Adli Bilişim Açısından, Tam Disk Şifrelemesine (FDE) Sahip Bilgisayarlardan Ağ Trafiğinin Koklanması (Sniffing) Yoluyla Delil Elde Edilmesi (Mayıs 2016)

Özgür Koca

Gazi Üniversitesi
Bilişim Enstitüsü, Adli Bilişim Anabilim Dalı
Tunus Caddesi No: 35 Kavaklıdere Çankaya/ANKARA
<be@gazi.edu.tr>

Yazan: *Özgür KOCA, (<ozgur.koca@linux.org.tr> / www.tankado.com),*
Danışman: *Yrd. Doç. Dr. Hüseyin ÇAKIR (<hcakir@gazi.edu.tr> / websitem.gazi.edu.tr/site/hcakir)*

Anahtar Kelimeler: *Disk şifrelemesi, FDE Full Disk Encryption, Yan Kanal Saldırısı (Side Channel Attack), Tempest, Ağ koklama (network sniffing), ARP şaşırtma (ARP spoofing), Network Monitoring, Network Tap, TrueCrypt, Bitlocker, EFS, Keylogger, BadUSB, Cold Boot, Bettercap, Tcpdump, Akustik Tempest, RF Tempest*

Özet

Bu çalışmada tam disk şifrelemesine (*FDE: Full Disk Encryption*) sahip olay yeri bilgisayarlarından delil elde etmede kullanılan teorik ve pratik yöntemler araştırılarak, şifreli disklerden adli delil elde etmede karşılaşılabilecek engellerin nasıl aşılabileceği incelenmiş ve uygulamalı olarak örneklendirilmiştir.

Adli bilişim ve olay yeri incelemeleri açısından ülkelerin mevzuatlarına ve adli bilişim uzmanlarının eğitimlerine göre değişen çeşitli delil elde etme pratikleri uygulanır. Bilgisayar çalışıyorsa ve oturum kilitli değilse ilk yapılması gerekenlerden biri bilgisayarın sürücülerinde bir disk şifreleme yazılımının çalışıp çalışmadığının araştırılmasıdır. Eğer varsa RAM'in kopyası alınarak şifreleme anahtarının elde edilmesi yoluna gidilir. Ancak bundan sonra disk imajı üzerinde bir adli inceleme gerçekleştirilmesi mümkün olabilir. Şifreleme anahtarı olmayan disk imajlarının şifrelerinin çözülmesi, kullanılan şifreleme türüne ve anahtarın uzunluğuna bağlı olarak çoğu zaman imkansız olmaktadır.

Olay yeri bilgisayarlarına ait disklerin *TrueCrypt*, *PGP*, *BitLocker*, *eCryptfs* ve *EFS*[1] gibi disk şifreleme yazılımları ile şifrelenmiş olduğu durumlarda, eğer bilgisayar oturumu kilitli ise, olay yeri inceleyicisinin şifreleme anahtarını elde etmeye yönelik uygulayacağı olağan senaryo büyük oranda sekteye uğrar.

Ancak böyle durumlara karşı kilitli ve çalışan sistemlerden şifreleme anahtarının elde edilmesi için uygulanabilecek birçok yöntem bulunmaktadır.

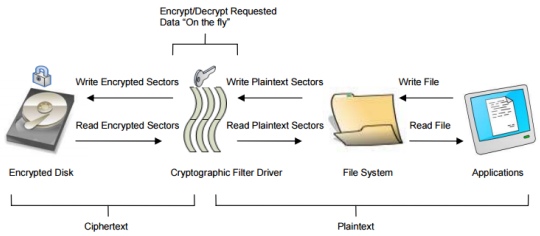
Bu çalışmada kilitli oturuma sahip FDE korumalı olay yeri bilgisayarlarından şifreleme anahtarını elde etmeye yönelik çok geniş bir literatür araştırması yapılmış, teorik ve pratik karşılığı olan ve uygulanan bir çok tekniğe yer verilmiş, yeni sayılabilecek bir teknik olan ağ trafiğinden delil elde edilmesi konusu örneklendirilerek gösterilmiştir.

[1] Disk Şifreleme Yazılımları - https://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software

Giriş

Diski tam şifrelenmiş bir bilgisayar kapatılıp, disk imajı alındığında elde edilen bilgiler de tamamen şifrelenmiş olduğundan üzerinde bir inceleme yapılması mümkün değildir. Ancak diskin şifreleme parolası veya anahtarı elde edildiğinde bu imaj adli bilişim incelemesi açsından anlam kazanabilmektedir[i].

FDE çözümleri çoğunlukla yazılım tabanlıdır. İşletim sisteminin çekirdek seviyesinde çalışan şifreleme yazılımı, disk ile dosya sistemi arasında yer alarak diske yazılan verilerin diske şifreli yazılmasını sağlar. Bu işlem kullanıcıdan tamamen yalıtılmış olarak gerçekleşir ve kullanıcı olağan dosya işlemlerini hiçbir farklılığa gerek olmadan gerçekleştirebilir. O kadar ki çoğu zaman disk verilerinin şifrelenerek yazıldığını fark edemez.



Şekil 1 - Tam Disk Şifrelemesinin Çalışması

FDE korumasına sahip bir bilgisayar sisteminin imaj alma işlemi öncesinde şifreleme anahtarını elde etmek için birçok yöntem vardır.

İnceleme yapılacak sistem ile bağlantılı olarak görev yapan bilgi teknolojileri çalışanları ve yöneticileri de şifreleme anahtarının elde edilmesi için yararlanılabilecek kaynaklardan biridir. Kurumsal organizasyonlarda şifreleme anahtarlarının korunması de belli prosedürlerle yerine getirilir.

Disk imajı alınmış bir sistemde şifreleme anahtarını elde etmek için kullanılan ilk yöntem Brute Force (Kaba Kuvvet) adı verilen olası tüm parolaları denemeyi öngören yöntemdir. Bu yöntemde öncelikle olay yerinden elde edilen bilgiler ışığında bir kelime listesi oluşturularak, şifrelenmiş veri üzerinde otomatize edilmiş parola denemeleri gerçekleştirilir. Bu teknikte en önemli unsur yeterince iyi bir parola kelime listesini oluşturabilmektir. Şüphelinin geçmişi ve ilgi alanları hakkında web üzerinde yapılacak bir araştırma ile elde edilen kelimeler listeye dahil edilir. Bu listeye şüphelinin flash bellek, diğer bilgisayar sistemleri ve not defteri gibi kişisel eşyalarının incelenmesi neticesinde elde edilecek bilgilerden toplanan olası kelimeler de dahil edilebilir. Yöntemin başarısı tamamen kelime listesinin kalitesine ve parolanın karmaşıklığına bağlı olarak sonuçlanır. Kişi yeterince uzun ve karmaşık bir parola kullanmışsa (Örneğin: harf,rakam ve sembollerden oluşan 20 karakterlik bir parola) bu yöntem yüksek oranda başarısızlıkla sonuçlanır. Diğer taraftan ilerleyen yıllarda diskin şifrelenmesinde kullanılan algoritmada keşfedilecek olası zafiyetler bu durumun içinden çıkılmasını sağlayabilir fakat adli incelemeyi dolayısıyla adaleti geciktirecek bu ihtimal de pratikte bir işe yaramayacaktır. Bunlardan dolayı şifreleme anahtarının farklı yöntemler ile elde edilmesi gerekliliği doğar. [iii]

Bu çalışmada FDE korumasına sahip diskin şifreleme anahtarına yönelik kaba kuvvet saldırısı dışında nasıl çözülebileceği hakkında kapsamlı bir araştırma yapılmış ardından uygulanabilirliği yüksek ve kısa sürede etkin sonuç verebilecek bir adli bilişim yöntemi üzerine odaklanılmıştır.

1. FDE Anahtarını Kullanıcı Oturumu İçinden Elde Etmek

FDE korumasına sahip bir bilgisayar sisteminde adli inceleme yapabilmenin bir diğer yolu da, sistem halen çalışmakta iken, sistemde oturum açarak dosya sistemine erişim sağlamaktır. Sistem de oturum açılabiliyorsa şifreleme anahtarının elde edilmesi bellek (RAM) taraması sonrası mümkün olmaktadır.[ii]

FDE korumasına sahip sistemde oturum açılmasını zorunlu kılan bu yöntem diskin şifreleme anahtarını elde etmek için uygulanabilecek en önemli yöntemdir. FDE korumalı olay yeri bilgisayarlarında kanun güçlerinin sıklıkla karşısına çıkan en büyük engel kilitli oturumlardır.

Kanun güçleri tarafından kilitli oturumları açmak için kullanılan bazı yöntemler şunlardır:

1.1 Keylogger Kullanmak

Donanımsal bir keylooger (tuş kayıtçısı) ile şifreleme anahtarı veya oturum parolası elde edilir. Donanımsal tuş kayıtçısı gizli olarak klavye ile bilgisayarın klavye giriş portu arasına bağlanarak basılan tuşlar kayıt altına alınır.

