Experiment 03

Aim:

To use **OSINT DORKS (Open-Source Intelligence – Search Engine Dorking)** to create and execute advanced search queries that verify the accuracy of information by cross-referencing various sources and critically evaluating the **reliability and credibility** of news articles or web content.

Theory:

Open-Source Intelligence (OSINT) refers to the process of collecting and analyzing publicly available information to generate meaningful insights — without hacking or illegal access. OSINT can be performed using tools, scripts, or even manually through advanced search queries.

One of the most powerful and underrated methods is **Google Dorking** — using specific search operators to mine sensitive or insightful data from public websites.

✅ **What are Google Dorks?**

Google Dorks are crafted queries that use **search engine operators** to filter and refine search results for targeted investigation. These dorks can uncover hidden files, public documents, login portals, usernames, email addresses, and more.

🔑 **Commonly Used Google Dork Operators:**

Operator	Function	Example
site:	Search within a specific website or domain	site:gov.in "cyber crime"
inurl:	Finds URLs containing the given keyword	inurl:admin
intitle:	Searches for keywords in the page title	intitle:"index of"
filetype:	Search specific file types	filetype:pdf confidential
ext:	Alias for filetype	ext:docx resume
cache:	Displays Google's cached version of a site	cache:example.com

link:	Finds pages that link to a given site	link:example.com
define:	Provides definitions of words	define:phishing
allintitle:	Finds pages with all specified words in the title	allintitle:login admin
allinurl:	Finds URLs containing all specified words	allinurl:admin login
allintext:	Finds text within the body of a page	allintext:"confidential salary"
*	Wildcard operator	"admin * login"
OR	Combines multiple search conditions	filetype:pdf OR filetype:docx
-	Excludes specific results	"report" -site:example.com
"	Exact phrase search	"Indian Cyber Law"

PROCEDURE:

1. **Open Google.com** in your browser.
2. Identify your **target** — a person, website, organization, or type of information.
3. Use **Dorking Operators** based on what you're searching for (emails, PDFs, directories, credentials).
4. Begin with general queries like:
   - site:gov.in "cybersecurity policy"
   - "John Smith" filetype:pdf OR filetype:docx
5. Use **exclusion operators** to avoid unreliable sources:
   - "data breach" -site:quora.com
6. Use **OR**, intitle:, inurl:, and filetype: combinations for deeper refinement.
7. Manually inspect the **URLs, site credibility**, and check for:
   - Source reputation (gov, edu, news)
   - Recency of information
   - Repetition or consistency across other sites

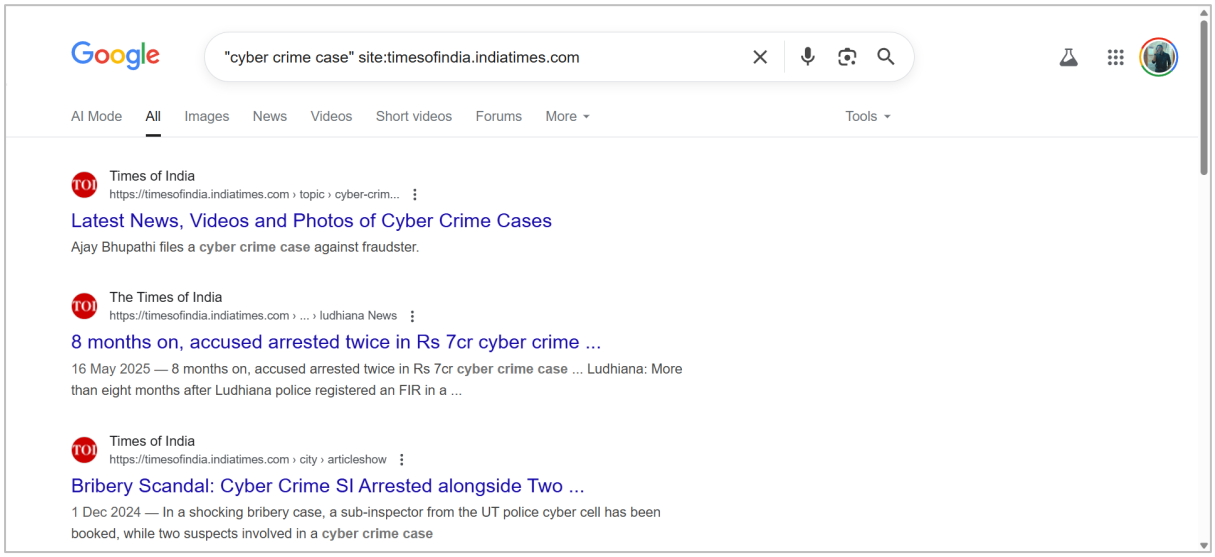
8. **Document any exposed files** with paths or metadata. Take screenshots if needed.
9. Summarize your results and confirm if the news or content is accurate or misleading.

