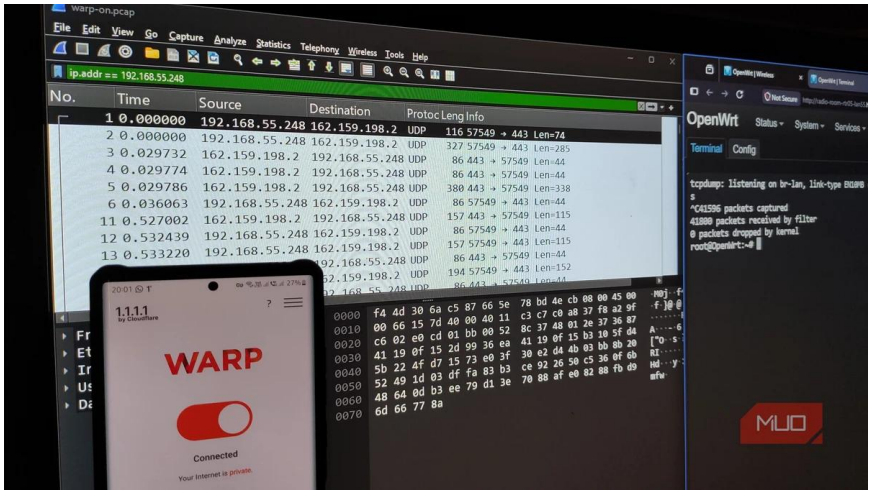
ভিপিএন ছাড়াই ফোনের ইন্টারনেট ট্রাফিক সুরক্ষিত রাখে যে অ্যাপ

