MEMORY FORENSICS

Yusuf BOLAT
112692048

İSTANBUL BİLGİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

Yrd. Doç. Dr. Leyla KESER BERBER

2015

MEMORY FORENSICS

HAFIZA ANALİZİ

Yusuf BOLAT
112692048

Yrd. Doç. Dr. Leyla KESER BERBER :

Yrd. Doç. Dr. Mehmet Bedii KAYA :

Öğr. Gör. İbrahim Halil SARUHAN :

Tezin Onaylandığı Tarih :

Toplam Sayfa Sayısı : 110

Anahtar Kelimeler (Türkçe)

1) Bellekte Adli Bilişim
2) Bellek İncelemesi
3) Bellek ve Adli Bilişim
4) Bellek ve parola
5) Bellek İmajı

Anahtar Kelimeler (İngilizce)

1) Memory Forensics
2) Memory Analysis
3) Memory and Computer Forensics
4) Memory and password
5) Memory Image

ÖZET

Bilişim denilince akla gelen ilk donanım bilgisayarlardır. Bilgisayarlarda işlenen ve depolanan veriler sabit veya geçici ortamlarda bulunmaktadır. Adli bilişim incelemeleri genellikle sabit ortamlarda bulunan veriler üzerinde yapılmakta ve geçici (uçucu) ortamlarda bulunan önemli veriler göz ardı edilmektedir. Oysa bellek incelemeleri ile işletim sistemi, sosyal medya ve e-posta parolalarına, ziyaret edilen internet site bilgilerine, çalıştırılmış uygulamalara, komut satırından girilen komutlar ve benzeri bilgilere erişmek mümkündür. Bu çalışmada; gerçekleştirilen uygulamalı örneklerin bir laboratuar ortamı yerine günlük hayatta kullanılan kişisel bilgisayarlar olması tercih edilmiş ve böylece bilgisayar belleği ile adli bilişim arasındaki ilişki ortaya çıkarılmaya çalışılmıştır.

Computers are the first hardware items when saying “informatics”. Datas which are processed and stored in computers present in fixed or temporary environments. Computer forensics investigations are generally conducted in fixed environments, and the important datas which are stored in temporary environments are ignored. However, it is possible to reach operating system informations, e-mail and social media passwords, internet site informations, commands etc. by means of memory investigations. Choosing personel computers as applied example instead of laboratory environmet, in this study the relationship between computer memory and computer forensics has been tried to be revealed.

İÇİNDEKİLER

KISALTMALAR

ABD	Amerika Birleşik Devletleri
AF	Anti Forensics
BEDO	Burst Extended Data Out
BİLGEM	Bilişim ve Bilgi Güvenliği İleri Teknolojileri Araştırma Merkezi
BIOS	Basic Input Output System
DC	Domain Controller
DDR	Double Data Rate
DIMM	Dual Inline Memory Module
DMA	Direct Memory Access
DRAM	Dynamic Random Access Memory
EDO	Extended Data Out
EDVAC	Electronic Discrete Variable Automatic Computer
EPROM	Erasable Programmable Read Only Memory
E.t.	Erişim Tarihi
f.	Fıkra
FPM	Fast Page Mode
GB	Giga Byte
IP	Internet Protocol
RAM	Read Only Memory
RAID	Redundant Array of Inexpensive Disks
RDRAM	Rambus Random Access Memory
SDRAM	Synchronous Dynamic Random Access Memory
SHA	Secure Hash Algorithm
SIMM	Single Inline Memory Module
sn.	Saniye
SPD	Serial Presence Detect
SRAM	Static Random Access Memory
MBR	Master Boot Record
MHz	Mega hertz
NIST	National Institute Of Standarts And Technology

NSA	National Securıty Agency
NVRAM	Non Volatile Random Access Memory
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
TCP/IP	Transmission Control Protocol/Internet Protocol
USB	Universal Serial Bus

KAYNAKÇA / ELEKTRONİK AĞ ADRESLERİ

Abbas-Maliky : Nidaa A. ABBAS / Sattar B. Sadkhan Al MALIKY, Multidisciplinary Perspectives in Cryptology and Information Security, sf.391,IGI Global,USA, 2014, https://books.google.com.tr/books?id=WgaXBQAAQBAJ,

Akhgar-Stanıforth-Bosco Babak AKHGAR / Andrew STANIFORTH / Francesca BOSCO, Cyber Crime and Cyber Terrorism Investigator's Handbook, sf.86, Elsevier Inc, USA, 2014, https://books.google.com.tr/books?id=GR2kAwAAQBAJ

Ashcroft : John ASHCROFT, Electronic Crime Scene İnvestigation: A Guide for First Responders, sf.52, Mart 2011 https://www.ncjrs.gov/pdffiles1/nij/187736.pdf

Başaranoğlu : Ertuğrul BAŞARANOĞLU / TÜBİTAK BİLGEM, Bellekten Parolaların Elde Edilmesi – 1 https://www.bilgiguvenligi.gov.tr/microsoft-guvenligi/bellekten-parolalarin-elde-edilmesi-1.html

Baykara-Daş-Karadoğan : Muhammet BAYKARA / Resul DAŞ / İsmail KARADOĞAN, 1. International Symposium on Digital Forensics and Security (ISDFS'13), 20-21 May 2013, Elazığ, Turkey Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi, sf.2, 20-21.05.2013 http://perweb.firat.edu.tr/personel/yayinlar/fua_721/721_80043.pdf

Berber : Leyla KESER BERBER, Adli Bilişim, CMK md. 134 ve Düşündürdükleri.. 10.07.2008 http://www.leylakeser.org/2008/07/adli-biliim-cmk-md-134-ve-dndrdkleri.html

Boileau : Adam BOILEAU, Hit by a Bus: Physical Access Attacks with Firewire, Computer Security Conference Presentation, Ruxcon 2006 http://www.security-assessment.com/files/presentations/ab_firewire_rux2k6-final.pdf

Brezinski : D. BREZINSKI, RFC3227:Guidelines for Evidence Collection and Archiving, Adavec Inc., Şubat 2002 https://www.ietf.org/rfc/rfc3227.txt

Canbek : Gürol CANBEK, Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Eylül 2005

Capehart : Barney CAPEHART, Information Technology for Energy Managers, sf.220, Fairmost Press Inc, USA, 2004 https://books.google.com.tr/books?isbn=0881734500

Carrier : Brain CARRIER, Digital Investigation Foundation, File System Forensic Analysis, sf.12-21, Pearson Education Inc, USA, 2005 http://sergiob.org/unam/DGSCA/forense/FileSystemAnalysis.pdf

Carvey : Harlan CARVEY, Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 8, 4.Edition, sf.11, Elsevier Inc, USA, 2014, https://books.google.com.tr/books?id=oiqSAgAAQBAJ

Carvey : Harlan CARVEY, Windows Forensics Analysis DVD Toolkit, Coauthor of Real Digital Forensics, sf.139, Syngress Publishing Inc, USA, 2014, http://160.216.223.99/vyuka/forensics/Windows%20Forensic%20Analysis%20DVD%20Toolkit%20%20Second%20Edition.pdf

Casey : Eoghan CASEY, Handbook of Digital Forensics and Investigation, sf.261-262, Elsevier Academic Press 2010, https://books.google.com.tr/books?isbn=0080921477

Çakır- Kılıç : Hüseyin ÇAKIR / Mehmet Serkan KILIÇ, Bilişim Suçlarına İlişkin Delil Elde Etme Yöntemlerine Genel Bir Bakış, Polis Bilimleri Dergisi, 15.03.2013, sf.14, http://www.pa.edu.tr/app_documents/D478B2AD-3813-4555-9629-6332F8CF8D33/cms_statik/_dergi/2013/3/4%20-%20D34%20Bili%C5%9Fim%20su%C3%A7lar%C4%B1%20veri%20elde%20etme.pdf

Çakır-Sert : Yrd.Doç.Dr. Hüseyin ÇAKIR, Ercan SERT; Uluslararası Terörizm ve Sınıraşan Suçlar Araştırma Merkezi (UTSAM) ve Gazi Üniversitesi, Endüstriyel Sanatlar Eğitim Fakültesi, Bilgisayar Eğitimi Bölümü tarafından hazırlanan "Bilişim Suçları ve Delillendirme Süreci" konulu makale, http://utsam.org/images/upload/attachment/utsas_2010_secilmis/Bili%C5%9Fim%20Su%C3%A7lar%C4%B1%20ve%20Delillendirme%20S%C3%BCreci.pdf

Ertürk : Ömer ERTÜRK, RAM İmajı Alınması ve Analizi İle Erişilebilecek Bilgiler 1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu Sunumu http://omererturk.wordpress.com

Garza : D. GARZA, Data Acquisition and Duplication, Computer Forensics Investigating Data & Image Files, sf.2-12, EC-Council, USA , 2010 https://books.google.com.tr/books?isbn=1435483510

Grant : Nicholas GRANT / Joseph SHAW, Unified Communications Forensics: Anatomy of Common UC Attacks, sf.127, Elsevier Inc, Boston, USA, 2014, https://books.google.com.tr/books?id=9lmatCF6L7YC

Halderman-Schoen-Heninger-Clarkson-Paul : J. Alex HALDERMAN / Seth D. SCHOEN / Nadia HENİNGER / William CLARKSON / William PAUL; Lest We Remember: Cold Boot Attacks on Encryption Keys, Princeton University, USENIX Security Symposium Paper, 21.02.2008, http://citpsite.s3-website-us-east-1.amazonaws.com/oldsite-htdocs/pub/coldboot.pdf

Harris : Ryan HARRIS, Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem, sf.44-49, Purdue University, Digital Forensics Research Conference Paper, 2006 http://www.dfrws.org/2006/proceedings/6-Harris.pdf

Henkoğlu : Türkay HENKOĞLU, Adli Bilişim (Dijital Delillerin Elde Edilmesi ve Analizi), sf.121, 2011, Ankara, Pusula Yayıncılık,

Huff : Howard R. HUFF, An Electronics Division Retrospective (1952-2002) and Future Opportunities in the Twenty-First Century, Journal of The Electrochemical Society, sf.50, 11.04.2002 http://jes.ecsdl.org/content/149/5/S35.full.pdf

İnternet : Adli Bilişim (Computer Forensic) http://edirnebarosu.org.tr/incelemeler/adli-bilisim-computer-forensic

İnternet : BitLocker'a yönelik 1394 DMA ve Thunderbolt DMA tehditlerini azaltmak için SBP-2 sürücüsünü ve Thunderbolt denetleyicilerini engelleme http://support.microsoft.com/kb/2516445

İnternet : CaptureGUARD Gateway -- Access to Locked Computers Http://www.windowsscope.com/index.php?page=shop.product_details&flypage=flypagetpl&product_id=30&manufacturer_id=0&option=com_virtuemart&Itemid=34&cid=10030

İnternet : Elcomsoft Forensic Disk Decryptor http://www.elcomsoft.com/efdd.html

İnternet : How to use and troubleshoot FireWire target disk mode http://support.apple.com/en-us/ht1661