Operators:

1. site:

- **Purpose**: Limit results to a specific website or domain

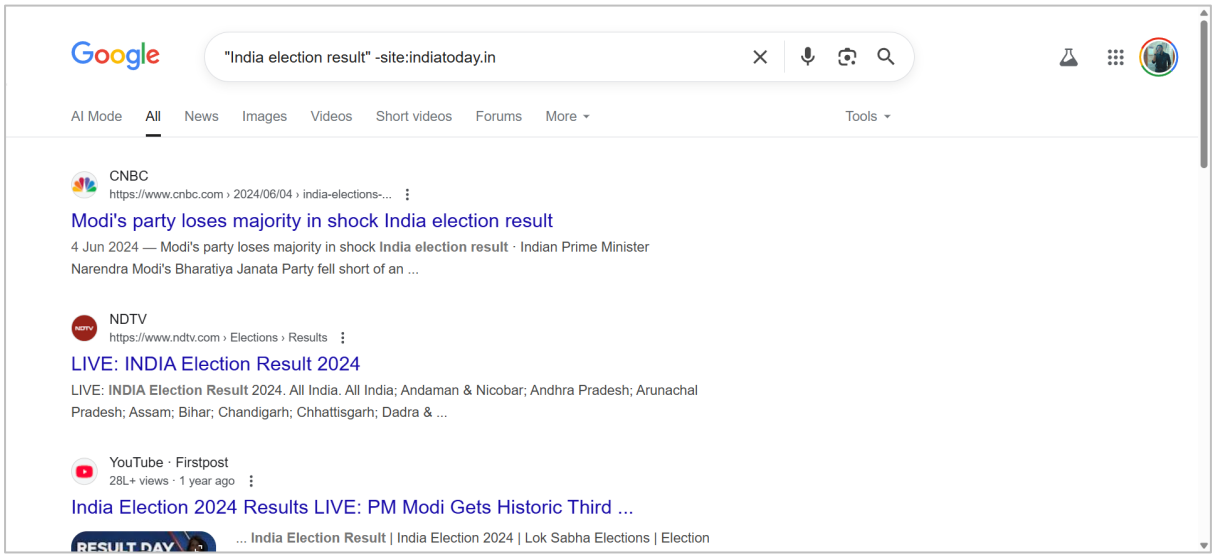
```
>> "cyber crime case" site:timesofindia.indiatimes.com
```



2. -site: (minus operator)

- **Purpose**: Exclude results from a specific domain

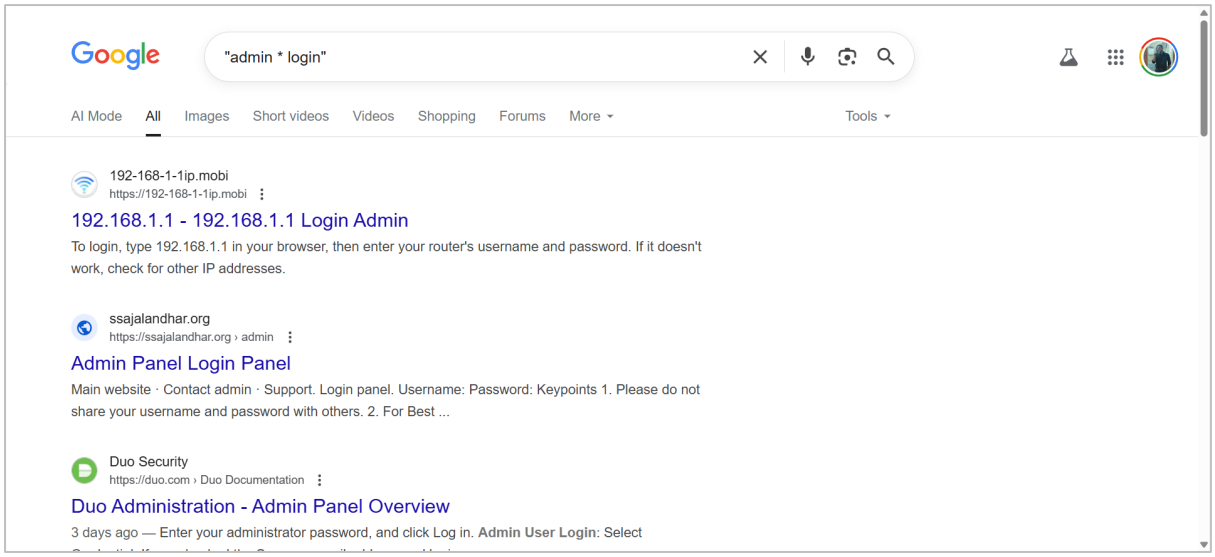
```
>> "India election result" -site:indiatoday.in
```