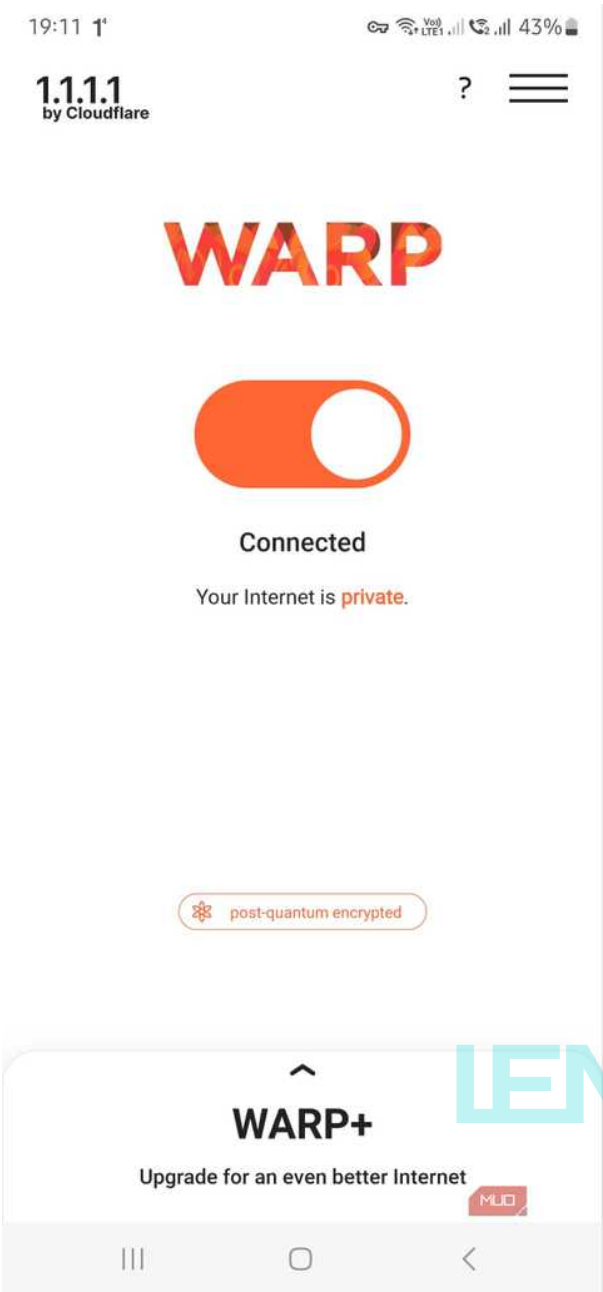


ছবি: সংগৃহীত

বাজারে থাকা বেশিরভাগ প্রাইভেসি অ্যাপের বৈশিষ্ট্য দেখলেই তাদের উদ্দেশ্য সম্পর্কে ধারণা পাওয়া যায়। সার্ভারের অবস্থান দেখানো মানচিত্র, বিভিন্ন ফিচারের তালিকা এবং অনেক ক্ষেত্রে মাসিক সাবস্ক্রিপশনের ব্যবস্থা থাকে এসব অ্যাপে। এর বিপরীতে Cloudflare WARP কিছুটা ভিন্নভাবে কাজ করে।

WARP ব্যবহারকারীর অবস্থান অন্য কোনো দেশে দেখানোর চেষ্টা করে না। এমনকি এটি ব্যবহারকারীকে বেনামিও করে না। এর মূল লক্ষ্য হলো ফোনের ইন্টারনেট ট্রাফিককে একটি এনক্রিপ্টেড রুটের মাধ্যমে পাঠানো, যাতে অবিশ্বস্ত নেটওয়ার্কে ইন্টারনেট ব্যবহারের সময় নিরাপত্তা বাড়ে।

ফ্রি 1.1.1.1 অ্যাপেও কোনো দেশের সার্ভার বেছে নেওয়ার জন্য মানচিত্র নেই। এটি এমন কোনো দাবি করে না যে ব্যবহারকারীর ফোন অন্য কোনো স্থানে অবস্থান করছে। একজন ব্যবহারকারী তার Samsung Galaxy Note 20 ফোনে অ্যাপটি ইনস্টল করে নিজের অবকাঠামোর মাধ্যমে ফোনের ট্রাফিক রাউট করেন এবং ফোন থেকে বের হওয়া ডেটা পর্যবেক্ষণ করেন।



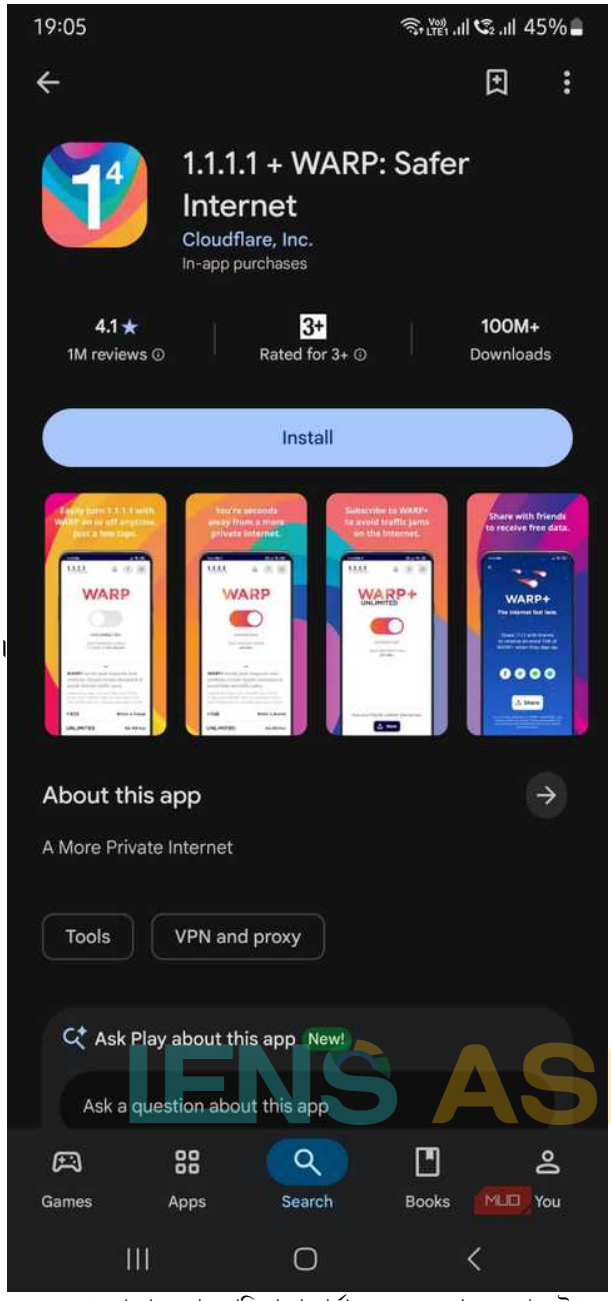
ফ্রি VPN অ্যাপ নিয়ে নানা ধরনের সংশয় থাকলেও Cloudflare-এর WARP পরীক্ষার পর ব্যবহারকারীর কাছে এটি ফোনে স্থায়ীভাবে চালু রাখার মতো একটি টুল হিসেবে বিবেচিত হয়েছে।

