

Çevrimiçi Oyun Yayınlarında Ağ Trafiği Tespiti ve Analizi: 2025 Yılına Yönelik Teknikler ve Trendler Raporu

Proje Özeti

Bu rapor, çevrimiçi oyun ortamlarında ağ trafiği tespiti ve analizine kapsamlı bir bakış sunmaktadır. Proje, çeşitli oyunların yayınılarında hangi IP adresi ve porta bağlandığını belirlemeyi ve bu tespiti Wireshark için hem Yakalama Filtreleri (Capture Filters) hem de Görüntüleme Filtreleri (Display Filters) listeleriyle desteklemeyi amaçlamaktadır. Ayrıca, 2025 yılına yönelik en son ve en etkili ilk 10 teknik ve trend derinlemesine araştırılarak, her biri için başlık, açıklama, potansiyel etkileri, uygulama alanları ve güvenilir kaynaklar sunulmaktadır. Bu çalışma, ağ performansı, güvenliği ve bütünlüğünü korumak için kritik öneme sahip olan ağ trafiği analizinin dinamik doğasını ele almaktadır.

1. Çevrimiçi Oyun Ağ Analizinin Gelişen Ortamı (2025)

Çevrimiçi oyunların gerçek zamanlı etkileşimler ve yüksek hacimli veri alışverişleriyle karakterize edilen dinamik dünyası, ağ trafiği analizi için benzersiz zorluklar ve fırsatlar sunmaktadır. Oyunlar giderek daha karmaşık ve birbirine bağlı hale geldikçe, optimum performans, sağlam güvenlik ve adil oyun deneyimi sağlamak için temel ağ iletişimlerini anlamak ve yönetmek büyük önem taşımaktadır. 2025 yılında bu alan, yapay zeka alanındaki ilerlemeler, şifreli kanallara artan bağımlılık ve bulut tabanlı mimarilerin yaygınlaşmasıyla hızlı bir dönüşüm geçirmektedir. Bu rapor, oyun ağ trafiğini tanımlamanın temel yönlerini incelemekte veümüzdeki yılda etkili analizi tanımlayacak en son teknikleri ve trendleri araştırmaktadır.

2. Oyun Ağ Trafiği Tanımlama Temelleri

Etkili ağ trafiği analizi, iletişim uç noktalarının ve protokollerinin hassas bir şekilde tanımlanmasıyla başlar. Çevrimiçi oyunlar için bu, istemci-sunucu ve eşler arası etkileşimler için kullanılan belirli IP adreslerini ve bağlantı noktalarını belirlemeyi ve ardından Wireshark gibi araçlar kullanarak özel paket yakalama ve görüntüleme filtrelerini uygulamayı içerir.

2.1. Oyun IP Adreslerini ve Portlarını Belirleme

Çeşitli oyun yayınıları tarafından kullanılan IP adreslerini ve portları belirlemek, herhangi bir ağ analizi için temel bir adımdır. Oyunlar genellikle oyun durumu senkronizasyonu, sesli sohbet ve eşleştirme gibi iletişimlerinin farklı yönleri için TCP ve UDP portlarının bir kombinasyonuna güvenirler.

Oyun sunucusu IP'lerini ve istemci-sunucu iletişim portlarını belirlemek için çeşitli yöntemler bulunmaktadır:

- **Resmi Dokümantasyon/Destek:** Oyun geliştiricileri veya yayıncıları, özellikle port yönlendirme için gerekli portların listelerini genellikle sağlarlar. Bu, en güvenilir kaynaktır.¹
- **Ağ İzleme Araçları:** Wireshark gibi araçlar, canlı trafiği yakalayarak analistlerin bir oyun istemcisinin bir sunucuya bağlandığında kullandığı hedef IP adreslerini ve portları gözlemlemesine olanak tanır.³
- **Paket Analizi:** Yakalanan paketlerin derinlemesine incelenmesi, temel protokoller ve port numaralarını ortaya çıkarabilir. Örneğin, TCP el sıkışmalarının (SYN, SYN-ACK, ACK) ve UDP akışlarının analizi, aktif bağlantıları gösterebilir.⁵
- **Oyun Motoru Özellikleri:** Unreal Engine ve Unity gibi oyun motorlarının kendi ağ gereksinimleri ve varsayılan portları vardır. Örneğin, Unreal Engine genellikle ağ iletişimini için 7777 portunu kullanırken, Unity istemcileri bir güvenlik duvarı tarafından belirli bir kaynak portun kullanılmasını gerektirmedikçe genellikle geçici portlara bağlanır.⁷

Aşağıdaki tablo, popüler oyunlar için yaygın olarak kullanılan portları özetlemektedir:

Tablo: Yaygın Oyun Portları (Örn. CS2, Valorant, PUBG)

Oyun Adı (Platform)	TCP Portları	UDP Portları	Güvenilir Kaynak(lar)
CS2 (Steam)	27015, 27036	27015, 27020, 27031-27036	1
Valorant (PC)	80, 443, 2099, 5222-5223, 8088, 8393-8400, 8446	3478, 3479, 3480, 7000-8000 (Oyun İstemcisi), 64000-64100 (Sesli Sohbet Ekipleri)	9
PUBG (Steam)	27015, 27036	27015, 27031-27036	11
PUBG (Xbox One/Series X)	3074	88, 500, 3074, 3544, 4500	11

PUBG (PlayStation 4/5)	3478-3480	3074, 3478-3479	11
Unreal Engine (Varsayılan)	-	7777 (Ortak Görüntüleyici için)	8
Unity Engine (İstemci)	Geçici portlar	Geçici portlar	7
Unity Engine (Sunucu)	-	7777 (Yapılabilir)	7

Oyunların temel tasarım tercihleri, özellikle türleri (örneğin, gerçek zamanlı nişancı oyunları ve sıra tabanlı strateji oyunları), temel ağ protokollerini (TCP ve UDP) ve bunların kullanım kalıplarını doğrudan belirler.¹² Bu, etkili ağ analizi için sadece pasif gözlem yapmak yerine, trafik davranışını tahmin etmek amacıyla oyun mekaniklerini anlamaların önemini vurgular. Örneğin, yüksek UDP trafik hacmi ve minimum yeniden iletim, bir hızlı aksiyon oyunu için normal kabul edilirken, TCP güvenilirliği bekleyen bir sıra tabanlı oyunda bir soruna işaret edebilir. Bu tür bir anlayış, normal oyun trafiğini anormalliliklerden veya potansiyel saldırılardan ayırt etmek için hayatı öneme sahiptir.

2.2. Wireshark ile Oyun Trafisi Analizi

Wireshark, ağ profesyonelleri için vazgeçilmez bir araç olup, sorun giderme, güvenlik analizi ve ağ protokollerini anlama için kritik derin paket inceleme yetenekleri sunar.¹⁴ Hem yakalama hem de görüntüleme için sunduğu filtreleme yetenekleri, tipik bir ağın geniş gürültüsünden ilgili oyun trafiğini izole etmenin merkezindedir.¹⁵

2.2.1. Oyun Trafisi için Wireshark Yakalama Filtreleri

Yakalama filtreleri, paketler depolanmadan önce uygulanır ve toplanan veri hacmini önemli ölçüde azaltarak analiz verimliliğini artırır. Yakalama başladıkten sonra geri alınamazlar.¹⁷

Bu filtrelerin temel amacı, yakalama dosyasına kaydedilen veri miktarını sınırlamak, böylece analizi hızlandırmak ve depolama yükünü azaltmaktadır.¹⁸ Ana bileşenleri arasında protokol belirtimi (örneğin, tcp, udp), ağ adresi filtreleme (host, net, src, dst), porta dayalı filtreleme (port, portrange) ve bayt ofsetleri kullanarak içerik eşleştirme bulunur.¹⁹ Yakalama filtreleri, C-sözdizimi değerlendirme operatörlerini (>, <, =, !=, vb.) ve mantıksal operatörleri (and, or, not) kullanır.¹⁷

Verimli veri toplama için en iyi uygulamalar şunlardır:

- **Hassasiyet:** Performans yükünü en aza indirmek için hassas ve spesifik filtreler kullanılması önerilir.¹⁹
- **Doğrulama:** Kapsamlı dağıtımdan önce filtrelerin kontrollü ortamlarda test edilmesi önemlidir.¹⁹
- **Halka Tampon (Ring Buffer):** Aralıklı sorunlar için, Wireshark'ı depolama alanını doldurmadan zaman içinde veri yakalamak üzere bir halka tampon (örneğin, her biri 10 MB'lık 10 dosya) kullanacak şekilde yapılandırmak faydalıdır.¹⁸
- **Karışık Mod (Promiscuous Mode):** Varsayılan olarak, Wireshark paketleri karışık modda yakalar; bu, ağ arayüzü tarafından görülen tüm paketleri, sadece yerel makineye yönelik olanları değil, içerir. Bu ayar tercihlerde etkinleştirilebilir/devre dışı bırakılabilir.³

Aşağıda, oyuna özgü protokollere ve yaygın oyun sorunlarına yönelik örnekler yer almaktadır:

Tablo: Oyun Trafiği için Wireshark Yakalama Filtresi Örnekleri

Filtre Amacı	Filtre Sözdizimi	Açıklama/Kullanım Durumu	İlgili Oyun/Protokol
Belirli Oyun Trafiğini Yakalama	host <oyun_sunucusu_IP_adresi> and (tcp port <oyun_tcp_portu> or udp port <oyun_udp_portu>)	Belirli bir oyun sunucusu IP'sine ve portlarına yönelik TCP veya UDP trafiğini yakalar.	CS2, Valorant, PUBG, Unreal Engine
CS2 (Steam) Trafiği	(tcp port 27015 or tcp port 27036) or (udp port 27015 or udp portrange 27031-27036)	CS2'nin Steam sürümü için gerekli TCP ve UDP portlarını yakalar.	CS2 ¹
Valorant Oyun İstemcisi Trafiği	udp portrange 7000-7999	Valorant oyun istemcisi tarafından kullanılan UDP port aralığını yakalar.	Valorant ⁹
Valorant Sesli Sohbet Trafiği	udp portrange 8000-8999	Valorant sesli sohbeti için kullanılan UDP port aralığını yakalar.	Valorant ⁹

PUBG (Steam) Trafiği	(tcp port 27015 or tcp port 27036) or (udp port 27015 or udp portrange 27031-27036)	PUBG'nin Steam sürümü için gerekli TCP ve UDP portlarını yakalar.	PUBG ¹¹
Unreal Engine Varsayılan Trafiği	udp port 7777	Unreal Engine'in varsayılan ağ portu olan UDP 7777'yi yakalar.	Unreal Engine ⁸
Protokole Göre Filtreleme	ip	Yalnızca IPv4 trafiğini yakalar, ARP/STP gürültüsünü hariç tutar.	Genel
Protokole Göre Filtreleme	udp veya tcp	Tüm UDP veya TCP trafiğini yakalar.	Genel
Protokole Göre Filtreleme	dns	Yalnızca DNS trafiğini yakalar.	Genel
istenmeyen Trafiği Hariç Tutma	not broadcast and not multicast	Yalnızca makinenize giden/gelen tek noktaya yayın trafiğini yakalar.	Genel
istenmeyen Trafiği Hariç Tutma	port not 53 and not arp	DNS ve ARP trafiği dışındaki her şeyi yakalar.	Genel
Potansiyel Sorunları Tespit Etme (örn. Port Tarama)	tcp port 22 and tcp[tcpflags] & tcp-syn!= 0	Port 22'deki SYN paketlerini arayarak potansiyel SSH kaba kuvvet saldırılarını tespit eder.	SSH
Yaygın Solucan Yayılma Girişimlerini Tespit Etme	dst port 135 or dst port 445 or dst port 1433 and tcp[tcpflags] & (tcp-syn)!= 0 and tcp[tcpflags] &	Yerel bir ağdan gelen yaygın solucan yayılma portlarındaki SYN paketlerini tespit eder.	Genel (Ağ IP aralığına göre ayarlanmalı) ²²

	(tcp-ack) = 0 and src net 192.168.0.0/24		
--	--	--	--

Modern oyunlar tarafından dinamik ve geniş port aralıklarının (örneğin, Valorant'ın 7000-7999 UDP aralığı) ve istemciler tarafından geçici portların (Unity) artan kullanımı, yüksek düzeyde spesifik tek port yakalama filtrelerinden daha geniş port aralıklarına veya süreç tabanlıfiltrelemeye doğru bir geçiş gerektirmektedir.⁷ Bu durum, yakalama filtrelerinin veri hacmini azaltmadaki hassasiyetini etkiler ve yükü yakalama sonrası görüntüleme filtrelerine veya harici süreç izleme araçlarına kaydırır.

