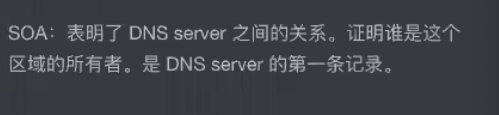
**Exercise 1: Explore DNS records (Not marked, No need to submit)**

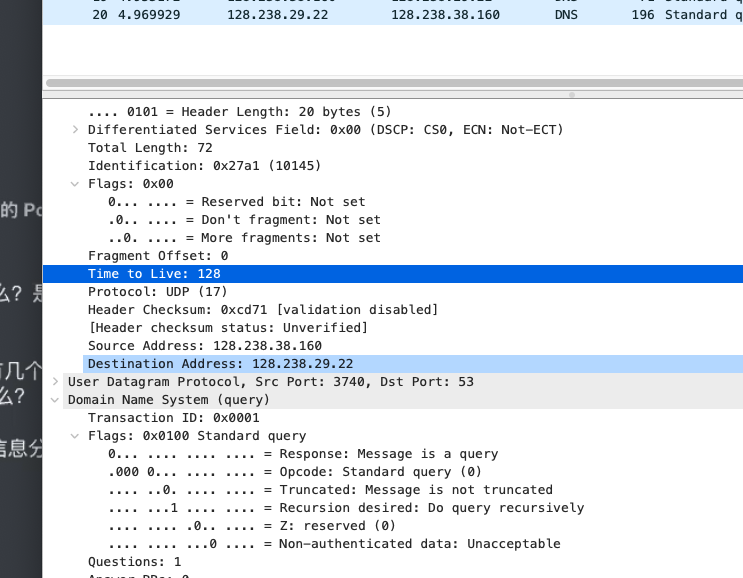




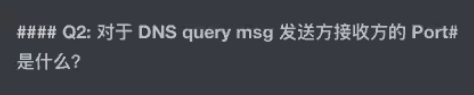
### Exercise 2: Tracing DNS with Wireshark (Not marked, No need to submit)

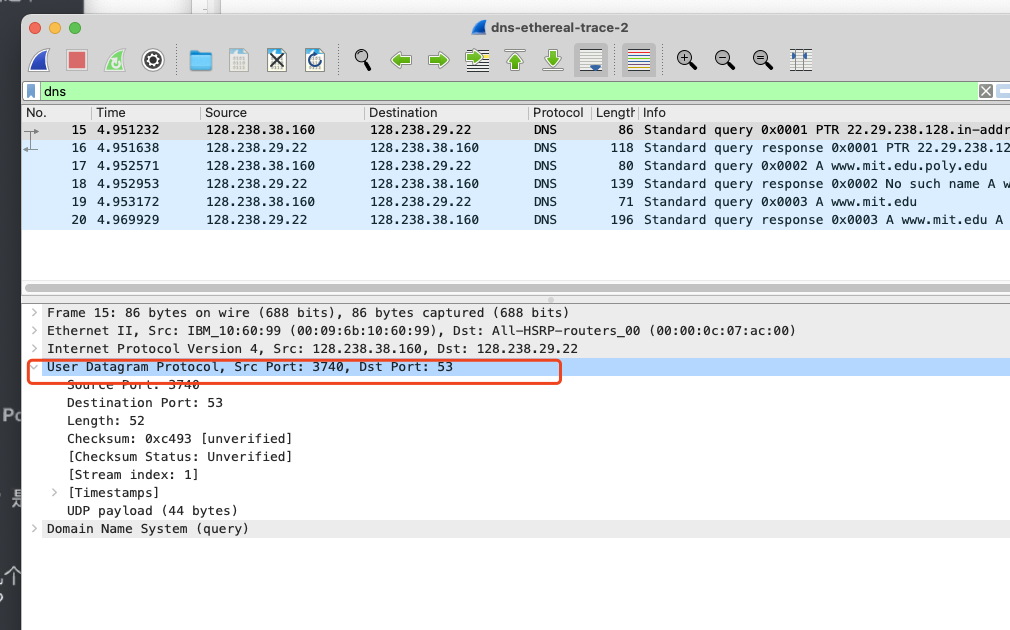
Question 1: What transport layer protocol is being used by the DNS messages?