এক সুইচেই সেটআপ, তবে Android চেয়েছে VPN ব্যবহারের অনুমতি

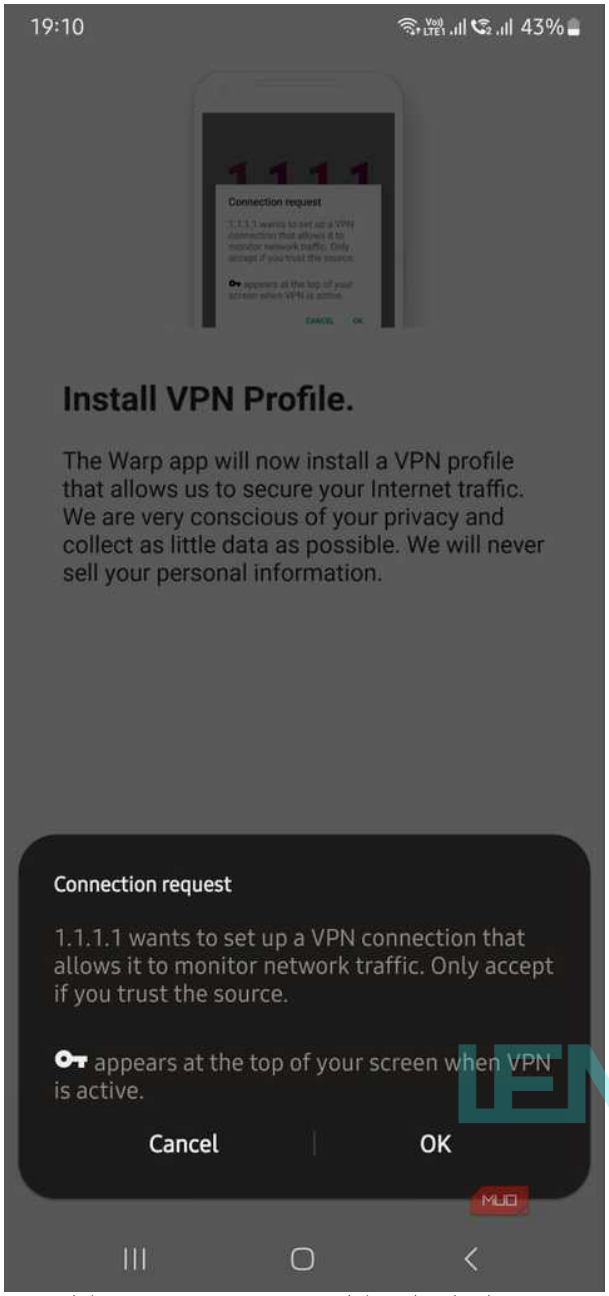
Cloudflare WARP অ্যাপটি Google Play Store এবং Apple App Store উভয় জায়গাতেই পাওয়া যায়। শুধু 1.1.1.1 লিখে সার্চ করলে একই ধরনের নামের একাধিক অ্যাপ দেখা যেতে পারে। Google Play Store-এ অ্যাপটির নাম 1.1.1.1 + WARP: Safer Internet এবং Apple App Store-এ 1.1.1.1 + WARP: Faster Internet। দুটির ডেভেলপারই Cloudflare, Inc.

