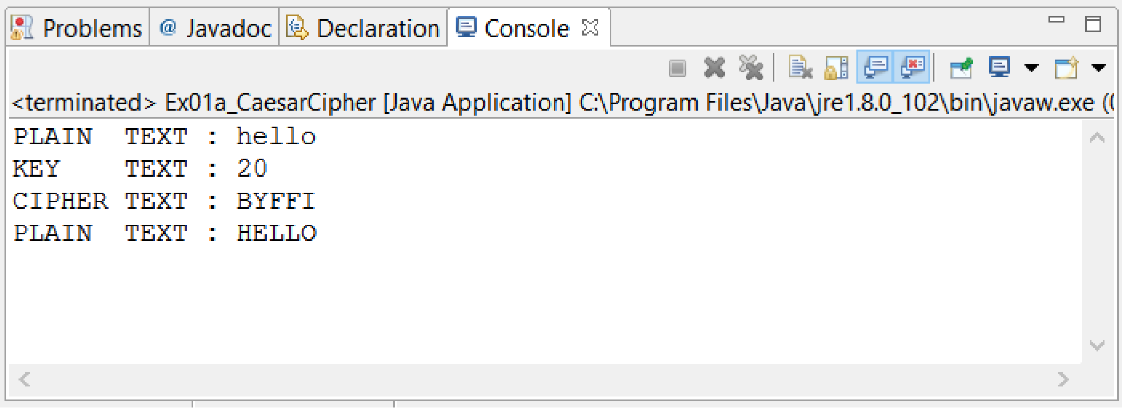
EX1A – CAESAR CIPHER

PROGRAM:

```
public class Ex01a_CaesarCipher {

	public static String crypt(String input, int key, boolean encrypt) {
		StringBuilder cipher = new StringBuilder("");
		for (char i : input.toCharArray()) {
			cipher.append((char) (((i - 'a' + (encrypt ? 1 : -1) * 
key) % 26 + 26) % 26 + 'a'));
		}
		return cipher.toString();
	}

	public static void main(String[] args) {
		String plain = "hello";
		int key = 20;

		System.out.println("PLAIN  TEXT : " + plain);
		System.out.println("KEY    TEXT : " + key);
		System.out.println("CIPHER TEXT : "
				+ crypt(plain, key, true).toUpperCase());
		System.out.println("PLAIN  TEXT : "
				+ crypt(crypt(plain, key, true), key, 
false).toUpperCase());
	}
}
```

OUTPUT:



```
<terminated> Ex01a_CaesarCipher [Java Application] C:\Program Files\Java\jre1.8.0_102\bin\javaw.exe ((
PLAIN  TEXT : hello
KEY    TEXT : 20
CIPHER TEXT : BYFFI
PLAIN  TEXT : HELLO
```

RESULT:

THE CAESAR CIPHER WAS SUCCESSFULLY CREATED

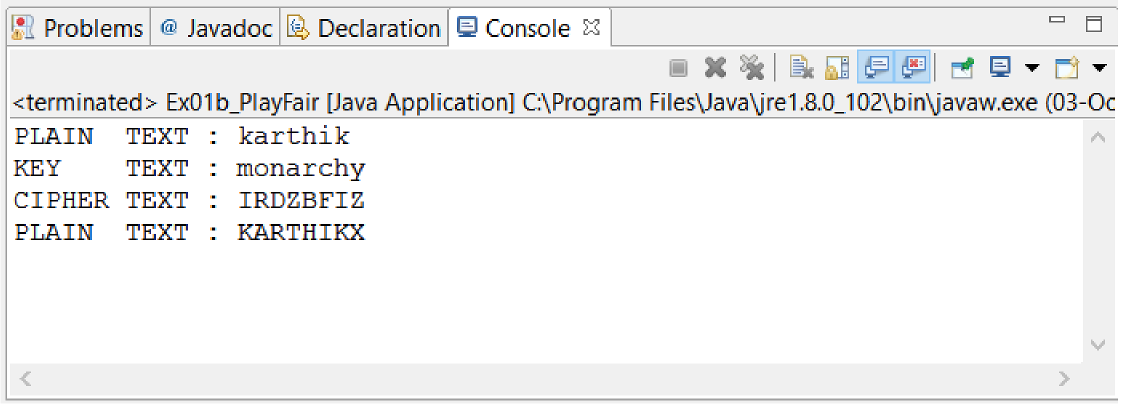
EX1B – PLAYFAIR CIPHER

PROGRAM:

```
public class Ex01b_PlayFair {
    public static int[][] processKey(String key) {
        int[][] keyMat = new int[26][2];

        int l = 0;
        for (char i : (key +
"abcdefghiklmnopqrstuvwxyz").toCharArray()) {
            if (key.indexOf(i + "") < 0 || l < key.length()) {
                keyMat[i - 'a'][0] = l / 5;
                keyMat[i - 'a'][1] = l++ % 5;
                if (i == 'i') {
                    keyMat[i - 'a' + 1][0] = l / 5;
                    keyMat[i - 'a' + 1][1] = l % 5;
                }
            }
        }

        return keyMat;
    }

    public static String crypt(String inputText, String key, boolean
encrypt) {
        int[][] keyMat = processKey(key);
        char[][] indMat = new char[5][5];
        for (int i = 0; i < keyMat.length; i++) {
            indMat[keyMat[i][0]][keyMat[i][1]] = (char) ('a' + i);
        }
        String cipherText = "";

        for (int i = 0; i < inputText.length(); i += 2) {
            char first = inputText.charAt(i);
            char second = i + 1 == inputText.length()
                    || first == inputText.charAt(i + 1) ? 'x' :
inputText
                    .charAt(i + 1);

            int fRow = keyMat[first - 'a'][0];
            int fCol = keyMat[first - 'a'][1];
            int sRow = keyMat[second - 'a'][0];
            int sCol = keyMat[second - 'a'][1];

            if (fRow == sRow) {
                fCol = ((fCol + (encrypt ? 1 : -1)) % 5 + 5) % 5;
                sCol = ((sCol + (encrypt ? 1 : -1)) % 5 + 5) % 5;
            } else if (fCol == sCol) {
                fRow = ((fRow + (encrypt ? 1 : -1)) % 5 + 5) % 5;
                sRow = ((sRow + (encrypt ? 1 : -1)) % 5 + 5) % 5;
            } else {
                int tCol = fCol;
                fCol = sCol;
                sCol = tCol;
            }

            cipherText += (indMat[fRow][fCol]) + "" +
(indMat[sRow][sCol]);
        }
```

```
            return cipherText;
      }

      public static void main(String[] args) {
            String plain = "karthik";
            String key = "monarchy";

            System.out.println("PLAIN  TEXT : " + plain);
            System.out.println("KEY    TEXT : " + key);
            System.out.println("CIPHER TEXT : "
                        + crypt(plain, key, true).toUpperCase());
            System.out.println("PLAIN  TEXT : "
                        + crypt(crypt(plain, key, true), key,
false).toUpperCase());
      }
}
```

OUTPUT:



```
<terminated> Ex01b_PlayFair [Java Application] C:\Program Files\Java\jre1.8.0_102\bin\javaw.exe (03-Oc
PLAIN  TEXT : karthik
KEY    TEXT : monarchy
CIPHER TEXT : IRDZBFIZ
PLAIN  TEXT : KARTHIKX
```

RESULT:

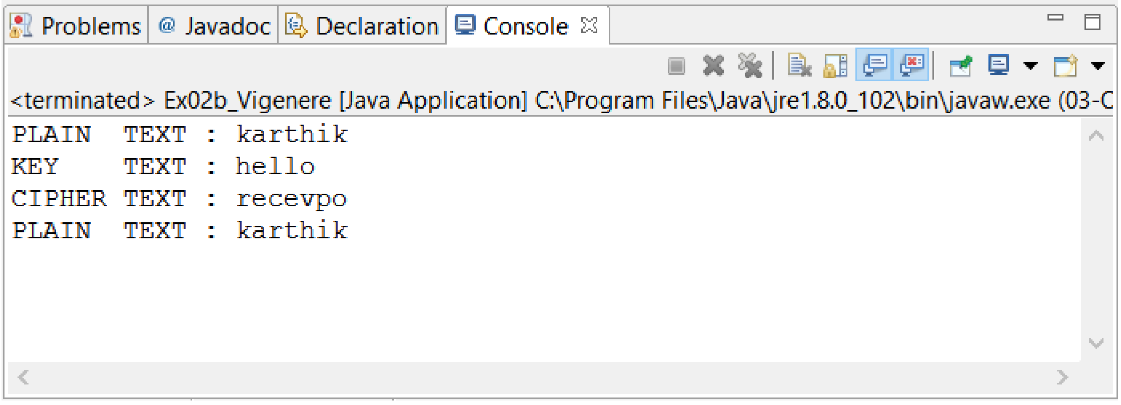
THE PLAY FAIR CIPHER ALGORITHM WAS IMPLEMENTED AND TESTED.

EX02A – VIGENERE CIPHER

PROGRAM:

```java
public class Ex02b_Vigenere {
      public static String cryptic(String input, String key, boolean 
encrypt) {
            StringBuilder output = new StringBuilder("");

            int j = 0;
            for (char i : input.toCharArray()) {
                  output.append((char) (((i - 'a' + (encrypt ? 
key.charAt(j) - 'a'
                              : -key.charAt(j) + 'a')) % 26 + 26) % 26 + 
'a'));
                  j = (j + 1) % key.length();
            }
            return output.toString();
      }

      public static void main(String[] args) {

            String plain = "karthik", key = "hello";

            System.out.println("PLAIN  TEXT : " + plain);
            System.out.println("KEY    TEXT : " + key);
            System.out.println("CIPHER TEXT : " + cryptic(plain, key, 
true));
            System.out.println("PLAIN  TEXT : "
                        + cryptic(cryptic(plain, key, true), key, false));
      }
}
```

OUTPUT:



```
<terminated> Ex02b_Vigenere [Java Application] C:\Program Files\Java\jre1.8.0_102\bin\javaw.exe (03-C
PLAIN  TEXT : karthik
KEY    TEXT : hello
CIPHER TEXT : recevpo
PLAIN  TEXT : karthik
```

RESULT:

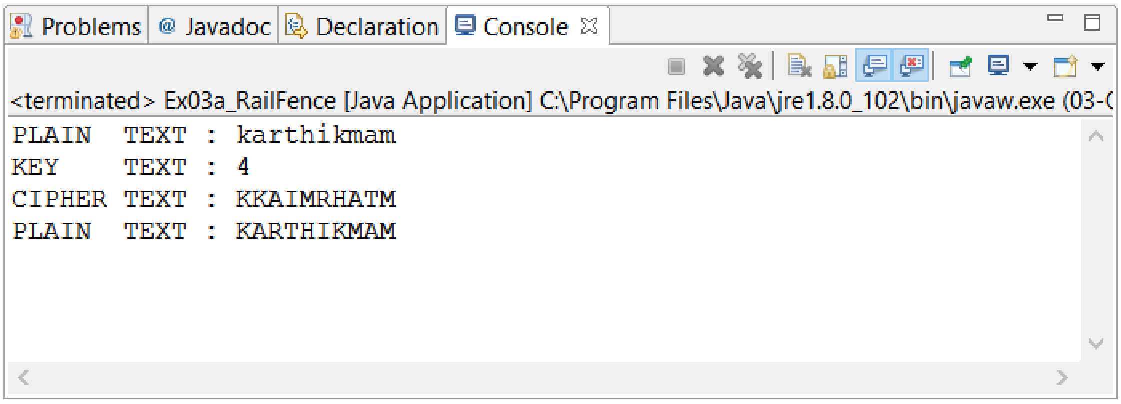
THE VIGENERE CIPHER ALGORITHM WAS SUCCESSFULLY IMPLEMENTED AND TESTED.

EX03A – RAIL FENCE ALGORITHM

PROGRAM:

```
public class Ex03a_RailFence {
	public static String crypt(String msg, int key, boolean encrypt) {
		char[] res = new char[msg.length()];

		for (int i = 0, k = 0; i < key; i++) {
			int inc = 2 * (key - i - 1);

			// format to take chars is j....(j + inc)....(j + 2 * 
(key - 1))
			for (int j = i; j < msg.length(); j += 2 * (key - 1)) {
				res[encrypt ? k++ : j] = msg.charAt(encrypt ? j : 
k++);
				if (i != key - 1 && i != 0 && (j + inc) < 
msg.length())
					res[encrypt ? k++ : j + inc] = 
msg.charAt(encrypt ? j + inc
							: k++);
			}
		}

		return new String(res);
	}

	public static void main(String[] args) {
		String plain = "karthikmam";
		int key = 4;

		System.out.println("PLAIN  TEXT : " + plain);
		System.out.println("KEY    TEXT : " + key);
		System.out.println("CIPHER TEXT : "
				+ crypt(plain, key, true).toUpperCase());
		System.out.println("PLAIN  TEXT : "
				+ crypt(crypt(plain, key, true), key, 
false).toUpperCase());
	}
}
```

OUTPUT:



<terminated> Ex03a_RailFence [Java Application] C:\Program Files\Java\jre1.8.0_102\bin\javaw.exe (03-(

```
PLAIN  TEXT : karthikmam
KEY    TEXT : 4
CIPHER TEXT : KKAIMRHATM
PLAIN  TEXT : KARTHIKMAM
```

RESULT:

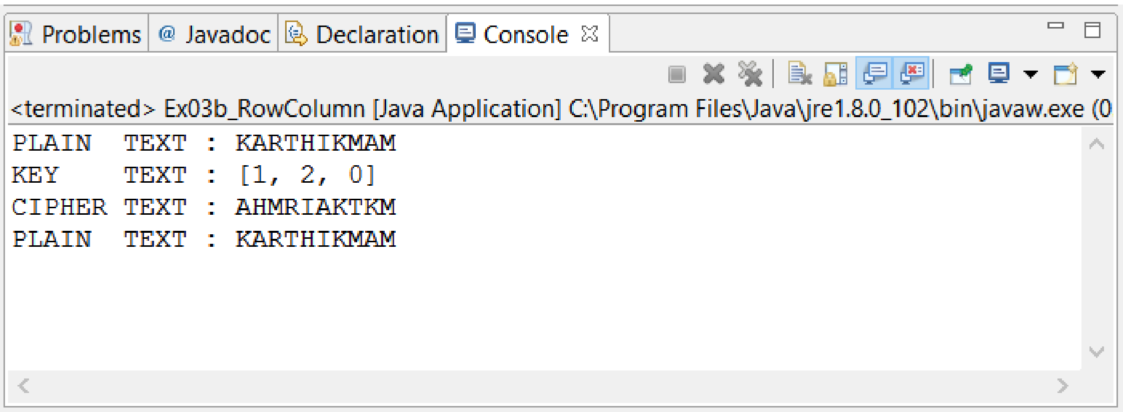
THE RAIL FENCE ALGORITHM WAS SUCCESSFULLY IMPLEMENTED AND TESTED.

EX03B – ROW COLUMN CIPHER

PROGRAM:

```
import java.util.Arrays;

public class Ex03b_RowColumn {
	public static String crypt(String msg, int[] key, boolean encrypt) {
		char[] res = new char[msg.length()];

		for (int i = 0, k = 0; i < key.length; i++)
			for (int j = key[i]; j < msg.length(); j += key.length)
				res[encrypt ? k++ : j] = msg.charAt(encrypt ? j :
k++);

		return new String(res);
	}

	public static void main(String[] args) {
		// TODO Auto-generated method stub

		String plain = "KARTHIKMAM";
		int[] key = { 1, 2, 0 };

		System.out.println("PLAIN  TEXT : " + plain);
		System.out.println("KEY    TEXT : " + Arrays.toString(key));
		System.out.println("CIPHER TEXT : " + crypt(plain, key, true));
		System.out.println("PLAIN  TEXT : "
				+ crypt(crypt(plain, key, true), key, false));

	}

}
```

OUTPUT:



```
<terminated> Ex03b_RowColumn [Java Application] C:\Program Files\Java\jre1.8.0_102\bin\javaw.exe (0
PLAIN  TEXT : KARTHIKMAM
KEY    TEXT : [1, 2, 0]
CIPHER TEXT : AHMRIAKTKM
PLAIN  TEXT : KARTHIKMAM
```

RESULT:

THE ROW COLUMN CIPHER WAS SUCCESSFULLY IMPLEMENTED AND TESTED.

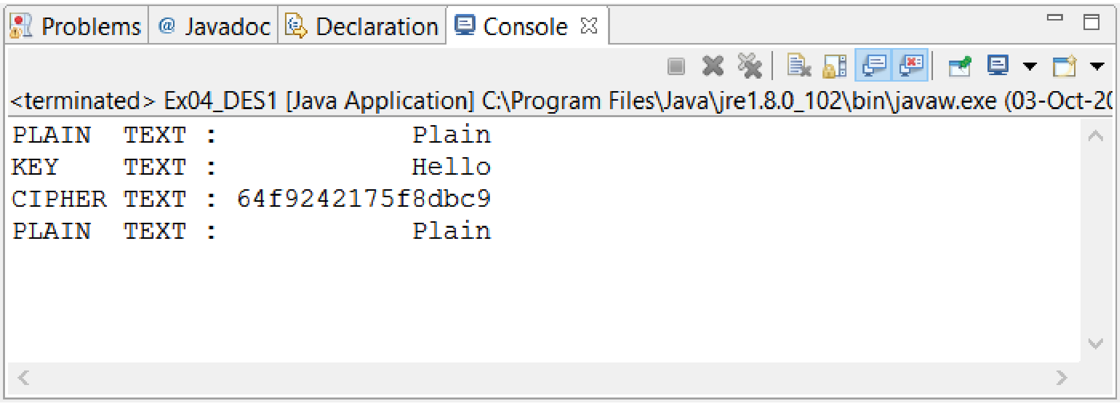
EX04 – DES

PROGRAM:

```
import java.math.BigInteger;

public class Ex04_DES {
      private static final long GET_32B = (1L << 32) - 1;
      private static final long GET_28B = (1L << 28) - 1;
      private static final long GET_56B = (1L << 56) - 1;

      private static final short[] PC1 = {
            57, 49, 41, 33, 25, 17,  9,
             1, 58, 50, 42, 34, 26, 18,
            10,  2, 59, 51, 43, 35, 27,
            19, 11,  3, 60, 52, 44, 36,
            63, 55, 47, 39, 31, 23, 15,
             7, 62, 54, 46, 38, 30, 22,
            14,  6, 61, 53, 45, 37, 29,
            21, 13,  5, 28, 20, 12,  4 };
      private static final short[] PC2 = {
            14, 17, 11, 24,  1,  5,
             3, 28, 15,  6, 21, 10,
            23, 19, 12,  4, 26,  8,
            16,  7, 27, 20, 13,  2,
            41, 52, 31, 37, 47, 55,
            30, 40, 51, 45, 33, 48,
            44, 49, 39, 56, 34, 53,
            46, 42, 50, 36, 29, 32 };
      private static final short[] L_ROT = { 1, 1, 2, 2, 2, 2, 2, 2, 1, 2,
2, 2, 2, 2, 2, 1 };
      private static final short[] IP = {
            58, 50, 42, 34, 26, 18, 10, 2,
            60, 52, 44, 36, 28, 20, 12, 4,
            62, 54, 46, 38, 30, 22, 14, 6,
            64, 56, 48, 40, 32, 24, 16, 8,
            57, 49, 41, 33, 25, 17,  9, 1,
            59, 51, 43, 35, 27, 19, 11, 3,
            61, 53, 45, 37, 29, 21, 13, 5,
            63, 55, 47, 39, 31, 23, 15, 7 };
      private static short[] IP_1 = {
            40, 8, 48, 16, 56, 24, 64, 32,
            39, 7, 47, 15, 55, 23, 63, 31,
            38, 6, 46, 14, 54, 22, 62, 30,
            37, 5, 45, 13, 53, 21, 61, 29,
            36, 4, 44, 12, 52, 20, 60, 28,
            35, 3, 43, 11, 51, 19, 59, 27,
            34, 2, 42, 10, 50, 18, 58, 26,
            33, 1, 41,  9, 49, 17, 57, 25 };
      private static final short[] E = {
            32,  1,  2,  3,  4,  5,
             4,  5,  6,  7,  8,  9,
             8,  9, 10, 11, 12, 13,
            12, 13, 14, 15, 16, 17,
            16, 17, 18, 19, 20, 21,
            20, 21, 22, 23, 24, 25,
            24, 25, 26, 27, 28, 29,
            28, 29, 30, 31, 32,  1 };
      private static long[][] S = {
                  { 14, 4, 13, 1, 2, 15, 11, 8, 3, 10, 6, 12, 5, 9, 0, 7,
0, 15, 7, 4, 14, 2, 13, 1, 10, 6, 12, 11, 9, 5, 3, 8, 4, 1, 14, 8, 13, 6,
2, 11, 15, 12, 9, 7, 3, 10, 5, 0, 15, 12, 8, 2, 4, 9, 1, 7, 5, 11, 3, 14,
10, 0, 6, 13 },
                  { 15, 1, 8, 14, 6, 11, 3, 4, 9, 7, 2, 13, 12, 0, 5, 10,
3, 13, 4, 7, 15, 2, 8, 14, 12, 0, 1, 10, 6, 9, 11, 5, 0, 14, 7, 11, 10, 4,
13, 1, 5, 8, 12, 6, 9, 3, 2, 15, 13, 8, 10, 1, 3, 15, 4, 2, 11, 6, 7, 12,
0, 5, 14, 9 },
                  { 10, 0, 9, 14, 6, 3, 15, 5, 1, 13, 12, 7, 11, 4, 2, 8,
13, 7, 0, 9, 3, 4, 6, 10, 2, 8, 5, 14, 12, 11, 15, 1, 13, 6, 4, 9, 8, 15,
3, 0, 11, 1, 2, 12, 5, 10, 14, 7, 1, 10, 13, 0, 6, 9, 8, 7, 4, 15, 14, 3,
11, 5, 2, 12 },
                  { 7, 13, 14, 3, 0, 6, 9, 10, 1, 2, 8, 5, 11, 12, 4, 15,
13, 8, 11, 5, 6, 15, 0, 3, 4, 7, 2, 12, 1, 10, 14, 9, 10, 6, 9, 0, 12, 11,
7, 13, 15, 1, 3, 14, 5, 2, 8, 4, 3, 15, 0, 6, 10, 1, 13, 8, 9, 4, 5, 11,
12, 7, 2, 14 },
                  { 2, 12, 4, 1, 7, 10, 11, 6, 8, 5, 3, 15, 13, 0, 14, 9,
14, 11, 2, 12, 4, 7, 13, 1, 5, 0, 15, 10, 3, 9, 8, 6, 4, 2, 1, 11, 10, 13,
7, 8, 15, 9, 12, 5, 6, 3, 0, 14, 11, 8, 12, 7, 1, 14, 2, 13, 6, 15, 0, 9,
10, 4, 5, 3 },
                  { 12, 1, 10, 15, 9, 2, 6, 8, 0, 13, 3, 4, 14, 7, 5, 11,
10, 15, 4, 2, 7, 12, 9, 5, 6, 1, 13, 14, 0, 11, 3, 8, 9, 14, 15, 5, 2, 8,
12, 3, 7, 0, 4, 10, 1, 13, 11, 6, 4, 3, 2, 12, 9, 5, 15, 10, 11, 14, 1, 7,
6, 0, 8, 13 },
                  { 4, 11, 2, 14, 15, 0, 8, 13, 3, 12, 9, 7, 5, 10, 6, 1,
13, 0, 11, 7, 4, 9, 1, 10, 14, 3, 5, 12, 2, 15, 8, 6, 1, 4, 11, 13, 12, 3,
7, 14, 10, 15, 6, 8, 0, 5, 9, 2, 6, 11, 13, 8, 1, 4, 10, 7, 9, 5, 0, 15,
14, 2, 3, 12 },
                  { 13, 2, 8, 4, 6, 15, 11, 1, 10, 9, 3, 14, 5, 0, 12, 7,
1, 15, 13, 8, 10, 3, 7, 4, 12, 5, 6, 11, 0, 14, 9, 2, 7, 11, 4, 1, 9, 12,
14, 2, 0, 6, 10, 13, 15, 3, 5, 8, 2, 1, 14, 7, 4, 10, 8, 13, 15, 12, 9, 0,
3, 5, 6, 11 } };
      private static short[] P = {
            16,  7, 20, 21,
            29, 12, 28, 17,
             1, 15, 23, 26,
             5, 18, 31, 10,
             2,  8, 24, 14,
            32, 27,  3,  9,
          19, 13, 30,  6,
            22, 11,  4, 25 };

      private static long mutate(long input, short[] table, long
originalLength) {
            long result = 0;
            for (int i = 0; i < table.length; i++) {
                  result = (result << 1) | (input >>> (originalLength -
table[i]))
                              % 2;
                  // System.out.printf("%x \n", result);
            }
            return result;
      }

      private long[] keys = new long[16];

      public Ex04_DES(long key) {
            long pKey = mutate(key, PC1, 64) & GET_56B;
            long c = pKey >>> 28;
            long d = pKey & GET_28B;

            for (int i = 0; i < 16; i++) {
                  c = ((c << L_ROT[i]) | (c >>> (28 - L_ROT[i]))) &
GET_28B;
                  d = ((d << L_ROT[i]) | (d >>> (28 - L_ROT[i]))) &
GET_28B;
                  keys[i] = mutate((c << 28) | d, PC2, 56);
            }
      }

      public long crypt(long msg, boolean encrypt) {
            msg = mutate(msg, IP, 64);

            long l = msg >>> 32;
            long r = msg & GET_32B;

            for (int i = 0; i < 16; i++) {
                  long temp = r;
                  r = l ^ f(r, keys[encrypt ? i : 16 - i - 1]);
                  l = temp;
                  // System.out.printf("%16s %16s %16x \n",
Long.toHexString(r),
                  // Long.toHexString(l), keys[encrypt ? i : 16 - i - 1]);
            }

            return mutate((r << 32) | l, IP_1, 64);
      }

      private long f(long r, long key) {
            r = mutate(r & GET_32B, E, 32) ^ key;

            long result = 0;
            for (int i = 7; i >= 0; i--) {
                  byte box = (byte) (r & 0x3F);
                  r = r >>> 6;

                  int row = ((box >>> 5) << 1) | (box & 1);
                  int col = (box >>> 1) & 0xF;

                  result |= S[i][row * 16 + col] << (28 - i * 4);
            }

            return mutate(result, P, 32);
      }

      public static void main(String[] args) {
            long plain = new BigInteger("Plain".getBytes()).longValue();
            long key = new BigInteger("Hello".getBytes()).longValue();

            Ex04_DES x = new Ex04_DES(key);

            System.out.printf("PLAIN  TEXT : %16s \n", new String(new
BigInteger(
                        plain + "").toByteArray()));
            System.out.printf("KEY    TEXT : %16s \n", new String(new
BigInteger(
                        key + "").toByteArray()));
            System.out.printf("CIPHER TEXT : %16s \n",
                        Long.toHexString(x.crypt(plain, true)));
            System.out.printf("PLAIN  TEXT : %16s \n", new String(new
BigInteger(""
                        + x.crypt(x.crypt(plain, true),
false)).toByteArray()));
```

```
        }
}
```

OUTPUT:



<terminated> Ex04_DES1 [Java Application] C:\Program Files\Java\jre1.8.0_102\bin\javaw.exe (03-Oct-2(

```
PLAIN  TEXT :             Plain
KEY    TEXT :             Hello
CIPHER TEXT : 64f9242175f8dbc9
PLAIN  TEXT :             Plain
```

RESULT:

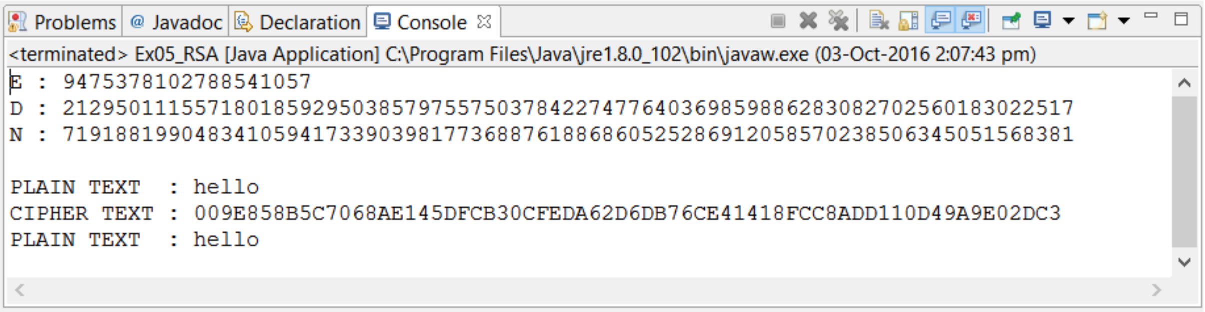
THE DES ALGORITHM WAS SUCCESSFULLY IMPLEMENTED AND TESTED.

