# WEB BROWSER ANALİZİ

Bengü Çağla SARI

Adli Bilişim Mühendisliği, Teknoloji Fakültesi, Fırat Üniversitesi, Elazığ, Türkiye

**ÖZET**

İnternet teknolojilerinin kullanımının artması beraberinde birçok işlemi kolay bir şekilde yapılabilir hale getirdi. Bankalardan, çeşitli alışveriş sitelerinden, eğitim kurumlarından, devlet kurumlarından ve daha birçok alanlarda internet üzerinden işlemler hızlı yapılır hale geldi. İşlemlerin yapılabilmesi için kullanılan internet de bu cihazların birbirleriyle bağlantı kurmasını sağlanır. Web tarayıcı programları(World Wide Web), ağ üzerinde internet sayfalarını kullanıcı tarafından görüntülenmesini sağlar. Bu sayede kullanıcılar aramak istedikleri internet sitelerini kolayca ziyaret edebilir. Web tarayıcıları kullanıcıya yarar sağlasa da kötü niyetli kullanıcılar için de saldırı aracı olabilir. Web tarayıcı araçları kullanıcıya ait Ip adresini, coğrafi konumu, tarama geçmişini, mouse hareketlerini, sosyal medya geçmişlerini ve buna bağlı olarak reklam verenlerin kullanıcıların isteklerine göre seçenek sunmasına, görüntü verileri gibi birçok veriyi depolar. Bu çalışmada toplanan tarama geçmişi verileri incelenmiştir.

**Anahtar Kelimeler:** web tarayıcı geçmişi, adli bilişim, web browser analizi

1. **GİRİŞ**

Web tarayıcıları kullanıcıların ziyaret etmek istedikleri web sitesinin url(web üzerindeki kaynağın adresidir)[2] adresini

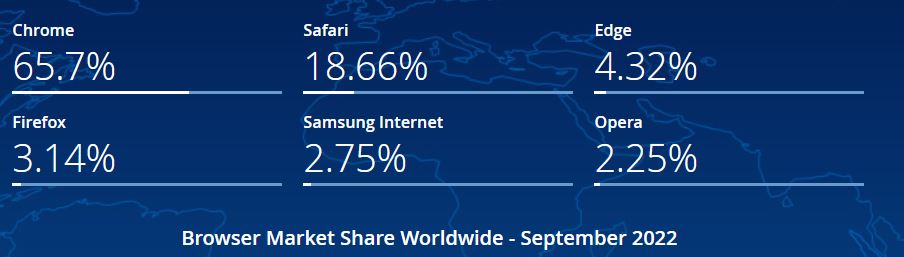
girmesi ile başlar. Girilen url adresinde web tarayıcısı önce dns’den(alan adı sunucusu) ıp adresi ister. Dns sistem adlarını ve bunlara karşılık gelen Ip adresini saklar. Tarayıcı istemci-sunucu modelinde istemci işlemini yapar. Http

protokolü(ağ üzerinden web sayfalarının görüntülenmesini sağlar)[3] ile istenen bilgiler web sunucusuna iletilir. Alınan istek sonucu sunucu bilgileri toplar ve web sayfası aracılığıyla iletir.

Web siteleri kullanıcıya ait bilgileri cookies adı verilen dosyalara kaydeder. Çerezler kullanıcı tarafından ziyaret edilen sayfaları cihaz hafızasında saklar. Kullanıcı ziyaret ettiği sayfaya tekrar gittiğinde sayfayı hatırlar, şifre istenip girildiği zaman girilen şifreyi hatırlar. Kullanıcıya ait ayrıntılı bilgileri hatırlayan çerezler de vardır. Bu çerezler kullanıcıya ait hedeflenmiş içerikleri sunar.

1. **WEB TARAYICILARI**

**1-Google Chrome:** 2008 yılında Google tarafından geliştirilmiştir. Kullanıcılar tarafından en çok tercih edilen web browser türüdür.

****

Şekil 1: En çok tercih edilen web browser türleri

Google Chrome kullanıcılara ait tarayıcı ayarlarını, yer işaretlerini, uzantılarını ve kayıtlı şifreleri saklar.

Windows 7, 8 ve 10 için: C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default

Mac için:

Users/<username>/Library/Application Support/Google/Chrome/Default

Linux için:

/home/<username>/.config/google-chrome/default

Google chrome ‘da birden fazla profil kullanılıyorsa chrome penceresinde chrome:// version yazılır. Bu ekranda kullanılan profile ait bilgilerin depolandığı dizin gösterilir.



Şekil 2 :Google Chrome Profil Yolu

Verilen dizin yoluna gidildiğinde kullanıcıya ait web data bilgileri, history bilgileri, log kayıtları, bookmarks verileri, favicons verileri, indirme bilgileri, oturum bilgileri verileri elde edilir.

