Lab 5 – Google Hack

Seneca | SCHOOL OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

NAME – Student ID	COURSE CODE	WEIGHT
Ishan Aakash Patel - 146151238	CYT130	5%

Homework Objectives

Upon completion of this lab, you will be able to perform the following:

- Use Google search engine to collect OSINT information;

Lab Materials

- Web browser (any kind);

Lab Instructions

- Open your web browser;
- Follow the lab's step-by-step instruction and complete all exercises;
- Enter your name and student ID above (Example: Boris Loza - bloza);
- Answer questions and add screenshots into the corresponding textboxes;
- Save the file on your computer for future reference;
- Save the file again as a "`.pdf`" file;
- Submit the PDF file for grading.

Working with Live Cameras in Google Search

The following Google hacking techniques can help attackers fetch live camera web pages that are not restricted by IP.

To fetch various IP based cameras:

inurl:top.htm inurl:currenttime

To find WebcamXP-based transmissions:

intitle:"webcamXP 5"

For general live cameras:

inurl:"lvappl.htm"

Google Dorks for Live IP cameras

1) allintitle: “Network Camera NetworkCamera”

2) intitle:”EvoCam” inurl:”webcam.html”

3) intitle:”Live View / – AXIS”

4) intitle:”LiveView / – AXIS” | inurl:view/view.shtml

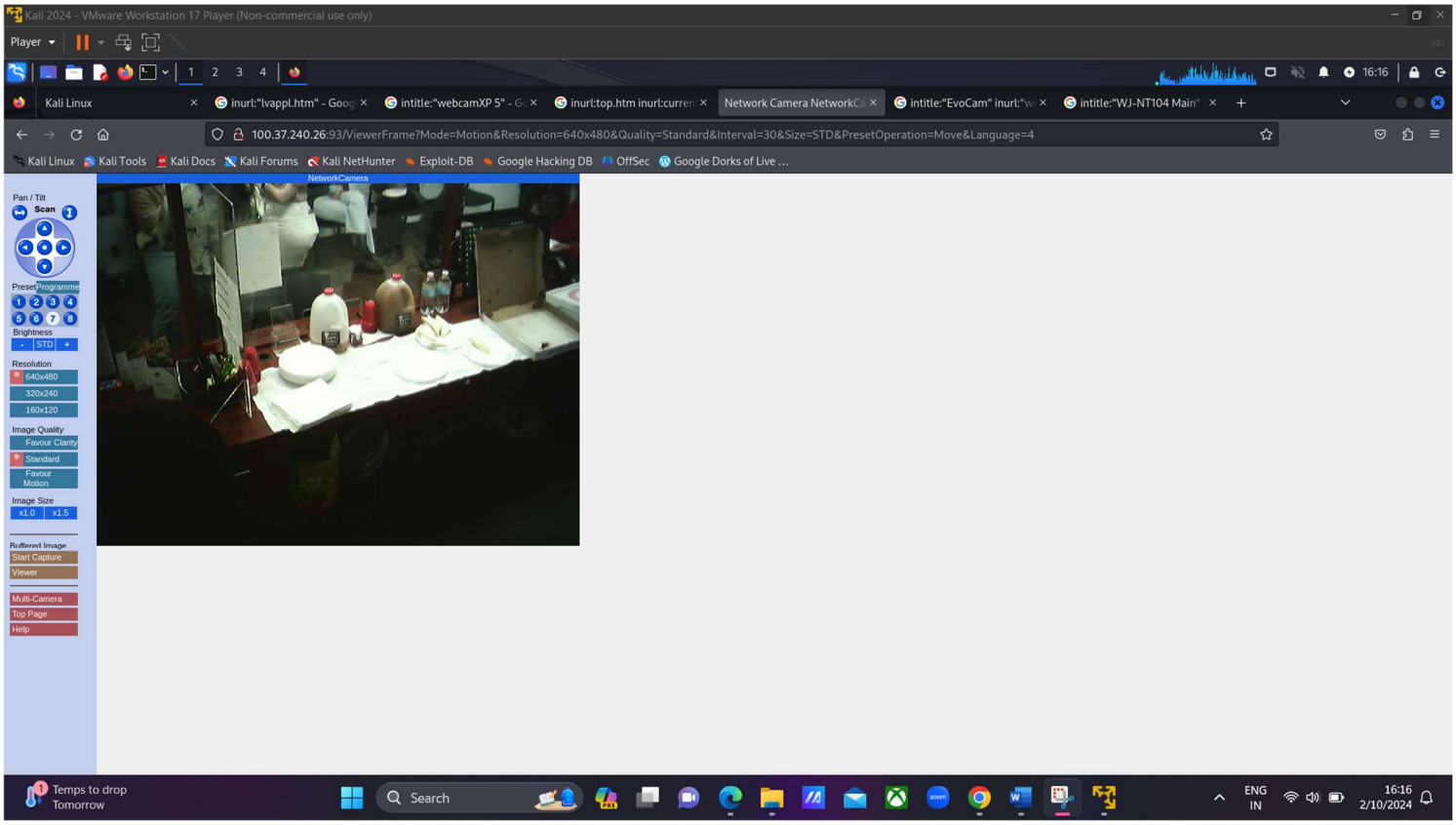
5) intitle:”WJ-NT104 Main”

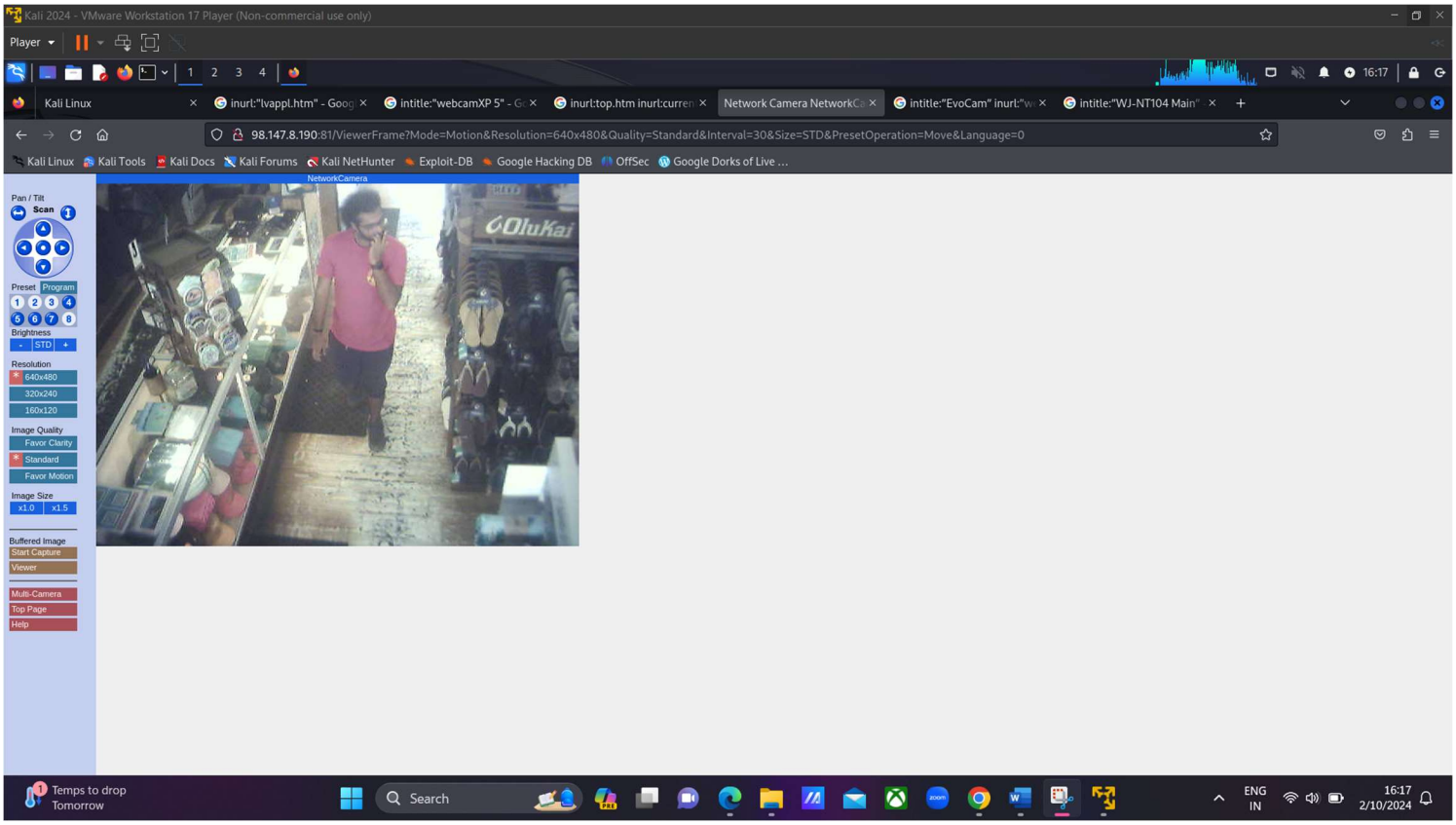
6) inurl:"lvappl.htm"

