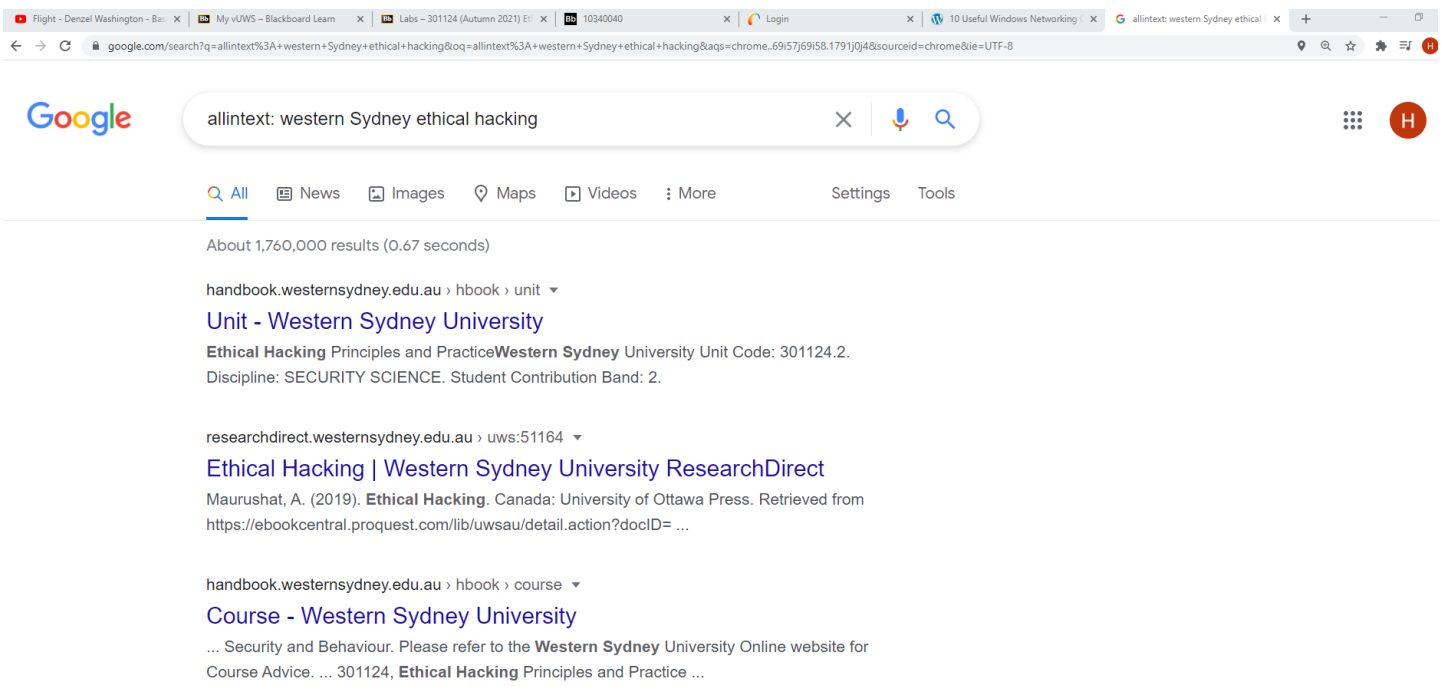
PART 1

1.1 Find webpages in which the title contains "zone" and the url contains "dns". Write the search string you use into your lab report.

"intitle:zone inurl:dns"

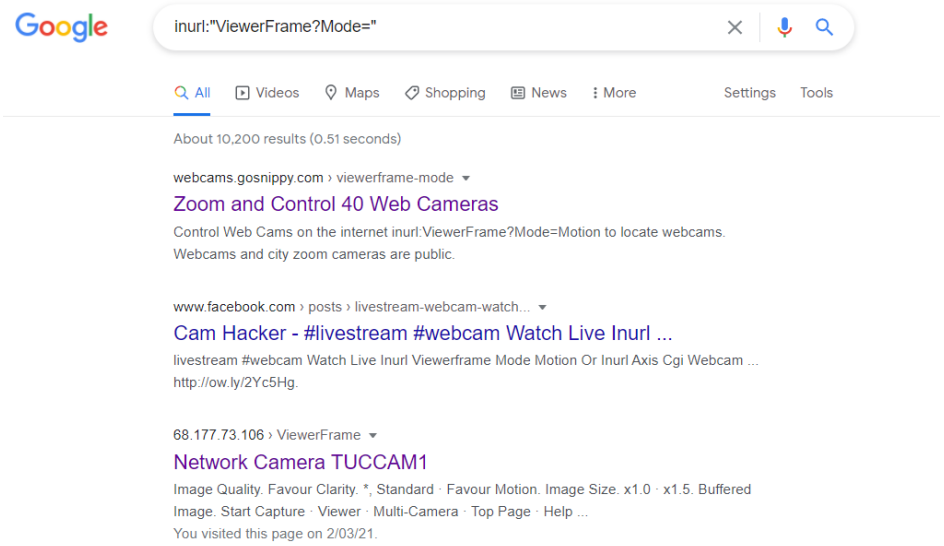
1.2 Visit the following website:
http://www.googleguide.com/advanced_operators_reference.html . Using it as a reference, explain what the operator "allintext:" does in your lab report. Then, enter **allintext: western Sydney ethical hacking** into Google and check whether the results reflect what "allintext:" should do. Take a screenshot of the Google search results and include this screenshot into your lab report. Since this screenshot is not related to VM use, you don't need to include VM ID in your screenshot. This rule will apply to future encounters of such scenarios.

