

IERG4210 2014-15 Term 2 Tutorial 9

Wenrui Diao

Department of Information Engineering
The Chinese University of Hong Kong


Outline

1. Domain Name
2. Assignment Phase 4b -- Apply SSL certificate

Domain Name

- A Level-2 domain name like storeXX.ierg4210.org has been assigned to you.
- XX → your shop ID
- Now you could assess your website via the above domain name.

Domain Name

4. Branch out **phase3b** in your repository, where TAs can checkout for inspection
 - Include a README.md file in your repo and document your application URL
- 

- If you can not access it, the reasons:
- You didn't provide your application URL (xxxx.elasticbeanstalk.com) in your github repository. Since I don't know your application URL, I can not set DNS configuration for you.
 - Solution: Send your name, SID, application URL and Shop ID to me: dw013@ie.cuhk.edu.hk
 - Upon receiving your email, I will process it in three days.
- Your application URL (xxxx.elasticbeanstalk.com) is inaccessible.
 - Solution: Debug by yourself

Outline

1. Domain Name
2. Assignment Phase 4b -- Apply SSL certificate

What is SSL / TLS?

- Transport Layer Security protocol, ver 1.0
 - De facto standard for Internet security
 - “The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating applications”
 - In practice, used to protect information transmitted between browsers and Web servers
- Based on Secure Sockets Layers protocol, ver 3.0
 - Same protocol design, different algorithms
 - TLS 1.1, 1.2, ...
- Deployed in nearly every web browser
- *More contents will be covered in the lecture.*

Regular web surfing - http: URL

Amazon.com: Online Shopping for Electronics, Apparel, Computers, Books, DVDs & more

http://www.amazon.com/

Most Visited Latest Headlines NY Times Google News Daily Weather 294 United Traffic Papers US9 IMC CSET Google Maps RSS Movies

amazon.com Hello. [Sign in](#) to get personalized recommendations. New customer? [Start here.](#) **FREE 2-Day Shipping, No Minimum Purchase: See details**

Your Amazon.com Today's Deals Gifts & Wish Lists Gift Cards [Your Account](#) Help

Shop All Departments Search All Departments GO Cart Wish List

Books > Movies, Music & Games > Digital Downloads > Kindle > Computers & Office > Electronics > Home & Garden > Grocery, Health & Beauty > Toys, Kids & Baby > Clothing, Shoes & Jewelry > Sports & Outdoors > Tools, Auto & Industrial >

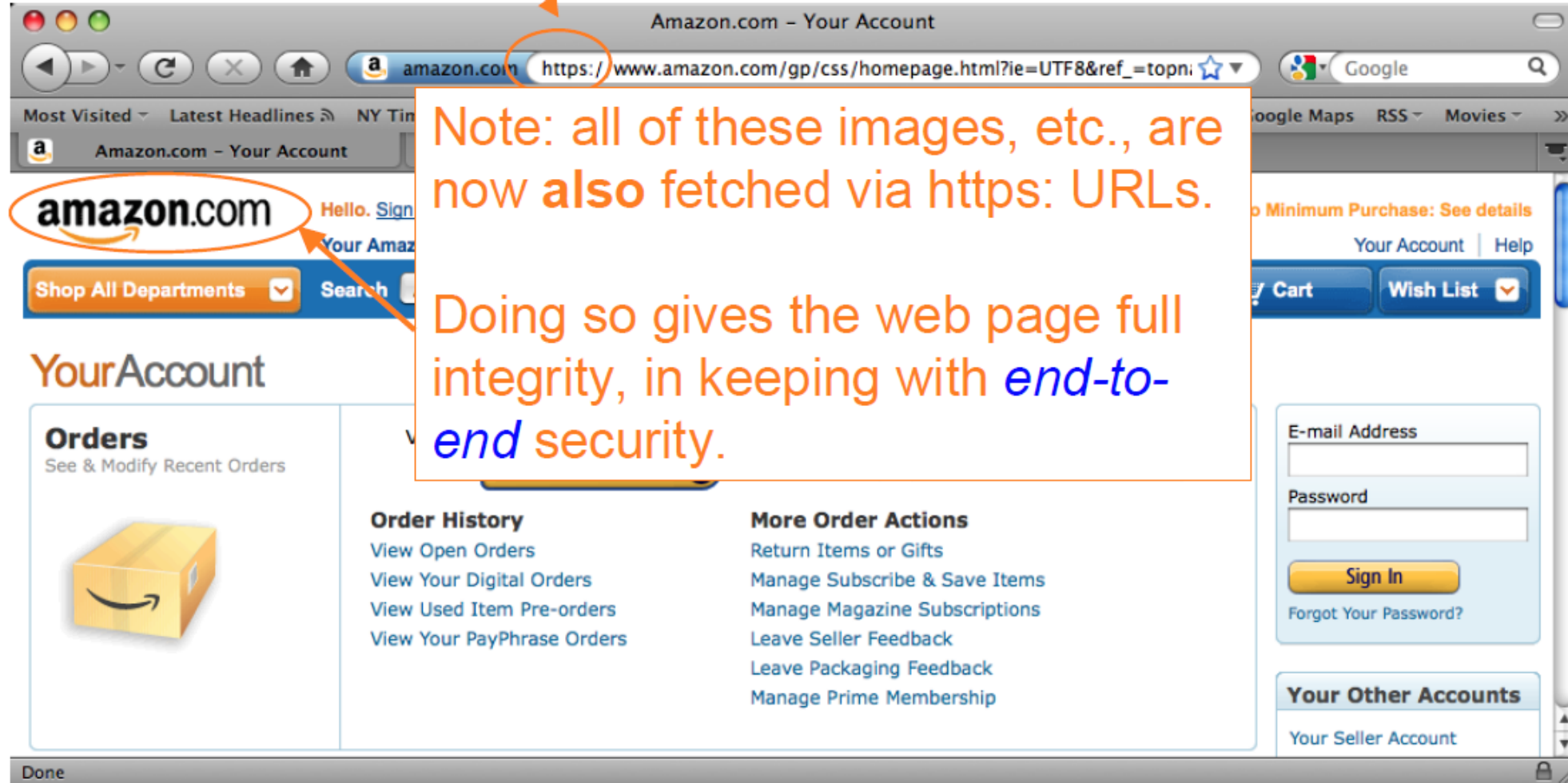
Kindle
You'll Do a Double Take.
Reads Like Real Paper,
Even in Bright Sunlight.