অ্যাপটি ইনস্টল করতে কোনো অ্যাকাউন্ট খোলা বা লগইন করার প্রয়োজন হয় না। শর্তাবলি গ্রহণ করার পর একটি বড় টগল সুইচ দেখা যায়। সেখানে জানানো হয়, ব্যবহারকারীর

ইন্টারনেট সংযোগ বর্তমানে প্রাইভেট নয়।



সেটআপের জন্য মূলত ওই সুইচটিই চালু করতে হয়। কোনো দেশের তালিকা বা সার্ভার বেছে নেওয়ার ব্যবস্থা নেই। ব্যবহারকারীকে বেনামি করে দেওয়ার প্রতিশ্রুতিও নেই। সুইচটি চালু করার পর Android থেকে VPN কানেকশনের অনুমতি চাওয়া হয়। কারণ WARP ফোনের সিস্টেম-লেভেল ট্রাফিক অ্যাক্সেস নিয়ে বিভিন্ন অ্যাপের সংযোগ একটি এনক্রিপ্টেড টানেলের মাধ্যমে পাঠায়। অনুমতি দেওয়ার কয়েক সেকেন্ডের মধ্যেই সংযোগ সক্রিয় হয়ে যায় এবং ফোনের ওপরে একটি ছোট চাবির আইকন দেখা যায়।



অ্যাপের ইন্টারফেসে ফোন কানেক্টেড এবং ইন্টারনেট প্রাইভেট দেখালেও বাস্তবে ট্রাফিক কীভাবে যাচ্ছে, তা যাচাই করতে পরবর্তী সময়ে সংযোগ পরীক্ষা করা হয় এবং ফোন থেকে বের হওয়া ট্রাফিক ক্যাপচার করা হয়।

1.1.1.1 এবং WARP একই নয়

Cloudflare-এর অ্যাপে দুটি আলাদা মোড রয়েছে। একটির নাম 1.1.1.1, অন্যটি WARP। দেখতে কাছাকাছি হলেও দুটির কাজের পরিধি আলাদা।

1.1.1.1 মোড মূলত DNS কোয়েরি পরিচালনা করে। যেমন, makeuseof.com-এর মতো একটি সহজে বোঝা যায় এমন ওয়েব ঠিকানাকে IP ঠিকানায় রূপান্তরের জন্য যে DNS লুকআপ প্রয়োজন হয়, সেটি DNS over HTTPS (DoH) অথবা DNS over TLS (DoT) ব্যবহার করে এনক্রিপ্ট করা হয়। তবে ফোনের অন্যান্য ইন্টারনেট ট্রাফিক স্বাভাবিক পথেই চলাচল করে।

WARP এর চেয়ে আরও বিস্তৃতভাবে কাজ করে। এটি ফোনের বিভিন্ন অ্যাপের ইন্টারনেট ট্রাফিকের পাশাপাশি DNS কোয়েরিও সংগ্রহ করে এবং Cloudflare-এর বৈশ্বিক এজ নেটওয়ার্কের মাধ্যমে পাঠায়। WARP কানেকশনে সাধারণত MASQUE প্রযুক্তি ব্যবহার করা হয়। এর মাধ্যমে HTTP/3 এবং QUIC ব্যবহার করে UDP পোর্ট 443-এর ওপর এনক্যাপসুলেটেড ট্রাফিক বহন করা হয়।

Cloudflare-এর নেটওয়ার্কে পৌঁছানোর পর WARP-এর এনক্রিপ্টেড টানেল শেষ হয় এবং ডেটা ডিক্যাপসুলেট হয়ে ইন্টারনেটের চূড়ান্ত গন্তব্যের দিকে যায়। তবে অ্যাপগুলোর নিজস্ব HTTPS এনক্রিপশন তখনও সক্রিয় থাকে, ফলে গন্তব্যে পৌঁছানো পর্যন্ত সেই স্তরের সুরক্ষা বজায় থাকে।

