1. Explain how the website can track if the users are violating the copyright rules and block the IP addresses.

The website can track if users are violating copyright rules through a combination of technical and legal measures. Here are some ways how this tracking might be implemented:

1) IP Tracking: As mentioned in the message, the website can track users' IP addresses. Each device connected to the internet has a unique IP address. By logging and monitoring these addresses, the website can identify and block specific IPs that are associated with copyright violations. However, this method has limitations, as IP addresses can change dynamically, and multiple users may share the same IP (e.g., in a large organization).

2) User Accounts and Authentication: The website may require users to create accounts and log in before taking a test. User accounts provide a way to tie activities to specific individuals. If a user is found to be in violation of copyright rules, their account can be flagged or blocked.

3) Browser Fingerprinting: Websites can use browser fingerprinting techniques to create a unique identifier for each user based on their browser and device characteristics. This can be used to track users even if they switch IP addresses. However, it's worth noting that browser fingerprinting is not foolproof and may have privacy implications.

4) Monitoring and Analysis of User Behavior: The website may analyze user behavior during the test. Unusual patterns, such as rapid completion of questions or repeated attempts to access restricted content, could trigger alerts for potential copyright violations.

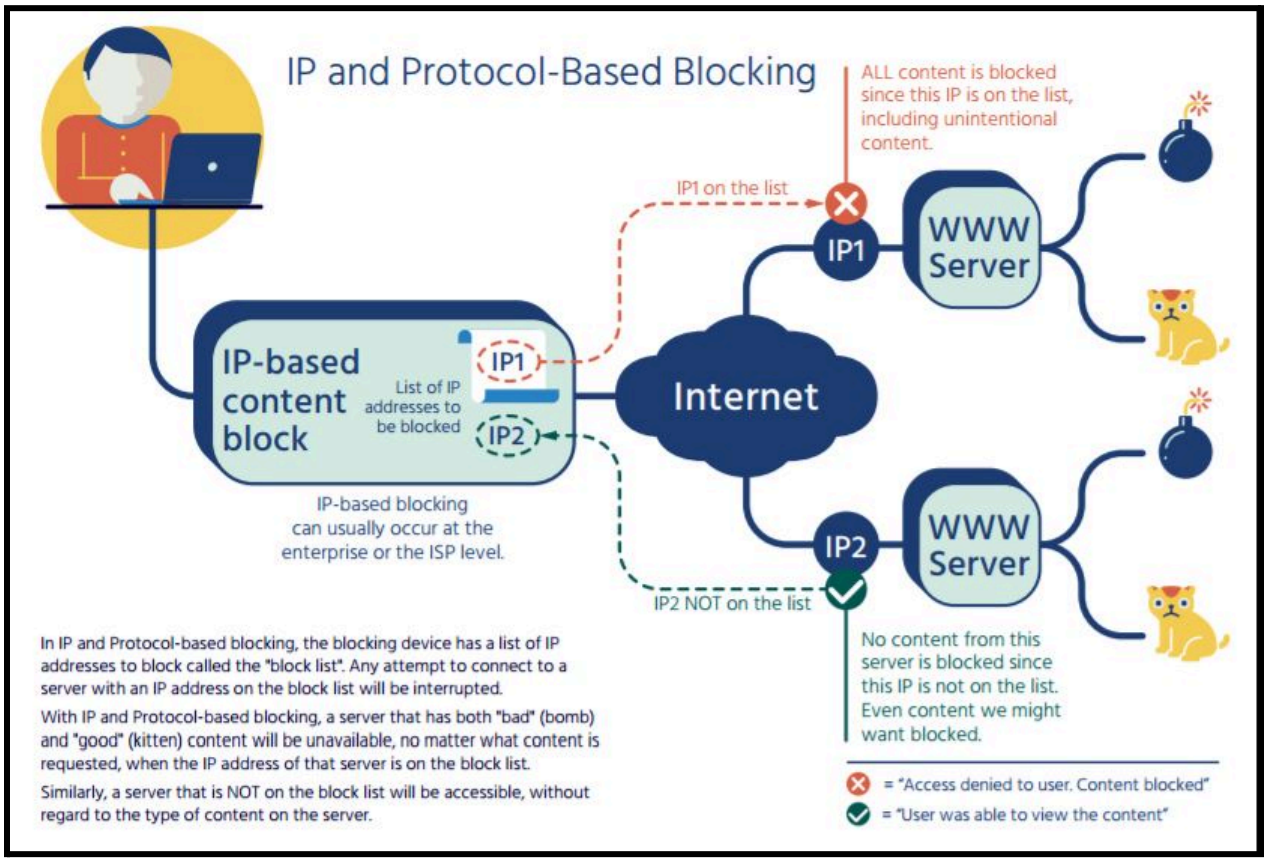
5) Digital Watermarking: The content presented to users during the test might be digitally watermarked in a way that's not visible to the user. If the website detects its content being reproduced or transmitted without authorization, it can trace the source back to the specific instance of access and take appropriate action.