If you start your query with allintext:, Google restricts results to those containing all the query terms you specify in the text of the page. For example, [allintext: travel packing list] will return only pages in which the words "travel," "packing," and "list" appear in the text of the page.



PART 2

2.1 The search string **inurl:"ViewerFrame?Mode="** allows you to find public webcams on the Internet. Please try it and grab a screenshot of your search results, and include the screenshot into your lab report.



2.2 Try the search string **filetype:xls username password -example** in Google. Explain in your lab report what this search string does, especially, what the operator "-" before "example" does by consulting the googleguide.com link mentioned above.

The query to find xls[spread sheet format] files that may contain passwords filetype:xls username password Precede each term you do not want to appear in any result with a "–" sign. The – sign indicates that you want to subtract or exclude pages that contain a specific term.

PART 3:

3.1 Execute the command 'whois smh.com.au'. Examine the output on 'Registrant', which means the company that registers this domain name. Write the company name into your lab report.

Registrant: Fairfax Metro Pty Limited

3.2 Execute the command 'whois transportnsw.info > whois.txt'. Explain what this command does in your lab report. (Hint: for the meaning of the operator '>', refer to lecture 1 slides.)

standard output of who is directed to the text-file whois.txt which will store the results of who-is operation.

3.3 Execute the command 'grep -i registrant whois.txt'. Explain what this command does in your lab report. Especially, what does the option '-i' means?

Grep looks for the parameter "registrant" in the output of the whois output text file whois.txt; the -i means to ignore case distinctions in patterns and input data, so that characters that differ only in case match each other. That is The -i option enables to search for a string case insensitively in the give file.

```
┌──(kali㉿kali)-[~]
└─$ grep -i registrant whois.txt
Registrant Organization: Transport NSW
Registrant State/Province: NSW
Registrant Country: AU
The Registrar of Record identified in this output may have an RDDS service that can be queried for additional i
nformation on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
```

3.4 Based on the output of the above command, which organisation registers the domain 'transportnsw.info'?

Registrant: Transport NSW

Part 4

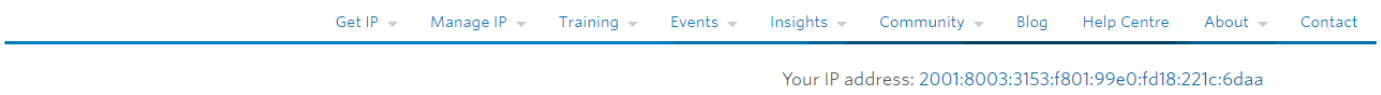
4.1 Visit the website 'www.apnic.net'. The first web page will show your IP address. Also, run an 'ipconfig' on your computer. Do you see the same IP address?

No. It is the temporary IPv6 address look below.

4.2 If not, please explain why you see this difference in your lab report.

It is the temporary one which does not include the MAC address.

```
Connection-specific DNS Suffix  . :
IPv6 Address. . . . . . . . . . . : 2001:8003:3153:f801:c46a:2c6:f167:4d57
Temporary IPv6 Address. . . . . . : 2001:8003:3153:f801:99e0:fd18:221c:6daa
```



4.3 Enter the IP address '13.8.8.8' into the top 'whois' search box in the www.apnic.net website. You'll notice that the authoritative answer comes from 'whois.arin.net'. Which "Regional Internet Registry" is this website responsible for?

APNIC (the Asia Pacific Network Information Centre) is the regional Internet address registry (RIR) for the Asia-Pacific region. 'whois.arin.net' is the American Register [American Registry for Internet Numbers]

4.4 Also answer the following questions regarding '13.8.8.8' in your lab report:

a) Which company does this IP address belong to?

Xerox Corporation

b) What's the range of IP addresses does this company own?

