CS 391 Final

1.

a)

src IP = 131.212.31.167
Dest IP = 128.119.245.12
src Port = 2096
Dst Port = 80

b) Yes
c) Yes
d)

Packet 3 = SYN
Packet 4 = SYN, ACK
Packet 5 = ACK

e)

Sequence # = 2573210089
Ack # = 1038395700

f) By making the first Sequence # random, an adversary can't guess the Sequence numbers for every packet, since each sequence # increments by 1 for the next packet. If the initial Sequence # was a predictable number like zero, then an adversary can just keep adding 1 to the sequence numbers to get all of the packet sequence numbers

2. a) IP address of DNS server = 192.168.170.20

b) UDP

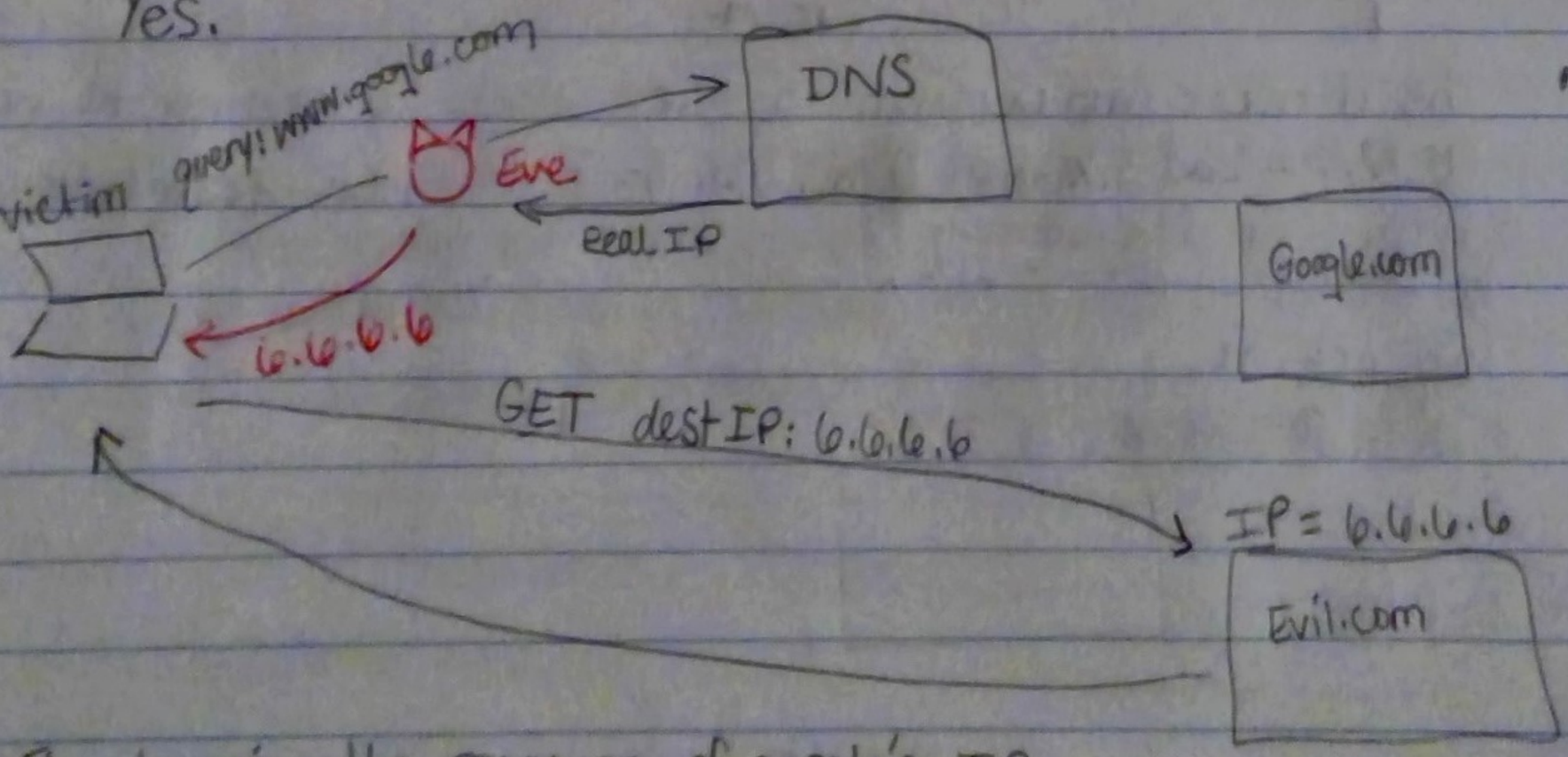
c) Find DNS response packet for google query in packet #15
alternate Domain name for www.google.com?
www.l.google.com

d) Is response authenticated w/ MAC or dig signatures?
No

e) No

f) An adversary can learn a lot from the Metadata.
If the victim has an illness, they may search certain medications. The victim's age and gender could be revealed, if the victim goes on certain shopping websites. Where the victim lives could be revealed if the victim searches for "restaurants near me".

g) changes response so google IP = 6.6.6.6
-Traffic from Google sent over HTTP
Can adversary modify traffic client receives from Google?
Yes.



