Cyber Security

Class no 05(Lab 3, Arabi Sir)

21 Sep 2024

# Reconnaissance:

* OSINT – Open Source Intelligence

Pentest Methodology

* <https://www.virustotal.com/gui/> 🡪 check is there any virus in crack file🡪 for any link must first try this link and then click the link
* <https://app.any.run/> 🡪virus check for file
* <https://leakpeek.com/> 🡪 check, is your data public?
* For a picture, first check property
* How to create a Share Folder in kali Linux 🡪See assignment
  + First turnoff the virtual machine then start again
  + Cd /media/sf\_JU 🡪sf mean shared file //terminal (use TAB button)
  + Store ch9 file in shared folder manually
  + Disk file check 🡪testdisk ch9 🡪Intel🡪advance🡪FAT32 🡪list🡪file🡪if there is a red file then go this file using cursor and type C and again C… file will be store in JU folder🡪convert file into ZIP 🡪then extract all🡪check properties of this picture 🡪
  + Terminal 🡪 cd /media/sf\_JU/Files/revendications/Pictures 🡪file location
    - Type exiftool 1000000000.jpg 🡪picture name 🡪 show all details about this picture
    - <https://www.gps-coordinates.net/> 🡪 add coordinate

┌──(shakil㉿kali)-[~]

└─$ **sudo -i**

[sudo] password for shakil:

┌──(root㉿kali)-[~]

└─# **cd /media/sf\_Share**

┌──(root㉿kali)-[/media/sf\_Share]

└─# **ls**

ch9

┌──(root㉿kali)-[/media/sf\_Share]

└─# **testdisk ch9**

TestDisk 7.2, Data Recovery Utility, February 2024

Christophe GRENIER <grenier@cgsecurity.org>

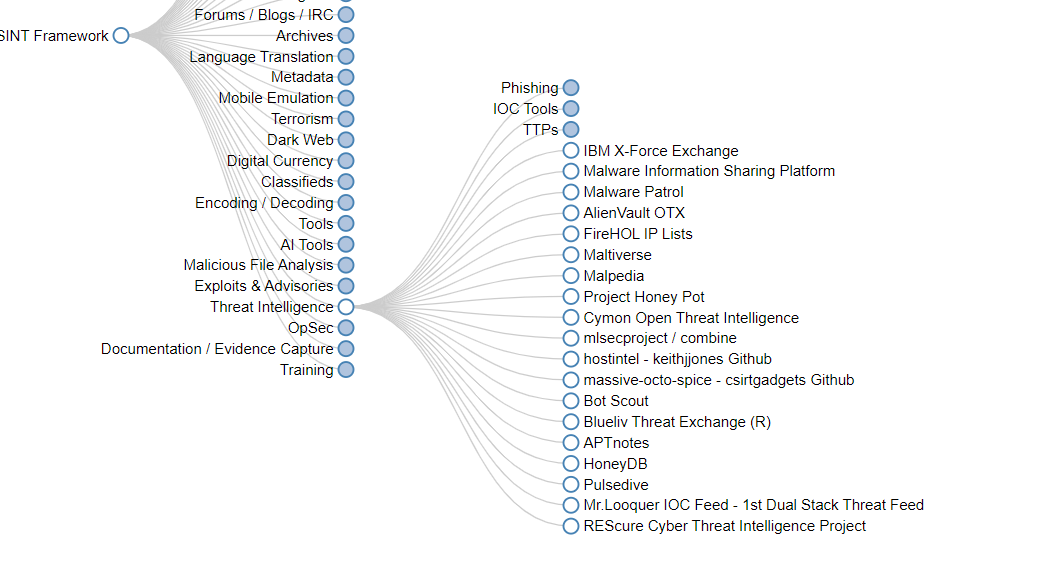
https://www.cgsecurity.org

┌──(root㉿kali)-[~]

