

Mawlana Bhashani Science and Technology University



Lab-Report

Report No: 04

Course code: ICT-4202

Course title: Wireless and Mobile Communication Lab

Date of Performance: 11.09.2020

Date of Submission: 18.09.2020

Submitted by

Name: Shourove Sutradhar Dip

ID: IT-16008

4th year 2nd semester

Session: 2015-2016

Dept. of ICT, MBSTU

Submitted To

Nazrul Islam

Assistant Professor

Dept. of ICT

MBSTU.

Experiment N0: 04

Name of Experiment: Protocol Analysis with Wireshark.

Objectives:

1. Learn how to analyze protocols.
2. Understand how network protocols work.
3. Learn to use Wireshark to capture network packets in real time and display them in human-readable format.
4. Learn to use Wireshark for network troubleshooting and communication protocol analysis.

Procedures:

Step 1- Capturing:

Packets and Protocols can be analyzed after capture. To capture, first I go to capture menu and select options. Then I start capturing on interface that has IP address.

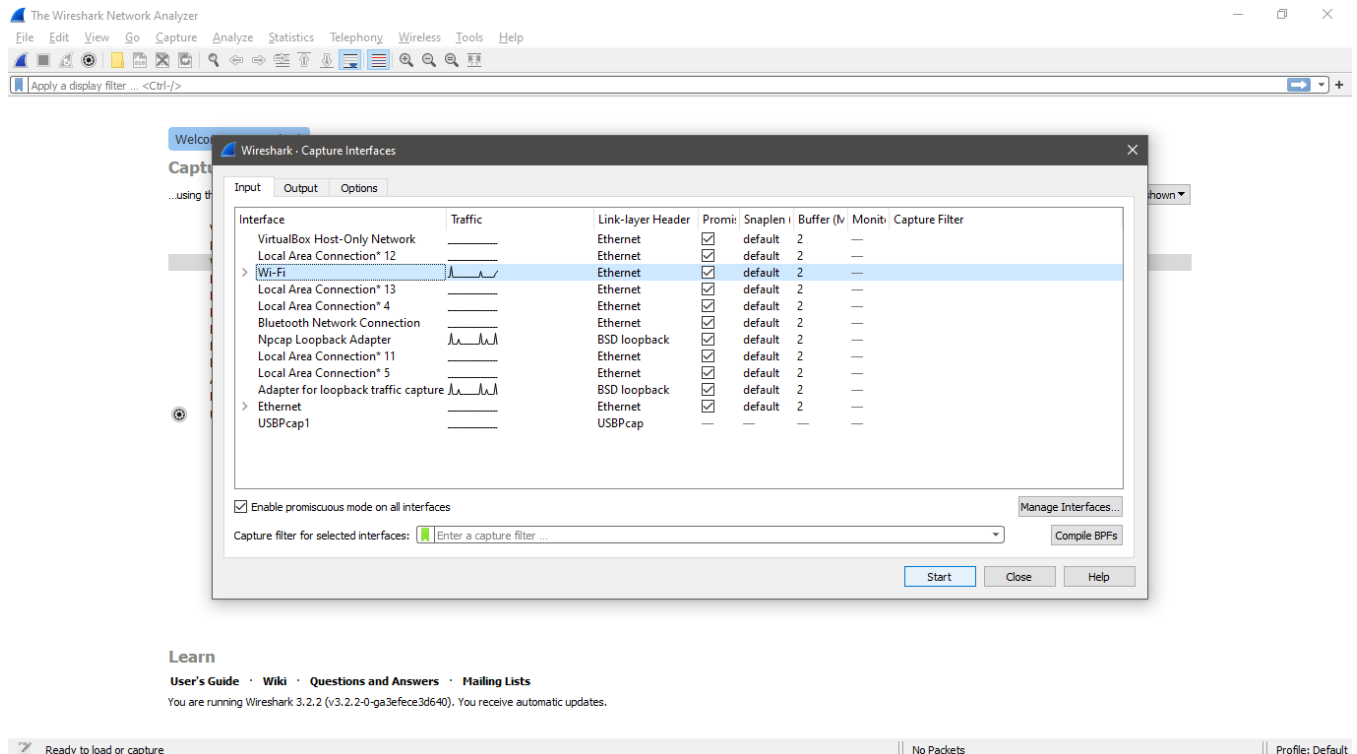


Figure-1.1: Starting Capture

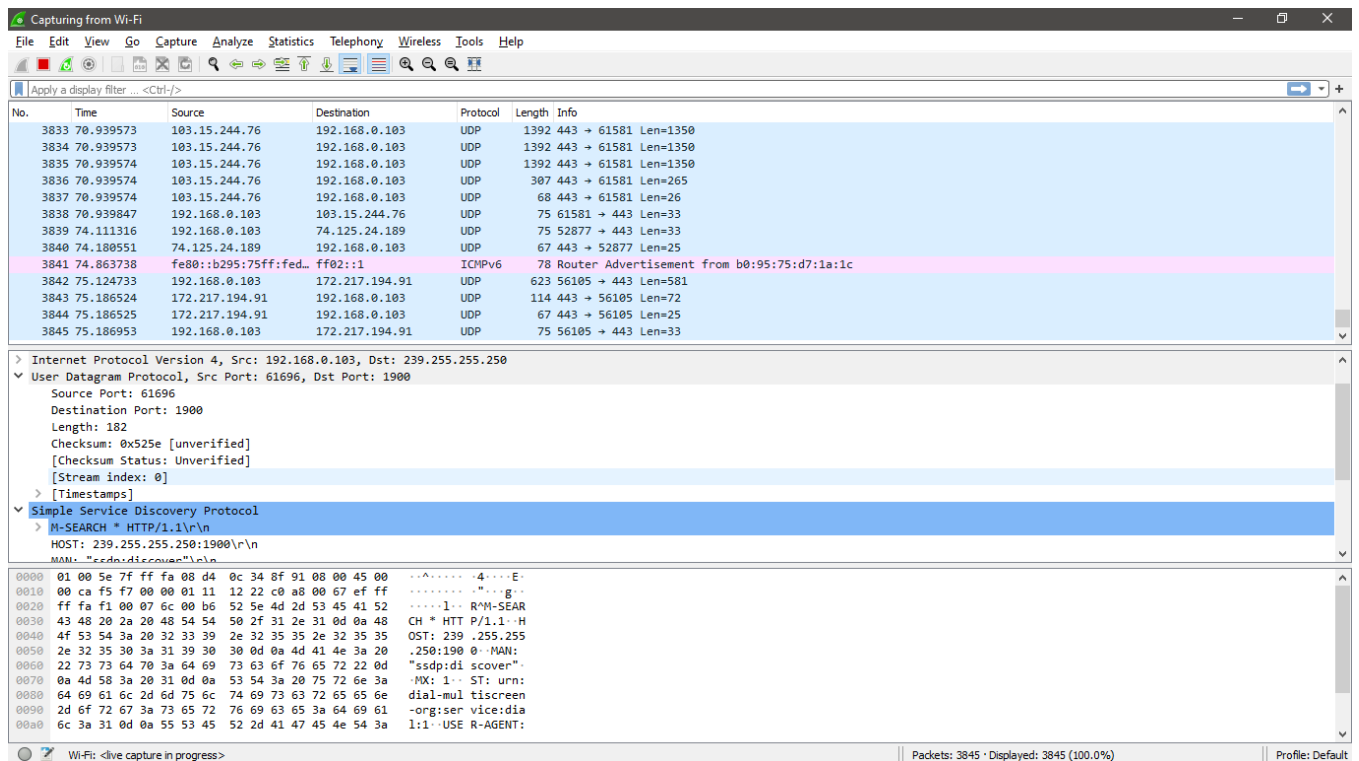


Figure-1.2: Dumped packages in main window of Wireshark

Step 2- Stopping Capture:

Capturing can be stopped by clicking on “Stop Capturing Packets” button on the main toolbar.

