



IT343

Applied Information Assurance

3rd Year, 1st Semester

Lab Report

Passive Information Gathering

Submitted to
Sri Lanka Institute of Information Technology

In partial fulfilment of the requirements for the
Bachelor of Science Special Honours Degree in Information Technology

28/02/2019

Declaration

I certify that this report does not incorporate without acknowledgement, any material previously submitted for a degree or diploma in any university, and to the best of my knowledge and belief it does not contain any material previously published or written by another person, except where due reference is made in text.

Registration Number : IT17122924

Name : Amarapala K.W.N.U.

Table of Contents

Declaration.....	i
List of Figures.....	iii
Chapter 1	1
Information Gathering	1
Introduction.....	1
Active Information Gathering	2
Passive Information Gathering.....	3
Chapter 2	5
Google Hacking Scenario	5
Site: Operator	6
Intitle: Operator	7
Filetype: Operator	8
Index Operator	10
Chapter 3	11
Shodan.io	11
Web Sites Search.....	14
Web cam Search.....	16
TPLink Search.....	19
Router Search.....	21
.....	21

List of Figures

Figure 2. 1: Search Results of Site: operator	6
Figure 2. 2: Search Results of Intitle: operator.....	7
Figure 2. 3: Search Results of Filetype: operator	8
Figure 2. 4: Search results of filetype: operator	9
Figure 2. 5: Excel file type results	9
Figure 2. 6: Search results of Index operator.....	10
Figure 2. 7: Direct download links for the searched file type	10
Figure 3. 1: Shordan.io homepage	11
Figure 3. 2: Shodan Register form.....	12
Figure 3. 3: verification email	12
Figure 3. 4: Shodan Login interface.....	13
Figure 3. 5: Shodan User interface	13
Figure 3. 6: SLT.lk information.....	14
Figure 3. 7: SLT.lk information Detailed information.....	14
Figure 3. 8: Dialog.lk information	15
Figure 3. 9: webcam search results	16
Figure 3. 10:webcam7 information.....	16
Figure 3. 11: webcam7 live recording.....	17
Figure 3. 12: Login pages of webcam7 systems	17
Figure 3. 13: webcam7 alerts.....	18
Figure 3. 14: tplink search results	19
Figure 3. 15: tplink login page.....	19
Figure 3. 16: tplink login page.....	20
Figure 3. 17: tplink accessed information	20
Figure 3. 18: Search results for routers	21
Figure 3. 19: router login page	22

Chapter 1

Information Gathering

Introduction

Information gathering is a process of collecting information about the target and the target's environment.

According to the Penetration Testing Execution Standard (PTES), There are 7 phases of penetration testing. The 7 phases are given below.

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modelling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

Under Intelligence Gathering phase, the pen testers collect as much as information as possible to be utilized when penetrating the target during the vulnerability assessment and exploitation phases.

There are main two types of gathering information,

- Active Information gathering
- Passive Information gathering

Active Information Gathering

Active information gathering is the way of gathering information by directly interacting with the target therefore Contact between the pen tester and the target is established in Active information gathering.

Active information gathering can be detected by the target.

Active Information gathering tools:

- Nmap scan
Nmap scanning Allows to run scans on targeted machines to see what ports are open on them and to see the running applications on them.

Examples to Active information gathering are given below.

- Port scanning for the open ports of the target
- Web application scan
- Vulnerability scan
- Calling the helpdesk of the target and trying to social engineering them

Passive Information Gathering

Passive information gathering is gathering information without directly interacting with the target therefore No contact between the pen tester and the target is established in passive information gathering. Passive information gathering cannot be detected by the target.

Passive information gathering uses publicly published information about the target by using google hacking, tools such as Netcraft, theHarvester etc.

There are so many ways and tools to gather information passively.

- Google hacking
- theHarvester
- Maltego
- The wayback machine
- Job postings
- NetCraft
- Whois
- NSlookup

Google hacking :

Google hacking is a Computer hacking technique that uses Google search and other google applications to find security holes in the configuration and computer code that website uses.

theHarvester :

theHarvester collects emails about targeted domains

Maltego :

Maltego is a data mining tool which helps to get and visualize intelligence gathering/information gathering.

The wayback machine :

This service stores archive copies of over 10 billion websites

Job postings :

Job postings tell the type of devices, software versions etc

NetCraft :

Allows to see detailed information about the web browsers and software and the web host involved with an arbitrary website

Whois

This service can tell information about domain holder, name of mail servers, domain nicknames, type of servers that the target uses.

NSlookup

This service can tell information about domain holder, name of mail servers, domain nicknames, type of servers that the target uses.

Chapter 2

Google Hacking Scenario

Google hacking is a passive information gathering method which uses a search engine to locate a security vulnerability on the internet. Google hacking is use to find security holes in the configuration and computer code that website uses.

Operators are used to search and gather information about the target.

Some operators are given below.

- Site:
- Intitle:
- Filetype:
- Index
- Inurl:
- Allintext:
- Link:
- Inanchor:
- Daterange:
- Numrange:
- Author:
- Group:
- Insubject:
- Allintitle:

Site: Operator

This operator finds the search term only on site specified by the searched term.

The query is given below

Site:lk. Universities

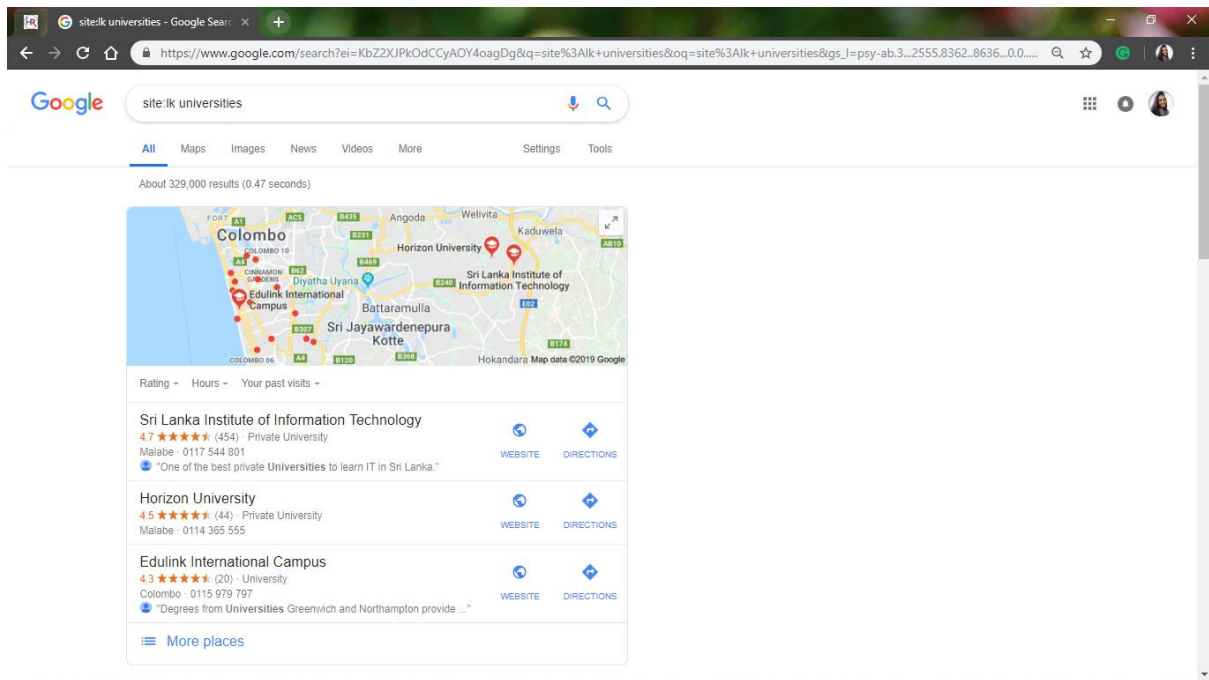


Figure 2. 1: Search Results of Site: operator

As the Figure 2.1 shows, it returns the results from Sri Lankan sites that include the term of “universities” anywhere on the page. An additional search term is required to use with “site:”

Intitle: Operator

The query includes “intitle:”, finds sites which contains searched term in the title of a page.

The query is given below.