Şekil 2 - Donanımsal Tuş Kayıtçısı

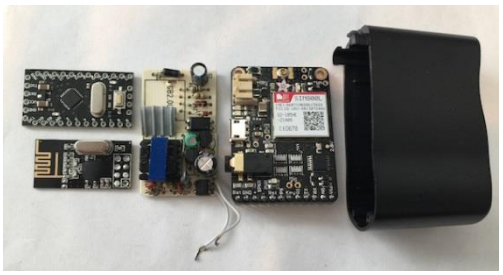
Bu konuyla ilgili *Amerikan Kolluk Kuvvetleri* (FBI) ve kanun koyucuları bilgisayara donanımsal bir tuş kayıtçısı (*keylogger*) bağlayarak parolayı elde etme yöntemini kullanmaktadırlar[i].

Donanımsal tuş kayıtçılarının gelişmiş sürümleri basılan tuşları depolamanın yanında kablosuz (Wireless) olarak aktararak da kanun güçlerinin erişimine sunar.

Şekil 3 - Kablosuz Donanımsal Tuş Kayıtçısı

1.2 Gizli Kablosuz Klavye Alıcısı Kullanmak

Olay yerinde kablosuz bir klavye kullanılıyor ve klavyenin marka/modeli biliniyorsa, kanun güçleri bu klavyeye uygun bir radyo frekansta alıcı kullanarak tuş basımlarını ele geçirebilirler.[iii]



Şekil 4 - Kablosuz Klavye Alıcısı (KeySweeper)

Key Sweeper adlı ürün klavyenin yakınına konuşlandırılarak basılan tuşlar canlı olarak (kablosuz aktarım sayesinde) elde edilebilmektedir. Bu yöntem FDE korumalı olay yeri bilgisayarına belli bir yakınlıkta bulunmayı gerektirdiğiden uygulama zorluğuna sahiptir.

1.3 Doğrudan Bellek Erişimi Kullanmak (DMA)

FDE korumasına sahip bir olay yeri bilgisayarının oturum ekranının kilitli olması şifreleme anahtarının elde edilmesine ve inceleme yapılmasına engel olur. Halen çalışmakta ve oturumu kilitli durumdaki bilgisayar sistemine giriş yapmak için kolluk güçleri tarafından DMA (*Direct Memory Acces: Doğrudan Bellek Erişimi*) saldırısı olarak adlandırılan yöntem de kullanılabilmektedir.[iv]

Bu yöntemde, çalışmakta olan bilgisayarın belleğine doğrudan erişim sağlamak için DMA (*Doğrudan Bellek Erişimine*)'ya izin veren portlar veya genişleme yuvaları (*PCIe, FireWire, ExpressCard, Thunderbolt*) ile bilgisayarın belleğine canlı olarak erişim sağlanmaktadır.[v]

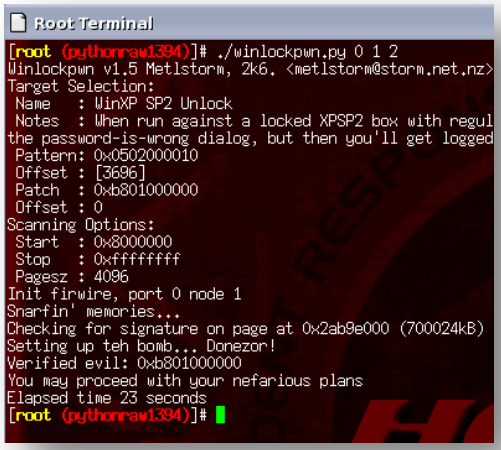
Bu erişim işletim sisteminden tam bağımsız olarak gerçekleşmektedir. Hem herhangi bir işletim sistemi türüne bağımlılık yoktur hem de işletim sisteminin bu işlemi engelleme şansı yoktur. DMA ile belleğe erişim sağlandığında dosya sisteminin şifreleme katmanını idare eden yazılımın kullanmakta olduğu şifreleme anahtarı ve oturum parolası RAM'den okunabilmektedir. Çünkü bu anahtar her an diske yazılan verileri şifrelemek için açık şekilde bellekte saklanmaktadır.

DMA'nın belleğe doğrudan erişim verdiği FireWire kontrolörü (*FireWire, USB2.0 dan daha hızlı video/görüntü aktarımına izin veren bir medya aktarım portudur*) kullanılarak bu işlem pratik olarak gerçekleştirilebilir.[2]

Şekil 5 - FireWire Portu

Bu amaçla oturumu kilitli Windows işletim sistemlerinde kullanılabilecek programlardan birisi de **Winlockpwn**'dir. Program aslında linux tabanlı bir python betiğidir. Olay yeri bilgisayarına FireWire kablosu ile bağlanarak çalıştırılır ve örneğin Windows işletim sisteminin oturum giriş ekranını baypas ederek oturumu açar.

Benzer şekilde ***Passware*** firması tarafından geliştirilen **Passware Kit Forensic** adlı adli bilişim yazılımının içinde gelen **FireWire Memory Imager** adlı yazılım bir FireWire kablosu ile hedef bilgisayarın FireWire portuna bağlanarak exploit çalıştırılabilmekte ve hedef bilgisayarın tam bir bellek kopyası elde edilebilmektedir.[3]

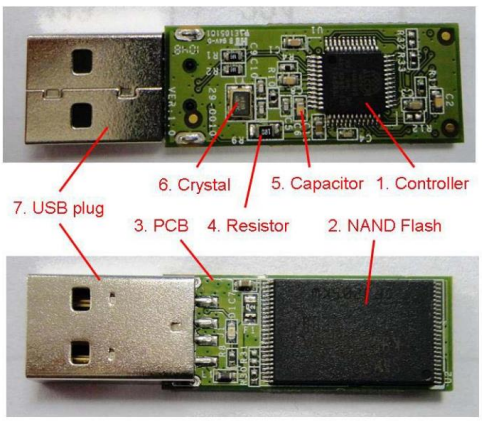


Şekil 6 - Winlockpwn ile Windows oturum kilit ekranının aşılması

1.4 Değiştirilmiş USB Firmware Yöntemi (BadUSB)

Bu yöntemde sıradan bir USB Flash belleğin USB Firmware'i (*öz yazılımı*) modifiye edilerek istenen kodun işletim sistemi tarafından otomatik olarak çalıştırılması sağlanır. Bu kod genellikle aktif oturumun parolasını sıfırlayan komutları içermektedir.

USB Firmware diğer adıyla USB öz yazılımı USB flaş belleğin işletim sistemi olarak düşünülebilir. Bir USB bellek donanımsal açıdan bellek ve usb giriş çıkış kontrolcüsü (USB Micro Controller) olmak üzere iki ana kısımdan oluşur.



Şekil 7 - USB Flash Donanım Bileşenleri

Bellek de veriler tutulurken, USB kontrolcüsü bilgisayarın usb kontrolcüsü ile iletişim kuran protokolü idare eder. Kontrolcü ve dolayısıyla içerisinde çalışmakta olan program flaş belleğin fiziksel

[2] Oturumu Kilit Ekranını Bypass Etmek için Winlockpwn Programı - http://wiki.airdump.cz/Winlockpwn

[3] Passware Firmasının FireWire Memory Imager İsimli Yazılımı - http://www.lostpassword.com/hdd-decryption.htm

özelliklerini (Disk boyutu, seri numarası, marka model vb) host bilgisayara bildirmek, bilgisayardan gelecek dosya taleplerini dinlemek, veri transferini başlatmak ve sonlandırmak, hatalı veri aktarımlarını düzeltmek gibi görevleri yerine getirir. Tüm bu işleri yerine getiren ve USB kontrolcüsü içinde çalışan yazılıma (*usb'nin işletim sistemi*) USB Firmware adı verilir.[vi]

Bu yöntemi kullanarak bilgisayarda kod çalıştırmaya izin veren ilk keşif **BadUSB** adıyla yayılmıştır. Bad USB Almanya merkezli SR Labs güvenlik şirketinin ortaya çıkardığı yeni bir güvenlik açığı tipidir. Bu açık kullanılarak bilgisayara USB yoluyla bağlanan her türlü cihaz bilgisayar üzerinde kod çalıştırmak için kullanılabilir. Bu zararlı kod USB Flash belleğin dosya sistemi üzerinde yer almadığı için Antivirüsler tarafından tespit edilemez ve engellenemez. [vii]

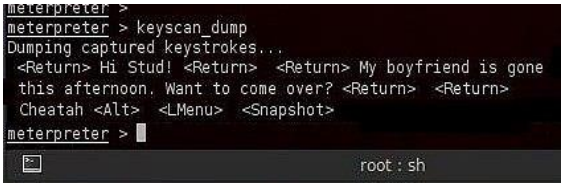
BadUSB için **Lumension** adlı firmanın Endpoint Security[4] adlı ürünü Device Control Policy özelliği ile bu işlemin başarıya ulaşmasını engelleyebilmektedir.

1.5 Yazılımsal Zaafiyet Suistimali (Exploit) Yöntemi

Olay yeri bilgisayarının ağına dahil olduktan sonra *Metasploit Framework* adı verilen zafiyet tarayıcısı ve suistimal aracı kullanılarak uzak sistem üzerinde zayıflık taraması yapılır ve uzaktan keylogger (tuş kayıtçısı) yüklenir.

