International Journal of Human Sciences
ISSN:1303-5134

Volume: 12 Issue: 2 Year: 2015

Web browsers forensic analysis review

Web tarayıcılarda adli analiz incelemesi

Erkan Baran[1]
Hüseyin Çakır[2]
Çelebi Uluyol[3]

Abstract

Nowadays, web browser tools are seen ıntensıvely durıng the usage of web applıcatıons. Because of that, browsers provıdes ınfrastructure of a largo majorıty of crımes. Because guılty or suspect can use the browsers to collect ınformatıons, to hıde hıs crıme, learn new crımınal methods or to apply they have learned. In thıs study, ıt ıs also seeked answers of how a process can be monıtored on the computers whıch are used on browsers, ın whıch fıles whıch datas are looked and when and whıch sıtes are accessed. Accordıng to research of W3counter web stats tool, Chrome Web browser, whıch has %43 persentage of across the world ın usage, ıs proses as the most demanded browser ın thıs study by users, and ıt ıs scented out ın thıs browser's related fıles. In these days, "hıdden mode" whıch take part ın vast majorıty of browsers ıs also examıned. Thıs feature of the browser, whıch ıs receıved reference, ıs tracked by testıng and ıs sought data ın RAM memory and fıle systems. Thus, " hıdden mode" effects are dıscussed ın provıdıng studıes about suspect or crımınal posıtıon people, what kınd of data can be obtaıned ın usıng " hıdden mode" ıs revealed.

Özet

Günümüzde internet uygulamalarının kullanımı sırasında web tarayıcı araçlarının yoğun bir şekilde kullanımı görülmektedir. Bu nedenle tarayıcılar, işlenen suçların büyük bir çoğunluğuna altyapı sağlar. Çünkü suçlu ya da şüpheli, tarayıcıları bilgi toplamak, suçunu gizlemek, yeni suç metotları öğrenmek ya da öğrendiklerini uygulamak için kullanabilir. Bu çalışmada da tarayıcıların kullanıldığı bilgisayarlar üzerinde bırakılan izlerin tespitinde nasıl bir süreç izlenebileceği, hangi dosyalarda hangi verilere bakılabileceği ve ne zaman hangi sitelere erişim sağlandığı gibi çeşitli sorulara cevaplar aranmaktadır. w3counter adlı internet istatistik aracının yaptığı araştırmaya göre, dünya genelinde %43'lük bir kullanım alanına sahip olan Chrome web tarayıcısı, kullanıcılar tarafından en çok talep gören tarayıcı olarak bu araştırma içinde referans alınmaktadır ve bu tarayıcıya ait ilgili dosyalarda izler sürülmektedir. Ayrıca günümüz tarayıcıların büyük bir çoğunluğunda yer alan "**gizli mod**" özelliği incelenmektedir. Referans alınan tarayıcının bu özelliği test edilerek iz sürülmekte, dosya sistemlerinde ve RAM bellekte veri aranmaktadır.Böylelikle "gizli mod" kullanımında ne tür veriler elde edilebileceği ortaya konarak şüpheli ya da suçlu konumundaki

[1] Bilgi Teknolojileri ve İletişim Kurumu, baranerk@gmail.com
[2] Yrd. Doç. Dr., Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim ABD, hcakir@gazi.edu.tr
[3] Öğr. Gör. Dr., Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim ABD, celebi@gazi.edu.tr

Baran, E., Çakır, H., & Uluyol, Ç. (2015). Web tarayıcılarda adli analiz incelemesi. *International Journal of Human Sciences*, *12*(2), 757-774. doi:10.14687/ijhs.v12i2.3244

Keywords: Forensic analysis, browser, cyber crimes, data.

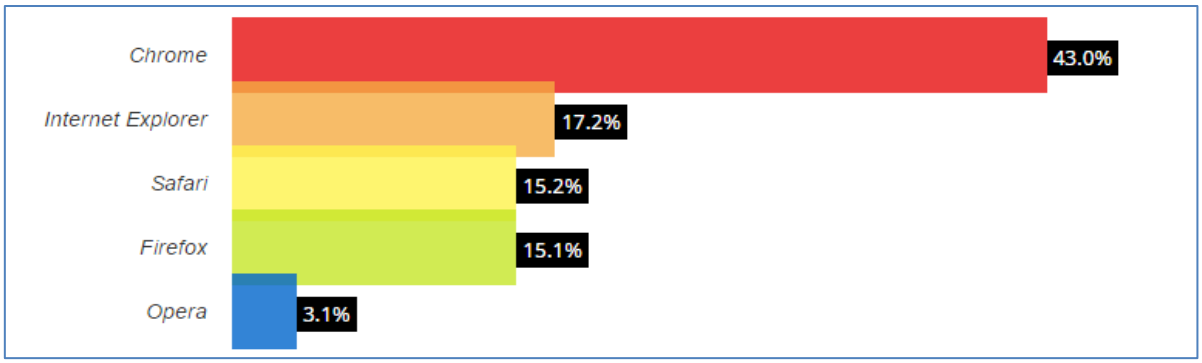
(Extended English abstract is at the end of this document)

kişilere ait delillendirme çalışmalarında "gizli mod" kullanımının etkileri tartışılmaktadır.

Anahtar Kelimeler: Adli analiz, tarayıcı, bilişim suçları, veri.

Giriş

Son yıllarda internet tabanlı teknoloji ve hizmetlerin hızlı gelişimi ve bu gelişmelerle beraber insanlığa hizmet veren birçok uygulamanın internet ortamına taşınmış olması internet tabanlı teknolojileri vazgeçilemez duruma getirmiştir. Ülkelerin bilişim teknolojilerine ve özellikle internete olan bağımlılığı her geçen gün artmakta, bankacılık hizmetlerinden enerji sektörüne, eğitim alanından sanayi altyapısına, sağlık hizmetlerinden askeri alandaki birçok projeye kadar bütün altyapı hizmetlerinde bu artış devam etmektedir. Bilişim teknolojilerine olan bağımlılığın gün geçtikçe bu denli artması suçlular için yeni bir ortam oluşturmuştur. Sanal ortam ya da internet ortamı diye adlandıracağımız bu ortamda işlenen suçların büyük bir çoğunluğunda şüpheli ya da suçlu konumundaki kişi web tarayıcı araçlarını kullanmaktadır. Web tarayıcı araçları, kullanıcıların web sayfaları ve web içerikleri ile etkileşimine izin veren yazılımdır. Bu yazılımın kullanımı sırasında ise bilgisayarlar üzerinde ciddi izler bırakılmakta ve bu izler kullanılan tarayıcı ve işletim sistemine göre farklılık arz etmektedir. Her bir işletim sistemi ve farklı olan her bir tarayıcı için bu izlerin yeri ve analizi farklıdır. Bu nedenle yapılan bu çalışmada tek bir tarayıcı üzerinde inceleme yapılmaktadır.

