(a)

3pts) The Top Level Domain ".dev" is currently in the HSTS preload list.
What does that mean for your new web project that runs at "pets-exam.dev"?

(b)

3pts) Your DNS resolver gives you the following record. What does that mean?

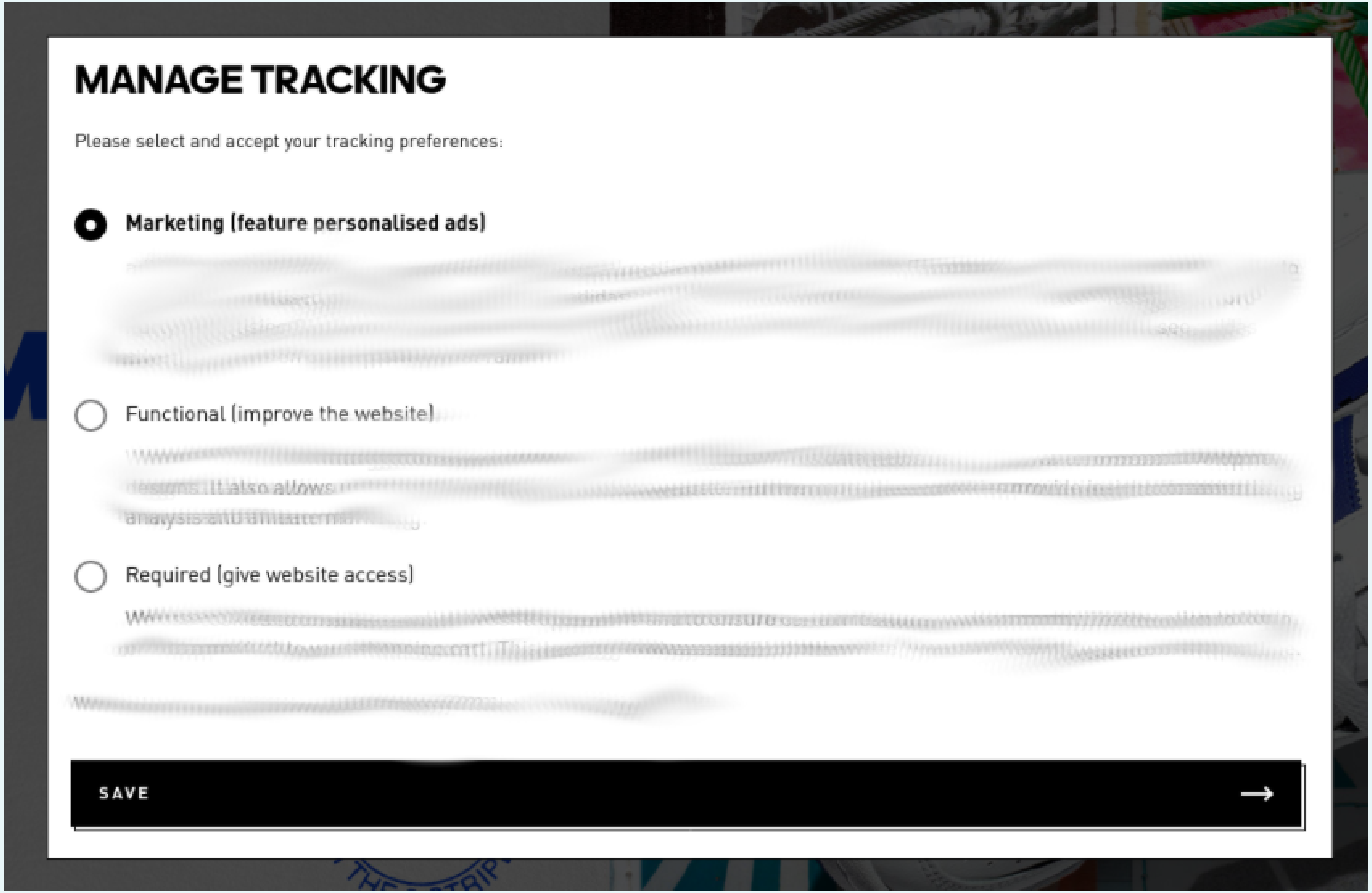
```
$ dig CAA pets-exam.dev
[...]
;; ANSWER SECTION:
pets-exam.dev.          3580    IN    CAA    128 issue "letsencrypt.org"
pets-exam.dev.          3580    IN    CAA    128 issue "globalsign.com"
[...]
```

