

FORENSIC EXAMINATION OF CHROME AND FIREFOX WEB BROWSERS

Bariş CEVİZ¹

Abstract

Today's users use web browsers to connect to the internet. For this reason, browsers provide infrastructure for crimes committed over the internet. Because the suspect or criminal uses web browsers to gather information, learn criminal methods or put what they have learned into practice. Chrome and Firefox were used in this research. As a result of a detailed examination of two different web browsers, answers were sought to various questions such as what kind of process can be followed in detecting traces left on the computer, and what kind of data can be obtained from which files. As a result of the researches carried out by the internet statistics tool Statcounter, the worldwide usage of the Chrome Web Browser with 67.23% and the Firefox Web Browser with a usage rate of 7.57% were used. The reasons for using the web browsers, which are the references of this research, are that the two browsers are the most used web browsers in the world and both have different file systems. In addition, in this research, "revealing the user's registered passwords and user names" was examined. Thus, by revealing what kind of data can be obtained in web browsers, its effects in the studies of obtaining evidence of criminal or suspicious persons will be investigated.

Keywords: Forensic Analysis, Chrome Web Browser, Firefox Web Browser, Cyber Crimes

CHROME VE FIREFOX WEB TARAYICILARININ ADLI İNCELEMESİ

Özet

Günümüz kullanıcıları internete bağlanabilmek için web tarayıcılarını kullanıyorlar. Bu sebeple internet üzerinden işlenen suçlarda tarayıcılar alt yapı sağlıyor. Çünkü şüpheli veya suçlu kişi, tarayıcıları bilgi toplamak, suç metotları öğrenmek ya da öğrendiklerini uygulamaya dökmek için web tarayıcılarını kullanıyor. Bu araştırmada Chrome ve Firefox kullanılmıştır. İki farklı web tarayıcısı detaylı bir inceleme sonucunda bilgisayar üzerinde bırakılan izleri tespitinde nasıl bir süreç izlenebileceği, hangi dosyalardan ne tür veriler elde edebileceği gibi çeşitli sorulara cevap aranmıştır. Statcounter isimli internet istatistik aracının yaptığı araştırmalar sonucunda dünya genelinde %67.23'lük bir kullanıma sahip Chrome Web Tarayıcısı ve %7.57'lik bir kullanıma sahip Firefox Web Tarayıcısı kullanılmıştır. Bu araştırmanın referans olan web tarayıcılarının kullanım sebepleri ise iki tarayıcıda dünyada en çok kullanılan web tarayıcıları ve ikisinin de farklı dosya sistemlerine sahip olması. Ayrıca bu araştırmada "kullanıcının kayıtlı şifreleri ve kullanıcı adlarının ortaya çıkarılması" incelenmiştir. Böylelikle web tarayıcılarında ne tür veriler elde edebileceği ortaya konarak suçlu ya da şüpheli kişilere ait delil elde etme çalışmalarında etkileri araştırılacaktır.

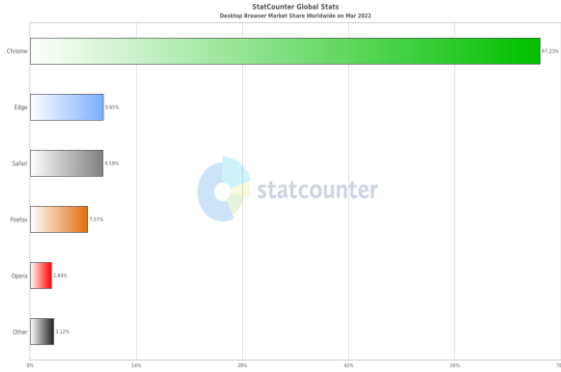
Anahtar Kelimeler: Adli analiz, Chrome Web Tarayıcısı, Firefox Web Tarayıcısı, Bilişim Suçları

¹ Adli Bilişim Mühendisliği, Fırat Üniversitesi, Teknoloji Fakültesi, baris.ceviz1@gmail.com

1. GİRİŞ (INTRODUCTION)

Günümüzde internet tabanlı teknoloji ve hizmetlerin hızlı gelişmesi ve bu gelişmelerle sonucunda uygulamaların internet üzerine aktarılması internet tabanlı teknolojilerini vazgeçilmez kılıyor. Bilişim teknolojilerinin gün geçtikçe çoğalması suçlular için yeni bir ortam oluşturmaktadır. İnternet ortamında işlenen suçların büyük bir çoğunluğu web tarayıcılar üzerinden işlenmektedir. Web tarayıcıları, kullanıcıların web sayfaları ve web içerikleri ile etkileşime izin veren yazılımlardır. Bu yazılımların kullanan bilgisayarlar üzerinde ciddi izler bırakılmaktadır ve farklı olan her bir tarayıcı için yeri ve analizi farklıdır. Bu yüzden

bu araştırmada iki farklı web tarayıcısında işlem yapılmaktadır.



