RAM BELLEKLERİNİN ADLİ BİLİŞİM İNCELENMESİ VE ANALİZ TEKNİKLERİ

- İstanbul Şehir Üniversitesi -

Bilgi Güvenliği Mühendisliği Yüksek Lisans Programı Bilgisayar Adli Analizi Dersi

NOT: Eğitmenlerimizden Huzeyfe Önal'ın İstanbul Şehir Üniversitesi 2016 bahar döneminde Yüksek Lisans Programı Adli Bilişim Dersi öğrencileri tarafından hazırlanmıştır.

Hazırlayan: Yavuz Kaşıkçı

Tarih: 29.05.2016

[RAM BELLEKLERİNİN ADLİ BİLİŞİM İNCELENMESİ VE ANALİZ TEKNİKLERİ]

Özet

Bilişim teknolojileri bazı klasik suçların daha kolay işlenmesine imkân vermesinin yanında, yeni tip suçların da ortaya çıkmasını sağlamıştır. Günümüzde internetin sağladığı imkânlar sayesinde siber suç işlemek için eskisi kadar teknik bilgi ve beceriye sahip olmaya gerek kalmamıştır. Bilişim suçlarının evrimi, sosyal medya kullanımının yaygınlaşması, malware yazılımların (kötü niyetli yazılımlar) sayısında ve etkisinde yaşanan artışlar, bulut teknolojilerinin yaygınlaşması, kriptolu disk alanlarının kullanımın artması gibi etkenler nedeniyle bilgisayarın RAM'inin (Geçici Bellek) kopyalanarak incelenmesini zorunlu bir standart haline getirmiştir. Artık, olay yeri ekipleri, bilgisayarın güç kablosunu çekmek bir yana, çalışır halde bulunan bir bilgisayarın ilk önce RAM'in kopyasının alınmasının bir zorunluluk olduğunu bilinmektedir.Bu makalede Linux sistemlere ait hafıza imajları üzerinde yapılacak analiz işlemler ele alınacaktır.

Giriş

Adli bilişim; elektromanyetik ve elektrooptik ortamlarda muhafaza edilen veya bu ortamlarca iletilen ses, görüntü, veri, bilgi veya bunların birleşiminden oluşan her türlü bilişim nesnesinin, mahkemede sayısal delil niteliği taşıyacak şekilde tanımlanması, elde edilmesi, saklanması, incelenmesi ve mahkemeye sunulması çalışmaları bütünüdür. [1]

Adli bilişimde elektronik ortamda bulunan bilgilerin uygun yazılımlar ve donanımlarla delile dönüştürme süreci, hukuki boyuttan daha çok teknik ve uzmanlık isteyen zahmetli bir iştir. Sürekli gelişen sistemler, yeni donanımlar, yazılımlar ve sosyal medya araçları, artan kullanıcı sayısı yüzünden sabit disklerin kopyalarını almak önemli bulguların sonuca ulaşmasında yeterli olmayabilmektedir. Bu nedenden dolayı diğer bir hafıza birimi olan RAM, bellek kullanan elektronik cihazların açılışından kapanışına kadar depolanan bilgilerin kopyalanması, incelenmesi ve kayıt altına alınması bakımından adli bilişim için önemli bir araçtır. Bilişim suçu işlenirken kullanılmış sistemler incelenirken en önemli adımlardan biri sistemin o an çalışan imajının alınmasıdır. Bu imajda en önemli parçayı fiziksel hafıza/belleğin kopyası oluşturulması önemlidir.

Ram Nedir ?

İlk zamanlar yaygın yazılabilir RAM, 1949-1952 yılları arasında geliştirildi. Manyetik çekirdek bellek olarak birçok bilgisayarda kullanıldı. Daha sonra 1960'ların sonu ve 1970'lerin başında statik ve dinamik entegre devreler geliştirildi. [2] Günümüz bilgisayarlarında hem okunabilen hem de yazılabilen RAM (Read Acces Memory – Rastgele Erişimli Hafıza)'lar kullanılır.