(c)

4pts) You configured the TLS settings of your project only with the most modern version TLS1.3 to ensure maximum security.
What are possible problems with this configuration?

The ongoing pandemic led to an increase in new online shops. One of these new online shops sparks your interest. Before you start using the online shop you want to verify how they use online tracking.

Below you see a screenshot of the online shop's tracking consent dialog.



MANAGE TRACKING

Please select and accept your tracking preferences:

● Marketing (feature personalised ads)

[redacted]

○ Functional (improve the website)

[redacted]

○ Required (give website access)

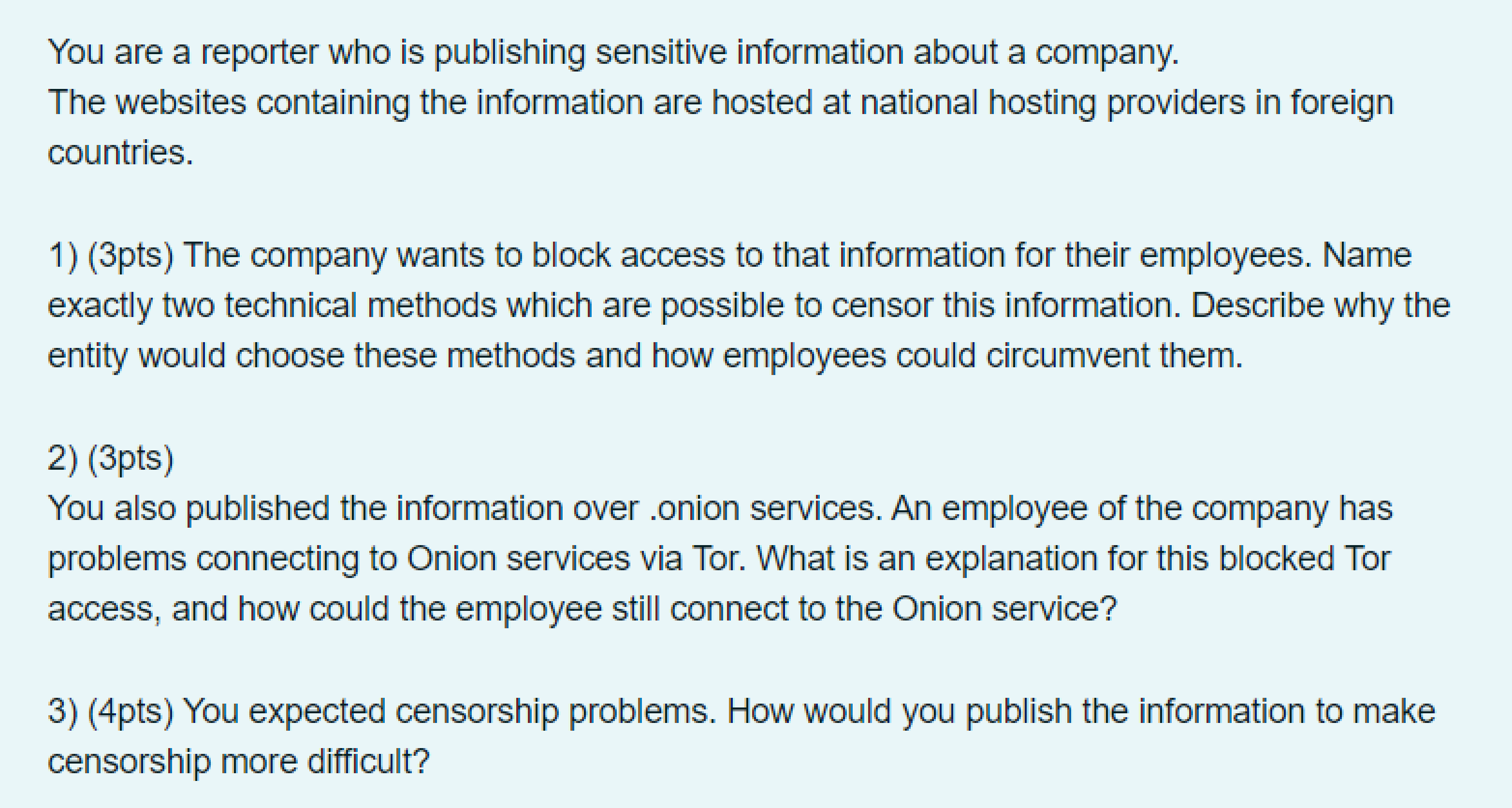
[redacted]