Intitle:SLIIT

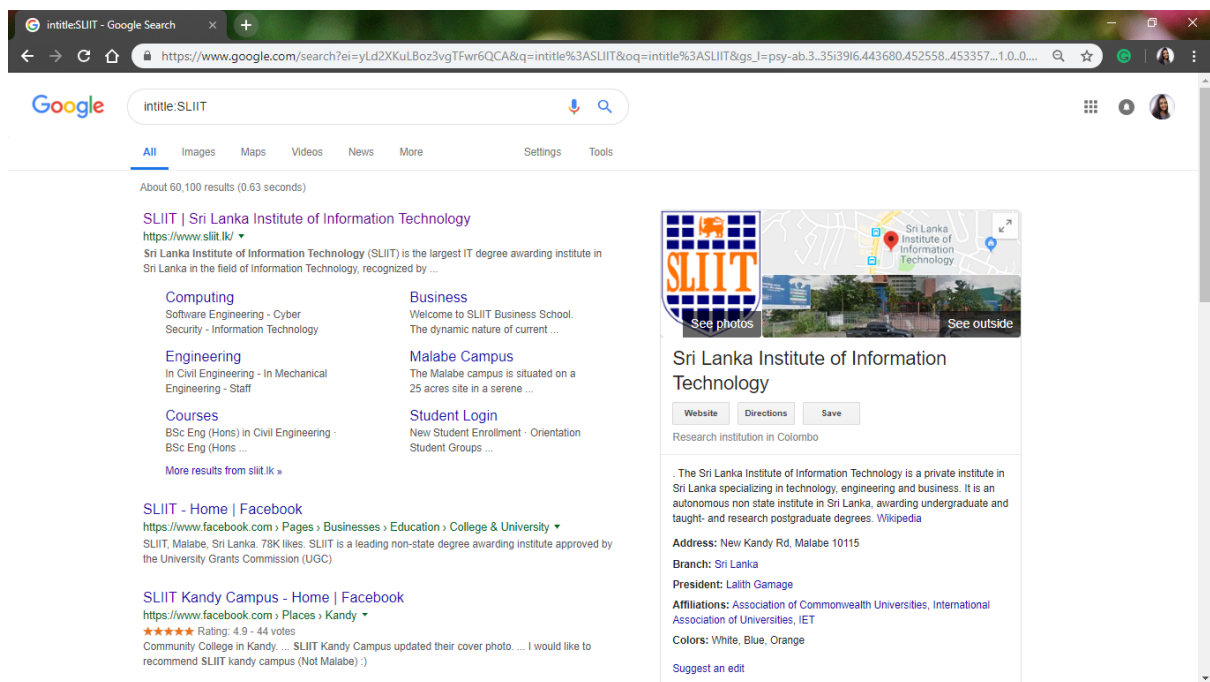


Figure 2. 2: Search Results of Intitle: operator

As the Figure 2.2 shows, it displays only the pages which contain the searched term “SLIIT” in the title.

Filetype: Operator

This gives the search results of files of a specific type only.

Google can search the list of files in the following file types.

pdf, ps, xls, doc, txt, ppt etc.

The query is given below.

filetype:pdf Harry Potter and the Deathly Hallows by J.K.Rowling

The query searches for the “Harry Potter and the Deathly Hallows by J.K.Rowling” word within pdf documents.

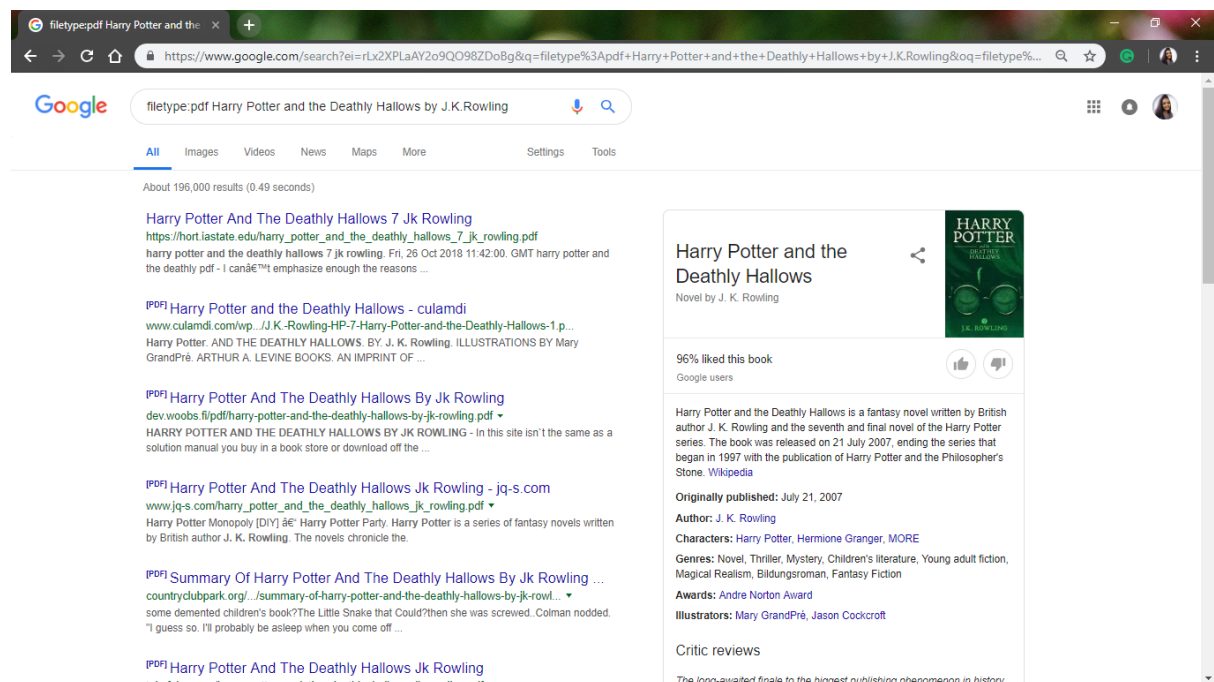
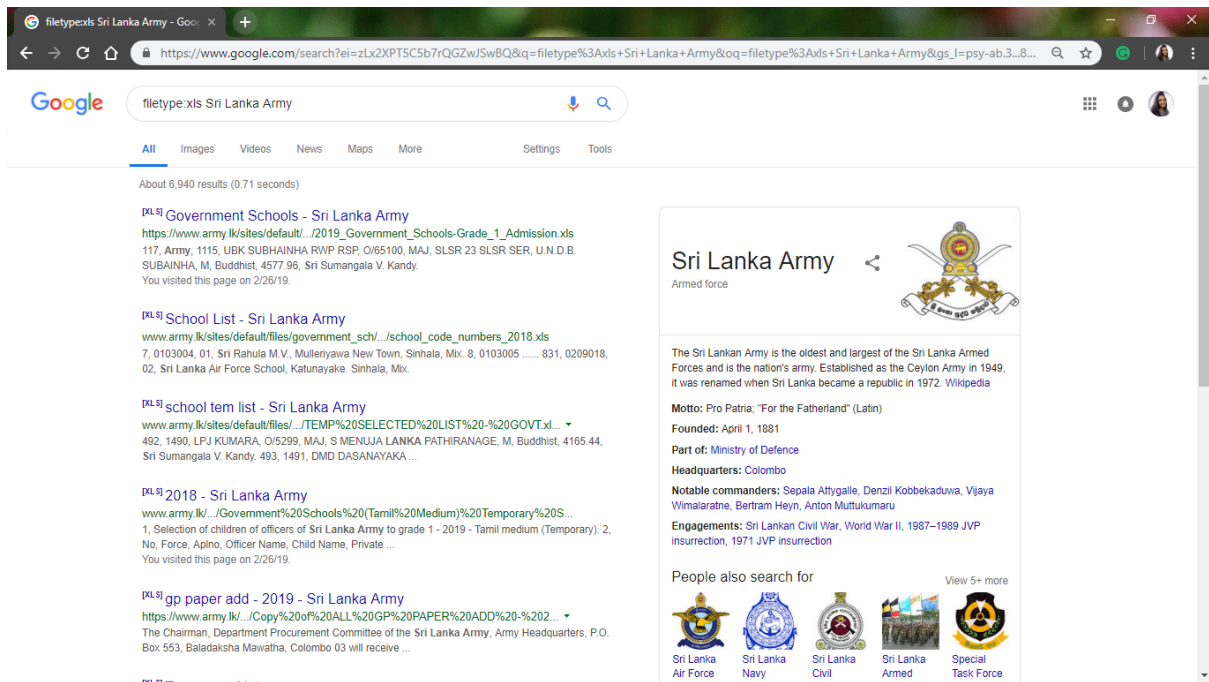


Figure 2. 3: Search Results of Filetype: operator

All the search results are in pdf file type.



Searched term is “Sri Lanka Army”, and all the searched results are in “Excel” file type.

