ANNA UNIVERSITY CHENNAI UNIVERSITY PRACTICAL EXAMINATION-2024 MAHA BARATHI ENGINEERING COLLEGE CHINNASALEM-606201



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BACHELOR OF ENGINEERING R-2021 CCS354 - NETWORK SECURITY LABORATORY

MAHA BARATHI ENGINEERING COLLEGE

CHINNASALEM-606 201



Bonafide Certificate

	Certified	that	this	is	the	bonafide	record	of	work	done	by
Selv	an/selvi		•••••	••••		Reg]	No:	••••			• • • • •
Year	r:	Sei	meste	r:		Brand	ch of:	••••			•••••
Deg	ree Examir	nation	in the	e Su	ıbject						

Signature Staff-In Charge

Signature of Head of the Department

Submitted for the University Practical Examination held on...... at MAHA BARATHI ENGINEERING COLLEGE, CHINNASALEM - 606 201

Signature of Internal Examiner

Signature of External Examiner

Date:....

Date:....

CONTENTS

Ex.No	Date	Name of the Experiment	Page. No	Marks	Staff Signature
01		IMPLEMENTING SYMMETRIC KEY ALGORITHM			
02(a)		IMPLEMENTING ASYMMETRIC KEY ALGORITHM			
02(b)		IMPLEMENTING KEY EXCHANGE ALGORITHM (DIFFIE-HELLMAN ALGORITHM)			
03		IMPLEMENTING DIGITAL SIGNATURES			
04		INSTALLATION OF WIRESHARK, TCPDUMP AND OBSERVE THE DATA TRANSFERRED IN CLIENT SERVER COMMUNICATION USING TCP/UDP AND IDENTIFY THE TCP/UDP DATAGRAM.			
05		CHECK MESSAGE INTERGRITY AND CONFIDENTIALITY USING SSL			
06		EXPERIMENT EAVESDROPPING, DICTIONARY ATTACKS, MITM ATTACK			
07		EXPERIMENT WITH SNIFF TRAFFIC USING ARP POISONING			
08		DEMONSTRATE INTRUSION DETECTION SYSTEM USING ANY TOOL			
09		EXPLORE NETWORK MONITORING TOOL			
10		STUDY TO CONFIGURE FIREWALL, VPN			

Ex:No:01

IMPLEMENTING SYMMETRIC KEY ALGORITHM

AIM

To implement symmetric encryption cryptography using the Java programming language.

PROCEDURE:

- 1. Class SecureRandom: This class helps generate a secure random number.
- 2. **Class KeyGenerator:** This class provides the functionality for key generator. The following are the standard KeyGenerator algorithms with the key sizes.
- 3. **Approach to generate symmetric key:** The following steps can be followed in order to generate a symmetric key.
 - Create a secrete key using *SecureRandom class* in java which is used to generate a random number. This will be used to Encrypt and Decrypt the data.
 - The KeyGenerator class will provide a *getInstance()* method which can be used to pass a string variable which denotes the Key Generation Algorithm. It returns a KeyGenerator Object.
- 4. Encryption and Decryption using the symmetric key: The following steps can be followed in order to perform the encryption and decryption.
 - Create the Initialization vector that is required to avoid repetition during the encryption process. This is basically a random number. The cipher class provides two functionalities the Encryption and Decryption.
 - Finally *doFinal()* method is invoked on cipher which Encrypts or decrypts data in a single-part operation, or finishes a multiple-part operation and returns a byte array.

PROGRAM

// Java program to implement the// encryption and decryption

import java.security.SecureRandom;

import java.util.Scanner;

import javax.crypto.Cipher;

import javax.crypto.KeyGenerator;

import javax.crypto.SecretKey;

import javax.crypto.spec .IvParameterSpec;

import javax.xml.bind.DatatypeConverter;

// Creating the symmetric

// class which implements

// the symmetric

public class symmetric {

private static final String AES = "AES";

// We are using a Block cipher(CBC mode)

private static final String AES_CIPHER_ALGORITHM =
"AES/CBC/PKCS5PADDING";

private static Scanner message;

// Function to create a

// secret key

public static SecretKey createAESKey()

throws Exception

{

SecureRandom securerandom = new SecureRandom();

KeyGenerator keygenerator = KeyGenerator.getInstance(AES);

keygenerator.init(256, securerandom);

SecretKey key = keygenerator.generateKey();

return key;

}

// Function to initialize a vector

// with an arbitrary value

public static byte[] createInitializationVector()

// Used with encryption

byte[] initializationVector = new byte[16];

```
SecureRandom secureRandom = new SecureRandom();
secureRandom.nextBytes(initializationVector);
```

return initializationVector;

}

{

// This function takes plaintext,

// the key with an initialization

// vector to convert plainText

// into CipherText.

```
public static byte[] do_AESEncryption( String plainText,
SecretKey secretKey, byte[] initializationVector) throws Exception
```

{

```
Cipher cipher =
Cipher.getInstance(AES_CIPHER_ALGORITHM);
```

IvParameterSpec ivParameterSpec = new IvParameterSpec(initializationVector);

cipher.init(Cipher.ENCRYPT_MODE, secretKey, ivParameterSpec);

return cipher.doFinal(plainText.getBytes());

}

// This function performs the

// reverse operation of the

// do_AESEncryption function.

// It converts ciphertext to

// the plaintext using the key.

public static String do_AESDecryption(byte[] cipherText, SecretKey
secretKey, byte[] initializationVector)

throws Exception

{

Cipher cipher = Cipher.getInstance (AES_CIPHER_ALGORITHM);

IvParameterSpec ivParameterSpec = new IvParameterSpec(initializationVector);

```
cipher.init(Cipher.DECRYPT_MODE, secretKey, ivParameterSpec);
```

byte[] result = cipher.doFinal(cipherText);

return new String(result);

}

// Driver code

public static void main(String args[])

throws Exception

{

SecretKey Symmetrickey = createAESKey();

System.out.println("The Symmetric Key is :"+ DatatypeConverter.printHexBinary(Symmetrickey.getEncoded()));

byte[] initializationVector = createInitializationVector();

```
String plaintext = "This is the message "+ "I want To Encrypt.";
```

// Encrypting the message

// using the symmetric key

```
byte[] cipherText = do_AESEncryption(plainText,
Symmetrickey, initializationVector);
```

System.out.println("The ciphertext or "+ "Encrypted Message is: " + DatatypeConverter.printHexBinary(cipherText));

// Decrypting the encrypted

// message

```
String decryptedText = do_AESDecryption( cipherText, Symmetrickey, initializationVector);
```

System.out.println("Your original message is: " + decryptedText);

```
}
```

}

OUTPUT:

Output The Symmetric Key is :AD243EE2408A41726D0D977692664A5A5B70117B9416BFF705C706A10F0A8AF0 Please Enter your Message : This is the message I want To Encrypt. The ciphertext or Encrypted Message is : 925AAB888938921CE8DF51BC022DC4DCB25C103C2652F5420EA290C8A694E2597A6BC747D00B80 Your original message is : This is the message I want To Encrypt.

RESULT:

Thus, the program implements a symmetric key algorithm using java and successfully verified the output.

Ex:No:02(a)

IMPLEMENTING ASYMMETRIC KEY ALGORITHM

AIM

To implement asymmetric key algorithm using the Java programming language.

PROCEDURE:

- 1. To generate a keypair(public, private). The following steps can be followed in order to generate asymmetric key:
 - We need to first generate public & private key using the *SecureRandom class*. SecureRandom class is used to generate random number.
 - The KeyGenerator class will provide *getInstance()* method which can be used to pass a string variable which denotes the Key Generation Algorithm. It returns KeyGenerator Object. We are using RSA algorithm for generating the keys.
 - Initializing the keyGenerator object with 2048 bits key size and passing the random number.
 - Now, the secret key is generated and if we wish to actually see the generated key which is an object, we can convert it into hexbinary format using DatatypeConverter.
- 2. Encryption and Decryption using the asymmetric key: In the above steps, we have created the public & private keys for Encryption and Decryption. Now, let us implement Asymmetric Encryption using the RSA algorithm. The following steps can be followed in order to implement the encryption and decryption.
 - The cipher class is used for two different modes the encryption and decryption. As Asymmetric encryption uses different keys, we use the private key for encryption and the public key for decryption.
 - The *doFinal()* method is invoked on cipher which encrypts/decrypts data in a single-part operation, or finishes a multiple-part operation and returns byte array.

• Finally we get the Cipher text after Encryption with ENCRYPT_MODE.

PROGRAM

// Java program to perform the

// encryption and decryption

// using asymmetric key

package java_cryptography;

import java.security.KeyPair;

import java.security.KeyPairGenerator;

import java.security.PrivateKey;

import java.security.PublicKey;

import java.security.SecureRandom;

import java.util.Scanner;

import javax.crypto.Cipher;

import javax.xml.bind

.DatatypeConverter;

public class Asymmetric {

// Generating public & private keys

// using RSA algorithm.

public static KeyPair generateRSAKkeyPair()

throws Exception

{

SecureRandom secureRandom

= new SecureRandom();

KeyPairGenerator keyPairGenerator

= KeyPairGenerator.getInstance(RSA);

keyPairGenerator.initialize(

2048, secureRandom);

return keyPairGenerator

.generateKeyPair();

}

// Encryption function which converts

// the plainText into a cipherText

// using private Key.

public static byte[] do_RSAEncryption(

String plainText,

PrivateKey privateKey)

throws Exception

{

Cipher cipher

= Cipher.getInstance(RSA);

cipher.init(

Cipher.ENCRYPT_MODE, privateKey);

return cipher.doFinal(

plainText.getBytes());

}

// Decryption function which converts

// the ciphertext back to the

// original plaintext.

public static String do_RSADecryption(

byte[] cipherText,

PublicKey publicKey)

throws Exception

{

Cipher cipher

= Cipher.getInstance(RSA);

cipher.init(Cipher.DECRYPT_MODE,

publicKey);

byte[] result

= cipher.doFinal(cipherText);

return new String(result);

}

// Driver code

public static void main(String args[])

throws Exception

{

KeyPair keypair

= generateRSAKkeyPair();

String plainText = "This is the PlainText "

+ "I want to Encrypt using RSA.";

byte[] cipherText

= do_RSAEncryption(

plainText,

keypair.getPrivate());

System.out.println(

"The Public Key is: "

+ DatatypeConverter.printHexBinary(

keypair.getPublic().getEncoded()));

System.out.println(

"The Private Key is: "

+ DatatypeConverter.printHexBinary(

keypair.getPrivate().getEncoded()));

System.out.print("The Encrypted Text is: ");

System.out.println(

DatatypeConverter.printHexBinary(

cipherText));

String decryptedText

= do_RSADecryption(

cipherText,

keypair.getPublic());

System.out.println(

}

}

"The decrypted text is: "

+ decryptedText);

OUTPUT:

🎯 Javadoc 🗟 Declaration 🧧 Console 🔀

🔳 🗙 💥 🗟 🚮 🗗 🚝

<terminated> Asymmetric [Java Application] C:\Program Files\Java\jre1.8.0_251\bin\javaw.exe (Jun 11, 2020, 1:14:25 PM – 1:15:00 PM)

Enter the plainText to Encrypt and Decrypt

This is the PlainText I want to Encrypt using RSA.

public_key is :30820122300D06092A864886F70D01010105000382010F003082010A0282010100B48C76513803517429532347B
private_key is :308204BC020100300D06092A864886F70D0101010500048204A6308204A20201000282010100B48C7651380351
The Encrypted Text is (ciphertext) : 9D873912E423E8EEB42F261EE7F0A29A36BDCA220D11A5E45021534EC85DFB0B499D0
The decrypted text is : This is the PlainText I want to Encrypt using RSA.

RESULT:

Thus, the program implements an asymmetric encryption using java and successfully verified the output.

Ex:No:2(b)

IMPLEMENTING KEY EXCHANGE ALGORITHM (DIFFIE-HELLMAN ALGORITHM)

AIM

To Implementation of Key Exchange Algorithm (Diffie-Hellman Algorithm) using java program

PROCEDURE:

The Diffie-Hellman algorithm is being used to establish a shared secret that can be used for secret communications while exchanging data over a public network using the elliptic curve to generate points and get the secret key using the parameters.

- For the sake of simplicity and practical implementation of the algorithm, we will consider only 4 variables, one prime P and G (a primitive root of P) and two private values a and b.
- P and G are both publicly available numbers. Users (say Alice and Bob) pick private values a and b and they generate a key and exchange it publicly. The opposite person receives the key and that generates a secret key, after which they have the same secret key to encrypt.

Step 1: Alice and Bob get public numbers P = 23, G = 9

Step 2: Alice selected a private key a = 4 and Bob selected a private key b = 3

Step 3: Alice and Bob compute public values

Alice: $x = (9^4 \mod 23) = (6561 \mod 23) = 6$

Bob: $y = (9^3 \mod 23) = (729 \mod 23) = 16$

Step 4: Alice and Bob exchange public numbers

Step 5: Alice receives public key y = 16 and Bob receives public key x = 6

Step 6: Alice and Bob compute symmetric keys Alice: $ka = y^a \mod p = 65536 \mod 23 = 9$ Bob: $kb = x^b \mod p = 216 \mod 23 = 9$

Step 7: 9 is the shared secret.

PROGRAM

// This program calculates the Key for two persons
// using the Diffie-Hellman Key exchange algorithm
class GFG {

```
// Power function to return value of a ^ b mod P
private static long power(long a, long b, long p)
{
    if (b == 1)
        return a;
    else
        return (((long)Math.pow(a, b)) % p);
}
```

// Driver code

public static void main(String[] args)

long P, G, x, a, y, b, ka, kb;

// Both the persons will be agreed upon the

// public keys G and P

// A prime number P is taken

P = 23;

System.out.println("The value of P:" + P);

// A primitive root for P, G is taken
G = 9;

System.out.println("The value of G:" + G);

// Alice will choose the private key a

// a is the chosen private key

a = 4;

System.out.println("The private key a for Alice:"

+ a);

// Gets the generated key

x = power(G, a, P);

// Bob will choose the private key b

// b is the chosen private key

b = 3;

System.out.println("The private key b for Bob:"

+ b);

// Gets the generated key

y = power(G, b, P);

// Generating the secret key after the exchange

// of keys

}

}

ka = power(y, a, P); // Secret key for Alice

kb = power(x, b, P); // Secret key for Bob

System.out.println("Secret key for the Alice is:"

+ ka);

System.out.println("Secret key for the Bob is:"

+ kb);

OUTPUT

The value of P : 23 The value of G : 9

The private key a for Alice : 4 The private key b for Bob : 3

Secret key for the Alice is : 9 Secret Key for the Bob is : 9

RESULT:

Thus, the program implements a Key Exchange Algorithm (DH algorithm) using java and successfully verified the output.

IMPLEMENTING DIGITAL SIGNATURES

AIM

To Implementation of Digital Signatures using java program.

PROCEDURE:

Let us implement the digital signature using algorithms SHA and RSA and also verify if the hash matches with a public key.

- 1. Create a method named Create_Digital_Signature() to implement Digital Signature by passing two parameters input message and the private key. In this method we will get an instance of the signature object passing the signing algorithm and assign it with a private key and finally pass the input this will return byte array.
- **2.** The next step is to generate asymmetric key pair using RSA algorithm and SecureRandom class functions.
- **3.** Finally verifying the signature using public key. Verify_Digital_Signature() method is used to check whether the signature matches by passing it the input, signature, and public key.

PROGRAM:

// Java implementation for Generating

// and verifying the digital signature

package java_cryptography;

// Imports

import java.security.KeyPair;

import java.security.KeyPairGenerator; import java.security.PrivateKey; import java.security.PublicKey; import java.security.SecureRandom; import java.security.Signature; import java.util.Scanner;

import javax.xml.bind.DatatypeConverter;

public class Digital_Signature_GeeksforGeeks {

// Signing Algorithm
private static final String

SIGNING_ALGORITHM

= "SHA256withRSA";

private static final String RSA = "RSA";

private static Scanner sc;

// Function to implement Digital signature
// using SHA256 and RSA algorithm
// by passing private key.
public static byte[] Create_Digital_Signature(
 byte[] input,
 PrivateKey Key)

throws Exception

Signature signature

= Signature.getInstance(

SIGNING_ALGORITHM);

signature.initSign(Key);

signature.update(input);

return signature.sign();

}

{

// Generating the asymmetric key pair

// using SecureRandom class

// functions and RSA algorithm.

public static KeyPair Generate_RSA_KeyPair()

throws Exception

{

SecureRandom secureRandom

= new SecureRandom();

KeyPairGenerator keyPairGenerator

= KeyPairGenerator

.getInstance(RSA);

keyPairGenerator

.initialize(

2048, secureRandom);

return keyPairGenerator

.generateKeyPair();

}

// Function for Verification of the

// digital signature by using the public key

public static boolean

Verify_Digital_Signature(

byte[] input,

byte[] signatureToVerify,

PublicKey key)

throws Exception

{

Signature signature

= Signature.getInstance(

SIGNING_ALGORITHM);

signature.initVerify(key);

signature.update(input);

return signature

.verify(signatureToVerify);

}

// Driver Code

public static void main(String args[])

throws Exception

String input

{

= "GEEKSFORGEEKS IS A"

+ " COMPUTER SCIENCE PORTAL";

KeyPair keyPair

= Generate_RSA_KeyPair();

// Function Call

byte[] signature

= Create_Digital_Signature(

input.getBytes(),

keyPair.getPrivate());

System.out.println(

"Signature Value:\n "

+ DatatypeConverter

.printHexBinary(signature));

System.out.println("Verification: "+ Verify_Digital_Signature(input.getBytes(), signature, keyPair.getPublic()));

}

}

OUTPUT:

Signature Value: 2492035AE7782EEB75E18C1C76651384FDE30178DBE806A67DA4C884D52BF15A35CB8D1F Verification: true

RESULT:

Thus, the program implements a Digital Signature Scheme using java and successfully verified the output.

Ex:No:04INSTALLATION OF WIRESHARK, TCPDUMP AND
OBSERVE THE DATA TRANSFERRED IN CLIENT
SERVER COMMUNICATION USING TCP/UDP AND
IDENTIFY THE TCP/UDP DATAGRAM.

AIM

To installation of wire shark, tcpdump observe the data transfer in client server communication using TCP/UDP and identify the TCP/UDP datagram.

PROCEDURE

Installation of Wire shark Software

Below are the steps to install the Wire shark software on the computer:

- 1 Open the web browser.
- 2 Search for 'Download Wire shark.'
- **3** Select the Windows installer according to your system configuration, either 32-bt or 64-bit. Save the program and close the browser.
- 4 Now, open the software, and follow the install instruction by accepting the license.
- 5 The Wire shark is ready for use.