[redacted]

1) (3 pt) Provide examples of services commonly used for "Marketing", "Functional" and "Required" tracking.

2) (4 pt) Describe how to verify if the tracking consent settings have an effect?

3) (3 pt) Describe the overall risks of relying on opt-out dialogs.

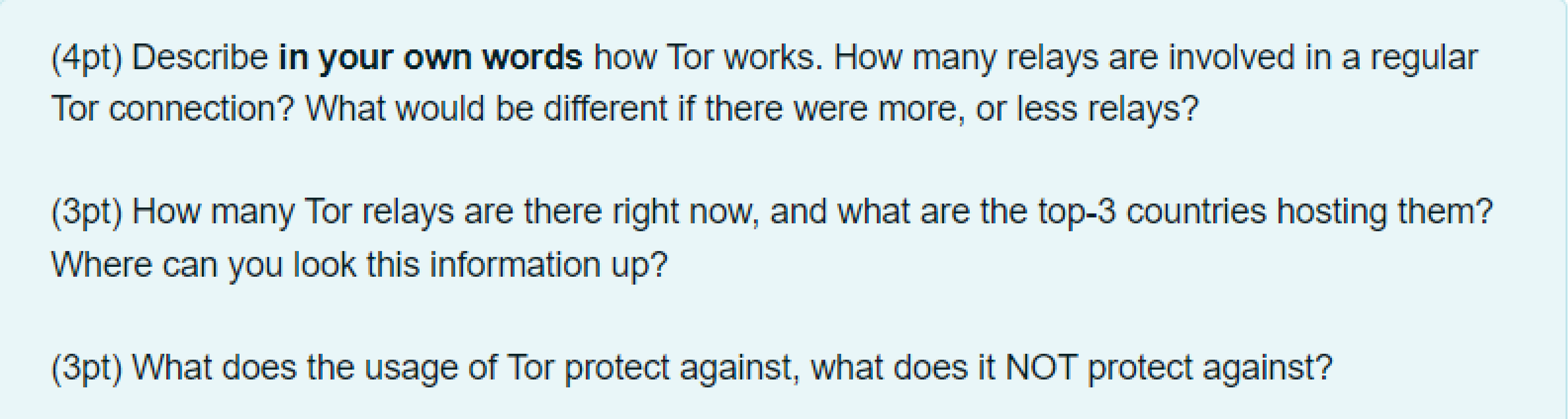


You are a reporter who is publishing sensitive information about a company.
The websites containing the information are hosted at national hosting providers in foreign countries.

1) (3pts) The company wants to block access to that information for their employees. Name exactly two technical methods which are possible to censor this information. Describe why the entity would choose these methods and how employees could circumvent them.

2) (3pts)
You also published the information over .onion services. An employee of the company has problems connecting to Onion services via Tor. What is an explanation for this blocked Tor access, and how could the employee still connect to the Onion service?

