

## গেইনিং একসেস

### গেইনিং একসেস

গেইনিং একসেস হলো আপনি যে তথ্যগুলো সংগ্রহ করেছেন সেই তথ্যগুলো দিয়ে সিস্টেম এ প্রবেশ করা।

বিভিন্নভাবে গেইনিং একসেস করা যায়-

১. সিস্টেম হ্যাকিং
২. সোশ্যাল ইঞ্জিনিয়ারিং
৩. DDoS আক্রমণ
৪. ওয়েবসার্ভার আক্রমণ
৫. ওয়্যারলেস আক্রমণ
৬. মোবাইল প্ল্যাটফর্ম
৭. ক্রিপ্টোগ্রাফি

নিচে আমরা যেসবভাবে গেইনিং একসেস করা যায় তার প্রত্যেকটি উপায় বিস্তারিত আলোচনা করবো-

## সিস্টেম হ্যাকিং

যেভাবে সিস্টেম হ্যাকিং করা হয়-

১. ক্র্যাকিং পাসওয়ার্ড
২. প্রিভিলেজ এস্কালাশন
৩. এক্সেকিউটিং অ্যাপ্লিকেশনস
৪. হিডিং ডাটা

ক্র্যাকিং পাসওয়ার্ড

ক্র্যাকিং পাসওয়ার্ড হলো পাসওয়ার্ড সংগ্রহ করা। আমরা যেভাবে পাসওয়ার্ড সংগ্রহ করতে পারি সেগুলোর মধ্যে উল্লেখযোগ্য হলো

- ডিফল্ট পাসওয়ার্ড সংগ্রহ করা
- সাধারণত আমরা যে পাসওয়ার্ডগুলো ব্যবহার করি
- পাসওয়ার্ড জেনারেটর ব্যবহার করা
- ডাম্পস্টার ডাইভিং এর মাধ্যমে
- সোশ্যাল ইঞ্জিনিয়ারিং করে ইত্যাদি

ডিফল্ট পাসওয়ার্ড সংগ্রহ করা

ডিফল্ট পাসওয়ার্ড আমরা বিভিন্ন ওয়েবসাইট থেকেও সংগ্রহ করতে পারি। এমনটি একটি উল্লেখযোগ্য সাইট হলো-( [www.routerpasswords.com](http://www.routerpasswords.com))

Default Router Passwords - The i x

Not secure | www.routerpasswords.com

Tasks Keep Security Drive CEH Mikrotik M Translate Rewriter LT Check spell PasswordG Slack 20 21 Devices

RouterPasswords.com

6.35/11kv overhead cable  
If you need it, please contact us: info@zmacable.com, zmacable.com

OPEN

Welcome to the internet's largest and most updated default router passwords database.

Select Router Manufacturer:

CISCO

Find Password

Manufacturer	Model	Protocol	Username	Password
CISCO	CACHE ENGINE	CONSOLE	admin	diamond
CISCO	CONFIGMAKER		cmaker	cmaker
CISCO	CNR Rev. ALL	CNR GUI	admin	changeme
CISCO	NETRANGER/SECURE IDS	MULTI	netrangr	attack
CISCO	BBSM Rev. 5.0 AND 5.1	TELNET OR NAMED PIPES	bbsd-client	changeme2
CISCO	BBSD MSDE CLIENT Rev. 5.0 AND 5.1	TELNET OR NAMED PIPES	bbsd-client	NULL
CISCO	BBSM ADMINISTRATOR Rev. 5.0 AND 5.1	MULTI	Administrator	changeme
CISCO	NETRANGER/SECURE IDS Rev. 3.0(5)S17	MULTI	root	attack
CISCO	BBSM MSDE ADMINISTRATOR Rev. 5.0 AND 5.1	IP AND NAMED PIPES	sa	(none)
CISCO	CATALYST 4000/5000/6000 Rev. ALL	SNMP	(none)	public/private/secret
CISCO	PIX FIREWALL	TELNET	(none)	cisco
CISCO	VPN CONCENTRATOR 3000 SERIES Rev. 3	MULTI	admin	admin
CISCO	CONTENT ENGINE	TELNET	admin	default
CISCO	AP1200 Rev. IOS	MULTI	Cisco	Cisco

সাধারণত আমরা যে পাসওয়ার্ডগুলো ব্যবহার করি

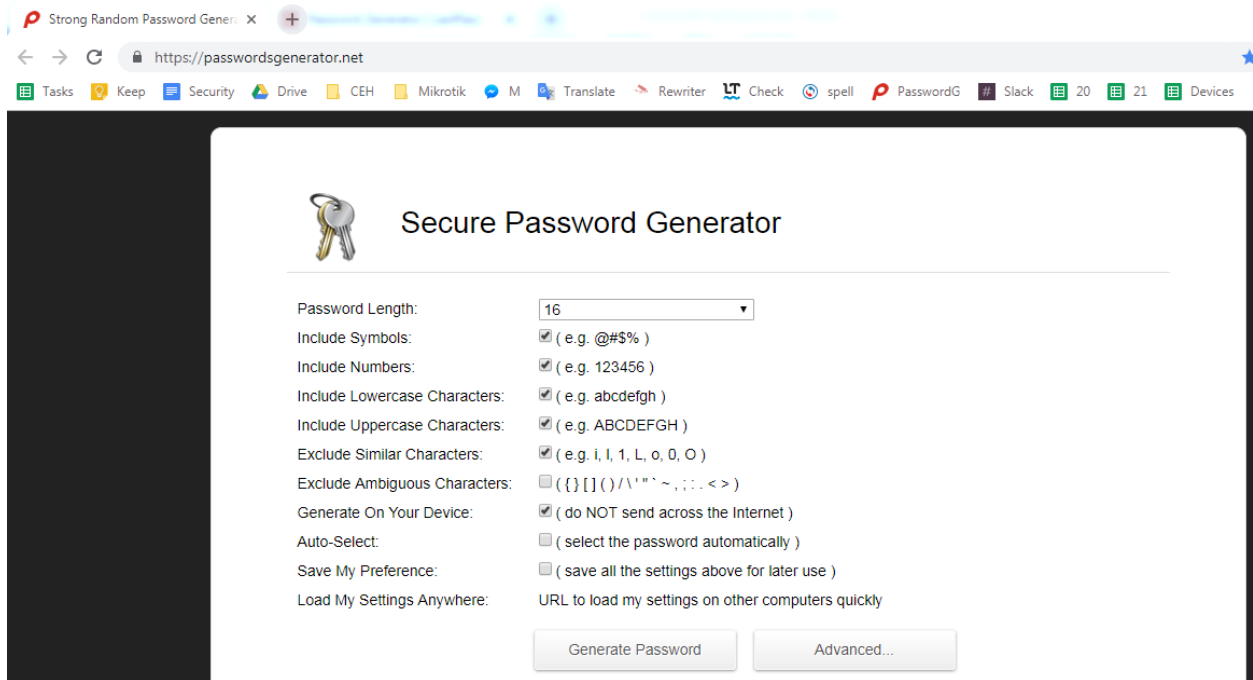
সাধারণত আমরা যে পাসওয়ার্ডগুলো ব্যবহার করি সেগুলো সহজেই অনুমান করা যায়। যেমন গত কয়েক বছর যে পাসওয়ার্ডসমূহ সবচেয়ে বেশি ব্যবহার করা হয়েছে সেগুলো হলো-

