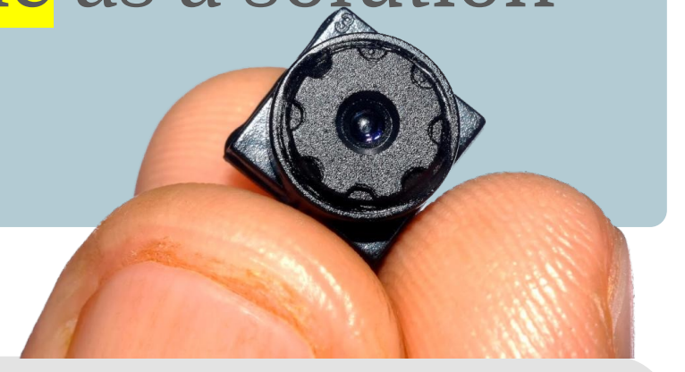
Detecting Hidden Camera through Wireshark

Yeon Kyung Ha
CSE 310 Course Project

Introduction

South Korea is facing a rise in hidden camera crimes, with victims increasing annually due to difficulty of detecting these small cameras. This project investigates the potential of using Wireshark to detect IP cameras by distinguish ARP packets and analyzing traffic volume as a solution to the problem.



Motivation

1 In South Korea, around 5,433 incidents of hidden camera crimes reported annually since 2020.

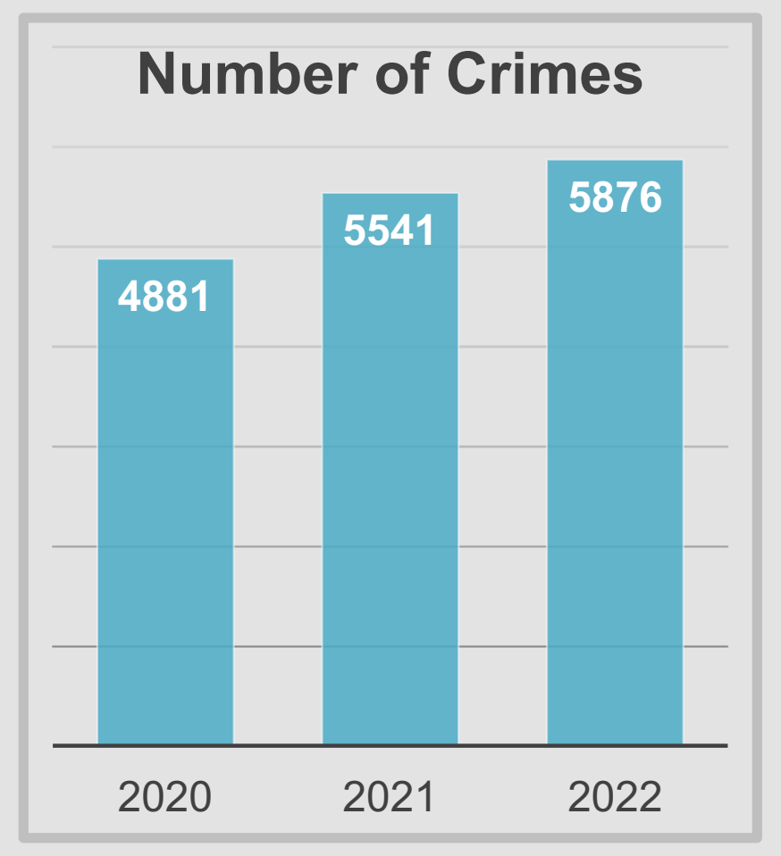


