Diploma Engineering

Laboratory Manual

(Cyber Security)

(4353204)

[Information and Communication Technology, Semester V]

Enrolment No	
Name	
Branch	
Academic Term	
Institute	

Directorate Of Technical Education Gandhinagar – Gujarat

DTE’s Vision:

- To provide globally competitive technical education;
- Remove geographical imbalances and inconsistencies;
- Develop student friendly resources with a special focus on girls’ education and support to weaker sections;
- Develop programs relevant to industry and create a vibrant pool of technical professionals.

Institute’s Vision:

Institute’s Mission:

Department’s Vision:

Department’s Mission:

Name of institute

<u>Certificate</u>

This is to certify that Mr./Ms ……………………………………………………………………. Enrollment No. ………………………………………….. of_ 5th _ Semester of *Diploma in Information and Communication Technology* of …………………………………………………………………….. (GTU Code) has satisfactorily completed the term work in course ………………………………………………………………………………………… for the academic year: ………………….. Term: Odd/Even_prescribed in the GTU curriculum.

Place:…………………..

Date: …………………..

Signature of Course Faculty

Head of the Department

Preface

The primary aim of any laboratory/Practical/field work is enhancement of required skills as well as creative ability amongst students to solve real time problems by developing relevant competencies in psychomotor domain. Keeping in view, GTU has designed competency focused outcome-based curriculum -2021 (COGC-2021) for Diploma engineering programmes. In this more time is allotted to practical work than theory. It shows importance of enhancement of skills amongst students and it pays attention to utilize every second of time allotted for practical amongst Students, Instructors and Lecturers to achieve relevant outcomes by performing rather than writing practice in study type. It is essential for effective implementation of competency focused outcome- based Green curriculum-2021. Every practical has been keenly designed to serve as a tool to develop & enhance relevant industry needed competency in each and every student. These psychomotor skills are very difficult to develop through traditional chalk and board content delivery method in the classroom. Accordingly, this lab manual has been designed to focus on the industry defined relevant outcomes, rather than old practice of conducting practical to prove concept and theory.

By using this lab manual, students can read procedure one day in advance to actual performance day of practical experiment which generates interest and also, they can have idea of judgement of magnitude prior to performance. This in turn enhances predetermined outcomes amongst students. Each and every Experiment /Practical in this manual begins by competency, industry relevant skills, course outcomes as well as practical outcomes which serve as a key role for doing the practical. The students will also have a clear idea of safety and necessary precautions to be taken while performing experiment.

This manual also provides guidelines to lecturers to facilitate student-centered lab activities for each practical/experiment by arranging and managing necessary resources in order that the students follow the procedures with required safety and necessary precautions to achieve outcomes. It also gives an idea that how students will be assessed by providing Rubrics.

Cybersecurity is a critical field that focuses on protecting systems, networks, and data from digital attacks, damage, or unauthorized access. This course on Cybersecurity aims to equip students with the necessary knowledge and skills to safeguard digital assets effectively. Students will explore various cybersecurity concepts such as cryptography, network security, threat analysis, incident response, ethical hacking, digital forensics, and cybersecurity management. Through hands-on exercises and practical examples, students will learn how to implement security protocols, detect vulnerabilities, and develop secure coding practices. This course will serve as a solid foundation for students interested in pursuing advanced topics in cybersecurity. By the end of this course, students will have a comprehensive understanding of cybersecurity principles and the ability to create secure and resilient solutions for real-world cyber threats.

Although we try our level best to design this lab manual, but always there are chances of improvement. We welcome any suggestions for improvement.

Programme Outcomes (POs) :

1. **Basic and Discipline specific knowledge:** Apply knowledge of basic mathematics, science and engineering fundamentals and engineering specialization to solve the *engineering* problems.

2. **Problem analysis**: Identify and analyse well-defined *engineering* problems using codified standard methods.

3. **Design/ development of solutions:** Design solutions for *engineering* well-defined technical problems and assist with the design of systems components or processes to meet specified needs.

4. **Engineering Tools, Experimentation and Testing:** Apply modern *engineering* tools and appropriate technique to conduct standard tests and measurements.

5. **Engineering practices for society, sustainability and environment:** Apply appropriate technology in context of society, sustainability, environment and ethical practices.

6. **Project Management:** Use engineering management principles individually, as a team member or a leader to manage projects and effectively communicate about well-defined engineering activities.

7. **Life-long learning:** Ability to analyze individual needs and engage in updating in the context of technological changes *in field of engineering.*

Practical Outcome - Course Outcome matrix

Course Outcomes (COs):

CO1: Understand the fundamental principles of cybersecurity, apply them to analyze, evaluate, and implement effective security measures in digital environments.

CO2: Implement security strategy encompassing authentication, authorization, defense against malicious software.

CO3: Secure web communications and applications by applying security protocols, managing ports, and implementing HTTPS, SSH, and VPN technologies.

CO4: Conduct ethical hacking and protect systems using Kali Linux tools and vulnerability assessment techniques.

CO5: Identify types of cyber crimes, understand their impact, and apply forensic techniques to investigate and prevent cyber criminal activities.

S. No.	**Practical Outcome/Title of experiment**	**CO1**	**CO2**	**CO3**	**CO4**	**CO5**
1.	Implement the following Substitution & Transposition Techniques concepts in python: a) Caesar Cipher b) Column Transformation	√	-	-	-	-
2.	Implement Public key Cryptography algorithm in python.	√	-	-	-	-
3.	Implement Message digest 5 and Secure Hash Function using python.	√	-	-	-	-
4.	Simulate a brute-force attack to crack passwords of varying strengths (weak, moderate, and strong) and measure the time it takes to crack each password. (Python code or any other tool)	√	-	-	-	-
5.	Set up squid proxy and Windows firewall to observe their effectiveness in blocking unauthorized network traffic.	-	√	-	-	-
6.	Create a Simple Packet Filter Script using *pydivert* package in python.	-	√	-	-	-
7.	Create malicious script for generating multiple folders using python.	-	√	-	-	-
8.	Create malicious script for keylogger using python. (use pynput package)	-	-	√	-	-

9.	Use Nmap to scan a network and identify open ports on a web server, then configure a firewall to block all ports except essential ones (e.g., 80 and 443), and use Nmap again to verify the configuration.	-	**-**	**√**	-	-
10.	a) Installation and configuration of Wireshark. b) Perform Password sniffing using Wireshark. (Analyse GET/POST Request)	-	-	**√**	-	-
11.	a) Installation and configuration of Kali Linux in Virtual box/VMware. b) Perform basic commands in Kali Linux.	-	-	-	**√**	-
12.	Perform Memory forensic using Memoryze tool. (https://fireeye.market/apps/211368)	-	-	-	-	**√**
13.	Perform web Artifact analysis and registry analysis using Autopsy. (https://www.sleuthkit.org/autopsy/)	-	-	-	-	**√**
14.	Create forensic images of entire local hard drives using FTK IMAGER tool. (https://go.exterro.com/l/43312/2023-05-03/fc4b78)	-	-	-	-	**√**

Industry Relevant Skills

The following industry relevant skills are expected to be developed in the students by performance of experiments of this course.

Proficiency in implementing and analyzing cryptographic algorithms and techniques for securing sensitive information.

Develop Skills in configuring security tools, monitoring network traffic, and conducting digital forensics investigations to identify and mitigate network vulnerabilities.

Guidelines to Course Faculty

1. Couse faculty should demonstrate experiment with all necessary implementation strategies described in curriculum.
2. Couse faculty should explain industrial relevance before starting of each experiment.
3. Course faculty should Involve & give opportunity to all students for hands on experience.
4. Course faculty should ensure mentioned skills are developed in the students by asking.
5. Utilise 2 hrs of lab hours effectively and ensure completion of write up with quiz also.
6. Encourage peer to peer learning by doing same experiment through fast learners.

Instructions for Students

1. Organize the work in the group and make record of all observations.
2. Students shall develop maintenance skill as expected by industries.
3. Student shall attempt to develop related hand-on skills and build confidence.
4. Student shall develop the habits of evolving more ideas, innovations, skills etc.
5. Student shall refer technical magazines and data books.
6. Student should develop habit to submit the practical on date and time.
7. Student should well prepare while submitting write-up of exercise.

Continuous Assessment Sheet

Enrolment No: **Name:**

Term:

Sr no	Practical Outcome/Title of experiment	Page	Date	Marks (25)	Sign
1	Implement the following Substitution & Transposition Techniques concepts in python: a) Caesar Cipher b) Column Transformation				
2	Implement Public key Cryptography algorithm in python.				
3	Implement Message digest 5 and Secure Hash Function using python.				
4	Simulate a brute-force attack to crack passwords of varying strengths (weak, moderate, and strong) and measure the time it takes to crack each password. (Python code or any other tool)				
5	Set up squid proxy and Windows firewall to observe their effectiveness in blocking unauthorized network traffic.				
6	Create a Simple Packet Filter Script using *pydivert* package in python.				
7	Create malicious script for generating multiple folders using python.				
8	Create malicious script for keylogger using python. (use pynput package)				
9	Use Nmap to scan a network and identify open ports on a web server, then configure a firewall to block all ports except essential ones (e.g., 80 and 443), and use Nmap again to verify the configuration.				
10	a) Installation and configuration of Wireshark. b) Perform Password sniffing using Wireshark. (Analyse GET/POST Request)				
11	a) Installation and configuration of Kali Linux in Virtual box/VMware. b) Perform basic commands in Kali Linux.				

12	Perform Memory forensic using Memoryze tool. (https://fireeye.market/apps/211368)				
13	Perform web Artifact analysis and registry analysis using Autopsy. (https://www.sleuthkit.org/autopsy/)				
14	Create forensic images of entire local hard drives using FTK IMAGER tool. (https://go.exterro.com/l/43312/2023-05-03/fc4b78)				

Date: ……………

Practical No.1: Implement the following Substitution & Transposition Techniques concepts in Python:

a) Caesar Cipher

b) Column Transformation.

A. **Objective:**

To develop an understanding of and ability to implement substitution and transposition cryptographic techniques, specifically Caesar Cipher and Column Transformation, using Python.

B. **Expected Program Outcomes (POs):**

PO1,PO2,PO3,PO4

C. **Expected Skills to be developed based on competency:**

This practical is expected to develop the following skills for the industry-identified competency:

1. Cryptographic Algorithm Implementation: Developing the skill to understand, implement, and test cryptographic algorithms such as Caesar Cipher and Column Transformation using Python, enhancing the ability to apply theoretical knowledge to practical security solutions.
2. Problem-Solving and Analytical Thinking: Enhancing the ability to analyze cryptographic problems, design appropriate solutions, and debug and optimize code, fostering strong analytical and problem-solving skills critical for tackling complex engineering challenges.

D. **Expected Course Outcomes(Cos)**

CO1: Understand the fundamental principles of cybersecurity, apply them to analyze, evaluate, and implement effective security measures in digital environments.

E. **Practical Outcome(PRo)**

Implement and apply substitution and transposition cryptographic techniques, such as Caesar Cipher and Column Transformation, using Python programming language..

F. **Expected Affective domain Outcome(ADos):**

1. Increased Confidence in Programming Skills: Successfully implementing cryptographic algorithms using Python may boost confidence in programming abilities, fostering a sense of accomplishment and self-efficacy.
2. Heightened Interest in Cybersecurity and Cryptography: Engaging with the complexities of cryptographic techniques could cultivate a deeper curiosity and appreciation for cybersecurity concepts, potentially sparking further exploration and interest in related fields.

G. **Prerequisite Theory:**

Caesar Cipher

The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

For example,

plain: meet me after the exam

cipher: PHHW PH DIWHU WKH HADP

Column Transformation

Column transposition encryption is a method where the plaintext is written into a grid of a certain number of columns and then read out column by column according to a specified order. To encode "MEET ME AFTER THE EXAM" using a columnar transposition, we follow these steps:

Choose a key (number of columns and the order): Let's choose the key "CIPHER" which we will map to numbers based on the alphabetical order of the letters (C=1, E=2, H=3, I=4, P=5, R=6).

Write the plaintext in rows: Fill in the text row by row into a grid with as many columns as there are letters in the key. If the text does not fill up the grid perfectly, pad the remaining spaces with a character such as 'X'.

Plaintext: MEET ME AFTER THE EXAM

key : CIPHER

C(1)	I(4)	P(5)	H(3)	E(2)	R(6)
M	E	E	T		M
E		A	F	T	E
R		T	H	E	
E	X	A	M		

Encrypted text: MERE TE TFHME XEATAME

H. Resources/Equipment Required

Sr.No.	Instrument/Equipment /Components/Trainer kit	Specification	Quantity
1	*Computer system with operating system*	*OS: Windows 10 or above /linux, Min 4GB RAM, 250GB HDD/SSD*	*1*
2.	*Python IDLE*		*1*

I. Safety and necessary Precautions followed:

a. Turn off power switch only after computer is shut down.

b. Do not plug out any computer cables.

J. Procedure to be followed/Source code :

K. Input-Output:

Caesar Cipher

```
Enter plain text: meet me after the exam
Enter integer number:4
Encrypted: qiix qi ejxiv xli ibeq
Decrypted: meet me after the exam
```

Column Transformation

```
Enter plain text: MEET ME AFTER THE EXAM
Enter Key: CIPHER
Encrypted text: MERE TE TFHME  XEATAME
Enter Key to decrypt: CIPHER
Decrypted text: MEET ME AFTER THE EXAM
```

L. Practical related Quiz.

a. What is a Caesar Cipher?
A) A cipher that shifts each letter by a fixed number of positions.
B) A cipher that replaces each letter with a symbol.
C) A cipher that changes the order of letters in each word.
D) A cipher that uses a key to transpose rows and columns.

b. What is the result of encrypting the message "HELLO" with a Caesar Cipher with a shift of 3?
A) KHOOR
B) JGNNU
C) EBIIK
D) IFMMP

c. What is a Column Transposition Cipher?
A) A cipher that shifts each letter by a fixed number of positions.
B) A cipher that replaces each letter with a symbol.
C) A cipher that changes the order of letters based on a grid and key.
D) A cipher that uses a key to transpose rows and columns.

d. What happens if the plaintext does not perfectly fit into the grid in a Columnar Transposition Cipher?
A) The plaintext is truncated.
B) The plaintext is left as is.
C) The grid is resized.

D) Padding characters are added to fill the grid.

e. Given the key "keyboard", which column order should be used for encryption in a Column Transposition Cipher?

M. References / Suggestions

a. Cryptography and Network Security :Principles and Practice by William Stallings
b. https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/
c. https://www.geeksforgeeks.org/columnar-transposition-cipher/

N. Assessment-Rubrics

Sr No.	Performance Indicators	Weightage in %	Marks	Obtained Marks
1	Analyse and identify suitable approach for problem solving	25	0-5	
2	Use of appropriate technology / software / tools	25	0-5	
3	Demonstrate problems as per instructions	20	0-5	
4	Interpret the result and conclusion	15	0-5	
5	Prepare a report/presentation for given problem	15	0-5	
	Total	**100**	**25**	

Sign with Date

Date: …………..

Practical No.2: Implement public key Cryptography algorithm (RSA) in python.

A. **Objective:**

To implement a public key cryptography algorithm in Python to enable secure communication over an insecure channel without requiring pre-shared secret keys.

B. **Expected Program Outcomes (POs)**

PO1, PO2, PO2, PO4

C. **Expected Skills to be developed based on competency:**

This practical is expected to develop the following skills for the industry-identified competency:

1. Understanding of Cryptographic Principles: Developing an understanding of cryptographic principles such as asymmetric encryption, key generation, and secure communication protocols.
2. Programming Proficiency in Python: Enhancing programming skills in Python, including knowledge of data structures, algorithms, and library usage, to implement the cryptographic algorithm effectively and efficiently.

D. **Expected Course Outcomes(Cos)**

CO1: Understand the fundamental principles of cybersecurity, apply them to analyze, evaluate, and implement effective security measures in digital environments.

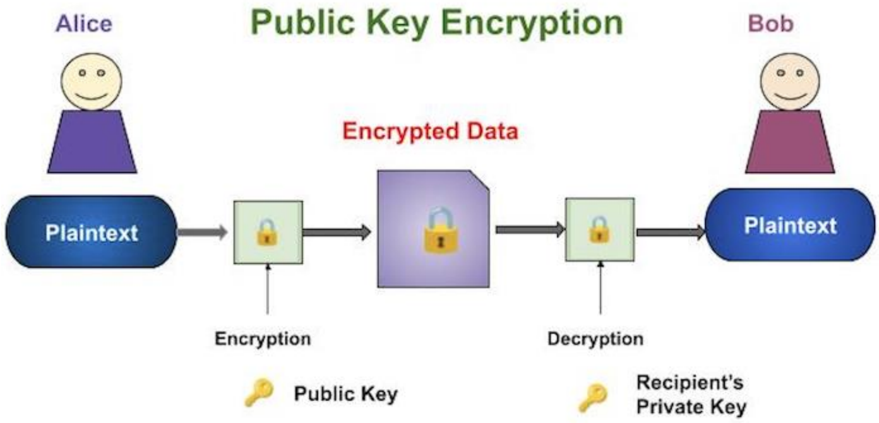
E. **Practical Outcome(PRo)**

Implementation of a functioning public key cryptography algorithm in Python capable of securely encrypting and decrypting messages between two parties.

F. **Expected Affective domain Outcome(ADos)**

a. Increased Confidence in Secure Communication: Participants may develop a sense of confidence in their ability to implement secure communication systems, fostering a belief in their capability to address complex security challenges.
b. Enhanced Appreciation for Cybersecurity Importance: Through hands-on experience with cryptography, participants may gain a deeper appreciation for the importance of cybersecurity measures in protecting sensitive information and maintaining privacy in digital communication.

G. **Prerequisite Theory:**



RSA Algorithm:

RSA (Rivest-Shamir-Adleman) is a widely used public-key cryptography algorithm that enables secure data transmission. The security of RSA relies on the practical difficulty of factoring the product of two large prime numbers.

Steps of RSA Algorithm:

Key Generation:

To generate an RSA public and private key pair, choose two large prime numbers p and q and form their product N = pq. Next, choose e relatively prime to (p − 1)(q − 1) and find the multiplicative inverse of e modulo (p − 1)(q − 1). Denote this inverse of e by d. At this point, we have N = pq, as well as e and d, which satisfy ed = 1 mod (p − 1)(q − 1). Now forget the factors p and q.

The number N is the modulus, whereas e is the encryption exponent and d is the decryption exponent. The RSA key pair consists of

Public key: (N , e)

and

Private key: d.

In RSA, encryption and decryption are accomplished via modular exponentiation. To encrypt with RSA, we raise the message M to the encryption exponent e, modulo N, that is,

$$C = M^e \bmod N.$$

To decrypt C, modular exponentiation with the decryption exponent d is used

$$M = C^d \bmod N$$

Given $C = M^e \bmod N$, we must verify that $M = C^d \bmod N = M^{ed} \bmod N$

Example:

Suppose we select the two "large" primes, p = 11 and q = 3. Then the modulus N = pq = 33 and (p − 1)(q − 1) = 20. Next, we choose the encryption exponent e = 3, which, as required, is relatively prime to (p − 1)(q − 1). We then compute the corresponding decryption exponent, which is d = 7, since ed = 3 · 7 = 1 mod 20. We have,

Public key: (N , e) = (33, 3)

and

Private key: d = 7.

Now suppose person A wants to send to person B the message is M = 15. Sender looks up receiver's public key (N , e) = (33, 3) and computes the ciphertext C as

$C = M^e \text{ mod } N = 3375 \text{ mod } 33=9$

which first person then sends to second person. To decrypt the ciphertext C = 9, second person uses her private
key d = 7 to find

$M = C^d \text{ mod } N = 4{,}782{,}969 \text{ mod } 33= 15$

and person B has recovered the original message M from the ciphertext C.

H. Resources/Equipment Required

Sr.No.	Instrument/Equipment /Components/Trainer kit	Specification	Quantity
1	*Computer system with operating system*		*1*
2.	*Python IDLE*		*1*

I. Safety and necessary Precautions followed

a. Turn off power switch only after computer is shut down.
b. Do not plug out any computer cables

J. Procedure to be followed/Source code :

K. Input-Output:

```
Enter plain text: I like cryptography
first prime no: 41
second prime no: 89
public key: (3649, 2567)
```

```
private key: (3649, 2423)
Original message: I like cryptography
Encrypted message: [3617, 1936, 745, 3325, 195, 2900, 1936, 3006, 3289, 1758, 2794, 3468,
                                     3463, 2821, 3289, 2494, 2794, 2061, 1758]
Decrypted message: I like cryptography
```

L. Practical related Quiz.

1. What is the main purpose of public key cryptography?
   A. To encrypt data using the same key for encryption and decryption
   B. To use separate keys for encryption and decryption
   C. To compress data before transmission
   D. To perform hashing on data

2. In public key cryptography, the public key is used to:
   A. Encrypt data
   B. Decrypt data
   C. Generate a shared secret
   D. Sign a digital certificate

3. What is the primary function of the private key in public key cryptography?
   A. To encrypt data
   B. To decrypt data
   C. To generate the public key
   D. To sign a message

4. What mathematical operation is performed to encrypt a message using the public key in RSA?
   A. Addition
   B. Subtraction
   C. Exponentiation
   D. Division

5. What is the primary reason for using large prime numbers in RSA?
   A. They make the key generation process faster.
   B. They reduce the size of the keys.
   C. They increase the difficulty of factoring the modulus n.
   D. They make encryption and decryption faster.

M. References / Suggestions:

a. https://www.geeksforgeeks.org/rsa-algorithm-cryptography/
b. https://www.tutorialspoint.com/cryptography/public_key_encryption.htm

N. Assessment-Rubrics:

Sr No.	Performance Indicators	Weightage in %	Marks	Obtained Marks
1	Analyse and identify suitable approach for problem solving	25	0-5	

2	Use of appropriate technology / software / tools	25	0-5	
3	Demonstrate problems as per instructions	20	0-5	
4	Interpret the result and conclusion	15	0-5	
5	Prepare a report/presentation for given problem	15	0-5	
	Total	**100**	**25**	

Sign with Date

Date: …………..

Practical No.3: Implement Message digest 5 and Secure Hash Function using python.

A. **Objective:**

To implement and understand the working of the Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) in Python to grasp the concepts of cryptographic hash functions.

B. **Expected Program Outcomes (POs)**

PO1,PO2,PO3,PO4

C. **Expected Skills to be developed based on competency:**

This practical is expected to develop the following skills for the industry-identified competency:

1. Understanding Cryptographic Hash Functions: Developing the ability to comprehend and explain how cryptographic hash functions like MD5 and SHA operate and their significance in data security.
2. Practical Implementation Proficiency: Gaining hands-on experience in implementing cryptographic algorithms using Python, enhancing programming skills and practical knowledge of cryptographic applications.

D. **Expected Course Outcomes(Cos)**

CO1: Understand the basic concepts of data structures, analysis terms, OOPs concepts,

and comprehend the concept of recursive functions.

E. **Practical Outcome(PRo)**

Upon completing this practical, students will be proficient in implementing cryptographic hash functions such as MD5 and SHA using Python. They will gain a thorough understanding of the principles behind these algorithms and their practical applications in data integrity and security. This experience will enhance their ability to apply cryptographic techniques in real-world scenarios, ensuring the protection of sensitive information.

F. **Expected Affective domain Outcome(ADos)**

1. Increased Appreciation for Data Security: Students will develop a heightened awareness and appreciation for the importance of data security and the role cryptographic hash functions play in protecting sensitive information.

2. Enhanced Confidence in Problem-Solving: Students will build confidence in their ability to tackle complex programming challenges and implement secure coding practices through hands-on experience with cryptographic algorithms.

G. **Prerequisite Theory:**

Introduction to Cryptographic Hash Functions

Cryptographic hash functions are mathematical algorithms that transform input data of any size into a fixed-size string of characters, which is typically a digest that appears random. The hash function should have several important properties:

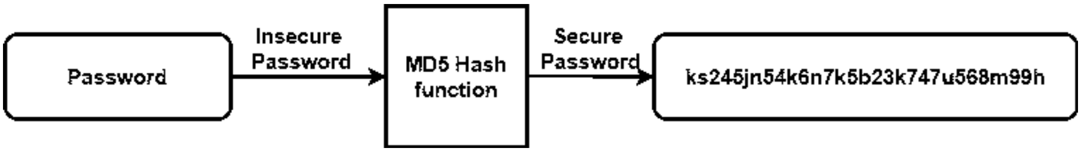
Deterministic: The same input always produces the same output.
Quick Computation: It is efficient to compute the hash value for any given input.
Pre-image Resistance: It should be computationally infeasible to reverse the hash function, meaning you should not be able to derive the original input from its hash.
Small Changes in Input Produce Large Changes in Output: A slight change in the input should produce a significantly different hash.
Collision Resistance: It should be infeasible to find two different inputs that produce the same hash output.

Message digest 5:

MD5 is a cryptographic hash function algorithm that takes the message as input of any length and changes it into a fixed-length message of 16 bytes. MD5 algorithm stands for the message-digest algorithm. MD5 was developed as an improvement of MD4, with advanced security purposes. The output of MD5 (Digest size) is always 128 bits. MD5 was developed in 1991 by Ronald Rivest.

Use Of MD5 Algorithm:

It is used for file authentication.
In a web application, it is used for security purposes. e.g. Secure password of users etc.
Using this algorithm, We can store our password in 128 bits format.



Working of the MD5 Algorithm:

MD5 algorithm follows the following steps

1. Append Padding Bits: In the first step, we add padding bits in the original message in such a way that the total length of the message is 64 bits less than the exact multiple of 512.

Suppose we are given a message of 1000 bits. Now we have to add padding bits to the original message. Here we will add 472 padding bits to the original message.

After adding the padding bits the size of the original message/output of the first step will be 1472 i.e. 64 bits less than an exact multiple of 512 (i.e. 512*3 = 1536).

