

# “VIDYALANKAR SCHOOL OF INFORMATION TECHNOLOGY, WADALA”

**AFFILIATED TO UNIVERSITY OF MUMBAI**

# CENTRE FOR DISTANCE AND ONLINE EDUCATION (CDOE)

**Ethical Hacking**

**SUBMITTED BY**

**Omkar Balu Auti**

**Application No.: 129457**

**SUBMITTED IN PARTIAL FUFILLMENT OF THE REQUIREMENTS FOR QUALIFYING MCA PART-II (SEMISTER- III) EXAMINATION**

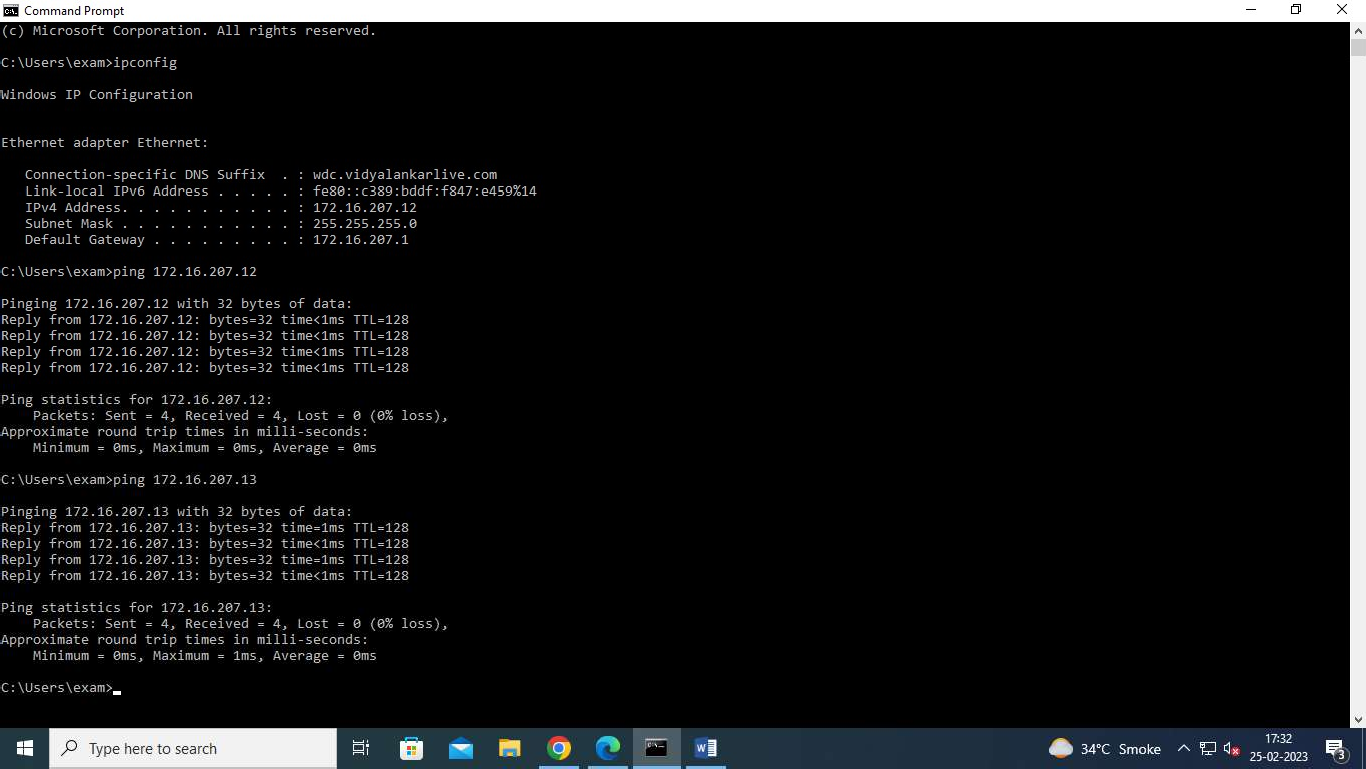
**2023 - 2024**

# INDEX

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr.**  **No.** | **Practical Name** | **Date** | **Signature** |
| 1 | BASIC COMMANDS |  |  |
| 2 | SCANNING NETWORKS AND SNIFFING |  |  |
| 3 | USING CRYPTOOL TO ENCRYPT AND DECRYPT PASSWORD USING RC4 ALGORITHM |  |  |
| 4 | DEVELOPING AND IMPLEMENTING MALWARES |  |  |
| 5 | HACKING WEB SERVERS, WEB APPLICATIONS |  |  |
| 6 | SQL INJECTION |  |  |
| 7 | CREATE A CIPHER USING CRYPTOOL |  |  |
| 8 | IMPLEMENT ENCRYPTION AND DECRYPTION USING CEASER CIPHER |  |  |

