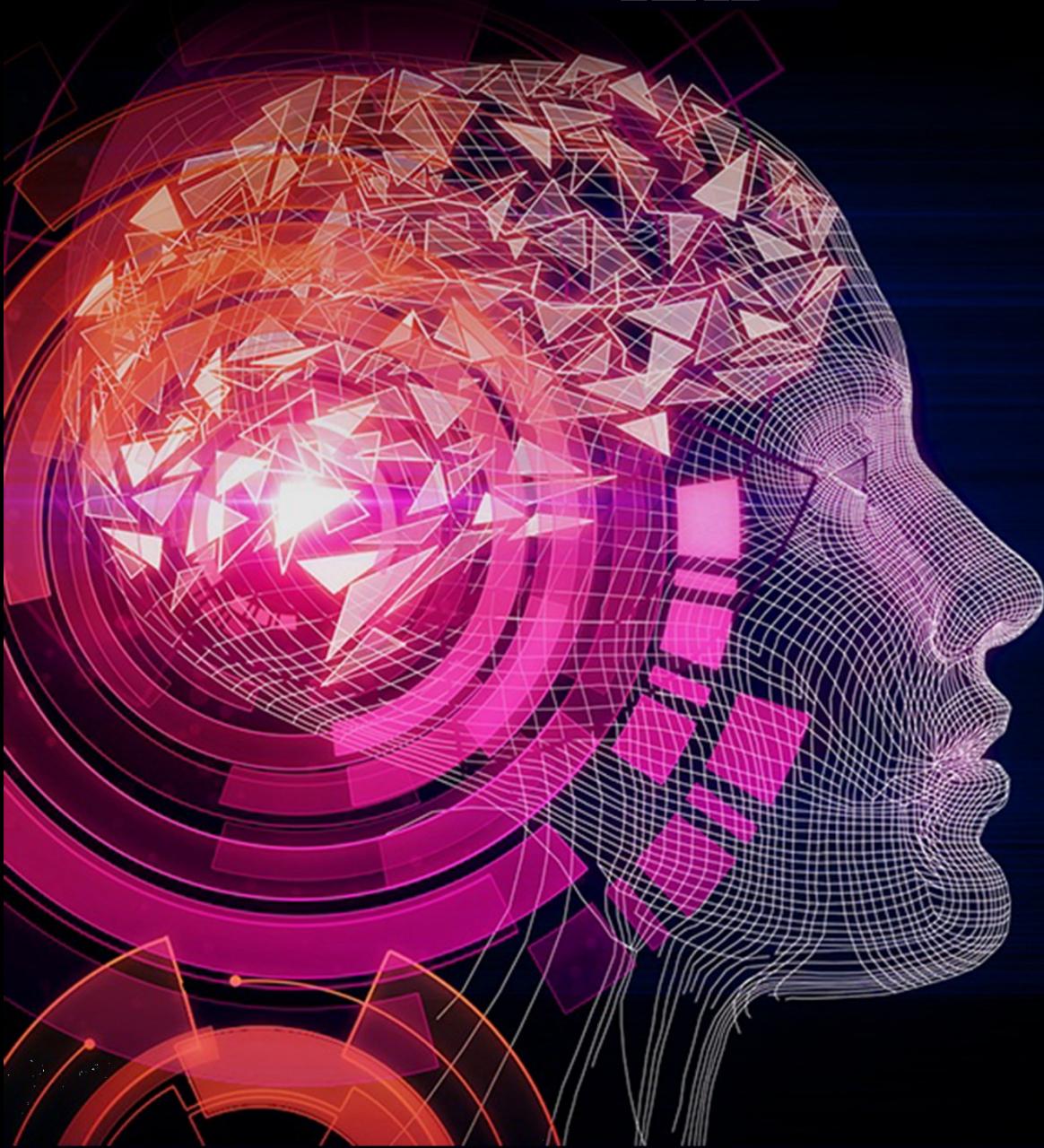


OSINT

Open Source Intelligence

جمع‌آوری موسندهات اطلاعات

KAP



گردآورندگان:

پیام حاتم زاده - کاوه شاکر - آرش قابو

به نام آنکه هستی از او نام یافت

پیشگفتار

در عصری که مردم همه اطلاعات در مورد خودشان را در شبکه‌های اجتماعی از طریق اینترنت قرار می‌دهند، شکار این اطلاعات با کمک OSINT بسیار آسان است. OSINT مخفف Open Source Intelligence یعنی جمع آوری هوشمند اطلاعات می‌باشد. تنها چیزی که مورد نیاز ما است استفاده مناسب از مجموعه‌ای ابزارهای هوشمند متن باز در فضای مجازی است. در این روش ما می‌توانیم تقریباً همه اطلاعات از قبیل شماره کارت‌های اعتباری ، اطلاعات شخصی، پروفایل‌های کامل هر شخص، سرورهای آسیب پذیر ، IP آدرس‌های خصوصی یا داخلی یک سازمان، گذر واژه‌های پنل های مدیریتی، موقعیت جغرافیایی IP آدرس‌ها و در مجموع بیش از ۸۰ درصد از اطلاعات مورد نظر خودمان را می‌توان تنها با استفاده از OSINT به دست آورد. در این کتاب تخصصی ما فقط بر روی ابزارهای OSINT که برای استفاده رایگان هستند متمرکز شده‌ایم. ما از ابزارهای متعددی استفاده خواهیم کرد که از لحاظ دسترسی به منابع عمومی به عنوان یک جادوگر در به دست آوردن اطلاعات محسوب می‌شوند.



هشدار !!!

هر گز موارد آموزش دیده را در مکان هایی که مجوز ارزیابی امنیتی آن را ندارید، تست نمایید. تمامی مطالب ارائه شده در این کتاب جنبه آموزشی داشته و هرگونه استفاده ناصحیح از این تکنیک ها بر عهده استفاده کننده از آن خواهد بود. همچنین تکنیک های بی شماری وجود داشته که به دلایل امنیتی در این کتاب پوشش داده نخواهد شد.

فهرست مطالب

۱	مقدمه
۲	این کتاب چه چیزهایی را شامل می‌شود؟
۲	ابزار مورد نیاز شما چه هستند؟
۲	این کتاب متعلق به کیست؟
۳	فصل ۱: مفاهیم پایه
۳	مقدمه
۴	اینترنت
۶	آدرس IP
۷	پورت
۸	پروتکل
۸	مک آدرس
۹	پست الکترونیک
۹	نام دامنه
۱۰	نشانی اینترنی - URL
۱۱	سرور
۱۱	جستجوگر وب
۱۱	مرورگر اینترنت
۱۲	مجازی سازی
۱۲	مرور وب
۱۵	محیط آزمایشگاه
۱۷	زبان برنامه نویسی
۱۸	مرورگر
۲۰	فصل ۲: اطلاعات متن باز و جستجوی پیشرفته رسانه های اجتماعی
۲۰	مقدمه
۲۱	جمع آوری هوشمند اطلاعات منبع باز
۲۲	چگونه استفاده OSINT از موتورهای جستجو
۲۵	وب ۲.۰
۲۶	رسانه های اجتماعی هوشمند
۲۷	شبکه های اجتماعی

۳۳.....	تکنیک‌های جستجو پیشرفته برای برخی از رسانه‌های اجتماعی خاص
۴۰.....	جستجو در وب‌سایت اجتماعی باز
۴۱.....	وب ۳.۰
۴۳.....	فصل ۳: در ک مرورگرها
۴۳.....	مقدمه
۴۴.....	نحوه عملکرد مرورگر
۴۴.....	تاریخچه مرورگرها
۴۵.....	معماری مرورگرها
۴۷.....	ویژگی‌های مرورگرها
۵۱.....	مرورگرها خام
۶۵.....	افرونهایا
۷۳.....	خطرات ناشی از مرورگرها
۷۴.....	فصل ۴: جستجو در وب
۷۴.....	مقدمه
۷۵.....	متا جستجو
۷۸.....	جستجوی افراد
۸۴.....	جستجوی شرکت و یا کسبوکار
۹۰.....	جستجوی رسانه‌های اجتماعی
۹۸.....	اطلاعات فنی
۱۰۲.....	جستجوی مجدد تصویر
۱۰۴.....	متفرقه
۱۱۱.....	فصل ۵: جستجوی پیشرفته وب
۱۱۱.....	مقدمه
۱۱۲.....	گوگل
۱۲۰.....	بینگ
۱۲۳.....	یاهو
۱۲۶.....	یاندکس
۱۳۹.....	فصل ۶: ابزارها و تکنیک‌های OSINT
۱۳۹.....	مقدمه
۱۴۰.....	CREEPY
۱۴۳.....	THEHARVESTER

۱۴۶.....	SHODAN
۱۴۸.....	SEARCH DIGGITY
۱۵۲.....	Recon-ng
۱۶۱.....	YAHOO PIPES
۱۶۴.....	MALTEGO
۱۷۴.....	فصل ۲: فرا داده
۱۷۴.....	مقدمه
۱۷۵.....	ابزار استخراج فرا داده
۱۸۸.....	ابزار حذف و یا DLP فراداده‌ها
۱۹۱.....	فصل ۸: ناشناس بودن آنلاین
۱۹۱.....	مقدمه
۱۹۱.....	ناشناس بودن آنلاین
۱۹۲.....	چرا نیاز به ناشناس بودن آنلاین داریم؟
۱۹۳.....	راه حل‌های ناشناس بودن آنلاین
۱۹۳.....	پروکسی
۱۹۶.....	پروکسی در اصطلاح ناشناس ساز
۱۹۶.....	انواع راه حل‌های پروکسی
۲۰۷.....	چگونگی راه اندازی دستی پروکسی در مرورگرها
۲۰۸.....	شبکه خصوصی مجازی
۲۱۲.....	شبکه‌های ناشناس
۲۱۴.....	پروژه اینترنت نامرئی
۲۱۸.....	فصل ۹: کاوش تاریک ترین گوشه‌های اینترنت (DEEPWEB)
۲۱۸.....	مقدمه
۲۱۹.....	CLEARWEB
۲۱۹.....	DARKWEB
۲۱۹.....	DEEPWEB
۲۲۰.....	چرا از deepweb استفاده می‌شود؟
۲۲۱.....	چرا به deepweb نیازی ندارید؟
۲۲۱.....	سروریس‌های DARKNET
۲۳۶.....	فصل ۱۰: مدیریت داده‌ها
۲۳۶.....	مقدمه

۲۳۷.....	داده
۲۳۷.....	اطلاعات
۲۳۷.....	فهیم
۲۴۰.....	ابزار مدیریت داده‌ها و تجزیه و تحلیل اطلاعات
۲۵۴.....	فصل ۱۱: امنیت آنلاین
۲۵۴.....	مقدمه
۲۵۷.....	بدافزار
۲۵۸.....	سیلاگر
۲۵۸.....	فیشینگ
۲۵۹.....	کلاهبرداری آنلاین
۲۶۰.....	دست آویزهای هکینگ
۲۶۱.....	رمز عبور ضعیف
۲۶۱.....	SHOULDER SURFING
۲۶۱.....	مهندسی اجتماعی
۲۶۲.....	آنٹی ویروس
۲۶۳.....	شناسایی فیشینگ و یا SCAMS
۲۶۴.....	به روز رسانی سیستم عامل و سایر برنامه‌ها
۲۶۴.....	افزونه‌های امنیتی
۲۶۶.....	ابزار امنیتی
۲۶۷.....	سیاست گذرواژه
۲۶۸.....	احتیاط در برابر مهندسی اجتماعی
۲۶۹.....	رمزگذاری داده‌ها
۲۷۱.....	فصل ۱۲: مبانی تجزیه و تحلیل شبکه‌های اجتماعی
۲۷۱.....	مقدمه
۲۷۲.....	گره‌ها
۲۷۲.....	لبه‌ها
۲۷۲.....	شبکه
۲۷۲.....	GEPHI
۲۷۵.....	صفات گره‌ها
۲۷۵.....	صفات لبه‌ها
۲۸۴.....	فصل ۱۳: پایتون

۲۸۴.....	مقدمه
۲۸۵.....	برنامه نویسی و اسکریپت نویسی
۲۸۵.....	مقدمه پایتون
۲۸۶.....	نصب پایتون
۲۸۶.....	اجرای پایتون
۲۸۶.....	برنامه HELLO WORLD
۲۸۸.....	انواع داده
۲۹۲.....	INDENTATION
۲۹۵.....	ماژول‌ها
۲۹۶.....	توابع
۲۹۸.....	کار با فایل‌ها
۳۰۱.....	ورودی کاربر
۳۰۲.....	اشتباهات رایج
۳۱۴.....	فصل ۱۴: مطالعات موردنی
۳۱۴.....	مقدمه
۳۱۴.....	مطالعه موردنی ۱ : MASHUP BLACKHAT
۳۱۶.....	مطالعه موردنی ۲ : A DEMO THAT CHANGED AUDIENCE VIEW
۳۱۹.....	مطالعه موردنی ۳ : AN EPIC INTERVIEW
۳۲۷.....	ماشین‌های Maltego
۳۳۲.....	فصل ۱۵: سایر موضوعات مرتبط
۳۳۲.....	مقدمه
۳۳۲.....	رمزگاری
۳۳۴.....	بازیابی / ترمیم داده‌ها
۳۳۷.....	INTERNET RELAY CHAT
۳۳۹.....	بیت کوین

مقدمه

در یک روز کاری معمولی قصد ارزیابی امنیتی شبکه‌ای را داشتیم، بنابراین پویش‌های خودکار و دستی را انجام دادیم. پس از انجام این فرایند، اطلاعات جالبی در مورد هدف پیدا کردیم. سپس شروع به پویش عمیق کردیم و به اطلاعاتی کافی در مورد هدف دست یافتیم و این فرآیند را به پایان رسانده و گزارش را به مشتری ارسال کردیم و آن‌ها از نتایج خوشحال شدند.

اواخر همان شب در مورد اسکن‌ها بحث کردیم و متوجه شدیم که در مورد هدف به دست آمد، در واقع اطلاعات عمومی بود. هدف ما، بیش از حد، اطلاعات خود را در فضای عمومی (اینترنت) منتشر کرده بود. این پایان کار در آن پروژه بود و تقریباً آن را فراموش کردیم. زمانی که در پروژه دیگری کار می‌کردیم، همین اتفاق دوباره افتاد؛ بنابراین تصمیم گرفتیم تمام ابزارها و تکنیک‌هایی را که از آن‌ها استفاده کردیم، مستند کنیم. هرگاه با روش جدیدی برای کشف اطلاعات عمومی مواجه شدیم، آن را به این مستند اضافه کرده و به‌زودی متوجه شدیم که مستند بسیار طولانی به وجود آمده و ما باید آن را طبقه‌بندی و فیلتر می‌کردیم.

اگر چه موضوعات شناخته شده و تیم‌ها به‌طور گسترده‌ای در حال استفاده از این روش‌ها هستند اما تلاش کردیم تا اطلاعاتی در خصوص آن در اینترنت به دست آوریم که هیچ چیز قابل توجهی نیافتنیم؛ بنابراین تصمیم گرفتیم، مستندمان را به یک کتاب تبدیل کنیم.

بنابراین فهمیدیم که اطلاعات عمومی زیادی وجود دارد که به راحتی قابل دسترس هستند. اغلب آن‌ها ممکن است در نگاه اول بسیار مفید نباشند، اما هنگامی که جمع‌آوری شده و همبسته می‌شوند، می‌توانند نتایج فوق العاده‌ای به ارمغان بیاورند. همچنین متوجه شدیم که این روش‌ها نه تنها برای جمع‌آوری اطلاعات در مورد اهداف کاربرد دارد، بلکه بسیاری از حرفه‌های دیگر نیز مانند بازاریابی از آن‌ها استفاده می‌کنند؛ بنابراین سعی کردیم که این

کتاب را به صورت ساده نگارش کنیم، بدون اینکه به جزئیات فنی اشاره‌ای کنیم. این کتاب از شناسایی اصول اولیه به منظور یادگیری بیشتر ابزارهایی که قبلًا با آن‌ها آشنا بوده‌ایم، شروع کرده و به موضوعات فنی بیشتری می‌پردازد.

این کتاب چه چیزهایی را شامل می‌شود؟

جمع‌آوری اطلاعات هوشمند از وب با توجه به پیچیدگی‌ها و وابستگی‌های متقابل به بخش‌های مختلف تقسیم شده است. اولین بخش در مورد اصول و اسکن عمیق است که اکثر ما با آن آشنا هستیم. بخش میانی در مورد ابزار و تکنیک‌های پیشرفته صحبت می‌کند و در بخش پایانی در مورد استفاده و اجرای آنچه در بخش‌های قبلی بحث کردہ‌ایم، صحبت می‌کنیم.

در حالی که کتاب را دنبال می‌کنید، پیشنهاد نمی‌شود که فقط آن را بخوانید، بلکه تمامی مطالب گفته شده را تمرین کنید. نمونه‌ها و تصاویر برای درک چگونگی کار و نتایج مورد انتظار هستند. این کتاب فقط در مورد استفاده از ابزارها نیست بلکه درک نحوه انجام کار آن‌ها و همچنین اطلاعات جمع‌آوری شده، می‌باشد. اکثر ابزارها قادر به جمع‌آوری اطلاعات می‌باشند، اما برای تکمیل، نیاز داریم تا این اطلاعات را به یکدیگر متصل کنیم. از سوی دیگر، ابزاری که استفاده خواهیم کرد ممکن است به روزرسانی، اصلاح و یا حتی بازنویسی شوند، بنابراین از نسخه به روز آن‌ها استفاده کنید.

ابزار مورد نیاز شما چه هستند؟

رایانه و یا لپ‌تاپ با هر سیستم عامل. مرورگرهای مختلف مانند موزیلا فایرفاکس و یا کروم و اتصال به اینترنت. خواندن‌گان برای دریافت و نصب ابزارها بر اساس نیاز هر فصل راهنمایی خواهند شد.

این کتاب متعلق به کیست؟

این کتاب به طور عمده به متخصصین امنیت اطلاعات و مدیریت ریسک، متمن‌کر می‌شود، اما برای هکرها نیز مفید خواهد بود و برای افرادی که نیاز به جمع‌آوری اطلاعات به عنوان بخشی از کار روزانه خود دارند مانند بازاریابی، فروش، روزنامه‌نگاری و غیره. این کتاب را می‌توان در هر دوره امنیت اطلاعات تا سطح متوسط برای مرحله شناسایی ارزیابی امنیتی استفاده کرد.

ما امیدواریم که شما به عنوان یک خواننده چیزی جدیدی را یاد بگیرید و در زندگی روزمره بتوانید از آن استفاده نمایید.

فصل ۱: مفاهیم پایه^۱

مقدمه

عصر اطلاعات، دوره تکامل انسان است که در آن همه ما رشد می‌کنیم. امروزه اینترنت بخش مهمی از زندگی ماست. همه ما زندگی دوگانه‌ای را شروع کرده‌ایم؛ یکی زندگی فیزیکی و دیگری زندگی مجازی (آنلاین)، جایی که ما به عنوان یک موجود مجازی هستیم. در این زندگی مجازی ما، نام‌های کاربری، نام‌های مستعار، تصاویر پروفایل و اطلاعات دیگری در مکان‌های مختلف داریم. ما اطلاعات عمده و گاهی ناخواسته‌ای در این دنیای مجازی به اشتراک می‌گذاریم. اگر از خودمان پرسیم در چند وب‌سایت ثبت‌نام کرده‌ایم، احتمالاً قادر به پاسخگویی به این سؤال به صورت دقیق نخواهیم بود. تعریف اجتماعی بودن در حال تغییر است از دیدار افراد به صورت شخصی و بودن در سایت‌های مختلف شبکه‌های اجتماعی. به نظر می‌رسد که تکنولوژی به سرعت در حال رشد است و ما باید به سرعت با آن خودمان را وفق شویم.

^۱ Information Overload

تکامل قدرت محاسبات بسیار سریع است. از دوران محدود داده‌ها به زمانی که اطلاعات زیادی وجود دارد، رسیدیم. فن‌آوری‌های امروز مانند داده‌های بزرگ^۱، رایانه‌های ابری^۲، کلمات کلیدی صنعت فناوری اطلاعات هستند که هر دو با مدیریت حجم زیادی از داده‌ها روبرو هستند. مطمئناً این تکامل، دارای مزايا و منافعی است؛ از دیدگاه استخراج اطلاعات، ما باید هر دو را درک و ارزیابی کنیم که چگونه می‌توانیم از مزیت آن‌ها استفاده کنیم. مانع اصلی در این مسیر، کمبود اطلاعات نیست، بلکه به صورت شگفت‌آور، فراوانی آن است. در این مرحله آنچه نیاز داریم، روش‌های مناسب و کارآمد برای استخراج هوشمند اطلاعات از این اقیانوس داده‌های عظیم است.

استخراج اطلاعاتی که می‌تواند منجر به نتیجه مثبتی شود، مانند جستجوی یک سوزن در یک انبار کاه است. اگرچه گاهی اوقات اطلاعات به صورت آشکار، آزاد و رایگان هستند، اما اگر ندانیم چگونه می‌توان آن را به موقع پیدا کنیم، منابع حیاتی زیادی را هدر خواهیم داد. در طول این کتاب با ابزار و تکنیک‌های عملی که به ما کمک می‌کنند تا اطلاعات را به موقع به دست آوریم، آشنا می‌شویم و همچنین به تجزیه و تحلیل چنین اطلاعاتی برای تصمیم‌گیری بهتر خواهیم رسید. این امر می‌تواند تفاوت زیادی در افرادی که با چنین اطلاعاتی به عنوان بخشی از کار روزانه خود درگیر هستند (مانند ارزیابان امنیتی، تحلیل گران حرفه‌ای و غیره) ایجاد کند. اکنون اینترنت را که همه ما تا به حال از آن استفاده کرده‌ایم، تشریح می‌کنیم.

اینترنت^۳

اینترنت، همان‌طور که می‌دانیم از پروژه‌ای DARPA در وزارت دفاع ایالات متحده، تکامل یافته است. شبکه اولیه برای اتصال دانشگاه‌ها و آزمایشگاه‌های تحقیقاتی در ایالات متحده استفاده شد. این پدیده به آرامی در سراسر جهان توسعه یافته و امروزه شبکه‌ای غولپیکر را به وجود آورده است که به ما اجازه می‌دهد تا در عرض چند ثانیه با کل جهان ارتباط برقرار کنیم.

¹ Big Data

² Cloud Computing

³ INTERNET

تعريف

به سادگی می‌توان گفت که اینترنت یک شبکه جهانی از رایانه‌های مرتبط با استفاده از روتراها و سرورهای اختصاصی است که به کاربران نهایی امکان دسترسی به داده‌های پراکنده در سراسر جهان را می‌دهد. این رایانه‌های متصل با مجموعه‌ای خاص از قوانین ارتباط برقرار می‌کنند (مانند IP یا پروتکل اینترنت برای انتقال داده‌ها).

چطور کار می‌کند؟

باید قبل از هر چیز بدانید که اینترنت چگونه کار می‌کند. پس وظیفه ماست که برخی از اصول را روشن کنیم، البته نه به صورت عمیق. همان‌طور که در بالا ذکر شد، اینترنت یک شبکه جهانی از رایانه‌های متصل است و تعداد زیادی از دستگاه‌ها به طور مشترک کار اینترنت را انجام می‌دهند، مثلاً روتراها، سرورهای، سوئیچ‌ها با سخت‌افزارهای دیگر مانند کابل‌ها، آنتن‌ها و غیره. همه این دستگاه‌ها با یکدیگر شبکه‌ای را تشکیل می‌دهند که کار انتقال داده را انجام می‌دهند.

همان‌طور که در هر ارتباطی شما باید نقاط انتهایی، میانی و پروتکل‌ها را داشته باشید، اینترنت نیز با این مفاهیم کار می‌کند. نقاط پایانی رایانه‌ها، لپ‌تاپ‌ها، رایانه‌های لوحی، تلفن‌های هوشمند و یا هر دستگاه دیگری است که کاربران از آن‌ها استفاده می‌کنند. نقاط میانی، سرورهای اختصاصی و روتراها متصل به یکدیگر هستند و پروتکل‌ها مجموعه‌ای از قوانینی هستند که ماشین‌ها برای انجام وظایف استفاده می‌کنند پروتکل کنترل انتقال IP / TCP. برخی از شیوه‌های انتقال داده‌ها عبارت‌اند از کابل تلفن، فیبر نوری، امواج رادیویی و غیره.

وب جهان‌گستر^۱

وب جهان‌گستر (WWW) که به سادگی به عنوان وب شناخته شده است زیر مجموعه‌ای از اینترنت و یا به عبارت ساده فقط بخشی از اینترنت است. وب شامل تمام وب‌سایت‌های عمومی متصل به اینترنت می‌باشد، از جمله میزبان‌هایی که به آن‌ها دسترسی پیدا می‌کنند.

این اساساً ساختاری است که شامل اسناد متصل بوده و در قالب صفحات وب نمایش داده می‌شود. این صفحات وب ممکن است حاوی انواع مختلف رسانه‌ای مانند متن ساده، تصاویر، فیلم‌ها و غیره باشند و از طریق برنامه کاربردی که معمولاً یک مرورگر وب است، قابل دسترسی هستند و شامل تعداد زیادی از صفحات متصل هستند.

^۱ World Wide Web



تفاوت‌های اساسی بین اینترنت و وب

برای بسیاری از ما وب مترادف با اینترنت است، هرچند که وب به اینترنت کمک می‌کند، اما هنوز هم بخشی از آن است. اینترنت پدر وب است. در وب، اطلاعات و مدارک توسط آدرس وب‌سایت‌ها (URL‌ها) و لینک‌ها، مرتبط هستند. آن‌ها توسط مرورگر هر دستگاه نهایی مانند رایانه یا گوشی هوشمند با استفاده از پروتکل HTTP و در حال حاضر با استفاده از پروتکل HTTPS قابل دسترسی هستند. HTTP یکی از پروتکل‌هایی است که در اینترنت استفاده می‌شود مانند پروتکل انتقال فایل (FTP)، پروتکل انتقال ایمیل ساده (SMTP) و غیره که بعداً مورد بحث قرار می‌گیرند.

بنابراین در حال حاضر با درک اصول اولیه اینترنت و وب، می‌توانیم بعضی از اصطلاحات و تکنولوژی‌های اولیه را یاد بگیریم که در طول این کتاب اغلب از آن‌ها استفاده می‌کنیم.

آدرس IP

هر کسی که تا به حال از رایانه استفاده کرده، باید در مورد آدرس IP چیزی شنیده باشد. اگرچه بعضی از ما ممکن است جزئیات فنی آن را درک نکرده باشیم، اما همه ما می‌دانیم که با آدرس رایانه مرتبط است. به عبارت ساده، آدرس IP، آدرس مجازی یک رایانه و یا یک دستگاه شبکه است که منحصر آن دستگاه را در یک شبکه مشخص می‌کند. اگر دستگاه ما به یک شبکه متصل باشد، می‌توانیم به راحتی آدرس IP دستگاه را پیدا کنیم. در مورد کاربر ویندوز می‌توان آن را باز کردن خط فرمان و تایپ کردن دستور "ipconfig" انجام داد. تقریباً به صورت مشابه در لینوکس و یا مک، باید ترمینال را باز کنیم و "ifconfig" را تایپ تا آدرس IP مربوط به سیستم را پیدا کنیم.

آدرس IP به عنوان آدرس منطقی نیز شناخته شده و دائمی نیست. پروتکل آدرس IP معمول IPv4 است، هرچند نسخه جدیدتر آن با نام IPv6 به زودی جایگزین آن می‌شود. IP به صورت چهار عدد ددهدی جداده توسط نقطه نشان داده می‌شود. به عنوان مثال، "۱۹۲.۱۶۸.۰.۱" که از ۰.۰.۰.۰ شروع و به ۲۵۵.۲۵۵.۲۵۵ ختم می‌شوند.

هنگامی که سعی کنیم آدرس IP مربوط به سیستم خود را با استفاده از هر یک از روش‌های ذکر شده در بالا پیدا کنیم، متوجه خواهیم شد که آدرس در محدوده ذکر شده قرار دارد.

آدرس IP از دو نوع است:

(۱) آدرس IP خصوصی

(۲) آدرس IP عمومی

آدرس IP خصوصی برای شناسایی یک دستگاه در یک شبکه محلی استفاده می‌شود که سیستم ما را از سیستم‌های دیگر منحصر به فرد می‌نماید. مجموعه‌ای از آدرس‌هایی که برای آدرس IP خصوصی استفاده می‌شود، وجود دارند:

۱۹۲.۱۶۸.۲۵۵.۲۵۵-۱۹۲.۱۶۸.۰.۰ ۱۷۲.۳۱.۲۵۵.۲۵۵-۱۷۲.۱۶۰.۰ ۱۰.۲۵۵.۲۵۵.۲۵۵-۱۰.۰.۰.۰

روش فوق می‌تواند برای بررسی آدرس IP خصوصی مورد استفاده قرار گیرد. آدرس IP عمومی آدرسی است که منحصراً یک سیستم را در اینترنت شناسایی می‌کند که به طور کلی توسط ارائه‌دهنده‌گان سرویس اینترنت^۱ ارائه می‌شود. زمانی که سیستم ما به اینترنت متصل است می‌توانیم آن را بررسی کنیم. این آدرس می‌تواند هر چیزی غیر از محدوده آدرس IP خصوصی باشد. ما می‌توانیم آن را در سیستمان (به رغم هر سیستم‌عامل) با مرور "whatsmyipaddress.com"^۲ بررسی کنیم.

پورت^۲

همه ما از پورت‌ها (در گاه) مانند پورت USB، پورت صوتی و غیره آگاه هستیم؛ اما در اینجا درباره پورت‌های سخت‌افزاری صحبت نمی‌کنیم؛ بلکه منظور ما پورت منطقی است. به صورت ساده، پورت‌ها را می‌توان به عنوان نقطه ارتباط تعریف کرد. پیش از این در مورد چگونگی شناسایی یک سیستم در شبکه بحث کردیم، سپس برای برقراری ارتباط با سیستم مقصد، آدرس مقصد با استفاده از شماره پورت پروتکل مربوطه تکمیل می‌شود. به‌زودی در مورد پروتکل‌ها بحث خواهیم کرد، اما در حال حاضر فرض بر این است که پروتکل مجموعه‌ای از قوانینی است که پس از آن، همه طرف‌های ارتباط برای تبادل داده‌ها از آن پیروی می‌کنند. فرض کنید یک وب‌سایت در یک سیستم با آدرس "۱۹۲.۱۶۸.۰.۲" اجرا می‌شود و ما می‌خواهیم با آن سرور از یک سیستم دیگر متصل به همان شبکه با آدرس "۱۹۲.۱۶۸.۰.۲" ارتباط برقرار کنیم؛ بنابراین فقط باید مرورگر را باز کرده و

¹ ISP

² PORT

"۱۹۲.۱۶۸.۰.۲:۸۰" را که در آن "۸۰" شماره پورت مورد استفاده برای ارتباط است و با پروتکل http مرتبط است، تایپ کنیم. اعداد پورت در محدوده ۰ تا ۶۵۵۳۵ قرار دارند.

پروتکل

پروتکل مجموعه استاندارد مقررات و الزامات مورد استفاده در ارتباط بین سیستم منبع و مقصد است که نحوه اتصال و مبادله داده‌ها با یکدیگر را مشخص می‌کند. به سادگی می‌توان اظهار داشت، مجموعه‌ای از قوانینی است که برای برقراری ارتباط بین دو نهاد در یک رسانه دنبال می‌شود.

برخی از پروتکل‌های محبوب و شماره‌های پورت مربوطه عبارت‌اند از:

- ❖ ۲۱ برای انتقال فایل استفاده می‌شود – پورت ۲۰، ۲۱
- ❖ ۲۲ SSH^۱ برای برقراری ارتباط امن با ماشین‌های دیگری استفاده می‌شود – پورت ۲۲
- ❖ ۲۳ Telnet برای ارتباط داده با دستگاه دیگری استفاده می‌شود – پورت ۲۳
- ❖ ۲۵ SMTP^۲ برای مدیریت ایمیل‌ها مورد استفاده قرار می‌گیرد – پورت ۲۵
- ❖ ۸۰ HTTP برای انتقال داده‌های وب استفاده می‌شود – پورت ۸۰

مک آدرس^۳

مک آدرس نیز به عنوان آدرس فیزیکی شناخته شده است. مک آدرس یا آدرس کنترل دسترسی به رسانه به صورت منحصر به فرد به واسطه شبکه توسط سازنده، اختصاص داده شده است. واسط شبکه رابطی است که برای اتصال کابل شبکه مورد استفاده قرار می‌گیرد. مک آدرس را با شماره‌ای هگزادسیمال نشان می‌دهند. به عنوان مثال A2: BA: C1: 2B: 1C:00 که سه مجموعه اول هگزادسیمال عدد تولید کننده واسط و مابقی شماره سریال آن می‌باشد. اکنون مک آدرس سیستم خودتان را پیدا کنید.

در مورد کاربر ویندوز می‌توان آن را با زدن خط فرمان و تایپ کردن دستور "ipconfig -all" و یا "getmac" انجام داد. تقریباً مشابه آن برای کاربر لینوکس و مک است. ما باید ترمینال را باز کنیم و "ifconfig -a" را تایپ

¹ File Transfer Protocol

² Secure Shell

³ Simple Mail Transfer Protocol

⁴ MAC Address

⁵ Interface

کنیم تا مک آدرس مربوط به سیستم را پیدا کنیم. حالا اجازه دهید مک آدرس رابط شبکه سیستمان و نام سازنده را پیدا کنیم. از سه کاراکتر اول هگزادرسیمال در گوگل برای نام سازنده جستجو کنید.

پست الکترونیک^۱

پست الکترونیک و یا ایمیل یکی از تکنولوژی‌هایی است که به طور گسترده‌ای برای ارتباطات دیجیتال استفاده می‌شود. پست الکترونیک راه حلی برای تبادل پیام دیجیتال از فرستنده به گیرنده است. ساختار کلی آدرس پست الکترونیک "username@domainname.com" است. بخش اول که قبل از نماد "@" است، نام کاربری است که هر کاربر برای استفاده از این سرویس با آن ثبت‌نام کرده است. قسمت دوم، نام دامنه ارائه دهنده سرویس پست الکترونیکی است. امروزه هر سازمانی که وب‌سایتی با یک نام دامنه ثبت کرده، سرویس پست الکترونیک را نیز ایجاد می‌کند؛ بنابراین اگر ما در یک شرکت با نام دامنه "xyz.com" کار کنیم، باید پست الکترونیک ما "ususername @ xyz.com"^۲ باشد. برخی از ارائه‌دهنده‌گان پست الکترونیکی محبوب گوگل، یاهو، AOL، Rediff و غیره هستند.

نام دامنه^۳

نام دامنه (DNS) یک سیستم نام‌گذاری برای منابع متصل به اینترنت است. این ساختار سلسله مراتبی نام‌گذاری سرورهای مختلف پراکنده در اینترنت را حفظ می‌کند.

برای مثال، google.com نام دامنه شرکت گوگل است که سرورهای خود را در مکان‌های مختلف قرار می‌دهد و به سرورهای مختلف آدرس‌های IP مختلف اختصاص داده می‌شود؛ بنابراین DNS اجازه می‌دهد یک کاربر فقط نام را به جای همه آن آدرس‌های IP به یاد داشته باشد. در این مثال ما می‌توانیم نام دامنه را به دو قسمت تقسیم کنیم. بخش اول نام عمومی است که به‌طور کلی با توجه به نام سازمان و یا هدف دامنه، خریداری شده است. گوگل نام سازمان در google.com است. قسمت دوم در مورد نوع دامنه توضیح می‌دهد مانند ".com" که دامنه تجاری است. این پسوند همچنین به عنوان دامنه‌های سطح بالا^۳ شناخته می‌شوند (TLDs). برخی از نمونه‌های TLDS عبارت‌اند از:

❖ net سازمان شبکه‌ای

¹ Email

² DOMAIN NAME

³ top level domains

- ❖ org سازمان‌های تجاری
- ❖ edu مؤسسه‌های آموزشی
- ❖ gov سازمان‌های دولتی
- ❖ mil اهداف نظامی

یکی دیگر از محبوب‌ترین پسوندها و یا دامنه سطح بالا، کد کشورها (ccTLD) است. برخی از نمونه‌ها عبارت‌اند از:

- ❖ in هند
- ❖ Us ایالات متحده
- ❖ UK بریتانیا
- ❖ IR ایران

DNS بخشی جدایی‌ناپذیر از اینترنت است. ما به‌سادگی باید نام منبع را به یاد داشته باشیم و DNS آن را به یک آدرس مجازی تبدیل می‌کند که به‌راحتی در اینترنت قابل دسترسی است. به عنوان مثال، google.com به آدرس 74.125.236.137 برای یک منطقه خاص در اینترنت تبدیل می‌شود.

نشانی اینترنتی - URL

یک URL می‌تواند به عنوان آدرس برای دسترسی به منابع وب استفاده شود که اساساً به عنوان آدرس وب شناخته می‌شود. به عنوان مثال، http://www.example.com/test.jpg را می‌توان به پنج قسمت تقسیم کرد که عبارت‌اند از:

- 1) http
- 2) www
- 3) example
- 4) com
- 5) /test.jpg

بخش اول پروتکل ارتباطی را مشخص می‌کند که http است. بخش دوم دامین اصلی را مشخص کرده و می‌تواند www و یا blog باشد. بخش سوم و چهارم نام و نوع نام دامنه را مشخص کرده که در قسمت DNS شرح دادیم. آخرین قسمت یک فایل "test.jpg" را مشخص می‌کند که باید به آن دسترسی پیدا کرد.

سرور

یک سرور، برنامه کامپیوتروی است که نوع خاصی از خدمات را برای دیگر برنامه‌های فراهم می‌کند. برنامه‌های دیگر که به عنوان مشتری شناخته می‌شوند می‌توانند در همان سیستم و یا در همان شبکه اجرا شوند. انواع مختلفی از سرورها وجود دارد که نیازهای سخت‌افزاری مختلفی بسته به عواملی مانند تعداد مشتریان، پهنای باند و غیره را به وجود می‌آورند. برخی از انواع سرورها عبارت‌اند از:

- ❖ وب سرور: برای سرویس دهی به وب‌سایت‌ها استفاده می‌شود.
- ❖ ایمیل سرور: برای میزبانی و مدیریت ایمیل‌ها استفاده می‌شود.
- ❖ فایل سرور: برای میزبانی و مدیریت توزیع فایل استفاده می‌شود.

جستجوگر وب

موتور جستجوی وب، نرم‌افزاری کاربردی است که وب را بر اساس نیاز کاربر بررسی می‌کند. برخی از موتورهای جستجو فراتر از آن بوده و اطلاعات را از پایگاه‌های مختلف استخراج می‌کنند. معمولاً موتورهای جستجو، نتایج را بر اساس خزیدن^۱ انجام داده و از الگوریتم‌های تجزیه و تحلیل داده نیز استفاده می‌کنند. نتایج یک موtor جستجو معمولاً در قالب نمایش URL‌ها ارائه می‌شود.

برخی از موتورها، جستجوی معمولی و بعضی از آن‌ها نیز اطلاعاتی از انجمان‌های مختلف و دیگر پورتال‌های بسته (نیاز به احراز هویت اولیه دارند) را فهرست می‌کنند. برخی از موتورهای جستجو همچنین نتایج جستجو را از موتورهای مختلف جستجو جمع‌آوری کرده و آن را به صورت یکجا ارائه می‌دهند.

مروگر اینترنت

مروگر وب یک برنامه کاربردی در سمت سرویس گیرنده است که کاربر نهایی را قادر می‌سازد تا با وب ارتباط برقرار کند. مروگر دارای نوار آدرسی است که در آن کاربر نیاز به وارد کردن آدرس وب (URL) دارد، این درخواست به سرور مقصد فرستاده شده و محتویات درون واسطه مروگر نمایش داده می‌شود. پاسخ درخواست فرستاده شده توسط میزبان شامل داده‌های خام با فرمتهای مرتبط داده‌ها است.

¹ Crawl

مرورگرهای پیشین قابلیت محدودی داشتند، اما امروزه با ویژگی‌های مختلف مانند دانلود محتوا، نشانه‌گذاری منابع، ذخیره اعتبارسنجی و افودنی‌های جدید، بسیار قدرتمند هستند. برنامه‌های کاربردی مبتنی بر ابر^۱ نیز از مرورگرها به عنوان نرم‌افزار واسطه طور گسترده استفاده می‌کنند.

مجازی‌سازی

مجازی‌سازی^۲ می‌تواند به عنوان روش تخصیص منابع فیزیکی با هدف ساده‌سازی و استفاده بهینه از منابع، توصیف شود که می‌تواند شامل هر چیزی از یک پلتفرم سخت‌افزاری تا یک دستگاه ذخیره‌سازی و یا سیستم‌عامل و غیره باشد. برخی از طبقه‌بندی‌های مجازی‌سازی عبارت‌اند از:

- ۱) سخت‌افزار و یا پلت‌فرم: ایجاد یک ماشین مجازی که مانند یک رایانه اصلی با یک سیستم‌عامل عمل می‌کند. دستگاهی که مجازی‌سازی می‌شود میزبان است و ماشین مجازی، ماشین مهمان است.
- ۲) دستکتاب‌پ مجازی: مفهوم جدا‌سازی دستکتاب منطقی از دستگاه فیزیکی. کاربر با ماشین میزبان در یک شبکه با استفاده از دستگاه دیگری تعامل می‌کند.
- ۳) نرم‌افزار: مجازی‌سازی سطح سیستم‌عامل را می‌توان به عنوان میزبانی از چند محیط مجازی در یک نمونه واحد سیستم‌عامل توصیف کرد. مجازی‌سازی برنامه، میزبانی برنامه‌های فردی در یک محیط جدا از سیستم‌عامل اصلی است. در مجازی‌سازی سرویس، رفتار مؤلفه سیستم وابسته، شبیه‌سازی شده است.
- ۴) شبکه: ایجاد یک فضای آدرس مجازی در فضای داخل شبکه یا زیر شبکه‌های شبکه است.

مرور وب^۳

تا اینجا بعضی از کلمات کلیدی که در فصل بعد با آن‌ها برخورد خواهیم کرد، پرداختیم. بیایید کمی عمیق‌تر شویم و سعی کنیم به درستی متوجه شویم که وقتی سعی می‌کنیم یک وب‌سایت را مرور کنیم چه اتفاقی می‌افتد. هنگامی که ما یک URL را در مرورگر وارد می‌کنیم، آن را به دو قسمت تقسیم می‌کند. فرض کنیم می‌خواهیم وارد <http://www.example.com> شویم. این آدرس از دو قسمت (۱) <http://www.example.com> و (۲) [example.com](#) تشکیل شده است که شامل پروتکل استفاده شده و نام دامنه برای تبدیل آن به یک آدرس IP است. بیایید مجدداً فرض کنیم که آدرس

¹ cloud-based applications

² VIRTUALIZATION

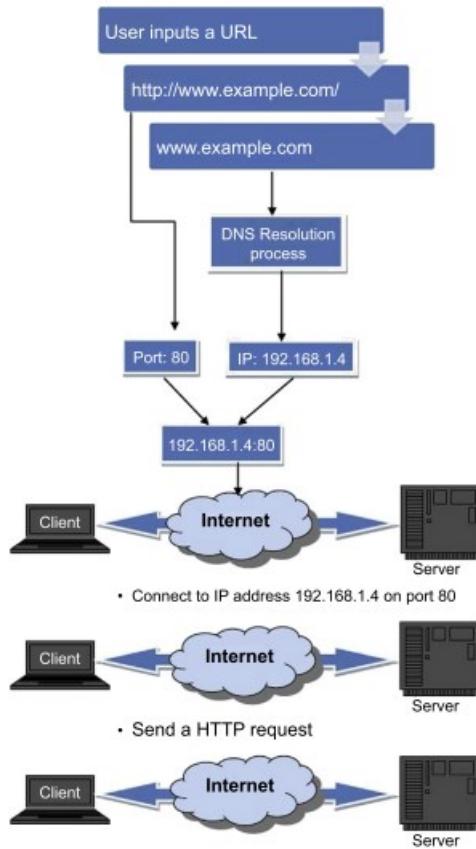
³ WEB BROWSING

IP مربوط به مثال "192.168.1.4" domain name "192.168.1.4:80" است و سپس مرورگر آن را به عنوان "192.168.1.4:80" پردازش می‌کند که ۸۰ شماره پورت مربوط به پروتکل HTTP است.

از اطلاعاتی که حاوی جزئیات در مورد DNS است برای تبدیل نام دامنه به آدرس IP استفاده می‌شود، اما چگونه؟ این بستگی به این دارد که آیا برای اولین بار از یک سایت بازدید می‌کنیم یا اغلب از این سایت بازدید می‌کنیم؛ برای هر دو مورد روش کاملاً مشابه است. ابتدا با بررسی حافظه پنهان مرورگر شروع می‌کند تا بررسی کند که آیا موردی وجود دارد یا خیر به عبارت دیگر بررسی می‌کند که آیا ما از این سایت پیش از این بازدید کردہ‌ایم و یا این اولین بار است. اگر حافظه پنهان مرورگر اطلاعاتی نداشته باشد، مرورگر سیستم را برای اینکه آیا دارای یک رکورد DNS در حافظه نهان خود است یا خیر، بررسی می‌کند. به طور مشابه اگر آن را پیدا نکرد، اطلاعات DNS مشابه در حافظه روتر جستجو می‌شود. در صورتی که هیچ رکورد DNS در ISP cache پیدا نشد، جستجوی اولیه از سرور root به دیگر سرورهای تحلیل نام برای تبدیل نام دامنه انجام می‌شود. چیزی که ما باید در مورد آن فکر کنیم این است که برخی از نام‌های دامنه با چندین آدرس IP مانند google.com همراه هستند که یک آدرس بر اساس مکان جغرافیایی کاربری که قصد استفاده از آن منبع را دارد، باز می‌گردد. این روش همچنین به عنوان DNS جغرافیایی شناخته شده است.

در بخش بالا متوجه شدیم که چگونه جستجوی DNS برای دست یابی به اطلاعات از حافظه پنهان مرورگر انجام می‌شود، اما این فقط برای سایت‌هایی است که ایستا هستند، زیرا سایت‌های پویا حاوی مطالب پویا هستند که به سرعت حذف می‌شوند. با این حال، این روند برای هر دو مورد کاملاً مشابه است.

بعد از DNS، مرورگر یک اتصال TCP به سرور باز می‌کند و یک درخواست بر اساس پروتکل ذکر شده در URL (به عنوان مثال HTTP) با مرورگر خود می‌فرستد (درخواست GET به سرور از طریق اتصال TCP). سپس مرورگر یک پاسخ HTTP از سرور با کد وضعیت دریافت خواهد کرد که به صورت ساده وضعیت سرور برای درخواست را مشخص می‌کند.



انواع مختلفی از کدهای وضعیت وجود دارند؛ از این رو فقط برای درک موضوع برخی از کدهای وضعیت پر کاربرد ذکر می‌شوند که بین ۱۰۰ تا ۵۰۵ بوده و با توجه به عدد اول آن‌ها به طبقات مختلف دسته‌بندی می‌شوند:

1XX: اطلاعاتی^۱

2XX: موفقیت‌آمیز^۲

3XX: هدایت^۳

4XX: خطای مشتری^۴

5XX: خطای سرور^۵

برخی از کدهای وضعیت پر کاربرد:

¹ Informational

² Successful

³ Redirection

⁴ Client-error

⁵ Server-error

❖ ۱۰۰: ادامه دهد^۱

❖ ۲۰۰: خوب^۲

❖ ۳۰۱: به طور دائمی نقل مکان کرد^۳

❖ ۳۰۲: یافت^۴

❖ ۴۰۰: درخواست بد^۵

❖ ۴۰۱: غیر مجاز^۶

❖ ۴۰۳: ممنوع است^۷

❖ ۴۰۴: پیدا نشد^۸

❖ ۵۰۰: خطای سرور داخلی^۹

❖ ۵۰۲: دروازه بد^{۱۰}

اگر مرورگر کد خطا دریافت کند، نمی‌تواند به درستی منابع را به دست آورد، در غیر این صورت پاسخ را ارائه می‌دهد. پاسخ معمولاً شامل کدهای HTML برای محتویات صفحه و پیوندهایی به منابع دیگر است که بیشتر تحت همان فرایند قرار می‌گیرند. اگر نیاز به کش صفحه پاسخ باشد، در حافظه پنهان ذخیره می‌شود. این روند کلی در پس زمینه اتفاق می‌افتد زمانی که سعی می‌کیم چیزی را در اینترنت با استفاده از یک مرورگر دریافت کنیم.

محیط آزمایشگاه

همان‌طور که مفاهیم اصلی را مورد بحث قرار دادیم، اکنون محیط آزمایشگاهی را برای تست‌های آینده ایجاد می‌کنیم.

¹ continue

² OK

³ moved permanently

⁴ found

⁵ bad request

⁶ unauthorized

⁷ forbidden

⁸ not found

⁹ internal server error

¹⁰ bad gateway

سیستم‌عامل

یک سیستم رایانه‌ای برای اجرای نیاز به سخت‌افزار اصلی مانند مادربرد، رم، هارددیسک و غیره دارد، اما سخت‌افزار بی‌ارزش است تا زمانی که یک سیستم‌عامل برای اجرا وجود نداشته باشد. سیستم‌عامل اساساً مجموعه‌ای از نرم‌افزارهایی است که می‌تواند سخت‌افزارهای پایه را مدیریت و خدمات اولیه را برای کاربران فراهم کند.

ویندوز

یکی از گسترده‌ترین سیستم‌عامل‌های مایکروسافت که در سال ۱۹۸۵ معرفی شد و پس از چندین سال بالغ شد. نسخه فعلی ویندوز ۱۰ است که سهم عمده‌ای از بازار دارد. سهولت استفاده یکی از ویژگی‌های اصلی این سیستم‌عامل است که به طور گسترده آن را قابل استفاده می‌نماید.

اگر چه در طول نوشتمن این کتاب ما از ویندوز هفت ۶۴ بیتی استفاده می‌کردیم، هر نسخه بالاتر از آن نیز به صورت مشابه با آن عمل می‌کند.

لینوکس

این سیستم‌عامل اغلب به دلیل ثبات و امنیت در میان توسعه‌دهنده‌گان، مدیران سیستم، متخصصان امنیتی و غیره مورد استفاده قرار می‌گیرد. هرچند که برای کاربران معمولی کمی متفاوت و دشوار به نظر می‌رسد، اما امروز به سطحی توسعه یافته که در آن رابط کاربری گرافیکی (GUI) ارائه شده توسط برخی از توزیع‌ها در مقابل واسطه گرافیکی ویندوز و مک قابل مقایسه است. قدرت این سیستم‌عامل در ترمینال آن (رابط خط فرمان) قرار دارد که اجازه استفاده از تمامی قابلیت‌های ارائه شده توسط سیستم را می‌دهد.

ما از توزیع تست نفوذ کالی لینوکس (<http://www.kali.org/>) در این کتاب استفاده خواهیم کرد که بر پایه توزیع دیبان است. اگر چه، دیگر توزیع‌ها مانند اوبونتو، Arch Linux و غیره نیز می‌توانند مورد استفاده قرار بگیرند زیرا اکثر دستورات مشابه‌ای دارند.

مک

این سری از سیستم‌عامل توسط اپل به خاطر طراحی فوق العاده آن به خوبی شناخته شده است. در گذشته، با توجه به گزینه‌های محدود موجود نرم‌افزاری، با انتقاداتی مواجه شده است، اما امروزه طیف وسیعی از برنامه‌های

نرم‌افزاری برای آن وجود دارد. گفته شده که نسبت به همتایانش (در استفاده معمولی) امن‌تر است، اما امروزه می‌دانیم که با برخی از مسائل امنیتی شدید مواجه شده است.

مک‌یک رابط خط فرمان قدرتمند (CLI) و همچنین واسطه گرافیکی (GUI) دارد که باعث می‌شود انتخاب خوبی برای هر عملیات محاسباتی باشد. اگرچه در هنگام نوشتن این کتاب از Mac OS X 10.8.2 استفاده کردیم، هر نسخه بعد از آن نیز برای کار یکسان خواهد بود.

اکثر ابزارهایی که در طول این کتاب استفاده می‌شوند، منبع آزاد / باز و همچنین مستقل از پلتفرم خواهند بود، هرچند استثنایی وجود دارد که در آن زمان و هنگام ورود، مشخص خواهد شد. توصیه می‌شود که یک ماشین مجازی از هر یک از انواع سیستم‌عامل‌های متفاوت (که در بالا بحث شد) جدا از سیستم پایه ایجاد کنید.

برای ایجاد یک ماشین مجازی می‌توان از نرم‌افزار مجازی‌سازی مانند VirtualBox یا VMware Player استفاده کرد. VMware Player اوراکل را می‌توان از <https://www.virtualbox.org/wiki/Downloads> دانلود کنید. VirtualBox می‌توان از <http://www.vmware.com/go/downloadplayer/> دانلود کرد.

زبان برنامه‌نویسی

زبان برنامه‌نویسی اساساً مجموعه‌ای از دستورالعمل‌ها است که اجازه می‌دهد با یک ماشین ارتباط برقرار کنید. با استفاده از زبان برنامه‌نویسی می‌توانیم رفتار یک ماشین و فرآیندهای خودکار را کنترل کنیم.

جاوا

جاوا زبان برنامه‌نویسی سطح بالا، توسعه یافته توسط SunMicro و در حال حاضر اوراکل است. با توجه به ثبات ارائه شده توسط آن، بهشت در برنامه‌های کاربردی تحت معماری سرور-مشتری مورد استفاده قرار می‌گیرد. جاوا یکی از محبوب‌ترین زبان‌های برنامه‌نویسی امروزه است.

جاوا در بسیاری از مرورگرها و همچنین برنامه‌های دیگر و در انواع مختلف سیستم‌عامل‌ها مانند ویندوز، لینوکس و مک اجرا می‌شود. آخرین نسخه جاوا را می‌توانید از <https://www.java.com/en/download/manual.jsp> دانلود کنید.

پایتون

زبان برنامه‌نویسی سطح بالا است که اغلب برای ایجاد اسکریپت‌های کوچک و کارآمد استفاده می‌شود. همچنین برای توسعه وب به‌طور گستره‌ای مورد استفاده قرار می‌گیرد. پشتیبانی و در دسترس بودن کتابخانه‌های شخص ثالث، آن را انتخاب مناسب‌تر برای بسیاری از افرادی که اغلب نیاز به خودکار سازی وظایف کوچک دارند، می‌کند. اگرچه این بدان معنا نیست که پایتون برای ایجاد برنامه‌های کاربردی کامل به اندازه کافی قادر تمند نیست. ما بعداً در مورد برنامه‌نویسی پایتون بحث خواهیم کرد.

نسخه فعلی Python 3.4.0 است، اگرچه ما از نسخه ۲.۷ استفاده خواهیم کرد. سری ۳.x تغییرات عمدی‌ای کرده که با ماقبل از آن سازگار نیست. اکثر اسکریپت‌هایی که ما استفاده می‌کنیم از نسخه ۲.۷ استفاده می‌کنند. آن را می‌توان از <https://www.python.org/download/releases/2.7.6/> دانلود کرد.

مرورگر

همان‌طور که در بالا توضیح داده شد، یک مرورگر نرم‌افزار کاربردی است که در سرویس گیرنده نصب شده و اجازه می‌دهد تا با وب ارتباط برقرار کنید.

کروم

توسعه یافته توسط گوگل و یکی از مرورگرهای رایج است. برای اولین بار در سال ۲۰۰۸ منتشر شد، امروز این مرورگر به یک انتشار بسیار پایدار تبدیل شده است. اکثر کدهای پایه آن (<http://www.chromium.org/Home>) به صورت آنلاین در دسترس است. امروزه کروم در تمام دستگاه‌هایی که برای مرور وب استفاده می‌شوند، یعنی لپ‌تاپ، تبلت یا گوشی هوشمند استفاده می‌شود. سهولت استفاده، ثبات، امنیت و افزودنی‌های ارائه شده توسط کروم به‌وضوح آن را یکی از بهترین مرورگرهای موجود می‌کند که می‌توانید آن را از <https://www.google.com/intl/en/chrome/browser/> دانلود کنید.

فایرفاکس

فایرفاکس یک مرورگر وب رایگان است و توسط شرکت موزیلا توسعه داده شده است. امکان سفارشی‌سازی ارائه شده توسط فایرفاکس اجازه می‌دهد تا آن را به میل خود تغییر دهید. یکی از بزرگ‌ترین ویژگی‌های فایرفاکس، لیست گسترهای از افرونهای مرورگر است که اجازه می‌دهد تا آن را برای موارد خاص طراحی

کنید. همانند کروم، برای سیستم‌عامل‌های مختلف در دسترس است که آن را می‌توانید از آدرس <https://www.mozilla.org/en-US/firefox/all/> دانلود کنید.

در این کتاب ما عمدتاً از کروم و فایرفاکس به عنوان مرورگر استفاده می‌کنیم. در فصل بعد هر دو را با توجه به نیازهایمان سفارشی خواهیم کرد. در این فصل ما تکنولوژی‌های اولیه و همچنین محیطی آزمایشگاهی را که استفاده می‌کنیم مشخص کردیم. انگیزه اصلی این بود که بنیادی را بسازیم تا زمانی که ما در دستور کار اصلی یعنی جمع‌آوری هوشمند اطلاعات از وب قرار گرفتیم، در ک درستی از آنچه با آن روبرو هستیم، داشته باشیم.

فصل ۲: اطلاعات متن‌باز و جستجوی پیشرفته رسانه‌های اجتماعی

مقدمه

همان‌طور که پیش از این بحث شد، وقت آن رسیده تا موضوع اصلی این کتاب را درک کنید، این همان جمع‌آوری هوشمند از منابع اطلاعاتی متن باز است که با اختصار OSINT شناخته شده است، اما قبل از آن باید تشخیص دهیم چگونه اطلاعات در دسترس عموم را مشاهده کرده و تا چه میزانی از آن را می‌توانیم بینیم.

برای اکثر ما اینترنت محدود به نتایج موتور جستجو است. اگر درباره یک کاربر عادی صحبت کیم که بخواهد اطلاعاتی از اینترنت بگیرد به‌طور مستقیم به یک موتور جستجو می‌رود؛ فرض کنید محبوب‌ترین موتور جستجو گوگل است و یک جستجوی ساده انجام می‌شود. یک کاربر عادی که از مکانیسم‌های جستجو پیشرفته ارائه شده توسط گوگل یا همتایانش بی‌اطلاع است، پرس‌وجو ساده‌ای را انجام می‌دهد که از آن به‌راحتی نتیجه می‌گیرد. بعضی وقت‌ها اطلاعاتی که از موتور جستجو دریافت می‌شوند به دلیل ایجاد ورودی‌های ضعیف، کاربردی نیستند. به عنوان مثال، اگر یک کاربر بخواهد برای رفع مشکل خطای پنجره آبی ویندوز جستجو کند، در نوار جستجوی موتور جستجو عبارت "صفحه‌نمایش لپ‌تاپ من به رنگ آبی" است. چگونه می‌توانم آن را حل کنم" وارد می‌کند. این پرسش ممکن است به نتیجه دلخواه در صفحه اول موتور جستجو نرسد، بنابراین می‌تواند کمی زمان گیر باشد. گرفتن اطلاعات مورد نظر از اینترنت بسیار آسان است، اما باید از کجا بدانیم که چگونه اطلاعات را به‌طور مناسب جمع‌آوری کنیم. یک تصور غلط رایج در میان کاربران این است که موتور جستجو ای که او ترجیح می‌دهد،

کل اینترنت را جستجو می‌کند، اما در سناریوی واقعی موتورهای جستجو مانند گوگل تنها بخش جزئی اینترنت را نشان می‌دهند. یکی دیگر از روش‌های معمول این است که نتایج دو موتور جستجو استفاده شود. همه ما این شوخی را شنیده‌ایم "اگر بخواهید بدن مردهای را پنهان کنید، نتیجه صفحه دو گوگل امن‌ترین مکان است." بنابراین جستجوی صحیح با استفاده از موتورهای جستجو بسیار اهمیت دارد.

جمع‌آوری هوشمند اطلاعات منبع باز

به سادگی می‌توان اظهار داشت، اطلاعات منبع باز اطلاعاتی هستند که از منابعی جمع‌آوری شده که به صورت آشکار در انتظار عموم حضور دارند. بر خلاف بیشتر روش‌های دیگر جمع‌آوری اطلاعات، این روش از اطلاعاتی که مخفی است استفاده نمی‌کند (هر چند برخی از استثنایات گاهی اوقات موردنیاز است).

OSINT از منابع عمومی مختلفی مانند:

- ❖ نشریات علمی: مقالات پژوهشی، نشریات کنفرانس و ...
- ❖ منابع رسانه‌ای: روزنامه، کانال‌های رادیویی، تلویزیون و غیره
- ❖ محتوای وب: وب‌سایتها، رسانه‌های اجتماعی و غیره
- ❖ داده‌های عمومی: اسناد دولتی باز، اطلاعیه‌های شرکت‌های دولتی و غیره استفاده می‌کند.

اغلب اوقات برخی از اطلاعات در فراهم آوردن زمینه برای دسترسی به اطلاعات دیگر، بسیار مفید هستند؛ اما این همه چیز نیست، یکی از بزرگ‌ترین و منحصر به فردترین‌ها مشکلات، فراوانی داده‌های OSINT اطلاعات بسیار زیاد را فیلتر کرده و آن‌ها را به یک شکل قابل استفاده تبدیل می‌کند.

OSINT برای مدت طولانی توسط دولت‌ها، مراکز نظامی و همچنین شرکت‌های تجاری برای رسیدن به مزایای رقابتی مورد استفاده قرار گرفته است. همان‌طور که بحث کردیم، منابع عمومی مختلفی وجود دارد که می‌توانیم اطلاعات را جمع‌آوری کنیم، اما در طی این کتاب، ما تنها از اینترنت به عنوان رسانه پایه استفاده می‌کنیم. این نوع خاص OSINT به عنوان WEBINT شناخته می‌شود، هر چند به خاطر تفاوت بین اینترنت و وب کمی مبهم به نظر می‌رسد (بحث در فصل ۱). با تمرکز بر یک نوع خاص از منبع شاید فکر کنید ما بخش بزرگی از OSINT را از دست می‌دهیم. این فکر تا چند دهه قبل درست بود، اما امروزه که بسیاری از داده‌ها به صورت دیجیتالی شده‌اند، این خط اختلاف به آرامی کاهش می‌یابد.

چگونه استفاده OSINT از موتورهای جستجو

موتورهای جستجو یکی از رایج‌ترین و آسان‌ترین روش‌های استفاده از OSINT می‌باشد. هر روز صدها جستجو در یک یا چند موتور جستجو، بسته به اولویت و رسیدن به برخی اهداف استفاده می‌شوند. اگر چه نتایج به نظر ساده می‌رسد، اما در پس آن الگوریتم‌های پیچیده استفاده می‌شود. نحوه استفاده از نمادهای مختلف، تفاوت زیادی در دقت نتیجه‌ای که ما در از یک موتور جستجو دنبال می‌کنیم، ایجاد می‌کند. در فصل بعد پرسش‌های را طراحی می‌کنیم تا بتوانیم دقیقاً نتیجه‌ای را که می‌خواهیم به دست آوریم. گوگل، یاهو و بینگ نمونه خوبی از موتورهای جستجو هستند.

اگر چه به نظر می‌رسد موتورهای جستجو دارای مقدار زیادی اطلاعات هستند، اما آن‌ها تنها اطلاعاتی را که از طریق برنامه‌هایی به نام عنکبوت یا روبات‌ها به دست می‌آورند، نشان می‌دهند. این عنکبوت‌ها قادر به خزیدن در بخشی از وب هستند که به عنوان وب سطحی شناخته می‌شود، بقیه آن وب تاریک یا darknet نامیده می‌شود. darknet مستند نیست زیرا به طور مستقیم از طریق لینک قابل دسترسی نیست. darknet یک صفحه تولیدشده به صورت پویا است که توسط موتورهای جستجوی وب قابل دستیابی نیست.

سایت‌های خبری

پیش از این رسانه‌های محبوب روزنامه‌ها، رادیو و تلویزیون بودند؛ اما پیشرفت در فن آوری اینترنت به طور چشمگیری سناریو را تغییر داده و امروزه هر آژانس خبری دارای یک وب‌سایت است که می‌توانیم تمام اخبار را در قالب دیجیتال از آن دریافت کنیم. امروزه حتی آژانس‌های خبری وجود دارند که فقط آنلاین هستند. این پیشرفت قطعاً دسترسی به اخبار را در هر زمان و هر مکانی که اتصال اینترنتی در دسترس است را آسان می‌کند. برای مثال، وب‌سایت خبری شرکت BBC Broadcasting Corporation است.

به غیر از آژانس‌های خبری، سایت‌هایی هستند که توسط فرد و یا یک گروهی از افراد ایجاد شده و برخی از آن‌ها بر موضوعاتی خاص متمرک هستند. این سایت‌ها عمدها در قالب وبلاگ‌ها، گروه‌های آنلاین، انجمان‌ها یا IRC‌ها (چت اینترنتی) و غیره قرار می‌گیرند و زمانی که به یک موضوع خاص نیاز داریم، بسیار مفید هستند.

وب‌سایت شرکت‌ها

هر شرکت بزرگ امروز یک وب‌سایت دارد که راهی برای ارتباط مستقیم با مشتریان آن‌ها است. به عنوان مثال، وب‌سایت شرکت General Motors است. ما می‌توانیم اطلاعات فراوانی درباره یک شرکت از

وبسایت آن بیاپیم. معمولاً یک وبسایت شرکتی شامل اطلاعاتی از کارکنان کلیدی، ایمیل‌ها، آدرس، تلفن شرکت و ... می‌باشد که می‌تواند برای استخراج اطلاعات بیشتر استفاده شوند.

امروزه برخی از وبسایت‌های شرکت‌های بزرگ همچنین اطلاعاتی را در قالب مقاله‌های سفید، مقاله‌های پژوهشی، وبلاگ‌ها، خبرنامه‌ها، مشتریان فعلی و غیره ارائه می‌دهند. این اطلاعات نه تنها در شناخت وضعیت فعلی شرکت به کار بردۀ می‌شوند، بلکه برنامه‌های آتی آن‌ها را نیز مشخص می‌نمایند.

وبسایت‌های اشتراک‌گذاری محتوا

انواع مختلفی از محتوای تولیدشده توسط کاربران وجود دارد که حاوی متن و انواع مختلف چندرسانه‌ای است. سایت‌هایی نیز وجود دارند که به ما اجازه می‌دهند نوع خاصی از محتوا مانند فیلم، عکس و غیره را به اشتراک بگذاریم. این نوع سایت‌ها وقتی که نیاز به نوع خاصی از رسانه‌ها مربوط به یک موضوع را داریم بسیار مفید هستند. یوتیوب و فلیکر نمونه خوبی از چنین سایت‌هایی هستند.

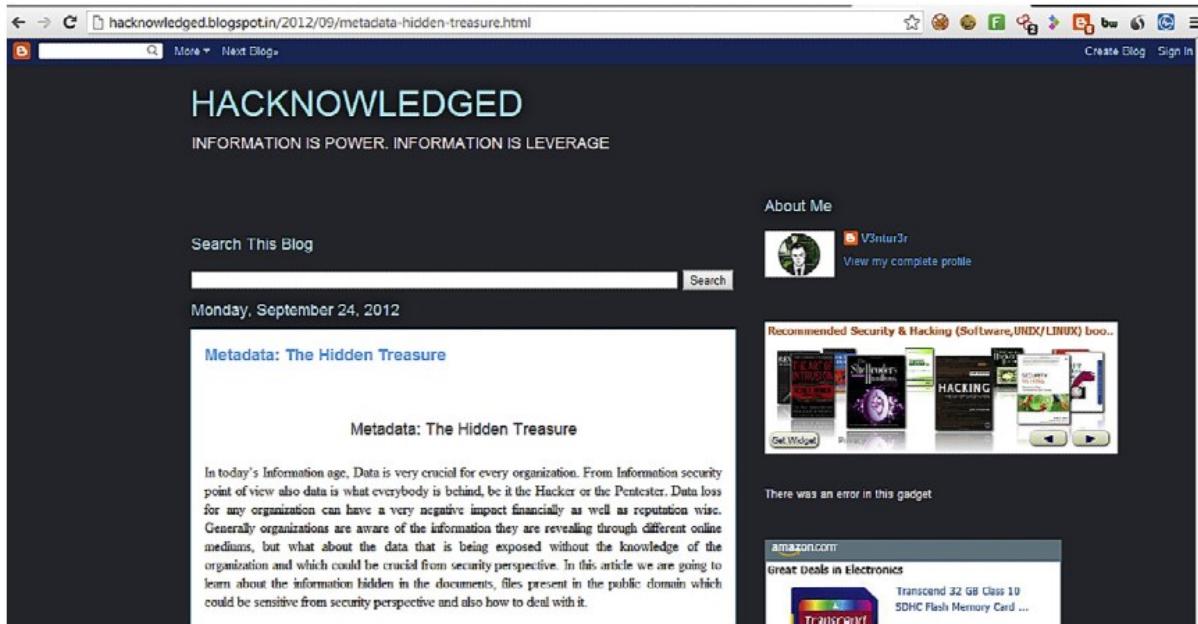
سایت‌های علمی

سایت‌های آکادمیک معمولاً حاوی اطلاعات درخصوص موضوعات خاص، مقالات پژوهشی، پیشرفت‌های آینده، اخبار خاص و غیره هستند. در اغلب موارد این اطلاعات می‌تواند در ایجاد زمینه برای توسعه فعلی و آینده نیز بسیار مهم باشد. سایت‌های علمی نیز در رسیدن به اطلاعاتی در زمینه مورد علاقه ما کمک کنند و همچنین در ک همبستگی بین آن‌ها نیز مفید است.

اطلاعات ارائه شده در سایت‌های دانشگاهی در درک پیشرفت‌هایی که در یک حوزه خاص رخ می‌دهند بسیار مفیدند. آن‌ها نه تنها در درک وضعیت فعلی، بلکه همچنین به ایجاد ایده‌هایی خلاقانه کمک می‌کنند.

وبلاگ‌ها

وبلاگ یا بلاگ‌ها به عنوان یک فرم دیجیتال از خاطرات شخصی می‌باشند، مگر اینکه عمومی باشند. معمولاً مردم از وبلاگ‌ها به سادگی به منظور بیان نظرات خود در مورد برخی از موضوعات مورد علاقه استفاده می‌کردند که در دهه گذشته تغییر کرده است. امروزه وبلاگ‌های شرکتی وجود دارد که در مورد دیدگاه‌های شرکت صحبت می‌کند و می‌توانند فعالیت‌های آن را آشکار کنند. وبلاگ‌هایی در موضوعات خاص نیز وجود دارند که می‌توانند برای موضوع و یا رویداد خاصی مورد استفاده قرار گیرند.



وبلاگ‌ها علاوه بر موضوع نوشته شده دارای اطلاعاتی در مورد نویسنده آن نیز هستند. در بسیاری از برنامه‌های استخدام شغلی، جستجوی وبلاگ متخصصی انجام می‌شود، زیرا می‌تواند برای فهم روانشناسی اولیه، مهارت‌های ارتباطی و غیره شخص مورد نظر استفاده شود.

سایت‌های دولتی

سایت‌های دولتی دارای مقدار زیادی اطلاعات عمومی هستند. این اطلاعات نه تنها در مورد دولت بلکه در مورد افرادی است که در آن خدمت می‌کنند. معمولاً سایت‌های دولتی وجود دارد که حاوی اطلاعاتی درباره شرکت‌های ثبت‌شده، مدیران و سایر اطلاعات آنها هستند. سایت‌هایی هستند که حاوی اطلاعات مربوط به بخش‌های خاص دولت هستند؛ همچنین سایت‌هایی وجود دارند که ما می‌توانیم در مورد مسائل عمومی شکایت کرده و وضعیت آن را بررسی کنیم و غیره. از دیدگاه ژئوپلیتیک، سایت‌های دولتی می‌توانند منبع خوبی از اطلاعات برای توسعه یک کشور، پیشرفت‌های جاری، برنامه‌های آینده و غیره باشند.

بنابراین امروز ما یا اینترنت برای دسترسی به اطلاعات، ارتباط برقرار می‌کنیم، اما همیشه این طور نیست. اگر هیچ وبلاگ، هیچ رسانه اجتماعی، هیچ محتوا‌ای به اشتراک گذاشته و غیره وجود نداشته باشد، پس چگونه اطلاعات را به دست بیاوریم؟

۲۰. وب

وب سایت‌های پیش از این عمدتاً به صورت استاتیک استفاده می‌شدند که ارتباط چندانی با آن وجود نداشت. کاربران به سادگی از آن برای باز کردن صفحات وب و مشاهده متن‌ها و تصاویر استفاده می‌کردند. در اواخر ۱۹۹۰، وب شروع به ساخت یک فرم جدید کرد. صفحات استاتیک با استفاده از محتوای تولیدشده توسط کاربر جایگزین شدند. وب سایت‌ها تعاملی شده و افراد شروع به همکاری آنلاین کردند. این ظهور وب ۲۰ بود.

وب ۲۰ عمیقاً وب را تغییر داد. پیش از این محتویات به اشتراک گذاشته شده توسط مدیران وب تنها اطلاعاتی بود که می‌توانستیم به آن‌ها دسترسی داشته باشیم. در حال حاضر افراد می‌توانند داده‌ها را در وب منتشر کنند و نظرات مشترک به چالش کشیده می‌شوند؛ بنابراین نحوه تولید اطلاعات تغییر کرد. اکنون منابع متعددی برای تائید یا بی‌اعتبار کردن یک داده وجود دارد. مردم می‌توانند اطلاعات، ارتباطات، محیط و همه چیزهایی که با آن‌ها ارتباط برقرار کرده‌اند، به اشتراک بگذارند.

از آن زمان به بعد افراد نه فقط بینندگان محتوای وب بلکه سازندگان آن نیز بودند. این ویژگی برای برقراری ارتباط و همکاری، مردم را به ایجاد محیط‌های جدید برای به اشتراک گذاری اطلاعات و اتصال در واقعیت مجازی تشویق کرد. پس پلتفرم‌هایی مانند پورتال‌های به اشتراک گذاری محتوا، شبکه‌های اجتماعی، و بلاگ‌ها، ویکی‌ها و غیره خلق شدند. دنیای مجازی به آرامی شروع به تبدیل شدن به خانه دوم و منبع فراوان اطلاعاتی کرد که قبلاً وجود نداشت.

این دنیای مجازی هم اکنون واقعیت ماست. توانایی ایجاد محتوا در اینجا به ما اجازه می‌دهد تا هرگونه اطلاعاتی که می‌خواهیم به اشتراک بگذاریم، اطلاعات شخصی، اطلاعات حرفه‌ای، احساسات، دوست داشتن و یا نداشتن وغیره. در اینجا می‌توانیم به دیگران در مورد خودمان بگوییم و در عین حال از دیگران نیز یاد بگیریم. ما می‌توانیم دیدگاه‌هایمان را درباره هر چیزی به اشتراک بگذاریم و آنچه دیگران به اشتراک می‌گذارند را در ک کنیم. این به ما اجازه می‌دهد تا با نشستن در گوشه‌ای با دنیا ارتباط برقرار کنیم.

امروزه این فضاهای فقط شامل حضور افراد حقیقی نیست، بلکه مردم به شکل اجتماعات و یا گروه‌ها نیز در آن وجود دارند؛ صفحات احزاب سیاسی، شرکت‌ها، محصولات و غیره نیز وجود دارند. همه چیزهایی که ما در زندگی واقعی استفاده می‌کنیم در دنیای مجازی تکرار شده‌اند. این قطعاً جهان را نزدیک‌تر کرده و بر زندگی ما تأثیر می‌گذارد.

وب در مرحله فعلی نه تنها بخشی از زندگی ما است، بلکه آن را نیز در بر می‌گیرد. با به اشتراک گذاشتن احساسات، خواسته‌ها، دوست داشتن و یا نداشتن آنلاین، ما اجازه می‌دهیم دیگران در مورد ما بدانند، شخصیت‌مان را در ک کنند و بالعکس. به طور مشابه محتوای ارسال شده در اینترنت نقش مهمی در تصمیم‌گیری ما ایفا می‌کند. آگهی‌هایی که می‌بینیم آنلاین هستند و به رفتار آنلاین ما جهت می‌دهند. یک هشدار سیاسی در توییتر یا ویدیویی در روزانه منتشر می‌شوند، در تصمیم‌گیری‌های ما تفاوت ایجاد می‌کند.

امروز وب ایجاب می‌کند تا فراوانی داده‌ها را داشته باشد که بسیار خوب است زیرا احتمال یافتن پاسخ سؤالات ما افزایش می‌یابد. مسئله این است که چگونه اطلاعات مربوطه را استخراج کنیم و این همان چیزی است که ما در این کتاب با آن رویرو می‌شویم که از این فصل شروع می‌شود.

رسانه‌های اجتماعی هوشمند^۱

همان‌طور که می‌دانیم، رسانه‌های اجتماعی بخشی جدایی‌ناپذیر از وب هستند. بیشتر این اطلاعات توسط کاربران ایجاد شده‌اند. اطلاعات رسانه‌های اجتماعی یا SOCMINT نامی است که برای اطلاعاتی که از سایت‌های رسانه‌های اجتماعی جمع‌آوری می‌شود، بکار برده می‌شود. بعضی از آن‌ها ممکن است باز باشند، یعنی بدون هرگونه احراز هویت در دسترس باشند و برخی ممکن است قبل از دسترسی به هرگونه اطلاعات، احراز هویت نیاز داشته باشند. با توجه به ماهیت بسته بودن، برخی افراد آن را به عنوان بخشی از OSINT نمی‌شمارند، اما به خاطر ساده بودن، ما آن را در نظر می‌گیریم. برخی از رسانه‌های اجتماعی عبارت‌اند از:

❖ وبلاگ‌ها مانند Blogger

❖ وب سایت‌های شبکه‌های اجتماعی مانند Facebook

❖ رسانه‌های اشتراک گذاری مانند Flickr

❖ پروژه‌های همکاری مانند Wikipedia

در حال حاضر که ایده روشن در مورد OSINT و رسانه‌های اجتماعی داریم، باید به درک یکی از بخش‌های جدایی‌ناپذیر از رسانه‌های اجتماعی و یک منبع اشتراک اطلاعات، یعنی شبکه‌های اجتماعی پردازیم.

شبکه‌های اجتماعی

وب‌سایت شبکه اجتماعی پلتفرمی است که به کاربران اجازه می‌دهد با یکدیگر بسته به زمینه‌های مورد علاقه، محل سکونت، ارتباطات واقعی زندگی و غیره ارتباط برقرار کنند. شبکه‌های اجتماعی امروزه بسیار محبوب هستند که هر کاربر اینترنتی تقریباً یک حضور در یک یا بیشتر از آن‌ها دارد. با استفاده از چنین وب‌سایت‌هایی می‌توانیم پروفایل اجتماعی خودمان را ایجاد کنیم، اطلاعات خود را اشتراک گذاری کرده و همچنین پروفایل دیگر افراد که مورد علاقه ماست را بررسی کنیم.

برخی از ویژگی‌های مشترک وب‌سایت‌های شبکه‌های اجتماعی عبارت‌اند از:

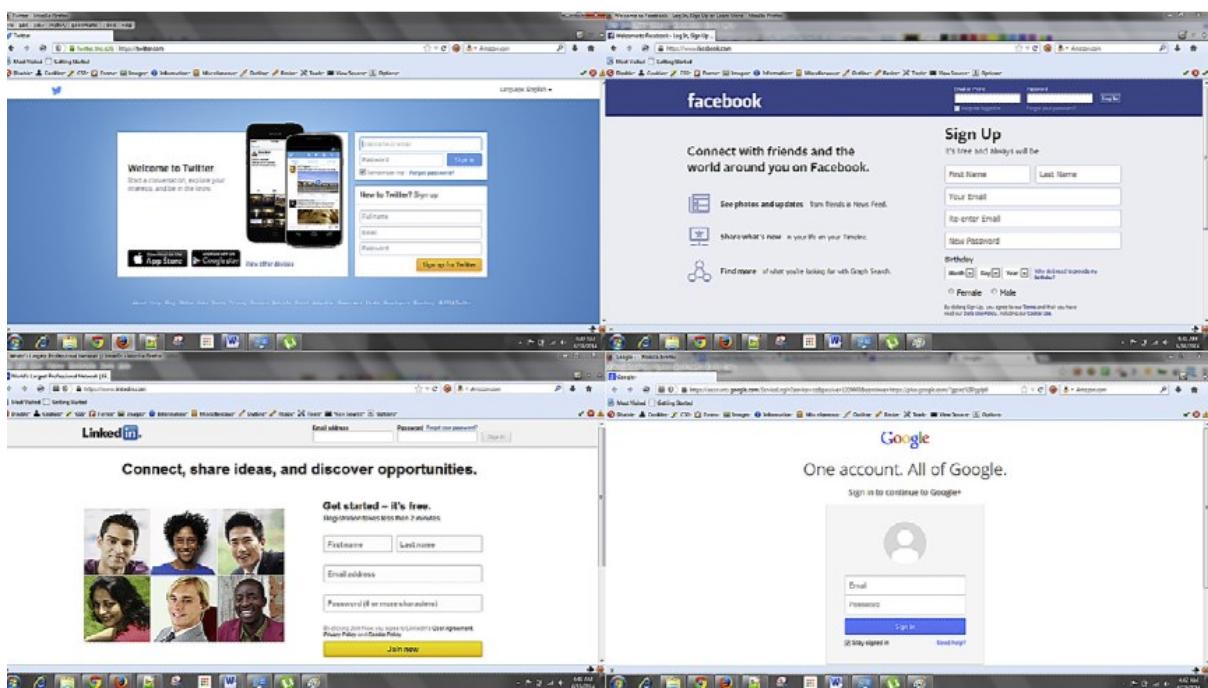
- ❖ به اشتراک گذاشتن اطلاعات شخصی
- ❖ ایجاد گروه‌های ذینفع
- ❖ به اشتراک گذاشتن نظرات
- ❖ ارتباط از طریق چت یا پیام شخصی

چنین وب‌سایت‌هایی در اتصال افراد، ایجاد روابط جدید، به اشتراک گذاشتن ایده‌ها و خیلی چیزهای دیگر بسیار مفید بوده‌اند. آن‌ها همچنین در درک فرد، شخصیت، ایده، دوست داشتن و یا نداشتن و غیره بسیار مفید هستند.

مقدمه شبکه‌های اجتماعی

چندین سایت شبکه اجتماعی محبوب وجود دارد که در آن قبلاً ثبت‌نام کرده‌ایم، اما چرا سایت‌های شبکه اجتماعی مختلفی وجود دارند؟ دلیل این است که شبکه اجتماعی بر جنبه‌های مختلف زندگی تمرکز دارند. برخی از آن‌ها بر روابط عمومی و دوستی مانند فیسبوک، Google+ و غیره تمرکز دارند؛ برخی بر جنبه‌های تجاری و یا حرفه‌ای مانند LinkedIn و برخی در میکروبلاگ و یا به اشتراک گذاری دیدگاه‌ها از قبیل توییتر تمرکز دارند. شبکه‌های اجتماعی زیادی با جنبه‌های مختلف وجود دارند، اما در این فصل تنها به برخی از موارد پرکاربرد آن اشاره می‌کنیم که عبارت‌اند از:

- ❖ فیسبوک
- ❖ LinkedIn
- ❖ توییتر
- ❖ Google+



فیسبوک

فیسبوک یکی از محبوب‌ترین و گسترده‌ترین سایت‌های شبکه اجتماعی است. فیسبوک در ۴ فوریه ۲۰۰۴ توسط مارک زوکربرگ با هم‌اتاقی کالج اش تأسیس شد. در ابتدا فیسبوک در میان دانشجویان دانشگاه هاروارد محدود شده بود، اما اکنون برای هر کسی که سن بالای ۱۳ سال دارد، باز است؛ اما هیچ مکانیزمی برای اثبات آن لازم نیست. در میان سایر سایت‌های شبکه اجتماعی، به دلیل بعضی از ویژگی‌های محبوب و جنبه‌های عمومی آن، دارای مخاطبان در گروه سنی مختلفی است. در حال حاضر بیش از یک میلیارد کاربر فعال در سراسر جهان دارد.

فیسبوک امکان ایجاد یک پروفایل شخصی را فراهم می‌کند که کاربر می‌تواند اطلاعاتی نظیر کار و تحصیل، مهارت‌های شخصی، وضعیت ارتباط، جزئیات مربوط به اعضای خانواده و اطلاعات اساسی مانند جنسیت، تاریخ تولد، اطلاعات تماس مانند شناسه ایمیل، جزئیات وبسایت و غیره و همچنین رویدادهای زندگی را به آن اضافه کند. همچنین امکان ایجاد یک صفحه برای استفاده شخصی یا تجاری را فراهم می‌کند که می‌تواند به عنوان یک پروفایل استفاده شود. ما همچنین می‌توانیم گروه‌ها را ایجاد کنیم، گروهی از علاقه‌مندی‌ها را بازیم، دیگر کاربران فیسبوک را بر اساس روابط یا منافع مشترک اضافه کنیم و دوستان را دسته‌بندی کنیم مانند چیزی که ما دوست داریم، در مورد چیزی توضیح دهیم، آنچه را که احساس می‌کنیم به اشتراک بگذاریم، جایی که هستیم را به اشتراک بگذاریم، آنچه ما در حال حاضر انجام می‌دهیم را به اشتراک بگذاریم و تصاویر و فیلم‌ها را اضافه

کنیم. همچنین می‌توانیم پیام‌ها را با شخصی یا گروهی به صورت عمومی یا خصوصی به اشتراک بگذاریم و با کسی گفتگو کنیم. اضافه کردن یادداشت‌ها، ایجاد رویدادها و بازی کردن برخی دیگر از ویژگی‌های آن است.

در حال حاضر ممکن است فکر کنید که چرا ما این اطلاعات را به اشتراک می‌گذاریم، چرا که به عنوان یک کاربر فیسبوک بسیاری از ما از همه این موارد آگاه هستیم. به این دلیل است که ما در OSINT کمک می‌کنیم. فیسبوک دارای بیش از یک میلیارد کاربر فعال است و به کاربران اجازه می‌دهد تا تقریباً همه چیز را به اشتراک بگذارند، بنابراین می‌توان گفت فیسبوک حاوی اطلاعاتی از اطلاعات ساخت‌یافته بیش از یک میلیارد کاربر است مانند آنچه دوست دارند، اطلاعات اساسی مانند نام و نام خانوادگی، سن، جنسیت، شهر کنونی، وضعیت کار، وضعیت ارتباط، بازدیدهای اخیر و همه چیز که یک گنج در زمان جمع‌آوری است. در حال حاضر، گرچه غالب ما از فیسبوک برای به دست آوردن اطلاعات استفاده نمی‌کنیم، اما هنوز از امکانات جستجوی آن برای یافتن شخص یا صفحه مورد نظر استفاده می‌کنیم؛ مانند یک دوست مدرسه؛ بنابراین ما نام را جستجو می‌کنیم و یا نام را با نام مدرسه جستجو می‌کنیم تا نتیجه‌ای را به دست آوریم. گزینه دیگری که می‌تواند مورد استفاده قرار گیرد این است که آیا یک گروه برای همکلاسی‌ها وجود دارد، ما می‌توانیم به طور مستقیم دوستانمان را جستجو کنیم. فیسبوک بر اساس علاقه‌مندی، مکان، تحصیلات، مدرسه، کالج، همکاران دوستانی را نیز به شما توصیه می‌کند. این گزینه همچنین کمک زیادی به جستجوی شخصی در فیسبوک می‌کند. ما راه‌های پیشرفته جستجوی در فیسبوک را آینده پوشش خواهیم داد.

فیسبوک اجازه می‌دهد حریم خصوصی را در بیشتر موارد ذکر شده در بالا انجام دهد. مثلاً افرادی که می‌خواهید با آن‌ها این اطلاعات را به اشتراک بگذارید، مانند عمومی، خصوصی و یا فقط دوستان را مشخص کنید. همچنین به کاربران اجازه می‌دهد که محتوای کاربران نامناسب را با گزارش هرزنامه و محتوای نامناسب مسدود کند؛ اما حدس بزنید چه چیزی بیشتری از این ویژگی‌ها وجود دارد که از آن بی‌اطلاع هستیم یا به سادگی آن‌ها را نادیده می‌گیریم.

LinkedIn

اگر مشغول به کار هستید و یا ارائه دهنده خدمات و یا کسب و کار هستید، LinkedIn بهترین مکان برای فعالیت شما است. LinkedIn می‌تواند به عنوان شبکه حرفه‌ای نامیده می‌شود که در آن مردم بیشتر به موارد تجاری علاقه دارند و بیش از ۲۵۹ میلیون عضو در بیش از ۲۰۰ کشور دارد.

اجازه می‌دهد تا ثبت‌نام و یک پروفایل ایجاد کنیم. این پروسه اساساً شامل نام، نام شرکت، موقعیت، محل کار فعلی، نوع صنعت فعلی و غیره می‌باشد. همچنین در اینجا می‌توانیم اطلاعاتی در مورد کارمان مانند موقعیت شغلی و مسئولیت‌ها، جزئیات آموزشی، جزئیات افتخار و جوايز، انتشارات، گواهینامه‌ها، مهارت‌ها، پروژه‌های انجام‌شده، تسلط بر زبان‌های مختلف، تقریباً زندگی حرفه‌ای‌مان، وارد کنیم. به غیر از آن LinkedIn همچنین به ما امکان می‌دهد اطلاعات شخصی مانند تاریخ تولد، وضعیت تأهل و اطلاعات تماس را اضافه کنیم.

مانند فیسبوک به ما اجازه می‌دهد که با سایر کاربران مرتبط باعلاقه‌مان ارتباط برقرار کنیم یا با آن‌ها سطح خاصی از ارتباط را داشته باشیم. برای حفظ امنیت، LinkedIn ما را محدود به دعوت دیگران می‌کند. همانند فیسبوک، گروه‌های مختلفی در LinkedIn وجود دارند که ما می‌توانیم برای به اشتراک گذاشتن به آن‌ها پیوندیم. همچنین ویژگی‌هایی را برای دوست داشتن، نظر دادن و به اشتراک گذاری هر چیزی که می‌خواهیم فراهم می‌کند و با دیگران از طریق پیام خصوصی ارتباط برقرار می‌کند. یکی از ویژگی‌های ساده و در عین حال غنی LinkedIn است که در فیسبوک ما تنها می‌توانیم دوستان متقابل بین دو کاربر را مشاهده کنیم، اما به ما نشان می‌دهد که چگونه با یک کاربر خاص ارتباط برقرار می‌کنیم، فقط با بازدید از پروفایل آن. همچنین نشان می‌دهد که چه چیزهای مشترکی بین دو نفر وجود دارد به‌طوری که به راحتی می‌توانیم در که کنیم که تا چه حد کاربر دیگری با ما شباهت دارد. نکته مهم دیگر این است که در LinkedIn اگر ما به پروفایل شخصی نفوذ کنیم، این کاربر متوجه خواهد شد که کسی پروفایل آن را دیده است. LinkedIn مانند فیسبوک همچنین به ما اجازه می‌دهد تا تقریباً همه چیز را تنظیم کنیم.

یک مکان عالی برای شغل یابی و همچنین ارائه‌دهندگان خدمات شغلی است. پروفایل می‌تواند به عنوان رزومه یا CV استفاده شود که در آن ارائه‌دهندگان خدمات شغلی می‌توانند مستقیماً بر اساس مهارت‌های مورد نیاز جستجو کنند. به غیر از آن صفحه نیازهای شغلی وجود دارد که ما می‌توانیم آن‌ها را جستجو یا ارسال کنیم. ما همچنین می‌توانیم شغل‌ها را بر اساس نوع صنعت یا شرکت فعلی خود دنبال کنیم. کاریابی می‌تواند بر اساس مکان، کلمه کلیدی، عنوان شغل یا نام شرکت جستجو شود.

در حال حاضر از دیدگاه OSINT مانند LinkedIn نیز دارای اطلاعات ساخت یافته زیادی است و می‌توان گفت که اطلاعات حرفه‌ای در مورد یک کاربر و شرکت خاص مانند نام کامل، شرکت فعلی، تجربه گذشته، مجموعه مهارت‌ها، نوع صنعت، شرکت‌های دیگر، جزئیات کار، جزئیات شرکت و غیره وجود دارد و با استفاده

از برخی از تکنیک‌های جستجو پیشرفته در LinkedIn می‌توانیم تمام آن اطلاعات را به‌طور کامل جمع‌آوری کنیم که به‌زودی آن را مورد بحث خواهیم کرد.

توییتر^۱

توییتر شبکه اجتماعی از نوع سرویس میکرو بلاگینگ است. توییتر به ما اجازه می‌دهد تا پیام کوتاه مبتنی بر ۱۴۰ کاراکتر (و یا کمتر) را به‌عنوان توییت بدون ثبت‌نام بخوانیم اما پس از ورود به سیستم، می‌توانیم توییت را بخوانیم و همچنین آن‌ها را بنویسیم. توییتر همچنین به‌عنوان سیستم پیامک اینترنتی شناخته شده است. امروزه توییتر به‌عنوان صدا یا سخنرانی یک فرد در نظر گرفته می‌شود. توییت‌ها به‌عنوان اظهارات در نظر گرفته می‌شوند و بخش‌هایی از بولتن خبری و غیره هستند. به دلیل وجود حساب‌های معتبر به‌عنوان صدای یک شخص در نظر گرفته شده است. تائید حساب یک ویژگی توییتر است که به افراد مشهور یا عمومی اجازه می‌دهد تا به جهان نشان دهند که این حساب واقعی است.

همانند دیگر سایت‌های شبکه‌های اجتماعی زمانی که ما در توییتر ثبت‌نام می‌کنیم، به ما اجازه می‌دهد که یک پروفایل ایجاد کنیم، هر چند حاوی اطلاعات بسیار محدودی از قبیل نام، عملکرد توییتر، پیام وضعیت، جزئیات وب‌سایت و غیره است.

مانند یک نام کاربری است که منحصرآ در توییتر ما را مشخص می‌کند. وقتی می‌خواهیم با یکدیگر ارتباط برقرار کنیم، از این Twitter handle استفاده می‌کنیم. Twitter handle به‌طور کلی با علامت "@" و سپس برخی از کاراکترهای حرفی شروع می‌شود، به‌عنوان مثال، @myTwitterhandle این اجازه را به ما می‌دهد تا پیام خصوصی مستقیم و یا عمومی از طریق توییت ارسال کنیم. همچنین به ما اجازه می‌دهد موضوعی را با استفاده از هشتک "#" دسته‌بندی کنیم. هشتک در ابتدای هر کلمه و یا عبارتی مانند LOL # استفاده می‌شود که معمولاً برای گروه‌بندی یک توییت و یا یک موضوع استفاده می‌شود.

یک کلمه، عبارت یا موضوع که بیشترین برچسب‌گذاری را در یک دوره زمانی داشته باشد، موضوع مورد علاقه^۲ نامیده می‌شود. این ویژگی به ما اجازه می‌دهد تا بدانیم در دنیا چه اتفاقی رخ می‌دهد. توییتر امکان دنبال کردن دیگر کاربران را فراهم می‌کند. ما می‌توانیم توییت‌های افراد دیگر را به اشتراک بگذاریم.^۳ این نیز به ما اجازه

¹ Twitter

² trending topic

³ retweets

می‌دهد تا توییتها مورد علاقه‌مان را مشخص کنیم؛ مانند سایر سایت‌های شبکه اجتماعی نیز به ما اجازه می‌دهد تصاویر و فیلم‌ها (با محدودیت‌های خاص) را به اشتراک بگذاریم. توییت‌های قابل مشاهده^۱ به‌طور پیش‌فرض عمومی‌اند، اما کاربر می‌تواند مشاهده توییت خود را فقط به دنبال کنندگانش محدود کند. امروزه توییتر برای اعلام بیانیه یا پاسخ به چیزی در اینترنت استفاده می‌شود. توییت معتبر به صورت مستقیم از شخص معتبر صورت گرفته است. شرکت‌ها از آن برای تبلیغات استفاده می‌کنند.

برخلاف دو شبکه اجتماعی که قبلًا مورد بحث قرار دادیم توییتر، اطلاعات شخصی و یا حرفه‌ای زیادی را شامل نمی‌شود، اما اطلاعاتی که ارائه می‌دهد مفید است. ما می‌توانیم اطلاعاتی در مورد اجتماعات جمع‌آوری کنیم، مثلاً اگر می‌خواهید اطلاعات بیشتری درباره بلاگ^۲ infosec را جستجو کنید، می‌توانید توییتر را با یک هشتک جستجو کنید و می‌توانید بسیاری از توییت‌های مربوط به آن را دریافت کنید. برخلاف سایر سایت‌های شبکه اجتماعی توییتر مقدار زیادی از اطلاعات ساختاری بر اساس عبارات، کلمات و یا موضوعات را دارد.

Google+

سایت شبکه اجتماعی شرکت گوگل است. همچنین به عنوان سرویس هویت سنجی شناخته شده که به ما اجازه می‌دهد با محتویات وب ارتباط برقرار کنیم. Google+ دومین سایت بزرگ شبکه اجتماعی پس از فیسبوک با میلیاردها کاربر ثبت شده و فعال است. همان‌طور که گوگل خدمات مختلفی نظیر Gmail، Play store، YouTube، Google Wallet و غیره ارائه می‌دهد، حساب Google+ می‌تواند به عنوان یک حساب پس‌زمینه برای این موارد استفاده شود.

همانند دیگر سایت‌های شبکه‌های اجتماعی که ما در آن‌ها عضو هستیم، Google+ نیز به ما اجازه می‌دهد ثبت‌نام کنیم، اما مزیتی که Google+ در سایر سایت‌های شبکه اجتماعی ایجاد می‌کند این است که کاربران جیمیل به صورت خودکار با یک کلیک می‌توانند عضو شوند؛ مانند سایر سایت‌های شبکه اجتماعی ما می‌توانیم پروفایلی را ایجاد کنیم که حاوی اطلاعات اساسی مانند نام، جزئیات آموزشی و غیره است.

برخلاف سایر سایت‌های شبکه اجتماعی، پروفایل Google+ به‌طور پیش‌فرض عمومی است. این به ما اجازه می‌دهد صفحه پروفایل خود را با اضافه کردن دیگر لینک‌های مختلف رسانه‌های اجتماعی مانند و بلاگ‌ها سفارشی کنیم.

¹ Visibility Tweets

ما می‌توانیم آن را به عنوان یک راه حل پس زمینه برای بسیاری از خدمات گوگل استفاده کنیم. بسیاری از کاربران دارای یک یا چند حساب جیمیل هستند که از آن‌ها فعالانه استفاده می‌کنند، اما در صورت استفاده از Google+ آن‌ها ممکن است همان تعداد حساب را داشته باشند، اما می‌توانند تنها از یک حساب کاربری فعال استفاده کنند؛ بنابراین این احتمال وجود دارد که تعداد کل حساب‌های ثبت شده به نسبت کاربران فعال بسیار کمتر از سایر سایت‌های شبکه‌های اجتماعی باشد.

مانند رقبای خود همچنین اجازه می‌دهد تا به ایجاد، پیوستن به گروه‌ها، پیگیری یا افروختن دوستان، اشتراک گذاری عکس‌ها، فیلم‌ها و مکان‌ها پردازیم، اما ویژگی‌ای که باعث می‌شود Google+ سایت بهتری باشد، دکمه +1 آن است. این دکمه‌ای مشابه در Face Book است، اما مزیت اضافه این است که وقتی شمارش +1 برای یک موضوع یا پیوند بالاتر باشد، رتبه صفحه^۱ در گوگل را افزایش می‌دهد.

در حال حاضر، OSINT از Google+، مانند سایر سایت‌های شبکه‌های اجتماعی استفاده می‌کند که دارای مقدار زیادی اطلاعات ساخت‌یافته از میلیاردها کاربر است. از ویژگی‌های دیگر که باعث می‌شود گوگل بیشترین منبع جمع‌آوری اطلاعات را داشته باشد این است که عمومی است؛ بنابراین هیچ احراز هویت برای دریافت اطلاعات لازم نیست. یکی دیگر از مزایای Google+ در مورد سایر منابع شبکه‌های اجتماعی این است که در اینجا می‌توانیم اطلاعاتی در مورد تمام محتویات گوگل که یک کاربر در اختیار دارد یا دیگر سرویس‌های گوگل که کاربر استفاده می‌کند، دریافت کنیم.

تکنیک‌های جستجو پیشرفته برای برخی از رسانه‌های اجتماعی خاص

بسیاری از سایت‌های رسانه‌های اجتماعی به نوعی از قابلیت جستجو استفاده می‌کنند تا بتوانیم چیزهایی یا افرادی باشیم که علاقه‌مند هستیم را دنبال کنیم. این ویژگی‌ها، اگر به صورت دقیق مورد استفاده قرار گیرند، می‌توانند برای جمع‌آوری اطلاعات پنهان یا غیرمستقیم اما مهم استفاده شوند.

فیسبوک

ما قبلًا در مورد چگونگی جمع‌آوری اطلاعات فیسبوک بحث کردیم که یک جعبه گنج است. جستجوی فیسبوک یکی از قابلیت‌هایی است که به ما کمک می‌کند تا اطلاعات بسیار گران‌قیمت را به دست آوریم.

^۱ PageRank

جستجوی فیسبوک یک ویژگی منحصر به فرد است که جستجوی افراد یا چیزهایی که به نحوی مرتبط با ما مرتبط هستند را بهبود می‌بخشد. ما می‌توانیم جستجوی گراف را برای کشف مکان‌ها، عکس‌ها و جستجوی افراد مختلف انتخاب کنیم. این روش منحصر به فرد به ما اجازه می‌دهد آنچه می‌خواهیم بر اساس حروف اول یا کلمات اول جستجو کنیم. جستجو از خود فیسبوک از قبیل افراد، صفحات، گروه‌ها و مکان‌ها و غیره شروع شده و اگر نتایج مناسب پیدا نشود، جستجو در موتور جستجوی بینگ^۱ آغاز می‌شود و نتایج مناسب را برای کاربر فراهم می‌کند. برای ارائه نتایج مرتبط‌تر، فیسبوک همچنین به رابطه ما یا حداقل منطقه مورد علاقه و تجربه گذشته‌مان نگاه می‌کند، به عنوان مثال، می‌توانیم آنچه آن‌ها دوست دارند، نظرات به اشتراک گذاشته‌شده، برچسب‌گذاری شده، ثبت‌نام شده و یا آنچه به طور مستقیم توسط ما و یا توسط دوستانمان مشاهده شده است را در رتبه‌بندی نتیجه دخیل کنیم. همچنین می‌توانیم نتایج بر اساس عناصر اجتماعی مانند افراد، صفحات، مکان‌ها، گروه‌ها، برنامه‌ها، رویدادها و نتایج وب فیلتر کنیم. تکنولوژی که فیسبوک در جستجوی گراف خود استفاده می‌کند می‌تواند به عنوان پایه وب معنایی تعریف شود که ما در پایان این فصل بحث خواهیم کرد.

در حال حاضر هرچند که ما در مورد ویژگی جستجو که می‌تواند ما را به یافتن چیزهای مختلف در فیسبوک راهنمایی کند پرداختیم، اما هنوز هم این سؤال مطرح است که چطور؟ حالا با چند سؤال ساده شروع می‌کنیم.

فقط عکس‌ها را در نوار جستجو قرار دهید و از طریق فیسبوک برخی از پرس‌وجوها مانند عکس‌های دوستان من، عکس‌های مورد علاقه من، عکس‌های من، عکس‌های X و غیره توسط فیسبوک پیشنهاد می‌شود و به همین ترتیب ما می‌توانیم بسیاری از نمایش‌های مرتبط با عکس را دریافت کنیم. ممکن است پرسش‌های خودمان را ایجاد کنیم بنابراین بر اساس عکس‌ها می‌توان نتیجه گرفت که در نهایت یک پرس‌وجو از قبیل "عکس‌هایی که توسط دوستانم قبل از سال ۲۰۱۳ در دهلی هند تحصیل کرده‌اند، گرفته شده"؛ بنابراین اساساً بر اساس کلمات کلیدی، ما می‌توانیم پرسش‌های پیچیده‌ای برای نتایج مورد نظر ایجاد کنیم؛ هرچند فیسبوک برخی از درخواست‌های غیرمنتظره را بر اساس کلمات کلیدی ذکر شده در نوار جستجو پیشنهاد می‌کند. به طور مشابه می‌توانیم افراد، مکان‌ها، رستوران‌ها، کارکنان یک شرکت خاص، موسیقی و غیره را جستجو کنیم.

برخی از پرسش‌های پایه مربوط به عناصر مختلف اجتماعی به شرح زیر است:

۱. موسیقی که ممکن است دوست داشته باشم

^۱ Bing

۲. شهرهایی که دوستان من بازدید کردند
۳. رستوران‌های ماقائو، چین
۴. افرادی که مرا دنبال می‌کنند
۵. زنانی که در ایالات متحده زندگی می‌کنند
۶. دوستان من که فیلم‌های X-Men را دوست دارند
۷. افرادی که فوتبال را دوست دارند

اکنون اجازه دهید از این پرسش‌های ساده برای ایجاد یک مجموعه پیچیده استفاده کنیم: "زنان مجرد با نام "رachel" در لس‌آنجلس و کالیفرنیا که عاشق فوتبال هستند و در ایالات متحده بازی می‌کنند". ما می‌توانیم پرس‌وجو را با استفاده از فیلترهایی بر اساس اطلاعات اساسی مانند نام، سن، جنسیت، کار، بر اساس تحصیلات مانند کلاس، دانشگاه، مدرک و بر اساس دوست و مخالف، بروجسب‌ها، روابط اجتماعی انجام دهیم. در حال حاضر خلاقيت ما است که می‌تواند ما را در ایجاد پرسش‌های متفاوت برای نتیجه مطلوب باری کند.

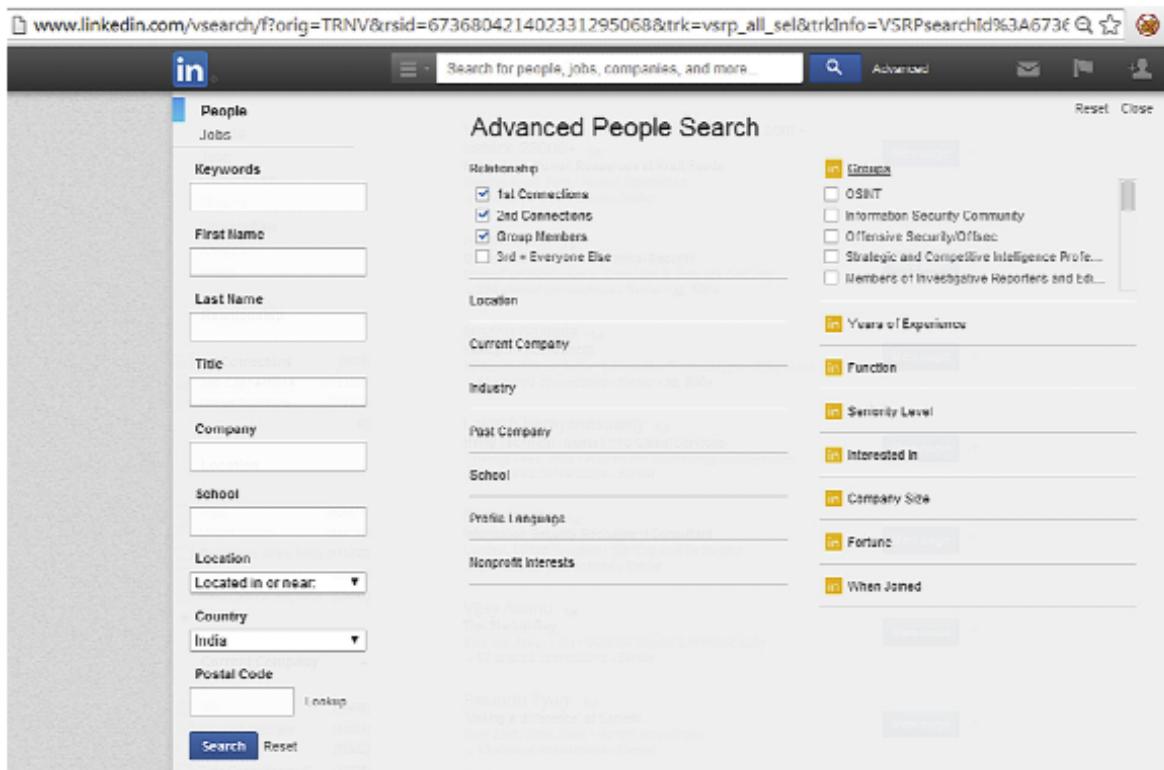
The screenshot shows a Facebook search results page. The search query is: "Single women named "Rachel" from Los Angeles, California who like Football and Game of Thrones". The results page features a profile picture of a woman named Rachel, followed by her name and a redacted section. Below her name, it says "University of Or...". It also lists her location as "From Los Angeles, California · Lives in Eugene, Oregon", her status as "Single", and her interests as "Likes Oregon Football, Game of Thrones and 731 others". It also mentions she "Studies Theatre at [redacted]". At the bottom of the results page, there is a note: "Relationship-based searches are still being built, so you may see additional results here in the future. Learn more about who can see each others' relationships in news feed, search and other places on Facebook." The page ends with "End of results".

LINKEDIN

دارای داده‌های ساختار یافته از میلیاردها کاربر است. بیایید ببینیم چگونه در این پلتفرم خاص جستجو LinkedIn کنیم. LinkedIn یک نوار جستجو در بالای صفحه برای جستجو افراد، مشاغل، شرکت‌ها، گروه‌ها، دانشگاه‌ها،

مقالات و بسیاری دیگر فراهم می‌کند. برخلاف فیسبوک، LinkedIn دارای صفحه جستجوی پیشرفته‌ای است که ما می‌توانیم از فیلترهای آن برای نتیجه کارآمد استفاده کنیم. لینک جستجوی پیشرفته در LinkedIn:

<https://www.linkedin.com/vsearch/p/?trk=advsrch&adv=true>



این صفحه جستجوی پیشرفته اجازه می‌دهد تا به جستجوی شغل و مردم بر اساس کار فعلی، شغل قبلی، عنوان شغلی، کد پستی، علاقه‌مندی، نوع صنعت و غیره بپردازیم.

ورودی‌های مختلف و استفاده از آن‌ها

- کلمه کلیدی: جعبه ورودی کلمه کلیدی به کاربر اجازه می‌دهد تا هر نوع کلیدواژه‌ای مانند *pentester* یا *نویسنده* و غیره را وارد کند.
- نام: می‌توانیم با استفاده از نام جستجو کنیم.
- نام خانوادگی: می‌توانیم از نام خانوادگی استفاده کنیم.
- عنوان: با استفاده از آن کاربر با یک منوی کشویی با چهار گزینه برای انتخاب مانند گذشته یا فعلی، گذشته، گذشته و فعلی برای غنی‌سازی جستجو روبرو می‌شود.

- شرکت: می‌توانیم با استفاده از نام شرکت جستجو کنیم. همچنین با یک منوی کشویی با گزینه‌هایی مورد استفاده قرار می‌گیرد.
- محل: این جعبه کشویی دارای دو گزینه می‌باشد.
- کشور: جستجو بر اساس کشور انجام می‌شود
- کد پستی: جستجو بر اساس کد پستی انجام می‌شود. یک دکمه جستجو برای کاربر وجود دارد تا بررسی کند که آیا کد پستی وارد شده برای مکان دلخواه است یا خیر. با وارد کردن کد پستی به‌طور خودکار درون جعبه کشویی موارد زیر را می‌توانید انتخاب کنید:

1. 10mi (15km)

2. 25mi (40km)

3. 35mi (55km)

4. 50mi (80km)

5. 75mi (120km)

6. 100mi (160km)

این می‌تواند برای انتخاب شعاع منطقه‌ای که می‌خواهید در جستجو همراه با کد پستی وارد کنید، مورد استفاده قرار گیرد.

- ارتباط: این جعبه حاوی گزینه‌هایی برای فعال کردن جستجوی اتصال مستقیم، اتصال جستجوی اتصال، جستجوی گروه و جستجو است. کاربر می‌تواند گزینه پنجم، یعنی $+3$ برای همه چیز را جستجو کند.
- محل: این گزینه برای اضافه کردن یک مکان دیگر است که قبلاً در کد پستی ذکر شده است.
- شرکت فعلی: این گزینه به کاربر اجازه می‌دهد اطلاعات شرکت فعلی را به صورت دستی اضافه کند.
- صنعت: این یک کاربر با گزینه‌های مختلف برای انتخاب یک یا چند صنعت در یک زمان فراهم می‌کند.
- شرکت گذشته: این گزینه اجازه می‌دهد تا به صورت دستی اطلاعات مربوط به شرکت را اضافه کنید.
- مدرسه: می‌توانیم جزئیات را به صورت دستی اضافه کنیم.
- زبان: انتخاب یک زبان را برای کاربر فراهم می‌کند.
- علاقه‌مندی‌ها: کاربر را قادر می‌سازد تا دو گزینه را انتخاب کند.

گزینه‌های موجود در سمت راست صفحه جستجوی پیشرفته فقط برای اعضای دارای حساب وجود دارد. دیگر قابلیت‌های اضافه شده نیز وجود دارد فقط برای کاربران دارای حساب که عبارت‌اند از:

- گروه‌ها
- تجربه
- عملکرد
- سطح ارشد
- علاقه‌مند به
- اندازه شرکت
- آینده
- زمانی که ثبت‌نام کردید

جدا از همه این LinkedIn ما را قادر به استفاده از اپراتورهای بولی می‌کند. در زیر اپراتورها با مثال‌های ساده آورده شده است:

AND: این را می‌توان برای اتحاد دو کلیدواژه مانند: 

developer AND tester

OR: می‌توان برای گزینه‌ها استفاده کرد. بگذارید بگوییم یک کارگزار می‌خواهد یک شخص را برای صنعت امنیتی استخدام کند: 

pentester OR "security analyst" OR "consultant" OR "security consultant" OR "information security engineer."

NOT: این را می‌توان برای حذف چیزی از چیزهای دیگر استفاده کرد مانند یک کارمند می‌خواهد فردی را برای برخی از کارها، اما نه از دامنه آموزش استخدام کند: 

developer NOT trainer

پرانتر: این اپراتور قدرتمند است که در آن کاربر می‌تواند برای گروه‌بندی از آن استفاده کند مانند:
(Pentester OR "Security Analyst" OR "Consultant" OR "Security Consultant" OR "Information Security Engineer")
NOT Manager 

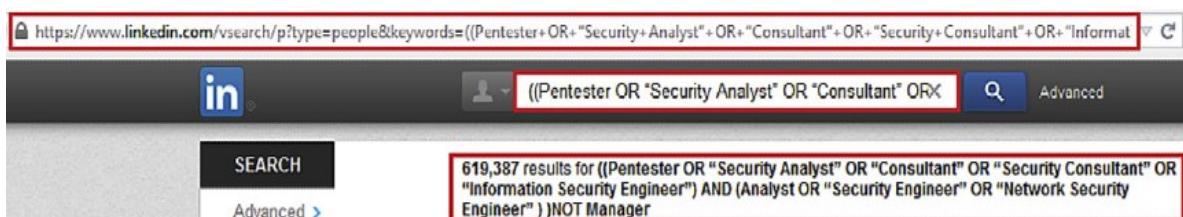
 نقل قول^۱: می‌توان آن را برای ساختن بیش از یک کلمه به عنوان کلمه کلیدی استفاده کرد مانند:

“Information Security Engineer”

اگر از کلمه‌ی مشابه بدون نقل قول استفاده کنیم، آن را به عنوان سه کلیدواژه مختلف در نظر می‌گیرد.

برخلاف موتورهای جستجو که می‌توانند کلمه کلیدی محدود در جعبه جستجو داشته باشند، LinkedIn اجازه می‌دهد تا کلمات کلیدی نامحدود را به عنوان یک افونه مهم برای جستجو استفاده کرد؛ بنابراین آزادی کاربر برای استفاده از هر تعداد کلیدواژه‌ای که او می‌خواهد با استفاده از اپراتورها برای ایجاد یک پرس‌وجو پیچیده برای به دست آوردن نتیجه مورد نظر فراهم است. مثال یک پرس‌وجوی پیچیده برای کارکنان حرفه‌ای امنیت اطلاعات، اما نه مدیران به صورت زیر است:

((Pentester OR “Security Analyst” OR “Consultant” OR “Security Consultant” OR “Information Security Engineer”) AND (Analyst OR “Security Engineer” OR “Network Security Engineer”)) NOT Manager.



تowییتر

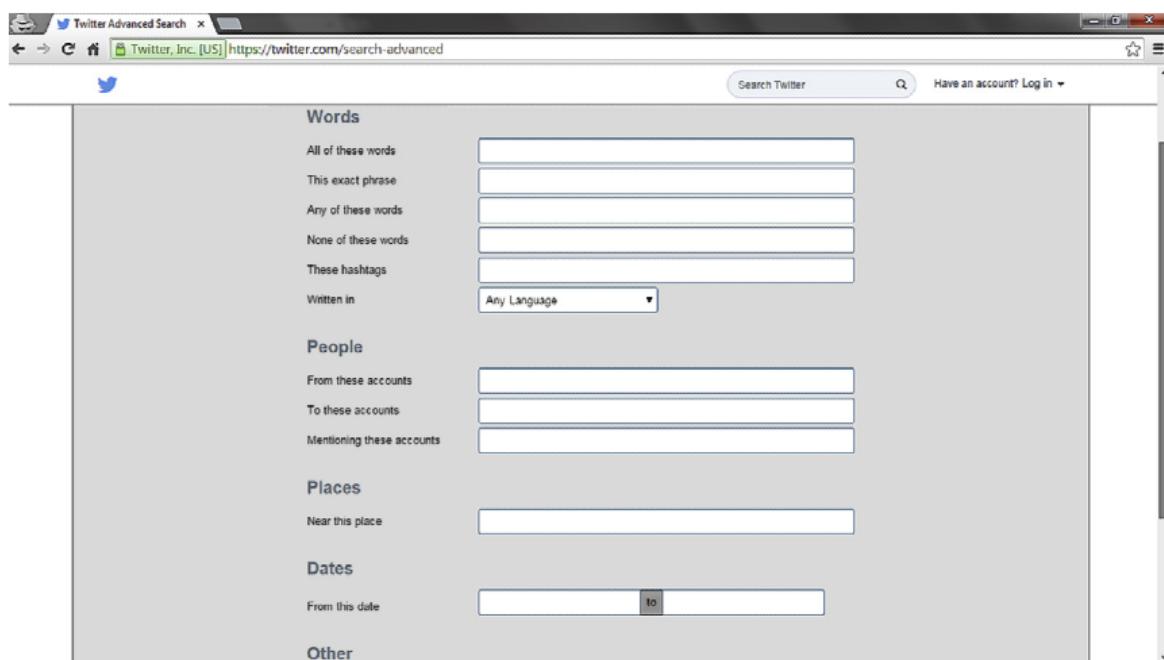
همان‌طور که پیش از این مورد بحث قرار گرفت توییتر اساساً یک میکروبلاگینگ در قالب توییت‌هاست و از این رو ما به دنبال توییت‌ها هستیم. به سادگی با وارد کردن یک کلمه کلیدی ما توییت‌های مرتبط با این کلمه را می‌بینیم، اما برای دسترسی به نتایج خاص‌تر نیاز به استفاده از برخی از اپراتورهای جستجوی پیشرفته وجود دارد که با برخی از آن‌ها آشنا می‌شویم.