Şekil 1: Dünya genelinde Tarayıcıların Kullanım Yüzdesi, Mart 2022



Şekil 2: Analiz Sırasında Sorulması Gereken Sorular

Şekil 2’de yer alan sorulardan faydalanılarak web tarayıcılarının adli incelemesinde yöntemlerin neler olduğunu belirleme, adli delil elde etme süreçlerinde yetkili kişilerde bir bilinç oluşturmak,

Dünya genelinde tarayıcıların kullanım yüzdeleri de dikkate alındığında en çok kullanılan web

tarayıcılarında Chrome’un üstünlüğü görülmektedir (Şekil 1). Bu araştırmada dünya genelinde en çok kullanılan web tarayıcılarından Chrome ve Firefox’a ait izler değerlendirilecektir hangi dosyalarda ne tür bilgiler olduğunu dikkat çekmek bu araştırmanın temel amacıdır.

2. CHROME VE FIREFOX WEB TARAYICILARININ ADLİ İNCELEMESİ

Chrome web tarayıcısı, Google tarafından geliştirilen ücretsiz bir web tarayıcısıdır. Eylül 2008’de Microsoft Windows sürümü yayınlanmış olup; daha sonra macOS, Linux, iOS ve Android sürümleri piyasaya sürülmüştür. Chrome’un kaynak kodlarının büyük kısmı Chromium adlı açık kaynak projesi kapsamında paylaşılır. Dahili bazı bileşenlerinin ise kaynak kodları paylaşılmaz.

Mozilla Firefox, Mozilla Corporation tarafından geliştirilen, açık kaynak kodlu bir web tarayıcısıdır. Firefox; Windows, macOS, Linux, Android ve iOS işletim sistemlerinde kullanılabilir. Firefox iOS için Apple getirdiği kısıtlamalar sonucu WebKit motorunu kullanır. Diğer işletim sistemlerinde ise Gecko motorunu kullanır. İlk olarak Chrome tarayıcısının adli analizini gerçekleştireceğiz ve verilerin nerede tutulduğu ve ne tür veriler tuttuğu hakkında bilgileri araştıracağız.

3. CHROME WEB TARAYICISI (CHROME WEB BROWSER)

Chrome web tarayıcısını bilgisayara indirmeniz halinde işletim sisteminde bırakılan veriler aşağıdaki dizinde yer alır.

Win10: C:\Users\%username%\AppData\Local

\Google\Chrome

Win7/8: C:\Users\%username%\AppData\Local

\Google\Chrome

Linux: \home\%username%\config\google-chrome

MacOS: \Users\%username%\Caches\Google\Chrome\

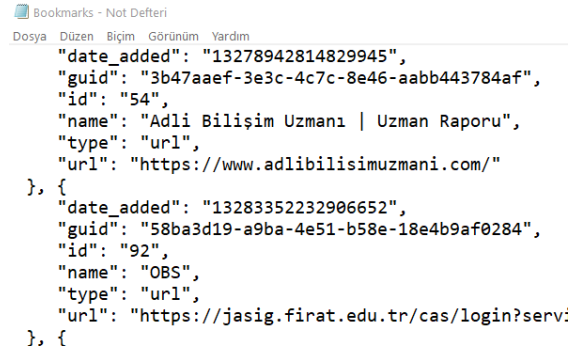
Chrome kayıt altına aldığı bütün verileri tek bir dosya dizini altında tutması adli incelemelerde kolaylık sağlamaktadır. Verilerin büyük bir çoğunluğu SQLite veri tabanında tutulduğu için verilere bakmak oldukça kolaydır.

Chrome tarayıcısının verilerine bakarak adli süreçlerde bir çok delil elde edebiliriz. Geçmiş bilgilerine bakarak suçlu ya da şüphelinin hangi sitelere girdiğini öğrenebilir, yer imlerine bakarak

hangi siteleri kayıt altına aldığını, ön bellek, kayıt altında tutulan form, kullanıcı adı ve şifrelerinin içeriklerine bakarak delil elde etme sürecinde kolaylık sağlanabilir. Bu nedenle aşağıda yer alan dosyalar delil elde etme sürecinde önemlidir.

3.1 Yer İmleri (Bookmarks)

“Kayıt edilen siteler hangileri?” sorusuna cevap ararken bakılması gereken ilk dosyadır. Siteye ait URL, sitenin eklenme/değiştirilme tarihi, başlık bilgileri ve sitenin bulunduğu menü başlığı ya da klasör gibi yer bilgilerini bookmarks dosyası içinde depolanır (Şekil 3).



Şekil 3: Chrome Bookmarks Dosyası Görüntüsü

Bookmarks dosyasının konumu,

C:\Users\baris\AppData\Local\Google\Chrome

\User Data\Default\ altında Bookmarks isimli dosyadan ulaşabilirsiniz.