1. **Basic Commands**

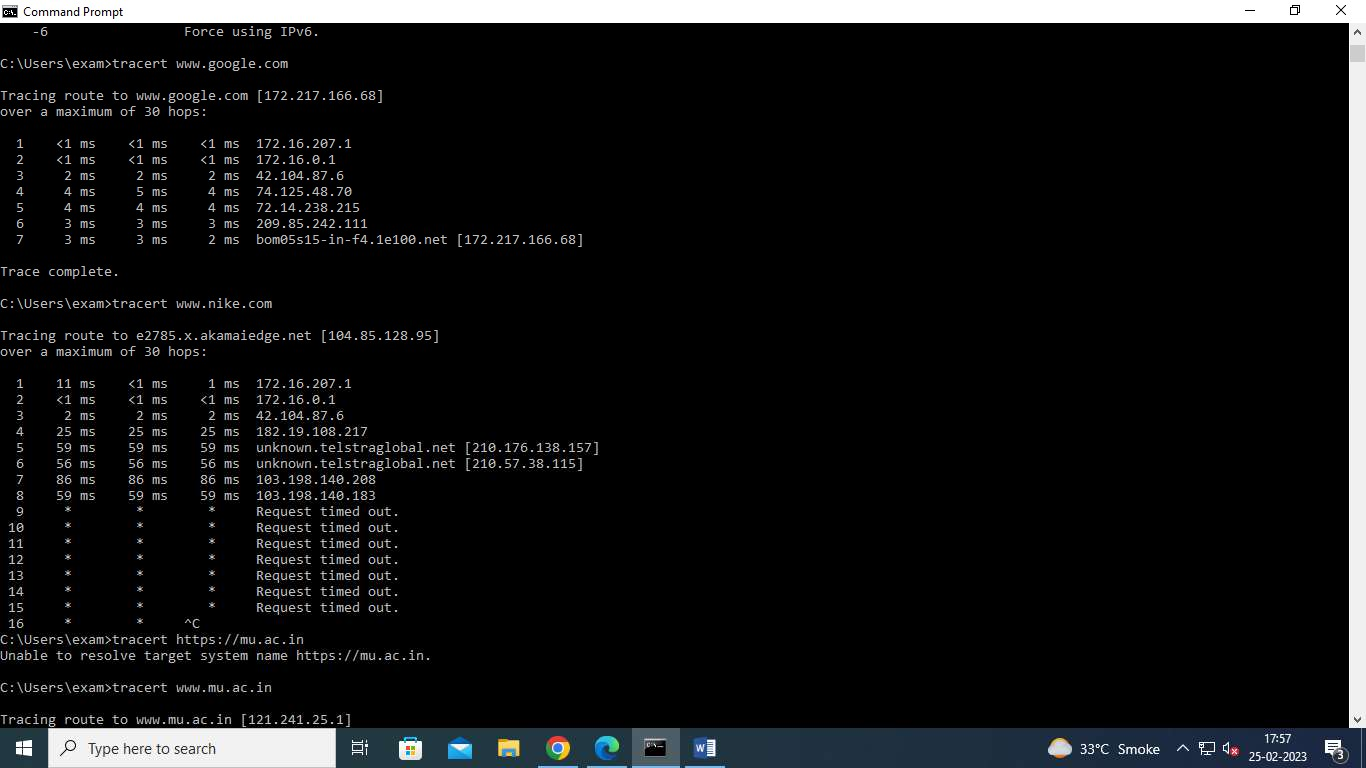
-ipconfig-



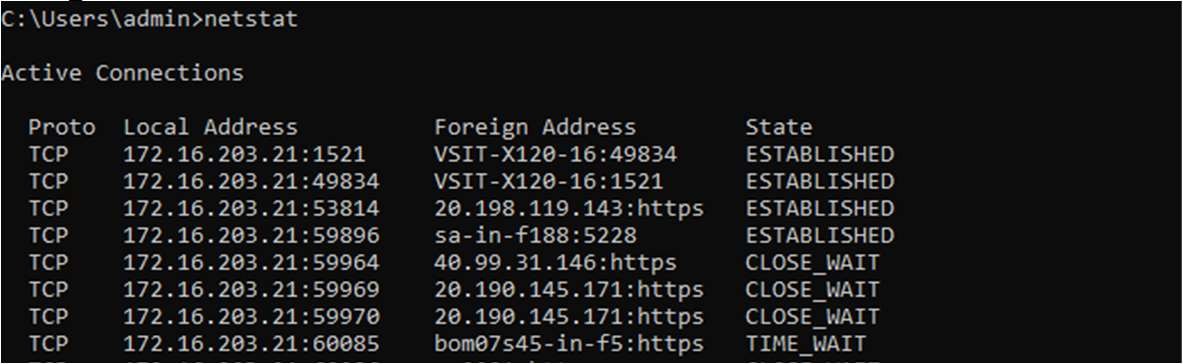
-ping



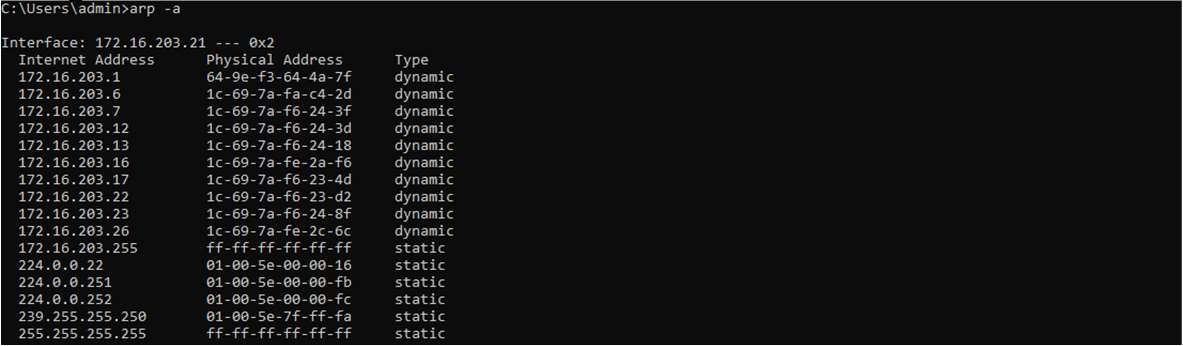
-tracert



**Step 4:- run netstat**



**Step 5:- run ARP command**



# WEBSITE INFORMATION

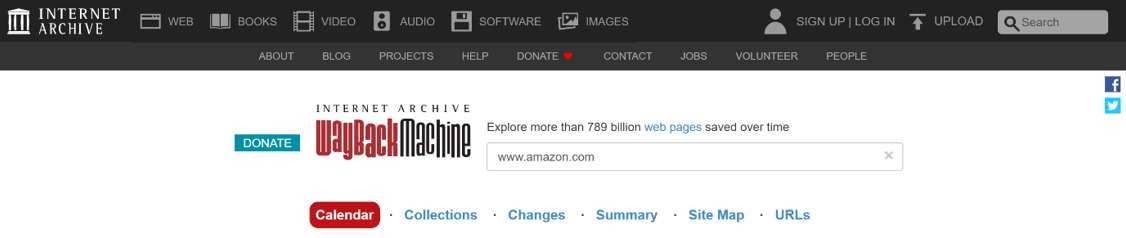
Website foot printing is the technique which is used to extract the details related to website. When we are browsing any website or any target website, we may provide this information

When hacker or any user wants to archived website or history of website, they can use www.archieve .org

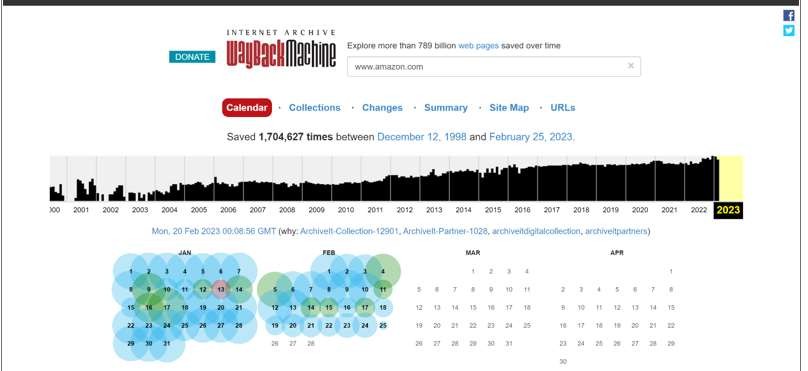
**Step 1:** Type [www.archieve.org](http://www.archieve.org/) in Google

**Step 3:** You can enter Domain name in the search box.

**Step 4:** Suppose we want to check for Amazon, so we entered the search box.



**Step 5:** For how the website was looking and are the pages are present on that website with different dates.



# TO TRACE ANY RECEIVED EMAIL

**Step1:** Type in google email Tracker pro download.Then click button to download emailtrackerPro.

**Step2:** Click on next button

**Step3:** Choose the components**.**

**Step4:** By clicking on finish button, finish the installation.

**Step5:** After the completion of installation add your email address by clicking on sign up button.

**Step6:** Fill this information.

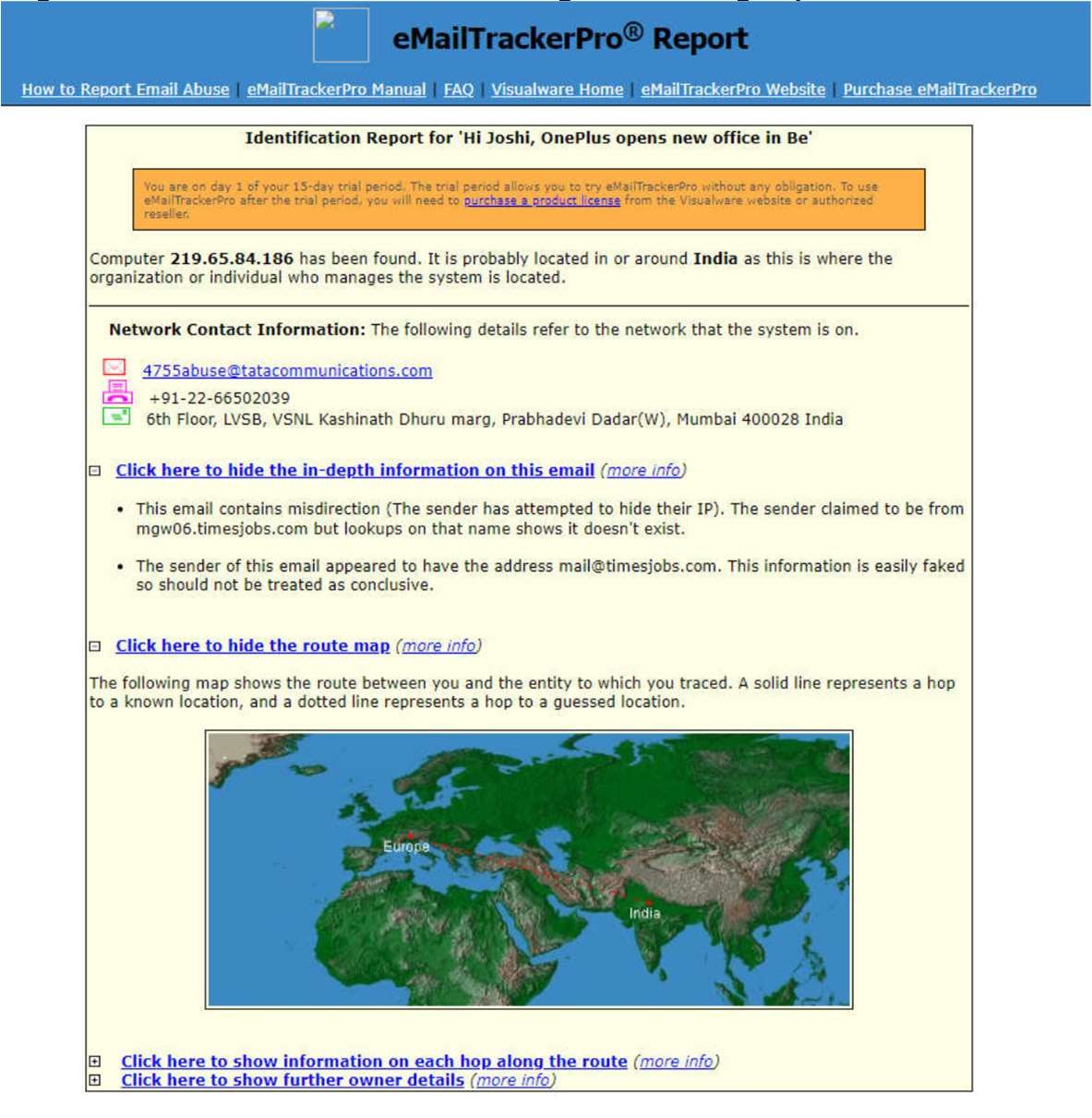
**Step7:** Now open any email that you want to trace and click on three dots and select show original message and copy the message in clipboard.

**Step8:** Now click on trace header button its display below window.

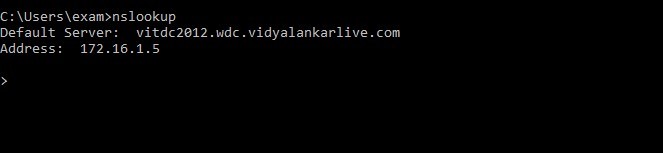
**Step9:** Now paste original message in the email headers section.

**Step10:** Click on Trace button.

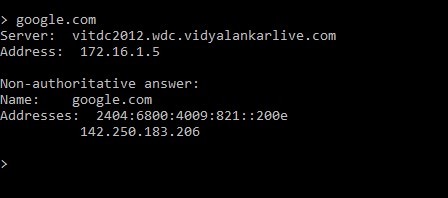
**Step11:** To view report click the button view report it displays all information.