RAM, "Random Access Memory" (Rasgele Erişimli Bellek) kelimelerinin baş harflerinden oluşan bir kısaltmadır. RAM, bilgilerin geçici olarak depolandığı bir hafıza türüdür. Bilgisayarlar genellikle o an üzerinde çalıştıkları programlar ve işlemlerle ilgili bilgileri RAM denen bu hafıza parçasında tutmaktadır. RAM ve sabit sürücü temel olarak aynı bilgileri saklamaktadır. Yani RAM bir nevi arada bir köprü durumunda olmakta, ancak bir köprünün yapacağından çok daha fazla işi yerine getirmektedir. Bilgisayarlardaki CD-ROM, disket, sürücü veya sabit disk gibi

depolama birimlerinden daha hızlı çalışmaktadır.. Belleklerin sabit disk gibi sürekli kayıt özellikleri bulunmamaktadır Bilgisayar çalıştığı sürece RAM faaliyetini devam ettirmekte, bilgisayar kapandığı zaman, RAM'da bulunan veriler silinmektedir.

RAM'lar birbirinden tamamen bağımsız hücrelerden oluşmaktadır. Bu hücrelerin herbirinin kendine ait sayısal bir adresi bulunmaktadır. Her hücrenin çift yönlü bir çıkışı bulunmakta, bu çıkış veri yolunda (Data Bus) mikroişlemciye bağlı olmaktadır. Bu adresleme yöntemiyle RAM'daki herhangi bir bellek hücresine istenildiği anda, diğerlerinden tamamen bağımsız olarak erişilebilmektedir.. "rastgele erişimli bellek" adı da buradan gelmektedir. RAM'da istenen kayda ya da hücreye kapasitesine göre anında erişilebilmektedir.

Modern Sistemlerde Ram Bellek Çalışma Sistemleri

RAM belleklerin görevi, en hızlı şekilde işlemciyle bilgi alışverişi sağlamaktır. Bu işlemi yapmak için gereken şey bellek yongalarıdır. Bu yongaların her biri belli bir depolama kapasitesine sahip olmaktadır.

Aynı devre üzerindeki bu yongaların toplam kapasitesi RAM belleğin kapasitesini vermektedir. RAM bellekler de çok sayıda transistör ve kapasitörden oluşmaktadır. Transistörlerin görevi, istenen verilerin kontrolünü sağlayıp aç-kapa yaparak veri geçişini sağlamaktır. Kapasitörse depolama gerçekleştirmekte ama depolama süreleri kısıtlı olmaktadır.. Bundan dolayı okuma yazma hızı saniyeler içinde birçok kez tekrarlanmaktadır. Düzenli bir iletişim olması için 0 (yok) 1 (var) sistemi çalışmaktadır. Bellek içinde iki eksenli düzlemde dizili bit adı verilen depolama birimleri yer almaktadır. Sıra ve sütunlar sayesinde bit'lerin yerleri adres haline dönüştürülmektedir. Adresin tanımlaması sıra ve sütun bilgisinden ibaret olmaktadır. Yazma ve okuma işlemleri sırasında bu adresler önemli rol oynamaktadır. RAM yapısında belirli bir kolona gönderilen sinyalden sonra bu sütundaki tüm hücreler aktifleşmektedir. Satır bilgisi de devreye girince değişiklik gerçekleşmektedir. Eğer kapasitör şarj durumu %50'nin üstündeyse 1, altındaysa 0 mesajı alınmaktadır. Saniyenin milyarda birinde gerçekleşen okuma ve yazma işlemleri son derece hızlı olmaktadır. Eski nesil anakartlarda statik RAM bütünleşik olarak gelmekteydi, ancak zamanla RAM yuvaları ortaya çıktı. Bu yuvalara yerleştirilen bellek modüllerinin merkezini oluşturan genelde yeşil renkli olan baskı devrenin görevi, ara bağlantıyı sağlamaktır. Ram Tipleri

Drram (Dinamik Ram): Transistör ve kapasitör birlikte çalışmaktadır. Transistör ve kapasitörlerin çalışma sistemlerine göre sürekli yenilenmesi gerekmekte, bu yüzden dinamik RAM denmektedir. Günümüz belleklerinde bu yöntem kullanılmaktadır.