Metasploit, çeşitli pentestler gerçekleştirmek için içerisinde exploitler, payloadlar, uxiliaryler ve encoderlerin bulunduğu bir framework yapısıdır. Metasploit; Linux, Windows Mac-OS ortamlarında çalışabilmektedir.[5]

Metasploit ile sadece direkt saldırı yapılmaz. Örneğin tuş kayıtçıları (keylogger) gibi çeşitli backdoor'lu dosyalar oluşturulup bunlar ile de hedef sistemde şifre öğrenmeye veya parola sıfırlamaya yönelik saldırılar gerçekleştirilebilir. Tuş kayıtçısı bir turuva atı gibi çalışır ve TCP/IP üzerinden basılan tuşların aktarılmasını sağlar.



Şekil 8 - Metasploit Keylogger'ın Çalışması

1.6 Tempest Yöntemlerini Kullanmak

TEMPEST, "gizlilik dereceli" bilgi işleyen elektrikli ve elektronik teçhizattan kaynaklanan istem dışı RF (Radyo Frekans), Işık, Ses, Titreşim verilerinin yakalanarak anlamlandırılması olarak tanımlanabilir. Başka bir tabirle elektronik bir sistemde gerçekleşen bilgi sızıntısı olarak da söylenebilir.[6]

Şekil 9 - Tempest

Tempest ile uzaktaki bir bilgisayarın yaydığı elektro manyetik ve ses dalgaları yorumlanarak klavyesi dinlenebilir, ekran görüntüsü alınabilir veya hangi assembly komutlarını çalıştırdığı öğrenilebilir. Tempest tekniği çok basit iki elektriksel prensibe dayanır.

1) İçerisinden elektrik akımı geçen iletkenin etrafında bir manyetik alan ve buna bağlı olarak bir radyo frekans ışınımı oluşur.
2) Bir iletken üzerine radyo frekans ışınımı gönderilirse iletken üzerinde buna bağlı olarak bir elektrik sinyali oluşturulabilir. (Elektrik jeneratörlerinin çalışma prensibi)

[4] Lumension Endpoint Security - https://www.lumension.com/kb/Home/General-Information/1694.aspx

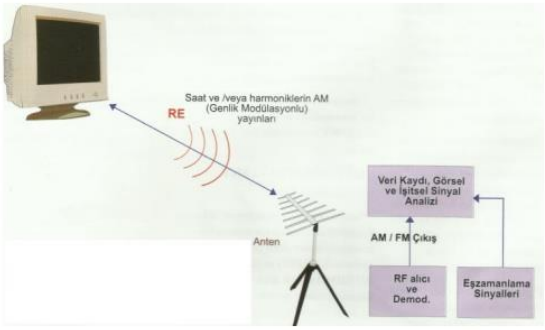
[5] Metasploit - http://www.hackings.org/2012/06/nedir-bu-metasploit.html

[6] TEMPEST - http://www.aysamakses.com/tr/bilgi-bankasi/tempest/

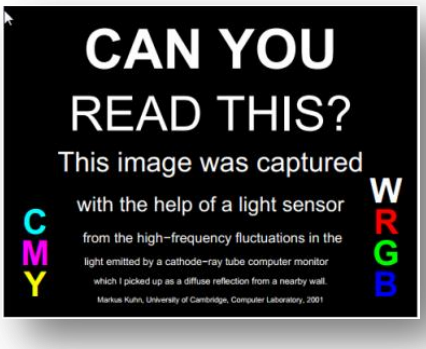
1.6.1 TEMPEST ile Monitörü İzlemek

Bu konuyla ilgili ilk akademik çalışma 1985 yılında Wim van Eck adında bir Hollandalı tarafından yapılmıştır. Bu makalede video kartından alınan elektromanyetik sinyaller sayesinde görüntünün başka bir yerde oluşturulmasının başarılabileceği ispatlanmıştır[viii].

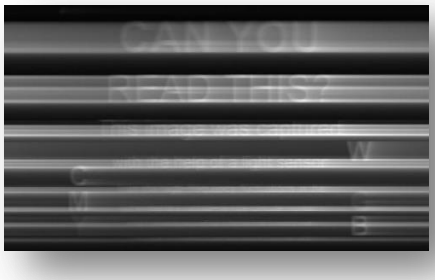
Bundan sonra yapılan çalışmalar cihazlardan alınabilecek her türlü dalganın bir şekilde analiz edilerek anlamlı veri haline dönüştürebileceğini göstermektedir. Örneğin yapılan bir çalışmada renkli CRT monitörlerden alınan sinyallerin çeşitli filtrelerden geçirilerek görüntü tekrar elde edilebilir. Aşağıda elde edilen görüntüler bulunmaktadır:



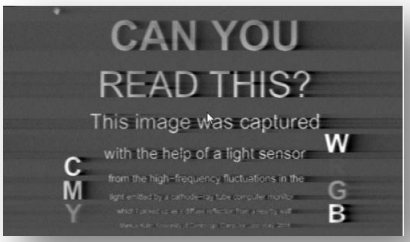
Şekil 10 - Tempest ile bir CRT Monitördeki Görüntünün Elde Edilme Düzeneği



Şekil 11 - Ekrandeki Orjinal Görüntü



Şekil 12 - Elde Edilmiş Görüntü



Şekil 13 - Filtre Edilmiş Görüntü

Şekil 14 - Başka Bir Filtre Kullanılarak Elde Edilmiş Görüntü

Ayrıca sadece CRT monitörlerde değil, flat-panel ve LCD monitörlerde de görüntü elde etmeye dair çalışmalar bulunmaktadır [ix]. Aşağıda bir diz üstü bilgisayarın ekranından elde edilen görüntüler bulunmaktadır:

Şekil 15 - 3m Uzaktaki Bir Laptop'tan Alınan Linux Açılış Ekranı

Şekil 16 - 10 m uzaktaki arada 3 duvar bulunan bir laptoptan alınan görüntü

1.6.2 RF Sinyalleri ile Klavyeyi Uzaktan Okumak

İsviçreli EPFL araştırma kuruluşunda 12 farkı marka model kablolu klavye ile yapılan tempest çalışmasında klavyerlerin 20m öteden tuş basımları alınmıştır.[7]

Blackhat konferansında yapılan bir sunumda PS/2 klavye üzerinde yazılan her tuş basımının elektrik hattında oluşturduğu sinyal sayesinde aynı elektrik hattını paylaşan uzak başka bir yerden elde edilebileceği gösterilmiştir. Bu sayede örneğin bir otelde yan odadaki yazılanlar alınabilir. Ayrıca ATM'lerin genellikle PS/2 klavye kullandığı düşünülürse bir başka potansiyel atak yeri olduğu görülebilir.

1.6.3 Lazer İle Klavyeyi Uzaktan Okumak

Blackhat konferansında yapılan başka bir sunumda, klavye tuşlarına basarken ekranda oluşan titreşimlerin lazer ile alınarak alıcıya yansıtılması sonucunda oluşan sinyallerin analiz edilerek klavyede yazılanların tespit edilebileceği gösterilmiştir.

Şekil 17 - Lazer Uygulanan Yansıma Yüzeyleri

1.6.4 Akustik Tempest Yöntemini Kullanmak

Bu yöntemde elektronik sistemin çıkardığı sesler odaklanmış bir akustik anten ile veyahut yakına yerleştirilmiş yeterli hassasiyetteki bir mikrofon ile alınarak analiz edilmekte ve karşılaştırmalı bir analizin sonucunda elektronik sistem tarafından işlenen veri ve çalıştırılan komutlar elde edilmektedir. [8]

Sistemin ana fikri tüm elektronik cihazların ihtiyaç duyduğu, şebeke gerilimini cihazın çalışma gerilimine indirgeyen regülatör devresinin içerdiği kapasitif (C) ve endüktif (L) elemanların, yüksek frekanslı sinyallerde tiz bir ses yayıyor olmasına dayanmaktadır. Yeterli hassasiyete ve filtreleme kabiliyetine sahip donanım ile cihazın işlediği veriye paralel olarak regülatör elemanlarının çektiği akımın orantılı olarak C ve L elemanları üzerinde yarattığı ses titreşimleri ile veri analizi yapılmaktadır.

[7] Tempest Keylogger - http://www.tankado.com/keylogger-donanim-yazilim/

[8] RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis - https://www.tau.ac.il/~tromer/acoustic/

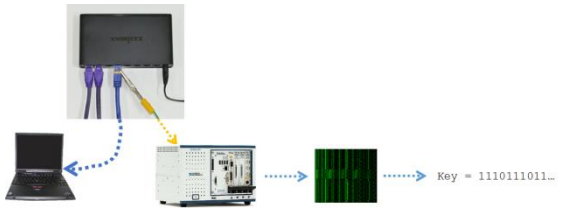
Şekil 18 - Voltaj regülatörlerinin gürültülü elemanları olan Bobin ve Kondansatörler

Şekil 19 - Akustik tempest ile uzaktaki bilgisayarın okunması

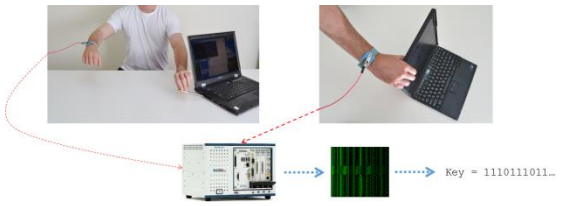
Bu yöntem ile bir şifreleme ve şifre çözme sırasında kullanılan şifreleme anahtarı alınabileceği gibi oturum açma sırasındaki parola girişleri de elde edilebilmektedir. [9]

