Ağ Adli Analizi ve Derin Paket İnceleme (DPI)

Packet Detective Raporu

Bölüm A: Teori ve İstihbarat (Research & Logic)

1. Mekanik ve Altyapı: "Ağı Dinlemek"

Promiscuous Mode (Gelişigüzel Mod)

Wireshark ' ı başlattığımızda Promiscuos Mode aktif etmemizdeki amaç girdiğimiz ortamdaki sadece bize söylenenleri veya herkese bağırılanları dışında ortamda diğer ucunda bulunan A kişisi ile B kişisi arasındaki fısıldaşmalardan da haberimizin olmasını istediğimizdendir .Bu mod kapalı olursa NIC sadece MAC adresi kendisi ile eşleşen adresleri, ağdaki her adrese gitmesi gereken MAC adreslerini ve NIC daha önce katıldığı protokol ve medya akışlarından gelen MAC adreslerini kabul eder. Mod kapalı olunca sadece bunlara erişir ve ağdaki diğer cihazlarından bir haber oluruz.

Hub vs. Switch Farkı:

Saldırgan yani 3.kişi ARP Poisoning yöntemini kullanarak Ali'ye ve Veli'ye birbirlerinin MAC adresi bende diyerek mesajları kendine atılmasını sağlar ve sonra bir şey olmamış gibi hedef kişileri ulaştırır.Ağın güvenliğini kötüye kullanıp adresleri manipüle etmeniz gerekir.

Port Mirroring (veya SPAN - Switched Port Analyzer), Switch'in yönetim paneline giriş yapılarak konfigüre edilen yasal bir izleme yöntemidir. Saldırganlar Switch'in şifresini kırıp yönetici yetkisini ulaşamayınca kullanamazlar. Ağ yöneticisi Switch'e Ali bağlı olduğu porttan geçenin kopsayını alarak 3. Kişinin portuna iletir. Ağdaki cihazların haberleri , adresleri değiştirilmez.

Pcap vs. Log:

Firewall loglar ,paketin ağa girip girmediğini, kaynal IP adresi, hedef IP adresini, port numaralarını kaydeder ama paketin içinde ne var olduğunu bilmez. Pcap (Packet Capture) dosyası, ağdan geçen paketin içeriğine kadar her şeyini bilir. Kesin delil olarak Pcap dosyasıdır. Pcap dosyaları kullanarak saldırganın ne yaptığı saniye saniyen yeniden canlandırılabilir. Firewall logunda dışarıdan gelen bir bağlantının "İzin Verildi (Allowed)" olarak görünmesi bir saldırı kanıtı değildir.

2. Protokol Anatomisi: "Dijital El Sıkışma"

3-Way Handshake (Üçlü El Sıkışma):

Bunu ben esnaf-müşteri öğreniğini verebilirim.

-Kolay gelsin ustam. (SYN)

- Sağol, buyur nasıl yardımcı olayım? (SYN-ACK)

- Eyvallah ustam, çikolata alacaktım. (ACK)

TCP ‘nin amacı verilerin karşı tarafa ulaşıp ulaşmadığını emin olmaktır. Alıcı veriyi aldıktan sonra yanıt vermesi alıcının da verisinin(ACK) göndericiye ulaştığını bilmesi için gereklidir sonuçta TCP’ de iletişim çift yönlüdür.

TCP vs. UDP:

Youtube ve Netflix yayınlarında UDP kullanım amacı eksiksiz verinin karşı tarafa ulaşmaması ilgilendirmez .Bu platformlarda hız önemli o anki sonradan gelen verinin kıymeti yoktur. Bankacılıkta ise hız değil ,verinin karşı tarafa eksiksiz ulaşması ön plandadır bu yüzden TCP protokolünü benimserler. Paket kayıplarında UDP’ nin umrunda olmaz açıkçası onun için zamanında gitmesi önemlidir. TCP ise bu durumda kaybolan paketi geri ister.

Sequence Number (Sıra Numarası):

Paketlerin üstüne numara yazılmasının sebebi interneteteki hiçbir veri tek bir bütün halde iletilemez.Ağ kablolarının ve cihazların taşıyabileceği maksimum bir boyut sınırı vardır.Paketi bütün halde iletemeyeceğimiz için parçalara bölmek zorundayız. Parçalar iletidikten sonra alıcı bunları neye göre anlamdıracağı için numaralandırmamız şart.

Parçalar internette aynı yol üzerinden ilerlemeyebilir. BU yüzden 5 numaralı paket 3 numaralı paketten önce ulaşabilir. Bu durumlarda TCP Tampon Belleği (Receive Buffer) devreye girer. Önce gelen paketi kabul ederek gelmesi istenen paket gelene kadar bekletir asla çöpe atmaz.

3. Kimlik ve Adresleme: "Postacı Kapıyı Çalar"

ARP Protokolü (Who has?):

Bilgisayarlar yazılımsal olarak IP adresleriyle (Örn: 192.168.1.1) iletişim kurmak üzere tasarlanmıştır, ancak veriyi fiziksel kablolardan veya havadan (Wi-Fi) aktaran donanımlar (Ağ Kartları ve Switch'ler) IP adresinden hiç anlamazlar; onların tek bildiği donanımsal kimlik olan **MAC adresidir**.

ARP bu noktada devreye girerek teslim etmemiz gereken dosyayı hedefteki IP adresine ulaştırmak zorundayız. Ön belliği kontrol ederek, ben bu IP adresiyle daha önce iletişime geçmiş miyim ? MAC adresini kaydetmiş miyim? Eğer kayıt bulamazsa ortama geçerek

request Boardcast paketi hazırlar ve switche yollar.Switch bu paketi ağdaki herkese iletir.Aradığı MAC adresini böylelikle bulur ve APR tablosuna kaydeder.

DHCP (DORA Süreci):

Bir cihaz ağa ilk bağlandığında ne kendi IP'si vardır ne de ağdaki sunucunun IP'sini bilir. Burada devreye DHCP sunucusu devreye girer ve DORA adı verilen 4 adımlı süreci başlar.

Discover sürecinde cihaz ağda boardcast paketi oluşturur ve ağa iletir. Offer sürecinde ağdaki cihazların çoğu beni ilgilendirmez diyerek paketi çöpe taşır ancak ağın sunucusu DHCP bu paketi alır ve IP adres önerisi sunar. Request sürecinde ise cihaz teklifi kabul eder ancak IP'yi hemen kullanmaya başlayamaz. Teklifi kabul ettiğini ve diğer sunucu tekliflerini reddettiğini bildirmek için tekrar boardcast paketi oluşturur ve ağa gönderir.

Acknowledge sürecinde ise DHCP sunucusu cihazın bu IP adresini kullanmasına onay verir ve cihaz IP adresini kullanmaya başlar.

DNS (İnternetin Rehberi):

Tarayıcıya google.com yazdığınızda bilgisayarınızın hiçbir fikri yoktur. Çünkü bilgisayarlar harflerden anlamaz, sadece IP adresleriyle (örneğin 142.250.190.46) iletişim kurabilirler. İşte bu "İsim -> Numara" çevirisini yapan devasa ve hiyerarşik sisteme DNS (Domain Name System) diyoruz.

Bilgisayarımız bu ismin IP karşılığını bulmak için sırasıyla :

Local Cache-Recursive DNS Resolver-Root Name Servers-TLD - Top Level Domain Servers-Authoritative Name Server

Bunlara request gönderir.

4. Şifreleme ve Kör Noktalar: "Sır Perdesi"

HTTPS ve Şifreleme:

Göremeyiz çünkü HTTPS (TLS/SSL) girdiğinde, TCP el sıkışmasından hemen sonra iletişimin "Payload" (Uygulama Katmanı) kısmı çelik bir kasaya kilitlenir. Göremediğimiz için elimizde sadece şu veriler olur:

Trafiğin hangi IP'den çıkıp hangi IP'ye gittiğini ve Hedef Port'u (HTTPS için 443) net bir şekilde görürüz.

Bağlantı ilk kurulduğunda, şifreli tünel tam olarak inşa edilmeden *hemen önce* bilgisayarınız sunucuya bir "Client Hello" (Merhaba) paketi gönderir.

Verinin içeriği şifreli olsa da **boyutu ve süresi** gizlenemez.

Özellikle eski TLS sürümlerinde (TLS 1.2 ve öncesi), sunucunun bilgisayarınıza gönderdiği dijital sertifikanın detayları (Kime ait olduğu, ne zaman süresinin dolduğu, hangi şifreleme algoritmalarının desteklendiği) açık metin olarak okunabilir.

Man-in-the-Middle (Ortadaki Adam):

Şifreli bir tünelin (HTTPS) dışından bakarak içindekileri okumak matematiksel olarak imkansıza yakındır. Çözmek için hedef sunucu ve cihaz arasına girer .Cihazdan gelen requesti namı değer havada yakalar ve hedef sunucuya giderek sertifikaya bakar. Ancak hedef sunucunun sertifikasına gönderemeyeceğinden kendi oluşturduğu sahte sertifikayı cihaza iletir. Kullanıcı hedef sunucudan geldiğini sanarak bilgilerini doldurur sahte sertifika da saldırgana gider. Saldırgan böylelikle kullanıcının bilgilerine ulaşır. Saldırgan bu bilgileri hedef sunucuyu çözmek için kullanır.

5. Saldırı İmzaları: "Suçluyu Tanımak"

Port Taraması (Port Scanning): Daha önce yakaladığımız o meşhur 3-Way Handshake (3'lü el sıkışma) kuralına uyar.

Cihaz [SYN] gönderir, hedef [SYN, ACK] ile cevap verir, cihaz [ACK] ile onaylar ve ardından veri aktarımı başlar. Her şey sıralı, eksiksiz ve amaca yöneliktir.

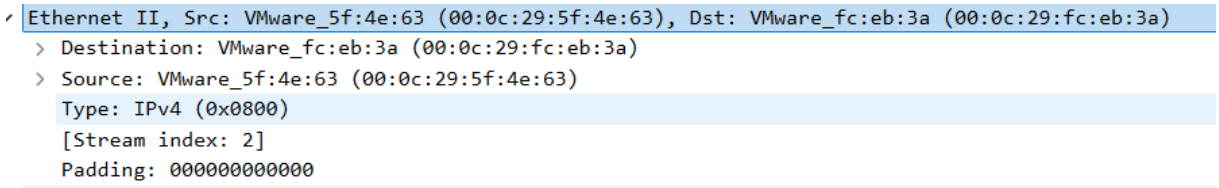
Wireshark ekranında bir port taraması (Örn: Nmap SYN Scan) başladığında sistemde adeta bir panik havası ve kırmızı bir dalga oluşur.

Denial of Service (DoS):

Kuyruk tamamen dolduğunda, siteye girmek isteyen gerçek ve masum bir kullanıcı [SYN] gönderdiğinde, sunucu "Kusura bakma, bekleme salonum tamamen dolu, sana yer ayıramam" diyerek o paketi çöpe atar. Sunucu fiziksel olarak çökmemiş olsa bile, dışarıdan gelen hiçbir yeni gerçek bağlantıyı kabul edemediği için fiilen "Hizmet Dışı" (Denial of Service) kalmış olur.

Bölüm B: Saha Eğitimi ve Araç Hakimiyeti (TryHackMe - Wireshark 101)

1. Arayüz ve Renkler (Task 3: Wireshark Overview):



- Paketin gittiği hedefin fiziksel **MAC Adresini** yazar. (TryHackMe sık sık "Hedef MAC adresi nedir?" diye sorar, cevap buradadır).

```
Transmission Control Protocol, Src Port: 60368, Dst Port: 135, Seq: 1, Ack: 1, Len: 0
   Source Port: 60368
   Destination Port: 135
   [Stream index: 0]
   [Stream Packet Number: 3]
 > [Conversation completeness: Complete, WITH_DATA (31)]
   [TCP Segment Len: 0]
   Sequence Number: 1    (relative sequence number)
   Sequence Number (raw): 658838936
   [Next Sequence Number: 1    (relative sequence number)]
   Acknowledgment Number: 1    (relative ack number)
   Acknowledgment number (raw): 1736896599
   0101 .... = Header Length: 20 bytes (5)
 > Flags: 0x010 (ACK)
   Window: 502
   [Calculated window size: 64256]
   [Window size scaling factor: 128]
   Checksum: 0xe2f3 [unverified]
   [Checksum Status: Unverified]
   Urgent Pointer: 0
 > [Timestamps]
 > [SEQ/ACK analysis]
   [Client Contiguous Streams: 1]
   [Server Contiguous Streams: 1]
```

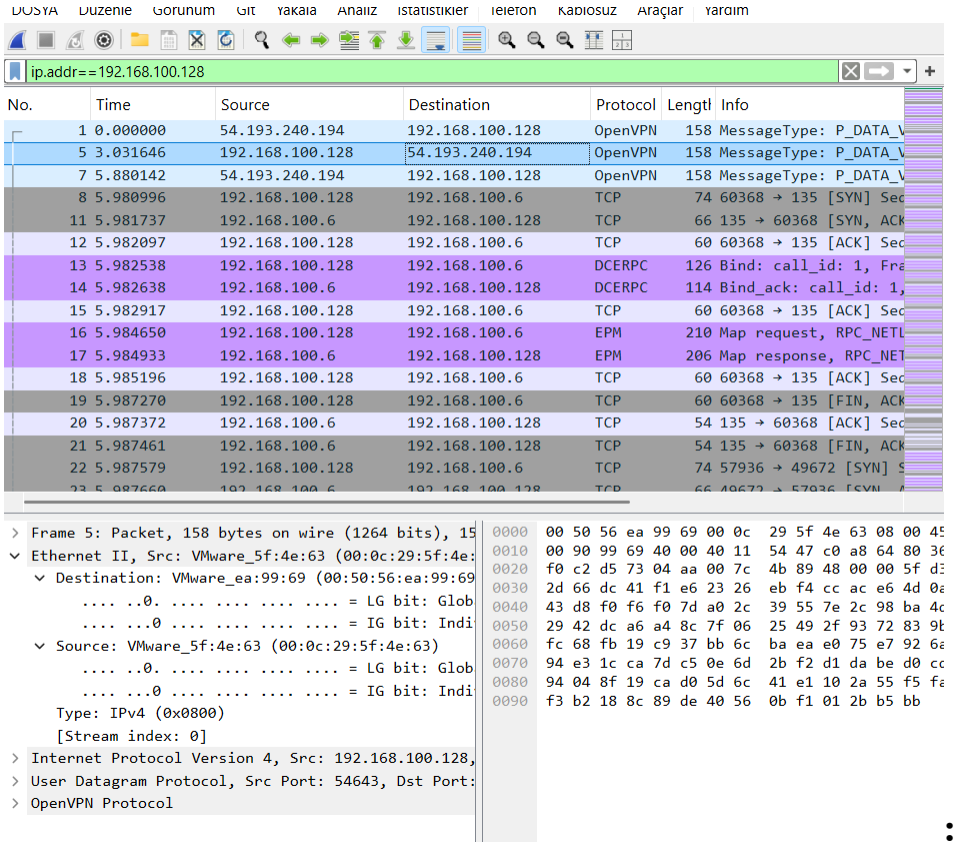
Hedef sunucunun port numarasını (Örn: 80 veya 443) yazar.

```
Internet Protocol Version 4, Src: 192.168.100.128, Dst: 192.168.100.6
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 40
   Identification: 0xa408 (41992)
 > 010. .... = Flags: 0x2, Don't fragment
   ...0 0000 0000 0000 = Fragment Offset: 0
   Time to Live: 64
   Protocol: TCP (6)
   Header Checksum: 0x4cf0 [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 192.168.100.128
   Destination Address: 192.168.100.6
   [Stream index: 2]
```

Paketi gönderen cihazın IP adresini görürsünüz (Örn: 192.168.1.10). Paketin gittiği Hedef IP adresini görürsünüz. Time to Live (TTL): Paketin yaşam süresi (Örn: 64) yazar.

Siyah renk,önceki mesajlarımızda konuştuğumuz o "güvenilir ve sıralı" TCP iletişiminin **bozulduğunu** gösterir. Şebekede bir tıkanıklık, veri kaybı veya bir saldırı dalgası olabilir.Kırmızı renk genellikle iletişimin agresif bir şekilde kesildiğini veya hedefin hiç var olmadığını gösterir.

2. Filtreleme Sanatı (Task 5: Filtering Captures)



:

Wiresharkta filtreleme binlerce ağdaki paket arasından kendi aradığımız paketi bulmamızı sağlar.Diğer paketler aslında bir yere gitmez sadece bizim için sessiz moda geçerler.