EX05 – RSA

PROGRAM:

```java
import java.math.BigInteger;
import java.util.Random;

import javax.xml.bind.DatatypeConverter;

public class Ex05_RSA {

    private static int bitLength = 128;
    private BigInteger n, e, d;

    public Ex05_RSA() {
        Random rnd = new Random();

        BigInteger p = BigInteger.probablePrime(bitLength, rnd);
        BigInteger q = BigInteger.probablePrime(bitLength, rnd);

        this.n = p.multiply(q);
        BigInteger phi = p.subtract(BigInteger.ONE).multiply(
                q.subtract(BigInteger.ONE));

        this.e = BigInteger.probablePrime(bitLength / 2, rnd);
        while (e.gcd(phi).compareTo(BigInteger.ONE) == 1
                && e.compareTo(phi) < 1) {
            e.add(BigInteger.ONE);
        }
        this.d = e.modInverse(phi);

        System.out.println("E : " + e);
        System.out.println("D : " + d);
        System.out.println("N : " + n);
        System.out.println();
    }

    public byte[] crypt(byte[] input, boolean encrypt) {
        return new BigInteger(input).modPow(encrypt ? e : d,
n).toByteArray();
    }

    public static void main(String[] args) {
        Ex05_RSA rsa = new Ex05_RSA();
        String plain = "hello";

        System.out.println("PLAIN TEXT  : " + plain);
        System.out.println("CIPHER TEXT : "
                +
DatatypeConverter.printHexBinary(rsa.crypt(plain.getBytes(),
                        true)));
        System.out.println("PLAIN TEXT  : "
                + new String(
                        rsa.crypt(rsa.crypt(plain.getBytes(),
true), false)));
    }

}
```

OUTPUT:



```
<terminated> Ex05_RSA [Java Application] C:\Program Files\Java\jre1.8.0_102\bin\javaw.exe (03-Oct-2016 2:07:43 pm)
E : 9475378102788541057
D : 2129501115571801859295038579755750378422747764036985988628308270256018302 2517
N : 7191881990483410594173390398177368876188686052528691205857023850634505156 8381

PLAIN TEXT  : hello
CIPHER TEXT : 009E858B5C7068AE145DFCB30CFEDA62D6DB76CE41418FCC8ADD110D49A9E02DC3
PLAIN TEXT  : hello
```

RESULT:

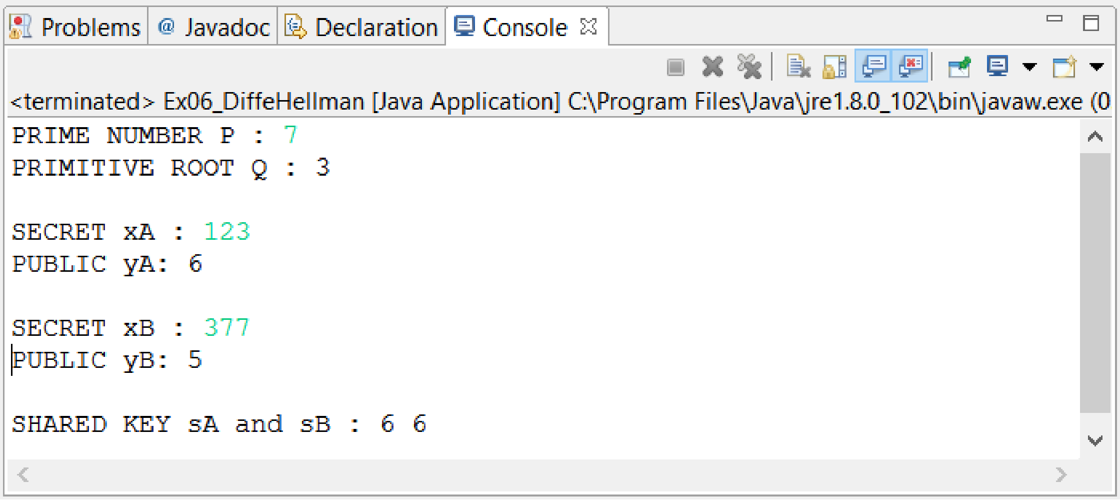
THE RSA ALGORITHM WAS SUCCESSFULLY IMPLEMENTED.

EX06 – DIFFE HELLMAN KEY EXCHANGE ALGORITHM

PROGRAM:

```
import java.math.BigInteger;
import java.util.ArrayList;
import java.util.Scanner;

public class Ex06_DiffeHellman {

        public static ArrayList<BigInteger> getPrimeFactors(BigInteger n) {
                ArrayList<BigInteger> res = new ArrayList<BigInteger>();

                for (BigInteger i = new BigInteger("2"); i.intValue() <
Math.sqrt(n
                                .intValue()); i = i.add(BigInteger.ONE))
                        if (i.isProbablePrime(100) == true && n.mod(i).intValue()
== 0)
                                res.add(i);

                return res;
        }

        public static BigInteger primitiveRoot(BigInteger n) {
                BigInteger phi = n.subtract(BigInteger.ONE);

                ArrayList<BigInteger> primeFactors = getPrimeFactors(phi);
                for (BigInteger i = new BigInteger("2"); i.intValue() <
n.intValue(); i = i
                                .add(BigInteger.ONE)) {
                        boolean flag = true;
                        for (BigInteger j = BigInteger.ZERO; j.intValue() <
primeFactors
                                        .size(); j = j.add(BigInteger.ONE))
                                if
(i.modPow(phi.divide(primeFactors.get(j.intValue())), n)
                                                .longValue() == 1)
                                        flag = false;
                        if (flag == true)
                                return i;
                }

                return BigInteger.ZERO;
        }

        private static Scanner stdIn = new Scanner(System.in);

        public static void main(String[] args) {
                System.out.print("PRIME NUMBER P : ");
                BigInteger p = new BigInteger(stdIn.nextInt() + "");
                BigInteger q = primitiveRoot(p);
                System.out.println("PRIMITIVE ROOT Q : " + q);

                System.out.println();
                System.out.print("SECRET xA : ");
                BigInteger xA = new BigInteger(stdIn.nextInt() + "");
                BigInteger yA = q.modPow(xA, p);
                System.out.println("PUBLIC yA: " + yA);

                System.out.println();
                System.out.print("SECRET xB : ");
                BigInteger xB = new BigInteger(stdIn.nextInt() + "");
                BigInteger yB = q.modPow(xB, p);
                System.out.println("PUBLIC yB: " + yB);

                System.out.println();
                BigInteger sharedKeyA = yB.modPow(xA, p);
                BigInteger sharedKeyB = yA.modPow(xB, p);
                System.out.println("SHARED KEY sA and sB : " + sharedKeyA + " "
                            + sharedKeyB);
        }

}
```

OUTPUT:



```
<terminated> Ex06_DiffeHellman [Java Application] C:\Program Files\Java\jre1.8.0_102\bin\javaw.exe (0
PRIME NUMBER P : 7
PRIMITIVE ROOT Q : 3

SECRET xA : 123
PUBLIC yA: 6

SECRET xB : 377
PUBLIC yB: 5

SHARED KEY sA and sB : 6 6
```

RESULT:

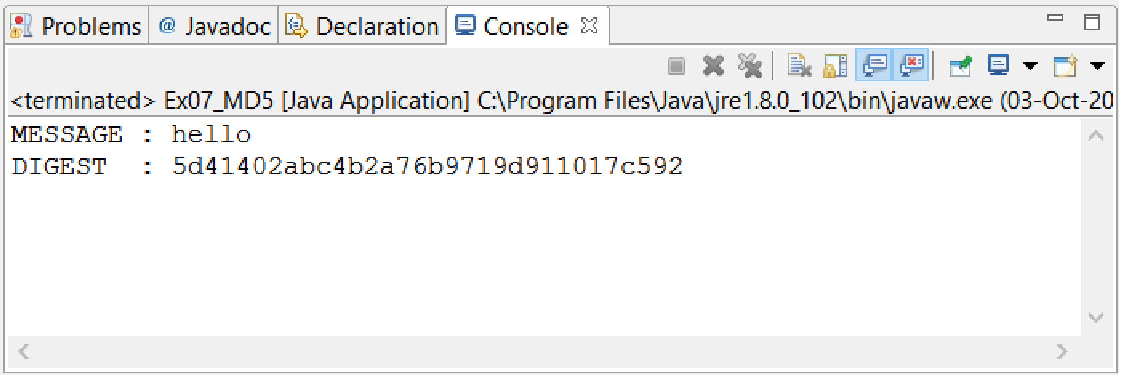
THE DH ALGORITHM WAS SUCCESSFULLY IMPLEMENTED.

EX07 – MD5 HASH ALGORITHM

PROGRAM:

```
import java.util.Arrays;

public class Ex07_MD5 {
      private static final int[][] S = {
            { 7, 12, 17, 22 },
            { 5,  9, 14, 20 },
            { 4, 11, 16, 23 },
            { 6, 10, 15, 21 }
      };
      private static final int[] T;
      static {
            T = new int[64];
            for(int i = 0; i < 64; i++)
                  T[i] = (int) (long) ((1L << 32) * Math.abs(Math.sin(i +
1)));
      }

      private static final int F(int x, int y, int z) { return (x & y) |
(~x & z); }
      private static final int G(int x, int y, int z) { return (x & z) | (y
& ~z); }
      private static final int H(int x, int y, int z) { return (x ^ y ^ z);
}
      private static final int I(int x, int y, int z) { return y ^ (x |
~z); }

      private static final int R(int n, int i) { return (n << i) | (n >>>
(32 - i)); }

      public static String digest(String msg) {
            int[] words = new int[(int) (((long) msg.length() + (64 -
msg.length() % 64)) / 4)];

            for (int i = 0; i < msg.length(); i++)
                  words[i >>> 2] |= msg.charAt(i) << (24 - (i % 4) * 8);
            words[msg.length() >>> 2] |= 0x80 << (24 - (msg.length() % 4) *
8);

            for (int i = 0; i < words.length; i++)
                  words[i] = Integer.reverseBytes(words[i]);

            words[words.length - 2] = msg.length() * 8;
            words[words.length - 1] = (int) ((msg.length() * 8) / (1L <<
32));

            int a = Integer.reverseBytes(0x01234567);
            int b = Integer.reverseBytes(0x89abcdef);
            int c = Integer.reverseBytes(0xfedcba98);
            int d = Integer.reverseBytes(0x76543210);

            for (int i = 0; i < words.length / 16; i += 16) {
                  int[] word = Arrays.copyOfRange(words, i, i + 16);

                  int aa = a;
                  int bb = b;
                  int cc = c;
                  int dd = d;
                  int count = -1;

                  for (int j = 0, inc = -1; j < 4; j++) {
                        a = b + R((a + F(b, c, d) + word[inc = ((inc + 1) %
16)] + T[count += 1] ), S[0][0]);
                        d = a + R((d + F(a, b, c) + word[inc = ((inc + 1) %
16)] + T[count += 1] ), S[0][1]);
                        c = d + R((c + F(d, a, b) + word[inc = ((inc + 1) %
16)] + T[count += 1] ), S[0][2]);
                        b = c + R((b + F(c, d, a) + word[inc = ((inc + 1) %
16)] + T[count += 1] ), S[0][3]);
                  }

                  for (int j = 0, inc = -4; j < 4; j++) {
                        a = b + R((a + G(b, c, d) + word[inc = ((inc + 5) %
16)] + T[count += 1] ), S[1][0]);
                        d = a + R((d + G(a, b, c) + word[inc = ((inc + 5) %
16)] + T[count += 1] ), S[1][1]);
                        c = d + R((c + G(d, a, b) + word[inc = ((inc + 5) %
16)] + T[count += 1] ), S[1][2]);
                        b = c + R((b + G(c, d, a) + word[inc = ((inc + 5) %
16)] + T[count += 1] ), S[1][3]);
                  }

                  for (int j = 0, inc = 2; j < 4; j++) {
                        a = b + R((a + H(b, c, d) + word[inc = ((inc + 3) %
16)] + T[count += 1] ), S[2][0]);
                        d = a + R((d + H(a, b, c) + word[inc = ((inc + 3) %
16)] + T[count += 1] ), S[2][1]);
                        c = d + R((c + H(d, a, b) + word[inc = ((inc + 3) %
16)] + T[count += 1] ), S[2][2]);
                        b = c + R((b + H(c, d, a) + word[inc = ((inc + 3) %
16)] + T[count += 1] ), S[2][3]);
                  }

                  for (int j = 0, inc = -7; j < 4; j++) {
                        a = b + R((a + I(b, c, d) + word[inc = ((inc + 7) %
16)] + T[count += 1] ), S[3][0]);
                        d = a + R((d + I(a, b, c) + word[inc = ((inc + 7) %
16)] + T[count += 1] ), S[3][1]);
                        c = d + R((c + I(d, a, b) + word[inc = ((inc + 7) %
16)] + T[count += 1] ), S[3][2]);
                        b = c + R((b + I(c, d, a) + word[inc = ((inc + 7) %
16)] + T[count += 1] ), S[3][3]);
                  }

                  a = a + aa;
                  b = b + bb;
                  c = c + cc;
                  d = d + dd;
            }

            return String.format("%x%x%x%x",
                        Integer.reverseBytes(a),
                        Integer.reverseBytes(b),
                        Integer.reverseBytes(c),
                        Integer.reverseBytes(d));
      }

      public static void main(String[] args) {
            String msg = "hello";

            System.out.println("MESSAGE : " + msg);
            System.out.println("DIGEST  : " + digest(msg));
      }
}
```

OUTPUT:



<terminated> Ex07_MD5 [Java Application] C:\Program Files\Java\jre1.8.0_102\bin\javaw.exe (03-Oct-20

```
MESSAGE : hello
DIGEST  : 5d41402abc4b2a76b9719d911017c592
```

RESULT:

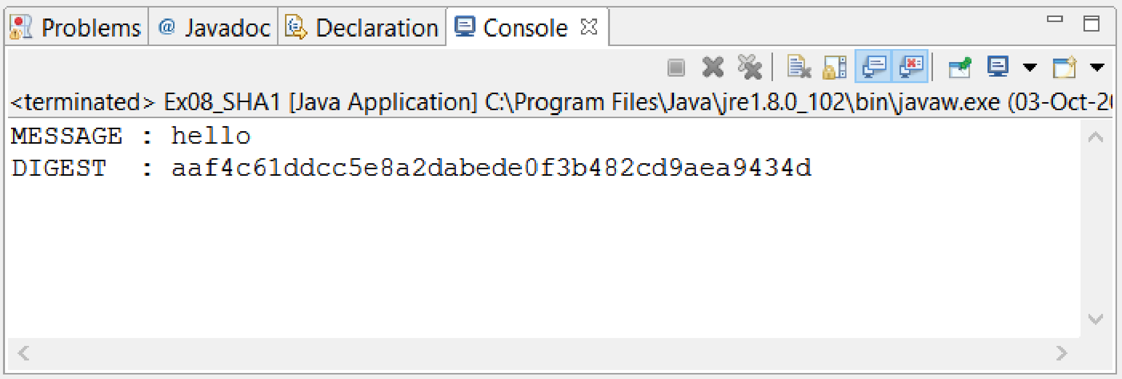
THE MD5 HASH ALGORITHM WAS SUCCESSFULLY IMPLEMENTED.

EX08 – SHA1 ALGORITHM

PROGRAM:

```
public class Ex08_SHA1 {

        private static int R(int n, int i) {
                return (n << i) | (n >>> (32 - i));
        }

        public static String digest(String msg) {
                int[] words = new int[(int) (((long) msg.length() + (64 -
msg.length() % 64)) / 4)];

                for (int i = 0; i < msg.length(); i++)
                        words[i >>> 2] |= msg.charAt(i) << (24 - (i % 4) * 8);

                words[msg.length() >>> 2] |= 0x80 << (24 - (msg.length() % 4) *
8);

                words[words.length - 1] = msg.length() * 8;

                int[] w = new int[80];

                int h0 = Integer.reverseBytes(0x01234567);
                int h1 = Integer.reverseBytes(0x89abcdef);
                int h2 = Integer.reverseBytes(0xfedcba98);
                int h3 = Integer.reverseBytes(0x76543210);
                int h4 = Integer.reverseBytes(0xf0e1d2c3);

                for (int i = 0; i < words.length; i += 16) {
                        int a = h0;
                        int b = h1;
                        int c = h2;
                        int d = h3;
                        int e = h4;

                        for (int j = 0; j < 80; j++) {
                                w[j] = (j < 16) ? words[i + j] : (R(w[j - 3]
                                        ^ w[j - 8] ^ w[j - 14] ^ w[j - 16], 1));

                                int t = R(a, 5) + e + w[j] +
                        ( j < 20 ? (0x5a827999 + ((b & c) | ((~b) & d)))
                        : j < 40 ? (0x6ed9eba1 + (b ^ c ^ d))
                        : j < 60 ? (0x8f1bbcdc + ((b & c) | (b & d) | (c & d)))
                        : (0xca62c1d6 + (b ^ c ^ d)));
                                e = d;
                                d = c;
                                c = R(b, 30);
                                b = a;
                                a = t;
                        }

                        h0 += a;
                        h1 += b;
                        h2 += c;
                        h3 += d;
                        h4 += e;
                }

                return String.format("%x%x%x%x%x", h0, h1, h2, h3, h4);
        }
        public static void main(String args[]) {
                String msg = "hello";

                System.out.println("MESSAGE : " + msg);
                System.out.println("DIGEST  : " + digest(msg));
        }
}
```

OUTPUT:



<terminated> Ex08_SHA1 [Java Application] C:\Program Files\Java\jre1.8.0_102\bin\javaw.exe (03-Oct-2(

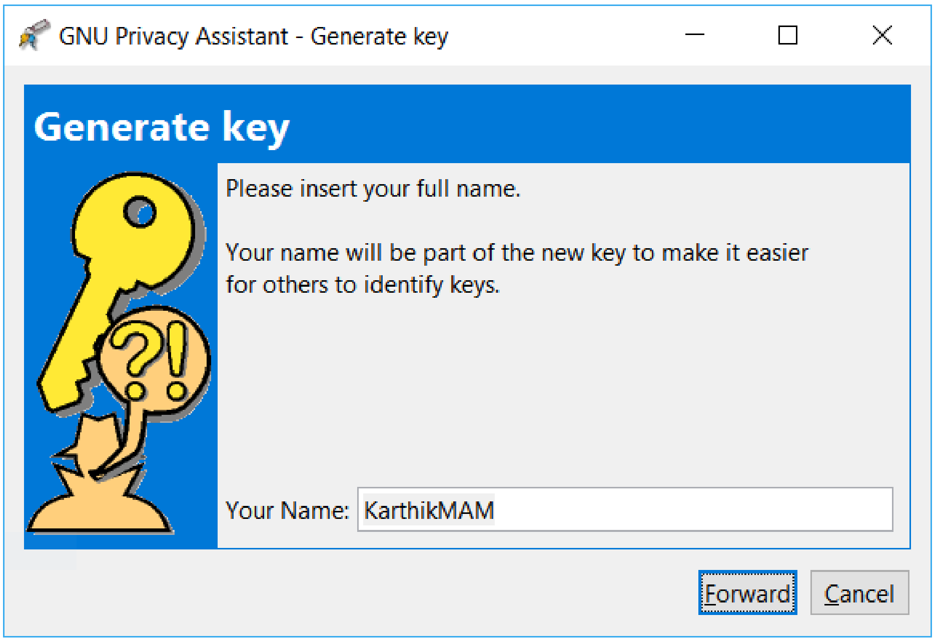
```
MESSAGE : hello
DIGEST  : aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d
```

RESULT:

THE SHA1 ALGORITHM WAS SUCCESSFULLY IMPLMENETED.

Ex 9 – PGP - GPG4Win

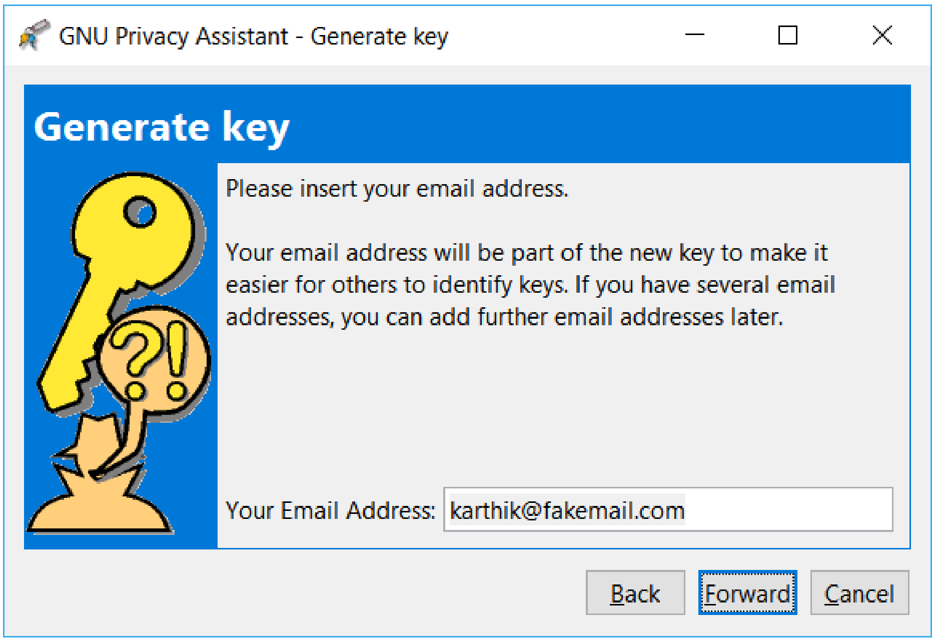
Public-Private Key Generation and Backup:



Please insert your full name.

Your name will be part of the new key to make it easier for others to identify keys.

Your Name: KarthikMAM

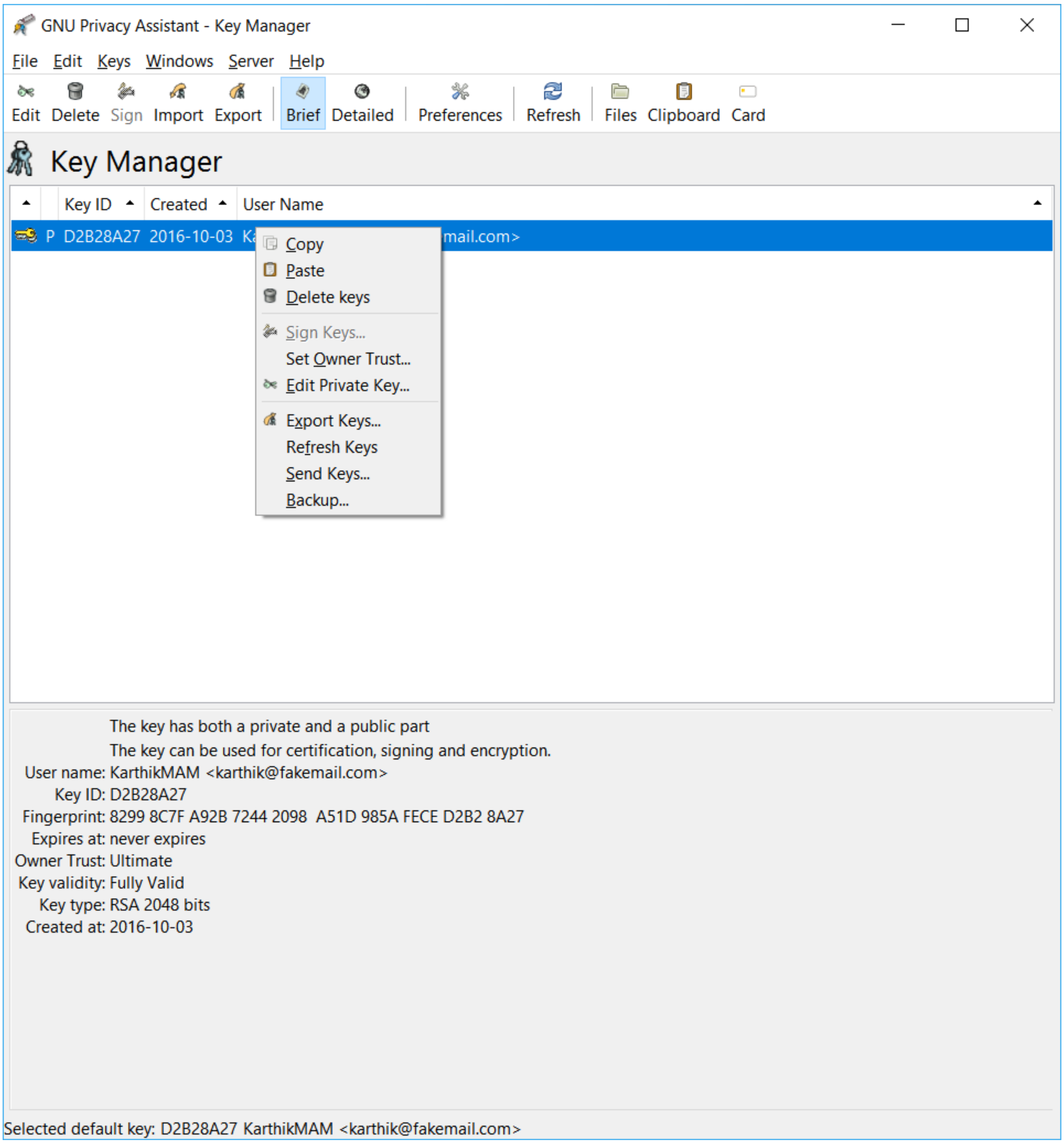


Please insert your email address.

Your email address will be part of the new key to make it easier for others to identify keys. If you have several email addresses, you can add further email addresses later.

Your Email Address: karthik@fakemail.com

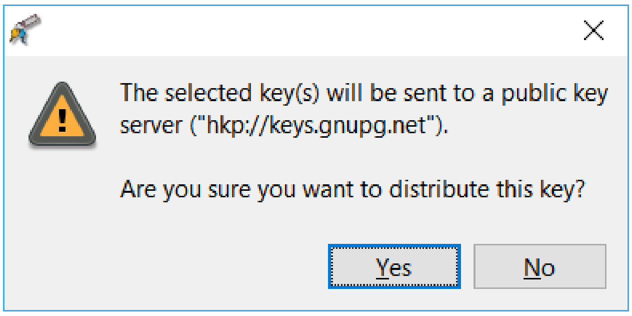
Distributing Public Key using hkp://keys.gnupg.net Public Key server:


GNU Privacy Assistant - Key Manager
File Edit Keys Windows Server Help
Edit Delete Sign Import Export Brief Detailed Preferences Refresh Files Clipboard Card
Key Manager
Key ID Created User Name
Copy
Paste
Delete keys
Sign Keys...
Set Owner Trust...
Edit Private Key...
Export Keys...
Refresh Keys
Send Keys...
Backup...