1.6.5 Elektromanyetik Sondalama Yöntemi

Yeni bir yan kanal saldırısı olan bu yöntemde cihazın gövdesinin toprağa (ground) göre sürekli değişim halinde olan elektrik potansiyelinin cihazın işlediği veri hakkında bilgi verme potansiyelinden yararlanılmaktadır. Yöntemde söz konusu potansiyel bilgisayarın Kasası, USB portu, Ethernet portu ve VGA gibi kapasitif bileşenlerindeki elektrik potansiyeli basit bir kablo ile alındıktan sonra güçlendirilmekte ve sayısallaştırılmaktadır. Bu şekilde bilgisayara veya bağlı olduğu diğer bileşenlere (ethernet kablosu, usb kablosu güç kablosu vb.) fiziksel temas gerçekleştirilerek birkaç saniye içerisinde RSA anahtarının kopyalanması mümkündür. [10]



Şekil 20 - Cihazın ethernet kablosundan potansiyel elektriğin kopyalanması



Şekil 21 - Cihaza dokunarak RSA anaharının kopyalanması

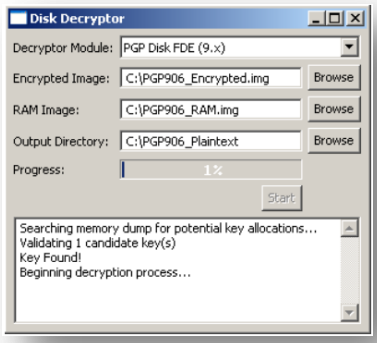
2. Şifreleme Anahtarının RAM'den Ayıklanması

Oturum açıldıktan sonra FDE korumalı sistemin disk şifreleme anahtarının elde edilmesi için yapılması gereken RAM'in bit kopyasının çıkartılmasıdır. Bu işleme Memory Dump adı verilmektedir. Hali hazırda kernel modda çalışmakta olan şifreleme sürücüsü şifreleme anahtarını RAM'de saklar. RAM dump'ı üzerinde yapılacak bir tarama ile şifreleme anahtarı elde edilebilir.

[9] Akustik yöntem ile elektronik sistemlerin koklanması - https://www.tau.ac.il/~tromer/ecdh/

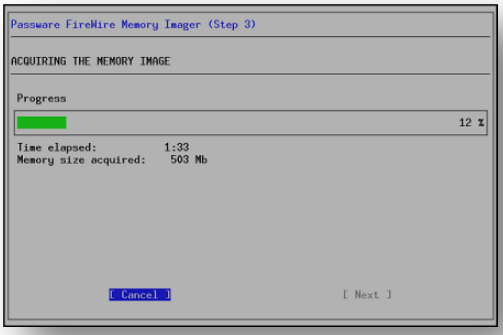
[10] Physical Side-Channel Key-Extraction Attacks On PCs - http://www.tau.ac.il/~tromer/handsoff/

2.1 FireWire ile Memory Dump Alma



Şekil 22 - Memory Dump üzerinde şifreleme anahtarı araması

Bu konuda **Passware** firmasının üretmiş olduğu *Passware FireWire Memory Imager*[11] adlı ürün en popüler yazılımlardan birisidir. Yazılım bir başka bilgisayara kurulmakta, bu bilgisayar FireWire portu aracılığı ile olay yeri bilgisayarına bağlanarak belleğin kopyası çıkartılmaktadır.



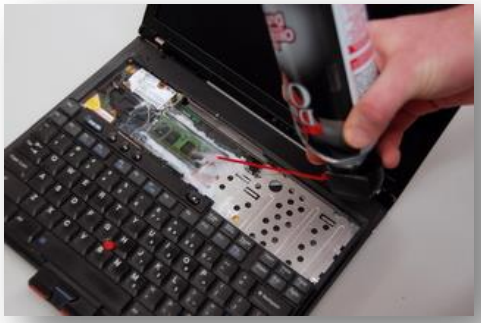
Şekil 23 - FireWire Memory Imager

Yazılım kopyasını çıkarttığı bellek kaydından BitLocker, TrueCrypt, FileVault2 ve PGP disk şifreleme yazılımlarına ait şifreleme anahtarlarını elde edebilmektedir.

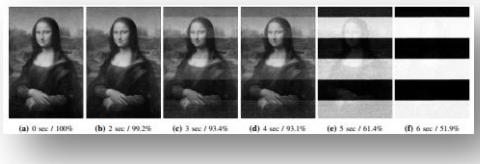
2.2 Coldboot yöntemi

Eğer hedef bilgisayarda oturum açılamıyorsa (parola korumalı oturum ve doğal olarak FDE koruması) bilgisayarın enerjisi kesildikten sonra RAM sökülerek bir okuyucuya bağlanarak dump'ı alınabilir. DRAM'ler enerjisi kesilse dahi saniyelerden dakikalara varan sürelerde üzerindeki veriyi muhafaza etmeye devam ederler.[12]

Bu işlem çok hızlı yapılması gereken bir işlemdir. İşlemin süresini uzatmak için RAM'e kontrollü biçimde sıvı nitrojen püskürtülerek dondurulması ve üzerindeki veriyi daha uzun süre muhafaza etmesi sağlanabilir.[13]



Şekil 24 - RAM sıvı nitrojen ile soğutulması



Şekil 25 – Bir DRAM üzerindeki coldboot attack'in zamana göre başarım durumu

Yukarıdaki şekilde coldboot yöntemi ile bir DRAM'dan elde edilebilecek verinin geçen zaman karşısında veri kaybı karşılaştırılmıştır. Şekilde DRAM'den dump edilen verinin oda sıcaklığında (25 santigrat derece) sırasıyla 1,2,3,4,5 ve 6. saniyelerdeki kayıp miktarına yer verilmiştir. [14] RAM türüne göre uygun sıcaklığın sağlanması durumunda (ki bu sıcaklık değeri işlem süresinin uzatmada doğru bir orantıya sahip değildir) DRAM üzerindeki veri dakikalarca korunabilmektedir. Bu işlemi engellemek için RAM modülünün bağlı olduğu

[11] Acquiring Memory Image Using Passware FireWire Memory Imager - http://www.lostpassword.com/hdd-decryption.htm

[12] Cooldboot Yöntemi - https://citp.princeton.edu/research/memory/

[13] Sıvı nitrojen ile RAM'in soğutulması - https://citp.princeton.edu/research/memory/media/

[14] Cold Boot Attack - https://www1.cs.fau.de/filepool/projects/coldboot/fares_coldboot.pdf

karta kalıcı olarak sabitlenmesi veya lehimlenmesi çözümü tavsiye edilmektedir.

3. Alternatif FDE Çözümü Olarak Ağ Trağinin Koklanması Yoluyla (Network Sniffing) Delil Elde Edilmesi

Buraya kadar şifreleme anahtarı bilinmeyen FDE korumasına sahip bir diskin adli incelemesinin hangi yöntemler kullanılarak yapılaceğine değindik.

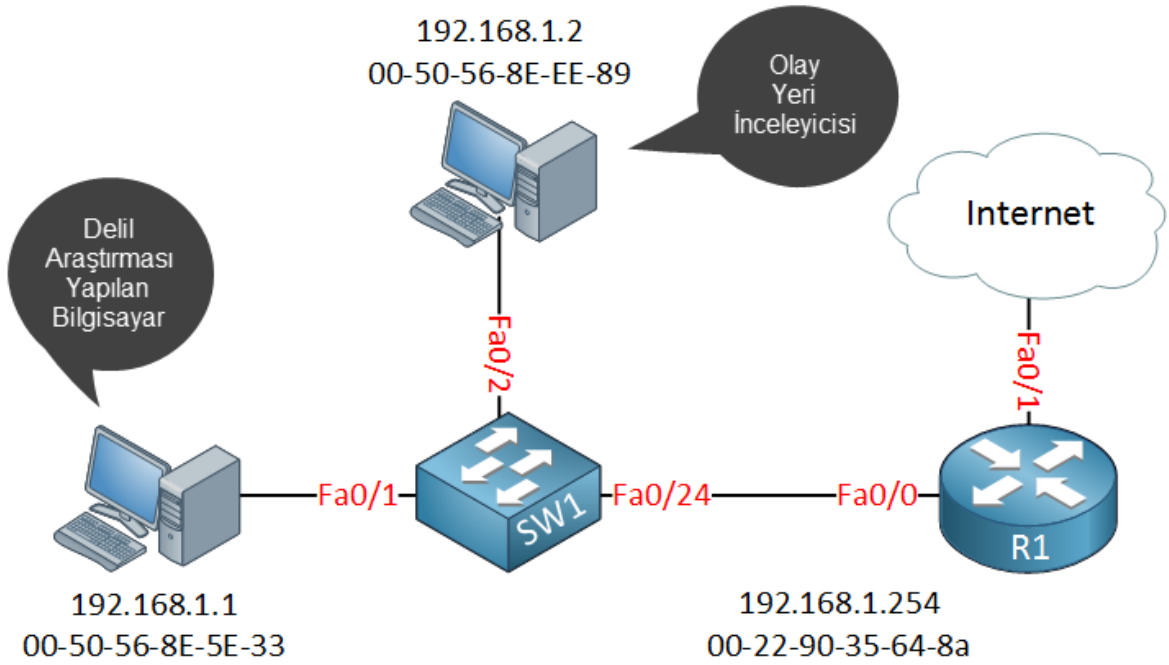
FDE korumalı bir bilgisayarın oturumuna erişim sağlanamadığı durumlarda bilgisayarın ağ trafiğini incelemek suça yönelik önemli deliller sunabilir. Bu bölümde suça konu olan olay yeri bilgisayarının ağ iletişimini adli incelemeci tarafından kaydedilerek, daha sonra bu kayıt üzerinde suça yönelik delil araştırmasının nasıl yapılabileceği anlatılacaktır.

