Enhancing Digital Government and Economy
Cyber Security Course
Classwork-05

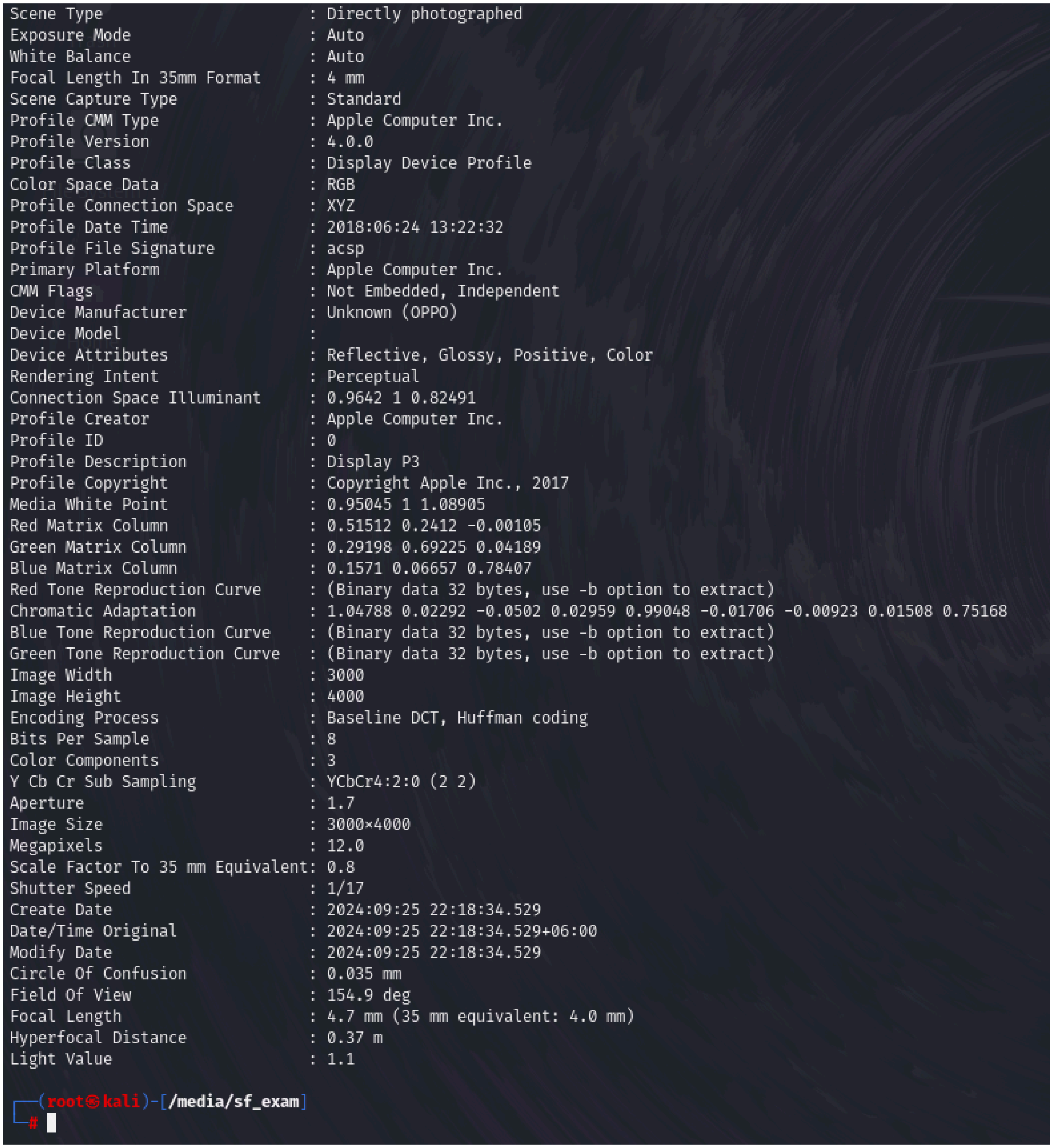
Submitted by,
Name: Koushiki Devi Agarwalla
Batch: JUR2B11
ID: 2111271

