DNS TÜNELLEME ARACI KULLANICI DOKÜMANTASYONU

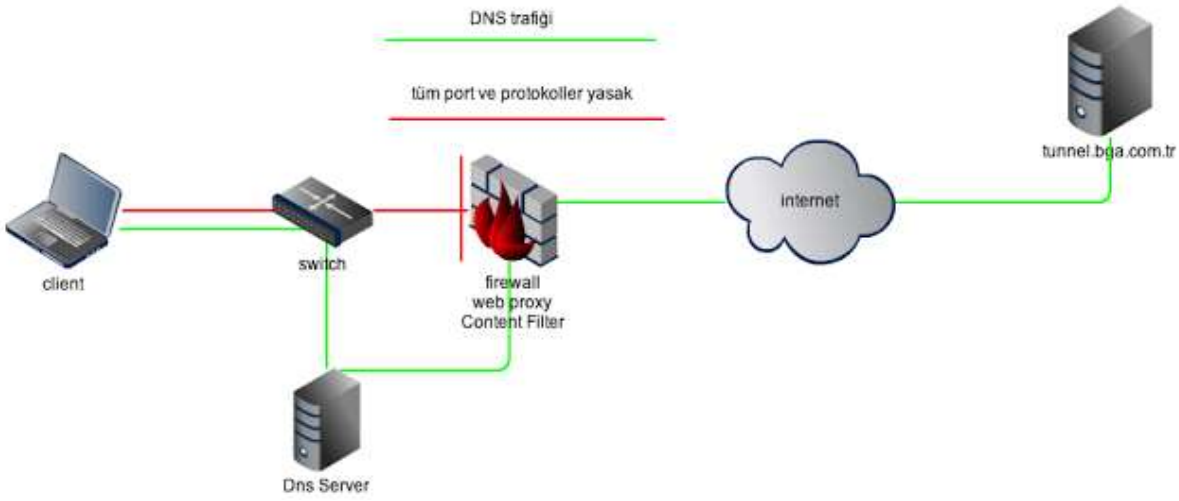
İÇİNDEKİLER

BGA DNS Tünelleme Aracı Hakkında
- Çalışma Prensibi
- Farkları
- Desteklediği Platformlar
- Bileşenler
- İletişim

Sunucu Kurulumları
- Ön Gereksinimler
- Yapılandırma Adımları
  - Sunucu Yapılandırması
  - İstemci Yapılandırması
- Form Uygulaması
- Konsol Uygulaması

BGA DNS Tunnel Aracı Hakkında

Çalışma Prensibi



DNS internetin yapı taşıdır ve kurum ağlarda yeni nesil saldırıların iletişim kanalı olarak da kullanılmaktadır. Bu araç, dns sorguları ile firewall, dlp, ips, content filter gibi sistemlere takılmadan veri kaçırma senaryolarını içerir. Yerel ağ testlerinizde, aktif ağ cihazların güvenilirliğini test ederken kullanabileceğiniz pratikliği sağlar.

Farkları

- Birden çok alan adını eş zamanlı kullanarak veri kaçırma işlemi yapabilmektedir.
- Tek yönlü veri transferi yapabilmektedir.
- Veri kaçırırken 3 farklı şifreleme yöntemi kullanabilmektedir. (bu durum tanınmasını zorlaştırır)

Desteklediği Platformlar

Windows tabanlı tüm sistemlerde çalışabilmektedir.

Bileşenleri

- **Client**: Bu uygulama, client-side çalışan ve veri kaçırma işlemleri için kullanılan console uygulamasıdır.
- **Client Form:** Bu uygulama, client-side çalışan ve veri kaçırma işlemleri için kullanılan Form uygulamasıdır.
- **Server:** Bu uygulama, server-side çalışır ve dns sorgularını yakalamak için kullanılır.

İletişim

Özellik talebiniz, hata bildirme yada destek durumlarında bilgi@bga.com.tr ile irtibata geçebilirsiniz.

Sunucu Kurulumları

Ön Gereksinimler:

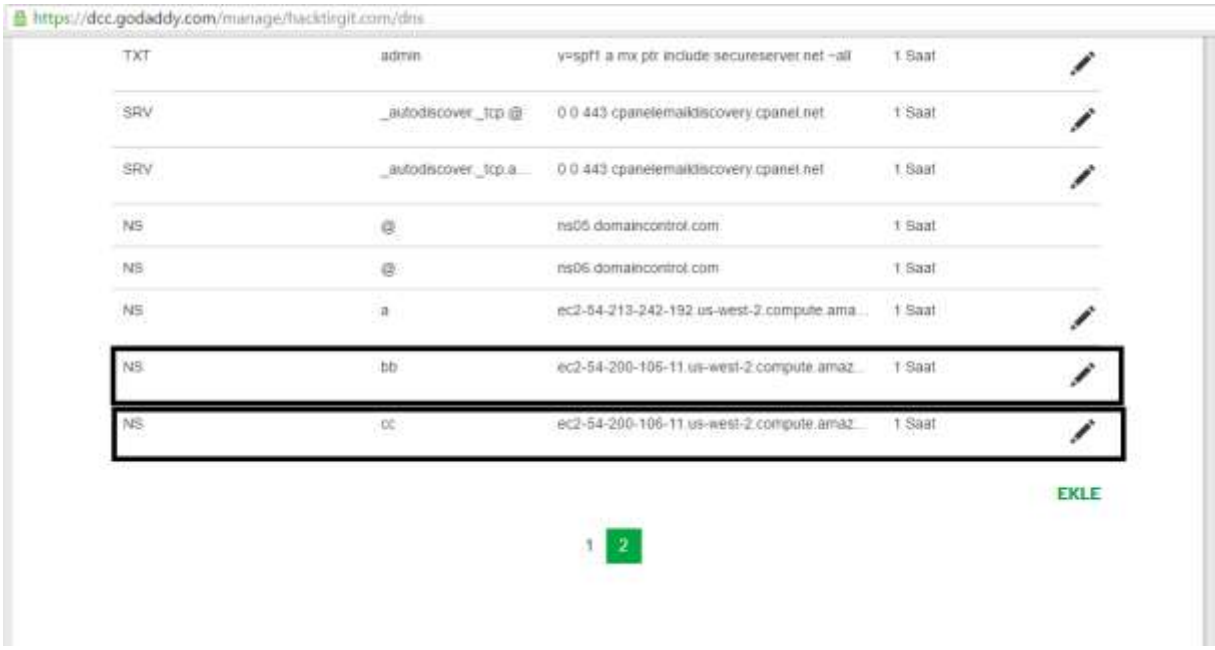
Server tarafında çalışan ve Dns sorgularını sniff eden araç için, aracı çalıştırdığımız platformda WinPcap yüklü olmalıdır ve dot net framework 4.0 üstü olmalıdır.

