T.C.

İSTANBUL 12. AĞIR CEZA MAHKEMESİ HAKİMLİĞİ'NE

T.C. İstanbul 12. Ağır Ceza Mahkemesi'nin2010/34sayılı davası kapsamında tarafımıza iletilmiş 5 no'lu sabit diskin dijital adli analiz incelemesi ile daha önce yazılmış bilirkişi raporlarının değerlendirmelerini de içerecek genel kapsamlı bir çalışma gerçekleştirilmektedir.Gerçekleştirilen ve devam eden çalışmaların özeti aşağıda verilmiştir.

TALEP EDİLEN ANALİZLER

Mahkeme dilekçesinde belirtilen ve bir kısım sanıklar ve müdafilerin talep dilekçeleri ve bu dilekçelerine ekledikleri bilirkişi mütalaalarında (rapor) iddia ettikleri hususları içerir bir heyet raporu tanzim edilmesi.

İNCELENEN DELİLLER

Tarafımıza"5 numaralı sabit disk" olarak iletilen disk imajı ile içindeki dosyalar incelenmektedir.

5 numaralı sabit diskin özellikleri:

- **Marka/Model:** SAMSUNG SP0802N
- **Seri Numarası:** 0637J2FWA19210
- **Firmware Sürümü:** TK100-23
- **Kapasite (in sectors reported Pwr-ON):**156,368,016 (80.0 GB)
- **Kapasite (in sectors reported by HPA):** 156,368,016 (80.0 GB)
- **Kapasite (in sectors reported by DCO):** 156,368,016 (80.0 GB)
- **HPA kullanımda mı:** Hayır
- **DCO kullnımda mı:** Hayır
- **ATA Şifreleme kullanımda mı:** Hayır
- **Arayüz:** IDE
- **ATA PIO mode:** PIO 4
- **ATA DMA mode:** UDMA 5

İNCELEME

1 Kullanılan Araçlar

Kullanılan araçlar şu şekildedir:

- **Tableau TD2:** Dijital imaj alma donanımıdır.
- **SIFT 2.14**: Dijital adli analiz programlarını içeren Linux İşletim Sistemi dağıtımıdır.
- **Encase 7.05.33.33:** Dijital adli analiz aracıdır.
- **FTK Imager 3.0.1:** Dijital adli analiz programıdır.
- **TSK (The Sleuth Kit)**: Dosya sistemi incelemesi için kullanılan dijital adli analiz aracıdır.
- **Exiftool 9.39**: Dosya içi üstverisini elde etmek için kullanılan programdır.

2 Metodoloji

Tarafımıza iletilen sabit diskin imajı üzerinde incelemeler yapılmaktave öncedenhazırlanmış bilirkişi raporları detaylı olarak değerlendirilmektedir.

Öncelikle literatürde ve kurumsal kaynaklarda konu ile ilgili araştırmalar yapılmıştır. Bununla beraber laboratuvar ortamında farklı konfigürasyondakisistemler üzerinde normal kullanıcı ve sistem davranışları modellenmektedir. İncelemeler sonunda elde edilen bulgular, modeller üzerinde sınanmaktadır.

3 İncelenen Konular

Sabit disk üzerinde kurulu işletim sisteminin ne olduğu ve ne zaman yüklendiği ilesistem kullanıcıları, sistem üzerinde kurulu olan programlar ve en son çalıştırılan programlar tespit edilmektedir. Bununla beraber en son açılan ve değiştirilen dokümanlar ile bu işletim sisteminin İnternete bağlı olup olmama durumu da incelenmektedir.

Dosya sistemi incelemeleri kapsamında sabit disk üzerinde oluşturulmuş bölümler ve üzerinde bulunan dosya sistemleri incelenmektedir.

Sabit diskte bulunan işletim sisteminde kurulubulunan Microsoft Office uygulamasınınsürümü ve ön tanımlıyapılandırma bilgileri belirlenmiştir.Microsoft Office programının davranışları kullanım şekilleri ve üst verilerinitespit amaçlı laboratuvar çalışmaları gerçekleştirilmektedir.

Zararlı yazılım incelemeleri kapsamında sabit disktefaaliyet gösteren zararlı yazılımlar analiz edilmekte ve bu zararlı yazılımların etki ve kabiliyetleri değerlendirilmektedir.

CR

SONUÇ

Şu ana kadar gerçekleştirilen inceleme ve yapılan laboratuvar testleri sonucunda normal kullanıcı veya sistem davranışları ile açıklanamayacak bir bulguya rastlanmamıştır.

İncelemeler hali hazırda devam etmekte olup, detaylı raporun ekleriyle beraber 29 Kasım 2013'e kadar tamamlanması hedeflenmektedir. 11.11.2013

Osman PAMUK	Burak AKOĞUZ	Erdem ALPARSLAN
Uzman Araştırmacı	Uzman Araştırmacı	Uzman Araştırmacı