Forensic Investigation Command in Linux::

```
cd /media/sf_filename
ls
apt install testdisk
testdisk ch9
intel partition
fAT - Advanced
list
c to copy
zip
extract
exiftool
cd/media/sf_filename/files/revendication/pictures
exiftool(tab)filename
```

image 01

Information of this image:



```
Scene Type                      : Directly photographed
Exposure Mode                   : Auto
White Balance                   : Auto
Focal Length In 35mm Format     : 4 mm
Scene Capture Type              : Standard
Profile CMM Type                : Apple Computer Inc.
Profile Version                 : 4.0.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 2018:06:24 13:22:32
Profile File Signature          : acsp
Primary Platform                : Apple Computer Inc.
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             : Unknown (OPPO)
Device Model                    :
Device Attributes               : Reflective, Glossy, Positive, Color
Rendering Intent                : Perceptual
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 : Apple Computer Inc.
Profile ID                      : 0
Profile Description             : Display P3
Profile Copyright               : Copyright Apple Inc., 2017
Media White Point               : 0.95045 1 1.08905
Red Matrix Column               : 0.51512 0.2412 -0.00105
Green Matrix Column             : 0.29198 0.69225 0.04189
Blue Matrix Column              : 0.1571 0.06657 0.78407
Red Tone Reproduction Curve     : (Binary data 32 bytes, use -b option to extract)
Chromatic Adaptation            : 1.04788 0.02292 -0.0502 0.02959 0.99048 -0.01706 -0.00923 0.01508 0.75168
Blue Tone Reproduction Curve    : (Binary data 32 bytes, use -b option to extract)
Green Tone Reproduction Curve   : (Binary data 32 bytes, use -b option to extract)
Image Width                     : 3000
Image Height                    : 4000
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Aperture                        : 1.7
Image Size                      : 3000x4000
Megapixels                      : 12.0
Scale Factor To 35 mm Equivalent: 0.8
Shutter Speed                   : 1/17
Create Date                     : 2024:09:25 22:18:34.529
Date/Time Original              : 2024:09:25 22:18:34.529+06:00
Modify Date                     : 2024:09:25 22:18:34.529
Circle Of Confusion             : 0.035 mm
Field Of View                   : 154.9 deg
Focal Length                    : 4.7 mm (35 mm equivalent: 4.0 mm)
Hyperfocal Distance             : 0.37 m
Light Value                     : 1.1

┌──(root㉿kali)-[/media/sf_exam]
└─# 
```

1. **The photo was taken** - 2024-9-25
2. **Device Manufacture-** Unknown (OPPO)
3. **Encoding process**-Baseline DCT, Huffman coding
4. **Image height:** 4000
5. **Image taken** : 2024:09:25 22:18:34

Reconnaissance:

- OSINT – Open Source Intelligence

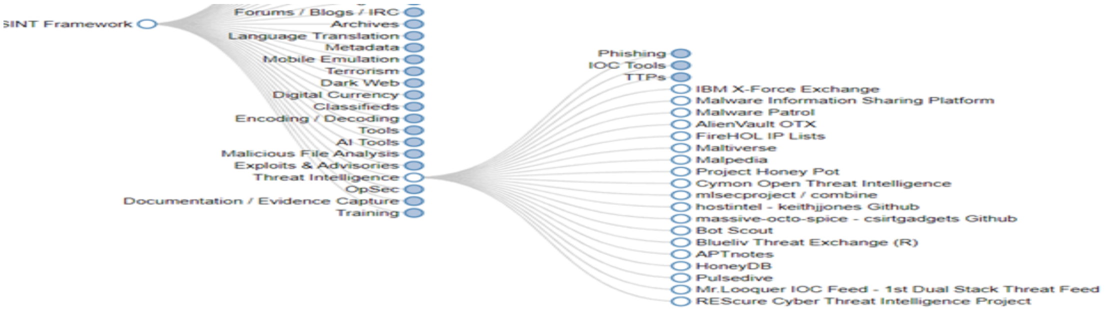
Pentest Methodology

- https://www.virustotal.com/gui/ check is there any virus in crack fileà 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 àSee 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 àtestdisk ch9 àIntelàadvanceàFAT32 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 folderàconvert file into ZIP àthen extract allàcheck properties of this picture à
    - Terminal cd /media/sf_JU/Files/revendications/Pictures àfile location
        - Type exiftool 32500002500.jpg picture name show all details about this picture
        - https://www.gps-coordinates.net/ add coordinate

```
┌──(shariful㉿kali)-[~]
└─$ sudo -i
[sudo] password for shariful:
┌──(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 3000000000000DD000000990038F20002.jpg
```

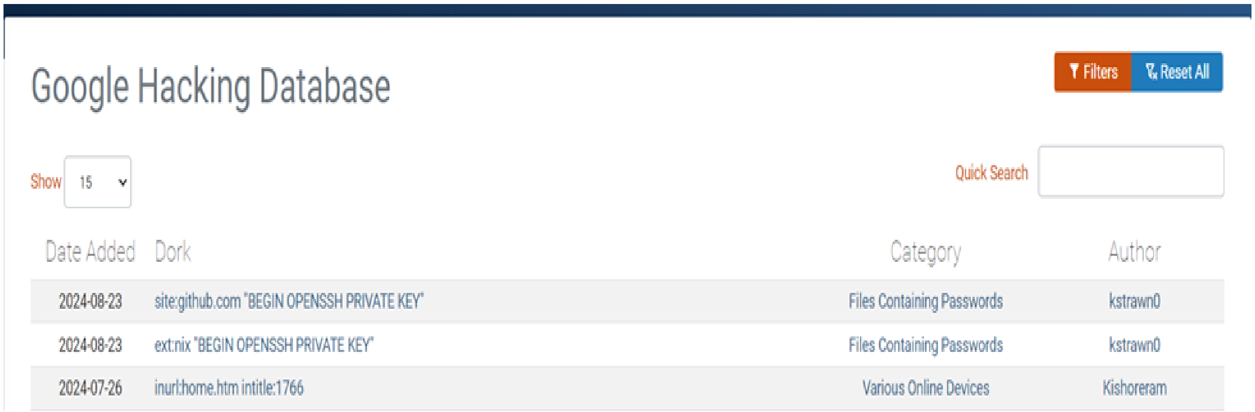
- https://osintframework.com/ Check fast
- Assignment :



- Exodus mobile aps: for check any aps permission. Very important aps
- https://osintleak.com/dashboard : **for user all details**
- intitle:index.of? pdf hacking à 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

