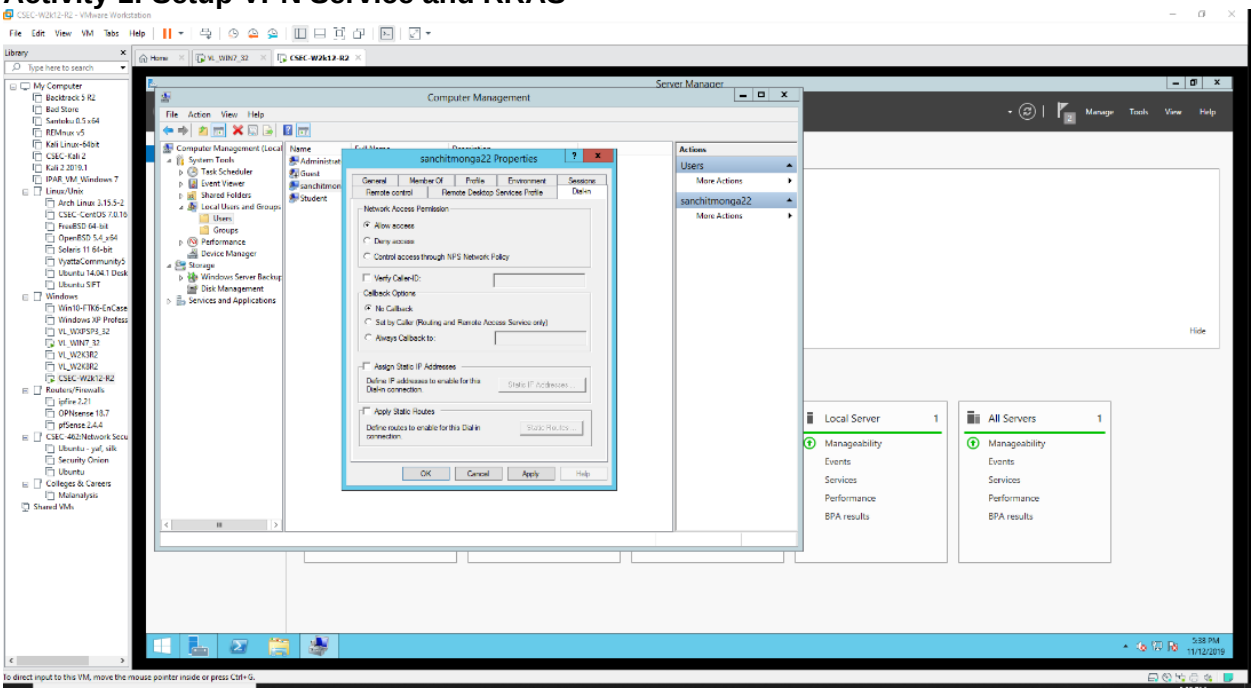
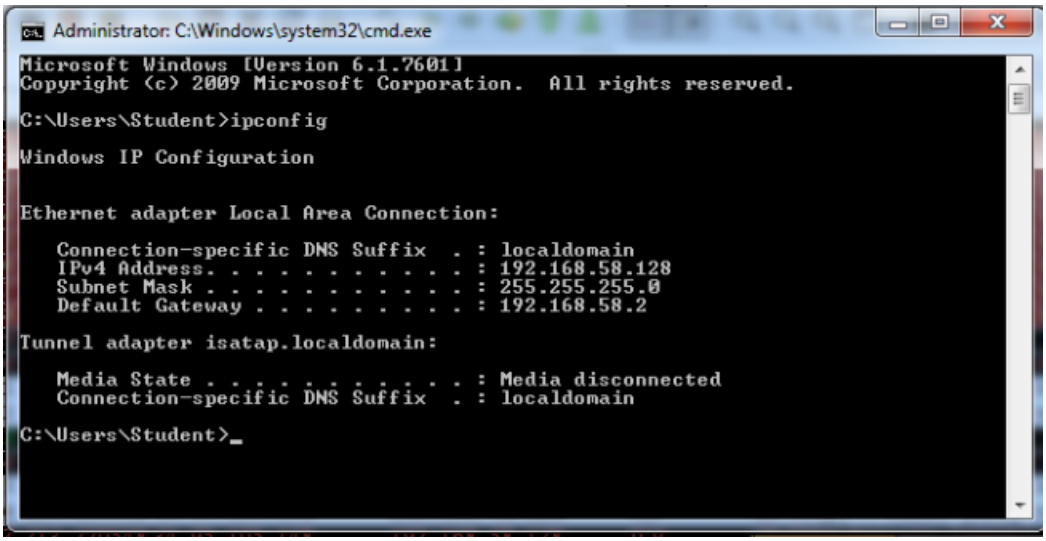
Name: Sanchit Monga