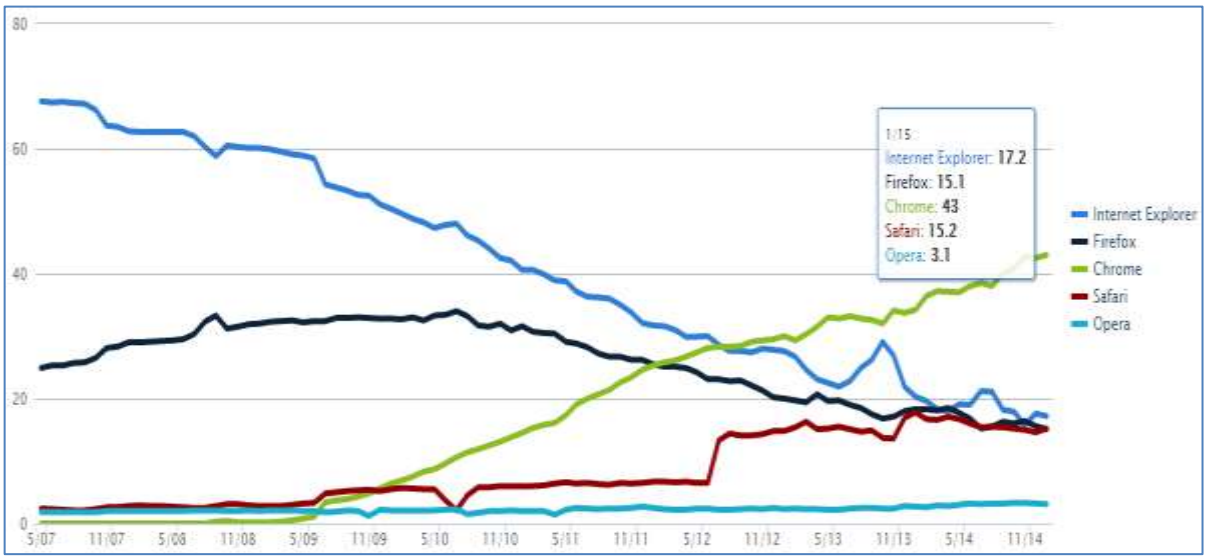


Şekil 1.1: Dünya Genelinde Tarayıcıların Kullanım Yüzdesi, Ocak-2015[4].

Dünya genelinde tarayıcıların kullanım yüzdeleri de dikkate alındığında Chrome, firefox ve internet explorer´ın üstünlüğü görülmektedir(Şekil 1.1). Bu çalışmada ise diğer tarayıcılar arasında % 43 'lük kullanım yüzdesinden dolayı Chrome web tarayıcısına ait izler değerlendirilmektedir.

[4] http://www.w3counter.com/globalstats.php?year=2015&month=1 Global Market Share

Baran, E., Çakır, H., & Uluyol, Ç. (2015). Web tarayıcılarda adli analiz incelemesi. *International Journal of Human Sciences*, *12*(2), 757-774. doi:10.14687/ijhs.v12i2.3244



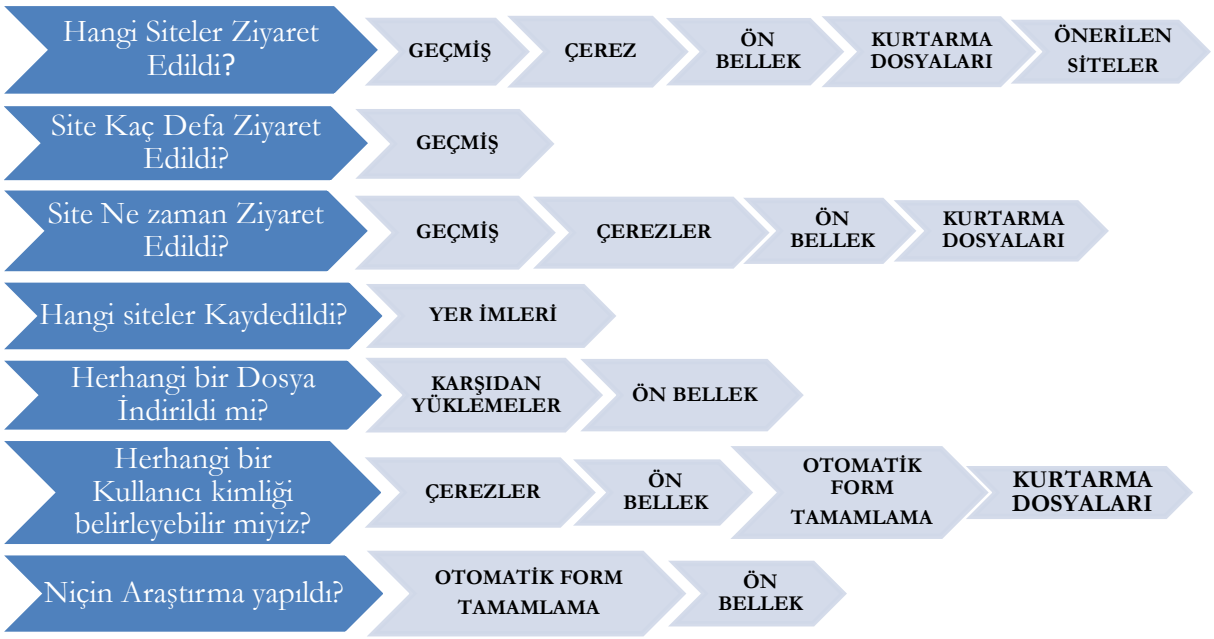
Şekil 1.2: Son Yedi Yılda Tarayıcıların Kullanım Grafiği, Ocak-2015[5].

Tarayıcıların son 7 yıldaki talep grafiği de dikkate alındığında ivme olarak en hızlı yükselişin **Chrome web** tarayıcısına ait olduğu görülmektedir (Şekil 1.2). Bu nedenle Chrome web tarayıcısına son yıllardaki yoğun talep bu çalışmada referans alınmasındaki en büyük etkendir. Bu tarayıcıya ait ön bellek (cache), internet geçmişi (history), çerezler (cookies) takip edilmekte ve ilgili diğer dosyalara bakılmaktadır. Ayrıca Chrome'un "***İncognito mode (gizli mod)***" özelliği incelenmektedir.

Chrome web tarayıcısının hızlı gelişimi dikkate alındığında bilişim suçları kapsamındaki yeri de göz ardı edilmemelidir. Bu nedenle bilişim suçlarının büyük bir çoğunluğunda tarayıcıların giriş kapısı olduğunu düşünürsek adli analiz çalışmalarında şekil 1.3 'te yer alan sorular delillendirme süreçlerine büyük kolaylık sağlayacaktır.

[5] http://www.w3counter.com/trends Global Market Share

Baran, E., Çakır, H., & Uluyol, Ç. (2015). Web tarayıcılarda adli analiz incelemesi. *International Journal of Human Sciences*, *12*(2), 757-774. doi:10.14687/ijhs.v12i2.3244



Şekil 1.3: Adli Analizde Sorulması Gerekenler (The SANS Instute, 2013).

Şekil 1.3'te yer alan sorular ışığında web tarayıcı araçlarının adli analizinde yöntemlerin neler olabileceğini saptamak, web tarayıcı araçları konusuna adli delillendirme süreçlerinde farkındalık oluşturmak, hangi dosyalarda ne tür verilerin olduğunu vurgulamak bu çalışmanın temel amacıdır. Bu konuda yapılan çalışmaların aksine "gizli mod" özelliğinin de incelenmesi bu çalışmayı farklı kılmaktadır. Böylelikle suçlulara bakir bir alan olarak sunulan internet dünyasında tarayıcıların yoğun bir şekilde kullanılması nedeniyle sanal dünyada bırakılan izlerin takibinde neler yapılabileceği ortaya konmaktadır.