در صورتی که بخواهیم توییت‌ها را برای عبارات خاص جستجو کنیم، می‌توانیم از " " استفاده کنیم تا عبارت دلخواه را جستجو کنیم. برای دنبال کردن هشتگ^۲، می‌توانیم به راحتی "# را تایپ کنیم. در صورتی که بخواهیم عبارتی را جستجو کنیم و عبارتی دیگر را حذف کنیم، می‌توانیم از عملگر "- " استفاده کنیم. برای مثال،

¹ Quotation

² hashtag

می‌خواهیم هک را جستجو کنیم، اما امنیت را نمی‌خواهیم، سپس می‌توانیم از security-hack استفاده کنیم. اگر بخواهیم که نتایج شامل یک یا هر دو عبارت باشد، ما می‌توانیم از اپراتور OR مانند Hack OR Security استفاده کنیم. برای جستجوی نتایج مربوط به یک حساب خاص توییتر، ما به‌سادگی توسط هندل توییتر^۱ استفاده می‌کنیم (Sudhanshu_C@). اپراتورهای فیلتر می‌توانند برای دریافت نوع خاصی از نتایج استفاده شوند. به عنوان مثال، برای دریافت توییتر حاوی لینک‌های ما می‌توانیم از filter:link استفاده کنیم. به عنوان مثال برای فیلتر بر اساس فرستنده و گیرنده می‌توان از From:sudhanshu_c, To:paterva استفاده کرد. به طور مشابه از Since و Until می‌توانید برای مشخص کردن جدول زمانی استفاده کنید، به عنوان مثال hack since:2014-01-27, hack until:2014-01-27. همه این اپراتورهای ذکر شده را می‌توان برای نتایج بهتر و دقیق‌تر ترکیب کرد. برای بررسی ویژگی‌های دیگر ما می‌توانیم از صفحه جستجوی پیشرفته توییتر در <https://Twitter.com/search-advanced> استفاده کنیم که دارای برخی از ویژگی‌های دیگر مانند فیلترینگ مبتنی بر مکان است.



جستجو در وبسایت اجتماعی باز^۲

در مورد شبکه‌های اجتماعی یاد گرفتیم و چگونگی جستجو در آنها را دیدیم، اما برخی از پلتفرم‌هایی که باید جستجو کنیم از هیچ یک از ویژگی‌های جستجوی پیشرفته مورد بحث ما پشتیبانی نمی‌کنند. نگران نباشید، یک جستجوی ساده گوگل به ما کمک خواهد کرد. اپراتور جستجوی گوگل به‌سادگی راهی برای محدود کردن

¹ Twitter handle

² OPEN SOCIAL MEDIA WEBSITE

نتایج جستجو توسط گوگل در یک محدوده خاص است؛ بنابراین آنچه اپراتور "site" انجام می‌دهد این است که نتایج جستجو را تنها به یک وب‌سایت خاص محدود می‌کند، مثلاً اگر می‌خواهیم کلمه "hack" را جستجو کنیم، اما فقط می‌خواهیم نتایج از وب‌سایت انگلیسی ویکی‌پدیا، پرس‌وجو شود در گوگل عبارت زیر وارد می‌شود: site:en.wikipedia.org hack. این نتایج برای کلمه hack در سایت مشخص شده است. در حال حاضر اگر می‌خواهیم در کلمات مختلف را جستجو کنیم، اپراتور دیگری در گوگل وجود دارد که مفید است که اپراتور OR است. این اپراتور به ما اجازه می‌دهد تا نتایج را برای هر یک از کلمات کلیدی که قبل و بعد از آن ذکر شده است، به دست آوریم. هنگامی که آن را با اپراتور site ترکیب می‌کنیم، به ما اجازه می‌دهد که نتایج جستجو را از آن سایت خاصی جستجو کنیم. به عنوان مثال، اگر ما بخواهیم کلمه "hack" را در فیسبوک و همچنین LinkedIn جستجو کنیم، می‌توانیم از site:Facebook.com OR site:LinkedIn.com hack استفاده کنیم. همان‌طور که می‌بینیم این اپراتورها ساده‌اند اما بسیار مؤثر هستند، ما در مورد این اپراتورها در گوگل و بعضی از موتورهای جستجوی کمتر شناخته شده در فصل‌های آینده بحث خواهیم کرد.

وب ۳۰

ما در مورد وب ۲۰، ارتباط آن و نحوه تأثیر آن و همچنین نحوه استفاده در برخی از شبکه‌های اجتماعی محبوب، بحث کردیم. بسیاری از داده‌های موجود در وب بدون ساختار هستند، هرچند موتورهای جستجو مانند گوگل، یاهو و غیره وجود دارند که به‌طور مداوم وب را فهرست می‌کنند، اما داده‌ها به هیچ وجه دارای ساختار استاندارد نیستند. این بدان معنی است که هیچ فرمت داده مشترک وجود ندارد که کل وب را دنبال کند. مشکل این است که هرچند موتورهای جستجوگر می‌توانند ما را راهنمایی کنند تا اطلاعاتی را که دنبال می‌کنیم پیدا کنیم، اما نمی‌توانند به ما در پاسخگویی به پرسش‌های پیچیده یا دنبالهای از پرسش‌ها کمک کنند. به همین دلیل وب معنایی^۱ به وجود آمد. وب معنایی اساساً یک مفهوم است که وب به دنبال یک فرمت داده مشترک است که اجازه می‌دهد داده‌ها معنی پیدا کنند. برخلاف وب ۲۰ که در آن عامل انسانی برای جمع‌آوری داده‌های خاص موردنیاز است، ماشین‌های وب معنایی قادر به پردازش داده‌ها بدون دخالت انسان هستند. این اجازه می‌دهد که داده‌ها نه تنها با لینک، بلکه معنا و روابط هم مرتبط باشند. این نه تنها به اشتراک‌گذاری داده را ممکن می‌سازد بلکه ماشین‌ها قادر به ایجاد ارتباط بین داده‌ها از حوزه‌های مختلف و ایجاد معنی خارج از آن خواهند بود. وب معنایی بخش مهمی از وب آتی و وب ۳۰ است و این رو نیز بسیاری از آن به عنوان وب معنایی یاد می‌کنند.

^۱ semantic web

به غیر از وب معنایی، جنبه‌های دیگری نیز وجود دارد که می‌تواند به وب ۳.۰ کمک کند، مانند جستجو شخصی، تجزیه و تحلیل زمینه، تحلیل احساسات و غیره. برخی از این ویژگی‌ها در برخی از قسمت‌های وب قابل مشاهده هستند، اما ممکن است به اندازه کافی بالغ نباشند، اما تکامل آن سریع و واضح است.

فصل ۳: درک مرورگرها

مقدمه

در فصل اول کمی درباره مرورگرهای وب به‌طور کلی بحث کردیم، سپس برخی از مرورگرهای محبوب مانند کروم و فایرفاکس معرفی و سعی شد فرآیند پشت مرورگر را به صورت ساده بیان کنیم. اکنون زمان آن است که بفهمیم دقیقاً چه اتفاقی در پس زمینه آن‌ها رخ می‌دهد. شما ممکن است فکر کنید که چرا این مورد نیاز است. دلیل تمرکز ما بر مرورگرهای وب در مورد جنبه‌های مختلف آن در جزئیات است زیرا اکثر ابزارهایی که ما در این کتاب استفاده می‌کنیم عمده‌تاً مبنی بر وب و ارتباط با این ابزار مبنی بر وب است و از مرورگرهای زیادی استفاده خواهد شد. به همین دلیل بسیار مهم است که نیاز است کار یک مرورگر را درک کنید. یادگیری روند درونی نحوه عملکرد مرورگر به ما کمک می‌کند تا انتخاب و استفاده از آن را به طور مناسب انجام دهیم. بعد‌ها همچنین در مورد راه‌هایی برای بهبود ویژگی‌های مرورگرهای مرورگرها یاد خواهیم گرفت. در حال حاضر بدون اتلاف وقت در تعاریف و توصیفاتی که قبلاً پوشش داده‌ایم، باید مستقیم به نقطه "اسرار عملیات مرورگر" برسیم.

نحوه عملکرد مرورگر

هنگامی که یک مرورگر را باز می‌کنیم، به طور کلی نوار آدرسی می‌بینیم که می‌توانیم آدرس و براکه می‌خواهیم مرور کنیم، وارد کنیم. یک دکمه نشانک^۱ برای ذخیره لینک‌ها برای استفاده در آینده نیز وجود دارد؛ دکمه نمایش نشانک، جایی است که همه نشانه‌های لینک شده ما در مرورگر وجود دارد؛ دکمه‌های عقب و جلو^۲ برای مرور صفحات استفاده می‌شود؛ دکمه خانه^۳ برای هدایت هر صفحه به صفحه اصلی که قبلاً در مرورگر تنظیم شده است و دکمه تنظیمات^۴ برای انجام تنظیمات مرورگر مانند تنظیم صفحه اصلی، محل دانلود، تنظیمات پروکسی و بسیاری از تنظیمات دیگر استفاده می‌شود. مکان این دکمه‌ها ممکن است با تغییر نسخه‌ها، تغییر کند تا تجربه کاربری بهتری را فراهم کند، اما در رابط مرورگرها شما تمام این دکمه‌ها را خواهید یافت.

همه مرورگرها دارای رابط کاربری کاملاً مشابه هستند، با اکثر ویژگی‌های مشترک که قبلاً مورد بحث قرار گرفت، اما هنوز امکانات و ویژگی‌هایی وجود دارد که هر مرورگر را منحصر به فرد می‌کند. مرورگرهای محبوبی مانند کروم، فایرفاکس، اینترنت اکسلپورر، اپرا و سافاری وجود دارند، اما همان‌طور که قبلاً در فصل ۱ مورد بحث قرار گرفتیم، ما بیشتر از دو مرورگر که در نسخه‌های منبع باز هستند شامل کروم و فایرفاکس استفاده می‌کنیم.

تاریخچه مرورگرها

اولین مرورگر توسط Tim Berners-Lee در سال ۱۹۹۱ نوشته شده بود که تنها نتایج متنی را نمایش می‌داد. اولین مرورگر گرافیکی تجاری کاربر پسند Mosaic بود. برای استانداردسازی فناوری وب یک سازمان به نام کنسرسیوم جهانی وب^۵ شناخته شد که در سال ۱۹۹۴ به عنوان W3C نامیده شد. تقریباً تمام مرورگرها در اواسط دهه ۱۹۹۰ وارد بازار شدند. مرورگرها امروزه بسیار قدرتمندتر از اوایل دهه ۱۹۹۰ هستند. تکنولوژی به سرعت از متن به چند رسانه‌ای تکامل یافته و هنوز هم در حال حرکت است، امروز مرورگرها انواع مختلفی از منابع وب مانند ویدیو، تصاویر، اسناد همراه با HTML و CSS را نمایش می‌دهند. نحوه نمایش این منابع توسط W3C مشخص شده است.

¹ bookmark

² back and forward

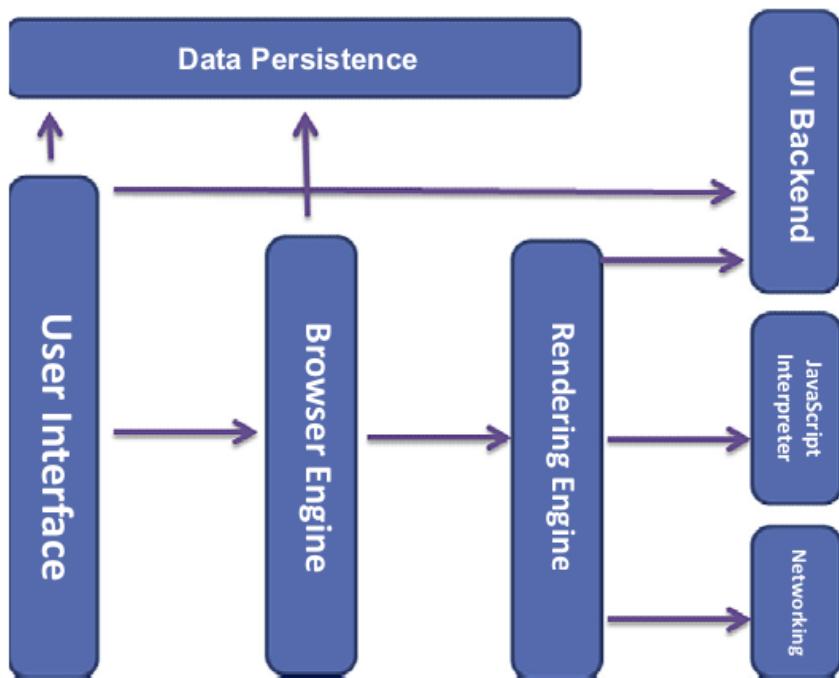
³ Home

⁴ Option

⁵ World Wide Web Consortium

معماری مرورگرها

معماری مرورگر از مرورگر به مرورگر متفاوت است، بنابراین بر اساس اجزاء رایج اگر معماری را استخراج کنیم، چیزی به شرح زیر خواهد بود.



رابط کاربر^۱

رابط کاربر در اینجا چیزی است که ما قبلاً در بالا بحث کردیم. همه چیز در مورد دکمه‌ها و میله‌ها برای دسترسی به ویژگی‌های عمومی است.

موتور مرورگر^۲

ترکیبی از موتور طرح^۳ با موتور رندر است. موتور طرح چیزی جز رابط کاربری نیست.

¹ USER INTERFACE

² BROWSER ENGINE

³ layout engine

موتور رندر^۱

مسئولیت نمایش دادن منابع وب مورد درخواست را با تجزیه^۲ مطالب انجام می‌دهد. به‌طور پیش فرض می‌تواند XML و تصاویر را تجزیه کند. از پلاگین‌ها و یا افزونه‌های مختلف برای نمایش سایر نوع داده‌ها مانند فلش، PDF و غیره استفاده می‌کند.

موتورهای مختلف رندر مانند Trident، Gecko و WebKit وجود دارند. موتور رندری که به‌طور گسترده استفاده می‌شود WebKit یا نسخه خاص آن است. Trident و Gecko موتورهای رندر منبع باز هستند در حالی که Trident نیست. فایرفاکس از Gecko استفاده می‌کند، Safari از WebKit استفاده می‌کند، اینترنت اکسپلورر از Trident استفاده می‌کند، Chrome و Opera از Blink استفاده می‌کنند که یک نوع از WebKit است. موتورهای مختلف رندر از الگوریتم‌های مختلف استفاده می‌کنند و همچنین روش‌های مختلفی برای تجزیه یک درخواست خاص دارند. بهترین مثال زمانی است می‌بینید برخی از وب‌سایتها با یک مرورگر خاص کار می‌کنند، زیرا این وب‌سایتها با موتور رندر مرورگر طراحی سازگار شده‌اند بنابراین در مرورگرهای دیگر به خوبی کار نمی‌کنند.

شبکه‌سازی^۳

این جزء اصلی مرورگر است. اگر نتواند کار کند، تمام فعالیت‌های دیگر با مشکل مواجه خواهد شد. اجزاء شبکه را می‌توان به عنوان مدیر سوکت^۴ توصیف کرد که از واکشی منابع مراقبت می‌کند. این یک بسته کامل است که شامل رابط برنامه‌نویسی نرم‌افزار، معیارهای بهینه‌سازی، خدمات و غیره است.

UI BACKEND

ویجت رابط کاربری را فراهم می‌کند و جعبه‌های مختلف، فونت‌ها و غیره را طراحی می‌کند.

متترجم جاوا اسکریپت^۵

برای تفسیر و اجرای کد اسکریپت جاوا استفاده می‌شود.

¹ RENDERING ENGINE

² parse

³ NETWORKING

⁴ socket manager

⁵ JAVASCRIPT INTERPRETER

ماندگاری داده^۱

زیرسیستمی است که تمام اطلاعات موردنیاز برای ذخیره در مرورگر مانند داده‌های نشست^۲ را ذخیره می‌کند که شامل بوک مارک‌ها، کوکی‌ها، حافظه‌های ذخیره‌سازی وغیره است. مرورگرها کوکی‌هایی را که حاوی جزئیات مرورگر هستند ذخیره می‌کنند و اغلب از طریق سایت‌های بازاریابی برای تبلیغات استفاده می‌شوند. بگذارید بگوییم ما می‌خواهیم هدفونی خریداری کنیم بنابراین از سایت بازدید کرده و هرگز آن را خریداری نکردیم. سپس سایت‌های بازاریابی این اطلاعات را دریافت می‌کنند و شروع به تبلیغ از همان محصول انجام می‌دهند. این قطعاً اهمیت خاص خود را دارد.

تحمل پذیری قطعی^۳

تمام مرورگرها دارای تحمل پذیری خطای سنتی هستند تا از اشتباهات شناخته شده برای جلوگیری از اشتباهات نحوی استفاده شود. مرورگرها این ویژگی منحصر به فرد را دارند تا دستورالعمل نامعتبر را به دست آورند و به همین دلیل هیچ خطای نحوی نامعتبری در نتیجه را دریافت نکنیم. هرچند مرورگرهای مختلف این خطاهای را به صورت متفاوتی به نمایش می‌گذارند، اما به هر حال تمام مرورگرها این کار را انجام می‌دهند.

چند رشته‌ای^۴

تقریباً هر پروسه در همه مرورگرها یک رشته هستند، با این حال، عملیات شبکه چند مرحله‌ای است. این کار با استفاده از ۲ تا ۶ موضوع موازی انجام می‌شود. در کروم، فرایند زبانه^۵ رشته اصلی است، در حالی که در مرورگرهای دیگر مانند فایرفاکس و سافاری فرایند رندر^۶ رشته اصلی است.

ویژگی‌های مرورگرها

مرورگر وب یک اصطلاح بسیار ساده و عمومی است که همه ما از آن آگاهیم، اما از اهمیت آن آگاهی نداریم. مرورگر وب پنجره‌ای برای ما فراهم می‌کند تا همه اطلاعات موجود در وب را مرور کنیم. مرورگرها می‌توانند برای هر دو هدف، مرور آنلاین و همچنین مرور آفلاین استفاده شوند. مرور آنلاین مروری است که ما به طور مرتب با اتصال به اینترنت انجام می‌دهیم. مرور آفلاین به معنی باز کردن محتوای محلی HTML در یک مرورگر

¹ DATA PERSISTENCE

² Session

³ ERROR TOLERANCE

⁴ THREADS

⁵ tab process

⁶ rendering process

است. مرورگر مدرن نیز ویژگی‌هایی برای ذخیره صفحات HTML برای مرور صفحات فراهم می‌کند. این ویژگی اجازه می‌دهد تا کاربر بدون نیاز به اتصال به اینترنت به مرور صفحات پردازد. همه ما از این ویژگی بعضی وقت‌ها استفاده کرده‌ایم. هنگامی که ما یک صفحه را برای نمایش اطلاعات ذخیره می‌کنیم، گاهی اوقات ممکن است ما متوجه شده باشیم که برخی از محتویات در یک صفحه در طول مرورگر گم شده‌اند. دلیل این امر آن است که هنگامی که یک صفحه را ذخیره می‌کنیم، فقط رسانه‌های مستقیم^۱ موجود در صفحه را ذخیره می‌کنند، اما اگر یک صفحه حاوی منابع از سایتی دیگر باشد، این موارد در دیدگاه غلط دیده می‌شوند. بیایید در مورد برخی از ویژگی‌های اضافه شده توسط مرورگرها بحث کنیم.

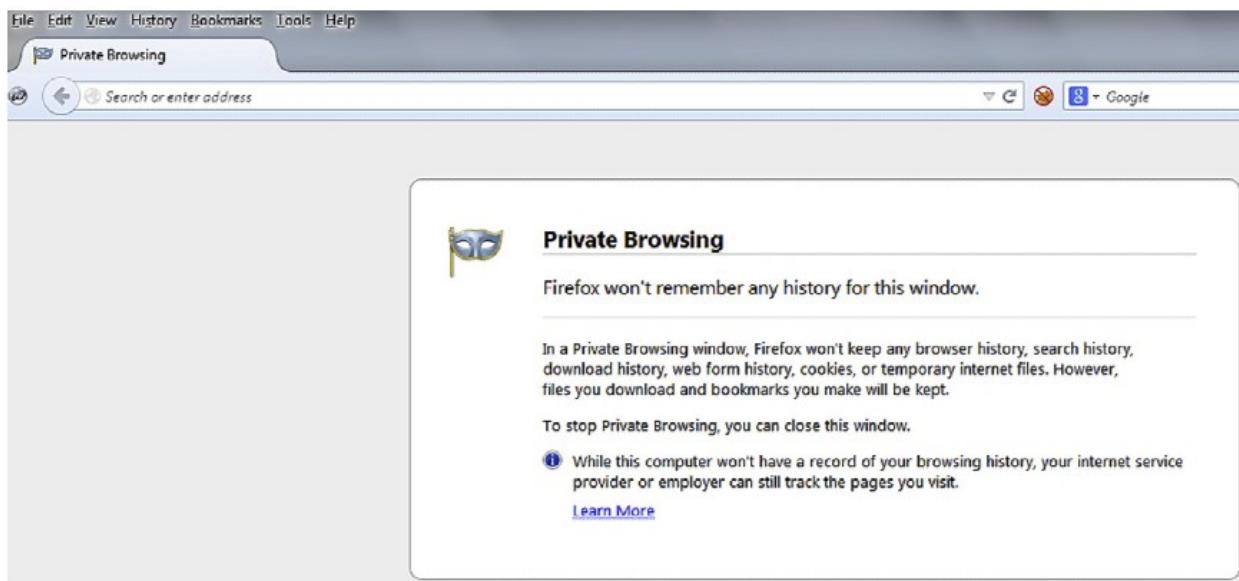
مرورگر خصوصی^۲

Incognito (ناشناس بودن) اصطلاح کروم برای مرورگر خصوصی است، در حالی که فایرفاکس از اصطلاح private browsing (مرورگر خصوصی) استفاده می‌کند که اجازه می‌دهد تا به مرورگر اینترنت بدون ذخیره سازی جزئیات نشست پردازیم. ما می‌توانیم از مرورگر خصوصی برای انجام معاملات آنلاین، خرید آنلاین، باز کردن ایمیل‌های رسمی در دستگاه‌های عمومی و موارد دیگر استفاده کنیم.

در فایرفاکس و کروم می‌توانیم این گزینه را در نزدیکی گزینه پنجره جدید پیدا کنیم. کلید میانبر برای باز کردن مرور ایمن در فایرفاکس Ctrl + Shift + P است و برای کروم Ctrl + Shift + N است. تفاوت بین پنجره مرورگر طبیعی و یک پنجره مرور خصوصی، وجود یک آیکون اضافی در پنجره نوار عنوان است. در فایرفاکس آن یک آیکون mask است در حالی که در کروم آیکون detective است. مرورگرها از این نوع آیکون‌های فانتزی استفاده می‌کنند.

¹ direct media

² PRIVATE BROWSING



در مرورگر خصوصی صفحات بازدید شده، جزئیات، ورودی فرم‌ها، ورودی نوار جستجو، رمزهای عبور، لیست دانلودها، فضاهای ذخیره شده، فایل‌های موقت و یا کوکی‌ها ذخیره نخواهند شد. اگر چه داده‌های بارگیری شده یا نشانه‌گذاری شده در مرورگر این در سیستم محلی ذخیره می‌شوند.

چرا از مرورگر خصوصی استفاده نمی‌شود؟

این روش تنها به کاربر کمک می‌کند که در سیستم محلی ناشناس باشد در حالی که ارائه دهنده خدمات اینترنت، مدیر شبکه یا مدیر وب می‌توانند جزئیات مرور را پیگیری کرده و همچنین کاربر را از کیلاگرهای^۱ یا جاسوس افزارها^۲ محافظت نخواهد کرد.

همیشه گزینه‌ای در دسترس برای حذف داده‌های ذخیره شده توسط مرورگر به صورت دستی وجود دارد. ما می‌توانیم به سادگی بر روی دکمه پاکسازی تاریخچه اخیر^۳ کلیک کرده و انتخاب کنیم که چه چیزی باید حذف شود.

کامل سازی خودکار^۴

تقریباً تمام مرورگرهای این قابلیت را دارند تا از آن برای ذخیره اطلاعات خاص مانند جزئیات فرم و رمزهای عبور استفاده کنند. این ویژگی دارای نامهای مختلف در مرورگرهای متفاوت است و یا با موتورهای مختلف رندر

¹ keyloggers

²

³ clear recent history

⁴ AUTOCOMPLETE

مشخص شده است. بعضی از نام‌های آن تکمیل رمز عبور خودکار، فرم پیش‌فرض، تکمیل فرم، Roboform، یادآوری رمز عبور^۱ و غیره هستند.

مرورگرها امکانی برای کاربر برای اینکه تنظیم کند آیا این اطلاعات ذخیره شوند و یا نه فراهم می‌کنند، اگر جواب بله باشد، چه و چه نوع آن باید ذخیره شود.

در فایرفاکس برای جلوگیری از ذخیره‌سازی رمز عبور، به Menu → Options → Security بروید و گزینه "Remember passwords for sites" را از حالت انتخاب خارج کنید. هر چند می‌توانیم رمز عبور را در قالب رمزگذاری شده با استفاده از تعریف مرورگر ذخیره کنیم.

در کروم به Menu → Settings → Show advanced settings → Under Passwords and forms بروید و گزینه "Enable Auto-fill to fill out web forms in single click" and "Offer to save your web password." را از حالت انتخاب خارج کنید.

بعضی از برنامه‌های وب آن را به عنوان یک آسیب‌پذیری یا خطر امنیتی احتمالی دانسته، بنابراین آنها از ویژگی autocomplete = off در مقدار جعبه ورودی استفاده می‌کنند و نمی‌خواهند مقادیر آن توسط مرورگر ذخیره شود، اما امروزه در اغلب مرورگرها نادیده گرفته شده و تمام داده‌ها و یا برخی از آنها بر اساس تنظیمات مرورگر ذخیره می‌شوند.

تنظیمات پروکسی^۲

ویژگی تنظیم پروکسی نیز یک ویژگی مهم ارائه شده توسط هر مرورگر است. این ویژگی به کاربر اجازه می‌دهد تا درخواست‌های ساخته شده توسط یک مرورگر را به پروکسی واسطه منتقل کنید.

اکثر شرکت‌ها از نوع خاصی از پروکسی‌ها برای جلوگیری از نشت اطلاعات استفاده می‌کنند و این تنظیمات را می‌توان در مرورگر انجام داد تا روند مرور را محدود و یا نظارت کند. گزینه‌های پروکسی نیز به طور گسترده‌ای توسط ارزیابان امنیتی برای ذخیره درخواست‌ها و پاسخ‌های فرستاده شده توسط مرورگر مورد استفاده قرار می‌گیرند. آنها به طور کلی از یک ابزار پروکسی استفاده کرده و تنظیمات را در مرورگر تنظیم می‌کنند.

¹ Password Autocomplete, Form Pre-filing, Form Autocomplete, Roboform, Remember password

² PROXY SETUP

در زندگی روزمره نیز می‌توان از راه اندازی پروکسی برای مرور ناشناس یا مرور یا بازدید از برخی صفحات فیلتر شده استفاده کرد. در این صورت کاربر تنها باید آدرس IP پروکسی و شماره پورت بعضی از کشورهای دیگر که در آن‌ها سایت یا محتوی در دسترس است، به دست آورده و سپس آن را در مرورگر برای تنظیم بازدید از آن صفحات استفاده کنند.

راه اندازی پروکسی در فایرفاکس

به منو زیر بروید و تنظیمات خود را اضافه کنید.

Menu → Options → Advanced → Network → Connection Settings → Manual proxy configuration

راه اندازی پروکسی در کروم

به منو زیر بروید و تنظیمات خود را اضافه کنید.

Menu → Settings → Show advanced settings → Under Network click on Change proxy settings → Click on LAN Settings → Check Use a proxy server for your LAN

مرورگرهای خام^۱

مرورگرهای خاصی به صورت پیش‌فرض با سیستم‌عامل‌های خاص مانند اینترنت اکسلپور برای ویندوز و سافاری برای مک وجود دارند. تقریباً تمام مرورگرها نسخه‌های خود را برای سیستم‌عامل‌های مختلف در دسترس دارند؛ اما مرورگرهایی که به طور گسترده‌ای مورد استفاده قرار می‌گیرند، همان چیزی است که از پیش با سیستم‌عامل نصب شده است، اما برخی از آن‌ها منبع باز و به راحتی برای سیستم‌عامل‌های مختلف در دسترس هستند مانند موزیلا فایرفاکس و گوگل کروم. اگر چه گوگل کروم عمدتاً توسط سیستم‌عامل ویندوز استفاده می‌شد، یکی از نسخه‌های منبع باز آن به طور کلی در بسیاری از سیستم‌عامل‌های لینوکس نصب شده و Chromium نامیده می‌شود. نام آن به مرورگر گوگل کروم شباهت دارد و ویژگی‌های آن‌ها نیز کمی متفاوت با یکدیگر هستند.

همان‌طور که قبل اشاره کردیم موتورهای رندر مرورگر مانند Gecko، WebKit و غیره وجود دارند و کروم از WebKit استفاده می‌کند و Chromium هم همین کار را می‌کند. این پروژه ابتدا در سال ۲۰۰۸ آغاز شد و در حال حاضر به بیش از ۳۵ نسخه به روز رسانی شده است. این مرورگری محبوب در میان جامعه منبع باز است. این مفهوم

^۱ RAW BROWSERS

در پشت پنجره گوگل کروم است که به عنوان فرایند اصلی مورد استفاده قرار می‌گیرد، زیرا پروژه Chromium برای ایجاد مرورگر سبک، سریع و کارآمد ساخته شده است که می‌تواند به عنوان پوسته وب نیز شناخته شود و تب را به عنوان فرایند اصلی می‌شناسد. مرورگرهای مختلف دیگری که بر اساس سورس کد پروژه Chromium منتشر می‌شوند وجود دارد. اپرا، Rockmelt و Comodo Dragon و بعضی از مرورگرهای مشهور دیگر بر اساس Chromium هستند.

در حال حاضر یک چیز از پاراگراف بالا روشن است که اگر مرورگر منبع باز باشد، کد نویسان از آن کد برای ایجاد مرورگرهای مختلف دیگر با اضافه کردن برخی از قابلیت‌های اضافی استفاده خواهد کرد، به عنوان مثال ایجاد مرورگرهای امنیتی و حفظ حریم خصوصی در Chromium Group برخی از ویژگی‌های امنیتی و حفظ حریم خصوصی در Comodo Group منتشر نمودند. به طور مشابه، فایرفاکس دارای نسخه‌های مختلف سفارشی است؛ بنابراین نسخه پایه را به عنوان مرورگر خام و مابقی را به عنوان مرورگرهای سفارشی شده در نظر بگیرید.

چرا نسخه‌های سفارشی مرورگرها به وجود آمدند؟

نسخه‌های سفارشی برای اهداف مختلف مورد استفاده قرار می‌گیرند تا از قدرت واقعی قابلیت‌های مرورگر خام به طور کامل استفاده کنند و بدین شکل از ویژگی‌های موجود در مرورگرهای خام بهتر استفاده شوند. مرورگرهای سفارشی می‌توانند به ما برای انجام نیازهای خاص کمک کنند. مثلاً ما مرورگری را می‌خواهیم که می‌تواند به ما در آنلاین بودن ۲۴*۷ شبکه‌های اجتماعی کمک کند. ما می‌توانیم افزونه‌های مختلف شبکه اجتماعی را در مرورگر انتخاب کنیم و یا نسخه‌ای از مرورگر را که حاوی ویژگی‌های موردنیاز است، بسازیم. به طور مشابه فرض کنید ما ارزیاب نفوذ یا تحلیلگر امنیتی هستیم، ممکن است مرورگر را برای انجام تست‌های مختلف امنیتی اجرا کنیم، بنابراین می‌توانیم یک مرورگر را سفارشی کنیم. یک کاربر عادی ممکن است نیاز داشته باشد که در هنگام مرور ناشناس باشد تا هیچ‌کس نتواند پیگیری آنچه را که در حال مرور است، انجام دهد، این کار را می‌توان با سفارشی‌سازی یک مرورگر انجام داد. در حال حاضر تعدادی از مرورگرهای سفارشی موجود در بازار برای انجام این اهداف وجود دارند و به همین ترتیب ما می‌توانیم مرورگرهای سفارشی را با توجه به میلمان ایجاد کنیم. البته که فرایند آن کمی پیچیده است و به برخی از زمینه‌های فنی نیاز دارد تا در ک کنیم.

پروژه Chromium دارای وب‌سایت رسمی، <http://www.chromium.org> است که می‌توانیم مستندات مختلف را پیدا کنیم و به سفارشی کردن مرورگر برای سیستم‌عامل‌های مختلف کمک کنیم. بخشی از Chromium در sourceforge

نگهداری می‌شود. از اینجا می‌توانید مرورگر و سورس کد مرورگر <http://www.sourceforge.net/projects/chromium> را دانلود کنید، در لیست مشترک شوید تا اخبار به روز شده در مورد پروژه را دریافت و اشکالات و درخواست‌های ویژگی را ارسال کنید. اگر علاقه‌مند هستید که Chromium را سفارشی کنید، اگر آدرس پست الکترونیک خودتان را به اشتراک بگذارید و همچنین مستندات موجود در source-forge را بررسی کنید. اولین گام برای سفارشی کردن هر مرورگر، دریافت سورس کد آن است. چگونه می‌توان سورس کد Chromium را دریافت کرد؟ این کاملاً آسان است، ما نیاز به دانلود آخرین نسخه tar یا فشرده از مرورگر داریم. بعداً با انجام untar یا unzip می‌توانیم سورس کد را همراه با جزئیات آن دریافت کنیم.

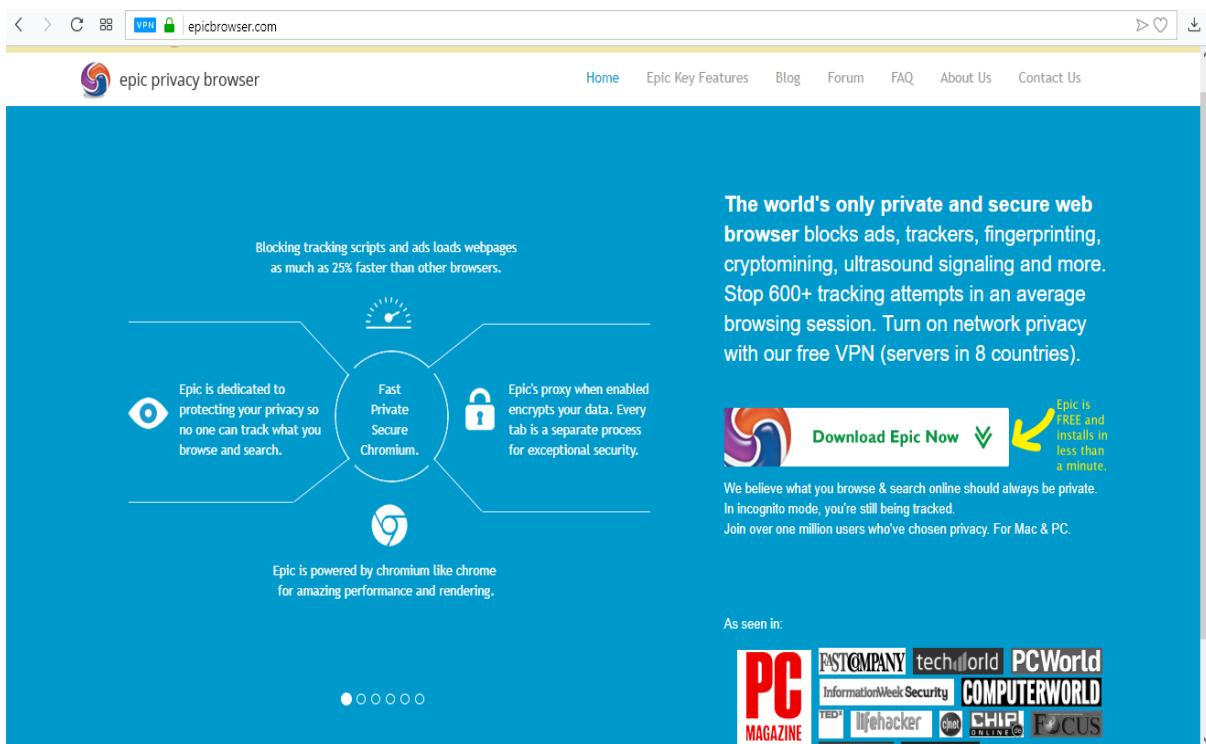
اکنون به بحث در مورد برخی از مرورگرهای سفارشی شده و ویژگی‌های آن‌ها می‌پردازیم.

برخی از مرورگرهای خوب شناخته شده EPIC¹

یک مرورگر حریم خصوصی است؛ شعار آن "ما معتقدیم که مرور و جستجو همیشه باید خصوصی باشد" Epic است. این امر به منظور گسترش حریم شخصی کاربران انجام می‌شود. این مرورگر بر اساس پروژه Chromium و توسط گروه مخفی توسعه داده شده است و برای ویندوز و OSX در دسترس است.

در بازدید از یک وبسایت رسمی، با پاراگرافی با عنوان "چرا حفظ حریم خصوصی مهم است؟" روبرو شدیم. این پاراگراف شامل برخی از دلایل منحصر به فرد و مؤثر آن است. Epic ابتدا بر اساس موزیلا فایرفاکس توسعه یافت اما بعداً به مرورگر مبتنی بر Chromium تغییر یافت. این کار بسیار شبیه به قابلیت مرور امن توسط فایرفاکس و کروم است. پس از خروج از مرورگر، داده‌های نشست مانند کوکی‌ها، حافظه‌های ذخیره شده و سایر داده‌های موقت را حذف می‌کند. سرویس‌های ارائه شده توسط کروم را برای ارسال هر نوع اطلاعات به هر سرور خاص حذف می‌کند و هیچ هدر رديابی برای جلوگیری از ردیابی توسط شرکت‌های جمع‌آوری داده‌ها اضافه نمی‌کند. همچنین اتصال SSL را در مرور استفاده می‌کند و حاوی یک پروکسی برای مخفی کردن آدرس IP کاربران است. برای جلوگیری از نشت تنظیمات جستجو، Epic تمام جزئیات جستجو را از طریق یک پروکسی هدایت می‌کند.

¹ <https://www.epicbrowser.com>



HconSTF¹

HconSTF چارچوب ارزیابی امنیتی Hcon را نشان می‌دهد. این چارچوب ارزیابی مبتنی بر مرورگر است. با افزونه‌های مختلف در مرورگر تکمیل شده است و به کاربر اجازه می‌دهد تا تست نفوذ، بهره‌برداری از آسیب پذیری‌های، تجزیه و تحلیل تروجان در وب به همراه OSINT به صورت نیمه‌رسمی را انجام دهد.

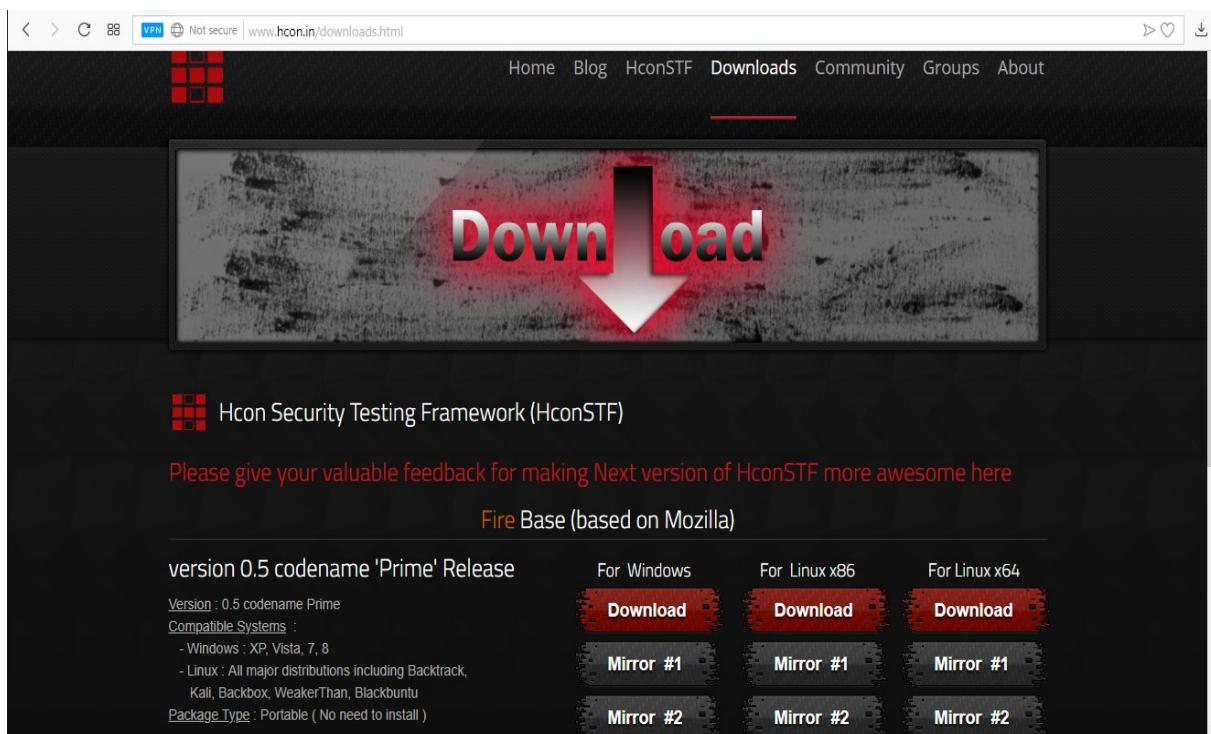
HconSTF دارای دو نوع است؛ یکی بر اساس فایرفاکس که به عنوان Base Fire شناخته می‌شود و دیگری بر اساس که به عنوان Base Aqua شناخته می‌شود. موتورهای رندر آن نیز مانند مرورگر Chromium متفاوت هستند. Base Raw از WebKit و Base Gecko از Base Fire استفاده می‌کند. هر دو نسخه با تعداد زیادی افزونه بارگذاری می‌شوند.

ایده اصلی یا الهام‌بخش این پروژه از hackerfox گرفته شده است، اما کاملاً مشابه آن نیست. Hackerfox نسخه قابل حمل فایرفاکس با تعداد زیادی افزونه‌های بارگیری شده توسط یانگون Ethical Hacker Group است. Hackerfox فقط حاوی افزونه‌ها است، در حالی که HconSTF (http://sourceforge.net/projects/hackfox/) پیشرفته‌تر است و شامل ابزارهای بهتری است. این مرورگر برای ویندوز و تمام نسخه‌های محبوب لینوکس و سیستم‌عامل‌های ۳۲ و ۶۴ بیتی در دسترس است. فرایند استفاده از آن بسیار آسان است، فقط بسته را دانلود کرده

¹ <http://www.hcon.in/downloads.html>

و آن را اجرا کنید، نیازی به نصب چیزی ندارید. اولین نسخه عمومی یا V0.3 به عنوان Hfox شناخته شد. یکی از آن‌ها به عنوان freedom شناخته و آن V0.5 Prime نامیده می‌شود.

همچنین دارای رابط کاربری بسیار کاربر پسند است و همه چیز آن کاملاً سازماندهی شده است. نویسنده آن همچنین یک کتابچه راهنمایی که حاوی تمام جزئیات در مورد پروژه از جمله تاریخ انتشار، معماری، جزئیات ابزار و تنظیمات با تصاویر است را فراهم می‌کند. HconSTF حاوی افزونه‌ها، اسکریپت‌ها و پلاگین‌های جمع‌آوری اطلاعات است. همچنین اجازه می‌دهد تا کاربر افزونه‌ها و اسکریپت‌ها را با انتخاب بروز رسانی (→ →) انجام دهد، اما اجازه نمی‌دهد که کاربر ارتقاء نسخه را انجام دهد. برای ارتقاء باید به صورت دستی سایت پروژه را دانلود کنید.



ابزار زیر را فراهم می‌کند:

- ❖ Recon/mapping
- ❖ Editors/debuggers
- ❖ Exploitation/audit
- ❖ Request manipulation
- ❖ Anonymity
- ❖ Cryptography

- ❖ Database
- ❖ Scripting/automation
- ❖ Network utilities
- ❖ Reporting

نسخه ۰.۵ Prime یا همراه با یک بسته شگفت‌انگیز برای کاربر مانند پایگاه داده یکپارچه (IDB) عرضه می‌شود. IDB برای حملات مختلف محبوب مانند SQL Injection و cross-site scripting (xss) استفاده می‌شود. به غیر از آن به کاربر لینک‌های جستجو سریع برای دریافت اطلاعات زیاد می‌دهد.

MANTRA¹

Mantra پروژه امنیت پروتکل برنامه باز (OWASP) است. این پروژه کاملاً شبیه به HconSTF است اما برخلاف HconSTF، به طور کامل به ارزیابی امنیتی وب اختصاص یافته است. به سادگی می‌توان گفت که یک چارچوب ارزیابی امنیتی وب مبتنی بر مرورگر است. نسخه اولیه از فایرفاکس استفاده کرد، اما نسخه‌های بعد از آن از Chromium بهره برداشت که به عنوان MOC در Mantra شناخته می‌شود. همانند سایر مرورگرهای چارچوب امنیتی سفارشی، نسخه‌های ۳۲ و ۶۴ بیتی معماری سیستم‌عامل ویندوز، لینوکس و مکینتاش را پشتیبانی می‌کند. Mantra دارای ویژگی‌های اضافه شده است که اکثر چارچوب‌های مبتنی بر مرورگر دیگر آن را ندارند. به عنوان مثال، آن در ۹ زبان مختلف مانند انگلیسی، پرتغالی، روسی، عربی، اسپانیایی، ترکی، فرانسوی، چینی ساده و سنتی در دسترس است. به خاطر اینکه در جامعه امنیتی بسیار محبوب است، به طور پیش فرض در سیستم‌عامل‌های امنیتی محبوب مانند Backtrack و Matriux نصب می‌شود.

افزونه‌های امنیتی از قبل در آن نصب شده و با رابط کاربری ساده و کاربر پسند آن، Mantra را جزء جدایی‌ناپذیر از زرادخانه ارزیابی هر برنامه وب کرده است. ابزارهای موجود در Mantra نه تنها بر تست برنامه‌های وب تمرکز می‌کند، بلکه بر روی سرویس‌های تحت وب و آزمایش نفوذ نرم‌افزار شبکه تمرکز می‌کنند. این ابزارها شامل ابزار برای تغییر عامل کاربر، دست‌کاری کوکی‌ها، دست‌کاری در پارامترها و ارزش‌های آن‌ها، افروختن پروکسی و بسیاری دیگر است. FireCAT نیز در Mantra گنجانده شده است و این ابزار را قوی‌تر می‌کند.

¹ <http://www.getmantra.com/>

Web app security testing with browsers

Introduction

Can you perform web application security testing just using a browser? Think of a scenario where you have to do security testing from a very limited environment where you have no access to run scripts or tools and all you have is a browser. This guide looks at web application security testing from such a locked down scenario. The goal is to cover as many security test cases as possible from a browser. Even though it's not possible to perform all web application related security test cases from browsers, some good coverage can be guaranteed with the help of the same. A browser alone cannot replace conventional web application security testing methodologies which involve proxies and scanners. Relying completely on security tests that can be done from a browser is never recommended.

One of the other potential use cases for this guide would be while preparing security testing reports. The most important section in any vulnerability finding write-up is 'reproduction steps'. Most security professionals make use of tools like Burp Suite or ZAP extensively for this step. However, the major audience (including developers) of the security testing won't be having enough knowledge about setting up the proxy and similar tools – making the vulnerability reproduction tough on their end. As a matter of fact, you might have been in post pen-testing meetings where stakeholders asked you to reduce the

برخی از ابزارهای آن به شرح زیر است:

- ❖ Information gathering
- ❖ Flagfox
- ❖ Passiverecon
- ❖ Wappalyzer
- ❖ Application audit
- ❖ Rest client
- ❖ Hackbar
- ❖ Dom inspector
- ❖ Editors
- ❖ Firebug
- ❖ Proxy
- ❖ Foxyproxy
- ❖ Network utilities
- ❖ Fireftp
- ❖ FireSSH
- ❖ Misc
- ❖ Event spy
- ❖ Session manager

به غیر از ابزارها، حاوی بوک مارک‌ها نیز می‌باشد. این بوک مارک‌ها به دو بخش تقسیم می‌شود. بخش اول به عنوان هکری شناخته می‌شوند. این مجموعه‌ای از لینک‌های ارزیابی نفوذ مختلف است که به کاربر در درک و

ارجاع یک حمله خاص کمک خواهد کرد. بخش دیگر شامل گالری است. این شامل تمام لینک‌های ابزاری است که می‌تواند برای تست نفوذ استفاده شوند.

شما می‌توانید هر دو نسخه Mantra را از آدرس <http://www.getmantra.com/download.html> یا لینک‌های دانلود زیر دانلود کنید. Mantra بر اساس فایرفاکس برای سیستم‌عامل‌های مختلف مانند ویندوز، لینوکس و مکینتاش در دسترس است در حالی که MOC تنها برای ویندوز در دسترس است.

Mantra based on Firefox can be downloaded from <http://www.getmantra.com/download.html>.

Mantra based on Chromium can be downloaded from <http://www.getmantra.com/mantra-on-chromium.html>.

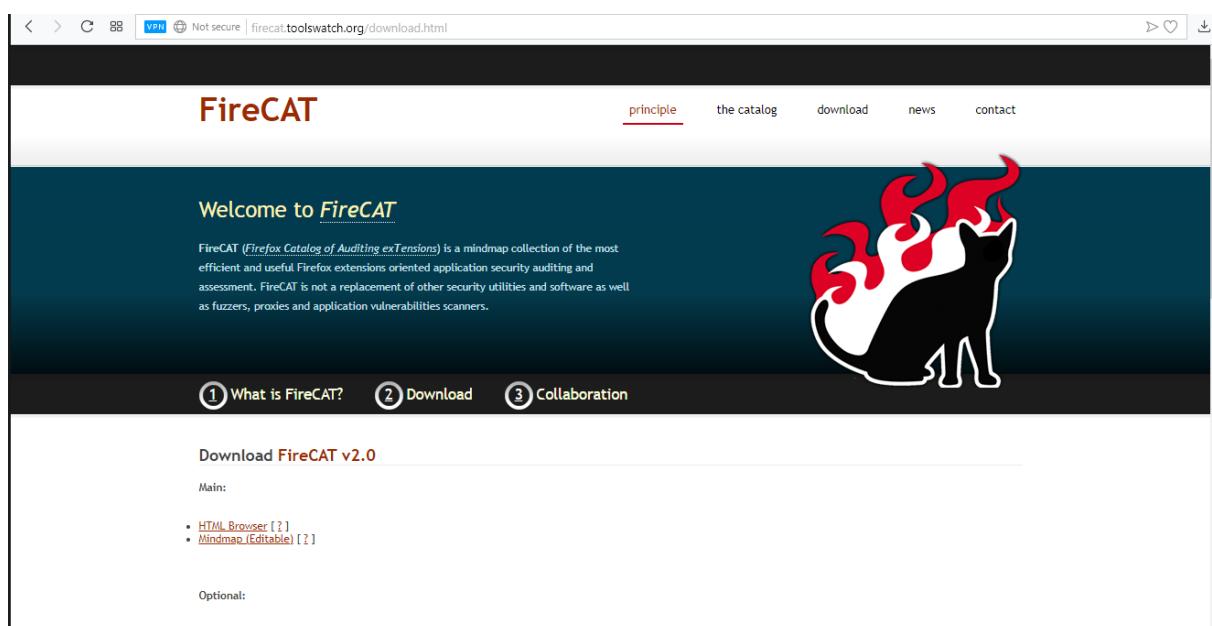
FireCAT¹

FireCAT یا فایرفاکس کاتالوگ، شامل افزونه‌های امنیتی مختلف به شیوه دسته‌بندی شده است. در حال حاضر با پروژه OWASP Mantra مشارکت کرده است. FireCAT شامل هفت دسته اصلی و بیش از ۱۵ زیر شاخه است

- Information gathering
 - Whois
 - Location info
 - Enumeration and fingerprint
 - Data mining
 - Googling and spidering
- Proxies and web utilities
- Editors
- Network utilities
 - Intrusion detection system
 - Sniffers
 - Wireless
 - Passwords
 - Protocols and applications
- Misc
 - Tweaks and hacks
 - Encryption/hashing

¹ <http://firecat.toolswatch.org/download.html>

- Antivirus and malware scanner
- Antispoof
- Antiphishing/pharming/jacking
- Automation
 - Logs and history
 - Backup/synchronization
 - Protection
- IT security related
- Application auditing



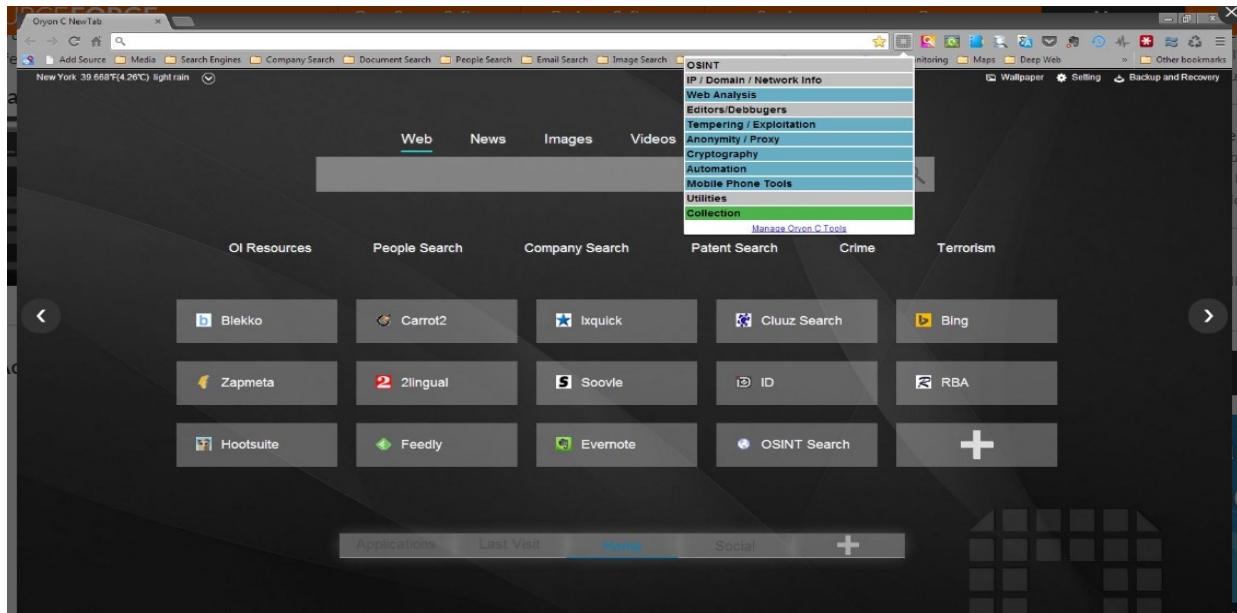
یک دسته با عنوان "IT security related" وجود دارد. این یکی از دسته‌های جالب است زیرا شما پلاگین‌هایی برای جمع‌آوری اطلاعات در مورد آسیب‌پذیری‌های رایج (CVE‌ها) و سوءاستفاده از منابع مختلف از قبیل پایگاه داده آسیب‌پذیری باز (OpenDocument Database OSDV)، طوفان پکت‌ها، SecurityFocus، Exploit-DB و غیره را دارید.

ORYON C¹

Oryon C یک چارچوب هوشمند پورتابل منع باز مبتنی بر مرورگر Chromium است که برای تحلیلگران و محققان OSINT قابل استفاده است؛ مانند دیگر مرورگرهای سفارشی، دارای ابزار و افزونه‌های پیش نصب شده برای پشتیبانی از OSINT می‌باشد. این مرورگر شامل پیوندهای آنلاین مختلف برای بررسی و تحقیق بهتر

¹ <http://sourceforge.net/projects/oryon/>

است. این پروژه توسط osintinsight انجام شده است بنابراین برخی از توابع کاربر می‌تواند تنها پس از اشتراک
برخی از بسته‌های OsintInsight استفاده شود.



یک مرورگر وب است که برای کمک به محققان در انجام تحقیقات OSINT طراحی شده است. این مرورگر با دهها ابزار پیش نصب شده و تعدادی از لینک‌های فهرست شده بر اساس طبقه‌بندی وجود دارد.

با خیال راحت از تمام گزینه‌های Oryon Browser استفاده کنید، توصیه می‌شود که مراحل زیر را انجام دهید:

۱. تنظیمات حریم خصوصی مرورگر خود را بررسی کنید. در صورت لزوم تمامی تنظیمات را بازنمانی کرده یا تغییرات لازم را انجام دهید.
۲. تاریخچه مرور را غیرفعال کنید
۳. پروکسی رایگان را فعال کنید
۴. یک حساب جیمیل اختصاصی ایجاد کنید
۵. ایجاد حساب‌های اختصاصی در فیسبوک و توییتر
۶. نگاهی به مجموعه‌ای از لینک‌ها
۷. از نوار ابزار Oryon Tools اطمینان حاصل کنید

۸. افروزدنی‌های نصب شده را بررسی کنید

۹. یک کپی از صفحه QueryTool را در GoogleDrive خود ذخیره و عملکرد آن را با موارد خود بررسی کنید

۱۰. ورود به کanal YouTube و تماشای ویدئوهای آموزشی عملی.

این یک ابزار کاربردی قابل حمل است بنابراین نیازی به نصب Oryon نیست، فقط آن را دانلود و اجرا کنید. این تنها از سیستم عامل ویندوز ۳۲ و ۶۴ بیت پشتیبانی می‌کند. فهرست عظیمی از افزونه‌های مفید و بوک مارک‌های طبقه‌بندی شده را نیز دارد.

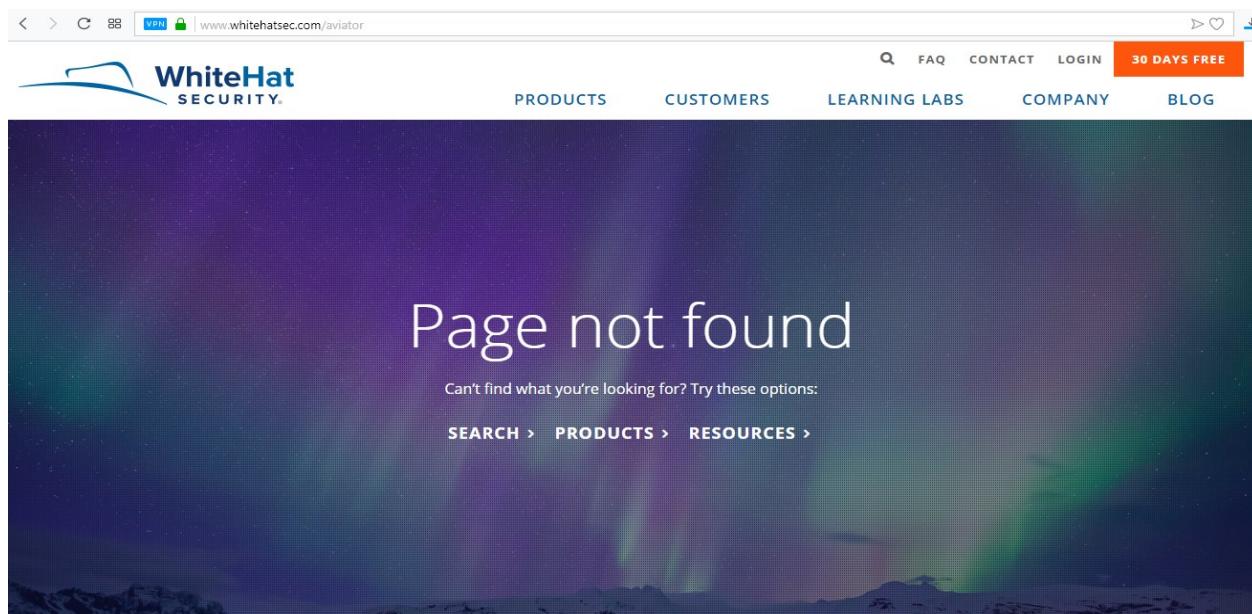
WhiteHat Aviator¹

اگر چه WhiteHat Aviator یکی از انواع مرورگر محبوب نیست، اما قطعاً محصولی از یک سازمان امنیتی معتبر با نام تجاری بزرگ است. WhiteHat Aviator یک مرورگر برای مرور خصوصی است. آن کاملاً شبیه مرورگر Epic است که پیش‌تر در این فصل مورد بحث قرار گرفت. این مرورگر تبلیغات، ردیابی آنلاین را حذف می‌کند تا اطمینان حاصل شود که کاربر در گشت‌وگذارش ناشناس است.

مانند مرورگر Epic، Aviator نیز بر اساس Chromium است. به‌طور پیش‌فرض در حالت ناشناس یا حالت مرور خصوصی اجرا می‌شود تا کاربر بتواند بدون نگهداشتن هر سابقه، کوکی و یا تنظیمات گشت‌وگذارش را انجام دهد. همچنین پخش خودکار انواع رسانه‌های مختلف را غیرفعال می‌کند، کاربر می‌بایست به یک رسانه مانند فلش در هر صفحه اجازه دهد اگر می‌خواهد آن را بینند. همچنین از موتور جستجوی خصوصی duckduckgo برای اجتناب از تنظیمات جستجوی رشته‌ای کاربر استفاده می‌کند.

برخلاف مرورگر Epic منبع باز نیست، بنابراین جامعه امنیتی باز نمی‌تواند کد را ممیزی کنند و یا به پیشرفت آن کمک کنند. این مرورگر برای ویندوز و همچنین سیستم عامل مکینتاش در دسترس است.

¹ <https://www.whitehatsec.com/aviator/>

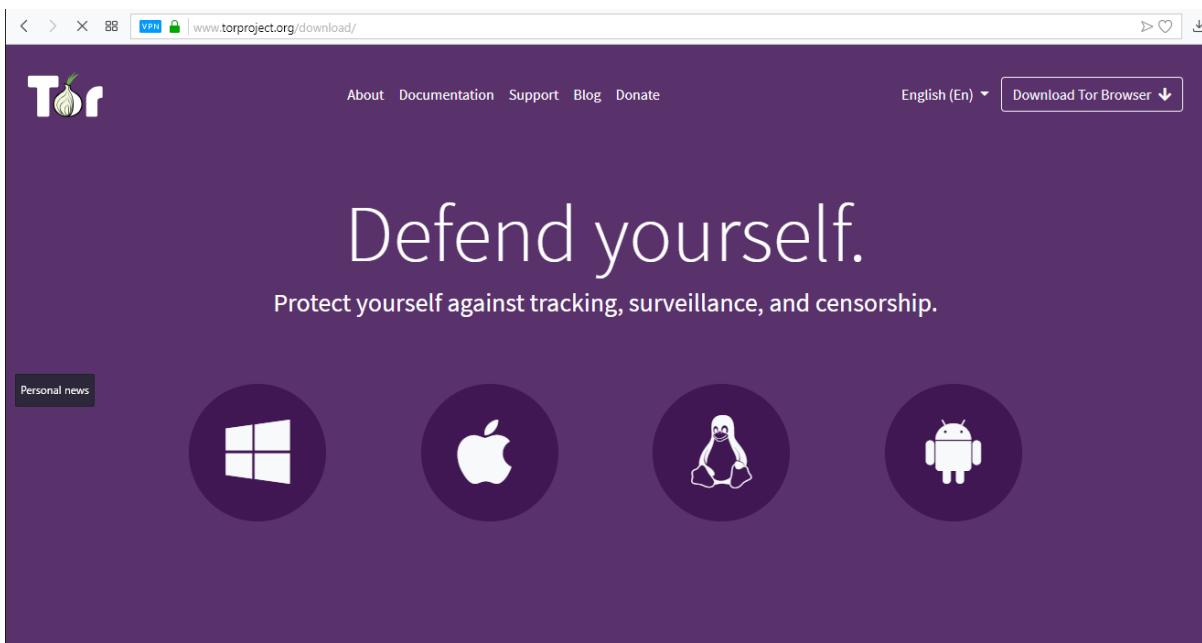


TOR BUNDLE¹

TOR پروژه بسیار محبوب است. اکثر ما قطعاً در بعضی از زمان‌ها از آن استفاده کرده و یا در مورد آن خوانده و شنیدیم. اگر چه در مورد جزئیات آن فصل بعد بحث خواهیم کرد، اما در حال حاضر در مورد اصول بسته نرم‌افزاری مرورگر tor بحث می‌کیم؛ مانند مرورگر Epic و Whitehat Aviator، مرورگر TOR نیز یک مرورگر محروم‌انه محور است؛ اما روش کار کاملاً متفاوت از آن‌ها دارد. Tor از شبکه volunteer distributed relay قبل از فرستادن یا دریافت ارتباط استفاده می‌کند. این باعث می‌شود که کاربر مکان‌یابی نشده و حریم خصوصی و ناشناسی بودن را برای کاربر ایجاد کند. با توجه به نوع مفهوم زنجیره پروکسی، می‌توان از آن برای مشاهده محتویاتی که برای یک مکان خاص مانند یک کشور مسدود شده‌اند استفاده شود. مرورگر Tor برای سیستم‌عامل‌های مختلف مانند ویندوز، لینوکس و مکینتاش در دسترس است و می‌تواند بدون نیاز به نصب استفاده شود. مرورگر Tor و یا قبلًاً به عنوان TBB شناخته می‌شد، مرورگر سفارشی بر اساس فایرفاکس است. این شامل دکمه‌های tor torcher، tor proxy و بسیاری از افزونه‌های دیگر است؛ مانند OWASP Mantra NoScript، HTTPS everywhere

۱۵ در نیز موجود است.

¹ <https://www.torproject.org/projects/torbrowser.html.en>



دسته بندی مرورگرهای سفارشی

همان‌طور که در مرورگرهای مختلف سفارشی یافتیم، پایه ساخت آن‌ها، موتور رندرینگی است که آن‌ها از آن استفاده می‌کنند. برای درک آسان، آن‌ها را به سه دسته تقسیم می‌کنیم.

۱. تست نفوذ

OSINT. ۲

۳. حریم خصوصی و ناشناس بودن^۱

در دسته اول می‌توانیم FireCAT، Mantra، HconSTF را قرار دهیم، در حالی که در رده OSINT می‌توانیم Whitehat Aviator، Epic و مرورگر Tor را در دسته حریم خصوصی و Oryon را اضافه و همچنین می‌توانیم مرورگر Whitehat Aviator، Epic و مرورگر Tor را در دسته حریم خصوصی و نامشخص بودن قرار دهیم. اگر دقیق‌تر نگاه کنیم آنچه مرورگرهای مختلف را در دسته‌های مختلف قرار می‌دهد، افزونه یا افزونه‌های است؛ بنابراین با اضافه کردن برخی از افزونه‌های کاربردی مشابه، می‌توانیم یک مرورگر سفارشی را برای یک هدف خاص ایجاد کنیم. اگر می‌خواهیم مرورگر خود را برای اهداف خاص ایجاد کنیم باید این را در نظر داشته باشیم.

^۱ Privacy and anonymity

مزایا و معایب هر یک از این مروگرها

یا باید با اولین مروگری که بحث کردیم شروع کنیم که مروگر Epic است. مزیت استفاده از این مروگر این است که به طور کامل بر حريم خصوصی و ناشناس بودن کاربر تمرکز دارد. جدا از آن، منبع باز است و می‌تواند توسط همه نوع کاربران، فنی و غیر فنی استفاده شود. تنها عیب آن پایداری است. آیا این مروگر آنچه را که قصد دارد می‌تواند انجام دهد؟ با تجربه کردن آن به این سؤال پاسخ خواهد داد.

مزیت استفاده از HconSTF این است که راه حلی یکپارچه برای محققان امنیت اطلاعات است. تنها عیب آن این است که به کاربر اجازه نمی‌دهد آن را به نسخه بعدی ارتقاء دهد.

مزیت OWASP Mantra این است که در زبان‌های مختلف برای حمایت از جامعه امنیتی از نقاط مختلف جهان در دسترس است. تنها نقطه ضعف این است که نسخه سبک یا MOC فقط برای ویندوز در دسترس است، نه برای سیستم‌عامل‌های دیگر مانند لینوکس یا مکیتاش.

مزیت Oryon C این است که در تمرینات OSINT بسیار مفید است، اما معایب مختلفی وجود دارد مانند استفاده از برخی از مأذول‌های موردنیاز کاربر برای اشتراک و همچنین فقط برای ویندوز در دسترس است. عیب Whitehat Aviator این است که منبع باز نیست و نسخه‌ای برای سیستم‌عامل لینوکس ندارد.

مزیت TBB ناشناس ماندن با استفاده از آن است و عیب آن این است که تنها با یک موتور رندر Gecko وجود دارد. همان‌طور که قبل از مورد این دسته‌بندی مروگرهای سفارشی صحبت کردیم؛ بر اساس این طبقه‌بندی، کاربر می‌تواند مروگر مورد استفاده را انتخاب کند، اما مروگرها برای ناشناس بودن و حريم خصوصی عمده‌تاً دارای دامنه وسیع‌تری هستند زیرا آن‌ها به هیچ‌یک از دسته‌های کاربر تعلق ندارند. هر کاربری که نگرانی در مورد حريم شخصی خود داشته باشد می‌تواند از این مروگرها استفاده کند؛ مانند خرید الکترونیکی، شبکه‌های خبری، شبکه‌های اجتماعی و همچنین پست الکترونیکی، این مروگر می‌تواند برای همه مفید باشد.

افزونه‌ها^۱

افزونه مرورگر، یا به عبارت دیگر پلاگین با توجه به مرورگرهای مختلف متفاوت است که در فایرفاکس آن را به عنوان addon و در کروم به عنوان extension شناخته شده است. اگرچه پلاگین جزء متفاوتی از افزودنی‌ها است، اما بعضی آن را مترادف افزونه استفاده می‌کنند. در واقع پلاگین می‌تواند بخشی از افزونه باشد.

افزونه‌های مرورگر معمولاً برای افزایش قابلیت مرورگر استفاده می‌شوند. آن‌ها چیزی جز برنامه‌های طراحی شده با استفاده از تکنولوژی وب مانند HTML، CSS و JavaScript نیستند. اگرچه به دلیل تفاوت در موتورهای رندر، ساختار و کد افزونه‌های در مرورگر مختلف، متفاوت هستند، اما امروزه ابزار و چارچوب‌های مختلفی برای طراحی افزونه متقابل مرورگرها وجود دارد.

افزونه‌ها بسیار محبوب هستند که هر کاربر وب ممکن است از آن در برخی موارد استفاده کرده باشد. برخی از افزونه‌های محبوب یوتیوب، ترجمه‌گوگل و hackbar در مورد تست نفوذ است.

ما می‌توانیم به راحتی در هر دو مرورگر، فایرفاکس و کروم به آسانی بر روی دکمه نصب کلیک کنید. افزودنی‌ها همیشه امن نیستند، بنابراین آن‌ها را عاقلانه انتخاب و از منابع قابل اعتماد و همچنین پس از بررسی دانلود کنید. گاهی اوقات باید مرورگر را برای اجرای یک افزونه خاص مجدداً راهاندازی کنیم. افزونه‌ها مانند سایر نرم‌افزارها همچنان به دنبال بهروز رسانی خود هستند و به صورت خودکار به روزرسانی می‌شوند. گاهی اوقات ممکن است بینیم که افزونه با نسخه مرورگر سازگار نیست، به این معنی است که دو گزینه وجود دارد: (۱) نسخه مرورگر قدیمی است، (۲) افزودن به روز شده برای مطابقت با نیازهای آخرین مرورگر نصب شده نیست. گاهی اوقات نیز ممکن است یک افزونه بر عملکرد مرورگر تأثیر بگذارد و حتی می‌تواند باعث کندی مرورگر شود؛ بنابراین افزودنی‌های خود را عاقلانه انتخاب کنید.

بیایید بعضی افزونه‌های معمولی که برای فایرفاکس و همچنین کروم برای استفاده روزمره استفاده می‌شود بحث کنیم. بیایید بینیم چه نوع افزونه‌هایی در دسترس هستند و برای چه هدف‌هایی استفاده می‌شوند.

همه ما از یوتیوب برای تماشای ویدئو و به اشتراک‌گذاری استفاده می‌کنیم. گاهی اوقات ما همچنین می‌خواهیم برخی از فیلم‌های یوتیوب را دانلود کنیم. تعدادی افزونه در دسترس است که نیازی به نصب نرم‌افزاری اضافی

^۱ ADDONS

دیگر نداریم. یکی دیگر از مسائل مهم در هنگام تماشای فیلم‌ها در یوتیوب، تبلیغات است. بعضی وقت‌ها مجاز دیدن فیلم‌ها بعد از ۵ ثانیه تبلیغ هستیم و بعضی اوقات ما باید ۲۰ ثانیه آگهی را تماشا کنیم. این بسیار آزاردهنده است بنابراین افرونهایی برای جلوگیری از مشاهده تبلیغات در یوتیوب وجود دارد. اکثر مردم به سایت‌های شبکه‌های اجتماعی معتقد هستند، ما معمولاً تعدادی از آن‌ها را حداقل یک‌بار در هر روز باز می‌کنیم. شبکه‌های اجتماعی مانند فیسبوک، LinkedIn، توییتر بخشی از زندگی ما هستند. گاهی اوقات ما نیاز به دیدن عکس‌های دوستان یا شخص دیگری در سایت‌های شبکه اجتماعی داریم و باید روی تصویر کلیک کرده تا آن را بزرگنمایی کنیم. این مقدار زیادی از زمان با ارزش را از بین می‌برد، بنابراین اگر ما می‌خواهیم افزونه برای بزرگنمایی تصویر داشته باشیم، از addons موجود به عنوان hoverzoom در فایرفاکس و همچنین کروم استفاده می‌کنیم.

افرونهای مختلف برای چت، اخبار، آب‌وهوا نیز موجود هستند. به نظر می‌رسد فکر کنید که افرونهایی برای تقریباً همه چیز وجود دارد، ما فقط باید کشف کنیم و قطعاً یکی از آن‌ها را پیدا خواهیم کرد که زندگی ما را ساده‌تر می‌کنند.

Shodan

این پلاگین برای کروم موجود است. کاربر فقط باید آن را نصب کند. در حالی که ما یک برنامه را مرور می‌کنیم، اطلاعات موجود در مورد سایت خاص را از پایگاه داده خود جمع‌آوری می‌کنیم و اطلاعاتی مانند آدرس IP و وب‌سایت، مالک آن IP، جایی که میزبانی شده است، همراه با پورت‌های باز و برخی از آسیب‌پذیری امنیتی محبوب مانند HeartBleed جمع‌آوری می‌شود. این برای تست گرهای نفوذ بسیار مفید است. تنها محدودیت این افزودنی این است که تنها نتایج مربوط به سایتها را نشان می‌دهد که اطلاعات آن در منابع شودان موجود است. این نتایج به‌طور کلی نتایج سایتها جدید را نشان نمی‌دهد زیرا ممکن است پایگاه داده‌های آن حاوی اطلاعاتی در مورد آن‌ها نباشد.

WAPPALYZER

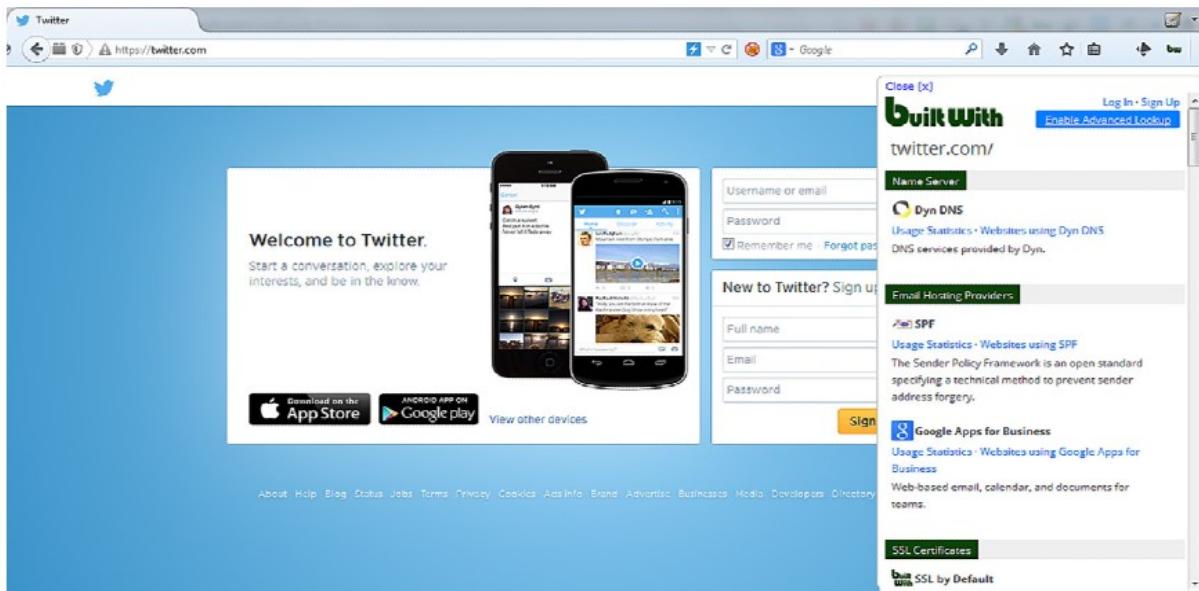
این افرونه محبوب نیز برای مرورگرهای فایرفاکس و کروم در دسترس است و تکنولوژی را که توسط برنامه وب مورد استفاده قرار می‌گیرد، کشف می‌کند. شبیه به shodan، برای wappalyzer فقط باید نصب شود. جزئیات در مورد تکنولوژی مورد استفاده در حالی که ما یک صفحه را مرور می‌کنیم، به دست می‌آورد. کاری که wappalyzer انجام می‌دهد این است که اطلاعات مربوط به تکنولوژی و نسخه‌ها از هدر پاسخ، سورس کد و

سایر منابع را جمع‌آوری می‌کند. شناسایی فن‌آوری‌های مختلف مانند CMS و یا سیستم‌های مدیریت محتوا، سیستم‌عامل‌های تجارت الکترونیک، جزئیات سرور، جزئیات سیستم عامل، جزئیات چارچوب JavaS-Cript و بسیاری از چیزهای دیگر. برخی از تکنولوژی‌های شناخته شده توسط آن عبارت‌اند از:

- ❖ Advertising networks
- ❖ Analytics platforms
- ❖ Content management system
- ❖ Databases
- ❖ E-commerce
- ❖ Issue trackers
- ❖ JavaScript frameworks
- ❖ Operating systems
- ❖ Programming languages
- ❖ Search engines
- ❖ Video players
- ❖ Wikis

BUILDWITH

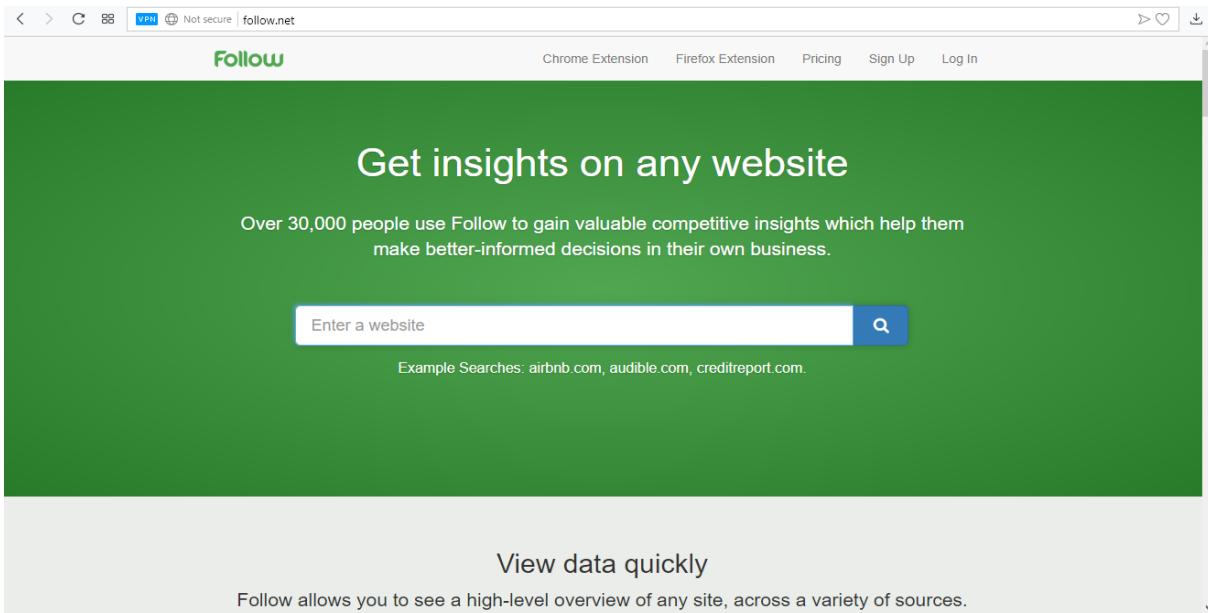
Buildwith شبیه به wappalyzer است. آن همچنین تکنولوژی‌هایی را که توسط برنامه‌های وب را استفاده می‌شود شناسایی می‌کند، با استفاده از سورس کد صفحه، بنر، نام کوکی‌ها و غیره. در حالی که wappalyzer منبع باز است، buildwith نیست. نسخه پولی buildwith دارای ویژگی‌های بیشتری از نسخه رایگان مانند تشخیص تماس با مخاطبین و تشخیص زیر دامنه و غیره است که می‌تواند بسیار مفید باشد.



FOLLOW

Follow.net ابزار هوشمندی است که به ما کمک می‌کند تا با حرکت آنلاین رقبای خود به روز شده و با استفاده از افزونه مرورگر ارائه شده توسط آن، دسترسی پیدا کنیم. مشکل عمدۀ برای ردیابی رقیب این است که ما باید زمان زیادی را صرف بازدید از وبسایت‌ها، و بلاگ‌ها، توییت‌ها، کانال یوتیوب و غیره کنیم. پس از بازدید از وبسایت‌های زیادی که داده‌های ساختاری از آن نداریم، می‌توانیم درک کنیم چه روندی دنبال شده است؛ بنابراین در اینجا follow.net است که گزارش زیادی در مورد اینکه چگونه رقیب ما در وب طی کرده است، می‌دهد. این اطلاعات را از منابع مختلف مانند آکسلا، توییتر، کلمات کلیدی جاسوسی و غیره جمع‌آوری می‌کند. همچنین اگر چیزی جدید به دست ما برسد، به ما اطلاع می‌دهد که مربوط به رقبای ما است.

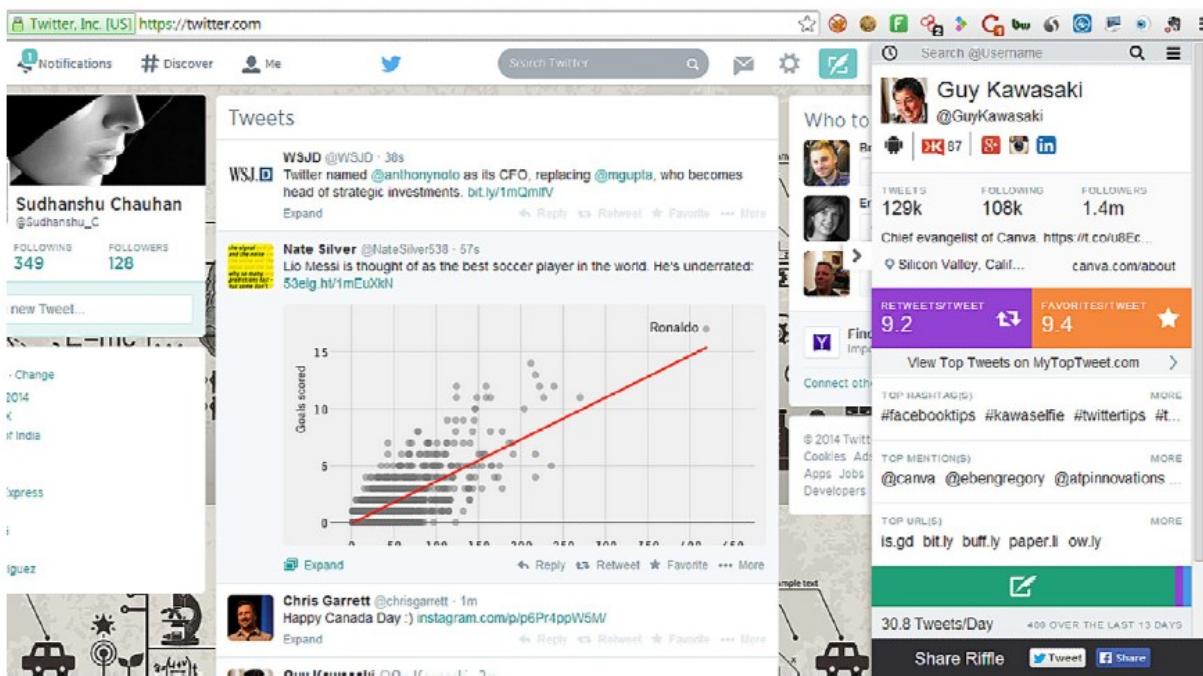
بنابراین اگر شروع به کسب و کار می‌کنیم و می‌خواهیم از رقیب یاد بگیریم، پس باید آن را داشته باشیم. افزونه Follow.net برای مرورگر فایرفاکس و کروم موجود است.



RIFFLE

شرکت CrowdRiff یک افزونه تحلیلی اجتماعی است. در سایت محبوب توییتر متمرکز است. برای ما یک داشبورد هوشمند توییتر را فراهم می‌کند که اطلاعات تحلیلی مفیدی درباره کاربران توییتر نشان می‌دهد.

این اطلاعات مفید را برای ایجاد یک حساب کاربری محبوب فراهم می‌کند با اشاره به برخی از توییت‌های محترمانه و حساب‌هایی که آنها را ارسال کرد. این نیز بینش سریع در مورد کاربر توییتر را فراهم می‌کند به‌طوری‌که به ما کمک می‌کند تا کاربر مورد نظر را در کنیم و به آن پاسخ دهیم.



WhoWorks.at

همانند Riffle در افزودن توییتر، ما باید یک افزونه خاص LinkedIn را اضافه کنیم. باید یک سناپ‌سینک کنیم که در آنجا فروشنده‌گان هستند و ما نیاز داریم اطلاعاتی در مورد کلیدی‌ترین افراد موجود در یک شرکت به دست آوریم، بنابراین چگونه می‌توانیم ادامه دهیم. ما به LinkedIn می‌رویم، برای آن شرکت خاص جستجو خواهیم کرد و سپس ارتباط درجه ۱، درجه ۲ و یا درجه ۳ را پیدا خواهیم کرد. بر اساس عنوان، ما ممکن است بخواهیم آنها را برای بحث در مورد کسب‌وکار اضافه کنیم. این راه حل قدیمی است. در حال حاضر راه دیگری برای انجام این کار در شیوه‌ای خودکارتر وجود دارد. حالا extension whoworks.at را در کروم نصب کنید، از وبسایت شرکتی که ما علاقه‌مند هستیم، بازدید کنید و اجازه دهید این افزونه به ما ارتباطات درجه ۱، درجه ۲ و ۳ را از این شرکت به همراه جزئیات مانند استخدامهای اخیر، تبلیغات و یا تغییرات عنوان

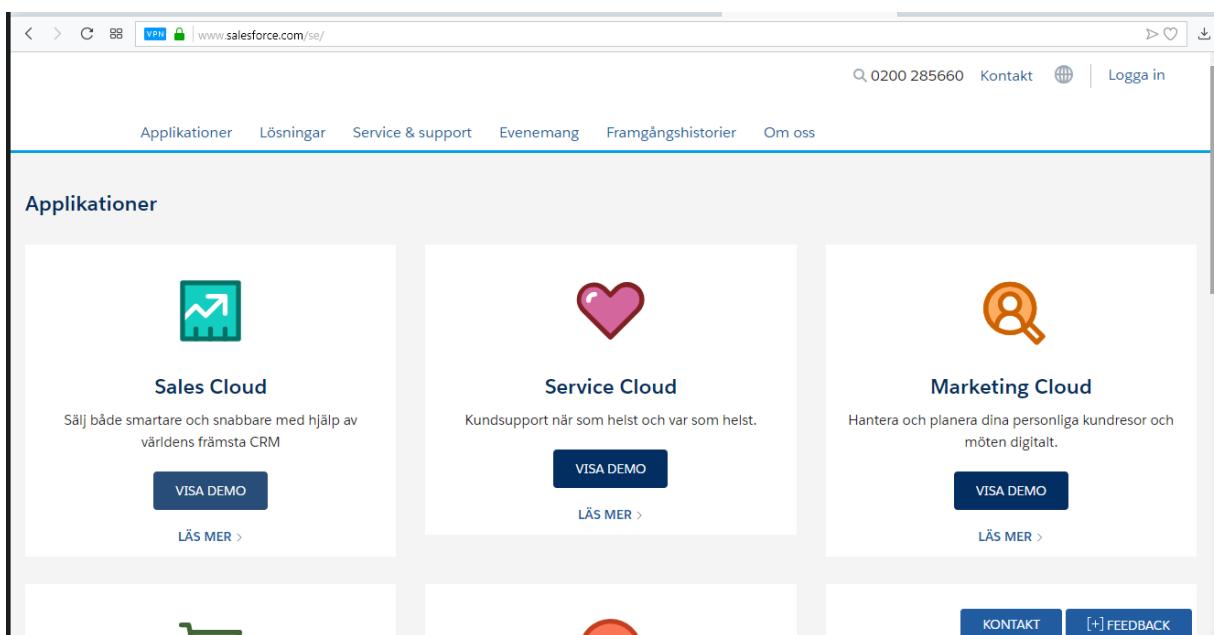
ONETAB

Onetab افزونه‌ای در مرورگرهای فایرفاکس و کروم است. این راه حل برای مدیریت زبانه‌ها است که به ما کمک می‌کند تا لیستی از زبانه‌هایی که در مرورگر باز هستند را داشته و آنها را در یک تب جداگانه بسازیم، مخصوصاً در گوگل کروم همان‌طور که قبلاً متوجه شدیم که این زبانه محور است. زبانه موضوع اصلی در کروم است،

بنابراین با استفاده از ONETAB می‌توانیم حافظه زیادی را ذخیره کنیم، زیرا تب‌ها را به یک لیست تبدیل می‌کند که بعداً می‌توان آن‌ها را به صورت یکجا در یک زمان به همان شکل که می‌خواستیم، بازگردانیم.

SALESLOFT

اکثر فروشنده‌گان باید از آن استفاده کرده باشند و یک افزودنی رؤیایی برای فروشنده‌گان است و اجازه می‌دهد تا لیستی از پرونده‌های مرور از شبکه‌های اجتماعی مختلف برای ایجاد منافع متمرکز بر یک بخش خاص از بازار ایجاد شود. همچنین اجازه می‌دهد تا یک کاربر برای انجام جستجوی خاص بر اساس عنوان، سازمان و یا نام صنعت را انجام دهد. از ویژگی‌های محبوب این است که برای جمع‌آوری اطلاعات تماس از یک چشم‌انداز LinkedIn را اجازه می‌دهد. اطلاعات تماس شامل نام، شناسه پست الکترونیکی و شماره تلفن است. این یک راه حل رایگان و سبک‌وزن برای هر شخص فروشنده است.



PROJECT NAPTHA

همه ما می‌دانیم که تقریباً غیرممکن است که متن موجود در هر تصویر را کپی کنیم، یکی از روش‌های این است که آن را به صورت دستی تایپ کنیم اما این یک تجربه عجیب و غریب است؛ بنابراین در اینجا راه حلی وجود دارد. این افزونی فوق العاده است که به ما آزادی برای کپی، برجسته‌سازی، ویرایش و همچنین ترجمه متن موجود در هر تصویر وب را با استفاده از تکنولوژی پیشرفته OCR می‌دهد. این برای کروم در دسترس است.

TINEYE

Tineye یک موتور جستجوی تصویر معکوس است، بنابراین افزودن آن نیز برای همین استفاده می‌شود. همان‌طور که ما کلمات کلیدی را در موتورهای جستجو وارد می‌کنیم تا نتایج موردنیاز را به دست آوریم، Tineye را می‌توان برای جستجوی یک تصویر خاص در پایگاه داده Tineye استفاده کرد. مقدار زیادی از تصاویر نمایه شده در پایگاه داده آن وجود دارد. روش اجرایی در پشت تکنولوژی شناسایی تصویر امضای منحصر به فرد برای هر تصویر است که در پایگاه داده وجود دارد. هنگامی که کاربر جستجوی یک تصویر را شروع می‌کند، امضای آن مقایسه و اغلب به نتیجه دقیق می‌رسد. به غیر از نتیجه دقیق نتایج مشابهی نیز ارائه می‌دهد. یکی دیگر از ویژگی‌های برجسته Tineye این است که می‌تواند تصاویر مرتب شده، تغییر اندازه داده شده و ویرایش شده را جستجو کند و نتایج تقریباً دقیق را به دست آورد. Tineye برای هر دو مرورگر فایرفاکس و کروم در دسترس است.

REVEYE

Reveye کاملاً شبیه به Tineye است. این افزونه فقط برای کروم در دسترس است. نتیجه جستجوی تصویر معکوس را بر اساس نتایج ارائه شده از جستجوی تصویر معکوس گوگل و نیز جستجوی Tineye می‌دهد.

CONTACTMONKEY

Contactmonkey یک افزونه بسیار مفید برای تمام حرفه‌ای‌ها، بهخصوص فروش است. به ما کمک می‌کند تا ایمیل‌ها را پیگیری کنیم. با استفاده از این افزونه ساده می‌توانیم شرایط ایمیل فرستاده شده مانند اینکه آن را باز کرده یا نه و در چه زمانی را رصد کنیم. این به ما کمک می‌کند تا بهترین زمان برای تماس با یک فرد را محاسبه کنیم. اگر چه نسخه رایگان دارای برخی محدودیت‌ها است اما هنوز بسیار مفید است.

اگر می‌خواهید تجربه کاربر خود را از مرورگر گوگل کروم بهبود ببخشید، به فهرست زیر نگاه شود. این لیست شامل برخی برنامه‌های افزودنی و برنامه‌های کروم است که ویژگی‌های آن را افزایش می‌دهد.

<http://digitalinspiration.com>

BOOKMARK

Bookmark یک ویژگی مشترک در هر مرورگر است. این به ما اجازه می‌دهد تا یک URL وب‌سایت را با یک نام برای استفاده بعدی ذخیره کنیم. اغلب اوقات ما صفحات جالب مختلفی را می‌یابیم، اما به دلیل کمبود زمان

نمی‌توانیم تمام آن صفحات را در آن زمان ببینیم. بوک مارک‌ها به ما کمک می‌کند که این لینک‌ها را برای استفاده در آینده ذخیره کند.

دو راه برای ذخیره بوک مارک‌ها وجود دارد:

۱. با کلیک کردن بر روی دکمه‌ی نشانک زمانی که ما در صفحه هستیم که نیاز به نشانه است.
۲. با کلیک کردن بر روی $ctrl + d$ وقتی که ما در صفحه‌ای هستیم که نیاز به نشانه‌گذاری دارد.

ما حتی می‌توانیم بوکمارک‌ها را از یک مرورگر به دیگری وارد کنیم و همچنین آن‌ها را صادر کنیم. همچنین می‌توانیم یک پوشه جدید برای لیست بوک مارک‌ها ایجاد کنیم. در فایرفاکس ما باید برای نشان دادن آن‌ها بر روی بوکمارک کلیک کرده و یا $ctrl + shift + B$ را فشار دهیم که تمام این گزینه‌ها را مستقیماً یا با کلیک راست بر روی آن صفحه دریافت می‌کنیم. به طور مشابه برای کروم ما باید به مدیر بوکمارک برویم. همچنین تمام گزینه‌های موجود در صفحه را پیدا خواهیم کرد و یا در غیر این صورت باید روی آن صفحه کلیک راست کنید تا این گزینه‌ها را دریافت کنید.

خطرات ناشی از مرورگرها

همان‌طور که در مورد مرورگرها صحبت کردیم، آن‌ها ابزار عالی هستند که به ما اجازه می‌دهند به وب دسترسی داشته باشیم و در دسترس بودن افزونه‌های مختلف به سادگی قابلیت‌های آن‌ها را افزایش می‌دهند. این استفاده گسترده از مرورگرها تهدید بزرگی نیز دارد. مرورگرها که یکی از رایج‌ترین نرم‌افزارهای کاربردی هستند، ابزاری مورد علاقه برای حمله بسیاری از مهاجمان اینترنتی هستند. مهاجمان سعی می‌کنند از آسیب‌پذیری‌های سمت cross-site گیرنده تنها با استفاده از مرورگرها، فیشنینگ، سرقت کوکی‌ها، بودن نشست‌ها، اسکریپت‌های و بسیاری دیگر استفاده کنند. به طور مشابه مرورگرها یکی از بزرگ‌ترین عامل‌هایی هستند که در نشت هویت نقش دارند؛ بنابراین، عاقلانه از مرورگر خود استفاده کنید. در فصل‌های بعد درباره برخی از روش‌های آنلاین این و ناشناس ماندن خواهیم گفت.

فصل ۴: جستجو در وب

مقدمه

در فصل دوم یاد گرفتیم که چگونه از جستجوی پیشرفته برخی از شبکه اجتماعی برای به دست آوردن نتایج دقیق استفاده کنیم، در فصل سوم به بررسی نحوه استفاده بهتر از مروگرهای رایج را یاد گرفته و این فصل درباره موتورهای جستجو بحث خواهیم کرد.

ما همه با موتورهای جستجو آشنا هستیم و در جستجوهای روزمره از آن‌ها استفاده می‌کنیم. همان‌طور که در فصل‌های قبلی مورد بحث قرار گرفت، آنچه اساساً موتورهای جستجو در وب انجام می‌دهند، از طریق خزیدن کرال‌ها انجام شده و صفحات وب را بر اساس طیف وسیعی از پارامترها مانند کلمات کلیدی، لینک‌ها و غیره پایش کرده و بر اساس کلمات کلیدی نمایه‌سازی نتایج انجام می‌شود. برخی از محبوب‌ترین موتورهای جستجو گوگل، یاهو و بینگ هستند.

موتورهای جستجو متفاوت از روش‌های مختلفی برای ارزیابی پیوندها استفاده می‌کنند و بر اساس الگوریتم آن‌ها، وب‌سایت‌ها و رتبه‌های مختلف را تعیین می‌کنند. هنگامی که برای یک اصطلاح جستجو می‌کنیم، موتورهای جستجو نتیجه‌های این صفات را ارائه می‌دهند. این رتبه‌ها بر مبنای عوامل مختلف در حال تغییر است و به همین دلیل ممکن است نتایج مشابهی را برای یک پرس‌وجو در تاریخ‌های مختلف دریافت کنیم.

بنابراین اکنون به عنوان یک کاربر معمولی با موتورهای جستجو و استفاده از آن‌ها آشنا هستیم. همان‌طور که پیش‌تر گفته شد، این فصل درباره موتورهای جستجو است؛ اما شامل موارد معمولی که ما هر روز استفاده می‌کنیم نیست. موتورهای جستجویی که در این فصل مورد استفاده قرار می‌گیرند، تخصصی هستند، برخی از این‌ها عملیات جستجوی خود را با شیوه‌ای متفاوت انجام داده و برخی از آن‌ها امکانات جستجو برای دامنه‌های خاص را فراهم می‌کنند؛ اما آیا واقعاً به موتورهای دیگری غیر از موتورهای جستجو مانند گوگل که بسیار پیشرفته و با ویژگی‌های جدید به روز رسانی می‌شوند، نیاز داریم؟ پاسخ بله است. اگر چه موتورهای جستجو مانند گوگل در آنچه انجام می‌دهند بسیار خوب هستند، آن‌ها نتایج عمومی را در قالب لینک‌های وب‌سایت ارائه می‌دهند که بر اساس کلمات کلیدی پرس‌وجو است، اما گاهی اوقات ما نیاز به پاسخ‌های خاص مربوط به دامنه خاص داریم، این زمانی است که ما به نوع خاصی از موتورهای جستجو نیاز داریم.

۱ متا جستجو

هنگامی که یک درخواست را به موتور جستجو ارسال می‌کنیم، در پایگاه داده خود برای نتایج مربوطه جستجو کرده و آن‌ها را ارائه می‌دهد، اما اگر بخواهیم نتایج حاصل از موتورهای جستجو چندگانه را دریافت کنیم، جایی است که موتور متا جستجو بکار می‌رود. موتورهای متا جستجو پرس‌وجو کاربر را به چندین منبع داده، مانند موتورهای جستجو، پایگاه‌های داده و غیره ارسال کرده و نتایج را در یک رابط واحد جمع می‌کنند. این باعث می‌شود که نتایج جستجو جامع‌تر و مرتبط‌تر بوده و همچنین در زمان جستجو چندین منبع صرفه‌جویی می‌کنند. موتورهای متا جستجو پایگاه داده‌ای از خودشان ایجاد نمی‌کنند، بلکه به پایگاه‌های مختلف دیگر برای جمع‌آوری نتایج متکی هستند.

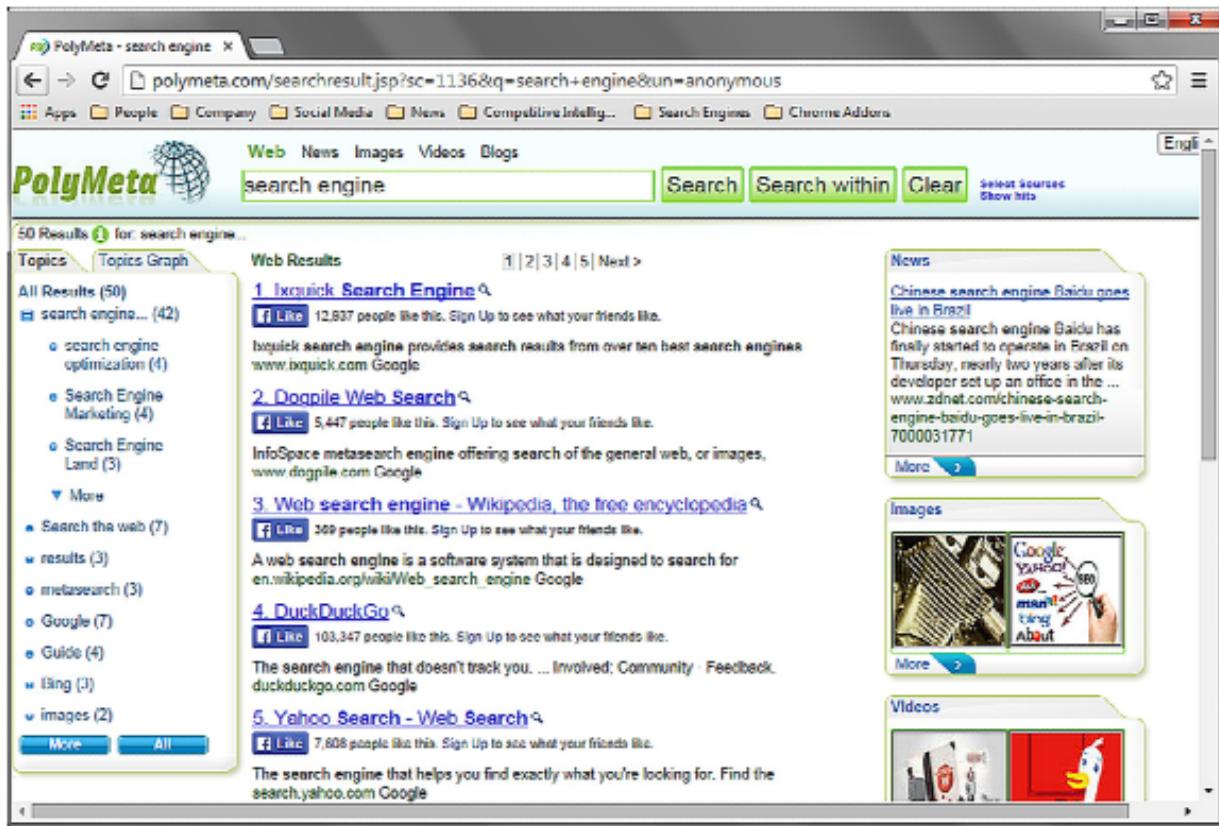
2 Polymeta²

متوار جستجوی پرکاربردی است که پرس‌وجو جستجو را به طیف وسیعی از منابع ارسال و سپس نتیجه هر یک از آن‌ها را به دست می‌آورد و بیشتر آن‌ها را رتبه‌بندی می‌کند. نتایج جستجو Polymeta نه تنها URL‌ها را شامل می‌شود، بلکه همچنین قابلیت جستجو در شبکه‌های اجتماعی را دارد. ما می‌توانیم در نتایج به دست آمده از

¹ META SEARCH

² <http://www.polymeta.com>

طریق جستجو با ویژگی‌های بیشتر تمرکز کنیم که به ما اجازه می‌دهد تا کلمات کلیدی را در داخل نتایج قبلی بکار ببریم.

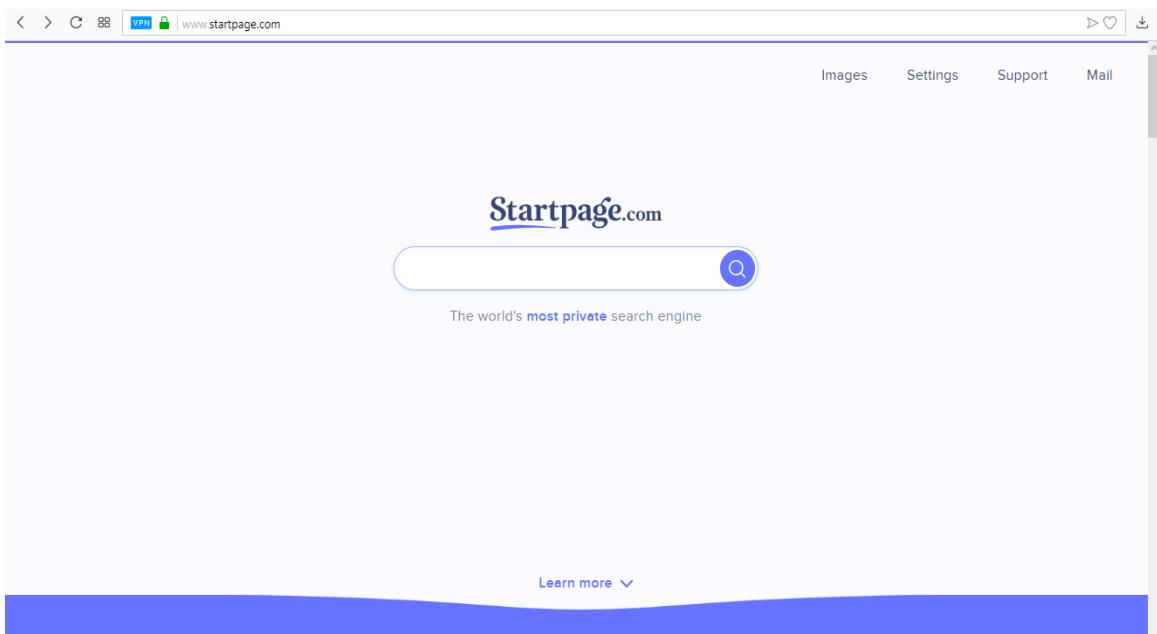


نتایج را به موضوعاتی تقسیم می‌کند که در داخل یک پنل در سمت چپ نمایش داده می‌شوند. نتایج اخبار، تصاویر، فیلم‌ها، و بلاگ‌ها در پانل‌های جداگانه در سمت راست نمایش داده می‌شوند. همچنین به ما اجازه می‌دهد که منابع را از یک لیست برای دسته‌های مختلف انتخاب کنیم.

Ixquick¹

Ixquick یکی دیگر از موتورهای متا جستجو است و به عبارت خود "خصوصی‌ترین موتور جستجو در جهان است". به غیر از توانایی عالی آن برای جستجو و ارائه نتایج از منابع مختلف، همچنین قابلیت استفاده از پروکسی برای دسترسی به نتایج را فراهم می‌کند. در نتایج جستجو خود، در زیر هر نتیجه یک گزینه به نام "proxy" وجود دارد، بنابراین ما را به URL نتیجه از طریق پروکسی (<https://ixquick-proxy.com>) می‌برد که به ما اجازه می‌دهد به عنوان یک کاربر ناشناس باشیم.

¹ <https://www.ixquick.com>



Ixquick علاوه بر وب معمولی، تصاویر و جستجوی ویدئویی، قابلیت جستجوی منحصر به فردی نظری جستجو در تلفن را فراهم می‌کند. ما نه تنها می‌توانیم شماره تلفن افراد را جستجو کنیم بلکه می‌توانیم جستجوی معکوس تلفن را انجام دهیم. به این معنی که ما باید شماره تلفن و کد کشور را انتخاب کنیم و اطلاعات مالک را برداریم. این قابلیت به ما اجازه می‌دهد تا شماره تلفن‌های کسب و کار را جستجو کنیم، ما فقط باید نام کسب و کار و جزئیات مکان را ارائه دهیم. Ixquick همچنین جستجوی پیشرفته را فراهم می‌کند که توسط URL زیر قابل دسترسی است.

<https://www.ixquick.com/eng/advanced-search.html>

 A screenshot of the 'Advanced Search' page on Startpage.com. The page has a header 'Advanced Search' with 'Home' and 'Settings' links. It features two main sections: 'Words' and 'Domain'. The 'Words' section contains seven input fields with dropdown menus for operators: 'All of these words', 'This exact phrase', 'At least one of these words', 'Without these words', 'Title contains', and 'URL contains'. Below these is a 'Domain' section with a single input field and a 'Search' button at the bottom right.

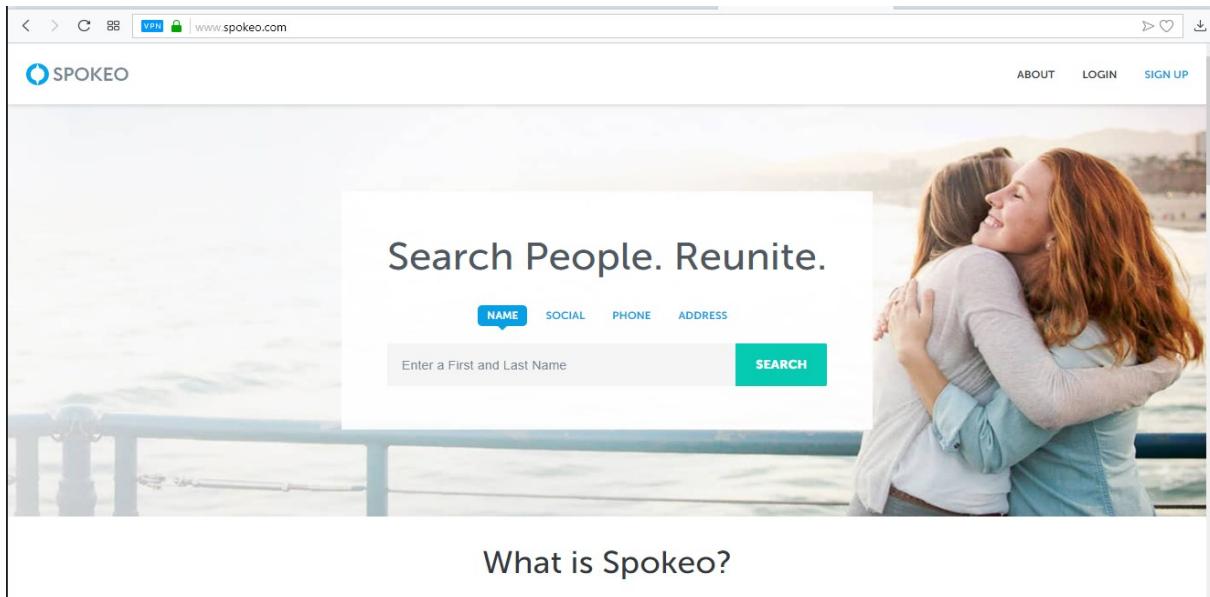
جستجوی افراد

در حال حاضر در ک درستی از نحوه کار متأ جستجو داریم، باید به یادگیری نحوه جستجو کردن افراد در اینترنت پردازیم. بسیاری از سیستم‌های رسانه‌ای محبوب مانند LinkedIn (linkedin.com)، Facebook (facebook.com) و غیره وجود دارد که می‌توانیم در آن‌ها اطلاعاتی در مورد افراد زیادی پیدا کنیم. در اینجا ما درباره موتورهای جستجو که نتایج این چنینی نشان می‌دهند، بحث خواهیم کرد. در این بخش یاد خواهیم گرفت که چگونه افراد آنلاین را جستجو و اطلاعات مرتبط را پیدا کنیم. اطلاعاتی که از این نوع تعاملات انتظار داریم عبارت‌اند از نام کامل، آدرس پست الکترونیکی، شماره تلفن، آدرس و غیره. این اطلاعات را می‌توان برای استخراج اطلاعات بیشتر مورد استفاده قرار داد. این نوع اطلاعات بسیار مناسب است زمانی که ما نیاز به اطلاعات در مورد فرد برای انجام حمله مهندسی اجتماعی و یا نیاز به درک از مشتری بالقوه داریم.

^۱Spokeo

جستجوی افراد به ویژه در ایالات متحده را انجام می‌دهد. اگر چه بیشتر اطلاعات ارائه شده توسط آن در حال حاضر کمتر از نسخه‌های قبلی است، اما از گذشته، یک پلت فرم عالی است که اطلاعات متنوعی را در ارتباط با فرد از اطلاعات اساسی مانند نام، ایمیل، به اطلاعاتی مانند محله، درآمد، پرونده‌های اجتماعی و خیلی بیشتر جمع آوری می‌کند. این اجازه می‌دهد تا افراد را با نام، ایمیل، تلفن، نام کاربری و حتی آدرس جستجو کنند. قیمت اطلاعات ارائه شده توسط آن به نظر منطقی می‌رسد و برای هر کسی که اطلاعات مربوط به افراد را می‌خواهد، توصیه می‌شود.

^۱ <http://www.spokeo.com>



What is Spokeo?

Pipl¹

Pipl یک مکان عالی برای شروع جستجوی افراد است که اجازه می‌دهد تا به جستجو با استفاده از نام، ایمیل، شماره تلفن و حتی نام کاربری پردازیم. نتایج جستجو را می‌توان با مشخص کردن مکان بهبود بخشید. برخلاف بسیاری از موتورهای جستجو که تنها از طریق وب سطح ردیابی می‌شوند، Pipl جستجوی وب عمیق را برای استخراج اطلاعات انجام می‌دهد (مفهوم وب عمیق به طور دقیق در فصل بعد بحث خواهد شد). این توانایی منحصر به فرد اجازه می‌دهد تا نتایجی را ارائه بدهد که موتورهای جستجو دیگر قادر به ارائه آن نخواهد بود. نتایج ارائه شده بسیار جامع هستند و همچنین به بخش‌هایی از قبیل Records Public، Pro files، Background و غیره طبقه‌بندی می‌شوند. در کل، این یکی از چندین مکانی است که افراد زیادی را بدون تلاش زیادی جستجو می‌کند و از این رو باید مورد استفاده قرار گیرد.

¹ <https://pipl.com/>

PeekYou¹

موتور جستجوی دیگری است که نه تنها اجازه می‌دهد تا با استفاده از انواع کلمات کلیدی معمول مانند نام، ایمیل، نام کاربری، تلفن و غیره به جستجو پردازد، بلکه با استفاده از شرایط مانند شهر، کار و مدرسه جستجو کنید. این نوع منحصر به فرد هنگامی که ما برای فارغ‌التحصیلان یا همکاران یا حتی افرادی در گذشته در شهر ما زندگی می‌کردند، بسیار مفید است. منابع اطلاعاتی که از آن استفاده می‌کنند بسیار وسیع هستند و بهترین بخش این است که همه چیز آزاد است.

¹ <http://www.peekyou.com/>

Free People Search Made Easy

Find friends, relatives and colleagues across the Web.

Name Username Phone

First Name Last Name Location

Yasni¹

ابزاری برای یافتن افراد با مجموعه‌ای از مهارت‌های خاص است. این ابزار نه تنها به ما اجازه می‌دهد تا افراد را با نام جستجو کنیم، بلکه حوزه‌های تخصصشان و یا حرفه‌شان را جستجو می‌کند. طیف گسترده نتایج ارائه شده توسط Yasni باعث می‌شود فردی که علاقه‌مند است پیدا شود. برخی از این دسته‌بندی‌ها عبارت‌اند از: تصاویر، تلفن و آدرس، پرونده‌های تجاری، اسناد و موارد دیگر.

I am looking for people that match...

Marketing, Distribution, Legal advice

Search

I offer... I can... I am...

Finance services, Consulting, Craftsman

Offer

What does the net know about...

First Name, Last Name, Nickname

Find out

Most clicked terms:

- Bank of America
- Booker Prize
- Europe
- JPMorgan
- Kobo
- Lenovo
- NSA
- World Series

Successful providers:

- Andrew Mathias @ Kilimanjaro Tanzanite ... Arusha
- "Kilimanjaro climb, Tanzania safaris - Budget travel deals online booking"

Show my Exposé here!

Important people / Exposé

Most clicked names:

- Chin Tang
- Hannah Cunningham
- Harry Louis
- Heather Donald
- Ilya Zverev
- Kris Evans
- Kylie Freeman
- Marat Kogut
- Natalie Wang
- Sumire Aida

Important people: Today - Overview / Names: Today - Overview / People searches: Today - Overview
People by keywords: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Legal Terms Privacy © 2019 yasni

naïin PLATINUM MEMBER

¹ <http://www.yasni.com>

LittleSis¹

یک ابزار جستجو برای عموم مردم نیست، بلکه بیشتر به افراد رده بالای سیاسی و تجاری متوجه است، بنابراین جستجو برای افراد معمولی در اینجا، اتفاق وقت است. اگر چه می‌تواند اطلاعات جالب و مفید در مورد سرمایه‌داران تجاری و قدرتمندان سیاسی را نشان دهد. به غیر از اطلاعات اساسی مانند معرفی، وزارت دفاع، جنسیت، خانواده، دوستان، آموزش و پرورش وغیره، همچنین اطلاعاتی مانند روابط‌شان را نشان می‌دهد که فهرستی از موقعیت‌ها و عضویت‌هایی را که فرد در آن داشته و یا دارد وغیره را نشان می‌دهد. این مکان خوبی برای تحقیق درباره افراد با قدرت و کسانی است که با آن‌ها مرتبط هستند.

MarketVisual²

موتور جستجوی تخصصی است که به ما اجازه می‌دهد تا حرفه‌ای را جستجو کنیم. ما می‌توانیم برای حرفه‌ها با نام، عنوان یا نام شرکت جستجو کنیم. هنگامی که جستجو کامل می‌شود، لیستی از اشخاص با اطلاعات مرتبط مانند تعداد روابط، عنوان و شرکت را نشان می‌دهد. بهترین بخش در مورد MarketVisual نمودارهایی است که از روابط ایجاد می‌کند. برای تجزیه و تحلیل، این داده‌ها را می‌توان به شکل‌های مختلف دانلود کرد. این یک ابزار عالی برای جستجو در بازار است.

¹ <http://littlesis.org>

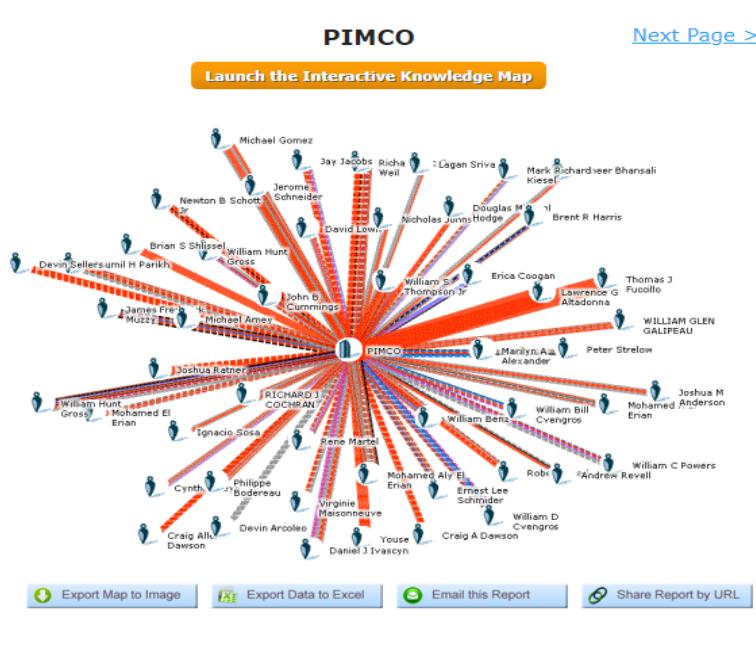
² <http://www.marketvisual.com/>

Search Professionals by Name, Company or Title:

Sample Searches:

- [Lawrence Ellison Oracle](#)
- [Microsoft Sales](#)
- [Adobe Founder](#)
- [William Gross Pimco](#)
- [Google Vice President Finance](#)
- [International Business Machines Director](#)

©2019 — IntellectSpace Corporation. All Rights Reserved.