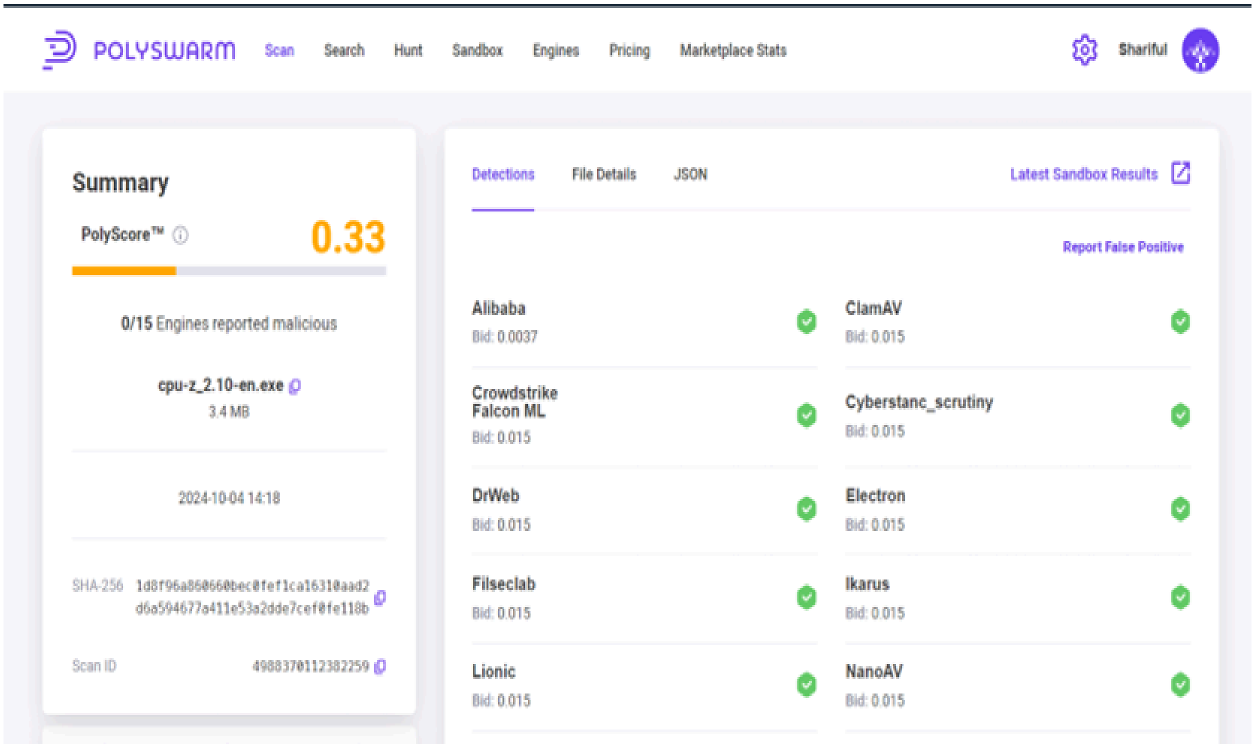


Google Hacking Database

Date Added	Dork	Category	Author
2024-08-23	site:github.com "BEGIN OPENSSH PRIVATE KEY"	Files Containing Passwords	kstrawn0
2024-08-23	ext:nix "BEGIN OPENSSH PRIVATE KEY"	Files Containing Passwords	kstrawn0
2024-07-26	inurl:home.htm intitle:1766	Various Online Devices	Kishoreram

