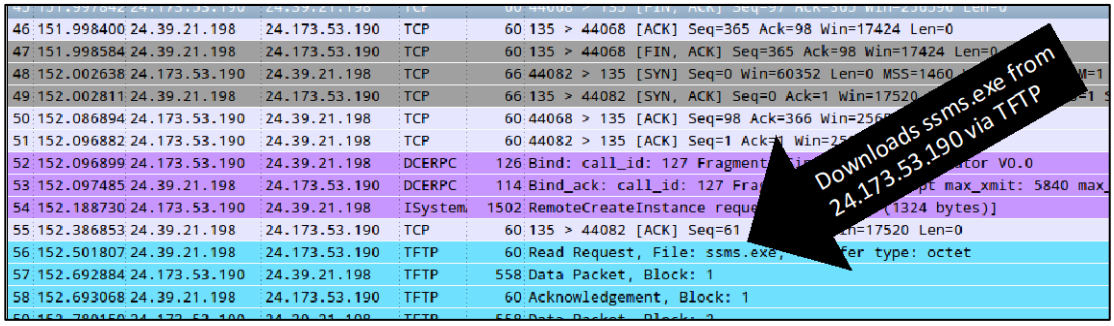
Part 1 – Analysis of 24.39.21.198

This section provides answers and a method of solving each of the lab questions. Note that there may be more than one way to arrive at the correct answer. You may discover a different solution to the same problem.

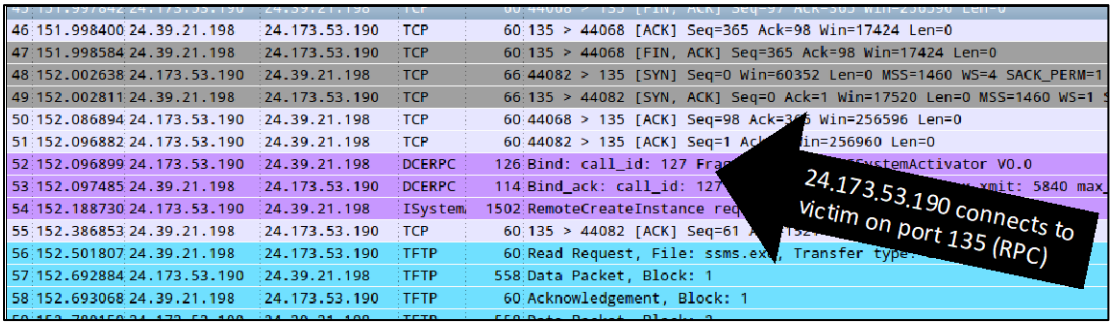
1. For the first several questions, start by filtering on the victim IP address in Wireshark to only show traffic going to and coming from it (i.e., ip.addr == 24.39.21.198). Near the beginning of the packet list, there is traffic indicating the victim requested ssms.exe from 24.173.53.190 using TFTP.



46	151.998400	24.39.21.198	24.173.53.190	TCP	60	135 > 44068 [ACK] Seq=365 Ack=98 Win=17424 Len=0
47	151.998584	24.39.21.198	24.173.53.190	TCP	60	135 > 44068 [FIN, ACK] Seq=365 Ack=98 Win=17424 Len=0
48	152.002638	24.173.53.190	24.39.21.198	TCP	66	44082 > 135 [SYN] Seq=0 Win=60352 Len=0 MSS=1460
49	152.002811	24.39.21.198	24.173.53.190	TCP	66	135 > 44082 [SYN, ACK] Seq=0 Ack=1 Win=17520
50	152.086894	24.173.53.190	24.39.21.198	TCP	60	44068 > 135 [ACK] Seq=98 Ack=366 Win=256
51	152.096882	24.173.53.190	24.39.21.198	TCP	60	44082 > 135 [ACK] Seq=1 Ack=1 Win=25
52	152.096899	24.173.53.190	24.39.21.198	DCERPC	126	Bind: call_id: 127 Fragment
53	152.097485	24.39.21.198	24.173.53.190	DCERPC	114	Bind_ack: call_id: 127 Fra
54	152.188730	24.173.53.190	24.39.21.198	ISystem	1502	RemoteCreateInstance reque
55	152.386853	24.39.21.198	24.173.53.190	TCP	60	135 > 44082 [ACK] Seq=61
56	152.501807	24.39.21.198	24.173.53.190	TFTP	60	Read Request, File: ssms.exe,
57	152.692884	24.173.53.190	24.39.21.198	TFTP	558	Data Packet, Block: 1
58	152.693068	24.39.21.198	24.173.53.190	TFTP	60	Acknowledgement, Block: 1

As noted in the course material and hints, attackers commonly use TFTP to download files. This traffic likely indicates *ssms.exe* as the name of the malware executable, *TFTP* as the download protocol, and *24.172.53.190* as the source. The download source may also be the IP address of the attacker as well. More analysis is necessary to confirm this hypothesis.

