TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

WINDOWS 7 VE 8 İŞLETİM SİSTEMLERİNDE FARONICS DEEPFREEZE STANDARD PROGRAMI KURULU SABİT DİSKLERİN ADLİ OLARAK İNCELENMESİ

Ahmet SALUK

FİZİKİ İNCELEMELER VE KRİMİNALİSTİK ANABİLİM DALI
YÜKSEK LİSANS TEZİ

DANIŞMAN
Yrd.Doç.Dr.Recep ERYİĞİT

Ankara
2016

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

WINDOWS 7 VE 8 İŞLETİM SİSTEMLERİNDE FARONICS DEEPFREEZE STANDARD PROGRAMI KURULU SABİT DİSKLERİN ADLİ OLARAK İNCELENMESİ

Ahmet SALUK

FİZİKİ İNCELEMELER VE KRİMİNALİSTİK ANABİLİM DALI
YÜKSEK LİSANS TEZİ

DANIŞMAN
Yrd.Doç.Dr.Recep ERYİĞİT

ANKARA
2016

Ankara Üniversitesi
Sağlık Bilimleri Enstitüsü Müdürlüğü'ne,

Yüksek Lisans/Doktora tezi olarak hazırlayıp sunduğum "Windows 7 Ve 8 İşletim Sistemlerinde FaronicsDeepfreezeStandard Programı Kurululu Sabit Disklerin Adli Olarak İncelenmesi" başlıklı tez; bilimsel ahlak ve değerlere uygun olarak tarafımdan yazılmıştır. Tezimin fikir/hipotezi tümüyle tez danışmanım ve bana aittir. Tezde yer alan deneysel çalışma/araştırma tarafımdan yapılmış olup, tüm cümleler, yorumlar bana aittir.
Yukarıda belirtilen hususların doğruluğunu beyan ederim.

Öğrencinin Adı Soyadı: Ahmet SALUK
Tarih:
İmza:

Ankara Üniversitesi Sağlık Bilimleri Entitüsü

Disiplinlerarası Adli Bilimler Anabilim Dalı
Fiziki İncelemeler ve KriminalistikYüksek Lisans Programı
çerçevesinde yürütülmüş olan bu çalışma, aşağıdaki jüri tarafından
Yüsek Lisans Tezi olarak kabul edilmiştir.

Tez Savunma Tarihi:14.01.2016

Prof.Dr. Cemal AKAY
G.A.T.A
Jüri Başkanı

Prof.Dr. Aslıhan AVCI
Ankara Üniversitesi Tıp Fakültesi
Üye

Yrdc.Doç.Dr.Recep ERYİĞİT
Ankara Üniversitesi Mühendislik Fakültesi
Üye

Tez hakkında alınan Jüri kararı Ankara Üniversitesi Sağlık Bilimleri Enstitüsü Yönetim Kurulu Kararı tarafından onaylanmıştır.

Pfor.Dr.Zafer KARAER
Sağlık Bilimleri Enstitüsü Müdürü

İÇİNDEKİLER

Etik Beyan ii

Kabul ve Onay iii

İçindekiler iv

Önsöz vi

Simgeler ve Kısaltmalar viii

Şekiller ix

1. GİRİŞ 1

1.1 Bilgisayar 2

1.1.1 Donanım 2
1.1.2 İşletim Sistemi 3
1.1.3 Yazılım 3
1.1.4 Antiforensics Yazılımlar 4
1.1.4.1 Deepfreeze Standart Yazılımı 4
1.1.4.1.1 Genel Özellikleri 4
1.1.4.1.2 Kurulum Esasları 6
1.1.4.1.3 Kullanım Esasları 10
1.1.4.1.4 Temel Özellikleri 12

2. GEREÇ VE YÖNTEM 14

2.1 Denemelerde Kullanılan Programlar ve Dosyalar 14
2.2 İncelemelerde Kullanılan Programlar 14
2.2.1 EnCaseLawEnforcement(Versiyon 6.19.1) 14
2.2.2 X-WaysForensics (Versiyon 16.7) 15
2.3 İncelemelerin Yöntemi 15
2.3.1 www.facebook.com İnternet Sitesinde Oturum Açma Tespiti 15
2.3.2 www.twitter.com İnternet Sitesinde Oturum Açma Tespiti 17
2.3.3 Internet Explorer Tarayıcısı Üzerinden Adres Çubuğuna Yazılarak İnternet Adreslerine Erişimin Tespiti 18
2.3.4 Silinmiş Dosyaların Kurtarılması 19
2.4 Yapılan İşlemlerin Sırası 21
2.4.1. Windows 7 Üzerinde Yapılan İşlemler 21
2.4.2. Windows 8 Üzerinde Yapılan İşlemler 22
2.5 Ulaşılmaya Çalışılan Sonuçlar 23

3. BULGULAR 24

3.1 Deepfreeze Yazılımının Kurulu Bulunup Bulunmadığı Bilgisi 24
3.2 www.facebook.com İnternet Sitesi Üzerinde Oturum Açma Bilgisi 25
3.3 www.twitter.com İnternet Sitesi Üzerinde Oturum Açma Bilgisi 26
3.4. Erişilen İnternet Adreslerine Ait Kayıt Bulunup Bulunmadığı Bilgisi 27
3.5 Silinmiş Dosyaların Tespit Edilip Edilemeyeceği Bilgisi 27

4. TARTIŞMA 30

5. SONUÇ VE ÖNERİLER 31
ÖZET 33
SUMMARY 34
KAYNAKLAR 35
ÖZGEÇMİŞ 37

ÖNSÖZ

Geçmiş yıllarda suçlular ilkel ve basit yollarla suç işlerken günümüzde teknolojinin tüm imkânlarından faydalanmaları neticesinde suç çeşitleri değişmekte ve bilişim cihazları ile işlenen suçlar hızla artmaktadır. Bilgisayarların yoğun olarak suç işlemede kullanılması suç ve bilgisayar arasında ilişki kurmanın veya suçu çözmeye yardımcı materyallerin bulunması olayın çözülmesinde önem arz etmektedir. Kullanılan bilgisayar ile veri depolama birimleri adli olaylara konu olabilmektedir. Çoğu kullanıcı, şahsi verilerini istenmeyen kişilerin erişimini engellemek amacıyla çeşitli yollar ile temin edilebilecekleri yazılımlar kullanabilmektedirler. Bu tür yazılımları kullanan kişilere ait bilgisayar veya veri depolayıcıları adli olaylarda suça konu olabilmekte ve çeşitli yazılımlar kullanmak suretiyle, verilere adli inceleme uzmanlarının erişimini engellenmek istemektedirler. Bu nedenle incelemeler esnasında, suç konusu izleri ortadan kaldırıcı programların, veri depolama birimlerinde kurulu olup olmadıklarının belirlenmesi veya bu yazılımların bırakabilecekleri suç konusuna ait verilerin tespit edilerek içeriklerine erişilmesi gerekmektedir.

Bu tür yazılımlardan biri olan Faronics Deepfreeze Standard yazılımı kurulu bilgisayarlardan verilerin ortaya çıkartılması, olaylara ilk müdahale eden kişi, birimler ya da adli inceleme yapan uzmanların eğitim, bilgi ve tecrübelerine bağlıdır. İncelemeler esnasında Deepfrezee yazılımının bilgisayarlarda ya da veri depolama birimlerinde kurulu olup olmadıklarının belirlenmesi ve adli incelemeler açısından bırakabileceği izlerin belirlenmesi gerekmektedir. Olayların çözümünde adli inceleme uzmanları tarafından yapılan incelemeler neticesinde elde edebilecekleri sonuçların etkisi, son derece önemlidir.

Çalışmam esnasında sunduğu kapsamlı bilgi ve tecrübesinden yararlandığım ve çalışmam boyunca bana gösterdiği sevgi ve anlayış için Sayın Yrdc.Doç. Dr. Recep ERYİĞİT'e, , bize derslerimizde çok önemli katkılar sağlayan hocalarımız Sayın Prof. Dr. Aslıhan AVCI' ya, Sayın Prof. Dr. İ. Hamit HANCI' ya, Sayın Prof. Dr. Cemal AKAY'a, tüm değerli hocalarımıza,
Yıllardır maddi ve manevi desteğini hiçbir zaman esirgemeyen sevgili eşim Kamer SALUK"a

Ankara Üniversitesi Disiplinlerarası Adli Bilimler Enstitüsü'nün her aşamasında görev alan tüm personellerine, çalışmalarımda uygun ortam sağlayarak destek veren sıralı amirlerime, yol gösteren, zaman ayıran, her türlü desteği sağlayan ve yardımlarını esirgemeyen mesai arkadaşlarıma sonsuz saygı ve teşekkürlerimi sunarım.

Ahmet SALUK

SİMGELER VE KISALTMALAR

ID: kimlik

NTFS : Yeni Teknoloji Dosyalama Sistemi

MFT: Ntfs dosya sistemi içerisinde kullanılan dosyaya ait bilgilerin tutulduğu sistem dosyasıdır

ŞEKİLLER

Şekil 1.1. Bilişim 1

Şekil 1.2. Bilgisayarlar 2

Şekil 1.3. İşletim Sistemleri 3

Şekil 1.4. Yazılımlar 3

Şekil 1.5. Deepfreeze yazılımı çalışma mantığı 6

Şekil 1.6. Deepfreeze yazılımı kurulumu 6

Şekil 1.7 Deepfreeze yazılımı kurulumu 7

Şekil 1.8. Deepfreeze yazılımı kurulumu 7

Şekil 1.9. Deepfreeze yazılımı kurulumu 8

Şekil 1.10. Deepfreeze yazılımı kurulumu 8

Şekil 1.11. Deepfreeze yazılımı kurulumu 9

Şekil 1.12. Deepfreeze yazılımı kurulumu 9

Şekil 1.13.. Deepfreeze yazılımı şifre ekranı 10

Şekil 1.14. Deepfreeze Yazılımı Kullanımı 10

Şekil 1.15. Deepfreeze Yazılımı Kullanımı 11

Şekil 1.16. Deepfreeze Yazılımı Kullanımı 11

Şekil 1.7. Deepfreeze Yazılımı Kullanımı 12

Şekil 2.1. Facebook oturum açma sayfası 17

Şekil 2.2. Twitter oturum açma sayfası 17

Şekil 2.3. Adres çubuğuna internet adresi yazılarak erişilmesi 19

Şekil 2.4. Silinen Dosyalar 20

Şekil 3.1. Deepfreeze yazılımı kurulmuş bilgisayar ekranı 24

Şekil 3.2.www.facebook.com üzerinde oturum açma verileri 25

Şekil 3.3. www.twitter. üzerinde oturum açma verileri 26

Şekil 3.4. Adres çubuğuna yazılarak erişilen sitelerin tespiti 27

Şekil 3.5. Kurtarılan "doc" uzantılı dosyalar ve silinmeden önceki görünümü 28

Şekil 3.6. Kurtarılan "jpg" uzantılı resim dosyaları ve

silinmeden önceki görünümü 28
Şekil 3.7. Kurtarılan "pdf" uzantılı dosyalar ve
silinmeden önceki görünümü 28
Şekil 3.8.. Kurtarılan "mp3" uzantılı dosyalar ve
silinmeden önceki görünümü 29
Şekil 5. 1. EnCase 6.19 internet erişim kayıtları arama seçeneği 31

1-GİRİŞ

İçinde yaşadığımız yüzyıl, insanlık adına ortaya konan buluşlarla, teknolojik gelişmelerle sosyal hayatımızda baş döndürücü değişiklikler meydana getirmiştir. İnsanoğlu akıl, zeka ve muhakeme gibi özellikleri sayesinde, ihtiyaçları doğrultusunda değişik alet ve araçlar üretmiştir. Teknolojik gelişmeler içerisinde en önemlilerden biri olan bilgisayar sistemlerinin son yıllarda en hızlı gelişen ürünlerden olduğu görülmektedir. Bilişim ile bütünleşen bilgisayar sistemleri, gündelik yaşamın her alanında kullanılmakta ve kullanımı giderek yaygınlaşmaktadır(Ketizmen, 2008). Bilişim sistemleri hayatımızı kolaylaştırmakla birlikte günlük hayata dair birçok işlem yapılabilmektedir.