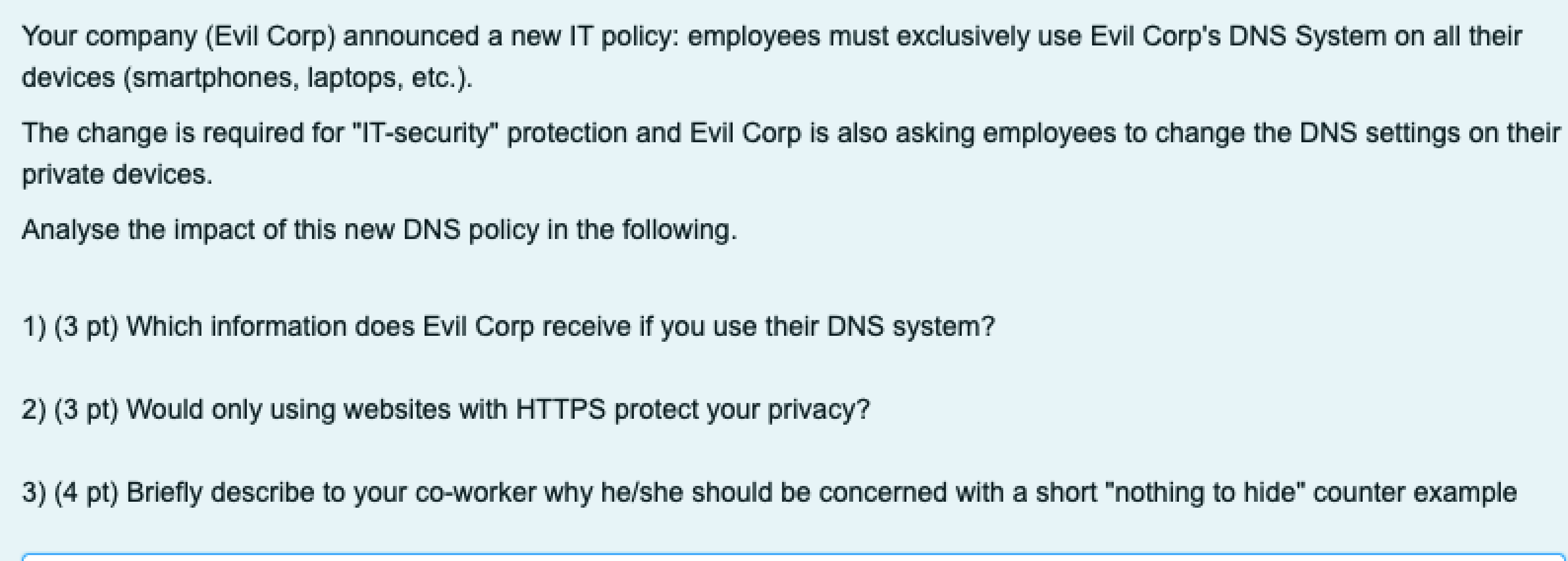
3) (4pts) You expected censorship problems. How would you publish the information to make censorship more difficult?



(4pt) Describe **in your own words** how Tor works. How many relays are involved in a regular Tor connection? What would be different if there were more, or less relays?

(3pt) How many Tor relays are there right now, and what are the top-3 countries hosting them? Where can you look this information up?

(3pt) What does the usage of Tor protect against, what does it NOT protect against?



Your company (Evil Corp) announced a new IT policy: employees must exclusively use Evil Corp's DNS System on all their devices (smartphones, laptops, etc.).

The change is required for "IT-security" protection and Evil Corp is also asking employees to change the DNS settings on their private devices.

Analyse the impact of this new DNS policy in the following.

1) (3 pt) Which information does Evil Corp receive if you use their DNS system?

2) (3 pt) Would only using websites with HTTPS protect your privacy?