[Shop now](#)

What's your Pay Phrase? "Strategic Insight" is still available! [Claim yours](#)

Warm Your Feet in UGG
These twin-faced, breathable sheepskin UGG boots keep your feet warm and cozy at any time of year. Multiple styles and colors available.

Web surfing with TLS/SSL - https: URL



The screenshot shows a web browser window titled "Amazon.com - Your Account". The address bar contains the URL "https://www.amazon.com/gp/css/homepage.html?ie=UTF8&ref_=topni". The Amazon logo is circled in orange. A text box with an orange border contains the following text:

Note: all of these images, etc., are now **also** fetched via https: URLs.

Doing so gives the web page full integrity, in keeping with *end-to-end* security.

The page content includes sections for "Orders", "Order History", "More Order Actions", and "Your Other Accounts".

Assignment Phase 4b -- Apply SSL certificate

- Certificate Application
 - -- Apply a 90-day free certificate from FreeSSL.su
- Certificate Installation
 - -- Elastic Beanstalk load balancer settings
- For more details, please check <http://ierg4210.github.io/web/assign-spec/AssignmentMarkingChecklist4.1.pdf>

Create a private key and CSR

- Openssl is preinstalled in most Linux distribution versions, like Ubuntu
- Generate the private key
- `$ openssl genrsa 2048 > privatekey.pem`

never upload it to github

```
diaowenrui@ubuntu:~/4210Amazon$ openssl genrsa 2048 > privatekey.pem
Generating RSA private key, 2048 bit long modulus
.....+++
.....
.....+++
e is 65537 (0x10001)
```

Create the Certificate Signing Request (CSR)

- `$ openssl req -new -key privatekey.pem -out csr.pem`

```
diaowenrui@ubuntu:~/4210Amazon$ openssl req -new -key privatekey.pem -out csr.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:HK
State or Province Name (full name) [Some-State]:Hong Kong
Locality Name (eg, city) []:Hong Kong
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CUHK
Organizational Unit Name (eg, section) []:IERG4210
Common Name (e.g. server FQDN or YOUR name) []:store97.ierg4210.org
Email Address []:diaowenrui@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

It will be shown in
your certificate.

To show your CSR:

- \$ cat csr.pem
- It will be used in the next step