Saldırganlar tarafından kullanılan gizleme tekniklerinin (Base64, dize birleştirme, PowerShell gibi meşru araçların kötüye kullanımı) artan karmaşıklığı, geleneksel imza tabanlı yakalama filtrelerinin etkinliğini doğrudan zorlamaktadır.²³ Belirli port ve bayrak tabanlı filtreler bilinen saldırısı kalıplarını hala tespit edebilse de, "Sistem Üzerinde Yaşayan" (Living-off-the-Land - LotL) saldırılara ve meşru araçların kötüye kullanımına doğru kayış, birçok kötü niyetli etkinliğin normal trafikle karışmasına neden olmaktadır. Bu durum, temel filtrelere atlatabilen ince anormallikleri belirlemek için yakalama filtreleriyle birlikte daha gelişmiş, davranış tabanlı tespit yöntemlerine (Bölüm 3.1 ve 3.3'te tartışıldığı gibi) ihtiyaç duyulduğunu göstermektedir.

2.2.2. Oyun Trafiği İçin Wireshark Görüntüleme Filtreleri

Görüntüleme filtreleri, paketler yakalandıktan sonra uygulanır ve yakalama sürecini etkilemeden depolanan verilerin esnek, gerçek zamanlı analizine olanak tanır. Değiştirilebilir, kaydedilebilir ve kaldırılabilirler.¹⁷

Bu filtrelerin amacı, Wireshark arayüzünde görüntülenen paketleri daraltmak ve derinlemesine analiz için belirli kriterlere odaklanmaktır.²⁷ Ana bileşenleri arasında protokol alanları (örneğin, ip.addr, tcp.port), karşılaştırma operatörleri (eq/==, ne/!=, gt/>, lt/〈, contains, matches), mantıksal operatörler (and/&&, or||, not/!) ve fonksiyonlar (len, count, upper, lower) bulunur.¹⁷ Filtreler, paket listesinin üstündeki filtre çubuğuuna girilir.³⁰ Filtreler, gelecekte kullanılmak üzere kaydedilebilir.³⁰

Aşağıda, belirli oyun olaylarını, anormallikleri veya performans metriklerini belirlemek için örnekler yer almaktadır:

Tablo: Oyun Trafiği İçin Wireshark Görüntüleme Filtresi Örnekleri

Filtre Amacı	Filtre Sözdizimi	Açıklama/Kullanım	İlgili Oyun/Protokol
--------------	------------------	-------------------	----------------------

		Durumu	
Temel Protokol Filtreleri	tcp	Tüm TCP paketlerini gösterir.	Genel
	udp	Tüm UDP paketlerini gösterir.	Genel
	http	Tüm HTTP paketlerini gösterir.	Genel
	dns	Tüm DNS paketlerini gösterir.	Genel
IP Adresi ve Port Filtreleri	ip.addr == 192.168.1.1	Belirli bir IP adresine giden/gelen paketleri gösterir.	Genel
	ip.src == 10.0.0.5	Belirli bir kaynak IP adresinden gelen paketleri gösterir.	Genel
	tcp.port == 80	TCP port 80'i kullanan paketleri gösterir.	HTTP
	udp.port == 7777	UDP port 7777'yi kullanan paketleri gösterir (örn. Unreal Engine).	Unreal Engine
	ip.addr == 192.168.1.100 and tcp.port == 80	IP adresi ve portu birleştirir.	Genel
Paket Uzunluğuna/Boyutuna Göre Filtreleme	frame.len > 1000	1000 bayttan büyük paketleri gösterir.	Genel
	tcp.len >= 100 and tcp.len <= 500	Yük uzunluğu 100 ile 500 bayt arasında olan TCP paketlerini	Genel ²⁷

		gösterir.	
İçeriğe Dayalı Filtreleme (Şifresiz Trafik için)	http.host contains "google"	"google" içeren ana bilgisayarlara giden HTTP trafiğini gösterir.	HTTP ²⁷
	frame contains "password"	Ham verilerinde "password" kelimesini içeren paketleri bulur (açık metin kimlik bilgilerini tespit etmek için kullanışlıdır).	Genel ²⁷
	http.request.method == "GET"	HTTP GET isteklerini gösterir.	HTTP ²⁷
Güvenlik Anormalliklerini Tespit Etme	tcp.flags.syn == 1 and tcp.flags.ack == 0	Potansiyel port tarama girişimlerini belirler.	Genel ²⁷
	dns and dnsqry.name contains "malicious"	Şüpheli DNS sorgularını tespit eder (potansiyel C2 iletişimini veya tünelleme).	DNS ³¹
	http.response.code >= 400	HTTP hata yanıtlarını belirler (web uygulaması saldırısı analizi için kullanışlıdır).	HTTP ²⁷
	ftp contains "530" or ssh contains "Failed"	Kaba kuvvet saldırısı tespiti için başarısız oturum açma girişimlerini belirler.	FTP, SSH ²⁷

Basit port ve IP filtrelemesinin ötesinde, paket *uzunluğunu* ve *paketler arası varış sürelerini* (IAT) görüntüleme filtreleri (örneğin, frame.len > X, frame.time_delta > Y) kullanarak analiz etmek, oyun trafiği için güçlü bir davranışsal imza görevi görebilir.³² Oluşturulan temel çizgilerden (baseline) önemli sapmalar (örneğin, oyuncu hareketi

güncellemeleri için alışılmadık derecede büyük paketler veya anormal derecede kısa/uzun IAT'ler) ağ performans sorunlarına, gizlenmiş kötü niyetli faaliyetlere²³ veya hatta hile önleme atlatma girişimlerine³⁴ işaret edebilir. Bu durum, statik imzaların ötesine geçerek Wireshark içinde dinamik davranış analizi yapılmasını gerektirir.

Açık metin içeriğe dayalı filtreler (örneğin, frame contains "password") şifrelenmemiş trafik için etkili olsa da, 2025 yılında şifrelemenin (HTTPS, TLS 1.3 ECH, SSH) yaygın olarak benimsenmesi nedeniyle kullanışlılıklarını azaltmaktadır.³⁵ Bu durum, ağ analistlerini, yükleri doğrudan incelemek yerine, şifreli oyun trafiği içindeki kötü niyetli faaliyetleri çıkarmak için *meta veri analizine* ve *davranışsal kalıplara* (paket boyutu, paketler arası varış süreleri, akış süresi, bağlantı kalıpları) daha fazla güvenmeye zorlamaktadır. Bu değişim, ETAD (Bölüm 3.2) ve yapay zeka destekli analiz (Bölüm 3.1) gibi tekniklerin önemini pekiştirmektedir.

Wireshark'ın gelişmiş görüntüleme filtrelerinden yararlanarak, analistler normal oyun akışından sapan gözlemlenen paket kalıplarına dayalı özel "oyun hile önleme imzaları" geliştirebilirler. Örneğin, imkansız oyuncu konumu güncellemelerini (paket sahteciliği³⁴) tespit etmek, udp.payload contains "teleport" (şifrelenmemişse) filtrelemesini veya alışılmadık hareket paketi dizilerinin analizini içerebilir. Benzer şekilde, zamanlama hilelerini³⁴ belirlemek, frame.time_delta analizi ile giden paketlerde anormal derecede uzun gecikmeleri ve ardından bir güncelleme patlamasını içerebilir. Bu, genel ağ güvenliğinin ötesine geçerek oyuna özgü adli analize yönelir ve hile önleme çabalarını doğrudan destekler (Bölüm 3.6).

3. Oyun Ağ Analizi İçin En İyi 10 Teknik/Trend (2025)

Ağ trafiği analizi alanı, yeni teknolojiler ve giderek karmaşıklaşan tehditler tarafından yönlendirilen hızlı bir evrim geçirmektedir. 2025 için, oyun ağ trafiğinin nasıl izlendiğini, güvence altına alındığını ve optimize edildiğini yeniden tanımlayacak birkaç önemli teknik ve trend öne çıkmaktadır.

3.1. Yapay Zeka Destekli Ağ Trafiği Analizi ile Anomali Tespiti

Yapay Zeka (YZ) ve Makine Öğrenimi (MÖ) modelleri, geleneksel imza tabanlı yöntemlerin genellikle gözden kaçıldığı anormal davranışların tespitini sağlayarak ağ trafiği analizinde devrim yaratmaktadır. Bu modeller, muazzam hacimli ağ verilerini işleyebilir, kullanıcılar ve varlıklar (cihazlar, uygulamalar) için normal davranışsal temel çizgileri öğrenebilir ve gerçek zamanlı sapmaları belirleyebilir.⁴² Bu, yeni uygulamaların tanınmasını, ani protokol değişikliklerini (örneğin, DoH, DoT) veya bot iletişimleri ve DDoS saldırıları gibi kötü niyetli faaliyetleri içerir.⁴³

2025'teki potansiyel etkileri şunlardır:

- **Proaktif Tehdit Tespiti:** YZ, sıfır gün saldırılarının ve geleneksel savunmaları atlatan sofistike, düşük hacimli şifreli tehditlerin daha hızlı ve doğru bir şekilde belirlenmesini sağlayacaktır.³⁵
- **Otomatik Yanıt:** SOAR (Güvenlik Orkestrasyonu, Otomasyon ve Yanıt) platformlarıyla entegrasyon, otomatik düzeltme eylemlerine olanak tanıyacak, manuel inceleme çabalarını azaltacak ve olay yanıt sürelerini iyileştirecektir.⁴⁵
- **Gelişmiş Karar Verme:** YZ aracılıarı, QoS etiketleme ve trafik önceliklendirme gibi rutin görevleri otomatikleştirerek daha akıllı yönlendirme ve iyileştirilmiş ağ verimliliği sağlayacaktır.⁴²
- **Saldırganlar İçin Giriş Bariyerinin Azalması:** Savunma için faydalı olsa da, YZ siber suçlular tarafından daha ikna edici kimlik avı saldırıları oluşturmak ve kötü niyetli komut dosyası üretimini otomatikleştirmek için silah olarak kullanılacak, bu da şifreli tehditlerde bir artıya yol açacaktır.³⁵

