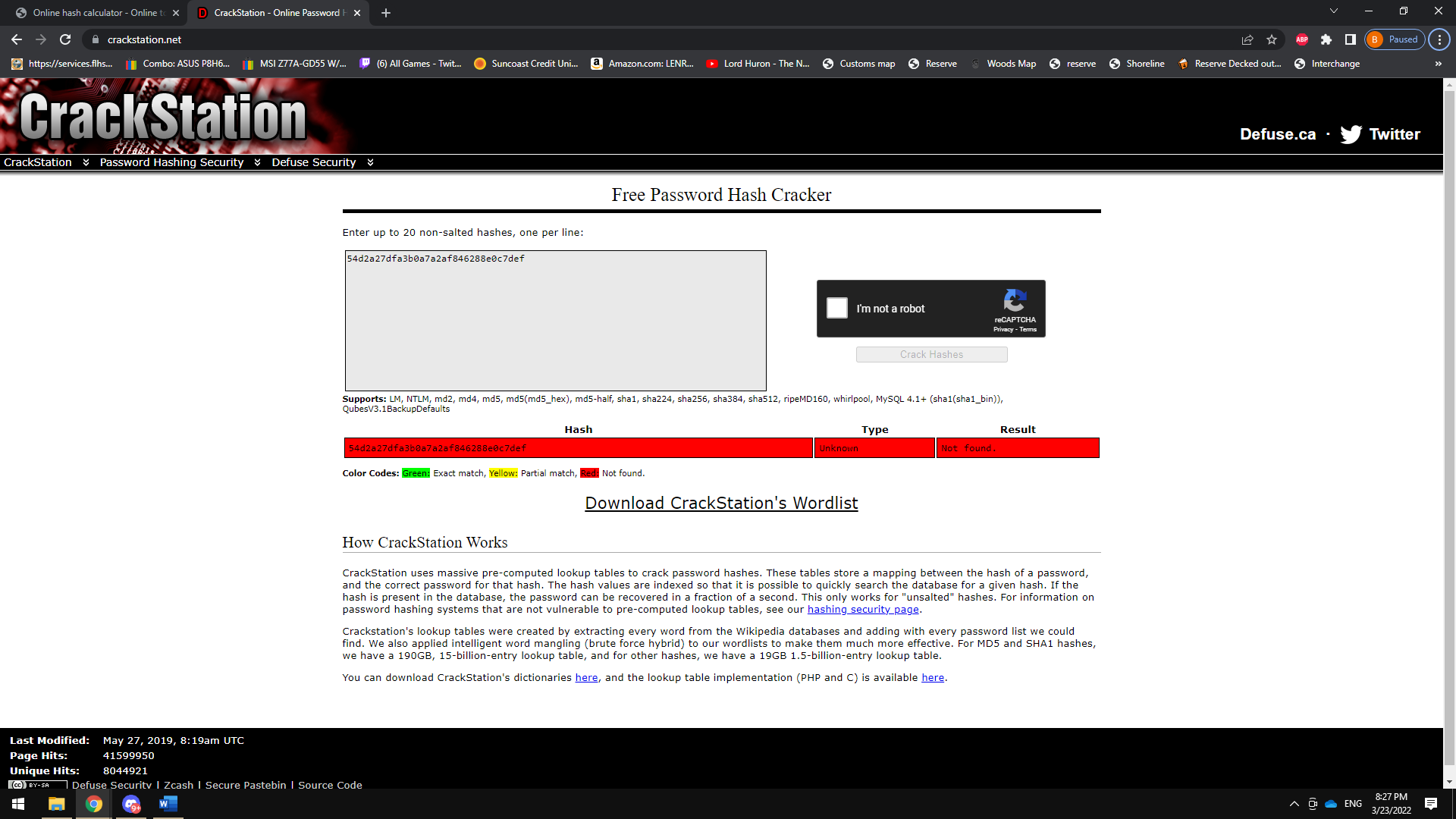
Data Breach 2. At US Heart disease treatment center impacts 287,000 individuals. A data breach at US Health Clinic South Denver Cardiology Associates (SDCA) . SDCA Admitted that an unnamed attacker broke into its systems and had access to confidential databases for three days between January 2, 2022, and January 5, 2022, before the breach was detected and thwarted.