**NS Lookup:**

**Step 1:** Type nslookup command in cmd

**Step 2:** For example, we put google.com it displays below information.

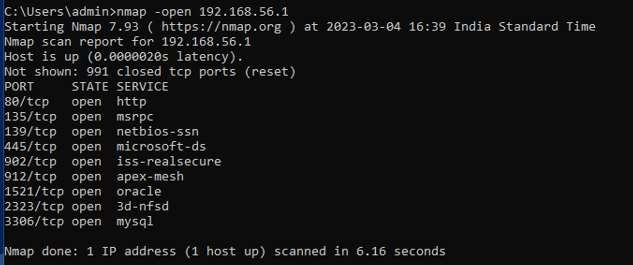


1. **Performing Port scanning using Nmap tool.**

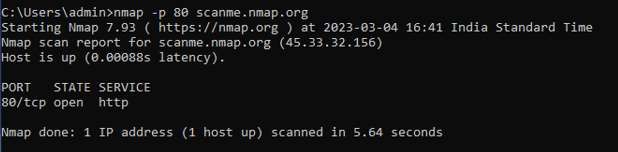
**Nmap Tool:** Nmap is a free, open source and multi-platform network security scanner used for network discovery and security auditing. Nmap can be extremely useful for helping you get to the root of the problem you are investigating, verify firewall rules or validate your routing tables are configured correctly.

1. Scan open ports (syntax: nmap –open ip\_address / url )

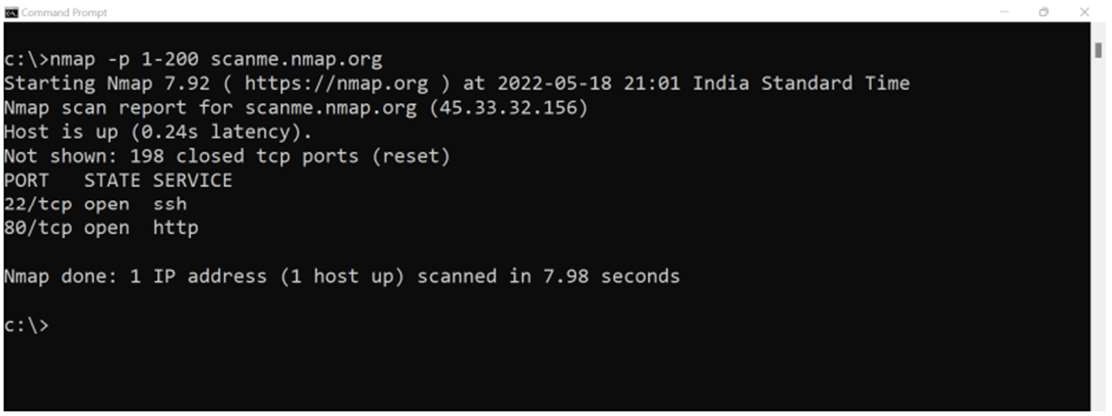


Scanning port with the IP Address.

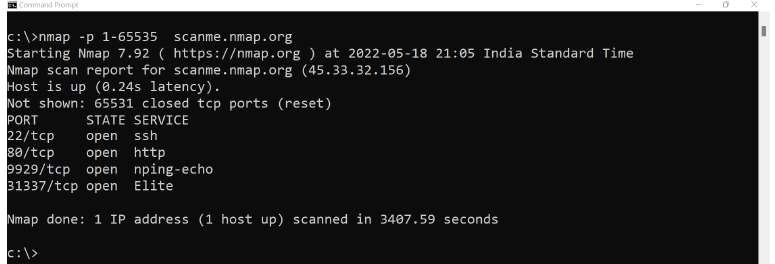
1. Scan single port (syntax: nmap -p 80 ip\_address)



1. Scan specified range of ports (syntax: nmap -p 1-200 ip\_address)



1. Scan entire port range (syntax: nmap -p 1-65535 ip\_address)



1. Scan top 100 ports (fast scan) (syntax: nmap -F ip\_address )



**Aim:** Performing Network scanning using Nmap tool.

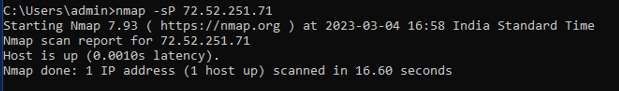
**Ping Scan**

Syntax: nmap -sP <IP Address>



**Host Scan**

Syntax:nmap -sP <target IP Range>



**If you see anything unusual in this list, you can then run a DNS query on a specific host, by using**

**Syntax: namp -sL <IP Address>**



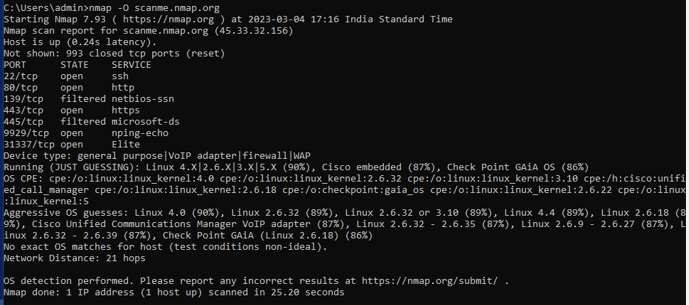
**UDP Scan**

syntax: nmap -sU <target>



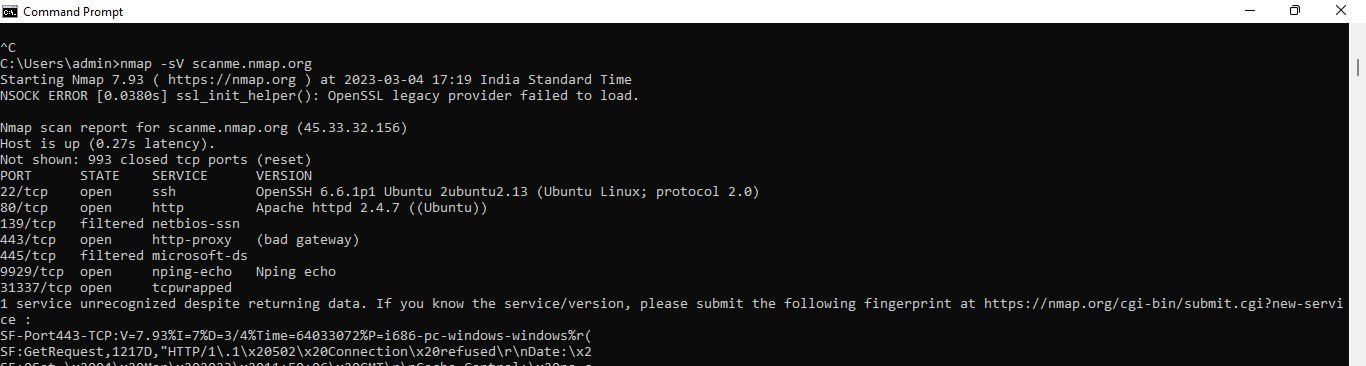
**OS Detection Scan**

Syntax: nmap -O <target>



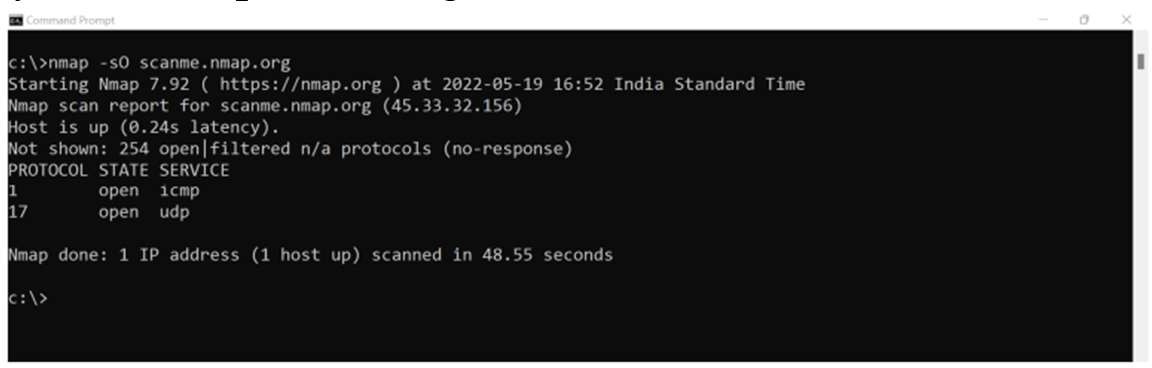
**Version Scan**

syntax: nmap -sV <target>



**Protocol Scan**

syntax: nmap -sO <target>

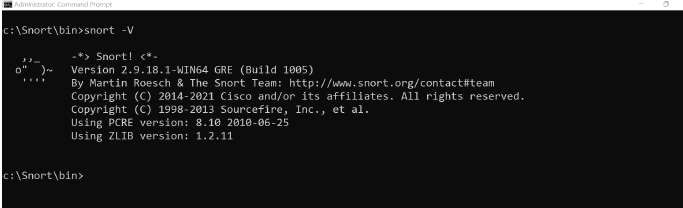


**>Aim:** Applying Intrusion Detection System using snort tool.

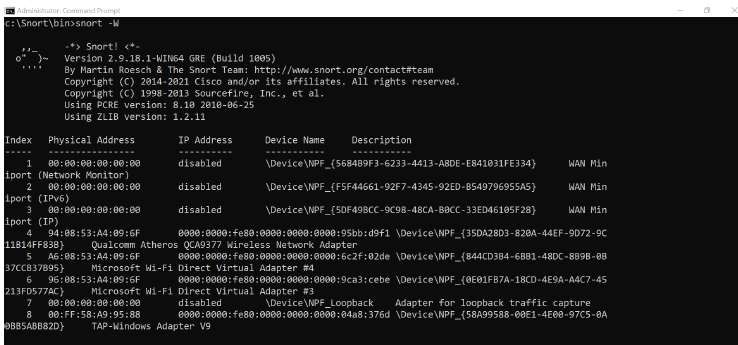
**Snort:**

Snort is a free open-source network intrusion detection system (NIDS) and intrusion prevention system (IPS). Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.

