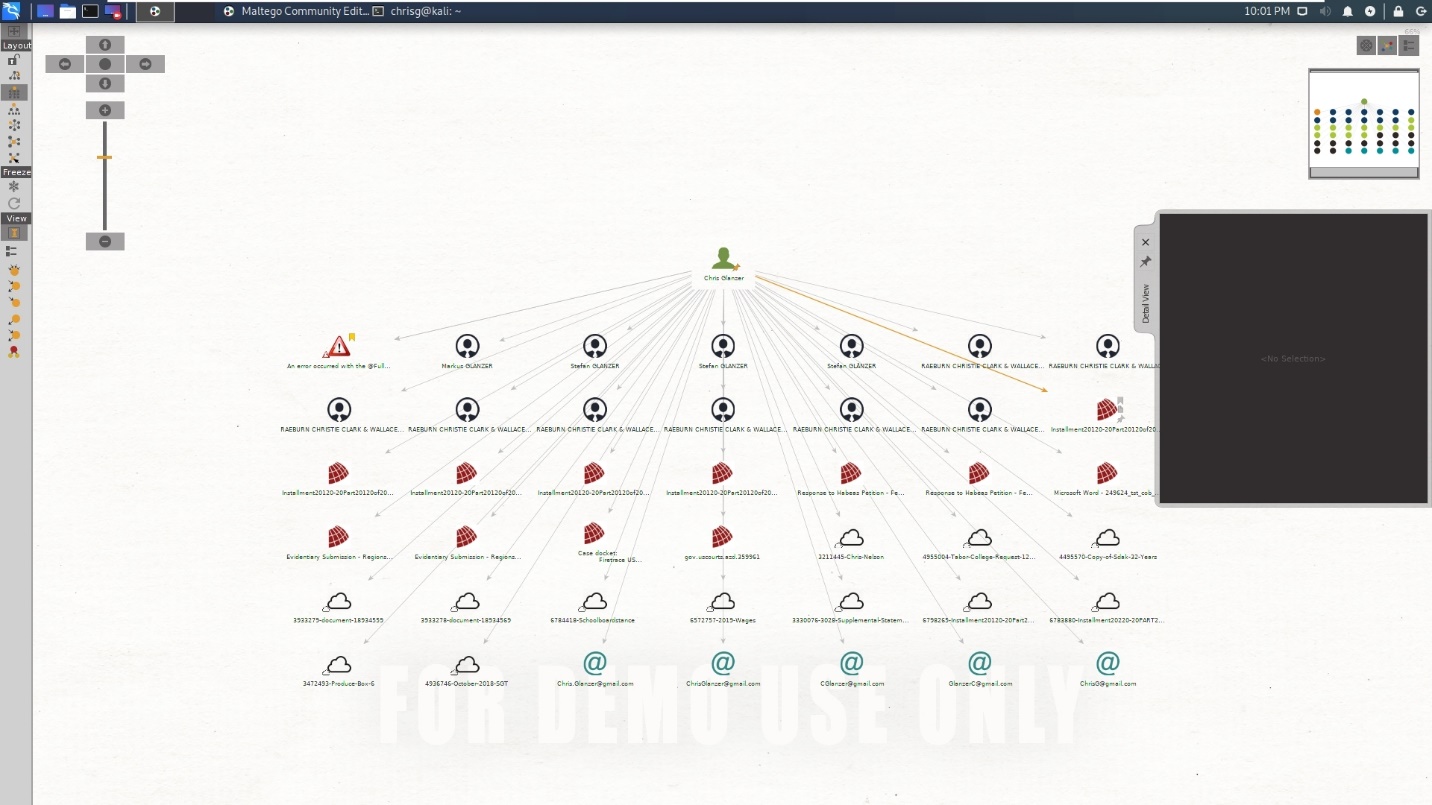
Assignment 2

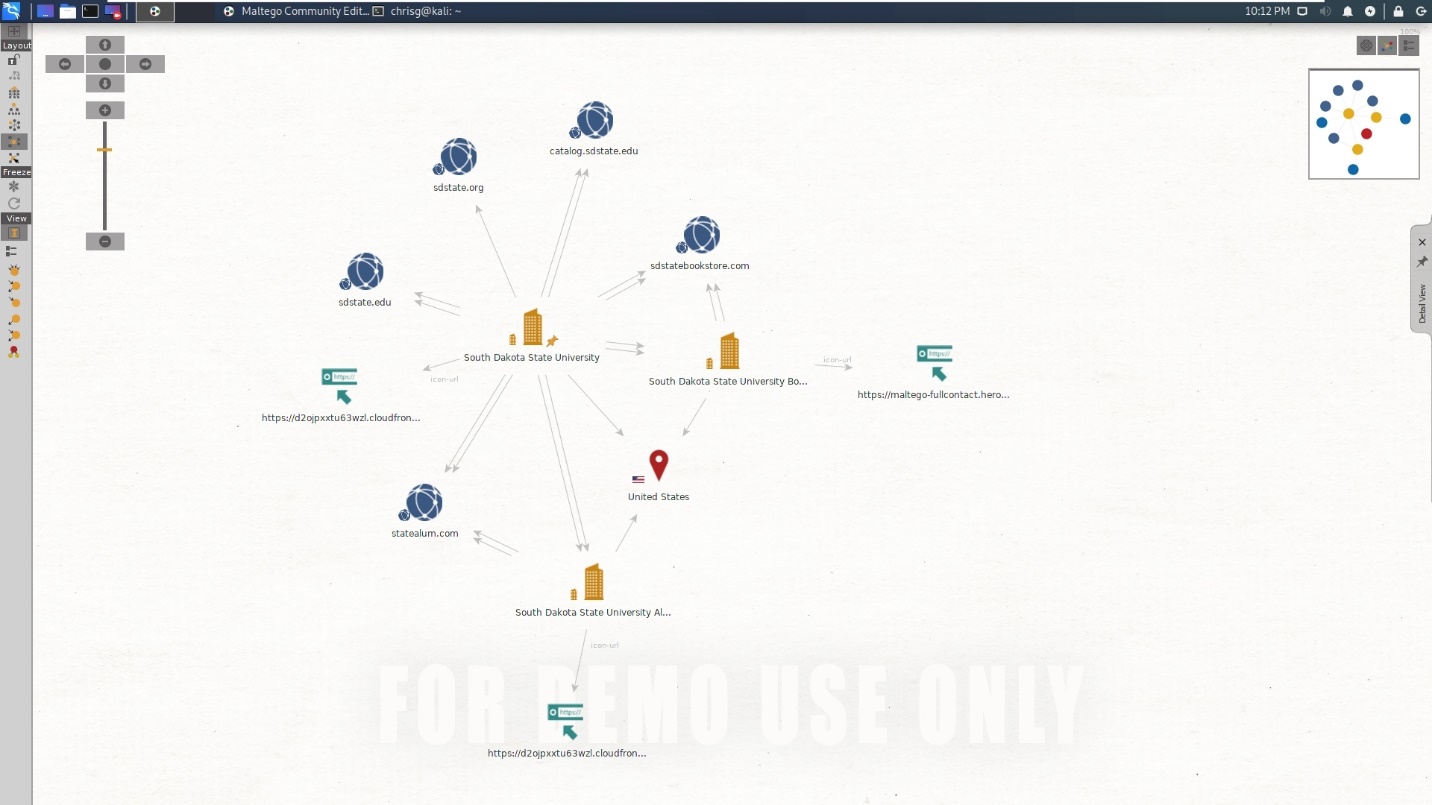
1. Investigate and read up on a tool called Maltego. Use whatever resources you see fit. Maltego is included in Kali Linux. Make use of this tool to search for 1. yourself and 2. a favorite actor or sports figure. Provide a screenshot.

