GİZLİ TANIK GARSON
(SD KART-ADLİ BİLİŞİM KAPSAMINDA ANALİZ-SONUÇ DEĞERLENDİRME)

İçindekiler

ADLİ BİLİŞİM TANIMLARI

Adli Bilişim Nedir ?

Adli bilişim, elektronik ortamlardan elde edilen bulguların, çeşitli teknik donanım ve yazılımlar kullanılarak hukuki delillere dönüştürülme süreci olarak tanımlanabilir. (*Kabaca şüpheliye ait bilgisayarın içerisinde bulunan hard diskin içerisinde yer alan tüm verinin başka bir hard diske aktarılması.)* Bu yönüyle adli bilişimin hukuki boyutundan ziyade, teknik yönü ön plana çıkmaktadır. Zira, elektronik sistemlerdeki bulguların, bunlardan ayrıştırılarak birer hukuki delile dönüştürülme süreci, oldukça zahmetli, son derece teknik bilgi gerektiren ve uzmanlık isteyen bir iştir. Yapılan işlemlerde gerek uygulanan yöntem gerekse kullanılacak ekipmanların uluslararası alan geçerliliği kabul edilmiş araç, gereç ve yazılımlarla yapılması elzemdir. Söz konusu dijital materyallerin hassas olduğu, içerisinde yer alan verilerin yanlış müdahale sonucu donanımsal arıza nedeni ile zarar görme ihtimalleri mevcut olduğundan titizlikle ve önceden belirlenmiş standart müdahale yöntemleri ile işlemlere başlanır. Bil hassa dijital materyalin adli kopyasının (imajının alınması) alınması öncesinde ve işlem bitene kadar video kaydı yapılması şeffaflık unsuru açısından elzem olmakla birlikte hali hazırda kolluk birimleri tarafından benimsenmiş bir davranış haline gelmiştir. Aynı zamanda yapılan imaj alma işlemi 2 (iki) kopya şeklinde olup, bir kopyası şüpheliye veya vekiline verilmek suretiyle, verilerin güvenirliliği objektif olarak sağlanmış olmaktadır.

Kanuni Dayanak

CMK 134

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma

(1) Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.

(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.

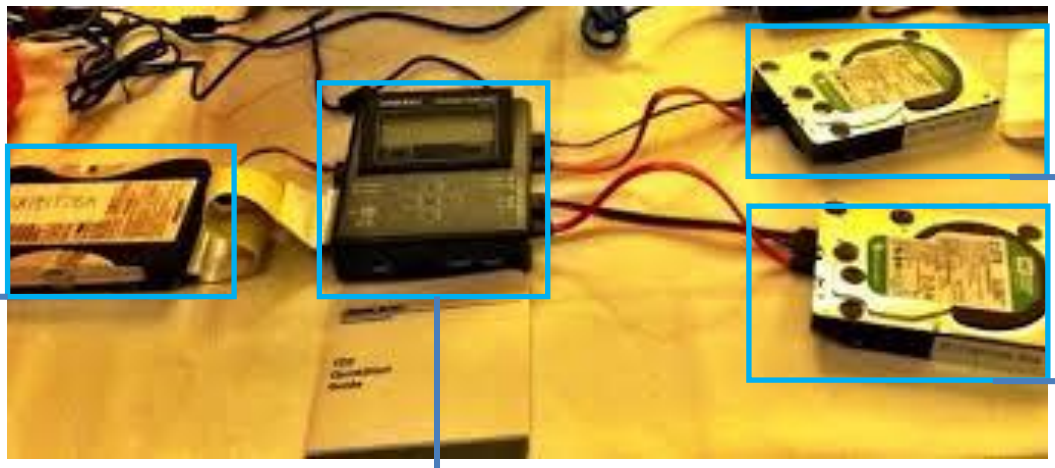
(3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.

(4) İstemesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

(5) Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır.

Adli Bilişim İşlem Süreçleri

- **Dijital Delile İlk Müdahale** (Materyal tespiti ve uygulanacak işlemlerde kullanılacak ekipmanların hazırlanması, canlı imaj alma ya da offline imaj alma işlemlerinin seçiminin yapılmasına bağlı olarak donanımsal müdahale)
- **Muhafaza altına alma** (Dijital materyalin olay yerinde, anti statik bileklik kullanmak suretiyle her türlü etkenden korumak, güvenlik bantlı ve köpüklü ambalajlar içerisine yerleştirilmesi gibi işlemlerin uygulanması)
- **İmaj alınması** (Adli kopya olarak da adlandırılan işlemde, uygun donanımlar kullanılarak, şüpheli ve ya vekili ya da hazurun nezaretinde, materyalin birebir aynı verilerden oluşan dijital klonunun oluşturulması)
- **İnceleme** (Dijital materyalin alınan kopyasını barındıran ve imaj dosyası olarak adlandırılan dosyalar açılmak suretiyle, verilere erişim sağlamak ve bu veriler üzerinde uluslararası geçerliliğe sahip lisanslı programlar marifetiyle inceleme yapılması)
- **Analiz** (Dijital verilerin incelenmesi esnasında, her türlü manipülasyon ihtimallerinin değerlendirilip, soruşturmaya ve şüpheliye olumsuz etki edebilecek yanlışlıkların tespit edilmesi, şifreli verilerin tespiti halinde şifrelerinin kırılması, silinmiş verilerin geri getirilmesi, zararlı yazılım tespiti gibi bir çok aşamadan geçilerek soruşturma dosyası kapsamında tespit edilen verilerin raporlanmak üzere hazırlanması)
- **Raporlama** (İnceleme ve analiz işlemleri tamamlanan materyale ait raporun, adli makamlara sunulmak üzere; Teknik detaylar içeren ve işlem süreçlerinin en başından en sonuna kadar anlatıldığı, yapılan tespitlerin ne anlama geldiği, hangi konumda olduğu, dijital imzaları, tarih ve zaman bilgileri, veriyi oluşturan, son erişen ve değiştiren kullanıcıların kim yada kimler olduğu, verinin yer aldığı işletim sisteminin ve sürüm, tarih gibi bilgiler, veriler üzerinde manipülasyon olup olmadığı gibi bilgilerin yer adlığı inceleme raporu)

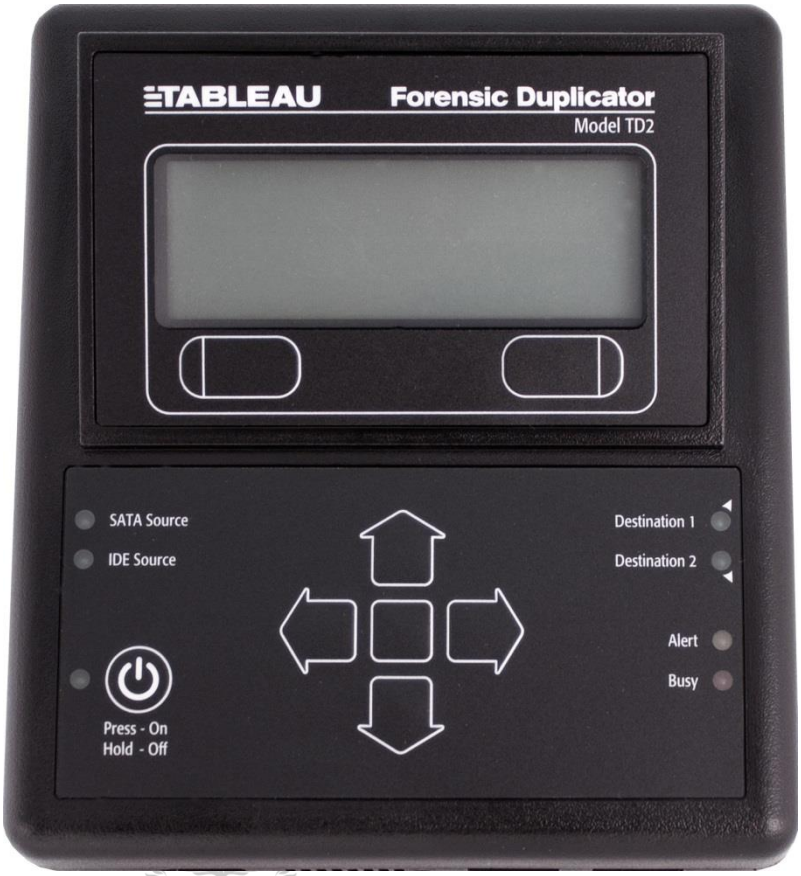


Şüpheliye ait Harddisk

Tableu marka imaj alma kiti (donanım)-imaj alma(adli kopya) işlemini gerçekleştiren cihaz

Kolluğa ait adli kopya

Şüpheli veya vekiline verilecek adli kopya



Yukarıda yer verilen resimde görüleceği üzere; Tableu marka TD2 Model imaj alma cihazı marifetiyle sol tarafta cihazın source (kaynak) bölümünde, imajı alınacak harddisk takılır, sağ tarafta destination(hedef) bölümünde, imajın aktarılacağı hard diskler takılır. Cihaz üzerinde yer alan ekranda, cihazın tarih ve saat bilgileri, imaj alma yöntemi (disk to imaj veya disk to disk), imaj alma işleminde kullanılacak format (E01 veya Raw), imajı alınacak materyale ait bilgiler yine cihaz üzerinde bulunan seçim ve yön tuşları ile görüntülenebilmekte ve değiştirilebilmektedir. Cihazın ön tarafında bulunan usb bağlantı noktalarından birine klavye bağlamak sureti ile soruşturma numarası, şüpheli bilgileri vb. bilgiler kolaylıkla yazılabilmektedir. İşlem tamamlandığında adli kopyaların olduğu harddisklerin içerisinde, imaj dosyaları ve bir de log denilen text dosyası bulunmaktadır. Bu log dosyasında, imajı alınan harddiskin marka, model, seri numarası bilgileri, imaj alma yöntemi ve formatı bilgileri, imajı alan kişi tarafından girilmiş ise soruşturma ve şüpheli bilgileri, imaj alma esnasında karşılaşılan hatalar var ise bunlara ait bilgiler, imaj dosyalarının isimleri numaralandırılmış şekilde yer almaktadır. Bu bilgiler içerisinde en önemli husus ise; İmajı alınan harddiske ait hash değeri bilgisidir. Hash değerine kısaca dijital imzada denilmektedir. Bu imza, imajı alınan harddisk içerisinde yer alan verilere özgü olarak cihaz tarafından belirli bir algoritmaya göre oluşturulan sayısal değerlerdir. Şöyle ki bu sayısal değerler tek yönlü bir algoritmik fonksiyondur.

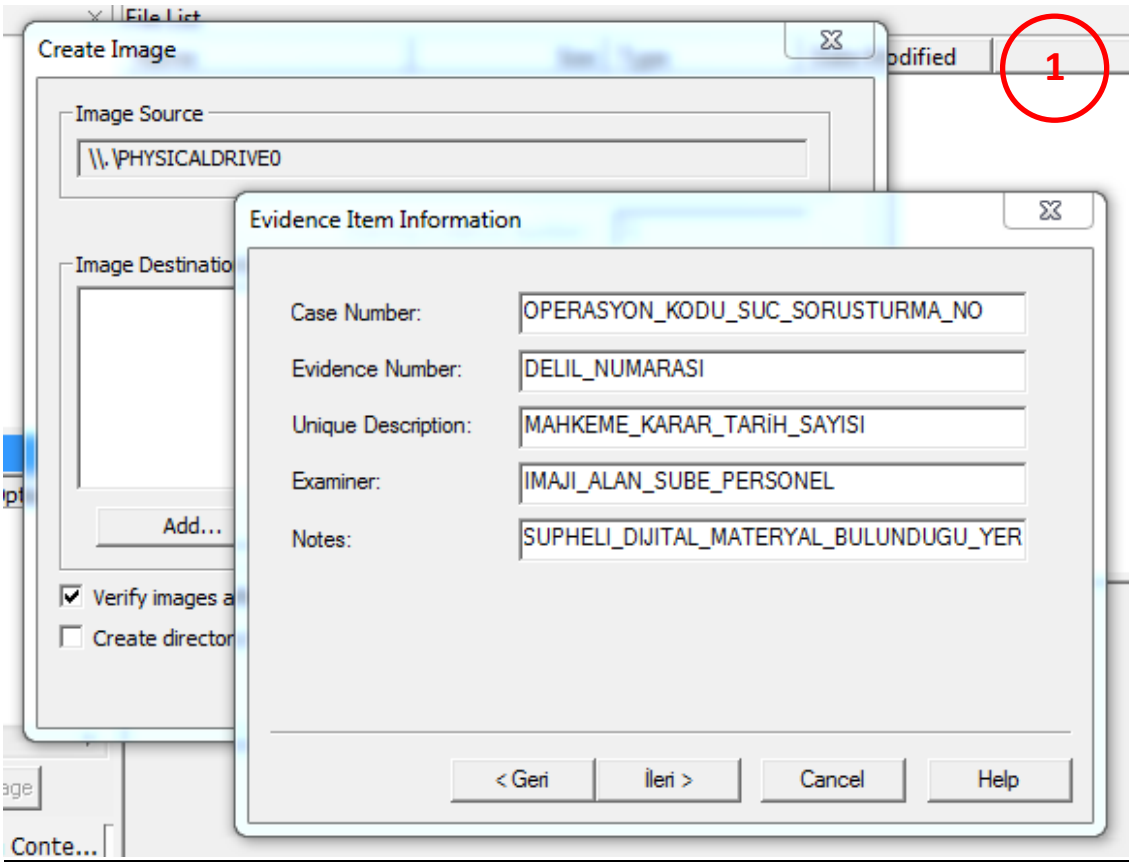
Kamera kaydı ile imaj alma işlemi tamamlandıktan sonra; Bir kopyası (yani bir hard disk) şüpheli veya vekiline verilir. Diğer kopyası ise incelenmek üzere kolluk görevlilerince alınır. Ancak hard diskler güvenlik bantlı ve içerisinde köpük olan dijital delil muhafaza poşetine koyulur. Tüm bu işlemler kolluk görevlilerince tutanak altına alınır. Arama-el koyma tutanağından farklı olarak "imaj alma tutanağı" isimli bir şablon tutanak doldurulur. Bu tutanakta soruşturma bilgileri, karar numaraları, şüpheli bilgileri, dijital materyale ait marka, model, seri numarası, imajın aktarıldığı hard disklere ait marka, model, seri numarası bilgileri, imaj alma işlemine başlanıldığı ve işlemin bittiği tarih, saat bilgisi, imaj alma işlemine ait hash (dijital imza) değeri, imajı alan kolluk görevlisinin isim, soy isim veya sicil bilgisi ile imzası, adli kopyayı teslim alan şüpheli veya vekilinin isim, soy isim ve imzası gibi bilgiler yer alır.

Görüleceği üzere yapılan işlemlerin objektif, şeffaf ve veri güvenliğini esas alan şekilde gerçekleşmesi için izlenmesi gereken adımlar, hem kolluk kuvvetlerinin hem adli makamların hem de şüpheli

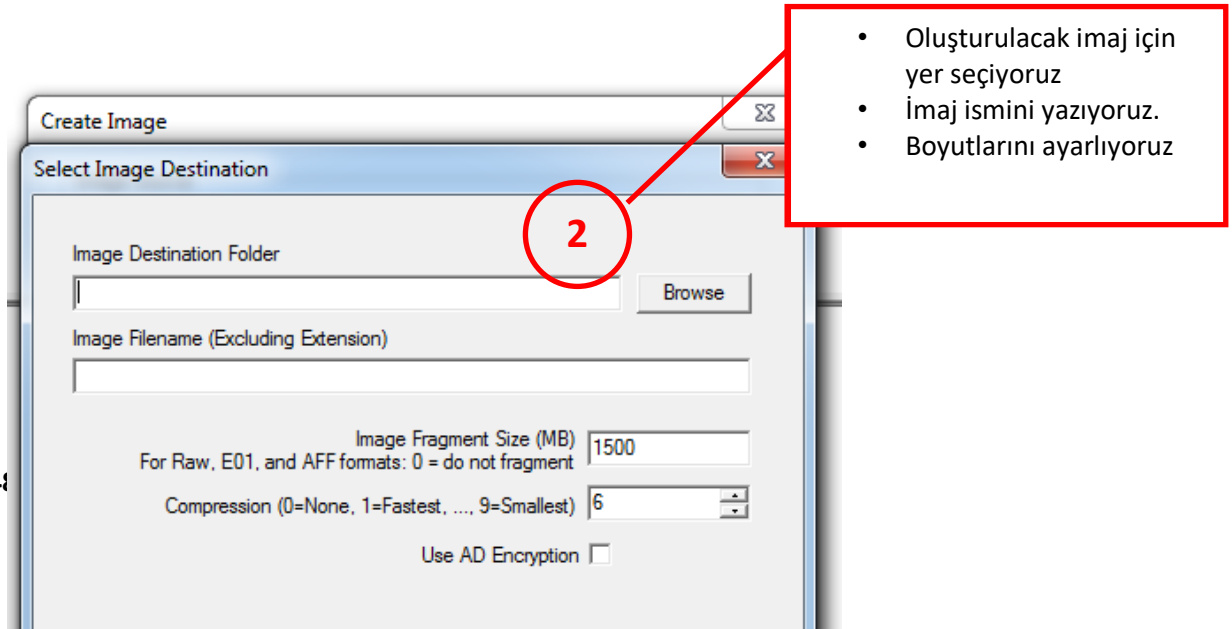
açısından güvenilirlik sağlamaktadır. **Ancak bu işlemlerin bir veya bir kaçının ihlal edilmesi şüpheye mahal vermektedir. Zira söz konusu dijital materyaller olunca yakın geçmişte ortaya konan manipülatif eylemler hatırlanmaktadır.**

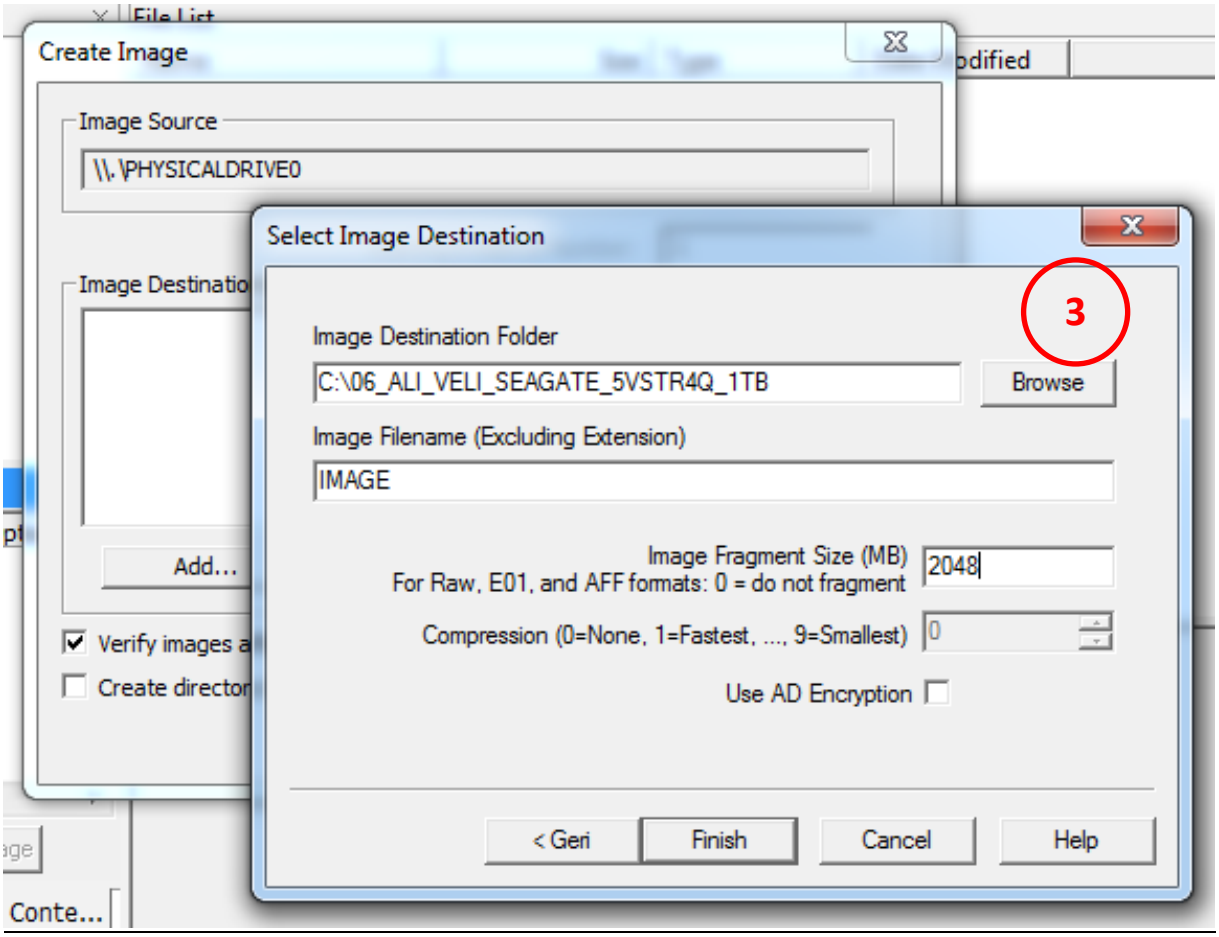
Grafiksel anlatım

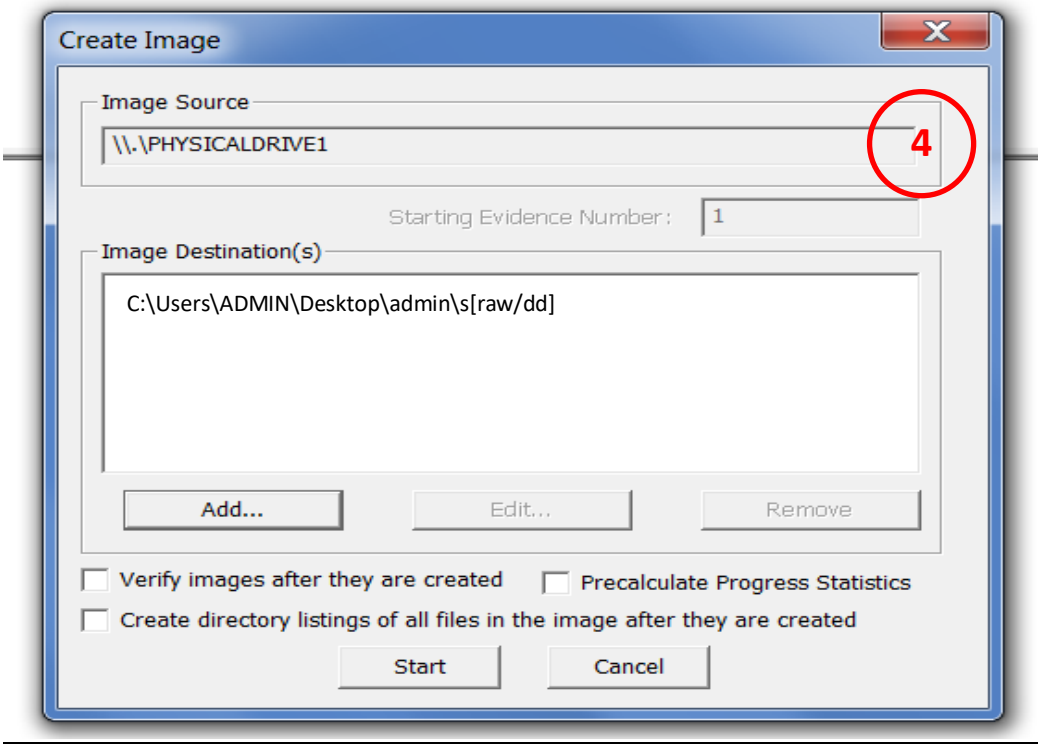
Gerek donanım gerek yazılım marifetiyle yapılan imaj işlemleri birçok yönden benzer özellikler taşımaktadır. Aşağıda ekran görüntülerine yer verilen işlem süreçlerinin açıklamalar ile anlatılması amaçlanmıştır.