**Answer:** The Daily swig had asked SDCA if it had identified the cause of the breach on its systems. No word back yet. I’d say the source of the breach would be authentication again or simply password changing. I feel as though most of the issues start here when it comes to data breaches. Companies prioritize on keeping information confidential but fail to authenticate a lot of times when it comes to these breaches.

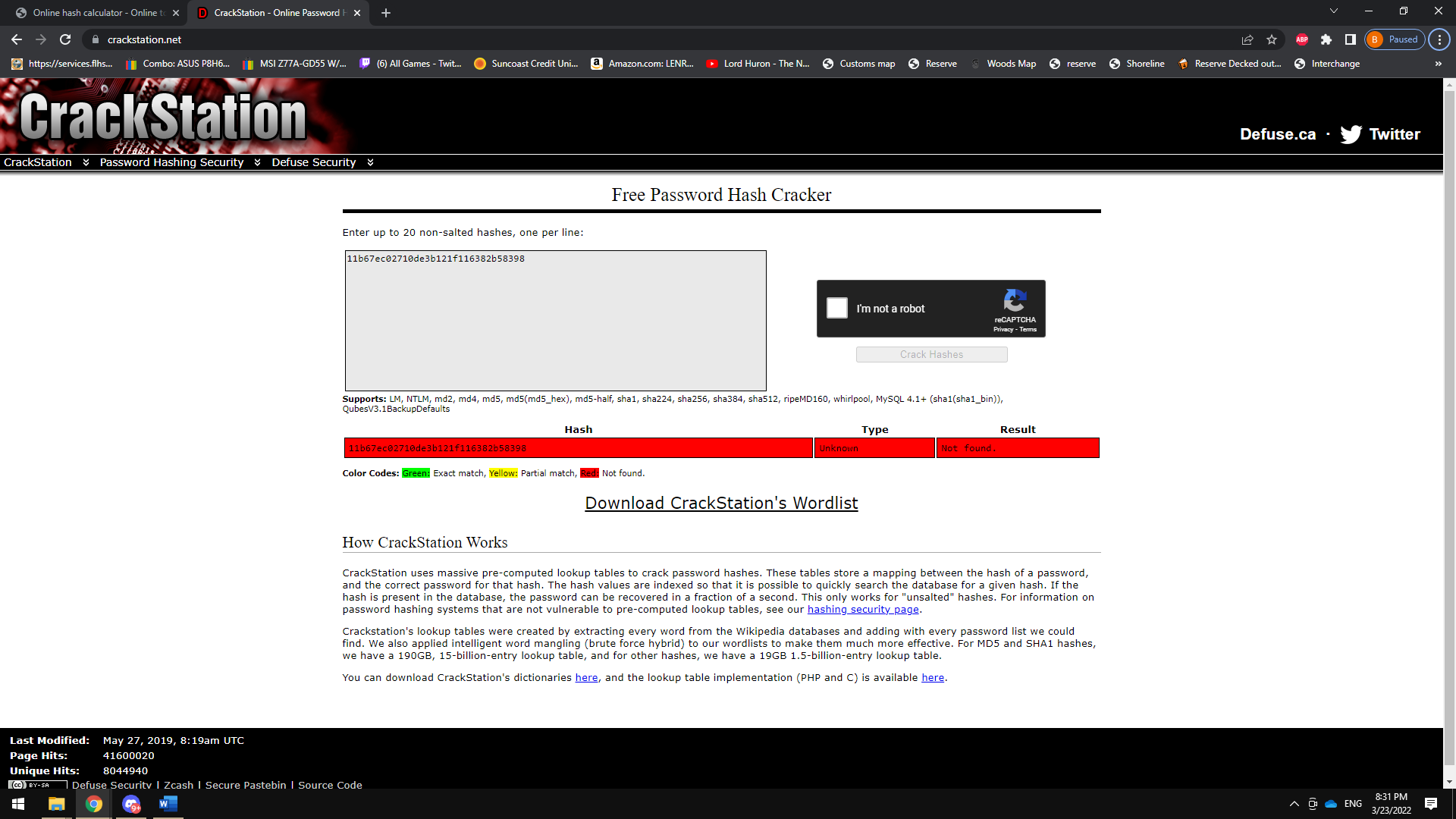
**Source**: <https://portswigger.net/daily-swig/data-breach-at-us-heart-disease-treatment-center-impacts-287-000-individuals>