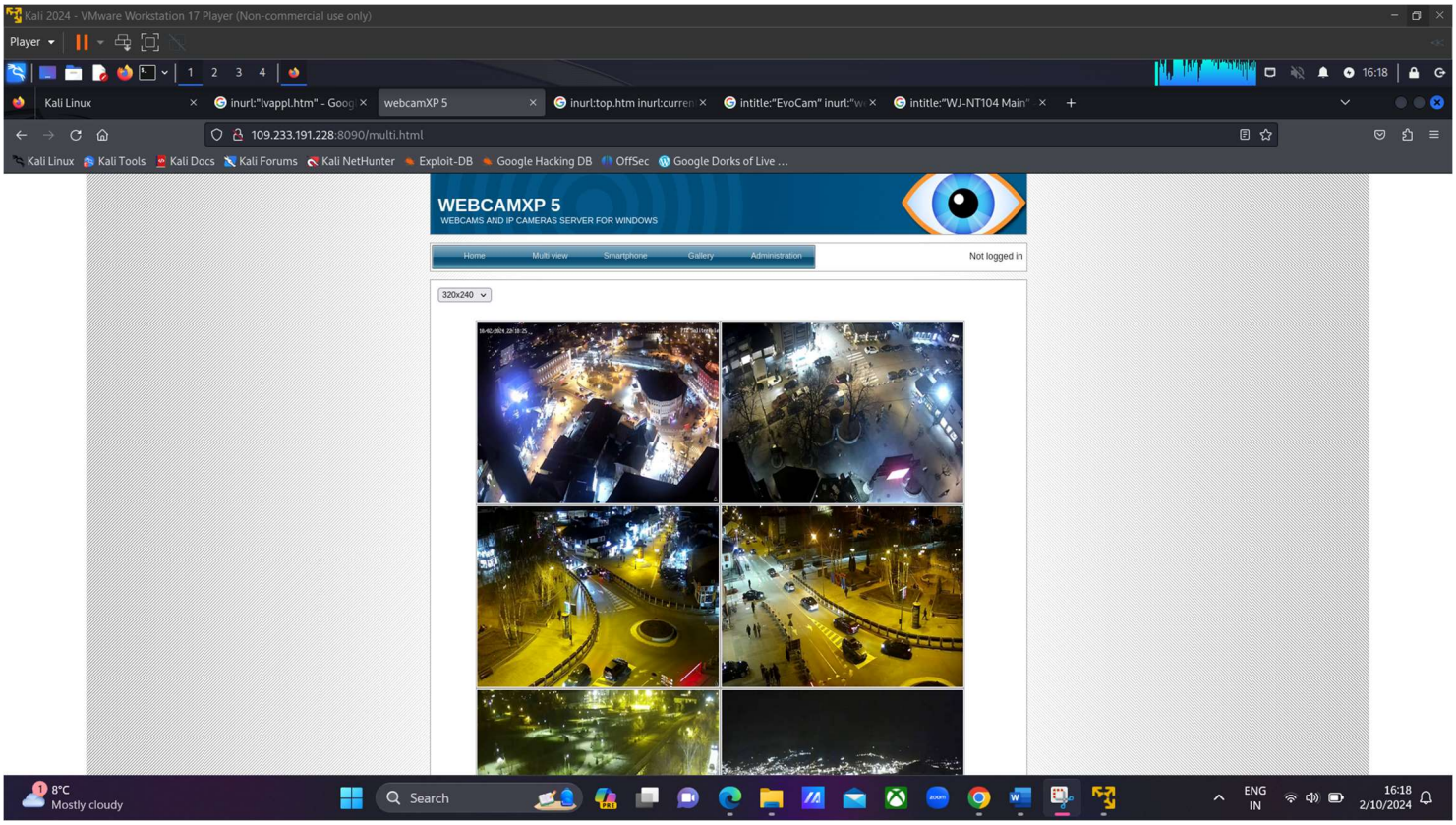
7) intitle:"webcamXP 5"

8) inurl:top.htm inurl:currenttime

Below are some of them which I found out:




Kali 2024 - VMware Workstation 17 Player (Non-commercial use only)
Player
Kali Linux
98.147.8.190:81/ViewerFrame?Mode=Motion&Resolution=640x480&Quality=Standard&Interval=30&Size=STD&PresetOperation=Move&Language=0
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Google Dorks of Live ...
NetworkCamera
Pan / Tilt
Scan
Preset
Program
Brightness
Resolution
640x480
320x240
160x120
Image Quality
Favor Clarity
Standard
Favor Motion
Image Size
x1.0
x1.5
Buffered Image
Start Capture
Viewer
Multi-Camera
Top Page
Help
Temps to drop
Tomorrow
Search
ENG
IN
16:17
2/10/2024

