BÖLÜM A

1. Mekanik ve Altyapı

Promiscuous Mode (Gelişigüzel Mod): Normalde bir bilgisayarın ağ kartı sadece kendisine gelen paketleri alır. Eğer ağ üzerindeki hedef MAC adresi kendisine ait değilse bu paketi çöpe atar. Ama biz wireshark ile bütün trafiği görmek isteriz. Bu modu açtığımızda programa paket ne olursa olsun bana göster emri vermiş oluruz. Eğer kapalı olsaydı sadece kendi MAC adresine adreslendirilmiş paketleri görürdük.

Hub vs. Switch Farkı: Hub, gelen paketi her porta gönderir. Bu yüzden izlemek çok kolaydır. Switch ise MAC adres tablosu tutar ve paketi sadece hedef cihazın portuna gönderir. böylece başka kişilerin ağ trafiği gözükmez. Switch ortamında başkalarının trafiğini görebilmenin iki yolu vardır. Başkasının trafiğini görmek için ya Switch'e "bu trafiği bana da kopyala" (Port Mirroring / yasal yöntem) dersin ya da ağdaki cihazları "Gateway benim" diye kandırırsın (ARP Poisoning / saldırgan yöntemi).

Pcap vs. Log: Log özet bilgi içerir kim?, nerede?, ne zaman? gibi soruları tutar (ÖRN: Saat 10:00'da 1.1.1.1'den bağlantı geldi). Pcap ise olayın kayıt dosyası gibidir. Paketin içindeki her byte'ı saklar. Değiştirilmesi de çok zordur. Kesin delil olarak Pcap seçilir çünkü ham veridir. Log da gelen paketin içeriğini göremezsin bu da onu kesin bir kanıt olamaktan çıkarır ama Pcap'te saldırganın gönderdiği zararlı kodu veya çaldığı şifreyi bizzat görebilirsin.

2. Protokol Anatomisi

3-Way Handshake (Üçlü El Sıkışma): TCP bağlantısı insanlar nasıl konuşarak anlaşıyorsa bilgisayarlarında güvenle konuşmasını sağlayan bağlantıdır. Bağlantı kurmak isteyen bilgisayar bir SYN bayrağı gönderir. bağlantı kurulmak istenen bilgisayar bu bayrağı alır , onaylar ve SYN-ACK bayrağı gönderir. En son adımda ise ilk bilgisayar bu cevabı doğruladıktan sonra ACK bayrağı gönderilir ve bağlantı kurulmuş olur. Böylece veri akışı başlar.

Analoji:

- Alo, beni duyuyor musun? (SYN)

- Evet duyuyorum, sen beni duyuyor musun? (SYN-ACK)

- Duyuyorum, başlayabiliriz. (ACK)

TCP vs. UDP: TCP olası bir paket kaybında tekrar gönderim yapar. Herşeyi sırasına göre göderir. Yavaştır ama güvenlidir bu yüzden banka girişleri gibi öenmli ve güvenlik aerz eden işlemlerde kullanılır. UDP ise paket kaybını önemsemez ve gönderim işlemine devam eder, onay beklemez ve hızlıdır. Bu yüzden Youtube/Netflix gibi platformlarda kullanılır.

Sequence Number (Sıra Numarası): TCP, verileri parçalara bölerek gönderir. Büyük bir

dosya, mesaj veya web sayfası; bilgisayar tarafından birçok küçük pakete ayrılır. Bu paketler internet üzerinden giderken farklı yollardan ilerleyebilir, farklı sırayla hedefe ulaşabilir, bazen kaybolabilir. İşte Sequence Number tam bu yüzden vardır. Sequence Number, her paketin üzerinde yazan bir sıra numarasıdır. Bu sayede alıcı taraf paketin hangi sırada olduğıunu, eksik paket olup olmadığını, yanlış sırayla gelen varmı anlar ve ona göre düzeltme yapar. Olurda paket 5'in paket 3'den önce gelmesi gibi bir durum oluştu. Bu durumda TCP bu sıra numarasına bakar. Eksik paket var der ve eksik olanı tekrar ister. Sonrada tümünü doğru sıraya sokup uygulamaya iletir.

3. Kimlik ve Adresleme

ARP (Who has?): IP adresi bir binanın dairesi gibidir ama paketi teslim etmek için kapı numarasını (MAC) bilmek gerekir. Cihaz şunu der: “192.168.1.1’in MAC adresi kimde? Bana söyler misiniz?”. Bu bir broadcast mesajıdır: FF:FF:FF:FF:FF:FF . İlgili kişi "O benim, MAC adresim budur" der.

DHCP (DORA Süreci): DORA süreci bir istemcinin ağ üzerinde IP adresi almasını sağlayan dört aşamalı iletişim mekanizmasıdır. İstemci önce ağda bir DHCP sunucusu olup olmadığını tespit etmek amacıyla DHCP Discover yayın paketi gönderir. Bu isteği alan DHCP sunucuları, istemciye kullanılabilir IP ve yapılandırma bilgilerini içeren DHCP Offer paketini yanıt olarak gönderir. İstemci, aldığı teklifler arasından seçtiği yapılandırmyı kabul etmek için DHCP Request paketi göndererek tercih ettiği sunucuya isteğini bildirir. Son olarak DHCP sunucusu, istemcinin talebini onaylayan DHCP ACK paketini gönderir ve istemci IP adresi ile ağ yapılandırmasını resmi olarak kullanmaya başlar.

DNS (İnternetin Rehberi): Tarayıcı google.com için bir DNS çözümlemesi talep eder. Bu istek ilk önce kayıt var mı diye işletim sisteminin DNS önbelleğine bakar eğer kayıt yoksa çözümleme devam eder. Bilgisayarın ağda kullandığı DNS sunucusuna (genelde modem veya internet sağlayıcının DNS’ine) “google.com’un IP’si nedir?” diye sorar. Yerel DNS bunu bilmiyorsa, en üst seviyedeki Root DNS sunucularına gider. Root sunucuları IP’yi bilmez ama hangi uzantıya ve sunucuya bakman gerektiğini söyler. DNS sunucusu bu kez .com uzantısını yöneten TLD sunuculara sorar. TLD de “google.com’un asıl sahibi şu DNS sunucusu” diyerek yönlendirir. Son olarak Google’ın yetkili DNS sunucusuna gidilerek google.com için kesin IP adresi alınır. DNS sunucusu IP’yi bilgisayara iletir. Bilgisayarda bu IP adresini kaydeder böylece tarayıcı artık Google'ın sunucularına bağlanabilir.

4. Şifreleme ve Kör Noktalar

HTTPS ve Şifreleme: TLS/SSL katmanı veriyi şifreler bu yüzden Wireshark'ta kullancı adı veya şifreleme trafik akışında gözükmez. Wireshark’ta görebileceğimiz tek şey: IP, Port, TLS versiyonu, sertifika bilgisi, SNI(sunucu adı). Yani sadece meta-data kalır.