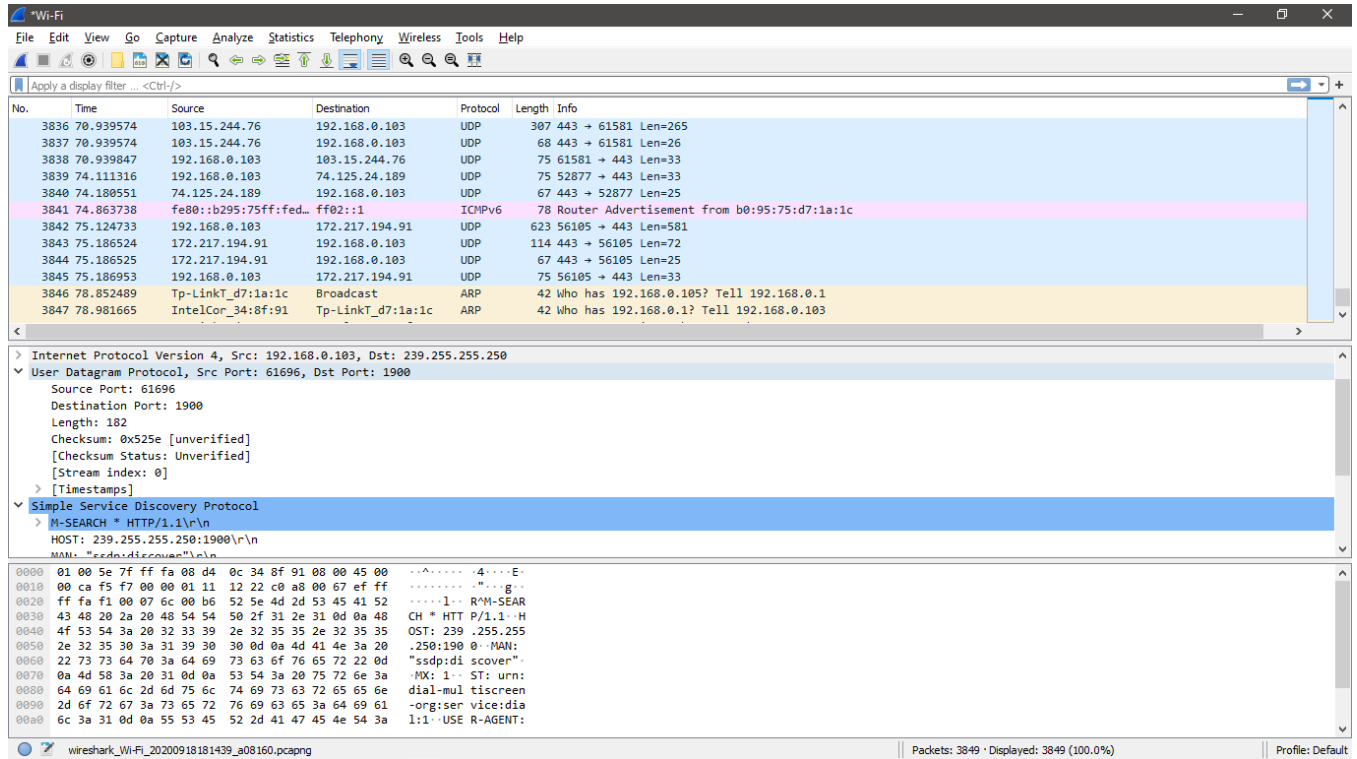


Figure-2: Stopping Capture

Step 3- Filtering:

We can filter the captures by entering the protocol name in “Apply a Display Filter” and enter.