2-CHROME WEB TARAYICISININ ADLİ OLARAK İNCELENMESİ

Microsoft Windows için geliştirilen beta sürümü 2 Eylül 2008 tarihinde, 43 farklı dilde kullanıma sunulmuştur. Daha sonra Mac OS X ve Linux sürümleri de geliştirilmiştir (wikipedia.org, 2014). 2015 Ocak ayı itibarıyla w3counter adlı internet istatistik aracının yaptığı araştırmaya göre, dünya genelinde %43'lük bir kullanım alanına sahip olan Chrome, aynı zamanda dünyanın en çok tercih edilen ve kullanılan internet tarayıcısıdır (w3counter.com, 2015). Bu nedenle Chrome tarayıcısına ait verilere yoğun bir şekilde rastlamak mümkündür.

Chrome tarayıcısının ***varsayılan*** olarak ayarlanması halinde işletim sistemlerinde bırakılan veriler aşağıdaki dizinde yer alır (Kocaman, 2014).

Baran, E., Çakır, H., & Uluyol, Ç. (2015). Web tarayıcılarda adli analiz incelemesi. *International Journal of Human Sciences*, *12*(2), 757-774. doi:10.14687/ijhs.v12i2.3244

Win7/8: %root%\Users\userprofile\AppData\Local\Google\Chrome\UserData\Default\

WinXP: %root%\DocumentsandSettings\userprofile\LocalSettings\ApplicationData\Google \Chrome\UserData\Default\

Linux: \home\userprofile\.config\google-chrome\Default\ApplicationCache

MacOS-x: \Users\userprofile\Caches\Google\Chrome\Default\Cache

Chrom'un tuttuğu bütün veri dosyalarının tek bir yerde toplanmış olması adli analiz bakımından kolaylık sağlamaktadır. Verilerin büyük bir çoğunluğu SQLite[6] veri tabanında olduğu için toplanan verilere bakmak kolaydır (The SANS Instute, 2013).

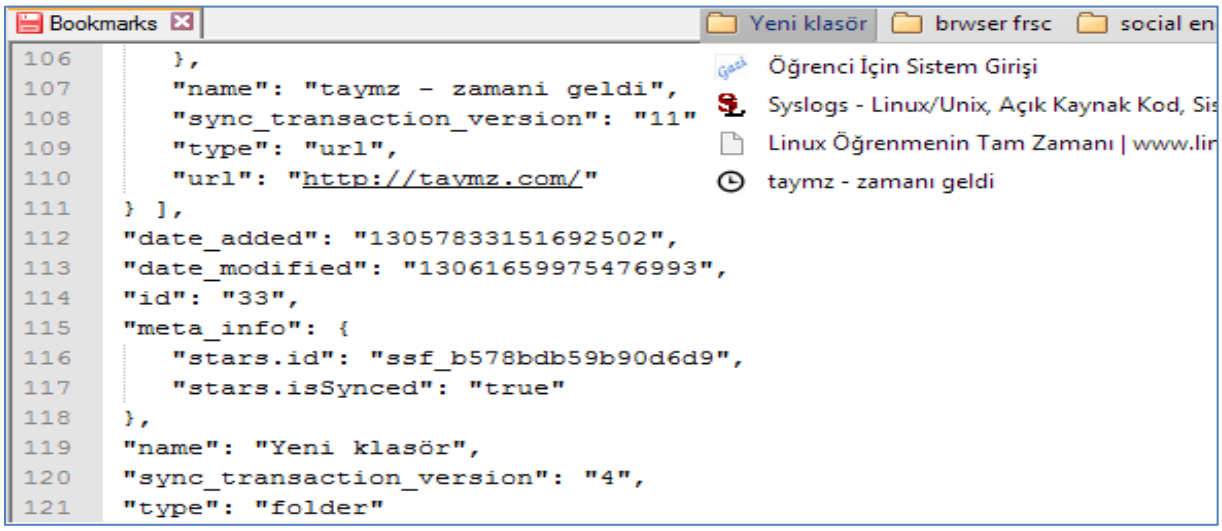
Chrome tarayıcısına ait dosyalar/veriler adli süreçlerde büyük önem arz etmektedir. Yer imlerinde suçlu ya da şüphelinin hangi siteleri bilgisayarına kaydettiğine bakılarak ilgi ve alaka gösterdiği alanların tespiti mümkündür. İnternet geçmişi dosyasına bakılarak bu sitelerin erişim tarihlerine bakılabilir. Yine ön belekte tutulan içeriklere göre delillendirme sürecine kolaylık sağlanabilir. Çerezler ve indirilenler geçmişi dosyalarına bakılarak hangi siteler üzerinden içerik elde edildiğine bakılabilir. Ayrıca otomatik form tamamlama/form geçmişi girdilerine bakılarak hangi kelimelerin kullanıldığı tespit edilebilir. Bu nedenle aşağıda yer alan dosyalar delillendirme süreçleri açısından önemlidir.

2.1. Yer İmleri

"Hangi siteler kaydedildi?" sorusuna cevap ararken bakılması gereken ilk dosyadır. Siteye ait URL, başlık bilgileri, sitenin eklenme/değiştirilme tarihi ve sitenin bulunduğu menü başlığı ya da klasör gibi yer bilgileri bookmarks dosyası içinde depolanır (Şekil 2.1). Fakat burada yer alan zaman damgası formatları farklı yapıda olduğu için anlaşılır değildir. Çeşitli kodlarla dönüştürülebilir.

[6] **SQLite**, dünyada en çok dağıtılan ve tavsiye edilen kaynak kodları halka açık, tamamen C/C++ programlama dilleriyle geliştirilmiş sunucu yazılımı ve yapılandırma gereksinimi olmayan, işlemsel ve ilişkisel bir SQL veri tabanı motorudur.

Baran, E., Çakır, H., & Uluyol, Ç. (2015). Web tarayıcılarda adli analiz incelemesi. *International Journal of Human Sciences*, *12*(2), 757-774. doi:10.14687/ijhs.v12i2.3244



Şekil 2.1 : Chrome Bookmarks Dosyası

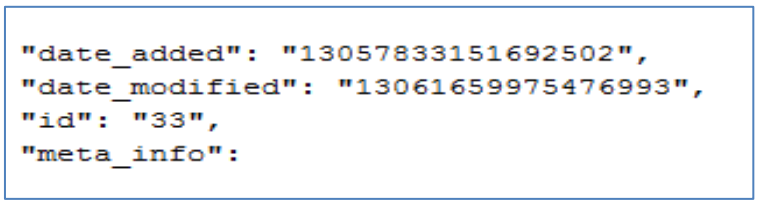
Bookmarks dosyası,

C:Users\userprofile\AppData\Local\Google\Chrome\UserData\Default\History

altında tutulmaktadır.

2.2. İnternet Geçmişi (History)

"Hangi siteler ziyaret edildi?", "Ne zaman ziyaret edildi?" ya da "Kaç defa ziyaret edildi?" şeklindeki soruların cevabını bu dosya içinde aramak mümkündür. .Sqlite veri tabanı formatında tutulan dosya içerisinde URL, başlık bilgileri, kaç defa ziyaret edildiği, en son ne zaman ziyaret edildiğine dair veriler tablo olarak tutulmaktadır. Tablolardaki Chrome zaman damgası formatı farklı bir yapıda olduğu için anlaşılır değildir.



Şekil 2.2: Chrome Zaman Formatı

Şekil 2.2 de yer alan 17 haneli belirsiz zaman damgası formatı çeşitli kodlarla anlaşılır hale getirilebilir.