- https://polyswarm.io/

Scan for big data/file



Summary

PolyScore™ 0.33

0/15 Engines reported malicious

cpu-z_2.10-en.exe
3.4 MB

2024-10-04 14:18

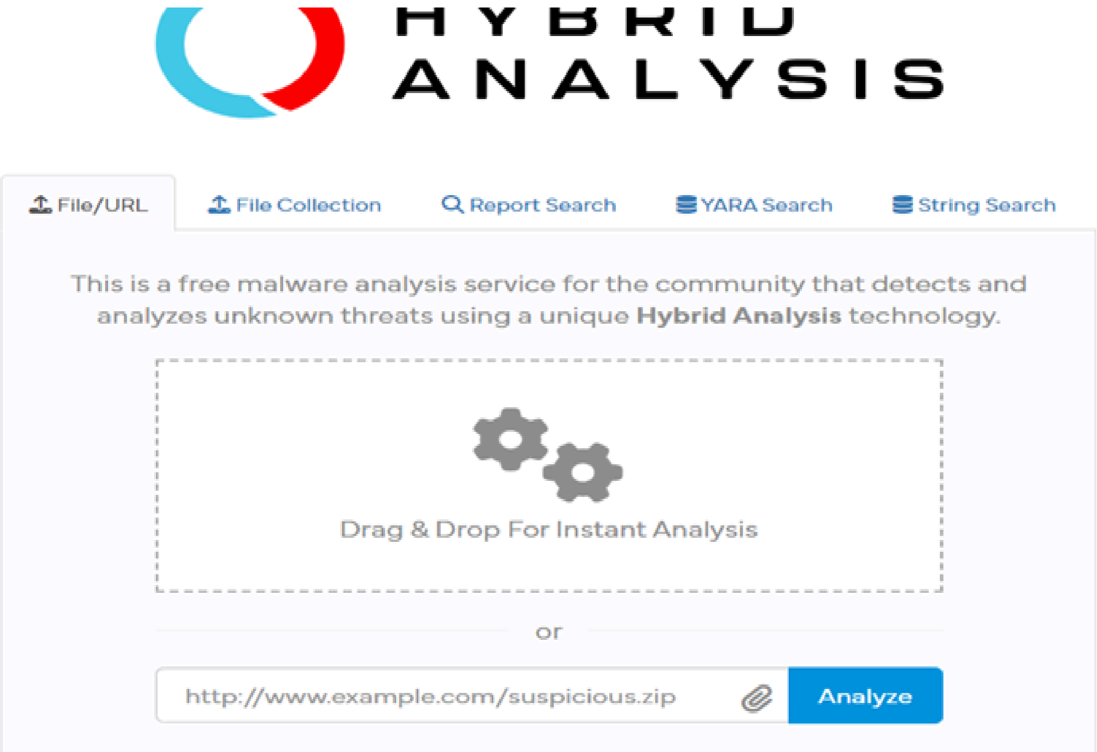
SHA-256 1d8f96a860660bec0fef1ca16310aad2d6a594677a411e53a2dde7cef0fe118b

Scan ID 4988370112382259

Alibaba Bid: 0.0037 ✓	ClamAV Bid: 0.015 ✓
Crowdstrike Falcon ML Bid: 0.015 ✓	Cyberstanc_scrutiny Bid: 0.015 ✓
DrWeb Bid: 0.015 ✓	Electron Bid: 0.015 ✓
Filseclab Bid: 0.015 ✓	Ikarus Bid: 0.015 ✓
Lionic Bid: 0.015 ✓	NanoAV Bid: 0.015 ✓

