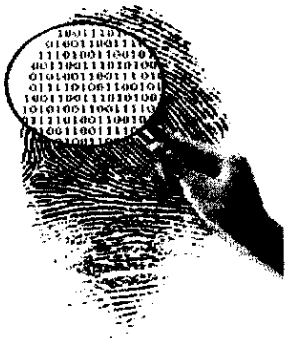
T.C.
İÇİŞLERİ BAKANLIĞI
EMNİYET GENEL MÜDÜRLÜĞÜ

SİBER SUÇLARLA MÜCADELE
DAİRE BAŞKANLIĞI

ADLİ BİLİŞİM ŞUBE MÜDÜRLÜĞÜ

İNCELEME RAPORU

Marmaris Sulh Ceza Hakimliğinin 2016/759 D.İş. sayılı kararına istinaden DVR cihazı (Unimo marka UDR-716CE model 121249333 seri numaralı DVR cihazı) incelemesi



İNCELEME RAPORU

İnceleme Talep Eden Makam Tarih ve Soruşturma No:	Marmaris Cumhuriyet Başsavcılığının 27/07/2016 tarih ve 2016/3382 sayılı soruşturması
İnceleme Kararı Veren Makam Tarih ve No:	Marmaris Sulh Ceza Hakimliğinin 2016/759 D.İş. sayılı kararı
İncelenmesi talep edilen Hususlar	DVR İncelemesi. 15.07.2016 saat 12:00 ile 16.07.2016 saat 09:00 arasına ait kayıtların incelenmesi
İnceleme Bitiş Tarihi:	08/08/2016

İNCELENEN MATERYAL BİLGİLERİ

No	Marka	Model	Seri No	Açıklama
1	Seagate	ST1000VX000-1CU162	Z1D3JBW2	1 TB Kapasiteli SATA sabit disk(Unimo marka UDR-716CE model 121249333 seri numaralı DVR cihazı içerisinden çıkarılan)GRAND YAZICI CLUB TURBAN OTEL'E AİT
2	Seagate	ST1000VX000-1CU162	Z1D3JC3P	1 TB Kapasiteli SATA sabit disk(Unimo marka UDR-716CE model 121249333 seri numaralı DVR cihazı içerisinden çıkarılan)GRAND YAZICI CLUB TURBAN OTEL'E AİT

İNCELEME SÜRECİ

Dijital materyalin incelenmesi, veri bütünlüğü korunmak suretiyle yazma korumalı olarak (**Write Blocker**), Adli Bilişim uygulamaları çerçevesinde ve uluslararası standartlara uygun şekilde adli kopya üzerinden gerçekleştirilmiştir. İnceleme için DVR cihazları için özel geliştirilmiş olan DVRExaminer 1.23 programı ve R Studio programı kullanılmıştır.

MATERYALE AİT TEKNİK BİLGİLER

(İncelenen materyalde bulunan "Seagate *Marka* Z1D3JBW2 ve Z1D3JC3P *seri nolu* 1 TB kapasiteli *Harddiskler'in" imajı)*

DEVICE (CİHAZ) BİLGİLERİ

1.Materyale Ait imajın Hash Değerleri	
MD5 Değeri	b234d822dafb1d4e516c5b7794b7ca18
SHA1 Değeri	8a993c8ac016af615171888716f8726359f07f75
Doğrulanan MD5 Değeri	b234d822dafb1d4e516c5b7794b7ca18
Doğrulanan SHA1 Değeri	8a993c8ac016af615171888716f8726359f07f75

2.Materyale Ait imajın Hash Değerleri	
MD5 Değeri	63e5204f6dd9e9273d927710eb1e53f4
SHA1 Değeri	4d19c70a123c451f646d86a9a14a8acfa9e9c94b
Doğrulanan MD5 Değeri	63e5204f6dd9e9273d927710eb1e53f4
Doğrulanan SHA1 Değeri	4d19c70a123c451f646d86a9a14a8acfa9e9c94b

OS (İŞLETİM SİSTEMİ) BİLGİLERİ

İşletim sistemi barındırmadığı DVR cihazı tarafından depo diski olarak kullanıldığı, dosya sisteminin Linux dosya sistemine benzediği tespit edilmiştir.

TEKNİK TERİMLER VE AÇIKLAMALAR

MD5 ve SHA1 Hash Değerleri

MD5 (Message-Digest algorithm 5), veri bütünlüğünü test etmek için kullanılan, Ron Rivest tarafından 1991 yılında geliştirilmiş bir kriptografik özet (tek yönlü şifreleme) algoritmasıdır. Girdi verinin boyutundan bağımsız olarak 128 bitlik özetler üretir.

SHA (Secure Hash Algorithm – Güvenli Özetleme Algoritması), Amerika'nın ulusal güvenlik kurumu olan NSA (National Security Agency) tarafından tasarlanmıştır.1993 yılında FIPS PUB 180 standardında yayınlanmıştır.