Army ID	Name	Rank	Service Number	Other Details
40 Army 1038	BGR KUMARASINGHE	O/67690	CAPT	SLA 8 SLA SER
41 Army 1039	G DAYARATHNA USP	O/69790	LT(QM)	SLA 10 SLA SER
42 Army 1040	DKSK DOLAGE USP psc	O/61731	COL	SLE SLE SER
43 Army 1041	WANS PERERA USP	O/61878	COL	SLE SLE SER
44 Army 1042	SDPC ARACHCHIGE	O/62362	LT COL	SLE 14 SLE SER
45 Army 1043	EJAS ASSADDUMEGEDARA psc	O/63269	MAJ	SLE 5 SLE SER
46 Army 1044	RDS WIJETHUNGA	O/64036	MAJ	SLE 12 SLE SER
47 Army 1045	PGPA WIJERATHNE RSP	O/64047	MAJ	SLE 5 SLE SER
48 Army 1046	JLN SILVA RSP	O/64540	MAJ	SLE 1 SLE SER
49 Army 1047	WKST KANNANGARA psc	O/64761	MAJ	SLE 9 SLE SER
50 Army 1048	MAPS PERERA	O/65022	MAJ	SLE 14 SLE SER
51 Army 1049	DG THILAKARATHNA RSP	O/65361	MAJ	SLE 9 SLE SER
52 Army 1050	WDDN WEERASINGHE psc	O/65632	MAJ	SLE 1 SLE SER
53 Army 1051	AAD ABEYSINGHE	O/65727	MAJ	SLE 8 SLE SER
54 Army 1052	HKMNK KALUMULLAGE	O/65830	MAJ	SLE 5 SLE SER
55 Army 1053	GAI GODEWATTA RSP	O/65843	MAJ	SLE 5 SLE SER
56 Army 1054	MJ SALGADU RSP	O/65861	MAJ	SLE 14 SLE SER
57 Army 1055	CR LAHANDASINGHE psc	O/65165	MAJ	SLE 1 SLE SER
58 Army 1056	HMS HERATH psc	O/66184	MAJ	SLE 12 SLE SER
59 Army 1057	MDCD MARAMBAGE psc	O/66300	MAJ	SLE 1 SLE SER
60 Army 1058	UA CHANDRASIRI	O/66449	CAPT	SLE 1 SLE SER
61 Army 1059	NML BANDARA	O/66695	CAPT	SLE 1 SLE SER
62 Army 1060	KM WIJESINGHE	O/66710	CAPT	SLE 1 SLE SER
63 Army 1061	KHAUK JAYASINGHE	O/66720	CAPT	SLE 5 SLE SER
64 Army 1062	LMJ SUDARSHANA RSP	O/66482	LT	SLE 5 SLE SER
65 Army 1063	S JAYASINGHE	O/69244	LT(QM)	SLE 1 SLE SER
66 Army 1064	MKGSK PADMASIRI USP	O/70158	LT(QM)	SLE 12 SLE SER
67 Army 1065	BD FERNANDO USP psc	O/62453	LT COL	SLSC 4 SLSC SER

Figure 2. 5: Excel file type results

Figure 2.5 shows the excel sheet which is downloaded by the search results of the query “Filetype:xls Sri Lanka Army”

Index Operator

The query “Index of mkv high school musical” gives the searched results in mkv file type.

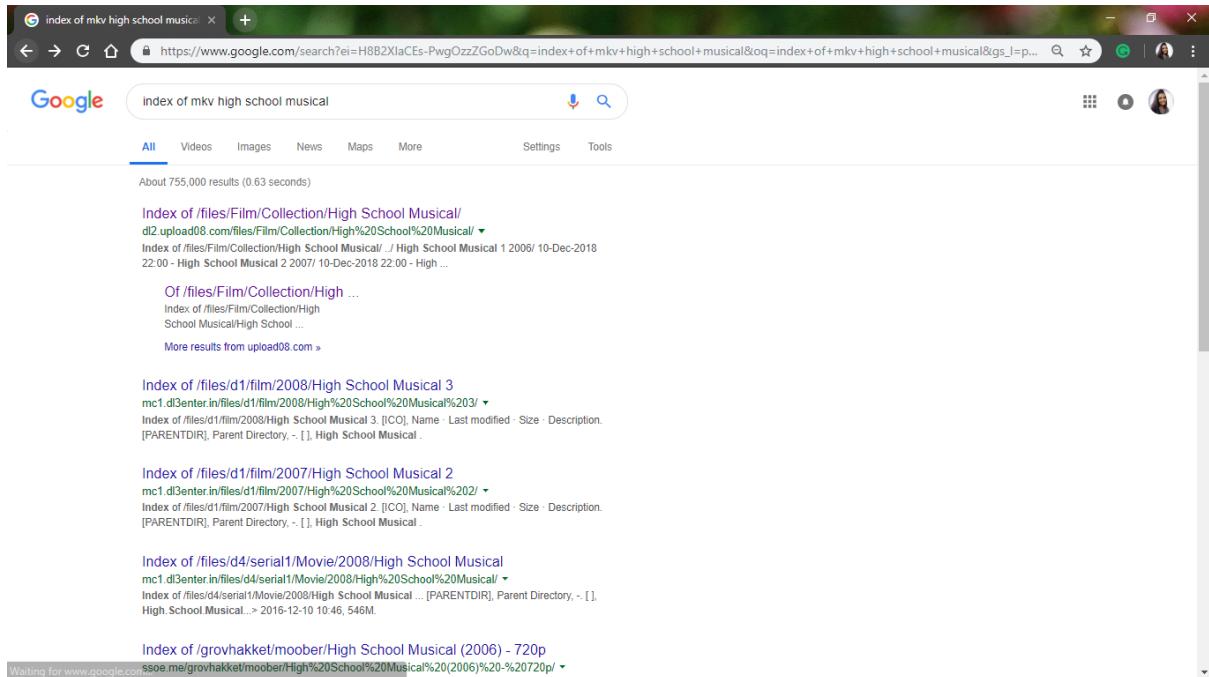


Figure 2. 6: Search results of Index operator

This directs to a page with direct downloadable links of the given file type.

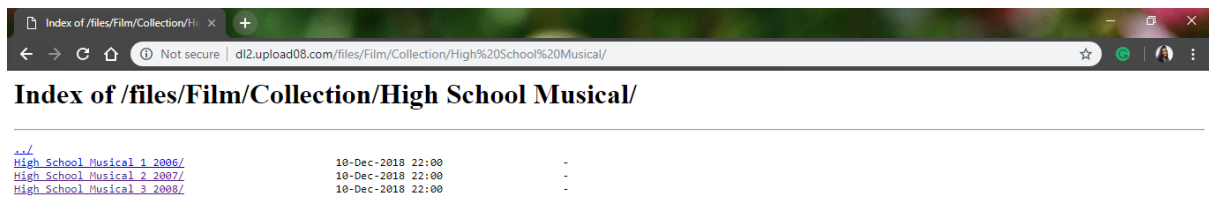


Figure 2. 7: Direct download links for the searched file type

Chapter 3

Shodan.io

Shodan is a search engine.

Go to the link given below. If you are a new user, Create a new account to register.

<https://www.shodan.io/>

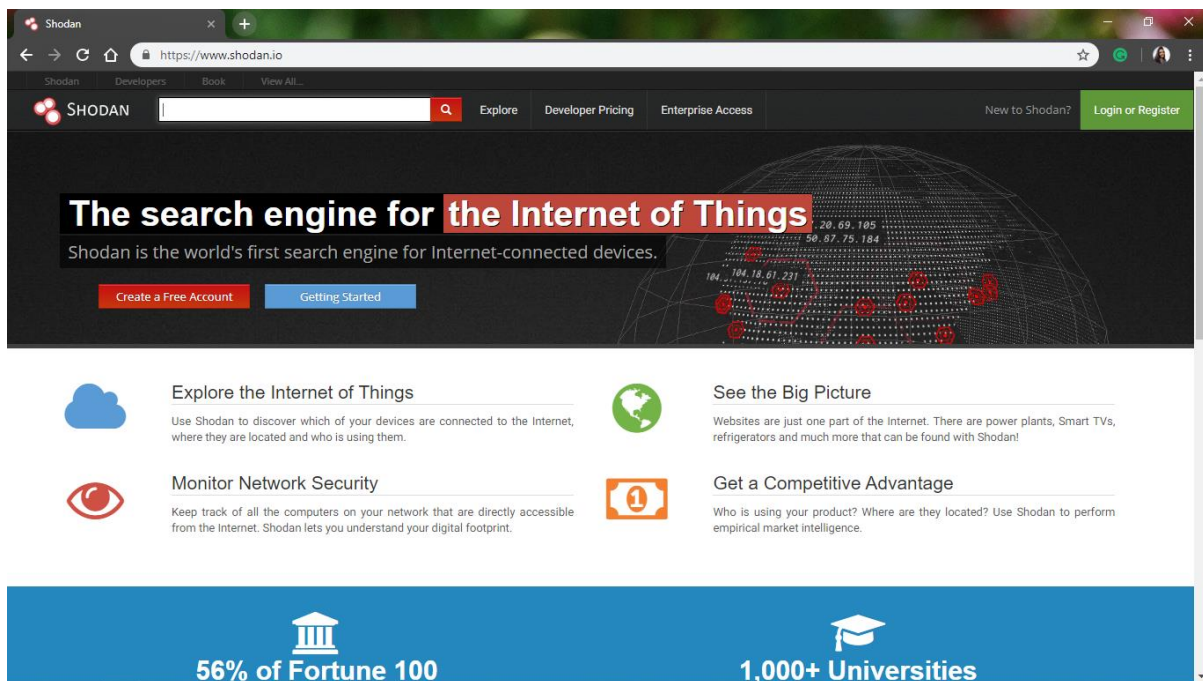


Figure 3. 1: Shordan.io homepage

Click [Login or Register] button to register

Shodan - Account Management

https://account.shodan.io/register

Error: Please check the form and fix any errors.