Learn Learn Learn Ministrue constant Ind Asso Constant Ind Ind Asso Constant Ind Ind Asso Constant Ind	Edit View Go	Capture Analyze Statistic	cs relephony wireless	Tools Help			
Were tweetend Dependent Internet Internet <tr< th=""><th>l 🔝 🔮 🖬 🔤</th><th>Ctrl-/></th><th></th><th>Q II</th><th></th><th></th><th>Expression</th></tr<>	l 🔝 🔮 🖬 🔤	Ctrl-/>		Q II			Expression
Number Image: State Stat							
Learn Learne de la concetor 1 Learne de la c		Welcome to Wireshark					
Learn Learn Learn Devices with a Contection 10 Lead Asis Contection		Capture	Cher				
Learn Learn Mark Connection 11 M			a capture litter			All interfaces shown	
Learn Learn Used Also Connection *1 Weifi Weifi Due for the Mark 2 connection *1 Weifi Due for the Mark 2 connection *1 Due for the Mar		Local Area Connec Local Area Connec	tion* 8				
Learn Lear Me Connection 1 Lear Area Connection 1 M.F.F. Wi-F. Wi-F. M. Lear Area Connection 1 M. M. M. M. M. M. M. M. M. M.		Npcap Loopback # Ethernet	Adapter ۸				
Learn Learn Wefi Wefi Geneticiton ¹ M Wefi Wefi Geneticiton ¹ M Learner Geneticiton ¹ M Wefi Wefi Geneticiton ¹ M The Face of Wefi Geneticiton ¹ M Second Second Seco		Local Area Connec	tion* 10				
W-fi M		Local Area Connec	tion* 1				
Learn Mer's Cale + Wiki + Questions and Answers + Maling Lists To are running Wirefark 3.0.3 (0-30-0-0-DDB/3200erd). You receive automatic updates. Exty to load or capter In products Type here to search Type here to search Wiref Co Type here to search Type here to search		Wi-Fi	М				
Learn User's Guide : Wikk : Questions and Assvers : Mailing Lats Ta se running Wirehark 3.0.3 (v)o.3.0-96 L3304/250ec)). You receive automatic updates. Text for bladd or capture Virefs for a second in the sec							
Learn Use's Guide :: Vilki : Questions and Answers :: Halling Lists Tou see running Wirelank 3.0.3 (3.0.3.0.9 cpi 1309/32/bled). You recove automatic updates. adv/ to load or captur: Interpretation of the set of the							
Learn User's Guide * Wild * Questions and Answers * Halling Lists Total end of the state of the							
Learn Her's Guide : Wild : Questions and Answers : Halling Lists To a serving Wireshork 1.0.3 (v1.0.3-0-g61205250bcc6). You receive automatic updates. advise for Capture Analyze Statistics Telephony Wireles Tools Help The Source Destination (Capture Capture Capture) (Capture) (Capt							
Learn Der's Guide - Wilk : Questions and Answers - Mailing List To are running Wireshark 3.0.3 (y3.0.3 - 9 d S1309/S20ec65). You receive automatic updates. The blad or capture The blad or capture The blad or capture Analyze Statistics Telephony Wireless Tools Help The Go Capture Analyze Statistics Telephony Wireless Tools Help The Statistics Telephony Wireless Tools Hirp Tools (text/html) B 25.8 (STATIST) Tools To							
Learn Der's Gueder : Wiki - Questions and Answers : Nalling Lists To are running Wirehark 3.0.3 (y.0.3.0.4 optis 2005/2006). You receive automatic updates. addy to lead or capture Type here to search Price							
Learn Ser's Guide * Wiki * Questions and Answers * Maling List To use running Wresherk 3.0.3 (v3.0.3-09 ds 13059206c6). You receive automatic updates. eady to load or capture Type here to search Type here to search							
Learn Ber's Guid: v. Wid: Questions and Answers: * Haling Lists. to are running Wireshark 3.0.3 (v10.0.30-g6130b92b0ec5). You receive automatic updates. early to load or capture No Padets Program Image: Statistics Telephony Wireless Tools Help Image: Statistics Telephony Wireless Tools Help Image: Statistics Telephony Wireless Tools Help Table Registry Image: Statistics Telephony Wireless Tools Table Registry Image: Statistics Telephony Wireless Table Regis							
Lern Use's dute '. Wiki '. Questions and Answers '. Mailing List: To are running Wireshark 3.0.3 (vis.0.3-0-gs13309250ecs). You receive automatic updates. eaty to load or capture No Packs Image: Statistic Sta							
Learn User's Guide · Wiki · Questions and Answers · Mailing Lists To user running Wireshark 3.0.3 (r):0.0-30-g613009250ecol). You receive automatic updates. and the bad or capture							
User's Guide • Wiki • Questions and Answers • Maling List: To user numming Wireshark 3.0.3 (V3.0.3-0.96130b92b0ec6). You receive automatic updates. extry to load or capture Image: Comparison of the compa		Learn					
It user running Wireshark 3.0.3 (v3.0.3-0-g6130592b0cc6). You receive automatic updates. text to load or capture Image: Comparison of the compariso		User's Guide 🕐 Wiki 🕚	Questions and Answers	· Mailing List	5		
ady to load or capture No Padets No Padets No Padets Adv (No Padets) O Type here to search Image: Control of the search Image: Control of the search Adv (No Padets) Adv (No		You are running Wireshark 3.	0.3 (v3.0.3-0-g6130b92b0ec	c6). You receive a	utomatic updates.		
eady to bad or capture No Padets Port							
A the lot of							
y a display filter _ <cuti-></cuti-> Source Destination Protect Length Info Time Source Destination Protect Length Info	oturing from Wi-Fi Edit View Go	Canture Analyze Statistic	cs Telephony Wireless	s Tools Help			- 0
Time Source Destination Protocol Length Info 32 25,683990 23.208.239.129 10.0.066 HTTP 265 HTTP/1.1 200 OK (text/html) 38 25,570122 10.0.0.66 23.209.239.129 TCP 54 62669 + 80 [FLN, ACK) Seq=83 Ack152 Win=77152 Len=0 38 25,88104 23.208.239.129 TCP 54 62669 + 80 [FLN, ACK) Seq=83 Ack=152 Win=71152 Len=0 40 25,881195 10.0.066 23.209.239.129 TCP 54 62669 + 80 [FLN, ACK) Seq=84 Ack=153 Win=17152 Len=0 41 27.081442 f680:71.661.2e7a:180c. ff02:11:2 DFCV6 148 Solicit XID: %r726786 CD: 0001000124c85b704099f385ab261 42 28.05727 10.0.0.3 23.255.255.25 SSDP 216 M-55Ack1+ HTTP/1.1 43 20.081169 10.0.0.23 23.255.255.255 SSDP 216 M-55Ack1+ HTTP/1.1 43 20.081169 10.0.0.23 23.255.255.255 SSDP 216 M-55Ack1+ HTTP/1.1 43 20.080124 116.0.0.23 23.255.255.255 SSDP 216 M-55Ack1+ HTTP/1.1 43 20.060124 10.0.0.2657 (cH:64)(atio6163615) (157) (157 bytes an wire (1336 bits)) 10.0.0.265 10.0.0.265 10.157 bytes on	turing from Wi-Fi Edit View Go	Capture Analyze Statistic ▲ C ۹. ⇔ ⇔ 🗿	cs Telephony Wireless	s Tools Help @ 1997			- 0
36 25.870122 10.0.0.66 23.200.239.129 TCP 54 62669 + 80 [F1N, ACK] Seq=83 Ack=152 Min=17152 Len=0 39 25.881064 23.200.239.129 10.0.0.66 TCP 54 62669 + 80 [F1N, ACK] Seq=132 Ack=454 Min=29312 Len=0 49 25.881064 23.200.239.129 10.0.0.66 TCP 54 62669 + 80 [F1N, ACK] Seq=132 Ack=454 Min=29312 Len=0 49 25.881064 23.200.239.129 10.0.0.66 TCP 54 62669 + 60 [F1N, ACK] Seq=132 Ack=454 Min=29312 Len=0 49 25.881059 10.0.0.63 23.200.239.129 TCP 54 62669 + 60 [F1N, ACK] Seq=132 Ack=454 Min=29312 Len=0 41 27.0934942 fe80:71.661:267.310c	turing from Wi-Fi Edit View Go	Capture Analyze Statistic	cs Telephony Wireless	s Tools Help Q III			- D Expression.
39 25.881064 23.200.239.129 10.0.0.66 TC 54 80 + 62669 [FUI, ACK) Seq-152 Ack-t84 Win-23312 Len-0 40 25.881054 23.200.239.129 TC 54 62669 + 80 + 62669 [FUI, ACK] Seq-152 Ack-t84 Win-23312 Len-0 40 25.881054 27.897 10.0.66 Z3.200.239.129 TC 54 62669 + 80 [ACK] Seq-84 Ack-153 Win=17152 Len-0 40 25.881054 27.877 10.0.67 27.810 [Control of the control of the contr	turing from Wi-Fi dit View Go a (a) (b) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c	Capture Analyze Statistic Capture Analyze Statistic Ctrl-/> Source 23. 246, 238, 139,	cs Telephony Wireless	s Tools Help Q. III Protocol Le	ngth Info 205 HTT2/1 1 200 nV (fact/(bas))		- D Expression.
40 22.081J95 10.00.000 25.200.239.129 10* 34 0.009 + 00 [AK] 50 (AK=15) KIN=1/152 Letter0 41 27.081494 128.00.000 25.200.259.129 10* 34 0.0209 + 00 [AK] 50 (AK=15) KIN=1/152 Letter0 41 27.081494 1680.17681:267.1160: T670:112 DHCPN 4 148 Solicit XDI: 0x726786 CID: 000100124:6557040997385ab261 42 28.081109 10.0.0.23 239.255.255.255 SSDP 216 H-SEARCH + HTTP/1.1 43 29.081109 10.0.0.23 239.255.255.255 SSDP 216 H-SEARCH + HTTP/1.1 44 28.04029 10.0.0.23 239.255.255.255 SSDP 216 H-SEARCH + HTTP/1.1 45 29.081109 10.0.0.23 239.255.255.255 SSDP 216 H-SEARCH + HTTP/1.1 45 29.081109 10.0.0.23 239.255.255.255 SSDP 216 H-SEARCH + HTTP/1.1 45 29.081169 10.0.0.0.0 10.0.0.0.0 10.0.0.0.0 10.0.0.0.0 45 11 167 500 10.0.0.0.0 10.0.0.0.0 10.0.0.0.0 10.0.0.0.0 45 29.051169 10.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.	turing from Wi-Fi citit View Go v a display filter <c Time 37 25.869900 38 25.879122</c 	Capture Analyze Statistic	cs Telephony Wireless	s Tools Help (a) Protocol Le HTTP TCP	ngh Info 205 HTTP/1.1 200 OK (text/html) 54 62669 → 80 [FIN, ACK] Seq=83 Ack=152 Win=17152 Len=0		- D
42 28.67237 10.0.0.23 239.755.255.250 SSDP 216 H-SEARCH * HTTP/1.1 43 29.081169 10.0.0.23 239.755.255.250 SSDP 216 H-SEARCH * HTTP/1.1 45 10.01.23 10.0.0.23 239.755.255.250 SSDP 216 H-SEARCH * HTTP/1.1 46 10.01.24 10.01.02 239.755.255.250 SSDP 216 H-SEARCH * HTTP/1.1 47 10.01.24 10.01.02 10.01.02 10.01.02 10.01.02 47 11.01.24 10.01.02 10.01.02 10.01.02 10.01.02 48 11.01.24 10.01.02 10.01.02 10.01.02 10.01.02 49 12.01.24 10.01.02 10.01.02 10.01.02 10.01.02 49 12.01.02 10.01.02 10.01.02 10.01.02 10.01.02 49 12.01.02 10.01.02 10.01.02 10.01.02 10.01.02 49 12.01.02 10.01.02 10.01.02 10.01.02 10.01.02 49 12.01.02 10.01.02 10.01.02 10.01.02 10.01.02 49 12.01.02 10.01.02 10.01.02 10.01.02 10.01.02	turing from Wi-Fi citit View Go 2 @ @ @ @ @ 2 a display filter <0 Time 37 25.869900 38 25.879122 39 25.881064	Capture Analyze Statistic	cs Telephony Wireless	s Tools Help () Frotocol Le HTTP TCP TCP	ngh info 285 HTP/1.1 200 OK (text/html) 54 62669 480 [F1M, ACK] Seq=83 Ack=152 Wim=17152 Len=0 54 80 + 62669 [F1M, ACK] Seq=152 Ack=84 Wim=29312 Len=0		- D
43 29.081169 10.0.0.23 239.255.250 SSDP 216 M-SEARCH * HTTP/1.1 10.00121 10.00120 10.00120 10.00120 10.00120 me 1: 167 bytes on wire (1336 bits), 167 bytes captured (1356 bits) on interface 0 10.00120 10.00120 mertet IJ, Src: XiaomiLo @isoloff (e44:6016:00:65), 1051: IPV4mest_7f:ff:fa (01:00:5e:7f:ff:fa) 10.00120 10.00120 ernet IJ, Src: XiaomiLo @isoloff (e44:601:00:56:276:ff:ff:fa) 10.00120 10.00120 10.00120 ernet IJ, Src: XiaomiLo @isoloff (e44:601:00:56:276:ff:ff:fa) 10.00120 10.00120 10.00120 ernet IJ, Src: XiaomiLo @isoloff (e44:601:00:56:7f:ff:fa) 10.00120 10.00120 10.00120 ernet IJ, Src: XiaomiLo @isoloff (e44:601:00:56:7f:ff:fa) 10.00120 10.00120 10.00120 ernet IJ, Src: XiaomiLo @isoloff (e44:601:00:56:7f:ff:fa) 10.00120 10.00120 10.00120 ernet IJ, Src: XiaomiLo @isoloff (e44:601:00:56:7f:ff:fa) 10.00120 10.00120 10.00120 ernet IJ, Src: XiaomiLo @isoloff (e44:601:00:56:7f:ff:fa) 10.00120 10.00120 10.00120 ernet IJ, Src: XiaomiLo @isoloff (e44:601:00:56:7f:ff:fa) 10.00120 10.00120 10.00120 ernet IJ, Src: XiaomiLo @isoloff (e44:601:00:56:7f:ff:f	turing from Wi-Fi dit View Go y a display filter Time 37 25.869900 38 25.870122 39 25.881064 40 25.881195 41 27.034942	Capture Analyze Statistic	cs Telephony Wireless Destination 10.0.0.66 23.200.239.129 10.0.0.66 23.200.239.129 10.0.0.66	s Tools Help Tools Help Protocol Le HTTP TCP TCP TCP DHCPV6	ngth Info 205 HTTP/1.1 200 OK (text/html) 54 62669 + 80 [FIN, ACK] Seq=33 Ack=152 Win=17152 Len=0 54 80 + 62669 + 80 [ACK] Seq=452 Ack=84 Win=29312 Len=0 54 62669 + 80 [ACK] Seq=44 Ack=153 Win=17152 Len=0 148 Solicit XID: exf26766 CID: 0001000124c85070409f385b251		- D
me 1: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface 0 ernet II, Src: XiaomiCo_06:a0:5f (e4:46:da:06:a0:5f), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa) ernet Protocol Version 4, Src: 10:0.0.40, Dst: 239.255.255.250 Datagezme Brotocol Src Datact 42575, Det Part: 1904	turing from Wi-Fi dit View Go C C C C C C C C C C C C C C C C C C C	Capture Analyze Statisti	cs Telephony Wireless Destination 10.0.0.66 23.200.239.129 10.0.0.66 23.200.239.129 .ff02:112 239.255.255.259	Tools Help TOOLS Help Protocol Le HTTP TCP TCP DHCPV6 SSDP	rngth Info 205 HTTP/1.1 200 OK (text/html) 54 62669 + 80 [FIN, ACK] Seq=153 Ack=152 Win=17152 Len=0 54 80 + 62669 + 80 [ACK] Seq=154 Ack=153 Win=17152 Len=0 54 62669 + 80 [ACK] Seq=44 Ack=153 Win=17152 Len=0 148 Solicit XID: 0xf26786 CID: 0001000124c85b70409f385ab261 216 H-5EARCH * HTTP/1.1		- D
ernet II, Src: XiaomiCo_06:a0:5f (e4:46:da:06:a0:5f), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa) ernet Protocol Version 4, Src: 10.0.0.40, Dst: 230.255.255.250 Datagezam Bortersion 4, Src: 10.0.0.40, Dst: 230.255.255.250	uring from Wi-Fi dit View Go @ @ @ @ @ Time 37 25.869900 38 25.870122 9 25.881064 40 25.881195 41 27.034942 42 28.057237 43 29.081169	Capture Analyze Statisti	cs Telephony Wireless Destination 10.0.0.66 23.200.239.129 10.0.0.66 23.200.239.129 	Tools Help	ngth Info 205 HTTP/1.1 200 OK (text/html) 54 62669 + 80 [FIN, ACK] Seq=83 Ack=152 Min=17152 Len=0 54 80 + 62669 [FIN, ACK] Seq=84 Ack=153 Min=17152 Len=0 54 62669 + 80 [ACK] Seq=84 Ack=153 Min=17152 Len=0 148 Solicit XID: 0x726786 CID: 0001000124c85b70409f385ab261 216 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1		- C
enter violatori visitori visitori visito 155.257.250	uring from Wi-Fi dit View Go @ @	Capture Analyze Statisti Capture Analyze Statisti Cht/> Source 23.200.239.129 10.0.0.66 fe80::7166:2e7a:18c. 10.0.0.23 10.0.0.23 10.0.0.23	cs Telephony Wireless Destination 10.0.0.66 23.200.239.129 10.0.0.66 23.200.239.129 .ff02:1:12 239.255.255.250 239.255.255.250 107 bytes captured	s Tools Help Q II Protocol Le HTTP TCP TCP TCP DHCPv6 SSDP SSDP SSDP SSDP SSDP	ngth info 205 HTFV/.1 200 OK (text/html) 54 6269 + 68 [FIN, ACK] Seq=83 Ack=152 Win=17152 Len=0 54 80 + 62669 + 80 [ACK] Seq=44 Ack=153 Win=2732 Len=0 148 Solicit XUI: 0x72764 Ack=153 Win=17152 Len=0 148 Solicit XUI: 0x72764 CID: 0001000124c35070409f385ab251 216 M-SEARCH * HTTP/1.1 ACCM CEARCH * HTTP/1.1 ACCM CEARCH * HTTP/1.1		- D
	uring from Wi-Fi dit View Go a display filter	Capture Analyze Statistic	cs Telephony Wireless Destination 10.0.0.66 23.200.239.129 10.0.0.66 23.200.239.129 10.0.0.66 23.200.239.129 1762:112 239.255.255.250 10.0.0.66 10.0.0.65 10.0.0.66 10.0.0.66 10.0.0.66 10.0.0.66 10.0.0.65 10.0.0.66 10.0.0.66 10.0.0.66 10.0.0.55 10.0.0.66 10.0.0.66 10.0.0.66 10.0.0.66 10.0.0.66 10.0.0.66 10.0.0.55 10.0.0.66 10.0.0.55 10.0.0.06 10.0.0.66 10.0.0.66 10.0.0.66 10.0.0.66 10.0.0.66 10.0.0.66 10.0.0.66 10.0.0.66 10.0.0.66 10.0.0.55 10.0.55 10	s Tools Help Q II Protocol Le HTTP TCP TCP DHCPv6 SSDP SSDP SSDP SSDP SSDP SSDP SSDP	rgth Info 205 HTTP/1.1 200 OK (text/html) 54 62669 + 60 [FIN, ACK] Seq=33 Ack=152 Win=17152 Len=0 54 80 + 62669 + 80 [ACK] Seq=34 Ack=153 Win=29312 Len=0 148 Solicit XID: 0x756786 CID: 0001000124c85b70409f385ab261 216 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 21		- D
ole Service Discovery Protocol	uring from Wi-Fi dit View Go a display fiter Time 37 25.869900 38 25.870122 38 25.831064 49 25.831064 40 25.831064 49 25.831064 40 25.831064 49 25.831064 40 25.831064 49 25.831064 40 25.831064 49 25.831064 40 25.831064 49 25.831064 40 25.831064 49 25.831064 40 25.831064 49 25.831064 40 25.831064 49 25.831064 40 25.831064 49 25.831064 40 25.831064 49 25.831064 40 25.831064 49 49 40 25.831064 49 49 49 40 25.831064 49 49 49 40 25.831064 49 49 49 40 25.831064 49 49	Capture Analyze Statisti	cs Telephony Wireless Destination 10.0.0.66 23.200.239.129 10.0.0.66 23.200.239.129 167.255.255.250 239.255.255.250 167.bytes captured 1 46ciai060:a0:57), Ds1 46ciai060:a0:57), Ds1 46b; Ds1: 239.255.250 195.Port: 1960	Tools Help Trop Protocol Le HTTP TCP TCP TCP TCP OHCPv6 SSDP CCOD (1366 bits) o (1: IPv4mcast 55.250	<pre>mgth Info 205 HTTP/1.1 200 OK (text/html) 54 62669 + 80 [FIN, ACK] Seq=152 Ack=152 Win=17152 Len=0 54 80 + 62669 + 80 [ACK] Seq=152 Ack=48 Win=23122 Len=0 148 Solicit XTD: 0xf26786 ClD: 0001000124c85b70409f385ab261 216 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 218 M-SEARCH * HTTP/1.1 219 M-SEARCH * HTTP/1.1 210 M-SEARCH * HTTP/1.1 210 M-SEARCH * HTTP/1.1 210 M-SEARCH * HTTP/1.1 211 M-SEARCH * HTTP/1.1 212 M-SEARCH * HTTP/1.1 213 M-SEARCH * HTTP/1.1 214 M-SEARCH * HTTP/1.1 215 M-SEARCH * HTTP/1.1 215 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 218 M-SEARCH * HTTP/1.1 219 M-SEARCH * HTTP/1.1 210 M-SEARCH * HTTP/1.1 210 M-SEARCH * HTTP/1.1 210 M-SEARCH * HTTP/1.1 211 M-SEARCH * HTTP/1.1 212 M-SEARCH * HTTP/1.1 214 M-SEARCH * HTTP/1.1 21</pre>		- O
	uring from Wi-Fi dit View Go C C C C C C C C C C C C C C C C C C C	Capture Analyce Statistic	cs Telephony Wireless Destination 10.0.0.66 23.200.239.129 10.0.0.66 23.200.239.129 10.0.0.66 23.200.239.129 1672:112 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250 246:da:06:da:057), Dst A40, Dst: 239.255.25 Dst Port: 1960	s Tools Help Q Ⅲ Protocol Le HTTP TCP TCP DHCPv6 SSDP SSDP SSDP SSDP SSDP SSDP SSDP SSDP SSDP SSDP	ngb Info 205 HTTP/1.1 200 OK (text/html) 54 62609 + 60 [FIM, ACK] Seq=33 Ack=152 Win=17152 Len=0 54 80 + 62609 + 80 [ACK] Seq=43 Ack=153 Win=22312 Len=0 148 Solicit XID: 0xf26766 CID: 0001000124c85b70409f385ab261 216 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.2 216		- D