Bu iki değer veri bütünlüğünü ve güvenliği açısından adli incelemelerde oldukça önemlidir.

Bilgiye(dataya) ilişkin olarak yapılan işlemler öncesinde ve sonrasında datanın 'hash' değeri alınır. Eğer 'hash' değeri işlem öncesinde ve sonrasında aynı ise datada herhangi bir değişiklik olmadığı ve eğer 'hash' değeri farklı ise datada değişiklik olduğu sonucuna varılır. Bu sayede bize incelenen materyalin imajı alındıktan sonra üzerinde değişiklik yapılıp yapılmadığı bilgisini veren değerlerdir.

DVR Cihazları Çalışma Prensibi

DVR Kayıt Cihazı Hakkında Bilgi DVR açılımı ingilizce bir terim olan "Digital video recorder"dır. Türkçesi ise "Sayısal Görüntü Kaydedici"dir. Dijital Kayıt Cihazları Güvenlik

Kamerası'ndan gelen görüntü ve sesleri içindeki elektronik devre sistemiyle HardDiskte depolar ve aynı zamanda gerek yerel ağ gerek uzaktan izleme gereksede yerinde izleme olanağı sunar. Dvr Kayıt Cihazı günümüz dünyasında 4 Kanal DVR Cihazı, 8 Kanal Dvr Cihazı, 16 Kanal Dvr Cihazı ve 32 Kanal Dvr Kayıt Cihazı olarak sıkça kullanılır.

DVR cihazı içerisinde yer alan ve kaydedilen video dosyalarının ham hallerinin bulunduğu diskler ile kamera kayıt cihazının kaç günlük kayıt tutacağı doğru orantılıdır.

Kullanıcı tarafından aksi belirtilmediği sürece DVR cihazı bünyesinde bulunan disk içerisine kayıtları yapar. Tüm disk dolduktan sonra ise en eski tarihli görüntüyü bularak bu video dosyalarını silip üzerine yeni tarihli video dosyalarını kayıt eder.

Ancak kullanıcı tarafından disk dolduğunda "bana haber ver ve kaydı durdur" gibi seçeneklerde mevcuttur.

Bir DVR cihazının 10 günlük kayıt depoladığı varsayılırsa 11. gün geldiğinde cihaz içerisinde tarama yaparak en eski tarihli video dosyasını bulur ve bu dosyayı siler. Bu dosyanın yerine ise en yeni tarihli görüntüyü kayıt eder.

Yani 10 günlük kayıt tutan bir dvr cihazı diski içerisinde 15 gün öncesine ait kayıt bulmak olanak dışındadır. Dvr cihazının özel dosya sistemi orijininde küçük ihtimal de olsa silinen bu dosyanın adı bulunabilir.

NTFS dosya sisteminde MFT gibi ayrı bir alanda tutulan bu dosya adı bilgisi de DVR dosya sistemine göre farklı bir alanda tutulabilir.

Veri üzerine veri yazma işlemine gerçek silme işlemi yani wipe denir. Veri kurtarma işlemleri neticesinde silinmiş bir verinin geri kurtarılmasını imkânsız hale getirmek için kullanılan wipe yönteminde silinmiş verinin üzerine veri yazılır bu sadece 00 ya da FF hex i olabileceği tamamen karışık bir algoritmada olabilir.

Bir disk wipe işlemine tabi tutulduktan sonra o diskten veri kurtarmak söz konusu değildir.