Create Account

Username
Niki_niko

That username already exists.

Password

Confirm Password

Email
kwnikiniamarapala@gmail.com

☐ Subscribe to the newsletter

By creating an account you are agreeing to our [Privacy Policy](#) and [Terms of Use](#)

CREATE

Figure 3. 2: Shodan Register form

Fill the form and click [Create] button to register.

An account activation email will be sent to your email afterwards.

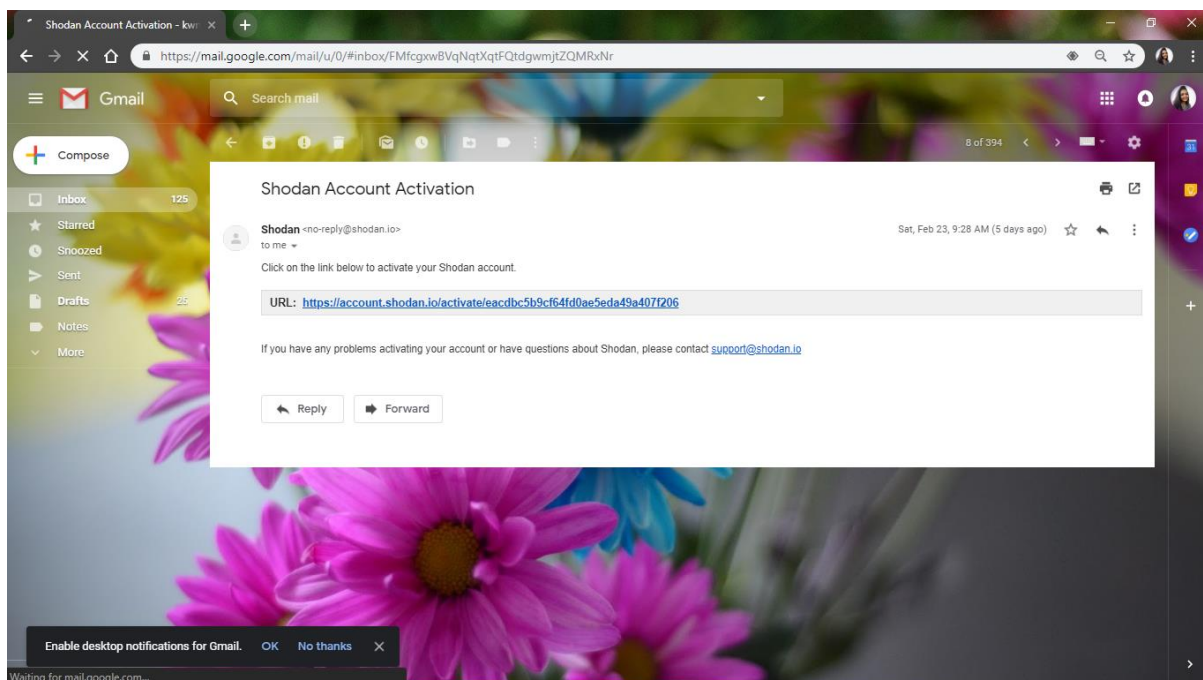


Figure 3. 3: verification email

After verifying the details, you will get the user interface of your “Shodan” account.

If you are a current user of Shodan, then click [Login or Register] button to log in to the account.

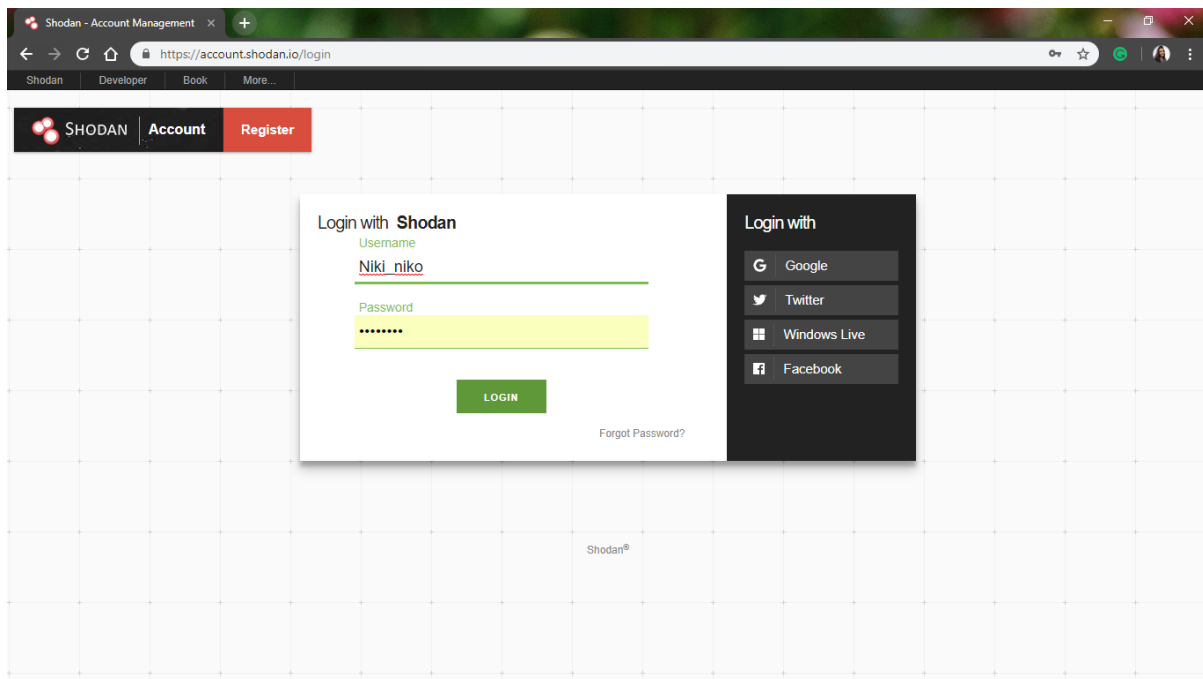


Figure 3. 4: Shodan Login interface

After clicking [Login], You will get the user interface of your “Shodan” account.