P D2B28A27 2016-10-03 Ka mail.com>

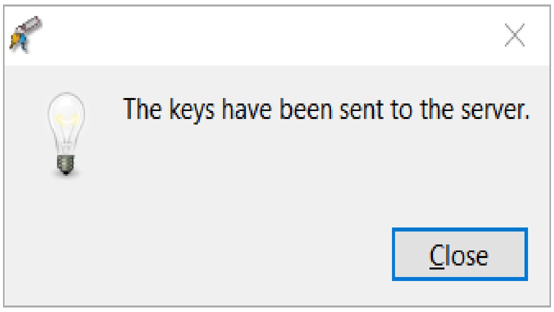
The key has both a private and a public part
The key can be used for certification, signing and encryption.
User name: KarthikMAM <karthik@fakemail.com>
Key ID: D2B28A27
Fingerprint: 8299 8C7F A92B 7244 2098 A51D 985A FECE D2B2 8A27
Expires at: never expires
Owner Trust: Ultimate
Key validity: Fully Valid
Key type: RSA 2048 bits
Created at: 2016-10-03

Selected default key: D2B28A27 KarthikMAM <karthik@fakemail.com>



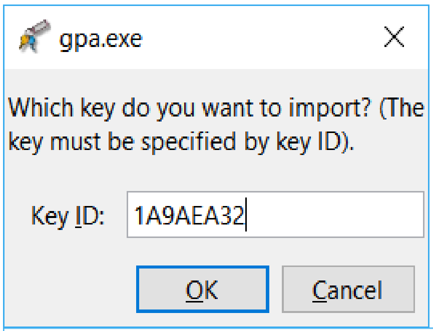
The selected key(s) will be sent to a public key server ("hkp://keys.gnupg.net").

Are you sure you want to distribute this key?



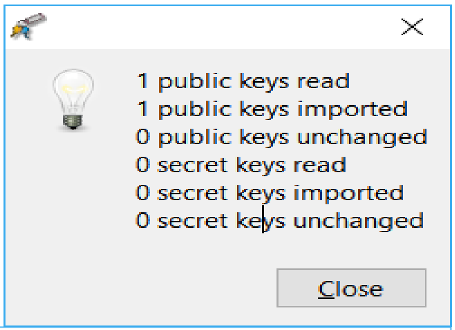
The keys have been sent to the server.

Retrieve keys from the server:

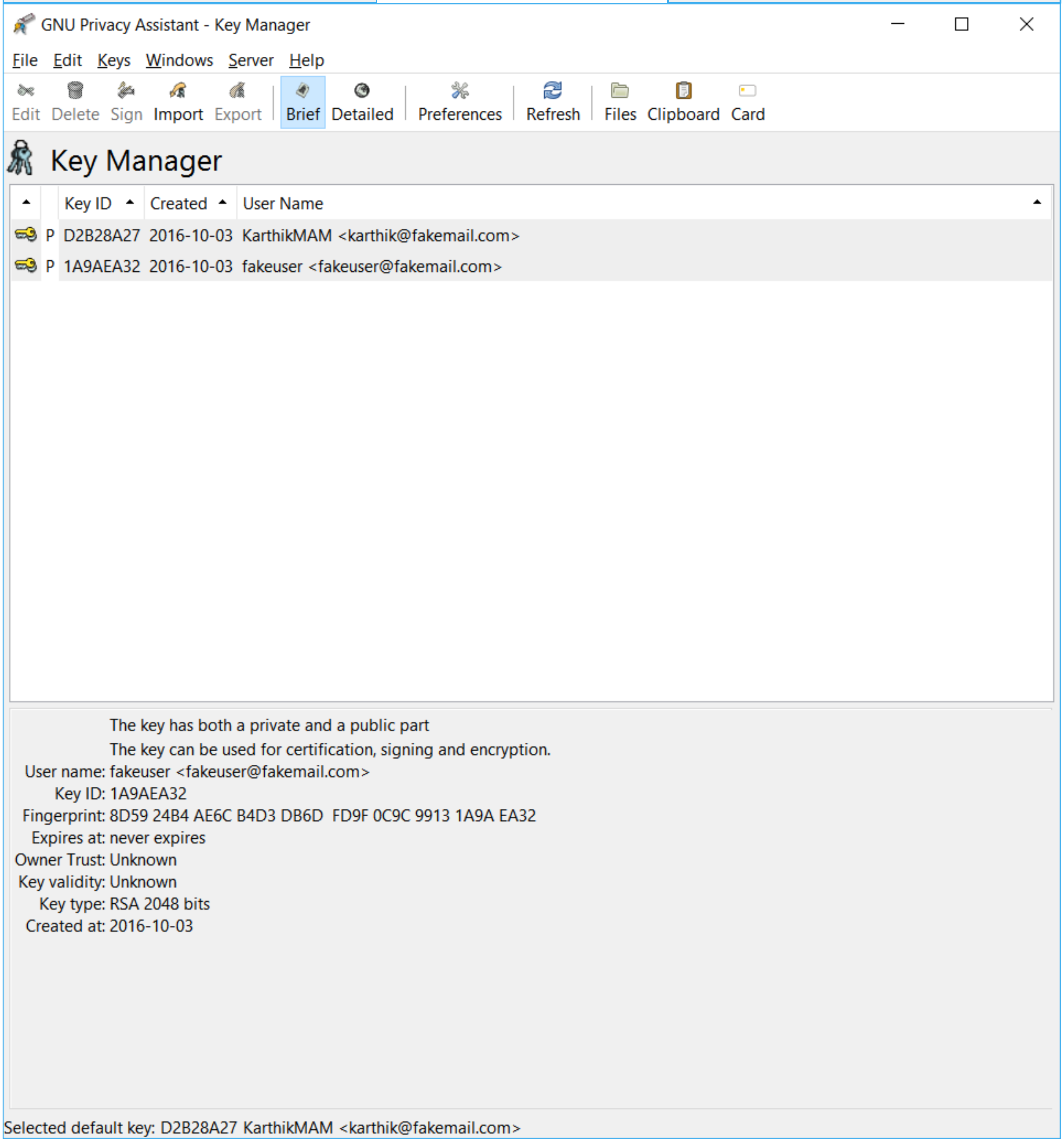


Which key do you want to import? (The key must be specified by key ID).

Key ID: 1A9AEA32



1 public keys read
1 public keys imported
0 public keys unchanged
0 secret keys read
0 secret keys imported
0 secret keys unchanged

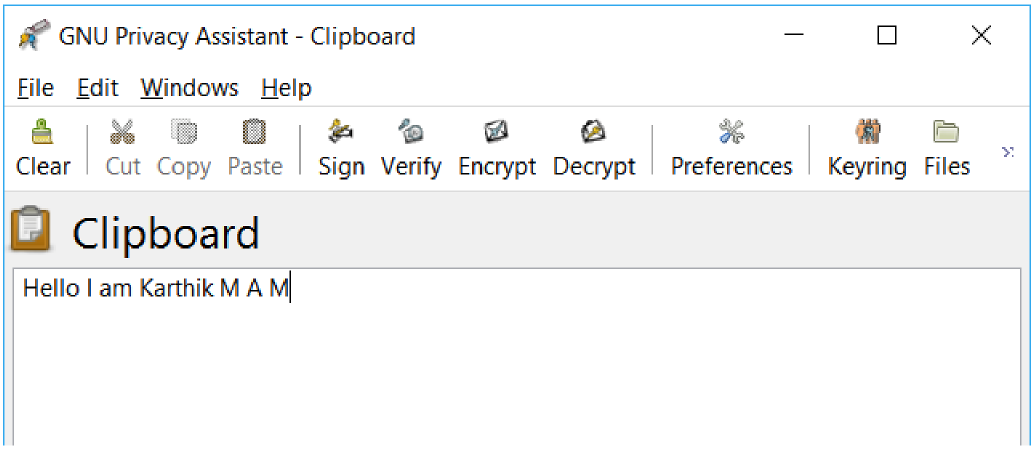

GNU Privacy Assistant - Key Manager
File Edit Keys Windows Server Help
Edit Delete Sign Import Export Brief Detailed Preferences Refresh Files Clipboard Card
Key Manager

		Key ID	Created	User Name
	P	D2B28A27	2016-10-03	KarthikMAM <karthik@fakemail.com>
	P	1A9AEA32	2016-10-03	fakeuser <fakeuser@fakemail.com>

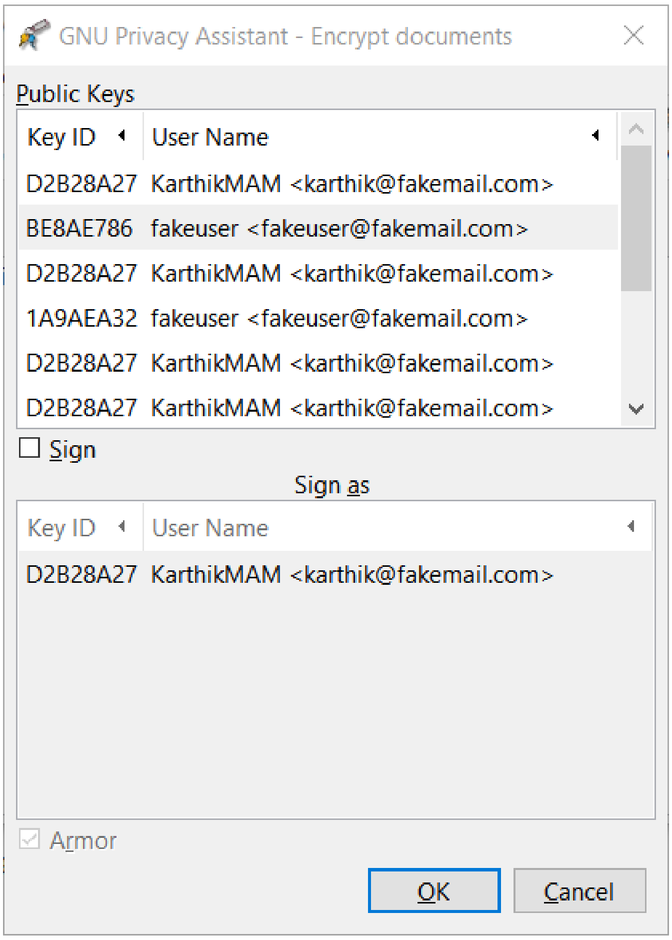
The key has both a private and a public part
The key can be used for certification, signing and encryption.
User name: fakeuser <fakeuser@fakemail.com>
Key ID: 1A9AEA32
Fingerprint: 8D59 24B4 AE6C B4D3 DB6D FD9F 0C9C 9913 1A9A EA32
Expires at: never expires
Owner Trust: Unknown
Key validity: Unknown
Key type: RSA 2048 bits
Created at: 2016-10-03

Selected default key: D2B28A27 KarthikMAM <karthik@fakemail.com>

Encrypting at Sender side:



Hello I am Karthik M A M



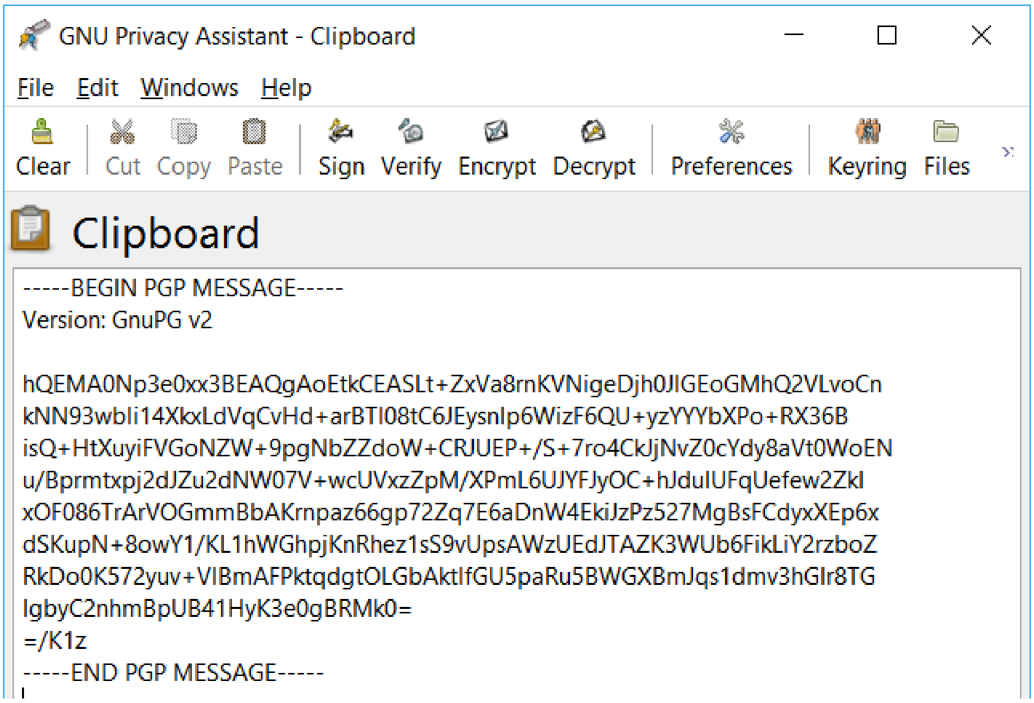
Key ID	User Name
D2B28A27	KarthikMAM <karthik@fakemail.com>
BE8AE786	fakeuser <fakeuser@fakemail.com>
D2B28A27	KarthikMAM <karthik@fakemail.com>
1A9AEA32	fakeuser <fakeuser@fakemail.com>
D2B28A27	KarthikMAM <karthik@fakemail.com>
D2B28A27	KarthikMAM <karthik@fakemail.com>

□ Sign

Sign as

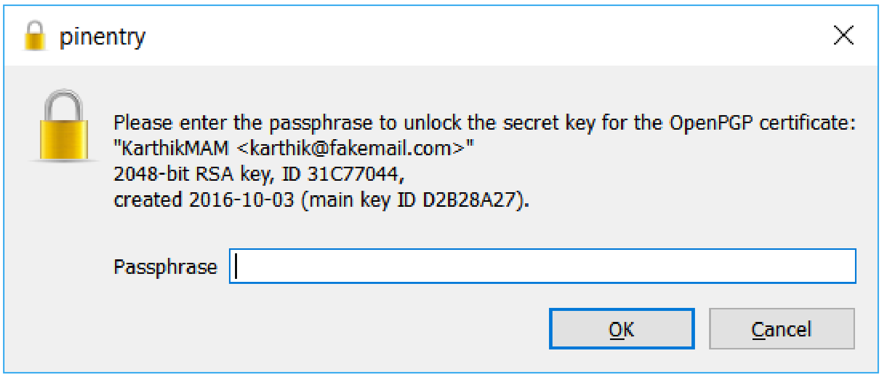
Key ID	User Name
D2B28A27	KarthikMAM <karthik@fakemail.com>

☑ Armor

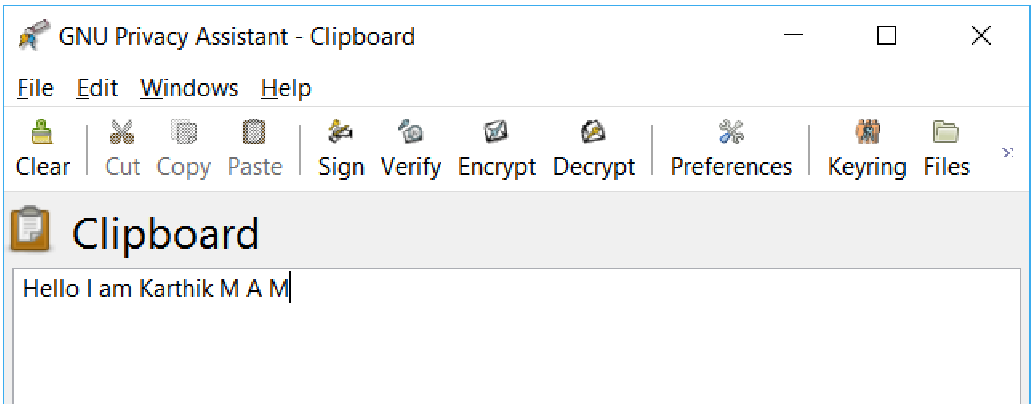


```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v2

hQEMA0Np3e0xx3BEAQgAoEtkCEASLt+ZxVa8rnKVNigeDjh0JIGEoGMhQ2VLvoCn
kNN93wbli14XkxLdVqCvHd+arBTI08tC6JEysnlp6WizF6QU+yzYYYbXPo+RX36B
isQ+HtXuyiFVGoNZW+9pgNbZZdoW+CRJUEP+/S+7ro4CkJjNvZ0cYdy8aVt0WoEN
u/Bprmtxpj2dJZu2dNW07V+wcUVxzZpM/XPmL6UJYFJyOC+hJduIUFqUefew2Zkl
xOF086TrArVOGmmBbAKrnpaz66gp72Zq7E6aDnW4EkiJzPz527MgBsFCdyxXEp6x
dSKupN+8owY1/KL1hWGhpjKnRhez1sS9vUpsAWzUEdJTAZK3WUb6FikLiY2rzboZ
RkDo0K572yuv+VIBmAFPktqdgtOLGbAktIfGU5paRu5BWGXBmJqs1dmv3hGlr8TG
IgbyC2nhmBpUB41HyK3e0gBRMk0=
=/K1z
-----END PGP MESSAGE-----
```

Decrypting at receiver side:



Please enter the passphrase to unlock the secret key for the OpenPGP certificate:
"KarthikMAM <karthik@fakemail.com>"
2048-bit RSA key, ID 31C77044,
created 2016-10-03 (main key ID D2B28A27).



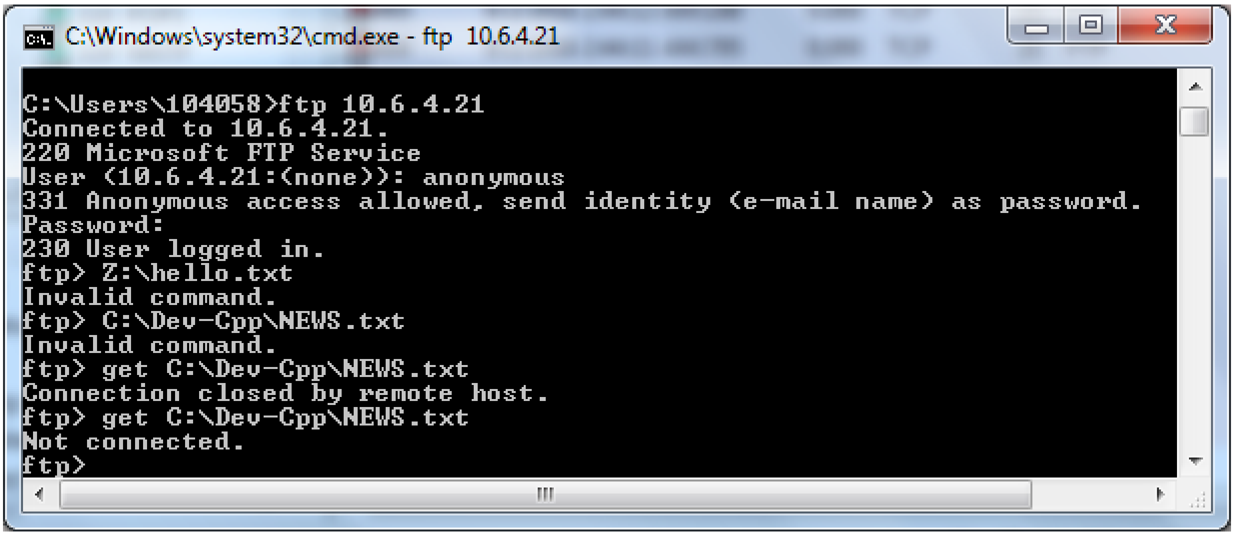
Hello I am Karthik M A M

Result:

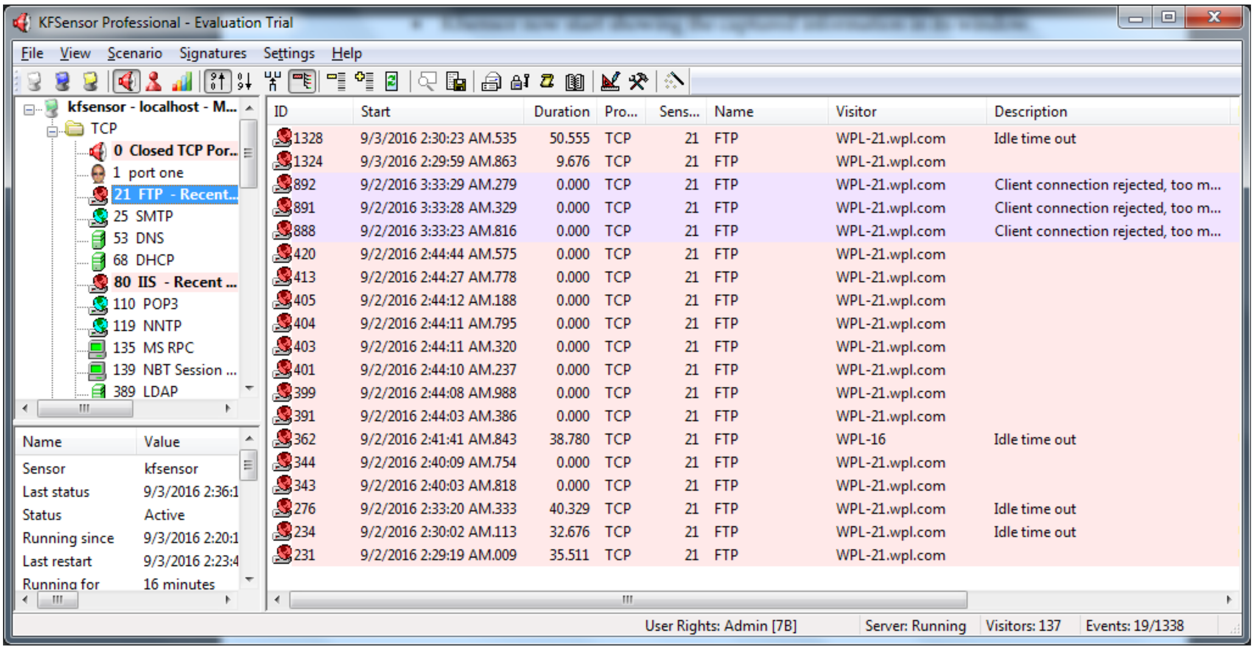
The GPA tool was used to

- **Create public – private key pair**
- **Share and retrieve public keys**
- **Encrypt and decrypt using them.**

FTP



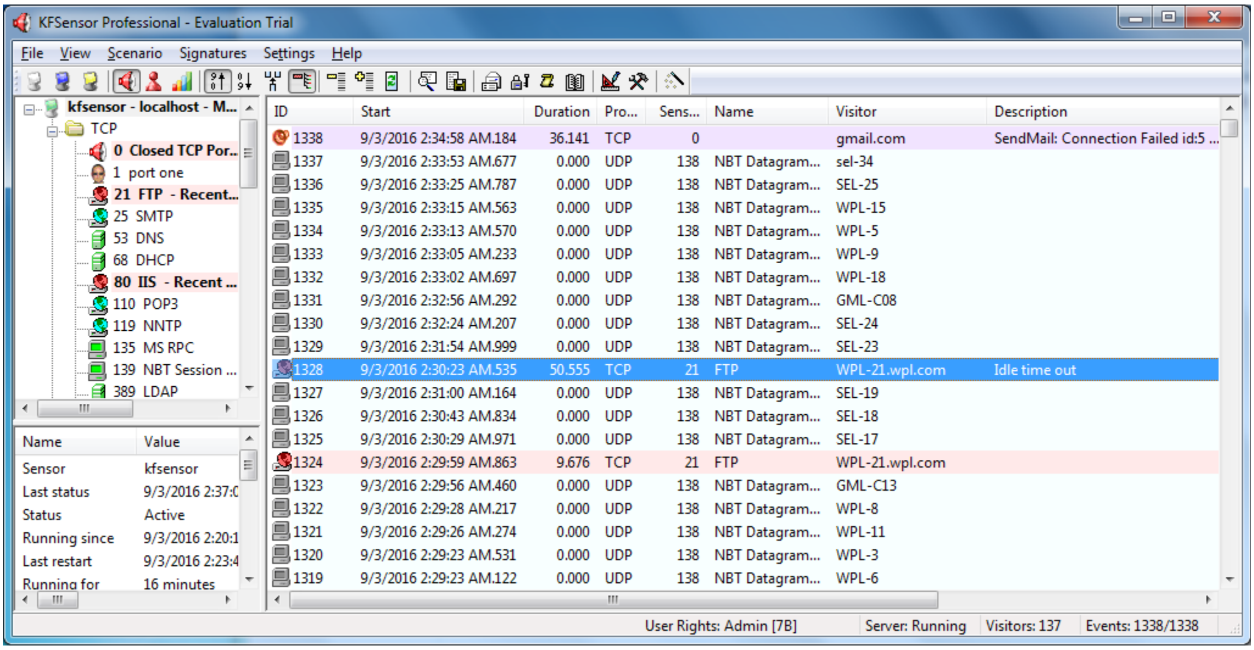
```
C:\Users\104058>ftp 10.6.4.21
Connected to 10.6.4.21.
220 Microsoft FTP Service
User (10.6.4.21:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
ftp> Z:\hello.txt
Invalid command.
ftp> C:\Dev-Cpp\NEWS.txt
Invalid command.
ftp> get C:\Dev-Cpp\NEWS.txt
Connection closed by remote host.
ftp> get C:\Dev-Cpp\NEWS.txt
Not connected.
ftp>
```



Name	Value
Sensor	kfsensor
Last status	9/3/2016 2:36:1
Status	Active
Running since	9/3/2016 2:20:1
Last restart	9/3/2016 2:23:4
Running for	16 minutes

ID	Start	Duration	Pro...	Sens...	Name	Visitor	Description
1328	9/3/2016 2:30:23 AM.535	50.555	TCP	21	FTP	WPL-21.wpl.com	Idle time out
1324	9/3/2016 2:29:59 AM.863	9.676	TCP	21	FTP	WPL-21.wpl.com	
892	9/2/2016 3:33:29 AM.279	0.000	TCP	21	FTP	WPL-21.wpl.com	Client connection rejected, too m...
891	9/2/2016 3:33:28 AM.329	0.000	TCP	21	FTP	WPL-21.wpl.com	Client connection rejected, too m...
888	9/2/2016 3:33:23 AM.816	0.000	TCP	21	FTP	WPL-21.wpl.com	Client connection rejected, too m...
420	9/2/2016 2:44:44 AM.575	0.000	TCP	21	FTP	WPL-21.wpl.com	
413	9/2/2016 2:44:27 AM.778	0.000	TCP	21	FTP	WPL-21.wpl.com	
405	9/2/2016 2:44:12 AM.188	0.000	TCP	21	FTP	WPL-21.wpl.com	
404	9/2/2016 2:44:11 AM.795	0.000	TCP	21	FTP	WPL-21.wpl.com	
403	9/2/2016 2:44:11 AM.320	0.000	TCP	21	FTP	WPL-21.wpl.com	
401	9/2/2016 2:44:10 AM.237	0.000	TCP	21	FTP	WPL-21.wpl.com	
399	9/2/2016 2:44:08 AM.988	0.000	TCP	21	FTP	WPL-21.wpl.com	
391	9/2/2016 2:44:03 AM.386	0.000	TCP	21	FTP	WPL-21.wpl.com	
362	9/2/2016 2:41:41 AM.843	38.780	TCP	21	FTP	WPL-16	Idle time out
344	9/2/2016 2:40:09 AM.754	0.000	TCP	21	FTP	WPL-21.wpl.com	
343	9/2/2016 2:40:03 AM.818	0.000	TCP	21	FTP	WPL-21.wpl.com	
276	9/2/2016 2:33:20 AM.333	40.329	TCP	21	FTP	WPL-21.wpl.com	Idle time out
234	9/2/2016 2:30:02 AM.113	32.676	TCP	21	FTP	WPL-21.wpl.com	Idle time out
231	9/2/2016 2:29:19 AM.009	35.511	TCP	21	FTP	WPL-21.wpl.com	