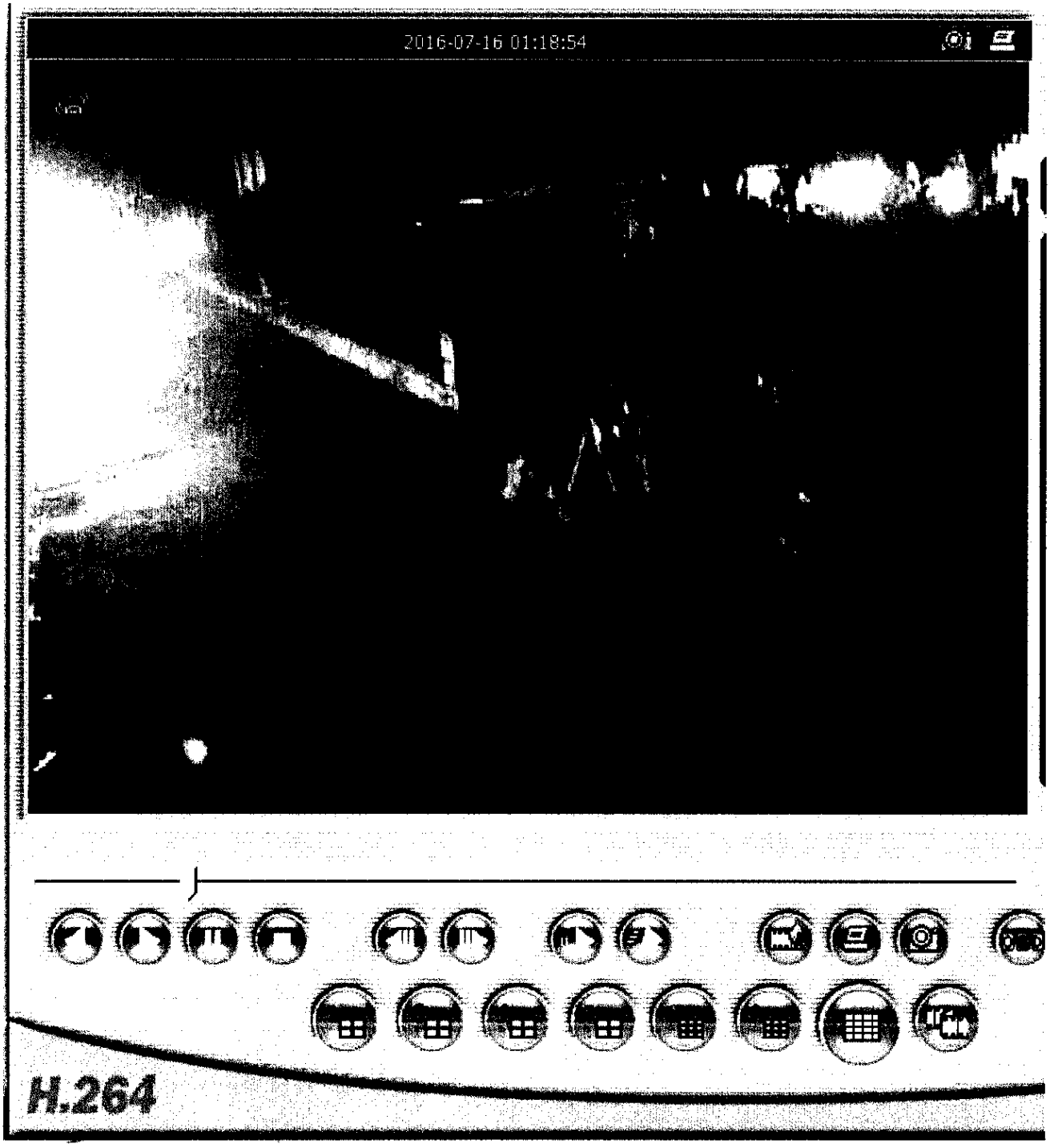
DVR cihazları içinde silinen video dosyasının üzerine yeni bir video dosyası yazıldığı için bu işlemde gerçek manada bir *gerçek silme* işlemidir. Tüm bu sebeplerden dolayı DVR cihazlarında daha önceki bir zamana ait üzerine veri yazılmış video görüntüsünü kurtarmak imkan dâhilinde değildir.

MATERYALE AİT İNCELEME DURUMU

(İncelenen materyalde bulunan "Seagate *Marka* Z1D3JBW2 ve Z1D3JC3P *seri nolu* 1 TB kapasiteli *Harddiskler'in" imajı)*