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

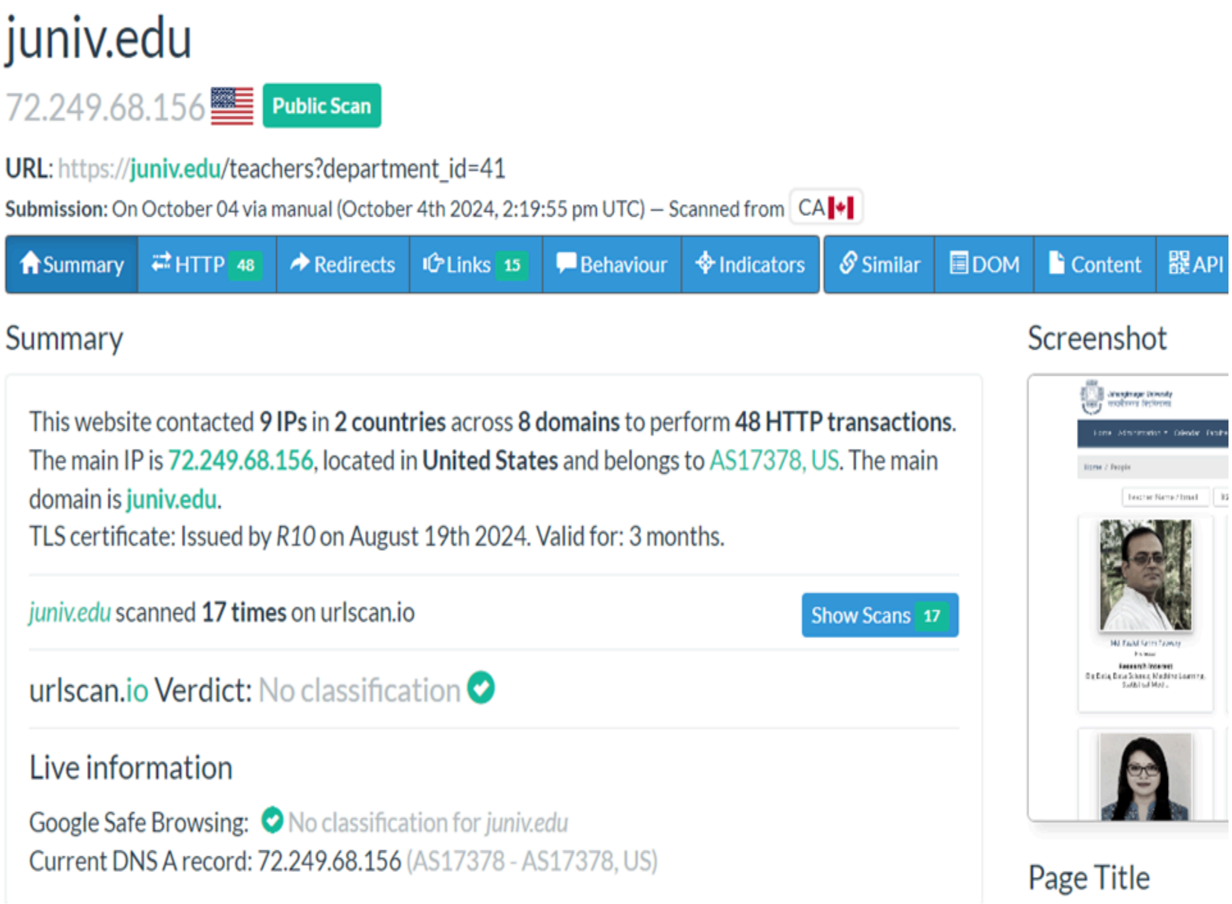
Free automated malware analysis



This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique **Hybrid Analysis** technology.

- https://urlscan.io/

Domain and IP information and all details about any URL



juniv.edu

72.249.68.156 Public Scan

URL: https://juniv.edu/teachers?department_id=41

Submission: On October 04 via manual (October 4th 2024, 2:19:55 pm UTC) — Scanned from CA

Summary

This website contacted **9 IPs** in **2 countries** across **8 domains** to perform **48 HTTP transactions**. The main IP is 72.249.68.156, located in **United States** and belongs to AS17378, US. The main domain is juniv.edu.

TLS certificate: Issued by *R10* on August 19th 2024. Valid for: 3 months.