Man-in-the-Middle (Ortadaki Adam): MITM’in sahte sertifika sunmasının nedeni, iletişimi güvenliymiş gibi göstererek gizlice dinlemek veya değiştirmek istemesidir. HTTPS kullanan sitelerde iletişim şifreli olduğu için, ortadaki saldırgan veriyi direkt göremez.Bu şifreyi

kırmanın yolu olmadığı için, MITM, “Kendimi gerçek siteymiş gibi gösterirsem, kullanıcı bana güvenir; ben de trafiği okuyabilirim.” gibi düşünür. Bu nu yapabilmesi içinde saldıeganın sahte bir SSL/TLS sertifikası oluşturması gerekir.

5. Saldırı İmzaları

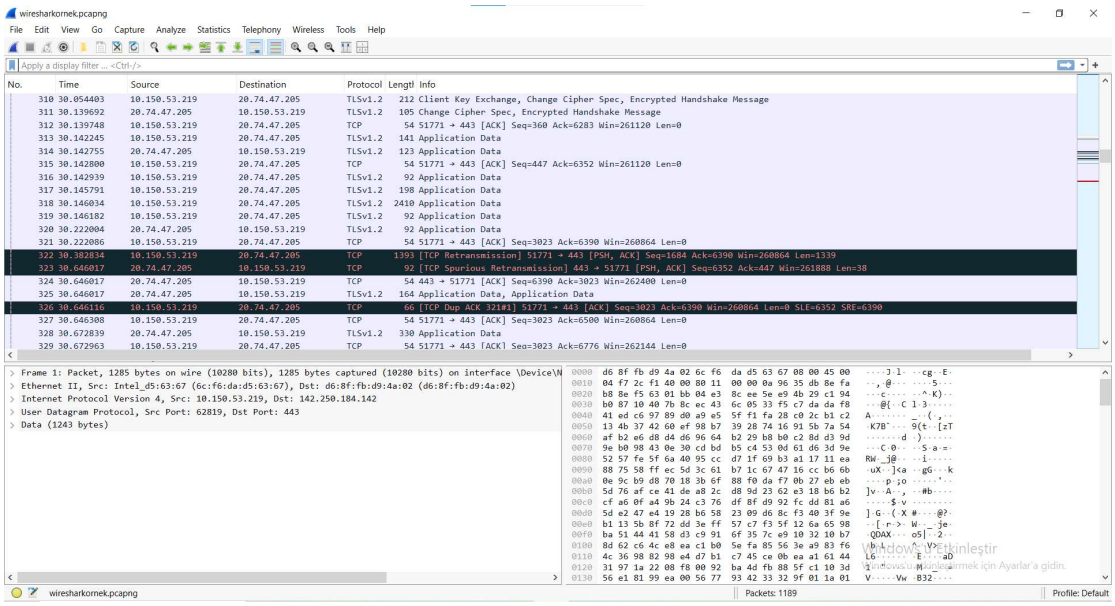
Port Taraması (Port Scanning): Normal bir kullanıcı bir siteye 1-2 posttan bağlanır ama saldırgan saniyeler içinde binlerce farklı porttan SYN bayrağı gönderir ve açık bir kapı arar. SYN gönderilir ama ACK gelmeden bağlantı kapatılır (Half-open scan). Wireshark'ta aynı IP'den gen binlerce SYN pakedi görmek port taraması yapılmaya çalışıldığının göstergesidir.

Denial of Service (DoS): Bir sistem SYN bayrağı yollayıp karşı taraftan SYN-ACK (ACK) ve ACK bekler geri dönüşü alana kadar yarım açık bağlantı sayılır(backlog queue). Bu yarım açık bağlantıların bir sınırı vardır saldırganda bunun farkında olduğu için aynı anda 100.000 tane SYN gönderir. Bu SYN'ler geri dönüş almadığı için yarım açık bağlantı kuyruğuna girerler. Yarım açık bağlantı kuyruğunun sınırına ulaşınca sistem kendini kilitler. Böylece yeni gelen bağlantılar da açılmaz.

BÖLÜM B

1. Arayüz ve Renkler

Soru 1



En üstte bulunan Frame başlığı, paketin yakalandığı zamana ve toplam boyutuna ilişkin genel bilgileri gösterir.

Ethernet II başlığı altında kaynak ve hedef MAC adresleri görülmektedir. Bu bilgiler OSI

modelinin 2. katmanı olan Data Link Layer'a aittir ve fiziksel ağ içerisindeki cihazların donanımsal adreslerini temsil eder.

Internet Protocol (IPv4) başlığı altında ise kaynak ve hedef IP adresleri yer almaktadır. Bu bölüm OSI modelinin 3. katmanı olan Network Layer'a karşılık gelmektedir ve paketlerin ağlar arasında yönlendirilmesnii sağlar.

Transmission Control Protocol (TCP) başlığı altında kaynak port, hedef port, sequence number ve bayrak bilgileri bulunmaktadır. Bu katman OSI modelinin 4. katmanı olan Transport Layer'a aittir ve uçtan uca güvenilir iletişimi sağlar.

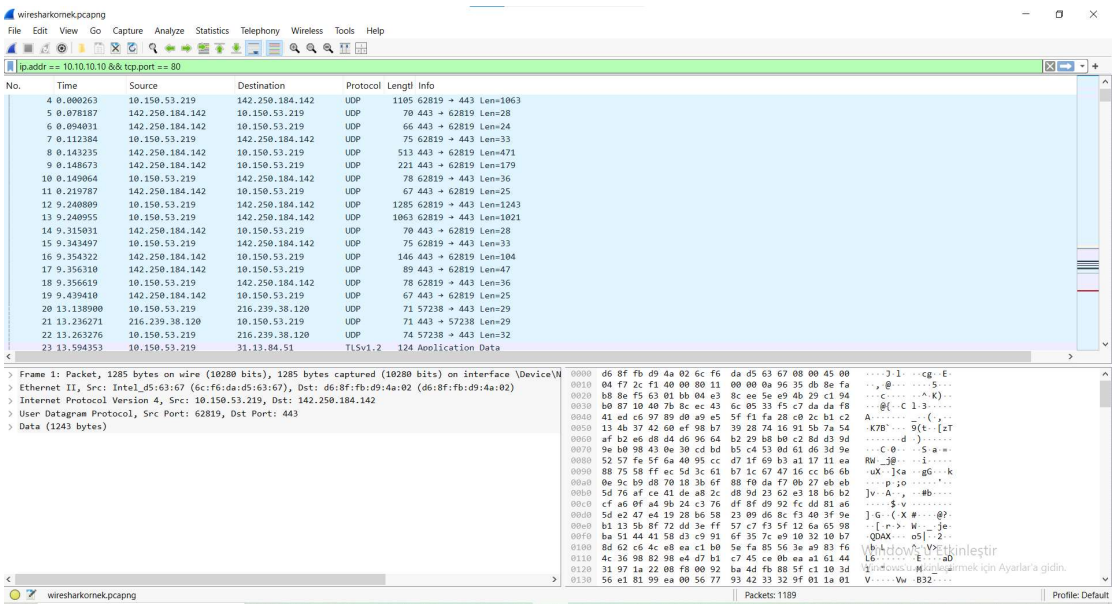
Soru 2

Wireshark'ta renkler analistlerin en büyük yardımcılarındandır binlerce paket arasından sorunlu olanları hemen fark etmemizi sağlar. Siyah ve kırmızı renkler ağdaki anomalileri temsil eder. Siyah paketler genellikle paket kaybı ve yeniden iletim (Retransmission) sorunlarını gösterir. Kırmızı paketler ise bağlantı hatalarını veya sıfırlamalarını (Reset) işaret eder. Analist için bu renkler, derinlemesine inceleme yapılması gereken sorunlu bölge demektir.