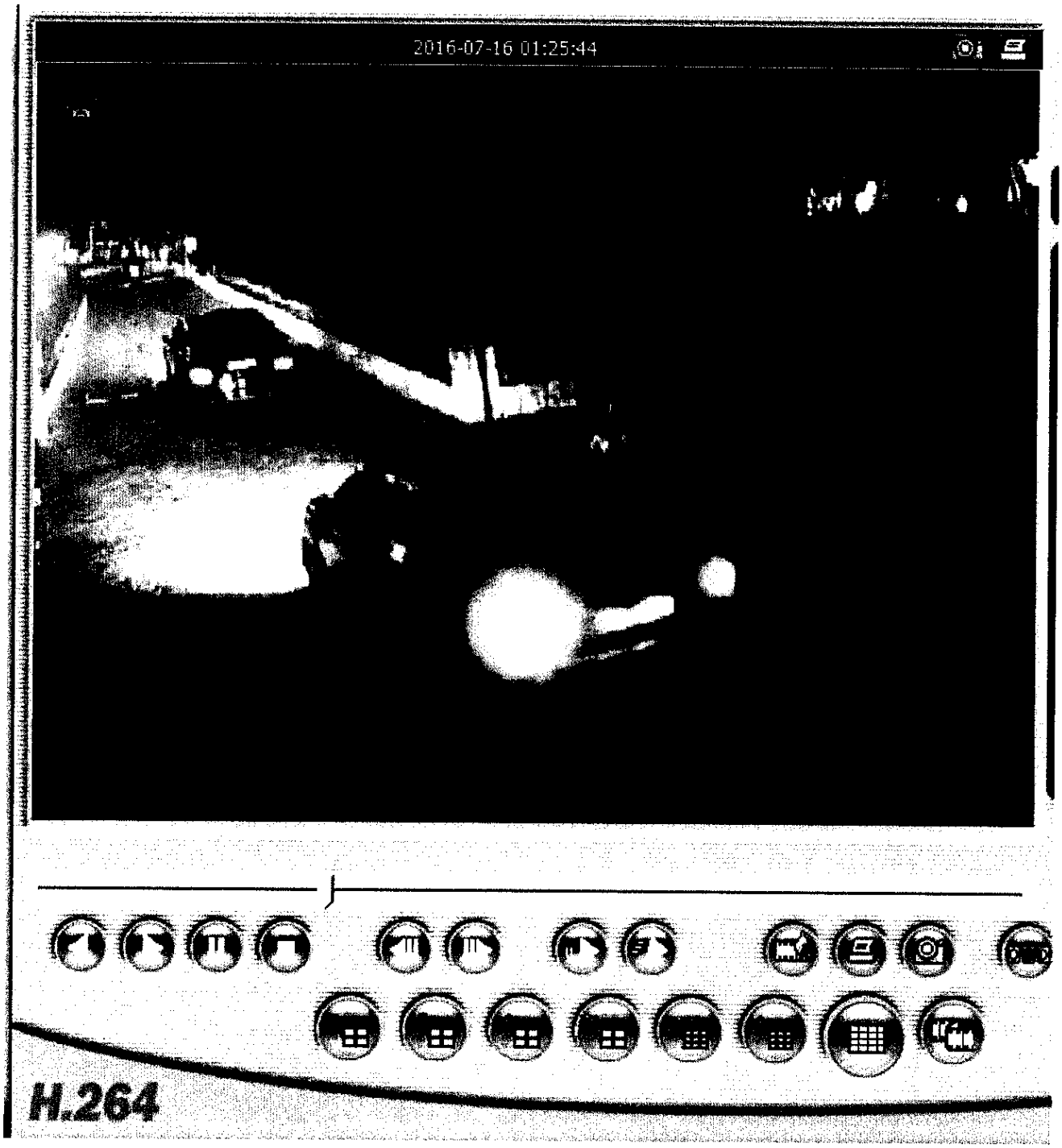
Tarafımıza incelenmek için gönderilen Unimo marka UDR-716CE model 121249333 seri numaralı DVR cihazı içerisinden çıkarılan 2 adet sabit diskin özel yazılımlarla yazma korumalı olarak incelemesi esnasında içerisinde inceleme talep yazısının eklerinde belirtilen 15/07/2016 saat 12:00 'den 16/07/2016 saat 09:00 'a kadar olan görüntüler cihazlar üzerinden export edilmiş ve Hitachi marka B9HP8WWF seri numaralı diskte ilgili klasöre kopyalanmıştır. Bu video dosyalarının Uniplayer H264 adlı bir oynatıcı ile görüntülenebilir halde olduğu tespit edilmiş ve bu oynatıcı programda export dosyalarının yanına kopyalanmıştır.

Cihaza ait 16 tane kamera olduğu bunların hemen hemen tamamı dış ortamları kayıt ettiği tespit edilmiştir. Ayrıca DVR cihazının saatinin 10 dakika ileri olduğu tespit edilmiştir. DVR cihazının ses kaydetmediği tespit edilmiştir.