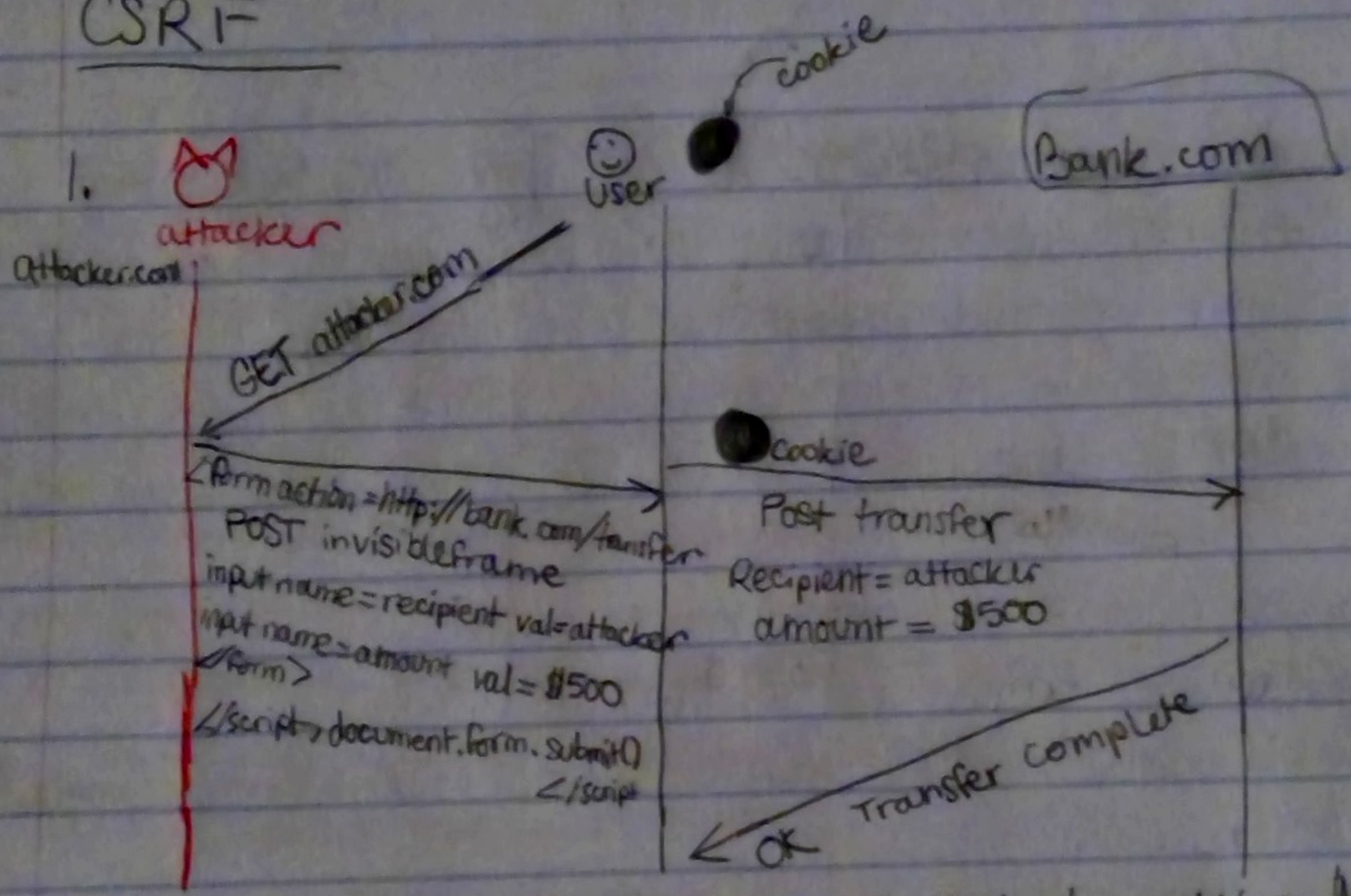
- Since traffic from Google is sent over HTTP traffic is not encrypted, Attacker can modify and drop packets.

- By changing the response of google's IP, the victim then thinks Evil.com is google and interacts with Evil.com as if it is google.