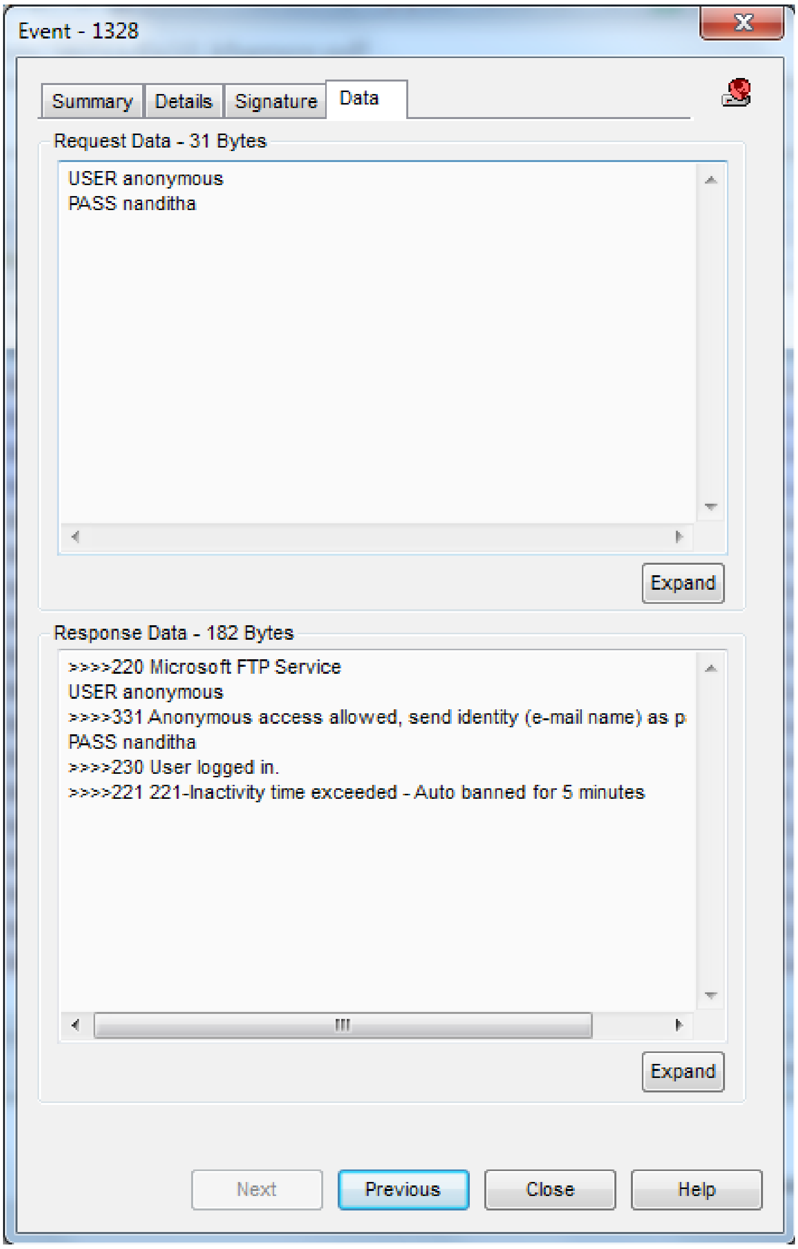
User Rights: Admin [7B]   Server: Running   Visitors: 137   Events: 19/1338



Name	Value
Sensor	kfsensor
Last status	9/3/2016 2:37:(
Status	Active
Running since	9/3/2016 2:20:1
Last restart	9/3/2016 2:23:4
Running for	16 minutes

ID	Start	Duration	Pro...	Sens...	Name	Visitor	Description
1338	9/3/2016 2:34:58 AM.184	36.141	TCP	0		gmail.com	SendMail: Connection Failed id:5 ...
1337	9/3/2016 2:33:53 AM.677	0.000	UDP	138	NBT Datagram...	sel-34	
1336	9/3/2016 2:33:25 AM.787	0.000	UDP	138	NBT Datagram...	SEL-25	
1335	9/3/2016 2:33:15 AM.563	0.000	UDP	138	NBT Datagram...	WPL-15	
1334	9/3/2016 2:33:13 AM.570	0.000	UDP	138	NBT Datagram...	WPL-5	
1333	9/3/2016 2:33:05 AM.233	0.000	UDP	138	NBT Datagram...	WPL-9	
1332	9/3/2016 2:33:02 AM.697	0.000	UDP	138	NBT Datagram...	WPL-18	
1331	9/3/2016 2:32:56 AM.292	0.000	UDP	138	NBT Datagram...	GML-C08	
1330	9/3/2016 2:32:24 AM.207	0.000	UDP	138	NBT Datagram...	SEL-24	
1329	9/3/2016 2:31:54 AM.999	0.000	UDP	138	NBT Datagram...	SEL-23	
1328	9/3/2016 2:30:23 AM.535	50.555	TCP	21	FTP	WPL-21.wpl.com	Idle time out
1327	9/3/2016 2:31:00 AM.164	0.000	UDP	138	NBT Datagram...	SEL-19	
1326	9/3/2016 2:30:43 AM.834	0.000	UDP	138	NBT Datagram...	SEL-18	
1325	9/3/2016 2:30:29 AM.971	0.000	UDP	138	NBT Datagram...	SEL-17	
1324	9/3/2016 2:29:59 AM.863	9.676	TCP	21	FTP	WPL-21.wpl.com	
1323	9/3/2016 2:29:56 AM.460	0.000	UDP	138	NBT Datagram...	GML-C13	
1322	9/3/2016 2:29:28 AM.217	0.000	UDP	138	NBT Datagram...	WPL-8	
1321	9/3/2016 2:29:26 AM.274	0.000	UDP	138	NBT Datagram...	WPL-11	
1320	9/3/2016 2:29:23 AM.531	0.000	UDP	138	NBT Datagram...	WPL-3	
1319	9/3/2016 2:29:23 AM.122	0.000	UDP	138	NBT Datagram...	WPL-6	

User Rights: Admin [7B] Server: Running Visitors: 137 Events: 1338/1338

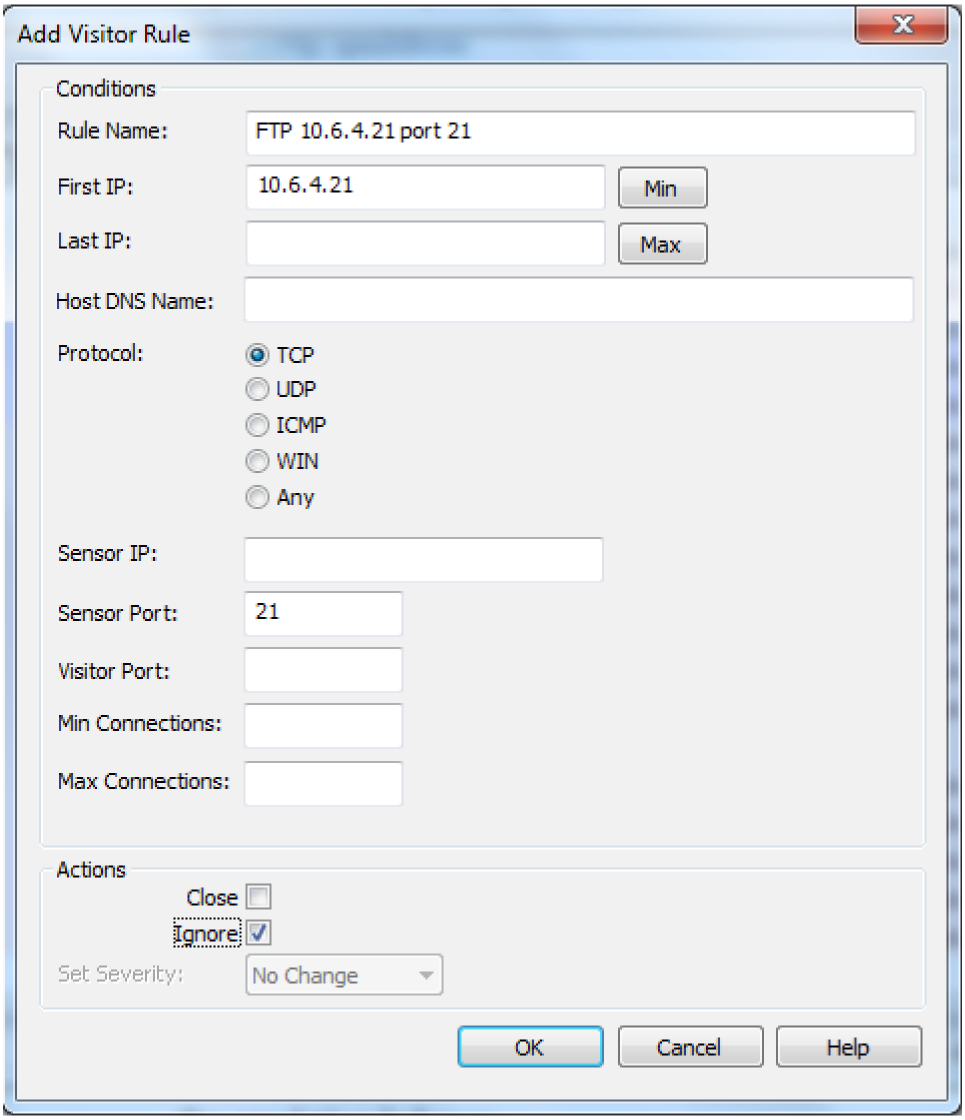


Request Data - 31 Bytes

```
USER anonymous
PASS nanditha
```

Response Data - 182 Bytes

```
>>>>220 Microsoft FTP Service
USER anonymous
>>>>331 Anonymous access allowed, send identity (e-mail name) as p
PASS nanditha
>>>>230 User logged in.
>>>>221 221-Inactivity time exceeded - Auto banned for 5 minutes
```



Conditions

Rule Name: FTP 10.6.4.21 port 21

First IP: 10.6.4.21

Last IP:

Host DNS Name:

Protocol:
● TCP
○ UDP
○ ICMP
○ WIN
○ Any

Sensor IP:

Sensor Port: 21

Visitor Port:

Min Connections:

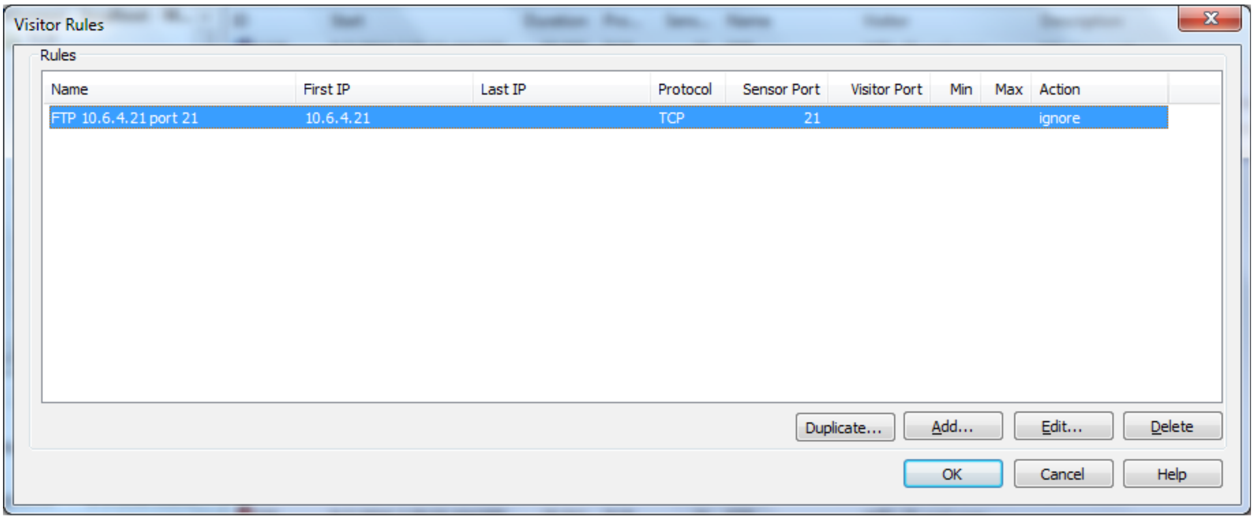
Max Connections:

Actions

Close ☐

Ignore ☑

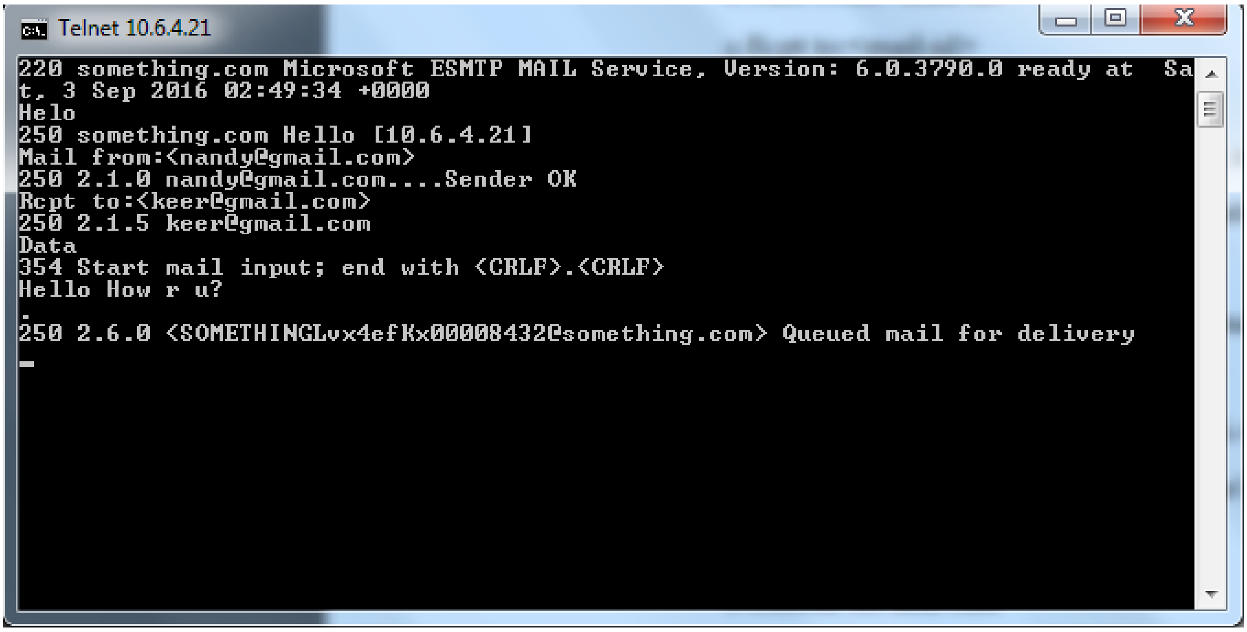
Set Severity: No Change



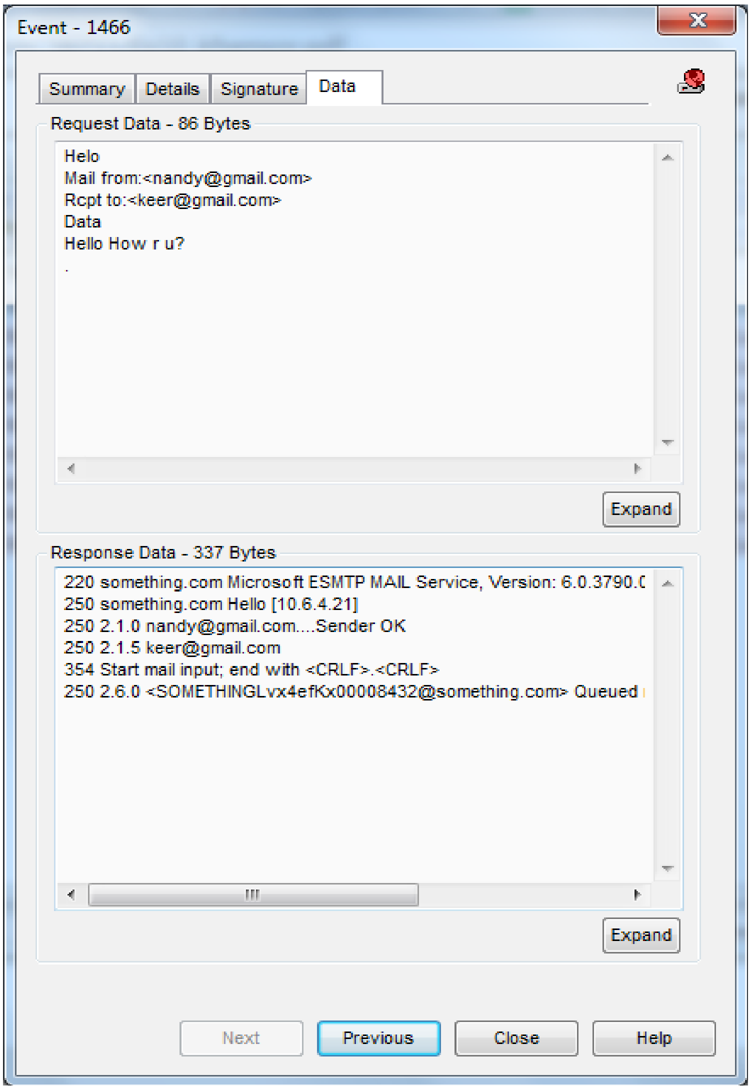
Rules

Name	First IP	Last IP	Protocol	Sensor Port	Visitor Port	Min	Max	Action
FTP 10.6.4.21 port 21	10.6.4.21		TCP	21				ignore

SMTP



```
220 something.com Microsoft ESMTP MAIL Service, Version: 6.0.3790.0 ready at  Sa
t, 3 Sep 2016 02:49:34 +0000
Helo
250 something.com Hello [10.6.4.21]
Mail from:<nandy@gmail.com>
250 2.1.0 nandy@gmail.com....Sender OK
Rcpt to:<keer@gmail.com>
250 2.1.5 keer@gmail.com
Data
354 Start mail input; end with <CRLF>.<CRLF>
Hello How r u?
.
250 2.6.0 <SOMETHINGLvx4efKx00008432@something.com> Queued mail for delivery
_
```



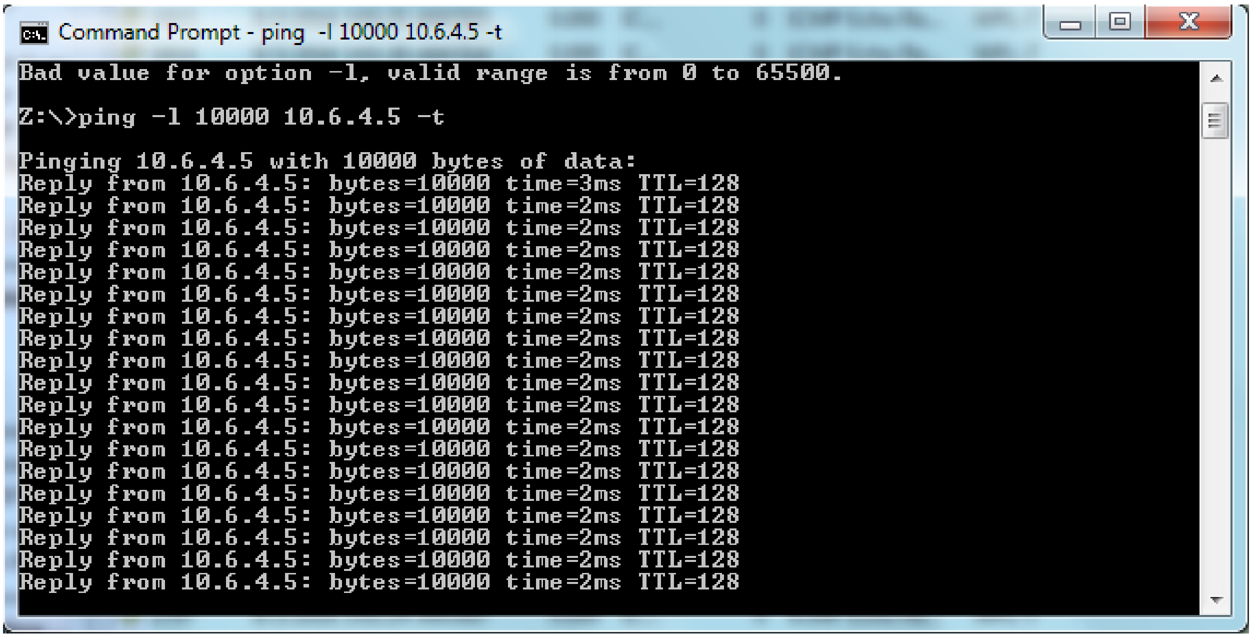
Request Data - 86 Bytes

```
Helo
Mail from:<nandy@gmail.com>
Rcpt to:<keer@gmail.com>
Data
Hello How r u?
.
```

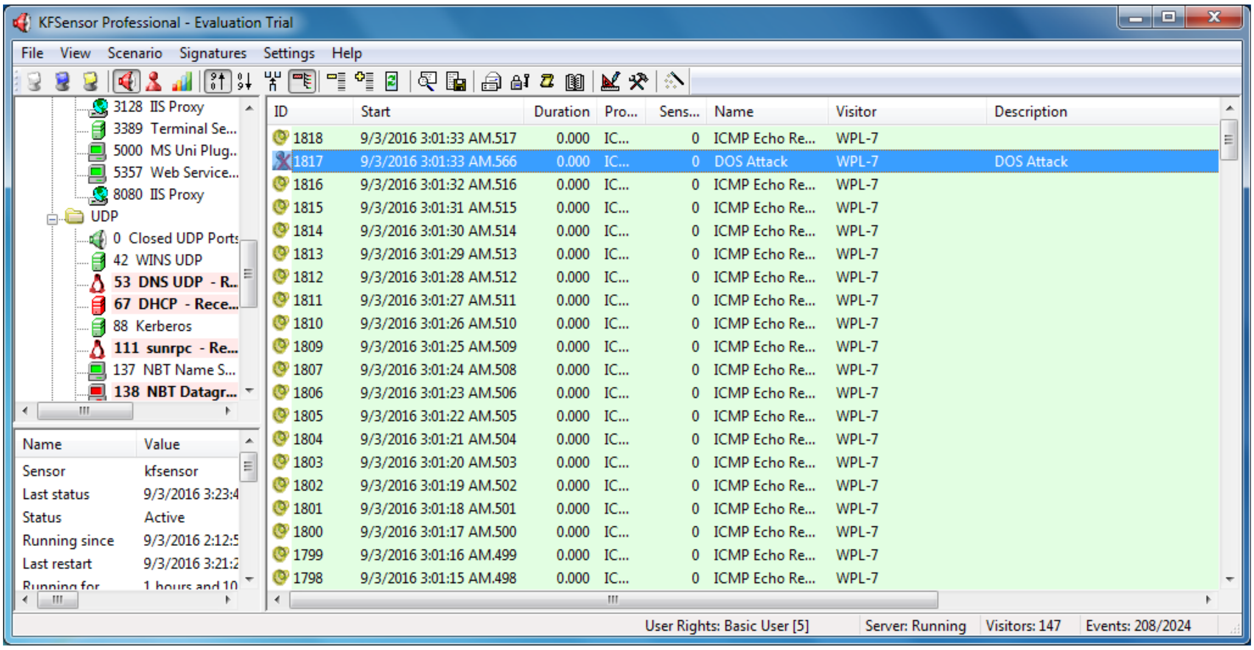
Response Data - 337 Bytes

```
220 something.com Microsoft ESMTP MAIL Service, Version: 6.0.3790.(
250 something.com Hello [10.6.4.21]
250 2.1.0 nandy@gmail.com....Sender OK
250 2.1.5 keer@gmail.com
354 Start mail input; end with <CRLF>.<CRLF>
250 2.6.0 <SOMETHINGLvx4efKx00008432@something.com> Queued
```

DOS



```
Bad value for option -l, valid range is from 0 to 65500.

Z:\>ping -l 10000 10.6.4.5 -t

Pinging 10.6.4.5 with 10000 bytes of data:
Reply from 10.6.4.5: bytes=10000 time=3ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
```

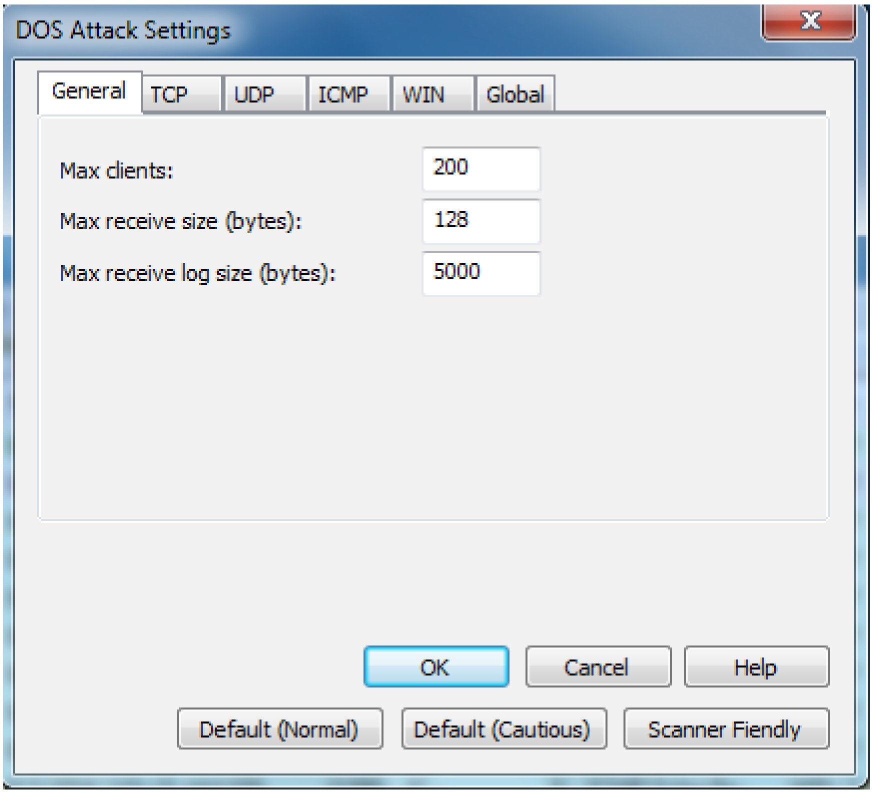


3128 IIS Proxy
3389 Terminal Se...
5000 MS Uni Plug..
5357 Web Service...
8080 IIS Proxy
UDP
0 Closed UDP Ports
42 WINS UDP
53 DNS UDP - R...
67 DHCP - Rece...
88 Kerberos
111 sunrpc - Re...
137 NBT Name S...
138 NBT Datagr...

