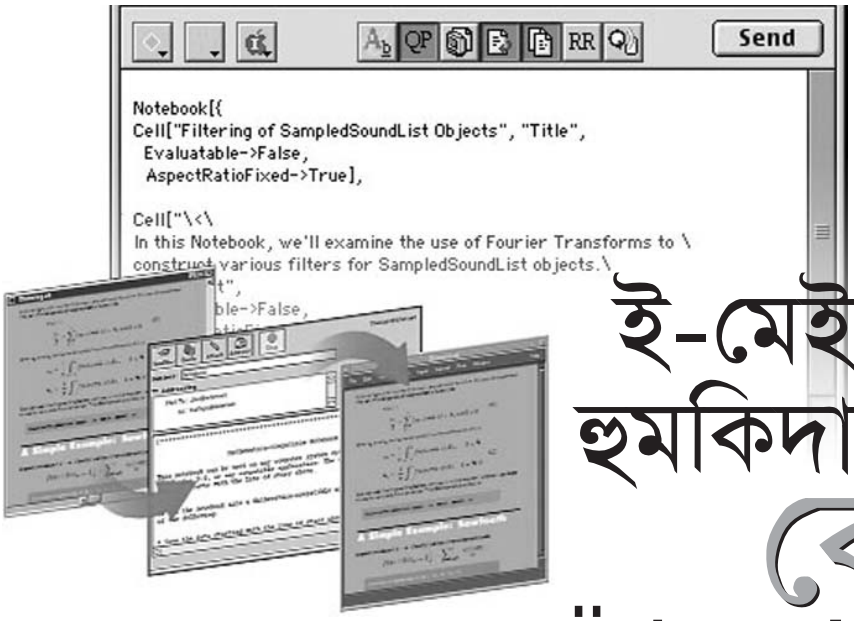


ই-মেইলে হুমকিদাতা কে

mÜvb Ki“b

লিখেছেন **আনোয়ার আসাদ**

এমন অনেক ই-মেইল আসে যা খুবই বিরক্তিকর। অপ্রয়োজনীয় মেইলের ভিড়ে প্রয়োজনীয় মেইল খুঁজে বের করা এক বিশাল ঝামেলা এবং সময় সাপেক্ষ। আবার মেইলের মাধ্যমে হুমকিও আসে। এসব কারণে মেইলটির অন্য প্রান্তের ব্যক্তিটি সম্পর্কে জানা অনেক সময় হয়ে পরে গুরুত্বপূর্ণ। বাংলাদেশ ইন্টারনেট সার্ভিস তথা আইএসপি সার্ভিসের সঙ্গে জড়িত প্রত্যেকের মাঝে একটি সমন্বয় গড়ে তুলতে পারলে এ ধরনের মেইল সন্ত্রাসীদের খুঁজে বের করা সহজ হতো। এ ক্ষেত্রে চীন একটি উজ্জ্বল দৃষ্টান্ত তৈরি করেছে। চীনে প্রতিটি সাইবার ক্যাফে তথা ইন্টারনেট ব্যবহারকারীর কার্যক্রম পর্যবেক্ষণ করা হয়। শুধু কি ইন্টারনেট? মোবাইল থেকে পাঠানো মেসেজও প্রেরকের কাছে পৌঁছার আগে সরকারি অফিস ঘুরে যায়। আর এ সবই সম্ভব হয়েছে তথ্য প্রযুক্তিকে নিয়ে সুনির্দিষ্ট অবকাঠামো গড়ে তোলার ফলে। আগাম ভবিষ্যতে তথ্য সন্ত্রাসীদের বিরুদ্ধে লড়তে হবে, তাই ভাবতে হবে এখনই। তবে ব্যক্তিগতভাবে কোনো মেইল প্রেরককে প্রাথমিকভাবে খুঁজে বের করা যায় কিভাবে তাই নিয়ে এই প্রতিবেদন।

একটি ই-মেইল হতে পারে প্রেরকটি রয়েছে ঢাকায় অথবা বাংলাদেশের বাইরে অর্থাৎ অন্য কোনো দেশে। এখন আপনার ইচ্ছে হলো জানার যে, সে এই মেইলটি কোথা থেকে করেছে- বাসা, সাইবার ক্যাফে, কলেজ-ভার্সিটি, অফিস অথবা অন্য কোনো জায়গা। কিভাবে জানবেন?