Python[7] kodu ile aşağıdaki gibi bir dönüşüm yapılabilir (forensicswiki.org, 2014);

```
date_string = datetime. datetime( 1601, 1, 1 )
            + datetime.timedelta( microseconds=timestamp )
```

[7] **Python**, nesne yönelimli, yorumlamalı, birimsel (modüler) ve etkileşimli yüksek seviyeli bir programlama dilidir.

Baran, E., Çakır, H., & Uluyol, Ç. (2015). Web tarayıcılarda adli analiz incelemesi. *International Journal of Human Sciences*, *12*(2), 757-774. doi:10.14687/ijhs.v12i2.3244

Kod kullanmak yerine Craig Wilson tarafından geliştirilen "DCode" aracı ile de zaman damgaları için format dönüşümü yapılabilir (The SANS Instute,2013).

Dosya içerisinde ziyaret edilen siteler aşağıdaki gibi sorgulanabilir (forensicswiki.org, 2014);

```
SELECT datetime (((visits.visit_time/1000000)-11644473600),
"unixepoch"), urls.url, urls.title FROM urls, visits WHERE
urls.id = visits.url;
```

İnternet geçmişi dosyası,

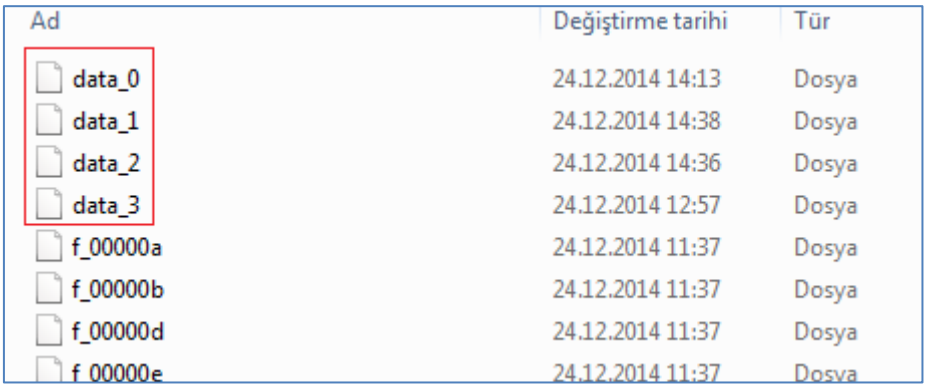
C: Users\userprofile\AppData\Local\Google\Chrome\UserData\Default\History

altında yer almaktadır.

2.3. Ön Bellek (Cache)

İnternet üzerindeki gezinti sırasında tarayıcı tarafından ziyaret edilen internet sitelerindeki resim, görüntü, ses ve diğer indirilebilir içeriklerin yer aldığı geçici kayıtlar oluşturulur. Bilgisayarda tutulan bu kayıtlara tarayıcı önbelleği adı verilir. Önbellekleme sistemi, aynı internet sitesi tekrar ziyaret edildiğinde belirli içeriklerin daha hızlı görüntülenmesi için geliştirilmiştir (eticaretsozlugu.com, 2014).

C:\root\Users\userprofile\AppData\Local\Google\Chrome\UserData\Default\Cache altında ön bellek dosyası görüntülenebilir ya da adres çubuğuna ***chrome://view-http-cache/*** yazılarak dosya içindeki veriler listelenebilir. Ön bellek veri tabanı en az beş dosyadan oluşur. Dosyalardan biri "**index**" ve diğer dördü "**data_#**" dosyasıdır.

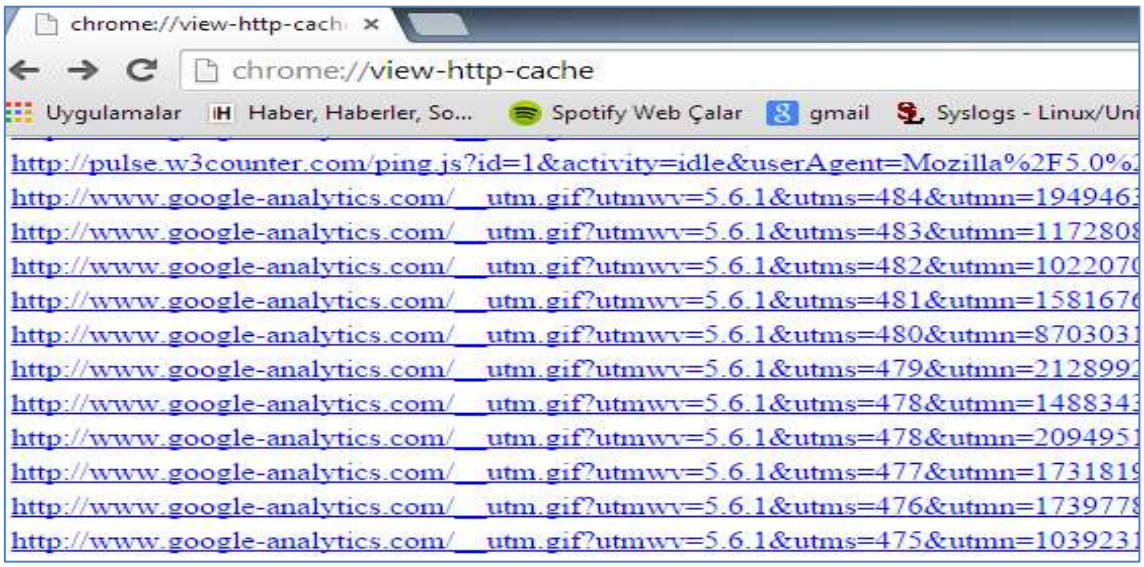


Şekil 2.3: Ön Bellek Data Dosyaları

Şekil2.4: Ön Bellek index Dosyası

Baran, E., Çakır, H., & Uluyol, Ç. (2015). Web tarayıcılarda adli analiz incelemesi. *International Journal of Human Sciences*, *12*(2), 757-774. doi:10.14687/ijhs.v12i2.3244

Ön bellek veri tabanına ait dosyalar şekil 2.3 ve şekil 2.4 'te görülmektedir. Bu dosyalara bakılarak geçici kayıtlara ait bilgilere ulaşılabilir.



Şekil 2.5 : *chrome://view-http-cache/* ile Ön Belleği Listeleme

Ziyaret edilen internet sitelerine ait bazı geçici kayıtlar şekil 2.5 'te görülmektedir. Adres çubuğuna *chrome://view-http-cache/* yazıldıktan sonra gelen içeriklerin üzerine tıklanarak şekil 2.6 'daki gibi içerik özellikleri de görülebilir.

Şekil 2.6 : *chrome://view-http-cache/* ile Ön Bellek Analizi

Baran, E., Çakır, H., & Uluyol, Ç. (2015). Web tarayıcılarda adli analiz incelemesi. *International Journal of Human Sciences*, *12*(2), 757-774. doi:10.14687/ijhs.v12i2.3244

Şekil 2.6 'da oluşturulan geçici içeriklerden birine ait içerik tipi, hangi sunucudan geldiği, içerik boyutu, url bilgisi, erişim tarihi gibi özellikler görülmektedir.

2.4. Çerezler (Cookies)

Web sunucusundan bilgisayara otomatik olarak yüklenen küçük dosyalardır. Çerezlerin içindeki bilgiler aynı bilgisayar o siteye her girişinde saklı durur. Çerezler, ziyaretçilerin kimliklerini belirleyerek web sitelerinin kişiselleştirilmesini sağlar. İnternet siteleri tarafından bilgisayara bırakılan bir tür tanımlama dosyasıdır (wikipedia.org , 2014).

