



DNS TÜNELLEME ARACI KULLANICI DOKÜMANTASYONU

İÇİNDEKİLER

BGA DNS Tünelleme Aracı Hakkında

Çalışma Prensipleri

Farkları

Desteklediği Platformlar

Bileşenler

İletişim

Sunucu Kurulumları

Ön Gereksinimler

Yapılandırma Adımları

Sunucu Yapılandırması

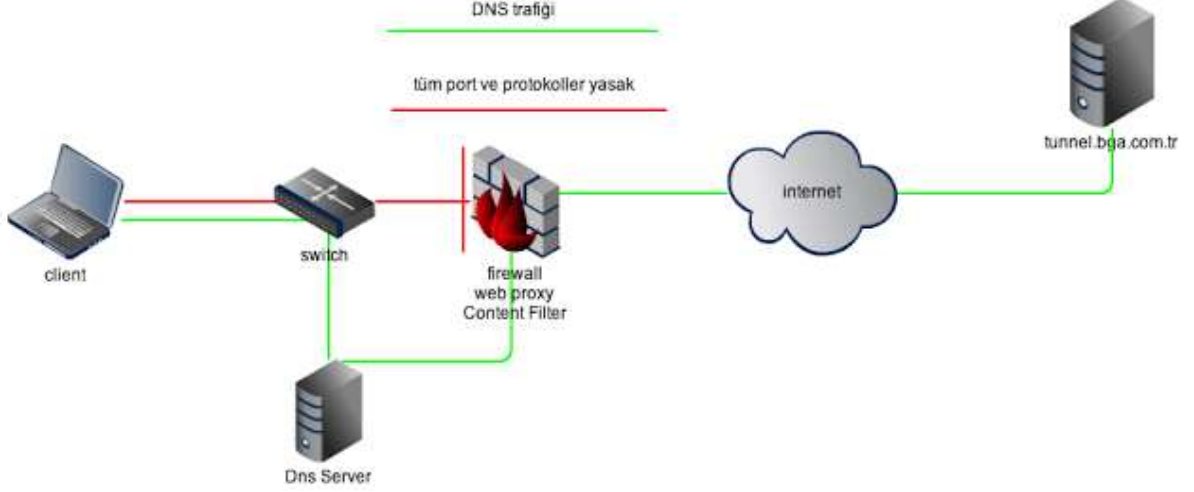
İstemci Yapılandırması

Form Uygulaması

Konsol Uygulaması

BGA DNS Tunnel Aracı Hakkında

Çalışma Prensipleri



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:

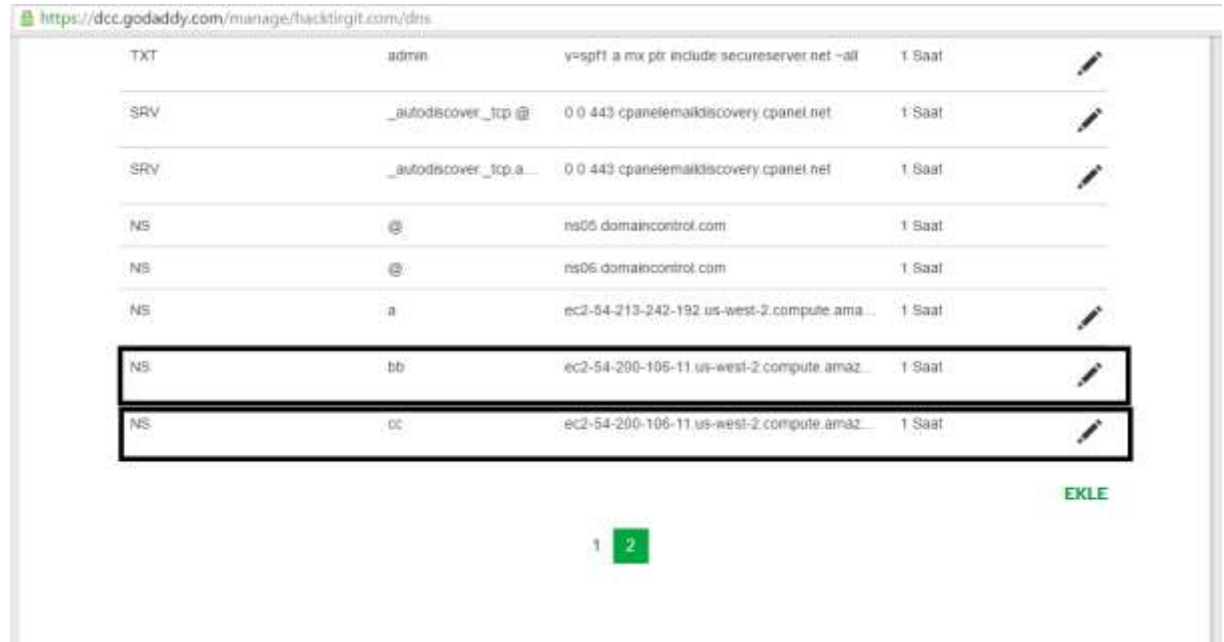
Server tarafında çalışan ve Dns sorgularını sniff eden araç için, aracı çalıştırdığımız platformda WinPcap yüklü olmalıdır ve dot net framework 4.0 üstü olmalıdır.