**Problem 4)**

**A.B. AND C.**

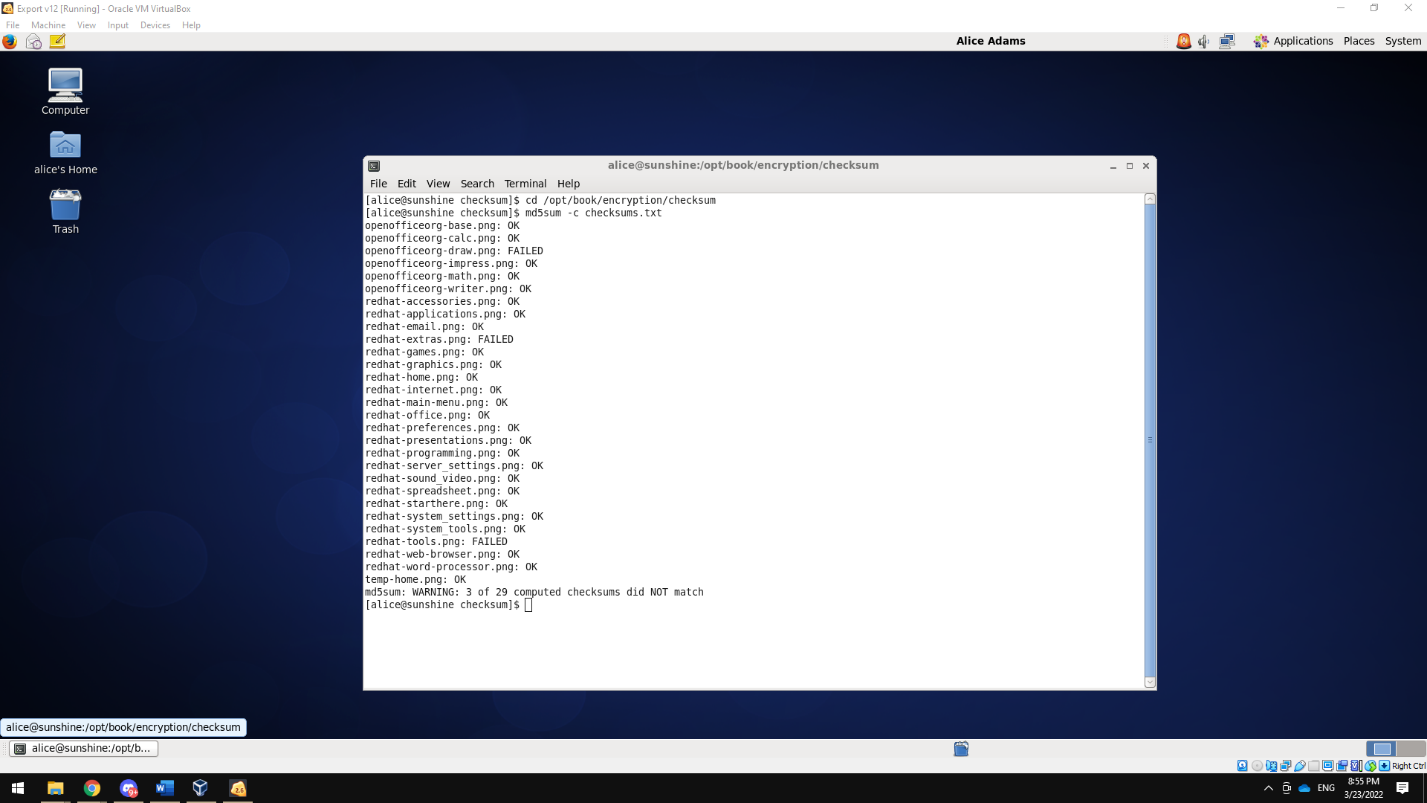
**D.**

**E.** The result came out to Type “ Unknown” and The Result was not found which is Highlighted in red from the Color Code it shows.