C:\Users\userprofile\AppData\Local\Google\Chrome\UserData\Default\Cookies altında yer alan çerez dosyası içerisinde çerez içeriğinin adı, hangi sunucudan gönderildiği, ne zaman oluşturulduğu, ne zaman sonlandırıldığı ve son erişim tarihi gibi zaman damgaları görüntülenebilir. .Sqlite formatında tutulan veri tabanı dosyasında her bir sütun sorgulanabilir.

HostName	CookiePath	CookieName	CookieValue	IsSecure	IsHttpOnly
.slideshare.net	/	test		false	false
.slideshare.net	/	_uv_id		false	false
www.slideshare.net	/	tos_update_bann...		false	false
.scorecardresear...	/	UID		false	false
.scorecardresear...	/	UIDR		false	false

Şekil 2.7 :Çerez Dosyasındaki Veriler

CreationDate	LastAccessedDate	ExpirationDate	uid	created	itemList_Id
2014-11-05T08:1...	2014-11-10T08:4...	2015-10-31T08:1...	80397AF4-8198-...	2014-12-24T09:3...	0
2014-11-05T08:1...	2014-11-10T08:4...	2016-11-04T08:1...	D30A2B48-ACEF...	2014-12-24T09:3...	0
2014-11-05T08:1...	2014-11-10T08:4...	2015-11-05T08:1...	133F7487-260F-...	2014-12-24T09:3...	0
2014-11-05T08:1...	2014-12-24T09:3...	2016-10-25T08:1...	D85BB405-3B20-...	2014-12-24T09:3...	0
2014-11-05T08:1...	2014-12-24T09:3...	2016-10-25T08:1...	7CBE5C29-60D5...	2014-12-24T09:3...	0
2014-11-05T08:1...	2014-11-10T08:4...	2016-11-04T08:1...	944BBAA2-9E6B...	2014-12-24T09:3...	0

Şekil 2.8 :Çerez Dosyasındaki Veriler

Dosya içerisinde çerez içeriğinin adı, hangi hosttan gönderildiği, ne zaman oluşturulduğu, ne zaman sonlandırıldığı ve son erişim tarihi gibi zaman damgaları görüntülenmektedir (Şekil 2.7 ve Şekil 2.8).

Baran, E., Çakır, H., & Uluyol, Ç. (2015). Web tarayıcılarda adli analiz incelemesi. *International Journal of Human Sciences*, *12*(2), 757-774. doi:10.14687/ijhs.v12i2.3244

2.5. İndirilenler Geçmişi

İndirme geçmişi temizlenmedikçe dosyaların yeri ve hangi URL üzerinden indirildiği bulunabilir. Veriler yine. Sqlite formatında tutulmaktadır. Veri tabanı içerisinde ayrıca indirilen dosyanın büyüklüğü, indirme işleminin başlatılma ve bitiş tarihleri bulunur.

2.6. Otomatik Form Tamamlama/Form Geçmişi

İnternet üzerinde bir sayfada herhangi bir işlem sırasında bilgilerin girdisi ilk defa yapılıyorsa Chrome tarafından bu bilgiler kaydedilir. Böylelikle İsim, adres, telefon numarası ya da bir e-posta adresi **autofill**[8] girdisi olabilir. Ayrıca Chrome tarafından çeşitli bloglarda, sitelerde, forumlarda yaptığımız araştırmalar sırasında kullanılan kelimeler de metin formatında kaydedilir ve bu alanlara tekrar geldiğimizde kullanmış olduğumuz kelimeler bize tekrar sunulur (support.google.com, 2014). Bu nedenle herhangi bir suç kapsamında ele geçirilen bir bilgisayar ya da alınan bir imaj üzerinde bu verilerin araştırılması önem arz etmektedir.

C:\Users\userprofile\AppData\Local\Google\Chrome\UserData\Default\WepData

Altında yer alan .sqlite uzantılı dosya içerisinde aşağıdaki gibi veri tabanı sorgusu yapılarak autofill girdilerine bakılabilir (superuser.com, 2014).

```
select *
from autofill
where name in (
  select name
  from autofill
  where value_lower like 'one-data-entry-of-you'
);
```

[8] İlk defa ziyaret edilen bir URL'de form olarak girilen verilerin kaydedilmesi.

Baran, E., Çakır, H., & Uluyol, Ç. (2015). Web tarayıcılarda adli analiz incelemesi. *International Journal of Human Sciences*, *12*(2), 757-774. doi:10.14687/ijhs.v12i2.3244

3.CHROME 'UN INCOGNITO MODE ÖZELLİĞİNİN İNCELENMESİ

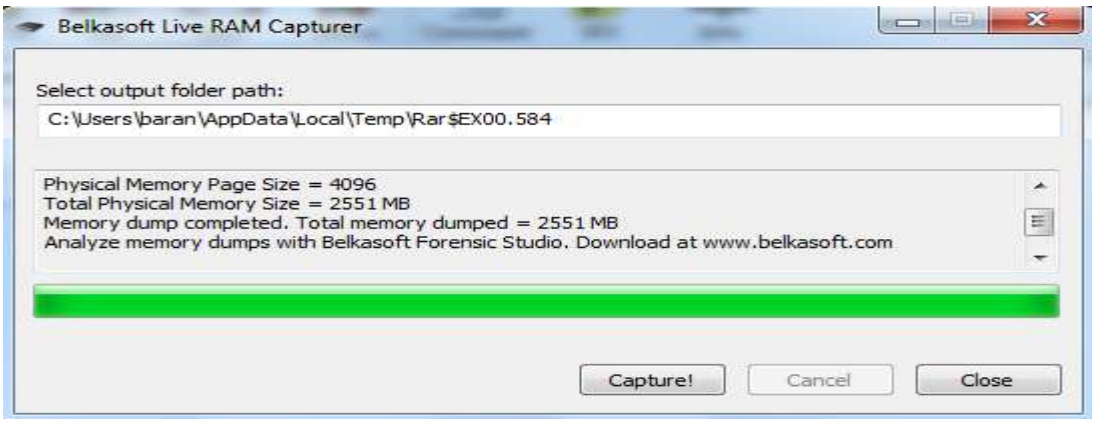
Birçok internet tarayıcısında **gizli tarama** veya **incognito** modu bulunmaktadır. Bu modlar kullanılarak tarayıcı geçmişi, çerezler, ön bellek, form geçmişi gibi dosyaların bilgisayara kaydedilmesi önlenir. Ancak aktivitelerin başka bir lokasyonda kaydedilip kaydedilmemesine müdahale edilemez (uzmanabi.com, 2014).

Chrome'un gizli modda kullanılması durumunda ziyaret edilen sitelere önceden mevcut çerezler aktarılmaz. Siteler, bu moddayken sisteme yeni çerezler bırakabilir; bu çerezler yalnızca geçici olarak saklanır ve gizli modda kalındığı sürece sitelere iletilir. Tarayıcıyı ve açık durumdaki tüm gizli pencereler kapatıldığında bu çerezler silinir (google.com/Privacy, 2014). Bu çalışmada da çerezler silindikten sonra ya da ilgili pencere kapatıldıktan sonra silinen dosyalara erişmek ya da bırakılan başka izlere ulaşmak mümkün mü sorularına cevap aranmaktadır.