	uring from Wi-Fi dit View Go a deplay fiter 3 deplay fiter Time 3 25.86990 38 25.870122 9 25.881064 40 25.881054 14 27.034942 42 28.057237 32 0.081169 5.881084 12 7.034942 12 7.034942 12 7.034942 12 7.034942 12 7.034942 12 7.034942 12 7.034942 12 7.034942 12 7.034942 12 8.081169 12 7.034942 12 8.081169 12 7.034942 12 8.081169 12 8.081169 13 10 9 00000000000000000000000000000000	Capture Analyze Statisti	cs Telephony Wireless Destination 10.0.0.66 23.200.239.129 10.0.0.66 23.200.239.129 10.0.0.66 23.200.239.129 167.255.255.250 239.255.255.250 167.bytes captured I 46c:a40:66:a45:75), Ds1 446:a40:66:a45:75), Ds1 440; Ds1: 239.255.25 Jst Port: 1900	s Tools Help Protocol Le HTTP TCP TCP TCP SSOP	<pre>mgth Info 205 HTTP/1.1 200 OK (text/html) 54 62669 + 80 [FIN, ACK] Seq=33 Ack=152 Win=17152 Len=0 54 80 + 62669 + 80 [ACK] Seq=44 Ack=153 Win=29312 Len=0 148 Solicit XTIO : 9x750786 ClD: 0001000124c85b70409f305ab261 216 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 217 HTTP/1.1 217 HTTP/1.1 218 HTTP/1.1 219 HTTP/1.</pre>		- D
	uring from Wi-Fi dit View Go Compared to the second second a display filter	Capture Analyze Statisti	cs Telephony Wireless Destination 10.0.0.66 23.200.239.129 .ff02:1:12 239.255.255.250 239.255.255.250 167 bytes captured 146:da:06:0:0:57), Ds1 .460, Ds1: 239.255.25 .460, Ds1: 239.255 .460, Ds1: 239.255	s Tools Help Protocol Le HTTP TCP TCP DTCPv SSOP	rngh info 205 HTTP/1.1 200 OK (text/html) 54 82669 + 80 [FIN, ACK] Seq=33 Ack=152 Win=17152 Len=0 54 80 + 62669 + 80 [ACK] Seq=44 Ack=153 Win=27152 Len=0 148 Solicit XDI: 0xf6786 CID: 0001000124c85b70409f385ab261 216 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1		- D
01 00 5c 7f ff fa c4 46 da 06 a0 5f 08 00 45 00 ·····F ·····F	uring from Wi-Fi dit View Go a display filter	Capture Analyze Statisti	cs Telephony Wireless	Robert Help Robert Help Protocol Le HTTP TCP TCP TCP TCP TCP TCP TCP	ngth info 205 HTFV/1.1 200 OK (text/html) 54 62669 + 68 [FIN, ACK] Seq=83 Ack-152 Win=17152 Len=0 54 80 + 62669 ; 60 [ACK] Seq=44 Ack-153 Win=27152 Len=0 148 Solicit XUI: 0x72676 CDI: 0001000124c35070409f385ab251 216 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 ACCM CEARCH * HTTP/1.1 AC		- C
01 00 5e 7f ff fa e4 46 da 06 a0 5f 08 00 45 00 ·····F ·····E· 00 99 75 e3 40 00 02 11 08 4f 0a 00 00 28 ef ff ···u@··· ····. ff aa 64 f0 76 c6 08 5 29 7d 42 2d 53 45 45 25 ······························	uring from Wi-Fi dit View Go a dipbay filter Time Time 37 25.869900 38 25.870122 38 25.81064 49 25.881064 40 25.881054 42 28.081269 41 27.034942 42 28.081269 42 29.081169 42 29.081169 45 29.081169 50 areas 56 areas Frotocol Datagram Protocol Datagram Protocol 01 00 5c 7f ff 60 97 5c 31 40 61 00 5c 7f ff fa a 64 40 75 c3 44 40	Capture Analyze Statisti	cs Telephony Wireless Destination 10.0.0.66 23.200.239.129 10.0.0.66 23.200.239.129 10.0.0.66 23.200.239.129 157.55.250 239.255.255.250 239.255.255.250 167.57 bytes captured 44:44:46:40:40:457), pst 0.40, pst: 239.255.25 Date Port: 1900 08.00 45 00 00 28 ef ff 00 28 ef ff 2.0.01	5 Tools Help	rgh Info 205 HTF7/1.1 200 OK (text/html) 54 62669 + 80 [FIN, ACK] Seq=83 Ack=152 Win=17152 Len=0 54 80 + 62669 [FIN, ACK] Seq=83 Ack=153 Win=27152 Len=0 148 Solicit XDI: 0x750766 CDI: 0001000124c85b70409f385ab261 216 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 218		- O
01 00 5c 7f ff fa e4 46 da 06 a0 5f 08 00 45 00 ······F ·····F: 00 99 75 c3 40 00 02 11 08 4f 0a 00 00 22 ef ff ·····ĝ··· O···()··· ff fa a6 4f 07 6c 00 85 29 7f 4d 25 34 54 15 5c ····O·1··)/PI-SEAR 45 48 54 54 30 34 54 54 55 43 71 31 62 31 64 68 38 56 77 170 /1.5 14 1 45 48 54 54 30 54 54 55 45 54 56 48 58 56 75 75 75 75 75 75 75 75 75 75 75 75 75	uning from Wi-Fi dit View Go Compared and the second second Time a display filter 7 25.869900 38 25.870122 9 25.881064 40 25.881054 41 27.034942 42 32.881169 43 32.881169 43 32.881169 43 32.881169 43 32.881169 43 32.881169 43 32.881169 43 32.881169 43 32.881169 43 32.881169 43 32.881169 43 32.881169 43 32.881169 43 32.881169 44 32.881169 43 32.881169 44 32.881169 45 32.484 46 35 46 47 47 48 48 48 48 48 48 48 48 48 49 55 44 48 48 40 55 47 ff ff a 41 64 68 48 48 48 41 64 68 48 48 48 41 64 68 48 48 48 41 64 68 48 48 48 41 65 44 68 48 48	Capture Analyze Statisti	cs Telephony Wireless Destination 10.0.0.66 23.200.239.129 10.0.0.66 23.200.239.129 10.0.0.66 23.200.239.129 167.252,55.250 239.255.255.250 167.bytes captured 446:da:08:0a:057), Dst A40, Dst: 239.255.25 Dst Port: 1960 08.00 45.00 29.25 cf ff 19.00 08.00 45.00 29.25 cf ff 19.00 20.25 cf ff 19.00 20.25 cf ff 19.00 20.25 cf ff 20.25	5 Tools Help Protoci Le HTTP TCP TCP TCP SSDP S	ngb Info 205 HTTP/1.1 200 OK (text/html) 54 62669 + 60 [FIM, ACK] Seq=33 Ack=152 Win=17152 Len=0 54 80 + 62669 + 80 [ACK] Seq=44 Ack=153 Win=27322 Len=0 148 Solicit XID: 0xf26766 CID: 0001000124c65b70409f385ab261 216 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 216		- D
01 00 5e 7f ff fa e4 46 da 06 a0 5f 08 00 45 00 ··^···F ···_··E· 00 99 75 e3 40 00 02 11 08 4f 0a 00 00 28 ef ff ·····ê····E· ff fa a6 4f 07 6c 08 52 97 dd 42 63 a5 41 52 ·····1···) JN-SEAR 43 48 20 a 22 43 53 45 56 71 31 c8 10 40 48 Cf ·····F ······F····· 4f 53 54 3a 20 32 33 39 2e 32 53 52 e2 23 53 50 57: 239 .255.255 23 25 53 a3 13 93 00 d0 40 44 41 46 3a 20 .255.255	uning from Wi-Fi dit View Go Compared Compared	Capture Analyze Statisti	cs Telephony Wireless Destination 10.0.0.66 23.200.239.129 10.0.0.66 23.200.239.129 10.0.0.66 23.200.239.129 239.255.255.250 239.255.255.250 10.0.0.66 23.200.239.129 10.0.0.66 23.200.239.129 10.0.0.66 23.250.255.250 239.255.255 10.0.0.66 23.200.239.129 10.0.0.66 23.250.255.250 239.255.255 250.250 239.255.255 250.250 239.255.255 250.250 239.255.255 250.250	5 Tools Help Protocol Le HTTP TCP TCP TCP TCP TCP TCP SSOP	<pre>ingh info 285 HTTP/1.1 200 OK (text/html) 54 62669 + 80 [FIN, ACK] Seq=33 Ack=152 Win=17152 Len=0 54 80 + 62669 + 80 [ACK] Seq=44 Ack=153 Win=17152 Len=0 148 Solicit XTIO: exf26786 ClD: 0001000124c85b70409f385ab261 216 H-SEARCH * HTTP/1.1 216 H-SEARCH * HTTP/1.1 216 H-SEARCH * HTTP/1.1 217 H TFACE 0 7f:ff:fa (01:00:5e:7f:ff:fa) </pre>		- D
01 00 5e 7f ff fa e4 46 da 06 a0 5f 08 00 45 00 ···^···F ····E· 00 99 75 e3 40 00 02 11 08 4f 0a 00 00 28 ef ff ·····ê···F ·····E· ff fa a6 4f 07 6c 00 85 29 7d 4d 2d 53 45 41 52 ····0·1··)}N-SEAR 44 82 02 a2 20 48 54 54 50 47 31 2e 31 00 49 48 Cf + NTT P/1.1··H 4f 53 54 3a 20 32 33 39 2e 32 33 52 e3 23 53 50 57: 239 .255.255 232 35 30 33 13 39 30 00 40 49 44 44 e3 a2 00 .255.255 232 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 00 "sadp:di acover". 94 46 83 a3 20 31 64 09 33 54 3a 20 75 26 es 3a "NS11-··ST	turing from Wi-Fi didt View Go	Capture Analyze Statisti	cs Telephony Wireless → → → → → → → → → → → → → → → → → → →	5 Tools Help	angh Info 205 HTTP/1.1 200 OK (text/html) 54 62699 + 80 [FIN, ACK] Seq=83 ACt=52 Min=17152 Len=0 54 62669 + 80 [ACK] Seq=84 Ack=153 Win=17152 Len=0 146 Solicit XUID: 0x72676 CID: 0001000124c350704097385ab201 216 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 Acc. Crance 0 7f:ff:fa (01:00:5e:7f:ff:fa)		- 0
01 00 5e 7f ff fa e4 46 da 06 a0 5f 08 00 45 00 ···^···F ···_··E· 00 99 75 e3 40 00 02 11 08 4f 0a 00 00 28 ef ff ·····g····E· ff fa a6 4f 07 6c 00 85 29 7d 4d 2d 53 45 41 52 ·····0···(·· 4f 63 64 60 7 6c 00 85 29 7d 4d 2d 53 45 41 52 ·····0·1··)}M··SEAR 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 59 57: 239 .255.255 22 27 37 3 64 70 3a 64 69 73 63 6f 76 65 72 22 0d "ssdp:ldi accover"· 0a 4d 56 3a 20 31 0d 0a 55 44 3a 20 75 72 6e 3a ··/W: 1·· S1: urn: 64 69 50 16 22 0d 75 6c 7 46 97 36 37 26 55 66 ed ial-mult tiscreen	Uning from Wi-Fi didt View Go	Capture Analyze Statisti	cs Telephony Wireless Destination 10.0.0.66 23.200.239.129 10.0.0.0.66 23.200.239.129 123.200.239.129 10.0.0.0.66 23.200.239.129 239.255.255.250 107 Dytes captured 46:da:06:a0:57), 051 040, 051: 239.255.25 0.05 Ports: 1900 053.454 152.052 0.05 Ports: 239.255.255.250 051.239.255.25 051.239.255.25 0.05 Ports: 1900 055.255.250 051.239.255.25 0.05 Ports: 1090 055.255.250 051.239.255.25 0.05 Ports: 1090 055.255.250 051.239.255.250 0.05 Ports: 1090 053.454 152.235.25 0.05 Ports: 1000 020.26 ff	Tools Help Q	rngh Info 205 HTP/1.1 200 OK (text/html) 54 62669 + 80 [FIN, ACK] Seq=83 Ack=152 Win=17152 Len=0 54 60 + 62669 [FIN, ACK] Seq=43 Ack=153 Win=17152 Len=0 148 Solicit XDI: 0xf26766 CDI: 0001000124c35b70409f385ab251 216 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 218 M-SEARCH * HTTP/1.2 218 M-SEARCH * HTTP/1.2 218 M-SEARCH * HTTP/1.2 218		- D
01.00 5c 7f ff fa c4 46 da 06 a0 5f 08 00 45 00 <t< td=""><td>turing from Wi-Fi didt View Go C C C C C C C C C C C C C C C C C C C</td><td>Capture Analyze Statisti</td><td>cs Telephony Wireless → ① □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □</td><td>s Tools Help</td><td>rgth Info 205 HTTP/1.1 200 OK (text/html) 54 025609 + 00 [FIN, ACK] Seq=35 ACk=152 Win=17152 Len=0 54 00 + 5060 FIN, ACK] Seq=43 ACk=153 Win=27312 Len=0 148 Solicit XII: 0x752765 CID: 0001000124c55b70409f385ab261 216 M-SEARCH * HTTP/1.1 ACK & CARACL * HTTP/1.1 ACK</td><td></td><td>- D</td></t<>	turing from Wi-Fi didt View Go C C C C C C C C C C C C C C C C C C C	Capture Analyze Statisti	cs Telephony Wireless → ① □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	s Tools Help	rgth Info 205 HTTP/1.1 200 OK (text/html) 54 025609 + 00 [FIN, ACK] Seq=35 ACk=152 Win=17152 Len=0 54 00 + 5060 FIN, ACK] Seq=43 ACk=153 Win=27312 Len=0 148 Solicit XII: 0x752765 CID: 0001000124c55b70409f385ab261 216 M-SEARCH * HTTP/1.1 ACK & CARACL * HTTP/1.1 ACK		- D
01 00 5e 7f ff fa e4 46 da 06 a0 5f 08 00 45 00 E 00 99 75 e3 40 00 02 11 08 4f 0a 00 00 28 ef ff E 17 fa a6 4f 07 6c 08 52 29 7d 4d 24 53 45 41 52	turing from Wi-Fi didt View Go	Capture Analyze Statistic Image: Capture Source Source Source 23.200.239.129 10.0.0.66 23.200.239.129 10.0.0.66 23.200.239.129 10.0.0.66 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.23 10.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.23 10.0.0.23	cs Telephony Wireless Destination 10.0.0.66 23.200.239.129 10.0.0.66 23.200.239.129 239.255.255.250 10.0.0.66 23.200.239.129 239.255.255.250 10.0.0.66 23.200.239.129 239.255.255.250 10.0.0.0.66 23.200.239.129 239.255.255.250 10.0.0.0.66 23.200.239.129 230.255.250 10.0.0.0.66 23.259.255.250 230.255.250 0.000 28 eff ff	5 Tools Help Protocol Le HTTP TCP TCP TCP SSOP	ngth info 205 HTTP/1.1 200 OK (text/html) 54 62669 + 80 [FIN, ACK] Seq=83 Ack=152 Min=17152 Len=0 54 6269 + 80 [ACK] Seq=46 Ack=153 Min=17152 Len=0 148 Solicit XID: 00:76786 CID: 0001000124c85b70409f385ab261 216 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 Act = centrix = intro: interface 0 7f:ff:fa (01:00:5e:7f:ff:fa)		- D
01 00 5e 7f ff fa e4 46 da 06 a0 5f 08 00 45 00 E- 00 99 75 e3 40 00 02 11 08 4f 0a 00 02 8e ff E- 11 6a 4f 07 5c 08 52 29 7d 4d 2d 53 45 41 52	uning from Wi-Fi dit View Go a depay filer . < Time 37 25.869909 38 25.870122 39 25.81064 40 25.88195 32 25.81064 40 25.881195 11 27.034942 42 28.057237 43 29.081169 11 307 byte: rnet Protocol r Datagram Protocol r Datagram Protocol r Datagram Protocol r Datagram Protocol d0 99 75 63 40 40 69 92 75 63 40 40 69 92 73 40 43 48 30 22 20 44 68 32 20 64 69 61 6c 20 46 67 67 33 6c 3a 31 0d 6a	Capture Analyze Statistic Image: Capture 23.280.239.129 10.0.0.66 23.280.239.129 10.0.0.66 10.0.0.23 10.0.0.66 7680:7168:2673:186.1 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.03 10.000 10.000 10.000 20.211 80.470 10.22 10.223 10.233 13.33 10.0	cs Telephony Wireless → → → → → → → → → → → → → → → → → → →	Tools Help Q	angth Info 205 HTTP/1.1 200 OK (text/html) 54 62669 + 80 [FIN, ACK] Seq=83 Ack=152 Min=17152 Len=0 54 62669 + 80 [FAR, JSeq=84 Ack=153 Win=17152 Len=0 54 62669 + 80 [ACK] Seq=84 Ack=153 Win=17152 Len=0 148 Solicit XID: 0*726766 CID: 0001000124c65b704097385ab261 216 H-SEARCH + HTTP/1.1 ALC - CEARCH + HTTP/1.1 ALC		- 0
81 00 5e 7f ff fa e4 46 da 06 a0 5f 08 00 45 00 •••••••••••••••••••••••••••••	uring from Wi-Fi dit View Go a dipby filter . < Time 37 25.869900 38 25.870122 38 25.870122 39 25.881955 41 27.031942 42 28.057237 41 27.031942 42 28.057237 41 27.031942 42 28.057237 41 27.031942 42 28.057237 42 28.057237 42 28.057237 42 28.057237 42 28.057237 42 28.057237 42 28.057237 42 28.057237 44 28.057237 44 53 54 36 22 35 30 36 44 53 54 36 22 35 30 36 22 37 37 36 4706 43 48 20 28 20 22 37 37 36 4706 44 53 54 36 22 35 30 36 23 33 30 46 36 45 36 24 45 36 25 36 26 45 36 27 57 28 57 29 57 29 57 29 57 29 57 20 57	Capture Analyze Statistic Image: Capture Q Ref Ref Temp Source 23.200.239.129 10.0.0.66 23.200.239.129 10.0.0.66 23.200.239.129 10.0.0.66 10.0.0.66 10.0.0.23 10.0.0.23 Source 23.200.239.129 10.0.0.23 10.0.0.23 10.0.0.23 Source 23.200.239.129 10.0.0.23 10.0.0.23 10.0.0.23 Source 23.200.239.125 10.0.0.23 10.0.0.23 10.0.0.23 Source 21.188.126.200.118 84.680.57 10.0.023 10.0.023 Fa e4.46 da 06.a90.57 10.0.023 10.0.023 Scource 77.33 10.333 30.333 32.335 33.333 32.335 33.333 33.333 32.335 33.333 32.335 33.333 33.33 33.33 33.33 33.33 33.33 33.33 33.33 33.33 33.33 33.33 34.64 37.64 37.33 35.46 37.35 37.35 35.73	cs Telephony Wireless Destination 10.0.0.66 23.200.239.129 10.0.0.66 23.200.239.129 123.200.239.129 10.0.0.66 23.200.239.129 239.255.255.250 239.255.255.250 239.255.255.250 239.252.25.250 167 bytes captured 46:dan06:a0:57), Dist 0.00 0.05 Dertr: 1900 1900 0.05 26 ef ff	Tools Help Q	ngth info 205 HTP/1.1 200 OK (text/html) 54 62669 + 86 [FIN, ACK] Seq=83 Act=52 Win=17152 Len=0 54 62669 + 00 [ACK] Seq=44 Act=153 Win=17152 Len=0 148 Solicit AUTO: 0xf26766 CDI: 0001000124C55070409f385ab251 216 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 ACCM_CFARCL * HTTP/1.1 ACCM_CF		- D
01 00 5e 7f ff fa e4 46 da 06 a0 5f 08 00 45 00 e. 00 99 75 e3 40 00 02 11 08 4f 0a 00 02 28 ef ff ê. 01 99 75 e3 40 00 02 11 08 4f 0a 00 02 28 ef ff ê. 01 43 20 22 23 45 54 54 52 13 12 81 00 40 48 6K + HTT P/1.1H 4f 53 43 20 22 33 39 2e 32 53 52 e 22 53 55 22 73 73 64 70 3a 64 69 73 63 76 65 72 22 04 04 45 83 20 31 04 0a 354 34 257 22 72 66 3a 04 45 83 20 31 04 0a 354 32 07 27 26 43 a 04 59 73 65 72 76 69 63 65 3a 64 69 61 06 69 04 60 0a	uning from Wi-Fi dit View Go C C C C C C C C C C C C C C C C C C C	Capture Analyze Statisti	cs Telephony Wireless Destination 10.0.0.66 23.200.239.129 10.0.0.66 23.200.239.129 123.255.255.250 10.0.0.0.66 23.200.239.129 123.255.255.250 10.7 bytes captured 46:da:06:a0:557), bst 167 bytes captured 46:da:06:a0:557, Dst Dst Port: 1900 1900 88:00:45:00 10.40, bst: 259.255.25 10.7 bytes captured 46:da:06:a0:557), bst 44:da:06:a0:557) Dst 10.7 bytes captured 46:da:06:a0:557 55.55 555 53:45:41:52	5 Tools Help	rgth Info 205 HTT9/1.1 200 OK (text/html) 54 62669 + 80 [FIN, ACK] Seq=83 ACk=152 Win=17152 Len=0 54 62669 + 80 [ACK] Seq=84 Ack=153 Win=27152 Len=0 148 Solicit XID: 0xf26766 CID: 0001000124c35b70409f385ab261 216 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 218 M-SEARCH * HTTP/1.1 218 M-SEARCH * HTTP/1.1 218 M-SEARCH * HTTP/1.1 219 M-SEARCH * HTTP/1.1 210 M-SEARCH * HTTP/1.2 210 M-SEARCH * HTTP/1.2 210 M-SEARCH * HTTP/1.2 210 M-S		
81.00 5c 7f ff fa e4 46 da 06 a0 5f 06 00 45 00 AF E 00 99 75 c3 40 00 02 11 08 4f 0a 00 00 28 cf ff E E 11 43 20 72 26 48 54 54 59 27 13 12 23 10 40 54 84 Cf	uning from Wi-Fi if View Go adapay fiter a maga fiter Time 3 25,869908 38 25,870122 92 55,881064 40 25,881054 41 27,034942 42 28,697237 12 29,081169 42 33 29,081169 41 00 5e 7f ff 41 00 5e 7f ff 46 59 57 c3 46 47 53 54 20 22 20 27 3 73 64 76 46 59 61 62 2d 22 73 73 64 76 46 59 61 62 2d 26 65 33 31 0d 0a	Capture Analyze Statistic Image: Capture Source Source Source 23.200.239.129 10.0.0.66 10.0.0.66 10.0.0.66 10.0.0.66 10.0.0.66 10.0.0.23 10.0.0.23 10.0.0.23 30.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 30.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 30.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 4.0.0.24 10.0.0.23 10.0.0.23 10.0.0.23 10.0.0.23 5.0.01 Arc Part (1336 bitts), Xitaonic (0.06:a0:5f (e4: Version 4, Src: 10.0.0) Scovery Protocol 7 10.0.02 11.00 de 46 a.00 fe 47 da 20 10.00 de 42 23 25 25 35 13.1 a0 23 30 22 25 25 35 13.1 a0 40 a.3 54 33 20 22 35 65 31 23 39 23 30 40 de 42 23 35 25 35 13.1 a0 40 a.3 54 35 46 37 36 67 76 67 31 a0 47 66 27 36 67 76 53 1 a0 40 a.23 55 45 a.20 76 69 63 65 10.00 de a.23 55 45 a.20 76 69 63 65 10.00 de a.23 55 45 a.20 77 65 69 63 65	cs Telephony Wireless	S Tools Help Protoci Le HTTP TCP TCP TCP SSOP	rgh Info 205 HTTP/1.1 200 OK (text/html) 54 62669 + 60 [FIN, ACK] Seq=33 Ack=152 Win=17152 Len=0 54 80 + 62669 + 80 [ACK] Seq=44 Ack=153 Win=27322 Len=0 148 Solicit XII: 0xf26768 CID: 0001000124c85b70409f385ab261 216 M-SEARCH * HTTP/1.1 Ack & CARACL * HTTP/1.2 Ack		- D
01.00 5e 7f ff fa e4 46 da 06 a0 5f 08 00 45 00 F E 00 99 75 e3 40 00 02 11 08 4f 0a 00 02 26 ef ff	uring from Wi-Fi dit View Go a diaplay fiter <1 Time 7 25.869960 38 25.870122 39 25.831064 40 40 56.77164 40 40 56.77364 40 40 56.222 40 45.6523 40 45.6523 40 45.6523 40 45.8310 40 45.8523 40 45.85253 40 45.85253 40 45.8525555 40 45.852555555555555555	Capture Analyze Statisti	cs Telephony Wireless	s Tools Help Protoci Le HTTP TCP TCP TCP TCP TCP TCP SSDP	ngh Info 205 HTTP/1.1 200 OK (text/html) 54 62609 - 80 [FIN, ACK] Seq=83 Ack=152 Min=17152 Len=0 54 62609 - 86 [ACK] Seq=452 Ack=154 Min=7152 Len=0 148 Solicit XID: 0xf26786 CID: 0001000124c85b70409f385ab261 216 M-SEARCH + HTTP/1.1 Acc = constant = interface 0 7f:ff:fa (01:00:5e:7f:ff:fa)		- 0