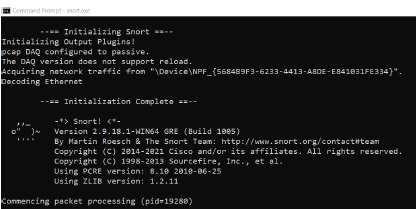
To check snort is installed use command: snort -V



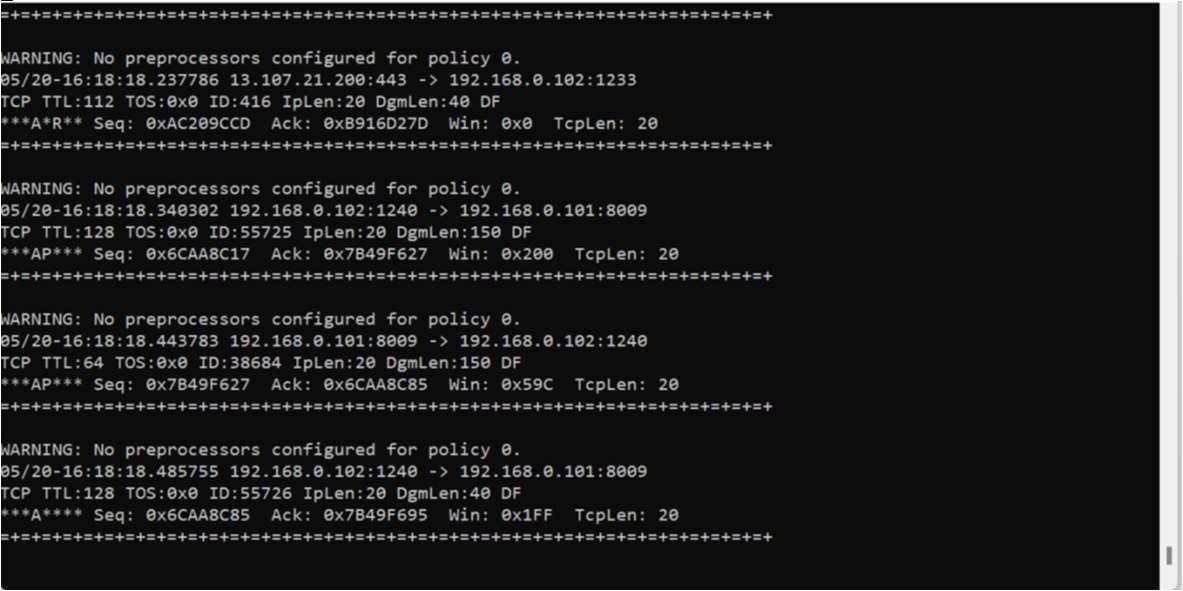
To see a list of interfaces run the following command: snort -W



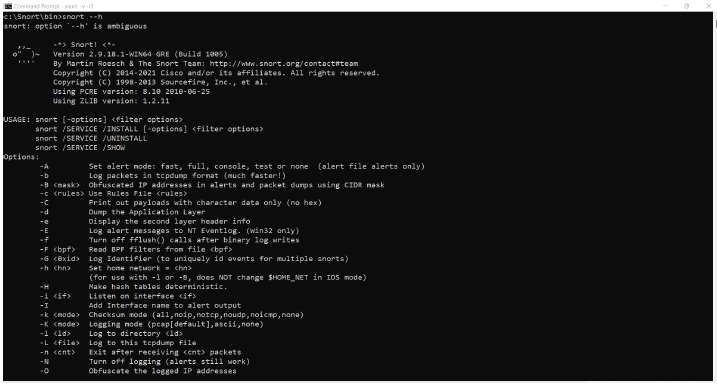
On command prompt execute the following command: Snort.exe



Once you press enter after writing the command you will start receiving packet information as shown below:-



To end capturing the packet details press ctrl +c.

The following command will invoke the Helps. **Snort –h**

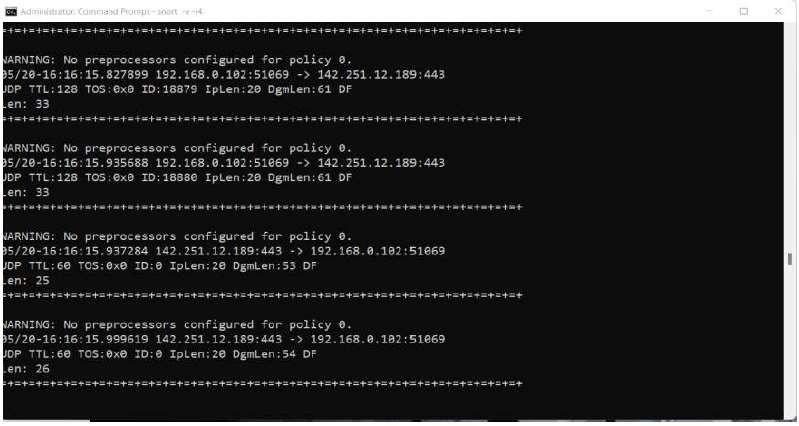
**Running Snort in Sniffer mode**

If you’re running Snort from the command line with two network adapters, specify which adapter to monitor:

C:\>snort -v -i#

The following command runs Snort as a packet sniffer with the verbose switch, outputting TCP/IP packet headers to the screen. Press Ctrl+C keys to stop the output. Snort/WinPcap summarizes its activities, as shown in the following screenshot.

**Command: Snort -v -i3**



After pressing ctrl +c Key you will get the report as follows:



**>Aim:** Performing network sniffing using Wireshark.

Computers communicate using networks. These networks could be on a local area network LAN or exposed to the internet. Network Sniffers are programs that capture low-level package data that is transmitted over a network. An attacker can analyze this information to discover valuable information such as user ids and passwords.

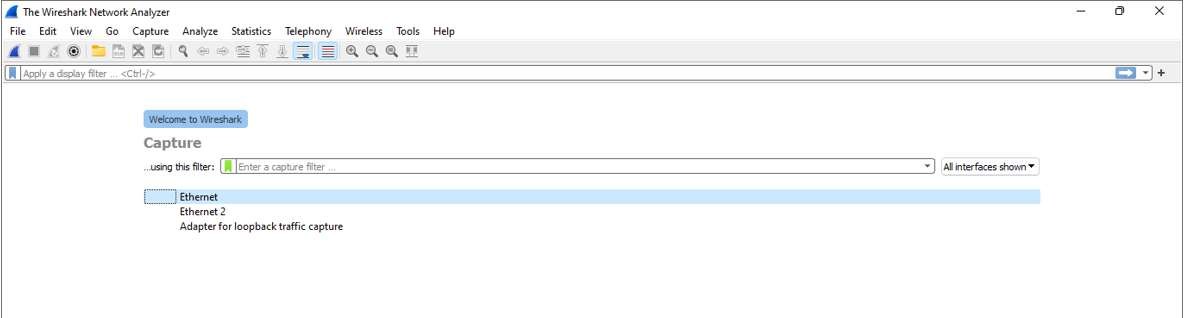
**Network sniffing is the process of capturing data packets sent over a network.** This can be done by the specialized software program or hardware equipment. Sniffing can be used to;

* Capture sensitive data such as login credentials
* Eavesdrop on chat messages
* Capture files that have been transmitted over a network The following are protocols that are vulnerable to sniffing
* Telnet
* Rlogin
* HTTP
* SMTP
* NNTP
* POP
* FTP
* IMAP

