**CEG4430/6430 Cyber Network Security**  
 **Project 1**

a.

a.   
b.

c.   
d.   
e.

f.

a.   
b.

c.   
d.   
e.

f.   
g.

h.   
i.

j.

protocol used in any connection in this trace? If so, please   
identify following information (11 Points)

**Parsing Network Packet Trace Using Wireshark**

**Objective**

To use the Wireshark tool to perform packet/traffic analysis of a given traffic trace.

This project must be completed individually.

**Pcap File:**

You can download a file of pcap network traffic trace from this URL (    
[https://www.dropbox.com/s/84cb2s774b8q602/botTrace?dl=0)](https://www.dropbox.com/s/84cb2s774b8q602/botTrace?dl=0)

Wireshark:

Please download and install Wireshark [(https://www.wireshark.org](https://www.wireshark.org/)[) on your own computer or in VCSL](https://www.wireshark.org)   
[virtual machine.](https://www.wireshark.org)

You should learn how to use the “display filter” function in Wireshark to facilitate your analysis.

**Questions:**

Please answer the following questions based on your analysis of the traffic.

1.

What is the first TCP packet captured in this trace? Please provide the following information for   
this packet. (2 Points)

Timestamp: Oct 29, 2007 15:58:45.682083000 Eastern Daylight Time  
 Source IP address: 192.168.1.132

Destination IP address: 192.168.1.128  
 Source Port: 1177

Destination Port: 6667

Sequence Number (absolute value): 0  
 Acknowledge Number (absolute value): 0

SYN Flag: Set  
 ACK Flag: Not Set

RST Flag: Not Set

2.   Does  this  trace  contain  any  UDP  packet?  If  so,  please  identify  the  first  UDP  packet  with  the   
 following information: (2 Points)

3.

Timestamp:   
 Source IP address:

Destination IP address:   
 Source Port:

Destination Port:   
 Checksum:

Is the IRC protocol (application-level)

IP address  of the server (2 Points)

b.   IP address(es)  of  clients  that  successfully  established  connections  with  the  server (2   
 Points)

c.   [You  can  find  the  IRC  protocol  at  https://www.ietf.org/rfc/rfc1459.txt.  Does  any  IRC](https://www.ietf.org/rfc/rfc1459.txt)   
 [client generate a packet that contains the following IRC keywords? Please show evidence](https://www.ietf.org/rfc/rfc1459.txt)

in your answer. (7 Points)

i.   
 ii.

iii.   
 iv.

v.   
 vi.

vii.

PRIVMSG   
PING

PONG   
JOIN

KICK   
MODE

TOPIC

4.

We  consider  Host-A  initiates  a  failed  TCP  session  to  Host-B  if  the  following  two  conditions  are   
satisfied: 1. Host-A  sends  a  SYN  packet  to  Host-B  (to  initiate  a  new TCP  session);  2.  Host-B

sends no packet to Host-A or only RST packet(s) (for this session). For all IRC clients observed in   
this  trace,  does  any  of  them  initiate  more  than  10  failed  connections?  If  so,  please  show  their  IP

addresses and evidence. (5 Points)