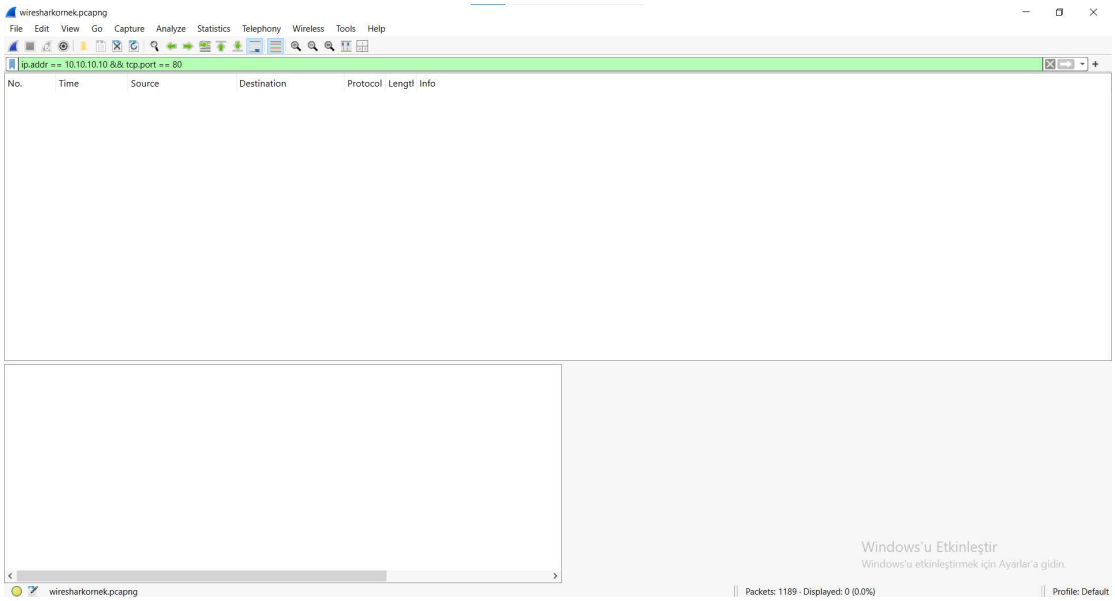
2. Filtreleme Sanatı

Sadece IP adresi 10.10.10.10 olan VE (AND) portu 80 olan paketleri görmek için filtreleme yerine yazmamız gereken filtre komutu ip.addr == 10.10.10.10 && tcp.port == 80 'dır.

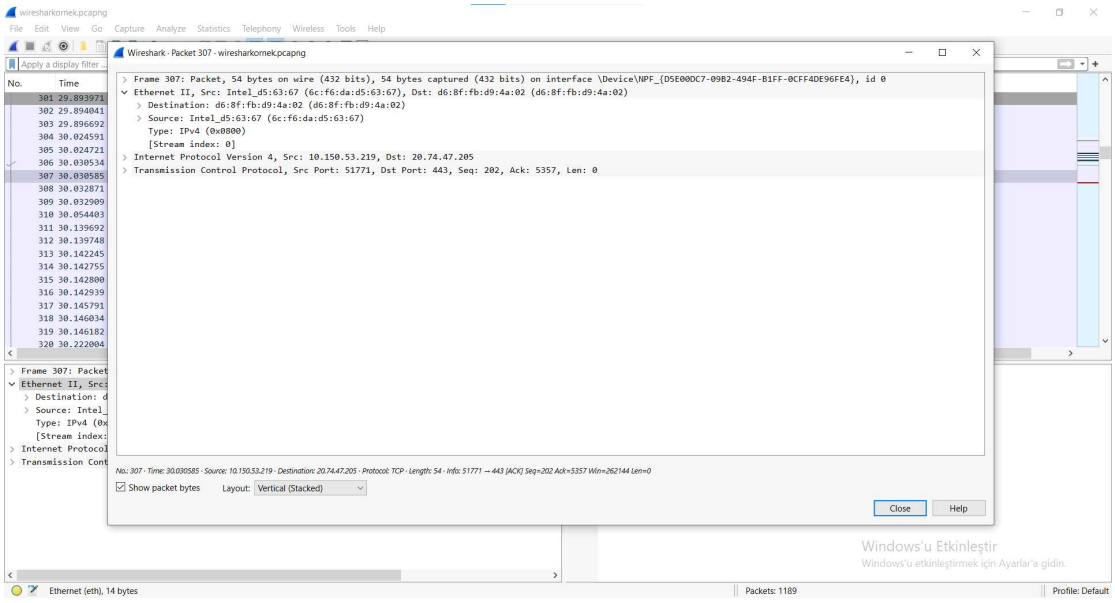
Kanıt



Filtre komutunu yazıp enter yaptıktan sonra ağdaki istenilen IP ve portd olan paketler sıralanır.