2.h) Assume Traffic is sent over HTTPS

- Since traffic sent over HTTPS is encrypted, the traffic cannot be modified or dropped without the victim computer being aware.
- However, traffic from google being sent over HTTPS doesn't stop the adversary from changing the IP address in the response from packet #15, so the victim could still be interacting with the website at IP 6.6.6.6 instead of Google.

2. CSRF

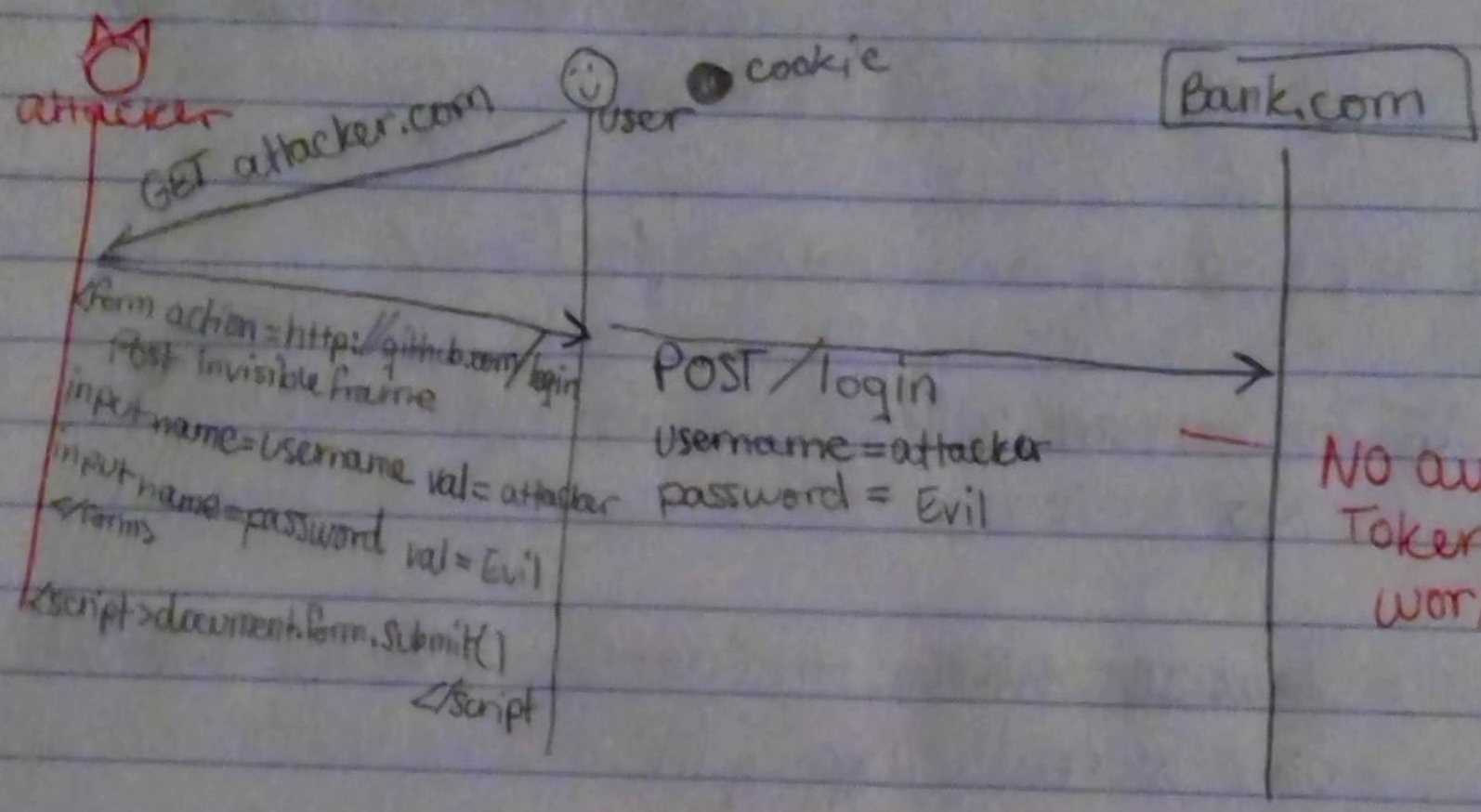


The attacker can perform a CSRF attack by getting the victim to go to the bad site that looks like Bank.com/transfer. The attacker creates a form that automatically submits & transfers money to himself. The transfer is POSTed to Bank.com/transfer without the victim making a GET request. The transfer is successful because the user's cookie is still active.

2. NO

3.

- Yes, there's an input for an authenticity token which make's sure that the user has seen the website. So, an attacker would not be able to submit the form because then the user would do a POST request before a GET request meaning the user has not seen the website before because they never asked for it.