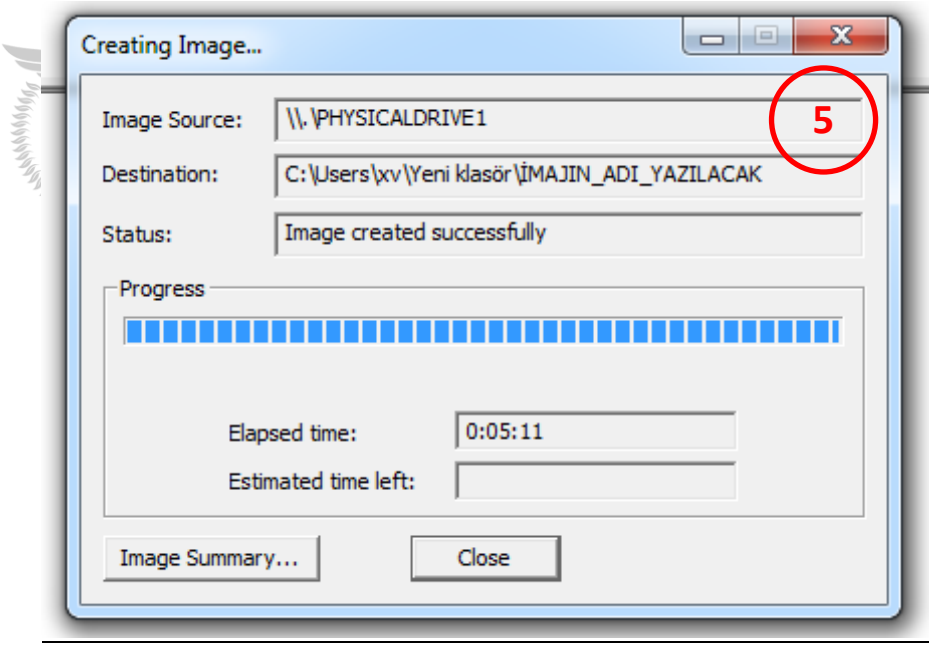


İmaj alma işlemi bittiğinde dosyalar ile birlikte program veya donanım tarafından oluşturulacak olan text türünde log dosyasının içerisinde bulunacak bilgiler başlangıçta yazılır.

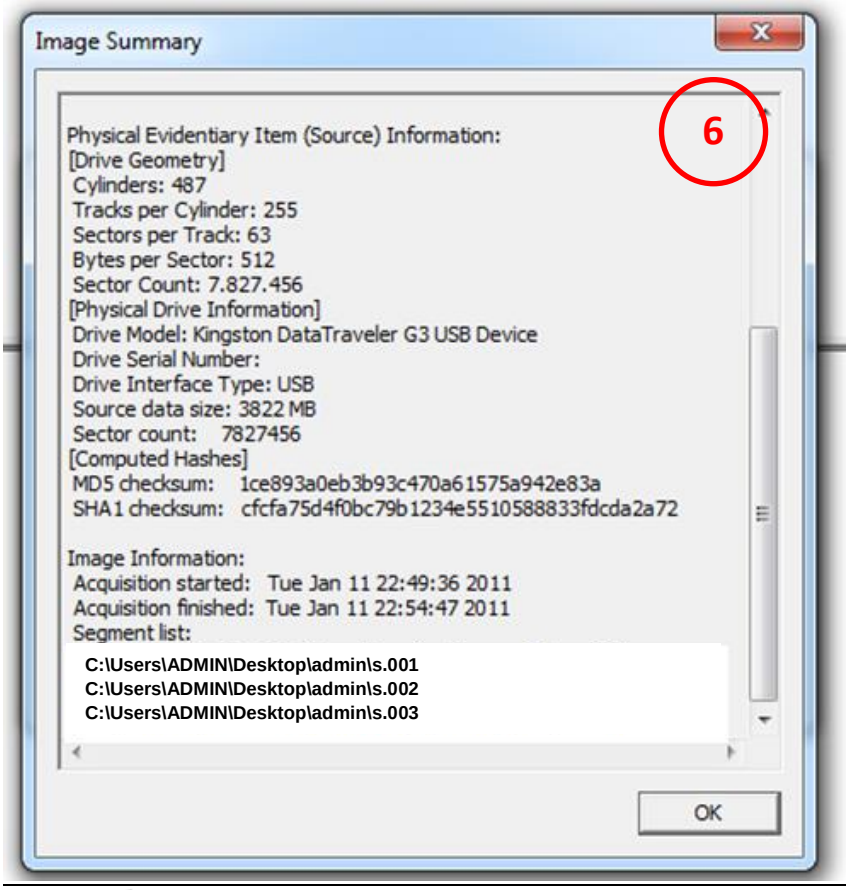


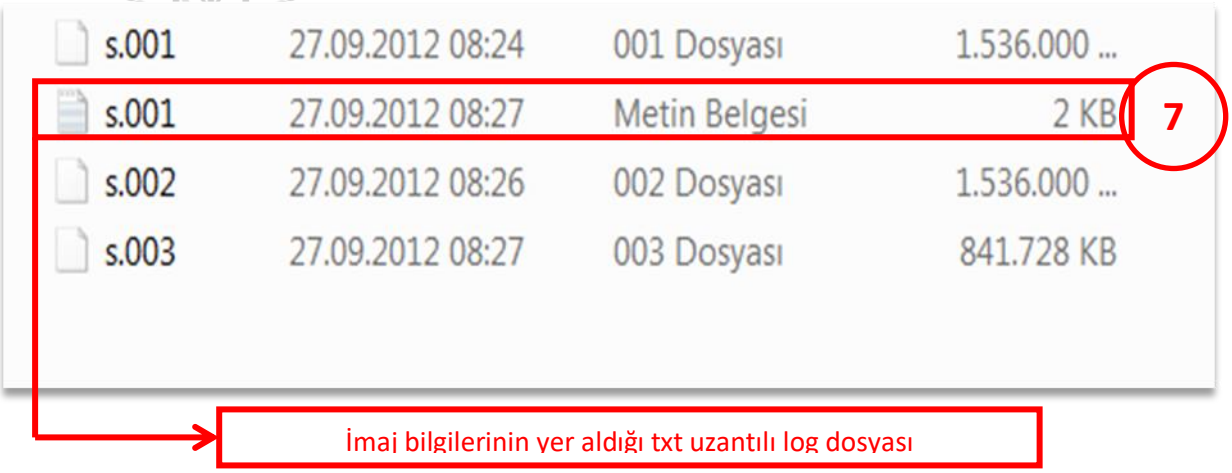

Create Image
Image Source
\\.\PHYSICALDRIVE0
Image Destinatio
Add...
Verify images a
Create director
Select Image Destination
3
Image Destination Folder
C:\06_ALI_VELI_SEAGATE_5VSTR4Q_1TB
Browse
Image Filename (Excluding Extension)
IMAGE
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment
2048
Compression (0=None, 1=Fastest, ..., 9=Smallest)
0
Use AD Encryption
< Geri
Finish
Cancel
Help



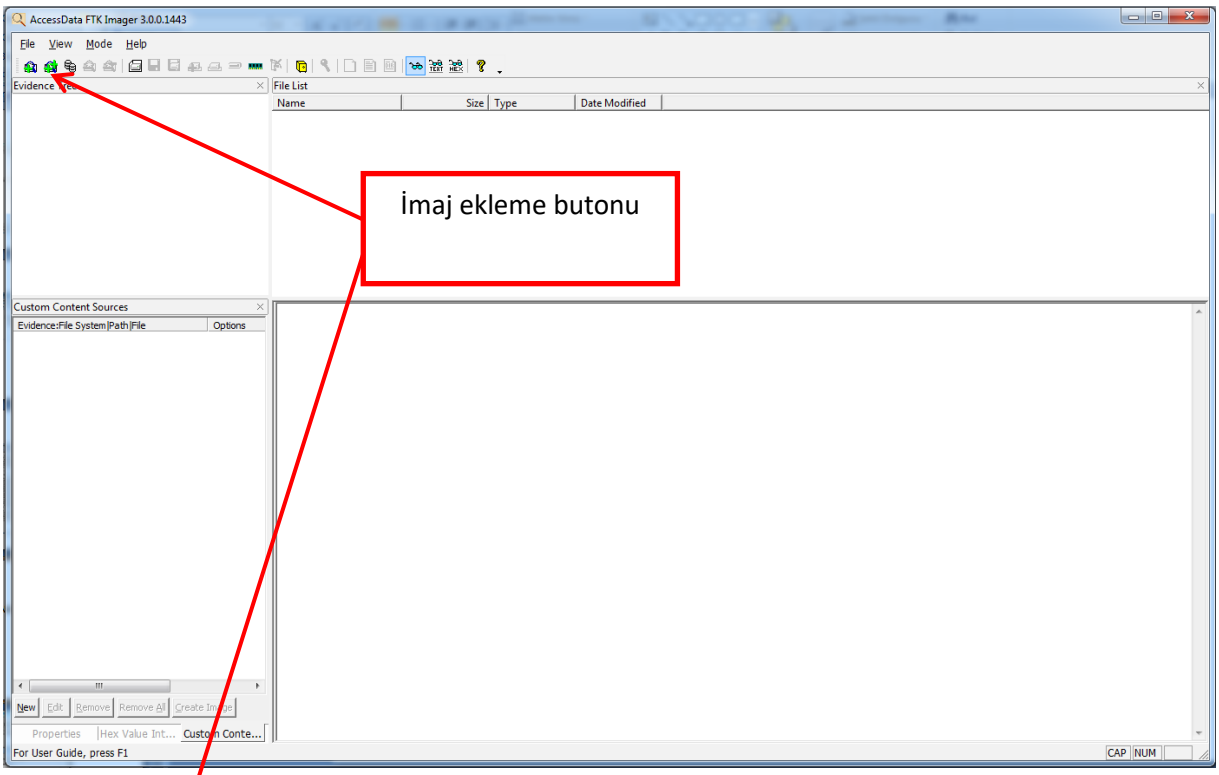


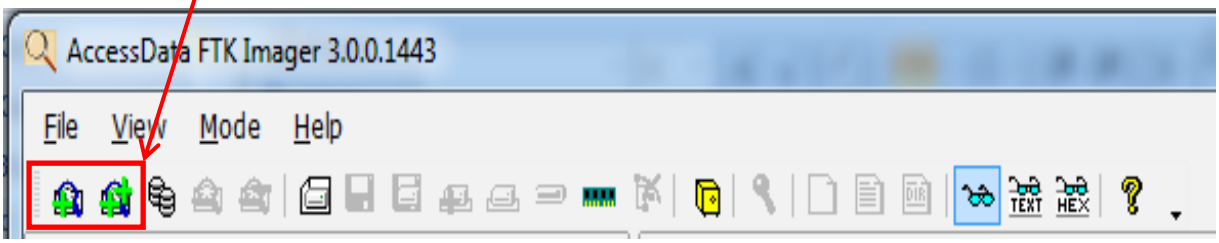
İmaj alma işlemi bitiğinde "Image Summary" butonuna basarak, imaj alma işlemine ait txt uzantılı log dosyasını görüntüleyebiliriz *(7 numaralı resim)*. Bu dosya içerisinde imajı alınan materyale ait bilgiler mevcuttur. Marka. Model, seri numarası, kapasite hash bilgileri, imaja başlama tarihi, imaj bitimine ait tarih ve olay bilgileri gibi bilgiler mevcuttur. Aşağıda ekran görüntüsüne yer verilmiştir.*6 Numaralı resim.*

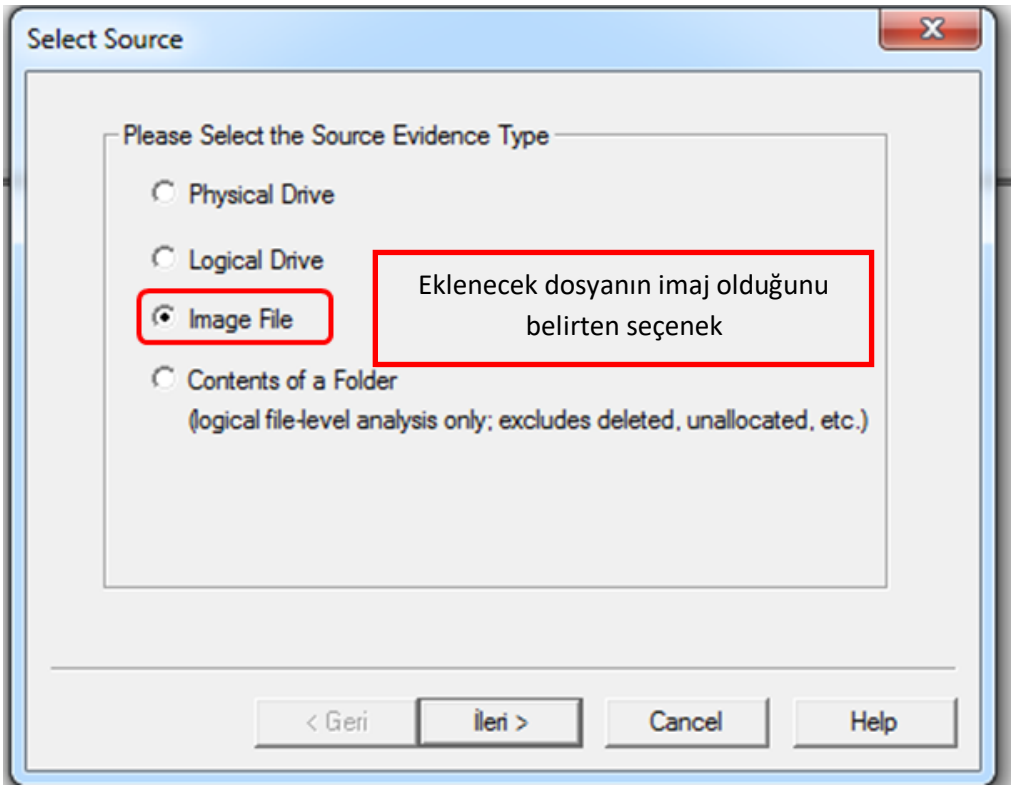


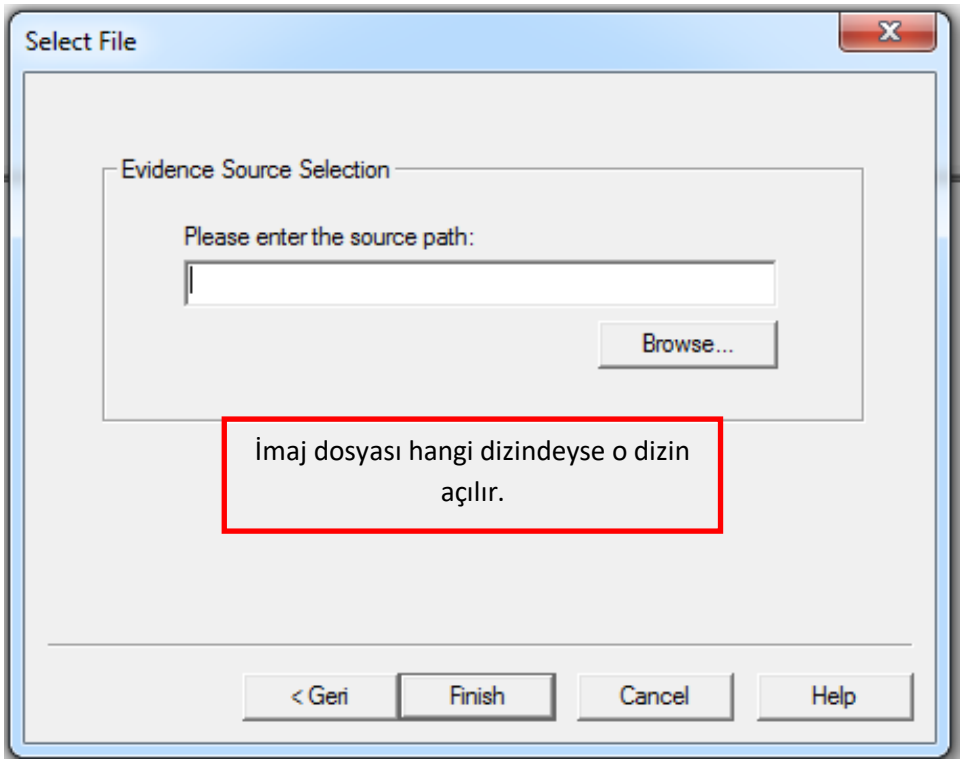


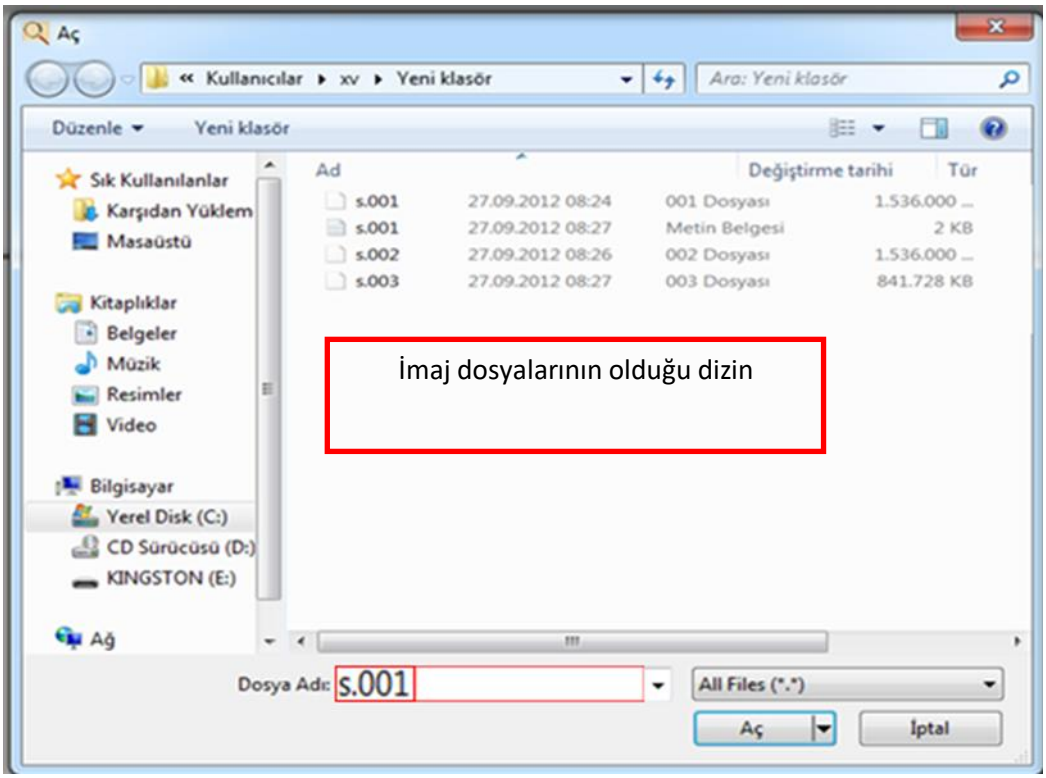
Diğer dosyalar ise imaj dosyalarıdır. Yani hangi materyalin (harddisk, sd kart, usb flash bellek vs.) imajını aldıysak o materyalin içindeki tüm veriler işte bu şekilde oluşturulan dosyaların içerisinde yer alır. Bu dosyalar şu şekilde incelenir; İnceleme programını açarak, ilgili menüden imaj dosyası ekleyi seçeriz ve yukarıdaki imaj dosyalarını seçeriz, program otomatik olarak bu imaj dosyalarını, klasör yapısında gösterir. İncelemeyi yapan kişi tıpkı bir bilgisayar kullanıcısının ekranında gördüğü şekilde dosyaları görebilir. Örnek ekran görüntülerine aşağıda yer verilmiştir.

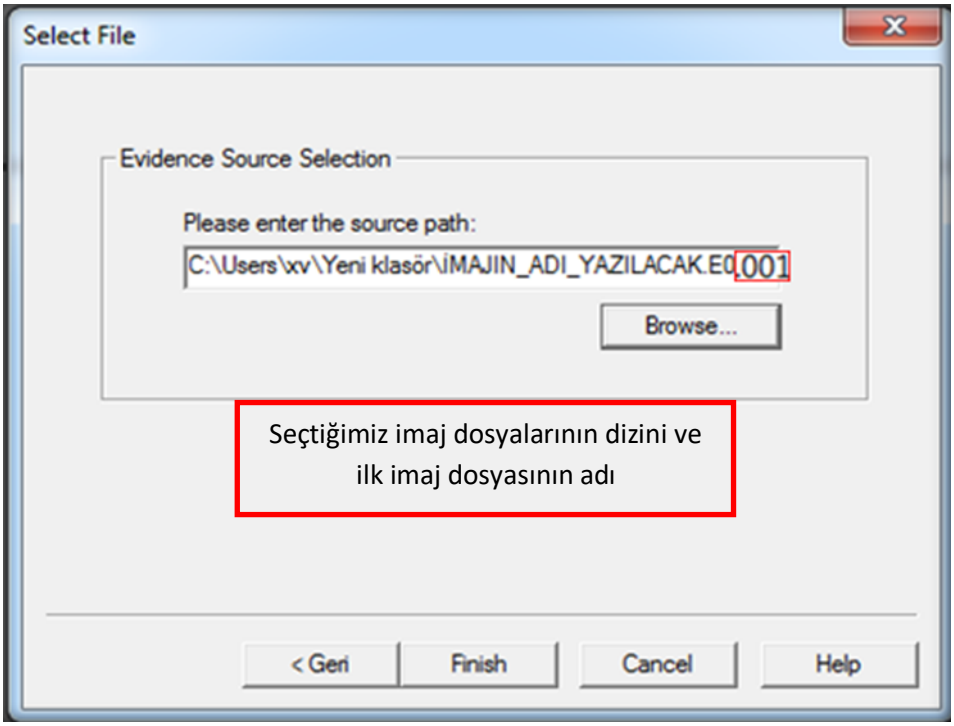

İmaj ekleme butonu


AccessData FTK Imager 3.0.0.1443
File
View
Mode
Help

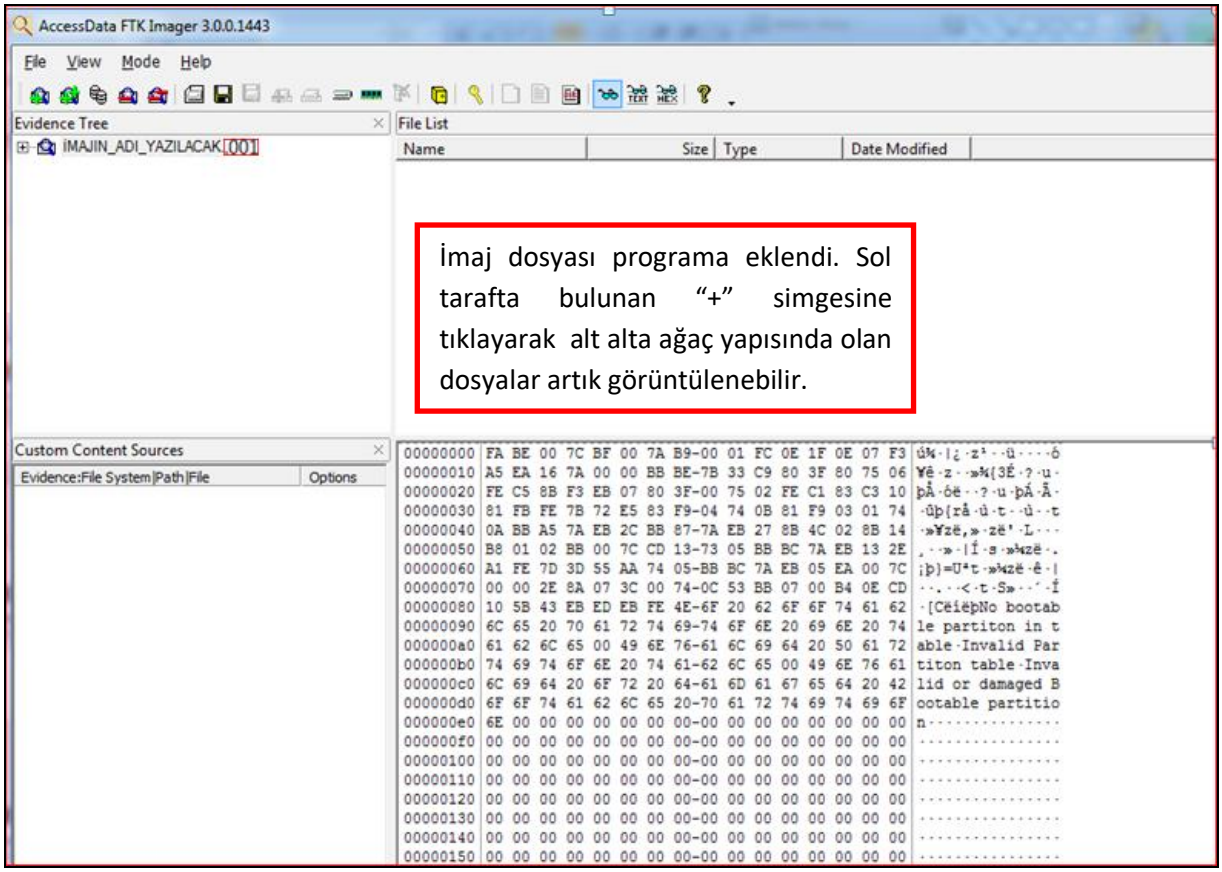

Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
Eklenecek dosyanın imaj olduğunu belirten seçenek
< Geri
İleri >
Cancel
Help