Figure 1. A growing trend of hidden camera crimes

2 According to the Seoul City government, 68.7% of 1,500 men and women expressed anxiety of hidden camera crimes.

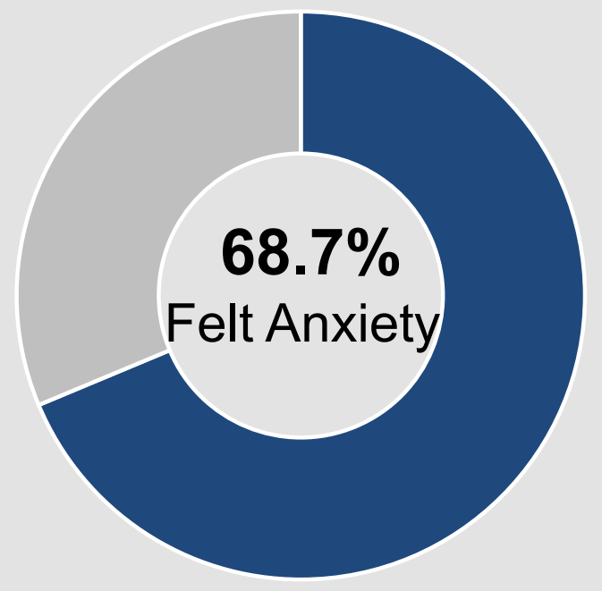


Figure 2. Almost two-thirds of citizens felt anxiety

3 In places suspected of illegal filming, individuals tended to search holes or cameras.

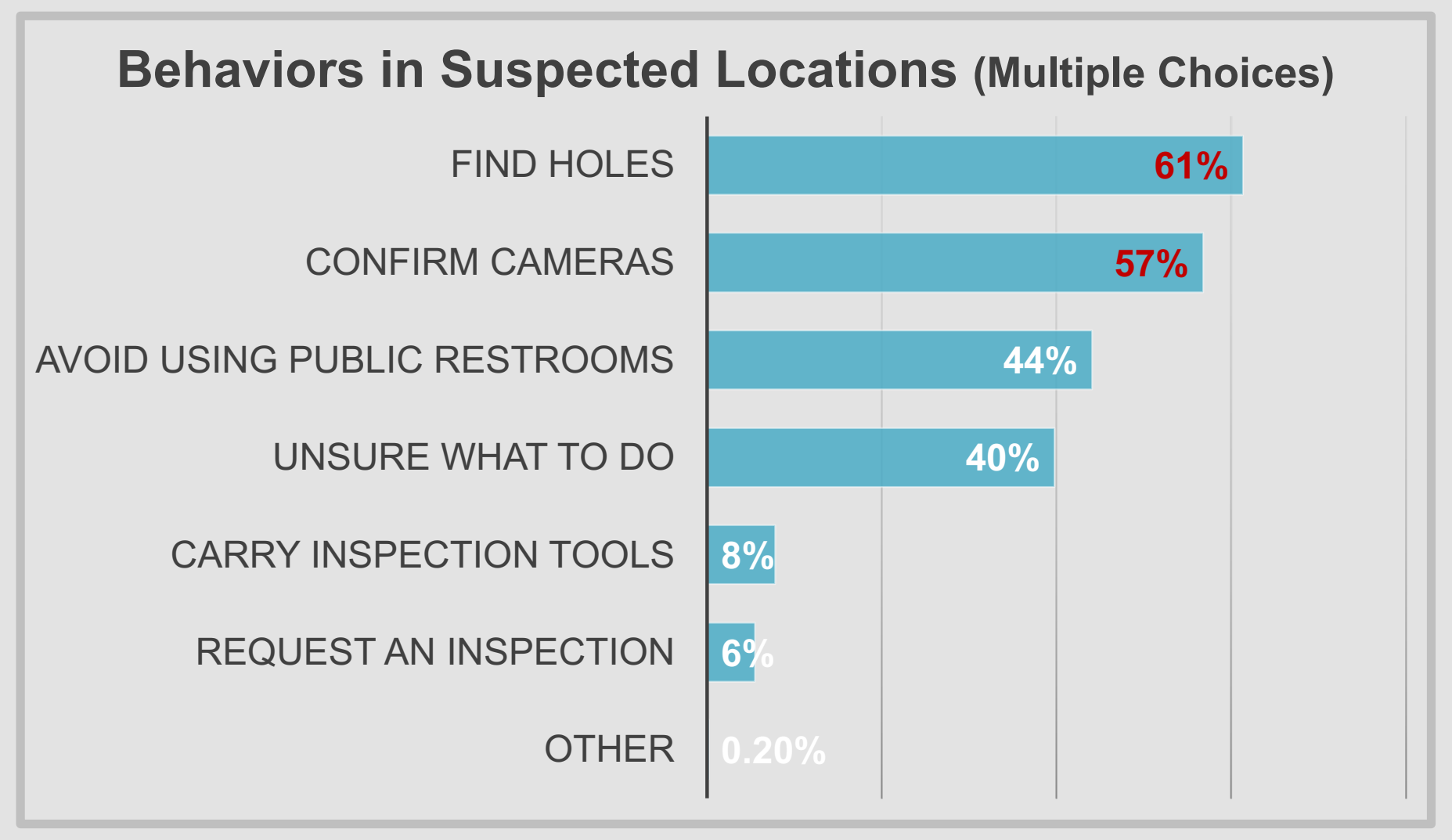


Figure 3. Most people tried to search the camera

However, hidden cameras are difficult to detect only with eyes. Thus, more efficient detecting methods are needed.

Background