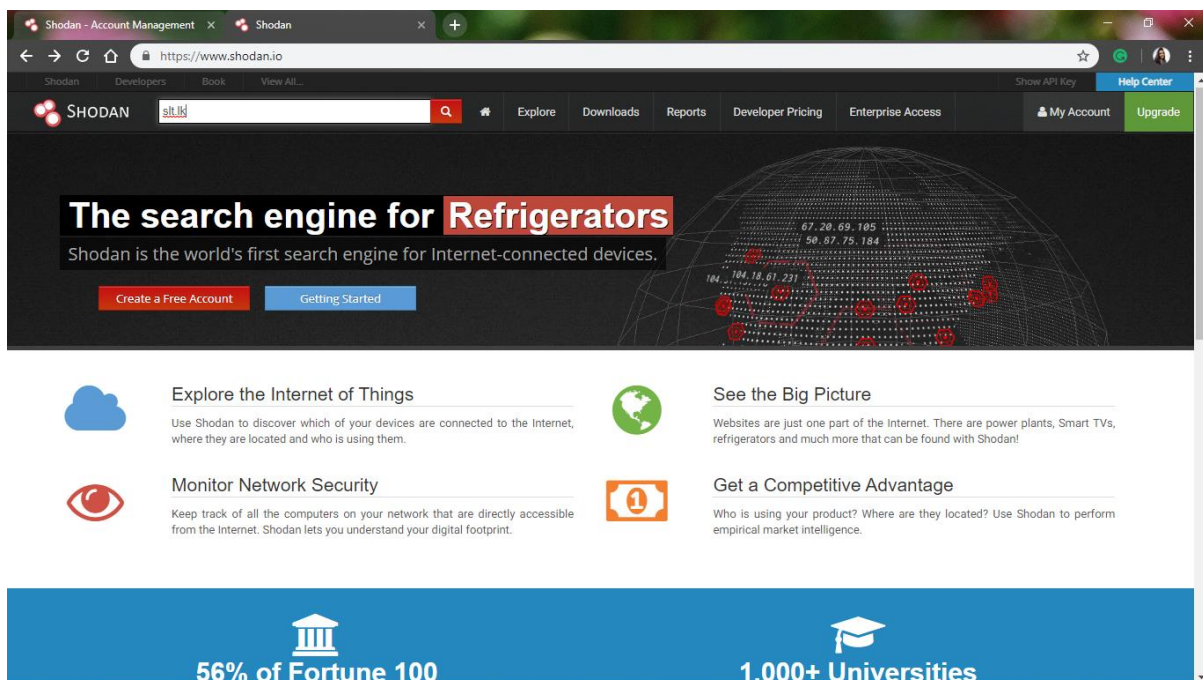
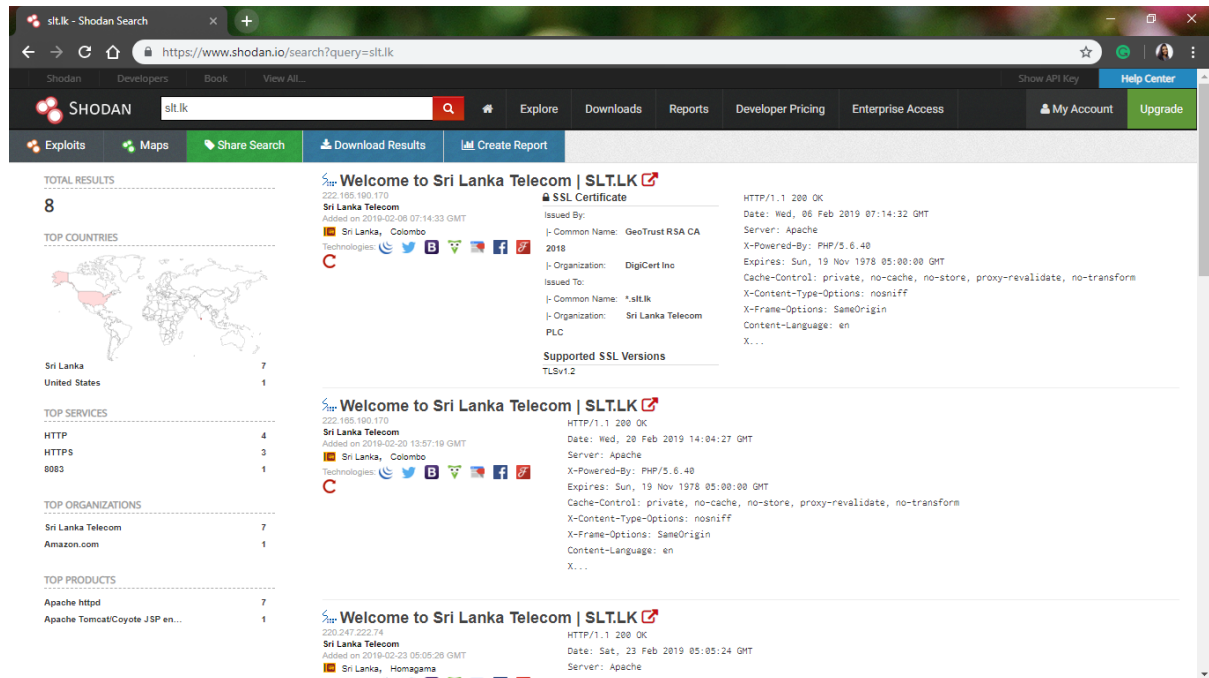


Figure 3. 5: Shodan User interface

Web Sites Search

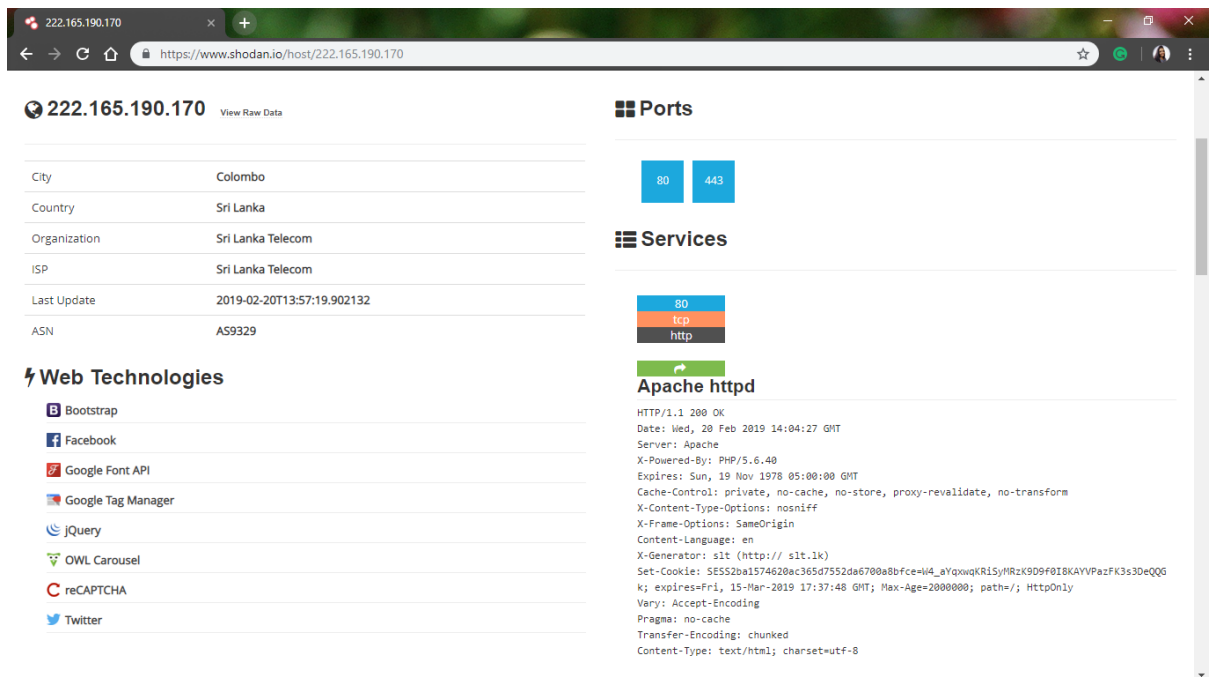
Type “slt.lk” on the search bar in order to get a detailed page of slt.lk information.



The screenshot shows the Shodan search interface with the query "slt.lk". The results page displays a summary of 8 total results, with a map showing the top countries (Sri Lanka and United States) and a list of top services (HTTP, HTTPS, 8083). The main content area shows the first result, "Welcome to Sri Lanka Telecom | SLT.LK", which includes an SSL certificate details, supported SSL versions, and a list of top products (Apache httpd, Apache Tomcat/Coyote JSP en...).

Figure 3. 6: SLT.lk information

In there, all the details about the servers, ip addresses etc can be found.



The screenshot shows the Shodan host details page for the IP address 222.165.190.170. The page displays a table of host information (City, Country, Organization, ISP, Last Update, ASN) and a list of web technologies (Bootstrap, Facebook, Google Font API, Google Tag Manager, jQuery, OWL Carousel, reCAPTCHA, Twitter). The "Ports" section shows 80 and 443. The "Services" section shows 80, tcp, and http. The "Apache httpd" section shows the server version (HTTP/1.1 200 OK) and various headers (Date, Server, X-Powered-By, Expires, Cache-Control, X-Content-Type-Options, X-Frame-Options, Content-Language, X-Generator, Set-Cookie, Vary, Pragma, Transfer-Encoding, Content-Type).

Figure 3. 7: SLT.lk information Detailed information

When we consider “dialog.lk”, all the information is only can accessed by authorized personnel only.