3. OSI ile Paket İlişkisi



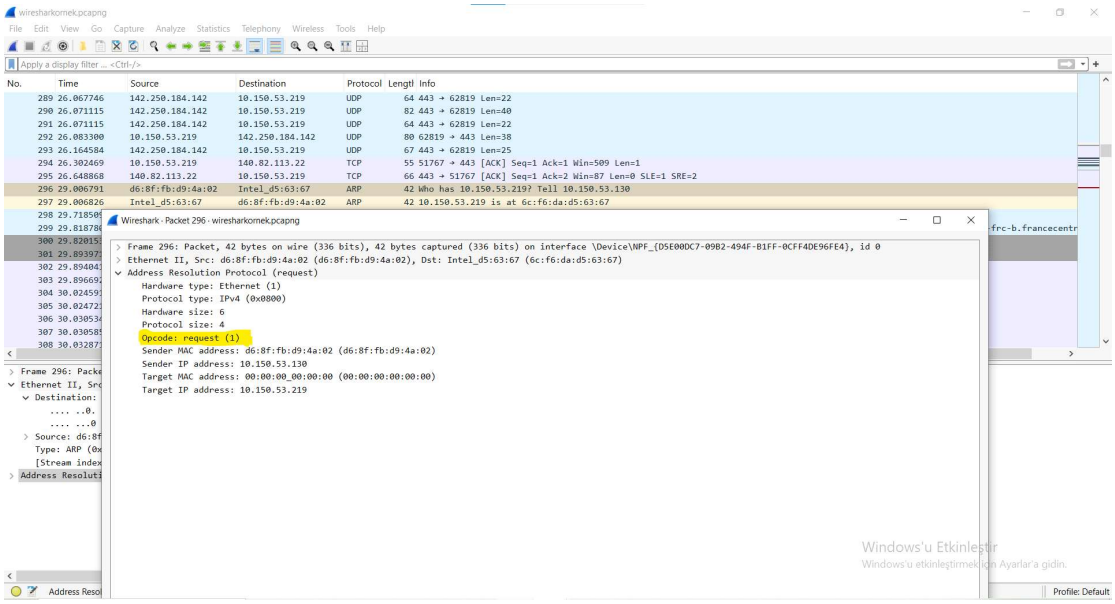
Ekran görüntüsünde görülen Source ve Destination adresleri MAC adresleridir. Çünkü Ethernet II OSI modelinin Layer 2 katmanına aittir ve bu katmanda cihazlar birbirini MAC adresleri ile tanırlar. IP adresleri ise Layer 3'te (Network katmanı) yer alır ve Internet Protocol başlığı altında gösterilir. Bu nedenle fotoğraftaki Source ve Destination bilgileri IP degil MAC adresidir.

4. ARP Trafiği

Opcode 1, "ARP Request" anlamına gelir. Yani bir cihaz ağda belirli bir IP adresine sahip olan cihazın MAC adresini öğrenmek için yayın (broadcast) şeklinde istek gönderir. Opcode 2 ise "ARP Reply" anlamına gelir. Bu durumda ilgili IP adresine sahip olan cihaz, kendi MAC

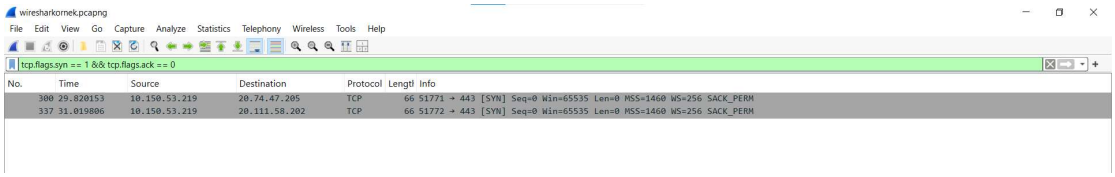
adresini içeren bir yanıt paketi gönderir.

Kanıt



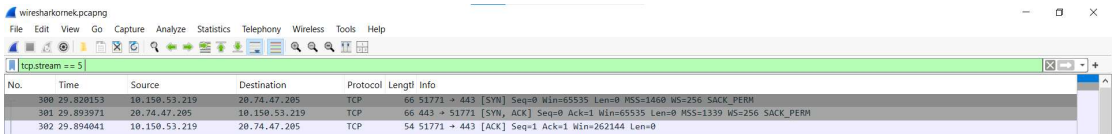
5. TCP El Sıkışması

Trafik içinde 3-Way Handshake işlemini bulmak için ilk olarak filtre kısmına tcp.flags.syn == 1 && tcp.flags.ack == 0 kodunu girdim bu bana ilk SYN paketlerini gösterdi.



Sonra filtre kısmına tcp.stream == 5 kodunu yazdım. Buda bana TCP sırasını verdi.

Kanıt

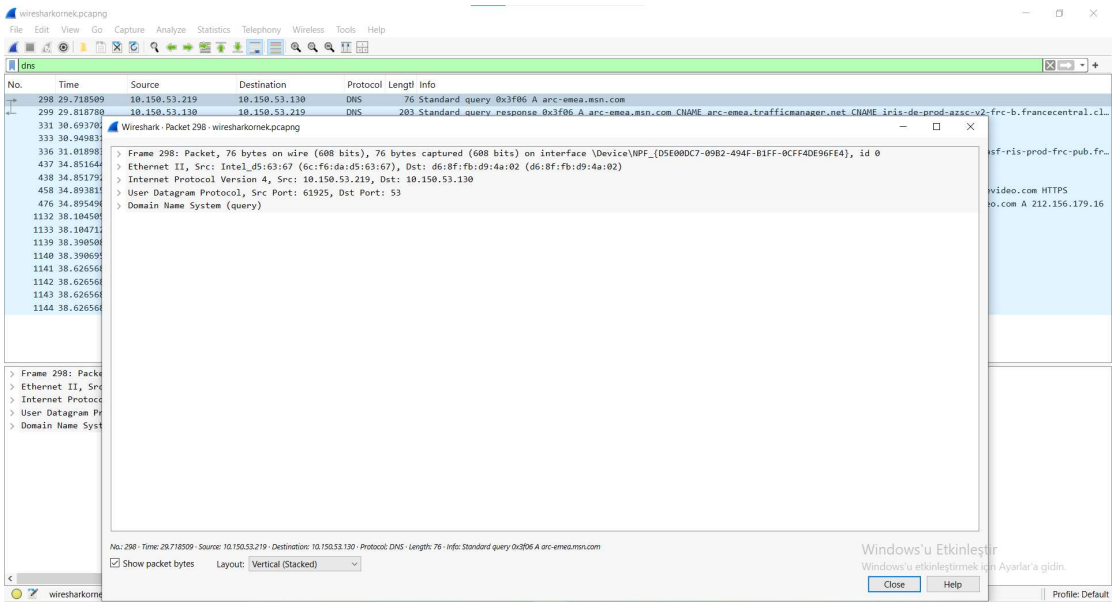


Sequence ve Acknowledgment numaralarının birer arttığını ve bağlantının başarıyla kurulduğu gördüm.

6. DNS Sorguları

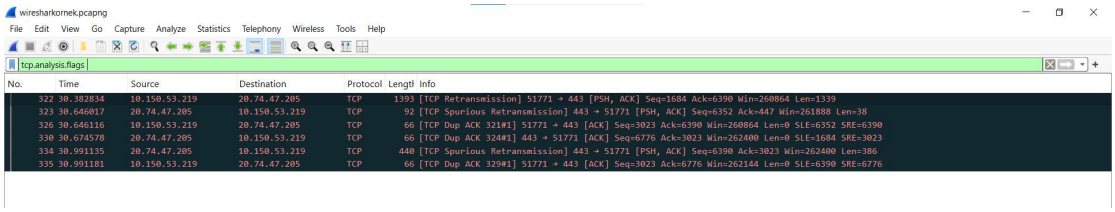
Bir bilgisayar google.com'a gitmek istediğinde önce DNS sunucusuna bir sorgu gönderir. Bu sorgu paketi varsayılan olarak UDP protokolü ile, genellikle 53 numaralı port üzerinden gönderilir. çünkü DNS sorguları küçük boyutludur ve hızlı olması için UDP tercih edilir.