Nodes in a Local Area Network (LAN) communicate using MAC addresses rather than IP addresses. Therefore, to send data from one node to a specific node within the same LAN, it is necessary to determine the MAC address of the destination node first. To obtain the MAC address, an ARP request packet containing the destination's IP address must be broadcasted. Upon receiving the ARP request packet, the destination node responds by sending its MAC address to the source, establishing the connection with the source.

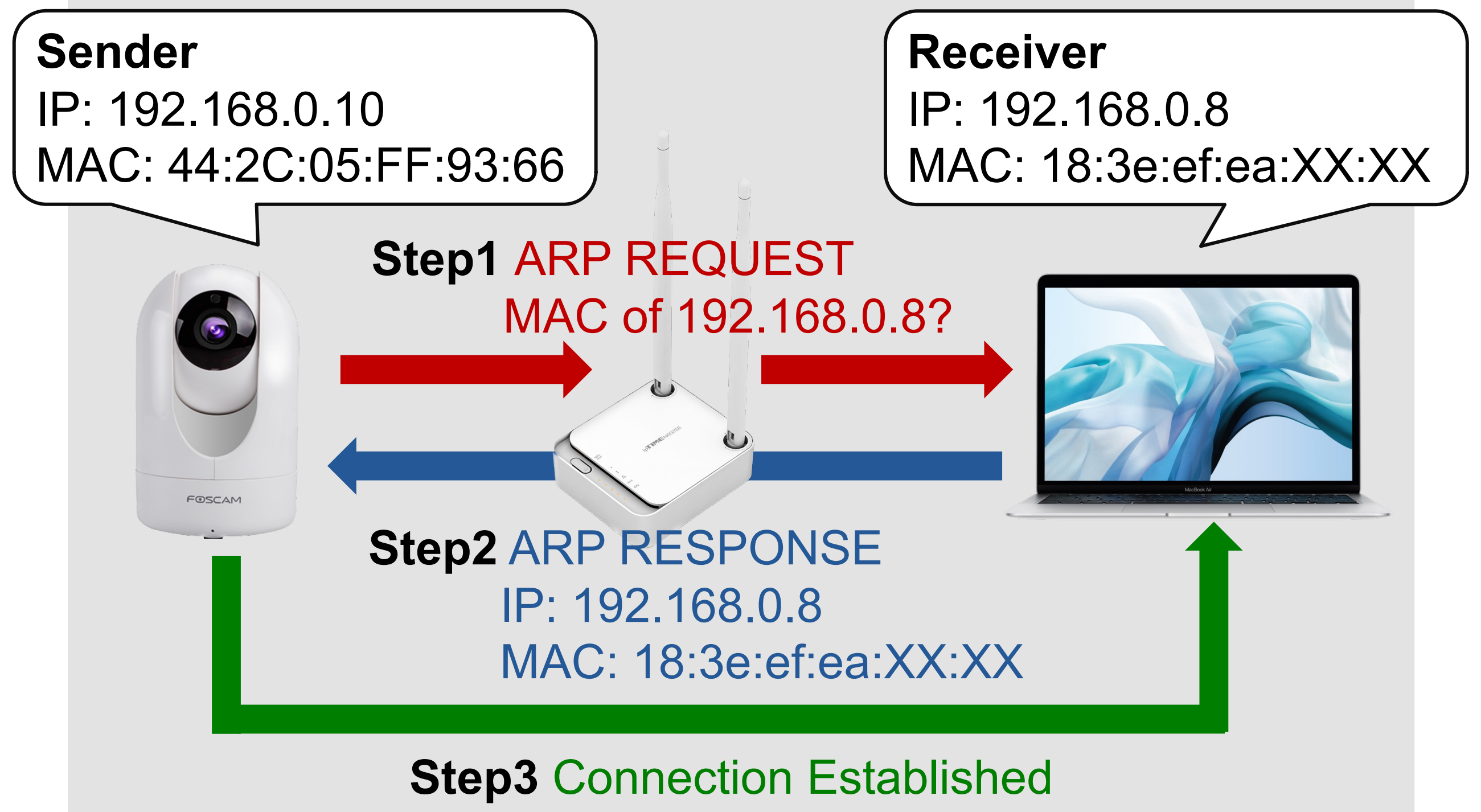
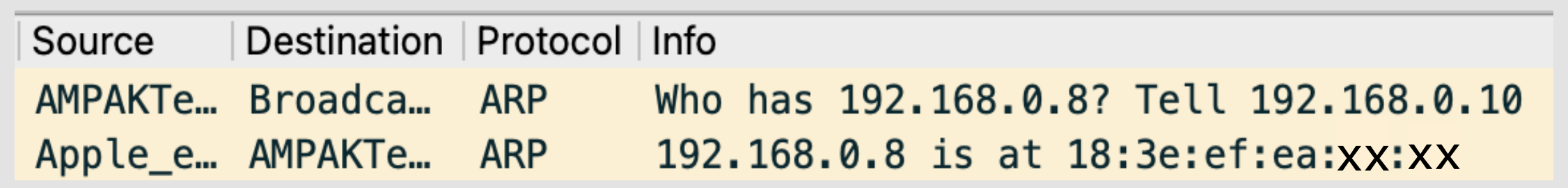