Şekil 1.1. Bilişim

Yaygın kullanılan bilgisayar sistemleri bazen suçlular tarafından kullanılmakta ve herhangi bir suça konu olabilmektedir. Suç işlemek için bilgisayar sisteminin kullananlar, işledikleri suçu gizlemek veya işledikleri suçun izlerini temizlemek

maksadıyla başka yazılım veya donanımlar kullanmış olabilirler. Suça konu olan bilişim sistemine ilk müdahale öncesinde araştırmasının yapılması ve ön bilgi sahibi olunması gerekmektedir. Müdahale edilmeden önce gerekli teknik bilgilere, bilgisayar, donanım ve yazılım bilgisine sahip olunması gerekmektedir.

1.1. Bilgisayar

Bilgisayar, girilen sayısal verileri işleyerek anlamlı bilgiler halinde bize sunan elektronik sistemdir. Bilgisayar çeşitli donanımlar ve bu donanımlar üzerine kurulu yazılımlar sayesinde çalışmaktadır. Bilgisayar denildiği zaman akılımıza üç bileşen gelmelidir; Donanım, işletim sistemi ve yazılım(Dinçel, 2008).

Şekil 1.2. Bilgisayarlar

1.1.1. Donanım

Donanım; bilgisayarların elektronik parçalarıdır. (sabit disk, ram, anakart, işlemci vs.) Adli incelemelere en fazla konu olan bilgisayar donanımı, sabit disklerdir. Sabit disk, üzerinde değişik boyutlarda veri depolama özelliği bulunan ve çeşitli yazılımlar sayesinde kullanılabilen veri depolayıcılardır.

1.1.2. İşletim Sistemi

İşletim sistemi; bilgisayar veya cep telefonu ile kullanıcı arasındaki ara yüzdür. (Windows XP, Windows Vista, Windows 7, Windows 8, Pardus, Ubuntu, Android, Mac OS, IOS) İşletim sistemi, sabit disk gibi çeşitli veri depolayıcıları üzerine kurulabilir. Bilgisayar donanımının çalışmasını sağlayan temel yazılımdır(TÜZEL, 2005)

Şekil 1.3. İşletim Sistemleri

1.1.3. Yazılım

Yazılımlar; Kullanıcıya çeşitli erişim kolaylığı sağlayan ve donanıma nasıl çalışması gerektiğini ya da donanımın yapacağı işlemleri komutlar halinde anlatan programlardır.

Şekil 1.4. Yazılımlar

1.1.4. Antiforensics Yazılımlar

Yazılımlar çok çeşitli amaçlara hizmet etmektedir. Bazı yazılımlar kullanıcının sabit disk üzerinde bıraktığı izleri ve dosyaları silmekte bazıları şifreleme özelliği ile kullanıcı harici, başkalarının erişimini engellemektedir. Antiforensics olarak tanımlanan yazılımlar; şifreleme, temizleme, üzerine veri yazarak temizleme istenilen bölümleri korumaya alma gibi çeşitli amaçlara yönelik hazırlanmıştır.

1.1.4.1. Deepfreeze Standard Yazılımı

1.1.4.1.1. Genel Özellikleri

Bilgisayar ağlarının hatta cihazların internet aracılığıyla birbirine bağlı olması nedeniyle, artık dijital sistemlerin birbirine zarar vermesi mümkün hale gelmiştir. Bilgisayar kullanıcıları, sistemlerinin zarar görmemesi ve bilgisayar hızının azalmaması için çeşitli yazılımlara ihtiyaç duymaktadırlar. Bu amaca yönelik olarak, bilgisayarda istenen bölümleri veya diskleri korumaya alan Faronics Deepfreeze yazılımı geliştirilmiştir. Yazılım ev kullanıcıları ve internet kafe işletenler için büyük kolaylıklar sağlamaktadır.

Deepfreeze yazılımı işletim sistemi üzerine kurulduktan sonra korumaya aldığı bölüm harici tüm işlemleri, Windows işletim sistemi önbelleğini kullanarak gerçekleştirmekte ve bilgisayar kapatıldıktan sonra verilere çoğunlukla silinmiş alanlardan erişilebilmektedir.

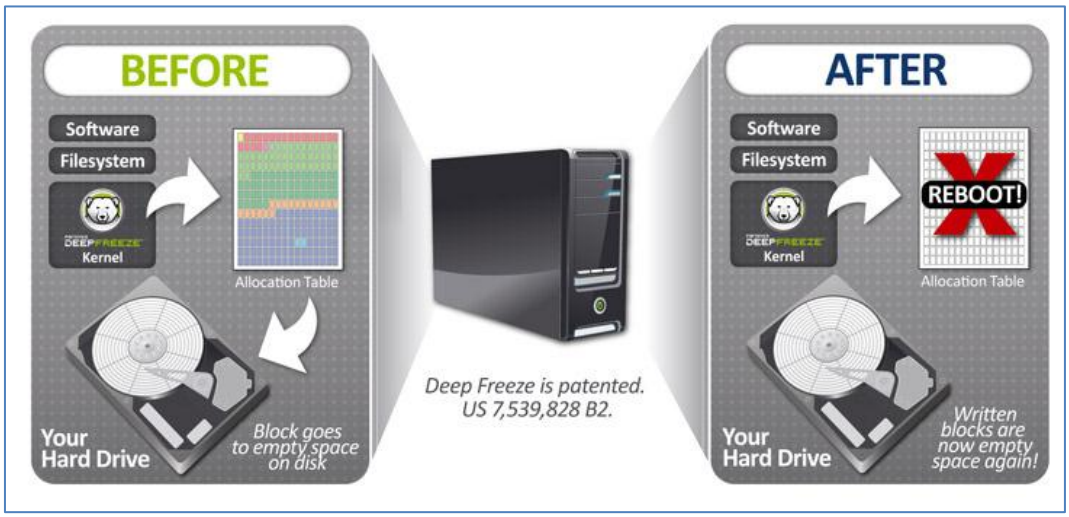
Faronics Deepfreeze, bilgisayarlara yazılımsal olarak zarar verilmesini engellemek amacıyla kullanılmaktadır. Deepfreeze kurulu bir bilgisayarda yaptığımız tüm değişiklerin (program yükleme-kaldırma, belge kaydetme, dosya silme, virüs(Kullanıcının izni ya da bilgisi dahilinde olmadan bilgisayarın çalışma

şeklini değiştiren ve kendini diğer dosyaların içerisinde gizlemeye çalışan bir tür bilgisayar programıdır.) bulaşması, duvar kağıdını değiştirme, vs.) etkili süresi sadece bilgisayarımızı kapatıp açma süresi kadardır. Bilgisayar her açıldığında deepfreeze'in ilk yüklendiği gibi olmaktadır.

Bilgisayarın mevcut yapılandırma ayarları ve belirlenen disk bölümündeki tüm dosyalar kaybolmadan ilk halini almaktadır. Bilgisayar her açılışta kendini orijinal ayarlarına dönmekte ve bu işlem için bekleme süresi gerekmemektedir. Bu sayede virüsden, kötü yazılımlardan, trojanlardan(Bilgisayar yazılımı bağlamında zararlı program barındıran veya yükleyen programdır. Truva atları masum kullanıcıya kullanışlı veya ilginç programlar gibi görünebilir ancak yürütüldüklerinde zararlıdırlar.), işletim sisteminin yavaşlaması ve yazılım düzensizliklerinden kaynaklı sorunlardan korumaktadır. Deepfreeze bilgisayarlara ait donanım ve yazılımların zarar görmemesi için zararlı yazılım (malware) tarama işleminde de kullanılabilmektedir (Sikorski, 2012).Deepfreeze yazılımı kullanımı esnasında herhangi bir kısıtlama olmaksızın bilgisayar üzerinde tüm işlemler yapılabilmektedir.

Deepfreeze yazılımı ev kullanıcıları ve internet kafe işletenler için sistem yapılandırmasının ve verilerin bozulmamasına ve sistemin korunmasına olanak tanımaktadır.

Deepfreeze yazılımı işletim sistemi üzerine kurulduktan sonra korumaya aldığı dosyalar harici tüm işlemleri mevcut alana yazılıyor gibi görülmekte ancak sistem çalışmadığı zaman veya elektrik kesildiğinde, söz konusu veriler mevcut alanlarda bulunmamaktadır. Şekil 1.5'de gösterilmiştir. Örneğin; Faronics Deepfreeze yazılımı ile korumaya alınmış bir disk bölümü üzerine dosya kopyaladığımızda dosya mevcut alanlarda gözükmektedir ancak bilgisayar kapandığında veya herhangi bir sebeple sistem üzerinde elektrik kesintisi olduğunda dosya silinmiş alanlarda bulunabilmektedir. Restart(bilgisayarın kapanıp-açılması) gerektirmeyen herhangi bir program yüklediğimizde program herhangi bir kısıtlama olmaksızın normal olarak çalışmaktadır ancak bilgisayar kapandığında veya herhangi bir sebeple sistem üzerinde elektrik kesintisi olduğunda Deepfreeze ilk yüklendiğindeki programları kullanılabilmektedir.

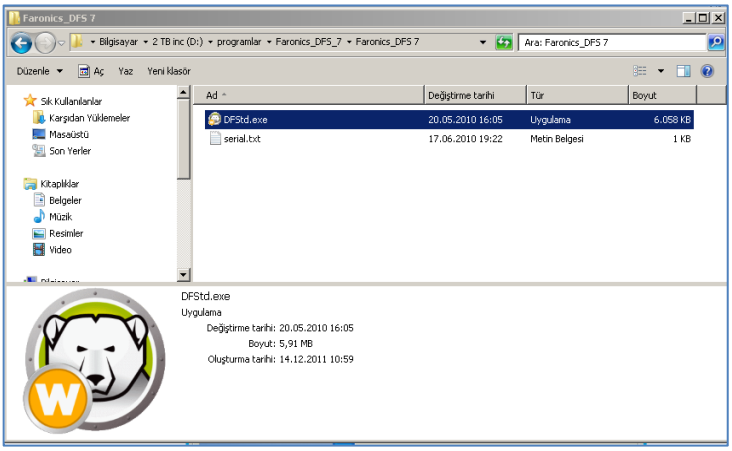


Şekil 1.5. Deepfreeze yazılımı çalışma mantığı(Deepfreeze, 2015)

1.1.4.1.2. Kurulum Esasları

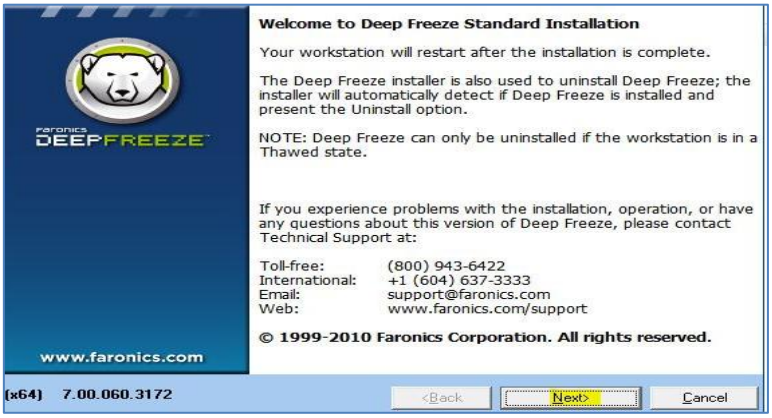
Çalışmamızın bu kısmında yazılımın kurulumu hakkında ayrıntılı bilgi verilecektir.