The screen/interface of the Wire shark is divided into five parts:

• First part contains a menu bar and the options displayed below it. This part is at the top of the window. File and the capture menus options are commonly used in Wire shark. The capture menu allows to start the capturing process. And the File menu is used to open and save a capture file.

- The second part is the packet listing window. It determines the packet flow or the captured packets in the traffic. It includes the packet number, time, source, destination, protocol, length, and info. We can sort the packet list by clicking on the column name.
- Next comes the packet header- detailed window. It contains detailed information about the components of the packets. The protocol info can also be expanded or minimized according to the information required.
- The bottom window called the packet contents window, which displays the content in ASCII and hexadecimal format.
- At last, is the filter field which is at the top of the display. The captured packets on the screen can be filtered based on any component according to your requirements. For example, if we want to see only the packets with the HTTP protocol, we can apply filters to that option. All the packets with HTTP as the protocol will only be displayed on the screen, shown below:



After connecting, you can watch the traffic below:

🖌 Canturing f	rom Ethernet				- n	×
File Edit V	liew Go Canture Ana	livze Statistics Telephony	Wireless Tools Heli			
			⊕ ⊖ ⊜ ₩	•		
		∽∽≚∙⊻⊒≡	444#			1
Apply a displ	ay filter <ctrl-></ctrl->				Expression	+
No. Tim	e Source	Destination	Protocol L	ength Info		_ ^
106 7.9	949564 192.168.1	9 20.189.74.1	L53 TCP	54 61759 → 443 [FIN, ACK] Seq=745 Ack=3945 Win=65024 Len=0		
107 8.0	077311 20.189.74	.153 192.168.1.9	Э ТСР	60 443 → 61759 [FIN, ACK] Seq=3945 ACk=746 Win=262144 Len=0		
108 8.0	0//509 192.168.1	9 20.189.74.1	153 TCP	54 61/59 + 443 [ACK] Seq=/46 Ack=3946 Win=65024 Len=0		
109 8	117412 34 230 26	9 104.85.64.8	37 TCP	54 61/56 + 443 [KST, ACK] Seq=//4 ACK=/069 Win=0 Len=0		
111 8	41/412 54.250.20	9 34 339 399	57 TCD	54 Apprilation Data		
112 9 0	903357 192.168.1	5 192 168 1 2	55 BROWSER	243 Hots Appound The DESKTOP-KCONTWO Workstation Server NT Workstation		
			biolisen	215 Hose Annoancement Bestron Records, NorReceipting Servery An NorReceipting		~
> Frame 1:	208 bytes on wire (1	664 bits), 208 bytes ca	ptured (1664 bits)	on interface 0		
> Ethernet	II, Src: Giga-Byt_63	:29:a3 (40:8d:5c:63:29:	a3), Dst: IPv6mcast	_0c (33:33:00:00:00:0c)		
> Internet	Protocol Version 6,	Src: fe80::71db:a5e9:6f	e7:85d, Dst: ff02::	c		
> User Data	agram Protocol, Src P	ort: 51190, Dst Port: 1	900			
> Simple Se	ervice Discovery Prot	ocol				
0000 33 33	00 00 00 0c 40 8d	5c 63 29 a3 86 dd 60 00	33····@· \c)···`			
0010 00 00	00 9a 11 01 fe 80	30 00 00 00 00 00 71 db	d			
0020 a5 e9	0 6T 67 08 50 TT 02 0	00 00 00 00 00 00 00 00 00 37 6c 00 9a 3f 5f 4d 3d		-		
0040 53 45	41 52 43 48 20 2a	20 48 54 54 50 2f 31 2e	SEARCH * HTTP/1			
0050 31 0d	0a 48 6f 73 74 3a	5b 46 46 30 32 3a 3a 43	1. Host: [FF02::0			
0060 5d 3a	31 39 30 30 0d 0a	53 54 3a 75 72 6e 3a 4d]:1900 ·· ST:urn:/	4		
0070 69 63	72 6f 73 6f 66 74	20 57 69 6e 64 6f 77 73	icrosoft Window	5		
0080 20 50	60 6f 60 20 50 72	50 55 20 52 55 73 5T 5C	Peer Na me Keso.	1		
0030 75 74	3a 49 50 56 36 3a	4c 69 6e 6b 4c 6f 63 61	V4:TPV6: LinkLock			
00b0 6c 0d	0a 4d 61 6e 3a 22	73 73 64 70 3a 64 69 73	l··Man:" ssdp:di	S S		
00c0 63 6f	76 65 72 22 0d 0a	4d 58 3a 33 0d 0a 0d 0a	cover" · · MX:3 · · ·			
🔘 🗹 Ethe	rnet: <live capture="" in="" progress<="" th=""><th>\$></th><th></th><th>Packets: 112 · Displayed: 112 (100.0%)</th><th>Profile: [</th><th>efault</th></live>	\$>		Packets: 112 · Displayed: 112 (100.0%)	Profile: [efault
• 0	Type here to search	9	H: 🧲 📜	۵ 🖈 🕺 🚺 🚺 💁 🚺	■ 口 句 00 10:49 AM 9/16/2019	2

Basic concepts of the Network Traffic

IP Addresses: It was designed for the devices to communicate with each other on a local network or over the Internet. It is used for host or network interface identification. It provides the location of the host and capacity of establishing the path to the host in that network. Internet Protocol is the set of predefined rules or terms under which the communication should be conducted. The types of IP addresses are IPv4 and IPv6.

- IPv4 is a 32-bit address in which each group represents 8 bits ranging from 0 to 255.
- IPv6 is a 128-bit address.

I 🖉 💿 📘 🚠	🗙 😂 🍳 👄 🔿 警	ા 💇 🖃 🖻 લાલ			
p.analysis.flags					Exp
Time	Source	Destination	Protocol	Length Info	
29 3.334936 46 13 579271	192.168.1.9	148.251.77.80	TCP	54 [TCP ACKed unseen segment] 61131 → 80 [ACK] Seq=1 Ack=2 Win=255 Len=0 60 [TCP Dup ACK 28#1] 80 → 61131 [ACK] Seq=1 Ack=1 Win=257 Len=0	
47 13.579381	192.168.1.9	148.251.77.80	TCP	54 [TCP Dup ACK 29#1] [TCP ACKed unseen segment] 61131 → 80 [ACK] Seq=1 Ack=2 Win=255 Len=0	
98 23.818241	192.168.1.9 148 251 77 80	148.251.77.80	тср	54 [TCP Dup ACK 29#2] [TCP ACKed unseen segment] 61131 → 80 [ACK] Seq=1 Ack=2 Win=255 Len=0 60 [TCP Dup ACK 28#3] 80 → 61131 [ACK] Seq=1 Ack=1 Win=257 Len=0	
135 34.061643	192.168.1.9	148.251.77.80	TCP	54 [TCP Dup ACK 29#3] [TCP ACKed unseen segment] 61131 → 80 [ACK] Seq=1 Ack=2 Win=255 Len=0	
ame 29: 54 byte hernet II, Src:	s on wire (432 bits), HewlettP_bd:3d:1d (1	54 bytes captured (4 8:60:24:bd:3d:1d), D	432 bits) on st: D-LinkIn	interface 0 db:f7:67 (74:da:da:db:f7:67)	
ternet Protocol ansmission Cont	Version 4, Src: 192. rol Protocol, Src Por	168.1.9, Dst: 148.25 t: 61131, Dst Port: 6	1.77.80 80, Seq: 1,	Ack: 2, Len: 0	
74 da da dh €	7 67 18 60 24 bd 3d	10 08 00 45 00 +		F.	
00 28 1f 6b 40	0 00 80 06 37 68 c0	a8 01 09 94 fb ·(·k	k@ 7h	<u>.</u>	
4d 50 ee cb 00	05090e6 44 e1 bc 3 ee	f4 88 51 50 10 MP	···P·· D····Q	P.	
00 11 00 01 00					
				Fig (5)	
				Fig (5)	
hernet				Fig (5)	_
hernet Edit View Go	Capture Analyze Stat	istics Telephony Wirel	ess Tools ⊢	Fig (5)	_
hernet Edit View Go II. Ø. ♥ ↓ ■ ■	Capture Analyze Stat	istics Telephony Wirel	ess Tools ⊦ ⊇, @, Ⅲ	Fig (5)	
hernet Edit View Go II ₫ Q III III IIIIIIIIIIIIIIIIIIIIIIII	Capture Analyze Stat	istics Telephony Wirel	ess Tools H Q Q III Protocol	Fig (5)	- -
hernet Edit View Go II 🖉 😨 🛄 📅 Time 22 1.458399	Capture Analyze Stat	istics Telephony Wirel	ess Tools H Q Q III Protocol UDP	Fig (5) Help Length Info 60 443 → 49927 Len=16	- - -
hernet Edit View Go I C P of dns or iano) Time 22 1.458399 23 1.468751	Capture Analyze Stat Source 216.58.200.174 192.166.1.9	istics Telephony Wirel Destination 192.168.1.9 216.58.200.174	ess Tools H Q Q III Protocol UDP UDP	Fig (5) Help Length Info 60 443 + 49927 + Len=16 70 49927 + 443 Len=28	- - - -
hernet Edit View Go (pp or dhs or icmp) Tme 22 1.458399 23 1.460751 25 2.159211	Capture Analyze Stat Source 216.58.200.174 192.168.1.25	istics Telephony Wirel	ess Tools F Q Q II Protocol UDP UDP SSDP	Fig (5) Help Length Info 68 443 + 49927 Len=16 70 49927 + 443 Len=28 216 M-5EARCH * HTTP/1.1	
hernet Edit View Go por drs or icmp) Time 22 1.458399 23 1.460751 25 2.15021 26 2.845392	Capture Analyze Stat Source 216.55.200.174 192.168.1.25 192.168.1.17	istics Telephony Wirel ■	ess Tools F Protocol UpP UDP SSDP SSDP	Fig (5) Help Length Info 60 443 + 49927 Len=16 70 49927 + 443 Len=28 216 M-5EARCH * HTTP/1.1 211 H-SEARCH * HTTP/1.1	-
hernet Edit View Go prordnsortom) Time 22 1.458399 23 1.468751 25 2.158211 25 2.158211 25 2.158212 26 2.845312 26 2.845312 26 2.845312 27 3.126627	Capture Analyze Stat Source 216.58.200.174 192.168.1.9 192.168.1.17 192.168.1.17 192.168.1.17	istics Telephony Wirel Destnation 192.168.1.9 216.58.200.174 239.255.255.250 239.255.255.250 239.255.255.255 239.255.255 239.255.255.255 239.255.255.255 239.255.	ess Tools H Q Q III Protocol UDP UDP SSDP SSDP SSDP SSDP SSDP	Fig (5)	- -
hernet Edit View Go por drs or icmp) Tme 22 1.458399 23 1.460751 25 2.15021 25 2.15021 26 2.845392 27 3.126627 28 3.334879 28 3.334879	Capture Analyze Stat	istics Telephony Wirel	ess Tools H Q Q III Protocol UDP UDP SSDP SSDP SSDP SSDP TCP	Fig (5) Help Length Info 68 443 + 49927 Len=16 70 49927 + 443 Len=28 216 M-5EARCH * HTTP/1.1 211 M-5EARCH * HTTP/1.1 215 M-5EARCH * HTTP/1.1 215 M-5EARCH * HTTP/1.1 216 88 - 61131 [ACK] Seq=1 Ack=1 Min=257 Len=0 29 400 Help Minor Control 400 Minor Seq (4 ack) Minor Seq (4 ack)	=
hernet Edit View Go ↓ 2 (1997) Time 22 1.458399 23 1.460751 25 2.196211 25 2.196211 25 2.196211 26 2.845392 27 3.126627 28 3.334679 29 3.334095 29 3.334095	Capture Analyze Stat Source 216.58.200.174 192.168.1.25 192.168.1.17 192.168.1.18 193.168.1.17 193.168.1.18 193.168.1.18 193.168.1.18 193.168.1.18 193.168.1.18 193.168.1.17 193.168.1.1	istics Telephony Wirel	ess Tools P Protocol UDP UDP SSDP SSDP SSDP SSDP	Fig (5) Length Info 60 443 + 49927 Len=16 70 49927 + 443 Len=28 216 M-SEARCH * HTTP/1.1 215 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 218 M-SEARCH * HTTP/1.1 218 M-SEARCH * HTTP/1.1 218 M-SEARCH * HTTP/1.1 219 M-SEARCH * HTTP/1.1 219 M-SEARCH * HTTP/1.1 219 M-SEARCH * HTTP/1.1 210	-
hernet Edit View Go por dhus or icmp) Tme 22 1.458399 23 1.466751 25 2.158211 26 2.845392 27 3.126627 28 3.334879 29 3.334879 29 3.334879 29 3.348795	Capture Analyze Stat Source 216.5.8.200.174 192.168.1.25 192.168.1.17 192.168.1.17 192.168.1.17 192.168.1.17 192.168.1.19 192.188.1.19 192.188.1.19 192.188.1.19 192.188.1.19 192.188.19	istics Telephony Wirel	ess Tools H Q Q II Protocol UDP SSDP SSDP SSDP TCP TCP (432 bits) o	Fig (5) Help Length Info 60 443 + 49927 Len-16 70 49927 + 443 Len-28 216 M-SEARCH * HTTP/1.1 211 M-SEARCH * HTTP/1.1 215 M-SEARCH * HTTP/1.1 60 80 + 61131 [ACK] Seq=1 Ack=1 Win=257 Len=0 54 [TPA Ackded unsense regenet] 61131 + 80 [ACK] Seq=1 Ack=2 Win=255 Len=0 TH M SEARCH * HTTP/1.1 60 No + 61131 [ACK] Seq=1 Ack=1 Win=257 Len=0 54 [TPA Ackded unsense regenet] 61131 + 80 [ACK] Seq=1 Ack=2 Win=255 Len=0 TH M SEARCH * HTTP/1.1	- - -
hernet Edit View Go por drs or icmp) Time 23 1.460751 25 2.1502 27 3.126627 28 3.334679 29 3.34679 29 3.34679 20 3.34679	Capture Analyze Stat Source 216.58.200.174 192.168.1.9 192.168.1.17 192.168.1.17 192.168.1.17 192.168.1.17 192.168.1.25 192.168.1.55	istics Telephony Wirel	ess Tools H Protocol UDP SSDP SSDP TCP TCP COD COD COD COD COD COD COD COD COD COD	Fig (5) leep Length Info 60 443 + 49927 Len-16 70 49927 + 443 Len-28 216 M-SEARCH * MTTP/1.1 211 M-SEARCH * MTTP/1.1 213 M-SEARCH * MTTP/1.1 215 M-SEARCH * MTTP/1.1 216 M-SEARCH * MTTP/1.1 217 M-SEARCH * MTTP/1.1 218 M-SEARCH * MTTP/1.1 219 M-SEARCH * MTTP/1.1 219 M-SEARCH * MTTP/1.1 219 M-SEARCH * MTTP/1.1 210 M-SEARCH * MTTP/1.1 210 M-SEARCH * MTTP/1.1 210 M-SEARCH * MTTP/1.1 211 M-SEARCH * MTTP/1.1 213 M-SEARCH * MTTP/1.1 214 M-SEARCH * MTTP/1.1 215 M-SEARCH * MTTP/1.1 215 M-SEARCH * MTTP/1.1 216 M-SEARCH * MTTP/1.1 217 M-SEARCH * MTTP/1.1 218 M-SEARCH * MTTP/1.1 219 M-SEARCH * MTTP/1.1 210 M-SEARCH * MTTP/1.1 210 M-SEARCH * MTTP/1.1 210 M-SEARCH * MTTP/1.1 211 M-SEARCH * MTTP/1.1 211 M-SEARCH * MTTP/1.1 212 M-SEARCH * MTTP/1.1 213 M-SEARCH * MTTP/1.1 213 M-SEARCH * MTTP/1.1 214 M-SEARCH * MTTP/1.1 215 M-SEARCH * MTTP/1.1 216 M-SEARCH * MTTP/1.1 217 M-SEARCH * MTTP/1.1 218 M-SEARCH * MTTP/1.1 219 M-SEARCH * MTTP/1.1 219 M-SEARCH * MTTP/1.1 219 M-SEARCH * MTTP/1.1 210 M-SEARCH * MTTP/1.	- X - * E
hernet Edit View Go prodisor cimp) Time 22 1:458399 23 1:466751 25 2:158211 25 2:158211 25 2:45332 27 3:126627 28 3:334679 29 3:334697 28 3:334679 29 3:334697 29 3:334697 29 3:334697 29 3:334697 29 3:334697 29 3:334697 29 3:334697 20 3:344677 20 3:34477 20 3:34577 20 3:34577 20 3:34577 20 3:345777 20 3:34577777777777777777777777777777777777	Capture Analyze Stat Source 216.58.200.174 192.168.1.9 192.168.1.7 192.168.1.17 192.168.1.7 193.17 193	istics Telephony Wirel Destruction 192,168,1,9 216,58,200,174 239,255,255,258 239,255,255,259 192,166,1,9 146,19,9 192,168,1,9 193,168,168,168,168,168,168,168,168,168,168	ess Tools H Q Q III Protocol UOP UOP SSDP SSDP SSDP SSDP SSDP SSDP SSDP SS	Fig (5) Length Info 60 443 + 49927 Len=16 70 49927 + 443 Len=28 216 M-SEARCH * HTTP/1.1 211 M-SEARCH * HTTP/1.1 215 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 218 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 218 M-SEARCH * HTTP/1.1 218 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 218 M-SEARCH * HTTP/1.1 218 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 218 M-SEARCH * HTTP/1.1 218 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 218 M-SEARCH * HTTP/1.1 218 M-SEARCH * HTTP/1.1 218 M-SEARCH * HTTP/1.1 219 M-SEARCH * HTTP/1.1 219 M-SEARCH * HTTP/1.1 210 M-SEARCH * HTTP/1.1 210 M-SEARCH * HTTP/1.1 210 M-SEARCH * HTTP/1.1 210	
hernet Edit View Go rpor das or icmp) Time 22 1.458399 23 1.460751 25 2.15021 26 2.845392 27 3.126627 28 3.34879 20 3.34779 20 3.34879 20 3.348797 20 3.348797 20	Capture Analyze Stat Source 216,58,200,174 192,168,1.9 192,168,1.25 192,168,1.17 193,168,1.17 192,168,1.17 193,105,1.17 193,105,1.17 193,105,1.17 194,105,1.17 194,105,1.17 194,105,1.17 194,105,1.17 194,105,1.17 194,1.15 19	istics Telephony Wirel	ess Tools H Q Q III Protocol UDP SSDP SSDP SSDP (432 bits) o Stits) o Stits) o Stits) o Stits) o Stits) o	Fig (5) Help Length Info 60 443 + 49927 Len-16 70 49927 + 443 Len-28 216 M-5EARCH + HTP/1.1 216 M-5EARCH + HTP/1.1 215 M-5EARCH + HTP/1.1 215 M-5EARCH + HTP/1.1 215 M-5EARCH + HTP/1.1 216 M-5EARCH + HTP/1.1 216 M-5EARCH + HTP/1.1 216 M-5EARCH + HTP/1.1 217 M-5EARCH + HTP/1.1 218 M-5EARCH + HTP/1.1 218 M-5EARCH + HTP/1.1 218 M-5EARCH + HTP/1.1 219 M-5EARCH + HTP/1.1 210 M-5EARCH + HTP/1.1 210 M-5EARCH + HTP/1.1 210 M-5EARCH + HTP/1.1 210 M-5EARCH + HTP/1.1 211 M-5EARCH + HTP/1.1 211 M-5EARCH + HTP/1.1 212 M-5EARCH + HTP/1.1 213 M-5EARCH + HTP/1.1 214 M-5EARCH + HTP/1.1 214 M-5EARCH + HTP/1.1 215 M-5EARCH + HTP/1.1 216 M-5EARCH + HTP/1.1 217 M-5EARCH + HTP/1.1 218	-
thermet Edit View Go rep or dris or icmo) Time 22 1.458399 23 1.460751 25 2.158211 26 2.845392 27 3.126627 28 3.334679 29 3.334996 29 3.334996 29 3.334996 29 3.334996 29 3.334996 29 3.334996 20 3.334976 20 3.334996 20 3.334976 20 3.34476 20 3	Capture Analyze Stat Surce 216.58.200.174 192.168.1.9 192.168.1.7 193.168.1.7 193.17 193.168.1.7 194.17 195.168.1.7 195.168.	istics Telephony Wirel	ess Tools F Protocol UDP SSDP SSDP TCP TCP Caller (432 bits) o Dst: D-LinkI 1-77.80 80, Seq: 1,	Fig (5) Help Length Info 60 443 + 49927 Len=16 70 49927 + 443 Len=28 216 M-SEARCH * HTTP/1.1 215 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 218 M-SEARCH * HTTP/1.1 218 M-SEARCH * HTTP/1.1 219 M-SEARCH * HTTP/1.1 219 M-SEARCH * HTTP/1.1 219 M-SEARCH * HTTP/1.1 210 M-SEARCH * HTTP/1.	-
thernet Edit View Go Tome 22 1.458399 23 1.466751 25 2.150211 26 2.845392 27 3.1266751 26 2.845392 27 3.1266751 28 3.34879 29 3.3426915 29 3.342915 29 3.342915 29 3.342915 29 3.342915 20 3.345915 20	Capture Analyze Stat Source 216.58.200.174 192.168.1.9 192.168.1.7 192.168.1.7 192.168.1.17 192.168.1.17 192.168.1.17 192.168.1.17 192.168.1.17 192.168.1.57 192.168.1.7 192.17 192	istics Telephony Wirel Destheaton 192,168,1.9 216,58,200,174 239,255,255,259 129,2168,1.9 129,2168,1.9 129,255,255,259 129,2168,1.9 128,227,280 128,224,124,234,21 168,1.9, Dst: 148,22 rt: 61131, Dst Port:	ess Tools H Q Q II Protocol UDP UDP SSDP SSDP SSDP SSDP TCP (432 bits) o Dst: D-Linkt 1.77.80 80, Seq: 1,	Fig (5) Hep Length Info 60 443 + 49927 Len-16 70 49927 + 443 Len-28 216 M-SEARCH * HTTP/1.1 211 M-SEARCH * HTTP/1.1 215 M-SEARCH * HTTP/1.1 215 M-SEARCH * HTTP/1.1 60 80 + 61131 [ACK] Seq=1 Ack=1 Win=257 Len=0 54 [TOP Added unsense regenet] 61131 + 80 [ACK] Seq=1 Ack=2 Win=255 Len=0 TAL SEARCH * HTTP/1.1 60 80 + 61131 [ACK] Seq=1 Ack=1 Win=257 Len=0 TAL SEARCH * HTTP/1.1 60 80 + 61131 [ACK] Seq=1 Ack=2 Win=255 Len=0 TAL SEARCH * HTTP/1.1 60 80 + 61131 [ACK] Seq=1 Ack=2 Win=255 Len=0 TAL SEARCH * HTTP/1.1 60 80 + 61131 [ACK] Seq=1 Ack=2 Win=255 Len=0 TAL SEARCH * HTTP/1.1 60 80 + 61131 [ACK] Seq=1 Ack=2 Win=255 Len=0 TAL SEARCH * HTTP/1.1 60 80 + 61131 [ACK] Seq=1 Ack=2 Win=255 Len=0 TAL SEARCH * HTTP/1.1 60 80 + 61131 [ACK] Seq=1 Ack=2 Win=255 Len=0 TAL SEARCH * HTTP/1.1 60 80 + 61131 [ACK] Seq=1 Ack=1 Win=257 Len=0 60 Ack: 2, Len: 0	
thernet Edit View Go in 20 20 10 10 10 10 10 10 10 10 10 10 10 10 10	Capture Analyze Stat Source 216.58.200.174 192.168.1.9 192.168.1.17 192.168.1.17 192.168.1.17 192.168.1.17 192.168.1.25	istics Telephony Wirel	ess Tools H Protocol UDP SSDP SSDP SSDP TCP TCP TCP TCP TCP TCP TCP TCP TCP TC	Fig (5) Help Length Info 60 443 + 49927 Len=16 70 49927 + 443 Len=28 216 M-5EARCH * HTTP/1.1 215 M-5EARCH * HTTP/1.1 215 M-5EARCH * HTTP/1.1 60 80 + 61131 [ACK] Seq=1 Ack=1 Win=257 Len=0 54 [TCP Added unseen segment] 61131 + 80 [ACK] Seq=1 Ack=2 Win=255 Len=0 54 [TCP Added unseen segment] 61131 + 80 [ACK] Seq=1 Ack=2 Win=255 Len=0 54 [TCP Added unseen segment] 61131 + 80 [ACK] Seq=1 Ack=2 Win=255 Len=0 54 [TCP Added unseen segment] 61131 + 80 [ACK] Seq=1 Ack=2 Win=255 Len=0 54 [TCP Added unseen segment] 61131 + 80 [ACK] Seq=1 Ack=2 Win=255 Len=0 54 [TCP Added unseen segment] 61131 + 80 [ACK] Seq=1 Ack=2 Win=255 Len=0	-
thermet Edit View Go produs or icmo) Time 22 1.458399 23 1.460751 25 2.150211 25 2.150211 25 2.35322 27 3.126627 28 3.33467 28 3.34679 29 3.34096 29 3.34096 29 3.34096 29 3.34096 20 3	Capture Analyze Stat Source 216.58.200.174 192.168.1.9 192.168.1.7 192.168.1.	istics Telephony Wirel Destination 192.168.1.9 216.58.200.174 239.255.255.250 239.255.255.250 239.255.255.250 192.168.1.9 148.0251.77.80 249.454.541.9 148.60:241:bd:341.0), Cl 186.1.9 Dst: 148.22 rt: 61131, Dst Port:	ess Tools I- Protocol UDP UDP SSDP SSDP SSDP TCP (432 bits) o Dst: D-Linkt 177.88 80, Seq: 1,	Fig (5) Help Length Info 00 443 + 49927 Len=16 70 49927 + 443 Len=28 216 M-SEARCH * HTTP/L1 211 M-SEARCH * HTTP/L1 215	
thernet Edit View Go produs or icmp) Time 22 1.458399 23 1.460751 25 2.15921 26 2.843392 27 3.126627 28 3.334879 29 5.45936 29 5.45936 20 5.845392 20 5.845492 20	Capture Analyze Stat No. 2 (10, 10, 10, 10, 10, 10, 10, 10, 10, 10,	istics Telephony Wirel	ess Tools H Q Q III Protocol UDP SSDP SSDP SSDP SSDP SSDP CP III Protocol UDP SSDP	Fig (5)	
thernet Edit View Go rep or dris or icmo) Time 22 1.458399 23 1.466751 25 2.15921 26 2.845392 27 3.126627 28 3.334679 29 3.34679 29 3.34679 20 3.34799 20 3.34799 20 3.34799 20 3.34799 20 3.34799 20 3.34799 20 3.3479	Capture Analyze Stat Source Source 216.55.200.174 192.168.1.25 192.168.1.17 193.168.1.17 193.17 193.17 193.17 193.17 193.17 193.1	istics Telephony Wirel	ess Tools - Protocol UDP SSDP TCP TCP FCP FCP FCP FCP FCP FCP FCP F	Fig (5)	_ •
hernet Edit View Go Time 22 1.458399 23 1.466751 25 2.158211 26 2.845392 27 3.1266751 26 2.845392 27 3.1266751 26 2.845392 27 3.1266751 28 3.334679 28 3.334679 28 3.334679 28 3.334679 28 3.334679 28 3.34679 28 3.44679 28 3.4467928 3.44679 28 3.44679 28 3.4467928 3.4467928 3.4467928 3.44679 28	Capture Analyze Stat Source 216.58.200.174 192.166.1.9 192.166.1.7 192.166.1.7 192.166.1.7 192.166.1.7 192.166.1.7 192.166.1.7 192.165.1.7 192.105.1.7 192.105.1.7 192.105.1.7 192.105.1.7 192.105.1.7 192.105.1.7 192.105.1.7 192.105.1.7 192.105.1.7 192.105.1.7 192.105.1.7 192.1.7 1	iddics Telephony Wirel	ess Tools - 	Fig (5) tep tergth Info 60 443 + 49927 Len=16 70 49927 + 443 Len=28 216 M-SEARCH * HTTP/1.1 211 M-SEARCH * HTTP/1.1 215 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 216 M-SEARCH * HTTP/1.1 217 M-SEARCH * HTTP/1.1 218 M-SEARCH * HTTP/1.1 218 M-SEARCH * HTTP/1.1 219 M-SEARCH * HTTP/1.1 210 M-SEARCH * HTTP/1.1 210 M-SEARCH * HTTP/1.1 210 M-SEARCH * HTTP/1.1 210 M-SEARCH * HTTP/1.1 211 M-SEARCH * HTTP/1.1	
hernet Edit View Go (me 22 1.458399 23 1.460751 25 2.15627 27 3.126627 28 3.334879 29 3.34697 29 3.3497 29 3.3497 20 3.3477 20 3.3497 20	Capture Analyze Stat Source 216.55.200.174 192.168.1.9 192.168.1.15 192.168.1.17 192.168.1.25 192.17 192.168.1.25 192.17 192.168.1.25 192.168.1.	istics Telephony Wirel	ess Tools H Q Q III Protocol UDP UDP SSDP SSDP SSDP SSDP SSDP SSDP SSDP SSDP SSDP SSDP (432 bits) o SSC: D-Link 80, Seq: 1, 	Fig (5)	