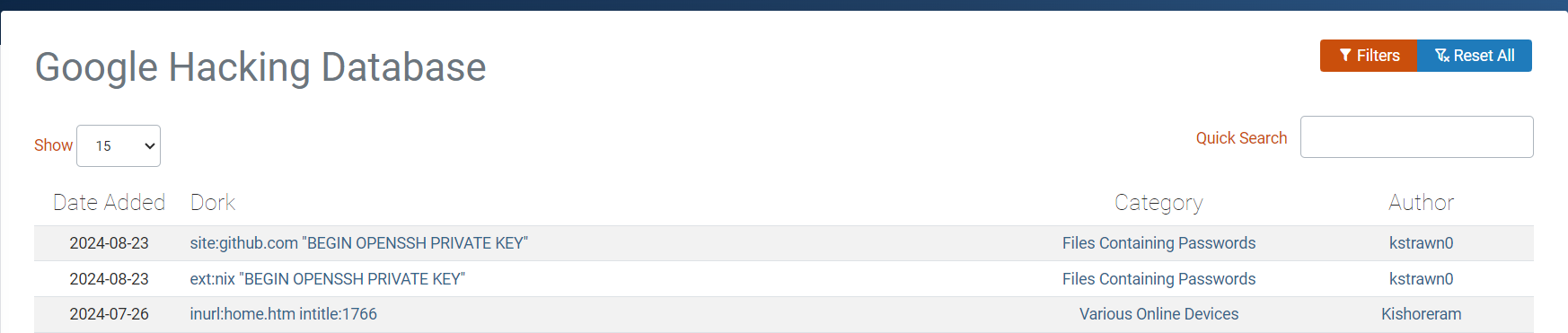
└─# **cd /media/sf\_Share/Files/revendications/Pictures** (Use TAB)

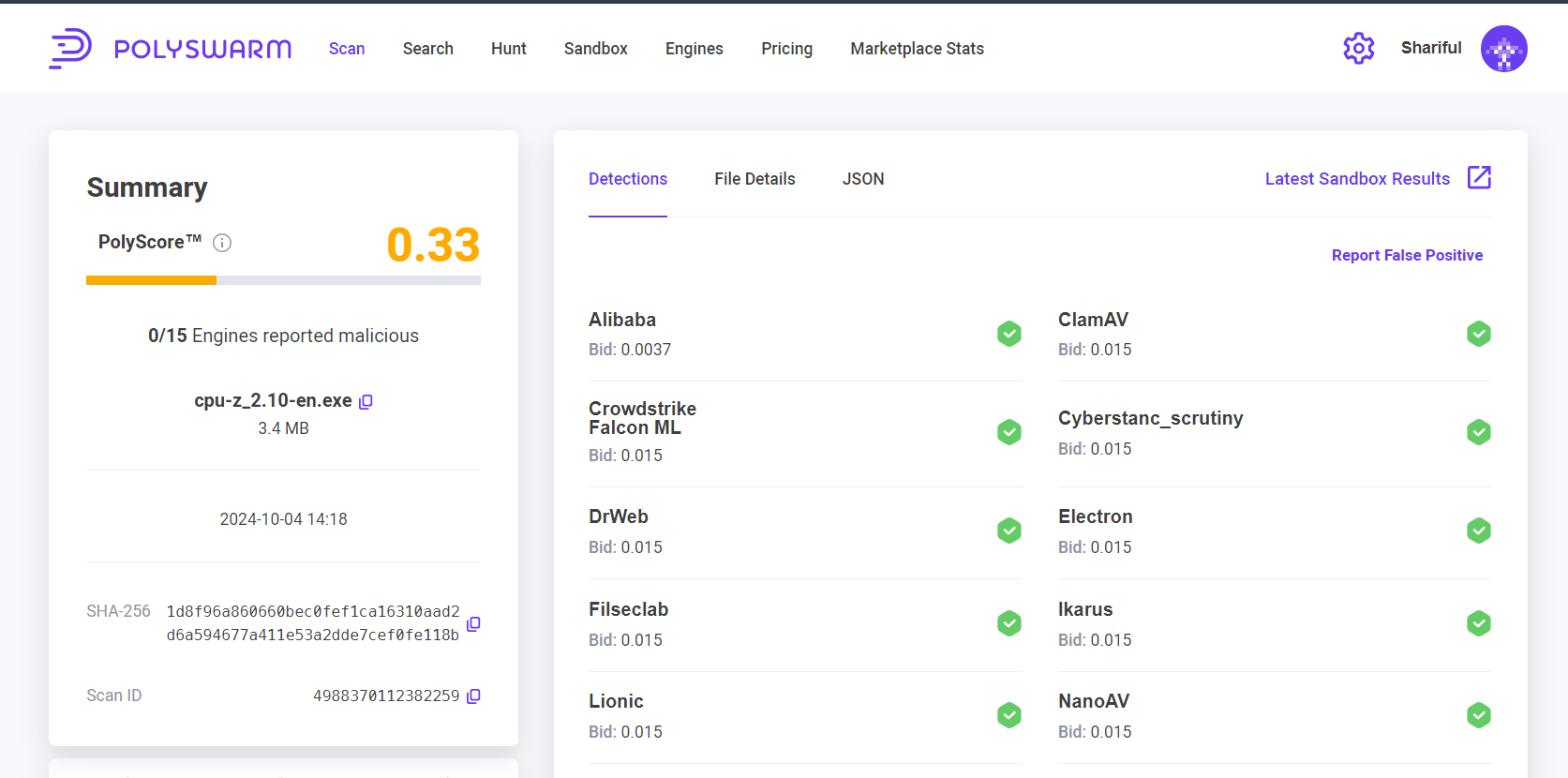
┌──(root㉿kali)-[/media/sf\_Share/Files/revendications/Pictures]