শুধু DNS এনক্রিপ্ট করার সুবিধা খুব বেশি আকর্ষণীয় না হলেও WARP-এর সুবিধা হলো, প্রতিটি অ্যাপ আলাদাভাবে কনফিগার করার প্রয়োজন হয় না। ব্রাউজার, Play Store, আবহাওয়ার অ্যাপ কিংবা ইমেইল অ্যাপ একই সুরক্ষিত রুট ব্যবহার করতে পারে।

Cloudflare-এর one.one.one.one হেল্প পেজ থেকেও যাচাই করা যায় যে WARP এবং Cloudflare DNS রিজলভার সক্রিয় রয়েছে।

OpenWRT রাউটার দিয়ে ফোনের ট্রাফিক পরীক্ষা

অ্যাপের নিজস্ব তথ্যের পাশাপাশি WARP বাস্তবে কীভাবে কাজ করছে, তা ফোনের বাইরে থেকে পরীক্ষা করা হয়। এজন্য একটি বিদ্যমান OpenWRT রাউটারে নতুন একটি ওয়্যারলেস নেটওয়ার্ক তৈরি করে Android ফোনটিকে সেখানে যুক্ত করা হয়।

এর ফলে ফোন থেকে ইন্টারনেটের দিকে যাওয়া ডেটা প্যাকেটগুলো রাউটারের মধ্য দিয়ে যাওয়ার সময় পর্যবেক্ষণ করা সম্ভব হয়।

সংযোগের কাঠামো ছিল:

Starlink Wi-Fi → OpenWRT রাউটার → WARP-Test SSID → Galaxy Note 20

Android ফোনটি রাউটারের 192.168.55.0/24 নেটওয়ার্কে একটি IP ঠিকানা পায়। এতে ফোন এবং ইন্টারনেটের মাঝখানে OpenWRT অবস্থান করে। ফলে Samsung ফোনে কোনো পরিবর্তন না করেই br-lan দিয়ে যাওয়া প্যাকেটগুলো পর্যবেক্ষণ করা যায়।

প্রথমে Cloudflare-এর নিজস্ব যাচাই ব্যবস্থা ব্যবহার করা হয়। তাদের ট্রেস পেজে WARP-এর অবস্থা warp=off থেকে warp=on দেখা যায়। একই সঙ্গে one.one.one.one হেল্প পেজে নিশ্চিত হওয়া যায়, WARP এবং Cloudflare DNS দুটিই সক্রিয়।

তবে যেহেতু এগুলো Cloudflare-এর নিজের সেবা সম্পর্কে Cloudflare-এর দেওয়া তথ্য, তাই আরও নিরপেক্ষভাবে ট্রাফিক পর্যবেক্ষণের জন্য সরাসরি প্যাকেট ক্যাপচার করা হয়।

এ সময় "tcpdump" ব্যবহার করে ফোনের ট্রাফিক সংগ্রহ করা হয়। পরীক্ষার জন্য ফোনে আবহাওয়া ও ইমেইল অ্যাপ চালানো হয় এবং Wikipedia ব্রাউজ করা হয়, যাতে বিভিন্ন ধরনের ডেটা ট্রাফিক তৈরি হয়। পরে সংগৃহীত ডেটা Wireshark প্যাকেট অ্যানালাইজারে নিয়ে বিশ্লেষণ করা হয়।

পরীক্ষায় দেখা যায়, ফোন থেকে বিপুলসংখ্যক UDP প্যাকেট একটি Cloudflare টানেল এন্ডপয়েন্টের দিকে যাচ্ছে। Wireshark বাইরের ট্রান্সপোর্ট শনাক্ত করতে পারলেও অ্যাপের নির্দিষ্ট রিকোয়েস্টগুলো WARP-এর MASQUE টানেলের মধ্যে আর দৃশ্যমান ছিল না। ট্রাফিকটি QUIC এবং UDP 443-এর মাধ্যমে চলছিল।