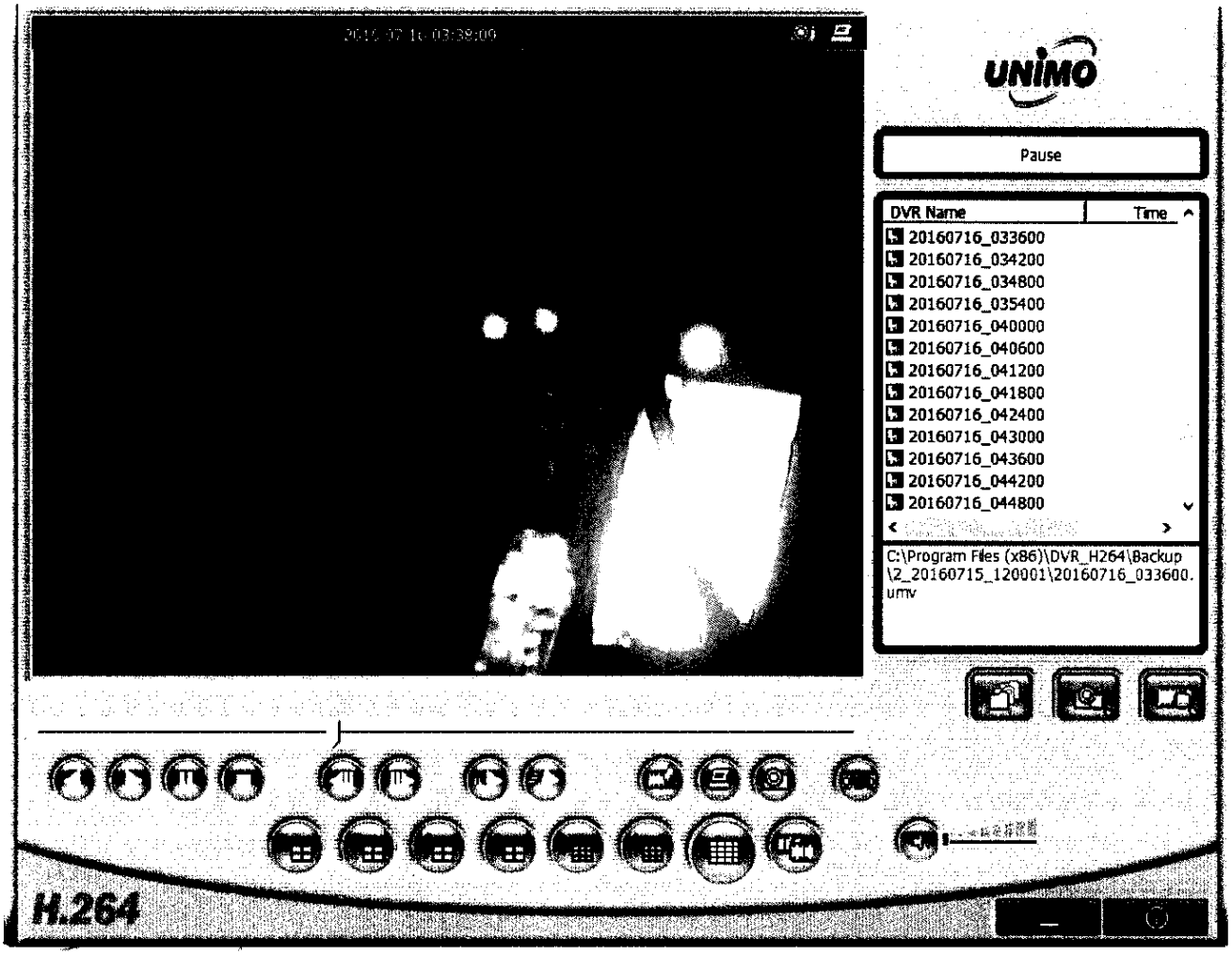


Üstteki ekran alıntısında 16/07/2016 saat 01:18:54 civarlarında kameranın görüş açısına elinde silah olan bir polis memurunun girdiği görülmüştür.

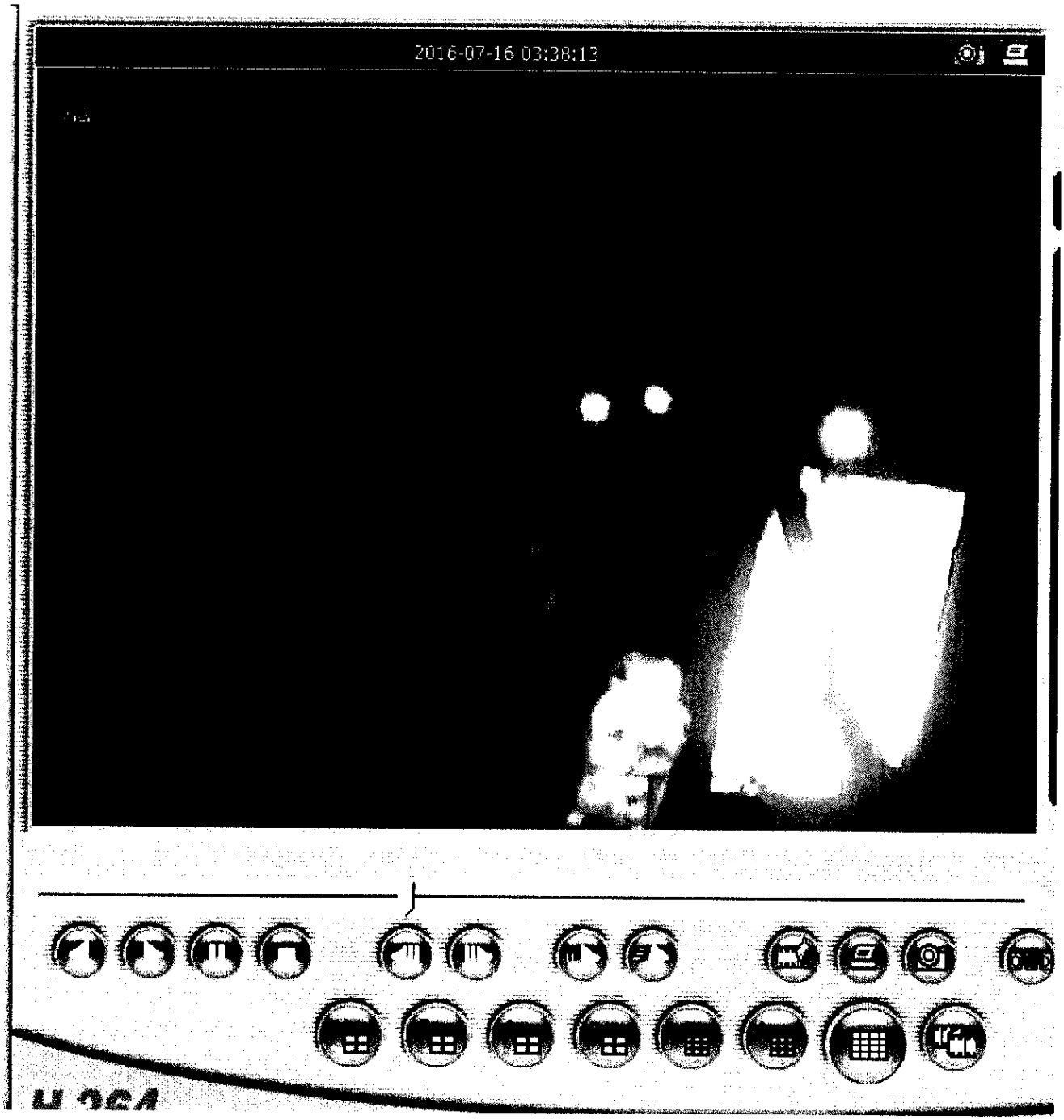
Üstteki ekran alıntısında 16/07/2016 saat 01:28:55 civarlarında kameranın görüş açısına giriş kapısı olduğu düşünülen yerden polislerin girdiği görülmüştür.