└─# **exiftool 1000000000000CC000000990038D2A62.jpg**

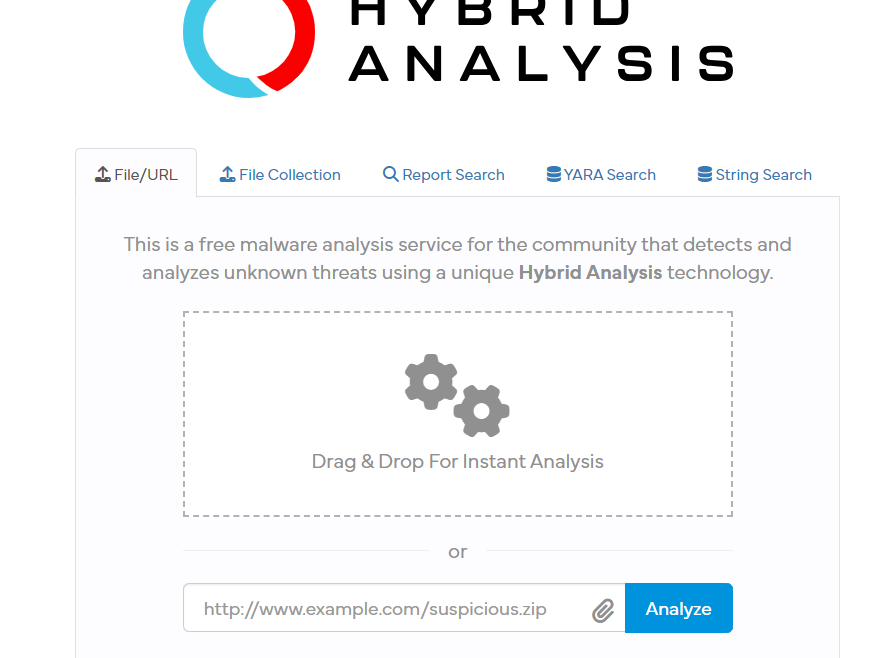
* <https://osintframework.com/> 🡪Check fast
* Assignment : 
* Exodus mobile aps: 🡪 for check any aps permission. Very important aps
* <https://osintleak.com/dashboard> : **for user all details**
* ?intitle:index.of? pdf hacking 🡪 for download any file/videos/ or goto <https://www.dorkgpt.com/>