Select File
Evidence Source Selection
Please enter the source path:
Browse...
İmaj dosyası hangi dizindeyse o dizin açılır.
< Geri
Finish
Cancel
Help

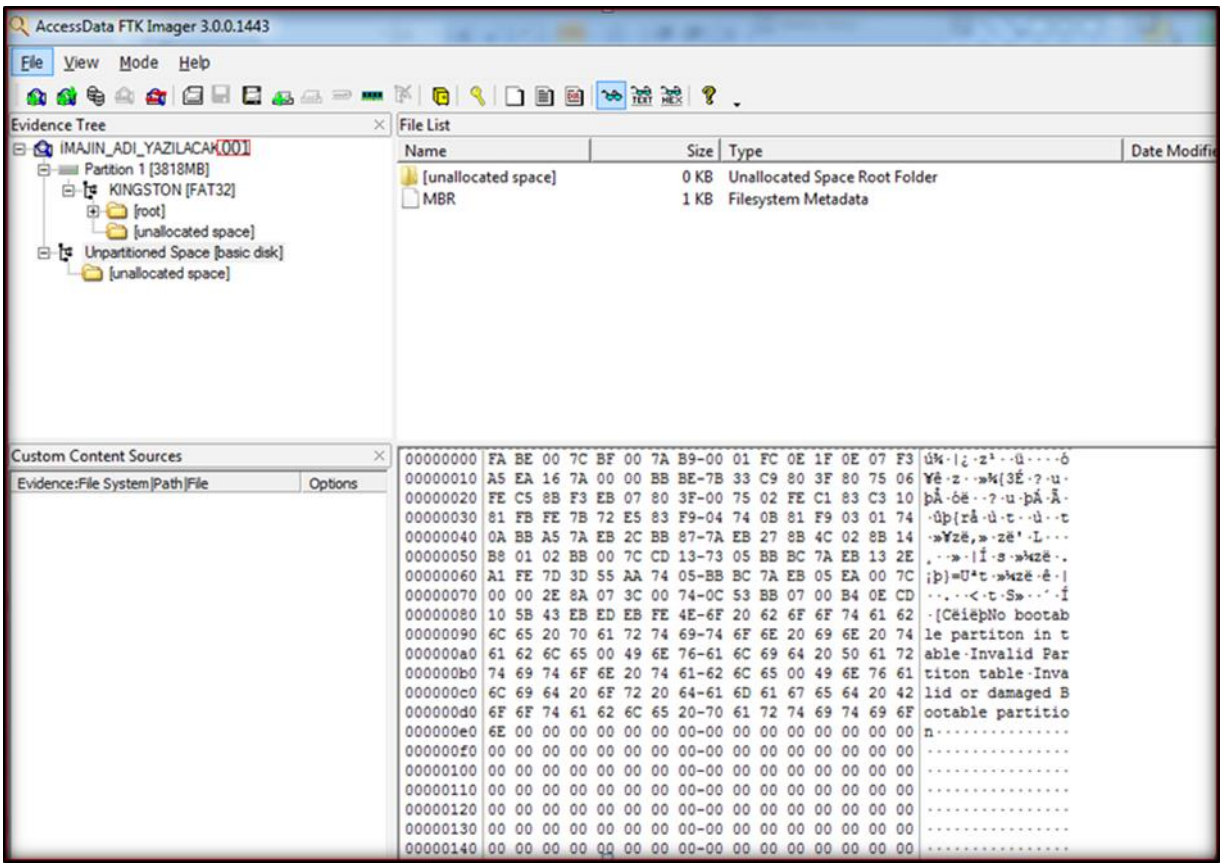

Aç
Kullanıcılar ▸ xv ▸ Yeni klasör
Ara: Yeni klasör
Düzenle
Yeni klasör
Sık Kullanılanlar
Karşıdan Yüklem
Masaüstü
Kitaplıklar
Belgeler
Müzik
Resimler
Video
Bilgisayar
Yerel Disk (C:)
CD Sürücüsü (D:)
KINGSTON (E:)
Ağ
Ad
Değiştirme tarihi
Tür
s.001 27.09.2012 08:24 001 Dosyası 1.536.000 ...
s.001 27.09.2012 08:27 Metin Belgesi 2 KB
s.002 27.09.2012 08:26 002 Dosyası 1.536.000 ...
s.003 27.09.2012 08:27 003 Dosyası 841.728 KB
İmaj dosyalarının olduğu dizin
Dosya Adı: s.001
All Files (*.*)
Aç
İptal

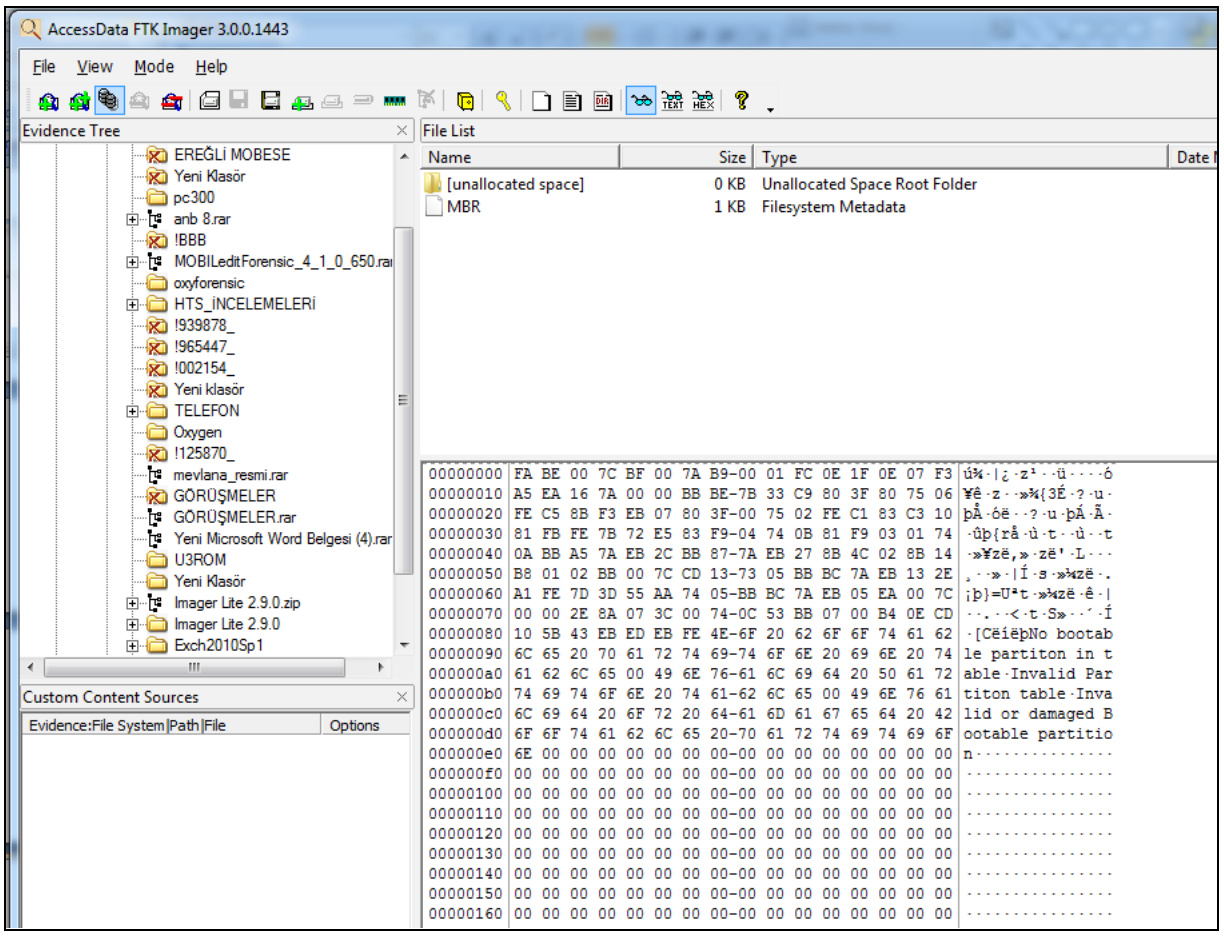


Seçtiğimiz imaj dosyalarının dizini ve ilk imaj dosyasının adı



İmaj dosyası programa eklendi. Sol tarafta bulunan "+" simgesine tıklayarak alt alta ağaç yapısında olan dosyalar artık görüntülenebilir.


AccessData FTK Imager 3.0.0.1443
File View Mode Help
Evidence Tree
İMAJIN_ADI_YAZILACAK001
Partition 1 [3818MB]
KINGSTON [FAT32]
[root]
[unallocated space]
Unpartitioned Space [basic disk]
[unallocated space]
File List
Name Size Type Date Modifi
[unallocated space] 0 KB Unallocated Space Root Folder
MBR 1 KB Filesystem Metadata
Custom Content Sources
Evidence:File System|Path|File Options
00000000 FA BE 00 7C BF 00 7A B9-00 01 FC 0E 1F 0E 07 F3
00000010 A5 EA 16 7A 00 00 BB BE-7B 33 C9 80 3F 80 75 06
00000020 FE C5 8B F3 EB 07 80 3F-00 75 02 FE C1 83 C3 10
00000030 81 FB FE 7B 72 E5 83 F9-04 74 0B 81 F9 03 01 74
00000040 0A BB A5 7A EB 2C BB 87-7A EB 27 8B 4C 02 8B 14
00000050 B8 01 02 BB 00 7C CD 13-73 05 BB BC 7A EB 13 2E
00000060 A1 FE 7D 3D 55 AA 74 05-BB BC 7A EB 05 EA 00 7C
00000070 00 00 2E 8A 07 3C 00 74-0C 53 BB 07 00 B4 0E CD
00000080 10 5B 43 EB ED EB FE 4E-6F 20 62 6F 6F 74 61 62
00000090 6C 65 20 70 61 72 74 69-74 6F 6E 20 69 6E 20 74
000000a0 61 62 6C 65 00 49 6E 76-61 6C 69 64 20 50 61 72
000000b0 74 69 74 6F 6E 20 74 61-62 6C 65 00 49 6E 76 61
000000c0 6C 69 64 20 6F 72 20 64-61 6D 61 67 65 64 20 42
000000d0 6F 6F 74 61 62 6C 65 20-70 61 72 74 69 74 69 6F
000000e0 6E 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
000000f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00000100 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00000110 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00000120 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00000130 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00000140 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

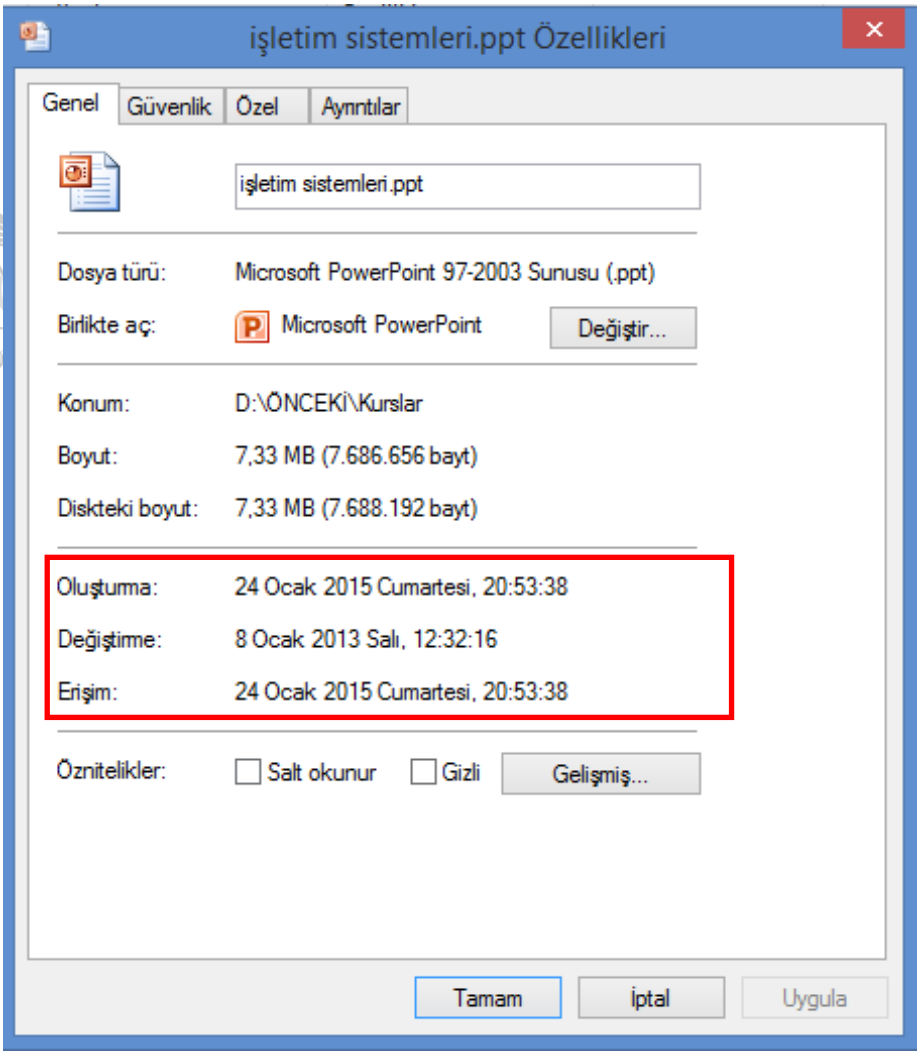

AccessData FTK Imager 3.0.0.1443
File View Mode Help
Evidence Tree
EREĞLİ MOBESE
Yeni Klasör
pc300
anb 8.rar
!BBB
MOBILeditForensic_4_1_0_650.rar
oxyforensic
HTS_İNCELEMELERİ
!939878_
!965447_
!002154_
Yeni klasör
TELEFON
Oxygen
!125870_
mevlana_resmi.rar
GÖRÜŞMELER
GÖRÜŞMELER.rar
Yeni Microsoft Word Belgesi (4).rar
U3ROM
Yeni Klasör
Imager Lite 2.9.0.zip
Imager Lite 2.9.0
Exch2010Sp1
File List
Name Size Type Date
[unallocated space] 0 KB Unallocated Space Root Folder
MBR 1 KB Filesystem Metadata
Custom Content Sources
Evidence:File System|Path|File Options
00000000 FA BE 00 7C BF 00 7A B9-00 01 FC 0E 1F 0E 07 F3
00000010 A5 EA 16 7A 00 00 BB BE-7B 33 C9 80 3F 80 75 06
00000020 FE C5 8B F3 EB 07 80 3F-00 75 02 FE C1 83 C3 10
00000030 81 FB FE 7B 72 E5 83 F9-04 74 0B 81 F9 03 01 74
00000040 0A BB A5 7A EB 2C BB 87-7A EB 27 8B 4C 02 8B 14
00000050 B8 01 02 BB 00 7C CD 13-73 05 BB BC 7A EB 13 2E
00000060 A1 FE 7D 3D 55 AA 74 05-BB BC 7A EB 05 EA 00 7C
00000070 00 00 2E 8A 07 3C 00 74-0C 53 BB 07 00 B4 0E CD
00000080 10 5B 43 EB ED EB FE 4E-6F 20 62 6F 6F 74 61 62
00000090 6C 65 20 70 61 72 74 69-74 6F 6E 20 69 6E 20 74
000000a0 61 62 6C 65 00 49 6E 76-61 6C 69 64 20 50 61 72
000000b0 74 69 74 6F 6E 20 74 61-62 6C 65 00 49 6E 76 61
000000c0 6C 69 64 20 6F 72 20 64-61 6D 61 67 65 64 20 42
000000d0 6F 6F 74 61 62 6C 65 20-70 61 72 74 69 74 69 6F
000000e0 6E 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
000000f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00000100 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00000110 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00000120 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00000130 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00000140 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00000150 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00000160 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

Tarih ve Zaman bilgilerini önemi

Dosya özelliklerine ait olan tarih ve zaman bilgileri bilgisayarda saklanır. Bunların çoğu açık olarak görülür (explorer özellikleri (properties)), bazıları da gizlidir. Tarih ve zaman tüm olaylar için çok önemlidir. Dosyaların ne zaman kim tarafından oluşturulduğunu, dosya üzerinde değişiklik yapıldığı tarihin ne olduğu, son erişim sağlayan kişi ve tarihin ne olduğu gibi bilgiler elde edilebilir bilgilerdir. Temelde 3 (üç) çeşit tarih vardır.

- Oluşturma Tarihi (Created Date)
- Değiştirme Tarihi (Modified Date)
- Erişim Tarihi (Accessed Date)

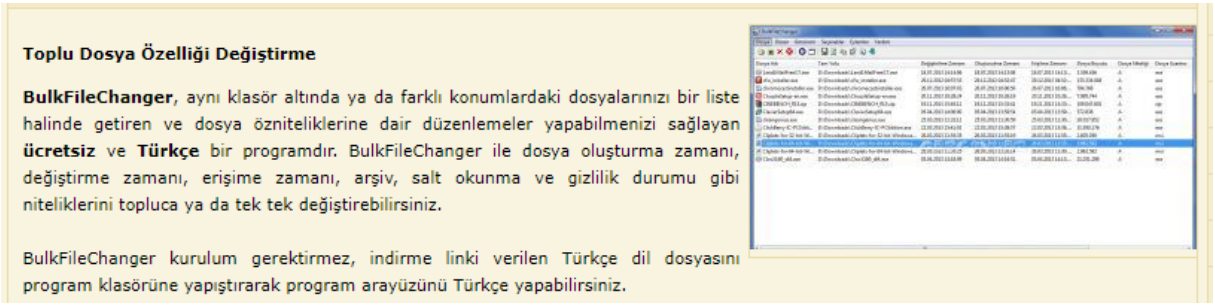
Bunlarla birlikte dosya eğer silinmiş ise silinme tarihi (Deleted Data) bilgiside mevcuttur. Söz konusu bilgiler Ntfs için MFT denilen (Master File table) alanında (dosya) mevcuttur. Ntfs bölümünden dosyaları almak gerekli bilgileri depolamak için kullanılmaktadır. Farklı dosyalar hakkında içerik oluşturan bir veri tablolama biçimidir. Ntfs üzerinde herhangi bir dosya oluşturulduğunda bununla birlikte Mft içinde bir kayıt oluşturulur.



Taşıma-Moving Files:

- **Aynı sürücü içerisinde orijinal dosya bir konumdan başka bir konuma taşınırsa ne olur?** Özellikleri aynı kalmakla birlikte erişim tarihi değişikliğe uğrar.
- **Bir sürücüdeki orijinal dosya başka bir sürücü içerisine taşınırsa ne olur ?** Yeni bir dosya oluşur, orijinali kalır, yeni dosya için yeni zaman oluşur, oluşturma tarihi değişir, erişim tarihi değişir, değiştirilme tarihi değişir.

Unutulmamalıdır ki tarih ve zaman bilgisinde rahatlıkla manipülasyon yapılabilir. Aşağıda Windows işletim sisteminde kullanılabilen bir manipüle programına ait bilgilere yer verilmiştir.



Kaynak: https://www.gezginler.net/indir/bulkfilechanger.html

Mac OS işletim sistemlerinde ise programa dahi gerek duyulmadan terminal (komut penceresi) kullanılarak ilgili komutlar marifetiyle istenilen dosyalarda istenilen tarih değişiklikleri yapılabilir.

"touch -mt YYYYMMDDhhmm.ss [file path]" komutu değiştirme tarihini,
"touch -at YYYYMMDDhhmm.ss [file path]" erişim tarihini,
"touch -t YYYYMMDDhhmm.ss [file path]" oluşturma tarihlerini değiştirir.

Linux işletim sistemlerinde ise" exiftool" isimli bir eklenti marifetiyle terminal (komut penceresi) kullanılarak ilgili kodlar ile istenilen dosyada istenilen değişiklikler yapılabilir.

Adli Bilişim Manipülasyonları

Bir dijital materyalin içerisinde yer alan verilerin çok farklı yöntemler ile değiştirilmesi, silinmesi veya veri eklenmesi mümkündür. Aşağıda maddeler olarak ve açıklamalarına teknik olarak yer verildiği üzere, her bir yöntemin teknik olarak ispatı mümkündür.

1. **Canlı imaj alma işleminde manipülasyon:** İmajı alınacak dijital materyal içerisine olay yerinde ekleme yapılabilir. Söz konusu bu durum genellikle, canlı imaj alma olarak adlandırılan işlemlerde gerçekleştirilebilir. Şöyle ki; Olay yerinde hali hazırda açık bir laptop yada masaüstü bir bilgisayar ya da bir sunucu olsun, işletim sistemi çalışıyorken, harici bir disk usb veya sata portlarından bağlanır. Ayrıca bir usb flash bellek takılır. Bu flash bellek içerisinde canlı imaj alma işlemini gerçekleştirmek için gereken portable (tak çalıştır) program bulunur. Program haricinde herhangi bir dosyanın daha önceden hazırlanarak bu usb bellek içinde olduğunu ve imaj alma işlemine başlamadan önce bu dosyanın bilgisayar içerisinde herhangi bir yere kopyalandığını varsayalım. Dosya kopyalama işlemini yapan kullanıcı bilgisini, kopyalandığı zamanın tarih ve saat bilgilerini saklar. Ancak yine portable bir program marifetiyle dosyanın oluşturan bilgisini, oluşturma tarihini değiştirerek örneğin 1 hafta öncesine almak mümkündür. Ve bu yapılan işlemlerin kayıtlarını tutan işletim sisteminin ilgili yerlerdeki log kayıtlarını geri getirilemeyecek şekilde silmek de mümkündür. Bu işlemden sonra alınacak imaj içerisinde artık bu dosyanın sonradan eklendiği ile ilgili bir veri bulunamayacaktır. Dolayısıyla şüphelinin bilgisayarında yer alan hard disk içerisinde aslında olmayan bir veri eklenmiş olacaktır. Burada belirtilen yöntemin uygulanmaması, uygulanamaması yada uygulanmasına mahal vermemek için, olay yerine girişten itibaren kamera kaydının yapılması uygulaması daim ve sürekli olmalıdır. Kamera kaydının yapılmadığı hiçbir işlem yüzde yüz güvenilir değildir.