Üstteki ekran alıntısında 16/07/2016 saat 01:25:44 civarlarında kameranın görüş açısına önde eskortluk eden bir motosiklet ve makam aracına benzer siyah araçların giriş yaptığı görülmüştür.



Üstteki ekran alıntısında 16/07/2016 saat 03:38:09 civarlarında kameranın görüş açısına bir grup asker girmektedir. Bu kısmın önceki görsellerde polislerinde giriş yaptığı alanla aynı olduğu anlaşılmıştır.



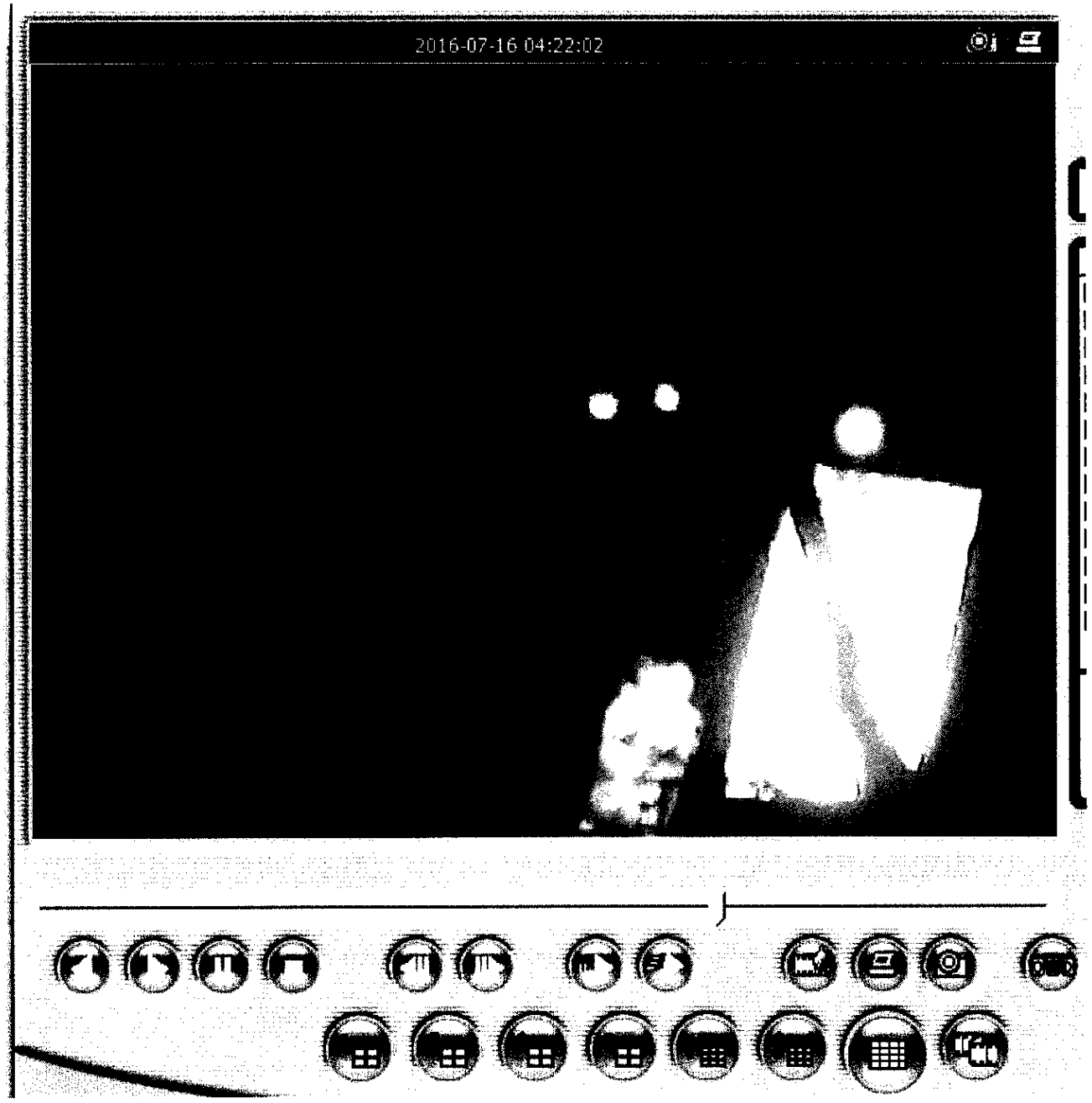
Üstteki ekran alıntısında 16/07/2016 saat 03:38:13 civarlarında kameranın görüş açısına giren askerlerin hızlı bir şekilde içeriye doğru giriş yaptıkları görülmüştür.