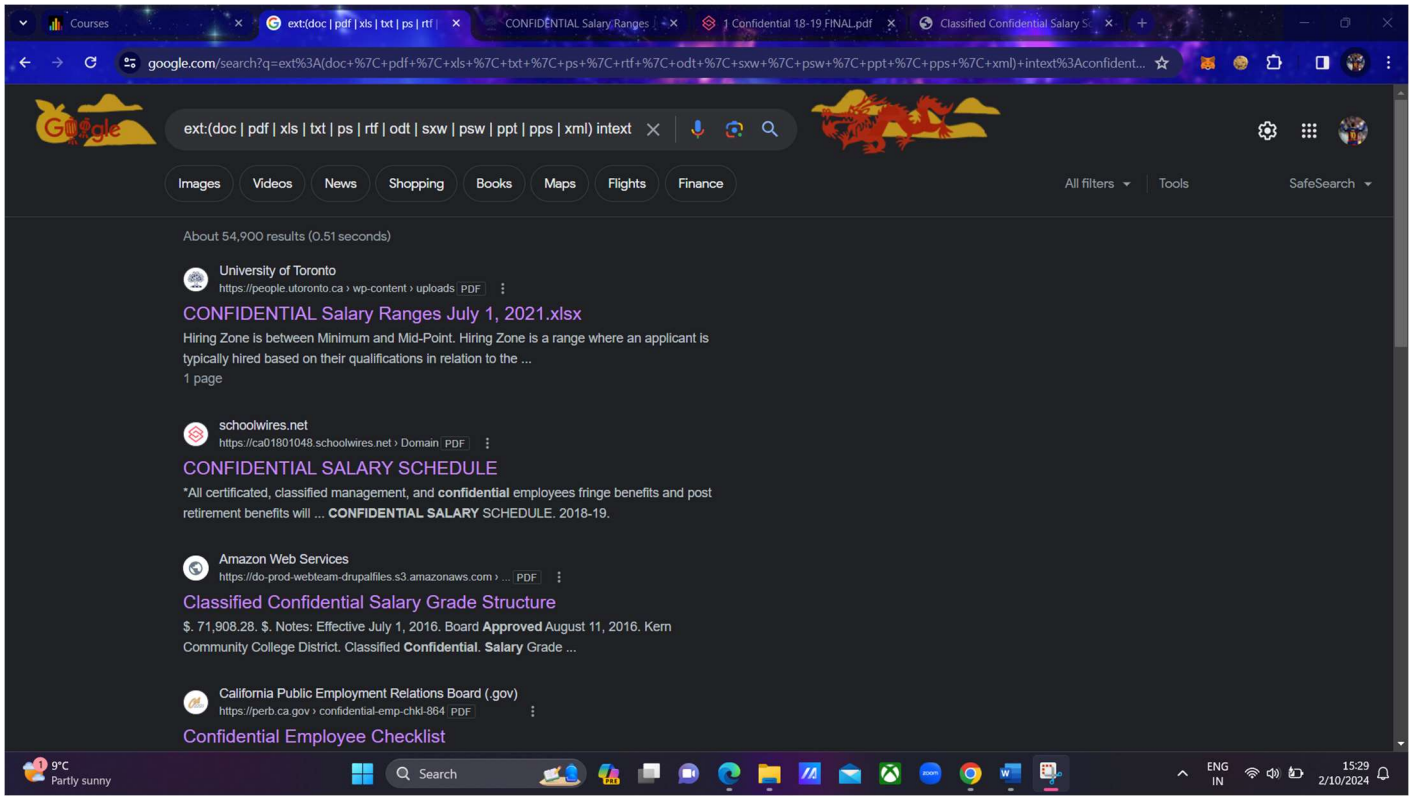

Kali 2024 - VMware Workstation 17 Player (Non-commercial use only)
Player
Kali Linux
webcamXP 5
109.233.191.228:8090/multi.html
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Google Dorks of Live ...
WEBCAMXP 5
WEBCAMS AND IP CAMERAS SERVER FOR WINDOWS
Home
Multi view
Smartphone
Gallery
Administration
Not logged in
320x240
8°C
Mostly cloudy
Search
ENG
IN
16:18
2/10/2024

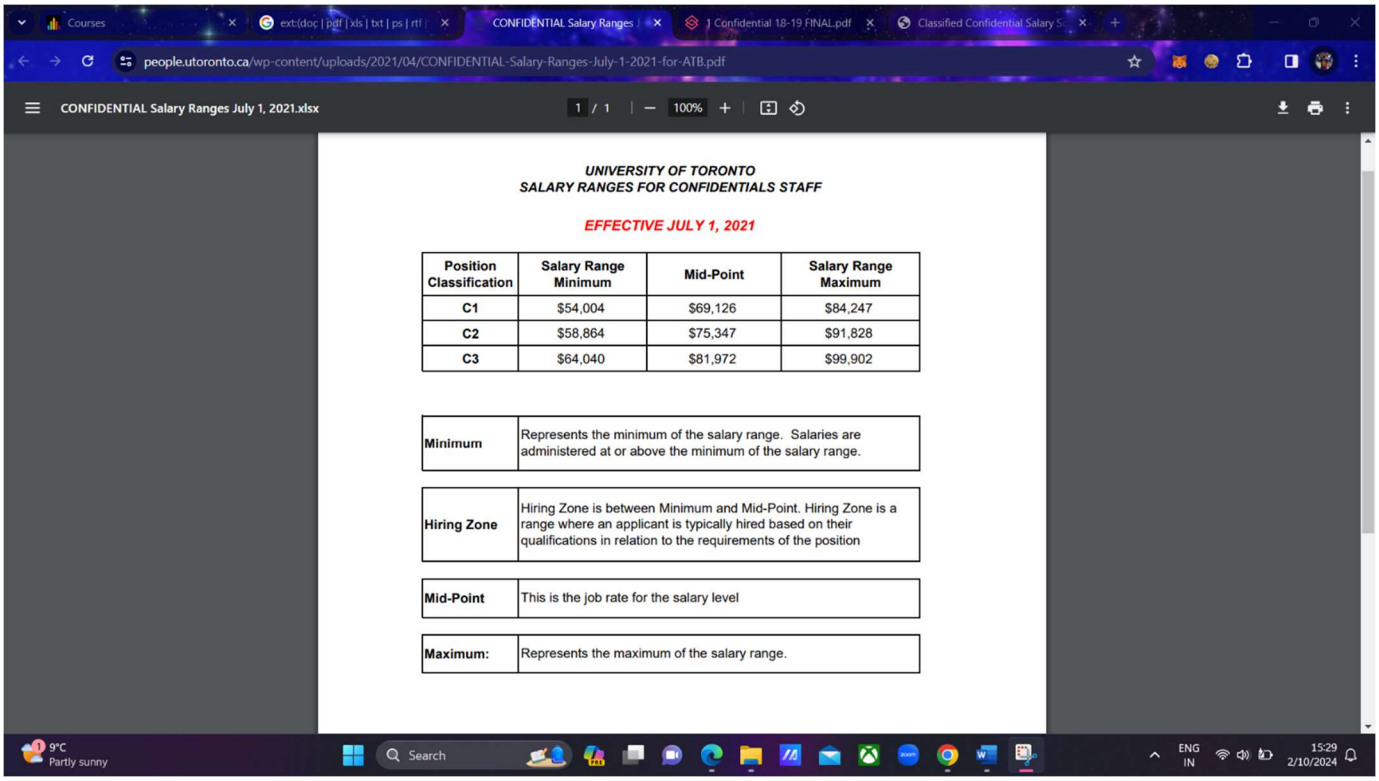
Proof of Lab

1. Attackers can take advantage of Google search logical operators such as AND, NOT and OR (case sensitive) as well as operators such as ~, – and *. The following link provides additional information on these operators.
2. Try the following example (insert the query into the search area of your web browser. You may copy this line from the lecture slides):