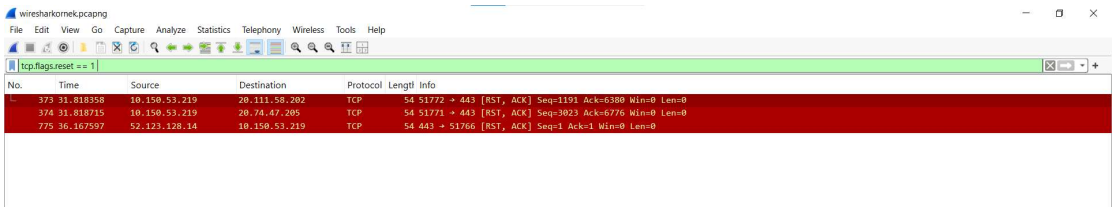
Kanıt



7. HTTP vs HTTPS

8. Saldırı Analizi



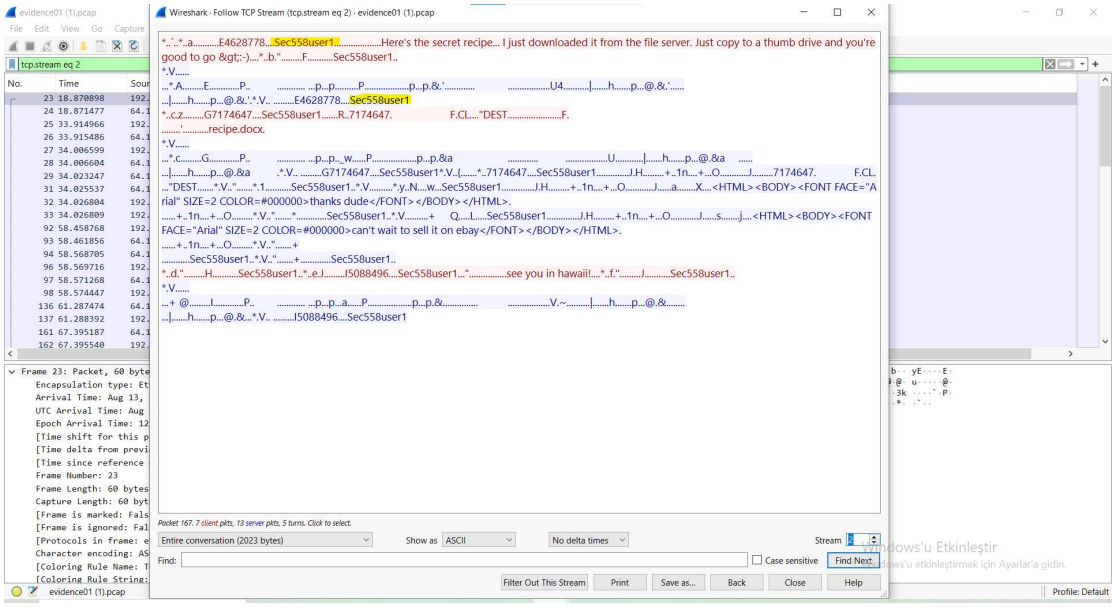


Wireshark analizinde şüpheli TCP akışı ve anormal veri trafiği gözlemledim. Bu durum exploit kullanımını göstermektedir.

BÖLÜM C

Vaka 1: Köstebek Avı (Ann's Bad AIM)

Suç Ortağı:

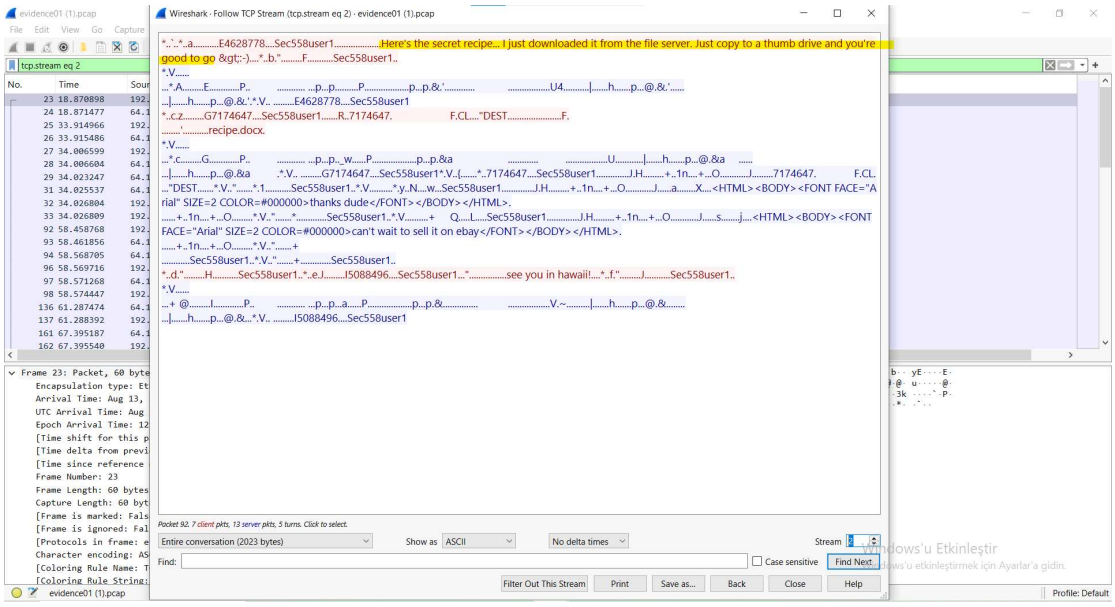


Ekran görüntüsündeki mesaj başlıklarında görüldüğü üzere Ann'in mesajlaştığı kişinin kullanıcı adı Sec558user1'dir.

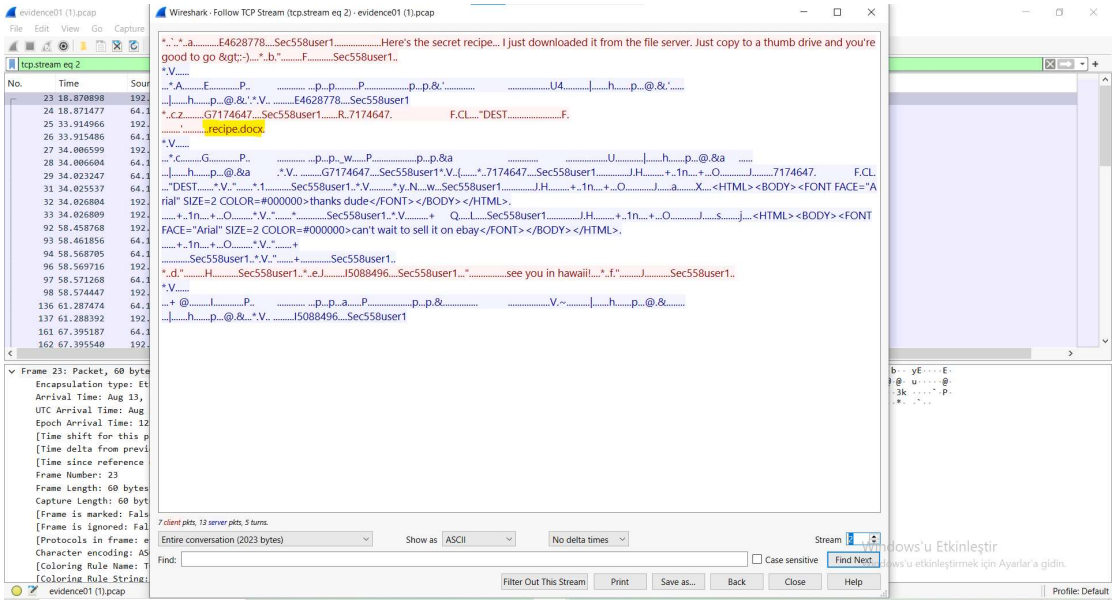
İlk Temas:

Yakalanan konuşmadaki ilk anlamlı mesaj şudur:

"Here's the secret recipe... I just downloaded it from the file server. Just copy to a thumb drive and you're good to go"



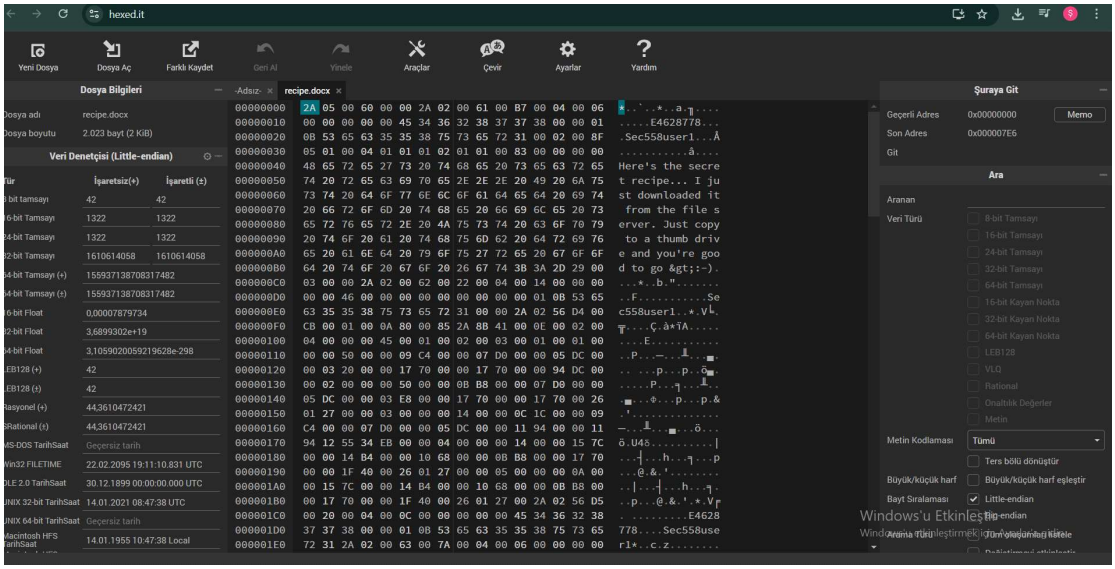
Dosya Transferi:



Konuşmanın devamında Ann'in karşı tarafa sızdırdığı dosyanın adı net bir şekilde görülmektedir: recipe.docx

Dosya Analizi:

Magic Bytes: recipe.docx bir Microsoft Word dosyasıdır. Bu tür dosyaları dışarı aktarıp bir Hex Editor ile açtığınızda ilk 4 baytın 50 4B 03 04 şeklinde olması gerekir.



Fakat benim ekranımdaki byte görünümü 2A 17 00 00 şeklinde. Bunun sebebi, dosyayı "Raw" olarak kaydederken dosyanın başına AIM protokolüne ait bazı başlık bilgilerinin (Header) dahil olmuş olmasıdır.

MD5 Hash değeri: Bu değeri bulabilmek için komut sistemine yazdığım komutu çalıştırdım ve gelen 32 bytelık değer MD5 Hash değei olmuş oldu. Bulduğum değer 75635e5c63f7997dd3d3a7ee8337905a'dır.

Komut İstemi

```
Microsoft Windows [Version 10.0.19045.6466]
(c) Microsoft Corporation. Tüm hakları saklıdır.

C:\Users\Şeyma>certutil -hashfile C:\Users\Şeyma\Desktop\recipe.docx MD5
MD5 hash of C:\Users\Şeyma\Desktop\recipe.docx:
75635e5c63f7997dd3d3a7ee8337905a
CertUtil: -hashfile command completed successfully.

C:\Users\Şeyma>
```

Büyük İfşa: "Here's the secret recipe... I just downloaded it from the file server. Just copy to a thumb drive and you're good to go".

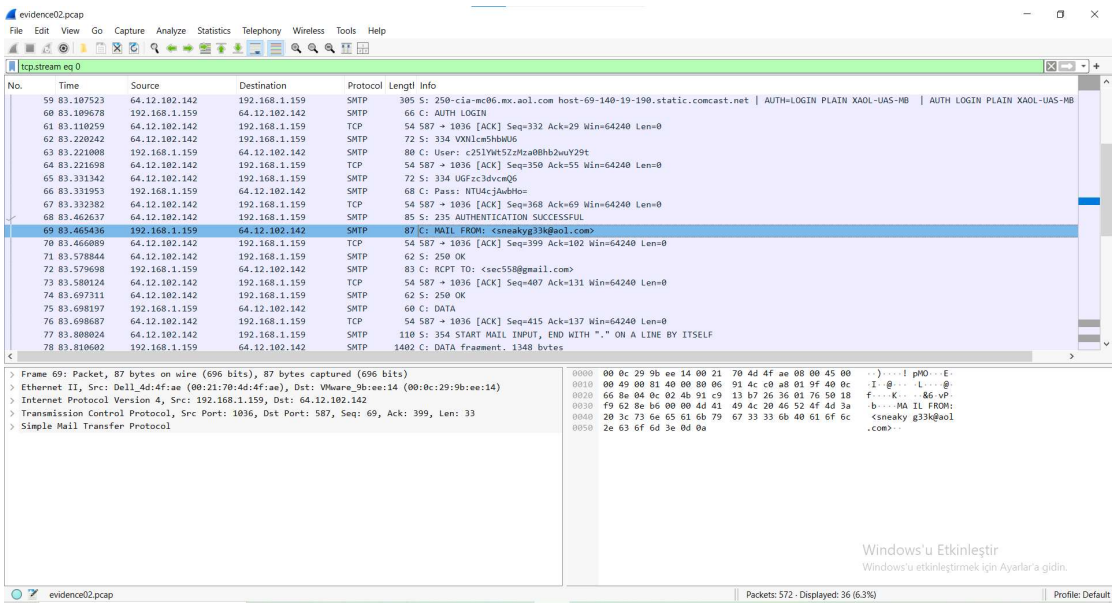
"Thanks dude."

