नाम: _____ दिनांक: _____ अंक: _____

अपना IP पता कैसे छिपाएँ वर्कशीट

IP पते छिपाना, लोकेशन मास्किंग, प्रॉक्सी, Tor, और DNS/WebRTC लीक रोकना

VPN सीखने का अवलोकन

शिक्षार्थी
छात्र का दर्जा
नेटवर्क डिफ़ेंडर ट्रैक

सुरक्षित
कनेक्शन की स्थिति
डेटा पैकेट की ढाल बनाना

सक्रिय
लीक सुरक्षा
DNS और IPv6 लीक सुरक्षा

स्वागत है! यह गतिविधि पैकेट आपको वर्चुअल प्राइवेट नेटवर्क (VPN) के मूल सिद्धांतों से परिचित कराता है। आप जानेंगे कि एन्क्रिप्टेड टनल आपके डेटा को कैसे सुरक्षित करती हैं, नेटवर्क प्रोटोकॉल कैसे काम करते हैं, और गोपनीयता लीक की पहचान और उन्हें कम कैसे करें।

वर्कशीट चेकपॉइंट

- [ ] **भाग 1-4: VPN अवधारणाओं और प्रोटोकॉल में महारत हासिल करें।**
- [ ] **भाग 5-7: क्रॉसवर्ड और वर्ड सर्च पहेलियाँ हल करें।**
- [ ] **भाग 8-9: केस स्टडी और कूट संदेश की चुनौती हल करें।**
- [ ] **भाग 10: बुनियादी और उन्नत FAQ पेज देखें।**
- [ ] **भाग 11: 10 रोचक वास्तविक तथ्यों को जानें।**
- [ ] **अतिरिक्त: झटपट सोचें चुनौती।**

VPN.com VPN गाइड खोलें

URL: https://www.vpn.com/hi/vpn/

आपका VPN लर्निंग रोडमैप

- समझाएँ कि IP पते कैसे काम करते हैं और वे स्थान कैसे लीक करते हैं।
- नेटवर्क पते छिपाने के लिए प्रॉक्सी, Tor और VPN की तुलना करें।
- DNS और WebRTC लीक का पता लगाने और उन्हें रोकने के तरीकों की पहचान करें।
- समझें कि वेबसाइटें उपयोगकर्ताओं को उनके सार्वजनिक IP से कैसे ट्रैक करती हैं।
- IP सुरक्षा के लिए मल्टी-हॉप रूटिंग और एन्क्रिप्टेड टनल का मूल्यांकन करें।

IP सुरक्षा वर्कशीट के निर्देश

बहुविकल्पीय और सही/गलत प्रश्नों के उत्तर दें, शब्द बैंक की मदद से रिक्त स्थान भरें, परिभाषाओं का मिलान करें, और क्रॉसवर्ड तथा वर्ड सर्च पहेलियाँ हल करें। अपने ज्ञान को अपना IP पता छिपाने और लीक रोकने पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

अपना IP छिपाना (परिचय)

आपका IP एड्रेस एक डिजिटल डाक पता है जो आपकी भौतिक लोकेशन और नेटवर्क की आदतें उजागर करता है। अपना IP छिपाना ऑनलाइन ट्रैकिंग, टारगेट प्रोफ़ाइलिंग और जियोलोकेशन ब्लॉकिंग के विरुद्ध सुरक्षा की पहली पंक्ति है। अपना एड्रेस सुरक्षित रूप से छिपाना समझने से ऑनलाइन आपकी गोपनीयता की रक्षा में मदद मिलती है।

प्रत्येक चेकपॉइंट को ध्यान से पढ़ें और सही उत्तर चुनें या लिखें।

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1. डिवाइस का सार्वजनिक IP एड्रेस आपकी देखी गई वेबसाइटों को क्या बताता है?

- A. उपयोगकर्ता का क्रेडिट कार्ड नंबर
- B. आपकी अनुमानित लोकेशन और आपके ISP का नाम
- C. पूरी लोकल फ़ाइल डायरेक्टरी
- D. कीबोर्ड की भाषा सेटिंग्स

2. कौन-सी विधि आपका IP छिपाती है और पूरे सिस्टम का सारा ट्रैफ़िक एन्क्रिप्ट करती है?

- A. मानक वेब प्रॉक्सी
- B. अपनी ब्राउज़र कुकीज़ साफ़ करना
- C. वर्चुअल प्राइवेट नेटवर्क (VPN)
- D. अपने नेटिव फ़ायरवॉल को अक्षम करना

3. मुफ़्त वेब प्रॉक्सी इस्तेमाल करने की एक प्रमुख गोपनीयता सीमा क्या है?

- A. यह सार्वजनिक नेटवर्क पर डेटा ट्रैफ़िक को एन्क्रिप्ट नहीं करता
- B. इसके लिए बाहरी ऑपरेटिंग सिस्टम इंस्टॉल करना पड़ता है
- C. यह संयुक्त राज्य अमेरिका में पूरी तरह अवैध है
- D. इसके लिए समर्पित टेलीफ़ोन लाइन कनेक्शन चाहिए

4. Tor नेटवर्क उपयोगकर्ताओं को उच्च गुमनामी कैसे देता है?

- A. कनेक्शन की स्पीड बढ़ाकर
- B. ट्रैफ़िक को स्वयंसेवकों द्वारा चलाए जा रहे तीन रिले से गुज़ारकर
- C. आपका नाम एक वैश्विक डेटाबेस में पंजीकृत करके
- D. पहुँच केवल सरकारी एजेंसियों तक सीमित करके

5. DNS लीक क्या है?

- A. गलत पते पर ईमेल भेजने की त्रुटि
- B. जब DNS क्वेरी VPN टनल को दरकिनार करके ISP के पास जाती हैं
- C. स्थानीय राउटर की पावर सप्लाई में हार्डवेयर विफलता
- D. लोकल नेटवर्क अडैप्टर ड्राइवर का अपडेट