13.0.0.0 – 13.23.255.255

PART 5

5.1 Enter the interactive mode of nslookup. Write your default DNS server hostname into your lab report.

Default Server: kwd-scem.cdms.westernsydney.edu.au

5.2 Use the commands under nslookup to find out the email server IP addresses for the domain 'gmail.com'. Write your steps and results into your lab report. (hint: you need to query 'MX' record to get email server hostnames first, and then query 'A' record to obtain IP addresses.)

```
C:\Users\User>nslookup
Default Server:  kwd-scem.cdms.westernsydney.edu.au
Address:  137.154.148.217

> set type=mx
> gmail.com
Server:  kwd-scem.cdms.westernsydney.edu.au
Address:  137.154.148.217

Non-authoritative answer:
gmail.com       MX preference = 40, mail exchanger = alt4.gmail-smtp-in.l.google.com
gmail.com       MX preference = 5, mail exchanger = gmail-smtp-in.l.google.com
gmail.com       MX preference = 10, mail exchanger = alt1.gmail-smtp-in.l.google.com
gmail.com       MX preference = 20, mail exchanger = alt2.gmail-smtp-in.l.google.com
gmail.com       MX preference = 30, mail exchanger = alt3.gmail-smtp-in.l.google.com

gmail.com       nameserver = ns1.google.com
gmail.com       nameserver = ns3.google.com
gmail.com       nameserver = ns2.google.com
gmail.com       nameserver = ns4.google.com
ns2.google.com  internet address = 216.239.34.10
ns3.google.com  internet address = 216.239.36.10
ns4.google.com  internet address = 216.239.38.10
ns1.google.com  internet address = 216.239.32.10
ns2.google.com  AAAA IPv6 address = 2001:4860:4802:34::a
ns3.google.com  AAAA IPv6 address = 2001:4860:4802:36::a
ns4.google.com  AAAA IPv6 address = 2001:4860:4802:38::a
ns1.google.com  AAAA IPv6 address = 2001:4860:4802:32::a
> set type=a
> gmail-smtp-in.l.google.com
Server:  kwd-scem.cdms.westernsydney.edu.au
Address:  137.154.148.217

Non-authoritative answer:
Name:    gmail-smtp-in.l.google.com
Address:  74.125.24.27

>
```

1st Step: set type=mx
2nd Step: Get the mail exchange server
3rd Step: set type=a
4th Step: Enter mail-exchange server

5.3 Change the DNS server for query to '8.8.8.8'. Write the command you use for this into your lab report.

```
> server 8.8.8.8
Default Server:  dns.google
Address:  8.8.8.8

>
```

5.4 Repeat 5.2. Do you get the same results? If not, include the differences in your lab report.

```
> server 8.8.8.8
Default Server:  dns.google
Address:  8.8.8.8

> set type=mx
> gmail.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
gmail.com       MX preference = 10, mail exchanger = alt1.gmail-smtp-in.l.google.com
gmail.com       MX preference = 20, mail exchanger = alt2.gmail-smtp-in.l.google.com
gmail.com       MX preference = 40, mail exchanger = alt4.gmail-smtp-in.l.google.com
gmail.com       MX preference = 30, mail exchanger = alt3.gmail-smtp-in.l.google.com
gmail.com       MX preference = 5, mail exchanger = gmail-smtp-in.l.google.com
> set type = a
Unrecognized command: set type = a
> set type=a
> gmail-smtp-in.l.google.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    gmail-smtp-in.l.google.com
Address:  74.125.200.27

>
```

The difference was in the address of the Non-Authoritative answer:
First: The server is from scem.edu, and the output ip-address: 74.125.24.27
Second: The server is from dns.google [8.8.8.8] and the output ip-address: 74.125.200.27

PART 6

6.1 Run the command 'dig gmail.com mx +short'. Explain what this command does in your lab report, especially the meanings of the three arguments to 'dig'.

dig' is a similar tool to 'nslookup'. Its unique feature is to give detailed output about what are contained in the DNS messages.

"gmail.com" is the site or domain we want to query

"mx" is equivalent to "set type=mx" which is the type of query

"+short" is to get the shorter version.

6.2 Run the command 'dig @8.8.8.8 gmail.com mx'. Explain the meaning of the argument '@8.8.8.8' in your lab report.

"@8.8.8.8" is to change the DNS server to 8.8.8.8 similar to question 5.3.

6.3 In the 'Answer Section' of the above output, how many email servers are returned for the domain 'gmail.com'?

5 Answers were responded.

```
;; ANSWER SECTION:
gmail.com.              3074    IN      MX      40 alt4.gmail-smtp-in.l.google.com.
gmail.com.              3074    IN      MX      5 gmail-smtp-in.l.google.com.
gmail.com.              3074    IN      MX      10 alt1.gmail-smtp-in.l.google.com.
gmail.com.              3074    IN      MX      20 alt2.gmail-smtp-in.l.google.com.
gmail.com.              3074    IN      MX      30 alt3.gmail-smtp-in.l.google.com.

;; Query time: 8 msec
```