Rank	2011 <sup>[4]</sup>	2012 <sup>[5]</sup>	2013 <sup>[6]</sup>	2014 <sup>[7]</sup>	2015 <sup>[8]</sup>	2016 <sup>[3]</sup>	2017 <sup>[9]</sup>
1	password	password	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345	12345678
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty
5	abc123	qwerty	abc123	qwerty	12345	football	12345
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789
7	1234567	letmein	111111	1234	football	1234567890	letmein
8	letmein	dragon	1234567	baseball	1234	1234567	1234567
9	trustno1	111111	iloveyou	dragon	1234567	princess	football
10	dragon	baseball	adobe123 <sup>[a]</sup>	football	baseball	1234	iloveyou

পাসওয়ার্ড জেনারেটর ব্যবহার করা

পাসওয়ার্ড জেনারেটর ব্যবহার করা করে আমরা খুব সহজেই র্যানডম পাসওয়ার্ড তৈরি করতে পারি। একটি উল্লেখযোগ্য পাসওয়ার্ড জেনারেটর সাইট হলো- [passwordsgenerator.net](http://passwordsgenerator.net)

এই সাইটে জেনারেট পাসওয়ার্ড এ ক্লিক করলেই নতুন পাসওয়ার্ড জেনারেট হবে। তারপর সেই পাসওয়ার্ড দিয়ে ট্রাই করতে হবে।



ডাম্পস্টার ডাইভিং এর মাধ্যমে

ডাম্পস্টার ডাইভিং এর মাধ্যমে এর মাধ্যমেও অনেক সময় পাসওয়ার্ড সংগ্রহ করা যায়। কারণ আমরা অনেক সময় পাসওয়ার্ড হয়তো কোন পেপারে লিখে রেখে দেই। তারপর কিছুদিন পর হয়তো মনে হলো এই পেপারটি আর দরকার নেই। তাই কোন ডাস্টবিন এ ফেলে দেই। ফলে এই ডাস্টবিন থেকে পেপার সংগ্রহ করে পাসওয়ার্ড পাওয়া যেতে পারে।



সোশ্যাল ইঞ্জিনিয়ারিং করে

সোশ্যাল ইঞ্জিনিয়ারিং করেও পাসওয়ার্ড সংগ্রহ করা হয়ে থাকে। যেমন আপনাকে একটি ফিশিং সাইটের লিংক দিয়ে বললো এই লিংকে ক্লিক করুন আপনি যখনই ক্লিক করবেন আপনার ইউজার নেইম এবং পাসওয়ার্ড দেখা যাবে।

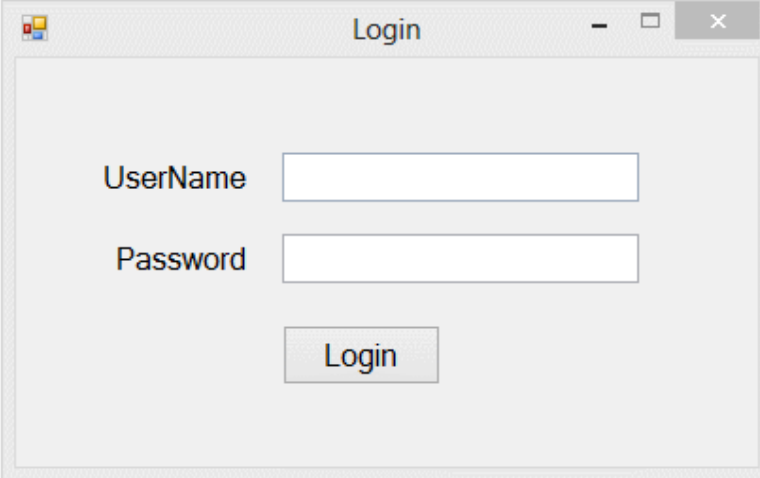


কিভাবে পাসওয়ার্ড ক্রেকিং থেকে সিস্টেমকে রক্ষা করবেন?

১. পাসওয়ার্ড তৈরি করার সময় অবশ্যই ৮ থেকে ১২ টি অক্ষর থাকতে হবে। যার মধ্যে নাম্বার, বড় ও ছোট হাতের অক্ষর এবং স্পেশাল সিম্বল থাকতে হবে।
২. প্রত্যেক মাসে পাসওয়ার্ড পরিবর্তন পলিসি থাকতে হবে।
৩. কোথায় পাসওয়ার্ড নোট করে রাখা যাবে না। মনে রাখতে হবে।
৪. কখনো পাসওয়ার্ড হিসেবে জন্ম তারিখ, ছেলে/মেয়ের নাম বা নিজের নাম ইত্যাদি দেওয়া যাবে না।
৫. কেউ রেনডম পাসওয়ার্ড ব্যবহার করে চেষ্টা করছে না কি তার লগ দেখতে হবে।

## প্রিভিলেজ এস্কালাশন

প্রিভিলেজ এস্কালাশন হলো পাসওয়ার্ড ক্রেকিং এর পাসওয়ার্ড সংগ্রহ করে সেই সিস্টেমে প্রবেশ করা।  
যদি সিস্টেম ডিজাইনে কোন ভুল থাকে অথবা প্রোগ্রামিং এ কোন বাগ থাকে তাহলে খুব সহজেই  
প্রিভিলেজ এস্কালাশন করা সম্ভব। যেমন আমরা অনেক সময় এক স্টেপ ভেরিফিকেশন এর মাধ্যমে লগিন  
করতে পারি। ফলে কেউ ইউজার নেইম এবং পাসওয়ার্ড জানতে পারলেই লগিন করতে পারবে।



The image shows a simple web form for logging in. The window has a title bar with the text 'Login' and standard minimize, maximize, and close buttons. Inside the window, there are two text input fields. The first is labeled 'UserName' and the second is labeled 'Password'. Below these fields is a button labeled 'Login'.

কিভাবে প্রিভিলেজ এস্কালাশন থেকে সিস্টেমকে রক্ষা করবেন?

১. টু ফ্যাক্টর অথেনটিকেশন ব্যবহার করতে হবে।
২. ফার্মওয়্যার এবং প্যাচ নিয়মিত আপডেট করতে হবে।
৩. একাধিক লগইন ইউজার থাকলে প্রিভিলেজড লেভেল সেট করতে হবে।

