EX.No:1	IMPLEMENTSYMMETRICKEYALGORITHMS

AIM:

TouseDataEncryptionStandard(DES)Algorithmforapracticalapplicationlike User MessageEncryption.

ALGORITHM:

1. CreateaDESKey.
2. CreateaCipherinstancefromCipherclass,specifythefollowing information and separated by aslash(/).
   a. Algorithmname
   b. Mode(optional)
   c. Paddingscheme(optional)
3. ConvertString into***Byte[]***arrayformat.
4. MakeCipherinencrypt mode,andencryptitwith ***Cipher.doFinal()*** method.
5. MakeCipherindecrypt mode,anddecryptitwith ***Cipher.doFinal()*** method.

PROGRAM:

DES.java

```
Importjava.security.InvalidKeyException;
importjava.security.NoSuchAlgorithmException;
importjavax.crypto.BadPaddingException;import
                                    javax.crypto.Cipher;
importjavax.crypto.IllegalBlockSizeException;
import                   javax.crypto.KeyGenerator;
importjavax.crypto.NoSuchPaddingException;
import javax.crypto.Secretey;
```

```
    publicclassDES
    {
        publicstaticvoidmain(String[]argv){
            try{
        System.out.println("MessageEncryptionUsingDESAlgorithm\n ---------- ");
                KeyGeneratorkeygenerator=KeyGenerator.getInstance("DES");Se
        cretKeymyDesKey=keygenerator.generateKey();
                CipherdesCipher;
                desCipher=Cipher.getInstance("DES/ECB/
                PKCS5Padding");desCipher.init(Cipher.ENCRYPT_MODE,myD
                esKey);byte[] text = "Secret Information
                ".getBytes();System.out.println("Message [Byte Format] : " +
                text);System.out.println("Message :"+new String(text));
                byte[] textEncrypted =
                desCipher.doFinal(text);System.out.println("EncryptedMessage:"
                +textEncrypted);desCipher.init(Cipher.DECRYPT_MODE,
                myDesKey);byte[]textDecrypted=desCipher.doFinal(textEncrypte
                d);
System.out.println("DecryptedMessage:"+newString(textDecrypted));
}catch(NoSuchAlgorithmExceptione){
    e.printStackTrace();
}catch(NoSuchPaddingExceptione){
    e.printStackTrace();
}catch(InvalidKeyExceptione){
    e.printStackTrace();
}catch(IllegalBlockSizeExceptione){
    e.printStackTrace();
}catch(BlockPaddingExceptione){
    e.printStackTrace();
}}}
```

OUTPUT:

```
MessageEncryptionUsingDESAlgorithm
__________________________________

Message[ByteFormat]:[B@4dcbadb4
Message:SecretInformation
EncryptedMessage:[B@504bae78
DecryptedMessage:SecretInformation
```

RESULT:

Thus the java program for DES Algorithm has been implemented andthe output verified successfully.

EX.No:2a	IMPLEMENTASYMMETRICKEYALGORITHMSANDKEY EXCHANGEALGORITHMS - RSAALGORITHM

AIM:

ToimplementRSA(Rivest–Shamir–Adleman)algorithmbyusingHTMLandJavascript.

ALGORITHM:

1. Choosetwoprimenumberpandq
2. Computethevalueofnandp
3. Findthevalueof***e***(publickey)
4. Computethevalueof***d***(privatekey)usinggcd()
5. Dotheencryptionanddecryption
    a. Encryptionisgivenas,

       $c=t^{e}modn$

    b. Decryptionisgivenas,

       $t=c^{d}modn$

PROGRAM:rsa.html

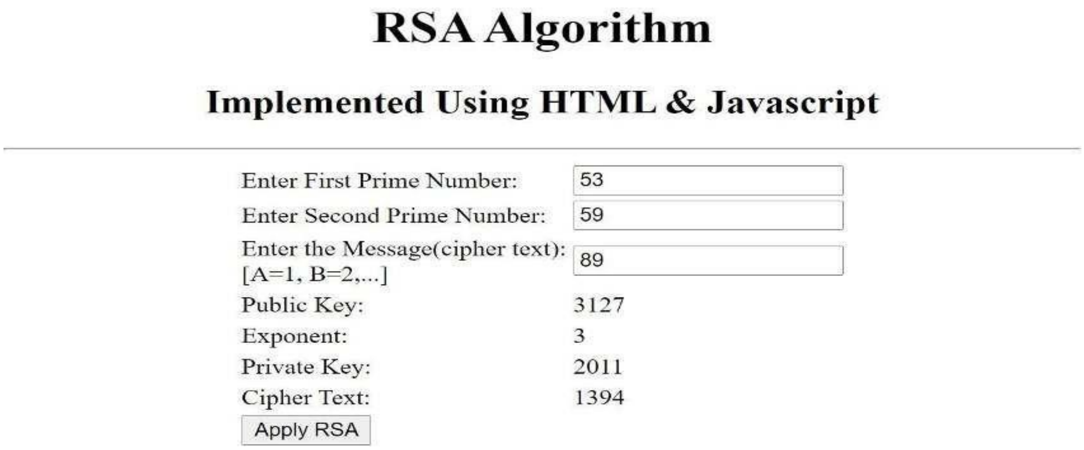
```
<html>
<head>
   <title>RSAEncryption</title>
   <metaname="viewport"content="width=device-width,initial-scale=1.0">
</head>

<body>
   <center>
      <h1>RSAAlgorithm</h1>
      <h2>ImplementedUsingHTML&Javascript</h2>
      <hr>
      <table>
```

```
<tr>
    <td>EnterFirstPrimeNumber:</td>
    <td><inputtype="number"value="53"id="p"></td>
</tr>
<tr>
    <td>EnterSecondPrimeNumber:</td>
    <td><inputtype="number"value="59"id="q"></p>
    </td>
</tr>
<tr>
    <td>EntertheMessage(ciphertext):<br>[A=1,B=2,...]</td>
    <td><inputtype="number"value="89"id="msg"></p>
    </td>
</tr>
<tr>
    <td>PublicKey:</td>
    <td>
        <pid="publickey"></p>
    </td>
</tr>
<tr>
    <td>Exponent:</td>
    <td>
        <pid="exponent"></p>
    </td>
</tr>
<tr>
    <td>PrivateKey:</td>
    <td>
        <pid="privatekey"></p>
```

```
                        </td>
                    </tr>
                    <tr>
                        <td>CipherText:</td>
                        <td>
                            <pid="ciphertext"></p>
                        </td>
                    </tr>
                    <tr>
                        <td><buttononclick="RSA();">ApplyRSA</button></td>
                        <\tr>
            <\table>
            </center>
        </body>
<scripttype="text/javascript">
functionRSA(){
vargcd,p,q,no,n,t,e,i,x;
gcd=function(a,b){return(!b)?a:gcd(b,a%b);}; p=
                        document.getElementById('p').value;
q=document.getElementById('q').value;
no=document.getElementById('msg').value;
n =p * q;
t=(p-1)* (q-1);
for(e=2;e<t;e++){
if(gcd(e,t)==1){
break;
}
}
for(i=0;i<10;i++){
x = 1 +i* t
if(x%e==0){ d =
x / e;
break;
}
}
ctt=Math.pow(no,e).toFixed(0);
ct =ctt% n;
dtt=Math.pow(ct,d).toFixed(0);
dt= dtt% n;
document.getElementById('publickey').innerHTML =
n;document.getElementById('exponent').innerHTML =
e;document.getElementById('privatekey').innerHTML=d;document.getElementById('ciph
ertext').innerHTML=ct;
}
</script>
</html>
```

OUTPUT:



RSA Algorithm

Implemented Using HTML & Javascript

Enter First Prime Number: 53
Enter Second Prime Number: 59
Enter the Message(cipher text): [A=1, B=2,...] 89
Public Key: 3127
Exponent: 3
Private Key: 2011
Cipher Text: 1394

RESULT:

Thus the RSA algorithm has been implemented using HTML&CSS and the output has been verified successfully.

EX.No:2b	IMPLEMENTASYMMETRICKEYALGORITHMSANDKEY EXCHANGE ALGORITHMS – DIFFIE-HELLMANKEYEXCHANGEALGORITHM

AIM:

ToimplementtheDiffie-HellmanKeyExchangealgorithmforagivenproblem.

ALGORITHM:

1. AliceandBobpubliclyagreetouseamodulus$p$=23andbase$g$=5(whichis aprimitiverootmodulo 23).
2. Alicechoosesasecretinteger$\boldsymbol{a}$=4,thensendsBob$A$=g^{a}mod$p$ o
   A=5^{4}mod 23=4
3. Bobchoosesasecretinteger$\boldsymbol{b}$=3,thensendsAlice$B$=g^{b}mod$p$
   - B=5^{3}mod23=10
4. Alicecomputes$\boldsymbol{s}$=B^{a}mod$p$
   - $\boldsymbol{s}$=10^{4}mod23=18
5. Bobcomputes$\boldsymbol{s}$=A^{b}mod$p$
   - $\boldsymbol{s}$=4^{3}mod23=18
6. AliceandBobnowshareasecret(thenumber18).

PROGRAM:DiffieHellman.java

```
classDiffieHellman{
   publicstaticvoidmain(Stringargs[]){
      intp=23;/*                    publiclyknown(prime
      number)*/intg=5;/*publiclyknown(primitiver
      oot)*/ intx=4;/*onlyAlice knowsthissecret*/
      int   y   =   3;   /*   only   Bob   knows   this   secret   */
      doublealiceSends            =(Math.pow(g,             x))%p;
      doublebobComputes=(Math.pow(aliceSends,y))%p;
      doublebobSends = (Math.pow(g,y)) %p;
```

```
        doublealiceComputes                    =(Math.pow(bobSends,x))%p;
        doublesharedSecret        =(Math.pow(g,(x*          y)))%          p;
        System.out.println("simulationofDiffie-Hellmankeyexchangealgorithm\
        n---------------- ");
        System.out.println("Alice     Sends     :     "     +     aliceSends);
        System.out.println("Bob          Computes          :          "          +
        bobComputes);System.out.println("Bob Sends : " + bobSends);
        System.out.println("AliceComputes:"+aliceComputes);System.out.println("S
        haredSecret :"+sharedSecret);
        /*sharedsecretsshould                    matchandequality                    istransitive*/
        if((aliceComputes==sharedSecret)&&(aliceComputes==bobCompute
          s))System.out.println("Success:SharedSecretsMatches!"+sharedSec
          ret);
        else
          System.out.println("Error:SharedSecretsdoesnotMatch");
      }}
```

OUTPUT:

```
SimulationofDiffie-Hellmankeyexchangealgorithm
--------------------------------------------------------------------------
AliceSends:4.0
BobComputes:18.0
BobSends:10.0
AliceComputes:18.0
SharedSecret :18.0
Success:SharedSecretsMatches!18.0
```

RESULT:

ThustheDiffie-Hellmankeyexchangealgorithmhasbeenimplementedusing Java Program and the output has been verified successfully.

EX.No:3	IMPLEMENTDIGITALSIGNATURESCHEMES

AIM:

ToimplementtheSIGNATURESCHEME-DigitalSignatureStandard.

ALGORITHM:

1. CreateaKeyPairGeneratorobject.
2. InitializetheKeyPairGeneratorobject.
3. GeneratetheKeyPairGenerator.
4. Gettheprivatekeyfromthepair.
5. Createasignatureobject.
6. InitializetheSignatureobject.
7. AdddatatotheSignatureobject.
8. CalculatetheSignature

PROGRAM:

```
importjava.security.KeyPair;
importjava.security.KeyPairGenerator;
importjava.security.PrivateKey;import
                java.security.Signature;
importjava.util.Scanner;
publicclassCreatingDigitalSignature{
publicstaticvoidmain(Stringargs[])throwsException{
Scannersc=newScanner(System.in);System.out.println("Entersome
text");Stringmsg =sc.nextLine();
    KeyPairGeneratorkeyPairGen=KeyPairGenerator.getInstance("DSA");keyPair
    Gen.initialize(2048);
    KeyPairpair=keyPairGen.generateKeyPair();
```

```
        PrivateKeyprivKey=pair.getPrivate();
        Signaturesign=Signature.getInstance("SHA256withDSA");sign.initSign(privK
        ey);
    byte[]bytes="msg".getBytes();
    sign.update(bytes);
    byte[]signature=sign.sign();
   System.out.println("Digital          signatureforgiventext:"+newString(signature,
"UTF8"));
    }
    }
```

OUTPUT:

```
Entersometext
Hihowareyou
Digitalsignatureforgiventext:0=@gRD???-?.????/yGL?i??a!?
```

RESULT:

Thusthe DigitalSignature Standard Signature Scheme hasbeenimplementedandthe output has been verified successfully

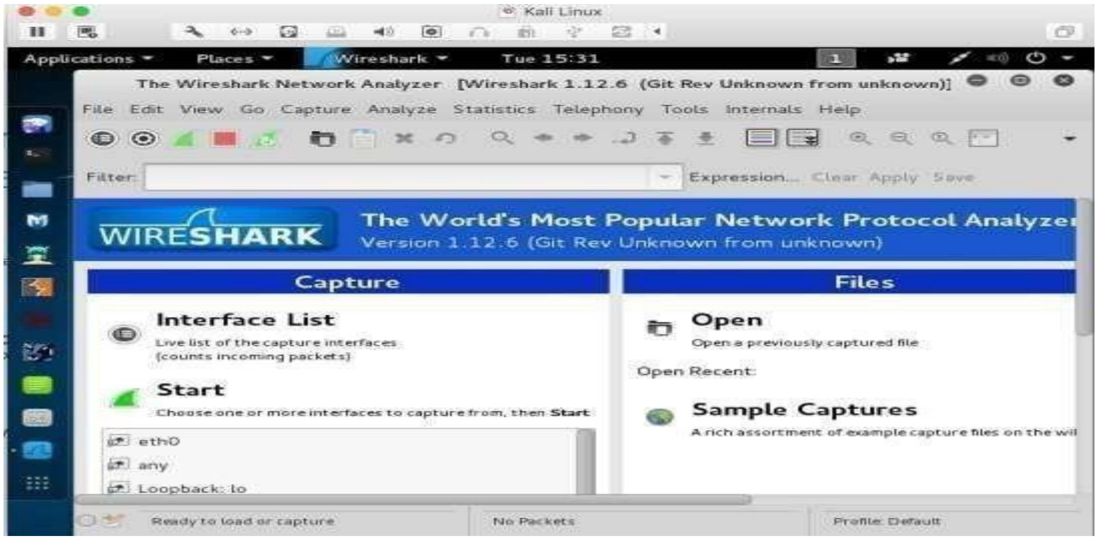
EX.No:4	INSTALLATION OF WIRE SHARK, TCPDUMP AND OBSERVE DATATRANSFERREDINCLIENT-SERVERCOMMUNICATION USINGUDP/TCPANDIDENTIFYTHEUDP/TCPDATAGRAM

AIM:

ToinstallationofWireshark,tcpdumpandobservedatatransferredinclient-servercommunicationusingUDP/TCP andidentifytheUDP/TCP datagram.

PROCEDURE:

The first part of the lab introduces packet sniffer, Wireshark. Wiresharkis a freeopen-source network protocol analyzer. It is used for network troubleshooting and communicationprotocol analysis. Wireshark captures network packets in real time and display them inhuman-readableformat.Itprovidesmanyadvancedfeaturesincludinglivecaptureandoffline analysis, three-pane packet browser, coloring rules for analysis. This document usesWireshark for the experiments, and it covers Wireshark installation, packet capturing, andprotocol analysis.



