Software Testing Lab (PMCA614P)

Reg No: 23MCA1030

Name: Vinayak Kumar Singh

Experiment: 6

Date: 15.03.2024

Penetration Testing

Question: We received a pcap file from an organization to investigate who has forwarded their secret receipt.

File used: **evidence01.pcap**

Procedure:

Step 1: Install Wireshark

Step 2: open Wireshark

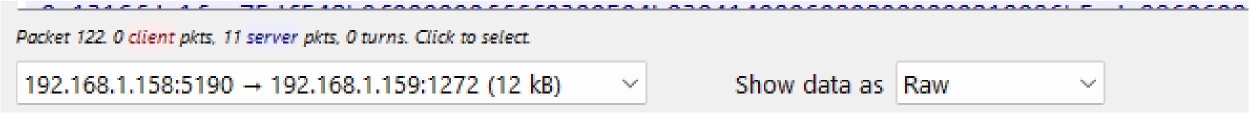
Step 3: Search TCP

Step 4: Right Click on any light green tcp follow then

Step 5: Go to follow -> TCP Stream

Step6: Increase Stream from 1 to 2

Step7: Select Raw Data like this



Packet 122. 0 client pkts, 11 server pkts, 0 turns. Click to select.

192.168.1.158:5190 → 192.168.1.159:1272 (12 kB)

Show data as Raw

Find the following from the enclosed file:

1. What is the name of users IM buddy?

Sec558user1

2. What was the first comment in the captured IM conversation?

Here's the secret recipe... I just downloaded it from the file server. Just copy to a thumb drive and you're good to go &gt;

3. What is the name of the file transferred?

recipe.docx

4. What is the magic number of the file you want to extract (first four bytes)?

OFT2

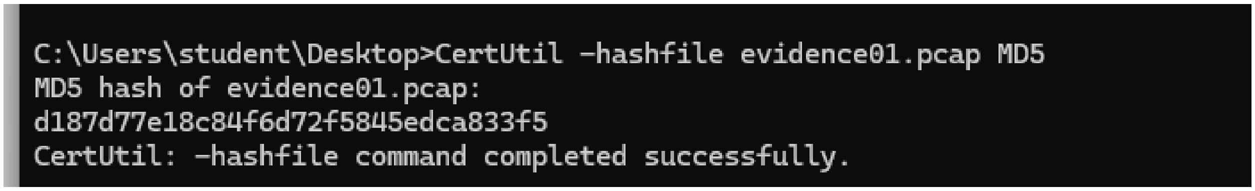
50 4B 03 04

5. What was the MD5sum of the file?

For windows:

1. Open cmd
2. Do cd desktop
3. Do dir
4. Then do CertUtil -hashfile evidence01.pcap MD5

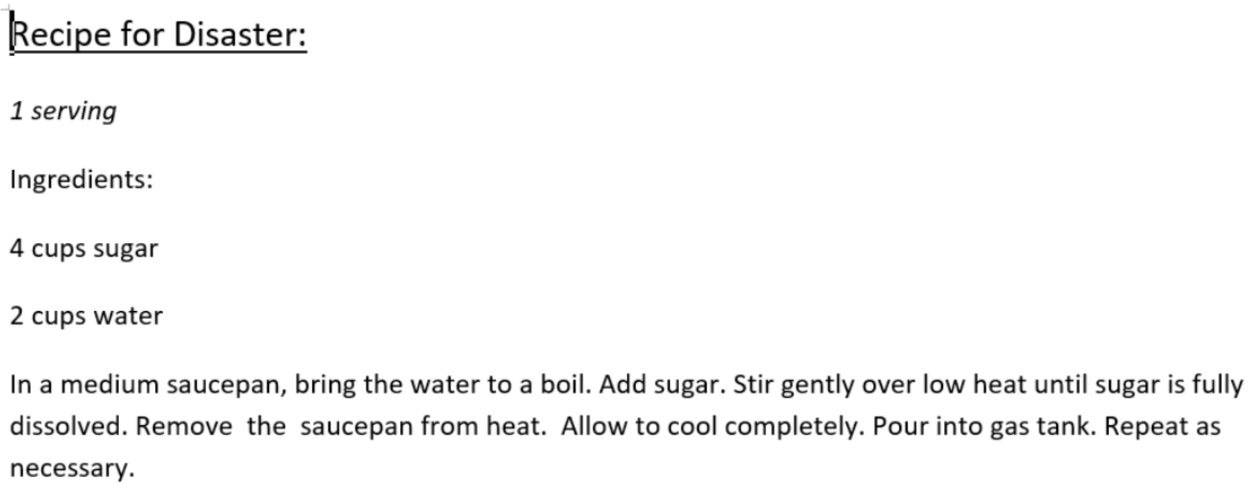
d187d77e18c84f6d72f5845edca833f5



```
C:\Users\student\Desktop>CertUtil -hashfile evidence01.pcap MD5
MD5 hash of evidence01.pcap:
d187d77e18c84f6d72f5845edca833f5
CertUtil: -hashfile command completed successfully.
```

6. What is the secret recipe?

recipe.docx



Recipe for Disaster:

1 serving

Ingredients:

4 cups sugar

2 cups water

In a medium saucepan, bring the water to a boil. Add sugar. Stir gently over low heat until sugar is fully dissolved. Remove the saucepan from heat. Allow to cool completely. Pour into gas tank. Repeat as necessary.