Length(original message + padding bits) = 512 * i – 64 where i = 1,2,3 . . .

2. Append Length Bits: In this step, we add the length bit in the output of the first step in such a way that the total number of the bits is the perfect multiple of 512. Simply, here we add the 64-bit as a length bit in the output of the first step.
i.e. output of first step = 512 * n – 64
length bits = 64.

After adding both we will get 512 * n i.e. the exact multiple of 512.

3. Initialize MD buffer: Here, we use the 4 buffers i.e. J, K, L, and M. The size of each buffer is 32 bits.

- J = 0x67425301
- K = 0xEDFCBA45
- L = 0x98CBADFE
- M = 0x13DCE476

4. Process Each 512-bit Block: This is the most important step of the MD5 algorithm. Here, a total of 64 operations are performed in 4 rounds. In the 1st round, 16 operations will be performed, 2nd round 16 operations will be performed, 3rd round 16 operations will be performed, and in the 4th round, 16 operations will be performed. We apply a different function on each round i.e. for the 1st round we apply the F function, for the 2nd G function, 3rd for the H function, and 4th for the I function.
We perform OR, AND, XOR, and NOT (basically these are logic gates) for calculating functions. We use 3 buffers for each function i.e. K, L, M.

- F(K,L,M) = (K AND L) OR (NOT K AND M)
- G(K,L,M) = (K AND L) OR (L AND NOT M)
- H(K,L,M) = K XOR L XOR M
- I(K,L,M) = L XOR (K OR NOT M)

After applying the function now we perform an operation on each block. For performing operations we need

add modulo 232
M[i] – 32 bit message.
K[i] – 32-bit constant.
<<<n – Left shift by n bits.

Now take input as initialize MD buffer i.e. J, K, L, M. Output of K will be fed in L, L will be fed into M, and M will be fed into J. After doing this now we perform some operations to find the output for J.

In the first step, Outputs of K, L, and M are taken and then the function F is applied to them. We will add modulo 232 bits for the output of this with J.
In the second step, we add the M[i] bit message with the output of the first step.
Then add 32 bits constant i.e. K[i] to the output of the second step.
At last, we do left shift operation by n (can be any value of n) and addition modulo by 232.
After all steps, the result of J will be fed into K. Now same steps will be used for all functions G, H, and I. After performing all 64 operations we will get our message digest.

<u>Secure Hash Algorithms:</u>
It works by transforming the data using a hash function: an algorithm that consists of bitwise operations, modular additions, and compression functions. The hash function then produces a fixed-size string that looks nothing like the original. These algorithms are designed to be one-way functions, meaning that once they're transformed into their respective hash values, it's virtually impossible to transform them back into the original data. A few algorithms of interest are SHA-1, SHA-2, and SHA-3, each of which was successively designed with increasingly stronger encryption in response to hacker attacks. SHA-0, for instance, is now obsolete due to the widely exposed vulnerabilities.

A common application of SHA is to encrypting passwords, as the server side only needs to keep track of a specific user's hash value, rather than the actual password. This is helpful in case an attacker hacks the database, as they will only find the hashed functions and not the actual passwords, so if they were to input the hashed value as a password, the hash function will convert it into another string and subsequently deny access. Additionally, SHAs exhibit the avalanche effect, where the modification of very few letters being encrypted causes a big change in output; or conversely, drastically different strings produce similar hash values. This effect causes hash values to not give any information regarding the input string, such as its original length. In addition, SHAs are also used to detect the tampering of data by attackers, where if a text file is slightly changed and barely noticeable, the modified file's hash value will be different than the original file's hash value, and the tampering will be rather noticeable.
SHA-1:

SHA-1 processes input data in blocks of 512 bits (64 bytes). If the input length is not a multiple of 512 bits, it is padded. The algorithm involves several steps:

1. Padding the Message: The message is padded so that its length is congruent to 448 modulo 512. Padding involves appending a single '1' bit followed by '0' bits until the length is 448 modulo 512. The final 64 bits of the message are used to store the original message length.
2. Initializing the Buffers: SHA-1 uses five constant 32-bit words to initialize buffers. These buffers are used to store intermediate and final results.
3. Processing the Message in Blocks: The padded message is processed in 512-bit blocks. Each block is expanded to an 80-word sequence using a specific expansion function. The core of the algorithm involves four rounds of processing, each consisting of 20 operations and making use of bitwise operations, modular additions, and logical functions.
4. Producing the Final Hash Value: After processing all blocks, the buffers are concatenated to produce the final 160-bit hash value.

H. Resources/Equipment Required

Sr.No.	**Instrument/Equipment /Components/Trainer kit**	**Specification**	**Quantity**
1	*Computer system with operating system*		*1*
2.	*Python IDLE*		*1*

I. Safety and necessary Precautions followed

- Turn off power switch only after computer is shut down.
- Do not plug out any computer cables

J. Procedure to be followed/Source code :

K. Input-Output:

(1)

```
Enter message: Hello World

MD5 hash of the entered message: b10a8db164e0754105b7a99be72e3fe5
```

```
Enter message again: Hello World

MD5 hash of the entered message again: b10a8db164e0754105b7a99be72e3fe5

Hashes match: Message has not been altered.
```

(2)

```
Enter message: Hello World

SHA-1 hash of the entered message: 0a4d55a8d778e5022fab701977c5d840bbc486d0

Enter message again: Hello World

SHA-1 hash of the entered message again:

0a4d55a8d778e5022fab701977c5d840bbc486d0

Hashes match: Message has not been altered.
```

L. Practical related Quiz/Exercise.

1. Which of the following properties is NOT a characteristic of a good cryptographic hash function?
   A. Deterministic
   B. Collision Resistance
   C. Pre-image Resistance
   D. Variable Output Size
2. What is the primary purpose of a cryptographic hash function?
   A. Encrypt data for secure transmission
   B. Generate random numbers
   C. Provide a unique fixed-size hash value for data integrity verification
   D. Compress data to save storage space
3. Which hash function produces a 160-bit hash value?
   A. MD5
   B. SHA-1
   C. SHA-256
   D. SHA-512
4. In the provided Python code example, which method is used to convert the hash object into a hexadecimal string?
   A. digest()
   B. hexdigest()
   C. update()
   D. encode()

5. What output size does the MD5 hash function produce?
   A. 128 bits
   B. 160 bits
   C. 256 bits
   D. 512 bits

M. References / Suggestions:

a. https://www.geeksforgeeks.org/what-is-the-md5-algorithm/

b. https://brilliant.org/wiki/secure-hashing-algorithms/

N. Assessment-Rubrics:

Sr No.	Performance Indicators	Weightage in %	Marks	Obtained Marks
1	Analyse and identify suitable approach for problem solving	25	0-5	
2	Use of appropriate technology / software / tools	25	0-5	
3	Demonstrate problems as per instructions	20	0-5	
4	Interpret the result and conclusion	15	0-5	
5	Prepare a report/presentation for given problem	15	0-5	
	Total	**100**	**25**	

Sign with Date

Date: …………..

Practical No.4: Simulate a brute-force attack to crack passwords of varying strengths (weak, moderate, and strong) and measure the time it takes to crack each password.

A. Objective:

The objective of this practical is to understand and quantify the time required to crack passwords of varying strengths using brute-force attacks, highlighting the importance of strong passwords for enhanced security.

B. Expected Program Outcomes (POs)

PO1,PO2,PO3

C. Expected Skills to be developed based on competency:

This practical is expected to develop the following skills for the industry-identified competency:

1. Analytical Skills: Develop the ability to analyze and compare the effectiveness of different password strengths against brute-force attacks by interpreting time-to-crack data and understanding the underlying principles of password security.

2. Technical Proficiency in Cybersecurity Tools: Gain hands-on experience with cybersecurity tools and techniques used for performing brute-force attacks, enhancing practical knowledge in cybersecurity methodologies and best practices.

D. Expected Course Outcomes(Cos)

CO2: Implement security strategy encompassing authentication, authorization, defence against malicious software.

E. Practical Outcome(PRo)

Students will gain a clear understanding of how password strength impacts security and will be able to quantify the time required to crack weak, moderate, and strong passwords using brute-force attacks.

F. Expected Affective domain Outcome(ADos)

1. Increased Awareness and Responsibility: Develop a heightened awareness of the importance of strong password practices and a sense of responsibility for maintaining personal and organizational cybersecurity.

2. Commitment to Best Practices: Foster a commitment to implementing and advocating for best practices in password creation and management to enhance overall security posture.

G. Prerequisite Theory:

Brute Force Attack Definition

A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks. The hacker tries multiple usernames and passwords, often using a computer to test a wide range of combinations, until they find the correct login information.

The name "brute force" comes from attackers using excessively forceful attempts to gain access to user accounts. Despite being an old cyberattack method, brute force attacks are tried and tested and remain a popular tactic with hackers.

Types of Brute Force Attacks

There are various types of brute force attack methods that allow attackers to gain unauthorized access and steal user data.

1. Simple brute force attacks

A simple brute force attack occurs when a hacker attempts to guess a user's login credentials manually without using any software. This is typically through standard password combinations or personal identification number (PIN) codes.

These attacks are simple because many people still use weak passwords, such as "password123" or "1234," or practice poor password etiquette, such as using the same password for multiple websites. Passwords can also be guessed by hackers that do minimal reconnaissance work to crack an individual's potential password, such as the name of their favourite sports team.

2. Dictionary attacks

A dictionary attack is a basic form of brute force hacking in which the attacker selects a target, then tests possible passwords against that individual's username. The attack method itself is not technically considered a brute force attack, but it can play an important role in a bad actor's password-cracking process.

The name "dictionary attack" comes from hackers running through dictionaries and amending words with special characters and numbers. This type of attack is typically time-consuming and has a low chance of success compared to newer, more effective attack methods.

3. Hybrid brute force attacks

A hybrid brute force attack is when a hacker combines a dictionary attack method with a simple brute force attack. It begins with the hacker knowing a username, then carrying out a dictionary attack and simple brute force methods to discover an account login combination.

The attacker starts with a list of potential words, then experiments with character, letter, and number combinations to find the correct password. This approach allows hackers to discover passwords that combine common or popular words with numbers, years, or random characters, such as "SanDiego123" or "Rover2020."

4. Reverse brute force attacks

A reverse brute force attack sees an attacker begin the process with a known password, which is typically discovered through a network breach. They use that password to search for a matching login credential using lists of millions of usernames. Attackers may also use a commonly used weak password, such as "Password123," to search through a database of usernames for a match.

5. Credential stuffing

Credential stuffing preys on users' weak password etiquettes. Attackers collect username and password combinations they have stolen, which they then test on other websites to see if they can gain access to additional user accounts. This approach is successful if people use the same username and password combination or reuse passwords for various accounts and social media profiles.

How Users Can Strengthen Passwords Against Brute Force Attacks

As a user, you can do a lot to support your protection in the digital world. The best defense against password attacks is ensuring that your passwords are as strong as they can be.

Brute force attacks rely on time to crack your password. So, your goal is to make sure your password slows down these attacks as much as possible, because if it takes too long for the breach to be worthwhile… most hackers will give up and move on.

Here are a few ways you can strength passwords against brute attacks:

Longer passwords with varied character types. When possible, users should choose 10-character passwords that include symbols or numerals. Doing so creates 171.3 quintillion (1.71×10^{20}) possibilities. Using a GPU processor that tries 10.3 billion hashes per second, cracking the password would take approximately 526 years. Although, a supercomputer could crack it within a few weeks. By this logic, including more characters makes your password even harder to solve.

Elaborate passphrases. Not all sites accept such long passwords, which means you should choose complex passphrases rather than single words. Dictionary attacks are built specifically for single word phrases and make a breach nearly effortless.

Passphrases — passwords composed of multiple words or segments — should be sprinkled with extra characters and special character types.

Create rules for building your passwords. The best passwords are those you can remember but won’t make sense to anyone else reading them. When taking the passphrase route, consider using truncated words, like replacing “wood” with “wd” to create a string that makes sense only to you. Other examples might include dropping vowels or using only the first two letters of each word.

Stay away from frequently used passwords. It's important to avoid the most common passwords and to change them frequently.

Use unique passwords for every site you use. To avoid being a victim of credential stuffing, you should never reuse a password. If you want to take your security up a notch, use a different username for every site as well. You can keep other accounts from getting compromised if one of yours is breached.

H. **Resources/Equipment Required :**

Sr.No.	Instrument/Equipment /Components/Trainer kit	Specification	Quantity
1	*Computer system with operating system*		*1*
2.	*Python IDLE*		*1*

I: Safety and necessary Precautions followed:

(1)Turn off power switch only after computer is shut down.

(2) Do not plug out any computer cables

J: Source code :

K. Input-Output :

```
Enter password using lowercase alphabet only:gpgs
Enter password using uppercase and lowercase  alphabet:GpGS
Enter password using uppercase, lowercase  alphabet and digits:G1pG

Weak Password
Starting time: 17:45:38
Password is: gpgs
Password crack at time: 17:45:39
Time to crack weak password: 0.63 seconds, Attempts: 312767

Moderate Password
Starting time: 17:45:39
Password is: GpGS
Password crack at time: 17:45:48
Time to crack moderate password: 9.21 seconds, Attempts: 4874102

Strong Password
Starting time: 17:45:48
Password is: G1pG
Password crack at time: 17:46:31
Time to crack strong password: 43.06 seconds, Attempts: 23617292
```

L. Practical related Quiz.

1. What is a brute-force attack?
   A. An attack that tries to guess passwords by using commonly used passwords from a list.
   B. An attack that systematically tries every possible combination of characters until the correct password is found.
   C. An attack that uses malware to steal passwords from a victim’s device.
   D. An attack that relies on social engineering techniques to obtain passwords.

2. Which factor does NOT significantly increase the strength of a password?
   A. Length of the password
   B. Use of a mix of uppercase, lowercase, digits, and symbols
   C. Use of common words and patterns
   D. Unpredictability of characters used

3. How does the length of a password affect the time required to crack it using brute-force methods?
   A. Longer passwords are easier to crack.
   B. The length of a password does not affect the time required to crack it.
   C. Longer passwords exponentially increase the time required to crack them.
   D. Longer passwords linearly increase the time required to crack them.

4. Which of the following is a characteristic of a weak password?
   A. It uses a combination of uppercase letters, lowercase letters, numbers, and symbols.
   B. It is longer than 12 characters.
   C. It contains common words or sequences like "12345" or "password".
   D. It is generated using a random password generator.

5. What is the main disadvantage of a brute-force attack?
   A) It requires extensive knowledge of the system.

B) It guarantees finding the password.
C) It is computationally intensive and time-consuming.
D) It relies on common password lists

M. References / Suggestions

a https://www.kaspersky.com/resource-center/definitions/brute-force-attack

b. https://www.geeksforgeeks.org/brute-force-attack

N. Assessment-Rubrics

Sr No.	Performance Indicators	Weightage in %	Marks	Obtained Marks
1	Analyse and identify suitable approach for problem solving	25	0-5	
2	Use of appropriate technology / software / tools	25	0-5	
3	Demonstrate problems as per instructions	20	0-5	
4	Interpret the result and conclusion	15	0-5	
5	Prepare a report/presentation for given problem	15	0-5	
	Total	**100**	**25**	

Sign with Date

Date: …………..

Practical No.5: Set up squid proxy and Windows firewall to observe their effectiveness in blocking unauthorized network traffic.

A. **Objective:**
To assess the effectiveness of Squid proxy and Windows firewall in blocking unauthorized network traffic.

B. **Expected Program Outcomes (POs)**
PO1,PO2,PO3,PO4

C. **Expected Skills to be developed based on competency:**

Two expected skills to be developed from this practical based on competency are:

1. Network Security Analysis: Understanding how to analyze network traffic and identify unauthorized or potentially harmful activities, which enhances skills in network security analysis.

2. Firewall Configuration: Gaining proficiency in configuring and managing firewalls, specifically in this case, configuring the Windows firewall to control network traffic effectively.

D. **Expected Course Outcomes(Cos)**

CO2: Implement security strategy encompassing authentication, authorization, defence against malicious software.

E. **Practical Outcome(PRo)**

To configure and evaluate the effectiveness of a Squid proxy server and Windows firewall in blocking unauthorized network traffic, thereby enhancing network security.

F. **Expected Affective domain Outcome(ADos)**

1. Develop an appreciation for the importance of network security in protecting organizational data and resources.
2. Cultivate a proactive attitude towards implementing and maintaining security measures to prevent unauthorized access and cyber threats.

G. **Prerequisite Theory:**

Squid Proxy:

Squid proxy is a reliable and secure method to handle traffic data on your network. It was developed in the 1900s to reduce latency and to promote faster download speeds. It is still in use today as a high-performance proxying, forwarding, and caching application, and is preferred by many educational institutions, organizations, and ISPs.

What is Squid proxy?

Squid is provided as free, open-source software, and can be used under the GNU General Public License (GPL) of the Free Software Foundation. Squid was originally designed to run on Unix-based systems, but it can also be run on Windows machines. It is available in multiple types and is deployed primarily to help reduce bandwidth congestion, increase loading speed, and optimize network traffic.

A proxy server is a dedicated computer or a software system running on a computer that acts as an intermediary between an endpoint device, such as a computer, and another server from which a user or client is requesting a service.

Squid is a Unix-based, specialized proxy server that acts as a caching proxy for web objects accessed through HTTP, HTTPS, FTP, and more. It is commonly used for several purposes, including caching, load balancing, filtering traffic from websites, and for security purposes.

Key Features of Squid Proxy Server:

Here are the Squid features, along with a detailed description of each and how they differentiate it from other similar proxy tools:

1. Access Control Lists: Squid allows you to set ACLs to manage which networks have access to the internet. This feature provides a high level of control over network access, which is not commonly found in all proxy servers.
2. Website Access Control: Squid can block or allow access to certain websites. This feature is particularly useful for organizations that want to restrict access to specific online content.
3. Content-Based Access Control: Squid can block or allow content based on MIME types (e.g., image, text, mpeg). This feature provides a granular level of control over the type of content that can be accessed, which is not typically offered by other proxy servers.
4. Time-Based Access Control: Squid allows you to set specific times during the day when users can access the internet. This feature can be useful for managing internet usage during work hours.
5. Caching: Squid can cache frequently accessed websites and files/media. This feature helps to reduce bandwidth usage and improve response times by reusing frequently-requested web pages.
6. IP Address Anonymization: Squid can hide users’ internal IP addresses. This feature enhances user privacy and is not commonly found in all proxy servers.
7. Load Balancing: Squid can load balance with other Squid proxies. This feature helps to distribute network traffic evenly across multiple servers, improving performance and reliability.

8. Clustering: Squid supports clustering, which allows multiple servers to work together to handle traffic, improving performance and reliability.
9. Traffic Interception with WCCP: Squid can intercept and redirect network traffic using the Web Cache Coordination Protocol (WCCP). This feature is not commonly found in all proxy servers.
10. Authentication: Squid supports various authentication methods, including LDAP, Active Directory, RADIUS, POP3, DB, etc. This feature provides a high level of control over who can access the proxy server.
11. Instant Messaging Control: Squid can allow or block Instant Messaging (IM). This feature is particularly useful for organizations that want to manage the use of IM applications.
12. Script Blocking: Squid can block coin-mining scripts from using CPU/memory on users' browsers. This is a unique feature that addresses a modern trend of unauthorized cryptocurrency mining.
13. Adaptation Protocol: Squid supports the C-ICAP / eCAP adaptation protocol. This feature allows Squid to be extended to support new protocols or features.
14. Dynamic Content Caching: Squid can cache dynamic content. This feature is not commonly found in all proxy servers and can significantly improve performance for dynamic websites.
15. Transparent Interception: Squid supports fully transparent interception with Squid-2, TPROXYv2, and WCCP. This feature allows Squid to intercept and handle network traffic without requiring any configuration changes on client devices.
16. Multiple Interception Ports: Squid supports configuring multiple interception ports using WCCPv2. This feature provides a high level of flexibility in how network traffic is intercepted and handled.
17. PHP Redirectors: Squid supports PHP redirectors. This feature allows Squid to be extended with custom logic written in PHP.
18. SMP Carp Cluster: Squid supports SMP Carp Cluster. This feature allows multiple Squid servers to work together to handle traffic, improving performance and reliability.
19. Torrent Filtering: Squid can filter torrent traffic. This feature is particularly useful for organizations that need to manage and control torrent traffic.

Windows Firewall:

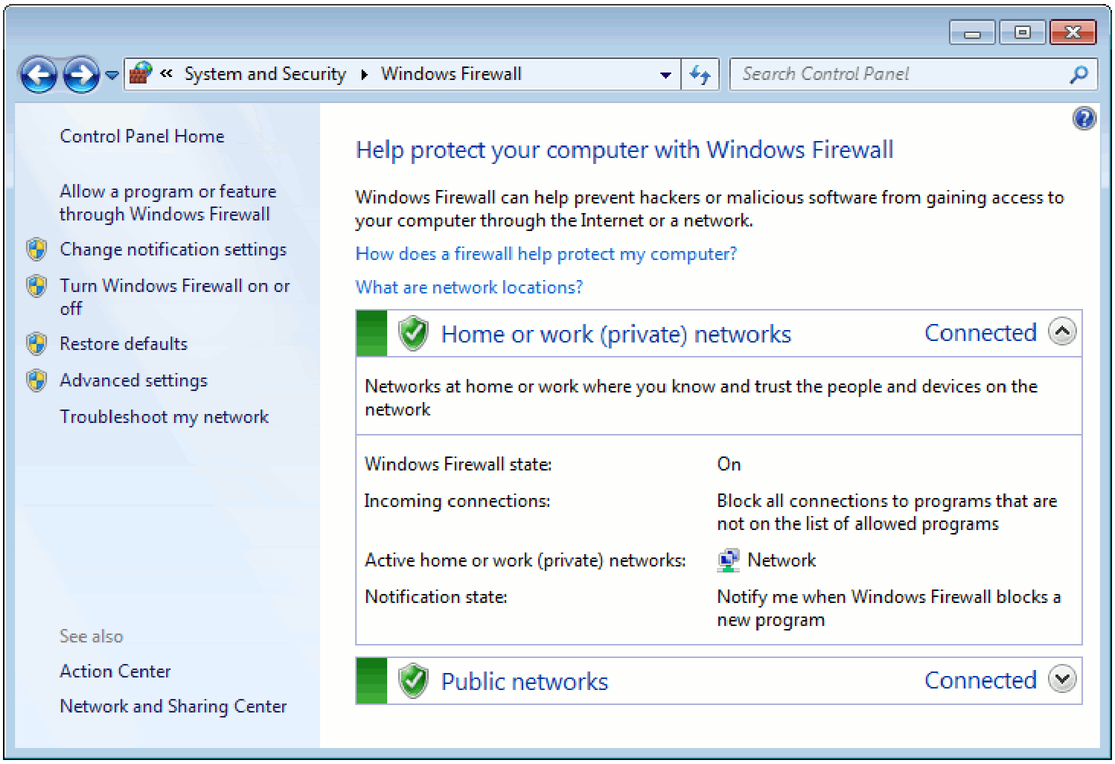
Windows includes a built-in firewall controlling data transfers between your computer and other computers over the network or Internet. The firewall lets users specify trusted programs that are allowed to transfer information between the local computer and certain remote computers, while blocking requests that come from other programs and computers.

When a test is running, it exchanges data with the test engine through a port. By default, it is port 2377. Therefore, you need to configure the firewall to allow traffic through the port to run tests successfully.

Checking if Firewall Is Running

To find out whether Windows Firewall is running:

- Open the Control Panel by clicking Start and then clicking Control Panel.
- In the search box, type Firewall and then select the Windows Firewall applet. The Windows Firewall window will open.


« System and Security ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Home or work (private) networks — Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active home or work (private) networks:	Network
Notification state:	Notify me when Windows Firewall blocks a new program

Public networks — Connected

H. Resources/Equipment Required

Sr.No.	Instrument/Equipment /Components/Trainer kit	Specification	Quantity
1	*Computer system with operating system*		*1*

I. Safety and necessary Precautions followed:

a. *Turn off power switch only after computer is shut down.*

b. *Do not plug out any computer cables*

J. Procedure:

Configure Squid proxy:

To configure a Squid proxy to deny access to specific websites, you'll need to modify the Squid configuration file (squid.conf). Here's a step-by-step guide to achieve this:

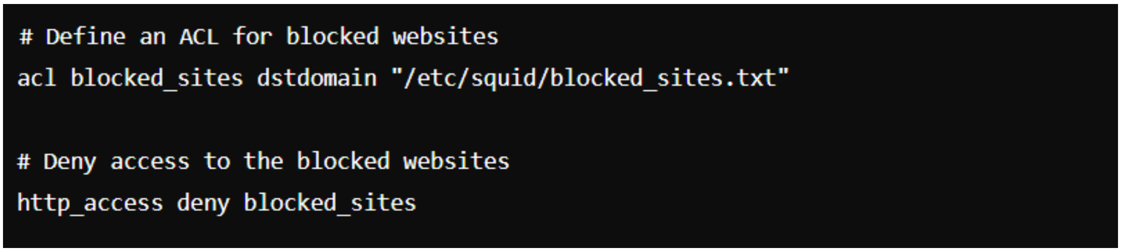
Locate the Squid Configuration File:
Typically, the Squid configuration file is located at /etc/squid/squid.conf or /etc/squid3/squid.conf, depending on your distribution and Squid version.

Open the Squid Configuration File:
Open the file in a text editor with superuser privileges.