Kendinize ait ve dns tünelleme süresince kullanabileceğiniz alan adları.

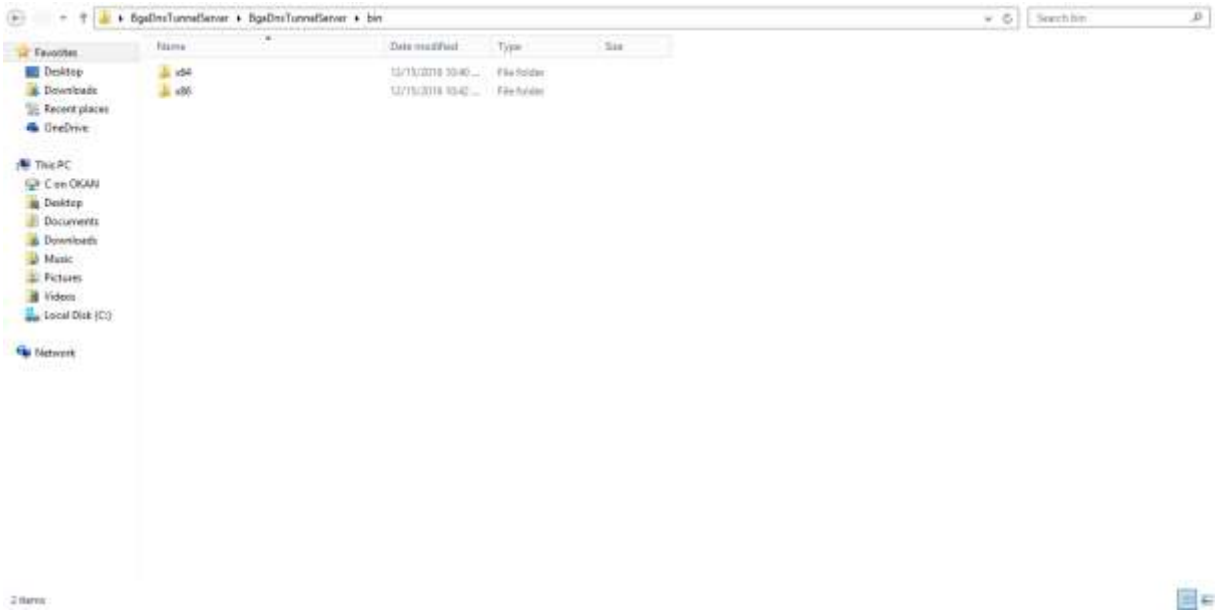
Yapılandırma Adımları

Sunucu yapılandırması

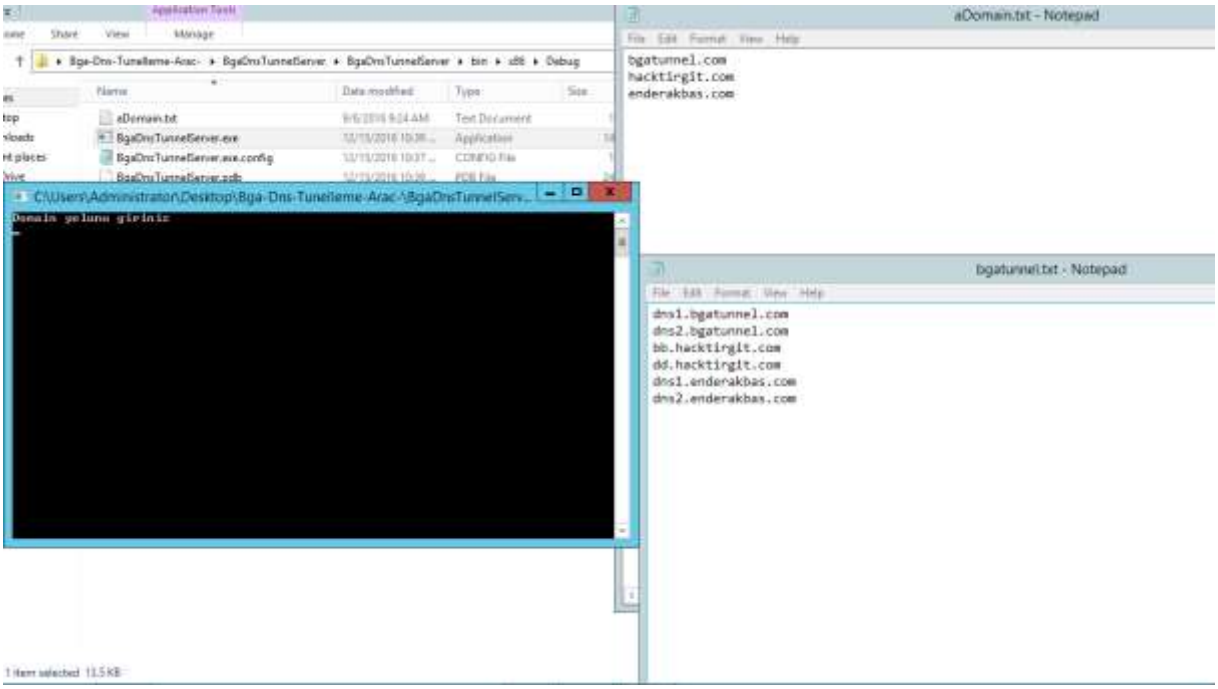
Öncelikle Dns tünelleme de kullanacağımız sub domainlerin nameserver kayıtlarını kendi sunucularımıza yönlendiriyoruz.