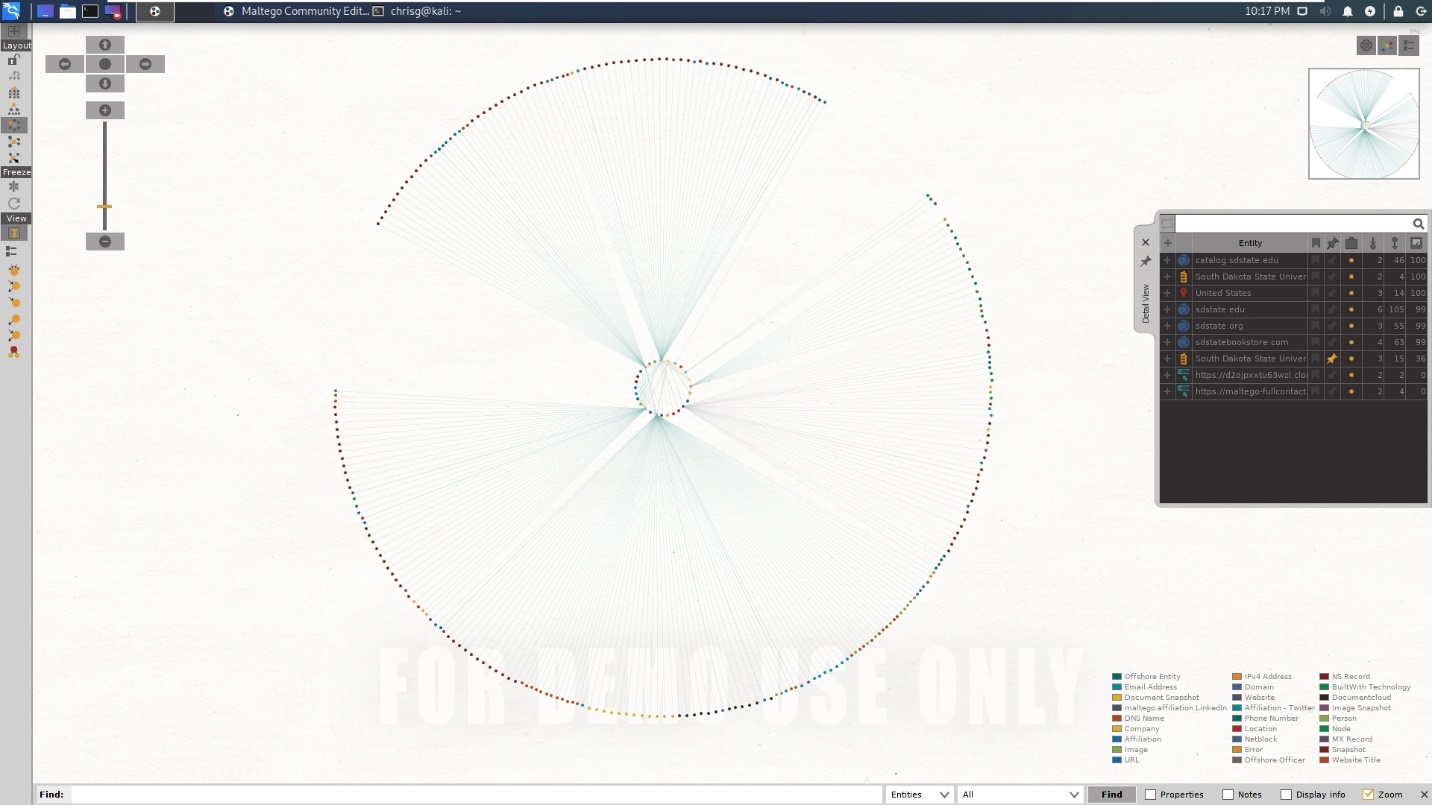
Keanu Reeves:  
  
Myself:

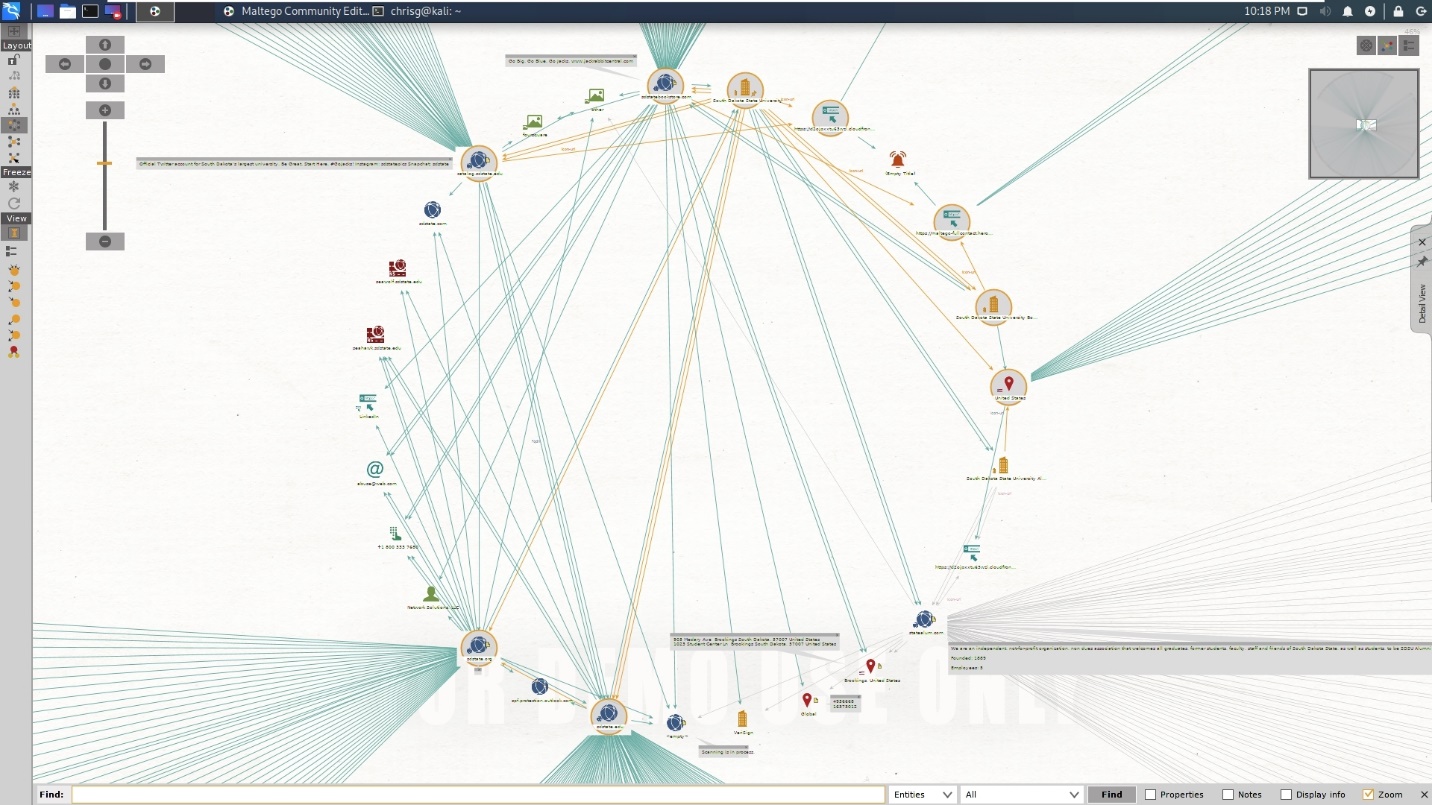


I’m not really living under a rock or anything, so the fact that none of the emails are mine, none of the people identified are known to me, and none of the documents have any relevance to me… maybe I need to fiddle with the plugins more.

2. Use Maltego to search for information about South Dakota University (SDSU). Note: This is not DSU. You were explicitly instructed to use only this tool to discover information about the target, so do not use any other tools. Do not use any active scanning against the target—no port scanning or exploitation. This is just information gathering. Show a few screenshots showing your results.

  
after performing the same transofrmations on just a couple of the domains, we have a huge number resources, some of which are beginning to tie together.