3.2 İnternet Geçmişi (Internet History)

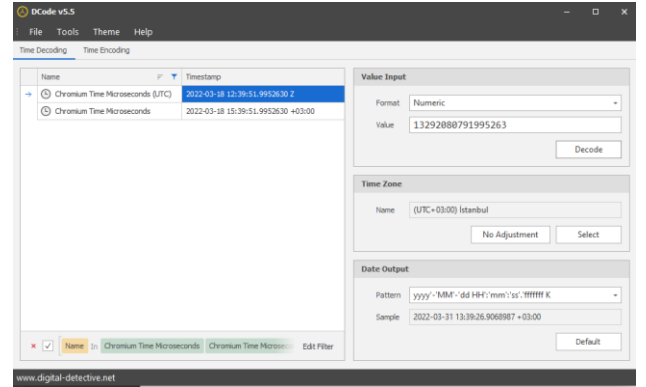
“Hangi siteler ziyaret edildi?”, “Ne zaman ziyaret edildi?”, “Kaç defa ziyaret edildi?” şeklinde sorulan soruların cevabını bu dosya içinde aramak mümkündür. SQLite veri tabanı formatında tutulan dosya içerisinde URL, başlık bilgileri, kaç defa ziyaret edildiği, en son ne zaman ziyaret edildiğine dair veriler tablo halinde tutulmaktadır.

	id	url	title	visit_count +1	typed_count	last_visit_time
	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre
1	6	https://twitter.com/...	Home / Twitter	411	1	13292080791995263
2	6067	https://wiflgsb.gov.tr/	Giriş	191	4	13292890356306457
3	3261	https://...	Instagram	115	5	13291911622135902
4	8	https://...	(1) YouTube	100	0	13292609742170594
5	13170	https://medium.com/	Medium	96	3	13291971877868435

Şekil 4: Chrome History Dosya Görüntüsü

Chrome web tarayıcısına ait History dosyası içinde yer alan tablolar kullanıcının Chrome üzerinden gerçekleştirdiği internet aktiviteleri hakkında bize detaylı bilgi vermektedir. Şekil 4’de gösterilen resimde bilgiler en çok girilen siteler yukarıdan aşağı

sıralanmıştır. Şekil 4’de görmüş olduğunuz last_visit_time sütunu içerisinde zaman damgaları mevcuttur bu zaman damgalarını anlaşılır bil hale getirmek için “DCode” aracını kullanabiliriz.



Şekil 5: DCode aracının ekran görüntüsü

İnternet Geçmişi dosyası History’nin konumu,

C:\Users\%username%\AppData\Local\Google\Chrome\User Data\Chrome\Default altında History isimli dosyadan ulaşabilirsiniz.

3.3 Çerezler (Cookies)

Çerezler, herhangi bir internet sitesi tarafından bilgisayara bırakılan bir tür tanımlama dosyası. Çere dosyalarında oturum bilgileri ve benzeri veriler saklanır. Çerez kullanan bir site ziyaret edildiğinde bu site, erişimin yapıldığı tarayıcıya sabit diske bir ya da daha fazla çerez bırakma konusunda talep gönderebilir.

Çerez dosyası içerisinde çerez isteğinin adı, hangi sunucudan gönderildiği, ne zaman oluşturulduğu, ne zaman sonlandırıldığı ve son erişim tarihi gibi zaman damgaları görüntülenebilir. SQLite formatında olan dosyanın içeriğine rahatlıkla bakabilirsiniz.

	creation_utc +1	ame_sit	host_key	name	value	rypted_va	path	expires_utc
	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre
1	13265832239248357		.adblock-for-...	_ga		BLOB	/	13328904239000000
2	13265832243274325		.youtube.com	VISITOR_INFO_LIVE		BLOB	/	13305565754693017
3	13265832243274359		.youtube.com	LOGIN_INFO		BLOB	/	13328904243274359
4	13265832835081810		.udemy.com	__udmy_2_v57r		BLOB	/	13323186514737358
5	13265832835081939		www.udemy.com	ud_firstvisit		BLOB	/	1329736835081939
6	13265832836039307		www.udemy.com	EUCookieMessageSh...		BLOB	/	13581192836000000
7	13265832839325618		.udemy.com	__ssid		BLOB	/	13392063239000000
8	13265832839829732		.intjs.rmtag.com	rmuid		BLOB	/	13309700955179194

Şekil 6: Chrome Cookies Dosya Görüntüsü

Çerez dosyasının konumu,

C:\Users\baris\AppData\Local\Google\Chrome\User Data\Default\Network altında Cookies dosyasından ulaşabilirsiniz.

3.4 Form Geçmişi (Form History)

İnternet üzerinde bir sayfada herhangi bir işlem sırasında bilgilerin girdisi ilk defa yapılıyorsa kullanıcı istediği takdirde bu bilgiler kayıt altına alınır. Böylelikle kayıt altına alınan isim, adres, telefon numarası, e-posta adresi, kimlik bilgileri otomatik doldurma girdisi olabilir. Bu nedenle herhangi bir suç kapsamında ele geçirilen bir bilgisayar ya da alınan bir imaj üzerinde bu verilerin araştırılması önem arz etmektedir.

	name	value	value_lower	date_created	date_last_used	count
	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre
32	account_setu...	Barış	barış	1622330019	1622330019	1
33	account_setu...	Ceviz	ceviz	1622330019	1622330019	1
34	account_setu...	██████████ Sokak	██████████ mah. ...	1622330019	1622330019	1
35	account_setu...	██████████ No:7	██████████ no:7	1622330019	1622330019	1
36	account_setu...	68100	68100	1622330019	1622330019	1
37	account_setu...	Aksaray	aksaray	1622330019	1622330019	1
38	account_setu...	54 ██████████	54 ██████████	1622330019	1622330019	1

Şekil 8: Web Data Dosyası İçerisinde Bulunan Veriler

Form geçmişlerinin kayıt altında tutulduğu dosya Web Data dosyasıdır. Web Data dosyası da verileri SQLite formatında tutmaktadır. Şekil 8’de görüldüğü üzere şüpheli ya da suçlunun ev adresi, telefon numarası gibi bilgilere buradan ulaşabilirsiniz.