2. **İmaj alındıktan sonra manipülasyon:** Şüpheliye ait dijital materyalin alınan imaj dosyaları, incelenmek üzere kolluk görevlileri tarafından birimlerine götürülür. Burada imaj içerisinde olmayan bir veri eklenmek istenirse yapılacak işlemlerden birisi şudur; Kolluğa ait hard disk içerisinde bulunan imaj dosyaları, adli bilişim yazılımları marifetiyle, restore denilen bir işlemle başkaca bir hard diske imaj içeriği aktarılır. Aktarım yapılan hard diskte artık şüphelinin hard diski ile aynı içerik mevcut olur. Bu hard disk içerisinde istenilen veri eklenir. Eklenen veri o anın tarih ve saat bilgisini taşıyacağından portable bir programla güncel tarih ve saat bilgisi istenilen bir zamana ayarlanır. Sonraki aşamada bu hard diskin imajı, daha önceden imaj hard diski olarak bilinen hard diske aktarılır. İmaj işlemi bittiğinde, içerisinde yer alan log dosyası eski kayıtlarla değiştirilir. Log dosyasının değiştirme tarihide olay yerinde yapılan imaj alma tarihi ile değiştirilir. Böylelikle elde edilen imaj dosyası orijinal imaj gibi olur. Tabi ki bu yöntemde farklı handikaplar mevcuttur. Yapılan bu manipülasyonun tespiti imaj dosyalarının incelenmesi ile tespit edilebilir. Ancak veriyi ekleyen ve veriyi inceleyen ve sonrasında inceleme raporunu hazırlayan aynı kişi olduğundan kendi kendini denetleyecek değildir. Başka bir görevli tarafından denetlenme uygulaması da yoktur.

3. **<u>İnceleme raporunda manipülasyon:</u>** Şüpheliye ait hard diskin imajı alındıktan sonra, elde edilen bu imaj dosyaları yine kollukça incelenmek üzere kendi birimlerine götürülür. Çeşitli yazılımlar marifetiyle inceleme işlemlerine başlanır. Yapılan incelemede soruşturmaya konu veya suç teşkil edebilecek herhangi bir veriye rastlanılmadığını varsayalım. Bu durumda inceleme raporunda işletim sistemi, kullanıcılar vb. bilgiler dışında bir şey olmaması gerekir. Ancak, örneğin çocuk pornografisi içeren bir resim dosyasını rapora ekleyip, teknik bilgilerine de yer verilirse bu raporun doğru olup olmadığı hiçbir zaman denetlenmeyeceği için, şüpheli daha önceki örneklerde olduğu gibi suçsuz yere zan altında kalarak cezai yaptırıma maruz kalacaktır.

4. **<u>Dosya üzerinde manipülsyon:</u>** Şüpheliye ait hard disk imajı alındıktan sonra, elde edilen bu imaj dosyaları yine kollukça incelenmek üzere kendi birimlerine götürülür. Adli bilişim yazılımları marifetiyle inceleme işlemine başlanır. Soruşturmaya konu ve ya suç teşkil edebilecek herhangi bir veriye rastlanıldığını varsayalım. Söz konusu soruşturma konusu terör suçları kapsamında olsun. Terör örgütünün hazırlamış olduğu dijital bir veri olan "**<u>liste" isimli excel dosyasının</u>** tespit edildiğini düşünelim. Normalde yapılması gereken, excel dosyasının içerisinde yer alan verilerin ekran görüntüsünün alınarak inceleme raporuna eklenmesi, dosyaya ait teknik bilgilere yer verilmesi ***<u>(dosya adı, dosya türü, dosya uzantısı, oluşturma tarihi, değiştirme tarihi, son erişim tarihi, hash değerleri, kullanıcı bilgileri vb.)</u>*** ve soruşturma makamlarına sunulmak üzere excel dosyasının tümüyle cd, dvd, flash disk veya hard diske export (çıkarılma) yapılmasıdır.

Ancak bahse konu "**<u>liste"</u>** isimli excel dosyasının, kolluk görevlilerince, kopyalanmak suretiyle **<u>"çalışma liste"</u>** olarak yeniden adlandırıldığını ve bu kopya excel dosyası içerisine, açıklama eklenmesi bahanesiyle, listede olmayan kişilerin eklenmesi, kayıtların değiştirilmesi veya silinmesi gayet tabi mümkündür. İstenilen değişikliklerin yapıldığı bu yeni excel dosyasının ekran görüntülerinin ve teknik bilgilerinin inceleme raporuna eklenmesi, dosyanın tümüyle cd, dvd, flash disk veya hard diske export (çıkarılma) edilmesinin artık hiçbir anlamı kalmayacaktır. Zira artık bambaşka bir dosya ve bu dosyaya ait bilgiler söz konusudur. Vahim olan ise soruşturma ve kovuşturma makamları bu hususları göz önünde bulundurmadığından; kolluk görevlilerinden, inceleme raporunda yer alan hususların ve cd, dvd, flash disk veya hard disk içerisindeki dijital verinin, imaj içerisinde yer alan excel dosyası ile karşılaştırma yapmaması yani kolluk görevlilerin vermiş olduğu veriye kesin kanaat getirmiş olmasıdır. Şüpheli şahsın itirazları var ise, mahkemece kolluk görevlilerinin almış olduğu imaj dosyasının bilirkişi veya dosyanın büyüklüğüne göre bilirkişi heyeti tarafından incelenmesine karar verilmesi olayın aydınlatılması, maddi gerçeğe ulaşılması, her türlü şüphenin ortadan kaldırılması açısından elzem bir karar olacaktır.

Ergenekon ve balyoz davalarında ortaya çıkan dijital manipülasyonlar

- Balyoz davasında, 19 Şubat 2010 tarihli **raporda CD'lerin 2003 tarihinde üretildiği** ve CD'lere sonradan ekleme yapılmadığı belirtildi. TUBİTAK dosyalarda sahtecilik tespit etmedi. Bağımsız bilirkişi raporlarında **CD'lerde 2007 tarihinde piyasa çıkan bilgisayar programı ile hazırlanmış dosyalar tespit edilince** mahkeme TUBİTAK'tan bir kez daha rapor istedi.

- Tutuklu sanık emekli Albay Hakan Büyük'ün evinde bulunduğu iddia edilen flash bellekteki, "Bilvanis Çiftliği/Eskişehir/Ek-A 926 Teklifler.doc." dosya yolunda yer alan bir dokümanın içeriğinde, **15 Haziran 2005 tarih ve 5365 Sayılı Yasanın 7. maddesi bulunan bir kanun tasarısı taslağının yer alması** ile bu dokümanın oluşturulma ve son kayıt tarihlerinin **2003 yılı olması** mümkün müdür? Peki, içeriğinde **12 Mayıs 2009 tarihine ait bir gazetenin** scan edilmiş görüntüsü olan dijital bir verinin oluşturulma tarihi **19.04.2007** olabilir mi?

- Bilindiği üzere, Balyoz Davası'nın ana kanıtlarını dijital belgeler teşkil ediyor. Balyoz Davası kapsamında 184'ü tutuklu 224 emekli ve muvazzaf askerin yargılanmasına gerekçeleri arasında gösterilen, Gölcük Donanma Komutanlığı İstihbarat Müdürlüğü'ne baskın düzenleyen özel yetkili Ergenekon savcısı Fikret Seçen'in "şüphelendiği" parke taşlarını kaldırtmasıyla "ele geçirilen" çuvallardan çıkan dijital "deliller" ise birçok çelişki barındırıyor. Bu dijital belgelerdeki zamansal çelişkiler "https://balyozdavasivegercekler.com"da bu konuda yayımlanan yazılar, belgelerin şüpheye yer bırakmayacak şekilde "kurgulanmış" olduğunu ispatlıyor.

- **İstanbul Anadolu 4. AĞIR Ceza Mahkemesi Dosya No: 2014/188 Karar No: 2015/143 C. Savcılığı Esas No: 2010/33824 Gerekçeli kararı;**

  "dijital deliller içinde eyer alan ve suç oluşturan belgelerin sanıklar tarafından oluşturulduğu yönünde kesin bir kanaate varılamamış, **bir kısmının sahte olarak oluşturulduğu kesin olarak belirlenmiş**, bir kısmının ise sahte olarak oluşturulduğu yönünde kuvvetli şüphe oluşmuş, ceza hukukunun temel prensiplerinden olan **"Şüpheden sanık yararlanır"** kuralı uyarınca **dijital delillerin hiçbirinin sanıkların aleyhine hükme esas alınamayacağı sonucuna varılmıştır**."

  Dijital delillerdeki sahteciliğe dair:
  "Mahkumiyet hükmüne esas alınan dijital delilerdeki çok sayıdaki dosyanın **oluşturulma ve değiştirilme tarihi üst verileri arasında çelişkiler bulunması,** Donanma Komutanlığında ele geçirilen 5 nolu harddiske n**ormal kullanıcı hareketi ile açıklanamayacak şekilde 6 ayrı zamanda saati güncel olmayan bir bilgisayardan tarih sıralamasına uymaksızın veriler yüklenmesi,** son olarak **28/07/2009 tarihinden sonra toplu şekilde veri yüklendiğinin anlaşılması**, Calibri ve Cambria yazı tiplerinin Office Open XML referanslarının Microsoft Office yazılımlarda ilk kullanılma tarihleri dikkate alındığında belgelerin **oluşturulma tarihinde de çelişkiler bulunması**, mahkumiyet hükmüne esas **tüm dijital verilerde zaman, mekan ve kişi yönünden birçok çelişkiler bulunması, belgelerin oluşturulma tarihlerinden çok sonraki durum ve olayları içermesi dikkate alındığında, sahtecilik yapıldığı kesin olarak**

belirlenen 11 ve 17 nolu CD ler dışındaki dijital delillerin de sahte olarak oluşturulduğu yönünde kuvvetli şüphe oluşmuştur."

- "…Bu mantıkla hareket edildiğinde sanıkların öncelikle dijital verilerin kendilerine aidiyetini ortadan kaldırmak için belgelerin üst veri yollarını değiştirmeleri daha kolay ve daha ise yarar bir yöntemken sanıkların bunu yapmayıp da sadece belgeler içinde çelişkiler oluşturmaları hayatın olağan akışına uygun bulunmamıştır….Ayrıca sanıkların dijital delillerin ele geçmemesi için önlem almak yerine yukarıda belirtilen yöntemi seçmeleri mantıklı bulunmamıştır. **Gerçekten bu suçun islenmesi halinde suçu isleyen ve ince ayrıntısına kadar düşünüp yakalanma ihtimalini de değerlendiren kişilerin öncelikle bu dijital verileri başkasının eline geçmesini engelleyecek şekilde muhafaza edecekleri, hatta çeşitli nedenlerle darbe girişimini gerçekleştiremeyeceklerini anlamaları halinde suç delili olan bu belgeleri yok edecekleri düşünülmüştür.**"

- Öte yandan davanın temelini teşkil eden CD'lerden 11 ve 17 numaralı CD'ler üzerinde yazılmış alan ve sanık Süha Tanyeri'nin eli ürünüymüş izlenimi uyandıran "Or.K.na" ve "K.Özel" şeklindeki el yazılarının bir insan eli ürünü değil de **bir yazı makinesi tarafından yazıldığını gösteren Amerikan Forensic Labratory isimli firmanın bilirkişi raporuna ve İstanbul Adli Tıp uzmanlarından Dr. Jale Bafra'nın uzman mütalaasına da değinilmemiştir.** Söz konusu rapor ve mütalaa, 2/5/2011 tarihli duruşmada tartışılmış olmasına ve CD'ler üzerindeki yazıların sanık Süha Tanyeri'nin davaya konu 1. Ordu Plan Semineri sırasında tuttuğu el yazısından kopyalandığı iddia olunmasına rağmen, İlk Derece Mahkemesi ve Yargıtay tarafından bu hususta bir açıklama yapılmadığı belirtilmiştir

- Suça konu HD5, CD'ler ve USB'deki bazı belgelerin tarih ve zamanlarının iki nedenin en az birinden dolayı gerçek takvim zamanını yansıtmadığı belirlenmiştir. Bu belgeler sistem zamanı güncel olmayan bilgisayarlarda oluşturulmuşlar ve/veya **üst verilerindeki tarih ve zaman bilgileri sonradan gerçek zamanı yansıtmayacak şekilde değiştirilmişlerdir.** CD'lerde değişiklik yapılıp yapılmadığı: CD'ler üzerindeki bazı dokümanlarda ilk kez Microsoft Office 2007'de kullanılmış olan Calibri ve Cambria yazı tipleri ve yine ilk kez Microsoft Office 2007'de kullanılmış olan Office Open XML şemalarına rastlanmıştır. Dosyalar içinde ikili (binary) sayısal verilerin aranmasını sağlayan Hex Editor Neo programı ile Cambria kelimesinin ASCII kodu olan 0x430061006D006200720069006100 hex (hexedecimal: 16 tabanı) dizisinin 11 nolu CD içerisinde taranması sonucu 4 dokümanda Cambria yazı tipine rastlanmıştır.

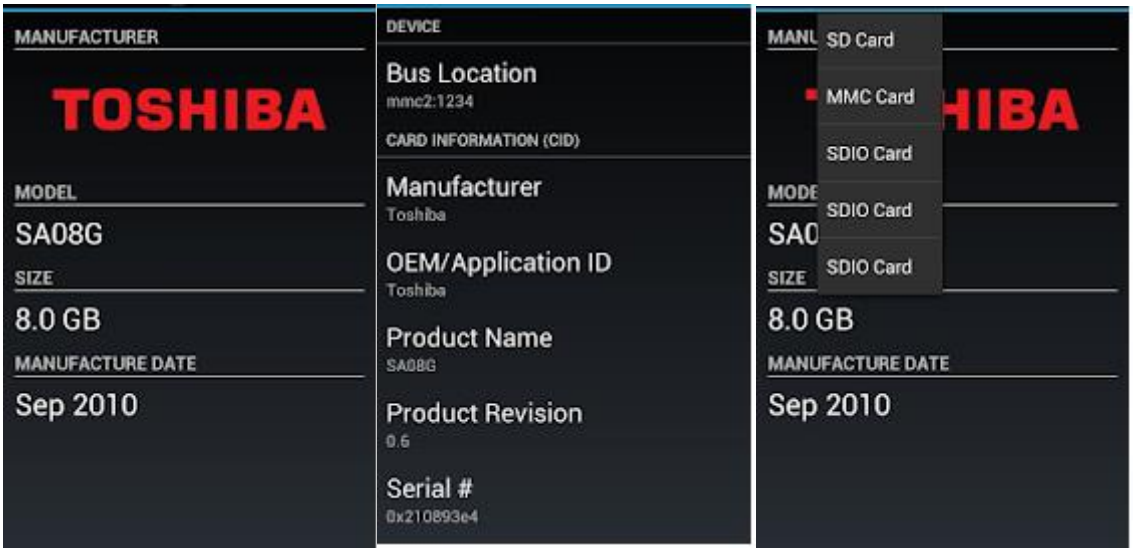
- **Anayasa mahkemesi kararı:** "… İlk Derece Mahkemesi, yalnızca Cumhuriyet Savcısı tarafından sunulan bilirkişi raporlarına itibar etmiş, **bu raporlara karşın başvurucuların savunmalarının bir parçası olarak sundukları bilirkişi rapor ve uzman görüşleri ise dikkate alınmamıştır.** Mahkeme ayrıca başvurucuların, mahkûmiyet kararının dayanağı olan **dijital verilerin gerçeği yansıtmadığı iddialarını değerlendirmek üzere mahkemenin bilirkişi heyeti tayin etmesi ve rapor aldırması yönündeki taleplerini de yeterli olmayan gerekçe ile reddetmiştir.**"

Garson Kod adlı Gizli Tanığın Teslim Ettiği Sd Kart-Siber Raporu

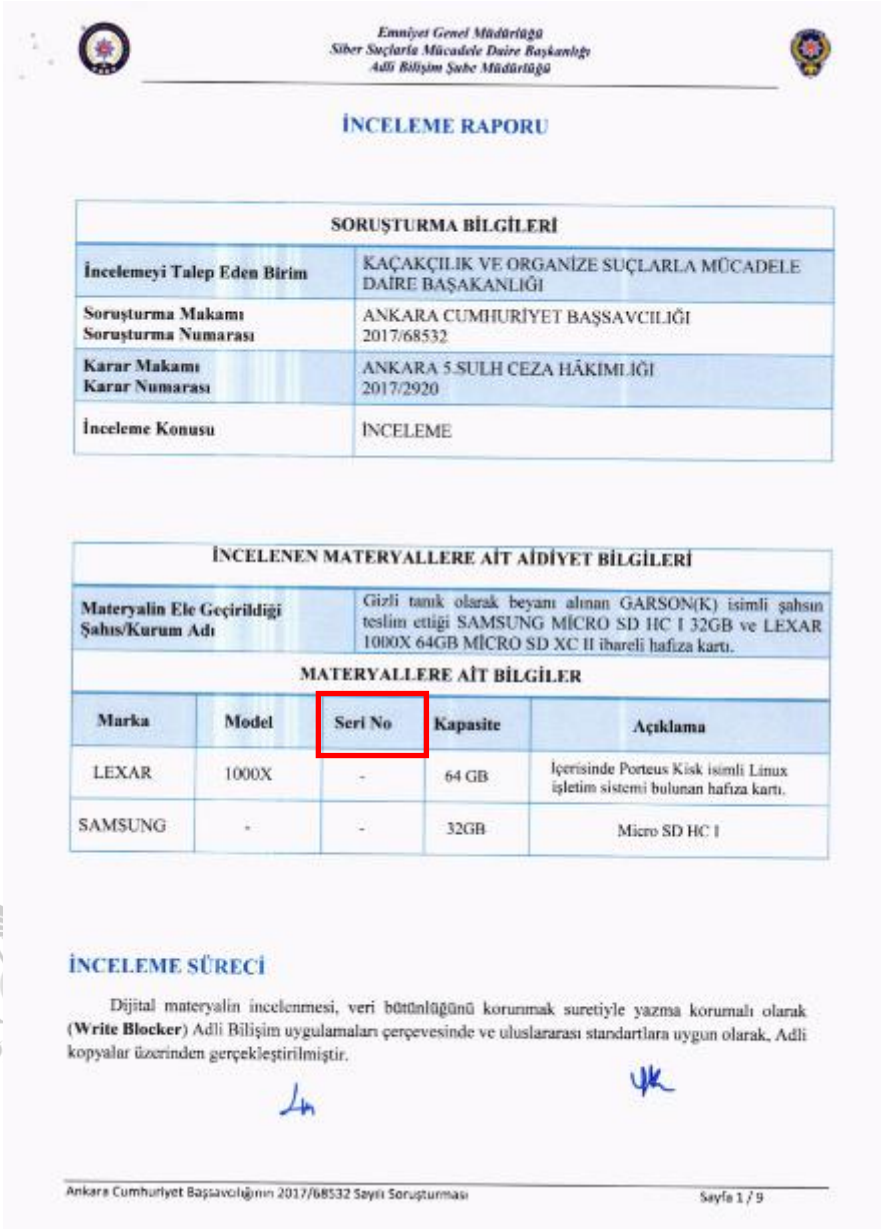
Kod adı garson olan gizli tanığın, 18.04.2017 tarihinde Ankara CBS'na dijital materyalleri teslim etmesi ile başlayan süreç; Söz konusu dijital materyaller içerisinde olduğu söylenen SD kart ve bu kartta tüm emniyet teşkilatı mensuplarının bilgileri ile birlikte fişleme kayıtlarının bulunduğu, söz konusu fişleme kayıtlarına istinaden idari ve adli işlemler başlatıldığı, yargılamaların devam ettiği ve tüm işlemlere dayanak teşkil eden, sd kart içindeki bir excel dosyası olduğu ve bu dosyayla ilgili mahkemelerce henüz bilirkişi incelemesi kararı verilmediği gibi isnat edilen suç karşısında sanıklara dijital materyale ait imaj kopyası verilmeyerek silahların eşitliği, savunma hakkı gibi evrensel, anayasal haklardan mahrum bırakıldığı ancak; Anayasal suç olan fişleme kayıtlarının hiçbir şekilde delil olamayacağı gibi delil olduğu varsayımı yapılarak iddia edilen **dijital materyalin manipüle edilmiş olabileceği göz ardı edilerek** yapılan yargılamalar ile ilgili olarak, söz konusu sd kart ve içerisinde yer alan excel dosyası ile ilgili emniyet birimlerinin hazırlamış oldukları raporlar teknik açıdan değerlendirilecektir.

1. Teslim ettiği SD kart: Lexark Marka 64 Gb aşağıda resmine yer verilen micro sd kartın üretim tarihinin tespit edilmesi olayın bütünlüğünün değerlendirilmesi açısından önemlidir. Ancak söz konusu karta ilişkin teknik rapor, mahkemelere intikal ettirilmemiştir. Seri numarası, model, kapasite, üretim tarihi, revizyon numarası, üretici firma bilgisi gibi bilgiler teknik raporda yer almamaktadır. Aşağıda olması gereken bilgilerin ekran görüntülerine yer verilmiştir.

Örnek resimler



2. Aşağıda Siber Suçlarla Mücadele Daire Başkanlığı Adli Bilişim Şube Müdürlüğü tarafından hazırlanan inceleme raporunun ekran görüntüsüne yer verilmiştir. Materyale ait bilgiler bölümünde seri numarası alanının boş olduğu ve üretim tarihi, revizyon numarası, üretici firma bilgisi gibi bilgilerin (yukarıda örnek resimlerde yer alan bilgilerin) **olmadığı görülmektedir.**



Emniyet Genel Müdürlüğü
Siber Suçlarla Mücadele Daire Başkanlığı
Adli Bilişim Şube Müdürlüğü

İNCELEME RAPORU

SORUŞTURMA BİLGİLERİ	
İncelemeyi Talep Eden Birim	KAÇAKÇILIK VE ORGANİZE SUÇLARLA MÜCADELE DAİRE BAŞAKANLIĞI
Soruşturma Makamı Soruşturma Numarası	ANKARA CUMHURİYET BAŞSAVCILIĞI 2017/68532
Karar Makamı Karar Numarası	ANKARA 5.SULH CEZA HÂKİMLİĞİ 2017/2920
İnceleme Konusu	İNCELEME

İNCELENEN MATERYALLERE AİT AİDİYET BİLGİLERİ	
Materyalin Ele Geçirildiği Şahıs/Kurum Adı	Gizli tanık olarak beyanı alınan GARSON(K) isimli şahsın teslim ettiği SAMSUNG MİCRO SD HC I 32GB ve LEXAR 1000X 64GB MİCRO SD XC II ibareli hafıza kartı.

MATERYALLERE AİT BİLGİLER

Marka	Model	Seri No	Kapasite	Açıklama
LEXAR	1000X	-	64 GB	İçerisinde Porteus Kisk isimli Linux işletim sistemi bulunan hafıza kartı.
SAMSUNG	-	-	32GB	Micro SD HC I

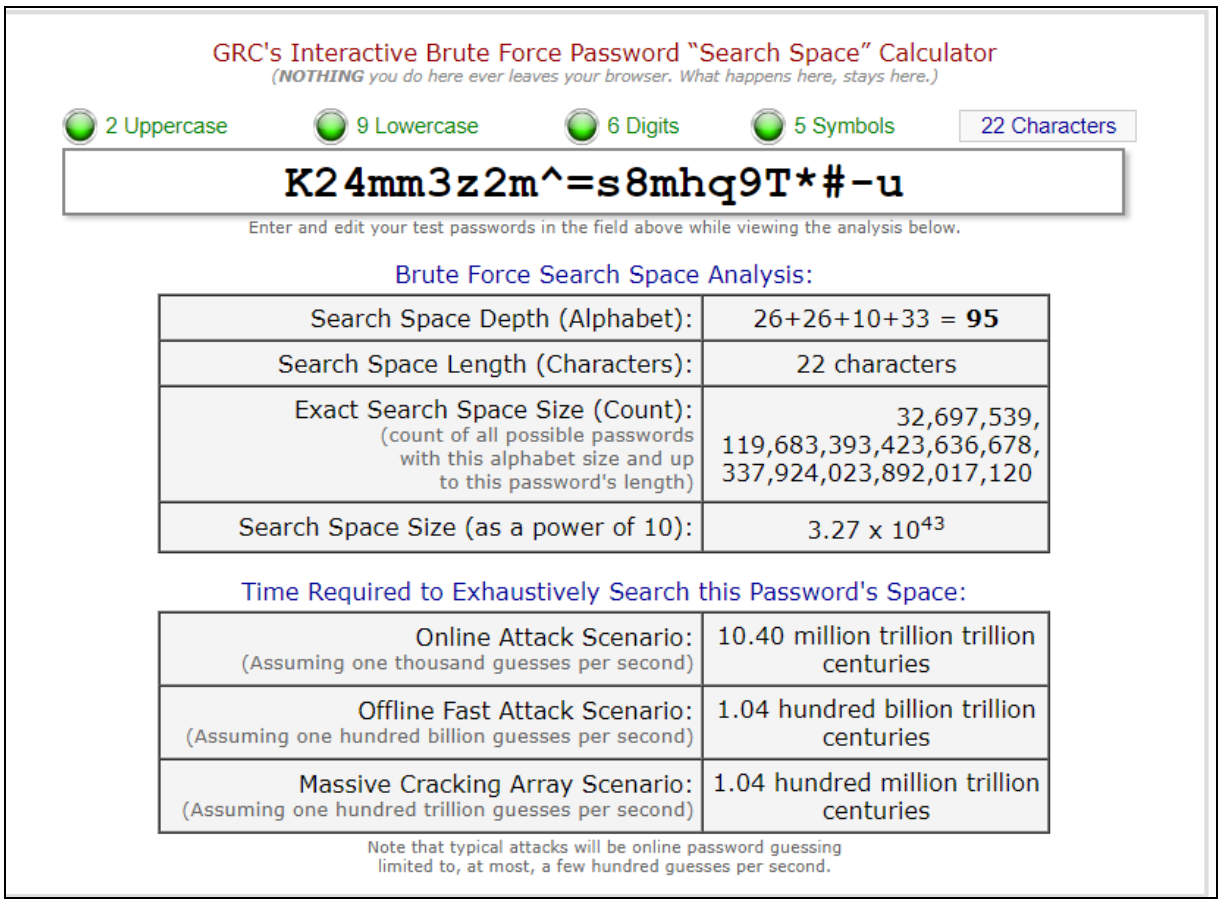
İNCELEME SÜRECİ

Dijital materyalin incelenmesi, veri bütünlüğünü korunmak suretiyle yazma korumalı olarak **(Write Blocker)** Adli Bilişim uygulamaları çerçevesinde ve uluslararası standartlara uygun olarak, Adli kopyalar üzerinden gerçekleştirilmiştir.