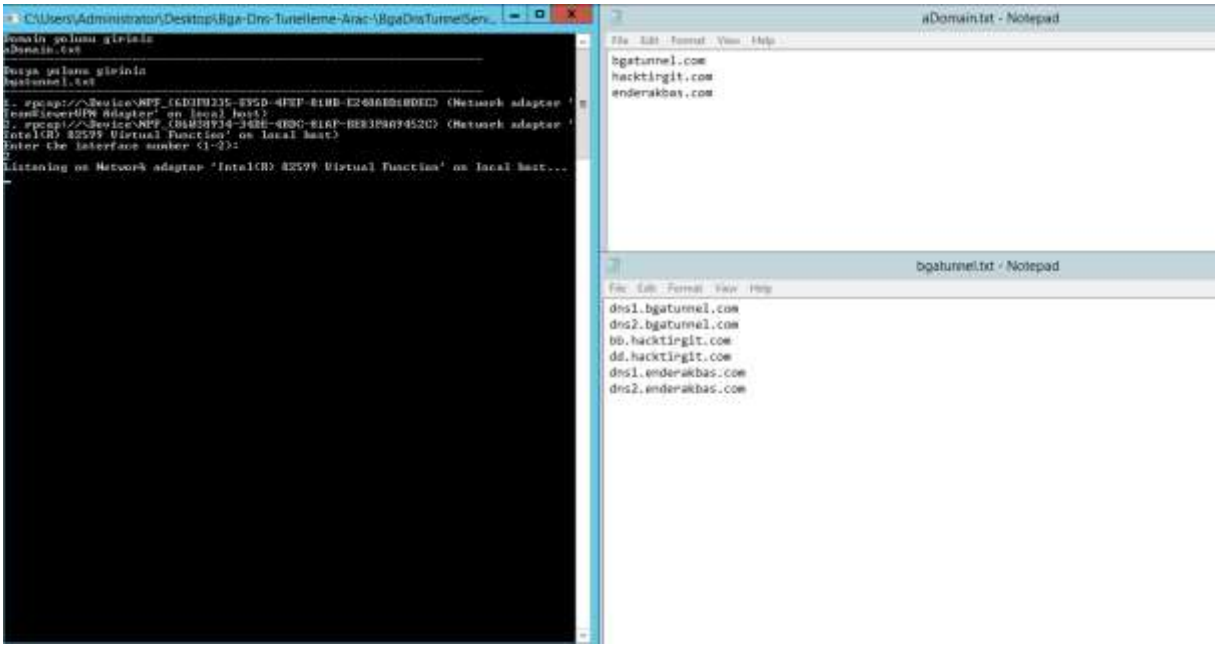
Bu işlemin ardından sunucumuz üzerinde bulunan BgaDnsTunnelServer/bin klasöründen kendi işlemci mimarimize uygun olan klasör seçimini yapıyoruz.



İşlemci mimarimize uygun olan klasöre girdikten sonra, dns tünelleme esnasında kullanacağımız domain ve subdomainleri bir .txt dosyasına kaydedip BgaDnsTunnelServer.exe programını çalıştırıyoruz. Program bir kere çalıştırıldıktan sonra tekrar çalıştırılmaya ihtiyaç duymaz. Girilen domain ve subdomain listesi dışında ki tüm bağlantılar geçersiz bağlantı olarak algılanır. Veri kaçakçılığını tanımlanan N tane farklı domaine bölerek kaçırır.



Programımız açıldıktan sonra “Domain yolunu giriniz” denilen yere domain adresimizin yazılı olduğu txt dosyamızın yolunu yazıyoruz. Hemen ardından gelen “Dosya yolunu giriniz” başlığı altına subdomainlerimizi kaydettiğimiz txt dosyasının konumunu yazıp, ardından gelen bölümde hangi ağı dinleyeceğimizi seçtikten sonra “enter’a” basıp dinleme işlemine başlıyoruz .