Web Data dosyasının konumu,

C:\Users\baris\AppData\Local\Google\Chrome\User Data\Default altında Web Data dosyasına ulaşabilirsiniz.

3.5 İndirilenler Geçmişi (Downloads History)

Kullanıcı indirme verilerini temizlemediği sürece kayıtları tarayıcı tarafından tutulur. Bu kayıtların içerisinde dosyaların yeri, hangi URL üzerinden indirildiği, ne zaman indirildiği, indirilen dosyanın büyüklüğü, indirme işleminin başlatılması ve bitiş tarihleri gibi bilgiler bulunur. Veriler SQLite formatında tutulmaktadır.

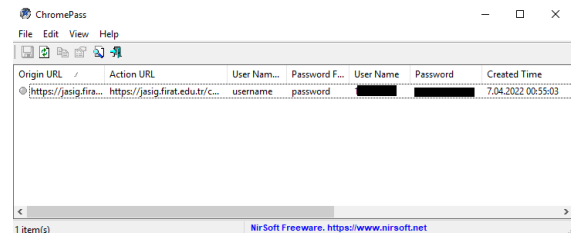
	id	guid	current_path	target_path	start_time
	Filtre	Filtre	Filtre	Filtre	Filtre
1	631	3e86b24d-725c-47d...		C:\Users\baris\Downloads\Adobe ...	13287481680169000
2	632	0be99fee-49f5-4372...	C:...	C:\Users\baris\Downloads\DumpIt.zip	13291462270380286
3	633	551a682b-7816-4b0...			13291462881821224
4	634	5204f124-4d69-4cbf...			13291462887159179
5	635	c0d53f19-6419-4aaa...			13291464266939794
6	636	f7cb240-9b24-493b...	C:\Users\baris\Downloads\pdf-...	C:\Users\baris\Downloads\pdf-redline.zip	13291464963897940
7	637	dc0e3fb-...	C:\Users\baris\Downloads\ug-...	C:\Users\baris\Downloads\ug-redline.pdf	13291465008533222
8	638	fe1c067-000f-4c91...	C:...		13291467784626569
9	639	ec90973-...	C:...		13291467849657035

Şekil 9: History Dosyası İçerisinde Bulunan İndirilenler Geçmişi

İndirilenler geçmişi dosya konumu, C:\Users\%username%\AppData\Local\Google\User Data\Chrome\Default altında History isimli dosyadan ulaşabilirsiniz.

3.6 Kayıtlı Hesaplar ve Parolalar(saved accounts and passwords)

Chrome web tarayıcısında şüpheli ya da suçlunun önceden oturum açtığı sitelerde kullanıcı adı ve şifrelerini kayıt altında tuttuğu bölüm bu kısımda araştırılmıştır. Bunu araştırmamızdaki sebep ise suçlu ya da şüpheli kişi bir web uygulamasından suç işlediğinde kolluk kuvvetlerine kendi rızası ile parola ve kullanıcı adını vermemesi durumunda adli uzmanlar çeşitli yöntemlere başvurarak şifreleri ve kullanıcı adlarını ulaşmaya çalışmaktadır. Bu süreç genellikle zor ve bazı durumlarda şüpheli ya da suçlu kişinin verilerine ulaşamamaktadır. Chrome kayıtlı kullanıcı adlarını ve parolarları C:\Users\%username%\AppData\Local\Google\Chrome\User Data\Default klasörü içerisinde “Login Data” dosyası içerisinde tutmaktadır. Verileri DB Browser for SQLite programı ile açıldığında parolalar görünmemektedir. Verilere ulaşmak için Nirsoft Chromepass uygulamasını kullanıldı. Şekil 10’da görebileceğiniz üzere bütün verilere ulaşabilirsiniz.



Origin URL	Action URL	User Nam...	Password F...	User Name	Password	Created Time
https://jagis.fira...	https://jagis.firat.edu.tr/c...	username	password	██████████	██████████	7.04.2022 00:55:03

Şekil 10: ChromePass Ekran Görüntüsü

4. FIREFOX WEB TARAYICISI (FIREFOX WEB BROWSER)

Firefox web tarayıcısını bilgisayarınıza indirmeniz halinde işletim sisteminde bırakılan veriler aşağıdaki dizinde yer alır.