Yapılacak işlem 3 ana kısımdan oluşmaktadır:

1. Olay yeri bilgisayarının ağına dahil olmak
2. Olay yeri bilgisayarının ağ trafiğinin ele geçirilmesi ve kaydedilmesi
3. Kaydedilen trafik üzerinde delil araştırmasının yapılması

3.1 Olay Yeri Bilgisayarının Ağına Dahil Olmak

Olay yeri bilgisayarının ele geçirilmesi için Kali Linux kurulmuş taşınabilir bir bilgisayar olay yerinde hali hazırda bulunan Switch ile aşağıda yer alan topolojideki ağa dahil olmuştur.



Şekil 26 - Olay yeri ağ topolojisi

Bu aşamadan sonra; incelemesi yapılacak bilgisayarların IP adreslerini öğrenmek için ***nmap*** ağ tarayıcısı kullanılarak bir ağ taraması gerçekleştirilmiştir.

```
kali@tankado.com ~ $ ifconfig eth0

eth0      Link encap:Ethernet  HWaddr b8:27:eb:9b:12:4f
          inet addr:10.1.1.1  Bcast:10.1.1.255  Mask:255.255.255.0
          inet6 addr: fe80::ba27:ebff:fe9b:124f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:142936 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13365 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7381997 (7.0 MiB)  TX bytes:2565720 (2.4 MiB)

kali@tankado.com ~ $ hostname -I
10.1.1.1 192.168.0.155

kali@tankado.com ~ $ nmap 192.168.0.0/24

Starting Nmap 6.47 ( http://nmap.org ) at 2016-05-20 02:34 EEST
Nmap scan report for 192.168.0.1
Host is up (0.033s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http

Nmap scan report for 192.168.0.155
Host is up (0.026s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap scan report for 192.168.0.100
Host is up (0.033s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
443/tcp   open  https
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
2968/tcp  open  enpp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49175/tcp open  unknown

Nmap done: 256 IP addresses (3 hosts up) scanned in 19.25 seconds
```

Şekil 27 - Bettercap Aracının Kurulması Ve Çalıştırılması

Ağ taraması sonucunda ağda inceleyicinin ki ile birlikte 3 cihazın bulunduğu 192.168.0.100 adresli olay yeri bilgisayarının Windows işletim sistemini kullandığı görülmüştür. 192.168.0.1 IP adresli bilgisayarın 80. Portu web tarayıcısı ile ziyaret edildiğinde cihazın bir MODEM olduğu anlaşılmıştır. Ayrıca route komut çıktısından da DHCP servisi çalışan ağın varsayılan yönlendiricisinin de bu cihaz olduğu görülmüştür.

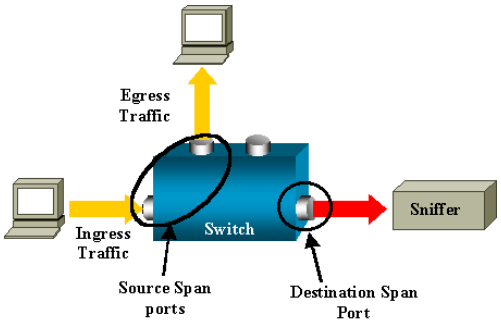
3.2 Olay Yeri Bilgisayarının Ağ Trafiğinin Kopyalanması ve Kaydedilmesi

Ağ incelemeleri gerek olaya müdahale ve gerekse inceleme analiz safhaları bilgisayar incelemelerinden farklı olduğunda bu alanda kullanılan yazılım, donanım, cihaz ve sistemler de farklıdır. Ağ üzerinde oluşan bir olayla ilgili kanıtları toplayabilmek için iki husus çok önemlidir:[x]

- Olay devam ederken gerçek zamanlı olarak ağın tamamının ya da olayla ilgili bölümünün kopyasının alınması.
- Olay bitmiş olsa bile, olayla ilgili hususları ortaya çıkartmak ve olayın nasıl cereyan ettiğini tespit etmek amacıyla ağın tamamının ya da olayla ilgili bölümünün kopyasının alınması.

3.2.1 Ağ Trafiğinin Port Mirroring Yöntemi ile Kopyalanması

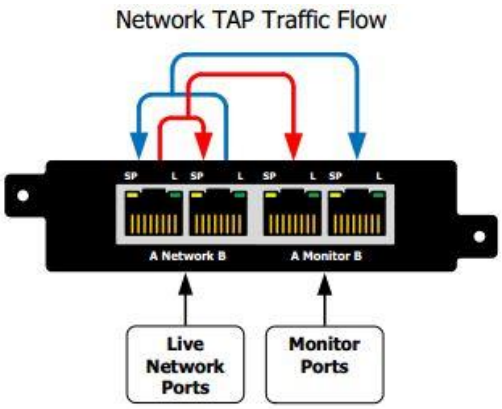
Adli incelemenin yapılacağı olay yerinde kullanılan ağ yapısına bağlı olarak ağı teşkil eden ve tüm trafiğin üzerinden geçtiği Switch'in (Ağ anahtarlayıcısı/yönlendiricisi) bir analiz portu bulunabilir. Analiz portu ile Switch üzerindeki istenilen portun analizi yapılabilir. Ayrıca gelişmiş Switch'lerde yer alan Port Mirroring (Port Aynalama) özelliği ile olay yeri bilgisayarının Switch üzerinde bağlı olduğu port, olay yeri inceleyicisinin bağlı olduğu switch portu ile eşleştirilebilir. Bu durumda olay yeri inceleyicisinin sadece kendi bilgisayarındaki paketleri kaydetmesi yeterli olur. Saldırganın tüm trafiğinin bir kopyası, olayı yeri inceleyicisinin ağ portuna da gönderilir.



Şekil 28 - Port Mirroring ile Trafiğin Kopyalanması

3.2.2 Ağ Trafiğinin Network Tap Cihazı İle Kopyalanması

Port Mirroring yapılamayan ağ ortamlarında switch üzerindeki trafiğin kopyalanması için Network Tap (Ağ Kayıt) cihazları kullanılabilir. Network Tap cihazları aynı switch üzerinde gerçekleştirilen port aynalama yönteminde olduğu gibi portlarından biri üzerindeki trafiği diğer portuna kopyalar . Bu cihazlar fiber optik bağlantıları da kopyalayabildiği gibi ethernet'de GBit'e varan hızları da destekleyebilmektedir.



Şekil 29 - Bir Network Tap Cihazı ve Bağlantı Şeması

3.2.3 Ağ Trafiğinin HUB ile Kopyalanması

Hub'lar switch'lerde olduğu gibi ağ destekli cihazları birbirine bağlayarak iletişim kurmalarını sağlayan bir elemandır. 90'lı yıllarda kullanılan ve artık yerini switch'lere bırakan HUB'lar, switch'lerden farklı olarak

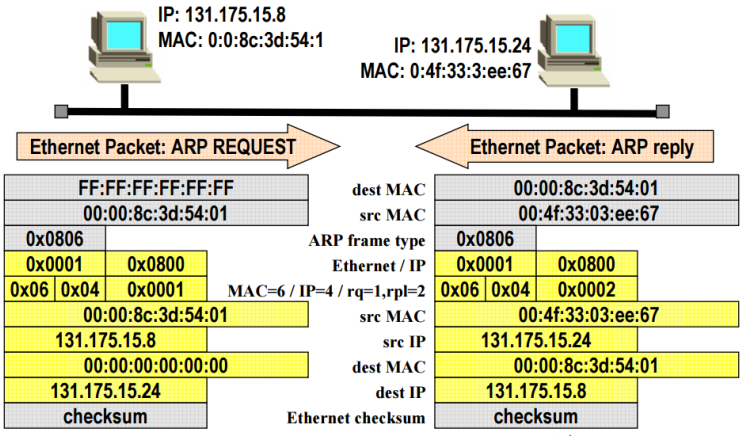
port anahtarlaması yapmaz, gelip giden veriyi tüm portlarına broadcast yaparak çalışır. Bu anlamda HUB'lar doğal bir Network Tap cihazıdır fakat günümüzde üretimi durduğundan bulunması zordur, bulunsa bile günümüz ağlarının iletişim hızlarını karşılayabilmeleri çok güçtür. Diğer taraftan HUB'lar brodcast yöntemi ile çalıştığından portlar arasında collision yani paket çarpışması sık karşılaşılan bir durumdur. Böyle durumlarda veri paketi zarar gördüğünden tekrar edilmesi istenir ve ağ da fazladan trafik oluşur. Bu nedenlerle adli bilişim açısından sağlıklı veriler vermesi zordur.