Define the Websites to Block:
You can create a list of domains to block by specifying them in a separate file. For instance, create a file called blocked_sites.txt

Add the domains you want to block, one per line:
example.com
badwebsite.com
anotherbadwebsite.com

Modify the Squid Configuration:
Add the following lines to your squid.conf file to reference the list of blocked sites and to deny access to them:

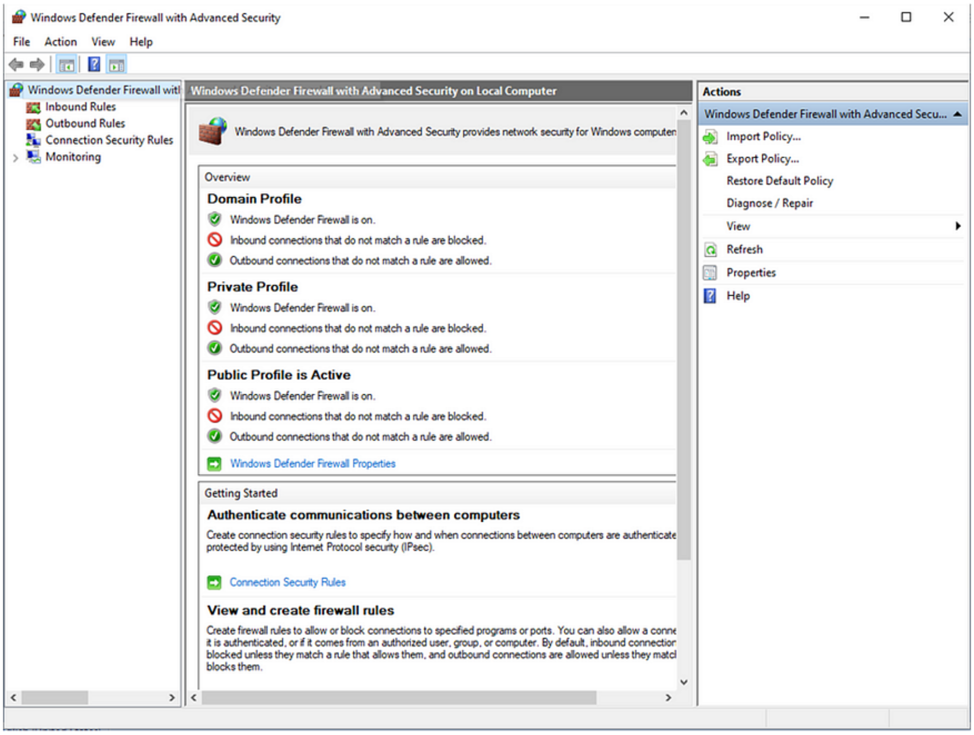


```
# Define an ACL for blocked websites
acl blocked_sites dstdomain "/etc/squid/blocked_sites.txt"

# Deny access to the blocked websites
http_access deny blocked_sites
```

Ensure these lines are placed before any http_access allow directives that could allow access.
After making these changes, restart the Squid service to apply the new configuration

Configure Windows Firewall to block url:

1. Click on Windows Defender Firewall in Control Panel.
2. You will find the "Advanced Settings" option on the left pane. Just click it. A new window will appear


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Defender Firewall with Advanced Security on Local Computer
Actions
Windows Defender Firewall with Advanced Secu...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help

Windows Defender Firewall with Advanced Security provides network security for Windows computer

Overview

Domain Profile

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile is Active

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

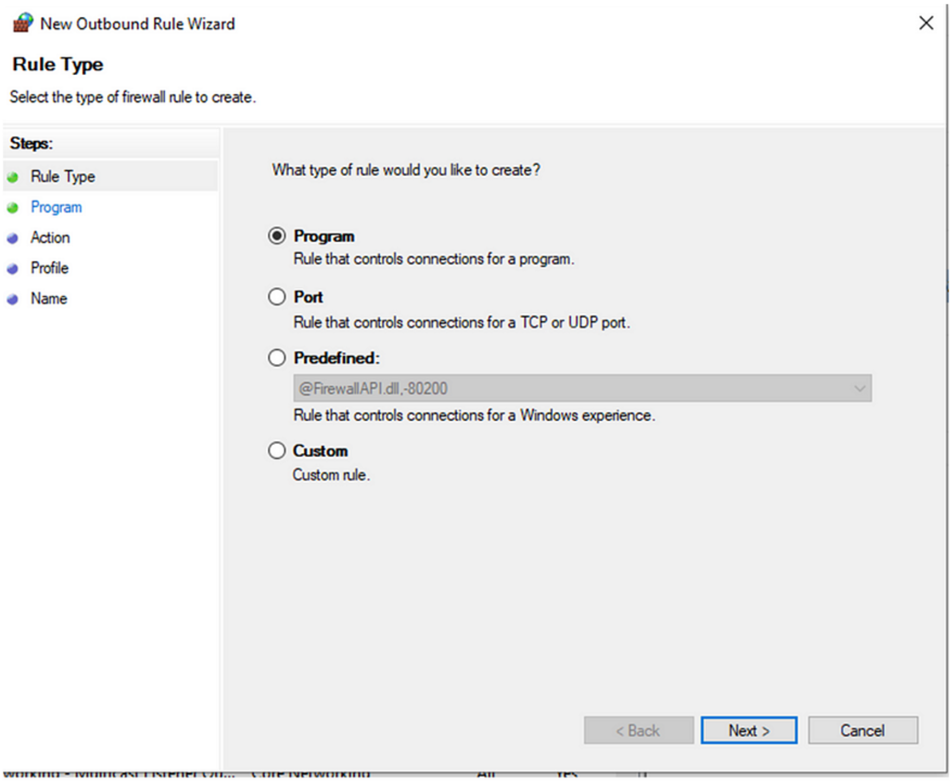
Create connection security rules to specify how and when connections between computers are authenticate protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a conne it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connectior blocked unless they match a rule that allows them, and outbound connections are allowed unless they matcl blocks them.

3. The left pane displays the Inbound Rules and Outbound Rules rules. The traffic that is permitted to the server on which ports and from which sources is determined by inbound firewall rules. Outbound firewall rules specify which ports and destinations are permitted for traffic to exit the server. A list of rules appears when you click on Outbound Rules in the left pane.
4. To create a new rule, select "New Rule" from the right pane. The Wizard for New Outbound Rules will launch.



New Outbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

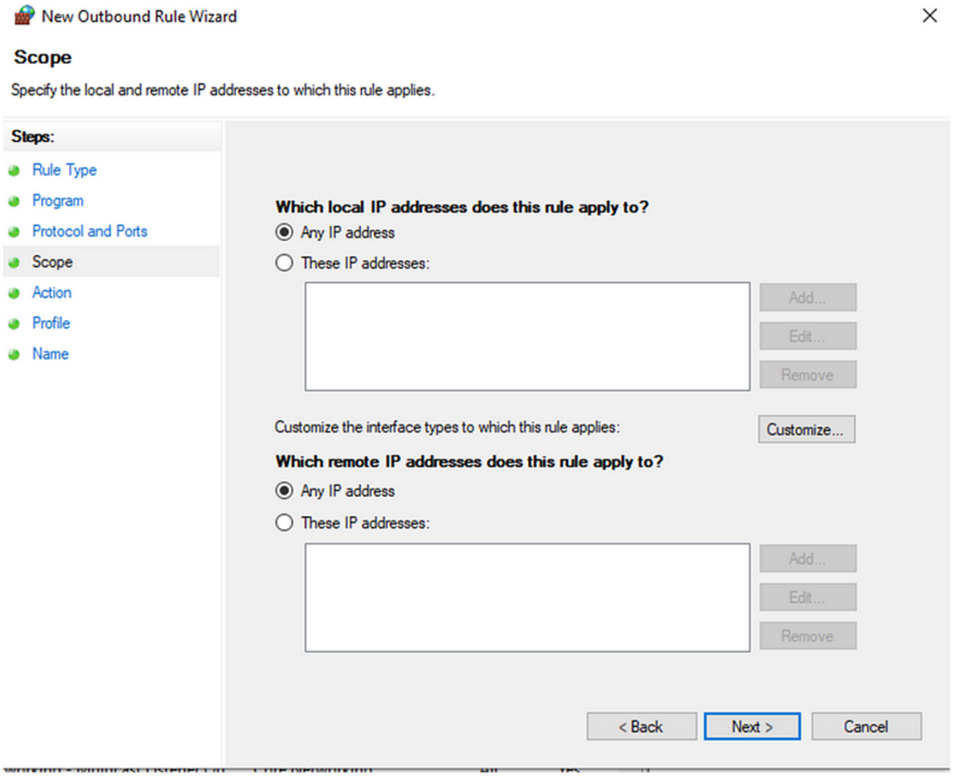
● **Program**
Rule that controls connections for a program.

○ **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
@FirewallAPI.dll,-80200
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

5. Click on Custom rule -> Next. You will reach Program Step -> Next. You will reach Protocol and Ports Step -> Next. When you get to the Scope stage, you must input the IP address of the website you want to block.



New Outbound Rule Wizard

Scope

Specify the local and remote IP addresses to which this rule applies.

Which local IP addresses does this rule apply to?

● Any IP address

○ These IP addresses:

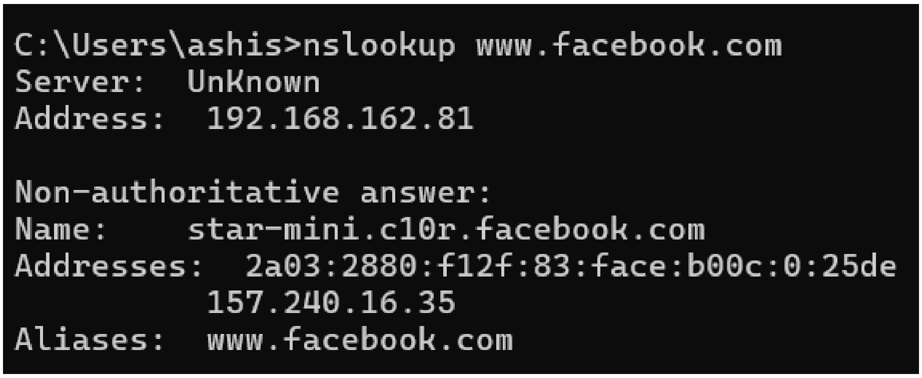
Customize the interface types to which this rule applies:

Which remote IP addresses does this rule apply to?

● Any IP address

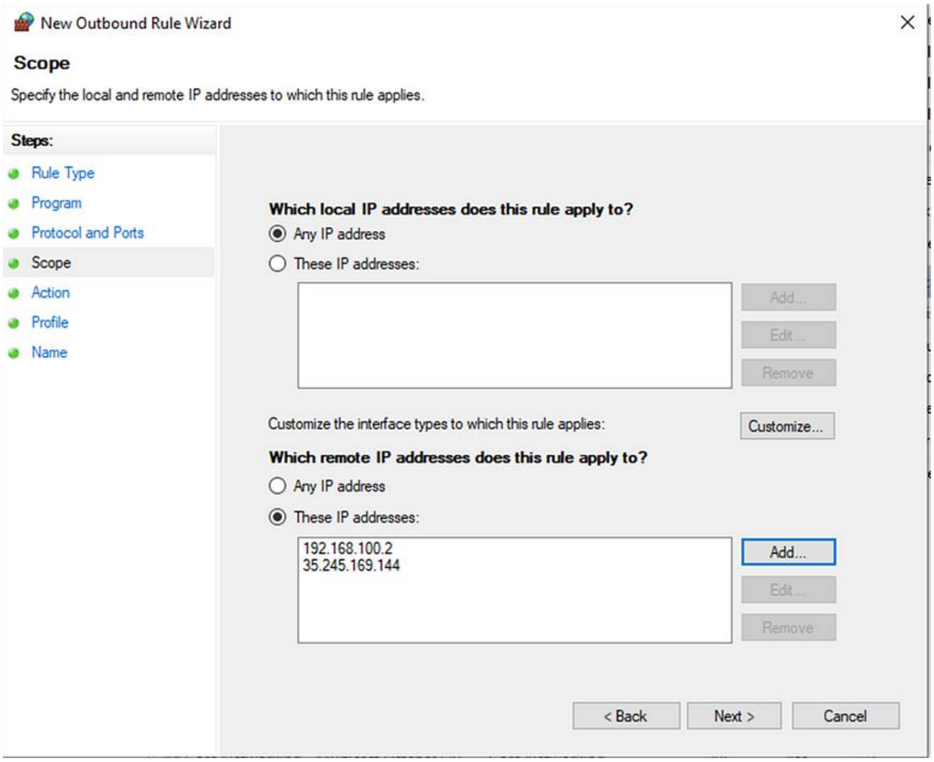
○ These IP addresses:

6. Let's say, I want to block this www.facebook.com I need to find it's IP address. To find IP address of any site, we can use nslookup command.



```
C:\Users\ashis>nslookup www.facebook.com
Server:  UnKnown
Address:  192.168.162.81

Non-authoritative answer:
Name:    star-mini.c10r.facebook.com
Addresses:  2a03:2880:f12f:83:face:b00c:0:25de
          157.240.16.35
Aliases:  www.facebook.com
```

7. Now that we got IP address, we can add this to the dialog box. Select "These IP addresses" in "Which remote IP addresses does this rule apply to?" section and click on Add.



New Outbound Rule Wizard

Scope

Specify the local and remote IP addresses to which this rule applies.

Which local IP addresses does this rule apply to?

● Any IP address

○ These IP addresses:

Customize the interface types to which this rule applies:

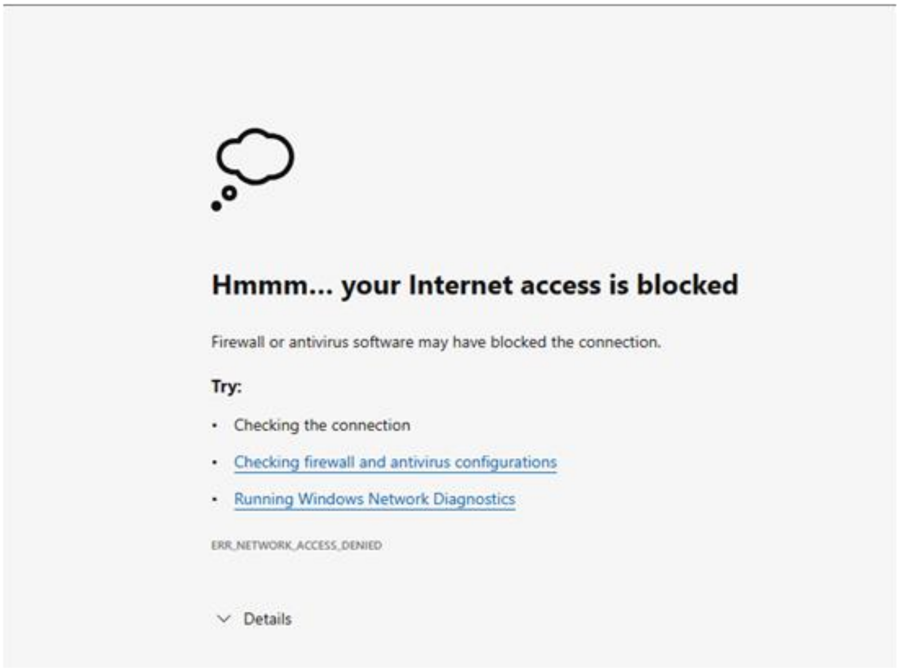
Which remote IP addresses does this rule apply to?

○ Any IP address

● These IP addresses:

192.168.100.2
35.245.169.144

8. Click on Next. Select ‘Block the connection’.
9. Press Next. You’ll get to the Profile step. Choose Next. Give this rule a name, then click Finish. Here we have given “demo” name.
10. Now check if the rule has been applied or not by trying to access that site.
11. Now check if the rule has been applied or not by trying to access that site.



Hmmm... your Internet access is blocked

Firewall or antivirus software may have blocked the connection.

Try:

- Checking the connection
- Checking firewall and antivirus configurations
- Running Windows Network Diagnostics

ERR_NETWORK_ACCESS_DENIED

Similarly, we can also block any port.

K. Observation:

L. Practical related Quiz:

1. What is the primary function of a Squid proxy server?
   - A) To provide antivirus protection
   - B) To cache web content and filter network traffic
   - C) To encrypt network communications
   - D) To monitor email traffic
2. Which of the following is a key feature of the Windows firewall?
   - A) Blocking spam emails
   - B) Encrypting internet traffic

C) Controlling incoming and outgoing network traffic based on predetermined security rules

D) Providing cloud storage solutions

3. In network security, what is the main purpose of blocking unauthorized network traffic?

A) To speed up internet connection

B) To reduce data storage costs

C) To prevent cyber attacks and unauthorized access

D) To increase bandwidth usage

4. What should be the first step in troubleshooting if the Squid proxy is not blocking certain websites as expected?

A) Restart the computer

B) Check the Squid configuration file for correct rules

C) Reinstall Squid

D) Disable the firewall

5. Which Windows utility can be used to monitor and analyze real-time network traffic?

A) Task Manager

B) Resource Monitor

C) Disk Management

D) Event Viewer

M. References / Suggestions:

a. https://www.alphr.com/block-websites-windows/

b. https://cloudinfrastructureservices.co.uk/how-to-block-websites-using-squid-proxy-server/

N. Assessment-Rubrics

Sr No.	Performance Indicators	Weightage in %	Marks	Obtained Marks
1	Analyse and identify suitable approach for problem solving	25	0-5	
2	Use of appropriate technology / software / tools	25	0-5	
3	Demonstrate problems as per instructions	20	0-5	
4	Interpret the result and conclusion	15	0-5	
5	Prepare a report/presentation for given problem	15	0-5	
	Total	**100**	**25**	

Sign with Date

Date: …………..

Practical No.6: Create a Simple Packet Filter Script using pydivert package in python.

A. **Objective:**

To create a basic packet filter script using the pydivert package in Python, which intercepts, analyzes, and potentially modifies network packets based on predefined criteria.

B. **Expected Program Outcomes (POs)**

PO1,PO2,PO3

C. **Expected Skills to be developed based on competency:**

This practical is expected to develop the following skills for the industry-identified competency:

1. Network Programming Proficiency: Developing the ability to intercept, analyze, and manipulate network packets using the pydivert package, which enhances understanding of low-level network operations and packet handling.
2. Python Scripting Expertise: Gaining practical experience in writing Python scripts for real-time network packet filtering and modification, improving coding skills and familiarity with Python libraries related to networking.

D. **Expected Course Outcomes(Cos)**

CO2: Implement security strategy encompassing authentication, authorization, defense against malicious software.

E. **Practical Outcome(PRo)**

Students will be able to create and deploy a simple packet filtering script using the pydivert package in Python, enabling them to intercept, analyze, and modify network packets based on specified rules, thus demonstrating an understanding of network security and packet manipulation techniques.

F. **Expected Affective domain Outcome(ADos)**

1. Increased Attentiveness to Network Security: Students will develop a heightened awareness of network security principles and the importance of monitoring and filtering network traffic to prevent malicious activities and ensure data integrity.
2. Enhanced Confidence in Technical Problem-Solving: By successfully creating and implementing a packet filter script, students will build confidence in their ability to tackle complex technical challenges and apply theoretical knowledge to practical, real-world scenarios in network management and security.

G. **Prerequisite Theory:**

Introduction to Packet Filtering

Packet filtering is a network security mechanism that controls the flow of data packets to and from a network. It involves inspecting the packets and making decisions based on a set of rules, such as allowing or blocking traffic based on IP addresses, port numbers, or protocols. Packet filtering is essential for protecting networks from unauthorized access, malware, and other security threats.

Overview of pydivert

PyDivert is a Python package that provides bindings to WinDivert, a Windows packet capture and manipulation library. WinDivert allows interception and modification of network packets at various stages of their journey through the network stack. PyDivert makes it possible to perform these tasks using Python, enabling the development of network applications such as firewalls, traffic analyzers, and packet injectors.

Key Concepts in Packet Filtering

Packet Interception: The process of capturing packets as they pass through the network stack. This can be done at different layers of the OSI model, depending on the requirements of the application.

Packet Analysis: Examining the contents of captured packets to determine their characteristics, such as source and destination IP addresses, port numbers, and protocols.

Packet Modification: Altering the contents of packets before allowing them to continue to their destination. This can be used to change packet headers, inject new data, or drop packets entirely.

Packet Forwarding: Deciding whether to allow a packet to proceed to its destination based on predefined rules. Packets can be dropped, redirected, or passed through without modification.

Installation of pydivert:

The pydivert package needs to be installed in the Python environment. This can be done using the pip package manager:

```
pip install pydivert
```

Defining a Filter

A filter is used to specify which packets to capture. The filter syntax is similar to that used by popular packet capture tools like Wireshark and tcpdump.

```
filter = "tcp.DstPort == 80"  # Capture only TCP packets destined for port 80 (HTTP)
```

Opening a Handle

Create a WinDivert object with the specified filter to start capturing packets:

```
with pydivert.WinDivert(filter) as w:
    # Packet processing code goes here
```

Intercepting and Processing Packets

Within the handle context, use a loop to capture and process packets. You can analyze, modify, or simply log the packet details.

```
with pydivert.WinDivert(filter) as w:
    print("Starting packet capture...")
    for packet in w:
        # Print packet details
        print(packet)

        # Optionally, modify the packet
        # packet.tcp.payload = b"Modified Payload"

        # Forward the packet
        w.send(packet)
```

H. Resources/Equipment Required

Sr. No.	Instrument/Equipment /Components/Trainer kit	Specification	Quantity
1	*Computer system with operating system*		*1*
2.	*Python IDLE*		*1*

I. Safety and necessary Precautions followed

1. *Turn off power switch only after computer is shut down.*
2. *Do not plug out any computer cables*

J. Source code :

Create a code to drop packets destined for port 443.

K. Input-Output :

Run above code and try to open website.

L. Practical related Quiz.

1. What is the purpose of PyDivert in Python?
   A) Interacting with databases
   B) Manipulating network packets
   C) Generating graphical user interfaces
   D) Analyzing image files

2. What does the WinDivert object represent in PyDivert?
   A) A database connection
   B) A file handle

C) A network interface
D) A handle to the network stack

3. How does the provided PyDivert script determine whether to block or allow a packet?
   A) By checking the packet payload
   B) By inspecting the packet headers
   C) By analyzing the packet routing table
   D) By querying a remote server

M. References / Suggestions:

1. https://pythonhosted.org/pydivert/
2. https://aidan-walz.medium.com/capturing-and-editing-packets-with-pydivert-4989ea4db316

N. Assessment-Rubrics

Sr No.	Performance Indicators	Weightage in %	Marks	Obtained Marks
1	Analyse and identify suitable approach for problem solving	25	0-5	
2	Use of appropriate technology / software / tools	25	0-5	
3	Demonstrate problems as per instructions	20	0-5	
4	Interpret the result and conclusion	15	0-5	
5	Prepare a report/presentation for given problem	15	0-5	
	Total	**100**	**25**	

Sign with Date

Date: …………..

Practical No.7: Create malicious script for generating multiple folders using python.

A. Objective:

To understand and experiment with the creation of a malicious Python script designed to generate multiple folders as a demonstration of potential security vulnerabilities.

B. Expected Program Outcomes (POs)

PO1,PO2,PO3

C. Expected Skills to be developed based on competency:

This practical is expected to develop the following skills for the industry-identified competency:

1. Understanding of Scripting Vulnerabilities: Recognizing the potential security risks associated with scripting languages like Python, including the ability to identify and mitigate vulnerabilities such as unauthorized folder creation.
2. Ethical Hacking Awareness: Gaining insights into how malicious actors might exploit scripting capabilities to perform unauthorized actions on a system, thereby fostering a proactive mindset towards cybersecurity and ethical hacking practices.

D. Expected Course Outcomes(Cos)

CO2: Implement security strategy encompassing authentication, authorization, defense against malicious software.

E. Practical Outcome(PRo)

Students will be able to create a Python script that can generate multiple folders, thereby gaining insight into potential security vulnerabilities and the importance of safeguarding against unauthorized file system manipulation.

F. Expected Affective domain Outcome(ADos)

1. Increased Awareness of Ethical Implications: Students may develop a heightened sensitivity to the ethical implications of scripting vulnerabilities, understanding the potential harm that can arise from unauthorized actions on a system.
2. Enhanced Sense of Responsibility: Engaging in activities that demonstrate the potential impact of malicious scripting may foster a greater sense of responsibility towards cybersecurity practices, encouraging students to prioritize security measures in their programming endeavors.

G. Prerequisite Theory:

Creating folders infinitely can serve as an exercise to understand the basics of programming loops, file system operations, and program control flow. Let's break down the key concepts involved:

- Loops: In Python, loops are used to execute a block of code repeatedly. There are mainly two types of loops:
    - While loop: Executes a block of code as long as the specified condition is true.
    - For loop: Executes a block of code for each item in an iterable object, such as lists, tuples, or strings.
- File System Operations: In this case, we're interacting with the file system to create folders. Python provides the os module, which includes functions for interacting with the operating system, including file and directory manipulation.
- Infinite Loop: An infinite loop is a loop that continues to execute indefinitely because the loop condition is always true. This can be useful in certain scenarios but should be used with caution to prevent unintended consequences, such as consuming excessive system resources or causing the program to hang.
- Termination: In a practical scenario, it's important to consider how to terminate the infinite loop. This could be achieved by adding a condition to break out of the loop based on a certain criteria, such as reaching a maximum number of iterations, user input, or external signals.

The os module in Python provides a portable way of using operating system-dependent functionality. Here's an explanation of the functions used in the script:

os.makedirs():

This function is used to recursively create directories.

Syntax: os.makedirs(path, mode=0o777, exist_ok=False)

path: The path at which directories need to be created. It can be absolute or relative.

mode: The permissions to be set for the directories. It is an octal number.

exist_ok: If exist_ok is True, the function does not raise an error if the directory already exists. If False (default), it raises a FileExistsError.

os.path.join():

This function is used to join one or more path components intelligently.

Syntax: os.path.join(path1[, path2[, ...]])

path1, path2, ...: Components of the path to be joined.

H. Resources/Equipment Required

Sr. No.	Instrument/Equipment /Components/Trainer kit	Specification	Quantity
1	*Computer system with operating system*		*1*
2.	*Python IDLE*		*1*

I. Safety and necessary Precautions followed

1. *Turn off power switch only after computer is shut down.*
2. *Do not plug out any computer cables*

J. Source code :

K. Input-Output :

L. Practical related Quiz.

1. Which Python module is used for interacting with the operating system, including file and directory manipulation?
   A) sys
   B) os
   C) io
   D) pathlib

2. What is the purpose of the os.makedirs() function in Python?
   A) Remove directories
   B) List directories
   C) Create directories recursively
   D) Rename directories

3. Which function is used to intelligently join one or more path components in Python?
   A) os.path.combine()
   B) os.path.join()
   C) os.path.concatenate()
   D) os.path.merge()

M. References / Suggestions:

1. https://www.geeksforgeeks.org/make-multiple-directories-based-on-a-list-using-python/
2. https://infosecwriteups.com/make-a-self-replicating-virus-in-python-bb29404e3f6b

N. Assessment-Rubrics

Sr No.	Performance Indicators	Weightage in %	Marks	Obtained Marks
1	Analyse and identify suitable approach for problem solving	25	0-5	
2	Use of appropriate technology / software / tools	25	0-5	
3	Demonstrate problems as per instructions	20	0-5	
4	Interpret the result and conclusion	15	0-5	
5	Prepare a report/presentation for given problem	15	0-5	
	Total	**100**	**25**	

Sign with Date

Date: …………..

Practical No.8: Create malicious script for keylogger using python. (use pynput package).

A. **Objective:**

To develop a keylogger script using Python with the pynput package to understand and demonstrate the principles of keystroke logging for educational purposes.

B. **Expected Program Outcomes (POs):**

PO1,PO2,PO3

C. **Expected Skills to be developed based on competency:**

This practical is expected to develop the following skills for the industry-identified competency:

1. Proficiency in Python programming: This practical will enhance the participant's ability to write Python scripts, including understanding syntax, utilizing libraries, and implementing advanced functionalities such as keylogging.
2. Understanding of cybersecurity concepts: By creating a keylogger, participants will gain insights into the methods used in cybersecurity attacks, including the importance of securing sensitive information and the potential risks associated with unauthorized access to keystroke data.

D. **Expected Course Outcomes(Cos)**

CO2: Implement security strategy encompassing authentication, authorization, defense against malicious software.

E. **Practical Outcome(PRo)**

Students will be able to develop a Python script utilizing the pynput package to create a keylogger capable of capturing and logging keystrokes, thereby gaining practical experience in cybersecurity techniques and enhancing their proficiency in Python programming.

F. **Expected Affective domain Outcome(ADos)**

1. Increased awareness of cybersecurity risks: By engaging in the creation of a keylogger, students may develop a deeper understanding of the potential vulnerabilities associated with keystroke logging, leading to heightened vigilance in safeguarding personal and sensitive information online.
2. Ethical considerations in technology usage: Through reflection on the implications of keylogging and the potential ethical dilemmas it poses, students may develop a greater sense of responsibility and ethical awareness regarding the use of technology and data privacy.

G. **Prerequisite Theory:**

Keylogging:

Keylogging is a cybersecurity technique used to monitor and record keystrokes made by a user on a computer or mobile device. It can be used for various purposes, including security auditing, parental control, and malicious activities such as identity theft or unauthorized access. Keyloggers can operate at different levels of the system, capturing keystrokes before they reach the operating system (kernel-level) or at the application level.

pynput Module:

The pynput module is a Python library that allows for controlling and monitoring input devices such as keyboards and mice. It provides functionalities to listen for and capture events like keystrokes and mouse movements. The module includes classes like Keyboard and Listener, which enable developers to interact with keyboards and capture input events efficiently.

- **Keyboard Listener:** The Listener class provided by the pynput module allows developers to monitor keyboard events such as key presses and releases. By creating a keyboard listener instance and defining callback functions, one can capture and process keystrokes in real-time.

- **Event Handling:** The pynput module handles events asynchronously, meaning it can listen for input events without blocking the execution of the main program. This allows for the creation of responsive keylogging scripts that do not interfere with other tasks or processes running on the system.

- **Cross-Platform Compatibility:** The pynput module is designed to work on multiple operating systems, including Windows, macOS, and Linux, making it a versatile choice for developing platform-independent keyloggers.

H. Resources/Equipment Required

Sr. No.	Instrument/Equipment /Components/Trainer kit	Specification	Quantity
1	*Computer system with operating system*		*1*
2.	*Python IDLE*		*1*

I. Safety and necessary Precautions followed

1. *Turn off power switch only after computer is shut down.*
2. *Do not plug out any computer cables*

J. Source code :

K. Input-Output :

L. Practical related Quiz.

1. What is the primary purpose of a keylogger?
   A) To enhance system performance
   B) To monitor and record keystrokes
   C) To block unauthorized access
   D) To display graphical user interfaces

2. Which of the following is a class provided by the pynput module to monitor keyboard events?
   - A) Mouse
   - B) Listener
   - C) EventHandler
   - D) Recorder
3. Which of the following is an example of an ethical use of a keylogger?
   - A) Recording keystrokes on a public computer without permission
   - B) Monitoring employee activity with their knowledge and consent
   - C) Stealing passwords and sensitive information
   - D) Installing it on a friend's computer without informing them
4. Why is it important to consider ethical implications when creating a keylogger?
   - A) To ensure the script runs efficiently
   - B) To prevent legal consequences and respect privacy
   - C) To enhance programming skills
   - D) To improve computer security

M. References / Suggestions:

1. https://www.fortinet.com/resources/cyberglossary/what-is-keyloggers
2. https://www.geeksforgeeks.org/how-to-use-pynput-to-make-a-keylogger/

N. Assessment-Rubrics

Sr No.	Performance Indicators	Weightage in %	Marks	Obtained Marks
1	Analyse and identify suitable approach for problem solving	25	0-5	
2	Use of appropriate technology / software / tools	25	0-5	
3	Demonstrate problems as per instructions	20	0-5	
4	Interpret the result and conclusion	15	0-5	
5	Prepare a report/presentation for given problem	15	0-5	
	Total	**100**	**25**	

Sign with Date

Date: …………..

Practical No.9: Use Nmap to scan a network and identify open ports on a web server/other PC, then configure a firewall to block all ports except essential ones (e.g., 80 and 443), and use Nmap again to verify the configuration.

A. Objective:

To use Nmap to identify open ports on a web server, configure a firewall to block all non-essential ports, and verify the configuration by using Nmap to ensure only essential ports (e.g., 80 and 443) remain open.

B. Expected Program Outcomes (POs):

PO1,PO2,PO3,PO4

C. Expected Skills to be developed based on competency:

This practical is expected to develop the following skills for the industry-identified competency:

1. Network Scanning and Analysis: Developing the ability to effectively use Nmap for identifying open ports and services on a web server.
2. Firewall Configuration and Management: Gaining proficiency in configuring and managing firewall rules to control network traffic, specifically allowing only essential ports to be accessible.

D. Expected Course Outcomes(Cos)

CO3: Secure web communications and applications by applying security protocols, managing ports, and implementing HTTPS, SSH, and VPN technologies.

E. Practical Outcome(PRo)

Students will be able to proficiently scan a network to identify open ports using Nmap, configure firewall rules to restrict network traffic to essential services, and verify the effectiveness of the firewall configuration through subsequent Nmap scans.

F. Expected Affective domain Outcome(ADos)

1. Attention to Detail: Demonstrating thoroughness and precision in network scanning and firewall configuration to ensure security measures are correctly implemented.
2. Proactive Security Mindset: Cultivating a proactive approach to network security by regularly monitoring, identifying potential vulnerabilities, and taking necessary actions to mitigate risks.

G. Prerequisite Theory:

Network Scanning: Network scanning is a process used to discover active devices on a network and gather information about them, such as their IP addresses, operating systems, and open ports. It is a crucial step in network security, helping to identify potential vulnerabilities that could be exploited by attackers.

Nmap (Network Mapper): Nmap is a powerful, open-source network scanning tool used for network discovery and security auditing. It is widely utilized by network administrators for various tasks, including:

- Host Discovery: Identifying active devices on a network.
- Port Scanning: Enumerating open ports on target devices to determine which services are running.
- Service Version Detection: Identifying the version of services running on open ports.
- OS Detection: Determining the operating system of a target device.
- Vulnerability Scanning: Identifying known vulnerabilities in services running on the network.

Nmap works by sending specially crafted packets to the target system and analyzing the responses to infer various characteristics and statuses of the network and its devices.

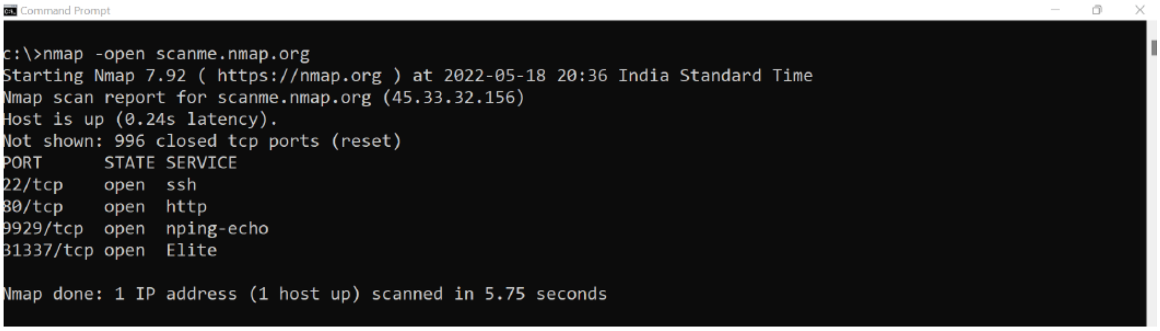
Scanning Port using Nmap tool

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.

Link to download nmap-7.95 for windows platform:
https://nmap.org/dist/nmap-7.95-setup.exe

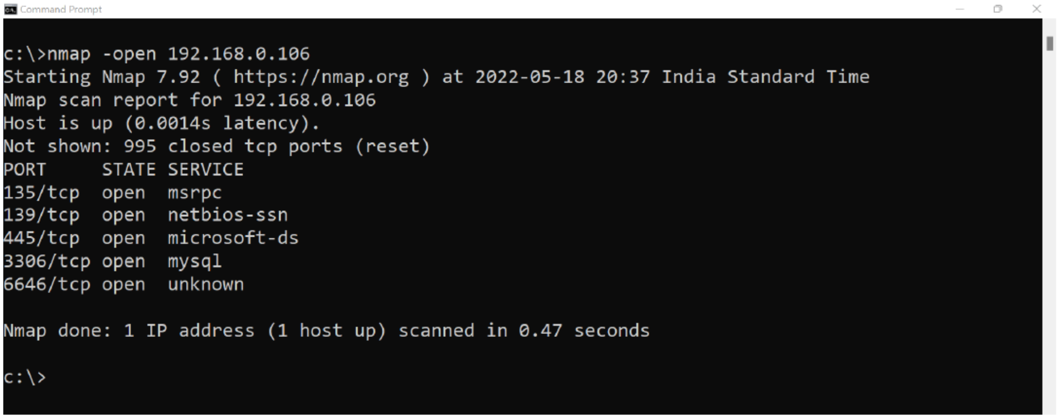
Afte downloading install it. Then run following commands

1) Scan open ports (syntax: nmap –open ip_address / url)



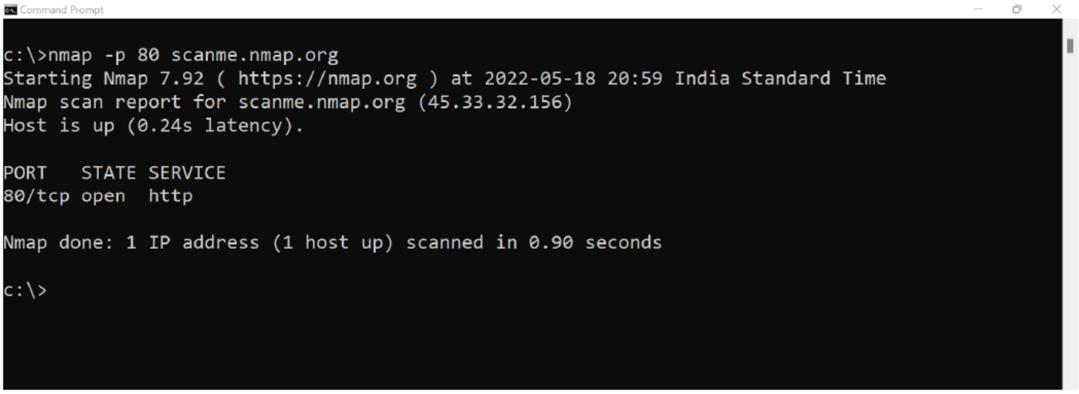
```
c:\>nmap -open scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-18 20:36 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.24s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 5.75 seconds
```

Scanning port with the IP Address.



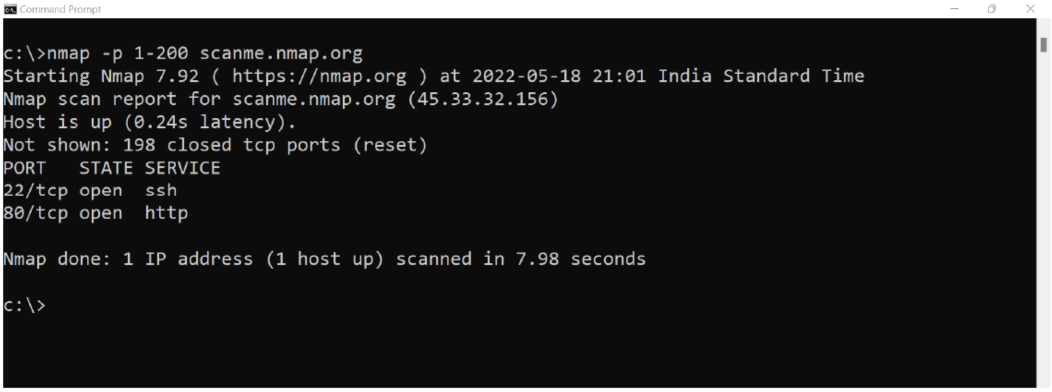
```
c:\>nmap -open 192.168.0.106
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-18 20:37 India Standard Time
Nmap scan report for 192.168.0.106
Host is up (0.0014s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
6646/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds

c:\>
```

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



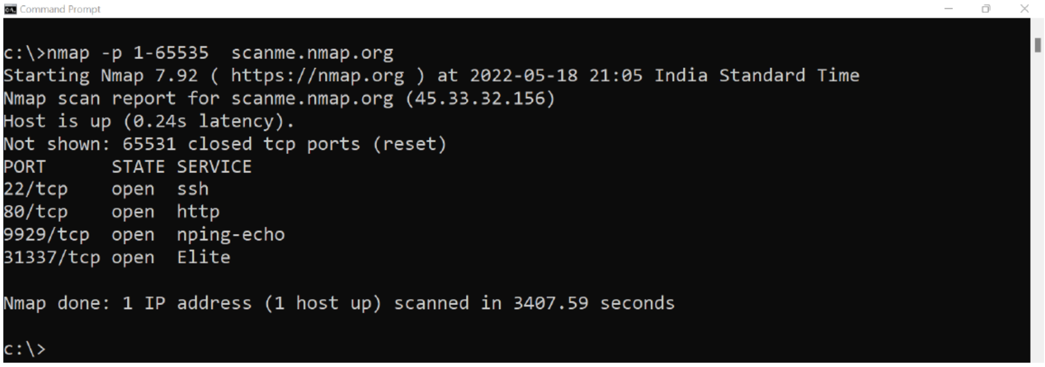
```
c:\>nmap -p 80 scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-18 20:59 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.24s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.90 seconds

c:\>
```

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



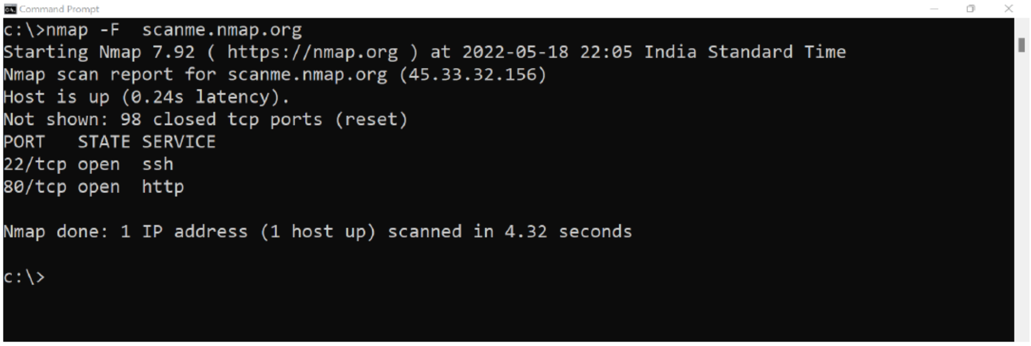
```
c:\>nmap -p 1-200 scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-18 21:01 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.24s latency).
Not shown: 198 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 7.98 seconds

c:\>
```

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



```
c:\>nmap -p 1-65535  scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-18 21:05 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.24s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 3407.59 seconds

c:\>
```

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



```
c:\>nmap -F  scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-18 22:05 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.24s latency).
Not shown: 98 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 4.32 seconds

c:\>
```

Network scanning using Nmap tool:

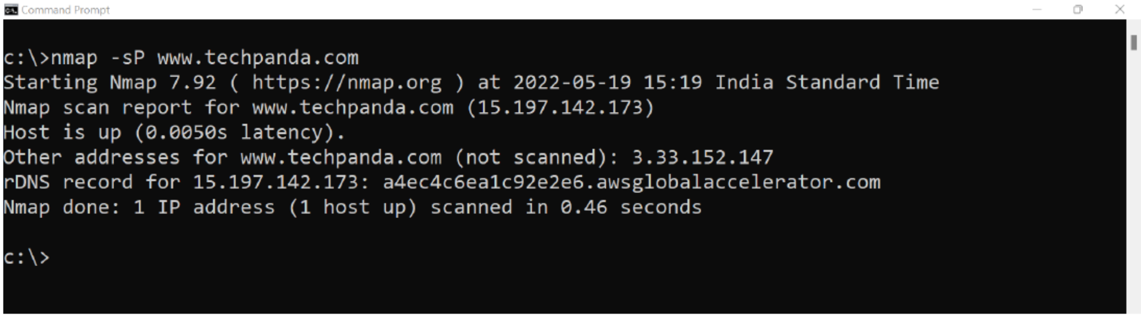
Network scanning is a technique that is used to gather information regarding computing systems by making the use of a computer network. Network scanning is mainly used for security assessment, system maintenance, and also for performing attacks by hackers.

The purpose of network scanning is as follows:

- Recognize available UDP and TCP network services running on the targeted hosts
- Recognize filtering systems between the user and the targeted hosts
- Determine the operating systems (OSs) in use by assessing IP responses
- Evaluate the target host's TCP sequence number predictability to determine sequence prediction attack and TCP spoofing.

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.

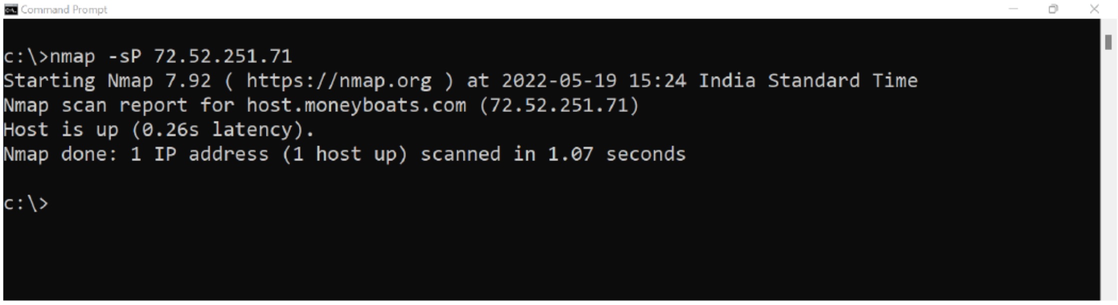
Syntax: nmap -sP <IP Address>



```
c:\>nmap -sP www.techpanda.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-19 15:19 India Standard Time
Nmap scan report for www.techpanda.com (15.197.142.173)
Host is up (0.0050s latency).
Other addresses for www.techpanda.com (not scanned): 3.33.152.147
rDNS record for 15.197.142.173: a4ec4c6ea1c92e2e6.awsglobalaccelerator.com
Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds

c:\>
```

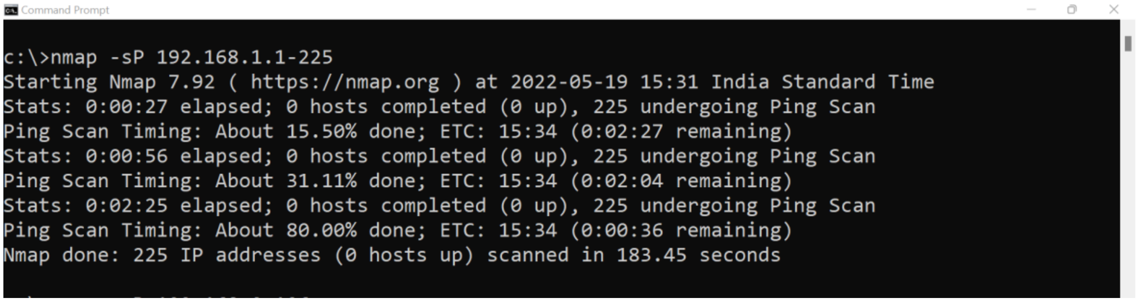
Host Scan – Unlike a ping scan, a host scan actively sends ARP request packets to all the hosts connected to your network. Each host then responds to this packet with another ARP packet containing its status and MAC address. This can be a powerful way of spotting suspicious hosts connected to your network.

Syntax:nmap -sP <target IP Range>



```
c:\>nmap -sP 72.52.251.71
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-19 15:24 India Standard Time
Nmap scan report for host.moneyboats.com (72.52.251.71)
Host is up (0.26s latency).
Nmap done: 1 IP address (1 host up) scanned in 1.07 seconds

c:\>
```

- Host scan Indetifies active host(s) in a network
- It Sends ARP request packets to all systems in the target.
- Host Scan Results, “Host is up” by receiving MAC address from each active host.



```
c:\>nmap -sP 192.168.1.1-225
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-19 15:31 India Standard Time
Stats: 0:00:27 elapsed; 0 hosts completed (0 up), 225 undergoing Ping Scan
Ping Scan Timing: About 15.50% done; ETC: 15:34 (0:02:27 remaining)
Stats: 0:00:56 elapsed; 0 hosts completed (0 up), 225 undergoing Ping Scan
Ping Scan Timing: About 31.11% done; ETC: 15:34 (0:02:04 remaining)
Stats: 0:02:25 elapsed; 0 hosts completed (0 up), 225 undergoing Ping Scan
Ping Scan Timing: About 80.00% done; ETC: 15:34 (0:00:36 remaining)
Nmap done: 225 IP addresses (0 hosts up) scanned in 183.45 seconds
```

H. Resources/Equipment Required

Sr. No.	Instrument/Equipment /Components/Trainer kit	Specification	Quantity
1	*Computer system with operating system*		*1*

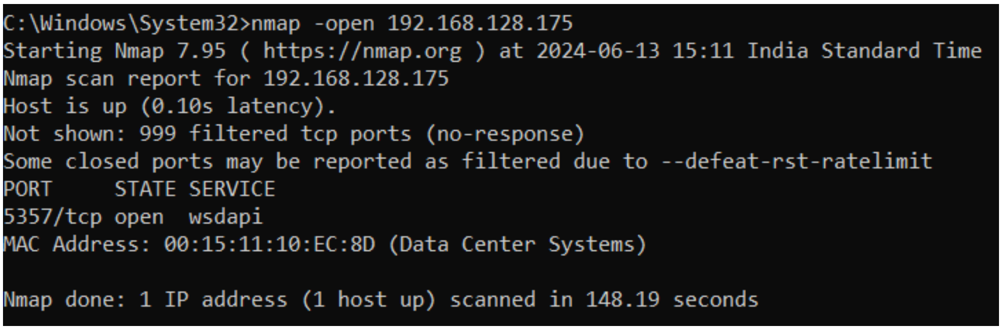
2.	*Python IDLE*		1

I. Safety and necessary Precautions followed

1. *Turn off power switch only after computer is shut down.*
2. *Do not plug out any computer cables*

J. Procedure :

1. Connect two PC/laptop with same hotspot or same LAN.
2. Let IP assigned to PC are 192.168.128.83 and 192.168.128.175
3. Run *nmap -open 192.168.128.175* command on one first PC (192.168.128.83)



```
C:\Windows\System32>nmap -open 192.168.128.175
Starting Nmap 7.95 ( https://nmap.org ) at 2024-06-13 15:11 India Standard Time
Nmap scan report for 192.168.128.175
Host is up (0.10s latency).
Not shown: 999 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 00:15:11:10:EC:8D (Data Center Systems)

Nmap done: 1 IP address (1 host up) scanned in 148.19 seconds
```

4. Find the port number which is open. (here port 5357 is open)
5. Now on other PC using Windows firewall using inbound rule block the connection to port 5357.
6. Now on first PC again run *nmap -open 192.168.128.175* or nmap -p 5357 *192.168.128.175* command and observe the output.
7. Also run the ping scan and host scan commands and observe the output.