3. Wildcard *

- **Purpose**: Acts as a placeholder for unknown terms

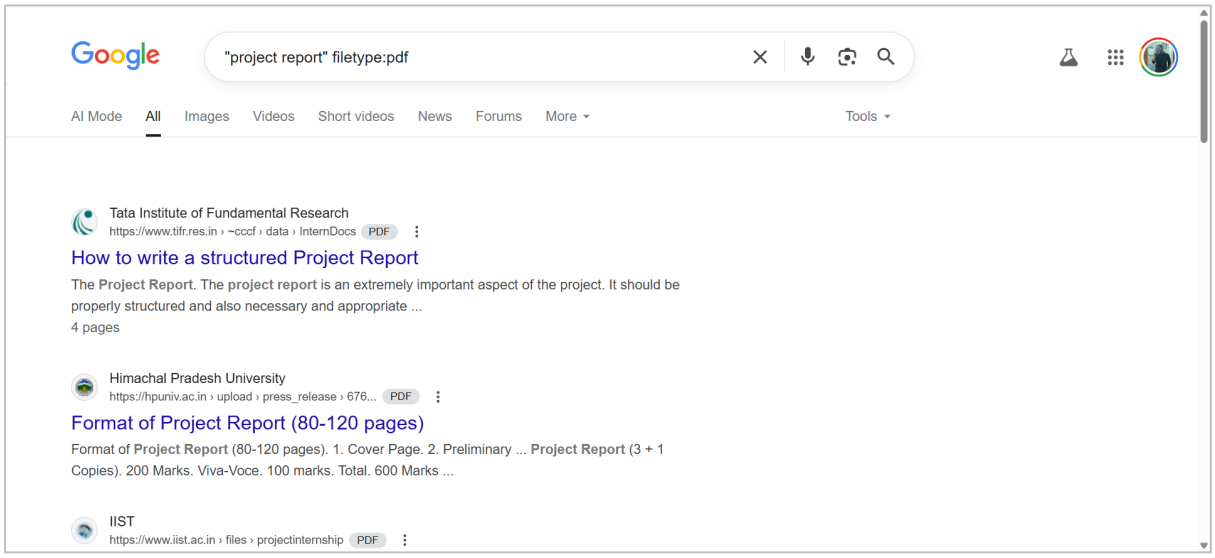
```
>> "admin * login"
```



4. filetype:

- **Purpose**: Search for specific file formats

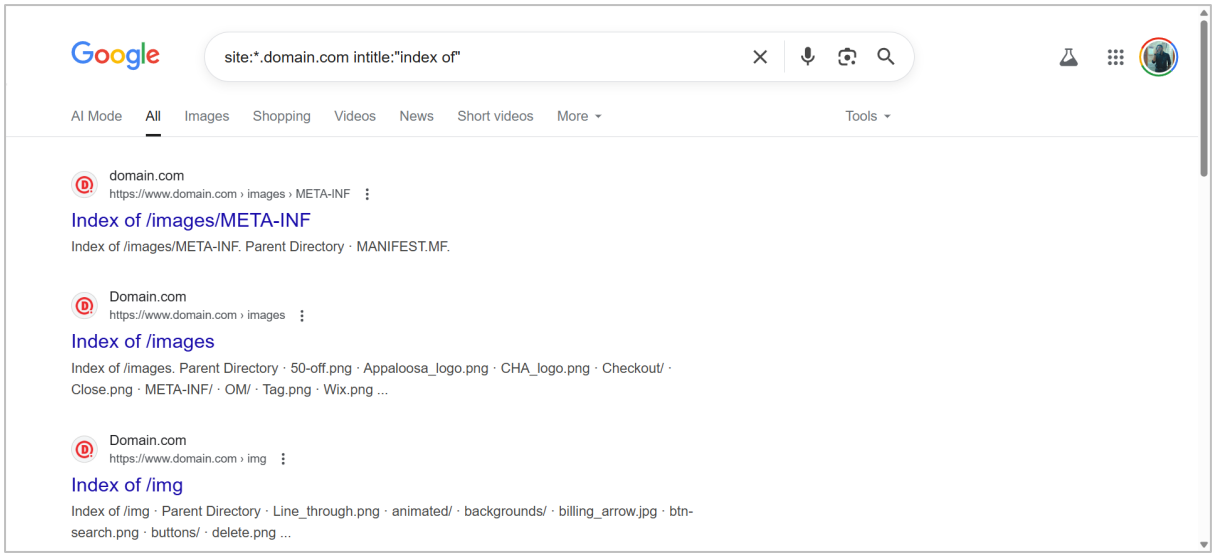
```
>> "project report" filetype:pdf
```



5. intitle:

- **Purpose**: Searches for terms in the webpage title

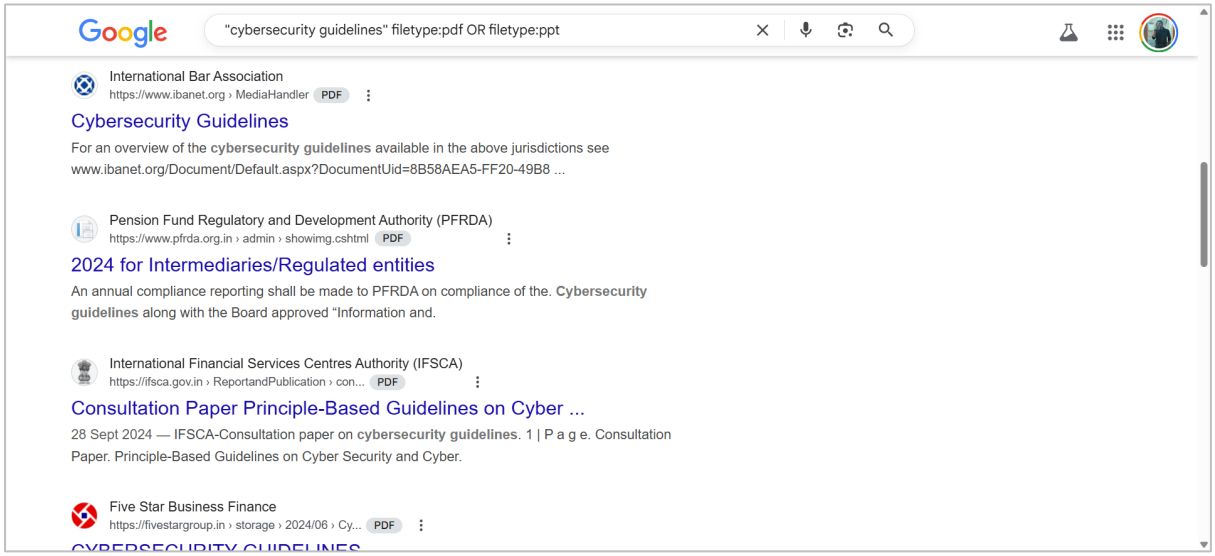
```
>> site:*.domain.com intitle:"index of"
```