1.1.4.1.2.1.Öncelikle DFStd.exe isimli program dosyasına çift tıklanır. Şekil 1.6.'da gösterilmiştir



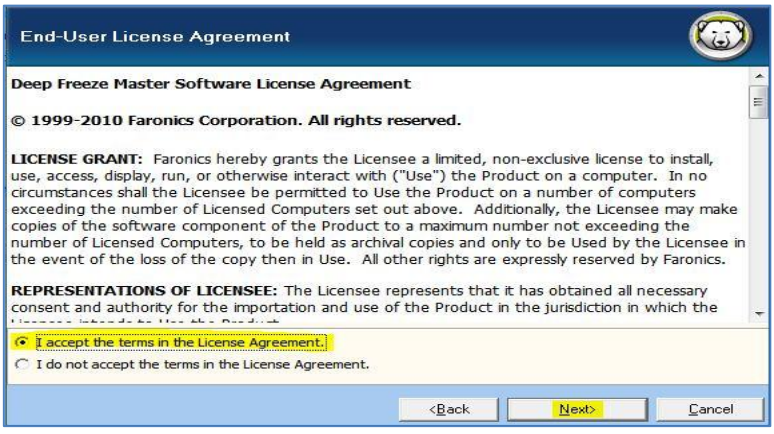
Şekil 1.6. Deepfreeze yazılımı kurulumu

1.1.4.1.2.2.Çıkan ekranda “Next” tıklanır. Şekil 1.7.’de gösterilmiştir



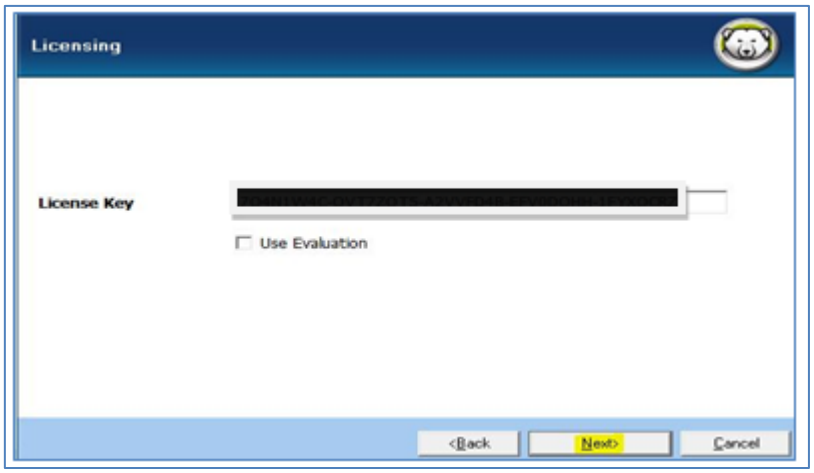
Şekil 1.7. Deepfreeze yazılımı kurulumu

1.1.4.1.2.3. Çıkan ekranda “I accept the terms in the License Agreement.” seçeneği işaretlenerek “Next” tıklanır. Şekil 1.8.’de gösterilmiştir



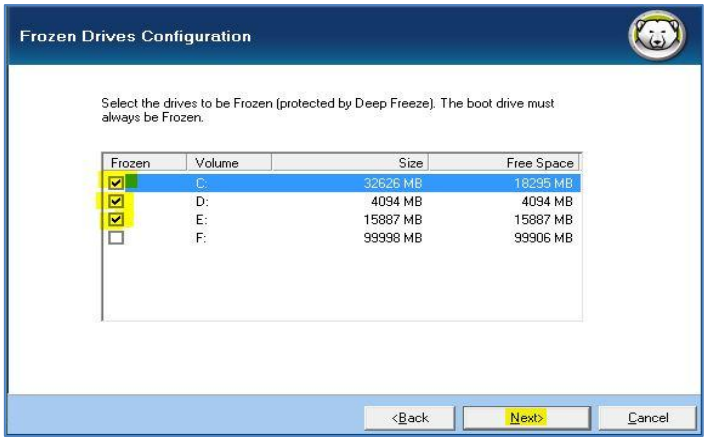
Şekil 1.8. Deepfreeze yazılımı kurulumu

1.1.4.1.2.4. Çıkan ekranda "LicenceKey." bilgileri girilerek "Next" tıklanır. "LicenceKey." bilgisi yok ise "Use Evaluation" seçeneği işaretlenerek "Next" tıklanır. Şekil 1.9.'da gösterilmiştir



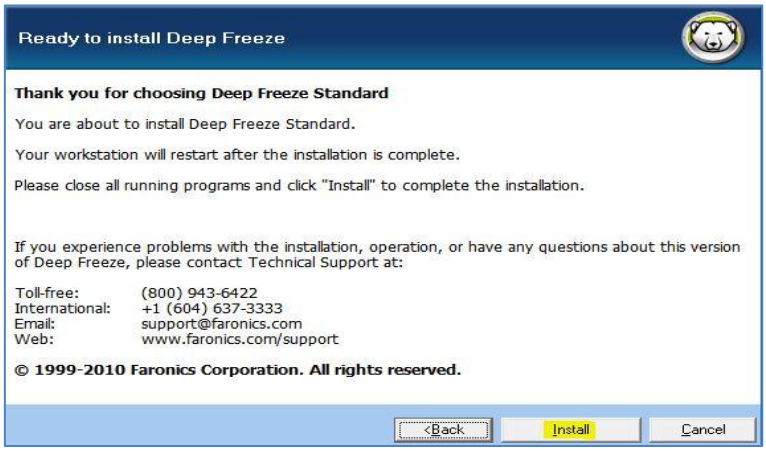
Şekil 1.9. Deepfreeze yazılımı kurulumu

1.1.4.1.2.5. Deepfreeze'in aktif olması istenen bölümler seçilerek "Next" tıklanır. Şekil 1.10.'da gösterilmiştir.



Şekil 1.10. Deepfreeze yazılımı kurulumu

1.1.4.1.2.6.“Install” tıklandığında program sistem üzerine kurulur ve bilgisayar kapanıp açılır. Şekil 1.11’de gösterilmiştir



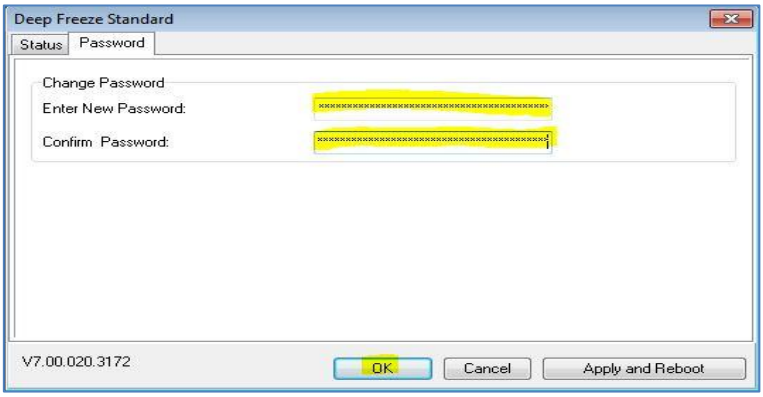
Şekil 1.11. Deepfreeze yazılımı kurulumu

1.1.4.1.2.7. Kurulum bittiğinde bilgisayar kapanıp açıldıktan sonra şifre ayarlama isteyip istemediği sorulur. “Yes” seçeneği seçilir. Şekil 1.12’de gösterilmiştir

Şekil 1.12. Deepfreeze yazılımı kurulumu

1.1.4.1.2.8. Şifre ayarlama ekranına şifremizi girerek doğrularız.(Şifre kısmına azami **41 karakter şifre** yazılabilir.) Şekil 1.13.’de gösterilmiştir. Şifre girmek zorunlu değildir. Şifre ekranı “NO ” seçeneği ile boş geçilebilir. Şifre girilirse unutulmaması

gerekir. Unutulursa sistem üzerinde değişiklik yapılamaz. Yeniden bilgisayarı formatlanması gerekir.

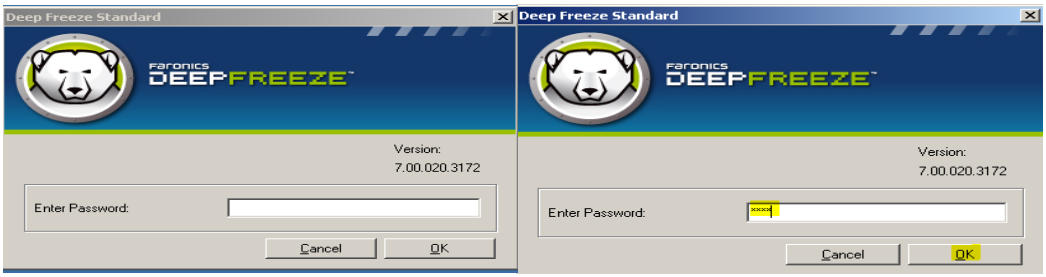


Şekil 1.13. Deepfreeze yazılımı şifre ekranı

1.1.4.1.3. Kullanım Esasları

Deepfreeze kurulu sistem üzerinde değişiklik yapmak istediğimiz zaman "sol Shift" basılı iken farenin (Mouse) sol tuşu ile görev çubuğunda bulunan tuşa çift tıklanır veya " Ctrl+Alt+Shift+F6" tuşlarına aynı anda bastığımızda şifre akranı açılır. Durum menüsündeki seçenekler ile değişiklikler yapılabilmesi için bilgisayarın kapanarak açılması gerekmektedir.

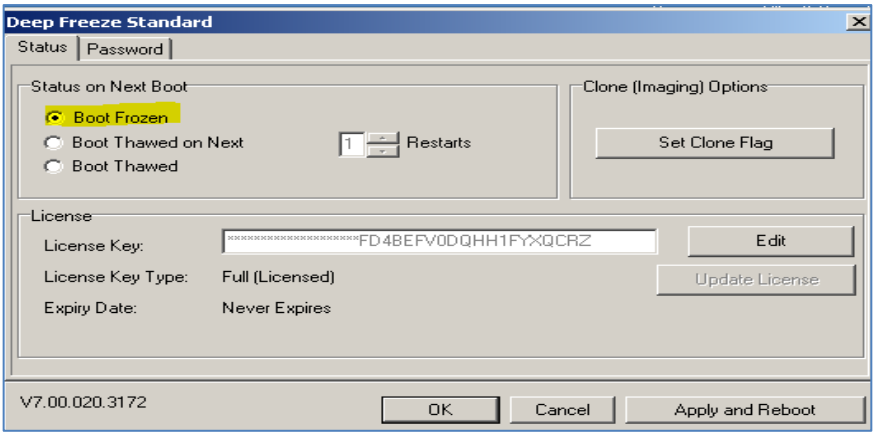
1.1.4.1.3.1.Şifre ekranına şifreyi girilir ve uygulaya ait durum menüsü açılır. Şekil 1.14.'de gösterilmiştir



Şekil 1.14. Deepfreeze Yazılımı Kullanımı

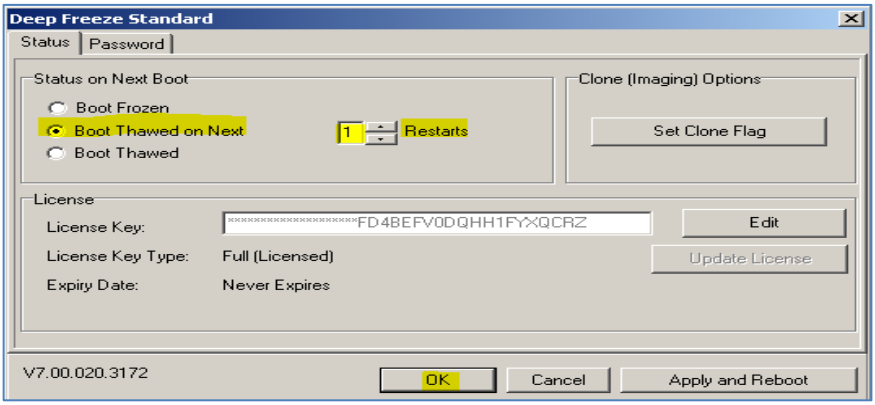
1.1.4.1.3.2. Programı Aktif/Pasif Etmek: Ayarlar menüsünde. "BootFrozen", "BootThawed On Next" ve "BootThawed" seçenekleri vardır.