The Wireshark Network Analyzer [Wireshark 1.12.6 (Git Rev Unknown from unknown)]

The World's Most Popular Network Protocol Analyzer
Version 1.12.6 (Git Rev Unknown from unknown)

Interface List
Live list of the capture interfaces (counts incoming packets)

Start
Choose one or more interfaces to capture from, then Start

Open
Open a previously captured file

Open Recent:

Sample Captures
A rich assortment of example capture files on the wi

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

Figure1:WiresharkinKaliLinux

Background

TCP/IPNetworkStack

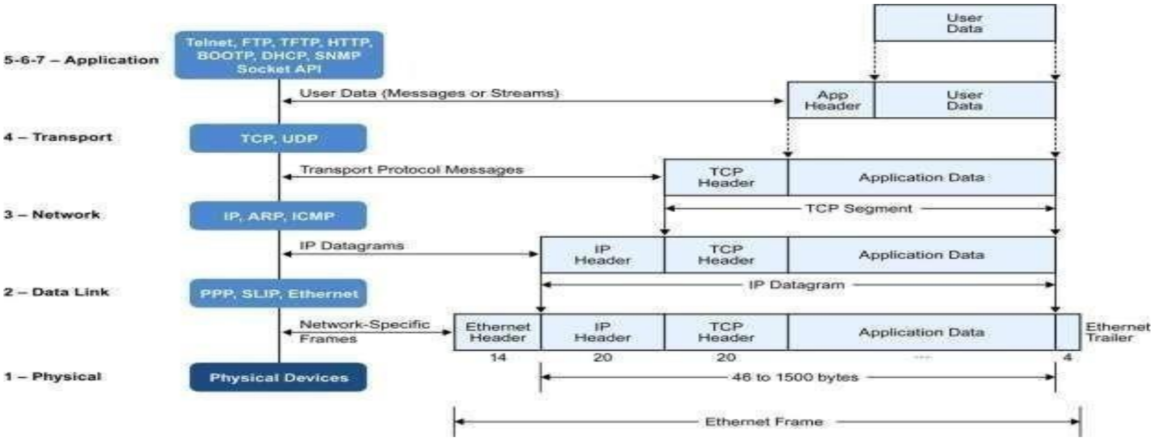
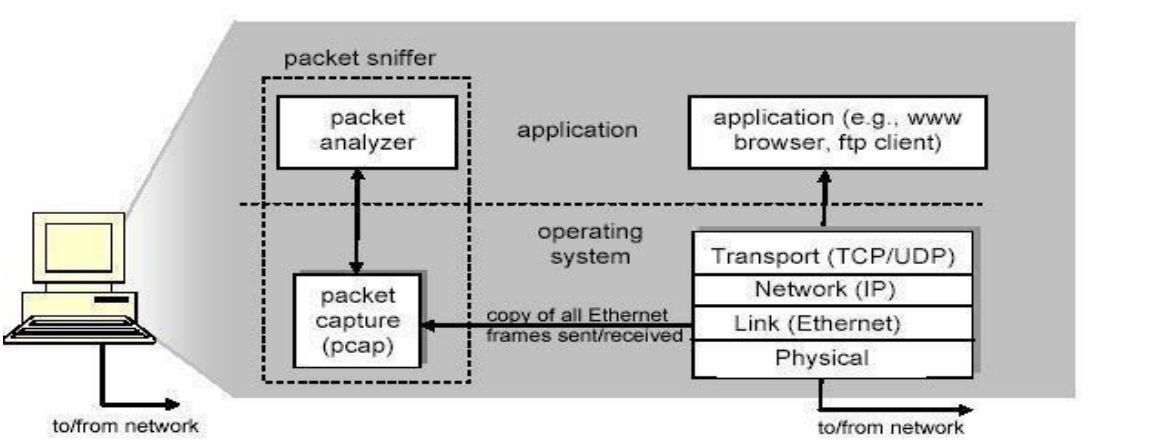


Figure2:EncapsulationofDataintheTCP/IPNetworkStack

PacketSniffer

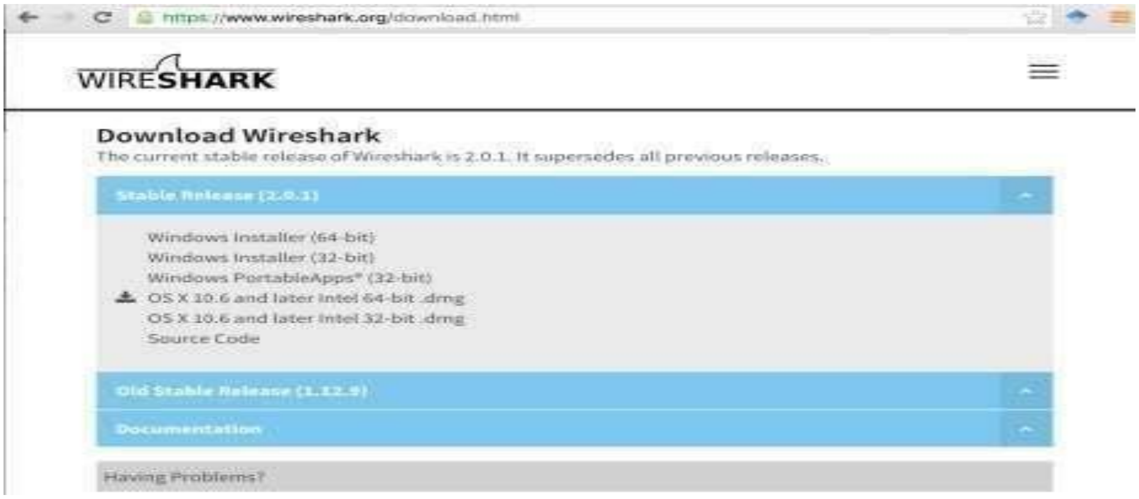
Packet sniffer is a basic tool for observing network packet exchangesin a computer.As thename suggests, a packet sniffer captures (“sniffs”) packets being sent/received from/by yourcomputer; it will also typically store and/or display the contents of the various protocol fields inthese captured packets. A packet sniffer itself is passive. It observes messages being sent andreceivedbyapplicationsandprotocolsrunning onyour computer,butneversends packetsitself.



GettingWireshark

TheKaiLinuxhasWiresharkinstalled.YoucanjustlaunchtheKaliLinuxVMandopenWiresharkt here.

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


https://www.wireshark.org/download.html
WIRESHARK
Stable Release (2.0.1)
Windows Installer (64-bit)
Windows Installer (32-bit)
Windows PortableApps® (32-bit)
OS X 10.6 and later Intel 64-bit .dmg
OS X 10.6 and later Intel 32-bit .dmg
Source Code
Old Stable Release (1.12.9)
Documentation
Having Problems?

Download Wireshark

The current stable release of Wireshark is 2.0.1. It supersedes all previous releases.

StartingWireshark:

WhenyouruntheWiresharkprogram,theWiresharkgraphicuserinterface

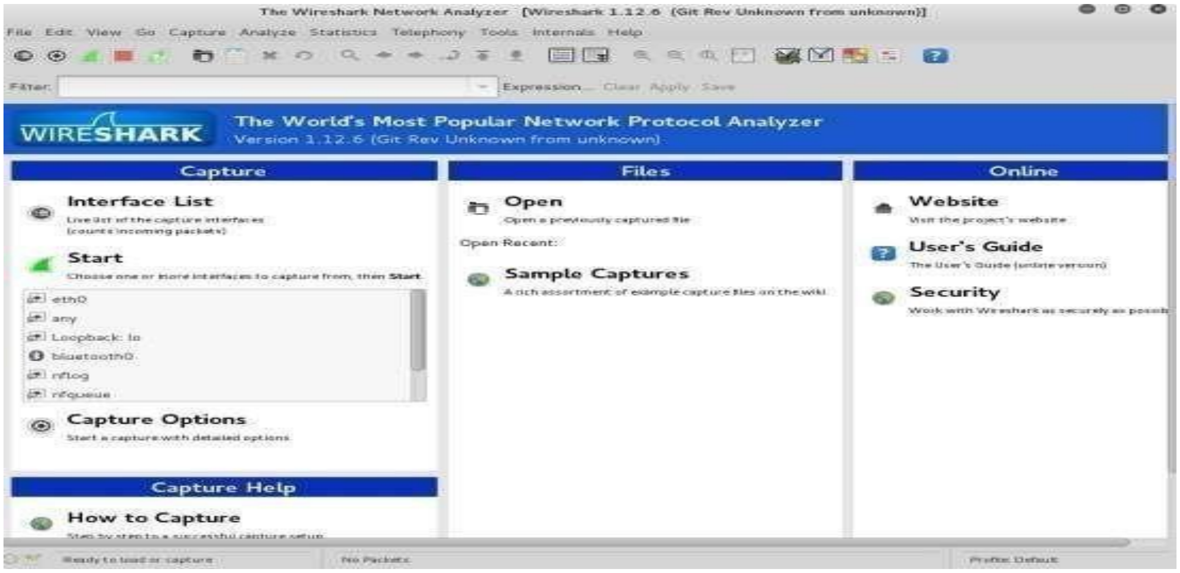
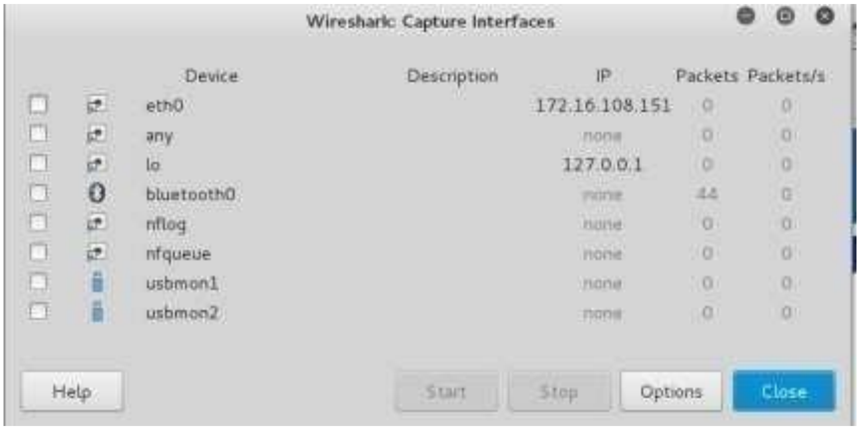

The Wireshark Network Analyzer [Wireshark 1.12.6 (Git Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.12.6 (Git Rev Unknown from unknown)
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
eth0
any
Loopback: lo
bluetooth0
nflog
nfqueue
Capture Options
Start a capture with detailed options
Capture Help
How to Capture
Step by step to a successful capture setup
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (online version)
Security
Work with Wireshark as securely as possib
Ready to load or capture
No Packets
Profile: Default

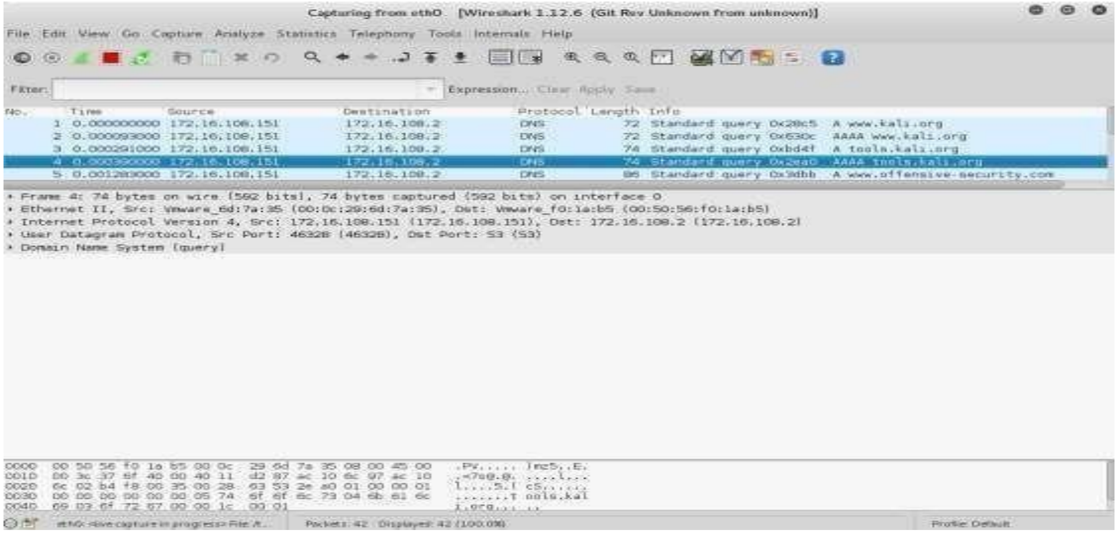
Figure: Currently,theprogramisnotcapturingthepackets

Then,youneedtochooseaninterface.IfyouarerunningtheWiresharkonyourlaptop, youneed to select WiFi interface. If you are at a desktop, you need to select the Ethernet interfacebeing used. Notethat there could bemultipleinterfaces. Ingeneral, you can select anyinterfacebutthatdoesnotmeanthattrafficwillflowthroughthatinterface.The network interfaces (i.e.,the physical connections) that your computer has to the networkare shown.



		Device	Description	IP	Packets	Packets/s
□		eth0		172.16.108.151	0	0
□		any		none	0	0
□		lo		127.0.0.1	0	0
□		bluetooth0		none	44	0
□		nflog		none	0	0
□		nfqueue		none	0	0
□		usbmon1		none	0	0
□		usbmon2		none	0	0

Afteryouselecttheinterface,youcanclickstarttocapturethepacketsasbelow.