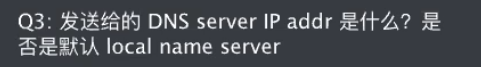


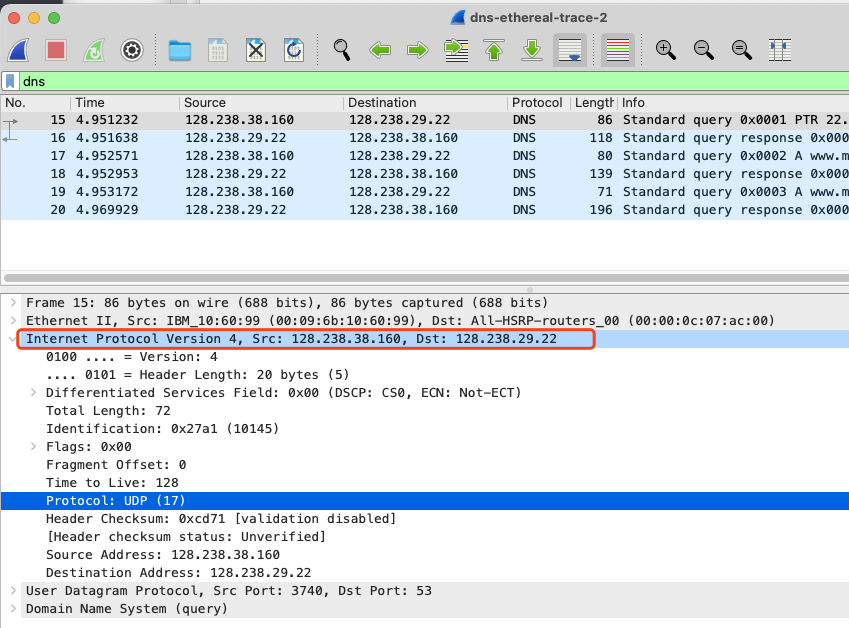
Question 2: What are the source and destination port for the DNS query message and the corresponding response?



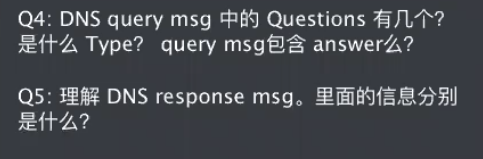


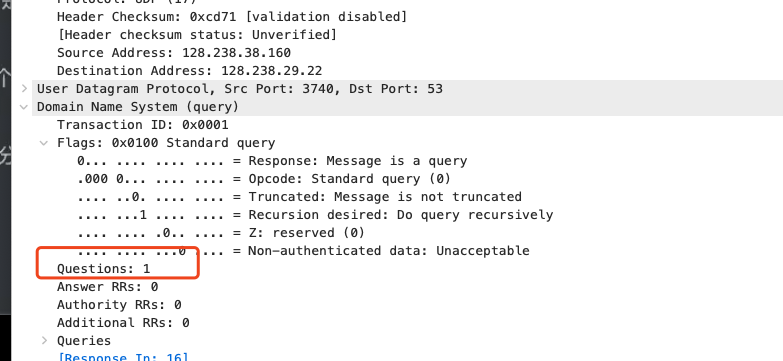
Question 3: To what IP address is the DNS query message sent? Is this the same as the default local DNS server?

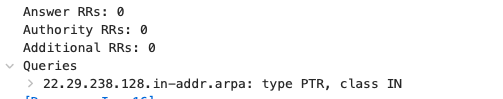




Question 4: How many “questions” are contained in the DNS query message? What “Type” of DNS queries are they? Does the query message also contain any “answers”?