3. OSI ile Paket İlişkisi (Task 6: Packet Dissection):

"Source" ve "Destination" adresleri, OSI modelinin 2. Katmanı olan Data link katmanına aittir. Bu adresler MAC adresidir.

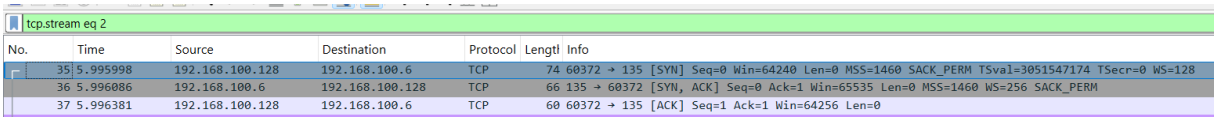
4. ARP Trafiği (Task 7: ARP Traffic)

```
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
    .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
Source: VMware_fc:eb:3a (00:0c:29:fc:eb:3a)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
  [Stream index: 3]
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: VMware_fc:eb:3a (00:0c:29:fc:eb:3a)
  Sender IP address: 192.168.100.6
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.100.128
```

Opcode1 ,cihazın ağda birini aradığı (soru sorduğu) anlamına gelir.(request)

Opcode 2,aranan kişinin bulunduğunu ve **cevap verdiğini** gösterir.(reply)

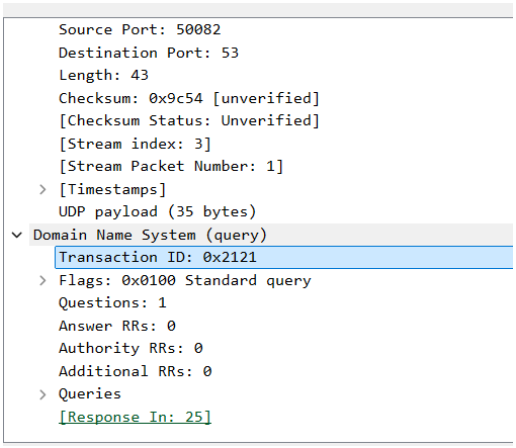
5. TCP El Sıkışması (Task 9: TCP Traffic)



tcp.stream eq 2

No.	Time	Source	Destination	Protocol	Length	Info
35	5.995998	192.168.100.128	192.168.100.6	TCP	74	60372 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3051547174 TSecr=0 WS=128
36	5.996086	192.168.100.6	192.168.100.128	TCP	66	135 → 60372 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
37	5.996381	192.168.100.128	192.168.100.6	TCP	60	60372 → 135 [ACK] Seq=1 Ack=1 Win=64256 Len=0

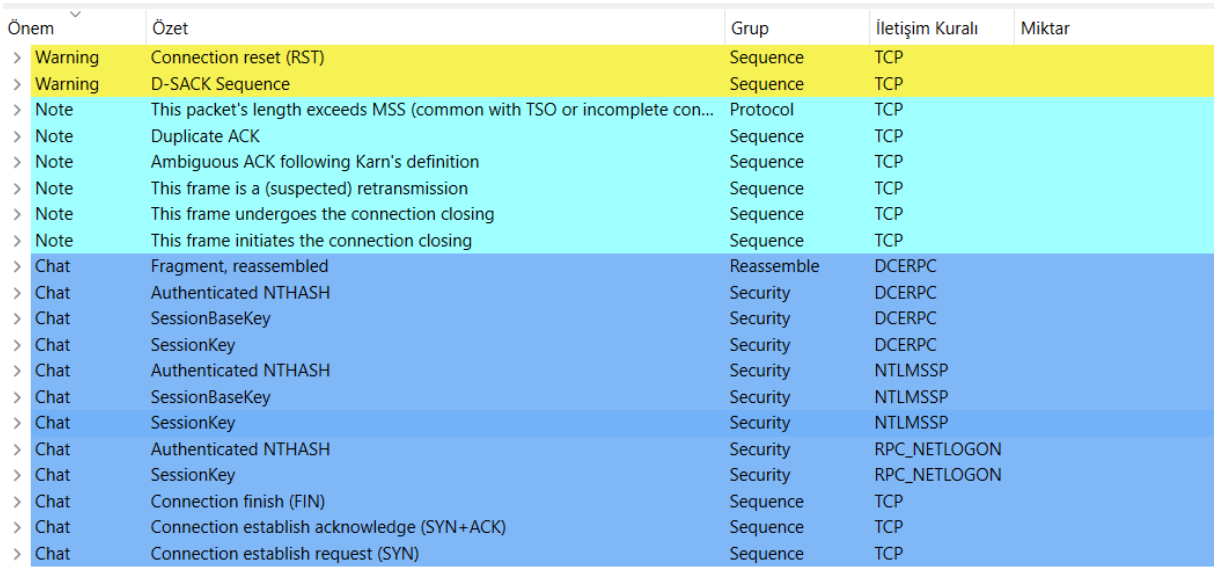
6. DNS Sorguları (Task 10: DNS Traffic)



```
Source Port: 50082
Destination Port: 53
Length: 43
Checksum: 0x9c54 [unverified]
[Checksum Status: Unverified]
[Stream index: 3]
[Stream Packet Number: 1]
> [Timestamps]
UDP payload (35 bytes)
v Domain Name System (query)
  Transaction ID: 0x2121
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  > Queries
  [Response In: 25]
```