İnternet : https://code.google.com/p/volatility/wiki/CommandReference21#cmdscan

İnternet : http://www.slideshare.net/cfbeek72/from-hybernation-file-to-malware-analysis-with-volatility

İnternet : Inception http://www.breaknenter.org/projects/inception

İnternet : Kayıt defteri nedir? http://windows.microsoft.com/tr-tr/windows-vista/what-is-the-registry

İnternet : Kayıt Defteri Düzenleyicisi nedir? http://windows.microsoft.com/tr-tr/windows/what-is-registry-editor#1TC=windows-7

İnternet : Microsoft Technet Kitaplığı - Komut kabuğuna genel bakış http://technet.microsoft.com/tr-tr/library/ cc737438%28v=ws.10%29.aspx

İnternet : MoonSols Windows Memory Toolkit http://www.moonsols.com/windows-memory-toolkit

İnternet : OS X Lion: Transfer files between two computers using target disk mode http://support.apple.com/kb/ph3838

İnternet : Physical memory attacks via Firewire/DMA - Part 1: Overview and Mitigation (Update) http://www.hermann-uwe.de/blog/physical-memory-attacks-via-firewire-dma-part-1-overview-and-mitigation

İnternet : Princetion University - Center For Information Technology Policy https://citp.princeton.edu/research/memory/media

İnternet : TrueCrypt Kullanılarak Şifrelenmiş Dosyaların Parolalarını Bulma http://blog.bga.com.tr/2012/03/truecrypt-kullanlarak-sifrelenmis.html

İnternet : VMware Workstation 5.5 What Files Make Up a Virtual Machine? https://www.vmware.com/support/ws55/doc/ws_learning_files_in_a_vm.html

İnternet : VMware vSphere 5.1 Documentation Center - ESXi and vCenter Server 5.1 Documentation - vSphere Virtual Machine Administration - Managing Virtual Machines - Using Snapshots To Manage Virtual Machines - Snapshot Files https://pubs.vmware.com/vsphere1/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-38F4D574-ADE7-4B80-AEAB-7EC502A379F4.html

İnternet	:	WindowsSCOPE Live Real-Time Cyber Investigation and Memory Forensics, 2011 BlueRISC Inc. http://www.windowsscope.com/index.php?option=com_docman&task=doc_download& gid=41&Itemid=
İnternet	:	Windows Kayıt Defteri'nde gezinti http://www.chip.com.tr/makale/kayit-defteri-gezisi-kayit-defteri-hiyerarsisi_2714_2.html
Karagülmez	:	Ali KARAGÜLMEZ, Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri, sf. 252-303, Seçkin Yayıncılık, Ankara, Ocak 2011 http://www.hukukmarket.com/images/contentspdf/137142.pdf
Karamanlı	:	Onur KARAMANLI, SAM Dosyası ve RAM'deki Bilgilerin Güvenliği https://www.bilgiguvenligi.gov.tr/donanim-guvenligi/sam-dosyasi-ve-ramdeki-bilgilerin-guvenligi-2.html
Ligh-Case-Levy-Walters	:	Michael Hale LIGH / Andrew CASE / Jamie LEVY / Aaron WALTERS, The Art Of Memory Forensics (Dececting Malware and Threads in Windows, Linux and Mac Memory), sf. 71, 471, 537-541, John Wiley & Sons, Inc., Indiana, USA, 2014 http://news.asis.io/sites/default/files/The%20Art%20of%20Memory%20Forensics.pdf
Malin-Casey-Aquilin	:	Cameron H. MALIN / Eoghan CASEY / James M. AQUILIN, A Malware Forensics: Investigating and Analyzing Malicious Code, sf.161-162, Elseiver Inc, USA, 2008, http://books.google.com.tr/books?id=lRjO8opcPzIC
Malin-Casey-Aquilina	:	Cameron H. MALIN / Eoghan CASEY / James M. AQUILIN, Linux Malware Incident Response : A Practitioner's Guide to Forensic Collection and Examination of Volatile Data : An Excerpt from Malware Forensic Field Guide for Linux Systems, sf. 9-16, Elseiver Inc, USA, 2013, https://books.google.com.tr/books?id=tjnFAwAAQBAJ
Malin-Casey-Aquilina	:	Cameron H. MALIN / Eoghan CASEY / James M. AQUILIN; Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides, sf.71-74, Elseiver Inc, USA, 2012, https://books.google.com.tr/books?id=3GFlrGkMDu4C
Marcella-Menendez	:	Albert MARCELLA / Doug MENENDEZ, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving..., sf.377, Taylor and Francis Group, USA, 2010, https://books.google.com.tr/books?id=nEqHuVht7HgC
Nozaki- Tipton	:	Harold F. TIPTON / Micki Krause NOZAKI, Information Security Management Handbook, Sixth Edition, 4. cilt, sf.426.427, Taylor and Francis Group, USA, 2010, https://books.google.com.tr/books?id=KUbaY0MMEvcC
Olczak	:	Anatole OLCZAK, The Korn Shell: Unix and Linux Programming Manual, Volume 1, sf.333, Pearson Education Limited, UK, 2001 http://books.google.com.tr/books?id=dCIJv94vXUMC
Ozbek	:	Murat OZBEK, I. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu (ISDFS'13), "Adli Bilişim Uygulamalarında Orijinal Delil Üzerindeki Hash Sorunları" konulu sunum, 20-21 Mayıs 2013, Elazığ, Türkiye, sf.6, http://www.bilgisayardedektifi.com/wp-content/uploads/2013/06/MuratOZBEK_Adli_Bilisimde_Orijinal_Delil_Uzerindeki_hash_Sorunlari_isdfs_bildiri.pdf

Özer-Başaranoğlu	:	Onur Samet ÖZER / Ertuğrul BAŞARANOĞLU, Windows İşletim Sisteminde Oturum Açma İşlemi – Winlogon, 26.11.2012 http://www.bilgiguvenligi.gov.tr/microsoft-guvenligi/windows-isletim-sisteminde-oturum-acma-islemi-winlogon.html
Öztürkci	:	Halil ÖZTÜRKCİ, Adli Bilişim İncelemelerinde Linux Memory Forensics – 1, http://halilozturkci.com/adli-bilisim-linux-memory-forensics-1
Öztürkci	:	Halil ÖZTÜRKCİ, Adli Bilişim İncelemelerinde Hibernation Dosyası Üzerinden Hafıza Analizi http://halilozturkci.com/adli-bilisim-incelemelerinde-hibernation-dosyasi-uzerinden-hafiza-analizi/
Öztürkci	:	Halil ÖZTÜRKCİ, Hafıza İmajından Network Paketlerini Elde Etme http://halilozturkci.com/hafiza-imajindan-network-paketlerini-elde-etme/
Öztürkci	:	Halil ÖZTÜRKCİ, Adli Bilişim İncelemelerinde Sanal Makinaların Hafıza Dosyalarının Kullanımı http://halilozturkci.com/adli-bilisim-incelemelerinde-sanal-makinalarin-hafiza-dosyalarinin-kullanimi
Öztürkci	:	Halil ÖZTÜRKCİ, Adli Bilişim İncelemelerinde Sabit Disk İmajları – Giriş http://pentesttools.net/adli-bilisim-araclari/96-adli-bilisim-incelemelerinde-sabit-disk-imajlari-giris
Öztürkçi	:	Halil ÖZTÜRKÇİ, FTK Imager İle Disk İmajı Alma http://halilozturkci.com/adli-bilisim-ftk-imager-ile-disk-imaji-alma/
Panek- Chellis	:	William PANEK / James CHELLİS, MCTS Windows Server 2008 Active Directory Configuration Study Guide: Exam 70-640, sf.44-46, Wiley Publishing Inc, Canada, https://books.google.com.tr/books?id=EsQRcBk5QM4C
Poşul	:	Abdulkadir POŞUL / TÜBİTAK BİLGEM, Pano (Clipboard), 10.05.2013 https://www.bilgiguvenligi.gov.tr/veri-gizliligi/pano-clipboard.html
Riley-Johansson	:	Jesper M. JOHANSSON / Steve RILEY, Protect Your Windows Network: From Perimeter to Data, sf.332. Pearson Education Inc, USA, 2005, https://books.google.com.tr/books?id=yZX2uAoAagwC, E.t. 02.10.2014
Russinovich	:	Mark RUSSINOVICH, Microsoft Technet Kitaplığı, ProcDump v7.01 http://technet.microsoft.com/en-us/sysinternals/dd996900.aspx
Saygı-Yeşil	:	Zülfükar SAYGI / Sezen YEŞİL, Telekomünikasyon Kurumu ile ODTÜ-Uygulamalı Matematik Enstitüsü Kriptografi Bölümü tarafından yürütülmüş olan "Açık Anahtar Altyapısı Konusunda Araştırma, Geliştirme ve Uygulamalar" proje makalesi, sf.3 http://www.ueimzas.gazi.edu.tr/pdf/bildiri/24.pdf
Shinder	:	Debra Littlejohn SHINDER, Scene of the Cybercrime: Computer Forensics Handbook, sf.380, Syngress Publishing, USA, 2002 https://books.google.com.tr/books?id=BLjomivi1asC
Stevens-Casey	:	Richard M. STEVENS / Eoghan CASEY, Digital İnvestigation 7 (2010) Extracting Windows command line details from physical memory, sf.57-63, Digital Forensics Research Conference Paper 2010, http://dfrws.org/2010/proceedings/2010-307.pdf

Şirikçi-Cantürk : Ahmet Serhat ŞİRİKÇİ / Nergis CANTÜRK, Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi, Bilişim Teknolojileri Dergisi, Cilt: 5, Sayı: 3, Eylül 2012 http://www.btd.gazi.edu.tr/article/viewFile/1041000152/pdf

Tilborg-Jajodia : Henk C.A. van TILBORG / Sushil JAJODIA, Encyclopedia of Cryptography and Security, sf.216, Spinger Science Business Media, London, UK, 2011 https://books.google.com.tr/books?id=UuNKmgv70lMC

Trivedi : Nisarg TRIVEDI, Study on Pagefile.sys in Windows System, Paper sf.5 Forensic Sciences University, Gujarat, India, Mart 2014 Http://www.iosrjournals.org/iosr-jce/papers/Vol16-issue2/Version-5/C016251116.pdf

Völzow- Kuhlee : Victor VÖLZOW / Lorenz KUHLEE, Computer-Forensik Hacks, sf.9, O'reilly Verlag, Germany, 2012, https://books.google.com.tr/books?id=bQblShv0v2EC

Türkiye Bilişim Derneği : Türkiye Bilişim Derneği Kamu Bilişim Platformu, IX Bilişim Teknolojilerinin Kullanılmasının Hukuksal Boyutu, Mayıs 2007 http://www.tbd.org.tr/usr_img/cd/kamubib14/raporlarPDF/RP2-2007.pdf

Valenzuela : Ismael VALENZUELA, Mac OS Forensics How-To: Simple RAM Acquisition and Analysis with Mac Memory Reader (Part 1) 28 Haziran 2011 http://digital-forensics.sans.org/blog/2011/01/28/mac-os-forensics-howto-simple-ram-acquisition-analysis-mac-memory-reader-part-1

Weidman : Georgia WEIDMAN, Penetration Testing: A Hands-On Introduction to Hacking, sf.213-214, No Starch Press Inc, USA, 2014, https://books.google.com.tr/books?id=4b1S0U1fIVAC

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

Memory Forensics

§ 1. Giriş

20 ve 21'nci yüzyılda bilgisayar ve bilişim teknolojilerinin gelişimi ile modern hayatta hızlı ve önemli gelişmeler olmuştur. Bu teknolojilere günlük hayatın hemen her yerinde, kimi zaman evlerde, kimi zaman kamu ve özel sektörde, kimi zaman ulaşım, enerji, iletişim, sağlık hizmetleri gibi alanlarda kullanılan kritik sistemlerin altyapılarında ve benzeri birçok alanda rastlanılmaktadır. Bilişim sistemlerinin bu denli geniş bir kullanım alanının olması bu sistemlere kötü niyetli kişilerinde ilgisini artırmış ve yeni bir suç işleme alanı oluşturmuştur. Adli ve idari makamlar tarafından bu alanda işlenen suçlarla mücadele edilmekte ve adli bilişim başlığı altında incelemeler yapılmaktadır.