TheyRule¹

همانند MarketVisual نیز ابزاری برای جستجوی حرفه‌ای در شرکت‌های بزرگ جهانی فراهم می‌کند. ابتدا به رابط آن نگاه می‌کنیم، این باعث می‌شود که شکنیم اطلاعاتی وجود داشته باشد، چرا که یک لیست کوچک از لینک‌ها در گوشہ بالا سمت چپ وجود دارد که در اندازه کوچک وجود دارند؛ اما هنگامی که ما شروع به بررسی این پیوندها می‌کنیم، می‌توانیم یک اقیانوس از اطلاعات جالب را پیدا کنیم. با کلیک بر روی لینک شرکت لیست گسترده‌ای از شرکت‌ها را فراهم می‌کند، هنگامی که بر روی یک شرکت کلیک می‌کنیم

¹ <http://theyrule.net>

شكل بصری آن را نمایش می‌دهد. حرکت روی این آیکون گزینه‌ای برای نشان دادن مدیران و جستجوی بیشتر را فراهم می‌کند. مدیران، بیشتر از طریق شکل نشان داده شده‌اند. اگر مدیر در بیش از یک هیئت‌مدیره باشد، پس از زدن روی آیکون آن، گزینه‌ای برای نشان دادن آن نیز فراهم می‌کند. همچنین گزینه‌ای برای پیدا کردن ارتباط بین دو شرکت فراهم می‌کند. به غیر از این نیز لیست‌های جالبی را که توسط دیگران از جمله بانک‌های Too Big To Fail Banks ایجادشده است، نیز به ما می‌دهد.

جستجوی شرکت و یا کسب و کار

امروز تقریباً هر شرکت دارای حضور آنلاین در قالب وب‌سایت، یک یا چند رسانه‌های اجتماعی و غیره می‌باشد. این رسانه‌ها اطلاعات زیادی در مورد سازمان دارند، اما گاهی اوقات ما نیاز به اطلاعات بیشتری داریم، مانند تحقیق در مورد رقبای تجارت، مشتریان بالقوه، شریکان بالقوه و غیره که می‌توانند به ما کمک کنند تا آن‌ها را بهتر در کنیم. باید برخی از آن‌ها را یاد بگیریم.

LinkedIn¹

LinkedIn یکی از محبوب‌ترین وب‌سایت‌های شبکه اجتماعی حرفه‌ای است. ما در مورد جستجوی LinkedIn در فصل قبلی بحث کردایم، اما جستجو در مورد شرکت‌ها توسط آن را نمی‌توانیم نادیده بگیریم. اکثر شرکت‌های سازنده تکنولوژی دارای پروفایل‌های LinkedIn هستند. این پروفایل برخی از اطلاعات جالب را که معمولاً در وب‌سایت‌های شرکتی پیدا نمی‌شود، مانند اندازه شرکت، نوع آن‌ها و غیره را فهرست می‌کند. همچنین تعداد کارکنان شرکت را مشخص می‌کند. ما می‌توانیم بسته به آنچه دنبال آن هستیم، به سادگی لیستی از این کارکنان را بینیم و پروفایل‌های آن‌ها را بررسی کنیم. به غیر از این می‌توانیم به طور منظم به روزرسانی‌های شرکت را در صفحه نمایه خود بینیم و درک کنیم که چه اتفاقی در آن می‌افتد. همچنین به ما اجازه می‌دهد که شرکت‌ها را با استفاده از یک حساب ثبت‌شده دنبال کنیم تا بتوانیم به طور منظم از آن‌ها اطلاعات دریافت کنیم.

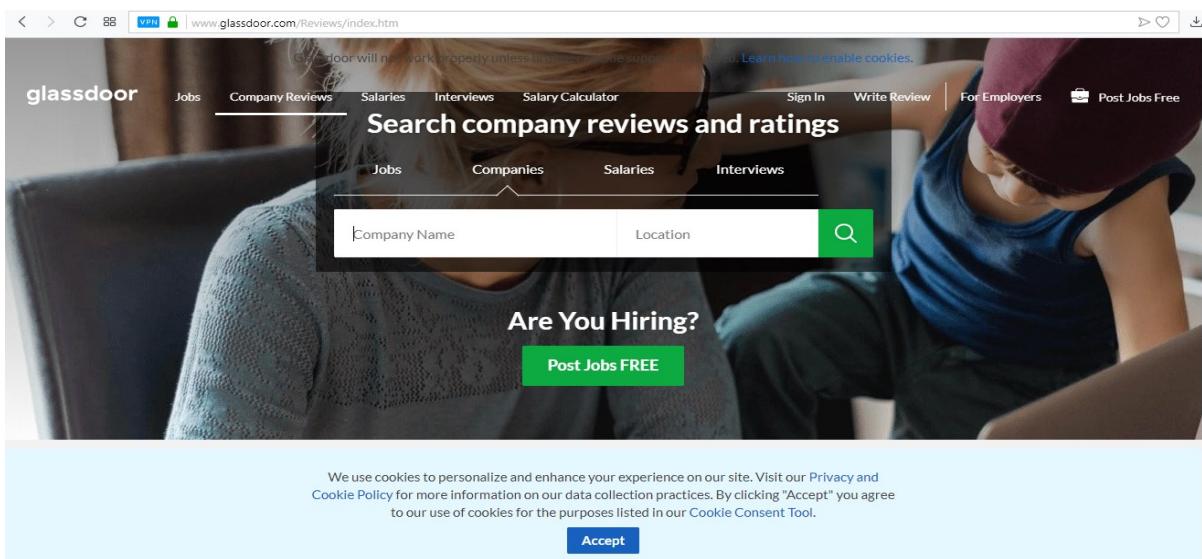
Glassdoor²

Glassdoor یک پلت فرم عالی برای شغل افراد است، همچنین اطلاعات زیادی در مورد شرکت‌ها فراهم می‌کند. به غیر از اطلاعات معمول مانند محل شرکت، درآمد، رقبا و غیره، ما همچنین می‌توانیم اطلاعاتی نظری جستجوی

¹ <https://www.linkedin.com/vsearch/c>

² <http://www.glassdoor.com/Reviews/index.htm>

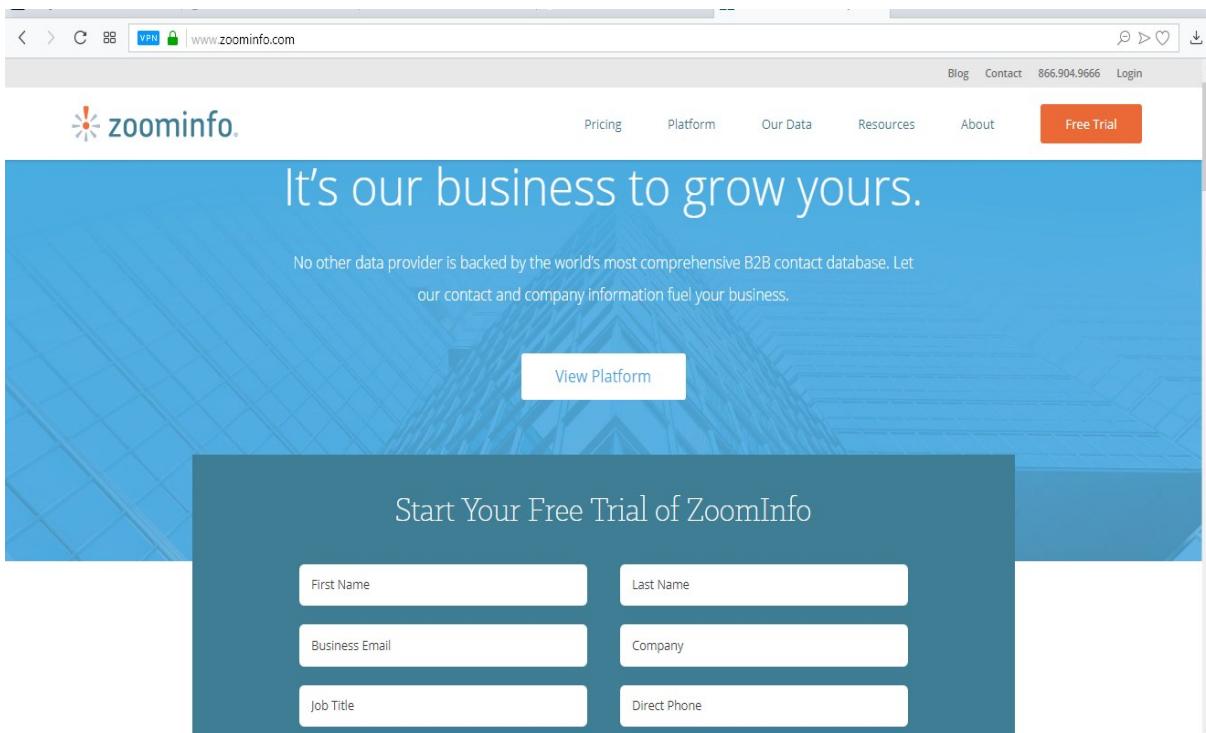
کارکنان، حقوق و دستمزد، فرصت‌های جاری و تجارب آن را پیدا کنیم. بهترین بخش این است که اطلاعات نه تنها توسط سازمان، بلکه کارمندان آن ارائه می‌شود، از این رو، دیدگاه بسیار دقیق از ساختار داخلی و کار را فراهم می‌کند. به مانند Glassdoor، LinkedIn گرینه‌ای برای پیگیری به روز رسانی شرکت فراهم می‌کند.



Zoominfo¹

Zoominfo پلت فرم تجاری کسب‌وکار است که عمدهاً توسط نماینده‌گان فروش و بازاریابی برای پیدا کردن جزئیات شرکت‌ها و همچنین افرادی که در آن‌ها کار می‌کنند، مانند ایمیل، شماره تلفن، آدرس، روابط و غیره استفاده می‌شود. هر چند حساب رایگان آن محدودیت‌های مختلفی دارد، اما ابزار بسیار خوبی برای پیدا کردن اطلاعات در مورد سازمان‌ها و کارمندانشان است.

¹ <http://www.zoominfo.com/>



جستجوی ایمیل

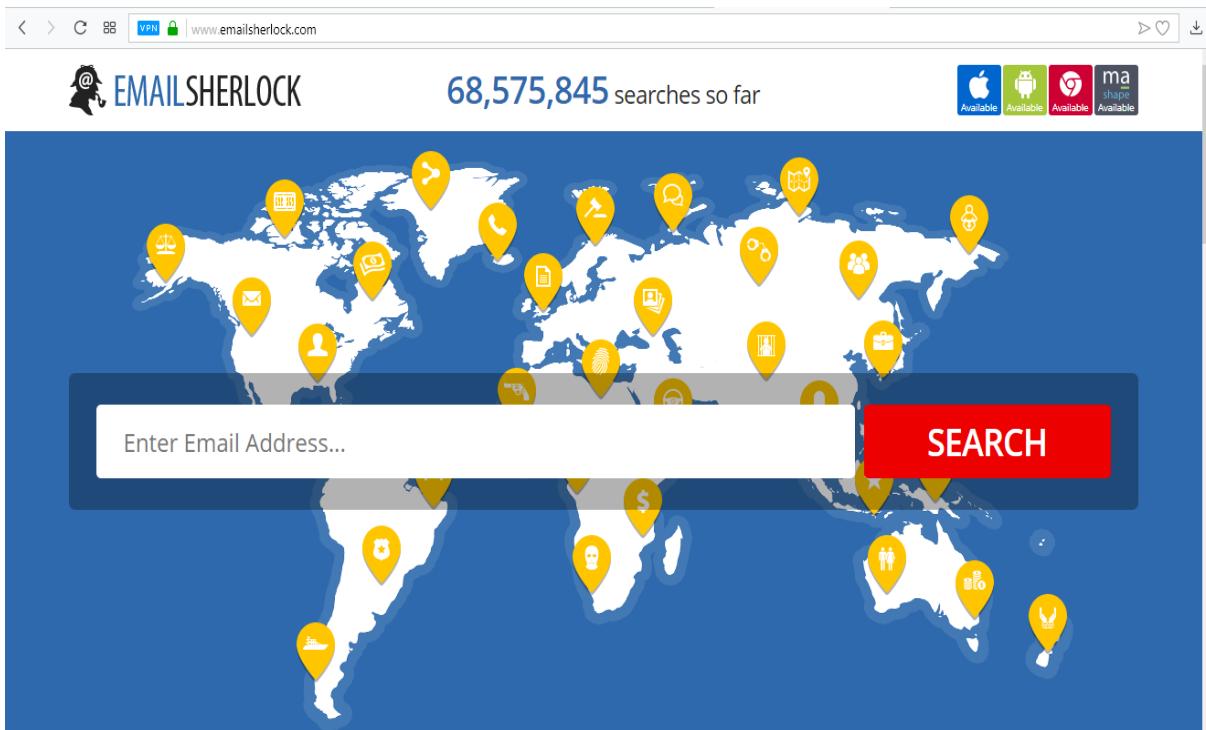
اکنون یاد گرفتیم که چگونه اطلاعات مربوط به افراد و شرکت‌ها را استخراج کنیم، بگذارید یک گام بیشتر برداریم و بینیم که چه اطلاعات دیگری می‌توانیم با استفاده از نام کاربری یک شخص استخراج کنیم که در بیشتر موارد آدرس ایمیل شخص است.

EmailSherlock¹

EmailSherlock یک موتور جستجوی ایمیل معکوس است. آنچه انجام می‌دهد این است که هنگامی که ما آدرس ایمیل ای به آن ارائه می‌کنیم، اگر این ایمیل در حساب کاربری طیف وسیعی از وبسایت‌ها و بیشتر رسانه‌های اجتماعی استفاده شده باشد، استخراج می‌شود. این نوع اطلاعات می‌تواند زمانی که ما فقط آدرس ایمیل فرد مورد علاقه را داریم، بسیار مفید باشد. هنگامی که می‌دانیم که این شخص خاص ثبت شده است، ما می‌توانیم پیش برویم و یک حساب کاربری در آن ایجاد کرده و ممکن است بتوانیم اطلاعاتی را که ما مجاز به دسترسی به آن نیستیم، استخراج کنیم. همانند EmailSherlock یک سرویس دیگر به نام UserSherlock وجود دارد که برای نام‌های کاربری مشابه است.

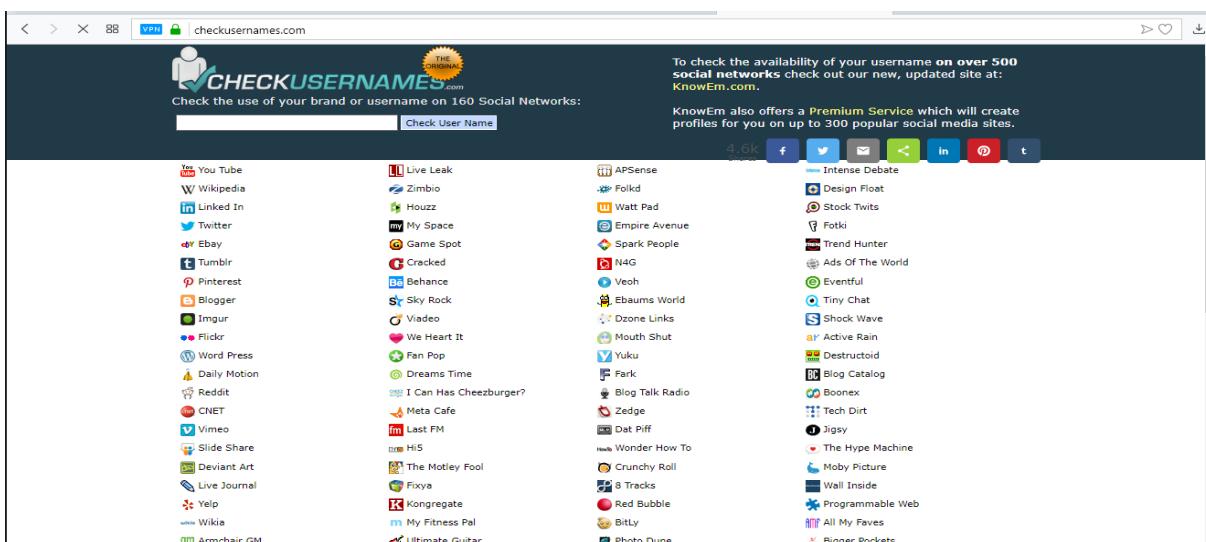
¹ <http://www.emailsherlock.com>

اگر چه نتایج ارائه شده توسط این سرویس‌ها ۱۰۰٪ دقیق نیستند، اما آن‌ها مکان خوبی برای شروع هستند.



CheckUsernames¹

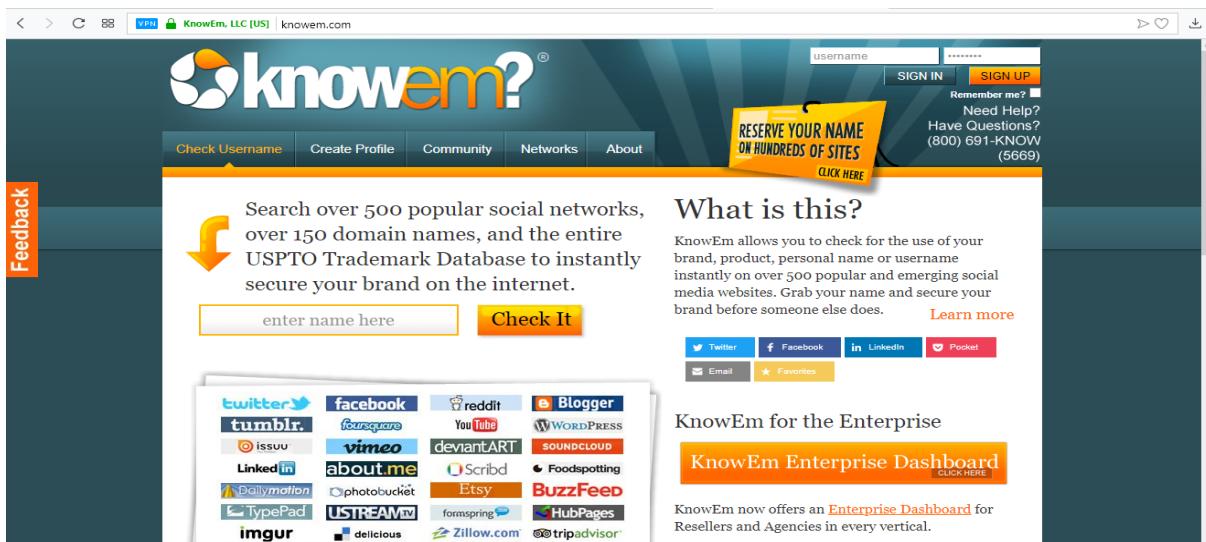
مشابه CheckUsernames نام کاربری ارائه شده به آن را از طریق لیست عظیمی از وبسایت‌های رسانه‌های اجتماعی بررسی می‌کند که آیا این نام کاربری در دسترس آن‌هاست یا خیر.



¹ <http://checkusernames.com>

KnowEm¹

وبسایت مورد بحث در بالا (checkusernames.com) طراحی شده و به همین ترتیب می‌توان آن را برای بررسی نام‌های کاربری مورد استفاده قرار داد، اما علاوه بر آن برای بررسی نام دامنه و علامت تجاری نیز مورد استفاده قرار می‌گیرد.



Facebook²

برخلاف بسیاری از سایت‌های شبکه اجتماعی، فیسبوک به ما اجازه می‌دهد که افراد را با استفاده از آدرس‌های ایمیل جستجو کنیم و یکی از بزرگ‌ترین شبکه‌های اجتماعی است.

جستجوی وب معنایی

در فصل ۲، ما در مورد وب معنایی بحث کردیم و این که چگونه یک بخش جدایی‌ناپذیر از وب آتی خواهد بود. اجازه دهید با بعضی از موتورهای جستجوی وب معنایی آشنا شویم و بینید که چقدر بالغ هستند.

DuckDuckGo³

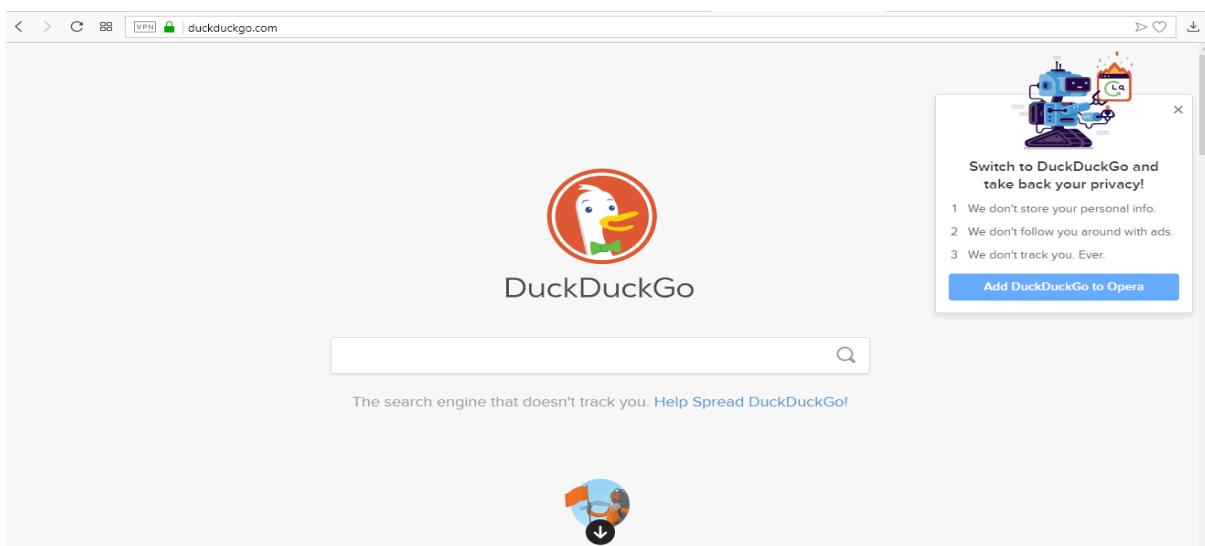
اگر چه نام DuckDuckGo ممکن است کمی برای یک موتور جستجو عجیب باشد، اما نتایج جستجو ارائه شده توسط آن بسیار شگفت‌انگیز است. نتایج جستجو ارائه شده توسط آن بسیار مربوط است. تبلیغات و ستون‌های فرعی زیادی وجود ندارد تا این فضای پر کند و به کاربر کمک می‌کند تا هدف خود را انتخاب کند و نتایج را

¹ <http://knowem.com>

² <https://www.facebook.com>

³ <https://duckduckgo.com>

مطابق با آن دریافت کند. همانند گوگل پاسخ به پرسش‌های ریاضی را نیز فراهم می‌کند و پاسخ‌هایی را برای پرسش‌ها مانند آب‌وهوا و مکان فراهم می‌کند. برگه تعریف به‌سادگی معنای کلیدواژه عرضه شده را فراهم می‌کند. نوار زیر جعبه پرس‌وجو بسیار مرتبط است و دسته‌بندی‌هایی را برای موضوعات ارائه می‌دهد. بسته به پرس‌وجو، مانند جستجوی گروه موسیقی آن را با فیلم‌های مربوطه نشان می‌دهد، در حالی که در جستجوی سواحل تایلند تصاویری از سواحل را نشان می‌دهد. رشد سریع ویژگی‌های باور نکردنی، آن را قابل رقابت با موتورهای جستجو بزرگ مانند گوگل، بینگ و یاهو کرده و به آرامی آن را سزاوار به رسمیت شناختن. می‌کند.



Kngine¹

موتور جستجوی عالی با قابلیت‌های معنایی است. برخلاف موتورهای جستجوی معمولی، ما اجازه داریم سوالات را مطرح و سعی کنیم به آن پاسخ دهیم. ما می‌توانیم پرس‌وجوی هایی مانند "چه کسی رئیس جمهور روسیه بین ۱۹۹۰ و ۲۰۱۰ بود" انجام داده و لیست را با نام، تصاویر و دیگر جزئیات مربوط به روسیه را بیینیم. به همین ترتیب جستجوی "GDP of Italy" مقدار زیادی اطلاعات مرتبط را به شکل داده‌ها و نمودارها و لینک‌های وب می‌دهد؛ بنابراین زمانی که سوالاتی در ذهن ما ظاهر شود ما مطمئناً می‌توانیم آن را امتحان کنیم.

¹ <http://kngine.com>

جستجوی رسانه‌های اجتماعی

رسانه‌های اجتماعی پلت فرمی وسیع هستند و تأثیرات آن‌ها نیز در سطح شخصی و یا شرکت مشابه است. قبل از مورد رسانه‌های اجتماعی و همچنین در مورد چگونگی جستجو از طریق برخی از شبکه خاص بحث کردیم، اکنون اجازه دهید برخی از موتورهای جستجوی رسانه‌های اجتماعی و قابلیت‌های آن‌ها را بررسی کنیم.

SocialMention^۱

آن چه SocialMention می‌کند، اساساً جستجو و تجزیه و تحلیل رسانه‌های اجتماعی در زمان است. بیایید جستجوی آن را به دو قسمت تقسیم کنیم. در بخش جستجو، SocialMention به دنبال سیستم‌های رسانه‌های مختلف اجتماعی مانند وی‌بلاگ‌ها، شبکه‌های اجتماعی، رویدادها وغیره و حتی از طریق نظرات است. نتایج به دست آمده می‌تواند بر اساس تاریخ و منبع طبقه‌بندی شوند و همچنین می‌تواند برای جدول زمانی مانند ساعت، روز، هفته وغیره فیلتر شوند. همچنین گزینه جستجوی پیشرفته را فراهم می‌کند که با استفاده از آن می‌توانیم پرسش‌ها را برای نتایج دقیق‌تر آماده کنیم. برخلاف موتورهای جستجوی معمولی، جستجوی رسانه‌های اجتماعی به‌طور خاص دارای یک مزیت بزرگ است که می‌تواند به درک رسیدن و شرایطی که در محتوا توسط افراد ایجاد شده جستجو کنیم. از این طریق، ما می‌توانیم درک بهتر موضوع را در مورد نحوه ارتباط افراد با این شرایط و سطح آن بیینیم.

اکنون اجازه دهید به بخش جستجو برویم، SocialMention نه تنها نتیجه جستجو را برای ما فراهم می‌کند، بلکه سطح ارتباطات مرتبط با آن را نشان می‌دهد. همچنین سطح قدرت، اشتیاق و دسترسی به شرایط پرس‌وجو ما در اقیانوس وسیعی از رسانه‌های اجتماعی را نشان می‌دهد. به غیر از این می‌توانیم کلمات کلیدی، کاربران، هشتگ‌ها و منابع مرتبط با پرس‌وجو را بیینیم. یکی از بهترین ویژگی‌های ارائه شده توسط این پلت فرم منحصر به فرد این است که نه تنها می‌توانیم این اطلاعات را مشاهده کنیم، بلکه آن را به صورت یک فایل CSV دانلود می‌کنیم. SocialMention همچنین اجازه می‌دهد تا هشدارهای ایمیل را برای کلمات کلیدی خاص راه‌اندازی کنیم. نوع اطلاعاتی که این پلتفرم فراهم می‌کند نه تنها برای استفاده شخصی مفید است، بلکه می‌تواند برای شرکت‌ها نیز تأثیر زیادی داشته باشد؛ ما می‌توانیم بررسی کنیم که چگونه نام تجاری ما در عرصه اجتماعی استفاده می‌شود.

^۱ <http://socialmention.com/>

socialmention*

Real-time social media search and analysis:

 in All

Trends:

Feedback

[About](#) - [Alerts](#) - [API](#) - [Trends](#) - [Follow us](#) - [FAQ](#)

social mention is a real time search platform

Blogs Microblogs Bookmarks Images Video All

fifa

Advanced Search Preferences

socialmention*



Mentions about fifa

Sort By: Date Results: Anytime

Results 1 - 15 of 161 mentions

- [@pepsi_jpn @MASSU_NO_FIFA](#) たかがジャンケンでジャンケンしたんじゃないですか？明日返答えてください。 twitter.com/mokun1/status/1117375242530213889
45 seconds ago - by  @mokun1 on [twitter](#)
- [RT @TwoSyncOfficial](#): For a chance to win 12k FIFA Points after the Fight For King game on Sunday, simply retweet this tweet and @ a friend... twitter.com/swfcmad/status/1117375204118941696
54 seconds ago - by  @swfcmad on [twitter](#)
- [RT @Aaruls12](#): Throwback to 2013 when FIFA president Sepp Blatter mocked Ronaldo in an interview & 2 days later Ronaldo replied with a hat-t... twitter.com/Babyfacee007/status/1117375175081721856
1 minute ago - by  @Babyfacee007 on [twitter](#)
- [RT @efootdefrance](#): 1/4 de finale #FIFAE Nations Cup BR VS FR ① 12h30 heure anglaise (13h30 en France) [#FiersdetreB...](http://https://t.co/sfFBXHBt07) [https://t.co/sfFBXHBt07](http://twitter.com/M_FIFA_FR/status/1117375103816409089) [#FiersdetreB...](http://twitter.com/M_FIFA_FR/status/1117375103816409089)
1 minute ago - by  @M_FIFA_FR on [twitter](#)

 RSS Feed

 Email Alert

 CSV/Excel File

 CSV Data

 Sentiment

 Top Keywords

 Top Users

 Top Hashtags

advertisement

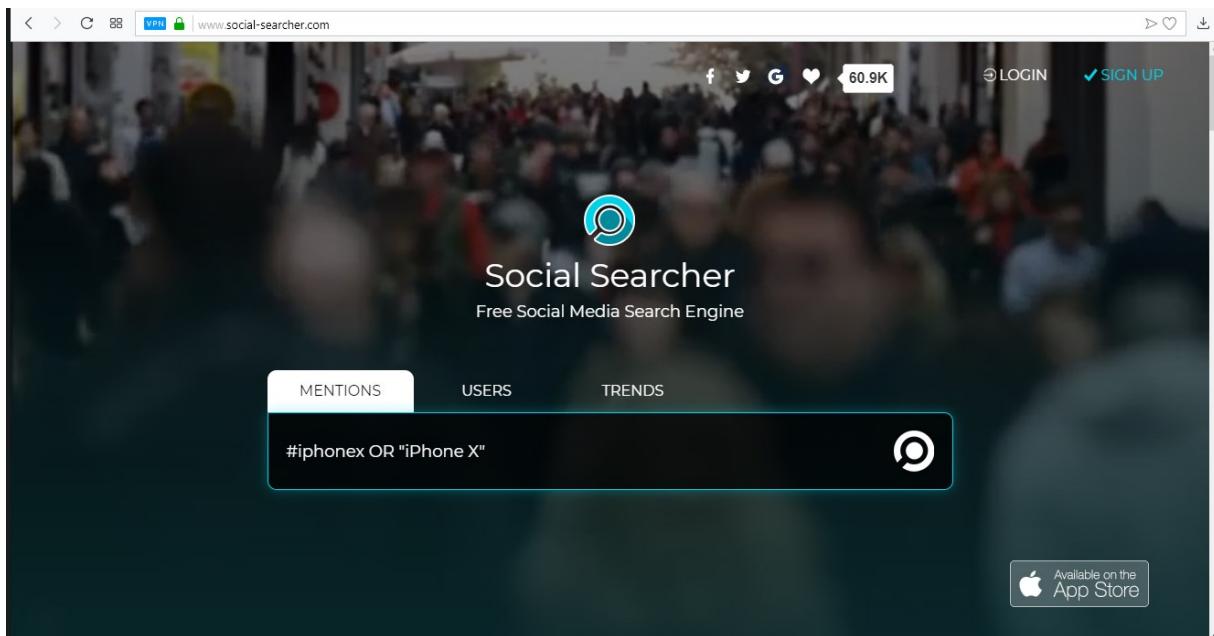


Social Searcher¹

یکی دیگر از موتور جستجوی رسانه‌های اجتماعی است. از فیسبوک، توییتر و Google+ به عنوان منابع استفاده می‌کند. رابط کاربری ارائه شده توسط این موتور جستجو ساده است. در برگه جستجو، نتایج جستجو به سه زبانه بر اساس منبع توزیع می‌شود، در زیر این برگه‌ها، پست‌ها با پیش‌نمایش فهرست شده‌اند که در شناسایی آنچه مربوط به ما هستند، بسیار مفید است. همانند SocialMention می‌توانیم هشدارهای ایمیل را نیز تنظیم کنیم.

¹ <http://www.social-searcher.com>

در زبانه جستجو، ما می‌توانیم تجزیه و تحلیل احساسات، کاربران، کلمات کلیدی، دامنه‌ها و خیلی بیشتر را بینیم. یکی از جالب‌ترین زبانه‌ها، زبانه ترند است که نتایج را با تعاملات بیشتر از قبیل دوست، retweets و غیره فهرست می‌کند.



توبیتر

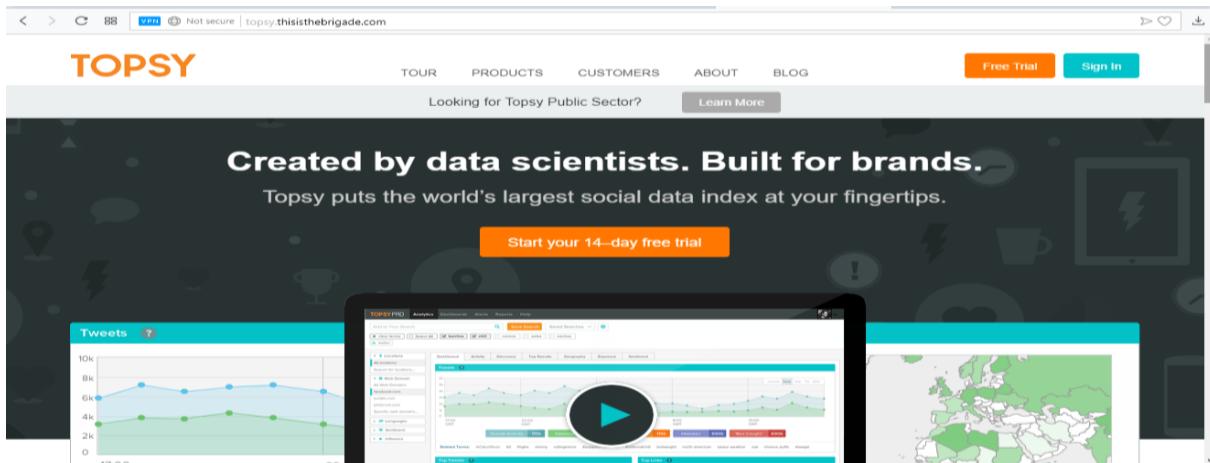
توبیتر یکی از محبوب‌ترین سایت‌های شبکه‌های اجتماعی است که تأثیر زیادی دارد. به غیر از قابلیت معمول آن برای میکروبلاگینگ، اجازه می‌دهد تا به درک هر کاربر در آن برسیم که آن را به عنوان ابزاری قدرتمند شناسایی کرده است. امروزه به طور گسترده‌ای برای ارتقاء بازار و همچنین تحلیل چشم‌انداز اجتماعی مورد استفاده قرار می‌گیرد.

Topsy¹

Topsy ابزاری است که به ما اجازه می‌دهد تا به جستجوی و نظارت بر توبیتر بپردازیم. با استفاده از آن می‌توانیم روند کلی کلمه کلیدی را در توبیتر بررسی کنیم و آن را تحلیل کنیم. رابط کاربری آن بسیار ساده است و مانند یک موتور جستجوی معمولی، فقط نتایج بر اساس توبیتر است. نتایج ارائه شده توسط آن می‌تواند به فریم‌های مختلف مانند یک روز، ۳۰ روز و غیره محدود شود. ما همچنین می‌توانیم نتایج را فیلتر کنیم تا فقط تصاویر، توبیت‌ها، لینک‌ها، ویدیوها و یا عکس‌ها را بینیم. یک فیلد دیگر وجود دارد که به ما اجازه می‌دهد فقط نتایجی

¹ <http://topsy.thisisthebrigade.com>

را که حاوی زبان‌های خاص را هستند بینیم. Topsy یک ابزار عالی برای نظارت بر بازار با استفاده از کلمات کلیدی خاص است.



Trendsmap¹

یک پلتفرم بصری عالی است که موضوعات متنوع را در قالب کلمات کلیدی، هشتک‌ها و توییت‌ها بر روی نقشه جهان نشان می‌دهد. این پلت فرم عالی است که با استفاده از نمایش بصری از ترندها برای درک اینکه چه چیزی در یک منطقه خاص از جهان داغ است. به غیر از نشان دادن این شکل بصری از اطلاعات، همچنین می‌توانیم در قالب یک موضوع یا یک مکان جستجو کنیم که باعث می‌شود فقط چیزی را که می‌خواهیم بینیم.

tweetbeep²

Tweetbeep مانند گوگل برای توییتر است. این یک سرویس عالی است که به ما اجازه می‌دهد موضوعات مورد علاقه در توییتر نظری نام تجاری، محصول یا به روز رسانی مربوط به شرکت‌ها و حتی لینک‌ها را نظارت کنیم. با هدف نظارت بر بازار، این یک ابزار عالی است که می‌تواند به ما کمک کند تا به سرعت به موضوعات مورد علاقه برسیم.

¹ <http://trendsmap.com>

² <http://tweetbeep.com>

The screenshot shows a dark-themed web page with a sidebar titled "Related Links". The links listed are:

- Twitter Followers
- Comprar Followers Instagram
- Followers on Instagram
- Instagram
- Instagram Followers

Below the sidebar, there is a small note: "2019 Copyright. All Rights Reserved." and a disclaimer about sponsored listings.

Twiangulate¹

یک ابزار عالی است که انجام triangulations توییتر را اجازه می‌دهد. با استفاده از آن می‌توانیم افرادی مرتبط توییتر را بیابیم. به طور مشابه، قابلیت را برای مقایسه دسترسی دو کاربر فراهم می‌کند. این ابزار عالی برای درک و مقابله با نفوذ مختلف کاربران توییتر است.

The screenshot shows the Twiangulate search interface. It features a search bar with the placeholder "example: BillGates + Oprah". Below the search bar are four input fields:

- Followed by:** An input field containing "@".
- Followers of:** An input field containing "@".
- Reach of:** An input field.
- Keywords:** An input field.

Below these fields is a "RETRIEVE" button. To the right of the search bar is a "Sign In" button and a "more tools" link. The main heading "Twiangulate" is displayed prominently at the top.

Make Twitter relevant.

Twiangulate powers
journalism, non-profits and PR:

- Find experts and insiders. Discover which accounts are followed by key people in a scribe swarm, gossip empire, artful sphere or judicious circle.

¹ <http://twiangulate.com/search>

جستجوی سورس کد

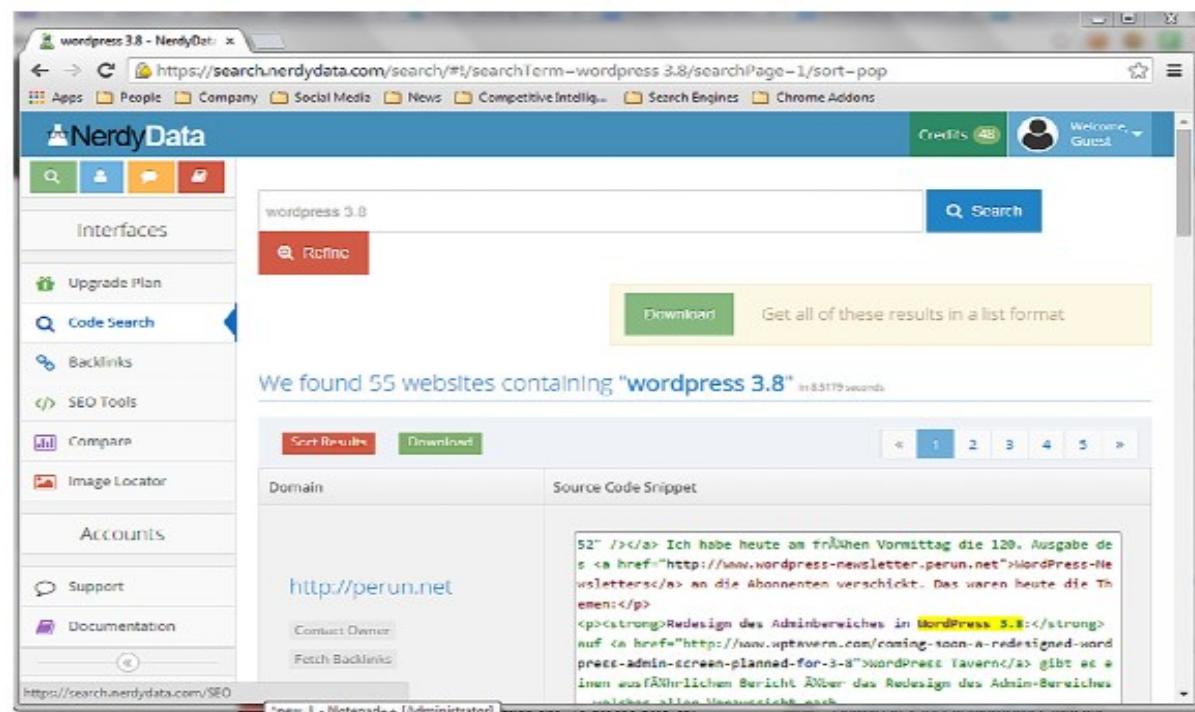
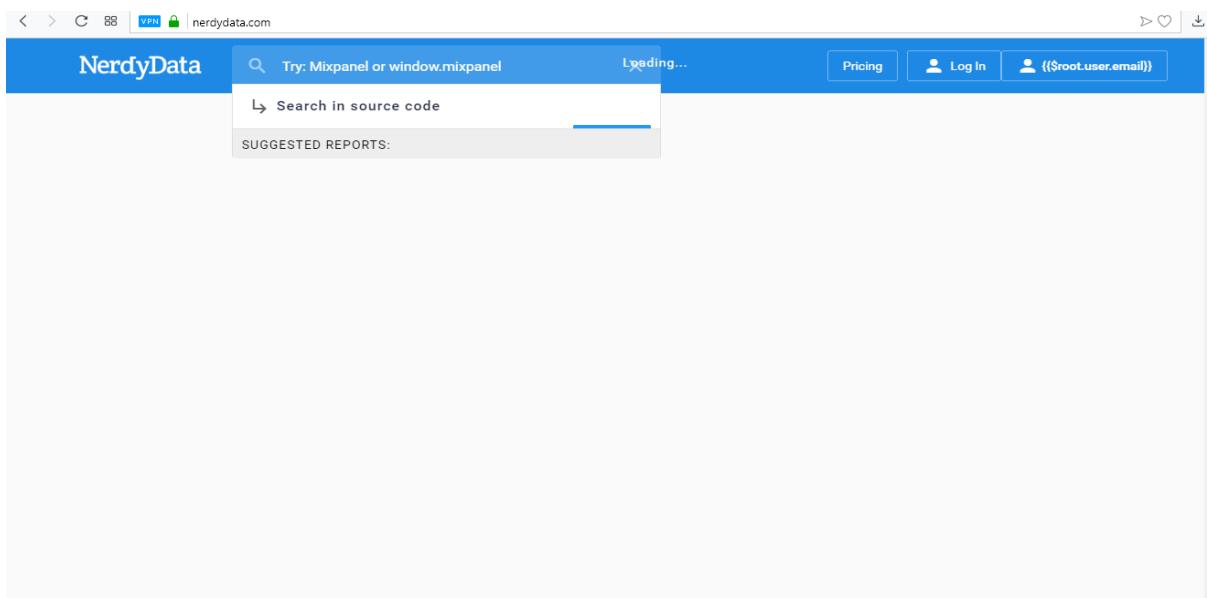
اکثر موتورهای جستجو فقط از متن‌های قابل مشاهده در صفحه وب استفاده می‌کنند، اما برخی از موتورهای جستجو وجود دارد که سورس کد موجود در اینترنت را نشان می‌دهند. این نوع موتورهای جستجو هنگامی که ما به دنبال تکنولوژی خاصی که در اینترنت استفاده می‌شود، مانند سیستم مدیریت محتوا یی چون ورد پرس، بسیار مفید می‌باشد. این موتورهای جستجو برای بهینه‌سازی موتورهای جستجو، تحلیل رقابتی، جستجوی کلیدواژه برای بازاریابی و توسط خلاقیت کاربر محدود می‌شوند.

با توجه به مسائل ذخیره‌سازی و مقیاس‌پذیری، قبل‌هیچ ارائه دهنده خدمات در این حوزه وجود نداشت، اما با پیشرفت‌های تکنولوژیکی، برخی از گزینه‌ها در حال شکل‌گیری هستند.

NerdyData¹

NerdyData یکی از اولین موتورهای جستجوی منحصر به فرد است که به ما اجازه می‌دهد که کد صفحه وب را جستجو کنیم. با استفاده از این پلتفرم بسیار ساده، به URL <https://search.nerdydata.com/> بروید، کلمه کلیدی مانند WordPress 3.7 را وارد کنید و NerdyData لیست وب‌سایت‌هایی را که حاوی این کلمه کلیدی در سورس کد هستند را فهرست می‌کند. نتایج نه تنها نشانی اینترنتی وب‌سایت‌ها را ارائه می‌دهد، بلکه بخش کد را با کلیدواژه برجسته شده در زیر بخش سورس کد نشان می‌دهد. به غیر از این، ویژگی‌های مختلفی از قبیل نویسنده، بازخورد دریافتی و دیگر موارد وجود دارد که می‌تواند بسیار مفید باشد اما اکثر آن‌ها رایگان نیستند، با این حال استفاده محدود از NerdyData بسیار مفید است و ارزش امتحان کردن را دارد.

¹ <http://nerdydata.com>

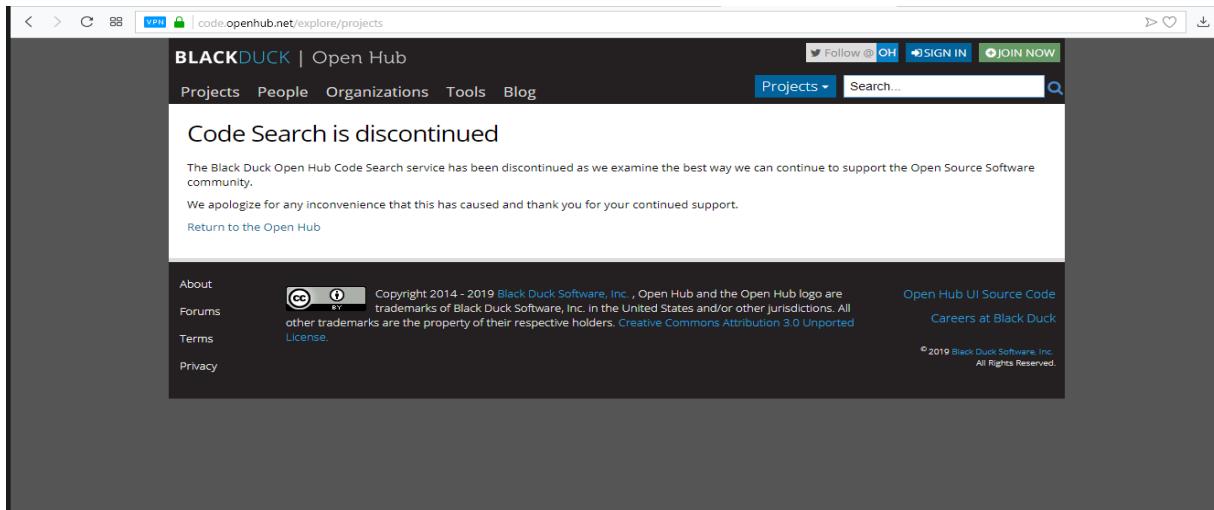


Ohloh code¹

یکی دیگر از موتورهای جستجوی عالی برای جستجوی سورس کد است، اما کمی متفاوت است که برای سورس کد متن باز جستجو می‌کند. این به این معنی است که منبع اطلاعاتی آن کدهایی است که در فضاهای باز هستند.

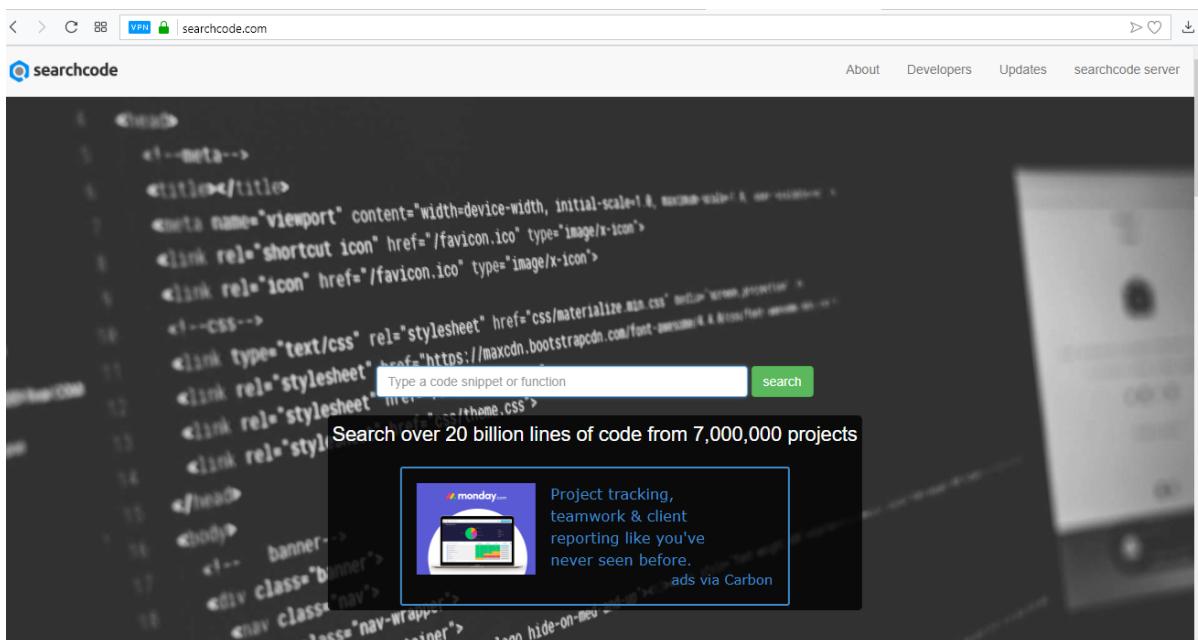
¹ <https://code.ohloh.net>

گزینه‌های بزرگی را فراهم می‌کند تا نتایج را بر اساس تعریف‌ها، زبان‌ها (برنامه‌نویسی)، برنامه‌های افزودنی و غیره از طریق یک نوار در سمت چپ با عنوان «نتایج کد فیلتر» فراهم کند.



Searchcode¹

همانند Ohloh، همچنین از مخزن سورس کد باز استفاده می‌کند. فیلترهای جستجو ارائه شده توسط Searchcode بسیار مفید هستند، برخی از آن‌ها مخزن، منبع و زبان هستند.



¹ <https://searchcode.com>

اطلاعات فنی

ما در مورد برخی از موتورهای جستجوی منحصر به فرد کار خواهیم کرد که به ما در جمع‌آوری اطلاعات مربوط به فن‌آوری‌های مختلف و خیلی چیزهای دیگر کمک می‌کند. در این بخش ما به شدت با آدرس‌های IP و شرایط مربوطه روبرو می‌شویم، بنابراین توصیه می‌شود از بخش "اصطلاحات پایه" در فصل اول استفاده کنید.

Whois¹

اساساً Whois سرویس ای است که به ما اجازه می‌دهد اطلاعات مربوط به ثبت کننده یک منبع اینترنتی مانند نام دامنه را به دست آوریم. با استفاده از Whois.net می‌توانیم جستجو Whois را برای یک دامنه یا آدرس IP انجام دهیم. رکورد whois معمولاً شامل اطلاعات ثبت کننده می‌شود. اطلاعات ثبت‌نام مانند نام، آدرس ایمیل، تاریخ ثبت‌نام، انقضا و غیره.

Robtex²

ابزار بسیار خوبی برای پیدا کردن اطلاعات در مورد منابع اینترنتی مانند آدرس IP، نام دامنه، سیستم Autonomous System (AS) و غیره است. رابط کاربری آن سیار ساده است. در گوش سمت چپ بالا یک نوار جستجو است که با استفاده از آن می‌توان اطلاعات را جستجو کرد. جستجو برای یک دامنه به ما اطلاعات مرتبط مانند آدرس IP، مسیر، شماره AS، محل و غیره را می‌دهد. به‌طور مشابه اطلاعات دیگری برای آدرس‌های IP، مسیر و غیره ارائه می‌شود.

¹ <http://whois.net>

² <http://www.robtex.com>

The screenshot shows the homepage of Robtex. At the top, there's a search bar with placeholder text "hostname, ipnumber, route or AS-number" and a "GO" button. Below the search bar, there are three main sections: "What is Robtex used for?", "What does Robtex do?", and "How to use Robtex?". Each section contains some descriptive text and links. At the bottom of the page, there's a note about using cookies and a "Got it!" button.

W3dt¹

W3dt منبع آنلاین بزرگ برای پیدا کردن اطلاعات مرتبط با شبکه است. بخش‌های مختلفی وجود دارد که ما می‌توانیم با استفاده از این پلت فرم انجام دهیم. بخش اول، ابزارهای نام دامنه (DNS) است که به ما امکان می‌دهد DNS server fingerprinting، DNS lookup معکوس، وغیره را انجام دهیم. بخش دوم، ابزار مربوط به شبکه و یا اینترنت مانند اسکن پورت، traceroute، MX رکورد و غیره است. بخش بعدی وب HTTP است که متشکل از ابزارهایی مانند Whois، decode، بازیابی هدر HTTP، جستجوی SSL certificate info، URL encode / ، وجود در نهایت برخی از ابزارهای عمومی (مانند ping) دارد. در کل مجموعه وسیعی از ابزارهای کارهای مفید مختلف را در یک رابط کاربری انجام دهیم.

¹ <https://w3dt.net/>



Shodan¹

تا کنون ما انواع مختلفی از موتورهای جستجو را استفاده کرده‌ایم که به ما کمک می‌کند تا از طریق روش‌های مختلف وب را کشف کنیم. چیزی که ما تا به حال با آن مواجه نبودیم یک موتور جستجوی اینترنتی است (تفاوت بین وب و اینترنت توضیح داده شده در فصل ۱ را به یاد داشته باشد). Shodan موتور جستجویی است که اینترنت را اسکن می‌کند و سرویس‌ها را بر اساس آدرس IP و پورت باز لیست می‌کند. این ابزار اجازه می‌دهد تا این اطلاعات را با استفاده از آدرس‌های IP، فیلترهای کشور و خیلی بیشتر جستجو کنیم. با استفاده از آن می‌توانیم اطلاعات ساده مانند وب‌سایتها را با نوع خاصی از وب سرور مانند IIS و یا آپاچی پیدا کنیم و همچنین اطلاعاتی را که می‌تواند بسیار حساس باشد مانند دوربین‌های IP بدون احراز هویت و سیستم‌های SCADA را از طریق اینترنت پیدا کرد.

اگرچه نسخه رایگان آن بدون ثبت‌نام، اطلاعات بسیار محدودی را ارائه می‌دهد که می‌تواند کمی با استفاده از یک حساب کاربری ثبت‌شده کاهش یابد، با این حال بهاندازه کافی برای درک قدرت این موتور جستجوی منحصر به فرد مناسب است. ما می‌توانیم قدرت این ابزار را از طریق افزودنی مرورگر یا از طریق رابط برنامه‌نویسی برنامه خود نیز استفاده کنیم. Shodan دارای یک سابقه پیشرفت بسیار فعال است و ویژگی‌های جدیدی را ارائه می‌دهد، بنابراین ما می‌توانیم انتظارات بیشتری از آن را در آینده داشته باشیم.

¹ <http://www.shodan.io>

The screenshot shows the Shodan homepage. At the top, there's a navigation bar with links for 'Shodan', 'Developers', 'Book', 'View All...', 'Explore', 'Pricing', 'Enterprise Access', 'New to Shodan?', and 'Login or Register'. Below the navigation is a search bar with the URL 'www.shodan.io'. The main feature is a large globe representing the internet, with numerous red dots indicating connected devices. Specific IP addresses like '67.20.69.105' and '56.87.75.184' are highlighted. Below the globe, there are four service offerings: 'Explore the Internet of Things' (with a cloud icon), 'See the Big Picture' (with a globe icon), 'Monitor Network Security' (with an eye icon), and 'Get a Competitive Advantage' (with a money icon). Each offering has a brief description.

WayBack Machine¹

WayBack Machine یک منبع عالی برای جستجوی یک وب‌سایت در گذشته است. به سادگی آدرس وب‌سایت را در نوار جستجو تایپ کنید و یک جدول زمانی را با عکس فوری موجود در تقویم نشان می‌دهد. این ابزار برای جستجوی اینکه چگونه وب‌سایت تکامل یافته، عالی است و بنابراین رشد گذشته را نظارت می‌کند. همچنین می‌تواند برای بازیابی اطلاعات از یک وب‌سایت که در گذشته موجود بود اما اکنون نیست، مفید باشد.

The screenshot shows the Wayback Machine website. At the top, there's a navigation bar with links for 'ABOUT', 'CONTACT', 'BLOG', 'PROJECTS', 'HELP', 'DONATE', 'JOBS', 'VOLUNTEER', 'PEOPLE', and 'SIGN IN'. Below the navigation is the 'INTERNET ARCHIVE' logo and the 'Wayback Machine' logo. A search bar with the placeholder 'http://...' and a 'BROWSE HISTORY' button are also present. The main content area features several historical web pages from different years. Below this, there are three sections: 'Tools' (listing 'Wayback Machine Availability API', 'WordPress Broken Link Checker', and '404 Handler for Webmasters'), 'Subscription Service' (describing 'Archive-It' and its capabilities), and 'Save Page Now' (with a form to enter a URL and a 'SAVE PAGE' button).

¹¹ <http://archive.org/web/web.php>

جستجوی مجدد تصویر

همه ما با عبارت "یک تصویر ارزش هزار کلمه را دارد" آشنا هستیم و همچنین از سیستم‌هایی مانند Google Deviantart³ ، Flickr² ، Images¹ که از تصاویر به عنوان کلمات کلیدی استفاده می‌کنند. معمولاً زمانی که ما نیاز به جستجوی اطلاعاتی داشته باشیم، یک کلمه کلیدی یا مجموعه‌ای از آن‌ها را به صورت متن داریم، به همین ترتیب موتورهای جستجویی که با آن‌ها آشنا شدیم، متن را به عنوان ورودی گرفته و نتایج را به ما می‌دهند، اما در اینجا ما تصویر داریم و می‌خواهیم بینیم این تصویر کجا در وب ظاهر شده است، کجا برویم؟ این جایی است که موتورهای جستجوی تصویر معکوس وارد می‌شوند که تصویر را به عنوان ورودی می‌گیرند و بر اساس آن وب را جستجو می‌کنند. اجازه دهید با برخی از آن‌ها آشنا شویم.

Google Images⁴

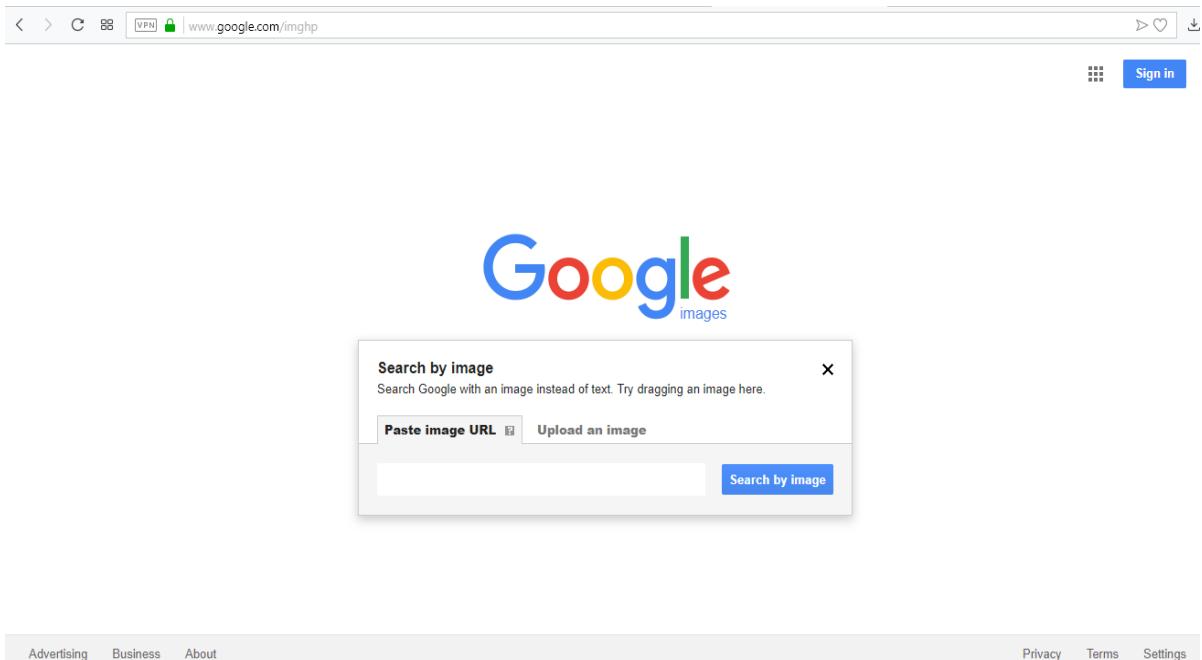
Google به ما اجازه می‌دهد تا تصاویر را در وب جستجو کنیم، اما آنچه بسیاری از ما آن آگاه نیستیم، جستجوی تصویر معکوس است. ما به سادگی باید به آدرس <http://images.google.com> برویم و روی آیکون دوربین کلیک و URL تصویر در وب و یا یک فایل تصویری ذخیره شده به صورت محلی را ارسال کنیم، ما همچنین می‌توانیم تصویر را به نوار جستجو بکشیم و رها کنیم و گوگل لینک با صفحات حاوی آن یا تصاویر مشابه در وب را نشان می‌دهد.

¹ <http://images.google.com>

² <https://www.flickr.com>

³ <http://www.deviantart.com>

⁴ <http://images.google.com>



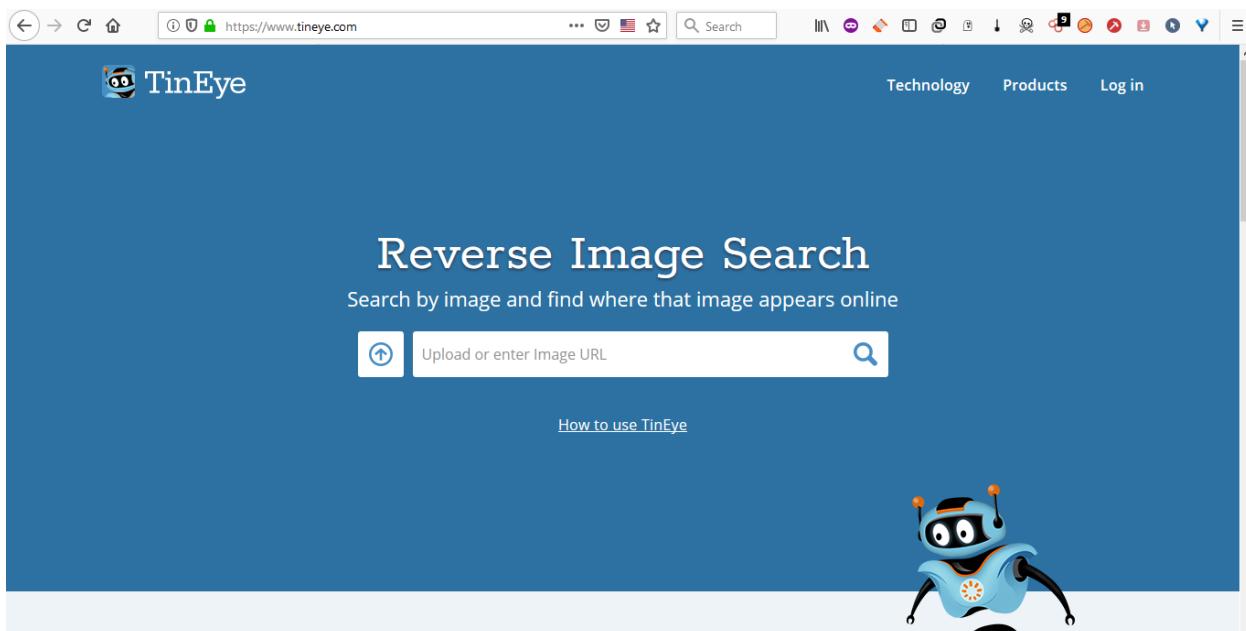
Advertising Business About

Privacy Terms Settings

TinEye¹

TinEye یکی دیگر از موتورهای جستجوی معکوس عکس است و دارای یک پایگاه داده بزرگ از تصاویر است. جستجو در TinEye مانند گوگل، بسیار ساده است، ما می‌توانیم URL تصویر را وارد کرده، آن را آپلود و یا کشیدن و رها کردن را انجام دهیم. همچنین پلاگینی را برای مرورگرهای اصلی فراهم می‌کند که کار را بسیار ساده‌تر می‌کند. اگر چه نتایج TinEye مانند گوگل جامع نیست، اما یک پلت فرم عالی برای این کار است و باید مورد استفاده قرار گیرد.

¹ <https://www.tineye.com>



ImageRaider¹

با سادگی لیست نتایج دامنه دلخواه را می‌دهد. اگر یک دامنه حاوی بیش از یک تصویر باشد، آن را نیز بیان می‌کند و پیوندهایی به آن تصاویر در نام دامنه ذکر شده است.

جستجوی تصویر معکوس می‌تواند برای پیدا کردن اطلاعات بیشتر در مورد فردی که ما با استفاده از روش‌های متداول اطلاعاتی در مورد آن کسب نکردیم، بسیار مفید باشد. همان‌طور که بسیاری از مردم از یک تصویر برای پروفایل‌های مختلف خود استفاده می‌کنند، ایجاد یک جستجوی تصویر معکوس می‌تواند ما را به جایی که در آن پروفایلی ایجاد کرده است، هدایت کند و همچنین اطلاعات قبل‌کشف نشده، به دست آید.

متفرقه

ما با لیست عظیمی از موتورهای جستجو که در دامنه خاصی عمل کرده و محبوب هستند، برخورد کردیم. در این بخش با انواع مختلفی از موتورهای جستجو که کمتر شناخته شده هستند اما در اهداف منحصر به فرد و موارد خاص بسیار مفید هستند، آشنا می‌شویم.

DataMarket²

¹ <http://www.ImageRaider.com>

² <http://datamarket.com>

یک پورتال باز است که متشکل از مجموعه داده‌های بزرگ است و داده‌ها را به شیوه‌ای عالی از طریق تصاویر ارائه می‌کند. جستجوی ساده نتایجی برای مباحث جهانی را ارائه می‌دهد که شامل لیستی از تصاویر مختلف مربوط به موضوع می‌باشد، به عنوان مثال جستجو برای کلمه کلیدی طلا، نتایجی نظیر آمار طلا، واردات / صادرات طلا و خیلی بیشتر را فراهم می‌کند. صفحه نتایج متشکل از یک نوار در سمت چپ است که لیستی از فیلترها را فراهم می‌کند که با استفاده از آن می‌توان نتایج ذکر شده را کاهش داد. همچنین اجازه می‌دهد تا ما اطلاعات خودمان را آپلود کنیم و از آن تصویر به دست آوریم. برای فهرستی عظیمی از موضوعاتی که DataMarket می‌کند، به لینک <http://datamarket.com/topic/list> مراجعه کنید.

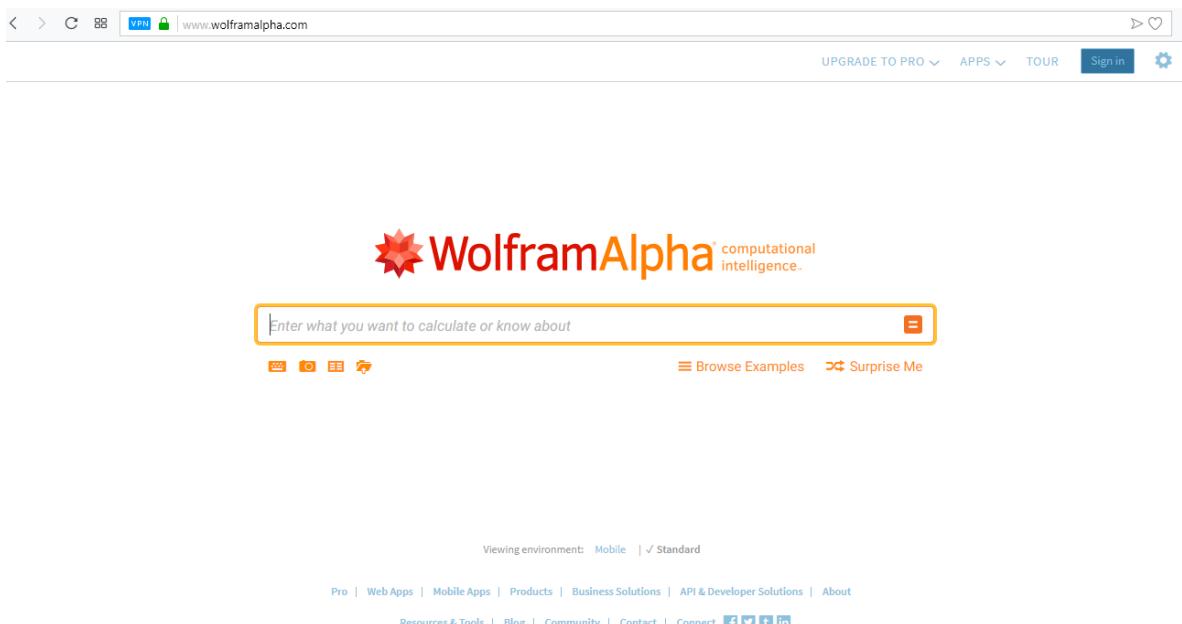


WolframAlpha¹

در این فصل ما درباره موتورهای جستجوی مختلف یاد گرفتیم که ورودی خاصی را گرفته و به ما لینک‌هایی ارائه می‌دهند که ممکن است پاسخ به سؤالاتی باشد که ما واقعاً دنبال آن هستیم، اما آنچه ما در حال حاضر در مورد آن یاد می‌گیریم، یک موتور جستجو نیست یک موتور دانش محاسباتی است. این بدان معنی است که نشانی‌های اینترنتی وبسایت‌های حاوی اطلاعات را ارائه نمی‌دهد، در عوض تلاش می‌کند تا پرس‌وجوهای طبیعی ما را درک کرده و بر اساس یک مجموعه داده‌های سازمان‌یافته، پاسخی واقعی به آن‌ها در فرم ارائه دهد.

¹ <http://www.wolframalpha.com>

برای مثال، ما می‌خواهیم بدانیم که هدف از دامنه mil. چیست، بنابراین می‌توانیم به سادگی پرس‌وجو "هدف از دامنه mil. اینترنت چیست؟" را وارد کنیم. برای مثال‌های بیشتری از حوزه‌های مختلف که قادر به پاسخ است، صفحه <http://www.wolframalpha.com/examples/> را بررسی کنید.



Addictomatic¹

معمولًاً ما از موتورهای مختلف برای جستجوی اطلاعات مربوط به یک موضوع بازدید می‌کنیم، اما متأسفانه انواع اخبار و رسانه‌های مختلف برای ایجاد یک داشبورد واحد برای هر موضوعی که مورد علاقه ما است، وجود دارد. در اینجا محتوای گردآوری شده در بخش‌های مختلف بسته به منبع نمایش داده می‌شود. همچنین به ما اجازه می‌دهد که این بخش‌ها را بر اساس اولویت برای قابلیت خواندن بهتر تغییر دهیم.

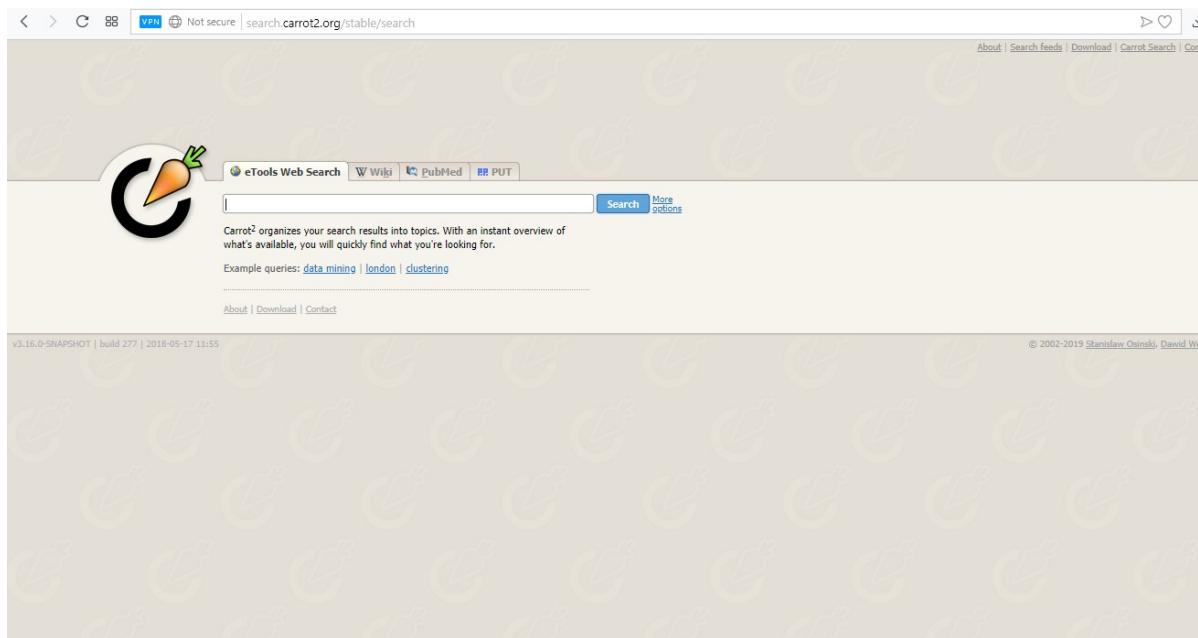
Carrot2²

Carrot2 یک موتور جستجوی خوشه‌ای است. این بدان معنی است که نتایج جستجو از موتورهای جستجو دیگر را می‌گیرد و این نتایج را به موضوعاتی با استفاده از الگوریتم‌های خوشه‌بندی تفکیک می‌کند. توانایی منحصر به فرد آن برای دسته‌بندی نتایج به موضوعات اجازه می‌دهد تا در کم بهتر و شرایط مرتبط را دریافت کنید. این خوشه‌ها نیز در اشکال مختلف جالب مانند پوشه‌ها، حلقه‌ها و FoamTree نمایان می‌شوند. برای استفاده از Carrot2

¹ <http://addictomatic.com>

² <http://search.carrot2.org/stable/search>

می‌توان از طریق رابط وب با استفاده از <http://search.carrot2.org/> و نیز از طریق نرم‌افزار کاربردی که از دانلود می‌شود، استفاده کرد.<http://project.carrot2.org/download.html>



Boardreader¹

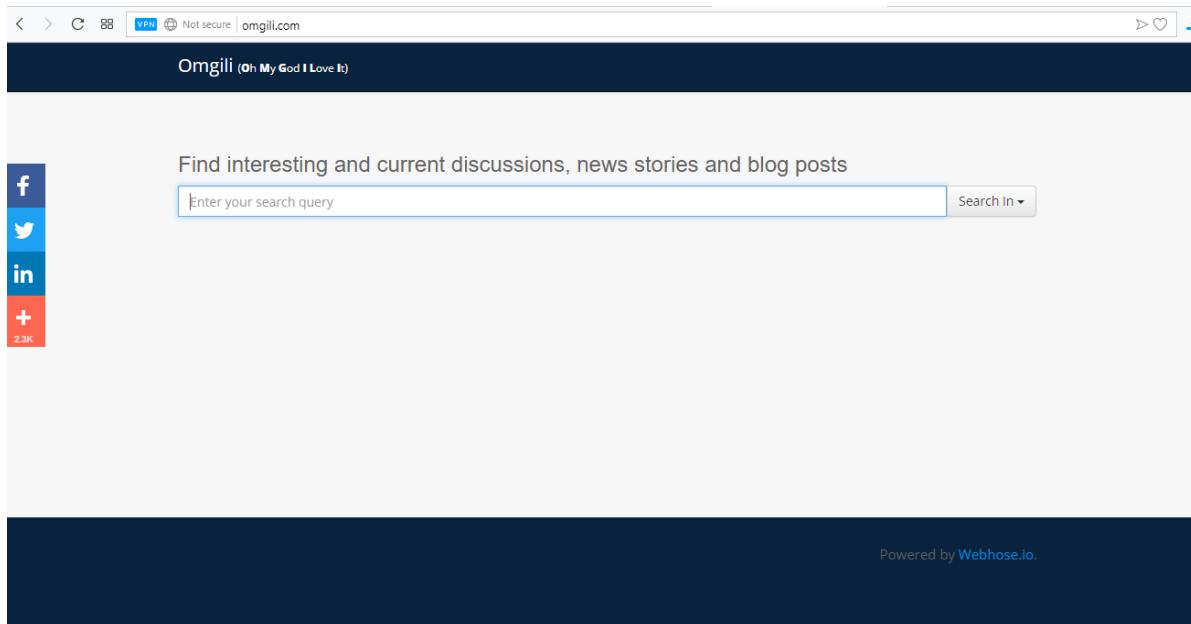
انجمن‌ها منبع غنی از اطلاعات هستند که تعامل زیاد و پرسش و پاسخ در این مکان‌ها اتفاق می‌افتد. اعضای آن‌ها از افراد تازه کار تا متخصصین در حوزه‌ی مرتبط با انجمن‌ها است. در مکان‌هایی مانند این، می‌توانیم پاسخ‌هایی به سوالاتی که در جای دیگر پیدا نمی‌شود، پیدا کنیم. چون آن‌ها صرفاً شامل محتوای تولیدشده توسط کاربر می‌شوند، اما چگونه آن‌ها را جستجو می‌کنیم؟ در اینجا پاسخ Boardreader است. این ابزار اجازه می‌دهد تا به جستجوی نتایج برای به دست آوردن نتایج حاوی محتوا با تعامل انسان باشیم. همچنین یک نمودار روند از کلیدواژه جستجو را نمایش می‌دهد تا میزان فعالیت مربوط به آن را نشان دهد. ویژگی‌های جستجوی پیشرفته ارائه شده توسط آن مانند مرتب‌سازی بر اساس ارتباط، وقوع بین تاریخ خاص، جستجوی خاص دامنه و غیره به ویژگی‌های آن اضافه شده است.

¹ <http://boardreader.com>

Omgili¹

همانند Boardreader نیز یک موتور جستجو انجمن‌ها است. این ابزار نتایج را در قالب جداول نمایش می‌دهد و این جداول حاوی اطلاعاتی از قبیل تاریخ، تعداد پست‌ها، نویسنده و غیره می‌باشد که می‌تواند در برآورد پیوند نتایج مفید باشد. یکی از این اطلاعات Thread است که اطلاعات بیشتر در مورد یک موضوع بدون بازدید از صفحه اصلی انجمن نام انجمن، تعداد نویسنده‌گان و پاسخ‌ها را به موضوع ارائه می‌دهد. همچنین به ما اجازه می‌دهد که نتایج را بر اساس جدول زمانی وقوع آن‌ها مانند ماه، هفته، روز و غیره فیلتر کنیم.

¹ <http://omgili.com/>



Truecaller¹

تقریباً هر کسی که از تلفن هوشمند استفاده می‌کند، از آن استفاده کرده است. بسیاری از افراد از نرم‌افزار مشهور Truecaller استفاده می‌کنند که به شناسایی فرد پشت شماره تلفن کمک می‌کند. Truecaller به سادگی به ما اجازه می‌دهد تا با شماره تلفن جستجو کرده و اطلاعات کاربر را با استفاده از پایگاه داده‌ی crowdsourced فراهم می‌کند.

موتورهای جستجوی دیگر عبارت‌اند از:

- ↳ Meta search engine
 - Search (<http://www.search.com/>)
- ↳ People search
 - ZabaSearch (<http://www.zabasearch.com/>)
- ↳ Company search
 - Hoovers (<http://www.hoovers.com/>)
 - Kompass (<http://kompass.com/>)
- ↳ Semantic
 - Sensebot (<http://www.sensebot.net/>)
- ↳ Social media search
 - Whostalkin (<http://www.whostalkin.com/>)
- ↳ Twitter search

¹ <http://www.truecaller.com>

- Mentionmapp (<http://mentionmapp.com/>)
 - SocialCollider (<http://socialcollider.net/>)
 - GeoChirp (<http://www.geochirp.com/>)
 - Twitterfall (<http://beta.twitterfall.com/>)
- ↳ Source code search
- Meanpath (<https://meanpath.com>)
- ↳ Technology search
- Netcraft (<http://www.netcraft.com>)
 - Serversniff (<http://serversniff.net>)
- ↳ Reverse image search
- NerdyData image search (<https://search.nerdydata.com/images>)
- ↳ Miscellaneous
- Freebase (<http://www.firebaseio.com>)

این فصل در مورد لیست عظیمی از موتورهای جستجو تحت دسته‌های مختلف بحث کردیم که به طور معمول استفاده نمی‌شوند، اما همان‌گونه که قبلاً دیده‌ایم، در سناریوهای مختلف بسیار مفیدند. همه برای جستجو به گوگل معتقد هستند و یکی از بهترین‌ها در بیشترین اوقات بوده است، اما گاهی اوقات نیاز به پاسخ‌های متفاوتی به پرسش‌ها داریم. موتورهای معرفی شده تلاش می‌کند تا جنبه‌های بیشتری از نیازهای جستجوی روزانه را پوشش دهد، اما مطمئناً باید موتورهای دیگری نیز وجود داشته باشند که برای حل مشکلات خاص مورد استفاده قرار گیرند.

در این فصل در مورد موتورهای جستجوی غیرمتعارف مختلف، ویژگی‌ها و قابلیت‌های آن‌ها یاد گرفتیم، اما درباره موتورهای جستجوی معمول مانند Google، Bing، Yahoo و غیره که ما هر روز استفاده می‌کنیم، بحث نشد! ما می‌دانیم که چگونه از آن‌ها استفاده کنیم؟ موتورهای جستجو که هر روز استفاده می‌کنیم دارای ویژگی‌های پیشرفته‌ای هستند که بسیاری از کاربران از آن اطلاع ندارند. این ویژگی‌ها به کاربران امکان می‌دهد تا نتایج را فیلتر کرده تا بتوانیم اطلاعات بیشتری را دریافت کنیم. در فصل بعد با موتورهای جستجوی متداول برخورد خواهیم کرد و یاد می‌گیریم چگونه از آن‌ها به طور مؤثر برای جستجوی بهتر و رسیدن به نتایج خاص‌تر استفاده کنیم.

فصل ۵: جستجوی پیشرفته وب

مقدمه

در فصل گذشته با برخی از موتورهای خاص که به ما اجازه می‌دهند، جستجوهای خاص را انجام دهیم، آشنا شدیم؛ حالا باید به عمق موتورهای جستجو متداول برویم که هر روز از آن‌ها استفاده می‌کنیم و بررسی کنیم چگونه می‌توانیم آن‌ها را به‌طور کامل مورد استفاده قرار داد. در این فصل، اساساً، ویژگی‌های جستجوی پیشرفته برخی از موتورهای جستجوی شناخته شده را درک خواهیم کرد و همه کارکردها و فیلترینگ‌هایی را که برای ارائه خدمات بهتر به ما ارائه می‌دهند، می‌بینیم.

بنابراین در حال حاضر سؤال اساسی در مورد موتور جستجو این است که چگونه در سراسر وب برای جمع‌آوری اطلاعات جستجو می‌کند. بگذارید یک‌بار در آن تجدیدنظر کنیم و به صورت عمیق آن را درک کنیم.

صفحات وب همان‌طور که آن‌ها را می‌بینیم، در واقع چیزی نیستند که به نظر می‌رسند. صفحات وب اساساً حاوی کد¹ HTML و در اغلب موارد جاوا اسکریپت‌ها و دیگر زبان‌های اسکریپتی هستند؛ بنابراین HTML اساساً یک زبان نشانه‌گذاری است و از تگ‌ها برای ساختن اطلاعات استفاده می‌کند، مثلاً تگ < h1 > / < h1 > برای ایجاد یک

¹ HyperText Markup Language

عنوان استفاده می‌شود. هنگامی که ما این کد HTML را از سرور دریافت می‌کنیم، مرورگرهای ما این کد را تفسیر کرده و صفحه وب را در فرم ارائه شده به ما نمایش می‌دهند. برای بررسی سورس کد سرویس دهنده یک صفحه وب، به سادگی با باز کردن صفحه وب، `Ctrl + L` را در مرورگر فشار دهید.

هنگامی که خزنده^۱ وب یک موتور جستجو به صفحه وب می‌رسد، به سراغ کد HTML آن می‌رود. اغلب این صفحات دارای پیوندهایی به صفحات دیگر هستند که توسط خزندها برای حرکت بیشتر در جمع‌آوری داده‌ها، استفاده می‌شود. محتوای جمع‌آوری شده توسط خزنده وب پس از آن توسط موتور جستجو بر اساس عوامل مختلف ذخیره می‌شود. صفحات بر اساس ساختار آن‌ها (کلمات کلیدی مورد استفاده، پیوند صفحات، رسانه‌ها موجود در صفحه و بسیاری دیگر از جزئیات) رتبه‌بندی می‌شوند. هنگامی که صفحه جمع‌آوری و نمایه شد، آماده ارائه به کاربر بر اساس پرس‌وجو از موتور جستجو است.

گوگل

گوگل یکی از موتورهای جستجوی پیشرفته است و برای اکثر ما، نقطه شروع اکتشاف وب است. جستجوی گوگل از طریق رابط کاربری بسیار ساده و قابل دسترس آن است که نه تنها رابط کاربری آن در طول سال‌ها تغییر کرده، بلکه ویژگی‌ها آن نیز دستخوش تغییراتی شده است. این ابزار لینک‌های ساده تا صفحات حاوی اطلاعات مربوط به ابزارهای مرتبط را ارائه می‌دهد که نه تنها به ما اجازه می‌دهد انواع مختلف رسانه‌ها را جستجو کنیم، بلکه این نتایج را با استفاده از ابزارهای مختلف محدود می‌کنیم. امروزه دسته‌های مختلفی از جستجو مانند تصاویر، اخبار، نقشه‌ها، فیلم‌ها و خیلی چیزهای دیگر وجود دارد. امروزه این فراوانی ویژگی‌های ارائه شده از سوی گوگل قطعاً زندگی ما را بسیار ساده‌تر ساخته و باعث می‌شود اطلاعات مربوط به سادگی پیدا شود. گاهی اوقات ما دچار اشکال در پیدا کردن اطلاعات دقیق می‌شویم و دلیل اصلی آن کمبود اطلاعات نیست، بلکه بر عکس فراوانی آن است.

بیایید نحوه انجام جستجوی گوگل و بهبود آن را بینیم؛ هر زمانی که بخواهیم چیزی را در گوگل جستجو کنیم، به سادگی برخی از کلمات کلیدی مرتبط با آن را در نوار جستجو تایپ می‌کنیم و اینتر را فشار می‌دهیم. بر اساس فهرست بندی گوگل به سادگی منابع مرتبط فراهم می‌شود. همچنین می‌توانیم نتایج موجود را بر اساس عوامل

^۱ crawler

مختلف فیلتر کنیم، باید از اپراتورهای جستجوی پیشرفته گوگل استفاده کنیم. بیایید به این اپراتورها و استفاده از آن‌ها نگاه کیم.

site

نتایج فقط برای سایت مشخص شده ارائه می‌شود. زمانی که جستجو را به یک دامنه خاص محدود کنیم بسیار مفید است. این کار را می‌توان با کلمه کلیدی دیگری نیز کرد و گوگل صفحات مربوطه را از سایت مشخص جستجو می‌کند. بسیار مفید است که دامنه‌های مختلف یک دامنه خاص را پیدا کنید.

مثال: site:gov, site:house.gov

The screenshot shows a Google search results page with the query 'site:house.gov'. The results are filtered under the 'All' tab. The first result is 'Congressman John Carter : Home' with a link to <https://carter.house.gov/>. The second result is 'U.S. Representative Morgan Griffith' with a link to <https://morgangriffith.house.gov/>. The third result is 'U.S. Congresswoman Gwen Moore' with a link to <https://gwenmoore.house.gov/>. The fourth result is 'Congressman Dave Loebsack' with a link to <https://loebsack.house.gov/>.

inurl

این اپراتور اجازه می‌دهد تا به دنبال کلمات کلیدی در^۱ URL پردازید. برای پیدا کردن صفحات دارای یک کلمه کلیدی برای صفحات خاص هستند، مانند "تماس با ما" مفید است. به طور کلی، URL‌ها شامل برخی از کلمات کلیدی مرتبط با محتوای بدنه صفحه هستند و به ما کمک می‌کند تا صفحه معادل برای کلیدواژه را پیدا کنیم.

مثال: inurl: hack

allinurl

^۱ uniform resource locator

همانند `inurl` این اپراتور اجازه می‌دهد تا کلمات کلیدی مختلف را در URL جستجو کنیم؛ با این تفاوت که می‌توانیم کلمات کلیدی چندگانه را در URL یک صفحه جستجو کنیم. این کار شانس گرفتن محتوای کافی از آنچه دنبال آن هستیم را افزایش می‌یابد.

مثال: `allinurl: hack security`

intext

این اپراتور اطمینان می‌دهد که کلیدواژه مشخص شده در متن صفحه وجود دارد. گاهی اوقات به خاطر SEO برخی از صفحات پیدا شده که تنها شامل کلمات کلیدی برای افزایش رتبه صفحه بوده ولی محتوای مرتبط با آن را ندارد. در این صورت می‌توانیم از این پارامتر پرس و جو برای دریافت محتوای مناسب از یک صفحه برای کلمه کلیدی که دنبال آن هستیم، استفاده کنیم.

مثال: `intext: hack`

allintext

همانند `intext`، این اپراتور اجازه می‌دهد تا کلمات کلیدی چندگانه را در متن جستجو کنیم. همان‌طور که قبلاً اشاره کردیم، جستجوی کلمات کلیدی چندگانه همواره کیفیت محتوا را در صفحه نتیجه افزایش می‌دهد.

مثال: `allintext: data marketing`

intitle

به ما اجازه می‌دهد که نتایج را با کلمات کلیدی موجود در عنوان صفحات (برچسب عنوان: `<title>XYZ</title>`) محدود کنیم؛ بنابراین این پارامتر پرس و جو همیشه به جستجوی یک کلمه کلیدی خاص کمک می‌کند.

مثال: `intitle: blueocean`

allintitle

این علامت اپراتور چندگانه `intitle` است.

مثال: `allintitle: blueocean market`

filetype

این اپراتور برای پیدا کردن فایلی از یک نوع خاص استفاده می‌شود. از انواع فایل‌هایی مانند doc, kml, swf, pdf و غیره پشتیبانی می‌کند. این اپراتور زمانی مفید است که فقط به دنبال نوع خاصی از فایل‌ها در یک دامنه خاص هستیم.

مثال: filetype:pdf, site:xyz.com, filetype:doc

ext

اپراتور ext برای جستجوی پسوند استفاده می‌شود و کار مشابهی با اپراتور filetype دارد.

مثال: ext: pdf

define

این اپراتور برای پیدا کردن معنی کلمه استفاده می‌شود. گوگل معنی و مفهوم را برای کلمه کلیدی ارائه می‌کند.

مثال: define: data

AROUND

این اپراتور زمانی مفید است که به دنبال نتایجی که حاوی دو کلمه کلیدی مختلف اما در ارتباط نزدیک هستند، باشیم. همچنین اجازه می‌دهد تا تعداد کلمات را به عنوان حداقل فاصله بین دو کلمه کلیدی مختلف در نتایج جستجو محدود کنیم.

مثال: A AROUND(6) Z

AND

یک عملگر بولی ساده که باعث می‌شود کلمات کلیدی در هر دو طرف در نتایج جستجو حضور داشته باشند.

مثال: data AND market

OR

یکی دیگر از اپراتورهای بولی که نتایج جستجویی را ارائه داده که شامل هر یک از کلمات کلیدی موجود در هر دو طرف اپراتور است.

مثال: data OR intelligence

NOT

یکی دیگر از اپراتورهای بولی است که نتایج جستجویی را که شامل کلیدواژه‌ای است، حذف می‌کند.

مثال: lotus NOTflower

” ”

این اپراتور وقتی که ما نیاز به جستجو برای نتایجی که حاوی دقیق کلیدواژه ارائه شده باشد، مفید است.

مثال: Example: "Time is precious"

-

این اپراتور نتایج جستجو را که شامل کلیدواژه‌ای است پس از آن است (بدون فضای) حذف می‌کند.

مثال: lotus –flower

*

این اپراتور به عنوان یک کلمه نامشخص استفاده می‌شود. ما می‌توانیم از آن برای به دست آوردن آنچه بخشی از آن را به خاطر نمی‌آوریم و یا برای بررسی انواع، استفاده کنیم.

مثال: * is precious

..

این اپراتور ویژه برای ارائه محدوده مورد استفاده قرار می‌گیرد. برای تعیین محدوده قیمت، زمان (تاریخ) و غیره بسیار کاربردی است.

مثال: japan volcano 1990..2000

info

اپراتور اطلاعاتی را درباره یک دامنه خاص ارائه می‌دهد. لینک‌هایی به انواع مختلف اطلاعات، مانند وبسایت‌های مشابه و غیره وجود دارد.

مثال: info:elsevier.com

related

این اپراتور برای پیدا کردن صفحات شبیه دامنه ارائه شده به کار می‌رود. هنگامی که به دنبال وب‌سایت‌هایی هستیم که خدمات مشابهی یک وب‌سایت را می‌دهد و یا برای پیدا کردن رقبای آن بسیار مفید است.

مثال: related:elsevier.com

cache

این اپراتور به آخرین حافظه پنهانی صفحه که گوگل آن را جستجو کرده است، هدایت می‌کند. در صورتی که برای یک وب‌سایت که قبلاً در دسترس بود نتیجه‌ای نباشد، این گزینه‌ای مناسب برای آزمایش است.

مثال: cache:elsevier.com

جستجوی پیشرفته گوگل نیز می‌تواند با استفاده از صفحه http://www.google.com/advanced_search انجام شود که به ما اجازه می‌دهد جستجو را با استفاده از اپراتورهای ذکر شده در بالا انجام دهیم.

The screenshot shows the Google Advanced Search interface. In the search bar, the URL is https://www.google.com/advanced_search. The search term 'rat' is entered in the main search input field. To the right, there are several sections with instructions and examples:

- Find pages with...**:
 - this exact word or phrase:** Put exact words in quotes: "rat terrier"
 - any of these words:** Type OR between all the words you want: miniature OR standard
 - none of these words:** Put a minus sign just before words that you don't want: -zodiac, -"Jack Russell"
 - numbers ranging from:** to Put two full stops between the numbers and add a unit of measurement: 10..35 kg, £300..£600, 2010..2011
- Then narrow your results by...**:
 - language:** any language Find pages in the language that you select.
 - region:** any region Find pages published in a particular region.
 - last update:** anytime Find pages updated within the time that you specify.
 - site or domain:** Search one site (like wikipedia.org) or limit your results to a domain

به غیر از اپراتورها، گوگل برخی از عملیات را ارائه می‌کند که به ما اجازه می‌دهد اطلاعات مربوط به رویدادهای فعلی را بررسی و همچنین برخی از چیزهای مفید دیگر را انجام دهیم. برخی از نمونه‌ها عبارت‌اند از:

time

به سادگی با وارد کردن این کلیدواژه، زمان فعلی محل اقامت ما را نشان می‌دهد. همچنین می‌توانیم از نام منطقه برای دریافت زمان فعلی خود استفاده کنیم.

مثال: time france

weather

این کلمه کلیدی شرایط آب‌وهوایی فعلی مکان ما را نشان می‌دهد. همانند کلمه کلیدی "time" می‌توانیم آن را نیز برای استفاده از شرایط آب‌وهوایی منطقه متفاوت استفاده کنیم.

مثال: weather Sweden

Calculator

گوگل همچنین معادلات ریاضی را حل می‌کند و همچنین ماشین حساب را فراهم می‌کند.

مثال: ۳/۴۴+۹۸۲۳*(۳۱۲-۳۹)

Convertor

گوگل می‌تواند برای تبدیل واحدهای مختلف مانند اندازه‌گیری، ارز، زمان و غیره مورد استفاده قرار گیرد.

مثال: 6 feet in meters

گاهی اوقات گوگل اطلاعات مربوط به رویدادهای جهانی را نیز همان‌طور که در زمان اتفاق می‌افتد نشان می‌دهد. برای مثال جام جهانی فیفا (FIFA World Cup).

همچنین به غیر از جستجو در وب، گوگل به ما اجازه می‌دهد که دسته‌های خاصی مانند تصاویر، اخبار، فیلم‌ها و غیره را جستجو کنیم. همه این دسته‌ها، مانند وب، دارای برخی از فیلترینگ‌های خاص خود هستند. این گزینه‌ها به سادگی می‌توانند با کلیک بر روی زبانه "Search tools" در زیر نوار جستجو قابل دسترسی باشد. ما می‌توانیم گزینه‌هایی را انتخاب کنیم که به ما امکان محدود کردن نتایج بر اساس کشور و زمان انتشار در وب را می‌دهد. برای تصاویر گزینه‌هایی مانند رنگ تصویر، نوع، حقوق استفاده کننده و غیره وجود دارد و به همین ترتیب فیلترهای مرتبط دیگری برای دسته‌های مختلف وجود دارد. این گزینه‌ها می‌توانند در پیدا کردن اطلاعات موردنیاز

یک دسته بسیار مفید باشند زیرا آن‌ها برای آن دسته خاص طراحی شده‌اند. به عنوان مثال اگر ما به دنبال یک عکس قدیمی از چیزی هستیم، ایده خوبی است که فقط نتایج سیاه و سفید را بینیم.

اپراتورهای مورد بحث ما قطعاً برای هر کس که نیاز به پیدا کردن اطلاعاتی در وب است بسیار مفید خواهد بود. این اپراتورهای ساده که مورد بحث قرار گرفته‌اند، به‌طور گسترده در امنیت سایبر استفاده می‌شوند تا بتوانند بدون کوچک‌ترین تماس با سیستم هدف، اطلاعات قابل ملاحظه و خطرناک را بازیابی کنند. این تکنیک استفاده از اپراتورهای موتور جستجوی گوگل برای پیدا کردن چنین اطلاعاتی گوگل هکینگ^۱ نامیده می‌شود.

هنگامی که نام گوگل هکینگ می‌آید، نام جانی لانگ به ذهن خطور می‌کند. جانی یکی از پیشگامان در زمینه ایجاد چنین عبارات جستجوی گوگل بود که می‌تواند اطلاعات حساس مربوط به هدف را فراهم کند. این عبارات به نام گوگل دورک^۲ محبوبیت زیادی دارند.

تعدادی از اپراتورها را مشاهده کردیم که می‌توانند نتایج جستجو را محدود به یک دامنه خاص، نوع فایل، مقدار عنوان و غیره کنند. در حال حاضر در گوگل هکینگ انگیزه ما یافتن اطلاعات حساس مربوط به هدف است؛ به عنوان مثال، اجازه بدھید بگوییم نام یک پوشه حساس را می‌دانیم که نباید به صورت عمومی به‌طور مستقیم برای هر کاربر در دسترس باشد، اما پس از نصب برنامه مربوطه، به‌طور پیش فرض عمومی می‌باشد؛ بنابراین اگر می‌خواهیم سایتها را پیدا کنیم که قابلیت دسترسی این دایرکتوری را تغییر نداده‌اند، می‌توانیم به‌سادگی از "inurl:/sensitive_directory_name/" استفاده کنیم و تعداد زیادی وب‌سایت را که تنظیمات را تغییر نداده‌اند، دریافت می‌کنیم. حالا اگر می‌خواهیم به وب‌سایت خاصی محدود شویم، می‌توانیم پرس‌وجو را با "site" به صورت "site:targetdomain.com inurl:/sensitive_directory_name/" ترکیب کنیم. به همین ترتیب می‌توانیم فیلد‌های حساس را نیز با استفاده از اپراتورها "site" و "filetype" پیدا کنیم.

بیاید مثال دیگری از گوگل هکینگ بینیم که می‌تواند ما را در کشف آسیب‌پذیری با ریسک بالا در وب‌سایت‌ها کمک کند. بسیاری از توسعه‌دهندگان وب‌سایت‌ها برای ایجاد ویژگی تعاملی و بصری جذاب از فرم‌فلش استفاده می‌کنند. فرم‌فلش برای ایجاد چندرسانه‌ای استفاده می‌شود. در حال حاضر بسیاری از SWF‌ها وجود دارند که به اسکریپت cross-site آسیب‌پذیرند (XSS). اگر می‌خواهیم بدانیم که آیا دامنه مورد نظر به چنین حمله آسیب‌پذیر است، می‌توانیم به‌سادگی از query "site: targetdomain.com filetype: swf" است، می‌توانیم به‌سادگی آسیب‌پذیر

¹ Google Hacking

² Google Dorks

استفاده کنیم. تعداد زیادی از عبارات جستجو برای پیدا کردن انواع مختلف صفحات مانند دایرکتوری حساس، شناسایی وب سرور، فایلی حاوی نام کاربری / رمز عبور، صفحات ورود سیستم مدیریت و غیره وجود دارد.

پایگاه داده گوگل هکینگ ایجاد شده توسط جانی لانگ در آدرس <http://www.hackersforcharity.org/ghdb/> یافت می‌شود. هرچند که به روز نمی‌شود، اما مکان بسیار خوبی برای فهم و یادگیری نحوه استفاده از گوگل برای یافتن اطلاعات حساس است. نسخه به روز شده در <http://www.exploit-db.com/google-dorks/> یافت می‌شود.

Date Added	Dork	Category	Author
2019-04-12	intext:[To Parent Directory] & ext:sql ext:cnf ext:config ext:log	Files Containing Juicy Info	Miguel Santareno
2019-04-12	ext:txt ext:sql ext:cnf ext:config ext:log & intext:"admin" intext:"root" intext:"administrator" & intext:"password" intext:"root" intext:"admin" intext:"administrator"	Files Containing Juicy Info	Miguel Santareno
2019-04-12	inurl:/pages/default.aspx inurl:/páginas/default.aspx	Various Online Devices	Miguel Santareno
2019-04-11	site:www.openbugbounty.org + intext:"Open Redirect" + intext:"Unpatched"	Advisories and Vulnerabilities	botsec0
2019-04-11	"Powered by ViewVC 1.0.3"	Various Online Devices	CrimsonTorso
2019-04-11	"/var/cache/registry/"	Sensitive Directories	deadroot
2019-04-10	inurl:_vti_bin/sites.asmx?wsdl intitle:_vti_bin/sites.asmx?wsdl	Files Containing Juicy Info	Miguel Santareno
2019-04-10	type:mil inurl:ftp ext:pdf ps	Sensitive Directories	botsec0
2019-04-10	site:com inurl:b2blogin ext:cfrm jsp php aspx	Pages Containing Login Portals	botsec0

بینگ

مایکروسافت مدت‌هاست که از موتورهای جستجوگر استفاده می‌کند که با نام‌های مختلف شناخته شده‌اند. بینگ آخرین موتور جستجوگر قدرتمند در این مجموعه است. برخلاف موتورهای قبلی، بینگ رابط کاربری ساده‌ای را فراهم می‌کند. همان‌گونه که مایکروسافت قسمت عمدۀ ای از بازار سیستم‌عامل را پوشش می‌دهد، چشم‌انداز کلی یک کاربر از لحاظ موتور جستجو این است که بینگ فقط یک محصول جانبی از یک غول تکنولوژی است و از این رو اکثر آن‌ها جدی نمی‌گیرند؛ اما متأسفانه اشتباه است. همانند تمام موتورهای جستجو، بینگ دارای برخی از ویژگی‌های منحصر به فرد است که شما را مجبور به استفاده از آن هنگامی که به آن ویژگی‌ها نیاز دارید، می‌کند. قطعاً این ویژگی‌ها، تأثیر زیادی در مورد نحوه جستجوی ما دارند. ما نه تنها درباره ویژگی‌های خاص

صحبت خواهیم کرد بلکه اپراتورهای عمومی که می‌توانند به ما در درک موتور جستجو و قابلیت‌های آن داشته باشند، می‌پردازیم.

+

این اپراتور در تمام موتورهای جستجو کاملاً مشابه است و اجازه می‌دهد تا یک یا چند کلمه کلیدی در یک پرس‌وجو جستجو استفاده شود. بینگ اطمینان حاصل خواهد کرد که کلمات کلیدی بعد از عملگر + باید در صفحات نتیجه ارائه شوند.

مثال: power + search

-

این اپراتور همچنین به عنوان عامل غیر شناخته می‌شود. این مورد برای رد کردن چیزی از مجموعه‌ای از چیزها، مانند حذف یک غذا استفاده می‌شود.

مثال: Italian food -pizza

در اینجا Bing همه غذاهای ایتالیایی را در دسترس قرار می‌دهد، اما نه پیتزا. ما می‌توانیم آن را در فرم دیگری بنویسیم که همچنین می‌تواند نتایج مشابهی را مانند مثال زیر به دست آورد.

مثال: Italian food NOT pizza

“”

این نیز در بسیاری از موتورهای جستجو مشابه است و برای جستجوی دقیق عبارت مورد استفاده در داخل نقل قول استفاده می‌شود.

مثال: “How to do Power Searching?”

|

این همچنین به عنوان OR عمل می‌کند که عمدتاً برای رسیدن به نتیجه از دو یا یکی از کلمات کلیدی اضافه شده با این اپراتور استفاده می‌شود.

ios OR android

مثال: ios | android

&

این اپراتور همچنین به عنوان عملگر AND شناخته می‌شود. این اپراتور پیش فرض است. اگر ما هیچ کاری انجام ندهیم و کلمات کلیدی چندگانه اضافه می‌کنیم، Bing جستجو را با استفاده از آن انجام داده و نتیجه را به ما می‌دهد.

مثال: power & search power AND search

همان‌طور که این عملگر پیش فرض است، بسیار مهم است که به یاد داشته باشیم که تا زمانی که از OR یا NOT در استفاده نکنیم، بینگ از آن‌ها استفاده نخواهد کرد.

0

این را می‌توان به عنوان اپراتور گروه نامید.

همان‌طور که پرانتز دارای ترتیب اول است، ما می‌توانیم اپراتورهای ترجیح داده شده مانند OR را در آن اضافه کنیم و یک پرس‌وجو گروهی ایجاد کنیم تا اپراتورهای اولویت پایین‌تر را اجرا کنیم.

مثال: android phone AND (nexus OR xperia)

site

این اپراتور به جستجوی یک کلمه کلیدی در یک وب‌سایت خاص کمک خواهد کرد. این اپراتور در اکثر موتورهای جستجو کاملاً مشابه است.

مثال: site: owasp.org clickjacking

filetype

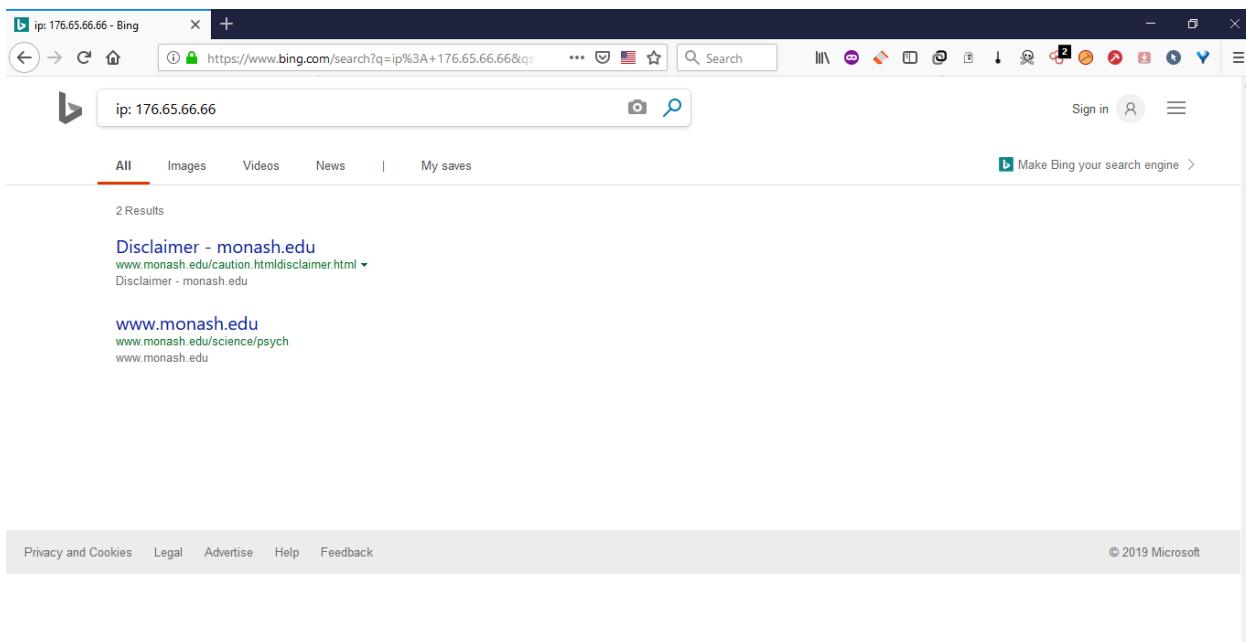
این اپراتور اجازه می‌دهد تا یک کاربر به جستجو نوع خاصی از فایل پردازد. بینگ از تمام انواع فایل‌ها پشتیبانی می‌کند.

مثال: hack filetype:pdf

ip

این اپراتور منحصر به فرد ارائه شده توسط بینگ به ما اجازه می‌دهد که صفحات وب را بر اساس آدرس IP جستجو کنیم. با استفاده از آن می‌توانیم جستجو IP معکوس را انجام دهیم، به این معنی که به ما اجازه می‌دهد که صفحاتی را که در IP خاص مشخص شده‌اند، جستجو کنیم.

مثال: ip: 176.65.66.66



feed

اپراتوری منحصر به فرد دیگر که توسط بینگ ارائه شده است، feed است که به ما اجازه می‌دهد تا صفحات وب حاوی کلیدواژه ارائه شده را جستجو کنیم.

یکی دیگر از ویژگی‌های که بینگ فراهم می‌کند، انجام جستجوی شبکه‌های اجتماعی با استفاده از صفحه feed است. <https://www.bing.com/explore/social>.

یاهو

یاهو یکی از قدیمی‌ترین موتورها در عرصه جستجو و بسیار محبوب است. صفحه جستجو یاهو دارای محتوای زیادی نظری اخبار، موضوعات مورد علاقه، آب و هوا، اطلاعات مالی و غیره است. اگر چه یاهو از لحاظ جستجوی پیشرفته در مقایسه با سایر موتورهای جستجو چندان پیشرفته نیست، اما آنچه ارائه شده، ارزش تلاش در مقایسه با دیگر موتورها را دارد. باید برخی از اپراتورهای مفید را بینیم.

این اپراتور برای اطمینان از اینکه نتایج جستجو شامل کلیدواژه‌ای است که بعد از آن استفاده می‌شود استفاده می‌شود.

مثال: data+

در مقابل اپراتور "+"، این اپراتور برای حذف هر کلمه کلیدی خاص از نتایج جستجو استفاده می‌شود.

مثال: info-

site

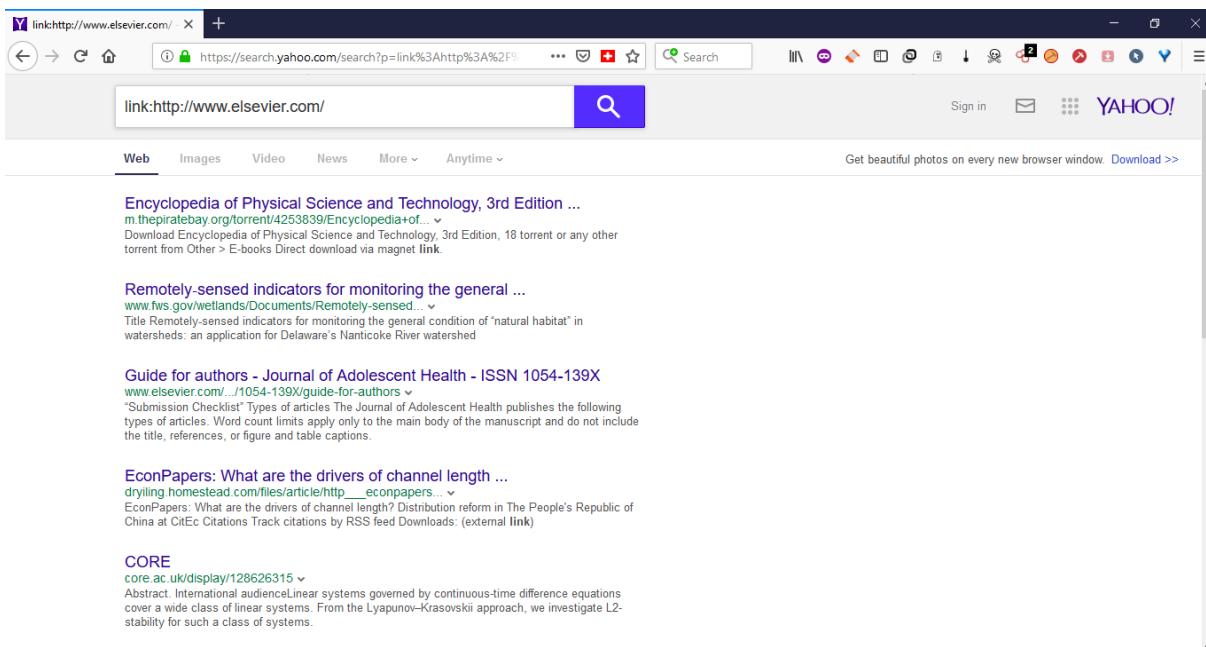
این اپراتور اجازه می‌دهد تا نتیجه را تنها به سایت ارائه شده محدود کنیم. ما می‌توانیم لینک‌هایی از وبسایت مشخص شده را مشاهده کنیم. دو اپراتور دیگر وجود دارد که مانند این اپراتور کار می‌کنند، اما نتایج دقیق و عمیق را به عنوان دامنه و نام میزبان ارائه نمی‌کنند. استفاده آن‌ها شبیه اپراتور "site" است.

مثال: site: elsevier.com

link

این اپراتور جالب است که اجازه می‌دهد تا به جستجوی صفحات وی‌بی که به صفحه خاص وب مرتبط هستند، پردازیم. با استفاده از این اپراتور، باید URL را با پروتکل `http://` و یا `https://` ارائه دهید.

مثال: link: <http://www.elsevier.com/>



define

ما می‌توانیم از این اپراتور برای پیدا کردن معانی لغات استفاده کنیم.

مثال: define:data

intitle

اپراتور برای به دست آوردن نتایجی که حاوی کلیدواژه خاص در برچسب عنوان هستند، استفاده می‌شود.

مثال: inttitle: data

به غیر از آن‌ها می‌توان به صفحه جستجو پیش‌رفته یاهو در <http://search.yahoo.com/search/options?fr=fp-top&p=> دسترسی پیدا کرد که به ما اجازه می‌دهد نتایج جستجوی خوبی را به دست آوریم. یکی دیگر از مواردی که یاهو ارائه می‌دهد جستجوی پیش‌رفته اخبار است که می‌تواند با استفاده از صفحه [انجام شود](http://news.search.yahoo.com/advanced).

The screenshot shows the Yahoo! Advanced Web Search interface at <https://news.search.yahoo.com/advanced>. The search bar contains the query 'Yandex'. The results page displays several search results from the Yahoo! News section, including links to 'Yahoo Search - Web Search', 'Yahoo Advanced Web Search', 'Yahoo News - Latest News & Headlines', and 'Yahoo Search - Web Search - Yahoo! News'. Below the search results, there is a section titled 'Http://news.search.yahoo.com/advanced - Video Results' which shows thumbnails of video clips related to Yandex.

یاندکس^۱

یاندکس موتور جستجوی روسیه است و در خارج از آن کشور محبوب نیست، اما یکی از قدرتمندترین موتورهای جستجو در دسترس است؛ مانند گوگل، بینگ، یاهو دارای کلمات کلیدی و داده‌های منحصر به فرد خود است. یاندکس محبوب‌ترین و گسترده‌ترین موتور جستجو در روسیه است. این موتور چهارمین موتور جستجو بزرگ در جهان است. به غیر از روسیه، در کشورهایی مانند اوکراین، قزاقستان، ترکیه و بلاروس نیز استفاده می‌شود. این امتیاز موتور جستجو است که استفاده از آن تنها به کشور خاص محدود می‌شود، اما در جامعه امنیتی ما آن را در نظر می‌گیریم. اکثر مردم با موتور جستجوی معمولی خود را خوشحال می‌کنند و یا فکر می‌کنند که همه اطلاعات اینترنت با استفاده از موتور جستجوی آنها به دست می‌آید؛ اما واقعیت این است که موتورهای جستجو مانند یاندکس دارای ویژگی‌های منحصر به فردی هستند که می‌توانند یک نتیجه کارآمد را در مقایسه با دیگر موتورهای جستجو ارائه دهند. در اینجا ما بحث خواهیم کرد که چگونه یاندکس می‌تواند در جستجوی داده‌ها در اینترنت و نحوه استفاده از آن به طور مؤثر باشد.

همان‌طور که قبل مانند موتورهای جستجو دیگر مورد بحث قرار گرفت، یاندکس اپراتورهای خود را دارد. بیایید با این اپراتورها و استفاده از آنها آشنا شویم.

¹ YANDEX

این اپراتور در تمام موتورهای جستجو عمل کاملاً مشابه انجام می‌دهد. در اینجا نیز اپراتور + برای شامل شدن کلمه کلیدی در صفحه نتایج جستجو استفاده می‌شود. کلمه کلیدی اضافه شده بعد از عملگر + کلمه اصلی در پرس‌وجو جستجو است. نتیجه موتور جستجو گر باید حاوی کلمه کلیدی باشد.

مثال: osint +tools

در اینجا صفحه نتیجه ممکن است کلمه کلیدی OSINT را نداشته باشد، اما باید شامل کلمه tools باشد؛ بنابراین، هنگامی که می‌خواهیم بر یک کلمه کلیدی خاص یا مجموعه‌ای از کلمات کلیدی در یاندکس تمرکز کنیم، باید از عملگر + استفاده کنیم.

~~

به عنوان اپراتور NOT استفاده می‌شود که برای حذف یک کلمه کلیدی از صفحه نتایج جستجو استفاده می‌شود. این می‌تواند در کنار گذاشتن یک‌چیز خاص از مجموعه‌ای از چیزها استفاده شود. مثلاً می‌خواهیم تلفن همراه خریداری کنیم، اما نه تلفن ویندوزی.

مثال: mobile phone ~~ windows

~

برخلاف ~~ که کلمات کلیدی را از صفحه نتایج جستجو حذف می‌کند، نتیجه جستجو را در صورت هم‌جوار بودن در یک جمله حذف می‌کند. این بدان معنی است که ممکن است همه کلمات کلیدی موجود در یک پرس‌وجو را در یک صفحه داشته باشیم، اما کلمه‌ای محروم شده باید در یک جمله با کلمات کلیدی دیگر ذکر شده باشند. این کمی پیچیده است بنابراین اجازه دهید به سادگی توضیح دهیم. بیایید با پرس‌وجوی بالا شروع کنیم:

mobile phone ~~ windows

در اینجا اگر صفحه حاوی هم تلفن همراه و همچنین ویندوز باشد، یاندکس این صفحه را از نتیجه جستجو حذف خواهد کرد.