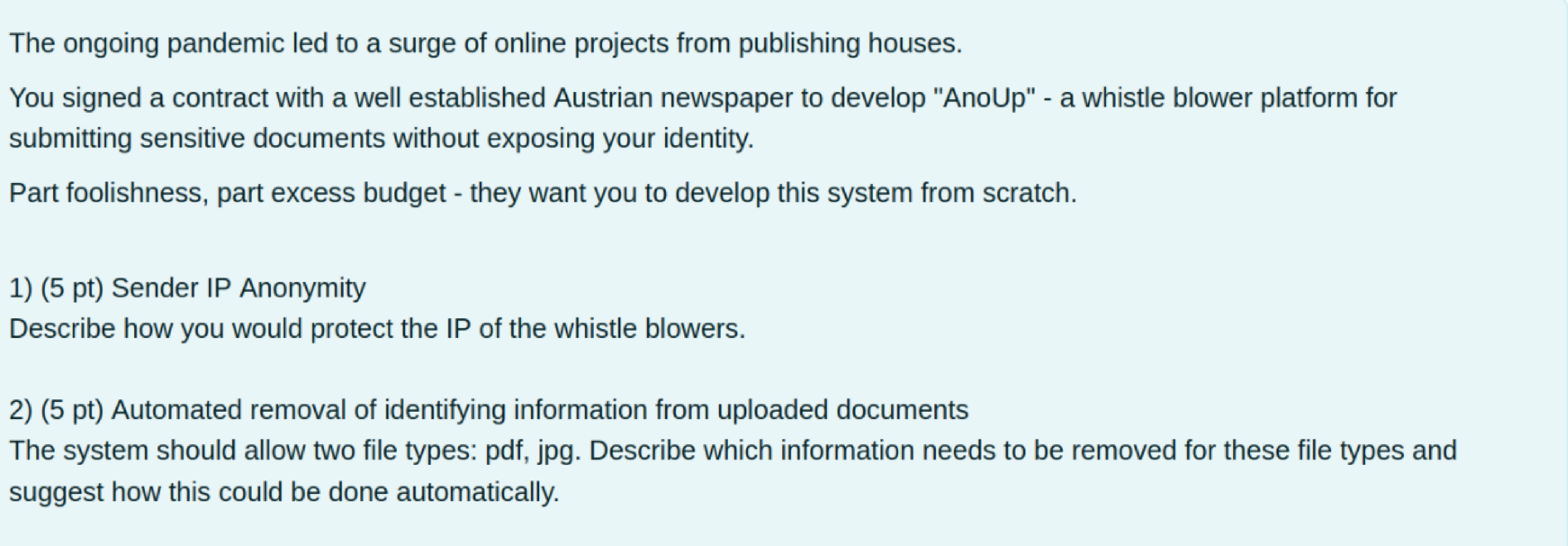
3) (4 pt) Briefly describe to your co-worker why he/she should be concerned with a short "nothing to hide" counter example

(4pt) Explain **in your own words** how Tor Onion (Hidden) services work. How many Tor relays are involved per connection?

(2pt) What is the difference between v2 and v3 Tor Onion services? Why are Onion Services v3 better than v2?

(2pt) Is it useful to have a TLS certificate for your Onion services? What are the benefits, if any?

(2pt) How do you get a onion domain like "facebookcorewwwi.onion"? Other domains look random compared to this. So, how does this work and why?