Activity 1: Setup VPN Service and RRAS

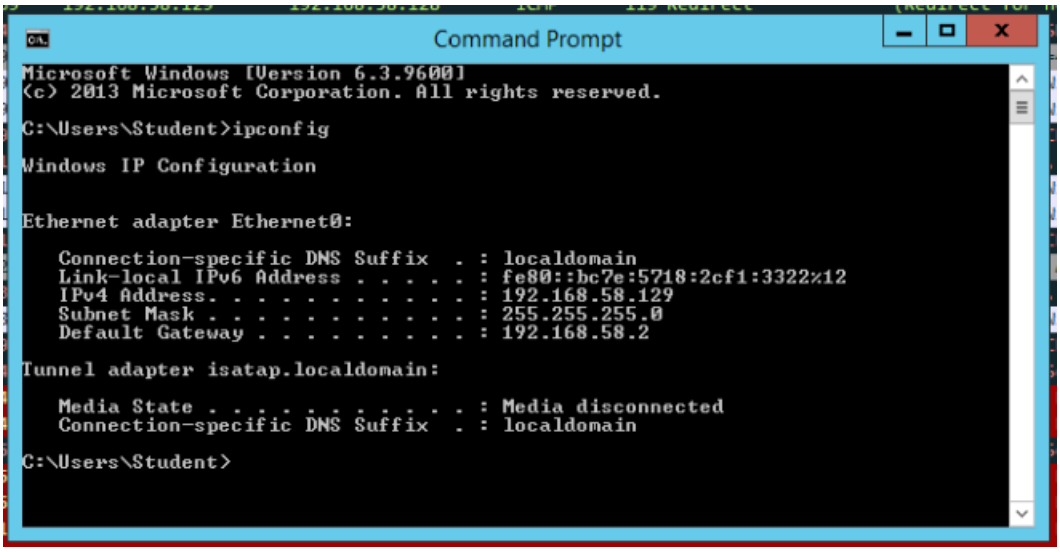


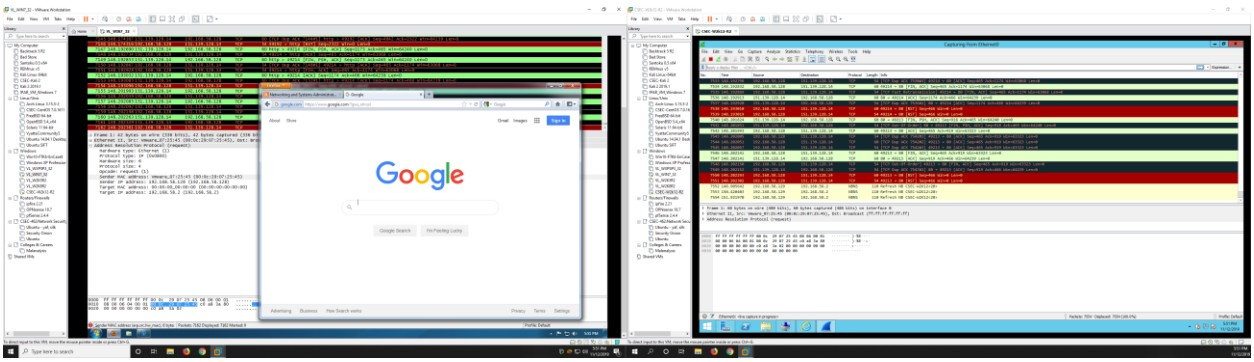
Activity 3: VPN Client – Network Connection Setup

Windows 7 VM Client



Windows Server 2016





1. (5 Points) After you successfully connected to the VPN server, what changes were made to the network connections.