Capturing from eth0 [Wireshark 1.12.6 (Git Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.   Time         Source           Destination     Protocol Length Info
    1 0.000000000  172.16.108.151   172.16.108.2    DNS          72 Standard query 0x28c5  A www.kali.org
    2 0.000093000  172.16.108.151   172.16.108.2    DNS          72 Standard query 0x630c  AAAA www.kali.org
    3 0.000291000  172.16.108.151   172.16.108.2    DNS          74 Standard query 0xbd4f  A tools.kali.org
    4 0.000390000  172.16.108.151   172.16.108.2    DNS          74 Standard query 0x2ea0  AAAA tools.kali.org
    5 0.001283000  172.16.108.151   172.16.108.2    DNS          86 Standard query 0x3dbb  A www.offensive-security.com

▸ Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▸ Ethernet II, Src: Vmware_6d:7a:35 (00:0c:29:6d:7a:35), Dst: Vmware_f0:1a:b5 (00:50:56:f0:1a:b5)
▸ Internet Protocol Version 4, Src: 172.16.108.151 (172.16.108.151), Dst: 172.16.108.2 (172.16.108.2)
▸ User Datagram Protocol, Src Port: 46328 (46328), Dst Port: 53 (53)
▸ Domain Name System (query)

0000  00 50 56 f0 1a b5 00 0c  29 6d 7a 35 08 00 45 00   .PV..... )mz5..E.
0010  00 3c 37 6f 40 00 40 11  d2 87 ac 10 6c 97 ac 10   .<7o@.@. ....l...
0020  6c 02 b4 f8 00 35 00 28  63 53 2e a0 01 00 00 01   l....5.( cS......
0030  00 00 00 00 00 00 05 74  6f 6f 6c 73 04 6b 61 6c   .......t ools.kal
0040  69 03 6f 72 67 00 00 1c  00 01                     i.org.... ..

eth0: <live capture in progress> File: /t...   Packets: 42 · Displayed: 42 (100.0%)   Profile: Default
```

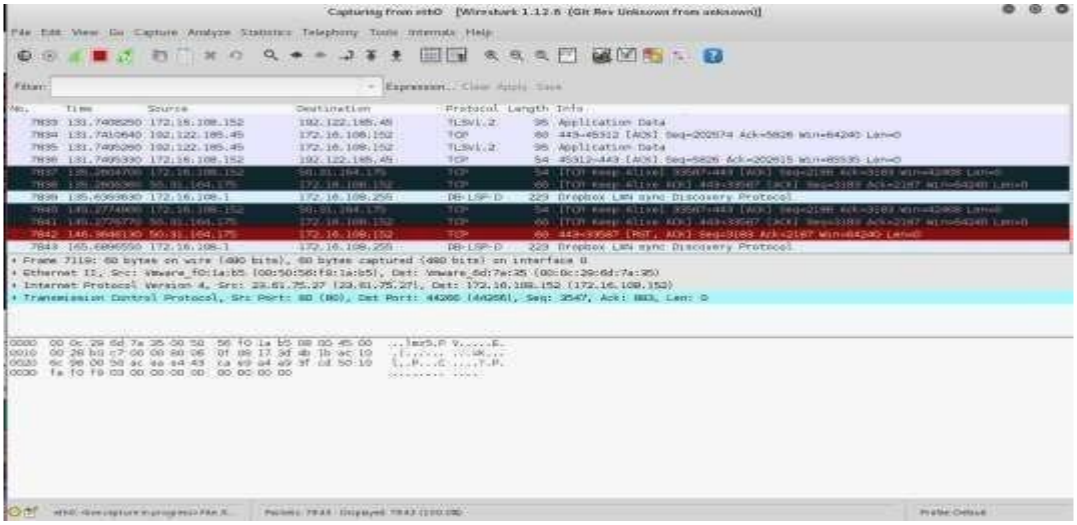
CapturingPackets

After downloading and installing Wireshark, you can launch it and click the name of an interfaceunder Interface List to start capturing packets on that interface. For example, if you want tocapture trafficonthewirelessnetwork,click yourwirelessinterface.

TestRun

Dothefollowingsteps:

1. StartuptheWiresharkprogram(selectaninterfaceandpressstarttocapturepackets).
2. Startupyourfavouritebrowser(ceweaselinKaliLinux).
3. Inyourbrowser,goto WayneStatehomepagebytypingwww.wayne.edu.
4. After your browser has displayed the http://www.wayne.edupage, stopWireshark packet capture by selecting stop in the Wireshark capture window. This will cause the Wireshark capture window to disappearand the main Wireshark window to display all packets captured since you began packet capture see image below:



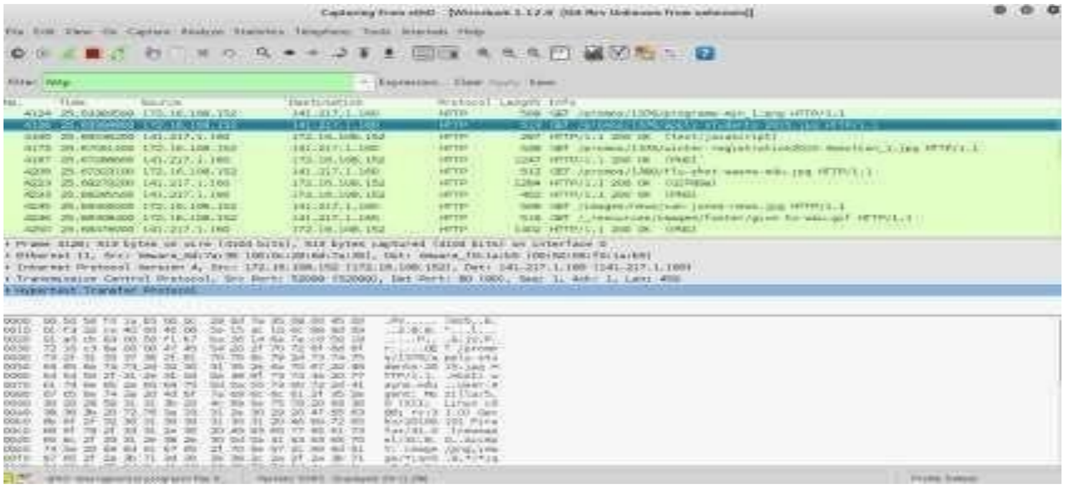
Capturing from eth0 [Wireshark 1.12.6 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.    Time         Source           Destination      Protocol  Length Info
 7833  131.7408250  172.16.108.152   192.122.185.45   TLSv1.2      95  Application Data
 7834  131.7410640  192.122.185.45   172.16.108.152   TCP          60  443→45312 [ACK] Seq=202574 Ack=5826 Win=64240 Len=0
 7835  131.7495260  192.122.185.45   172.16.108.152   TLSv1.2      95  Application Data
 7836  131.7495330  172.16.108.152   192.122.185.45   TCP          54  45312→443 [ACK] Seq=5826 Ack=202615 Win=65535 Len=0
 7837  135.2604700  172.16.108.152   50.31.164.175    TCP          54  [TCP Keep-Alive] 33567→443 [ACK] Seq=2186 Ack=3183 Win=42808 Len=0
 7838  135.2606380  50.31.164.175    172.16.108.152   TCP          60  [TCP Keep-Alive ACK] 443→33567 [ACK] Seq=3183 Ack=2187 Win=64240 Len=0
 7839  135.6369830  172.16.108.1     172.16.108.255   DB-LSP-D    229  Dropbox LAN sync Discovery Protocol
 7840  145.2774800  172.16.108.152   50.31.164.175    TCP          54  [TCP Keep-Alive] 33567→443 [ACK] Seq=2186 Ack=3183 Win=42808 Len=0
 7841  145.2776770  50.31.164.175    172.16.108.152   TCP          60  [TCP Keep-Alive ACK] 443→33567 [ACK] Seq=3183 Ack=2187 Win=64240 Len=0
 7842  146.3846130  50.31.164.175    172.16.108.152   TCP          60  443→33567 [RST, ACK] Seq=3183 Ack=2187 Win=64240 Len=0
 7843  165.6896550  172.16.108.1     172.16.108.255   DB-LSP-D    229  Dropbox LAN sync Discovery Protocol
▸ Frame 7119: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: Vmware_f0:1a:b5 (00:50:56:f0:1a:b5), Dst: Vmware_6d:7a:35 (00:0c:29:6d:7a:35)
▸ Internet Protocol Version 4, Src: 23.61.75.27 (23.61.75.27), Dst: 172.16.108.152 (172.16.108.152)
▸ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 44266 (44266), Seq: 3547, Ack: 883, Len: 0

0000  00 0c 29 6d 7a 35 00 50  56 f0 1a b5 08 00 45 00   ..)mz5.P V.....E.
0010  00 28 b3 c7 00 00 80 06  0f 08 17 3d 4b 1b ac 10   .(...... ...=K...
0020  6c 98 00 50 ac ea a4 43  ca e9 a4 a9 3f cd 50 10   l..P...C ....?.P.
0030  fa f0 f9 03 00 00 00 00  00 00 00 00               ........ ....
```

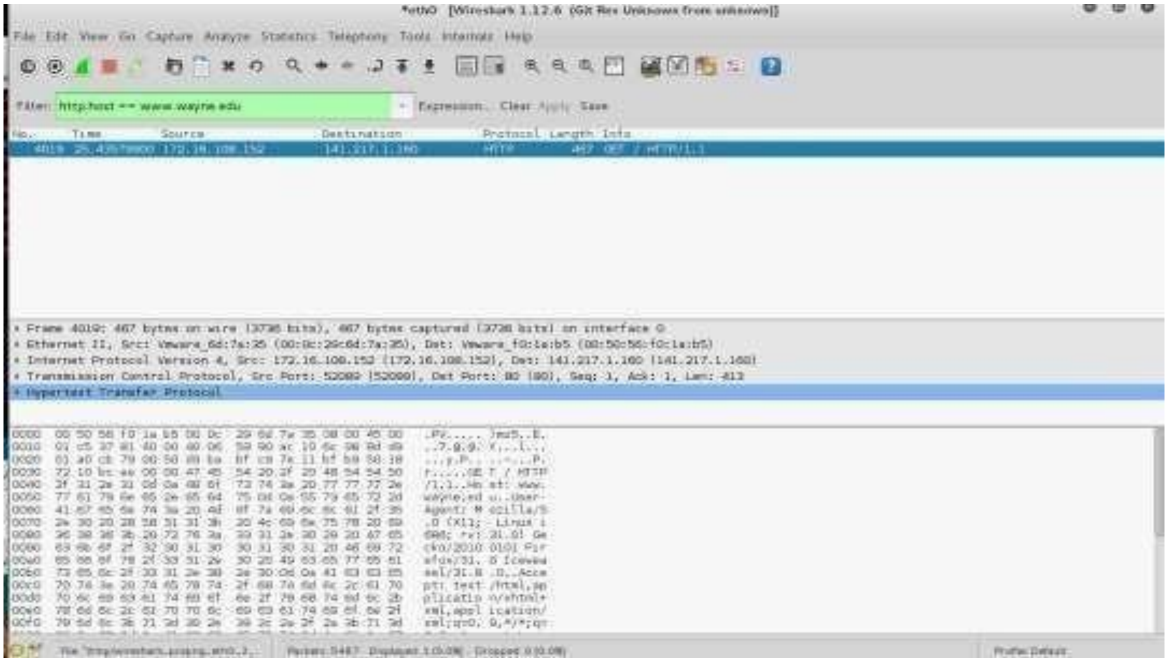
eth0: <live capture in progress> File: ... Packets: 7843 · Displayed: 7843 (100.0%) Profile: Default



Capturing from eth0 [Wireshark 1.12.6 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http
Expression... Clear Apply Save

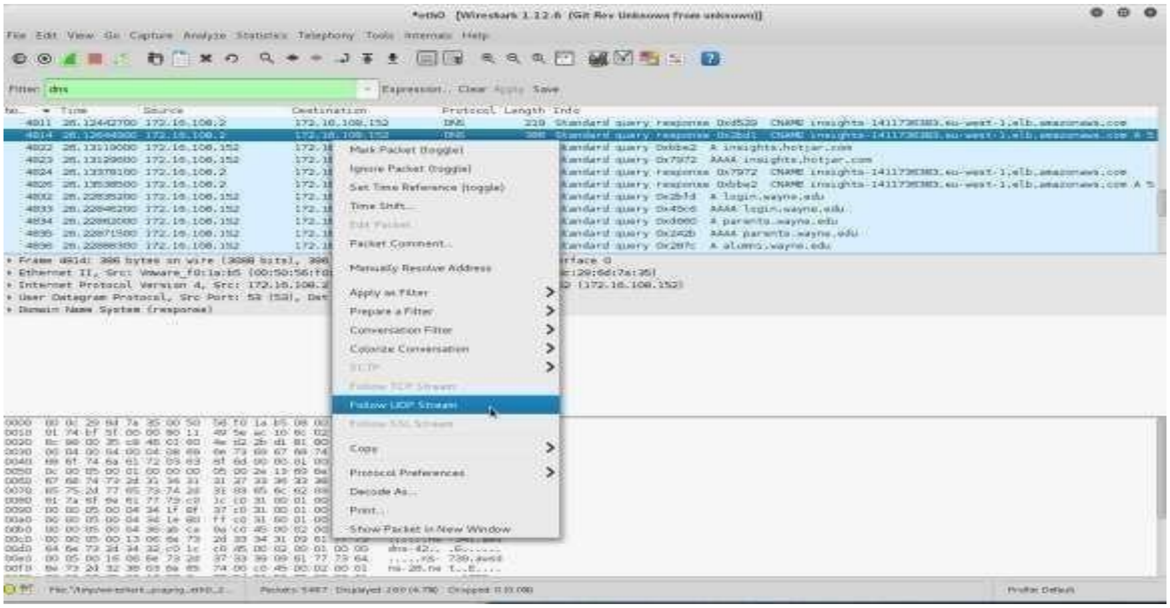
```
No.    Time         Source           Destination      Protocol  Length Info
 4124  25.53380500  172.16.108.152   141.217.1.160    HTTP        566  GET [illegible] HTTP/1.1
 4126  25.[illegible]  172.16.108.152   141.217.1.160    HTTP        [illegible]  GET [illegible] HTTP/1.1
 4165  25.[illegible]  141.217.1.160    172.16.108.152   HTTP        [illegible]  HTTP/1.1 200 OK  (text/javascript)
 4175  25.[illegible]  172.16.108.152   141.217.1.160    HTTP        [illegible]  GET [illegible].jpg HTTP/1.1
 4187  25.[illegible]  141.217.1.160    172.16.108.152   HTTP        [illegible]  HTTP/1.1 200 OK  (PNG)
 4209  25.[illegible]  172.16.108.152   141.217.1.160    HTTP         512  GET [illegible].jpg HTTP/1.1
 4223  25.[illegible]  141.217.1.160    172.16.108.152   HTTP        [illegible]  HTTP/1.1 200 OK  [illegible]
 4243  25.[illegible]  141.217.1.160    172.16.108.152   HTTP        [illegible]  HTTP/1.1 200 OK  (PNG)
 4245  25.[illegible]  172.16.108.152   141.217.1.160    HTTP        [illegible]  GET [illegible].jpg HTTP/1.1
 4246  25.[illegible]  172.16.108.152   141.217.1.160    HTTP        [illegible]  GET /_resources/images/footer/[illegible].gif HTTP/1.1
 4250  25.[illegible]  141.217.1.160    172.16.108.152   HTTP        [illegible]  HTTP/1.1 200 OK  (GIF)
▸ Frame 4126: 512 bytes on wire (4096 bits), 512 bytes captured (4096 bits) on interface 0
▸ Ethernet II, Src: Vmware_6d:7a:35 (00:0c:29:6d:7a:35), Dst: Vmware_f0:1a:b5 (00:50:56:f0:1a:b5)
▸ Internet Protocol Version 4, Src: 172.16.108.152 (172.16.108.152), Dst: 141.217.1.160 (141.217.1.160)
▸ Transmission Control Protocol, Src Port: 52000 (52000), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 458
▸ Hypertext Transfer Protocol
```