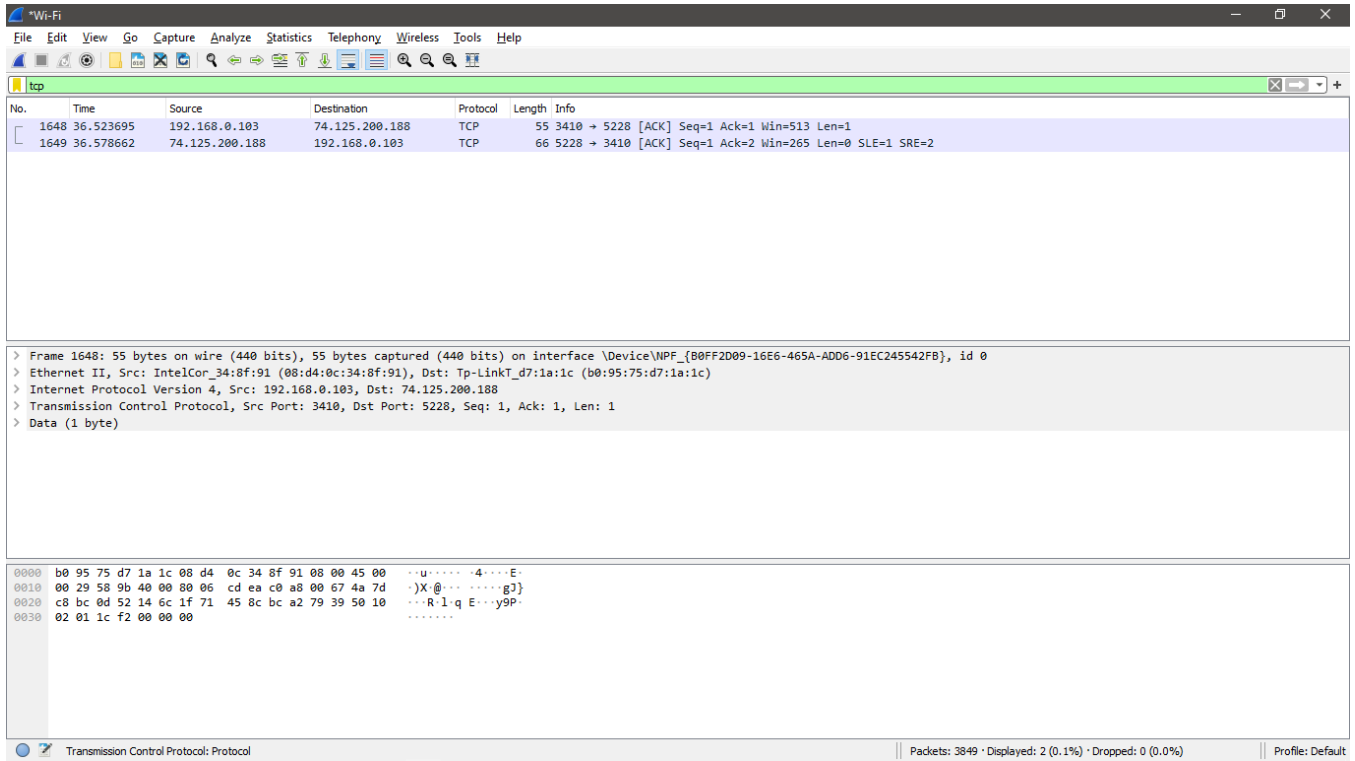


Figure-3: Filtering by TCP protocols

Step 4- Analyzing Protocols:

The analysis has to be performed manually. The given example below shows TCP segment with SYN and ACK fields set to 1.

The image shows a Wireshark packet capture window titled "Wi-Fi". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. The "Current filter: tcp" is applied. The packet list shows two packets:

No.	Time	Source	Destination	Protocol	Length	Info
1648	36.523695	192.168.0.103	74.125.200.188	TCP	55	3410 → 5228 [ACK] Seq=1 Ack=1 Win=513 Len=1
1649	36.578662	74.125.200.188	192.168.0.103	TCP	66	5228 → 3410 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2

The packet details pane for packet 1648 shows the following structure:

- > Frame 1648: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{B0FF2D09-16E6-465A-ADD6-91EC245542F8}, id 0
- > Ethernet II, Src: IntelCor_34:8f:91 (08:d4:0c:34:8f:91), Dst: Tp-LinkT_d7:1a:1c (b0:95:75:d7:1a:1c)
- > Internet Protocol Version 4, Src: 192.168.0.103, Dst: 74.125.200.188
- > Transmission Control Protocol, Src Port: 3410, Dst Port: 5228, Seq: 1, Ack: 1, Len: 1
 - Source Port: 3410
 - Destination Port: 5228
 - [Stream index: 0]
 - [TCP Segment Len: 1]
 - Sequence number: 1 (relative sequence number)
 - Sequence number (raw): 527517068
 - [Next sequence number: 2 (relative sequence number)]
 - Acknowledgment number: 1 (relative ack number)
 - Acknowledgment number (raw): 3164764473
 - 0101 = Header Length: 20 bytes (5)
 - > Flags: 0x010 (ACK)
 - Window size value: 513
 - [Calculated window size: 513]
 - [Window size scaling factor: -1 (unknown)]
 - Checksum: 0x1cf2 [unverified]
 - [Checksum Status: Unverified]
 - Urgent pointer: 0