Sdram (Eş Zamanılı Dinamik Ram): Dinamik belleklerin üst teknolojisidir. Daha fazla enerji harcamakta, yüksek hızlarda sinyal hatalarını önlemekte, hızlı ve verimli çalışmaktadır.

Ddrsdram (Çift Veri Hızı Eş Zamanlı Dinamik Ram): İsminden anlaşıldığı gibi eş zamanlı dinamik belleklerden hızı ve bant genişliği olarak iki kat hızlı olmaktadır., Günümüzde en yaygın olarak kullanılan RAM türüdür.

[RAM BELLEKLERİNİN ADLİ BİLİŞİM İNCELENMESİ VE ANALİZ TEKNİKLERİ]

Adli Bilişim İncelemelerinde Ram Belleklerin Önemi

Geçmiş yıllarda adli bilişim vakalarında RAM bellek kopyalaması kuralı bulunmamaktaydı. İncelenmesi gereken bilgisayarların, direk güç kaynağından kapatıldıktan sonra üzerinde çalışma kuralı geçerli olmaktaydı. Bu durum, RAM belleklerde bulunan değerli bilgilere erişilmesini imkansız hale getirmekteydi. Hızla gelişen işlemci teknolojilerine göre sabit disklerin hızının yetersiz kalması, RAM belleklerin bilgisayarların veri işleyişi açısından önemli bir role sahip oldu. Teknoloji ve kapasiteler arttıkça RAM belleklerin içinde bulunan kaydedilmemiş dosyalar, şifreler, kullanıcı bilgileri gibi veriler adli bilişim adına önem taşıdığından olay yeri ekipleri, bilgisayarın güç kablosunu çekmek bir yana, çalışır halde bulunan bir bilgisayarın ilk önce RAM bellek kopyasının alınmasının bir zorunluluk olduğunu bilmektedir. RAM bellek incelemeleri, adli vakalardaki asıl delillerin bulunması veya asıl delilere ulaşmaya yardım etmesi ve vakaların hızlı şekilde sonuçlanmasında kritik rol oynamaktadır. Sadece sabit disklerin incelenmesi kesin sonuç bulmak için yeterli olmamaktadır. RAM içerisinde erişilebilecek tüm veriler, aslında işlemci tarafından işlenen tüm veriler olmaktadır. En önemli soru ise, bu verilerin zarar verilmeden hangi yöntemle kopyalanacağı, nasıl bir analiz programı kullanılacağı ve bu analiz sonucunda nelere ulaşılabileceği hususudur.

Ram İncelemelerinde Elde Edilebilecek Bulgular

- Gizli programlar,
- Aktif Network bağlantıların durumu,
- Kullanıcı şifreleri,
- Encryption anahtarları,
- Kaydedilmemiş dokümanlar,
- Çalışan prosesler ve hizmetlere ait bilgiler,
- Korumalı yazılımlara ait paketlenmemiş ve kriptolanmamış ham veriler, sistem bilgileri (Örn: En son kapanmadan bu yana geçen zaman),
- Sisteme oturum açan kullanıcılara ait bilgiler, kayıt defteri bilgileri,
- Açık ağ bağlantıları ve ARP önbellek,
- Sohbet kayıtları, sosyal ağ kalıntıları ve MMORPG oyunlarındaki iletişim kayıtları,
- Tarayıcı yazılımlara ait izler ve kayıt bilgileri, ziyaret edilen adres bilgileri,
- Web e-posta üzerinden yapılan en son işlemler,
- Bulut sistemlerine ait teknik bilgi ve veriler,
- Kriptolu disk alanlarına ait anahtarlar,
- En son bakılan fotoğraflar,
- Sistemde çalışan kötü niyetli yazılımlar.