4. Web Crypto Audit

1. www.gap.com

a) Tracking pixels:

bbtrack.com
doubleclick.net
twitter
sp.analytics.yahoo.com
cdnssl.clicktale.net
wkxpphj-qx.global.ssl.fastly.net
optimizely.com

b) Yes, because HTTPS protects against man-in the middle attacks and not against XSS or tracking pixels which come from javascript code.
Also, the tracking pixel can from a site that uses HTTP, while the website with the pixel on it uses HTTPS.

c) Which cookie controls the regions? Value set for UK site?

.co.uk/
gapcanada.ca

locale cookie

locale value for UK = en_GB

2. https://app.carta.com/acounts/login/

a) Do you send a certificate to app.carta.com?
No

b) Cookies allow the website to know that the user is really logging in

c) The user knows that the server is really carta because Carta has a certificate that is signed by a certificate Authority to confirm that the certificate is valid

d) $h = H(p)$ $H = SHA256$
Yes because SH256 computes h quickly so a dictionary attack will also be quick. Additionally, the passwords aren't being hashed with a salt, which would have made a dictionary attack more difficult.

3. www.coindesk.com

a) i) First two bytes of the public key in certificate
30 82

ii) What entity holds the secret key to this public key?
Coindesk has the secret key

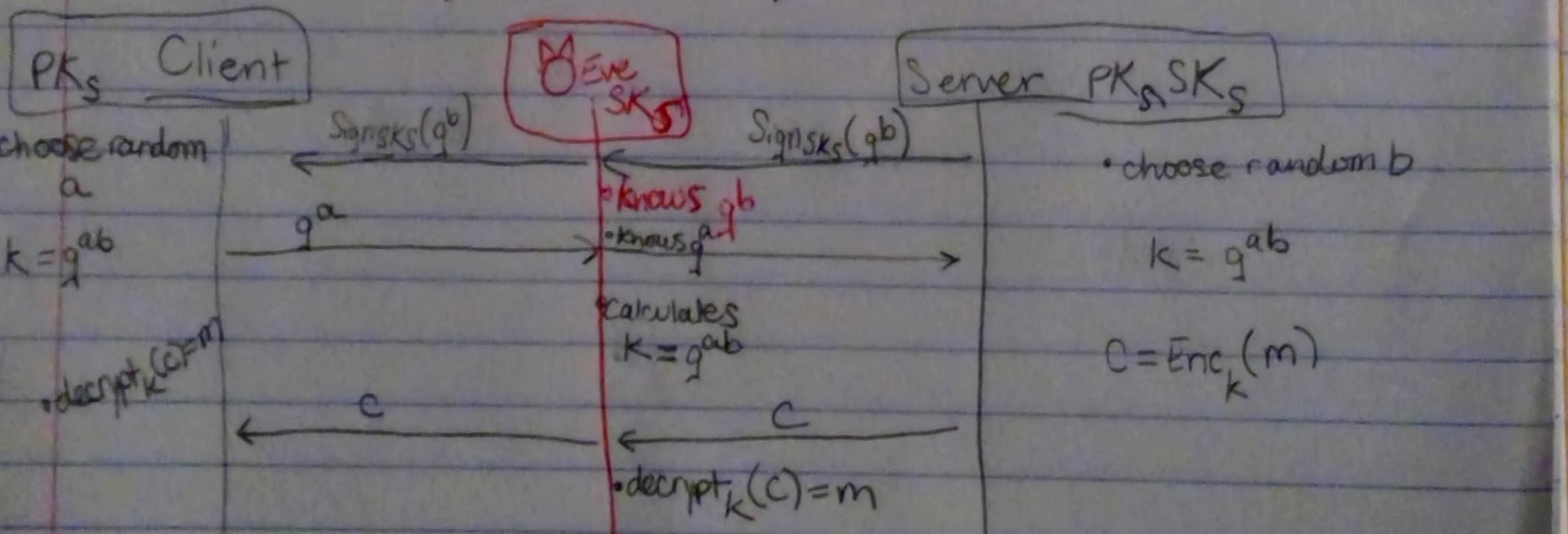
iii) Amazon

iv) The purpose of the signature is to confirm that the website for coindesk is valid and coindesk is really who they say they are

v) My browser obtained the certificate from Amazon Root Certificate Authority and the Amazon Root CA is shipped with the computer operating system

b) The Root certificate is issued by the operating system because the OS ships with a list of CAs to be trusted

c) Yes, because the adversary can decrypt messages by learning the symmetric key after decrypting with SK_S



4. Digital Signatures, Bitcoin

$A = SK_A, PK_A$ — t = time

$B = SK_B, PK_B$ — s = signed keys, amount, time

a = amount of Bitcoin — θ = Signed amount

original = $t||s$ — modified = $t||s||\theta$

$t+s$ — (t, s, θ)

Since the transaction is in a tuple and θ is not connected to the other parts of the transaction, the adversary can drop θ so that the transaction doesn't go through