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.



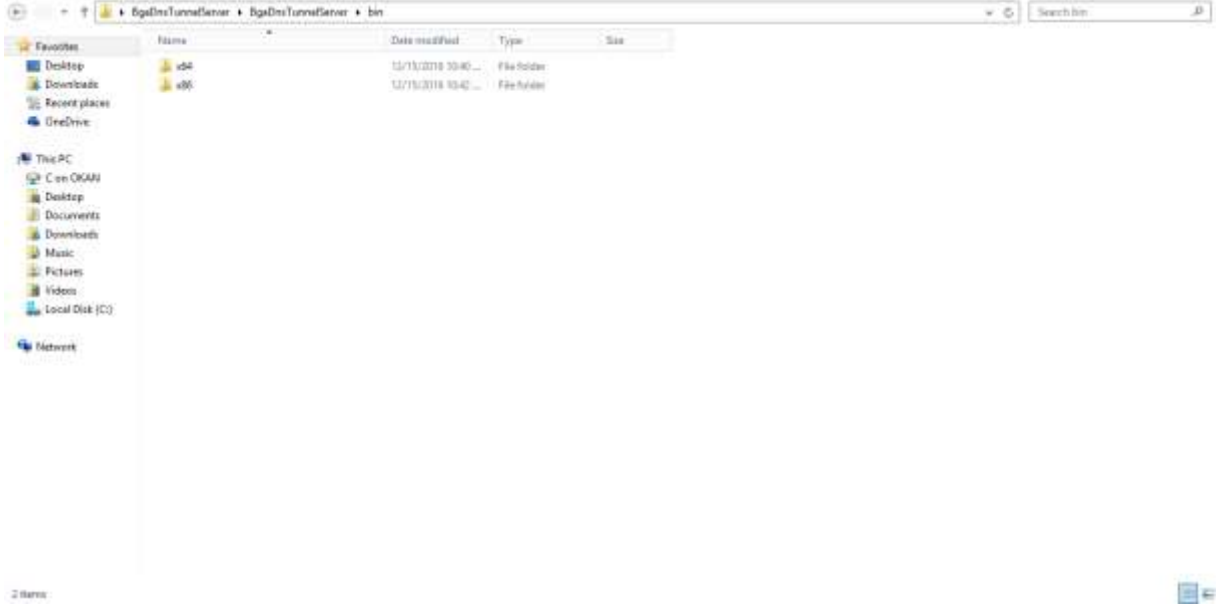
Type	Name	Value	TTL	Action
TXT	admin	y=spf1 a mx ptr include:secureserver.net ~all	1 Saat	
SRV	_autodiscover_tcp.@	0 0 443 cpanelmaildiscovery.cpanel.net	1 Saat	
SRV	_autodiscover_tcp.a...	0 0 443 cpanelmaildiscovery.cpanel.net	1 Saat	
NS	@	ns06.domaincontrol.com	1 Saat	
NS	@	ns06.domaincontrol.com	1 Saat	
NS	a	ec2-54-213-242-192.us-west-2.compute.ama...	1 Saat	
NS	bb	ec2-54-200-106-11.us-west-2.compute.ama...	1 Saat	
NS	cc	ec2-54-200-106-11.us-west-2.compute.ama...	1 Saat	