Name	Value
Sensor	kfsensor
Last status	9/3/2016 3:23:4
Status	Active
Running since	9/3/2016 2:12:5
Last restart	9/3/2016 3:21:2
Running for	1 hours and 10

ID	Start	Duration	Pro...	Sens...	Name	Visitor	Description
1818	9/3/2016 3:01:33 AM.517	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1817	9/3/2016 3:01:33 AM.566	0.000	IC...	0	DOS Attack	WPL-7	DOS Attack
1816	9/3/2016 3:01:32 AM.516	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1815	9/3/2016 3:01:31 AM.515	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1814	9/3/2016 3:01:30 AM.514	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1813	9/3/2016 3:01:29 AM.513	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1812	9/3/2016 3:01:28 AM.512	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1811	9/3/2016 3:01:27 AM.511	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1810	9/3/2016 3:01:26 AM.510	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1809	9/3/2016 3:01:25 AM.509	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1807	9/3/2016 3:01:24 AM.508	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1806	9/3/2016 3:01:23 AM.506	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1805	9/3/2016 3:01:22 AM.505	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1804	9/3/2016 3:01:21 AM.504	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1803	9/3/2016 3:01:20 AM.503	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1802	9/3/2016 3:01:19 AM.502	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1801	9/3/2016 3:01:18 AM.501	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1800	9/3/2016 3:01:17 AM.500	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1799	9/3/2016 3:01:16 AM.499	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1798	9/3/2016 3:01:15 AM.498	0.000	IC...	0	ICMP Echo Re...	WPL-7	

User Rights: Basic User [5] Server: Running Visitors: 147 Events: 208/2024

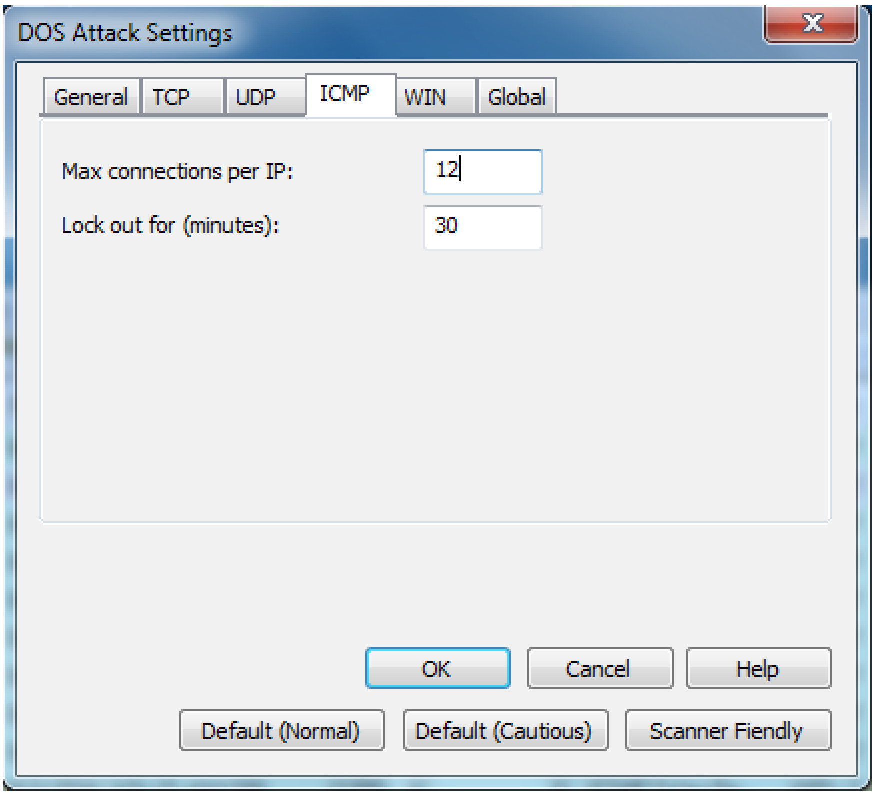


DOS Attack Settings

Max clients: 200

Max receive size (bytes): 128

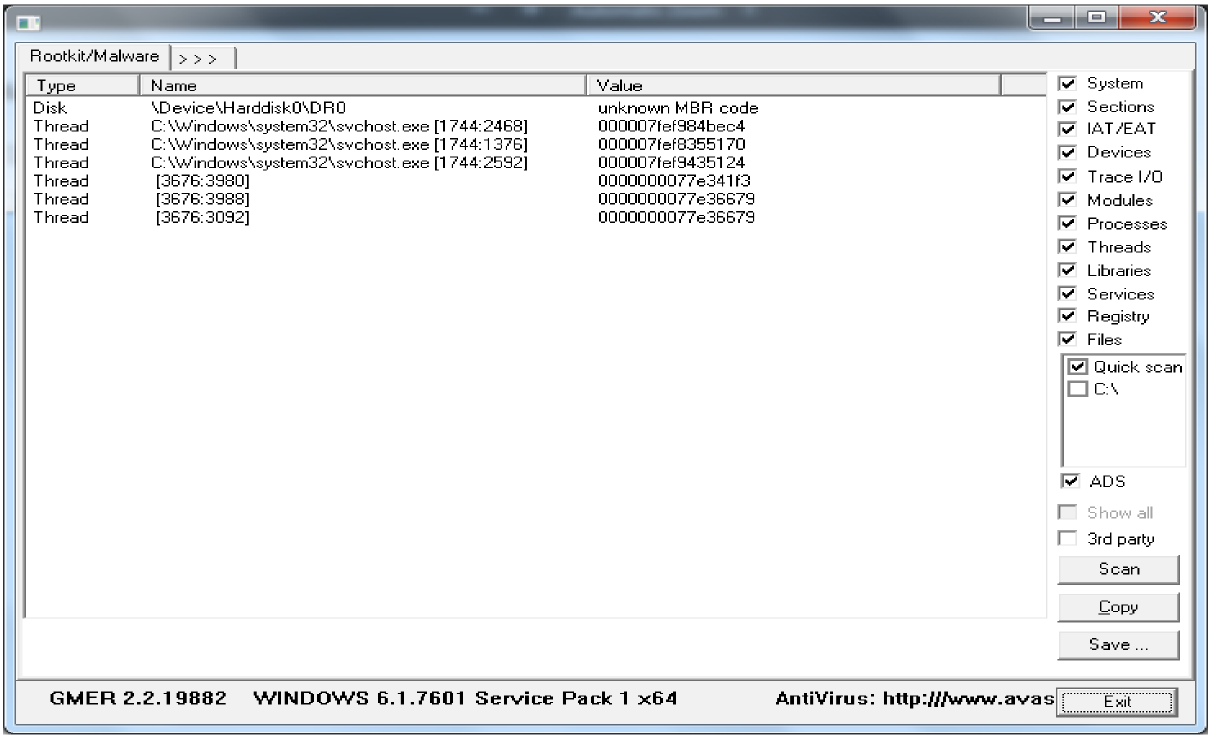
Max receive log size (bytes): 5000



DOS Attack Settings

Max connections per IP: 12

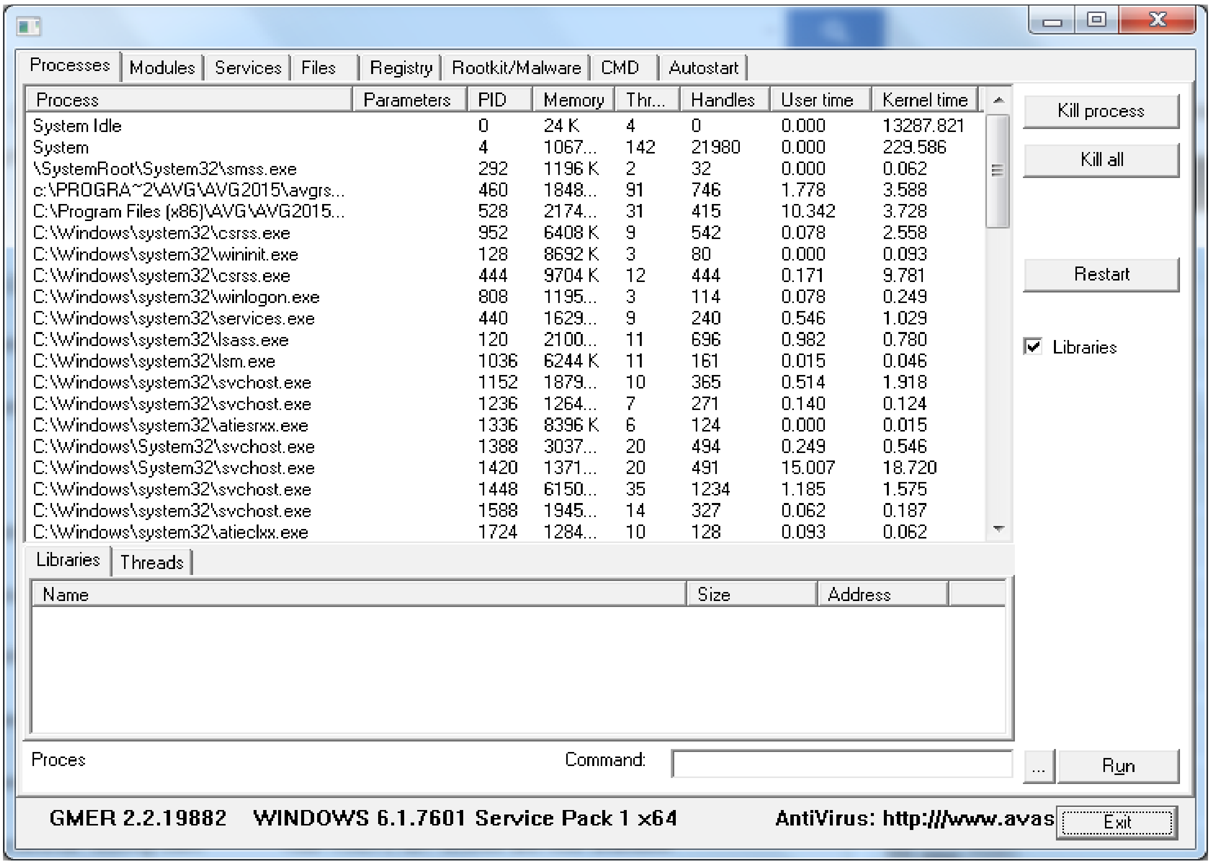
Lock out for (minutes): 30



Type	Name	Value
Disk	\Device\Harddisk0\DR0	unknown MBR code
Thread	C:\Windows\system32\svchost.exe [1744:2468]	000007fef984bec4
Thread	C:\Windows\system32\svchost.exe [1744:1376]	000007fef8355170
Thread	C:\Windows\system32\svchost.exe [1744:2592]	000007fef9435124
Thread	[3676:3980]	0000000077e341f3
Thread	[3676:3988]	0000000077e36679
Thread	[3676:3092]	0000000077e36679

☑ System
☑ Sections
☑ IAT/EAT
☑ Devices
☑ Trace I/O
☑ Modules
☑ Processes
☑ Threads
☑ Libraries
☑ Services
☑ Registry
☑ Files
☑ Quick scan
☐ C:\
☑ ADS
☐ Show all
☐ 3rd party

GMER 2.2.19882 WINDOWS 6.1.7601 Service Pack 1 x64 AntiVirus: http://www.avas



Process	Parameters	PID	Memory	Thr...	Handles	User time	Kernel time
System Idle		0	24 K	4	0	0.000	13287.821
System		4	1067...	142	21980	0.000	229.586
\SystemRoot\System32\smss.exe		292	1196 K	2	32	0.000	0.062
c:\PROGRA~2\AVG\AVG2015\avgrs...		460	1848...	91	746	1.778	3.588
C:\Program Files (x86)\AVG\AVG2015...		528	2174...	31	415	10.342	3.728
C:\Windows\system32\csrss.exe		952	6408 K	9	542	0.078	2.558
C:\Windows\system32\wininit.exe		128	8692 K	3	80	0.000	0.093
C:\Windows\system32\csrss.exe		444	9704 K	12	444	0.171	9.781
C:\Windows\system32\winlogon.exe		808	1195...	3	114	0.078	0.249
C:\Windows\system32\services.exe		440	1629...	9	240	0.546	1.029
C:\Windows\system32\lsass.exe		120	2100...	11	696	0.982	0.780
C:\Windows\system32\lsm.exe		1036	6244 K	11	161	0.015	0.046
C:\Windows\system32\svchost.exe		1152	1879...	10	365	0.514	1.918
C:\Windows\system32\svchost.exe		1236	1264...	7	271	0.140	0.124
C:\Windows\system32\atiesrxx.exe		1336	8396 K	6	124	0.000	0.015
C:\Windows\System32\svchost.exe		1388	3037...	20	494	0.249	0.546
C:\Windows\System32\svchost.exe		1420	1371...	20	491	15.007	18.720
C:\Windows\system32\svchost.exe		1448	6150...	35	1234	1.185	1.575
C:\Windows\system32\svchost.exe		1588	1945...	14	327	0.062	0.187
C:\Windows\system32\atieclxx.exe		1724	1284...	10	128	0.093	0.062

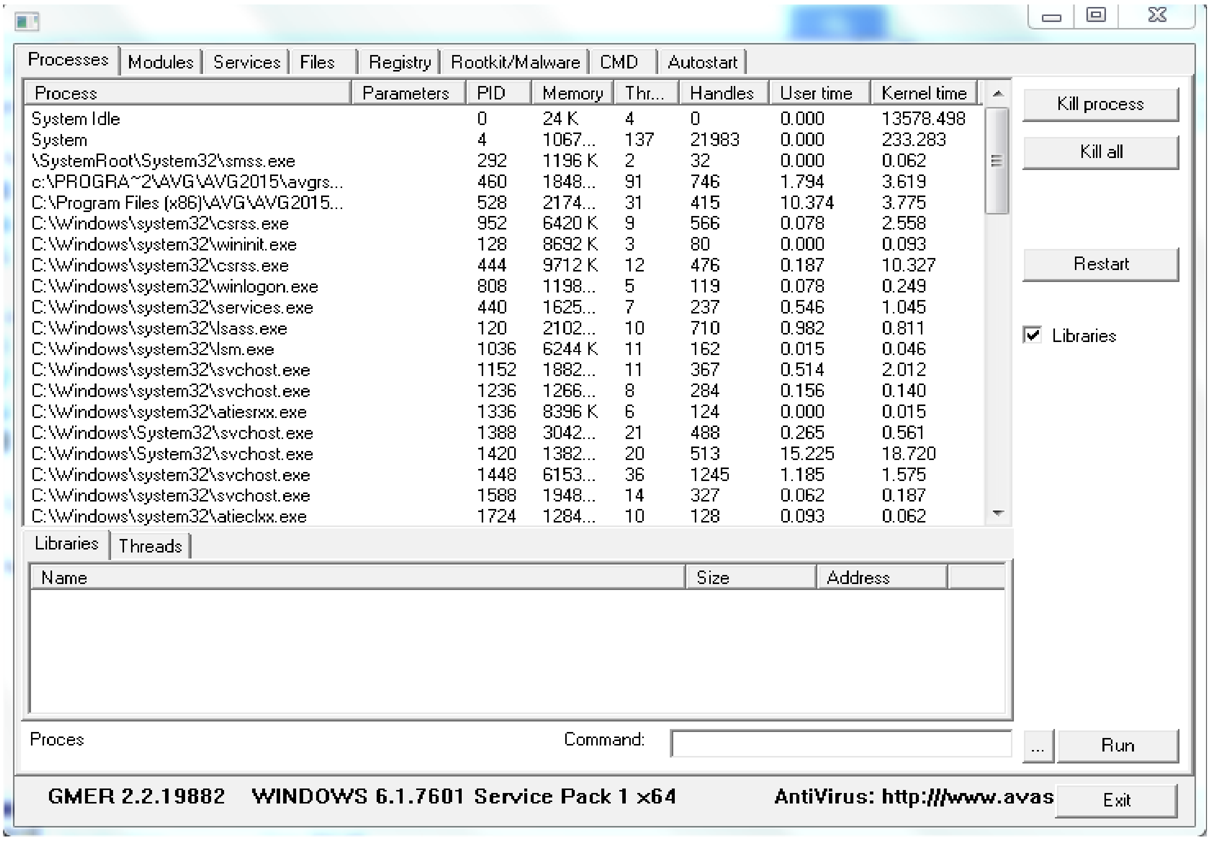
☑ Libraries

Name	Size	Address

Proces

Command:

GMER 2.2.19882 WINDOWS 6.1.7601 Service Pack 1 x64 AntiVirus: http://www.avas

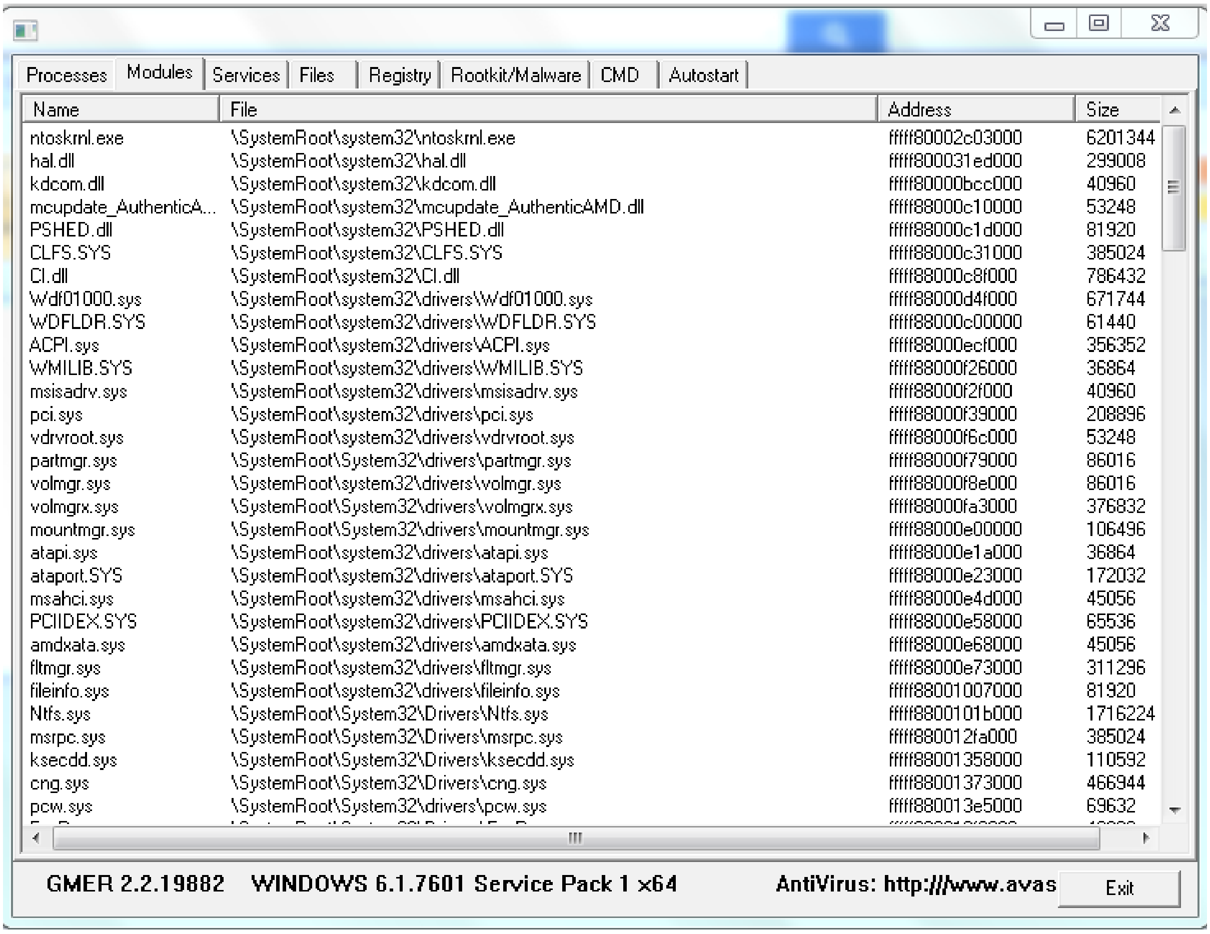


Process	Parameters	PID	Memory	Thr...	Handles	User time	Kernel time
System Idle		0	24 K	4	0	0.000	13578.498
System		4	1067...	137	21983	0.000	233.283
\SystemRoot\System32\smss.exe		292	1196 K	2	32	0.000	0.062
c:\PROGRA~2\AVG\AVG2015\avgrs...		460	1848...	91	746	1.794	3.619
C:\Program Files (x86)\AVG\AVG2015...		528	2174...	31	415	10.374	3.775
C:\Windows\system32\csrss.exe		952	6420 K	9	566	0.078	2.558
C:\Windows\system32\wininit.exe		128	8692 K	3	80	0.000	0.093
C:\Windows\system32\csrss.exe		444	9712 K	12	476	0.187	10.327
C:\Windows\system32\winlogon.exe		808	1198...	5	119	0.078	0.249
C:\Windows\system32\services.exe		440	1625...	7	237	0.546	1.045
C:\Windows\system32\lsass.exe		120	2102...	10	710	0.982	0.811
C:\Windows\system32\lsm.exe		1036	6244 K	11	162	0.015	0.046
C:\Windows\system32\svchost.exe		1152	1882...	11	367	0.514	2.012
C:\Windows\system32\svchost.exe		1236	1266...	8	284	0.156	0.140
C:\Windows\system32\atiesrxx.exe		1336	8396 K	6	124	0.000	0.015
C:\Windows\System32\svchost.exe		1388	3042...	21	488	0.265	0.561
C:\Windows\System32\svchost.exe		1420	1382...	20	513	15.225	18.720
C:\Windows\system32\svchost.exe		1448	6153...	36	1245	1.185	1.575
C:\Windows\system32\svchost.exe		1588	1948...	14	327	0.062	0.187
C:\Windows\system32\atieclxx.exe		1724	1284...	10	128	0.093	0.062

☑ Libraries

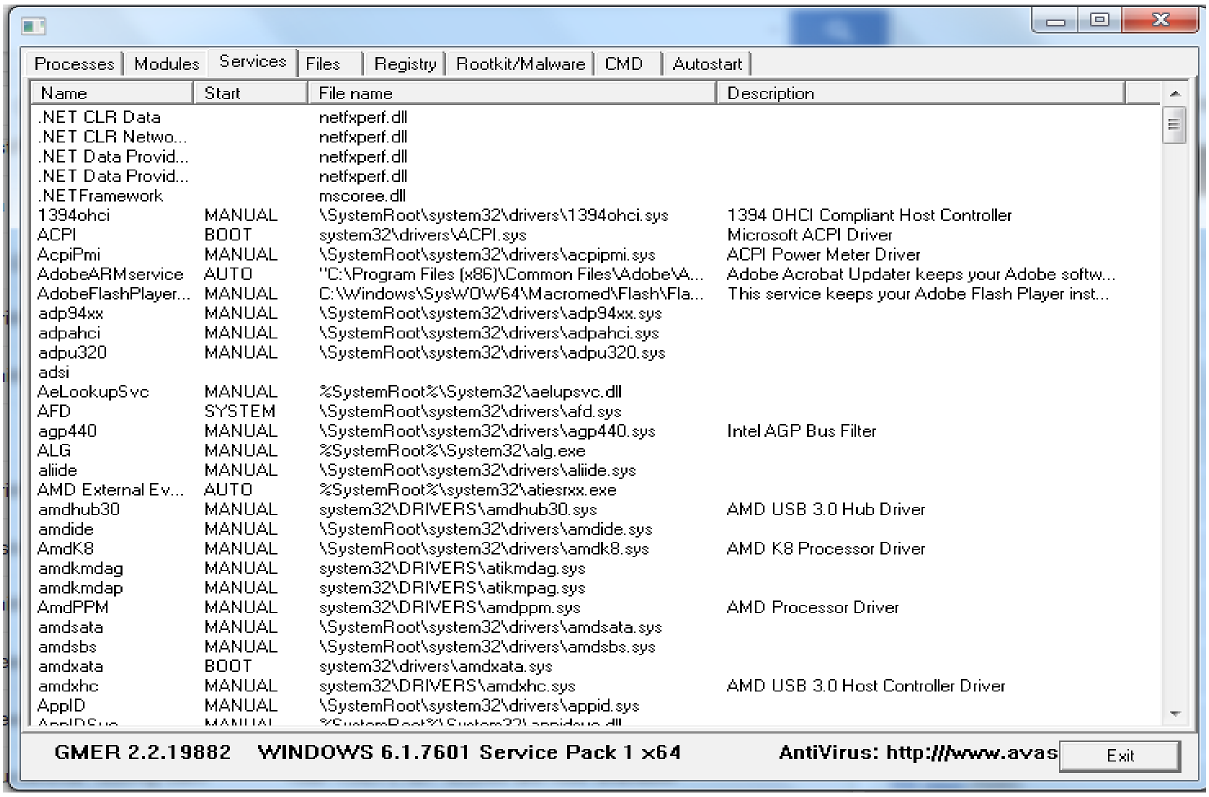
Name	Size	Address

GMER 2.2.19882 WINDOWS 6.1.7601 Service Pack 1 x64 AntiVirus: http://www.avas



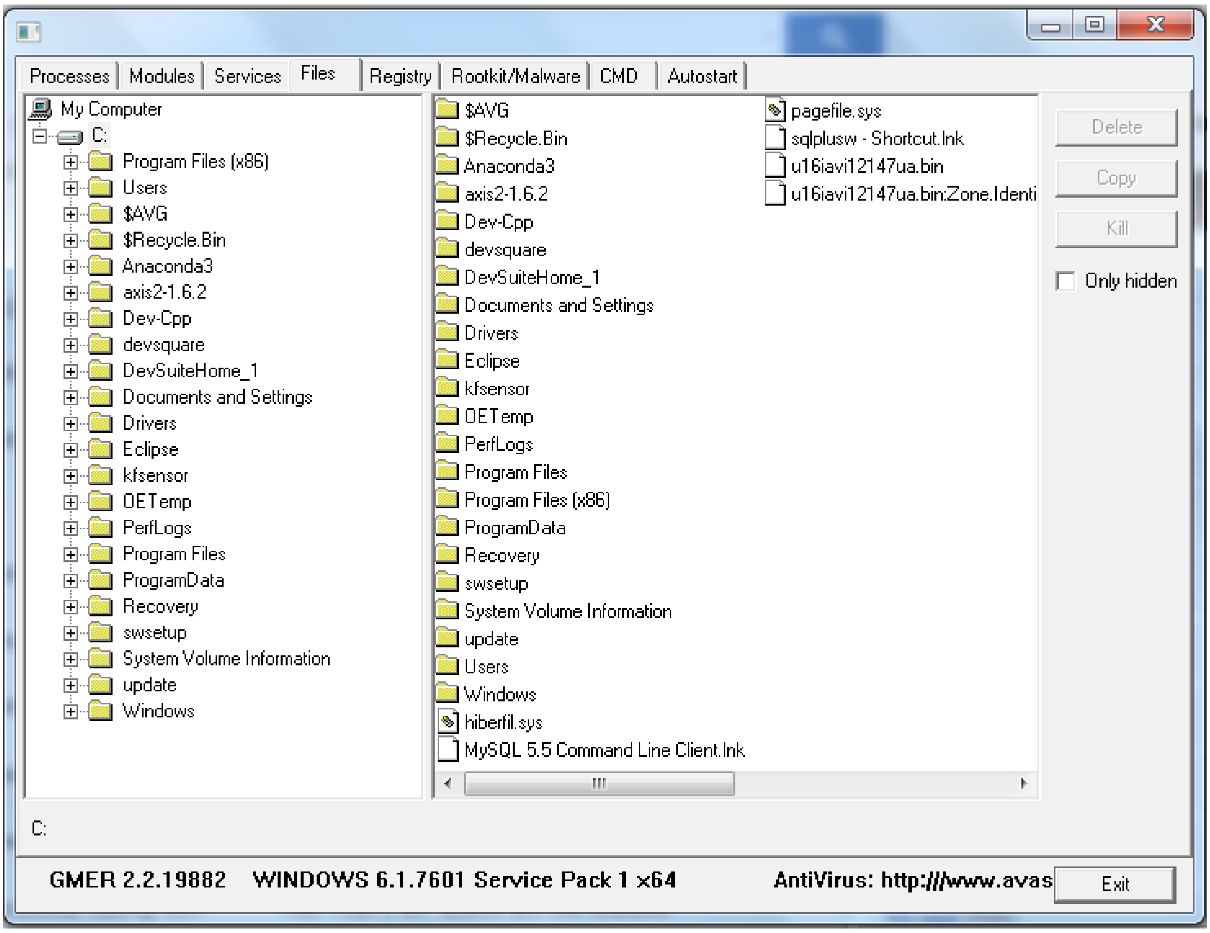
Name	File	Address	Size
ntoskrnl.exe	\SystemRoot\system32\ntoskrnl.exe	fffff80002c03000	6201344
hal.dll	\SystemRoot\system32\hal.dll	fffff800031ed000	299008
kdcom.dll	\SystemRoot\system32\kdcom.dll	fffff80000bcc000	40960
mcupdate_AuthenticA...	\SystemRoot\system32\mcupdate_AuthenticAMD.dll	fffff88000c10000	53248
PSHED.dll	\SystemRoot\system32\PSHED.dll	fffff88000c1d000	81920
CLFS.SYS	\SystemRoot\system32\CLFS.SYS	fffff88000c31000	385024
CI.dll	\SystemRoot\system32\CI.dll	fffff88000c8f000	786432
Wdf01000.sys	\SystemRoot\system32\drivers\Wdf01000.sys	fffff88000d4f000	671744
WDFLDR.SYS	\SystemRoot\system32\drivers\WDFLDR.SYS	fffff88000c00000	61440
ACPI.sys	\SystemRoot\system32\drivers\ACPI.sys	fffff88000ecf000	356352
WMILIB.SYS	\SystemRoot\system32\drivers\WMILIB.SYS	fffff88000f26000	36864
msisadrv.sys	\SystemRoot\system32\drivers\msisadrv.sys	fffff88000f2f000	40960
pci.sys	\SystemRoot\system32\drivers\pci.sys	fffff88000f39000	208896
vdrvroot.sys	\SystemRoot\system32\drivers\vdrvroot.sys	fffff88000f6c000	53248
partmgr.sys	\SystemRoot\System32\drivers\partmgr.sys	fffff88000f79000	86016
volmgr.sys	\SystemRoot\system32\drivers\volmgr.sys	fffff88000f8e000	86016
volmgrx.sys	\SystemRoot\System32\drivers\volmgrx.sys	fffff88000fa3000	376832
mountmgr.sys	\SystemRoot\System32\drivers\mountmgr.sys	fffff88000e00000	106496
atapi.sys	\SystemRoot\system32\drivers\atapi.sys	fffff88000e1a000	36864
ataport.SYS	\SystemRoot\system32\drivers\ataport.SYS	fffff88000e23000	172032
msahci.sys	\SystemRoot\system32\drivers\msahci.sys	fffff88000e4d000	45056
PCIIDEX.SYS	\SystemRoot\system32\drivers\PCIIDEX.SYS	fffff88000e58000	65536
amdxata.sys	\SystemRoot\system32\drivers\amdxata.sys	fffff88000e68000	45056
fltmgr.sys	\SystemRoot\system32\drivers\fltmgr.sys	fffff88000e73000	311296
fileinfo.sys	\SystemRoot\system32\drivers\fileinfo.sys	fffff88001007000	81920
Ntfs.sys	\SystemRoot\System32\Drivers\Ntfs.sys	fffff8800101b000	1716224
msrpc.sys	\SystemRoot\System32\Drivers\msrpc.sys	fffff880012fa000	385024
ksecdd.sys	\SystemRoot\System32\Drivers\ksecdd.sys	fffff88001358000	110592
cng.sys	\SystemRoot\System32\Drivers\cng.sys	fffff88001373000	466944
pcw.sys	\SystemRoot\System32\drivers\pcw.sys	fffff880013e5000	69632