Ankara Cumhuriyet Başsavcılığının 2017/68532 Sayılı Soruşturması Sayfa 1 / 9

3. **Aynı raporun 2.sayfasında**; Lexark Marka 64 Gb kapasiteli hafıza kartının imajının, Sandisk marka Cruzer Glide 3.0 ibareli 128 gb kapasiteli flash belleğe klonlandığı (imaj içindeki verinin birebir aktarılması) ve bu flash disk <u>üzerinde çalışma yapıldığı belirtilmektedir. İşlemlerin ne olduğu açıklanmamıştır.</u> Yapılan işlemler neticesinde "Porteus" isimli Linux işletim sisteminin kurulu olduğu belirtilmiştir. Porteus Linux işletim sisteminin boot (başlatma) aşamasında birçok yöntem denenerek şifre değeri geçilmiştir denmekte ve işletim sisteminin başlatıldığı anın ekran görüntülerine yer verilmiştir. Ancak; İlk olarak söz konusu işletim sistemini canlandırma olarak adlandırılan (işletim sisteminin bir program vasıtasıyla sanal olarak kullanılabilir hale getirme) işlemin nasıl yapıldığı, hangi programın kullanıldığı gibi bilgilere yer verilmemiştir. Ayrıca, "boot (başlatma) aşamasında birçok yöntem denenerek şifre değeri geçilmiştir" ibaresi izaha muhtaçtır. Zira işletim sistemine giriş aşamasında şifre olduğu kabul edilmiş ancak şifre ekranının nasıl geçildiği anlatılmamıştır. Oysa "<u>şifre değeri geçilmiştir</u>" ibaresi, ancak şifrenin bilindiği ve bilinen şifrenin, şifre sorulan ekranda ilgili alana girilmesi ve sistemin kabul etmesi halinde söylenebilir. Bu bağlamda şifre biliniyorsa, nasıl, nereden, kim tarafından sağlandığı ya da temin edildiği ya da öğrenildiğinin belirtilmesi gerekmektedir. Diğer bir yöntem ise şifre kırma olarak adlandırılan ve ilgili şifre kırma programları kullanılmak

suretiyle brute force(kaba saldırı), dictionary atacc (Sözlük saldırısı) , Rainbow Table (hash kullanımı), Hybrid (sözlük saldırısına özel karakter ekelme) gibi yöntemler kullanılarak şifrenin bulunması olayıdır. Söz konusu her iki durumda da şifrenin ne olduğunun belirtilmesi gerekmektedir. Çünkü; Yakın geçmişte tanıklık ettiğimiz dijital kumpaslarda, bilhassa Ergenekon ve balyoz davaları, askeri casusluk davalarında dijital verilerin şifreli olduğu ve söz konusu şifrelerin günümüz donanımları ile dahi çözülemeyeceği zira şifrelerin çok uzun ve farklı karakterler içerdiği *(Örn: K24mm3z2m^=s8mhq9T*#-u aşağıda bu şifrenin çözümünün ne kadar zaman alacağına ilişkin tablonun ekran görüntüsüne yer verilmiştir*)*, yahut bazı şifrelerin komik olarak nitelendirilecek şekilde "qsxedc123" gibi klavye üzerinde bulunan tuşların yukarıdan aşağıya çapraz veya aşağıdan yukarıya sistematik olacak şekilde oluşturulan şifreler olduğu görülmüştür. Açıklanan nedenlere her iki halde de (şifrenin uzun veya tahmin edilebilir şekilde kısa olması) şifrenin ne olduğunun teknik raporda yazılması olayın aydınlatılması açısından elzemdir.



GRC's Interactive Brute Force Password "Search Space" Calculator

(**NOTHING** you do here ever leaves your browser. What happens here, stays here.)

2 Uppercase | 9 Lowercase | 6 Digits | 5 Symbols | 22 Characters

K24mm3z2m^=s8mhq9T*#-u

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+26+10+33 = **95**
Search Space Length (Characters):	22 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	32,697,539, 119,683,393,423,636,678, 337,924,023,892,017,120
Search Space Size (as a power of 10):	3.27×10^{43}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	10.40 million trillion trillion centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	1.04 hundred billion trillion centuries
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	1.04 hundred million trillion centuries

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

Görüleceği üzere Saniyede yüz trilyon tahmin yapabilen bir donanım olduğunu varsayarsak, 1,04 yüz milyon trilyon yüzyılda sonuç elde edebileceğiz

MATERYALE AİT TEKNİK BİLGİLER

(LEXAR Marka 64 GB Kapasiteli Hafıza Kartı)

Ankara Cumhuriyet Başsavcılığı Anayasal Düzene Karşı İşlenen Suçlar Soruşturma Bürosunun 18.04.2017 tarih ve 2017/68532 numaralı soruşturması ile Ankara 5.Sulh Ceza Hâkimliğinin 2017/2920 D.İş kararına istinaden gizli tanık olarak GARSON(K) isimli şahıstan ele geçen LEXAR marka 64GB kapasiteli hafıza kartının alınan adli kopyasına ilişkin veriler aşağıda sunulmuştur.

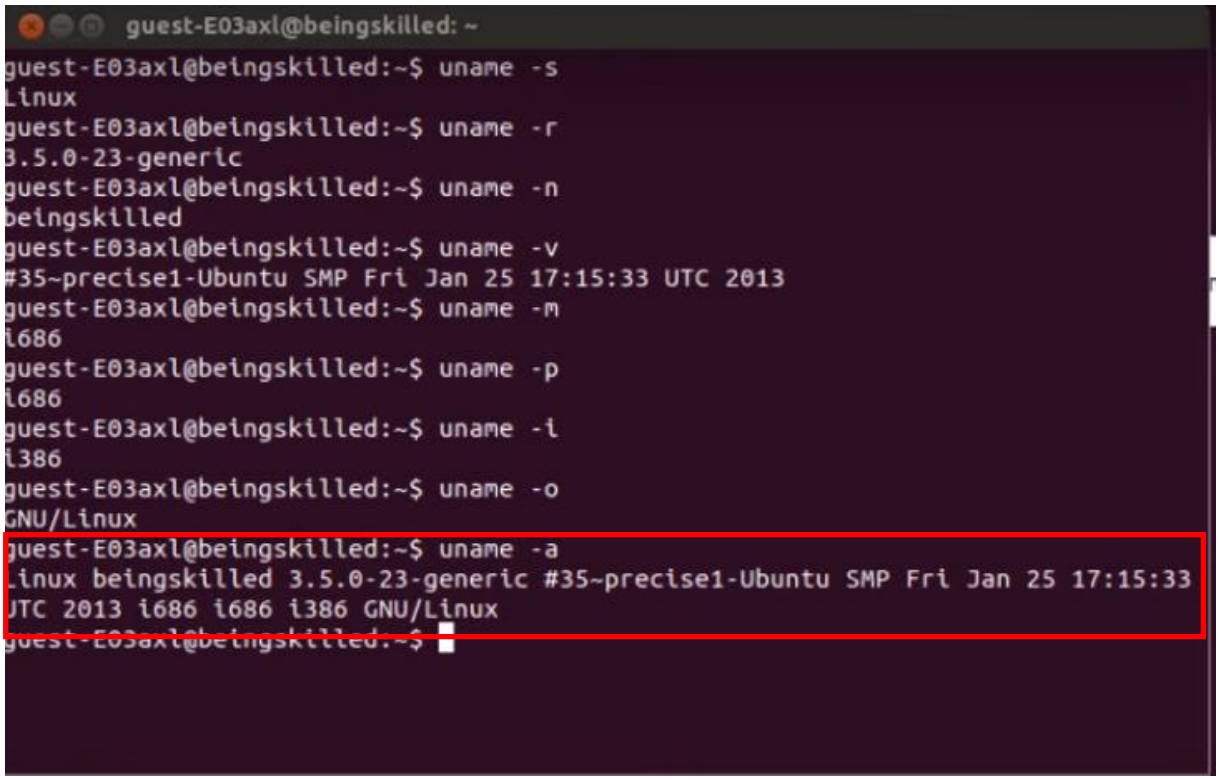
İmaj(Adli Kopya) Alma İşlemi	
İmaj Başlama Zamanı	Wed Apr 19 1:02:35 2017
İmaj Bitiş Zamanı	Wed Apr 19 1:11:55 2017
MD5 Hash Değeri	4095a1ece0617e47c362306ae19d10a3
SHA1 Hash Değeri	2f7acad7fad379a996277c696213b9a1c6764ad8
MD5 Hash Değeri Doğrulama	4095a1ece0617e47c362306ae19d10a3
SHA1 Hash Değeri Doğrulama	2f7acad7fad379a996277c696213b9a1c6764ad8

Bahse konu adli kopya üzerinde uluslararası adli bilişim standartlarına uygun standart adli bilişim teknikleri ile yapılan incelemelerde, verinin şifreli olduğu ve anlamlı veri gelmediği görülmüştür. Bunun üzerine adli kopya alma aracı yardımı ile tarafımızca birebir yedeği (clone) Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı Ulusal Suçlarla Mücadele Şube Müdürlüğünce temin edilen Sandisk marka Cruzer Glide 3.0 ibareli 128GB kapasiteli kutusundan açılmamış durumdaki Flash Belleğe alınmıştır. Sandisk marka 128 GB kapasiteli USB bellek üzerinde yapılan çalışmalar uluslararası adli bilişim standartlarına uygun write block (yazma korumalı) olarak gerçekleştirilmiştir. İşlemlerin neticesinde "Porteus" isimli Linux işletim sisteminin kurulu olduğu görülmüştür.

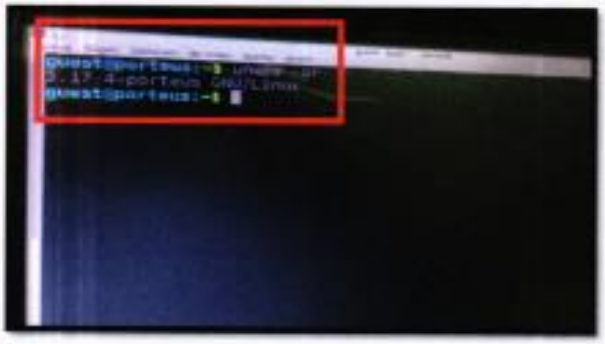
Porteus Linux işletim sisteminin boot (başlatma) aşamasında birçok yöntem denenerek şifre değeri geçilmiştir.

4. Aynı raporun 3.sayfasında "şifre değeri geçilerek" ibaresi tekrar edilmiş olup işletim sisteminin açıldığı belirtilmiştir. İşletim sistemini 3.17.4-proteus GNU/Linux olduğu belirtilmiştir. Ancak söz konusu işletim sistemini teknik bilgilerine yer verilmemiştir. İşletim sisteminin piyasaya sürüldüğü tarih, çalışması için gerekli olan donanım ölçümleri gibi bilgilere yer verilmemiştir. Oysa" http://ftp.vim.org/ftp/os/Linux/distr/porteus/x86_64/archive/" adresinde proteus Linux işletim sistemine ait dosyalar son güncelleme tarihlerine göre versiyonlarının yer adlığı bölümde proteus v3.0 19 Nisan 2014 tarihinde, Porteus-v3.1-rc1 18 Ekim 2014 tarihinde Porteus-v3.1-rc2 18 Kasım 2014 tarihinde, **Porteus-v3.1 18 ocak 2015 tarihinde**, **Porteus-v3.2.1 24 Aralık 2016 tarihinde**, Porteus-v3.2 12 Kasım 2016 tarihinde, Porteus-v3.2rc5 31 Aralık 2016 tarihinde, Porteus-v4.0 16 Haziran 2018 tarihlerinde son güncelleme tarihleri mevcuttur. Bu bağlamda her ne kadar Proteus 3.17.4 versiyonu Linux geliştiricilerinin paylaşım platformlarında listelenen versiyonlar arasında bulunmasa da bahse konu versiyon tarih itibarı ile 2015-2016 yılları arasında geliştirildiği, piyasaya sürüldüğü anlaşılmaktadır. Sonraki sürümler ise *(Porteus-v3.2 12 Kasım 2016 tarihinde, Porteus-v3.2rc5 31 Aralık 2016 tarihinde)* tarihlerinde yayınlanmasına **rağmen güncellenmediği görülmektedir. Ancak, ilerleyen sayfalarda yer verileceği üzere Microsoft Office programlarının 2017 versiyonunun kullanıldığı görülmektedir.**

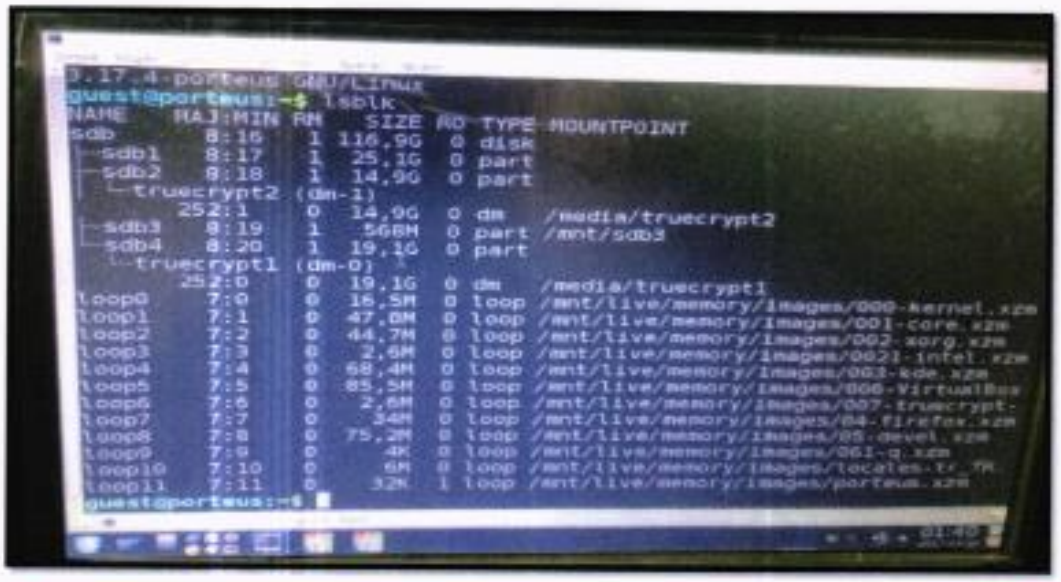
Ayrıca raporda, Porteus işletim sistemi içerisinde terminale yazılan "uname –or" kodu marifetiyle işletim sistemi bilgisinin görüldüğü belirtilmiştir. Ancak, Linux işletim sistemine aşina olan herkes bilir ki kullanılan kodlara ait bir çok parametre eklenebilir. "uname –or" komutu ile sadece işletim sisteminin versiyon ve isim bilgisi görüntülenebilirken "uname –a" komutu kullanılması durumunda işletim sistemine ait tüm elde edilebilir bilgiler görüntülenebilmektedir. Aşağıda örnek ekran görüntüsüne yer verilmiştir. Dikkat edileceği üzere işletim sistemine ait tarih bilgisi de söz konusu komut kullanılmış olsaydı görülebilecekti. Eğer adli bilişim uzmanları tarafından yapıldıysa söz konusu işlem, işletim sisteminin tarih bilgisinin görüntülenmemesi için kasıtlı olarak "uname-or" komutunun kullanıldığı anlaşılmaktadır.



Şifre değeri geçilerek işletim sistemi açılmıştır. Açılan işletim sisteminin Linux işletim sistemi sürüm bilgisi elde edebilmek için terminal (komut istemci) açılarak komut satırına **"uname -or"** komutu yazılmış ve yüklü işletim sisteminin, **3.17.4-porteus GNU**/Linux olduğu görülmüştür.



Ayrıca Porteus Linux işletim sistemi üzerindeki dosya sistemi ile biçimlendirilmiş alanlara ait bilgiye terminal ekranında **"lsblk"** komutu yazılarak listelenmiş olup ekran alıntısına aşağıda yer verilmiştir.



Lsblk komutu ile listelenen bölüm ve kapasite bilgilerinde disk ismi "sdb" olarak isimlendirilmiş olup 25.1 G kapasiteli **SDB1**, 14.9 G kapasiteli **SDB2**, 568 M kapasiteli **SDB3** ve 19.1 G kapasiteli **SDB4** alanlarından oluşmaktadır.

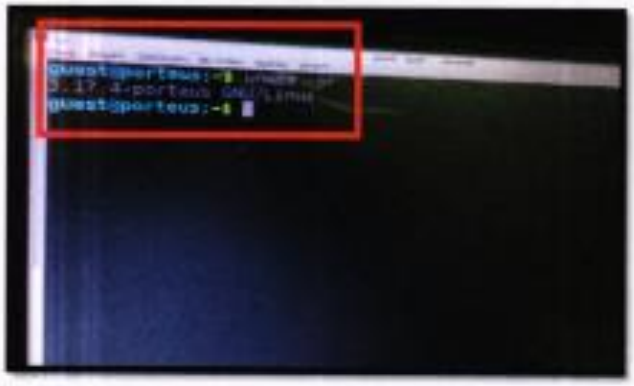
5. Aynı raporun 4.sayfasında "Porteus Linux işletim sisteminde yapılan incelemeler neticesinde Linux işletim sisteminin en alt katman olduğu" belirtilmiştir. Belirtilen söz konusu ibare mantık olarak geçersizdir. Zira bir işletim sistemi zaten başlı başına bir yönetim arabirimi olarak kendisi katmandır. İşletim sistemleri (Windows, Linux, Macos vs.) işletim sistemleri kullanıcı ile donanım arasında bir yazılım katmanı olmakla birlikte kendi içlerinde mimari özellikleri değişmektedir. Raporun devamında söz konusu işletim sistemi üzerinde "2 (iki) tane Windows işletim sisteminin VirtualBox sanallaştırma uygulamasında yüklü olduğu görülmüştür" ibaresi olduğu görülmektedir. Söz konusu ibareden Porteus isimli Linux işletim sisteminde VirtualBox sanallaştırma uygulamasının yüklü olduğu anlaşılmaktadır. Ancak söz konusu programın version numarasına yer verilmemiştir. Programın version numarasının ne olduğu, çalıştırabileceği sanal işletim sistemlerinin de bilinmesini sağlayacaktır. Ancak bu duruma yer verilmemiştir.

Sanal işletim sistemlerinin Windows 8.1 olduğu belirtilmiştir. **Ancak sanal işletim sistemlerinin** hangisinin hangi tarihte kurulduğu, device bilgileri, partition bilgileri, os bilgileri (product name, Register owner, System root, Product Id, insatll date), diğer kullanıcı bilgileri (user name, Security Identifier, Last passeord change Time, Last logon, Last Failede logon,Logon count vs.) **bilgilerine yer verilmemiştir. Oysa bu bilgiler çok önemlidir. Bir işletim sistemi hakkında verilecek bilgiler verinin bütünlüğünün korunup korunmadığı, her hangi bir veri değiştirilip yahut ekleme, çıkarma yapılıp yapılmadığı ile ilgili olarak intiba oluşturulmasında büyük etkendir. Raporu yazan birim olan Siber Suçlarla Mücadele Daire Başkanlığı, Adli Bilişim Şube Müdürlüğünün daha önceki raporları istenildiğinde aslında bu bilgilere yer verildiği görülecektir. Ancak bahse konu raporda bu bilgilere yer verilmemesi, bilmediklerinden değil bilhassa bilinmesini istemediklerinden olduğu aşikardır.**

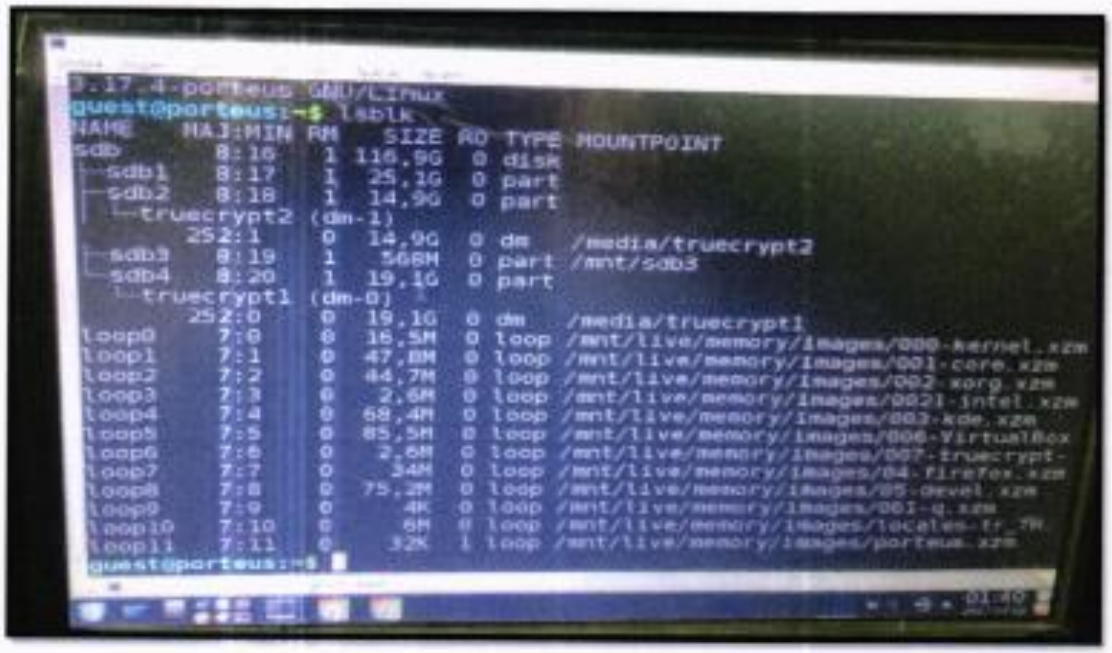
Ayrıca raporun ilgili sayfasında belirtilen "Windows işletim sistemine sahip sanal makinalarda can isimli kullanıcının oluşturulduğu.." ibaresi ile işletim sisteminin açıldığı ve içerisine giriş yapıldığı görülmektedir. Ancak; bir işletim sistemi açıldığında kullanıcı şifresinin olması büyük olasılıktır. Kaldı ki gizli tanıktan elde edilen sd kart üzerinde yapılan bir çalışma olduğu ve soruşturma konusu ile dijital materyalin içerdiği iddia edilen bilgiler göz önüne alındığında, işletim sisteminde kullanıcı şifresinin olmaması beklenemez. Hatta şifrenin basit, tahmin edilebilir olması da beklenemez. Dikkat edilirse, işletim sistemine girişte şifre olup olmadığı bilgisine yer verilmemiş adeta ne kadar az bilgi verilirse o kadar faydalı mantalitesi ile hareket edildiği görülmektedir. Sorulması gereken en haklı soru; işletim sisteminde şifre var mıydı? Var ise şifre nasıl bilindi ? Şifre bilinmiyordu ise nasıl çözüldü ? Hangi yöntem kullanıldı ? Yoksa şifre daha önceden mi biliniyordu ? Şifre ile ilgili bir bilgiye niçin yer verilmedi ?