K. Input-Output :

L. Practical related Quiz.

1. What is the default port for HTTPS traffic?
   A. 80
   B. 21
   C. 443
   D. 25
2. Which Nmap command would you use to scan all ports on a target machine?
   A. nmap -p 1-65535 <target_ip>

B. nmap -A <target_ip>
C. nmap -O <target_ip>
D. nmap -sV <target_ip>

3. What does the -p option in Nmap specify?
A. The type of scan to perform
B. The ports to scan
C. The target IP address
D. The scan timing template

4. When configuring a firewall, which of the following ports should generally be allowed to enable secure web traffic?
A. 21 and 22
B. 80 and 443
C. 25 and 110
D. 53 and 69

5. What is the purpose of the -O option in Nmap?
A. Service version detection
B. OS detection
C. Scan all ports
D. Enable aggressive scan options

M. References / Suggestions:

1. https://www.action1.com/how-to-block-or-allow-tcp-ip-port-in-windows-firewall/
2. https://builtin.com/articles/nmap-port-scanning

N. Assessment-Rubrics

Sr No.	Performance Indicators	Weightage in %	Marks	Obtained Marks
1	Analyse and identify suitable approach for problem solving	25	0-5	
2	Use of appropriate technology / software / tools	25	0-5	
3	Demonstrate problems as per instructions	20	0-5	
4	Interpret the result and conclusion	15	0-5	
5	Prepare a report/presentation for given problem	15	0-5	
	Total	**100**	**25**	

Sign with Date

Date: …………..

Practical No.10: a) Installation and configuration of Wireshark.
b) Perform Password sniffing using Wireshark. (Analyse GET/POST Request).

A. Objective:

To install and configure Wireshark and then use it to capture and analyze network traffic, specifically to sniff and examine GET/POST requests to identify any transmitted passwords.

B. Expected Program Outcomes (POs)

PO1,PO2,PO3,PO4

C. Expected Skills to be developed based on competency:

This practical is expected to develop the following skills for the industry-identified competency:

1. Proficiency in installing, configuring, and using Wireshark for network traffic analysis.
2. Ability to identify and analyze HTTP GET/POST requests, including detecting potential security vulnerabilities such as plaintext password transmission.

D. Expected Course Outcomes(Cos)

CO3: Secure web communications and applications by applying security protocols, managing ports, and implementing HTTPS, SSH, and VPN technologies.

E. Practical Outcome(PRo)

Students will be able to effectively use Wireshark to capture and analyze network traffic, demonstrating the ability to identify and interpret HTTP GET/POST requests, including any plaintext passwords transmitted, thereby understanding potential security vulnerabilities in network communications.

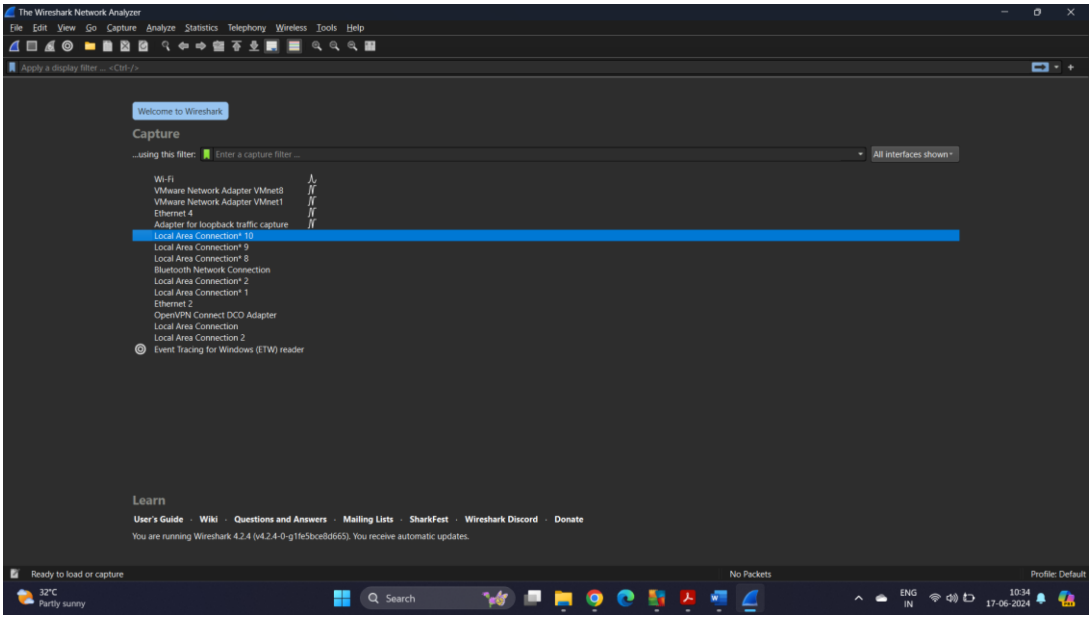
F. Expected Affective domain Outcome(ADos)

1. Develop an increased awareness of the importance of network security and the potential risks associated with unencrypted data transmission.
2. Cultivate a proactive attitude towards implementing best practices in securing sensitive information during network communications.

G. Prerequisite Theory:

Wireshark:

Wireshark is a free open- source network protocol analyzer. It is used for network troubleshooting and communication protocol analysis. Wireshark captures network packets in real time and display them in human-readable format. It provides many advanced features including live capture and offline analysis, three-pane packet browser, coloring rules for analysis. This document uses Wireshark for the experiments, and it covers Wireshark installation, packet capturing, and protocol analysis.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
32°C
Partly sunny
Search
ENG
IN
10:34
17-06-2024

Wi-Fi
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Ethernet 4
Adapter for loopback traffic capture
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
Local Area Connection* 2
Local Area Connection* 1
Ethernet 2
OpenVPN Connect DCO Adapter
Local Area Connection
Local Area Connection 2
Event Tracing for Windows (ETW) reader

You are running Wireshark 4.2.4 (v4.2.4-0-g1fe5bce8d665). You receive automatic updates.

Ready to load or capture · No Packets · Profile: Default

Fig-1- Wireshark home screen on windows

Packet Sniffer

Packet sniffer is a basic tool for observing network packet exchanges in a computer. As the name suggests, a packet sniffer captures ("sniffs") packets being sent/received from/by your computer; it will also typically store and/or display the contents of the various protocol fields in these captured packets. A packet sniffer itself is passive. It observes messages being sent and received by applications and protocols running on your computer, but never sends packets itself.

Figure 2 shows the structure of a packet sniffer. At the right of Figure 2 are the protocols (in this case, Internet protocols) and applications (such as a web browser or ftp client) that normally run on your computer. The packet sniffer, shown within the dashed rectangle in Figure 3 is an addition to the usual software in your computer, and consists of two parts. The packet capture library receives a copy of every link-layer frame that is sent from or received by your computer. Messages exchanged by higher layer protocols such as HTTP, FTP, TCP, UDP, DNS, or IP all are eventually encapsulated in link-layer frames that are transmitted over physical media such as an Ethernet cable. In Figure 1, the assumed physical media is an Ethernet, and so all upper-layer protocols are eventually encapsulated within an Ethernet frame. Capturing all link-layer frames thus gives you access to all messages sent/received from/by all protocols and applications executing in your computer.

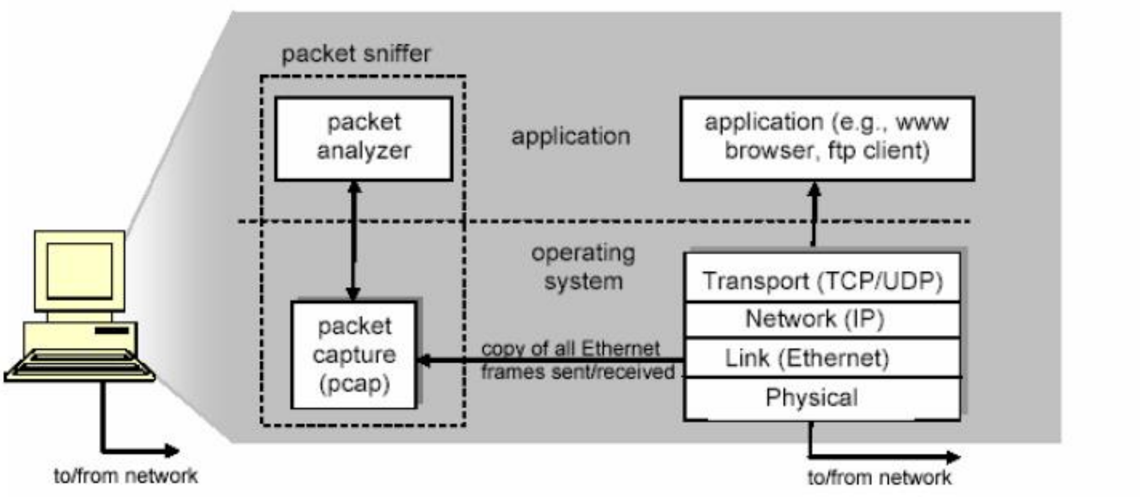
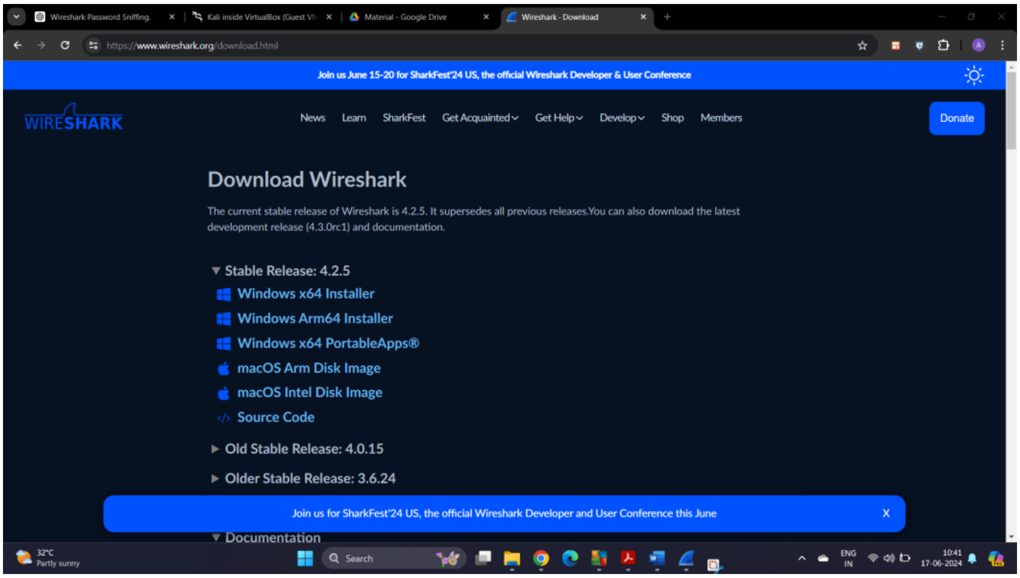


Fig-2-Packet sniffer structure

The second component of a packet sniffer is the packet analyzer, which displays the contents of all fields within a protocol message. In order to do so, the packet analyze must “understand” the structure of all messages exchanged by protocols. For example, suppose we are interested in displaying the various fields in messages exchanged by the HTTP protocol in Figure 2. The packet analyzer understands the format of Ethernet frames, and so can identify the IP datagram within an Ethernet frame. It also understands the IP datagram format, so that it can extract the TCP segment within the IP datagram. Finally, it understands the TCP segment structure, so it can extract the HTTP message contained in the TCP segment. Finally, it understands the HTTP protocol and so, for example, knows that the first bytes of an HTTP message will contain the string “GET,” “POST,” or “HEAD”.

Getting Wireshark:
Wireshark can also be downloaded from here:
https://www.wireshark.org/download.html



Join us June 15-20 for SharkFest'24 US, the official Wireshark Developer & User Conference

Download Wireshark

The current stable release of Wireshark is 4.2.5. It supersedes all previous releases.You can also download the latest development release (4.3.0rc1) and documentation.

▼ Stable Release: 4.2.5
- Windows x64 Installer
- Windows Arm64 Installer
- Windows x64 PortableApps®
- macOS Arm Disk Image
- macOS Intel Disk Image
- Source Code

▶ Old Stable Release: 4.0.15

▶ Older Stable Release: 3.6.24

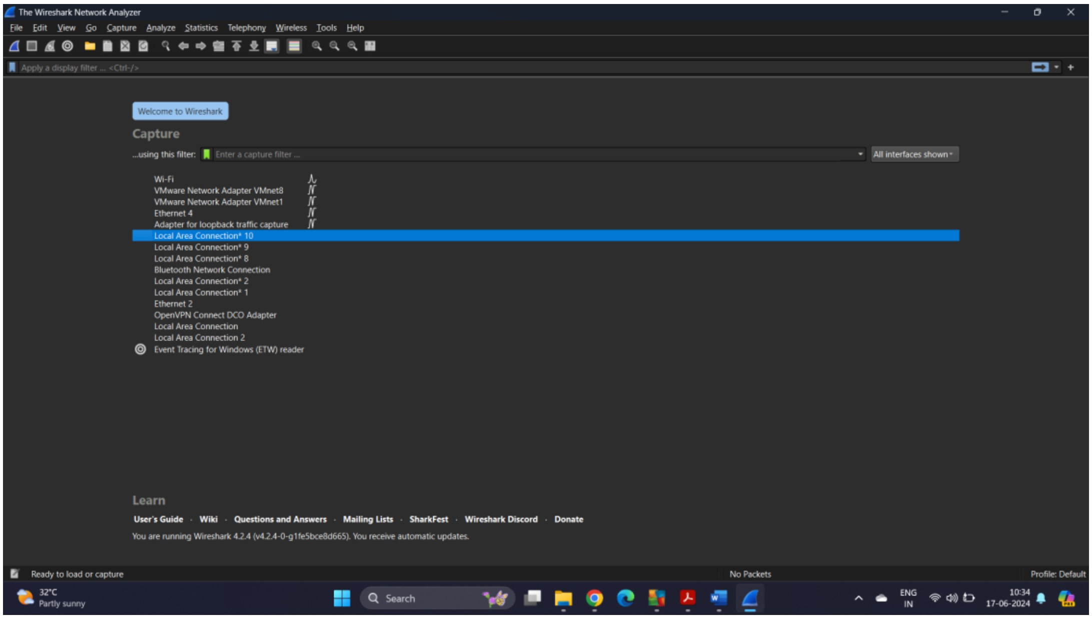
Join us for SharkFest'24 US, the official Wireshark Developer and User Conference this June X

▼ Documentation

Fig-3- Wireshark download page

Starting Wireshark

When you run the Wireshark program, the Wireshark graphic user interface will be shown as Figure 4. Currently, the program is not capturing the packets.


The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
32°C
Partly sunny
Search
ENG
IN
10:34
17-06-2024

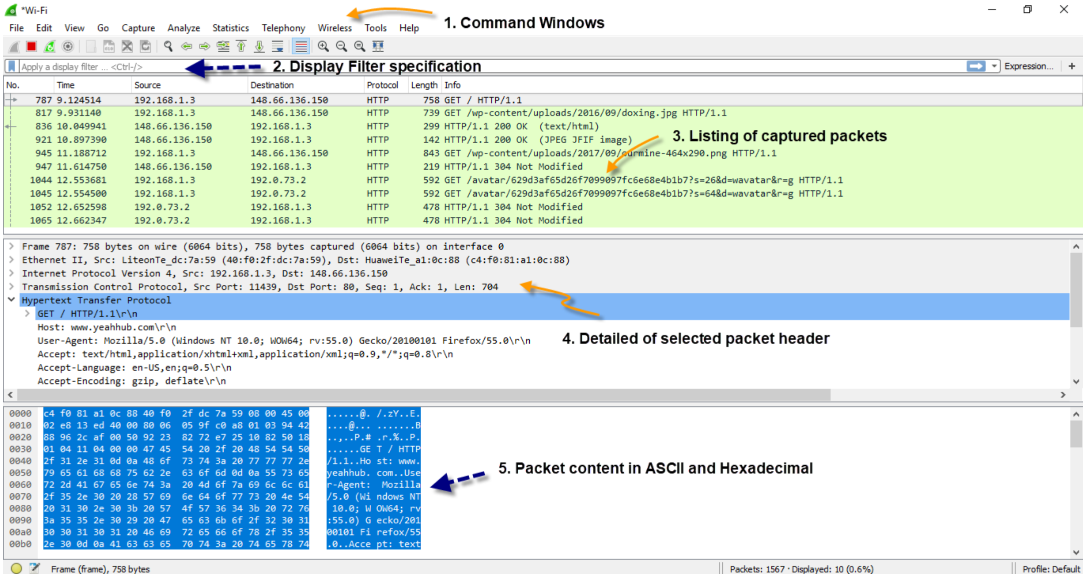
Wi-Fi
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Ethernet 4
Adapter for loopback traffic capture
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
Local Area Connection* 2
Local Area Connection* 1
Ethernet 2
OpenVPN Connect DCO Adapter
Local Area Connection
Local Area Connection 2
Event Tracing for Windows (ETW) reader

You are running Wireshark 4.2.4 (v4.2.4-0-g1fe5bce8d665). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

Fig-4- Initial Graphic User Interface of Wireshark

Then, you need to choose an interface. If you are running the Wireshark on your laptop, you need to select WiFi interface. If you are at a desktop, you need to select the Ethernet interface being used. Note that there could be multiple interfaces. In general, you can select any interface but that does not mean that traffic will flow through that interface.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
1. Command Windows
Apply a display filter ... <Ctrl-/>
2. Display Filter specification
Expression...
3. Listing of captured packets
4. Detailed of selected packet header
5. Packet content in ASCII and Hexadecimal

```
No.    Time        Source          Destination     Protocol Length Info
   787 9.124514    192.168.1.3     148.66.136.150  HTTP     758 GET / HTTP/1.1
   817 9.931140    192.168.1.3     148.66.136.150  HTTP     739 GET /wp-content/uploads/2016/09/doxing.jpg HTTP/1.1
   836 10.049941   148.66.136.150  192.168.1.3     HTTP     299 HTTP/1.1 200 OK  (text/html)
   921 10.897390   148.66.136.150  192.168.1.3     HTTP     142 HTTP/1.1 200 OK  (JPEG JFIF image)
   945 11.188712   192.168.1.3     148.66.136.150  HTTP     843 GET /wp-content/uploads/2017/09/curmine-464x290.png HTTP/1.1
   947 11.614750   148.66.136.150  192.168.1.3     HTTP     219 HTTP/1.1 304 Not Modified
  1044 12.553681   192.168.1.3     192.0.73.2      HTTP     592 GET /avatar/629d3af65d26f7099097fc6e68e4b1b7?s=26&d=wavatar&r=g HTTP/1.1
  1045 12.554500   192.168.1.3     192.0.73.2      HTTP     592 GET /avatar/629d3af65d26f7099097fc6e68e4b1b7?s=64&d=wavatar&r=g HTTP/1.1
  1052 12.652598   192.0.73.2      192.168.1.3     HTTP     478 HTTP/1.1 304 Not Modified
  1065 12.662347   192.0.73.2      192.168.1.3     HTTP     478 HTTP/1.1 304 Not Modified
```

```
> Frame 787: 758 bytes on wire (6064 bits), 758 bytes captured (6064 bits) on interface 0
> Ethernet II, Src: LiteonTe_dc:7a:59 (40:f0:2f:dc:7a:59), Dst: HuaweiTe_a1:0c:88 (c4:f0:81:a1:0c:88)
> Internet Protocol Version 4, Src: 192.168.1.3, Dst: 148.66.136.150
> Transmission Control Protocol, Src Port: 11439, Dst Port: 80, Seq: 1, Ack: 1, Len: 704
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: www.yeahhub.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
```

```
0000  c4 f0 81 a1 0c 88 40 f0  2f dc 7a 59 08 00 45 00   ......@. /.zY..E.
0010  02 e8 13 ed 40 00 80 06  05 9f c0 a8 01 03 94 42   ....@... .......B
0020  88 96 2c af 00 50 92 23  82 72 e7 25 10 82 50 18   ..,..P.# .r.%..P.
0030  01 04 11 04 00 00 47 45  54 20 2f 20 48 54 54 50   ......GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1..Ho st: www.
0050  79 65 61 68 68 75 62 2e  63 6f 6d 0d 0a 55 73 65   yeahhub. com..Use
0060  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
0070  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54   /5.0 (Wi ndows NT
0080  20 31 30 2e 30 3b 20 57  4f 57 36 34 3b 20 72 76    10.0; W OW64; rv
0090  3a 35 35 2e 30 29 20 47  65 63 6b 6f 2f 32 30 31   :55.0) G ecko/201
00a0  30 30 31 30 31 20 46 69  72 65 66 6f 78 2f 35 35   00101 Fi refox/55
00b0  2e 30 0d 0a 41 63 63 65  70 74 3a 20 74 65 78 74   .0..Acce pt: text
```

Frame (frame), 758 bytes | Packets: 1567 · Displayed: 10 (0.6%) | Profile: Default

Fig-5- Wireshark Graphical User Interface

The Wireshark interface has five major components:

The **command menus** are standard pulldown menus located at the top of the window. Of interest to us now is the File and Capture menus. The File menu allows you to save captured packet data or open a file containing previously captured packet data, and exit the Wireshark application. The Capture menu allows you to begin packet capture.

The **packet-listing window** displays a one-line summary for each packet captured, including the packet number (assigned by Wireshark; this is not a packet number contained in any protocol's header), the time at which the packet was captured, the packet's source and destination addresses, the protocol type, and protocol-specific information contained in the packet. The packet listing can be sorted according to any of these categories by clicking on a column name. The protocol type field lists the highest- level protocol that sent or received this packet, i.e., the protocol that is the source or ultimate sink for this packet.

The **packet-header details window** provides details about the packet selected highlighted) in the packetlisting window. (To select a packet in the packet-listing window, place the cursor over the packet's oneline summary in the packet-listing window and click with the left mouse button.). These details include information about the Ethernet frame and IP datagram that contains this packet. The amount of Ethernet and IP-layer detail displayed can be expanded or minimized by clicking on the right- pointing or downpointing arrowhead to the left of the Ethernet frame or IP datagram line in the packet details window. If the packet has been carried over TCP or UDP, TCP or UDP details will also be displayed, which can similarly be expanded or minimized. Finally, details about the highest-level protocol that sent or received this packet are also provided.

The **packet-contents window** displays the entire contents of the captured frame, in both ASCII and hexadecimal format.

Towards the top of the Wireshark graphical user interface, is the **packet display filter field**, into which a protocol name or other information can be entered in order to filter the information displayed in the packet-listing window (and hence the packet-header and packet-contents windows). In the example below, we'll use the packet-display filter field to have Wireshark hide (not display) packets except those that correspond to HTTP messages.