1.1.4.1.3.2.1.BootFrozen : Sistemin korumada olduğu durumunu ifade eden normal çalışma modudur. Bu seçenek seçili olduğu zaman bir sonraki Windows açılışında program aktif olacaktır. Şekil 1.15'de gösterilmiştir.



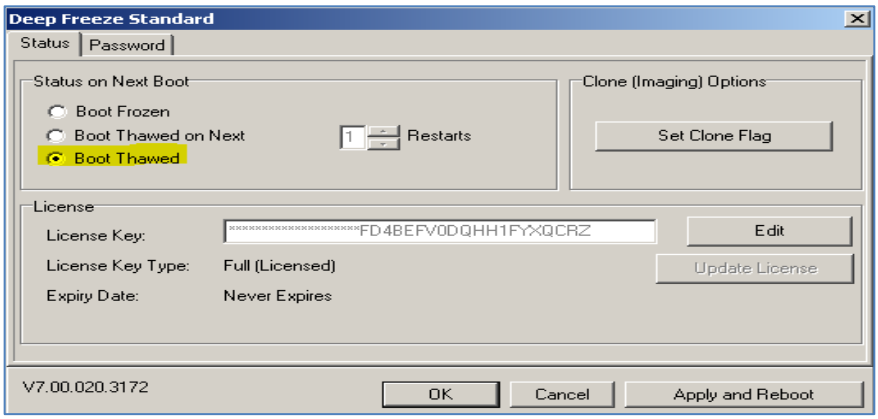
Şekil 1.15. Deepfreeze Yazılımı Kullanımı

1.1.4.1.3.2.2.BootThawed On Next : Bu seçeneği seçersek yandaki "Restarts" kutusu da aktif olur. "Restarts" kutusu içerisindeki sayı kadar bilgisayar açılıp kapandıktan sonra sistem tekrar korumaya alınacak (BootFrozen) konuma gelir. İlk kapatıp açmadan sonra istenen değişiklik sistem üzerinde yapılabilir. Bilgisayarın açılma ve kapanma işlemi kullanıcı tarafından yapılmaktadır. "Restarts" kutusuna en fazla "99" yazılabilmektedir. Şekil 1.16'da gösterilmiştir.



Şekil 1.16. Deepfreeze Yazılımı Kullanımı

1.1.4.1.3.2.3.BootThawed: Sistemin üzerinde deepfreeze uygulamasının pasif olduğu konumdur. Bu konumda da istenen değişiklikler yapılabilir. Durum menüsü açıldıktan sonra "BootThawed" seçeneği tıklanarak bilgisayar kapanıp açıldıktan sonra istenen değişiklikler yapılabilmektedir. Değişiklikler yapıldıktan sonra "BootFrozen" seçeneği ile sistem korumalı duruma getirilebilir. Şekil 1.17'de gösterilmiştir.



Şekil 1.17. Deepfreeze Yazılımı Kullanımı

1.1.4.1.4. Temel Özellikleri

- Bilgisayarın donanımları ve yazılımlarını virüslerden ve trojanlardan korur.
- Tüm programların kaydını tutar, yeniden başlatıldığında siler.
- Birden çok sabit diski ve sürücüyü destekler.
- SCSI(Sabit Disk, CD sürücü, tarayıcı, yazıcı gibi aygıtları paralel arabirim standartlarından daha uyumlu ve gelişmiş bir şekilde kontrol eden standarttır(SCSI 2015), ATA(Bilgisayar donanımı içerisinde bir veri taşıma teknolojisidir. Özellikle sabit diskten ya da sabit diske veri aktarımı işlevini yerine getirir(ATA, 2015), SATA(Bilgisayar donanımı içerisinde bir veri taşıma teknolojisidir. Özellikle sabit diskten ya da sabit diske veri aktarımı işlevini yerine getirir(SATA, 2015), ve IDE(Bilgisayar donanımı içerisinde

bir veri taşıma teknolojisidir. Özellikle sabit diskten ya da sabit diske veri aktarımı işlevini yerine getirir.) sabit disk desteği mevcuttur.

- Güvenli bir şifre koruması mevcuttur.
- Windows işletim sisteminin desteklediği disk bölümleri (FAT16, FAT32, NTFS) ile formatlanmış diskleri destekler.
- Bazı Mac işletim sistemlerinde de çalışır(Standard, 2013).
- 5 dile uyarlanmıştır. (İngilizce,Fransızca,Almanca,İspanyolca ve Japonca)

2.GEREÇ VE YÖNTEM

2.1. Denemelerde Kullanılan Programlar ve Dosyalar

- FaronicsDeepfreezeStandard (Versiyon 7.00.020.3172 - Windows 7 üzerinde kullanılan versiyon),
- FaronicsDeepfreezeStandard (Versiyon 8.10.060.4579 Windows 8 üzerinde kullanılan versiyon),
- VMware Workstation(Versiyon 9.0 - Sanal işletim sistemi çalıştırma programıdır.),
- Windows 7 Professional,64 bit,
- Windows 8 N 64 bit,
- Internet Explorer 8,
- Internet Explorer 10,
- (6) adet ".mp3" uzantılı dosya,
- (6) adet ".pdf" uzantılı dosya,
- (6) adet ".jpg" uzantılı dosya,
- (6) adet ".doc" uzantılı dosya denemelerde kullanılmıştır.

2.2. İncelemelerde Kullanılan Programlar

2.2.1.EnCase Law Enforcement(Versiyon 6.19.1)

Amerika' da kurulu bulunan Guidence Software firması tarafından geliştirilmiş çok maksatlı adli bilişim yazılımıdır. EnCase tarafından tespit edilen veriler dünyanın çeşitli mahkeme ve sistemlerinde kullanılmaktadır(EnCase, 2013). Yazılım ile veri depolama biriminde bulunan mevcut ve silinmiş tüm alanlar incelenebilmekte, bu alanlarda anahtar kelime araması, veri kurtarma, internet geçmişi, e-posta ve sohbet

kayıtları tespiti, şifreli dosya tespiti yapılabilmektedir. EnCase, birçok kolluk kuvveti ve bilgi güvenliği uzmanı tarafından kullanılan bir adli bilişim yazılımıdır(Mohay, 2003).

2.2.2. X-Ways Forensics (Versiyon 16.7)

Almanya' da kurulu bulunan X-Ways Software Technology AG Firmasının üretmiş olduğu bir yazılımdır(x-ways, 2014). EnCase yazılımı ile benzer özellikler taşımaktadır(SALUK, 2014). Veri depolama birimlerinde bulunan mevcut ve silinmiş tüm alanlar incelenebilmekte, bu alanlarda anahtar kelime araması, veri kurtarma, internet geçmişi, e-posta ve sohbet kayıtları tespiti, şifreli dosya tespiti yapılabilmektedir.

2.3. İncelemelerin Yöntemi

2.3.1. www.facebook.com İnternet Sitesinde Oturum Açma Tespiti

Harvard üniversitesi öğrencisi Mark Zuckerberg tarafından Amerika'da 4 Şubat 2004 tarihinde kurulan sosyal paylaşım sitesi Facebook'un bir milyar dan fazla üyesi vardır(Facebook, 2015). İnternet sitesi üyelik yöntemi ile çalışmaktadır. Siteye üye olunduktan sonra site üzerinde işlemler yapılabilmektedir. Üye olunmadan yapılan işlemler çok kısıtlıdır.

Sabit disk üzerinde Facebook sitesinde oturum açılıp açılmadığı adli bilişim incelemeleri açısından bilgisayarı kullananları tespit etmek için önemlidir. Oturum açıldıktan sonra resim-video yükleme, mesaj atma, sohbet yapma gibi birçok işlem yapıldığı ve suç işlemek amacıyla da kullanılabildiğinden dolayı oturum açma bilgisi önem arz etmektedir.

Sabit disk üzerinde facebook üzerinde oturum açma bilgisi tespit etmek için öncelikle bir e-posta hesabı bulunması veya facebook sitesinden üye olunması gerekmektedir. E-posta hesabı alındıktan sonra www.facebook.com adresine üye olunarak oturum açılması gerekmektedir. Her e-posta adresi ve kullanıcıya bir ID(kimlik) numarası atanmaktadır. Kullanıcı bundan sonraki işlemlerini ID numarası üzerinden yapmaktadır. Facebook şirketi sabit disk üzerinden çalışan uygulamasını değiştirdiğinde aratılacak anahtar kelimeler değişmekte ve yeni anahtar kelimeler oluşturulması gerekmektedir. Bu kapsamda her inceleme öncesi Facebook üzerinden yeniden oturum açılması ve oturum açıldığında ne gibi verilerin aranacağı önceden tespit edilmelidir.

Çalışmamızda "ahmetdenemedf@hotmail.com" e-posta hesabı kullanılmıştır. Şekil 2.1.'de gösterilmiştir. Facebook'da internet explorer üzerinden oturum açma bilgisi güncel olarak **"viewerid"** , "**viewer=**" , "**ahmetdenemedf**" ve ahmetdenemedf@hotmail.com kullanıcı adına atanmış facebook ID numarası olan "**100004962159111**" anahtar kelimeleri EnCase 6.19.1 adli bilişim yazılımı üzerinden aratılmış ve sonuçlar değerlendirilmiştir.