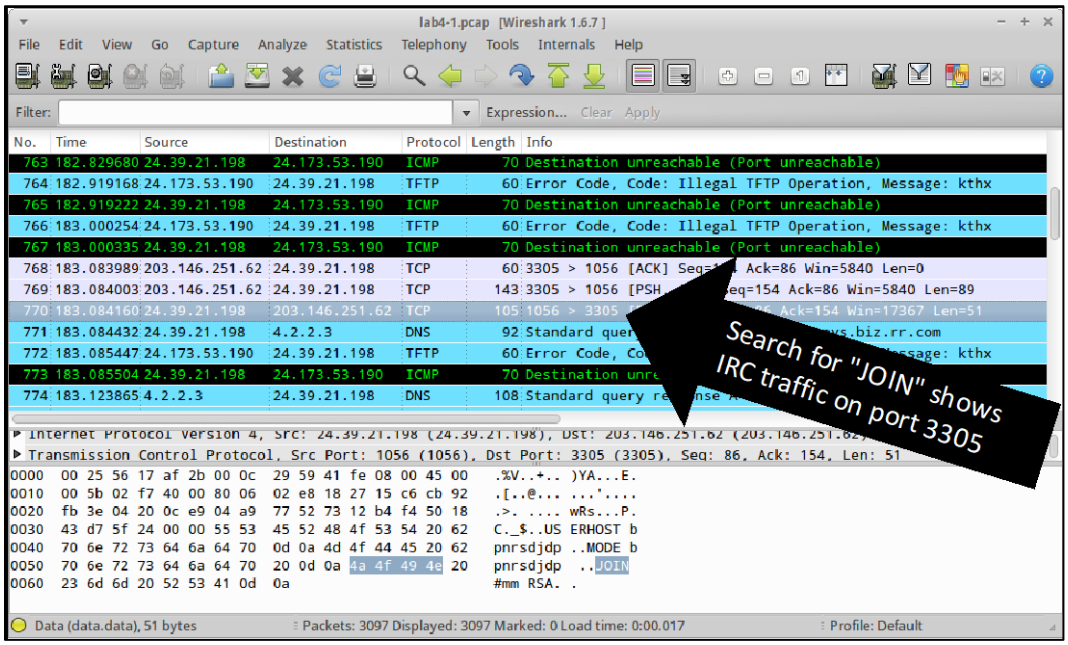
2. Further analyze the packets leading up to the TFTP session by working backwards in the packet list. Notice 24.173.53.190 also connected to the victim over TCP port 135 (i.e., RPC protocol) immediately before the TFTP session. Attackers commonly use this port to compromise older Windows systems.



46	151.998400	24.39.21.198	24.173.53.190	TCP	60	135 > 44068 [ACK] Seq=365 Ack=98 Win=17424 Len=0
47	151.998584	24.39.21.198	24.173.53.190	TCP	60	135 > 44068 [FIN, ACK] Seq=365 Ack=98 Win=17424 Len=0
48	152.002638	24.173.53.190	24.39.21.198	TCP	66	44082 > 135 [SYN] Seq=0 Win=60352 Len=0 MSS=1460 WS=4 SACK_PERM=1
49	152.002811	24.39.21.198	24.173.53.190	TCP	66	135 > 44082 [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 MSS=1460 WS=1
50	152.086894	24.173.53.190	24.39.21.198	TCP	60	44068 > 135 [ACK] Seq=98 Ack=366 Win=256596 Len=0
51	152.096882	24.173.53.190	24.39.21.198	TCP	60	44082 > 135 [ACK] Seq=1 Ack=1 Win=256960 Len=0
52	152.096899	24.173.53.190	24.39.21.198	DCERPC	126	Bind: call_id: 127 Fragment
53	152.097485	24.39.21.198	24.173.53.190	DCERPC	114	Bind_ack: call_id: 127
54	152.188730	24.173.53.190	24.39.21.198	ISystem	1502	RemoteCreateInstance req
55	152.386853	24.39.21.198	24.173.53.190	TCP	60	135 > 44082 [ACK] Seq=61
56	152.501807	24.39.21.198	24.173.53.190	TFTP	60	Read Request, File: ssms.exe, Transfer type:
57	152.692884	24.173.53.190	24.39.21.198	TFTP	558	Data Packet, Block: 1
58	152.693068	24.39.21.198	24.173.53.190	TFTP	60	Acknowledgement, Block: 1