*eth0 [Wireshark 1.12.6 (Git Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http.host == www.wayne.edu
Expression... Clear Apply Save

```
No.    Time          Source            Destination       Protocol Length Info
  4019 25.43579000  172.16.108.152    141.217.1.160     HTTP      467  GET / HTTP/1.1

▸ Frame 4019: 467 bytes on wire (3736 bits), 467 bytes captured (3736 bits) on interface 0
▸ Ethernet II, Src: Vmware_6d:7a:35 (00:0c:29:6d:7a:35), Dst: Vmware_f0:1a:b5 (00:50:56:f0:1a:b5)
▸ Internet Protocol Version 4, Src: 172.16.108.152 (172.16.108.152), Dst: 141.217.1.160 (141.217.1.160)
▸ Transmission Control Protocol, Src Port: 52089 (52089), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 413
▸ Hypertext Transfer Protocol

0000  00 50 56 f0 1a b5 00 0c  29 6d 7a 35 08 00 45 00   .PV..... )mz5..E.
0010  01 c5 37 81 40 00 40 06  59 90 ac 10 6c 98 8d d9   ..7.@.@. Y...l...
0020  01 a0 cb 79 00 50 88 ba  bf c8 7e 11 bf b9 50 18   ...y.P.. ..~...P.
0030  72 10 bc ee 00 00 47 45  54 20 2f 20 48 54 54 50   r.....GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1..Ho st: www.
0050  77 61 79 6e 65 2e 65 64  75 0d 0a 55 73 65 72 2d   wayne.ed u..User-
0060  41 67 65 6e 74 3a 20 4d  6f 7a 69 6c 6c 61 2f 35   Agent: M ozilla/5
0070  2e 30 20 28 58 31 31 3b  20 4c 69 6e 75 78 20 69   .0 (X11;  Linux i
0080  36 38 36 3b 20 72 76 3a  33 31 2e 30 29 20 47 65   686; rv: 31.0) Ge
0090  63 6b 6f 2f 32 30 31 30  30 31 30 31 20 46 69 72   cko/2010 0101 Fir
00a0  65 66 6f 78 2f 33 31 2e  30 20 49 63 65 77 65 61   efox/31. 0 Icewea
00b0  73 65 6c 2f 33 31 2e 38  2e 30 0d 0a 41 63 63 65   sel/31.8 .0..Acce
00c0  70 74 3a 20 74 65 78 74  2f 68 74 6d 6c 2c 61 70   pt: text /html,ap
00d0  70 6c 69 63 61 74 69 6f  6e 2f 78 68 74 6d 6c 2b   plicatio n/xhtml+
00e0  78 6d 6c 2c 61 70 70 6c  69 63 61 74 69 6f 6e 2f   xml,appl ication/
00f0  78 6d 6c 3b 71 3d 30 2e  39 2c 2a 2f 2a 3b 71 3d   xml;q=0. 9,*/*;q=
```



```
No.  ▾ Time          Source            Destination       Protocol Length Info
  4811 26.12442700  172.16.108.2      172.16.108.152    DNS       219  Standard query response 0xd529  CNAME insights-1411736383.eu-west-1.elb.amazonaws.com
  4814 26.12644300  172.16.108.2      172.16.108.152    DNS       386  Standard query response 0x2bd1  CNAME insights-1411736383.eu-west-1.elb.amazonaws.com A 5
  4822 26.13119000  172.16.108.152    172.1            Standard query 0xbbe2  A insights.hotjar.com
  4823 26.13129600  172.16.108.152    172.1            Standard query 0x7972  AAAA insights.hotjar.com
  4824 26.13378100  172.16.108.2      172.1            Standard query response 0x7972  CNAME insights-1411736383.eu-west-1.elb.amazonaws.com
  4826 26.13538500  172.16.108.2      172.1            Standard query response 0xbbe2  CNAME insights-1411736383.eu-west-1.elb.amazonaws.com A 5
  4832 26.22835200  172.16.108.152    172.1            Standard query 0x2b7d  A login.wayne.edu
  4833 26.22846200  172.16.108.152    172.1            Standard query 0x45c6  AAAA login.wayne.edu
  4834 26.22862000  172.16.108.152    172.1            Standard query 0xd060  A parents.wayne.edu
  4835 26.22871500  172.16.108.152    172.1            Standard query 0x242b  AAAA parents.wayne.edu
  4836 26.22886300  172.16.108.152    172.1            Standard query 0x287c  A alumni.wayne.edu
▸ Frame 4814: 386 bytes on wire (3088 bits), 386                          rface 0
▸ Ethernet II, Src: Vmware_f0:1a:b5 (00:50:56:f0                          c:29:6d:7a:35)
▸ Internet Protocol Version 4, Src: 172.16.108.2                          2 (172.16.108.152)
▸ User Datagram Protocol, Src Port: 53 (53), Dst
▸ Domain Name System (response)
```

RESULT:

Installation of Wireshark, tcpdump and observe datatransfer redinclient-server communication using UDP/TCP and identify the UDP/TCP datagram.

EX.No:5	**CHECKMESSAGEINTEGRITYAND CONFIDENTIALITYUSINGSSL**

AIM:

TochecktheMessageIntegrityandConfidentiality usingSSL.

PROCEDURE:

SSLSessioninDetails

Handshaking-Cipher suit Negotiation

ClientsendsaplaintextClient_Hellomessageandsuggestssomecryptographicparameters(collectivelycalledciphersuit)tobeusedfortheircommunicationsession.TheClient_Hellomessagealsocontainsa 32-byterandom numberdenoted asclient_random.Forexample,.

Client_Hello:

ProtocolVersion:TLSv1ifyoucan,elseSSLv3.

KeyExchange:RSAifyoucan,elseDiffe-Hellman.

SecretKeyCipherMethod:3DESifyoucan,elseDES.

Message Digest:SHA-1ifyoucan,elseMD5.

DataCompressionMethod:PKZipifyoucan,elsegzip.

Client RandomNumber:32bytes

The stronger method (in terms of security) shall precede the weaker one, e.g. RSA (1024-bit)precedesDH,3DESprecedesDES,SHA-1 (160-bit)precedesMD5 (128-bit).

Server responds with a plaintext Server_Hello to state the ciphersuit of choice (server decidesontheciphersuit).Themessagealsocontainsa32-byte random number denote d as server_random.

Forexample,

Server_Hello:

ProtocolVersion:TLSv1

KeyExchange:RSA.

SecretKeyCipherMethod:DES.

Message Digest:SHA-1

DataCompressionMethod:PKZip.

ServerRandomNumber:32bytes

Handshaking-KeyExchange

The server sends its digital certificate to the client, which is supposedly signed by a root CA. Theclient uses the root CA'spublic key to verify the server's certificate (trusted root-CAs' public keyare pre-installed inside the browser). It then retrieves the server's public key from the server'scertificate.(If the server'scertificateis signed by a sub-CA,the clienthas to build a digitalcertificate chain, leadingtoatrustedroot CA,toverifythe server'scertificate.)
ThenextstepistoestablishtheSessionKey:

1. The client generates a 48-byte (384-bit) random number called pre_master_secret, encryptsitusingthe verifiedserver'spublickeyandsends itto theserver.

2. Server decrypts the pre_master_secret using its own private key. Eavesdroppers cannotdecrypt thepre_master_secret,astheydonotpossesstheserver'sprivate key.

3. Client and serverthen independently and simultaneously create the sessionkey,based onthe pre_master_secret, client_random and server_random. Notice that both the server andclient contribute to the session key,through the inclusion of the random number exchangein the hello messages. Eavesdroppers can intercept client_random and server_random astheyare sentin plaintext,butcannotdecrypt thepre_master_secret.

4. InaSSL/TLSsession,thesessionkeyconsistsof6secretkeys(tothwartcrypto-analysis).3 secretkeysareusedforclient-to-servermessages,andtheother3secretkeysareused forserver-to-clientmessages.Amongthe3secretkeys,oneisusedforencryption(e.g.,

DESsecret key), one is used for message integrity (e.g., HMAC) and one is used for cipherinitialization.(Cipherinitializationuses arandomplaintextcalled InitialVector (IV) toprime thecipherpump.)

5. Client and server use the pre_master_secret (48-byte random number created by the clientandexchangesecurely),client_random,server_random,andapseudo-randomfunction(PRF)togenerateamaster_secret.Theycanusethemaster_secret,client_random,server_random,andthepseudo-randomfunction(PRF)togenerateallthe6shared secretkeys. Once the secret keys are generated, the pre_master_secret is no longer needed andshould bedeleted.
6. Fromthispointonwards,alltheexchangesareencryptedusingthesessionkey.
7. The client sends Finished handshake message using their newly created session key. Serverrespondswith aFinishedhandshakemessage.

MessageExchange

Clientandservercanusetheagreed-uponsessionkey(consistsof6secretkeys)forsecureexchange of messages

Sendingmessages:

1. Thesendercompressesthemessageusingtheagreed uponcompression method(e.g.,PKZip,gzip).
2. ThesenderhashesthecompresseddataandthesecretHMACkeytomakean HMAC, to assur e message integrity.
3. The sender encrypts the compressed data and HMAC using encryption/decryption secret key, to assure message confidentiality.

ASSLSessionTrace

WecoulduseOpenSSL'ss_client(withdebugoption)toproduceaSSLsessiontrace

> **openssls_client?**

(Displaytheavailableoptions)

ThefollowingcommandturnsonthedebugoptionandforcestheprotocoltobeTLSv1:

- **openssls_client-connectlocalhost:443-CAfileca.crt-debug-tls1**

Loading'screen'intorandomstate–done

```
CONNECTED(00000760)
writeto00988EB0[009952C8](102bytes=>102 (0x66))
0000-16 03 01 00 61 01 0000-5d03 01 40 44 35 27 5c....a...]..@D5'\
0010-5ae87426e94937 e2-063b1c6d7737d1aeZ.t&.I7..;.mw7..
0020-44 07 86 4798 fa84 1a-8df472 00 00 3600 39D..G............................. r..6.9
0030-00 38 00 35 00 1600 13-00 0a00 33 00 3200 2f.8.5.......3.2./
0040-00 07 00 66 0005 0004-00 63 00 6200 61 00 15...f.....c.b.a..
0050-00 12 00 09 00 65 00 64-0060 00 14 00 11 00 08.....e.d.`......
0060-00 06 00 03 01                                    .....
0066-<SPACES/NULS>

readfrom00988EB0[00990AB8](5bytes=>5(0x5))
0000 - 16 03 01 00 2a                *
```

TraceAnalysis

Thedatatobetransmittedisbrokenupintoseriesoffragments.Eachfragmentis protected forintegrityusingHMAC.

EachSSLrecordbeginswith a5-byteheader:

Byte0:RecordContentType.FourContentTypes aredefined,asfollows:

ContentType	**HexCode**	**Description**
Handshake	0x16	Therecordcarriesahandshaking
messageApplication_Data	0x17	EncryptedApplicationData
Change_Cipher_Spec0x14		Toindicateachangeinencryptionmethods.
Alert	0x15	Tosignalvarioustypesoferrors

Byte1&2:SSLversion(0x0301forTLSv1,0x0300forSSLv3).

Byte3&4:Therecord length,excluding the5-byte header.

Client_Hello

Thefirsthandshakemessageisalwayssentbytheclient,calledclient_hellomessage.Inthismessage, the client tells the server its preferences in terms of protocol version, ciphersuit, andcompression method. The client also includes a 32-byte random number (client_random) in themessage, which is made up of a 4-byte GMT Unix time (seconds since 1970), plus another 28randombytes.

Server_Hello

In response to the client_hellomessage, the server returns a server_hellomessage to telltheclientitschoiceofprotocolversion,ciphersuitandcompressionmethod.Theserveralsoincludes a32-byterandomnumber(server_random) inthemessage.

Certificate

The certificate message consists of a chain of X.509 certificates in the correct order. The firstcertificate belongs to the server, and the next certificate contains the key that certifies the firstcertificate (i.e., the server's certificate), and so on. The client uses theserver's public key (containedinsidetheserver'scertificate)toeitherencryptthepre_master_secretorverifytheserver_key_exchange, dependingonwhichciphersuitis used.

Server_Key_Exchange

Server_Hello_Done

This is an empty message indicating thatthe server has sent all the handshaking messages. This isneededbecausethe servercansendsomeoptionalmessagesafter thecertificatemessage

Client_Key_Exchange

The client_key_exchange message contains the pre_master_secret when RSA key exchangeis used. The pre_master_secret is 48-byte, consists of protocol version (2 bytes) and 46 randombytes.

Certificate_Verify

Change_Cipher_Spec

UnknownHandshakingMessage(D4)-tocheck

Application_Data

Client-to-Server-theHTTPrequestmessage:GET/test.htmlHTTP/1.0

Server-to-Client -theHTTPresponsemessage

RESULT:

ThustheconfidentialityandIntegrityusingSSLwasverified.

EX.No:6	EXPERIMENTEAVESDROPPING,DICTIONARY ATTACKS,MITMATTACKS

AIM:

Toexperimenteavesdropping,Dictionaryattacks,MITMattacks.

PROCEDURE:

Password cracking is a term used to describe the penetration of a network, system, or resourcewith or without the use of tools to unlock a resource that has been secured with a password.Password cracking tools may seem like powerful decryptors, but in reality are little more thanfast,sophisticatedguessingmachines.

Typesofpasswordbreaking

Dictionaryattack

Asimple*dictionary*attackisusuallythefastestwaytobreakintoamachine.Adictionaryfile(atext file full of dictionary words) is loaded into a cracking application, which is runagainst useraccountslocatedby theapplication

Bruteforceattack

A*bruteforce*attackisaverypowerfulformofattack, thoughitmayoftentakealongtime towork depending on the complexity of the password. The program will begin trying any andeverycombinationofnumbers andlettersandrunning them againstthehashedpasswords.

Hybridattack

Another well-known form of attack is the *hybrid* attack. A hybrid attack will add numbers orsymbols to the search words to successfully crack a password. Many people change theirpasswordsbysimplyaddinganumber tothe endoftheir currentpassword.Therefore, thistype of attack is the most versatile, while it takes longer then a standard dictionary attack itdoesnottakeas long as a bruteforceattack.

Task1–MicrosoftOfficePasswordRecovery

Manyapplicationsrequireyoutoestablishan IDandpasswordthatmaybesavedandautomatically substituted for future authentication. The password will usually appear on thescreen as a series of asterisks. This is fine as long as your system remembers the password foryou but what if it "forgets" or you need it for use on another system. Fortunately, many utilitieshave been written to recover such passwords. In this task, you will use OfficeKey to recover thepasswordforaMSword document.

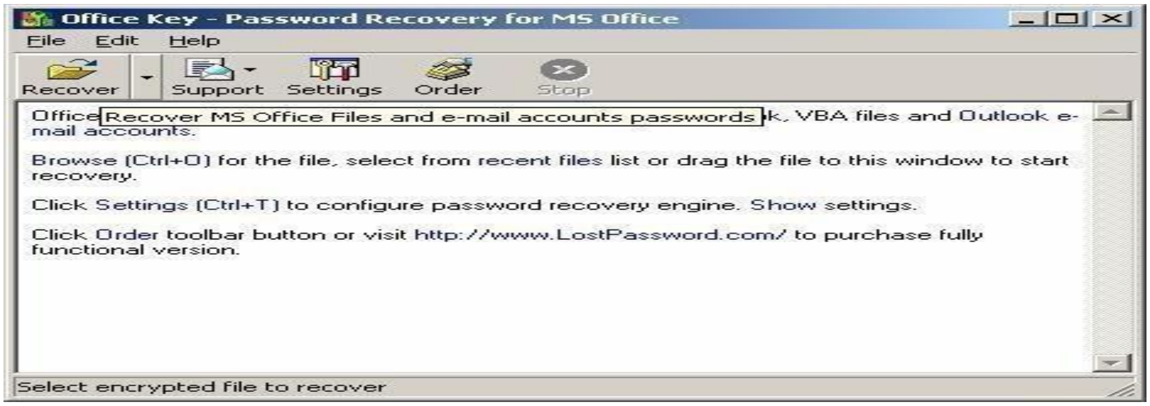
Step1: Findthefolder“Lab1”onyourdesktop,andopenit.

YouwillfindOfficeKeyandaMSdocumentin thefolder.

Step2: Openthe OfficeKey–PasswordRecoverytool

Step3: Pressthe“Recover”buttonintheupperleftcorner,orselectFileRecover

Step4: ChoosethepasswordprotectedMSOfficeFileyouhavesavedtotheDesktop.


Office Key - Password Recovery for MS Office
File
Edit
Help
Recover
Support
Settings
Order
Stop
Recover MS Office Files and e-mail accounts passwords

Office Recover MS Office Files and e-mail accounts passwords k, VBA files and Outlook e-mail accounts.