Win10: C:\Users\%username%\AppData\Roaming\Mozilla\Firefox

C:\Users\baris\AppData\Local\Mozilla

Firefox verilerinin büyük bir kısmını Roaming klasörü altında tutar. Web tarayıcılarının mimarileri hemen hemen birbirine benzer bu yüzden bir web tarayıcısının mimarisini biliyorsanız başka bir web tarayıcının mimarisini kolaylıkla öğrenebilirsiniz.

Firefox tarayıcısında da Chrome da uyguladığımız işlemleri ve aynı senaryoyu uygulayacağız ama

ekstra olarak bir şüphelinin ya da suçlunun bilgisayarının alınmış olan imaj dosyasında kayıt altında tutulan şifrelere nasıl ulaşabileceğimizi araştıracağız.

4.1 Yer İmleri (Bookmarks)

Firefox web tarayıcısında yer imleri bir SQLite dosyası halinde tutulmaktadır.

Dosyanın konumu, C:\Users\%username%\AppData\Roaming\Mozilla\Firefox\Profiles\default-release klasörü altında “places.sqlite” dosyası içerisinde moz_bookmarks tablosu içerisinde ulaşabilirsiniz.

id	type	fk	parent	position	title	keyword_id	older_type	dateAdded	lastModified
10	1	3	7	2	Get Involved			164733958866000	164733958866000
11	1	4	7	3	About Us			164733958866000	164733958866000
12	1	5	3	0	Getting Started			1647339588676000	1647339588676000
13	1	8	3	1	Gmail			1647339639479000	1647339639479000
14	2		3	2	Kurs			1647339639479000	1648549343520000
15	1	9	14	0	Udemy			1647339639479000	1647339639479000

Şekil 11: Firefox Web Tarayıcısı Yer İmleri

Firefox web Tarayıcısında kullanılan zaman damgalarını saat dilimine çevirmek isterseniz, DB Browser for SQLite aracının SQL kodu yürütme alanına

```
Select strftime('%d-%m-%Y', (*Name of Column* / 1000000), 'unixepoch') FROM /* Name of Table*/
```

Bu SQL komutunu çalıştırırsanız size bütün sütün da bulunan zaman damgalarını okunabilir hale getirebilirsiniz.

SQL 1	Select strftime('%d-%m-%Y', (dateAdded / 1000000), 'unixepoch') FROM moz_bookmarks
me('%d-%m-%Y', (dateAdded / 1000000), 'unixepoch')	
96	15-03-2022
97	17-03-2022
98	25-03-2022
99	25-03-2022
100	29-03-2022
101	30-03-2022
102	30-03-2022
103	30-03-2022

Şekil 12: SQL kodunun örnek bir çıktısı

4.2 İnternet Geçmişi (History)

Firefox web tarayıcısında veriler genellikle aynı veri tabanında tutuluyor.

Dosyanın konumu, C:\Users\%username%\AppData\Roaming\Mozilla\Firefox\Profiles\default-release klasörü altında “places.sqlite” dosyası içerisinde moz_places tablosu içerisinde ulaşabilirsiniz.

id	url	title	rev_host	visit_count	hidden	typed	frequency	last_visit_date	guid
72	https://...	File ...	ten.relssek...	0	0	0	250	1648631667393000	gwAPLXHM
73	https://gaissecurity.co...	FILE	moc.ytruc...	0	0	0	86		8qVjAzCPf
74	https://...	FILE	moc.irelta...	0	0	0	86		4Kw7B3kgf
75	https://...	FILE	moc.amrat...	0	0	0	86		Y7FQmGKEI
76	https://gaissecurity.com/	FILE	moc.ytruc...	0	0	0	86		5xgAVfZDfh
77	https://pindr.com/tr/q/...	Phot...	moc.rhlp...	0	0	0	54	1645979667497000	dz2nEbwTw
2087	https://...	Adli ...	moc.etutts...	0	0	0	545	1648630309144000	sFQ7Hjg7e
2149	https://...	on-...	ku.ca.reipa...	0	0	0	150	1648566413043000	YzjCB7_EVf
2153	https://...	Digit...	moc.tcerid...	0	0	0	405	1648566408528000	UZv8WwxB8
2304	https://dfirdiva.com/	Yeni...	moc.avdrifd...	0	0	0	318	1647447887229000	eZEueqGEv
2312	https://dfirdiva.com/...	Ücr...	moc.avdrifd...	0	0	0	109	1647360545926000	DhURLStW

Şekil 13: Firefox Web Tarayıcısı İnternet Geçmişi

4.3 Çerezler (Cookies)

Firefox web Tarayıcısında Çerezler C:\Users\%username%\AppData\Roaming\Mozilla\Firefox\Profiles\default-release klasörü altında “cookies.sqlite” içerisinde bulabilirsiniz.