The above protocols are vulnerable if login details are sent in plain text

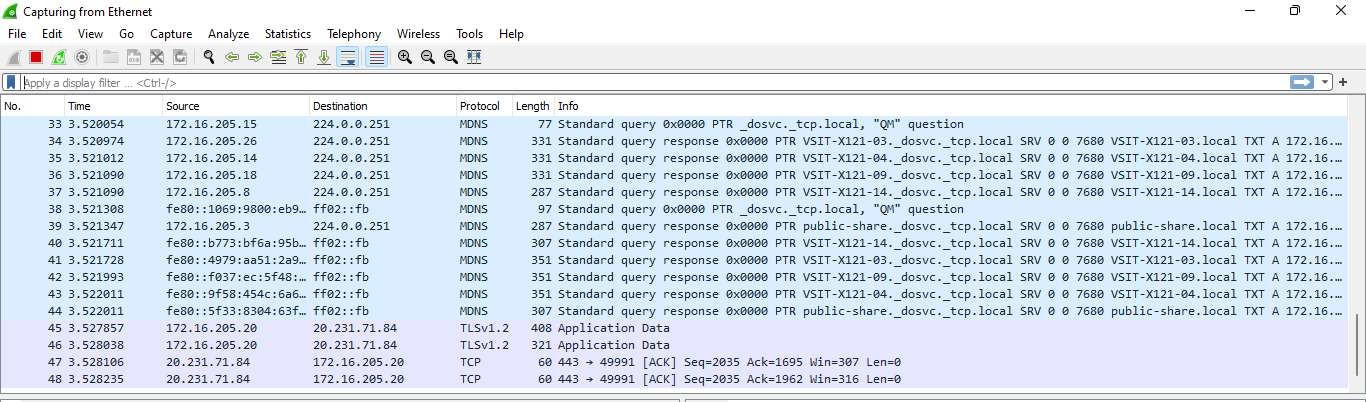
**Network sniffing using Wireshark:**

1. **Wireshark userinterface:**

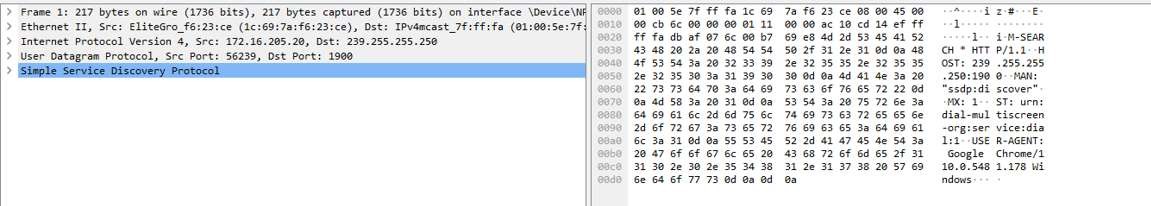


1. **Capturing Live Network Data:**

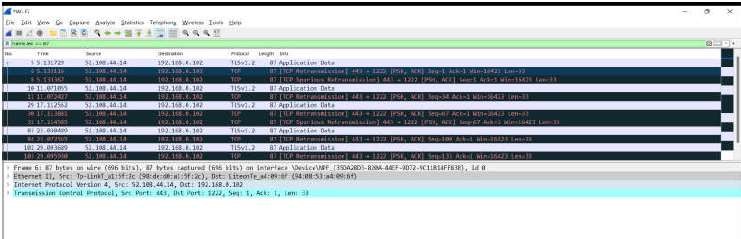
**Once you doble click on the inface you will start getting packet detail entering and leaving the network as shown below:**



1. **Viewing Captured Packets:**



1. **Filtering Packets:**

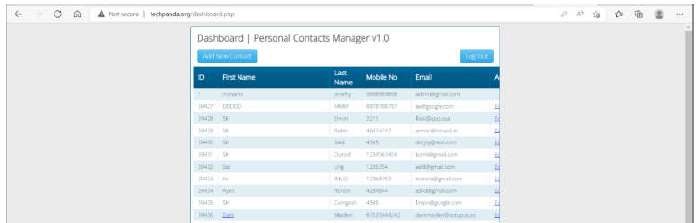


1. **Sniffing the network using Wireshark:**

**Step 1:** Start Wireshark and start capturing network

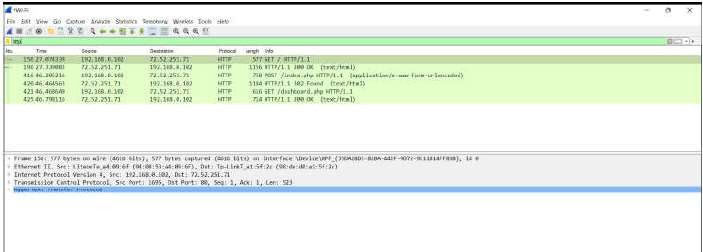
**Step 2** : Login to a web application that does not use secure communication. We will login to a web application on <http://www.techpanda.org/> address with the login name is

[admin@google.com,](mailto:admin@google.com) and the password is Password2010.



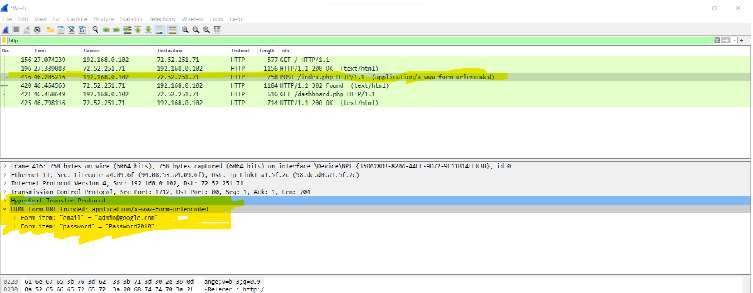
**Step3:** Go Back to wireshark and stop the live capture.

**Step 4:** Enter filter for HTTP protocol results only using filter textbox and press enter key.



**Step5:** Select frame from packet list with post/index.php

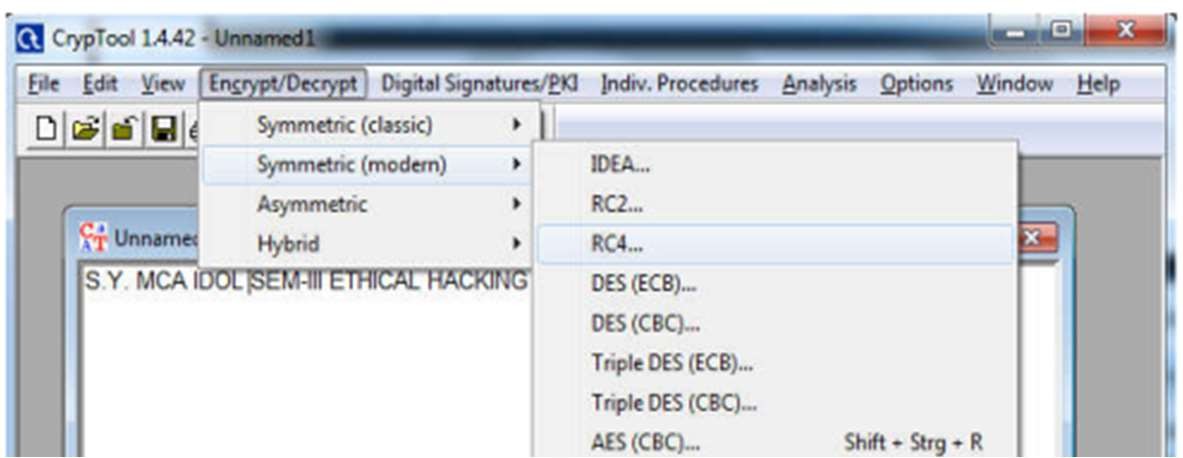
**Step 6:** Look for the summary that says HTML Form URL Encoded: application/x-www-form-urlencoded



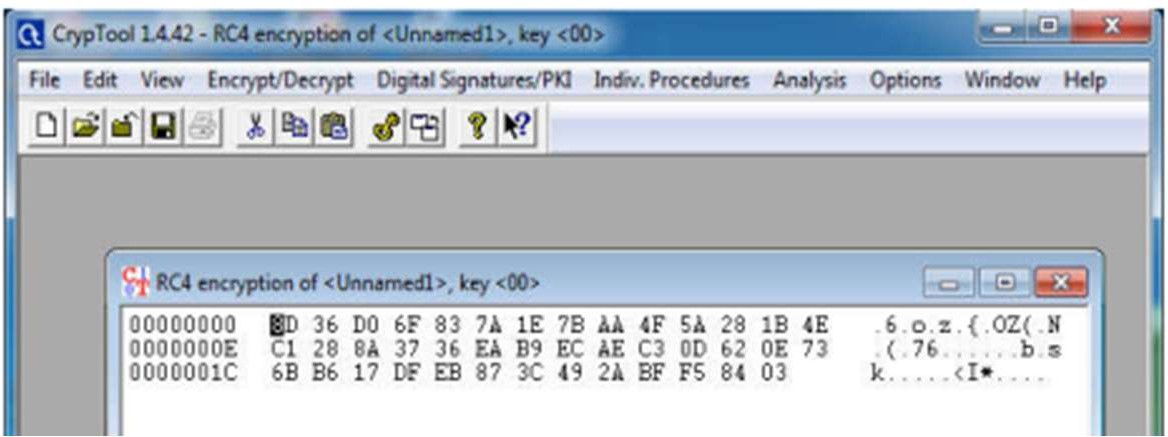
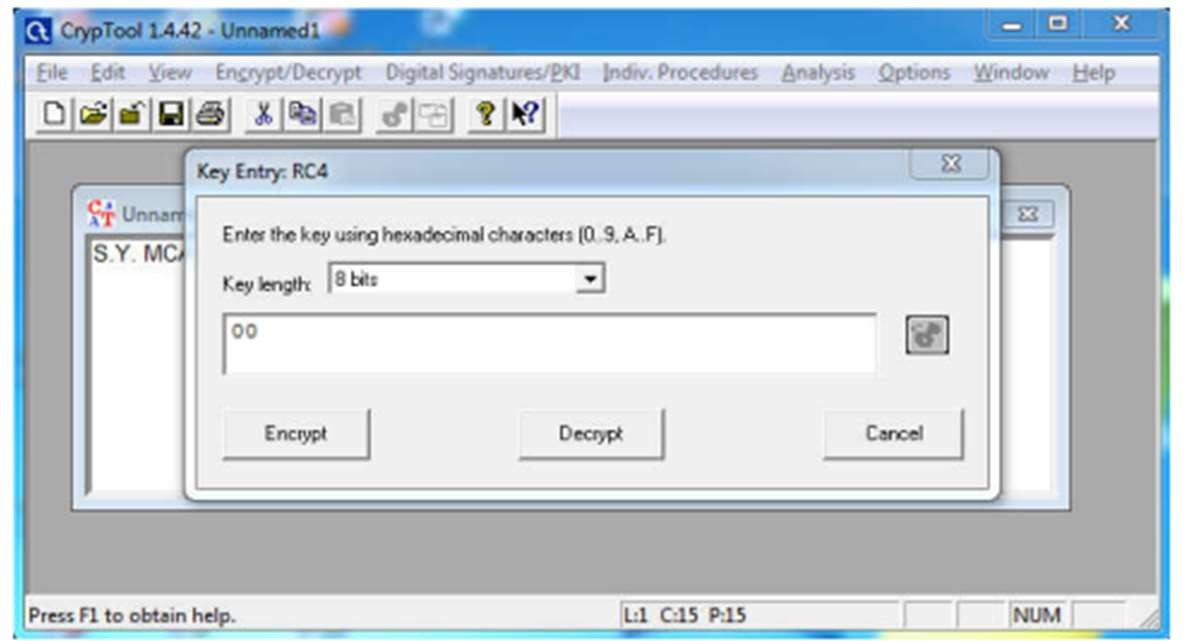
1. **Using CrypTool to encrypt and decrypt password using RC4 algorithm Step-1**

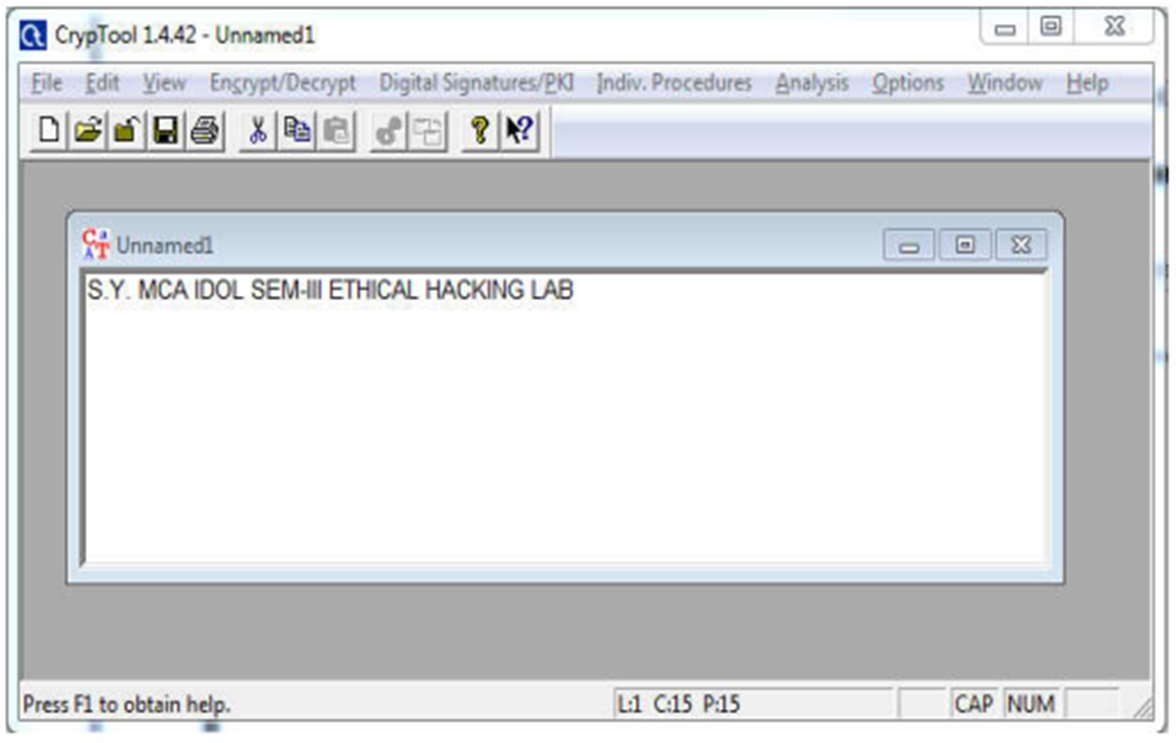
**Step 2:**

* Click Encrypt/Decrypt Tab
* Select Symmetric (Modern)
* Using RC4.

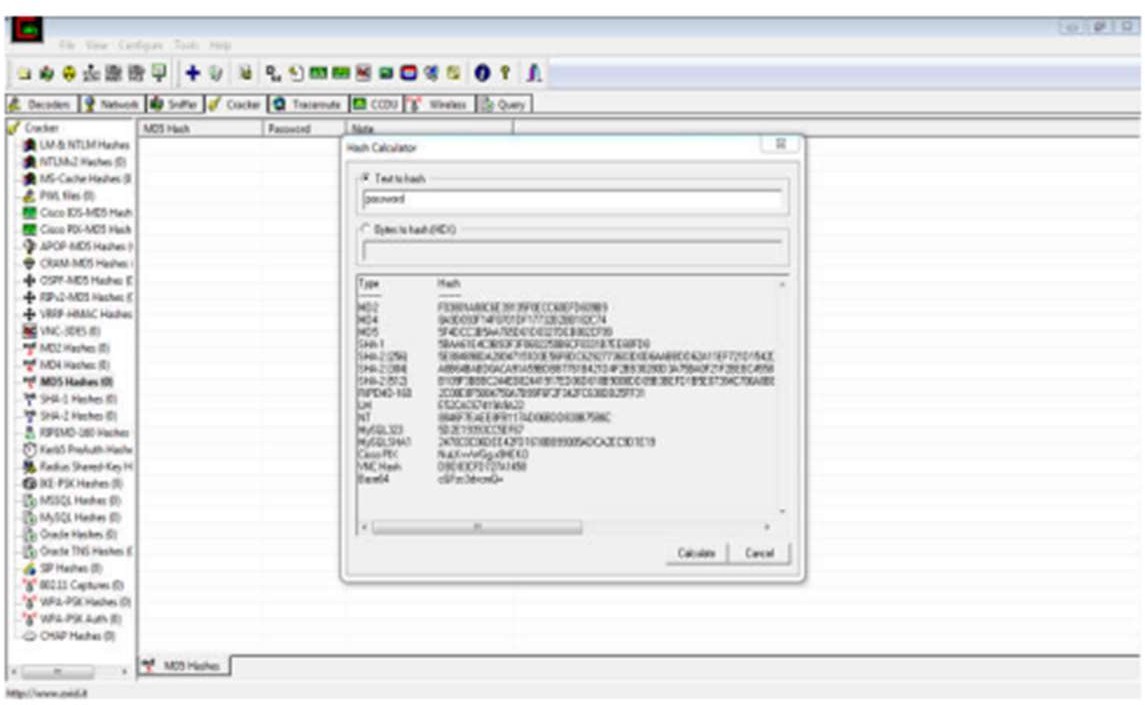


**Step 3: Encryption using RC4.**



**Step 4:Decryption using RC4. ** **Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords.**

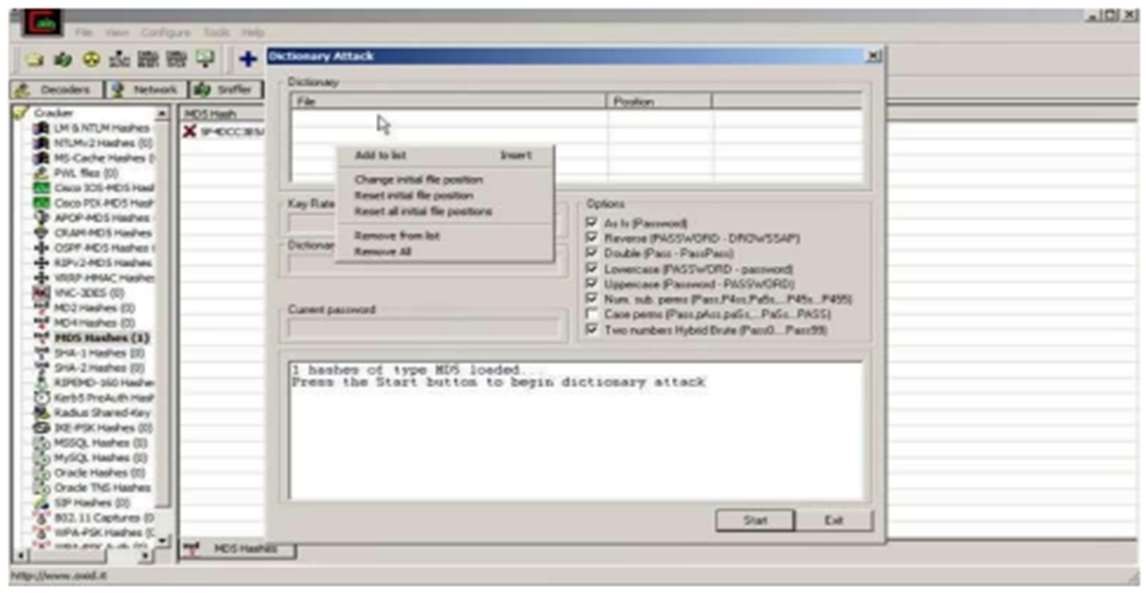
1. Install chain and Abel software.
2. Click on Hash Calculator