Şekil 2.1. Facebook oturum açma sayfası

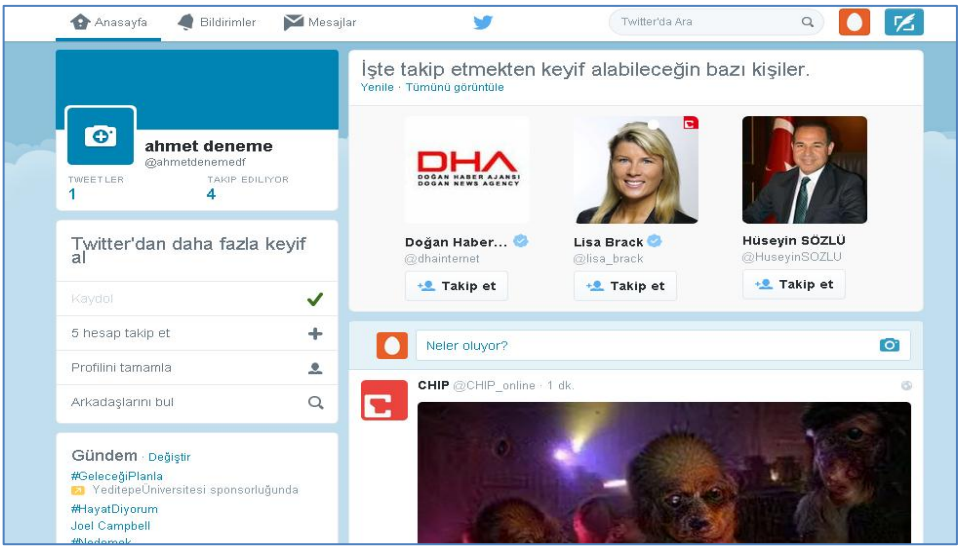
2.3.2. www.twitter.com İnternet Sitesinde Oturum Açma Tespiti

2006 yılında Jack Dorsey tarafından geliştirilen sosyal paylaşım sitesi twitter'ın 350 milyondan fazla üyesi vardır(Twitter, 2015). Facebook gibi arkadaşlık sistemi ile değil de takipçi sistemiyle çalışmaktadır. Site, üyelik yöntemi ile çalışmakta ve Siteye üye olunduktan sonra site üzerinde işlemler yapılabilmektedir. Üye olunmadan yapılan işlemler facebook gibi çok kısıtlıdır.

Oturum açılıp açılmadığı adli bilişim incelemeleri açısından bilgisayarı kullananları tespit etmek için önemlidir. Oturum açıldıktan sonra resim-video yükleme, mesaj atma, sohbet yapma gibi birçok işlem yapıldığı ve suçlular tarafından kullanılabildiğinden dolayı oturum açma bilgisi önem arz etmektedir.

Çalışmamız da "ahmetdenemedf@hotmail.com" e-posta hesabı kullanılmıştır. Şekil 2.2'de gösterilmiştir. Twitter'da internet explorer üzerinden oturum açma bilgisi güncel olarak "**data-user-id=**", "**data-user-screenname=**",

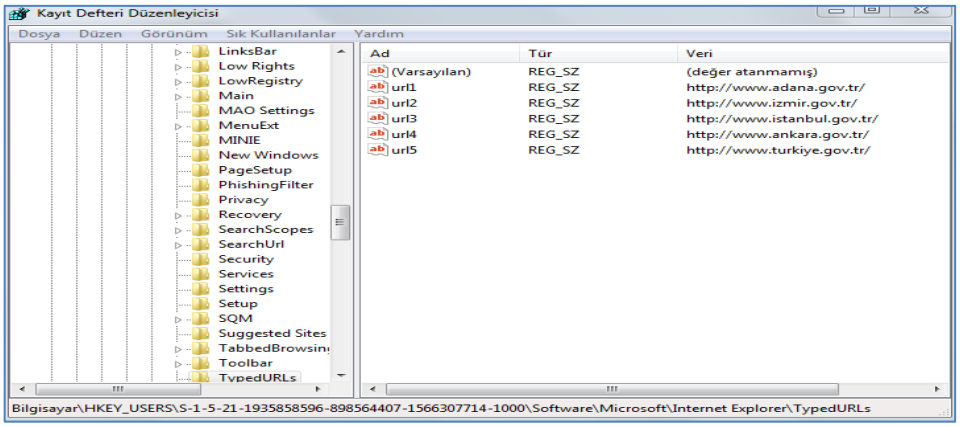
"**ahmetdenemedf**" ve ahmetdenemedf@hotmail.com kullanıcı adına atanmış Twitter ID numarası olan "**3062880227**" anahtar kelimeleri EnCase 6.19. adli bilişim yazılımı üzerinden aratılmış ve sonuçlar değerlendirilmiştir.



Şekil 2.2. Twitter oturum açma sayfası

2.3.3. Internet Explorer Tarayıcısı Üzerinden Adres Çubuğuna Yazılarak İnternet Adreslerine Erişimin Tespiti

Explorer tarayıcısı üzerinden adres çubuğuna yazılarak enter tuşuna basıldığında Windows registry'(kayıt defteri)nde "**HYKEY_USER\USER-SID\Software\Microsoft\Internet Explorer\TypedURLs**" yolunda işletim sistemi tarafından maksimum "**25**" adet kayıt tutulur(typedurls, 2015). Şekil 2.3.'de gösterilmiştir. Bahse konu kayıtlar, EnCase 6.19 adli bilişim yazılımı ile incelenmiştir.

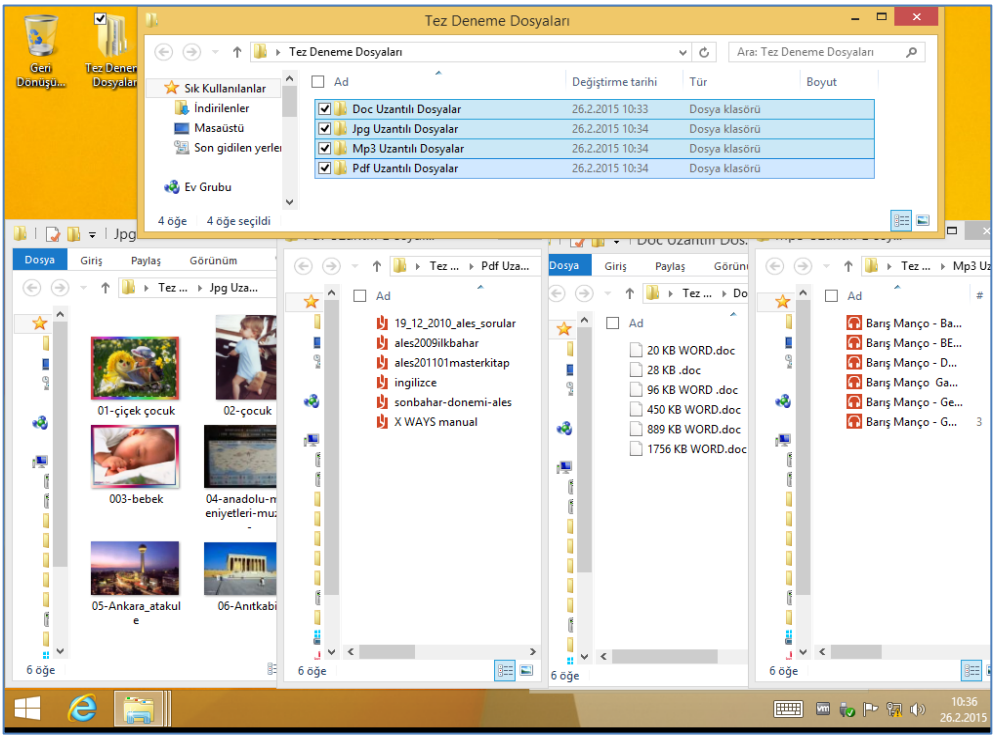


Şekil 2.3. Adres çubuğuna internet adresi yazılarak erişilmesi

2.3.4 .Silinmiş Dosyaların Kurtarılması

Ntfs(New tecnology file system-Windows işletim sisteminde kullanılan Yeni teknoloji dosyalama sistemidir.) Dosyalama sisteminde bir dosya oluşturulduğunda ilk olarak MFT(Master File Tablo) ve $LogFile(Windows işletim sistemi tarafından dosyaların günlüklerinin tutulduğu dosyadır(Logfile 2015)). dosyaları içerisinde kayıt tutulur ve $Bitmap(Windows işletim sistemi tarafından sektörlerin kullanılıp kullanılmadığının kaydını tutan dosyadır(Bitmap 2015).) ilgili dosyanın kullandığı alanları dolu olarak gösterir. Dosya normal yollarla "Delete" tuşu veya "Shift + Delete" tuşu ile silindiğinde dosya sadece silinmiş olarak işaretlenir ve Mft kaydı içerisinde 22 ve 23'üncü baytlarına yazılır(Sammes T ve Jenkinson B, 2007). Mft kaydı içerisinde 22 ve 23'üncü baytlarındaki veriler "00 00" ise silinmiş dosya, "01 00" ise mevcut dosya, "02 00" ise silinmiş dizin(klasör) ve "03 00" ise mevcut dizin anlamına gelmektedir. Dosyanın içerik bilgileri silinmez. İçerik bilgileri silinmediği için kurtarma yazılımları çoğunlukla dosyaları kurtarabilmektedir. Eğer dosyalama sisteminin olduğu bölüm formatlanmış, bozulmuş veya silinmiş ise farklı kurtarma metotları kullanılmaktadır.

Bu çalışmada masaüstüne (6) adet “.mp3” uzantılı dosya, (6) adet “.pdf” uzantılı dosya, (6) adet “.jpg” uzantılı dosya ve (6) adet “.doc” uzantılı dosya kopyalanmıştır. Bahse konu kopyalanan dosyaların tamamı klavyede bulunan shift+delete tuşlarına basılarak çöp kutusuna gönderilmeden doğrudan silinmiş ve bilgisayar kapatılmıştır. Şekil 2.4.’de gösterilmiştir. Silinen dosyaların kurtarılması için X-Ways16.7 yazılımı kullanılarak kurtarma işlemi yapılmış ve sonuçlar değerlendirilmiştir.



Şekil 2.4. Silinen Dosyalar

2.4. Yapılan İşlemlerin Sırası

Bütün işlemler, VMware Workstation programı üzerinde oluşturulan sanal işletim sistemlerinde yapılmıştır. Ayrıca doğrulama yapmak için sabit diskler üzerinde de aynı işlemler yapılmıştır.

2.4.1. Windows 7 Üzerinde Yapılan İşlemler

Sekiz adet Windows 7 Professionel 64 bit işletim sistemleri VMware Workstation sanal işletim sistemi programı üzerine yüklenmiştir. (4) adet Windows 7 Professionel 64 bit işletim sisteminden;

Bir adedinde, Internet Explorer 8 tarayıcısı üzerinden "**www.facebook.com"** sosyal paylaşım sitesi üzerinden "**ahmetdenemedf@hotmail.com**" kullanıcı ismiyle oturum açılmış, kapatılmış ve bilgisayar kapatılmıştır.

Bir adedinde, Internet Explorer 8 tarayıcısı üzerinden "**www.twitter.com**" sosyal paylaşım sitesi üzerinden "**ahmetdenemedf@hotmail.com**" kullanıcı ismiyle oturum açılmış, kapatılmış ve bilgisayar kapatılmıştır.

Bir adedinde Internet Explorer 8 tarayıcısı üzerinden "**www.turkiye.gov.tr, www.ankara.gov.tr, www.istanbul.gov.tr, www.izmir.gov.tr** ve **www.adana.gov.tr**" adresleri, adres çubuğuna yazılarak internet adreslerine erişim sağlanmıştır. İnternet tarayıcısı kapatılarak bilgisayar kapatılmıştır.

Bir adedinin masaüstüne (6) adet ".mp3" uzantılı dosya, (6) adet ".pdf" uzantılı dosya, (6) adet ".jpg" uzantılı dosya ve (6) adet ".doc" uzantılı dosya kopyalanmıştır.

Bahse konu kopyalanan dosyaların tamamı klavyede bulunan shift+delete tuşlarına basılarak çöp kutusuna gönderilmeden doğrudan silinmiş ve bilgisayar kapatılmıştır.

Diğer dört adet Windows 7 Professionel 64 bit işletim sistemi üzerine Faronics Deepfreeze Standard (Versiyon 7.00.020.3172) yazılımı yüklenmiştir. Bahse konu bu işletim sistemlerinde de yukarıda belirtilen aynı işlemler yapılmıştır.