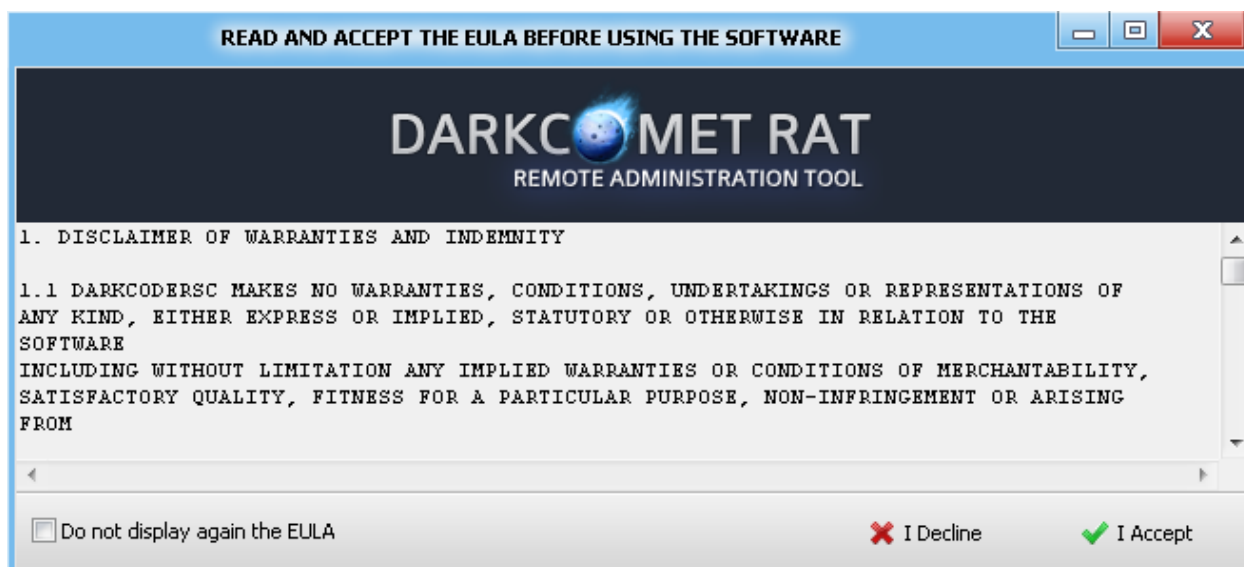


## এক্সেকিউটিং অ্যাপ্লিকেশনস

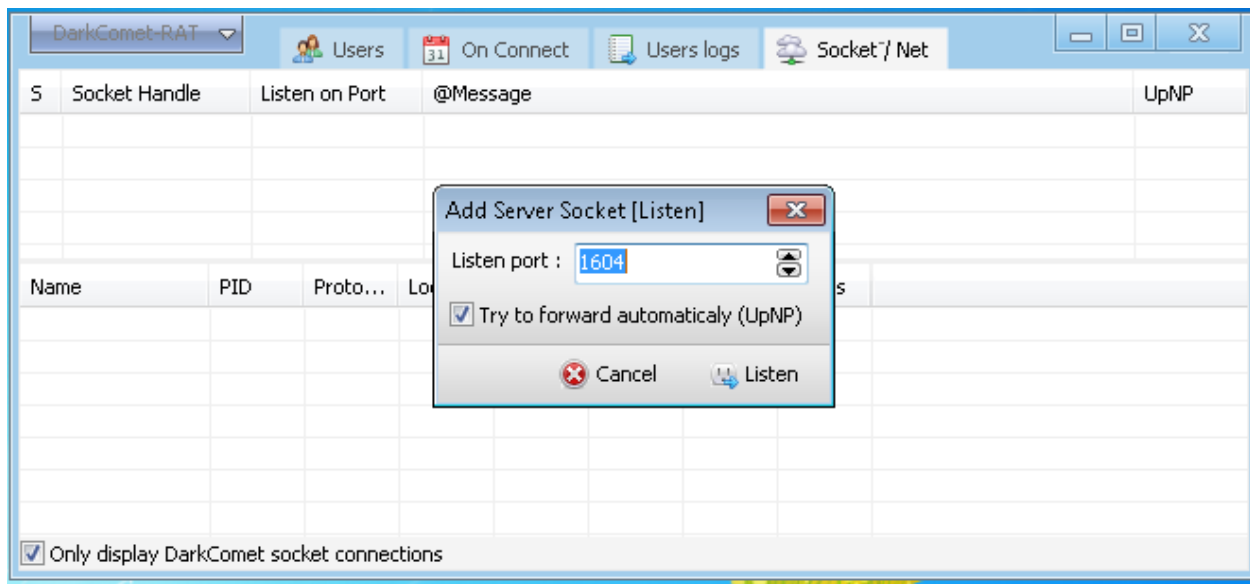
এক্সেকিউটিং অ্যাপ্লিকেশনস এর মাধ্যমে হ্যাকাররা সিস্টেমকে নিজের করে নেয়। এই ধাপে হ্যাকাররা বিভিন্ন অ্যাপ্লিকেশনস এক্সিকিউ করে তখন হ্যাকাররা রিমুটলি সিস্টেম এ লগিন করতে পারে। সাধারণত যে টুলগুলো ব্যবহার করে থাকে সেগুলোর মাঝে একটি হলো ডার্ক কমেট।

এবার দেখি ডার্ক কমেট এপ্লিকেশনটি কিভাবে কাজ করে।

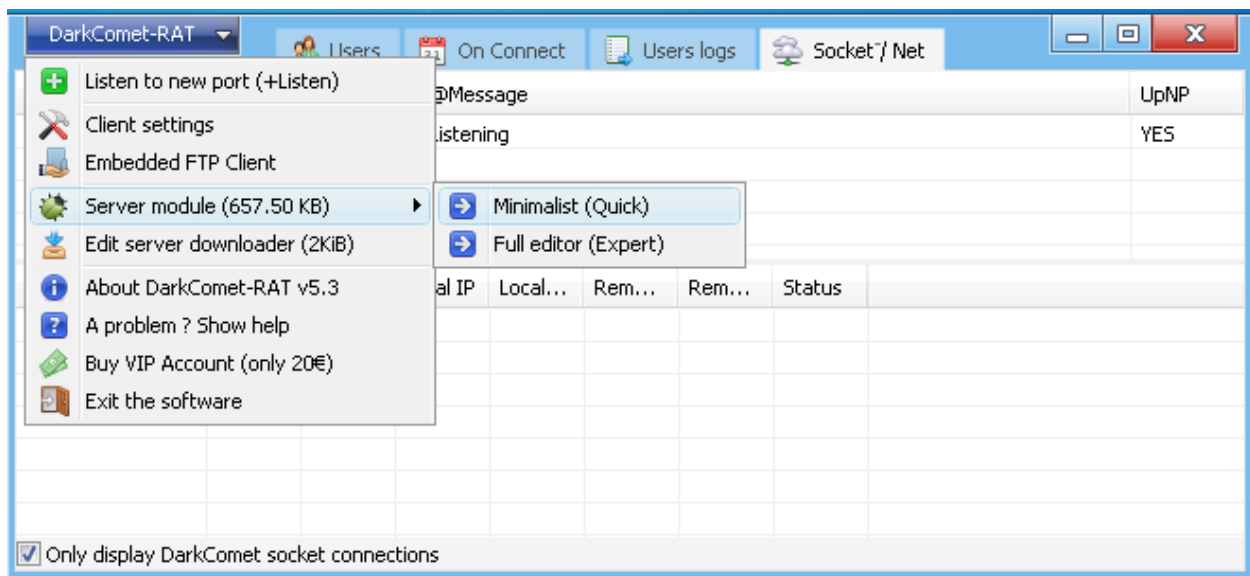
ধাপ-০১: প্রথমে এপ্লিকেশনটি ইন্সটল করতে হবে।