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 b0 95 75 d7 1a 1c 08 d4 0c 34 8f 91 08 00 45 00  ..u.....4....E-
0010 00 29 58 9b 40 00 00 06 cd ea c0 a8 00 67 4a 7d  ..)X@.....gJ}
0020 c8 bc 0d 52 14 6c 1f 71 45 8c bc a2 79 39 50 10  ...R.l.q E...yP-
0030 02 01 1c f2 00 00 00  .....
```

The status bar at the bottom indicates: wireshark_Wi-Fi_20200918181439_a08160.pcapng | Packets: 3849 · Displayed: 2 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

Figure-4: Analyzing TCP protocols

Step 5- Plotting a flow graph:

The Plotting can be done through the “Statistics” menu. First we select the “Statistics” menu and then go to “Flow Graph”. Then for a plotting the flow of a particular protocol, we can select an option from “Flow Type”. Here the given example below shows the “TCP Flows” has been selected as the “Flow Type”.

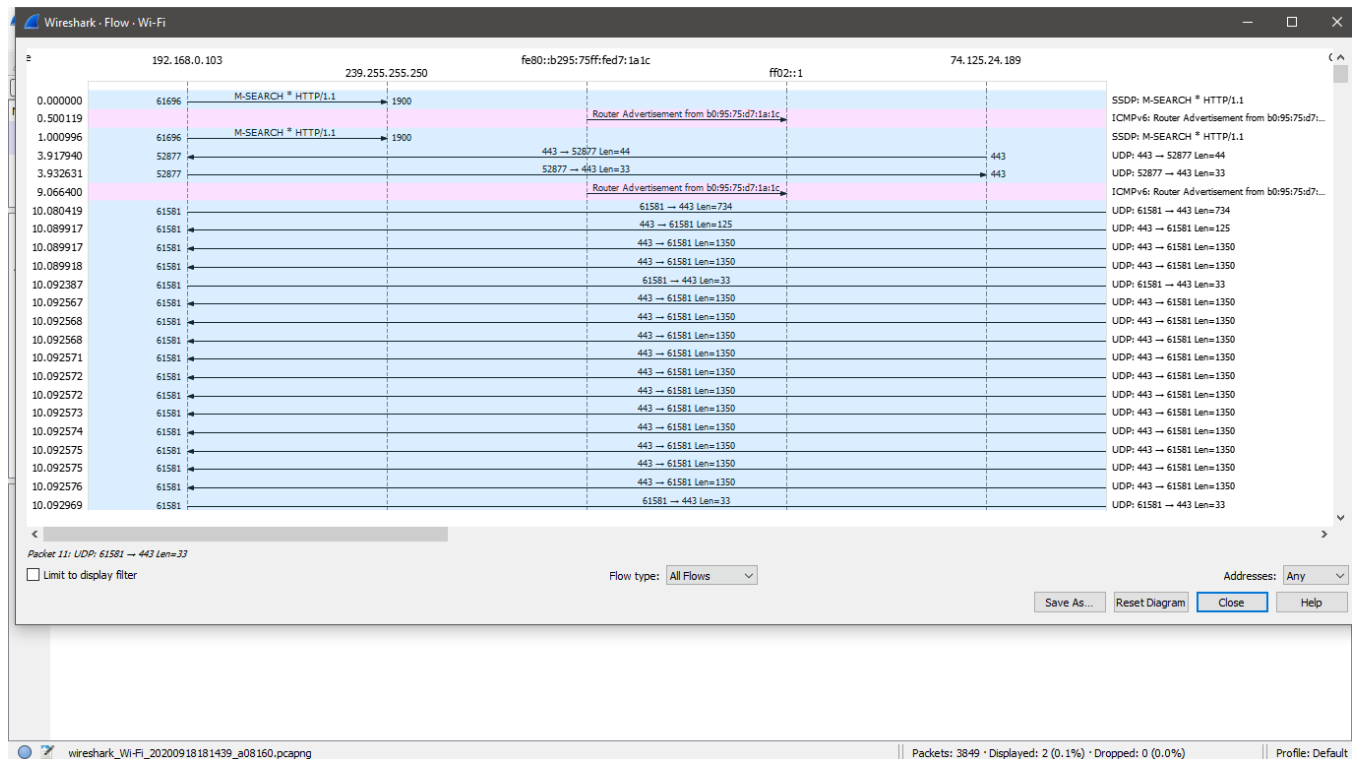


Figure-5.1: Plotting a graph for all flows

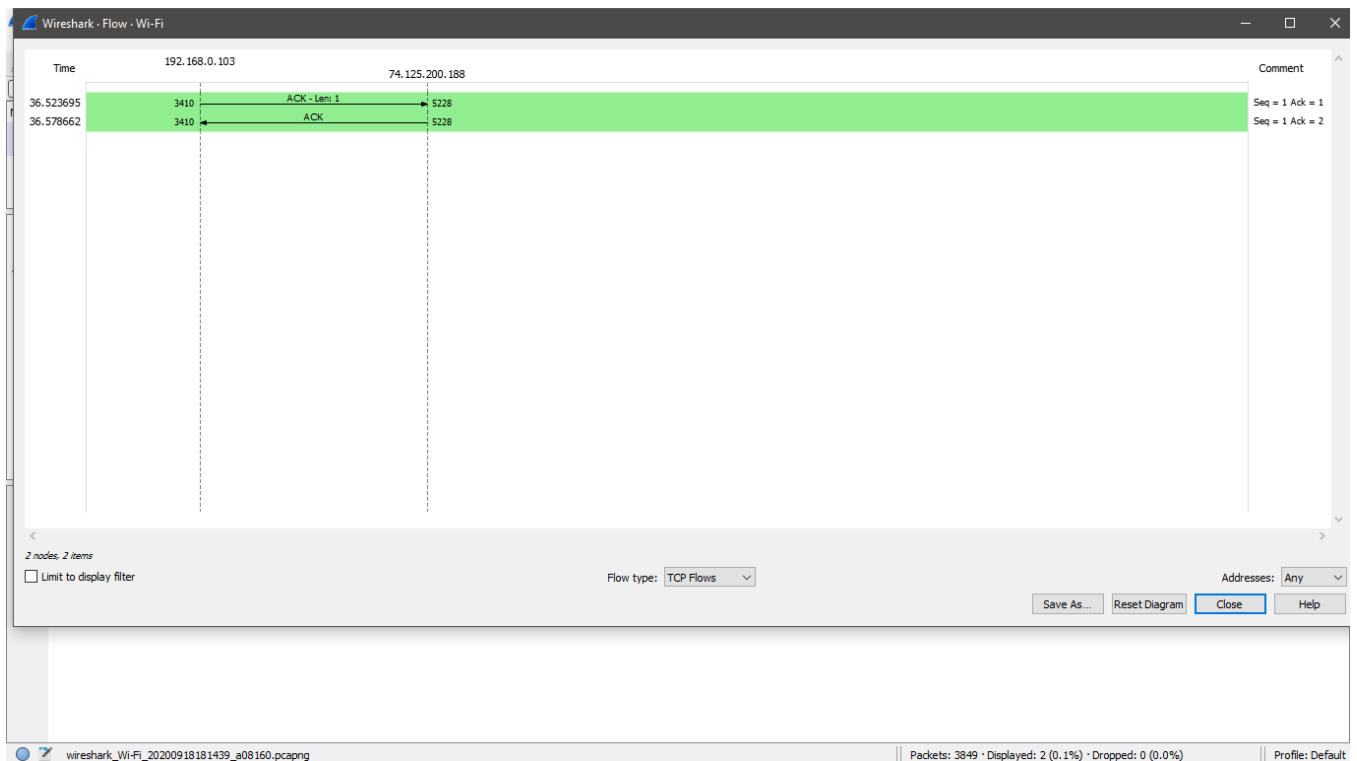


Figure-5.2: Plotting a graph for TCP flows

Conclusion:

From this lab, we've learnt how to analyze a protocol after capturing them by using Wireshark. The analysis helps us to understand how packets and protocols are transferred. The Wireshark helps us to visualize the flow of the protocols which helps us to understand the protocol flow more accurately.