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न 6

6. प्रॉक्सी सर्वर VPN की तरह ही बैकग्राउंड OS ट्रैफ़िक को एन्क्रिप्ट करता है।

○ सही ○ गलत

7 प्रश्न 7

7. Tor रूटिंग अत्यंत सुरक्षित है, लेकिन नेटवर्क ब्राउज़िंग की गति घटाती है।

○ सही ○ गलत

8 प्रश्न 8

8. WebRTC लीक सक्रिय VPN सत्र के दौरान आपका असली IP उजागर कर सकते हैं।

○ सही ○ गलत

9 प्रश्न 9

9. VPN चालू होने और कोई लीक न होने पर आपका ISP नहीं देख सकता कि आप कौन-सी वेबसाइट देखते हैं।

○ सही ○ गलत

10 प्रश्न 10

10. अपना IP पता छिपाने से ब्राउज़र फ़िंगरप्रिंटिंग के ज़रिए होने वाली ट्रैकिंग रुक जाती है।

○ सही ○ गलत

चेकपॉइंट 3: मुख्य शब्द भरें

नीचे दिए गए प्रत्येक वाक्य को पढ़ें और रिक्त स्थान को वर्ड बैंक के सही शब्द से भरें।

1. सुरक्षित टनल को बायपास करके आपकी डोमेन क्वेरी उजागर करने वाली स्थिति _____ कहलाती है।
2. वीपीएन आपके ट्रैफ़िक को _____ ज़रिए कूट-रूप में बदलकर असली आईपी छिपाता है।
3. वेब _____ ब्राउज़र ट्रैफ़िक को मोड़ता है, लेकिन पैकेट पेलोड को एन्क्रिप्ट नहीं करता।
4. _____ नेटवर्क की बहु-परतीय एन्क्रिप्शन प्रणाली उच्च स्तर की गुमनामी देती है।
5. आपका सार्वजनिक _____ आपके टेलीकॉम प्रदाता द्वारा दिया जाता है और आपका क्षेत्र बताता है।
6. क्षेत्रीय मीडिया रोक से बचना _____ मास्किंग के ज़रिए संभव होता है।

शब्दावली शब्द-बैंक

आईएसपी ट्रैकिंग | आईपी पता | एन्क्रिप्शन | टोर | डीएनएस लीक | प्रॉक्सी | लोकेशन | WEBRTC API

अपने उत्तर यहाँ लिखें:

1.
2.
3.
4.
5.
6.

चेकपॉइंट 4: नेटवर्क अवधारणा मिलान

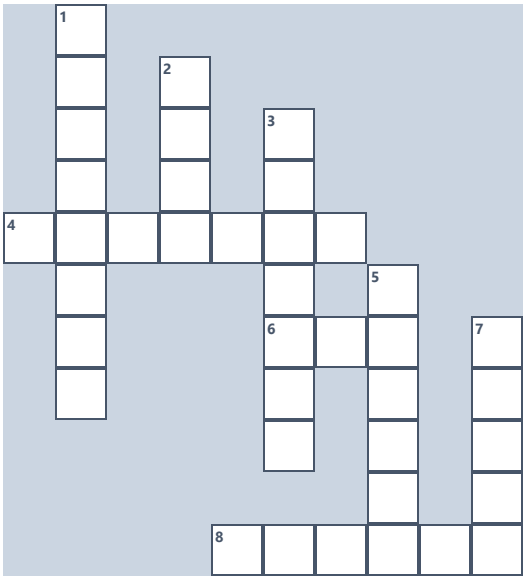
परिभाषा मिलान

बाईं ओर के प्रत्येक शब्दावली पद को दाईं ओर की सही परिभाषा से मिलाएँ; भरने योग्य इनपुट बॉक्स में संबंधित अक्षर (A-H) लिखें।

☐	**1. IP पता**	**A**	डिवाइस का सारा ट्रैफ़िक एन्क्रिप्ट करता है और उसे VPN सर्वर से गुज़ारता है।
☐	**2. VPN टनल**	**B**	डेटा को तीन स्वयंसेवी सर्वरों से गुज़ारता है और हर चरण पर परतें एन्क्रिप्ट करता है।
☐	**3. Tor नेटवर्क**	**C**	भौगोलिक ब्लॉक बायपास करने के लिए कनेक्शन को दूसरे देश के सर्वर से रूट करना।
☐	**4. वेब प्रॉक्सी**	**D**	इंटरनेट पर किसी डिवाइस इंटरफ़ेस की पहचान कराने वाला अद्वितीय संख्यात्मक लेबल।
☐	**5. DNS लीक**	**E**	सिस्टम एन्क्रिप्शन के बिना एप्लिकेशन लेयर पर ब्राउज़र ट्रैफ़िक को रीडायरेक्ट करता है।
☐	**6. WebRTC API**	**F**	आपकी टेलीकॉम कंपनी द्वारा बिना एन्क्रिप्ट किए इंटरनेट ट्रैफ़िक के गंतव्यों की लॉगिंग।
☐	**7. लोकेशन मास्किंग**	**G**	वे क्वेरी जो VPN टनल के बाहर रिज़ॉल्व होती हैं, जिससे देखे गए डोमेन ISP को दिख जाते हैं।
☐	**8. ISP ट्रैकिंग**	**H**	वॉइस/वीडियो के लिए ब्राउज़र सुविधा जो टनल को बायपास करके असली IP पते उजागर कर सकती है।

चेकपॉइंट 5: क्रॉसवर्ड पहेली

सक्रिय सफ़ेद खानों में अक्षर टाइप करके क्रॉसवर्ड पहेली हल करें। संख्याएँ नीचे दिए गए संकेतों से मेल खाती हैं।



बाएँ से दाएँ

4. आपके डिवाइस और वीपीएन सर्वर के बीच एन्क्रिप्टेड रास्ता (7)

6. वह कंप्यूटर जिससे वीपीएन जुड़ता है (3)

8. नेटवर्क पर किसी उपकरण का पहचान-पता (6)

ऊपर से नीचे

1. इंटरनेट प्रदाता द्वारा आपकी गतिविधि पर नज़र रखना (8)

2. जानकारी को कूट-भाषा में बदलने की प्रक्रिया (4)

3. वीपीएन सुरंग के बाहर डोमेन-अनुरोधों का उजागर हो जाना (7)

5. परतदार रूटिंग वाला गुमनाम ब्राउज़िंग तंत्र (6)

7. आपके डिवाइस को नेटवर्क पर मिलने वाली पहचान-संख्या (5)

चेकपॉइंट 5, वैकल्पिक: सुलभ क्रॉसवर्ड संकेत

स्क्रीन-रीडर और कीबोर्ड उपयोगकर्ता क्रॉसवर्ड के उत्तर सीधे नीचे दिए गए टेक्स्ट फ़ील्ड में टाइप कर सकते हैं।

बाएँ से दाएँ

4 बाएँ से दाएँ: आपके डिवाइस और वीपीएन सर्वर के बीच एन्क्रिप्टेड रास्ता (7 अक्षर):

6 बाएँ से दाएँ: वह कंप्यूटर जिससे वीपीएन जुड़ता है (3 अक्षर):

8 बाएँ से दाएँ: नेटवर्क पर किसी उपकरण का पहचान-पता (6 अक्षर):

ऊपर से नीचे

1 ऊपर से नीचे: इंटरनेट प्रदाता द्वारा आपकी गतिविधि पर नज़र रखना (8 अक्षर):

2 ऊपर से नीचे: जानकारी को कूट-भाषा में बदलने की प्रक्रिया (4 अक्षर):

3 ऊपर से नीचे: वीपीएन सुरंग के बाहर डोमेन-अनुरोधों का उजागर हो जाना (7 अक्षर):

5 ऊपर से नीचे: परतदार रूटिंग वाला गुमनाम ब्राउज़िंग तंत्र (6 अक्षर):

7 ऊपर से नीचे: आपके डिवाइस को नेटवर्क पर मिलने वाली पहचान-संख्या (5 अक्षर):

चेकपॉइंट 6: छिपे शब्द खोजें

नीचे दी गई ग्रिड में छिपे 8 प्रमुख शब्दावली शब्द खोजें। शब्द क्षैतिज, ऊर्ध्वाधर या तिरछे हो सकते हैं।

ड	रे	स	ख	नि	फ	ढ	मा	ना	का	रे	दे	सि	मी	क
पि	ता	ता	ति	ज	श	भ	ऊ	टो	अ	ऊ	ए	रि	वि	श
य	वि	प	व	वा	पा	ल	च	से	र	कि	य	घ	प	के
की	व	पी	ता	प	र्क	व	ट	ने	सि	ने	री	त	की	कि
सि	ना	ई	ने	पा	आ	ते	ण	ए	ता	सा	ट	मी	न	नी
क	ऋ	आ	ले	घ	ई	ति	वी	जि	ला	ए	जी	व	ले	ड
ली	ल	द	जे	घ	ए	के	च	पी	से	दे	री	ए	र्क	पी
स	उ	अ	जे	मि	स	घ	व	आ	ए	च	र	मी	च	ट
ए	थ	फ	ग	ना	पी	सी	का	ज	फ	न	नी	र्व	जी	ता
न	ठ	से	लि	ट	ट्रै	आ	इ	से	रा	के	ट	री	स	पा
ए	वा	सि	य	नि	किं	पि	ने	ख	के	न	वे	न	ऊ	ड
डी	नी	दे	दि	भ	ग	आ	नि	जे	प्श	वे	वे	ष	ल	ण
प	कि	से	य	ह	ह	ते	रा	न्क्रि	द	सा	सी	थ	जे	इ
मे	ला	ढ	पे	ऋ	वे	नी	ए	वे	उ	थ	ह	जे	त	य
मी	रे	मि	दि	ए	ह	जे	जा	ढ	वी	रा	दा	पी	व	ला

शब्दावली शब्द-सूची

आईपीपता, वीपीएनटनल, टोरनेटवर्क, डीएनएसलीक नेटवर्कपता, आईएसपीट्रैकिंग, सर्वर, एन्क्रिप्शन

चेकपॉइंट 6, वैकल्पिक: सुलभ शब्दावली मिलान

वर्ड सर्च के 8 शब्दावली पदों में से प्रत्येक को उसकी सही परिभाषा से मिलाएँ; खाली स्थान में अक्षर (A-H) लिखें।

शब्दावली के शब्द

- **A. आईपीपता**
- **B. वीपीएनटनल**
- **C. टोरनेटवर्क**
- **D. डीएनएसलीक**
- **E. आईएसपीट्रैकिंग**
- **F. सर्वर**
- **G. एन्क्रिप्शन**
- **H. नेटवर्कपता**

परिभाषाएँ और मिलान फ़ील्ड

1. _____ वीपीएन सुरंग के बाहर डोमेन-अनुरोधों का उजागर हो जाना।
2. _____ जानकारी को कूट-भाषा में बदलने की प्रक्रिया।
3. _____ वह कंप्यूटर जिससे वीपीएन जुड़ता है।
4. _____ आपके डिवाइस को नेटवर्क पर मिलने वाली पहचान-संख्या।
5. _____ परतदार रूटिंग वाला गुमनाम ब्राउज़िंग तंत्र।
6. _____ नेटवर्क पर किसी उपकरण का पहचान-पता।
7. _____ इंटरनेट प्रदाता द्वारा आपकी गतिविधि पर नज़र रखना।
8. _____ आपके डिवाइस और वीपीएन सर्वर के बीच एन्क्रिप्टेड रास्ता।

चेकपॉइंट 7: उलझे शब्दों की चुनौती

नीचे के अक्षरों को सुलझाकर VPN की प्रमुख अवधारणाएँ और शब्द पता करें। अपने उत्तर भरे जा सकने वाले इनपुट बॉक्स में लिखें।

1. प पी आ ता ई
2. र्क टो ने व ट र
3. स ई आ पी ट्रै ग कि ए
4. न प्शा ए न्क्रि
5. ट ल न ए वी न पी
6. ली न स डी ए क ए
7. र र्व स
8. व ता ने प र्क ट