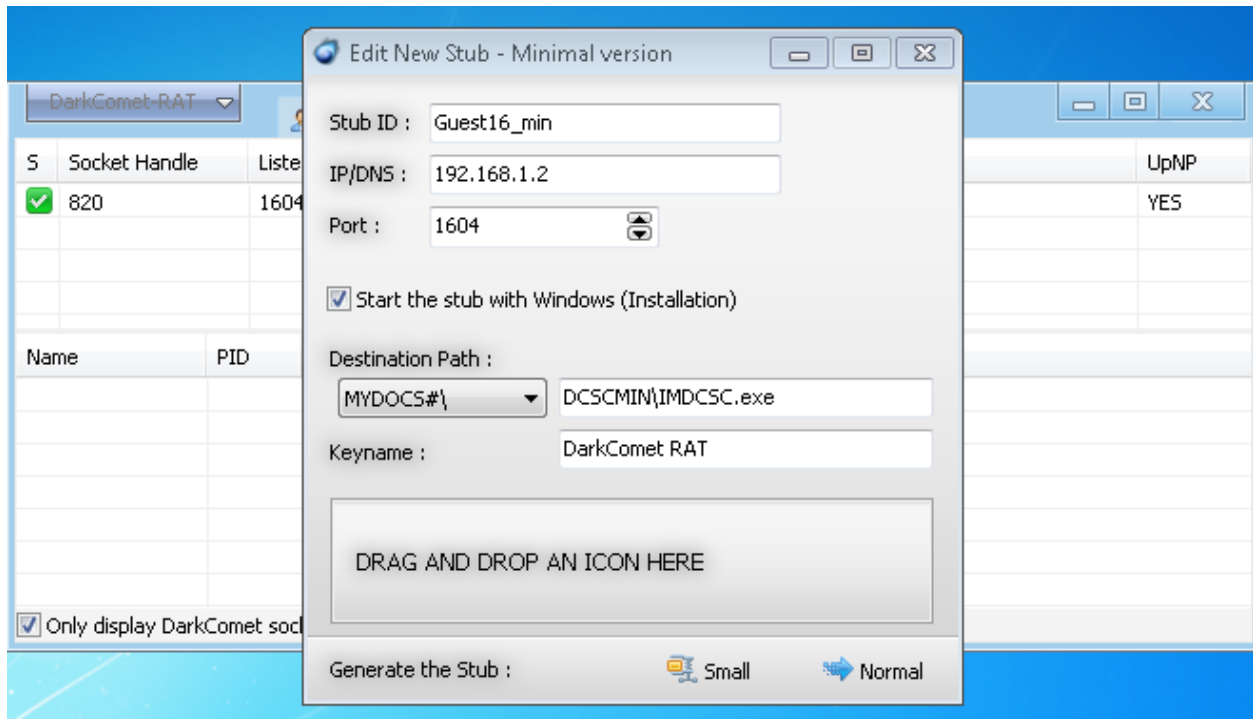
ধাপ-০২: লিসেনিং পোর্ট ১৬০৪ সিলেক্ট করতে হবে।



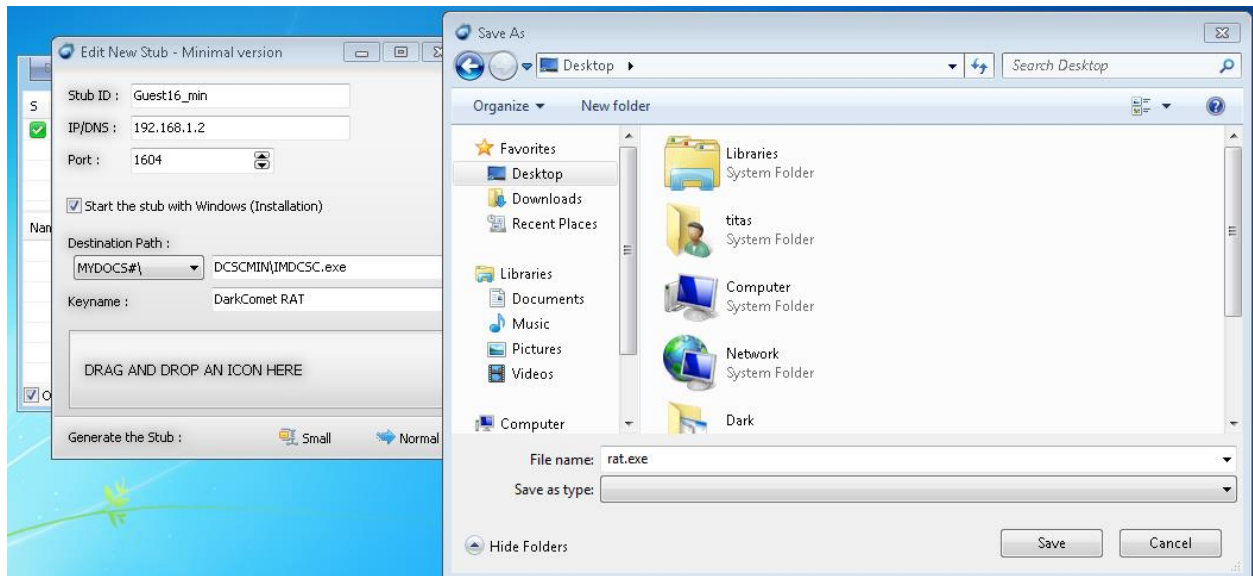
ধাপ-০৩: একটি .exe তৈরি করতে হবে যে পিসি থেকে হ্যাকড পিসি একসেস করা হবে।



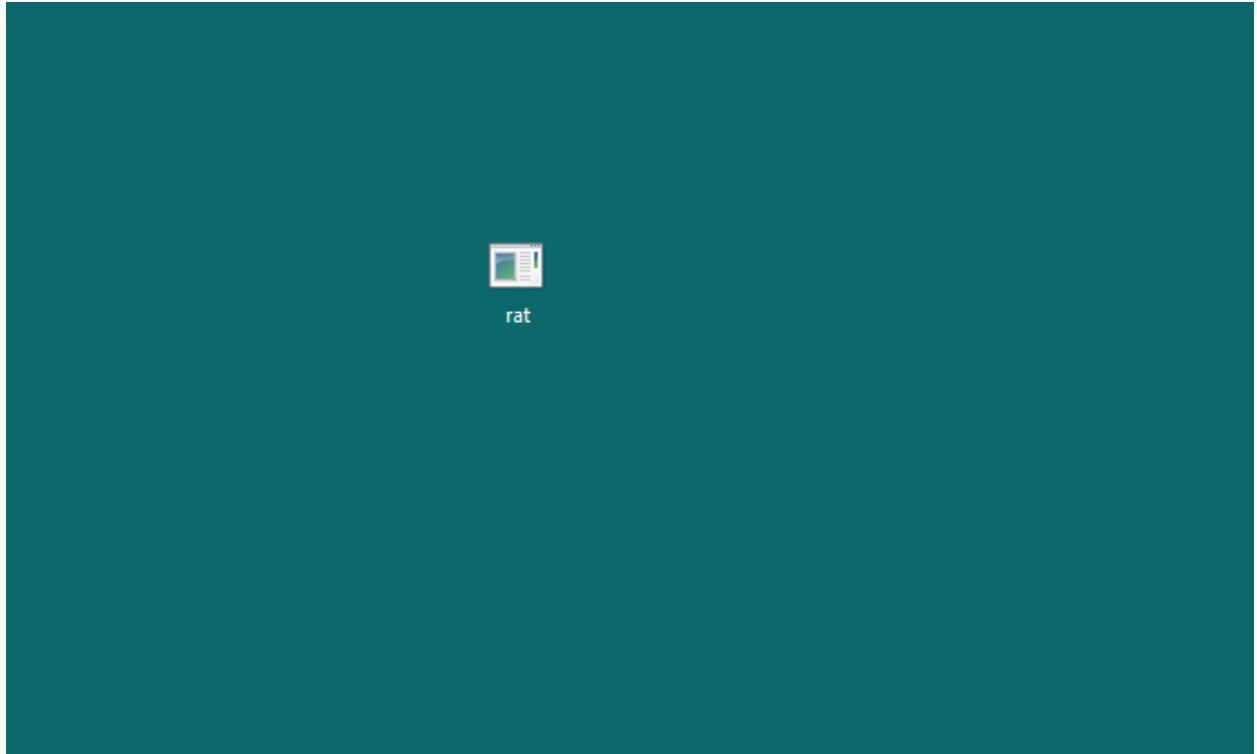
ধাপ-০৪: যে পিসি থেকে একসেস করা হবে সেই পিসির আইপি দিতে হবে।