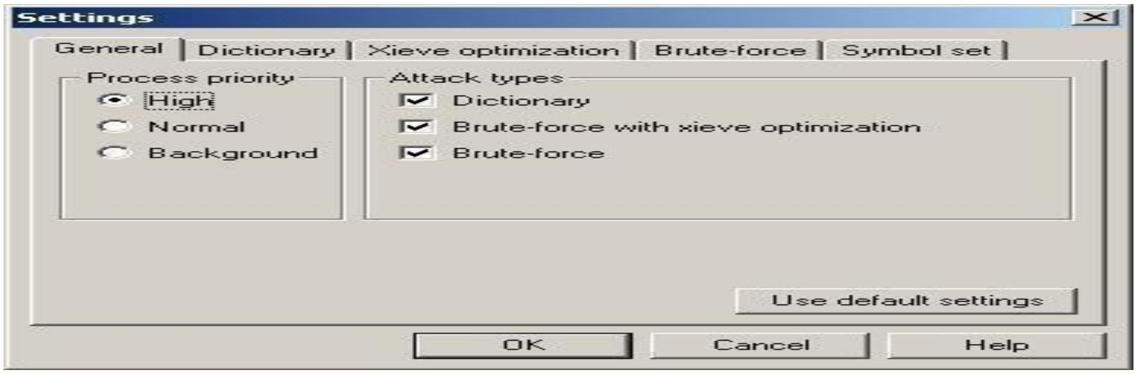
Browse (Ctrl+O) for the file, select from recent files list or drag the file to this window to start recovery.

Click Settings (Ctrl+T) to configure password recovery engine. Show settings.

Click Order toolbar button or visit http://www.LostPassword.com/ to purchase fully functional version.

Select encrypted file to recover

Step 5: After running the first password auditing session, check to see if Office key has crackedthe password. If the password has not been cracked press the Settings button on theuppertoolbar.



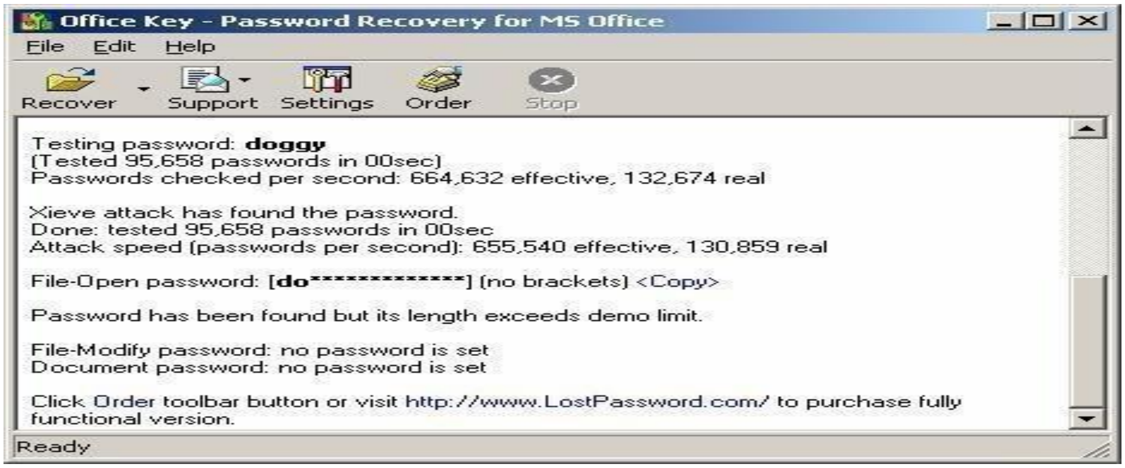
Process priority

● High
○ Normal
○ Background

Attack types

☑ Dictionary
☑ Brute-force with xieve optimization
☑ Brute-force

Step6: OnceintheSettings menuyouwillbeabletomodifythesearchparameters andcustomize amoretargetedsearch



```
Testing password: doggy
(Tested 95,658 passwords in 00sec)
Passwords checked per second: 664,632 effective, 132,674 real

Xieve attack has found the password.
Done: tested 95,658 passwords in 00sec
Attack speed (passwords per second): 655,540 effective, 130,859 real

File-Open password: [do*************] (no brackets) <Copy>

Password has been found but its length exceeds demo limit.

File-Modify password: no password is set
Document password: no password is set

Click Order toolbar button or visit http://www.LostPassword.com/ to purchase fully
functional version.
```

Ready

Step7: Repeatsteps3and4until thepassword hasbeencrackedand openstheMS Office File.
Step8: WritedownthecontentsoftheMSworddocumentandthepasswordinto yourlabreportandsubmitittoyour TA

RESULT:

ThustheexperimentforEavesdropping,Dictionaryattacks,MITMattackswas done successfully.

EX.No:7	EXPERIMENTWITHSNIFFTRAFFICUSINGARP POISONING

AIM

PerformanExperimenttoSniffTrafficusingARPPoisoning

PROCEDURE:

ARP is the acronym for Address Resolution Protocol. It is used to convert IP address to physicaladdresses [MAC address] on a switch. The host sends anARP broadcast on the network, and therecipient computer responds with its physical address [MAC Address]. The resolved IP/MACaddressis then used to communicate. **ARP poisoningissendingfakeMACaddressestotheswitchsothatitcanassociatethefake MAC addresses with the IP address of a genuine computer onanetworkandhijack the traffic**.

ARPPoisoningCountermeasures:

Static ARP entries: these can be defined in the local ARP cache and the switch configured toignoreall auto ARP reply packets. The disadvantage of this method is, it’s difficult to maintain on large networks. IP/MACaddressmappinghastobedistributedtoallthecomputersonthenetwork.

ARPpoisoningdetectionsoftware:thesesystemscanbeusedtocrosschecktheIP/MAC address resolution and certify them if they are authenticated. Uncertified IP/MAC addressresolutionscanthenbeblocked.

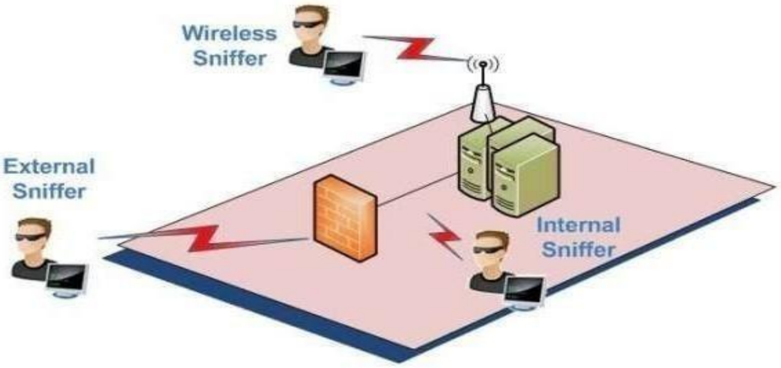
Whatisnetworksniffing?

Computerscommunicatebybroadcastingmessagesonanetworkusing IPaddresses.Onceamessagehasbeensentonanetwork,therecipientcomputerwiththematchingIP addressrespondswithits MACaddress.

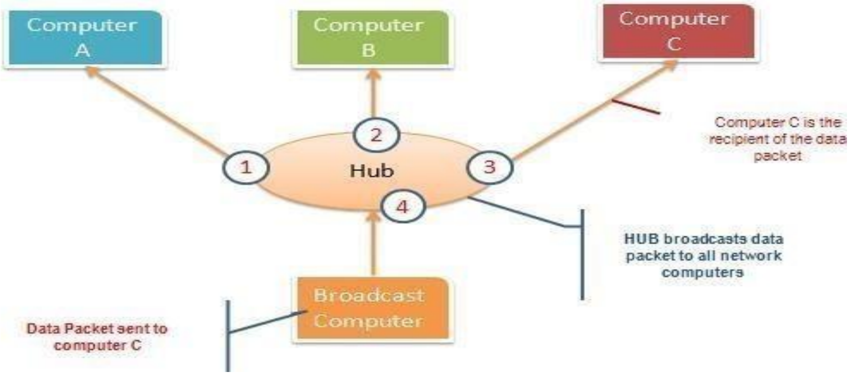
Networksniffingistheprocessofinterceptingdatapacketssentovera network.

PassiveandActiveSniffing

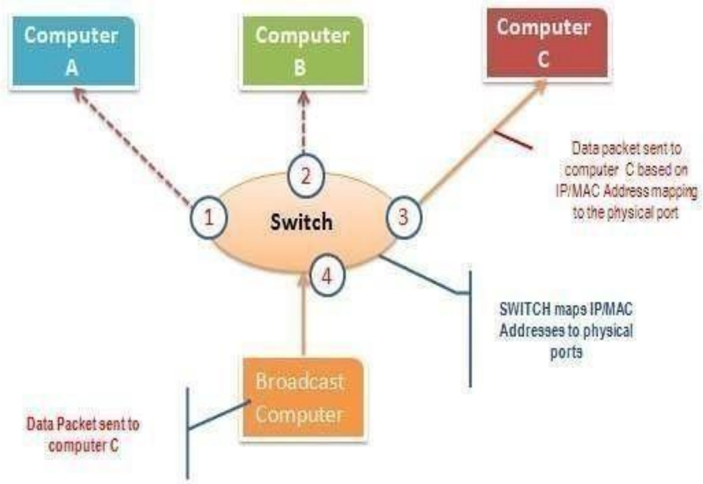
Beforewelookatpassiveandactivesniffing,let’slookattwomajordevicesusedto networkcomputers; hubs and switches.



Ahubworksbysendingbroadcastmessagestoalloutputportsonitexcepttheonethathassentthebroadcast.


Computer A
Computer B
Computer C
Computer C is the recipient of the data packet
1
2
Hub
3
4
HUB broadcasts data packet to all network computers
Broadcast Computer
Data Packet sent to computer C

Aswitchworksdifferently;itmapsIP/MACaddressestophysicalportson it.


Computer A
Computer B
Computer C
Switch
1
2
3
4
Data packet sent to computer C based on IP/MAC Address mapping to the physical port
SWITCH maps IP/MAC Addresses to physical ports
Broadcast Computer
Data Packet sent to computer C

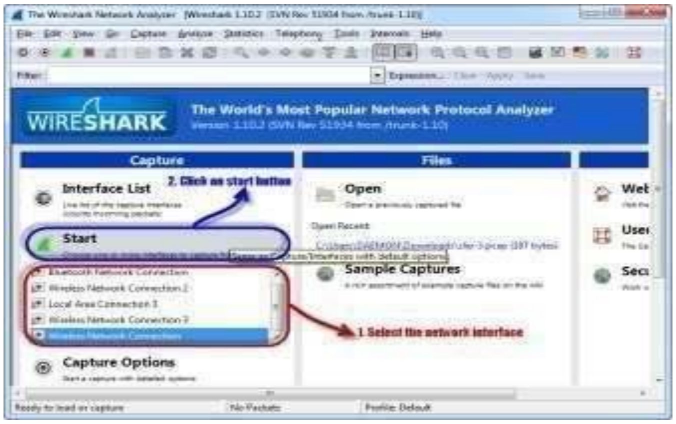
Passive sniffing is intercepting packages transmitted over a network that uses a hub. It iscalledpassivesniffingbecauseitisdifficulttodetect.Itisalsoeasy toperformas thehubsendsbroadcastmessagestoallthecomputers onthenetwork.

Activesniffingisinterceptingpackagestransmittedoveranetworkthatusesaswitch. Therearetwomainmethods used tosniff switchlinkednetworks,ARP Poisoning,andMACflooding.

SniffingthenetworkusingWireshark

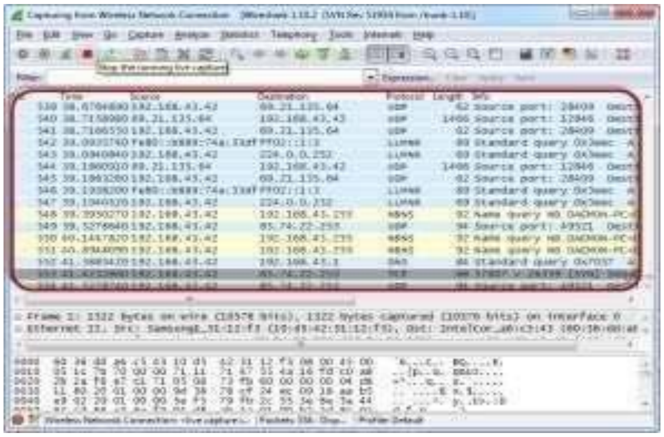
DownloadWiresharkfromthislinkhttp://www.wireshark.org/download.html

- OpenWireshark
- Youwillgetthefollowingscreen

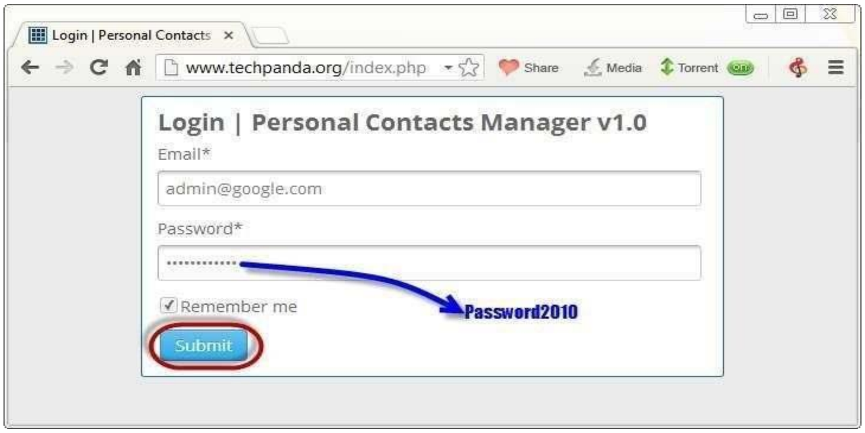

The Wireshark Network Analyzer [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.10.2 (SVN Rev 51934 from /trunk-1.10)
Capture
Files
Interface List
2. Click on start button
Start
Bluetooth Network Connection
Wireless Network Connection 2
Local Area Connection 3
Wireless Network Connection 3
Wireless Network Connection
1 Select the network interface
Capture Options
Open
Open Recent:
Sample Captures
Web
User
Seci
Ready to load or capture
No Packets
Profile: Default

Selectthenetworkinterfaceyouwanttosniff.Noteforthisdemonstration,weareusingawirelessnetworkconnection.Ifyouareonalocalareanetwork,thenyoushouldselectthelocalareanetworkinterface.