Fig (6)

Edit View Go	Capture Analyze Statis	stics Telephony Wireless	s Tools Help
= 🔬 💿 🔚 🛅	X © 9 ⇔ ⇒ ≅	🗿 🕭 🚍 📃 Q, Q, (Q. II
p.port == 80 udp.port	t == 80		Expression.
Time	Source	Destination	Protocol Length Info
21 20.353464	23.76.156.49	23.76.156.49	ICP 06 80 → 01/89 [SYR, ALK] Seq=0 ACK=1 W1n=29200 Len=0 MSS=1460 SALK_PERM=1 WS=128 TCP 54 61789 → 80 [ACK] Seq=1 ACK=1 W1n=6538 Len=0
23 20.354107	192.168.1.9	23.76.156.49	HTTP 136 GET /ncc.txt HTTP/1.1
24 20.362389	23.76.156.49	192.168.1.9	TCD 60.00 \ 61700 [ArV] Soc-1 Ack=83 Win=29312 Len=0
25 20.363300	23.76.156.49	192.168.1.9	Mark/Unmark Packet Ctri+M tml)
20 20.303030	23.76.156.49	25.70.150.49	Ignore/Unignore Packet Ctrl+D H=05 Ack=122 win=05306 Len=0
38 39 371663	100 100 1 0	22 76 156 40	Set/Unset Time Reference Ctrl+T
rame 24: 60 bytes	on wire (480 bits),	60 bytes captured (48	8 Time Shift Ctrl+Shift+T
thernet II, Src: I	D-LinkIn_db:†7:67 (7	4:da:da:db:f7:67), Dst	t Packet Comment Ctrl+Alt+C
ransmission Contro	ol Protocol. Src Por	t: 80. Dst Port: 61789	o 9 Edit Resolved Name
			Apply as Filter
			Prepare a Filter
			Conversation Filter
18 60 24 bd 3d	1d 74 da da db f7 6	67 08 00 45 00 ·`\$·=	Colorize Conversation
00 28 51 02 40	00 3c 06 78 9f 17	4c 9c 31 c0 a8 ·(Q·@	9 SCTP +
01 09 00 50 f1	5d 9c 22 0d 32 5a 0	0f f1 f2 50 10 ···P	Follow TCP Stream Ctrl+Alt+Shift+T
. 30 E3 52 DC 00	00 00 00 01 10 80 I		UDP Stream Ctrl+Alt+Shift+U
			Copy TLS Stream Ctrl+Alt+Shift+S
			Protocol Preferences + HTTP Stream Ctrl+Δlt+Shift+H
			Decode As
			Show Packet in New Window
Ethernet Edit View Go	Capture Analyze Stat	tistics Telephony Wirele	ess Tools Help
Ethernet Edit View Go	Capture Analyze Stat	tistics Telephony Wirele:	ess Tools Help 2. Q. III
Ethernet Edit View Go 	Capture Analyze Stat	tistics Telephony Wireles	ess Tools Help
Ethernet Edit View Go cp.flags.syn=1 Time 268 81.417971	Capture Analyze Stat	tistics Telephony Wireles	ess Tools Help کو س اللہ Protocol Length Info TCP 66 7650 + 62553 [SYN, ACK] Seq=0 Ack=1 Min=65535 Len=0 MSS=1460 MS=256 SACK PERM=1
Ethernet Edit View Go Edit View Go cp.flags.syn==1 Time 268 81.417971 408 121.442966	Capture Analyze Stat	tistics Telephony Wirele Telephony Wirele Telephony Q Q Destination 192.168.1.9 192.168.1.5	ess Tools Help Q Q II Protocol Length Info TCP 66 7580 + 62553 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSs=1460 WS=256 SACK_PERM=1 TCP 66 62554 + 7680 [SYN] Seq=0 Win=64240 Len=0 MSs=1460 WS=256 SACK_PERM=1
Ethernet Edit View Go C C C C C C C C C C C C C C C C C C C	Capture Analyze Stat Capture Analyze Stat Source 192.168.1.5 192.168.1.5	tistics Telephony Wirele Telephony Wirele Destination 192.168.1.9 192.168.1.9	ess Tools Help Q Q II Protocol Length Info TCP 667 7680 + 62553 [SYN, ACK] Seq=0 Ack=1 Min=65535 Len=0 MSS=1460 MS=256 SACK_PERM=1 TCP 667 7680 + 62554 + 7680 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 MS=256 SACK_PERM=1 TCP 667 7680 + 62554 [SYN, ACK] Seq=0 Ack=1 Min=65535 Len=0 MSS=1460 MS=256 SACK_PERM=1 TCP 667 7680 + 62554 [SYN, ACK] Seq=0 Ack=1 Min=65535 Len=0 MSS=1460 MS=256 SACK_PERM=1
Ethernet Edit View Go Complete phlogs.syn=1 Time 268 81.417971 408 121.444157 536 161.458617	Capture Analyze Stat	tistics Telephony Wireles	ess Tools Help R Q II Protocol Length Info TCP 66 7680 + 62553 [SYN, ACK] Seq=0 Ack=1 Min=65535 Len=0 MSS=1460 MS=256 SACK PERM=1 TCP 66 62554 + 7680 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 MS=256 SACK PERM=1 TCP 66 62555 + 7680 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 MS=256 SACK PERM=1 TCP 66 62555 + 7680 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 MS=256 SACK PERM=1 TCP 66 62555 + 7680 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 MS=256 SACK PERM=1
Ethernet Edit View Go Image: Sym = 1 Image: Sym = 1 Time Image: Sym = 1 268 81.417971 408 121.44296 409 121.444157 536 161.4536517 537 161.4539554	Capture Analyze Stat	tistics Telephony Wirele Destination 192.168.1.9 192.1	ess Tools Help Protocol Length Info TCP 66 7680 + 62553 [SVN, ACK] Seq=0 Ack=1 Min=65535 Len=0 MSS=1460 MS=256 SACK_PERM=1 TCP 70 66 7680 + 62554 [SVN] Seq=0 Ack=1 Min=65535 Len=0 MSS=1460 MS=256 SACK_PERM=1 70 66 7680 + 62554 [SVN, ACK] Seq=0 Ack=1 Min=65535 Len=0 MSS=1460 MS=256 SACK_PERM=1 70 66 7680 + 62555 [SVN, ACK] Seq=0 Ack=1 Min=65535 Len=0 MSS=1460 MS=256 SACK_PERM=1 70 66 7680 + 62555 [SVN, ACK] Seq=0 Ack=1 Min=64240 Hen=0 MSS=1460 HS=256 SACK_PERM=1 70 66 7680 + 62555 [SVN, ACK] Seq=0 Ack=1 Min=64240 Hs=256 SACK_PERM=1 70 66 7680 + 62555 [SVN, ACK] Seq=0 Ack=1 Min=64240 Hs=256 SACK_PERM=1 70 66 7680 + 62555 [SVN, ACK] Seq=0 Ack=1 Min=64240 Hs=256 SACK_PERM=1 70 66 7680 + 62555 [SVN, ACK] Seq=0 Ack=1 Min=64240 Hs=256 SACK_PERM=1 70 86 7880 + 82555 [SVN, ACK] Seq=0 Ack=1 Min=64240 Hs=256 SACK_PERM=1 70 86 7880 + 82555 [SVN, ACK] Seq=0 Ack=1 Min=64240 Hs=256 SACK_PERM=1 70 86 7880 + 82555 [SVN, ACK] Seq=0 Ack=1 Min=64240 Hs=256 SACK_PERM=1 70 86 7880 + 82555 [SVN, ACK] Seq=0 Ack=1 Min=64240 Hs=256 SACK_PERM=1 70 86 7880 + 82555 [SVN, ACK] Seq=0 Ack=1 Min=64240 Hs=256 SACK_PERM=1 70 86 7880 + 82555 [SVN, ACK] Seq=0 Ack=1 Min=64240 Hs=256 SACK_PERM=1 70 86 7880 + 82555 [SVN, ACK] Seq=0 Ack=1 Min=64240 Hs=256 SACK_PERM=1 70 86 7880 + 82555 [SVN, ACK] Seq=0 Ack=1 Min=64255 Hs=255 SACK_PERM=1 70 86 7880 + 82555 [SVN, ACK] Seq=0 Ack=1 Min=64255 Hs=255 SACK_PERM=1 70 86 7880 + 82555 [SVN, ACK] Seq=0 Ack=1 Min=64255 Hs=2555 Hs=255 SACK_PERM=1 70 86 7880 + 82555 [SVN, ACK] Seq=0 Min=6420 Hs=2555 Hs=255 SACK_PERM=1 70 86 7880 + 82555 [SVN, ACK] Seq=0 Min=6420 Hs=2555 Hs=25555 Hs=25555 Hs=2555 Hs=2555 Hs=25555 Hs=25555 Hs=25555 Hs=2555
Time Time 268 81.41.7971 408 121.444157 336 14.458617 536 161.458617 536 161.458617 537 161.458617 538 188.302184	Capture Analyze Stat Source 192,168,1.5 192,168,1.5 192,168,1.5 192,168,1.5 192,168,1.5 192,168,1.5 192,168,1.9 193,200,29,129 193,200,200,200,200,200,200,200,200,200,20	tistics Telephony Wireles Total Content of the second sec	ess Tools Help Protocol Length Info Protocol Length Info TCP 66 7680 + 62553 [SYN, ACK] Seq=0 Ack+1 Win+65535 Len+0 MSS-1460 WS+256 SACK PERM+1 TCP 66 7680 + 62554 + 7680 [SYN] Seq=0 Ack+1 Win+65353 Len+0 MSS-1460 WS+256 SACK PERM+1 TCP 66 7680 + 62554 [SYN] Seq=0 Ack+1 Win+65353 Len+0 MSS-1460 WS+256 SACK PERM+1 TCP 66 7680 + 62555 [SYN, ACK] Seq=0 Ack+1 Win+65353 Len+0 MSS-1460 WS+256 SACK PERM+1 TCP 66 7680 + 62555 [SYN, ACK] Seq=0 Ack+1 Win+65353 Len+0 MSS-1460 WS+256 SACK PERM+1 TCP 66 7680 + 62555 [SYN], ACK] Seq=0 Ack+1 Win+65353 Len+0 MSS-1460 WS+256 SACK PERM+1 TCP 66 62555 + 7680 [SYN] Seq=0 Win+64240 Len+0 MSS-1460 WS+256 SACK PERM+1 TCP 66 62555 (SYN, ACK] Seq=0 Ack+1 Win+2540 MS+256 SACK PERM+1 TCP 66 7680 + 62555 [SYN], ACK] Seq=0 Win+64240 Len+0 MSS-1460 WS+256 SACK PERM+1 TCP 66 7680 + 62555 [SYN], ACK] Seq=0 Win+04240 Len+0 MSS-1460 WS+256 SACK PERM+1 TCP 66 7680 + 62555 [SYN], ACK] Seq=0 Win+04240 Len+0 MSS-1460 WS+256 SACK PERM+1 TCP 66 7680 + 62555 [SYN], ACK] Seq=0 Win+04240 Len+0 MSS-1460 WS+256 SACK PERM+1 TCP 66 7680 + 62555 [SYN], ACK] Seq=0 Win+04240 Len+0 MSS-1460 WS+256 SACK PERM+1 TCP 66 7680 + 62555 [SYN], ACK] Seq=0 Win+04240 Len+0 MSS-1460 WS+256 SACK PERM+1 TCP 66 7680 + 62555 [SYN], ACK] Seq=0 Win+04240 Len+0 MSS-1460 WS+256 SACK PERM+1 TCP 66 7680 + 62555 [SYN], ACK] Seq=0 Win+04240 Len+0 MSS-1460 WS+256 SACK PERM+1 TCP 66 7680 + 62555 [SYN], ACK] Seq=0 Win+04240 Len+0 MSS-1460 WS+256 SACK PERM+1 TCP 66 7680 + 62555 [SYN], ACK] Seq=0 ACK+1 Win+05531 Len+0 MS-1460 WS+256 SACK PERM+1 TCP 67 7680 + 62556 [SYN], ACK] Seq=0 ACK+1 Win+05531 Len+0 MS-1460 WS+256 SACK PERM+1 TCP 67 7680 + 62556 [SYN] Seq=0 ACK+1 Win+05531 MIN+05531 MIN+05531 TCP 76 7680 + 62556 [SYN] Seq=0 Win+0 MIN+054240 Len+0 MS-1460 WS+256 SACK PERM+1 TCP 76 7680 + 62556 [SYN] Seq=0 Win+0 MIN+054240 Len+0 MS-1460 WS+256 MIN+0 MIN+0548
thernet Edit View Go thermet dit View Go thermet thermet thermet thermet thermet thermet thermet ther	Capture Analyze Stat	tistics Telephony Wireles To a a a a a a a a a a a a a a a a a a a	ess Tools Help R Q II Protocol Length Info TCP 66 7680 + 62553 [SVN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 MS=256 SACK_PERM=1 TCP 70 F0 66 62555 + 7680 [SVN] Seq=0 Win=64240 Len=0 MSS=1460 MS=256 SACK_PERM=1 70 F0 66 62555 + 7680 [SVN] Seq=0 Win=64240 Len=0 MSS=1460 MS=256 SACK_PERM=1 70 F0 66 62555 + 7680 [SVN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 70 F0 66 62555 + 80 [SVN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 70 F0 66 62555 + 80 [SVN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 70 F0 66 62555 = 80 [SVN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 70 F0 66 62555 [SVN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 70 F0 66 62556 [SVN] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128 SSR bits/ on interface 0
thernet Edit View Go	Capture Analyze Stat	tistics Telephony Wirele To a a a a a a a a a a a a a a a a a a a	ess Tools Help R Q II Protocol Length Info TCP 66 7680 + 62553 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK PERM=1 TCP 66 62554 = 77880 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM=1 TCP 66 62555 + 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM=1 TCP 66 62555 + 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM=1 TCP 66 62555 + 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM=1 TCP 66 62555 + 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM=1 TCP 66 62555 [SYN, ACK] Seq=0 Ack=1 Win=25200 Len=0 MSS=1460 SACK PERM=1 TCP 66 62555 [SYN, ACK] Seq=0 Ack=1 Win=25200 Len=0 MSS=1460 SACK PERM=1 TCP 66 62555 [SYN, ACK] Seq=0 Ack=1 Win=25200 Len=0 MSS=1460 SACK PERM=1 TCP 50 0 + 26555 [SYN, ACK] Seq=0 Ack=1 Win=25200 Len=0 MSS=1460 SACK PERM=1 TCP 50 0 + 26555 [SYN, ACK] Seq=0 Ack=1 Win=25200 Len=0 MSS=1460 SACK PERM=1 TCP 50 0 + 26555 [SYN, ACK] Seq=0 Ack=1 Win=25200 Len=0 MSS=1460 SACK PERM=1 TCP 50 0 + 26555 [SYN, ACK] Seq=0 Ack=1 Win=25200 Len=0 MSS=1460 SACK PERM=1 TCP 50 0 + 26555 [SYN, ACK] Seq=0 Ack=1 Win=25200 Len=0 MSS=1460 SACK PERM=1 TCP 50 0 + 26555 [SYN, ACK] Seq=0 Ack=1 Win=25200 Len=0 MSS=1460 SACK PERM=1 TCP 50 0 + 26556 [SYN] Seq=0 + 26555 [SYN, ACK] Seq=0 Ack=1 Win=25200 Len=0 MSS=1460 SACK PERM=1 TCP 50 0 + 26556 [SYN] Seq=0 + 26556 [SYN] Seq=0 Ack=1 Win=25200 Len=0 MSS=1460 SACK PERM=1 WS=128 S528 bits) on interface 0 S528 bits) ON INTERF
Ethemet Edit View Go Ideostration Ideostration Time 266 81.417971 408 121.44296 408 121.44457 537 161.45861 537 161.459554 588 188.302284 588 188.310225 rame 6: 66 bytes rame 7: 66 bytes	Capture Analyze Stat Source 192,168,1.5 192,168,1.9 192,169,1.9 192,169,1.9 192,169,1.9 192,169,1.9 192,100,1.9 192,100,1.9 192,100,1.9 192,100,1.9 192,100,1.9 192,100,1.9 192,100,1.9 192,100,1.9 192,100,1.9 192,100,1.9 192,100,1.9 192,100,1.9 192,100,1.9 192,100,1.9 192,100,1.9 193,100,1.9	tistics Telephony Wirele To a to a	ess Tools Help
Ethernet Edit View Go Image: Control of the state of	Capture Analyze Stat	tistics Telephony Wireles Destruston 192.168.1.9 192.168.1.9 192.168.1.5 192.168.1.5 192.168.1.5 192.168.1.9 66.bytes captured (5: 186.81.9 Oct 192.161 186.81.9 Oct 192.161 186.81.9 Oct 192.161 186.81.9 Oct 192.161 186.81.9 Oct 192.161 186.81.9 Oct 192.161 186.81.9 Oct 192.161 192.163.1.9 Oct 192.163.1.9 Oct 192.163.1.9 Oct 192.163.1.9 Oct 192.163.1.9 Oct 192.163.1.9 Oct 192.1.9 Oct 192.163.1.9 Oct 192.163.1.9 Oct 192.1.9 Oct 192.1	ess Took Help ess Took Help ess Took Help ess Took Help
Ethernet Edit View Go Comparison of the second of the se	Capture Analyze Stat	tistics Telephony Wirele To a a a a a a a a a a a a a a a a a a a	ess Tools Help
Ethernet Edit View Go Colorstant Colorstant Time 268 81.417971 408 121.44296 408 121.444157 537 161.45817 537 161.45817 537 161.45817 537 188.302184 588 188.310225 Frame 6: 66 bytes Frame 6: 66 bytes Frame 6: 66 bytes	Capture Analyze Stat Source 192,168,1.5 192,168,1.9 192,168,1.9 192,168,1.9 192,168,1.9 192,168,1.9 192,168,1.9 192,168,1.9 192,168,1.9 192,168,1.9 192,168,1.5 192,128,1.5 193,128,1.5 194,128,1.5 194,128,1.5 194,128,1.5 194,128,1.5 194,128,1.5	tistics Telephony Wirele Telephony Wirele Destnation 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 23.200.239.129 192.168.1.9 66 bytes captured (57 18:60:24:40:3d:1d), D 18:60:24:40:3d:1d), D 19:60:25:1, D st Port: 12:1d 19:60:24:40:3d:1d), D 19:60:25:1, D st Port: 12:1d 19:60:24:40:3d:1d 19:70:24:40:3d:1d 19:70:24:40:3d:1d 19:70:24:40:3d:1d 19:70:24:40:3d:1d 19:70:24:40:3d:1d 19:70:24:40:3d:1d 19:70:24:40:3d:1d 19:70:24:40:3d:1d 19:70:24:40:3d:1d 19:70:24:40:3d:1d 19:70:24:40:3d:1d 19:70:24:40:3d:1d 19:70:24:40:3d:1d 19:70:24:40:3d:1d 19:70:24:40:3d:1d 19:70:24:40:3d:1d 19:70:24:40:3d:1d 19:70:24:40:3d:1d 19:70:24:40:3d:1d 19:70:24:70:24:70:24:7	ess Tools Help R Q II Protocol Length Info TCP 66 7680 + 62553 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 MS=256 SACK PERM=1 TCP 66 62554 + 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM=1 TCP 66 62555 + 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM=1 TCP 66 62555 + 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM=1 TCP 66 62555 + 7680 [SYN] Seq=0 Ack=1 Win=5533 Len=0 MSS=1460 WS=256 SACK PERM=1 TCP 66 62556 [SYN, ACK] Seq=0 Ack=1 Win=2533 Len=0 MSS=1460 HS=256 SACK PERM=1 TCP 66 80 + 62556 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128 S28 bits) on interface 0 D51: Dell_24:19:135 (10:7d:11a:24:f9:35) 68.1.5 7680, Seq: 0, Len: 0