अतिरिक्त गतिविधि: झटपट सोचें

हर श्रेणी में 3 उत्तर। जो सबसे पहले सूची भर दे, वह जीतता है।

1	यात्रा के दौरान VPN इस्तेमाल करने के कारण			
2	आपके जाने-पहचाने ब्राउज़र			
3	ऐसी चीज़ें जिन्हें VPN छिपा सकता है			
4	गोपनीयता से जुड़े शब्द			
5	इस वर्कशीट के वे शब्द जिन्हें आप याद रखना चाहते हैं			
6	ऐसी चीज़ें जिनका कोई वेबसाइट आपके IP से अंदाज़ा लगा सकती है			
7	IP एड्रेस में मौजूद अंक या चिह्न			
8	VPN के बारे में मिथक			
9	आपके जाने-पहचाने VPN सेवाएँ			
10	ऐसी चीज़ें जो आपका इंटरनेट प्रदाता देख सकता है			
11	अच्छे VPN प्रदाता के वादे			
12	ऐसी चीज़ें जो आपका असली IP लीक कर सकती हैं			
13	अपनी लोकेशन छिपाने के कारण			
14	अपना IP एड्रेस छिपाने के तरीके			
15	ऐसे डिवाइस जो VPN इस्तेमाल कर सकते हैं			

चेकपॉइंट 8: VPN केस स्टडी

नीचे दिए गए वास्तविक परिदृश्यों को हल करने के लिए सीखी हुई अवधारणाओं का उपयोग करें।

सारा (कॉफ़ी शॉप की छात्रा)

👱 "नमस्ते! मैं Coffee & Bytes में बैठा हूँ। यहाँ 'Free_Wi-Fi_No_Password' नाम का एक असुरक्षित सार्वजनिक नेटवर्क है। मैं अपने स्कूल के ईमेल में लॉग इन करना और अपना असाइनमेंट अपलोड करना चाहता हूँ, लेकिन मुझे हैकरों की चिंता है। VPN के बिना इस नेटवर्क का उपयोग करने के क्या जोखिम हैं, और VPN मेरे डेटा को कैसे सुरक्षित करता है?"

Alex (यात्री छात्र)

👱 "अरे नहीं! मैं एक प्रोजेक्ट के लिए विदेश यात्रा पर हूँ और अपने गृह देश के एक सर्वर पर होस्ट की गई जीव विज्ञान डॉक्यूमेंट्री देखने की कोशिश कर रहा हूँ। लेकिन साइट पर लिखा आ रहा है 'यह वीडियो आपकी वर्तमान लोकेशन में उपलब्ध नहीं है।' मुझे ब्लॉक क्यों किया जा रहा है, और VPN इसे देखने में कैसे मदद कर सकता है?"

चेकपॉइंट 9: कूट संदेश को डिकोड करें

अपनी IP मास्किंग की ट्रेनिंग पूरी करने के लिए, अपने डिजिटल निशान छिपाने के बारे में यह गुप्त संदेश डिक्रिप्ट करें।

अक्षर-से-संख्या एन्क्रिप्शन कुंजी

अ=1 आ=2 इ=3 ई=4 उ=5 ऊ=6 ऋ=7 ए=8 ऐ=9 ओ=10 औ=11 ऑ=12
क=13 ख=14 ग=15 घ=16 ङ=17 च=18 छ=19 ज=20 झ=21 ञ=22 ट=23 ठ=24
ड=25 ढ=26 ण=27 त=28 थ=29 द=30 ध=31 न=32 प=33 फ=34 ब=35 भ=36
म=37 य=38 र=39 ल=40 व=41 श=42 ष=43 स=44 ह=45 ा=46 ि=47 ी=48
ु=49 ू=50 ृ=51 े=52 ै=53 ो=54 ौ=55 ॉ=56 ं=57 ँ=58 ः=59 ़=60
्=61

1	33	32	46		33	28	46		19	47	33	48		33	61	39	27	46	40	48

44	52		19	49	33	46	8	58

डिकोड किया गया संदेश:

सुझाव: हर संख्या वर्णमाला में उस अक्षर की स्थिति दर्शाती है (जैसे 1 = अ, 2 = आ, 61 = ्)।

चेकपॉइंट 10: बुनियादी VPN FAQ (भाग A)

वर्चुअल प्राइवेट नेटवर्क के उपयोग के बारे में संभावित ग्राहकों के सबसे आम सवाल और जवाब देखें।

Q1: VPN क्या है और यह कैसे काम करता है?

वर्चुअल प्राइवेट नेटवर्क (VPN) आपके इंटरनेट कनेक्शन को एन्क्रिप्ट करता है और आपके ट्रैफ़िक को एक सुरक्षित रिमोट सर्वर से भेजता है। इससे आपका सार्वजनिक IP पता छिप जाता है और VPN टनल से गुज़रने वाले ट्रैफ़िक के बारे में स्थानीय नेटवर्क पर नज़र रखने वाले और आपका ISP जो देख सकते हैं, वह सीमित हो जाता है।

Q2: मुझे VPN का उपयोग क्यों करना चाहिए?

VPN आपकी डिजिटल गोपनीयता की रक्षा करता है, सार्वजनिक Wi-Fi नेटवर्क (जैसे कैफ़े या हवाई अड्डे) पर आपके कनेक्शन को सुरक्षित करता है, जब ISP एन्क्रिप्टेड ट्रैफ़िक का प्रकार पहचान नहीं पाता तब गतिविधि-आधारित थ्रॉटलिंग को घटा सकता है, वैश्विक सामग्री तक पहुँचने के लिए भौगोलिक प्रतिबंधों को बायपास करता है, और दूरस्थ कार्य के संसाधनों को सुरक्षित करने में मदद करता है।

Q3: क्या VPN मुझे ऑनलाइन पूरी तरह गुमनाम बना देता है?

नहीं। VPN आपका IP पता छिपाता है और ट्रैफ़िक एन्क्रिप्ट करता है, फिर भी आपको ब्राउज़र कुकी, सक्रिय खातों (जैसे Google या Facebook), ब्राउज़र फ़िंगरप्रिंटिंग, या VPN प्रदाता द्वारा आपका डेटा लॉग करने से ट्रैक किया जा सकता है।

Q4: क्या वेब प्रॉक्सी मेरा IP पता छिपाता है?

हाँ, लेकिन केवल उस ट्रैफ़िक के लिए जो उससे होकर भेजा जाए, आम तौर पर आपका ब्राउज़र। अधिकांश वेब प्रॉक्सी आपका डेटा एन्क्रिप्ट नहीं करते, इसलिए आपका ISP या नेटवर्क ऑपरेटर अब भी देख सकता है कि आप क्या भेजते और पाते हैं।

Q5: क्या अपना IP छिपाना क़ानूनी है?