juniv.edu scanned **17 times** on urlscan.io

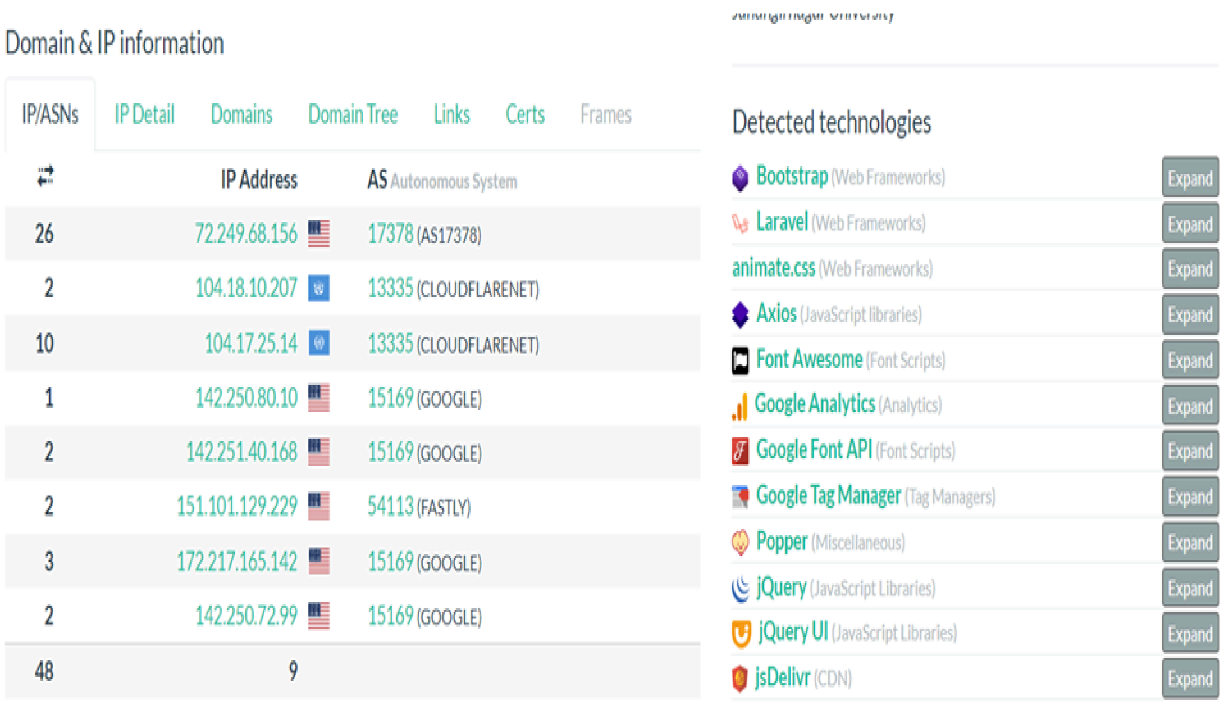
urlscan.io Verdict: No classification ✓

Live information

Google Safe Browsing: ✓ No classification for *juniv.edu*

Current DNS A record: 72.249.68.156 (AS17378 - AS17378, US)

Page Title



Jahangirnagar University

Domain & IP information

⇄	IP Address	AS Autonomous System
26	72.249.68.156	17378 (AS17378)
2	104.18.10.207	13335 (CLOUDFLARENET)
10	104.17.25.14	13335 (CLOUDFLARENET)
1	142.250.80.10	15169 (GOOGLE)
2	142.251.40.168	15169 (GOOGLE)
2	151.101.129.229	54113 (FASTLY)
3	172.217.165.142	15169 (GOOGLE)
2	142.250.72.99	15169 (GOOGLE)
48	9	