#	originalAttribute	name	value	host	path	expiry	lastAccessed	creationTime
34	OSID	1a9b839p70RbPgcKEM...	myaccount.goog...	/	/	1710411729	1647339728709000	1647339728709000
35	Secure-OSID	1a9b839p70RbPgcKEM...	myaccount.goog...	/	/	1710411729	1647339728709000	1647339728709000
40	OTZ	6417262_44_48_123900...	myaccount.goog...	/	/	1649931740	1649183854634000	1647339739791000
91	Host-GMAIL_SCH_CMN	1	mail.google.com	/	/	1649931740	1649183854634000	1647339739791000
92	Host-GMAIL_SCH_CM5	1	mail.google.com	/	/	1649931740	1649183854634000	1647339739791000
93	Host-GMAIL_SCH_CML	1	mail.google.com	/	/	1649931740	1649183854634000	1647339739791000
224	OTZ	6417262_44_48_123900...	ops.google.com	/	/	1649931745	1649238065166000	1647339745490000
235	OTZ	6417262_44_48_123900...	contacts.google...	/	/	1649931746	1649183305777000	1647339746052000
330	moz-stub-attribution-code	c291cmNPShub3QgcZVL...	www.mozilla.org	/	/	1647426282	1647366619715000	1647339882330003
331	moz-stub-attribution-sig	61c0f64650726043880b4...	www.mozilla.org	/	/	1647426282	1647366619715000	1647339882330004

Şekil 14: Firefox Web Tarayıcısı Çerezler

4.4 Form Geçmişi (Form History)

Firefox web tarayıcısında form geçmişi C:\Users\%username%\AppData\Roaming\Mozilla\Firefox\Profiles\default-release klasörü altında “formhistory.sqlite” içerisinde ulaşabilirsiniz.

id	fieldname	value	timesUsed	firstUsed	lastUsed	guid
1	username	195509032	4	1649080707120000	1649245615382000	NnpG3J2eT...
2	searchbar-...	türk telekom ...	1	1649081163928000	1649081163928000	+rkzVfWVR...
3	searchbar-...	twitter	1	1649083172555000	1649083172555000	bvUlm+...
4	searchbar-...	burp suite	1	1649141641789000	1649141641789000	/...
5	searchbar-...	revo uninstaller	1	1649146900059000	1649146900059000	T5uVafn/...
6	searchbar-...	aladdin shared	1	1649148705133000	1649148705133000	8RHU5SuAT...

Şekil 15: Firefox Web Tarayıcısı Form Geçmişi

4.5 İndirilenler Geçmişi (Downloads History)

Firefox web warayıcısının indirme geçmişi C:\Users\%username%\AppData\Roaming\Mozilla\Firefox\Profiles\default-release klasörü altında “places.sqlite” dosyası içerisinde “moz_annos” tablosundan ulaşabilirsiniz.

id	place_id	_attribul	content	flags	expiration	type	dateAdded	lastModified
1	122	4786	1 file:///C:/Users/boris/Downloads/...	0	4	3	1648657029170000	1648657029170000
2	123	4786	2 ("state":1,"endTime":...	0	4	3	1648657029563000	1648657029563000
3	124	4809	1 file:///C:/Users/boris/Downloads/...	0	4	3	1649141660710000	1649141660710000
4	125	4809	2 ("state":1,"endTime":...	0	4	3	1649141660758000	1649141660758000
5	126	4854	1 file:///C:/Users/boris/Downloads/...	0	4	3	1649146932421000	1649146932421000
6	127	4854	2 ("state":1,"endTime":...	0	4	3	1649146933659000	1649146933659000
7	128	4899	1 file:///C:/Users/boris/Downloads/beyaz-...	0	4	3	1649154996124000	1649154996124000

Şekil 16: Firefox Web Tarayıcısı İndirilenler Geçmişi

4.6 Kayıtlı Hesaplar ve Parolalar(saved accounts and passwords)

Firefox web tarayıcısında şüpheli ya da suçlunun önceden oturum açtığı sitelerde kullanıcı adı ve şifrelerini kayıt altında tuttuğu bölüm bu kısımda araştırılmıştır. Bunu araştırmamızdaki sebep ise suçlu ya da şüpheli kişi bir web uygulamasından suç işlediğinde kolluk kuvvetlerine kendi rızası ile parola ve kullanıcı adını vermemesi durumunda adli bilişim inceleme uzmanları çeşitli yöntemlere başvurarak şifreleri ve kullanıcı adlarını ulaşılmaya çalışmaktadır. Bu süreç genellikle zor ve bazı durumlarda şüpheli ya da suçlu kişinin verilerine ulaşılamamaktadır. Bu çalışmada iki farklı yöntem sunulmaktadır. İlk olarak Firefox Decrypt aracı ile kullanıcı adı ve şifrelere ulaşmak. İkincisi, suçlu ya da şüphelinin imajı alınan bilgisayarında belirli dosyaların dışarı çıkartılarak sanal ortamda kullanıcı adı ve şifrelerine ulaşmak. Firefox kullanıcı adı ve şifreleri

C:\Users\%username%\AppData\Roaming\Mozilla\Firefox\Profiles\default-release klasörü altında “logins.json” dosyasında tutar.

```
1 {"nextId":69,"logins":[{"id":1,"hostname":"https://twitter.com",
"httpRealm":null,"formSubmitURL":"https://twitter.com",
"usernameField":"session[username_or_email]","passwordField":"session
[password]",
"encryptedUsername":"MDoEEpGAAAAAAAAAAAAAAAEwFAYIKoZThvcNwCECKoP8b9euZ
MOBBAHAL107B5y6YtCPAMwT0",
"encryptedPassword":"MDoEEpGAAAAAAAAAAAAAAAEwFAYIKoZThvcNwCECEHixn6m8d
b8BB88e5IN3vZnrdaNR7qpes","guid":"(27362be0-c07f-4475-a143-3d0a83732859)",
"encType":1,"timeCreated":1621174943998,"timeLastUsed":1621174943998,
"timePasswordChanged":1621174943998,"timesUsed":1},{id":2,
```

Şekil 17: Logins.json Dosyasının Görüntüsü

Şekil 17’de görmüş olduğunuz dosya görüntüsünde kullanıcı adı ve şifrenin encrypted bir şekilde olduğunu rahatlıkla görebilirsiniz. Burada bulunan şifreleri ve kullanıcı adlarını elde etmek için Firefox Decrypt aracını kullanacağız.

```
Komut İstemi
Website: https://twitter.com
Username: 
Password: 

Website: https://www.udemy.com
Username: @gmail.com
Password: 

Website: https://jasig.firat.edu.tr
Username: 
Password: 

Website: https://www.baykarakademi.com
Username: @gmail.com
Password: 

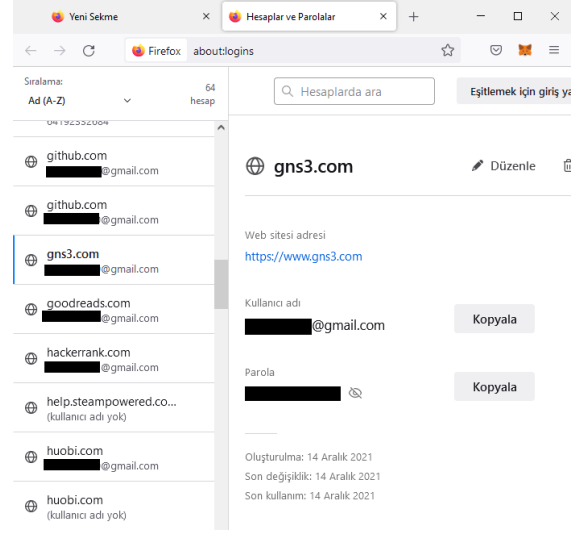
Website: https://github.com
Username: @gmail.com
Password: 
```

Şekil 18: Firefox Decrypt Görüntüsü

İkinci yöntemde ise imajı alınan bilgisayarın Şekil 19’da bulunan dosyalar dışarı aktarılır. Elimizde bulunan bu dosyaları sanal makinemize kurmuş olduğumuz Firefox web tarayıcısında aynı klasör konumuna yapıştırıyoruz. Ardından Firefox web tarayıcısının arama çubuğunu “about:logins” kısmında şüpheli ya da suçlunun kaydettiği tüm hesaplara erişebilirsiniz(Şekil 20).

key4.db	15.03.2022 13:20	Data Base File	288 KB
logins.json	6.04.2022 14:46	JSON Kaynak...	37 KB
logins-backup.json	5.04.2022 22:24	JSON Kaynak...	37 KB

Şekil 19: Dışarı Aktarılması Gereken Dosyalar



Şekil 20: “about:logins” Ekranından Bir Çıktı

5. KULLANILAN PROGRAMLAR (USED PROGRAMS)

- DB Browser for SQLite
- HxD
- Chromepass
- Firefox Decrypt
- Dcode

6. SONUÇ ve ÖNERİLER (RESULTS AND SUGGESTIONS)

Adli bilişim elektronik ortamda mevcut verilerin güvenliğinin sağlanması için alınması gereken önlemleri, hukuki sürece yardımcı olabilecek şekilde verilerin incelenmesi ve değerlendirilmesi olarak tanımlanabilir. Günümüzde elektronik ortamda yaygın kullanılan programlar ve uygulamaların kendilerine ait özel dosya yapısı bulunmaktadır. Bir adli bilişim uzmanı yaygın kullanılan bu uygulamaların dosya yapısını düzgün ve belirli standartlara uygun olarak analiz edebilirse hem hukuki süreci hızlandırmış olur hem de amaçlanan verinin elde edilmesi mümkün hale gelebilir. Bu çalışmada Google Chrome web tarayıcısı v.100.0.4896.75 ve Mozilla Firefox web tarayıcısı v.99.0 sürümüne sahip bir bilgisayar incelenerek çeşitli vakalarda adli bilişim uzmanları için elde edilebilecek veriler değerlendirilmiştir. Adli bilişim inceleme uzmanlarının uygulama dosyaları, bu dosya içeriklerinin neler olduğunu ve hangi verilerin

tutulduğunun bilinmesi incelemeyi kolaylaştırmaktadır. Bu nedenle çalışmada sunulan bulgular Google Chrome ve Mozilla Firefox Web Tarayıcılarının yapısını ortaya koymaktadır.

Google Chrome ve Mozilla Firefox web tarayıcılarının yer imleri, internet geçmişi, çerezler, form geçmişi, indirilenler geçmişi, kayıtlı hesaplar ve parolalar başlıkları ile ele alınarak incelenmiştir. Yer imlerinde kayıt altında tutulan web sitelerini bulurken, internet geçmişinde suçlu ya da şüphelinin hangi web sitelerine girdiği tespit edilebilir. Çerezlerine ulaşarak suçlu ya da şüpheli hangi web sitelerinde ne tür veriler barındırıyor bunlara ulaşılabilir, form ve indirilenler geçmişinde suçlu ya da şüpheli özel verilerine ve internet üzerinden ne indirdiğine ulaşabiliriz. Kayıtlı hesaplar ve parolalar da suçlu ya da şüphelinin rızası ile vermediği parolaları adli bilişim inceleme uzmanları kolaylıkla tespit edebilir.

Web tarayıcı araçlarının adli analizinde farklı tarayıcı türleri ve farklı işletim sistemleri için yöntemler neler olabileceği tek bir çalışmada içerisinde anlatmak mümkün olmadığı için bu çalışmada Windows 10 işletim sistemi üzerinde Chrome ve Firefox web tarayıcısı referans alınmıştır.

KAYNAKLAR (REFERENCES)

Wikipedia, “Google Chrome”, 2 Nisan 2022, Erişim Tarihi: 4 Nisan 2022

Wikipedia, “Mozilla Firefox”, 5 Mart 2022, Erişim Tarihi: 4 Nisan 2022

Erkan Baran, Hüseyin Çakır, Çelebi Uluyol, “Web Tarayıcılarda Adli Analiz”, Journal of Human Sciences, Ekim 2015, Erişim Tarihi: 4 Nisan 2022

Yusuf Can Çakır, “Mozilla Firefox Adli İncelemesi”, Yapay Akademi, 4 Kasım 2021, Erişim Tarihi: 4 Nisan 2022

“Profiller - Firefox'un yer imlerinizi, parolalarınızı ve diğer kullanıcı verilerini tuttuğu yer”, Mozilla Firefox Support, Erişim Tarihi: 4 Nisan 2022

“Firefox Sürümleri”, Mozilla Firefox, Erişim Tarihi: 4 Nisan 2022

Nitesh Malviya, “Browser Forensics: Firefox”, Infosec Institute, 16 Ekim 2020, Erişim Tarihi: 4 Nisan 2022

Xosé Fernández-Fuentes, Tomás F. Pena, José C. Cabaleiro, “Digital forensic analysis methodology for private browsing: Firefox and Chrome on Linux

as a case study” 26 Nisan 2021, Erişim Tarihi: 5 Nisan 2022

R.Bagley, R.I. Ferguson, P. Leimich, “Firefox Browser Forensic Analysis Via Recovery Of Sqlite Artefacts From Unallocated Space”, Canterbury Christ Church University, Ekim 2012, Erişim Tarihi: 5 Nisan 2022

Halil Öztürkci, “Google Chrome Üzerinde Adli Bilişim İncelemesi”, Halil Öztürkci Ali Bilişim ve Bilişim Güvenliği Günlüğü, 27 Temmuz 2015, Erişim Tarihi: 5 Nisan 2022

Statcounter, “Browser Market Share Worldwide”, Mart 2022, Erişim Tarihi: 4 Nisan 2022

Kristinn Guðjónsson, “Google Chrome Forensics”, SANS Blog, 21 Ocak 2010, Erişim Tarihi: 4 Nisan 2022

Emad Sayed Noorulla, “Web Browser Private Mode Forensics Analysis”, Rochester Institute of Technology, 30 Haziran 2014, Erişim Tarihi: 5 Nisan 2022

Craig Wilson, “Decoding Other Timestamp Formats”, Digital Detective, 25 Haziran 2021, Erişim Tarihi: 05 Nisan 2022

DB Browser for SQLite, 18 Mayıs 2021, Erişim Tarihi: 5 Nisan 2022

Renata Alves, Firefox Decrypt, 01 Şubat 2021, Erişim Tarihi: 6 Nisan 2022

ChromePass, Nirsoft, 19 Mart 2022, Erişim Tarihi: 6 Nisan 2022

Oleg Skulkin, Igor Mikhaylov, “An Overview Of Web Browser Forensics”, Erişim Tarihi: 05 Nisan 2022

Nasreddine Bencherchali, “Web Browsers Forensics”, Medium Nasreddine Bencherchali, 20 Ekim 2019, Erişim Tarihi: 04 Nisan 2022

Ahmad Ghafarian, “Forensics Alaysis of Privacy of Portable Web Browsers”, Annual ADFSL Conference on Digital Forensics, Security and Law, 25 Mayıs 2016, Erişim Tarihi: 4 Nisan 2022

Hasan Fayyad-Kazan, Sondas Kassem-Moussa, Hussin J Hejase, Ale J Hejase, “Forensic Analysis of Private Browsing Mechanisms: Tracing Internet Activities”, Journal Of Forensic Science And Research, 8 Mart 2021, Erişim Tarihi: 06 Nisan 2022