कई देशों में हाँ, लेकिन कुछ देश VPN और IP पता छिपाने वाले अन्य उपकरणों पर रोक या प्रतिबंध लगाते हैं। अपना IP छिपाने से कोई अवैध कार्य कभी वैध नहीं हो जाता, इसलिए उपयोग से पहले स्थानीय कानून जाँच लें।

चेकपॉइंट 10: बुनियादी VPN FAQ (भाग B)

वर्चुअल प्राइवेट नेटवर्क के उपयोग के बारे में संभावित ग्राहकों के सबसे आम सवाल और जवाब देखें।

Q6: क्या Tor मेरा IP छिपाता है?

हाँ। Tor आपके ट्रैफ़िक को तीन स्वयंसेवी रिले (गार्ड, मिडिल और एग्ज़िट) से भेजता है, इसलिए वेबसाइटें एग्ज़िट रिले का एड्रेस देखती हैं, और कोई एक रिले यह नहीं जानता कि आप कौन हैं और कहाँ जा रहे हैं। [1]

Q7: मेरा IP क्या जानकारी उजागर करता है?

आपका सार्वजनिक IP आम तौर पर आपका ISP और अनुमानित लोकेशन, जैसे आपका देश या शहर, उजागर करता है। साइट इसका उपयोग आपकी विज़िट को आपस में जोड़ने और जियो-ब्लॉक लगाने के लिए भी कर सकती हैं।

Q8: मैं कैसे जाँचूँ कि यह छिपा हुआ है?

अपने VPN से जुड़ें, फिर IP-जाँच वाली साइट पर जाएँ और DNS तथा WebRTC लीक टेस्ट चलाएँ। दिखाए गए IP और DNS सर्वर VPN के होने चाहिए, आपके ISP के नहीं। अगर आपका असली IP दिखे, तो लीक सुरक्षा चालू करें।

Q9: क्या मैं अपने फ़ोन और स्मार्ट TV पर VPN उपयोग कर सकता हूँ?

हाँ। आधुनिक VPN प्रोवाइडर iOS, Android, macOS, Windows, Linux और स्मार्ट टीवी के लिए समर्पित ऐप्स, साथ ही आपके घर के नेटवर्क के सभी डिवाइस की सुरक्षा के लिए राउटर सेटअप देते हैं।

Q10: Kill Switch क्या है?

Kill Switch एक सुरक्षा सुविधा है जो VPN कनेक्शन टूटने पर आपके उपकरण को इंटरनेट से अपने-आप डिस्कनेक्ट कर देती है। इससे आपका बिना एन्क्रिप्शन वाला डेटा या असली IP पता लीक होने से बचता है।

चेकपॉइंट 10: उन्नत VPN FAQ (भाग C)

वर्चुअल प्राइवेट नेटवर्क और सुरक्षित टनलिंग प्रोटोकॉल के तकनीकी और संरचनात्मक पहलुओं को जानें।

Q1: IP पता छिपाने के बाद भी वेबसाइटें मुझे ट्रैक क्यों कर सकती हैं?

अपना IP छिपाने से ब्राउज़र फ़िंगरप्रिंटिंग नहीं रुकती। ट्रैकर आपके स्क्रीन रेज़ोल्यूशन, इंस्टॉल किए गए फ़ॉन्ट और ब्राउज़र सेटिंग जैसे विवरणों को मिलाकर एक पहचानकर्ता बना सकते हैं, और कुकी या साइन-इन किए गए खाते भी आपकी पहचान कर सकते हैं, इसलिए गोपनीयता-केंद्रित ब्राउज़र भी इस्तेमाल करें। [3]

Q2: डबल VPN या Multi-Hop रूटिंग क्या है?

मल्टी-हॉप आपके ट्रैफ़िक को क्रम में दो या अधिक VPN सर्वरों से रूट करता है। इससे एन्क्रिप्शन की दूसरी परत जुड़ती है और अगर एक सर्वर से समझौता हो जाए, तो आपके असली IP पते को दूसरे हॉप से छिपाए रखने में मदद मिलती है।

Q3: WebRTC लीकिंग क्या है और VPN इसे कैसे रोकता है?

WebRTC एक ब्राउज़र प्रोटोकॉल है जो VPN सक्रिय होने पर भी आपके असली लोकल और सार्वजनिक IP पते उजागर कर सकता है। प्रीमियम VPN अपने डेस्कटॉप/मोबाइल ऐप और ब्राउज़र एक्सटेंशन में WebRTC अनुरोधों को ब्लॉक या स्पूफ़ करते हैं।

Q4: क्या IPv6 ट्रैफ़िक मेरा असली IP पता लीक कर सकता है?

हाँ, यदि आपका VPN केवल IPv4 टनल करता है। तब आपका डिवाइस IPv6 ट्रैफ़िक टनल के बाहर भेज सकता है, जिससे आपके ISP द्वारा दिया गया एड्रेस उजागर हो जाता है। ऐसा VPN उपयोग करें जो IPv6 को टनल या ब्लॉक करता हो, और IPv6 लीक टेस्ट से इसकी पुष्टि करें।

Q5: ऑब्फ़स्केशन VPN ब्लॉक को कैसे बायपास करता है?

ऑब्फ़स्केशन (या "Stealth VPN") VPN ट्रैफ़िक पैकेट को ऐसा रूप देता है कि वे सामान्य HTTPS वेब ट्रैफ़िक (पोर्ट 443) जैसे दिखें। इससे सरकारों या स्कूल/ऑफ़िस नेटवर्क द्वारा VPN रोकने के लिए इस्तेमाल की जाने वाली डीप पैकेट इंस्पेक्शन (DPI) को पार करने में मदद मिलती है।

चेकपॉइंट 10: उन्नत VPN FAQ (भाग D)

वर्चुअल प्राइवेट नेटवर्क और सुरक्षित टनलिंग प्रोटोकॉल के तकनीकी और संरचनात्मक पहलुओं को जानें।

Q6: क्या स्प्लिट टनलिंग मेरा असली IP पता उजागर करती है?

हाँ, उन ऐप्स के लिए जिन्हें आप बाहर रखते हैं। टनल के बाहर भेजा गया ट्रैफ़िक आपके असली IP का उपयोग करता है, और RFC 8828 के अनुसार जब तक ब्राउज़र इसे सीमित न करे, WebRTC स्प्लिट-टनल VPN के नीचे ISP का एड्रेस उजागर कर सकता है। [2]

Q7: साझा IP पता क्या है और यह गोपनीयता में कैसे मदद करता है?

साझा IP के साथ, कई VPN उपयोगकर्ता एक ही समय में एक ही पते से ऑनलाइन दिखते हैं। इससे किसी वेबसाइट के लिए किसी एक विज़िट को आपसे जोड़ना, केवल आपके द्वारा इस्तेमाल किए जाने वाले डेडिकेटेड IP की तुलना में, काफ़ी कठिन हो जाता है।

Q8: क्या मेरा ISP देख सकता है कि मैं अपना IP छिपाने के लिए VPN उपयोग कर रहा हूँ?

आमतौर पर हाँ। आपका ISP देख सकता है कि आप VPN सर्वर के IP पते से जुड़ रहे हैं, कब जुड़ रहे हैं और कितना डेटा भेज रहे हैं, लेकिन आप कौन-सी वेबसाइट देखते हैं या एन्क्रिप्टेड टनल के भीतर क्या सामग्री है, यह नहीं देख सकता।

Q9: DNS Leak सुरक्षा क्या है?

DNS लीक सुरक्षा आपके डिवाइस को वेबसाइट लुकअप क्वेरी (DNS क्वेरी) अपने ISP के सर्वरों के बजाय VPN के निजी, एन्क्रिप्टेड DNS सर्वरों से भेजने के लिए बाध्य करती है। इससे आपका ISP यह ट्रैक नहीं कर पाता कि आप कौन-सी साइटें देखते हैं।

Q10: अपना IP छिपाने के लिए प्रॉक्सी बेहतर है या VPN?

VPN आमतौर पर बेहतर होता है। वह डिवाइस के हर ऐप के लिए आपका IP छिपाता है और ट्रैफ़िक को एन्क्रिप्ट करता है, जबकि वेब प्रॉक्सी आमतौर पर केवल ब्राउज़र को कवर करता है और अक्सर कोई एन्क्रिप्शन नहीं जोड़ता।

भाग 11: 10 रोचक VPN तथ्य और वास्तविक दुनिया की अंतर्दृष्टियाँ

VPN के इतिहास, बाज़ार और तकनीक से जुड़े इन बेहद उपयोगी, वास्तविक तथ्यों और अंतर्दृष्टियों को देखें।

1. पहला VPN प्रोटोकॉल

PPTP (Point-to-Point Tunneling Protocol), जो 1990 के दशक में Microsoft के नेतृत्व वाले समूह का शुरुआती VPN प्रोटोकॉल था, अब असुरक्षित माना जाता है, इसलिए आधुनिक VPN WireGuard या OpenVPN का उपयोग करते हैं।

2. फ़िंगरप्रिंटिंग

अपना IP छिपाने से ब्राउज़र फ़िंगरप्रिंटिंग नहीं रुकती, जो स्क्रीन रेज़ोल्यूशन और इंस्टॉल किए गए फ़ॉन्ट जैसे विवरणों से आपकी पहचान कर सकती है। [3]

3. WireGuard क्रांति

WireGuard में दक्षता के लिए डिज़ाइन किया गया अत्यंत सुव्यवस्थित कोडबेस है, जिससे पारंपरिक प्रोटोकॉल की तुलना में सुरक्षा कमज़ोरियों के लिए उसका ऑडिट करना आसान होता है।

4. WebRTC पते का उजागर होना

RFC 8828 चेतावनी देता है कि जब तक ब्राउज़र इसे सीमित न करे, WebRTC VPN का सार्वजनिक पता और वह ISP पता, दोनों खोज सकता है जिस पर VPN चल रहा है। [2]

5. 5-Eyes गठबंधन की उत्पत्ति

अमेरिका, ब्रिटेन, कनाडा, ऑस्ट्रेलिया और न्यूज़ीलैंड की Five Eyes खुफ़िया साझेदारी मित्र राष्ट्रों के बीच द्वितीय विश्व युद्ध के समय के सिग्नल्स-इंटेलिजेंस सहयोग से विकसित हुई।

6. डीप पैकेट इंस्पेक्शन

उन्नत फ़ायरवॉल नेटवर्क पैकेट मेटाडेटा का विश्लेषण करने और मानक VPN कनेक्शन की विशेषताओं को ब्लॉक करने के लिए Deep Packet Inspection (DPI) लगाते हैं।

7. TOR सर्किट का पुनः उपयोग

Tor एक ही सर्किट का लगभग दस मिनट उपयोग करता है और फिर नया बनाता है, जिससे आपकी ब्राउज़िंग गतिविधि को आपस में जोड़ना कठिन हो जाता है। [1]

8. विकेंद्रीकृत VPN

विकेंद्रीकृत VPN (dVPN) ट्रैफ़िक को पीयर-संचालित नोड के नेटवर्क में बाँटते हैं, जिससे किसी एक केंद्रीकृत प्रदाता पर निर्भरता घटती है।

9. TOR बनाम VPN गुमनामी

VPN ट्रैफ़िक को एक ही प्रदाता के ज़रिए टनल करता है, जबकि Tor (The Onion Router) गोपनीयता बढ़ाने के लिए ट्रैफ़िक को तीन स्वयंसेवी रिले (गार्ड, मिडिल, एग्ज़िट) से भेजता है। [1]

10. प्रॉक्सी बनाम VPN टनल

वेब प्रॉक्सी आपके ब्राउज़र ट्रैफ़िक के लिए साइट को दिखने वाला IP पता बदल देता है, लेकिन VPN के विपरीत वह आमतौर पर उस ट्रैफ़िक को एन्क्रिप्ट नहीं करता और आपके डिवाइस के अन्य ऐप्स को कवर नहीं करता। [5]

तकनीकी संदर्भ और स्रोत

इस वर्कशीट में उपयोग किए गए उद्धृत प्रकाशन, क्रिप्टोग्राफ़िक विनिर्देश और आधिकारिक दस्तावेज़ मानक।

शैक्षणिक और उद्योग संदर्भ

[1] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.
https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.
https://coveryourtracks.eff.org/learn

[4] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[5] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.
https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

उत्तर कुंजी: IP पता छिपाना, लोकेशन मास्किंग, प्रॉक्सी, Tor और DNS/WebRTC लीक रोकना

1 **प्रश्न 1** सही उत्तर: B

शिक्षण नोट

डिवाइस का सार्वजनिक IP एड्रेस आपकी देखी गई वेबसाइटों को क्या बताता है? → आपकी अनुमानित लोकेशन और आपके ISP का नाम

2 **VPN सिस्टम एन्क्रिप्शन** लेटेंसी सही उत्तर: C

शिक्षण नोट

केवल ब्राउज़र ट्रैफ़िक को रीडायरेक्ट करने वाली प्रॉक्सी के विपरीत, VPN पूरे सिस्टम में एन्क्रिप्टेड टनल बनाता है, जो बैकग्राउंड ऐप्लिकेशन, गेम और OS क्वेरी को सुरक्षित करता है। उद्धरण: Tor Project Relays, W3C WebRTC API।

3 **प्रॉक्सी में एन्क्रिप्शन की कमी** वाई-फ़ाई सुरक्षा सही उत्तर: A

शिक्षण नोट

वेब प्रॉक्सी केवल ब्राउज़र ट्रैफ़िक को आगे भेजते हैं और पैकेट पेलोड को एन्क्रिप्ट नहीं करते, यानी आपका नेटवर्क ऑपरेटर या ISP अब भी आपके कंटेंट ट्रैफ़िक का पता लगा सकता है। उद्धरण: IETF Proxy Vulnerabilities।

4 **प्रश्न 4** सही उत्तर: B

शिक्षण नोट

Tor नेटवर्क उपयोगकर्ताओं को उच्च गुमनामी कैसे देता है? → ट्रैफ़िक को स्वयंसेवकों द्वारा चलाए जा रहे तीन रिले से गुज़ारकर

5 **DNS टनल लीक** गोपनीयता सही उत्तर: B

शिक्षण नोट

DNS लीक तब होता है जब डोमेन नाम रेज़ोल्यूशन अनुरोध VPN टनल को बायपास करके सीधे आपके ISP के रेज़ॉल्वर तक पहुँच जाते हैं, जिससे देखे गए डोमेन के रिकॉर्ड उजागर हो जाते हैं। संदर्भ: DNSSEC Tunnel Testing, EFF Tracking Evasion।

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 **प्रॉक्सी सीमा का विवरण** IP मास्किंग — **सही उत्तर: गलत**

शिक्षण नोट

प्रॉक्सी एप्लिकेशन लेयर पर काम करते हैं और उनमें VPN टनल जैसा सिस्टम-व्यापी नेटवर्क ड्राइवर एकीकरण नहीं होता। उद्धरण: IETF Proxy Vulnerabilities.

7 **प्रश्न 7** — **सही उत्तर: सही**

शिक्षण नोट

परतदार एन्क्रिप्शन के साथ तीन स्वयंसेवी रिले से ट्रैफ़िक गुज़ारने से लेटेंसी बढ़ती है, इसलिए Tor आमतौर पर सीधे कनेक्शन से धीमा होता है।

8 **प्रश्न 8** — **सही उत्तर: सही**

शिक्षण नोट

WebRTC लोकल एड्रेस उजागर कर सकता है, और कुछ VPN सेटअप में टनल के नीचे ISP द्वारा दिया गया सार्वजनिक IP भी (RFC 8828)।

9 **प्रश्न 9** — **सही उत्तर: सही**

शिक्षण नोट

DNS या WebRTC लीक न होने पर ISP को VPN सर्वर तक केवल एन्क्रिप्टेड ट्रैफ़िक दिखता है, आपकी देखी गई साइटें नहीं।

10 **फ़िंगरप्रिंटिंग की सीमाएँ** नो-लॉग्स — **सही उत्तर: गलत**

शिक्षण नोट

फ़िंगरप्रिंटिंग डिवाइस कॉन्फ़िगरेशन मेट्रिक (स्क्रीन रिज़ॉल्यूशन, फ़ॉन्ट, प्लगइन) को निशाना बनाती है, जो IP छिपे होने पर भी दिखाई देते रहते हैं। उद्धरण: EFF Tracking Evasion।

शब्दावली कुंजियाँ और ग्रेडिंग रूब्रिक

शिक्षक के लिए ग्रेडिंग रूब्रिक: हर सही मिलान (कुल 8 अंक) और संदर्भ शब्द (कुल 6 अंक) के लिए 1 अंक दें।

चेकपॉइंट 4: उत्तर – अवधारणा मिलान

D 1. IP पता	A 2. VPN टनल	B 3. Tor नेटवर्क	E 4. वेब प्रॉक्सी
G 5. DNS लीक	H 6. WebRTC API	C 7. लोकेशन मास्किंग	F 8. ISP ट्रैकिंग

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 डीएनएस लीक	2 एन्क्रिप्शन	3 प्रॉक्सी	4 टोर
5 आईपी पता	6 लोकेशन		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

1 D – डीएनएसलीक	2 G – एन्क्रिप्शन	3 F – सर्वर	4 A – आईपीपता
5 C – टोरनेटवर्क	6 H – नेटवर्कपता	7 E – आईएसपीट्रैकिंग	8 B – वीपीएनटनल

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी IP पता, VPN टनल और Tor नेटवर्क को अपने शब्दों में समझा सकते हैं और हर एक का उदाहरण दे सकते हैं।

केस स्टडी:
विद्यार्थियों से कहें कि वे अपनी सिफ़ारिशें राय के बजाय वर्कशीट के तथ्यों पर आधारित करें।