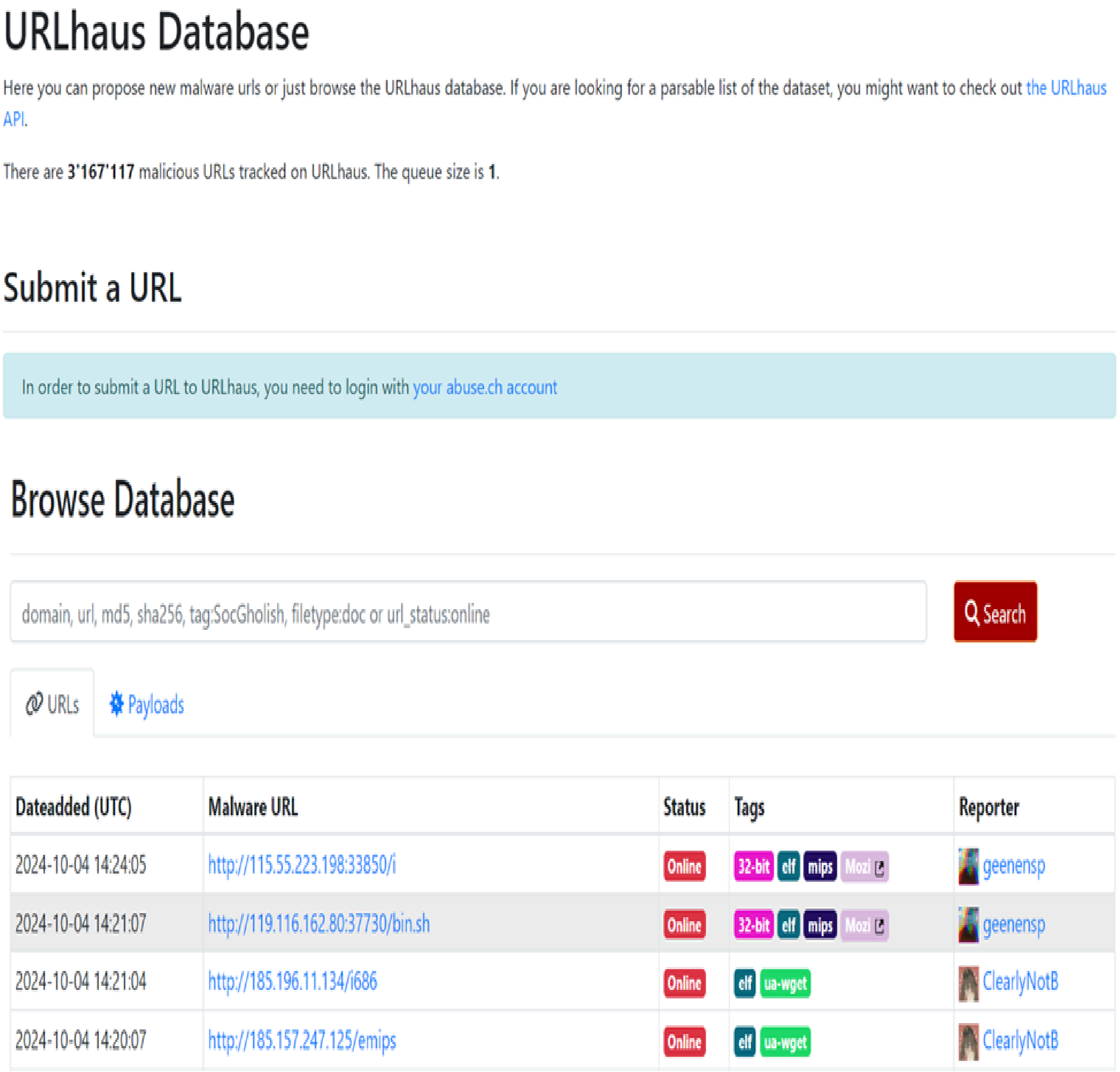
Detected technologies

Bootstrap (Web Frameworks)
Laravel (Web Frameworks)
animate.css (Web Frameworks)
Axios (JavaScript libraries)
Font Awesome (Font Scripts)
Google Analytics (Analytics)
Google Font API (Font Scripts)
Google Tag Manager (Tag Managers)
Popper (Miscellaneous)
jQuery (JavaScript Libraries)
jQuery UI (JavaScript Libraries)
jsDelivr (CDN)

- https://talosintelligence.com/

- https://urlhaus.abuse.ch/browse/

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



URLhaus Database

Here you can propose new malware urls or just browse the URLhaus database. If you are looking for a parsable list of the dataset, you might want to check out the URLhaus API.

There are **3'167'117** malicious URLs tracked on URLhaus. The queue size is **1**.

Submit a URL

In order to submit a URL to URLhaus, you need to login with your abuse.ch account

Browse Database

domain, url, md5, sha256, tag:SocGholish, filetype:doc or url_status:online
Search
URLs
Payloads

Dateadded (UTC)	Malware URL	Status	Tags	Reporter
2024-10-04 14:24:05	http://115.55.223.198:33850/i	Online	32-bit elf mips Mozi	geenensp
2024-10-04 14:21:07	http://119.116.162.80:37730/bin.sh	Online	32-bit elf mips Mozi	geenensp
2024-10-04 14:21:04	http://185.196.11.134/i686	Online	elf ua-wget	ClearlyNotB
2024-10-04 14:20:07	http://185.157.247.125/emips	Online	elf ua-wget	ClearlyNotB

- Assignment: world wide CC tv access

- https://abuse.ch/ à 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
2. https://claude.ai/new

Just search and see:

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