Bir diğer konu ise raporda Windows işletim sisteminde *(hangisi olduğuna yer verilmemiş)* TrueCrypt şifresinin olduğu bilgisine yer verilmiştir. (***TureCrypt Nedir ?*** *(Anında şifreleme (OTFE) için kullanılan, ücretsiz bir yardımcı programdır. Bir dosya içinde sanal şifreli bir disk oluşturabilir veya bir bölümü veya tüm depolama aygıtını şifreleyebilir (önyükleme öncesi kimlik doğrulama), çok güçlü şifreleme algoritmaları kullanılmaktadır. (AES, Serpent, Triple DES, Twofish, AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES, Twofish-Serpent) TrueCrypt şifrelemeleri halen çözülebilmiş değildir. Ancak şifrelerin tahmin edilmesi yöntemi kullanılabilir ki bu da günümüz teknolojileri ile pek mümkün değildir.))*

Şifre değeri geçilerek işletim sistemi açılmıştır. Açılan işletim sisteminin Linux işletim sistemi sürüm bilgisi elde edebilmek için terminal (komut istemci) açılarak komut satırına **"uname -or"** komutu yazılmış ve yüklü işletim sisteminin, **3.17.4-porteus GNU**/Linux olduğu görülmüştür.



Ayrıca Porteus Linux işletim sistemi üzerindeki dosya sistemi ile biçimlendirilmiş alanlara ait bilgiye terminal ekranında **"lsblk"** komutu yazılarak listelenmiş olup ekran alıntısına aşağıda yer verilmiştir.



Lsblk komutu ile listelenen bölüm ve kapasite bilgilerinde disk ismi "sdb" olarak isimlendirilmiş olup 25.1 G kapasiteli **SDB1**, 14.9 G kapasiteli **SDB2**, 568 M kapasiteli **SDB3** ve 19.1 G kapasiteli **SDB4** alanlarından oluşmaktadır.

6. **Aynı raporun 5.sayfasında**; yukarıda yer verildiği üzere TrueCrypt programından bahsedilerek **" TrueCrypt ile şifreli olduğu görülen Windows sanal makinanın şifre değeri geçilerek gizli veri alanlarını aktif duruma getirilmiştir."** İbaresine yer verilmiştir. Öncelikle bilişim alanında az çok bilgi sahibi olan herkes bilir ki **"şifre değerinin geçilmesi" diye bir şey yoktur.** Şifreli verilere ancak 2 (iki) şekilde erişilebilir. İlki şifre biliniyordur ve ilgili alana bilinen şifre değeri yazılarak veriye erişilir. İkinci yöntem ise şifre bilinmiyordur ancak şifre programları ve yeterli donanımlarla *(bilgisayar işlemcisi, ekran kartları veya özel FPGA kartlar)* şifre tahmin edilmeye çalışılır. İkinci yöntemin de kendi aralarında farklı metotları vardır bunlar, brute force(kaba saldırı), dictionary atacc (Sözlük saldırısı) , Rainbow Table (hash kullanımı), Hybrid (sözlük saldırısına özel karakter ekelme) gibi yöntemler kullanılarak şifrenin bulunması olayıdır. *(Sayfa 22)*

   TrueCrypt ile şifreli bir alan yukarıda bahsedilen şekillerde, şifre her halükarda şifre ekranına yazılarak erişilebilir. Ancak Siber Suçlarla Mücadele Daire Başkanlığı Adli Bilişim Şube Müdürlüğü personeli tarafından hazırlanan inceleme raporunda *(İnceleme raporu 5. sayfa)* görüleceği üzere **şifrenin ne olduğu belirtilmemiş** oysa ilgili birimin önceki şifre çözüleme raporları incelendiğinde şifrelerin ne olduğuna yer verildiği görülecektir.

   İkinci olarak şifrenin daha önceden bilindiği için mi ?, biliniyorsa nasıl bilindiği ?, kim tarafından şifrenin verildiği ?, şifrenin uzunluğunun ne olduğu ?, şifrenin kaç farklı karakter içerdiği ?, şifre programlar sayesinde tahmin edildiyse ne kadar sürdüğü ? programın hangi donanımları kullandığı ?, saniyede kaç şifre denediği ? gibi bilgilerin olmazsa olmaz cevaplanması mutlak suretle gerekli olduğu bir durumdur. Zira daha önce; Yakın geçmişte tanıklık ettiğimiz dijital kumpaslarda, bilhassa Ergenekon ve balyoz davaları, askeri casusluk davalarında dijital verilerin şifreli olduğu ve söz konusu şifrelerin günümüz donanımları ile dahi çözülemeyeceği zira şifrelerin çok uzun ve farklı karakterler içerdiği *(Örn: K24mm3z2m^=s8mhq9T*#-u aşağıda bu şifrenin çözümünün ne kadar zaman alacağına ilişkin tablonun ekran görüntüsüne yer verilmiştir*(Sayfa 22))*, yahut bazı şifrelerin komik olarak nitelendirilecek şekilde "qsxedc123" gibi klavye üzerinde bulunan tuşların yukarıdan aşağıya çapraz veya aşağıdan yukarıya sistematik olacak şekilde oluşturulan şifreler olduğu görülmüştür.

   Açıklanan nedenlere her iki halde de (şifrenin uzun veya tahmin edilebilir şekilde kısa olması) şifrenin ne olduğunun teknik raporda yazılması olayın aydınlatılması açısından elzemdir. **Basit haliyle şifrenin ne olduğu neden gizlenmektedir?**

   Nurettin PAY isimli şüphelinin 04/10/2016 günü Kars Terörle Mücadele Şube Müdürlüğü görevlilerince Müdafi huzurunda alınan şüpheli ifadesinde; "veriler TrueCrypt programı kullanılmak suretiyle 25 farklı karakter kullanılarak şifrelenir" beyanında bulunmuştur Bu bağlamda inceleme raporunda belirtilen "şifre geçilmiştir" ibaresinin geçerli olmadığı ortaya çıkmaktadır. Özetle şifre alanı geçilebilir olsaydı niçin şifreleme programları var olmuştur ?.

1) **CTRL + ALT + O ile açılan işletim sistemine ait ekran görüntüleri**

Yine TrueCrypt ile şifreli olduğu görülen Windows sanal makinanın şifre değeri geçilerek gizli veri alanlarını aktif duruma getirilmiştir.

7. Aynı raporun 6.sayfasında; *"Windows işletim sisteminin açılamsı sonrasında AccessData FTK Imager 3.1.3.2 Lite isimli uluslararası adli bilişim standartlarına uygun portable (kurulumsuz) olarak çalışabilen adli kopya alma yazılımı kullanılmak suretiyle VirtualBox sanallaştırma yönetiminde kurulu Windows işletim sisteminin adli kopyası alınmış olup imaj işlemine ilişkin bilgilere aşağıda yer verilmiştir."* denmektedir. Yapılan işlem özetle şöyledir;

Sandisk Marka Cruzer Glide 3.0 ibareli 128 gb kapasiteli flash bellek içerisinde yer alan lexar marka 64 gb kapasiteli hafıza kartının imajı klonunda, Linux işletim sisteminin çalıştırılması ve içerisinde Windows sanal işletim sistemlerinin bulunması bunlardan birinin (hangisi olduğu belirtilmemiş) yine sanal olarak açılması ve AccessData FTK Imager 3.1.3.2 Lite isimli programın çalıştırılmak suretiyle imajının alınmasıdır.

Yapılan bu işleme ait imaj alma bilgilerine yer verilse de işletim sistemine ait hiçbir bilgiye yer verilmemiştir. *(İşletim sisteminde kullanıcının ne zaman hangi tarihte oluşturulduğu, işletim sistemine ait hangi tarihte kurulduğu, device bilgileri, partition bilgileri, os bilgileri (product name, Register owner, System root, Product Id, insatll date), diğer kullanıcı bilgileri (user name, Security Identifier, Last passeord change Time, Last logon, Last Failede logon,Logon count vs.))* Dolayısıyla işletim sisteminde yer alan hiçbir verinin güvenilir olduğu söylenemez. Raporda genele olarak da hiçbir dosyanın tarih bilgilerine de yer verilmemiş hatta ekran görüntülerinde yer alan dosya bilgileri bölümü bilinçli bir şekilde gizlenmiştir.

Yukarıda belirtilen hususlara ek olarak, raporun yine 6.sayfasında "M" harfi aranmış olan mantıksal alanın TrueCrypt **ile şifreli olduğu ve şifrenin geçildiği belirtilmiştir**. **Şurası açık, net, kesin ve değişmez bir durumdur ki hiçbir şifreli dosya, disk, diskin bir bölümü vb. geçilemez ve böyle bir şey mümkün değildir.** *(bu raporun 21.Sayfasında geniş olarak yer verilmiştir)* Söz konusu şifreli alanın geçilmesi ibaresi tekrar eden bir ibare olarak inceleme raporunda yer aldığı görülmektedir.

Bu durumda şifrenin ne olduğu belirtilmiyor, şifrenin nasıl elde edildiği belirtilmiyor, şifre program marifetiyle tahmin edildiyse hangi donanım ve yazılım kullanıldığı ve söz konusu işlemin ne kadar sürdüğü belirtilmiyorsa, **o halde şifrenin tıpkı Ergenekon, Balyoz ve Askeri Casusluk soruşturmalarında olduğu gibi önceden kolluk görevlileri tarafından bilindiği, bu nedenle izahatının yapılamayacağı ve raporda bu hususa bu yüzden yer verilmediği anlaşılmaktadır.**

Çünkü; Garson kod adlı gizli tanığın ifadelerinde, verilerin şifreli olduğu ve 22 haneli farklı karakterlerden oluştuğunu göz önüne alacak olursak böyle bir şifrenin program kullanılmak suretiyle yeryüzünde var olan en hızlı donanımların bile ulaşamayacağı saniyede yüz trilyon tahmin sayısı olsa bile 1,04 yüz milyon trilyon yüzyılda sonuç elde edebileceği sonucu ortaya çıkmaktadır. Görüleceği üzere bu durum netice almanın imkansız olduğu anlamına gelmektedir. Bir diğer yöntem ise dijital verinin adli bilişi programıyla veriden sözlük oluşturma yöntemidir(Dictionary attac işlemi için). Yani dijital materyal içerisindeki tüm verinin adli bilişim programları vasıtasıyla, bir metin dosyası içerisine metin, rakam ve sembollerden oluşan verinin yazılmasıdır.

Elde edilecek bu metin dosyası, şifre çözümleme programlarına eklenir ve şifreli dosya, disk, disk alanı gibi şifreli verilere sözlük atak yapılması sağlanır. Şifre sözlüğü içerisinde eşleşen bir kayıt olması durumunda program şifrenin bulunduğu uyarısını verir.

Ancak bu yöntem şimdiye kadar yapılan denemelerde pek başarılı olamamıştır. Çünkü, bir kişi eğer bir veriyi şifrelemek yoluyla gizlemek istiyorsa, veriyi şifrelemek için kullandığı şifreyi bilgisayarında muhafaza etmez.

Yani bir dosyaya farklı programlar ile şifre koyup ardından şifreyi bilgisayarda şifresiz bir dosya içerisine yazması beklenemez. Kaldı ki gizlilik prensibini varlık felsefesi haline getiren, bir örgüt olan Fetö terör örgütünün çok gizli bilgiler içerdiği iddia edilen dosyaları ile ilgili böyle bir şey yapması (şifreyi açık bir şekilde bilgisayarda bulundurması) beklenilmesi imkansız olan bir durumdur.

Aşağıda Sakarya Cumhuriyet Başsavcılığının 2018/26648 soruşturma numaralı 2018/7235 Esas ve 2018/1186 numaralı iddianamesinde;

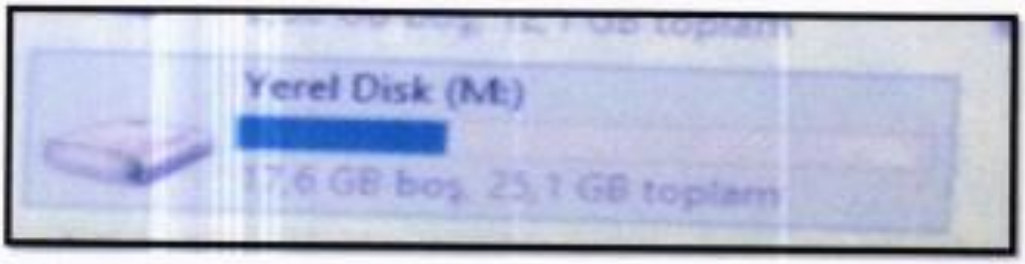
"FETÖ /PDY silahlı terör örgütü tanımı ve Kars Cumhuriyet Başsavcılığınca FETÖ/PDY ye yönelik olarak yürütülen 2016/3303 sayılı soruşturma kapsamında hakkında adli işlem yapılan Nurettin PAY isimli şahsın 04/10/2016 günü Kars Terörle Mücadele Şube Müdürlüğü görevlilerince Müdafi huzurunda alınan şüpheli ifadesi akışında özetle; " denilerek şüphelinin ifadesine yer verilmiştir. *"**Bir bilgisayara True Crypte programı kurulur. Bu program aracılığıyla Flash veya SD card komple şifrelenir. Şifreleme yapılırken 25 farklı karakter (noktalama işaretleri, büyük ve küçük harflere dikkat edilir) kullanılır.** Gönderilecek belge bu Flash veya SD card'ın içine atılır. Gönderilecek belge Flash veya **SD cardın içerisindeyken bu belge resim, müzik veya film dosyasına çevrilir. Ayrıca bu Flash veya SD card içerisine yaklaşık 100 adet normal resim, müzik veya film dosyası atılarak Flash veya SD card SULANDIRILIR. "* görüleceği üzere şifreleme işleminde 25 farklı karakter kullanıldığı şüpheli tarafından beyan edilmiştir.

Windows işletim sisteminin açılması sonrasında "AccessData FTK Imager 3.1.3.2 Lite" isimli uluslararası adli bilişim standartlarına uygun portable (kurulumsuz) olarak çalışabilen adli kopya alma yazılımı kullanılmak suretiyle VirtualBox sanallaştırma yönetiminde kurulu Windows işletim sisteminin adli kopyası alınmış olup imaj işlemine ilişkin bilgilere aşağıda yer verilmiştir.

İmaj Alma İşlemi	
İmaj Başlama Zamanı	Wed Apr 19 19:23:42 2017
İmaj Bitiş Zamanı	Wed Apr 19 20:16:24 2017
MD5 Hash Değeri	8c1fb40dbf9b4e0324238b6becad5fb7
SHA1 Hash Değeri	0ed65346711e958c215c24dc1d24095032edda19
MD5 Hash Değeri Doğrulama	8c1fb40dbf9b4e0324238b6becad5fb7
SHA1 Hash Değeri Doğrulama	0ed65346711e958c215c24dc1d24095032edda19

"Ctrl + alt + o" kısa yol tuşları ile birlikte açılan ve TrueCrypt şifresi geçilen Windows işletim sistemine ait "can" isimli kullanıcının masa üstü görüntüsüne yukarıda yer verilmiştir.

"Arşiv" isimli disk kısa yolunun kullanıcı masa üstünde olduğu görülmüştür. Arşiv isimli alanın kısa yolu incelendiğinde, Porteus Linux üzerinden "sdb1" isimli alanın 25.1 GB kapasiteye sahip olduğu ve ayrı bir alan olarak tanımlandığı görülmüştür. Sdb1 isimli alan Arşiv olarak isimlendirilmiş olup içerisinde birçok ofis dokümanı ve belge barındırdığı görülmüştür. Sdb1 isimli alana ait Arşiv diskinin "ctrl + alt + o" kısa yol tuşları ile açılan Windows işletim sisteminde "M" isimli mantıksal alan olarak görüldüğü tespit edilmiş olup ekran alıntısına aşağıda yer verilmiştir.



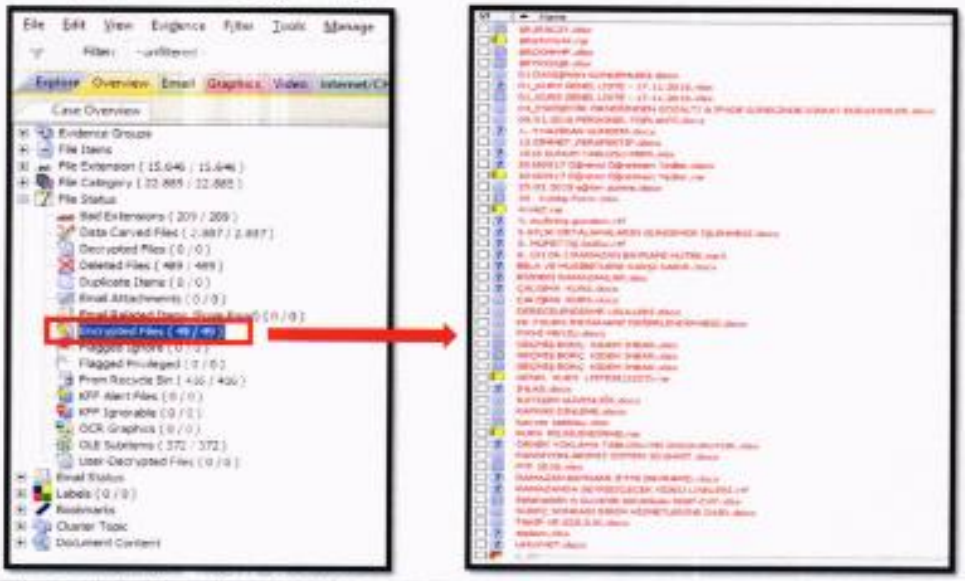
2) TrueCrypt şifresi geçilerek kullanımı aktif hale getirilen işletim sistemindeki Arşiv isimli alana ait adli kopya alma işlemi;

İmaj Alma İşlemi	
İmaj Başlama Zamanı	Thu Apr 20 15:33:04 2017
İmaj Bitiş Zamanı	Thu Apr 20 17:40:29 2017
MD5 Hash Değeri	adc2b0a00d63e14f6b139101a5f5d5e8
SHA1 Hash Değeri	d9146d873574ac87e0c920de82580e3780c3d674
MD5 Hash Değeri Doğrulama	adc2b0a00d63e14f6b139101a5f5d5e8
SHA1 Hash Değeri Doğrulama	d9146d873574ac87e0c920de82580e3780c3d674

8. Aynı raporun 7.sayfasında; “Arşiv” isimli alanın adli kopyası üzerinde yapılan inceleme sonucunda 22.885 adet dosyanın bulunduğu, 13.346 adet doküman dosyası, 59 adet çalıştırılabilir formatta dosya, 923 adet grafik dosyası, 4 adet sunum dosyası, 368 adet elektronik tablolama dosyasının bulunduğu belirtilmektedir. Bununla birlikte 49 adet şifreli dosya olduğu belirtilmekte ve inceleme programına ait ekran görüntüsüne yer verilmiştir. Ekran görüntülerinden anlaşılacağı üzere; Dosyalara ait bilgileri içeren sütunlara yer verilmemiştir. Olması gereken bilgiler ise; Oluşturma tarihi, son erişim tarihi, hash bilgileri (dijital imza), oluşturan kullanıcı bilgisi, dosya boyutları vb. bilgilerdir. Söz konusu bilgiler adli bilişim incelemelerinde veri bütünlüğü açısından olmazda olmaz bir husustur.

Bahse konu soruşturma kapsamında tespiti yapılan "Arşiv" isimli alanın adli kopyası üzerinde "AccessData Forensic Toolkit Version 6.2.1.10" ile yapılan incelemeler sonucu 22885 adet dosyanın bulunduğu ve bu dosyalardan 13346 adet doküman dosyası, 59 adet çalıştırılabilir formatta dosya, 923 adet grafik dosyası, 4 adet sunum dosyası, 368 adet elektronik tablolamama dosyasının bulunduğu görülmüştür.

Yine "Arşiv" isimli alanın adli kopyası üzerinde yapılan incelemelerde 49 adet şifreli dosya ve 489 adet silinmiş dosyanın bulunduğu görülmüştür.



9. Aynı raporun 8.sayfasında yine Windows işletim sistemine ait adli kopyanın alındığı belirtilmiş ancak işletim sistemine ait hiçbir bilgiye yer verilmemiştir.

Ayrıca "Arşiv" isimli alanın adli kopyası üzerinde yapılan işlemlerde yukarıda ekran alıntısında da yer alan 49 adet şifreli dosyaya yönelik yapılan şifre çözümleme işlemlerinde şifreli dosyaların birçoğunda başarılı sonuç alınmıştır. Yine adli kopya üzerinde yapılan incelemelerde "\NONAME [NTFS]\[root]\as.pptx" ile "\NONAME [NTFS]\[root]\as2.pptx" isimli dosyalar tarafımızca incelendiğinde kimlik bilgilerinin değiştirilmiş olduğundan veri tipinin "Passware Recovery Kit Forensic" şifre kırma yazılımınca TrueCrypt dosyasına benzediği görüldüğünden şifre çözümleme işlemleri devam etmektedir.

3) CTRL + ALT + N ile açılan işletim sistemine ait ekran görüntüleri

"Ctrl + alt + n" kısa yol tuşları ile birlikte açılan Windows işletim sistemine ait "can" isimli kullanıcının masa üstü görüntüsüne yukarıda yer verilmiştir.

Yazma korumalı LEXAR marka 64 GB kapasiteli hafıza kartının birebir kopyası bulunan Sandisk marka 128 GB kapasiteli USB bellek canlandırılarak üzerindeki sanal Windows işletim sisteminin açılması sonrasında "AccessData FTK Imager 3.1.3.2 Lite" isimli uluslararası adli bilişim standartlarına uygun portable (kurulumsuz) olarak çalışabilen adli kopya alma yazılımı kullanılmak suretiyle VirtualBox sanallaştırma yönetiminde kurulu Windows işletim sisteminin adli kopyası alınmış olup imaj işlemine ilişkin bilgilere aşağıda yer verilmiştir.

İmaj Alma İşlemi	
İmaj Başlama Zamanı	Wed Apr 19 17:35:42 2017
İmaj Bitiş Zamanı	Wed Apr 19 18:28:20 2017
MD5 Hash Değeri	613b6580fa970f675278bc4666cdaa16
SHA1 Hash Değeri	368945512e0906fe960891435ac12b5c96cc4b13
MD5 Hash Değeri Doğrulama	613b6580fa970f675278bc4666cdaa16
SHA1 Hash Değeri Doğrulama	368945512e0906fe960891435ac12b5c96cc4b13

10. **Aynı raporun 9.sayfasında;** Sonuç ve Değerlendirme başlığı altında inceleme raporu hakkında bilgilere yer verildiği görülmektedir. *""Arşiv" isimli alanın adli kopyası üzerinde yapılan işlemlerde yukarıda şifreli dosyaların olduğu ekran alıntısında da yer alan 49 adet şifreli dosyadan 32 adet dosya "AccessData Forensic Toolkit Version 6.2.10" yazılımı ile export (dışa aktarım) yapılmıştır. 17 adet şifreli dosyanın kimlik bilgileri yazılım tarafından görülemediğinden çıkartılamamıştır. 32 adet şifreli dosyaya yönelik yapılan şifre çözümleme işlemlerinden 27 adet dosyada başarılı sonuç alınmıştır. Hali hazırda 5 adet şifreli dosyaya yönelik şifre çözümleme işlemleri devam etmektedir. "* denilmektedir.