**F.**

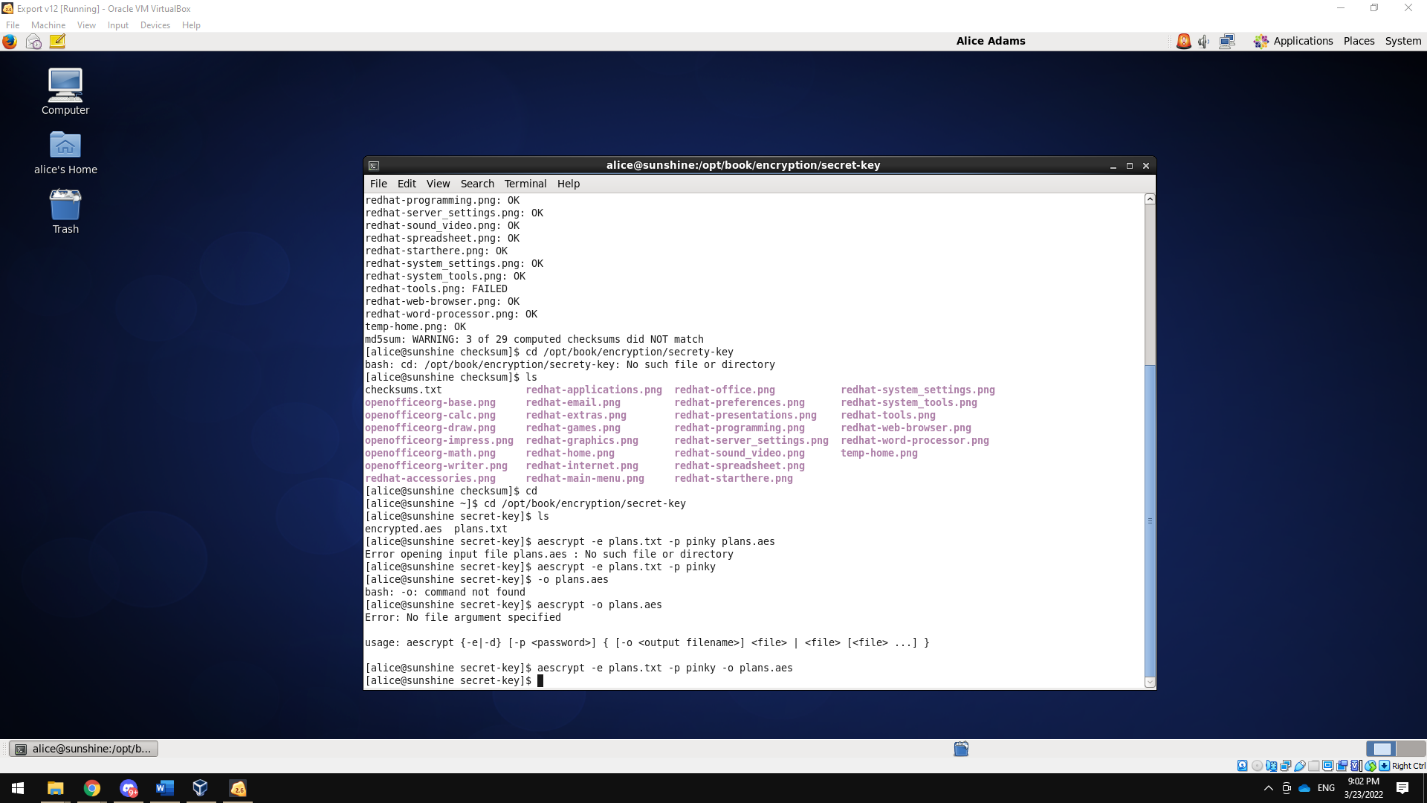
G. The same result was given as the previous password with the hash.

G1. I will say I tried the word “chicken” and the color code did come back green so that one was successful.