GMER 2.2.19882 WINDOWS 6.1.7601 Service Pack 1 x64 AntiVirus: http://www.avas



Name	Start	File name	Description
.NET CLR Data		netfxperf.dll	
.NET CLR Netwo...		netfxperf.dll	
.NET Data Provid...		netfxperf.dll	
.NET Data Provid...		netfxperf.dll	
.NETFramework		mscoree.dll	
1394ohci	MANUAL	\SystemRoot\system32\drivers\1394ohci.sys	1394 OHCI Compliant Host Controller
ACPI	BOOT	system32\drivers\ACPI.sys	Microsoft ACPI Driver
AcpiPmi	MANUAL	\SystemRoot\system32\drivers\acpipmi.sys	ACPI Power Meter Driver
AdobeARMservice	AUTO	"C:\Program Files (x86)\Common Files\Adobe\A...	Adobe Acrobat Updater keeps your Adobe softw...
AdobeFlashPlayer...	MANUAL	C:\Windows\SysWOW64\Macromed\Flash\Fla...	This service keeps your Adobe Flash Player inst...
adp94xx	MANUAL	\SystemRoot\system32\drivers\adp94xx.sys	
adpahci	MANUAL	\SystemRoot\system32\drivers\adpahci.sys	
adpu320	MANUAL	\SystemRoot\system32\drivers\adpu320.sys	
adsi			
AeLookupSvc	MANUAL	%SystemRoot%\System32\aelupsvc.dll	
AFD	SYSTEM	\SystemRoot\system32\drivers\afd.sys	
agp440	MANUAL	\SystemRoot\system32\drivers\agp440.sys	Intel AGP Bus Filter
ALG	MANUAL	%SystemRoot%\System32\alg.exe	
aliide	MANUAL	\SystemRoot\system32\drivers\aliide.sys	
AMD External Ev...	AUTO	%SystemRoot%\system32\atiesrxx.exe	
amdhub30	MANUAL	system32\DRIVERS\amdhub30.sys	AMD USB 3.0 Hub Driver
amdide	MANUAL	\SystemRoot\system32\drivers\amdide.sys	
AmdK8	MANUAL	\SystemRoot\system32\drivers\amdk8.sys	AMD K8 Processor Driver
amdkmdag	MANUAL	system32\DRIVERS\atikmdag.sys	
amdkmdap	MANUAL	system32\DRIVERS\atikmpag.sys	
AmdPPM	MANUAL	system32\DRIVERS\amdppm.sys	AMD Processor Driver
amdsata	MANUAL	\SystemRoot\system32\drivers\amdsata.sys	
amdsbs	MANUAL	\SystemRoot\system32\drivers\amdsbs.sys	
amdxata	BOOT	system32\drivers\amdxata.sys	
amdxhc	MANUAL	system32\DRIVERS\amdxhc.sys	AMD USB 3.0 Host Controller Driver
AppID	MANUAL	\SystemRoot\system32\drivers\appid.sys	

GMER 2.2.19882 WINDOWS 6.1.7601 Service Pack 1 x64 AntiVirus: http://www.avas



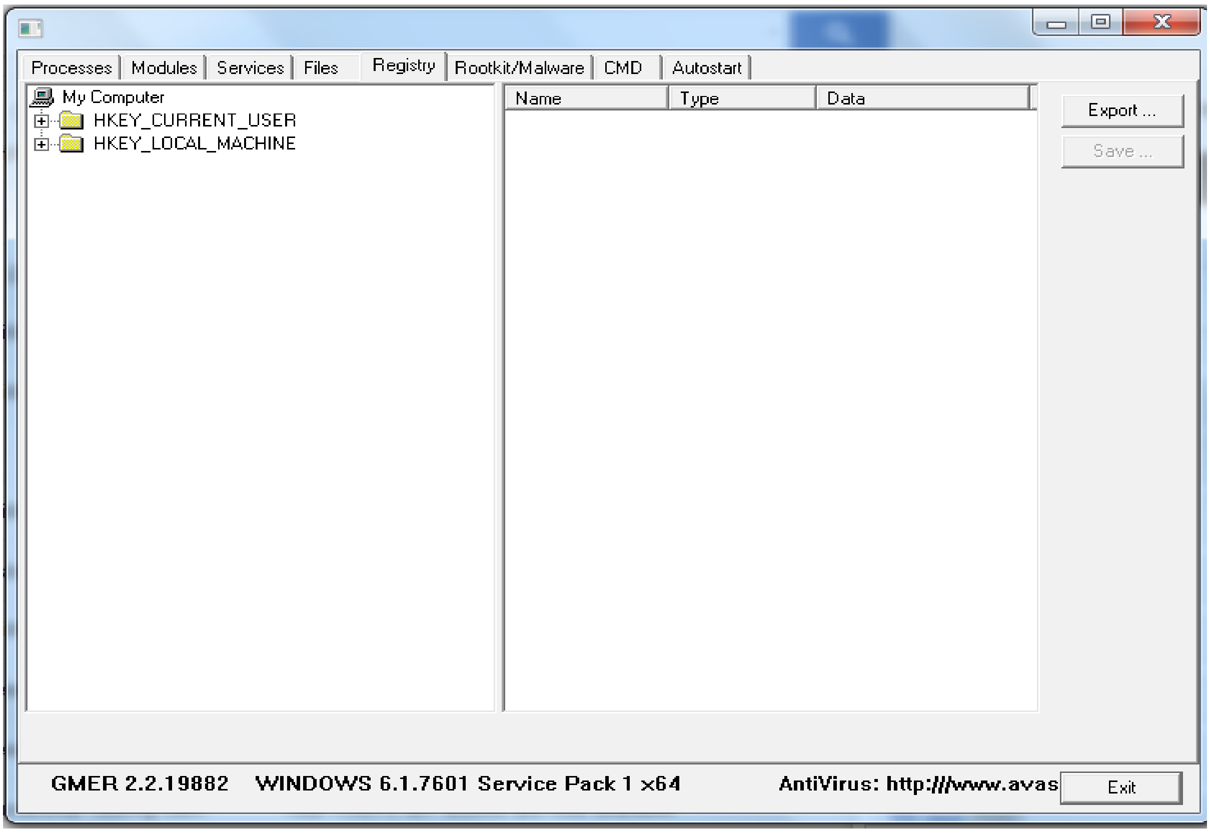
My Computer
C:
Program Files (x86)
Users
$AVG
$Recycle.Bin
Anaconda3
axis2-1.6.2
Dev-Cpp
devsquare
DevSuiteHome_1
Documents and Settings
Drivers
Eclipse
kfsensor
OETemp
PerfLogs
Program Files
ProgramData
Recovery
swsetup
System Volume Information
update
Windows

$AVG
$Recycle.Bin
Anaconda3
axis2-1.6.2
Dev-Cpp
devsquare
DevSuiteHome_1
Documents and Settings
Drivers
Eclipse
kfsensor
OETemp
PerfLogs
Program Files
Program Files (x86)
ProgramData
Recovery
swsetup
System Volume Information
update
Users
Windows
hiberfil.sys
MySQL 5.5 Command Line Client.lnk
pagefile.sys
sqlplusw - Shortcut.lnk
u16iavi12147ua.bin
u16iavi12147ua.bin:Zone.Identi

□ Only hidden

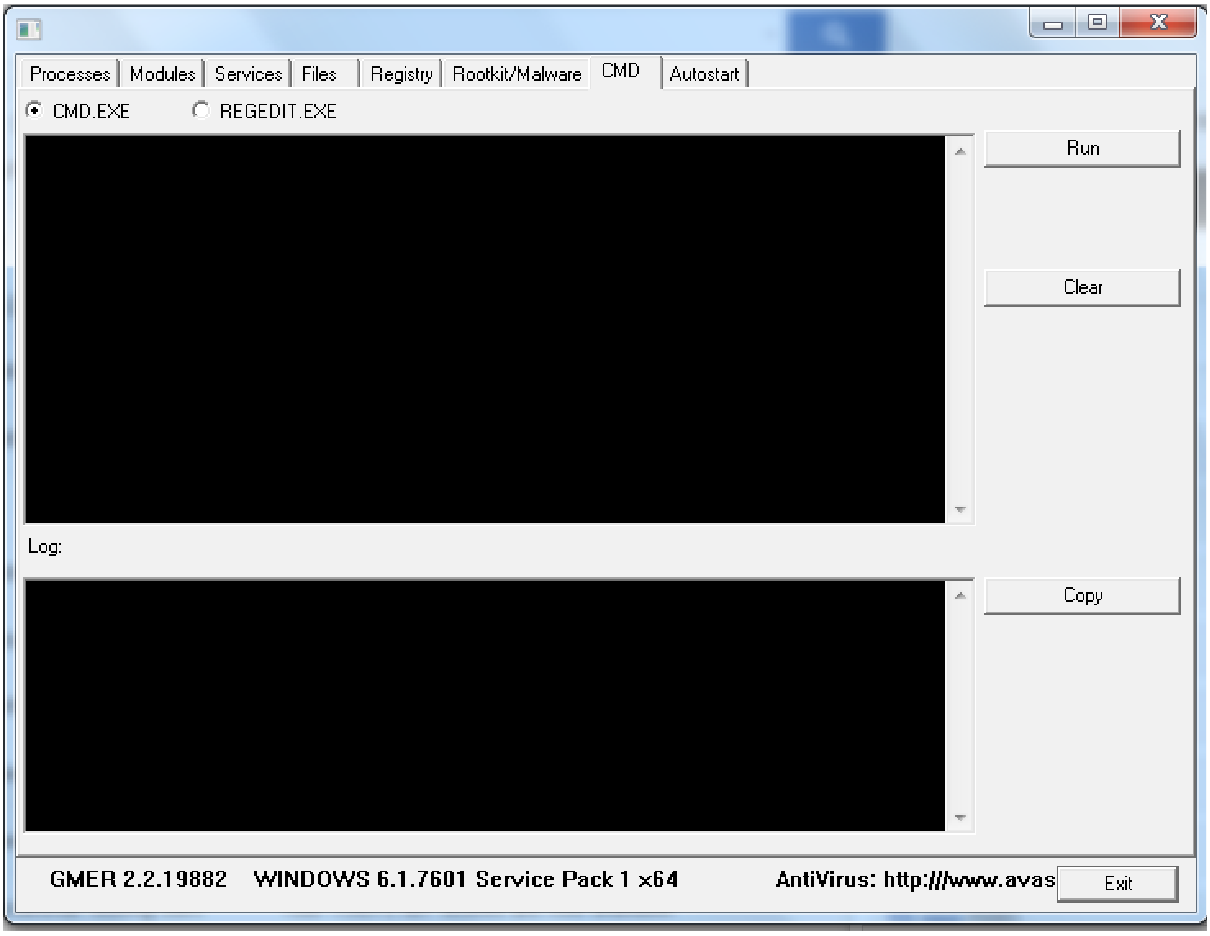
C:

GMER 2.2.19882 WINDOWS 6.1.7601 Service Pack 1 x64 AntiVirus: http://www.avas



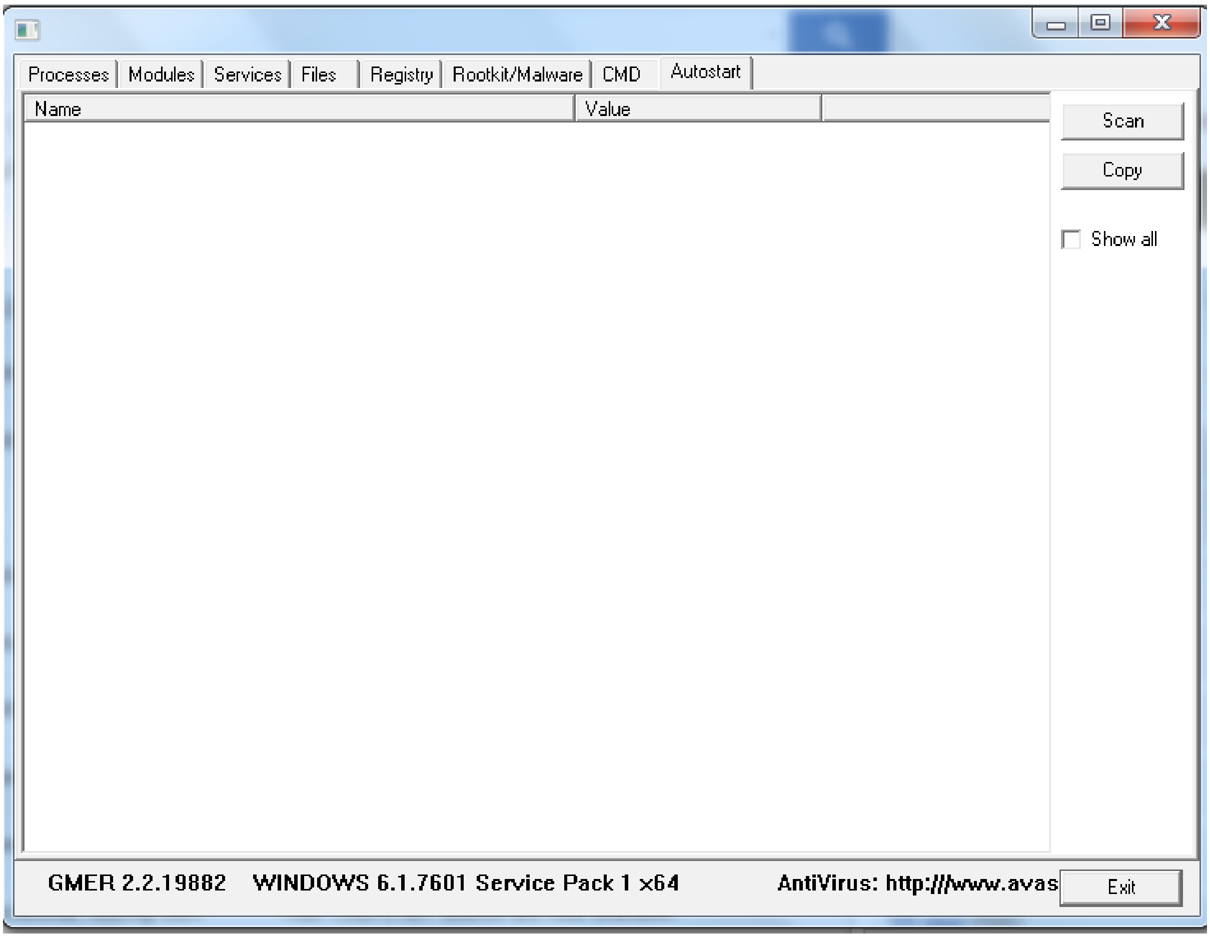
My Computer
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE

GMER 2.2.19882   WINDOWS 6.1.7601 Service Pack 1 x64   AntiVirus: http://www.avas



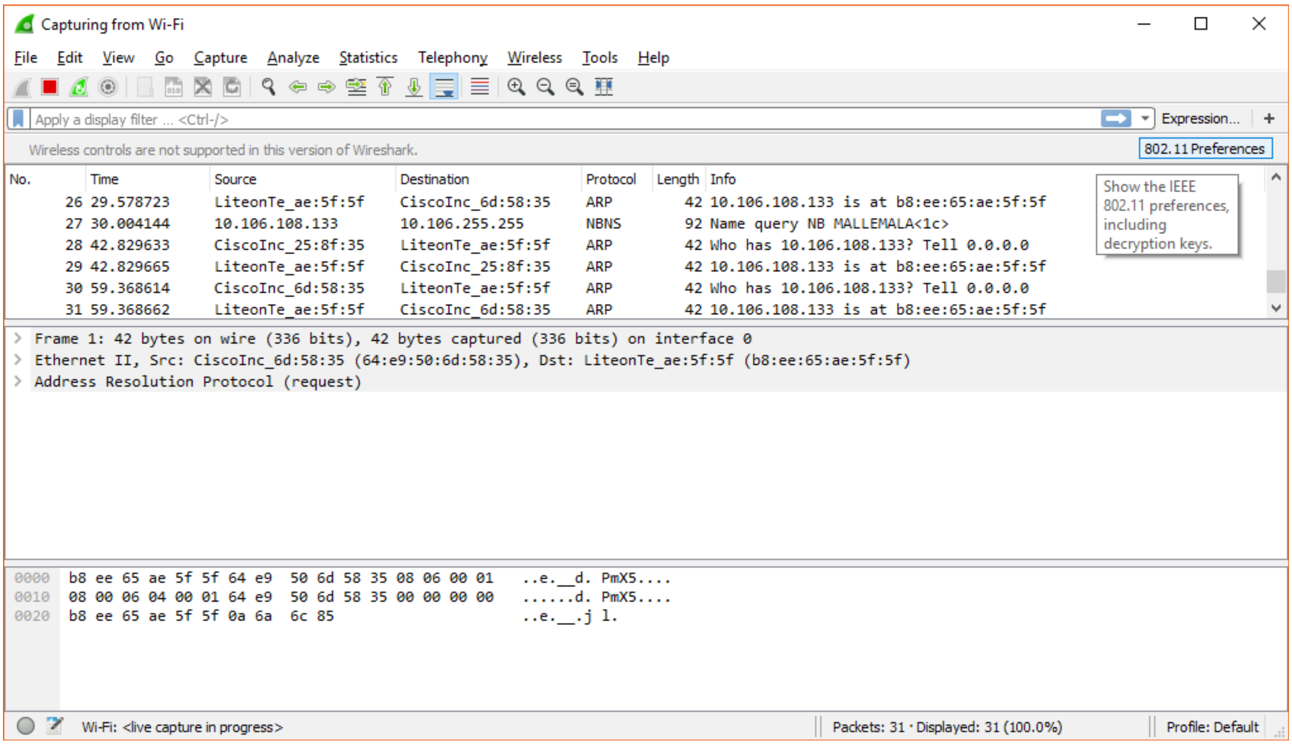
● CMD.EXE   ○ REGEDIT.EXE

GMER 2.2.19882   WINDOWS 6.1.7601 Service Pack 1 x64   AntiVirus: http://www.avas



□ Show all

GMER 2.2.19882   WINDOWS 6.1.7601 Service Pack 1 x64   AntiVirus: http://www.avas


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
802.11 Preferences
Show the IEEE 802.11 preferences, including decryption keys.

Wireless controls are not supported in this version of Wireshark.

```
No.  Time       Source            Destination        Protocol Length Info
  26 29.578723  LiteonTe_ae:5f:5f CiscoInc_6d:58:35  ARP          42 10.106.108.133 is at b8:ee:65:ae:5f:5f
  27 30.004144  10.106.108.133    10.106.255.255     NBNS         92 Name query NB MALLEMALA<1c>
  28 42.829633  CiscoInc_25:8f:35 LiteonTe_ae:5f:5f  ARP          42 Who has 10.106.108.133? Tell 0.0.0.0
  29 42.829665  LiteonTe_ae:5f:5f CiscoInc_25:8f:35  ARP          42 10.106.108.133 is at b8:ee:65:ae:5f:5f
  30 59.368614  CiscoInc_6d:58:35 LiteonTe_ae:5f:5f  ARP          42 Who has 10.106.108.133? Tell 0.0.0.0
  31 59.368662  LiteonTe_ae:5f:5f CiscoInc_6d:58:35  ARP          42 10.106.108.133 is at b8:ee:65:ae:5f:5f
```

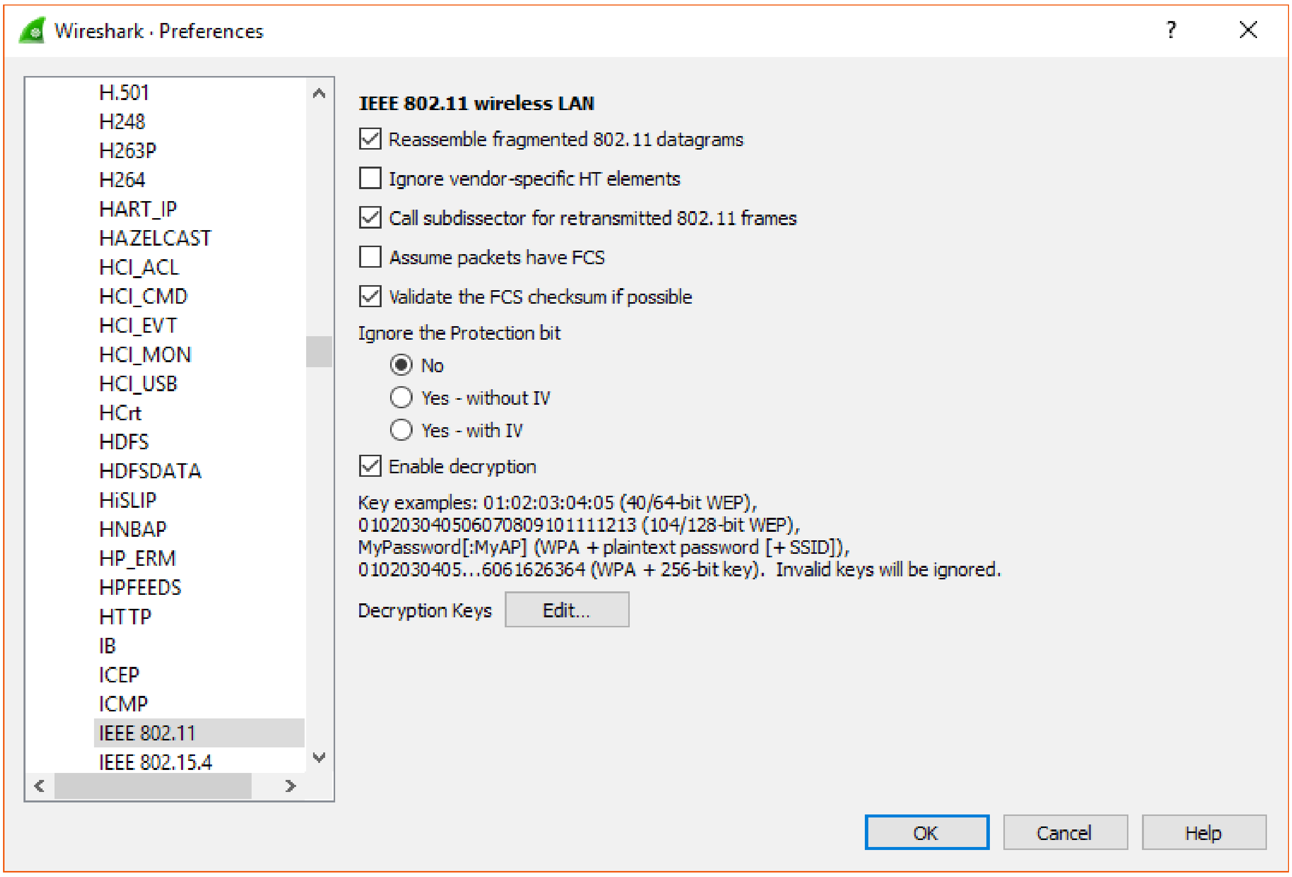
```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: CiscoInc_6d:58:35 (64:e9:50:6d:58:35), Dst: LiteonTe_ae:5f:5f (b8:ee:65:ae:5f:5f)
> Address Resolution Protocol (request)
```

```
0000  b8 ee 65 ae 5f 5f 64 e9  50 6d 58 35 08 06 00 01   ..e.__d. PmX5....
0010  08 00 06 04 00 01 64 e9  50 6d 58 35 00 00 00 00   ......d. PmX5....
0020  b8 ee 65 ae 5f 5f 0a 6a  6c 85                     ..e.__.j l.
```

Wi-Fi: <live capture in progress>

Packets: 31 · Displayed: 31 (100.0%)