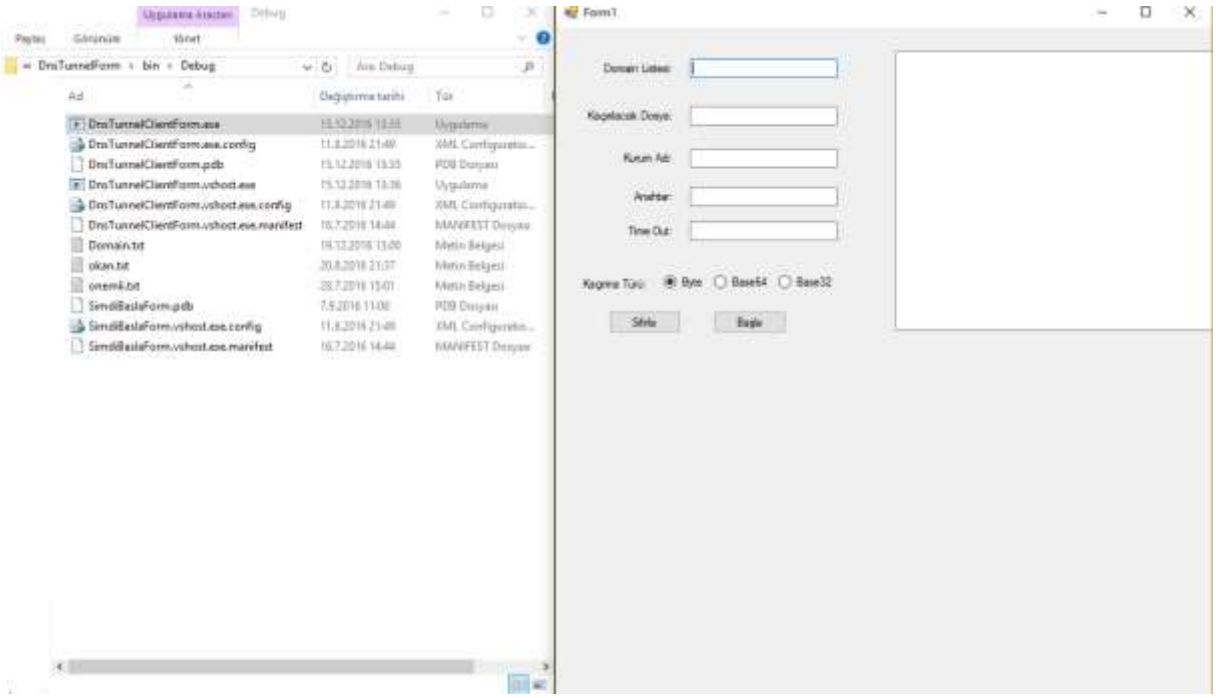


Bu işlemleri tamamladıktan sonra Client tarafında, dosya kaçırma işlemini gerçekleştirecek olan programımızı çalıştırma safhasına geçiyoruz. Bunun için Console ekranında işlemlerimizi gerçekleştireceksek DnsTunnelClient.exe, Form ekranında DnsTunnelClientForm.exe' yi çalıştıracağız.