   *ext:(doc | pdf | xls | txt | ps | rtf | odt | sxw | psw | ppt | pps | xml) (intext:confidential salary **OR** intext:"budget approved") inurl:confidential*

3. Take a screenshot of the first web page and insert it in the form below.



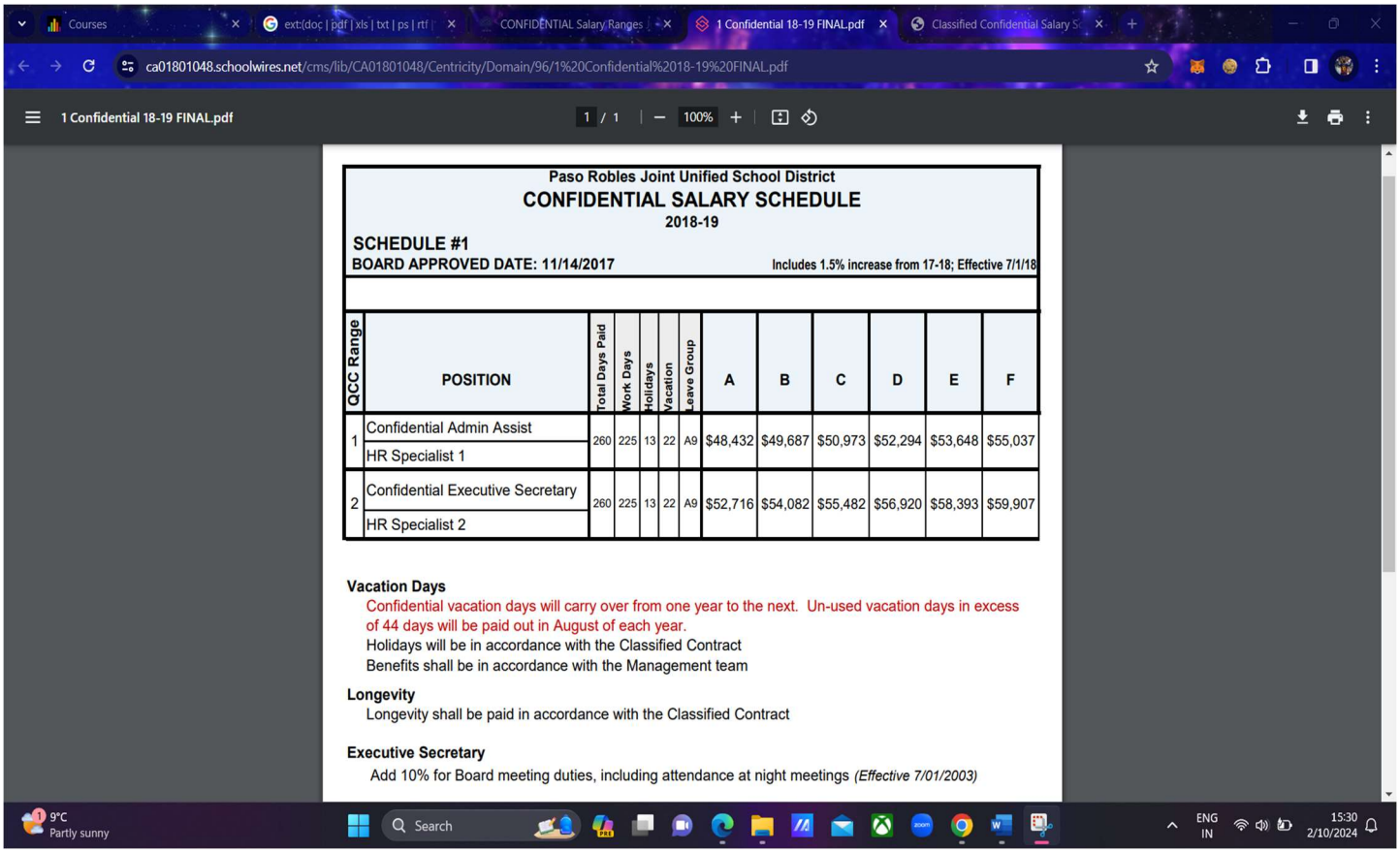


UNIVERSITY OF TORONTO
SALARY RANGES FOR CONFIDENTIALS STAFF

EFFECTIVE JULY 1, 2021

Position Classification	Salary Range Minimum	Mid-Point	Salary Range Maximum
C1	$54,004	$69,126	$84,247
C2	$58,864	$75,347	$91,828
C3	$64,040	$81,972	$99,902

Minimum	Represents the minimum of the salary range. Salaries are administered at or above the minimum of the salary range.
Hiring Zone	Hiring Zone is between Minimum and Mid-Point. Hiring Zone is a range where an applicant is typically hired based on their qualifications in relation to the requirements of the position
Mid-Point	This is the job rate for the salary level
Maximum:	Represents the maximum of the salary range.



Paso Robles Joint Unified School District

CONFIDENTIAL SALARY SCHEDULE

2018-19

SCHEDULE #1

BOARD APPROVED DATE: 11/14/2017 — **Includes 1.5% increase from 17-18; Effective 7/1/18**

QCC Range	POSITION	Total Days Paid	Work Days	Holidays	Vacation	Leave Group	A	B	C	D	E	F
1	Confidential Admin Assist HR Specialist 1	260	225	13	22	A9	$48,432	$49,687	$50,973	$52,294	$53,648	$55,037
2	Confidential Executive Secretary HR Specialist 2	260	225	13	22	A9	$52,716	$54,082	$55,482	$56,920	$58,393	$59,907