site:juniv.edu filetype:doc

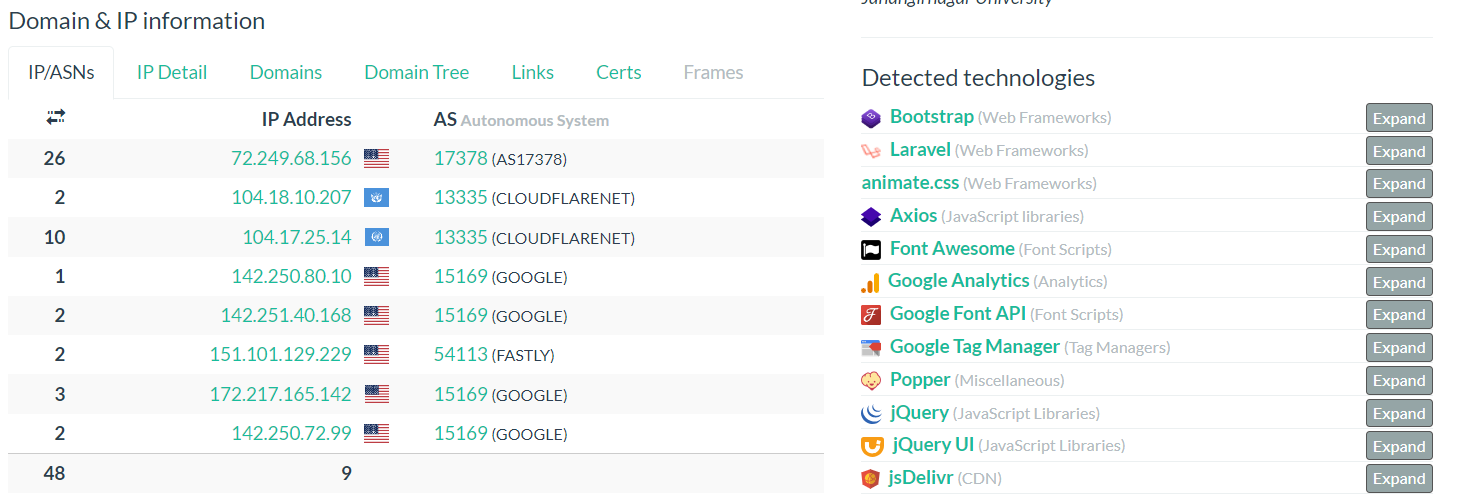
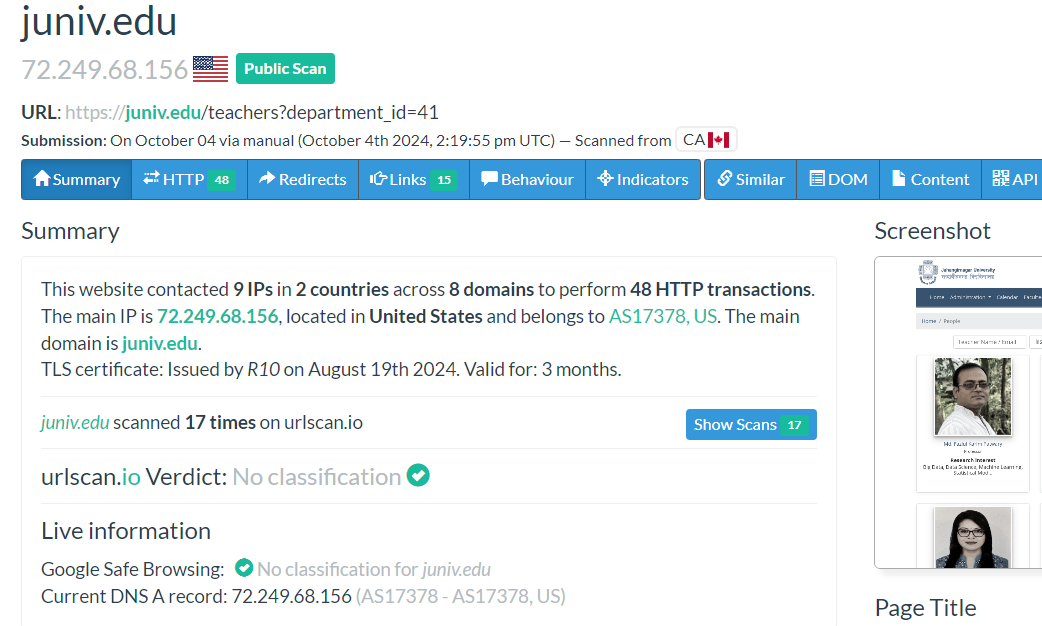
* dorkgpt. Com theke j kono 5 ta search er assignment
* <https://www.exploit-db.com/google-hacking-database> 🡪 Exploit database
* <https://polyswarm.io/>