   When successfully connection to the vpn was made, the vpn basically acts as a bridge called a WAN Miniport (PPTP) which basically runs through your current local area connection.

2. (5 Points) What is the purpose of this addition?

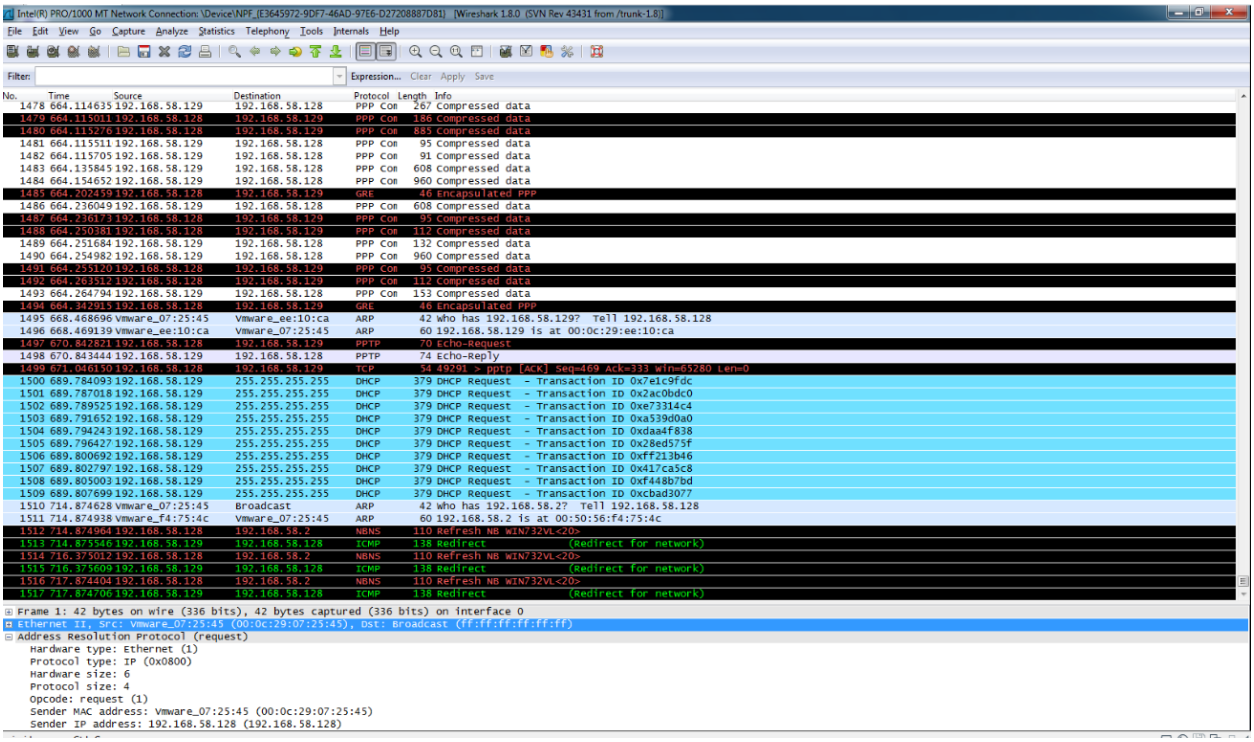
   Using MS CHAP V2 authentication and MPPE 128 encryption, it helps re-route and protect outgoing connections by sending your outgoing packets to the vpn first, then transferring it to the destination from the vpn, thus in a sense, hiding your source computer's vpn.

3. (30 Points) Fill in the following IP addresses from your setup in Activity 1 & 3.

