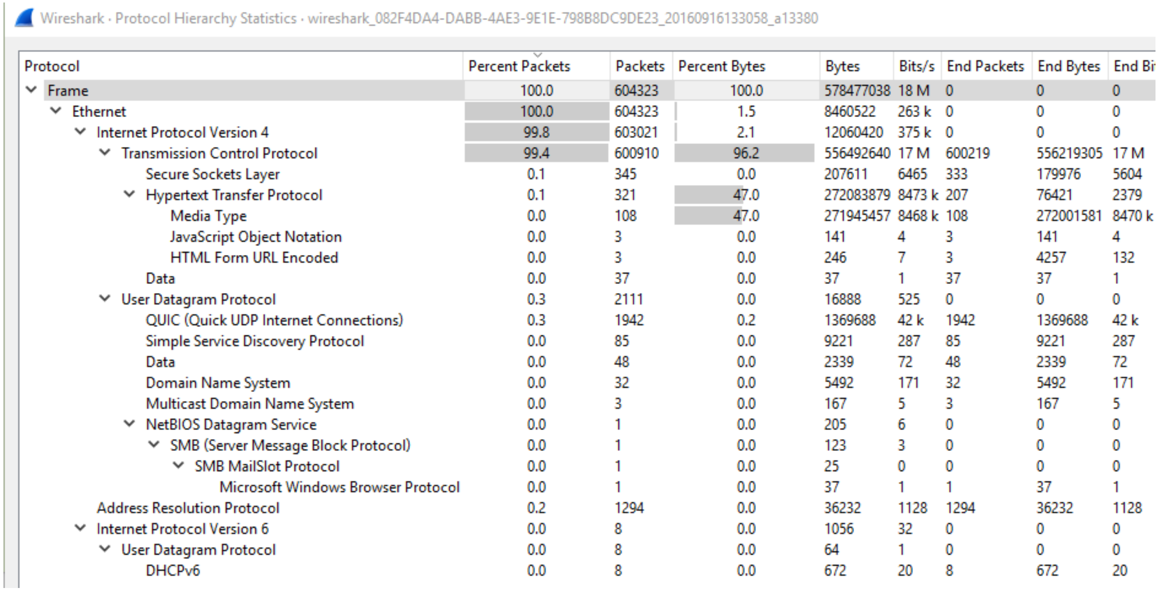
COMP 307 Mini A1
Name: Simon Hsu
ID: 260610820

a) Trottier Engineering Building:

b) Brutopia

1. Identify the exact location where you were when recording your two wifi packet recording sessions.
   a. 3630 University St, Montreal, QC H3A 2B2
   b. 1219 Rue Crescent, Montréal, QC H3G 2B1

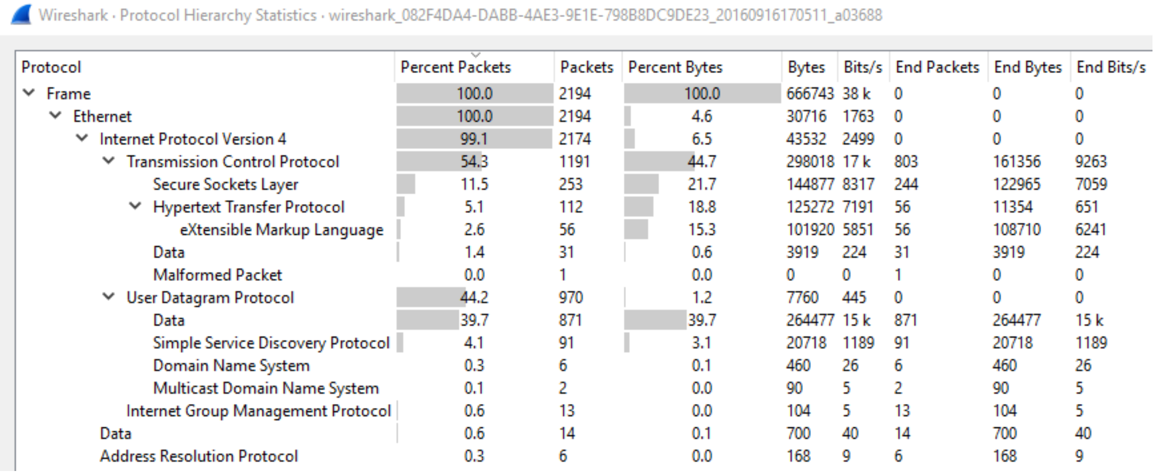
2. Look at each session individually and report the quality of the security. Specifically, based on your data set, what percentage of packets revealed packet header information, and what percentage of packets revealed payload information. Write a short evaluation.
   a. Based on my data set, some packets revealed packet header information and majority of packets don't revealed payload information.