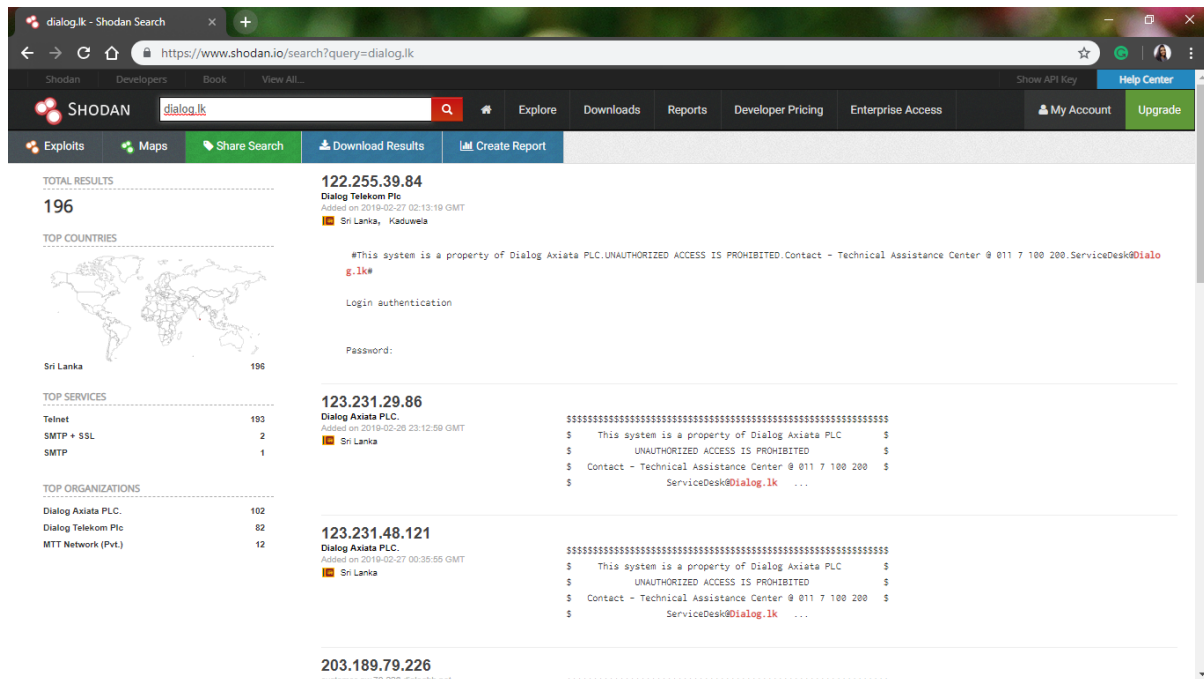


Figure 3. 8: Dialog.lk information

Web cam Search

Type “Web cam 7” in the search bar.

The screenshot shows the Shodan search engine interface. The search bar contains 'web cam 7'. The results page displays 20 total results. On the left, there are filters for 'TOP COUNTRIES' (United States: 7, Italy: 2, United Kingdom: 2, France: 2, Viet Nam: 1) and 'TOP SERVICES' (Synology: 8, HTTPS: 5, 8083: 3, 8001: 1, Qconn: 1). Below these are 'TOP ORGANIZATIONS' (MOJOHOST: 4, Orange: 2, WiMore S.r.l.: 1, Virgin Media: 1). The main results list shows two entries:

- 199.182.110.186** (MOJOHOST, United States, Farmington):
 - Added on 2019-02-20 11:26:00 GMT
 - HTTP/1.1 200 OK
 - Date: Wed, 20 Feb 2019 12:27:13 GMT
 - Server: Apache
 - X-Powered-By: PHP/5.6.19
 - Vary: User-Agent, Accept-Encoding
 - Cache-Control: max-age=600, private, proxy-revalidate
 - Transfer-Encoding: chunked
 - Content-Type: text/html; charset=UTF-8
- 82.21.179.118** (Virgin Media, United Kingdom, Reading):
 - Added on 2019-02-20 07:29:00 GMT
 - HTTP/1.1 200 OK
 - Content-Length: 8968
 - Vary: Accept-Encoding
 - Server: TornadoServer/4.1
 - Etag: "03e8fa942661e69a2f885fda824b79e078788560"
 - Date: Wed, 20 Feb 2019 07:18:07 GMT
 - Content-Type: text/html; charset=UTF-8

Figure 3. 9: webcam search results

Click on the IP address links to go to their information pages.

The screenshot shows the Shodan host information page for IP address 109.206.96.230. The page features a satellite map of Belgrade, Serbia, with a red pin indicating the location. Below the map, the host information is displayed:

- 109.206.96.230** (View Raw Data)
- City: Belgrade
- Country: Serbia
- Organization: TRUF d.o.o.
- ISP: TRUF d.o.o.
- Last Update: 2019-02-26T18:48:21.478762
- ASN: AS52026

On the right side, there are sections for 'Ports' (8080) and 'Services' (webcam 7 httpd). The 'Services' section shows the following details:

- 8080 tcp http-simple-new
- HTTP/1.1 200 OK
- Connection: close
- Content-Type: text/html; charset=utf-8
- Content-Length: 7569
- Cache-control: no-cache, must revalidate
- Date: Tue, 26 Feb 2019 18:49:17 GMT
- Expires: Tue, 26 Feb 2019 18:49:17 GMT
- Pragma: no-cache
- Server: webcam 7

Figure 3. 10:webcam7 information

Go to the IP address to get the access to the selected webcam7.

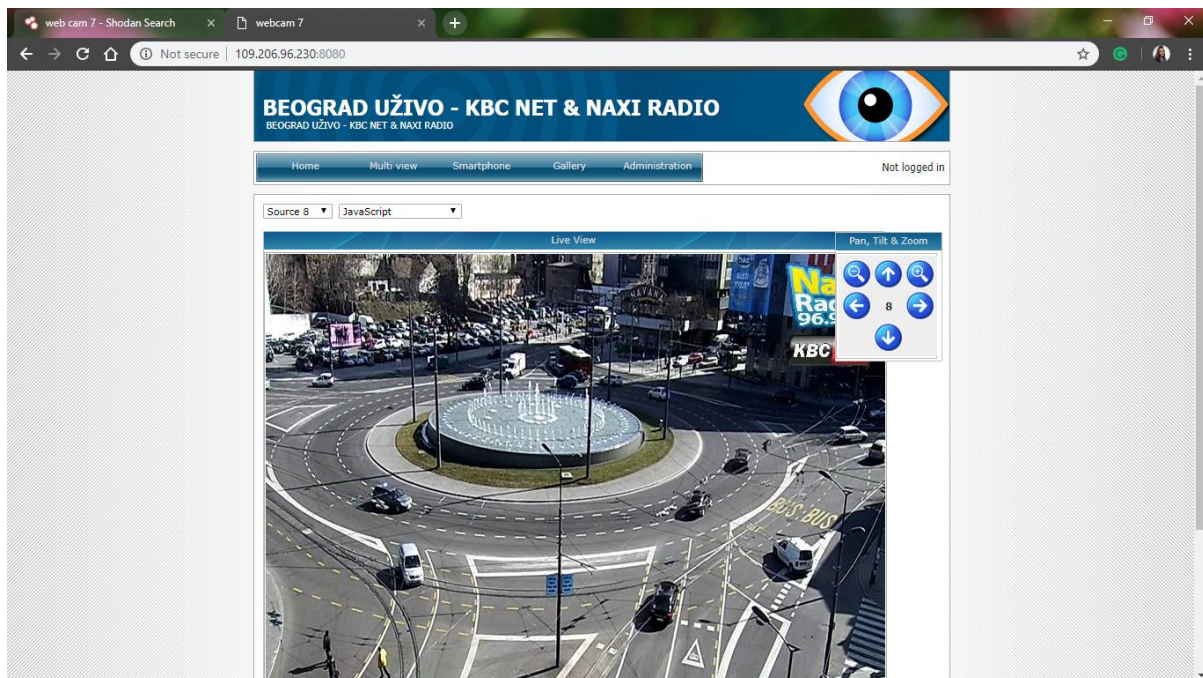


Figure 3. 11: webcam7 live recording

You will be directly directed to the live recording of the webcam7 in IP address 109.206.96.230:8080

Some webcam7 system require the username and password to get the access.

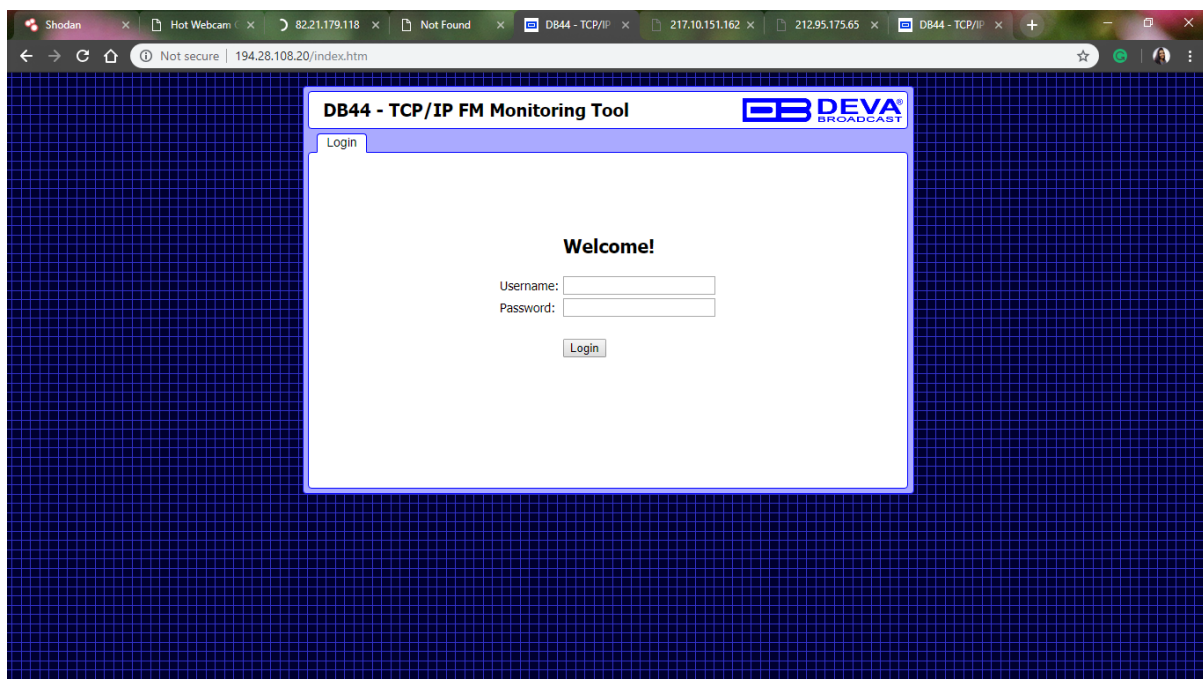
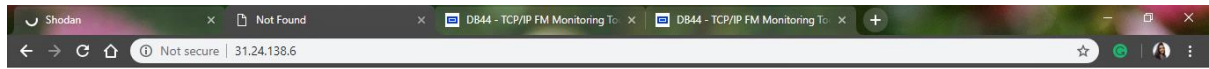