Adli bilişim; suçun aydınlatılabilmesi için bilimsel metotlar kullanılarak, çeşitli varyasyonlardaki dijital medyalar üzerinde bulunan, suçla ilgili dijital delillerin bozulmadan ve zarar görmeden anlaşılabilir bir şekilde adli makamlar önüne sunulmaya hazır hale getirilmesini sağlayan ve başlı başına bilimsel teknik prensiplerin uygulandığı bir delil inceleme sürecinin bütünüdür.[1] Adli Bilişim biliminin inceleme alanında olan dijital delillere;

- Bilgisayarlar,
- Hard diskler, CD, DVD ve Disketler,
- USB Hardisk ve USB Flash Disklerde vs.
- ZIP, DAT, DLT gibi teyp veri yedekleme birimlerinde,
- Hafıza Kartları,
- Dijital Kameralar ve Fotoğraf Makineleri, Medya Çalarlar,
- Cep Telefonları ve Akıllı Telefonlar,
- Bazı Yazıcı, Tarayıcı, Fotokopi ve Fax Cihazları,
- Network Cihazları,

[1] Ahmet Hakan EKİZER, Adli Bilişim (Computer Forensics), http://www.ekizer.net/adli-bilisim-computer-forensics, E.t. 02.08.2014

örnek verilebilir.

Adli bilişim çalışmaları çeşitli sınıflandırılmalara tabi tutulmuş olsa da basit anlamda 4 aşamadan oluşmaktadır.[2] Bu aşamalar;

- Delil toplama (collection),
- Delillerin incelenmesi (examination),
- Sonuçların değerlendirilmesi (analysis),
- Raporlama (reporting)'dır.

Bilişim denilince akla ilk gelen donanım bilgisayardır. Bilgisayarlar, adli bilişim açısından hem içerisinden delil elde edilen hem de delil elde etme sürecinde kullanılan bir araçtır.[3]

Fiziksel bir bilgisayar üzerinde bulunabilecek deliller, sabit disk denilen depolama ünitesinde veya çalışır konumda bulunan bilgisayarın belleğinde (RAM) bulunabilir. Sabit disklerin yapıları gereği üzerinde bulunan veriler kalıcı iken bellekte bulunan veriler uçucudur. Bu nedenle sabit disk incelemeleri bellek incelemelerine oranla nispeten daha kolaydır. Ayrıca adli bilişim incelemeleri de genellikle sabit diskler üzerinde gerçekleştirilmektedir. Oysa bellek incelemesi ile elde edilebilecek oldukça önemli veriler bulunmaktadır. Açık durumda olan bilgisayarın belleğinden; işletim sistemine ait parola, sosyal medya ve e-posta hesaplarına ait parolalar, ziyaret edilen internet siteleri, çalıştırılan uygulamalar, komut satırından girilen komutlar gibi bilgilere erişilebilir. Ancak bu bilgilerden bazılarına sabit disk incelemesi ile ulaşmak mümkün değildir.

Türk Hukukunda Adli Bilişime ilişkin olan hükümler incelendiğinde;

---

[2] Ali KARAGÜLMEZ, Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri, sf. 252, Seçkin Yayıncılık, Ankara, Ocak 2011, http://www.hukukmarket.com/images/contentspdf/137142.pdf, E.t. 04.08.2014

[3] Adli Bilişim (Computer Forensic), http://edirnebarosu.org.tr/incelemeler/adli-bilisim-computer-forensic/ E.t. 04.08.2014

- Ceza Muhakemesi Kanunu'nun (CMK) 134'ncü maddesi,
- Adli ve Önleme Aramaları Yönetmeliği'nin 17'nci maddesi,
- Suç Eşyası Yönetmeliği'nin 9'uncu maddesi

ile düzenlendiği görülmektedir.[4]

CMK 134'ncü maddesinin 1'nci bendi gereğince; adli bir konuda şüpheliye ait materyalde arama yapılabilmesi için hakim tarafından verilmiş mahkeme kararı olması gerekmektedir. Mahkeme kararı olmadan şüphelinin kullandığı dijital materyalde inceleme yapılması mümkün değildir.

2'nci bendinde ise; mahkeme kararı ile incelenecek materyallere ancak varsa şifrelerin çözülememesi veya gizlenmiş bilgilere ulaşılamaması durumunda el konulabileceği ayrıca şifrelerin çözülmesi ve gerekli kopyaların alınması durumunda, el konulan cihazların vakit geçirilmeden iade edilmesi hükmü bulunmaktadır.

Bu bağlamda; vakit geçirilmeden el konulan cihazların iade edilebilmesi adına, adli inceleme yapan kişi ya da kurumların bellek incelemesi ile sistemlere ait parolaların elde edilebileceği düşünüldüğünde, bellek incelemesinin adli bilişim incelemelerinde bir standart haline getirilmesi gerekmektedir.

Bu çalışmada; kısaca belleğin tanımı ve çeşitleri hakkında bilgiler verilmiş, bellek incelemesi ile erişebilecek bilgilere, uygulamalı örnekler ile nasıl ulaşılabileceği gösterilmiştir. Böylece bellek ile adli bilişim arasında ilişki ortaya çıkarılmaya çalışılmıştır. Örneklemelerin oluşturulduğu ve incelemelerin yapıldığı bilgisayarların günlük hayatta kullanılan kişisel bilgisayarlar olması tercih edilmiştir. Böylece çalışmanın bir laboratuar ortamında gerçekleştirilmesi yerine günlük hayatta yaşanabilecek senaryolar çerçevesinde oluşturulması hedeflenmiştir. Kullanılan yazılımların çoğunlukla ücretsiz ve açık kaynaklı

[4] Leyla Keser BERBER, Adli Bilişim, CMK md. 134 ve Düşündürdükleri..., 10 Temmuz 2008, http://www.leylakeser.org/2008/07/adli-biliim-cmk-md-134-ve-dndrdkleri.html, E.t. 04.06.2014

olması tercih edilmiş, ancak bazı bölümlerde ücretli yazılımların demo sürümleri de kullanılmıştır.

§ 2. Bellek nedir?

Bilgisayarlar temelde 3 ana bileşenden oluşmaktadır. Bunlar; merkezi işlem birimi (işlemci), bellek (RAM), giriş/çıkış aygıtları (klavye, mouse, sabit disk, yazıcı vb.) ‘dır.

İşlemcinin çalıştırdığı programlar ve programlara ait bilgiler bellek üzerinde saklanmaktadır. Bellek geçici bir depolama alanıdır. Bellek üzerindeki bilgiler güç kesildiği anda kaybolmaktadır. Bu nedenle bilgisayarlarda verileri daha uzun süreli ve kalıcı olarak saklamak için farklı birimler mevcuttur.

Uzun süreli saklanan veriler;

- Sabit Diskler,
- CD/DVD’ler,
- Disketler,
- Manyetik Veri Depolama Birimleri (Yedekleme Kasetleri) üzerinde,
- BIOS'un saklandığı EPROM'lar,
- ...

Kısa süreli saklanan veriler ise;

- Sistem bellekleri,
- İşlemcilerin içindeki “Cache” diye tabir edilen bellekler,
- Grafik kartlarının üzerindeki bellekler,
- ...

üzerinde depolanmaktadır.

Bellek kavramının bilişim sistemlerinde bu derece geniş bir donanım yelpazesi olmasına rağmen, hemen her bilgisayar, tablet, akıllı telefon v.b

kullanıcısı için bellek denilince akla ilk gelen kavram sistem RAM'i olmaktadır. RAM ise Random Access Memory kelimelerinin baş harflerinin kısaltılmasıdır. RAM Türkçe'ye çevrildiğinde "Rastgele Erişilebilir Bellek" anlamına gelmektedir. Random kelimesi rastgele anlamından çok bilgiye erişimin doğrudan gerçekleştiğini özetlemekte ve verilere manyetik teyplerdeki ya da DVD-ROM'lardaki sıralı erişimin aksine, sırasız yani doğrudan ve hızlı bir şekilde erişim imkanı vermesidir. Kısaca RAM'in organize ve kontrol ediliş biçimi, verinin doğru olarak belirli depolama bölgelerinden okunması ve yazılmasını sağlar. Erişimde sağladıkları hız, RAM'lerin sistemde bu denli önemli ve performansı belirleyici olmalarında en önde gelen etkendir.

RAM bellekler kısa süreli veri saklama imkânı sağlamaktadır. Enerjilerinin kesilmesi durumunda üzerinde bulunan veriler kaybolmaktadır. Uzun süreli veri depolayabilen donanımlar ise enerji kaynağına ihtiyaç duymazlar. Bu tür veri depolama birimlerine ise ROM bellek denilmektedir. ROM bellek; Read Only Memory kelimelerinin baş harflerinin kısaltılmış halidir. ROM bellekler sadece okunabilen devrelerden oluşur. İsminden de anlaşıldığı üzere ROM belleklerin üzerinde bulunan verinin son kullanıcılar tarafından değiştirilmemesi beklenmektedir.