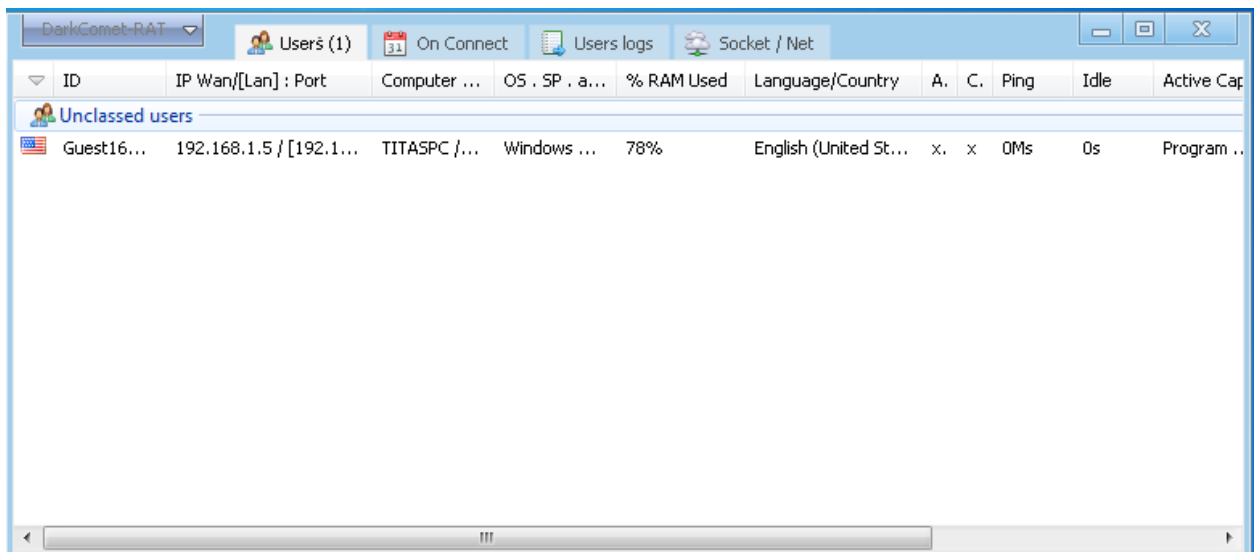
ধাপ-০৫: একটি .exe তৈরি করতে হবে।



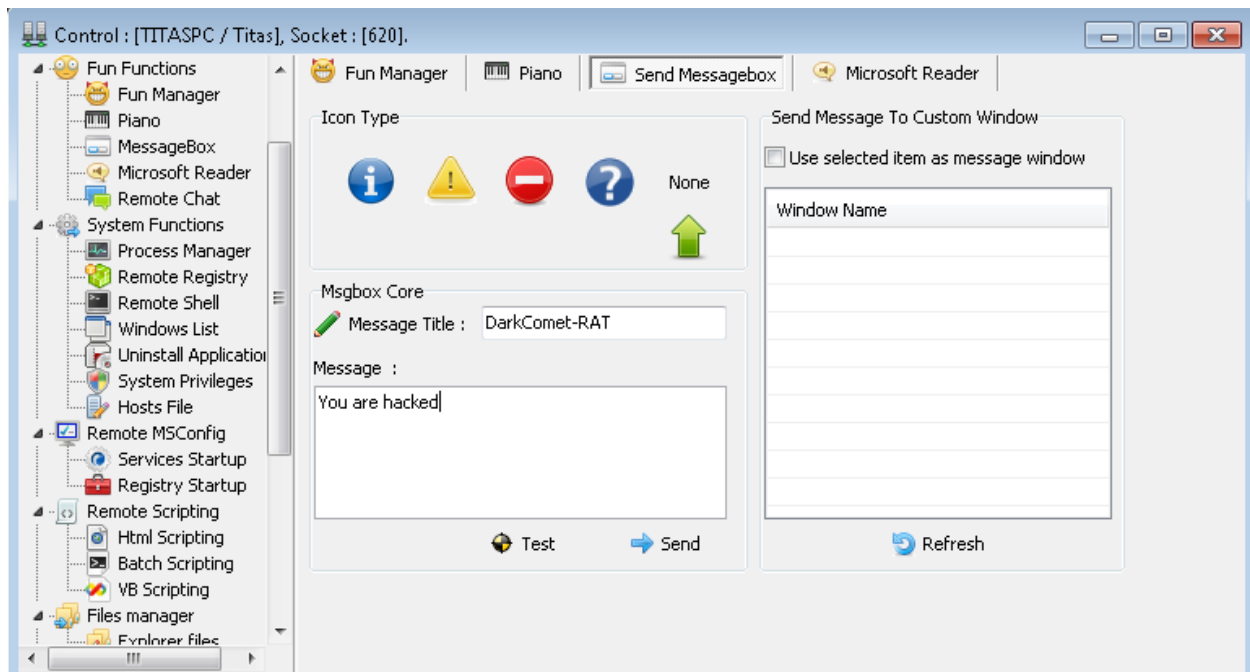
ধাপ-০৬: .exe ফাইলটি যে পিসিকে হ্যাক করা হবে সেই পিসিতে রাখতে হবে।



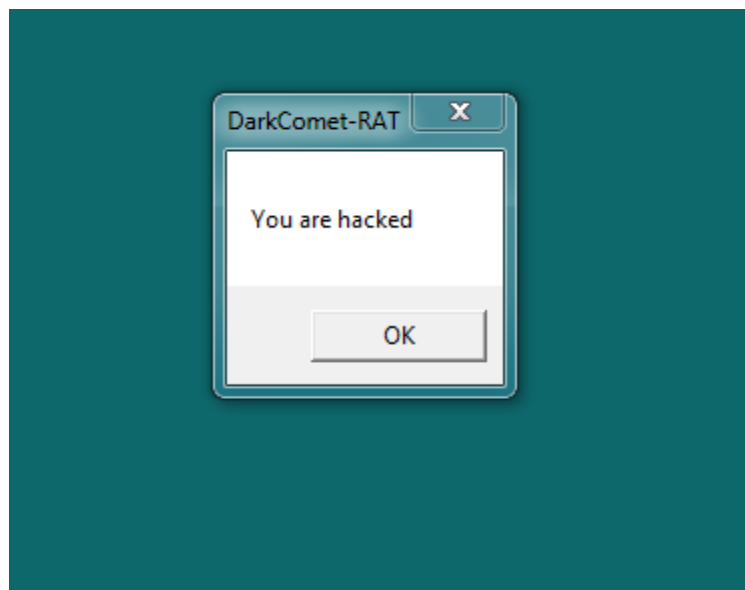
ধাপ-০৭: যখনই হ্যাকড পিসিতে এই .exe টি রান করা হবে। তখনই হ্যাকার এর পিসিতে ইউজার লিস্টে শো করতে থাকবে।



ধাপ-০৮: এখন হ্যাকার এর হাতে রিমুট পিসি সে সবকিছুই করতে পারবে। এখানে হ্যাকড পিসিতে একটি ম্যাসেজ শো করানোর চেষ্টা করা হচ্ছে।



ধাপ-০৯: হ্যাকড পিসিতে এই ম্যাসেজ শো হচ্ছে।



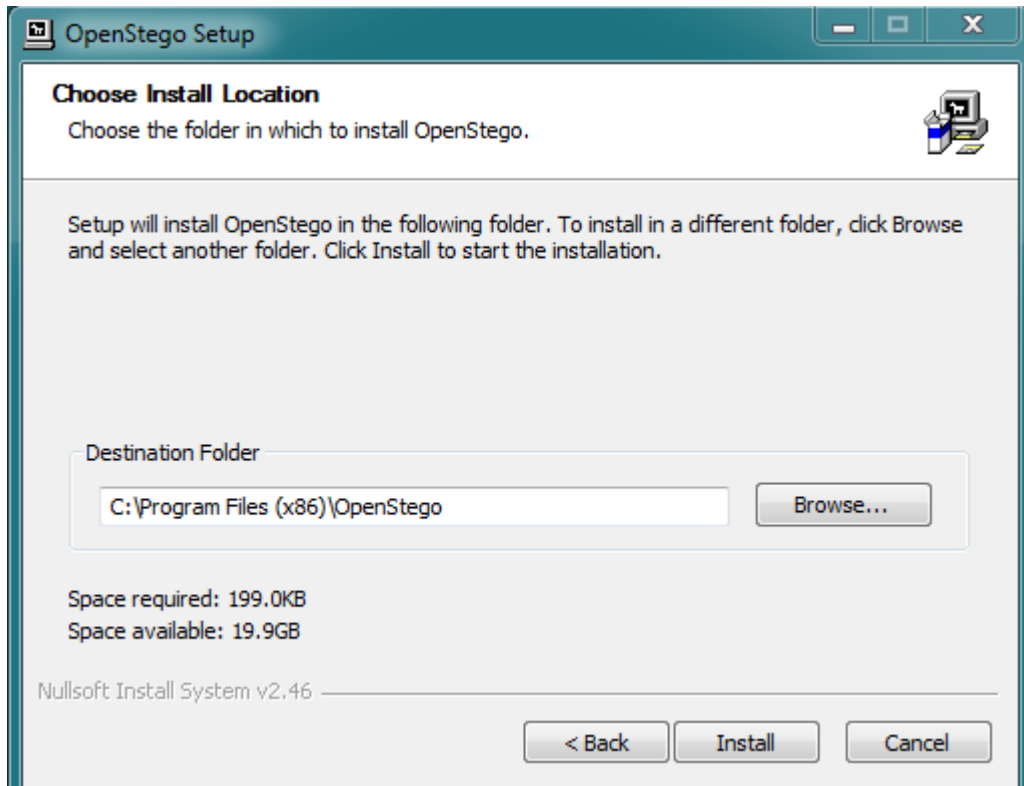
এ ধরনের পরিস্থিতি থেকে রক্ষা পাওয়ার উপায় হলো কোন ধরনের অপরিচিত .exe ফাইলে ক্লিক না করা।

হিডিং ডাটা

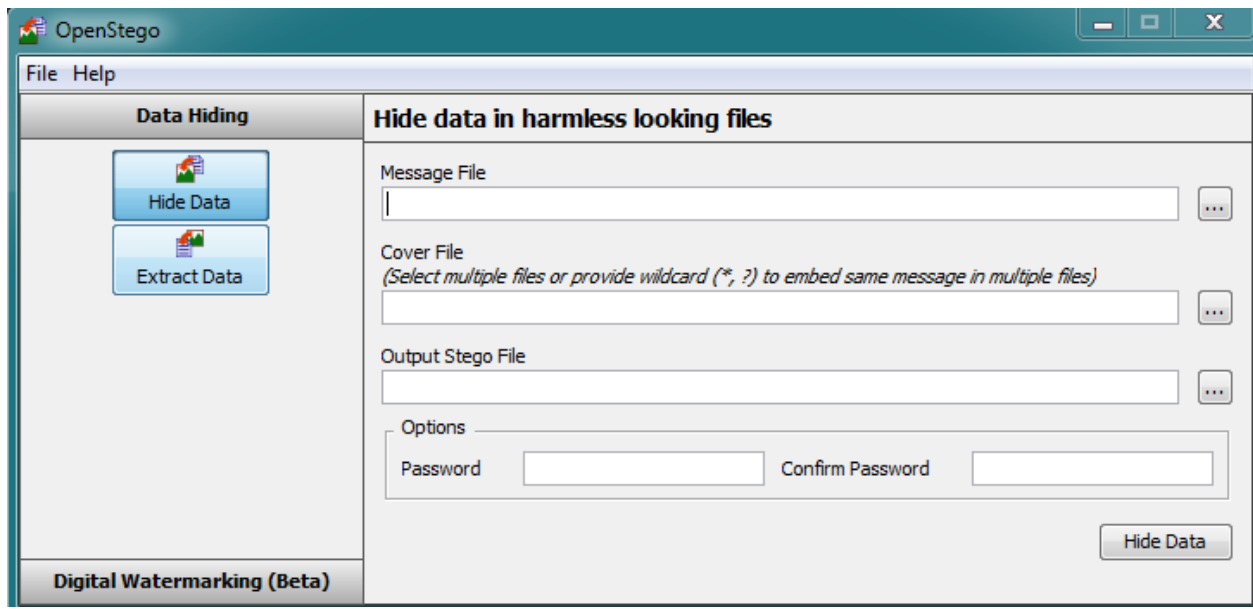
স্টেনোগ্রাফি টুলস ব্যবহার করে খুব সহজেই ডাটা হাইড করে স্থানান্তর করা যায়। যেমন- OpenStego

চলেন দেখি কিভাবে OpenStego দিয়ে ছবির মাঝে লেখা সংযুক্ত করা যায়।

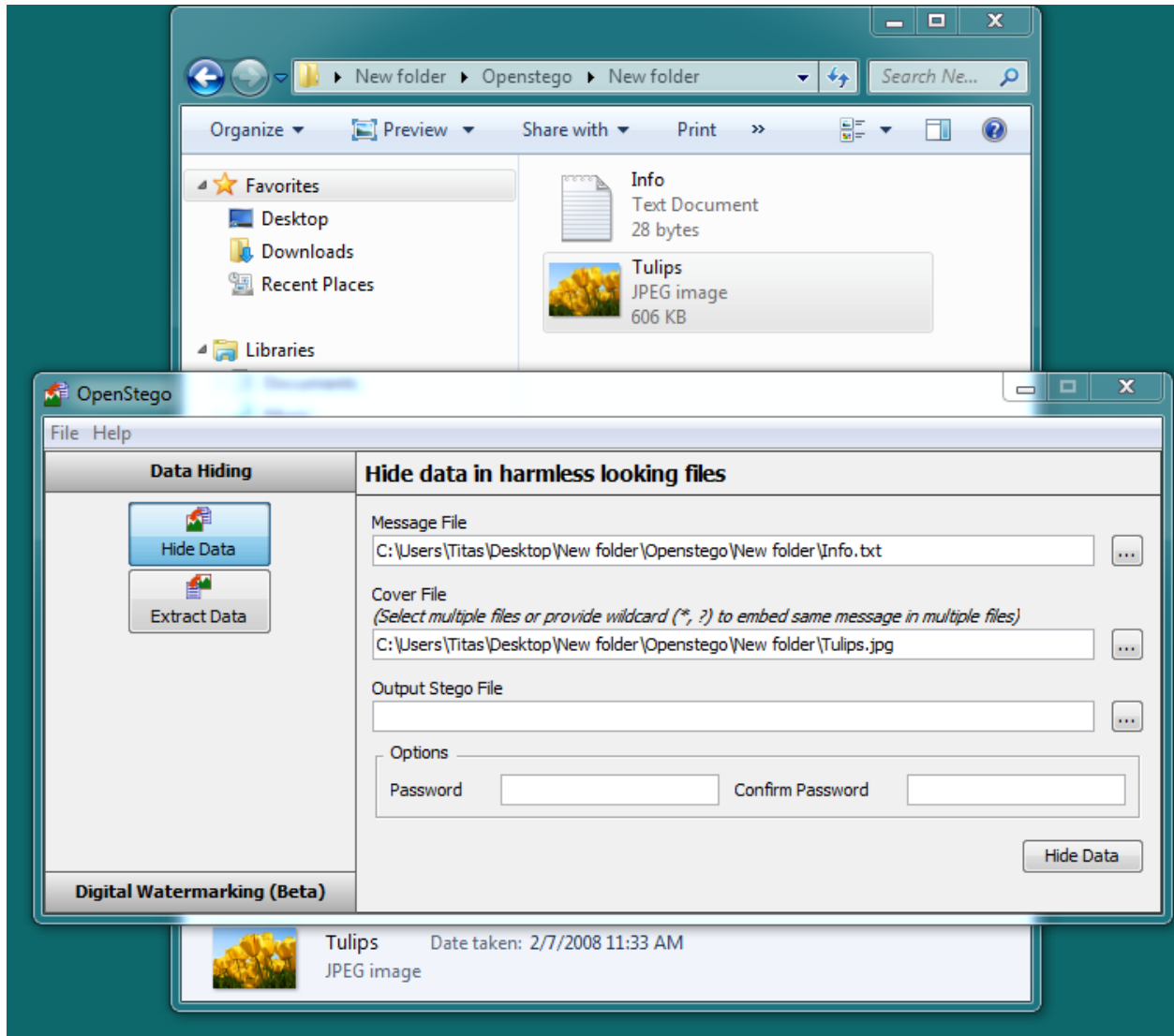
ধাপ-০১: প্রথমে OpenStego সফটওয়্যারটি ইন্সটল করতে হবে।