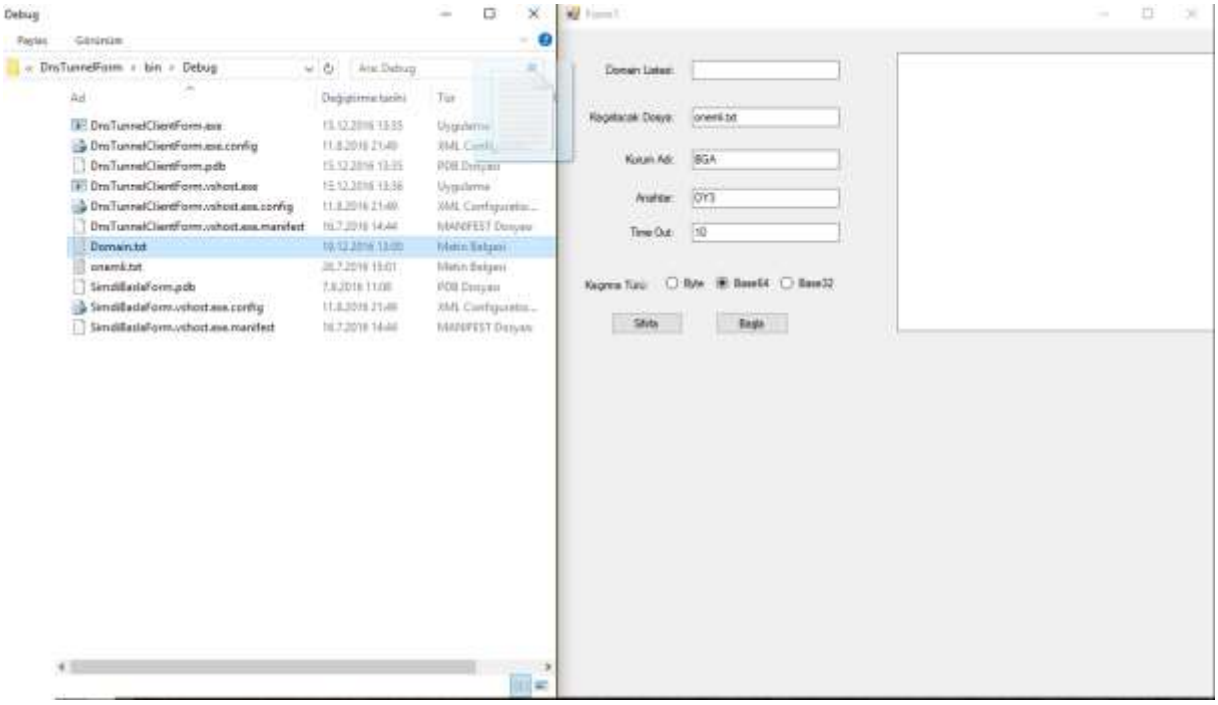
İstemci Yapılandırması

1. Form Uygulaması

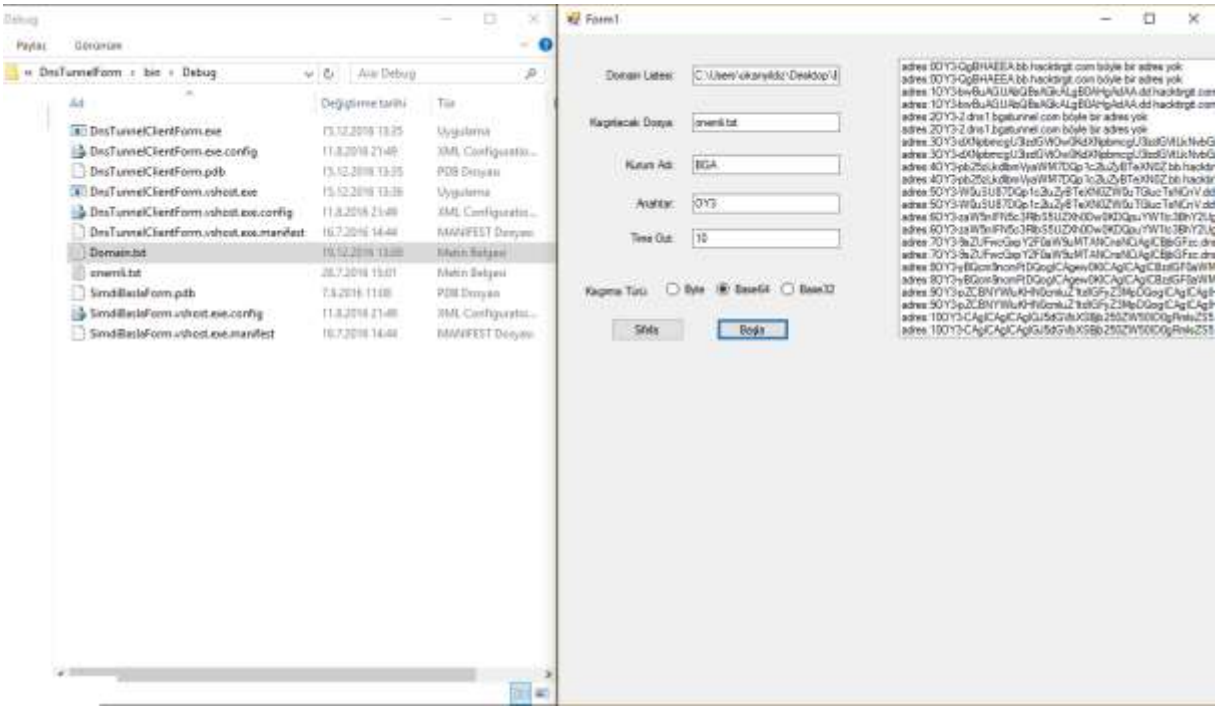
Client tarafında çalışan ve dosya kaçırma işlemini gerçekleştiren programımızın Form uygulamasını çalıştırmak için DnsTunnelClientForm.exe' yi çalıştırıyoruz.



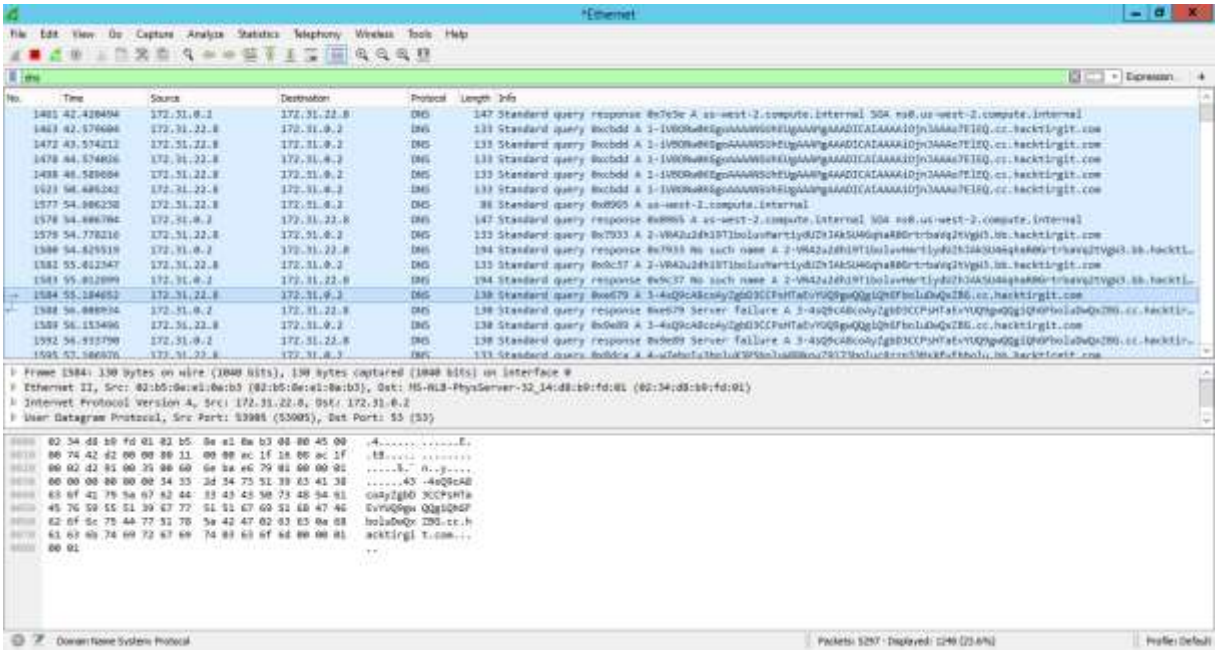
Domain listemizi oluşturduktan sonra, saldırı esnasında kullanacağımız subdomainlerin kayıtlı olduğu txt dosyasına domain listesinin yanındaki kutucuğa, saldırı esnasında kaçıracağımız dosyayı, "Kaçırılacak Dosya" kutucuğuna sürükle bırak yapıyoruz. İşlem tamamlandıktan sonra kaçırdığımız dosya kurumun adını taşıyan bir klasör içerisinde oluşturulacaktır. Time out bölümüne milisaniye cinsinden bir değer girerek programın çalışma hızını belirledikten sonra dosya kaçırma işlemi yapan kişi kendine özel bir anahtar kelime tanımlıyor.



Saldırı esnasında dosyamızı hangi türden kaçırmak istiyorsak (Byte ,Base64 veya Base32), onu işaretleyip, başla butonu ile Dns sorgularımızı oluşturuyoruz. Sıfırla butonu ile de programa önceden aktardığımız dosyaları, bellekten atıyoruz. İlk dns sorgusu console uygulamasında olduğu gibi karşı tarafta programı o dosya adıyla kaydetmek için olan dosyanın adı ve son sorgu bitti.example.com sorgusu ile programı sonlandırmak için yolladığımız özel sorgu.