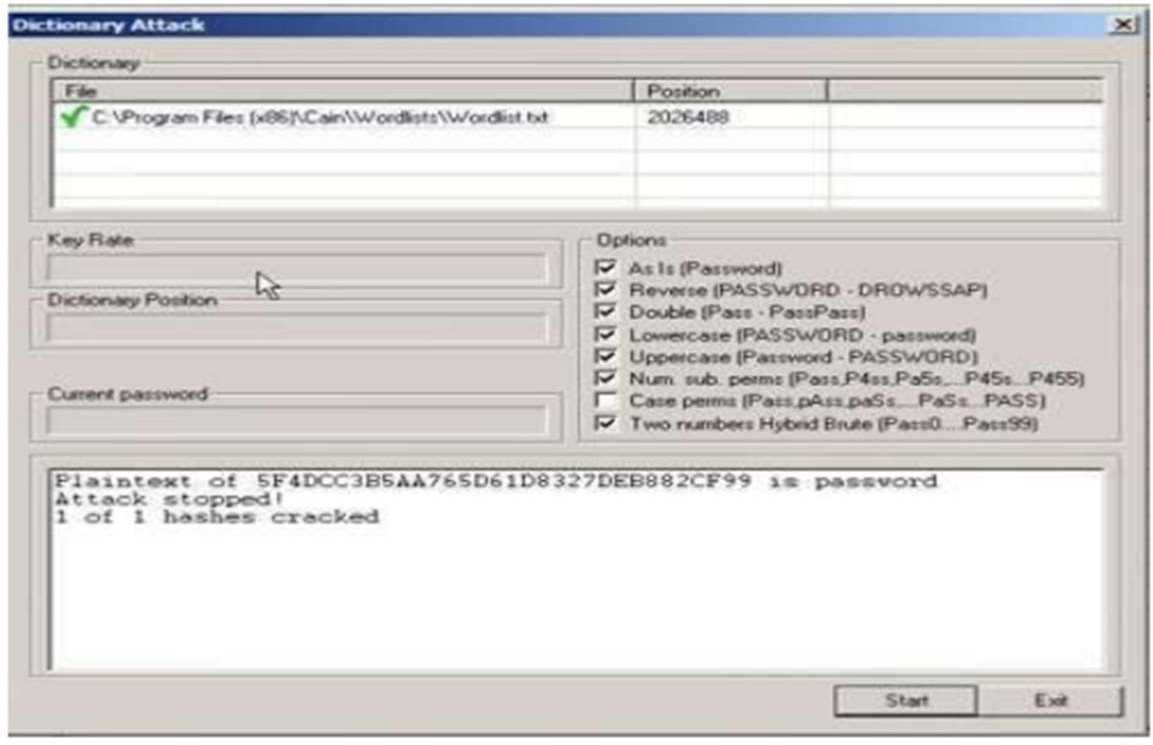
3:- Enter the password to convert into hash Paste the value into the field you have converted e.g(MD5)



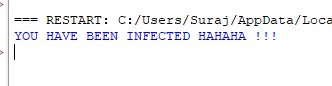
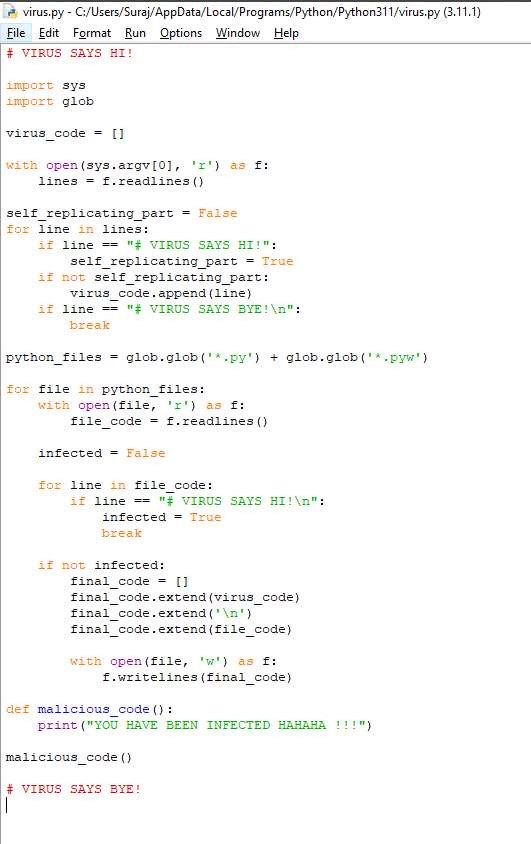
4:- Right Click on the hash and select the dictionary attack.



5:- Then right click on the file and select (Add to List) and then select the Wordlist 6:- Select all the options and start the dictionary attack



1. Developing and implementing malwares



1. **Hacking web servers, web applications**

Hacking a website by Remote File Inclusion, Disguise as Google Bot to view hidden content of a website, to use Kaspersky for Lifetime without Patch

File inclusion attack simulation using dvwa, lamp stack in debian 11.

**Setting DVWA website.**

Download the zip file and extracted it in /var/www/html folder after installation and entered the command sudochmod -R 777 /var/www/html/dvwa

this command will allow the website to be hosted on apache.

Next I have also followed the readme in the dvwa zip file to setup the database in mariadb

Note, if you are using MariaDB rather than MySQL (MariaDB is default in debian), then you can't use the database root user, you must create a new database user. To do this, connect to the database as the root user then use the following commands:

```mysql

mysql> create database dvwa; Query OK, 1 row affected (0.00 sec)

mysql> create user dvwa@localhost identified by 'p@ssw0rd'; Query OK, 0 rows affected (0.01 sec)

mysql> grant all on dvwa.\* to dvwa@localhost; Query OK, 0 rows affected (0.01 sec)

mysql> flush privileges;

Query OK, 0 rows affected (0.00 sec)

```

Then keep the DVWA config to default containing variables are set to the following by default:

$*\_DVWA[ 'db\_*server'] = '127.0.0.1';

$*\_DVWA[ 'db\_*port'] = '3306';

$*\_DVWA[ 'db\_*user' ] = 'dvwa';

$*\_DVWA[ 'db\_*password' ] = 'p@ssw0rd';

$*\_DVWA[ 'db\_*database' ] = 'dvwa';

At this point we need to change the phpini file located in

/etc/php/7.4/apache2 folder for php 7.4 To allow for

1. allow\_url\_fopen = On
2. allow\_rul\_include = On

also find the ip address of the server using hostname,ifconfig,netstat command

Now you can carry out file inclusion attack

Set the security level of DVWA to low

Then try the file inclusion attack by changing the path ?page=index.php

with /etc/passwd or any other linux folder.

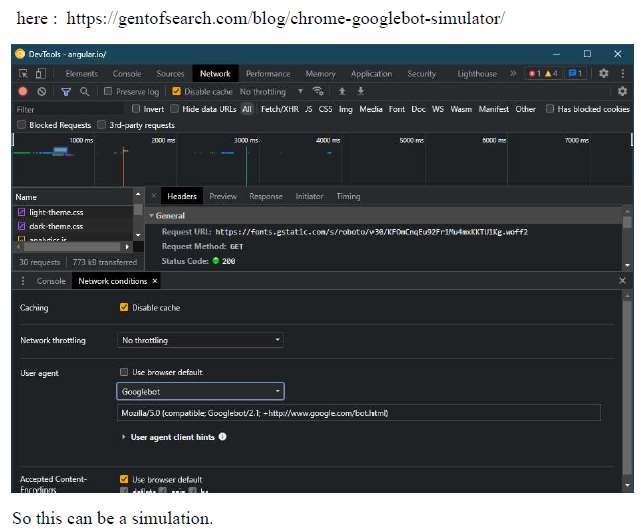


**Quick way to setup the DVWA virtual machine If you do not want to install from scratch :**

**Just download the ovf file and import it in virtualbox, it will create the virtual machine with DVWA installed and all the configuration done.**

DISGUISE AS GOOGLE BOT TO VIEW HIDDEN CONTENT OF A WEBSITE

Simulate GoogleBot to view hidden content of website



# KASPERSKY LIFETIME VALIDITY

Install Kaspersky AV

Then disable self defence in settings

Open regedit or registry editor in windows Open Folder Path (for 32bit OS)

HKEY\_LOCAL\_MACHINE\SOFTWARE\KasperskyLab\protected\ APV8\environment Look for Product code (License code)

Right Click on product code and modify it by changing last 3-4 characters of the product key.

Close Registry edit and click on the Kaspersky icon in the taskbar and exit it Turn on Kaspersky AV again and click on activate beta version

The trial license would have been activated had it been 2009,

since it is almost 13 years later the server has been updated and this trick doesn’t work

Lastly re-enable the self defence option

That was Kaspersky trial License extension by randomly creating new productcode and trying to get another 30 day trial.

# SQL INJECTION

SQL Injection (SQLi) is a type of an injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL Injection vulnerabilities to bypass application security measures.

**SQL Injection Attack Performed**

SQL is a query language that was designed to manage data stored in relational databases. You can use it to access, modify, and delete data. Many web applications and websites store all the data in SQL databases. Successful SQL Injection attack can have very serious consequences.

* Attackers can use SQL Injections to find the credentials of other users in the database.
* An SQL Injection vulnerability could allow the attacker to gain complete access to all data in a database server.
* An attacker could use SQL Injection to alter balances, void transactions, or transfer money to their account.
* Attacker can delete records from a database or even drop tables.
* An attacker could use an SQL Injection as the initial vector and then attack the internal network behind a firewall.

SQL Injection can be classified into three major categories –

1. **In-band SQLi (Classic SQLi)**

In-band SQL Injection occurs when an attacker is able to use the same communication channel to both launch the attack and gather results. The two most common types of in-band SQL Injection are

1. **Inferential SQLi (Blind SQLi)**

Inferential SQL Injection, unlike in-band SQLi, may take longer for an attacker to exploit, however, it is just as dangerous as any other form of SQL Injection. In an inferential SQLi attack, no data is actually transferred via the web application and the attacker would not be able to see the result of an attack in-band (which is why such attacks are commonly referred to as “blind SQL Injection attacks”). Instead, an attacker is able to reconstruct the database structure by sending payloads, observing the web application’s response and the resulting behavior of the database server.