Üstteki ekran alıntısında 16/07/2016 saat 03:40:47 zamanında bir önceki asker grubundan yaklaşık 2 dakika sonra ellerindeki silahlardan yansıyan laser olduğu düşünülen ışıklarla beraber başka bir asker grubunun girdiği görülmektedir.

Üstteki ekran alıntısında 16/07/2016 saat 03:37:59 civarında askeri grubun otel içine doğru hareket ettiği görülmüştür.

Üstteki ekran alıntısında gösterildiği üzere 16/07/2016 saat 03:43:26 civarlarında silahlı askeri gruptan bir kısmının içeri giriş yaptıkları noktadan çıkış yaptıkları görülmüştür.

Üstteki ekran alıntısında görüldüğü üzere 16/07/2016 saat 04:00:47 civarında otel sakini olduğu düşünülen kişilerin koşarak hareket ettikleri görülmüştür.



Üstteki ekran alıntısında görüldüğü üzere 16/07/2016 tarihi saat 04:22:02 civarlarında askeri bir personel grubunun tekrardan otel girişine yöneldiği görülmüştür.

Üstteki ekran alıntısında görüldüğü üzere 16/07/2016 tarihi saat 04:22:05 civarlarında diğer açıdan otel içini gösteren kamerada askerlerin otel içinde hareket ettikleri görülmüştür.

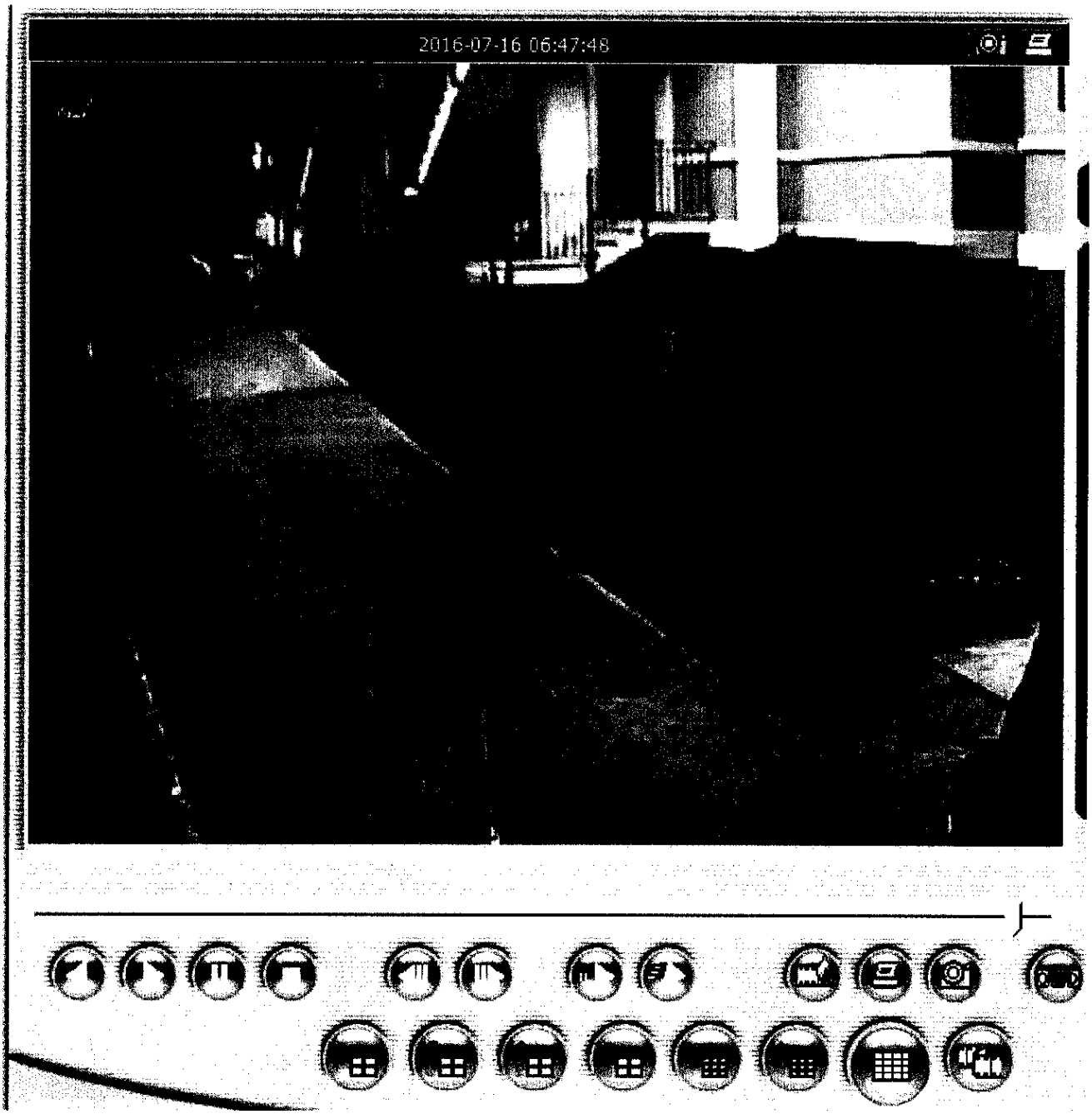
Üstteki ekran alıntısında görüldüğü üzere 16/07/2016 tarihi saat 04:28:05 civarlarında askerlerin tekrar çıkış kapısına doğru geldiği ancak bu sırada üstteki bazı teçhizatları çıkarılmış halde bir askerin belirli bir süre oturduğu görülmüştür.