UDP protokolüne gider.

8. Saldırı Analizi (Task 13: Analyzing Exploit)



Önem	Özet	Grup	İletişim Kuralı	Miktar
Warning	Connection reset (RST)	Sequence	TCP	
Warning	D-SACK Sequence	Sequence	TCP	
Note	This packet's length exceeds MSS (common with TSO or incomplete con...	Protocol	TCP	
Note	Duplicate ACK	Sequence	TCP	
Note	Ambiguous ACK following Karn's definition	Sequence	TCP	
Note	This frame is a (suspected) retransmission	Sequence	TCP	
Note	This frame undergoes the connection closing	Sequence	TCP	
Note	This frame initiates the connection closing	Sequence	TCP	
Chat	Fragment, reassembled	Reassemble	DCERPC	
Chat	Authenticated NTHASH	Security	DCERPC	
Chat	SessionBaseKey	Security	DCERPC	
Chat	SessionKey	Security	DCERPC	
Chat	Authenticated NTHASH	Security	NTLMSSP	
Chat	SessionBaseKey	Security	NTLMSSP	
Chat	SessionKey	Security	NTLMSSP	
Chat	Authenticated NTHASH	Security	RPC_NETLOGON	
Chat	SessionKey	Security	RPC_NETLOGON	
Chat	Connection finish (FIN)	Sequence	TCP	
Chat	Connection establish acknowledge (SYN+ACK)	Sequence	TCP	
Chat	Connection establish request (SYN)	Sequence	TCP	

BÖLÜM C: Vaka Analizi (Evidence Files)

Vaka 1: Köstebek Avı (Ann's Bad AIM):

Suç Ortağı: Sec558user1..

İlk Temas: 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: recipe.docx

Dosya Analizi (File Carving):

```
PS C:\Users\LENOVO> Get-FileHash -Algorithm MD5 C:\Users\LENOVO\Documents\OneDrive\Desktop\3.sınıf\recipe.docx

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             52C13D8C0A99AC0D3210E8E8EDB046BF                                       C:\Users\LENOVO\Documents\One...

PS C:\Users\LENOVO>
```

50 4B 03 04

Büyük İfşa:

Recipe for Disaster:

1 serving

Ingredients:

4 cups sugar

2 cups water

In a medium saucepan, bring the water to a boil. Add sugar. Stir gently over low heat until sugar is fully dissolved. Remove the saucepan from heat. Allow to cool completely. Pour into gas tank. Repeat as necessary.

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

Kimlik Bilgileri: MAIL FROM: <sneakyg33k@aol.com>

Güvenlik İhlali: : Username: c25lYWt5ZzMza0Bhb2wuY29t

Password: NTU4cjAwbHo=

Gizli Sevgili: RCPT TO: <sec558@gmail.com>

Bavul Hazırlığı: Sorry-- I can't do lunch next week after all. Heading out of town. =

Another time! -Ann

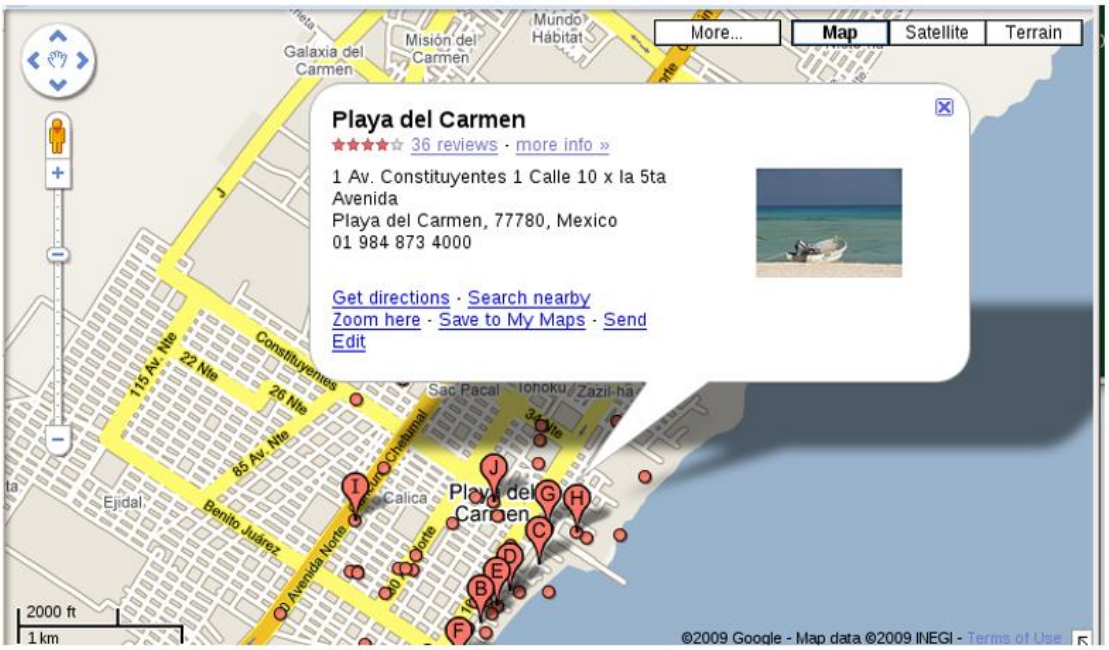
Eklenti Analizi: secretrendezvous.docx

```
PS C:\Users\LENOVO> Get-FileHash -Algorithm MD5 C:\Users\LENOVO\Documents\OneDrive\Desktop\secretrendezvous.docx

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             9E423E11DB88F01BBFF81172839E1923                                       C:\Users\LENOVO\Documents\One...
```

Konum Tespiti:

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



BÖLÜM D: Mühendislik Vizyonu ve Etik (Reflection)

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

Hukuki Boyut: Ortak bir Wi-Fi ağına bağlanmak yasaldır. Ancak, o ağın içindeki trafiği manipüle etmek, dinlemek için ağ cihazlarını (Router/Modem) kandırmak (örneğin ARP Zehirlenmesi yapmak) veya yakaladığınız bir şifreyle (geçen görevlerde yaptığınız gibi) başkasının e-posta hesabına girmek bu kapsama girer.

Profesyonel Duruş: Bir Siber Güvenlik Uzmanı, (Kendi ev ağı veya özel laboratuvarı hariç) yazılı izni (RoE - Rules of Engagement) olmayan hiçbir ağda Promiscuous Mode açmaz.

2. **Veri Yorumlama: "Görünenin Ötesi" :**

Analiz: Saldırgan, kurbanı kandırmak için uzantıyı değiştirmek zorundadır; ancak silahının (zararlı yazılımın) çalışabilmesi için Magic Bytes'ı (Header'ı) orijinal ve sağlam bırakmak *mecburiyetindedir*. İşte adli bilişim analistleri de tam olarak saldırganın bu mecburiyetinden faydalanarak gerçekleri ortaya çıkarır.

3. **Gürültü ve Sessizlik: "Ağda İz Bırakmak"**

"Sessiz sızma" sadece filmlerde veya savunması çok zayıf, alarmları bozuk sistemlerde geçerli bir yanılsamadır. Veri iletişimi kavramlarının temeline, verinin OSI katmanlarında nasıl paketlenip cihazlardan (switch, router) nasıl yönlendirildiğine indiğimizde gerçeği net olarak görürüz: Bir ağda hareket etmek için mutlaka paket göndermek ve almak zorundasınızdır.