- Clickonstartbuttonas shownabove



- Openyourwebbrowserandtypeinhttp://www.techpanda.org/



Login | Personal Contacts Manager v1.0

Email*

admin@google.com

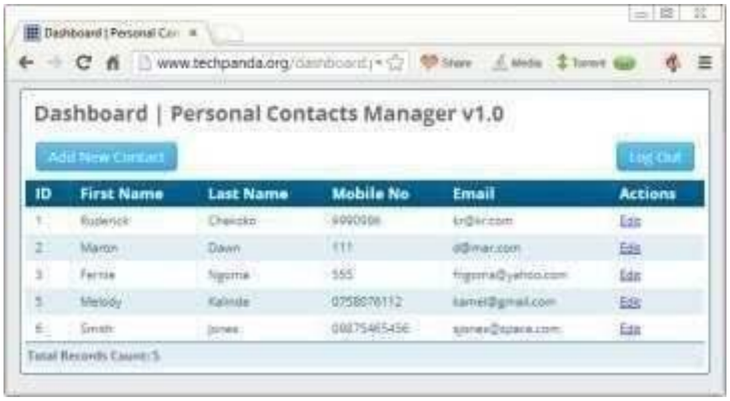
Password*

••••••••••••

☑ Remember me

Submit

- Theloginemailis**admin@google.com**andthepasswordis**Password2010**
- Clickonsubmitbutton
- Asuccessfullogonshouldgiveyouthefollowingdashboard

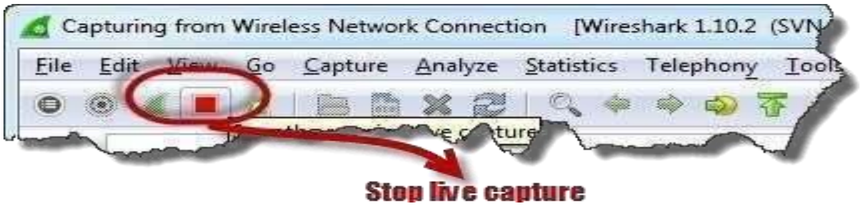


Dashboard | Personal Contacts Manager v1.0

ID	First Name	Last Name	Mobile No	Email	Actions
1	Roderick	Chewcko	9990008	kr@kr.com	Edit
2	Marion	Dawn	111	d@mar.com	Edit
3	Fernie	Ngoma	555	fngoma@yahoo.com	Edit
5	Melody	Kalinde	0758976112	kamel@gmail.com	Edit
6	Smith	Jones	00875465456	sjones@space.com	Edit

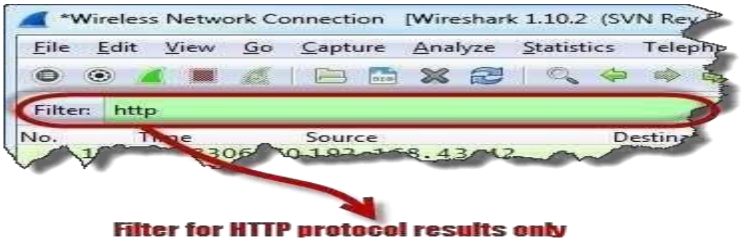
Total Records Count: 5

- GobacktoWiresharkandstopthelivecapture


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

Stop live capture

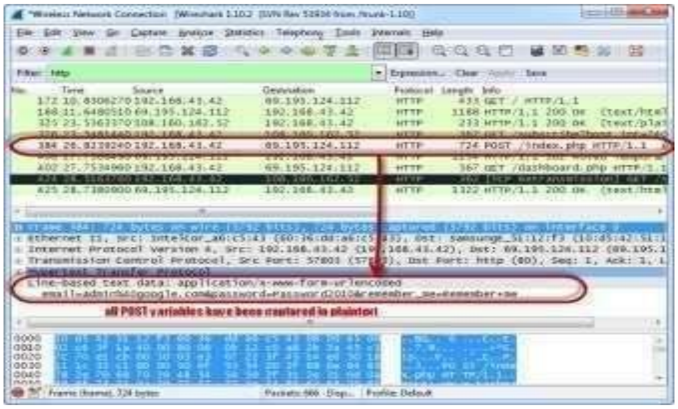
- FilterforHTTPprotocolresultsonlyusingthefiltertextbox



Filter: http

Filter for HTTP protocol results only

- LocatetheInfocolumnandlookforentrieswiththeHTTPverbPOSTandclickonit



Filter: http

```
No.  Time         Source          Destination     Protocol Length Info
 172 10.8306270 192.168.43.42   69.195.124.112  HTTP      433 GET / HTTP/1.1
 188 11.6480510 69.195.124.112  192.168.43.42   HTTP     1168 HTTP/1.1 200 OK  (text/html)
 325 23.5363370 108.160.162.52  192.168.43.42   HTTP      233 HTTP/1.1 200 OK  (text/plain)
 384 26.8238240 192.168.43.42   69.195.124.112  HTTP      724 POST /index.php HTTP/1.1
 402 27.7534900 192.168.43.42   69.195.124.112  HTTP      367 GET /dashboard.php HTTP/1.1
 425 28.7380900 69.195.124.112  192.168.43.42   HTTP     1322 HTTP/1.1 200 OK  (text/html)

Frame 384: 724 bytes on wire (5792 bits), 724 bytes captured (5792 bits) on interface 0
Ethernet II, Src: IntelCor_a6:c5:43 (60:36:dd:a6:c5:43), Dst: Samsunge_51:12:f3 (10:d5:42:51:1
Internet Protocol Version 4, Src: 192.168.43.42 (192.168.43.42), Dst: 69.195.124.112 (69.195.1
Transmission Control Protocol, Src Port: 57801 (57801), Dst Port: http (80), Seq: 1, Ack: 1, L
Hypertext Transfer Protocol
Line-based text data: application/x-www-form-urlencoded
  email=admin%40google.com&password=Password2010&remember_me=remember+me
```

all POST variables have been captured in plaintext

- Justbelowthelogentries,thereisapanelwithasummaryofcaptureddata.Look forthesummarythatsaysLine-basedtextdata: application/x-www-form-url encoded
- You should be able to view the plaintext values of all the POST variables submitted totheserver viaHTTP protocol.

Result:

Thus the experiment toSniff Traffic using ARP Poisoning was performed.

EX.No:8	DEMONSTRATEINTRUSIONDETECTIONSYSTEM USINGANYTOOL

AIM:

TodemonstrateIntrusionDetectionSystem(IDS)usingSnortsoftwaretool.

STEPSONCONFIGURINGANDINTRUSIONDETECTION:

1. DownloadSnortfromtheSnort.orgwebsite.(http://www.snort.org/snort-downloads)
2. DownloadRules(https://www.snort.org/snort-rules).Youmustregistertogettherules. (Youshoulddownloadtheseoften)
3. Doubleclickonthe.exeto installsnort.Thiswillinstallsnortinthe“C:\Snort”folder.ItisimportanttohaveWinPcap(https://www.winpcap.org/install/)installed
4. ExtracttheRulesfile.YouwillneedWinRARforthe.gzfile.
5. Copyallfilesfromthe“rules”folderoftheextractedfolder.Nowpastetherulesinto *“C:\Snort\rules”*folder.
6. Copy “snort.conf” file from the “etc” folder of the extracted folder. You must paste it into “C:\Snort\etc”folder.Overwrite anyexisting file. Remember if you modify your snort.conf fileanddownloadanewfile,youmustmodify itforSnortto work.
7. Openacommandprompt(cmd.exe)andnavigatetofolder“C:\Snort\bin”folder.
8. Tostart(execute)snortinsniffermodeusefollowingcommand:

snort-dev-i3

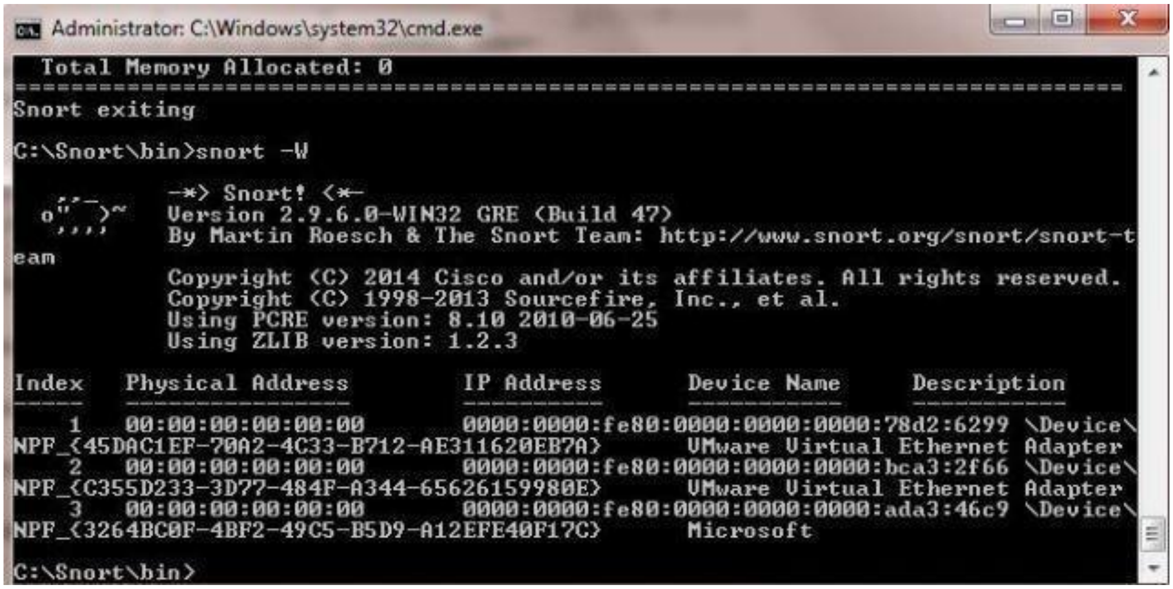
-iindicatestheinterfacenumber.Youmustpickthecorrectinterfacenumber.

Inmycase,itis3.

-devisusedtorunsnorttocapturepacketsonyournetwork.

Tocheckttheinterfacelist,usefollowingcommand:

snort-W



Administrator: C:\Windows\system32\cmd.exe

```
  Total Memory Allocated: 0
================================================================================
Snort exiting

C:\Snort\bin>snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.6.0-WIN32 GRE (Build 47)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-t
eam
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

Index   Physical Address         IP Address        Device Name      Description
-----   -----------------        ----------        -----------      -----------
    1   00:00:00:00:00:00        0000:0000:fe80:0000:0000:0000:78d2:6299 \Device\
NPF_{45DAC1EF-70A2-4C33-B712-AE311620EB7A}       VMware Virtual Ethernet Adapter
    2   00:00:00:00:00:00        0000:0000:fe80:0000:0000:0000:bca3:2f66 \Device\
NPF_{C355D233-3D77-484F-A344-6562615998 0E}       VMware Virtual Ethernet Adapter
    3   00:00:00:00:00:00        0000:0000:fe80:0000:0000:0000:ada3:46c9 \Device\
NPF_{3264BC0F-4BF2-49C5-B5D9-A12EFE40F17C}       Microsoft

C:\Snort\bin>
```

Findinganinterface

YoucantellwhichinterfacetousebylookingattheIndexnumberandfinding Microsoft.As you canseein theabove example,theotherinterfacesareforVMWare.

TorunsnortinIDSmode,youwillneedtoconfigurethefile“snort.conf”accordingto your networkenvironment.

Tospecifythenetworkaddressthatyouwanttoprotectinsnort.conffile,lookforthe following line.varHOME_NET192.168.1.0/24(You willnormallysee anyhere)

YoumayalsowanttosettheaddressesofDNS_SERVERS,ifyouhavesomeonyournetwork.

examplesnort

ChangetheRULE_PATHvariabletothe path ofrules folder.varRULE_PATHc:\

snort\rules

pathtorules

Changethepathofalllibraryfileswiththe nameandpathonyoursystem.andyoumustchangethepathofsnort_dynamicpreprocessorvariable.

C:\Snort\lib\snort_dynamiccpreprocessor

Youneedtodothistoalllibraryfilesinthe“C:\Snort\lib”folder.Theoldpathmight be:“/usr/local/lib/…”.youwillneedtoreplacethatpathwithyoursystempath.UsingC:\Snort\libChangethe path of the“dynamicengine” variablevalue inthe “snort.conf”file..

dynamicengineC:\Snort\lib\snort_dynamicengine\sf_engine.dll

Addthepathsfor“includeclassification.config”and“includereference.config”files.includec:\snort\etc\classification.config

includec:\snort\etc\reference.config

Removethecomment(#)onthelinetoallowICMPrules,ifitiscommentedwitha#.include $RULE_PATH/icmp.rules

Youcanalsoremovethecommentof ICMP-inforulescomment,ifit iscommented.include $RULE_PATH/icmp-info.rules

Toaddlogfilestostorealertsgeneratedbysnort,searchforthe“outputlog”testin snort.conf andaddthefollowing line:

outputalert_fast:snort-alerts.ids

Comment(adda#)thewhitelist $WHITE_LIST_PATH/white_list.rulesandtheblacklist

Changethenested_ipinner,\tonested_ip inner#,\Comment out(#)followinglines:

#preprocessornormalize_ip4

#preprocessornormalize_tcp:ipsecnstream

#preprocessor normalize_icmp4

#preprocessornormalize_ip6

#preprocessornormalize_icmp6

Savethe“snort.conf”file.

TostartsnortinIDSmode,runthefollowingcommand:

snort-cc:\snort\etc\snort.conf-lc:\snort\log-i3(Note:3isusedformyinterfacecard)Ifalogiscreated,selecttheappropriateprogramto openit.YoucanuseWordPardorNotePad++toreadthefile.

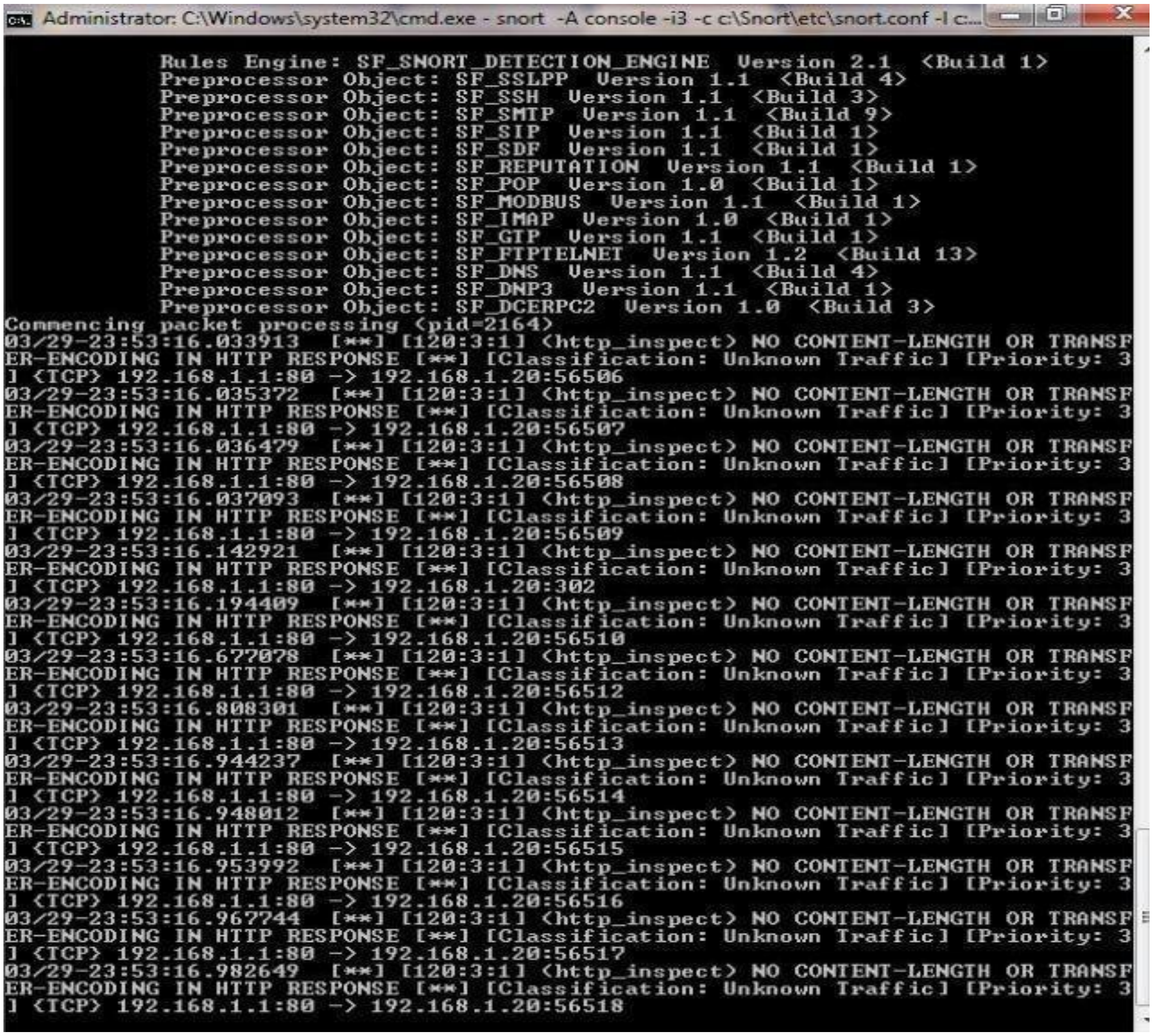
Togenerate Log filesin ASCIImode, you can usefollowing command while runningsnort in IDSmode:

```
snort-Aconsole-i3-cc:\Snort\etc\snort.conf-lc:\Snort\log-Kascii
```

Scanthecomputerthatisrunning snortfromanothercomputerbyusingPINGorNMap (ZenMap).

Afterscanningorduringthescanyoucancheckthesnort-alerts.ids filein thelogfoldertoinsureitisloggingproperly.You willseeIP address foldersappear.

Snortmonitoringtraffic–


Administrator: C:\Windows\system32\cmd.exe - snort -A console -i3 -c c:\Snort\etc\snort.conf -l c...

```
          Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.1  <Build 1>
          Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
          Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
          Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
          Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
          Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
          Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
          Preprocessor Object: SF_POP  Version 1.0  <Build 1>
          Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
          Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
          Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
          Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
          Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
          Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
          Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
Commencing packet processing (pid=2164)
03/29-23:53:16.033913  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56506
03/29-23:53:16.035372  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56507
03/29-23:53:16.036479  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56508
03/29-23:53:16.037093  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56509
03/29-23:53:16.142921  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:302
03/29-23:53:16.194409  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56510
03/29-23:53:16.677078  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56512
03/29-23:53:16.808301  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56513
03/29-23:53:16.944237  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56514
03/29-23:53:16.948012  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56515
03/29-23:53:16.953992  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56516
03/29-23:53:16.967744  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56517
03/29-23:53:16.982649  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56518
```

RESULT:

ThustheIntrusionDetectionSystem(IDS)hasbeendemonstratedbyusingthe Open SourceSnortIntrusion DetectionTool.

EX.No:9	EXPLORENETWORKMONITORINGTOOLS

AIM:

ToexploreaboutNetworkmonitoringtools

Networkmonitoringisanessentialpartofnetworkmanagement.Itinvolvesusingvarious tools tomonitorasystemnetworkanddetermineslownessandweakconnections,amongotherissues.Knowingmoreaboutthesetoolscanhelpyouunderstandthembetterandusetherightones that suityour requirements.

PROCEDURE:

WhatAreNetworkMonitoringTools?

Networkmonitoringtoolsaresoftwarethatyoucanusetoevaluatenetwork connections.Thesesoftwareprogramscanhelpyoumonitoranetworkconnectionandidentifynetworkissues,whichmayincludefailingnetworkcomponents,slowconnectionspeed,networkoutageorunidentifiableconnections.Networkmanagementandmonitoringtools canalsohelyouresolvetheseissuesorestablishsolutionsthatpreventspecificissuesfromoccurringinthefuture.

NetworkMonitoringTools

Hereareeightmonitoringtoolsalongwiththeirdescriptionsandfeatures:

1. SolarWindsNetworkPerformanceMonitor

SolarWindsNetworkPerformanceMonitorisamulti-vendormonitoringtool.Itallowsuserstomonitor multiple vendors' networks at the same time. Italsoprovidesnetworkinsightsfothoroughvisibilityintothehealthofthenetworks.Someprominentfeaturesincludenetworkavailabilitymonitoring,intelligentnetworkmapping,criticalpathvisualisation,performanceanalysisandadvancedalerting.SolarWindsalsoallowsuserstotrackVPNtunnelstatus.ItpromptswhenaVPNtunnelisavailabletohelpusersensureastable connection between sites. SolarWinds provides aseven-dayfree trial,afterwhich userscanchoose a preferredsubscriptionplan.

2. DatadogNetworkMonitoring

DatadogNetworkMonitoringoffersservicesforon-premisesdevicesandcloudnetworks.Ahighlightingfeatureofthistoolisthevisualisations.It offers various graphical representationsof allthe network connections on a system. It alsoallows users to track key metrics like network latency,connection churn and transmissioncontrolprotocol(TCP)retransmits.Userscanmonitorthehealthofanetworkconnectionat different endpoints at the application, IP address, port or process ID layers.Otherprominentfeaturesincludeautomatedlogcollectionanduserinterfacemonitoring.

3. PaesslerPRTGNetworkMonitor

Paessler's network connection monitoring tool provides a clean user interface and network visibility onmultiple devices. Users can track the health of different connection types like local area networks(LAN),wideareanetwork(WAN),servers,websites,applicationsandservices.Thetoolsalsointegrate with various technologies, which makes it easier to use it for different types of applications. Itprovides distribute monitoring, allowing users to track network connections on devices in differentlocations. The tool also provides apps for mobile platforms that can help users to track network healthonmobilephones.

4. ManageEngineOpManager

ManageEngine OpManager is a good network monitoring and managing tool for users that prefer in-depth view of network health and issues. This tool provides over 2000networkperformancemonitorsthatallowuserstotrackandmonitortheirconnectionsandperformdetaileda nalysesoniss ues.Italsoprovides over 200 dashboard widgets that can help users customise theirdashboardtotheirownsuitability.OtherfeaturesincludeCPU,memoryanddisk utilisationmonitoringonlocalandvirtualmachines.Italsoallowssettingnetwork performance threshold and notifies the user in case of aviolation.

5. Domotz

Domotzisanexpansivetoolthatprovidesalistoffeaturesformonitoringnetwork connections. Itallows users to customise their network monitoring preferences. Users can write scripts the retrieve thedata they wish to evaluate. It also allows connection to open ports on remote devices while ensuringnetwork security. Users can also scan and monitor network connections globally. Domotz also allowsto backup and restore network configuration for switches, firewalls and access points and alerts whenthere is achangein theconfiguration.

6. Checkmk

Checkmk is a tool that allows users to automate it completely. You can customise its operations andenable it to perform tasks automatically. It also identifies network and security components without theuser requiring manual set up. For example, the tool can identify a firewall even if the user has not set itup. Its Agent Bakery feature enables usersto manageagents and automate agentupdating. Thisreduces manual effort to monitor network connections. The tool also includes over 2000 plug-ins forenhancing network monitoring.

7. ProgressWhatsupGold

ProgressWhatsupGoldisabasicnetworkmonitoring software.Itprovidesaminimaluserinterfacewithessentialfeatureslikedevice monitoring,applicationmonitoring,analysingnetworktraffic andmanagingconfigurations.Thetoolallowsuserstomonitorclouddevices,inspectsuspiciousconnections,automateconfigurationbackupsand identify,and resolve bandwidthissues.

OtherToolsForNetworkMonitoring

Herearethreeadditionaltoolsfornetworkmonitoring:

- FortraIntermapper: This tool enables users to monitor network connections using networkmaps, allowing them to get a holistic view of all the connections. Italso provides variouscolour codes for different networkstatus, along with real-time notifications through text, emailand sound.

NagiosCore:NagiosCoreisamonitoringenginethatworksastheprimaryapplicationfor allNagiosprojects,includingtheNagiosNetworkAnalyser.ItintegrateswithotherNagiosapplicationsandprovidesuserswithfeatureslikeavisualdashboard,customapplicationmonitoring,automatedalertsystem,advancedusermanagementandnetworksecuritymonitoring

- Zabbix: Zabbix provides a thorough network monitoring solution with features like servermonitoring,cloudmonitoring,applicationmonitoringandservicemonitoring.The toolalsoincludesfeatureslikemetric collection,

ToChooseaNetworkMonitoringAndManagementTool:

Understandtherequirements

Understanding why you require network monitoring software is important in the process. Define whatfeature you want and for what purpose. This can help you identifythe right tool for your use. It mayalsohelp youchoosethecorrectsubscription planonpaidtools.

Browsemultipletools

Onceyouidentifythe requirements,considerbrowsingmultipletools.Visitthewebsitesof the toolsand look for the features you require. Spend time studying the features and understand how they can beusefulto yourrequirements. Youcanalsoidentifyafewtoolsandcomparetheirfeaturestoeachother.

Considerthebudget

Some tools may be free to use, while some may require you topurchase a subscriptionplan Paid tools typically offer a freetrial period of upto 30days.Once you identify which tool you may liketous ,see if it is free or requires payment.If it is a paid tool,try exploring its features and efficiency duringt hetrialperiod.Consider keeping a backup tool incase the tool that you choose does not fit your usage.

RESULT:

Thus the network monitoring tools was explored.

EX.No:10	**STUDYTOCONFIGUREFIREWALL,VPN**

AIM:

TostudythefeaturesoffirewallinprovidingnetworksecurityandtosetFirewallSecurityin windows.

PROCEDURE:

FirewallinWindows7

Windows7comeswithtwofirewallsthatworktogether.Oneisthe**Windows Firewall**, and the other is **Windows Firewall with Advanced Security (WFAS)**.Themaindifferencebetweenthemisthe complexityofthe rules configuration. Windows Firewall uses simple rules thatdirectlyrelate toa program or a service. The rulesinWFAScanbeconfiguredbasedonprotocols,ports,addressesandauthentication.By default,bothfirewallscomewithpredefinedsetofrulesthatallowustoutilizenetwork resources.Thisincludesthingslikebrowsingtheweb,receivinge-mails,etc.Other standardfirewall exceptions are File andPrinterSharing,NetworkDiscovery, PerformanceLogsandAlerts,RemoteAdministration,WindowsRemoteManagement,Remote Assistance,RemoteDesktop,WindowsMediaPlayer,WindowsMediaPlayerNetworkSharing Service

With firewall in Windows 7 we can configure inbound and outbound rules. By default, all outboundtraffic is allowed, and inbound responses to that traffic are also allowed. Inbound trafficinitiatedfrom externalsourcesis automaticallyblocked.

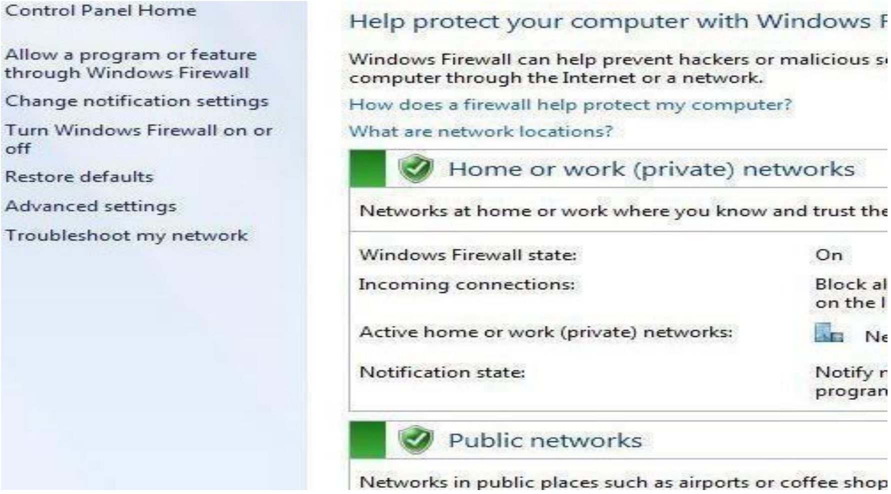
Whenwefirstconnecttosomenetwork,wearepromptedtoselectanetworklocation. This feature is known as Network Location Awareness(NLA). This feature enables us to assign a network profileto the connection based on the location. Different network profiles contain different collections offirewall rules. In Windows 7, different network profiles can be configured on different interfaces. Forexample, our wired interface can have different profile than our wireless interface.

Therearetwodifferent networkprofilesavailable:

- Public
- Home/Work-privatenetwork

ConfiguringWindowsFirewall

ToopenWindowsFirewallwecangoto**Start>ControlPanel>Windows**


Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your computer with Windows F

Windows Firewall can help prevent hackers or malicious s computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Home or work (private) networks

Networks at home or work where you know and trust the

Windows Firewall state: On

Incoming connections: Block al on the l

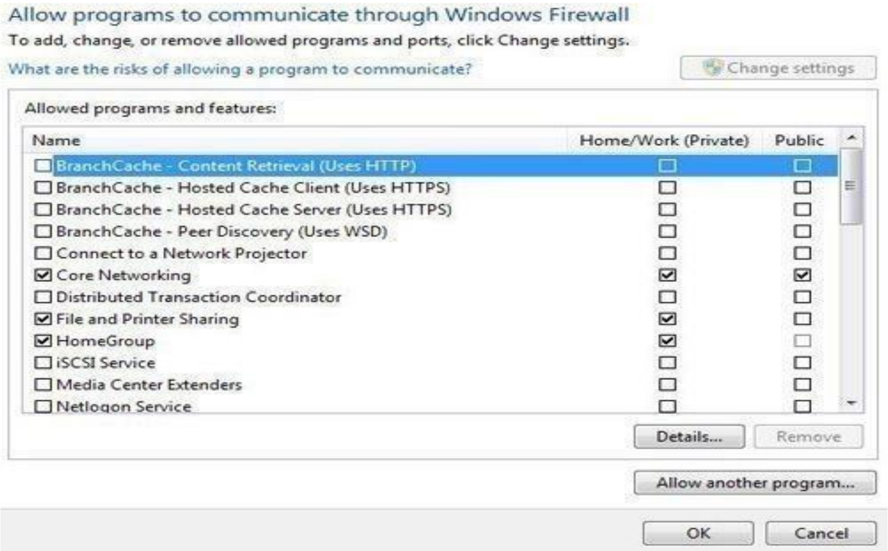
Active home or work (private) networks: Ne

Notification state: Notify r progran

Public networks

Networks in public places such as airports or coffee shop

Bydefault,Windows Firewallisenabledfor bothprivate(home or work)and public networks. Itis also configured to block all connectionsto programs that are not on the list of allowed programs.To configure exceptions we can go to the menu on the left and select "Allow a program or featurethroughWindows Firewall"option.



Allow programs to communicate through Windows Firewall

To add, change, or remove allowed programs and ports, click Change settings.

What are the risks of allowing a program to communicate?

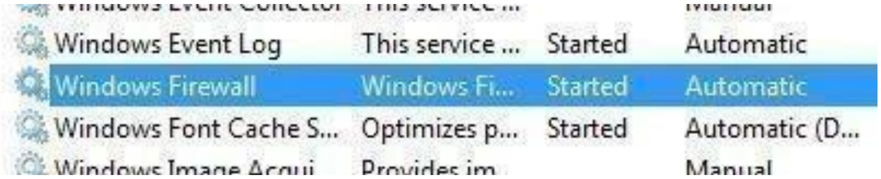
Allowed programs and features:

Name	Home/Work (Private)	Public
□ BranchCache - Content Retrieval (Uses HTTP)	□	□
□ BranchCache - Hosted Cache Client (Uses HTTPS)	□	□
□ BranchCache - Hosted Cache Server (Uses HTTPS)	□	□
□ BranchCache - Peer Discovery (Uses WSD)	□	□
□ Connect to a Network Projector	□	□
☑ Core Networking	☑	☑
□ Distributed Transaction Coordinator	□	□
☑ File and Printer Sharing	☑	□
☑ HomeGroup	☑	□
□ iSCSI Service	□	□
□ Media Center Extenders	□	□
□ Netlogon Service	□	□

FirewallCustomization

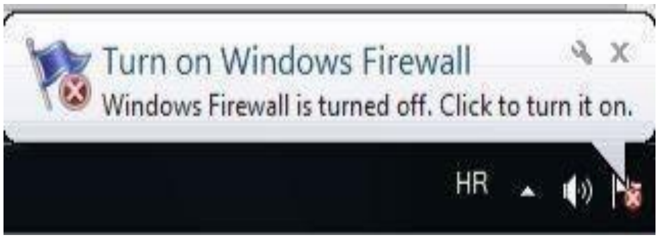
Note that we can modify settings for each type of network location (private or public).Interestingthing here is that we can block all incoming connections, including those in thelistofallowedprograms.