Uygulama alanları şunlardır:

- **Oyun Güvenliği:** Ağ trafiğindeki alışılmadık oyuncu davranış kalıplarını analiz ederek oyun içi hileleri (örneğin, aimbotlar, hız hileleri) tespit etme.⁵⁰
- **Ağ Performans Optimizasyonu:** Darboğazları belirleme, bakım ihtiyaçlarını tahmin etme ve ağ kaynaklarını değişen taleplere dinamik olarak uyarlama.⁴²
- **Dolandırıcılık Önleme:** Anormal oturum açma girişimlerini veya veri transferlerini işaretleyerek oyun platformları içindeki tehlikeye atılmış hesapları ve içерiden gelen tehditleri tespit etme.⁵²
- **Bulut Güvenliği:** Geleneksel izlemenin zorlandığı karma ve çoklu bulut oyun ortamlarında görünürlük ve güvenlik sağlama.⁴²

2025'te artan ağ trafiği hacmi, hızı ve şifrelemesi⁴³, geleneksel imza tabanlı tespit yöntemlerini sofistike tehditlere ve gizleme tekniklerine²³ karşı giderek daha etkisiz hale getirmektedir. Yapay zeka destekli ağ analizi, modern oyun ağ güvenliği için sadece bir geliştirme değil, bir zorunluluk haline gelmiştir. Bu durum, reaktif, bilinen tehdit tespitinden, karmaşık oyun ekosistemlerindeki yeni saldırıları ve ince sapmaları belirlemek için proaktif, uyarlanabilir davranışsal anomalî tespitine doğru temel bir paradigma değişimini temsil etmektedir. Bu, ağ güvenliği ekipleri ve araç setleri için yapay zeka/makine öğrenimi yeteneklerine önemli bir yatırım yapılmasını gerektirmektedir.

3.2. Şifreli Trafiğin Şifre Çözmeden Analizi (ETAD)

Web trafiğinin %95'inin artık şifrelenmesi ve Şifreli İstemci Merhaba (ECH) ile TLS 1.3'ün standart haline gelmesiyle, açık metin görünürlüğüne dayanan geleneksel Derin

Paket İncelemesi (DPI) giderek zorlanmaktadır. ETAD teknikleri, şifreli trafiğin meta verilerini, akış özelliklerini (paket boyutu, paketler arası varış süreleri, akış süresi) ve davranışsal kalıplarını analiz etmeye odaklanarak, yükü şifrelemeden uygulama türünü çıkarmayı, anormallikleri tespit etmeyi ve tehditleri belirlemeyi amaçlar.⁵⁷

2025'teki potansiyel etkileri şunlardır:

- **Gizliliğin Korunması:** ETAD, hassas yük verileri şifreli kaldığı için güvenlik ekiplerinin kullanıcı gizliliğine saygı duyarken tehditlere karşı görünürlüğü sürdürmesine olanak tanır.³⁷
- **TLS 1.3 ECH Kör Noktalarının Aşılması:** ETAD, TLS 1.3 ECH'nin TLS el sıkışmasının daha önce açık olan kısımlarını (örneğin, Sunucu Adı Göstergesi - SNI) gizlemesile bile ağ görünürlüğü için uygulanabilir bir çözüm sunar.³⁷
- **Saldırıların Artan Karmaşıklığı:** Tehdit aktörleri, geleneksel sistemler tarafından tespit edilmekten kaçınmak için şifreli kanalları ve düşük hacimli C2 iletişimlerini yoğunlaştıracaktır.³⁵
- **Güvenlik Aracı Odağında Değişim:** Güvenlik çözümleri, şifreli trafik kalıplarını, akış boyutlarını ve zamanlama anormalliklerini analiz etmek için makine öğrenimi/derin öğrenme modellerini giderek daha fazla entegre edecektir.⁵⁷

Uygulama alanları şunlardır:

- **Kötü Amaçlı Yazılım ve C2 Tespiti:** Anormal trafik kalıplarını veya akış özelliklerini tespit ederek şifreli kötü amaçlı yazılım iletişimini ve gizli komuta-kontrol (C2) faaliyetlerini belirleme.³⁵
- **Uygulama Parmak İzi:** QoS sağlama veya politika uygulama için farklı uygulamaları (örneğin, oyun, akış, tarama) benzersiz şifreli trafik profillerine göre sınıflandırma.⁴³
- **İçeriden Gelen Tehdit Tespiti:** Şifreli kanallar içinde alışılmadık veri sızdırma veya erişim kalıplarını belirleme.⁵⁷
- **Ağ Performans Optimizasyonu:** İçerik incelemesi yapmadan trafik türlerini ve hacimlerini anlayarak verimli bant genişliği tahsis ve yük dengeleme sağlama.⁵⁷

"Şimdi Topla, Sonra Şifre Çöz" (Harvest Now, Decrypt Later - HNDL) taktiklerinin ortaya çıkan tehdidi, yani saldırganların gelecekteki kuantum bilgisayarları kullanarak şifrelerini çözmek amacıyla şu anda şifrelenmiş verileri toplama niyeti³⁵, ETAD'a kritik bir uzun vadeli boyut katmaktadır. ETAD şifre çözmeden gerçek zamanlı anomali tespitine odaklanırken, HNDL tehdidi, hassas kullanıcı verileri veya fikri mülkiyet içeriyorsa, görünüşte zararsız şifreli oyun trafiğinin bile saldırganlar için değerli olabileceği anlamına gelir. Bu durum, sadece anlık tehditler için sağlam ETAD'ı değil, aynı zamanda gelecekteki kuantum şifre çözme yeteneklerine karşı oyun iletişimlerini

geleceğe hazırlamak için Kuantum Sonrası Criptografi (PQC) standartlarına (Bölüm 3.9) proaktif bir geçiş de gerektirmektedir.

3.3. Oyun Güvenliği İçin Kullanıcı ve Varlık Davranış Analizi (UEBA)

Kullanıcı ve Varlık Davranış Analizi (UEBA), bir ağdaki kullanıcılar (oyuncular, geliştiriciler) ve varlıklar (cihazlar, oyun sunucuları, uygulamalar) için normal davranışın bir temel çizgisini oluşturmak için gelişmiş analitik, makine öğrenimi ve istatistiksel modellemeyi kullanan bir güvenlik sürecidir. Bu temel çizgiden herhangi bir önemli sapma, potansiyel güvenlik ihlallerini, içерiden gelen tehditleri veya tehlikeye atılmış hesapları gösteren uyarıları tetikler. UEBA, hassasiyetini zamanla artırarak sürekli olarak değişikliklere uyum sağlar.⁵²

2025'teki potansiyel etkileri şunlardır:

- **Gelişmiş İçeriden Tehdit Tespiti:** UEBA, meşru erişime sahip ancak bunu kötüye kullanan içерiden kişilerin (örneğin, geliştiriciler, yöneticiler) kötü niyetli veya ihmalkar faaliyetlerini tespit etmek için kritik öneme sahiptir.⁵²
- **Proaktif Tehlikeye Atılmış Hesap Tespiti:** Yabancı konumlardan veya alışılmadık zamanlarda beklenmedik oturum açma girişimleri veya alışılmadık veri transferleri gibi şüpheli faaliyetleri işaretleyerek hesapları tehlikeye atılmaktan korur.⁵²
- **Uyarlanabilir Tehdit Tespiti:** UEBA'nın sürekli öğrenmesi, gelişen siber tehditlere uyum sağlamasına ve geleneksel imza tabanlı sistemlerin gözden kaçırabilecegi sofistike saldırıları (örneğin, APT'ler, düşük profilli C2) belirlemesine olanak tanır.⁶¹
- **Azaltılmış Yanlış Pozitifler:** Normal davranışını anlayarak, UEBA güvenlik ekipleri için uyarı yorgunluğunu en aza indirebilir ve onların gerçek tehditlere odaklanmasılığını sağlayabilir.⁶¹

Uygulama alanları şunlardır:

- **Oyun Geliştirme Güvenliği:** Kod depolarına, derleme sunucularına, uzaktan hata ayıklamaya erişim gibi geliştirici faaliyetlerini izleyerek yetkisiz erişim, büyük veri sızdırma veya ayrıcalık yükseltme gibi anormallikleri tespit etme.⁶¹
- **Hile Önleme Sistemleri:** Oyuncu eylemlerindeki (örneğin, imkansız hareket, hızlı istatistiksel sıçramalar) hileye işaret eden davranışsal anormallikleri belirleme, sunucu tarafı ve istemci tarafı hile önleme sistemlerini tamamlama.³⁴
- **Bulut Ortamı Güvenliği:** Çoklu bulut altyapılarında varlık davranışını izleyerek yanlış yapılandırmaları, bulut varlıklarına yetkisiz erişimi ve gölge BT'yi tespit etme.⁵⁴
- **Uzaktan Çalışma Güvenliği:** Uzaktan çalışan geliştiriciler ve oyuncular için alışılmadık oturum açma kalıplarını veya ağ bağlantılarını izleyerek uzaktan erişimi

güvence altına alma.⁴⁵

2025'te UEBA, özellikle karmaşık bulut ve uzaktan çalışma ortamlarında faaliyet gösteren yazılım geliştirme ekipleri için geleneksel ağ güvenliği ve uygulama güvenliği arasında kritik bir köprü haline gelmektedir. Geliştiriciler için davranışsal temel çizgiler (örneğin, tipik kod deposu erişim süreleri, derleme sunucusu etkileşimleri, uzaktan hata ayıklama oturumları) oluşturarak, UEBA, tehlkiye atılmış geliştirici hesapları, içерiden gelen tehditler veya tedarik zinciri saldırılарını gösteren anormallikleri proaktif olarak tespit edebilir.⁵⁴ Örneğin, bir geliştiricinin normal çalışma saatleri dışında bir üretim veritabanına erişmesi veya daha önce böyle bir eylemi olmayan bir kullanıcının bir sürüm kontrol sisteminden⁸⁹ aniden büyük bir indirme yapması işaretlenecektir. Bu ayrıntılı, bağlama duyarlı izleme, gelişen tehditlere karşı yazılım geliştirme yaşam döngüsünü güvence altına almak için hayatı öneme sahiptir.