Bu süreçte yapılan analiz çalışmalarına bakıldığında her bir tarayıcının farklı semptomlar sergilediği görülmektedir. Dosya sistemlerinde ve RAM bellekte yapılan dosya kurtarma çalışmalarında işletim sistemlerine ve kullanılan tarayıcılara göre farklı sonuçlar ortaya çıkmaktadır (Norulla, 2014).

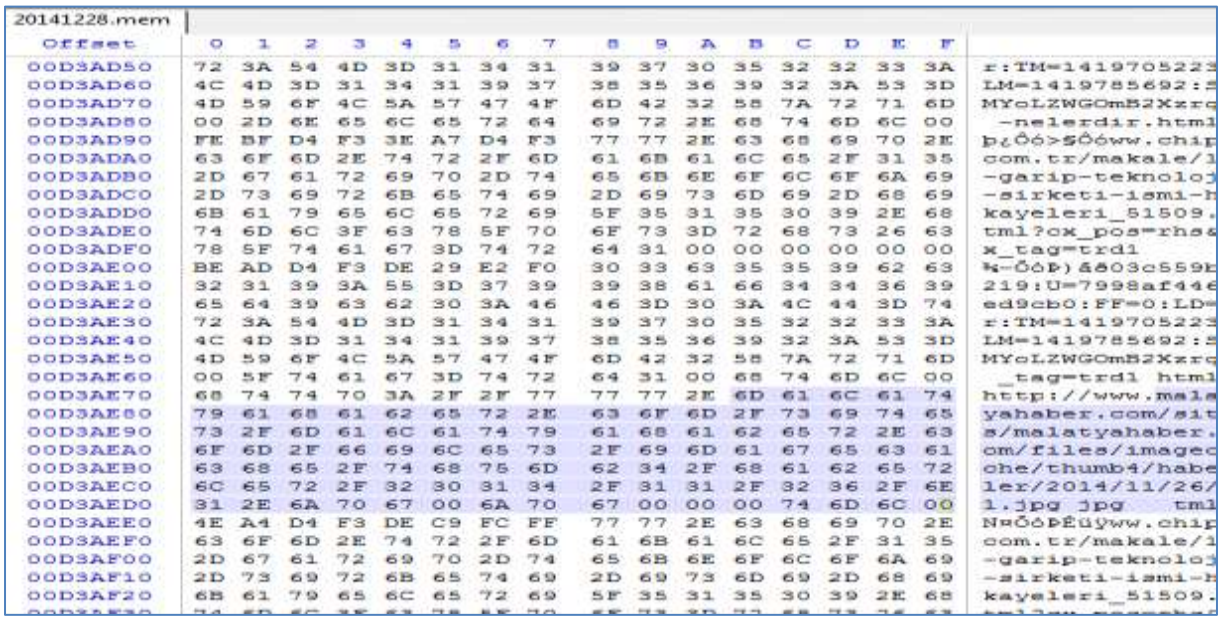
Gizli mod özelliğinin bırakılan izler noktasında takibi için yapılan incelemede Chrome web tarayıcısı gizli modda açılarak internete erişim sağlandıktan sonra tüm pencereler kapatılmış ve Win7/8 üzerinde ***Recuva*** aracı ile yapılan file system analizinde chrome web tarayıcısının internet geçmişi ile alakalı herhangi bir dosya tutmadığı görülmüştür.

Fakat RAM bellek üzerinde yapılan aynı çalışma sonrası kullanılan ***Belkasoft RAM Capturer*** aracı ile ram içerikleri yakalanmış ve ***winhex*** ile analiz edilmiştir. Taranan sitelerin RAM de tutulduğu görülmüştür.



Şekil 3.1 : Belkasoft Live RAM Capturer ile RAM içeriklerinin Yakalanması

Baran, E., Çakır, H., & Uluyol, Ç. (2015). Web tarayıcılarda adli analiz incelemesi. *International Journal of Human Sciences*, *12*(2), 757-774. doi:10.14687/ijhs.v12i2.3244



Şekil 3.2 : Elde Edilen RAM içeriklerinin **Winhex** ile Analizi

Yukarıdaki analize bakıldığında incognito modda siteler kapatıldıktan sonra RAM de verilerin durduğu görülmektedir(Şekil 3.2). Yapılan analiz sonucunda Chrome 'un gizli mod özelliğinin canlı bellek üzerinde başarısız olduğunu ve adli analiz noktasında veri elde edilebileceğini göstermiştir. Ancak RAM belleğin elektrik kesintisi ya da makinenin kapatılması durumunda sıfırlanacağı unutulmamalıdır.

Tarayıcı Verileri	**Verilere Ait Chrome Dosya Adı**	**Dosya Formatı**
İnternet Geçmişi	-History -Archived History -Top Sites	SQLite
Ön Bellek Dosyaları	-Data_# , f_###	N/A
Çerezler	-Cookies	SQLite
Yer İmleri	-Bookmarks -Bookmarks.bak	JSON
İndirme Geçmişi	-History	SQLite
Otomatik Tamamlama/ Form Geçmişi	-History -Web Data -Network Action Predictor	SQLite
Kurulan Eklentiler	-Preferences	JSON

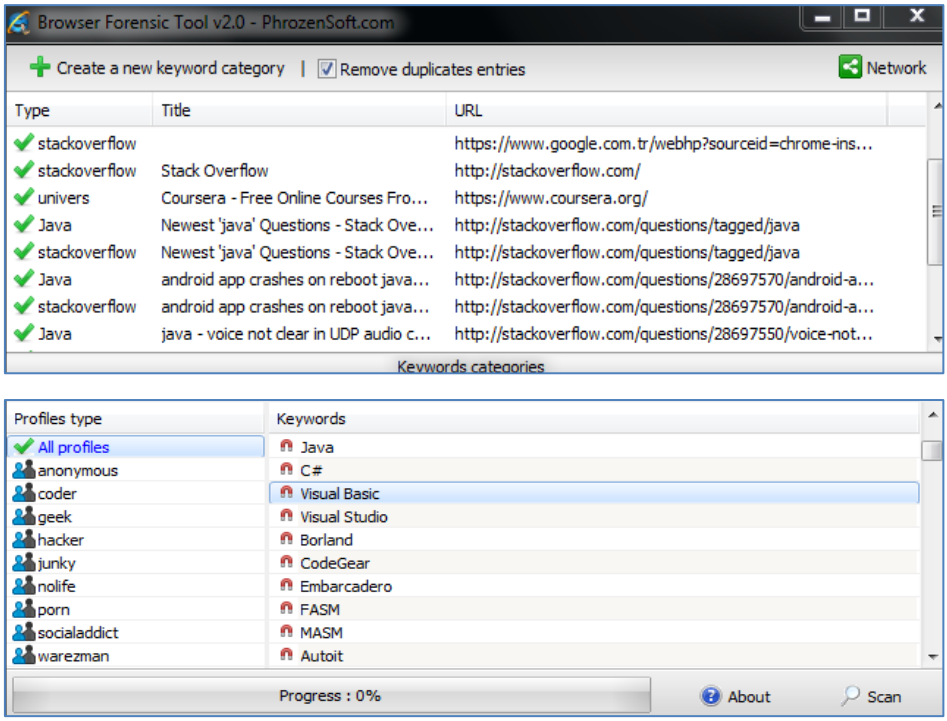
Şekil 3.3: Chrome Veri Türleri ve Dosya Formatları

Baran, E., Çakır, H., & Uluyol, Ç. (2015). Web tarayıcılarda adli analiz incelemesi. *International Journal of Human Sciences*, *12*(2), 757-774. doi:10.14687/ijhs.v12i2.3244

4. Adli Analizde Kullanılabilecek Araçlar

Tarayıcıların tuttuğu verilerin değerlendirilmesinde klasik yöntemlerin yerine çeşitli araçlar kullanmak adli süreci hızlandıracağından daha faydalı olacaktır. Bu araçlardan en çok kullanılanlar:

Browser Forensic Tool: History arama motorudur. Google Chrome, Comodo Dragon, Internet Explorer, Opera Browser, RockMelt gibi tarayıcılara ait history geçmişinde aratılan bir kelimeyi hızlı bir şekilde çekmektedir. Aratılan kelime URL ile birlikte gösterilir. Ayrıca uygulama üzerinde varsayılan olarak gelen çeşitli kategorilerde kelime listesi mevcuttur ve isteğe göre yeni kelimeler eklenebilir (phrozensoft.com, 2014).