EKLE

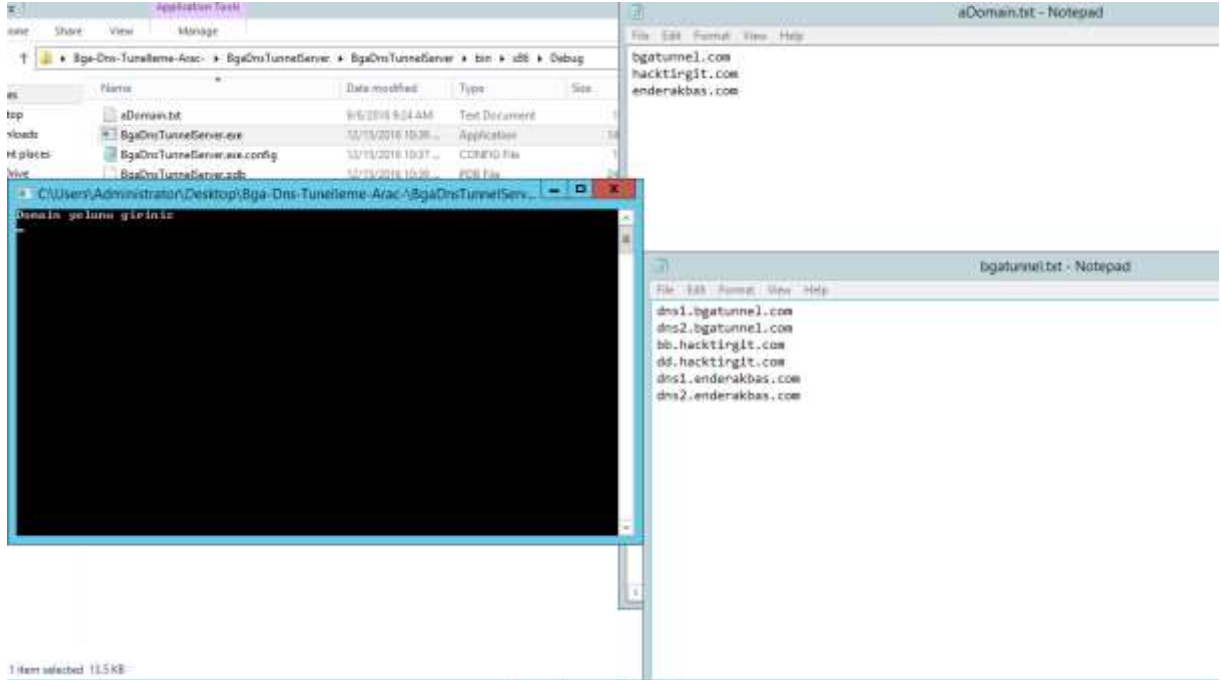
1 2

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

[DNS TÜNELLEME ARACI KULLANICI DOKÜMANTASYONU]

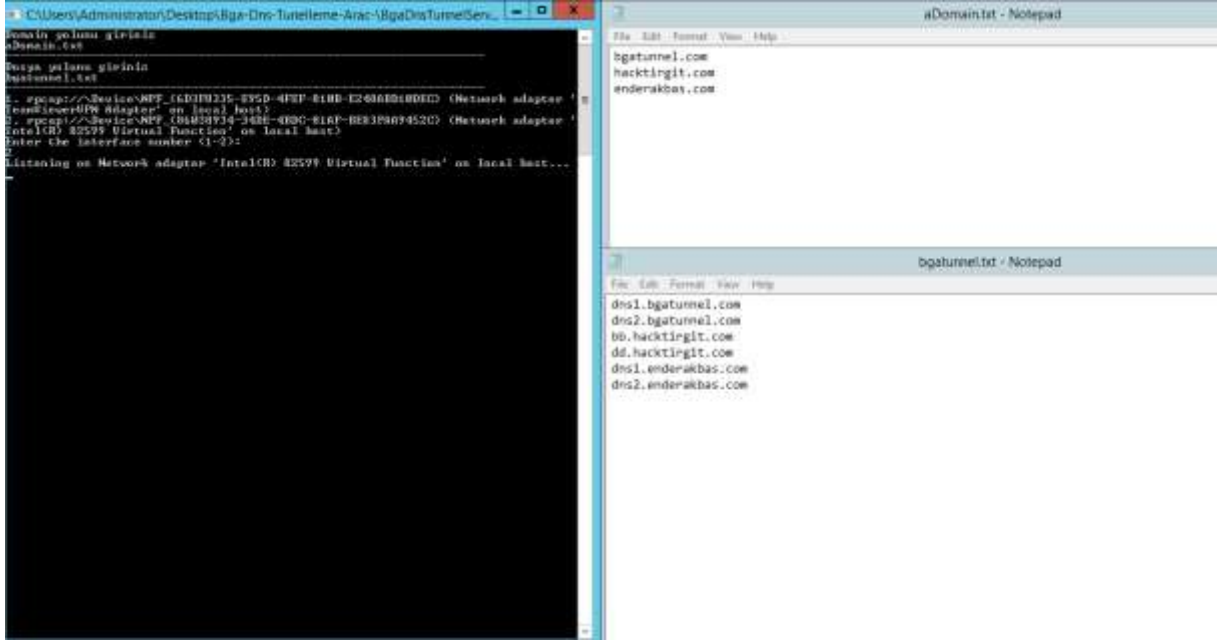


İşlemci mimarimize uygun olan klasöre girdikten sonra, dns tünelleme esnasında kullanacağımız domain ve subdomainleri bir .txt dosyasına kaydedip BgaDnsTunnelServer.exe programını çalıştırıyoruz. Program bir kere çalıştırdıktan sonra tekrar çalıştırılmaya ihtiyaç duymaz. Girilen domain ve subdomain listesi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



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 .