সাধারণত যখন আমরা কোনো একটি ই-মেইল পেয়ে থাকি তখন শুধু ই-মেইলে কি লেখা আছে তাই দেখতে পাই। কিন্তু প্রতিটি ই-মেইলে আরো কিছু তথ্য থাকে যেগুলো দেখা যায় না। এই তথ্যগুলো থাকে ই-মেইল। হেডার নামক ফিল্ডের অধীনে। নিচে ই-মেইল হেডার ফিল্ডসহ একটি ই-মেইলের উদাহরণ দেয়া হলো :

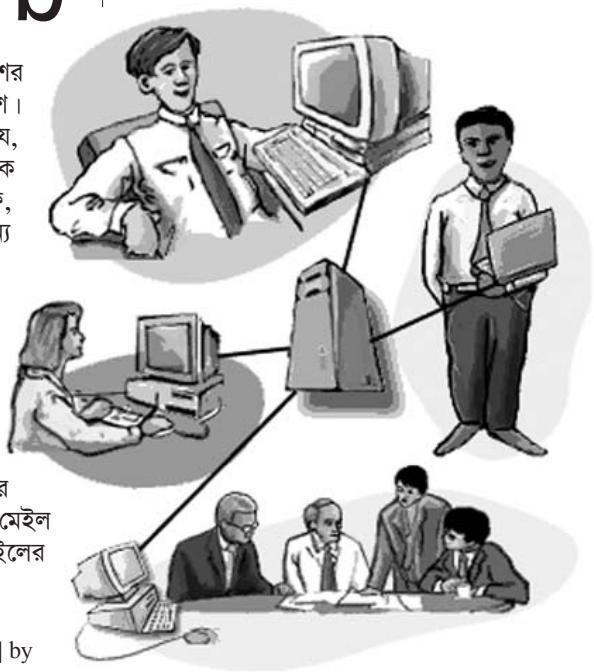
Return-Path : <x@yahoo.com>
Received : from [203.127.89.138] by any.com
(Microsoft Exchange Internet Mail Service Version 5.5.2448.0) with SMTP id Ex4TRA; Sat, 13 APR 2004 05:52:35+0600
From : x@yahoo.com
Reply- To : x@yahoo.com
To : y@yahoo.com
Date : Sat, 13 APR 2004 06:31:21+0600
Subject : Reply Urgent
X-Mailer : mPOP Web-Mail 2.19
Mime-Version : 1.0
Content-Type : text/plain; charest 'us-ascii'
Message-ID : (auto-002963@any.com)
X-Mozilla-Status : 8003
X-UIDL : 1169

Dear A.
How are You?.....
Your's B

এখন আপনি যদি চান যে আপনার ই-মেইলগুলো হেডারসের তথ্য দেখবেন, তাহলে যা করবেন তা হলো :

ইয়াহু ব্যবহাকারীরা :

Option-এ ক্লিক করুন → Mail Preferences ক্লিক করুন → Show Headers-এ ক্লিক করুন → 'All' ক্লিক করুন → 'Save'-এ ক্লিক করুন।



হটমেইল ব্যবহারকারীরা

Option → 'Additional Options'-এর অধীনে Mail Display Headings ক্লিক করুন → Message Headers → 'Full' → OK করুন।

আউটলুক এক্সপ্রেস ব্যবহারকারীরা

আউটলুকের ইনবক্সে থাকা মেইল মেসেজটি সিলেক্ট করে মাউসের রাইট বাটনে ক্লিক করে Properties সিলেক্ট করুন। সেখান থেকে Details অপশনটি সিলেক্ট করুন।