مثال: mobile phone ~ windows

اما برای مثال بالا، تمام صفحاتی که حاوی تلفن همراه و همچنین ویندوز است اگر در جمله یکسان باشند، نشان داده نمی‌شود.

&&

اپراتور && برای نشان دادن صفحات حاوی هر دو کلیدواژه در نتیجه جستجو استفاده می‌شود.

مثال: power && searching

این نتایج تمام صفحاتی را که حاوی هر دو این کلمات کلیدی هستند ارائه خواهد داد.

&

این اپراتور برای نمایش صفحات حاوی کلمات کلیدی در یک جمله بکار برد می‌شود. این جستجو نتایج بیشتری برای هر دو کلیدواژه فراهم می‌کند.

مثال: power & searching

/number

این یک اپراتور ویژه است که می‌تواند برای مقاصد مختلف بر اساس تعداد استفاده شده پس از / استفاده شود. این کار برای تعریف نزدیکی کلمات کلیدی استفاده می‌شود و کاملاً شبیه به اپراتور AROUND گوگل و اپراتور NEAR بینگ است. شماره‌ای که با / استفاده می‌شود، فاصله را بین دو کلمه کلیدی تعریف می‌کند.

مثال: power /4 searching

یاندکس اطمینان حاصل خواهد کرد که صرف نظر از موقعیت کلمه کلیدی، صفحه نتایج باید دارای دو کلمه کلیدی با چهار حرف فاصله از یکدیگر باشد. این بدان معناست که منظور پرس‌وجو با کلمات کلیدی ممکن است در صفحه نتیجه تغییر کند.

اگر نیاز داریم که جهت کلمات نیز در نظر گرفته شود، چه کار کنیم؟ اضافه کردن علامت + با عدد.

مثال: power / + 4 search

فقط صفحاتی که این دو کلمه کلیدی با فاصله ۴ کلمه‌ای در یک جهت وجود دارد را نشان می‌دهد.

اگر به معکوس آن نیاز داریم، مثلاً باید نتایج کلیدواژه "search" را اول و بعد از آن "power" با فاصله ۴ کلمه‌ای باشد و نه برعکس. در آن صورت - بسیار مفید خواهد بود که می‌توانیم استفاده کنیم. - برای معکوس کردن آنچه ما انجام دادیم بکار برد همی شود.

مثال: power /-4 searching

تنها صفحه‌هایی را نشان می‌دهد که در آن به ترتیب کلمات کلیدی searching و power با تعداد ۴ کلمه فاصله هستند.

به عنوان مثال می‌خواهیم یک مرز را برای یک کلمه کلیدی در رابطه با دیگری تنظیم کنیم؛ در این مورد باید کلیدواژه را در موقعیت دوم مشخص کنیم.

مثال: power /(-3 +4) searching

در اینجا ما یک مرز برای جستجو در رابطه با "power" ایجاد می‌کنیم. این به این معنی است که صفحه‌ای در نتایج نمایش داده می‌شود اگر "searching" در ۳ کلمه قبل یا ۴ کلمه بعد از "power" باشد.

زمانی که ما در جستجوی نام دو نفر هستیم، این می‌تواند مفید باشد. در صورتی که نمی‌توانیم حدس بزنیم چه نامی برای اولین بار وارد خواهد شد و کدام نام بعدی از آن خواهد آمد؛ بنابراین بهتر است شعاعی برای این دو نام ایجاد شود و پرس و جو به هدف ما خواهد رسید.

همان‌طور که در مورد جستجوی بر اساس کلمات بحث کردیم، اکنون اجازه دهید تا برخی از نکات را در جستجوی جمله ذکر کنیم. برای جستجوی کلمات کلیدی بر اساس جمله، می‌توانیم اپراتور && را با اپراتور شماره استفاده کنیم.

مثال: power && /4 searching

در این مورد می‌توانیم نتایج صفحات حاوی این دو کلمه کلیدی با ۴ جمله تفاوت، بدون در نظر گرفتن موقعیت کلمه کلیدی به دست آوریم. این بدان معنی است که "power" ممکن است اول باشد و "searching" پس از آن یا برعکس.

!

این اپراتور کاری ویژه‌ای انجام می‌دهد و یکی از کلمات کلیدی مورد علاقه ما است. به کاربر اجازه می‌دهد تا فقط یک کلیدواژه خاص را بدون جستجوی همه موارد مشابه جستجو کند. آنچه دقیقاً در جستجوی عموم اتفاق می‌افتد این است که شما یک کلمه کلیدی را جستجو کنید، مثلاً، شما AND را جستجو می‌کنید و ابتدا نتایج AND خواهد آمد و سپس به AMD و غیره گسترش خواهد یافت. اگر بخواهیم فقط نتیجه را برای کلیدواژه‌ی AND داشته باشیم، از این اپراتور استفاده کنید.

مثال: !and

این کلمه موتور جستجو را محدود می‌کند تا صفحاتی که حاوی این کلیدواژه AND هستند را فقط نشان دهد.

!!

این می‌تواند برای جستجوی فرهنگ لغت کلمه کلیدی مورد استفاده قرار گیرد.

مثال!!: and!!

()

وقتی می‌خواهیم یک پرس‌وجو پیچیده با کلمات کلیدی و اپراتورهای مختلف ایجاد کنیم، می‌توانیم از پرانتز برای گروه‌بندی استفاده کنیم. همان‌طور که قبل از این پرانتزا استفاده کردیم، اکنون شاهد مثال دیگری برای درک قدرت واقعی آن هستیم.

مثال: power && (+searching | !search)

Yandex [power && (+searching | Isearch)] Registration Log in

Web Images Video News Translate Disk Mail Ad

2 million results found

- Power Searching with Google - Course** coursebuilder.withgoogle.com + Power Searching with Google. Google Search makes it amazingly easy to find information. Come learn about the powerful advanced tools we provide to help you find...
- Free power search tool that allows you to search your...** power-search.net + Power-Search.net is an online tool that allows searching in multiple search engines, simultaneously. By using this website you can easily perform searches in major search...
- Power Search - Скачать на ПК бесплатно** malavida.com + 9/10 - Скачать Power Search бесплатно. ... Power Search. PowerSearch это мощный поиск, способный находить файлы в скрытых файлах в большом количестве...
- Power Search by Inspyder - Search and Scrape Any Website** inspyder.com + Power Search enables you to quickly search a website for content that is not normally indexed by search engines. Searching within a website's HTML code, Power Search...
- 96. Google Power Searching Techniques - YouTube** youtube.com + Power searching: Advanced Google search for education - Продолжительность: 1:36:24 Google Videos 12 108 просмотров.

””

اکنون می‌خواهیم یک رشته خاص یا مجموعه‌ای از کلمات کلیدی را جستجو کنیم، چه کاری باید انجام دهیم؟ در اینجا اپراتور "" مورد استفاده قرار می‌گیرد که کاملاً شبیه به گوگل است. این به کاربر اجازه می‌دهد که دقیقاً کلمات کلیدی را که در داخل آن قرار دارد، جستجو کند.

مثال: "What is OSINT"

برای رشته کلمات به صورت دقیق جستجو می‌کند و اگر در دسترس باشد، نتیجه را به ما می‌دهد.

*

این اپراتور را می‌توان به جای هر کلمه‌ای استفاده کرد. استفاده از این اپراتور در اکثر موتورهای جستجو کاملاً مشابه است. این اپراتور برای کلمه گم شده یا پیشنهاد کلمات کلیدی مرتبط با کلمات کلیدی دیگر مورد استفاده در جستجو استفاده می‌شود.

مثال: osint is * of technology

از آن برای تکمیل پرس‌وجو با کلمات کلیدی مرتبط استفاده می‌شود. در این مورد می‌تواند هر چیزی باشد. ما همچنین می‌توانیم از این اپراتور با نقل قول دوگانه استفاده کنیم تا نتایج کارآمدتر و دقیق‌تر به دست آید.

مثال: "OSINT is * of technology"

این نیز کاملاً مشابه اپراتور OR گوگل است و اجازه می‌دهد تا برای کلمات کلیدی مختلفی که می‌خواهیم نتایج برای هر یک از آن‌ها داشته باشیم، جستجو کنیم. مثلاً من می‌خواهم یک لپ‌تاپ بخرم و گزینه‌های مختلفی دارم:

مثال: dell | toshiba | macboo

در اینجا می‌توان نتیجه را برای هر یک از این سه گزینه به دست آورد، اما همه در یک نتیجه نیست.

<>

این یک اپراتور غیرمعمول است که به عنوان AND بدون رتبه‌بندی شناخته می‌شود. این اپراتور اساساً برای اضافه کردن کلمات کلیدی اضافی به لیست کلمات کلیدی بدون تأثیر بر رتبه‌بندی وب‌سایت‌ها در نتیجه استفاده می‌شود؛ بنابراین در کلمات ساده می‌توان آن را برای تگ کردن کلمات کلیدی اضافی به لیست پرس‌وجو بدون تأثیر بر روی رتبه‌بندی صفحه استفاده شود.

مثال: power searching <> OSINT

علاوه بر جستجوی OSINT همراه با دو کلمه کلیدی دیگر، OSINT تأثیری در رتبه‌بندی صفحات نتیجه ندارد.

title

این کاملاً با intitle معادل است. می‌توان از آن برای جستجو در عنوان صفحات با کلمه کلیدی که بعد از پارامتر پرس‌وجو مشخص شده است، استفاده کرد.

مثال: title: osint

صفحات حاوی OSINT در عنوان صفحه را ارائه می‌دهد. به‌طور مشابه می‌توانیم از این پارامتر پرس‌وجو برای جستجوی بیش از یک کلمه کلیدی استفاده کنیم.

مثال: title:(power searching)

url

این پارامتر برای جستجوی دقیق URL ارائه شده توسط کاربر در پایگاه داده یاند کس استفاده می‌شود.

مثال: url: http://attacker.in

در اینجا یاندکس نتایج‌های را در صورت وجود و تنها در صورتی که URL در پایگاه داده آن وجود داشته باشد، ارائه می‌دهد.

Inurl

این اپراتور معادل Inurl سایر موتورهای جستجو است.

مثال: inurl:osint

mime:type

این پارامتر پرس‌و‌جواب بسیار شبیه به پارامتر filetype گوگل است و به کاربر کمک می‌کند تا نوع خاصی از فایل را جستجو کند.

مثال: osint mime: pdf

Yandex search results for "osint mime:pdf". The results show 4 thousand findings. The top result is "OSINT tools for security" from archive.fosdem.org, with a PDF and View link. The second result is "Open Source Intelligence (OSINT)" from fas.org, with a PDF and View link. The third result is "Open source intelligence" from ai-intelligence.eu, with a PDF and View link. The fourth result is "OSINT from a UK perspective: considerations from the law" from shura.shu.ac.uk, with a PDF and View link.

این جستجو کلیه پیوندهای PDF را که حاوی کلمات کلیدی osint هستند ارائه می‌دهد.

انواع فایل‌های پشتیبانی شده توسط MIME یاندکس عبارت‌اند از:

PDF, RTF, SWF, DOC, XLS, PPT, DOCX, PPTX, XLSX, ODT, ODS, ODP, ODG

host

این اپراتور می‌تواند برای جستجو تمام میزبان‌های موجود مورد استفاده قرار گیرد. این اپراتور بیشتر در تست‌های نفوذ مورد استفاده قرار گیرد.

مثال: host:owasp.org

rhost

این کاملاً شبیه به "host" است، اما "rhost" جستجو برای میزبان معکوس است. این همچنین می‌تواند توسط آزمایش کنندگان نفوذ مورد استفاده قرار گیرد تا تمام جزئیات میزبان معکوس را دریافت کند.

این را می‌توان به دو روش استفاده کرد.

مثال:

rhost:org.owasp.*

rhost:org.owasp.www

site

این اپراتور بهترین دوست یک تست نفوذ یا هکر است. این اپراتور در بیشتر موتورهای جستجو در دسترس است. این اپراتور تمام اطلاعات مربوط به زیر دامنه URL ارائه شده را فراهم می‌کند.

برای آزمایش کنندگان نفوذ یا هکرها یافتن مکان آسیب‌پذیری مهم است. همان‌طور که در بیشتر موارد، سایت‌های اصلی نسبت به زیر دامنه‌ها بسیار امن هستند، ارائه جزئیات زیر دامنه‌ها به هکر یا تست نفوذ کمک می‌کند و سپس کار انجام می‌شود؛ بنابراین اهمیت این اپراتور در صنعت امنیتی کاملاً احساس می‌شود.

مثال: site:http://www.owasp.org

این عبارت تمام زیر دامنه‌های موجود دامنه owasp.com و همچنین تمام صفحات را ارائه می‌دهد.

date

این پرس‌وجو می‌تواند برای محدود کردن داده‌های جستجو به یک تاریخ خاص در پرس‌وجو مورد استفاده قرار گیرد.

مثال: date:201408*

در این مورد، فرمت تاریخ استفاده شده YYYYMMDD است، اما در مورد DD ما از اپراتور "استفاده کردیم، بنابراین نتایج را محدود به اوت ۲۰۱۴ می‌کنیم. ما همچنین می‌توانیم با تغییر در پرس‌وجو، آن را به یک تاریخ خاص از اوت ۲۰۱۴ محدود کنیم.

مثال: date:20140808

این نتایج فقط مربوط به آن تاریخ است. ما همچنین می‌توانیم از "به جای": استفاده کنیم و همان کار را خواهیم کرد؛ بنابراین پرس‌وجو بالا را می‌توان به شکل زیر تغییر داد:

مثال: date = 201408* date = 20140808

همان‌طور که قبلاً هم بحث کردیم می‌توانیم نتایج جستجو را به یک دوره زمانی خاص محدود کنیم. بگذارید بگوییم می‌خواهیم چزی را از یک تاریخ خاص به بعد جستجو ببریم. در آن صورت می‌توانیم از عبارت زیر استفاده کنیم:

مثال: date=>20140808

این نتایج از ۸ آگوست ۲۰۱۴ تا تاریخ فعلی ارائه خواهد کرد، اما اگر می‌خواهید هر دو تاریخ شروع و تاریخ پایان را محدود کنید. در این مورد از عبارت زیر استفاده کنید:

مثال: date=20140808..20140810

در اینجا ما نتایج را از ۸ آگوست ۲۰۱۴ تا ۱۰ آگوست ۲۰۱۴ دریافت خواهیم کرد.

domain

برای تعیین نتایج جستجو بر اساس دامنه‌های سطح بالا "TLDs" می‌تواند مورد استفاده قرار گیرد. اغلب این نوع جستجوی دامنه برای به دست آوردن نتایج از حوزه‌های مشخص کشور انجام می‌شود. مثلاً می‌خواهیم لیستی از سرویس‌های امنیتی CERT را از کشورهای مختلف ارائه شده، به دست آوریم. در این صورت ما می‌توانیم در کشور خاص جستجو کنیم. مثلاً می‌خواهیم این اطلاعات را برای نیوزیلند دریافت کنیم که TLD آن nz است؛ بنابراین می‌توانیم از پرس‌وجو مانند زیر استفاده کنیم:

به عنوان مثال: "cert empanelled company" domain:nz

lang

این اپراتور می‌تواند برای جستجو صفحات نوشته شده در زبان‌های خاص استفاده شود.

- ↳ RU: Russian
- ↳ UK: Ukrainian
- ↳ BE: Belorussian
- ↳ EN: English
- ↳ FR: French
- ↳ DE: German
- ↳ KK: Kazakh
- ↳ TT: Tatar
- ↳ TR: Turkish

اگرچه همیشه می‌توانیم از مترجم گوگل برای ترجمه صفحه از هر زبان به زبان انگلیسی یا به هر زبان دیگر استفاده کنیم، این ویژگی افزوده شده توسط یاندکس است تا حداقل نیازهای منطقه‌ای، مورد استفاده مردم قرار گیرد.

بنابراین برای جستجوی یک صفحه، ما باید فرم کوتاه زبان را ارائه دهیم.

مثال: power search lang: en

این عبارت صفحات را به زبان انگلیسی جستجو می‌کند که شامل کلمات کلیدی مشخص شده است.

cat

برای جستجوی چیزهای مختلف بر اساس شناسه منطقه یا شناسه موضوعی استفاده می‌شود. با استفاده از این گزینه می‌توانیم نتیجه را بر اساس منطقه یا موضوع اختصاص داده شده در پایگاه داده یاندکس جستجو کنیم.

جزئیات کدهای منطقه‌ای:  <http://search.yaca.yandex.ru/geo.c2n>.

جزئیات کدهای موضوعی:  <http://search.yaca.yandex.ru/cat.c2n>.

صفحات، حاوی اطلاعاتی به زبان روسی هستند، بنابراین می‌توانیم از ترجمه گوگل برای ترجمه آن استفاده کنیم.

یکی از ویژگی‌های یاندکس، رابط کاربری جستجوی پیشرفته آن در لینک زیر است:

<http://www.yandex.com/search/advanced?&lr=10558>

در اینجا باید فقط آنچه را که می‌خواهیم انتخاب کنیم و مهم‌تر از همه، بیشتر اپراتورهایی که در بالا مورد بحث قرار دادیم را پوشش می‌دهد؛ بنابراین به آن صفحه بروید، آنچه را که می‌خواهید انتخاب کنید و با استفاده از جستجو کنید.

به طور قطع پس از گذراز تمام این اپراتورها، می‌توانیم به راحتی تأثیر جستجوی پیشرفته را احساس کنیم. جستجوی پیشرفته، کاربر را با اطلاعات سریع‌تر، کارآمدتر و قابل اطمینان‌تر روبرو می‌کند. این تلاش‌های دستی ما را برای دریافت اطلاعات مورد نظر، کاهش می‌دهد و کیفیت محتوا نیز در جستجوی پیشرفته، بهتر است، زیرا جستجو را محدود به چیزی که در واقع دنبال آن هستیم، می‌کنیم که می‌تواند جستجوی دامنه خاص کشور، نوع خاصی از فایل یا محتوای از یک تاریخ خاص باشد. با استفاده از جستجوی کلیدواژه ساده این کارها را نمی‌توان انجام داد.

ما در عصری هستیم که همه چیز اطلاعات است؛ بنابراین فاکتور اطمینان ضروری است و اگر اطلاعات مهم قابل اطمینان را از شبکه در مدت زمان بسیار کم بخواهیم، باید روی جستجوی پیشرفته تمرکز کنیم. ما می‌توانیم از هر موتور جستجو معمولی استفاده کنیم. اکثر موتورهای جستجوگر اپراتورهای بسیار مشابهی برای رسیدن به اهداف دارند، اما ویژگی‌های خاصی در برخی از آن‌ها وجود دارد؛ بنابراین به دنبال آن ویژگی‌های خاص و استفاده از موتورهای جستجوی مختلف برای جستجوی پیشرفته سفارشی باشید.

موتورهای جستجوی مختلف و اپراتورهای آن‌ها و چگونگی استفاده از این اپراتورها برای جستجوی بهتر و نتایج دقیق‌تر را یاد گرفتیم. برخی از اپراتورها و چگونگی کمک آن‌ها به محدود کردن نتایج را دیدیم و این که چگونه می‌توان آن‌ها را با سایر اپراتورها مورد استفاده قرار داد تا یک پرس‌وجو عالی ایجاد کنند که به طور مستقیم ما را به آنچه می‌خواهیم، برساند. اگرچه برخی از اپراتورها برای موتورهای جستجوی مختلفی وجود دارند که کارشان کمتر انجام می‌شود، اما با توجه به اینکه تکنیک‌های خوش و نمایه‌سازی موتورهای جستجو مختلف، متفاوت است، ارزشمند است که بدانیم کدام یک از آن‌ها، نتایج را بسته به شرایط موردنیاز ما بهتر می‌کند. یکی از چیزهایی که باید در نظر داشته باشید این است که ارائه‌دهندگان جستجو در حال از بین بردن اپراتورها یا ویژگی‌هایی هستند که به طور مرتب به اندازه کافی مورد استفاده قرار نمی‌گیرند و بعضی از ویژگی‌های در بعضی مناطق قابل دسترسی نیستند.

ما دیدیم که چگونه می‌توانیم نتایج مطلوب را با استفاده از تکنیک‌های کوچک اما مؤثر به دست آوریم. تأثیر این تکنیک‌ها نه تنها محدود به پیدا کردن لینک وب‌سایت‌ها نیست بلکه با خلاقیت از آن‌ها می‌توان در زمینه‌های

مختلف استفاده کرد. به غیر از یافتن اطلاعات در وب که مطمئناً برای همه مفید است، این تکنیک‌ها می‌توانند برای پیدا کردن اطلاعاتی خاص استفاده شود. به عنوان مثال یک حرفه‌ای بازاریابی می‌تواند اندازه و بوسایت رقیب را با استفاده از اپراتور "site" به دست آورد و یا ایمیل یک شرکت را با استفاده از عبارت زیر پیدا کند:

"*@randomcompany.com."

همچنین دیدیم که چگونه دورکها توسط متخصصان امنیت سایبری برای پیدا کردن اطلاعات حساس و خطرناک فقط با استفاده از کلمات کلیدی ساده و اپراتورها استفاده می‌شود. در اینجا نه تنها در مورد اپراتورها بلکه در مورد چگونگی استفاده از آن‌ها به صورت خلاقانه نیز یاد گرفتیم.

تا کنون عمدهاً بر برنامه‌های مبتنی بر مرور وب تمرکز کرده‌ایم. در فصل بعدی، در حال یادگیری در مورد ابزارهای مختلفی هستیم که باید به عنوان برنامه کاربردی نصب شوند و از ویژگی‌های مختلف برای استخراج اطلاعات مربوط به فیلد‌های مختلف، با استفاده از روش‌های مختلف استفاده کنند.

فصل ۶: ابزارها و تکنیک‌های OSINT

مقدمه

در فصل‌های قبلی، در مورد اصول اینترنت و روش‌های مؤثر برای جستجوی آن یاد گرفتیم. جستجوی رسانه‌های اجتماعی در موتورهای جستجو غیرمتعارف را دیدیم و تکنیک‌های مؤثر برای استفاده از موتورهای جستجو را آموختیم. در این فصل یک قدم به جلو حرکت خواهیم کرد و درباره برخی از ابزارهای خودکار و خدمات مبتنی بر وب که اغلب برای شناسایی حرفه‌ای از حوزه‌های مرتبط با اطلاعات مختلف، مخصوصاً امنیت اطلاعات استفاده می‌شود، بحث خواهد شد. ما از نصب بهمنظور درک رابط کاربری شروع خواهیم کرد و بیشتر در مورد قابلیت و استفاده از آن‌ها یاد خواهیم گرفت. برخی از این ابزارها رابط گرافیکی را فراهم می‌کنند و برخی از آن‌ها بر اساس خط فرمان هستند؛ اما آن‌ها از طریق رابط کاربری قضاوت نمی‌شوند، بلکه از طریق قابلیت و ارتباط آن‌ها در زمینه کاری ما قضاوت می‌شوند.

قبل از هر کار، باید پیش نیازهایی را نصب کنیم تا در هنگام نصب و استفاده از آن‌ها هیچ مشکلی نداشته باشیم. بسته‌هایی که ما نیاز داریم عبارت‌اند از:

✓ آخرین نسخه جاوا

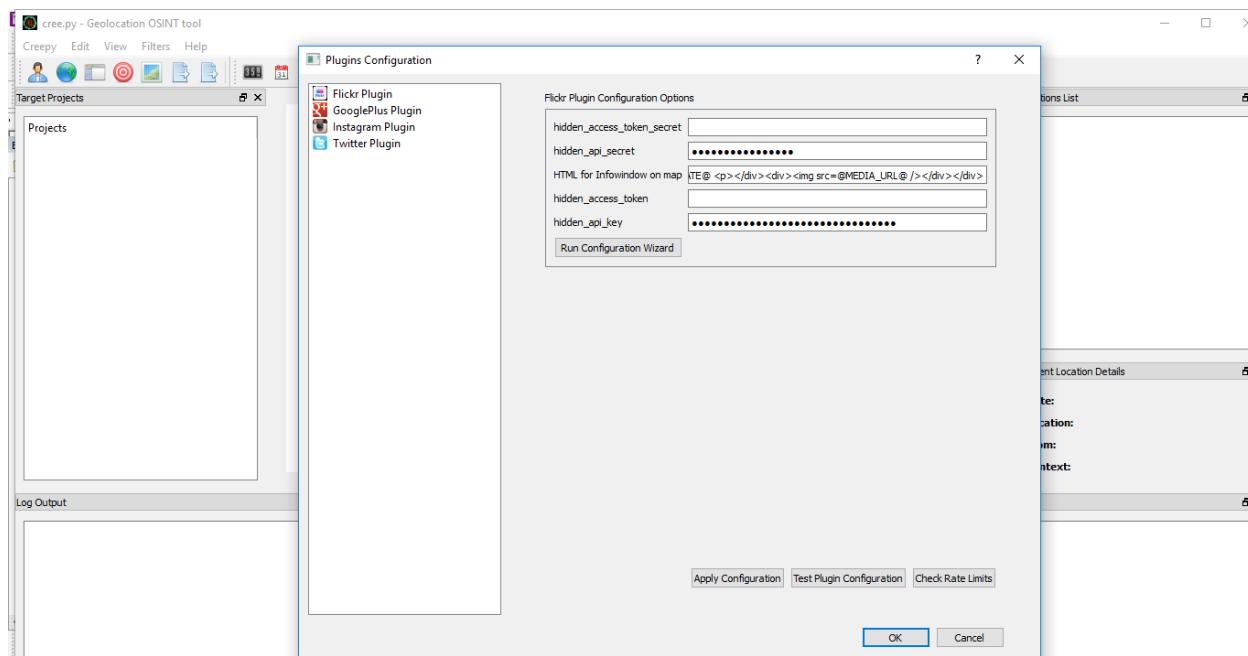
✓ پایتون ۲.۷

Microsoft.NET Framework v4 ✓

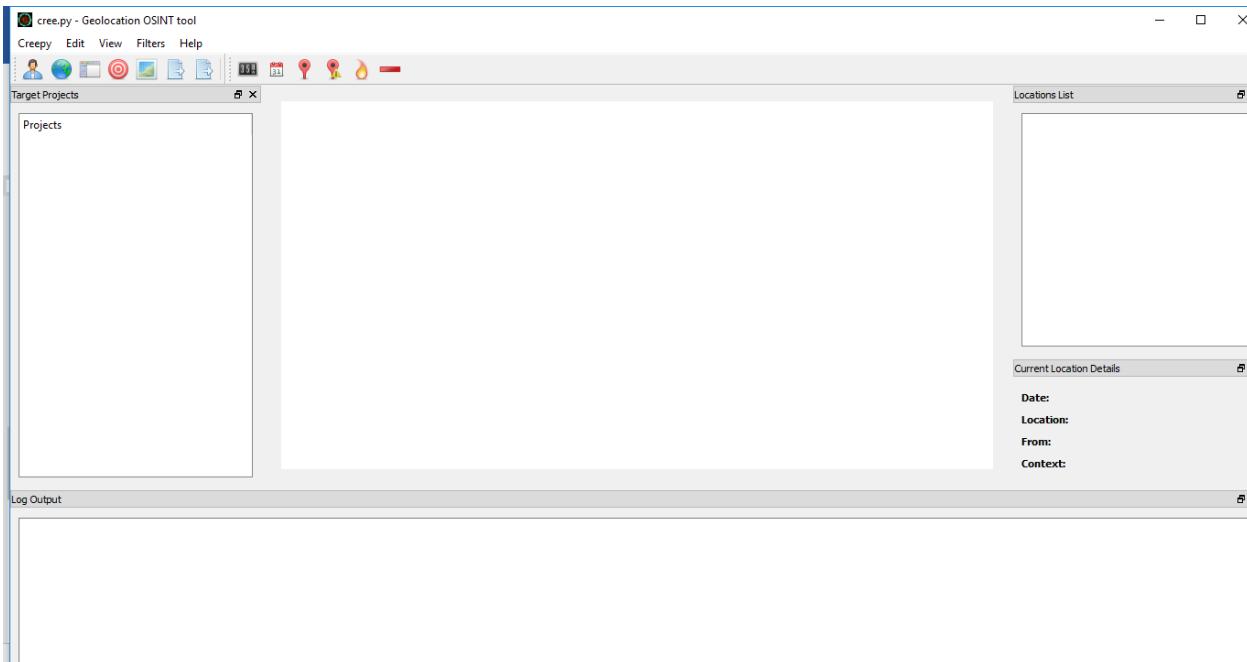
CREEPY

اکثر ما به شبکه‌های اجتماعی معتقد‌یم و اشتراک‌گذاری تصویر یکی از ویژگی‌های مورد استفاده آن‌ها است؛ اما گاهی اوقات هنگامی که ما این تصاویر را به اشتراک می‌گذاریم ممکن است شامل مکان دقیقی که در آن تصویر گرفته شده است، باشد.

Creepy یک برنامه پایتونی است که می‌تواند اطلاعات را استخراج و موقعیت جغرافیایی را بر روی یک نقشه نشان دهد. در حال حاضر از توییتر، فلیکر و نمایش مشخصات عمومی پشتیبانی می‌کند. این موقعیت جغرافیایی را بر اساس اطلاعات EXIF ذخیره شده در تصاویر، اطلاعات جغرافیایی موجود از طریق رابط برنامه‌نویسی برنامه (API) و برخی از تکنیک‌های دیگر استخراج می‌کند.



آن را می‌توان از <https://github.com/ilektrojohn/creepy> دانلود کرد. نیاز به انتخاب نسخه با توجه به پلت فرم و نصب آن وجود دارد. مرحله بعد از نصب Creepy این است که پلاگین‌هایی را که در آن در دسترس است، نصب کنید، برای این کار به سادگی باید بر روی دکمه Configuration موجود در زیر برگه edit کلیک کنید. در اینجا می‌توانیم پلاگین‌ها را انتخاب کنیم و با استفاده از وایزارد آن‌ها را مطابق نیاز خود تنظیم کنیم. هنگامی که انجام می‌شود، می‌توانیم بررسی کنیم که آیا به درستی کار می‌کند یا نه؛ بنابراین از دکمه Configuring Test Plugin استفاده می‌کنیم.



پس از فاز نصب، می‌توانیم یک پروژه جدید را با کلیک کردن بر روی نماد person در نوار بالا شروع کنیم. در اینجا می‌توانیم نام پروژه و جستجو برای افراد در پورتال‌های مختلف را تنظیم کنیم. از نتایج جستجو، ما می‌توانیم شخص مورد علاقه را انتخاب و او را در فهرست هدف قرار دهیم و آن را پایان دهیم. پس از این، پروژه ما تحت نوار پروژه در سمت راست نمایش داده می‌شود.

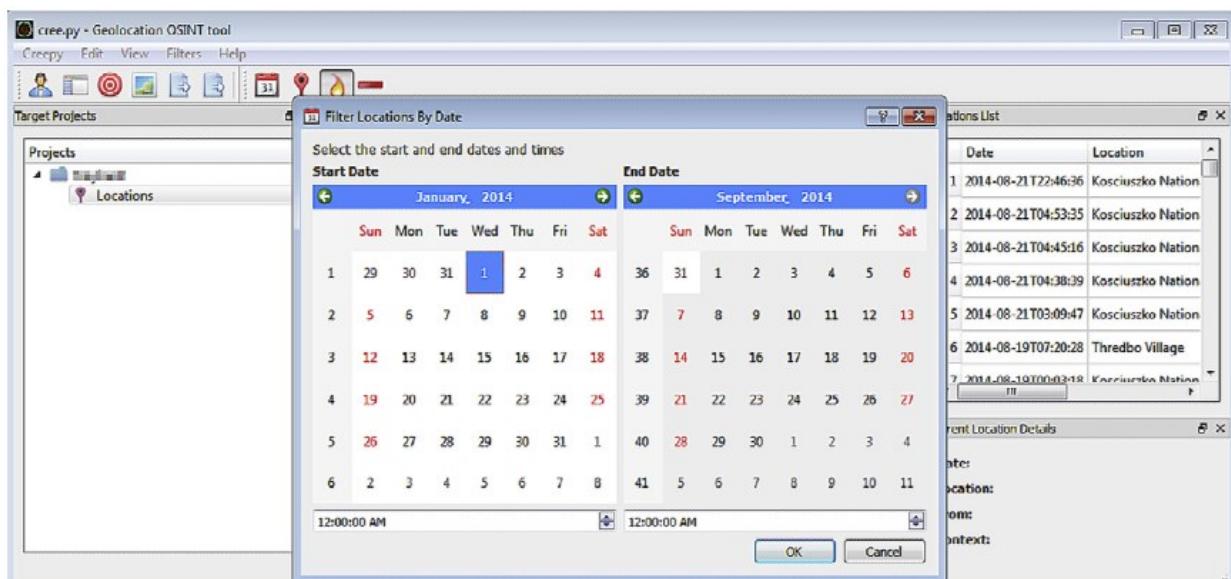
Plugin	Picture	Username	Full Name	User Id
Twitter Plugin		testuserNo1	testuser number...	49628700
Twitter Plugin		nakachi86	testuser	177183359
Twitter Plugin		jjtacc	JJ TestUser	348697535
Twitter Plugin		testuser1112	testnguser22	158275283

Plugin	Picture	Username	Full Name	User Id

حالا به سادگی نیاز به انتخاب پروژه و با کلیک بر روی آیکون هدف و یا کلیک راست بر روی پروژه و کلیک بر روی Analyze Current Project وجود دارد. پس از این، Creepy تجزیه و تحلیل را شروع خواهد کرد. پس از انجام تجزیه و تحلیل، Creepy نتایج را بر روی نقشه نمایش می‌دهد.



اکنون می‌توانیم نتایجی را که در آن نقشه با نشانگرها بر اساس موقعیت جغرافیایی مشخص شده است را ببینیم. در حال حاضر Creepy به ما اجازه می‌دهد که این نتایج را بر اساس فیلترهای مختلف محدود کنیم.



با کلیک بر روی دکمه تقویم، می‌توانیم نتایج را بر اساس یک دوره زمان بندی، انتخاب کنیم. همچنین می‌توان نتایج را بر اساس منطقه فیلتر کرد که ما می‌توانیم آن را به شکل شعاع در کیلومتر از یک نقطه انتخابی تعریف

کنیم. همچنین می‌توانیم نتایج را به صورت نقشه heat به جای نشانگرها مشاهده کنیم. علامت منفی (–) که در انتهای آن وجود دارد می‌تواند برای حذف همه فیلدهای اعمال شده بر روی نتایج استفاده شود.

نتایجی که از Creepy دریافت می‌کنیم، می‌تواند به صورت فایل CSV و همچنین KML برای نمایش نشانگرها در یک نقشه دیگر استفاده شود، ذخیره شود.

Creepy را می‌توان برای مرحله‌ی جمع‌آوری اطلاعات در طی یک آزمون (آزمون نفوذ) و همچنین به عنوان یک ابزار اثبات برای نشان دادن به کاربران که اطلاعات آن‌ها آشکار است، استفاده کرد.



THEHARVESTER

یک ابزار هوشمند منبع باز (OSINT) برای به دست آوردن آدرس‌های ایمیل، نام کارمند، پورت‌های باز، زیر دامنه، میزبان‌ها و غیره از منابع عمومی مانند موتورهای جستجویی مانند گوگل، بینگ و سایت‌های دیگر مانند LinkedIn است. این یک ابزار ساده پایتونی است که برای استفاده آسان است و شامل توابع جمع‌آوری اطلاعات مختلف است. به عنوان یک ابزار پایتونی کاملاً قابل فهم است که برای استفاده از این ابزار باید Python را در سیستم مان نصب کنیم. این ابزار توسط Christian Martorella ایجاد شده و یکی از ابزارهای ساده، محبوب و گسترده مورد استفاده در جمع‌آوری اطلاعات است.

را می‌توانید در آدرس زیر باید:

<http://www.edge-security.com/theharvester.php>

به طور کلی نیاز به وارد کردن نام دامنه یا نام شرکت برای جمع آوری اطلاعات مربوطه مانند آدرس های ایمیل، زیر دامنه ها یا سایر جزئیات ذکر شده در پاراگراف فوق را داریم؛ اما همچنین می توانیم از کلمات کلیدی برای جمع آوری اطلاعات مرتبط استفاده کنیم.

ما می‌توانیم جستجو را محدود کنیم، مثلاً از کدام منیع عمومی می‌خواهیم برای جمع‌آوری اطلاعات استفاده کنیم. منابع زیادی وجود دارند که TheHarvester برای جمع‌آوری اطلاعات استفاده می‌کند اما قبل از اینکه به این موضوع پردازیم، نحوه استفاده از TheHarvester را در کمی کنیم.

EX: theharvester -d example.com -l 500 -b Google

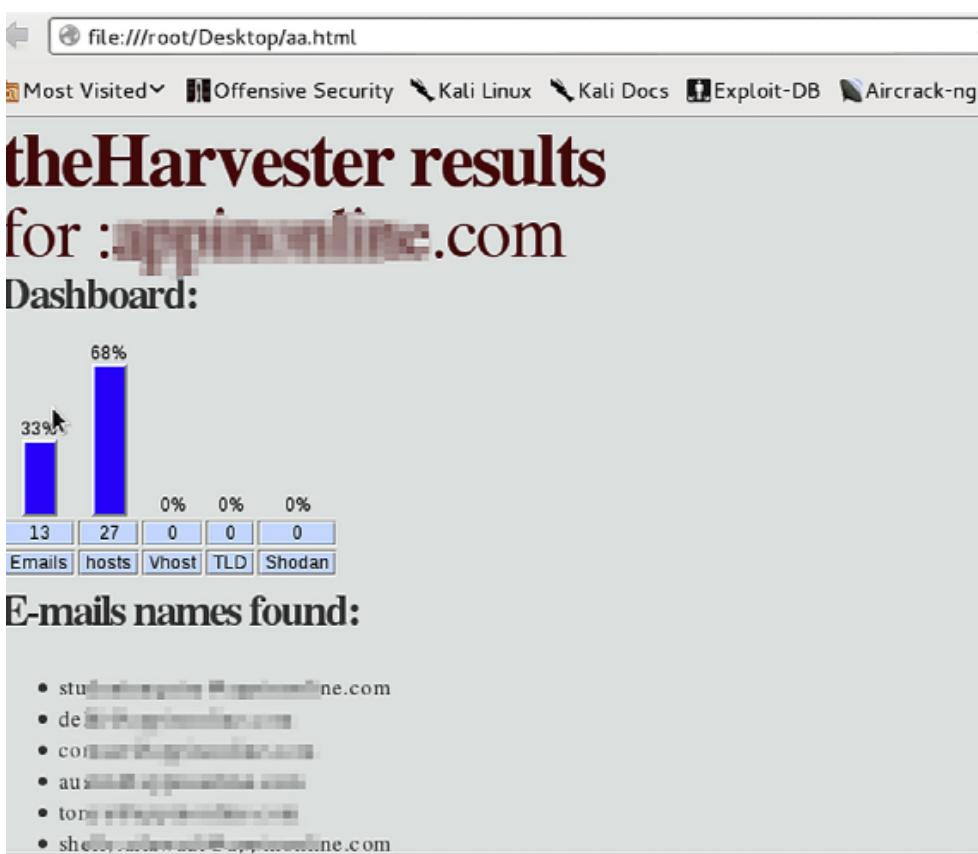
d: نام دامنه یا نام شرکت

؛ محدودت تعداد نتیجه

b: مشخص نمودن منبع داده ماتند دستور بالا در گوگل، اما به غیر از این می‌توان از LinkedIn و غیره به عنوان منبع برای جمع‌آوری اطلاعات استفاده کرد.

گزنهای دیگری نیز وجود دارد، مانند:

-s = to start with a particular result number (the default value is 0)
 -v = to get virtual hosts by verifying hostnames via DNS resolution
 -f = for saving the data. (formats available either html or xml)
 -n = to perform DNS resolve query for all the discovered ranges
 -c = to perform DNS bruteforce for all domain names
 -t = to perform a DNS TLD expansion discovery
 -e = to use a specific DNS server
 -l = To limit the number of result to work with
 -h = to use Shodan database to query discovered hosts.



منابع مورد استفاده آن عبارت اند از گوگل، Bing، Google profiles، LinkedIn، pretty good privacy (PGP) servers، Exalead، people123، name servers، Yandex، Shodan، Jigsaw، Google، Bing، Yandex، Exalead و موتورهای موتورهای جستجویی هستند که به عنوان منبع در backend استفاده می‌شوند، در حالی که Shodan موتور جستجو است اما نه یک موتور رایج متعارف و قبلاً در مورد بحث کرده‌ایم. سرورهای PGP مانند سرورهای کلیدی¹ مورد استفاده

¹ key servers

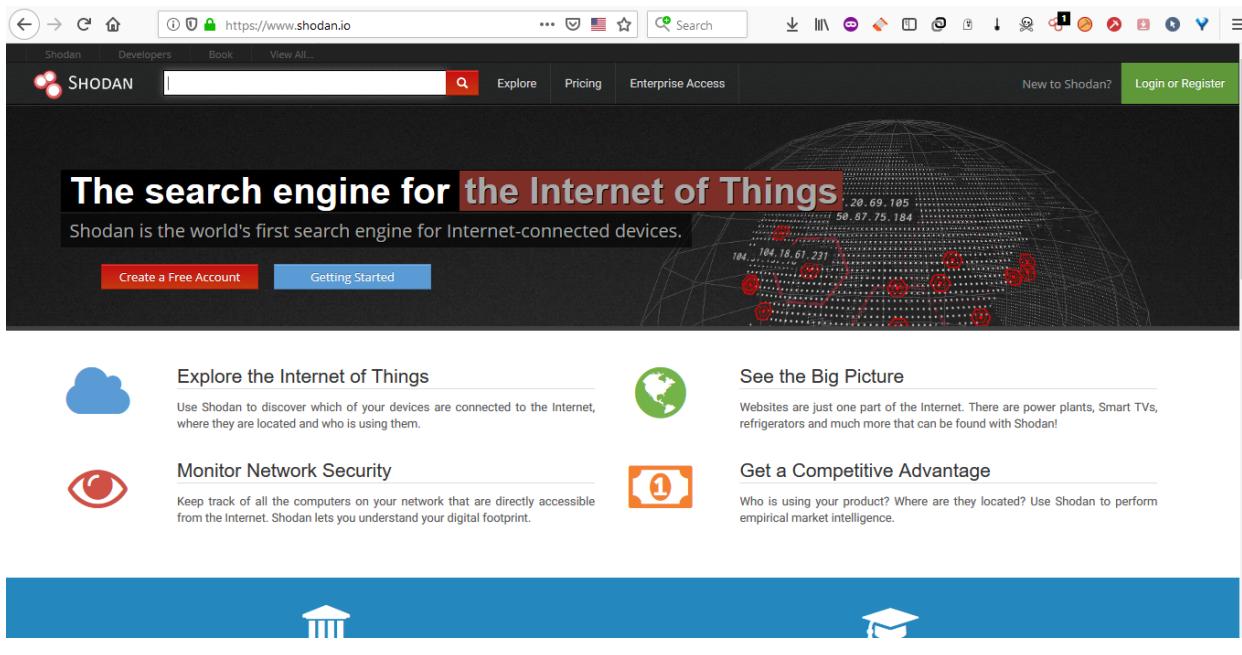
برای امنیت داده‌ها هستند و همچنین منبع خوبی برای جمع‌آوری اطلاعات الکترونیکی هستند. People123 برای جستجوی یک فرد خاص است و Jigsaw^۱ برای کالاهای فروشی است. TheHarvester منابع مختلف جمع‌آوری اطلاعات را برای برداشت ایمیل از گوگل، Bing، سرورهای PGP و بعضی اوقات Exalead می‌گیرد و درخواست‌های خاص خود را در پس‌زمینه برای دریافت نتیجه دلخواه می‌گیرد. به‌طور مشابه برای Exalead دامنه‌های زیر مجموعه و یا نامهای میزبان آن دوباره از گوگل، Yandex، Bing، Excaliate PGP سرور و استفاده می‌کند؛ و نهایتاً برای گرفتن لیست نام کارمندان، از LinkedIn، Google Profiles و People123 به‌عنوان منبع اصلی استفاده می‌کند.

<https://github.com/laramies/theHarvester>

SHODAN

ما قبلاً درباره Shodan مختصرآ در فصل ۴ بحث کرده‌ایم، اما این موتور جستجوی منحصر به فرد به بیش از یک پاراگراف در مورد استفاده و تأثیر آن نیاز دارد. همان‌طور که پیش‌تر گفته شد، Shodan یک موتور جستجوی رایانه‌ای است. اینترنت شامل انواع مختلفی از دستگاه‌های متصل به آن و در دسترس عموم است. اکثر این دستگاه‌ها یک بتر دارند که در پاسخ به درخواست فرستاده شده توسط یک مشتری ارسال می‌شوند. بسیاری از این بترها حاوی اطلاعاتی هستند که می‌تواند حساس باشند، مانند نسخه سرور، نوع دستگاه، حالت تائید هویت و غیره. Shodan به ما اجازه می‌دهد تا این دستگاه‌ها را از طریق اینترنت جستجو کنیم و همچنین می‌توانیم نتایج را محدود کنیم.

^۱ cloud-based



یک حساب کاربری برای استفاده از این ابزار عالی و حذف برخی از محدودیت‌های اعمال شده در آن ایجاد کنید. پس از ورود به برنامه به‌سادگی به صفحه داشبورد در <https://www.shodan.io/> بروید. در اینجا می‌توانیم برخی از جستجوهای اخیر و همچنین جستجوهای محبوب ساخته شده در این پلتفرم را بینیم. این صفحه همچنین یک مرجع سریع برای فیلتری که ما می‌توانیم استفاده کنیم را نشان می‌دهد. اجازه دهید جستجوهای محبوب را که ذکر شده است را مشاهده کنیم. در اینجا می‌بینیم که جستجوهای مختلفی وجود دارد که بسیار جالب هستند مانند وب کم، رمز عبور پیش فرض، SCADA و غیره. کلیک بر روی یکی از این‌ها به‌طور مستقیم ما را به صفحه نتیجه می‌برد و جزئیات ماشین‌ها را در اینترنت با آن لیست می‌کند کلمات کلیدی اختصاصی صفحه <https://www.shodan.io/> لیست تمام فیلترهایی را که می‌توانیم در Shodan برای انجام جستجوی انجام دهیم، مانند کشور، نام میزبان، پورت و غیره را نشان می‌دهد. "+", "-", "||"

اجازه دهید یک جستجوی ساده در Shodan برای کلمه کلیدی "webcam" انجام دهیم. Shodan به‌سادگی بیش از ۱۵،۰۰۰ نتیجه برای این کلمه کلیدی پیدا کرده است؛ هر چند نمی‌توانیم تمام نتایج را در نسخه رایگان مشاهده کنیم، با این حال آنچه دریافت می‌کنیم به اندازه کافی در دسترس بودن چنین دستگاه‌هایی در اینترنت است. برخی از این‌ها ممکن است توسط نوعی از مکانیزم تائید هویت، مانند نام کاربری و رمز عبور محافظت شوند، اما برخی از آن‌ها ممکن است به هیچ وجه بدون هیچ گونه مکانیزم قابل دسترس باشند. ما می‌توانیم به‌سادگی باز کردن آدرس IP ذکر شده در مرورگر به آن دسترسی یابیم (ممکن است که این کار بسته به قوانین کشور و غیره غیرقانونی

باشد). ما با استفاده از فیلتر "country" می‌توانیم این نتایج را به یک کشور محدود کنیم؛ بنابراین پرس‌وجو جدید ما "webcams country:us" است که به ما یک لیست از وب کم‌های ایالات متحده آمریکا می‌دهد.

The screenshot shows the Shodan search interface with the query "webcam". The results page displays a world map with red dots indicating found cameras. A sidebar on the left shows "TOTAL RESULTS" (5,400), "TOP COUNTRIES" (United States: 951, Korea, Republic of: 598, Germany: 502, Poland: 334, Italy: 294), and "TOP SERVICES" (HTTP (8080): 1,794, 8081: 874, HTTP: 231, HTTPS: 188, 8083: 142). The main content area lists four specific camera findings:

- 5.15.241.199**: Located in Romania, Sibiu. Tags: ufanet. Response: HTTP/1.1 401 Unauthorized. Headers: Content-Length: 0, WWW-Authenticate: Digest realm="IP Webcam", nonce="1555300517", qop="auth"
- 188.108.118.165**: Located in Germany, Kiel. Tags: dsl-188-108-118-165. Response: HTTP/1.1 401 Unauthorized. Headers: Content-Length: 0, WWW-Authenticate: Digest realm="IP Webcam", nonce="342377613", qop="auth"
- 84.24.175.195**: Located in Netherlands, Waalwijk. Tags: ziggo. Response: HTTP/1.1 401 Unauthorized. Headers: Content-Length: 0, WWW-Authenticate: Digest qop="auth", realm="IP Webcam", nonce="1555301703"
- 203.189.37.161**: Located in Japan, Nasushiobara. Tags: 1037161. Response: HTTP/1.0 200 OK. Headers: Content-type: text/html, Connection: close, Server: MJPG-Streamer/0.2, Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0

برای دریافت فهرستی از ماشین‌ها با پروتکل FTP در هند، می‌توانیم از "port:21 country:in" استفاده کنیم. ما همچنین می‌توانیم آدرس IP خاص یا محدوده‌ای از آن را با استفاده از فیلترینگ "net" جستجو کنیم. Shodan اطلاعات زیادی را ارائه می‌دهد و کاربرد آن تنها توسط خلاقیت کاربران محدود می‌شود.

به غیر از این API برای ادغام داده‌های درخواست شده ما، ارائه می‌دهد. همچنین برخی از خدمات دیگر ارائه شده توسط آن به صورت غیر رایگان وجود دارد و برای هر کسی که در زمینه امنیت اطلاعات کار می‌کند، ارزش دارد. اخیراً پیشرفت‌هایی در Shodan و خدمات مربوط به آن وجود دارد که باعث می‌شود این محصول برای علاقه‌مندان به امنیت اطلاعات رشد کند.

SEARCH DIGGITY

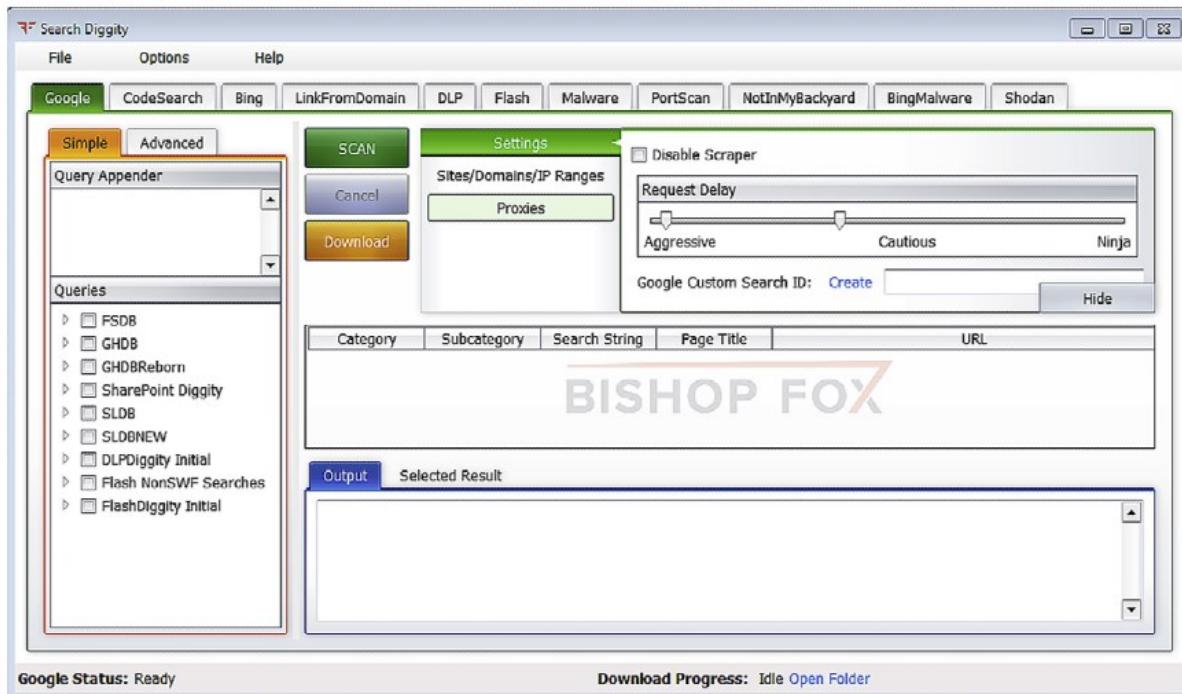
در فصل گذشته در مورد استفاده از ویژگی‌های پیشرفته جستجو در موتورهای جستجو مختلف و همچنین در مورد اصطلاح گوگل هکینگ بحث کردیم. برای انجام چنین عملیاتی، باید فهرست عملیاتی را که می‌خواهیم استفاده کنیم را داشته و باید آن را برای دیدن اینکه آیا چیزی آسیب‌پذیر است تایپ کنیم، اما اگر ابزاری وجود داشته باشد که شامل یک پایگاه داده‌ای از چنین عباراتی داشته باشد، ما می‌توانیم آن را اجرا کنیم. در اینجا وارد Search Diggity می‌شویم. Search Diggity توسط Bishop Fox ایجاد شده و دارای پایگاه داده بزرگ از پرس‌وجوها برای

موتورهای جستجوی مختلف است که به ما اجازه جمع‌آوری اطلاعات مربوط به هدف را می‌دهد. آن را می‌توانید از آدرس زیر دریافت کنید:

<http://www.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools>

پیش نیاز اساسی برای نصب آن مایکروسافت .NET Framework v4 است. هنگامی که برنامه را دانلود کرده و نصب کردیم، چیزهایی که ما نیاز داریم عبارت جستجو و کلید API هستند. این کلید شناسه / API لازم است تا بتوانیم تعداد بیشتری از جستجوها را بدون محدودیت‌های بیشمار انجام دهیم. ما می‌توانیم چگونگی دریافت و استفاده از این کلیدها را در بخش محتوا در زبانه راهنمای همچنین با جستجوی ساده گوگل پیدا کنیم. هنگامی که همه کلیدها (Shodan، Bing، Google و غیره) در جای خود قرار گرفتند، ما می‌توانیم از این ابزار استفاده کنیم.

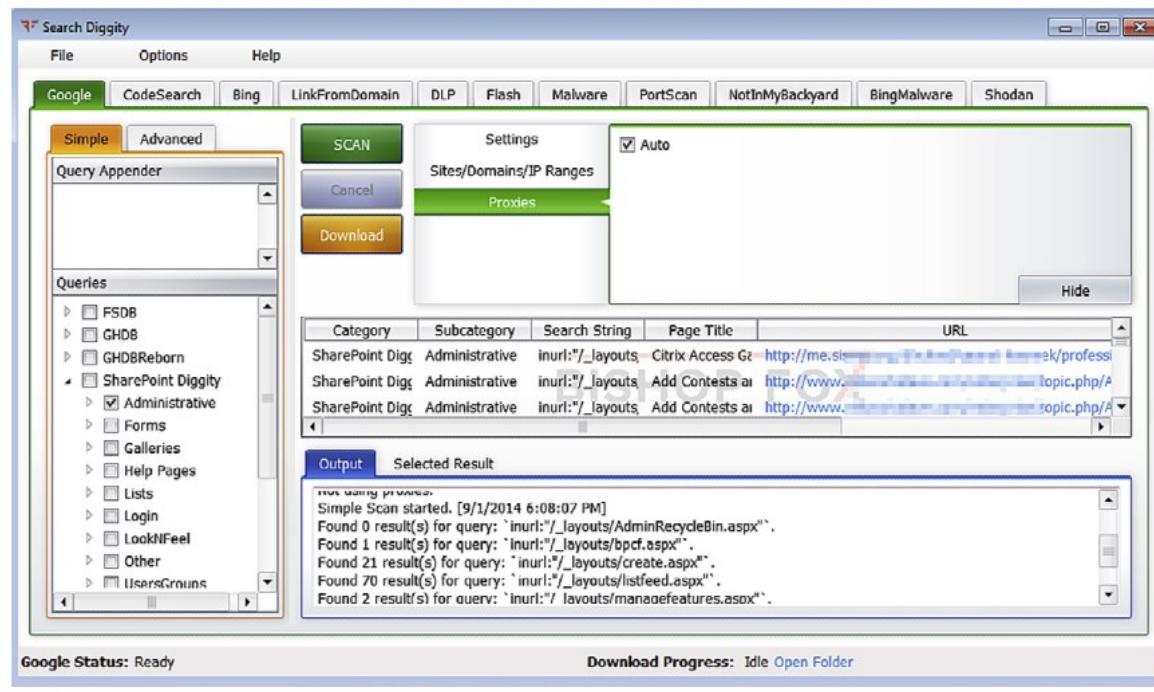
The screenshot shows the Bishop Fox website's navigation bar with links for SERVICES, SUCCESS STORIES, NEWS & EVENTS, and RESOURCES (which is highlighted). Below the navigation is a secondary menu with links for TOOLS, ADVISORIES, PUBLICATIONS, DOWNLOADS, SLIDES, WHITE PAPERS AND GUIDES, VIDEOS, STYLE GUIDE, and VULNERABILITY DISCLOSURE POLICY. The main content area features a heading 'Attack Tools' and a sub-section titled 'Google Hacking Diggity Project'. On the left, there's a sidebar with sections for ATTACK TOOLS, SEARCHDIGGITY, HACKING DICTIONARIES, HACKING GOOGLE CUSTOM SEARCH, and a link to the 'SearchDiggity - Tool Screenshot Gallery'. The right side contains descriptive text about the tools and a callout for 'SearchDiggity v 3' which includes a logo and the text 'The Search Engine Hacking Tool Arsenal'.



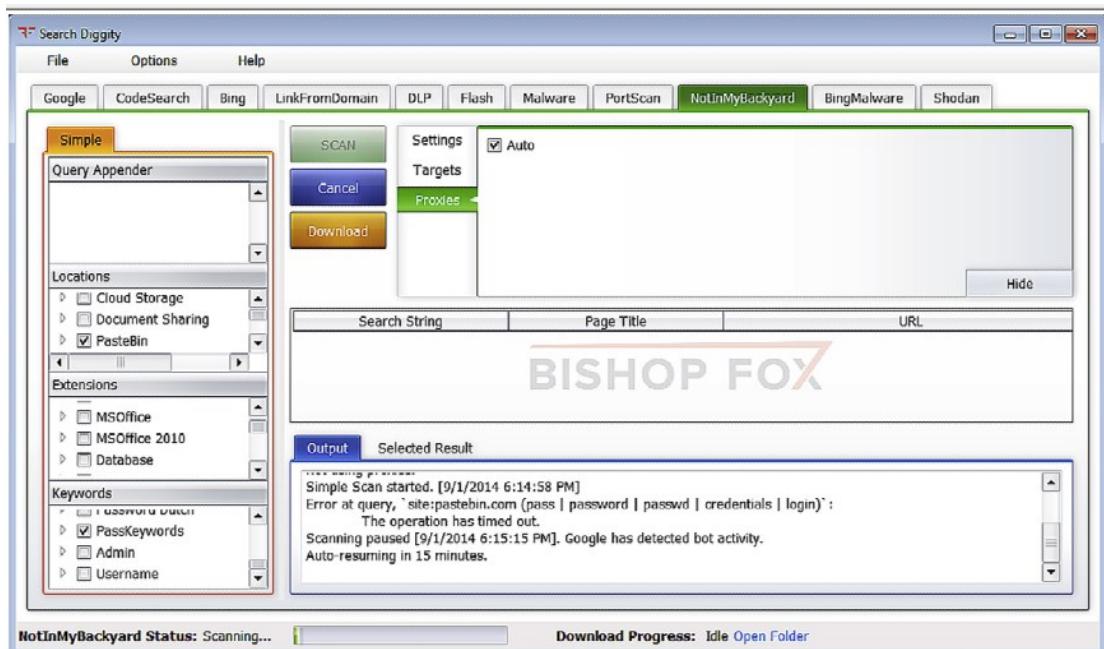
زبانه‌های زیادی مانند Shodan، Google، DLP، Bing، Flash و غیره وجود دارد. هر یک از این زبانه‌ها توابع خاصی را برای انجام جستجوی هدفمند و شناسایی اطلاعات، استفاده می‌کند که می‌تواند از دیدگاه امنیت اطلاعات حیاتی باشد.

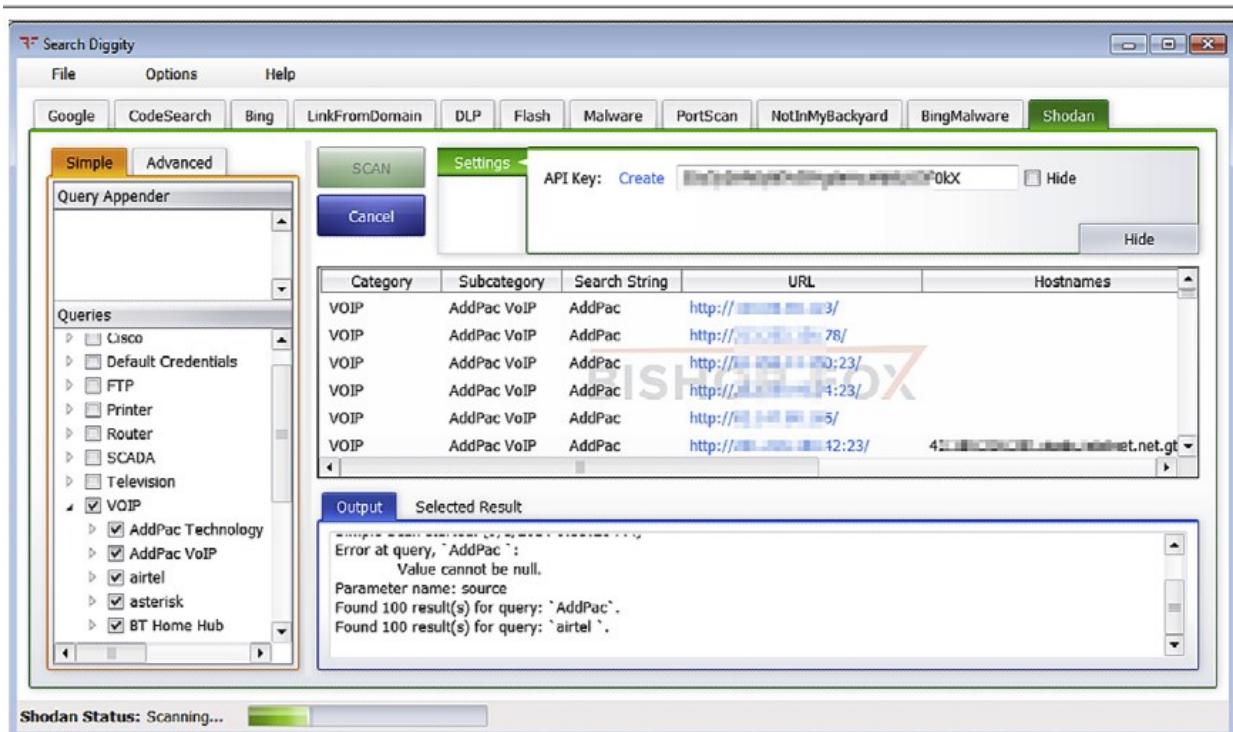
برای استفاده از این ابزار، نیاز به انتخاب یکی از زبانه‌ها در بالای صفحه و نوع نمایش داده‌ها که می‌خواهیم استفاده کنیم، داریم. همچنین می‌توانیم دامنه‌ای را که می‌خواهیم مورد هدف قرار دهیم را مشخص کنیم و به سادگی اسکن را انجام دهیم. بسته به آنچه آنلاین در دسترس است، این ابزار به ما نتایجی برای پرسش‌های مختلف مربوط به نوع پرس‌وجو انتخاب شده، ارائه می‌دهد. به شدت توصیه می‌شود فقط پرس‌وجوهایی را انتخاب کنید که واقعاً علاقه‌مند به آن هستید، چرا که به ما کمک می‌کند تعداد کل پرسش‌ها را محدود کنیم. در حال حاضر پرسش‌ها به درستی طبقه‌بندی شده‌اند تا بر اساس آن شناسایی و انتخاب شوند.

اجازه دهید از پرسش‌ها برای شناسایی صفحات اداری شیرپوینت استفاده کنیم. برای این منظور فقط باید زبانه گوگل و از منوی سمت چپ در زیر مجموعه SharePoint Diggity گزینه Administrative را انتخاب و اسکن را اجرا کنید.



برای اینکه این اسکن را هدفمندتر کنیم، می‌توانیم یک لیست از اهداف را در زیر گزینه Ranges مشخص کنیم. همان‌طور که اسکن را شروع می‌کنیم می‌توانیم نتایج را با اطلاعات مختلف مانند دسته، عنوان صفحه، URL و غیره ببینیم. به همین ترتیب می‌توانیم از اسکن Bing استفاده کنیم که دارای مجموعه‌ای از پرسش‌های جستجو است.





Recon-ng

ابزارهای زیادی برای شناسایی وجود دارد، اما باید توجه ویژه‌ای به Recon-ng شود. این ابزار منبع باز است و توسط (@) Tim Tomes به زبان پایتون نوشته شده است. بسیاری از محققان، برنامه نویسان و توسعه‌دهندگان نیز در این پروژه شرکت کرده‌اند. این پروژه یکی از چارچوب‌های کلی OSINT است. این چارچوب به تمام علاقه‌مندان OSINT برای انجام مراحل مختلف شناسایی به صورت خودکار کمک می‌کند.

Recon-ng به طور عمده بر روی شناسایی منابع مبتنی بر وب تمرکز می‌کند و کاربران آن را با مژول‌های مستقل منحصر به فرد، دقیق و بسیار موردنیاز مبتنی بر فرمان، برای انجام شناسایی عمیق و سریع استفاده می‌کنند. با استثنای آن، به گونه‌ای ساخته شده است که اگر یک تازه وارد در حوزه امنیت بخواهد آن را توسعه دهد، می‌تواند به راحتی با کمی دانش پایتون کار کند. فقط به دلیل استفاده از مژول‌های ساختار یافته، مستندات کامل و استفاده از توابع بومی پایتون است که یک کاربران مشکلی برای دانلود و نصب و نیاز به مژول‌های شخص ثالث پایتون برای کار خاص را ندارند.

این ابزار را می‌توان از آدرس زیر دانلود کنید:

<https://bitbucket.org/LaNMaSteR53/recon-ng>

راهنمای کاربر:

https://bitbucket.org/LaNMaSteR53/recon-ng/wiki/Usage_Guide

راهنمای توسعه:

https://bitbucket.org/LaNMaSteR53/recon-ng/wiki/Development_Guide

با استثنای چشم‌انداز توسعه‌دهنده، نویسنده همچنین بر سهولت استفاده برای کاربران متمرکز بوده است. این چارچوب کاملاً مشابه Metasploit است که یک ابزار بسیار محبوب برای بهره‌برداری در جامعه امنیت اطلاعات است. اگر از جامعه امنیت اطلاعات هستید یا تجربه قبلی استفاده از Metasploit دارید، استفاده از Recon-*ng* کاملاً مشابه است. نصب Recon-*ng* بسیار آسان است؛ برای اجرای فقط نیاز به پایتون ۲.۷.x نصب شده در سیستم دارید. از یک ترمینال *recon.ng* را فراخوانی کنید. برای بررسی تمام دستورات در دسترس می‌توانیم از دستور *help* استفاده کنیم که تمام دستورات موجود را نشان می‌دهد:

> *help*

<i>add</i>	Adds records to the database
<i>back</i>	Exits the current context
<i>del</i>	Deletes records from the database
<i>exit</i>	Exits the framework
<i>help</i>	Displays this menu
<i>keys</i>	Manages framework API keys
<i>load</i>	Loads specified module
<i>pdb</i>	Starts a Python Debugger session
<i>query</i>	Queries the database
<i>record</i>	Records commands to a resource file
<i>reload</i>	Reloads all modules
<i>resource</i>	Executes commands from a resource file
<i>search</i>	Searches available modules
<i>set</i>	Sets module options
<i>shell</i>	Executes shell commands
<i>show</i>	Shows various framework items
<i>spool</i>	Spools output to a file
<i>unset</i>	Unsets module options
<i>use</i>	Loads specified module
<i>workspaces</i>	Manages workspaces

در این چارچوب برخی از ویژگی‌های مانند فضای کاری ارائه شده است که شامل تنظیمات مختلف، پایگاه داده و غیره و یک مکان مستقل برای یک پروژه واحد است. برای مشاهده فضاهای کاری، می‌توانیم از دستور زیر استفاده کنیم:

> help workspaces

این فرمان برای مدیریت فضای کاری از قبیل فهرست کردن، افزودن، انتخاب و حذف فضاهای کاری استفاده می‌شود. اگر کاربر فضای کاری را تنظیم نکند، آنگاه تحت فضای کاری پیش فرض قرار می‌گیرد. اگر بخواهیم بدانیم در کدام فضای کاری هستیم، از دستور زیر استفاده می‌کنیم:

> show workspaces

+-----+

|Workspaces|

+-----+

| default |

+-----+

و ما چیزی شبیه به این داریم که نشان می‌دهد در زیر فضای کاری پیش فرض هستیم.

اگر بخواهیم فضای کاری را تغییر دهیم، مثلاً osint، از دستور زیر استفاده می‌شود:

> workspaces add osint

خط فرمان فضای کاری را نشان می‌دهد که به صورت پیش فرض در نصب تازه به شکل زیر است:

[recon-ng] [default] >

بعد از دستور بالا، به شکل زیر تغییر خواهد کرد:

[recon-ng] [osint] >

اکنون وقت آن است که دستورات و قابلیت‌های آن را بررسی کنیم. اگر از این ابزار برای اولین بار استفاده می‌کنید، دستور العمل پس از «Show»، «Help» است.

[recon-ng] [osint] > show

با استفاده از این فرمان، می‌توانید جزئیات موجود در بنرهای، شرکت‌ها، مخاطبین، اعتبارها، داشبوردها، دامنه‌ها، میزبان‌ها، کلیدها، نشتهای، مکان‌ها، ماثول‌ها، بلوک‌ها، گزینه‌ها، پورت‌ها، طرح‌ها، آسیب‌پذیری‌ها را بینید. اساساً recon-ng شامل پنج بخش مختلف از ماثول‌ها است.

1. Discovery

2. Exploitation
3. Import
4. Recon
5. Reporting

```
[recon-ng v4.1.7, Tim Tomes (@LaNMaSteR53)]

[57] Recon modules
[5] Reporting modules
[2] Exploitation modules
[2] Discovery modules
[1] Import modules

[recon-ng](default) > show modules

Discovery
-----
discovery/info_disclosure/cache_snoop
discovery/info_disclosure/interesting_files

Exploitation
-----
exploitation/injection/command_injector
exploitation/injection/xpath_bruter

Import
-----
import/csv_file

Recon
-----
recon/companies-contacts/facebook
recon/companies-contacts/jigsaw
recon/companies-contacts/jigsaw/point_usage
recon/companies-contacts/jigsaw/purchase_contact
recon/companies-contacts/jigsaw/search_contacts
recon/companies-contacts/linkedin_auth
recon/companies-contacts/linkedin_crawl
recon/contacts-contacts/mangle
recon/contacts-contacts/namechk
recon/contacts-contacts/rapporitive

root@kali: ~
```

با استفاده از دستورات زیر می‌توانید جزئیات بیشتری را از گزینه‌های موجود در مورد این پنج بخش ببینید:

[recon-ng] [osint] > show modules

اکنون می‌توانیم از این مژوول‌ها بر اساس الزامات استفاده کنیم. برای استفاده از هر یک از این مژوول‌ها، ابتدا باید مژوول را با استفاده از دستور زیر بارگیری کنیم، اما قبل از این باید بدانیم که این چارچوب دارای یک قابلیت منحصر به فرد برای بارگیری مژوول با تکمیل خودکار است و یا اگر مژوول‌های بیشتری با یک کلمه کلیدی در دسترس باشد تمام لیست مژوول‌ها لیست می‌شوند. ما می‌خواهیم pwnedlist را بررسی کنیم:

[recon-ng] [osint] > load pwnedlist

در حال حاضر recon-ng بررسی خواهد کرد که آیا این رشته با یک یا چند مژوول مرتبط است یا خیر؟ اگر با یک مژوول مرتبط باشد، آن را بارگذاری خواهد کرد و یا تمام مژوول‌های موجود که حاوی این کلمه کلیدی هستند را نشان می‌دهد.

همان‌طور که کلمه کلیدی pwnedlist با ماثول‌های چندگانه‌ای مرتبط است، در نتیجه آن‌ها را نشان می‌دهد. ما می‌خواهیم از ماثول recon / contacts-creds / pwnedlist استفاده کنیم:

[recon-ng] [osint] > load recon/contacts-creds/pwnedlist

هنگامی که یک ماثول بارگیری می‌شود، نام آن به خط فرمان اضافه می‌شود:

[recon-ng] [osint] [pwnedlist] >

همان‌طور که می‌دانیم، باید تنظیمات مورد نیاز را بررسی کنیم. برای بررسی آن فرمان به شرح زیر است:

[recon-ng] [osint] [pwnedlist] > show options

این فرمان تمام اطلاعات موردنیاز را به صورت جدولی نشان می‌دهد مانند نام فایل مورد نظر، وضعیت فعلی یا مقدار آن و ...

The screenshot shows a terminal window titled 'root@kali: ~'. The window has a decorative background featuring a dragon and the text 'Black Hills Information Security Consulting | Research | Development | Training http://www.blackhillsinfosec.com'. The terminal content is as follows:

```

File Edit View Search Terminal Help
[recon-ng v4.1.7, Tim Tomes (@LaNMaSteR53)]
57] Recon modules
5] Reporting modules
2] Exploitation modules
2] Discovery modules
1] Import modules

[recon-ng][default] > workspaces add osint
[recon-ng][osint] > load pwnedlist
!] Multiple modules match 'pwnedlist'.

Recon
-----
recon/contacts-creds/pwnedlist
recon/domains-creds/pwnedlist/account_creds
recon/domains-creds/pwnedlist/api_usage
recon/domains-creds/pwnedlist/domain_creds
recon/domains-creds/pwnedlist/domain_ispwned
recon/domains-creds/pwnedlist/leak_lookup
recon/domains-creds/pwnedlist/leaks_dump

[recon-ng][osint] > load recon/contacts-creds/pwnedlist
[recon-ng][osint][pwnedlist] > show options
Name      Current Value    Req Description
-----  -----
SOURCE   google@gmail.com  yes  source of input (see 'show info' for details)

[recon-ng][osint][pwnedlist] > 

```

اگر هنوز گیج هستید، این چارچوب دستور دیگری برای توضیح دقیق‌تر درباره یک ماثول دارد:

[recon-ng] [osint] [pwnedlist] > show info

این دستور اطلاعات دقیق شامل نام مژاول، مسیر، نام نویسنده و توضیحات آن را ارائه می‌دهد. همان‌طور که در بالا ذکر شد ما نیاز به اضافه کردن SOURCE به عنوان ورودی برای اجرای این مژاول داریم و همچنین نوع ورودی مورد نیاز نیز در بخش پایین همان فایل ذکر شده است. ما می‌توانیم دستور مانند زیر را وارد کنیم:

```
[recon-ng] [osint] [pwnedlist] > set SOURCE google@gmail.com
```

این فرمان به عنوان یک ورودی مناسب و ارزشمند ارائه شده است. حالا دستور زیر برای اجرای این مأموریت بکار برده می‌شود:

[recon-ng] [osint] [pwnedlist] > run

```
File Edit View Search Terminal Help
[recon-ng][osint][pwnedlist] > set SOURCE google@gmail.com
SOURCE => google@gmail.com
[recon-ng][osint][pwnedlist] > run
[*] google@gmail.com => Pwned! Seen at least 27 times, as recent as 2014-08-28.

-----
SUMMARY
-----
[*] 1 total (0 new) items found.
```

شناسه فوق الذکر در جایی پنهان شده است. اگر می خواهیم از بعضی از ماثول های دیگر استفاده کنیم، می توانیم به راحتی از دستور "load" با نام ماثول برای بارگیری از آن استفاده کنیم.

ما به راحتی می‌توانیم از این ابزار استفاده کنیم. دستورات و رویکردها کاملاً یکسان باقی خواهند ماند. ابتدا مژول را جستجو، انتخاب و بارگیری کنید، فیلدهای آن را بررسی کنید، مقادیر را به فیلدهای موردنیاز بدھید و سپس آن را اجرا کنید. در صورت لزوم، فرآیند مشابهی را برای گسترش شناسایی تکرار می‌کنیم. اکنون اجازه دهید برخی از سناریوها و مژول‌هایی را که می‌تواند مفید باشند، بحث خواهیم کرد.

مورد ۱:

اگر ما بخواهیم پایگاه داده‌ای از مشتریان آینده را جمع‌آوری کنیم، مژول‌های خاص موجود را وجود دارد که بسیار مفید خواهند بود. اگر می‌خواهیم این اطلاعات را از سایت‌های شبکه‌های اجتماعی جمع‌آوری کنیم، LinkedIn تنها مکانی است که ما می‌توانیم نام دقیق و جزئیات دیگر را در مقایسه با سایت‌های دیگر که عموماً از نام مستعار تشکیل شده‌اند، دریافت کنیم و اگر ما فروشنده هستیم، ممکن است از پورتال‌هایی مانند Sales Force یا Jigsaw شنیده باشیم، جایی که می‌توانیم اطلاعاتی رایگان یا با پرداخت معقول از پول دریافت کنیم؛ و امروزه غالب فروش‌ها برایمیل متمرکز می‌شود؛ بنابراین گرفتن ایمیل‌های معتبر از یک سازمان هدف همیشه نیمی از کار برای تیم فروش است؛ بنابراین در اینجا در خصوص منابع موجود برای دریافت این اطلاعات و مژول‌های مربوط به آن را بحث خواهد کرد.

مژول‌های موجود:

- recon/companies-contacts/facebook
- recon/companies-contacts/jigsaw
- recon/companies-contacts/linkedin_auth

این‌ها برخی از مژول‌هایی هستند که می‌توانند برای جمع‌آوری اطلاعات مانند نام، موقعیت، آدرس و غیره مفید باشند.

اما آدرس‌های ایمیل، کلیدی برای تماس هستند؛ بنابراین اجازه دهید به برخی از گزینه‌های جمع‌آوری آدرس‌های ایمیل نگاه کنیم. ما می‌توانیم برخی از جزئیات شناسه ایمیل را از پایگاه داده Whois جمع‌آوری کنیم. موتورهای جستجو همچنین نقش مهمی در جمع‌آوری آدرس‌های ایمیل با استفاده از سرورهای PGP بازی می‌کنند.

مژول‌های موجود:

- recon/domains-contacts/pgp_search
- recon/domains-contacts/whois_pocs

مورد ۲:

ردیابی فیزیکی گوشی‌های هوشمند به‌طور عمدی و یا غیرمستقیم به کاربران اجازه می‌دهد موقعیت جغرافیایی خود را با اطلاعاتی که آن‌ها به سایت‌های عمومی مختلف مانند یوتیوب، پیکاسا و غیره آپلود می‌کنند، اضافه کنند. در این صورت می‌توانیم با کمک رسانه‌های برچسب‌گذاری شده، اطلاعات را جمع‌آوری کنیم. از آن می‌توان برای تجزیه و تحلیل رفتار، درک خواسته‌های فرد و ناسازگاری و غیره استفاده کرد.

ماژول‌های موجود:

- recon/locations-pushpins/flickr
- recon/locations-pushpins/picasa
- recon/locations-pushpins/shodan
- recon/locations-pushpins/twitter
- recon/locations-pushpins/youtube

مورد ۳:

اگر سازمان و یا شخصی بخواهد بررسی کند که آیا شناسه ایمیل شرکت و یا شخصی‌اش هک شده است، ماژول‌های خاصی وجود دارد که می‌تواند مفید باشد. همانند آنچه قبلاً در بالا به آن اشاره شد:

- recon/contacts-creds/pwnedlist
- recon/contacts-creds/haveibeenpwned
- recon/contacts-creds/should_change_password

مورد ۴:

برای تست نفوذ‌گران، این ابزار مانند گنجینه پنهانی است؛ زیرا می‌توانند ارزیابی پسیو را انجام دهند. اولین روش برای انجام هر آزمایش نفوذ، جمع‌آوری اطلاعات است. ما می‌خواهیم تست نفوذ وب را انجام دهیم و اولین چیزی که می‌خواهیم، این است که چه فناوری یا سرویس در حال اجرا است. ما می‌توانیم بعداً از آن‌ها بهره‌برداری کنیم. در این مورد، recon-ng دارای یک ماژول برای پیدا کردن جزئیات تکنولوژی است.

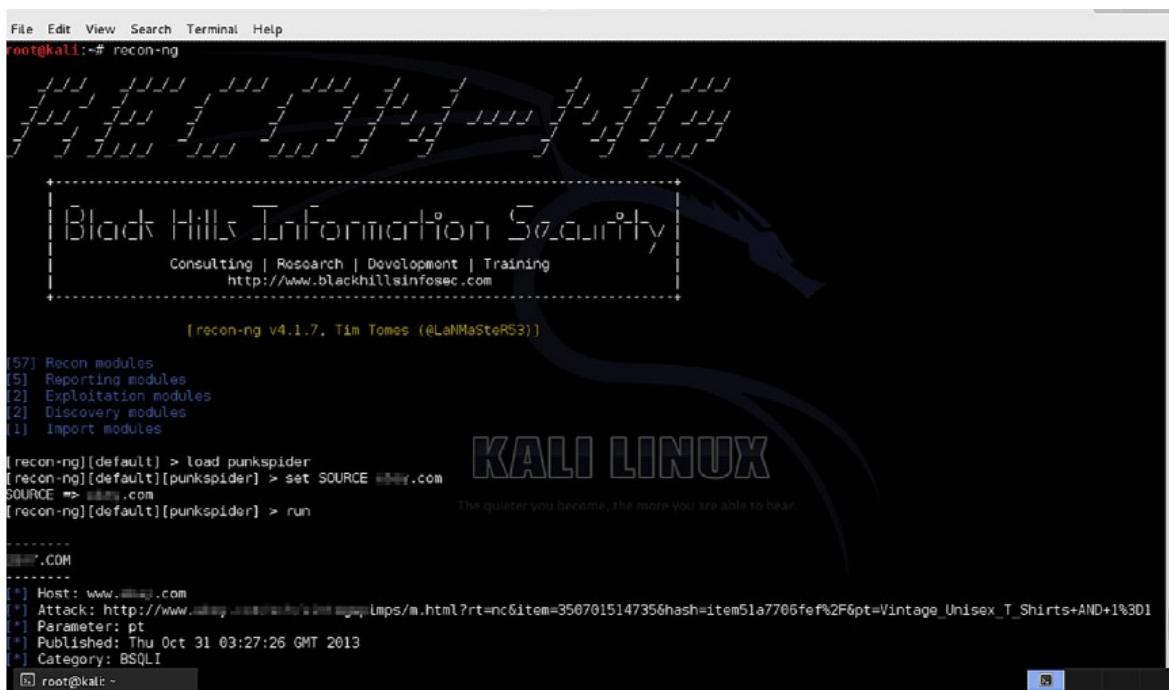
ماژول موجود:

- recon/domains-contacts/builtwith

پس از دریافت این جزئیات، به طور کلی به آسیب‌پذیری‌های موجود در شبکه مرتبط با آن فن‌آوری نگاه می‌کنیم؛ همچنین می‌توانیم به آسیب‌پذیری‌های مرتبط با آن دامنه نگاه کنیم که با استفاده از ماژول punkspider ممکن است. Punkspider با استفاده از یک اسکنر، وب را اسکن کرده و به جمع‌آوری آسیب‌پذیری‌های دقیق و ذخیره آن در پایگاه داده خود که می‌تواند مورد استفاده قرار گیرد، می‌پردازد.

ماژول‌های موجود:

- recon/domains-vulnerabilities/punkspider
- recon/domains-vulnerabilities/xssed



```
File Edit View Search Terminal Help
root@kali:~# recon-ng
[recon-ng v4.1.7, Tim Tomes (@LaNMaSteR53)]
[57] Recon modules
[5] Reporting modules
[2] Exploitation modules
[2] Discovery modules
[1] Import modules
[recon-ng][default] > load punkspider
[recon-ng][punkspider] > set SOURCE www.blackhillsinfosec.com
SOURCE => www.blackhillsinfosec.com
[recon-ng][punkspider] > run
[recon-ng][punkspider] >
[recon-ng][punkspider] > .COM
[*] Host: www.blackhillsinfosec.com
[*] Attack: http://www.blackhillsinfosec.com/m.html?rt=nc&item=3507015147356hash=item51a7706fef%2F&pt=Vintage_Unisex_T_Shirts+AND+1%3D1
[*] Parameter: pt
[*] Published: Thu Oct 31 03:27:26 GMT 2013
[*] Category: BSQLI
[recon-ng][punkspider] >
[recon-ng][punkspider] > root@kali:~
```

در تست نفوذ شبکه، پورت اسکن یک‌چیز مهم است و این چارچوب دارای ماژول‌هایی برای انجام اسکن پورت می‌باشد.

ماژول موجود:

- recon/netblocks-ports/census_2012

به غیر از این، ماثولهای بهره‌برداری مستقیم نیز وجود دارد مانند:

- exploitation/injection/command_injector
- exploitation/injection/xpath_bruter

ماژولهای مختلف برای انجام کارهای مختلف وجود دارند. یکی از مهم‌ترین کارها در میان آن‌ها سرقت اعتبار است. محققان هنوز هم در این پروژه مشارکت دارند و برنامه نویسان این ویژگی‌ها را گسترش می‌دهند. سهولت استفاده و ساختار ماثوله، این چارچوب را یکی از ابزارهای محبوب OSINT تبدیل کرده است.

YAHOO PIPES

برنامه‌ای منحصر به فرد از یاهو است که کاربر را قادر به انتخاب منابع اطلاعاتی مختلف با برخی قوانین سفارشی مطابق با الزامات خود برای تأمین فیلتر خروجی می‌کند. بهترین چیز در مورد این ابزار GUI cool است که در آن یک کاربر معمولی اینترنت نیز می‌تواند pipes خود را برای به دست آوردن اطلاعات مورد نظر از منابع مختلف ایجاد کند.

برای علاقه‌مندان OSINT، تنها چیزی که اهمیت دارد، اطلاعات موردنیاز است. اطلاعات در قسمت‌های مختلف وب وجود دارند. منابع مختلفی برای دریافت اطلاعات به‌طور مرتب وجود دارند. مشکل این است که چگونه اطلاعاتی را که در منابع متعدد ارائه شده، به دست آوریم. اگر ما اطلاعات موردنیاز را از طریق مجموعه‌ای از کارهای دستی به دست آوریم، نیاز به تلاش بسیار زیادی می‌باشد؛ بنابراین برای تسهیل روند این برنامه به ما بسیار کمک خواهد کرد. الزامات مورد نیاز آن عبارت‌اند از:

- ✓ یک مرورگر وب
- ✓ اتصال به اینترنت
- ✓ شناسه کاربری یاهو

بخار اینکه این ابزار یک برنامه وب است، می‌توانیم از هر نقطه به آن دسترسی داشته باشیم و استفاده از رابط کاربر پسند آن را قابل استفاده‌تر می‌کند. ما می‌توانیم از URL زیر استفاده کنیم.

<https://pipes.yahoo.com/>

از این URL دیدن کنید، با یاهو وارد شوید. یکی دیگر از نکات مهم این نرم‌افزار، مستندسازی درست آن است. به غیر از این می‌توانیم پیوندهایی به آموزش‌های مختلف (متن و همچنین ویدئو) را در سایت ببینیم که چگونه می‌توانیم شروع کنیم و دیگر موارد پیشنهادی. علاوه بر این برای هدف خاص، پیوندهای از popular pipes وجود دارند. بیایید pipe خودمان را بسازیم.

برای ایجاد یک pipe شخصی باید بر روی دکمه ایجاد pipe در برنامه کلیک کنید که به <http://pipes.yahoo.com/pipes/pipe.edit> هدایت خواهد شد.

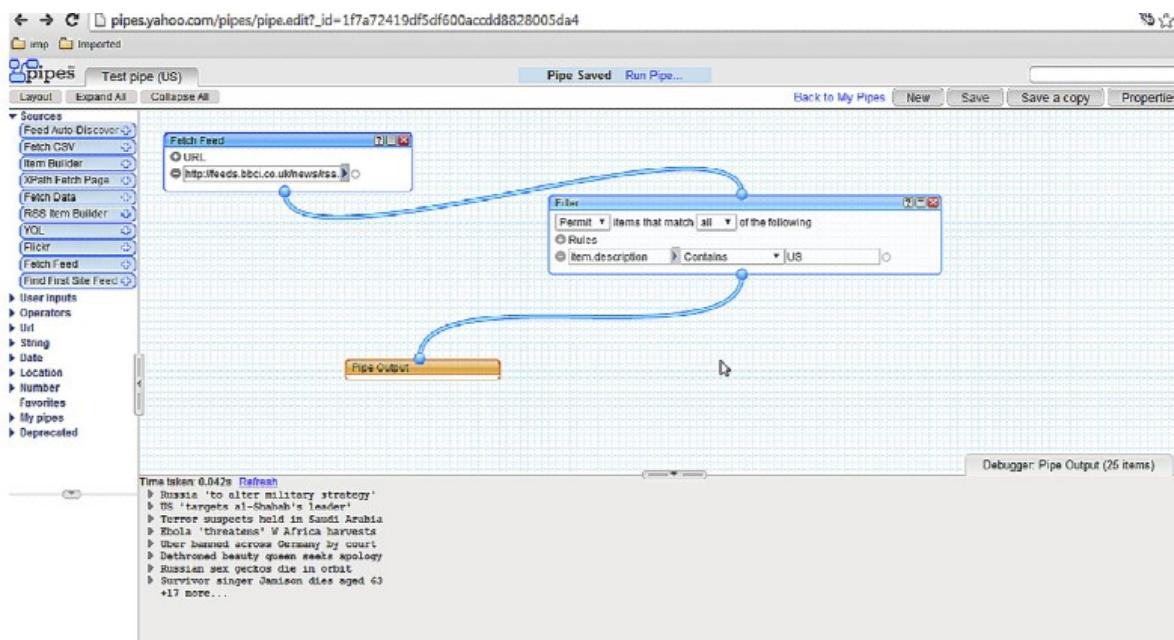
در گوشه سمت راست بالا می‌توانیم زبانه‌هایی مانند new و properties را پیدا کنیم. به‌طور پیش فرض هیچ کار ضروری برای انجام با این زبانه‌ها وجود ندارد. برای ایجاد یک pipe جدید، در سمت چپ از ما زبانه‌ها مختلفی از جمله operators ، user inputs و sources و URL وجود دارد.

این‌ها زبانه‌هایی هستند که ما می‌توانیم از آن‌جا ماثول‌ها را برای طراحی pipe استفاده کنیم. اساساً یک pipe با یک و یا چندین منبع شروع می‌شود. سپس نیاز به ایجاد برخی از فیلترهای مورد نیاز با استفاده از اپراتورها مانند تاریخ، محل وغیره وجود دارد و پس از آن نیاز به اضافه کردن خروجی برای دریافت اطلاعات مورد نظر فیلتر شده است.

بنابراین برای شروع اجازه دهید تا یک منبع از sub source بکشیم، گزینه‌های مختلف در دسترس مانند CSV، Fetch feed و غیره وجود دارد. اجازه دهید از فیلدهای واکشی به عنوان یک منبع بسیار خوبی از اطلاعات استفاده کنیم. Fetch Feed sub tab را به مرکز برنامه بکشید. وقتی هر چیزی را به مرکز می‌کشیم، یک جعبه خروجی برای ما تولید و از ما می‌خواهد که URL feed را اضافه کنیم. ما از URL به صورت edition=int!<http://feeds.bbci.co.uk/news/rss.xml> استفاده می‌کنیم.

برای انجام آزمایش، فقط یک نمونه منبع را نشان می‌دهیم، اما می‌توانیم چندین منبع را نیز برای یک pipe اضافه کنیم. در حال حاضر بسیار مهم است که یک فیلتر مناسب ایجاد کنیم که خروجی مناسب را به ما می‌دهد. اکنون filter sub tab را از برگه Operators بکشید. به‌طور پیش فرض contains و برخی فضاهای خالی برای پر کردن وجود دارند. Permit را به all تغییر دهید و در اولین فضای خالی "contains" را همراه با US (ایالات متحده) اضافه کنید؛ بنابراین فیلتر، داده‌هایی را در اختیار شما قرار می‌دهد که در «توضیحات مورد نظر» کلمه کلیدی «آمریکا» داشته باشد.

جمع‌آوری هوشمند اطلاعات



در حال حاضر pipe را از Pipe Output box به Filters box و Fetch Feed box متصل کنید. ابتدا pipe را ذخیره و سپس آن را اجرا کنید تا خروجی را در برگه جدید دریافت کنید.

ما می‌توانیم سناریوهای دیگر مانند جمع‌آوری تصاویر از یک فرد خاص از flicker استفاده کنیم، اطلاعات را از طریق URL، تاریخ و محل سکونت و بسیاری دیگر فیلتر کنیم. این کار را ممکن است با pipe های سفارشی ایجاد کنید. این ابزار آزادی لازم برای ایجاد pipe ها فراتر از تخیل ما را فراهم می‌کند.

MALTEGO

ابزار OSINT زیادی در بازار وجود دارند، اما یکی از بهترین ابزار به دلیل قابلیت‌های منحصر به فردش، Maltego است. برنامه OSINT است که پلتفرمی را فراهم می‌کند که نه تنها اطلاعات را استخراج، بلکه این داده‌ها را در یک فرمت که به آسانی قابل درک و تجزیه و تحلیل است، نشان می‌دهد. این سرویس یکپارچه برای بسیاری از نیازها، مجتمع است و به کاربران امکان می‌دهد تا افزودنی‌های سفارشی برای پلتفرم (که ما بعداً آن را مورد بحث قرار می‌دهیم) بسته به نیاز ایجاد کنند.

در حال حاضر Maltego در دو نسخه در دسترس است: تجاری و عمومی. نسخه تجاری پولی است و نیاز به یک کلید مجوز برای آن داریم. نسخه عمومی رایگان است و فقط نیاز به ثبت‌نام در سایت وجود دارد. اگرچه نسخه عمومی دارای محدودیت‌هایی در مقایسه با نسخه تجاری مانند محدودیت در استخراج اطلاعات، پشتیبانی از کاربر وغیره است، اما هنوز هم خوب است که قدرت این ابزار عالی را احساس کنید. در طول این فصل از نسخه عمومی برای اهداف آزمایشی استفاده می‌کنیم. بیایید بینیم این ابزار چگونه کار می‌کند و چگونه می‌توانیم از آن استفاده کنیم.

اولاً برخلاف بسیاری از نرم‌افزارهای کاربردی که برای این منظور استفاده می‌شوند، Maltego یک رابط کاربری گرافیکی را فراهم می‌کند. این ابزار اساساً بر روی معماری سرویس گیرنده-سرور^۱ کار می‌کند، بدین معنا که آنچه ما به عنوان یک کاربر می‌گیریم، یک سرویس گیرنده Maltego است که برای انجام عملیات خود، با یک سرور ارتباط برقرار می‌کند. قبل از هر چیز، بلوک‌های ساختمان Maltego در زیر ذکر شده‌اند.

ENTITY

Entity یک قطعه داده است که به عنوان ورودی به منظور استخراج اطلاعات بیشتر گرفته می‌شود. Maltego قادر به گرفتن یک واحد یا گروهی از آن‌ها به عنوان ورودی برای استخراج اطلاعات است. آن‌ها توسط آیکون‌ها بر اساس نامشان نشان داده می‌شوند. به عنوان مثال Entity دامنه xyz.com توسط آیکونی مانند جهان نشان داده شده است.

TRANSFORM

¹ client-server

یک تکه از کد است که یک Entity (یا گروهی از آنها) را به عنوان ورودی می‌گیرد و داده‌ها را به صورت Entity (ها) را بر اساس رابطه استخراج می‌کند. به عنوان مثال DomainToDNSNameSchema که این NameSchema مختلف را علیه یک دامنه (entity) تست کند.

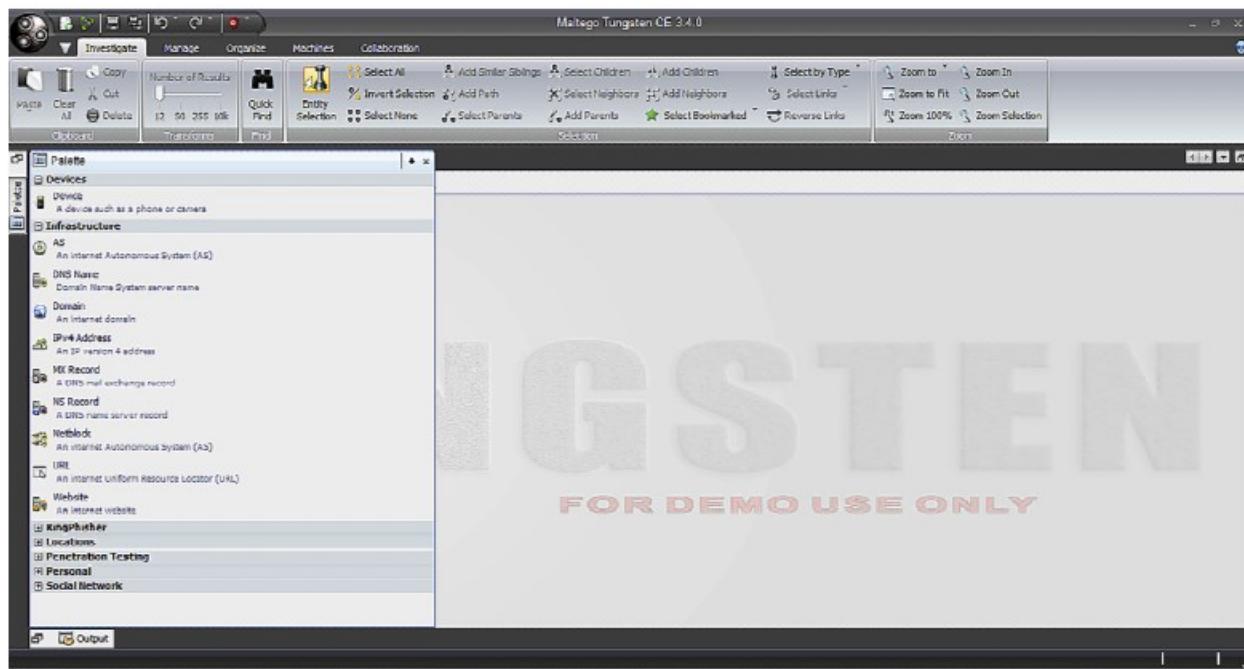
MACHINE

یک machine اساساً مجموعه‌ای از transforms برنامه‌نویسی است. یک machine در مواردی که داده‌های اولیه (به شکل یک Entity) و داده‌های خروجی مورد نظر به طور مستقیم از طریق یک transform ارتباطی ندارند، بسیار مفید است که می‌توان از طریق یک سری تغییرات به صورت سفارشی رديابی شوند. به عنوان مثال Footprint L1: تبدیلی است که یک دامنه را به عنوان ورودی می‌گیرد و انواع مختلفی از اطلاعات مرتبط با سازمان را ایجاد می‌کند مانند ایمیل،¹ AS و غیره.

ابتدا همان‌طور که در بالا ذکر شد، باید یک حساب کاربری برای نسخه عمومی ایجاد کنیم. هنگامی که ما یک حساب کاربری داریم و باید آن را از <https://www.pater va.com/web6/products/download3.php> دانلود کنیم. نصب برنامه بسیار ساده است و تنها نیاز به جواودارد. هنگامی که نصب کامل شد، فقط نیاز به باز کردن برنامه و ورود با استفاده از اعتبار ایجادشده در طول روند ثبت‌نام دارد.

اکنون که فرآیند نصب و راه‌اندازی کامل شد، اجازه دهید به رابط Maltego برویم و در ک کنیم که چگونه کار می‌کند. هنگامی که به برنامه وارد شده‌اید، ما با یک گراف خالی شروع می‌کنیم تا بتوانیم برنامه را از ابتدا در ک کنیم. در حال حاضر Maltego یک صفحه خالی با گزینه‌های مختلف در نوار بالا و یک نوار در سمت چپ ارائه می‌دهد. این واسطی است که ما روی آن کار خواهیم کرد.

¹ Autonomous System



در گوشه بالا سمت چپ، لوگوی Maltego است، با کلیک کردن بر روی آن گزینه‌هایی برای ایجاد یک گراف جدید، ذخیره نمودار، تنظیمات واردات / صادرات و غیره فهرست می‌شود. نوار بالا، گزینه‌های متعددی را ارائه می‌دهد بگذارید آنها را با جزئیات درک کنیم.

INVESTIGATE

این اولین گزینه در نوار بالا است که توابع اساسی مانند برش، کپی، چسباندن، جستجو، انتخاب پیوند / نهاد را فراهم می‌کند. یکی از گزینه‌های مهم ارائه شده توسط آن Select by Type است، این گزینه‌ها زمانی که مقدار زیادی از اطلاعات موجود در نمودار وجود داشته باشد پس از اجرای مجموعه‌ای متفاوت از transform ها و machine ها و وقتی ما به دنبال نوع خاصی از داده‌ها هستیم، مفید است.

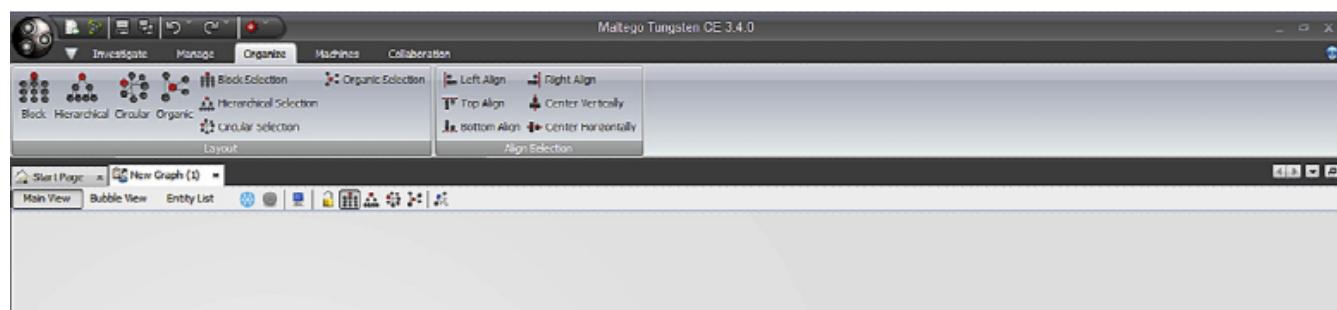
MANAGE

گزینه Manage به طور عمده به مدیریت entity و transform با برخی از توابع جزئی دیگر مانند یادداشت‌ها و ترتیبات پانل‌های مختلف می‌پردازد. در زیر برگه Entities گزینه‌هایی برای ایجاد، مدیریت و واردات / صادرات entity ها وجود دارد. به همین ترتیب برگه Transform گزینه‌هایی را برای ایجاد، مدیریت و ایجاد Transform های محلی جدید ارائه می‌دهد (درباره ایجاد Transform محلی در فصل بعد بحث خواهیم کرد).



ORGANIZE

هنگامی که استخراج داده‌ها انجام شود، باید گراف برای درک بهتر آن تنظیم کنیم، این جایی است که گزینه Organize وارد می‌شوند. با استفاده از گزینه‌های زیر می‌توانیم طرح گراف کامل را انتخاب کنیم entity‌ها به اشکال مختلف مانند سلسله مراتبی، مدور، بلوک و غیره نشان داده می‌شوند. همچنین می‌توانیم هماهنگ‌سازی entity‌ها را با استفاده از توابع در برگه Align Selection تنظیم کنیم.



MACHINES

همان‌طور که قبلاً توضیح داده شد، machine‌ها بخش جدایی‌ناپذیر از برنامه هستند. زبانه Machines گزینه‌هایی را برای اجرای یک ماشین فراهم می‌کند، تمام machine‌ها در یک زمان متوقف می‌کند، machine‌ها جدیدی را ایجاد می‌کنند (که ما در فصل بعد بحث خواهیم کرد) و برای مدیریت آن‌ها استفاده می‌شود.

COLLABORATION

این برگه برای استفاده از ویژگی‌های معرفی شده در آخرین نسخه Maltego است که اجازه می‌دهد تا کاربران مختلف به عنوان یک تیم کار کنند. با استفاده از گزینه‌های آن، کاربران می‌توانند نمودارهای خود را با دیگر کاربران به اشتراک گذاشته و همچنین از طریق چت ارتباط برقرار کنند. این ویژگی در محیط‌های تیمی بسیار مفید است.

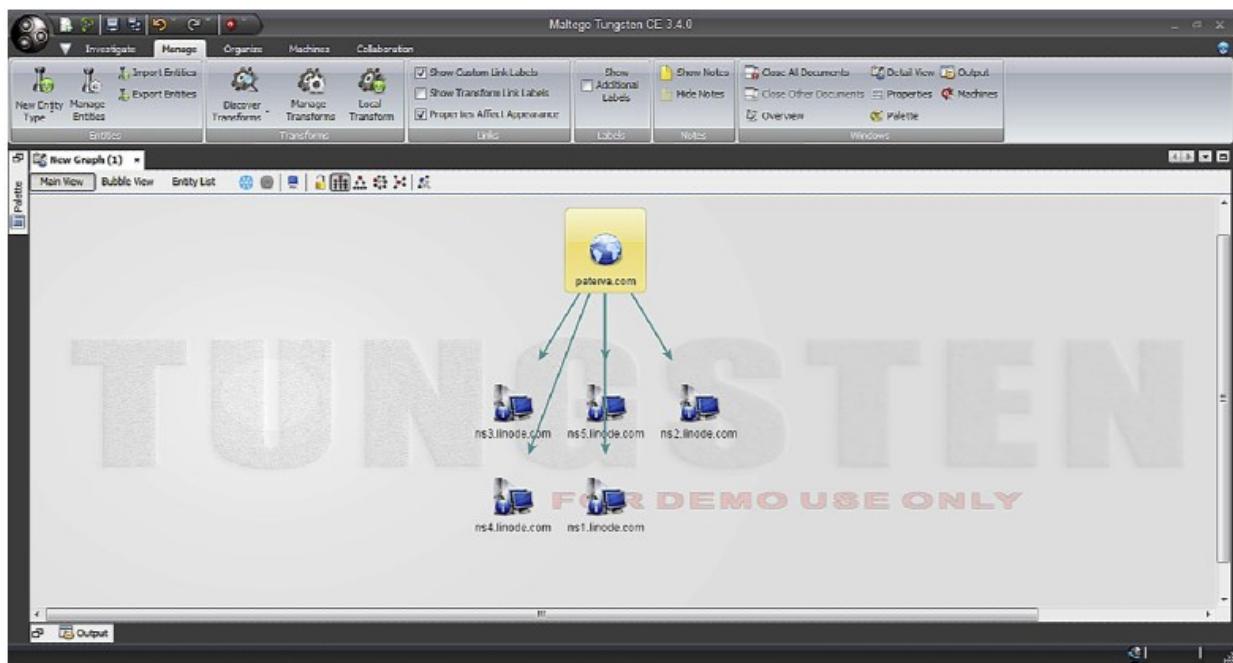
نوار سمت چپ برای فهرست انواع مختلف entity ها در Maltego استفاده می‌شود. entity های ذکر شده بر اساس دامنه خود دسته‌بندی می‌شوند. در حال حاضر Maltego به طور پیش فرض بیشتر از بیست entity را فراهم می‌کند. اکنون با رابط کاربری آشنا هستیم و می‌توانیم به کار کردن با Maltego ادامه دهیم.

اول از همه برای شروع Maltego به یک entity پایه نیاز داریم. برای آوردن یک entity به نمودار، فقط نیاز به کشیدن و رها کردن نوع entity ای از نوار سمت چپ داریم که باید از آن شروع کنیم. هنگامی که موجودیت را در نمودار داریم، می‌توانیم دو بار بر روی نام نهاد کلیک کنیم تا پارامترهای آن را به میلمان تغییر دهیم یا با کلیک بر روی آیکون entity که پنجره جزئیات را باز می‌کند می‌توانیم داده‌ها را تغییر و یا ایجاد و یا در مورد این entity، یک تصویر را ضمیمه کنید و غیره.

هنگامی که پارامترهای یک نهاد را تعیین کردیم، باید بر آن entity راست کلیک کرده و Transform هایی که برای آن نوع خاص مشخص شده‌اند را بررسی کنیم. در برگه Run Transform می‌توانیم All Transforms را در بالای صفحه بینیم که تمام Transform های موجود را بر اساس entity خاص لیست می‌کند. در زیر این برگه می‌توانیم زبانه‌های مختلفی را مشاهده کنیم که حاوی Transform های طبقه‌بندی شده در دسته‌های مختلف است. آخرین برگه All Transforms است، با استفاده از آن تمام Transform های ذکر شده در یک‌بار اجرا می‌شوند. این کار زمان و منابع زیادی را اتخاذ می‌کند و ممکن است به مقدار زیادی از داده‌ها منجر شود که مانع خواهیم.

حالا بگذارید مثال یک دامنه را ساخته و برخی Transform ها را اجرا کنیم. برای انجام این کار به سادگی domain را از نوار چپ به صفحه نمودار بکشید و رها کنید. اکنون بر روی برچسب entity دو بار کلیک کنید و آن را به google.com تغییر دهید. حالا بر روی آن راست کلیک کرده و به DNS Name - NS بروید و All Transforms را انتخاب کنید. این Transform اسم سرور را برای دامنه پیدا خواهد کرد. هنگامی که تبدیل را انتخاب می‌کنیم، می‌توانیم بینیم که نتایج بر روی صفحه گراف شروع به اضافه شدن می‌کنند. نوار پیشرفت در پایین رابط نشان می‌دهد که آیا تبدیل کامل شده یا هنوز اجرا می‌شود. حالا می‌بینیم که Maltego یک رکورد نام (server name) را برای دامنه پیدا کرده است. ما می‌توانیم تمام سوابق ذکر شده NS را انتخاب کنیم و یک Transform سرور (NS) را برای آنها انتخاب کرد. برای انجام دهیم، برای انجام این کار به سادگی، منطقه حاوی تمام رکورد را انتخاب و برای انتخاب واحد را روی آنها انجام دهیم. برای انجام این کار به سادگی، منطقه حاوی تمام رکورد را انتخاب کرده و برای انتخاب یک Transform کلیک راست کنید. بیایید "To Netblock [Blocks delegated to this NS]" را انجام دهیم. این Transform بررسی خواهد کرد که آیا رکورد NS دارای netblocks delegated است. در پنجره گراف می‌توانیم در

بالای صفحه بینیم که برخی از گزینه‌های مانند Bubble View وجود دارد که نشان می‌دهد که نمودار به عنوان یک نمودار شبکه اجتماعی با بسته به اندازه entity‌ها و تعداد لبه‌های ورودی و خروجی است؛ فهرست entity‌ها، لیست همهٔ موجودات در نمودار را نشان می‌دهد.



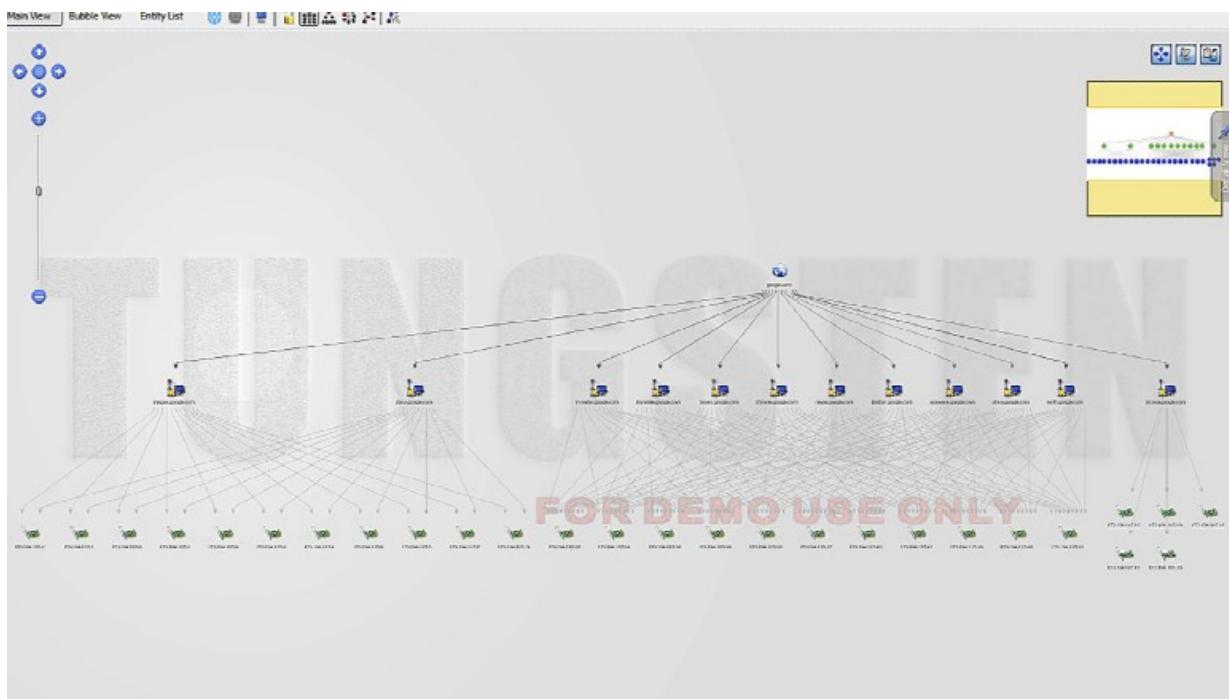
همچنین می‌توانیم یک ماشین را اجرا کنیم. یک دامنه با مقدار google.com ایجاد کنید. حالا به‌سادگی بر روی آن کلیک راست کرده، به برگه Run Machines بروید و machine را انتخاب کنید. برای این مثال، بگذارید برای راحتی L1 Footprint را اجرا کنیم. این footprint یک machine پایه را بر روی دامنه ارائه شده، انجام می‌دهد. هنگامی که این machine به‌طور کامل اجرا شو، یک گراف با نهادهای مختلف مانند سرورهای نام، آدرس‌های IP، وب‌سایت‌ها، شماره‌های AS و غیره نمایش داده می‌شود. اکنون برخی از سناریوهای خاص برای استخراج داده‌ها را مشاهده می‌کنیم.

تبديل دامنه به آدرس IP وب‌سایت

یک domain entity ایجاد کرده و "To Website DNS [using Search Engine]" را اجرا کنید. این یک جستجو در موتور جستجو برای وب‌سایت‌ها است و پاسخ را به عنوان website entities نمایش می‌دهد. اکنون تمام website entities را بعد از اجرای Transform انتخاب کرده و "To IP Address [DNS]" را انجام دهید. این به‌سادگی یک DNS را اجرا و آدرس‌های IP وب‌سایت‌ها را دریافت می‌کند. این توالی Transform‌ها می‌تواند به ما در

در کم محدوده IP متعلق به سازمان (مالک دامنه) کمک کند. همچنین می‌توانید بینید که کدام وبسایت‌ها دارای چندین آدرس IP اختصاص یافته هستند. اطلاعاتی مانند این برای یک عمق عمیق حیاتی است.

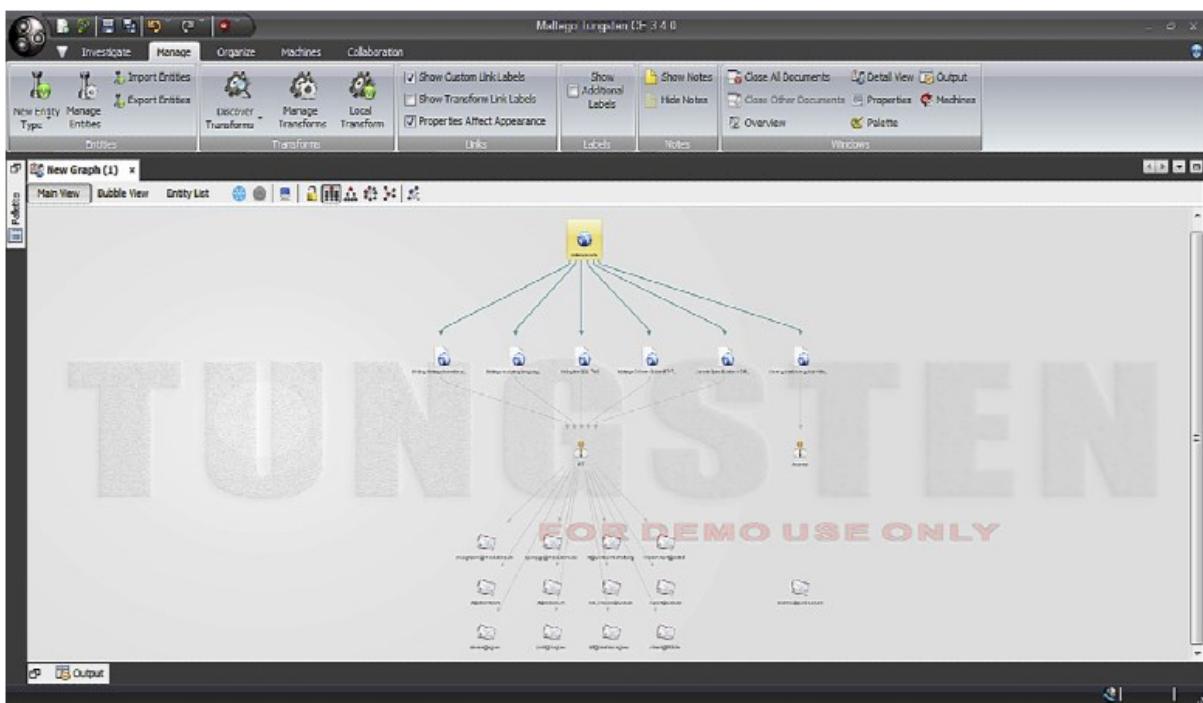
مثال: دامنه = google.com



تبديل دامنه به آدرس پست الکترونیکی

یک مجموعه از Transform‌ها برای استخراج آدرس ایمیل به‌طور مستقیم از یک دامنه وجود دارد، اما برای این مثال، ما یک روش متفاوت را با استفاده از فرادراده دنبال خواهیم کرد. باید مجدداً یک دامنه را در نظر بگیریم و "Files and Documents from Domain." را انجام دهیم؛ بنابراین فایل‌هایی در دامنه لیست شده، جستجو خواهد شد. هنگامی که یک دسته از فایل‌ها را می‌گیریم، می‌توانیم آن‌ها را انتخاب و "Parse meta information." را انجام دهیم. این Transform فرادراده را از فایل‌های ذکر شده استخراج می‌کند. اکنون همه Transform‌ها را در مجموعه "Email addresses from person" بر روی نهادها و دامنه مناسب (دامنه‌ای که آدرس ایمیل مورد نظر در آن است) انجام دهیم. ما می‌توانیم نتیجه این Transform پایانی را بینیم و آن را با نتیجه اجرای Transform استخراج مستقیم ایمیل در دامنه مقایسه کنیم و بینیم که نتایج متفاوت هستند.