Şekil 4.1: Browser Forensic Tool

Mandiant Web historian (Mandiant Redline): Web geçmişini ayrıntılı raporlar ile sunarak analiz etmeyi sağlayan uygulamanın Eylül 2014 itibariyle Mandiant Redline ile konsolide olduğu görülmektedir (mandiant.com, 2014).

İnternet Explorer, Firefox, Google Chrome ve Safari dahil olmak üzere tüm popüler internet tarayıcılarına uyum sağlamaktadır. Uygulama, kullanıcı dostu ara yüzü ile birleştiğinde web geçmişini, çerezleri ve desteklenen tarayıcıların indirme tarihini ayrıntılı tarama yoluyla izlemeye olanak sağlar (Alemdar, 2012).

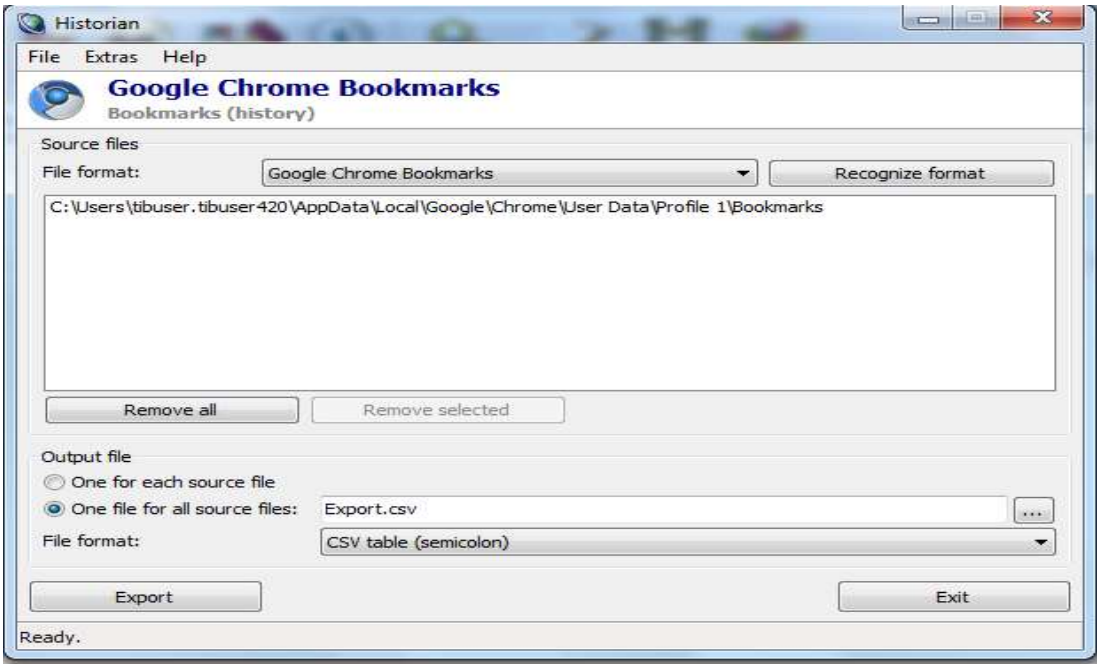
Baran, E., Çakır, H., & Uluyol, Ç. (2015). Web tarayıcılarda adli analiz incelemesi. *International Journal of Human Sciences*, *12*(2), 757-774. doi:10.14687/ijhs.v12i2.3244

Şekil 4.2: Mandiant Redline Analiz Aracı

Pasco and galleta: Açık kaynak kodlu uygulamalardır. Pasco, İnternet Explorer index.dat dosyasını, galleta ise internet explorer çerez verilerini ayrıştırmak için kullanılır (Samuel, 2007). Uygulama sadece bu amaçlar için kullanıldığında verimli sonuçlar alınabilir fakat diğer veri dosyalarına ait analizler için aynı durum söz konusu değildir. Linux işletim sistemleri ile uyumludur (Sonntag, 2012).

Historian: Windows işletim sistemlerinde çalışan uygulama Chrome, firefox, opera ve internet explorer ile uyumludur. Geçmiş, yer imleri, çerezler, ön bellek, form alanları ve çeşitli tarayıcı dosyalarına ait veriler CSV ya da metin formatında export edilebilir (gaijin.at, 2014).
Dosyaların export edilmesi sırasında uyguma tarafından ayrıca bir hash değeri oluşturulur (Sonntag, 2012).

Baran, E., Çakır, H., & Uluyol, Ç. (2015). Web tarayıcılarda adli analiz incelemesi. *International Journal of Human Sciences*, *12*(2), 757-774. doi:10.14687/ijhs.v12i2.3244



Şekil 4.3: Historian tarayıcı analiz aracı

Adli analiz süreçlerinde Browser Forensic Tool, Mandiant Web historian (Mandiant Redline), Pasco and galeta ve Historian araçlar dışında başka uygulamalarda mevcuttur fakat büyük bir çoğunluğu dar kapsamlı olup belirli dosya analizlerini gerçekleştirmektedir.

5. SONUÇ ve ÖNERİLER

Web tarayıcı araçları, bilişim teknolojilerinde kullanıcıların internete açılmasını sağlayan ilk kapıdır. Bilişim suçları ve internet arasındaki kenetlenmiş ilişki de göz önüne alındığında, bilişim suçları kapsamında suçlu ya da şüpheli konumundaki kişilerin suçla ilişkisinin tespitinde tarayıcıların adli analizi önem arz etmektedir. El konulan bir teknolojik cihazın bu kapsamda değerlendirilmesi delillendirme sürecine kolaylık sağlayacaktır.

Yapılan bu çalışmada bir bilişim suçu kapsamında tarayıcıların kullanılması sonucu bilgisayarda bırakılan izlerin neler olabileceği, hangi dosyalarda ne tür veriler olduğu, hangi sorulara cevaplar aranması gerektiği üzerinde durulmuştur. Ayrıca bazı araçlar yardımıyla tarayıcıların "gizli mod" durumunda kullanılması halinde bırakılan izlerin yakalanması üzerine analizler yapılmıştır. Tarayıcıların adli analizinde kullanılabilecek bazı araçlardan bahsedilmiştir.

Web tarayıcı araçlarının adli analizinde farklı tarayıcı türleri ve farklı işletim sistemleri için yöntemlerin neler olabileceğini tek bir çalışma içerisinde anlatmak mümkün olmadığı için bu çalışmada windows işletim sistemi üzerinde Chrome web tarayıcısı referans alınmıştır. Bu nedenle yapılan bu çalışma farkındalık oluşturmak adına genel resmin küçük bir parçasıdır.