Ram Bellek Adli Kopya Alma Teknikleri

Basit modellerin aksine (belki ortak inanç) modern SDRAM modülleri, içeriğini bilgisayar kapatılmadan hemen kaybetmemektedir. Bu süreç, oda sıcaklığında birkaç saniye sürmekte; ancak düşük sıcaklıklarda dakika kadar uzatılabilmektedir. Bu nedenle, normal çalışma belleğinde saklanan tüm verileri kurtarmak mümkün olmaktadır (SDRAM modülleri gibi). Bu durum, bir soğuk çizme saldırısı ya da buz adam saldırısı olarak da adlandırılımaktadır

5.1 FTK Imager;

AccessData firması tarafından üretilmiş bir yazılımdır. Depolama birimlerinin içeriğini göstermek ya da kopya almak için kullanılmaktadır. RAM belleklerin birebir kopyası alınabilmektedir. Alınan kopyalar Windows Explorer üzerinden açılarak sabit disk sürücüsü gibi işlem görmesini sağlanmaktadır. Güncel versiyonlarını ücretsiz kullanıma izin vermektedir.

5.2 Belkasoft Live RAM Capturer,

Hata düzeltme sistemi bulunan, güvenilir şekilde RAM kopyasını ve canlı analizini yapabilen bir adli araçtır. Küçük ve ücretsiz bir programdır. XP, Vista, Windows 7 ve 8, 2003 ve 2008 Server Windows işletim sistemleriyle uyumludur.

5.3 Encase v7

Guidance Software firmasının ürünü olan Encase v7 ile de RAM imajı alınabilmektedir. Encase v7 ücretli bir yazılım olup imaj alma özelliği ücretsiz olarak kullanılabilmektedir. Sistem üzerinde kurulum yapılarak kullanılacağı için RAM bellek üzerinde çok fazla proses kullanarak RAM üzerindeki verilere kalıcı zarar verebilmektedir. [3]

Analiz Yöntemleri

6.1 Volatility

Windows, Linux, Mac OSX ve Android telefonlara uyumludur. Canlı RAM analizi yapamaz. Volatility programı ile öğrenebilecek bilgiler aşağıda yer almaktadır:

- İmajın alındığı zaman bilgileri,
- Çalışan uygulamalar,
- Açık network(ağ) portları(soketleri),
- Her bir uygulama yada proses tarafından açılan dosyalar,
- Her bir uygulama yada proses tarafından açılan registry anahtarı,
- İşletim sisteminin Kernel (Çekirdek) modülleri.

•6.2 Belkasoft Evidence Center

İOS, Blackberry, Android ve Windows için RAM analizi yapar. Ücretli yazılımdır. Elde edilen tüm kanıtlar canlı analiz edebilmektedir.

6.3 Internet Evidence Finder

JADsoftware firması tarafından geliştirilmiş olan internet evidence finder, sabit disk üzerinde bulunan verilerin analizini yapmaya yarayan özel bir yazılımdır. Sabit disk üzerinde pagefile.sys ve hiberfile.sys dosyalarını da tespit ederek sadece onlar üzerinde de analiz yapmaya yarayan ücretli bir yazılım olup hem sabit disk hem de RAM ve bunların imajları üzerinde kullanılabilmektedir. Açılış paneli üzerinde seçim yapma özelliği ile kullanışlı bir yazılımdır. [3] Internet Evidence Finder programı ile aşağıda yer alan analizler yapılmaktadır:

6.4 X-Ways Capture

Linux da, sadece Windows altında çalışmaktadır. Fiziksel RAM ve tüm çalışan işlemler sanal bellek dökümünü almaktadır. Ayrıca kullanıcı etkileşimi olmadan otomatik olarak önceden adımları çalıştırmaktadır. Otomatik olarak çeşitli şifreleme şemaları / şifre korumasını tespit etmektedir. Bilinen ya da bilinmeyen şifreleme yazılımlarınıfarklı yöntemler ile aramakta ve bunları bildirmektedir. Tüm bulgular ve eylemlerin yer aldığı ayrıntılı bir günlük oluşturmaktadır.