H. Resources/Equipment Required

Sr. No.	Instrument/Equipment /Components/Trainer kit	Specification	Quantity
1	*Computer system with operating system*		*1*

I. Safety and necessary Precautions followed

1. *Turn off power switch only after computer is shut down.*
2. *Do not plug out any computer cables*

J. Procedure :

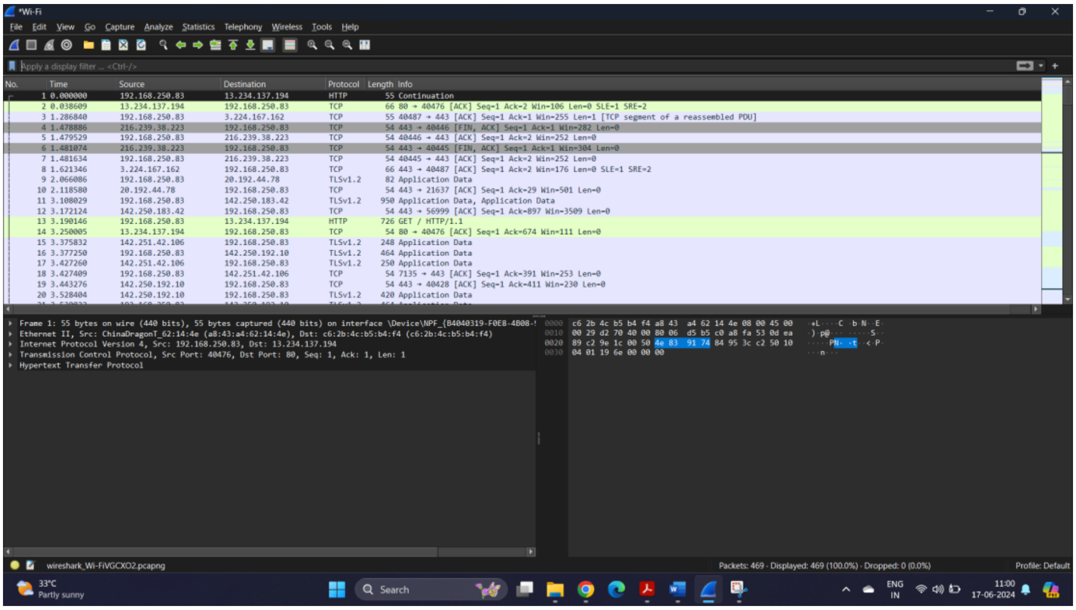
Capturing packets:

1. Start up the Wireshark program (select an interface and press start to capture packets).

2. Start up your any browser.

3. In your browser, go to GTU homepage by typing http://www.gtu.ac.in

4. After your browser has displayed the http://www.gtu.ac.in page, stop Wireshark packet capture by selecting stop in the Wireshark capture window. This will cause the Wireshark capture window to disappear and the main Wireshark window to display all packets captured since you began packet capture see image below:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source           Destination      Protocol Length Info
   1 0.000000  192.168.250.83   13.234.137.194   HTTP        55 Continuation
   2 0.038609  13.234.137.194   192.168.250.83   TCP         66 80 → 40476 [ACK] Seq=1 Ack=2 Win=106 Len=0 SLE=1 SRE=2
   3 1.286840  192.168.250.83   3.224.167.162    TCP         55 40487 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1 [TCP segment of a reassembled PDU]
   4 1.478886  216.239.38.223   192.168.250.83   TCP         54 443 → 40446 [FIN, ACK] Seq=1 Ack=1 Win=282 Len=0
   5 1.479529  192.168.250.83   216.239.38.223   TCP         54 40446 → 443 [ACK] Seq=1 Ack=2 Win=252 Len=0
   6 1.481074  216.239.38.223   192.168.250.83   TCP         54 443 → 40445 [FIN, ACK] Seq=1 Ack=1 Win=304 Len=0
   7 1.481634  192.168.250.83   216.239.38.223   TCP         54 40445 → 443 [ACK] Seq=1 Ack=2 Win=252 Len=0
   8 1.621346  3.224.167.162    192.168.250.83   TCP         66 443 → 40487 [ACK] Seq=1 Ack=2 Win=176 Len=0 SLE=1 SRE=2
   9 2.066086  192.168.250.83   20.192.44.78     TLSv1.2     82 Application Data
  10 2.118580  20.192.44.78     192.168.250.83   TCP         54 443 → 21637 [ACK] Seq=1 Ack=29 Win=501 Len=0
  11 3.108029  192.168.250.83   142.250.183.42   TLSv1.2    950 Application Data, Application Data
  12 3.172124  142.250.183.42   192.168.250.83   TCP         54 443 → 56999 [ACK] Seq=1 Ack=897 Win=3509 Len=0
  13 3.190146  192.168.250.83   13.234.137.194   HTTP       726 GET / HTTP/1.1
  14 3.250005  13.234.137.194   192.168.250.83   TCP         54 80 → 40476 [ACK] Seq=1 Ack=674 Win=111 Len=0
  15 3.375832  142.251.42.106   192.168.250.83   TLSv1.2    248 Application Data
  16 3.377250  192.168.250.83   142.250.192.10   TLSv1.2    464 Application Data
  17 3.427260  142.251.42.106   192.168.250.83   TLSv1.2    250 Application Data
  18 3.427409  192.168.250.83   142.251.42.106   TCP         54 7135 → 443 [ACK] Seq=1 Ack=391 Win=253 Len=0
  19 3.443276  142.250.192.10   192.168.250.83   TCP         54 443 → 40428 [ACK] Seq=1 Ack=411 Win=230 Len=0
  20 3.528404  142.250.192.10   192.168.250.83   TLSv1.2    420 Application Data
```

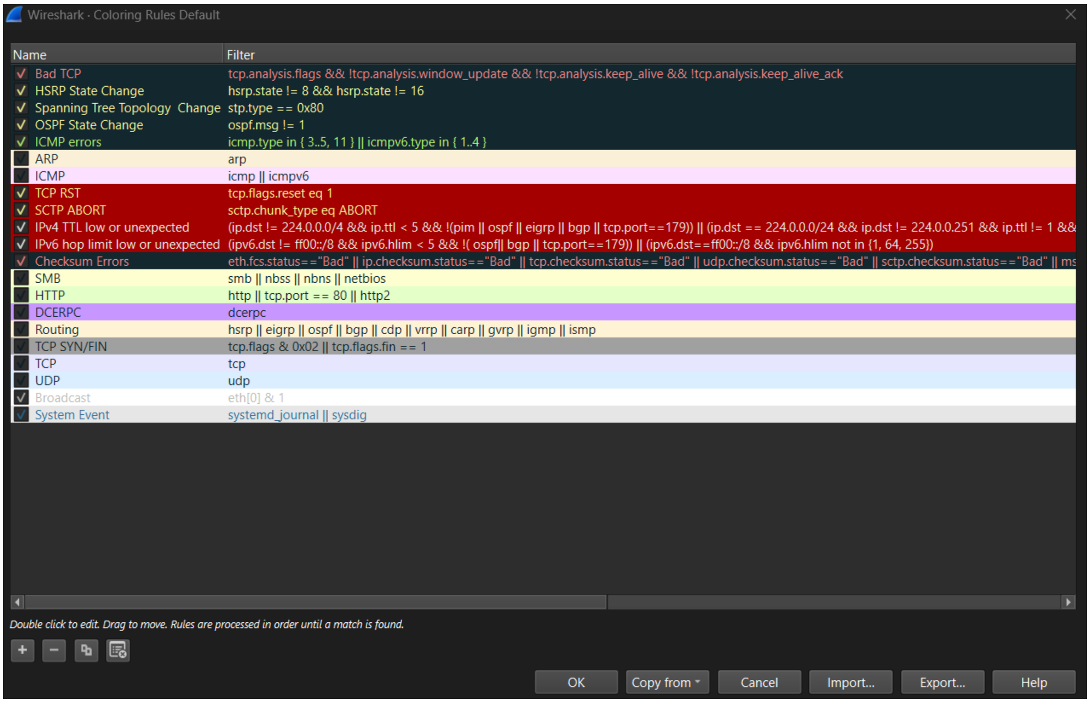
```
> Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{B4040319-F0E8-4B08-
> Ethernet II, Src: ChinaDragonT_62:14:4e (a8:43:a4:62:14:4e), Dst: c6:2b:4c:b5:b4:f4 (c6:2b:4c:b5:b4:f4)
> Internet Protocol Version 4, Src: 192.168.250.83, Dst: 13.234.137.194
> Transmission Control Protocol, Src Port: 40476, Dst Port: 80, Seq: 1, Ack: 1, Len: 1
> Hypertext Transfer Protocol
```

```
0000  c6 2b 4c b5 b4 f4 a8 43  a4 62 14 4e 08 00 45 00   ·+L····C ·b·N··E·
0010  00 29 d2 70 40 00 80 06  d5 b5 c0 a8 fa 53 0d ea   ·)·p@··· ·····S··
0020  89 c2 9e 1c 00 50 4e 83  91 74 84 95 3c c2 50 10   ·····PN· ·t··<·P·
0030  04 01 19 6e 00 00 00                               ···n···
```

```
wireshark_Wi-FiVGCXO2.pcapng          Packets: 469 · Displayed: 469 (100.0%) · Dropped: 0 (0.0%)          Profile: Default
```

Fig-6- Wireshark packet capture screen

5. Color Coding: You'll probably see packets highlighted in green, blue, and black. Wireshark uses colors to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems — for example, they could have been delivered out-of-order.


Wireshark · Coloring Rules Default

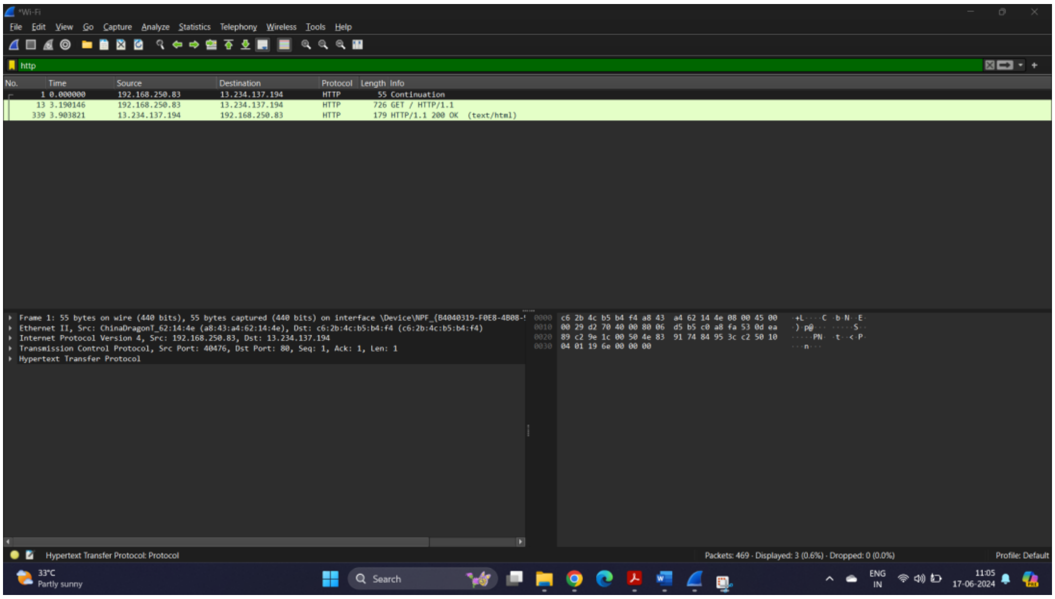
Name	Filter
✓ Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack
✓ HSRP State Change	hsrp.state != 8 && hsrp.state != 16
✓ Spanning Tree Topology Change	stp.type == 0x80
✓ OSPF State Change	ospf.msg != 1
✓ ICMP errors	icmp.type in { 3..5, 11 } || icmpv6.type in { 1..4 }
✓ ARP	arp
✓ ICMP	icmp || icmpv6
✓ TCP RST	tcp.flags.reset eq 1
✓ SCTP ABORT	sctp.chunk_type eq ABORT
✓ IPv4 TTL low or unexpected	(ip.dst != 224.0.0.0/4 && ip.ttl < 5 && !(pim || ospf || eigrp || bgp || tcp.port==179)) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 &&
✓ IPv6 hop limit low or unexpected	(ipv6.dst != ff00::/8 && ipv6.hlim < 5 && !(ospf|| bgp || tcp.port==179)) || (ipv6.dst==ff00::/8 && ipv6.hlim not in {1, 64, 255})
✓ Checksum Errors	eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad" || sctp.checksum.status=="Bad" || ms
✓ SMB	smb || nbss || nbns || netbios
✓ HTTP	http || tcp.port == 80 || http2
✓ DCERPC	dcerpc
✓ Routing	hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
✓ TCP SYN/FIN	tcp.flags & 0x02 || tcp.flags.fin == 1
✓ TCP	tcp
✓ UDP	udp
✓ Broadcast	eth[0] & 1
✓ System Event	systemd_journal || sysdig

Double click to edit. Drag to move. Rules are processed in order until a match is found.

Fig-7-Default color coding

6. You now have live packet data that contains all protocol messages exchanged between your computer and other network entities! However, as you will notice

the HTTP messages are not clearly shown because there are many other packets included in the packet capture. Even though the only action you took was to open your browser, there are many other programs in your computer that communicate via the network in the background. To filter the connections to the ones we want to focus on, we have to use the filtering functionality of Wireshark by typing "http" in the filtering field as shown below:

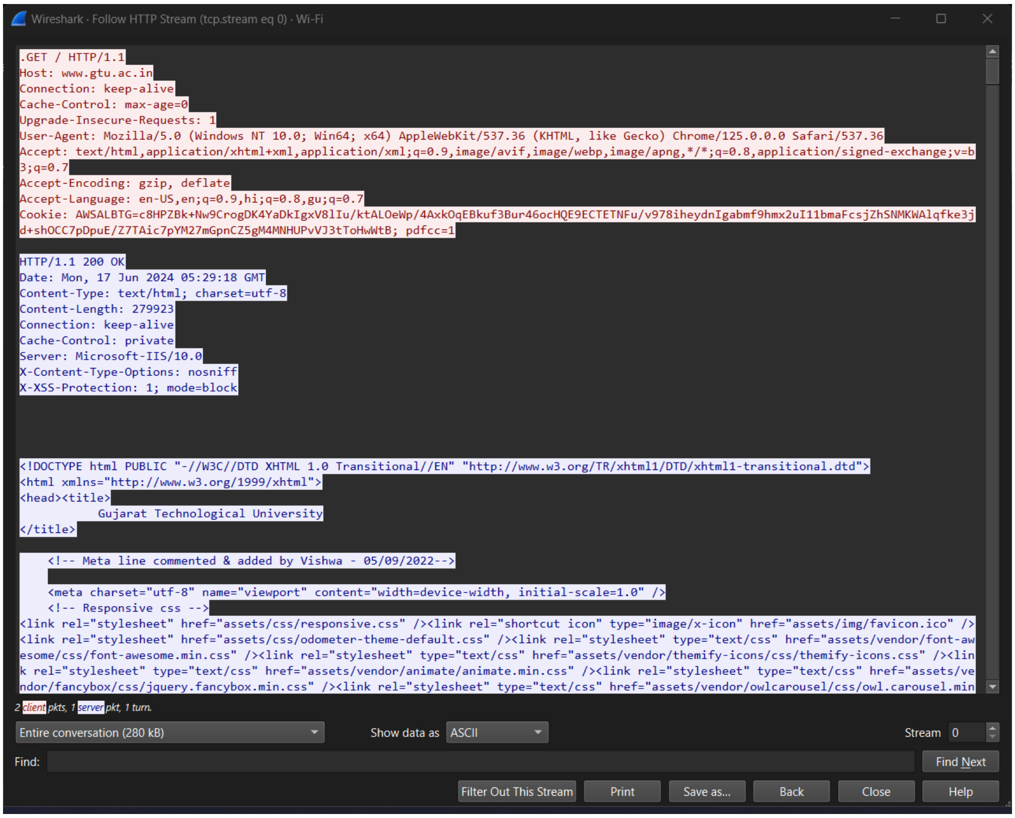


```
http

No.   Time       Source           Destination      Protocol Length Info
    1 0.000000   192.168.250.83   13.234.137.194   HTTP        55 Continuation
   13 3.190146   192.168.250.83   13.234.137.194   HTTP       726 GET / HTTP/1.1
  339 3.903821   13.234.137.194   192.168.250.83   HTTP       179 HTTP/1.1 200 OK  (text/html)

> Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{B4040319-F0E8-4B08-
> Ethernet II, Src: ChinaDragonT_62:14:4e (a8:43:a4:62:14:4e), Dst: c6:2b:4c:b5:b4:f4 (c6:2b:4c:b5:b4:f4)
> Internet Protocol Version 4, Src: 192.168.250.83, Dst: 13.234.137.194
> Transmission Control Protocol, Src Port: 40476, Dst Port: 80, Seq: 1, Ack: 1, Len: 1
> Hypertext Transfer Protocol

0000  c6 2b 4c b5 b4 f4 a8 43  a4 62 14 4e 08 00 45 00
0010  00 29 d2 70 40 00 80 06  d5 b5 c0 a8 fa 53 0d ea
0020  89 c2 9e 1c 00 50 4e 83  91 74 84 95 3c c2 50 10
0030  04 01 19 6e 00 00 00

Hypertext Transfer Protocol: Protocol          Packets: 469 · Displayed: 3 (0.6%) · Dropped: 0 (0.0%)          Profile: Default
```

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
33°C
Partly sunny
Search
ENG
IN
11:05
17-06-2024

Fig-8-Http filtered packets

7. Let's try now to find out what are those packets contain by following one of the conversations (also called network flows), select one of the packets and press the right mouse button, then click follow-> HTTP Stream you should see something similar to the screen below:



```
.GET / HTTP/1.1
Host: www.gtu.ac.in
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,hi;q=0.8,gu;q=0.7
Cookie: AWSALBTG=c8HPZBk+Nw9CrogDK4YaDkIgxV8lIu/ktALOeWp/4AxkOqEBkuf3Bur46ocHQE9ECTETNFu/v978iheydnIgabmf9hmx2uI11bmaFcsjZhSNMKWAlqfke3j
d+shOCC7pDpuE/Z7TAic7pYM27mGpnCZ5gM4MNHUPvVJ3tToHwWtB; pdfcc=1

HTTP/1.1 200 OK
Date: Mon, 17 Jun 2024 05:29:18 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 279923
Connection: keep-alive
Cache-Control: private
Server: Microsoft-IIS/10.0
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block



<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head><title>
           Gujarat Technological University
</title>

    <!-- Meta line commented & added by Vishwa - 05/09/2022-->

    <meta charset="utf-8" name="viewport" content="width=device-width, initial-scale=1.0" />
    <!-- Responsive css -->
<link rel="stylesheet" href="assets/css/responsive.css" /><link rel="shortcut icon" type="image/x-icon" href="assets/img/favicon.ico" />
<link rel="stylesheet" href="assets/css/odometer-theme-default.css" /><link rel="stylesheet" type="text/css" href="assets/vendor/font-aw
esome/css/font-awesome.min.css" /><link rel="stylesheet" type="text/css" href="assets/vendor/themify-icons/css/themify-icons.css" /><lin
k rel="stylesheet" type="text/css" href="assets/vendor/animate/animate.min.css" /><link rel="stylesheet" type="text/css" href="assets/ve
ndor/fancybox/css/jquery.fancybox.min.css" /><link rel="stylesheet" type="text/css" href="assets/vendor/owlcarousel/css/owl.carousel.min
```

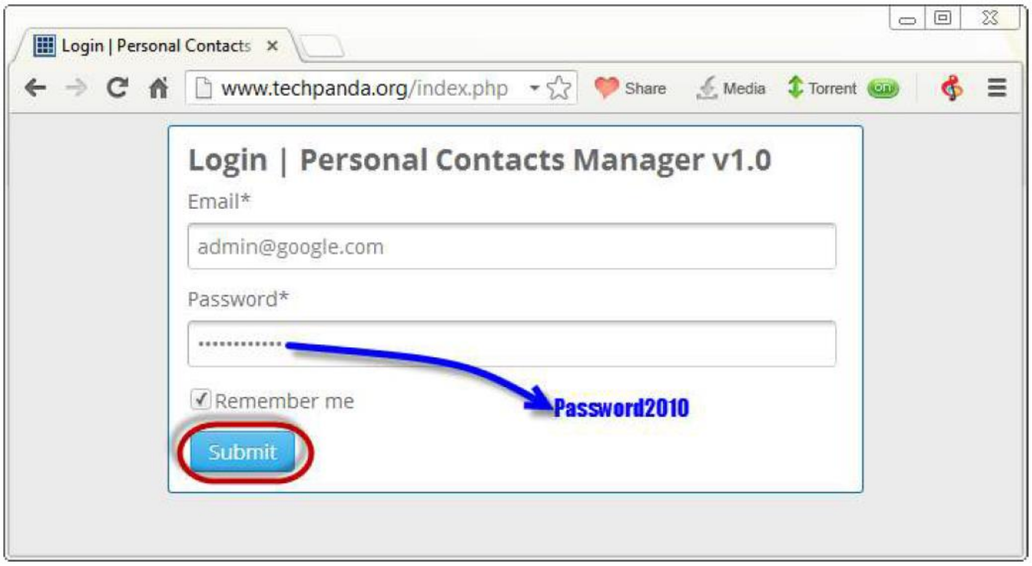
2 client pkts, 1 server pkt, 1 turn.

Entire conversation (280 kB)   Show data as ASCII   Stream 0

Fig-9-HTTP stream

Password sniffing using Wireshark:

1. Open Wireshark
2. Select the network interface you want to sniff. Note for this demonstration, we are using a wireless network connection. If you are on a local area network, then you should select the local area network interface.
3. Open your web browser and type in http://www.techpanda.org/



www.techpanda.org/index.php

Login | Personal Contacts Manager v1.0

Email*

admin@google.com

Password*

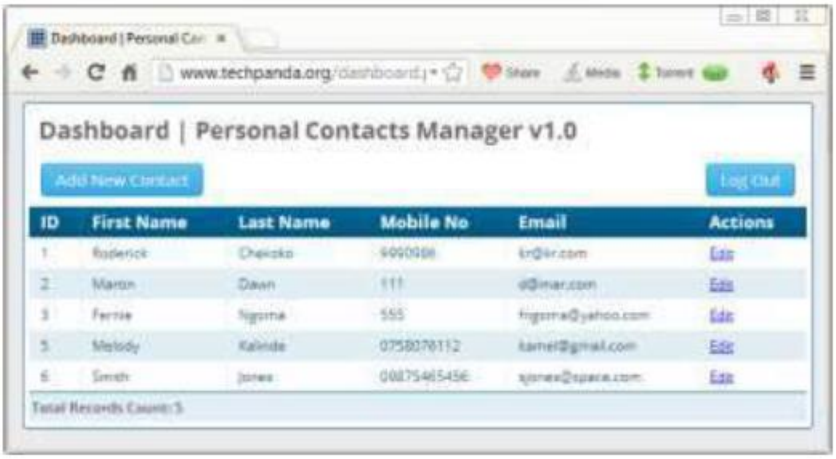
••••••••••••

Password2010

☑ Remember me

Submit

4. The login email is admin@google.com and the password is Password2010
5. Click on submit button
6. A successful logon should give you the following dashboard

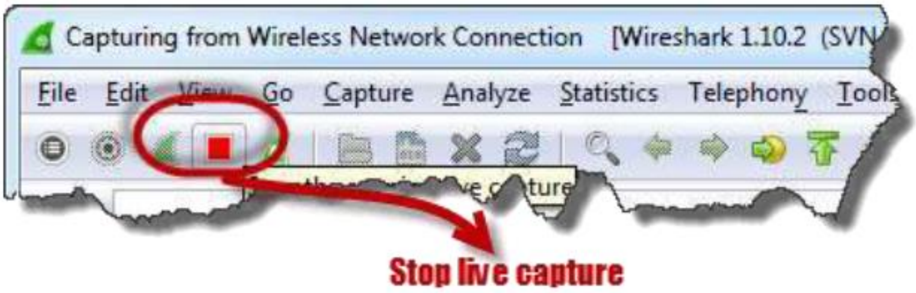


Dashboard | Personal Contacts Manager v1.0

ID	First Name	Last Name	Mobile No	Email	Actions
1	Roderick	Chekoko	9990998	kr@kr.com	Edit
2	Martin	Dawn	111	d@mar.com	Edit
3	Fernie	Ngoma	555	fngoma@yahoo.com	Edit
5	Melody	Kalinde	0758076112	kamel@gmail.com	Edit
6	Smith	Jones	00875465456	sjones@space.com	Edit

Total Records Count: 5

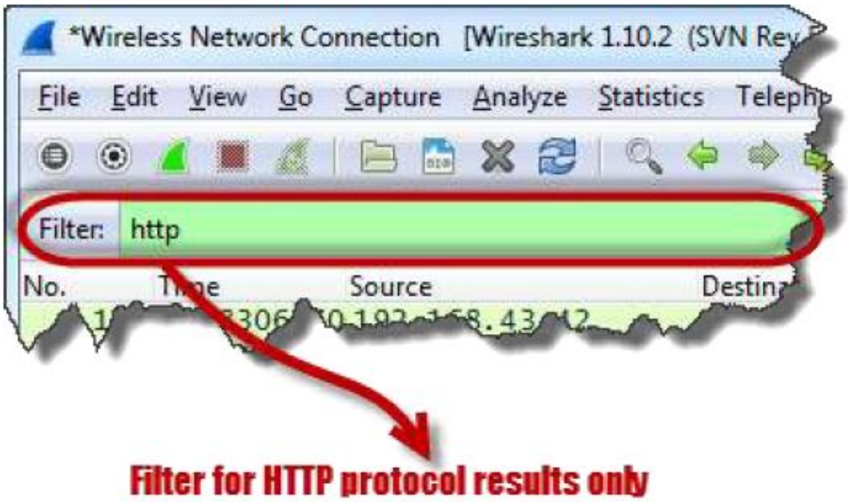
7. Go back to Wireshark and stop the live capture



Capturing from Wireless Network Connection [Wireshark 1.10.2 (SVN
File Edit View Go Capture Analyze Statistics Telephony Tools

Stop live capture

8. Filter for HTTP protocol results only using the filter textbox

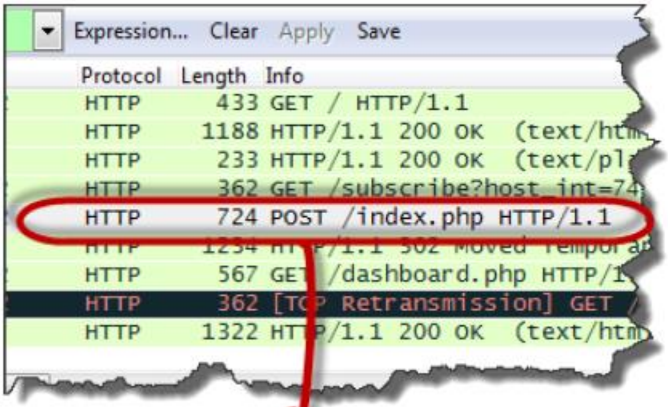


*Wireless Network Connection [Wireshark 1.10.2 (SVN Rev
File Edit View Go Capture Analyze Statistics Teleph
No. Time Source Destin

Filter: http

Filter for HTTP protocol results only

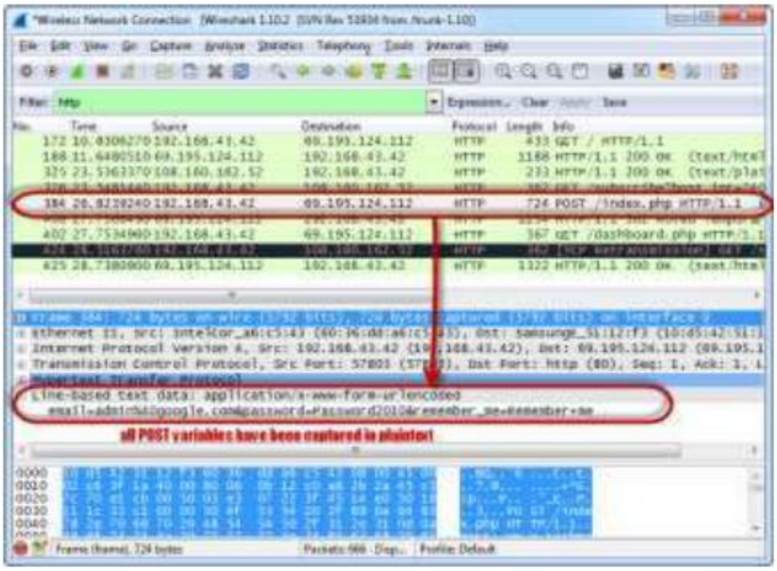
9. Locate the Info column and look for entries with the HTTP verb POST and click on it



```
Protocol  Length  Info
HTTP         433  GET / HTTP/1.1
HTTP        1188  HTTP/1.1 200 OK  (text/htm
HTTP         233  HTTP/1.1 200 OK  (text/pl
HTTP         362  GET /subscribe?host_int=74
HTTP         724  POST /index.php HTTP/1.1
HTTP        1234  HTTP/1.1 302 Moved Tempora
HTTP         567  GET /dashboard.php HTTP/1
HTTP         362  [TCP Retransmission] GET /
HTTP        1322  HTTP/1.1 200 OK  (text/htm
```

Look for POST verb under Info column

10. Just below the log entries, there is a panel with a summary of captured data. Look for the summary that says Line-based text data: application/x-www-form-urlencoded