6. OR

- **Purpose**: Search for either of two keywords

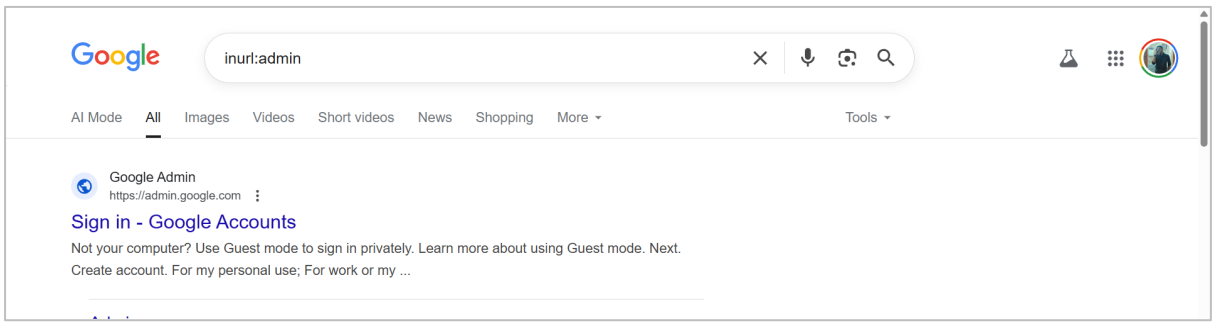
```
>> "cybersecurity guidelines" filetype:pdf OR filetype:ppt
```



7. inurl:

- **Purpose**: Finds keywords inside URLs

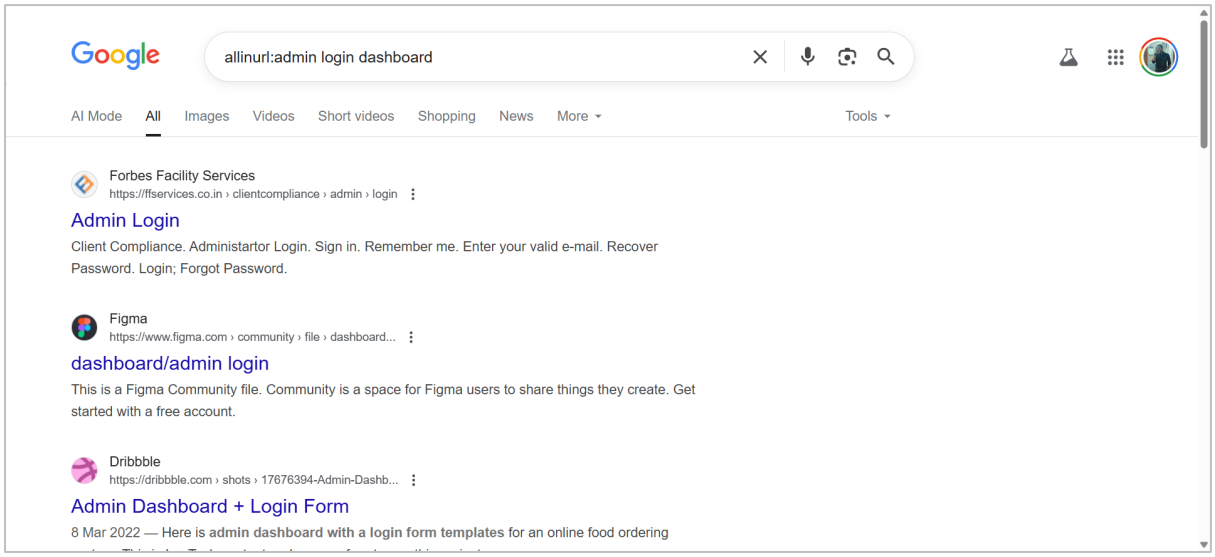
```
>> inurl:admin
```



8. allinurl:

- **Purpose**: Matches all words inside URLs

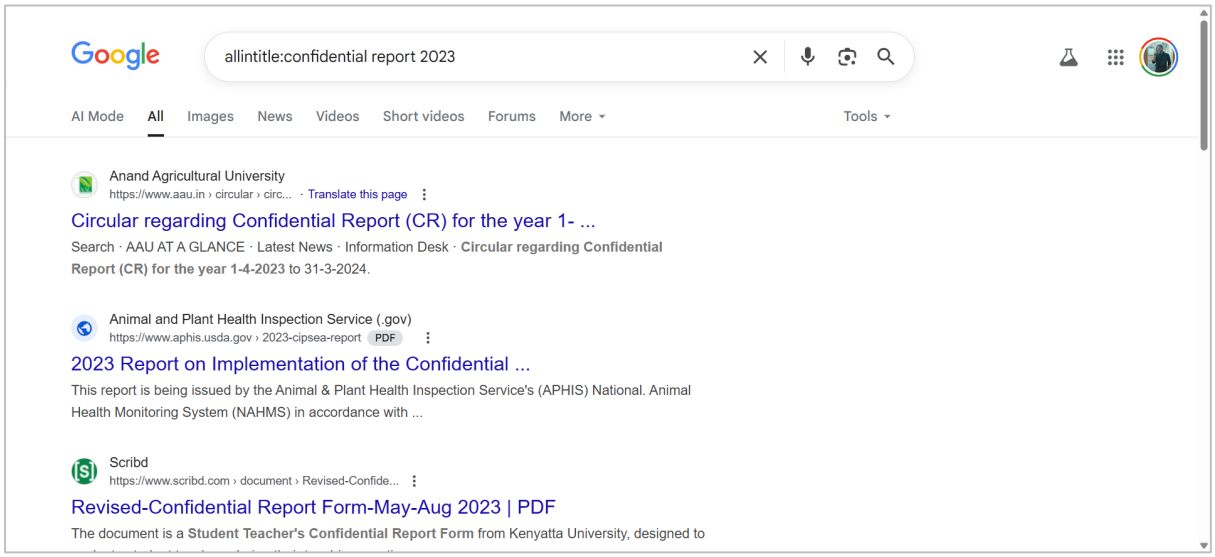
```
>> allinurl:admin login dashboard
```



9. allintitle:

- **Purpose**: Finds all given keywords in page titles

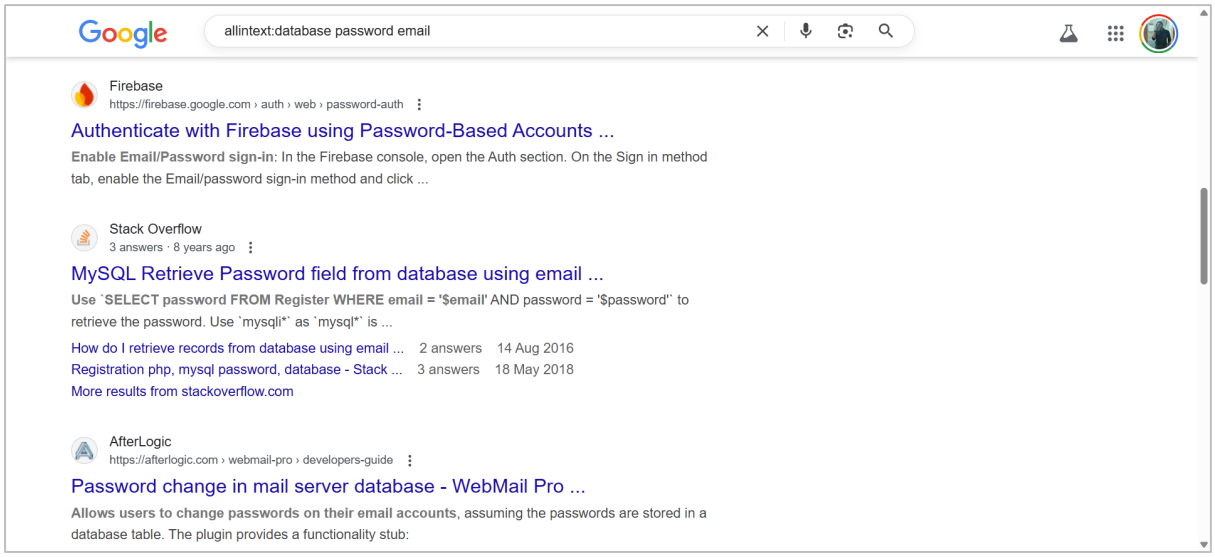
```
>> allintitle:confidential report 2023
```



10. allintext:

- **Purpose**: Finds all given words in the body text of the page

```
>> allintext:database password email
```



Conclusion:

In this experiment, we have effectively used **Google Dorking techniques** under the scope of OSINT to extract, verify, and validate publicly available information. By employing a variety of **search operators**, we enhanced the precision of our investigation and successfully cross-referenced news and data across multiple sources. This methodology highlights the **power of advanced search logic** in gathering intelligence — vital for both cybersecurity analysts and ethical researchers.