3.2.4 Ağ Trafiğinin ARP Şaşırtma (Layer 2) Yöntemi ile Kopyalanması

Konsoluna ulaşılamayan kilitli durumdaki olay yeri bilgisayarının ağ trafiğinin kaydedilebilmesi için inceleyici, MITM (Man–in-the-Middle) tekniği ile hedef (192.168.0.100) bilgisayara ARP-Spoofing saldırısı düzenleyerek, olay yeri bilgisayarı (192.168.0.100) ile Router / Modem (192.168.0.1) arasındaki tüm trafiği ele geçirecek ve kendi üzerinden geçmesini sağlayacaktır. Böylece disk verilerine ulaşılamama ihtimali olan olay yeri bilgisayarının o anda gerçekleştirdiği ağ ve internet aktivitelerinden çeşitli suçlara yönelik delillere ulaşılabilmesi mümkün olacaktır.

ARP Spoofing saldırısı OSI'nin 2. katmanında (Datalink Katmanı) çalışan ARP protokolünün bir güvenlik zafiyetinden faydalanır. ARP mantıksal adreslerin (Network Katmanı) yani IP adreslerinin, fiziksel adreslere (DataLink Layer) yani MAC adreslerine dönüştürülmesi/çözümlenmesi için kullanılan bir protokoldür. Protokolün çalışması şu şekilde gerçekleşir: OSI'nin 2. Katmanında yer alan ethernet kartı, wireless router ve switch'ler sadece MAC adreslerini kullanarak iletişim kurabilirler. OSI'nin daha üst katmanlarında tüm işler IP adresleri ile halledildiği için IP adreslerinin MAC adreslerine dönüştürülmesi gerekir. IP adresi bilinen bir bilgisayarın MAC adresini öğrenmek için ilgili bilgisayar tüm ağa bir ARP REQUEST isteği yayınlar yani broadcast eder. Bu istek bir erhetnet frame'i içerisine yerleştirilerek ağdaki tüm bilgisayarlara ulaştırılır. IP adresinin sahibi olan bilgisayar bu isteği içerisine kendi MAC adresini yerleştirdiği nir ARP REPLY çerçevesi ile sadece isteği yapan bilgisayara yanıtlar. İsteği yapan bilgisayarda ilgili IP<->MAC eşlemesini kendi ARP tablosuna (ARP önbelleğine) kaydeder ve iki dakika boyunca burada saklar ve tekrar aynı IP adresi için ARP REQEST mesajı göndermez.

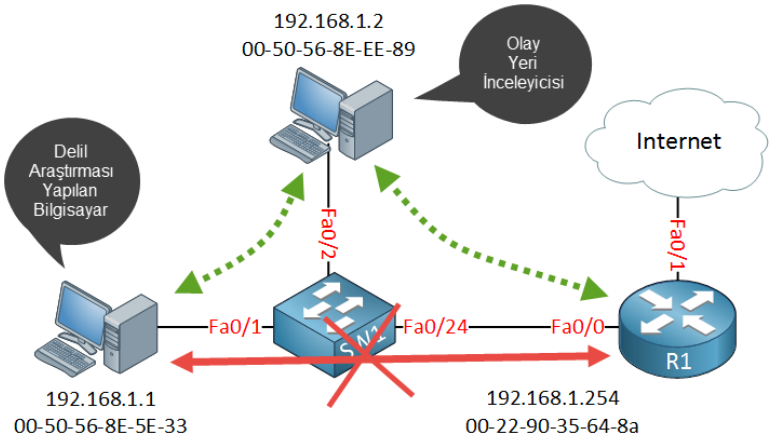
ARP Spoof'ing saldırısı tam da bu işleyiş içerisinde yerini alır. ARP protokolünün tasarımı gereği tüm ARP REPLY çerçeve paketleri koşulsuz olarak işleme konulur. Yani bir bilgisayar ARP REQUEST isteği göndermediği halde kendisine gelen tüm ARP REPLY cevaplarını doğru kabul eder ve ARP tablosunu bunlarla günceller. MITIM saldırısı yapmak isteyen kişi sürekli olarak hedef bilgisayarı ARP REPLY bombardımana tabi tutar ve ARP önbelleğini istedi MAC adresi ile güncel kalmasını sağlar.



Şekil 30 - ARP REQUEST ve ARP REPLY Çerçeve Paketlerinin Yapısı

Bu örnekte network'e bağlı bir olay yeri inceleyicisi gateway'in IP adresini ve kendi mac adresini içeren ARP REPLY anonsları yaparak diğer cihazların mac adres tablosunu güncellemekte ve artık default gateway'e (Modem/Router) ulaşmak istediğinde gitmesi gereken cihaz olarak olay yeri bilgisayarını görmesini sağlamaktadır.

Olay yeri inceleyicisi internete çıkmak için kendisine gelen bu paketleri dinleyip okuyabilir. Bu paketleri gerçek default gateway adresine yönlendir. Router da internet üzerinden gelen cevapları tekrar olay yeri inceleyicisine gönderir. Çünkü router'a bu istek paketlerini gönderen cihaz olay yeri inceleyicisiin cihazıdır. Olay yeri inceleyicisi yine bu cevap paketlerini de inceleyerek gerçek sahibine yönlendirir. Bu işlem sırasında gidip gelen tüm paketler kendi üzerinden geçtiği için şifreleme kullanılmadı ise tüm paketlerin içeriğine erişebilir.



Şekil 31- ARP Spoofing ile Olay Yeri Bilgisayarının Trafiğinin Ele Geçirilmesi

ARP spoofing saldırısı ile ağ trafiğini ele geçirmek için *Bettercap* adlı MITM (ortadaki adam) saldırı aracından faydalanılmıştır. *Bettercap* bilgisayar ağlarında MITM saldırısı

yaparak, HTTP, HTTPS ve TCP trafiklerini kaydetmek ve canlı olarak değiştirmek için geliştirilmiş açık kaynak kodlu esnek bir araçtır.

```
kali@tankado.com ~ $ apt-get update
kali@tankado.com ~ $ apt-get install bettercap
kali@tankado.com ~ $ bettercap -T 192.168.0.100 -X --sniffer-output
evidence.pcap

 _          _   _
| |__   ___| |_| |_ ___ _ __ ___ __ _ _ __
| '_ \ / _ \ __| __/ _ \ '__/ __/ _` | '_ \
| |_) |  __/ |_| ||  __/ | | (_| (_| | |_) |
|_.__/ \___|\__|\__\___|_|  \___\__,_| .__/
                                     |_| v1.5.3
http://bettercap.org/


[I] Starting [ spoofing:✔ discovery:✘ sniffer:✔ tcp-proxy:✘ http-proxy:✘
https-proxy:✘ sslstrip:✘ http-server:✘ dns-server:✘ ] ...

[I] [eth0] 192.168.0.199 : 00:0C:29:78:5C:02 / eth0 ( VMware )
[I] [GATEWAY] 192.168.0.1 : FC:4A:E9:3A:08:84 ( Castlenet Technology )
[I] [SNIFFER] Saving packets to /root/Desktop/evidences/evidence1.pcap .
[I] [TARGET] 192.168.0.100 : 50:E5:49:C5:49:0D ( Giga-byte Technology )
```

Şekil 32 - Bettercap'in Kurulumu ve Çalıştırılması

Yukarıdaki komutlar ile paket listeleri güncellenmiş ardından *apt-get* paket yükleycisi ile *bettercap* aracının kurulumu yapılmıştır.

bettercap aracının *–T* (*target*) parametresine verilen 192.168.0.100 IP adresi ile olay yeri bilgisayarının ağ geçidi ile olan trafiği inceleyicinin bilgisayarına yönlendirilmiş tüm ağ ve internet trafiği ***evidence.pcap*** paket dosyasına kaydedilmesi sağlanmıştır. Yaklaşık olarak 2 saatlik kayıtın sonunda 15GB'lık bir paket dosyası oluşmuştur. Bettercap çalıştığı süre boyunca sürekli olarak olay yeri bilgisayarına içerisinde Modem'in IP adresi 192.168.0.1 ve kendi MAC adresi olan ARP REPLY mesajları göndermektedir.

3.3 Kaydedilen Trafik Üzerinde Delil Araştırmasının Yapılması

evidence.pcap dosyası trafiğin kaydedildiği süre boyunca olay yeri bilgisayarı ile Modem arasındaki tüm veri trafiğini içermektedir. Pcap biçimli kayıt dosyasında inceleme yapmak için birçok araç vardır. Gerçekleşen veri trafiği hakkında bilgi edinmek için öncelikle trafiği katmanlarına ayırmakta fayda vardır. Bu katmanlardan kasıt OSI'nin 2. , 3., 4. Ve üst katmanlarında gerçekleşen ağ iletişimini anlamak üzerinedir. Böylece olay yeri bilgisayarının hem yerel ağ hem de uygulama düzeyindeki veri paketleri ile gerçekleşen trafiği hakkında genel bir fikir sahibi olunabilir. [xi]

3.3.1 Ağ Trafik Kaydının Protokol Analizinin Yapılması

Katman incelemesi için *tshark* isimli araç oldukça kullanışlı özellikler ve inceleme scriptleri sunar. Paket dosyasının içerdiği ağ verilerinin protokol dağılımını görmek için io,phs script'inin çıktısını inceleyelim:

```
kali@tankado.com ~ $ tshark -q -r evindence.pcap -z io,phs
Protocol Hierarchy Statistics
Filter:

eth                                      frames:1069453 bytes:2114008088
  ip                                     frames:1069453 bytes:2114008088
    tcp                                  frames:1013605 bytes:2087160006
      ssl                                frames:13 bytes:4464
      data                               frames:198050 bytes:3332399
      ftp                                frames:100003 bytes:12728
      http                               frames:10007 bytes:101071
      smtp                               frames:1485 bytes:102071
    udp                                  frames:55241 bytes:26803164
      quic                               frames:47849 bytes:26119339
      nbns                               frames:4651 bytes:427892
      dns                                frames:2500 bytes:197370
      nbdgm                              frames:241 bytes:58563
        smb                              frames:241 bytes:58563
          mailslot                       frames:241 bytes:58563
            browser                      frames:241 bytes:58563
    icmp                                 frames:607 bytes:44918
===================================================================
```

Tablo 1 - Trafik Dosyasının Protokol Dağılımı

Yukarıdaki çıktıda ilk dikkat çekenler SSL, SMTP ve FTP kullanımıdır. Yani olay yeri bilgisayarı inceleme kaydı sırasında FTP ve SMTP trafiği gerçekleştirmiştir. Bunun haricinde konsolu kilitli olan bilgisayarın normal dışı sayıda DNS trafiği gerçekleştirmiş olması da dikkat çekicidir. İlerleyen aşamalarda gerçekleşen bu iletişimin suç unsurları taşıyıp taşımadığı incelenecektir.

3.3.2 İletişim Kurulan Suç Ağlarına ait IP Adreslerinin Belirlenmesi

Tcpdump ve diğer string parselleme araçları ile kayıt dosyasında yapılan araştırma sonucu 2 saatlik iletişim sırasında aşağıdaki IP adresleri ile birçok kereler iletişim gerçekleştiği tespit edilmiştir:

```
kali@tankado.com ~ $ tcpdump -tnr evidence.pcap | awk -F '.' '{print
$1"."$2"."$3"."$4}'| sort | uniq -c | sort -n | tail
reading from file evidence01.pcap, link-type EN10MB (Ethernet)
7 IP 192.168.0.1
24 IP 64.12.25.91
28 IP 192.168.1.157
31 IP 205.188.13.12
38 IP 192.168.1.158
120 IP 27.247.180.15
. . .
```

Tablo 2 - İletişim Kurulan IP Adresleri

Komutun çıktısında yer alan her bir IP adreslerine whois sorgusu yapıldığında iletişimin ağırlıklı olarak "54.208.99.166" IP adresli Tayvan'dan hizmet veren bir porno networkünün sunucusuna odaklandığı anlaşılmıştır.

```
kali@tankado.com ~ $ whois -h whois.cymru.com 27.247.180.15
AS      | IP               | AS Name
9674    | 27.247.180.15    | FET-TW RedShine Adult Industry Inc. Taiwan
```

Tablo 3 - Hedef IP adresini Whois Sorgusu

3.3.3 Çocuk Pornosu Yayınının Tespiti

Olay yeri bilgisayarının önemli bir orandaki trafiği bu porno sunucusu (27.247.180.15) ile gerçekleşmiştir. Sunucu ile gerçekleşen iletişim hakkında daha detaylı bilgilere ulaşmak için trafiği oluşturan paketler zaman damgası ve paket sırasına göre TCP oturumlarına ayrıştırılması gerekmektedir. Böylece olay yeri bilgisayarı ile ilgili IP adresi arasında ne tür bir veri iletişimi olduğu görülebilecektir.

```
kali@tankado.com ~ $ tcpflow –r evidence.pcap
kali@tankado.com ~ $ find 027.247.180.015*
192.168.0.100.54142-027.247.180.015.00021
192.168.0.100.51146 027.247.180.015.00021
192.168.0.100.53142 027.247.180.015.00021
192.168.0.100.54144 027.247.180.015.00021
192.168.0.100.56142 027.247.180.015.00021
192.168.0.100.54843 027.247.180.015.00021
192.168.0.100.59141 027.247.180.015.00021
192.168.0.100.50942 027.247.180.015.00021
. . .
```

Tablo 4 - Trafik Kayıt Dosyasının TCP Oturumlarının Ayrıştırılması

TCP oturumları ayrıştırılıp listelendiğinde olay yeri bilgisayarı ile ilgili porno sunucusu arasında birçok FTP bağlantısı gerçekleştiği görülmüştür. İlgili FTP bağlantısının ne amaçla kullanıldığı öğrenmek için hedef port olarak 21. Kullanan TCP oturumlarının içeriği ***xxd*** hex görüntüleyicisi ile incelendiğinde olay yeri bilgisayarının sunucuya resim ve görüntü dosyalarını yüklediği görülmüştür.

```
kali@tankado.com ~ $ xxd 192.168.0.100.50942 027.247.180.015.00021
0000   b8 27 eb 26 2f fd 50 e5 49 c5 49 0d 08 00 45 00  .'.&/.P.I.I...E.
0010   00 57 28 c5 40 00 80 06 4f c2 c0 a8 00 64 c0 a8  .W(.@...O....d..
0020   00 65 cd a7 00 15 48 7b 3e 6a bd df 0d 35 50 18  .e....H{>j...5P.
0030   3f d4 54 7f 00 00 53 54 4f 52 20 37 33 35 30 35  ?.T...STOR child
0040   34 5f 31 30 31 35 31 32 36 31 34 35 34 35 32 36  porn_gazi_test001
0050   32 32 35 5f 32 35 35 30 35 35 37 31 35 5f 6e 2e  _225_255055715_n.
0060   6a 70 67 0d 0a                                   jpg..
. . .
```

Tablo 5 - TCP Oturumunda FTP Analizinin Yapılması

Yukarıdan da görülebileceği gibi **192.168.0.100. 50942 027.247.180.015. 00021** isimli TCP oturum kaydı incelendiğinde olay yeri bilgisayarı tarafından STOR komutu ile FTP sunucusuna ***childporn_gazi_test001_225_255055715_n.jpg*** isimli resim dosyasının yüklediği görülmüştür.

3.3.4 SPAM Mail Gönderimi

Olay yeri bilgisyarının 027.247.180.015 IP adresli makinanın 22. Portu (SMTP) ile olan binlerce oturumu incelendiğinde 2 saatli süre içerisinde 5000'den fazla SMTP oturumu açıldığı görülmüştür.

```
kali@tankado.com ~ $ find 027.247.180.015.00022*
192.168.0.100.64142-027.247.180.015.00022
192.168.0.100.61146 027.247.180.015.00022
192.168.0.100.63142 027.247.180.015.00022
192.168.0.100.64144 027.247.180.015.00022
192.168.0.100.66142 027.247.180.015.00022
192.168.0.100.64843 027.247.180.015.00022
192.168.0.100.69141 027.247.180.015.00022
192.168.0.100.60942 027.247.180.015.00022
. . .
```

Tablo 6 - SMTP TCP Oturumlarının Tespiti

TCP oturumlarının içeriği incelendiğinde aynı içerikteki mesajın rasgele e-posta adreslerine gönderildiği tespit edilmiştir.

```
kali@tankado.com ~ $ xxd 192.168.0.100.10942 027.247.180.015.00022
0000   00 1f 33 d9 81 60 00 e0 1c 3c 17 c2 08 00 45 00  ..3..`...<....E.
0010   05 dc 25 4f 40 00 80 06 ed f0 0a 0a 01 04 4a 35  ..%O@.........J5
0020   8c 99 05 be 00 19 7e c4 54 47 ae ec 63 7e 50 10  ......~.TG..c~P.
0030   fe 31 d6 82 00 00 46 72 6f 6d 3a 20 22 47 75 72  .1....From: "Gur
0040   70 61 72 74 61 70 20 53 69 6e 67 68 22 20 3c 67  partap Singh" <g
0050   75 72 70 61 72 74 61 70 40 70 61 74 72 69 6f 74  urpartap@patriot
0060   73 2e 69 6e 3e 0d 0a 54 6f 3a 20 3c 72 61 6a 5f  s.in>..To: <raj_
0070   64 65 6f 6c 32 30 30 32 69 6e 40 79 61 68 6f 6f  deol2002in@yahoo
0080   2e 63 6f 2e 69 6e 3e 0d 0a 53 75 62 6a 65 63 74  .co.in>..Subject
01a0   65 52 31 4b 68 38 69 2b 68 55 79 56 6f 30 41 3d  : PORN FOR YOU!.
....
01a0   65 52 31 4b 68 38 69 2b 68 55 79 56 6f 30 41 3d  eR1Kh8i+hUyVo0A=
01b0   3d 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 61 6e 67 75  =..Content-Langu
01c0   61 67 65 3a 20 65 6e 2d 75 73 0d 0a 78 2d 63 72  age: en-us..x-cr
01d0   2d 68 61 73 68 65 64 70 75 7a 7a 6c 65 3a 20 53  -hashedpuzzle: S
...
0240   41 62 77 42 73 41 44 49 41 4d 41 41 77 41 44 49  CHILD PORN ADVER
0250   41 61 51 42 75 41 45 41 41 65 51 42 68 41 47 67  TISING FOR YOU !
0260   41 62 77 42 76 41 43 34 41 59 77 42 76 41 43 34  LETS CLICK ABOVE
...
```

Tablo 7 - Örnek SMTP Oturumun İçeriğinin Görüntülenmesi

Eposta mesajının *Subject* ve *Content* kısmından görülebileceği gibi olay yeri bilgisayarından çocuk pornosu konulu çok sayıda e-posta gönderimi yapılmıştır.