```
No.  Time        Source          Destination     Protocol Length Info
172 10.0306270 192.168.43.42   69.195.124.112  HTTP      433 GET / HTTP/1.1
188 11.6480510 69.195.124.112  192.168.43.42   HTTP     1188 HTTP/1.1 200 OK  (text/html
325 23.5363370 108.160.162.52  192.168.43.42   HTTP      233 HTTP/1.1 200 OK  (text/plai
384 26.8228240 192.168.43.42   69.195.124.112  HTTP      724 POST /index.php HTTP/1.1
402 27.7534900 192.168.43.42   69.195.124.112  HTTP      367 GET /dashboard.php HTTP/1.1
425 28.7380900 69.195.124.112  192.168.43.42   HTTP     1322 HTTP/1.1 200 OK  (text/html

Line-based text data: application/x-www-form-urlencoded
  email=admin%40google.com&password=Password2010&remember_me=remember+me
```

Wireless Network Connection [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http
Expression... Clear Apply Save
Frame (frame), 724 bytes
Packets: 966 · Disp...
Profile: Default

all POST variables have been captured in plaintext

11. You should be able to view the plaintext values of all the POST variables submitted to the server via HTTP protocol.

K. Input-Output :

Perform Password sniffing for given below url

http://testphp.vulnweb.com/login.php

L. Practical related Quiz.

1. Which of the following protocols can Wireshark capture and analyze?
   - a) HTTP
   - b) HTTPS
   - c) FTP
   - d) All of the above
2. What is the primary purpose of Wireshark in network security?
   - a) To create network firewalls
   - b) To monitor and analyze network traffic
   - c) To configure routers
   - d) To prevent DDoS attacks
3. When analyzing a GET request in Wireshark, where can you find the requested URL?
   - a) In the Ethernet frame
   - b) In the IP header
   - c) In the HTTP request line
   - d) In the TCP segment
4. Which filter would you use in Wireshark to display only HTTP traffic?
   - a) ip.addr == 192.168.1.1
   - b) tcp.port == 80
   - c) http
   - d) port 443
5. What is a potential risk of transmitting passwords over HTTP?
   - a) Passwords are encrypted and secure
   - b) Passwords can be easily intercepted in plaintext
   - c) Passwords are protected by SSL/TLS
   - d) Passwords are hidden in the IP header

M. References / Suggestions:

1. https://www.geeksforgeeks.org/sniffing-of-login-credential-or-password-capturing-in-wireshark/
2. https://builtin.com/articles/nmap-port-scanning

N. Assessment-Rubrics

Sr No.	Performance Indicators	Weightage in %	Marks	Obtained Marks
1	Analyse and identify suitable approach for problem solving	25	0-5	

2	Use of appropriate technology / software / tools	25	0-5	
3	Demonstrate problems as per instructions	20	0-5	
4	Interpret the result and conclusion	15	0-5	
5	Prepare a report/presentation for given problem	15	0-5	
	Total	**100**	**25**	

Sign with Date

Date: …………..

Practical No.11: a) Installation and configuration of Kali Linux in Virtual box/VMware.
b) Perform basic commands in Kali Linux.

A. Objective:

To install and configure Kali Linux in VirtualBox/VMware and to perform basic commands, demonstrating fundamental Linux skills and understanding of virtual environments.

B. Expected Program Outcomes (POs)

PO1,PO4

C. Expected Skills to be developed based on competency:

This practical is expected to develop the following skills for the industry-identified competency:

1. Virtual Machine Management: Developing the competency to install, configure, and manage operating systems within virtual environments such as VirtualBox and VMware.
2. Linux Command Proficiency: Gaining proficiency in executing and understanding basic Linux commands within the Kali Linux distribution, essential for effective navigation and system management.

D. Expected Course Outcomes(Cos)

CO4: Conduct ethical hacking and protect systems using Kali Linux tools and vulnerability assessment techniques.

E. Practical Outcome(PRo)

Students will be able to successfully install and configure Kali Linux in a virtualized environment (VirtualBox/VMware) and perform basic Linux commands, equipping them with essential skills for cybersecurity tasks and system administration.

F. Expected Affective domain Outcome(ADos)

1. Increased Confidence in Technical Skills: Students will develop confidence in their ability to set up and manage virtual machines and navigate a Linux environment, fostering a sense of self-efficacy in handling technical tasks.
2. Enhanced Problem-Solving Attitude: Students will cultivate a proactive and analytical mindset when troubleshooting installation and configuration issues, encouraging persistence and a solution-oriented approach to technical challenges.

G. Prerequisite Theory:

Virtualization

Definition: Virtualization is the process of creating a virtual (rather than actual) version of something, such as an operating system, server, storage device, or network resources.

Virtual Machines (VMs): VirtualBox and VMware are virtualization software that allows multiple operating systems to run concurrently on a single physical machine. VMs are created within these virtualization environments, providing isolated environments where different operating systems, such as Kali Linux, can be installed and used.

Advantages of Virtualization:

Resource Utilization: Virtualization enables efficient utilization of hardware resources by allowing multiple virtual machines to run on a single physical machine.

Isolation: Each virtual machine operates independently of others, providing a sandboxed environment for testing, development, and security purposes.

Flexibility: VMs can be easily provisioned, replicated, and moved across different physical machines, providing flexibility in managing and scaling infrastructure.

Kali Linux:

Kali Linux is a Debian-derived Linux distribution that is maintained by Offensive Security. It was developed by Mati Aharoni and Devon Kearns. Kali Linux is a specially designed OS for network analysts, Penetration testers, or in simple words, it is for those who work under the umbrella of cybersecurity and analysis. The official website of Kali Linux is Kali.org. It was not designed for general purposes, it is supposed to be used by professionals or by those who know how to operate Linux/Kali.

Advantages:

- It has 600+ Penetration testing and network security tools pre-installed.
- It is completely free and open source. So you can use it for free and even contribute for its development.
- It supports many languages.
- Great for those who are intermediate in linux and have their hands on Linux commands.
- Could be easily used with Raspberry Pi.

H. Resources/Equipment Required

Sr. No.	Instrument/Equipment /Components/Trainer kit	Specification	Quantity
1	*Computer system with operating system*		*1*

I. **Safety and necessary Precautions followed**

1. *Turn off power switch only after computer is shut down.*
2. *Do not plug out any computer cables*

J. **Procedure :**

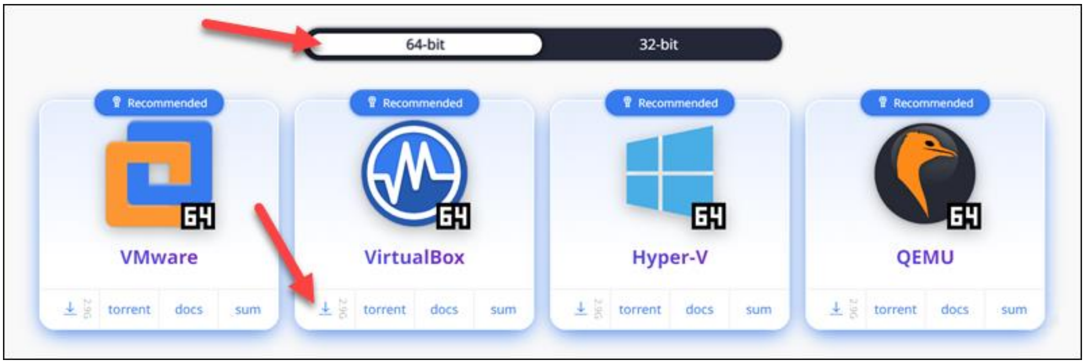
(a) Running Kali Linux Pre-Built VM on VirtualBox:

A quick way to run a Kali Linux VM is by using a pre-built VirtualBox image. The section below explains how to obtain and start a pre-built Kali Linux image on VirtualBox.

Download and install Oracle virtual box from url : **https://www.virtualbox.org/wiki/Downloads**

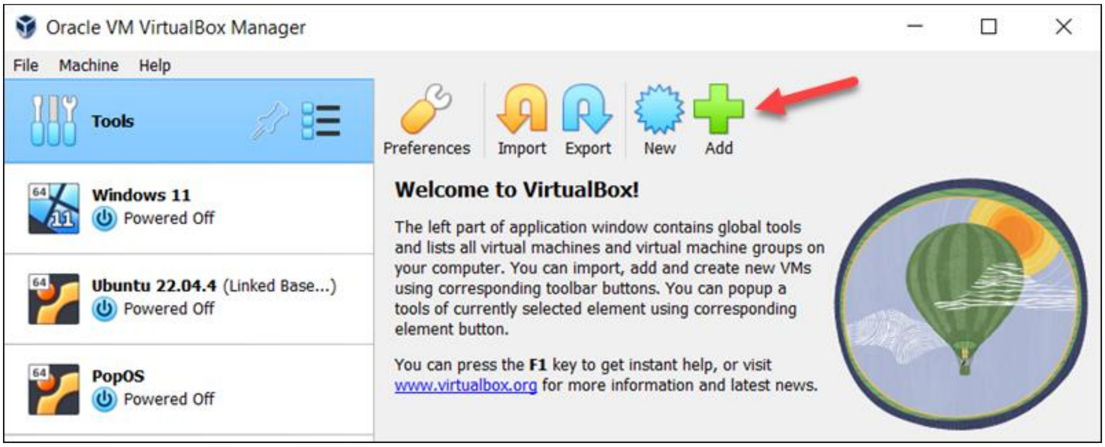
1. Visit the Pre-built VMs page on the official Kali Linux website.

2. Select the desired architecture and click the download button in the bottom left corner of the VirtualBox card.



3. Wait for the 7z file to download, then unpack it to a directory of your choice.

4. Open VirtualBox Manager and select the Add button in the top menu.



Windows 11
Powered Off

Ubuntu 22.04.4 (Linked Base...)
Powered Off

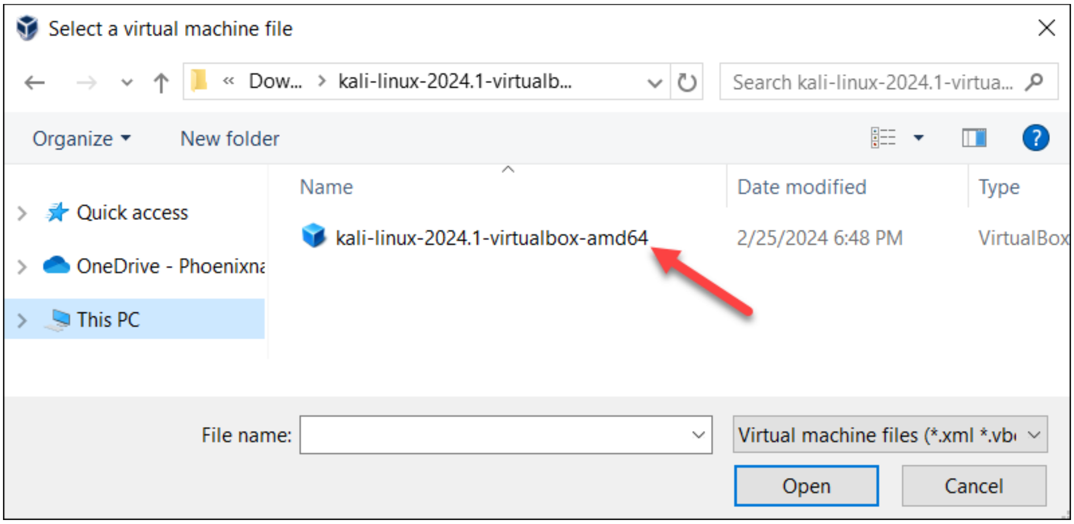
PopOS
Powered Off

Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

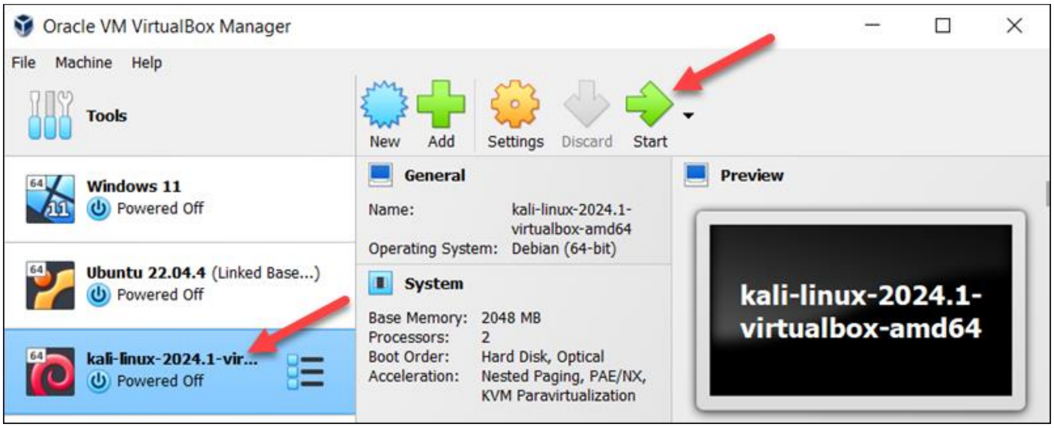
5. Locate the virtual machine file you downloaded and unpacked. Double-click the file to open it.


Select a virtual machine file
« Dow... › kali-linux-2024.1-virtualb...
Search kali-linux-2024.1-virtua...
Organize ▾
New folder
Quick access
OneDrive - Phoenixna
This PC
File name:
Virtual machine files (*.xml *.vb
Open
Cancel

Name	Date modified	Type
kali-linux-2024.1-virtualbox-amd64	2/25/2024 6:48 PM	VirtualBox

A Kali Linux VM instance appears in the menu on the left side of the screen.

6. Select the instance and click the Start button in the top menu.


Oracle VM VirtualBox Manager
File
Machine
Help
Tools
New
Add
Settings
Discard
Start
Preview
kali-linux-2024.1-virtualbox-amd64

Windows 11
Powered Off

Ubuntu 22.04.4 (Linked Base...)
Powered Off

kali-linux-2024.1-vir...
Powered Off

General

Name: kali-linux-2024.1-virtualbox-amd64
Operating System: Debian (64-bit)

System

Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

Wait for the system to boot up.

7. On the login screen, use username kali and password kali to log in.

(b) Perform basic commands in Kali Linux.

1. pwd (Print Working Directory):
   Usage: Displays the current directory you are in.
2. ls (List):
   Usage: Lists files and directories in the current directory.
   Examples:

```
ls          # Lists all files and directories
ls -l       # Lists files and directories in long format
ls -a       # Lists all files including hidden files
```

3. cd (Change Directory):
   Usage: Changes the current directory to the specified directory.
   Examples:

```
cd /path/to/directory  # Changes to specified directory
cd ..                  # Moves up one directory level
cd ~                   # Changes to the home directory
```

4. touch:

   Usage: Creates an empty file or updates the timestamp of an existing file.
   Example:

```
touch filename.txt
```

5. cp (Copy):
   Usage: Copies files or directories from one location to another.
   Examples:

```
cp source.txt destination.txt           # Copies a file
cp -r /source/directory /destination    # Copies a directory recursively
```

6. mv (Move):
   Usage: Moves or renames files and directories.
   Examples:
   ```
   mv oldname.txt newname.txt           # Renames a file
   mv /source/directory /destination    # Moves a directory
   ```
7. rm (Remove):
   Usage: Deletes files or directories.
   Examples:
   ```
       rm filename.txt       # Deletes a file
       rm -r directoryname   # Deletes a directory recursively
   ```
8. top:
   Usage: Displays real-time system processes and resource usage.
9. ifconfig (Interface Configuration):
   Usage: Configures network interfaces (often requires root privileges).
   Example:
   ```
           Ifconfig
   ```
10. ping:
    Usage: Checks connectivity to a host.
    Example:
    ```
                    ping www.example.com
    ```
11. netstat (Network Statistics):
    Usage: Displays network connections, routing tables, interface statistics, etc.
    Example:
    ```
            netstat -tuln
    ```
12. apt-get update:
    Usage: Updates the list of available packages and their versions.
13. apt-get upgrade:
    Usage: Installs the newest versions of all packages currently installed.

14. apt-get install:

    Usage: Installs new packages.
    Example:
    ```
            sudo apt-get install packagename
    ```
15. Whoami- prints the username of the current user who is logged in.
16. Date: display system date and time
17. Cal- displays the current month's formatted calendar
18. Sudo- stands for "superuser do" and is used to execute commands with elevated privileges, typically as the root user or another user with administrative permissions.
19. useradd - Add a new user
20. passwd - Change user password. Allows changing the password of a user account
21. usermod - Modify user properties.
22. groupadd - Add a new group.
23. userdel - Delete a user.
24. ps - Display information about active processes.

25. top - Display dynamic real-time information about running processes.
26. kill/killall - Kill Process: Terminates a process by PID or name.
27. clear - Clear Screen: Clears the terminal screen.
28. logout/exit - Logout/Exit: Logs out of the current session or exits the terminal
29. history - Command History: Displays the command history of the current session

K. Observations :

Write output of basic Linux command:

L. Practical related Quiz.

1. What is the primary purpose of using virtualization software like VirtualBox or VMware?
   a) To increase the processing speed of your computer.
   b) To allow multiple operating systems to run concurrently on a single physical machine.
   c) To enhance the graphical user interface of the operating system.
   d) To convert a physical machine into a virtual machine.

2. Which command is used to display the current directory in a Linux system?
   a) ls
   b) pwd
   c) cd
   d) dir

3. What does the ls -a command do in Linux?
   a) Lists files and directories with detailed information.
   b) Lists all files including hidden files.
   c) Changes the current directory.
   d) Creates an empty file.

4. Which command is used to copy a directory and its contents in Linux?
   a) mv
   b) cp
   c) cp -r
   d) rm -r
5. What is the purpose of the top command in Linux?
   a) To display the current directory.
   b) To show real-time system processes and resource usage.
   c) To list all files in the current directory.
   d) To change the file permissions.

M. References / Suggestions (lab manual designer should give)

1. https://phoenixnap.com/kb/how-to-install-kali-linux-on-virtualbox

N. Assessment-Rubrics

Sr No.	Performance Indicators	Weightage in %	Marks	Obtained Marks
1	Analyse and identify suitable approach for problem solving	25	0-5	
2	Use of appropriate technology / software / tools	25	0-5	
3	Demonstrate problems as per instructions	20	0-5	
4	Interpret the result and conclusion	15	0-5	
5	Prepare a report/presentation for given problem	15	0-5	
	Total	**100**	**25**	

Sign with Date

Date: …………..

Practical No.12: Perform Memory forensic using Memoryze tool.

A. Objective:

To utilize the Memoryze tool to analyze and extract forensic evidence from a computer's memory, aiding in the detection of malicious activities and security breaches.

B. Expected Program Outcomes (POs)

PO1,PO2,PO3,PO4

C. Expected Skills to be developed based on competency:

This practical is expected to develop the following skills for the industry-identified competency:

1. Proficiency in Memory Forensics Analysis: Developing the ability to use Memoryze to thoroughly analyze and interpret data from a computer's memory, identifying signs of malware, rootkits, and other malicious activities.
2. Incident Response and Investigation: Enhancing skills in conducting comprehensive forensic investigations, enabling effective response to security incidents by understanding memory artifacts and utilizing forensic tools to gather and preserve digital evidence.

D. Expected Course Outcomes(Cos)

CO5: Identify types of cyber crimes, understand their impact, and apply forensic techniques to investigate and prevent cyber criminal activities.

E. Practical Outcome(PRo)

Students will be able to effectively utilize the Memoryze tool to perform detailed memory forensics, identifying and analyzing malicious activities and security breaches.

F. Expected Affective domain Outcome(ADos)

1. Increased Vigilance and Ethical Responsibility: Students will develop a heightened sense of vigilance and ethical responsibility in handling digital evidence and conducting forensic investigations, ensuring integrity and confidentiality.
2. Enhanced Analytical Mindset: Students will cultivate an analytical mindset, fostering critical thinking and problem-solving skills when investigating and interpreting memory forensics data.

G. Prerequisite Theory:

Mandiant Memoryze is a free live memory acquisition and analysis tool designed for incident responders and forensic investigators. It allows you to capture and analyze system memory, both on live systems and from memory image files. It's a valuable tool for investigating malware, rootkits, and other suspicious activity.

Here are some key features of Memoryze:

Acquisition:

- Capture full system memory without relying on API calls.
- Image a process' entire address space to disk, including loaded DLLs, EXEs, heaps, and stacks.
- Image a specified driver or all loaded drivers in memory.
- Include the paging file in analysis on live systems.

Analysis:

- Enumerate all running processes, even those hidden by rootkits.
- Search for specific indicators of compromise (IOCs) such as malicious file names, registry keys, and network connections.
- Export data for further analysis with other tools.

Visualization:

- Use Redline™, Mandiant's free tool for investigating hosts, to visualize Memoryze's output.
- Alternatively, use an XML viewer.
- Memoryze is powerful but has a bit of a learning curve, so here are some helpful resources:

H. Resources/Equipment Required

Sr. No.	Instrument/Equipment /Components/Trainer kit	Specification	Quantity
1	*Computer system with operating system*	*Windows 10 or above, 4GB RAM, 250GB HDD/SSD*	*1*

I. Safety and necessary Precautions followed:

1. Backup critical data: Always create a backup of any critical data on the target system before proceeding. Memoryze can potentially disrupt ongoing processes or cause data loss.
2. Choose the right mode: Memoryze offers two main modes: "Live Acquisition" and "Image Analysis." Select the appropriate mode based on your needs. Live Acquisition is for analyzing running systems, while Image Analysis is for analyzing previously captured memory images.

3. Check available resources: Ensure sufficient free disk space to accommodate the captured memory image, which can be several gigabytes depending on the system size.

J. Procedure :

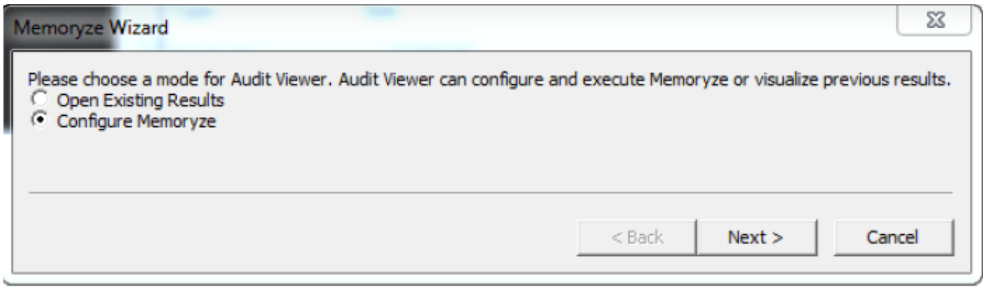
• To install Memoryze, download the MSI file from the Mandiant Web site (mentioned previously in this topic) and install it (D:\Mandiant directory).

• Then, to install Audit Viewer, download the zipped archive, and be sure that you've downloaded the dependencies (i.e., Python 2.5 or 2.6, wxPython GUI extensions) as described at the Mandiant Web site (if you've already installed and tried Volatility, you already have Python installed).

• Unzip the Audit Viewer files into the directory D:\Mandiant\AV

TASK: Opening the Memory Image for Review

- Audit Viewer to open it for analysis. Run auditviewer.exe
- Select "Configure Memoryze". While tempting, ignore the option "Open Existing Results" — it refers to re-opening an existing analysis file.



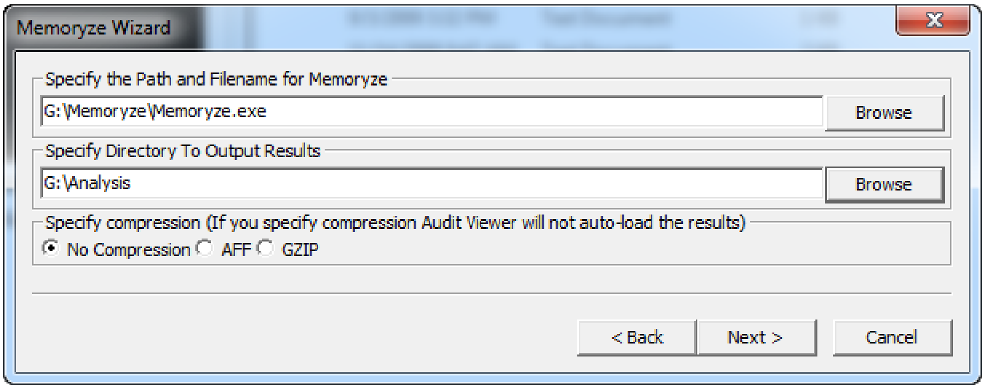
Memoryze Wizard

Please choose a mode for Audit Viewer. Audit Viewer can configure and execute Memoryze or visualize previous results.

○ Open Existing Results

● Configure Memoryze

- Click next and tell AuditViewer where your copy of memoryze.exe is located and where you would like to save the analysis results.



Memoryze Wizard

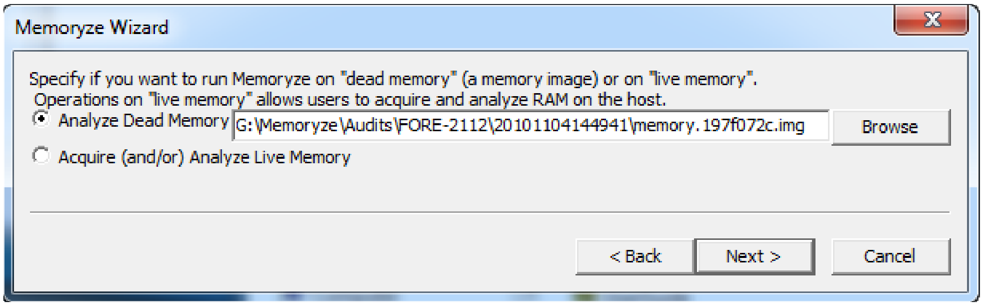
Specify the Path and Filename for Memoryze: G:\Memoryze\Memoryze.exe

Specify Directory To Output Results: G:\Analysis

Specify compression (If you specify compression Audit Viewer will not auto-load the results)

● No Compression ○ AFF ○ GZIP

- Next tell AuditViewer to analyze "dead" memory and browse to the location of the memory image just acquired.

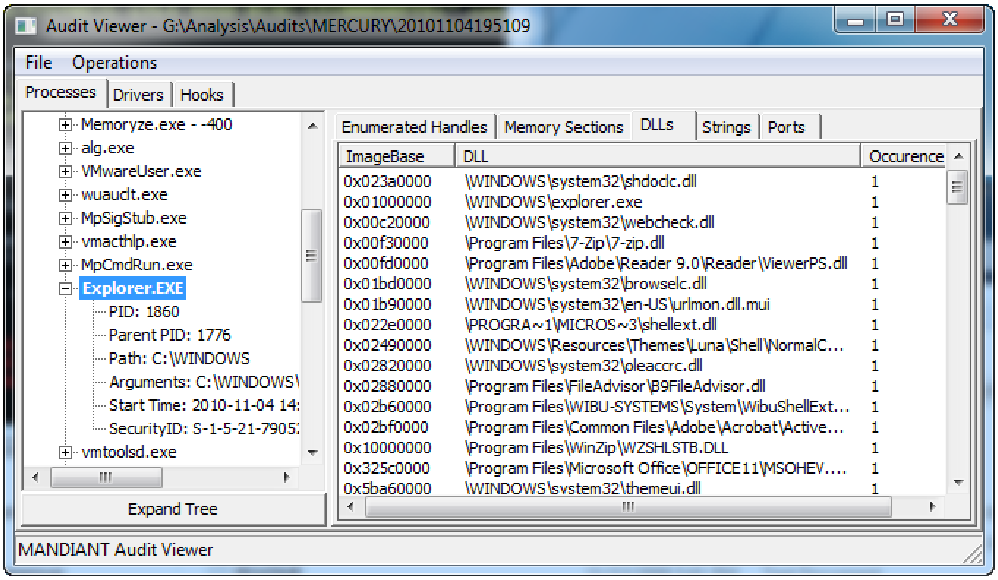


Specify if you want to run Memoryze on "dead memory" (a memory image) or on "live memory".
Operations on "live memory" allows users to acquire and analyze RAM on the host.

● Analyze Dead Memory G:\Memoryze\Audits\FORE-2112\20101104144941\memory.197f072c.img

○ Acquire (and/or) Analyze Live Memory

- Finally, the AuditViewer wizard will step you through a series of analysis and acquisition options