```
(local-dev-env)diaowenrui@ubuntu:~/4210Amazon$ cat csr.pem
-----BEGIN CERTIFICATE REQUEST-----
MIICzDCCABQCAQAwYYxCzAJBgNVBAYTAkhLMRIwEAYDVQQIDAlIb25nIETvbmcx
DTALBgNVBAoMBENVSEsxETAPBgNVBAsMCeIFUkc0MjEwMRwwGgYDVQQDBNzaG9w
OTcuaWVzZzQyMTAub3JnMSMwIYJKoZIhvcNAQkBFhRkdzAxM0BpZS5jdWhrLmVk
dS5oazCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAL+li/d7J6HKNUjZ
G4+Ds3W2bhDLi12n57/bU0xHn6c9yME3bkAUtAJAx1jHQrh5KUv5bdJzJp7jyDVJ
pt5Ny/hBoQiGmyYGXqe2MwD0q/HQhNq0eiEBWtrBXregLeHZlhf3x4JPxuZwef6k
civS3ZdjgQdWRrhDyY1W9FvQb4JXpvQITwWxCl3kBgSYHLQ0bLKMffw0y6Mmasad
/YuMXdhzEEzIqBzF5oDzk+2g/BqZmiExCE9Z2n4CVU/o3DTTV3LVf97yzIushHqI
ZPKEmRXXljdkMIq201HLqe0Y6VtCzpZg2YP4hvLSnTw+0t79nVQyiTc7qzdvr3ej
Y68fgZ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IBAQAkRcJn0M/nZUgZa3qGAbF7
c/voxp91Crq0qQ2AF9vImZKP2IR0dXHEy67UkMcOjluASPSEZ6GAmUXBtPierev
biShLaSIEv3UU0JuxMNB6pZ6sa9kBCVRCBP95xpTXccqUS0+r+0fllIhk2jdkyj
Ss1V6Io5RVrE2IzCUjNFnc4BmbX959+1qZ8sHZk80Pz8tcTz3wWt0NXBhU2HFHv
x7qGDx+tSPJd6rsTYAIFe2UI0jufWupVXoiTCy3TDH472Td4l+kwX3HNDnjRdG8D
Zmxfu5jKVqQocZ5ddVQ1WqwWpUSXzpv7xbgrF/I1yr5fKviekPgUBgICUVcnAeIU
-----END CERTIFICATE REQUEST-----
```

Certificate Application

- Go to <http://www.freessl.su/>

Change to your own Information.
This Email address will be used to
receive the certificate.

Your Name:
Example: *John Smith*

Your E-mail:
Example: *test@example.com*

Phone:
Example: *8(495)2295670*

Select the server software used to generate the CSR:
Example: *Apache-SSL*

CSR (Generating a Certificate Signing Request):
Example:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDUDCCArkCAQAwdTEWMBQGA1UEAxMNdGVzdC50ZXN0LmNvbTESMBAGA1UECXMJ
TWYfa2V0aW5nMREwDwYDVQQKEwhUZXR0IE9yZzESMBAGA1UEBxMjVGVzdCBDaXR5
.....
Rq+blLr5X5iQdzyF1pLqP1Mck5Ve1eCz0R9/OekGSRno7ow4TVyxAF6J6ozDaw7e
GisfZw40VLT0/6IGvK2jX0i+t58RFQ8WYTOcTRIPnkG8B/uV
-----END CERTIFICATE REQUEST-----
```

hiShLaSIEv3UU0JuxMNB6pZ6sa9kBCVRCPEP95xpTXccqUS0+r+0f11Ihk2jdky.i
Ss1V6Io5RVrE2IzCUjNFnc4EmbX959+1qZ8sHZk80Pz8tcTzM3wWtONXBhU2HFHv
x7qGDx+tSPId6rsTYAIFe2UIQjufWupVXoiTCy3TDH472Id41+kwX3HNDnjRdG8D
Zmxfu5iKVqQocZ5ddVQ1WqWpUSXzpv7xbgrF/I1yr5fKviekPgUBgICUVcnAeIU
-----END CERTIFICATE REQUEST-----

Next >>>

Certificate Application

- For Domain Control Validation, choose admin@ierg4210.org as the approved email address to prove domain ownership. The TA team upon receiving an email from Comodo will help you authorize such a SSL cert application.

Please select the approved email address to which you would like us to send the domain control validation email.

