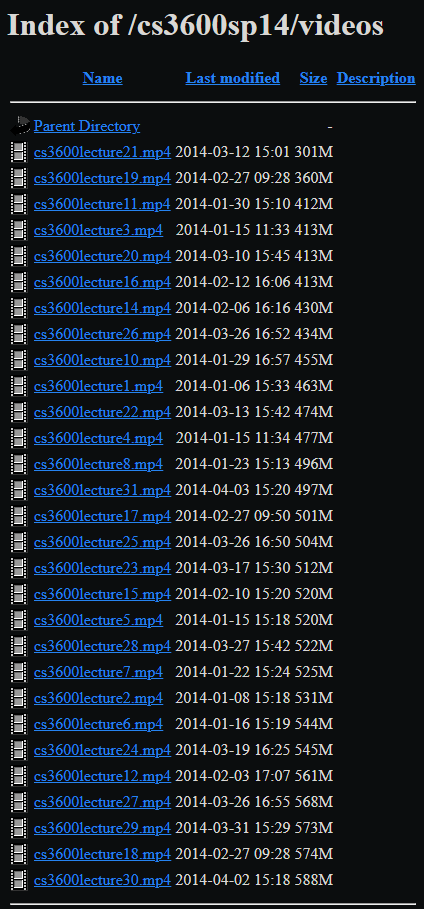
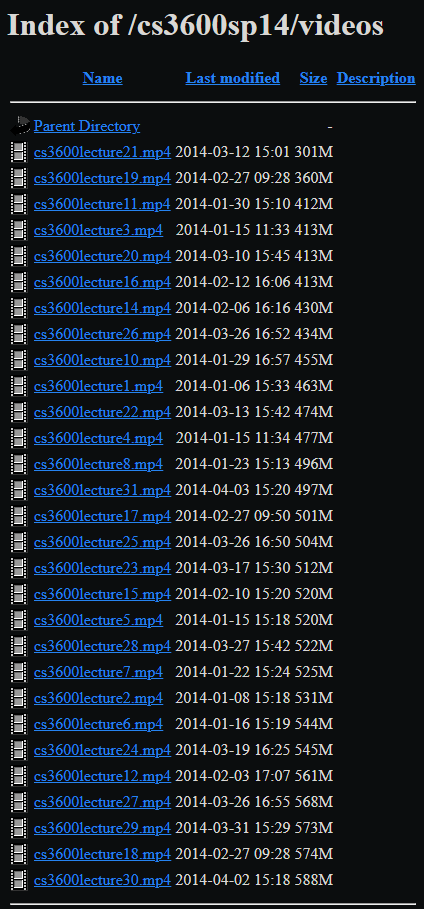
Google Hacking

Ryan Scott

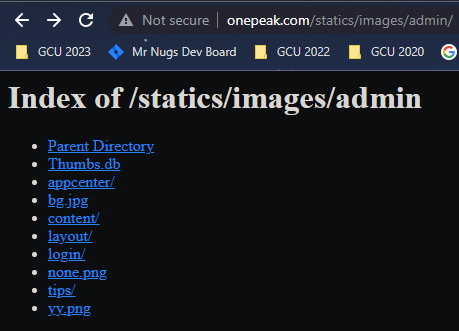
Grand Canyon University  
Information Security II

Prof. Christine Bakke

**Screenshot of MP4 Access:**

As a result of my Google Dorking, I gained free access to computer science lectures at some random college called “Northeastern University”!

**Screenshot of Database Access:**



A file called Thumbs.db contains data about posts, who posted them, and how many likes they have received on some random Chinese social media. I was definitely not supposed to have access to this!

**How To Remove Pages from Google Search Results**

1. First, the user must visit the Google Remove outdated content page.
2. Next, the user must enter the URL of the page they want to remove from search results.
3. The user must then select a reason for the removal request from a list of options provided.
4. Finally, the user must submit the removal request to Google.

(Removals and SafeSearch Reports Tool - Google, n.d.).

**Google’s Advice for Permanent Removal**

1. Getting rid of the content starts with removing it from the web. Google will eventually remove the content from search results if it can no longer be found online.
2. Next, you need to request that Google's cache be cleared of your requested content. You can do this by using Google's removal request tool.
3. If the content still appears in search results after following the above steps, the user can file a legal takedown request to have it removed.

(Removals and SafeSearch Reports Tool - Google, n.d.).

**Google Hacking vs CFAA**

In Google hacking, vulnerable web servers and websites are found by using Google's search features, (Sluiter, 2020). On the other hand, the Computer Fraud and Abuse Act (CFAA) is a federal law in the United States that prohibits unauthorized access to computers and computer networks, (Computer Fraud and Abuse Act Reform, n.d.).

There have been several legal cases where individuals have been charged under the CFAA for using Google hacking to gain unauthorized access to computers and networks. For example, in the case of United States v. Morris, a student at Cornell University used a program to exploit vulnerabilities in computer systems, including using Google to search for vulnerable computers. The student was the first to be charged under the CFAA for his actions, (LexisNexis, n.d.).

Therefore, it can be argued that information obtained by a Google Dork search could potentially be subject to the CFAA if the search is used to gain unauthorized access to computer systems and networks. However, it ultimately depends on the specific circumstances of each case and whether or not the use of Google hacking constituted unauthorized access under the CFAA, (Computer Fraud and Abuse Act Reform, n.d.).

# References

Computer Fraud And Abuse Act Reform. (n.d.). Electronic Frontier Foundation. <https://www.eff.org/issues/cfaa> (Computer Fraud and Abuse Act Reform, n.d.)

Offensive Security’s Exploit Database Archive. (n.d.). <https://www.exploit-db.com/google-hacking-database> (Offensive Security’s Exploit Database Archive, n.d.)

Removals and SafeSearch reports Tool - Search Console Help. (n.d.). <https://support.google.com/webmasters/answer/9689846?hl=en> (Removals and SafeSearch Reports Tool - Search Console Help, n.d.)

Sluiter, P. W. P. (2020, May 29). Google Dorking or Hacking Credit Cards SSN and Passwords with Google. YouTube. <https://youtu.be/nDpy0eg2xK8> (Sluiter, 2020)

Sluiter, S. (2021). GitHub - shadsluiter/GoogleHacking: Related to Google Hacking aka Dorking. GitHub. <https://github.com/shadsluiter/GoogleHacking> (Sluiter, 2021)

United States v. Morris | Case Brief for Law School | LexisNexis. (n.d.). Community. <https://www.lexisnexis.com/community/casebrief/p/casebrief-united-states-v-morris>