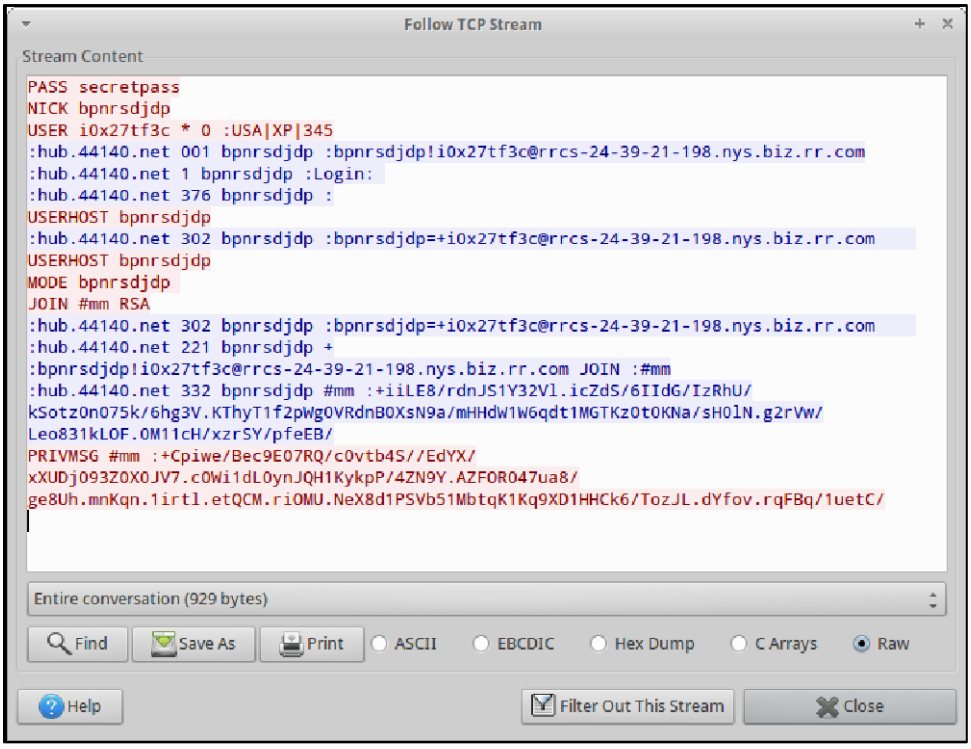
This session may have included an RPC exploit that compromised the victim system and initiated the download of the ssms.exe file. This information likely indicates *24.172.53.190* as the attacker as well, making *TCP port 135* and *RPC* the exploited port and protocol.

3. For the remaining questions, use Wireshark to identify potential "phone home" attempts (a.k.a., C2). As noted in the course materials and hints, bots have been known to use IRC for C2 communication. Use Wireshark's "Find Packet" feature to look for indications of IRC. Select **Edit** > **Find Packet** and enter "JOIN" in the text field. Be sure to select "String" and "Packet bytes" in the respective **Find** and **Search In** portions of the window and press **Find** when ready.



One of the first results appears to indicate the victim "phoning home" to *203.146.251.62* over *TCP port 3305* using the *IRC* protocol. Note, IRC usually runs over TCP port 6667, making this traffic even more suspicious. More analysis is necessary to confirm this hypothesis.

4. Further analyze this packet using Wireshark's analysis capabilities. Right-click on the suspect packet and select **Follow TCP Stream**.



This stream confirms IRC C2 communication as noted in the course materials. Red text indicates what the victim sent to the channel and/or operator. Blue text shows what the victim host received (e.g., activities taking place in the channel like messages/files from the IRC server and advertisements from other compromised hosts).

Answers

- What was the IP address of the attacker? **24.172.53.190**
- What port & protocol were exploited on the victim? **135/TCP & RPC**
- What was the name of the malware executable? **ssms.exe**
- What protocol was used to download the malware? **TFTP**
- What IP was the malware downloaded from? **24.172.53.190**
- What port & protocol were used to "phone home?" **3305/TCP & IRC**
- What IP address did the victim "phone home" to? **203.146.251.62**