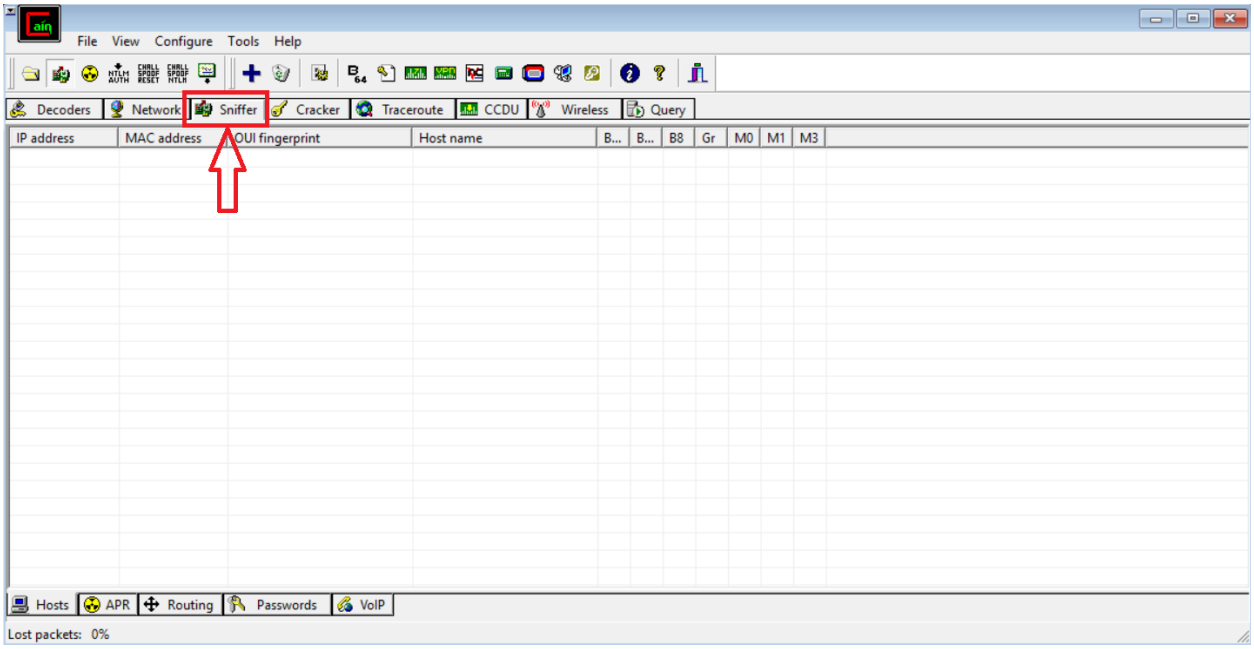
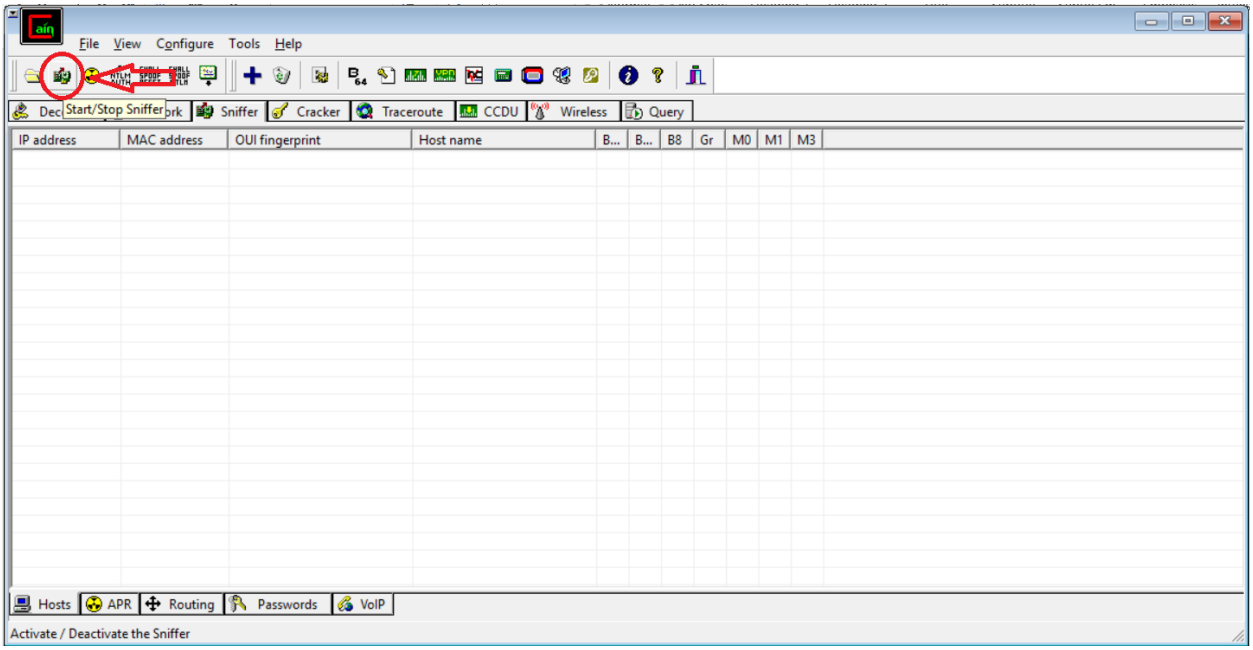
آماده‌سازی Cain & Abel

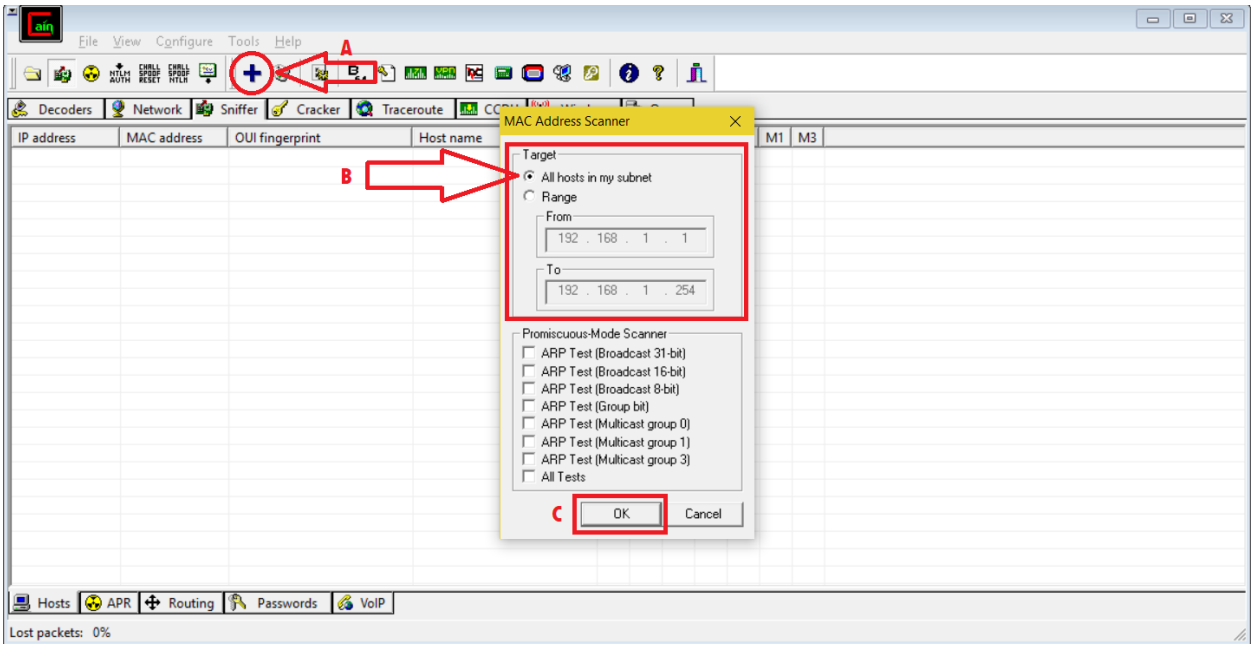
در ابتدا نوارِ مربوط به Sniffer را انتخاب می‌کنیم:



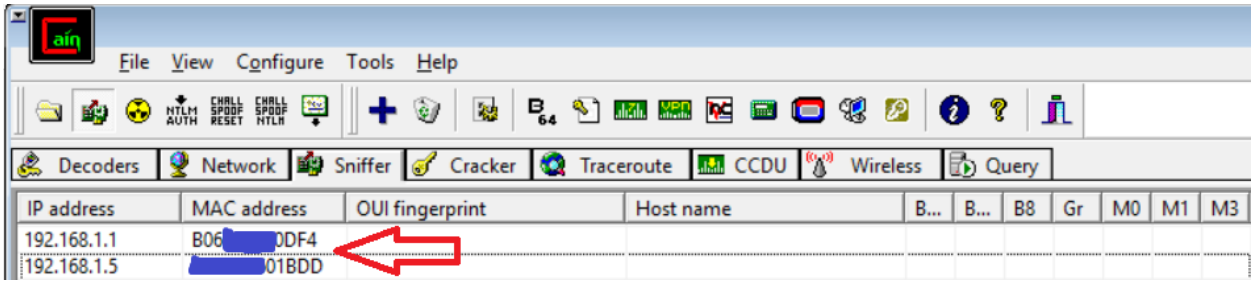
سپس Sniffer را روشن می‌کنیم:



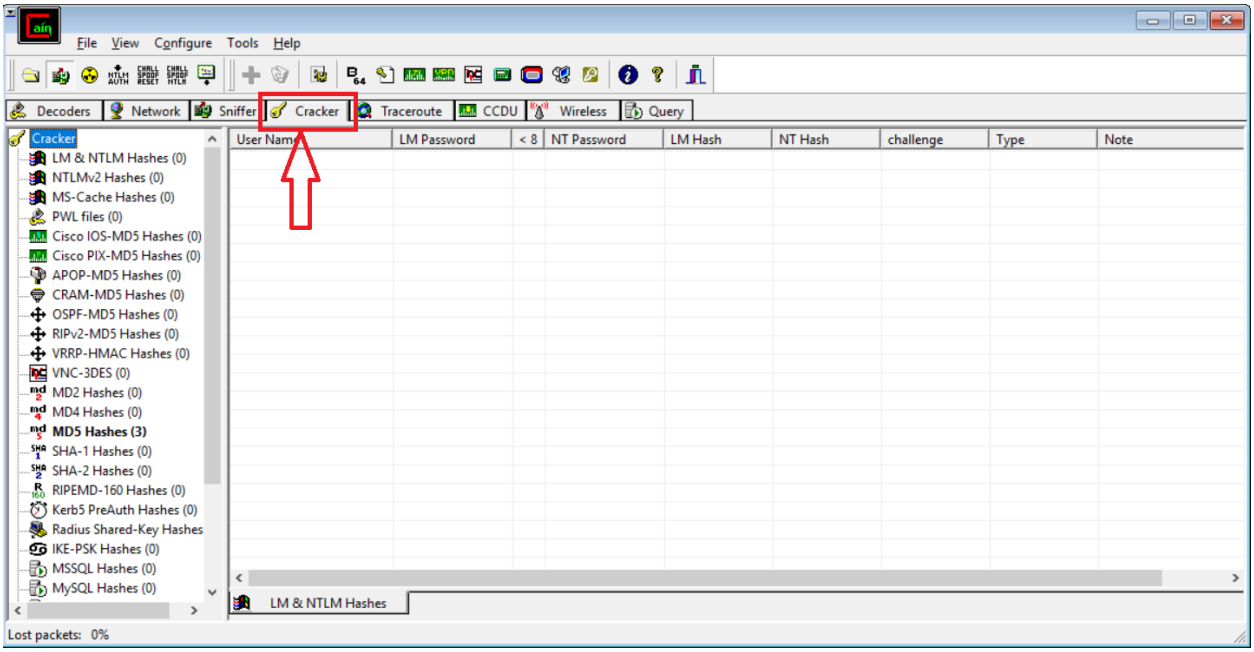
ابتدا گزینه‌ی اضافه کردن آدرس‌های جدید را انتخاب کرده و سپس به اسکن تمام IPهای موجود در شبکه می‌پردازیم تا دستگاه‌های متصل را پیدا کنیم:



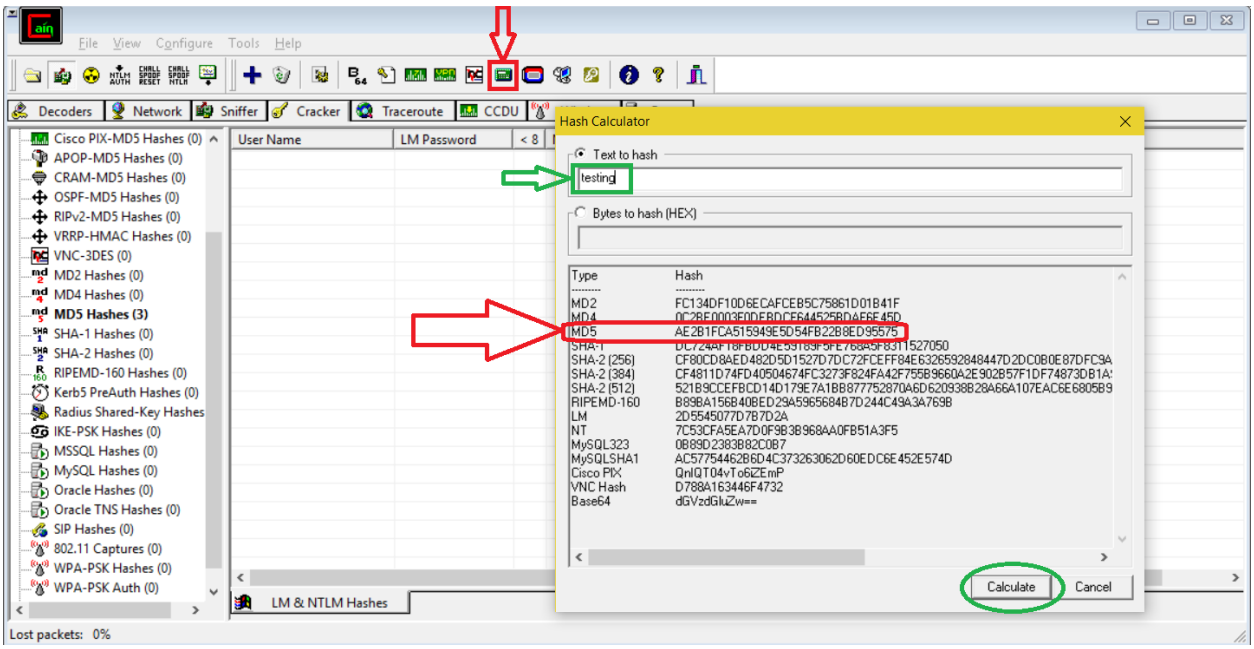
نتیجه‌ی جست‌وجو را نمایان می‌شود:



سپس نوار Cracker را انتخاب می‌کنیم:

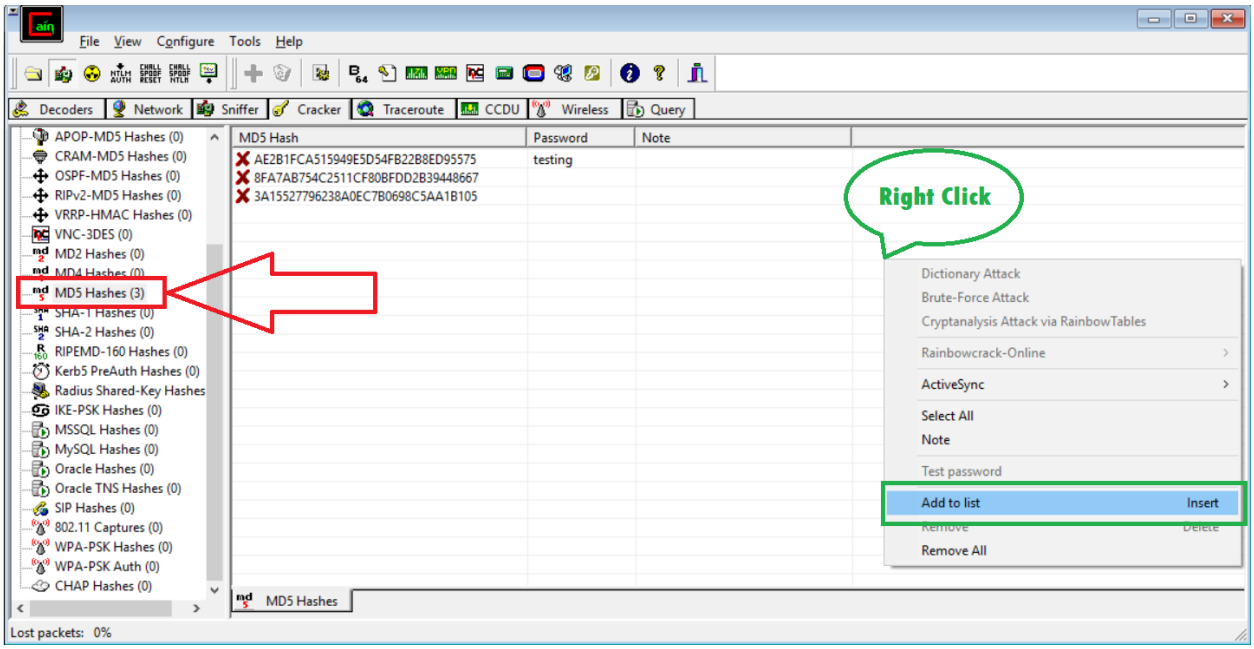


سپس برای ارزیابی و تست عملکرد، مقدار Hashشده‌ی گذرواژه‌های نمونه را به آن اضافه می‌کنیم. برای این کار می‌توان از ابزار *HASH CALCULATOR* تعبیه‌شده در ***Cain & Abel*** استفاده کرد:

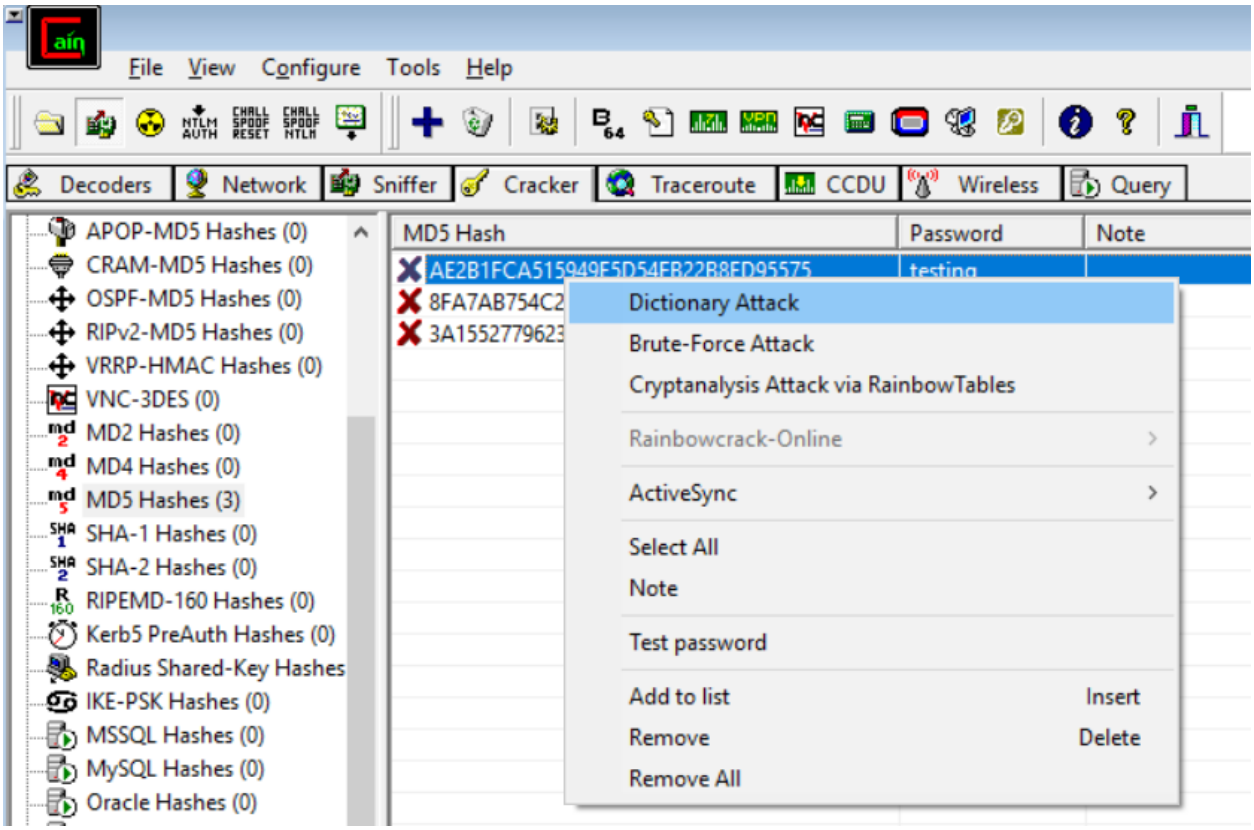


برای سادگی کار و سریع‌تر شدن محاسبه‌ی Hashها در ادامه‌ی کار، از MD5 استفاده می‌کنیم.

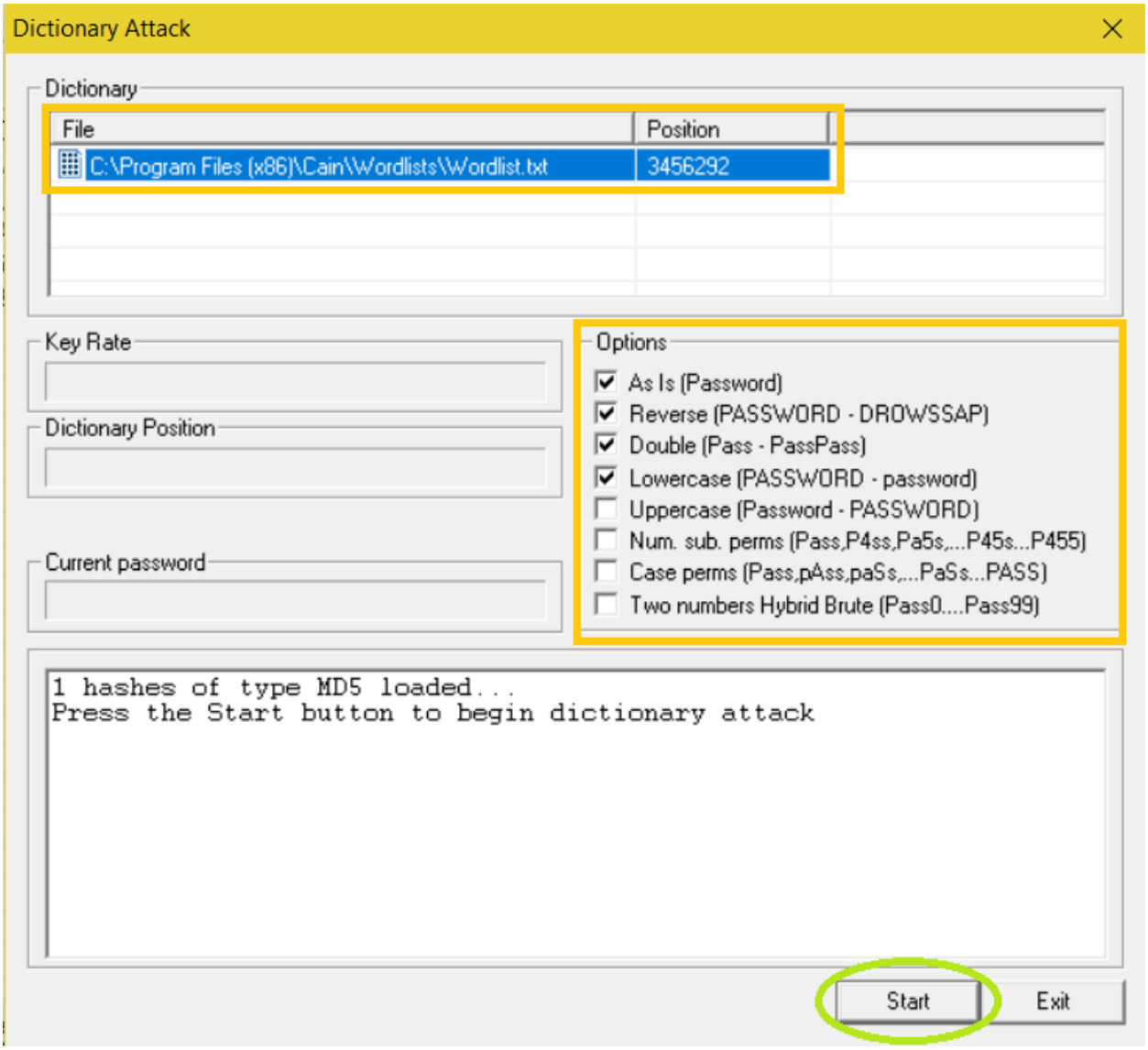
سپس از نوار سمت چپ، گزینه‌ی MD5 Hashes را انتخاب می‌کنیم و مقادیر مورد نظر را به آن اضافه می‌کنیم:



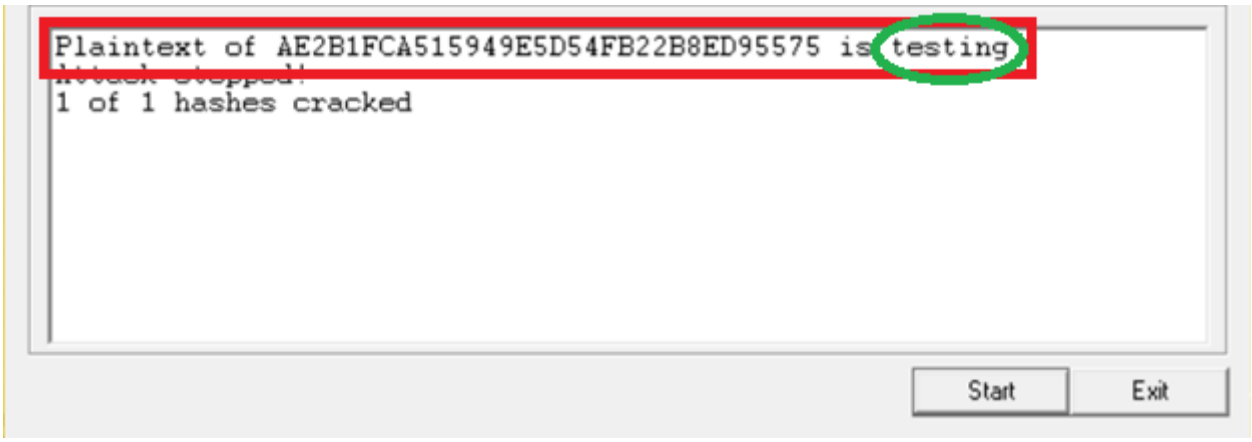
حال انواع حملات را انجام می‌دهیم:



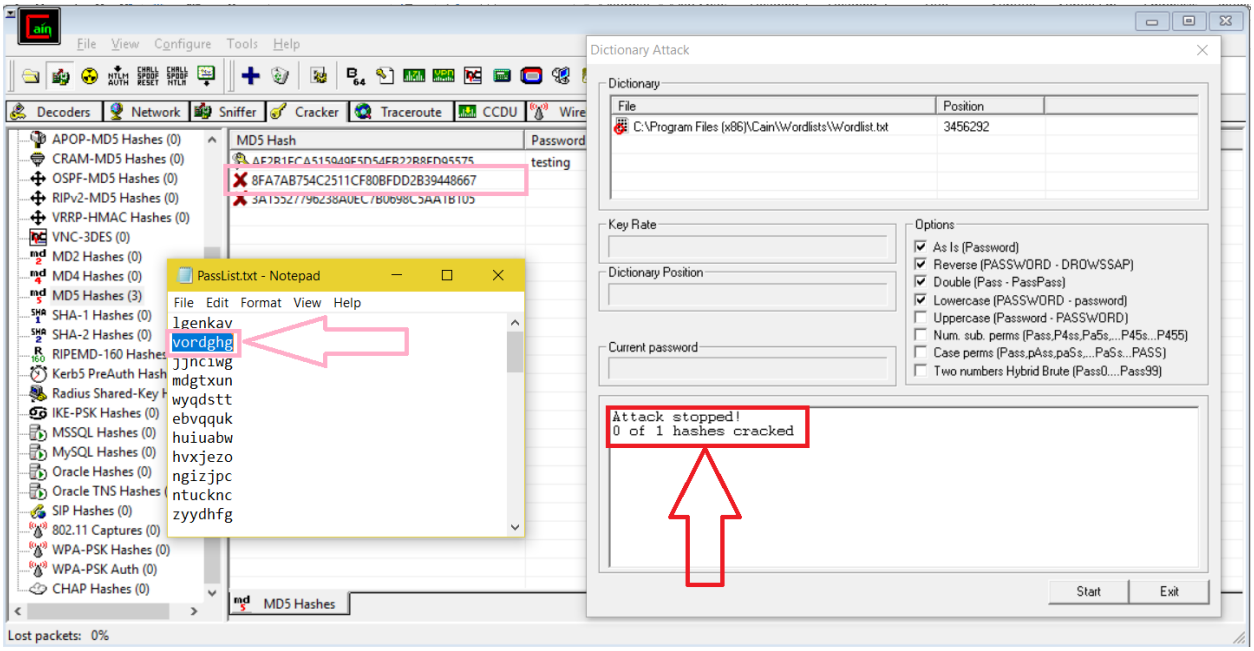
تنظیمات مربوطه را انجام می‌دهیم:



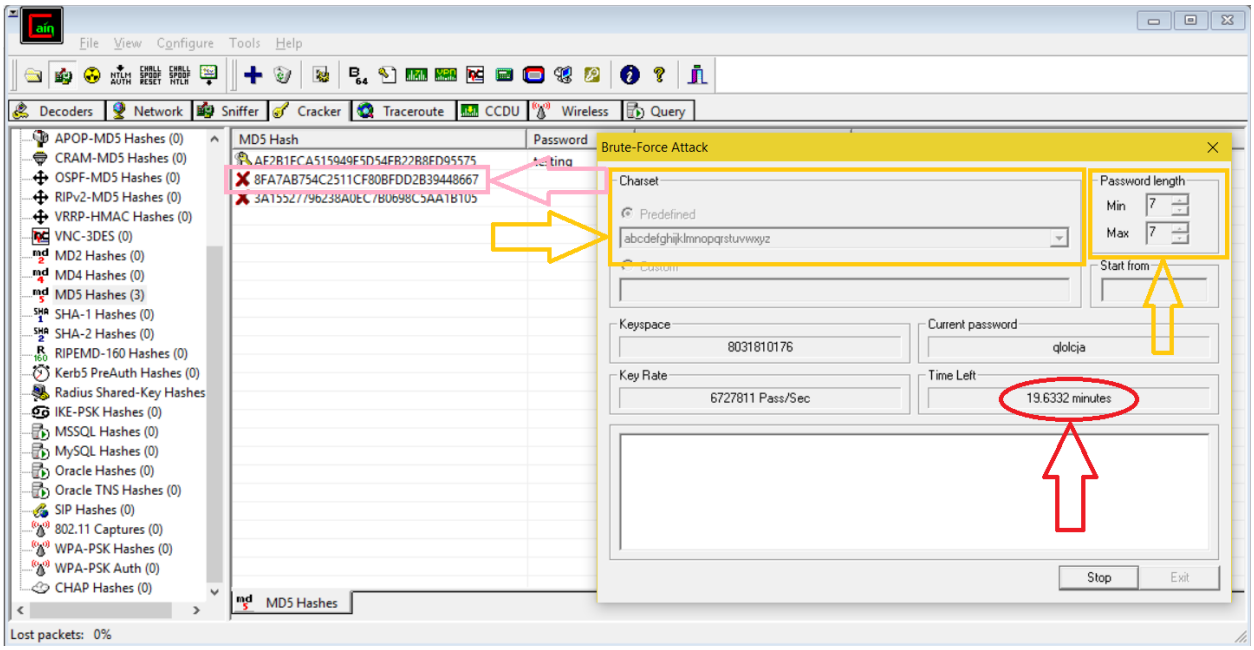
سپس نتیجه نمایان می‌شود:



پس به این ترتیب دیدیم که اگر گذرواژه‌ها ساده و از کلمات معنادار و پرتکرار باشند، به سرعت توسط حمله‌ی Dictionary قادر به پیدا کردن آن‌ها خواهیم بود؛ اما در مثال بعدی، می‌بینیم که این نوع از حمله، برای گذرواژه‌ی تصادفی و غیرمعقول و یا به طور کلی، غیر شفاف، نمی‌تواند نتیجه‌ای بیابد:

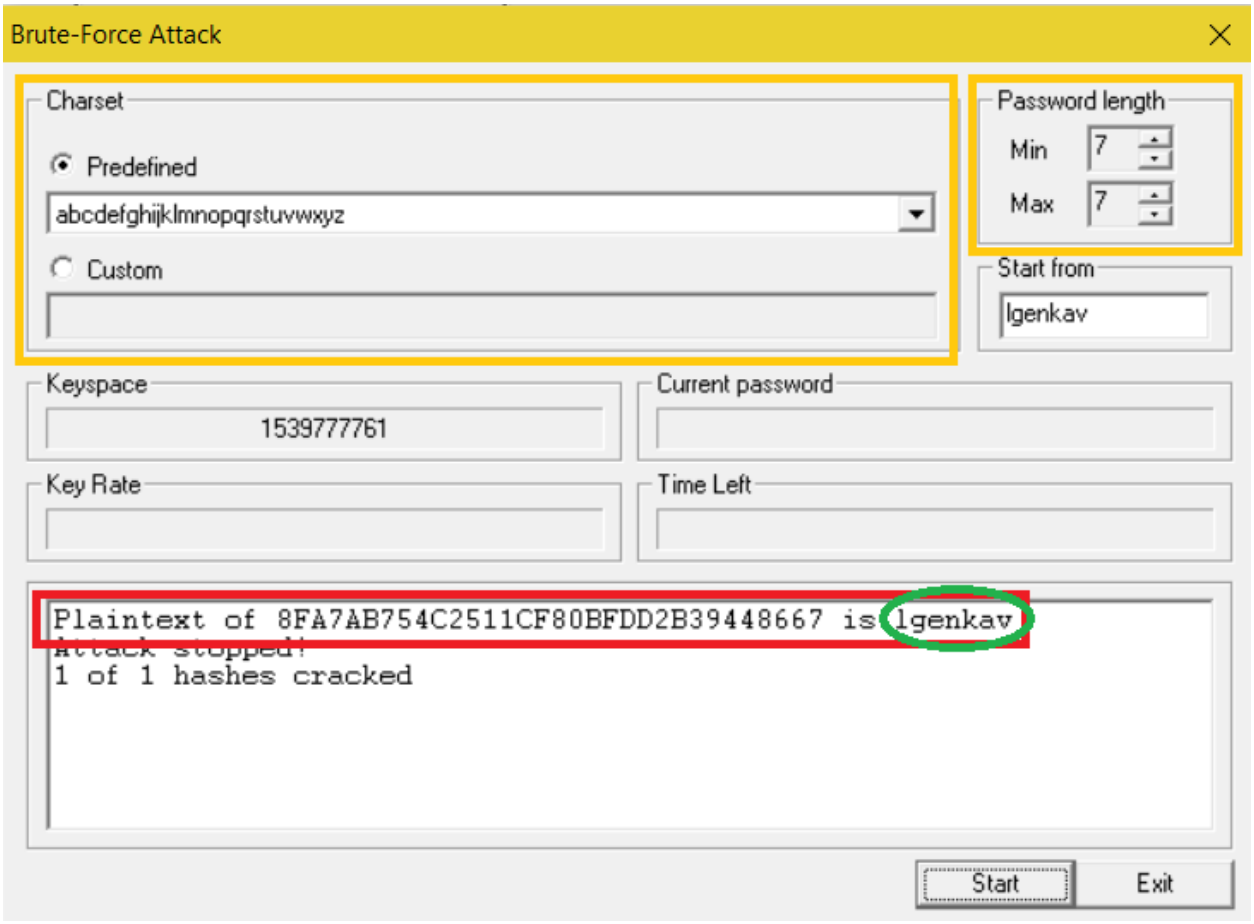


پس به سراغ گزینه‌ی بعدی می‌رویم و از حمله‌ی Brute-Force استفاده می‌کنیم:



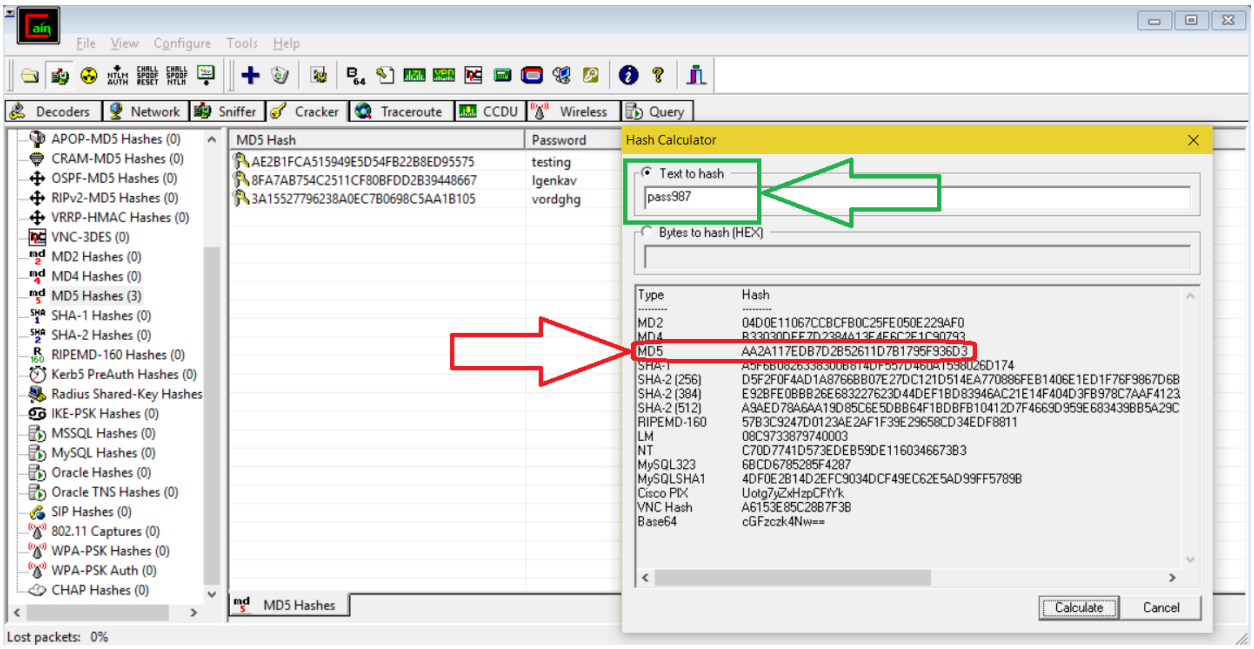
می‌بینیم که زمان قابل توجهی نیاز است تا به نتیجه برسیم اما این زمان همچنان معقول به نظر می‌رسد.

نتیجه پس از حدود ۲۰ دقیقه به دست می‌آید:

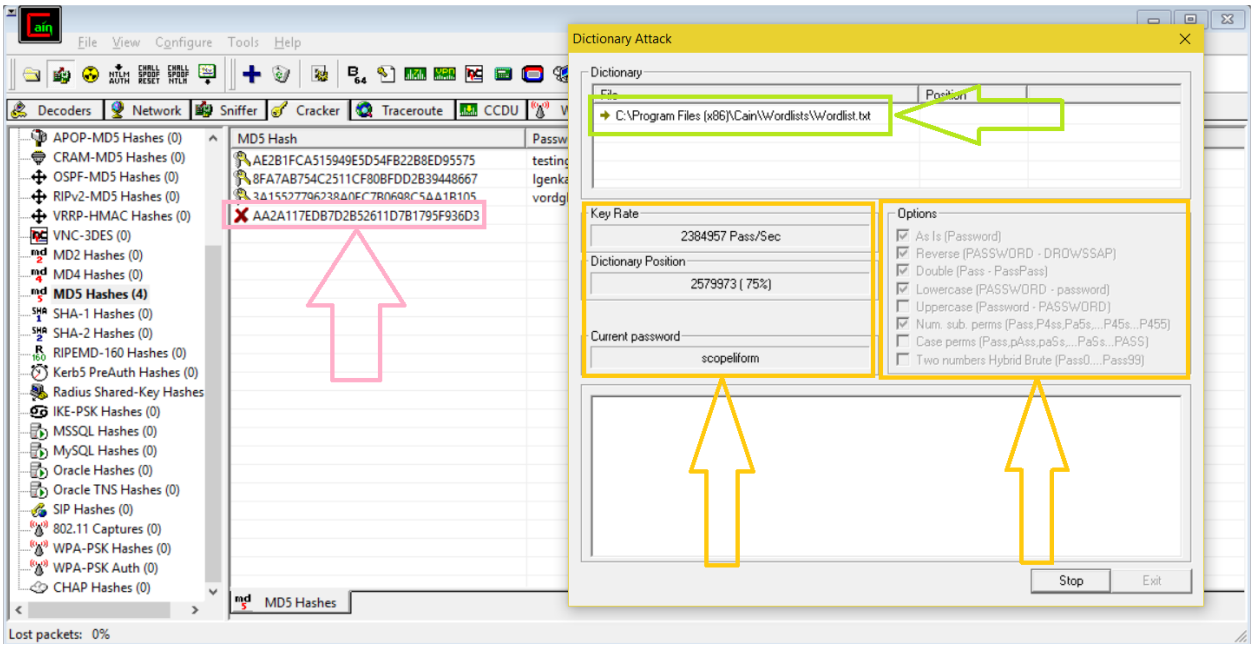


همین فرایندها را برای دسته‌ی دوم و سوم گذرواژه‌های مطرح شده اجرا می‌کنیم.

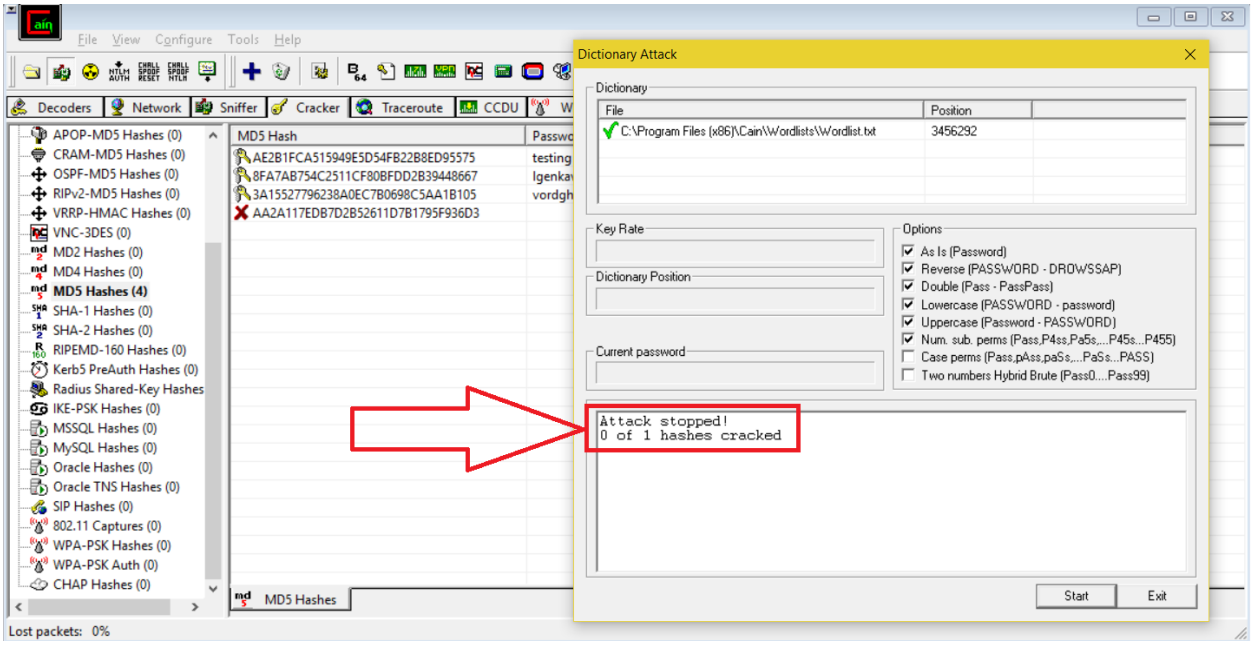
ابتدا برای گذرواژه‌ای ساده داریم:



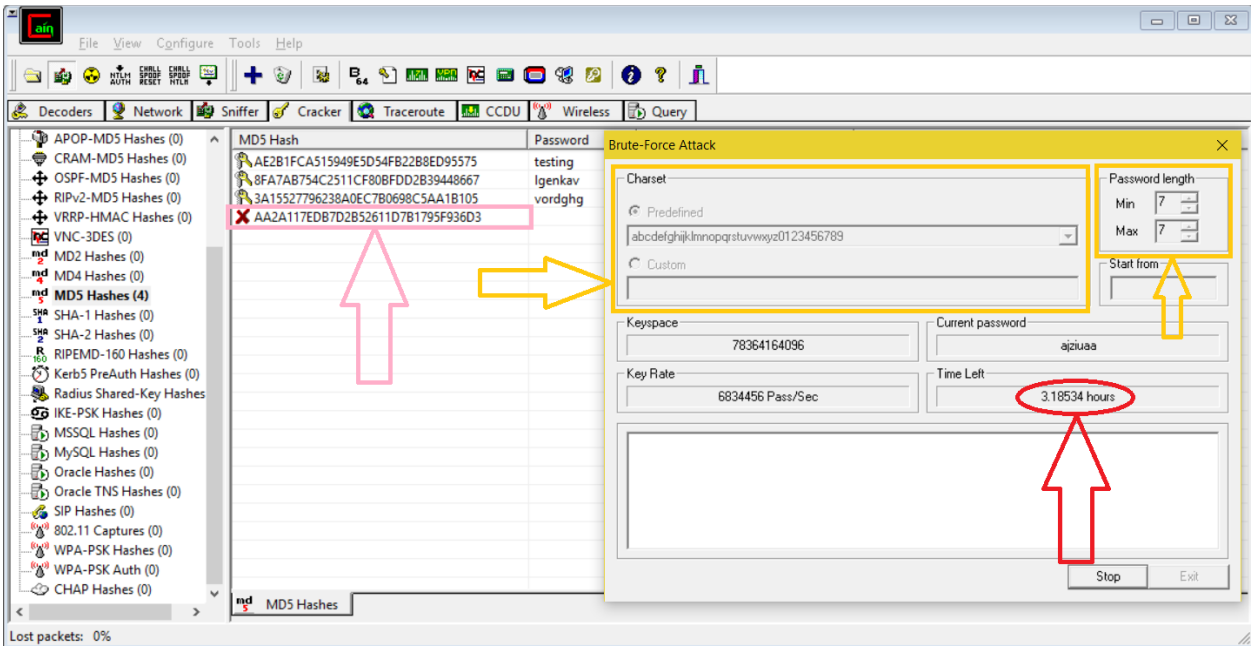
حمله‌ی Dictionary را اجرا می‌کنیم:



با استفاده از حمله‌ی Dictionary مشاهده می‌شود که حتی برای یک گذرواژه‌ی ساده که فقط عدد به آن اضافه کردیم، به نتیجه‌ای نمی‌رسیم و این گواه بر آن است که با اضافه کردن اعداد به گذرواژه‌ها، امنیت آن‌ها به مقدار قابل توجهی افزایش پیدا می‌کند:

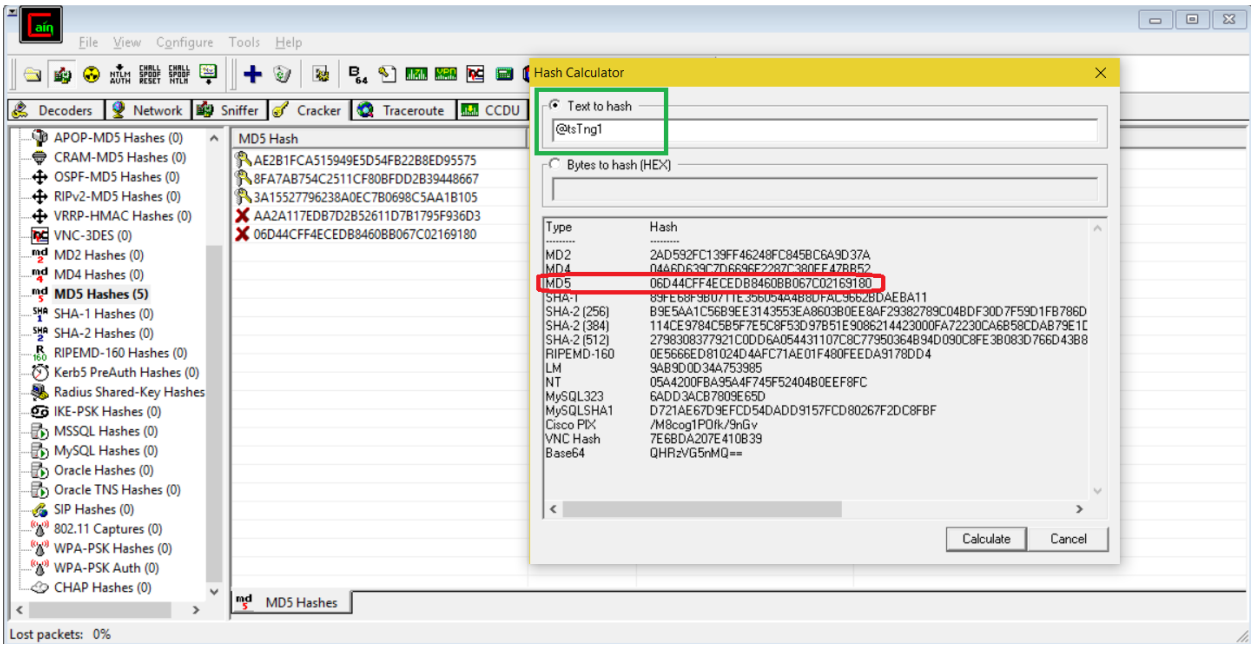


پس به سراغ گزینه‌ی بعدی می‌رویم و از حمله‌ی Brute-Force استفاده می‌کنیم:

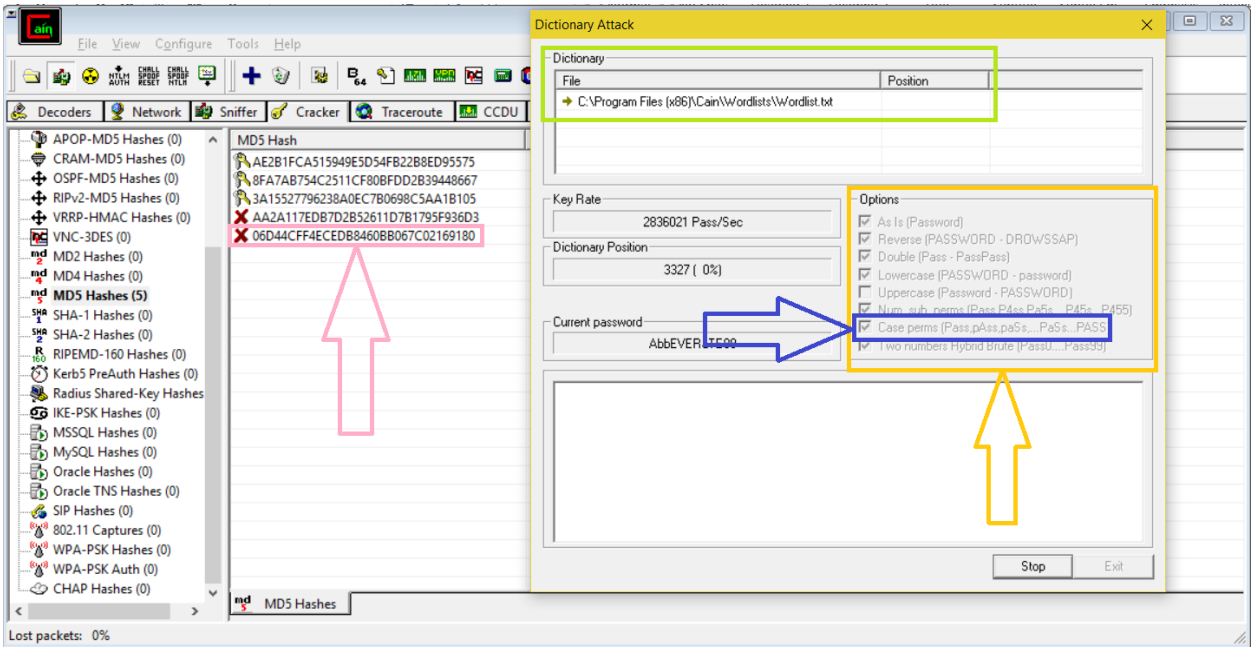


همان‌طور مشاهده می‌شود، زمان مورد نیاز برای آن که به نتیجه برسیم، تقریباً ۱۰ برابر شده است!

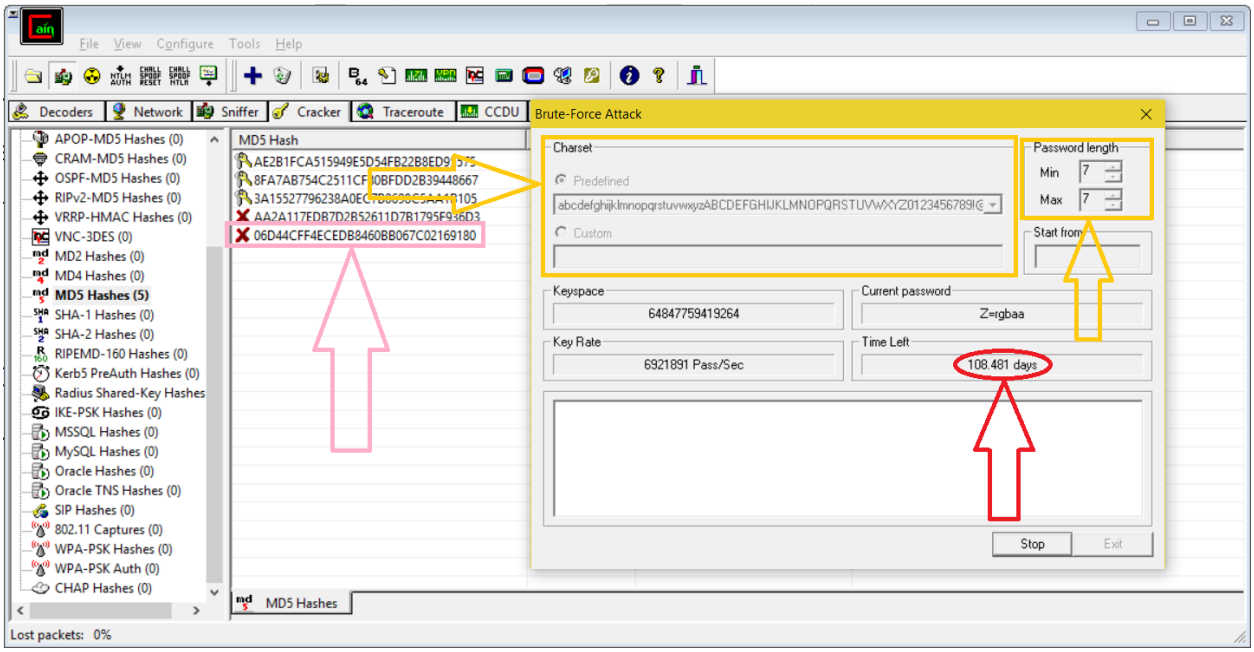
ابتدا برای گذرواژه‌ای ساده داریم:



به دلیل استفاده از ترکیب حروف بزرگ و کوچک، مشاهده می‌شود که حتی حمله‌ی Dictionary نیز به زمان قابل توجهی نیاز دارد تا به نتیجه برسد:



با توجه به نتایج فوق، می‌توان نتیجه گرفت که حمله‌ی Brute-Force نیز در زمانی قابل قبول قادر نیست به نتیجه‌ی مطلوب برسد اما برای اثبات فرضیه‌مان، این نوع حمله را نیز اجرا می‌کنیم:

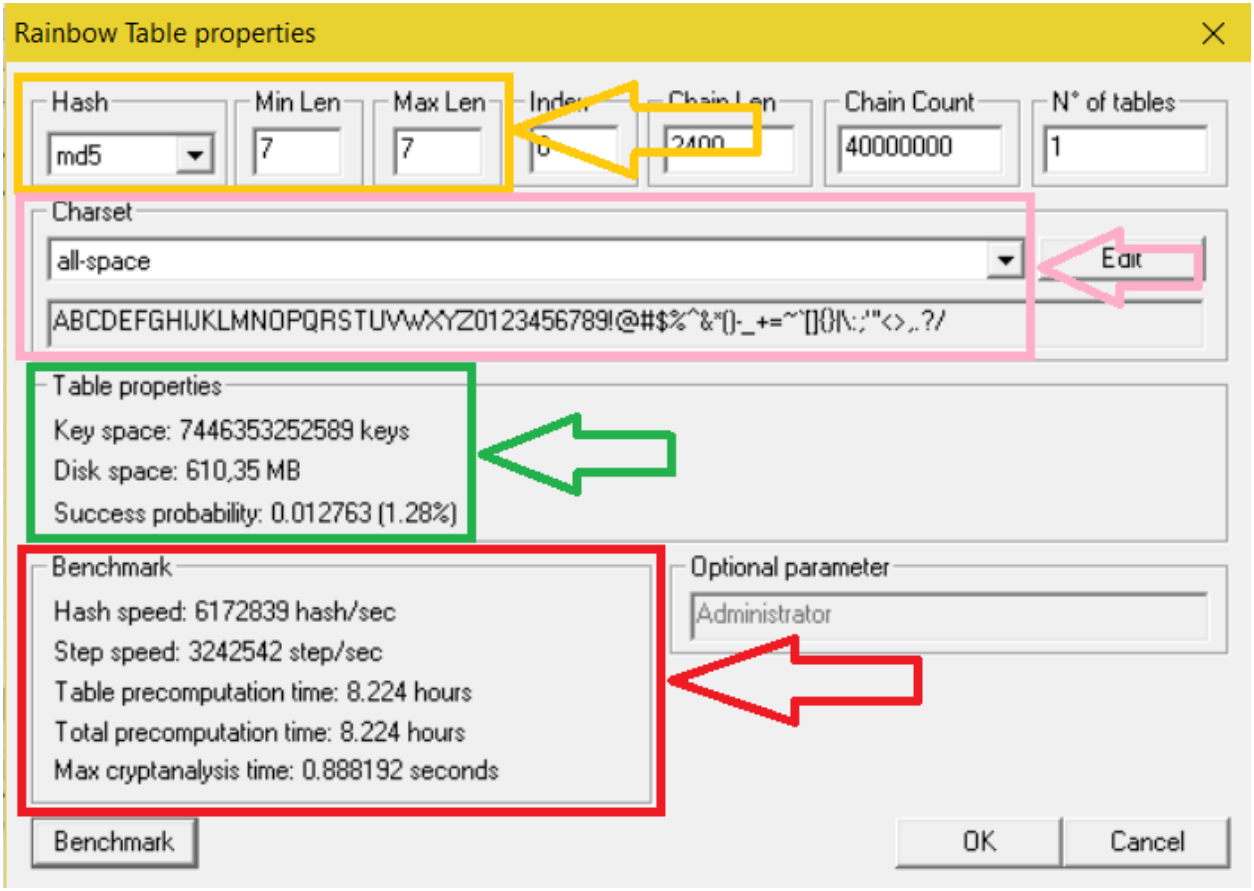


همان‌طور که مشاهده می‌شود، زمان لازم برای به نتیجه رسیدن، بسیار زیاد است و در عمل، استفاده از این روش منطقی به نظر نمی‌رسد.

با توجه به نتایج این دو روش و مقایسه‌ای که میان آن دو انجام دادیم، نتیجه می‌گیریم که روش Dictionary که در آن گذرواژه‌ها با استفاده از یک لیست از گذرواژه‌های رایج مورد بررسی قرار می‌گیرند، در زمان کمتری نتیجه می‌دهد ولی لزوماً به نتیجه نمی‌رسد اما روش Brute-Force که در آن تمام گذرواژه‌های ممکن با استفاده از کاراکترهای معین بررسی می‌شود، حتماً به نتیجه خواهد رسید اما زمان بسیار زیادی نیاز دارد که گاهی اوقات عملاً نشدنی به نظر می‌رسد اما در تئوری قطعاً نتیجه‌بخش است. پس نمی‌توان مطلقاً نظر داد و گفت کدام مؤثرتر است؛ زیرا هرکدام مزایا و معایبی دارند.

اجرای برنامه‌ی winrtgen.exe

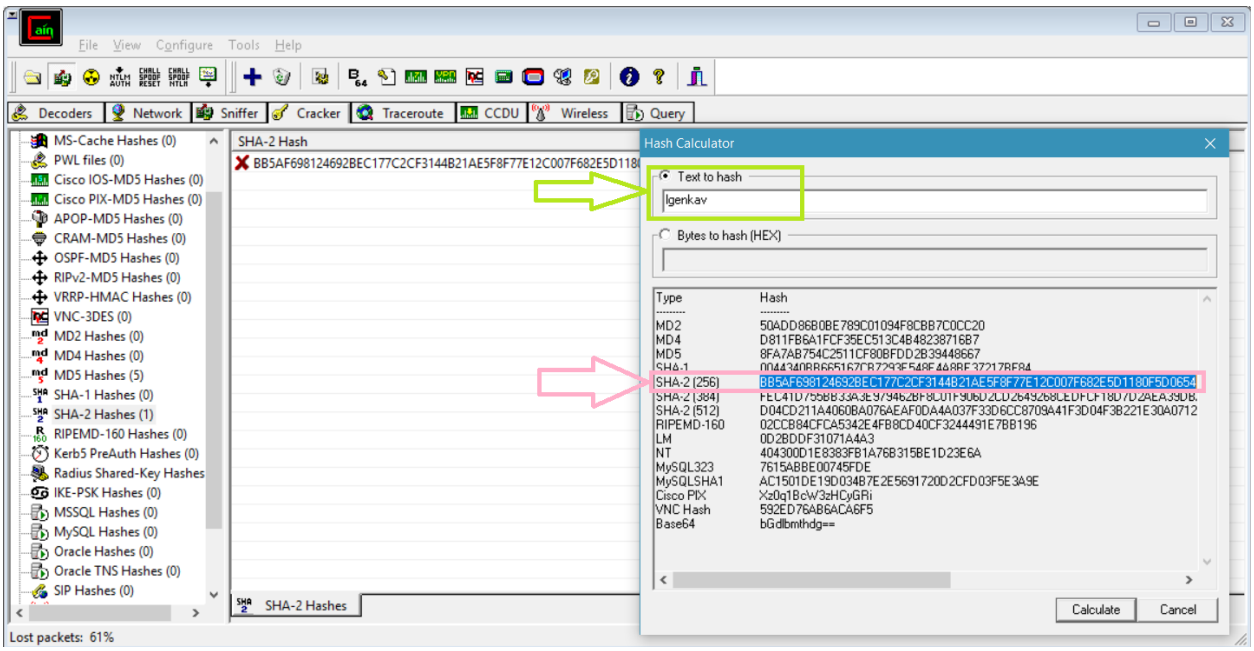
به طور کلی، Rainbow Tableها، جدول‌هایی شامل مقادیر Hashشده‌ی از قبل محاسبه شده است. حال با استفاده از برنامه‌ی فوق، یک تحلیل مختصر ارائه می‌دهیم:



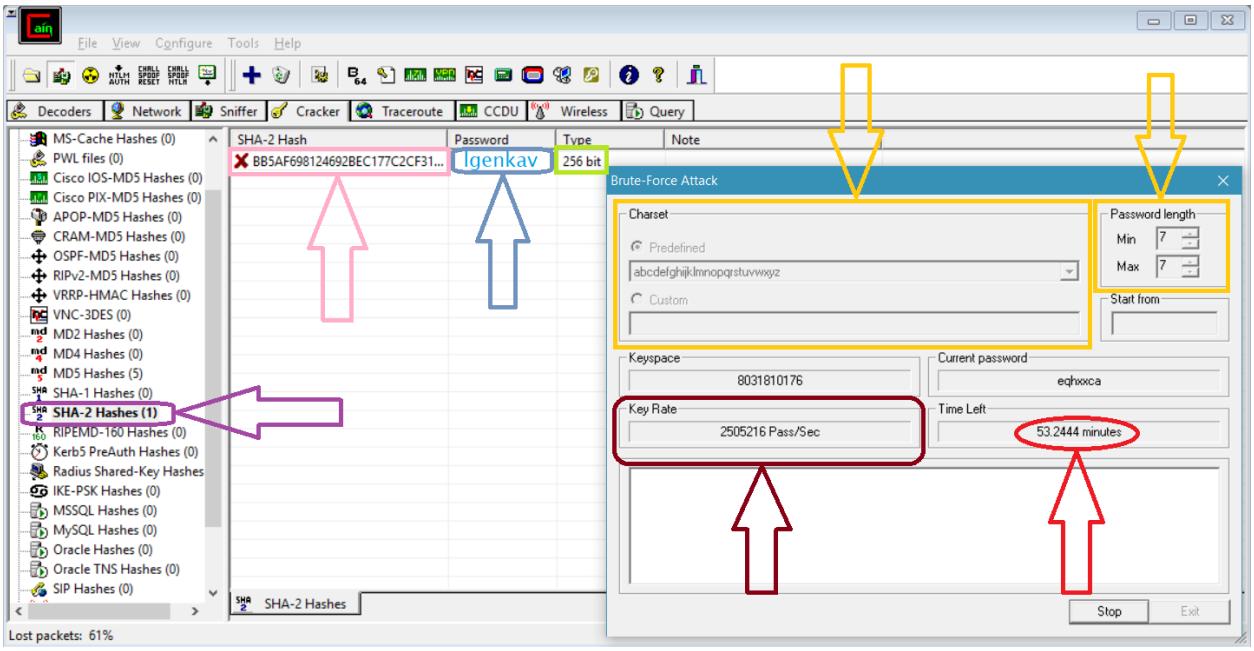
همان‌طور که مشاهده می‌شود، برای دسته‌ی سوم گذرواژه‌ها با طول۷ کاراکتر، به حدود ۸ ساعت زمان برای ساخت این جدول زمان لازم است و حافظه‌ی زیادی نیز می‌طلبد اما در مقابل، حداکثر زمان لازم برای Cryptanalysis، کمتر از یک ثانیه خواهد بود؛ به عبارتی با یک‌بار محاسبه‌ی مقادیر Hash، می‌توان صرفاً به مقایسه‌ی این مقادیر پرداخت و دیگر نیازی به محاسبه‌ی مجدد نیست. به عبارتی دیگر، یک‌بار محاسبات را انجام می‌دهیم و نتیجه را ذخیره می‌کنیم تا در آینده از آن استفاده کنیم و نیازی به صرف زمان مجدد نداشته باشیم.

الگوریتم‌های ذخیره‌سازی مختلف

همان‌طور که قبلاً بیان شد، ما از MD5 Hash برای ذخیره‌سازی گذرواژه‌ها استفاده کردیم. حال از SHA-2 Hash نسخه‌ی ۲۵۶ بیتی استفاده می‌کنیم:



سپس، برای همان گذرواژه‌ای که قبلاً بررسی کردیم، حمله‌ی Brute-Force را دوباره اجرا می‌کنیم:



همان‌طور که مشاهده می‌شود سرعت محاسبه‌ی مقادیر SHA-2 Hash برای گذرواژه‌های یکسان، کمتر از نصف سرعت محاسبه‌ی مقادیر MD5 Hash همان گذرواژه‌هاست و به همین نسبت نیز زمان بیشتری مورد نیاز است تا گذرواژه‌های ذخیره شده با الگوریتم SHA-2 را بررسی کنیم و به نتیجه برسیم. به نظر می‌رسد سرعت محاسبه‌ی MD5 Hash بر روی سخت‌افزار یکسان، بیشتر از انواع دیگر توابع Hash است.

آیا *Cain & Abel* بدافزار است؟

بسیاری از آنتی‌ویروس‌ها و حتی مرورگر *Google Chrome* آن را بدافزار تشخیص می‌دهند اما در حقیقت می‌توان گفت که این ابزار، مانند یک چاقو است که استفاده‌های مختلفی دارد؛ می‌توان با آن آسیب‌پذیری‌های یک شبکه‌ی داخلی را مورد ارزیابی قرار داد و ایرادات آن را برطرف کرد یا می‌توان از آن برای دسترسی و شنود غیرمجاز استفاده کرد. بنابراین در حقیقت، این که چه کسی کاربر نرم‌افزار است و هدف او از استفاده از آن تعیین‌کننده است.

اما فارغ از بحث‌های اخلاقی، می‌توان چنین گفت که این نرم‌افزار رفتارهایی نشان می‌دهد که معمولاً مطلوب کاربران عادی نیستند و از این جهت می‌توان آن را یک بدافزار قلمداد کرد و رفتارهای آن برای کاربران عادی را خطرناک دانست.

اما خود این برنامه، ماهیت یک بدافزار را ندارد و صرفاً یک ابزار کاربردی در زمینه‌ی امنیت اطلاعات است اما آنتی‌ویروس‌ها با در نظر گرفتن این که اکثر کاربران آن‌ها، کاربران عادی هستند و کارهایی از قبیل بررسی آسیب‌پذیری یک شبکه را انجام نمی‌دهند، به جهت رعایت احتیاط، آن را بدافزار قلمداد می‌کنند؛ زیرا ممکن است باعث اختلال در کارهای معمول کاربران شود و عملکرد کل سیستم را تحت تأثیر قرار دهد. به عنوان مثال، این نرم‌افزار به هیچ عنوان نباید توسط یه کارمند عادی بانک، روی یک کامپیوتر اجرا شود؛ زیرا تمام شبکه‌ی داخلی بانک را تحت تأثیر قرار می‌دهد و ممکن است اطلاعات مهم مالی از دست بروند. پس فقط مختصصان امنیت و شبکه باید بتوانند از آن استفاده کنند.