Figure 4. The process for data transmission within the LAN



```
Source     Destination  Protocol  Info
AMPAKTe…   Broadca…     ARP       Who has 192.168.0.8? Tell 192.168.0.10
Apple_e…   AMPAKTe…     ARP       192.168.0.8 is at 18:3e:ef:ea:xx:xx
```

Figure 5. ARP request & ARP response packets in Wireshark

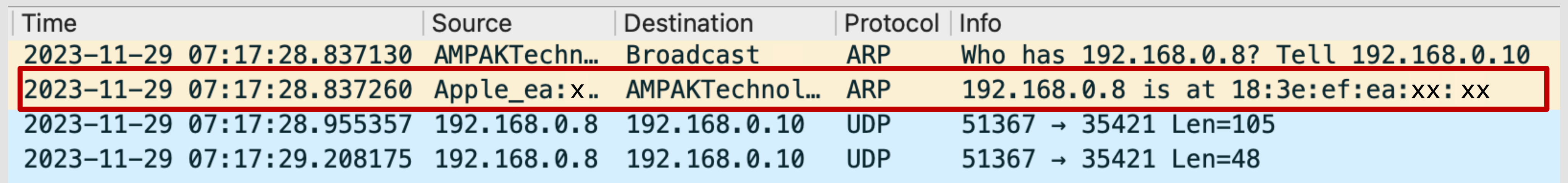
Materials

Methodology

1. Refer to the device manual to check the MAC address of the IP camera.
2. Connect the laptop to Wi-Fi and stream video from the IP camera using Foscam VMS.
3. Launch Wireshark and capture LAN packets for one minute.
4. Apply the filter "arp.opcode==2" in the filter window to isolate ARP response packets.
5. Retrieve packets where the destination is not the router, noting source and destination.
6. Access the "Statistics" menu and navigate to the "Conversations" window.
7. Examine the conversations between source and destination for the remaining ARP response packets.
8. Identify conversations with a high packet exchange rate.
9. Verify if the destination MAC address of ARP response packet associated with the conversation having the highest packet exchange, corresponds to the MAC address of the IP camera.