Baran, E., Çakır, H., & Uluyol, Ç. (2015). Web tarayıcılarda adli analiz incelemesi. *International Journal of Human Sciences*, *12*(2), 757-774. doi:10.14687/ijhs.v12i2.3244

KAYNAKÇA

Alemdar, H.(2012). Web Historian: PC den Tüm Tarayıcıların Geçmişini Analiz Etme,

Autofiil Forms, https://support.google.com/chrome/answer/142893?hl=en , Erişim Tarihi: 25.12.2014

Browser Forensic Tool v2.0, https://www.phrozensoft.com/processdl_2.html , , Erişim Tarihi: 23.12.2014

Çerez (İnternet) , http://tr.wikipedia.org/wiki/%C3%87erez_(internet) , Erişim Tarihi: 28.12.2014

Global Market Share , http://www.w3counter.com/globalstats.php, Erişim Tarihi: 23.02.2015

Google Chrome , http://www.forensicswiki.org/wiki/Google_Chrome#Disk_Cache , Erişim Tarihi: 23.12.2014

Google Chrome Privacy Notice,

Google Chrome view saved form data,

Google Chrome, http://tr.wikipedia.org/wiki/Google_Chrome , Erişim Tarihi: 17.12.2014

Historian , http://www.gaijin.at/en/dlhistorian.php , Erişim Tarihi: 25.12.2014

http://superuser.com/questions/224261/google-chrome-view-saved-form-data , Erişim Tarihi: 27.12.2014

http://www.bilgisayarkurdu.com/web-historian-pc-den-tum-tarayicilarin-gecmisini-analiz- etme-17488/ Erişim Tarihi: 24.12.2014

http://www.eticaretsozlugu.com/tarayici-onbellegi-onbellek-cache-nedir.html , Erişim Tarihi: 28.12.2014

http://www.uzmanabi.com/icerik/internette-gezinirken-kisisel-verilerimi-nasil-koruyabilirim-34411.imo , Erişim Tarihi: 28.12.2014

https://www.google.com/chrome/browser/privacy/ . Erişim Tarihi: 28.12.2014

Internet Browser Forensic, The SANS Instute,2013

Kocaman, H. (2014). http://birbitbilgi.com/adli-bilisim-eposta-tarayici.html, Erişim Tarihi: 17.12.2014)

Norulla, E.S. (2014). Web Browser Private Mode Forensics Analysis. Yayınlanmamış Yüksek Lisans Tezi, Rochester Institute of Technology, Computing and Information Sciences, ABD.

Samuel, P. (2007). Internet Explorer Forensics: Reconstructing Internet Activity Using Pasco and Galleta, Term Project, China.

Sonntag, M. (2012). Automating Web History Analysis., Johannes Kepler University Linz, Institute for Information Processing and Microprocessor Technology , Avusturya.

Web Historian, https://www.mandiant.com/resources/download/web-historian , Erişim Tarihi: 23.12.2014

Baran, E., Çakır, H., & Uluyol, Ç. (2015). Web tarayıcılarda adli analiz incelemesi. *International Journal of Human Sciences*, *12*(2), 757-774. doi:10.14687/ijhs.v12i2.3244

Extended English Abstract

In recent years, with the rapid development of internet-based Technologies - services and with having moved many applications to internet, internet-based technologies has become indispensable. In every day, internet dependincies of ICT infrastructure of banking services, energy sector, education, industrial infrastructure, military projects, and health services keep increasing. This rapid increase of the dependence on information technology has created a new environment every day for criminals. The criminals use web browsers to achieve their goals in internet environment also called virtual environment. Therefore, the web browser tools , users of information technology is the first door which opened to the internet.Web browsers provide opening of files such as HTML which is located on web servers. In other words, web browsers transfer, interpret and display HTML files which used for documents on the WEB. Intensive use of web browsers provides infrastructures for cyber-crimes. Because, criminals or suspects use web browsers to gather information, to hide the crime, to learn new methods of crime or to apply what they have learned. Therefore, in forensic, examination of the web browsers, defining data as digital evidence, acquiring data, storing data, analysis and submission data to the court make judicial authorities' job easier.

When it is considered the percent of browser using arond the world ,it seems that chrome, firefox and internet explorer are superiors. Although In this study, chrome web browser is evaluated tracks belonging to chrome because of its % 43 percentage of using among other browsers. Due to reasons mentioned above in this study, Chrome web browser on a Windows operating system has been investigated. According to the survey of internet statistics from W3Counter, with a usage of 43 %, Chrome web browser is most demanding by user. Each operating system and the location and analysis of tracks left to differ from each browser is different. Therefore, this study was conducted examinations carried out on a single browser. When fast devoloping of chrome web browser is considered, it shouldn't be ignored the place of information crime. Therefore, if we consider the vast majority of informatics crimes in the browser of forensic analysis is important considering that the entrance to the questions below. Which sites are visited? , How many times site is visited? , When the site was visited?, Which sites have been saved?,Was it downlanded any files? ,Can we identify any user identity?,Why was the research? These questions show the way to this research. As a result of cyber crime, the tracks left on the computer, datas in the files, the questions that should be answered are examined. The analysis has made with the help of some tools to examine the leftover datas in case of browsing in "incognito mode". Using a variety of tools instead of the conventional method for the evaluation of the data will be useful to speed up the judicial process. Therefore, ıt has mentioned about some tools that can be used in forensic analysis of the browser. It is emphasized which questions should be answered by looking the contents of bookmarks, browsing history, cache, cookies, downloads, autofill inputs. These files is specified the place on the operating system. Files/datas of Chrome browser are of great importance in the judicial process. It is possible to identify the fields of interest and relevance of criminal or suspicious by looking which sites are tracked in the bookmarks . Internet history files can be viewed by looking at the history of access to this site. According to contents in memory cache, the preliminary process is still provided ease. By looking cookies and downloaded content, it can be viewed to obtain the content on which sites at the history file. Additionally, automatic form completion / form can be identified by use of words by looking at the history entry. Because of this, the fils mentioned above are important for proving process.

Additionally, the use of Chrome 's incognito mode feature was investigated whether left any trace or not . Different symptoms has seen when analysing different browsers. File recovery operations on harddisks and RAM memories give different results depends on operating system and

Baran, E., Çakır, H., & Uluyol, Ç. (2015). Web tarayıcılarda adli analiz incelemesi. *International Journal of Human Sciences*, *12*(2), 757-774. doi:10.14687/ijhs.v12i2.3244

browser. In order to trace leftovers in Chrome's "incognito mode", after browsing by Chrome in "incognito mode" on Win7/8, all tabs closed. And, using Recuva filesystem analysis has made. It's seen that Chrome in "incognito mode" has not left any data. However, analysis of RAM contents by using Belkasoft RAM Capture tool and WinHex, it's been found the leftover datas from Chrome's incognito mode. Results showed that forensic analysis of RAM contents can give useful data even if Chrome's incognito mode feature has used. However, it should be noted that powering off the PC in any way, RAM data vanish.

For each operating system and browser, the location of leftover data and analysis of them are different. In this study is taken up references just a single browser because it is imposible to describe what can be for operating systems and different browsers types for forensic analysis of web browsers tools in a sigle operation. Therefore, this analysis on Chrome is just an example to emphasize that what could be the forensic techniques, to increase awarenesss of forensic evidence processes, to show what kind of data could be find in which files.