Scan for big data/file

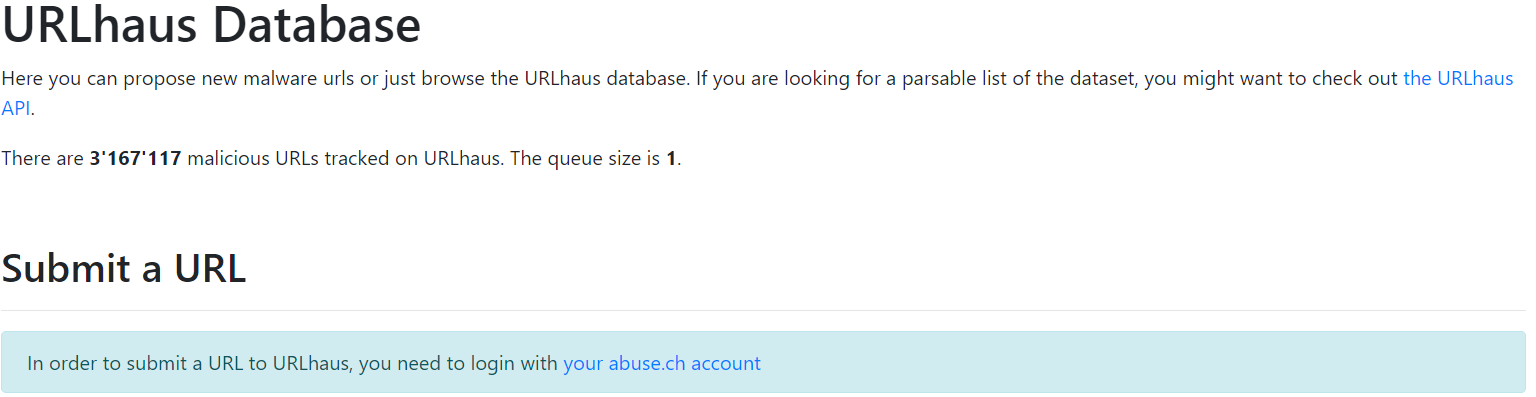
* <https://www.hybrid-analysis.com/>

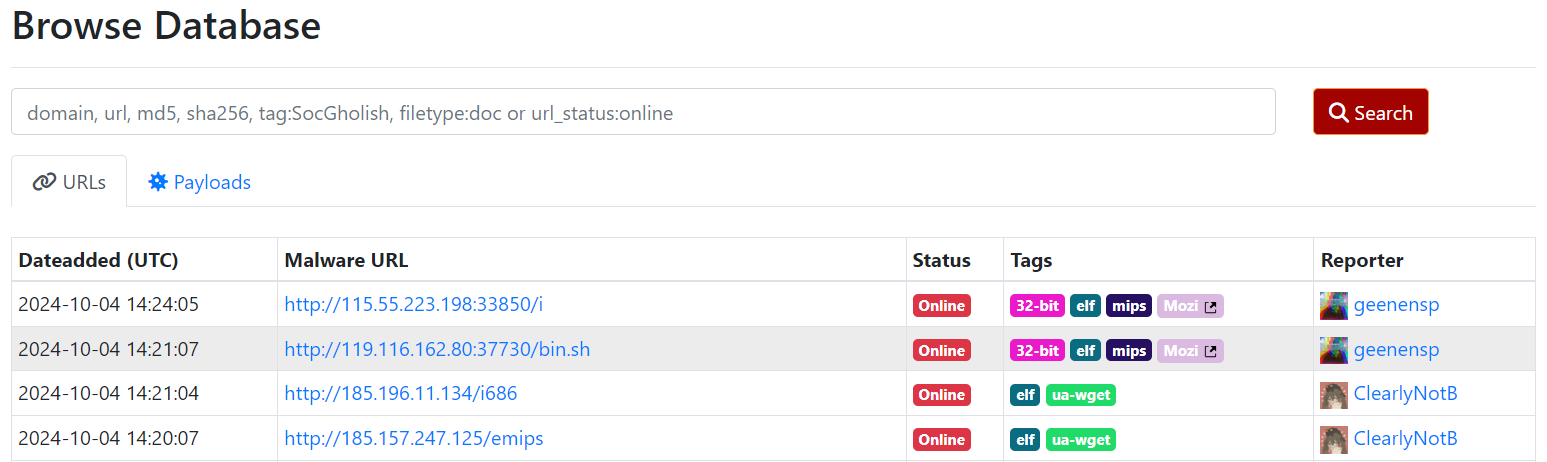
Free automated malware analysis

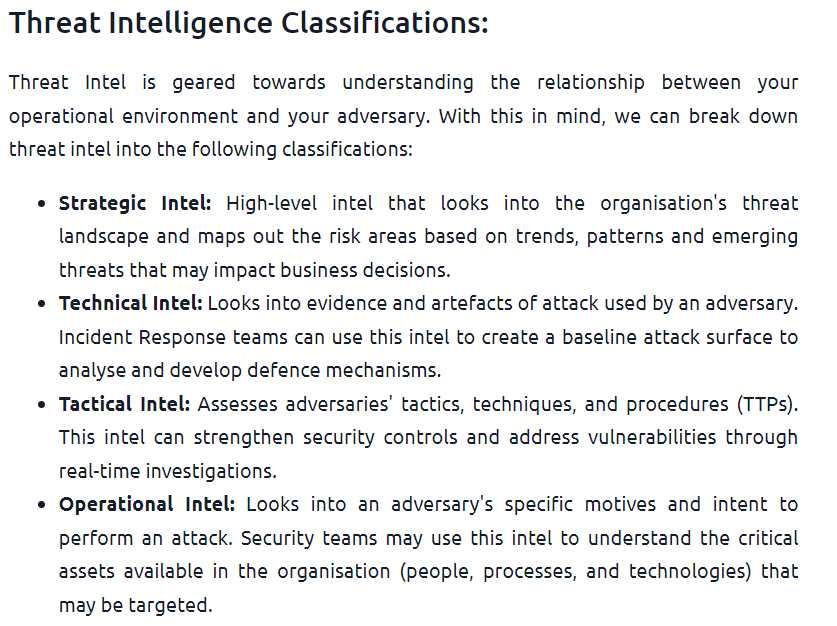
* <https://urlscan.io/>

Domain and IP information and all details about any URL

* <https://talosintelligence.com/>
* <https://urlhaus.abuse.ch/browse/>

List of all malware website, anyone can submit a website as a malware. 



* Assignment: world wide CC tv access
* 
* <https://abuse.ch/> 🡪 check 6 category assignment

**# Link from Arabi Sir:**

https://polyswarm.network/scan

https://metadefenderopswat.com/

https://analyze.intezer.com/

https://www.hybrid-analysis.com/

https://app.any.run/

https://tria.ge/submit/file

**OSINT Tools Collections #1**

OSRFramework: https://lnkd.in/dY2TZARX

OSINTLeaks: <https://osintleak.com/>

ChatGPT like web:

1. [Poe](https://poe.com/)
2. <https://claude.ai/new>

**Just search and see:**

* intitle:"webcamxp 5"
* site:juniv.edu filetype:pdf
* <http://insecam.org/en/byrating/>