Wireshark · Protocol Hierarchy Statistics · wireshark_082F4DA4-DABB-4AE3-9E1E-798B8DC9DE23_20160916133058_a13380

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bi
Frame	100.0	604323	100.0	578477038	18 M	0	0	0
Ethernet	100.0	604323	1.5	8460522	263 k	0	0	0
Internet Protocol Version 4	99.8	603021	2.1	12060420	375 k	0	0	0
Transmission Control Protocol	99.4	600910	96.2	556492640	17 M	600219	556219305	17 M
Secure Sockets Layer	0.1	345	0.0	207611	6465	333	179976	5604
Hypertext Transfer Protocol	0.1	321	47.0	272083879	8473 k	207	76421	2379
Media Type	0.0	108	47.0	271945457	8468 k	108	272001581	8470 k
JavaScript Object Notation	0.0	3	0.0	141	4	3	141	4
HTML Form URL Encoded	0.0	3	0.0	246	7	3	4257	132
Data	0.0	37	0.0	37	1	37	37	1
User Datagram Protocol	0.3	2111	0.0	16888	525	0	0	0
QUIC (Quick UDP Internet Connections)	0.3	1942	0.2	1369688	42 k	1942	1369688	42 k
Simple Service Discovery Protocol	0.0	85	0.0	9221	287	85	9221	287
Data	0.0	48	0.0	2339	72	48	2339	72
Domain Name System	0.0	32	0.0	5492	171	32	5492	171
Multicast Domain Name System	0.0	3	0.0	167	5	3	167	5
NetBIOS Datagram Service	0.0	1	0.0	205	6	0	0	0
SMB (Server Message Block Protocol)	0.0	1	0.0	123	3	0	0	0
SMB MailSlot Protocol	0.0	1	0.0	25	0	0	0	0
Microsoft Windows Browser Protocol	0.0	1	0.0	37	1	1	37	1
Address Resolution Protocol	0.2	1294	0.0	36232	1128	1294	36232	1128
Internet Protocol Version 6	0.0	8	0.0	1056	32	0	0	0
User Datagram Protocol	0.0	8	0.0	64	1	0	0	0
DHCPv6	0.0	8	0.0	672	20	8	672	20

   b. Based on my data set, majority of packets revealed packet header information and some revealed payload information, this could be the result of using cellphone on insecured websites (no HTTPS encryption).



Wireshark · Protocol Hierarchy Statistics · wireshark_082F4DA4-DABB-4AE3-9E1E-798B8DC9DE23_20160916170511_a03688

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	2194	100.0	666743	38 k	0	0	0
Ethernet	100.0	2194	4.6	30716	1763	0	0	0
Internet Protocol Version 4	99.1	2174	6.5	43532	2499	0	0	0
Transmission Control Protocol	54.3	1191	44.7	298018	17 k	803	161356	9263
Secure Sockets Layer	11.5	253	21.7	144877	8317	244	122965	7059
Hypertext Transfer Protocol	5.1	112	18.8	125272	7191	56	11354	651
eXtensible Markup Language	2.6	56	15.3	101920	5851	56	108710	6241
Data	1.4	31	0.6	3919	224	31	3919	224
Malformed Packet	0.0	1	0.0	0	0	1	0	0
User Datagram Protocol	44.2	970	1.2	7760	445	0	0	0
Data	39.7	871	39.7	264477	15 k	871	264477	15 k
Simple Service Discovery Protocol	4.1	91	3.1	20718	1189	91	20718	1189
Domain Name System	0.3	6	0.1	460	26	6	460	26
Multicast Domain Name System	0.1	2	0.0	90	5	2	90	5
Internet Group Management Protocol	0.6	13	0.0	104	5	13	104	5
Data	0.6	14	0.1	700	40	14	700	40
Address Resolution Protocol	0.3	6	0.0	168	9	6	168	9

COMP 307 Mini A1
Name: Simon Hsu
ID: 260610820

3. Looking at each session individually, select a sender IP address and try to deduce what they were trying to do.
   a. I used the filter to select a sender IP address, the address which i picked have a lot of unreadable data, it can be interepreted as the sender is visiting secure website that has already been encoded.
   b. I sued the same method as i did in Trottier building to select a sender IP address and i was able to deduce the sender was on sort of communication with another IP address via visiting some website.

4. Now, comparing your two data sets. Which location was more secure? Could you identify the default security that was present at each data set?
   Based on the two data sets, trottier building is more secure due to the fact the McGill wifi is more secure and encrypted compare to Brutopia(hotspot). Some of the default security that is presented: wired network vs. wireless(one is easier to trace), encryption/authentication/permision of packets in order to secure the packets and to prevent 3rd person from reading the packets; security budget and knowledge of cyberattacking: McGill campus might understand more than Brutopia and want to provide the students a more secure environment for the users to enjoy surfing the net.