ধাপ-০২: সফটওয়্যারটি ওপেন করতে হবে।

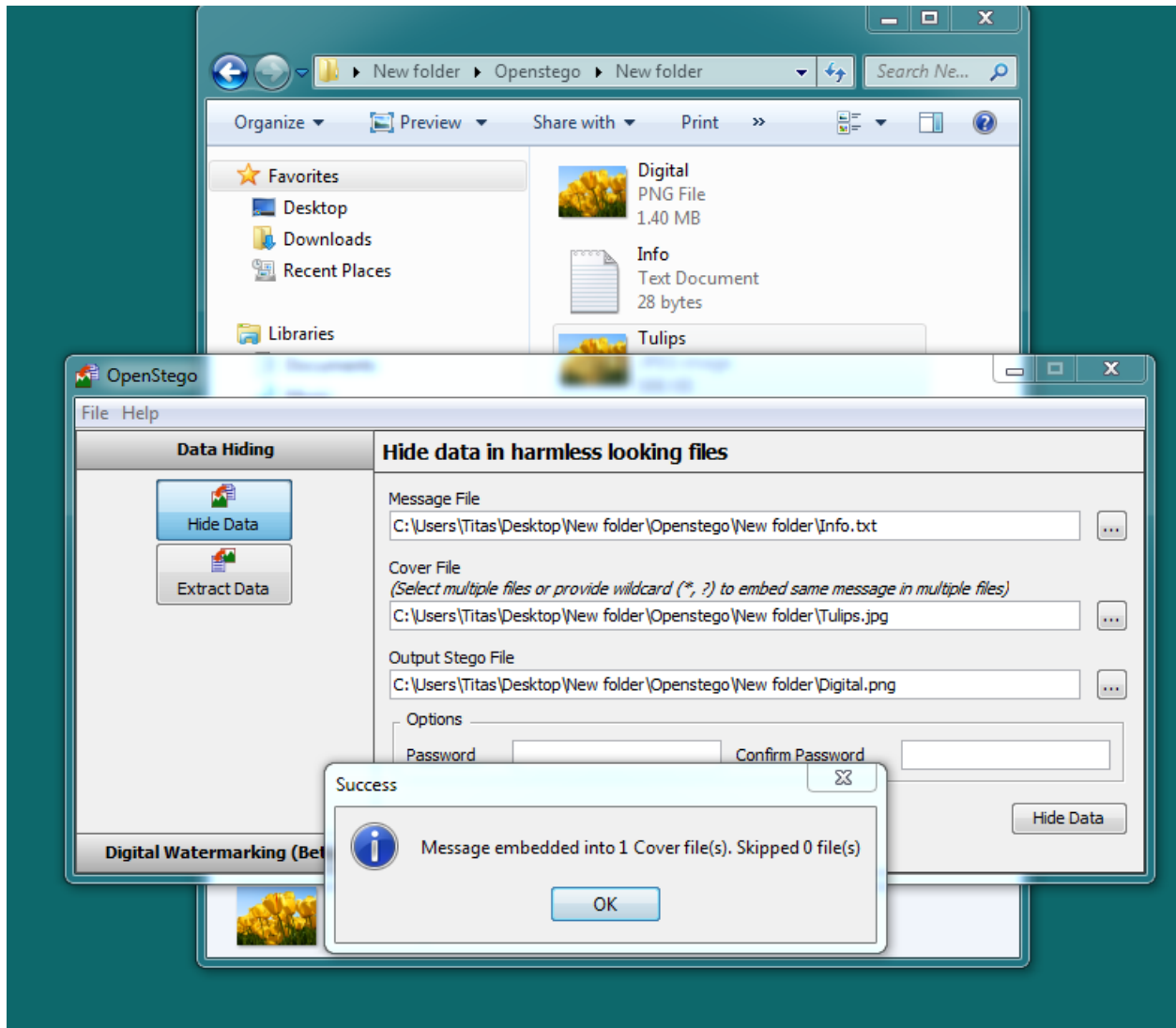


ধাপ-০৩: যে ফাইলটি হাইড করতে চান সেই ফাইলটি দিতে হবে।

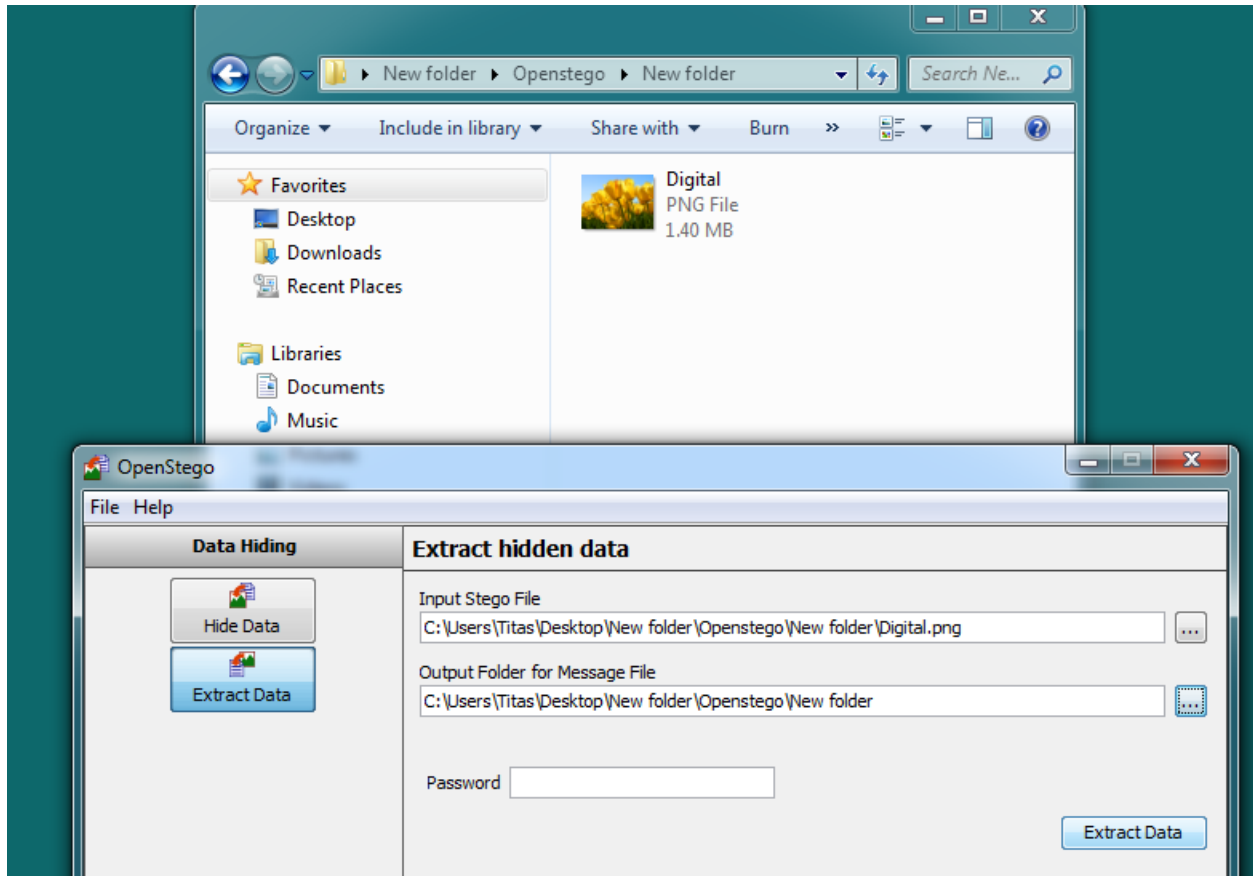


খাপ-০৪: হাইড ডাটাতে ক্লিক করলেই ডাটা হাইড হয়ে যাবে।

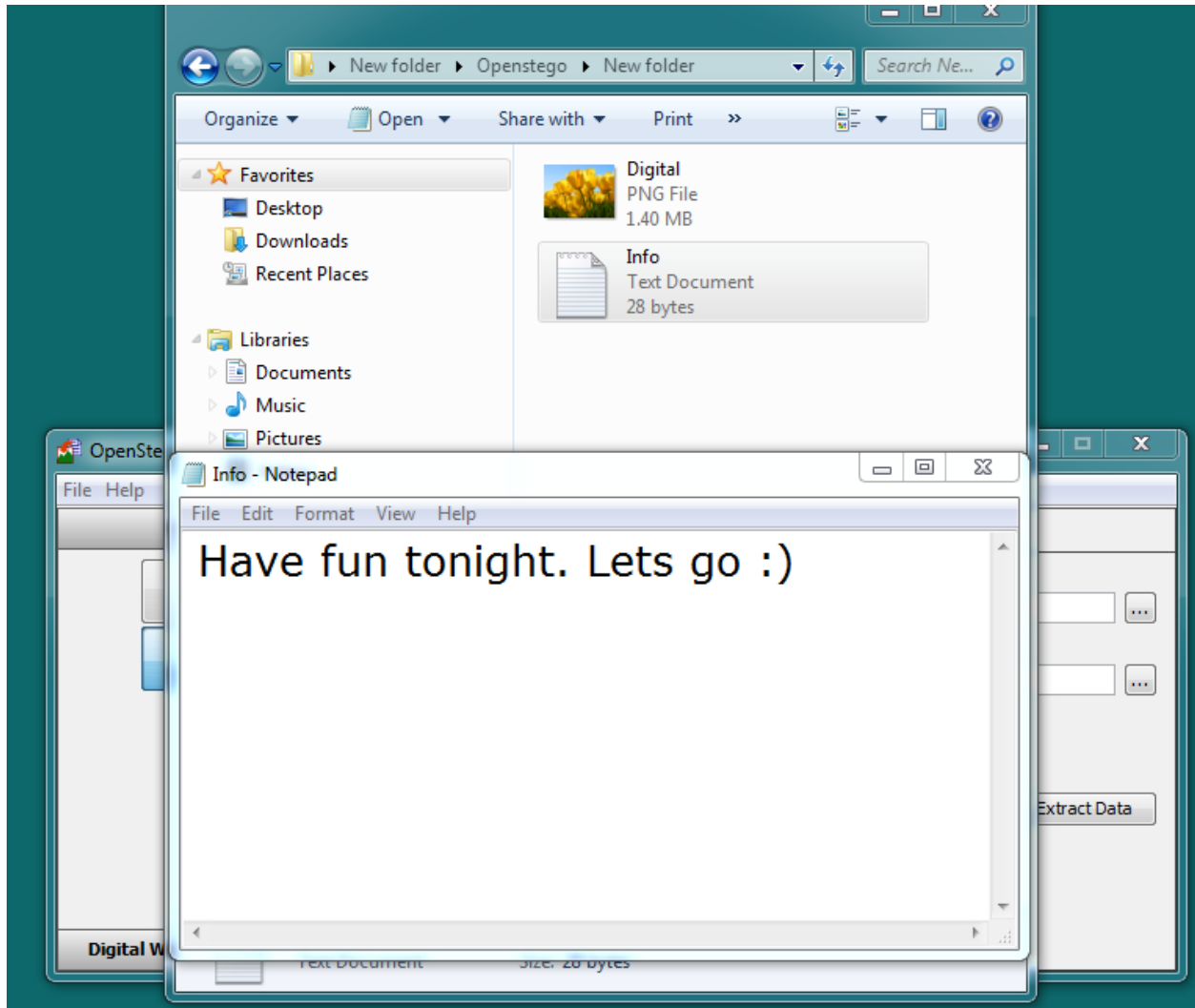




ধাপ-০৫: একইভাবে আনহাইড করতে চাইলে এক্সট্রাক্ট ডাটাতে ক্লিক করলেই হয়ে যাবে।



খাপ-০৬: হিডেন ফাইলের আউটপুট



কিভাবে হিডিং ডাটা ডিটেক্ট করা যায়?

স্টেনোগ্রাফি ডিটেকশন টুল ব্যবহার করে খুব সহজেই ডিটেক্ট করা যায় ।