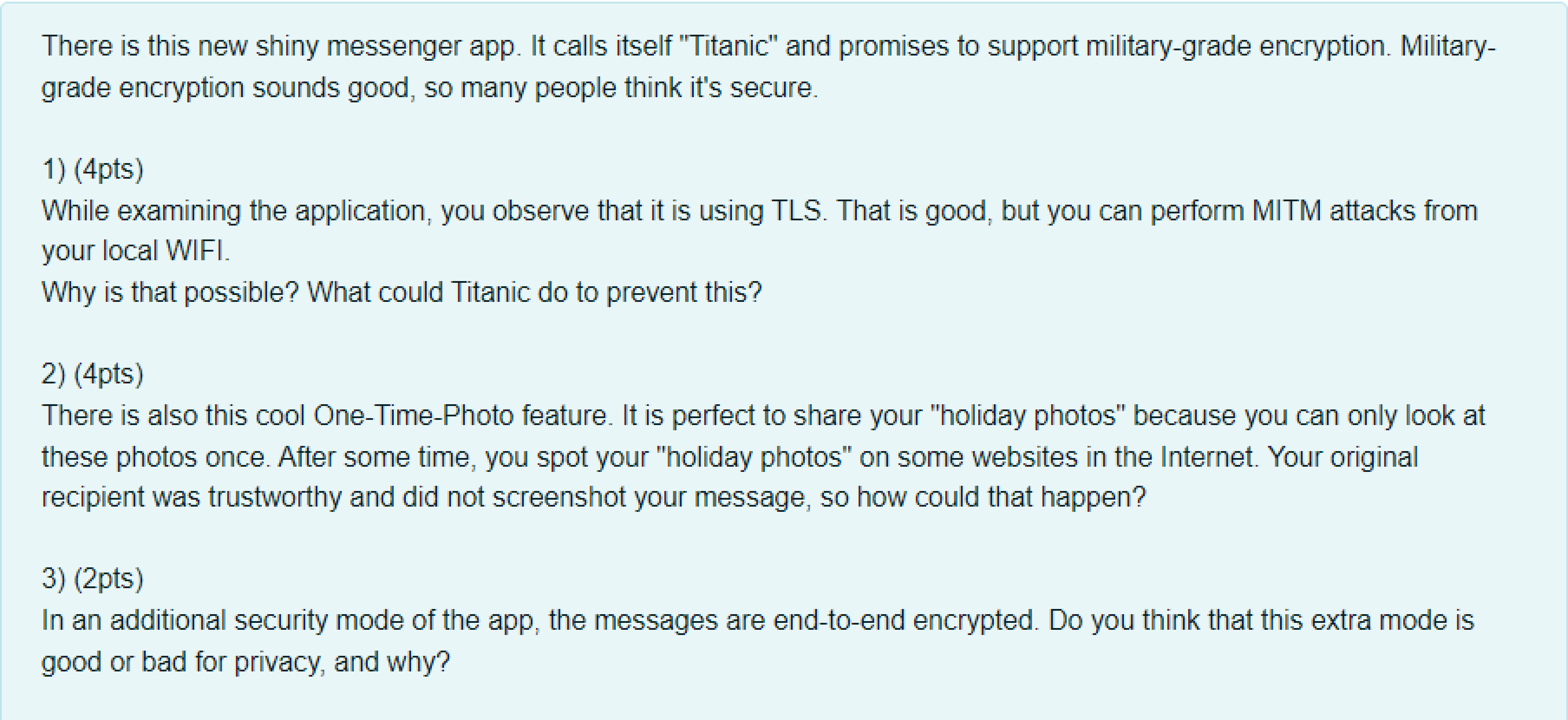
The ongoing pandemic led to a surge of online projects from publishing houses.

You signed a contract with a well established Austrian newspaper to develop "AnoUp" - a whistle blower platform for submitting sensitive documents without exposing your identity.

Part foolishness, part excess budget - they want you to develop this system from scratch.

1) (5 pt) Sender IP Anonymity
Describe how you would protect the IP of the whistle blowers.

2) (5 pt) Automated removal of identifying information from uploaded documents
The system should allow two file types: pdf, jpg. Describe which information needs to be removed for these file types and suggest how this could be done automatically.



There is this new shiny messenger app. It calls itself "Titanic" and promises to support military-grade encryption. Military-grade encryption sounds good, so many people think it's secure.