به عنوان مثال: Domain = paterva.com



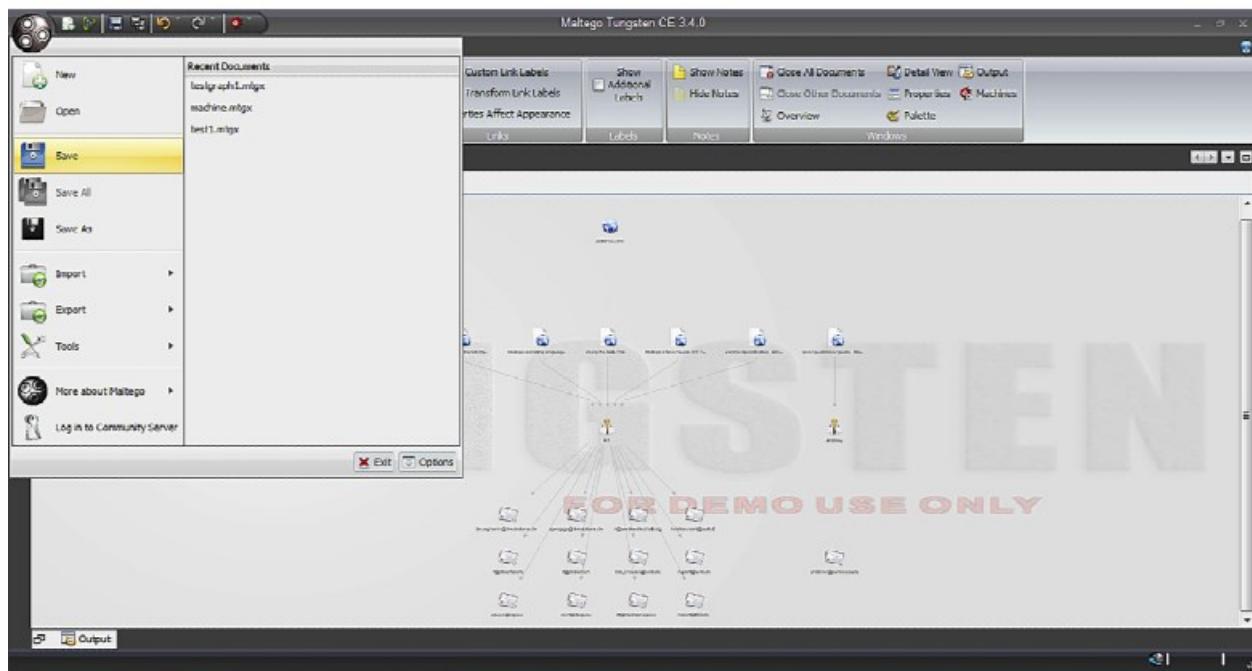
تبديل فرد به وبسایت

برای این مثال، ما از "Person - Email address" استفاده خواهیم کرد. بیاید یک entity person بگذاریم و مقدار Andrew MacPherson را به آن اختصاص دهیم و machine را در این entity اجرا کنیم. هنگامی که مجموعه‌ای از Transform شناسه‌های مربوط به ایمیل با استفاده از Transform های مختلف می‌کند. گزینه‌ای برای entity های انتخاب شده که تا کنون ثبت شده است، فراهم می‌کند. از مثال بالا ما اجرا شدند، گزینه‌ای برای entity های انتخاب شده که تا کنون ثبت شده است، فراهم می‌کند. از مثال بالا ما می‌دانیم andrew@punks.co.za یک آدرس ایمیل معتبر است، بنابراین تنها با این entity خاص می‌رویم. آنچه ما به عنوان یک نتیجه نهایی به دست می‌آوریم، وبسایت‌هایی هستند که این آدرس خاص را می‌سازند، با اجرای

.“To Website [using Search Engine]”

این‌ها نمونه‌هایی بودند که به‌وضوح نشان‌دهنده قدرت این ابزار پیچیده‌اند. استخراج یک نوع خاص از داده از نوع داده‌های دیگر می‌تواند به روش‌های مختلف (با استفاده از سری‌های مختلف از Transform ها) انجام می‌شود. بهترین راه برای رسیدن به آنچه ما می‌خواهیم این است که مجموعه‌ای از Transform ها را انجام دهیم، داده‌های موردنیازمان را به دست آورده، سپس به ترتیب Transform ها را به صورت همزمان اجرا کنیم. این تمرین نه تنها کمک می‌کند تا اعتبار اطلاعاتی که دریافت کرده‌ایم را تائید کنیم، بلکه گاهی اوقات اطلاعات منحصر به فرد را نیز تولید می‌کند.

Maltego حتی اجازه می‌دهد که گرافی که ما در یک فایل واحد در قالب mtgx تولید کرده‌ایم را برای استفاده به اشتراک گذاری بعدی ذخیره کنیم. این ویژگی به ما اجازه می‌دهد که محیط سفارشی را با دیگران به اشتراک بگذاریم و حتی از ماشین‌های مختلف استفاده کنیم.



به غیر از طراحی پیش‌ساخته، Maltego به ما اجازه می‌دهد تا تغییرات خودمان را ایجاد کنیم. این ویژگی به ما اجازه می‌دهد ابزار را سفارشی کنیم تا داده‌ها را از منابع مختلف دیگر استخراج کنیم که برای هدف خاص مفید می‌باشد، به عنوان مثال یک API که اجازه می‌دهد نام شرکت را از شماره تلفن دریافت کنیم.

برای تبدیل سفارشی دو گزینه داریم:

Local transforms: این Transform‌ها به صورت محلی در دستگاهی که مشتری در حال اجرا است، ذخیره می‌شود. آن‌ها برای ایجاد و استقرار ساده هستند. نکته مهم این است که اگر بخواهیم آن را بر روی دستگاه‌های مختلف اجرا کنیم، باید آن‌ها را به طور جداگانه بر روی هر یک از آن‌ها نصب کنیم و همین امر برای به روز رسانی هاست.

TDS transforms: TDS مخفف سرور توزیع شده تبدیل^۱ است که یک برنامه وب است که اجازه توزیع و همچنین مدیریت Transform‌ها را می‌دهد. مشتری به سادگی TDS را بررسی می‌کند و Transform‌ها را فراخوانی می‌کند. در مقایسه با Transform‌های محلی، آن‌ها به راحتی راه‌اندازی و به روز رسانی می‌شوند.

^۱ transform distribution server

ما خواهیم آموخت که چگونه در فصل بعد تغییرات را ایجاد کنیم؛ بنابراین این‌ها بعضی از ابزارهایی هستند که می‌توانند بخش مهمی از اطلاعات را جمع‌آوری کنند. بعضی از این‌ها بیشتر بر امنیت اطلاعات متمرکز هستند و بعضی از آن‌ها عمومی هستند. در اینجا مهم است که ابزارهای متعددی وجود دارد که می‌تواند به ما کمک کنند تا اطلاعات مربوطه را در عرض چند دقیقه استخراج کنیم و در صورتی که به طور مناسب و با کارایی مورد استفاده قرار گیرند این ابزارها می‌توانند در فرایند استخراج داده‌ها نقش مهمی را بازی کنند. در فصل بعد ما در مورد دنیای هیجان‌انگیز فراداده‌ها یاد خواهیم گرفت. با موضوعاتی مانند فراداده، چگونگی مفید بودن آن، چگونگی استخراج آن و غیره رویرو خواهیم شد. همچنین با موضوعاتی مانند چگونگی استفاده از آن بر علیه مان و نحوه جلوگیری از این اتفاقات آشنا خواهیم شد.

فصل ۷: فراداده^۱

مقدمه

در چند فصل اخیر ما به‌طور گستره‌ای در مورد چگونگی پیدا کردن اطلاعات آنلайн آموخته‌ایم. ما درباره موتورهای جستجو و تکنیک‌های مختلف برای استفاده بهتر از آنها و همچنین ابزارهایی که می‌توانند فرایند استخراج داده‌ها را خودکار کنند، یاد گرفتیم. در این فصل با نوع خاصی از داده روبرو خواهیم شد که بسیار متفاوت بوده اما معمولاً نادیده گرفته می‌شوند.

فراداده پیش از این تنها اصطلاحی بود که تنها در حوزه علوم اطلاعات در مورد آن صحبت شده بود، اما با انتشار اخبار اخیر که نشان می‌دهد آژانس امنیت ملی فراداده‌هایی راجع به سوابق تلفن‌های شهرورندانش را مورد سوءاستفاده قرار داده است، به یک موضوع شناخته شده تبدیل شد. اگر چه هنوز بسیاری از مردم دقیقاً نمی‌دانند که فراداده چیست و چگونه می‌توان از آنها استفاده کرد و چگونه از دیدگاه امنیت اطلاعات می‌توانیم خودمان را حفظ کنیم.

تعریف اساسی فراداده "اطلاعات مربوط به داده‌ها" است، اما گاهی اوقات کمی گیج کننده است؛ بنابراین برای درک بهتر می‌توانیم بگوییم که فراداده چیزی است که محتوای داده را به نحوی توصیف می‌کند، اما بخشی از محتوای آن نیست. به عنوان مثال در یک فیلم ویدئویی طول ویدیو می‌تواند فراداده باشد که نشان می‌دهد چه

^۱ METADATA

مدت زمان ویدئو پخش خواهد شد، اما این بخشی از خود ویدیو نیست. به طور مشابه برای یک فایل تصویری، مشخصات دوربین روی آن عکس، می‌تواند فراداده‌ی آن باشد یا زمانی گفتن تصویر که در واقع محتوای تصویر نیست. همه ما با این نوع داده‌ها در برخی موقع مواجه شده‌ایم. فراداده می‌تواند هر چیزی باشد، نام تولید کننده محتوا، زمان ایجاد، اطلاعات کپیرایت و غیره.

ایجاد فراداده عمدهاً مدت‌ها قبل در کتابخانه‌ها آغاز شده بود، زمانی که افراد اطلاعاتی در قالب کتیبه‌ها داشتند که راهی برای طبقه‌بندی و پیدا کردن آن‌ها در زمان نیاز بود. امروزه در عصر دیجیتال ما همچنان از فراداده‌ها برای دسته‌بندی، جستجو، اتصال فایل‌ها و خیلی بیشتر استفاده می‌کنیم. اکثر فایل‌هایی که در سیستم‌های رایانه‌ای ما وجود دارند نوعی فراداده دارند. همچنین یکی از اجزای کلیدی موردنیاز برای ایجاد وب معنایی است.

فراداده در مدیریت و سازماندهی فایل‌ها بسیار مفید است و از این رو امروزه به‌طور گسترده‌ای مورد استفاده قرار می‌گیرد. اغلب موارد ما حتی بین محتوای واقعی و فراداده‌ای آن تمایزی نمی‌بینیم. آن‌ها معمولاً به فایل توسط نرم‌افزار پایه‌ای که برای ایجاد فایل استفاده می‌شود، اضافه می‌شوند. برای یک تصویر می‌تواند دوربین، برای یک فایل docx می‌تواند سیستم‌عامل مورد استفاده و برای یک فایل صوتی می‌تواند دستگاه ضبط باشد. معمولاً این بی‌عیب و نقص است زیرا داده‌ای را که می‌تواند از دیدگاه امنیت اطلاعات حساس باشد، آشکار سازد.

تعداد زیادی از مکان‌هایی که در آن از فراداده استفاده می‌شود، از فایلی در سیستم‌های ما تا وب‌سایت‌های اینترنتی وجود دارد. در این فصل، ما عمدهاً بر استخراج فراداده از مکان‌هایی که از دیدگاه امنیت اطلاعات حیاتی هستند، تمرکز می‌کنیم.

ابزار استخراج فراداده

در مورد برخی از ابزارهایی که می‌توان برای استخراج فراداده استفاده کرد، بحث می‌کنیم.

JEFFREY'S EXIF VIEWER

Exif^۱ (فرمت تصویر قابل تبادل) اساساً یک استاندارد است که توسط دستگاه‌هایی که تصاویر و فایل‌های صوتی را اداره می‌کنند مانند ویدیو، دوربین‌های تلفن هوشمند و غیره، استفاده می‌شود. شامل اطلاعاتی مانند رزولوشن تصویر، دوربین استفاده شده، نوع رنگ، فشرده‌سازی و غیره است. تلفن‌های هوشمند امروزی شامل یک دوربین،

^۱ exchangeable image file format

GPS و اتصال به اینترنت هستند. در بسیاری از گوشی‌های هوشمند زمانی که ما بر روی یک عکس کلیک می‌کنیم، به طور خودکار موقعیت جغرافیایی ما با استفاده از دستگاه GPS ثبت می‌شود. ما در شبکه‌های اجتماعی فعال هستیم و این تصاویر را با تمام جهان به اشتراک می‌گذاریم.

The screenshot shows the homepage of Jeffrey Friedl's Image Metadata Viewer. It features a search bar at the top with the URL "exif.regex.info/exif.cgi". Below the search bar is a "reCAPTCHA" verification box. A sidebar on the right contains links to "Some of my other stuff" such as "My Blog", "Lightroom plugins", "Pretty Photos", and "Photo Tech". The main content area includes fields for "URL" and "File", and a "View Image Data" button.

This tool remains available so long as I can keep it free and the bandwidth doesn't cost me too much. A gift of thanks is always appreciated, but certainly not required. [Send a gift via PayPal](#), or perhaps an Amazon gift certificate (to: jfriedl@yahoo.com), or perhaps send me some good karma by doing something kind for a stranger.

If you have questions about this tool, please [see the FAQ](#).

Works with these file types: 3FR, 3G2, 3GP, 3GP2, 3GPP, A, AA, AAE, AAX, ACMF, ACR, AFM, AI, AIF, AIFC, AIFF, AIT, AMFM, APE, APNG, ARW, ASF, AVI, AZW, AZW3, BMP, BPG, BTF, CHM, CIFF, COS, CR2, CR3, CRM, CRW, CS1, DC3, DCM, DCP, DCR, DFONT, DIB, DIC, DICM, DIVX, DV, DIVU, DLL, DNG, DOC, DOCM, DOCX, DOT, DOTM, DOTX, DPX, DR4, DS2, DSS, DV, DVB, DVR-MS, DYLIB, EIP, EPS, EPS2, EPS3, EPSF, EPUB, ERF, EXE, EXIF, EXR, EXV, F4A, F4B, F4P, F4V, FFF, FLA, FLAC, FLIF, FLIR, FLV, FP, FPX, GIF, GPR, GZ, GZIP, HDR, HEIC, HEIF, HTM, HTML, ICAL, ICO, ICM, ICS, IDML, IQ, IND, INDD, INDT, INX, ISO, ITC, J2C, J2K, JNG, JP2, APNG, Animated Portable Network Graphics, KDC, KEY, KTH, LA, LFF, LFR, LNK, M2T, M2TS, M4V, M4A, M4B, M4P, M4V, MAX, MEF, MIE, MIF, MIFF, MKRA, MKRS, MKV, MNG, MOBI, MODD, MOI, MOS, MOV, MP3, MP4, MPC, MPEG, MP6, MPO, MQV, MRW, MTS, MXF, NEF, NEWEK, NMNITEMPLATE, NKW, NUMBERS, O, ODB, ODC, ODF, ODG, ODI, ODP, ODS, ODT, OFR, OGG, OGV, OPUS, ORF, OTF, PAC, PAGES, PBM, PCD, PCT, PDB, PDF, PEF, PFA, PFB, PFM, PGF, PGM, PICT, PLIST, PAP, PNG, POT, POTM, POTX, PPM, PP5, PPSM, PPSS, PPT, PPTM, PPTX, PRC, PS, PS2, PS3, PSB, PSD, PSDT, PSP, PSPFRAME, PSPIMAGE, PSPSHAPE, PSPTUBE, QIF, QT, QTI, QTIF, R3D, RA, RAF, RAM, RAR, RAW, RIF, RIFF, RM, RMVB, RPM, RSRC, RTF, RV, RW2, RWL, RWZ, SEQ, SKETCH, SO, SR2, SRF, SRW, SVG, SWF, THM, THMX, TIF, TIFF, TORRENT, TS, TTC, TIF, TUB, VCARD, VCF, VOB, VRD, VSD, WAV, WDP, WEBM, WMA, WMV, WTV, WV, X3F, XCF, XHTML, XLA, XLAM, XLS, XLSB, XLSM, XLSX, XLT, XLTM, XLTX, XMP, and ZIP.
Powered by Phil Harvey's [ExifTool](#). Max file size 80 megabytes. Photos and data viewed with this service are not shared with anyone else, nor are they saved beyond the temporary period needed for the service to function.

یک برنامه آنلاین است (<http://regex.info/exif.cgi>) که به ما اجازه می‌دهد که اطلاعات موجود در هر تصویری را بیینیم. ما می‌توانیم به سادگی آن را از دستگاه آپلود یا نشانی اینترنتی را برای فایل ارائه دهیم. اگر یک تصویر شامل geolocations باشد، به صورت مختصات ارائه می‌شود. Exif Viewer بر اساس ابزار Exif توسط Phil Harvey است که از <http://www.sno.phy.queensu.ca/~phil/exiftool> دانلود شده است. این نه تنها اجازه می‌دهد تا اطلاعات Exif را بخوانیم، بلکه آن‌ها را در فایل‌ها نیز می‌نویسد. ابزار Exif از لیست گسترده‌ای از فرمتهای مختلف مانند XMP، GFIF، ID3 و ... پشتیبانی می‌کند که همچنین در صفحه آن ذکر شده‌اند.

¹ سیستم موقعیت‌یابی جهانی

Basic Image Information	
Target file: WP_20140922_10_40_53_Pro.jpg	
Camera:	Nokia Lumia 630
Exposure:	Auto exposure, 1/8 sec, f2.4, ISO 1600
Flash:	Off. Did not fire
Date:	September 22, 2014 10:40:53AM (timezone not specified) (12 hours, 48 minutes, 17 seconds ago, assuming image timezone of 5½ hours ahead of GMT)
Location:	Latitude/longitude: 28° 35' 30.7" North, 77° 22' 17.5" East (28.591863, 77.371538)
Location guessed from coordinates: E-88, E-block, Sector 52, New Okhla Industrial Development Area, Uttar Pradesh 201307, India	
Map via embedded coordinates at: Google , Yahoo , WikiMapia , OpenStreetMap , Bing (also see the Google Maps pane below)	
Altitude: 176 meters (577 feet) Timezone guess from earthtools.org : 5½ hours ahead of GMT	
File:	916 × 1,632 JPEG (1.5 megapixels)
Color Encoding:	WARNING: Color space tagged as sRGB, without an embedded color profile. Windows and Mac browsers and apps treat the colors randomly. Images for the web are most widely viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for more information.

```
C:\Users\o.o\Downloads\Compressed\exiftool(-k).exe
Luminance : 0 80 0
Measurement Observer : CIE 1931
Measurement Backing : 0 0 0
Measurement Geometry : Unknown
Measurement Flare : 0%
Measurement Illuminant : D65
Media Black Point : 0.01205 0.0125 0.01031
Red Matrix Column : 0.43607 0.22249 0.01392
Red Tone Reproduction Curve act> : <Binary data 2060 bytes, use -b option to extract>
Technology : Cathode Ray Tube Display
Viewing Cond Desc : Reference Viewing Condition in IEC 61966-2-1
Media White Point : 0.9642 1 0.82491
Profile Copyright : Copyright International Color Consortium, 2009
Chromatic Adaptation : 1.04791 0.02293 -0.0502 0.0296 0.99046 -0.0170
? -0.00925 0.01506 0.75179
Image Width : 2048
Image Height : 1152
Encoding Process : Progressive DCT, Huffman coding
Bits Per Sample : 8
Color Components : 3
Y Cb Cr Sub Sampling : YCbCr4:2:0 <2 2>
Image Size : 2048x1152
-- press any key --
```

با استفاده از مکان جغرافیایی در تصاویری که به اشتراک می‌گذاریم، هر کسی می‌تواند به راحتی پیگیری کند که دقیقاً در زمان کلیک روی آن کجا بوده است. این می‌تواند توسط افراد بد مورد سوءاستفاده قرار گیرد؛ بنابراین باید مراقب باشید اگر تصاویر و مکان‌هایتان را به اشتراک می‌گذارید.

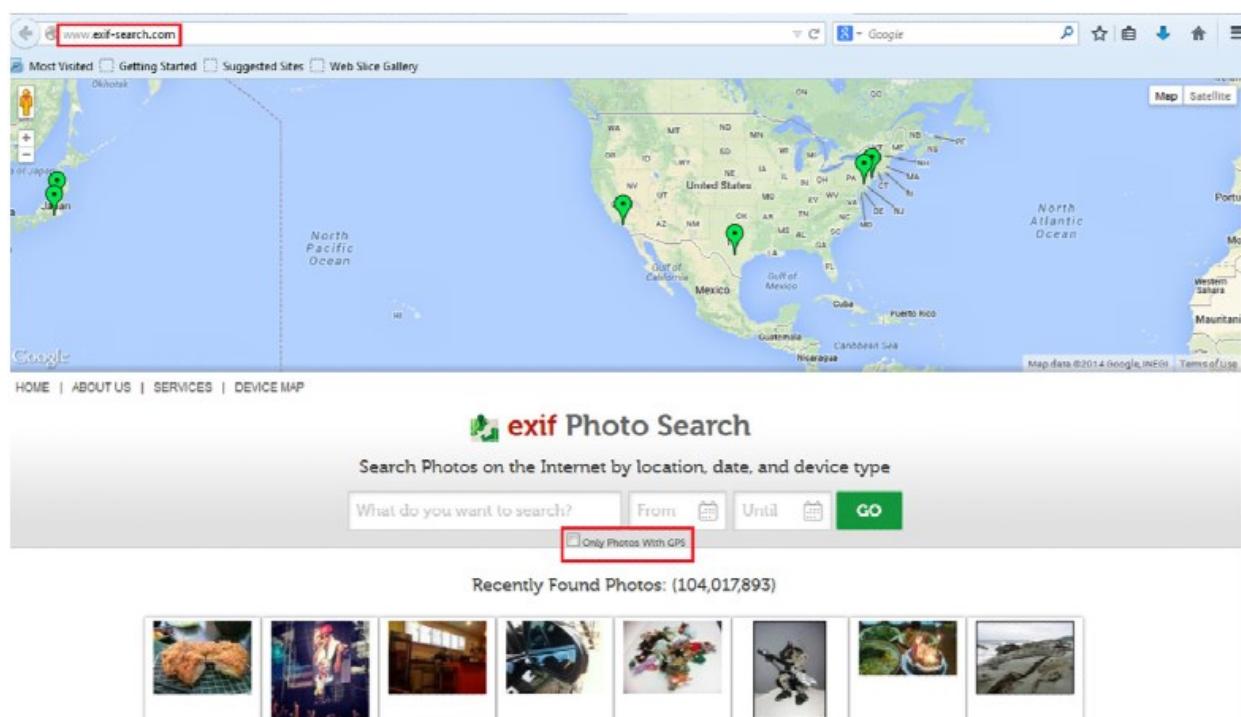
EXIF SEARCH

ما فقط درباره Exif و قدرت آن برای واکشی مختصات جغرافیایی بحث کردیم. یک موتور جستجوی اختصاصی Exif Search که به ما اجازه می‌دهد تا از طریق تصاویر Geotagged شده، جستجو کنیم که به نام [\(http://www.exif-search.com/\)](http://www.exif-search.com/) است.

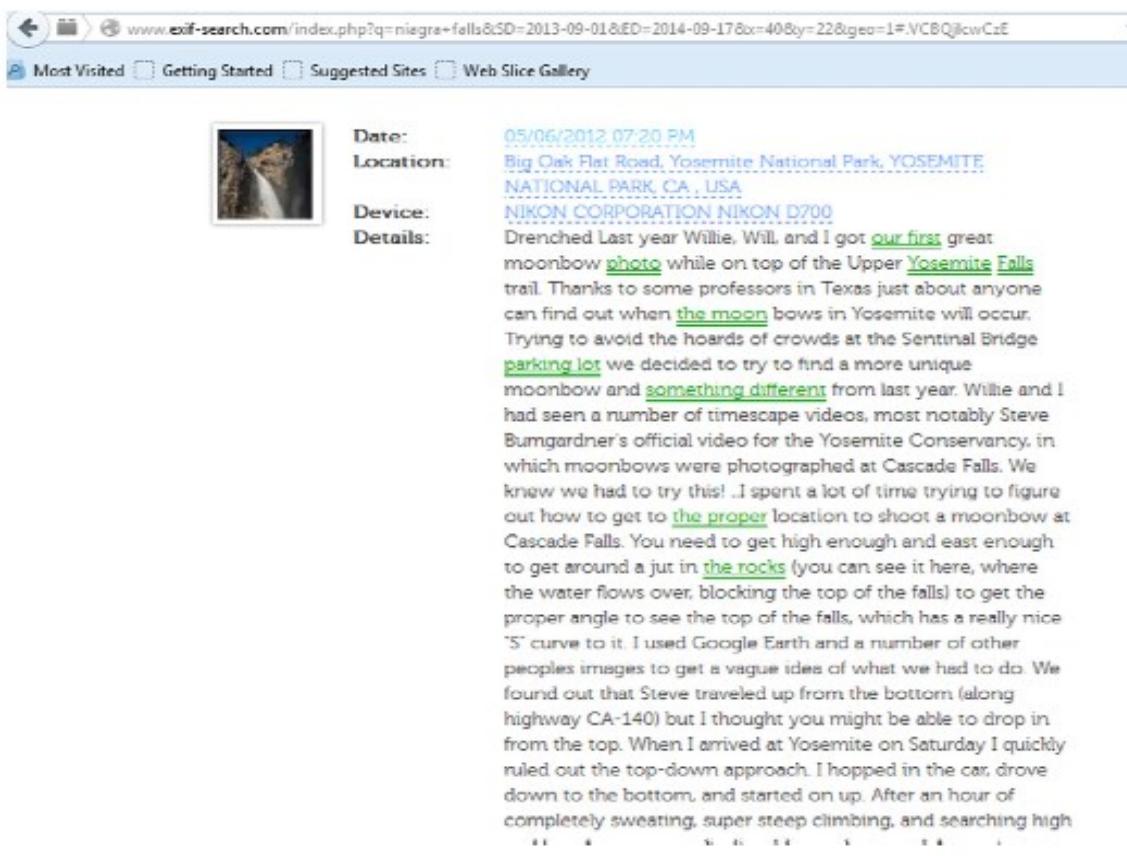
این موتور جستجو اطلاعات مربوط به تصاویر را از سراسر اینترنت فراهم می‌کند. این شامل تعداد زیادی از تصاویر قابل جستجو از دستگاه‌های مختلف تلفن همراه است. Exif به طور کامل با موتورهای جستجوی سنتی تصویر متفاوت است که فقط یک نتیجه به ما ارائه می‌دهد. همچنین فراداده آن را نیز فراهم می‌کند.

هنگامی که ما در Exif Search جستجو می‌کنیم، تصویر و اطلاعات آن را در پایگاه داده خود جستجو و نتیجه را به ما می‌دهد. در حال حاضر بیش از ۱۰۰ میلیون تصویر با فراداده دارد و دائمًا پایگاه داده خود را به روز رسانی می‌کند.

این موتور جستجو بر اساس مکان، تاریخ و نوع دستگاه را فراهم می‌کند. همچنین به ما اجازه می‌دهد که داده‌ها را بر اساس مکان، تاریخ یا نوع دستگاه طبقه‌بندی کنیم. یکی دیگر از ویژگی‌های منحصر به فرد این موتور جستجو این است که به ما اجازه می‌دهد که ما نتایج را فقط برای تصاویری که حاوی داده‌های GPS هستند انتخاب کنیم. جعبه کوچک آن در زیر نوار جستجو در دسترس است.



همچنین از تعداد زیادی دستگاه پشتیبانی می‌کند. این لیست را می‌توان در آدرس <http://www.exif-search.com/devices.php> پیدا کنید، برخی از آن‌ها عبارت‌اند از کانن، نیکون، اپل و فوجی فیلم و غیره.



The screenshot shows a web browser window with the URL www.exif-search.com/index.php?q=niegra+falls&SD=2013-09-01&ED=2014-09-17&ox=40&oy=22&geo=1#.VCBQjIcwCzE. Below the address bar are links for 'Most Visited', 'Getting Started', 'Suggested Sites', and 'Web Slice Gallery'. The main content area displays the EXIF metadata for a photograph. It includes:

- Date:** 05/06/2012 07:20 PM
- Location:** Big Oak Flat Road, Yosemite National Park, YOSEMITE NATIONAL PARK, CA, USA
- Device:** NIKON CORPORATION NIKON D700
- Details:** Drenched Last year Willie, Will and I got our first great moonbow photo while on top of the Upper Yosemite Falls trail. Thanks to some professors in Texas just about anyone can find out when the moon bows in Yosemite will occur. Trying to avoid the hoards of crowds at the Sentinel Bridge parking lot we decided to try to find a more unique moonbow and something different from last year. Willie and I had seen a number of timescape videos, most notably Steve Burngardner's official video for the Yosemite Conservancy, in which moonbows were photographed at Cascade Falls. We knew we had to try this! I spent a lot of time trying to figure out how to get to the proper location to shoot a moonbow at Cascade Falls. You need to get high enough and east enough to get around a jut in the rocks (you can see it here, where the water flows over, blocking the top of the falls) to get the proper angle to see the top of the falls, which has a really nice 'S' curve to it. I used Google Earth and a number of other peoples images to get a vague idea of what we had to do. We found out that Steve traveled up from the bottom (along highway CA-140) but I thought you might be able to drop in from the top. When I arrived at Yosemite on Saturday I quickly ruled out the top-down approach. I hopped in the car, drove down to the bottom, and started on up. After an hour of completely sweating, super steep climbing, and searching high

ivMeta

فایل‌های ویدئویی مشابه فایل‌های تصویری می‌توانند مختصات GPS را در فرادراده خود داشته باشند. ivMeta یک ابزار ایجادشده توسط رایین وود (<http://digi.ninja/projects/ivmeta.php>) است که به ما اجازه می‌دهد فرادراده‌هایی مانند نسخه نرم‌افزاری، تاریخ، مختصات GPS، شماره مدل را از فیلم‌های آیفون استخراج کنیم. آیفون یکی از محبوب‌ترین گوشی‌های هوشمند موجود است و دارای فناوری عالی است. بیش از یک میلیون کاربر از آن استفاده می‌کنند. بدون شک در کیفیت دوربین در بین دستگاه‌ها و برنامه‌ها برای ایجاد تصاویر و فیلم‌ها منحصر به فرد است. کاربران آیفون بسیاری از داده‌های خود را هر روز در سایت‌های مختلف شبکه‌های اجتماعی آپلود می‌کنند. اگرچه گزینه‌ای در دستگاه برای غیرفعال کردن برچسب‌گذاری جغرافیایی وجود دارد، تنظیم پیش‌فرض و استفاده از GPS اجازه می‌دهد تا متنی در مورد هر تصویر یا ویدیو گرفته شده اضافه شود. در این مورد این ابزار برای جمع‌آوری تمام اطلاعات از فیلم‌های آیفون مفید است. این ابزار یک اسکریپت پایتون است، بنابراین برای اجرا باید پایتون را نصب کرد (+2.7). این می‌تواند در فارنزيک فیلم‌های آیفون بسیار مفید باشد.

```
C:\Windows\system32\cmd.exe
C:\Users\o.o\Downloads\Compressed\ivmeta>ivmeta.py -v IMG_1002.MOV
ivMeta 1.0 Robin Wood <robin@digininja.org> <www.digininja.org>
*****
Parsing: IMG_1002.MOV
*****
Type starts at 4 and ends at 128 <length 116>
Type Marker: qt
+ Maker starts at 36595221 and ends at 36595234 <length 5>
Maker: Apple
+ Version starts at 36595147 and ends at 36595160 <length 5>
Software version: 7.1.1
+ Date starts at 36595164 and ends at 36595196 <length 24>
Date: 2014-07-06T13:27:49+0530
GPS: Not found
+ Model starts at 36595200 and ends at 36595217 <length 9>
Model: iPhone 5s

C:\Users\o.o\Downloads\Compressed\ivmeta>
```

HACHOR-METADATA

بر اساس کتابخانه پایتون hachoir است که برای استخراج Hachoir-metadata فراداده استفاده می‌شود. همان‌طور که کتابخانه پایه آن پایتونی است، این ابزار یک ابزار پایتونی است که می‌تواند برای استخراج فراداده‌ها از تصویر، صدا و ویدئو و همچنین آرشیوها استفاده شود. این ابزار از بیش از ۳۰ فرمت مختلف برای استخراج فراداده پشتیبانی می‌کند که یک ویژگی منحصر به فرد است.

برخی از ویژگی‌های دیگر که این ابزار را از سایر ابزارهای مشابه جدا می‌کند این است که از فایل‌های غیر معابر و ناقص شده و جلوگیری از داده‌ها تکراری استفاده می‌کند. به غیر از این، همچنین به کاربران اجازه می‌دهند تا با اضافه کردن اولویت به مقادیر، فراداده‌ها را فیلتر کنند. این ابزار به‌طور کلی برای نسخه‌های مختلف لینوکس قابل دسترسی است و می‌تواند از URL زیر دانلود شود:

<https://bitbucket.org/hypo/hachoir/wiki/Install>.

برخی از فرمتهای محبوب پشتیبانی شده توسط این ابزار عبارت‌اند از zip, bzip2, gzip, tar و غیره، در فایل‌های فشرده و png, jpeg, gif, ico, bmp و غیره در تصاویر. همچنین فرمت محبوبی که توسط این ابزار پشتیبانی می‌شود، Adobe PhotoShop Document (PSD) از نرم‌افزار بسیار محبوب PhotoShop برای ویرایش تصویر در صنعت چندرسانه‌ای، است. پشتیبانی از این فرمت که به‌طور خاص برای کسانی که می‌خواهند به استخراج فرداده از آن پردازنند. در صوت از mpeg و real پشتیبانی می‌کند. در ویدئو از فرمت flv پشتیبانی می‌کند. این نیز به دلیل اینکه

به طور گسترده در یوتیوب، یکی از بزرگ‌ترین سایت به اشتراک‌گذاری ویدئو استفاده می‌شود مهم است و همچنین از mov، پشتیبانی می‌کند. دیگر فرمتهای پشتیبانی شده محبوب عبارت‌اند از exe. همچنین از فایل‌های تورنت^۱ پشتیبانی می‌کند که راه حل آسان برای بسیاری از نیازهای به اشتراک‌گذاری داده است؛ بنابراین استخراج فراداده تورنت به‌طور خاص یکی از ویژگی‌های منحصر به فرد آن است. چه کسی حتی فکرش را می‌کند که فرا داده‌ها را از ttf یا فونتها استخراج می‌کند، اما بله این ابزار همچنین از فرمت ttf پشتیبانی می‌کند. بسیاری از فرمتهای دیگر نیز پشتیبانی می‌شوند. ما می‌توانیم جزئیات آن را از آدرس زیر دریافت کنیم:

<https://bitbucket.org/hypo/hachoir/wiki/hachoir-metadata>.

اساساً یک ابزار خط فرمان است. اگر هیچ‌یک از سوئیچ‌ها را اجرا نکنید، اطلاعات زیادی را ارائه می‌دهد:

#hachoir-metadata xyz.png

ما همچنین می‌توانیم این ابزار را با فرمتهای متعدد و متفاوت در یک زمان اجرا کنیم تا نتیجه مورد نظر را به دست آوریم:

#hachoir-metadata xyz.png abc.mp3 ppp.fl v

وقتی ما فقط نیاز به جزئیات MIME داریم می‌توانیم از دستور زیر استفاده کنیم:

#hachoir-metadata --mime xyz.png abc.mp3 ppp.fl v

هنگامی که ما نیاز به اطلاعات بیشتر از MIME داریم، می‌توانیم از سوییچ type استفاده کنیم:

#hachoir-metadata --type xyz.png abc.mp3 ppp.fl

برای مشاهده راهنمای ابزار برای گزینه‌های دیگر می‌توانیم از دستور زیر استفاده کنیم:

#hachoir-metadata - help

FOCA

¹ torrent

روزانه با تعداد زیادی از فایل‌هایی مانند DOC، PDF و غیره کار می‌کنیم. بعضی اوقات آن‌ها را ایجاد، گاهی اوقات ویرایش و گاهی اوقات آن‌ها را می‌خوانیم. به غیر از داده‌هایی که ذکر کردیم، فراداده‌ها نیز به آن‌ها اضافه می‌شود. برای یک کاربر عادی این داده‌ها ممکن است بی‌عیب و نقص باشند، اما در واقع می‌توانند اطلاعات حساس زیادی در مورد سیستم مورد استفاده برای ایجاد آن‌ها را نشان دهند.

اکثر سازمان‌ها امروزه در وب‌سایت‌ها و شبکه‌های اجتماعی حضور دارند. به غیر از صفحات وب، سازمان‌ها همچنین از فایل‌های مختلفی برای اشتراک گذاری اطلاعات با عموم استفاده می‌کنند و این فایل‌ها ممکن است حاوی فراداده باشند. در فصل ۵ ما در مورد چگونگی استفاده از موتورهای جستجو برای پیدا کردن فایل‌ها در وب‌سایت‌ها بحث کردیم (به عنوان مثال در "site: xyzorg.com filetype: pdf" Google) بنابراین به سادگی باید آن‌ها را دانلود و از یک ابزار استفاده کنیم که می‌تواند از آن‌ها فراداده را استخراج کند.

ابزاری است که این روند را برای ما انجام می‌دهد. اگر چه FOCA به معنی مهروموم در اسپانیایی است، این ابزار به معنای «استخراج اطلاعات سازمانی با جمع‌آوری بایگانی^۱» است. آن را می‌توان از <https://www.elevenpaths.com/labstools/foca/index.html> دانلود کنید. پس از دانلود فایل زیپ، به سادگی آن را استخراج و فایل برنامه را داخل فolder bin اجرا کنید.

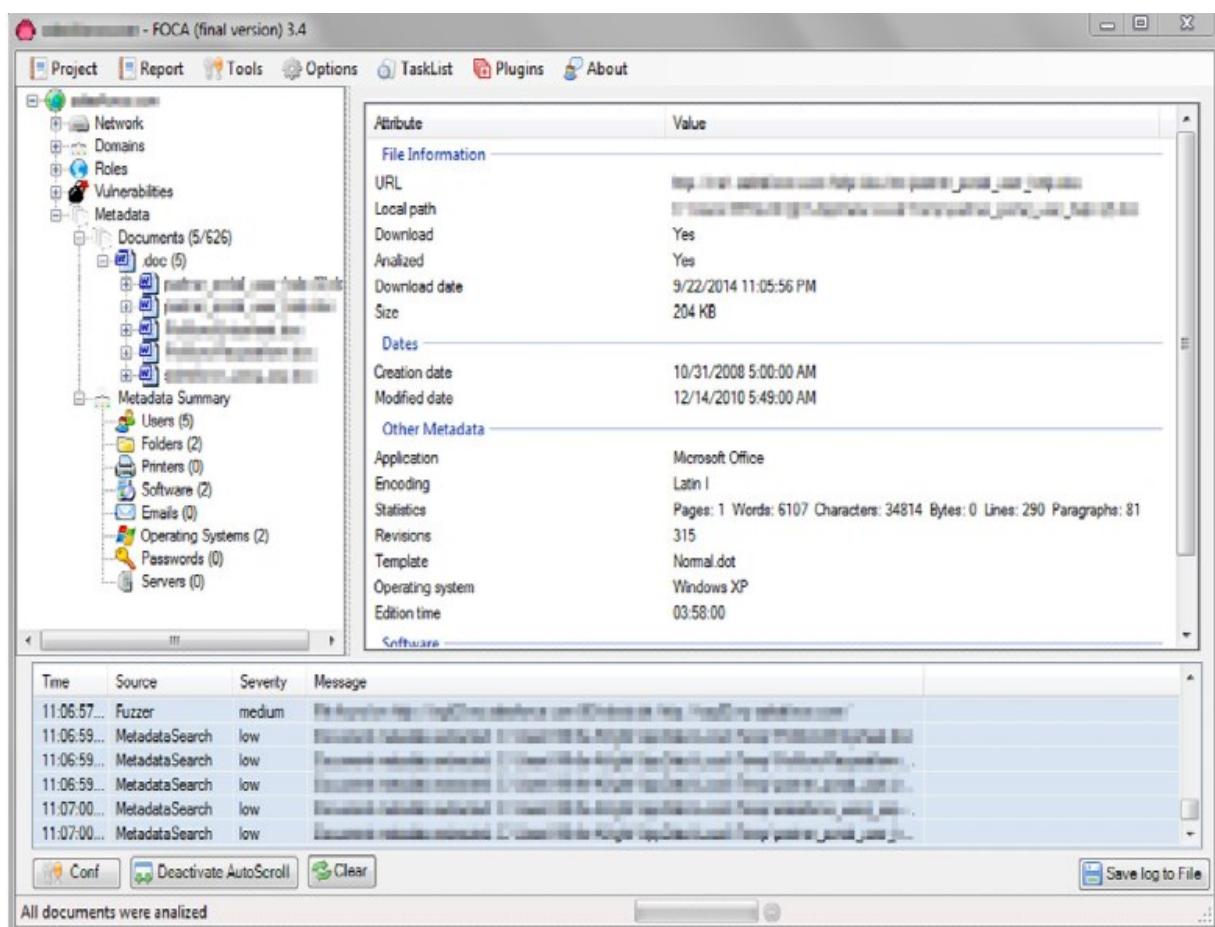
برای استفاده از FOCA به سادگی نیاز به ایجاد یک پروژه جدید و ارائه یک نام و دامنه برای اسکن دارید. هنگامی که فایل پروژه ذخیره می‌شود، FOCA به ما اجازه می‌دهد که موتورهای جستجو و افزونه‌هایی را که باید جستجو کنیم را انتخاب کنیم. پس از آن می‌توانیم به سادگی با کلیک کردن بر روی دکمه «Search All» شروع کنیم. هنگامی که بر روی این دکمه کلیک می‌کنیم، FOCA موتورهای جستجوی مختلف را برای جستجوی انواع فایل‌های ticked در دامنه ذکر شده شروع می‌کند. هنگامی که این جستجو کامل می‌شود، لیست تمام اسناد پیدا شده، نوع، URL، اندازه و غیره نمایش داده خواهد شد.

اکنون لیست اسناد موجود در دامنه را داریم. چیزی که باید انجام دهیم این است که با کلیک راست روی هر فایل و انتخاب گزینه All / Download آن را دانلود کنیم. پس از اتمام دانلود، فایل (ها) آماده برای بازرسی می‌شوند؛ بنابراین باید بر روی فایل کلیک راست کرده و بر روی گزینه Extract Meta Data کلیک کنید. هنگامی

¹ Fingerprinting Organizations with Collected Archives

که کامل شد، می‌توانیم بینیم که تحت گزینه Metadata در نوار سمت راست FOCA تمام اطلاعات استخراج شده از سند (ها) را ذکر کرده است.

این اطلاعات ممکن است شامل نام کاربری سیستم مورد استفاده برای ایجاد فایل، نسخه دقیق برنامه کاربردی مورد استفاده برای ایجاد آن، مسیر سیستم و خیلی بیشتر باشد که برای مهاجم بسیار مفید خواهد بود. اگرچه استخراج فراداده تنها عملکردی است که توسط FOCA ارائه نمی‌شود، ما همچنین می‌توانیم از آن برای شناسایی آسیب‌پذیری، انجام تجزیه و تحلیل شبکه، جستجوی پشتیبان‌گیری و جمع‌آوری اطلاعات بسیار بیشتر استفاده کنیم.



METAGOOFIL

همانند FOCA، ابزار دیگری برای استخراج فراداده از اسناد موجود در اینترنت است. Metagoofil اساساً یک ابزار خط فرمان مبتنی بر پایتون است. این ابزار را می‌توان از <https://code.google.com/p/metagoofil/> دانلود کرد. استفاده از این ابزار نسبتاً آسان است و چند سوئیچ ساده وجود دارد که می‌تواند برای انجام کار استفاده شود.

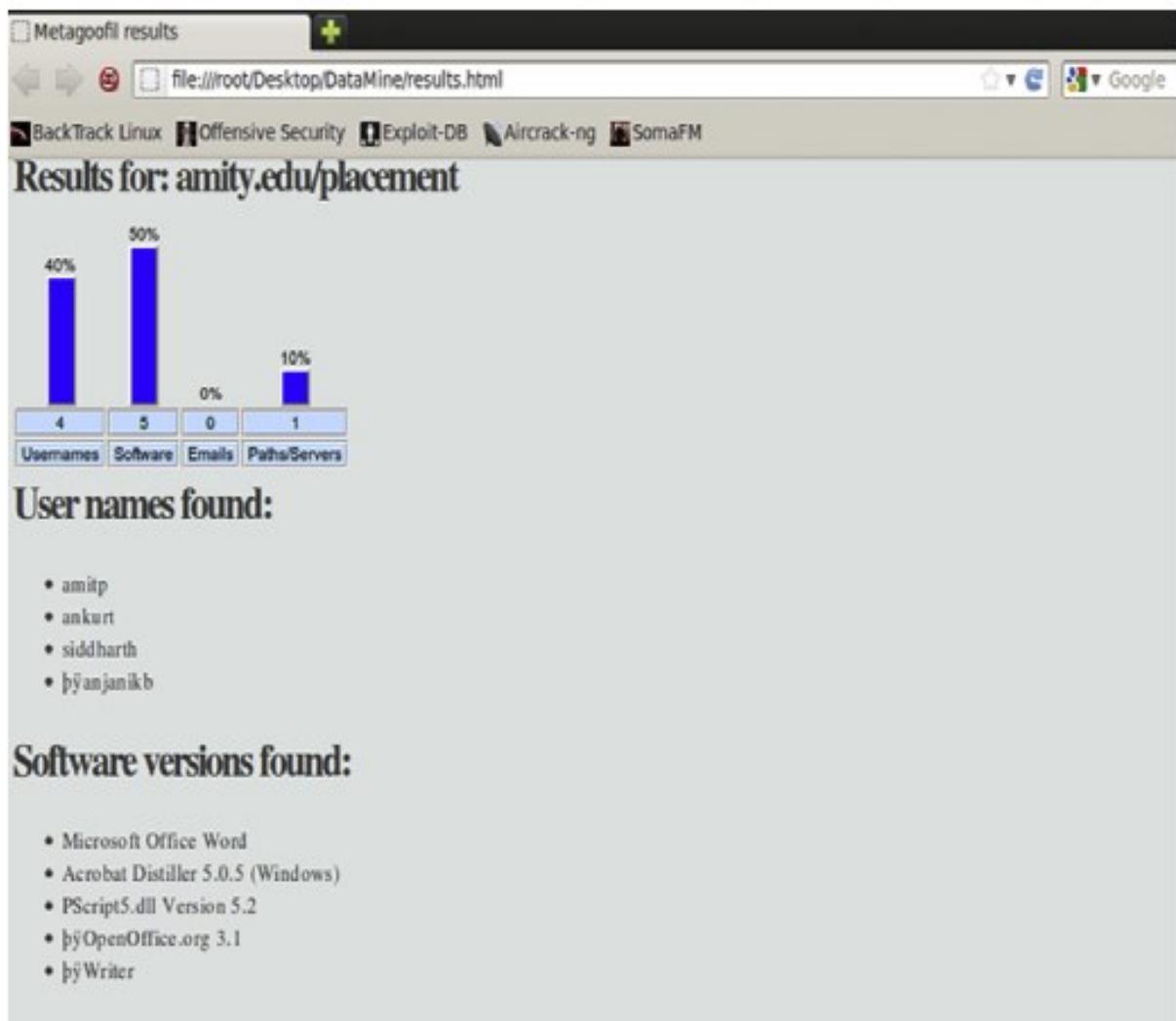
فهرست سوئیچ‌ها به شرح زیر است:

- d: domain to search
- t: filetype to download (pdf, doc, xls, ppt, odp, ods, docx, xlsx, pptx)
- l: limit of results to search (default 200)
- h: work with documents in directory (use “yes” for local analysis)
- n: limit of files to download
- o: working directory (location to save downloaded files)
- f: output file

ما می‌توانیم پرس‌وجوهایی مانند موارد زیر را برای انجام یک اسکن در حوزه هدف ارائه دهیم و نتیجه را در قالب یک فایل HTML ذخیره کنیم که می‌تواند به راحتی در هر مرورگر خوانده شود:

```
metagoofil -d example.com -t doc,pdf -l 100 -n 7 -o /root/Desktop/meta -f /root/Desktop/meta/result.html
```

همانند FOCA MetagooFil همچنین جستجوی اسناد را با استفاده از موتور جستجو انجام داده و آن‌ها را برای انجام فرآیند استخراج فراداده با استفاده از کتابخانه‌های مختلف پایتون دانلود می‌کند. پس از تکمیل فرآیند استخراج، نتایج به سادگی در کنسول نمایش داده می‌شود. همان‌طور که در بالا ذکر شد، این نتایج همچنین می‌تواند به عنوان یک فایل HTML برای آپنده با استفاده از سویچ ۴ ذخیره شوند.



به طور مشابه ابزارهای دیگری وجود دارند که می‌تواند برای استخراج فراداده از فایل‌های مختلف استفاده شوند، بعضی از آن‌ها در زیر آمده است:

- MediaInfo—audio and video files (<http://mediaarea.net/en/MediaInfo>)
- Gspot—video files (<http://gspot.headbands.com/>)
- VideoInspector—video files (<http://www.kcsoftwares.com/?vtb#help>)
- SWF Investigator—SWF/flash files <http://labs.adobe.com/downloads/swfinvestigator.html>)
- Audacity—audio files (<http://audacity.sourceforge.net/>)

IMPACT

اطلاعات جمع‌آوری شده با استفاده از استخراج فراداده می‌تواند مفید باشد و برای ایجاد حملات مختلف به قربانیان و حتی سازمان‌های دولتی استفاده شود. سناریوی زندگی واقعی می‌تواند بدتر از آنچه انتظار داریم باشد. اطلاعاتی که از فرآیند فوق جمع‌آوری شده شامل اطلاعات دقیق دستگاه، موقعیت جغرافیایی، اطلاعات مربوط به نام

کاربری، نرم‌افزار مورد استفاده، سیستم‌عامل و غیره است که برای مهاجم بسیار حیاتی است. این اطلاعات را می‌توان بر علیه قربانی با استفاده از روش‌های ساده مانند مهندسی اجتماعی یا بهره‌برداری از هر نوع آسیب‌پذیری خاصی که قربانی را به‌طور شخصی در زندگی واقعی به خطر می‌اندازد، مورد استفاده قرار داد، زیرا محل دقیق محل را نیز فراهم می‌کند. همه این موارد ممکن است فقط به خاطر اطلاعاتی که اغلب هیچ‌کس اهمیت نمی‌دهد و یا برخی حتی ممکن است از آن‌ها آگاه نباشند اتفاق بیافتد شود.

همان‌طور که مشاهده کردیم، اطلاعات حساس از طریق اسناد و فایل بدون آنکه به ما داده شود، استخراج شد و امکان تبدیل این داده‌ها به عنوان ابزاری علیه قربانی و استفاده از آن‌ها به عنوان یک بردار حمله وجود دارد. در حال حاضر راه حلی برای جلوگیری از آن وجود دارد که با نام حفاظت از نشت داده (DLP) شناخته می‌شود.

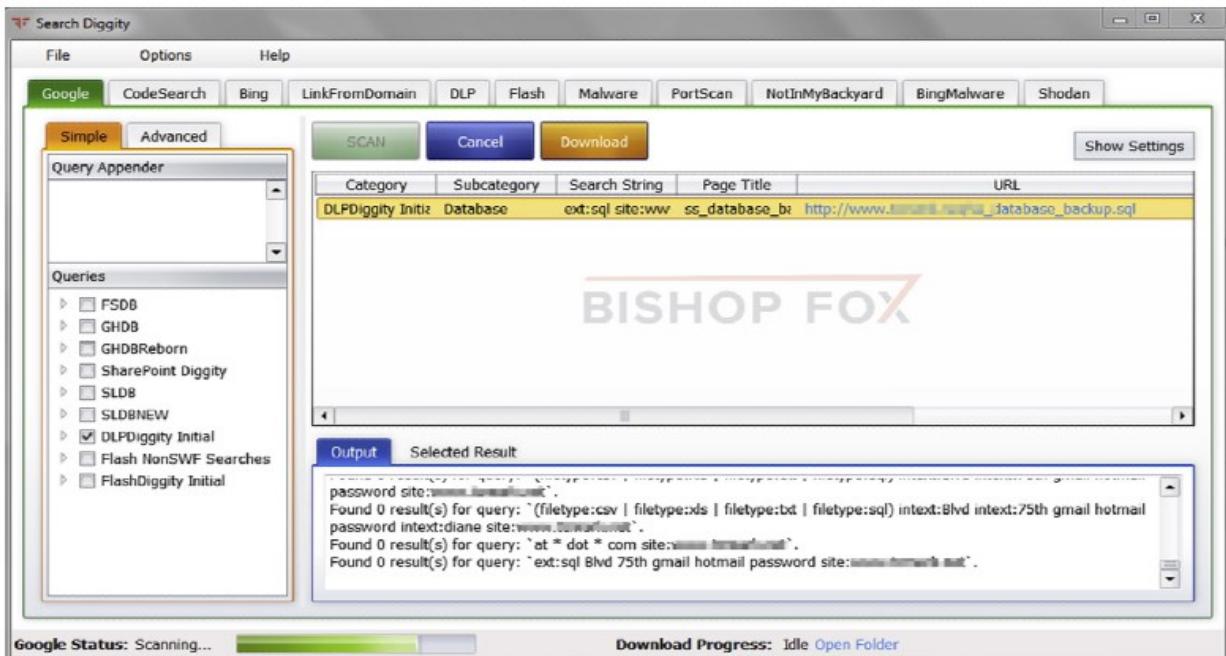
SEARCH DIGGITY

در فصل گذشته ما در مورد ویژگی‌های جستجوی پیشرفته این ابزار جالب یاد گرفتیم. Search Diggity ابزار ایجاد شده توسط Bishop Fox است که دارای مجموعه‌ای بزرگ از پارامترها و پایگاه داده گسترده‌ای از پرس‌وجوها برای موتورهای جستجو مختلف است که به ما اجازه جمع‌آوری اطلاعات مربوط به هدف را می‌دهد؛ اما در این فصل بیشتر به یکی از ویژگی‌های خاص این ابزار علاقه‌مند هستیم که DLP است.

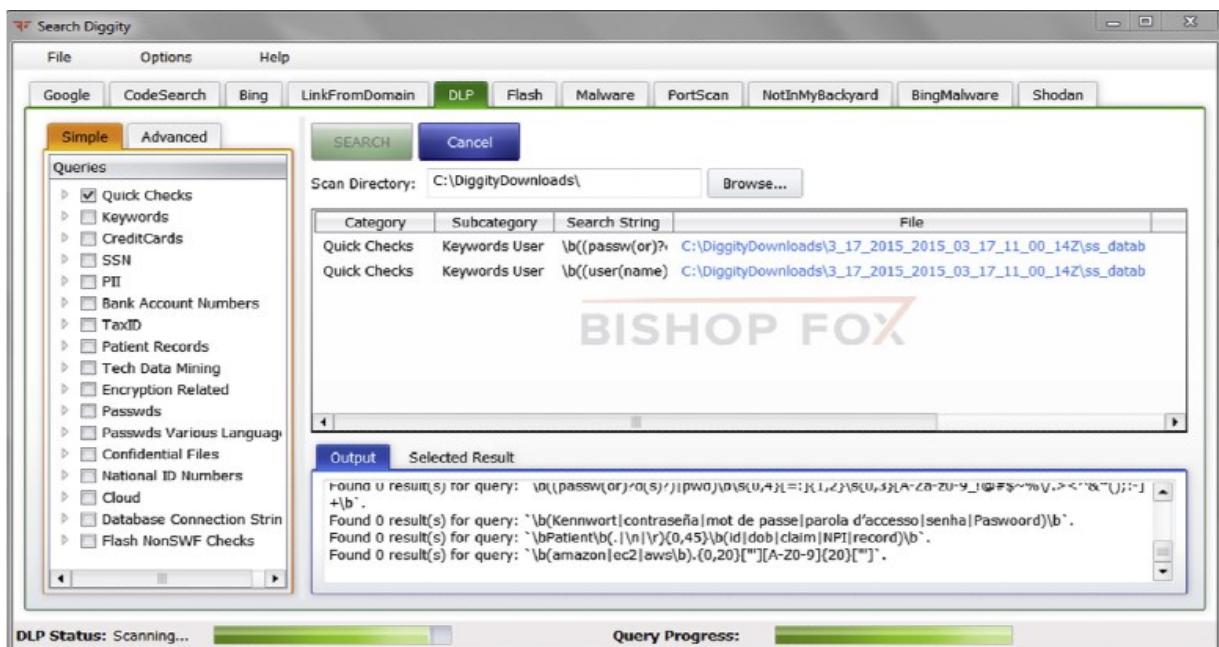
تعداد زیادی از گزینه‌ها برای انتخاب در نوار جانبی از برگه DLP در Search Diggity وجود دارد. برخی از گزینه‌ها عبارت‌اند از کارت اعتباری، شماره حساب بانکی، رمزهای عبور، فیلدهای حساس و غیره

این برگه DLP به‌طور کلی وابسته است. ما نمی‌توانیم به‌طور مستقیم از آن استفاده کنیم. ابتدا باید برخی از پرس‌وجوها را در دامنه مورد علاقه‌مان اجرا کنیم سپس تمامی فایل‌هایی که بعد از اتمام این پرس‌وجو پیدا می‌کنیم را دانلود تا مسیر آن را در برگه DLP قرار گیرد تا مطمئن شوید که آیا اطلاعات حساس در معرض عموم قرار می‌گیرد یا نه. برای انجام این کار می‌توانیم برگه google یا برگه bing را انتخاب کنیم که به معنای موتور جستجوی گوگل یا بینگ است و در آن‌ها باید گزینه initial DLPDiggity را برای شروع جستجو برای تهیه نسخه پشتیبان، تنظیمات، جزئیات مالی، جزئیات پایگاه داده، سیاهه‌های مربوطه و سایر فایل‌ها انتخاب کنید. اگرچه تنظیمات خاصی برای گزینه initial DLPDiggity وجود دارد، اجازه دهد همه تنظیمات به صورت پیش‌فرض باشد. پس از اتمام پرس‌وجو، تمام فایل‌های موجود را در قالب جدول در قسمت نتایج این ابزار به دست خواهیم آورد. تمام

فایل‌هایی که دریافت کرده را انتخاب کرده و دانلود کنید. تمام فایل‌ها را در مسیر پیش فرض و در یک پوشه به نام DiggityDownloads ذخیره می‌کند.



اکنون زبانه را به DLP تغییر دهید. در بالای آن می‌توانیم به صورت پیش فرض در مسیر DiggityDownloads شامل نتیجه اسکن حضور داشته باشیم؛ بنابراین فقط یک یا چند گزینه موجود در برگه DLP را انتخاب کنید. در اینجا ما گزینه Quick Check را انتخاب می‌کنیم و بر روی Search کلیک تا نتیجه را به دست آوریم.



نتیجه ممکن است گاهی اوقات ترسناک باشد مانند اینکه شماره کارت اعتباری، شمار کلمه عبور و ... را نشان دهد. این قدرت این ابزار است؛ اما تمرکز اصلی ما این نیست که اطلاعات حساس را کشف کنیم بلکه DLP است؛ بنابراین تمام جزئیات را از نتیجه نهایی ابزار دریافت کنید. نتیجه نشان می‌دهد به شیوه‌ای آسان و قابل درک، در چه صفحه و یا سند چه داده‌هایی در دسترس است. به طوری که مالک دامنه می‌تواند آن را حذف یا رمزگذاری کند تا از دست رفتن اطلاعات جلوگیری شود.

ابزار حذف و یا DLP فراداده‌ها

DLP یک روش مهم برای جلوگیری از دست رفتن اطلاعات است. مثال بالا کاملاً عمومی است تا چگونگی کار DLP را به ما بفهماند. در حال حاضر ما بیشتر علاقه‌مند به حذف فراداده‌ها هستیم بنابراین ابزارهای مختلفی برای حذف فراداده‌ها وجود دارند. ما همچنین می‌توانیم آن‌ها را به عنوان ابزار DLP فراداده بیان کنیم. برخی از آن‌ها در زیر ذکر شده است.

METASHIELD PROTECTOR

یک راه حل است که به جلوگیری از دست دادن اطلاعات از طریق مدارک رسمی منتشرشده در وبسایت کمک می‌کند. این ابزار با وب سرور وب‌سایت یکپارچه شده است. تنها محدودیت این موضوع این است که تنها برای وب سرور IIS قابل دسترسی است. به غیر از این، طیف وسیعی از اسناد اداری را پشتیبانی می‌کند. برخی از انواع فایل‌های محبوب عبارت‌اند از doc، ppt، docx، pptsx، xls، xlsx، jpeg و pdf و غیره. در درخواست برای هر یک از این انواع سند، آن را پاک و سپس آن را ارائه می‌دهد. MetaShield Protector را می‌توان در https://www.elevenpaths.com/services/html_en/metashield.html یافت. این ابزار در <https://www.elevenpaths.com/labstools/emetrules/index.html> موجود است.

MAT

MAT و یا چهار چوب ناشناس کننده فراداده، ابزاری گرافیکی است که به حذف فراداده از انواع مختلف فایل‌ها کمک می‌کند. این ابزار در پایتون توسعه یافته و از کتابخانه hachoir برای این منظور استفاده می‌کند. همان‌طور که قبلًا مذکور درباره کتابخانه hachoir پایتون و یکی از پروژه‌های در بخش hachoir-metadata بحث کردیم، این پروژه دیگر بر اساس همان کتابخانه است. جزئیات مربوط را می‌توان در اینجا <https://mat.boum.org/> یافت.

بهترین چیز در مورد MAT این است که منبع باز است و از طیف گسترده‌ای از پسوندهای فایل مانند png، jpeg، torrent، mp3، tar، pdf،xlsx، pptx، docx وغیره پشتیبانی می‌کند.

MyDLP

این محصول توسط Comodo است که طیف وسیعی از محصولات امنیتی و خدمات را فراهم می‌کند. MyDLP یک راه حل یکپارچه برای جلوگیری از نشت اطلاعات بالقوه است. در سازمان نه تنها اسناد بلکه ایمیل‌ها، دستگاه‌های USB و سایر دستگاه‌های مشابه نیز منبع احتمالی نشت اطلاعات هستند و در این مورد به سازمان اجازه می‌دهد به راحتی این راه حل را برای نظارت، بازرسی و جلوگیری از تمام داده‌های بحرانی خروجی به کار بیندد. جزئیات MyDLP را می‌توان در اینجا پیدا کنید. <http://www.mydlp.com>

OpenDLP

OpenDLP یک ابزار پیشگیری از دست دادن اطلاعات تحت کنترل منبع باز است که تحت GPL منتشر شده است. از یک برنامه وب متصرکر، می‌تواند اطلاعات حساس در انواع مختلف سیستم عامل مانند ویندوز و یونیکس و همچنین انواع مختلف پایگاه‌های داده مانند MySQL و MSSQL را شناسایی کند. این پروژه را می‌توان در اینجا پیدا کنید. <https://code.google.com/p/opendlp/>

DOC SCRUBBER

نرم‌افزار رایگان برای پاک کردن اطلاعات پنهان از اسناد است. برخی از ویژگی‌های محبوب آن اجازه می‌دهد تا فایل‌های doc را در یک زمان پاک کنید. Doc Scrubber را می‌توان از آدرس زیر دانلود کنید.

<http://www.javacoolsoftware.com/dsdownload.html>

MOVING GEO-TAGS

همان‌طور که قبلاً توضیح دادیم چگونه اطلاعات جغرافیایی می‌تواند برای یک کاربر در دیدگاه مهاجم خط‌ناک باشد، زیرا مکان دقیق مربوط به یک کاربر را نشان می‌دهد، در اینجا برخی از تنظیمات در Picasa می‌تواند به ما برای حذف این برچسب‌های geotag کمک کند. پیکاسا، برنامه سازماندهی و ویرایش تصویر گوگل است که می‌تواند به حذف geotag‌ها از تصاویر کمک کند. صفحه راهنمای و پشتیبانی آن در آدرس زیر است:

<http://support.google.com/picasa/bin/answer.py?hl=en&answer=70822>

ما همچنین می‌توانیم از ابزار Exif که قبلاً مورد استفاده قرار گرفت برای حذف چنین اطلاعاتی استفاده کنیم. گرچه عمدتاً فراداده برای سازمان و در ارتباط داده‌ها استفاده می‌شود، همچنین می‌تواند در طی تحقیقات سایبری و همچنین تست نفوذ مورد استفاده قرار گیرد. همان‌طور که قبلاً بحث شد، اکثر آن‌ها بی‌ضرر هستند، اما گاهی اوقات می‌توانند برخی از اطلاعات حساس را افشاء کنند. همان‌طور که بسیاری از افراد و سازمان‌ها از وجود آن اطلاع ندارند، به آن توجه زیادی نمی‌کنند. راه حل‌های مورد بحث در بالا باید استفاده شده تا خطر ناشی از چنین اطلاعاتی را کاهش دهد.

فصل ۸: ناشناس بودن آنلاین

مقدمه

ناشناس بودن تعریف اساسی اصطلاح "بدون نام بودن است". به‌سادگی شخصی ناشناس است که هویت او شناخته نشده باشد. از لحاظ روان شناختی، ناشناس بودن ممکن است به عنوان کاهش پاسخگویی به اقدامات انجام‌شده توسط فرد درک شود. ناشناس بودن نیز با حریم خصوصی همراه است زیرا گاهی اوقات مطلوب نیست که یک پیوند مستقیم با یک شخص خاص داشته باشیم، هر چند گاهی به موجب قانون لازم است احرار هویت قبل و یا در طی یک عمل انجام شود. در دنیای واقعی، اشکال مختلف شناسایی مانند کارت ملی، گواهینامه رانندگی، پاسپورت و غیره وجود دارد که به‌طور گسترده قابل قبول است.

ناشناس بودن آنلاین

در فضای مجازی هیچ فرم مشخصی از سیستم تائید شناسه^۱ وجود ندارد. ما معمولاً از اسم مستعار برای ایجاد بیانیه‌ها استفاده می‌کنیم. این نام مستعار معمولاً به هویت واقعی ما مربوط نبوده و از این رو احساس ناشناسی را ارائه می‌دهد؛ اما ناشناس بودن موجود در اینترنت کامل نیست. ما در حال حاضر ممکن است نام، کد ملی و یا شماره گذرنامه را شناسایی نکنیم، اما آدرس خارجی خود را نشان می‌دهیم. این آدرس IP را می‌توان برای پیگیری رایانه مورد استفاده قرار داد. همچنین در بعضی از سیستم‌ها مانند وب‌سایت‌های شبکه‌های اجتماعی، یک اعتبار مجازی ایجاد می‌کیم که اطلاعات آن با دنیای فیزیکی ما مرتبط است. برخی از وب‌سایت‌ها نیز از کاربران خواسته‌اند تا

^۱ ID

برخی از انواع اطلاعاتی را که می‌توانند به طور مستقیم به یک شخص مرتبط باشند ارائه دهند؛ بنابراین اساساً ما در فضای سایبر کاملاً ناشناس نیستیم. معمولاً می‌توان اطلاعاتی برای ردیابی دستگاه و یا شخص استفاده کرد.

چرا نیاز به ناشناس بودن آنلاین داریم؟

دلایل زیادی برای ناشناس بودن وجود دارد. افراد مختلف دلایل مختلفی دارند که ممکن است بعضی از آن‌ها به دلیل خواسته‌های کاری مانند کسانی که به تحقیقات سایبری و یا روزنامه‌نگاری و برخی ممکن است به خاطر نگرانی از حریم خصوصی باشد. زمان‌هایی است که ما می‌خواهم اظهار نظر کنیم، اما انجام آن به طور آشکار ممکن است مشکلاتی را ایجاد کند، بنابراین می‌خواهیم ناشناس باشیم. همان‌طور که در زندگی فیزیکی می‌گوییم، افرادی که بعد از انجام جرم و جنایت به دنبال جناحتکار هستند، در زندگی مجازی یا در اینترنت به همان نحو در زیرزمین زندگی می‌کنند. مجرمان سایبری و هکرها می‌خواهند ناشناس باشند.

ناشناس بودن فقط یک انتخاب است و همیشه به دلیل نیاز ندارد این یک شیوه زندگی مجازی است و در حالی که بعضی‌ها می‌خواهند از آن لذت ببرند. در دنیای فیزیکی ما نیازمندیم و یا تمایل داریم که در اینترنت ناشناس باشیم. ممکن است فقط به خاطر نگرانی ما از حفظ حریم خصوصی باشد، ما می‌خواهیم بیانیه‌ای صادر کنیم، اما این کار را با هویت واقعی انجام نمی‌دهیم، ما باید چیزی را بدون اینکه به طور مستقیم مشارکت کنیم، به اطلاع شخصی برسانیم. با استثنای دلایل ذکر شده، شاید فقط بخواهیم محدودیتی را که توسط مقامات (به عنوان مثال Wi-Fi دانشگاه) برای بازدید از برخی از بخش‌های وب مورد استفاده قرار می‌گیرد، دور بزنیم. انگیزه پشت آن می‌تواند هر چیزی باشد، اما ضروری است که دلیلی وجود دارد.

افراد ممکن است فقط هویت خود را پنهان می‌کنند. همچنین می‌توانید کاری که انجام می‌دهید را پنهان کنید. یک مثال ساده می‌تواند به ما کمک کند تا آن را در ک کنیم. مثلاً ما می‌خواهیم چیزی بخریم و برای خرید آن از یک سایت تجارت الکترونیک بازدید کردیم. ما محصول را دوست داشتیم اما به دلایلی آن را خرید نکردیم؛ همان‌طور که ما به طور معمول در وب گردی هستیم، ممکن است تبلیغات همان نوع محصول را در سراسر اینترنت پیدا کنیم. این فقط یک سیاست بازاریابی برای غول‌های تجارت الکترونیک با ردیابی کوکی‌های کاربر برای در ک خواسته‌ها و ارسال تبلیغ به آن‌ها است.

برخی ممکن است این را دوست داشته و بعضی ممکن است نداشته باشد. برای جلوگیری از چنین سناریوهایی افراد ممکن است ترجیح دهند ناشناس باشند. گزینه مرور خصوصی در اغلب مرورگرها وجود دارد و مرورگرها ناشناس کننده‌ای وجود دارند که این کار را برای ما انجام می‌دهند.

در این فصل ما راه‌های مختلفی برای ناشناس ماندن در اینترنت خواهیم داشت. ۱۰۰٪ نمی‌توان در اینترنت ناشناس ماندن را تضمین کرد اما با ابزارها و تکنیک‌هایی که در این فصل ذکر شده، می‌توانیم هویت مان را تا سطح معقولی پنهان کنیم.

راه حل‌های ناشناس بودن آنلاین

راه‌های زیادی برای ناشناس بودن وجود دارد و بسیاری از جنبه‌های آن وجود دارد. برخی ممکن است بر روی پنهان سازی اطلاعات شخصی مانند سایت‌های شبکه‌های اجتماعی با استفاده از نام‌های مستعار، اطلاعات عمومی یا جعلی، شناسه عمومی ایمیل و سایر جزئیات تمرکز کنند. برخی ممکن است بخواهند در هنگام مرور ناشناس باشند تا هیچ کس نتواند بفهمد به کدام منابع نگاه کرددند. برخی ممکن است بخواهند آدرس‌های هویتی مجازی خود را مانند آدرس IP و غیره پنهان کنند.

راه‌های مختلفی برای دستیابی به شرایط فوق وجود دارد؛ اما راه‌حل‌های مهم و محبوب در دسترس پروکسی یا شبکه خصوصی مجازی^۱ (VPN) هستند. اگر چه روش‌های دیگری نیز هستند ولی هنوز هم این دو مورد به طور گسترده‌ای مورد استفاده قرار می‌گیرند و ما در این فصل به طور عمدۀ بر آن‌ها تمرکز خواهیم کرد.

پروکسی^۲

پروکسی کلمه‌ای است که به طور کلی برای انجام کارها با واسطه کسی یا چیزی استفاده می‌شود. به طور مشابه در تکنولوژی، پروکسی را می‌توان به عنوان یک عنصر واسط که در خواست فرستاده شده توسط منبع را به مقصد منتقل و پاسخ مقصد را جمع‌آوری و دوباره آن را به منبع ارسال می‌کند، در نظر گرفت.

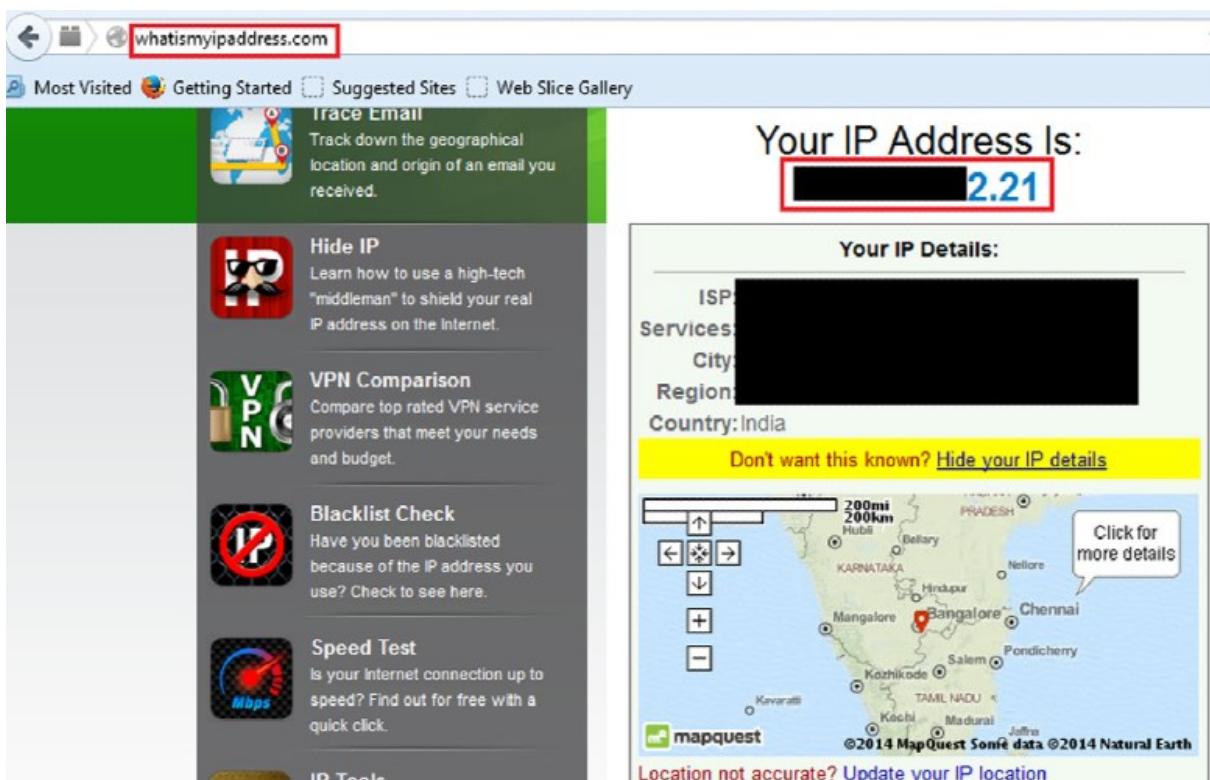
این یکی از راه‌حل‌های پر استفاده برای ناشناس بودن است. تنها دلیل استفاده از پروکسی، پنهان کردن آدرس IP است. راه‌حل‌های مختلف برای استفاده از پروکسی موجود است مانند پروکسی وب، نرم‌افزار پروکسی و غیره. اساساً تمام راه‌حل‌ها بر اساس یک اصل اساسی برای هدایت ترافیک به مقصد از برخی آدرس‌های دیگر IP است.

¹ virtual private network

² PROXY

اگرچه پروکسی می‌تواند برای بسیاری از اهداف دیگر استفاده شود، ما فقط بر ناشناس بودن تمرکز خواهیم کرد. قبل از تمرکز به جنبه‌های فنی بسیار حرفه‌ای پروکسی، باید نگاهی به برخی از کارهای ناشناس بیندازیم. همان‌طور که در فصل‌های قبل یاد گرفتیم که چگونه از موتورهای جستجو استفاده می‌کنیم و به جستجوی پیشرفته پردازیم. اکنون وقت آن رسیده است که بینیم چگونه یک موتور جستجو را می‌توان به عنوان یک پروکسی برای ناشناس بودن استفاده کنیم.

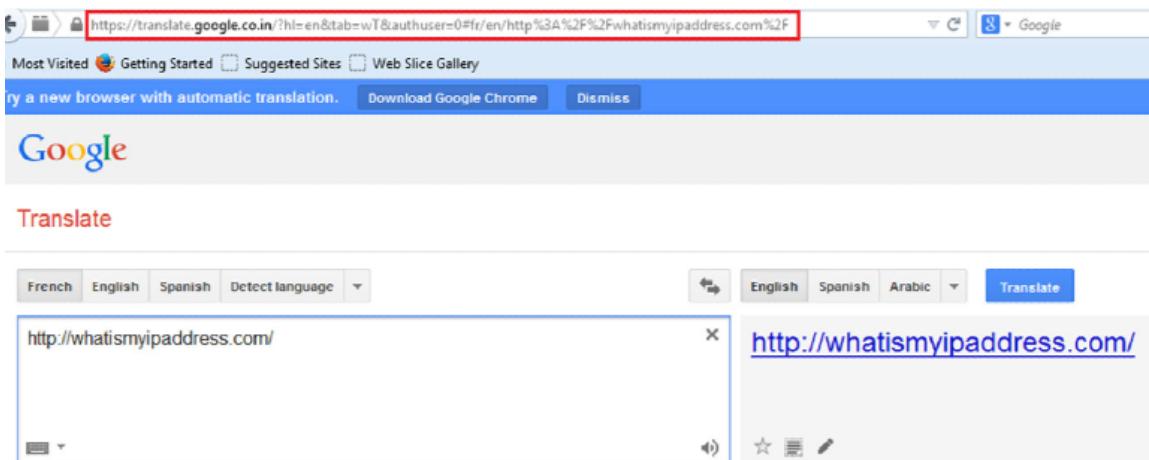
همان‌طور که گوگل، موتور جستجوی محبوبی است، می‌توان از آن به عنوان پروکسی با ویژگی Google Translate آن استفاده کرد. گوگل سرویس‌های خود را در بسیاری از کشورها به غیر از زبان‌های انگلیسی ارائه می‌دهد و همچنین از چندین زبان پشتیبانی می‌کند. Google Translate اجازه می‌دهد که کاربر محتوای وب را در هر زبانی؛ که می‌خواهد، بخواند. به عنوان مثال، محتوای غیر انگلیسی ممکن است به زبان انگلیسی ترجمه شود و بالعکس؛ بنابراین این ویژگی به کاربر اجازه می‌دهد از سرور گوگل برای ارسال درخواست و جمع‌آوری پاسخ از طرف خود که پایه اساسی پروکسی است، استفاده کند.



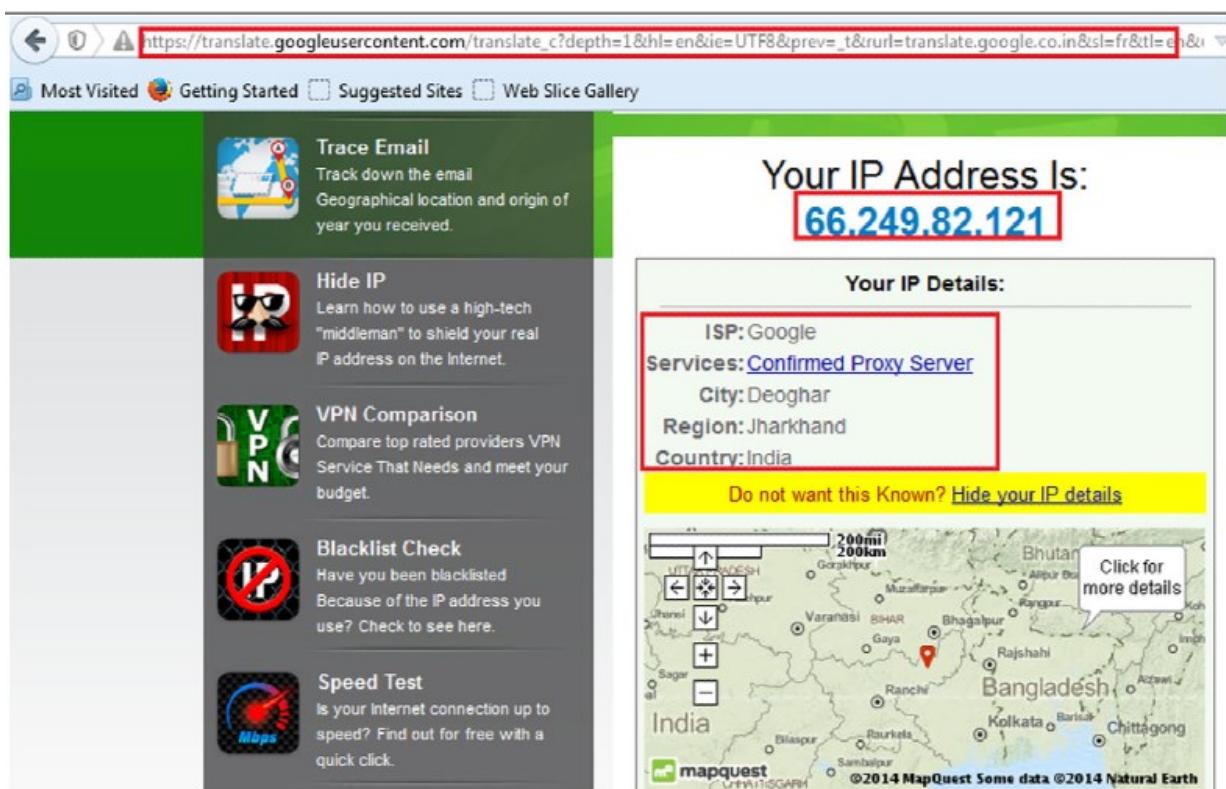
در ابتدا با آدرس IP خودمان به یک سایت به نام <http://whatismyipaddress.com/> رفته و بعد از استفاده از Google Translate برای بررسی همان سایت نگاه خواهیم کرد. کار این سایت این است که آدرس IP مورد استفاده برای

ارسال درخواست به سایت را بگوید. اگر برای مرور طبیعی از طریق Google Translate، آدرس IP متفاوت باشد، به این معنی است که ما با استفاده از Google Translate ناشناس شدیم.

اکنون translate.google.com را بینید هر زبان را در منع و هر زبان دیگری در مقصد انتخاب کنید تا این صفحه وب را ترجمه کنید همان‌طور که در تصویر زیر نشان داده شده است.



در حال حاضر بر روی ترجمه کلیک کنید تا بررسی کنید که آیا آدرس IP مطابق با آدرس واقعی است که در تصویر بالا برای مرور مستقیم در دسترس است یا نه.



ما می‌توانیم از تصویر بالا بینیم که آدرس‌های IP مرور مستقیم و مرور با استفاده از Google Translate متفاوت هستند؛ بنابراین ثابت شده که ما می‌توانیم از Google Translate به عنوان پروکسی سرور برای رسیدن به هدفمان استفاده کنیم. در بسیاری از موارد این کار خواهد کرد. اگرچه بسیار ساده و مؤثر است اما از لحاظ ناشناس بودن کامل ممکن است مفید نباشد، اما هنوز هم می‌توانیم از این روش برای ناشناس بودن استفاده کنیم.

پروکسی در اصطلاح ناشناس ساز

همان‌طور که دیدیم، می‌توانیم از ویژگی موتور جستجو به عنوان پروکسی استفاده کنیم؛ اما نکته‌ای که باید در نظر گرفته شود سطوح ناشناس بودن است. سطوح مختلف ناشناس بودن بر اساس راهکارهای مختلف پروکسی وجود دارد. برخی از پروکسی‌ها فقط اطلاعات ما را پنهان می‌کنند، اما در سیاهه‌های مربوط به آن‌ها نگهداری می‌شود و بعضی اوقات بعضی از پروکسی‌ها به عنوان پروکسی سرور شناسایی می‌شوند. این بهترین راه حل نیست اگر می‌خواهید ناشناس باشد. راه حل‌های وجود دارند که پروکسی سرور شناخته نمی‌شود و همچنین زمانی که کاربر جلسه را به پایان رساند تمام جزئیات کاربر را حذف می‌کند. این بهترین راه حل برای ناشناس بودن کامل است. آن‌ها بستگی به الزام ما برای انتخاب سرویس و یا نوع پروکسی که ما می‌خواهیم استفاده کنیم دارد.

انواع راه حل‌های پروکسی

در حال حاضر انواع مختلفی از راه حل‌های پروکسی وجود دارد که بعضی از آن‌ها برای گمنام بودن و همچنین بر اساس نوع مبتنی بر نرم افزارهای کاربردی و یا مبتنی بر وب است؛ بنابراین اجازه دهید برخی از ابزارهای موجود مبتنی بر برنامه را بررسی کنیم.

پروکسی‌های مبتنی بر نرم افزارهای کاربردی

پروکسی مبتنی بر کاربرد فقط یک نرم افزار یا ابزار است که می‌تواند در سیستم عامل ما نصب شود تا از آن به عنوان راه حل پروکسی استفاده شود.

Ultrasurf

این یک پروکسی مبتنی بر برنامه کاربردی است که در <http://ultrasurf.us> یافت می‌شود. هم اکنون به عنوان افزونه کروم نیز موجود است. اگر ما برای دانلود و نصب آن در سیستم عامل تبل هستیم، ممکن است از افزونه کروم استفاده کنیم که هدف ما است. این پلاگین را می‌توانیم در آدرس زیر پیدا کنیم:

<https://chrome.google.com/webstore/detail.ultrasurf/mjnbc1mflcpookeapghfshapeffmpodij?hl=en>.

ابتدا نسخه پلاگین خود را بررسی و سپس به نسخه نرم‌افزاری بروید. بهترین قسمت این افزونه استفاده آسان آن است و از بسیاری از زبان‌ها مانند انگلیسی، فرانسوی، پرتغالی و رومی و غیره پشتیبانی می‌کند. هنگامی که افزونه کروم در مرورگر اضافه می‌شود، نماد آن را در نوار افودنی سمت راست بالا در سمت راست نوار آدرس می‌بینیم. هنگامی که ما بخواهیم از آن استفاده کنیم با کلیک بر روی آیکون، یک پنجره کوچک باز خواهد شد و سپس سوئیچ موجود در آن پنجره را به ON تغییر دهید. سپس افزونه به سرور آن متصل می‌شود. هنگامی که به سرور متصل می‌شود، می‌توانیم ناشناس مرور کنیم. درصورتی که ما فراموش کردیم که افزونه را فعال کنیم و یا در حال تلاش برای وصل شدن به سرور باشد یا قادر به اتصال سرور نیست، همه چیزهایی که ما مرور می‌کنیم همانند مرور معمولی است؛ بنابراین در ذهن داشته باشید که قبل از مرور، آن را به سرور متصل کنید و یا تمام مراحل ناشناس سازی بیهوده خواهد بود.

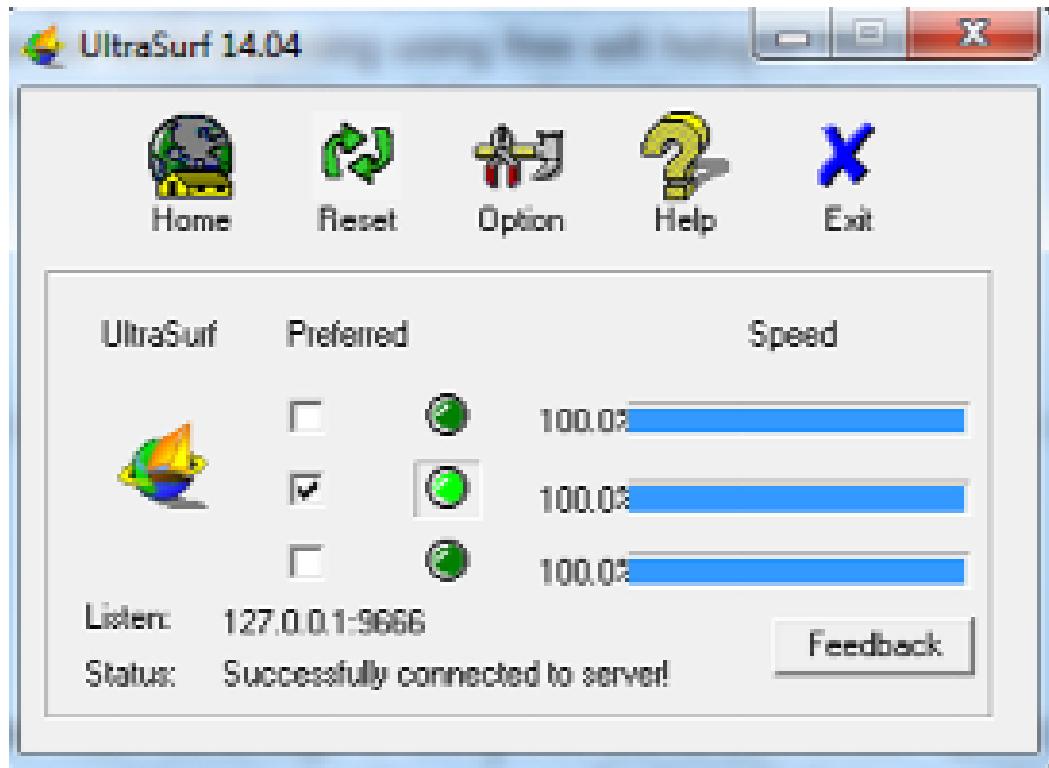
نسخه برنامه را می‌توان به راحتی از لینک <http://ultra.surf.us/download/u.zip> دانلود کنید.

این یک فایل فشرده است، فایل را استخراج کرده و می‌توانیم آن را استفاده کنیم. بهترین بخش این فرآیند این است که ما نیاز به نصب برنامه نداریم. ما می‌توانیم به سادگی روی آن دو بار کلیک کنیم و تنظیمات موردنیاز در سیستم ما انجام شده و اجازه می‌دهد ناشناس مرور کنیم. تنظیمات پیش فرض اجازه می‌دهد که اینترنت اکسلورر را با دو بار کلیک بر روی برنامه باز کنید. ما می‌توانیم تنظیمات برنامه را با استفاده از برگه گزینه‌ها تغییر دهیم.

اگر چه این ابزار قبل از اعراضات ضد سانسور در چین طراحی شده بود، اما اکنون به طور گسترده به عنوان یک راه حل پرورکسی استفاده می‌شود. این نه تنها به کاربر کمک می‌کند تا جزئیات را پنهان کند بلکه کاربر را قادر می‌سازد با استفاده از مکانیزم رمزنگاری ارتباط برقرار کند. این را می‌توان در بسیاری از مناطق مختلف استفاده کرد، اما استفاده عمومی از آن در حالی که در حال مرور با استفاده از Wi-Fi رایگان می‌باشیم. از آنجا که در این مورد، احتمال دسترسی و جمع‌آوری اطلاعات ما وجود دارد.

مزیت اصلی استفاده از این ابزار سرعت اتصال است. به طور کلی هنگامی که ما از هر نوع پرورکسی استفاده می‌کنیم، به خار اینکه مسیریابی از طریق آن سرور تغییر می‌یابد، سرعت اتصال به طور قابل توجهی کاهش می‌یابد و کاربر می‌تواند آن را احساس کند؛ اما در این مورد در مقایسه با دیگر پرورکسی‌ها بسیار سریع است. به غیر از این می‌توانیم سرعت اتصال را در ابزار بینیم و سه گزینه اتصال را فراهم می‌کند، کاربر می‌تواند هر لحظه برای جلوگیری از افت سرعت به هر یک از آن‌ها تغییر دهد. برای تشخیص بین مرور طبیعی و مرور با استفاده از Ultrasurf، این ابزار

نماد قفل را در گوشه سمت راست مرورگر فراهم می‌کند تا اطمینان حاصل شود که کاربر در حال مرور ناشناس است.



یک اشکال کوچک در مورد این ابزار این است که این ابزار تنها از ویندوز پشتیبانی می‌کند. یکی دیگر از مشکلات این است که راه حل‌های بررسی IP، آن را به عنوان پروکسی سرور شناسایی می‌کند؛ اما همان‌طور که پیش از این مورد بحث قرار گرفتیم، این می‌تواند در شرایط مختلف بر اساس الزامات مورد استفاده قرار گیرد و استفاده از آن آسان است. فقط دانلود، اجرا و مرور ناشناس.

JonDo

https://anonymous-proxy-jap.com که قبلًا به نام JAP بود، یک ابزار پروکسی است که در servers.net/en/jondo.html موجود است.

این ابزار برای طیف گسترده‌ای از سیستم‌عامل‌های مانند ویندوز، مک، برای انواع مختلف لینوکس و همچنین برای آندروید در دسترس است. مستندات کامل در مورد چگونگی نصب و استفاده از آن وجود دارد. راه حل‌های

مختلف پروکسی با انواع مختلفی مرورگرها عرضه می‌شوند. همچنین یک نوع از آن را برای مرور ناشناس در فایرفاکس به نام JonDoFox وجود دارد.

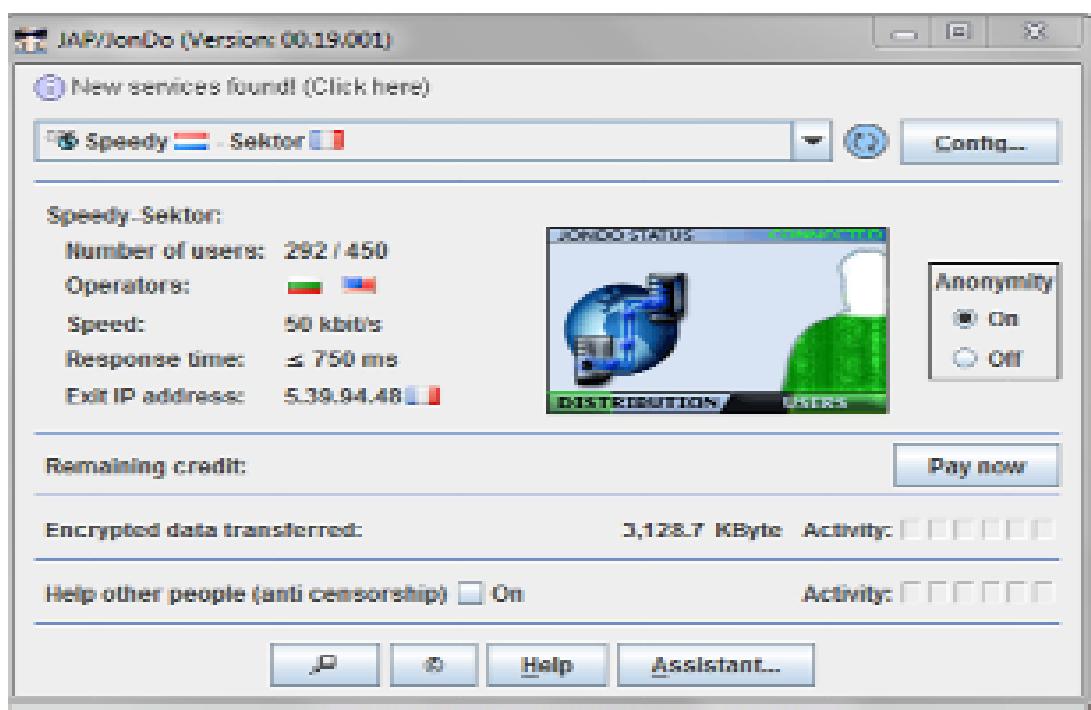
قبل از بررسی JonDo، ابتدا به مرورگر فایرفاکس یعنی JonDoFox نگاه می‌کنیم. این را می‌توان در <https://anonymous-proxy-servers.net/en/jondofox.html> یافت.

همانند JonDoFox، نیز برای سیستم عامل‌های مختلف مانند ویندوز، مک و لینوکس در دسترس است. کاربر می‌تواند بر اساس سیستم عامل خود آن را از URL بالا دانلود کند. مستندات نحوه نصب نیز در کنار لینک دانلود در دسترس است؛ اجازه دهید دانلود و نصب شود.

کاربران ویندوز بعد از دانلود JonDoFox.paf را دریافت خواهند کرد. پس از نصب، پروکسی فایرفاکس را به نام JonDoFox ایجاد خواهد کرد. اگر کاربر همان را انتخاب کند، پروکسی شامل بسیاری از افزونه‌های فایرفاکس مانند مدیر کوکی، adblocker و غیره می‌باشد که به کار خواهد افتاد؛ اما برای استفاده از آن برای ناشناس بودن، نیاز به نصب برخی از نرم‌افزارهای وابسته مانند Tor و غیره وجود دارد.

خوب است که از JonDoFox استفاده کنید، اما کاربر باید تمام نرم‌افزارهای وابسته را نصب کند. برخی ممکن است دوست نداشته باشند این کار را انجام دهنند اما هنوز این یک راه حل عالی برای مرور ناشناس است.

مانند JonDo، JonDoFox را می‌توان از آدرس فوق دریافت کرد. این به شما فایل نصبی را می‌دهد. کاربر ویندوز بعد از دانلود یک "Exefile" "JonDoSetup.paf" دریافت خواهد کرد. می‌تواند بر روی سیستم عامل نصب شده و همچنین نسخه قابل حمل آن می‌تواند با استفاده از درایو USB استفاده شود. کاربر باید بر اساس الزامات خود انتخاب کند. تنها وابستگی این نرم‌افزار جاوا است؛ هنگامی که JonDo نصب می‌شود، ما می‌توانیم بر روی نماد آن دو بار کلیک کنیم تا باز شود. به طور پیش فرض پس از نصب آن یک آیکون ایجاد می‌شود و در شروع راه‌اندازی ویندوز شروع به کار می‌کند.



JonDo نامحدود و اتصال سریع به کاربران پولی اختصاص دارد؛ اما می‌توانیم از همان نسخه رایگان استفاده کنیم؛ اما برای اولین بار ما باید آن را با کد رایگان فعال کنیم. ثبت نام را می‌توانید در <https://shop.anonymous-proxy.com> انجام دهید؛ اما باید آدرس ایمیل را برای دریافت آن ارائه دهیم.

پس از ارائه آدرس ایمیل، یک لینک در شناسه ایمیل دریافت خواهد کرد. برای دریافت کد رایگان به پیوند مراجعه کنید. پس از دریافت کد رایگان، آن را در نرمافزار قرار دهید تا فرایند نصب را تکمیل شود.

The screenshot shows a web browser window with the URL ip-check.info/index.php?auth=519968171&14130960364552=14130960364552-897474106-505003929&refer=.... The page displays the JonDoFox logo and navigation links for JONDONYM, PREMIUM, DOWNLOAD, BLOG, SUPPORT, and CHECK IT!. Below the navigation, it says "By moving your mouse pointer over the underlined text fields, you get detailed information about the individual test results." A table provides information about the user's IP: Your IP (5.39.94.48), Your location (France), Your ISP provider (OVH SAS), and Reverse DNS (velvet.gurufolk.biz). It also includes a Traceroute button and Whos IP/Whos Domain links. A table below lists various system attributes with their values and ratings.

Attribute	Value	Rating
Cookies	Your browser does not store any cookies.	good
Authentication	protected	good
Cache (E Tags)	protected	good
HTTP session	stateless	good
Referrer	hidden (changed when switching the website)	good
Signature	8ab3a24c5ad09f4a3a6a5c03cad9446 (Firefox)	good
UserAgent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.116 Safari/537.36	good
SSL session_id	15045562709C7288E7E11E9B9E1A46R3AE7C7E1A245R204EE27388C569B93EC	neutral

اگر می‌خواهید از JonDoFox استفاده کنید باید JonDoFox را نیز نصب کنید؛ همان‌طور که قبل از JonDoFox را پوشش داده‌اید، می‌توانیم فرض کنیم که در سیستم موجود است. هنگامی که هر دو برنامه نرم‌افزاری در یک سیستم نصب شوند، اگر می‌خواهیم فقط از JonDoFox استفاده کنیم، ما می‌توانیم آن را باز کردن فایرفاکس با پروفایل JonDoFox استفاده کنیم. برای بررسی اینکه آیا در حال مروء ناشناس هستیم، فقط باید آدرس IP را با استفاده از whatismyipaddress.com بررسی کنیم.

The screenshot shows a web browser window with the URL www.whatismyip.com. The page features the WhatIsMyIP logo and navigation links for Create Account and Log In. It displays the user's IP address as 5.39.94.48. Below this, it shows the following details: Proxy: No Proxy Detected, City: Roubaix, State/Region: Nord-pas-de-calais, Country: Fr - France, and ISP: Ovh Sas. There is a green "MORE IP INFORMATION" button. On the right side, there are two vertical menus: "IP Tools" (Internet Speed Test, IP Address Lookup, IP Address Hostname Lookup, IP WHOIS Lookup, Server Headers Check, Blacklist Check, Traceroute, User Agent Info) and "How To" (Change My IP, DVR / Security, Cameras, Email).

اگر می‌خواهیم از JonDo استفاده کنیم، باید در یک مرورگر هم همین کار را بکنیم. در مورد موزیلا به Tools → Options → Advanced → Network → Connection Settings → Configure Configure Manual ۱۴۰۰.۱.۱۲۷.۰.۰.۰ به عنوان پورت پیش فرض مورد استفاده توسط JonDo استفاده کنید.

پس از انجام این کار، فایرفاکس را با پروفایل JonDoFox JonDo باز کنید، آیکون JonDo را در گوشة بالا سمت راست مشاهده خواهید کرد. در اینجا کلیک کنید تا یک برگه باز شود. برای بررسی آدرس IP، "Test Anonymity" را انتخاب کنید.

JonDo مجموعه‌ای از سرورهای پروکسی را فراهم می‌کند که می‌تواند کاملاً به راحتی از جعبه کشویی تغییر کند؛ بنابراین JonDo به عنوان راه حل پروکسی IP شناخته شده است.

همان‌طور که قبلاً در مورد نحوه استفاده از JonDo و راه حل آن برای ناشناس بودن کامل بحث کرده‌ایم. این ابزار دارای ویژگی‌های گوناگونی است، اما یکی از مهم‌ترین آن‌ها سازگاری آن با سیستم‌عامل‌های مختلف است. این باعث می‌شود JonDo در راه‌حل‌های پروکسی منحصر به فرد باشد.

پروکسی مبتنی بر وب

راهکارهای پروکسی مبتنی بر وب، روش ساده و کارآمد برای ناشناس ماندن هستند. بهترین چیز، استفاده بدون نیاز به نصب و بدون وابستگی است که بهترین استفاده آن در رایانه‌های مشترک یا رایانه‌های عمومی برای مرور و بعضی اوقات هنگام استفاده از اتصالات WiFi باز است. رابط کاربری ساده، آن‌ها را برای استفاده بسیار محبوب می‌کند. فقط مرورگر را باز کرده و پروکسی را باز کنید و شما می‌توانید به هر کجا می‌خواهید، بروید.

راه‌حل‌های پروکسی مبتنی بر وب زیادی وجود دارد. بعضی از آن‌ها فقط برای مرور استفاده شده و برخی ممکن است ویژگی‌های بیشتری از قبیل ارسال ایمیل به صورت ناشناس یا خواندن اخبار را داشته باشند. این فقط بسته به نیاز ما و سطح ناشناس بودن ارائه شده، انتخاب یک پروکسی خاص مبتنی بر وب انجام می‌شود.

anonymous.org

اگر کاربر فقط می‌خواهد به طور ناشناس مرور کند، گزینه‌های مختلف مرور آنلاین ناشناس در دسترس وجود دارد. یکی از این موارد، anonymous.org است.

این یک سایت رایگان است که مرور ناشناس را برای کاربران خود با دو زبان مختلف انگلیسی و هلندی فراهم می‌کند. از سایت بازدید کنید، زبان مورد نظر خود را انتخاب و سپس نام سایت را در ناحیه جستجو تایپ کنید و بر روی جستجوی ناشناس کلیک تا سایت را مرور کنید.

The screenshot shows the homepage of [Anonymouse.org](http://anonymouse.org/). The main title is "AnonWWW". Below it are three buttons: "AnonEmail", "AnonWWW", and "AnonNews". A text block explains that many people surf the web under the illusion that their actions are private and anonymous, but this is not true due to calling cards and browser logs. It emphasizes that this service allows users to surf the web without revealing personal information, being fast, easy, and free. A search bar at the top right asks for a website address, with examples like "http://www.yahoo.com". Below the search bar are two buttons: "Your Calling Card without Anonymouse" and "Your Calling Card with Anonymouse". A sidebar ad for "Organize Easy" Agile project management software is visible, along with links to Members, Terms of Service, Privacy Policy, Help / FAQ, and Contact Info. Copyright information from 1997-2019 is also present.

عیب اصلی این سایت این است که پروتکل فقط HTTP را پشتیبانی می‌کند (نه HTTPS)؛ اما همان‌طور که در تصویر زیر می‌بینیم، به عنوان پروکسی سرور شناخته نمی‌شود و آدرس IP نیز از یک مکان دیگر است.

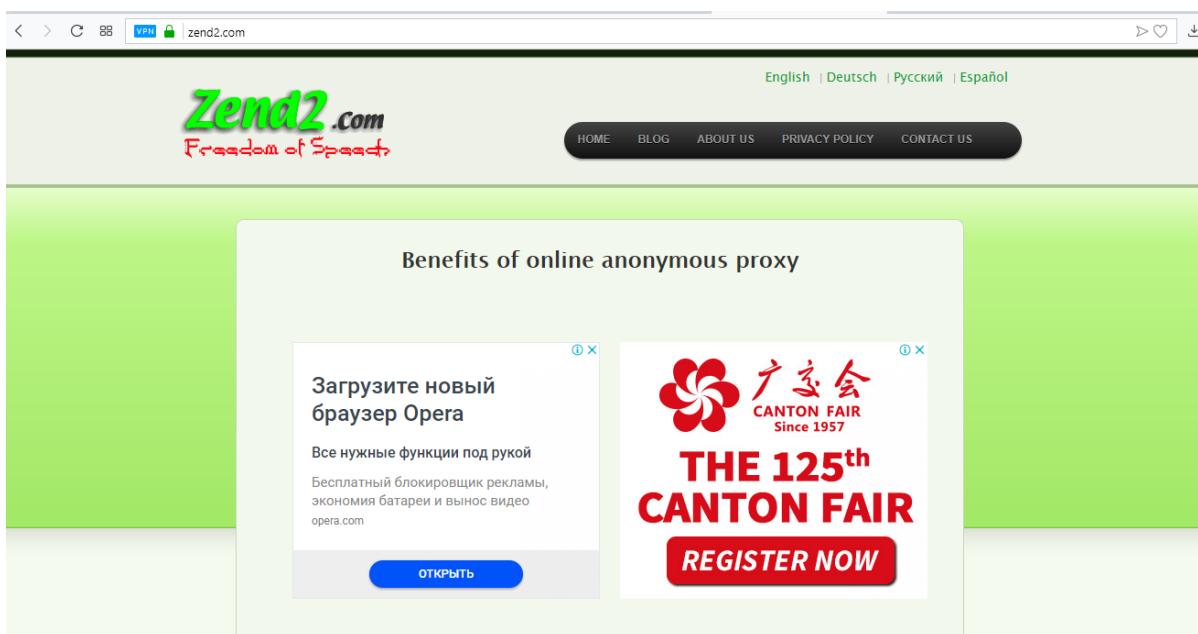
The screenshot shows a web browser window with the URL whatismyipaddress.com in the address bar. The page displays the IP address "193.200.150.152" prominently. To the left, there is a sidebar with various tools: "Trace Email", "Hide IP", "VPN Comparison", "Blacklist Check", and "Speed Test". The main content area shows "Your IP Address Is: 193.200.150.152" and "Your IP Details: ISP: velia.net INternetdienste GmbH Services: None Detected Country: Europe". It also features a map of Europe with a red dot indicating the location, and a note about hiding IP details. A message at the bottom says "Location not accurate? Update your IP location".

همان‌طور که در مورد مزایا و معایب این سرویس بحث کردیم، این راه حل پروکسی بسیار خوب برای مرور به صورت ناشناس است و برخی از ویژگی‌های دیگر مانند ارسال ایمیل و بررسی اخبار الکترونیکی در دسترس وجود دارد.

Zend2

این نیز یک راه حل پروکسی مبتنی بر وب است که بخلاف anonymous.org که تنها از پروتکل HTTP پشتیبانی می‌کند از https نیز پشتیبانی می‌کند؛ بنابراین کاربر نمی‌تواند از anonymous.org برای مرور سایت‌های محبوب مانند فیسبوک و یوتیوب استفاده کند زیرا این سایت‌ها از اتصال https استفاده می‌کنند.

هیچ‌گونه محدودیتی در سایت‌های https یا سایت‌های SSL ندارد. این اجازه می‌دهد تا کاربر به مرور سایت‌های http و https بپردازد؛ بنابراین کاربر می‌تواند از ایمیل خود نیز استفاده کند.



به غیر از آن، برای دو منبع وب محبوب مانند فیسبوک و یوتیوب، [YouTube](https://zend2.com/youtube-proxy/) و [صفحه پروکسی](https://zend2.com/facebook-proxy/) برای یوتیوب: <https://zend2.com/facebook-proxy/> حاوی دستورالعمل‌هایی برای رفع فیلتر یوتیوب است که در مدرسه، دانشگاه، دفتر یا اینترنت اکسپلورر مسدود شده است. در حالی که صفحه پروکسی فیسبوک شامل اطلاعات کلی درباره این پروکسی وب است.

اگر چه می‌توانیم از تمام این سه رابطه کاربری برای بازدید از هر سایت استفاده کنیم، اما می‌خواهیم آن را به عنوان واسطه بین کاربر و سرور استفاده کنیم. کاربر برخی از پارامترها را نیز می‌تواند انتخاب کند از جمله:

✓ رمزنگاری URL

✓ رمزگذاری صفحه

✓ اجازه دادن به کوکی‌ها

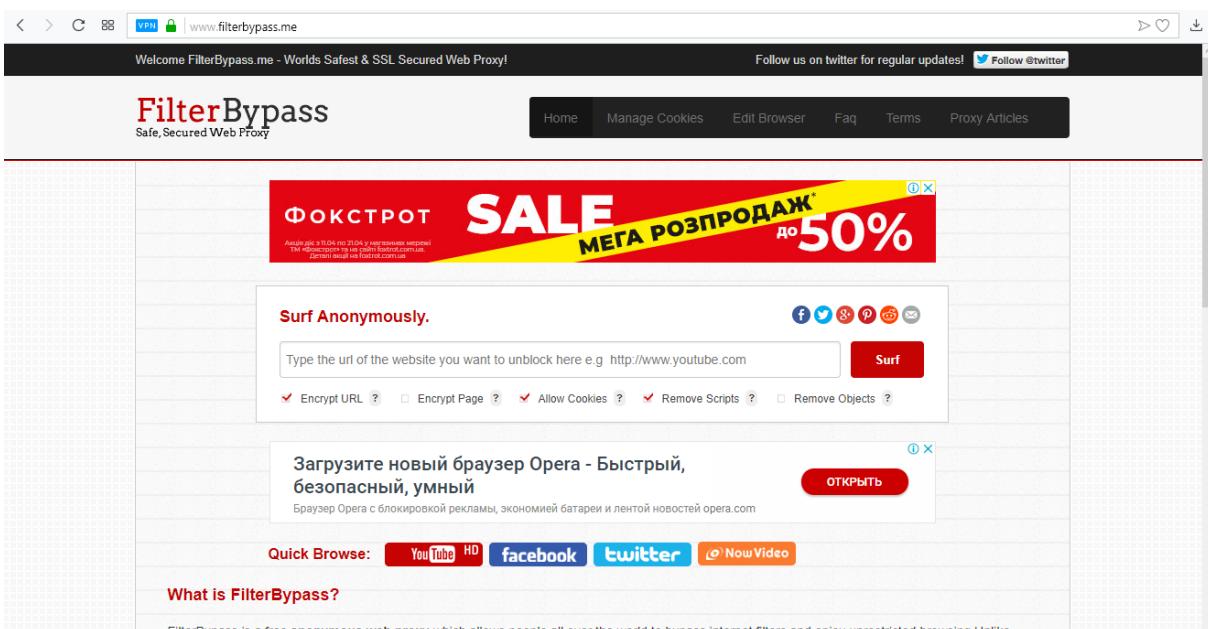
✓ حذف اسکریپت‌ها

✓ حذف اشیاء

✓ کاربر می‌تواند هر آنچه می‌خواهد در هر مورد بررسی کند.

FilterBypass.me

همانند zend2، کاربران می‌توانند با استفاده از گزینه‌های دیگر مانند رمزگذاری URL، اجازه کوکی و غیره در گشت‌وگذارها ناشناس بمانند. تنها نقص این پروکسی این است که نمی‌تواند برخی از سایت‌های ارائه ایمیل را حل کند، اما جدا از آن رابط کاربر شامل لینک‌هایی به سایت محبوب است که می‌تواند به طور مستقیم با استفاده از آن سایت‌هایی مانند فیسبوک، یوتیوب، DailyMotion، توییتر و غیره بازدید شوند.



Boomproxy.com

این کاملاً شبیه به anonymous.org است، زیرا تنها از سایت‌های http پشتیبانی می‌کند اما تنها ویژگی اضافی موجود در اینجا این است که حاوی گزینه‌هایی مانند رمزگذاری URL، حذف اشیاء و غیره است.

برخی از پروکسی‌های دیگر به شرح زیر می‌باشند:

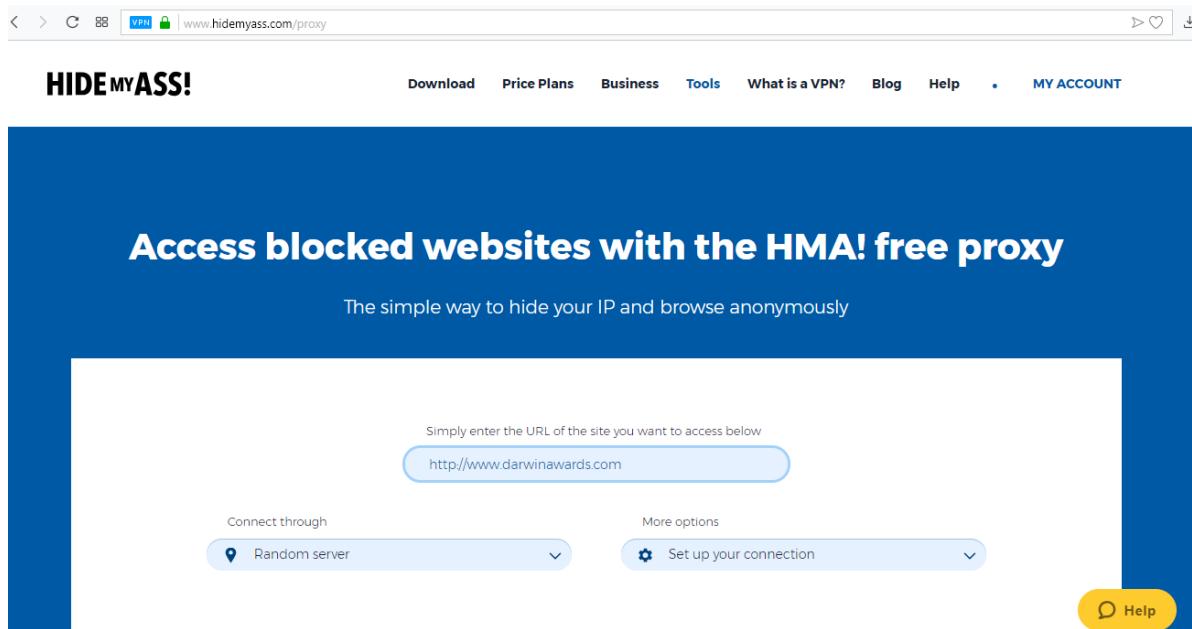
↳ <http://www.internetcloak.com/>

↳ <http://www.crownproxy.com/>

- ↳ <http://www.hidesurf.us/>
- ↳ <http://www.webevade.com/>
- ↳ <http://www.proxyemails.com/>
- ↳ <http://www.proxytopsite.us/>
- ↳ <http://www.proxysites.net/>
- ↳ <http://www.everyproxy.com/>
- ↳ <http://www.ip-hide.com/>
- ↳ <http://www.greatproxies.com/>
- ↳ <http://proxy.org/>
- ↳ <http://www.proxyservers.info/>
- ↳ <http://thehiddenguide.com>

چگونگی راه‌اندازی دستی پروکسی در مرورگرها

سایت‌های زیادی وجود دارد که آدرس پروکسی را به صورت IP آدرس و شماره پورت ارائه می‌دهند. به این دلیل که لیست ممکن است بعضی اوقات به روز شود و در عین حال سرور پروکسی ممکن است دیگر کار نکند. اگر چه ما می‌توانیم مقدار زیادی از سایت‌ها را دریافت کنیم، اما <http://proxylist.hidemyass.com/>. خوب است.



مزیت عمده این است که برای کاربر لیست به روز شده‌ای از آخرین آدرس‌های IP پروکسی و شماره‌های پورت را همراه با سرعت مورد انتظار، سطح ناشناس بودن و نام کشور که IP آن متعلق به آن است، فراهم می‌کند.

به استثنای آن کاربر همچنین می‌تواند شرایط موردنیاز را بر اساس کشور، پروتکل پشتیبانی شده، سرعت اتصال، سطح ناشناس بودن و بسیاری موارد دیگر محدود کند؛ بنابراین این یکی از بهترین منابع در مورد استفاده از پروکسی با IP و پورت است.

اگر چه در بیشتر موارد IP و پورت کار می‌کنند، اما قبل از استفاده از آن، بهتر است که آزمایش کنید آیا IP زنده^۱ است یا خیر.

بنابراین به سادگی یک آدرس IP و پورت مربوطه بر اساس الزامات مانند بر اساس سرعت، پروتکل، سطح ناشناسی تان و کشور را انتخاب کنید. سعی کنید آخرین موردی که اخیراً در فهرست بهروزرسانی شده را انتخاب کنید. سپس خط فرمان را در مورد ویندوز و ترمینال در مورد مک و لینوکس باز کنید. در مورد ویندوز نوع ipconfig را با آدرس IP انتخاب شده برای بررسی اینکه آیا IP زنده است یا خیر، تایپ کنید و در مک و لینوکس دستور ifconfig را با آدرس IP انتخاب شده، تایپ کنید.

هنگامی که ما IP را زنده می‌بینیم، آن را در مرورگر تنظیم می‌کنیم. در مورد موزیلا فایرفاکس ما آن را زودتر انجام دادیم، اما این روند را تکرار خواهیم کرد.

Firefox

Go to Tools → Options → Advanced → Network → Connection Settings → select Manual proxy configuration and use the chosen IP address and port number in respective fields.

Chrome

Go to Settings → Show advanced settings → under Network tab click on Change proxy settings → click on LAN settings → check Use a proxy server for LAN then use the chosen IP address and port number in respective fields.

شبکه خصوصی مجازی^۲

به طور واضح اجازه ایجاد یک شبکه خصوصی در یک شبکه عمومی که در اختصار VPN نامیده می‌شود. اکثر سازمان‌ها از یک شبکه خصوصی داخلی برای عملیات روزانه استفاده می‌کنند، اما گاهی اوقات مردم نیاز به دسترسی به این شبکه‌ها از جایی که اتصال مستقیم به این شبکه وجود ندارد، دارند. این زمانی است که VPN به کار می‌آید و اجازه می‌دهد تا کاربران به شبکه خصوصی از اینترنت، به صورت امن دسترسی یابند.