IP and Protocol-Based Blocking

IP-based blocking places barriers in the network, such as firewalls, that block all traffic to a set of IP addresses. Protocol-based blocking uses other low-level network identifiers, such as a TCP/ IP port number that can identify a particular application on a server or a type of application protocol. These simplest approaches to blocking content don’t actually directly block content they block traffic to known IP addresses or TCP/IP ports or protocols associated with some content or an application. IP and protocol-based blocking may also be done by software on user’s computers, typically for network security purposes.

For example, if the goal was to block all content hosted in the mythical country of Elbonia, IP blocking could be used if the set of all IP addresses hosting content in Elbonia were known. Similarly, if the goal was to block all VPN services (which are used to encrypt traffic and hide

both the destination and the content), protocol-based blocking could be used to stop VPN services using well-known protocols or TCP/IP port numbers.



A variation on IP blocking is throttling of traffic. In this scenario, not all traffic is blocked, only a certain percentage. Users may perceive the service as very slow, or as simply going “up and down.” This can be used to discourage users from using a service by making it seem unreliable, or encourage the use of alternative services, without revealing that blocking is occurring. (This can also be done for network and bandwidth management reasons at both the ISP or enterprise level.)

Both IP and Protocol-based blocking use devices that sit between the end-user and the content, and thus requires the blocking party (such as the user’s ISP) to have complete control over the connection between the end-user and the Internet. A user who is not “behind” the blocking device, or who uses technology such as a VPN that conceals the true destination of their traffic, will not be affected by this type of blocking.

Generally, IP blocking is a poor filtering technique that is not very effective, is difficult to maintain effectively, has a high level of unintended additional blockage, and is easily evaded by publishers who move content to new servers (with new IP addresses).

IP blocking also does not work when information providers use content delivery networks (CDNs), since the IP addresses of the information are highly dynamic and constantly changing.[4] CDNs also use the same IP address for many different customers and types of content, causing a high level of unintended service interruption.

Blocking technique	Speed of implementation	Cost	Blocking effectiveness	Difficulty of circumvention	Ease of administrative or judicial process	Integrity of network performance	Impact on legitimate services / law abiding consumers
IP address	✓✓	✓✓✓	✓	✓	✓	✓✓	✓
DNS*	✓✓✓	✓✓✓	✓✓✓	✓	✓✓✓	✓✓✓	✓
Shallow Packet Inspection	✓✓	✓✓✓	✓	✓	✓	✓	✓
Deep Packet Inspection	✓	✓	✓✓✓	✓✓	✓✓✓	✓	✓✓✓
URL	✓✓	✓✓	✓✓	✓✓	✓✓✓	✓✓	✓✓✓

✓ = Worst ✓✓✓ = Best

IP and protocol blocking work better when used to block specific applications, rather than specific content. For example, VPN traffic may be blocked by TCP/IP port and protocol blocks, combined with IP address blocks of known public VPN services. This is a common and highly effective technique.

IP blocking is also most effective when the content is hosted in a particular server in a specific data center, or a very specific set of files are of concern. IP-based blocking is not very effective for larger hosting services distributed across many data centers or which use content distribution networks (CDNs) to speed access.

2. Can the IP address be tracked, if the incognito mode is turned on?

Despite your browser history remaining hidden, incognito mode does not improve your security in any other way – your IP address will remain visible and the websites you visit will still be able to store data about your actions – if you accept the use of cookies, they will still be stored on your computer, and be able to gather information about your browsing habits etc. To reiterate – the incognito mode in a web browser is primarily used to hide your browsing history – It is not a complex security feature that can protect you from malicious attacks or attempts to retrieve your personal data.