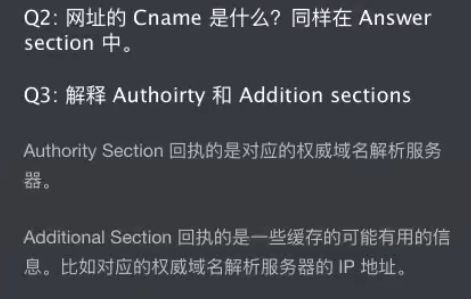
Question 5: Examine the DNS response message. Provide details of the contents of the “Answers”, “Authority” and “Additional Information” fields. What can you infer from these?

**Exercise 3: Digging into DNS (marked, include in the lab report)**

**Question 1**. What is the IP address of [www.eecs.berkeley.edu](https://eecs.berkeley.edu/). What type of DNS query is sent to get this answer?

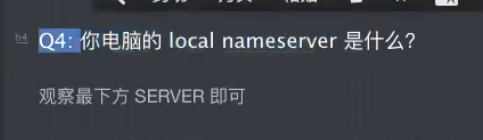


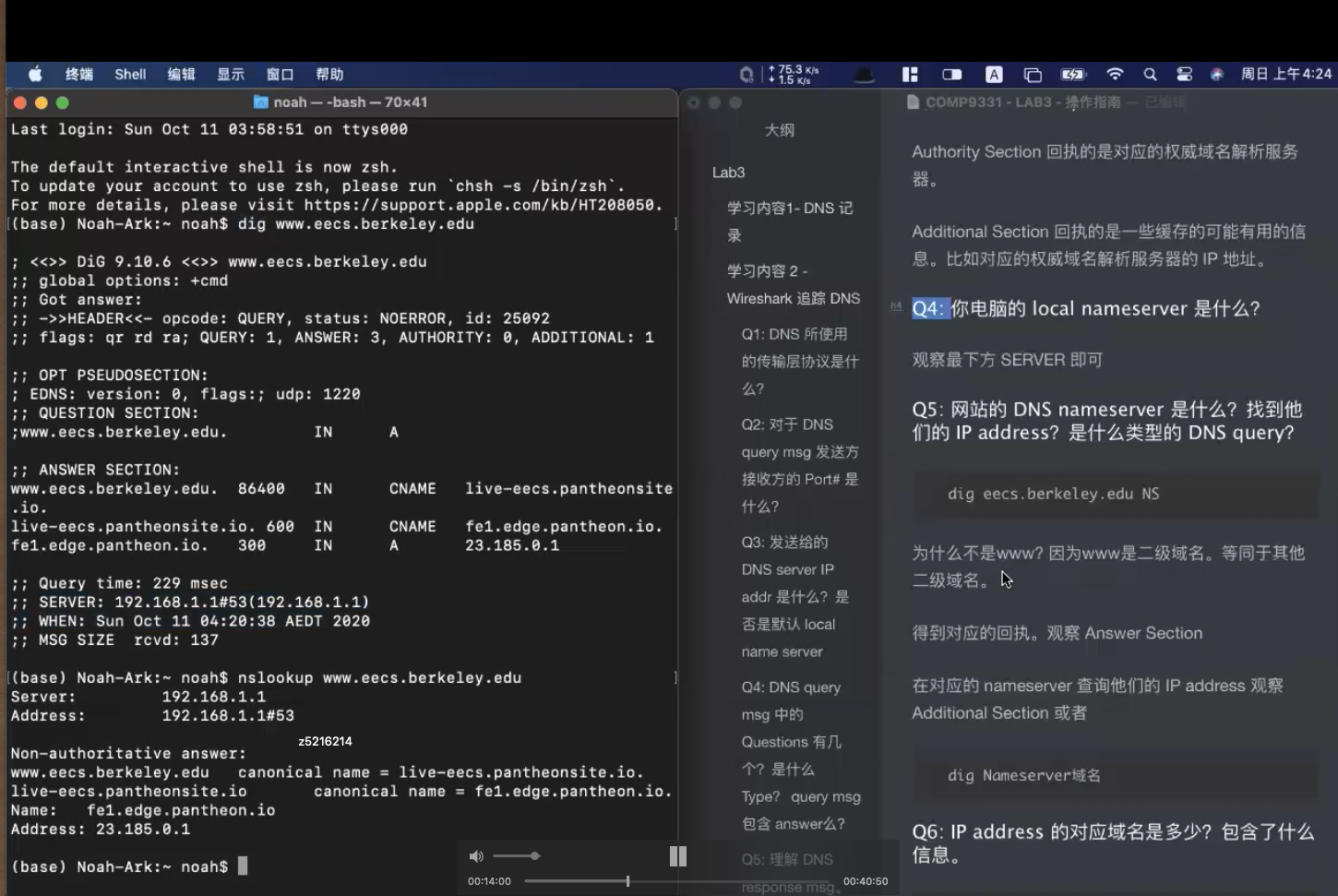
**Question 2.** What is the canonical name for the eecs.berkeley webserver (i.e. [www.eecs.berkeley.edu](http://www.eecs.berkeley.edu/))? Suggest a reason for having an alias for this server.



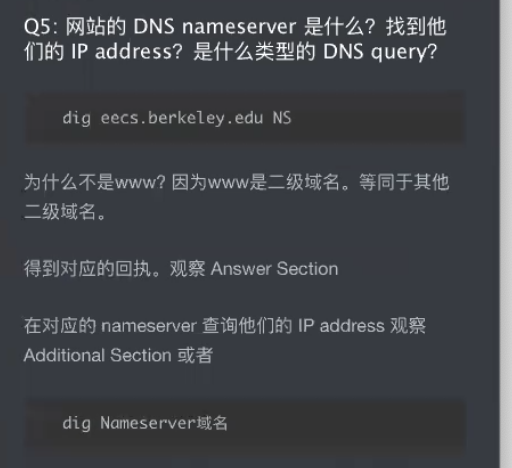
**Question 3**. What can you make of the rest of the response (i.e. the details available in the Authority and Additional sections)?

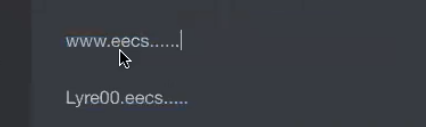
**Question 4**. What is the IP address of the local nameserver for your machine?



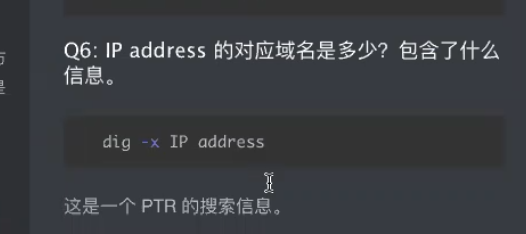


**Question 5.** What are the DNS nameservers for the “eecs.berkeley.edu.” domain (note: the domain name is eecs.berkeley.edu and not [www.eecs.berkeley.edu](https://eecs.berkeley.edu/). This is an example of what is referred to as the apex/naked domain)? Find out their IP addresses? What type of DNS query is sent to obtain this information?





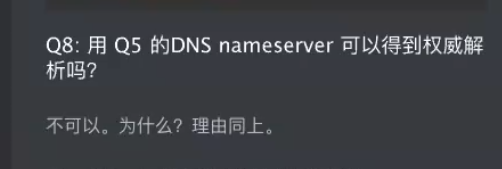
**Question** **6**. What is the DNS name associated with the IP address 111.68.101.54? What type of DNS query is sent to obtain this information?



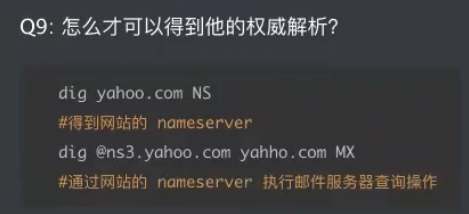
**Question** **7**. Run dig and query the CSE nameserver (129.94.242.33) for the mail servers for Yahoo! Mail (again the domain name is yahoo.com, not [www.yahoo.com](http://www.yahoo.com/)). Did you get an authoritative answer? Why? (HINT: Just because a response contains information in the authoritative part of the DNS response message does not mean it came from an authoritative name server. You should examine the flags in the response to determine the answer)



**Question** **8**. Repeat the above (i.e. Question 7) but use one of the nameservers obtained in Question 5. What is the result?



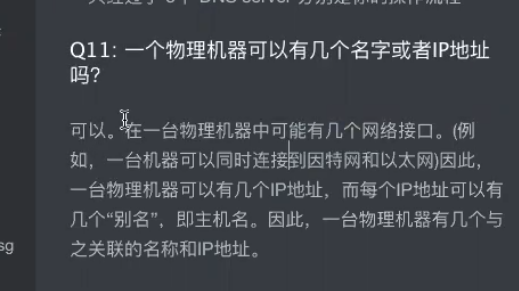
**Question** **9**. Obtain the authoritative answer for the mail servers for Yahoo! Mail. What type of DNS query is sent to obtain this information?



**Question** **10**. In this exercise, you simulate the iterative DNS query process to find the IP address of your machine (e.g. lyre00.cse.unsw.edu.au). If you are using VLAB Then find the IP address of one of the following: lyre00.cse.unsw.edu.au, lyre01.cse.unsw.edu.au, drum00.cse.unsw.edu.au or drum01.cse.unsw.edu.au. First, find the name server (query type NS) of the "." domain (root domain). Query this nameserver to find the authoritative name server for the "au." domain. Query this second server to find the authoritative nameserver for the "edu.au." domain. Now query this nameserver to find the authoritative nameserver for "unsw.edu.au". Next query the nameserver of unsw.edu.au to find the authoritative name server of cse.unsw.edu.au. Now query the nameserver of cse.unsw.edu.au to find the IP address of your host. How many DNS servers do you have to query to get the authoritative answer?

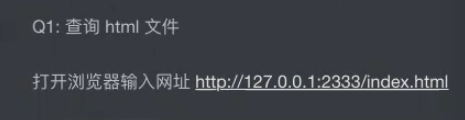


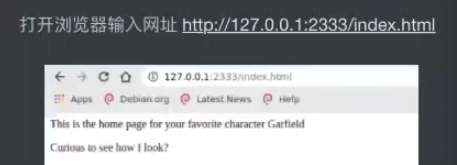
Question 11. Can one physical machine have several names and/or IP addresses associated with it?



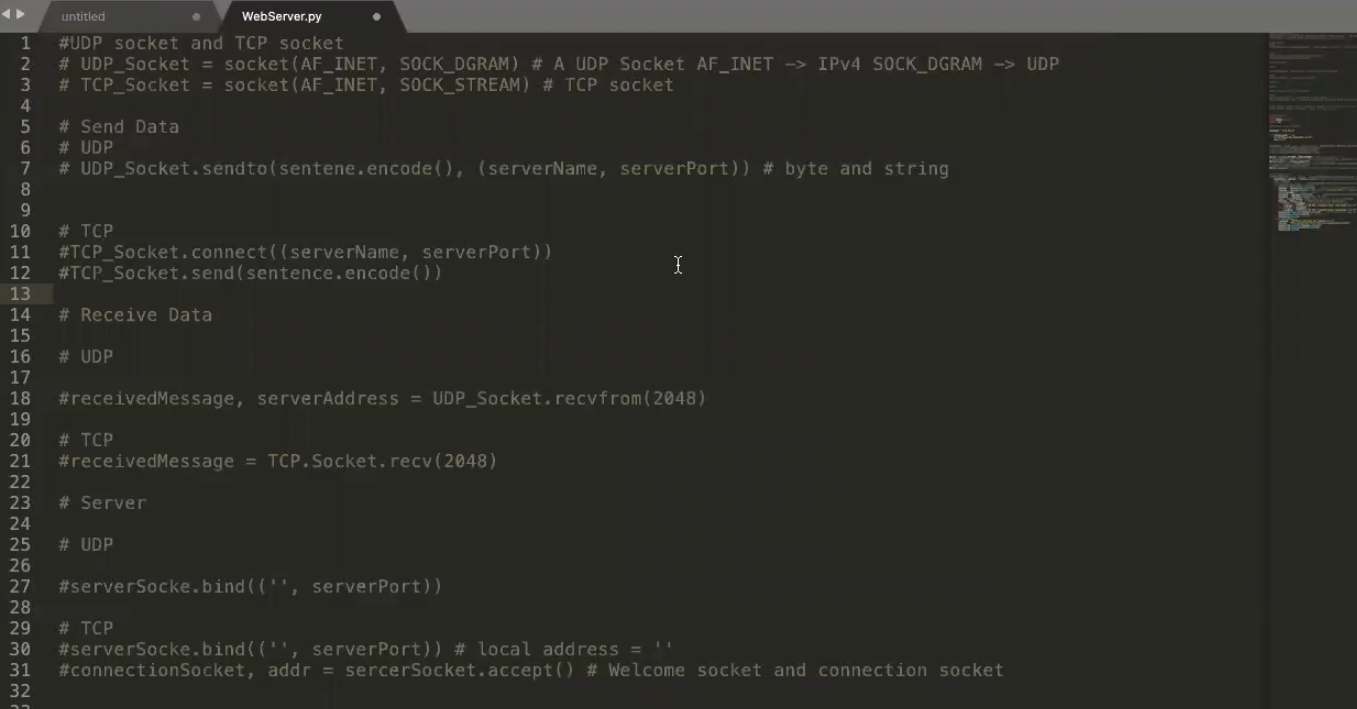
**Exercise 4: A Simple Web Server (Marked, submit your code )**