"Can't wait to sell it on ebay."

"See you in hawaii!."

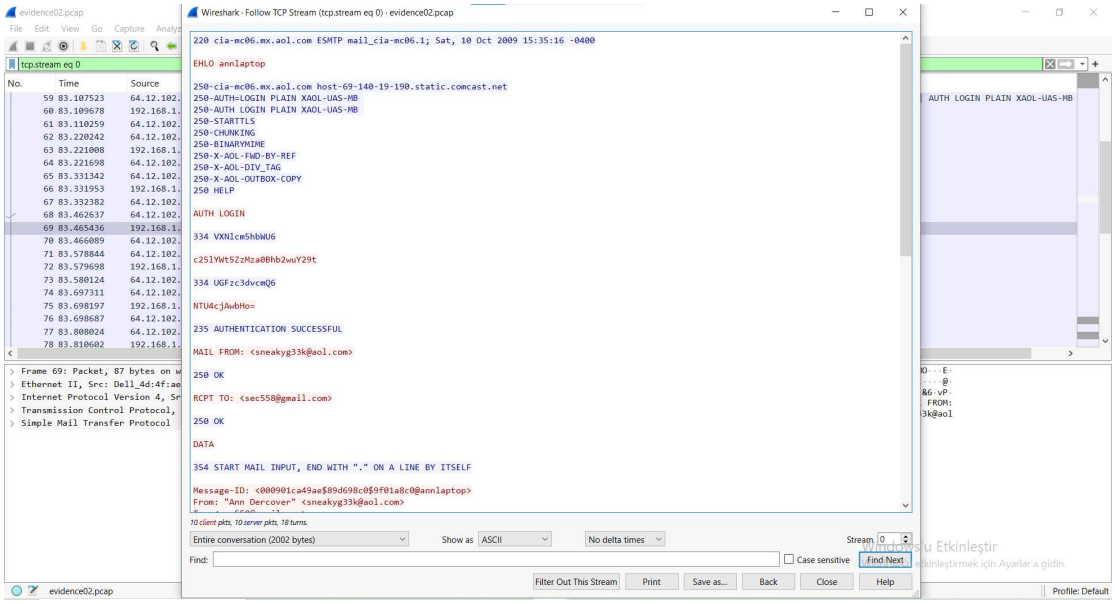
Vaka 2: Kaçış Planı (Ann's Secret Lover)

Kimlik Bilgileri:



Mail: sneakyg33k@aol.com

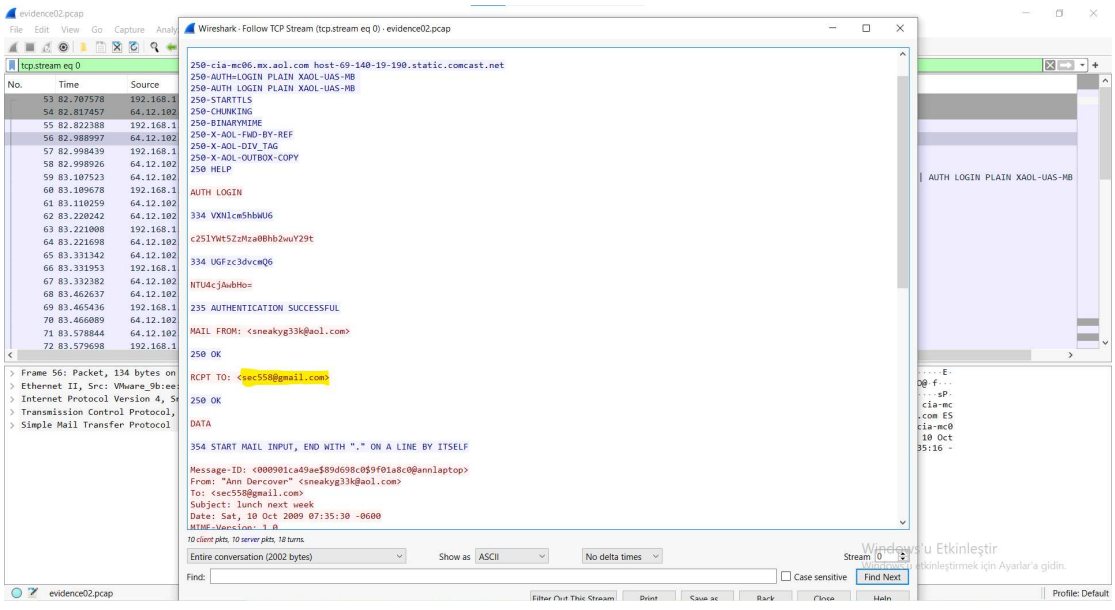
Güvenlik İhlali:



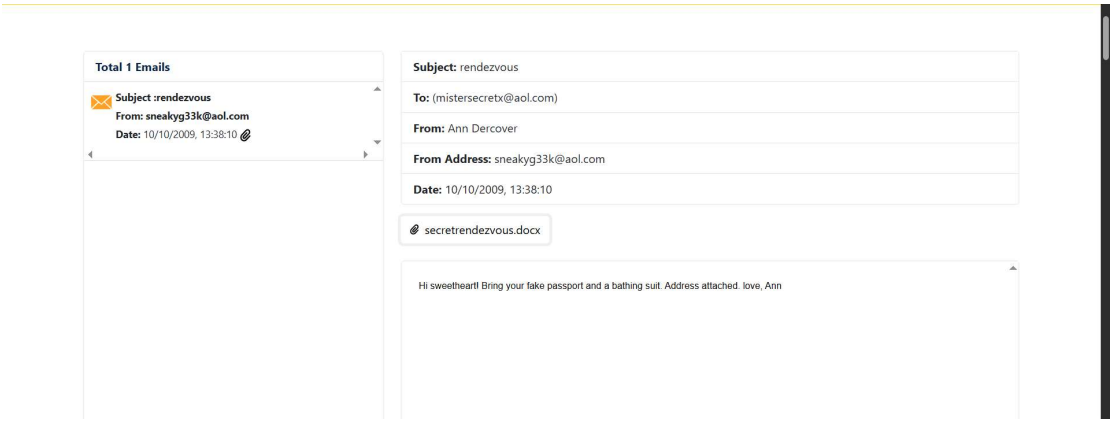
Kullanıcı Adı: c251YWt5Z3Mza0BhaG2wuy29t

Şifre: NTU4cjAwbHo=

Gizli Sevgili: sec558@gmail.com



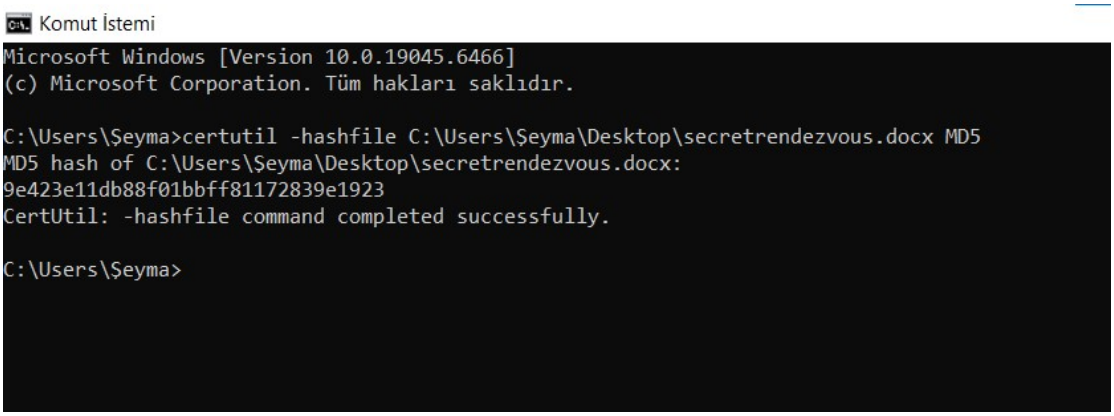
Bavul Hazırlığı: Ann eşya olarak sahte pasaport ve mayo istemiştir.



Eklenti Analizi:

Eklenti adı: secret_map.png

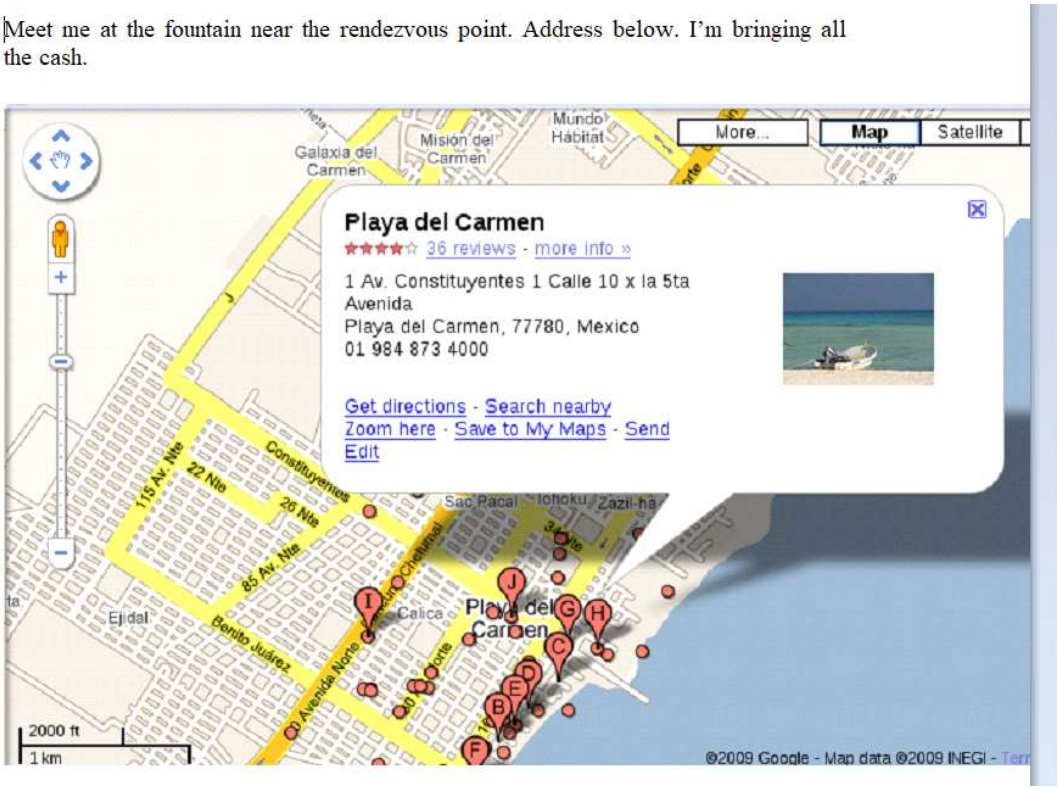
MD5 Hash Değeri:



Konum Tespiti: ilk olarak stream değeri 1 olan paketi File -> Export Objects -> IMF sırasıyla yapıp açılan ekranda rendezvous.eml dosyasını kaydettim. Bu dosyayı online görünteyilici ile açtım ordaki secretrendezvous.docx dosyasını açarak Ann'ın konumunu öğrendim

Konum:Playa Del Carmen/Mexico

Meet me at the fountain near the rendezvous point. Address below. I'm bringing all the cash.



BÖLÜM D

1. Kırmızı Çizgi: Etik ve Hukuk (TCK Kapsamı)

Hukuki Boyut: Bir kafede izinsiz ağ trafiği dinlemek, Türk Ceza Kanunu kapsamında ciddi sonuçlar doğurur. TCK Madde 243'e göre bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girmek veya orda kalmaya devam etmek suçtur. Wireshark ile ağdaki paketleri yakalamak, sistemin verilerine izinsiz erişim sağladığı için bu madde kapsamına girer. TCK Madde 132'ye göre ise kişiler arasındaki haberleşlmenin gizliliğini ihlal eden kişi cezalandırılır. Ann ve sevgilisi arasındaki gibi e-postaları veya mesajları izinsiz okumak doğrudan bu suçu oluşturur.

Profesyonel Duruş: Bir Siber Güvenlik Uzmanı, yazılı izni (pentest onayı) olmayan bir ağda asla Promiscuous Mode açmaz. Çünkü bu eylem siber güvenlik uzmanının kariyerinin sonu olıur. Yaptığı bu davranış Hacking olarak kabul edilir ve siciline işler. Bir saldırgan ile uzman arasındaki en önemli fark izindir.

2. Veri Yorumlama: "Görünenin Ötesi"

Dosya uzantısına güvenme, içeriğe güven prensibi bir dosyanın kimliğinin isminden değil, içindeki ilk birkaç bayttan (Magic Bytes) gelmesidir. Saldırgan uzantıyı değiştirebilir ama dosyanın başındaki bu sihirli baytları değiştirirse, o dosyayı açacak olan uygulama (Örn: Word veya Resim Görüntüleyici) dosyanın yapısını tanıyamaz ve Dosya bozuk veya desteklenmiyor hatası verir. Dosyanın çalışması için o imzanın orada olması şarttır.

3. Gürültü ve Sessizlik: "Ağda İz Bırakmak"

Teknik olarak tamamen sessiz bir sızma mümkün değildir. Basit bir port taraması dahi ağda binlerce paketlik bir gürültü oluşturur.Bu gürültü, savunma tarafı (SOC/Blue Team) için açık bir kanıttır, sistemler anomaliyi fark ederek saldırganı anında tespit eder. Mükemmel suç yoktur Ann'in vakasında gördüğümüz üzere, e-posta silinse bile trafik kayıtları (pcap) silinemeyen kesin kanıtlar sunar.