İndirme ve Arama Geçmişi:

C:\Users\XXX\AppData\Local\Google\Chrome\User Data\Default\History

Cookies:

C:\Users\XXX\AppData\Local\Google\Chrome\User Data\Default\Cookies

Cache:

C:\Users\XXX\AppData\Local\Google\Chrome\User Data\Default\Cache

Bookmarks:

C:\Users\XXX\AppData\Local\Google\Chrome\User Data\Default\Bookmarks

Form History:

C:\Users\XXX\AppData\Local\Google\Chrome\User Data\Default\Web Data

Favicons:

C:\Users\XXX\AppData\Local\Google\Chrome\User Data\Default\Favicons

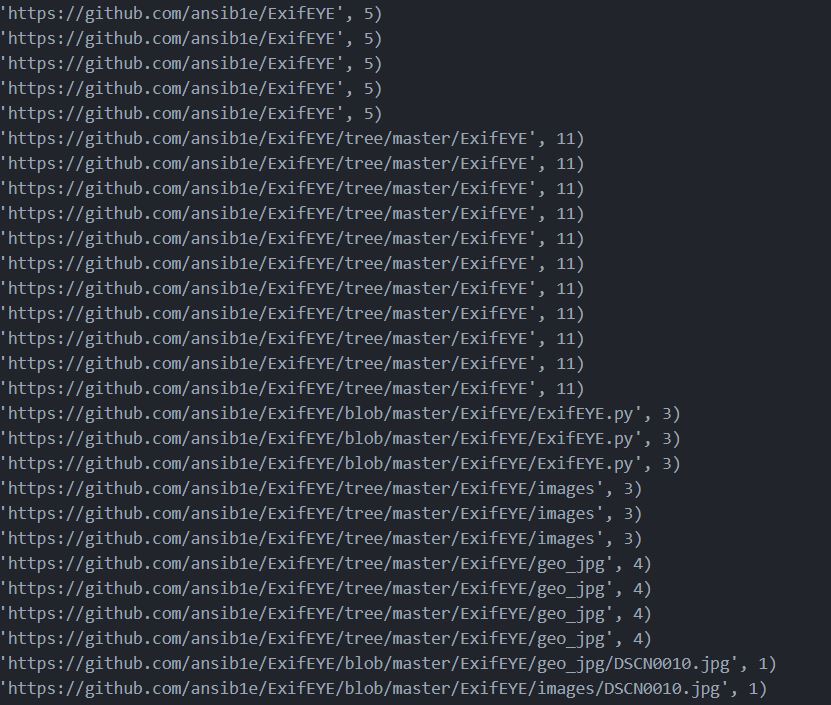
Logins:

C:\Users\XXX\AppData\Local\Google\Chrome\User Data\ChromeDefaultData\Login Data

Session Data:

C:\Users\XXX\AppData\Local\Google\Chrome\User Data\Default\Current Session

Yazılan kod sonucu elde edilen web tarayıcı geçmişi:



Şekil 3: Chrome Tarayıcı Geçmişi

**2- Internet Explorer:** Microsoft tarafından geliştirilmiş olup 1995 yılında kullanıcılara sunulmuştur.

Internet Explorer kullanıcılara ait navigasyon geçmişi bilgilerini, çeşitli formlarda aratılan kelimeleri, yer imlerini, eklentileri, önbellek dosyalarını, form verilerini, favicons verilerini, oturum verilerini, thumbnails dosyalarını, favorilere kaydedilen verileri tutar.

Cookies:

C:\Users\%username%\AppData\Local\Temp\Low\Cookies

Web Cache:

C:\Users\%username%\AppData\Local\Microsoft\Windows\WebCache

History:

C:\Users\%username%\AppData\Local\Microsoft\Windows\History

Recovery:

C:\Users\%username%\AppData\Local\Microsoft\Internet Explorer\Recovery

**3-Mozilla Firefox:**

Mozilla Vakfı tarafından 2002 senesinde kullanıcıların hizmetine sunulmuştur. Genel olarak kişisel verilerin gizliliği konusunda tercih edilir. Kişiselleştirilebilir özelliklere sahip olan tarayıcıdır.

Mozilla Firefox kullanıcılara ait araç çubukları, yüklenilen uzantıları, kayıtlı şifreleri, çerez bilgilerini, indirilenleri, verilen izinleri, yapılan aramaları, kaydedilen oturum açma bilgilerini, yer imleri bilgilerini kaydeder.

C:\Users\<your Windows login username>\AppData\Roaming\Mozilla\Firefox\Profiles\

Cache:

C:\Users\[User]\AppData\Local\Mozilla\Firefox\Profiles\xxxxxxxx.default\Cache

Navigation History:

C:\Users\XXX\AppData\Roaming\Mozilla\Firefox\Profiles\[profileID].default\places.sqlite

Bookmarks Backups:

C:\Users\XXX\AppData\Roaming\Mozilla\Firefox\Profiles\[profileID].default\bookmarkbackups\

Cookies:

C:\Users\XXX\AppData\Local\Mozilla\Firefox\Profiles\[profileID].default\cache2\entries

Form History:

C:\Users\XXX\AppData\Roaming\Mozilla\Firefox\Profiles\[profileID].default\formhistory.sqlite

Favicons:

C:\Users\XXX\AppData\Roaming\Mozilla\Firefox\Profiles\[profileID].default\favicons.sqlite

Downloads:

C:\Users\XXX\AppData\Roaming\Mozilla\Firefox\Profiles\[profileID].default\downloads.sqlite

Thumbnails:

C:\Users\XXX\AppData\Local\Mozilla\Firefox\Profiles\[profileID].default\thumbnails

**4-Opera:**

1995 yılında Opera Software firması tarafından geliştirilmiştir. Kişiselleştirilebilir özellikleri ve kullanıcılara vpn hizmeti sunar.