ROM bellek denildiğinde akla ilk gelen bilgisayarın yazılımlarını ve donanımlarını hazır hale getiren BIOS'dur. Basic Input Output System (Temel Giriş Çıkış Sistemi)'nin kısaltması olan BIOS; işlemci, bellek, yonga seti, video adaptörü, disk denetleyicileri, disk sürücüleri, klavye, fare gibi bileşenlerinin testini gerçekleştirir. BIOS'un temel işlevi; bilgisayarı diğer donanım ve yazılımların çalışmasına hazır hale getirmek, işletim sistemini yüklemek ve başlatmaktır. Bilgisayar başlatıldığında BIOS'un ilk işi RAM'i okumak ve klavye, fare, sabit disk, CD/DVD sürücüsü gibi sistem aygıtlarını tanımlamak ve

kullanıma hazırlamaktır. BIOS, işletim sistemleri ile donanımlar arasındaki sürücüler toplamını içeren bir arabirim yazılımıdır.[5]

I. Belleklerin tarihçesi

İlk bellek sistemleri vakum tüplerinden oluşturulmuştu, ancak kullanımında başarılı sonuçlar alınamamıştır. Belleğin bilinen tarihi 1800'lü yıllara kadar uzanmaktadır. Belleklerin tarihi gelişimi ile ilgili olarak kısaca;

1834 yılında Charles BABBAGE şahsına ait analitik motorda salt okunur bellek kullanmıştır.

1939 yılında Helmut SCHREYER neon lambalar kullanarak prototip bellek icat etmiştir.

1950 yılında sadece sekiz adet satılan ilk ticari bilgisayar sadece 256 (40-bit) kelime ana bellek kapasitesine sahipti.[6]

1952 yılında imal edilen ilk bilgisayarlardan olan EDVAC, ikilik tabanda otomatik toplama, çıkarma, çarpma, programlanmış bölme işlemi ve bu işlemlerin otomatik olarak sağlamasını yaparken sadece 1,000 adet 44-bit kelimelik belleğe (Daha sonra belleği 1024 kelimeye yani 5,5 kilobayta çıkarılmıştır.) sahip bir cihazdı.[7]

1949-1952 yılları arasında yazılabilir bellekler geliştirildi ve manyetik çekirdek bellek olarak birçok bilgisayarda kullanıldı.

---

[5] İnternet, ''Vikipedi Özgür Ansiklopedisi'', 2014, http://tr.wikipedia.org/wiki/BIOS, E.t. 04.06.2014

[6] Mary BELLİS; History of Computer Memory, http://inventors.about.com/od/rstartinventions/a/Ram.htm, E.t. 19.08.2014

[7] İnternet, ''Vikipedi Özgür Ansiklopedisi'', 2014, http://tr.wikipedia.org/wiki/EDVAC, E.t. 19.08.2014

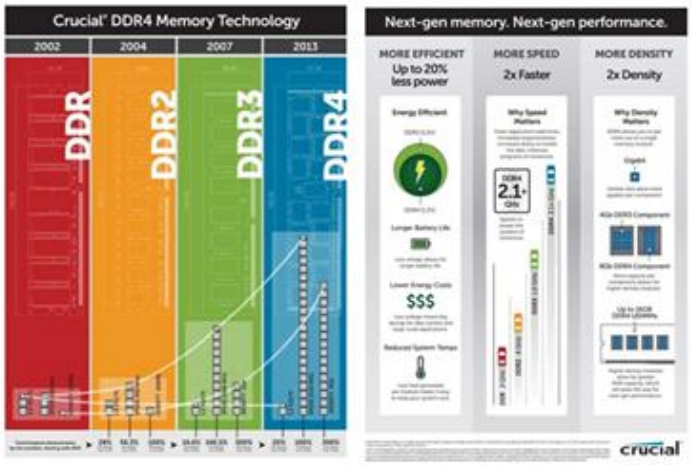
1960 ve 1970'li yıllarda statik ve dinamik devrelerin geliştirilmesi ile birlikte;[8]

1968 yılında Dr. Robert H. DENNARD tarafından ilk defa tek transistör hücreli DRAM için patent (patent nu: US3811076 A) alınmıştır.[9]

1970 yılında 256 K kapasiteli SRAM yongasını Fairchild CORPORATION tarafından icat edilmiştir.[10]

1990'lı yıllarda teknolojik gelişmelerin hızla artması ile birlikte EDO RAM, SD-RAM, RD-RAM, DDR RAM, DDR2 RAM, DDR3 RAM gibi bellekler kullanıldı. Günümüzde bu RAM çeşitlerinden çoğunlukla DDR RAM'lerin kullanıldığı ve diğer RAM çeşitlerinin ise tarihe karıştığı görülmektedir.

Aşağıdaki grafikte DDR RAM'lerin zaman içinde hız, kapasite ve kullandıkları enerji miktarlarında meydana gelen değişiklikler gösterilmektedir.[11]



Şekil 1 - DDR RAM'lerin hız, kapasite ve enerji miktarları

[8] http://tr.wikipedia.org/wiki/RAM, E.t. 19.08.2014

[9] Howard R. HUFF, An Electronics Division Retrospective (1952-2002) and Future Opportunities in the Twenty-First Century, Journal of The Electrochemical Society, sf.50, 11.04.2002 http://jes.ecsdl.org/content/149/5/S35.full.pdf, E.t. 19.09.2014

[10] Mary BELLİS; History of Computer Memory, http://inventors.about.com/od/rstartinventions/a/Ram.htm, E.t. 19.08.2014

[11] Crucial® DDR4 Memory Technology, http://www.crucial.com/usa/en/memory-ddr4-info, E.t. 20.08.2014

Bu grafikten çıkarılabilecek sonuç; zaman içinde az enerji ile daha hızlı ve yüksek kapasitelere ulaşıldığı görülmektedir. Bu gelişmeler teknoloji kullanıcılarına zaman, kapasite ve yeşil enerji olarak geri dönmektedir.

II. Bellek çeşitleri

Bellek çeşitlerini; RAM'den veri okumak ya da RAM'e veri yazmak için kullanılan protokoller belirlemektedir. Genel anlamda belleklerin DRAM ve SRAM olmak üzere iki ana çeşidi vardır. Günümüzde en popüler RAM türü olan DDR bellektir. Buradaki DDR (Double Data Rate) kısaltması, çift veri hızlı bellekler anlamında kullanılmaktadır. Bir önceki nesil bellek türlerine isim veren SDR (Single Data Rate) kısaltması ise tek veri hızlı RAM'leri simgelemektedir. DDR ve SDR bellekler senkron olarak çalışmaktadır. Yani veri akışı bir saat işaretiyle düzende tutulmaktadır.

A. Dynamic Random Access Memory (DRAM)

DRAM daha çok kişisel bilgisayarlarda kullanılan hafıza türüdür. Bu teknolojide transistör ve kondanstörler birlikte kullanılmaktadır. Veriler kondansatörlerde tutulmakta, okuma ve yazma işlemleri için de transistörler kullanılmaktadır. Kondansatörler yapıları gereği çok hızlı enerji harcamaktadır. Bu nedenle üzerlerinde bulunan verileri koruyabilmek için enerjisinin sürekli yenilenmesi gerekmektedir. Dinamik ifadesi buradan gelmektedir. Bu durum DRAM‘ler için bir avantaj gibi gözükmekle beraber sürekli yenileme ihtiyacı sebebiyle de bir dezavantajtır. Sürekli yenileme ihtiyacı DRAM’lerin SRAM’lerden daha yavaş çalışmasına neden olmaktadır.

DRAM’lerin yapıları oldukça basittir. Her 1 bitlik veriyi saklamak için 1 kondansatör ve 1 transistör kullanılmaktadır. Bu nedenle diğer RAM çeşitlerine göre daha ekonomiktir.

Fast Page Mode (FPM) DRAM - Hızlı Sayfalama Modlu RAM);

Geçmişte birçok bilgisayar FPM DRAM kullanılmaktaydı. FPM DRAM'ler günümüzde kullanılan sistemlerin hızına ayak uyduramayacak kadar çok yavaştı. Bellek kontrolcüsü; bellek içerisinde bir veriye ulaşmak istiyorsa o verinin adresini tam olarak bilmesi gereklidir. Normal RAM'lerde adres her işlem sonrası yeniden istenir. FPM'de ise veri bir defa istendikten sonra verinin tam adresi hafızada tutularak ve sonraki kullanımlarda tekrar adres bilgisini tespit etmeye gerek kalmadan direk verinin kullanımı sağlamaktadır. 33 MHz'ten daha hızlı çalışan işlemcilerde veriler çok hızlı istendiği için FPM'ler düzgün çalışamamaktaydı. Bu nedenle yerlerini EDO DRAM'lere bırakmıştır.

Şekil 2 - Fast Page Mode (FPM) DRAM

Extended Data Out (EDO) Genişletilmiş Veri Çıkışlı RAM);

EDO RAM'ler; FPM DRAM'lerin performansının % 30 arttırılmış ve 33 MHz'ten yüksek hızlarda çalışamama açığını kapatmak amacıyla geliştirilmiştir. Ayrıca FPM DRAM'lere göre bir avantajı da işlem yapma esnasında önce başlatılan komut ya da istek tamamlanmadan sonraki işlemi başlatabilmesidir. SRAM'lerin gelişimine kadar en çok kullanılan RAM çeşididir. EDO RAM'lerde 66MHz'ten daha hızlı çalışamamaktadır. FPM destekleyen bir sistemde EDO bellek kullanılmakta ancak performansta bir artış sağlanamamaktadır.

EDO RAM'ler 1990'lı yıllarda video kartlarında sıklıkla kullanılmıştır. Düşük maliyetine rağmen yüksek maliyetli Video RAM'lere yakın performans göstermiştir.

Şekil 3 - Extended Data Out (EDO) RAM

Burst Extended Data Out (BEDO) (Genişletilmiş Veri Çıkışlı RAM);

EDO RAM'lerin geliştirilmiş versiyonudur. EDO RAM'lere göre daha fazla ve hızlı veri gönderebilme özelliğine sahiptir. 66 MHz hızında çalışmakta ancak üstündeki hızları desteklememektedir.

Rambus RAM (RDRAM);

İsmini üreticisi olan Rambus şirketinden almıştır. 800 Mhz hızında çalışabilmektir. Paralel çalışan kanallar ile yüksek çalışma hızına sahiptir. RDRAM'lerin diğer RAM'lerden farkı ve onu üstün kılan özelliği en yakın özelliklere sahip belleklerden bile en az iki katı hızda çalışıyor olmalarıydı.

Yüksel performansla çalışmasına rağmen pek yaygınlaşmamasının sebebi fiyatının yüksek olmasıdır.

Şekil 4 - Rambus RAM (RDRAM)

Synchronous Dynamic RAM (SDRAM)- Senkronize Dinamik RAM);

SDRAM'ler EDO RAM'lerden sonra geliştirilmiş ve DDR-SDRAM olarak kullanılan DRAM türüdür. İlk kez Pentium II işlemcili bilgisayarlarda kullanılmıştır. SDRAM'ler 100 MHz sistem hızı ile uyumlu olarak çalışabilmekteydi.

Asenkron ara yüzde, işlemci bellekten bilgi alabilmek için beklemek zorundadır. Senkron çalışması ile bilgi alış verişi sistem hızıyla uyumlu bir şekilde yapılmaya başlandığından işlemcinin boşuna bekleme sorunu ortadan kaldırılmış ve veriye erişim hızının çok daha yüksek olması sağlanmıştır.