Görüleceği üzere; 32 adet dosyadan 27 sinden başarılı sonuç alınmıştır denilmektedir. Ancak şifrelerin çözümlemesi (bulunması) için ne yapıldığına hiç yer verilmemiştir. Bu işlem için hangi programın ve hangi donanımların kullanıldığına da yer verilmemiştir. Dosyaların ne olduğu (hangi tür) da belirtilmemiştir. Dosya türleri üzerinde yapılan şifre denemeleri büyük farklılık göstermektedir.

Örneğin; donanım olarak i5 işlemci ve Nvdia GeForce GTX780 ekran kartı kullanılması durumunda; Ms Office 2007 dosyasında saniyede 16.530 şifre denemesi, Ms Office 2010 dosyasında saniyede 32.870 şifre denemesi, Rar 3 ve 4 versiyonlarında saniyede 16.010 şifre denemesi yapılabilmektedir. Dolayısıyla kullanılan donanım ve yazılımların belirtilmemesi, şifrelerin nasıl çözümlendiğine yer verilmemesi soru işaretleri doğurmakta, en belirgin ihtimalin ise şifrelerin bilindiği neticesi olacaktır.

Bir diğer konu ise; **Raporun 9.sayfası olan Genele Sonuç ve Değerlendirme başlığı altında**, "..*Hali hazırda 5 adet şifreli dosyaya yönelik **şifre çözümleme işlemleri** devam etmektedir…"* denilmekte, ancak **Aynı raporun 5.sayfasında**; "TrueCrypt ile şifreli olduğu görülen Windows sanal makinanın **şifre değeri geçilerek** gizli veri alanlarını aktif duruma getirilmiştir." İbaresine yer verilmiştir. O halde düz mantıkla şifre değeri madem geçilebiliyor 5 adet şifreli dosyanın şifre çözümleme işlemleri neden devam ediyor? Ya da şifre çözümlemeye ne gerek vardır? Görüleceği üzere burada bir çelişki vardır. Şifre değerinin geçilmesi diye bir şey olmadığı konusu bu raporun 27.sayfasında detaylı bir şekilde anlatılmıştır.

Şifre değerinin geçilmesi diye bir şey olmadığı, inceleme raporunu yazan 2 kişi tarafından da bilinmesine rağmen neden bu tabiri kullandıklarının cevabı ise teknik olarak açıklanması gereken bir durum değil bilakis, şifrenin elde edilmesi olayının açıklanamayacak mahiyette olmasındandır. Görüleceği üzere Siber Suçlarla Mücadele Daire Başkanlığı Adli Bilişim şube Müdürlüğü görevlilerince hazırlanan inceleme raporu, kendi içinde çelişkiler, teknik manipülasyonlar, soru işaretleri ve veri gizlemenin yanı sıra, önceden hazırlanmış, müdahale edilmiş, veri bütünlüğünün bozulmuş olma şüphelerini bariz bir şekilde ortaya koymaktadır.
Aşağıda söz konusu raporun 9.sayfasına ait ekran görüntüsüne yer verilmiştir.

MATERYALE AİT TEKNİK BİLGİLER

(SAMSUNG Marka 32 GB Kapasiteli Hafıza Kartı)

Bahse konu Samsung marka 32GB kapasiteli "MİCRO SD HC I" ibareli hafıza kartının alınan adli kopyası üzerinde yapılan incelemelerde anlamlı veri görülemediği bununda sebep bahse konu SD kart üzerinde herhangi bir inceleme işlemi gerçekleştirilememiştir. Alınan adli kopyaya ait bilgilere aşağıda yer verilmiştir.

İmaj Alma İşlemi	
İmaj Başlama Zamanı	Wed Apr 19 1:14:50 2017
İmaj Bitiş Zamanı	Wed Apr 19 1:40:07 2017
MD5 Hash Değeri	39823595e8a14db7d592ba1b1188aeb8
SHA1 Hash Değeri	36ecddf5bb74cbc9e5b3d4853850240a31ece1c3
MD5 Hash Değeri Doğrulama	39823595e8a14db7d592ba1b1188aeb8
SHA1 Hash Değeri Doğrulama	36ecddf5bb74cbc9e5b3d4853850240a31ece1c3

SONUÇ ve DEĞERLENDİRME

Ankara Cumhuriyet Başsavcılığı Anayasal Düzene Karşı İşlenen Suçlar Soruşturma Bürosunun 18.04.2017 tarih ve 2017/68532 numaralı soruşturması ile Ankara 5.Sulh Ceza Hâkimliğinin 2017/2920 D.İş kararına istinaden gizli tanık olarak GARSON(K) isimli şahıstan ele geçen LEXAR marka 64GB kapasiteli hafıza kartı ve SAMSUNG Marka 32 GB kapasiteli hafıza kartı Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığının "62018024-87055.(63044)/2017-68532" sayılı yazısı ile incelenmesi talep edilmiştir.

Tarafımızca LEXAR marka 64GB kapasiteli hafıza kartının alınan adli kopyası üzerinde yapılan çalışmalar sonucu şifreli kısımlar geçilerek veriler üzerinde herhangi bir çalışma, değerlendirme yapılmaksızın soruşturmacı birim tarafından kullanılmak üzere anlamlı hale getirilmiş olunup çıkarım yapılarak ekte sunulmuştur.

Ayrıca SAMSUNG Marka 32 GB kapasiteli hafıza kartının alınan adli kopyası üzerinde yapılan çalışmalar sonucu anlamlı veri elde edilememiştir.

"Arşiv" isimli alanın adli kopyası üzerinde yapılan işlemlerde yukarıda şifreli dosyaların olduğu ekran alıntısında da yer alan 49 adet şifreli dosyadan 32 adet dosya "AccessData Forensic Toolkit Version 6.2.1.10" yazılımı ile export (dışa aktarım) yapılmıştır. 17 adet şifreli dosyanın kimlik bilgileri yazılım tarafından görülemediğinden çıkartılamamıştır. 32 adet şifreli dosyaya yönelik yapılan şifre çözümleme işlemlerinde 27 adet dosyada başarılı sonuç alınmıştır. Hali hazırda 5 adet şifreli dosyaya yönelik şifre çözümleme işlemleri devam etmektedir.

Yine adli kopya üzerinde yapılan incelemelerde "\NONAME [NTFS]\[root]\as.pptx" ile "\NONAME [NTFS]\[root]\as2.pptx" isimli dosyalar tarafımızca incelendiğinde kimlik bilgilerinin değiştirilmiş olduğundan veri tipinin "Passware Recovery Kit Forensic" şifre kırma yazılımınca TrueCrypt dosyasına benzediği görüldüğünden şifre çözümleme işlemleri devam etmektedir.

İncelemeler neticesinde elde edilen tüm dosyalar dışa aktarım (export) yapılarak rapor ekinde bulunan MAXTOR marka NM12B3RA barkod numaralı 1 TB kapasiteli harici disk içerisinde sunulmuştur.

Arz ederiz. 05/06/2018 saat 10:30.

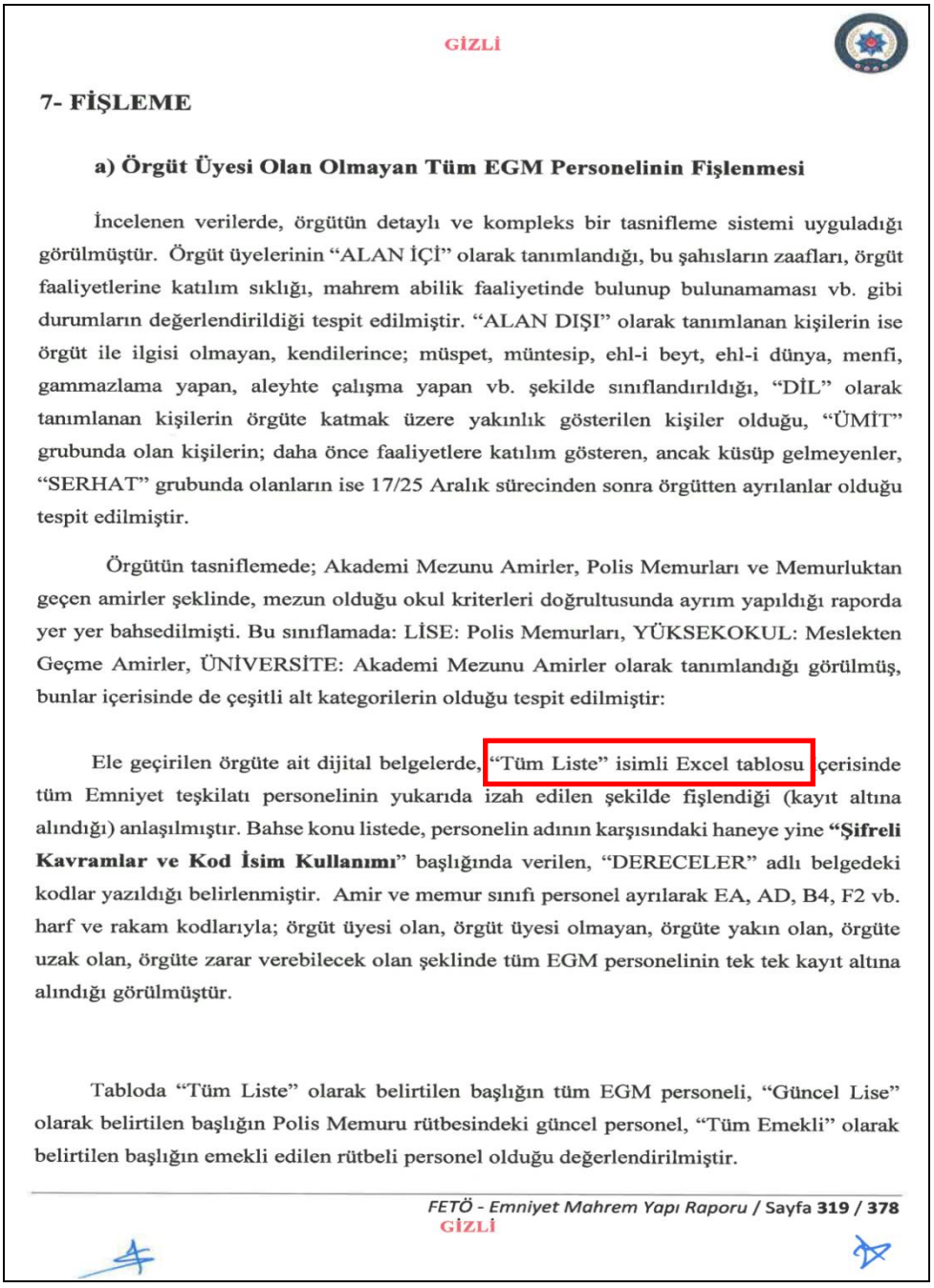
[redacted]
Polis Memuru
Adli Bilişim Görevlisi

[redacted]
Polis Memuru
Adli Bilişim Görevlisi

Sd Kart içindeki Fişlemeler- Kom Daire Raporu

Kaçakçılık ve Organize suçlarla mücadele daire başkanlığı görevlilerince 16.08.2017 tarihinde "FETÖ SİLAHLI TERÖR ÖRGÜTÜ EMNİYET MAHREM YAPILANMASI RAPORU" ismi ile oluşturulan; Fetö terör örgütünün tanımı, ideoloji, örgütlenme, gizlilik, çalışma biçimleri ve örgüte ait diğer bilgiler ile değerlendirmelere yer verilen bu raporda, Emniyet personelinin örgüt tarafından fişlendiği ve fişlemelerin kodlama yöntemiyle yapıldığı bilgisine yer verilmiştir. Söz konusu raporun ilgili sayfaları adli bilişim teknikleri açısından incelenerek tespit ve değerlendirmelere yer verilecektir.

1. Aşağıda KOM daire başkanlığı görevlilerince hazırlanana raporun 319.sayfasına yer verilmiştir. Raporun ilgili sayfasında; "Ele geçirilen örgüte ait dijital belgelerde, "**Tüm Liste**" isimli Excel tablosu içerisinde tüm Emniyet teşkilatı personelinin yukarıda izah edilen şekilde fişlendiği (kayıt altına alındığı) anlaşılmıştır" denilmektedir. Burada belirtildiği üzere dijital materyal içerisinde "Tüm Liste" isimli bir excel dosyasının olduğu belirtilmektedir.



GİZLİ

7- FİŞLEME

a) Örgüt Üyesi Olan Olmayan Tüm EGM Personelinin Fişlenmesi

İncelenen verilerde, örgütün detaylı ve kompleks bir tasnifleme sistemi uyguladığı görülmüştür. Örgüt üyelerinin "ALAN İÇİ" olarak tanımlandığı, bu şahısların zaafları, örgüt faaliyetlerine katılım sıklığı, mahrem abilik faaliyetinde bulunup bulunamaması vb. gibi durumların değerlendirildiği tespit edilmiştir. "ALAN DIŞI" olarak tanımlanan kişilerin ise örgüt ile ilgisi olmayan, kendilerince; müspet, müntesip, ehl-i beyt, ehl-i dünya, menfi, gammazlama yapan, aleyhte çalışma yapan vb. şekilde sınıflandırıldığı, "DİL" olarak tanımlanan kişilerin örgüte katmak üzere yakınlık gösterilen kişiler olduğu, "ÜMİT" grubunda olan kişilerin; daha önce faaliyetlere katılım gösteren, ancak küsüp gelmeyenler, "SERHAT" grubunda olanların ise 17/25 Aralık sürecinden sonra örgütten ayrılanlar olduğu tespit edilmiştir.

Örgütün tasniflemede; Akademi Mezunu Amirler, Polis Memurları ve Memurluktan geçen amirler şeklinde, mezun olduğu okul kriterleri doğrultusunda ayrım yapıldığı raporda yer yer bahsedilmişti. Bu sınıflamada: LİSE: Polis Memurları, YÜKSEKOKUL: Meslekten Geçme Amirler, ÜNİVERSİTE: Akademi Mezunu Amirler olarak tanımlandığı görülmüş, bunlar içerisinde de çeşitli alt kategorilerin olduğu tespit edilmiştir:

Ele geçirilen örgüte ait dijital belgelerde, "Tüm Liste" isimli Excel tablosu içerisinde tüm Emniyet teşkilatı personelinin yukarıda izah edilen şekilde fişlendiği (kayıt altına alındığı) anlaşılmıştır. Bahse konu listede, personelin adının karşısındaki haneye yine **"Şifreli Kavramlar ve Kod İsim Kullanımı"** başlığında verilen, "DERECELER" adlı belgedeki kodlar yazıldığı belirlenmiştir. Amir ve memur sınıfı personel ayrılarak EA, AD, B4, F2 vb. harf ve rakam kodlarıyla; örgüt üyesi olan, örgüt üyesi olmayan, örgüte yakın olan, örgüte uzak olan, örgüte zarar verebilecek olan şeklinde tüm EGM personelinin tek tek kayıt altına alındığı görülmüştür.

Tabloda "Tüm Liste" olarak belirtilen başlığın tüm EGM personeli, "Güncel Lise" olarak belirtilen başlığın Polis Memuru rütbesindeki güncel personel, "Tüm Emekli" olarak belirtilen başlığın emekli edilen rütbeli personel olduğu değerlendirilmiştir.

FETÖ - Emniyet Mahrem Yapı Raporu / Sayfa **319** / **378**

GİZLİ

2. 23.07.2018 tarihinde KOM (Kaçakçılık ve Organize Suçlarla Mücadele) daire başkanlığı Ulusal Güvenliğe yönelik Suçlarla Mücadele Şube müdürlüğünde görevli kişi tarafından oluşturulan rapor içeriğinde, Ankara Cumhuriyet Başsavcılığı Anayasal Düzene karşı işlenen suçlar soruşturma bürosunun 18.04.2017 tarih ve 2017/68532 numaralı soruşturması ile Ankara 5.Sulh ceza hâkimliğinin 2017/2920 D.iş kararına istinaden gizli tanık olarak GARSON (k) isimli şahıstan ele geçen LEXAR marka 64 GB kapasiteli hafıza kartının adli kopyası içerisinde yer aldığı belirtilen ve içerisinde, tüm Emniyet teşkilatı personelinin fişleme bilgilerinin yer aldığı belirtilen dosyaların bulunduğu klasör ve dosya isimlerinin olduğu görülmektedir;

RAPOR

Ankara Cumhuriyet Başsavcılığının 18.04.2018 tarih ve 2017/68532 sayılı soruşturma talimat kapsamında gizli tanık GARSON(K) isimli şahıstan alındığı bildirilen;

1- Siyah renkli, üzerinde Samsung 32gb Micro SD HC I,
2- Beyaz açık kahve renkli, üzerinde Lexar 1000x 64gb Micro SD XC II,
3- Samsung marka SM-A510F model beyaz renkli gövde arka kapağında 357765/07/561383/3 İMEİ S/N: R58H61ZYLEF numaralı cep telefonu,

Hakkında Ankara 5. Sulh Ceza Hâkimliğinin 2017/2920 D.iş sayılı kararı gereğince inceleme yapılarak, yapılacak inceleme sonucu ele geçirilecek verilerin metin haline getirilmesi, kopyasının alınması ve hazırlanacak rapor ile eşyaların gönderilmesi istenmiştir.

21.04.2018 tarih ve 2017/2632151-74190 sayılı yazımız ile alınan materyallerin iki ayrı imajının alınarak bir imaj diskin Cumhuriyet Başsavcılığınıza gönderildiği, diğer imaj diskin ise Ulusal Güvenliğe yönelik Suçlarla Mücadele Şube Müdürlüğümüzce çelik kasa içerisinde muhafaza altına alındığı bildirilmiştir.

Konu ile ilgili olarak yukarıda özellikleri yazılı materyaller ile ilgili olarak Ankara Cumhuriyet Başsavcılığının 18.04.2018 tarih ve 2017/68532 sayılı talimatı gereği ilgi Siber Suçlarla Mücadele Daire Başkanlığının 05.07.2018 tarih ve 25984256-83041-(22171) 6750-126991 sayılı yazısı ile 1 ve 2 nolu materyaller hakkında tanzim edilen İnceleme Raporu (9 sayfa) rapor ile Maxtor marka NM12B3RA barkod numaralı hard disk ve 3 numaralı materyal hakkında tanzim edilen Teknik Çıkarım (Export) Raporu ile eki bir adet CD, daha önce Ulusal Güvenliğe yönelik Suçlarla Mücadele Şube Müdürlüğümüzce çelik kasa içerisinde muhafaza altına alındığı bildirilen bir adet imaj diskin Ankara Cumhuriyet Başsavcılığının 2017/68532 sayılı soruşturma dosyasına gönderilmesi gerekmektedir.

Daire Başkanlığımızca hazırlanan "*FETÖ Silahlı Terör Örgütü Emniyet Mahrem Yapılanması Raporu*"nda ayrıntıları ile bildirildiği üzere ele geçirilen veriler içerisinde bulunan bir kısım verilerin ülkemiz genelinde yürütülmekte olan ve kısıtlılık kararı bulunan soruşturmalar ile ilgili olduğu ve bu soruşturmaların temelini oluşturan verilerin bulunduğu tespit edilmiştir.

Mevcut haliyle export edilmiş verilerin tamamının paylaşılması durumunda, bu soruşturmanın konusu olmayan veya paylaşıldığında kısıtlılık kararı bulunan soruşturmaların gizliliğinin ihlal etmemize neden olacak bilgiler bulunduğu değerlendirilmektedir.

Bu itibarla yapılan çalışmalarda;

"LİSE SEKRETARYA" klasörü içerisinde yer alan "Güncel Liste 25 Ocak 2016 İHRAÇ ÇALIŞMA. xlsx" isimli veri içerisinde EGM personeli hakkında fişleme verileri ile personelin telefon, sicil, adres ve çalıştığı birim bilgilerinin yer aldığı, liste içerisinde yer alan birçok EGM personeli ile ilgili olarak ülkemiz genelindeki Cumhuriyet Başsavcılıklarınca üzerinde kısıtlılık kararı bulunan soruşturma yürütüldüğü,

"SOSYOLOJİ-PDR USULSÜZ ÇALIŞMALAR" klasörü içerisinde yer alan "Müdahil Olunamayan Alımlar. xlsx" isimli veri içerisinde EGM personeline ilişkin TCKN kimlik bilgilerinin bulunduğu,

"TEOĞ 2016" klasörü içerisinde yer alan "64bin.xlsx" ve "120 000.xlsx" isimli veriler içerisinde ByLock kullanıcı listelerinin ID numaraları ve kullanıcıları ile birlikte yer aldığı, liste içerisinde yer alan birçok şahıs ile ilgili olarak ülkemiz genelindeki Cumhuriyet Başsavcılıklarınca üzerinde kısıtlılık kararı bulunan soruşturma yürütüldüğü,

"LİSE SEKRETARYA" klasörü içerisinde yer alan "2015 ÜMİT.xlsx" isimli veri içerisinde EGM personeli hakkında fişleme verilerinin yer aldığı, liste içerisinde yer alan bir çok EGM personeli ile ilgili olarak ülkemiz genelindeki Cumhuriyet Başsavcılıklarınca üzerinde kısıtlılık kararı bulunan soruşturma yürütüldüğü,

Sayfa **1** / **2**

"YENİ" klasörü içerisinde yer alan "PERSONEL" klasörü içerisinde yer alan "Tüm liste.xlsx" isimli veri içerisinde EGM personeli hakkında fişleme verilerinin yer aldığı, liste içerisinde yer alan bir çok EGM personeli ile ilgili olarak ülkemiz genelindeki Cumhuriyet Başsavcılıklarınca üzerinde kısıtlılık kararı bulunan soruşturma yürütüldüğü,

"YENİ" klasörü içerisinde yer alan "SOSYOLOJİ" klasörü içerisinde yer alan "AKADEMI BILGI. xlsx" isimli veri içerisinde EGM personeli hakkında fişleme verilerinin yer aldığı, liste içerisinde yer alan birçok EGM personeli ile ilgili olarak ülkemiz genelindeki Cumhuriyet Başsavcılıklarınca üzerinde kısıtlılık kararı bulunan soruşturma yürütüldüğü,

"KURS" klasörü içerisinde Ankara Cumhuriyet Başsavcılığına yürütülmekte olan kamuoyunda KPSS soruşturması olarak bilinen 2010/100074 sayılı soruşturma ile ilgili olarak ayrıntılı bilgilerin yer aldığı,

Ayrıca veri içerisinde bir çok kişinin kişisel bilgilerinin (TC Kimlik numarası, Telefon numarası, adres bilgisi vs.) yer aldığı tespit edilmiştir.

Konu ile ilgili olarak; üzerinde kısıtlılık kararı bulunan soruşturmalar dışında, EGM personelinin Sicil, ad soyad, adres, çalıştığı birim vs. gibi birçok bilginini yer aldığı bilhassa terörle mücadele, istihbarat ve KOM birimlerinde aktif çalışmakta olan personelin kimlik bilgilerinin deşifre edilmesinin telafisi olmayan durumlara sebebiyet verebileceği değerlendirilmektedir.

İş bu rapor tarafımdan tanzimli imza altına alınmıştır. 23.07.2018 saat 14.00

282332
Polis Memuru

Yukarıda ekran görüntülerine yer verilen evraklarda belirtilen;

- LİSE SEKRETERYA klasörü içerisinde yer alan **"Güncel Liste 25 Ocak 2016 İHRAÇ ÇALIŞMA.xlsx"** isimli excel dosyası
- SOSYOLOJİ-PDR USULSÜZ ÇALIŞMALAR klasörü içerisinde yer alan **"Müdahil Olunamayan Alımlar.xlsx"** isimli excel dosyası
- LİSE SEKRETERYA klasörü içerisinde yer alan **"2015 ÜMİT.xlsx"** isimli excel dosyası
- YENİ Klasörü içerisinde yer alan "PERSONEL" klasörü içerisinde yer alan **"TümListe.xlsx"** isimli excel dosyası
- YENİ klasörü içerisinde yer alan "SOSYOLOJİ" klasörü içerisinde yer alan **"AKADEMI BILGI.xlsx"** isimli excel dosyaları

İle ilgili olarak gerek KOM daire gerek Siber Suçlarla Mücadele Daire başkanlıklarınca hazırlanan inceleme raporu, rapor vb. evraklarda söz konusu dijital dosyalarla ilgili teknik bilgilere yer verilmemiştir. Oysa dijital bir dosyanın var olduğuna dair teknik bilgiler, veri bütünlüğü açısından elzemdir. Dosyalara ait hash bilgileri *(dijital imza, hash'i hesaplanan veriye özel ve parmak izi gibi benzersiz bir değerdir),* meta data olarak bilinen tarih ve zaman bilgileri, veriyi oluşturan, son erişen ve değiştiren kullanıcıların kim yada kimler olduğu, tarih gibi bilgileri ve en önemlisi ise imaj alma işlemine ait log dosyasına yer verilmemiştir. Bu nedenlerden dolayı yukarıda maddeler halinde yer verilen excel dosyalarının içeriğine değil yalnızca teknik bilgilerinin mahkemeye sunulması gerekmektedir. Aşağıda dosyalara ait talep edilen teknik bilgiler maddeler halinde sıralanmıştır.