Figure 3. 12: Login pages of webcam7 systems

Some webcam7 systems do not give the access even to load the login page.



Not Found

HTTP Error 404. The requested resource is not found.

Figure 3. 13: webcam7 alerts

TPLink Search

Type “tplink” in the search bar.

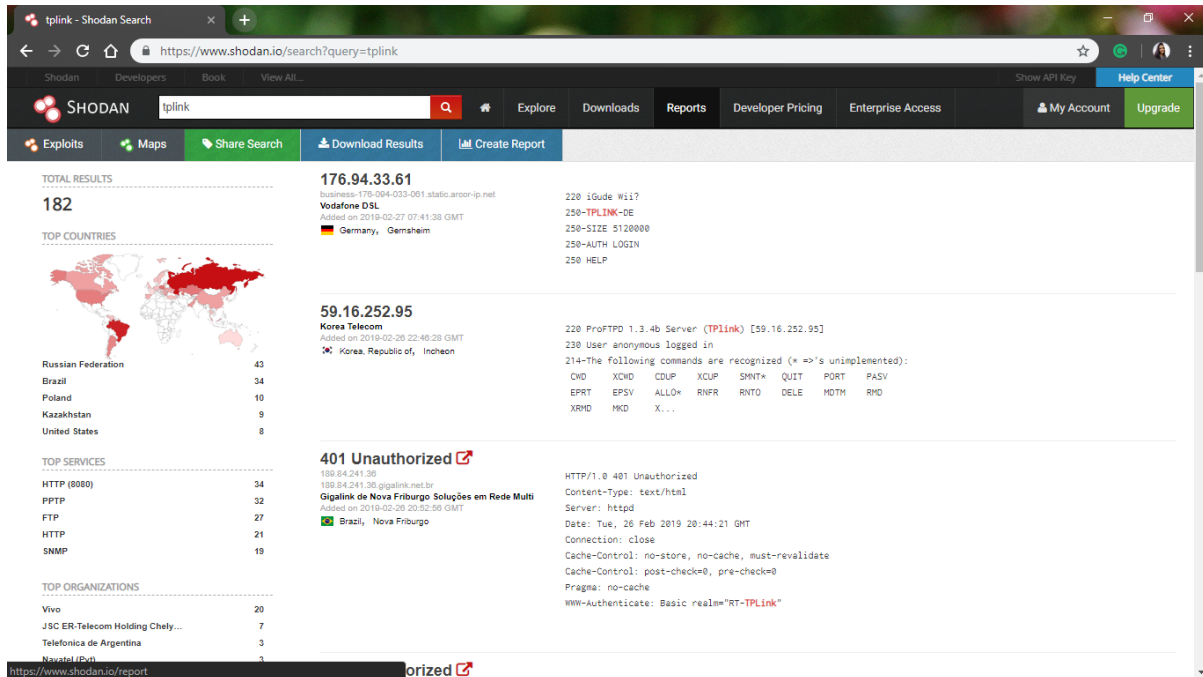


Figure 3. 14: tplink search results

Click on a link to get access to a tplink.

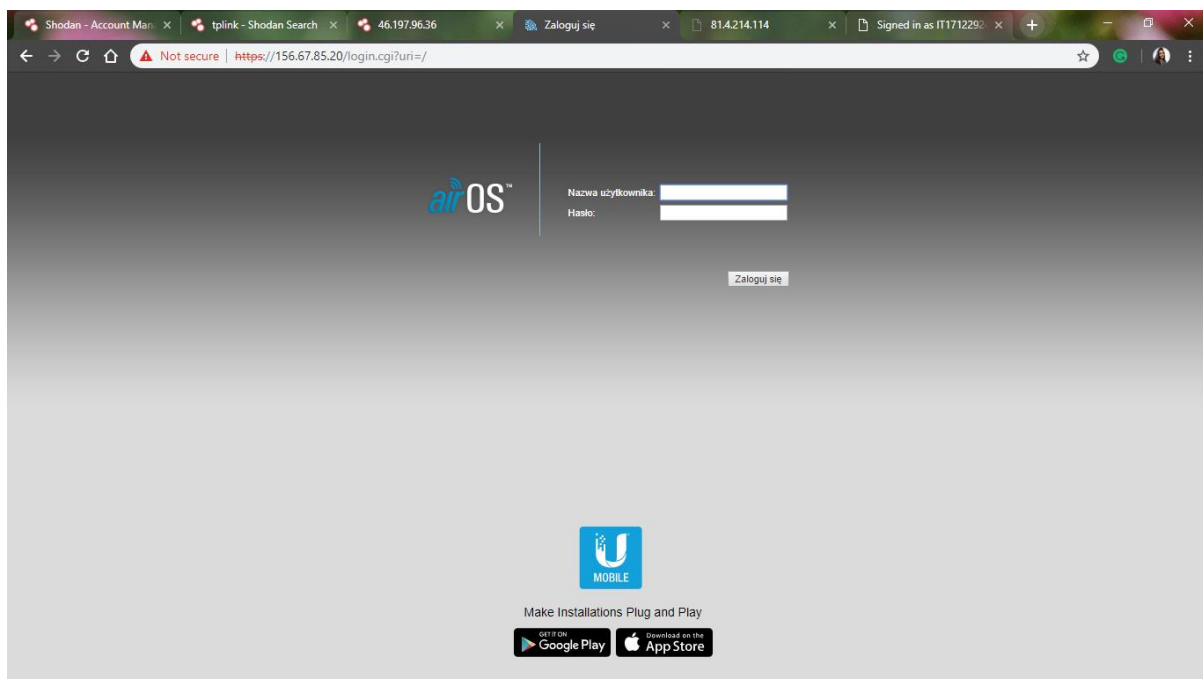


Figure 3. 15: tplink login page

Some IP addresses may direct to a login page.

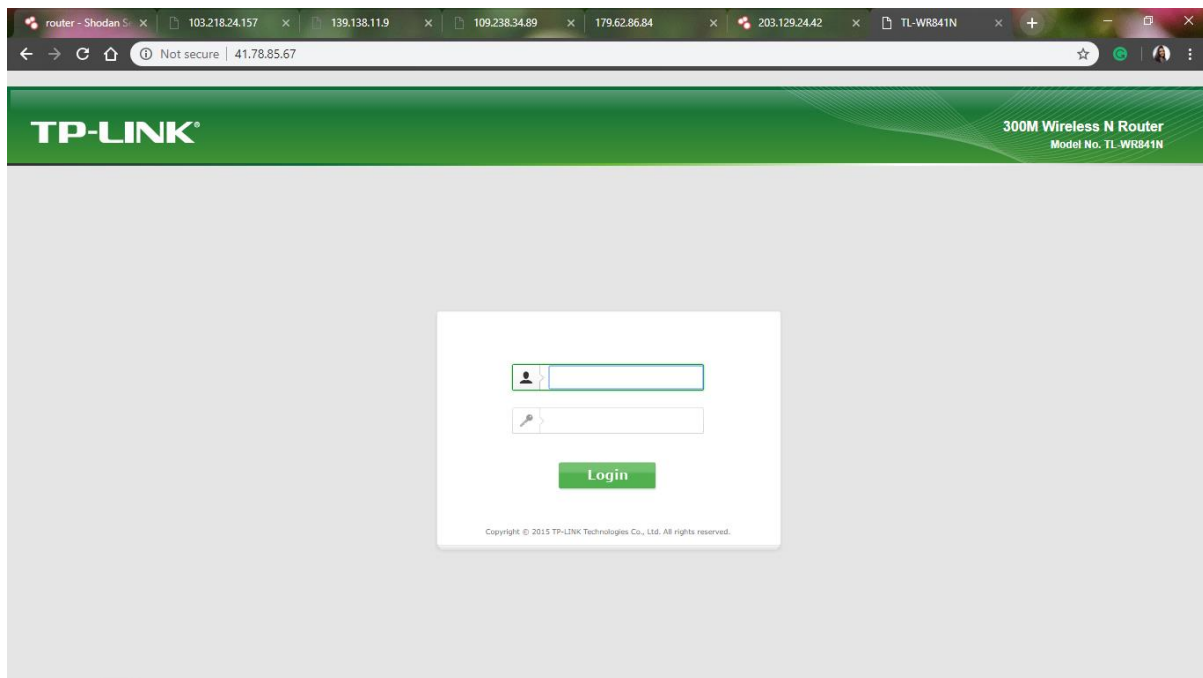


Figure 3. 16: tplink login page

Try some paddwords and user names for those.