```
⊞ Memoryze.exe - -400
⊞ alg.exe
⊞ VMwareUser.exe
⊞ wuauclt.exe
⊞ MpSigStub.exe
⊞ vmacthlp.exe
⊞ MpCmdRun.exe
⊟ Explorer.EXE
    PID: 1860
    Parent PID: 1776
    Path: C:\WINDOWS
    Arguments: C:\WINDOWS\
    Start Time: 2010-11-04 14:
    SecurityID: S-1-5-21-7905:
⊞ vmtoolsd.exe
```

ImageBase	DLL	Occurence
0x023a0000	\WINDOWS\system32\shdoclc.dll	1
0x01000000	\WINDOWS\explorer.exe	1
0x00c20000	\WINDOWS\system32\webcheck.dll	1
0x00f30000	\Program Files\7-Zip\7-zip.dll	1
0x00fd0000	\Program Files\Adobe\Reader 9.0\Reader\ViewerPS.dll	1
0x01bd0000	\WINDOWS\system32\browselc.dll	1
0x01b90000	\WINDOWS\system32\en-US\urlmon.dll.mui	1
0x022e0000	\PROGRA~1\MICROS~3\shellext.dll	1
0x02490000	\WINDOWS\Resources\Themes\Luna\Shell\NormalC...	1
0x02820000	\WINDOWS\system32\oleaccrc.dll	1
0x02880000	\Program Files\FileAdvisor\B9FileAdvisor.dll	1
0x02b60000	\Program Files\WIBU-SYSTEMS\System\WibuShellExt...	1
0x02bf0000	\Program Files\Common Files\Adobe\Acrobat\Active...	1
0x10000000	\Program Files\WinZip\WZSHLSTB.DLL	1
0x325c0000	\Program Files\Microsoft Office\OFFICE11\MSOHEV....	1
0x5ba60000	\WINDOWS\system32\themeui.dll	1

Mandiant does a great job of documenting their tools, and this is no exception. At the conclusion of the wizard, a progress meter is displayed, culminating in an interactive view of all of the identified processes and their corresponding dlls, handles, memory sections, etc.

K. Practical Proposed Suggested task:

•Monitoring Performing Live Memory Analysis

•LiME: A command-line tool for acquiring and analyzing memory images on Linux systems.

L. References / Suggestions

1. User Guide :: Memoryze User Guide PDF https://fireeye.market/assets/apps/211368/documents/701164_en.pdf
2. Download :: Mandiant Memoryze 3.0 (https://fireeye.market/apps/211368)

M. Assessment-Rubrics:

Sr No.	Performance Indicators	Weightage in %	Marks	Obtained Marks
1	Analyse and identify suitable approach for problem solving	25	0-5	
2	Use of appropriate technology / software / tools	25	0-5	
3	Demonstrate problems as per instructions	20	0-5	
4	Interpret the result and conclusion	15	0-5	
5	Prepare a report/presentation for given problem	15	0-5	
	Total	**100**	**25**	

Sign with Date

Date: …………..

Practical No.13: Perform web Artifact analysis and registry analysis using Autopsy.

A. Objective:

To utilize Autopsy for conducting web artifact analysis and registry analysis to uncover digital evidence from web browsing activities and system registry changes.

B. Expected Program Outcomes (POs)

PO1,PO2,PO3,PO4

C. Expected Skills to be developed based on competency:

This practical is expected to develop the following skills for the industry-identified competency:

1. Proficiency in Digital Forensic Analysis: Develop the ability to effectively use Autopsy for identifying, extracting, and analyzing web artifacts and registry entries, enhancing skills in uncovering and interpreting digital evidence.
2. Technical Investigation and Reporting: Gain competency in conducting thorough digital investigations, documenting findings, and creating detailed forensic reports that can be used in legal or investigative contexts.

D. Expected Course Outcomes(Cos)

CO5: Identify types of cyber crimes, understand their impact, and apply forensic techniques to investigate and prevent cyber criminal activities.

E. Practical Outcome(PRo)

Students will be able to successfully identify, extract, and analyze web artifacts and registry data using Autopsy, demonstrating the ability to uncover and interpret digital evidence for forensic investigations.

F. Expected Affective domain Outcome(ADos)

1. Increased Attention to Detail: Develop a heightened sense of meticulousness and precision in examining digital evidence, ensuring thoroughness and accuracy in forensic investigations.
2. Enhanced Ethical Awareness: Foster a stronger commitment to ethical standards and integrity in handling digital evidence, recognizing the importance of confidentiality, legality, and impartiality in forensic analysis.

G. Prerequisite Theory:

Web Artifact Analysis:

- Reconstruct user browsing activity:
  Identify websites visited, search terms used, files downloaded, timestamps, and user preferences.

  Understand user actions, interests, and potential motivations.
- Gather evidence of online behavior:

Uncover potential criminal activity, policy violations, or unauthorized access.

Support investigations into cybercrime, fraud, data breaches, or intellectual property theft.

- Identify malicious websites or downloads:

  Detect malware, phishing attempts, or other online threats.

  Protect systems and networks from potential harm.

- Track user interactions with web applications:

  Understand how users engage with online services or platforms.

  Investigate potential misuse of web applications or services.

Registry Analysis Objectives:

- Reveal system configuration and settings:

  Identify installed software, hardware details, network configurations, user accounts, and system modifications.

  Understand system changes and potential vulnerabilities.

- Track user activity on the system:

  Identify recently accessed files, programs, connected devices, and network connections.

  Understand user actions and patterns of behavior.

- Detect malware and system tampering:

  Uncover malicious software, unauthorized system changes, or attempts to hide evidence.

  Investigate system compromises and security incidents.

- Gather evidence of software usage:

  Determine when specific programs were installed or used.

  Investigate software licensing compliance or unauthorized software installations.

H. Resources/Equipment Required

Sr. No.	Instrument/Equipment /Components/Trainer kit	Specification	Quantity
1	*Computer system with operating system*	*Windows 10 or above, 4GB RAM, 250GB HDD/SSD*	*1*

I. Safety and necessary Precautions followed:

1. Preserving Data Integrity
2. Protecting Sensitive Data

3. Preventing Malware Infection
4. Document every step.
5. Adhere to legal and ethical guidelines.

J. Procedure :

The Autopsy is a cyber-forensic tool used for the analysis of Windows and UNIX file systems (NTFS, FAT, FFS, EXT2FS, and EXT3FS). It can also be used to recover deleted files and also show various sectors of uploaded images making it easier to make an in-depth analysis of the image.

Autopsy in Windows

- Download the Windows Installer Package of Autopsy from http://sleuthkit.org/autopsy/download.php.
- Choose the 64-bit or 32-bit version subject to your computer's specification (Start button > Settings > System > About > System Type).
- Run the downloaded .msi file (if Windows prompts with User Account Control, click 'Yes').
- Select the location of installation for Autopsy or click 'Next' if the default location (C:\Program Files) is OK.

Autopsy in Kali Linux

- Install Java Runtime Environment (JRE): If not already present, install JRE 8 or above using

  sudo apt install default-jre
- Execute the below command in the terminal for installing the Autopsy browser on the Linux system.

  sudo apt-get install autopsy
- Open a terminal window and type autopsy to launch the application.

Launch Autopsy:

Create a New Case:

- Click "New Case" to start a new investigation.
- Provide a case name and optional description.
- Select a case type (single-user or multi-user) and choose a case directory to store case files.

Add Data Source:

- Click "Add Data Source" and choose the type of evidence you want to analyze:
- Disk Image (.img, .raw, .e01, etc.)
- Local Drive (analyze a drive connected to the system)
- Logical File Set (analyze a specific folder or set of files)
- If using a disk image, specify its location and use a write blocker if necessary.

Ingest and Analyze:

Click "Ingest" to start processing the data.

Autopsy will automatically extract and parse various artifacts, including:

- Web artifacts (history, bookmarks, cookies, downloads)
- Registry data

Navigate through the "Results" section to view extracted artifacts, organized by category.

Use filters, keyword searches, and timeline analysis to refine your findings.

Create comprehensive reports to document your analysis and findings.

K. Practical Proposed Suggested task:

- Files and folders Analysis
- Deleted files Analysis
- Emails Analysis
- Metadata Analysis
- Images Analysis
- Other relevant forensic data Analysis

L. References / Suggestions

1. https://www.sleuthkit.org/autopsy/web_artifacts.php
2. https://www.autopsy.com/category/blog/
3. https://www.sans.org/blog/a-step-by-step-introduction-to-using-the-autopsy-forensic-browser/
4. https://www.youtube.com/watch?v=JVQmJIw5a4Q

M. Assessment-Rubrics:

Sr No.	Performance Indicators	Weightage in %	Marks	Obtained Marks
1	Analyse and identify suitable approach for problem solving	25	0-5	
2	Use of appropriate technology / software / tools	25	0-5	
3	Demonstrate problems as per instructions	20	0-5	
4	Interpret the result and conclusion	15	0-5	
5	Prepare a report/presentation for given problem	15	0-5	
	Total	**100**	**25**	

Sign with Date

Date: ………….

Practical No.14: Create forensic images of entire local hard drives using FTK IMAGER tool.

A. Objective:

To create forensic images of entire local hard drives using FTK Imager to ensure data integrity and preserve digital evidence for analysis and investigation.

B. Expected Program Outcomes (POs)

PO1,PO2,PO3,PO4

C. Expected Skills to be developed based on competency:

This practical is expected to develop the following skills for the industry-identified competency:

1. Skill in Digital Evidence Collection: Ability to effectively use FTK Imager to create accurate and reliable forensic images of local hard drives, ensuring data integrity and compliance with legal standards.
2. Competence in Data Preservation and Documentation: Skill in preserving digital evidence through proper imaging techniques and maintaining detailed documentation of the imaging process for use in forensic investigations and legal proceedings.

D. Expected Course Outcomes(Cos)

CO5: Identify types of cyber crimes, understand their impact, and apply forensic techniques to investigate and prevent cyber criminal activities.

E. Practical Outcome(PRo)

Students will be able to create forensic images of entire local hard drives using FTK Imager, demonstrating proficiency in digital evidence collection and data preservation techniques for forensic investigations.

F. Expected Affective domain Outcome(ADos)

1. Recognize the importance of maintaining data integrity and preserving digital evidence in forensic investigations.
2. Appreciate the meticulous documentation required to ensure the admissibility of forensic images in legal proceedings.

G. Prerequisite Theory:

Technical Skills:

1.Basic Computer Literacy:

- Understanding of file systems (FAT, NTFS, exFAT), storage devices (hard drives, USB drives, SSDs), and operating systems (Windows, Mac, Linux).

- Familiarity with Windows and Linux environments is particularly helpful.

2.Disk Imaging Principles:

- Knowledge of disk imaging techniques, including sector-based vs. file-based imaging, and the implications of each method.
- Understanding of different image formats (e.g., raw, E01, AFF) and their benefits.
- While FTK Imager has a graphical interface, basic command-line skills can be helpful for advanced tasks and automation.

4.Hashing and Verification:

- Familiarity with cryptographic hash functions like MD5 and SHA-256, and their role in ensuring evidence integrity.
- Understanding how to generate and verify hash values for image files.

5.Data Backup and Storage:

- Knowledge of proper data backup and storage principles to ensure secure handling of evidence images.

Investigative Skills:

1. Logical Thinking and Analysis:

- Ability to analyze digital evidence, identify patterns, and draw logical conclusions.
- Understanding of how files are stored and accessed on different operating systems.

2.Attention to Detail:

- Meticulousness in examining data, as small details can hold vital clues.

3.Report Writing and Documentation:

- Clear and concise written communication skills to document findings and the investigation process accurately.

4.Understanding of Digital Forensics Principles:

- Knowledge of chain of custody, evidence handling procedures, and legal considerations for working with digital evidence.

H. Resources/Equipment Required

Sr. No.	Instrument/Equipment /Components/Trainer kit	Specification	Quantity
1	*Computer system with operating system*	*Windows 10 or above, 4GB RAM, 250GB HDD/SSD*	*1*

I. Safety and necessary Precautions followed:

1. Preserving Data Integrity.
2. Protecting Sensitive Data.
3. Document every step.
4. Follows to legal and ethical guidelines.

J. Procedure :

- Forensic Toolkit, or FTK, is a computer forensics software originally developed by AccessData, an Exterro company. It scans a hard drive looking for various information.
- FTK is also associated with a standalone disk imaging program called FTK Imager. This tool saves an image of a hard disk in one file or in segments that may be later on reconstructed.
- It calculates MD5 and SHA1 hash values and can verify the integrity of the data imaged is consistent with the created forensic image.
- The forensic image can be saved in several formats, including DD/raw, E01, and AD1.

Installing FTK Imager:

1.Download the Software:

https://go.exterro.com/l/43312/2023-05-03/fc4b78

download the FTK Imager executable file (.exe) for Windows.

Windows OS:

2. Run the Installation Wizard

Linux Ubuntu OS:

Install WINE: Ensure that you have WINE installed on your Linux system.

Use the following commands:

```
sudo dpkg --add-architecture i386
sudo apt update
sudo apt install wine64 wine32
```

Run FTK Imager Installer with WINE:

Open a terminal and navigate to the directory where you downloaded the FTK Imager installer.

Run the installer using WINE. Replace ftkimager_installer.exe with the actual filename of the FTK Imager installer you downloaded.

Use the following commands:

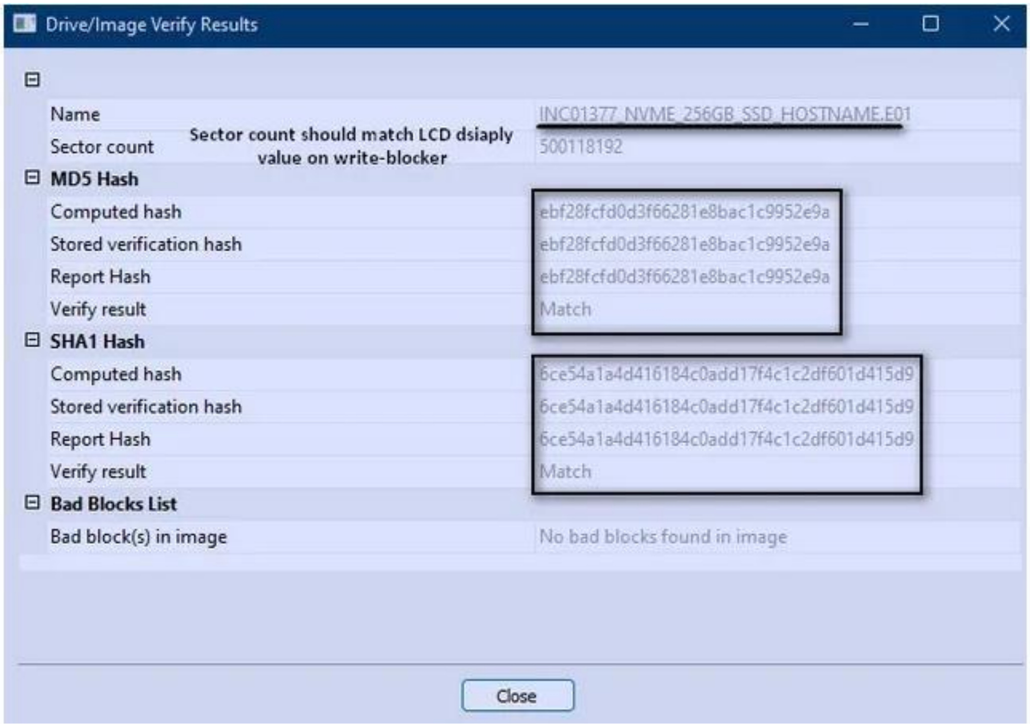
```
wine ftkimager_installer.exe
wine ~/.wine/drive_c/Program\Files/AccessData/FTK\ Imager/FTK\ Imager.exe
```

3. Complete the Installation

4. Launch FTK Imager

Creating a Forensic Image

1. Open FTK Imager and select "File" from the menu.
2. Choose "Create Disk Image..."
3. In the "Disk Image Information" window, provide details such as the source (e.g., the hard drive you want to image) and destination for the forensic image.
4. Choose the type of image you want to create (e.g., physical or logical) and configure any additional settings.
5. Click "Finish" to start the imaging process.
6. The final result shown is the summary page of the operation.

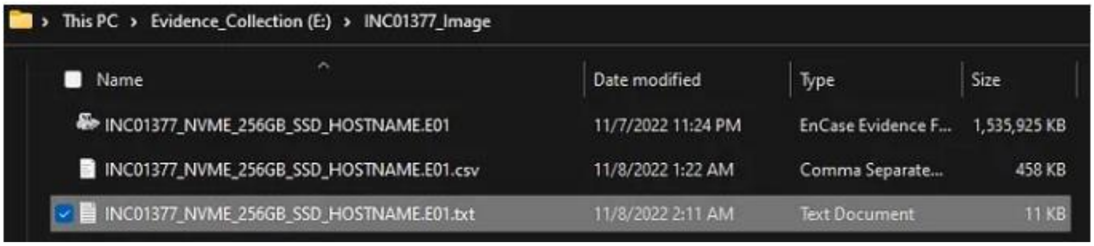


Drive/Image Verify Results

Name	INC01377_NVME_256GB_SSD_HOSTNAME.E01
Sector count	500118192
MD5 Hash	
Computed hash	ebf28fcfd0d3f66281e8bac1c9952e9a
Stored verification hash	ebf28fcfd0d3f66281e8bac1c9952e9a
Report Hash	ebf28fcfd0d3f66281e8bac1c9952e9a
Verify result	Match
SHA1 Hash	
Computed hash	6ce54a1a4d416184c0add17f4c1c2df601d415d9
Stored verification hash	6ce54a1a4d416184c0add17f4c1c2df601d415d9
Report Hash	6ce54a1a4d416184c0add17f4c1c2df601d415d9
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Sector count should match LCD dsiaply value on write-blocker

7. If you navigate to the root of the “Incident/Case#_Image” directory that you created.
8. You will see a text file pre-pended with the image filename; this document contains the summary information that we need to solidify our chain of custody documentation, along with the foundation of analysis which starts with verifying the image hash prior to analyzing.

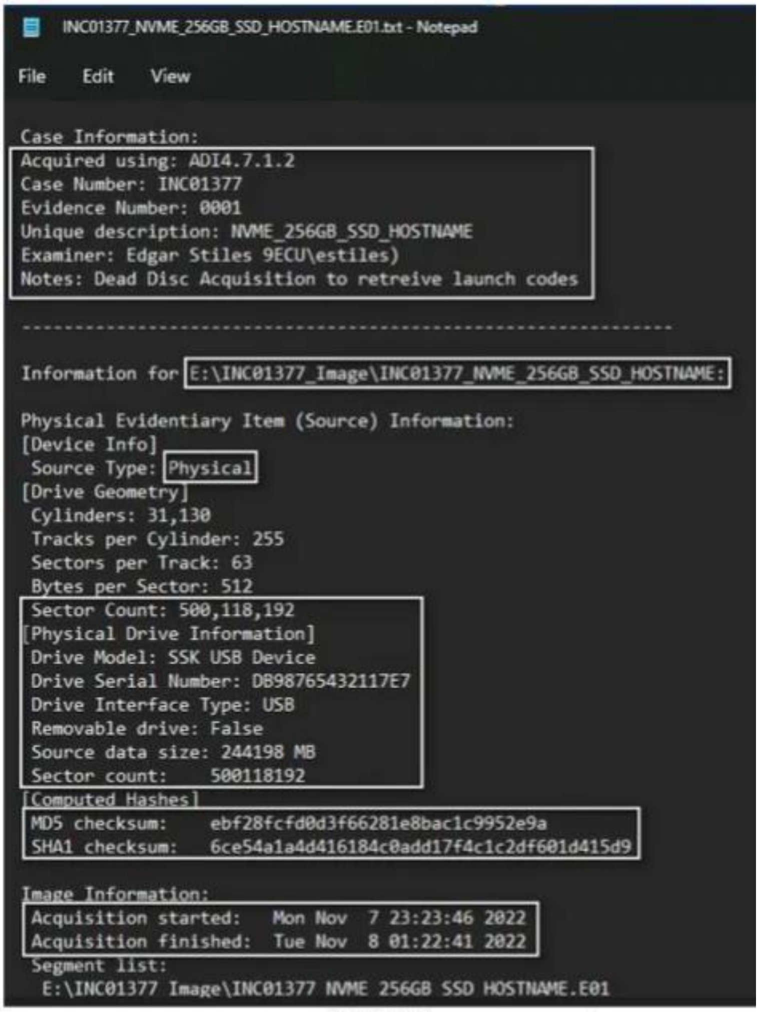


This PC › Evidence_Collection (E:) › INC01377_Image

Name	Date modified	Type	Size
INC01377_NVME_256GB_SSD_HOSTNAME.E01	11/7/2022 11:24 PM	EnCase Evidence F...	1,535,925 KB
INC01377_NVME_256GB_SSD_HOSTNAME.E01.csv	11/8/2022 1:22 AM	Comma Separate...	458 KB
INC01377_NVME_256GB_SSD_HOSTNAME.E01.txt	11/8/2022 2:11 AM	Text Document	11 KB

The E01 file is the base file name of the image, which will be followed by the next 1500MB fragment, at E02 and so on. The .csv file is used to store the directory structure, if available.

9. Open the summary text file and explore the contents.



```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: INC01377
Evidence Number: 0001
Unique description: NVME_256GB_SSD_HOSTNAME
Examiner: Edgar Stiles 9ECU\estiles)
Notes: Dead Disc Acquisition to retreive launch codes

--------------------------------------------------------------

Information for E:\INC01377_Image\INC01377_NVME_256GB_SSD_HOSTNAME:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 31,130
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 500,118,192
[Physical Drive Information]
 Drive Model: SSK USB Device
 Drive Serial Number: DB98765432117E7
 Drive Interface Type: USB
 Removable drive: False
 Source data size: 244198 MB
 Sector count:    500118192
[Computed Hashes]
 MD5 checksum:    ebf28fcfd0d3f66281e8bac1c9952e9a
 SHA1 checksum:   6ce54a1a4d416184c0add17f4c1c2df601d415d9

Image Information:
 Acquisition started:   Mon Nov  7 23:23:46 2022
 Acquisition finished:  Tue Nov  8 01:22:41 2022
 Segment list:
  E:\INC01377 Image\INC01377 NVME 256GB SSD HOSTNAME.E01
```

This summary report is a crucial piece of information needed to augment the chain of custody documentation as this shows the computed hash (pre-image) and stored hash (post-image) match exactly; therefore the Report Hash indicates a valid image. Also shown near the top of the summary page is the sector count of the storage device, as seen by FTK Imager.

K. Practical Proposed Suggested task:

- Capturing Memory
- Analysing Image dump
- Mounting Image to Drive
- Custom Content Image using AD encryption
- Decrypt AD Encryption
- Files and folders Analysis

- Deleted files Analysis

L. References / Suggestions :

1. https://www.sleuthkit.org/autopsy/web_artifacts.php
2. https://www.autopsy.com/category/blog/
3. https://www.sans.org/blog/a-step-by-step-introduction-to-using-the-autopsy-forensic-browser/
4. https://www.youtube.com/watch?v=JVQmJIw5a4Q

M. Assessment-Rubrics:

Sr No.	Performance Indicators	Weightage in %	Marks	Obtained Marks
1	Analyse and identify suitable approach for problem solving	25	0-5	
2	Use of appropriate technology / software / tools	25	0-5	
3	Demonstrate problems as per instructions	20	0-5	
4	Interpret the result and conclusion	15	0-5	
5	Prepare a report/presentation for given problem	15	0-5	
	Total	**100**	**25**	

Sign with Date