Alternative email addresses (Level 2)

- admin@ierg4210.org
- administrator@ierg4210.org
- hostmaster@ierg4210.org
- postmaster@ierg4210.org
- webmaster@ierg4210.org

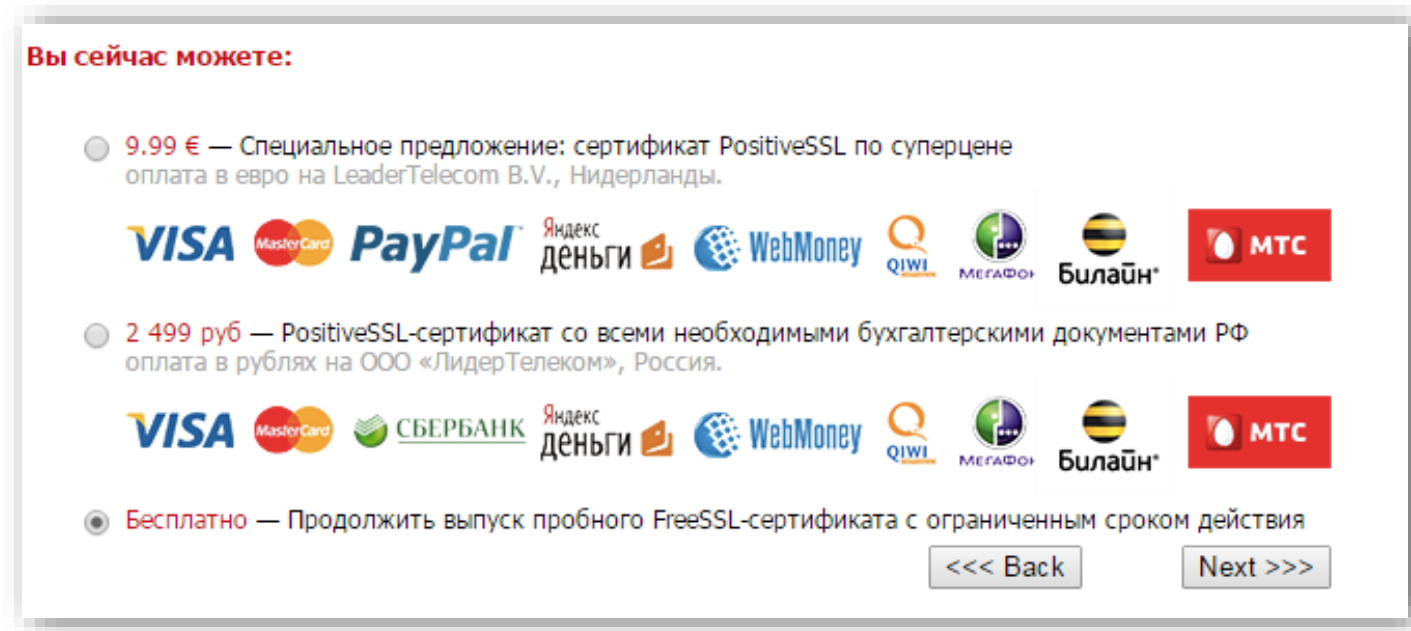
Alternative email addresses (Level 3)

- admin@shop97.ierg4210.org
- administrator@shop97.ierg4210.org
- hostmaster@shop97.ierg4210.org
- postmaster@shop97.ierg4210.org
- webmaster@shop97.ierg4210.org

<<< Back Next >>>

Certificate Application

- Choose the last one.



- It then take an hour or up to 2 days to have the cert signed by Comodo and emailed to you (in an attachment ssl_certificate.zip).

Upload the private key and signed cert

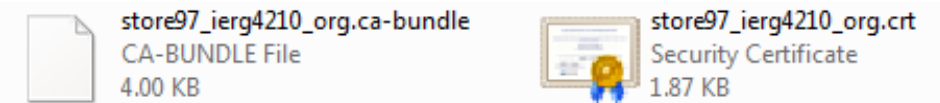
- Install the aws client
- `$. local-dev-env/bin/activate`
- `$ pip install aws`
- `$ pip install awscli`

- You may need to set the access key (which you got in your previous phase) if you face the permission deny problem
- `$ aws configure`

Upload the private key and signed cert

- `$ aws iam upload-server-certificate --server-certificate-name comodo-signed-shop97-2015 --certificate-body file://~/4210Amazon/cert/store97_ierg4210_org.crt --private-key file://~/4210Amazon/cert/privatekey.pem --certificate-chain file://~/4210Amazon/cert/store97_ierg4210_org.ca-bundle`

```
(local-dev-env)diaowenrui@ubuntu:~/4210Amazon/cert$ aws iam upload-server-certificate --server-certificate-name comodo-signed-shop97-2015 --certificate-body file://~/4210Amazon/cert/store97_ierg4210_org.crt --private-key file://~/4210Amazon/cert/privatekey.pem --certificate-chain file://~/4210Amazon/cert/store97_ierg4210_org.ca-bundle
{
  "ServerCertificateMetadata": {
    "ServerCertificateId": "ASCAJ2MCSDBGJWT500G36",
    "ServerCertificateName": "comodo-signed-shop97-2015",
    "Expiration": "2015-06-12T23:59:59Z",
    "Path": "/",
    "Arn": "arn:aws:iam::096581827784:server-certificate/comodo-signed-shop97-2015",
    "UploadDate": "2015-03-15T03:10:14.648Z"
  }
}
```



Change them according to your received files.