1. **Out-of-band SQLi**

Out-of-band SQL Injection occurs when an attacker is unable to use the same channel to launch the attack and gather results. Out-of-band techniques, offer an attacker an alternative to inferential time-based techniques, especially if the server responses are not very stable (making an inferential time-based attack unreliable).

**Prevent SQL Injections (SQLi)**

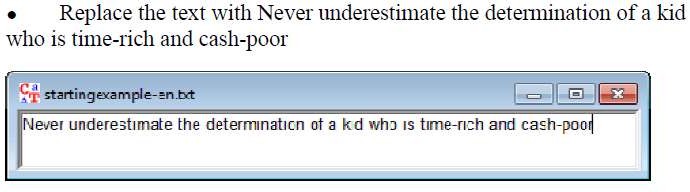
Step 1: Train and maintain awareness Step 2: Don’t trust any user input Step 3: Use whitelists, not blacklists Step 4: Adopt the latest technologies Step 5: Employ verified mechanisms

Step 6: Scan regularly (with Acunetix)

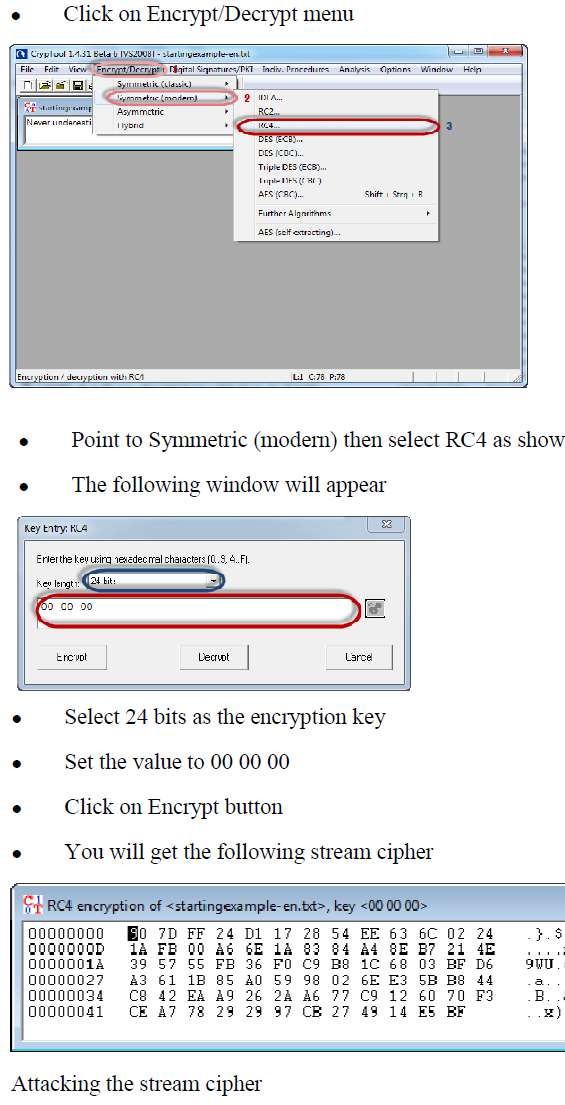
1. **Create a cipher using cryptool Creating the RC4 stream cipher**

Step 1) Download and intall Crypt Tool

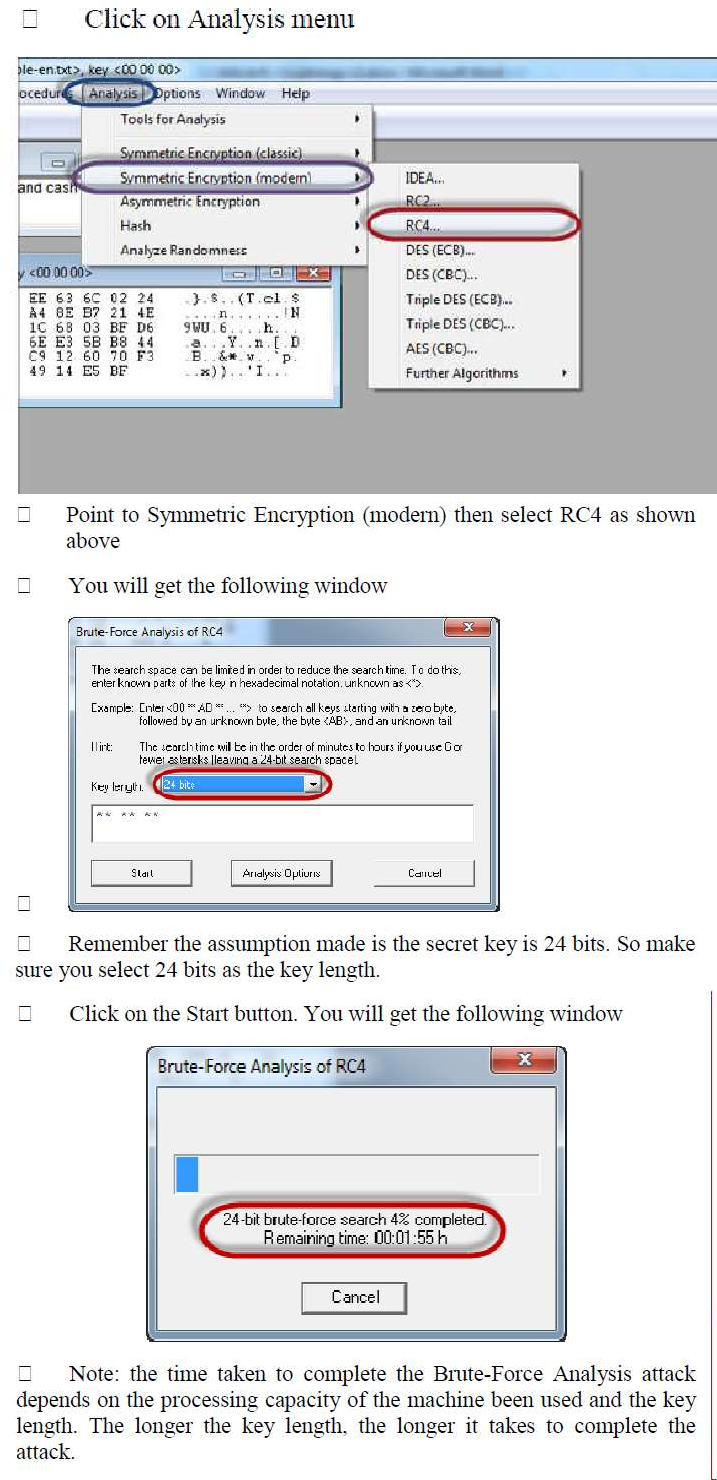
Step 2) Open Crypt Tool and replace the text



Step 3) Encrypt the text

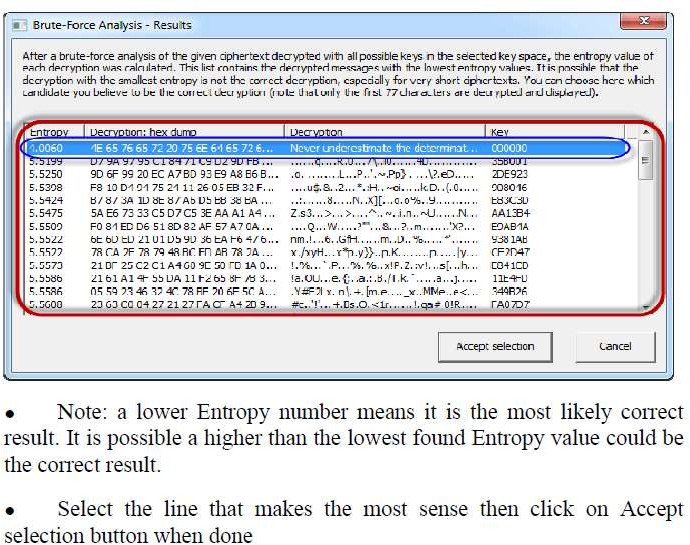


Step 4) Select encryption key Step 5) Start Analysis



Step 6) Analyse the results





1. Implement encryption and decryption using caeser cipher

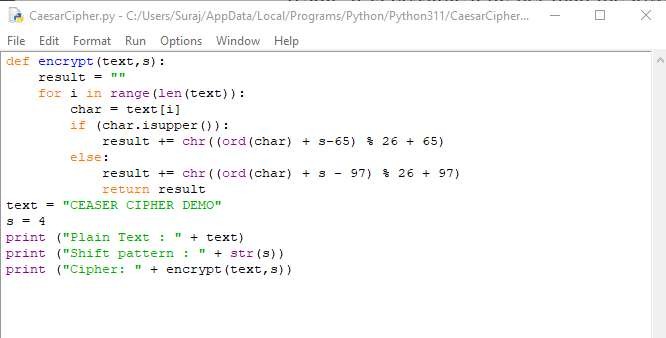
**Algorithm of Caesar Cipher**

The algorithm of Caesar cipher holds the following features −

Caesar Cipher Technique is the simple and easy method of encryption technique.

It is simple type of substitution cipher.

Each letter of plain text is replaced by a letter with some fixed number of positions down with alphabet.



**Output:**