Vacation Days

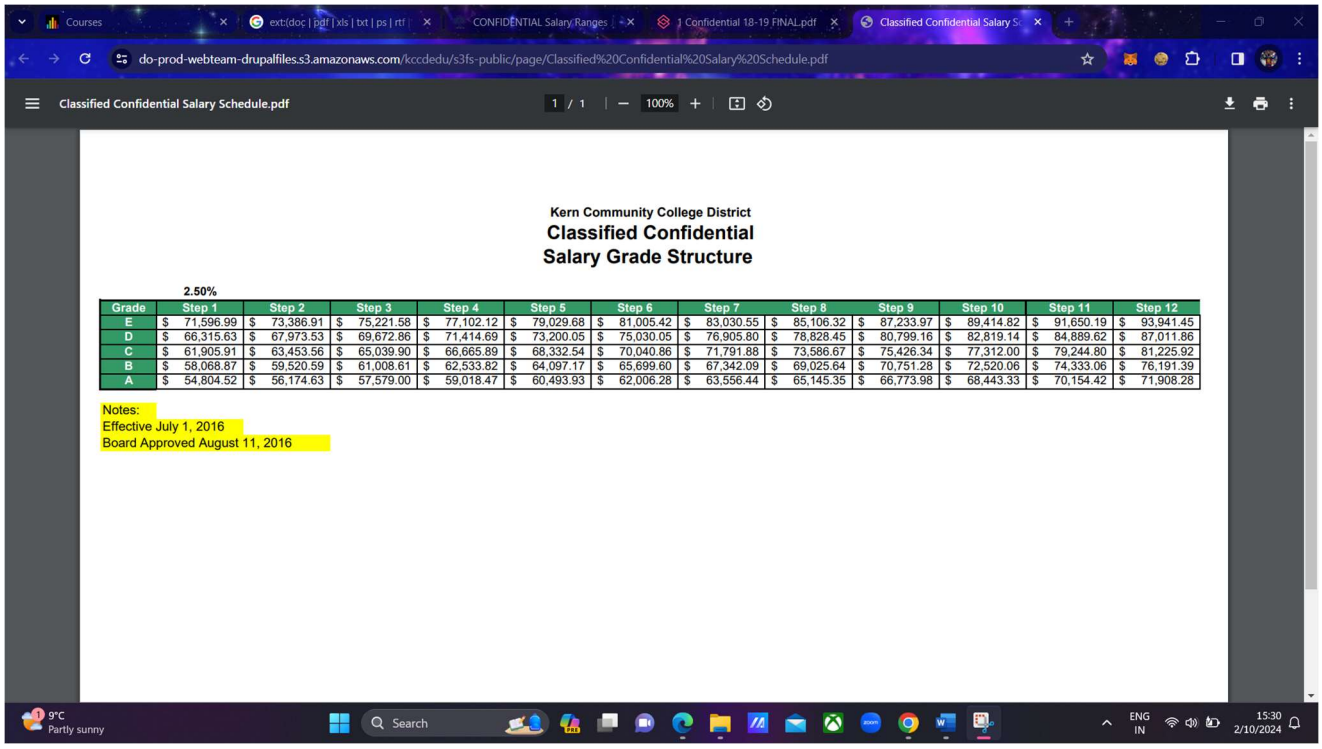
Confidential vacation days will carry over from one year to the next. Un-used vacation days in excess of 44 days will be paid out in August of each year.
Holidays will be in accordance with the Classified Contract
Benefits shall be in accordance with the Management team

Longevity

Longevity shall be paid in accordance with the Classified Contract

Executive Secretary

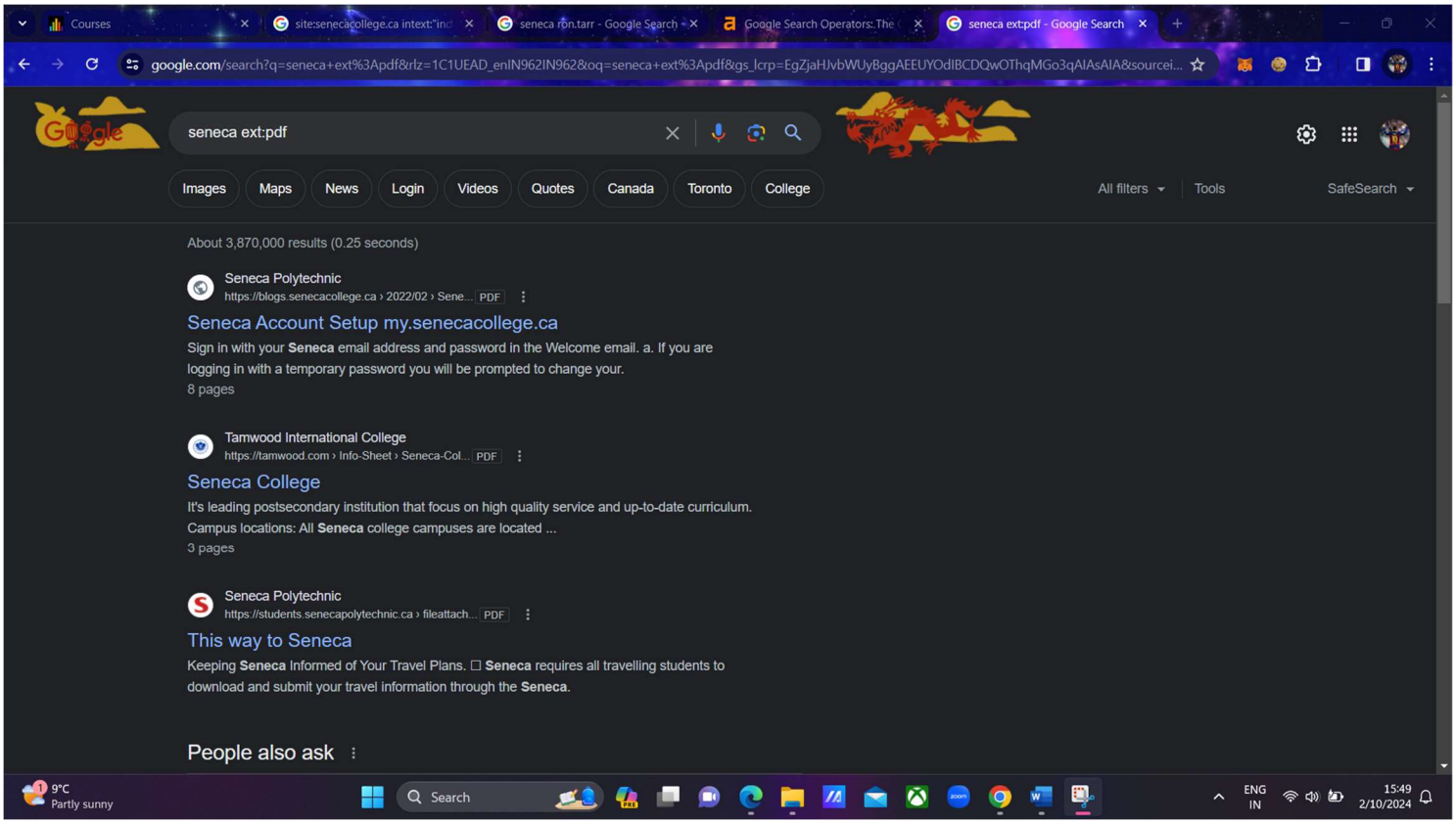
Add 10% for Board meeting duties, including attendance at night meetings *(Effective 7/01/2003)*



4. Answer the following question:

- What does the ext do in a Google search?
  This command is filetype command basically it specifies the search in which type of file you want – file extension.

  For Eg – Seneca ext:pdf
  This will give me all the Seneca results which are available in form of a pdf.