¹ Live

² VIRTUAL PRIVATE NETWORK

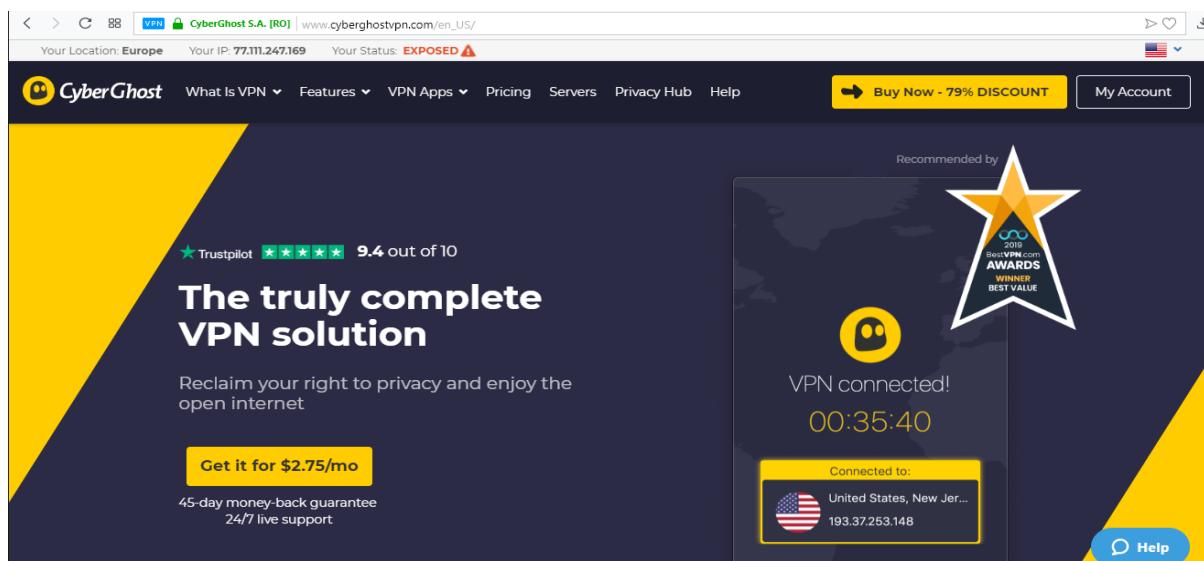
VPN اساساً یک نقطه مجازی برای اتصال بین دو ماشین است. سرور VPN در یک نقطه نصب شده و کاربر با استفاده از یک سرویس VPN به آن دسترسی می‌یابد. VPN از مکانیزم‌ها و فنون مختلف مانند احراز هویت، حق دسترسی، رمزگذاری و غیره استفاده می‌کند تا ضمن برقراری اتصال، آن را امن نگه دارد. موارد زیادی برای استفاده و پیاده‌سازی VPN و نحوه عملکرد آن وجود دارد، اما در این فصل تمرکز اصلی ما بر استفاده از آن برای ناشناس ماندن است.

ناشناس بودن مبتنی بر VPN شبیه به ناشناس بودن پروکسی است، تنها تفاوت عمدۀ این است که اتصال به سرور با استفاده از یک VPN لایه‌ای اضافی از امنیت را دارد، البته نباید فراموش کنیم که در اینجا به ارائه دهنده سرویس VPN اعتماد داریم.

سرвис‌های مختلفی وجود دارد که به صورت آنلاین در دسترس هستند و اکثر آن‌ها پولی هستند. در اینجا ما دو سرویس را ارائه می‌کنیم که نسخه رایگان ارائه می‌دهند، اما آن‌ها دارای محدودیت‌هایی مانند زمان محدود، سرعت و غیره هستند.

cyberghostvpn.com

یکی از بهترین ارائه‌دهندگان ناشناس ماندن مبتنی بر VPN CyberGhost است. این سرویس نسخه رایگان و پولی را فراهم می‌کند. برای استفاده از این سرویس ما نیاز به دانلود سرویس گیرنده آن از وبسایت CyberGhost را داریم. هنگامی که سرویس گیرنده دانلود می‌شود، می‌توانیم به سادگی آن را نصب کنیم و برنامه را شروع کنیم.





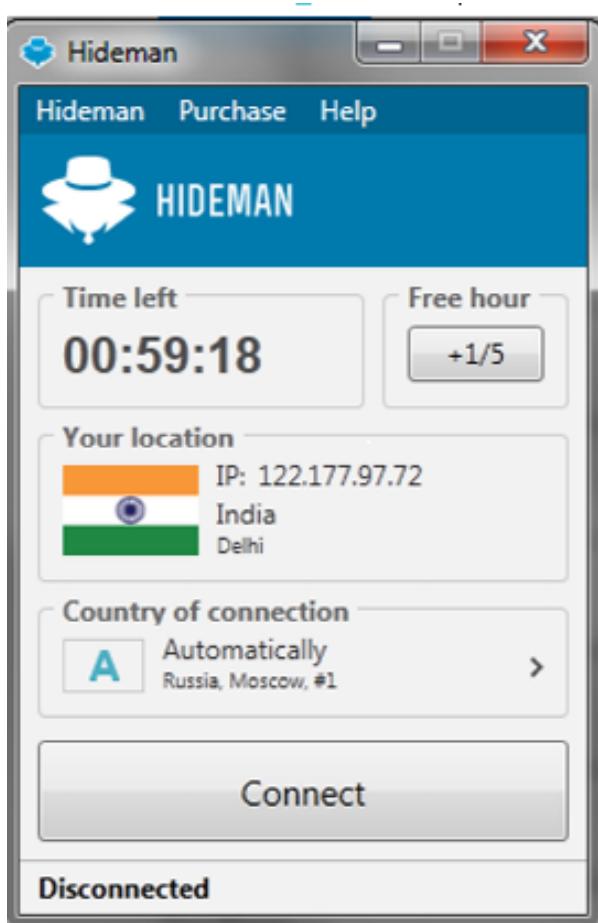
رابط کاربری نرم‌افزار بسیار ساده است. ما می‌توانیم تنظیمات را تغییر دهیم و همچنین آن را به یک حساب پولی ارتقاء دهیم. در صفحه اصلی، برنامه آدرس IP فعلی را با محل آن در نقشه، نشان می‌دهد. برای شروع استفاده از سرویس نیاز به کلیک بر روی دکمه پاور وجود دارد. هنگامی که روی آن کلیک می‌کنیم، CyberGhost اتصال به یکی از سرورها را آغاز می‌کند و هنگامی که اتصال ایجاد شود یک مکان جدید نمایش داده می‌شود.



در منوی تنظیمات CyberGhost همچنین می‌توانیم تغییراتی مانند کنترل حریم خصوصی و پروکسی ایجاد کنیم که به ما اجازه می‌دهد هویت مان را در هنگام اتصال به اینترنت پنهان کنیم.

Hideman

برنامه مشابه CyberGhost Hideman دیگری است که به ما امکان می‌دهد هویت مان را پنهان کنیم. سرویس گیرنده برنامه را می‌تواند از <https://www.hideman.net/> دانلود کنید؛ مانند CyberGhost، در Hideman نیز لازم نیست قبل از استفاده، تغییرات زیادی را ایجاد کنید، به سادگی برنامه را نصب و استفاده کنید. هنگامی که برنامه نصب شد، رابط گرافیکی کوچکی را فراهم می‌کند که IP و محل ما را نشان می‌دهد. در زیر آن گزینه‌ای وجود دارد که ما می‌توانیم کشور اتصال را انتخاب کنیم که به طور پیش فرض به صورت خودکار تنظیم شده است. هنگامی که این کار انجام شود، ما فقط باید بر روی دکمه اتصال کلیک کرده و ارتباط گیری شروع می‌شود. در حال حاضر Hideman برای ۵ ساعت در هفته رایگان است.



به غیر از سرویس‌های ذکر شده، راه‌های دیگری برای استفاده از VPN برای ناشناس بودن وجود دارد. برخی از ارائه‌دهندگان خدمات (ISP‌ها) VPN را فراهم می‌کنند که می‌تواند به هر سرویس گیرنده VPN متصل شود و مورد استفاده قرار گیرد.

شبکه‌های ناشناس^۱

یک شبکه ناشناس در نحوه عملکرد کمی متفاوت است. در اینجا ترافیک از طریق مسیری که تعدادی از کاربران مختلف در داخل اینترنت ایجاد کرده‌اند، مسیریابی می‌شوند. معمولاً کاربران شبکه مشارکت می‌کنند و به یکدیگر کمک می‌کنند تا رمز عبور را رله کنند. شبکه ساخته شده به‌طوری است که منبع و مقصد هرگز به‌طور مستقیم با یکدیگر ارتباط ندارند، اما ارتباط از طریق گره‌ها در چندین بار انجام می‌شود و از این رو ناشناس بودن به دست می‌آید.

The Onion Router

"The Onion Router" مخفف "Tor" است که یکی از محبوب‌ترین و گسترده‌ترین روش استفاده شده برای ناشناس ماندن آنلاین است. اساساً یک نرم‌افزار و یک شبکه باز است که به کاربران اجازه می‌دهد تا به صورت ناشناس به وب دسترسی داشته باشند. این پروژه به عنوان یک پروژه تحقیقاتی نیروی دریایی ایالات متحده آغاز شد و اکنون توسط یک سازمان غیرمستقیم اداره می‌شود. کاربر به سادگی نیاز به دانلود و نصب نرم‌افزار Tor و شروع به آن دارد. این برنامه یک پروکسی SOCKS محلی را راه‌اندازی می‌کند، سپس به شبکه Tor متصل می‌شود.

Tor از رمزنگاری لایه‌ای با تونل‌های دو طرفه استفاده می‌کند. این بدان معنی است که هنگامی که کاربر به شبکه Tor متصل می‌شود، بسته داده را با سه لایه رمزگذاری (تنظیمات پیش‌فرض) به گره ورودی شبکه Tor ارسال می‌کند. در حال حاضر این گره بالاترین لایه رمزگذاری را حذف می‌کند همان‌طور که کلید آن را دارد، اما بسته داده هنوز رمزگذاری شده است، بنابراین این گره می‌داند که فرستنده کیست، اما نه داده. در حال حاضر بسته داده‌ها به گره دوم حرکت می‌کند که به همان ترتیب لایه رمزگذاری بالا را نیز حذف می‌کند چون فقط همان کلید را دارد، اما این گره داده‌ها و همچنین فرستنده اصلی را نمی‌شناسد. بسته به گره بعدی شبکه Tor متصل می‌شود که آخرین لایه رمزگذاری را با استفاده از کلید که فقط برای آن لایه کار می‌کند، حذف می‌کند. در حال حاضر این گره آخر که گره خروج نیز نامیده می‌شود، بسته‌ی داده‌ای را در فرم خام خود دارد (بدون

^۱ ANONYMOUS NETWORKS

رمزگذاری)، بنابراین می‌داند که داده‌ها چه هستند، اما نمی‌دانند که فرستنده واقعی داده کیست. این بسته داده‌های خام پس از ارسال از فرستنده اصلی به اینترنت عمومی به گیرنده مورد نظر فرستاده می‌شود. همان‌طور که قبل‌اگفته شد این کار دو طرفه است بنابراین فرستنده می‌تواند پاسخ را به روش مشابه دریافت کند. یکی از چیزهایی که باید در اینجا ذکر شود این است که گره‌های شبکه Tor که بین آن‌ها بسته داده‌ها تبادل می‌شود، به صورت تصادفی انتخاب می‌شوند، هنگامی که کاربر می‌خواهد به یک سایت دیگر دسترسی داشته باشد، مشتری Tor دیگر مسیر تصادفی دیگری بین گره‌های شبکه Tor را انتخاب می‌کند. این فرایند کامل به عنوان onion routing شناخته می‌شود.

بنابراین Tor در مورد آنچه انجام می‌دهد خیلی خوب است و ما فقط یاد گرفتیم که چگونه کار می‌کند؛ اما همان‌طور که نیاز به استفاده از گره‌های مختلف (نقاط رله) و همچنین توابع رمزگاری وجود دارد، باعث می‌شود بسیار کند باشد. به غیر از این ما همچنین به گره‌های خروجی داده‌ها اعتماد داریم (آن‌ها می‌توانند بسته خام را بیینند).

Tor در قالب‌های مختلف به عنوان یک بسته نرم‌افزاری مرورگر و یا به عنوان یک بسته کامل سیستم عامل و غیره در دسترس است. بسته نرم‌افزاری مرورگر توصیه شده زیرا کاملاً به طور پیش فرض تنظیم شده است و برای استفاده بسیار آسان است و با تنظیمات اضافی که به حفظ امنیت کاربر کمک می‌کند. بسته نرم‌افزاری مرورگر اساساً یک مرورگر فایرفاکس قابل حمل با Tor است. همچنین حاوی برخی افزونه‌های اضافی مانند HTTPS Everywhere است. مرورگر Tor را می‌توانید از <https://www.torproject.org/download/download-easy.html.en> دانلود کنید. هنگامی که آن را دانلود می‌کنیم، ما فقط باید فایل Exe را اجرا کنیم و آن را در دایرکتوری ذکر شده استخراج کنیم. پس از اتمام، نیاز به اجرای برنامه Start Tor Browser را داریم که مرورگر فایرفاکس قابل حمل با Tor است. یا به طور مستقیم به شبکه Tor متصل شده و یا آن را قبل از رفتن تنظیم کنید. کاربران عمومی فقط باید بر روی دکمه اتصال کلیک کنند، در صورتی که شبکه ما متصل به پروکسی یا سایر تنظیمات پیشرفت نیازمند باشد، می‌توانیم روی دکمه Configure کلیک کنیم تا این تنظیمات را برای اولین بار انجام دهیم. هنگامی که به شبکه وصل شویم، مرورگر Tor به محض اتصال باز خواهد شد. جدا از این بسته‌های دیگر که به ما اجازه می‌دهد پل، رله و خروج از گره را اجرا کنیم از <https://www.torproject.org/download/download.html.en> دانلود می‌شود.



به غیر از اجازه دادن به کاربران برای گشت و گذار در وب به صورت ناشناس، Tor همچنین سرویس جالب دیگری را ارائه می‌دهد که در فصل بعدی آن را یاد خواهیم گرفت.

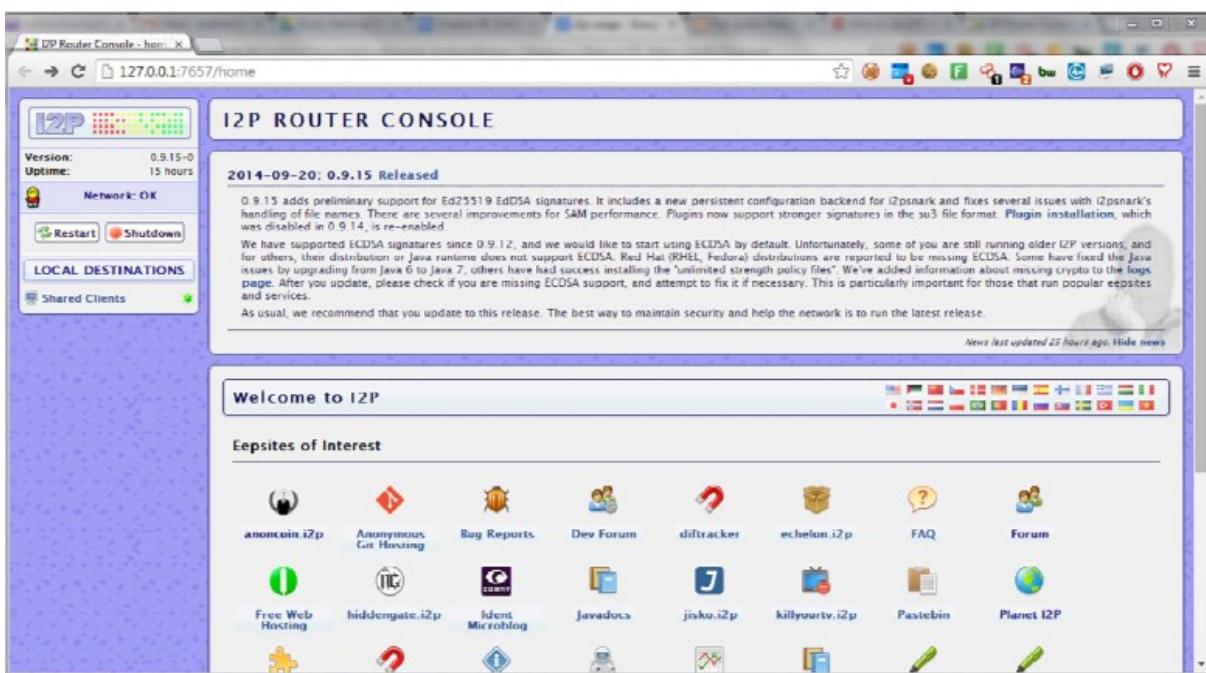
پروژه اینترنت نامرئی

I2P مخفف Invisible Internet Project است. همانند Tor، I2P یک شبکه ناشناس است؛ مانند هر شبکه، گره‌های متعددی در این شبکه وجود دارد که برای انتقال بسته‌های داده استفاده می‌شود. در مقابل Tor، I2P بیشتر بر سرویس دهی داخلی مرکزی است. این به این معنی است که مرکز اصلی Tor این است که اجازه دهیم مردم به وب به صورت ناشناس دسترسی پیدا کنند (در فصل بعد توضیح داده شده است)، در حال حاضر فقط می‌توان گفت که بخشی از وب بدون هیچ محدودیتی قابل دسترسی است، در حالی که I2P به اجازه استفاده ناشناس از وب می‌پردازد اما در چارچوب برنامه‌ها و یا ویژگی‌های موجود در آن، مانند خدمات پست الکترونیکی، IRC ها، تورنت ها و غیره.

برخلاف Tor، I2P از رمزنگاری لایه‌ای روی اتصالات یک طرفه استفاده می‌کند. هر برنامه سرویس دهنده I2P دارای روتراهای I2P است که تونل‌های ورودی و خروجی را ایجاد می‌کند؛ بنابراین هر مشتری دارای نقاط ورودی و خروجی متفاوت است. هنگامی که مشتری نیاز به ارسال یک پیام به مشتری دیگر دارد، آن را با مشخص کردن هدف به تونل خروجی خود ارسال می‌کند. بسته به تنظیمات، این پیام از طریق تعدادی از مشتریان آپلود می‌شود

و در نهایت به گره ورودی هدف و سپس به هدف می‌رسد. برای دریافت پیام به ترتیب معکوس، فرایند مشابهی دنبال خواهد شد، اما گره‌های مربوطه متفاوت خواهند بود زیرا تونل‌های ورودی و خروجی از یکدیگر، برای هر گره جدا می‌شوند. هر محتوایی که بر روی I2P منتقل شده با استفاده از رمزگذاری لایه‌بندی منتقل می‌شود. لایه‌های رمزنگاری عبارت‌اند از رمزنگاری مسیر بین گره شروع تونل خروجی فرستنده به گره پایانی تونل ورودی گیرنده؛ رمزنگاری که بین گره شروع تونل خروجی به گره پایان آن و گره شروع تونل ورودی به گره پایان آن است؛ رمزنگاری انتقال بین هر گره و گره بعدی.

I2P را می‌توان از <https://geti2p.net/en/download> دانلود کرد. نصب نرم‌افزار بسیار ساده است. پس از اتمام نصب، ماقبل باید "Start I2P" را باز کنیم، کنسول آن باز می‌شود. در صورتی که صفحه وب باز نشود، می‌توانیم به سادگی به آدرس <http://127.0.0.1:7657/home> برویم و صفحه‌ای را نشان خواهد داد. هنگامی که برنامه به دیگر گره‌ها اتصال ایجاد کند، وضعیت "Network: OK" را دریافت می‌کنیم. حالا باید یک مرورگر را برای اتصال از طریق I2P تنظیم کنیم، برای این منظور باید تنظیمات پروکسی دستی را به آدرس 127.0.0.1 و پورت 4444 تنظیم کنیم. همچنین پیشنهاد می‌شود که "No Proxy for" localhost, 127.0.0.1 را به جعبه "را به جعبه" اضافه کنید. هنگامی که تنظیمات پروکسی انجام شد، می‌توانیم با استفاده از این مرورگر به صورت ناشناس به مرور اینترنت پردازیم.



همانند تور، P2P خدمات دیگری نیز ارائه می‌دهد که ما در فصل بعدی بحث خواهیم کرد. افزونه مرورگر مانند FoxyProxy (<http://getfoxyproxy.org/>) می‌تواند مورد استفاده قرار گیرد.

تکنیک‌های که در این فصل مورد بحث قرار گرفته‌اند می‌توانند به هم متصل شده تا امکان شناسایی را دشوارتر کنند. به عنوان مثال، ما می‌توانیم به یک پروکسی مبتنی بر VPN متصل شویم و از آن برای اتصال به یک سرور پروکسی در کشوری دیگر و سپس با استفاده از یک پروکسی مبتنی بر وب برای دسترسی به یک وب‌سایت استفاده کنیم. در این مورد، سرور وب آدرس IP سرور پروکسی مبتنی بر وب را که برای اتصال به آن استفاده می‌شود و آدرس IP سرور پروکسی که از طریق VPN متصل می‌شود را دریافت می‌کند. ما همچنین می‌توانیم طول این زنجیره را با اتصال پروکسی‌ها به یکدیگر افزایش دهیم. همچنین تکنیکی به نام proxy bouncing or hopping وجود دارد که کاربر از یک پروکسی به دیگری با استفاده از یک ابزار خودکار یا اسکریپت سفارشی با لیست پروکسی‌ها می‌رود، به این ترتیب کاربر هویت خود را تغییر می‌دهد و از این رو، ردیابی بسیار دشوار است.

برخی از سناریوهایی که در آن شخص پس از استفاده از این ابزار و یا تکنیک‌ها گرفتار می‌شوند:

- کاربر در یک شبکه اختصاصی (مثلًاً دانشگاه) شناخته شده است و همچنین مشخص است که کدام یک از آن‌ها به پروکسی خاص و یا Tor در یک زمان مشخص متصل شدند.
- نقاط ورود و خروج. در یک شبکه ناشناس مانند Tor نقطه ورود و نقطه خروج می‌تواند بسته‌های داده را با توجه به اندازه یا امضا مرتبط کند و شاید شناسایی فرستنده واقعی ممکن باشد.
- نشت DNS. گاهی اوقات حتی زمانی که ما به یک شبکه ناشناس وصل می‌شویم، ماشین‌های ما ممکن است درخواست‌های DNS را به سرور DNS پیش فرض به جای سرور DNS ناشناس شبکه ارسال کنند. این بدان معنی است که سرور پیش فرض در حال حاضر ممکن است یک ورودی داشته باشد که این آدرس خاص توسط این IP در این نقطه زمان درخواست شده است.
- نشت اطلاعات شخصی. گاهی اوقات افرادی که در اینترنت ناشناس هستند، اطلاعاتی را که می‌توان از به‌طور مستقیم به آن‌ها رسید، مانند شماره تلفن‌ها، شناسه‌های منحصر به فرد و غیره را استفاده می‌کنند.
- فراداده. همان‌طور که در فصل گذشته بحث شد، داده‌های پنهانی در فایلی که ما استفاده می‌کنیم وجود دارد که ممکن است برای ردیابی یک فرد استفاده شود.

- هک کردن. حفره‌های امنیتی در هر محصول فناوری اطلاعات وجود دارد که می‌تواند مورد استفاده قرار گیرد تا هویت واقعی افراد مورد استفاده را شناسایی کند.
- همبستگی پایه. همان‌طور که در سناریوی اول نشان داده شد، همبستگی می‌تواند برای تعیین یک فرد بر اساس عوامل مختلف مانند زمان بندی، مکان، استفاده محدود و سایر عوامل استفاده شود.

برخی از پیشنهادات و یا هشدارها برای استفاده از Tor در <https://www.tor-project.org/download/download-easy.html.en#warning> ذکر شده است. آن‌ها باید در استفاده از هر وسیله و یا تکنیک مورد بحث در بالا، در صورت لزوم، دنبال شوند. همچنین از یک مرورگر جداگانه برای استفاده ناشناس استفاده کنید و افرونه و یا پلاگین هایی را که لازم نیست، نصب نکنید.

بنابراین در مورد راه‌های مختلف برای ناشناس ماندن آنلاین در اینترنت یاد گرفتیم، اما همان‌طور که قبل‌اگفته شد، ناشناس بودن ۱۰۰٪ نمی‌تواند تضمین شود. آنچه می‌توانیم انجام دهیم این است که سعی کنیم اطلاعات کمی در مورد خودمان ابراز کنیم. روش‌های مورد بحث در این فصل، روش‌های محبوب و مؤثر برای انجام این کار هستند. ناشناس بودن آنلاین می‌تواند موارد استفاده مختلفی نظیر حفظ حریم خصوصی، اعتراض، دسترسی به آنچه توسط مقامات محدود شده، تجارت، اجرای قانون، روزنامه‌نگاری محدود شود، اما همچنین می‌تواند توسط افراد برای انجام فعالیت‌های غیرقانونی مانند هک، تجارت آنلاین غیرقانونی، پول‌شویی، فروش مواد مخدر و غیره استفاده شود.

در فصل بعد، موضوع را گسترش خواهیم داد و با تارنمای darknet و سایر شرایط مرتبط آن آشنا خواهیم شد. ما در مورد ابزارهایی مثل Tor و I2P بیشتر بحث خواهیم کرد تا بینیم که چه قسمت‌هایی از اینترنت را هنوز لمس نکرده‌ایم، چگونگی دسترسی به آن و یا ایجاد آن و آنچه ما می‌توانیم انتظار آن را داشته باشیم.

فصل ۹: کاوش تاریک‌ترین گوشه‌های اینترنت (Deepweb)

مقدمه

ما در مورد ابزار و تکنیک‌های مختلف مربوط به چگونگی ناشناس ماندن آنلاین یاد گرفتیم. در اینجا با مفاهیم دیگری مانند deepweb و darknet آشنا خواهیم و برخی از تفاوت‌های اساسی آنها را در کم خواهیم کرد.

یکی از راه‌های مؤثر برای ناشناس ماندن، اتصال به شبکه‌های ناشناس مثل Tor و I2P بود. ما این موضوع را آموخته می‌خواهیم ببینیم چه چیز دیگری با آن می‌توانیم انجام دهیم و نحوه ارتباط آن با موضوع موردنبحث این فصل چیست.

در گذشته شبکه‌هایی مانند darknet و deepweb خیلی محبوب نبودند. آنها عمدتاً موضوع مورد علاقه افرادی بود که می‌خواستند ناشناس باشند و حوزه کارشان مرتبط با فناوری اطلاعات (به ویژه امنیت اطلاعات) بود. اخیراً برخی از اخبار مربوط به این موضوعات منتشر شده که مردم را به آنچه دارند، چگونه کار می‌کنند، چه انتظاری از آن وجود دارد و غیره، علاقه‌مند کرده است. ما تمام این موارد را در اینجا پوشش خواهیم داد.

قبل از رفتن به جزئیات فنی، ببینید به واژه‌های پایه‌ای که در این فصل در مورد آنها بحث خواهیم کرد، بپردازیم:

CLEARWEB

ما در فصل‌های قبلی در مورد نحوه کار موتورهای جستجو صحبت کرده‌ایم. به‌سادگی می‌توان گفت، با مرور لینک‌ها در یک صفحه وب وغیره کار می‌کند؛ بنابراین بخشی از وب که توسط یک موتور جستجو قابل دسترسی است، Clearweb نامیده می‌شود. این بدان معنی است که هر چیزی که ما در نتیجه یک موتور جستجو دریافت می‌کنیم بخشی از وب Clearweb است.

DARKWEB

به عنوان یک کاربر، ما بر روی لینک‌های مختلف در یک صفحه وب کلیک کرده‌ایم، اما این تنها راه ارتباط ما با یک وب‌سایت نیست. گاهی اوقات ما باید متنی را برای دریافت صفحه مورد نظر (به عنوان مثال در کادر جستجو) وارد کنیم، گاهی اوقات قبل از دسترسی به یک صفحه خاص (مثلًاً ورود به وب‌سایت شبکه اجتماعی) باید احراز هویت کنیم، گاهی اوقات قبل از آن چیزهایی مانند CAPTCHA باید وارد شوند.

بنابراین به غیر از وب که توسط موتورهای جستجو قابل دسترسی است، مقدار زیادی از داده‌ها در صفحاتی که توسط عنکبوت و یا خزنده‌ها وب دیده نمی‌شود، وجود دارند که. این قسمت از وب به نام darknet یا darkweb شناخته می‌شود.

DEEPWEB

اکنون بر اساس دسترسی توسط موتور جستجو، وب را به دو قسمت تفکیک کردیم، Clearweb و Darkweb. حالا کمی عمیق‌تر می‌شویم.

اکنون شامل بخش بزرگی از وب اصلی است. در داخل این darkweb بخش دیگری وجود دارد که به عنوان deepweb نامیده می‌شود. این فضای نیز برای موتورهای جستجو خاصی قابل دسترسی است، اما به‌طور مستقیم توسط مرورگرهای استاندارد که هر روز استفاده می‌کنیم، قابل دسترسی نیستند. این قسمت از وب در داخل darkweb است و با برنامه‌های کاربردی و تنظیمات خاص، دسترسی به آن‌ها امکان پذیر می‌شود و از این رو deepweb نامیده می‌شود.

اکنون در ک درستی از web و deepweb داریم. ما از نحوه دسترسی به darkweb آگاهیم. صفحات مانند پروکسی رسانه‌های اجتماعی که نیاز به ورود به سیستم دارند، صفحه نتایج جستجو در یک وب‌سایت، صفحات تولیدشده به صورت پویا، بعضی از نمونه‌هایی از آن هستند. با این حال اگر ما نیاز به دسترسی به deepweb داشته

باشیم، باید تنظیمات خاصی را انجام دهیم. قبل از وارد شدن به این جزئیات، کمی در مورد deepweb بحث می‌کنیم.

همان‌طور که قبلاً گفته شد deepweb بخشی از darkweb است. حالا سؤال این است که چگونه زمانی که داخل darkweb وجود دارد به‌طور مستقیم قابل دسترسی نیست؟ پاسخ این است که آن در قالب یک شبکه در داخل اینترنت وجود دارد که به خودی خود یک شبکه عظیم است، بدین معنی که darkweb به عنوان بخشی از اینترنت ایجاد می‌شود، اما برای دسترسی به این شبکه اختصاصی ما باید مجوز داشته باشیم. هنگامی که ما وسیله‌ای برای اتصال به آن داریم، می‌توانیم به آن دسترسی داشته باشیم.

در deepweb ما می‌توانیم انواع چیزهایی مانند مواد مخدر غیرقانونی، سلاح، هنر و همه نوع بازار سیاه را پیدا کنیم. از سوی دیگر، توسط اشخاص برای صحبت آزادانه، مبالغه ایده‌ها و غیره استفاده می‌شود.

چرا از deepweb استفاده می‌شود؟

اگر ما خبرنگار سایبری، روزنامه‌نگار اینترنتی، خبرنگار دولتی و یا محقق سایبری باشیم، این مکان برای ماست. این کار به ما کمک خواهد کرد که بدانیم چگونه فضای مجازی زیرزمینی کار می‌کند. این به ما ایده‌هایی در مورد اهداف و الگوهای جرائم اینترنتی و غیره می‌دهد. این به ما امکان در پیش‌بینی الگوی حملات آتی کمک می‌کند تا به درک تفکر جامعه زیرزمینی از طریق تکنولوژی که بیشترین استفاده را دارد، برسیم.

این شبکه آزادی بیان را فراهم می‌کند، بنابراین اگر می‌خواهید اعتراض کنید، این مکان برای شماست. برای بررسی جنایات سایبری می‌تواند یک مکان محبوب باشد. همان‌طور که بسیاری از انجمان‌های زیرزمینی در اینجا کار می‌کنند، این احتمال وجود دارد که دلایل کافی را از این مکان به دست آورید. این شبکه همچنین می‌تواند برای پیگیری فعالیت‌های آنلاین یک فرد یا گروه مورد استفاده قرار گیرد.

خدمات اختصاصی برای استفاده بهینه از deepweb از قبیل امکانات آپلود فایل ایمن وجود دارد که در آن فعالان یا خبرگان می‌توانند اسناد را به صورت ناشناس ارسال کنند. خدماتی در ارتباط با افرادی که در حال گسترش حقایقی هستند و دیگران باید بدانند، به اشتراک گذاشتن آنچه در اطراف آنها وجود دارد و اتفاق می‌افتد و غیره. انجمان‌های آنلاین برای بحث در مورد فن آوری، سیاست و خیلی چیزهای دیگر وجود دارد؛ بنابراین اگر ما این نوع الزامات خاص و یا دلایل مشابهی را داشته باشیم، می‌توانیم از deepweb استفاده کنیم.

چرا به deepweb نیازی ندارید؟

به غیر از استفاده از این فضا برای انگیزه‌های اخلاقی، برخی از افراد نیز از آن برای انجام بسیاری از فعالیت‌های غیرقانونی استفاده می‌کنند. مکان‌های بسیاری در این شبکه وجود دارد که ممکن است توانیم فروش مواد مخدر، استفاده جعلی، پول‌شویی، هکرها و غیره را پیدا کنیم. بعضی از وب‌سایت‌ها حتی استخدام قاتل هم انجام می‌دهند. به غیر از این ممکن است وب‌سایت‌هایی نیز وجود داشته باشد که بسیاری از موارد مزاحم را ارائه می‌دهند. باید در هنگام دسترسی یا دانلود هرگونه محتوی از چنین مکان‌هایی بسیار مراقب باشید، ممکن است دسترسی به آن در رایانه‌های ما غیرقانونی باشد.

سروریس‌های DARKNET

TOR

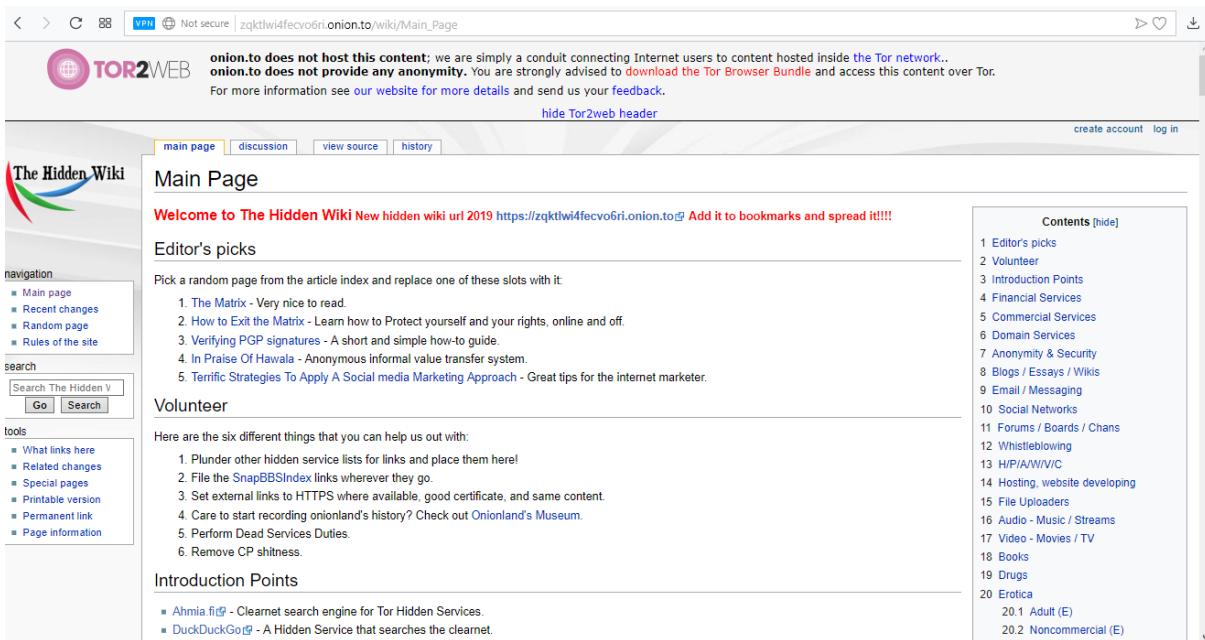
یکی از محبوب‌ترین بخش‌های deepweb، دامنه onion است. در فصل گذشته دیدیم که چگونه کار می‌کند و همچنین چگونه در ناشناس ماندن استفاده می‌شود. Tor همچنین ما را قادر می‌سازد تا یکی از بزرگ‌ترین بخش‌های deepweb را ایجاد و به آن دسترسی داشته باشیم. ما در مورد چگونگی استفاده از بسته نرم‌افزاری مرورگر Tor برای دسترسی به وب معمولی آگاهی داریم، در حال حاضر همان ابزار را می‌توان برای دسترسی به مکان‌هایی که به طور مستقیم دستیابی نمی‌شوند، استفاده کرد.

به سادگی باید بسته نرم‌افزاری مرورگر Tor را دانلود و آن را استخراج و مرورگر Tor را اجرا کنیم. هنگامی که اتصال به شبکه Tor ساخته می‌شود، به غیر از دسترسی به وب‌سایت‌ها، Tor اجازه می‌دهد تا وب‌سایت‌های *.onion را ایجاد و یا به آن‌ها دسترسی یابیم که از طریق مرورگرهای معمولی بدون Tor قابل دسترسی نیستند و پیام خطای "صفحه وب در دسترس نمی‌باشد"، نشان داده می‌شود؛ در حالی که آن وب‌سایت از طریق مرورگر Tor یا یک مرورگر تنظیم شده برای دسترسی به اینترنت از طریق Tor به عنوان یک پروکسی، باز خواهد شد.

شروع به بررسی این دامنه‌ها مبتنی بر Tor می‌کنیم. یکی از رایج‌ترین مکان‌ها برای شروع "The Hidden Wiki" به آدرس http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page شامل com، org یا سایر نام‌های دامنه آشنا نیست، بلکه onion است. اگر سعی کنید این URL را در یک مرورگر معمولی باز کنید، آیا باز می‌شود؟ در حال حاضر این URL را در مرورگر Tor باز کنید. یک صفحه وب که حاوی یک صفحه ویکی است با لیست عظیمی از دیگر دامنه‌های دسته‌بندی onion دریافت می‌کنیم. دسته‌بندی‌های ذکر

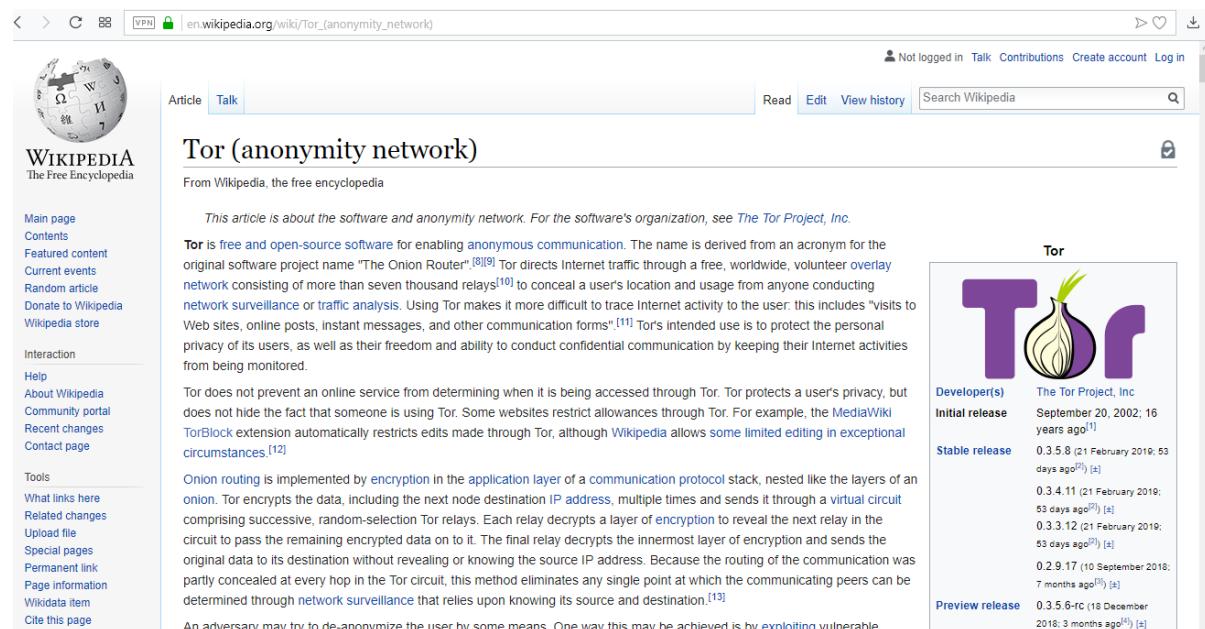
شده شامل خدمات مالی، ناشناس بودن و امنیت، اطلاع‌رسانی ناگهانی، به اشتراک‌گذاری P2P و غیره می‌باشد.

ما می‌توانیم این ویکی و برخی از پیوندهای جالب موجود در آن را بررسی کنیم.



The screenshot shows the homepage of The Hidden Wiki, a dark-themed website. At the top, there's a banner from TOR2WEB with text about the Tor network. Below it, the main navigation bar includes links for 'main page', 'discussion', 'view source', and 'history'. A sidebar on the left contains sections for 'navigation' (Main page, Recent changes, Random page, Rules of the site), 'search' (Search The Hidden V, Go, Search), and 'tools' (What links here, Related changes, Special pages, Printable version, Permanent link, Page information). The main content area features a heading 'Main Page' and a red banner 'Welcome to The Hidden Wiki New hidden wiki url 2019 https://zqktlwi4fecvo6ri.onion.to Add it to bookmarks and spread it!!!!'. Below this, there are three sections: 'Editor's picks' (a list of 5 items), 'Volunteer' (a list of 6 items), and 'Introduction Points' (a list of 2 items). To the right, a 'Contents' sidebar lists 20 categories ranging from 'Editor's picks' to 'Erotica' with sub-categories like 'Adult (E)' and 'Noncommercial (E)'. The overall layout is cluttered with many links and sections.

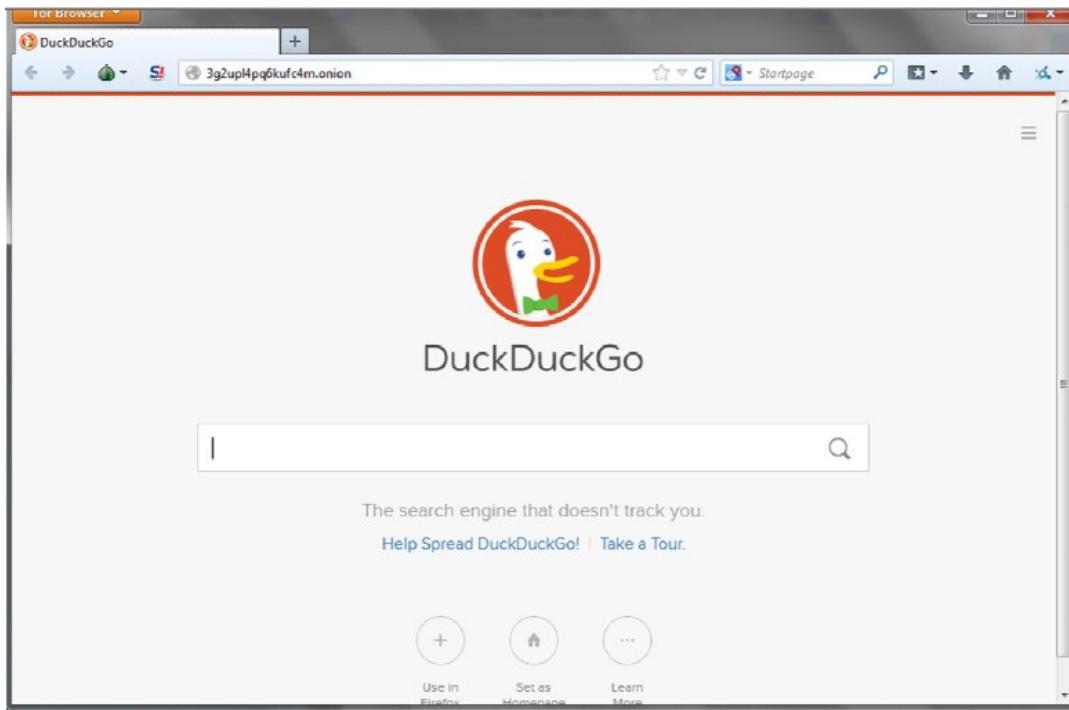
به همین ترتیب ویکی دیگری نیز به نام "Tor Wiki" وجود دارد که لیست گسترده از دامنه‌های onion را فهرست می‌کند. این ویکی باعث می‌شود که استفاده از دامنه‌های ذکر شده با علامت‌گذاری آنها به عنوان تائید، احتیاط یا کلاهبرداری آسان‌تر باشد.



The screenshot shows the English Wikipedia article on 'Tor (anonymity network)'. The page has a standard Wikipedia layout with a sidebar on the left containing links for 'Main page', 'Contents', 'Featured content', etc. The main content starts with a brief introduction and then delves into the technical details of how Tor works. It explains that Tor is free and open-source software that directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. The article also discusses the privacy of its users and the challenges of being monitored. On the right side, there is a large image of the Tor logo (a stylized purple onion) and a table providing information about the project's releases:

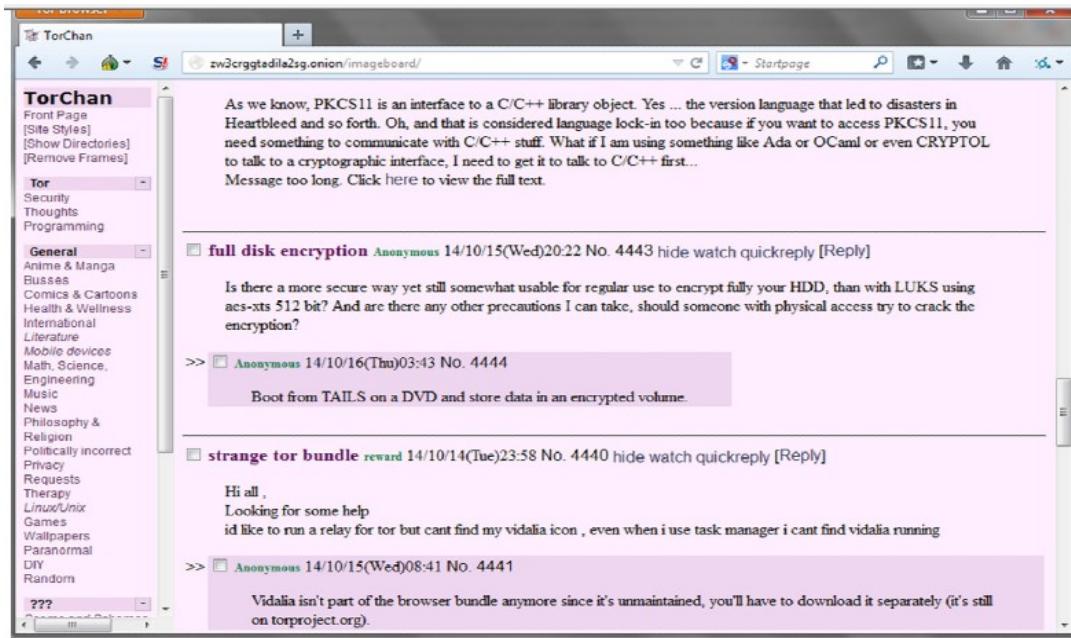
	Developer(s)	Initial release	Stable release	Preview release
	The Tor Project, Inc.	September 20, 2002; 16 years ago ^[1]	0.3.5.8 (21 February 2019; 53 days ago ^[2]) [ε]	0.3.4.11 (21 February 2019; 53 days ago ^[3]) [ε]
			0.3.3.12 (21 February 2019; 53 days ago ^[4]) [ε]	0.2.9.17 (10 September 2018; 7 months ago ^[5]) [ε]
				0.3.5.6-rc (18 December 2018; 3 months ago ^[6]) [ε]

موتور جستجو DuckDuckGo که ما در فصل قبلی بحث کردیم، دارای یک نشانی اینترنتی، است. با استفاده از آن می‌توانیم [deepweb](http://3g2upl4pq6kufc4m.onion/) را از دامنه Tor جستجو کنیم.



همچنین برخی از موتورهای جستجو مانند TORCH به آدرس <http://xmh57jrzrnw6insl.onion> به آدرس deepweb وجود دارد، اما آن‌ها به درستی کار می‌کنند.

همان‌طور که می‌بینیم در لیست ویکی‌ها، بازارهای مختلفی وجود دارد که مواد مخدر غیرقانونی را به فروش می‌رسانند. یکی از محبوب‌ترین آن‌ها به نام "Silk Road" نامیده شد که توسط FBI کشف شد، اما یک سایت جدید جای آن را گرفته و "Road Silk Road 2.0" نامیده است. به‌طور مشابه، بسیاری از مکان‌های دیگر نیز وجود دارد که شامل موارد غیرقانونی مانند انجمان‌های مختلف، چت‌های ارتباطی اینترنتی (IRC) برای افراد هم‌جنس گرا می‌باشند. یکی از آن‌ها Torchan <http://zw3crggtadila2sg.onion/imageboard/> است. موضوعات مختلفی از قبیل برنامه‌نویسی، ادبیات، حفظ حریم خصوصی و غیره وجود دارد که مردم در موردشان بحث می‌کنند.



تا کنون ما شاهد چگونگی دسترسی به وب‌سایت‌های دامنه onion بودیم، اکنون ببینید چگونه آن‌ها می‌توانند ایجاد کنند. برای ایجاد یک سایت onion ابتدا باید یک سرور وب محلی داشته باشیم. XAMPP یکی از گزینه‌هایی است که از Apache به عنوان یک سرور استفاده می‌کند. هنگامی که سرور نصب و برای میزبانی یک وب‌سایت محلی تنظیم شد، ما باید فایلی "torrc" را اصلاح کنیم. این فایل را می‌توانید در محل "Tor Browser \ Data \ Tor" پیدا کنید. این فایل را در ویرایشگر باز و خطوط زیر را به آن اضافه کنید:

```
HiddenServiceDir C:\Tor\Tor_Browser\hidden
HiddenServicePort 80 127.0.0.1:80
```

مسیر در مقابل "HiddenServiceDir" مسیری است که Tor برای ایجاد اطلاعات مربوط به سرویس مخفی، ایجاد می‌کند. قسمت قبل از "HiddenServicePort" حاوی پورتی است که کاربران Tor که آن‌ها برای اتصال به سرویس استفاده می‌کنند و بخش بعدی مکانی است که در آن سرویس به طور محلی اجرا می‌شود.

Name	Date modified	Type	Size
Browser	10/1/2014 3:33 PM	File folder	
Data	10/1/2014 3:33 PM	File folder	
Docs	10/1/2014 3:33 PM	File folder	
Tor	10/1/2014 3:33 PM	File folder	
hostname	10/28/2014 1:28 AM	File	1 KB
private_key	10/28/2014 1:28 AM	File	1 KB
Start Tor Browser	1/1/2000 5:30 AM	Application	37 KB

هنگامی که این اطلاعات به فایل اضافه شد، آن را ذخیره و Tor را راهاندازی مجدد کنید. هنگامی که شروع می‌شود، دو فایل در پوشه فوق ذکر شده: **hostname** و **private_key** ایجاد می‌شود. **hostname** حاوی نام‌هایی است که می‌توانند برای دسترسی به صفحات وب از طریق Tor در دامنه onion استفاده شوند. محتويات فایل **private_key** باید مخفی نگهداشته شود تا هیچ‌کس دیگر نتواند سرویس ما را جعل کند.

ما شاهد چگونگی ایجاد سرویس پنهان تور هستیم، اما برای اینکه اینکه ایمن و ناشناس باشیم، باید اقدامات مختلفی انجام دهیم:

- سرور را تنظیم کنید تا هیچ اطلاعاتی نشود کنید (به عنوان مثال، نشانگر سرور، پیام‌های خط).
- در این دستگاه هیچ سرویسی را اجرا نکنید که ممکن است به هر حمله آسیب پذیر باشد یا هویت شما را فاش کند.
- امنیت برنامه وب را بررسی کنید.

Tor همچنین به ما اجازه می‌دهد تا خدمات پنهان را از طریق رله‌ها^۱ اجرا کنیم اما توصیه نمی‌شود. رله‌ها گره‌هایی هستند که در انتقال شبکه‌های توزیع شرکت می‌کنند و به عنوان روتربرا آن عمل می‌کنند. رله‌ها از انواع مختلفی هستند: رله‌های متوسط - که شروع و گره‌های متصل در زنجیره انتقال بسته هستند. رله خروج - که گره نهایی در زنجیره است و به طور مستقیم به گیرنده متصل می‌شود. پل‌ها - که رله‌هایی هستند که به طور عمومی به عنوان رله‌های Tor شناخته نمی‌شوند. پل‌ها هنگامی که ما از طریق یک شبکه تحت نظارت / مدیریت شده (به عنوان مثال، شبکه دانشگاه) به اینترنت متصل می‌شوند مفید می‌باشند، زیرا کاربر را به Tor از این شبکه متصل می‌کند. برنامه‌ها

¹ relays

برای اجرای این سرویس‌ها می‌توانند از صفحه <https://www.torproject.org/download/download.html.en> دانلود شوند.

I2P

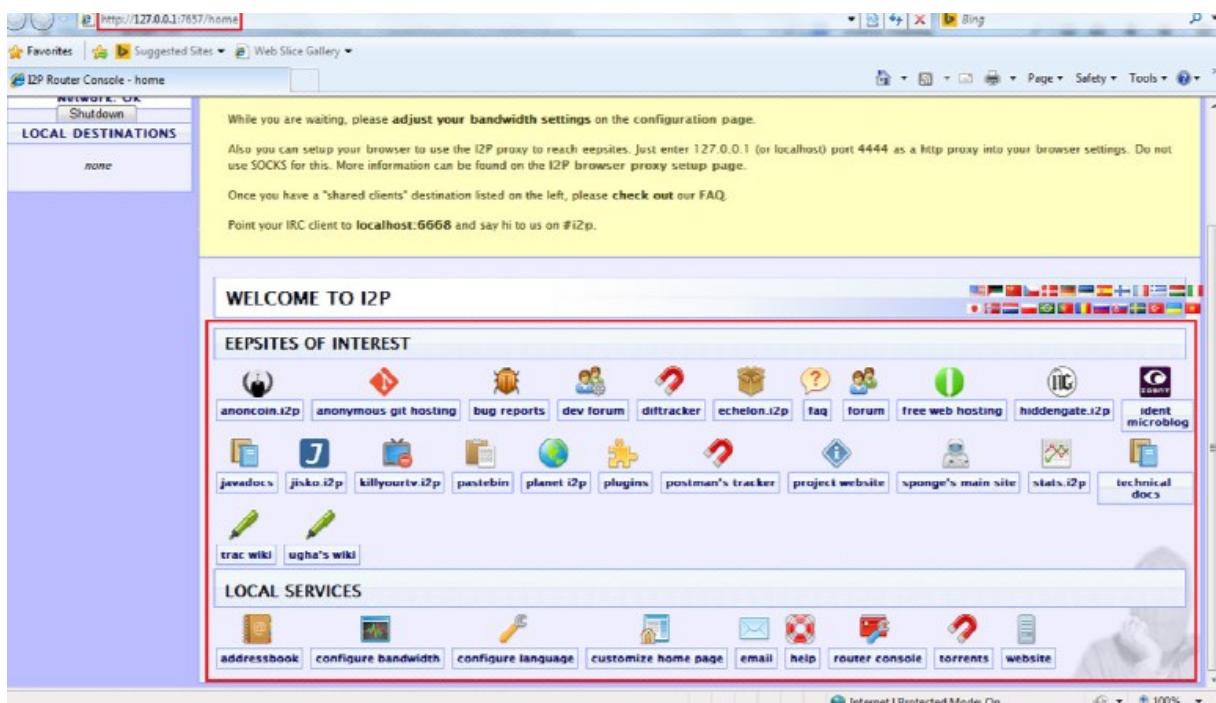
همانند Tor ما یاد گرفتیم که چگونه با استفاده از I2P ناشناس شویم. در حال حاضر در این فصل ما بر روی بخش ناشناسی تمرکز نمی‌کنیم اما بر روی چگونگی استفاده از I2P برای دسترسی به و یا ایجاد وبسایت در deepweb تمرکز خواهد کرد.

اگرچه تعداد زیادی از مکان‌های خدمات پنهانی مربوط به I2P وجود دارد و در بیشتر مکان‌ها سایت‌ها صحت خدمات ارائه شده را ادعا می‌کنند، بهتر است قبل از استفاده یا دسترسی به هر یک از آن‌ها برای جلوگیری از پیامدهای ناشناخته، آن‌ها را بررسی کنیم.

ما قبلاً می‌دانیم که چگونه I2P را نصب کنیم، همان‌طور که در فصل گذشته یاد گرفتیم. ما می‌توانیم به راحتی آن را از URL زیر دانلود و نصب کنیم:

<https://geti2p.net/en/download>

در اینجا می‌توانید بسته نرم‌افزاری را برای ویندوز، مک، نسخه‌های مختلف لینوکس و همچنین برای اندروید دریافت کنید. بسته نرم‌افزاری را با توجه به دستگاه و سیستم عامل خود دانلود و نصب کنید. پس از نصب هنگامی که شما I2P را باز می‌کنید، آدرس (<http://127.0.0.1:7657/home>) localhost باز شده و یا همان‌طور که در فصل گذشته یاد گرفتیم، ما باید به صورت دستی این آدرس وب را در نوار آدرس مرورگر تایپ کنیم. پس از باز کردن در مرورگر هنگامی که ما Network OK را در گوشہ بالای سمت چپ صفحه دیدیم، تنظیمات پراکسی مرورگر را به ۱۲۷.۰.۰.۱:۴۴۴۴ برای دسترسی به سایتها تنظیم کنید و برای IRC می‌توانیم از localhost: 6668 در سرویس گیرنده IRC استفاده کنیم و می‌توانیم #i2p را برای چت استفاده کنیم. پس از تغییر تنظیمات پروکسی مرورگر، ما قادر خواهیم بود به سایتها eepsite با سایتها i2p با مراجعه کنیم.



بعضی از سایت‌ها در صفحه اصلی روتر ذکر شده‌اند که در شکل زیر نشان داده شده است.

به عنوان مثال، میزبان ناشناس گیت: <http://git.repo.i2p/>

در اینجا، اگرچه باید برخی جزئیات را ارائه دهیم، اما هویت ما به آدرس IP واقعی ما پیوند داده نمی‌شود،

به این ترتیب می‌توانیم ناشناس از git استفاده کنیم.

Windows
Mac OS X
GNU/Linux / BSD / Solaris
Debian / Ubuntu
Android
Source package
Automatic updates
Manual updates

Dependency
Java Runtime Version 7 or higher. (Oracle, OpenJDK, or IcedTea Java Version 7 or 8 recommended, except Raspberry Pi: OpenJDK 9 for ARM, PowerPC: IBM Java SE 7 or 8)
Determine your installed Java version here or type `java -version` at your command prompt.
Java 9 support is in development and it is not recommended for general use.

Release Notes

- Release Notes
- Change Log
- Debian Change Log
- Android Change Log

Clean installs

i2pinstall_0.9.39_windows.exe
Mirror: sigterm.no

select alternate mirror
sig

SHA256:
61e2cd75553ba647c58960a2dc2c

در اینجا می‌توانیم جزئیات نحوه استفاده از خدمات میزبانی وب رایگان را به دست آوریم. جزئیات دیگر وجود دارد که می‌تواند در انجمن مطرح شده در URL زیر آن را مشاهده کنید:

<http://open4you.i2p/index.php>

اگر می‌خواهیم وب‌سایتی را در deepweb میزبانی کنیم، سایت زیر مفید است.

Pastebin: <http://pastethis.i2p/>

این وب‌سایت به طور کلی برای ذخیره متن آنلاین در مدت زمان معلوم برای استفاده شخصی است؛ اما محبوبیت آن به عنوان یک منبع برای ارائه مدارک، آخرین اخبار سایبری، جزئیات نقص سایت، جزئیات هدف حمله سایبری وغیره است. هرچند که ما به طور معمول باید اطلاعات خاصی را برای ثبت چیزی ارائه دهیم، در اینجا هیچ جزئیاتی مورد نیاز نیست.

ما همچنین می‌توانیم تمام جزئیات آن را از آدرس زیر پیدا کنیم:

<http://pastethis.i2p/all/>

این یک انجمن عمومی برای بحث در مورد موضوعات مختلف در بخش‌های متفاوت است. موضوعات ممکن است در رابطه با I2P یا چیز دیگری باشد. بسته به منطقه مورد علاقه، عضویت، ورود، خواندن، ایجاد و یا ویرایش پست‌ها را بر اساس مجوزهای ارائه شده توسط سایت ایجاد کنید.

Id3nt یک سایت میکروبلاگینگ مانند توییتر است. در اینجا می‌توانیم هر چیزی که می‌خواهیم پست کنیم، می‌توانیم دیدگاه‌هایمان را به اشتراک بگذاریم، درباره یک موضوع خاص صحبت کنیم و به برخی پست‌های مورد علاقه پاسخ دهیم. این سایت کاملاً شبیه به سایت‌های میکروبلاگینگ معمول است.

نحوه ایجاد سایت با استفاده از I2P

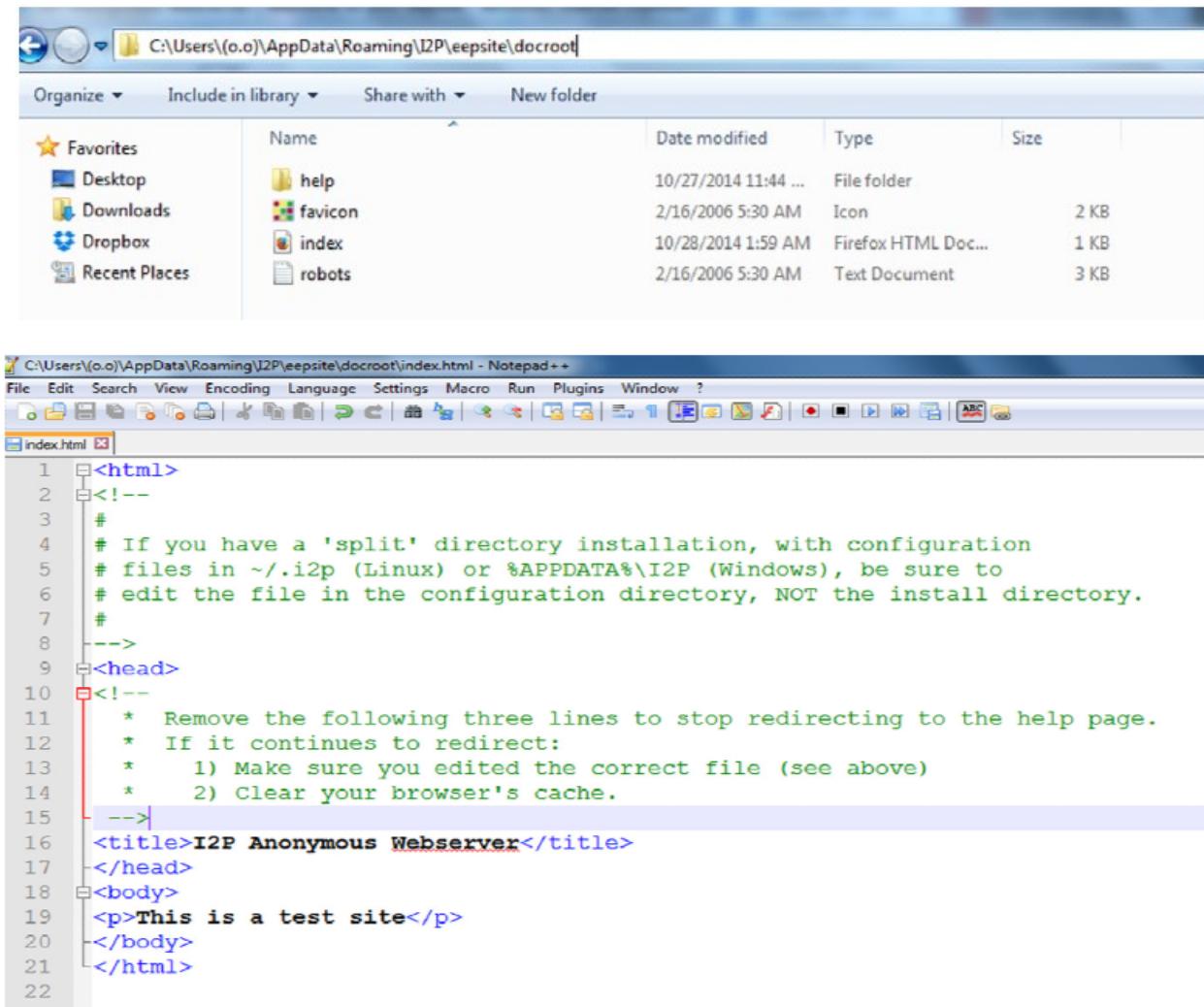
برای ایجاد وب سرور I2P ناشناس، باید فایلی را از مسیر زیر ویرایش کنیم.

ویندوز:

%APPDATA%\I2P\eebsite\docroot

لینوکس:

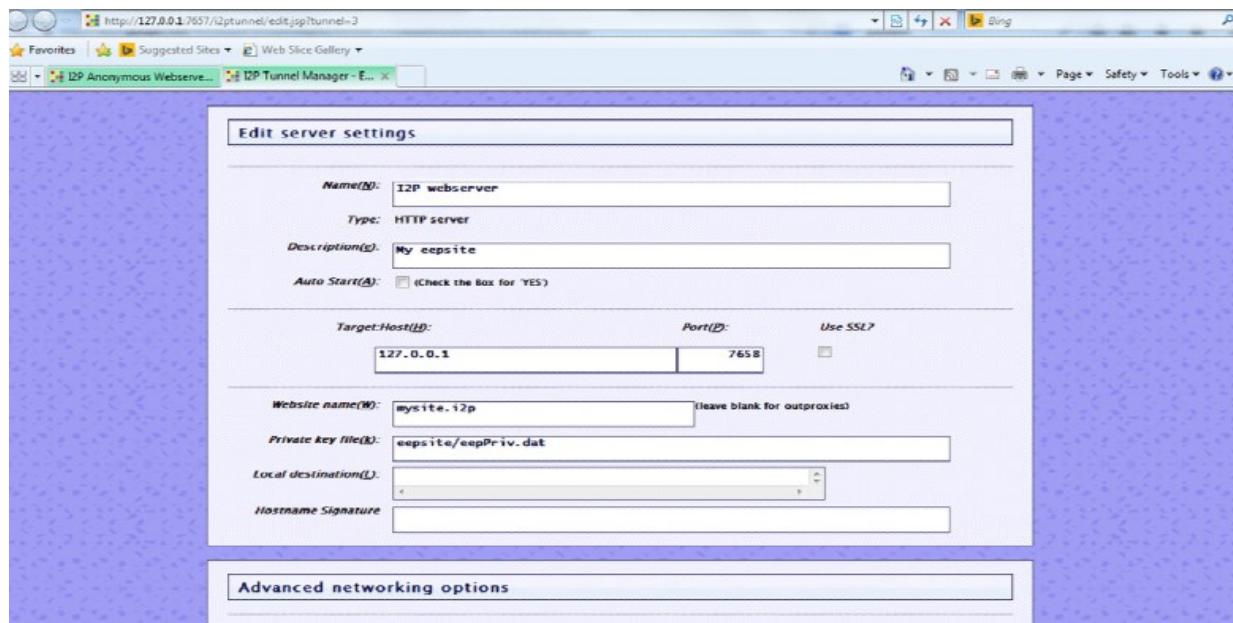
./ ~ i2p / eebsite / docroot /



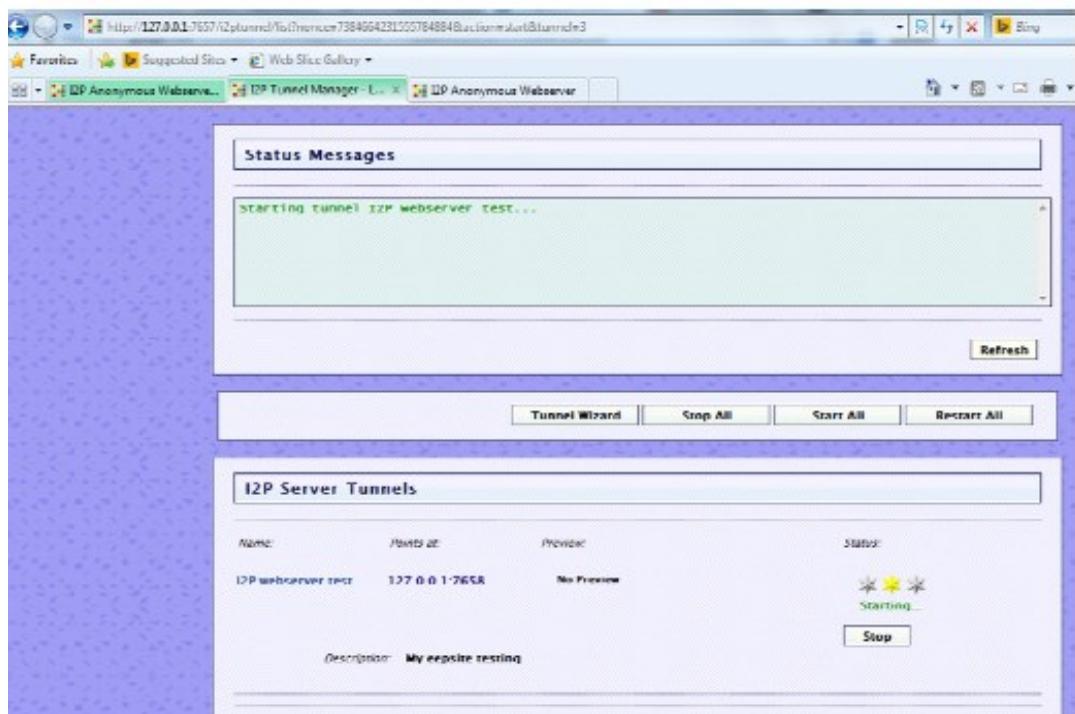
پس از اتمام ویرایش‌ها، باید تنظیمات سرور را از آدرس زیر انجام دهیم:

URL زیر انجام دهیم: <http://127.0.0.1:7657/i2ptunnel/edit.jsp>

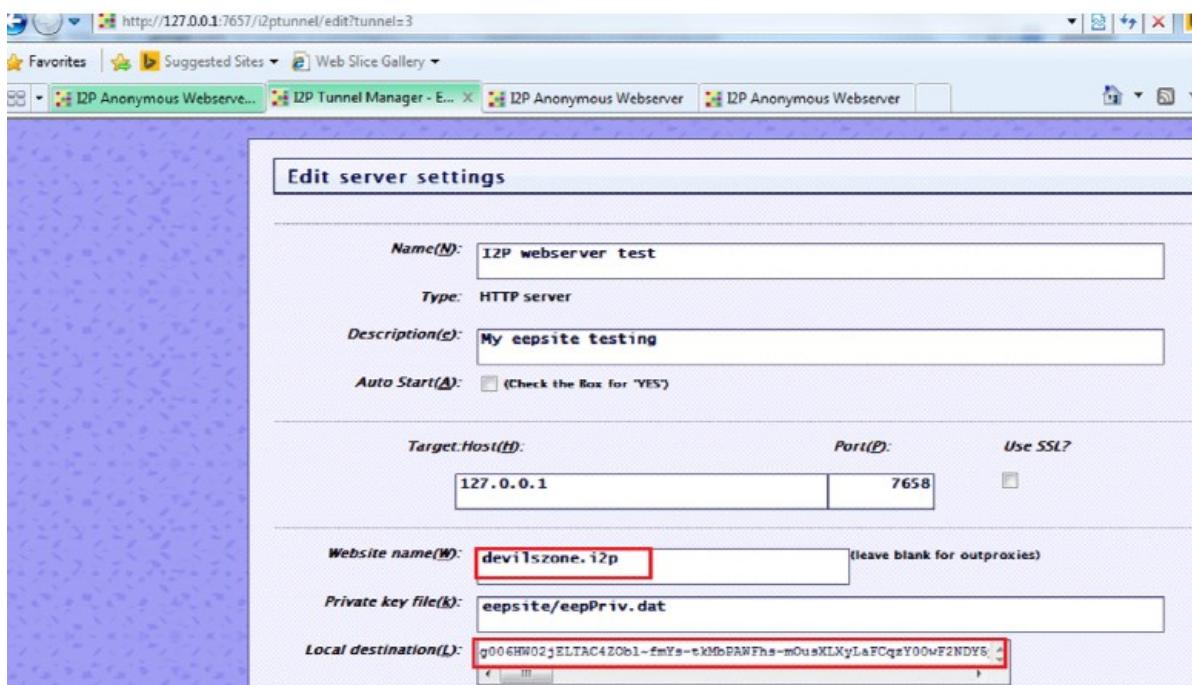
تنظیمات در زیر نشان داده شده‌اند:



به طور پیش فرض سایت ایجاد شده می‌تواند به صورت محلی از مسیر <http://127.0.0.1:7658> قابل دسترسی باشد. اگر چه می‌توانیم آن را از تنظیمات سرور ویرایش کنیم، علاوه بر این می‌توانیم نام، توضیحات، پروتکل، شماره IP و شماره پورت و همچنین نام دامنه را از صفحه ویرایش بالا تغییر دهیم. گزینه‌های پیشرفته خاصی وجود دارد؛ اما بسیار ساده هستند، بنابراین می‌توانیم به راحتی وب سرور را محدود سازیم و هر کسی می‌تواند به استفاده از نام دامنه ارائه شده دسترسی پیدا کند. پس از اتمام تنظیمات، آن را ذخیره کنید. ما صفحه را در شکل زیر نشان داده‌ایم، شروع می‌کنیم.



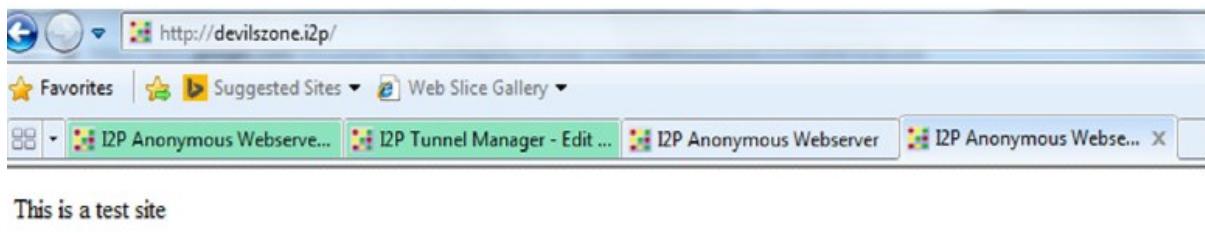
بعضی اوقات نیاز به اضافه کردن نام دامنه و کلید طولانی base64 تولید شده توسط صفحه در لیست آدرس روتر برای دسترسی به سایت داریم که در تصویر زیر نشان داده شده است.



اکنون می‌توانیم به صفحه توسط نام دامنه دسترسی داشته باشیم. در این مورد نام به شکل زیر است:

<http://devilszone.i2p/>

در تصویر زیر نمونه مشابه با استفاده از نام دامنه در مرورگر نشان داده شده است.

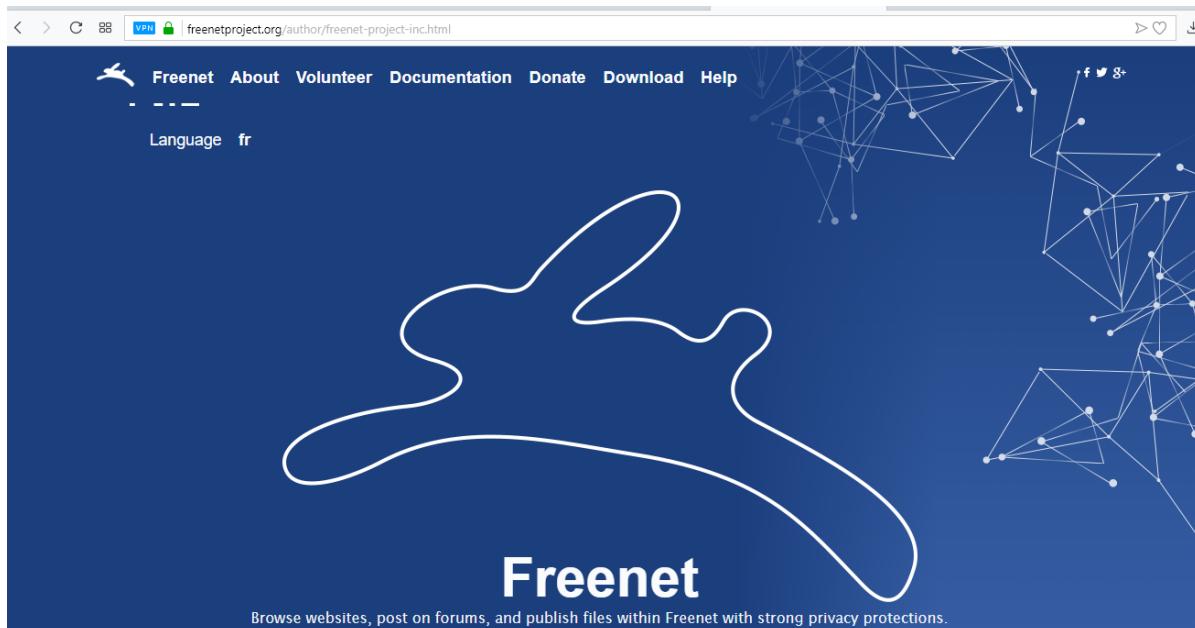


در اینجا آموختیم که چگونه سایت‌های مختلف داخلی اینترنت را با نام دامنه i2p.* مرور کنیم، نحوه دسترسی به آنها با استفاده از I2P، نحوه ایجاد سایت I2P برای ارائه خدمات را نیز بررسی کردیم. این به ما کمک می‌کند تا deepweb را به راحتی در ک کنیم.

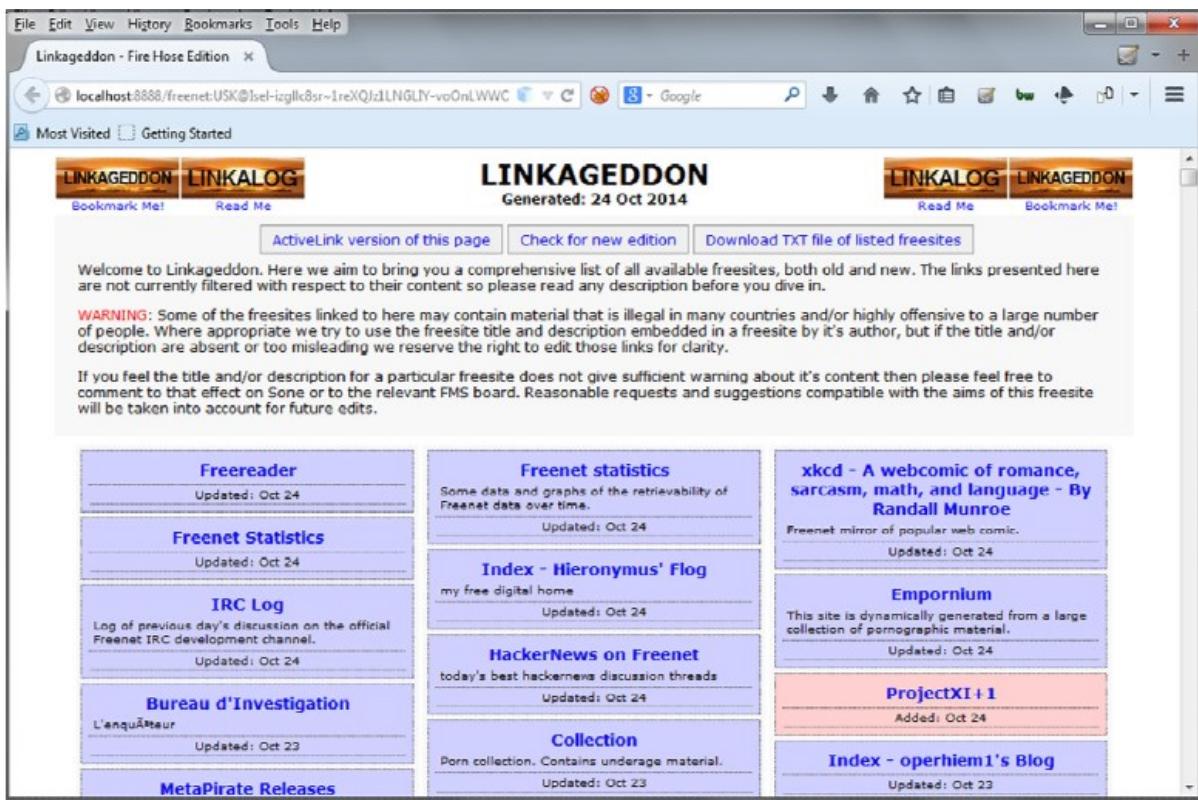
FREENET

همانند Tor و I2P، یک شبکه ناشناس دیگر به نام freenet وجود دارد. یکی از قدیمی‌ترین شبکه‌ها است و برای به اشتراک‌گذاری قابلیت‌های P2P اشتراک فایل شناخته شده است. برنامه‌های کاربردی آن را می‌توان از دانلود کرد. پس از دانلود، به سادگی برنامه را نصب کنید و آن را اجرا کنید.

یک مرورگر را اجرا می‌کند. صفحه نشان داده شده به ما مجموعه‌ای از گزینه‌هایی برای تعیین امنیت و محدودیت استفاده از داده‌های مورد نظر می‌دهد و سپس بر اساس آن تنظیمات، سایت را ایجاد می‌کند. هنگامی که نصب کامل شد، با صفحه اصلی Freenet روبرو خواهیم شد. این صفحه شامل پیوندهایی به وب‌سایت‌های به نام freenets (شبیه به ویکی‌های Tor) و مستندات مرتبط با سایر نرم‌افزارهای مرتبط و نحوه استفاده از آن است. در صفحه اصلی یک جعبه جستجو وجود دارد که اجازه می‌دهد تا از طریق freesites جستجو کنیم. با استفاده از پلاگین‌های خاص مانند freetalk و freemail همچنین می‌توانیم از freenet برای برقراری ارتباط از طریق آن استفاده کنیم.



شاخص Enzo یکی از شاخص‌هایی است که بسیاری از freesite‌ها را فهرست می‌کند و آن‌ها را تحت دسته‌بندی‌ها ارائه می‌دهد. فهرست دیگر Linkageddon است.



همچنین ما را قادر می‌سازد تا با افرادی که قبلًا می‌شناسیم ارتباط برقرار کنیم و از freenet به آدرس <http://localhost:8888/freenet> استفاده کنیم. برای این منظور نیاز به مبادله یک فایل به نام `noderefs` با دوستانمان دارید و این را در صفحه ذکر شده ارائه می‌دهیم و فقط روی دکمه افروزن در پایین کلیک کنید. با آدرس <http://localhost:8888/freeworld> می‌توانیم عملیات اشتراک گذاری را انجام دهیم. همانند سایر شبکه‌های مورد بحث، اجازه می‌دهد تا وب‌سایت خود را ایجاد و به اشتراک بگذاریم. Freenet و یکی خود را در آدرس <https://wiki.freenetproject.org> از جمله تنظیم freesites را فهرست می‌کند.

به غیر از این شبکه‌های ذکر شده، شبکه‌های دیگری نیز وجود دارند که قابلیت‌های مشابهی را ارائه می‌دهند، اما در مورد `deepweb`، نحوه دسترسی، نحوه ایجاد و آنچه از آن انتظار داریم صحبت کردیم. ما همچنین

در این فصل ما از جستجوی اینترنت معمولی استفاده کردیم و در مورد بعضی مناطق کمتر شناخته شده آن یاد گرفتیم. ما در مورد `deepweb`، نحوه دسترسی، نحوه ایجاد و آنچه از آن انتظار داریم صحبت کردیم. ما همچنین برخی از منابع مرتبط را به اشتراک گذاشته‌ایم.

تا کنون ما در مورد ابزارها، تکنیک‌ها و منابع اطلاعاتی یاد گرفتیم که ممکن است به ما کمک کنند تا از طریق اینترنت به نحو بهتر و کارآمدتر استفاده کنیم. ما در ادامه باید در مورد برخی از ابزارها مدیریت و تجزیه و تحلیل داده‌های جمع‌آوری شده یاد بگیریم تا بتوانیم اطلاعات خام را بهتر درک کنیم و اطلاعات جمع‌آوری شده را به صورت هوشمندانه مورد استفاده قرار دهیم.

سلب مسئولیت

بخشی از اینترنت که در این فصل بحث شد ممکن است شامل موارد غیرقانونی و یا مزاحم باشد. به خوانندگان توصیه می‌شود احتیاط لازم را به عمل آورند!

فصل ۱۰: مدیریت داده‌ها

مقدمه

تا کنون در مورد جمع‌آوری داده‌ها با روش‌های مختلف آموخته‌ایم. به طور کلی مردم فکر می‌کنند که OSINT به معنی جمع‌آوری داده‌ها از منابع باز مبتنی بر اینترنت است؛ اما تنها به جمع‌آوری محدود نمی‌شود، زیرا اگر داده‌های جمع‌آوری شده از منابع مختلف به درستی طبقه‌بندی نشده باشند و یا روابط بین آن‌ها پیدا نشود، آن‌ها فقط مقدار عظیمی از داده‌های تصادفی که قابل استفاده نیستند، می‌باشند؛ بنابراین نیاز به مدیریت داده‌ها و تجزیه و تحلیل آن‌ها وجود دارد که این موضوع را در این فصل مورد بحث قرار خواهیم داد، اما اکنون آنچه تا به امروز آموخته‌ایم و نحوه جمع‌آوری داده‌های مختلف با استفاده از منابع مختلف را بازخوانی می‌کنیم.

از ابتدا با استفاده از روش‌های مختلف بر روی استخراج داده‌ها تمرکز کردیم. با موتورهای جستجو شروع کرده که آن‌ها معمولاً به تمامی سؤالات یک کاربر عادی پاسخ می‌دهند. همچنین یاد گرفتیم که چگونه از موتورهای خاص دیگر برای دریافت اطلاعات خاص استفاده کنیم. برخی از ویژگی‌های محبوب موتورهای جستجوی اصلی که آن‌ها را در مقایسه با سایرین منحصر به فرد می‌کند را بررسی کردیم. علاوه بر این در مورد برخی از ابزارها و تکنیک‌های جالب برای پیدا کردن داده‌هایی که به طور آشکار در دسترس هستند، یاد گرفتیم. بعدها آموختیم که چگونه اطلاعات مورد نظر را از وب به طور مؤثر دریافت کنیم. سپس فراداده را مطرح کردیم و گفتیم که چگونه می‌توانند مفید باشند. آموختیم که چگونه اطلاعات را از فراداده‌ها به دست آوریم و چگونه می‌توانیم از آن‌ها برای اهداف مختلف استفاده کنیم و در نهایت، Deep Web را پوشش دادیم. Deep Web بخشی از وب است که

مستقیماً توسط موتورهای جستجو معمولی نمایش داده نمی‌شود. ما یاد گرفتیم که چگونه برای دسترسی به اطلاعات بیشتر به آن دسترسی پیدا کنیم.

بنابراین در حال حاضر می‌توانیم بگوییم که ما یاد گرفتیم که چگونه داده‌ها را از منابع مختلف مستقیماً با استفاده از برخی از راه حل‌های شناخته شده جمع‌آوری کنیم و همچنین با استفاده از ابزارهای غیراستاندارد که درب‌های بیشتری را برای جمع‌آوری داده‌ها باز می‌کنند. اکنون باید کمی درباره داده‌ها، اطلاعات و فهم و اینکه چگونه از یکدیگر تمایز داده می‌شوند، بحث می‌کنیم.

داده^۱

"داده" یکی از رایج‌ترین واژه‌ها در هر زمینه، به ویژه فناوری اطلاعات است. اگر داده را بخواهیم با کلمات ساده توصیف کنیم به معنی شکل خام یک موجودیت است. آن تصویری از حقایق در یک فرم پایه است. به عنوان مثال، اگر یک رشته متنی به شکل `info@xyz.com`, `abc.inc`, `john xyz.com`, `28 CTO` وغیره داشته باشیم، می‌توانیم بینیم اشیاء معینی وجود دارند، اما معنای خاصی ندارند. در فرم خام، داده‌ها ارزش زیادی ندارند.

اطلاعات^۲

فرم پردازش شده (سیستماتیک) داده‌ها، اطلاعات نامیده می‌شود. وقتی داده‌ها بر اساس ویژگی‌های طبقه‌بندی می‌شوند، می‌توان آن را اطلاعات نامید. در حقیقت می‌توانیم بگوییم اطلاعات شامل داده‌های جمع‌آوری شده و سازمان یافته است. از این رو برای دستیابی به اطلاعات باید داده‌ها را پردازش کنیم. باید همان مثال قبل را باز نویسی کنیم: `abc.inc` نام شرکت است. `john xyz.com` یک دامنه است، `info@xyz.com` یک کاربری است، `28` سن است، `CTO` یک آدرس ایمیل ثبت شده در `xyz.com` است و `xyz.com` یک موقعیت شغلی است.

فهم^۳

وقتی اطلاعات متنوعی را بر اساس روابط آن‌ها با یکدیگر پردازش می‌کنیم و معنای آن را به دست می‌آوریم، آن چیزی که دریافت می‌کنیم، فهم است؛ بنابراین داده‌ها را استخراج کرده و برای دستیابی به اطلاعات، آن‌ها را تجزیه و تحلیل می‌کنیم. از همان مثال قبلی می‌توان نتیجه گرفت که `info@xyz.com` و `xyz.com` متعلق به یک دامنه هستند. ممکن است جان `28` ساله بوده و به عنوان `CTO` در شرکت `abc.inc` کار می‌کند. این‌ها پیش‌بینی‌های اولیه

¹ Data

² INFORMATION

³ INTELLIGENCE

هستند که ممکن است مثبت کاذب باشند، بنابراین باید بعداً آن‌ها را اعتبار سنجی کنیم، اما در حال حاضر اطلاعات نسبی به دست آمده است، بنابراین می‌توانیم نتیجه گیری کنیم. جان ۲۸ ساله به عنوان CTO در شرکت abc.inc کار کرده و نام دامنه شرکت آن xyz.com و شناسه ایمیل info@xyz.com برای برقراری ارتباط با او است.

برای اعتبارسنجی نیاز به استخراج اطلاعات از منابع دیگر داریم. مثلاً باید بدانیم که نام کارمند CTO از شرکت کسی به نام جان است و آیا فردی با نام جان در abc.con کار می‌کند که آدرس ایمیل آن info@xyz.com است و اطلاعات مشابهی که ممکن است برای اثبات نظر ما درست یا غلط باشد. اکنون فرض کنید ما یک فروشنده هستیم و کار ما این است که با مدیریت شرکت‌های مختلف ارتباط برقرار کنیم، پس اگر اعتبار این اطلاعات درست باشد، می‌توانیم با او تماس بگیریم و ایمیل خود را بسته به گروه سنی و سایر اطلاعاتی که در مورد او داریم ارسال کنیم. تعریف فهم ممکن است در افراد مختلف متفاوت باشد. تعریف ما بر اساس تجربه است.

همان طور که قبلاً نیز بحث کردیم، داده‌ها فرم خام دارند که فقط حاوی موجودیت‌ها است. موجودیت به معنای چیزی ملموس یا ناملموس است. ممکن است نام، مکان، شخصیت یا هر چیزی دیگری باشد. اگر فقط داده باشد برای ما بی‌ارزش است. ما نمی‌دانیم که آن در چه مورد هست. ما می‌توانیم مقدار زیادی از داده‌های تصادفی را دریافت کنیم اما برای استفاده از آن باید درک کنیم که چه اطلاعاتی در مورد آن‌ها وجود دارد. فرض کنید، ما ۱۰۰۰ عبارت تصادفی داریم، چه باید بکنیم؟ اگر متوجه شویم که آن‌ها شامل نام‌های کاربری یا رمزهای عبور هستند، ۱۰۰۰ عبارت تصادفی، ارزش زیادی دارند. ما می‌توانیم از آن‌ها به عنوان دیکشنری در حمله بروت فورس و یا غیره استفاده کنیم. این اطلاعات همیشه ارزشمند هستند.

مدیریت اطلاعات بسیار مهم است. داده‌های مدیریت شده را می‌توان به سرعت برای پیدا کردن روابط مورد استفاده قرار داد. فرض کنید تعداد زیادی داده داریم و می‌دانیم که داده‌ها شامل نام، شناسه ایمیل، شماره تلفن همراه و غیره هستند. اگر ما این داده‌ها را به طور سیستماتیک در ردیف‌ها و ستون‌ها مدیریت نکنیم، همبستگی آن‌ها را از دست داده و زمانی که نیاز به مجموعه‌ای خاص از داده‌ها داریم، مانند نام و نام خانوادگی، با مقدار زیادی از داده‌های مدیریت نشده روبرو می‌شویم.

بنابراین همیشه مهم است که داده‌ها را به انواع مختلف، دسته بندی کرده و به نحوی طبقه بندی کنیم تا بتوانیم از آن به راحتی استفاده کنیم. همان‌طور که در فصل‌های قبلی دیدیم، منابع مختلفی از اطلاعات وجود دارند. هر منبع

در کار خود منحصر به فرد است. هنگامی که اطلاعات از منابع مختلف با هم جمع می‌شوند، تصویری کامل ایجاد می‌کنند و به ما اجازه می‌دهد تا از دیدگاه وسیع‌تر آن را بینیم.

درست است که داده‌ها را از منابع مختلف جمع‌آوری می‌کنیم، اما حتی پس از آن منابع بسیاری هنوز وجود دارند. چیزی که حقیقت دارد این است که با راه اندازی یک ابزار نمی‌توان تمام داده‌ها را جمع‌آوری کرد. جمع‌آوری داده‌ها باید در جهت رسیدن به نتیجه مطلوب پایانی باشد. استخراج داده‌ها از منابع مختلف، برای مطابقت و تفسیر آن‌ها با توجه به نیازهای ما انجام می‌شود. در اکثر موارد ممکن نیست که بتوانیم تمام اطلاعاتی را که می‌خواهیم از یک منبع واحد دریافت کنیم؛ بنابراین برای جمع‌آوری تصویر کلی باید اطلاعات مختلف را از منابع متفاوت جمع‌آوری کنیم.

به عنوان مثال، ما باید شرایطی را فراهم کنیم که تمام اطلاعات مربوط به یک فرد به نام جان را جمع کنیم. چگونه باید آن را انجام بدھیم؟ نام جان کاملاً نامشخص است و دریافت تمام اطلاعات بسیار مشکل خواهد بود. باید با برخی از اطلاعات اولیه شروع کنیم. شاید بتوانیم تصویری از جان را کشف کنیم، ممکن است با جستجوی ساده‌ی گوگل برای بررسی تصویر شروع کنیم، ممکن است تصویری را دریافت نکنیم، اما اگر تصویری را دریافت کنیم؛ صفحه‌ای که گوگل تصویر را در آن یافته است، برای به دست آوردن اطلاعات بیشتر در مورد جان مرور می‌کنیم؛ اما اگر پس از آن سعی کنیم سایت‌های شبکه‌های اجتماعی مانند فیسبوک یا LinkedIn را جستجو کنیم، این احتمال وجود دارد که بتوانیم عکس و همچنین پروفایل جان را در یکی از سایت‌های شبکه اجتماعی و یا همه آن‌ها بیابیم. اگر پروفایلی را به دست آوریم، می‌توانیم اطلاعات بیشتری از قبیل شناسه ایمیل، نام شرکت، موقعیت، وضعیت اجتماعی، شهر فعلی، محل اقامت دائمی آن را دریافت کنیم.

پس از دریافت این جزئیات می‌توانیم از شناسه ایمیل برای بررسی مکان‌های دیگر استفاده کنیم مانند سایت‌ها، وبلاگ‌ها، انجمن‌ها و غیره. منابع اینترنتی مختلفی وجود دارند که می‌توانند به ما برای به دست آوردن این جزئیات کمک کنند. سپس می‌توانیم به صورت دستی از این سایت‌ها برای جمع‌آوری اطلاعات بیشتر، بازدید کنیم. این فقط یک نمونه از مراحل مختلف جمع‌آوری داده‌ها با در نظر گرفتن یک خروجی به عنوان ورودی گام دیگر و جمع‌آوری داده‌ها برای تکمیل نتایج است.

همان‌طور که از مثال فوق مشخص شد، پردازش داده‌ها یک فرآیند گام به گام است که شامل تعدادی از منابع مختلف است و همچنین نتیجه یک فرآیند به طور کلی به عنوان نقطه شروع برای سایر فرآیندها مورد استفاده قرار

می‌گیرد؛ بنابراین ارتباط بین داده‌های جمع آوری شده برای ردیابی بسیار دشوار خواهد بود، اگر آن را از ابتداء شروع نکنیم. اگر به دنبال داده‌های خاصی بدون مرتب سازی آنها در یک شیوه ساختاری بگردیم، جستجو برای رسیدن به روابط بین داده‌ها بسیار مشکل خواهد بود؛ بنابراین تمام داده‌ها در مورد یک موجودیت بدون دانستن ارتباط و ساختار بین آنها، بی‌ارزش خواهد بود؛ بنابراین باید داده‌ها را به صورت ساختاری مدیریت کنیم.

راه‌های مختلفی برای ساختار سازی اطلاعات جمع آوری شده وجود دارد، اما بهترین راه این است که آنها را با توجه به موجودیت‌های والدین و فرزندان مرتب کنید. فرض کنید ما ایمیلی را از نام شخص پیدا کردیم، پس نام و نام خانوادگی والد و ایمیل فرزند آن خواهد بود. اگر ما چیزی از ایمیل دریافت کنیم، مانند نام دامنه، آنگاه ایمیل به والد تبدیل خواهد شد، به این صورت می‌توانیم تمام اطلاعات جمع آوری شده را سازماندهی کنیم.

داده‌ها را همچنین می‌توان با استفاده از ردیف‌ها و ستون‌ها در یک صفحه اکسل به راحتی ذخیره کرد، اما روند ردیابی کمی مشکل می‌شود. برای رسیدن به هر گره باید تعدادی از آنها را جستجو کنیم و فرم متنی داده‌ها به آسانی قابل یادآوری نیست. این تنها دلیل آن است که نمودارها و گراف‌ها برای پردازش‌های پیچیده یا آماری به کار می‌روند تا به راحتی قابل یادآوری و درک باشند. این یکی از دلایل اصلی محبویت Maltego است. همان‌طور که Maltego در ک خروجی آسانی را فراهم می‌کند، نمایش داده در شکل گراف، می‌تواند در سهولت تجزیه و تحلیل و شفاف سازی روابط ایجاد شده بین موجودیت‌ها کمک کند.

ابزار مدیریت داده‌ها و تجزیه و تحلیل اطلاعات

اکسل

در تجزیه و تحلیل داده‌ها، راه‌های ساده‌ای برای طبقه‌بندی داده‌ها وجود دارد که برای مدت طولانی در صنعت استفاده می‌شده است. یکی از این ابزارها اکسل است. برخی نیز آن را به عنوان صفحه گسترده نامیده‌اند. رابط کاربری آسان، ردیف‌ها و ستون‌ها را به شیوه‌ای جداگانه تفکیک می‌کند که یک روش عالی برای طبقه‌بندی داده‌ها است. این ابزار زمانی که فقط مقادیر استاتیک برای موجودیت‌های مختلف مانند جزئیات یک کاربر داریم، بسیار مفید است. فرض کنید که می‌خواهیم داده‌ای را مدیریت کنیم که شامل نام کاربری، شناسه ایمیل، سازمان و موقعیت شغلی باشد. برای هر کاربر در یک ردیف، تمام جزئیات در ستون‌ها را اضافه می‌کنیم. برای این نوع کار، اکسل یا صفحه گسترده بهترین گزینه ممکن است.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Title	First Name	Middle Name	Last Name	Suffix	E-mail Address	E-mail 2	A	E-mail 3	A Business	Business	Business	Business
2	Mr.	Reza		Shahriari		reza.shahriari@gmail.com							
3	Mr.	Ali		Maleki		ali.maleki@gmail.com							
4	Mr.	Abdol		Rezaei		abdol.rezaei@gmail.com							
5	Mr.	Saeed		Khodabandeh		saeed.khodabandeh@gmail.com							
6	Mr.	Amir		Yazdi		amir.yazdi@gmail.com							
7	Mr.	Ali		Shahriari		ali.shahriari@gmail.com							
8	Mr.	Reza		Maleki		reza.maleki@gmail.com							
9	Mr.	Abdol		Rezaei		abdol.rezaei@gmail.com							
10	Mr.	Saeed		Khodabandeh		saeed.khodabandeh@gmail.com							
11	Mr.	Amir		Yazdi		amir.yazdi@gmail.com							
12	Mr.	Ali		Shahriari		ali.shahriari@gmail.com							
13	Mr.	Reza		Maleki		reza.maleki@gmail.com							
14	Mr.	Abdol		Rezaei		abdol.rezaei@gmail.com							
15	Mr.	Saeed		Khodabandeh		saeed.khodabandeh@gmail.com							
16	Mr.	Amir		Yazdi		amir.yazdi@gmail.com							
17													
18													
19													
20													
21													
22													
23													
24													

اکسل دارای ویژگی‌های قالب بندی عالی است که می‌توانیم فرمول‌ها را اعمال، داده‌ها را فیلتر، نظرات را اضافه کرده، دکمه‌های کشویی را ایجاد و بسیاری دیگر از کارها را انجام دهیم. نکته‌ی آخر این است که اکسل یک ابزار عالی برای دسته بندی داده‌ها است اگر همه داده‌ها را بر اساس یک موجودیت اولیه طبقه بندی کنیم، اما اگر بیش از یک موجودیت اولیه داشته باشیم، ممکن است مشکل ایجاد شود. در این مورد باید یک جدول جداگانه را در همان صفحه و یا صفحه جداگانه ایجاد کنیم. سپس باید به صورت دستی ارتباط بین داده‌ها را با مقایسه جدول‌ها یا صفحه‌ها پیگیری کنیم. این کار زمانی که بیش از یک موجودیت اولیه با مقدار زیادی داده داریم، مشکل است.

پایگاه داده SQL

به عنوان یک زبان پرس و جو ساختاریافته برای مدیریت داده شناخته شده طراحی شده است. با استفاده از پایگاه داده‌های SQL می‌توانیم داده‌ها را در یک فرم جدولی در یک سیستم ذخیره کنیم. این کار به ما اجازه می‌دهد تا عناصر پایگاه داده را وارد کرده و سپس به پرس و جو، حذف و بهروز رسانی آن‌ها بپردازیم. پایگاه‌های داده SQL دارای ویژگی‌های عالی مدیریت داده‌ها هستند و به طور گسترده‌ای در صنعت برای ذخیره مقدار زیادی از اطلاعات مورد استفاده قرار می‌گیرد. تنها دلیل محبوبیت آن در صنعت این است که با استفاده از پرس و جوهای ساده، قادر به مدیریت پایگاه داده هستیم.

ما در مورد مشکلی در پاراگراف بالا بحث کردیم که وقتی که جداول چندگانه وجود دارد، یافتن ارتباط و دستیابی به داده‌ها در مورد یک موجودیت خاص بسیار مشکل است. در اینجا SQL به عنوان ناجی می‌آید. در SQL با نوشتند درخواست‌های ساده می‌توانیم داده‌های یک موجودیت خاص را از جداول چندگانه به‌آسانی استخراج کنیم. تعداد زیادی از DBMS یا نرم افزارهای مدیریت داده در دسترس هستند. بعضی از آن‌ها منبع باز و برخی دیگر نیستند، برخی از DBMS‌های محبوب MySQL، SQL Server، MSSQL، Oracle و غیره هستند. جدا از پایگاه داده‌های مبتنی بر SQL، بعضی از پایگاه داده‌های NoSQL نیز وجود دارند که اجازه می‌دهد داده‌های غیر متّنی نیز ذخیره شود.

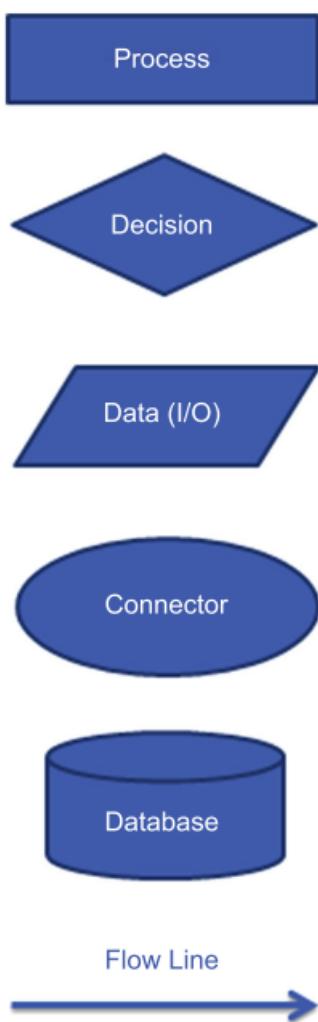
Table	Action	Rows	Type	Collation
adminnotification_inbox	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8_ger
admin_assert	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8_ger
admin_role	Browse Structure Search Insert Empty Drop	2	InnoDB	utf8_ger
admin_user	Browse Structure Search Insert Empty Drop	1	InnoDB	utf8_ger
api2_acl_attribute	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8_ger
api2_acl_role	Browse Structure Search Insert Empty Drop	2	InnoDB	utf8_ger
api2_acl_rule	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8_ger
api2_acl_user	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8_ger
api_assert	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8_ger
api_role	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8_ger
api_rule	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8_ger
api_session	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8_ger
api_user	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8_ger
captcha_log	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8_ger

مشکل اصلی، عدم استفاده کاربر معمولی از آن‌است. اگر چه نصب و پیکربندی آن بسیار سخت نیست اما نیاز به دانش فنی و همچنین دانستن نحوه ایجاد پرس و جو SQL برای مدیریت پایگاه داده است. اگرچه ابزار و چارچوب‌های خاصی برای سهولت استفاده کاربر وجود دارند که ویژگی‌هایی مانند تکمیل خودکار فرمان، اصلاح نحوه دستورها و غیره را فراهم می‌کنند، اما هنوز نیاز به درک زبان وجود دارد. آن‌ها در واقع برای نگهداری و کار با مقدار زیادی از داده‌ها طراحی شده‌اند و از این رو برای استفاده معمولی در ذخیره سازی داده‌ها، خیلی کاربردی نیستند.

فلوچارت‌ها

اکسل و پایگاه داده‌های SQL داده‌ها را در فرم متنی ذخیره می‌کنند؛ بنابراین می‌توانیم فقط فرم متنی را داده‌ها را وارد کرده و آن‌ها را دسته بندی کنیم، اما فلوچارت، شکل گرافیکی را به داده‌ها اضافه می‌کند. نمادهای خاصی برای انواع مختلف داده‌ها وجود دارد که به کاربر اجازه می‌دهد تا نه تنها داده‌ها را به صورت گرافیکی مدیریت کند، بلکه ویژگی‌هایی را فراهم می‌کند تا به راحتی روابط را با نمادها و فلش‌های مختلف نمایش می‌دهند.

فلوچارت یک نوع نمودار است که مجموعه‌ای از داده، جریان کار یا فرآیند را نشان می‌دهد. مراحل را به عنوان جعبه‌های مختلف و روابط را با اتصال آن‌ها با فلش نشان می‌دهد. این نمودار گرافیکی می‌تواند برای سهولت در کم و نگه داشتن چیزها بسیار مفید باشد. فلوچارت‌ها برای تجزیه و تحلیل و مدیریت داده‌های مختلف استفاده می‌شوند و دارای جعبه‌های ویژه برای مقاصد مختلف هستند. چند نمونه از آن در تصاویر زیر آورده شده است.

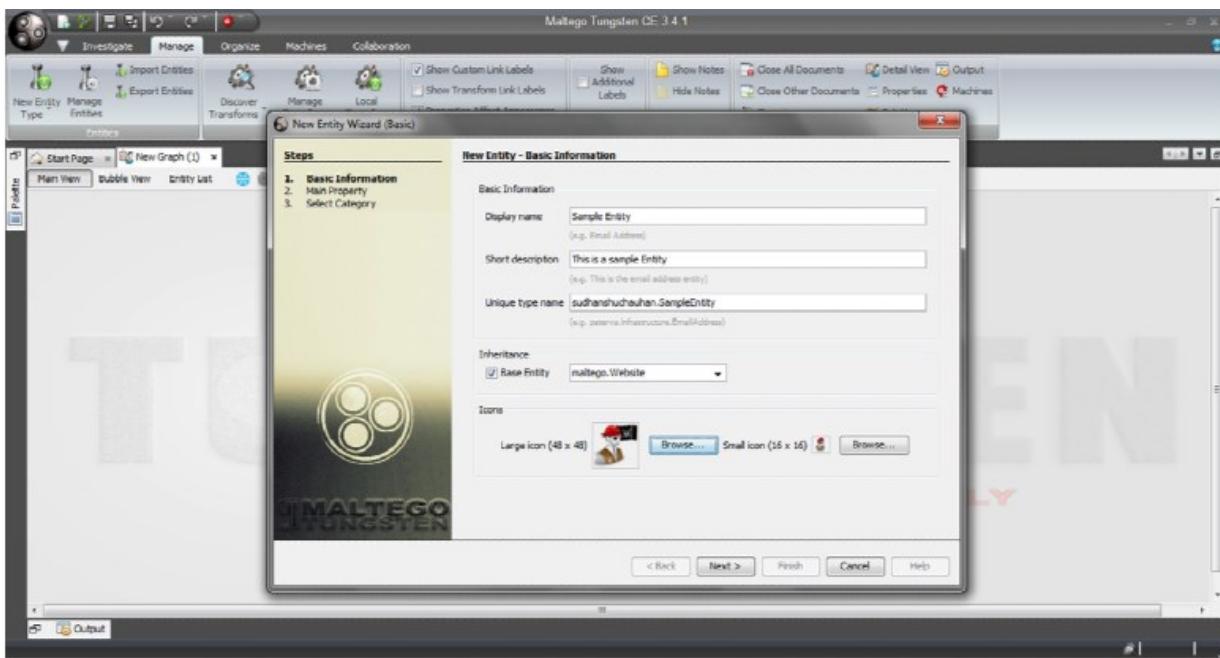


تا کنون درباره شیوه‌های که معمولاً برای ذخیره داده‌ها و یا مدیریت آن‌ها استفاده می‌شود، بحث کردیم. اکنون اجازه دهید چیز متفاوتی یاد بگیریم و بینیم که چه گزینه‌های دیگری نیز وجود دارند که می‌توانند به ما در مدیریت و تجزیه و تحلیل داده‌ها کمک کنند.

Maltego

هر گونه جستجو، بدون استفاده از Maltego کامل نیست. این ابزار بخش جدایی ناپذیر از OSINT است. ما قبلاً در مورد این ابزار و در مورد چگونگی استفاده از آن برای استخراج داده‌ها بحث کردیم. دلیل محبویت و گستردگی استفاده از Maltego به غیر از ویژگی‌های استخراج دادها، نحوه نمایش آن‌ها است. Maltego مجموعه‌ای از ویوهاي مختلف از قبیل اصلی، حباب و غیره دارد. همچنین می‌توانیم نوع نمایش را تغییر دهیم. نتیجه بسیار ساده است زیرا می‌توان گفت که انواع مختلف آیکون‌ها برای انواع مختلفی از موجودیت‌ها استفاده شده و روابط بین آن‌ها به‌وسیله فلش‌ها به‌خوبی بیان می‌شوند.

اطلاعات را با یک مدل ارتباطی مناسب و سازنده نشان می‌دهد. به غیر از استخراج داده‌ها با استفاده از Transform ها و Machine های مختلف، می‌توانیم اطلاعاتی که از منابع مختلف پیدا کرده‌ایم را در یک نمودار برای ایجاد یک تصویر بزرگ‌تر قرار دهیم. برای این کار به‌سادگی باید نوع موجودیت مناسب را از نوار سمت چپ انتخاب کرده و آن را به نمودار وارد کنیم، سپس داده‌هایی را که پیدا کرده‌ایم را وارد و به‌سادگی آن را به موجودیت یا نهادهای مربوطه مرتبط کنیم. اگر موجودیت مناسب برای نوع داده را پیدا نکنیم، Maltego اجازه می‌دهد تا یک موجودیت جدید ایجاد کنیم و از آن با توجه به نیازمان استفاده کنیم. این باعث می‌شود تا استفاده از ویژگی‌های داده کاوی بسیار آسان بوده و بتوان از آن برای تجزیه و تحلیل داده‌ها استفاده کرد.



CASEFILE

ابزار دیگری از آدرس زیر قابل دریافت است:

<https://www.paterva.com/web6/products/casefile.php>

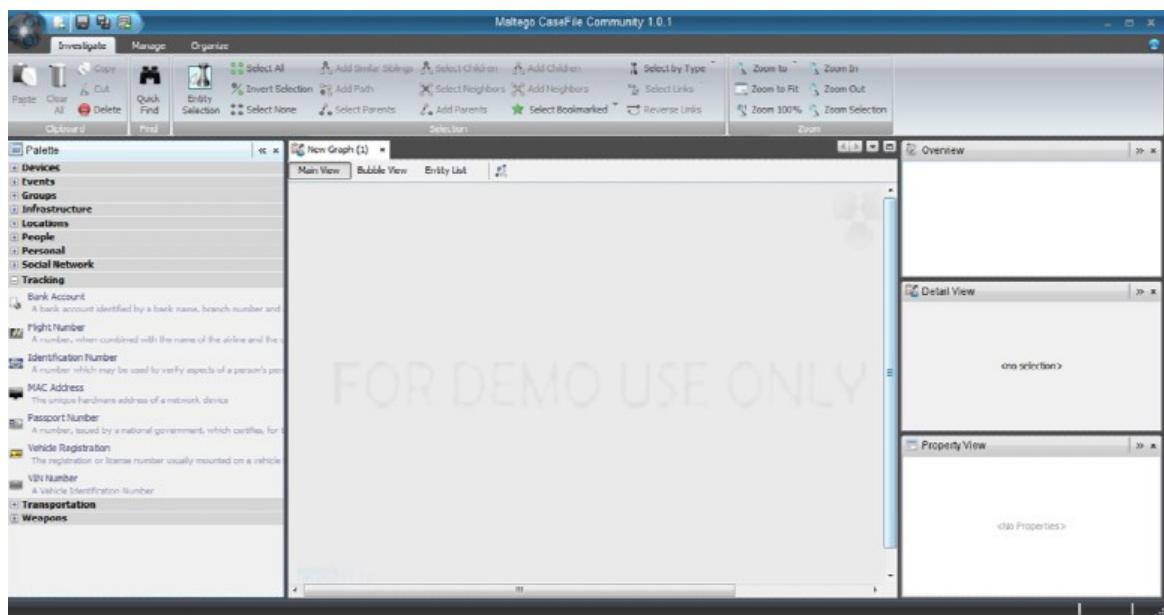
همانند CaseFile Maltego توسط محققان برای جمع‌آوری اطلاعات مربوط به یک موجودیت مورد استفاده قرار می‌گیرد. CaseFile به ما کمک می‌کند تا یک نقشه اطلاعاتی را ایجاد کنیم. در این ابزار رابط کاربری ساده، برای اضافه کردن، پیوند و تجزیه و تحلیل سریع و مؤثر داده‌ها، فراهم است. انگیزه ایجاد این ابزار، تجزیه و تحلیل داده‌ها است.

همان‌طور که این ابزار برای تجزیه و تحلیل داده‌ها در نظر گرفته شده است، شامل بسیاری از موجودیت‌های زندگی روزانه است که می‌تواند در طول جمع‌آوری اطلاعات یافت شوند. برخی از دسته‌های آن‌ها عبارت‌اند از دستگاه‌ها، مکان‌ها، موقعیت‌های مکانی، زیرساخت‌ها و غیره. همچنین قادر به اضافه کردن موجودیت‌های سفارشی می‌باشد. یکی دیگر از ویژگی‌های هیجان‌انگیز CaseFile این است که می‌توان از آن برای داده‌های ذخیره شده در صفحات اکسل و یا فایل‌های CSV استفاده کرد که باعث می‌شود که داده‌های ما در این فرم‌ها بر جسته‌تر شوند.

رابط کاربری CaseFile بسیار مشابه OSINT است و در بخش Maltego بسیار محبوب و به طور گسترده‌ای مورد استفاده قرار می‌گیرد، اگر کاربر Maltego بخواهد CaseFile را امتحان کند، بدون هیچ مشکلی می‌تواند از آن استفاده کند. گزینه‌های موجود برای ایجاد نمودارها نیز کاملاً یکسان هستند.

همانند Maltego، برای ایجاد یک نمودار جدید در CaseFile، باید تمام موجودیت‌هایی را که اطلاعاتی از آن در اختیار داریم را اضافه و داده‌های مربوطه به آن‌ها را وارد کنیم، سپس ارتباطات میان آن‌ها را برای ایجاد یک تصویر کامل برقرار می‌کنیم. اگر چه CaseFile ویژگی استخراج داده ندارد، اما ویژگی نمایش گرافیکی اطلاعات آن وقتی که از داده‌های منابع مختلف استفاده و نیاز به اتصال آن‌ها به یکدیگر داریم، بسیار مفید است.

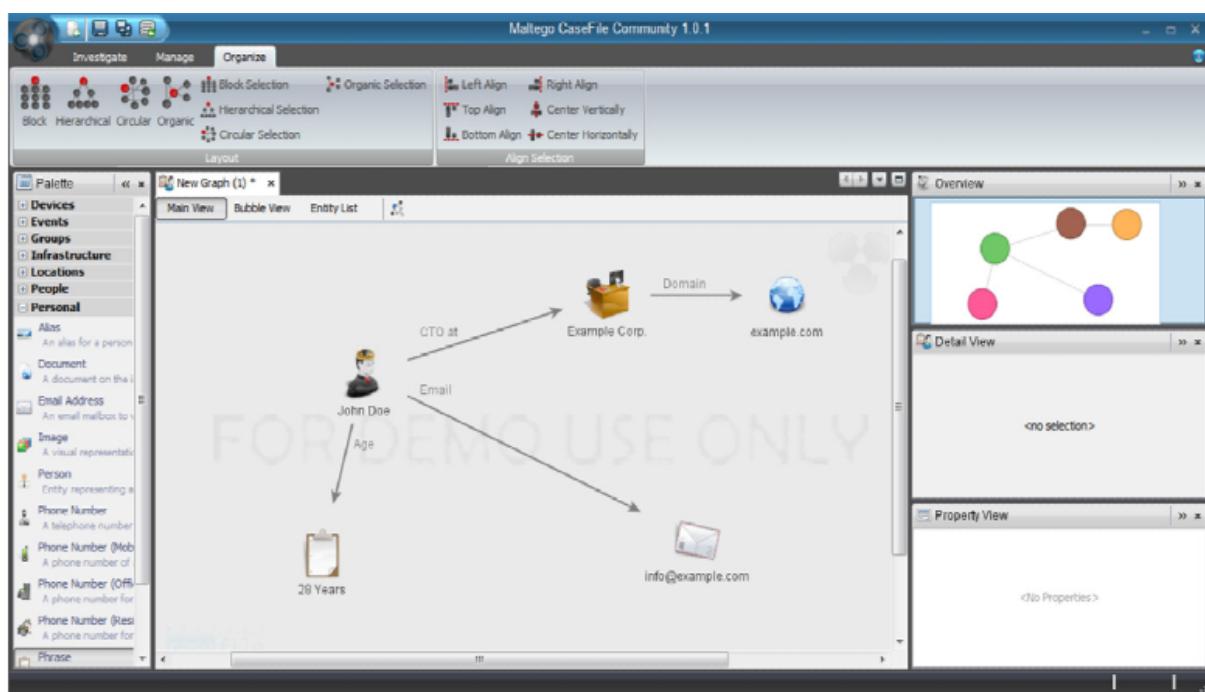
حاوی سه زبانه قرار داده شده در بالای واسطه به نام‌های Investigate، Manage و Organize است. در زیر زبانه Investigate توابع مانند cut، copy، paste، entity selection، graph zooming و graph selection است. این گزینه‌ها به ما اجازه می‌دهد تا به سرعت گراف و موجودیت‌های درون آن را بسازیم. زبانه دیگر Manage است که اجازه می‌دهد تا موجودیت‌ها را مدیریت و موجودیت‌های جدید را اضافه کنیم. همچنین می‌توانیم یادداشت‌هایی را اضافه کنیم و با ویژگی‌های مربوط به پنجره CaseFile کار کنیم. آخرین زبانه Organize است که ویژگی‌هایی مانند مدیریت طرح گراف در ساختارهای مختلف ارائه می‌دهد و همانگی لازم را با توجه به نیاز انجام می‌دهد.



بنابراین همه چیز Maltego مانند CaseFile است و ما می‌توانیم برای اهداف مختلف از جستجو تا تجزیه و تحلیل داده‌ها از آن استفاده کنیم؛ مانند Maltego همچنین در دو شکل ارائه می‌شود: یکی عمومی یا نسخه رایگان و دیگری نسخه تجاری است. هر دو نسخه را می‌توان در آدرس زیر پیدا کنید:

<https://www.paterva.com/web6/products/download2.php>

همچنین از سیستم عامل‌های مختلف مانند ویندوز، مک و لینوکس پشتیبانی می‌کند. فرایند نصب آن کاملاً آسان و مشابه Maltego است.