Results

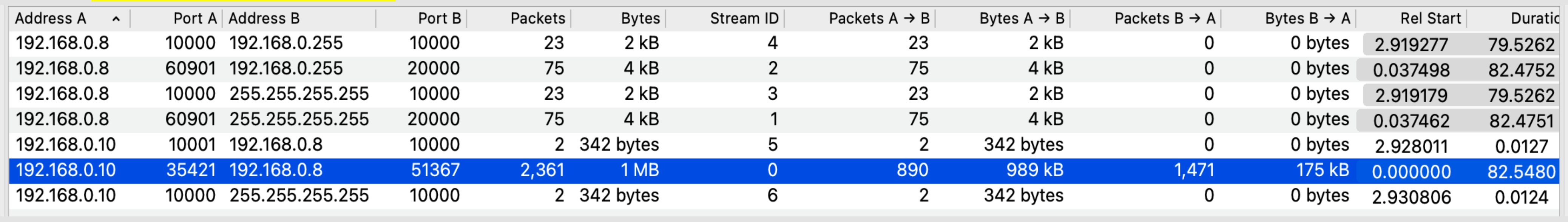
1 An ARP response packet sending from 192.168.0.8 to 192.168.10 was found.



```
Time                        Source          Destination     Protocol  Info
2023-11-29 07:17:28.837130  AMPAKTechn…     Broadcast       ARP       Who has 192.168.0.8? Tell 192.168.0.10
2023-11-29 07:17:28.837260  Apple_ea:x..    AMPAKTechnol…   ARP       192.168.0.8 is at 18:3e:ef:ea:xx: xx
2023-11-29 07:17:28.955357  192.168.0.8     192.168.0.10    UDP       51367 → 35421 Len=105
2023-11-29 07:17:29.208175  192.168.0.8     192.168.0.10    UDP       51367 → 35421 Len=48
```

Figure 6. Captured Packets

2 About 85% of the packets came from the conversation between 192.168.0.10 and 192.168.0.8.



Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duratic
192.168.0.8	10000	192.168.0.255	10000	23	2 kB	4	23	2 kB	0	0 bytes	2.919277	79.5262
192.168.0.8	60901	192.168.0.255	20000	75	4 kB	2	75	4 kB	0	0 bytes	0.037498	82.4752
192.168.0.8	10000	255.255.255.255	10000	23	2 kB	3	23	2 kB	0	0 bytes	2.919179	79.5262
192.168.0.8	60901	255.255.255.255	20000	75	4 kB	1	75	4 kB	0	0 bytes	0.037462	82.4751
192.168.0.10	10001	192.168.0.8	10000	2	342 bytes	5	2	342 bytes	0	0 bytes	2.928011	0.0127
192.168.0.10	35421	192.168.0.8	51367	2,361	1 MB	0	890	989 kB	1,471	175 kB	0.000000	82.5480
192.168.0.10	10000	255.255.255.255	10000	2	342 bytes	6	2	342 bytes	0	0 bytes	2.930806	0.0124

Figure 7. Conversation statistics

3 MAC address of 192.168.0.10 matched with the MAC address of the IP camera.

Conclusion

The challenge of this project was to identify IP cameras using Wireshark. Throughout the experiment, both the sender and receiver within the LAN were discovered through ARP response packets. Moreover, the sender was confirmed as the medium transmitting video contents by analyzing the excessive packet volume. As a result, these processes proved the presence of an IP camera. Thus, the project demonstrates that hidden cameras can be detected through packet analysis using Wireshark.

Future Work

1 Since this experiment was conducted with an isolated network with only a laptop, an IP camera, and a Wi-Fi router, future work could involve investigating whether the proposed method effectively works within public network.

2 Furthermore, future projects should discuss how to use Wireshark when an IP camera and a receiver are not in the same LAN, such as operating through cloud services.

References

[1] "불법촬영에 대한 시민의식조사." 2019
[2] Statista Research Department, "Number of spycam related crimes in South Korea from 2011 to 2022," Statista, https://www.statista.com/statistics/1133121/south-korea-number-of-spycam-crimes/ (accessed Dec. 6, 2023).

Acknowledgment

Special thanks to Professor Aruna Balasubramanian for her guidance and encouragement in exploring ARP packets. Also, sincerely appreciate Professor Ji-hoon Ryoo for providing equipment and valuable advice. Lastly, thanks to colleagues Hyo-jong Jung and Seong-woong Park for their insights on the approach at the project's inception.