1. İmaja ait log dosyası (bu dosya imaj alma işleminin ardından imaj alma işlemin yapan donanım ya da yazılım tarafından oluşturulan, içerisinde sürece ait bilgiler olmak üzere tarih ve saat bilgisi, imajı alınan materyale ait bilgiler, imajın aktarıldığı materyale ait bilgiler, oluşturulan imaj dosyaları, hash değerleri, imaj hataları vb. bilgiler barındırır. **Teknik bilgi dışında bir veri söz konusu olmadığından gizlilik içeren bir veri olduğu öne sürülemez**)

2. Metada Bilgileri (üst veri): Dosya adı, türü, oluşturma tarihi, değiştirme tarihi, son erişim tarihi, sahiplik bilgileri. **Teknik bilgi dışında bir veri söz konusu olmadığından gizlilik içeren bir veri olduğu öne sürülemez**)

3. Dijital materyalin imaj alınması işleminde yapılan görüntü kaydı *(Bilindiği üzere kolluk tarafından ya olay yerinde ya da kolluk birimlerinde imaj alma işlemi yapılmaktadır. Olay yerinde alınıyor ise şüpheli-vekili ve hazurunların nezaretinde imaj alma işlemi gerçekleşir. Kolluk biriminde alınıyorsa, şüpheli veya vekili nezaretinde eğer mümkün değilse kamera kaydı eşliğinde alınmaktadır. Bu konuda Siber Suçlarla Mücadele Daire Başkanlığı Adli Bilişim Şube Müdürlüğünden kamera eşliğinde alınan imajlara ait tutanakların örnek olarak gönderilmesi talep edildiğinde, uygulanan yöntemin var olduğu görülecektir.)*

4. İmaj alma tutanağı (**Teknik bilgi dışında bir veri söz konusu olmadığından gizlilik içeren bir veri olduğu öne sürülemez**)

Yukarıda yer verilen dosyalarla ilgili olarak, dosyaların bulunduğu partition (disk bölümü), file path(dosya konumu) ve metadata (üst veri) bilgileri ile birlikte hash değerlerinin, inceleme yapan birim-talep eden birim(adli bilişim incelemesi yapabilen) tarafından oluşturulan raporlarda yer verilmesi gerekirdi. Zira herhangi bir dijital inceleme yapıldığında, raporda yer verilen dosyalarla ilgili olarak teknik bilgiler tablosu standart olarak yer almaktadır. Aşağıda Siber Suçlarla Mücadele Adli Bilişim Bürolarınca yapılan bir dijital materyal incelemesi neticesinde oluşturulan inceleme raporuna örnek olarak yer verilmiştir.

MATERYALE AİT TEKNİK BİLGİLER

DEVICE (CİHAZ) BİLGİLERİ

Description (Açıklama)	FLYCMPTR
Total Size (Toplam Kapasite)	250.059.350.016 Bytes (232,9 GB)
Total Sectors (Toplam Sektör)	488.397.168
Acquisition MD5 (Edinme MD5)	0xD29582538DC7639C24C73744CF3EACF9
Verification MD5 (Doğrulama MD5)	0xD29582538DC7639C24C73744CF3EACF9

PARTITIONS (BÖLME) BİLGİLERİ

Name (İsim)	Id (Id No)	Type (Tip)	Start Sector (Başlangıç Sektörü)	Total Sectors	Size
	07	NTFS	2.048	716.800	350 MB
	07	NTFS	718.848	306.483.200	146,1 GB
	07	NTFS	307.202.048	181.192.704	86,4 GB

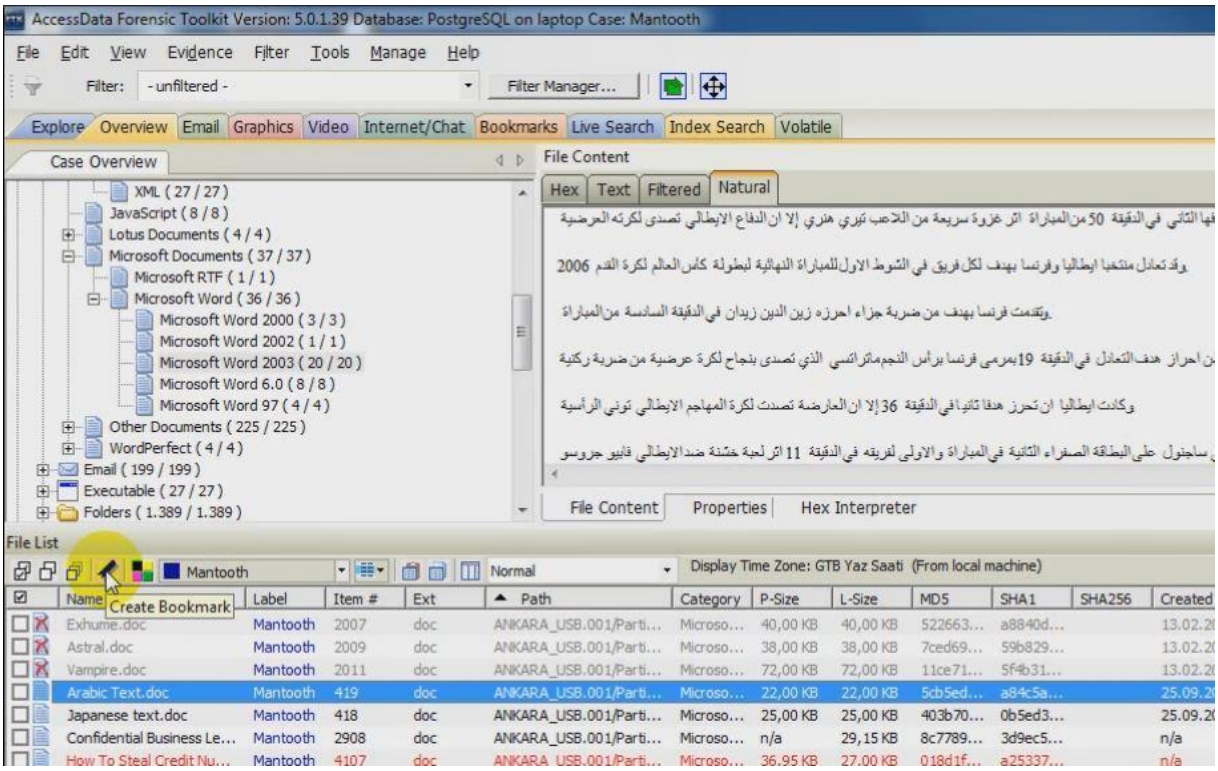
OS (İŞLETİM SİSTEMİ) BİLGİLERİ

Product Name (Ürün Adı)	**Windows Server 2012 Standard**
Registered Owner (Kayıtlı Sahip)	**Windows Kullanıcısı**
System Root (Sistem Kökü)	C:\Windows
Product ID (Ürün Kodu)	40184-30308-00001-AA436
Install Date (Kurulum Tarihi)	25/09/13 16:35:05

İŞLETİM SİSTEMİNE KAYITLI KULLANICI BİLGİLERİ

User Name (Kullanıcı Adı)	Administrator
Security Identifier (Güvenlik Kimliği)	S-1-5-21-3762345826-2132207924-3785302939-500
Last Password Change Time	27.09.2013 12:59:33 +00:00
Last Logon (Son Giriş)	11/03/14 14:45:28
Last Failed Logon (Son Hatalı Giriş)	20.02.2014 13:25:46 +00:00
Logon Count(Giriş Sayısı)	32

Dosya Adı	derlemelerim.tif
Dosya Uzantısı	.tif
Doya Oluşturma T.	26.02.2014 12:14:38 (2014-02-26 10:14:38 UTC)
Değiştirme Tarihi	06.03.2014 08:16:39 (2014-03-06 06:16:39 UTC)
Dosya Boyutu	385122304
Hash Değeri	12374c3342275094b92dd1834dbda141
Dosya Yolu	IMAGE.E01/NONAME[NTFS]/[root]/Users/Admin/Desktop/dosyam



Görüleceği üzere bir dijital materyal incelemesinde materyale ait teknik bilgilerin yanı sıra, inceleme programı üzerinden tespit edilen dosyalara ait ekran görüntüsünde dosya ile ilgili bilgiler görünecek şekilde yer verilir. Bu itibarla gerek KOM gerek SİBER daire başkanlıklarının ilgili şubelerince oluşturulan raporlarda sadece dosya isimlerine yer verilerek dosyaların var olduğuna dair hiçbir destekleyici teknik bilginini olmaması bahse konu dosyalar hakkında şüpheleri akla getirecektir.

GENEL SONUÇ VE DEĞERLENDİRME

Raporda gerek adli bilişim tanımları, uygulamaları, imaj alma, dosya tarih ve zaman bilgilerinin önemi, şifreleme, şifre çözümleme, süre hesapları, dijital verilerde manipülasyon, hash değeri ve önemi, hazırlanan raporlar ve eksiklikleri gibi konulara yer verilmiş olup aşağıda maddelere halinde tespit ve değerlendirmelere yer verilmiştir.

1. Adli bilişim, elektronik ortamlardan elde edilen bulguların, çeşitli teknik donanım ve yazılımlar kullanılarak hukuki delillere dönüştürülme sürecidir. Yapılan işlemler uluslararası uygulamalar ile standart özellikler taşımalıdır. Uygulamalardaki en çok önem verilen ortak hususlardan birisi veri güvenliğinin sağlanması olmuştur.

2. Dijital materyaller üzerinde doğrudan inceleme yapılamaz.*(Write block kullanımı hariç)* İmaj (adli kopya) alma işlemi bitirildikten sonra imaj dosyası üzerinde inceleme yapılır. Böylelikle veri güvenilirliğinin gerektirdiği işlemlerden biri sağlanmış olur aksi halde dijital veri içerisine ekleme, çıkarma, silme gibi işlemlerin yapılmadığının ispatı mümkün olmayacaktır.

3. Unutulmamalıdır ki tarih ve zaman bilgisinde rahatlıkla manipülasyon yapılabilir. Gerek harici bir program kullanılmak suretiyle gerek işletim sistemi tarih ve zaman bilgilerinin değiştirilmesi suretiyle oluşturulan dosyaların tarih ve saat bilgileri kolaylıkla değiştirilebilir. Bu durum uluslararası adli bilişim uygulamalarında artık bilinen sıradan bir bilgidir.

4. İmaj alma işlemi sırasında veya sonrasında olabileceği gibi yalnızca inceleme raporlarında da manipülasyon yapılabilir. Bu durumun en zayıf halkası ilgili bölümde bahsedildiği gibi kontrol sisteminin olmamasıdır. İşlem süreçleri sonrasında ise mahkemece delillerin ortaya konulması gerekmektedir. Delillerin ortaya konulmasından maksat, tanıkların ve bilirkişilerin dinlemesi, keşif yapılması ve **diğer ispat araçlarının ileri sürülmesi, açıklanması, incelenmesi ve tartışılır lığının sağlanmasıdır**. Ortaya konulup tartışılmayan bir delil CMK.nun 217/1. maddesi uyarınca hükme esas alınamaz *(Sayfa 15-16)*

5. Garson (k) isimli gizli tanık, **18.04.2017 tarihinde** Ankara Cumhuriyet Başsavcılığına 2 adet sd kart 1 adet cep telefonu **teslim etmiştir**. Siber Suçlarla Mücadele Daire Başkanlığı Adli Bilişim Şube Müdürlüğünce hazırlanan inceleme raporunun 2.sayfasında, söz konusu iki adet SD karttan Lexar Marka 64 Gb kapasiteli kartın **imajının 19.04.2017 tarihinde alındığı** belirtilmektedir. Bu materyale ait imaj dosyasının incelenerek KOM daire başkanlığına gönderilmesi ise **05.06.2018 tarihinde** yapılmıştır. Ancak haklarında fişleme bilgileri olduğu öne sürülerek 9103 polis memurun görevden uzaklaştırılma tarihi ise **26.04.2017 tarihidir.**

6. Yukarıda yer verilen maddeler bağlamında, **imaj dosyası daha incelenmeden içeriğini görmüş olmaları gibi mantık dışı bir sonuç ortaya çıkmaktadır.** Örnek vermek gerekirse, yerin kaç metre altında olduğu bilinmeyen bir sandığın varlığı tespit edilmiş, daha kazı çalışmaları başlamadan sandığın içerisinde iç içe 6 adet sandık olduğu ve içerisinde sayıları ve türlerine yer verilen mücevherler olduğu iddia edilerek, değerleri belirlenmiş, satışı yapılmış daha sonra kazı çalışmalarına başlanmıştır. Görüleceği üzere benzetme yöntemiyle verilen bu örnekte olduğu gibi, söz konusu sd kart la ilgili olarak da 6 aşamadan oluşan *(imaj alma, imaj içeriğinde Linux işletim sisteminin olduğunu görme, bunun içerisinde de sanal Windows işletim sistemlerinin olduğunu görme, bunun içerisinde de trueCrypt ile şifrelenmiş disk alanlarının olduğunu görme, bunun içinde de klasörler içerisinde excel dosyalarının olduğunu görme ve export-dışa aktarım işlemleri yapıldığı hazırlanan raporlardan anlaşılmaktadır.)* ve tüm süreçlerde ulaşılmak istenen alan-veri-dosya-sistemlerin şifreli olduğu belirtilmiş ve ancak **05.06.2018 tarihinde nihayete eren bir çalışma** neticesinde elde edilen veriler, nasıl oluyorsa **26.04.2017 tarihinden önce elde edilerek,** inceleme ve analiz yapılmak suretiyle, listeler hazırlanarak resmi yazışmalar yapılarak 9103 polis memuru görevden uzaklaştırılmıştır.

a. **Dijital materyalin imaj içeriği incelenmeden, verinin ne olduğu bilinemez**. Kaldı ki imaj dosyası içeriğine hızlıca bakıp verileri görüp daha sonra inceleme raporu tanzim etmek gibi bir durum olsa bile söz konusu sd kart için bunun mümkün olmayacağı, siber suçlarla mücadele daire başkanlığı adli bilişim şube müdürlüğünce hazırlanan inceleme raporundan anlaşılmaktadır. Zira raporun ilgili sayfalarında açıklandığı üzere, sd kart içinde Linux işletim sistemi, bu işletim sistemi içerisinde sanal Windows işletim sistemlerinin bulunması, bu işletim sistemlerinden birinin içerisinde de şifreli (true crypt) disk alanı olduğu ve imajının alındığı daha sonra elde edilen imaj dosyasının incelendiği ve işletim sistemleri başta olmak üzere neredeyse tüm verilerin şifreli olduğu göz önüne alındığında, **inceleme raporu bitmeden imaj dosyasına bakılarak verilere ulaşmak mümkün değildir.**

b. Söz konusu sd kart içerisinde yer aldığı iddia edilen excel dosyaları içerisinde, tüm emniyet teşkilatı personelinin fişlendiği belirtilmektedir. Ancak Sd kartı teslim eden garson kod adlı gizli tanık ve kart içindeki dosyalar ile ilgili olarak adli makamlarca soruşturma, kovuşturma ve karar aşamaları beklenmemiş yani dijital dosyaların-verilerin delil olup olamayacağı konusunda bir karar beklenmesine gerek duyulmamış, etraflıca araştırmak, verilerin elde edilişi şeklinin tespit edilmesi, verileri elde eden kişilerin tespit edilmesi ve olaya bütüncül olarak bakılarak maddi gerçeğe ulaşmak gibi bir gayret, tutum ve davranış yapılmamıştır. Adeta alelacele işlemler yapılmış oldubitti ye getirilmiştir. Gerek KOM gerek Siber suçlar birimlerinin adli bilişim büroları (dijital veri incelemeye haiz birimler) inceledikleri dijital materyallerde, öncelikli olarak soruşturma kapsamında olmak üzere, suç unsuru olabileceği değerlendirilebilecek verileri, tanzim ettikleri inceleme raporunda yer vermek üzere tamamlanan raporu adli makamlara sunmakla görevlidirler. Hukuken yasama, yürütme, yargı erklerinin birbirine üstünlüklerinin olmadığı görev ve yetkilerinin ayrı olduğu ve bu hususların anayasa, yasa ve kanunlar ile düzenleyici işlemlerle belirlenmesi gibi, kolluk kuvvetleri de suç önleme, suçüstü ve suç sonrası durumlarda yetki ve görevlidirler. Bu bağlamda yargı alanına giren ve bir şeyin delil olup olamayacağı kararına yalnızca mahkemelerin karar

verebileceği bir hususla ilgili olarak, kollukça açıkça fonksiyon gaspı (görev gaspı) yapılmıştır.

c. Yukarıda yer verilen hususla ilgili olarak, kolluk tarafından ilgili birimlerce yapılan dijital incelemelerde, tespit edilen bulgulara istinaden hiçbir zaman, hiçbir idari merci tarafından gerek idari yaptırım adı altında gerek idari önlem adı altında şimdiye kadar bir işlem tesis edilmemiştir. Örnek vermek gerekirse; Tehdit-şantaj suçu nedeniyle şüpheli hakkında verilen yakalama, arama-el koyma kararına istinaden, kolluk görevlilerince elde konulan dijital materyalin incelenmesi esnasında, resim ve video dosyaları bulunduğu, bu dosyalardan soruşturmaya konu olabileceği değerlendirilebilecek dosyaların olduğu ve bunların yanı sıra çocuğun cinsel istismarı içerikli videolar oluğunu varsayalım. Video dosyasında istismarı gerçekleştiren kişinin adı, soyadı ve unvanı gibi bilgilerin de başka bir kişi tarafından açıkça söylendiğini, söz konusu kişinin Mili Eğitim bakanlığında görevli bir memur olduğunun konuşmalardan anlaşıldığını varsayalım. Bu durumda kolluk görevlileri söz konusu memurla ilgili olarak Milli Eğitim bakanlığına bildirip ve bakanlığında ilgili kişiyi görevden uzaklaştırdığını varsayalım. Görüleceği üzere böyle bir işlem ne yasalarımızca ne de çağdaş hukuk devletinin gerekleri ile bağdaşmayacaktır. Yapılması gereken ise, tespit edilen bulguların adli makamlara intikal ettirilmesi ve yargı kararlarının sonucunun beklenmesidir. Aksi halde her dijital materyal içerisinde bulunan veri ile ilgili idari işlem yapılacaksa o halde soruşturma ve kovuşturma makamlarına ne gerek vardır. Zira yapılan işlem *(sd kart içerisindeki excel belgeleri içerisinde olduğu iddia edilen ve anayasal suç teşkile eden fişleme bilgilerine istinaden 9103 polis memurunun görevden uzaklaştırılması ve sırf görevden uzaklaştırıldığı için, başka bir idari işlem olan 8 Temmuz 2018 tarihinde KHK ile ihraç edilen polis memurları)* idare tarafından yapılan yargısız infaz ve peşin hüküm işlemidir.

7. Raporun 39, 40 ve 41.sayfalarında yer verildiği üzere, sd kart içerisinde olduğu iddia edilen ve anayasal suç teşkil eden fişleme bilgilerinin yer aldığı excel dosyalarına ait; Metada Bilgileri (üst veri): Dosya adı, türü, oluşturma tarihi, değiştirme tarihi, son erişim tarihi, sahiplik bilgileri*(Teknik bilgi dışında bir veri söz konusu olmadığından gizlilik içeren bir veri olduğu öne sürülemez)*ne KOM ve SİBER birimlerince yer verilmediği, dijital materyale ait imaj alma işlemlerini içeren log dosyasına yer verilmediği, konu ile ilgili olarak yapılan yargılamalarda mahkemelere dahi ne dosya içeriğinin *(gizlilik kaydı bulunduğu gerekçesiyle)* ne de dosyalara ait yukarıda yer verilen teknik özelliklerinin yer verilmediği, aksine şeffaflıktan çok uzak işlem süreçlerinin ısrarla gizlilik bahanesiyle saklandığı görülmektedir. **Tüm hususlar göz önüne alındığında anlaşılacağı üzere tek mantıklı açıklaması; teslim edilen SD kart, imaj alma işlemi yapılmadan incelenmiş, bu itibarla dosyaların erişim bilgileri ve değiştirme tarihi bilgileri değişmiş olduğundan, gerek KOM gerek SİBER daire başkanlıklarınca hazırlanan raporlarda dosyalara ait teknik bilgilere yer verilmemiştir.** Çünkü bu durumda yani tarih ve saat bilgilerinin değiştiği söz konusu olunca, dosya içerisine bakmakla, içerisine veri eklemek, çıkarmak veya değiştirmek arasında hiçbir fark yoktur *(son erişim tarihi açısından)*. Bununla beraber söz konuş işlemler gerçekleştiğinde elbette "son değiştirme tarihi" bilgisi de değişecektir. Hal böyle olunca gerek inceleme gerek export raporlarında bu duruma yer vermek dijital verilerin güvensiz, değiştirilmiş ve geçersiz olduğunu belirtmekle aynı anlama gelecektir. Ayrıca şifreli verilerin çözülüp çözülmediğinin, çözüldüyse nasıl çözüldüğünün veya çözülmediyse şifrenin nasıl elde edildiğinin belirtilmemesi, netice de her halükarda şifrenin ne

olduğunun, kaç basamaklı ve kaç farklı karakter grubundan oluştuğunun yani şifre çözümleme raporlarının olmaması da söz konusu dijital materyalin (SD kart) teslim edildiği tarihten itibaren süre gelen ve devam eden süreç boyunca şaibeler ve gayri resmi işlemler şüphesini güncel tutmaya devam edecektir.

8. Tüm bu hususlar göz önüne alındığında; Öncelikle belirtmek gerekir ki; bu raporda yer verilen hususlarla ilgili olarak yapılan işlemlerin en baştan denetlenmesi, incelenmesi ve hiçbir mağduriyete yer vermemek, mağduriyetleri gidermek ve kasten yahut hata ile yapılan eylemlerin müsebbibi olan görevlileri ortaya çıkararak adli makamlara intikal ettirmek adalet ve güvenirliğin, tarihe ve geleceğe örnek bir davranış sergilemenin gereğidir.

9. Adil Yargılanma kapsamında; iki adet SD kartın çözüm raporundaki en önemli hata olan **hash bilgileri *(dijital imza, hash'i hesaplanan veriye özel ve parmak izi gibi benzersiz bir değerdir),* metadata olarak bilinen tarih ve zaman bilgileri, veriyi oluşturan, son erişen ve değiştiren kullanıcıların kim yada kimler olduğu**, **tarih gibi bilgileri ve en önemlisi ise imaj alma işlemine ait log dosyasına yer verilmemiştir**. Bu doğrultuda ise CMK 217 kapsamında, sanık ve müdafi ine Yargıtay kararları doğrultusunda delilin elde ediliş şeklinin okutulması neticesinde verilecek beyan kapsamında hazırlanan bu raporda; Veri bütünlüğünün bozulması ve raporda bahsettiğimiz diğer hususlar neticesinde ilgili delilin elde edilişinde hukuka ve adli bilişim kurallarına aykırı işlem tesis edilmesi neticesinde Anayasa 38/6 Ceza Muhakemesi Kanunu ***m.206/2-a, 217/2, 230/1-b*** maddeleri uyarınca hukuka aykırı delil kapsamında değerlendirilmelidir.

Avukat / Adli Bilirkişi
Mesut Can TARIM