MagicTree

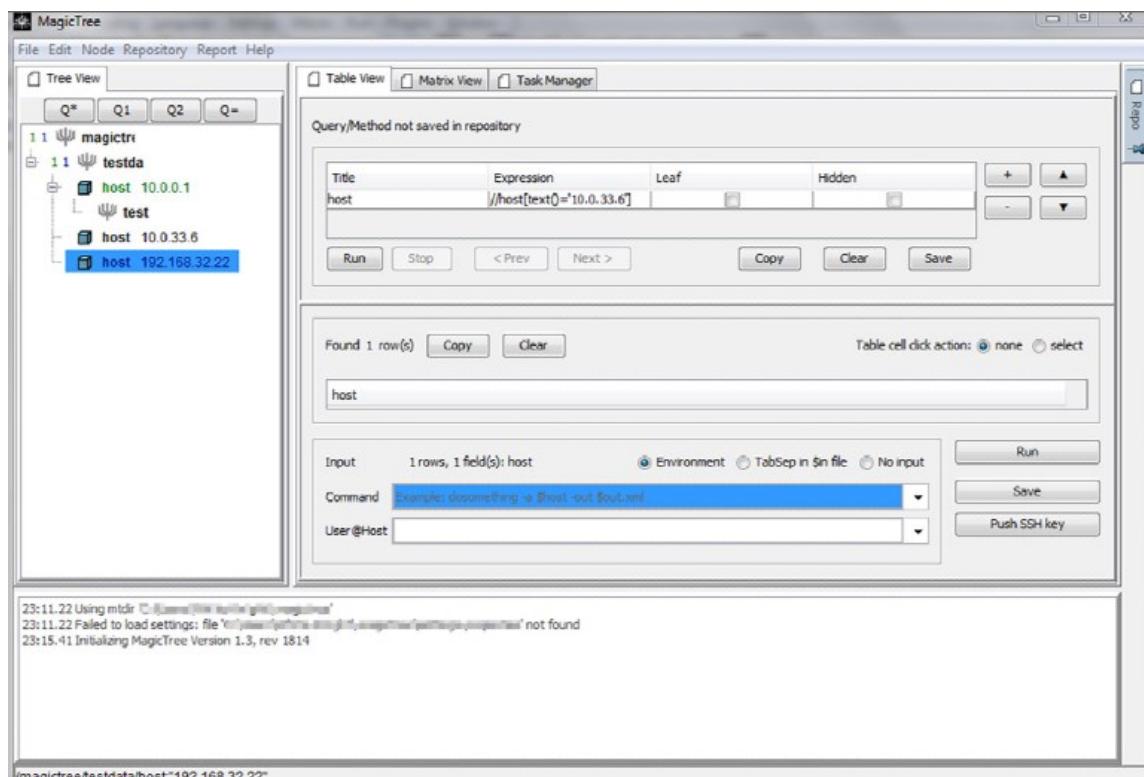
این ابزار اساساً برای تست نفوذگرها است که نیاز به مدیریت داده‌هایی که در طول آزمایش امنیتی دریافت می‌کنند، دارند. MagicTree برای حل برخی از مشکلات که هر تست نفوذگر در کار خود با آن مواجه است ساخته شده که جزئیات را از داده‌های تولید شده توسط ابزارهای مختلف، پیدا می‌کند. در طی یک تست نفوذ، ارزیاب به دنبال نقاط ضعف، خطرات احتمالی یا آسیب پذیری در هر برنامه یا شبکه می‌باشد تا بتوانند آن‌ها را برطرف کنند. در این فرایند از ابزارهای زیادی برای خودکارسازی فرایند تست استفاده می‌کنند و نتیجه این ابزارها بسته به دامنه، اندازه و تعداد آسیب پذیری‌های موجود، زیاد است. به طور کلی در هر تست نفوذ شبکه، ارزیاب با مشکل مواجه است، زیرا محدوده کار همیشه بزرگ بوده و ابزارهای استفاده شده همواره نتایج زیادی را فراهم

می‌کنند. در آن صورت MagicTree به عنوان یک ناجی به حساب می‌آید. این ابزار از ابزارهای عمومی تست نفوذ شبکه مانند Nmap و Nessus پشتیبانی می‌کند و به کاربران اجازه می‌دهد تا داده‌های تولید شده توسط آنها را وارد کنند. بعدها داده را می‌توان مورد استفاده قرار داد، تجزیه و تحلیل و یا برای تولید گزارش استفاده کرد. برای استفاده از MagicTree ابتدا باید آن را دانلود و نصب کنیم. ما می‌توانیم آن را از URL زیر دانلود کنیم که شامل یک jarfile است:

<http://www.gremwell.com/download>.

بنابراین می‌تواند در هر سیستم عاملی با نصب جاوا از آن استفاده کرد. برای شروع کار با MagicTree آن را باز کرده و آدرس شبکه یا آدرس میزبان را به محدوده اضافه کنید تا MagicTree بتواند یک درخت داده را ایجاد کند. مزیت ذخیره داده‌ها در شکل درخت این است که اگر بعداً بخواهیم داده‌های دیگری را اضافه کنیم، بر درخت فعلی تأثیری نمی‌گذارد، فقط باید یک درخت جدید ایجاد کنیم. این ابزار داده‌ها را در فرم جدول یا لیست ذخیره می‌کند و از اشکال XPath برای استخراج داده‌ها استفاده می‌کند. قالب‌های گزارش زیادی وجود دارد که می‌توانند سفارشی شده و برای تولید گزارش استفاده شوند.

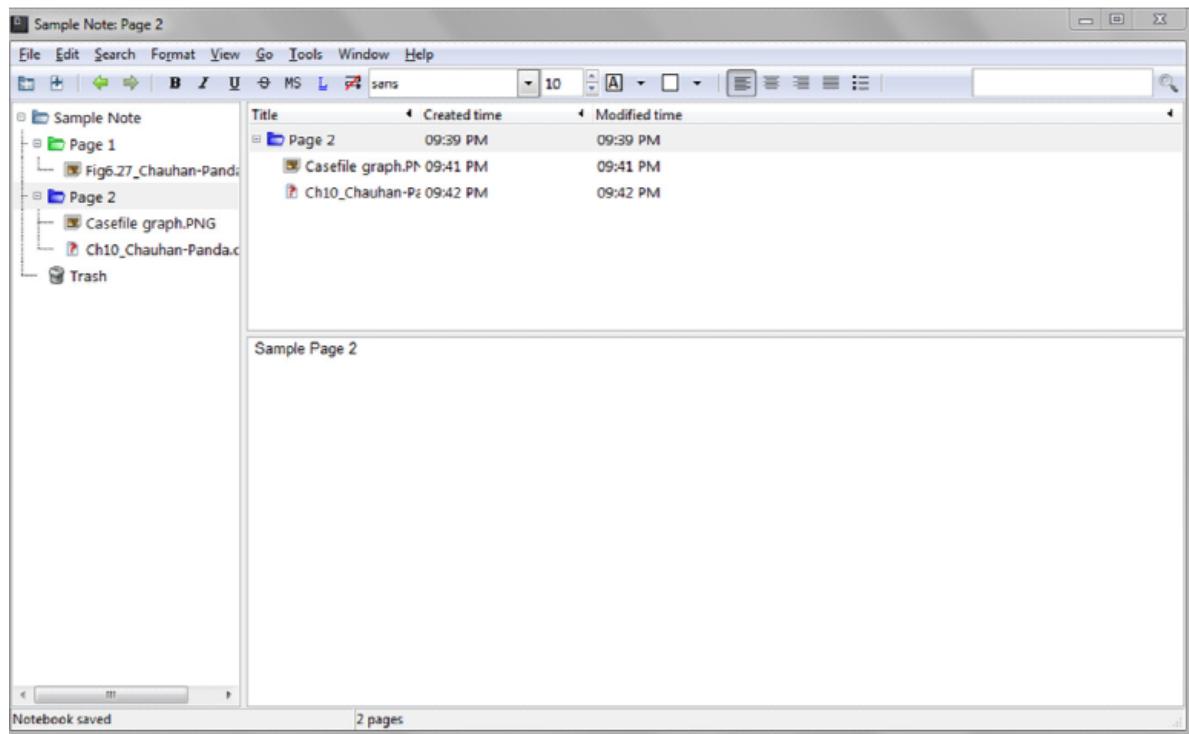
تنها محدودیت این ابزار این است که تنها از گزینه ورود اطلاعات XML پشتیبانی می‌کند؛ بنابراین نمی‌توانیم از ابزارهایی که خروجی‌های دیگری را تولید می‌کنند، استفاده کنیم. اگرچه این یک محدودیت است، اما هنوز هم این ابزار برای خودکارسازی بازیابی اطلاعات از هر ابزار، مفید است و همچنین برای تست نفوذ‌گرها بسیار توصیه می‌شود.



KeepNote

همان‌طور که نام KeepNote نشان می‌دهد برنامه‌ای است که برای یادداشت برداری استفاده می‌شود. این یک برنامه cross-platform است که می‌توانید از <http://keepnote.org> آن را دانلود کنید. برخلاف ابزارهای سنتی برای یادداشت برداری مانند Notepad، KeepNote شامل ویژگی‌های مختلفی است که باعث می‌شود تا قابلیت‌های بیشتری را داشته باشد و اجازه می‌دهد تا رسانه‌های مختلفی را در آن قرار دهیم.

برای شروع یادداشت برداری با استفاده از KeepNote باید ابتدا notebook جدیدی را از گزینه File ایجاد کنیم. هنگامی که یک notebook ایجاد شد، می‌توانیم صفحات جدید را به notebook اضافه کنیم. در حال حاضر در این صفحات می‌توانیم یادداشت‌هایمان را حفظ و آنها را دسته بندی کنیم. ما می‌توانیم به سادگی متن را در قسمت پایین سمت راست رابط قرار دهیم. همچنین به غیر از این می‌توانیم رسانه‌های مختلف مانند تصاویر را به آن اضافه کنیم.



برخی از ویژگی‌های مفید KeepNote که در سایر برنامه‌های کاربردی مشابه وجود دارند، سازماندهی سلسله مراتبی، چک کردن املا کلمات، ضمیمه رسانه‌ها، اتصال به یکدیگر وغیره است. همچنین این برنامه دارای بسیاری از پسوندها پشتیبانی می‌کند. برنامه‌های افزودنی آن را می‌توانید در <http://keepnote.org/extensions.shtml> بباید.

LUMIFY

یکی از بهترین گزینه‌های موجود برای تجزیه و تحلیل داده‌ها در به صورت منبع باز، Lumify است. همان‌طور که Lumify منبع باز است، کد آن در <https://github.com/lumifyio/lumify> در دسترس است. یک روش ساده‌تر برای استفاده و آزمایش Lumify از طریق ماشین مجازی است که می‌توانید در آدرس زیر آن را بباید:

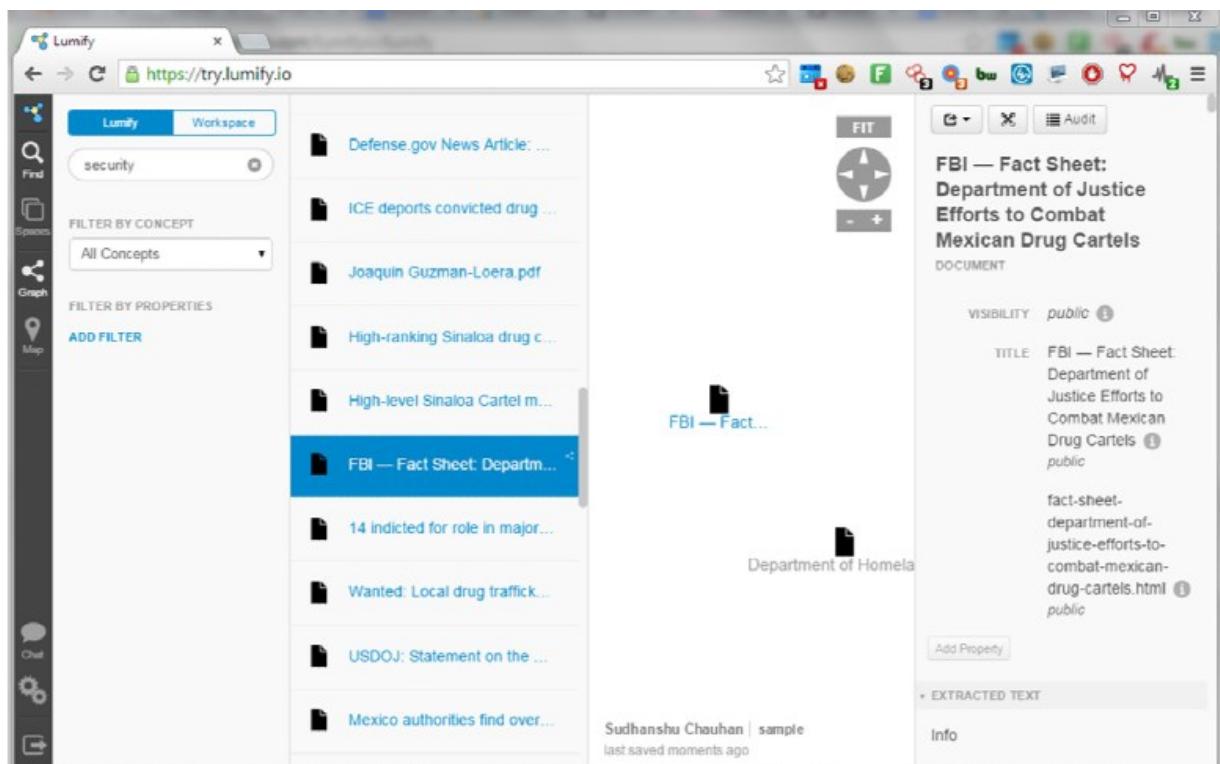
<https://github.com/lumifyio/lumify/blob/master/docs/prebuilt-vm.md>

Lumify دارای رابط مبتنی بر وب است. بر اساس مدل مبتنی بر گراف، می‌توانیم داده‌هایمان را در آن وارد و عملیات تحلیلی را بر روی آن‌ها انجام دهیم. چندین موجودیت با فیلد داده در آن وجود دارد که می‌توانیم برای نشان دادن اطلاعات، استفاده کنیم. به غیر از آن، همچنین ویژگی‌های پیشرفته‌ای مانند ادغام نقشه^۱ را فراهم می‌کند که با

^۱ Map integration

استفاده از آن می‌توانیم داده‌ها را بر روی نقشه جهانی نمایش دهیم و فضای کاریمان را به اشتراک بگذاریم. این کار اجازه می‌دهد تا اطلاعات را با دیگر اعضای تیم اشتراک گذاشته و کار به شیوه‌ای تیمی انجام شود.

طیف گسترده‌ای از ویژگی‌ها و سهولت استفاده، Lumify را به یک انتخاب عالی برای نیازهای نمایش داده و تجزیه و تحلیل اطلاعات کرده است. برخی از نمونه‌های خوب استفاده از Lumify را می‌توان در صفحه اصلی یافت. <http://lumify.io/>



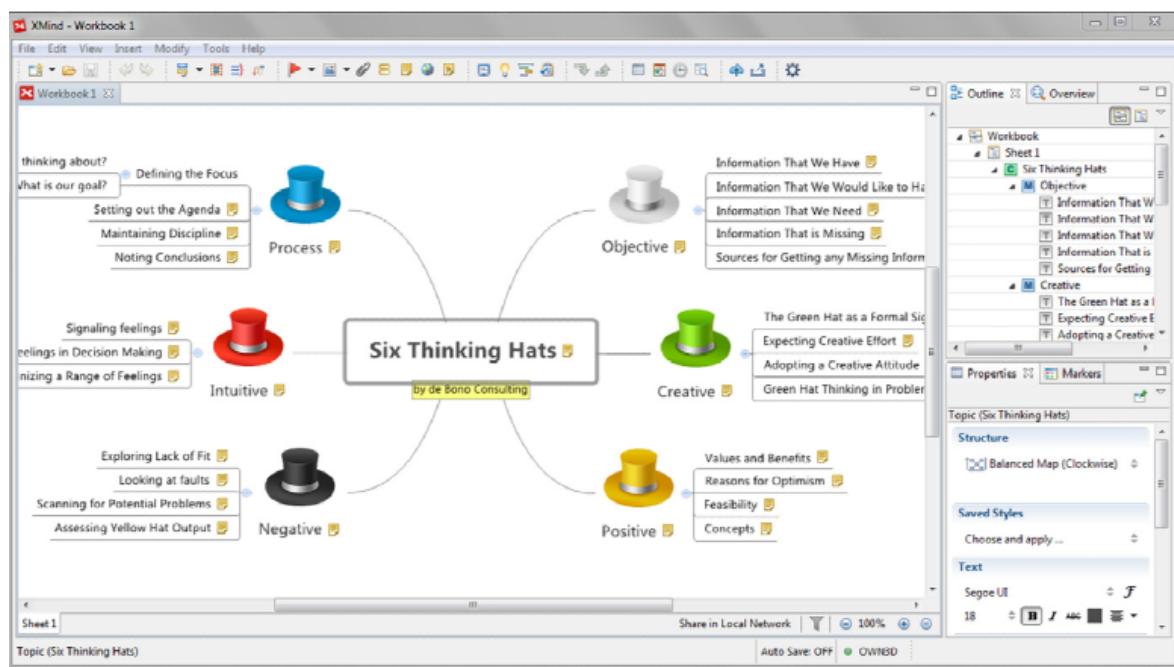
Xmind

بعضی از ابزارها برای سازماندهی داده‌ها را دیدیم. در واقع اصطلاحی که برای سازماندهی بصری اطلاعات استفاده می‌شود، نقشه ذهنی^۱ نامیده می‌شود. همان‌طور که نام نقشه ذهنی نشان می‌دهد ایده‌ها و افکار ما در مورد هر موضوع است. معمولاً یک نقشه ذهنی در اطراف یک ایده مرکزی ایجاد شده و سپس از آن گسترش می‌یابد. ایده مرکزی در دیاگرام باقی مانده و تمام اطلاعات اطراف آن می‌چرخد. این در واقع زنجیره‌ای از ایده‌ها و اطلاعات مرتبط است که در جهت‌های مختلف گسترش می‌یابد که با استفاده از شاخه‌ها، زیر شاخه‌ها از شاخه‌های

¹ mind map

اصلی ایجاد می‌شوند و به همین ترتیب گسترش می‌یابند. نقشه‌های ذهنی شامل اشکال مختلف برای نشان دادن اطلاعات یا ایده‌هایی مانند تصاویر، متن، رنگ‌ها، اشکال وغیره است.

یکی از معروف‌ترین و ابزارهای مناسب برای ایجاد نقشه‌های ذهنی Xmind است. لینک دانلود آن را می‌توان در <http://www.xmind.net/download/> بیابید. هنگامی که رابط کاربری Xmind را باز می‌کنیم، لیست گسترده‌ای از قالب‌ها و تم‌ها را ارائه داده که از آن‌ها بر اساس نیازمان انتخاب می‌کنیم. پس از انتخاب، می‌توانیم با ویرایش فیلد‌های داده، تغییر یا اضافه کردن موارد جدید را شروع کنیم. Xmind به ما اجازه می‌دهد تا اطلاعات را در قالب متن، تصویر، نشانگر، خلاصه، پیوست، یادداشت‌های صوتی وغیره قرار دهیم. انواع مختلف داده‌های مجاز Xmind باعث می‌شود تا نقشه‌ای ذهنی ایجاد شود که واقعاً می‌تواند ایده‌های ما را به نمایش بصری برساند تا نمودارهایی برای مدیریت پروژه، برنامه‌ریزی، تصمیم‌گیری وغیره ایجاد کنیم.



اگر چه نسخه رایگان Xmind در مقایسه با نسخه حرفه‌ای محدودیت‌هایی دارد، اما راههای زیادی برای نمایش ایده‌های ما در شیوه خلاقانه و مؤثر را فراهم می‌کند.

مدل‌ها و روش‌های مختلفی وجود دارد که در زمینه‌های مختلف برای فرایند تجزیه و تحلیل داده‌ها استفاده می‌شود. بعضی از آن‌ها عمومی هستند و برخی کاربرد خاص دارند. در اینجا یک رویکرد اساسی ارائه می‌دهیم که عموماً به کار رفته و می‌تواند مطابق با نیازهای خاص تغییر کند:

- ✓ اهداف: تصمیم بگیرید که به کدام سؤال باید پاسخ داد.
- ✓ شناسایی منابع: شناسایی و لیست کردن منابع که می‌تواند داده‌های مربوط به هدف ما را فراهم کنند.
- ✓ جمع‌آوری: جمع‌آوری داده‌ها با استفاده از روش‌های مختلف از تمامی منابع ممکن.
- ✓ تمیز کردن: از داده‌های جمع‌آوری شده، هر چیزی که بی‌اهمیت است باید باشد حذف شده و شکاف موجود باید پر شود.
- ✓ سازمان‌دهی داده‌ها: داده‌های پاک نشده باید به نحوی سازمان‌دهی شوند که به دسترسی آسان و سریع کمک کنند.
- ✓ مدل‌سازی داده‌ها: انجام مدل‌سازی با استفاده از تکنیک‌های مختلف مانند نمایش گرافیکی، تجزیه و تحلیل آماری و سایر روش‌های تجزیه و تحلیل داده‌ها.
- ✓ قرار دادن در چارچوب: پس از تجزیه و تحلیل داده‌ها، نیاز به تفسیر آن و سپس تصمیم‌گیری بر اساس آن وجود دارد.

برخلاف فصل‌های قبلی که در آن بر روی جمع‌آوری داده‌ها تمرکز کردیم، در این فصل تمرکز ما بر مدیریت اطلاعات است. جمع‌آوری داده‌ها مهم است اما مدیریت آن و نشان دادن آن به یک فرم که تجزیه و تحلیل آن را کنند، بسیار مهم است. همان‌طور که پیش از این در این فصل آموخته‌ایم که داده‌های خام خیلی قابل استفاده نیستند، باید آن‌ها را سازمان‌دهی و تجزیه و تحلیل کرده تا به یک فرم عملی تبدیل شوند. ابزارهای ذکر شده در این فصل در این فرآیند به ما کمک می‌کند. هنگامی که داده‌ها را تجزیه و تحلیل کردیم به اطلاعاتی دست خواهیم یافت که در تصمیم‌گیری به ما کمک می‌کنند.

در فصل بعدی ما در مورد امنیت آنلاین بحث خواهیم کرد. روز به روز فضای مجازی نامن‌تر می‌شود. بدافزارهای جدید در حال ظهور هستند، تکنیک‌های حمله پیشرفتهایی کنند، اسکمرها^۱ در حال توسعه تکنیک‌های جدید برای فریب مردم هستند و غیره. با این همه ما باید از خودمان محافظت کنیم. ما در مورد ابزارها و تکنیک‌ها برای کاهش شکاف در امنیت بحث خواهیم کرد و یاد می‌گیریم چگونه ریسک خود را به حداقل برسانیم.

¹ scammers

فصل ۱۱: امنیت آنلاین

مقدمه

در فصل‌های قبلی ما در مورد اینترنت بحث کردیم. از ابزارهای گوناگون برای دسترسی به آن در قالب‌های مختلف استفاده کردیم. با برخی از مناطق کمتر دیده شده از آن آشنا شده و در مورد چگونگی ناشناس ماندن در هنگام انجام کار با آن یاد گرفتیم. همچنین در مورد برخی از ابزارهایی که در تجزیه و تحلیل اطلاعاتی که از این منابع اطلاعاتی عظیم جمع‌آوری کردیم، بحث کردیم. در این فصل قصد داریم تا موضوعی را که در عصر دیجیتال امروز بسیار مورد توجه قرار گرفته را مس کنیم که امنیت آنلاین است. اینترنت محل خوبی است که ما می‌توانیم چیزهای مختلفی یاد بگیریم، آن را با دیگران به اشتراک بگذاریم. اینترنت در حال حاضر در سراسر جهان به آسانی در دسترس است. ما دارای دستگاه‌هایی هستیم که به ما اجازه می‌دهند حتی در حال حرکت هم به آن متصل باشیم.

امروز به اینترنت برای بسیاری از نیازهایمان مانند خرید، پرداخت صورتحساب‌ها، ثبت‌نام برای یک رویداد یا حضور در شیوه‌های اجتماعی متکی هستیم. حتی کسب و کارهای ما برای عملیات روزانه به اینترنت نیاز دارند. ما به عنوان کاربر اینترنت استفاده از سیستم‌عامل‌های مختلف، با کلیک بر روی دکمه‌های مختلف، بازدید از لینک‌های مختلف را به صورت روزانه انجام می‌دهیم. برای یک کاربر معمولی، ممکن است به نظر خیلی ساده برسد ولی مقدار زیادی از پیاده‌سازی فنی در پشت صحنه آن انجام می‌شود.

این دنیای مجازی هم مانند دنیای فیزیکی دارای مسائل امنیتی است. این خبر جدیدی نیست که افراد روزمره قربانی جرائم اینترنتی می‌شوند. تهدیدات مختلفی وجود دارد که ما در این دنیای دیجیتال با آن‌ها مواجه هستیم و گاهی حتی آن‌ها را نمی‌شناسیم. به عنوان مثال، همه ما هرزنامه‌ها را دریافت می‌کنیم که در قرعه‌کشی مقدار زیادی پول به دست آورده‌ایم و باید برخی از اطلاعات حساس را برای دریافت آن به اشتراک بگذاریم. اگرچه بسیاری از ما این پیام‌ها را نادیده می‌گیریم، برخی از مردم پاسخ می‌دهند و قربانی می‌شوند. به طور مشابه، قبلًا دیده‌ایم که اطلاعاتی که ما در اینترنت به اشتراک می‌گذاریم ممکن است چیزی درباره ما نشان دهد که ما قصد نشان دادن آن‌ها را نداریم. افشاء سهوی این نوع اطلاعات می‌تواند برای ما زیان آور باشد. به تازگی موارد متعددی گزارش شده که هکرها به یک ماشین کارمند حمله کرده تا بتوانند به اطلاعات شرکت‌ها دسترسی پیدا کنند. دلیل اصلی موفقیت این حملات، فقدان آگاهی امنیتی در میان کاربران است. اگرچه در ک جنبه‌های فنی امنیتی سایبری می‌تواند برای یک فرد غیر فنی نیاز نباشد، اما برای هر کاربر در ک اینکه چگونه برخی از حملات مشترک انجام می‌شوند، چگونه می‌توانند آن‌ها را شناسایی کنند و در نهایت چگونه می‌توانند با آن‌ها مقابله کنند، ضروری است. سوالی که عمدتاً توسط افراد مطرح می‌شود این است که چرا ما هک می‌شویم، هرچند اطلاعات حساس و یا مالی در رایانه‌هایمان نداریم. به جای پاسخ دادن به این سوال، در مورد برخی از روش‌های حمله یاد گرفته و سپس بحث می‌کنیم که چرا کسی به یک کاربر معمولی حمله می‌کند.

ما در جهانی هستیم که در آن دوست داریم زمان بیشتری را صرف زندگی آنلاین اجتماعی کنیم. دلیل آن ممکن است هر چیزی از خرید، ایمیل، مکالمه آنلاین اجتماعی، چت، پیام، یا شارژ آنلاین یا بانکی باشد. ممکن است برای استفاده حرفة‌ای از اینترنت استفاده می‌کنیم، زیرا ممکن است بخشی از کار روزانه ما باشد یا برای استفاده شخصی برای مرور یا گشت‌وگذار. به هر حال انگیزه بحث در مورد این موضوع، این است که اینترنت در حال حاضر بخشی جدایی‌ناپذیر از زندگی ما است و عدم استفاده از آن بسیار سخت است.

پیش‌تر ما فقط در مورد حریم خصوصی در اینترنت بحث می‌کنیم: نحوه حفظ حریم خصوصی با استفاده از راه حل‌های مختلف آنلاین، تنظیمات مرورگر یا برنامه‌های ناشناس کننده، در حالی که جنبه‌های دیگری را از دست می‌دهیم که امنیت است؛ بنابراین باید برخی از نکات امنیتی در مورد اینترنت را بیان کنیم.

وقتی از امنیت می‌گوییم، صرفاً در مورد استفاده از برنامه‌های ایمن یا بازدید از سایت‌های ایمن نیست و یا اجرای سیاست‌های امنیتی در سیستم مانند بروز رسانی آنتی‌ویروس و فایروال نمی‌شود. این مورد، همچنین به امنیت اطلاعات اینترنت اشاره دارد.

نه تنها امن سازی داده‌های یک سازمان، بلکه داده‌های کاربران نیز بسیار مهم است؛ بنابراین در مورد امنیت داده‌ها، ما باید بر روی داده‌های سازمانی و همچنین داده‌های کاربران تمرکز کنیم. به عنوان مثال، بگذارید بگوییم یک سازمان مکانیزم امنیتی مناسب را برای ایمن‌سازی داده‌های خود به کار می‌گیرد. انواع نرم‌افزارهای امنیتی از طریق آنتی‌ویروس، فایروال، سیستم تشخیص نفوذ، سیستم پیشگیری از نفوذ و تمامی ابزارهای امنیتی دیگر که در یک سیستم نصب شده یا اجرا شده‌اند، اما اگر خلاً امنیتی منابع انسانی وجود داشته باشد، همه این پیاده‌سازی‌های امنیتی بیهوده‌اند؛ بنابراین هم داده‌های کاربران و هم داده‌های سازمانی مهم‌اند و ما باید از هر دو مراقبت کنیم.

ما کمی درباره چگونگی افشاء اطلاعات فراداده و چگونگی پیشگیری از نشت داده‌ها و یا از دست دادن اطلاعات (DLP) برای تأمین امنیت را مورد بحث قرار دادیم؛ اما از دیدگاه کاربر نیز بسیار مهم است که جزئیات عمومی را که می‌تواند در برابر ما یا امنیت ما مورد استفاده قرار گیرد را در نظر بگیریم.

بنابراین قبل از افشاء هرگونه اطلاعات در اینترنت، به آن فکر کنید. راه دیگر این است که یک پاسخ اشتباه به سوالات امنیتی را انتخاب کنید. به عنوان مثال، برای این سؤال که رنگ موردعلاعقه شما چیست، اگر پاسخی مانند گاو نر را ارائه دهیم، حدس پاسخ مشکل و امنیت حساب شما افزایش می‌یابد. بازنمانی گذر واژه یکی از نمونه‌هایی برای چنین عملی است؛ روش‌های دیگری نیز وجود دارد که می‌تواند ما را در برابر حملاتی مانند حمله مهندسی اجتماعی، حمله فیشنینگ ساده و غیره ایمن کند. تنها راه محافظت از اطلاعات کاربر آنلاین، آگاهی است. آگاهی از نشت اطلاعات و اجتناب از آن را داشته باشید.

هر نوع اطلاعاتی که ارائه دهیم می‌تواند در برابر ما استفاده شود. اطلاعات می‌توانند هر چیزی باشند؛ بنابراین بهتر است از افشاء اطلاعات خاص در اینترنت جلوگیری شود. پیشگیری بهتر از درمان است، بنابراین داده‌های خود را با توجه به آن‌ها به اشتراک بگذارید.

اگر ما در زمینه امنیت کار می‌کنیم، باید اهمیت جمع‌آوری اطلاعات را بدانیم که مصدق جمله: "اگر می‌خواهید پیروزی را به دست آورید، ابتدا باید دشمن خود را بشناسید" است. هر اطلاعات بیشتری در مورد یک فرد یا

سازمان بدانیم، بهتر می‌بتوانیم در آن‌ها نقاط ضعف را پیدا کنیم و بعد از آن می‌توان از آن بهره‌برداری کرد. حالا ما درباره تهدیدات مشترک صحبت خواهیم کرد.

بدافزار^۱

بدافزار کلمه‌ای است که از ترکیب دو کلمه، مخرب^۲ و نرم‌افزار^۳ آمده است. تعریف ساده‌ای که می‌تواند از آن برداشت شود این است که هر نرم‌افزاری که فعالیت‌های مخرب را انجام می‌دهد می‌تواند به عنوان نرم‌افزار مخرب در نظر گرفته شود. انواع مختلف بدافزار بر اساس رفتار آن‌ها وجود دارند. بدافزارهای مختلف دارای ویژگی‌های مختلف و حالت‌های مختلف در گسترش هستند. اگر در مورد آلوده کردن یک مخاطب یا هدف استفاده شوند، به جمع‌آوری اطلاعات مربوط به او می‌تواند بسیار کمک کنند. اگر ما شخص قربانی را می‌شناسیم، می‌توانیم نرم‌افزار مورد علاقه‌اش را به بدافزار آلوده کرده و آن را به طور مستقیم با یک دستگاه ذخیره‌سازی یا فرستادن پیوند دانلود از راه دور ارسال کنیم. اگر برای اولین بار آن را اجرا کنیم، جمع‌آوری اطلاعات در مورد سیستم‌عامل و سیستم‌های امنیتی بر روی آن بسیار کمک خواهد کرد؛ بنابراین اگر یک لینک از یک شخص شناخته شده یا یک غریبه به عنوان یک کاربر دریافت کردید، آن را مستقیماً نصب نکنید. قبل از نصب دوباره فکر کنید که آیا ممکن است قربانی نرم‌افزارهای مخرب شوید. اکثر موارد بدافزارها از طریق سایت‌های اینترنتی مانند موزیک رایگان یا میزبانی نرم‌افزار رایگان و غیره منتشر می‌شوند؛ بنابراین، به عنوان یک کاربر، قبل از هر چیز منبع را بررسی کنید. طبقه‌بندی‌های مختلفی از نرم‌افزارهای مخرب وجود دارد، برخی از آن‌ها در زیر آمده است.

ویروس^۴

ویروس یا Vital Information Resources Under Seize اصطلاحی است که نام آن از ویروس‌های بیولوژیکی که به افراد منتقل شده و می‌تواند علت بیماری‌های مختلف باشند، گرفته شده است. به طور مشابه، ویروس رایانه‌ای کد مخربی است که وقتی در یک سیستم اجرا می‌شود، سیستم را آلوده می‌کند و فعالیت‌های مخرب مانند حذف اطلاعات، تخریب حافظه، اضافه کردن داده‌های تصادفی زمانی و غیره را انجام می‌دهد. تنها ضعف ویروس این است که نیاز به یک عامل برای اجرا دارد. برای جلوگیری از ویروس، از نرم‌افزار ضدویروس بروز شده استفاده کنید.

¹ MALWARES

² malicious

³ software

⁴ VIRUS

تروجان^۱

تروجان نرم‌افزار مخرب بسیار جالبی است، به‌طور کلی به عنوان یک هدیه به ما در بازدید از سایت‌ها ارائه می‌شود، به عنوان مثال با تبلیغاتی مانند برای برنده آفون شدن در اینجا کلیک کنید و یا در بازی محبوب به صورت رایگان شرکت کنید. کاربر آن را پس از دانلود نصب می‌کند، سپس یک backdoor ایجاد خواهد کرد و دسترسی کامل را به مهاجم خواهد داد؛ بنابراین برای گسترش یک تروجان، مهاجم یک برنامه محبوب، مانند بازی، فیلم یا آهنگ را انتخاب و آلوده می‌کند و با این کار شанс آلوده کردن افراد بیشتر را زیاد می‌کند.

تروجان‌ها قابلیت باز انتشاری ندارند بلکه پشت برنامه دیگری پنهان می‌شوند. توصیه می‌شود هر چیزی که به صورت رایگان ارائه می‌شود را نصب نکنید. شما هرگز نمی‌دانید که در داخل این نرم‌افزار چه چیزی پنهان است و همچنین برای حفاظت بهتر از ضد‌ویروس استفاده کنید.

باج افزار^۲

همان‌طور که از نام آن پیداست، این بدافزار بسیار جالب است که پس از آلوده شدن سیستم، برخی از منابع مهم سیستم رایانه‌ای ما را مسدود می‌کند و پس از آن درخواست پول می‌کند تا دسترسی را از پس بدهد. به‌طور معمول، باج افزارها از تکنولوژی‌های رمزگذاری برای نگهداری داده‌های ما به عنوان اسیر استفاده می‌کنند.

کیلاگر^۳

کیلاگر یک تکه از نرم‌افزار مخرب است که تمام کلیدهای فشرده شده را جمع‌آوری و به مهاجم ارسال می‌کند؛ بنابراین، هنگامی که کاربر هر کلمه اعتباری را برای ورود به سایت وارد می‌کند، اعتبارنامه می‌تواند ثبت و به مهاجم ارسال شود و بعداً می‌تواند توسط مهاجم برای انتقال حساب استفاده شود. توصیه می‌شود در تایپ کردن کلمات اعتباری در هر سایت مالی، همیشه از صفحه کلید روی صفحه‌نمایش (مجازی) استفاده کنید.

فیشینگ^۴

یکی از قدیمی‌ترین و محبوب‌ترین حملات است که در بسیاری از حملات علیه شرکت‌ها نیز مورد استفاده قرار می‌گیرد. این یک حمله ساده است که حمله‌کننده با فرستادن یک لینک جعلی که حاوی یک صفحه کاملاً شبیه به صفحه اصلی سایت است، کاربر را ترغیب به ورود به سیستم می‌کند. هنگامی که کاربر وارد سایت شود، کلمات

¹ TROJAN

² RANSOMWARE

³ KEYLOGGER

⁴ PHISHING

اعتباری به مهاجم ارسال شده و کاربر می‌تواند به سایت واقعی هدایت شود. ضعف عمدۀ در این حمله، آدرس سایت است. اگر یک کاربر آدرس سایت را به درستی تائید کند، احتمال اجرای حمله فیشنینگ وجود ندارد.

اطلاعات موردنیاز در اینجا این است که کدام سایت دارای حساب کاربری است و اهداف اغلب از آن بازدید می‌کنند؛ بنابراین مهاجم بعداً می‌تواند یک صفحه جعلی از آن ایجاد و کاربر را فریب می‌دهد.

روش‌های جدیدی از تکنیک‌های حمله فیشنینگ در حال حاضر وجود دارد. برخی از آن‌ها فیشنینگ دسکتاب^۱ هستند که در آن در فایل host سیستم قربانی یک رکورد از نام دامنه سایت اصلی را با آدرس صفحه جعلی تغییر می‌دهد؛ بنابراین هنگامی که یک کاربر آدرس IP یا نام دامنه را در مرورگر تایپ می‌کند به صفحه جعلی هدایت شده و صفحه جعلی به جای صفحه واقعی بارگذاری می‌شود.

یکی دیگر از این حملات محبوب فیشنینگ، tabnabbing^۲ است. در tabnabbing زمانی که کاربر یک صفحه جدید را باز می‌کند، صفحه اصلی با تغییر مسیر URL تغییر خواهد کرد. همچنین حملات فیشنینگ محبوب دیگر spear phishing است.

کلاهبرداری آفلاین^۳

یکی از موضوعاتی که به طور گسترده در معرض آن قرار داریم، ایمیل‌های اسپم و کلاهبرداری^۳ است. اکثر کاربران ایمیل هر روز چنین ایمیل‌هایی را دریافت می‌کنند. این ایمیل‌ها معمولاً تلاش می‌کنند تا کاربران را به ارسال اطلاعات شخصی خود ترغیب کنند و در نهایت پول خود را از دست دهند. گاهی اوقات این به صورت یک جایزه بزرگ قرعه‌کشی است که ما برنده شده‌ایم.

¹ desktop phishing

² ONLINE SCAMS AND FRAUDS

³ spam mails and scams

Maxwell Toto

Nov 24 at 10:42 PM

Beloved Friend,

I am writing this mail to you with heavy tears in my eyes and great sorrow in my heart because my Doctor told me that I will die in three months time. Based on this development I want to will my money which is deposited in a security company. I am in search of a reliable person who will use the Money to build charity organization for the saints and the person will take 20% of the total sum. While 80% of the money will go to charity organization and helping the orphanage. I grew up as an Orphan and I don't have anybody/family member after the missing of my adopted son with Malaysia Airlines Flight MH370. Meanwhile at this point I do not have anyone to take care of my wealth. The total money in question is \$7.5million dollars. I will provide you with other information's once you indicate your willingness.

Please contact me on my personal email on: maxtobo555@gmail.com

Yours sincerely,
maxwell toto

کلاه برداران^۱ آنلاین همچنین سعی می‌کنند از نوشتن داستان‌هایی مانند اینکه که در سرزمین‌های خارجی گیر کرده‌اند و به کمک ما نیاز دارند از ماهیت انسانی سوء استفاده می‌کنند. گاهی اوقات مهاجمان همچنین به عنوان ارائه دهنده خدمات ایمیل درخواست بازنشانی رمز عبور را می‌کنند. طرح‌های مختلف Ponzi وجود دارد که توسط کلاه برداران مورد استفاده قرار می‌گیرند و هدف نهایی سرقت پول ما است.

دست آویزهای هکینگ^۲

مواردی وجود دارد که متوجه شدیم حتی کاربران با سیستم عامل‌های به روز رسانی شده، آنتی‌ویروس و فایروال نیز با مشکلاتی مواجه هستند و قربانی حمله هک شده‌اند. دلیل آن برخی از برنامه‌های کاربردی محبوب است که می‌تواند در هر سیستم عامل یافت شوند. برخی از این برنامه‌ها عبارت‌اند از Adobe Acrobat Reader یا مرورگرهای وب. این نوع برنامه‌ها به طور گستردۀ ای مورد سوء استفاده قرار می‌گیرند که تقریباً تمام سیستم عامل‌ها را پوشش می‌دهند و همچنین به طور گستردۀ ای مورد استفاده قرار می‌گیرند؛ بنابراین هدف قرار دادن این برنامه‌ها به یک مهاجم امکان می‌دهد که تا حد ممکن کاربران را هک کند. آن‌ها پلاگین‌های مرورگر یا افزودنی‌های مرورگر را ایجاد می‌کنند که می‌توانند به کاربر برای تکمیل یک فرایند به طور خودکار کمک کنند و همین‌طور در پشت صحنه می‌توانند اطلاعات آن را جمع‌آوری کنند. به عنوان مثال، جمع‌آوری تمام اقدامات انجام شده توسط کاربر در مرورگر.

¹ Scammers

² HACKING ATTEMPTS

رمز عبور ضعیف^۱

کلمه عبور ضعیف همیشه نقش مهمی در هک شدن بازی می‌کند. برای سهولت استفاده، کاربران از رمز عبور پیچیده استفاده نمی‌کنند و به همین دلیل از کلمات عبور ساده مانند ۱۲۳۴۵، ۱۲۳۴۶، شماره تلفن همراه خود و غیره استفاده می‌کنند. رمز عبور ضعیف همیشه دارای طول و کاراکترهای مورد استفاده مناسب نیستند، بنابراین به سادگی حدس زده می‌شوند. نام @۱۲۳۴۵، به نظر می‌رسد بسیار پیچیده باشد اما می‌تواند حدس زده شود؛ بنابراین در ساخت رمز عبور از نام، مکان یا شماره تلفن خود استفاده نکنید. کلمه عبور ضعیف می‌تواند حدس زده شود. اگر رمز بسیار کوچک باشد، مهاجم می‌تواند آن را با استفاده از حمله بروت فورس به دست آورد؛ بنابراین سعی کنید از رشته‌های تصادفی با کاراکترهای خاص استفاده کنید. اگر چه از دیدگاه امنیتی می‌تواند دشوار به نظر برسد اما کاملاً امن است.

رمز عبور قوی نیز لازم است به درستی ذخیره شود. برای مثال، من یک گاو صندوق فلزی بزرگ برای ذخیره همه‌چیزهای ارزشمندی خودم دارم و کلید آن را در بالای آن گذاشتم. این امنیتی را فراهم نمی‌کند. این نه تنها امن نیست بلکه در مورد باعث ناامنی نیز می‌شود است. به طور مشابه، اگر یک رمز عبور بسیار پیچیده ایجاد کنیم و آن را روی کاغذی بنویسیم و روی میز قرار دهیم!!!

SHOULDER SURFING

SHOULDER SURFING همیشه یک چالش شناخته شده است، شخصی که شما می‌شناسید و با شما کار می‌کند. اگر او می‌خواهد حساب کاربری شما را هک کند، در حالی که شما کلمه عبور را تایپ می‌کنید بسیار ساده است. تنها راه برای آن این است که برخی از کاراکترهای رمز عبور صحیح را وارد و سپس برخی از کاراکترهای اشتباه را وارد کنید. سپس کاراکترهای اشتباه را حذف و رمز عبور را کامل کنید.

مهندسی اجتماعی^۲

زمانی که ما از مهندسی اجتماعی می‌خوانیم، اولین چیزی که به ذهن ما می‌رسد این است: «هیچ وصله‌ای برای حماقت انسان وجود ندارد» و یا اینکه انسان ضعیف‌ترین پیوند در زنجیره امنیتی است. این حمله‌ای است که در برابر اعتماد کاربر انجام می‌شود. در این حمله، مهاجم ابتدا برنده اعتماد فربانی شده و سپس تمام اطلاعاتی را که

¹ WEAK PASSWORD

² SOCIAL ENGINEERING

برای اجرای یکی از حملات لازم است را ، جمع‌آوری می‌کند. تنها راه جلوگیری از قربانی بودن عدم اعتماد به همه است. هیچ‌گونه اطلاعاتی را که ممکن است با امنیت مربوط باشد، افشا نکنید.

بنابراین این‌ها بعضی از چالش‌های مربوط به امنیت است که ما با آن رویرو هستیم، اما ما تنها مشکل را پوشش داده‌ایم. بایاید بینیم راه حل چیست.

آن‌تی‌ویروس^۱

همان‌طور که ما کردیم انواع مختلفی از بدافزارها وجود دارد و هر یک از دارای روش حمله و هدف منحصر به فرد است. انواع مختلفی از آن‌ها وجود دارند و اکثر کاربران رایانه با این مشکل مواجه هستند.

آن‌تی‌ویروس یکی از محصولات امنیتی است که به‌طور گستره‌ای توسط سازمان‌ها و همچنین افراد مورد استفاده قرار می‌گیرد. یک آن‌تی‌ویروس اساساً یک بسته نرم‌افزاری است که بدافزارهای موجود در دستگاه‌های رایانه ما را تشخیص می‌دهد و تلاش می‌کند تا آن را پاک‌سازی کند. آن‌تی‌ویروس‌ها از روش امضا و اکتشافی^۲ برای شناسایی کد مخرب استفاده می‌کنند که می‌تواند موجب آسیب دیجیتالی شوند. همان‌طور که بدافزارهای جدید شناسایی می‌شوند، امضاها و اکتشافات جدید ایجاد شده در نرم‌افزار به‌روز می‌شوند تا ما را از تهدید جدید حفظ کنند.

در گذشته بسیاری از آن‌تی‌ویروس‌ها سرعت سیستم را کاهش داده و استفاده از آن‌ها دشوار بود. همچنین به‌روزرسانی‌های مکرر نیز افراد زیادی را آزار می‌داد. به تازگی آن‌تی‌ویروس‌ها نیز تکامل یافته و کارآمدتر شده‌اند. بسیاری از راه‌حل‌ها همچنین ویژگی‌های اضافی مانند کنترل هرزنامه‌ها و سایر راه‌حل‌های امنیتی آنلاین را همراه با آن‌تی‌ویروس فراهم می‌کنند. به‌روزرسانی‌ها به‌طور منظم نه فقط برای ویژگی‌ها بلکه برای به‌روز نگهداشت پایگاه داده برای حفظ امنیت انجام می‌شوند. در بازار آن‌تی‌ویروس رایگان و همچنین تجاری مختلفی وجود دارند، اما مهم این است که کدام از آن‌ها دارای آخرین به‌روزرسانی‌ها است زیرا بدافزارهای جدید هر روز در حال ظهور هستند. یکی دیگر از چیزهایی که باید در نظر داشته باشید این است که برخی از بدافزارها نیز به‌عنوان ضدویروس ظاهر می‌شوند و از این رو باید هنگام انتخاب یک آن‌تی‌ویروس بسیار مراقب باشیم و فقط آن‌ها را باید از منابع قابل اعتماد دانلود کنیم.

¹ ANTIVIRUS

² signature and heuristics

شناسایی فیشینگ و یا SCAMS^۱

ما روزانه با تعداد زیادی از کلاهبرداری‌های آنلاین و فیشینگ روبرو می‌شویم. امروزه خدمات پست الکترونیکی به‌طور خودکار آن‌ها را شناسایی و به بخش هرزنامه انتقال می‌دهند، اما هنوز برخی از این‌ها مدیریت می‌شوند. در اینجا چند نکته برای شناسایی این کلاهبرداری آنلاین وجود دارد:

- ✓ زبان و دستور زبان ضعیف: معمولاً^۲ این دسته از ایمیل‌ها با زبان ضعیف و دستور زبان اشتباه نوشته شده‌اند.
- ✓ آدرس فوق العاده طولانی و دامنه عجیب و غریب: URL‌های ذکر شده در چنین ایمیلی و یا URL‌های صفحه فیشینگ را می‌توان با سادگی با اشاره ماوس بر روی لینک مشاهده کرد. معمولاً چنین آدرس‌هایی بسیار طولانی هستند و دامنه‌های عجیبی دارند. این برای مخفی کردن دامنه اصلی استفاده می‌شود و دامنه صفحه‌ای که در نوار آدرس مرورگر phishing شده است نشان داده می‌شود.
- ✓ تنظیم ضعیف صفحه: ترتیب متن و تصاویر به‌طور کلی ضعیف است زیرا بسیاری از مهاجمان از ابزارهایی برای ایجاد چنین ایمیل استفاده می‌کنند.
- ✓ آدرس ایمیل: ایمیل اصلی باید بررسی شود تا فرستنده را تائید کند.
- ✓ گم شدن HTTPS: اگر صفحه معمولاً HTTPS است و در این زمان HTTPS نباشد، این نشانه هشدار دهنده است.
- ✓ درخواست اطلاعات شخصی و یا حساس: معمولاً هیچ سازمانی اطلاعات شخصی یا حساس را از طریق پست الکترونیکی درخواست نمی‌کند. در صورت دریافت چنین ایمیلی، قبل از ارسال چنین اطلاعاتی بهتر است با تماس با سازمان، تائید شود.
- ✓ ضمیمه‌های مشکوک: گاهی اوقات ضمیمه این نوع ایمیل‌ها به شکل فرم یا سند از پسوندهای عجیب و غریب از قبیل xyz.doc.exe برای پنهان کردن نوع فایل اصلی استفاده می‌کنند. این پیوست‌ها نباید باز شود. در صورتی که پیوست باید باز شود، باید آن را در یک محیط کنترل شده مانند یک ماشین مجازی بدون اتصال باز کرد.

^۱ IDENTIFY PHISHING/SCAMS

به روز رسانی سیستم عامل و سایر برنامه‌ها^۱

یکی از روش‌های عمدۀ استفاده شده توسط مهاجمان برای دسترسی به ماشین‌های ما، استفاده از برنامه‌های موجود در سیستم ما است. سیستم عامل استفاده شده و یا برنامه‌های در حال اجرا بر روی آن شامل آسیب‌پذیری‌هایی می‌باشند. مهاجمان از کدهای اکسلپلوبیت^۲ برای حمله به این آسیب‌پذیری‌های خاص استفاده می‌کنند و از سیستم‌های رایانه‌ای دسترسی می‌گیرند. آسیب‌پذیری‌های جدید به صورت منظم کشف می‌شوند و از این‌رو، خطر افزایش می‌یابد. از سوی دیگر، تکه‌هایی از این آسیب‌پذیری‌ها نیز توسط فروشنده‌گان منتشر می‌شود. به روز رسانی نرم‌افزارهای دستگاه ما یک روش مؤثر برای به حداقل رساندن خطر حمله به آن است.

تقریباً تمام سیستم عامل‌ها دارای مکانیزمی هستند که اجازه می‌دهد تا آن‌ها را با آخرین وصله‌های موجود به روز کنند. آن‌ها همچنین به ما اجازه می‌دهند تا به صورت دستی وصله‌ها را در صورت موجود بودن بررسی و نصب کنند. جدا از این، برنامه‌های دیگری که ما از آن‌ها استفاده می‌کنیم مانند پخش کننده‌های چندرسانه‌ای و غیره، دارای وصله‌هایی هستند و بعضی از آن‌ها به صورت خودکار به روز می‌شوند در حالی که بعضی از آن‌ها باید به طور جداگانه دانلود و نصب شوند.

یک برنامه مبتنی بر ویندوز است که به ما کمک می‌کند تا نرم‌افزارهای قدیمی را شناسایی کنیم و همچنین ما را قادر به انجام به روز رسانی خودکار می‌کند. این ابزار می‌تواند به سادگی در پس زمینه اجرا شده و برنامه‌هایی را که نیاز به روز رسانی دارند شناسایی کند. می‌تواند وصله مناسب را دانلود کرده و همچنین آن را نصب کند. در صورتی که قادر به انجام آن نباشد به کاربر هشدار داده و همچنین دستورالعمل‌های مفید را ارائه می‌دهد.

افزونه‌های امنیتی^۳

مرورگرهای وب یکی از رایج‌ترین برنامه‌های کاربردی در هر پلت فرم و همچنین رسانه‌ای برای بیشتر حملات هستند. بایید با بعضی از افزونه‌های که می‌تواند به ما در حفظ امنیت آنلاین کمک کند، آشنا شویم.

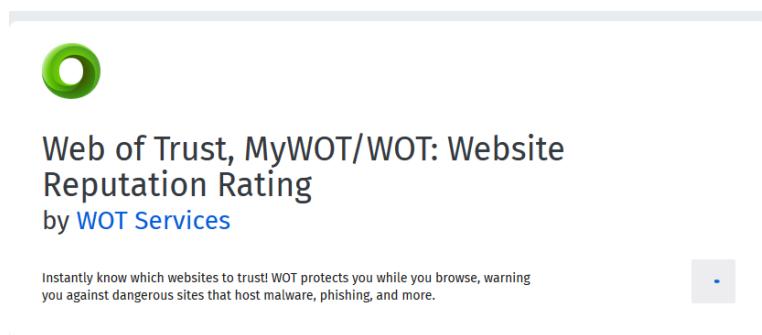
WEB OF TRUST (WOT)

^۱ UPDATE OPERATING SYSTEM AND OTHER APPLICATIONS

^۲ exploit

^۳ ADDONS FOR SECURITY

WOT یک سرویس است که اعتبار وب‌سایت را بر اساس روش crowdsourced بررسی می‌کند. بر اساس بررسی crowd، این افزونه به ما اجازه می‌دهد تا میزان اعتماد و ایمنی کودک آن را ارزیابی کنیم. به همین ترتیب کاربران همچنین می‌توانند یک وب‌سایت را رتبه‌بندی کنند و از این طریق به ایجاد وب امن‌تر کمک کنند. جزئیات و نظرات مربوط به وب‌سایتی که بازدید می‌کنید نیز می‌توانید مشاهده کنید که به کاربران کمک می‌کند که تصمیم‌گیری آگاهانه داشته باشند. استفاده از آن بسیار ساده است، از وب‌سایت بازدید و بر روی افزونه WOT در نوار مرور گر کلیک کنید و جزئیات مربوط به آن را نمایش می‌دهد. افزونه در [برای مرورگرهای مختلف در دسترس است.](https://www.mywot.com/en/download)



HTTPS EVERYWHERE

HTTPS Everywhere یک افزونه مرورگر متوجه می‌کند که امنیت است. بعضی از وب‌سایتها دارای HTTP و همچنین صفحات HTTPS هستند، اما به طور پیش فرض از HTTPS استفاده نمی‌کنند یا گاهی اوقات پشتیبانی HTTPS محدود را فراهم می‌کنند. HTTPS Everywhere از HTTPS را بر روی سیستم عامل‌ها اجبار می‌کند و از این طریق به انتقال امن اطلاعات بین سرویس‌گیرنده و سرور کمک می‌کند. افزونه در <https://www.eff.org/HTTPS-EVERYWHERE> در دسترس است.

NoScript

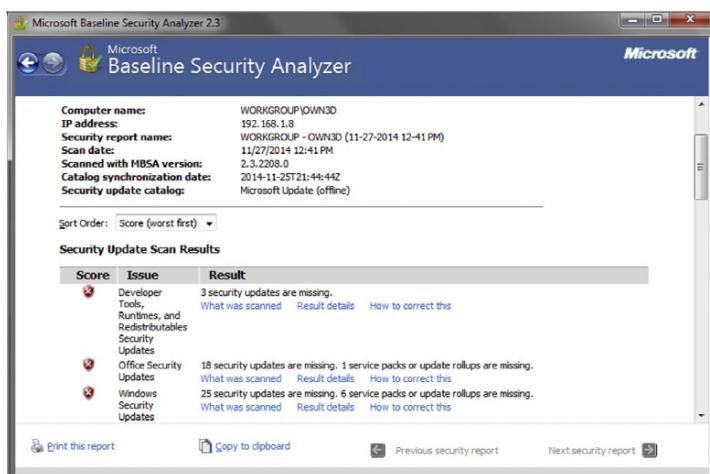
NoScript یک افزونه مرورگر است که به ما امکان می‌دهد تا اجرای جاوا اسکریپت و تکنولوژی‌های مشابه فعال محتوای را در وب‌سایتها مدیریت کنیم. ما می‌توانیم لیست برنامه‌های کاربردی مورد اعتماد داشته و ما باقی را مسدود کنیم. این به ما اجازه می‌دهد از حملات Cross-Site Scripting (XSS) و Clickjacking در امان باشیم که به طور گسترده مورد بهره‌برداری قرار می‌گیرد. NoScript برای مرورگرهای مبتنی بر فایرفاکس در دسترس است و آن را می‌توانید در آدرس <https://noscript.net/> بیایید. جایگزین آن برای مرورگر کروم ScriptSafe است.

https://chrome.google.com/webstore/detail/scriptsafe/oiigbmnaad_bkfbmpb_fi_jl_fl_ahbdbdgdf?hl=en

ابزار امنیتی

اگر چه همه ما از درک فنی استفاده از اسکن آسیب‌پذیری کامل برخوردار نیستیم ولی آن را حس می‌کنیم، برخی از ابزارهای ساده وجود دارند که به ما اجازه می‌دهد اسکن را انجام دهیم و آسیب‌پذیری‌های اساسی را در دستگاه مان شناسایی کنیم.

برای سیستم‌ها مبتنی بر ویندوز (MBSA) یک برنامه کاربردی Microsoft Baseline Security Analyzer (MBSA) است. این توسط مایکروسافت ارائه شده و به ما کمک می‌کند تا امنیت پایه ویندوز و سرویس‌های مرتبط را آزمایش کنیم. این اساساً برای کمبودهای وصله‌های نرم‌افزاری و خطاهای نامطلوب رایج است تا بتوان آن‌ها را وصله کرد. به غیر از سیستم‌عامل پایه، همچنین سرویس‌های مایکروسافت و برنامه‌های کاربردی دیگر نیز بررسی می‌شود.



به طور مشابه Linux Basic Security Audit (LBSA) وجود دارد. این اسکریپتی است که با هدف امن ساختن سیستم‌های مبتنی بر لینوکس نوشته شده است. هر چند تنظیمات باید بسته به شرایط موردنیاز تغییر کرده و ممکن است برای تمام سناریوهای مناسب نباشد. اطلاعات بیشتر در مورد آن را می‌توان در <http://wiki.metawerx.net/wiki/LBSA> ببینید.

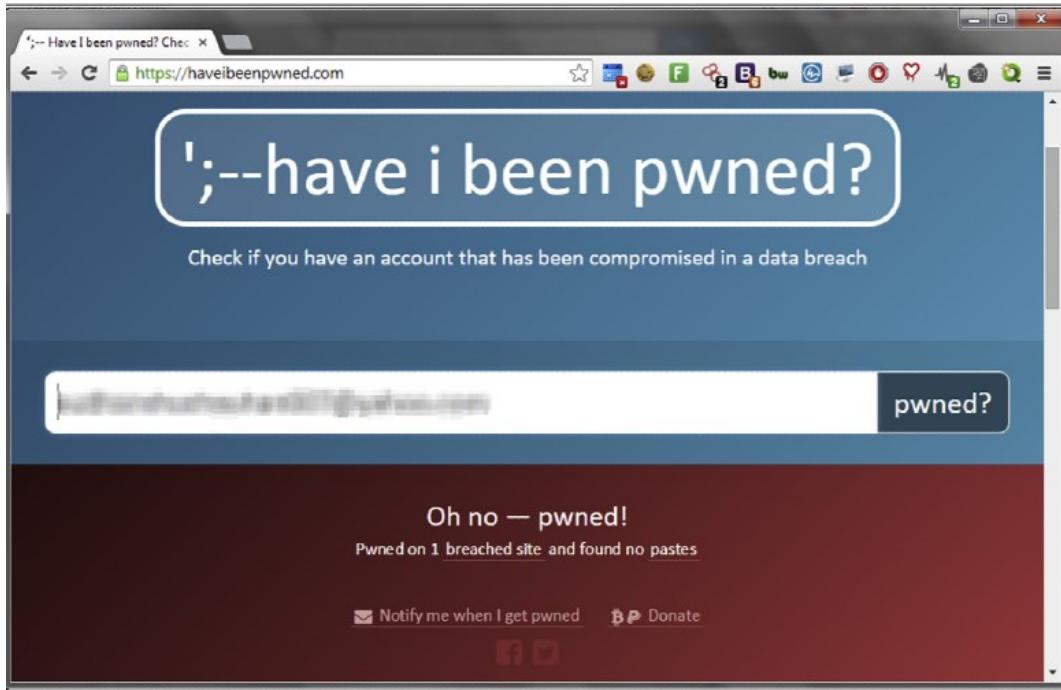
با استفاده از چنین ابزارهای رایگان و آسان، قطعاً می‌توانیم شکاف‌های امنیتی را شناسایی و اقدامات لازم را برای وصله کردن آن‌ها انجام دهیم.

سیاست گذرواژه

همان‌طور که ما از کلیدها برای حفظ احراز هویت در دنیای واقعی استفاده می‌کنیم، از کلمات عبور در دنیای دیجیتال استفاده می‌کنیم. رمزهای عبور ترکیبی از کاراکترها از مجموعه‌های مختلف حروف، رقم‌ها، کاراکترهای خاصی است که ما برای دسترسی به آن‌ها ارائه می‌دهیم و ثابت می‌کنیم که ما صاحب قانونی داده‌ها و یا سرویس خاص هستیم. با استفاده از کلمه عبور ما به رایانه‌ها، پروفایل‌های اجتماعی و حتی حساب‌های بانکی دسترسی داریم. اگرچه کلمه عبور از چنین حساسیتی برخوردارند، اکثر ما رمز عبور ضعیفی را انتخاب می‌کنیم. این به خاطر تمایل ما به انتخاب چیزهایی است که بتوانیم به آسانی آن‌ها را به یاد داشته باشیم. حمله کننده از این ضعف انسانی سوءاستفاده کرده و سعی می‌کند با استفاده از تکنیک‌های مختلف به اطلاعات ارزشمند ما دسترسی پیدا کند.

بدون در نظر گرفتن جزئیات فنی چنین حملاتی، برخی از آن‌ها سعی می‌کنند اسم، نام پدر، مادر، خواهر، برادر، همسر، تاریخ تولد و غیره را حدس بزنند؛ بروت فورس، تلاش برای هر ترکیب احتمالی با استفاده از ابزار و یا اسکریپت‌های خودکار است. مانع توانیم کنترلی را برای کاهش این مسائل داشته باشیم، اما می‌توانیم تلاش کنیم تا رمزهای عبور به اندازه کافی قوی داشته باشیم. توصیه‌های عمومی برای کلمه عبور این است که باید حداقل ۸ کاراکتر طول داشته باشند، باید شامل کاراکترها (حروف کوچک و بزرگ)، رقم‌ها و کاراکترهای خاص باشند. این ترکیب باید به گونه‌ای باشد تا حتی افرادی که ما را می‌شناسند نتوانند به راحتی حدس بزنند. گاهی اوقات مردم حتی پس از پیروی از این قوانین یک رمز عبور ضعیف ایجاد می‌کنند، یکی از مثال‌هایی مانند Pa\$\$w0rd است. ابزارهایی هستند که به مهاجمان اجازه می‌دهند لیستی از این ترکیبات را ایجاد و از آن برای حمله به حساب کاربری استفاده کنند. یک برنامه آنلاین وجود دارد که می‌تواند برای بررسی پیچیدگی گذرواژه ما استفاده شود و به ما می‌گوید چقدر طول می‌کشد تا حدس زده شود: <https://howsecureismypassword.net/>.

جدا از این، ما نباید از یک رمز عبور برای حساب‌های مختلف استفاده کنیم، زیرا در صورتی که یک حساب هک شود، می‌تواند برای دسترسی حساب‌های دیگر ما به کار رود. برای حل مشکل به خاطر سپردن کلمات عبور زیاد، می‌توان از یک مدیر رمز عبور مانند LastPass (<https://lastpass.com/>) استفاده کرد. گزینه‌های دیگری نیز وجود دارد.



همچنین سرویس‌های مختلفی وجود دارد که به ما اجازه می‌دهد تا بررسی کنیم که آیا هر یک از حساب‌های مربوط به آدرس‌های ایمیل ما به خطر افتاده است. یکی از این سرویس‌های رایگان [HaveIBeenPwned](#) به آدرس زیر است:

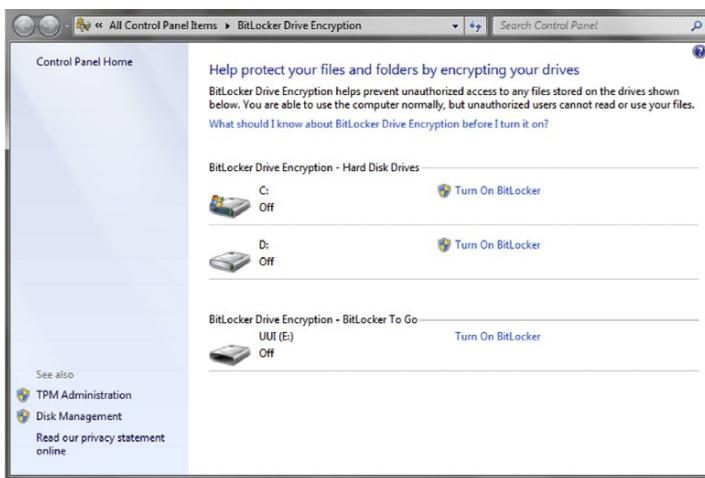
<http://haveibeenpwned.com/>

احتیاط در برابر مهندسی اجتماعی

یکی از تکنیک‌های اصلی استفاده شده توسط هکرهای استخراج اطلاعات حساس از قربانیان، مهندسی اجتماعی است. ما به عنوان انسان به طور طبیعی تمایل داریم به دیگران کمک کنیم. با استفاده از این و دیگر نقاط ضعف مشابه در طبیعت انسانی (در زمینه امنیت)، ما توسط مهاجمان مورد سوءاستفاده قرار می‌گیریم. برای محافظت در برابر چنین حملاتی، آگاهی امنیتی بسیار مهم است. مردم باید بدانند که چه اطلاعاتی حساس است. به عنوان مثال، ممکن است به نظر برسد که گفتن نسخه مرورگر ما در شرکت، هیچ آسیبی نمی‌رساند، اما این اطلاعات برای مهاجم بسیار مهم‌اند؛ بنابراین قبل از اینکه فرد اعتماد کند باید هویت شخص مقابله تائید شود. برای تائید اینکه آیا شخصی راست می‌گوید، باید آن را بررسی کند. در صورت شک و تردید، بهتر است از کسی در مقام بالاتر بپرسد.

رمزگذاری داده‌ها

انگیزه بسیاری از حملات، دسترسی به داده‌ها است. یک گام برای جلوگیری از این اتفاق، استفاده از یک نرم‌افزار رمزگذاری دیسک است. آنچه انجام می‌دهد این است که فایل‌های مشخص شده در دستگاه ما را با یک روش رمزگذاری قوی رمزگذاری می‌کند و از رمز عبور محافظت می‌کند. حتی اگر دستگاه سرفت شود، دریافت اطلاعات را برای مهاجمین بسیار سخت می‌کند. راه حل‌های زیادی وجود دارد که این قابلیت‌ها را ارائه می‌دهند مانند TrueCrypt، BitLocker. توصیه می‌شود آسیب‌پذیری عمومی نرم‌افزار رمزگذاری که در حال استفاده از آن هستید را بررسی کنید. به طور مشابه توصیه می‌شود که تمام داده‌های حساس آنلاین را به صورت رمزگذاری ذخیره و ارسال کنید.



برخی از روش‌های عمومی که به ما کمک می‌کنند امنیت آنلاین را حفظ کنیم و داده‌هایمان را ایمن نگهداشیم عبارت‌اند از:

- ✓ نشانی‌های اینترنتی را که به آن‌ها اعتماد ندارید، باز نکنید.
- ✓ قبل از کلیک کردن بر روی «Accept» توافق نامه، آن را کاملاً مطالعه کنید.
- ✓ از منابع نامشخص دانلود نکنید.
- ✓ رفتار غیرطبیعی را نادیده نگیرید (راه‌اندازی مجدد سیستم، تخریب هارد دیسک بدون هیچ دلیلی و غیره).
- ✓ پشتیبان گیری از اطلاعات مهم به صورت منظم.

انگیزه‌های متعددی در پشت چنین حملاتی وجود دارد و برخلاف باورهای عمومی فقط شرکت‌های بزرگ در خطر نمی‌باشند. همان‌طور که قبلاً اشاره شد بیشتر حملات به شکل اسپم و یا فیشنینگ به سادگی مورد استفاده قرار

می‌گیرند تا مستقیماً پولی از قربانی به دست آورند، اما بعضی از حملات دلیل بزرگتری دارند. برخی از حملات به منظور استخراج اطلاعات هستند که می‌توانند در حملات بعدی مورد استفاده قرار گیرند. برای مثال، حمله به رایانه شخصی یک کارمند برای استخراج اطلاعات آن که امکان دسترسی به شبکه شرکت را فراهم می‌کند. به طور مشابه، برخی از مهاجمان نیاز به دسترسی به دستگاه‌های قربانی دارند تا بتوانند بعداً برای اهداف مختلف مانند استخراج بیت کوین و یا به عنوان یک پروکسی برای حمله به دیگران (زامبی) و غیره استفاده کنند.

بنابراین در مورد برخی از روش‌های مشترک استفاده شده توسط مهاجمان و همچنین نحوه شناسایی آن‌ها و حفاظت از آن‌ها یاد گرفتیم. دنیای مجازی کاملاً ناامن است، هرچند که محصولات و سرویس‌های مختلفی وجود دارد که می‌تواند به کم کردن ریسک، ما کمک کند که هیچ کدام از آن‌ها امنیت صد درصدی را نمی‌توانند تضمین کنند. افرادی که ضعیف‌ترین پیوند در زنجیره امنیتی هستند، ساده‌ترین هدف برای مهاجمان‌اند. تنها با آگاهی ما، در کدام روش‌های مهاجم و اقدامات احتیاطی مناسب است که زندگی دیجیتال ما امن‌تر می‌شود.

فصل ۱۲: مبانی تجزیه و تحلیل شبکه‌های اجتماعی

مقدمه

در یکی از فصل‌های اخیر اهمیت مدیریت داده‌ها و تجزیه و تحلیل را مورد بحث قرار دادیم. همچنین درباره ابزارهای خاصی که در این روند مفید بودند، یاد گرفتیم. در این فصل با یک موضوع مرتبط که تجزیه و تحلیل شبکه‌های اجتماعی^۱ (SNA) است، روپرتو خواهیم شد. SNA به طور گسترده‌ای در علوم اطلاعات برای یادگیری مفاهیم مختلف مورد استفاده قرار می‌گیرد. این موضوع وسیع است و در بسیاری از زمینه‌ها کاربرد دارد و در این فصل ما سعی خواهیم کرد جنبه‌های مهم موضوع و ابزار موردنیاز برای آن را پوشش دهیم تا خوانندگان بتوانند با توجه به نیازهای شخصی آن را بیشتر استفاده کنند.

شبکه اجتماعی که در مورد آن صحبت می‌کنیم ساختاری است که از عناصر مختلف اجتماعی و رابطه بین آن‌ها تشکیل شده است. در این شبکه گره‌ها، موجودیت‌ها و لبه‌ها، روابط هستند. این بدان معناست که با استفاده از SNA می‌توانیم روابط بین موجودیت‌های مختلف را اندازه‌گیری و نقشه‌بندی کنیم، این‌ها معمولاً افراد، رایانه‌ها، مجموعه‌ای از آن‌ها یا سایر عوامل مرتبط هستند. SNA از نمایه‌های بصری شبکه به منظور درک بهتر آن و پیاده‌سازی نظریه‌های ریاضی برای به دست آوردن نتایج استفاده می‌کند. ابزارهای مختلفی وجود دارد که می‌تواند برای انجام SNA مورد استفاده قرار گیرد و آن‌ها در صورت نیاز مورد بررسی قرار خواهیم داد.

¹ social network analysis

اکنون با برخی از مفاهیم اساسی آشنا می‌شویم.

گره‌ها^۱

گره‌ها برای نشان دادن موجودیت‌ها استفاده می‌شوند. موجودیت‌ها بخش مهمی از شبکه‌های اجتماعی هستند، زیرا کل تجزیه و تحلیل در اطراف آن‌ها متمرکز است. آن‌ها عمدتاً به شکل دایره شکل گرفته‌اند.

لبه‌ها^۲

لبه‌ها برای نشان دادن روابط استفاده می‌شوند. روابط برای تعیین اینکه چگونه یک گره به دیگری متصل است، مورد نیاز است. این ارتباط بسیار مهم است زیرا کمک می‌کند تا به تجزیه و تحلیل‌های مختلفی نظری چگونگی انتقال اطلاعات در شبکه و غیره کمک کند. تعداد لبه‌های متصل به یک گره درجه آن را تعیین می‌کند. اگر یک گره دارای سه پیوند به موجودیت‌های دیگر باشد، درجه آن ۳ است.

شبکه^۳

شبکه به صورت بصری نمایش داده شده و حاوی گره‌ها و لبه‌ها است. پارامترهای مختلف گره‌ها و لبه‌ها مانند اندازه، رنگ و غیره ممکن است بسته به تحلیل مورد نیاز انجام شود.

شبکه‌ها می‌توانند مستقیم و یا غیرمستقیم باشند، بدین معنی که لبه‌ها ممکن است به صورت خطوط ساده یا به صورت فلش نشان داده شوند. این در درجه اول بستگی به روابط بین لبه‌ها دارد. به عنوان مثال، در شبکه‌ای از ارتباط متقابل مانند دوستان، می‌تواند یک شبکه بدون جهت باشد اما برای یک شبکه از روابط مانند کسی که دوست دارد که می‌تواند شبکه را جهت دار باشد. حال که ما یک ایده اولیه SNA را دانستیم، بباید با یکی از ابزارهای مورد استفاده از آن آشنا شویم.

GEPHI

Gephi یک ابزار ساده و مؤثر برای استفاده از SNA است. این ابزار را می‌توان از <http://gephi.github.io> دانلود کرد و روند نصب آن بسیار ساده است. پس از نصب، این ابزار برای استفاده آماده است. رابط کاربری آن ساده و به

¹ NODES

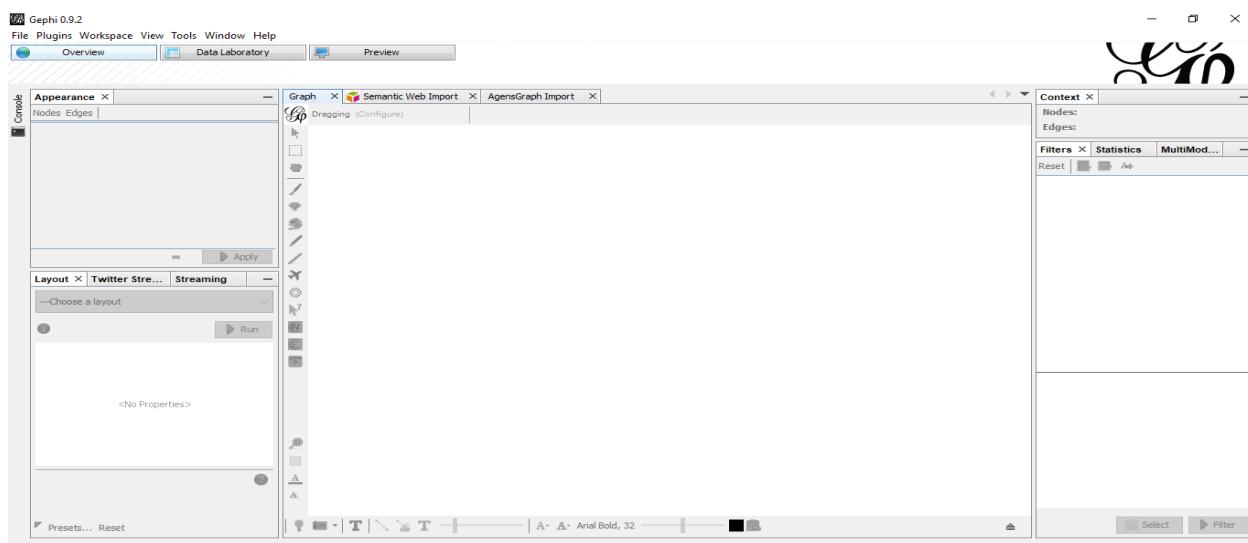
² EDGES

³ NETWORK

بخش‌های مختلف تقسیم می‌شود. سه زبانه در گوشه بالا سمت چپ وجود دارد که اجازه می‌دهد با شبکه‌های مختلف کار کند. این سه زبانه عبارت‌اند از: Preview و Data Laboratory و Overview.

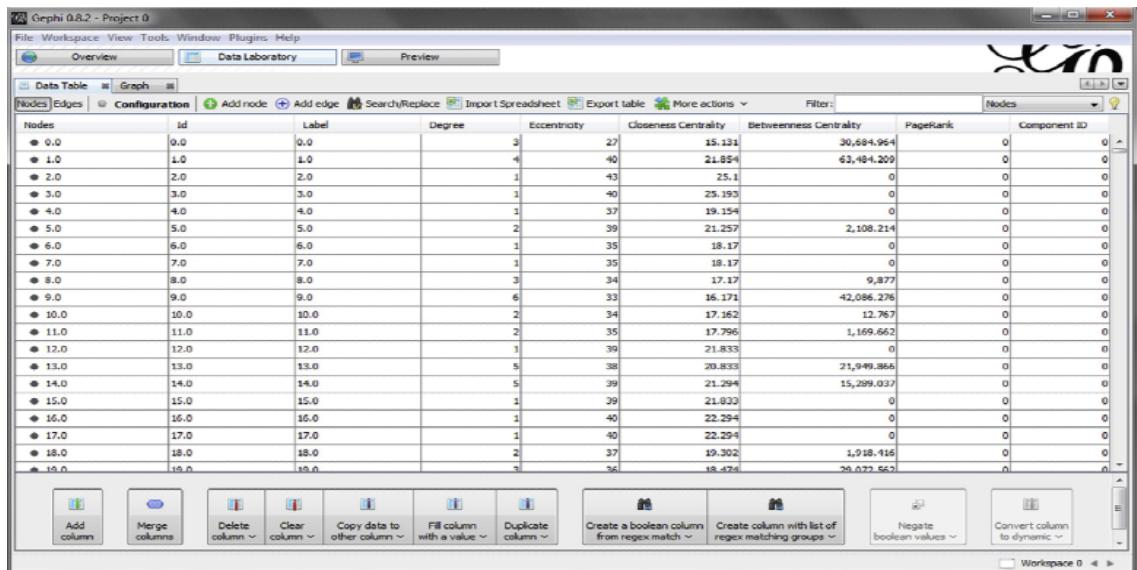
بررسی اجمالی Gephi

زبانه Overview اطلاعات پایه‌ای در مورد شبکه ارائه می‌دهد و شبکه را نمایش می‌دهد. این ابزار عمدتاً به سه بخش تقسیم می‌شود. پانل سمت چپ شامل بخش‌هایی است که اجازه می‌دهد پارسیشن‌بندی و رتبه‌بندی گره‌ها و لبه‌ها و طرح‌بندی‌های مختلف را برای شبکه بر اساس الگوریتم‌های مختلف انجام دهیم. بخش وسط شامل فضایی است که شبکه را نمایش می‌دهد و ابزاری برای کار با گراف است. بخش‌های سمت راست حاوی اطلاعات در مورد شبکه مانند تعداد گره‌ها و لبه‌ها و عملیات مانند محاسبه درجه، تراکم و سایر آمار شبکه است.



DATA LABORATORY

در زبانه Data Laboratory می‌توانید با داده‌های خود در فرم خام کار کنید. در این برگه، اشخاص و روابط آن‌ها در قالب یک صفحه گسترده نمایش داده می‌شوند. در اینجا می‌توانیم گره‌های جدید و لبه‌ها را اضافه، آن‌ها را جستجو و داده‌ها را وارد و یا صادر کنیم. ما همچنین می‌توانیم روی ستون‌ها کار کنیم و آن‌ها را حذف، کپی و غیره کنیم. همچنین داده‌ها موجود می‌توانند بر اساس پارامترهای مختلف با کلیک روی نام ردیف مرتب شوند.



The screenshot shows the Gephi software interface. At the top, there's a menu bar with File, Workspace, View, Tools, Window, Plugins, and Help. Below the menu is a toolbar with icons for Overview, Data Laboratory, Preview, Add node, Add edge, Search/Replace, Import Spreadsheet, Export table, and More actions. A filter bar is also present. The main area displays a network graph with nodes and edges. To the right of the graph is a detailed table of node statistics. The table has columns for Nodes, Id, Label, Degree, Eccentricity, Closeness Centrality, Betweenness Centrality, PageRank, and Component ID. The data shows various nodes with their respective values for each metric.

Nodes	Id	Label	Degree	Eccentricity	Closeness Centrality	Betweenness Centrality	PageRank	Component ID
0.0	0.0	0.0	3	27	15.131	30,684.964	0	0
1.0	1.0	1.0	4	40	21.854	63,484.209	0	0
2.0	2.0	2.0	1	43	25.1	0	0	0
3.0	3.0	3.0	1	40	25.193	0	0	0
4.0	4.0	4.0	1	37	19.154	0	0	0
5.0	5.0	5.0	2	39	21.257	2,108.214	0	0
6.0	6.0	6.0	1	35	18.17	0	0	0
7.0	7.0	7.0	1	35	18.17	0	0	0
8.0	8.0	8.0	3	34	17.17	9,877	0	0
9.0	9.0	9.0	6	33	16.171	42,086.276	0	0
10.0	10.0	10.0	2	34	17.162	12.767	0	0
11.0	11.0	11.0	2	35	17.796	1,169.662	0	0
12.0	12.0	12.0	1	39	21.833	0	0	0
13.0	13.0	13.0	5	38	20.833	21,949.866	0	0
14.0	14.0	14.0	5	39	21.294	15,299.037	0	0
15.0	15.0	15.0	1	39	21.933	0	0	0
16.0	16.0	16.0	1	40	22.294	0	0	0
17.0	17.0	17.0	1	40	22.294	0	0	0
18.0	18.0	18.0	2	37	19.302	1,918.416	0	0
19.0	19.0	19.0	1	36	18.476	26,577.562	0	0

Preview

در زبانه Preview می‌توانیم تنظیمات مختلف مربوط به خواص گراف شبکه مانند ضخامت لبه‌ها، رنگ گره‌ها، عرض مرزها و غیره را تغییر دهیم. این به ما کمک می‌کند که مقادیر مختلف پارامترهای مختلف را تعیین کنیم تا بتوانیم با تمایز آن‌ها را بر اساس خواص مختلف گراف، قابل تشخیص کنیم. تنظیمات را می‌توان در پنل سمت چپ انجام داد و تغییرات در بقیه قسمت‌های موجود برای پیش‌نمایش نشان داده می‌شوند.

ابزارهای دیگری برای SNA وجود دارد که برخی از آن‌ها عبارت‌اند از:

SocNetV (<http://socnetv.sourceforge.net/>)

NodeXL (<http://nodexl.codeplex.com/>)

EgoNet (<http://sourceforge.net/projects/egonet/>)

اصطلاح شبکه در اینجا کاملاً مشابه استفاده از آن در علوم رایانه یا علوم دیگر از قبیل ریاضی یا فیزیک است. تعریف اصطلاحات ممکن است در زمینه‌های مختلف مطالعه تغییر کنند، اما شبکه اتصال موجودیت‌های مختلف با روابط است. برای ایجاد یک رویکرد ساده‌تر به شبکه ما از گره برای موجودیت‌ها لبه برای رابطه استفاده خواهیم کرد.

برای ایجاد یک شبکه معنی‌دار و با درک آسان و نمایش گرافیکی، باید بر روی بعضی از نقاط تمرکز کنیم مانند برجسته کردن گره‌ها و لبه‌های به کار رفته و مهم، حذف گره‌ها بدون داده یا لبه‌ها، گروه‌های مشابه گره‌ها بر

اساس موقعیت جغرافیایی، جامعه یا هر چیز دیگری که به‌طور گسترده‌ای مربوط به آن هستند. این‌ها شیوه‌های اولیه یا نکات یاد شده در هنگام ایجاد یک شبکه معنی دار و دارای درک آسان است.

اجزاء یک شبکه مانند لبه و گره دارای مشخصه‌های خاصی هستند که بر اساس آن می‌توانیم یک شبکه را ایجاد کنیم. این ویژگی‌ها در درک شبکه و اجزای آن نقش مهمی ایفا می‌کنند. بیایید با یک گره شروع کنیم.

همان‌طور که قبلاً مورد بحث قرار گرفت، گره دارای پارامتری به نام درجه است. درجه را می‌توان برای محاسبه احتمال این گره استفاده کرد و چیزی نیست جز تعداد لبه‌ایی که به گره متصل هستند. اگر چه جهت دار بودن و یا نبودن لبه‌ها مهم است. بیایید بگوییم تعداد لبه‌ای هدایت شده به سمت گره X، پنج است و لبه‌ای هدایت شده از X، دو است. پس درجه X برابر ۷ است، زیرا ترکیبی از (2) in-grade (5) + out-grade است.

صفات گره‌ها^۱

هر گره در یک شبکه می‌تواند طیفی از صفات را داشته باشد که می‌تواند برای تشخیص بعضی از خواص یک گره استفاده شود. این صفات می‌توانند در ساده‌ترین حالت در فرم باینری باشد مانند بله / خیر و یا متأهل / مجرد باشند.

در صورتی که گزینه‌های موجود بیش از دو باشند صفات را می‌توان به صورت دسته‌ای تنظیم کرد مانند اگر ما می‌خواهیم عنصری را به عنوان یک گره به نام رابطه تعریف کنیم. به عنوان مثال: ۱. دوست، ۲. خانواده، ۳. همکار.

مقادیر صفات می‌توانند به صورت پیوسته باشند مانند بر اساس برخی از اطلاعات مانند تاریخ تولد، موقعیت شغلی و غیره.

صفات لبه‌ها^۲

DIRECTION

بر اساس جهت، می‌توان دو نوع عمدۀ لبه یافت.

1. Directed edges
2. Undirected edges

¹ NODE ATTRIBUTES

² EDGE ATTRIBUTES

Directed edges

لبهای جهت دار لبهایی با ارتباط دو طرفه هستند. بهترین مثال لبه $2 \rightarrow X$ است. در اینجا X در یک جهت مرتبط با 2 است. ما می‌توانیم بگوییم 2 فرزند X .

Undirected edges

این می‌تواند برای ایجاد روابط متقابل، مانند $2 \rightarrow \leftarrow X$ یا $2-X$ استفاده شود. این رابطه می‌تواند هر چیزی مانند X و 2 دوست یا همکلاس و یا همکار می‌باشد.

TYPE

این می‌تواند نوع رابطه‌ای باشد که در یک گروه قرار می‌گیرد. فرض کنید که گره‌ها و لبهای مختلفی وجود دارد اما اگر برخی از لبه‌ها با مشابه باشند، در یک گروه قرار می‌گیرند و ما می‌توانیم به راحتی آن‌ها را تشخیص دهیم. TYPE می‌تواند هر چیزی مانند دوستان، همکار، نسبی و غیره باشد و نقش مهمی در تمایز لبهای مختلف دارد.

WEIGHT

تعداد اتصالی است که دو گره می‌توانند داشته باشند. به عنوان مثال، اگر $2 \rightarrow \leftarrow X$ با بیش از یک لبه غیرمستقیم و یا مستقیم به هم متصل شوند، وزن آن لبه آن عدد است. به عنوان مثال، X با 2 در پنج راه ارتباط دارد و سپس وزن آن لبه 5 است. ما می‌توانیم به سادگی پنج لبه را بین این دو گره ترسیم کنیم یا می‌توانیم بین آن‌ها لبه عمیق‌تری بسازیم تا بتوانیم در کمک کنیم که این دو گره شامل یک لبه با وزن بالاتر هستند.

وزن نیز می‌تواند دو نوع باشد:

1. Positive
2. Negative

Positive weight

بر اساس احتمال یک رابطه است. برای درک آسان می‌توانیم درباره یک سیاستمدار صحبت کنیم. افراد زیادی هستند که دوست دارند یک سیاستمدار خاص باشند؛ بنابراین رابطه‌ای که با آن‌ها برقرار می‌شود، وزن مثبت است.

Negative weight

همان‌طور که می‌دانیم، منفی بودن یا تنفر یا نامعلوم بودن می‌تواند یک عامل در یک رابطه باشد. این را می‌توان با وزن منفی اندازه‌گیری کرد.

RANKING

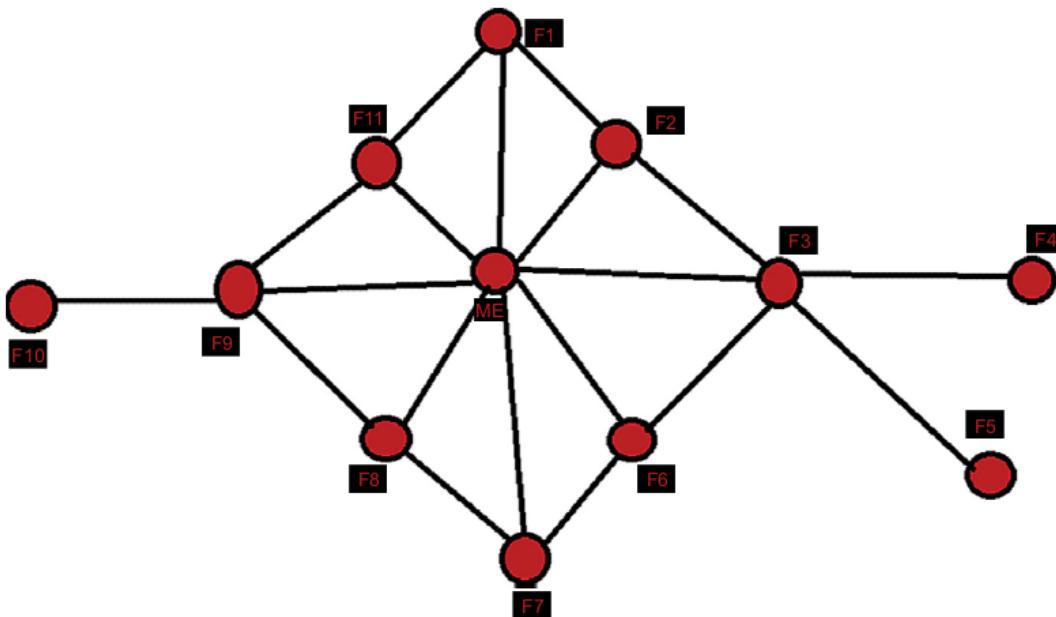
بر اساس اولویت‌های ارتباط بین دو گروه ایجاد شده، لبه‌ها می‌توانند رتبه‌های مختلفی داشته باشند؛ مانند موضوع مورد علاقه اول X ریاضی و موضوع مورد علاقه دوم فیزیک است؛ بنابراین برای جداسازی بین این اولویت‌ها، برای درک آسان در یک شبکه رتبه‌بندی به وجود می‌آید.

BETWEENNESS

سناریوهای خاصی وجود دارد که ما می‌توانیم بینیم که دو گروه مختلف از گروه‌های متصل به یکدیگر توسط یک لبه وجود دارد؛ بنابراین این نوع لبه‌ها یک کیفیت منحصر به فرد را برای ترکیب دو گروه یا مجموعه‌ای از گروه‌ها در نظر می‌گیرند و می‌توانند به عنوان BETWEENNESS نامیده شوند.

بسیاری از ویژگی‌های دیگر نیز وجود دارند. در حال حاضر ما می‌توانیم بگوییم که دانش پایه‌ای در مورد شبکه، اجزای آن و ویژگی‌های آن داریم، به‌طوری که اگر در آینده شانس ایجاد یک شبکه یا درک یک شبکه داده شده را به دست آوریم، می‌توانیم حداقل اصول اولیه آن را به درستی درک کنیم.

اصول اصلی شبکه و اجزای آن در بالا ذکر شد، اما ما هنوز موضوع اصلی SNA را پوشش نداده‌ایم. همان‌طور که قبلًا در این فصل بحث شد، درباره نقشه‌برداری و اندازه‌گیری روابط بین موجودیت‌های مختلف است. این اشخاص می‌توانند افراد، گروه‌ها، سازمان‌ها، دستگاه‌ها، برنامه‌ها و دیگر موجودیت‌های مرتبط باشند. گروه‌ها در شبکه معمولاً افراد هستند، اما می‌توان آن‌ها را بر اساس آنچه در شبکه می‌بینیم، در نظر بگیریم، در حالی که لینک‌ها نشان‌دهنده روابط یا جریان‌های بین گروه‌ها هستند. SNA هر دو تجزیه و تحلیل ریاضی و گرافیکی روابط را ارائه می‌دهد که با استفاده از آن یک تحلیلگر می‌تواند نتیجه‌گیری‌های متعددی بگیرد. صفاتی که به اجرا در می‌آیند مانند درجه، betweenness و مابقی مورد تحت پوشش قرار گرفته‌اند.



این یک شبکه نمونه از دوستان است که لبها سطح ارتباطات بین هر یک از آنها را تعیین می‌کند. این یک شبکه ساده برای درک جنبه‌های مختلف SNA در مورد چگونگی پیدا کردن اطلاعات مهم مختلف با نگاه کردن به یک شبکه است.

اولین چیزی که ما می‌توانیم به راحتی پیدا کنیم گره فعال در شبکه است. گره فعال یا hub، گره‌ای است که دارای بالاترین درجه لبه است. در این مورد، کاملاً مشخص است که گره "me" بالاترین درجه لبها را دارد و درجه آن ۸ است، می‌توان نتیجه گرفت که گره "me" فعال‌ترین گره است و تقریباً تمام گره‌های دیگر را متصل می‌کند. چیز دیگری که ما می‌توانیم نتیجه گیری کنیم که گره "me" به کسانی که دوست مشترک دارند متصل است. این‌ها بعضی از مفروضاتی هستند که می‌توانند از شبکه استخراج شوند.

دو گره وجود دارد که نقش حیاتی در شبکه ایفا می‌کنند. گره‌های F3 و F9. این دو گره بعضی از گره‌ها را به خوش گره "me" متصل می‌کنند. F3 و F9 تنها نقطه اتصال F4 و F5 و F10 هستند. این دو گره تصمیم می‌گیرند چه اطلاعاتی به خوش ارسال و چه اطلاعاتی دریافت شود. اکنون وقت آن است که از آن استفاده کنید. گره با بالا، تأثیر بیشتری در جریان داده‌ها دارد؛ بنابراین در این مثال گره F3 دارای بالاترین betweenness است با مقدار ۲ است، بنابراین می‌تواند به عنوان قوی‌ترین گره در این شبکه در نظر گرفته شود. به عبارت دیگر می‌تواند یک نقطه شکست برای استحکام گره‌ها باشد که به طور مستقیم در خوش ارتباطی ندارند. به این ترتیب می‌توان نتیجه گرفت که مکان نقش حیاتی در یک شبکه را دارد. این مکان است که می‌تواند یک گره را مهم

کند. گره‌ها همچنین می‌توانند به عنوان گره‌های مرزی^۱ نامیده شوند. همان‌گونه که این گره‌ها دارای ایده‌ها و اطلاعات از هر دو قسمت از شبکه مانند خوش و بخش گسترده می‌باشند، این گره‌ها می‌توانند نوآوران باشند که می‌توانند ایده‌ها و خدمات جدیدی را با ترکیب ایده‌ها از هر دو بخش شبکه‌ای ایجاد کنند.

اگر ما به مرکز گرایی^۲ شبکه نگاه کنیم، می‌توانیم به راحتی ساختار شبکه را در ک کنیم. این اجازه می‌دهد تا ما مکان‌های فردی و اهمیت آن را در ک کنیم. اگر یک شبکه بسیار متراکم باشد و تنها یک نقطه شکست داشته باشد، شبکه را می‌توان به راحتی با غیرفعال کردن آن گره تقسیم کرد؛ بنابراین همیشه خوب نیست است که یک شبکه متراکم باشد. در مورد مثال ما، این یک شبکه کمتر متراکم است. اگرچه ما دارای یک هاب و دو گره betweenness هستیم، اما یک شبکه خوب داریم، زیرا غیرفعال کردن هاب به طور مستقیم بر شبکه اثر نخواهد گذاشت، زیرا هنوز مسیری برای انتقال اطلاعات از یک گره به دیگری وجود دارد. گرچه شکست گره F3 و F9 یک زیر شبکه ایجاد می‌کند، بخش عمدات از این شبکه یا خوش گره "me" تحت تأثیر قرار نخواهد گرفت.

دسترسی شبکه نیز یک موضوع است که در اینجا بحث می‌شود. دسترسی شبکه چیزی جز استفاده از کوتاه‌ترین مسیر است که (به طور کلی با یک گره یا دو گره تفاوت است) آیا یک گره قادر به برقراری ارتباط با هر گره دیگر است یا نه. این را می‌توان به راحتی در سایت محبوب شبکه‌های اجتماعی LinkedIn، در ک کنید. از مفهوم مشابهی برای جستجوی شبکه استفاده می‌کند. اگر بخواهیم با یک فرد خاص ارتباط برقرار کنیم، چه تعداد از اتصالات درجه اول، دوم و سوم را نشان می‌دهد، بنابراین می‌توانیم از هر یک از آن‌ها برای معرفی استفاده کنیم. همان‌طور که در LinkedIn همواره بهتر است از اولین درجه اتصال برای معرفی شدن استفاده کنید زیرا این کوتاه‌ترین مسیر برای رسیدن به یک اتصال است، بنابراین تمام اتصالات مستقیم ما در LinkedIn مهم است. به طور مشابه در مورد این شبکه، همیشه یک مرکز به عنوان یک گره همسایه است. از آنجا که این گره همسایه است که نقش حیاتی در ارتباط دارد. اگر گره همسایگی شما یک مرکز است و به همه متصل است، به همین ترتیب مانند نقش بوقیله او به همه متصل می‌شویم و دسترسی شبکه ما را گسترش می‌دهد. در اینجا در این شبکه جدا از گره F4، F5 و F10 بقیه گره‌ها که تحت خوش گره "me" قرار می‌گیرند، به دلیل گره "me" از شبکه بسیار خوبی برخوردار هستند.

¹ boundary spanners

² centralities

برای دریافت اطلاعات از منابع مختلف، ما باید موقعیتی داشته باشیم که در آن کوتاه‌ترین مسیرهای یک گره واحد را داشته باشیم، زیرا این امر به ما امکان می‌دهد اطلاعات مشابه با دیدگاه‌های مختلف در یک شبکه را دریافت کنیم. این اساساً بستگی به ادغام شبکه دارد. هرگونه اطلاعاتی که در اختیار شما قرار می‌گیرد، باید از طریق گره "me" جریان یابد؛ بنابراین، دیدگاه‌های مختلف در مورد اطلاعات بسیار دشوار خواهد بود. اگر گره‌های F1، F2، F3، F6، F7، F8، F9، F11 به یکدیگر مانند توپولوژی مش پیوندند، بیشتر گره‌ها، مسیرهای کوتاه دیگری را جایگزین می‌کنند.

اغلب اوقات در شبکه توسعه یافته به گره‌هایی مانند F4، F5 و F10 ارزش نمی‌گذاریم. این گره‌ها بخشی از خوشه نیستند و همین امر آن‌ها را بسیار مهم می‌سازد. آن‌ها کسانی هستند که اطلاعات بسیار کم از خوشبندی شبکه دریافت می‌کنند اما از دیدگاه شبکه‌ای دارای ایده‌های تازه هستند. آن‌ها می‌توانند اطلاعات ارزشمند بیرونی را به خوشه ارائه دهند. برای این شبکه ممکن است خارجی باشند اما برای برخی از شبکه‌ها باید محلی باشند و این اطلاعات را می‌توان به خوشه "me" با استفاده از آن‌ها منتقل کرد. این گره‌ها نیز به عنوان گره‌های جانی^۱ نامیده می‌شوند.

یک شبکه هیچ موقع نتیجه یا گزارش نیست. این بیشتر شبیه یک آینه است که چندین چیز را در مورد یک شبکه نشان می‌دهد و همیشه لزوماً خوب نیست؛ بنابراین سعی کنید از اجزای کلیدی شبکه برای درک رفتار شبکه استفاده کنید.

با توجه به موقعیت گره، یک گره به‌طور خاص یا بر عکس کار می‌کند. می‌توانیم گفت که با توجه به نقش گره می‌توان موقعیت خود را در یک مکان خاص در یک شبکه پیدا کرد؛ بنابراین هر دو جهت، موقعیت بر اساس نقش یا نقش بر اساس مکان بسیار مهم‌اند تا یک شبکه را درک کنیم. اکنون اجازه دهید برخی از نقش‌ها را بررسی کنیم و سپس سعی کنیم چندین نقش را در شبکه قبلی بینیم.

نقش بر اساس مکان گره:

Star/Hub

¹ peripheral nodes

استار یک موجودیت است که بسیار مرکزی است. قبلًا ما از اصطلاح هاب برای این گره استفاده کردیم که شامل تعداد زیادی از اتصالات است، این همان است؛ بنابراین ما می‌توانیم از عبارت استار و یا هاب استفاده کنیم، می‌توانیم بینیم که ما یک گره استار داریم که "me" است.

Gatekeeper/Boundary spanners

یک موجودیت که میانجی است و یا می‌تواند کنترل جریان بین یک بخش از شبکه با یکدیگر را انجام دهد، قبلًا ما آن را گره‌های مرزی نام‌گذاری کردیم. در مثال قبلی ما F9 و F3 دروازه‌بان هستند.

Bridge

این تنها لبه است لینک بین دو یا چند گروه است. در مثال قبلی، سه پل وجود داشت:

(1) F9 → F10 (2) F3 → F4 (3) F3 → F5.

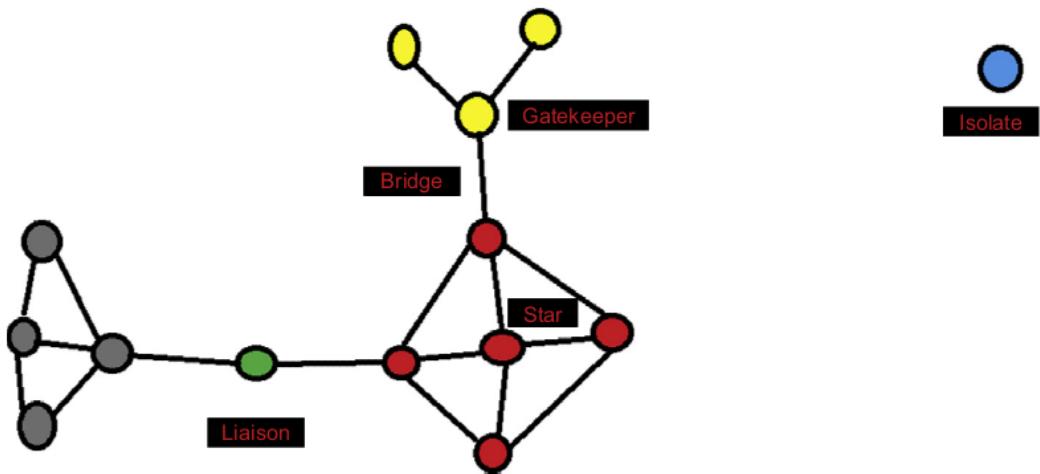
Liaison

موجودیتی‌هایی که دارای پیوندهایی به دو یا چند گروه‌اند که در غیر این صورت نمی‌توانند پیوندی داشته باشند، اما عضو یک گروه نیستند. در مثال قبلی ما، چنین گره‌ای را که در موقعیت ارتباط قرار داشت، ندارد.

Isolate

همان‌طور که از نام آن مشخص است، یک موجودیت جدا است که هیچ ارتباطی با موجودیت‌های دیگر ندارد؛ به‌طور کلی گره بدون linkless یا edgeless. در مثال قبلی ما هیچ گره جداگانه‌ای نداریم.

در اینجا یک شبکه جدید که حاوی تمام نقش‌هاست برای درک آسان، آورده شده است.

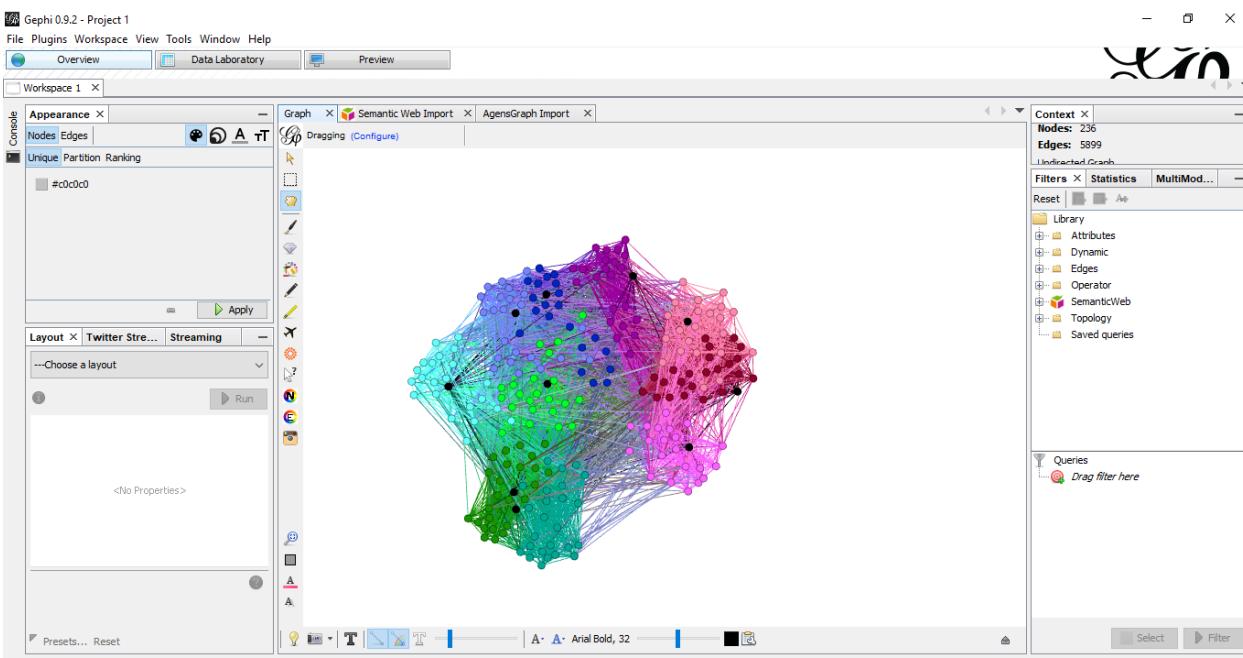


SNA می‌تواند در بسیاری از موارد برای درک جریان اطلاعات مفید باشد؛ ما می‌توانیم از شرایطی مانند پیش‌بینی نتایج نظرسنجی کاربران آنلاین استفاده کنیم یا اینکه چگونه و در چه حد یک اطلاعات در شبکه‌ای از دوستان جریان می‌یابد، درک یک فرهنگ‌سازمانی و حتی حوادث در یک فرایند را پیدا کنید.

برای مثال ساده‌تر، برای استفاده از آن در سناریوی عمومی، می‌توانیم یک شبکه از کاربران توییتر یک جامعه و یا یک سازمان ایجاد کنیم و بینیم چه کسی دنبال چه کسی و چه چیزی است. این به ما کمک می‌کند تا درک کنیم که بازیکنان کلیدی در این ساختار کدامند که بیشترین تأثیر را ایجاد می‌کنند. به طور مشابه ما همچنین می‌توانیم درک کنیم که پیروان و رهبران کدامند. در یک شبکه حرفه‌ای در یک سازمان، می‌توان آن را برای شناسایی افرادی که سلسله مراتب را ایجاد می‌کنند و چگونه می‌توان آن را بهبود بخشد.

به طور مشابه می‌توان آن را برای تجزیه و تحلیل شبکه‌ای از افراد متصل به منظور شناسایی اینکه چگونه یک یماری قابل انتقال در شبکه گسترش می‌یابد و ارتباطات باید قبل از اینکه کل شبکه آلوده شود، شکسته شود. مثال دیگر می‌تواند در شبکه‌ای از رهبران بازار در یک صنعت باشد تا بتواند هویت مشترکان آنها را در آن شبکه مشخص کند.

بسیاری از ویژگی‌ها و توابع که در فصل مورد بحث قرار گرفته‌اند می‌توانند به‌طور خودکار با استفاده از Gephi محاسبه شوند، همچنین این ابزار دارای الگوریتم‌های زیادی است که می‌تواند برای انجام طراحی، شناسایی عناصر کلیدی، پیاده‌سازی فیلترها و انجام سایر عملیات دیگر استفاده شود. همچنین می‌توانید با استفاده از گزینه‌های مختلف پلاگین که در زیر دکمه tools وجود دارد آن را گسترش داد.



SNA توسط سیستم‌های مختلف شبکه‌های اجتماعی و سازمان‌هایی که با مردم ارتباط برقرار می‌کنند استفاده می‌شود؛ به همین ترتیب در بسیاری از حوزه‌های کاربردی که به علم اطلاعات بستگی دارد قابل استفاده است.

ما در این فصل چیز جدیدی آموختیم و می‌توانیم با استفاده از یک شبکه ساده‌تر برای درک آسان هر سیستم پیچیده‌ای در آینده استفاده کنیم. در اینجا ما مبانی مفاهیم SNA را پوشش می‌دهیم. این موضوع کاربردهای بسیار زیادی در زمینه‌های مختلف دارد. هدف ما در اینجا این است که موضوع را معرفی کنیم تا خوانندگان بتوانند با آن آشنا شده و اهمیت آن را درک کنند و از این رو برای استفاده عمیق‌تر آن را در آینده بررسی کنند.

در فصل بعدی در مورد اصول اولیه پایتون یاد خواهیم گرفت. اگرچه اصول برنامه‌نویسی به صورت کامل تحت پوشش قرار می‌گیرند، اما بهتر است قبل از ورود به آن مفاهیم اساسی برنامه‌نویسی را مطالعه کنید.

فصل ۱۳: پایتون

مقدمه

پس از پوشش موضوعات جالب مربوط به استفاده از ابزارهای خودکار مختلف، در این فصل به یادگیری ایجاد برخی از آن‌ها می‌پردازیم. گاهی اوقات نیاز به انجام وظایف خاصی داریم ولی قادر به پیدا کردن ابزارهایی که مورد نیاز است، نیستیم. این زمانی است که ما نیاز به دانش برنامه‌نویسی داریم، به‌طوری که بتوانیم به سرعت کدی را برای انجام عملیات دلخواه ایجاد کنیم. این فصل برای یادگیری اصول زبان برنامه‌نویسی پایتون است. ما متوجه خواهیم شد که چگونه از پایتون استفاده کنیم، اصول اساسی آن چه هستند و پس از آن ابزارهای ساده‌اما مفید را ایجاد خواهیم کرد. توصیه می‌شود، قبل از شروع این فصل برخی از اصطلاحات اصلی دانش برنامه‌نویسی را فرا بگیرید، زیرا ما فقط ملزمات اساسی مربوط به زبان را پوشش می‌دهیم و به‌طور مستقیم به سمت کدنویسی حرکت می‌کنیم. اگرچه نمونه‌هایی که استفاده می‌شود ساده‌اند، اما به عنوان تجربه جدید در برنامه‌نویسی مفیدند.

هر کسی که علاقه‌مند به علوم رایانه‌ای است با مفاهیم برنامه‌نویسی آشنایی دارد. به عبارت ساده، برنامه نویسی فرایند ایجاد برنامه‌ای برای حل یک مشکل است. برای ایجاد برنامه نیاز به یک زبان داریم که با استفاده از آن می‌توانیم دستورالعمل‌هایی را برای رایانه برای انجام کار مشخص، ارائه دهیم. هدف ساده یک برنامه رایانه‌ای این است که یک سری از دستورالعمل‌ها را به‌طور خودکار بسازیم.

برنامه نویسی و اسکریپت نویسی^۱

زبان مورد بحث در این فصل پایتون است که معمولاً به عنوان یک زبان اسکریپتی شناخته می‌شود، بنابراین قبل از هر چیز باید معنی آن را بدانیم. معمولاً کد نوشته شده در یک زبان برنامه‌نویسی به کد ماشین با استفاده از برنامه کامپایلر تبدیل می‌شود تا اجرا شود. برای مثال، کد نوشته شده در زبان C++ برای ایجاد یک executable که می‌تواند در یک سیستم عامل ویندوزی اجرا شود، کامپایل شده است.

برنامه دیگری به نام مترجم وجود دارد که اجازه می‌دهد بدون استفاده از کامپایل، یک کد اجرا شود؛ بنابراین اگر محیط اجرای یک قطعه کد، مترجم باشد، یک اسکریپت است. معمولاً پایتون در چنین شرایطی اجرا می‌شود و از این رو معمولاً زبان برنامه‌نویسی اسکریپتی نامیده می‌شود. این بدان معنا نیست که زبان اسکریپتی را نمی‌توان کامپایل کرد اما به سادگی معمول نیست.

مقدمه پایتون

پایتون یک زبان برنامه‌نویسی سطح بالا است که توسط Guido Van Rossum ایجاد شده که بر خوانایی کد تأکید دارد. پایتون بسیار سریع است و اجازه می‌دهد مشکل با حداقل مقدار کد حل شود و از این رو در میان افرادی که نیاز به ایجاد اسکریپت‌های سریع دارند، مانند تست نفوذگرها، بسیار محبوب است. نسخه‌های مختلف پایتون وجود دارد اما ما بر روی نسخه ۲.۷ در این فصل تمرکز خواهیم کرد. اگر چه آخرین نسخه آن ۳.۴ است، اما اکثر ابزار و کتابخانه‌های پایتون در اینترنت بر اساس نسخه ۲.۷ است و نسخه ۳.x با ماقبل آن سازگار نیست و از این رو از آن استفاده نمی‌کنیم.

دستورالعمل اصلی این فصل این نیست که یک دوره پایتون ایجاد شود که به خودی خود یک کتاب جداگانه نیاز دارد. در اینجا ما سریعاً به اصول اولیه می‌پردازیم و سپس به سمت ایجاد اسکریپت‌های کوچک و مفید برای نیازهای عمومی می‌رویم. هدف این است که با آموزش پایتون، قطعه‌های سریع را ایجاد و یا ابزارهای موجود را سفارشی کنیم. این فصل تلاش می‌کند تا امکان ایجاد برنامه‌های کارآمد را در یک زمان محدود فراهم، ابزارهایی را برای دستیابی به آن‌ها فراهم و سپس آن را در صورت نیاز گسترش دهد.

^۱ PROGRAMMING VERSUS SCRIPTING

جایگزین‌های دیگری برای پایتون وجود دارد که عمدتاً روبي^۱ و پرل يکی از قدیمی‌ترین زبان‌های برنامه‌نویسی است و روبي به طور گسترده‌ای برای توسعه وب (Ruby on Rails) استفاده می‌شود. با این حال پایتون يکی از ساده‌ترین زبان‌ها است که به سرعت در حال ایجاد چیزی با کارایی بالا است. پایتون نیز برای توسعه وب مورد استفاده قرار می‌گیرد.

نصب پایتون

نصب پایتون در ویندوز بسیار ساده است، به سادگی نسخه ۲.۷ از <https://www.python.org/downloads/> و نصب نمایید. پایتون در لینوکس و سایر محیط‌های مشابه از قبل نصب شده است.

اگر چه، لازم نیست اما بسیار توصیه می‌شود که Setuptools و Pip را برای نصب آسان و مدیریت بسته‌های پایتون نصب کنید. جزئیات مربوط به Setuptools و Pip را می‌توان در <https://pypi.python.org/pypi/setuptools> و <https://pypi.python.org/pypi/Pip> ببینید.

اجرای پایتون

ما می‌توانیم پایتون را اساساً به دو روش اجرا کنیم، یکی این است که به طور مستقیم با مترجم ارتباط برقرار کنیم، جایی که دستورات را از طریق تعامل مستقیم ارائه و خروجی آن را می‌بینیم (اگر وجود داشته باشد) و یکی دیگر از طریق اسکریپت‌ها، جایی که کد آن را به فایلی با پسوند py ذخیره کرده و آن را با استفاده از مترجم اجرا می‌کنیم. اگر چه نوشتمن اسکریپت روش بهتری برای نوشتمن یک کد است که می‌تواند بعداً مورد استفاده و اصلاح قرار گیرد اما حالت تعاملی نیز بسیار مفید است. ما به سرعت می‌توانیم نحوه کار کرد یک فرمان و ویژگی‌های آن را بررسی کنیم، ما می‌توانیم به سرعت چیزی را امتحان کنیم و نتایج را ببینیم و می‌توانیم کد را به راحتی تست و اشکال‌زدایی کنیم.

برنامه HELLO WORLD

برای نوشتمن برنامه Hello World معمولی، می‌توانیم با تایپ کردن کلمه Python به مترجم پایتون برویم و کد زیر را بنویسیم.

```
print "Hello World"
```

^۱ Ruby

```
C:\Python27>python
Python 2.7.3 (default, Apr 10 2012, 23:24:47) [MSC v.1500 64 bit (AMD64)] on win
32
Type "help", "copyright", "credits" or "license" for more information.
>>> print "Hello World"
Hello World
>>>
```

برای ایجاد اسکریپت دستور فوق را در یک فایل متنی نوشته و با نام helloworld.py ذخیره کنید. در ویندوز می‌توانیم اسکریپت را به صورت ساده با از دستور خط فرمان و یا با دو بار کلیک کردن روی آن اجرا کنیم. در محیط لینوکس می‌توانیم این اسکریپت را مستقیماً با استفاده از نماد ./ اجرا کنیم، اما برای اولین بار باید دسترسی فایل اجرایی را با استفاده از دستور chmod بالا بیریم.

chmod 755 helloworld.py.

/helloworld.py

اگرچه اجباری نیست، اما خوب است که در اسکریپت خود نماد sheban را تعریف کنید. برای این منظور ما باید خط زیر را در شروع اسکریپت وارد کنیم:

`#!/usr/bin/python`

به سادگی مشخص می‌کند مترجم موردنیاز برای اجرای این فایل کجا است. این تنها در محیط لینوکس پشتیبانی می‌شود، اما وجود آن در کد هیچ‌گونه تغییری در محیط ویندوز ندارد، بنابراین بهتر است آن را وارد کنید تا کد مشابه در هر دو محیط اجرا شود. اگر چندین مفسر در لینوکس نصب شوند، می‌توانیم به راحتی مسیر محیط را به یک مفسر مناسب تغییر دهیم، مثلاً اگر هر دو پایتون ۳.۰ و ۲.۷ نصب شده باشند، می‌توانیم از دستور زیر برای استفاده از ۲.۷ برای اجرای کد استفاده کنیم:

`#!/usr/bin/Python2.7`

IDENTIFIERS

در برنامه‌نویسی، IDENTIFIERS نام‌هایی هستند که برای شناسایی متغیر، تابع، کلاس و سایر اشیاء مشابه استفاده شده در یک برنامه استفاده می‌شود. در پایتون، آن‌ها می‌توانند با یک الفبای یا خط زیر شروع شده و در ادامه الفبا، رقم‌ها باشد. آن‌ها همچنین می‌توانند یک کاراکتری باشند؛ بنابراین ما می‌توانیم IDENTIFIERS را بر طبق آن ایجاد کنیم، به غیر از کلمات خاصی که برای اهداف خاص ذخیره می‌شوند، مثلاً if، try و غیره. پایتون به حروف کوچک و بزرگ حساس است به این معنی که Test و test متفاوت هستند.