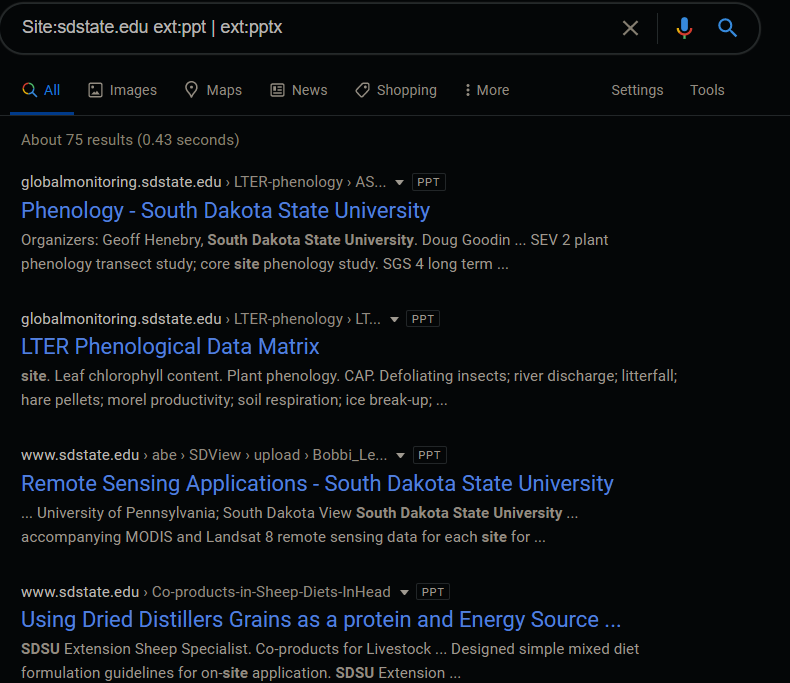
**Google Dorks**

*Note: Do not “try your best” or guess. Use the correct Google directives.*

3. Using Google, how do you find PowerPoint files that are on SDSU? Provide search term and

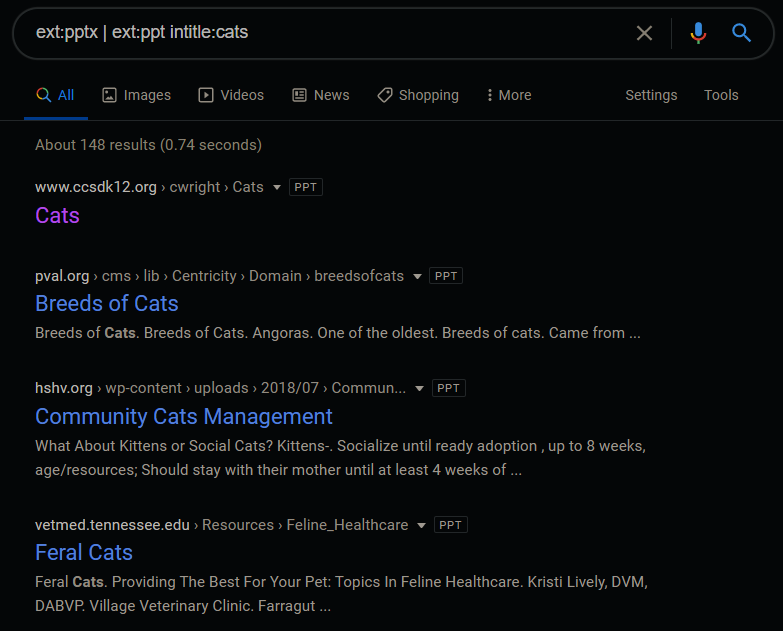
screenshot of results.

Site:sdstate.edu ext:ppt | ext:pptx



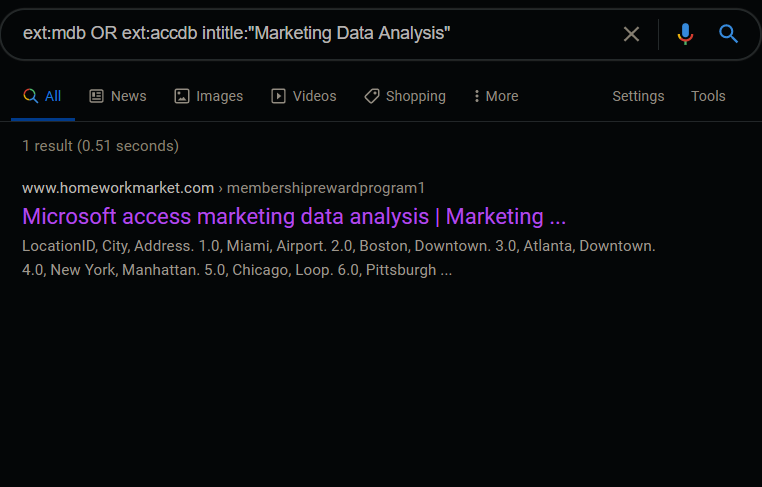
4. Using Google, how do you find PowerPoint files with the word cats in the title? Provide search term and screenshot of results.

ext:pptx | ext:ppt intitle:cats

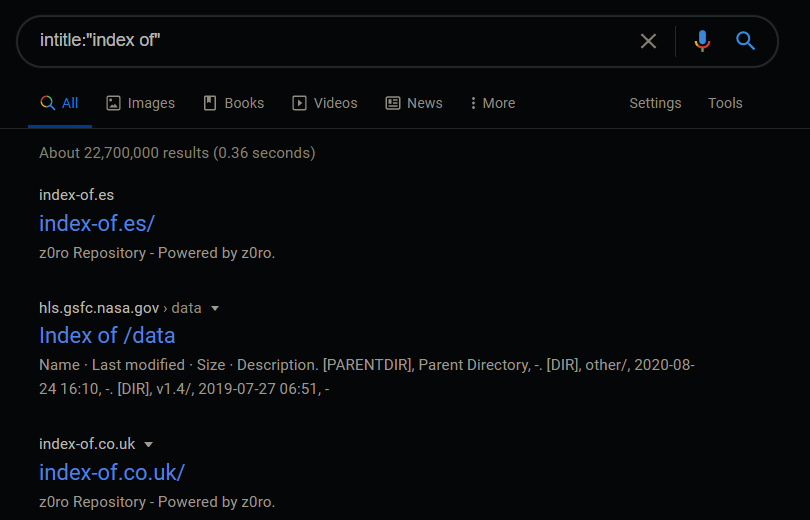


5. Using Google, how do find Microsoft Access files about marking (marketing?) data analysis? Provide search term and screenshot of results.

*Note: I know access has a bunch of alternative file extensions, but when I string them together usint the |/OR operator it returns no matches, which is confusing me. Is there a limit to the number of ‘arguments’ in a google query? or is something causing it to filter the results?*ext:mdb OR ext:accdb intitle:"Marketing Data Analysis"



6. Using Google, use in title directive to find sites that have "index of" in the title.

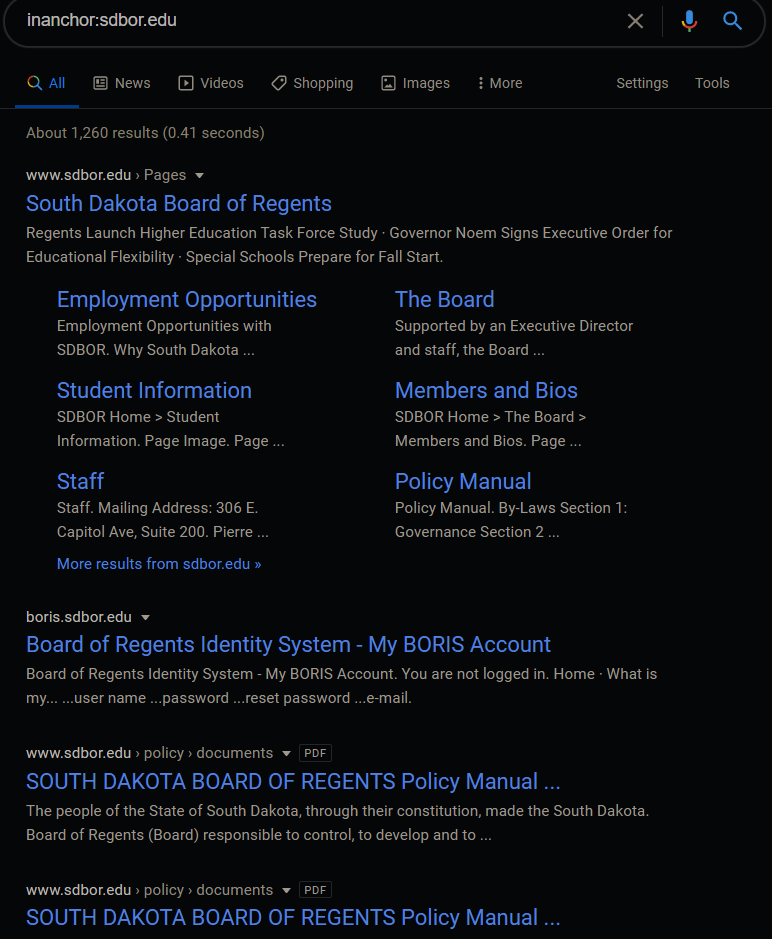
intitle:"index of" 

7. What benefit does “index of” have for us as penetration testers?

An index implies the presence of an enumerable structure – which means there’s other stuff to find following the same url scheme.

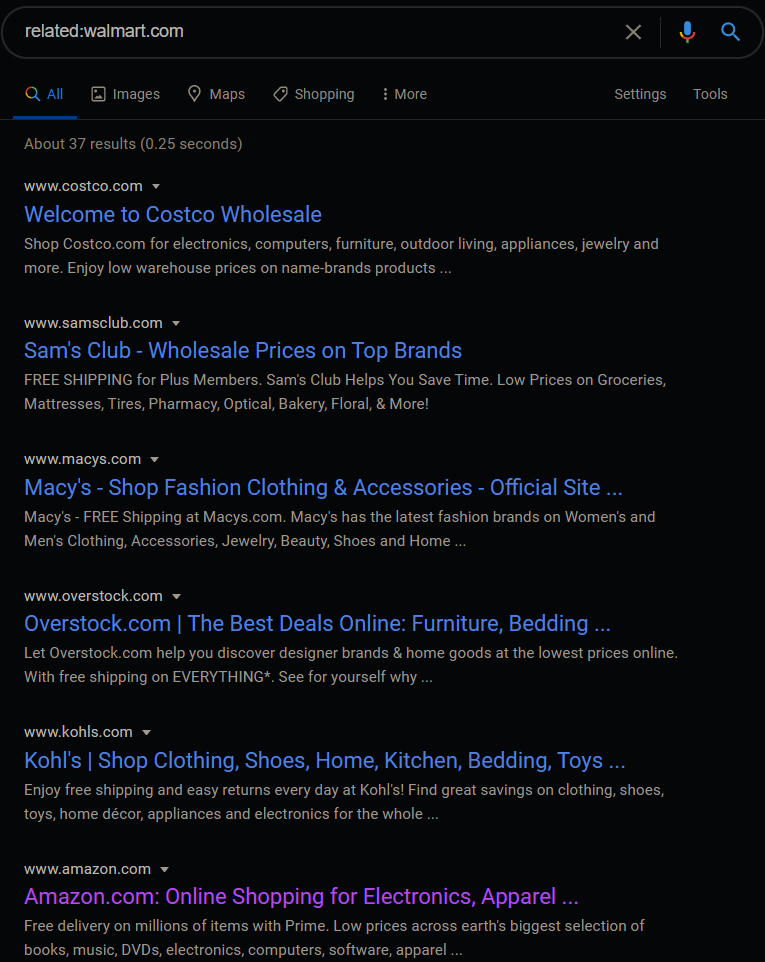
8. Using Google, make use of a directive to show all sites that linked to sdbor.edu.

inanchor:sdbor.edu

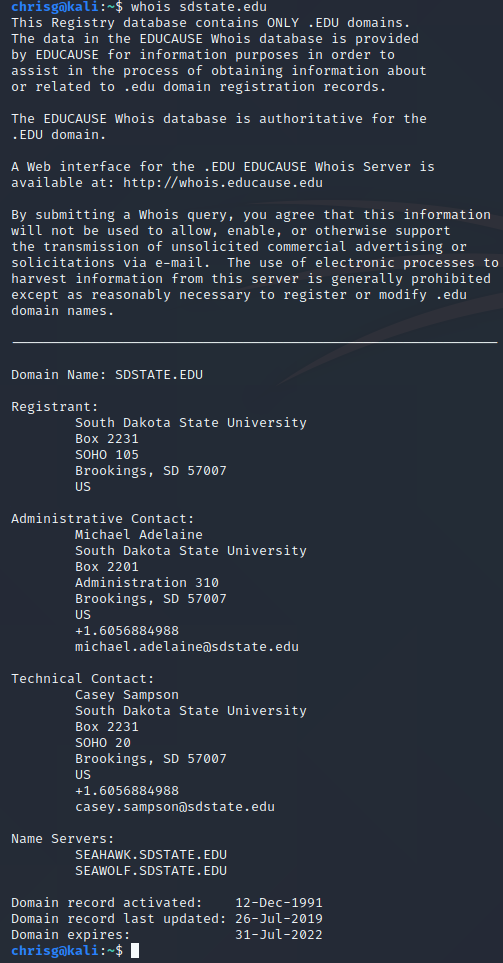


9. Using Google, make use of a directive to show all sites that are similar to Walmart.

related:Walmart.com



10. Use Kali Linux to do a whois on SDSU. Provide a screenshot and include it in the same Word/PDF.



11. Run Netcraft on SDSU and show a couple screenshots of your results. Anything stand out to you as interesting?

12. How can you defend against whois being misused against your organization?

13. What is the difference between these Google directives: allintext:[term] and intext:[term]. Explain and give an example with screenshots.

Note: Maltego is available in Kali under Information Gathering.