Ethernet Edit View Go Construction Construction Edit View Go Construction Time 268 81.417971 268 81.417971 268 81.417971 268 81.417971 268 81.417971 268 81.417971 268 81.417971 268 81.417971 268 183.310225 Frame 6: 66 bytes thernet II, Srci Frame 6: 66 bytes Thernet Frotocol Framewission Contr	Capture Analyze Stat	tistics Telephony Wirele Telephony Wirele Destination 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 66 bytes captured (5; 18:66:14,9 ost: 192.161 18:66:14,9 ost: 192.161 nrt: 62551, Dst Port: 7	ess Took Help Cook Help Cook Help Cook Help Protocol Length Info Cook Help Cook Help Protocol Length Info Cook Help TCP 66 7680 + 62553 [SVN, ACK] Seq=0 Ack+1 Win+65535 Len=0 MS5-1460 W5-256 SACK PERM+1 TCP 66 7680 + 62554 [SVN] Seq=0 Ack+1 Win+65535 Len=0 MS5-1460 W5-256 SACK PERM+1 TCP 66 7680 + 62555 [SVN, ACK] Seq=0 Ack+1 Win+5535 Len=0 MS5-1460 W5-256 SACK PERM+1 TCP 66 7680 + 62555 [SVN, ACK] Seq=0 Ack+1 Win+5535 Len=0 MS5-1460 W5-256 SACK PERM+1 TCP 66 7680 + 62555 [SVN, ACK] Seq=0 Ack+1 Win+25200 Len=0 MS5-1460 W5-256 SACK PERM+1 TCP 66 80 + 62556 [SVN, ACK] Seq=0 Ack+1 Win+25200 Len=0 MS5-1460 SACK_PERM+1 TCP 66 80 + 62555 [SVN, ACK] Seq=0 Ack+1 Win+25200 Len=0 MS5-1460 SACK_PERM+1 TCP 66 80 + 62555 [SVN, ACK] Seq=0 Ack+1 Win+25200 Len=0 MS5-1460 SACK_PERM+1 TCP 66 80 + 62555 [SVN, ACK] Seq=0 Ack+1 Win+25200 Len=0 MS5-1460 SACK_PERM+1 TCP 66 80 + 62555 [SVN, ACK] Seq=0 Ack+1 Win+25200 Len=0 MS5-1460 SACK_PERM+1 TCP 66 80 + 62555 [SVN, ACK] Seq=0 Ack+1 Win+25200 Len=0 MS5-1460 SACK_PERM+1 TCP 66 80 + 62555 [SVN, ACK] Seq=0 Ack+1 Win+25200 Len=0 MS5-1460 SACK_PERM+1 TCP 66 80 + 62555 [SVN, ACK] Seq=0 Ack+1 Win+25200 Len=0 MS5-1460 SACK_PERM+1 TCP 66 80 + 62555 [SVN, ACK] Seq=0 Ack+1 Win+25200 Len=0 MS5-1460 SACK_PERM+1 TCP 66 80 + 62555 [SVN, ACK] Seq=0 Ack+1 Win+25200 Len=0 MS5-1460 SACK_PERM+1 TCP 66 80 + 62555 [SVN, ACK] Seq=0 Ack+1 Win+25200 Len=0 MS5-1460 SACK_PERM+1 TCP 66 80 + 62555 [SVN, ACK] Seq=0 Ack+1 Win+25200 Len=0 MS5-1460 SACK_PERM+1 W5-128 S28 bits) on interface 0 S10 - S10 - S
Ethernet Edit View Go Chiposophia Chiposophia Edit View Go Chiposophia Time 268 81.437971 268 81.437971 268 18.142956 469 121.444157 537 161.459554 537 161.459554 537 161.459554 537 163.30225 Transe 6: 66 bytes thernet II, Src: Internet Protocol Transmission Contr	Capture Analyze Stat Capture Analyze Stat Source 192,168,1.5 192,168,1.5 192,168,1.5 192,168,1.5 192,168,1.5 192,168,1.5 192,168,1.9 23,200,239,129 on wire (528 bits), HewlettP_bd:3d:1d (Version 4, Src: 192 on Protocol, Src Po	tistics Telephony Wireles Destination 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 18.66:24:bd:3d:1d), Di 18.66:24:bd:3d:1d), Di 18.66:24:24:24:24:24:24:24:24:24:24:24:24:24:	ess Tools Help
Ethernet Edit View Go Edit View Go Composition Edit View Go Composition Time 268 81.417971 408 121.44296 408 121.444357 537 161.458617 537 161.458617 537 161.458617 537 161.458617 537 168.302284 558 188.302284 558 188.302284 558 188.302284 558 188.30228 0 10 70 1a 24 99 0 00 34 33 66 40	Capture Analyze Stat Source 192.168.1.5 192.168.1.9 192.169.1.9	tistics Telephony Wireles	
Ethernet Edit View Go	Capture Analyze Stat	tistics Telephony Wirele To a to a	
Ethernet Edit View Go Composition Edit View Go Composition Time 268 81.417971 268 81.417971 268 81.417971 268 81.417971 268 21.444157 268 218.30245 267 188.30245 267 188.30245 267 188.30245 268 188.31024 268 218.3102 268 218.3102 268 218.3102 268 218.3102 268 218.3102 268 218.3102 268 218.3102 268 218.3102 268 218.3102 268 218.3102 268 218.3102 268 218.3102 268 218.310 268 218 26	Capture Analyze Stat Capture Analyze Stat Source 192.168.1.5 192.168.1.5 192.168.1.5 192.168.1.5 192.168.1.5 192.168.1.5 192.168.1.5 192.168.1.9 23.200.239.129 on wire (528 bits), HewlettP_bdi3di1d (Version 4, Src: 192 rol Protocol, Src Pe 193.18 60 24 bd 3d 00 80 66 3e ff fc 00 3c 64 65 bd 01 10 90 40 55 bd 01 10 90 40 40 40 40 40 40 40 40 40 40 40 40 40	tistics Telephony Wireles Destruction 192_168.1.9 192_1	
Ethernet Edit View Go Chorsesyneel Time 268 61.417971 409 121.444157 538 161.458617 537 161.458617 537 161.458617 537 161.458617 537 161.458617 537 161.458617 537 161.458617 537 161.458617 537 161.458617 547 161.45867 547 161.45867 547 161.45867 547 161.45867 547 161.45867 547 161.45867 547 161.45867 547 161.45867 547 161.4587 547 1	Capture Analyze Stat Source 192.168.1.5 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 23.200.239.129 on wire (528 bits), Hewlettp-dbi3didd (Version 4, Src: 192 rol Protocol, Src Po 00 80 60 3e ff c0 80 a6 C5 fb ab 80 80 80 60 20 44 65 b4 61	tistics Telephony Wirele To a Destruction 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 23.200.239.129 192.168.1.9 23.200.239.129 192.168.1.9 18:60:24:164:3d:1d), D 1.168.1.9, Dst: 192.164 Int: 62551, Dst Port: 3 1d 08 00 45 00 03 03 06 01 01 	
Ethernet Edit View Go Construction Construction Edit View Go Construction Constr	Capture Analyze Stat Source 192,168,1.5 192,168,1.9 192,169,1.9 192,169,1.9 194,100,1.9	tistics Telephony Wirele To a to a second s	
Ethernet Edit View Go Characteristic (Characteristic) Edit View Go Characteristic) Time 268 51.437971 268 51.437971 268 51.437951 587 151.458557 587 158.39214 Frame 6: 66 bytes thernet II, Src: Frame 6: 66 bytes thernet II, Src: Transmission Contr 0 10 7d 1a 24 f9 0 00 34 38 66 44 0 10 57 45 77 16 0 61 95 77 90 0 44 92	Capture Analyze Stat Capture Analyze Stat Source 192.168.1.5 192.168.1.5 192.168.1.5 192.168.1.5 192.168.1.5 192.168.1.5 192.168.1.5 192.168.1.9 23.200.239.129 on wire (528 bits), HewlettP_bdi3di1d (Version 4, Src: 192 oil Protocol, Src Pe 0 00 65 ac ff. 6 00 a 65 5 f ba b 00 00 ac 5 f ba b 00	tistics Telephony Wireles Destruction 192_168.1.9 192_1	
Ethernet Edit View Go Chorsesyn=2 Time 268 61.417971 378 61.42966 409 121.444157 537 161.458617 537 161.458617 537 161.458617 537 161.458617 537 161.458617 537 161.458617 537 161.458617 537 161.458617 537 161.458617 547 161.4587 547 161.	Capture Analyze Stat Source 192.168.1.5 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 23.200.239.129 on wire (528 bits), Hewlettp-dbi3d:dd (Version 4, Src: 192 rol Protocol, Src Po 00 80 66 3e ff c0 80 a6 c5 fb ab 60 80 a6 c5 fb	tistics Telephony Wireles Telephony Wireles Destruction 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 23.200.239.129 192.168.1.9 23.200.239.129 192.168.1.9 18:60:24:164:3d:1d), D 1.168.1.9, Dst: 192.164 18:60:24:164:3d:1d), D 1.168.1.9, Dst: 192.164 10:60:2551, Dst Port: 7 10:60:2551, Dst Port: 7 10:60:26:26:26:26 00:00:00:80:20:27 00:00:00:27 00:00:00:27 10	
Ethernet Edit View Go Control	Capture Analyze Stat	tistics Telephony Wirele Destruction 192.168.1.9 192.168.1.9 192.168.1.5 192.168.1.5 192.168.1.9 192.168.1.9 66 bytes captured (5: 186.81.9 00: 192.161 186.81.9 00: 192.161 1168.19 00: 192.161 1168.19 00: 192.161 1168.19 00: 192.161 1168.19 00: 192.161 1168.19 00: 192.161 117.168.19 00: 192.161 118.69 00: 08.0 08.00 00: 08.00 00: 192.161 118.69 00: 08.0 118.69 00: 192.161 118.69 00: 08.0 118.69 00: 08.0 1	
Ethernet Edit View Go Chopsbyth=1 Time 268 81.437971 268 81.437971 268 81.437971 268 81.437954 468 121.444157 537 161.459554 537 168.30214 587 168.30214 587 168.30214 588 188.31024 587 168.30214 588 188.31024 588 1888 1888 1884 588 188 1884 588 1888 1884 588 1888 1884 58	Capture Analyze Stat Capture Analyze Stat Source 192.168.1.5 192.168.1.5 192.168.1.9 192.168.	tistics Telephony Wireles Destruction 192_168.1.9 192_1	ess Tools Help
Ethernet Edit View Go Chorsestant Chorsestant Edit View Go Chorsestant Time 268 81,437971 336 161,438617 337 161,439817 337 161,439817 537 161,439817 537 161,439817 537 161,439817 587 188,302184 587 188,302184 587 188,302184 588 188,310225 Frame 6: 66 bytes thernet II, Src: internet Protocol Framelission Contr 0 10 7d 1a 24 59 0 00 34 38 66 40 0 10 574 57 1e 0 46 22 F7 00 0 46 2	Capture Analyze Stat Source 192,168,1.5 192,168,1.9 192,168,1.9 192,168,1.9 192,168,1.5 192,164,1.5	tistics Telephony Wireles	ess Tools Help
Ethernet Edit View Go Composition Time 268 81.417971 268 81.417971 268 81.417971 268 81.417971 268 81.417971 353 6161.45954 557 188.302184 557 188.302184 557 188.302184 558 188.310225 Trame 6: 66 bytes thernet Frotcool reassission Contr 0 01 07 d 1a 24 69 0 09 34 38 66 40 01 05 74 57 16 0 16 70 1a 77 06 0 04 62	Capture Analyze Stat Source 192.166.1.5 192.166.1.9 192.167.10 192.10	tistics Telephony Wirele Destruction 192.168.1.9 192.168.1.9 192.168.1.5 192.168.1.9 192.168.1.9 192.168.1.9 66 bytes captured (5: 186.81.9, 085.1.9 186.81.9, 085.1.9 1168.92, 085.1.9 10 08 09 45 09 09 09 09 88 08 2 03 09 09 01 01 1 0 08 09 11 1 1 0 08 09 11 1 1 0 08 09 11 1 1 0 00 09 01 1 1 0 00 09 08 08 0 1 0 00 00 08 08 0 1 0 00 08 08 0 1 0 00 00 08 08 0 1 0 00 00 08 0 1 0 00 00 08 08 0 1 0 00 08 08 0 1 0 00 08 08 0 1 0 00 00 08 08 0 1 0 00 00 08 08 0 1 0 00 0 1 0 00 08 0 1 0 00 08 0 1 0 00 0 1 0 00 00 08 0 1 0 00 0 1 0 00 00 0 1 0 00 00 08 00 0 1 0 00 00 08 00 0 1 0 00 00 08 08 0 1 0 00 00 00 08 08 0 1 0 00 00 08 08 0 1 0 00 00 00 08 08 0 1 0 00 00 00 08 08 0 1 0 00 00 08 08 0 1 0 00 00 08 0 1 0 00 00 00 00 00 00 00 00 00 00 00 00	
Ethernet Edit View Go Choose Syntael Time 268 81.417971 468 121.44291 448 121.44291 448 121.444157 535 161.458517 537 161.458517 537 161.458517 537 161.458517 537 161.459554 587 188.382184 588 188.31024 588 188.31024 588 188.31024 588 188.31024 588 188.31024 581 183.30218 788 383.302 788 383 383.302 788 385	Capture Analyze Stat	tistics Telephony Wireles Destruction 192_168_1.9 192_168.1.9 192_	<pre>ss Tools Help</pre>
thernet Edit View Go i ()	Capture Analyze Stat Source 192.168.1.5 192.168.1.9	tistics Telephony Wireles	<pre>sr Tools Help</pre>
thernet Edit View Go	Capture Analyze Stat Source 192.168.1.5 192.168.1.9	tistics Telephony Wirele To a Destruction 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 192.168.1.9 23.200.239.129 192.168.1.9 66 bytes captured (51 18:60:24:164:3d:1d), D 1.168.1.9, Dst: 192.164 nrt: 62551, Dst Port: 3 1d 08 00 45 00	
thernet Edit View Go Stop:Synes Time 268 81.447971 408 121.442966 409 122.444267 537 161.459637 537 161.459534 537 186.302184 537 186.302184 109 7d 1a 24 f9 00 34 38 664 01 05 f4 57 18 10 7d 1a 24 f9 00 34 38 664 01 05 f4 57 18 fa f0 3b f7 00 04 02	Capture Analyze Stat Source 192,168,1.5 192,168,1.5 192,168,1.9	tistics Telephony Wireles Destruction 192.168.1.9 192.168.1.9 192.168.1.5 192.168.1.9 192.1	<pre>sr Tools Help R R R R R R For for for for for for for for for for f</pre>

Wireshark packet sniffing

- Open the Wireshark Application.
- Select the current interface. Here in this example, interface is Ethernet that we would be using.
- The network traffic will be shown below, which will be continuous. To stop or watch any particular packet, you can press the red button below the menu bar.

	Capti	uring fro	m Ethern	iet											
File	E	dit Vie	w Go	Capt	ure A	Analyze	Sta	tistics	Tele	phony	Wireless	s Tools	Help		
		0	010	\times	6 9	÷	€ 🗧	Ŷ	& [$\Theta_{\mathbf{Q}}$	् 🎹			
	Apply	a display	filter <	<ctrl-></ctrl->											
No.		Time		S	ource				Destin	ation		Protoc	ol Len	gth	Info
	29	92 14.2	92031	f	e80::3	3d37:c	0cd:6	53a	ff02:	:1:2		DHCP	v6 1	L45	Solicit XID: 0xef2214 CID: 000100012478f05e588a5a4a43cd
11	29	93 14.3	25924	1	92.168	3.1.11			192.1	68.1.2	55	UDP		62	2008 → 2008 Len=20
	29	94 14.3	27047	1	92.168	3.1.11			192.1	68.1.2	55	UDP		62	2007 → 2007 Len=20
li i	29	95 14.4	41599	1	92.168	3.1.11			192.1	68.1.2	55	UDP		62	2008 → 2008 Len=20
	29	96 14.4	42756	1	92.168	3.1.11			192.1	68.1.2	55	UDP		62	2007 → 2007 Len=20
	29	97 14.5	22281	f	e80::b	ddd:7	b9a:d	160	ff02:	:1:ffc	d:a83c	ICMP	v6	86	Neighbor Solicitation for fe80::75e0:e904:d2cd:a83c from 10:e7:c6:7a:af:de
Ĺ	29	98 14.5	46693	1	92.168	3.1.11			192.1	68.1.2	55	UDP		62	2008 → 2008 Len=20
> > > >	Fram Ethe Inte Jser Data	net I rnet I Datag	2 bytes I, Src: rotocol ram Pro ytes)	s on w Hewl Vers otocol	vire (lettP_ sion 4 L, Src	496 b 8d:41 , Src Port	its), :2b (: 192 : 200	62 84:34 .168 8, D	bytes 4:97: .1.11 st Po	captu 8d:41: , Dst: rt: 20	red (490 2b), Ds [.] 192.160 08	6 bits) t: Broad 8.1.255	on int Icast (erfa ff:	ace 0 ff:ff:ff:ff:ff)
000	00	ff ff i	ff ff f	f ff	84 34	97 8	Bd 41	2b @	98 00	45 00		···4 ···A	+••E•		
001	10	00 30 e	ec e7 0	0 00	80 11	c9 7	7a c0	a8 0	01 Øb	c0 a8	-0	· · · z ·			
002	20	01 ff (97 d8 0	7 d8	00 1c	06 1	fe 42	43 2	20 31	35 44		· · · · · · · · B	C 15D		
003	30	45 53 4	4b 54 4	f 50	2d 44	37 3	30 51	53 3	37 35		ESKTO	DP-D 70Q	S75		

I/O GRAPHS





the steps to understand the TCP Stream graphs:

- Open the Wireshark. Click on the interface to watch the network traffic.
- Apply the filter as 'tcp.'
- Click on the option 'Statistics 'on the menu bar and select 'TCP Stream graphs' and select 'Time sequence (tcptrace). You can also choose other options in the 'TCP Stream graphs' category depending on your requirements. Now the screen will look as:





WIRESHARK DECRYPTION

The decryption process is used for the data to be in a readable format. Below are the steps for the decryption process.