2.4.2. Windows 8 Üzerinde Yapılan İşlemler

Sekiz adetWindows 8 N 64 bit işletim sistemleri VMware Workstation sanal işletim sistemi programı üzerine yüklenmiştir. (4) adet Windows 8 N 64 bit işletim sisteminden;

Bir adedinde Internet Explorer 10 tarayıcısı üzerinden "**www.facebook.com"** sosyal paylaşım sitesi üzerinden "**ahmetdenemedf@hotmail.com**" kullanıcı ismiyle oturum açılmış, kapatılmış ve bilgisayar kapatılmıştır.

Bir adedinde, Internet Explorer 10 tarayıcısı üzerinden "**www.twitter.com**" sosyal paylaşım sitesi üzerinden "**ahmetdenemedf@hotmail.com**" kullanıcı ismiyle oturum açılmış kapatılmış ve bilgisayar kapatılmıştır.

Bir adedinde, Internet Explorer 10 tarayıcısı üzerinden "**www.turkiye.gov.tr, www.ankara.gov.tr, www.istanbul.gov.tr, www.izmir.gov.tr** ve **www.adana.gov.tr**" adresleri, adres çubuğuna yazılarak internet adreslerine erişim sağlanmıştır. İnternet tarayıcısı kapatılarak bilgisayar kapatılmıştır.

Bir adedinin masaüstüne (6) adet ".mp3" uzantılı dosya, (6) adet ".pdf" uzantılı dosya, (6) adet ".jpg" uzantılı dosya ve (6) adet ".doc" uzantılı dosya kopyalanmıştır.

Bahse konu kopyalanan dosyaların tamamı klavyede bulunan shift+delete tuşlarına basılarak çöp kutusuna gönderilmeden doğrudan silinmiş ve bilgisayar kapatılmıştır.

Diğer (4) adet Windows 8 N 64 bit işletim bit işletim sitemi oluşturulmuş vebunlardan (4) adedi üzerine FaronicsDeepfreezeStandard (Versiyon 8.10.060.4579) yazılımı yüklenmiştir. Bahse konu bu işletim sistemlerinde de yukarıda belirtilen aynı işlemler yapılmıştır.

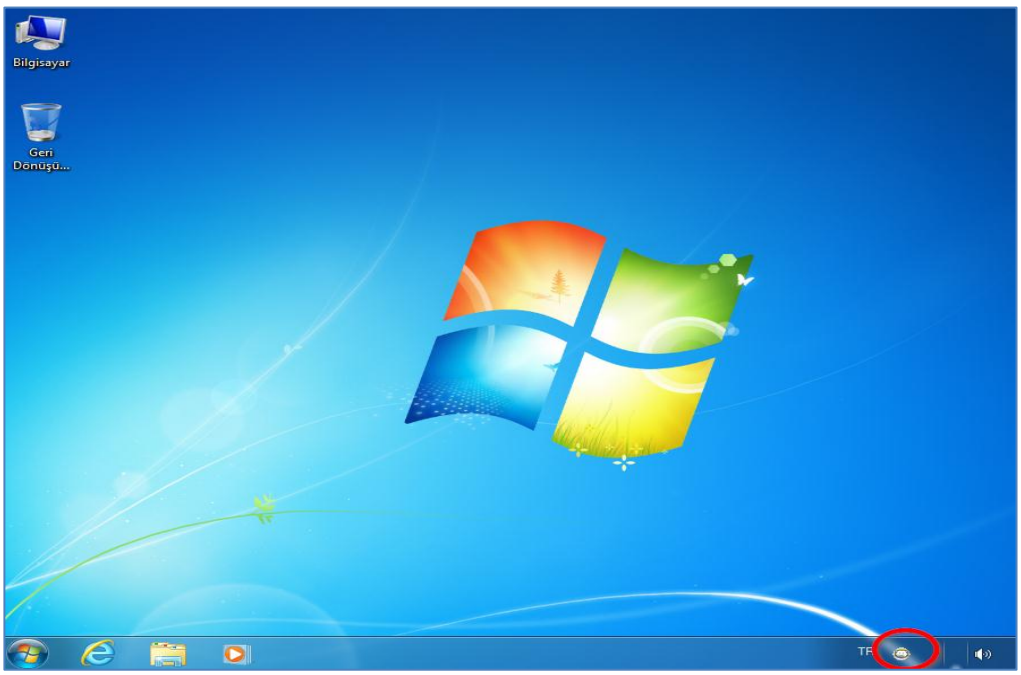
2.5. Ulaşılmaya Çalışılan Sonuçlar

- Deepfreeze yazılımının bilgisayarda kurulu bulunup bulunmadığı bilgisi,
- www.facebook.com internet sitesi üzerinde oturum açma bilgisi,
- www.twitter.com internet sitesi üzerinde oturum açma bilgisi,
- Adres çubuğuna yazılarak erişilen internet adreslerine ait kayıt bulunup bulunmayacağı bilgisi,
- Silinmiş dosyaların kurtarılıp kurtarılamayacağı bilgisi,
- Deepfreeze yazılımı yüklü olan sabit disk incelemesi ile yüklü olmayan sabit disk incelemesi arasındaki farklılıkların tespit edilmesine yönelik denemeler yapılmıştır.

3. BULGULAR

3.1. Deepfreeze Yazılımının Kurulu Bulunup Bulunmadığı Bilgisi

Deepfreeze kurulmuş bilgisayar ekranı Şekil 3.1'de gösterilmiştir. Yazılım ikonu(küçük resim) gizlenmemiş ise kutup ayısı şeklinde ikon olarak görev çubuğu üzerine görüntülenmektedir.



Şekil 3.1. Deepfreeze yazılımı kurulmuş bilgisayar ekranı

Deepfreeze yazılımının bilgisayarda kurulu olup olmadığına yönelik olarak; masa üstünde simgesinin olup olmadığına bakılır ve Windows 7 için "C:\Program Files (x86)\Faronics\DeepFreeze" dosyasının olup olmadığı, Windows 8 için

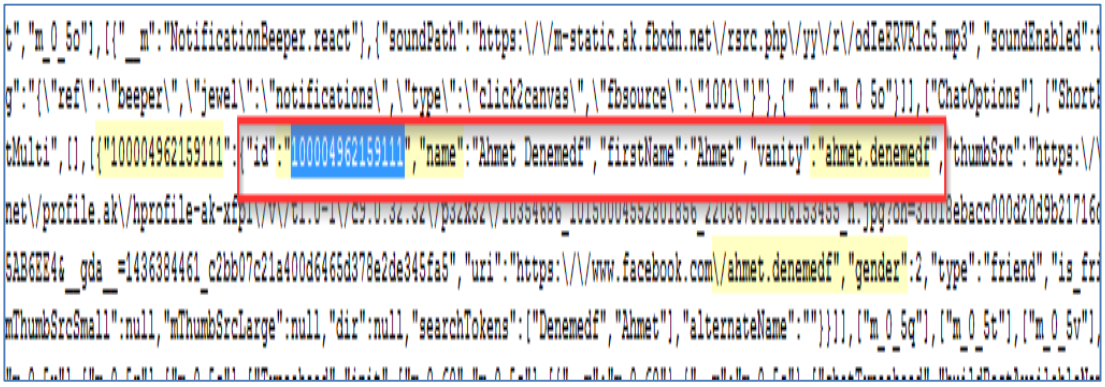
"C:\Program Files (x86)\Faronics\DeepFreeze" dosyasının olup olmadığı kontrol edilir.

Yazılımının bilgisayarda kurulu bulunup bulunmadığı öncelikli olarak olaya ilk müdahale eden birimler tarafından araştırılmalıdır.

3.2. www.facebook.com İnternet Sitesi Üzerinde Oturum Açma Bilgisi

Internet Explorer 8 ve 10 üzerinden "www.facebook.com" sitesinde oturum açıldığında oturum açma bilgisinin tespit edilebilmek için **navAccountName** (Facebook oturum açma verisi), **headerTinymanName**(Facebook oturum açma verisi), **"viewerid**(Facebook oturum açma güncel verisi) "**viewer=**(Facebook oturum açma güncel verisi) , "**ahmetdenemedf**" ve ahmetdenemedf@hotmail.com kullanıcı adına atanmış facebook ID numarası olan "**100004962159111**" numarası anahtar kelimesi aratılmıştır. Anahtar kelime aratılması sonucunda;

Deepfreeze yazılımı yüklü olan ve olmayan Windows 7 ve 8 Professionel işletim sistemleri üzerinde ahmetdenemedf@hotmail.com kullanıcı adına atanmış facebook ID numarası olan "**100004962159111**" numarası ve facebook ID numarasının kime ait olduğu bilgisi(Şekil 3.2) sabit diskin **silinmiş alanlarından** tespit edilmiş olup bahse konu sabit disk üzerinde facebook üzerinden oturum açıldığı tespit edilmiştir.

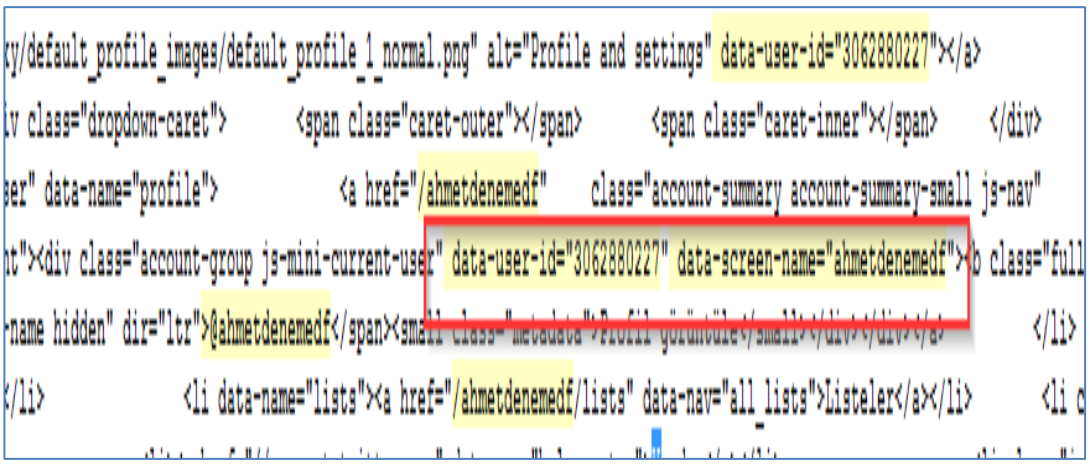


Şekil 3.2 www.facebook.com internet adresi üzerinde oturum açma verileri

3.3 www.twitter.com internet sitesi üzerinde oturum açma bilgisi

Internet Explorer 8 ve 10 üzerinden "www.twitter.com" sitesinde oturum açıldığında oturum açma bilgisinin tespit edilebilmek için **data-screen-name=** (Twitter'da oturum açan kullanıcı ID numarasını vermektedir.**)** ve **data-user-id=** (Twitter'da oturum açan kullanıcı ID numarasını vermektedir.), **viewerid**(Twitter'da oturum açan kullanıcı ID numarasını vermektedir.) ve ahmetdenemedf@hotmail.com kullanıcı adına atanmış "**@ahmetdenemedf**" kullanıcı adı Twitter ID numarası olan "**3062880227**" anahtar kelimeleri aratılmıştır

Deepfreeze yazılımı yüklü olan ve olmayan Windows 7 ve 8 Professionel işletim sistemleri üzerinde ahmetdenemedf@hotmail.com kullanıcı adına atanmış "**@ahmetdenemedf**" kullanıcı adı Twitter ID numarası olan "**3062880227**" kullanıcının oturum açma bilgisi sabit diskin **silinmiş alanlarından** tespit edilmiş olup bahse konu sabit disk üzerinde twitter üzerinden oturum açıldığı tespit edilmiştir. Şekil 3.3. 'de gösterilmiştir.