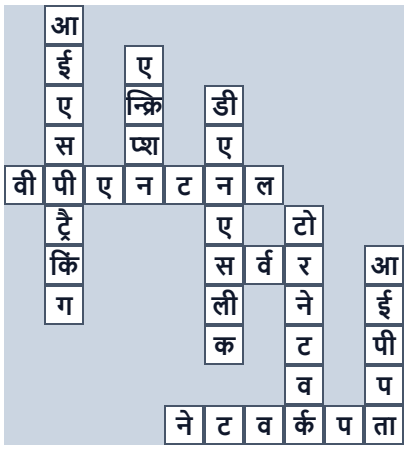
स्रोतों का मूल्यांकन:
विद्यार्थियों से वर्कशीट के स्रोतों में कम से कम एक कथन की पुष्टि करवाएँ और चर्चा करें कि आँकड़े, कीमतें और नियम समय के साथ क्यों बदल सकते हैं।

पहेलियों की कुंजियाँ और शिक्षक नोट

शब्द खोज समाधान

ड	रे	स	ख	नि	फ	ढ	मा	ना	का	रे	दे	सि	मी	क
पि	ता	ता	ति	ज	श	भ	ऊ	टो	अ	ऊ	ए	रि	वि	श
य	वि	प	व	वा	पा	ल	च	से	र	कि	य	घ	प	के
की	व	पी	ता	प	र्क	व	ट	ने	सि	ने	री	त	की	कि
सि	ना	ई	ने	पा	आ	ते	ण	ए	ता	सा	ट	मी	न	नी
क	ऋ	आ	ले	घ	ई	ति	वी	जि	ला	ए	जी	व	ले	ड
ली	ल	द	जे	घ	ए	के	च	पी	से	दे	री	ए	र्क	पी
स	उ	अ	जे	मि	स	घ	व	आ	ए	च	र	मी	च	ट
ए	थ	फ	ग	ना	पी	सी	का	ज	फ	न	नी	र्व	जी	ता
न	ठ	से	लि	ट	ट्रै	आ	इ	से	रा	के	ट	री	स	पा
ए	वा	सि	य	नि	किं	पि	ने	ख	के	न	वे	न	ऊ	ड
डी	नी	दे	दि	भ	ग	आ	नि	जे	प्श	वे	वे	ष	ल	ण
प	कि	से	य	ह	ह	ते	रा	न्क्रि	द	सा	सी	थ	जे	इ
मे	ला	ढ	पे	ऋ	वे	नी	ए	वे	उ	थ	ह	जे	त	य
मी	रे	मि	दि	ए	ह	जे	जा	ढ	वी	रा	दा	पी	व	ला

क्रॉसवर्ड समाधान



क्रॉसवर्ड समाधान के लिए शिक्षक गाइड

बाएँ से दाएँ

4 बाएँ से दाएँ: वीपीएनटनल आपके डिवाइस और वीपीएन सर्वर के बीच एन्क्रिप्टेड रास्ता (7 अक्षर)

6 बाएँ से दाएँ: सर्वर वह कंप्यूटर जिससे वीपीएन जुड़ता है (3 अक्षर)

8 बाएँ से दाएँ: नेटवर्कपता नेटवर्क पर किसी उपकरण का पहचान-पता (6 अक्षर)

ऊपर से नीचे

1 ऊपर से नीचे: आईएसपीट्रैकिंग इंटरनेट प्रदाता द्वारा आपकी गतिविधि पर नज़र रखना (8 अक्षर)

2 ऊपर से नीचे: एन्क्रिप्शन जानकारी को कूट-भाषा में बदलने की प्रक्रिया (4 अक्षर)

3 ऊपर से नीचे: डीएनएसलीक वीपीएन सुरंग के बाहर डोमेन-अनुरोधों का उजागर हो जाना (7 अक्षर)

5 ऊपर से नीचे: टोरनेटवर्क परतदार रूटिंग वाला गुमनाम ब्राउज़िंग तंत्र (6 अक्षर)

7 ऊपर से नीचे: आईपीपता आपके डिवाइस को नेटवर्क पर मिलने वाली पहचान-संख्या (5 अक्षर)

अक्षर-फेर शब्द और कूट संदेश हल कुंजी

शब्द-अनस्क्रैम्बल गतिविधि और Secret Cipher Challenge की ग्रेडिंग कुंजी।

शब्द अनस्क्रैम्बल कुंजी

1. पपीआताई — **आईपीपता**
2. र्कटोनेवटर — **टोरनेटवर्क**
3. सईआपीट्रैगकिंए — **आईएसपीट्रैकिंग**
4. नप्शएन्क्रि — **एन्क्रिप्शन**
5. टलनएवीनपी — **वीपीएनटनल**
6. लीनसडीएकए — **डीएनएसलीक**
7. रर्वस — **सर्वर**
8. वतानेपर्कट — **नेटवर्कपता**

गुप्त कूट चुनौती कुंजी

"अपना पता छिपी प्रणाली से छुपाएँ"

केस स्टडी के उत्तर

A परिदृश्य A: सार्वजनिक नेटवर्क की सुरक्षा

स्निफ़िंग और एन्क्रिप्शन | सारा की दुविधा

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- जोखिम: पैकेट स्निफ़िंग, डेटा इंटरसेप्शन और मैन-इन-द-मिडिल हमले। उसी कॉफ़ी शॉप नेटवर्क पर मौजूद कोई व्यक्ति उसके लॉगिन विवरण या होमवर्क फ़ाइल को कैप्चर कर सकता है।
- VPN सुरक्षा: नेटवर्क पैकेट पेलोड को एन्क्रिप्ट करती है, जिससे VPN के सही कॉन्फ़िगर होने पर इंटरसेप्ट किया गया टनल ट्रैफ़िक निष्क्रिय स्थानीय-नेटवर्क जासूसों के लिए अपठनीय हो जाता है।

B परिदृश्य B: ब्लॉक किए गए संसाधनों तक पहुँचना

जियो-ब्लॉकिंग और IP | Alex की दुविधा

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- ब्लॉक होने का कारण: स्ट्रीमिंग होस्ट जियो-ब्लॉकिंग का उपयोग करता है, जो यात्री के लोकल IP पते को उसके भौतिक देश से जोड़ता है और क्षेत्रीय लाइसेंसिंग के आधार पर उसे ब्लॉक कर देता है।
- VPN कैसे मदद करता है: ट्रैफ़िक को उसके गृह देश के सर्वर से गुज़ारकर उसकी असली लोकेशन छिपाना। साइट को गृह देश का IP दिखता है, जिससे एक्सेस मिल जाता है।