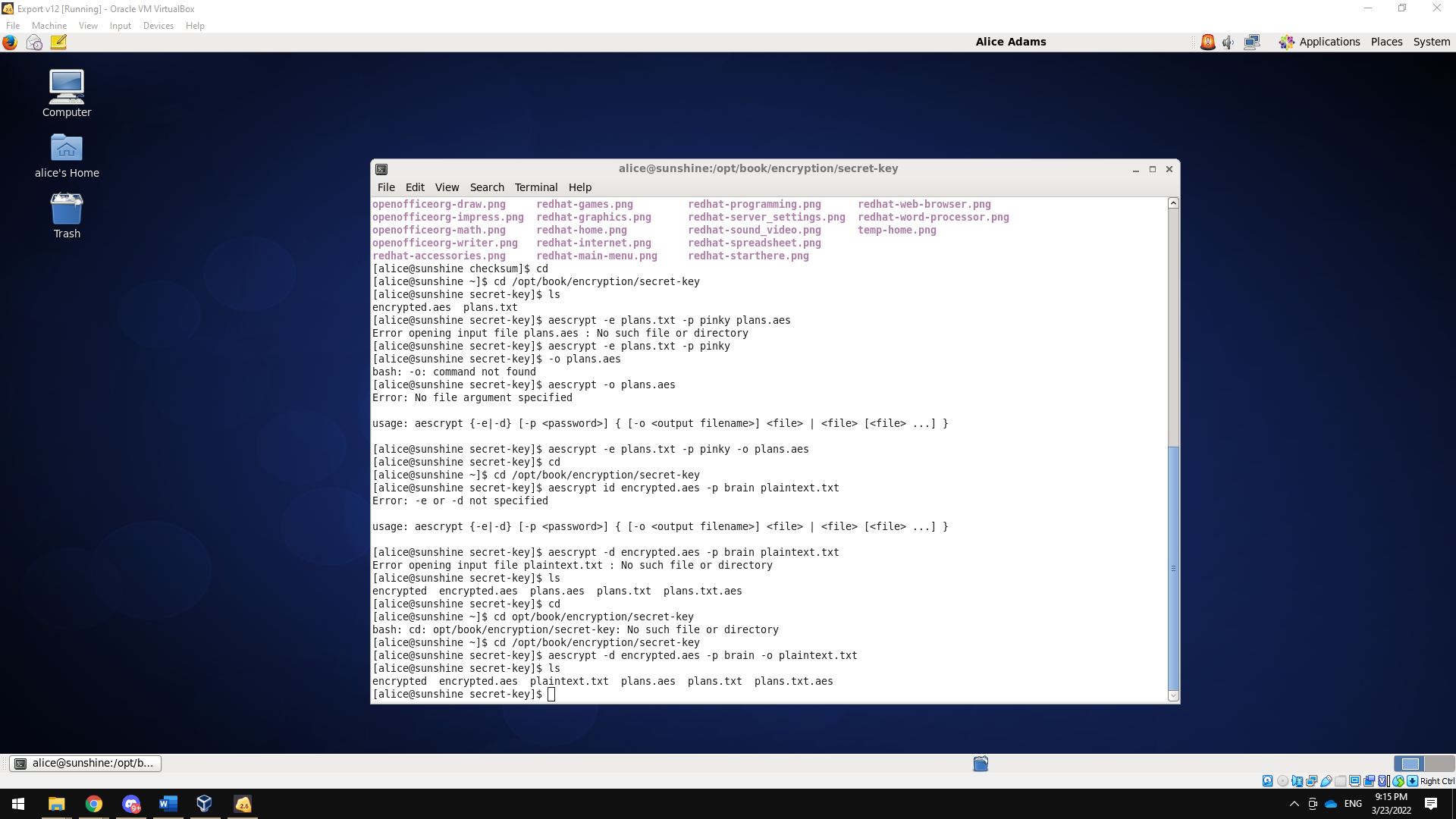
**Problem 5)**

“FAILED” could mean that the files didn’t go through properly meaning several things from a virus that could potentially be in the file to a simple size error and its not able to open due to the formatting of the png file.

**Problem 6)**

****

1. AES (Advanced Encryption Standard) Is a symmetric block cipher chosen by the U.S. for primarily protection of Classified information. AES feather is that you have the same key to Encrypt or Decrypt something versus RSA which is what’s mainly used for website logins is a Asymmetric Cipher meaning you have a public key and a Secret key.

**Problem 7) **