Şekil 3.3.www.twitter.com internet adresi üzerinde oturum açma verileri

3.4. Erişilen internet adreslerine ait kayıt bulunup bulunmadığı bilgisi

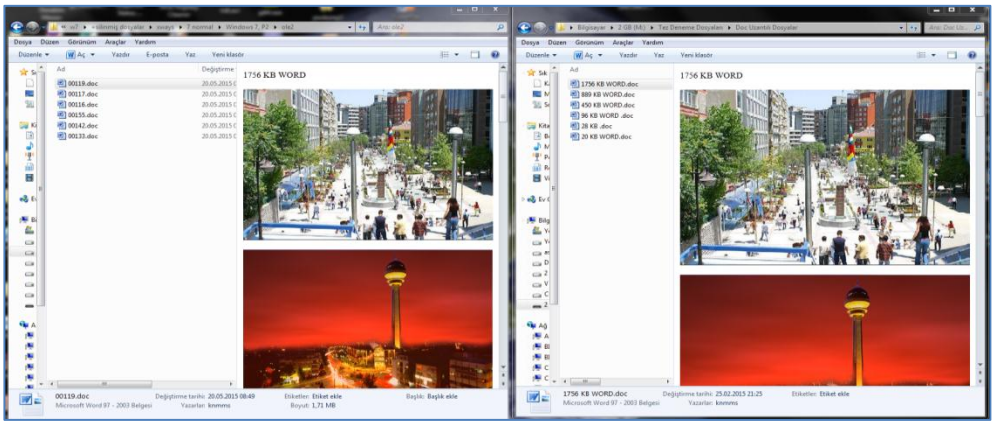
Deepfreeze yazılımı yüklü olmayan Windows 7 ve 8 işletim sistemlerinde registry(Windows işletim sistemlerinde bulunan kayıt defteri) dosyalarından "typed URL" adresleri mevcut alanlarda tespit edilmiştir. Şekil 3.4'de gösterilmiştir.

Şekil 3.4 Adres çubuğuna yazılarak internet sitesine erişilen sitelerin tespiti

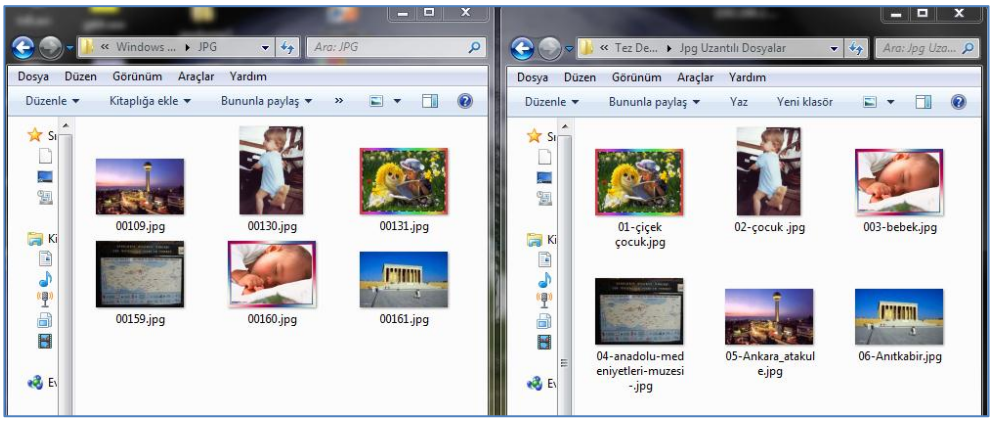
Deepfreeze yazılımı yüklü Windows 7 ve 8 işletim sistemlerinde bahse konu adresler silinmiş alanlardan tespit ediliştir. İnceleme esnasında, EnCase 6.19 adli bilişim yazılımı kullanılmıştır.

3.5 Silinmiş Dosyaların Tespit Edilip Edilemeyeceği Bilgisi

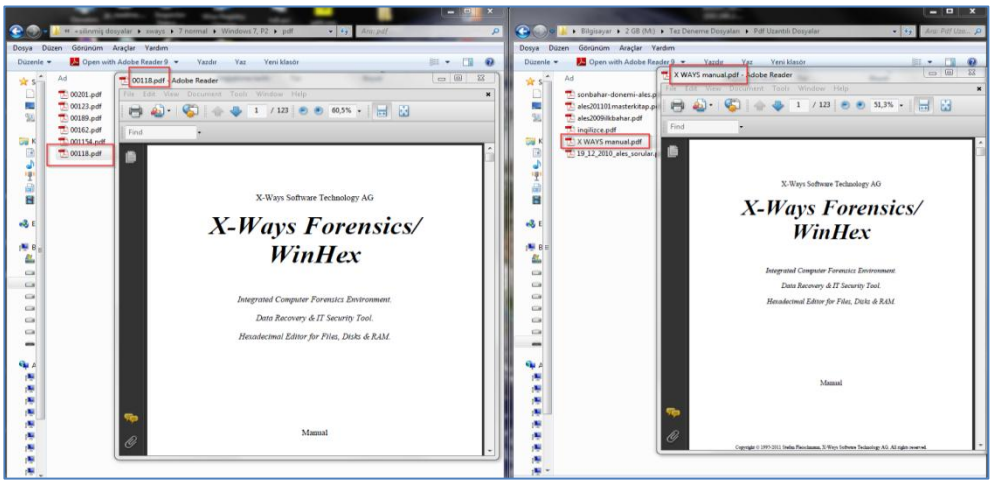
Deepfreeze yazılımı yüklü olan ve olmayan Windows 7 ve 8 Professionel işletim sistemleri üzerinde silinen dosyaları kurtarma işlemi yapıldığında dosyaların kurtarılabildiği tespit edilmiştir. Şekil 3.5, Şekil 3.6, Şekil 3.7 ve Şekil 3.8'de gösterilmiştir.



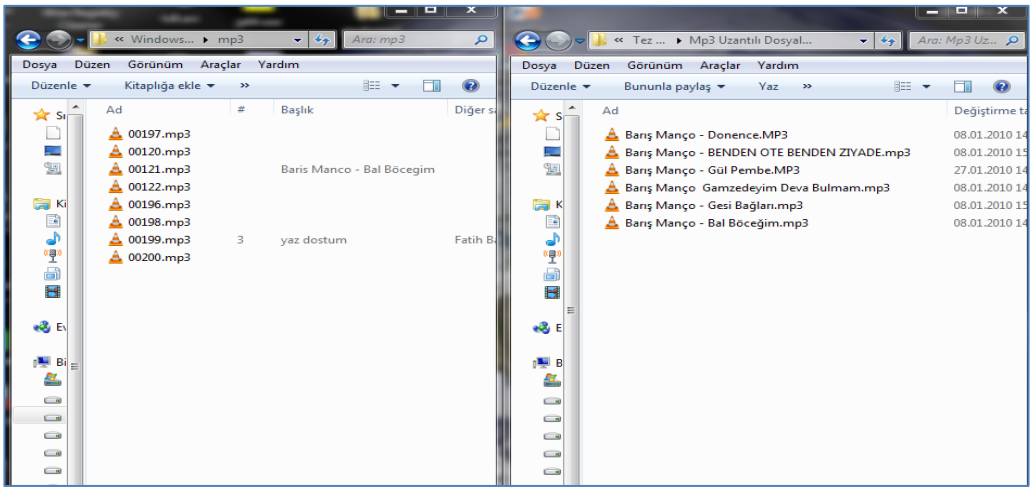
Şekil 3.5. Kurtarılan "doc" uzantılı dosyalar ve silinmeden önceki görünümü



Şekil 3.6. Kurtarılan "jpg" uzantılı resim dosyaları ve silinmeden önceki görünümü



Şekil 3.7. Kurtarılan "pdf" uzantılı dosyalar ve silinmeden önceki görünümü



Şekil 3.8. Kurtarılan "mp3" uzantılı dosyalar ve silinmeden önceki görünümü

Silinen dosyaların kurtarılması için X-Ways16.7 yazılımı kullanılmıştır.

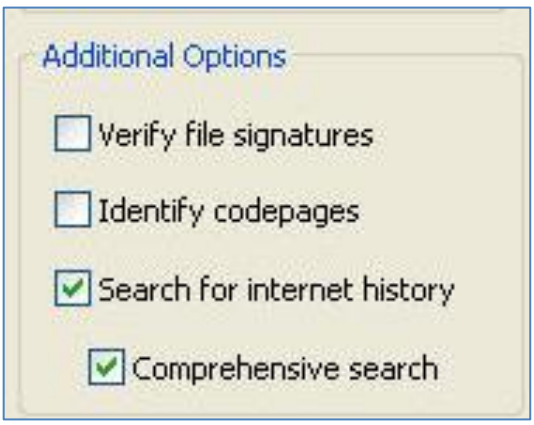
4. TARTIŞMA

- Bu çalışmada Windows 7 ve 8 İşletim Sistemlerinde Faronics Deepfreeze Standard yazılımı kurulu sabit disklerin adli olarak incelenmesi için yapılabilecek uygulamalar ve bu uygulamaların sonuçları ele alınmıştır.
- www.facebook.com isimli internet sitesi üzerinde oturum açma bilgisi içeren veriler silinmiş alanlar içerisinden tespit edilmiştir.
- www.Twitter.com isimli internet sitesi üzerinde oturum açma bilgisi içeren veriler silinmiş alanlar içerisinden tespit edilmiştir.
- Erişilen internet adreslerine ait kayıtların tamamı "silinmiş alanlar" içerisinden tespit edilmiştir. Deepfreeze yazılımı kurulu olmayan disklerde mevcut alanlarda bulunduğu görülmüştür.
- **"NTFS"** dosya sistemi ile formatlanmış(Veri depolama birimini, işletim sisteminin kullanımına hazır hale getirmek) bölümlerde dosyaların kurtarılabildiği tespit edilmiştir.
- Bilinenin aksine Faronics Deepfreeze Standard yazılı yüklü bilgisayarlar üzerinde verilerin ve dosyaların kurtarılabildiği tespit edilmiştir.

5. SONUÇ VE ÖNERİLER

- Olay yerinden delilleri toplayan personel, bilişim sitemleri konusunda yeterli bilgiye sahip olmalı delilleri yok edebilecek yazılımlara karşı dikkatli davranmalıdır.

- İncelemeye alınan sabit disklerden, silinmiş internet erişim kayıtları isteniyor ise; EnCase Law Enforcement Versiyon 6.19.1'da "Search" seçeneğinden "Comprehensive Search"(EnCase Law Enforcement 6.19.1 programı üzerinde "search" menüsünde "Search for internet history" seçeneği altında bulunan "kapsamlı arama" özelliğidir.) " seçeneği mutlaka seçilmelidir. Şekil 5.1.' de gösterilmiştir.



Şekil 5.1. EnCase 6.19 internet erişim kayıtları arama seçeneği.

- Sosyal paylaşım(facebook ve twitter) sitelerinin izleri araştırılırken doğrulama yapılarak geçmiş ve güncel verilere göre analiz yapılmalıdır.

- İstenen verilerin elde edilebilmesi; **bilgisayarın ne kadar yoğun kullanıldığına** ve **kullanılan disk içeriğinde daha önce veri bulunup bulunmadığına** bağlı olarak değişmektedir. İstenen verilerin üzerine veri yazılmış, veriler silinmiş veya temizlenmiş olabilmektedir.