3.3.5 Port Taramasının Tespiti

Yasalarımıza göre bir bilgisayar sistemine port taraması yapılması suç olarak kabul edilmektedir. Bilindiği gibi port taraması bir sisteme saldırı yapmadan önceki en önemli hazırlık aşamasını oluşturmaktadır. Bu nedenle trafiği kaydedilen olay yeri bilgisayarının pcap dosyası üzerinde, bro [15]adlı paket analiz aracı ile aşağıdaki scan policy çalıştırılmıştır.

```
kali@tankado.com ~ $ bro -C -r evidence.pcap -b policy/misc/scan
kali@tankado.com ~ $ cat notice.log
#separator \x09
#set_separator      ,
#empty_field (empty)
#unset_field -
#path  notice
#open  2016-05-21-03-52-58
#fields      ts     uid    id.orig_h     id.orig_p     id.resp_h     id.resp_p
       fuid   file_mime_type      file_desc     proto  note   msg    sub    src
       dst    p      n      peer_descr    actions       suppress_for dropped
       remote_location.country_code     remote_location.region
       remote_location.city       remote_location.latitude
       remote_location.longitude
#types time   string addr   port   addr   port   string string string enum   enum
       string string addr   addr   port   count  string set[enum]     interval
       bool   string string string double double
1463696364.000000   CapYIY1uP2fDZhukad  192.168.0.10056969  85.17.141.85 21
       -      -      -      tcp    Weird::Activity     SYN_after_partial   -
       192.168.0.10085.17.141.85 21     -      bro    Notice::ACTION_LOG
       3600.000000  F      -      -      -      -      -
1463696626.000000   -      -      -      -      -      -      -      -      -
       Scan::Port_Scan     192.168.0.100 scanned at least 15 unique ports of
host 64.50.185.52 in 0m40s remote 192.168.0.10064.50.185.52 -      -      bro
       Notice::ACTION_LOG  3600.000000  F      -      -      -      -      -
#close 2016-05-21-03-53-41
```

Tablo 8 - Trafik Dosyasından Port Tarama Analizinin Yapılması

bro aracının oluşturduğu *notice.log* çıktısına göre **192.168.0.100** IP adresli olay yeri bilgisayarımız **2016-05-21-03-53-41** zamanında **64.50.185.52** IP adresli bilgisayara **40 saniye** süren ve **15 ayrı** portun yoklandığı bir tarama gerçekleştirilmiştir.

[15] The Bro Network Security Monitor - https://www.bro.org/

4. Sonuç

Bu çalışmada Tam Disk Şifrelemesine sahip bir olay yeri bilgisayarında adli incelemenin nasıl yapılabileceği hakkında bir literatür taraması yapılmış, yeni bir inceleme yöntemi olarak ağın koklanması tekniği uygulamalı olarak gösterilmiştir.

Özellikle TEMPEST (bilgi kaçağı) kavramı diğer bilişim güvenliği terimlerine nispeten daha az bilinen ancak uygun yöntemler kullanıldığında imkansız olabilecek bir adli incelemeyi mümkün kılabilme potansiyeline sahip bir teknolojiye işaret etmektedir. Diğer taraftan bu teknolojinin pratik hayatta kullanımına yönelik yazılım ve donanımlarının etkili bir ürün haline gelememesi bir dezavantajdır. Buradan hareketle bilgi kaçaklarını kullanan teknolojilerin geliştirilmesi konusuna ağırlık verilmesi gerekmektedir.

Oturumu kilitli ve tam disk şifrelemesine sahip bir bilgisayarın disk imajı üzerinde adli inceleme yapmanın imkansızlığı yanında ağ ve internet odaklı bir suça yönelik adli inceleme yapılırken, ağ trafiğinin dinlenerek kaydedilmesi ve bu kayıt üzerinden adli incelemenin gerçekleştirilmesi, atılı suçları kanıtlayacak nitelikte bilgiler elde etmek açısından kullanışlı olmakla beraber bu konuda meslek örgütlerinin ve standart kuruluşlarının birlikteliği sağlayacak usul ve esasları düzenlemesine ihtiyaç vardır.

Çalışmada olay yeri bilgisayarının ağ trafiği üzerinde pornografik resim varlık araştırması, pornografik resimlerin internet üzerinden dağıtılması, spam mail gönderimi ve port taraması suçlarının tespiti örneklendirilmiştir. Bu örnekler BOT NET'lerin komuta kontrol merkezini açığa çıkarmak, DDOS saldırısı yapan bilgisayarlar hakkında delil elde etmek ve bilişim sistemlerine karşı işlenebilecek olan diğer ağ temelli suçları ortaya çıkarmak ve delil elde etmek olarak çeşitlendirilebilir.

Yapılan çalışmada işe yarar ölçüde delillere ulaşmak için ağ trafiğinin yeterli süre kayıt altında alınması gerektiği anlaşılmıştır. Bu süre olay yeri inceleyicisinin atılı suçun türüne göre sezgisel olarak karar verebileceği bir süre olacaktır. Uzun süreler kayıt yapılması delil elde etme sürecinde olay yeri inceleyicisinin daha fazla veriye sahip olmasını sağlayacağı kesindir.

Olay yeri bilgisayarının ağ trafiğinin, olay yeri inceleyicisinin bilgisayarına yönlendirilerek kayıt altına alınması, elde edilecek delillerin güvenilirliği açısından tek taraflı bir doğruluk sunmaktadır. Şüpheli bu kayıtların doğruluğunu ve varlığını inkar edebilme hakkına sahiptir. Ancak bu konuda adli bilişim hassasiyetleri dikkate alınarak geliştirilebilecek ağ kayıt yazılım ve donanımları verilerin değiştirilmezliği konusunda güvence verebilecek nitelikte hazırlanabilir. Yine bu konu standart kuruluşlar ve meslek örgütlerinin ortaklaşa geliştirebileceği prosedürlere bağımlı konumdadır. Yapılan literatür araştırmasında kayıt ve inceleme aşamalarına kadar bu hassasiyetleri yerine getiren bir yazılım ya da çözüme rastlanılmamıştır.

MITM yöntemi kapsamında ARP Spoof Attack tekniği ile gerçekleştirilen ağ trafiğinin kaydedilmesi uygulamasında olay yeri bilgisayarının bu tekniğe karşı savunması olma ihtimali vardır. Olay yeri bilgisayarı statik ARP kayıtları bulunduruyor olabilir veya bir saldırı tespit yazılımı çalıştırıyor olabilir. Bu durumlarda olay yeri bilgisayarına karşı ARP Spoof Attack tekniğini uygulamak yerine ağ bağlantısı port mirroring veya network tapper gibi fiziksel bir ağ aygıtı ile kopyalanmaya çalışılmalıdır. Benzer şekilde hem yazılımsal hem de cihaz bazlı trafik kayıtlarında TLS/SSL gibi OSI'nin 4. Katmanını ilgilendiren güvenlik önlemlerine karşı anlamlı bir veri, dolayısıyla da delil elde edilememe ihtimali de vardır. Yine de FDE korumasına sahip bir olay yeri bilgisayarında ağın koklanması yöntemin uygulanması, adaletin ivedilikle gerçekleşmesi adına kolluk güçlerine çok önemli bir avantaj sağlamaktadır.

Kaynaklar

[i] **The Impact of Full Disk Encryption on Digital Forensics** - Eoghan Casey, Director of Training, Gerasimos J. Stellatos, Digital Forensic Examiner Stroz Friedberg, LLC 1150 Connecticut Ave, NW Washington, DC 20036 202-464-5800 {ecasey, gstellatos}@strozllc.com

[ii] **Extracting Disk Encryption Keys From Volatile Memory** - https://cryptome.org/0003/RAMisKey.pdf

[iii] **KEYSWEEPER** - http://samy.pl/keysweeper/

[iv] **DMA Attack Wikipedia** - https://en.wikipedia.org/wiki/DMA_attack

[v] **Memory Forensics over the IEEE 1394** - https://freddie.witherden.org/pages/ieee-1394-forensics.pdf

[vi] **Product Category Rules (PCR) for preparing an Environmental Product Declaration (EPD) for USB Flash Drive** - http://pcr-library.edf.org.tw/data/taiwan/EDF201103_EPD-PCR_Electronic_USB%20Flash%20Drive.pdf

[vii] **BadUSB: USB'den bağlanan cihazların hepsi bir tehdit kaynağı olabilir** - http://www.tankado.com/badusb-usbden-baglanan-cihazlarin-hepsi-bir-tehdit-kaynagi-olabilir/

[viii] **Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?** - http://ftp.cerias.purdue.edu/pub/doc/equipment/EMRSnooping.pdf

[ix] **Electromagnetic Eavesdropping Risks of Flat-Panel Displays -** http://www.cl.cam.ac.uk/~mgk25/pet2004-fpd.pdf

[x] **Adli Bilişim ve Elektronik Deliller – Seçkin Yayın Evi Ankara 2015**
Bölüm: Elektronik Verilerin Delillendirilmesi, Şükrü Durmaz, Sayfa:292/6.Bölüm

[xi] **Linux Yaz Kampında Bro ve Tshark ile Trafik Analizi** http://kogungor.com/index.php/2015/10/20/somenin-maceralari-bolum-i/