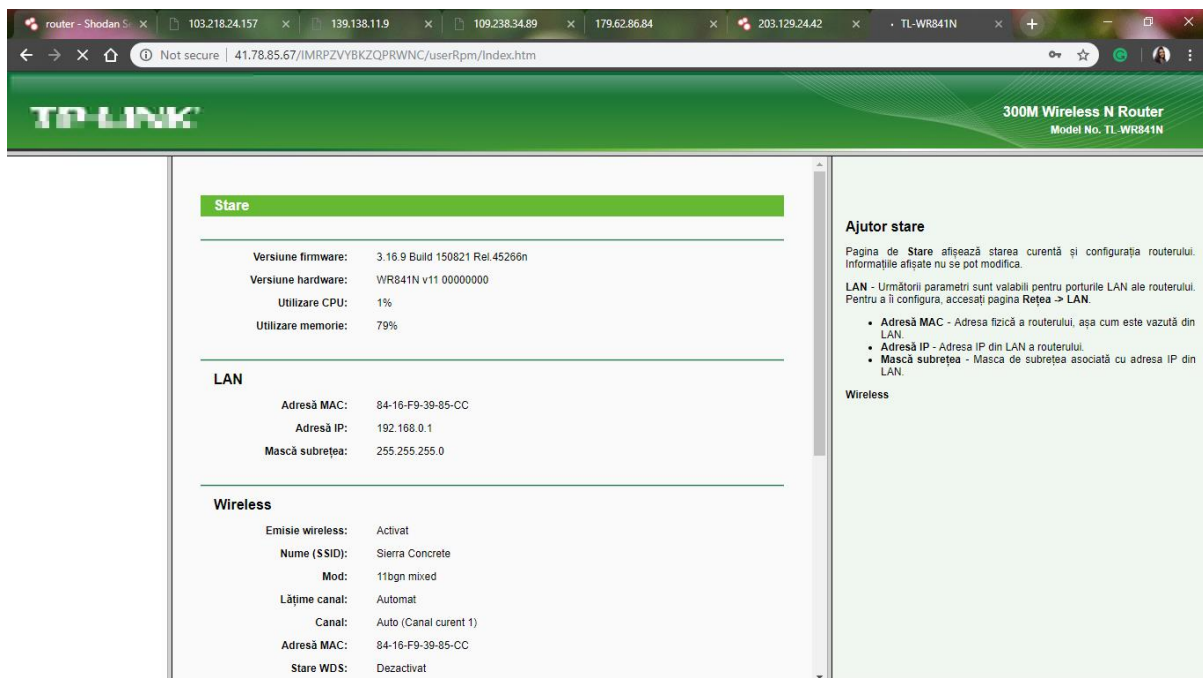


Figure 3. 17: tplink accessed information

Try the following login credentials for the tplink which holds the ip number 41.78.85.67

Username: admin

Password: admin

You will be directed to a page contains all its information.

Router Search

Search for “Routers”.

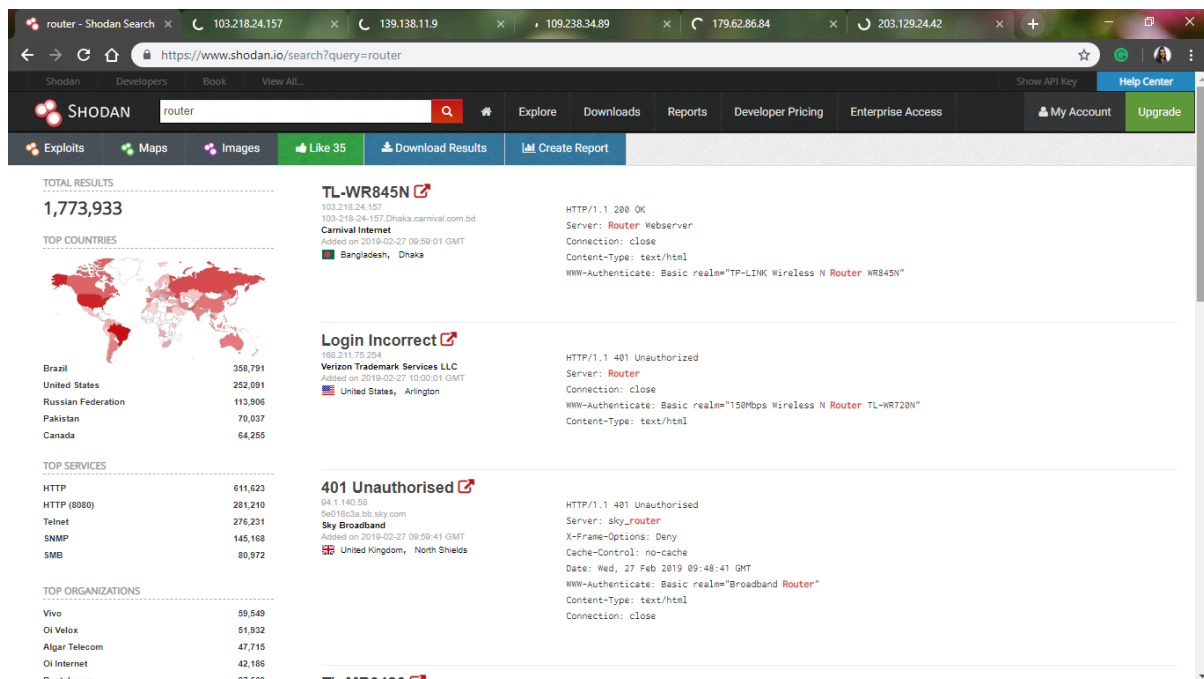


Figure 3. 18: Search results for routers

Click on a link inorder to get its page.

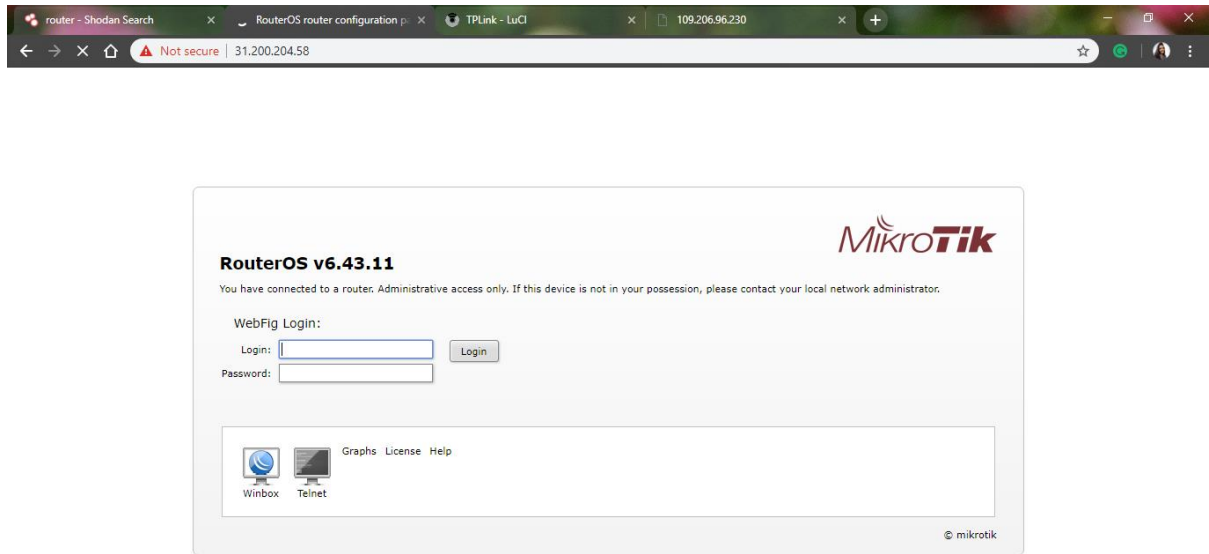


Figure 3. 19: router login page