সাধারণত হেডারে যেসব তথ্য থাকে তার মাধ্যমে কোনো কম্পিউটার অথবা ব্যবহারকারীকে শনাক্ত করা যায়। তবে ব্যবহারকারীকে শনাক্ত করা খুব একটা সহজ কাজ নয়; কারণ, কোনো ব্যবহারকারী তার তৈরিকৃত ই-মেইল ঠিকানাটিতে ভুল তথ্যও দিতে পারে। যা হোক, হেডারের যে তথ্যটি কোনো একজন ই-মেইল প্রেরক অথবা তার ব্যবহারকৃত কম্পিউটার খুঁজে বের করার জন্য ব্যবহৃত হয় সেটি হলো Received.

তাহলে আসুন আমরা দেখি কিভাবে আমরা উপরের ই-মেইলটির Received-এর তথ্যগুলোর সাহায্যে একটি কম্পিউটারকে অর্থাৎ কোথা থেকে ই-মেইলটি করা হয়েছে তা খুঁজে পেতে পারি।

Received : from [203.127.89.138] by any.com

(Microsoft Exchange Internet mail Service Version 5.5.2448.0) with SMTP id Ex4Tra ; Eat, 13 APR 2004 05:52:35+0600

ই-মেইলটি 203.127.89.138 থেকে any.com, এই সাইটের মেইল সার্ভারে এসেছে। SMTP (Simple Mail Transfer Protocol-এর সাহায্যে) হলো একটি ল্যাঙ্গুয়েজ বা ভাষা যা যেকোনো ই-মেইল মেসেজ পাঠানোর জন্য ইন্টারনেট ই-মেইল সফটওয়্যারগুলো ব্যবহার করে। যা হোক, এই মেইলটি any.com গ্রহণ করেছে Saturday অর্থাৎ শনিবারে এবং তারিখ হলো এপ্রিলের ১৩, ২০০৪ সালে ০৫:৫২:৩৫ ঢাকা সময়ে (চার-ডিজিট নম্বর '+0600' বোঝায় যে এটি GMT Green with Mean Time থেকে কত আগে বা পরে। এখানে +0600 হলো, GMT-এর সঙ্গে ৬ ঘন্টা যোগ করার পর যে সময় হবে সেটি। আর ৬ ঘন্টা যোগ করতে হয় ঢাকার সময়ের সঙ্গে। আপনারা যদি চান তবে সহজেই এটি করতে পারেন। মাউসের সাহায্যে ডেস্কটপের যেখানে সময় দেখায় তার ওপর ডাবল ক্লিক করুন। এবার Time Zone সিলেক্ট করুন। (GMT +06:00)-এ মাউস দিয়ে সিলেক্ট করুন। দেখবেন পাশে লেখা আছে Dhaka। অর্থাৎ এতে বোঝা যায় যে, মেইলটি ঢাকা থেকে করা হয়েছে। + 0600 না থেকে যদি -1000 থাকতো, তবে বোঝা যেত মেইলটি করা হয়েছে Hawaii দ্বীপপুঞ্জ থেকে)।

203.127.89.138 হলো একটি আইপি ঠিকানা (IP Address)। IP হলো Internet Protocol-এর সংক্ষিপ্ত রূপ। সাধারণত ইন্টারনেট নেটওয়ার্কের সঙ্গে যুক্ত হবার জন্য প্রতিটি কম্পিউটারের একটি IP ঠিকানা থাকতে হয়। আর একটি কম্পিউটারের আইপি ঠিকানার সঙ্গে অন্য কম্পিউটারের আইপি ঠিকানা কখনোই মিলবে না। অনেকটা

আমাদের বাসার টেলিফোন নাম্বারের মতো।

প্রতিষ্ঠানসমূহ যারা একটি অথবা একের অধিক কম্পিউটার ব্যবহার করে তারা এই আইপি ঠিকানা কিনে নেয়। এ আইপি ঠিকানা তখন ইন্টারনেটের বিভিন্ন রেজিস্ট্রির একটিতে সংরক্ষণ করা হয়।