Profile: Default



IEEE 802.11 wireless LAN

☑ Reassemble fragmented 802.11 datagrams

□ Ignore vendor-specific HT elements

☑ Call subdissector for retransmitted 802.11 frames

□ Assume packets have FCS

☑ Validate the FCS checksum if possible

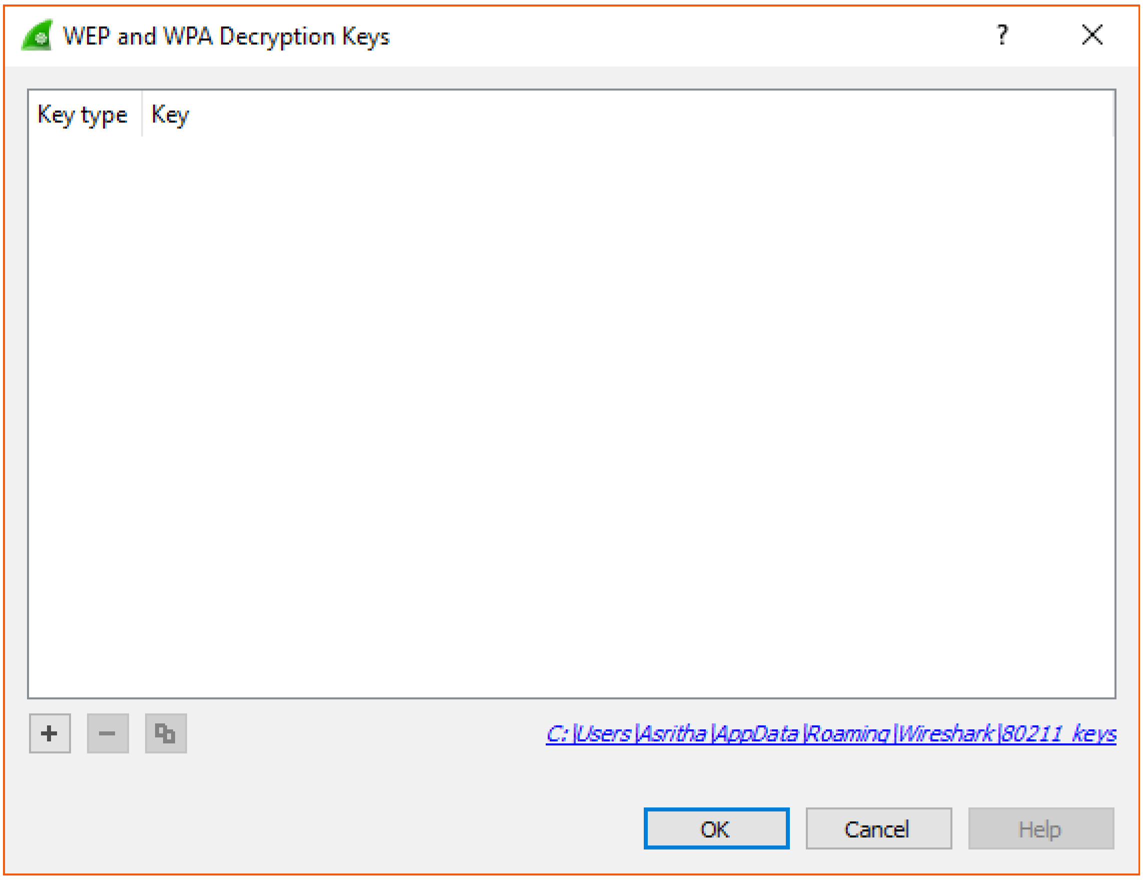
Ignore the Protection bit

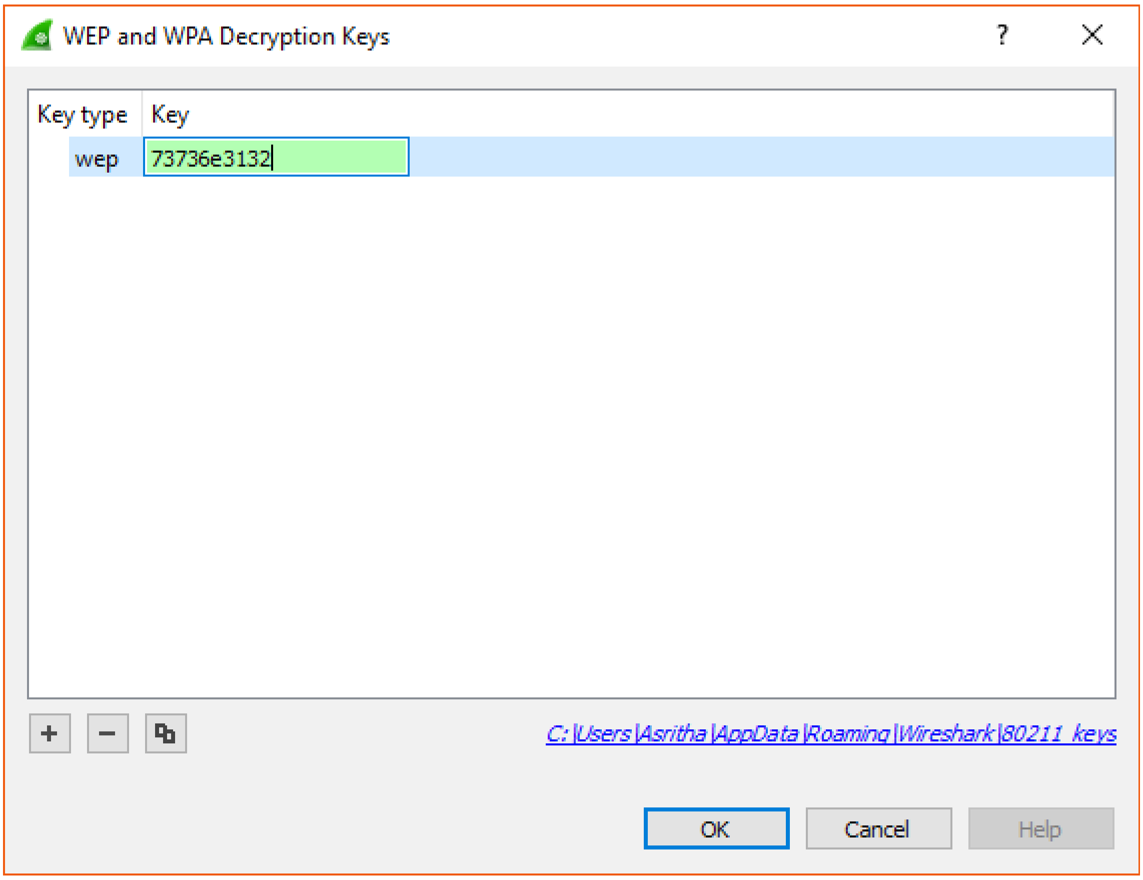
- ● No
- ○ Yes - without IV
- ○ Yes - with IV

☑ Enable decryption

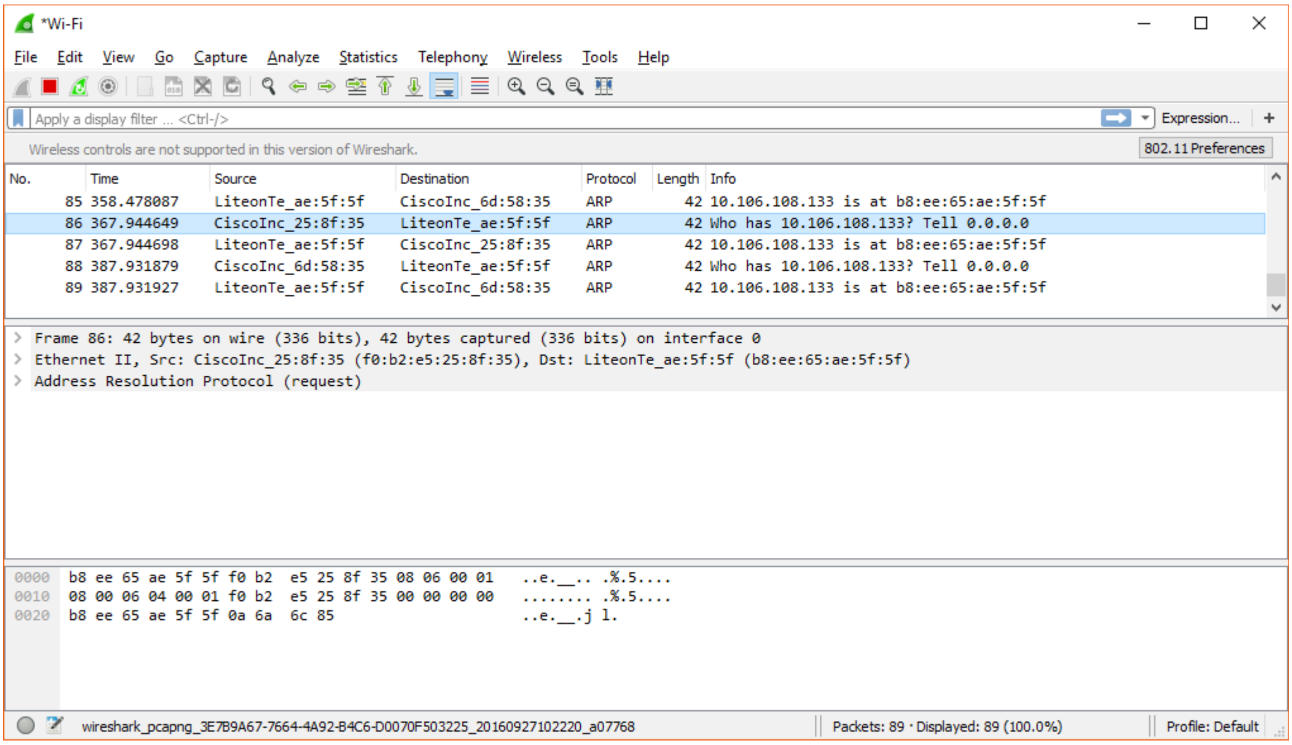
Key examples: 01:02:03:04:05 (40/64-bit WEP),
010203040506070809101111213 (104/128-bit WEP),
MyPassword[:MyAP] (WPA + plaintext password [+ SSID]),
0102030405...6061626364 (WPA + 256-bit key). Invalid keys will be ignored.

Decryption Keys Edit...


WEP and WPA Decryption Keys
?
Key type
Key
C:\Users\Asritha\AppData\Roaming\Wireshark\80211_keys
OK
Cancel
Help


WEP and WPA Decryption Keys
?
C:\Users\Asritha\AppData\Roaming\Wireshark\80211_keys
OK
Cancel
Help

Key type	Key
wep	73736e3132

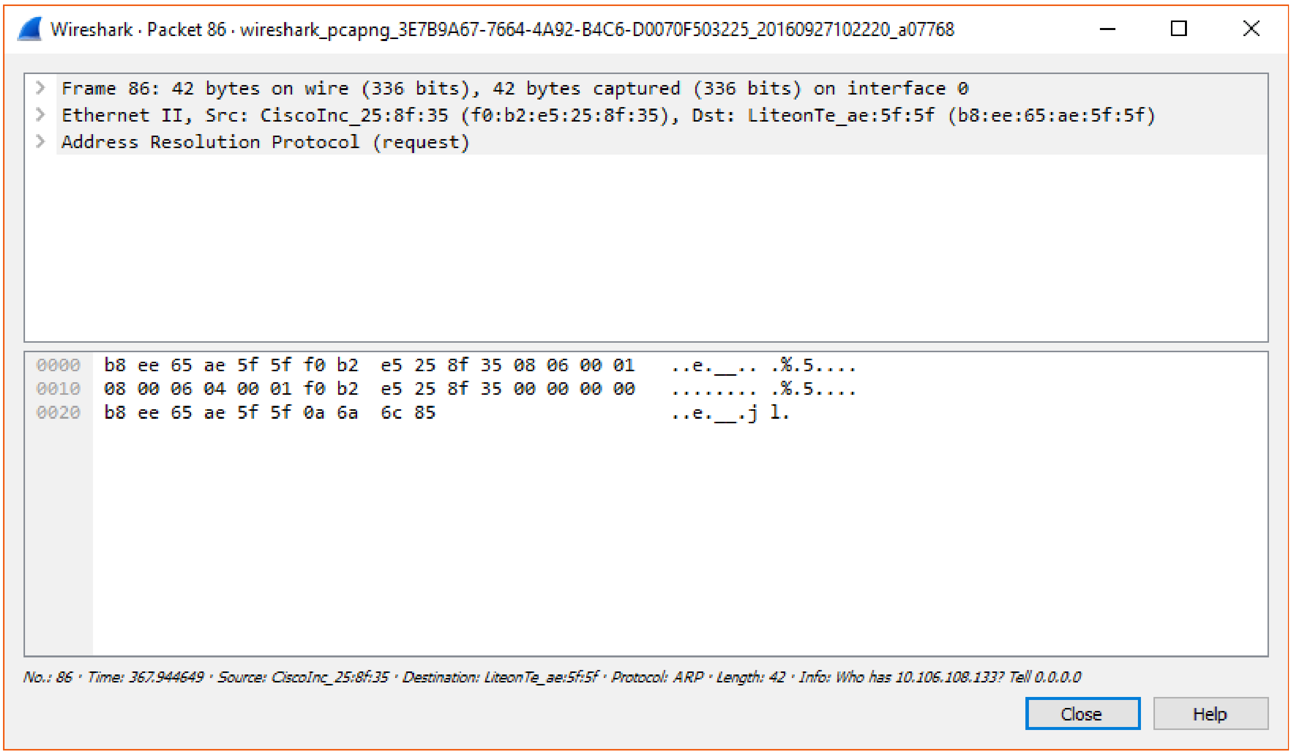

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
Wireless controls are not supported in this version of Wireshark.
802.11 Preferences

```
No.     Time        Source              Destination         Protocol  Length  Info
     85 358.478087  LiteonTe_ae:5f:5f   CiscoInc_6d:58:35   ARP           42  10.106.108.133 is at b8:ee:65:ae:5f:5f
     86 367.944649  CiscoInc_25:8f:35   LiteonTe_ae:5f:5f   ARP           42  Who has 10.106.108.133? Tell 0.0.0.0
     87 367.944698  LiteonTe_ae:5f:5f   CiscoInc_25:8f:35   ARP           42  10.106.108.133 is at b8:ee:65:ae:5f:5f
     88 387.931879  CiscoInc_6d:58:35   LiteonTe_ae:5f:5f   ARP           42  Who has 10.106.108.133? Tell 0.0.0.0
     89 387.931927  LiteonTe_ae:5f:5f   CiscoInc_6d:58:35   ARP           42  10.106.108.133 is at b8:ee:65:ae:5f:5f
```

```
> Frame 86: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: CiscoInc_25:8f:35 (f0:b2:e5:25:8f:35), Dst: LiteonTe_ae:5f:5f (b8:ee:65:ae:5f:5f)
> Address Resolution Protocol (request)
```

```
0000  b8 ee 65 ae 5f 5f f0 b2  e5 25 8f 35 08 06 00 01   ..e.__.. .%.5....
0010  08 00 06 04 00 01 f0 b2  e5 25 8f 35 00 00 00 00   ........ .%.5....
0020  b8 ee 65 ae 5f 5f 0a 6a  6c 85                     ..e.__.j l.
```

wireshark_pcapng_3E7B9A67-7664-4A92-B4C6-D0070F503225_20160927102220_a07768 | Packets: 89 · Displayed: 89 (100.0%) | Profile: Default


Wireshark · Packet 86 · wireshark_pcapng_3E7B9A67-7664-4A92-B4C6-D0070F503225_20160927102220_a07768
Close
Help

```
> Frame 86: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: CiscoInc_25:8f:35 (f0:b2:e5:25:8f:35), Dst: LiteonTe_ae:5f:5f (b8:ee:65:ae:5f:5f)
> Address Resolution Protocol (request)
```

```
0000  b8 ee 65 ae 5f 5f f0 b2  e5 25 8f 35 08 06 00 01   ..e.__.. .%.5....
0010  08 00 06 04 00 01 f0 b2  e5 25 8f 35 00 00 00 00   ........ .%.5....
0020  b8 ee 65 ae 5f 5f 0a 6a  6c 85                     ..e.__.j l.
```

No.: 86 · Time: 367.944649 · Source: CiscoInc_25:8f:35 · Destination: LiteonTe_ae:5f:5f · Protocol: ARP · Length: 42 · Info: Who has 10.106.108.133? Tell 0.0.0.0

INTRUSION DETECTION SYSTEM

AIM : To install, configure and test the Intrusion Detection System Snort.

STEPS :

1. Double-click the WinPcap_4_1_3.exe installer and the follow the on-screen prompts.
2. Double-click the Snort_2_9_8_2_Installer.exe and follow the on-screen prompts.
3. Create a sub-folder under c:\Snort called "rules" and another one called "preproc_rules".
4. Open the Snort rules package.
5. Extract the contents of the "rules" folder in the archive to c:\Snort\rules.
6. Extract the contents of the "preproc_rules" folder in the archive to c:\Snort\preproc_rules.
7. Ignore contents of so_rules folder and etc folder.
8. Change to Snort program directory : cd \snort\bin
9. Check the installed version for Snort : snort -V
10. Check network interfaces : snort -W
11. Open C:\Snort\etc\snort.conf and do the following

Step 1: Set the network variables

```
ipvar HOME_NET 10.0.0.0/8
ipvar EXTERNAL_NET !$HOME_NET
var RULE_PATH c:\Snort\rules
#var SO_RULE_PATH ../so_rules
(comment out)
var PREPROC_RULE_PATH c:\Snort\prepoc_rules
```

Step 2: Configure the decoder

```
config logdir: c:\Snort\log
(uncomment)
```

Step 3: Configure the base detection engine (NO CHANGES)

Step 4: Configure dynamic loaded libraries

```
dynamicpreprocessor directory c:\Snort\lib\snort_dynamicpreprocessor
dynamicengine c:\Snort\lib\snort_dynamicengine\sf_engine.dll
# dynamicdetection directory /usr/local/lib/snort_dynamicrules
(comment out)
```

Step 5: Configure preprocessors

Normalization Preprocessor (Comment out all lines)

```
#preprocessor normalize_ip4
#preprocessor normalize_tcp: ips ecn stream
#preprocessor normalize_icmp4
#preprocessor normalize_ip6
#preprocessor normalize_icmp6
```

Reputation Preprocessor (Comment out all lines)

```
#preprocessor reputation: \
#memcap 500, \
#priority whitelist, \
#nested_ip inner, \
#whitelist $WHITE_LIST_PATH/white_list.rules, \
#blacklist $BLACK_LIST_PATH/black_list.rules
```

If Reputation Preprocessor is not commented, then you will need to create blacklist and whitelist rules files.

Step 6: Configure output plugins (NO CHANGES)
Step 7: Customize your rule set (NO CHANGES)
Step 8: Customize preprocessor and decoder rule set

(Uncomment these lines and change / to \)

```
include $PREPROC_RULE_PATH\preprocessor.rules
include $PREPROC_RULE_PATH\decoder.rules
```

Step 9: Customize shared object rule set (NO CHANGES)

12. Open c:\Snort\rules\local.rules and add these rules.

```
alert icmp any any -> any any (msg:"ICMP Testing Rule"; sid:1000001; rev:1;)
alert tcp any any -> any 80 (msg:"TCP Testing Rule"; sid:1000002; rev:1;)
alert udp any any -> any any (msg:"UDP Testing Rule"; sid:1000003; rev:1;)
```

13. Run command prompt as administrator.
14. Start Snort using the -A option

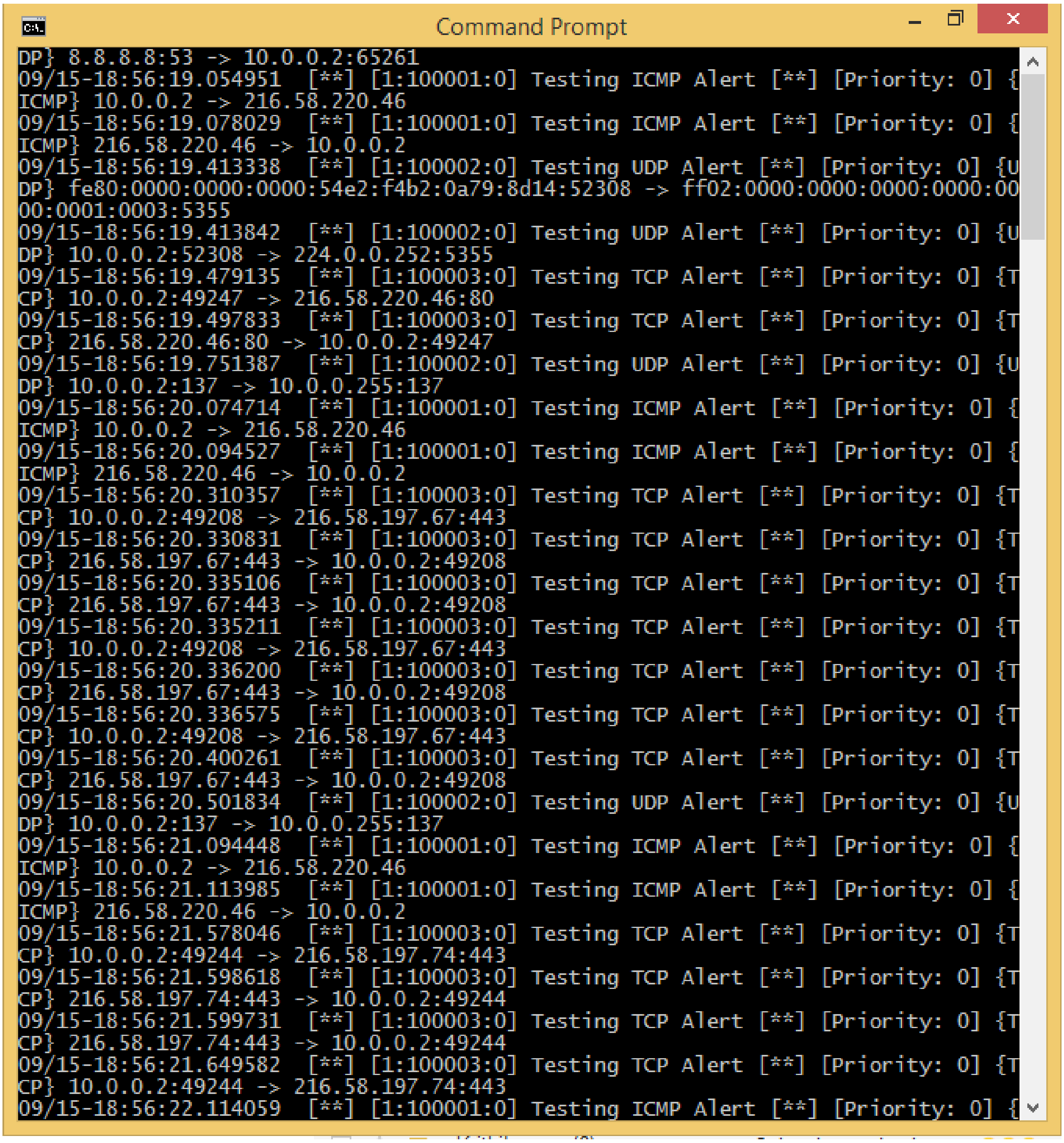
```
cd \Snort\bin
snort -i 1 -c c:\Snort\etc\snort.conf -A console
```

14. Open another command prompt and send a ping to some host.

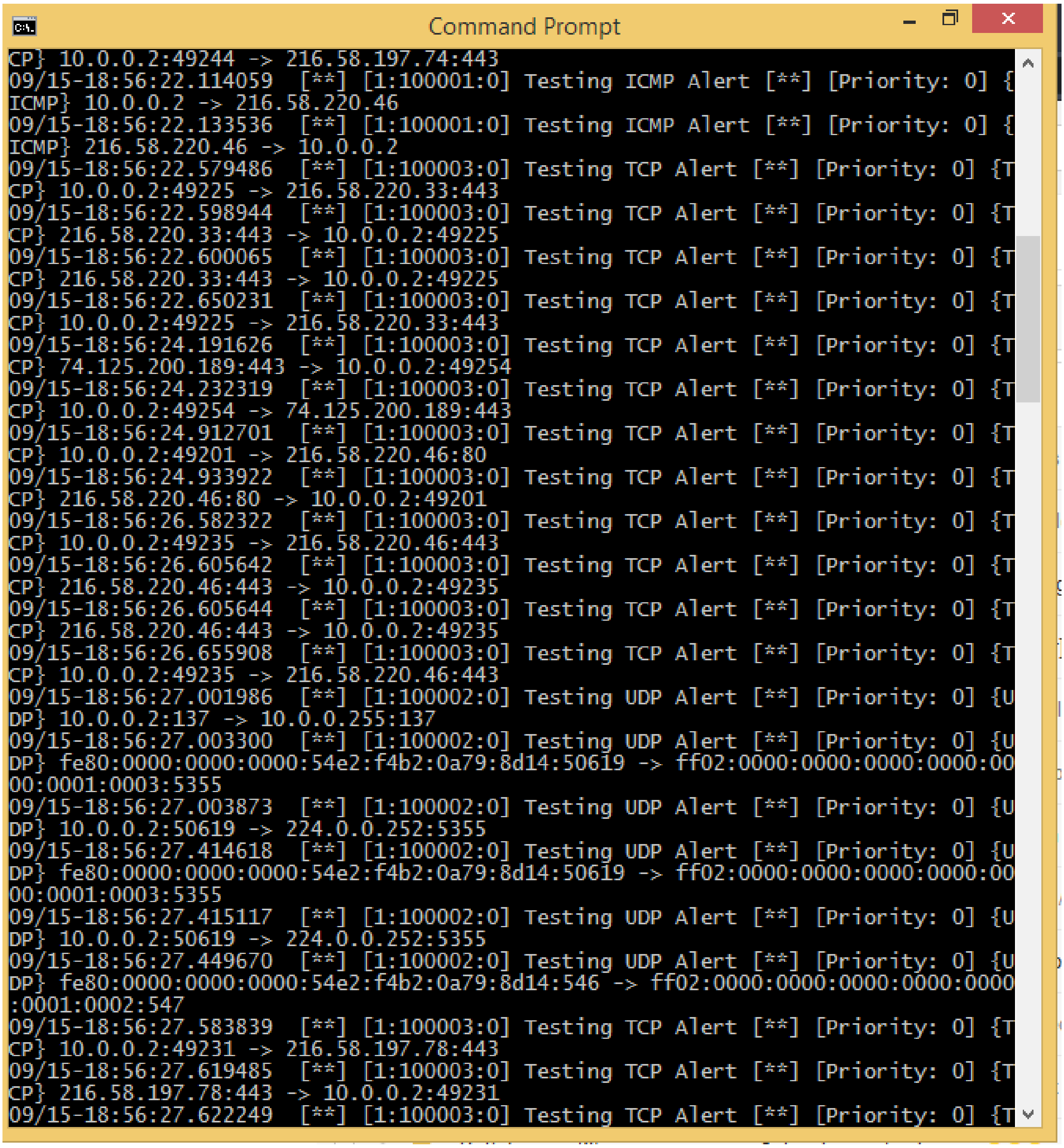
```
ping google.com
```

15. Open web browser and browse any page.
16. Check the alerts in the first command prompt.
17. To stop Snort, press Ctrl + C.
18. View the statistics that are displayed.