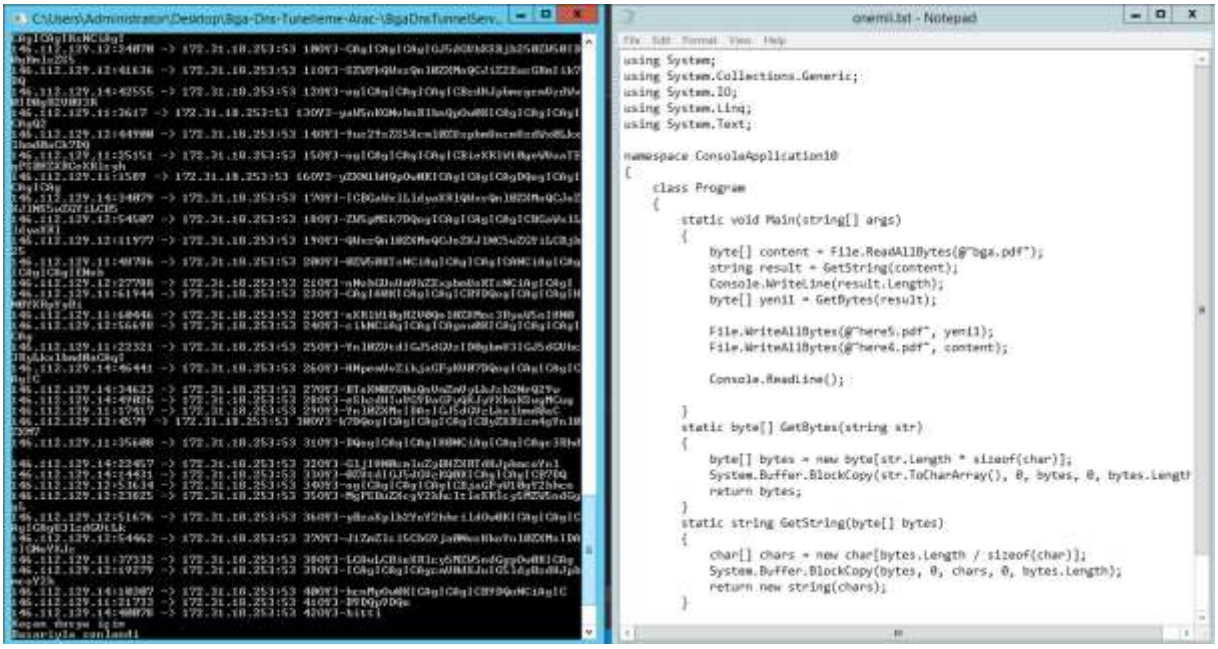


Dosya kaçırma sürecinde Client tarafında, Wireshark aracıyla yakalanan anlık trafik aşağıdaki gibidir.



Dosya kaçırma işleminde ki tüm trafiği şuradan indirebilirsiniz.

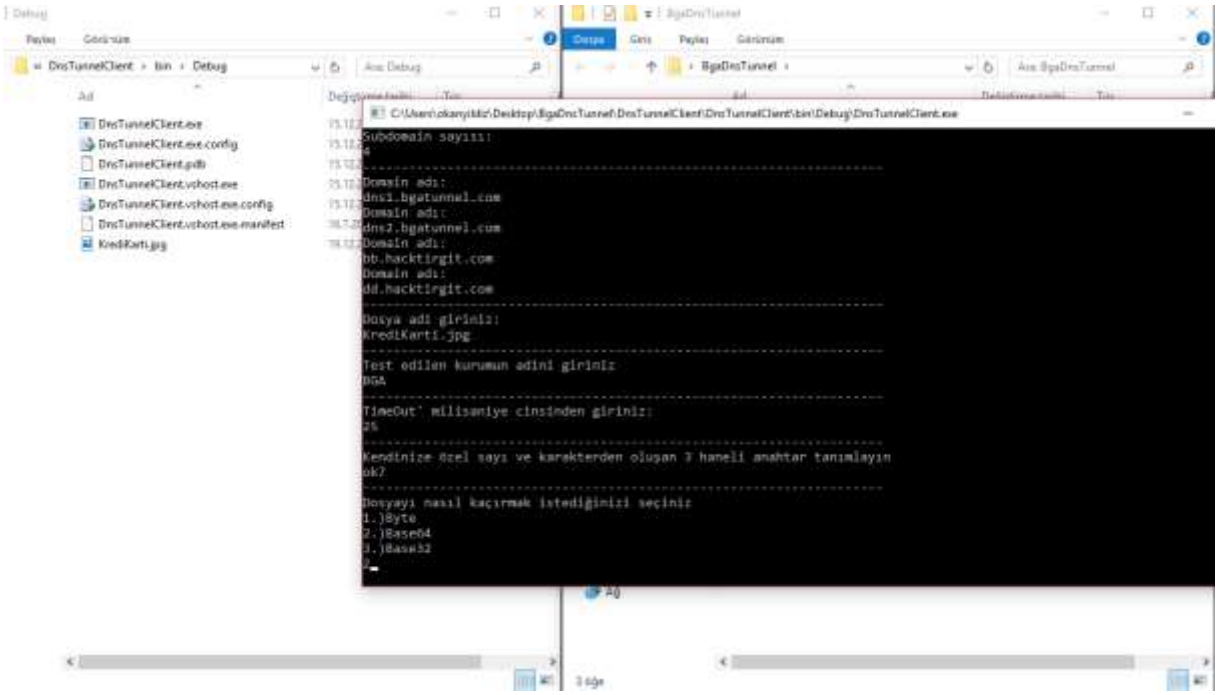
Bitti mesajını alan program, bitti mesajını aldığı master anahtardan gelen bağlantıları kendisi yorumlayarak ilgili klasör altına, kaçırılan dosyayı oluşturur.