1) (4pts)

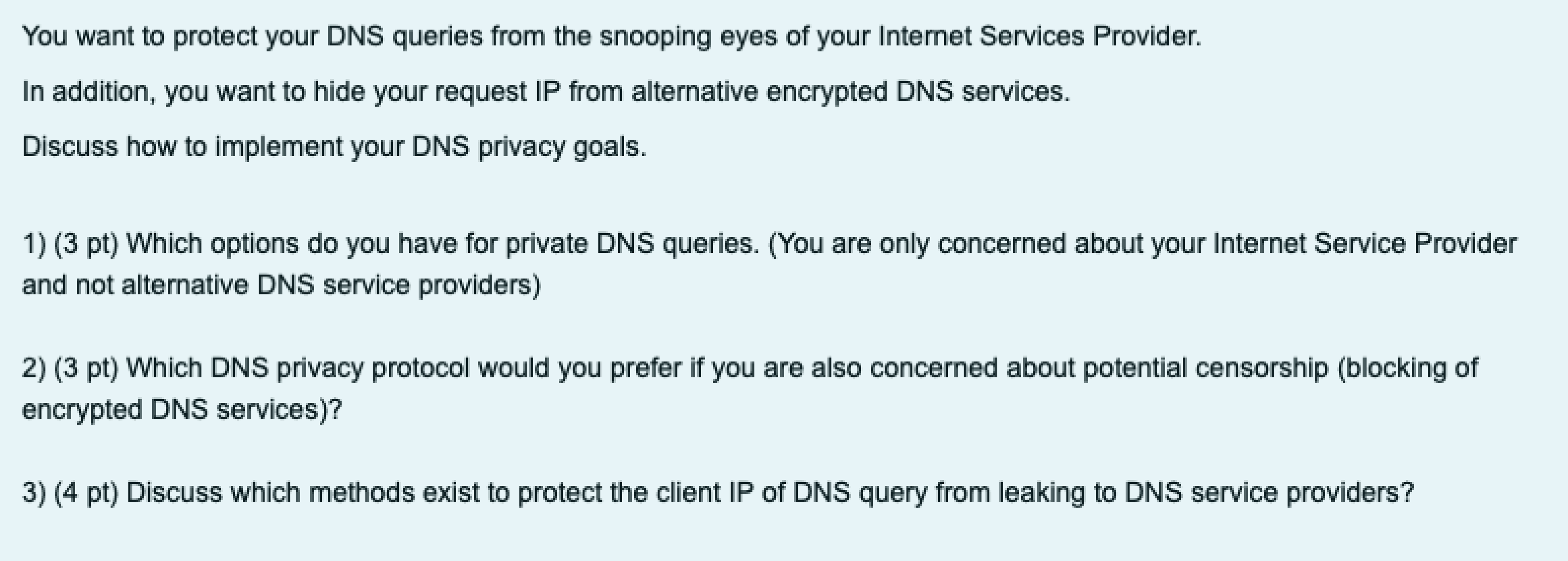
While examining the application, you observe that it is using TLS. That is good, but you can perform MITM attacks from your local WIFI.
Why is that possible? What could Titanic do to prevent this?

2) (4pts)

There is also this cool One-Time-Photo feature. It is perfect to share your "holiday photos" because you can only look at these photos once. After some time, you spot your "holiday photos" on some websites in the Internet. Your original recipient was trustworthy and did not screenshot your message, so how could that happen?

3) (2pts)

In an additional security mode of the app, the messages are end-to-end encrypted. Do you think that this extra mode is good or bad for privacy, and why?



You want to protect your DNS queries from the snooping eyes of your Internet Services Provider.

In addition, you want to hide your request IP from alternative encrypted DNS services.

Discuss how to implement your DNS privacy goals.

1) (3 pt) Which options do you have for private DNS queries. (You are only concerned about your Internet Service Provider and not alternative DNS service providers)

2) (3 pt) Which DNS privacy protocol would you prefer if you are also concerned about potential censorship (blocking of encrypted DNS services)?

3) (4 pt) Discuss which methods exist to protect the client IP of DNS query from leaking to DNS service providers?