Gelişen anakart teknolojilerine paralel olarak PC100 (100 MHz hızında) ve PC133 (133 MHz hızında) standartlarında SDRAM'ler ile geliştirilmiştir.

Double Data Rate (DDR) SDRAM (Çift Veri Oranlamalı SDRAM);

DDR-RAM'ler SDRAM'lerin gelişmiş halidir. Birçok yerde DDR-RAM'ler DDR SDRAM olarak geçmektedir. Yüksek performans ve veri iletişimi isteyen; 3D, Video ve internet uygulamaları için geliştirilmiştir. Bütün bu uygulamalar için gerekli performans ve hız için gerekli bant genişliğine sahiptir. DDR ismini almasının sebebi SDRAM'lerdeki gibi saat frekansının sadece yükselen kısmında değil saat frekansının hem yükselen hem alçalan kısmında veri transfer edebilmesidir. SDRAM'lara oranla yaklaşık iki kat bant genişliğine sahiptir. Böylece performansta da yaklaşık iki kat artış sağlamaktadır.

SDRAM'lerin 100 ve 133 MHz olan hızları DDR-RAM'lerde 266, 333 ve 400 MHz'lere yükseltilmiş ve veri yolu genişliği ikiye katlanmıştır. DDRRAM'lerde 184 pin ayak iğne sayısı sahiptir. Ayrıca sistemden 2.5 Volt'luk enerji çekimi söz konusudur.

Şekil 5 - Double Data Rate (DDR) SDRAM

DDR2 RAM;

Bu DDR-RAM'lerin ikinci nesil ürünüdür. DDR-RAM'lerden biraz daha farklı bir sinyal yapısına ve daha az elektrik tüketimi yapacak şekilde geliştirilmiştir. Sinyal yapısının farklı olması sebebiyle ana kart ile olan bağlantı sayısında artış söz konusudur. DDR-RAM'lerde 184 pin olan ayak sayısı 240 pine yükselmiş ve 2.5 Volt'luk enerji ihtiyacı da 1.8 Volt'a düşürülmüştür. Voltajda meydana gelen düşüş belleklerin ısınma sorununu ortadan çözmekte ve çalışma performansını olumlu yönde doğrudan etkilemektedir.

Şekil 6 - DDR2 RAM

DDR3 SDRAM;

DDR3-RAM’lerin bir önceki nesil olan DDR2-RAM’lerden farkı, band genişliğinin yüksek olması, daha az elektrik enerjisine ihtiyaç duyması ve işlem tampon bölgesinin ikiye katlanması sonucu daha hızlı reaksiyon süresine sahip olmasıdır.

DDR-RAM’lerin 2,5 Volt ve DDR2-RAM'lerin 1,8 Volt'luk enerji ihtiyacına karşın DDR3-RAM’ler 1,5Volt’luk enerji gereksinimiyle çalışmakta ve DDR2'lere oranla %30 daha az güç harcamaktadır. DDR3-RAM ve DDR2-RAM’lerin 240 pin olan ayak sayısı ve boyutlarının aynı olmasına rağmen enerjisi kullanımı nedeniyle birbirlerinden farklıdırlar. Ayrıca çentikleri de farklı yerdedir. DDR3-RAM’ler 1.5Volt ile çalışıyor olması sebebiyle daha az ısınmaktadır. Daha az voltaj sarfiyatı ile enerji ihtiyacı düşürülmüş ve böylece kullanıldığı dizüstü/mobil bilgisayar sistemlerinin pil ömrünü uzatmıştır.

Şekil 7 - DDR3 RAM

B. Static Random Access Memory (SRAM)

Bu tip RAM'lerde veriler yüklendikten sonra sabit kalmaktadır. Bu nedenle enerjisini sürekli yenilenmesi gerekmemektedir. SRAM’ler; DRAM'den daha hızlı ve daha güvenilirdir ancak DRAM’ler kadar yaygın değildir. SRAM'lerin üretim maliyetleri DRAM'lere oranla çok daha yüksektir. Önbellek olarak kullanılan L1, L2 ve L3 cacheler de SRAM teknolojisi kullanılmaktadır.

SRAM’de her 1 bitlik veri 4 transistörde toplanmaktadır. 2 tane ek transistör okuma ve yazma işlemleri boyunca 4 transistöre yardımcı olmaktadır. Yani bellekte 1 bitlik veri depolamak için 6 transistör kullanılır. Bu nedenle SRAM teknolojisi pahalı bir teknoloji olmakla beraber DRAM’lere göre çok daha hızlı çalışmaktadır.

C. Diğer bellek çeşitleri

EPROM (Erasable Programmable Read Only Memory); Bu tip belleklerde elektrik kesintisinde bilgi kaybolmamaktadır. EPROM'ların içinde bulunan veriler temizlenerek yeniden programlanabilir ancak sadece okunabilir şekilde çalışmaktadır. Dinamik bir yazma işlemi gerçekleştirilememektedir. Bilgisayarlar anakartlarına ait BIOS (Basic Input Output System) sistemlerinde kullanılmaktadır. (BIOS bilgisayarların açılması ve gerekli donanımları anakartın tanıması için kullanılan küçük yazılımdır.) EPROM'lar üzerinde bulunan verileri uzun süreler boyunca saklayabilmektedir.

NVRAM (Non Volatile Random Access Memory - Kalıcı Rasgele Erişilebilir Bellek); Yönlendirici (router), anahtar (switch) ve benzeri ağ cihazlarında kullanılan bellek türüdür. Bu tip RAM'lere veriler yazıldıktan sonra elektrik enerjisi kesilse bile veriler kaybolmamaktadır.

Video RAM; Ekran kartlarında kullanıldığından bu şekilde adlandırılmaktadır.

Flash Memory; Elektrik enerjisinin olmadığı durumlarda verileri hafızasında tutabilen yapıya sahiptir. Flash Memory'ler EPROM'un bir çeşididir. Tek farkı Flash Memory'lere veri yazma işlemi de yapılmaktadır.

Ç. Bellek yuvaları

Bellekler anakart üzerinde çeşitli yuvalara (socket) yerleştirilmektedir. Anakart üzerindeki bellek yuvaları sahip oldukları veri yolunun genişliğine göre DIMM (Dual Inline Memory Module) ve SIMM (Single Inline Memory Module) gibi kısaltmalarla adlandırılmaktadır. Dizüstü bilgisayarlarda kullanılan bellekler daha az yer kaplamaları amacıyla daha küçük olarak imal edilmekte ve MicroDIMM veya SODIMM olarak isimlendirilmiştir.

SIMM (Single Inline Memory Module);

RAM'in anakart üzerine montajının yapıldığı soketin adıdır. SIMM modüllerde 72 pin ve 30 pin ayağı olan iki soket tipi vardır. EDO ve FPM belleklerin montesi için kullanılmaktadır.

DIMM (Dual Inline Memory Module);

SIMM in çalışma hızının 2 kat artırılacak şekilde getirilmiştir. DIMM soketler 168, 184, 240 pin sayısına sahiptir. SDR, DDR, DDR2, DDR3 belleklerin montesi için kullanılmaktadır. Farklı pin sayısına sahip bellekler, farklı pin sayısına sahip DIMM yuvalarına üzerlerinde bulunan centik yerlerinin farklı olması sebebiyle yerleştirilememektedir.

SODIMM (Small Outline DIMM) ve MicroDIMM;

Dizüstü bilgisayarlarda kullanılmak için tasarlanmıştır. DIMM yuvaları ile aynı özelliklere sahip fakat boyut olarak daha küçüktür.

SDR SODIMM 100 veya 144, DDR1 SODIMM 200, DDR2 SODIMM 200, DDR3 SODIMM 204 pin olarak üretilmiştir.

SDR MicroDIMM 144, DDR1 MicroDIMM 172, DDR2 MicroDIMM 172, DDR3 MicroDIMM 214 pin olarak üretilmiştir.

RIMM;

RDRAM bellekler için tasarlanan RIMM yuvaları 184 ve 232 pine sahiptir.

SORIMM;

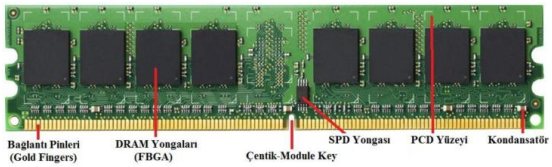
Dizüstü RDRAM belleklerde kullanılan SORIMM yuvaları 160 pin iğneye sahiptir.

III. Belleklerin fiziksel yapısı

Bellekler, mikroişlemcilere benzemektedir. Mikroişlemciler de olduğu gibi silikon baskı devreler üzerine işlenmiş çok sayıda transistör ve kapasitenin, çoğunlukla veriye erişim ve verinin saklanması işlemlerini yerine getirmesi amacıyla oluşturulmuştur. Bu nedenle mikroişlemci ve belleklerin gelişimi birbirleri ile paralellik göstermektedir. Ortak hedefleri; sabit büyüklükteki devrelere daha küçük devre elamanlarının (transistör, kondansatör, direnç vb.) montesini yapmak suretiyle daha hızlı ve daha çok işlem yapılmasını sağlamaktır. Üretim teknolojilerinde yaşanan gelişmelerle bu hedefe kısmen ulaşılmakta, ulaşılamayan kısımlarda ise devreye geliştirilen algoritma ve protokoller girmektedir.

A. Bellek bileşenleri

Bellek üzerinde; bellek yongaları, dirençler ve kondansatörlerin yanı sıra SPD (Serial Presence Detect) denilen bir ROM yongası bulunmaktadır.



Şekil 8 - Bellek bileşenleri

SPD yongası üzerinde bellek ile ilgili çeşitli parametreler saklanmaktadır. Bilgisayarın açılışı (boot) sırasında BIOS tarafından SPD üzerindeki bu parametreler okunmaktadır. BIOS'a belleğin çalışabileceği frekans ve zamanlamayı bildirmekle görevlidir. Böylece anakart ile bellek arasındaki iletişim sağlanmaktadır. SPD yongasında belleğin kapasitesi, üretim tarihi, seri numarası, üretici firma kodu gibi diğer bilgilerde yer almaktadır.[12]

Bellek yongaları ise tıpkı mikroişlemciler gibi, kılıflanmış tümleşik devrelerdir. Verinin en temel hali olan 1 bitlik veriyi yani ikilik düzendeki 0 veya

[12] İnternet, ''Vikipedi Özgür Ansiklopedisi'', 2014, http://en.wikipedia.org/wiki/Serial_presence_detect, E.t. 19.08.2014

1 bilgisini saklamakla sorumlu RAM hücresidir. Bir yongada üzerinde bu hücrelerden milyonlarca adet kullanılmakta olduğundan, bellek hücreleri en az alan kaplayacak, en az fireyle en verimli şekilde çalışabilecek şekilde tasarlanmaya çalışılmaktadır.

B. Belleklerin çalışma prensibi

Belleğin çalışma prensibi anlamak için önce bu tüm devrenin yapısını incelenmelidir. Bellek yongası; belli sayıda satır ve sütunlardan oluşan iki boyutlu bir tablo olarak düşünülmektedir. Tablonun yapıtaşları ise RAM hücreleridir. Bu tablo üzerindeki herhangi bir hücreye erişmek (yazmak ya da okumak) için o hücrenin tablodaki konumunu, yani, hangi satır ve sütunun kesişim noktasında bulunduğunun bilinmesi gerekmektedir. Bu konum bilgisine adres denilmektedir. Erişimi kolaylaştırmak için genelde bellek tablosu yonga üzerinde daha küçük alt tablolara bölünmüştür. Bu alt tablolara da banka (bank) denilmektedir. Adres bilgisi satır ve sütün numaralarının yanı sıra bir banka numarasını da içermektedir. Bu sayede bellek yongası hangi bankanın kaçıncı satırındaki kaçıncı sütunundaki hücreye erişim yapmak istendiğini bilir ve o bilgiye bu sayede ulaşılmış olur.[13]

Registered Memory [Buffered Memory]

Register memory, hafızada bulunan verilerin konumunun tutulduğu bir index tablosunun, hafızanın belli ve küçük bir kısmında tutularak adreslenmesidir. Bu tip belleklerde veri istekleri öncelikle belleğin hafızasında kontrol edilmekte ve eğer varsa ilgili adrese yönlendirilmekte, yok ise yönlendirilmemektedir. Yani var olan verilere ulaşmak için iki arama operasyonu yapılmaktadır. Bu nedenle diğerlerine göre biraz daha yavaş çalışmaktadır.

[13] Semih ERCAN, M.Yasin AYDIN, Mehmet Emin KORKUSUZ, Balıkesir Üniversitesi 2010-2011 yılı Bilgisayar Dersi Proje Raporu (RAM), https://docs.google.com/document/d/1Mp_gprLO4xWBUxND5mSjYiQe-rqwAc5IHbFYrSJ0hG0/edit?hl=tr, E.t. 12.07.2014

UnRegistered Memory [Unbuffered Memory]

Unregistered Memory de Registered Memory'de olduğu gibi bir ön kontrol işlemi yoktur. Bellekten bir veri isteği yapıldığında tüm kayıtlı veriler içinde arama yapılmaktadır.

ECC Memory (Error Correction Code Memory)

Belleklerde oluşabilecek hatalarının bir bölümünün yine bellek tarafından düzeltilmesidir. ECC Memory'ler bünyesinde bulunan her hataları tespit edebilmekte ancak sadece her 64-bit'lik bellek yongası içindeki sadece 1 hatayı düzeltebilmektedir. FPM ve EDO belleklerde bu işleme parity (eşlik) denilmektedir.

Bellekler elektronik bileşenlerdir. Bir elektronik maddenin içindeki ayaklar elektrik akımı ile açılmakta ve kapanmaktadır. Ortamda fazlaca manyetik alan ve enerji ile ilgili sorun var ise bu ayakların açılıp kapanmasında yanlışlıklar meydana getirebilmektedir. Bu nedenle ECC Memory'e ihtiyaç duyulmaktadır.

CAS Latency (Column Address Strobe Latency)

Belleklerin içinde bulunan veriye ulaşılması için gerekli olan süreye CAS Latency denilmektedir.

IV. Band genişliği

Bant genişliği, bilişim dünyasında en çok sözü edilen kavramlardandır. İşlemcilerde, ekran kartlarında, yonga setlerinde, internet bağlantılarında, kısaca verinin transfer edildiği her ortamda bu kavram kullanılmaktadır. Bant genişliği, bir ortamda verinin ne kadar hızlı taşındığının ölçüsüdür. Kısaca, birim zamanda taşınan veri miktarıdır. Bu tanımı belleklere uygulandığında, bellek ile anakart arasında belli bir süre içerisinde taşınan veri miktarıdır.

SDR bellekleri ele alırsak; zaman işaretinin her yükselen kenarında 128 bit veri yolu ile zamanın frekansı birimi olan Hertz (Hz)'in çarpımı bit/saniye

cinsinden band genişliğini verecektir. Örneğin, saat frekansı 166 MHz (Mega Hertz) olan belleğin bant genişliği;

128bit X 166MHz = 21248000000 bit/sn. = 2.47 Giga Byte/sn. (GB/s)

olarak hesaplanır.

DDR belleklerde ise veri transferi saatin sadece yükselen değil aynı zamanda düşen kenarında da gerçekleştiği ve dolayısıyla aynı sürede iki kat daha fazla bilgi taşınabildiği için bant genişliği;

2.47 X 2 = 4.94 GB/s olarak hesaplanır.[14]

§ 3. Belleklerde bulunan bilgiler

Belleklerin hızı sabit disklere oranla çok daha yüksektir. Bu nedenle ihtiyaç duyulan verilere en seri şekilde erişilebilmek için bilgisayarlar çalıştırıldıkları andan itibaren bazı bilgileri geçici olarak belleklere aktarmaktadır. Bellek üzerinde işlemci tarafından işlenen birçok veri bulunmaktadır. Örneğin bellek üzerinde;

- Çalışan işlemler ve hizmetlere ait bilgiler,
- Sistem bilgileri (Örn: Sistemin zamanı),
- Kullanıcılara ait bilgiler,
- Ağ bağlantısı bilgileri,
- Panoda bulunan bilgiler,
- Sistemde çalışan yazılımlar ait bilgiler,
- Komut satırından girilen komutlar,
- Kayıt defteri bilgileri,
- Sosyal medya ve e-mail şifreleri,
- Ziyaret edilen site bilgileri,
- E-posta bilgileri,

[14] Semih ERCAN, M.Yasin AYDIN, Mehmet Emin KORKUSUZ, Balıkesir Üniversitesi 2010-2011 Bilgisayar Dersi Proje Raporu (RAM),

- Disk bazlı şifreleme sistemine ait parolalar,
- İşletim sistemine ait parolalar,

ve benzeri bir çok bilgi bulunmaktadır. Bu bilgiler işlemci tarafından çalıştırılan ilgili uygulamalar vasıtasıyla kullanılmaktadır. Uygulamalar kapatılmış olsa dahi bellek üzerinde; belleklerin kapasitesine ve kullanım oranına göre hala bilgi bulunabilir.

§ 4. Bellek ve adli bilişim

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. Kısaca; bilişim cihazlarından delil elde etme sürecidir.[15] Bu süreç; genel anlamda delil toplama (collection), delillerin incelenmesi (examination), sonuçların değerlendirilmesi (analysis) ile raporlama ve sonuç (reporting) aşamalarından oluşmaktadır.[16]

Bilişim suçları çoğunlukta sosyal medya üzerinden, bulut bilişim marifetleriyle, kötücül yazılım (malware) kullanma ve benzeri yöntemler ile işlenmektedir. Bu yöntemlerin tercih edilme sebebi bilgisayarların sabit diskini kullanmadan direkt olarak bellekte çalışabilmeleri ve belleklerin dinamik yapısı gereği bünyesinde bulunan veriler sürekli değişmekte olduğundan ve bilgisayarın kapatılması veya yeniden başlatılması durumunda bellekte iz bırakılmamasıdır. Önceleri bilişim suçları için yapılan olay yeri incelemelerinde; öncelikle bilgisayarların enerjileri kesilirdi. Bu işlemin sebebi bilgisayarın kapanması veya açılması ile çalışan yazılımlar marifetiyle (Örn. wipe ve deep freze) veya uzaktan

[15] Ahmet Serhat ŞİRİKÇİ / Nergis CANTÜRK "Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi" Bilişim Teknolojileri Dergisi, Cilt: 5, Sayı: 3, Eylül 2012 http://www.btd.gazi.edu.tr/article/viewFile/1041000152/pdf, E.t. 09.09.2014.

[16] Albert MARCELLA / Doug MENENDEZ, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving..., sf.377, Taylor and Francis Group, USA, 2010, https://books.google.com.tr/books?id=nEqHuVht7HgC, E.t. 10.10.2014.

erişim yöntemi ile delillerin zarar görmesinin engellenmesiydi. Bu yöntemin kullanılması bellekte bulunan önemli olabilecek verilerin yok olmasına sebep olmaktadır.

Zira artık pek çok bilişim suçu vakasının çözümünde, sadece sabit disk adli kopyasının incelenmesi kesin sonucu bulmak için yeterli olmamaktadır. Uçucu delil olarak kabul edilen bellek analizi ve ağ aktivite analizinin yapılması bir zorunluluk halini almıştır.[17] Bu bilgilerin analizi için çalışan sistem belleğinin kopyası oluşturulmadan sistem kapatılmamalıdır.

Ayrıca kapatılmış işletim sistemlerinin açılırken oluşturabileceği geçici dosyalar ve geçici hafıza disk alanları (Hiberfil.sys, pagefile.sys vb.) daha önceden silinmiş olan veri alanlarının üzerine yazılabileceği için silinmiş verilerin delil niteliğinde kurtarılabilme olasılığını ortadan kaldırmış olacak ve dolayısı ile delilin bütünlüğünü bozmuş olacaktır. Bu nedenle incelemesi yapılacak bilgisayar sistemleri kapalı durumda iseler kesinlikle açılmamalıdır.

Bellek analizi adli bilişim incelemelerinin olmazsa olmazlarının başında gelmektedir. Müdahale edilen canlı sistemler üzerinden elde edilen bellek imajı üzerinde yapılan analizler ile çok değerli sayısal deliller elde edilebilmektedir. Adli bilişim uzmanları olay müdahalelerinde mutlaka hafızanın imajını almalı ve bu imajı analiz etmeyi süreçlerinin bir parçası haline getirmelidir. Şimdiye kadar genellikle Windows sistemlerin hafızalarına ilişkin adli analiz yöntemleri geliştirilmişti. Son zamanlarda artık Linux ve Mac OS X sistemlerin hafızalarının analizine ilişkin de çalışmaların yapıldığına görülmektedir. Özellikle "volatility" aracı ile gerçekleştirilen birçok hafıza analizi sonucunda elde edilen deliller kritik birçok olayın çözülmesine yardımcı olmaktadır.[18]

---

[17] Polat DUĞAN, Bilişim Suçlarında Ram'in Önemi http://www.difose.com/blog/index.php/malware-analizi/92-bilisim-suclarinda-ram-analizi E.t. 03.10.2014

[18] Halil ÖZTÜRKCİ, Adli Bilişim İncelemelerinde Linux Memory Forensics – 1, http://halilozturkci.com/adli-bilisim-linux-memory-forensics-1, E.t. 26.03.2014

I. İmaj nedir?

Adli bilişim alanında yapılan incelemeler delilin orijinalinde herhangi bir değişiklik meydana getirmemesi için delilin birebir kopyası üzerinde gerçekleştirilmektedir. Delillerden kopya oluşturulurken özel yazılım ve donanımlar kullanılmaktadır. Birebir kopya delilin üzerindeki bütün verilerin kopyasının alınması anlamına gelmektedir. Alınan birebir kopya; mevcut verileri, silinmiş verileri, gizli bölümlerini, veri depolama biriminde bulunan diğer verileri de kapsamaktadır.[19] Kullanılan "birebir aynısı" terimi, orijinal medyanın her sektör ve byte'ının kopyalanması anlamındadır. Kopyalama işlemi sırasında yazma korumalı cihaz ve yazılımlar kullanılmakta[20] ve bu sayede delil bütünlüğü sağlanmaktadır. Delilin birebir kopyasına imaj (image) denilmektedir.

Bir adli bilişim uzmanından herhangi bir konuda inceleme yapılması istendiğinde; adli bilişim uzmanı öncelikle orijinal delilden imaj oluşturmalı ve ardından oluşturduğu imajdan da bir kopya oluşturarak çalışmalarına başlamalıdır. Bu işlemin amacı; imaj dosyasının delil kadar kıymetli olmasıdır. Örneğin delile ait imajın CD ortamında olduğunu varsayıldığında; CD'nin çizilmesi, bozuk bir CD okuyucu ile okunmaya çalışılması gibi nedenle hasar görmesi veya bozulması durumunda da inceleme yapılamayacaktır. Bu nedenle inceleme de ilk yapılacak işlem delilden imaj almak ve imajın da kopyasının oluşturulması olmalıdır.

İmaj oluşturma işlemleri farklı yazılım ve donanımlar kullanarak gerçekleştirmektedir. Yazılımlara; Encase Forensics, Forensic Tool Kit, ProDiscover, SMART, The Sleuth Kit/Autopsy, donanımlara ise; Tableau yazma-

---

[19] Ahmet Serhat ŞİRİKÇİ / Nergis CANTÜRK, "Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi" Bilişim Teknolojileri Dergisi, Cilt: 5, Sayı: 3, Eylül 2012 http://www.btd.gazi.edu.tr/article/viewFile/1041000152/pdf, E.t. 19.06.2014

[20] Harold F. TİPTON / Micki Krause NOZAKİ, Information Security Management Handbook, Sixth Edition, 4. cilt, sf.426.427 Taylor and Francis Group, USA, 2010, https://books.google.com.tr/books?id=KUbaY0MMEvcC,, 2011.

koruma cihazları, Voom Technology cihazları, Solo-III vb. imaj oluşturma cihazları örnek olarak verilebilir.[21]

A. Donanımsal imaj

İncelemeye başlamadan önce delil toplama aşamasındayken hem olay yerinde hem de laboratuar ortamında imaj oluşturmada kullanılabilecek birçok donanım bulunmaktadır. Bu donanımların olmazsa olmazı yazma korumalı olmalarıdır. Bu donanımlardan bazıları doğrudan analiz bilgisayarına bağlanabilmekte bazıları ise Firewire veya USB portları aracılığı ile işlem yapmaktadır.[22] İmaj oluşturma cihazlarının bir tarafına yazma korumalı olarak delil, diğer tarafına imajın oluşturulacağı veri depolama birimi yerleştirilerek imaj oluşturma işlemi gerçekleştirilir.

Şekil 9 - Donanımsal imaj oluşturma cihazları

B. Yazılımsal imaj (sabit disk)

Yazılımsal imaj oluşturan yazılımlar, işletim sistemini kullanmadan, kopyası alınacak aygıt ile direkt olarak bağlantı kurmakta ve imaj

[21] B. CARRIER, ‘‘Digital Investigation Foundation’’, File System Forensic Analysis, Editor: Carrier, B., Addison Wesley Professional, NJ, 12-21, 2005, http://sergiob.org/unam/DGSCA/forense/FileSystemAnalysis.pdf, E.t. 19.06.2014

[22] D. GARZA; ‘‘Data Acquisition and Duplication’’, Computer Forensics Investigating Data & Image Files, Editor: Garza, EC-Council, NY, 2010. https://books.google.com.tr/books?isbn=1435483510, Sf.2-12, E.t. 07.08.2014

oluşturulmaktadır. Bilinen adli imaj alma yazılımları ve genel özellikleri aşağıda anlatılmıştır.[23]

Accessdata FTK Imager; Tüm dünyada en çok tanınan ve bilinen adli kopya alma yazılımlarındandır. Çeşitli yapıda bulunan dijital delilleri yine çeşitli formatlarda en seri ve hızlı şekilde kopyalanmasına imkan sağlamaktadır. Ayrıca, alınan bir adli kopyayı mevcut işletim sistemine disk olarak bağlanmasına da imkan sağlamaktadır. Kullanımı kolay ve kullanıcı dostu bir yazılımdır.

Guidance Software EnCase Forensic Imager; Accessdata firması ile rekabet içerisinde bulunan Guidance Software tarafından üretilen ücretsiz bir yazılımdır. FTK Imager'dan farklı olarak mobil cihazların da adli imajını oluşturmaktadır. Ancak mobil cihaz adli kopyalarını incelemek için lisanslı EnCase yazılımı gerekmektedir.

GETDATA Forensic Imager; GETDATA firması tarafından geliştirilen yazılım, adli imaj alma ve farklı adli imajları birbirine çevirebilmektedir.

ProDiscover Standart; TechPathways firması tarafından geliştirilen yazılımın adli imaj alma ve farklı imajları birbirine çevirme sürümü (standart sürüm) ücretsiz olarak indirilip kullanılabilmektedir.

SANS Investigate Forensic Toolkit (SIFT): SANS tarafından geliştirilen ve eğitimi verilen çalıştırılabilir bir DVD çözümüdür.

Sleuthkit (Autopsy): Temel adli bilişim olay müdahalesi ve temel inceleme işlemleri yapabilen programların bir arada bulunduğu açık kaynak kodlu yazılımıdır.

RAPTOR: Alvarez&Marsal tarafından geliştirilen ve içerisinde pek çok özel yazılımı barındıran bir çalıştırılabilir Linux DVD'sidir.

---

[23]Açık Kaynak Adli Bilişim Çözümleri, http://www.difose.com/blog/index.php/acik-kaynak-yazilim/118-acik-kaynak-adli-bilisim-cozumleri#, E.t. 12.10.2014

DEFT (DART) Linux**:** Bir bilişim suçu vakasında delilleri toplayıp, toplanan deliller üzerinde hızlı bir şekilde incelemeye imkan sağlayan yazılımların bir arada bulunduğu güzel bir açık kaynak Linux DVD'sidir. Hem bilgisayarı Linux işletim sistemi ile boot ederek çalıştırmakta, hem de Windows işletim sistemi üzerinde çalışmaktadır.

CAINE (Computer Aided INvestigative Environment) Linux: Adli bilişimde olaya müdahale için gerekli olan temel yazılımların bulunduğu bir uygulama DVD'sidir.

WinFE: Windows platformunda çalışan ücretsiz adli bilişim çözümüdür. İçeriğinde, ücretsiz olarak tek tek kullanılabilen pek çok yazılım bir araya getirilerek sunulmuştur.

SUMURI (Paladin 4) Linux: Adli bilişimde delil toplamak, canlı inceleme yapmak, analiz ve raporlama yapabilmek için temel bir program setinin sunulduğu çözümdür. Çalıştırılabilir DVD ve USB sürümleri bulunmaktadır.

Matriux: Bir grup Linux gönüllüsü tarafından geliştirilen ve adli bilişimde kullanılan pek çok açık kaynaklı yazılımın bir arada yer aldığı sürümdür.

MASTERKEY: Adli bilişimde olaya müdahale ve temel inceleme için geliştirilen, CD ve USB sürümü olan bir Linux çözümüdür.

Grml Live Linux: Adli bilişimde olaylara müdahale ve temel incelemeler için geliştirilen, CD ve USB sürümü olan bir Linux çözümüdür.

Forensic Hard Copy: Adli bilişimde olaylara müdahale, temel incelemeleri esas alan bir Linux çözümüdür.

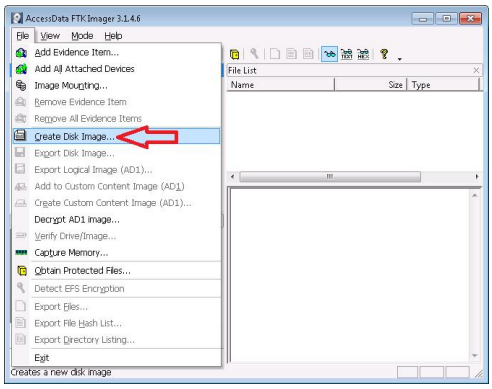
1. Windows ortamında imaj alma

Adli bilişim incelemelerinin en önemli adımlardan birisi, sabit disk üzerinde herhangi bir değişiklik meydana getirmeden imajlarının oluşturulmasıdır. AccessData firması tarafından geliştirilip ücretsiz şekilde kullanıma FTK Imager

yazılımı dijital delil dosyaları üzerinde ön inceleme yapıp bu dosyaların imajının oluşturulmasına imkan tanımaktadır. Bu yazılım ile sabit ve harici disklerin, hafıza kartlarının, zip sürücülerin, CD ve DVD'lerin, dizinlerin yada tek bir dosyanın imajı oluşturulabilmektedir. Aynı zamanda FTK Imager bu ortamlardaki dijital delillerin imajları oluşturulmadan ön izlenme yapma imkanı da tanımaktadır.

Ayrıca diğer adli bilişim yazılımları tarafından oluşturulan imajlar üzerinde de analiz yapabilmekte ve Windows işletim sistemi üzerinden imajların bir sabit disk gibi kullanılmasına da olanak sağlamaktadır.[24] FTK Imager yazılımının diğer işletim sistemleri (Reahat, Ubuntu, Debian, Fedora, Mac) içinde geliştirilmiş sürümleri de vardır.

Yazılım çalıştırdığında[25] ekrana çıkan pencerede File menüsünden "Create Disk Image" seçeneği ile disk imajı oluşturma aşamasına geçilmektedir.