انواع داده^۱

پایتون متغیرهای مختلفی دارد، اما با ارزش به آن منتقل می‌شود و نیازی به بیان صریح ندارد. در واقع نوع داده بنام متغیر مرتبط نیست، اما ارزش متغیر به سادگی به آن اشاره می‌کند؛ بنابراین یک متغیر را می‌توان به نوع داده دیگری اختصاص داد پس از آن که قبلاً به نوع داده‌های دیگری اشاره داشته است.

```
C:\>Python27>python
Python 2.7.3 (default, Apr 10 2012, 23:24:47) [MSC v.1500 64 bit (AMD64)] on win
32
Type "help", "copyright", "credits" or "license" for more information.
>>> test=10
>>> test
10
>>> test="This is a test"
>>> test
'This is a test'
>>>
```

انواع داده استفاده شده عبارت‌اند از:

- ↳ Numbers
- ↳ String
- ↳ Lists
- ↳ Tuples
- ↳ Dictionaries

برای نمایش عدد، به سادگی یک متغیر را با مقدار عددی اختصاص داده استفاده کنید، به عنوان مثال:

```
>>>samplenum=10
```

فقط می‌دانیم که انواع مختلفی از عددی مانند float، long و غیره وجود دارد.

برای تعریف یک رشته می‌توانیم از نقل قول (هم‌تکی و هم‌دوتایی) استفاده کنیم، به عنوان مثال:

```
>>>samplestr="This is a string"
>>>samplestr2='This is another string'
```

ما همچنین می‌توانیم هر دو نوع نقل قول را در یک فرم استفاده کنیم. برای ایجاد چند رشته‌ای می‌توانیم نقل قول‌های سه‌گانه را استفاده کنیم.

¹ DATA TYPES

```
>>> tripquot="""This is triple Quotes
... Another line
... Yet another
... And one more"""
>>> tripquot
'This is triple Quotes\nAnother line\nYet another\nAnd one more'
```

ما همچنین می‌توانیم از اپراتور `%` برای استفاده از انواع مختلف داده استفاده کنیم. مقادیر در بعداً به آن‌ها منتقل می‌شوند. `d` برای عدد صحیح است و `s` برای رشته‌ها و `f` برای `float` استفاده می‌شوند.

Example code

```
>>> sample_str="There are total %d number of floors in the %s building"%(4,'xyz')
>>>sample_str
```

There are total 4 number of floors in the xyz buildin

پایتون یک نوع داده جالب را به نام لیست ارائه می‌دهد و با توجه به نام آن لیستی از متغیرهای مختلف است. برای ایجاد یک لیست می‌توانیم از براکت `([])` استفاده کنیم و متغیرها را با کاما جدا می‌کنیم.

```
>>>samplelist=[123, "str", 'xyz', 321, 21.22]
>>>samplelist
[123, "str", 'xyz', 321, 21.22]
>>>samplelist[1]
'str'
```

Tuples مشابه لیست‌ها هستند اما غیرقابل تغییر هستند و با استفاده از پرانتز ایجاد می‌شوند.

```
>>> samplelist=[123, "str", 'xyz', 321, 21.22]
>>> samplelist
[123, 'str', 'xyz', 321, 21.22]
>>> samplelist[1]
'str'
>>> sampletup=(123, "str", 'xyz', 321, 21.22)
>>> sampletup
(123, 'str', 'xyz', 321, 21.22)
>>> sampletup[2]
'xyz'
>>> sampletup[2]=21
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
TypeError: 'tuple' object does not support item assignment
>>> samplelist[2]=21
>>> samplelist[2]
21
```

دیکشنری یکی دیگر از انواع داده جالب است که شامل کلید بالارزش‌های مرتبط با آن‌ها است. کلید باید منحصر به فرد باشد در حالی که ارزش می‌تواند تغییر کند.

```
>>>sampledict={'test1':'123','test2':'234','test3':'345'}
```

```
>>>sampledict['test1']
```

```
'123'
```

```
>>>sampledict['test4']='456'
```

```
>>>sampledict['test3']='333'
```

```
>>>sampledict
```

```
{'test1': '123', 'test2': '234', 'test3': '333', 'test4': '456'}
```

توابع مختلفی که توسط اشیاء مختلف ارائه می‌شوند، می‌توانند به جای نوشتن مجموعه‌ای کامل از کد برای انجام آن در زمان‌های مختلف کمک خوبی باشند. برای پیدا کردن آن‌ها می‌توانیم از `dir` و `help` کمک بگیریم.

```
>>>dir(sampledict)
```

```
>>>help(sampledict)
```

```
>>> dir(sampledict)
['__class__', '__cmp__', '__contains__', '__delattr__', '__delitem__', '__doc__',
 '__eq__', '__format__', '__ge__', '__getattribute__', '__getitem__', '__gt__',
 '__hash__', '__init__', '__iter__', '__le__', '__len__', '__lt__', '__ne__',
 '__new__', '__reduce__', '__reduce_ex__', '__repr__', '__setattr__', '__setitem__',
 '__sizeof__', '__str__', '__subclasshook__', 'clear', 'copy', 'fromkeys', 'get',
 'has_key', 'items', 'iteritems', 'iterkeys', 'itervalues', 'keys', 'pop',
 'popitem', 'setdefault', 'update', 'values', 'viewitems', 'viewkeys', 'viewvalues']

>>> help(sampledict)
Help on dict object:

class dict(object):
    dict() -> new empty dictionary
    dict(mapping) -> new dictionary initialized from a mapping object's
        (key, value) pairs
    dict(iterable) -> new dictionary initialized as if via:
        d = {}
        for k, v in iterable:
            d[k] = v
    dict(**kwargs) -> new dictionary initialized with the name=value pairs
        in the keyword argument list. For example: dict(one=1, two=2)

    Methods defined here:

    __cmp__(...)
        x.__cmp__(y) <==> cmp(x,y)

    __contains__(...)
        D.__contains__(k) -> True if D has a key k, else False

    __delitem__(...)
        x.__delitem__(y) <==> del x[y]

    __eq__(...)
        x.__eq__(y) <==> x==y

    __ge__(...)
        x.__ge__(y) <==> x>=y

    __getattribute__(...)
        x.__getattribute__('name') <==> x.name

    __getitem__(...)
        x.__getitem__(y) <==> x[y]

    __gt__(...)
        x.__gt__(y) <==> x>y

    __init__(...)
        x.__init__(...) initializes x; see help(type(x)) for signature

    __iter__(...)
        x.__iter__() <==> iter(x)
```

ما بعضی از اصول اولیه کار بر روی داده‌ها را نشان دادیم اما عملیات بسیار بیشتری وجود دارد که می‌تواند بر روی

این نوع داده‌ها انجام شود. برخی از آن‌ها در زیر نشان داده شده است:

```
>>>a=12
>>>b=2
>>>a*b
24
>>>a="test"
>>>b="next"
>>>a+b
'test next' >>>lt1=['1','2','3'] >>>lt2=['4','5','6'] >>>lt1+lt2
['1', '2', '3', '4', '5', '6']
```

ما می‌توانیم عملیات مختلف را بر روی این عناصر انجام دهیم. بعضی از نمونه‌ها در زیر نشان داده شده‌اند.

```

>>>a=1
>>>b=2
>>>a+b
3
>>>a="test"
>>>b="string"
>>>a+b
'teststring'
>>>a.upper()
'TEST'
>>>c="This is a string" >>>c.find('ring')
12
>>>c.find('xyz')
-1 >>>sample_list=['qw','er','ty',123] >>>sample_list.append(456) >>>sample_list
['qw', 'er', 'ty', 123, 456]

```

INDENTATION

اجازه دهید به مفهوم `import` پردازیم. پایتون قابلیت خواندن کد را دارد. برخلاف سایر زبان‌ها مانند C++, برآکت ها برای مشخص کردن بلوک‌های کد استفاده نمی‌شود، در حالی که از `indentation` استفاده می‌کند؛ بنابراین هنگام ایجاد یک بلوک از کد، ما باید فضاهای خالی¹ را برای نشان دادن ساختار ارائه دهیم. یک نکته مهم این است که ما می‌توانیم تعداد زیادی از فضاهای خالی¹ را برای دندانه‌دار شدن کد داشته باشیم اما در یک بلوک تمام عبارات باید همان مقدار را داشته باشند. بعضی از `spaces` برای ایجاد فضای خالی استفاده می‌کنند و بعضی از `tab` استفاده می‌کنند، بهتر است فقط از یکی از آن‌ها استفاده کنید. نمونه‌هایی که در فصل بعد ارائه می‌شوند بر این مفهوم کار خواهند کرد و ما از فضاهای خالی استفاده می‌کنیم.

اساسی‌ترین عبارت شرطی `if` است. منطق ساده است، اگر شرط ارائه شده درست باشد این دستور را اجرا کند، در غیر این صورت حرکت خواهد کرد. ساختار اصلی `if` و شرایط مرتبط در زیر نشان داده شده است.

`if condition:`

`then_this_statement elif condition:`

`then_this_statement else:`

¹ whitespaces

this_condition

Example code

```
#!/usr/bin/python  
a=10  
b=12  
c=15  
  
if (a==b):  
    print "a=b"  
  
elif (b==c): print "b=c"  
  
elif (c==a): print "c=a"  
  
else:  
  
    print "none"
```

این را در یک فایل متنی بنویسید و آن را با نام if_con.py ذخیره کنید. این کد هنگامی که در پایتون اجرا می‌شود پاسخ "none" را به وجود می‌آورد. شرایط elif و else هنگام استفاده از عبارت if اجباری نیستند و ما می‌توانیم عبارت‌های elif چندگانه داشته باشیم. به همین ترتیب می‌توانیم if تو در تو داشته باشیم، فقط باید توجهات خاصی در نظر گرفته شود.

if condition:

```
then_this_statement  
if nested_condition:  
    then_this_nested_statement  
else nested-else_condition:  
    then_this_nested-else_statement
```

حلقه while دستور بعدی است. در اینجا ما شرط را ارائه می‌دهیم و حلقه اجرا خواهد شد تا این شرایط درست باشد. ساختار حلقه while در زیر نشان داده شده است.

```
while this_condition_statement_is-true: run_this_statement  
run_this_statement
```

Example code

```
#!/usr/bin/python a=10
c=15
while (a<c):
print a
a=a+1
```

Output

```
10
11
12
13
14
```

ما همچنین می‌توانیم دستور `break` و `continue` را برای کنترل جریان حلقه استفاده کنیم. `break` برای خارج شدن از حلقه فعلی مورد استفاده قرار می‌گیرد و دستور `continue` برای انتقال کنترل به شروع حلقه استفاده می‌شود. یک دستور جالب دیگر به نام `pass` وجود دارد که هیچ کاری را انجام نمی‌دهد، به عنوان یک حفره یا سوراخ کننده^۱ استفاده می‌شود.

یکی دیگر از عبارات شرطی مفید برای حلقه، `for` است. با استفاده از آن ما می‌توانیم به تعداد اقلام موجود در یک شی از قبیل یک لیست، تکرار کنیم.

Example code

```
#!/usr/bin/python
sample_tup=('23','test',12,'w2')
for items in sample_tup:
print items
```

Output

```
123
Test
12
```

¹ placeholder

w2

ما به سادگی می‌توانیم مقادیر فردی را در نمونه `sample_tup` مرتب کنیم و آن‌ها را در داخل آیتم‌های متغیر قرار داده و چاپ کنیم.

Example code

```
#!/usr/bin/python  
  
str="String"  
  
for items in str:  
    print items
```

Output

```
S  
T  
R  
I  
N  
G
```

ما همچنین می‌توانیم از ویژگی‌های اشیاء (از طریق `dir` و `help`) برای تکرار هدف استفاده کنیم. همانند ما همچنین می‌توانیم از عبارت `break` و `continue` در `for` استفاده کنیم.

ماژول‌ها^۱

گاهی اوقات نیاز به استفاده مجدد از کد یا مدیریت آن بر اساس نیاز وجود دارد، این است که در آن ماژول‌ها به کمک می‌آیند. اگر اجزای متعددی از یک کد وجود داشته که در بعضی جاهای دیگر نیز مورد نیاز هستند، بنابراین به جای اینکه این اجزاء را دوباره بسازیم، می‌توانیم آن‌ها را به‌طور جداگانه ایجاد و ذخیره کنیم و آن‌ها را در صورت لزوم فراخوانی کنیم. به عنوان مثال، ایجاد یک برنامه برای یک خودرو سواری و دیگری برای کامیون، هر دو اجزای مشترک مانند ترمز، شتاب دهنده و غیره را دارند، بنابراین ما این اجزاء را یک‌بار به‌سادگی کد نویسی می‌کنیم. ماژول در سازماندهی و مدیریت کد بسیار مفید است.

¹ MODULES

ماژول‌ها می‌توانند متغیرها، توابع و کلاس‌ها را تعریف کنند. هنگامی که ماژول را ایجاد می‌کنیم و آن‌ها را در فضاهای جداگانه ذخیره می‌کنیم، می‌توانیم آن‌ها را به کد وارد و از ویژگی‌های آن‌ها استفاده کنیم.

Example code

```
#!/usr/bin/python
```

```
y="Module String"
```

ماژول را به نام `x.py` ذخیره کنید. یک فایل دیگر به نام `mod.py` ایجاد کنید و کد زیر را در آن ذخیره کنید:

Example code

```
#!/usr/bin/python
```

```
import x
```

```
print x.y
```

Output

```
Module String
```

بنابراین ما به سادگی یک ماژول با یک متغیر ایجاد کردیم، آن را به در کد دیگری نام‌گذاری و از متغیر آن استفاده کردیم. با استفاده از ماژول‌ها می‌توانیم برنامه‌های پیچیده‌ای را بدون ایجاد تمام کد در یک فایل واحد ایجاد کنیم. ما همچنین می‌توانیم یک ماژول را با استفاده از دستور زیر صدا بزنیم:

“`from module_name import desired_portion`”.

توابع^۱

توابع برای گروه‌بندی یک مجموعه از کد به عنوان یک قابلیت واحد کمک می‌کند که در کدهایی با تعداد زیادی خط مفید است. تابع با کلیدواژه `def` شروع می‌شود و به دنبال آن نام تابع و سپس درون پرانتز آن آرگومان‌ها قرار می‌گیرند و سپس کولون. تابع همچنین شامل یک عبارت بازگشتی برای خاتمه دادن به آن و ارسال مقادیر بازگشتی هستند (می‌توانند `null` باشند). برای صدای زدن یک تابع می‌توان نام آن را همراه مقادیر مورد نظر (داخل پرانتز) استفاده کنیم.

^۱ Function

Example code

```
#!/usr/bin/python

def simplefunc(atr_arg):
    print "Print me first"
    print atr_arg
    return
str="Sample String" simplefunc(str)
```

Output

Print me first

Sample String

CLASSES

با استفاده از کلاس‌ها می‌توانیم گروه‌های مختلف را دسته‌بندی کنیم. برای ایجاد یک کلاس مانند کلمه کلیدی `class` به دنبال یک نام برای کلاس و سپس یک کولون شروع کنیم.

Example code

```
#!/usr/bin/python

class sample_class:
    def __init__(self, classarg):
        self.cla=classarg
    def firstfunc(self):
        print "First Function" return self.cla+" Return"
    def secfunc(self):
        print "Second Function" return self.cla+" Return"
classobj=sample_class("Argument") print classobj.firstfunc()
print classobj.secfunc()
```

Output

First Function Argument Return Second Function Argument Return

در اینجا تابع `__init__` سازنده کلاس و اولین تابع است که در کلاس اجرا می‌شود. متغیر `classobj` شیء کلاس `sample_class` است و با استفاده از آن می‌توانیم با اشیاء درون کلاس ارتباط برقرار کنیم. همان‌طور که

قبل‌آب‌حث کردیم می‌توانیم این را به عنوان یک ماثول ایجاد و آن را درون یک برنامه دیگر قرار دهیم. اجازه دهید مثال دیگری را از صدا کردن ماثول‌ها بینیم.

Example code

```
#!/usr/bin/python

class sample_class:

def __init__(self, classarg):
    self.cla=classarg

def firstfunc(self):
    print "First Function" return self.cla+" Return"

def secfunc(self):
    print "Second Function" return self.cla+" Return"

classobj=sample_class("Argument")
```

این فایل به نام mod.py ذخیره می‌شود و یک فایل دیگر آن را به عنوان یک ماثول صدا می‌زند:

Example code

```
#!/usr/bin/python

from mod import *

print classobj.firstfunc()
```

Output

First Function

Argument

در پایتون ما می‌توانیم دایرکتوری از ماثول‌ها را برای سازماندهی بهتر از طریق بسته‌ها ایجاد کنیم. آن‌ها ساختار سلسله مراتبی هستند و می‌توانند شامل ماثول‌ها و زیر بسته‌ها باشند.

کار با فایل‌ها

گاهی اوقات نیاز به ذخیره یا بازیابی داده‌ها از فایل‌ها وجود دارد و ما یاد خواهیم گرفت که چگونه با فایلی در پایتون کار کنیم.

اول از همه، برای باز کردن یک فایل، ما باید یک شیء را برای استفاده از تابع باز کنیم:

```
>>>sample_file=open('text.txt','w')
```

در اینجا نام sample_file یک شیء است و با استفاده از تابع open باز می‌شود. اگر فایلی با نام text.txt قبلاً وجود نداشته باشد، ایجاد خواهد شد و اگر در حال حاضر وجود داشته باشد، آن را رونویسی خواهد کرد. بخش آخر در داخل پرانتز حالت را توصیف می‌کند، در اینجا w است که به معنی حالت نوشتن است. بعضی دیگر از حالت‌های معمول استفاده شده برای خواندن r، برای افزودن a، برای خواندن و نوشتن بدون نوشتن مجدد + و برای خواندن و نوشتن با نوشتن مجدد w+ است.

حالا ما یک شی را ایجاد کرده‌ایم، بگذارید پیش برویم و برخی از داده‌ها را به فایل ارسال کنیم.

```
>>>sample_file("test data")
```

ما با نوشتن داده‌ها در فایل را انجام می‌دهیم و می‌توانیم آن را ببینیم:

```
>>>sample_file.close()
```

اکنون برای خواندن فایل می‌توانیم موارد زیر را انجام دهیم:

```
>>>sample_file=open('text.txt','r')
```

```
>>>sample_file.read()
```

'test data'

```
>>>sample_file.close()
```

به طور مشابه می‌توانیم داده‌ها را به فایل‌ها با استفاده از حالت a و تابع read اضافه کنیم. پایتون دارای چندین درج و همچنین مازول‌های شخص ثالث و بسته‌های است که بسیار مفید هستند. برای نوشتن کد خاص با استفاده از پایتون بهتر است ابتدا مازول‌های موجود را جستجو کنیم. این موجب صرفه‌جویی در زمان با نوشتن مقدار زیادی کد از طریق وارد کردن مازول‌ها و استفاده از توابع موجود است. اجازه دهید برخی از این‌ها را بررسی کنیم.

Sys

همان‌طور که در فایل راهنمای آن توضیح داده شده است، این مازول امکان دسترسی به بعضی از اشیاء که توسط مترجم و توابع مورد استفاده و نگهداری شده است ارتباط برقرار می‌کند. برای استفاده از آن ما آن را به برنامه وارد می‌کنیم.

```
import sys
```

برخی از ویژگی‌های مفید ارائه شده توسط آن `version`, `stdin`, `stdout`, `args`, `exit()` و غیره هستند.

Re

بسیاری از ما نیاز به انجام تطبیق الگو برای استخراج اطلاعات مربوطه از مقدار زیادی از آن داریم. این است که عبارات منظم مفید هستند. پایتون مژول `re` را برای انجام چنین عملیاتی فراهم می‌کند.

```
import re
```

Os

ماژول `os` در پایتون اجازه می‌دهد تا ویژگی‌های وابسته به سیستم عامل را انجام دهد.

```
import os
```

برخی از کاربردهای نمونه آن برای ایجاد دایرکتوری با استفاده از تابع `mkdir`, تغییر نام پرونده با استفاده از تابع `rename`, از بین بردن یک فرآیند با استفاده از تابع `kill` و نمایش لیست ورودی‌ها در یک دایرکتوری با استفاده از `function listdir` هستند.

Urllib2

این مژول اجازه می‌دهد تا عملیات مرتبط با URL مانند باز کردن یک صفحه وب را انجام دهد. هنگام کار با برنامه‌های کاربردی وب بسیار مفید است.

```
import urllib2
```

بسیاری از مژول‌های مفید دیگر مانند Scapy (network), Scrapy (web scraping), nose (testing), mechanize (stateful web browsing) و دیگر مواردی هستند که مقدار زیادی از قابلیت‌ها را در دامنه خود ارائه می‌دهند. برخی از مژول‌ها داخلی هستند و بعضی از آن‌ها باید جداگانه نصب شوند.

ورودی کاربر^۱

بعضی از برنامه‌ها نیاز به ورودی کاربر دارند. در اینجا دو روش برای انجام این کار وجود دارد: با استفاده از ماثول Sys ما می‌توانیم ورودی کاربر را از خط فرمان انجام دهیم.

Example code

```
#!/usr/bin/python

import sys

a=sys.

argv[1]

print a

print a*4

a=int(a)

print a

print a*4
```

این را به عنوان usrinp.py ذخیره کنید و آرگومان خط فرمان را وارد کنید.

C:\Python27>usrinp.py 2

Output

```
2
2222
2
8
```

یک لیست است که ورودی‌های خط فرمان را دریافت می‌کند که در آن شاخص `*` برای رزرو شده است. ما همچنین می‌توانیم مقادیر متعدد را منتقل کنیم و با تغییر مقدار index از argv آن را تکرار کنیم. در اینجا ما همچنین یک تبدیل نوع ساده (رشته به عدد صحیح) را نشان دادیم.

یکی دیگر از روش‌های ورودی در زمان اجرا است، این را می‌توان با استفاده از `raw_input` انجام داد.

Example code

^۱ USER INPUT

```
#!/usr/bin/python  
  
import sys  
  
a=raw_input("Enter something: ")  
  
print a*4
```

هنگام اجرای این کد، پیام "Enter something: " چاپ شده که و منتظر ورودی برای تولید پاسخ می‌ماند. برای مقدار ورودی a خروجی aaaa را تولید می‌کند.

اشتباهات رایج

برخی از اشتباهات رایج در هنگام اجرای کد پایتون به شرح زیر است.

Indentation

همان‌طور که در مثال‌های بالا نشان داده شده است، پایتون برای گروه‌بندی کد از فضای خالی استفاده می‌کند. برخی از space استفاده می‌کنند و بعضی از tab استفاده می‌کنند. هنگام اجرای کد نوشته شده توسط شخص یا اصلاح آن، گاهی اوقات با خطای دندانه‌ای مواجه می‌شویم. برای رفع این خطا، کد را برای دقت مناسب بررسی کنید و موارد را اصلاح کنید؛ همچنین اطمینان حاصل کنید که زبانه‌ها و همچنین فضاهای خالی در کد، از بین نرفته باشد.

Libraries

گاهی اوقات یک کد کاملاً درست وجود دارد، اما با یک خطای کتابخانه‌ای اجرا نمی‌شود. دلیل آن عدم وجود کتابخانه‌ای است که در کد نامیده شده است. اگرچه این یک اشتباه تازه کارها است، گاهی اوقات افراد با تجربه نیز خطا را دقیق را نمی‌خوانند و به دنبال خطا در کد می‌گردند. راه حل ساده نصب کتابخانه موردنیاز است.

Interpreter version

گاهی اوقات این کد برای یک نسخه خاص از زبان نوشته شده است و زمانی که در محیطی دیگر اجرا می‌شود، با خطا مواجه می‌شود. برای اصلاح آن، نسخه موردنیاز را نصب کنید و آن را در کد همان‌طور که قبلًا در این فصل نشان داده شده است مشخص کنید یا کد را با استفاده از مترجم خاص اجرا کنید. گاهی اوقات کدهای متعددی وجود دارد که نیاز به نسخه‌های مختلف دارند. برای حل این مشکل می‌توان از virtualenv استفاده کرد که

به ما امکان می‌دهد یک محیط مجازی مجزا ایجاد کنیم که در آن می‌توان تمام وابستگی‌ها را برای اجرای کد در برداشته باشد.

Permission

گاهی اوقات مجوزهای فایلی برای اجرای کد به درستی تنظیم نمی‌شوند بنابراین تغییرات با استفاده از chmod انجام می‌شود.

Quotes

هنگام کپی کردن کد از بعضی از منابع مانند اسناد و وبسایت‌ها، تبدیل بین (`) و quote (`') باعث خطای شود. این خطای شناسایی کرده و تغییرات را بر اساس کد انجام دهد.

بنابراین ما مبانی مربوط به زبان را پوشش دادیم، اجازه دهید نمونه‌هایی را بینیم که می‌تواند به ما در درک مفاهیم و کاربرد عملی آن کمک کنند و همچنین به بعضی موضوعاتی که در بالا بحث نشده، معرفی شوند.

همانند shodan که در فصل قبل بحث شد، سرویس دیگری به نام zoomeye وجود دارد. در این مثال ما یک اسکریپت ایجاد می‌کنیم که با استفاده از آن zoomeye را پرس‌وجو م و آدرس IP را از صفحه نتیجه استخراج می‌کنیم. ما باید پرس‌وجو را از خط فرمان وارد کنیم.

برای این کار ابتدا URL را ایجاد می‌کنیم و با ترکیب URL اصلی و عبارت جستجو از طریق خط فرمان آن را کامل می‌کنیم. سپس درخواست را به این آدرس با استفاده از تابع urlopen از ماثول urlib2 ارسال خواهیم کرد. علاوه بر این، صفحه پاسخ را تجزیه می‌کنیم و با استفاده از BeautifulSoup آدرس IP را از آن استخراج می‌کنیم.

```
C:\Python27>zoomeye.py scada
72.151.104.252
71.254.128.29
71.173.17.144
71.2.16.3
70.89.39.181
70.35.179.4
69.230.124.110
69.84.65.21
69.66.105.74
69.66.28.149

C:\Python27>zoomeye.py camera
72.160.160.189
72.160.36.15
72.161.28.32
72.160.160.189
72.160.57.80
72.160.36.15
72.160.11.136
72.169.201.10
72.161.40.71
72.169.203.70
```

```
#!/usr/bin/python

import sys
import urllib2
from bs4 import BeautifulSoup
url="http://www.zoomeye.org/search?q="
term=sys.argv[1]
comurl=url+term
response=urllib2.urlopen(comurl)
soup = BeautifulSoup(response)
for item in soup.findAll("a",{'class':'ip'}):
    print item.string
```

برای مثال بعدی ما یک extension برای Burp Suite ایجاد خواهیم کرد. Burp Suite یک پروکسی کاربردی است که برای ارزیابی امنیتی وب استفاده می‌شود. این ابزار اجازه می‌دهد تا extension ایجاد کنیم که از طریق آن ما می‌توانیم قابلیت‌های آن را گسترش دهیم. برای گسترش ما به سادگی نام میزبان هدف را استخراج خواهیم کرد.

```
#!/usr/bin/python

# A sample burp extension in python (needs jython) which extracts hostname from the request (Target Tab).
from burp import IBurpExtender
from burp import IMenuItemHandler
import re
```

```
import urllib2

class BurpExtender(IBurpExtender):

def registerExtenderCallbacks(self, callbacks): self.mCallbacks = callbacks
self.mCallbacks.registerMenuItem("Sample Extension", hostnamefunc())

class hostnamefunc(IMenuItemHandler):

def menuItemClicked(self, menuItemCaption, messageInfo):
print "--- Hostname Extract ---"
if messageInfo:
request1=HttpRequest(messageInfo[0].getRequest())
req=request1.request
host=req[1]
print host
print "DONE"

class HttpRequest:

def __init__(self, request):
self.request=request.tostring().splitlines()
```

برای اینکه این فرمت را اجرا کنیم، ابتدا باید Jython را نصب کنیم و آن را در زیر زبانه options در extender قرار دهیم. پس از انجام این کار می توانیم Extension مان را در زبانه Extensions در برنامه extender اضافه کنیم. برای استفاده از Extension فقط باید بر روی یک دامنه هدف تحت زبانه target کلیک راست و بر روی Extension در منوی راست کلیک کنید، نتیجه در Extensions in tab extender نشان داده می شود. مثال ساده است برای نمایش یک افزونه با استفاده از پایتون، ما می توانیم آن را با انجام سایر عملیات بر روی نام میزبان افزایش دهیم.

MALTEGO TRANSFORMS

در فصل قبلی در مورد Maltego که یک ابزار ساده و مؤثر در جمع آوری اطلاعات منبع باز است (OSINT) بحث کردیم. ما یاد گرفتیم که چگونه از آن استفاده کنیم، چه ویژگی هایی را ارائه می دهد، چه عناصری دارد و غیره. باید از دانش پایتون که به دست آوردیم برای گسترش این چارچوب استفاده کنیم. همان طور که در فصل قبلی ذکر شد، قدرت transform Maltego در های آن قرار دارد. برای فراخوان سریع یک transform، اساساً تکه ای از کد نیاز است که یک نهاد (یا یک گروه از نهادها) را به عنوان ورودی در اختیار گرفته و داده ها را به صورت موجودیت

(یا نهادها) بر اساس رابطه استخراج کند. Maltego تغییرات داخلی زیادی را ایجاد و به روز رسانی چارچوب را انجام می‌دهد، اما همچنین اجازه می‌دهد تا موارد جدید ایجاد و از آن‌ها استفاده کنند، این امر می‌تواند بسیار مفید باشد، زمانی که نیازهای خاصی داریم.

قبل از هر چیز نیاز به نصب کتابخانه پایتونی MaltegoTransform ایجاد شده توسط Andrew MacPherson وجود دارد. این کتابخانه را می‌توانید از صفحه https://www.paterva.com/web6/documentation/develo_per-local.php دانلود کنید. برخی از نمونه‌های transform‌های ایجاد شده با استفاده از این کتابخانه نیز در پایین صفحه وجود دارد. هنگامی که کتابخانه را اضافه کردیم، آماده هستیم که اولین transform را ایجاد کنیم.

برای ایجاد هر برنامه ابتدا باید یک دستور کار داشته باشیم؛ بنابراین ابتدا چیزی را مشخص کنیم که در طول کار بر OSINT مفید خواهد بود. یک سرویس به نام (<https://haveibeenpwned.com>) HavelBeenPwned ایجاد شده توسط Troy Hunt وجود دارد که به کاربران اجازه می‌دهد تا بررسی کنند که آیا حساب آن‌ها به خطر افتاده است یا خیر. همچنین یک رابط برنامه‌نویسی کاربردی (API) فراهم می‌کند که با استفاده از آن می‌توانیم همان عملکرد را انجام دهیم. ما از API V1 استفاده خواهیم کرد (<https://haveibeenpwned.com/API/v1>) و یک آدرس ایمیل برای بررسی اینکه آیا ایمیل ارائه شده ما با حسابی مرتبط است، ارائه می‌دهیم.

برای استفاده از API فقط نیاز به ارسال درخواست GET به سرویس داریم که در شکل زیر نشان داده شده است و پاسخ JSON برای نشان دادن نام وب‌سایت را فراهم می‌کند.

<https://haveibeenpwned.com/api/breachedaccount/{account}>

ابتدا مسیر مترجم را مشخص کنید:

```
#!/usr/bin/python
```

ما باید کتابخانه MaltegoTransform را وارد کنیم:

```
from MaltegoTransform import *
```

بعد از وارد کردن کتابخانه اصلی، باید برخی از کتابخانه‌های دیگر را که موردنیاز است وارد کنیم. کتابخانه sys برای ورودی کاربر و urllib2 برای درخواست GET است.

```
import sys  
import urllib2
```

پس از وارد شدن تمام کتابخانه‌های موردنیاز، ما باید تابع () MaltegoTransform را به یک متغیر اختصاص دهیم و ورودی کاربر (آدرس ایمیل) را از رابط Maltego به آن منتقل کنیم.

```
mt = MaltegoTransform()  
mt.parseArguments(sys.argv)
```

اکنون می‌توانیم مقدار ایمیل را به یک متغیر منتقل کنیم تا بتوانیم آن را برای ایجاد URL موردنیاز برای ارسال درخواست GET استفاده کنیم.

```
email=mt.getValue()
```

باید یک متغیر ایجاد کنیم و URL پایه را در آن ذخیره کنیم.

```
hibp="https://haveibeenpwned.com/api/breachedaccount/"
```

اکنون که دو قسمت URL را داریم، می‌توانیم به راحتی آن‌ها را برای ایجاد URL کامل تر کیم.

```
getrequrl=hibp+email
```

باید درخواست GET را با استفاده از تابع urlopen در کتابخانه urllib2 بفرستیم و پاسخ را در یک متغیر ذخیره کنیم. حالا باید یک حلقه را اجرا کنیم تا مقادیر ذخیره شده در متغیر response را به متغیر برای Transform اضافه کنیم.

```
try:
```

```
    response = urllib2.urlopen(getrequrl)  
    for rep in response:  
        mt.addEntity("maltego.Phrase","Pwned at " + rep)  
    except: print ""
```

در این مرحله باید خروجی متغیر را بازگردانیم.

```
mt.returnoutput()
```

حالا به سادگی این را به عنوان emailhibp.py ذخیره کنید.

```
#!/usr/bin/python

from MaltegoTransform import *
import sys
import urllib2

mt = MaltegoTransform() mt.parseArguments(sys.argv)
email=mt.getValue() hibp="https://haveibeenpwned.com/api/breachedaccount/"

getrequrl=hibp+email

try:
    response = urllib2.urlopen(getrequrl)

for rep in response:
    mt.addEntity("maltego.Phrase","Pwned at " + rep)

except: print ""

mt.returnoutput()
```

اکنون برای بررسی اینکه کد ما به درستی اجرا می‌شود، فقط باید این برنامه را در ترمینال اجرا و آدرس ایمیل را به عنوان یک آرگومان خط فرمان وارد کنیم.

مثال:

```
./emailhibp.py foo@bar.com
```

یا:

```
python./emailhibp.py foo@bar.com
```

```
C:\Python27>emailhibp.py foo@bar.com
<MaltegoMessage>
<MaltegoTransformResponseMessage>
<Entities>
<Entity Type="maltego.Phrase">
<Value>Pwned at ["Adobe", "Gawker", "Stratfor"]</Value>
<Weight>100</Weight>
</Entity>
</Entities>
<UIMessages>
</UIMessages>
</MaltegoTransformResponseMessage>
</MaltegoMessage>
```

ما می‌توانیم بینیم که پاسخ، یک خروجی XML است و حاوی رشته زیر است:

"Pwned at ["Adobe", "Gawker", "Stratfor"]"

این به این معنی است که کد ما به درستی کار می‌کند و می‌توانیم از آن به عنوان یک Transform استفاده کنیم. Maltego نتیجه XML را می‌گیرد و آن‌ها تجزیه می‌کند تا یک خروجی ایجاد کند. اکنون گام بعدی ما این است که این را به عنوان یک Transform در Maltego ثبت کنیم.

زیر زبانه manage بر روی دکمه Local Transform Setup کلیک کنید تا Local Transform را راهاندازی کنید. این وایزارد به ما کمک می‌کند تا Transform ما را ثبت کنیم و در نمونه‌های Maltego قرار گیرد.

در name field Transform نام را وارد کرده و کلید tab را برای ایجاد یک Transform ID به صورت خودکار فشار دهید. اکنون توضیح کوچکی برای تبدیل در زمینه توصیف و نام نویسنده در Author field بنویسید. بعد باید انتخاب کنیم که کدام نوع موجودیت ورودی این Transform می‌باشد که در اینجا آدرس ایمیل خواهد بود. هنگامی که نوع موجودیت ورودی انتخاب شده است، می‌توانیم مجموعه Transform را که تحت آن Transform ما ظاهر می‌شود را نیز انتخاب کنیم که می‌توانید none را انتخاب کنید.



حالا روی Next کلیک کنید و به مرحله دوم بروید. در اینجا در قسمت فرمان ما باید مسیری را برای محیط برنامه‌نویسی که برای اجرای کد Transform استفاده می‌کنیم، فراهم کنیم. در این مورد به صورت زیر خواهد بود:

/usr/bin/python (for Linux)

C:\Python27\python.exe (for Windows)

هنگامی که محیط تنظیم شد، می‌توانیم به parameters field برویم، در اینجا مسیر اسکریپت Transform را وارد می‌کنیم. مثلاً

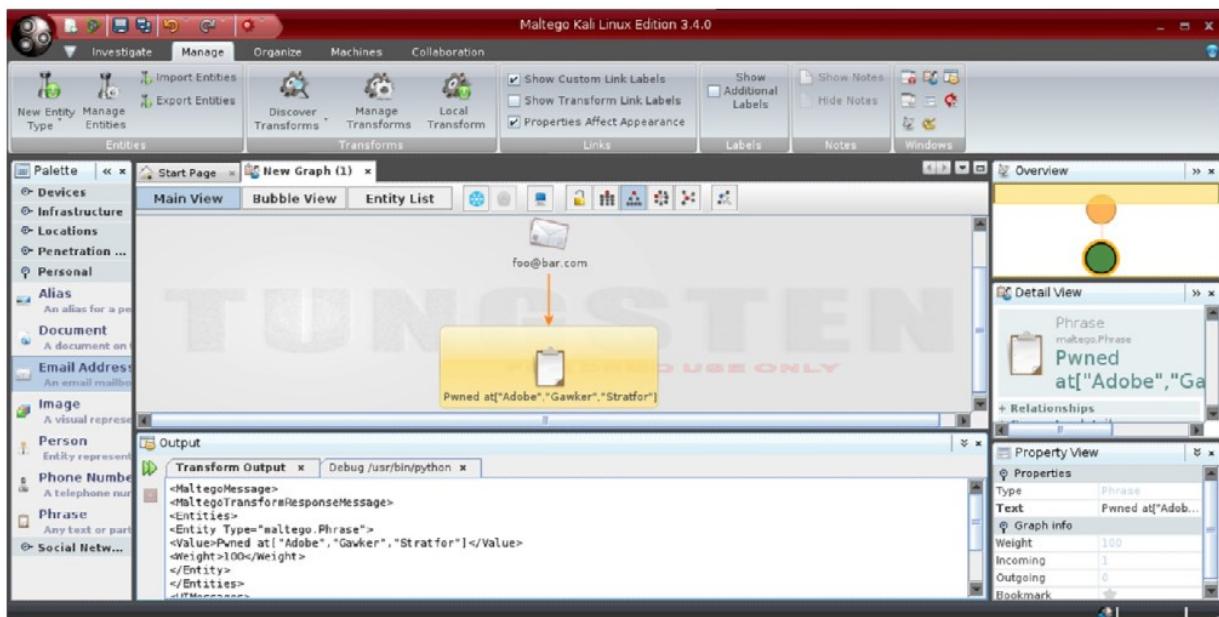
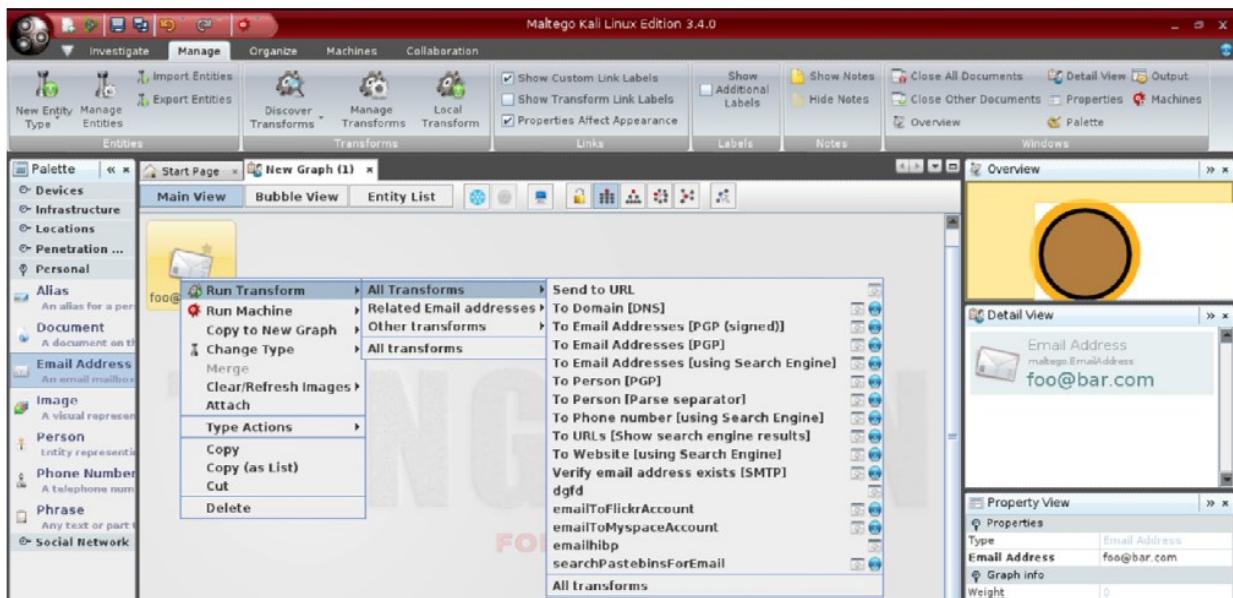
/root/Desktop/transforms/emailhibp.py (for Linux)

C:\Python27\transforms\emailhibp.py (for Windows)

نکته در اینجا این است که اگر ما Transform را با استفاده از دکمه مرورگر ارائه شده در مقابل فیلد Parameters انتخاب کنیم، به سادگی نام فایل را در فیلد می‌گیریم، اما باید مسیر مطلق Transform آن را ارائه کنید.



پس از آنکه همه اطلاعات کامل شد، Transform ما آماده اجرا است. برای تائید این، به سادگی یک موجودیت آدرس ایمیل را انتخاب و Transform را از منوی راست کلیک انتخاب کنید.



اکنون ما اولین Transform مان را ایجاد کردہ‌ایم و همچنین یاد گرفتیم که چگونه در Maltego آن را ثبت کنیم.

اجازه دهید یک Transform ساده دیگر ایجاد کنیم. برای این مثال ما از وبسایت <http://www.my-ip-neighbors.com/>

استفاده خواهیم کرد. این سایت اجازه می‌دهد تا یک جستجوی معکوس دامنه به IP را انجام دهید. در حقیقت

آدرس‌های IP یک دامنه را نشان می‌دهد. همان‌طور که در Transform قبلی یک آدرس ایمیل را به عنوان ورودی

ارائه می‌دهیم، نیازمند یک نام دامنه هستیم، اما این وبسایت هیچ سرویس API‌ای را ارائه نمی‌دهد و از این رو ما

درخواست خام GET را ارسال می‌کنیم و دامنه‌ها را خارج از صفحه وب با عبارات منظم و در کتابخانه "re"

استخراج می‌کنیم:

```
#!/usr/bin/python

from MaltegoTransform import *
import sys
import urllib2
import re
mt = MaltegoTransform()
mt.parseArguments(sys.argv)
url=mt.getValue()
mt = MaltegoTransform() opencname="http://www.my-ip-neighbors.com/?domain="
getrequrl=opencname+url header={'User-Agent':Mozilla'} req=urllib2.Request(getrequrl,None,header)
response=urllib2.urlopen(req) domains=re.findall("(?:[0-9]*[a-z][a-z\\\\.\\d\\-]+)\\.(?: [0-9]*[a-z][a-z\\-]+))(?!\\w\\.)",response.read())
for domain in domains:
    mt.addEntity("maltego.Domain", domain)
mt.returnoutput()
```

می‌تواند برای ایجاد عبارات منظم استفاده شود.

به طور مشابه، می‌توانیم بسیاری از Transform‌ها را ایجاد کنیم که از خدمات آنلاین، ابزار محلی (مانند اسکن Nmap) و موارد بیشتر با استفاده از پایتون استفاده کنند. نمونه‌هایی دیگر در <https://github.com/SudhanshuC/Maltego>- transforms یافت می‌شوند. برخی از Transform‌های جالب دیگری نیز در <https://github.com/cmlh> یافت می‌شوند،
همچنین یک جستجو را آنها می‌توانید کنید.

(<https://github.com/search?utf8=%E2%9C%93&q=maltego+transform>)

همچنین یک چارچوب مبتنی بر پایتون به نام Canari موجود است که اجازه می‌دهد تا Maltego Transform را به راحتی (<http://www.canariproject.com/>) ایجاد کنید.

موضوعات مختلفی وجود دارد که ما آن را پوشش نداده‌ایم به خاطر اینکه موضوع بسیار گسترده است. در زیر منابعی معرفی می‌شوند که می‌توانند برای یادگیری پایتون مفید باشند.

یک منبع عالی برای یادگیری بیشتر در مورد پایتون و استفاده از آن، پایتون docs است (<https://docs.python.org/2/>).

لیست بزرگ دیگری از ابزار مبتنی بر پایتون با تمرکز بر تست نفوذ در <https://github.com/dloss/python-pentest>- tools موجود است. این ابزار می‌توانند برای ایجاد چیزی جالب و مفید با تغییر، ترکیب و اضافه کردن به منابع ذکر شده مفید باشند. این فهرست بر اساس عملکرد ابزار به بخش‌های مختلف تقسیم می‌شود.

بنابراین برخی از اصول اولیه زبان پایتون را پوشش دادیم و همچنین یادگرفتیم که چگونه چارچوب Maltego را از طریق آن گسترش دهیم. در این فصل سعی بر یادگیری در مورد ایجاد ابزارهای سفارشی کردیم.

این فصل فقط مقدمه‌ای است که ما می‌توانیم به سادگی ابزارهایی با حداقل مقدار برنامه‌نویسی را ایجاد کنیم. قطعاً نیاز به بهبود کدها در شرایط عملکردی و ساختاری وجود دارد، اما هدف ما نشان دادن یک دید کلی بود.

اگرچه ما سعی کردیم تا آنجا که ممکن است این زمینه را پوشش دهیم اما هنوز چیزهای زیادی برای یادگیری اسکریپت پایتون وجود دارد. پایتون دارای مجموعه‌ای بزرگ از منابع مفید و بسیار قدرتمند است و با استفاده از آن می‌توانید ابزار قدرتمند recon-ng (<https://bitbucket.org/LaNMaSteR53/recon-ng>) را ایجاد کنید. یک راه عالی برای این یادگیری بیشتر، تمرکز بیشتر و ایجاد ابزارهایی است که می‌توانند مفید باشند.

در فصل بعد به برخی از نمونه‌ها و سناریوهای واقعی می‌برداریم که در آن می‌توانیم از دانش‌هایی ترکیبی به دست آمده، استفاده کنیم.

فصل ۱۴: مطالعات موردنی

مقدمه

پس از کار با بسیاری از ابزارها و تکنیک‌ها و فرایند جمع‌آوری و تجزیه و تحلیل اطلاعات، در حال حاضر وقت آن رسیده است تا برخی از سناریوهای واقعی را مشاهده کنید که همه این موارد دارای استفاده عملی هستند. در این فصل ما از سناریوهای واقعی را که در آن از OSINT برای جمع‌آوری اطلاعات موردنیاز است، استفاده کردی‌ایم؛ بنابراین بدون اتلاف وقت بگذارید به‌طور مستقیم به مطالعه مورد ۱ برویم.

مطالعه موردنی ۱: MASHUP BLACKHAT

یکی از دوستان ما از کنفرانس Black Hat آیالات متحده بازگشت و او در مورد جلسات و همه چیز بسیار خوشحال بود. دوست ما برای یک شرکت امنیتی پیشرو کار می‌کند و فروش ایالات متحده را به عهده دارد. او در مورد یک راهنمایی یک فرد خاص که در آنجا بود، بسیار هیجان‌زده بود. فردی که او ملاقات کرد، در مقام ارشد یک شرکت تولید بازی بود و علاقه‌مند به خدماتی بود که توسط شرکت دوست ما ارائه می‌شد. آن‌ها جلسه بسیار خوبی داشتند و دوست ما فراموش کرد پیشنهادش را به وی تحويل دهد.

❖ مشکل شماره ۱: او نام کامل او را فراموش کرده اما نام شرکت و محل شرکت او را به یاد می‌آورد.

❖ مشکل شماره ۲: در حال بحث شخص دیگر گفت که بسیاری از افراد برای ارائه پیشنهادها به او از نام دیگری در LinkedIn استفاده می‌کند.

❖ مشکل شماره ۳: موقعیت شخص دیگر را می‌دانیم، اما موقعیت منحصر به فردی نظیر مدیر عامل یا CTO نیست.

هنگامی که او با این مورد پیش ما آمد، احساس کردیم که می‌توانیم او را پیدا کنیم. اطلاعاتی در مورد شخص وجود دارد هر چند که شامل اطلاعات اولیه مانند آدرس ایمیل و یا نام کامل نیست.

اولین چیزی که از او پرسیدیم این بود که آیا می‌تواند تصویر شخص را تشخیص داد یا این که او را فراموش کرده، او گفت: «بله»؛ بنابراین مهم‌ترین مسئله در این مورد این بود که اگر تعدادی از افراد را پیدا کنیم و او صحبت فرد را تائید کند.

مرحله ۱:

طبق معمول ابتدا با یک جستجوی ساده گوگل با نام، موقعیت و نام شرکت شروع کردیم. فرض کنید موقعیت او مدیر ارشد است و نام شرکت abc.inc است. پرس‌وجو استفاده شده به شکل زیر است:

Senior manager abc.inc

مرحله ۲:

در فیسبوک سعی کردیم پروفایلی معادل آن را بیابیم، اما هرگز منجر به نتیجه نشود.

مرحله ۳:

ما به LinkedIn رفیم تلاش کردیم و موفق نشدیم.

مرحله ۴:

ما به صفحه پروفایل این شرکت رفته و سعی کردیم از همه پروفایل‌های کارکنان بازدید کنیم اما متوجه شدیم که بیش از ۷۰۰۰ کارمند ثبت شده در LinkedIn وجود دارد و این واقعاً یک کار سخت برای پیدا کردن کسی در آنجا است.

مرحله ۵:

همان‌طور که در فصل ۲ ارائه شد، این ابزار ویژگی جستجوی پیشرفته را فراهم می‌کند و ما برخی از داده‌های مستقیم برای فیلدها را داریم؛ بنابراین تصمیم گرفتیم از آن استفاده کنیم.

<https://www.linkedin.com/vsearch/p/?trk=advsrch&adv=true>

ما اطلاعات را در فیلدهای مانند عنوان، شرکت و مکان به عنوان اطلاعات دوستان ذخیره کردیم. در نتیجه پروفایل‌های معادل زیادی دریافت کردیم، اما این بار نتایجی بسیار کمتر از آنچه بود. در نتیجه بیست و یکمین فردی که به تازگی در کنفرانس حضور داشته را به دست آوردیم. پس از بازدید از پروفایل، اطلاعات کمی در مورد این شخص به دست آمد که ما آنچه را که دنبال آن بودیم، یافتیم.

پس از آن چه کاری انجام شد؟

ما ممکن است شناسه اصلی، شناسه شرکت و سایر جزئیات را با استفاده از منابع مختلف مانند Google Maltego یا ساده دریافت کنیم. با استفاده از تصویر ما ممکن است جستجوی تصویر معکوس را برای دریافت تصویر مربوطه و منابع انجام دهیم. ممکن است وبلاگ‌ها یا وبسایت‌هایی که توسط آن شخص ایجاد شده و بسیاری دیگر را دریافت کنیم. امکانات بی‌حد و حصری وجود دارد اما ما در اینجا کار را متوقف کردیم زیرا خارج از محدوده کاری ما بود. ما این لینک را به دوست خود فرستادیم.

A DEMO THAT CHANGED AUDIENCE VIEW :۲

ما نمی‌توانیم این نسخه آزمایشی را فراموش کنیم؛ چرا که دیدگاه ما در مورد امنیت را تغییر داد. ما در یک پروژه با یک مشتری کار می‌کردیم که می‌خواست با سازمان ما همکاری کند. به ما گفته شد که باید برخی گزارش‌های کیفی را ارائه دهیم و سپس باید یک گزارش در خصوص مشتریان آینده ارائه دهیم. بعدها به ما اطلاع داده شد که برخی از نمایندگان از جمله مدیر عملیاتی و یک مشاور ارشد از ما بازدید خواهند کرد. ما از مدیریت درخواست کردیم تا اجازه دهد که آن‌ها را در برنامه انجام OSINT ما حضور یابند و بعد از آن گزارش بدھیم. مدیریت ما در این مورد موافقت کرد، بنابراین یک نسخه آزمایشی ویژه OSINT را آماده کردیم.

ما اسم نمایندگان را داشتیم، بنابراین اولین چیزی که انجام دادیم این بود که به سرعت پروفایل آن‌ها بازدید شد تا درباره آن‌ها بیشتر بدانیم. LinkedIn در این امر به ما کمک کرد. ما در مورد دوستان و زمینه‌های فنی کمی اطلاعات کسب کردیم. ما متوجه شدیم که هر دو دارای پس‌زمینه فنی بسیار خوبی در امنیت بودند، بنابراین ما نسخه پشتیبان

تهیه کردیم. سپس ما به سمت جمع‌آوری داده‌های مختلف در مورد یک سازمان یا یک برنامه (برنامه و ب بدون ارسال یک بسته) حرکت کردیم.

❖ مشکل: ما نمی‌توانیم چیزی را نشان دهیم که نیاز به دسترسی به محیطی دارد که ما مجوز آن را نداریم.

تصمیم گرفتیم از وب‌سایت مشتری شروع کنیم و سپس به سمت چیزی‌های جالب برویم. مراحل زیر دنبال شدند:

مرحله ۱:

ما را باز کردیم و نام دامنه مشتری را اضافه کردیم. یک گزینه در Maltego برای اضافه کردن یک دامنه به عنوان یک موجود وجود دارد و ما همین کار را انجام دادیم و سپس بعضی از Transform‌ها را انجام دادیم تا داده‌های مختلف مانند رکوردهای نام سرور و بسیاری دیگر را به دست آوریم.

مرحله ۲:

استفاده از buildwith transform، تکنولوژی‌های مورد استفاده را نشان داد. Transform‌های دیگر به ما کمک کرد تا برخی از دامنه‌های / زیر دامنه‌ها دیگر را کشف کنیم.

مرحله ۳:

در یکی از دامنه‌ها، ما دریافتیم که یک نسخه بسیار قدیمی از PHP مورد استفاده قرار می‌گیرد؛ بنابراین آنچه انجام دادیم این بود که به سادگی برنامه را در یک مرورگر باز کردیم که پلاگین‌های Shodan و PunkSpider فعال بودند. لحظه‌ای که این برنامه را در مرورگر باز کردیم، Shodan نشان داد که برنامه به Heartbleed آسیب‌پذیر است و برخی از پورت‌های حساس باز توسط PunkSpider شناسایی شد که آسیب‌پذیری‌های SQL injections و blind cross-site scripting وجود دارد.

با جستجوی پیشرفته گوگل برای پارامترهای مشابه، آسیب‌پذیر به SQL و XSS در دامنه‌های دیگر آن‌ها کشف شد. این نشان می‌دهد که آن‌ها نیز ممکن است با آسیب‌پذیری‌های مشابه، تهدید شوند.

site:example.com inurl:vulnpar

آن‌ها از نتایج شکفت‌زده شدند. آن‌ها به ما گفتند که این سایت بسیار قدیمی و استفاده از آن بسیار دشوار بود و به خاطر برخی از دلایل فنی آن را فراموش کرده بود؛ اما ما برخی از حقایق جالب در مورد این نرم‌افزار را پیدا کردیم و خوشحال شدیم.

مرحله ۴:

سپس Maltego را باز کردیم و Transform با نام "Domain to Email address" را برای جمع‌آوری آدرس‌های ایمیل استفاده کردیم.

مرحله ۵:

سپس Transform نوشته شده توسط خودمان با نام HavelBeenPwned را اجرا کردیم. این Transform بر اساس API ارائه شده توسط Troy Hunt است. این Transform در صورتی که شناسه ایمیل هر شخص در آن وجود داشته باشد، هشدار خواهد داد. پس از اجرای این Transform با تمام شناسه‌های ایمیل که از نام دامنه دریافت کردیم، خوسبختانه متوجه شدیم که دو حساب کاربری همکارانشان در سایت مبتنی بر محصول شرکت، مورد نفوذ قرار گرفته‌اند.

برای مشتریان ما چیز جدید بود و آن‌ها بلافضله به همکاران خود در مورد این موضوع اطلاع دادند. اگرچه توجه ما را جلب کرد، اما ما می‌خواستیم تأثیر چنین اطلاعاتی را نشان دهیم. ما می‌توانستیم به سادگی توضیح دهیم که سایتهايی برای دریافت رمزهای خاص مربوط به این شناسه‌های ایمیل مانند pastebin وجود دارد، اما ما سعی کردیم تصویر بزرگ‌تری را نشان دهیم.

مرحله ۶:

سپس این دو شناسه ایمیل را انتخاب کردیم و Transform دیگری را که توسط خودمان نوشته شده بود انتخاب کردیم که "Email-Rapportive" است. بر اساس Rapportive service به آدرس <http://www.rapportive.com/> است. این ابزار اطلاعات مربوط به شخص بر مبنای آدرس ایمیل را پیدا می‌کند و نتیجه را به ما می‌دهد. نتیجه پیوند پروفایل LinkedIn، فیسبوک، توییتر همراه با نام و عنوان شغلی فرد است؛ بنابراین اساساً به ما کمک می‌کند که حضور در شبکه‌های اجتماعی و برخی از جزئیات مهم مانند نام کامل را به دست آوریم.

مرحله ۷:

پس از آن ما از Maltego machine را بر روی پست الکترونیک تولید شده در مرحله قبلی اجرا کردیم. یک machine چیزی جز یک مجموعه‌ای از یک یا چند Transform نیست که به طور جمعی اجرا می‌شود. درباره این موضوع در فصل ۶ بحث کردیم؛ این machine دیگر آدرس‌های ایمیل با الگوی مشابه را در سرویس‌های ایمیل مانند Gmail، Yahoo، Outlook و غیره پیدا می‌کند. نتایج بسیار زیادی دریافت کردیم و آن‌ها را توضیح دادیم که افرادی هستند که از رمز عبور مشابه برای شناسه‌های مختلف ایمیل استفاده می‌کنند؛ بنابراین اگر کسی بتواند رمز عبور مرتبط با یک شناسه پست الکترونیکی را جمع‌آوری کند، می‌تواند تمام دیگر شناسه‌های ایمیل و جزئیات وب‌سایت ثبت شده را پیدا کند و این احتمال وجود دارد که مهاجم بتواند بر اساس اطلاعات به برخی یا همه حساب‌های قربانی برسد.

ما نمایندگان را در خصوص رسیک مربوط به این سناریو هشیار کردیم و آن‌ها خوشحال بودند که ما یک نسخه واقعی به آن‌ها ارائه کردیم. تنها سؤال از طرف آن‌ها این بود که هرچند IPS / IDS و فایروال‌ها در زیرساخت آن‌ها نصب شده‌اند، اگر کسی سعی کند همین کار را انجام دهد، آیا آدرس IP ورود به سیستم دریافت خواهد شد؟

پاسخ این است که ما از تمام اطلاعات موجود در دسترس استفاده کردیم تا نشان دهیم چگونه می‌توانیم به امنیت بررسیم. ابزارهای مورد استفاده، بسته‌های مخرب به زیرساخت اصلی ارسال نمی‌کنند که تقریباً شناسایی افرادی را که چنین کارهایی را انجام می‌دهند، غیرممکن است. به غیر از این، تکنیک‌های مختلف گمنامی مانند تور و پروکسی وجود دارد که ما می‌توانیم از طریق آن هویت مان را پنهان کنیم.

این درک آن‌ها را درباره امنیت تغییر داد. امنیت فقط تأمین امنیت شبکه یا زیرساخت شما نیست. این نیز با آنچه در اینترنت به اشتراک گذاشته می‌شود، مرتبط است.

مطالعه موردنی ۳: AN EPIC INTERVIEW

یکی از دوستان ما به دنبال استخدام در حوزه امنیتی بود. یک صبح پنج‌شنبه او از یک شرکت مشاوره در مورد افتتاح یکی از شرکت‌های امنیتی پیشرو تماس گرفت. تماس اول به خوبی انجام شد و همه چیز به نفع او بود. انتظار می‌رود که حقوق و دستمزد و همه چیز خوب باشد اما تنها مشکل این بود که او هیچ تجربه‌ای در این زمینه نداشت؛ بنابراین او کمی درباره مصاحبه نگران بود. بعد از دو روز دوباره با او تماس گرفتند که شما برای مصاحبه فنی انتخاب شده بودید و می‌توانید یک روز یا بیشتر متوجه تماس آفای John Doe باشید.

اولین چیزی که او با ما در میان گذاشت، این بود: "من فقط می‌خواهم جزئیات کمی درباره این شخص به دست بیاورم تا بتوانم در ک کنم که چه سؤالاتی ممکن است بپرسد، در ک تجربه و انتظاراتش." ما سه نفر تصمیم گرفتیم با OSINT به جمع‌آوری اطلاعات John Doe پردازیم.

❖ مشکل ۱: ما فقط نام آن را داریم، اما جزئیات موقعیتی او نیست.

❖ مشکل ۲: قاب زمانی ثابت نیست، ما دقیقه نمی‌دانیم چقدر زمان داریم.

بنابراین پیشنهاد کردیم که از وبسایت شرکت بازدید نماییم تا خدمات ارائه شده را در ک کنیم و از جزئیات دیگر مانند با خبر شویم. در همین حال شروع به جستجوی اطلاعات بیشتر در مورد شخص آقای John Doe کردیم.

مرحله ۱:

نام شخص و نام شرکت را به طور مستقیم در LinkedIn جستجو کردیم. ما پروفایل آن را پیدا کردیم که متشکل از اطلاعات زیادی از قبیل تجربه فعلی و قبلی او است. ما متوجه شدیم که شخص یکی از مدیران فنی این شرکت است. پروفایل LinkedIn شامل برخی از مقالات و آخرین دستاوردهای آن بود. این فرد به تازگی OSCP (Security Certified Professional) را دریافت کرده است. ما همچنین لینک حساب GitHub او را از پروفایل LinkedIn پیدا کردیم. ما از مقالاتش بازدید کردیم. بیشتر مقالات در مورد چگونگی پیدا کردن اشکالات در بسیاری از سایتها می‌باشد که شامل برخی از 0Day ها در سیستم‌های محبوب CMS بود.

مرحله ۲:

پس از دریافت این اطلاعات، از حساب GitHub اش بازدید کردیم. او تمام اسکریپت‌هایش را برای تست فرایند تست در پایتون نوشته بود.

مرحله ۳:

ما یک جستجوی ساده گوگل را با نام او انجام دادیم و پیوندهای بسیاری با یک حساب slideshare داشتیم. ما از حساب slideshare بازدید کردیم. سخنرانی‌هایی در مورد چگونگی نوشتن قوانین IDS وجود داشت. در یکی از پست‌های قدیمی‌تر ما یک پیوند نظر به وبلاگ‌های قدیمی‌ترش پیدا کردیم.

مرحله ۴:

ما از این و بلاگ قدیمی او بازدید کردیم که متشکل از سفرهای مختلف جاده‌ای است که او با موتورسیکلت‌ش انجام داده بود.

مرحله ۵:

ما توییتر را جستجو کردیم و یک پست جالب پیدا کردیم که او اخیراً در یکی از کنفرانس‌های امنیتی محظوظ در گوا، هند شرکت کرده بود.

مرحله ۶:

ما از سایت کنفرانس بازدید کردیم و متوجه شدیم که شخصی آقای John Doe در مورد مانیتورینگ شبکه صحبت کرده است.

مرحله ۷:

او را در فیسبوک جستجو کردیم و اطلاعاتی در مورد محل تولدش، مکان فعلی، جزئیات آموزشی و همه چیز به دست آوردیم.

مرحله ۸:

در Yasni جستجو کرده و یک پیوند به وب‌سایت دیگری از جامعه امنیت محلی را به ما نشان داد که در آن شماره تلفن او را به عنوان لیدر پیدا کردیم. ما این شماره تلفن را از طریق Truecaller تائید کرده و آن را بررسی کردیم.

تقریباً ۲۵ تا ۳۰ دقیقه طول کشید تا متوقف شدیم. در عین حال دوست ما با تمام اطلاعاتی که دریافت کرد، آماده بود. بر اساس اطلاعاتی که در منابع مختلف جمع‌آوری کرده‌ایم، این نتیجه گیری شده است.

- ✓ شماره تلفن را ذخیره کنید و با نام به او خوشنامد بگویید.
- ✓ اولین چیزی که باید از او بپرسید این است که سخنرانی‌اش در گوا چگونه بود.
- ✓ خلاصه سخنرانی‌اش را بشنوید و به او بگوید عالی است و شما از اینکه آنجا نبودید تأسف می‌خورید.
- ✓ سؤالاتی را در مورد نوشتن قوانین IDS بدانید و برای پاسخگویی به slideshare مراجعه کنید.
- ✓ برخی از سؤالات در مورد ابزار خودکار و همچنین در پایتون انتظار می‌رود؛ بنابراین یک نسخه آموزش سریع پایتون موردنیاز بود.

- ✓ انتظار می‌رود سؤالاتی در مورد آزمون نفوذ شبکه پرسد.
- ✓ انتظار می‌رود سؤالاتی در مورد امنیت نرم‌افزار وب، مشکلات احتمالی و 0Day پرسد.
- ✓ اگر او درباره سرگرمی‌ها از شما می‌پرسد، سفرهای جاده‌ای را به او بگو و چطور می‌خواهد یک موتورسیکلت داشته باشد.
- ✓ اگر از شما سؤال مربوط به چشم‌انداز کرد، چشم‌انداز موجود شرکت با افکار شخصی‌اش را به او بگویید.
- ✓ اگر او پرسید با برنامه‌های آینده خود را به کجا می‌خواهد برسانید، به او بگوئید که می‌خواهید گواهینامه OSCP را دریافت کنید و یک لیدر Red team باشد.

دوست ما دانش و تجربیات بسیار خوبی داشت و به علت تخصصش و با تکالیف کوچکی در شرکت، انتخاب شد. آقای John Doe نه تنها از مهارت‌های فنی، بلکه به دلیل اشتراکات زیادی که با دوست ما داشت خوشحال بود.

این‌ها برخی از مطالعات موردنی جالب بودند، بیاید در مورد برخی از انواع اولیه اطلاعات مربوط به اشخاص و نحوه مقابله با افشاگران آن‌ها را یاد بگیریم.

بسیار آسان است که با اطلاعات اولیه مانند نام، شناسه ایمیل برای جمع‌آوری تمام اطلاعات دیگر شروع کنیم، اما مواردی وجود دارد که ممکن است اطلاعات اولیه را نداشته باشیم اما این بدان معنا نیست که ما نمی‌توانیم این اطلاعات اولیه را از اطلاعات ثانویه به دست آوریم. این فرآیند ممکن است کمی سخت باشد اما ممکن است؛ بنابراین اکنون به طور خاص درباره جزئیات شخص صحبت خواهیم کرد. چه چیزی را می‌توان در مورد یک فرد جمع‌آوری کرد؟ کجا و چگونه؟ در زیر برخی از اطلاعاتی که ممکن است برای جمع‌آوری اطلاعات در مورد یک فرد مفید باشد، آورده شده است:

شخص:

- ✓ نام کوچک
- ✓ نام خانوادگی
- ✓ نام شرکت
- ✓ آدرس ایمیل (شخصی)
- ✓ آدرس ایمیل (شرکت)

- ✓ شماره تلفن (شخصی)
- ✓ شماره تلفن (شرکت)
- ✓ آدرس (صفحه شخصی)
- ✓ آدرس (شرکت)
- ✓ آدرس حساب فیسبوک
- ✓ URL حساب کاربری LinkedIn
- ✓ آدرس حساب توییتر
- ✓ URL حساب Flicker
- ✓ وبلاگ شخصی و یا URL وبسایت
- ✓ کلیدواژه‌ها
- ✓ متفرقه

از لیست بالا می‌توانیم از هر نقطه‌ای شروع کنیم و بیشترین اطلاعات را جمع‌آوری کنیم. مراحل ممکن است با آنچه ما به عنوان منبع اولیه دریافت کردیم، متفاوت با یکدیگر باشند، اما از همان ابزارها و یا تکنیک‌ها فقط در جهت‌های مختلف استفاده می‌کنیم.

هر آنچه ما به عنوان یک منبع می‌گیریم، اساساً باید با جستجو ساده گوگل و یا هر موتور جستجو سنتی مانند Yandex آغاز شود. اگر ما اطلاعات نسبی را به دست آوریم، با استفاده از همان اطلاعات می‌توانیم اطلاعات مرتبط دیگر را جمع‌آوری کنیم.

فرض کنید ما نام و نام خانوادگی داریم و سپس می‌توانیم به سادگی از یک درخواست گوگل برای دریافت نتایج استفاده کنیم. فرض کنید با استفاده از گوگل ما قادر به گرفتن وبلاگ یا وبسایت شخصی آن هستیم.

از آن سایت دیدن کنید تا اطلاعات مربوطه را برای جزئیات مربوط به شخص جستجو کنید، مانند زمینه مورد علاقه، سن، تاریخ تولد، پست الکترونیکی، محل تولد، جزئیات آموزشی، یا هر گونه اطلاعاتی که می‌توانید برای دریافت اطلاعات دیگر استفاده کنید.

فرض کنید ما جزئیات آموزشی را داریم. فیسبوک را با کنید و سعی کنید با نام و جزئیات آموزشی جستجو کنید. ما می‌توانیم پروفایل شخص را به دست آوریم. در فیسبوک ما اطلاعات زیادی از قبیل شرکتی که در حال

کار بر روی آن هستید، دوستان، عکس‌های او و برخی دیگر از لینک‌ها همراه با آدرس ایمیل شخص نیز دریافت خواهید کرد.

در حال حاضر با استفاده از نام شرکت و نام شخص می‌توانیم پروفایل LinkedIn را به آسانی دریافت کنیم و می‌توانیم آدرس ایمیل آن را حدس بزنیم. به طور کلی شرکت‌ها از یک الگوی معمول برای ایجاد آدرس ایمیل استفاده می‌کنند. باید بگوییم نام شرکت abc.inc است و سایت آن www.abc.com است. الگو به این شکل است، از اولین حرف نام و نام خانوادگی بدون هیچ فضایی استفاده می‌کند؛ بنابراین از نام شخص و نام شرکت ما می‌توانیم به راحتی آدرس ایمیل را طراحی کنیم یا می‌توانیم از ابزارهایی مثل harvester برای برداشتن آدرس ایمیل از نام دامنه شرکت استفاده کنیم و پس از بررسی همه ایمیل‌ها، ما به راحتی می‌توانیم بررسی کنیم که ایمیل با شخص مرتبط است. به این ترتیب می‌توان اطلاعات را از طریق همبستگی آن‌ها دریافت یا جمع‌آوری کرد.

جمع‌آوری اطلاعات شرکت در مقایسه با اطلاعات شخصی بسیار ساده است. اکثر اطلاعات شرکت، عمومی است؛ بنابراین می‌توانیم آن را در وب‌سایت آن دریافت کنیم و می‌توانیم برای کسب اطلاعات از نام شرکت، شروع کنیم. این می‌تواند به عنوان یک نقطه شروع برای دریافت تمام اطلاعات، استفاده شود؛ بنابراین، اگر نام شرکت را می‌دانیم، می‌توانیم بقیه اطلاعات را کاملاً راحت به دست آوریم. در زیر فهرستی از اطلاعاتی است که ما به طور کلی در مورد جزئیات شرکت به دنبال آن هستیم، لیست شده است:

شرکت:

- ✓ نام شرکت
- ✓ سال تأسیس
- ✓ مدیران
- ✓ سایت اینترنتی
- ✓ نام ثبت‌نامی
- ✓ شماره تلفن
- ✓ نشانی
- ✓ کلیدواژه‌ها
- ✓ تعداد کارکنان

- ✓ نمونه‌های پست الکترونیکی
- ✓ پست الکترونیکی HR
- ✓ نقاط قابل دسترسی
- ✓ آدرس حساب فیسبوک
- ✓ URL حساب کاربری LinkedIn
- ✓ آدرس حساب توییتر
- ✓ URL حساب flicker
- ✓ دیگر ویلاگ / وبسایت URL / Subdomains
- ✓ متفرقه

اگر ما نام شرکت را می‌دانیم، می‌توانیم به راحتی با هر موتور جستجو که می‌خواهیم آدرس اینترنتی و وبسایت را به دست آوریم. هنگامی که وبسایت ثبت شده را دریافت می‌کنیم، می‌توانیم اطلاعاتی از قبیل سال تأسیس، مدیران، شماره تلفن، آدرس، پست الکترونیک HR، دسترسی‌های باز و در مواردی پیوند به شبکه اجتماعی مختلف را به دست آوریم. پرس‌وجو ساده‌ی Whois نیز اطلاعات زیادی می‌یابد.

مکان‌های دیگری وجود دارد که ما می‌توانیم تمام این اطلاعات را به دست آوریم. ما می‌توانیم این اطلاعات را در LinkedIn و Glassdoor، Zoominfo و Glassdoor بینیم. برای باز کردن آن می‌توانیم در پورتال‌های شغلی نیز نگاه کنیم. کارکنان آن را می‌توان به راحتی با استفاده از LinkedIn پیدا کرد و یا در غیر این صورت ما می‌توانیم به راحتی از ابزار مانند Maltego harvester برای دریافت الگوهای ایمیل استفاده کنیم. کلمات کلیدی و همه موارد را می‌توان به راحتی در قسمت متأ وبسایت، از طریق SEO های مختلف و خدمات SEM مانند SEMRush یافته.

این بخش کمی فنی و اغلب موردنیاز توسط افراد فنی مانند مدیران، مشاوران فناوری اطلاعات، تست نفوذ‌گرها و غیره است. در این مورد، برای انجام یک ارزیابی فنی، اساساً تحلیلگران با نام دامنه یا آدرس IP کار می‌کنند، بنابراین از دیدگاه OSINT می‌توان این اطلاعات را به عنوان اطلاعات اولیه در نظر گرفت. از آن‌ها، ممکن است بقیه اطلاعات ذکر شده در زیر را دریافت کنید:

دامنه:

✓ دامنه

- ✓ نشانی IP
- ✓ سرور نام
- ✓ سرور MX
- ✓ شخص
- ✓ سایت اینترنتی
- ✓ زیردامین ها
- ✓ نمونه‌های ایمیل
- ✓ فایل‌ها
- ✓ متفرقه

بنابراین، دامنه را به عنوان یک موجودیت اولیه می‌گیریم و از آن تمام اطلاعات دیگر که در بالا ذکر شد را دریافت کنید. اگر می‌خواستیم آدرس IP آن دامنه را دریافت کنیم، فقط باید یک فرمان ping ساده در خط فرمان یا ترمینال بر اساس سیستم عامل مان استفاده کنیم.

ping <domain name>

این دستور اجرا خواهد شد و آدرس IP دامنه را ارائه می‌دهد.

برای سایر اطلاعات خاص دامنه، ابزارهایی به صورت رایگان در اینترنت موجود می‌باشند که به ما اطلاعات مختلفی از قبیل نام شرکت ثبت شده، جزئیات نام سرور، ایمیل، آدرس IP، محل و بسیاری بیشتر را می‌دهند. منابعی مانند w3dt.net می‌توانند در اینجا بسیار مفید باشند. به طور مستقیم با استفاده از ابزار دامنه می‌توانیم اطلاعات زیادی در مورد یک دامنه پیدا کنیم، یا می‌توانیم از یک transform Maltego استفاده کنیم.

ما همچنین می‌توانیم از ابزار harvester برای جمع‌آوری زیر دامنه، آدرس ایمیل و غیره از نام دامنه استفاده کنیم. از آدرس‌های پست الکترونیکی می‌توانیم برای پروفایل‌های افراد در سایت‌های مختلف شبکه‌های اجتماعی جستجو کنیم.

و برای دریافت زیر دامنه‌ها و یک فیلد خاص از دامنه می‌توان از Google، Search-Diggity، Knock و یا Knock استفاده کرد.

برای دریافت زیردامنهای مختلف می‌توانیم از اپراتور site استفاده کنیم یا یک اسکریپت پایتونی ایجاد کنیم که نام‌های زیر دامنه را از لیست دریافت و آن را همراه با دامنه ارائه می‌دهد:

site:domainname

برای به دست آوردن یک نوع خاص از فایل از دامنه با یک کلمه کلیدی می‌توانیم از ext filetype یا استفاده کنیم و می‌توانیم جستجوی زیر را اجرا کنیم:

site:domainname keyword filetype:ppt

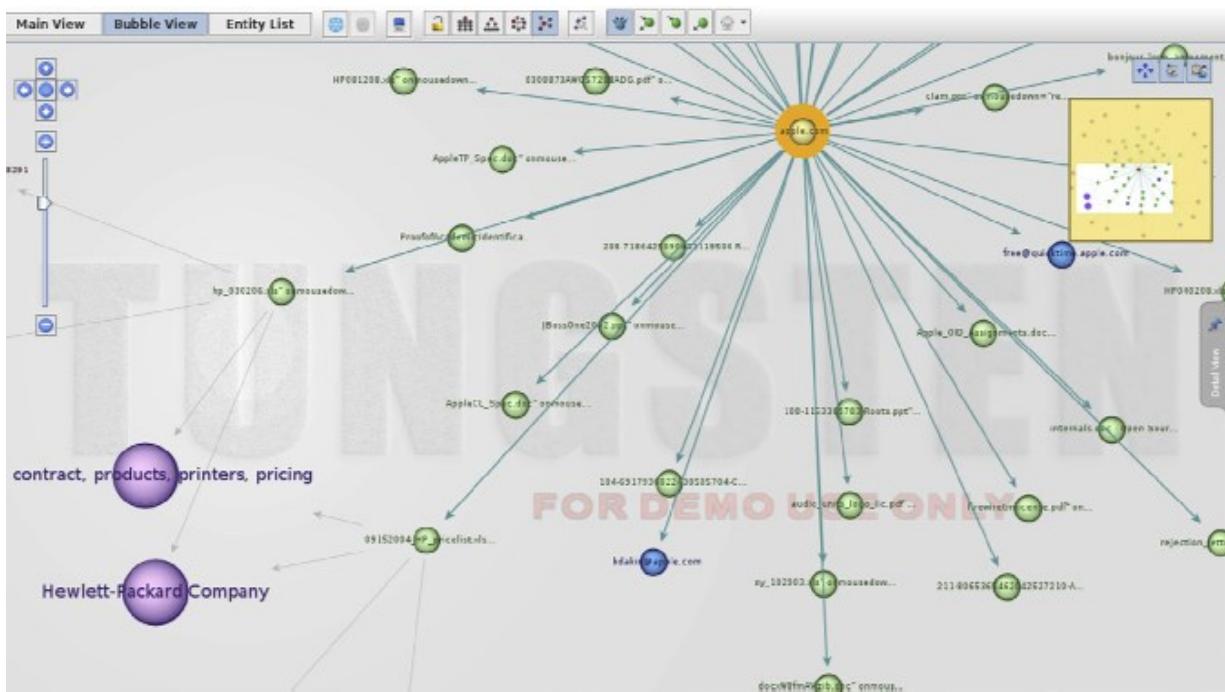
بنابراین می‌توانیم تمام اطلاعات خاص دامنه را از منابع مختلف دریافت کنیم.

این‌ها برخی از مطالعات موردی و نمونه‌هایی بود که OSINT می‌تواند جمع‌آوری کند که در زندگی شخصی و حرفة‌ای ما مفید است. همان‌طور که قبلاً در موضوع قول داده بودیم، ما در مورد ماشین‌های Maltego یاد خواهیم گرفت.

ماشین‌های^۱ Maltego

این فصل بیشتر درباره ترکیب دانش‌هایی است که تاکنون به آن پرداخته شده است، به همین ترتیب در Maltego ما یاد خواهیم گرفت که چگونه ماشین‌های Maltego را ایجاد کنیم. اگر چه ما قبلاً یک ماشین Maltego را ایجاد کردیم، اما برای فراخوان سریع مجموعه‌ای از transform‌ها آن را ایجاد کرده است. این اجازه می‌دهد تا ما یک نوع واحد را به عنوان ورودی انتخاب و به سمت نوع دیگری که به طور مستقیم به آن متصل نیستم حرکت کنیم، از طریق یک مجموعه و یا ترتیبی از transform‌ها. در Maltego بعضی از ماشین‌های داخلی ساخته شده مانند Company Stalker وجود دارد که حوزه دامنه را به عنوان ورودی می‌گیرد و انواع مختلفی از transform‌ها را به صورت پیوسته اجرا می‌کند تا انواع مختلفی از اطلاعات از قبیل آدرس ایمیل، فایل‌ها و غیره را دریافت کند.

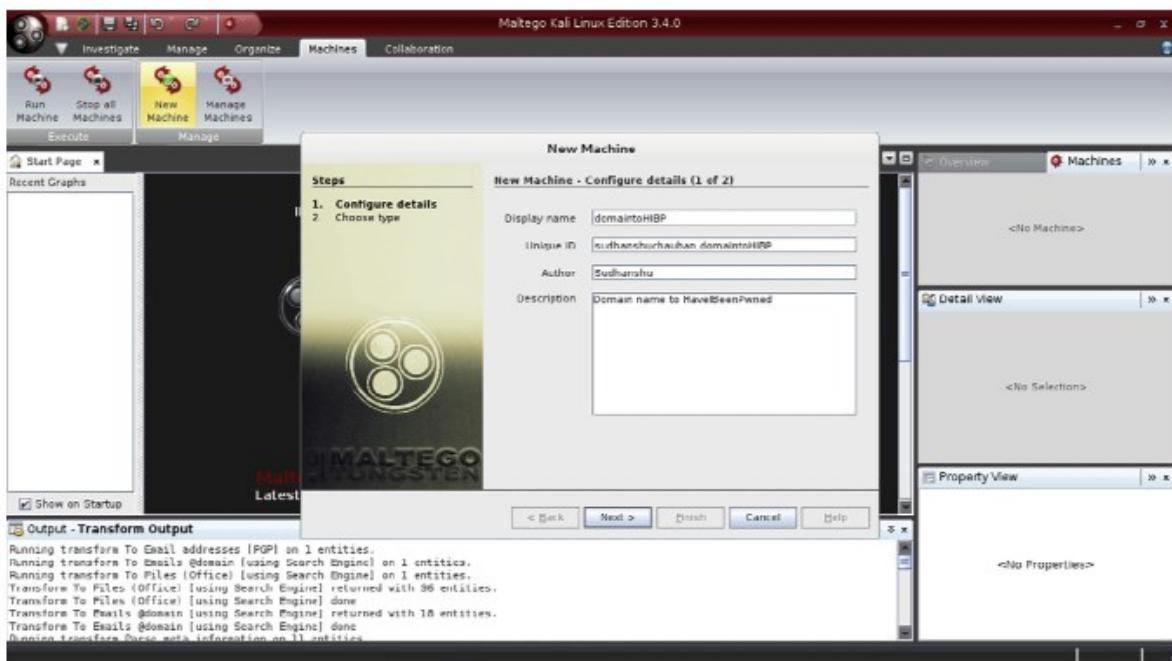
¹ MACHINES



برای ساختن ماشین خود باید از PDF استفاده کنیم. مستندات MSL در یک MSL در <http://www.paterva.com/MSL.pdf> در دسترس است. اسناد واضح و ساده است و هر کسی که دارای مهارت‌های برنامه‌نویسی باشد، می‌تواند به راحتی آن را درک کند. همان‌طور که تمام شرایط و فرآیند به‌وضوح مشخص شده، مانند این نکات را پوشش دهیم، بنابراین برای ایجاد یک ماشین ساده با استفاده از transform‌های محلی که در فصل قبلی ایجاد کردیم، به سرعت پیش می‌رویم.

ایجاد یک ماشین Maltego بسیار ساده است، ابتدا باید به زبانه machine برویم، در آن می‌توانیم گزینه New Machine گزینه را پیدا کنیم. با کلیک بر روی آن، پنجره‌ای ایجاد می‌شود که در آن باید نام و سایر مشخصات توصیفی مربوط به دستگاه ما را وارد کنیم. در مرحله بعد ما باید نوع دستگاهی که می‌خواهیم ایجاد کنیم انتخاب کنیم. برای این منظور ما سه گزینه داریم:

- ↳ Macro: runs once
- ↳ Timer: runs periodically until stopped
- ↳ Blank: a blank template



هنگامی که ما نوع دستگاه را انتخاب کردیم، می‌توانیم کدی برای دستگاه مان بنویسیم و از transform های پانل سمت راست با دو بار کلیک بر روی آن در موقعیت مناسب، استفاده کنیم. بلوک start حاوی transform ها و اجزای دیگر اجرایی است. توابع run برای اجرای یک transform خاص استفاده می‌شوند. برای اجرای توابع به صورت موازی ما می‌توانیم آنها را در داخل مسیرها قرار دهیم. در داخل "paths" ما می‌توانیم مسیرهای مختلفی ایجاد کنیم که هم‌زمان با یکدیگر اجرا می‌شوند، اما عملیات در داخل یک مسیر به طور پیوسته اجرا می‌شود. به همین ترتیب می‌توانیم مقادیر مختلفی مانند ورودی‌های کاربر، فیلتر و غیره را استفاده کنیم.

باید یک ماشین ساده ایجاد کنیم که عناصر ایمیل را از یک دامنه ارائه شده استخراج می‌کند و بیشتر بر مبنای HIBP محلی در این زمینه اجرا می‌شود. برای این منظور باید نام دستگاه را ارائه دهیم و نوع ماکرو را انتخاب کنیم. سپس د باید transform های داخلی را که می‌تواند ایمیل‌ها را از دامنه را استخراج کند، انتخاب می‌کنیم. وقتی که نیاز داریم به موازات این کار را انجام دهیم، باید "paths" جداگانه را برای هر ایمیل ایجاد کنیم. کد نهایی ما این گونه است:

```
machine("sudhanshuchauhan.domaintoHIBP",
displayName:"domaintoHIBP",
author:"Sudhanshu",
description: "Domain name to HaveIBeenPwned") {
start {
```

```
paths{
path{
run("paterva.v2.DomainToEmailAddress_AtDomain_SE")
run("sudhanshuchauhan.emailhibp")
}

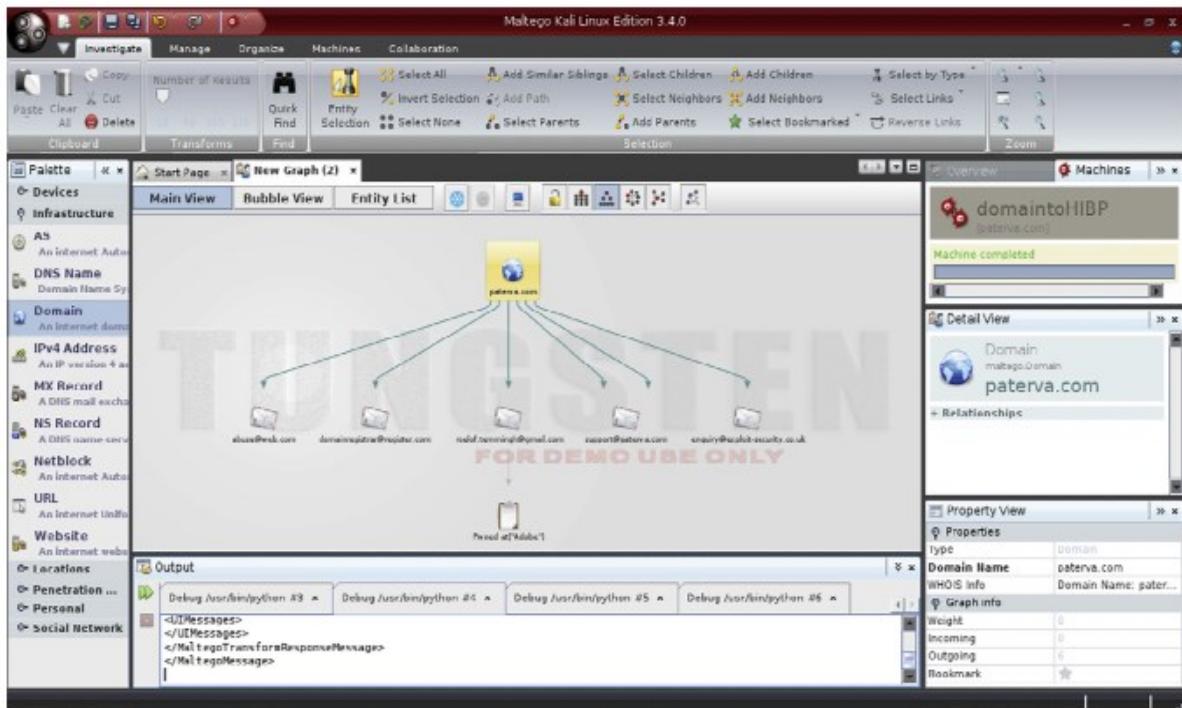
path{
run("paterva.v2.DomainToEmailAddress_SE")
run("sudhanshuchauhan.emailhibp")
}

path{
run("paterva.v2.DomainToEmailAddress_Whois")
run("sudhanshuchauhan.emailhibp")
}

path{
run("paterva.v2.DomainToEmailAddress_PGP")
run("sudhanshuchauhan.emailhibp")
}

}
}
}
}
```

دو چیز مهم که باید در نظر داشته باشید این است که transform محلی ما باید قبل از ساختن دستگاه در Maltego ثبت شود و در هنگام ایجاد یک توالی باید داده‌های ورودی و خروجی مورد توجه قرار گیرد.



بنابراین ما آموختیم که چگونه ماشین Maltego را ایجاد کنیم. اگرچه هنوز یادگیری مربوط به Maltego بسیار بیشتر است، ما تلاش کرده‌ایم که جنبه‌های مهم آن را بیان کنیم.

در این فصل در مورد ترکیب تمام دانش‌هایی که تا به حال به دست آورده‌ایم، یادگرفته‌ایم و همچنین برخی از سناریوهای نمونه‌های عملی را دیدیم. این در پروژه‌های واقعی مهم است. این فقط در مورد دانستن چیزها نیست بلکه در مورد اجرا و استفاده از آن‌ها به صورت یکپارچه با توجه به وضعیت و ایجاد یک نتیجه مفید است.

در فصل بعدی و آخر در مورد برخی موضوعات عمومی مربوط به اینترنت یاد می‌گیریم که اغلب به‌طور مستقیم یا غیرمستقیم به جمع‌آوری اطلاعات مرتبط می‌شوند. داشتن یک درک اولیه از این اصطلاحات برای هر کسی که از اینترنت برای اهداف تحقیق استفاده می‌کند، مفید خواهد بود.

فصل ۱۵: سایر موضوعات مرتبط

مقدمه

در فصل‌های قبلی موضوعات مختلفی که به جمع‌آوری و تفسیر داده‌ها کمک می‌کند را فرا گرفتیم. ما در مورد رسانه‌های اجتماعی، موتورهای جستجو، فراداده، وب‌دارک و خیلی چیزهای دیگر آموختیم. در این فصل برخی از موضوعاتی را که به طور مستقیم با OSINT ارتباط ندارند، اما به محاسبات و اینترنت و تکامل آن وابستگی دارند، بیان می‌کنیم. اگر اطلاعاتی را که در فصل‌های قبلی ارائه شده را تمرین کنید، احتمالاً با این موضوعات در جایی روبرو خواهید شد.

رمزگاری^۱

همیشه نیاز به انتقال پیام از یک مکان به مکان دیگر وجود دارد. مردم پیش از این پیام‌ها را از طریق پیام‌رسان‌ها که برای رساندن آن‌ها مسافت‌های طولانی سفر می‌کردند، می‌فرستادند. تا جایی که نیاز به انتقال امن شد. در شرایط مانند جنگ، پیامی که توسط دشمن افشاء می‌شود، می‌تواند کل وضعیت را تغییر دهد. برای مقابله با چنین سناریوهایی اختراع تکنیک‌های برای پنهان کردن پیام اصلی شروع شد، به‌طوری‌که حتی اگر پیام لو رود، کسی به جز گیرنده مورد نظر نتواند از محتوى آن مطلع شود. یکی از ساده‌ترین مثال‌ها، Caesar cipher است که در آن هر حرف با یک تفاوت موقعیت الفبایی ثابت جایگزین می‌شود، بنابراین اگر تفاوت موقعیت ۴ (به سمت

^۱ CRYPTOGRAPHY

راست) باشد، A تبدیل به D می‌شود، B تبدیل به E می‌شود و غیره. در دوران مدرن، تکنولوژی پیشرفت زیادی کرده و بنابراین تکنیک‌های رمزگذاری زیادی به وجود آمدند.

انواع رمزگاری کلید متقارن^۱

در این نوع رمزگاری هر دو طرف (فرستنده و گیرنده) از یک کلید برای رمزگذاری و رمزگشایی پیام استفاده می‌کنند. الگوریتم^۲ DES متداول‌ترین استاندارد رمزگذاری داده است، همچنین انواع مدرن آن مانند Triple DES نیز وجود دارد.

کلید نامتقارن^۳

در این نوع رمزگاری، دو کلید عمومی و خصوصی وجود دارد. همان‌طور که نام آن نشان می‌دهد کلید عمومی به طور آشکار توزیع شده اما کلید خصوصی باقی می‌ماند. کلید عمومی برای رمزگذاری پیام استفاده می‌شود در حالی که فقط کلید خصوصی می‌تواند رمزگشایی کند. این روش مشکل مهم کلید متقارن را حل کرد که نیاز به کلیدهای متعدد برای برقراری ارتباط بود. RSA نمونه خوبی از الگوریتم کلید نامتقارن است.

هش کردن^۴

به‌طور ساده، هش کردن تبدیل یک رشته کاراکتر به یک مقدار ثابت است. معمولاً هش کوچک است. برخی از معمول‌ترین الگوریتم‌های هش عبارت‌اند از: MD5، SHA1 و غیره.

کد گذاری^۵

به‌طور ساده، فرایند تبدیل یک کاراکتر به شکل دیگر به‌منظور انتقال داده، ذخیره‌سازی و غیره است، مانند ترجمه یک زبان به زبان دیگر به‌طوری که طرف دیگر می‌تواند آن را درک کند. کد گذاری‌های معمول عبارت‌اند از US-ASCII، UTF-8 و غیره.

^۱ Symmetric key

^۲ Data Encryption Standard

^۳ Asymmetric key

^۴ hashing

^۵ Encoding

تفاوت اساسی آن‌ها در این است که متن رمز شده برای تبدیل به متن ساده نیاز به کلید دارد و عمدتاً برای اطمینان از محروم‌گری پیام استفاده می‌شود. در هش کردن، متن هش شده را نمی‌توان به متن اصلی تغییر داد و به طور عمدت برای بررسی و اعتبار یکپارچگی استفاده می‌شود. متن کد شده را می‌توان با هر کلیدی رمزگشایی کرد.

هر گونه اطلاعات دیجیتالی که در دستگاه‌هایی نظیر رایانه، لپ‌تاپ، دستگاه تلفن همراه و غیره ذخیره می‌شوند، به همان اندازه اهمیت دارند. همان‌طور که این دستگاه‌ها شخصی هستند، اطلاعات نیز شخصی بوده، بنابراین باید با دقت مراقب آن‌ها باشید. هر گونه مشکل سخت‌افزاری، سوءاستفاده از نرم‌افزار و یا سرقت منجر به ازین رفتن این اطلاعات مهم می‌شود و یا با اشتباهات سهوی ازین بروود که پیامدهای آن بسیار بدتر است؛ بنابراین ذخیره‌سازی هر گونه اطلاعات مهم در فرم دیجیتال مستلزم تلاش معنی دار برای ایجاد امنیت آن است. راه حل‌های بسیاری رایگان و همچنین تجاری برای ذخیره داده‌ها به صورت امن در این دستگاه‌ها وجود دارد. هر یک از آن‌ها را بر اساس سطح اطمینان مورد نیاز از اطلاعات انتخاب کنید. به غیر از ذخیره داده‌ها به صورت امن به صورت محلی در هر دستگاه، راه حل‌های ابری برای ذخیره اطلاعات در یک مکان وجود دارد به طوری که ما می‌توانیم برای ذخیره و بازیابی از آن استفاده کنیم. هم‌زمان با ذخیره و انتقال داده‌ها توصیه می‌شود که از نسخه پشتیبان تهیه شده برای جلوگیری از دست رفتن اطلاعات، استفاده کنید. این راه حل‌ها به شدت بر اساس رمزنگاری یا رمزگذاری است. امروز اغلب به طور روزانه از تکنولوژی‌هایی مانند TLS / SSL، PGP، امضای دیجیتال، رمزنگاری دیسک و غیره استفاده می‌کنیم؛ بنابراین در اینجا می‌توان نتیجه گرفت که رمزگذاری نقش حیاتی در زندگی روزمره ما دارد تا زندگی دیجیتال یا معجازی ما را ایمن سازد.

با افزایش قدرت محاسبات توانایی افشاری پیام‌های رمزگذاری شده نیز تکامل یافته است. حملات مانند حمله بروت فورس و حمله دیکشنری به سرعت انجام می‌شوند. همچنین در الگوریتم‌ها نقاط ضعفی وجود دارند که باعث می‌شود که آن‌ها شکسته شوند. با توجه به زمان و توان محاسباتی کافی، هر متن رمزنگاری می‌تواند رمزگشایی شود، بنابراین امروزه الگوریتم‌ها تلاش می‌کنند تا این زمان را افزایش دهند که متن رمزگشایی در بعد از زمان مورد استفاده برای شکستن آن، بی‌ارزش باشد.

بازیابی / ترمیم داده‌ها

با توجه به پیشرفت‌های تکنولوژیکی، امروزه ترجیح می‌دهیم همه چیز را در قالب دیجیتال ذخیره کنیم. فردی که باید اسناد خود را ارسال کند، نمی‌خواهد از یک فروشگاه فتوکپی بازدید کند. او می‌خواهد برای یک‌بار اسکن

نسخه‌های کاغذی را انجام داده و از همان تعدادی کپی نرم‌افزاری داشته باشد. این فقط یک نمونه ساده برای درک رفتار انسان در حال حاضر است؛ ذخیره داده‌های مهم در کپی نرمال و یا به صورت دیجیتال برخی از خطرات امنیتی را ایجاد می‌کند. همان‌طور که ذکر شد، آسیب دستگاه و یا حذف تصادفی می‌تواند منجر به از بین رفتن اطلاعات مهم ما شود. ما فقط برخی اقدامات احتیاطی را آموختیم، اما اگر حذف شد چه؟

راه‌های ممکنی برای بازیابی وجود دارند. برای یک کاربر ساده، بازیابی داده تنها زمانی ممکن است که داده‌ها هنوز در سطل زباله یا سطل آشغال وجود داشته باشند، اما این کار چندان پر فایده‌ای نیست. قابلیت بازیابی اطلاعات فراتر از آن است. این به خاطر ماهیت عملکرد ذخیره‌سازی داده‌ها و عملکرد حذف سیستم عامل است. برای درک آن باید پایه اساسی ذخیره‌سازی داده‌ها یا نحوه ذخیره‌سازی داده‌ها در دستگاه‌های ذخیره‌سازی مختلف را درک کنیم.

أنواع مختلفي از دستگاه‌های ذخیره‌سازی مانند نوار، دستگاه‌های ذخیره‌سازی مغناطيسي، دستگاه‌های ذخیره‌سازی نوري و تراشه‌ها وجود دارند. نوارها به طور کلي به صورت شخصي استفاده نمي شوند، قبلًا بخشی جدایي ناپذير از سистем ذخیره‌سازی سازمانی بودند، اين امكان وجود دارد که آن را نداشته باشيد، بنابراین اجازه دهيد درباره آن صحبت نکنيم. به غير از نوار، سه دستگاه ديگر به طور گسترده استفاده مي شوند. دستگاه‌های مغناطيسي چيزی جز دستگاه‌های ديسك سخت ما نیستند که به طور معمول به عنوان هاردديسك شناخته مي شوند و تمام داده‌ها را ذخیره مي کند. هنگامی که داده‌ها را از سیستم حذف مي کنيم، سیستم عامل اطلاعات را از روی ديسك مغناطيسي حذف نمي کند، بلکه تنها آدرس را از جدول آدرس حذف مي کند. اگر چه اين مفهوم برای تمام رسانه‌های ديگر مانند ديوي دی کاملاً مشابه خواهد بود، اما به دليل استفاده از اين دستگاه‌های ذخیره‌سازی برای تهيه نسخه پشتيبان و ذخیره‌سازی عمومي، تنها بر روی هاردديسك تمرکز خواهيم داشت. همان‌طور که بحث كردیم حذف داده‌ها از سیستم به معنی حذف اطلاعات مربوط به مكان حافظه از جدول آدرس است؛ بنابراین جدول آدرس و نحوه کار آن چيست؟ اين کاملاً ساده است به طور کلي وقتی که داده‌ها را در دستگاه ذخیره مي کنيم، از حجم هاردديسك کم مي شود. مكان حافظه شروع و محل پيان داده‌ها در هاردديسك مهم است. تمام اين جزئيات حافظه در يك جدول به نام جدول آدرس ذخیره مي شوند؛ بنابراین هنگامی که برای یک داده خاص جستجو مي کنيم، سیستم جدول آدرس را بررسی مي کند تا مكان‌های حافظه اختصاص داده شده برای آن را بیابد. هنگامی که به آن مكان حافظه دست مي‌يابد، داده‌ها را برای ما بازیابي مي‌کند. به خار اينکه بعد از حذف داده‌ها، داده‌ها هنوز هم در

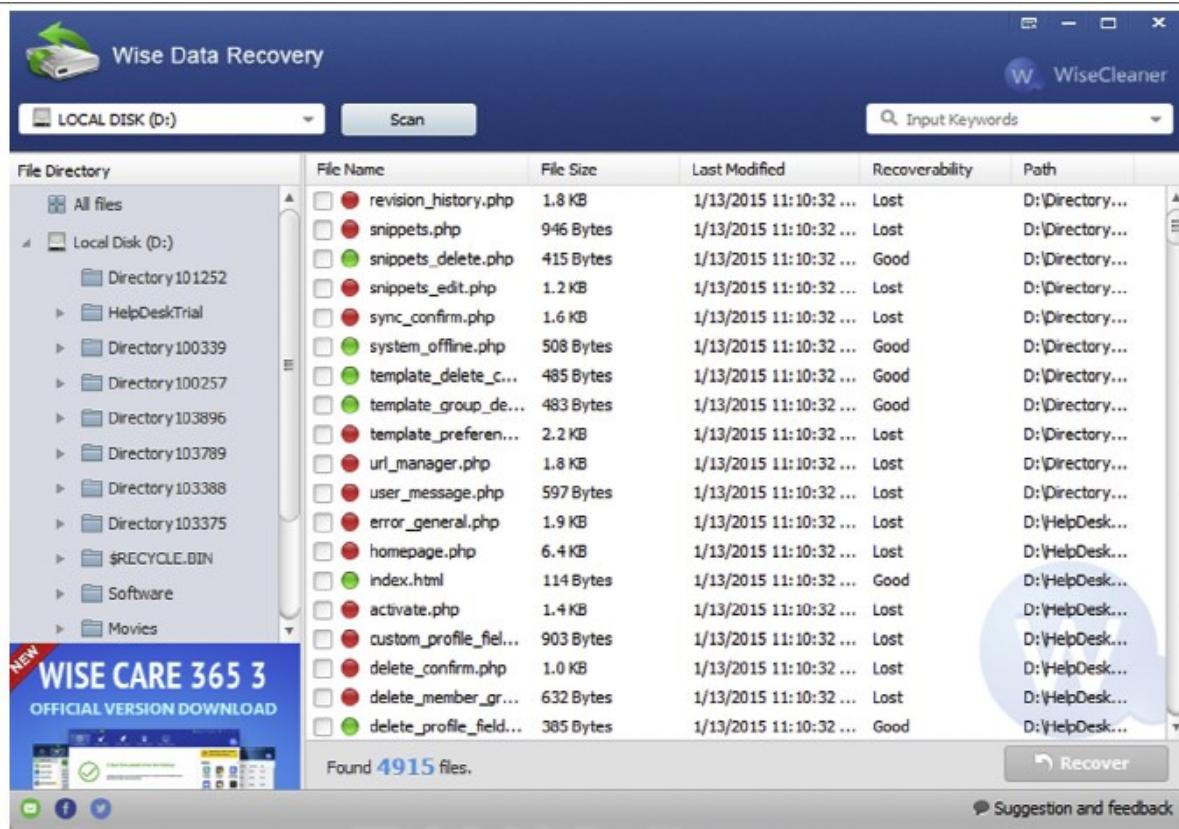
دیسک سخت وجود دارد؛ ما می‌توانیم آن‌ها را بازیابی کنیم، مگر اینکه توسط سایر داده‌ها دوباره آن را بازنویسی کنیم. در اینجا حذف کردن به معنای حذف داده‌ها از سیستم و همچنین سطل زباله است؛ بنابراین اکنون این ایده‌ای وجود دارد که چرا داده‌ها پس از حذف می‌توانند بازیابی شوند اما سؤال اصلی همچنان وجود دارد. چگونه؟ باید نگاهی به آن داشته باشیم.

ابزارهای زیادی در اینترنت وجود دارد که فایل‌های حذف شده از سیستم عامل‌های مختلف را بازیابی کند، برخی از آن‌ها رایگان و برخی از آن‌ها پولی هستند. روند بازیابی بسیار آسان است. نرم‌افزار را در سیستم عامل نصب و سپس برنامه را باز کنید. به‌طور کلی تمامی ابزارهای بازیابی با یک GUI کاربر پسند یا رابط کاربری گرافیکی عرضه می‌شوند. دستورالعمل‌های ساده را دنبال و مسیر را کامل تا داده‌ها را با موفقیت بازیابی کنید.

نرم‌افزار Wise Data Recovery یک مثال خوب از چنین ابزارهایی است که از آدرس زیر قایل دانلود است:

<http://www.wisecleaner.com/wistedatarecoveryfree.html>

نصب و استفاده از آن بسیار ساده است. درایو برای بازیابی اسکن شده را انتخاب کنید. وقتی فایلی با وضعیت بازیابی باشد، می‌توانیم آن‌ها را انتخاب و بر روی دکمه Recover در پایین سمت راست برای انجام عملیات بازیابی کلیک کنید.



اکنون می‌دانیم که گاهی اوقات ممکن است اطلاعاتی را که حذف کردہ‌ایم، بازیابی کنیم. همچنین باید بدانیم ابزارهایی وجود دارند که می‌توانند اطلاعات را از دیسک حذف کنند. یکی از این ابزار FileShredder در وب سایت <http://www.filesredder.org/> است.

INTERNET RELAY CHAT

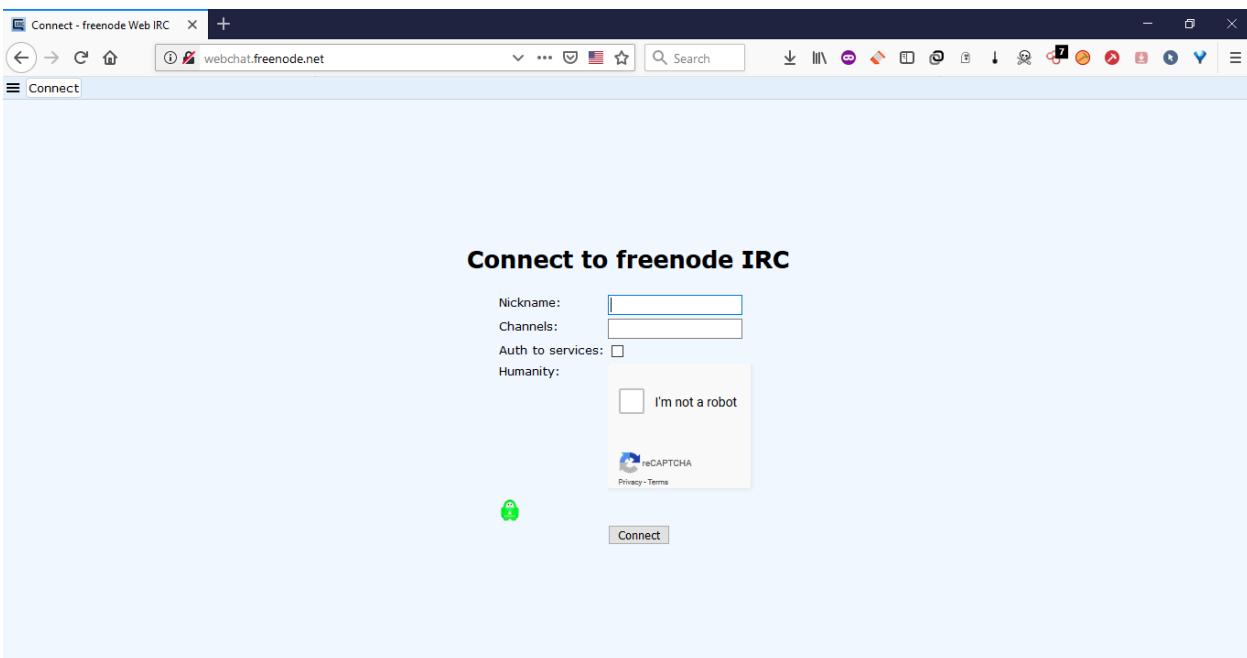
IRC یا رله چت اینترنتی مانند مدرسه قدیمی برای بسیاری است. این برنامه توسط Jarkko Oikarinen در اواخر دهه ۱۹۸۰ توسعه داده شد. اگرچه دو دهه را پشت سر گذاشت، ولی محبوبیت این برنامه هنوز هم وجود دارد. مردم هنوز دوست دارند از IRC استفاده کنند. داده‌های آماری می‌گوید که نیمی از کاربران، آن را در دهه گذشته از کنار گذاشته‌اند، اما به عنوان یک محصول قدیمی، هنوز هم مردم مایل به استفاده از آن به عنوان یک دستاورده بزرگ هستند.

IRC کاملاً مشابه هر برنامه چت دیگر است. این برنامه معماری سرور-서ویس گیرنده دارد و از پروتکل TCP برای ارتباط استفاده می‌کند. پیش از آن از ارتباط متنی استفاده می‌کرد، اما در حال حاضر TLS یا Transport Layer Security را برای ارتباط رمزگذاری شده پشتیبانی می‌کند. دلیل اصلی توسعه آن این بود که آن را به عنوان یک نرم‌افزار چت گروهی بکار ببرید. در اصطلاح عمومی ما انواع مختلف از گروه‌های چت را به عنوان اتاق چت

می‌نامیم. در IRC آن را به عنوان کanal نامیده می‌شود. برخلاف دیگر سرویس گیرندگان چت، کاربر مجبور به ثبت‌نام نیست، اما یک کاربر باید یک نام مستعار برای شروع چت فراهم کند. کاربر می‌تواند در کanal و همچنین به‌طور مستقیم با کاربر دیگری با استفاده از گزینه پیام خصوصی گپ بزند.IRC به‌طور گسترده در انجمان‌های مختلف بحث، استفاده می‌شود و ما دوست داریم هر زمان که فرصتی برای استفاده داشته باشیم از آن استفاده کنیم.

به‌طور معمول برای استفاده از IRC، باید یک سرویس گیرنده IRC را در سیستم خود نصب کنیم. سرویس گیرندگان زیادی در اینترنت و برای انواع سیستم‌عامل‌ها وجود دارند؛ بنابراین یک سرویس گیرنده را بر اساس سیستم‌عامل‌تان، دانلود کنید. هنگامی که یک سرویس گیرنده IRC را نصب می‌کنیم، به یک کanal متصل می‌شویم تا اتصال با عضو دیگر کanal برقرار شود.

فرایند چت نیز کاملاً مشابه فرایند چت معمولی است. این اساساً چت آنلاین است. یک کاربر یک پیام را در یک خط ارسال می‌کند و دیگری پاسخ خواهد داد. با توجه به ناشناس بودن آن، بیشتر هکرهای ترجیح می‌دهند از IRC استفاده کنند. سؤال اصلی اینجاست که چگونه آن در OSINT به ما کمک می‌کند. این بسیار ساده است زیرا کanal‌های مختلفی وجود دارد که ما می‌توانیم بر اساس علاقه‌مان انتخاب کنیم و پرس‌وجو خود را مطرح و از کارشناسان مختلف پاسخ بگیریم. ما باید در زمان مناسب برای بحث در مورد آنچه در دنیای سایبر اتفاق می‌افتد، باشیم. ما می‌توانیم سناریوی روشن در مورد آنچه در سراسر جهان اتفاق می‌افتد را به دست آوریم، مثلاً اگر به اندازه کافی خوش شانس باشیم، ممکن است پیش‌بینی‌های آینده را نیز داشته باشیم که کدام گروه در حال آماده شدن برای حمله انکار سرویس (DDOS) بر علیه شرکتی است، اهداف احتمالی کدام‌اند. اطلاعاتی که در اینجا دریافت می‌کیم می‌توانند برای تعیین فضای مجازی، فضای سایبری و پیش‌بینی آینده، بحث در مورد موضوع خاص و غیره باشند.. پلت فرم IRC مبتنی بر وب <http://webchat.freenode.net/> است. به سادگی نام مستعار و نام کanal را وارد و شروع به جستجو کنید.



بیت کوین^۱

هر کس به امنیت اطلاعات علاقه داشته باشد و یا رسانه‌های جهان به خصوص مجله‌های فنی را پیگیری کند باید واژه "بیت کوین" را شنیده باشد. بسیاری باید از این موضوع آگاهی داشته باشند، بنابراین درباره بعضی از واقعیت‌های مهم درباره بیت کوین صحبت خواهیم کرد. بیت کوین را می‌توان به عنوان ارز الکترونیکی و یا پول نقد دیجیتالی نامید که توسط Satoshi Nakamoto طراحی شد. برخلاف ارزهای معمولی، از یک مفهوم غیرمت مرکز به نام peer-to-peer برای معاملات استفاده می‌کند. این پروتکل مبتنی بر پروتکل رمزگاری منبع باز در قالب هش SHA-256 در فرم هگزادسیمال است. واحد کوچک‌تر یک بیت کوین به عنوان ساتوش^۲ نامیده می‌شود. ۱۰۰ میلیون ساتوش یک بیت کوین را ایجاد می‌کند. بیت کوین همچنین می‌تواند به عنوان سیستم پرداخت پنهان استفاده شود زیرا هیچ بانک، سازمان، یا فردی قدرت کنترل آن ندارد و یا آن را تحت تأثیر قرار نمی‌دهد. بیت کوین همیشه در قالب دیجیتال است و می‌تواند در یک کلیک به هر فردی در سراسر جهان منتقل شود. برای این نیز، جوانب مثبت و منفی وجود دارد. بعضی از جوانب مثبت این است که ما می‌توانیم بیت کوین را به هر ارز خارجی، مستقل از کشور تبدیل کنیم. ما می‌توانیم آن را به صورت ناشناس انتقال دهیم، از این رو در مخفی سازی بسیار محبوب است. هیچ کس نمی‌تواند، بیت کوین جعلی را ایجاد و یا آن را بی‌ارزش کند. به طور مشابه، تعداد زیادی از جوانب

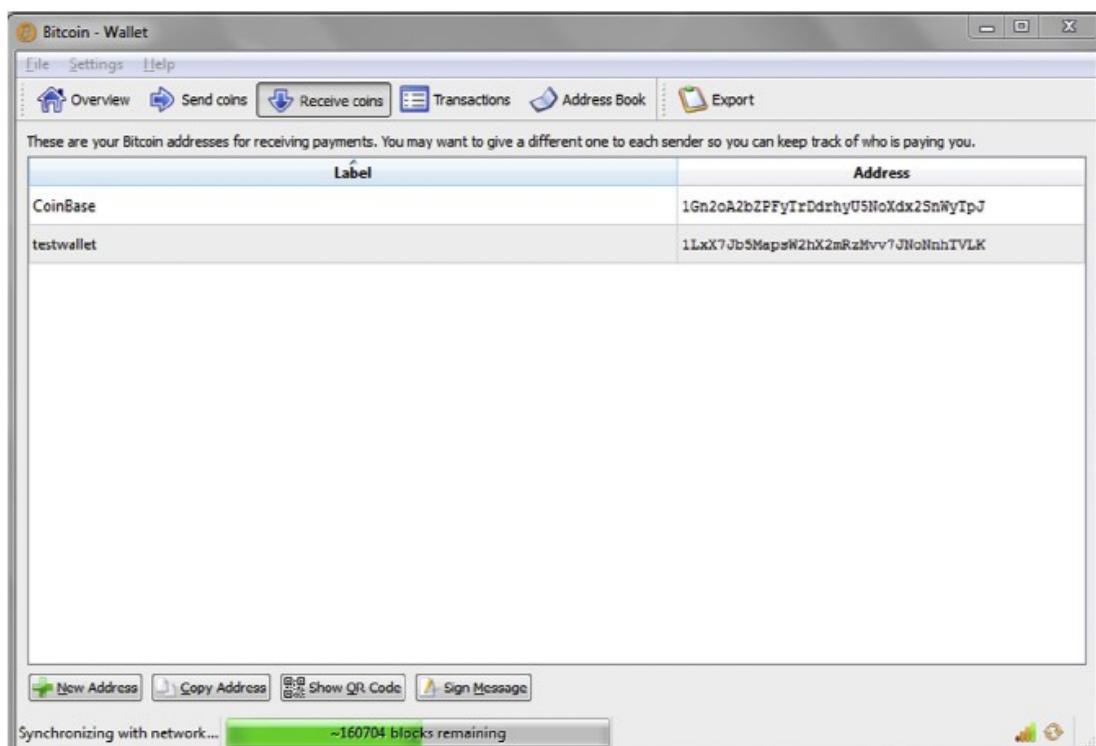
¹ Bitcoin

² satoshis

منفی دارد مانند اینکه یک معامله نمی‌تواند معکوس شود. امنیت بیت کوین کم است زیرا همیشه در فرم دیجیتال وجود دارد. هنگامی که یک پول بیت کوین پاک می‌شود، برای همیشه از بین می‌رود.

در حال حاضر ما کمی در مورد بیت کوین اطلاع یافته‌یم؛ بنابراین مهم است بدانید که چگونه آن را می‌توانید ذخیره کنید. ما می‌توانیم بیت کوین را فقط به صورت دیجیتال ذخیره کنیم، زیرا این یک داده دیجیتال است. برای ذخیره بیت کوین ما به یک کیف پول بیت کوین نیاز داریم. ضعف اصلی این است که اگر تصادفاً کیف پولمان را حذف کردیم، تمام پول را از دست می‌دهیم؛ بنابراین، در زمان‌های مناسب پشتیبان گیری کنید تا از چنین حادثه‌ای جلوگیری شود. سایت اولیه پروژه به آدرس زیر است:

<http://www.bitcoin.org/bitcoin>



همه چیز به پایان رسید. ما یک سفر طولانی به بسیاری از موضوعات داشتیم، در مورد بسیاری از ابزارها، تکنیک‌ها و روش‌های مختلف برای جستجوی اطرافمان بحث کردیم. همچنین برخی از سناریوهای و نمونه‌های مرتبط را دیدیم. همه ما امیدواریم بتوانیم بگوییم این یک تجربه یادگیری عالی بوده است. یک نکته مهم که باید در ذهن ما باشد این است که در جهان امروز "اطلاعات، قدرت است" و در قدرت مسئولیت بزرگی است. از دانش موجود در این کتاب برای اهداف اخلاقی استفاده کنید و به ایجاد یک دنیای بهتر کمک کنید.

هرگز موارد آموزش‌دهید را در مکان‌هایی که مجوز ارزیابی امنیتی آن را ندارید، تست ننمایید. تمامی مطالب ارائه شده در این کتاب جنبه آموزشی داشته و هرگونه استفاده ناصحیح از این تکنیک‌ها بر عهده استفاده‌کننده از آن خواهد بود.