সাধারণত তিনটি প্রধান রেজিস্ট্রি রয়েছে যেগুলো সমগ্র পৃথিবীর বিভিন্ন অংশ কাভার করে। The American Registry ov Internet Numbers (ARIN-www arin. net) তারা আমেরিকা এবং সাব-সাহারান আফ্রিকার জন্য আইপি ঠিকানা দেয়; Asia Pacific Network Information Center (APNIC-www.apnic.net), তারা এশিয়ায় আইপি ঠিকানায় দেয়; Reseaux IP Europeens (RIPE NCC-www.ripe.net) কাভার করে ইউরোপ। এখন কোনো একটি আইপি অ্যাড্রেস তা কোন প্রতিষ্ঠানের জানার জন্য এসব সাইটের ডাটাবেজ বা WHOIS নামে পরিচিত, তাতে খুঁজে দেখতে হবে।

এখন 203. 127. 89. 138 এই আইপিটি যেহেতু ঢাকার (এশিয়ার অন্তর্গত) কোনো একটি প্রতিষ্ঠানের, এর জন্য আমরা যাবো APNIC-এর সাইটে, নিচের ঠিকানা আমাদের এক্সপ্লোরারে টাইপ করার মাধ্যমে,

http://www.apnic.net/Whois/

অতঃপর সার্চ বক্সে 203.127.89.138 টাইপ করে সার্চ করলে আমরা পেয়ে যাবো এটি কোন দাতা জন্য। ধরি, সার্চ করার পর আমরা পেলাম যে এটি ঢাকার একটি ইন্টারনেট সার্ভিস দাতা প্রতিষ্ঠানের (ISP-Internet Service Provider) কোম্পানির।

এখন যা করতে হবে তা হলো, এই ISP কোম্পানির সঙ্গে যোগাযোগ করে জানতে হবে ঐ সময়ে অর্থাৎ ০৫:৫২:৩৫ সময়ে ঐ দিনে কে এই আইপি ব্যবহার করেছে। প্রতিটি ISP তাদের ব্যবহারকারী এবং মেসেজগুলোসহ প্রভৃতি বিষয় সম্বন্ধে যাবতীয় তথ্য সংরক্ষণ করে, যাকে বলা হয় Log. এখন আমরা যদি ই-মেইলের উপরের হেডারের তথ্য ISP-কে দিতে পারি তবে তারা সেই Log চেক করে বলে দিতে পারবে কোন কম্পিউটার অথবা কে সেই ব্যবহারকারী।

মনে করুন, উপরের হেডারসহ আইপি দেবার পর ISP কোম্পানি একটি রিপোর্ট করল যে, এটি একটি সাইবার ক্যাফের কম্পিউটারের আইপি, সে ক্ষেত্রে আমরা শুধু কম্পিউটারটি শনাক্ত করতে পারবো, ব্যবহারকারীকে নয়।

অনেক সময় একটি প্রতিষ্ঠান ISP কোম্পানির কাছ থেকে আইপি নেবার পর, যে কম্পিউটারের জন্য আইপি নিয়েছে সেটিকে সার্ভার হিসেবে ব্যবহার করে আরও কম্পিউটার ক্লায়েন্ট হিসেবে যোগ করে। সেই সার্ভারের কম্পিউটার তখন সেই ক্লায়েন্টদের ডায়নামিক আইপি প্রদান করে। এর ফলে আপনি যে কোনো ক্লায়েন্ট কম্পিউটার থেকে ব্রাউজ করলে বা ই-মেইল পাঠালে তা সার্ভারের আইপি প্রদর্শন করে। এ ক্ষেত্রে কোন কম্পিউটার ব্যবহার করে ই-মেইল পাঠানো হয়েছে তা জানা কষ্টকর। শুধু জানা যাবে সেই প্রতিষ্ঠান কোনটি। ই-মেইল ট্রেসিংয়ের জন্য ইন্টারনেটে বিভিন্ন ধরনের সফটওয়্যার (Traceroute, Mail Trackerpro) পাওয়া যায়।