শুধু প্যাকেট পড়তে না পারাকে এককভাবে এনক্রিপশনের চূড়ান্ত প্রমাণ বলা যায় না। কারণ HTTPS ট্রাফিকও মাঝপথে থাকা পর্যবেক্ষকের কাছে অপাঠ্য থাকে। তবে WARP-এর নির্বাচিত টানেল মোড, Android-এর সক্রিয় কানেকশন, warp=on ফলাফল এবং UDP স্ট্রিম—সবগুলো তথ্য একই দিক নির্দেশ করে।

WARP বেনামি করে না, তৈরি করে নিরাপদ একটি রুট

WARP-এর সবচেয়ে বড় সীমাবদ্ধতা হলো, এটি ব্যবহারকারীকে ইন্টারনেটে অদৃশ্য বা বেনামি করে না। Android-এ একই সময়ে একটি ডিভাইস-ওয়াইড টানেল চালানো যায়। ফলে WARP চালু থাকলে অন্য কোনো প্রাইভেসি অ্যাপ একইভাবে পাশাপাশি কাজ করতে পারে না; প্রয়োজনে সেটিকে WARP-এর জায়গা নিতে হবে।

এ ছাড়া WARP মূলত আস্থার জায়গাটি পরিবর্তন করে, পুরোপুরি সরিয়ে দেয় না। ক্যাফে, হোটেল, মোবাইল অপারেটর বা ISP দেখতে পারে যে কোনো ফোন Cloudflare-এর সঙ্গে এনক্রিপ্টেড ট্রাফিক আদান-প্রদান করছে। তবে WARP টানেলের ভেতরে থাকা নির্দিষ্ট রিকোয়েস্টগুলো তারা সরাসরি দেখতে পারে না। Cloudflare টানেলের অপর প্রান্তে থেকে ট্রাফিক গ্রহণ করে এবং সেখান থেকে সেটিকে ইন্টারনেটের গন্তব্যে পাঠায়।

WARP ব্যবহারকারীর পরিচয় গোপন রাখে না, জিও-রেস্ট্রিকশন বা ভৌগোলিক সীমাবদ্ধতা দূর করে না এবং ব্যবহারকারীকে নিজের হোম নেটওয়ার্কে ফিরে যাওয়ার সুযোগও দেয় না।

তবে যারা শুধু পাবলিক Wi-Fi বা অবিশ্বস্ত নেটওয়ার্কে তুলনামূলক নিরাপদভাবে ইন্টারনেট ব্যবহার করতে চান, তাদের জন্য এসব সীমাবদ্ধতা বড় সমস্যা নাও হতে পারে। কারণ WARP-এর মূল উদ্দেশ্য অন্য দেশে অবস্থান করছে এমন দেখানো নয়; বরং পাবলিক Wi-Fi অপারেটর বা ISP যেন ব্যবহারকারীর প্রতিটি অনলাইন রিকোয়েস্ট সরাসরি দেখতে না পারে, সেটি নিশ্চিত করা।

একটি সাধারণ টগল সুইচ চালু করেই WARP সেই এনক্রিপ্টেড রুট তৈরি করে। এর জন্য Cloudflare কোনো অ্যাকাউন্ট বা বাধ্যতামূলক সাবস্ক্রিপশনও চায় না।

হোম নেটওয়ার্কে প্রবেশের মতো নির্দিষ্ট প্রয়োজনে আলাদা টুলের প্রয়োজন হতে পারে। কিন্তু যেসব নেটওয়ার্ককে পুরোপুরি বিশ্বাস করা যায় না, সেখানে ইন্টারনেট ট্রাফিকের জন্য অতিরিক্ত সুরক্ষিত রুট তৈরিতে WARP কার্যকর একটি বিকল্প হতে পারে।

এই সহজ সেটআপ এবং পরীক্ষায় পাওয়া সুরক্ষার ফলাফলই WARP-কে Android ফোনে স্থায়ীভাবে ব্যবহার করার মতো একটি টুলে পরিণত করেছে।

সূত্র: MakeUseOf