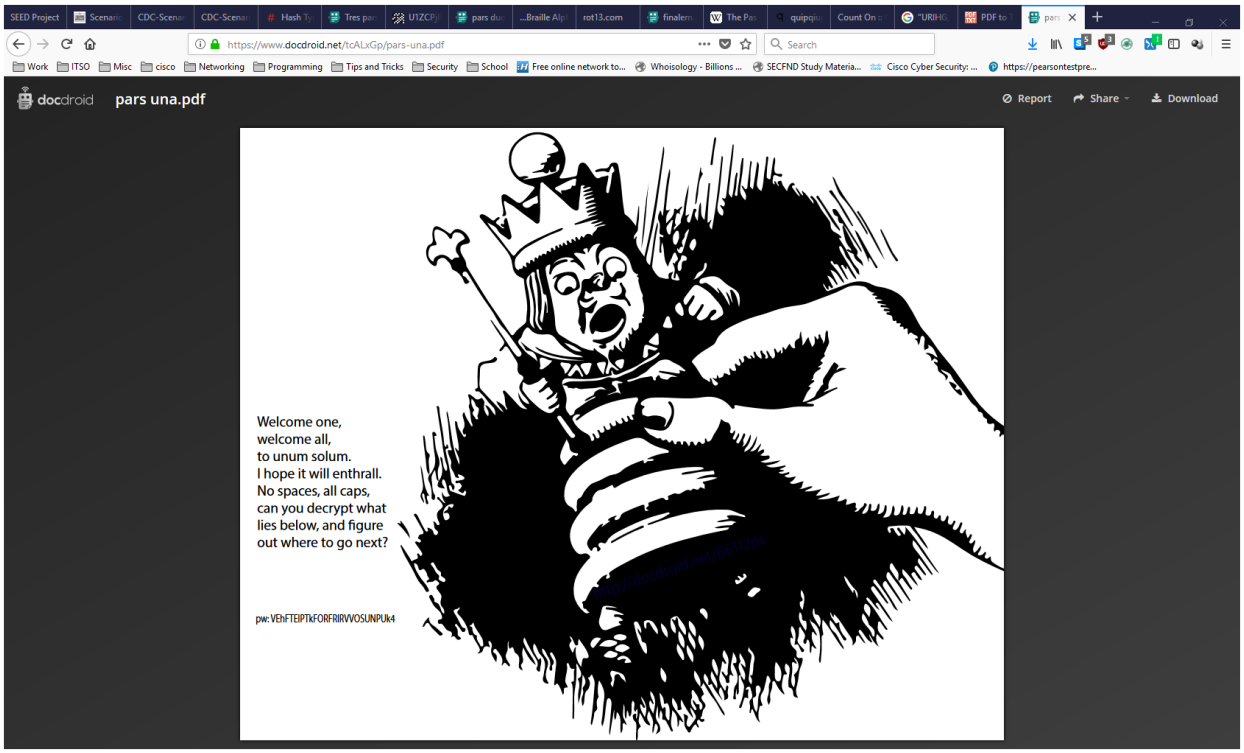
Given the scenario, http://blogs.anl.gov/cyberdefense/wp-content/uploads/sites/59/2016/02/CDC-Scenario_redacted_2018.pdf . I felt that the text was blacked out or obfuscated in some way and the original text was not redacted. Later I noticed in the lower left corner, there is a link, http://docdroid.net/tcALxGp. Its hard to see because the opacity is ~10%. Used a website, http://pdftotext.com/ to extract the text:

> *http://docdroid.net/tcALxGp*
>
> *Your team has just been hired as the network and security administrators of cyber systems that work in conjunction with the production and delivery of natural gas infrastructure for the Natural Gas Demand Corporation (NGDC). NGDC is the nation's only start-to-finish natural gas production, transmission, and distribution company. NGDC handles all aspects of this highly valued product from extracting the raw gas resources, processing, transportation, and distribution to residential, commercial, industrial, and electric power consumers. NGDC recently has been hit with multiple "minor" cyber attacks against their pipeline transmission infrastructure and have not successfully been able to review, update, or patch their systems with appropriate mitigation solutions without having to stop all operations. These attacks were assumed to be achieved by the hacker organization known as RedCrew. The motivation was a protest about the newly appointed distributer: GREENEnergy. NGDC has hired you and your team as subject matter experts help secure this network and has requested that you secure their user supply and marketing portal (distribution) network. These two networks require high availability and should not be taken offline for any reason unless dictated by the Chief Executive Officer – Ronald Variable. Unfortunately, there has not been a solid security team at NGDC in about three years and the network architecture drawings and operational technology (OT) topology are largely out of date. Additionally, NGDC is requesting that a new File-Sharing client and IT communications be set up to allow customers and NGDC to be able to interact without utilizing credentials. The current system is broken and has no authentication measures. There has been little or no funding provided for this task until you as a team can demonstrate your capabilities to resolve their issues. This means that you and your team must secure these complex IT and OT systems utilizing free or open-source materials and best practices while maintaining full functionality for the company operators and the end users.*

Followed the link to a pdf named pars una.pdf:

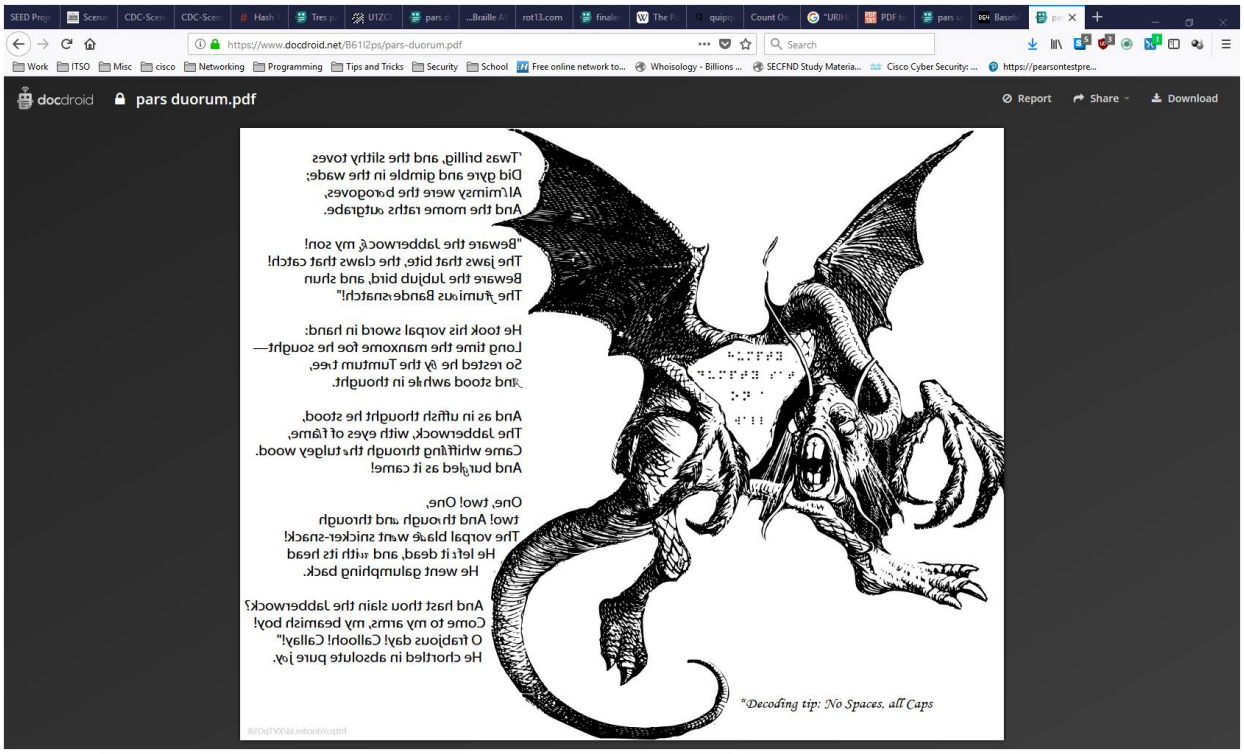


Extracted the PDF text again:

> *Welcome one, welcome all, to unum solum. I hope it will enthrall. No spaces, all caps, can you decrypt what lies below, and figure out where to go next?*
>
> *http://docdroid.net/B61l2ps*
> *pw: VEhFTElPTkFORFRIRVVOSUNPUk4*

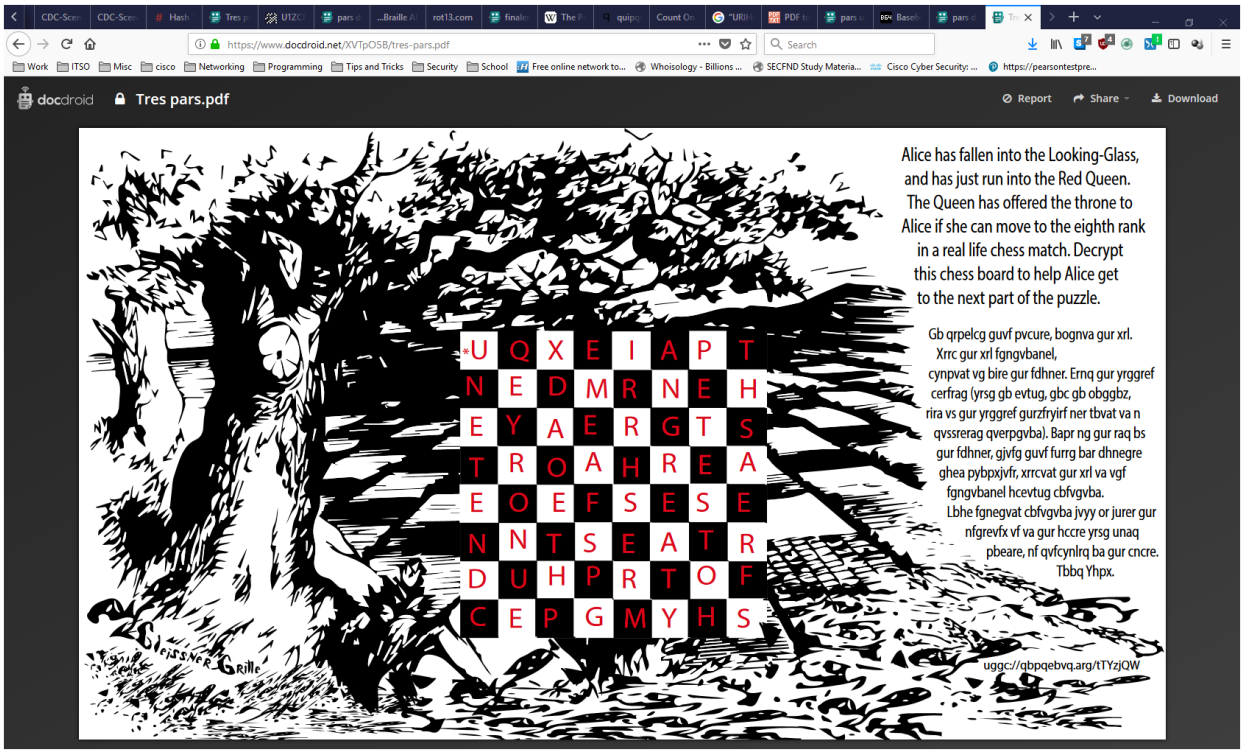
So from there I figured the text was encoded somehow. I used the website https://md5hashing.net/hash_type_checker to detect hashing. The result is Base64 and decoded it reveals the password, THELIONANDTHEUNICORN .

Using the link and password led me to this PDF:



The text is backwards and there is a link in the lower left corner, http://docdro.id/XVTpO5B imgur.com/U1ZCPjP . I also extracted the text again and got this link too, imgur.com/U1ZCPjP . More about this link later. I figured the characters inside the jabberwocky were Braille, which reveled HUMPTYDUMPTYSATONAWALL .

Following the link and password, led me to another pdf:

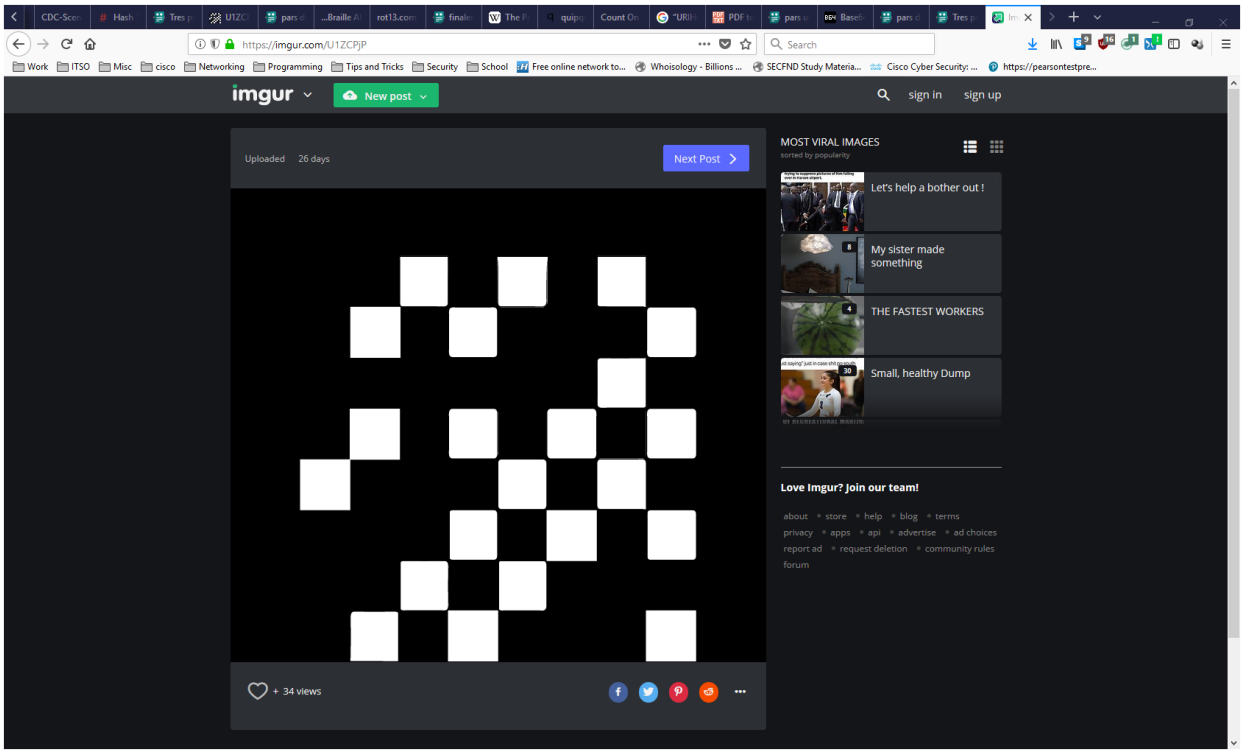


Looking to the right there is garbled text and a link to another website. Since the link is uggc://qbpqebvq.arg/tTYzjQW I assumed Caesar cipher, ROT-13, I decrypted the text to:

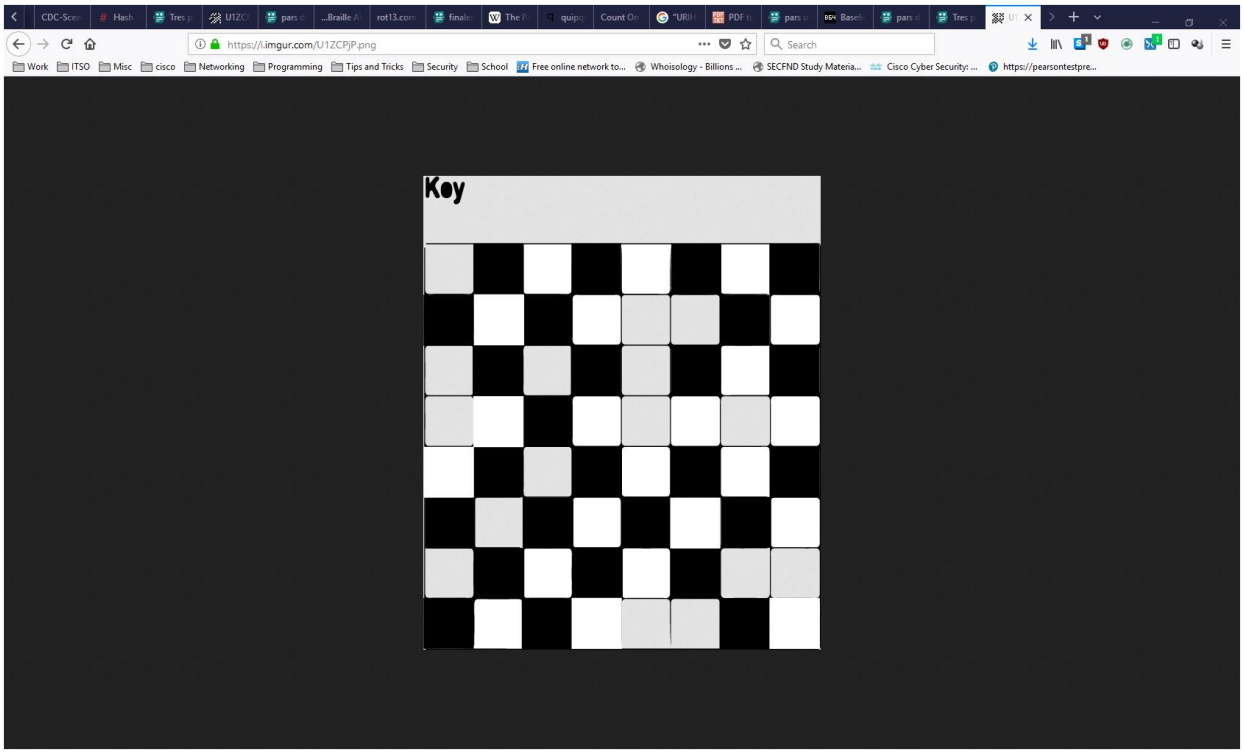
> *To decrypt this cipher, obtain the key. Keep the key stationary, placing it over the square. Read the letters present (left to right, top to bottom, even if the letters themselves are going in a different direction). Once at the end of the square, twist this sheet one quarter turn clockwise, keeping the key in its stationary upright position. Your starting position will be where the asterisk is in the upper left hand corner, as displayed on the paper. Good Luck.*

The link was also ROT-13, http://docdroid.net/gGLmwDJ .

Remember this link, imgur.com/U1ZCPjP ?



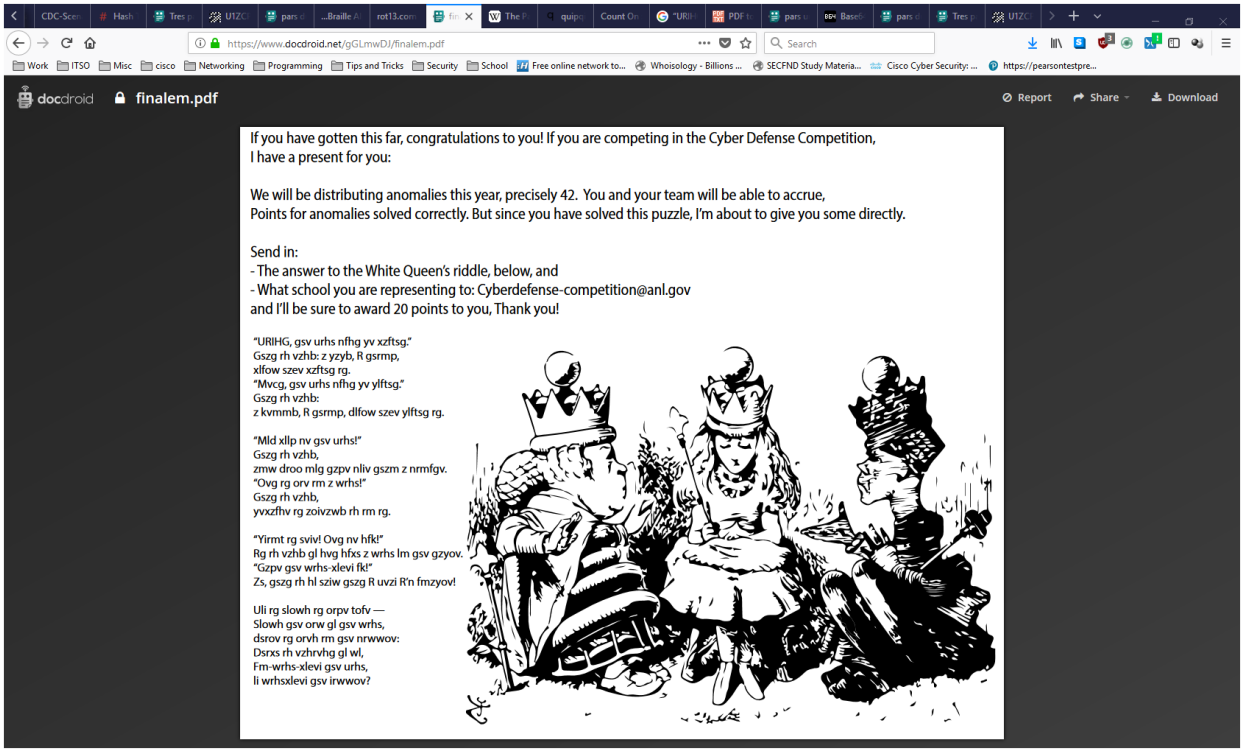
I right clicked on the image to “View Image”



It might be are to see some squares are grey and I figured they were the squares that would should the underlying characters for the previous PDF. I followed the instructions given and turned 4 times to get

the phrase, “U R NEAR THE END OF MY CRYPTOGAME. THE PASSPHRASE FOR THE NEXT STAGE IS REDQUEEN.”

The link and password let to the final PDF:



I just googled “White Queens riddle” since the theme of the PDF’s are quotes from Alice in Wonderland. I was able to find the quote. Using a known-plaintext attack since I had the plaintext and ciphertext, it was just a simple substitution cipher URIHG=FIRST . This website helped, https://quipqiup.com/ .Not needed but for my own gins and giggles. The answer is oysters.

FIRST, the fish must be caught.”
That is easy: a baby, I think, could have caught it.
“Next, the fish must be bought.”
That is easy: a penny, I think, would have bought it.

“Now cook me the fish!”
That is easy, and will not take more than a minute.
“Let it lie in a dish!”
That is easy, because it already is in it.

“Bring it here! Let me sup!”
It is easy to set such a dish on the table.
“Take the dish-cover up!”
Ah, that is so hard that I fear I’m unable!

For it holds it like glue —
Holds the lid to the dish, while it lies in the middle:
Which is easiest to do,
Un-dish-cover the fish, or dishcover the riddle?