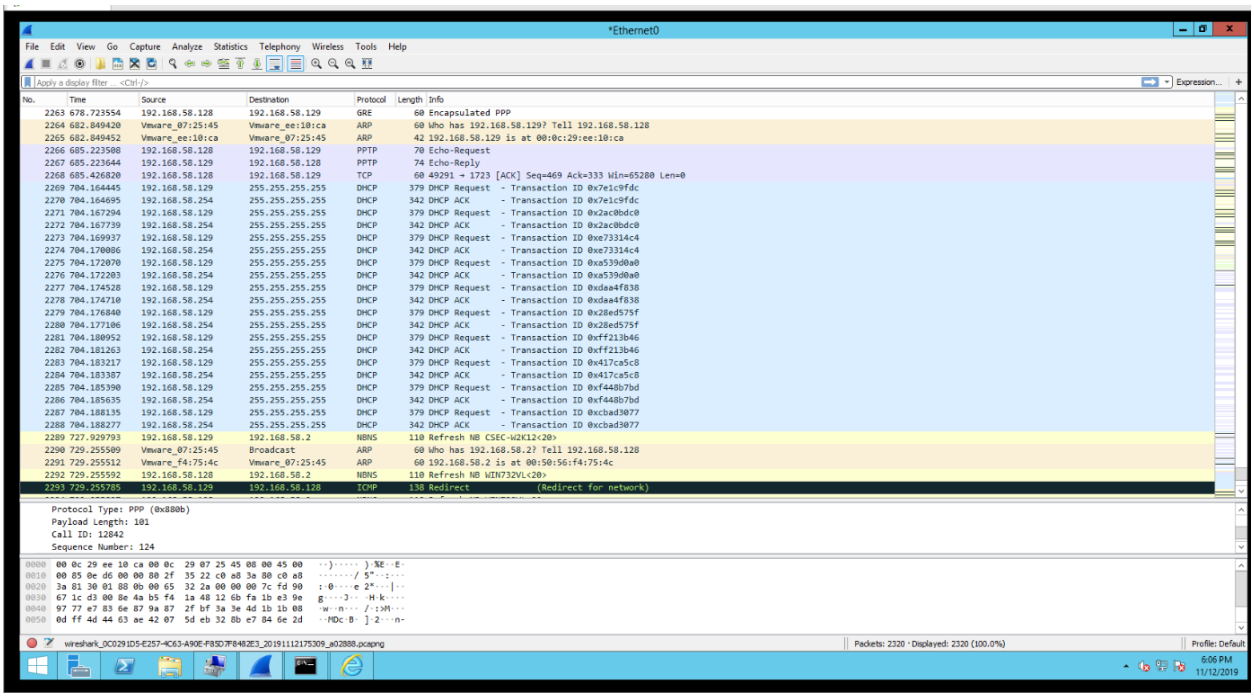
IP Address of VPN Server Ethernet interface	192.168.58.129
IP Address of Windows 7 VM Client	192.168.58.128
IP Address Associated with the VPN client at the VPN Server: **You can get this IP Address after you finish Activity 3**	192.168.58.255

Activity 4: Analyzing VPN traffic

Windows 7 capture



Windows Server 2016



4. (10 Points) What was different between the capture in Activity 3 and the capture in Activity 4? Use the screenshots you capture to justify your answers.
   The VPN is activated and sending all requests through the VPN server and back through encapsulated PPP packages and GRE.

5. (30 Points) What were the two protocols that Wireshark showed being used between your client and the VPN server?
   Briefly describe the function provided by this protocol
   It uses two protocols of PPTP and GRE:
   (i) PPTP stands for point to point tunneling protocol and sends encapsulated PPP packets between the server and the client.
   (ii) GRE stands for Generic Routing Encapsulation and creates a private point to point connection and encases multiple protocols into one for transferring data from server to client and vice versa.

6. (20 Points) What would happen if the VPN Server Firewall was on and was blocking Port number 500? What protocols use this port?

   It won't be possible to establish VPN tunneling as it won't allow a vpn key to authenticate with the server.

   Port 500 is used by most IPSEC-based VPN systems for the establishment of securely encrypted "tunnels" between endpoint machines.