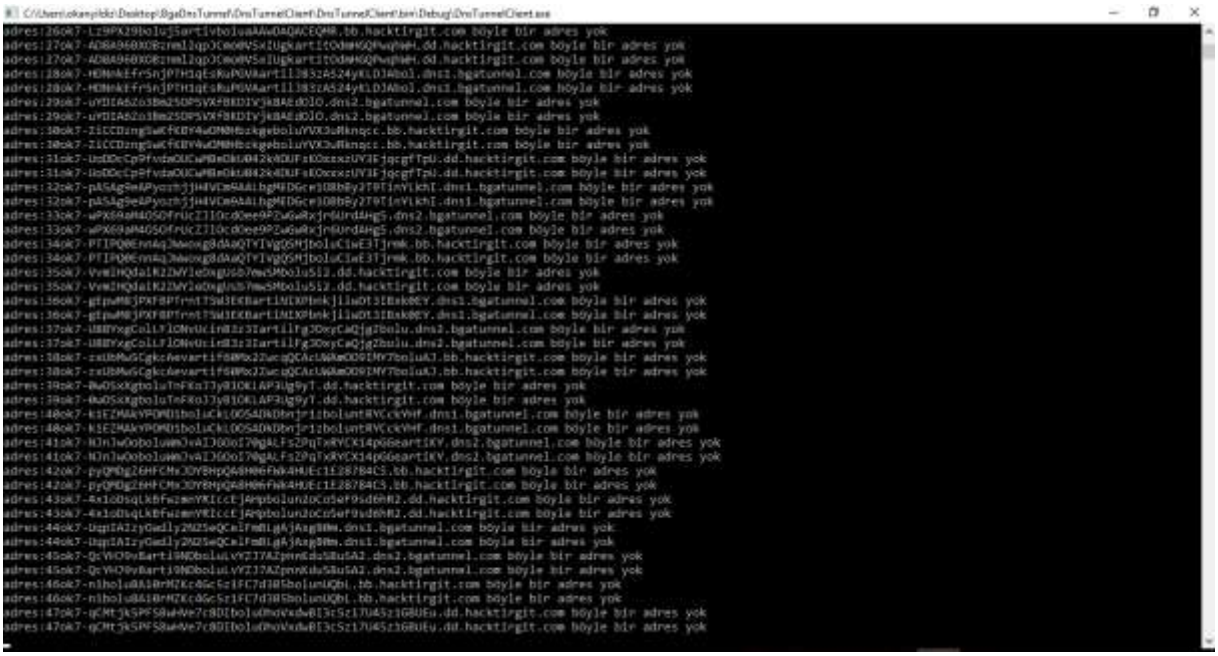


2. Console Uygulaması

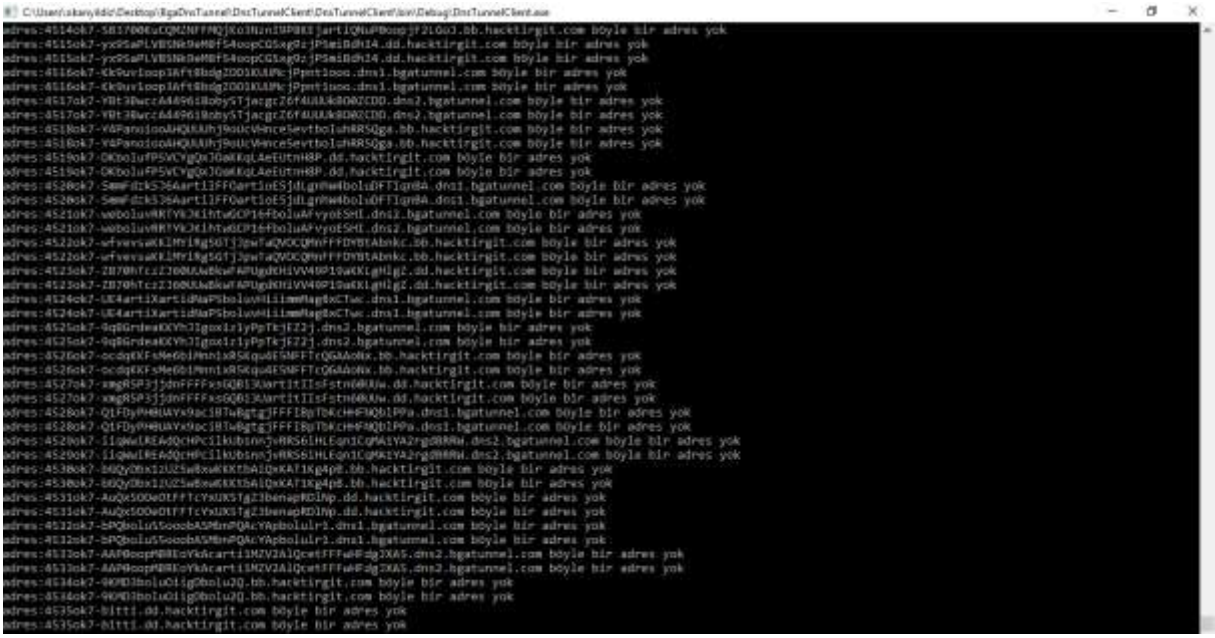
DnsTunnelClient.exe dosyasını çalıştırdıktan sonra karşımıza gelecek olan ekrandaki "Subdomain Sayısı" kısmına, saldırı esnasında kaç adet domain adresi kullanacaksak yazıyoruz. Ardından gelen "domain adı" bölümüne ise saldırı esnasında kullanacağımız subdomainlerimizin adını yazıyoruz. Bir sonraki adımda karşımıza gelen "Dosya adi giriniz" bölümünde kaçıracağımız dosyanın yolunu giriyoruz.

Örn: "C:\Users\testuser\Desktop\MuhasebeKayitlari.pdf". Bir sonraki adımda karşımıza çıkacak olan kurum adını giriniz bölümünde test ettiğimiz kurumun adını giriyoruz. İşlem tamamlandıktan sonra kaçırdığımız dosya kurumun adını taşıyan bir klasör içerisinde oluşturulacaktır. Time out giriniz bölümüne milisaniye cinsinden bir değer girerek programın çalışma hızını belirledikten sonra dosya kaçırma işlemi yapan kişi kendine özel bir anahtar kelime tanımlıyor. Bir sonraki adımda karşımıza çıkacak olan ekranda ise "Byte" ,"Base64" veye "Base32" türlerinden hangisini kullanarak dosyayı kaçıracağımızı seçip, dosya kaçırma işlemini başlatıyoruz.