Opera kullanıcılara ait kurulum son güncelleme bilgilerini, yer imlerini, çerezleri, indirilenleri, geçmişleri, tercihleri, arama tercihlerini, arama geçmişlerini, hızlı arama ayarlarını, yazılan url’leri, son oturumları, önbellek klasör bilgilerini tutar.

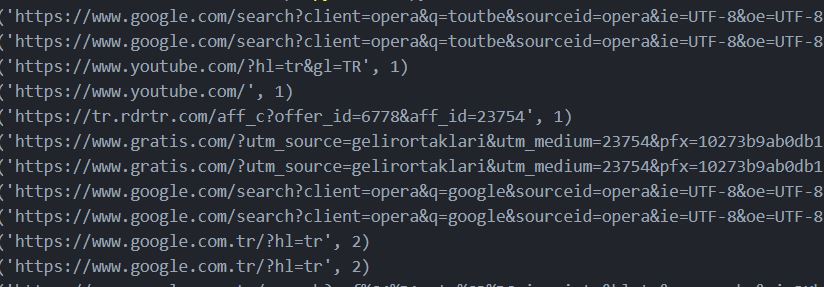
Windows İçin:

C:\Users\[user]\AppData\Local\Opera

C:\Users\BENGÜÇAĞLA\AppData\Roaming\Opera Software\Opera Stable

Mac OS:

~/Library/Application Support/Opera



Şekil 4: Opera Geçmiş Bilgileri

**5-Microsoft Edge:**

Microsoft tarafından Internet Explorer’ın yerini alarak yapılan web tarayıcısıdır.

Kullanıcılara ait html sayfaları, indirmeler, resimler gibi önbellek dosyalarını, yer imlerini, son göz atma oturumlarını, taramaların geçmişlerini, favori sitelerini, log dosyalarını saklı tutar.

Profile Path:

C:\Users\XX\AppData\Local\Packages\Microsoft.MicrosoftEdge\_XXX\AC

History:

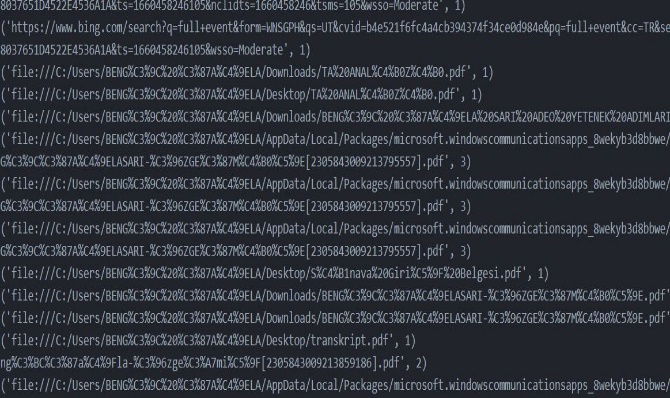
C:\Users\XX\AppData\Local\Microsoft\Edge\User Data\Default\History

Cache:

C:\Users\XXX\AppData\Local\Packages\Microsoft.MicrosoftEdge\_XXX\AC\#!XXX\MicrosoftEdge\Cache

Session:

C:\Users\XX\AppData\Local\Packages\Microsoft.MicrosoftEdge\_XXX\AC\MicrosoftEdge\User\Default\Recovery\Active



Şekil 5: Microsoft Edge Geçmiş Bilgileri

**KAYNAKÇA**

[1]ArtofTesting. “What is a web browser” <https://artoftesting.com/what-is-a-web-browser>

[2]ArtofTesting. “What is the URL” <https://artoftesting.com/what-is-url>

[3] Hosting. “HTTP nedir?” <https://www.hosting.com.tr/bilgi-bankasi/http-nedir/>

[4] Bencherchali Nasreddine. “Web Browser Forensics” <https://nasbench.medium.com/web-browsers-forensics-7e99940c579a>

[5] Rathod Dr. Digvijaysinh . Web Browser Forensıcs: Google Chrome, Volume:8, No:7, July 2017

[6]Infosec, “Browser Forensics:IE 11”, <https://resources.infosecinstitute.com/topic/browser-forensics-ie-11/>

[7] How-To-Geek. “How to Find Your Chrome Profile Folder on Windows, Mac and Linux”. <https://www.howtogeek.com/255653/how-to-find-your-chrome-profile-folder-on-windows-mac-and-linux/>