3.4. Derin Paket İncelemesi (DPI) Gelişmeleri ve Zorlukları

Derin Paket İncelemesi (DPI), bir paketin bir inceleme noktasından geçerken veri kısmını (yük) ve başlığını inceleyen bir teknolojidir. Bu, ağ kullanım kalıpları, uygulama tanımlaması ve tehdit tespiti hakkında ayrıntılı bilgiler sağlar. DPI pazarı, artan siber saldırılar, 5G ve IoT'nın benimsenmesi ve Sıfır Güven güvenlik çerçevelerinin genişlemesiyle önemli bir büyümeye yaşamaktadır.⁶⁷

2025'teki potansiyel etkileri şunlardır:

- **Gelişmiş Tehdit Tespiti:** Genellikle YZ ve MÖ içeren yeni nesil DPI, kötü amaçlı yazılım ve fidye yazılımı gibi sofistike siber tehditleri proaktif olarak azaltarak tehdit tespitinin hassasiyetini artıracaktır.⁶⁷
- **Ağ Optimizasyonu:** DPI, ağ kullanımına ilişkin ayrıntılı bilgiler sağlayarak operatörlerin bant genişliğini önceliklendirmesine ve yüksek performanslı oyunlar için kritik olan sorunsuz kullanıcı deneyimleri sağlamasına olanak tanır.⁶⁷
- **Şifreleme ile İlgili Zorluklar:** TLS 1.3 ECH'nin yaygın olarak benimsenmesi, daha fazla trafiğin tamamen opak hale gelmesiyle geleneksel DPI'yi giderek körlestirecek ve şifrelemeye dayanmayan analize doğru itecektir.³⁷
- **Maliyet ve Karmaşıklık:** DPI sistemlerini uygulamak ve yönetmek karmaşık ve maliyetli olabilir, özel donanım, yazılım ve yetenekli personel gerektirebilir ve doğru yapılandırılmazsa gecikmeye neden olabilir.⁶⁷

Uygulama alanları şunlardır:

- **Ağ Güvenliği:** Veri paketleri içinde gizlenmiş kötü niyetli içeriği tespit etme ve engelleme, belirli saldırı türlerini belirleme ve güvenlik politikalarını uygulama.⁶⁸
- **Uygulama Kontrolü:** Hizmet Kalitesi (QoS) için belirli uygulamaları tanımlama ve

yönetme (örneğin, oyun trafiğini büyük indirmelere göre önceliklendirme).⁶⁷

- **Uyumluluk:** Hassas veri akışını kontrol ederek kuruluşların yasal gerekliliklere uymasına yardımcı olma.⁶⁸
- **Trafik Şekillendirme:** Uygulama türüne veya kullanıcı önceliğine göre trafiği şekillendirerek ağ performansını optimize etme, rekabetçi oyunlar için kritik öneme sahip.⁶⁸

DPI geleneksel olarak yük incelemesine dayanırken, 2025'te TLS 1.3 ECH'nin yaygın olarak benimsenmesi³⁷, şifre çözmeden derin içerik görünürüğünü sağlama yeteneğini temelden zorlamaktadır. Bu durum, DPI çözümlerini, içeriği değil, şifreli trafik *meta verilerini ve davranışsal kalıpları* (ETAD ilkeleri) analiz etmek için yapay zeka ve makine öğrenimi⁶⁷ kullanmaya zorlamaktadır. Bu nedenle, oyun ağlarındaki DPI'nin geleceği, belirli oyun protokolü yüklerini (şifrelenmemişse) incelemekten ziyade, akış özelliklerine dayalı uygulama türlerini belirlemek, anormallikleri tespit etmek ve politikaları uygulamak veya yasal ve etik olarak izin verilen yerlerde şifre çözme proxy'leriyle entegre olmakla ilgili olacaktır.

3.5. Oyun Ağlarında Sıfır Güven Mimarisi (ZTA) Entegrasyonu

Sıfır Güven Mimarisi (ZTA), "asla güvenme, her zaman doğrula" ilkesiyle çalışan bir güvenlik çerçevesidir. Bir ağ çevresindeki her şeyin güvenli olduğunu varsaymak yerine, ZTA her kullanıcıyı, cihazı ve isteği potansiyel olarak kötü niyetli olarak ele alır, sürekli doğrulama ve katı erişim kontrolleri gerektirir. Benimsenmesi, Derin Paket İncelemesi (DPI) pazarı için önemli bir itici güçtür ve akış tabanlı izleme ile giderek daha fazla entegre edilmektedir.⁴⁵

2025'teki potansiyel etkileri şunlardır:

- **Gelişmiş Güvenlik Durumu:** ZTA, en az ayırmalı erişim ve sürekli kimlik doğrulama uygulayarak saldırının yüzeyini önemli ölçüde azaltır, bu da saldırganların zayıf noktaları kullanmasını veya oyun ağları içinde yanal hareket etmesini çok daha zor hale getirir.⁵⁰
- **İçeriden Gelen Tehditlerin Azaltılması:** Kullanıcı ve varlık davranışını sürekli doğrulayarak, ZTA, özellikle UEBA ile entegre edildiğinde, içерiden gelen tehditlere ve tehlikeye atılmış hesaplara karşı oldukça etkilidir.⁵²
- **Güvenli Bulut Oyunculuğu:** ZTA, geleneksel çevre tabanlı güvenlik modellerinin yetersiz kaldığı karma ve çoklu bulut oyun ortamlarını güvence altına almak için kritik öneme sahiptir.⁶⁸
- **Gelişmiş Uyumluluk:** ZTA, kullanıcı davranışları hakkında ayrıntılı bilgiler sağlayarak ve anormal faaliyetlerin hızlı bir şekilde belirlenmesini sağlayarak kuruluşların katı veri koruma ve gizlilik gerekliliklerini karşılamasına yardımcı olur.⁶¹

Uygulama alanları şunlardır:

- **Oyuncu Hesap Güvenliği:** Oyuncu oturum açmaları ve oyun içi işlemler için çok faktörlü kimlik doğrulama (MFA) ve sürekli doğrulama uygulama.⁷⁰
- **Oyun Sunucusu Koruması:** Oyun sunucularını ve geliştirme ortamlarını mikro segmentlere ayırma, yalnızca yetkili hizmetlerin ve kullanıcıların bunlarla iletişim kurabilmesini sağlama.⁴⁵
- **Geliştirici Ortamı Güvenliği:** Hassas kod depolarına, derleme sunucularına ve hata ayıklama araçlarına erişimi, katı kimlik ve erişim yönetimi (IAM) politikaları uygulayarak güvence altına alma.⁵⁴
- **Uzaktan Oynama/Bulut Oyunculuğu:** Konumdan bağımsız olarak her bağlantıyı doğrulayarak oyuncular ve geliştiriciler için güvenli ve ölçeklenebilir uzaktan bağlantı sağlama.⁴⁵

2025'te Sıfır Güven Mimarisi'nin (ZTA) yaygın olarak benimsenmesi, özellikle oyun ağlarında, ayrıntılı ağ görünürüğünde büyük bir artışı zorunlu kılmaktadır. ZTA'nın "ihlal varsayımları" zihniyeti⁵⁵, ağ içindeki yanal (doğu-batı) hareket de dahil olmak üzere her bağlantının sürekli izlenmesini ve doğrulanmasını gerektirir.⁴⁵ Bu durum, protokol kullanımını, uygulama davranışını ve kullanıcı faaliyetleri hakkında ayrıntılı bilgi sağlayabilen gelişmiş DPI⁶⁸ ve akış tabanlı izleme⁴⁵ çözümlerinin entegrasyonunu teşvik etmektedir. Bu kapsamlı görünürlük olmadan, ZTA'nın temel ilkeleri olan mikro segmentasyon doğrulaması ve içерiden gelen tehdit tespiti etkili bir şekilde gerçekleştirilemez, bu da Wireshark ve entegre platformlar gibi ağ analizi araçlarını ZTA uygulaması için daha da kritik hale getirmektedir.

3.6. Ağ Adli Bilişimini Kullanan Gelişmiş Hile Önleme Sistemleri

Geleneksel hile önleme sistemleri genellikle istemci tarafında imza tabanlı tespit veya bellek taramasına dayanır ve bu da hile geliştiricileriyle sürekli bir "kedi-fare" oyununa yol açar. 2025'teki gelişmiş hile önleme sistemleri, paket sahteciliği, zamanlama hileleri (örneğin, kasıtlı olarak geciktirilmiş güncellemeler) ve imkansız oyuncu eylemleri gibi ağ trafiğindeki ince anomalilikleri tespit etmek için sunucu tarafı davranış analizi ve ağ adli bilişimini giderek daha fazla kullanmaktadır.³⁴

2025'teki potansiyel etkileri şunlardır:

- **Daha Sağlam Hile Tespiti:** Tespit mantığını sunucu tarafına kaydırmak ve ağ trafiği kalıplarını analiz etmek, hile önleme sistemlerini istemci tarafı atlatmalara ve polimorfik hilelere karşı daha dirençli hale getirir.⁵¹
- **Gelişmiş Oyuncu Deneyimi:** Daha adil oyun ortamları, daha yüksek oyuncu tutma ve memnuniyetine yol açar ve bir oyuncunun ticari başarısını doğrudan etkiler.³⁴

- **YZ Destekli Anomali Tespiti:** YZ/MÖ entegrasyonu, hileye işaret eden "super insan" davranışlarını veya alışılmadık ağ etkileşimlerini belirlemek için gerçek zamanlı davranış analizi yapılmasına olanak tanır.⁵⁰
- **Artan Sunucu Tarafı İşleme:** Hile tespiti için oyun sunucusunda daha fazla yetki, performans düşüşünü önlemek için artan işleme gücü ve optimize edilmiş ağ kodu gerektirir.⁶⁴

Uygulama alanları şunlardır:

- **Gerçek Zamanlı Oyun Bütünlüğü:** İstemci tarafından bildirilen eylemler ile sunucu tarafından doğrulanın oyun durumu arasındaki tutarsızlıkları analiz ederek hız hileleri, işinlanma ve aimbotlar dahil olmak üzere çeşitli ağ tabanlı hile biçimlerini tespit etme ve azaltma.³⁴
- **Paket Manipülasyon Tespiti:** Paket dizileri, paketler arası varış süreleri ve yük tutarlılığı analizi yoluyla paket sahteciliğini (yanlış bilgi göndermek için ağ paketlerini değiştirmeye) ve zamanlama hilelerini (ilden paketleri kasıtlı olarak geciktirmeye) belirleme.
- **Davranışsal Profilleme:** Normal oyuncu ağ davranışının profillerini oluşturma ve otomatik hile araçlarını veya komut dosyalarını düşündüren sapmaları işaretleme.⁵⁰
- **Adli Soruşturma:** Ciddi hile veya istismar durumlarında olay sonrası analiz ve kanıt toplama için ayrıntılı ağ trafiği günlükleri sağlama.³⁴

2025'te hile önleme sistemlerinin evrimi, daha geniş siber güvenlik ve ağ adli bilişim teknikleriyle güçlü bir yakınsama göstermektedir. Paket sahteciliği tespiti, zamanlama hile analizi ve ağ trafiğinin davranışsal profilini çıkarma gibi yöntemler³⁴, gelişmiş ağ anomali tespiti ve tehdit avcılığı ilkelerinin doğrudan uygulamalarıdır. Bu durum, Wireshark gibi araçların derin paket incelemesi ve davranışsal kalıp tanıma için kullanılması da dahil olmak üzere genel ağ güvenliği analizi uzmanlığının, oyun endüstrisinde etkili hile önleme çözümleri geliştirmek için giderek daha fazla aktarılabilir ve kritik olduğunu göstermektedir. Oyun geliştiricileri ve güvenlik ekipleri, oyunları içinde siber suçlarla mücadele ederek, kurumsal ağ güvenliğinde karşılaşılan zorlukları yansımaktadır.

3.7. Bulut Yerel Ağ İzleme ve Analizi (Örn. Stratoshark)

Oyun geliştirme ve dağıtımının giderek çoklu bulut ve karma ortamlara kaymasıyla, geleneksel ağ izleme araçları görünürlük boşlukları ve entegrasyon karmaşıklıklarıyla karşılaşmaktadır. Stratoshark gibi bulut yerel ağ izleme çözümleri, Wireshark gibi geleneksel paket analizi araçlarının yeteneklerini, sadece ağ paketleri yerine sistem çağrılarını ve günlükleri analiz ederek bulut iş yüklerine genişletir. Bu, kapsayıcılar, Kubernetes ve sunucusuz işlevler içindeki etkinlik hakkında derinleşimli görünürlük

sağlar.⁷¹

2025'teki potansiyel etkileri şunlardır:

- **Birleşik Bulut Görünürlüğü:** Stratoshark ve benzeri araçlar, bulut ortamlarında sistem çağrılarını, dosya G/Ç'yi, komut yürütütmelerini ve ağ etkinliğini analiz etmek için tanık bir Wireshark benzeri arayüz sunar, geleneksel paket yakalamanın zor olduğu yerlerde kapsamlı görünürlük sağlar.⁷¹
- **Gelişmiş Bulut Güvenliği:** Bulut yerel güvenlik araçlarıyla (örneğin, Falco) entegrasyon sayesinde, bu çözümler çalışma zamanı güvenliği için bağımsız görünürlük sağlayabilir, dinamik bulut ortamlardaki tehditleri tespit etmeye ve bunlara yanıt vermeye yardımcı olabilir.⁷³
- **Bulut Yerel Uygulamalarda Sorun Giderme:** Geliştiriciler, kapsayıcılar içindeki dahili sistem etkinliğini ve ağ etkileşimlerini analiz ederek performans sorunlarını teşhis edebilir ve karmaşık mikro hizmet iletişimini hata ayıklayabilir.⁵⁴
- **Veri Dağılımı ve Yanlış Yapılandırmaların Giderilmesi:** Bulut yerel izleme, bulut ihlallerinin yaygın nedenleri olan bilinmeyen varlıklarını belirlemeye, risklerini haritalandırmaya ve yapılandırma sapmalarını işaretlemeye yardımcı olur.⁵⁴

Uygulama alanları şunlardır:

- **Bulutta Oyun Sunucusu İzleme:** AWS, Azure veya Google Cloud'da barındırılan oyun sunucularının davranışları hakkında derinleşimli bilgiler edinme, dahili süreç iletişimini ve kaynak kullanımını dahil.⁵⁴
- **Kapsayıcılı Oyun Geliştirme:** Oyun geliştirme, test etme ve dağıtım için kullanılan Docker kapsayıcıları veya Kubernetes kümeleri içindeki ağ trafiğini ve sistem çağrılarını analiz etme.⁵⁴
- **Bulut Güvenlik Durumu Yönetimi (CSPM):** Çoklu bulut oyun altyapısında güvenlik yanlış yapılandırmalarını ve güvenlik açıklarını belirleme ve düzeltme.⁵⁴
- **DevSecOps Entegrasyonu:** Bulut yerel oyun geliştirme için CI/CD işlem hatlarına güvenlik kontrolleri ve izleme gömme, yapay zeka tabanlı kod tarama ve otomatik düzeltme kullanma.⁷⁰

2025'in bulut yerel oyun ortamlarında, "ağ trafiği" kavramı geleneksel ağ paketlerinin ötesine geçmektedir. Stratoshark gibi araçlar⁷¹, kritik etkileşimlerin çoğunu, sadece ağ üzerinde değil, sistem çağrıları katmanında (örneğin, ağ işlemleriyle ilgili süreçler arası iletişim, dosya G/Ç) gerçekleştigini kabul etmektedir. Bu soyutlama, Wireshark'ın harici ağ arayızları için hayatı önemini korurken, dahili bulut görünürlüğünün ağ etkinliğini *ima eden sistem düzeyindeki olayları* analiz etmeyi gerektirdiği anlamına gelir. Bu paradigma değişimi, geleneksel paket yakalamanın yetersiz kaldığı dağıtılmış, kapsayıcılı ve sunucusuz oyun altyapılarında kapsamlı görünürlük elde etmek için oyun

geliştiricileri ve güvenlik profesyonelleri için yeni araç setleri ve uzmanlık gerektirmektedir.

3.8. Uzaktan Paket Yakalama ve Akış Tabanlı İzleme Entegrasyonu

Ağlar bulut ortamlarını, şube ofislerini ve uzaktan çalışan iş gücünü kapsayacak şekilde daha dağıtık hale geldikçe, ağ trafigini uzaktan yakalama ve analiz etme yeteneği kritik hale gelmektedir. Akış tabanlı izleme (örneğin, NetFlow, sFlow, IPFIX), trafik kalıpları, kaynaklar, hedefler ve bant genişliği tüketimi hakkında üst düzey bilgiler sağlarken, uzaktan paket yakalama (Wireshark aracları veya ağ TAP'leri gibi araçlar kullanarak) dağıtılmış konumlardan tek tek paketlerin ayrıntılı, derinlemesine analizini sunar. Bu iki yaklaşımın entegrasyonu, kapsamlı ağ görünürlüğü sağlar.⁵⁷

2025'teki potansiyel etkileri şunlardır:

- **Kapsamlı Görünürülük:** Üst düzey akış verilerini ayrıntılı paket yakalama ile birleştirmek, ağ davranışına ilişkin bütünsel bir görünüm sağlayarak anormalliklerin daha hızlı belirlenmesini ve kök neden analizini mümkün kılar.⁵⁷
- **Verimli Sorun Giderme:** Uzaktan paket yakalama, BT ekiplerinin dağıtılmış ortamlarda belirli ağ sorunlarını (örneğin, oyunlarda gecikme, paket kaybı) fiziksel olarak bulunmadan teşhis etmesine olanak tanıyarak olay yanıt sürelerini iyileştirir.⁶⁵
- **Uzaktan/Bulutta Gelişmiş Güvenlik:** Bu entegrasyon, çoklu bulut ve uzaktan erişim senaryolarında şifreli trafik içindeki içерiden gelen tehditleri, yanal hareketi ve gizli tehditleri tespit etmek için hayatı öneme sahiptir.⁵⁷
- **Ölçeklenebilirlik:** Akış tabanlı izleme, minimum CPU/bellek ayak izi sunarak dağıtılmış sensörler için uygun hale gelirken, paket yakalama daha derinleşimli inceleme için seçici olarak tetiklenebilir.⁵⁷

Uygulama alanları şunlardır:

- **Dağıtılmış Oyun Sunucusu Yönetimi:** Coğrafi olarak dağıtılmış veri merkezleri ve bulut bölgeleri arasında oyun sunucusu performansını ve bağlantısını izleme ve sorun giderme.⁴⁵
- **Uzaktan Geliştirme Ortamı İzleme:** Uzaktan oyun geliştirme ekiplerinin ağ etkinliğine görünürlük kazandırma, kaynaklara güvenli erişim sağlama ve şüpheli trafigi belirleme.⁶⁵
- **Bulut Oyun Altyapısı:** Bulut tabanlı oyun platformlarından gelen trafik akışlarını analiz etme ve paketleri yakalama, performansı optimize etme, bant genişliğini yönetme ve güvenlik tehditlerini tespit etme.⁴⁵
- **Olay Yanımı ve Adli Bilişim:** Şüpheli kalıpları belirlemek için akış verilerini kullanma ve ardından güvenlik olaylarının ayrıntılı adli analizi için paket yakalama ile

derinlemesine inceleme.⁵⁷

AKİŞ tabanlı izlemenin uzaktan paket yakalama araçlarıyla (Wireshark gibi) 2025'te entegrasyonu, güçlü bir "genel bakıştan mikroskopik analize" ağ analizi iş akışı oluşturmaktadır. AKİŞ verileri (NetFlow, sFlow) başlangıçtaki alarm sistemi görevi görerek, dağıtılmış oyun ağlarındaki geniş anomalilikleri veya eğilimleri belirler.⁴⁵ Bir ilgi alanı işaretlendiğinde, kök neden analizi, uygulama katmanı performans sorunları veya derin güvenlik incelemeleri için ayrıntılı paket düzeyinde bilgi elde etmek amacıyla belirli bir konumda (örneğin, belirli bir oyun sunucusu, bir geliştiricinin uzaktan makinesi) uzaktan paket yakalama başlatılabilir.⁴⁵ Bu katmanlı yaklaşım, kaynak kullanımını optimize ederken kapsamlı görünürlük sağlar ve karmaşık, dağıtılmış oyun altyapılarını yönetmek için vazgeçilmez hale gelir.

3.9. Kuantum Sonrası Kriptografi (PQC) Hazırlığı ve Ağ Etkileri

2030'larda kriptanalitik olarak ilgili kuantum bilgisayarların beklenen gelişiyile, mevcut açık anahtarlı şifreleme standartları (örneğin, RSA, ECC) savunmasız hale gelecektir. Kuantum Sonrası Kriptografi (PQC), hem klasik hem de kuantum bilgisayarların saldırılara karşı güvenli olacak şekilde tasarlanmış kriptografik algoritmaları ifade eder. Tehdit aktörleri, kuantum bilişim uygulanabilir hale geldiğinde şifrelerini çözmek amacıyla şifreli iletişimleri ("şimdi topla, sonra şifre çöz" - HNDL) arşivleyerek buna şimdiden hazırlanmaktadır. NIST, ilk PQC standartlarını Ağustos 2024'te tamamlamıştır.³⁵

2025'teki potansiyel etkileri şunlardır:

- **Veri Maruz Kalma Riski:** Bugün güçlü klasik algoritmalarla şifrelenmiş veriler bile, gelecekte kuantum bilgisayarlar tarafından şifresi çözülebilir, bu da hassas oyun verileri (oyuncu bilgileri, fikri mülkiyet) için uzun vadeli bir risk oluşturur.³⁵
- **Benimseme Aciliyeti:** Kuruluşlar, eski sistemlerin geçişinin karmaşıklığına rağmen, verilerini gelecekteki şifre çözme tehditlerine karşı korumak için PQC standartlarını benimsemeye öncelik vermelidir.³⁵
- **Ağ Analizi Evrimi:** Ağ analizi araçları, uzun vadeli veri güvenliğini ve uyumluluğunu sağlamak için bu yeni kriptografik standartları dahil etmek ve doğrulamak üzere evrimleşmeliidir.³⁵
- **Artan Gizleme:** Tehdit aktörleri, PQC benimsenmesinin yavaş bir süreç olduğunu bilerek gizlilik için şifreli kanalları kullanmaya devam edebilir, bu da mevcut ETAD tekniklerini daha da kritik hale getirir.³⁵

Uygulama alanları şunlardır:

- **Oyun Veri Koruması:** Hassas oyuncu verilerini (örneğin, kişisel bilgiler, ödeme

ayrıntıları, oyun içi varlıklar) ve fikri mülkiyeti (oyun kodu, tasarım belgeleri) PQC'ye dayanıklı şifreleme ile güvence altına alma.⁴⁷

- **Güvenli Oyun Güncellemeleri:** Oyun yamalarının ve güncellemelerinin geliştiricilerden oyunculara bütünlüğünü ve gizliliğini sağlama, tedarik zinciri saldırısını önlemeye.
- **Güvenli İletişim Kanalları:** Oyun istemcileri, sunucular ve geliştirme ortamları arasındaki güvenli iletişim için PQC uygulama (örneğin, TLS, SSH).
- **Uzun Vadeli Arşiv Güvenliği:** Onlarca yıl boyunca gizli kalması gerekebilecek arşivlenmiş oyunla ilgili verileri (örneğin, oyuncu günlükleri, işlem geçmişleri) koruma.

TLS 1.3 gibi modern şifreleme protokollerini, geçici oturum anahtarlarını kullanarak Mükemmel İleri Gizlilik (PFS) hedeflese de³⁷, "Şimdi Topla, Sonra Şifre Çöz" (HNDL) kuantum tehdidi, özellikle *uzun vadeli statik anahtarlar* tarafından korunan verileri veya yaygın PFS benimsenmesinden önce yakalanan verileri hedef almaktadır. Kuantum Sonrası Kriptografi (PQC) standartlarına geçişin yavaş ve karmaşık olması⁴⁷, oyun kuruluşlarının sadece yeni sistemler için PQC uygulamakla kalmayıp, mevcut şifreli veri arşivlerinin riskini de değerlendirmeleri gerektiği anlamına gelir. Bu durum, ağ analizi için ikili bir zorluk ortaya koymaktadır: mevcut iletişimleri PQC ile belirlemek ve korumak, ayrıca geçmiş verilerin kuantum güvenlik açığını geriye dönük olarak değerlendirmek, potansiyel olarak yeniden şifreleme veya güvenli silme stratejileri gerektirmektedir.

3.10. Wireshark için Betikleme ve Otomasyon (Örn. Lua, Python)

Wireshark, etkileşimli paket analizi için güçlü bir grafik kullanıcı arayüzü (GUI) sunsa da, Lua ve Python (örneğin, pyshark gibi kütüphaneler aracılığıyla) gibi betik dilleri, Wireshark'in yeteneklerinin gelişmiş otomasyonunu, özelleştirilmesini ve entegrasyonunu sağlar. Bu, özel oyun protokoller için özel ayıristırıcılar yazmayı, filtrelemeyi genişletmek için ardıl ayıristırıcılar oluşturmayı, tap'lar kullanarak belirli veri noktalarını toplamayı ve büyük veri kümeleri için analiz iş akışlarını otomatikleştirmeyi içerir.⁷⁷

2025'teki potansiyel etkileri şunlardır:

- **Özel Protokol Analizi:** Geliştiriciler, özel oyun protokoller için özel ayıristırıcılar oluşturabilir, bu da Wireshark'in oyuna özgü verileri yerel olarak tanımayacağı şekilde derinlemesine anlamasını ve görüntülemesini sağlar.⁷⁷
- **Otomatik Tehdit Avcılığı:** Betikler, belirli kalıpları arama, tehlike göstergelerini (IOC) ayıklama veya büyük yakalama dosyalarından raporlar oluşturma gibi tekrarlayan analiz görevlerini otomatikleştirebilir.⁷⁹

- **CI/CD ile Entegrasyon:** Ağ analizi, oyun geliştirme için otomatik test işlem hatlarına entegre edilebilir, geliştirme sırasında ağ performansı ve güvenliğinin sürekli izlenmesine olanak tanır.³
- **Gelişmiş Filtreleme ve Veri Çıkarma:** Ardıl ayırtıcılar ve tap'lar, harici araçlarda daha fazla analiz için yüksek düzeyde özelleştirilmiş filtrelere mekanizmalarının ve belirli veri noktalarının çıkarılmasını sağlar.⁷⁷

Uygulama alanları şunlardır:

- **Oyun Protokolü Tersine Mühendisliği:** Belgelenmemiş oyun protokollerini ve iletişim kalıplarını anlamak için Lua'da ayırtıcılar prototipleme.⁸⁶
- **Otomatik Performans Testi:** Otomatik oyun testleri sırasında ağ performansı metriklerini (örneğin, gecikme, paket kaybı) yakalamak ve analiz etmek için Wireshark'ı betikleme.³
- **Özel Hile Önleme Mantığı:** Bir oyunun protokolüne özgü hileye işaret eden belirli ağ kalıplarını belirlemek ve işaretlemek için betikler geliştirme.³⁴
- **Geliştirici Aracı Trafik Analizi:** Oyun geliştirme araçları (örneğin, Git, SVN, Jenkins, TeamCity, Visual Studio, GDB) tarafından oluşturulan ağ trafiğini analiz ederek güvenlik risklerini veya performans darboğazlarını belirleme.⁸⁸

Oyunların ağ trafiğini analiz etmenin ötesinde, *oyun geliştirme araçlarının* (örneğin, sürüm kontrolü için Git/SVN, CI/CD için Jenkins/TeamCity, uzaktan hata ayıklama için Visual Studio/GDB) benzersiz ağ imzalarını belirlemek ve analiz etmek, Wireshark betikleme ve otomasyonu için kritik ve genellikle gözden kaçan bir uygulama alanını temsil etmektedir. Bu araçların her biri, belirgin iletişim kalıpları, protokoller (örneğin, Git/SVN HTTP/HTTPS üzerinden, Jenkins/TeamCity REST API çağrıları, Visual Studio uzaktan hata ayıklama TCP 6510 üzerinde, GDB uzaktan seri protokolü)³³ ve portlar sergiler. Wireshark'ı Lua veya Python ile betiklemek, bu belirli imzaların tespitini otomatikleştirebilir, güvenlik ekiplerinin kaynak koduna yetkisiz erişimi, tehlkiye atılmış derleme ortamlarını veya kötü niyetli hata ayıklama faaliyetlerini izlemesini sağlayarak tüm oyun geliştirme tedarik zincirini güvence altına alabilir. Bu, proaktif güvenlik için çok önemli bir alandır, çünkü geliştirme ortamındaki bir uzlaşma, nihai oyun ürünü üzerinde yıkıcı aşağı akış etkilerine sahip olabilir.

4. Sonuç ve Gelecek Görünümü

2025'te oyun ağ analizi alanı, hızlı teknolojik ilerleme ve tırmanan bir siber güvenlik silahlanma yarışı ile karakterizedir. Oyuna özgü IP adreslerini ve portlarını belirlemenin temel tekniklerinden, anomalî tespiti için en son yapay zekadan yararlanmaya ve kuantum sonrası kriptografik tehditlere hazırlanmaya kadar, ağ profesyonellerine yönelik talepler her zamankinden daha yüksektir. Wireshark, UEBA ve Sıfır Güven gibi

daha geniş güvenlik çerçeveleriyle entegrasyonu ve otomasyon ve özel protokol analizi için güçlü betikleme yoluyla yetenekleri artırılan bir köşe taşı aracı olmaya devam etmektedir.

Bu raporda elde edilen bilgiler, kritik bir değişimi vurgulamaktadır: oyunlarda etkili ağ analizi, basit paket incelemesinin ötesine geçerek davranışsal analizi, meta veri yorumlamayı ve sistem düzeyinde görünürlüğü, özellikle bulut yerel ve şifreli ortamlarda kapsamaktadır. Hile önleme mekanizmalarının genel siber güvenlik uygulamalarıyla yakınsaması, bu alanların birbirine bağlılığını daha da vurgulamaktadır. Oyunlar karmaşıklık ve erişim açısından gelişmeye devam ettikçe, sürekli öğrenme ve uyarlanabilir stratejilerle desteklenen proaktif, çok katmanlı bir yaklaşım, çevrimiçi oyun deneyimlerinin performansını, güvenliğini ve bütünlüğünü sağlamak için temel olacaktır. Gelecek görünümü, yapay zekanın daha derin entegrasyonuna, daha sofistike şifreli trafik analizine ve gelişen tehditlere karşı tüm geliştirme ve dağıtım hattını güvence altına almaya güçlü bir vurgu yapmaktadır.

Alıntılanan çalışmalar

1. CS2 Port Forwarding: A Simple Guide to Optimize Your Gaming ..., erişim tarihi Haziran 5, 2025, <https://blog.clash.gg/cs2-port-forwarding>
2. Counter-Strike: Global Offensive Port Forwarding in 2025 - PureVPN, erişim tarihi Haziran 5, 2025, <https://www.purevpn.com/port-forwarding/counter-strike-global-offensive>
3. Network Traffic Analysis with Wireshark - DEV Community, erişim tarihi Haziran 5, 2025, <https://dev.to/attiliohimeki/network-traffic-analysis-with-wireshark-4cbf>
4. Introduction to Wireshark | Network Programming in Python Tutorial - Studytonight, erişim tarihi Haziran 5, 2025, <https://www.studytonight.com/network-programming-in-python/introduction-to-wireshark>
5. Capture and Analyze Network Traffic with Wireshark - LabEx, erişim tarihi Haziran 5, 2025, <https://labex.io/tutorials/wireshark-capture-and-analyze-network-traffic-with-wireshark-415956>
6. How to interpret the data payload in a TCP stream for Cybersecurity | LabEx, erişim tarihi Haziran 5, 2025, <https://labex.io/tutorials/wireshark-how-to-interpret-the-data-payload-in-a-tcp-stream-for-cybersecurity-415400>
7. Frequently asked questions | Unity Transport | 2.0.2, erişim tarihi Haziran 5, 2025, <https://docs.unity3d.com/Packages/com.unity.transport@2.0/manual/faq.html>
8. Networking Requirements for the Collab Viewer in Unreal Engine - Epic Games Developers, erişim tarihi Haziran 5, 2025, <https://dev.epicgames.com/documentation/en-us/unreal-engine/networking-requirements-for-the-collab-viewer-in-unreal-engine>

9. How to Fix Lag in Valorant – Hone Blog, erişim tarihi Haziran 5, 2025, <https://hone.gg/blog/how-to-fix-lag-in-valorant/>
10. The Ultimate Valorant Port Forwarding Guide | PureVPN, erişim tarihi Haziran 5, 2025, <https://www.purevpn.com/uk/blog/valorant-port-forwarding/>
11. How to Perform PUBG: Battlegrounds Port Forwarding on Your Router, erişim tarihi Haziran 5, 2025, <https://www.purevpn.com/port-forwarding/playerunknowns-battlegrounds>
12. What is a Game Server? A Complete Beginner's Guide - Liquid Web, erişim tarihi Haziran 5, 2025, <https://www.liquidweb.com/gaming/>
13. The Difference between Gaming Servers & Chat Servers - PubNub, erişim tarihi Haziran 5, 2025, <https://www.pubnub.com/blog/difference-between-gaming-and-chat-servers/>
14. What Is Wireshark and How to Use It | Cybersecurity - CompTIA, erişim tarihi Haziran 5, 2025, <https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it>
15. Mastering Wireshark: The Ultimate Guide to Network Traffic Analysis - SecureMyOrg, erişim tarihi Haziran 5, 2025, <https://securemyorg.com/mastering-wireshark-securemyorg/>
16. 8 Essential Network Traffic Analysis Tools - Black Cell, erişim tarihi Haziran 5, 2025, <https://blackcell.io/8-essential-network-traffic-analysis-tools/>
17. Advanced Filtering Techniques in Wireshark - Comparitech, erişim tarihi Haziran 5, 2025, <https://www.comparitech.com/net-admin/wireshark-filtering-techniques/>
18. Tips on how to reduce or limit Wireshark's Capture file size - Community, erişim tarihi Haziran 5, 2025, <https://community.five9.com/s/article/Wireshark-Tips-on-how-to-reduce-Wireshark-s-Output-file-and-Packet-Capture-best-practices-for-Five9-Traffic>
19. How to validate capture filter rules - LabEx, erişim tarihi Haziran 5, 2025, <https://labex.io/tutorials/wireshark-how-to-validate-capture-filter-rules-419617>
20. Wireshark for BEGINNERS // Capture Network Traffic - YouTube, erişim tarihi Haziran 5, 2025, <https://www.youtube.com/watch?v=nWvscuxqais>
21. Wireshark - Infosec, erişim tarihi Haziran 5, 2025, <https://www.infosecinstitute.com/resources/hacking/wireshark/>
22. CaptureFilters - Wireshark Wiki, erişim tarihi Haziran 5, 2025, <https://wiki.wireshark.org/CaptureFilters>
23. Obfuscated Threats – The Invisible Danger in Cybersecurity ..., erişim tarihi Haziran 5, 2025, <https://www.nextron-systems.com/2025/04/09/obfuscated-threats-the-invisible-danger-in-cybersecurity/>
24. Obfuscated Files or Information - Red Canary Threat Report, erişim tarihi Haziran 5, 2025, <https://redcanary.com/threat-detection-report/techniques/obfuscated-files-information/>
25. Guide to Wireshark display filters - ITTavern.com, erişim tarihi Haziran 5, 2025, <https://www.ittavern.com/guide-to-wireshark-display-filters/>
26. Wireshark Cheat Sheet: All the Commands, Filters & Syntax - StationX, erişim

- tarihi Haziran 5, 2025, <https://www.stationx.net/wireshark-cheat-sheet/>
27. Analyze Network Traffic with Wireshark Display Filters - LabEx, erişim tarihi Haziran 5, 2025,
<https://labex.io/tutorials/wireshark-analyze-network-traffic-with-wireshark-display-filters-415944>
28. 6.4. Building Display Filter Expressions - Wireshark, erişim tarihi Haziran 5, 2025,
https://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html
29. Steps of Building Display Filter Expressions in Wireshark - GeeksforGeeks, erişim tarihi Haziran 5, 2025,
<https://www.geeksforgeeks.org/steps-of-building-display-filter-expressions-in-wireshark/>
30. How to identify suspicious network activities using Wireshark in Cybersecurity - LabEx, erişim tarihi Haziran 5, 2025,
<https://labex.io/tutorials/wireshark-how-to-identify-suspicious-network-activities-using-wireshark-in-cybersecurity-415497>
31. TryHackMe: Wireshark Traffic Analysis Walkthrough (SOC Level 1) - Jasper Alblas, erişim tarihi Haziran 5, 2025,
<https://www.jalblas.com/blog/thm-wireshark-traffic-analysis-walkthrough/>
32. Network game traffic modelling - SciSpace, erişim tarihi Haziran 5, 2025,
<https://scispace.com/pdf/network-game-traffic-modelling-2glxfvtw2o.pdf>
33. Delving Into Windows CE, Part 2: Analyzing Windows CE ... - Claroty, erişim tarihi Haziran 5, 2025,
<https://claroty.com/team82/research/delving-into-windows-ce-part-2-analyzing-windows-ce-debugging-constructs>
34. Addressing Network Packet-based Cheats in Multiplayer Games: A Secret Sharing Approach - arXiv, erişim tarihi Haziran 5, 2025,
<https://arxiv.org/html/2501.10881v1>
35. 5 Encrypted Attack Predictions for 2025 | Zscaler, erişim tarihi Haziran 5, 2025,
<https://www.zscaler.com/de/blogs/security-research/5-encrypted-attack-predictions-2025>
36. 5 Encrypted Attack Predictions for 2025 | Zscaler, erişim tarihi Haziran 5, 2025,
<https://www.zscaler.com/blogs/security-research/5-encrypted-attack-predictions-2025>
37. TLS 1.3 ECH - How to Preserve Visibility into Encrypted Traffic | Enea, erişim tarihi Haziran 5, 2025,
<https://www.enea.com/insights/tls-1-3-ech-how-to-preserve-critical-traffic-visibility-for-enterprise-and-network-security-while-safeguarding-privacy/>
38. Wireshark Network Traffic Analysis - GitHub, erişim tarihi Haziran 5, 2025,
<https://github.com/seblex9/wireshark>
39. How secure is the Subversion connection to an https URL - Super User, erişim tarihi Haziran 5, 2025,
<https://superuser.com/questions/148510/how-secure-is-the-subversion-connection-to-an-https-url>
40. Wireshark is not displaying http and https packets - Stack Overflow, erişim tarihi

Haziran 5, 2025,

<https://stackoverflow.com/questions/50085714/wireshark-is-not-displaying-http-and-https-packets>

41. Wireshark Essentials: Mastering Network Traffic Analysis | Lenovo US, erişim tarihi Haziran 5, 2025, <https://www.lenovo.com/us/en/glossary/wireshark/>
42. Key 2025 Network Trends Every IT Leader Needs to Know – Plixer, erişim tarihi Haziran 5, 2025,
<https://www.plixer.com/blog/key-2025-network-trends-every-it-leader-needs-to-know/>
43. www.arxiv.org, erişim tarihi Haziran 5, 2025, <https://www.arxiv.org/pdf/2503.22161>
44. Best User Behavior Analytics (UEBA) Solutions for 2025, erişim tarihi Haziran 5, 2025, <https://www.peerspot.com/categories/user-entity-behavior-analytics-ueba>
45. Flow-Based Monitoring in 2025: Enhancing Network Visibility and ..., erişim tarihi Haziran 5, 2025, <https://securemyorg.com/flow-based-monitoring-in-2025/>
46. Open Source UEBA Tools & Commercial Alternatives in 2025 - Research AIMultiple, erişim tarihi Haziran 5, 2025,
<https://research.aimultiple.com/open-source-ueba/>
47. 2025 Thales Data Threat Report Reveals Nearly 70% of Organizations Identify AI's Fast-Moving Ecosystem as Top GenAI-Related Security Risk - Business Wire, erişim tarihi Haziran 5, 2025,
<https://www.businesswire.com/news/home/20250520290850/en/2025-Thales-Da ta-Threat-Report-Reveals-Nearly-70-of-Organizations-Identify-AIs-Fast-Moving -Ecosystem-as-Top-GenAI-Related-Security-Risk>
48. Six Cybersecurity Trends That Will Define 2025 from HP Wolf Security | HP® Official Site, erişim tarihi Haziran 5, 2025,
<https://www.hp.com/us-en/newsroom/blogs/2025/six-cybersecurity-trends-2025.html>
49. Cybersecurity Predictions and Trends in 2025 - Zscaler, erişim tarihi Haziran 5, 2025, <https://www.zscaler.com/learn/cybersecurity-predictions-2025>
50. Game Development Security Trends in 2025 - SecuritySenses, erişim tarihi Haziran 5, 2025,
<https://securitysenses.com/posts/game-development-security-trends-2025>
51. How Anti-Cheat Works in Online Games - CXOToday.com, erişim tarihi Haziran 5, 2025, <https://cxotoday.com/sponsored/how-anti-cheat-works-in-online-games/>
52. The 2025 Guide to User & Entity Behavior Analytics (UEBA), erişim tarihi Haziran 5, 2025, <https://www.teramind.co/blog/user-and-entity-behavior-analytics-guide/>
53. Top 15 UEBA Use Cases for Today's SOCs in 2025 - Research AIMultiple, erişim tarihi Haziran 5, 2025, <https://research.aimultiple.com/ueba-use-cases/>
54. Cloud Security Challenges in 2025: Tackling Multi-Cloud, Containers, and Misconfiguration Risks - CyberSRC, erişim tarihi Haziran 5, 2025,
<https://cybersrcc.com/2025/05/12/cloud-security-challenges-in-2025-tackling-m ulti-cloud-containers-and-misconfiguration-risks/>
55. Cloud Security in 2025: Key Challenges and Effective Solutions - IntentTech Insights, erişim tarihi Haziran 5, 2025,
<https://intenttechpub.com/blog/cloud-security-in-2025-top-challenges-and-how>

-to-overcome-them/

56. Network Traffic Analysis Solutions Market Insights 2025-2034: Growth Dynamics, Trends, and Strategic Opportunities, erişim tarihi Haziran 5, 2025,
<https://blog.tbrc.info/2025/03/network-traffic-analysis-solutions-market-analysis-3/>
57. Metadata vs PCAP vs NetFlow: What's Best for Threat Detection? | Fidelis Security, erişim tarihi Haziran 5, 2025,
<https://fidelissecurity.com/cybersecurity-101/network-security/metadata-vs-pcap-vs-netflow/>
58. Unsupervised Learning Methods for Analyzing Network Traffic - DZone, erişim tarihi Haziran 5, 2025,
<https://dzone.com/articles/unsupervised-learning-methods-for-analyzing-network-traffic>
59. Guide to Threat Detection with Network Traffic Pattern Analysis ..., erişim tarihi Haziran 5, 2025,
<https://fidelissecurity.com/threatgeek/network-security/network-traffic-pattern-analysis/>
60. TLS 1.3 Impact on Network-Based Security, erişim tarihi Haziran 5, 2025,
<https://potaroo.net/ietf/all-ids/draft-camwinget-tls-use-cases-03.html>
61. What is UEBA (User and Entity Behavior Analytics)? - Palo Alto Networks, erişim tarihi Haziran 5, 2025,
<https://www.paloaltonetworks.com/cyberpedia/what-is-user-entity-behavior-analytics-ueba>
62. What is UEBA? Guide to User & Entity Behavior Analytics - OpenText, erişim tarihi Haziran 5, 2025, <https://www.opentext.com/what-is/ueba>
63. What Is User and Entity Behavior Analytics (UEBA)? | Microsoft ..., erişim tarihi Haziran 5, 2025,
<https://www.microsoft.com/en-us/security/business/security-101/what-is-user-entity-behavior-analytics-ueba>
64. To ban or not to ban: Comparing server- and client-side anti-cheat solutions - i3D.net, erişim tarihi Haziran 5, 2025,
<https://www.i3d.net/ban-or-not-comparing-server-client-side-anti-cheat-solutions/>
65. Remote Network Management in 2025: A Complete Implementation ..., erişim tarihi Haziran 5, 2025,
<https://thehtoclub.com/news/remote-network-management/>
66. CI/CD Vulnerabilities: The Jenkins and TeamCity Case Studies - Checkmarx, erişim tarihi Haziran 5, 2025,
<https://checkmarx.com/blog/navigating-the-rising-tide-of-ci-cd-vulnerabilities-the-jenkins-and-teamcity-case-studies/>
67. Unlocking the Future of Deep Packet Inspection and Processing ..., erişim tarihi Haziran 5, 2025,
<https://www.datainsightsmarket.com/reports/deep-packet-inspection-and-processing-1977238>
68. Deep Packet Inspection Market Size to Hit USD 254.37 Billion by 2034, erişim tarihi Haziran 5, 2025,
<https://www.statista.com/statistics/1134037/deep-packet-inspection-market-size/>

Haziran 5, 2025,

<https://www.precedenceresearch.com/deep-packet-inspection-market>

69. ThreatLabz 2025 VPN Report: Why 81% of Organizations Plan to Adopt Zero Trust by 2026, erişim tarihi Haziran 5, 2025,
<https://www.zscaler.com/blogs/security-research/threatlabz-2025-vpn-report-why-81-organizations-plan-adopt-zero-trust-2026>
70. Web App Security: 2025 Complete Guide | Savvycom Software, erişim tarihi Haziran 5, 2025,
<https://savvycomsoftware.com/blog/web-app-security-complete-guide-2025/>
71. Wireshark • Go Deep, erişim tarihi Haziran 5, 2025, <https://www.wireshark.org/>
72. Stratoshark: Extending Wireshark's legacy into the cloud | Sysdig, erişim tarihi Haziran 5, 2025,
<https://sysdig.com/blog/stratoshark-extending-wiresharks-legacy-into-the-cloud/>
73. Stratoshark: Wireshark for the cloud - now available! - Help Net Security, erişim tarihi Haziran 5, 2025,
<https://www.helpnetsecurity.com/2025/01/22/stratoshark-wireshark-cloud/>
74. Best Packet Capture Tools for Network Analysis Guide - MoldStud, erişim tarihi Haziran 5, 2025,
<https://moldstud.com/articles/p-best-packet-capture-tools-for-network-analysis-guide>
75. Remote Packet Capture | Daqscribe, erişim tarihi Haziran 5, 2025,
<https://daqscribe.com/wiki/resources/remote-packet-capture/>
76. The 21 Best Remote Monitoring and Management Software Of 2025 - The CTO Club, erişim tarihi Haziran 5, 2025,
<https://thectoclub.com/tools/best-remote-monitoring-and-management-software/>
77. Lua - Wireshark Wiki, erişim tarihi Haziran 5, 2025, <https://wiki.wireshark.org/lua>
78. Lua/Examples - Wireshark Wiki, erişim tarihi Haziran 5, 2025,
<https://wiki.wireshark.org/Lua/Examples>
79. BHKO407/Wireshark-network-analysis-traffic: The objective of this project is to analyze network protocols using Wireshark and Python scripting. - GitHub, erişim tarihi Haziran 5, 2025,
<https://github.com/BHK0407/Wireshark-network-analysis-traffic>
80. Wireshark MCP server for AI agents - Playbooks, erişim tarihi Haziran 5, 2025,
<https://playbooks.com/mcp/shubham-s-pandey-wireshark>
81. shubham-s-pandey/WiresharkMCP: Wireshark Packet Analyzer with MCP Integration This project integrates the MCP (Message Communication Protocol) server with Wireshark to analyze and interact with network packets. The tool enables packet capture, analysis, and management using MCP while leveraging Wireshark's Lua scripting capabilities. - GitHub, erişim tarihi Haziran 5, 2025,
<https://github.com/shubham-s-pandey/WiresharkMCP>
82. wireshark - wireshark.org protocol dissector with Osmocom additions (obsolete), erişim tarihi Haziran 5, 2025,
<https://cgit.osmocom.org/wireshark/commit/services?id=c09f3ed774a8a124eb171>

0cc332677627da04aff

83. TryHackMe_and_HackTheBox/Wireshark Packet Operations.md at master - GitHub, erişim tarihi Haziran 5, 2025,
https://github.com/jesusgavancho/TryHackMe_and_HackTheBox/blob/master/Wireshark%20Packet%20Operations.md
84. Call The Jenkins REST API From PowerShell | Documentation and Support, erişim tarihi Haziran 5, 2025,
<https://octopus.com/docs/support/call-jenkins-rest-api-from-powershell>
85. How to Do API Testing on Mobile Apps - Mobot App Testing Platform, erişim tarihi Haziran 5, 2025,
<https://www.mobot.io/blog/how-to-do-api-testing-on-mobile-apps>
86. Most Effective learning path to Reverse engineer network server of old games? - Reddit, erişim tarihi Haziran 5, 2025,
https://www.reddit.com/r/HowToHack/comments/1ids89n/most_effective_learning_path_to_reverse_engineer/
87. Exploring the Unreal Engine Client-Server Model - A Guide to Multiplayer Game Development - MoldStud, erişim tarihi Haziran 5, 2025,
<https://moldstud.com/articles/p-exploring-the-unreal-engine-client-server-model-a-guide-to-multiplayer-game-development>
88. TryHackMe_and_HackTheBox/Wireshark Traffic Analysis.md at master - GitHub, erişim tarihi Haziran 5, 2025,
https://github.com/jesusgavancho/TryHackMe_and_HackTheBox/blob/master/Wireshark%20Traffic%20Analysis.md
89. Git vs. SVN: Which version control system is right for you? - Nulab, erişim tarihi Haziran 5, 2025,
<https://nulab.com/learn/software-development/git-vs-svn-version-control-system/>
90. Hacking SVN, GIT, and Mercurial - Infosec, erişim tarihi Haziran 5, 2025,
<https://www.infosecinstitute.com/resources/hacking/hacking-svn-git-and-mercurial/>
91. Scaling Network Connections from the Jenkins Controller, erişim tarihi Haziran 5, 2025, <https://www.jenkins.io/blog/2018/09/10/scaling-network-connections/>
92. Development/Tips - Wireshark Wiki, erişim tarihi Haziran 5, 2025,
<https://wiki.wireshark.org/Development/Tips>
93. Debugging software with Visual Studio Code - Renode - documentation - Read the Docs, erişim tarihi Haziran 5, 2025,
<https://renode.readthedocs.io/en/latest/debugging/vscode.html>
94. How to use Wireshark for monitoring network activity in Cybersecurity | LabEx, erişim tarihi Haziran 5, 2025,
<https://labex.io/tutorials/wireshark-how-to-use-wireshark-for-monitoring-network-activity-in-cybersecurity-415120>
95. How to connect local agents to your TeamCity (Cloud) server - YouTube, erişim tarihi Haziran 5, 2025, <https://www.youtube.com/watch?v=dvyDCzOJJZw>
96. On-prem TeamCity Server to Bitbucket Server SSH Auth Cancel error., erişim tarihi Haziran 5, 2025,

<https://teamcity-support.jetbrains.com/hc/en-us/community/posts/1121513102593-8-On-prem-TeamCity-Server-to-Bitbucket-Server-SSH-Auth-Cancel-error>

97. Claroty explores Windows CE debugging protocols in OT environments, uncovers hidden vulnerabilities - Industrial Cyber, erişim tarihi Haziran 5, 2025,
<https://industrialcyber.co/system-design-architecture/claroty-explores-windows-ce-debugging-protocols-in-ot-environments-uncovers-hidden-vulnerabilities/>
98. packet-gdb.c « dissectors « epan - wireshark - wireshark.org protocol dissector with Osmocom additions (obsolete), erişim tarihi Haziran 5, 2025,
<https://cgit.osmocom.org/wireshark/tree/epan/dissectors/packet-gdb.c?id=ad6fc87d64de30cdcdca18168a117d2ec24591da>
99. Content Based vs Context Based Signatures for Enhanced Security | Fidelis Security, erişim tarihi Haziran 5, 2025,
<https://fidelissecurity.com/cybersecurity-101/learn/content-based-and-context-based-signatures/>
100. What is Code Signing? The Definitive Roadmap to Secure Code Signing | Keyfactor, erişim tarihi Haziran 5, 2025,
<https://www.keyfactor.com/education-center/what-is-code-signing/>
101. Network traffic analysis for IR: SSH protocol with Wireshark - Infosec, erişim tarihi Haziran 5, 2025,
<https://www.infosecinstitute.com/resources/incident-response-resources/network-traffic-analysis-for-ir-ssh-protocol-with-wireshark/>
102. Jenkins Jenkins master-slave communication issues. - Doctor Droid, erişim tarihi Haziran 5, 2025,
<https://drdroid.io/stack-diagnosis/jenkins-jenkins-master-slave-communication-issues>
103. Network Analysis with Wireshark - LabEx, erişim tarihi Haziran 5, 2025,
<https://labex.io/tutorials/wireshark-network-analysis-with-wireshark-415958>
104. Useful Wireshark features and tests for communicat... - Qlik Community - 1713499, erişim tarihi Haziran 5, 2025,
<https://community.qlik.com/t5/Official-Support-Articles/Useful-Wireshark-features-and-tests-for-communication/ta-p/1713499>
105. Walkthrough / Solution to SBT's Wireshark Challenge Activity - DEV Community, erişim tarihi Haziran 5, 2025,
<https://dev.to/immah/walkthrough-solution-to-sbts-wireshark-challenge-activity-36hf>
106. 4.7. Debugger - Wireshark, erişim tarihi Haziran 5, 2025,
https://www.wireshark.org/docs/wsdd_html_chunked/ChToolsDebugger.html
107. Wireshark · Display Filter Reference: GDB Remote Serial Protocol, erişim tarihi Haziran 5, 2025, <https://www.wireshark.org/docs/dfrref/g/gdb.html>
108. Debugging with GDB - Renode - documentation, erişim tarihi Haziran 5, 2025,
<https://renode.readthedocs.io/en/latest/debugging/gdb.html>
109. Network traffic analysis using Wireshark - LevelBlue, erişim tarihi Haziran 5, 2025,
<https://levelblue.com/blogs/security-essentials/network-traffic-analysis-using-wireshark>

110. Wireshark for Security Professionals, erişim tarihi Haziran 5, 2025,
https://computerscience.unicam.it/marcantoni/reti/laboratorio_wireshark/Wireshark%20for%20Security%20Professionals%20-%20Using%20Wireshark%20and%20the%20Metasploit%20Framework.pdf
111. TeamCity REST API | TeamCity On-Premises Documentation - JetBrains, erişim tarihi Haziran 5, 2025,
<https://www.jetbrains.com/help/teamcity/teamcity-rest-api.html>
112. Get Maximum from TeamCity Integration through REST API - Stiltsoft, erişim tarihi Haziran 5, 2025,
<https://stiltsoft.com/blog/get-maximum-from-teamcity-integration-through-rest-api/>
113. packet-gdb.c « dissectors « epan - wireshark - wireshark.org protocol dissector with Osmocom additions (obsolete), erişim tarihi Haziran 5, 2025,
<https://cgit.osmocom.org/wireshark/tree/epan/dissectors/packet-gdb.c?id=443a7ed259f40ba5cfcc7d9c1e0fe5d7fee0d18c>