[DNS TÜNELLEME ARACI KULLANICI DOKÜMANTASYONU]



```
Cağrı Administrator\Desktop\Bga-Dns-Tunelleme-Araci\BgaDnsTunellemeServis...
Domain adını giriniz
adomain.test

Baya yolumuz görünün
bgaatunnel.txt

1. ipconfig /all
2. ipconfig /all
3. ipconfig /all
4. ipconfig /all
5. ipconfig /all
6. ipconfig /all
7. ipconfig /all
8. ipconfig /all
9. ipconfig /all
10. ipconfig /all
11. ipconfig /all
12. ipconfig /all
13. ipconfig /all
14. ipconfig /all
15. ipconfig /all
16. ipconfig /all
17. ipconfig /all
18. ipconfig /all
19. ipconfig /all
20. ipconfig /all
21. ipconfig /all
22. ipconfig /all
23. ipconfig /all
24. ipconfig /all
25. ipconfig /all
26. ipconfig /all
27. ipconfig /all
28. ipconfig /all
29. ipconfig /all
30. ipconfig /all
31. ipconfig /all
32. ipconfig /all
33. ipconfig /all
34. ipconfig /all
35. ipconfig /all
36. ipconfig /all
37. ipconfig /all
38. ipconfig /all
39. ipconfig /all
40. ipconfig /all
41. ipconfig /all
42. ipconfig /all
43. ipconfig /all
44. ipconfig /all
45. ipconfig /all
46. ipconfig /all
47. ipconfig /all
48. ipconfig /all
49. ipconfig /all
50. ipconfig /all
51. ipconfig /all
52. ipconfig /all
53. ipconfig /all
54. ipconfig /all
55. ipconfig /all
56. ipconfig /all
57. ipconfig /all
58. ipconfig /all
59. ipconfig /all
60. ipconfig /all
61. ipconfig /all
62. ipconfig /all
63. ipconfig /all
64. ipconfig /all
65. ipconfig /all
66. ipconfig /all
67. ipconfig /all
68. ipconfig /all
69. ipconfig /all
70. ipconfig /all
71. ipconfig /all
72. ipconfig /all
73. ipconfig /all
74. ipconfig /all
75. ipconfig /all
76. ipconfig /all
77. ipconfig /all
78. ipconfig /all
79. ipconfig /all
80. ipconfig /all
81. ipconfig /all
82. ipconfig /all
83. ipconfig /all
84. ipconfig /all
85. ipconfig /all
86. ipconfig /all
87. ipconfig /all
88. ipconfig /all
89. ipconfig /all
90. ipconfig /all
91. ipconfig /all
92. ipconfig /all
93. ipconfig /all
94. ipconfig /all
95. ipconfig /all
96. ipconfig /all
97. ipconfig /all
98. ipconfig /all
99. ipconfig /all
100. ipconfig /all

Listening on Network adapter 'Intel(R) 82579 Virtual Function' on local host...

aDomain.txt - Notepad
bgaatunnel.com
hacktingit.com
enderakbas.com

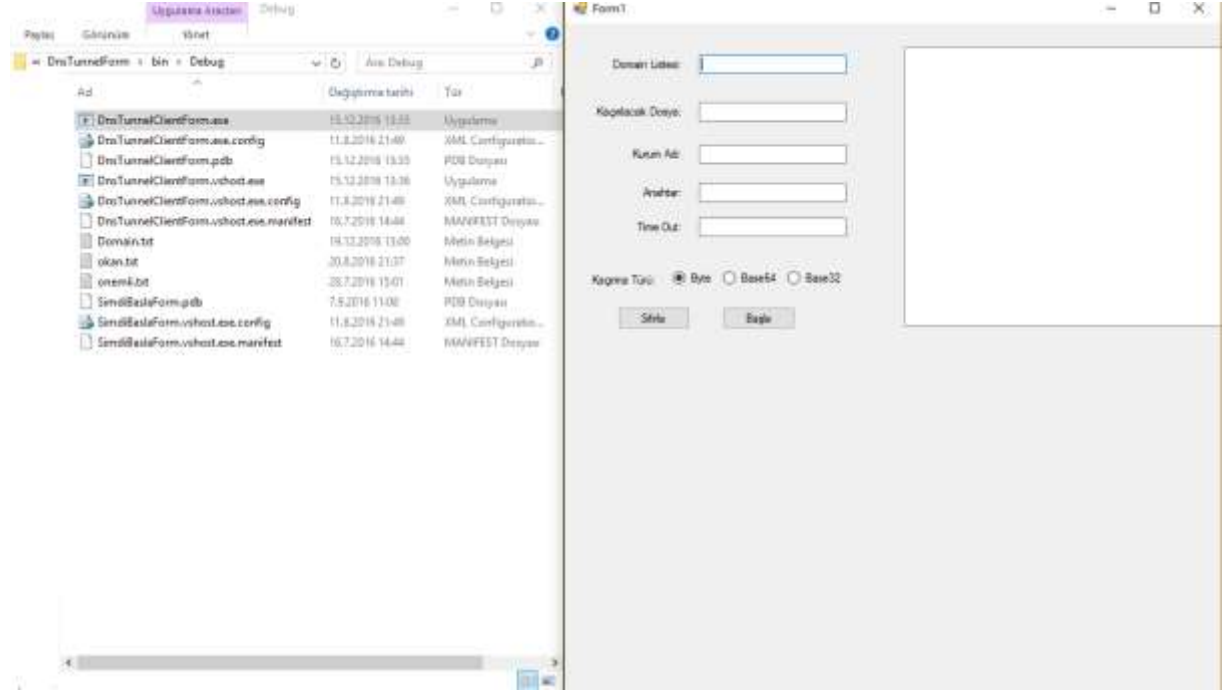
bgaatunnel.txt - Notepad
dns1.bgaatunnel.com
dns2.bgaatunnel.com
bb.hacktingit.com
dd.hacktingit.com
dns1.enderakbas.com
dns2.enderakbas.com
```

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 çalıştıracacağız.

İstemci Yapılandırması

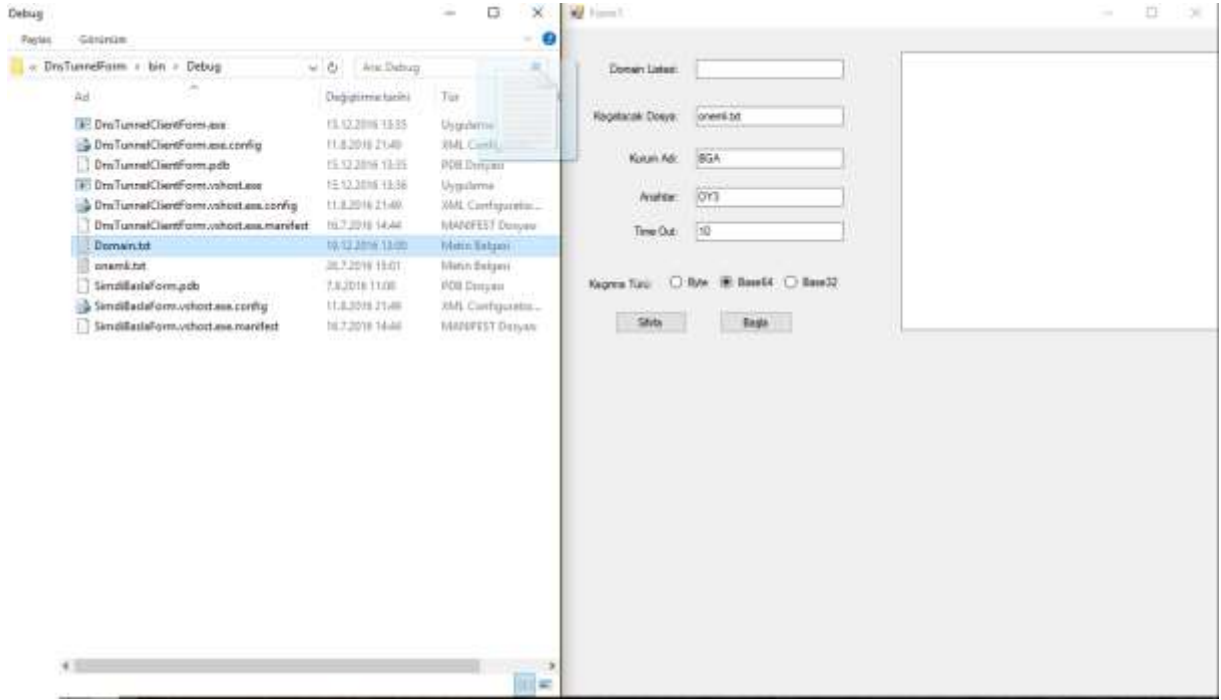
1. Form Uygulaması

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

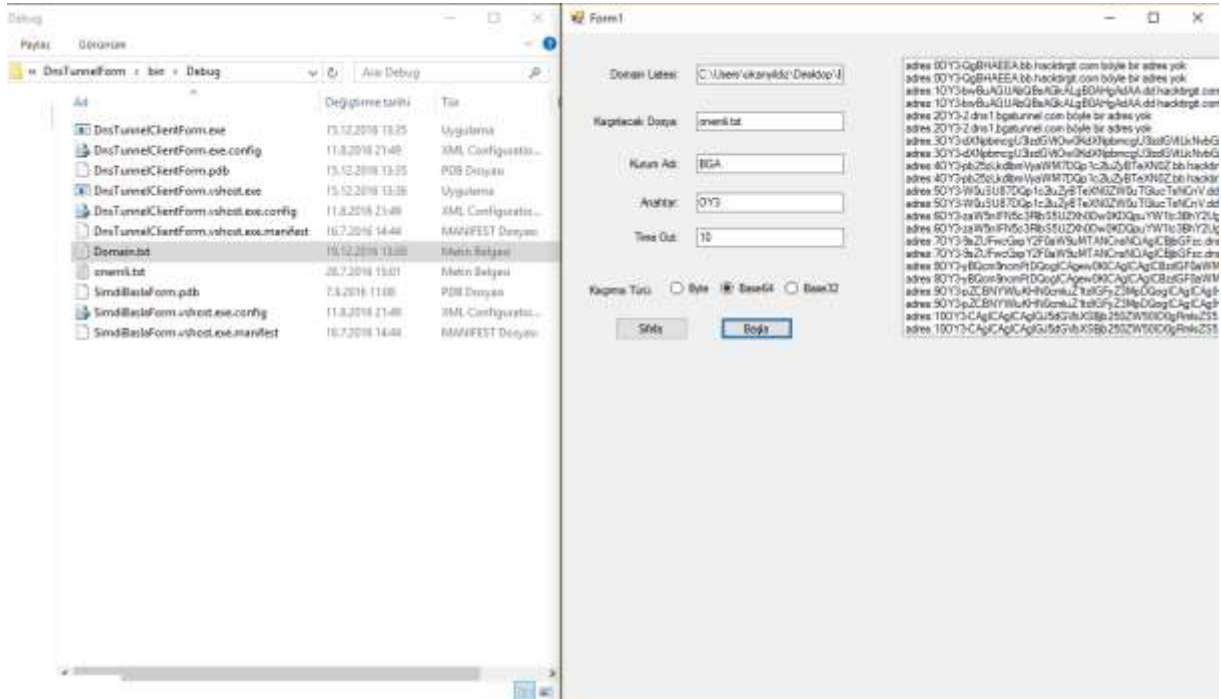


Domain listemizi oluşturduktan sonra, saldırı esnasında kullanacağımız subdomainlerin kayıtlı olduğu txt dosyasına domain listesinin yanındaki kutucuğa, saldırı esnasında kaçıracağımız dosyayı, "Kaçırılacak Dosya" kutucuğuna sürükleyip bırakıyoruz. İşlem tamamlandıktan sonra kaçıracağımız dosya kurumun 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.

[DNS TÜNELLEME ARACI KULLANICI DOKÜMANTASYONU]

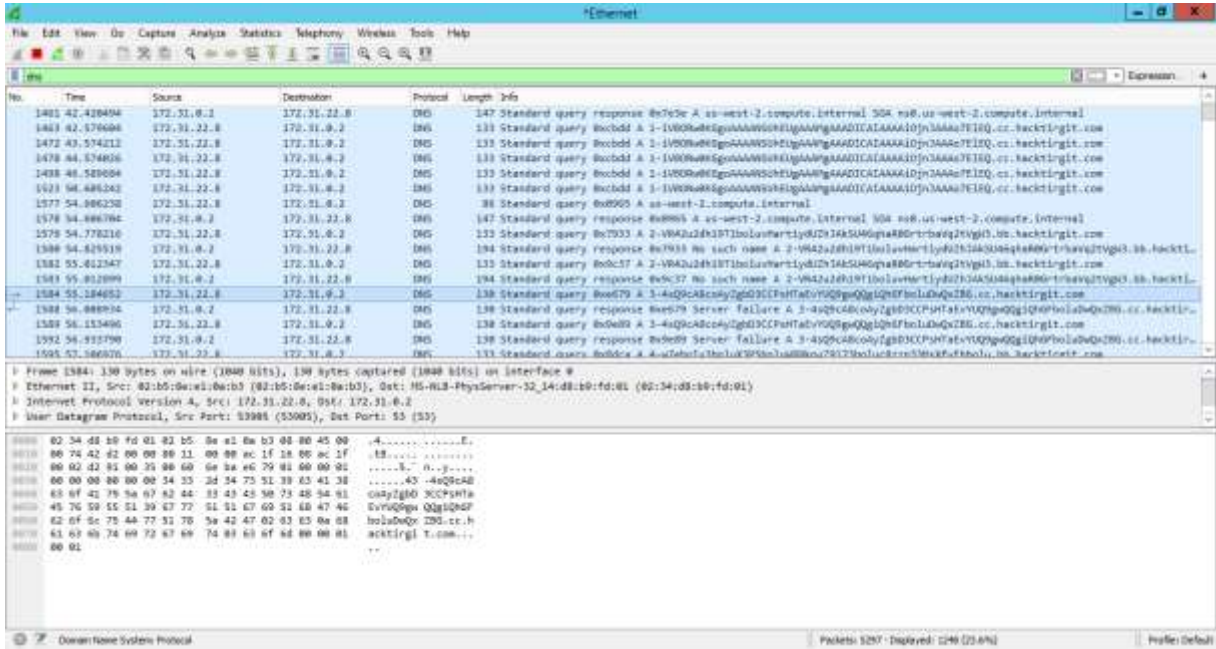


Saldırı esnasında dosyamızı hangi türden kaçırmak istiyorsak (Byte ,Base64 veya Base32), onu işaretleyip, başla butonu ile Dns sorgularımızı oluşturuyoruz. Sıfırla butonu ile de programa önceden aktardığımız dosyaları, bellekten atıyoruz. İlk dns sorgusu console uygulamasında olduğu gibi karşı tarafta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



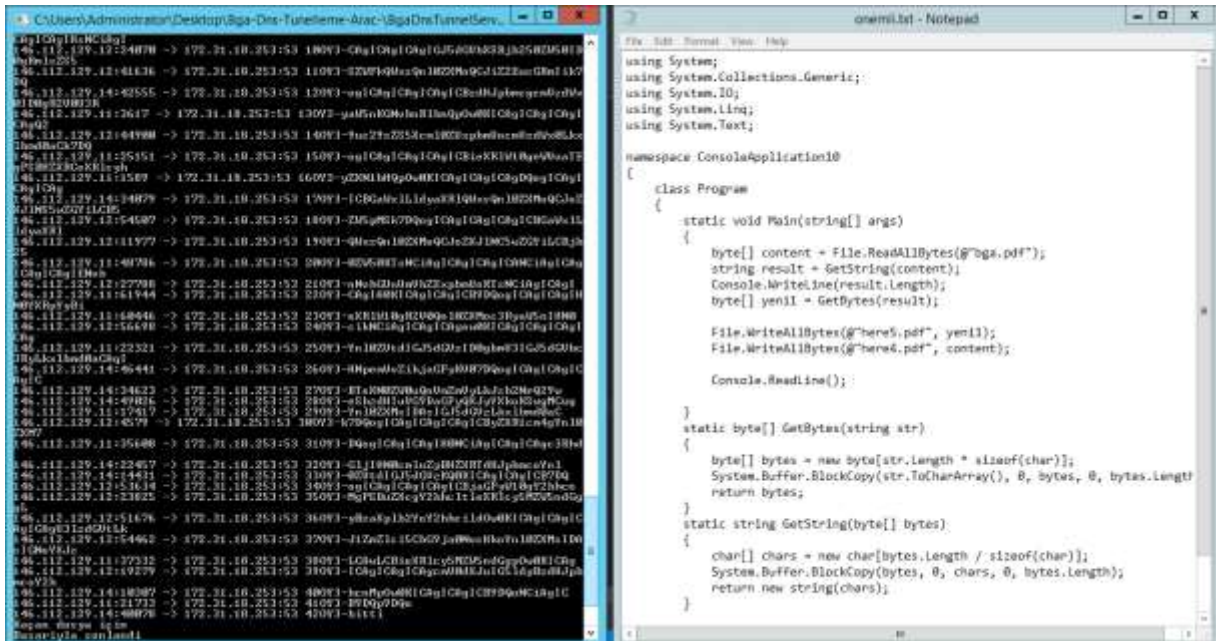
Dosya kaçırmaya sürecinde Client tarafında, Wireshark aracılığıyla yakalanan anlık trafik aşağıdaki gibidir.

[DNS TÜNELLEME ARACI KULLANICI DOKÜMANTASYONU]



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.



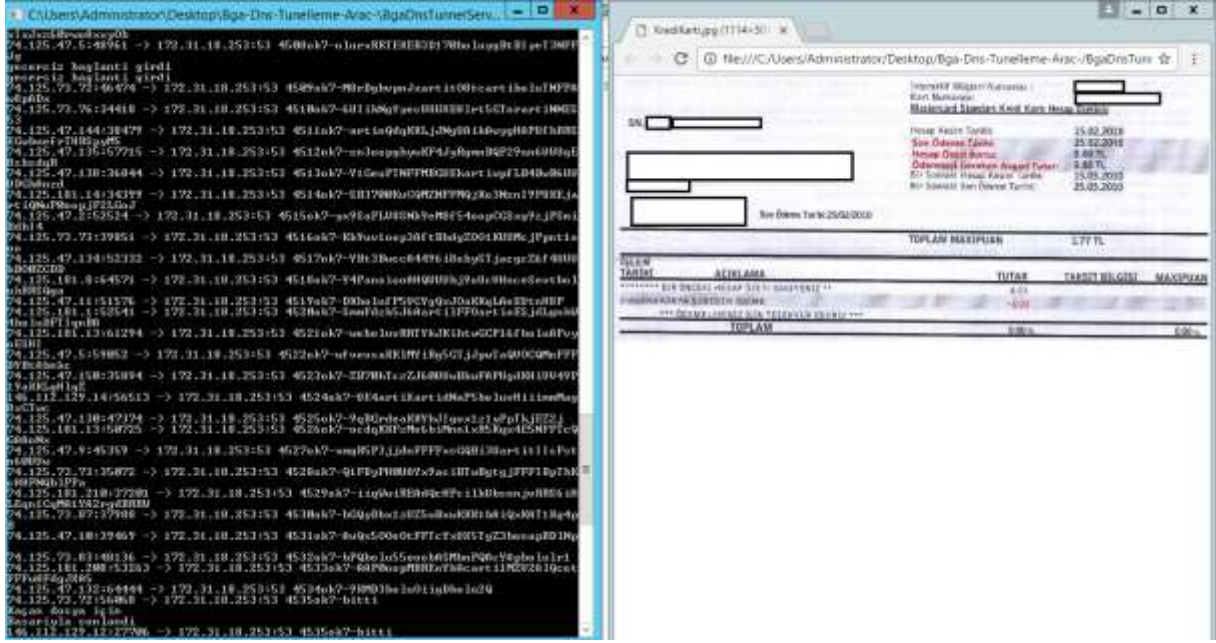
2. Console Uygulaması

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 adı 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” veya “Base32” türlerinden hangisini kullanarak dosyayı kaçıracağımızı seçip, dosya kaçırma işlemi başlatıyoruz.

```
Subdomain sayısı:
-----
Domain adı:
-----
Domain adı:
-----
Domain adı:
-----
Domain adı:
-----
Dosya adı giriniz:
-----
Test edilen kurumun adını giriniz:
-----
TimeOut' milisaniye cinsinden giriniz:
-----
Kendinize özel sayı ve karakterden oluşan 7 haneli anahtar tanımlayın:
-----
Dosyayı nasıl kaçırmak istediğinizi seçiniz:
1.)Byte
2.)Base64
3.)Base32
```


[DNS TÜNELLEME ARACI KULLANICI DOKÜMANTASYONU]



BGA Bilgi Güvenliđi A.Ş. Hakkında

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

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

Gerçekleştirdiđi başarılı danışmanlık projeleri ve eğitimlerle sektörde saygın bir yer edinen BGA Bilgi Güvenliđi, kurulduđu günden bugüne alanında lider finans, enerji, telekom ve kamu kuruluşlarına 1.000'den fazla eğitim ve danışmanlık projeleri gerçekleştirmiştir.

BGA Bilgi Güvenliđi, kurulduđu 2008 yılından beri ülkemizde bilgi güvenliđi konusundaki bilgi ve paylaşımların artması amacı ile güvenliğe-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 Güvenliđi AKADEMİSİ Hakkında

BGA Bilgi Güvenliđi A.Ş.'nin eğitim ve sosyal sorumluluk markası olarak çalışan Bilgi Güvenliđi AKADEMİSİ, siber güvenlik konusunda ticari, gönüllü eğitimlerin düzenlenmesi ve siber güvenlik farkındalıđını arttırıcı gönüllü faaliyetleri yürütülmesinden sorumludur. Bilgi Güvenliđi 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.