Sonuçlar

RAM belleklerin bilgisayarın açılışından kapanışına kadar olan bilgilerin bir kaydını tutuğu ve RAM belleklerin çalışma kuralına göre güç kaynağı kesildiği zaman bu bilgilerin silinmesi durumu mevcuttur. Bu kopyaların içinde adli vakalarda kullanılacak önemli bilgilerin bulunmasına yardımcı olması bakımından RAM kopyasının alınması mecburi duruma gelmiştir.

RAM imajlarından alınan kopyanın incelenmesi RAM belleklerin en zor kısımlarından biridir ve uzmanlık ister. RAM belleklerde hiyerarşik yapının bulunmaması analiz programlarının önemini artırmıştır.

BGA Bilgi Güvenliği A.Ş. Hakkında

BGA Bilgi Güvenliği A.Ş. 2008 yılından bu yana siber güvenlik alanında faaliyet göstermektedir. Ülkemizdeki bilgi güvenliği sektörüne profesyonel anlamda destek olmak amacı ile kurulan BGA Bilgi Güvenliği, stratejik siber güvenlik danışmanlığı ve güvenlik eğitimleri konularında kurumlara hizmet vermektedir.

Uluslararası geçerliliğe sahip sertifikalı 50 kişilik teknik ekibi ile, faaliyetlerini Ankara ve İstanbul ve USA'da sürdüren BGA Bilgi Güvenliği'nin ilgi alanlarını "*Sızma Testleri, Güvenlik Denetimi, SOME, SOC Danışmanlığı, Açık Kaynak Siber Güvenlik Çözümleri, Büyük Veri Güvenlik Analizi ve Yeni Nesil Güvenlik Çözümleri*" oluşturmaktadır.

Gerçekleştirdiği başarılı danışmanlık projeleri ve eğitimlerle sektörde saygın bir yer edinen BGA Bilgi Güvenliği, kurulduğu günden bugüne alanında lider finans, enerji, telekom ve kamu kuruluşlarına 1.000'den fazla eğitim ve danışmanlık projeleri gerçekleştirmiştir.

BGA Bilgi Güvenliği, kurulduğu 2008 yılından beri ülkemizde bilgi güvenliği konusundaki bilgi ve paylaşımların artması amacı ile güvenlik e-posta listeleri oluşturulması, seminerler, güvenlik etkinlikleri düzenlenmesi, üniversite öğrencilerine kariyer ve bilgi sağlamak için siber güvenlik kampları düzenlenmesi ve sosyal sorumluluk projeleri gibi birçok konuda gönüllü faaliyetlerde bulunmuştur.

BGA Bilgi Güvenliği AKADEMİSİ Hakkında

BGA Bilgi Güvenliği A.Ş.'nin eğitim ve sosyal sorumluluk markası olarak çalışan Bilgi Güvenliği AKADEMİSİ, siber güvenlik konusunda ticari, gönüllü eğitimlerin düzenlenmesi ve siber güvenlik farkındalığını arttırıcı gönüllü faaliyetleri yürütülmesinden sorumludur. Bilgi Güvenliği AKADEMİSİ markasıyla bugüne kadar "Siber Güvenlik Kampları", "Siber Güvenlik Staj Okulu", "Siber Güvenlik Ar-Ge Destek Bursu" , "Ethical Hacking yarışmaları" ve "Siber Güvenlik Kütüphanesi" gibi birçok gönüllü faaliyetin destekleyici olmuştur.