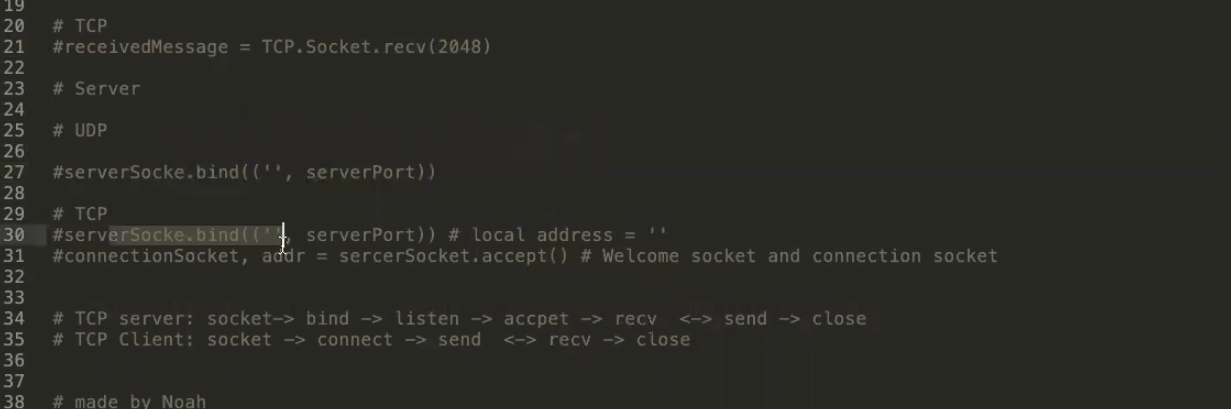




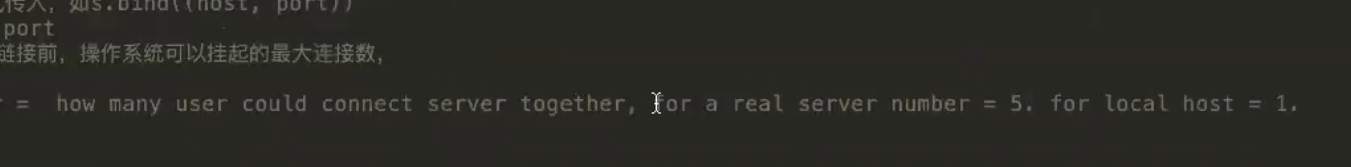




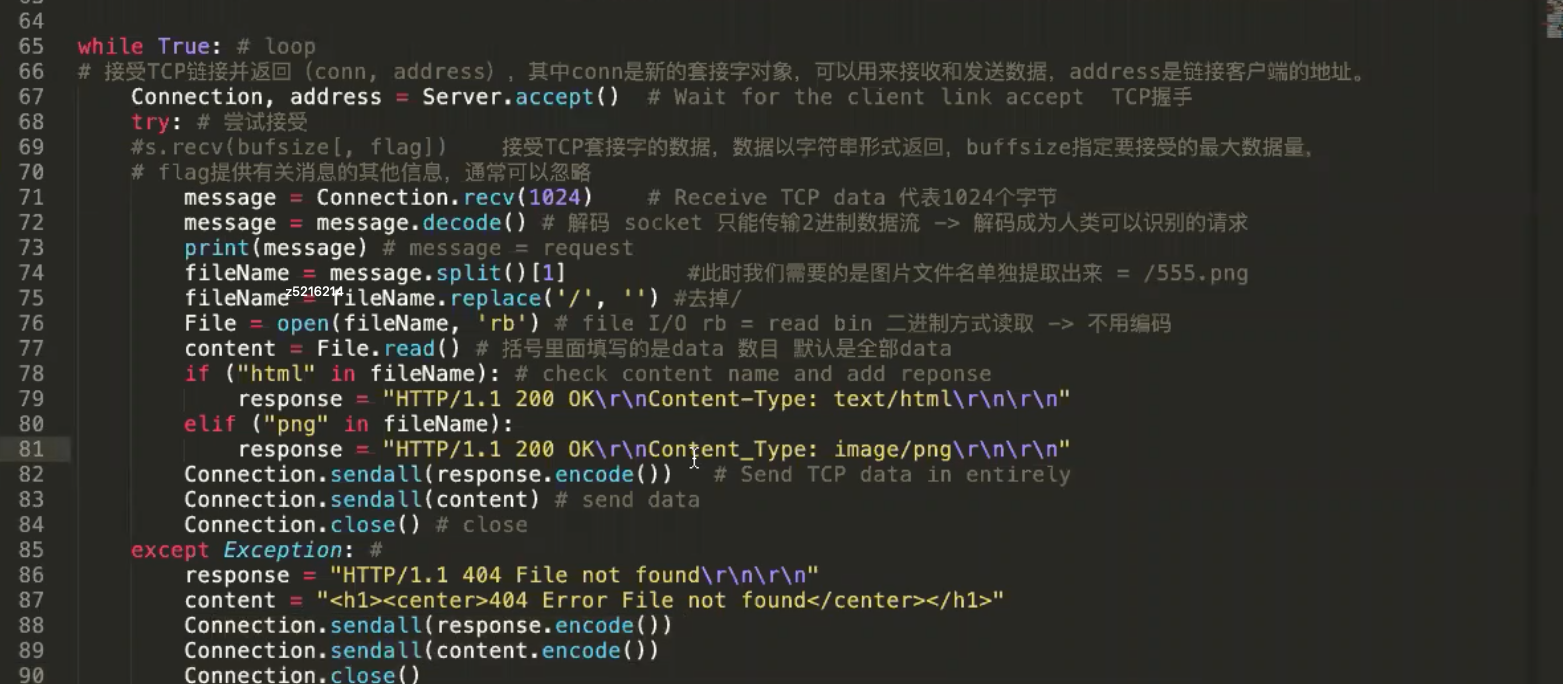










1