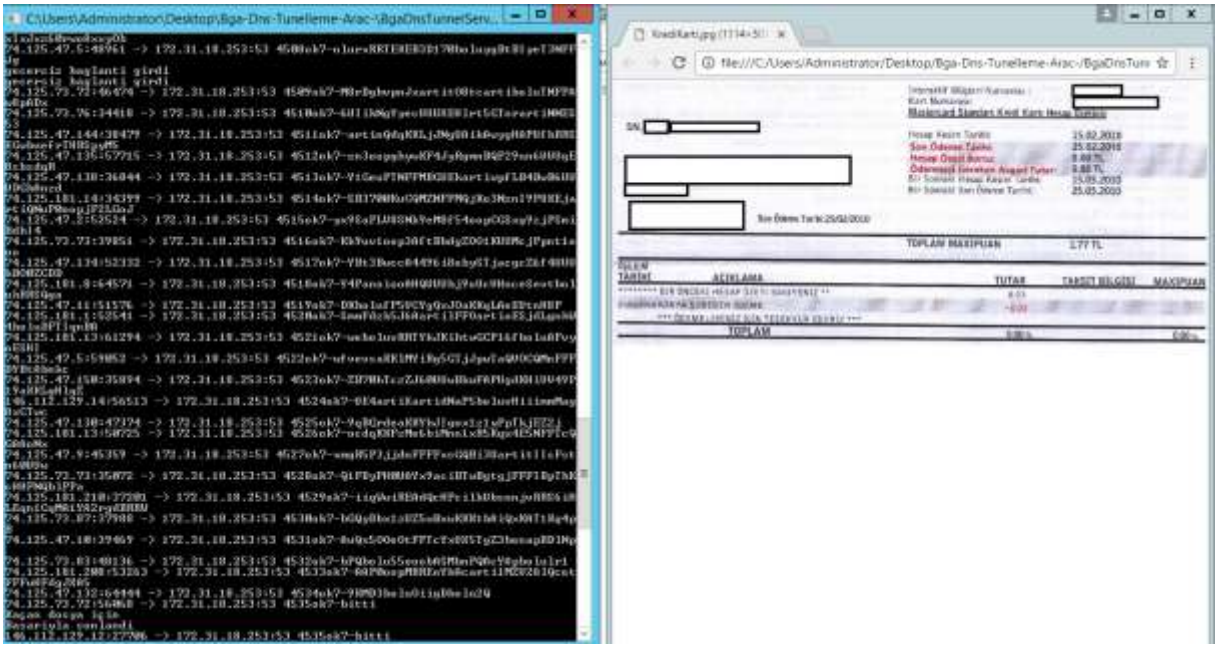




Dns sorgulama işlemleri başladığında; Sunucumuza ilk olarak kurum adı ile gelen istekler, yollanacak paketler bittiğinde programın bitti sorgusu ile sonlanacaktır.



Bitti mesajını alan program, bitti mesajını aldığı master anahtardan gelen bağlantıları kendisi yorumlayarak ilgili klasör altına, kaçırılan dosyayı oluşturur.



BGA Bilgi Güvenliği A.Ş. Hakkında

BGA Bilgi Güvenliği A.Ş. 2008 yılından bu yana siber güvenlik alanında faaliyet göstermektedir. Ülkemizdeki bilgi güvenliği sektörüne profesyonel anlamda destek olmak amacı ile kurulan BGA Bilgi Güvenliği, stratejik siber güvenlik danışmanlığı ve güvenlik eğitimleri konularında kurumlara hizmet vermektedir.

Uluslararası geçerliliğe sahip sertifikalı 50 kişilik teknik ekibi ile, faaliyetlerini Ankara ve İstanbul ve USA'da sürdüren BGA Bilgi Güvenliği'nin ilgi alanlarını "*Sızma Testleri, Güvenlik Denetimi, SOME, SOC Danışmanlığı, Açık Kaynak Siber Güvenlik Çözümleri, Büyük Veri Güvenlik Analizi ve Yeni Nesil Güvenlik Çözümleri*" oluşturmaktadır.

Gerçekleştirdiği başarılı danışmanlık projeleri ve eğitimlerle sektörde saygın bir yer edinen BGA Bilgi Güvenliği, kurulduğu günden bugüne alanında lider finans, enerji, telekom ve kamu kurul uşlarına 1.000'den fazla eğitim ve danışmanlık projeleri gerçekleştirmiştir.

BGA Bilgi Güvenliği, kurulduğu 2008 yılından beri ülkemizde bilgi güvenliği konusundaki bilgi ve paylaşımların artması amacı ile güvenlik e-posta listeleri oluşturulması, seminerler, güvenlik etkinlikleri düzenlenmesi, üniversite öğrencilerine kariyer ve bilgi sağlamak için siber güvenlik kampları düzenlenmesi ve sosyal sorumluluk projeleri gibi birçok konuda gönüllü faaliyetlerde bulunmuştur.

BGA Bilgi Güvenliği AKADEMİSİ Hakkında

BGA Bilgi Güvenliği A.Ş.'nin eğitim ve sosyal sorumluluk markası olarak çalışan Bilgi Güvenliği AKADEMİSİ, siber güvenlik konusunda ticari, gönüllü eğitimlerin düzenlenmesi ve siber güvenlik farkındalığını arttırıcı gönüllü faaliyetleri yürütülmesinden sorumludur. Bilgi Güvenliği AKADEMİSİ markasıyla bugüne kadar "Siber Güvenlik Kampları", "Siber Güvenlik Staj Okulu", "Siber Güvenlik Ar-Ge Destek Bursu" , "Ethical Hacking yarışmaları" ve "Siber Güvenlik Kütüphanesi" gibi birçok gönüllü faaliyetin destekleyici olmuştur.