Elastic Beanstalk load balancer settings

- EC2 Dashboard → Network & Security → Load Balancers → Edit listeners

Edit listeners ✕

The following listeners are currently configured for this load balancer:

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port	Cipher	SSL Certificate	
HTTP	80	HTTP	80	N/A	N/A	✕
HTTPS (Secure HTTP)	443	HTTP	80	Change	comodo-signed-shop97-2015	Change ✕

[Add](#)

[Cancel](#) [Save](#)

Add HTTPS Protocol

Choose the certificate
you uploaded

Elastic Beanstalk load balancer settings

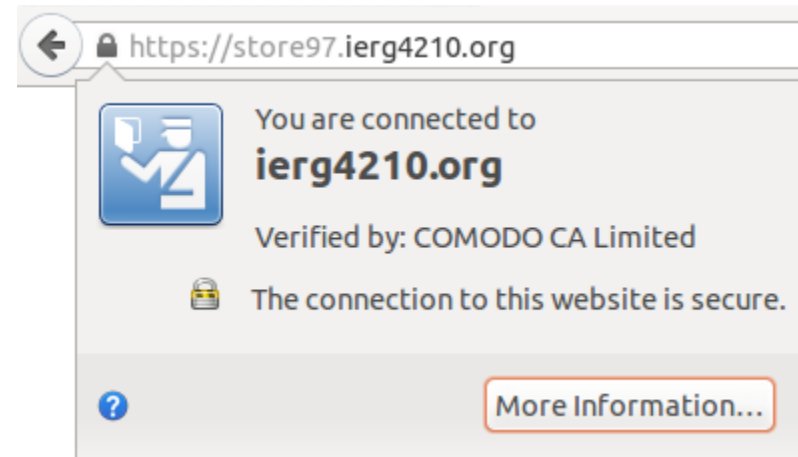
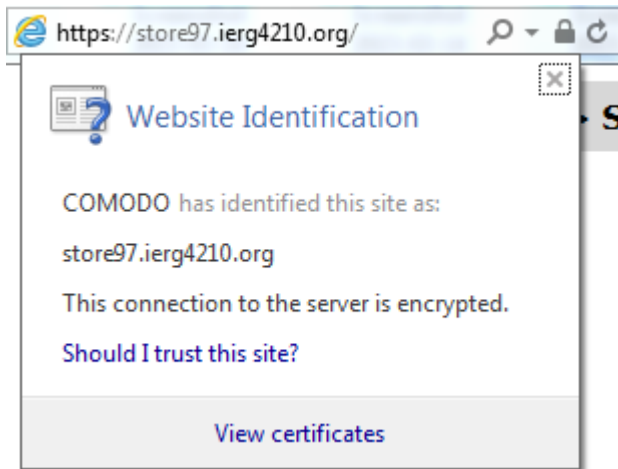
- EC2 Dashboard → Network & Security → Security Groups → Choose the one with the description “ELB created security group used when no security group is specified during ELB creation - modifications could impact traffic to future ELBs”
- Edit inbound rules

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
HTTP ▾	TCP	80	Anywhere ▾ 0.0.0.0/0 ✕
HTTPS ▾	TCP	443	Anywhere ▾ 0.0.0.0/0 ✕

Add rules for HTTPS

Test

- After a few mins, visit your website <https://shopXX.ierg4210.org> to verify.



Enforce the admin panel /admin to https

```
app.use('/admin', function(req, res, next) {
  var schema = req.headers['x-forwarded-proto'];

  if (schema === 'https') {
    // Already https; don't do anything special.
    next();
  }
  else {
    // Redirect to https.
    res.redirect('https://' + req.headers.host + req.url + '/admin');
  }
});
```

Demo and Q&A

- Ref (prepared by Dr. Fung):
 - <https://github.com/ierg4210/shop-samples/blob/master/SETUP-CERT.md>
-
- Some contents are borrowed from
 - <http://inst.eecs.berkeley.edu/~cs161/fa14/>
 - <http://www.stanford.edu/class/cs259>