- Antiforensics yazılım olarak bilinen Faronics Deepfreeze Standard yazılıımı yüklü bilgisayarların incelemesinde; bilgisayar kapatıp açıldıktan sonra işlem yapılan dosyaların ve verilerin tamamen yok olmadığı sonucuna varılmıştır. İncelemeler esnasında; Faronics Deepfreeze Standard yazılımı yüklü bilgisayarda "herhangi bir şey çıkmaz" düşüncesinin yanlış olduğu tespit edilmiş olup incelemelerin daha kapsamlı yapılması gerektiği sonucuna varılmıştır.

- Tespiti istenen veriler sabit diskin "Mevcut Alanlarında" bulunması ile "Silinmiş Alanlarda" bulunmasının farklı anlamlar ifade etmesi, Deepfreeze yüklendikten sonra korumaya alınan bölümlerde yapılan işlemler neticesinde tespit edilen veriler ve dosyaların silinmiş alanlarda bulunabilmesi, Deepfreeze yüklenmemiş bilgisayarlarda tespit edilebilen ancak deepfreeze programı yüklenmesi neticesinde tespit edilemeyen verilere erişebilmesi maksadıyla; Deepfreeze yazılımı yüklendiği tespit edilen sabit disklere el konulması esnasında bilgisayarların **birebir kopyasının(imajının) bilgisayar açıkken alınmasının** uygun olacağı değerlendirilmektedir.

ÖZET

Windows 7 ve 8 İşletim Sistemlerinde Faronics Deepfreeze Programı Kurulu Sabit Disklerin Adli Olarak İncelenmesi

Bu çalışmada, bu alanda var olan kaynak eksikliğini gidermek amacı ile Deepfreeze Standard yazılımının özellikleri ve adli bilişim uygulamalarında erişilebilecek sonuçlarla ilgili çeşitli bilgiler verilmeye çalışılmıştır.

Bu çalışma içinde, Windows İşletim Sistemlerinde Faronics Deepfreeze yazılımı kurulu yüklü sabit disklerde internet erişim kayıtları, facebook oturum açma , twitter oturum açma ve silinmiş dosyaların tespit edilmesi için yapılabilecek uygulamalar ve bu uygulamaların sonuçları ele alınmıştır.

Yapılan uygulamalarda erişilen internet adreslerine ait kayıtların tamamının "silinmiş adreslenmemiş alanlar" içerisinden tespit edildiği ve daha önce işlem yapılarak bilgisayarın kapatılması sonucu mevcut alanlarda bulunmayan dosyaların kurtarılabildiği tespit edilmiştir.

Yaygın olarak Antiforensics yazılım olarak bilinen Deepfreeze yazılımı yüklü sabit disklerin incelenmesi esnasında; "Deepfreeze yüklü ise herhangi bir şey tespit edilemez" düşüncesinin yanlış olduğu, doğru olmadığı tespit edilmiş ve ayrıntılı inceleme neticesinde birçok veriye erişilebildiği sonucuna varılmıştır

Anahtar Sözcükler : Adli Bilişim, Adreslenmemiş Alanlar, Deepfreeze, İnternet Geçmişi ve Veri Kurtarma

SUMMARY

Forensic Examinations Of Faronics Deepfreeze Programs On The Windows 7 And 8 Operation Systems

In this study, it is given some of knowledges including features of the DeepFreeze Software Standardandt here sult of its Computer Forensics examinations in order to contribute to existing sources in this field.

Within this workout, the application that can analyse deleted data, facebook login, twitter login and internet history from a Windows computer having intalled Faronics Deepfreeze software and the findings of those software are tried to be researched.

Within the tests, internet history logs can be found in the unallocated areas and deleted data that has been deleted because of shut down also be recovered.

Commonly Deepfreeze software is known as an antiforensics tool that mosty in computer forensics experts think no data can be recovered from a Deepfreeze installed system but this workout showed those thoughts are totally wrong and lots of important data can be gathered from unallocated areas.

Keywords: Computer forensics, data recovery, Deepfreeze, internet history and Unallocated Clusters

KAYNAKLAR

DİNÇEL T. 2008, DİNÇEL T, *BİLGİSAYAR ÖGRENİYORUM*, 2008, PUSULA YAYINCILIK2008:1

KETİZMEN, 2008, KETİZMEN M, Türk Ceza Hukukunda BİLİŞİM SUÇLARI, ADALET YAYINEVİ, 2008:18

MOHAY G.M. 2003. Computer and Intrusion Forensics, 2003:67

SALUK A, BAKAN M. 2014,ÇAKIR, H, ADLİ BİLİŞİM VE ELEKTRONİK DELİLLER,SEÇKİN YAYINCILIK

SAMMES T, ve JENKİNSON B. Forensic Computing, 2007 SpringerScience+Business Media.2007:390

SIKORSKI, M. 2012**.** Honig A, PracticalMalware Analysis, No StarchPressInc, 2012:467

TÜZEL Ş, ÇÖMLEKÇİ M, *Pc Donanımı*, ALFA YAYINCILIK,1. Baskı 2005:7

ATA 2015. Erişim Adresi:[http://tr.wikipedia.org/wiki/ATA] Erişim Tarihi:26/01/2015

Bitmap 2015 . Erişim Adressi:[http://www.forensicfocus.com/hidden-data-analysis-ntfs] Erişim Tarihi : 25.12.2015

Deepfreeze, 2015. Erişim Adresi:[http://www.faronics.com/en-uk/products/deep-freeze] Erişim Tarihi:11/05/2014

Deepfreeze Erişim Adresi:[http://en.wikipedia.org/wiki/Deep_Freeze_(software) Erişim Tarihi:02/05/2012

EnCase, 2013. Erişim Adresi:[en.wikipedia.org/wiki/EnCase].Erişim Tarihi:10/12/2014.

Facebook, 2015.Erişim Adresi:[https://tr.wikipedia.org/wiki/Facebook]. Erişim Tarihi:10/08/2015.

Logfile2015. Erişim Adresi:[http://www.forensicswiki.org/wiki/Logfile_Analysis] Erişim Tarihi : 25.12.2015

SATA 2015. Erişim Adresi:[http://tr.wikipedia.org/wiki/SATA] Erişim Tarihi:27/01/2015

SCSI 2015. Erişim Adresi:[http://tr.wikipedia.org/wiki/SCSI] Erişim Tarihi:25/01/2015

Standard, 2013. Erişim Adresi:[http://www.atmcomputer.com/asp/product/31301/Faronics-Deep-Freeze-Standard] Erişim Tarihi:25/02/2013

Twitter, 2015. Erişim Adresi:[https://tr.wikipedia.org/wiki/Facebook] Erişim Tarihi:10/06/2015

Typedurls, 2015. Erişim Adresi:[http://forensicartifacts.com/ 2010/08/typedurls]. Erişim Tarihi:01/08/2015.

x-ways, 2014. Erişim Adresi:[www. x-ways.net/corporate/contact.html] Erişim Tarihi:06/01/2014

ÖZGEÇMİŞ

1-Bireysel Bilgiler

Adı	: Ahmet
Soyadı	: SALUK
Doğum yeri ve tarihi	: KESKİN – 20.12.1982
Uyruğu	: Türkiye Cumhuriyeti
Medeni durumu	: Evli
İletişim adresi ve telefonu	: Jandarma Kriminal Daire Başkanlığı Beytepe-ÇANKAYA/ ANKARA İş Tel:0312 4647289 Cep Tel: 0531 797 1971

II- Eğitim

2014 – Ankara Üniversitesi Disiplinlerarası Adli Bilimler Enstitüsü, Fiziki İncelemeler ve Kriminalistik Yüksek Lisans
2002 – 2012 Eskişehir Anadolu Üniversitesi İktisat Fakültesi
2000 - 2001 Jandarma Astsubay Okulu
1996 - 2000 Anadolu İletişim Meslek Lisesi

Yabancı Dili : İngilizce

Yabancı Dil Puan ve Türü : KPDS – 63

III – Ünvanlar

- İzmir İl Jandarma-Ödemiş İlçe Jandarma Komutanlığı-Ovakent Jandarma Karakol K.lığı-Önleme Müdahale Unsur Komutanı
- Şırnak-Beytüşşebep-Mezraa 6.Jandarma Komando Tabur Komutanlığı-Komando Tim K.Yrdc.lığı
- Afyonkarahisar İl Jandarma Komutanlığı Olay Yeri İnceleme Tim Komutanlığı
- Jandarma Kriminal Daire Başkanlığı Bilişim Teknolojileri İnceleme Şube

Müdürlüğü- Veri ve Donanım İnceleme Uzmanlığı

IV – Mesleki Deneyim

- Jandarma Kriminal Daire Başkanlığı Bilişim Teknolojileri İnceleme Şube Müdürlüğü- Veri ve Donanım İnceleme Uzmanlığı
- Afyonkarahisar İl Jandarma Komutanlığı Olay Yeri İnceleme Tim Komutanlığı

V-Üye Olduğu Bilimsel Kuruluşlar

Yoktur.

VI- Bilimsel İlgi Alanları

- Kitap-Adli Bilişim ve Elektronik Deliller Kitabı- 5. Bölüm Yazarı-Seçkin Yayıncılık 2014-Ankara
- Sunum-Microsoft Office Word 2010 Yazılımı İle Oluşturulan Belgelerde Üst Veri (Metadata) Analizi –ISDF (International Symposium on DigitalForensicsand Security) Uluslararası Adli Bilişim ve Güvenlik Sempozyumu-11.05.2015
- Makale-Microsoft Office Word 2010 Yazılımı İle Oluşturulan Belgelerde Üst Veri (Metadata) Analizi - Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:1, No:2, S:20-26, 2015

VII- Bilimsel Etkinlikleri

- Seminer-Hash Değerleri Konulu-Ankara Üniversitesi Disiplinlerarası Adli Bilimler Entitüsü Sunum Salonu 17.11.2014
- Sabit Disk Onarımı ve Veri Kurtarma Kursu- **ÇİN-CHENGDU-SALVATİONDATA FİRMASI**(14-18.04.2014)

VIII- Diğer Bilgiler

- Olay Yeri İnceleme Temel Kursu Jandarma Okullar Komutanlığı(18.04.2005 – 27.05.2005)
- VII. Adli Bilimler Kongresi (11-14.05.2006)
- TCK&CMK Semineri Afyonkarahisar PMYOM (10-11.03. 2007)
- Jandarma Adli Bilimler Semineri JKDB-(11-12.04.2007)
- 6. AB Uluslararası Adli ve Polis İşbirliği Kursu Denizli EGM (31.03.2008-03.04.2008)
- Jandarma Kriminal Semineri JKDB-(15-17.04.2009)
- Temel Eğitim Katılım Sertifikası (13.09.2010-08.10.2010)
- TS EN ISO/IEC Temel Eğitimi ve AKREDİTASYON Eğitimi(14 – 15.09.2010)
- Mert Teknoloji – Cep Telefonu Tamir Kursu (01-18.022011)
- Gazi Üniversitesi-Endüstriyel Elektronik Kursu(10.01.2011-03.04.2011)
- TADOC – Veri Madenciliği (21-25.05.2012)
- TADOC – Windows Vista ve Windows 7 Adli İncelemeleri (18-22.06.2012)
- Linux Sistem Yönetimine Giriş(12-23.11.2012)
- Beyaz Şapkalı Hackher(07-11.12.2012)
- Veri Kurtarma Eğitimi (24-28.12.2012)
- 2.Uluslararası Adli Bilim Kurumları Birliği Kongresi(23-26.10.2013)
- Bilişim Hukuku Ve Adli Bilişim Sertifika Programı (07.-11.09.2015)
- I-2 Bilgisayar Destekli Suç ve Suçlu Analiz Programı Kursu(12-23.10.2015)