- Open the Wireshark and then select the particular interface as explained above.
- $_{\circ}~$ Go to the 'Edit' option and select the 'Preferences' option.
- A dialogue will appear as shown below:

📕 *Ethernet						- 0 X	1
File Edit View	Go Capture Analyze	Statistics Telephony Wireless Tools Help					
🥖 🔳 🖉 💿	📙 🛅 🔀 🛅 🔍 👄 考) 🕾 T 🕗 📃 📃 Q, Q, Q, 🎹					
Apply a display fil	lter <ctrl-></ctrl->					Expression	+
The product of the second seco	Wireshark - Preference Columns Font and Colors Layout Capture Expert Filter Buttons Name Resolution Protocols RSA Keys Statistics Advanced	es		? X Browse	Detatime 7 Join group 224.0.0.251 for any sources / Join group 224.0.0.252 for any sources / 7 Join group 224.0.0.252 for any sources Join group 224.0.0.252 for any sources 1 Join group 224.0.0.252 for any sources Join group 224.0.0.252 for any sources 1 Join group 239.255.255.250 for any sources Join group 239.255.102.18 for any sources 1 Join group 239.255.102.18 for any sources Join group 230.255.250 for any sources 1 Join group 230.255.102.18 for any sources Join group 230.255.250 for any sources 1 Join group 230.255.255.250 for any sources Join group 230.255.255.250 for any sources 1 Join group 224.0.0.252 for any sources	Bytes 0.001335 0.027316 0.027316 0.005192 0.005192 0.00222 0.00222 0.00223 0.005632 0.005632 0.005632 0.005639 0.005639 0.005639 0.005639 0.005639 0.000522 0.000522 0.000522 0.000522 0.000523 0.000523 0.00519 0.00519 0.00519 0.00519 0.00519 0.00519 0.00519	
 Frame 56: 62 Frame 56: 62 Ethernet II, Destinati Source: H Source: H Juser Datagra Data (28 byt Data (28 byt<	<pre></pre>	2008, Dst Port: 2008 d 41 2b 08 00 45 00 3 c0 a8 01 0b c0 a8 42 43 20 31 35 44 9 51 53 37 35 ESKTOP-D 70Q575	CK Cancel	Help	Joan group 224.6.0.22 Tor any sources / _ Devices: 1080 - Deviced: 1080 / 100 0%) - Promeet: 0	(m (nsc)) Profile-Defi	↓

- Select the 'Protocol' option in the left column.
- From the drop-down list, select the 'IEEE 802.11' option. Check the box of decryption and click on the Edit option under it.
- A box will appear. Click on the option shown below:

*Ethernet								— ć	
File Edit View Go Capture Analyze St	tatistics 1	Felephony W	ireless Too	ols Help					
∡ ■ ∅ ⊛ 📙 🗟 🗙 🖨 🔍 ⇔ ⇔	🖻 🚹 🕹		0,0,1						
Apply a display filter <ctrl-></ctrl->		Control Incontrol						Expre	ession +
No. Ti	ime	Source		Destination	Protocol	Info	Deltatime	E	lytes ^
51 2	.158325	192.168.1.9		224.0.0.22	IGMPv3	Membership Report / Join group 224.0.0.251 for any sources	/	0.001335	_
52 2	.185841	192.168.1.1	2	224.0.0.22	IGMPv3	Membership Report / Join group 224.0.0.252 for any sources	/	0.027516	
53 2	.191033	192.168.1.5		224.0.0.22	IGMPv3	Membership Report / Join group 239.255.255.250 for any sour	ces	0.005192	
54 2	.196685	192.168.1	WEP and	d WPA Decryption Keys		7 X 52 for any sources		0.005652	
55 2	.223708	192.168.1				52 for any sources	/	0.027023	
56 2	.225930	192.168.1	Vertera	V				0.002222	
57 2	.226148	192.168.1	Key type	Key				0.000218	
58 2	.236934	192.168.1	wep	· · · · ·		55.250 for any sour	ces	0.010786	
59 2	.283930	192.168.1	wep			55.250 for any sour	ce	0.046996	
60 2	.289569	192.168.1	wpa-p	sk		02.18 for any source	es	0.005639	
61 2	.289571	192.168.1	inpu p.			52 for any sources	/	0.000002	
62 2	.301238	192.168.1				55.250 for any sour	ce	0.011667	
63 2	.335060	192.168.1						0.033822	
64 2	.335382	192.168.1						0.000322	
65 2	.337680	192.168.1				52 for any sources	/	0.002298	
66 2	.343007	192.168.1				52 for any sources	/	0.005327	
67 2	.428026	192.168.1				51 for any sources	/	0.085019	
68 2	.431205	192.168.1				55.250 for any sour	ce	0.003179	
69 2	.440515	192.168.1				52 for any sources	/	0.009310	
<		**** ***						0 000000	>
> Frame 56: 62 bytes on wire (496 bits	s), 62 by	tes captur							
Ethernet II, Src: HewlettP_8d:41:2b	(84:34:9	7:8d:41:2b							
> Destination: Broadcast (ff:ff:ff:	*****)							
<pre>> Source: HewlettP_8d:41:2b (84:34:</pre>	97:80:41	:20)							
Type: 1PV4 (0x0800)			+ -	4 ~ V UG					
> Internet Protocol Version 4, Src: 19	92.168.1.	11, Dst: 1			0	K Copy from Z Capcel Help			
> User Datagram Protocol, Src Port: 20	908, UST	Port: 2008							
> Data (20 bytes)		_							
0000 ff ff ff ff ff ff 84 34 97 8d 4	1 2b 08	00 45 00	4	· · A+ · · E ·					
0010 00 30 f7 ee 00 00 80 11 be 73 c	0 a8 01	0b c0 a8	0	· s · · · · ·					
0020 01 ff 07 d8 07 d8 00 1c 06 fe 4	2 43 20	31 35 44		··BC 15D					
0030 45 53 4b 54 4f 50 2d 44 37 30 5	1 53 37	35	SKIOP-D 1	/002/5					
🦲 🍞 - Hear Datanzam Drotocol (udo) - 8 hutae						Darkater 1080 - Dienlavadi 1080 (100	0%) · Dropped: 0 //	1 (196)	Irofila- Dafarili

- Select the option wpa-pwd and set the password accordingly.
- The data will be decrypted.
- But the above decryption process is only possible if there is a proper handshake.

RESULT:

Thus, the installation of wire shark, tcpdump observes the data transfer in client server communication using TCP/UDP and identify the TCP/UDP datagram successfully install and output is verified.

CHECK MESSAGE INTERGRITY AND CONFIDENTIALITY USING SSL

AIM:

To Check Message Intergrity And Confidentiality Using SSL.

PROCEDURE:

Installing & Configuring HTTP with SSL (HTTPS) Public Key Cryptography (Asymmetric Cryptography)

In public key cryptography, a matching pair of keys is used; one for encryption and the other for decryption. One of the key is called the public key (can be published or sent over the network and known to all users). The other is called the private key (kept secretly by the owner).

 $K_E \,{\neq}\, K_D$

In some public-key algorithms, such as RSA, both keys can be used for encryption. In other algorithms, one key is for encryption only and the other for decryption.

Handshaking - Key Exchange

Once the ciphersuit to be used are negotiated and agree-upon, the client and server will establish a session key:

- 1. The client uses server's public key to encrypt a secret and sends to the server.
- 2. Only the server has the matching private key to decrypt the secret (not the Eavesdroppers).
- 3. The client and server then use this secret to generate a session key independently and simultaneously.

This session key would then be used for secure communication for this particular communication session

1. The client generates a 48-byte (384-bit) random number called pre_master_secret, encrypts it using the verified server's public key and sends it to the server.

- 2. Server decrypts the pre_master_secret using its own private key. Eavesdroppers cannot decrypt the pre_master_secret, as they do not possess the server's private key.
- 3. Client and server then independently and simultaneously create the session key, based on the pre_master_secret, client_random and server_random. Notice that both the server and client contribute to the session key, through the inclusion of the random number exchange in the hello messages. Eavesdroppers can intercept client_random and server_random as they are sent in plaintext, but cannot decrypt the pre_master_secret.
- 4. In a SSL/TLS session, the session key consists of 6 secret keys (to thwart crypto-analysis). 3 secret keys are used for client-to-server messages, and the other 3 secret keys are used for server-to-client messages. Among the 3 secret keys, one is used for encryption (e.g., DES secret key), one is used for message integrity (e.g., HMAC) and one is used for cipher initialization. (Cipher initialization uses a random plaintext called Initial Vector (IV) to prime the cipher pump.)
- 5. Client and server use the pre_master_secret (48-byte random number the client and created exchange by securely), client_random, server_random, and a pseudo-random function a master_secret. (PRF) to generate They can use the master_secret, client_random, server_random, and the pseudo-random function (PRF) to generate all the 6 shared secret keys. Once the secret keys are generated, the pre_master_secret is no longer needed and should be deleted.
- 6. From this point onwards, all the exchanges are encrypted using the session key.
- 7. The client sends Finished handshake message using their newly created session key. Server responds with a Finished handshake message.

Message Exchange

Client and server can use the agreed-upon session key (consists of 6 secret keys) for secure exchange of messages.

Sending messages:

1. The sender compresses the message using the agreed-upon compression method (e.g., PKZip, gzip).

- 2. The sender hashes the compressed data and the secret HMAC key to make an HMAC, to assure message integrity.
- 3. The sender encrypts the compressed data and HMAC using encryption/decryption secret key, to assure message confidentiality.

Retrieve messages:

- 1. The receiver decrypts the ciphertext using the encryption/decryption secret key to retrieve the compressed data and HMAC.
- 2. The receiver hashes the compressed data to independently produce the HMAC. It then verifies the generated HMAC with the HMAC contained in the message to assure message integrity.
- 3. The receiver un-compresses the data using the agreed-upon compression method to recover the plaintext.

OUTPUT

> openssl s_client ?

(Display the available options)

The following command turns on the debug option and forces the protocol to be TLSv1:

> openssl s_client -connect localhost:443 -CAfile ca.crt -debug -tls1

Loading 'screen' into random state - done CONNECTED(00000760)

```
write to 00988EB0 [009952C8] (102 bytes => 102 (0x66))

0000 - 16 03 01 00 61 01 00 00-5d 03 01 40 44 35 27 5c ....a...]..@D5'\

0010 - 5a e8 74 26 e9 49 37 e2-06 3b 1c 6d 77 37 d1 ae Z.t&.I7..;.mw7..

0020 - 44 07 86 47 98 fa 84 1a-8d f4 72 00 00 36 00 39 D..G.....r..6.9

0030 - 00 38 00 35 00 16 00 13-00 0a 00 33 00 32 00 2f .8.5.....3.2./

0040 - 00 07 00 66 00 05 00 04-00 63 00 62 00 61 00 15 ...f....c.b.a..

0050 - 00 12 00 09 00 65 00 64-00 60 00 14 00 11 00 08 .....e.d.`.....

0060 - 00 06 00 03 01 .....

0066 - <SPACES/NULS>
```

read from 00988EB0 [00990AB8] (5 bytes => 5 (0x5)) 0000 - 16 03 01 00 2a* read from 00988EB0 [00990ABD] (42 bytes => 42 (0x2A)) 0000 - 02 00 00 26 03 01 40 44-35 27 cc ef 2b 51 e1 b0 ...&..@D5'..+Q.. 0010 - 44 1f ef c4 83 72 df 37-4f 9b 2b dd 11 50 13 87 D....r.7O.+..P.. 0020 - 91 0a a2 d2 28 b9 00 00-16(.... 002a - <SPACES/NULS>

read from 00988EB0 [00990AB8] (5 bytes => 5 (0x5)) 0000 - 16 03 01 02 05

read from 00988EB0 [00990ABD] (517 bytes => 517 (0x205)) 0000 - 0b 00 02 01 00 01 fe 00-01 fb 30 82 01 f7 30 820...0. 0010 - 01 60 02 01 01 30 0d 06-09 2a 86 48 86 f7 0d 01 .`..0...*.H.... 0020 - 01 04 05 00 30 4d 31 0b-30 09 06 03 55 04 06 130M1.0...U... 0030 - 02 55 53 31 10 30 0e 06-03 55 04 0b 13 07 74 65 .US1.0...U....te 0040 - 73 74 31 30 31 31 0c 30-0a 06 03 55 04 03 13 03 st1011.0...U.... 0050 - 63 68 63 31 1e 30 1c 06-09 2a 86 48 86 f7 0d 01 chc1.0...*.H.... 0060 - 09 01 16 0f 63 68 63 40-74 65 73 74 31 30 31 2echc@test101. 0070 - 63 6f 6d 30 1e 17 0d 30-34 30 32 32 36 30 36 35 com0...040226065 0080 - 36 35 34 5a 17 0d 30 35-30 32 32 35 30 36 35 36 654Z..0502250656 0090 - 35 34 5a 30 3b 31 0b 30-09 06 03 55 04 06 13 02 54Z0:1.0...U.... 00a0 - 55 53 31 0c 30 0a 06 03-55 04 03 13 03 63 68 63 US1.0...U....chc 00b0 - 31 1e 30 1c 06 09 2a 86-48 86 f7 0d 01 09 01 16 1.0...*.H..... 00c0 - 0f 63 68 63 40 74 65 73-74 31 30 31 2e 63 6f 6d .chc@test101.com 00d0 - 30 81 9f 30 0d 06 09 2a-86 48 86 f7 0d 01 01 01 0..0...*.H..... 00e0 - 05 00 03 81 8d 00 30 81-89 02 81 81 00 cd e4 9e0. 00f0 - 7c b6 d2 34 4e d3 53 46-25 c7 53 88 25 60 e6 46 |..4N.SF%.S.%`.F 0100 - db 64 3a 73 61 92 ac 23-92 cd 2c 94 a9 8f c6 7f .d:sa..#..... 0110 - 47 73 c0 d9 8d 34 b7 2c-dd c9 86 bd 82 6f ce ac Gs...4.....o. 0120 - d8 e2 ba 0f e5 f5 3a 67-2c 89 1a 1b 03 eb 21 85:g,....!. 0130 - 28 e3 29 98 84 ed 46 75-82 fa 0f 30 a3 a9 a5 71 (.)...Fu...0...g 0140 - 46 4c d6 0d 17 c4 19 fd-44 fb e2 18 46 a6 9d ab FL.....D...F... 0150 - 91 de 6b a1 7f fe 30 06-28 5d d8 d3 29 00 c3 1d ...k...0.(]...)... 0160 - 4c 13 00 61 8f f3 85 51-f5 68 d8 69 25 02 03 01 L.a...Q.h.i%... 0170 - 00 01 30 0d 06 09 2a 86-48 86 f7 0d 01 01 04 05 ...0...*.H..... 0180 - 00 03 81 81 00 29 fd bf-5a ed 70 8f 53 a4 e9 14)..Z.p.S... 0190 - 4c 5e ba 84 c6 54 1b f2-c0 3c c4 30 0f 7f 12 80 L^...T...<0....

01a0 - 4e 01 b7 fd 39 50 f1 41-0d d8 aa 77 d9 87 25 1a N...9P.A...w..%. 01b0 - 1e e2 97 88 4f 53 75 c8-70 22 6a 01 61 0f 51 3eOSu.p"j.a.Q> 01c0 - 13 19 9c 64 f2 76 14 e8-85 25 23 a2 11 c4 8c f8 ...d.v...%#..... 01d0 - 23 2c d1 c3 d3 71 3a e6-71 54 10 07 dc 72 ff ee #,...q:.qT...r.. 01e0 - e8 3e cf 8e 77 73 e9 9f-f5 9a 90 60 4d a0 aa 03 .>..ws....`M... 01f0 - 32 1f 11 6f 2e 9a 5f 3c-77 05 22 0c 81 bf 29 96 2...o._ 5 (0x5)) 0000 - 16 03 01 01 8d

read from 00988EB0 [00990ABD] (397 bytes => 397 (0x18D)) 0000 - 0c 00 01 89 00 80 e6 96-9d 3d 49 5b e3 2c 7c f1=I[.,]. 0010 - 80 c3 bd d4 79 8e 91 b7-81 82 51 bb 05 5e 2a 20y....Q..^* 0020 - 64 90 4a 79 a7 70 fa 15-a2 59 cb d5 23 a6 a6 ef d.Jy.p...Y..#... 0030 - 09 c4 30 48 d5 a2 2f 97-1f 3c 20 12 9b 48 00 0e ...0H../..<...H.. 0040 - 6e dd 06 1c bc 05 3e 37-1d 79 4e 53 27 df 61 1e n....>7.yNS'.a. 0050 - bb be 1b ac 9b 5c 60 44-cf 02 3d 76 e0 5e ea 9b\`D..=v.^.. 0060 - ad 99 1b 13 a6 3c 97 4e-9e f1 83 9e b5 db 12 51Q 0070 - 36 f7 26 2e 56 a8 87 15-38 df d8 23 c6 50 50 85 6.&.V...8..#.PP. 0080 - e2 1f 0d d5 c8 6b 00 01-02 00 80 11 3f 5f fa e4k....? .. 0090 - 79 9a 0b d9 e0 67 37 c4-2a 88 22 b0 95 b7 a7 be y....g7.*.".... 00a0 - 93 79 9d 51 ae 31 47 99-df 47 dd 80 5e 3d 2a 4a .y.Q.1G..G..^=*J 00b0 - 29 8b fd c1 63 5e 48 e8-e3 fd ac 95 1b 3a 5f 75)...c^H.....: u 00c0 - 98 2d 3c 9c ba 68 18 7b-be 38 2c 69 3d 41 b7 c3 .-<..h.{.8,i=A.. 00d0 - 08 a1 da b0 a8 a4 fe 9a-d6 1e 56 ff 4c 8c 6e 6bV.L.nk 00e0 - 18 f1 ec 9d 22 a9 90 27-c1 c6 2c 0e bd 0e 13 d4"..'... 0100 - 12 4f bb ce ba f1 76 fb-80 08 37 00 80 30 99 ad .O....v...7..0. 0110 - 9b fc 3a 14 6b a8 2c c5-fe 7b bd 1c 92 ec 19 a6k....{.... 0120 - 75 2d 69 4e f4 9f 74 60-5d d4 3e 06 97 38 bc b5 u-iN..t`].>..8.. 0130 - 0e 3c 1f f2 99 e6 55 4a-36 42 a8 f2 b7 32 2a 1e .<....UJ6B...2*. 0140 - a3 87 b3 f3 79 43 28 d1-7a 0d db 7c 11 26 f3 68yC(.z..|.&.h 0150 - b1 73 b6 78 4b f3 22 20-e4 f7 27 08 ab 74 92 92 .s.xK." ..'..t.. 0160 - 79 26 61 40 1e e9 90 11-e8 b1 cf 99 d9 9f c7 68 y&a@.....h 0170 - 48 e8 f2 a5 d5 d7 0e e1-88 9a bd 0f 40 85 af 2d H.....@..-0180 - da 76 3a 10 6e b9 38 4d-37 9c 41 c8 9f .v:.n.8M7.A..

read from 00988EB0 [00990AB8] (5 bytes => 5 (0x5)) 0000 - 16 03 01 00 04 read from 00988EB0 [00990ABD] (4 bytes => 4 (0x4)) 0000 - 0e 0004 - <SPACES/NULS>

write to 00988EB0 [00999BE0] (139 bytes => 139 (0x8B)) 0000 - 16 03 01 00 86 10 00 00-82 00 80 63 c2 3c 69 26c...dU.....]n.. 0030 - 05 f1 db 44 f3 13 a8 24-3a 76 0e 3e 1a 6e 55 0c ...D...:v.>.nU. 0040 - 31 9b 04 99 30 ff 8f d2-8d 8e 0d b1 67 ac 43 ee 1...0.....g.C. 0050 - b2 3f d3 c7 c5 33 81 e1-3f d2 47 6f 5d 8a fb 4c .?...3..?.Go]..L 0060 - 62 c7 23 b3 f7 ad 3c a9-0c 87 4a 08 07 55 ba 06 b.#...
 0070 - 34 18 0c 5f d9 35 f0 2b-90 9a 9d 6b 87 62 41 0f 4.._.5.+...k.bA. 0080 - b3 47 74 5f 5b b8 59 5a-b2 21 dd ...Gt_[.YZ.!.

write to 00988EB0 [00999BE0] (6 bytes => 6 (0x6)) 0000 - 14 03 01 00 01 01

write to 00988EB0 [00999BE0] (45 bytes => 45 (0x2D)) 0000 - 16 03 01 00 28 0f 31 83-e0 f8 91 fa 33 98 68 46(.1.....3.hF 0010 - c0 60 83 66 28 fe d3 a5-00 f0 98 d5 df 22 72 2d .`.f(......"r-0020 - e4 40 9b 96 3b 4c f9 02-13 a7 e7 77 74 .@..;L.....wt

read from 00988EB0 [00990AB8] (5 bytes => 5 (0x5)) 0000 - 14 03 01 00 01

```
read from 00988EB0 [00990ABD] (1 bytes => 1 (0x1))
0000 - 01
```

read from 00988EB0 [00990AB8] (5 bytes => 5 (0x5)) 0000 - 16 03 01 00 28(

read from 00988EB0 [00990ABD] (40 bytes => 40 (0x28)) 0000 - d4 0b a6 b7 e8 91 09 1e-e4 1e fc 44 5f 80 cc a1D_... 0010 - 5d 51 55 3e 62 e8 0f 78-07 f6 2f cd f9 bc 49 8d]QU>b..x../...I. 0020 - 56 5b e8 b2 09 2c 18 52- V[....,R] Certificate chain 0 s:/C=US/CN=chc/emailAddress=chc@test101.com i:/C=US/OU=test101/CN=chc/emailAddress=chc@test101.com

Server certificate -----BEGIN CERTIFICATE-----MIIB9zCCAWACAQEwDQYJKoZIhvcNAQEEBQAwTTELMAkGA1UEBh MCVVMxEDAOBgNV BAsTB3Rlc3QxMDExDDAKBgNVBAMTA2NoYzEeMBwGCSqGSIb3DQEJ ARYPY2hjQHR1 c3QxMDEuY29tMB4XDTA0MDIyNjA2NTY1NFoXDTA1MDIyNTA2NTY1 NFowOzELMAkG A1UEBhMCVVMxDDAKBgNVBAMTA2NoYzEeMBwGCSqGSIb3DQEJA RYPY2hjOHRlc3Ox MDEuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDN5J58 ttI0TtNTRiXH U4glYOZG22Q6c2GSrCOSzSyUqY/Gf0dzwNmNNLcs3cmGvYJvzqzY4roP5f U6ZyyJ GhsD6yGFKOMpmITtRnWC+g8wo6mlcUZM1g0XxBn9RPviGEamnauR3mu hf/4wBihd 2NMpAMMdTBMAYY/zhVH1aNhpJQIDAQABMA0GCSqGSIb3DQEBBA UAA4GBACn9v1rt cI9TpOkUTF66hMZUG/LAPMQwD38SgE4Bt/05UPFBDdiqd9mHJRoe4peIT 1N1yHAi agFhD1E+ExmcZPJ2FOiFJSOiEcSM+CMs0cPTcTrmcVQQB9xy/+7oPs+Od3 Ppn/Wa kGBNoKoDMh8Rby6aXzx3BSIMgb8plq3LOxiu -----END CERTIFICATE-----

```
subject=/C=US/CN=chc/emailAddress=chc@test101.com
issuer=/C=US/OU=test101/CN=chc/emailAddress=chc@test101.com
```