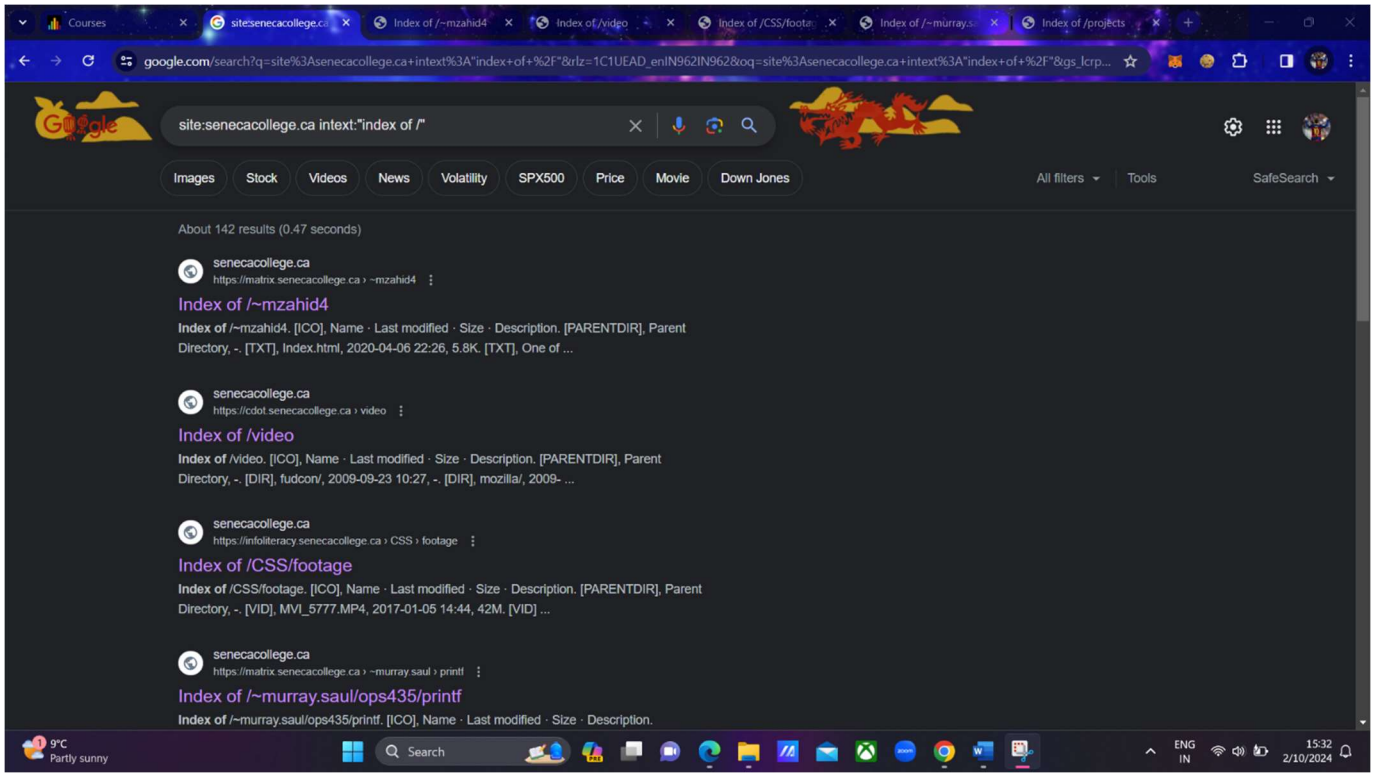


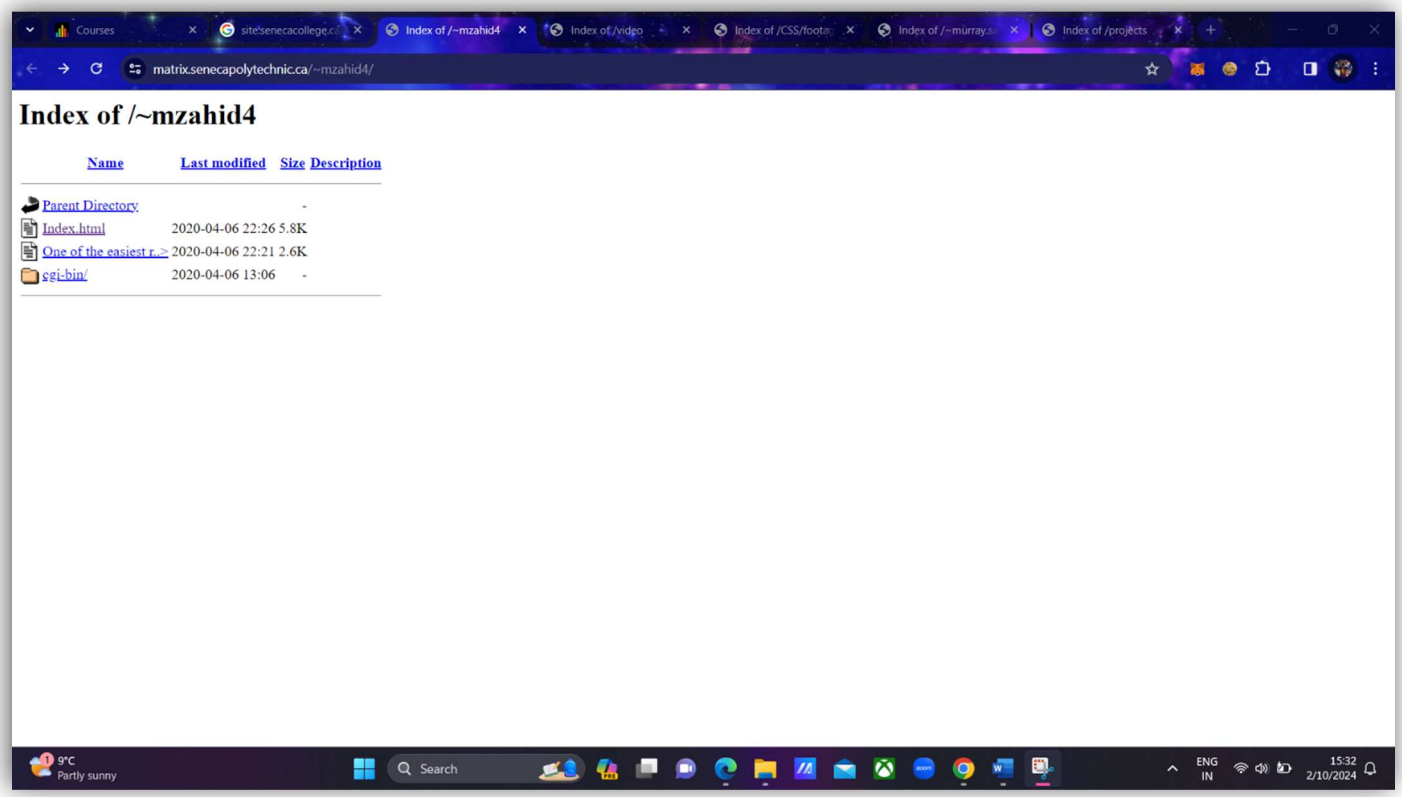
Open a web browser and type the following command:

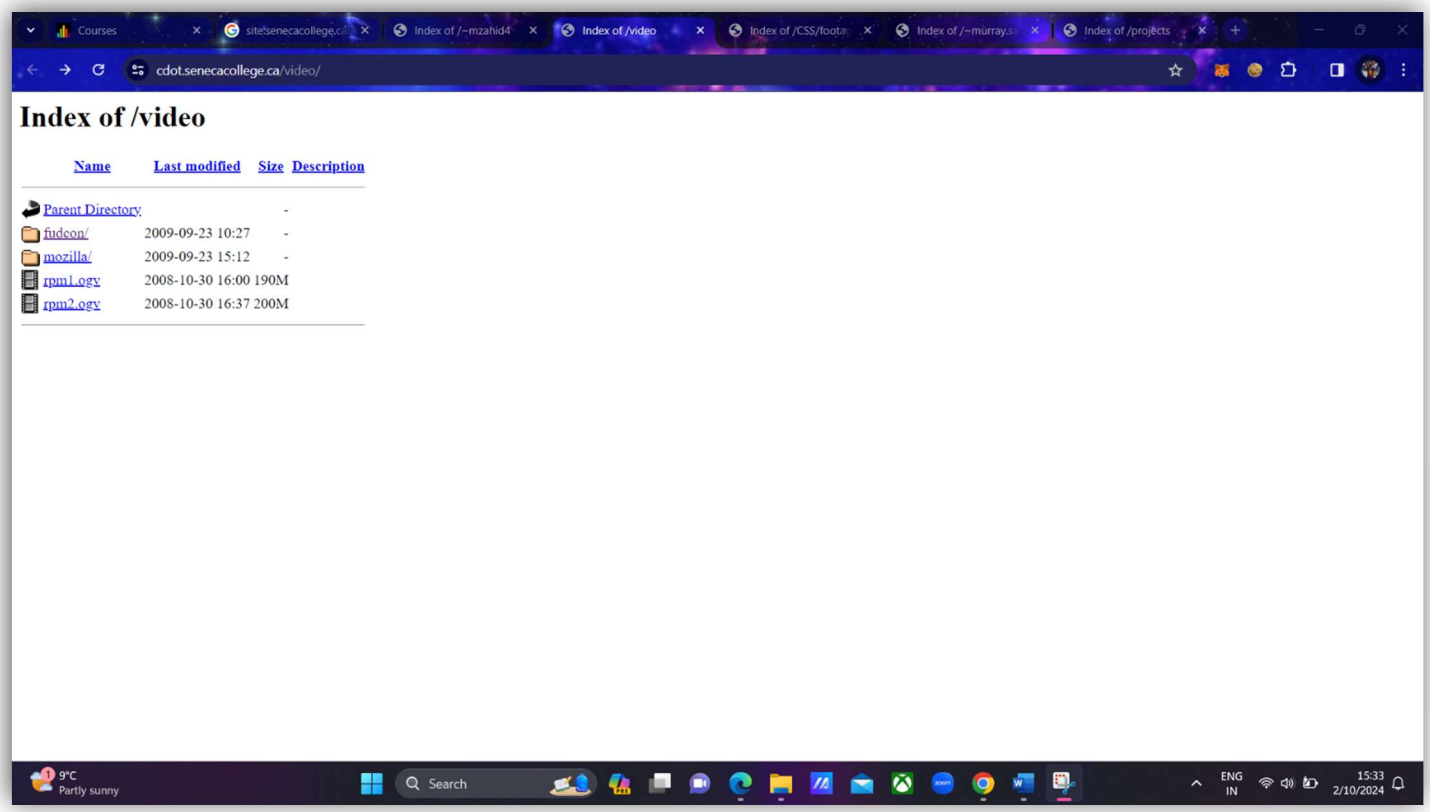
site:*senecacollege.ca* **intext:***"index of /"*

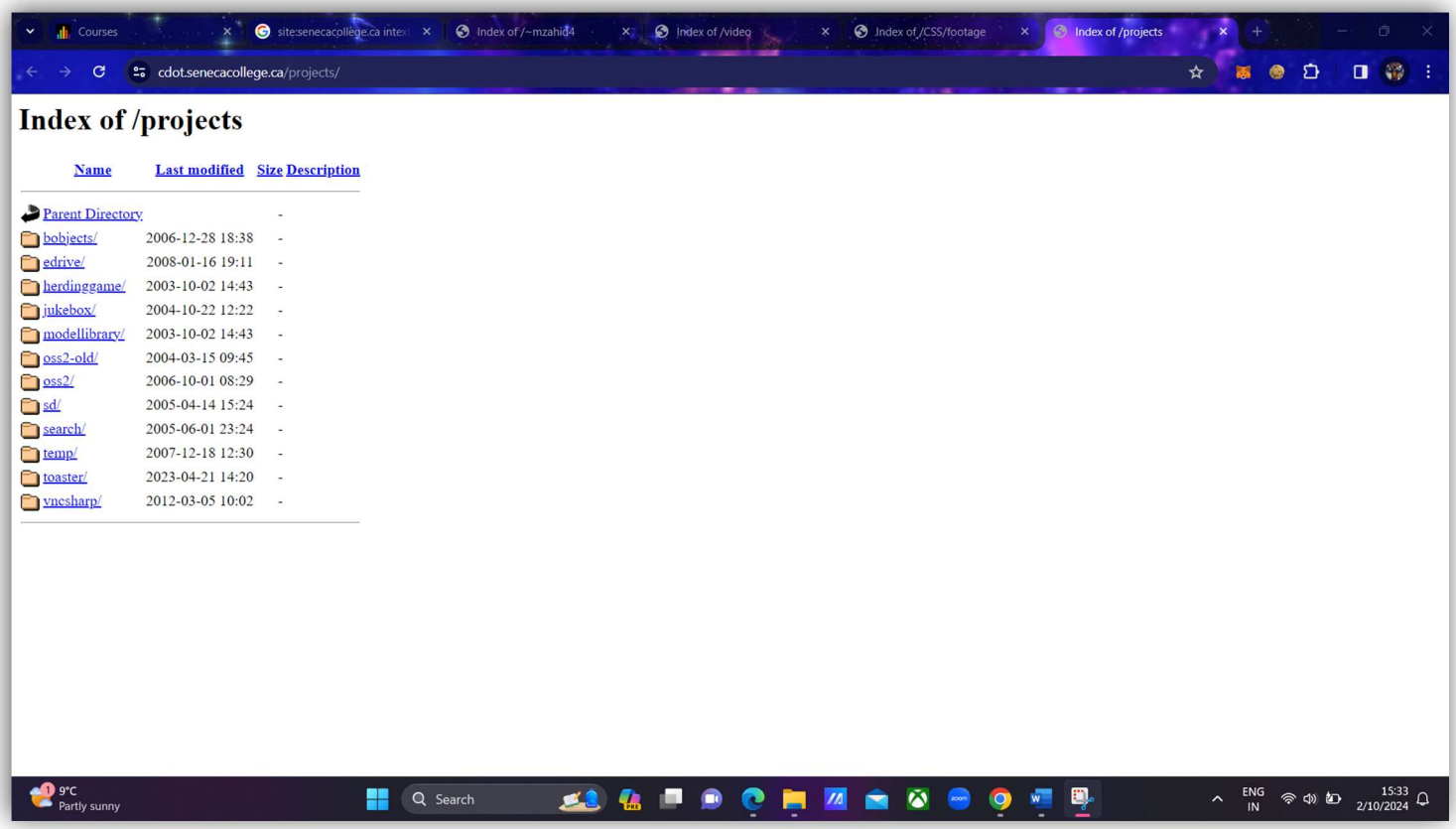
This search quarry will list all hidden directories (*intext:* query) on the *senecacollege.ca* (*site:* query) website.