Üstteki ekran alıntısında görüldüğü üzere 16/07/2016 saat 04:29:26 civarında otel içinden askeri grubun çıkış kapısına doğru hızlıca hareket ettiği görülmektedir.

Üstteki ekran alıntısında gösterildiği üzere 16/07/2016 saat 04:29:26 civarında önceki kısımlarda oturduğundan bahsedilen askeri personelde olmak üzere otelden çıkış yaptıkları görülmüştür.

Üstteki ekran alıntısında 16/07/2016 tarihi saat 05:00:57 civarında askerlerin çıkışından kısa zaman sonra otele ambulansların oldukça hızlı bir şekilde geldikleri ve hızlıca otelden ayrıldıkları görülmüştür.

Üstteki ekran alıntısında görüldüğü üzere 16/07/2016 saat 05:08:02 civarında bir önceki ambulanstan yaklaşık 8 dakika sonra başka bir ambulansın hızlıca otele girdiği ve yine hızlıca otelden ayrıldığı görülmüştür.



Üstteki ekran alıntısında görüldüğü üzere olay günü sabahı saat 06:47:48 civarında otel içerisinde birçok noktada polislerin uzun ya da kısa namlulu silahlarla alanda turladıkları görülmüştür.

İnceleme talep yazısında belirtilen zaman aralıklarına ait görüntüler tarafınızdan değerlendirilmek üzere Hitachi marka B9HP8WWF seri numaralı diskte ilgili klasöre kopyalanmıştır.

DVR cihazına ait yapılan incelemelerde inceleme konusu ile alakalı saatler içerisinde dvr cihazına ait kamera görüş alanlarında polislerin koruma amaçlı bekledikleri, siyah renkli makam otosu benzeri araçların giriş çıkış yaptıkları, askeri bir grubun otele giriş yaptığı askerlerin otelden ayrılmasından hemen sonra otele ambulansların geldiği görülmüştür. Kameralara giren alanlarda çatışma görülmemiş olup, otelden çıkış yaptıktan sonra da otel kameralarının görüş açılarına askeri personel girişi olmamıştır.

SONUÇ VE DEĞERLENDİRME

Marmaris Sulh Ceza Hâkimliğinin 2016/759 D.İş. sayılı kararına istinaden DVR cihazı içerisinde inceleme talep yazısı eklerinde belirtilen 15/07/2016 ve 16/07/2016 tarihine ait tüm kayıtlar tarafınızdan değerlendirilmek üzere export edilmiştir.

Tüm inceleme işlemleri uluslararası adli bilişim standartlarına göre tamamlanmıştır.

İş bu rapor yirmi bir(21) sayfadan ibarettir.

Bu rapor iki(2) nüsha olacak şekilde çoğaltılmıştır.

Arz ederim. 08/08/2016

Adli Bilişim Uzmanı

Sicil:349435

İmza: