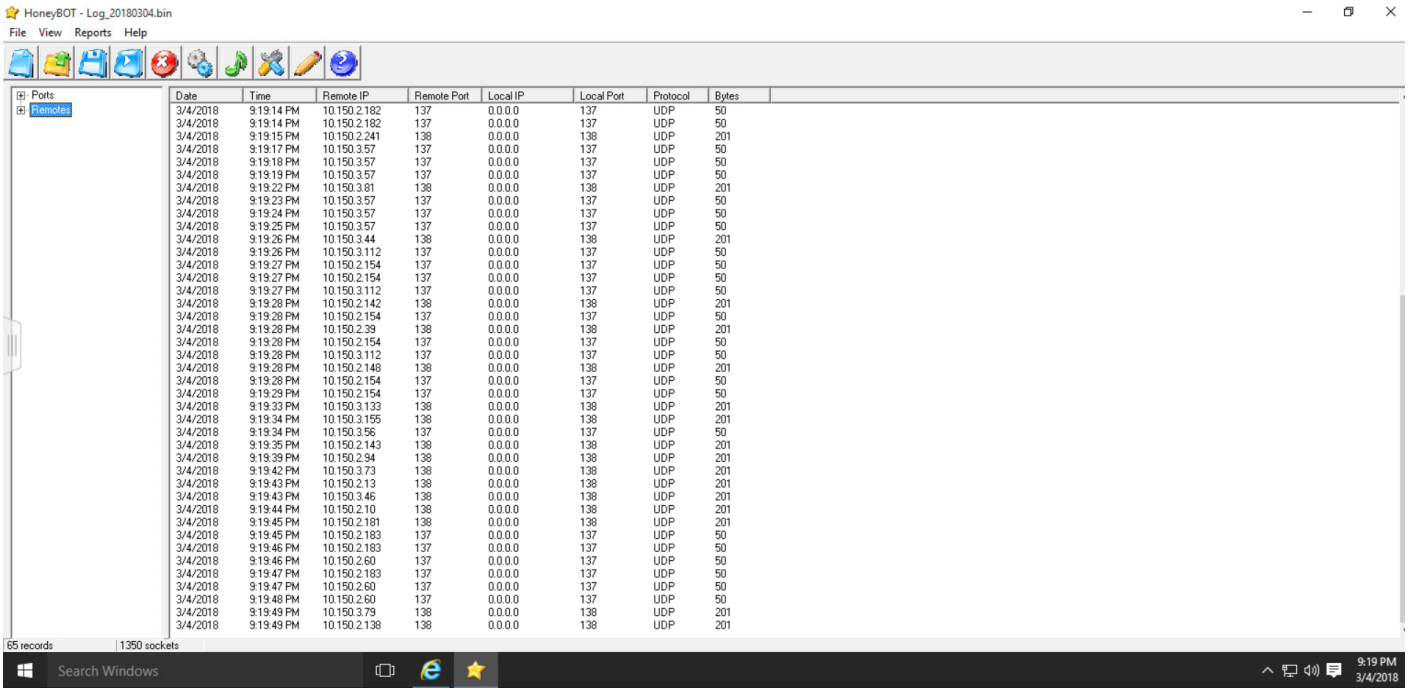
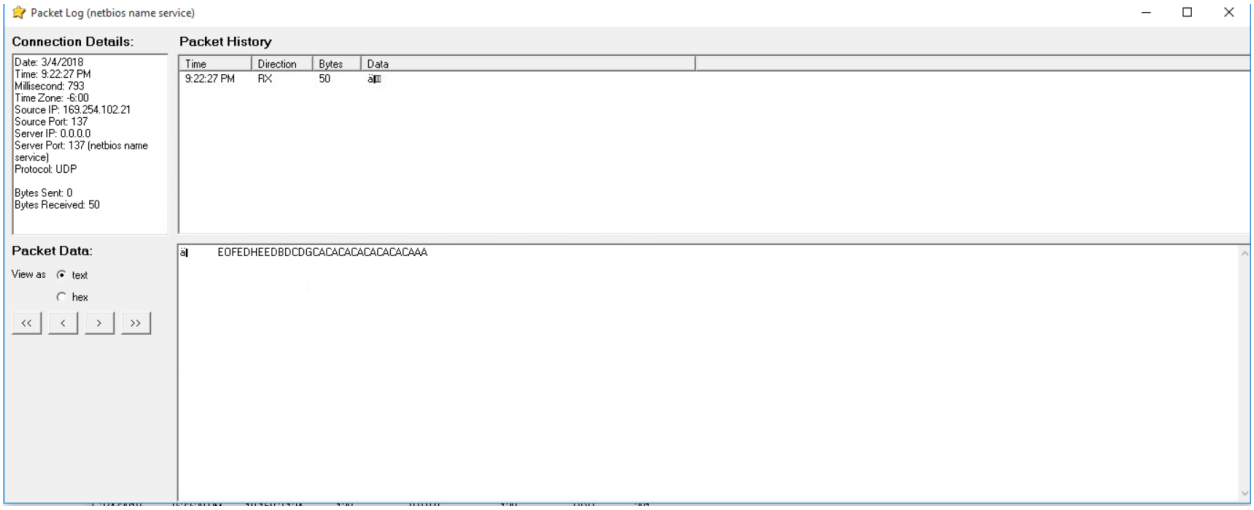
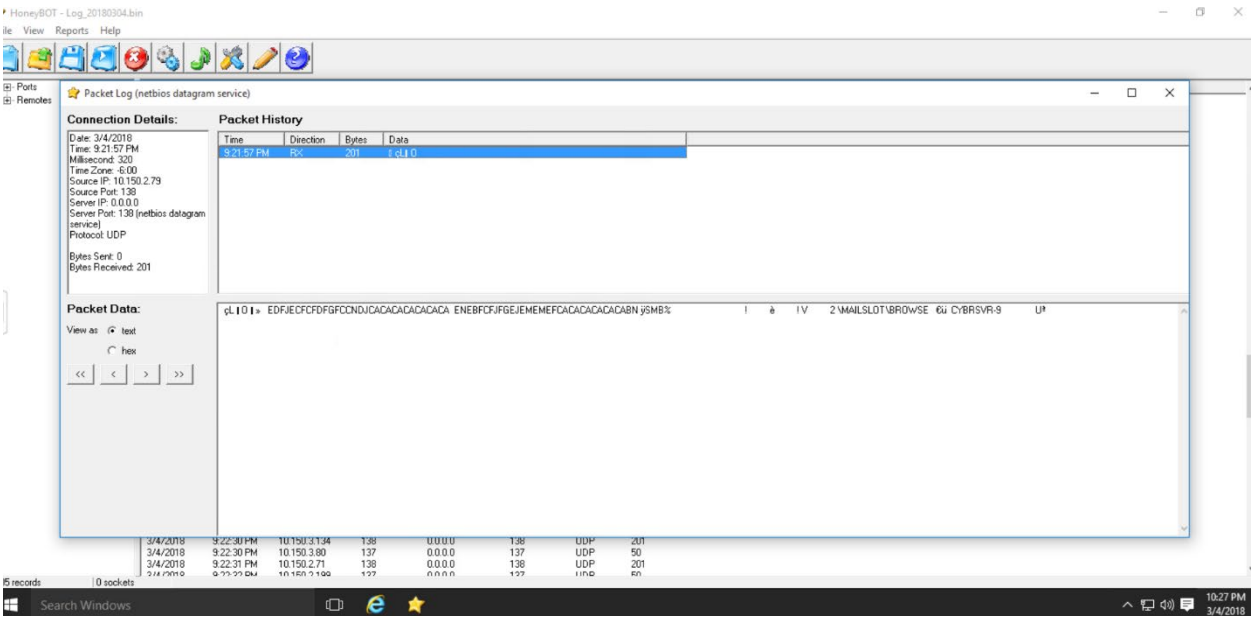
+

Due to issues with the VM server I was only able to get two ports 137 and 138. If there is a way to gain access to all the ports I will redo the project

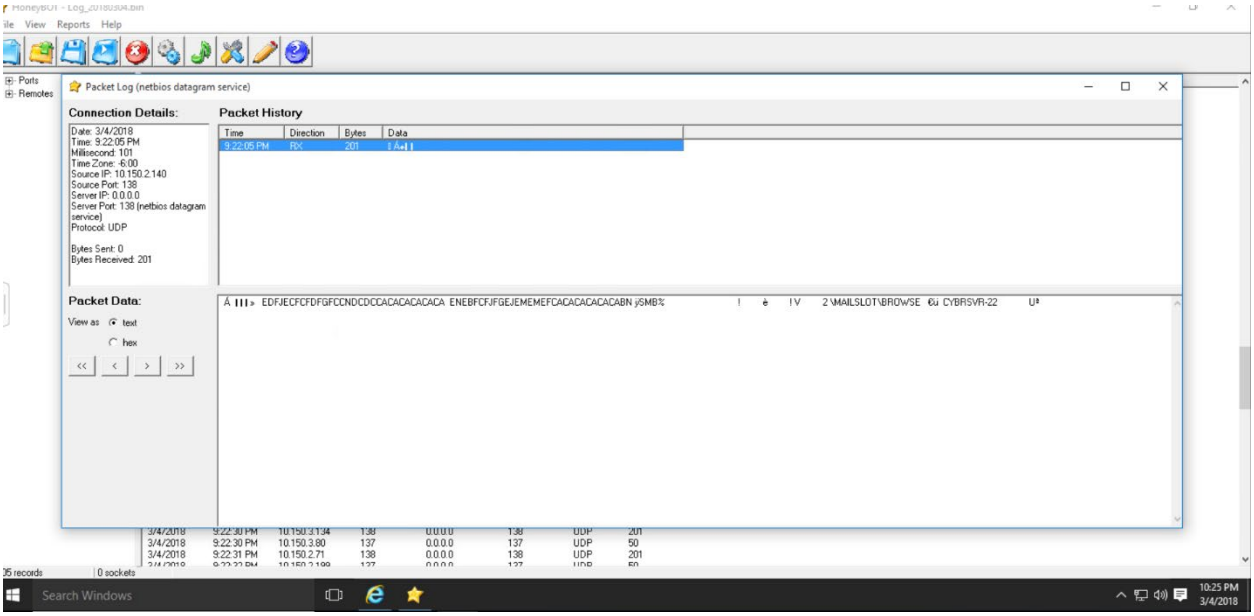




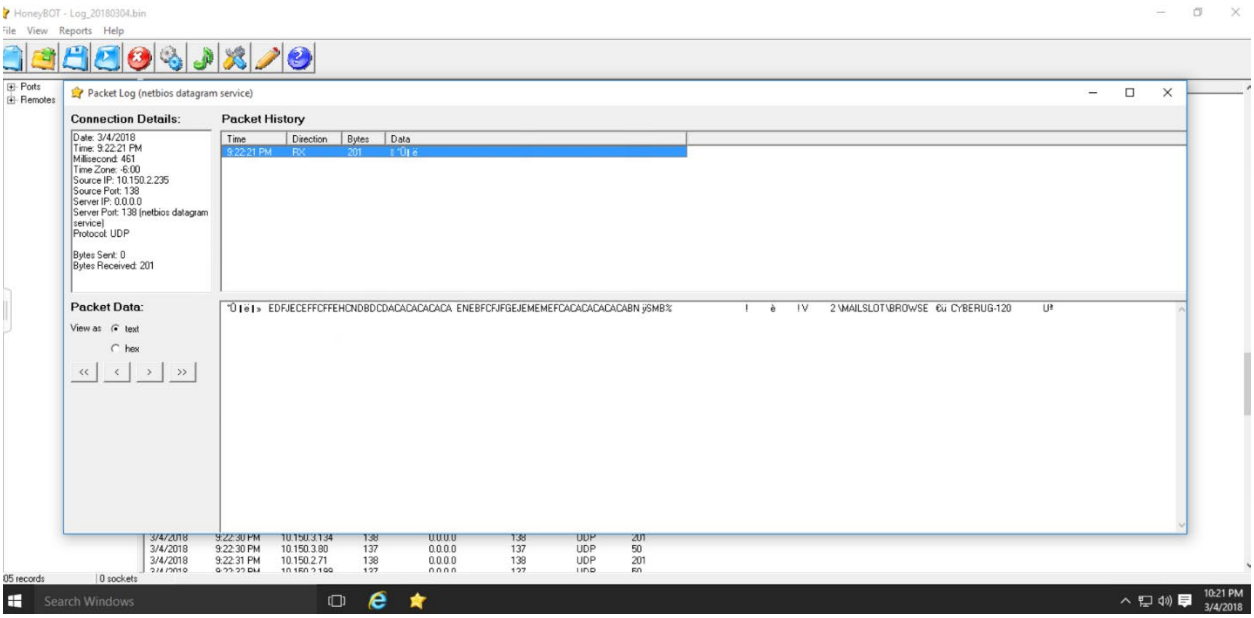
The Packet log detail shows that it was accessed on March 4, 2018, at 9:22 PM. Honeypot received the data, but there was not any sent out. The RX in the description box lets me know that information was collected. Also, the connection details box, further confirms this by showing the number of bytes sent out and received. The server port and the local port are the same. The port that the remote IP address attempted to access was UDP port 137. Port 137 is also known as NetBIOS name server. The remote host sent a message to local host to get the IP address for the NetBIOS name.



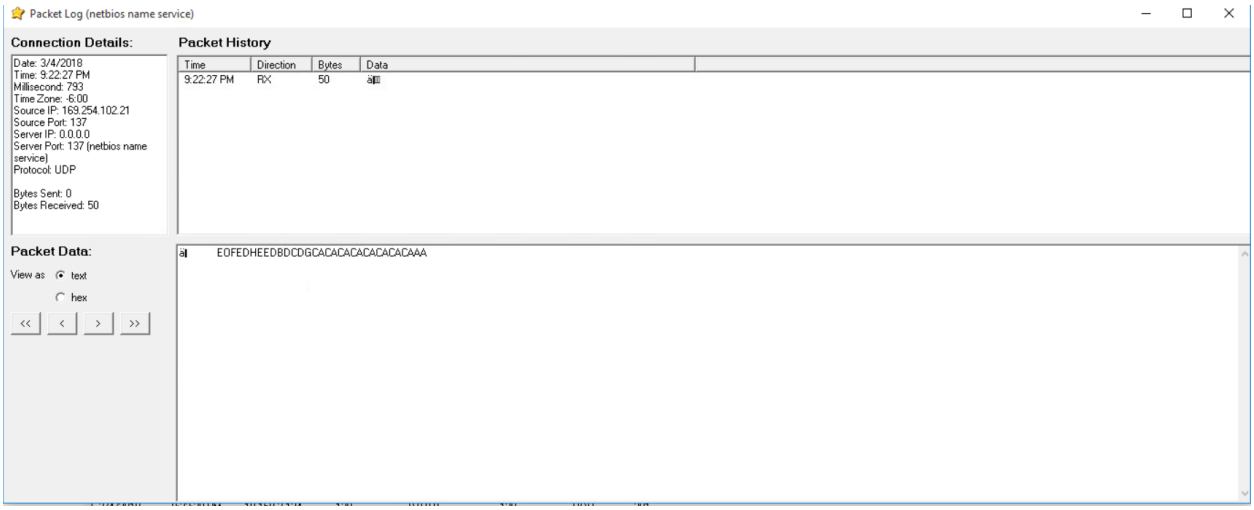
The Packet entry in the screenshot below was logged on 3/4/18 at 9:21:57 PM. The local host received 201 bytes from the remote host at IP: 10.150.2.79. The remote host sent information through the 138 ports. NetBIOS datagrams are exchanged over the internet using this port. There was also mail browser message sent to the UDP port 138.



The Packet above was accessed at 9:22:05 PM on March 4th, 2018. This was another attempt made by the remote host to send a message to the UDP port 138. There was 201 bytes received but HoneyBOT didn't send anything back. Which is why there is 0 bytes sent. The remote server didn't get response previously so it attempts to make another connection by sending a mail slot to cyberserv-22.



This Packet log shows another attempt made by a different IP address to send a message over UDP port 138. The remote host tried to send the message to a different local host cyber-rug 120. HoneyBOT didn't sent an announcement message back to the server port 138.



This Packet was logged at 9:22:27 PM on March 4, 2018. A NetBIOS name service request was made by the remote host. The remote host IP address is 169.254.102.21. The name service request was made over the UDP port 137. This was an attempt to find out the IP Address of the NetBIOS name server. HoneyBOT didn't respond to the request.