5. Click on **"/~ron.tarr**" and review the results. Take a screenshot of the web page output and insert it below.


site:senecacollege.ca intext:"index of /"
Images
Stock
Videos
News
Volatility
SPX500
Price
Movie
Down Jones
All filters
Tools
SafeSearch
About 142 results (0.47 seconds)
senecacollege.ca
https://matrix.senecacollege.ca › ~mzahid4
Index of /~mzahid4
Index of /~mzahid4. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. [TXT], Index.html, 2020-04-06 22:26, 5.8K. [TXT], One of ...
senecacollege.ca
https://cdot.senecacollege.ca › video
Index of /video
Index of /video. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. [DIR], fudcon/, 2009-09-23 10:27, -. [DIR], mozilla/, 2009- ...
senecacollege.ca
https://infoliteracy.senecacollege.ca › CSS › footage
Index of /CSS/footage
Index of /CSS/footage. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. [VID], MVI_5777.MP4, 2017-01-05 14:44, 42M. [VID] ...
senecacollege.ca
https://matrix.senecacollege.ca › ~murray.saul › printf
Index of /~murray.saul/ops435/printf
Index of /~murray.saul/ops435/printf. [ICO], Name · Last modified · Size · Description.
9°C
Partly sunny
Search
ENG
IN
15:32
2/10/2024


matrix.senecapolytechnic.ca/~mzahid4/
Index of /~mzahid4
Name
Last modified
Size
Description
Parent Directory -
Index.html 2020-04-06 22:26 5.8K
One of the easiest r..> 2020-04-06 22:21 2.6K
cgi-bin/ 2020-04-06 13:06 -
9°C
Partly sunny
Search
ENG
IN
15:32
2/10/2024


Courses
Index of /~mzahid4
Index of /video
Index of /projects
cdot.senecacollege.ca/video/
Index of /video
Name Last modified Size Description
Parent Directory -
fudcon/ 2009-09-23 10:27 -
mozilla/ 2009-09-23 15:12 -
rpm1.ogv 2008-10-30 16:00 190M
rpm2.ogv 2008-10-30 16:37 200M
9°C
Partly sunny
Search
ENG
IN
15:33
2/10/2024


Courses
Index of /~mzahid4
Index of /video
Index of /CSS/footage
Index of /projects
cdot.senecacollege.ca/projects/
Index of /projects
Name Last modified Size Description
Parent Directory -
bobjects/ 2006-12-28 18:38 -
edrive/ 2008-01-16 19:11 -
herdinggame/ 2003-10-02 14:43 -
jukebox/ 2004-10-22 12:22 -
modellibrary/ 2003-10-02 14:43 -
oss2-old/ 2004-03-15 09:45 -
oss2/ 2006-10-01 08:29 -
sd/ 2005-04-14 15:24 -
search/ 2005-06-01 23:24 -
temp/ 2007-12-18 12:30 -
toaster/ 2023-04-21 14:20 -
vnesharp/ 2012-03-05 10:02 -
9°C
Partly sunny
Search
ENG
IN
15:33
2/10/2024

6. Answer the following questions:
    a. What does the **intext** do in a Google search?

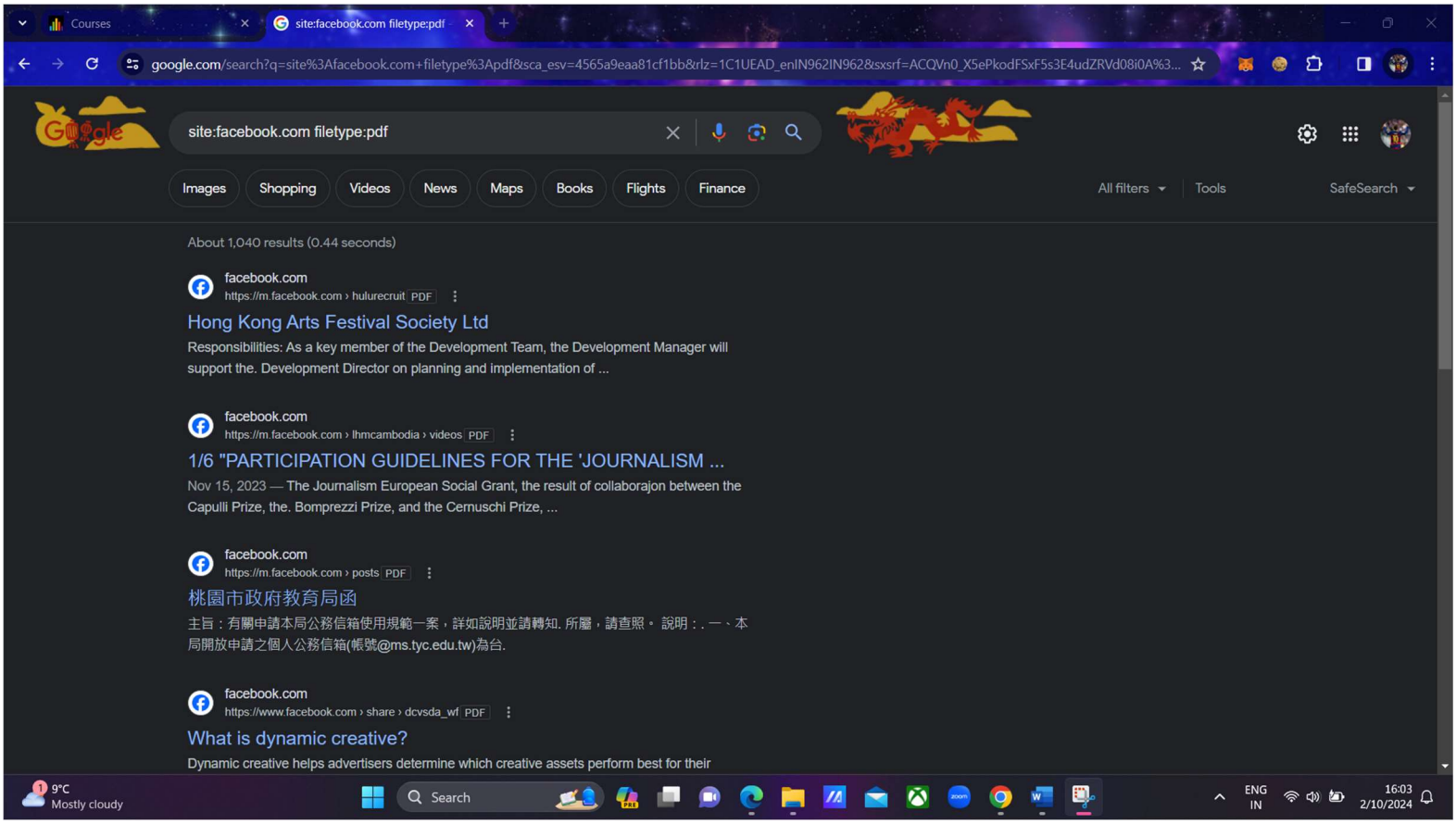
    Basically, intext command search for the pages with a particular word in their content.

    For Eg – intext:Seneca college

    b. What query should you type into Google search to look for “pdf” files from specific URL?

    site:(website url) filetype:pdf

    Eg: site:facebook.com filetype:pdf



Part 7: Useful Google Dorks for Ethical Hacking

- https://web.archive.org/web/20140822191407/http://www.boris-koch.de/wp-content/uploads/2011/01/Liste-Google-Hacking.pdf
- https://www.exploit-db.com/google-hacking-database
- https://gist.github.com/stevenswafford/393c6ec7b5375d5e8cdc
- https://gbhackers.com/latest-google-dorks-list/

Submit your Lab (Use this submission template)

- **Doublecheck all your answers.**
- **Save the file on your computer for future reference.**
- **Save the file again as a "`.pdf`" file.**
- **Submit the PDF file for grading.**