No client certificate CA names sent

SSL handshake has read 1031 bytes and written 292 bytes ---New, TLSv1/SSLv3, Cipher is EDH-RSA-DES-CBC3-SHA Server public key is 1024 bit SSL-Session: Protocol : TLSv1 Cipher : EDH-RSA-DES-CBC3-SHA Session-ID: Session-ID-ctx: Master-Key: 57FDDAF85C7D287F9F9A070E8784A29C75E788DA2757699B 20F3CA50E7EE01A66182A71753B78DA218916136D50861AE Key-Arg : None Start Time: 1078211879 Timeout : 7200 (sec)Verify return code: 0 (ok)

GET /test.html HTTP/1.0

write to 00988EB0 [009952C8] (82 bytes => 82 (0x52)) 0000 - 17 03 01 00 18 74 fa 45-35 2d b1 24 59 cf ad 96t.E5-.Y... 0010 - 34 30 01 7d be 8e 70 f9-41 62 11 f1 36 17 03 01 40.}..p.Ab..6... 0020 - 00 30 56 61 ba 2d d3 58-5d e6 6a 83 78 07 87 7a .0Va.-.X].j.x..z 0030 - db b2 a7 40 c7 6d c1 4a-20 3b 82 7d aa 15 e8 65 ...@.m.J ;.}..e 0040 - 3b 92 bd c8 20 e9 9d 41-f1 77 51 d9 ae 31 c4 2c ;....A.wQ..1., 0050 - 32 5a 2Z

write to 00988EB0 [009952C8] (58 bytes => 58 (0x3A)) 0000 - 17 03 01 00 18 39 2f df-43 75 91 13 34 1b 12 049/.Cu..4... 0010 - 7d ef 8d e1 86 54 4f 67-c8 1d cd 07 a4 17 03 01 }....TOg...... 0020 - 00 18 53 d9 22 9d eb 6e-8b 79 f8 e4 82 2f ba ea ...S."..n.y.../.. 0030 - 03 a5 3f 12 85 2e 9f 64-ff dc ...?...d..

read from 00988EB0 [00990AB8] (5 bytes => 5 (0x5)) 0000 - 17 03 01 01 48H read from 00988EB0 [00990ABD] (328 bytes => 328 (0x148)) 0000 - bd eb 8b 9c 01 ac 73 30-8f ca a4 8b 2a 6f bd 02s0....*o.. 0010 - d7 fc 71 18 61 47 f2 1d-70 8b 10 7d 98 28 a4 50 ...q.aG..p.. }.(.P 0020 - f3 0f 42 e8 c5 e1 3e 53-34 bd c7 62 34 1b 5e 8c ...B...>S4..b4.^. 0030 - 99 2d 89 c6 b3 f0 19 96-22 97 43 b8 8f 9d 76 42 .-....".C...vB 0040 - 95 a5 7c db 3b 22 dd 57-29 8d e8 d4 28 3e 89 d8 ...|.;".W)...(>... 0050 - 46 e5 dc 35 51 56 f8 44-d1 82 44 a0 65 b0 93 22 F..5QV.D..D.e.." 0060 - 4b 0a eb 07 26 c9 2a e2-45 4c de 07 0c bb 3e c6 K...&.*.EL....>. 0070 - bc 37 94 cd ec 94 2f 35-76 37 13 4d 0f 88 9c b1 .7..../5v7.M.... 0080 - d7 1c 58 8a 35 5b 32 bc-12 2b 9c e6 5b d4 86 bd ...X.5[2..+..[... 0090 - 39 fc 99 18 79 ec f7 53-db 59 74 49 da 07 69 54 9...y..S.YtI..iT 00a0 - f4 66 aa 36 34 39 f9 0b-87 50 9e 76 db 9f d0 44 .f.649...P.v...D 00b0 - 0c 0d e7 65 80 9b b8 51-56 3d d0 db aa 55 ff ca ...e...QV=...U.. 00c0 - 74 38 24 c1 8c d7 32 cf-ab 03 b3 59 29 0f 80 18 t8\$...2...Y)... 00d0 - 6a d4 e0 7e fd 41 8c f7-1d 81 12 a7 00 b3 71 39 j..~.A......q9 00e0 - 78 1e 3c 17 42 d4 99 22-69 7b 2d 09 ef d8 6e f4 x.<.B.."i{-...n. 00f0 - 64 f6 61 34 72 8c 89 f5-a8 ea 1c b1 0d 08 ff 17 d.a4r.... 0100 - 51 3e 46 2b 38 75 61 6a-1e 34 f4 14 14 38 0d 5e Q>F+8uaj.4...8.^ 0120 - 6c a3 12 c0 a1 3d e1 14-96 d3 1a f9 c9 f2 aa d6 1...=.... 0130 - 12 d5 36 ae 36 f2 18 f5-df c6 ef 34 d7 7d 2b 70 ...6.6.....4. }+p 0140 - 99 88 47 93 91 09 56 b1-...G....V.

HTTP/1.1 200 OK

Date: Tue, 02 Mar 2004 07:18:08 GMT Server: Apache/1.3.29 (Win32) mod_ssl/2.8.16 OpenSSL/0.9.7c Last-Modified: Sat, 07 Feb 2004 10:53:25 GMT ETag: "0-23-4024c3a5" Accept-Ranges: bytes Content-Length: 35 Connection: close Content-Type: text/html

<h1>Home page on main server</h1>

read from 00988EB0 [00990AB8] (5 bytes => 5 (0x5))

0000 - 15 03 01 00 18

read from 00988EB0 [00990ABD] (24 bytes => 24 (0x18)) 0000 - a5 47 51 bd aa 0f 9b e4-ac d4 28 f2 d0 a0 c8 fa .GQ......(..... 0010 - 2c d4 e5 e4 be c5 01 85- ,......

....

closed

write to 00988EB0 [009952C8] (29 bytes => 29 (0x1D)) 0000 - 15 03 01 00 18 d4 19 b9-59 88 88 c0 c9 38 ab 5cY....8.\ 0010 - 98 8c 43 fd b8 9e 14 3d-77 5e 4c 68 03 ...C....=w^Lh.

RESULT:

Thus, the check message intergrity and confidentiality using SSL can verified the output successfully.

Ex:No:06

EXPERIMENT EAVESDROPPING, DICTIONARY ATTACKS, MITM ATTACK

AIM

To experiment eavesdropping, dictionary attack, MITM attack.

PROCEDURE

Man in the Middle (MITM) against Diffie-Hellman:

A malicious Malory, that has a MitM (man in the middle) position, can manipulate the communications between Alice and Bob, and break the security of the key exchange.

- 1. Selected public numbers p and g, p is a prime number, called the "modulus" and g is called the base.
- Selecting private numbers.
 let Alice pick a private random number a and let Bob pick a private random number b, Malory picks 2 random numbers c and d.
- 3. Intercepting public values,

Malory intercepts Alice's public value $(g^{a}(mod p))$, block it from reaching Bob, and instead sends Bob her own public value $(g^{c}(modp))$ and Malory intercepts Bob's public value $(g^{b}(mod p))$, block it from reaching Alice, and instead sends Alice her own public value $(g^{d}(modp))$

- 4. Computing secret key Alice will compute a key $S_1=g^{da} \pmod{p}$, and Bob will compute a different key, $S_2=g^{cb} \pmod{p}$
- 5. If Alice uses S_1 as a key to encrypt a later message to Bob, Malory can decrypt it, re-encrypt it using S_2 , and send it to Bob. Bob and Alice won't notice any problem and may assume their communication is encrypted, but in reality, Malory can decrypt, read, modify, and then re-encrypt all their conversations.

PROGRAM:

import java.util.Random;

import java.util.Scanner;

public class Main {

public static void main(String[] args) {

Scanner scanner = new Scanner(System.in);

Random random = new Random();

System.out.print("Enter a prime number : ");

```
int p = scanner.nextInt();
```

System.out.print("Enter a number : ");

```
int g = scanner.nextInt();
```

class A {

```
private int n;
```

public A() {

this.n = random.nextInt(p) + 1;

}

```
public int publish() {
```

return (int) Math.pow(g, n) % p;

```
public int compute_secret(int gb) {
    return (int) Math.pow(gb, n) % p;
}
```

```
class B {
```

}

private int a;

private int b;

private int[] arr;

```
public B() {
```

```
this.a = random.nextInt(p) + 1;
this.b = random.nextInt(p) + 1;
this.arr = new int[]{a, b};
}
public int publish(int i) {
```

return (int) Math.pow(g, arr[i]) % p;

}

```
public int compute_secret(int ga, int i) {
    return (int) Math.pow(ga, arr[i]) % p;
    }
}
A alice = new A();
A bob = new A();
B eve = new B();
System.out.println("Alice selected (a) : " + alice.n);
```

System.out.println("Bob selected (b) : " + bob.n);

System.out.println("Eve selected private number for Alice (c) : " + eve.a);

System.out.println("Eve selected private number for Bob (d) : " + eve.b);

```
int ga = alice.publish();
```

int gb = bob.publish();

```
int gea = eve.publish(0);
```

```
int geb = eve.publish(1);
```

}

}

System.out.println("Alice published (ga): " + ga);

System.out.println("Bob published (gb): " + gb);

System.out.println("Eve published value for Alice (gc): " + gea);

System.out.println("Eve published value for Bob (gd): " + geb);

Output: Enter a prime number (p) : 227 Enter a number (g) : 14

Alice selected (a) : 227

Bob selected (b) : 170

Eve selected private number for Alice (c) : 65 Eve selected private number for Bob (d) : 175

Alice published (ga): 14

Bob published (gb): 101

Eve published value for Alice (gc): 41 Eve published value for Bob (gd): 32

Alice computed (S1) : 41

Eve computed key for Alice (S1): 41

Bob computed (S2) : 167

Eve computed key for Bob (S2) : 167

RESULT

Thus, the above program experiment eavesdropping, dictionary attacks, MITM attacks are executed successfully and output are verified.

EXPERIMENT WITH SNIFF TRAFFIC USING ARP POISONING

AIM

To experiment with sniff traffic using ARP poisoning.

PROCEDURE

Step 1 – Install the VMware workstation and install the Kali Linux operating system.

Step 2 – Login into the Kali Linux using username pass "root, toor".

Step 3 – Make sure you are connected to local LAN and check the IP address by typing the command **ifconfig** in the terminal.



Step 4 – Open up the terminal and type "Ettercap -G" to start the graphical version of Ettercap.



Step 5 - Now click the tab "sniff" in the menu bar and select "unified sniffing" and click OK to select the interface. We are going to use "eth0" which means Ethernet connection.



Step 6 – Now click the "hosts" tab in the menu bar and click "scan for hosts". It will start scanning the whole network for the alive hosts.

Step 7 – Next, click the "hosts" tab and select "hosts list" to see the number of hosts available in the network. This list also includes the default gateway address. We have to be careful when we select the targets.

lost List ×			
IP Address	MAC Address	Description	
192.168.121.1	00:50:56:C0:00:08		
192.168.121.2	00:50:56:FD:27:1D		
192.168.121.129	00:0C:29:AD:8F:25		
fe80::9040:ab7d:ee93:21fe	00:0C:29:AD:8F:25		
192.168.121.254	00:50:56:F2:40:DC		
Delete Host		Add to Target 1	Add to Target 2
Delete Host ua: no scripts were specimed	, not starting up!	Add to Target 1	Add to Target 2
Delete Host ua: no scripts were specimed tarting Unified sniffing	, not starting up:	Add to Target 1	Add to Target 2
Delete Host ua: no scripts were specimed tarting Unified sniffing	, not starting up:	Add to Target 1	Add to Target 2
Delete Host ua: no scripts were specified tarting Unified sniffing andomizing 255 hosts for so canning the whole petmask	, not starting up: anning for 255 bosts	Add to Target 1	Add to Target 2

Step 8 – Now we have to choose the targets. In MITM, our target is the host machine, and the route will be the router address to forward the traffic. In an MITM attack, the attacker intercepts the network and sniffs the packets. So, we will add the victim as "target 1" and the router address as "target 2."

In VMware environment, the default gateway will always end with "2" because "1" is assigned to the physical machine.

Step 9 – In this scenario, our target is "192.168.121.129" and the router is "192.168.121.2". So we will add target 1 as **victim IP** and target 2 as **router IP**.

```
Host 192.168.121.129 added to TARGET1
Host 192.168.121.2 added to TARGET2
```

Step 10 – Now click on "MITM" and click "ARP poisoning". Thereafter, check the option "Sniff remote connections" and click OK.



Step 11 - Click "start" and select "start sniffing". This will start ARP poisoning in the network which means we have enabled our network card in "promiscuous mode" and now the local traffic can be sniffed.

Note – We have allowed only HTTP sniffing with Ettercap, so don't expect HTTPS packets to be sniffed with this process.

Step 12 - Now it's time to see the results; if our victim logged into some websites. You can see the results in the toolbar of Ettercap.

RESULT:

Thus, the above experiment with sniff traffic using ARP poisoning are executed successfully and output are verified.

DEMONSTRATE INTRUSION DETECTION SYSTEM USING ANY TOOL

AIM

To demonstrate intrusion detection system using any tool (SNORT).

PROCEDURE

In Windows:

- **Step-1:** Download SNORT installer from https://www.snort.org/downloads/snort/Snort_2_9_15_Installer.exe
- **Step-1:** Execute the Snort_2_9_15_Installer.exe

Different SNORT Modes:

1. Sniffer Mode –

```
ToprintTCP/IPheaderusecommand./snort-vTo print IP address along with header use command./snort -vd
```

2. Packet Logging -

To store packet in disk you need to give path where you want to store the logs. For this command is./snort -dev -l ./SnortLogs.

3. Activate network intrusion detection mode -

To start this mode use this command ./snort -dev -l ./SnortLogs -h 192.127.1.0/24 -c snort.conf

RESULT

Thus the above demonstrate intrusion system using SNORT are installed successfully and output are verified.

EXPLORE NETWORK MONITORING TOOL

PROCEDURE

1. Sematext Experience



Sematext Experience is a real user monitoring solution that offers **100%** visibility into your website or web app that affects your users' experience.

Here is what puts Sematext on the top of our list:

- Easy installation
- Single page application support
- Individual session performance
- Inspect Page load events
- Monitor your Apdex score
- Real-time automatic alerts

Sematext Experience allows you to inspect **individual sessions** to get **pagelevel specifics**. This helps assess the user's satisfaction to prevent customer loss due to poor performance. Furthermore, you can set up alerts for **Apdex score**, **script errors**, and **page load time** and receive **real-time notifications** whenever performance anomalies are detected. this, in turn, will enable you to troubleshoot issues faster.

SEMATEXT EXPERIENCE

Sematext Experience was designed so DevOps and BizOps can work together. Having easy access to all your actionable data provides your whole team with in-depth insights. With this data, effectual decisions can be made with ease to ensure your customers are always satisfied.

Pricing

• From \$9/mo

Pros

- Combine the power of metrics, logs, and end-user monitoring under one roof with Sematext Cloud
- First-class support for popular frontend frameworks such as React, Ember, and Angular
- URL grouping for both page-load events and HTTP requests
- Powerful cost control using data sampling
- Has a solution for synthetic monitoring
- Error tracking

2. Dynatrace RUM



Part of Dynatrace's digital experience monitoring toolset, Dynatrace RUM is a powerful website monitoring service that offers complete real-time visibility of customer experience. You can monitor the activity of all mobile and web application users across all devices and browsers to assess and improve user satisfaction.

With Dynatrace RUM you can also collect business-relevant metrics, allowing you to correlate performance issues with potential business impact.

Features

- Map the whole user journey
- Replay individual customer sessions
- Business-relevant, user transaction monitoring
- Real-time AI-based analysis

Pricing

• Available on request

Pros

- Intuitive non-technical dashboard usability
- Interactive interfaces and visual reports for ROI tracking

• Mobile monitoring breakdowns

Cons

- Reportedly pricey
- The UI can be overwhelming at first

3. AppDynamics Browser RUM



AppDynamics's RUM tool tracks customers' journey to provide full visibility into their interaction with your webapp. You receive browser-user insights to help you optimize web experiences. Self-learning algorithms use the app's behavior to dynamically baseline web metrics with automatic anomaly detection and resolution.

Features

- Real-time intelligent alerting
- Backend and frontend monitoring in same solution
- Business transaction correlation
- Browser snapshot waterfalls
- Dynamic performance baselining

Pricing

• Available in two options: Lite (free) version and Pro version. Pricing available on request

Pros

- Free training
- Self-learning platform

Cons

• Reportedly pricey



4. New Relic Browser

New Relic is mostly known for their APM tool, but they completed their monitoring tools set with a RUM solution, New Relic Browser.

New Relic Browser has advanced RUM features that give you access to insights from the users' perspective by focusing on browser performance. It monitors the entire life cycle of a page or a view, from the moment users enter the app until they disconnect.

Features

- Browser Pageviews and Page Load Times
- Java Errors and Instance details
- AJAX Timing and Call Reports
- Browser Session Traces
- Filterable Geography Analytics
- Route changes in apps with single page application (SPA) architecture
- Individual session performance

Pricing

• Pricing information available on request. Also has a free (Lite) version with fewer features

Pros

• Synthetic monitoring option available

Cons

- Most features are available for Pro accounts only
- Reports are not very comprehensive
- Missing detailed HTTP resources metrics

5. Pingdom

	s pingdom	 ⊘ Visitor Insights / MyWebsite ✓ 	📋 Last 1 hour 👻
₩	Experience Monitoring	Experience Performance All pages - All platform	ns v All browsers v All countries v
	Uptime Transactions Page Speed Visitor Insights (RUM) Maintenance	Image: Set store (now) Feb 20, 07:00 - Now (GMT+1) Set store (now) Image: Set store (now) 12 4.13 s 1 HOUR AGO CHANGE 38 > 0.00 %	BOUNCE RATE (NOW) ③ 54% 1 HOURADO 40% ★ 30.21%
Ĩ	Reports	✓ Load time by geography ⊙	
⊡	Sharing		
ሐ	Integrations		16.0
ନ୍ୟ	Users and teams		12.9
	Settings		84
ୟ	Support		3. 45
•0	Changelog		
		Platform Platfo	Sessions by geography 💿
6	Stove Johnson PROFESSIONAL OWNER		United states 1 011 • 0.14%

Pingdom is a unified performance monitoring tool that brings together transaction, uptime, and real user monitoring.

Pingdom allows you to filter data from specific users to get greater insights on the regional performance of your website and make optimizations to deliver a better experience to your most valuable users. It's highly scalable, allowing you to monitor millions of pageviews without compromising your data.

Features

- Tailored incident management
- Real-time data and alerting
- Website and server monitoring
- Mobile accessibility

Pricing

• The basic setup starts at 10/month, up to 199 - 15,000

Pros

- Customizable, fast and comprehensive alerting and reporting
- Synthetic and end user monitoring
- Notifications to multiple destinations (text message, email)

Cons

- Expensive if you increase volume or scale up as there is no data sampling available
- No error tracking or error management

RESULT:

Thus, the above process are explore network monitoring tools and view the output

AIM

To study to configure firewall, VPN using Google cloud services.

PROCEDURE

Google Cloud firewall rules

Google Cloud firewall rules apply to packets sent to and from virtual machine (VM) instances within your VPC network and through Cloud VPN tunnels.

Consolegcloud

- 1. In the Google Cloud console, go to the **VPN tunnels** page.
- 2. Go to VPN tunnels
- 3. Click the VPN tunnel that you want to use.
- 4. In the VPN gateway section, click the name of the VPC network. This action directs you to the VPC network details page that contains the tunnel.
- 5. Click the Firewall rules tab.
- 6. Click Add firewall rule. Add a rule for TCP, UDP, and ICMP:
 - **Name:** Enter allow-tcp-udp-icmp.
 - Source filter: Select IPv4 ranges.
 - Source IP ranges: Enter a Remote network IP range value from when you created the tunnel. If you have more than one peer network range, enter each one. Press the **Tab** key between entries. To allow traffic from all source IPv4 addresses in your peer network, specify 0.0.0.0/0.
 - **Specified protocols or ports:** Select tcp and udp.
 - **Other protocols:** Enter icmp.
 - **Target tags:** Add any valid tag or tags.
- 7. Click Create.

If you need to allow access to IPv6 addresses on your VPC network from your peer network, add an allow-ipv6-tcp-udp-icmpv6 firewall rule.

Click **Add firewall rule**. Add a rule for TCP, UDP, and ICMPv6:

- **Name:** Enter allow-ipv6-tcp-udp-icmpv6.
- Source filter: Select IPv6 ranges.
- Source IP ranges: Enter a Remote network IP range value from when you created the tunnel. If you have more than one peer network range, enter each one. Press the Tab key between entries. To allow traffic from all source IPv6 addresses in your peer network, specify ::/0.
- **Specified protocols or ports:** Select tcp and udp.
- Other protocols: Enter 58. 58 is the protocol number for ICMPv6.
- **Target tags:** Add any valid tag or tags.

Click Create.

CONCLUSION

The purpose of this study was to explore the role of the firewall in network security. This was done by researching five more specific problems. Two of them were concerned with the relationship between firewalls and network services, and it is in this area we believe this study makes its foremost contribution. With regard to the question about firewall configurations, our results are in line with findings from other studies, not least those by Wool. Realistically, we do not consider our results to be that revolutionary nor reliable. VPNs allow users or corporations to connect to remote servers, branch offices, or to other companies over a public internetwork, while maintaining secure communications. In all these cases, the secure connection appears to the a private network communication-despite the fact this user as that communication occurs over a public internetwork. VPN technology is designed to address issues surrounding the current business trend towards increased telecommuting and widely distributed global operations, where workers must be able to connect to central resources and communicate with each other.