Windows Firewall is actually a Windows service. As you know, services canbe stoppedand started. If the Windows Firewall service is stopped, the Windows Firewall will notwork.



Windows Event Collector	This service ...		Manual
Windows Event Log	This service ...	Started	Automatic
Windows Firewall	Windows Fi...	Started	Automatic
Windows Font Cache S...	Optimizes p...	Started	Automatic (D...
Windows Image Acqui...	Provides im...		Manual

FirewallService
Inourcasetheserviceisrunning.Ifwestopit,wewillgetawarningthatweshouldturnon ourWindowsFirewall.



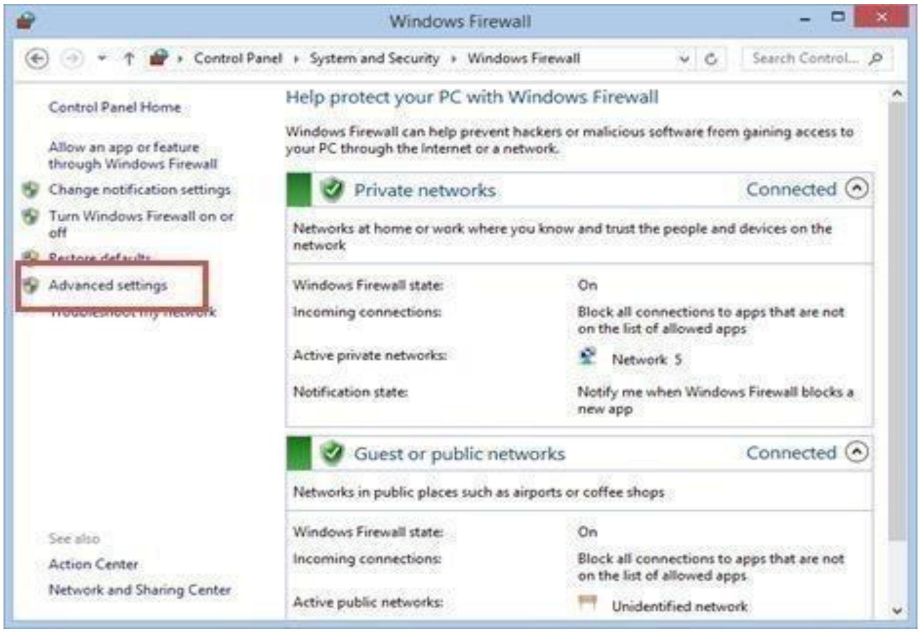
Turn on Windows Firewall
Windows Firewall is turned off. Click to turn it on.

HowtoStart&UsetheWindowsFirewallwithAdvancedSecurity

The *Windows Firewall with Advanced Security* is a tool which gives you detailed controlovertherulesthatareappliedbythe*WindowsFirewall*.Youcanviewallthe rulesthatare used by the *Windows Firewall*, change their properties, create new rules or disableexistingones.

Youhaveseveralalternativestoopeningthe*WindowsFirewallwithAdvancedSecurity*:

OneistoopenthestandardWindowsFirewallwindow,bygoingto*"ControlPanel->SystemandSecurity->WindowsFirewall"*.Then,clickortap*Advancedsettings*.


Windows Firewall
Control Panel › System and Security › Windows Firewall
Search Control...
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center

Help protect your PC with Windows Firewall

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

Private networks — Connected

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

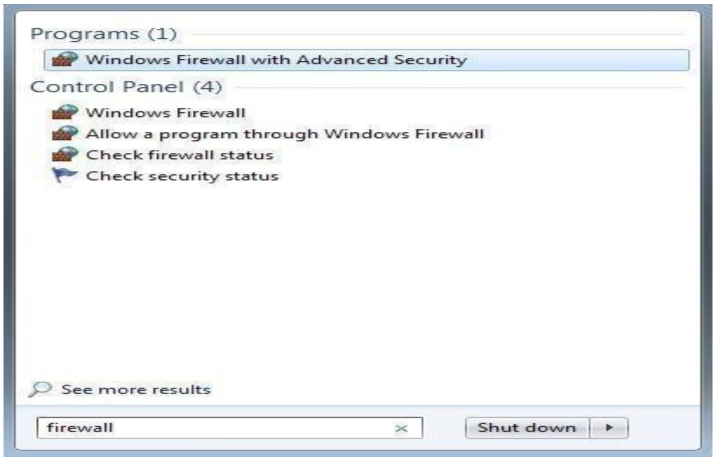
Windows Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	Network 5
Notification state:	Notify me when Windows Firewall blocks a new app

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	Unidentified network

InWindows7,anothermethodistosearchforthe word*firewall*inthe*StartMenu*searchboxandclickthe"*WindowsFirewall withAdvanced Security*"result.



firewall

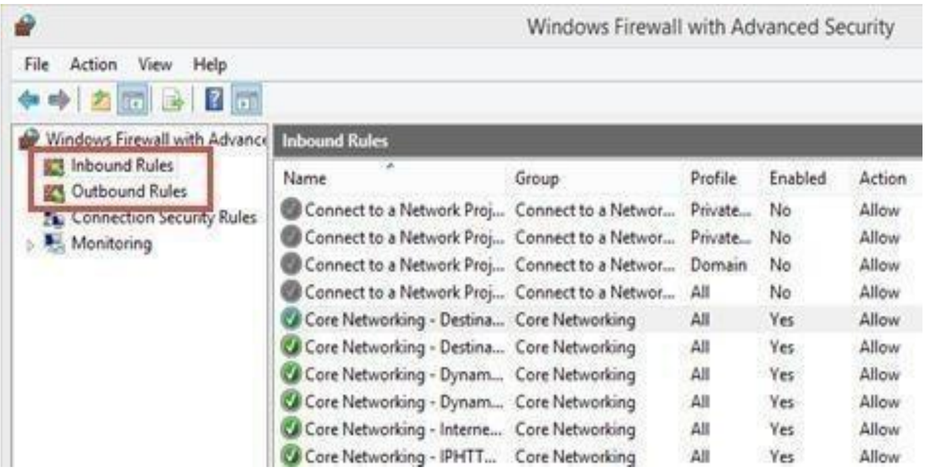
WhatAreTheInbound&OutboundRules?

In order to provide the security you need, the *Windows Firewall* has a standard set ofinbound and outbound rules, which are enabled depending on the location of the networkyouareconnectedto.

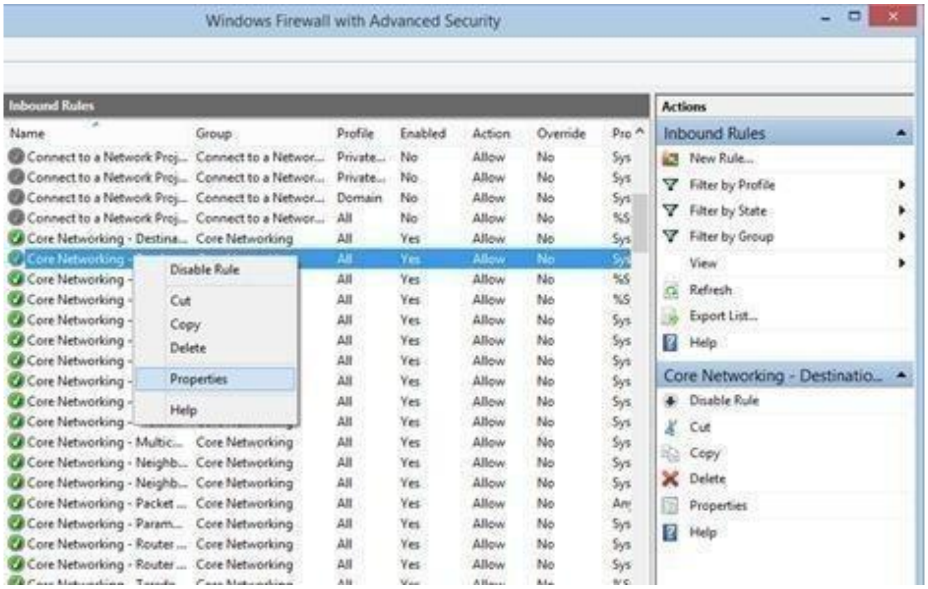
Inbound rules are applied to the traffic that is coming from the network and the Internet toyour computer or device. Outbound rules apply to the traffic from your computer to thenetworkortheInternet.

These rules can be configured so that they are specific to: computers, users, programs,services, ports or protocols. You can also specify to which type of network adapter (e.g.wireless,cable,virtualprivatenetwork)oruserprofileitisapplied to.

In the *Windows Firewall withAdvancedSecurity*,youcanaccessallrules and edittheir properties. All you have to do is clickor tap the appropriate unit in the left-sidepanel.


Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules

Name	Group	Profile	Enabled	Action
Connect to a Network Proj...	Connect to a Networ...	Private...	No	Allow
Connect to a Network Proj...	Connect to a Networ...	Private...	No	Allow
Connect to a Network Proj...	Connect to a Networ...	Domain	No	Allow
Connect to a Network Proj...	Connect to a Networ...	All	No	Allow
Core Networking - Destina...	Core Networking	All	Yes	Allow
Core Networking - Destina...	Core Networking	All	Yes	Allow
Core Networking - Dynam...	Core Networking	All	Yes	Allow
Core Networking - Dynam...	Core Networking	All	Yes	Allow
Core Networking - Interne...	Core Networking	All	Yes	Allow
Core Networking - IPHTT...	Core Networking	All	Yes	Allow



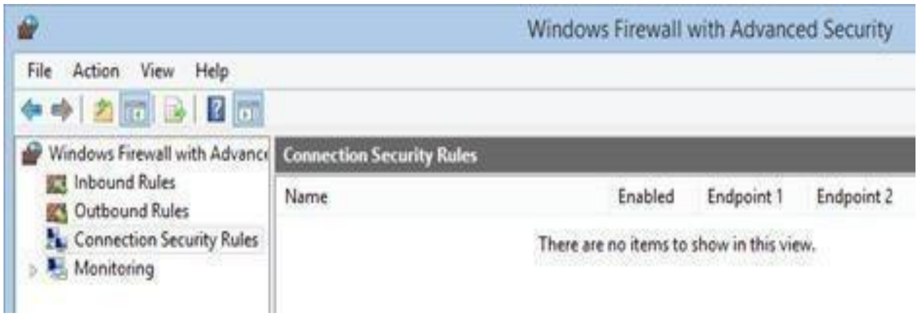
Name	Group	Profile	Enabled	Action	Override	Pro
Connect to a Network Proj...	Connect to a Networ...	Private...	No	Allow	No	Sys
Connect to a Network Proj...	Connect to a Networ...	Private...	No	Allow	No	Sys
Connect to a Network Proj...	Connect to a Networ...	Domain	No	Allow	No	Sys
Connect to a Network Proj...	Connect to a Networ...	All	No	Allow	No	%S
Core Networking - Destina...	Core Networking	All	Yes	Allow	No	Sys
Core Networking -		All	Yes	Allow	No	Sys
Core Networking -		All	Yes	Allow	No	%S
Core Networking -		All	Yes	Allow	No	%S
Core Networking -		All	Yes	Allow	No	Sys
Core Networking -		All	Yes	Allow	No	Sys
Core Networking -		All	Yes	Allow	No	Sys
Core Networking -		All	Yes	Allow	No	Sys
Core Networking -		All	Yes	Allow	No	Sys
Core Networking -		All	Yes	Allow	No	Sys
Core Networking - Multic...	Core Networking	All	Yes	Allow	No	Sys
Core Networking - Neighb...	Core Networking	All	Yes	Allow	No	Sys
Core Networking - Neighb...	Core Networking	All	Yes	Allow	No	Sys
Core Networking - Packet ...	Core Networking	All	Yes	Allow	No	Any
Core Networking - Param...	Core Networking	All	Yes	Allow	No	Sys
Core Networking - Router ...	Core Networking	All	Yes	Allow	No	Sys
Core Networking - Router ...	Core Networking	All	Yes	Allow	No	Sys
Core Networking - Teredo...	Core Networking	All	Yes	Allow	No	%S

WhataretheConnectionSecurityRules?

Connection security rules are used to secure traffic between two computers while itcrosses the network. One example would be a rule which defines that connectionsbetweentwospecificcomputersmustbeencrypted

Ifyouwanttoseeiftherearanysuchrulesonyourcomputer,clickortap*"ConnectionSecurity*

*Rules"*on the panel on the left.By default,there are no suchrulesdefinedonWindowscomputersanddevices.Theyaregenerallyusedinbusinessenvironmentsand suchrulesaresetbythe networkadministrator.

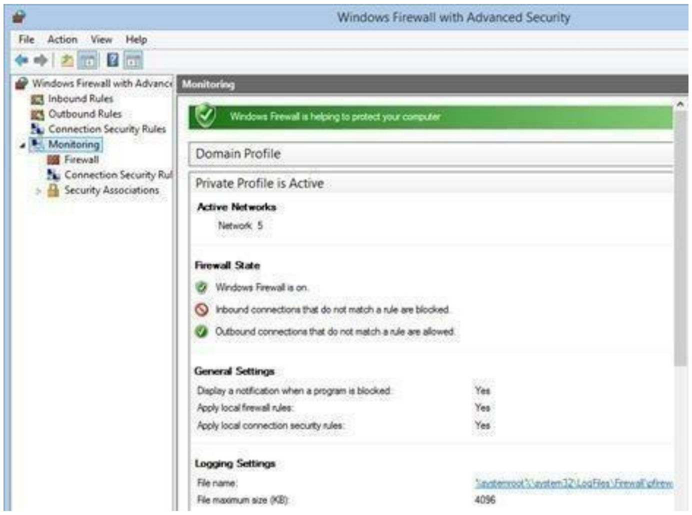

Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Connection Security Rules

Name	Enabled	Endpoint 1	Endpoint 2

There are no items to show in this view.

WhatdoestheWindowsFirewallwithAdvancedSecurityMonitor?

The *Windows Firewall with Advanced Security* includes some monitoring features aswell. Inthe *Monitoring* section you can find the following information: the firewallrulesthatareactive (both inbound and outbound), the connection security rules that are active and whetherthere areany activesecurity associations.



Windows Firewall is helping to protect your computer

Domain Profile

Private Profile is Active

Active Networks

Network 5

Firewall State

Windows Firewall is on.

Inbound connections that do not match a rule are blocked.

Outbound connections that do not match a rule are allowed.

General Settings

Display a notification when a program is blocked:	Yes
Apply local firewall rules:	Yes
Apply local connection security rules:	Yes

Logging Settings

File name:	%systemroot%\system32\LogFiles\Firewall\pfirew
File maximum size (KB):	4096

RESULT:

Thus study of the features of firewall linproviding network security and to set Firewall Security in windows.