Snort showing alerts for TCP, UDP and ICMP packets :

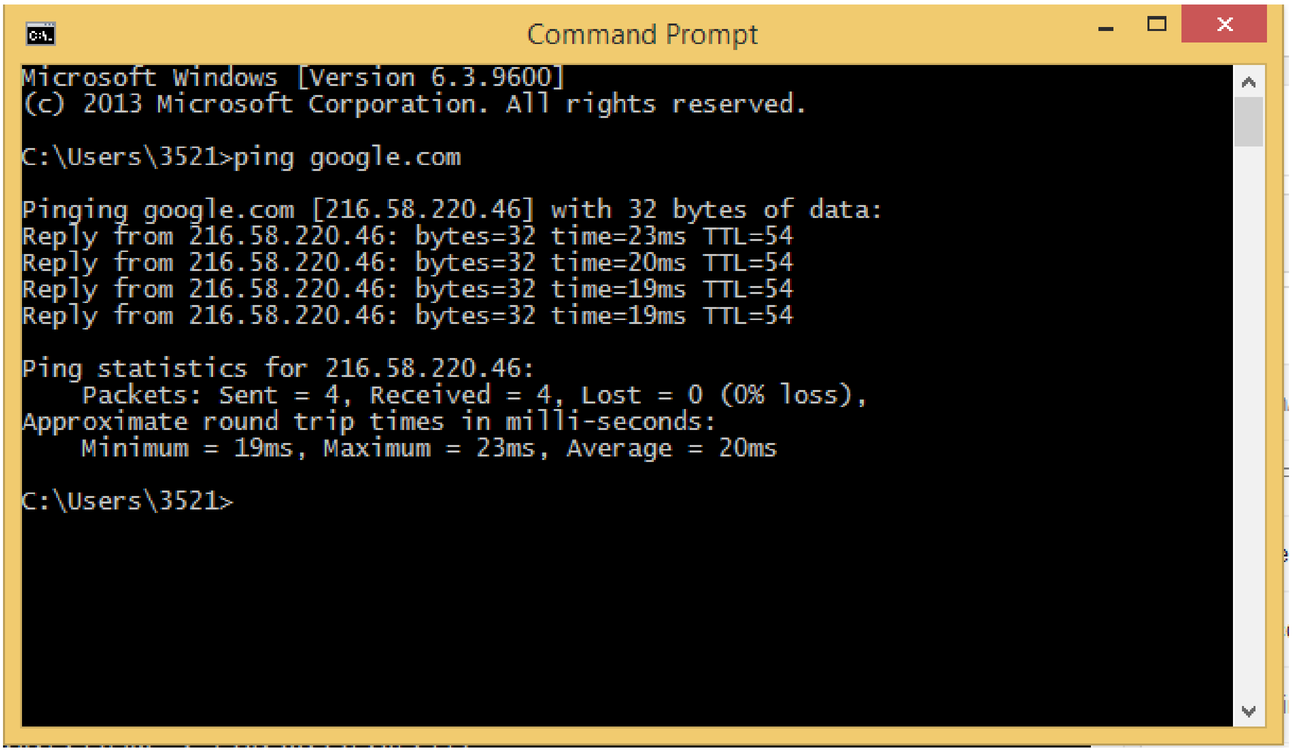


```
DP} 8.8.8.8:53 -> 10.0.0.2:65261
09/15-18:56:19.054951  [**] [1:100001:0] Testing ICMP Alert [**] [Priority: 0] {
ICMP} 10.0.0.2 -> 216.58.220.46
09/15-18:56:19.078029  [**] [1:100001:0] Testing ICMP Alert [**] [Priority: 0] {
ICMP} 216.58.220.46 -> 10.0.0.2
09/15-18:56:19.413338  [**] [1:100002:0] Testing UDP Alert [**] [Priority: 0] {U
DP} fe80:0000:0000:0000:54e2:f4b2:0a79:8d14:52308 -> ff02:0000:0000:0000:0000:00
00:0001:0003:5355
09/15-18:56:19.413842  [**] [1:100002:0] Testing UDP Alert [**] [Priority: 0] {U
DP} 10.0.0.2:52308 -> 224.0.0.252:5355
09/15-18:56:19.479135  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49247 -> 216.58.220.46:80
09/15-18:56:19.497833  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.220.46:80 -> 10.0.0.2:49247
09/15-18:56:19.751387  [**] [1:100002:0] Testing UDP Alert [**] [Priority: 0] {U
DP} 10.0.0.2:137 -> 10.0.0.255:137
09/15-18:56:20.074714  [**] [1:100001:0] Testing ICMP Alert [**] [Priority: 0] {
ICMP} 10.0.0.2 -> 216.58.220.46
09/15-18:56:20.094527  [**] [1:100001:0] Testing ICMP Alert [**] [Priority: 0] {
ICMP} 216.58.220.46 -> 10.0.0.2
09/15-18:56:20.310357  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49208 -> 216.58.197.67:443
09/15-18:56:20.330831  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.197.67:443 -> 10.0.0.2:49208
09/15-18:56:20.335106  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.197.67:443 -> 10.0.0.2:49208
09/15-18:56:20.335211  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49208 -> 216.58.197.67:443
09/15-18:56:20.336200  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.197.67:443 -> 10.0.0.2:49208
09/15-18:56:20.336575  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49208 -> 216.58.197.67:443
09/15-18:56:20.400261  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.197.67:443 -> 10.0.0.2:49208
09/15-18:56:20.501834  [**] [1:100002:0] Testing UDP Alert [**] [Priority: 0] {U
DP} 10.0.0.2:137 -> 10.0.0.255:137
09/15-18:56:21.094448  [**] [1:100001:0] Testing ICMP Alert [**] [Priority: 0] {
ICMP} 10.0.0.2 -> 216.58.220.46
09/15-18:56:21.113985  [**] [1:100001:0] Testing ICMP Alert [**] [Priority: 0] {
ICMP} 216.58.220.46 -> 10.0.0.2
09/15-18:56:21.578046  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49244 -> 216.58.197.74:443
09/15-18:56:21.598618  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.197.74:443 -> 10.0.0.2:49244
09/15-18:56:21.599731  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.197.74:443 -> 10.0.0.2:49244
09/15-18:56:21.649582  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49244 -> 216.58.197.74:443
09/15-18:56:22.114059  [**] [1:100001:0] Testing ICMP Alert [**] [Priority: 0] {
```



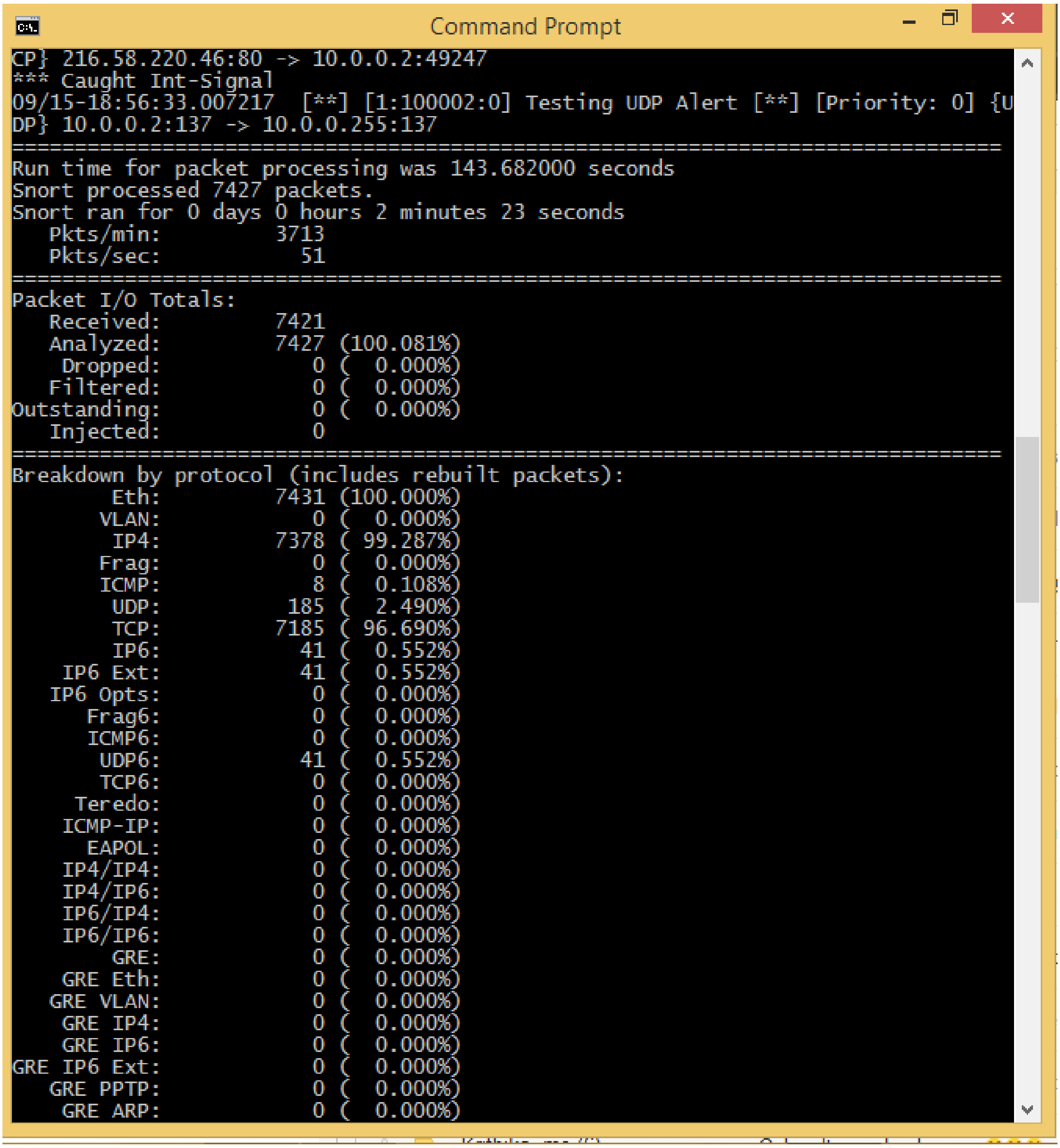
```
CP} 10.0.0.2:49244 -> 216.58.197.74:443
09/15-18:56:22.114059  [**] [1:100001:0] Testing ICMP Alert [**] [Priority: 0] {
ICMP} 10.0.0.2 -> 216.58.220.46
09/15-18:56:22.133536  [**] [1:100001:0] Testing ICMP Alert [**] [Priority: 0] {
ICMP} 216.58.220.46 -> 10.0.0.2
09/15-18:56:22.579486  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49225 -> 216.58.220.33:443
09/15-18:56:22.598944  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.220.33:443 -> 10.0.0.2:49225
09/15-18:56:22.600065  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.220.33:443 -> 10.0.0.2:49225
09/15-18:56:22.650231  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49225 -> 216.58.220.33:443
09/15-18:56:24.191626  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 74.125.200.189:443 -> 10.0.0.2:49254
09/15-18:56:24.232319  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49254 -> 74.125.200.189:443
09/15-18:56:24.912701  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49201 -> 216.58.220.46:80
09/15-18:56:24.933922  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.220.46:80 -> 10.0.0.2:49201
09/15-18:56:26.582322  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49235 -> 216.58.220.46:443
09/15-18:56:26.605642  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.220.46:443 -> 10.0.0.2:49235
09/15-18:56:26.605644  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.220.46:443 -> 10.0.0.2:49235
09/15-18:56:26.655908  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49235 -> 216.58.220.46:443
09/15-18:56:27.001986  [**] [1:100002:0] Testing UDP Alert [**] [Priority: 0] {U
DP} 10.0.0.2:137 -> 10.0.0.255:137
09/15-18:56:27.003300  [**] [1:100002:0] Testing UDP Alert [**] [Priority: 0] {U
DP} fe80:0000:0000:0000:54e2:f4b2:0a79:8d14:50619 -> ff02:0000:0000:0000:0000:00
00:0001:0003:5355
09/15-18:56:27.003873  [**] [1:100002:0] Testing UDP Alert [**] [Priority: 0] {U
DP} 10.0.0.2:50619 -> 224.0.0.252:5355
09/15-18:56:27.414618  [**] [1:100002:0] Testing UDP Alert [**] [Priority: 0] {U
DP} fe80:0000:0000:0000:54e2:f4b2:0a79:8d14:50619 -> ff02:0000:0000:0000:0000:00
00:0001:0003:5355
09/15-18:56:27.415117  [**] [1:100002:0] Testing UDP Alert [**] [Priority: 0] {U
DP} 10.0.0.2:50619 -> 224.0.0.252:5355
09/15-18:56:27.449670  [**] [1:100002:0] Testing UDP Alert [**] [Priority: 0] {U
DP} fe80:0000:0000:0000:54e2:f4b2:0a79:8d14:546 -> ff02:0000:0000:0000:0000:0000
:0001:0002:547
09/15-18:56:27.583839  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 10.0.0.2:49231 -> 216.58.197.78:443
09/15-18:56:27.619485  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
CP} 216.58.197.78:443 -> 10.0.0.2:49231
09/15-18:56:27.622249  [**] [1:100003:0] Testing TCP Alert [**] [Priority: 0] {T
```

Pinging google to create ICMP packets to check if Snort alerts us of those packets :

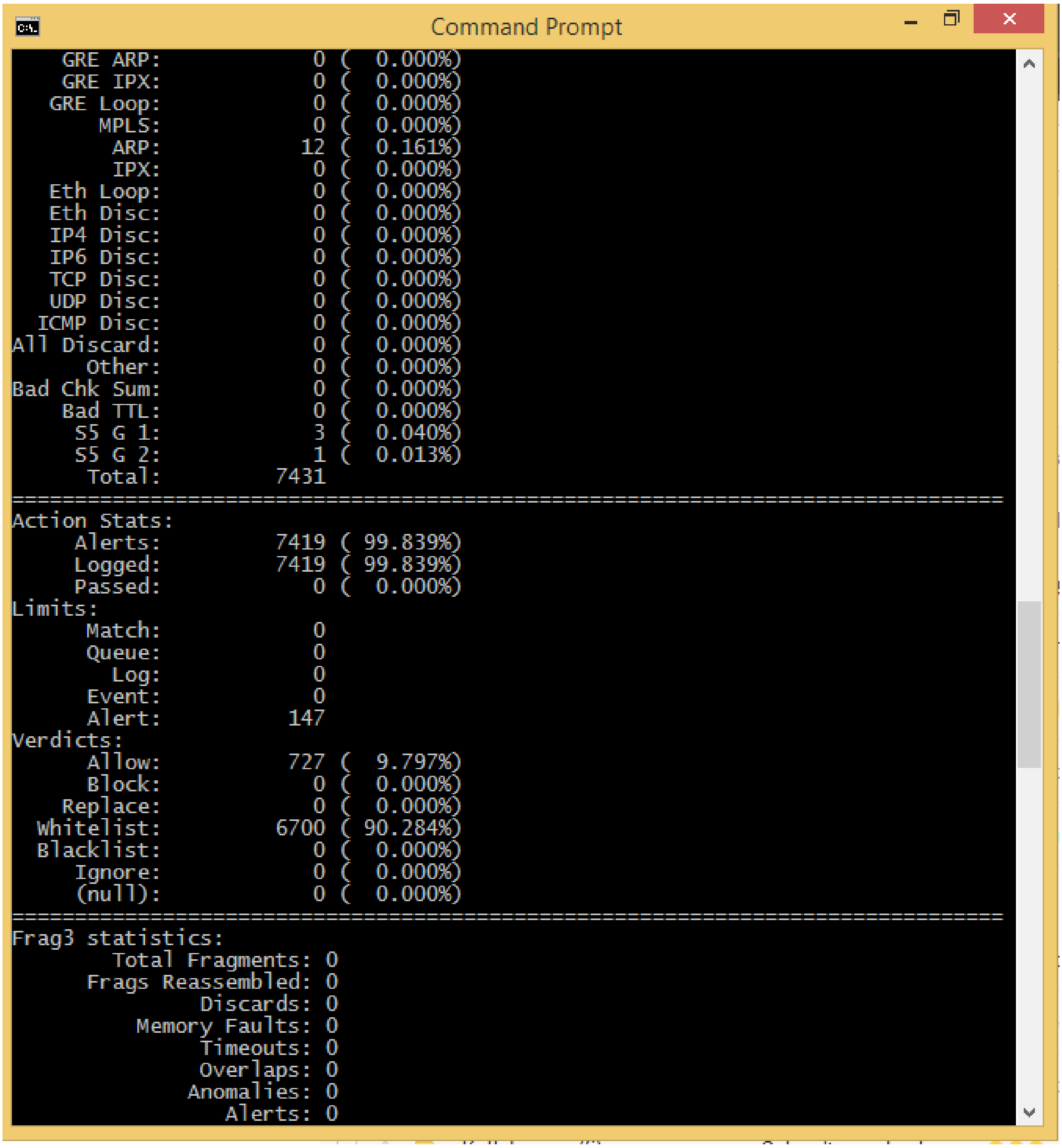


```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\3521>ping google.com

Pinging google.com [216.58.220.46] with 32 bytes of data:
Reply from 216.58.220.46: bytes=32 time=23ms TTL=54
Reply from 216.58.220.46: bytes=32 time=20ms TTL=54
Reply from 216.58.220.46: bytes=32 time=19ms TTL=54
Reply from 216.58.220.46: bytes=32 time=19ms TTL=54

Ping statistics for 216.58.220.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 23ms, Average = 20ms

C:\Users\3521>
```

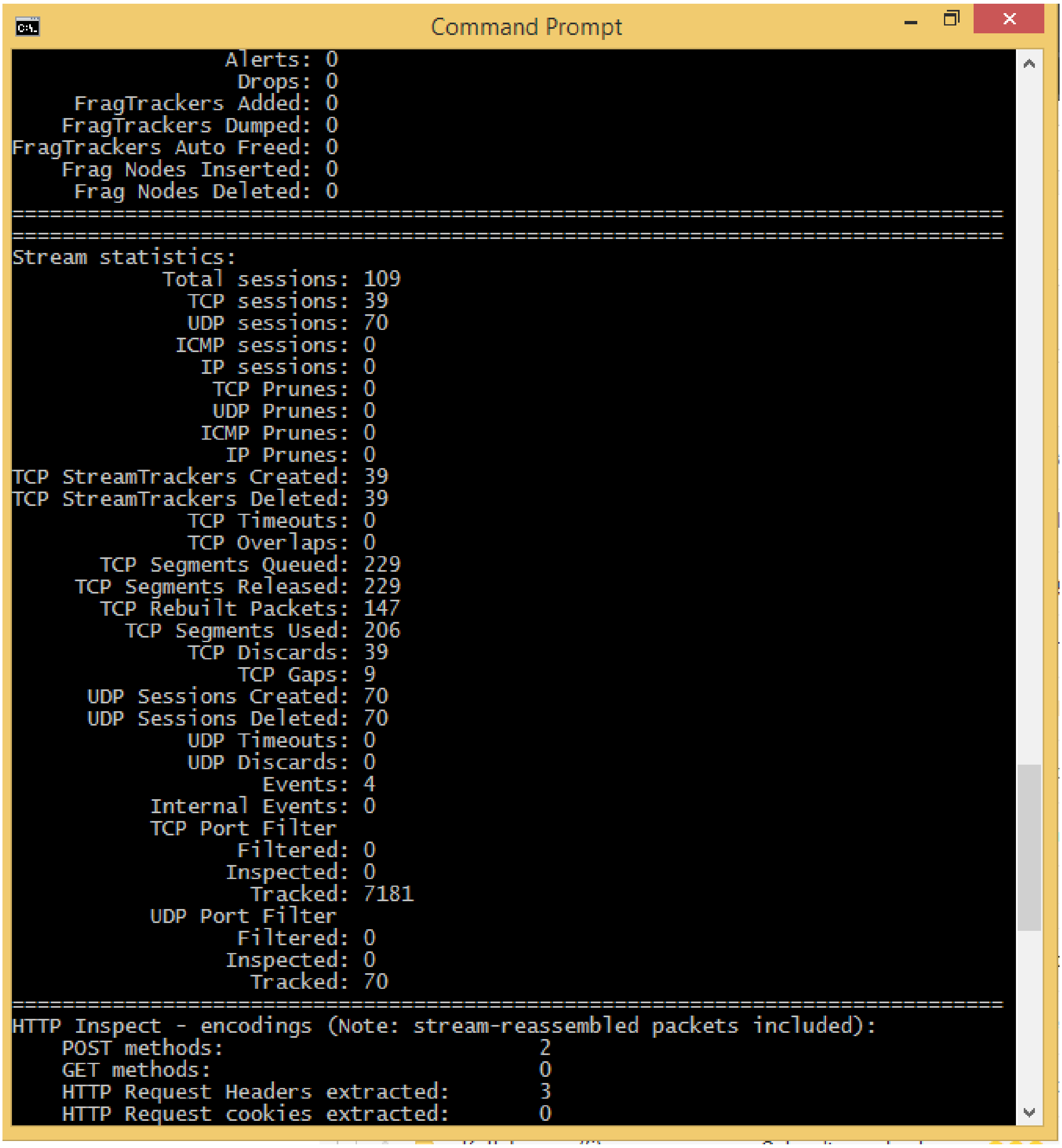
Snort showing packet analysis results :



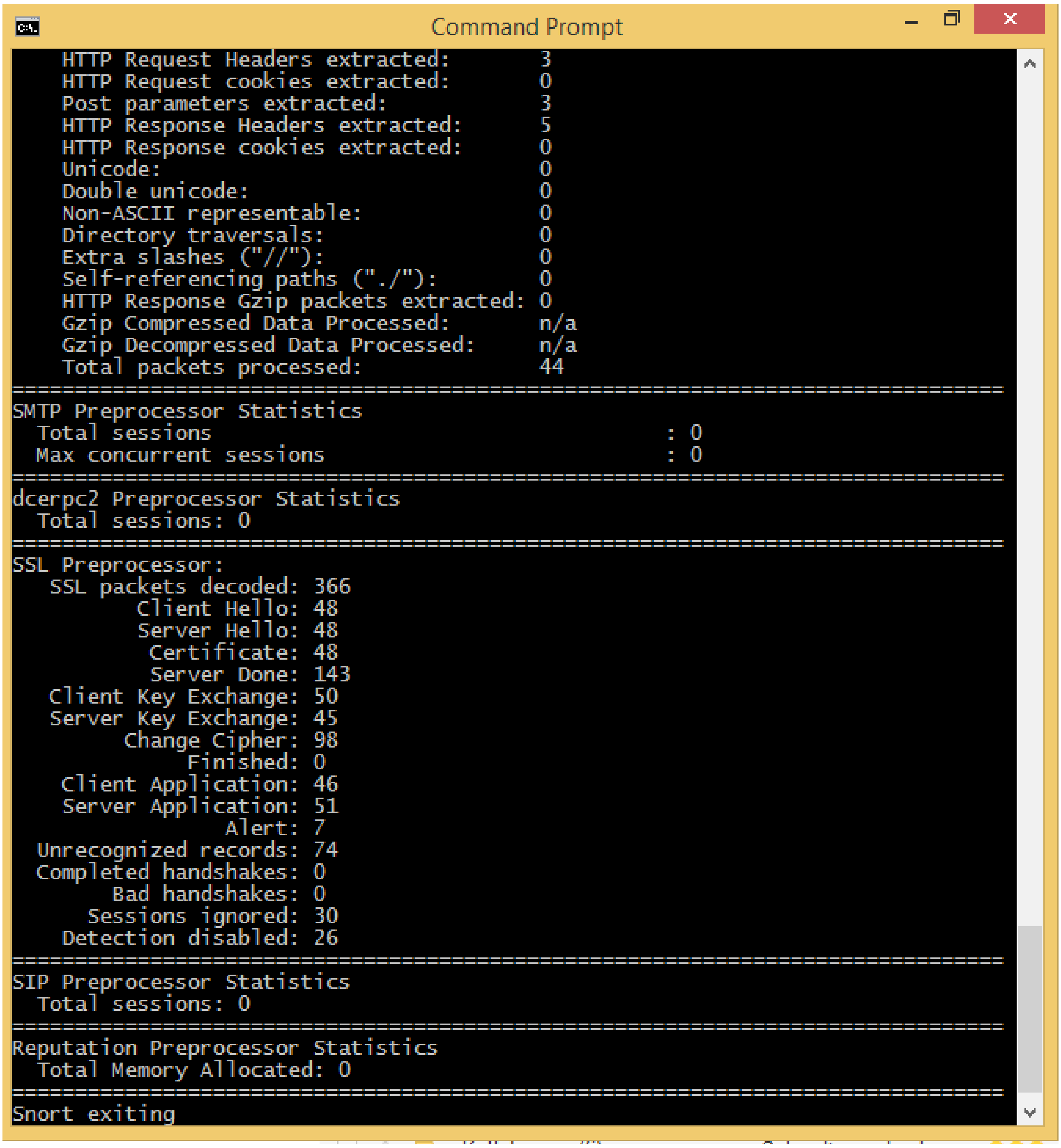
```
CP} 216.58.220.46:80 -> 10.0.0.2:49247
*** Caught Int-Signal
09/15-18:56:33.007217  [**] [1:100002:0] Testing UDP Alert [**] [Priority: 0] {U
DP} 10.0.0.2:137 -> 10.0.0.255:137
===============================================================================
Run time for packet processing was 143.682000 seconds
Snort processed 7427 packets.
Snort ran for 0 days 0 hours 2 minutes 23 seconds
   Pkts/min:         3713
   Pkts/sec:           51
===============================================================================
Packet I/O Totals:
   Received:         7421
   Analyzed:         7427 (100.081%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:         7431 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:         7378 ( 99.287%)
       Frag:            0 (  0.000%)
       ICMP:            8 (  0.108%)
        UDP:          185 (  2.490%)
        TCP:         7185 ( 96.690%)
        IP6:           41 (  0.552%)
    IP6 Ext:           41 (  0.552%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:           41 (  0.552%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
      EAPOL:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
```



```
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:           12 (  0.161%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:            0 (  0.000%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:            0 (  0.000%)
      Other:            0 (  0.000%)
Bad Chk Sum:            0 (  0.000%)
    Bad TTL:            0 (  0.000%)
     S5 G 1:            3 (  0.040%)
     S5 G 2:            1 (  0.013%)
      Total:         7431
================================================================================
Action Stats:
     Alerts:         7419 ( 99.839%)
     Logged:         7419 ( 99.839%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
      Event:            0
      Alert:          147
Verdicts:
      Allow:          727 (  9.797%)
      Block:            0 (  0.000%)
    Replace:            0 (  0.000%)
  Whitelist:         6700 ( 90.284%)
  Blacklist:            0 (  0.000%)
     Ignore:            0 (  0.000%)
     (null):            0 (  0.000%)
================================================================================
Frag3 statistics:
        Total Fragments: 0
      Frags Reassembled: 0
               Discards: 0
          Memory Faults: 0
               Timeouts: 0
               Overlaps: 0
              Anomalies: 0
                 Alerts: 0
```



```
                 Alerts: 0
                  Drops: 0
     FragTrackers Added: 0
    FragTrackers Dumped: 0
FragTrackers Auto Freed: 0
    Frag Nodes Inserted: 0
     Frag Nodes Deleted: 0
===============================================================================
===============================================================================
Stream statistics:
            Total sessions: 109
              TCP sessions: 39
              UDP sessions: 70
             ICMP sessions: 0
               IP sessions: 0
                TCP Prunes: 0
                UDP Prunes: 0
               ICMP Prunes: 0
                 IP Prunes: 0
TCP StreamTrackers Created: 39
TCP StreamTrackers Deleted: 39
              TCP Timeouts: 0
              TCP Overlaps: 0
       TCP Segments Queued: 229
     TCP Segments Released: 229
       TCP Rebuilt Packets: 147
         TCP Segments Used: 206
              TCP Discards: 39
                  TCP Gaps: 9
      UDP Sessions Created: 70
      UDP Sessions Deleted: 70
              UDP Timeouts: 0
              UDP Discards: 0
                    Events: 4
           Internal Events: 0
           TCP Port Filter
                  Filtered: 0
                 Inspected: 0
                   Tracked: 7181
           UDP Port Filter
                  Filtered: 0
                 Inspected: 0
                   Tracked: 70
===============================================================================
HTTP Inspect - encodings (Note: stream-reassembled packets included):
    POST methods:                         2
    GET methods:                          0
    HTTP Request Headers extracted:       3
    HTTP Request cookies extracted:       0
```



```
    HTTP Request Headers extracted:       3
    HTTP Request cookies extracted:       0
    Post parameters extracted:            3
    HTTP Response Headers extracted:      5
    HTTP Response cookies extracted:      0
    Unicode:                              0
    Double unicode:                       0
    Non-ASCII representable:              0
    Directory traversals:                 0
    Extra slashes ("//"):                 0
    Self-referencing paths ("./"):        0
    HTTP Response Gzip packets extracted: 0
    Gzip Compressed Data Processed:       n/a
    Gzip Decompressed Data Processed:     n/a
    Total packets processed:              44
===============================================================================
SMTP Preprocessor Statistics
  Total sessions                                    : 0
  Max concurrent sessions                           : 0
===============================================================================
dcerpc2 Preprocessor Statistics
  Total sessions: 0
===============================================================================
SSL Preprocessor:
   SSL packets decoded: 366
          Client Hello: 48
          Server Hello: 48
           Certificate: 48
           Server Done: 143
   Client Key Exchange: 50
   Server Key Exchange: 45
         Change Cipher: 98
              Finished: 0
    Client Application: 46
    Server Application: 51
                 Alert: 7
  Unrecognized records: 74
  Completed handshakes: 0
        Bad handshakes: 0
      Sessions ignored: 30
    Detection disabled: 26
===============================================================================
SIP Preprocessor Statistics
  Total sessions: 0
===============================================================================
Reputation Preprocessor Statistics
  Total Memory Allocated: 0
===============================================================================
Snort exiting
```