Şekil 10 - Windows ortamında imaj alma - 1

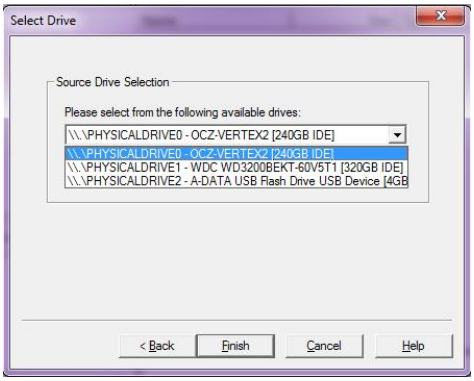
Ardından "Select Source" başlıklı pencerede imaj oluşturulacak kaynak tipi belirlenir. Bu ekrandan bilgisayar üzerinde bulunan sabit diskin tamamı veya bir bölümü (C, D, E) yada belirli bir dizin (belgelerim, masaüstü) veya sadece bir

[24] Halil ÖZTÜRKÇİ; FTK Imager İle Disk İmajı Alma, http://halilozturkci.com/adli-bilisim-ftk-imager-ile-disk-imaji-alma, E.t. 30.08.2014

[25] Yazılımın son sürümüne (3.1.4) "http://accessdata.com/product-download" adresinden erişilebilir, E.t. 01.01.2015

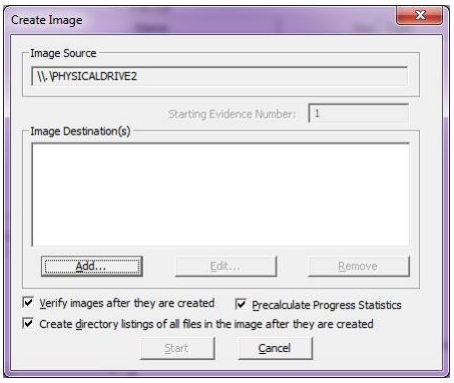
dosya (harcamalar.xls, notlarım.doc) veya CD/DVD sürücüye takılmış herhangi bir CD/DVD seçilebilmektedir.

Bir sonraki ekranda hangi tip formatının imajı alınacak ise seçiminin yapıldığı “Source Drive Selection” penceresi gelmektedir. Eğer imaj alınacak ortam tipi sabit disk olarak seçilmiş ise işletim sistemi tarafından algılanan sabit diskler listelenecektir.



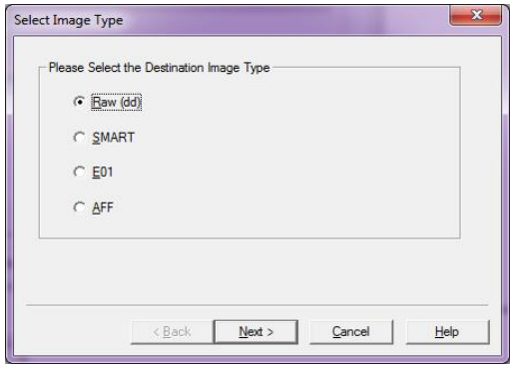
Şekil 11 - Windows ortamında imaj alma - 2

Disk seçildikten sonra gelen pencerede imaj dosyasının oluşturulacağı yer belirlenir. Bu pencereden “Verify images after they are created” seçeneğinin işaretlendiğinde imaj oluşturma işleminden sonra bir doğrulama işlemi gerçekleştirilir. “Precalculate Progress Statistics” seçeneği ise imaj alma işleminin ne kadar süreceği hesaplamaktadır. “Create directory listings of all files in the image after they are created” seçeneği imaj alınacak diskin içinde yer alan dosyalara ait detayları csv formatında imaj ile aynı dizinde oluşturmaktadır.



Şekil 12 - Windows ortamında imaj alma - 3

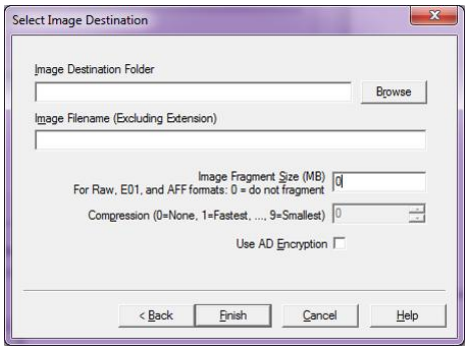
FTK Imager tarafından dört farklı formatta (raw (dd), SMART, E01 ve AFF) disk imajı oluşturulabilmektedir. Tercih edilen format seçilerek devam edilir.



Şekil 13 - Windows ortamında imaj alma - 4

Ardından imaj dosyası ile ilgili ayrıntı bilgilerinin girilmesi gereken pencere gelmektedir. Bu bilgiler; imaj dosyası ile aynı dizinde bulunan imaj işlemine ait özet bilginin bulunduğu text dosyası içinde yer alacaktır.

Sonraki ekranda imaj dosyasının oluşturulacağı dizin belirlenmektedir. “Image Fragment Size(MB)” kısmına 0 (sıfır) yazıldığında tek bir imaj dosyası oluşacaktır. İmaj dosyası parçalara bölünmek istediğinde bu rakam değiştirilmelidir. “Compression” seçeneği imaj sıkıştırma desteği sunan formatlardan birinin seçilmesi durumunda aktif olmakta ve sıkıştırma oranını belirlemektedir. İmajın şifrelenmesi istenirse “Use AD Encryption” seçeneği seçilmelidir.



Şekil 14 - Windows ortamında imaj alma - 5

"Finish" butonu ile imaj alma işlemi başlar. Ardından gelecek pencerede işleminin ne kadar sürede tamamlandığı işlemin hızı gibi bilgileri bulunmaktadır.

Sabit diskin tamamının veya bir bölümü üzerinden imaj alınabileceğinden bahsedilmişti. Sabit diskin tamamına fiziksel disk bir bölümüne ise mantıksal disk denilmektedir. Bu şekilde oluşturulan imaj dosyalarının genel özellikleri incelendiğinde;

Fiziksel imaj; MBR'den en son sektöre kadar fiziksel diskin tamamının kopyalanması esasına dayanmakta ve en iyi delil olarak sıfatlandırılmaktadır. Disklerde RAID yapısı kullanılmamışsa ya da imajı alınacak cihaz, özel bir cihaz değilse fiziksel imaj alınmalı sonrasında mantıksal imajlara bölünmelidir.[26]

Mantıksal imaj; Fiziksel sabit diskin tamamının değil, sadece dosya sistemi katmanı bazında bölümlerin (partition) imajları alınacaksa tercih edilmelidir. RAID sürücüleri ya da şifrelenmiş sürücülerin imajlarının alınmasında kullanılması önerilmektedir.

2. Linux ortamında imaj alma

Linux dağıtımlarında kullanılabilecek "dd"[27] komutu, sabit disk üzerindeki boş alanlarda dahil olmak üzere tüm veriyi bire bir başka bir diske kopyalayabilmekte veya imaj dosyası oluşturabilmektedir.[28] İncelenecek diskin imajının oluşturulması istendiğinde aşağıdaki komut kullanılabilir.

```
dd if=/dev/hdb of=/mnt/yedek/diskimaji.img
```

Yukarıdaki komutta /dev/hdb sabit diskinin /mnt/yedek dizininde diskimaji.img adı ile oluşturulması sağlanmıştır.

---

[26] Halil ÖZTÜRKCİ. Adli Bilişim İncelemelerinde Sabit Disk İmajları – Giriş, http://pentesttools.net/adli-bilisim-araclari/96-adli-bilisim-incelemelerinde-sabit-disk-imajlari-giris, E.t. 06.06.2014

[27] Yazılımın son sürümüne (0.5) "http://www.chrysocome.net/download" adresinden erişilebilir, E.t. 30.08.2014

[28] Harun ŞEKER; "Adli Analiz İşlemlerine Başlamak", http://www.cehturkiye.com/adli_analiz_islemleri.pdf, sf.2, E.t. 19.06.2014

Sabit diskler bir başka diske kopyalanmak suretiyle de analiz işlemi yapılabilir. İncelenecek diskin, Linux işletim sisteminde "/dev/hdb" olarak görülmekte olduğunu ve bu diski aynı kapasitede "/dev/hdc" olarak görünen bir başka hedef diske birebir kopyalamak istediğimizi varsayalım. Kopyalama işlemi için kullanılacak komut aşağıdadır.

dd if=/dev/hdb of=/dev/hdc

Sabit diskin başka bir diske kopyalanmak suretiyle incelenmesi durumunda dikkat edilmesi gerekli olan bir husus hedef diskin hiç kullanılmamış veya kullanılmış ise de diskin tamamen boş olmasıdır. Yani hedef diskte tüm bit'lerin 0 (sıfır) olmasıdır. Hedef diski tamamen sıfırlar ile doldurmak için kullanılacak komut aşağıdadır. Kullanılmış disklere komut uygulandıktan sonra kopyalama işlemi yapılabilir.

dd if=/dev/zero of=/dev/hdc bs=4096

3. Mac ortamında imaj alma

Mac işletim sistemlerinde imaj almak için Mac bilgisayarlara özgü olan "Target Disk Mode" özelliği kullanılabilir. Bu özellik firewire portu aracılığı ile kullanılmaktadır. Target disk modu; firewire bağlantı noktası ile Mac bilgisayara ait sabit disklerinin, başka bir bilgisayara bağlı harici sabit disk gibi kullanılmasını sağlamaktadır.[29] Target disk modunu kullanmak için öncelikle mac bilgisayarın firewire portuna firewire kablosu bağlanır ve mac bilgisayarı ekranında firewire simgesi görülünceye kadar "T" tuşuna basılı tutularak başlatılır. Bu noktadan sonra imaj alma işlemi Windows veya Linux işletim sistemli bir bilgisayar üzerinden geçekleştirilebilir.[30]

[29] OS X Lion: Transfer files between two computers using target disk mode http://support.apple.com/kb/ph3838, E.t. 31.10.2014

[30] How to use and troubleshoot FireWire target disk mode, http://support.apple.com/en-us/ht1661, E.t. 07.10.2014

Ayrıca target disk modunun donanımsal imaj alma cihazları tarafından desteklenmesi durumunda da imaj alma işlemi gerçekleştirilebilir.[31]

4. Uzak ortama imaj alma

Sabit diskin kopyasını almak için harici bir saklama ortamının bulunmadığı veya kullanılamadığı durumlarda network ortamında bulunan başka bir bilgisayara imaj oluşturulabilir. Bu işlem için "dd" komutuna ek olarak Linux araçlarından "netcat"[32] komutu kullanabilir. Network ortamında imaj oluşturabilmek için bir kaynak yani imajı oluşturulacak bilgisayar, birde imajın oluşturulacağı hedef bilgisayara ihtiyaç vardır.

Network üzerinden imaj alma işleminde, hedef bilgisayar "netcat" komutu ile belirlenen bir TCP portunu dinlemeye başlayacak ve porta gelen verileri bir dosyaya yazacaktır. Bunun için kullanılacak komut aşağıdadır.

```
nc -lvp 8080 | dd of=/mnt/yedek/diskimaji.img
```

Bu komut ile belirlenen 8080 numaralı TCP portu dinlemeye başlanmış ve gelen veriler "dd" komutuna aktarılmak suretiyle "diskimaji.img" dosyasının oluşturulması sağlanmıştır.

Kaynak bilgisayarda, hedef bilgisayara disk imajının oluşturulması için;

```
dd if=/dev/hda | nc 192.168.0.2 8080
```

komutu verildiğinde "dd" aracı "/dev/hda" diskini okuyacak ve hedef sistemin (192.168.0.2 şeklindeki IP adresine) 8080 numaralı TCP portuna aktaracaktır. Bu şekilde "netcat" ve "dd" komutları birlikte kullanılmak suretiyle network ortamında imaj alma işlemi gerçekleştirilebilir.

---

[31] Tableau T9 FireWire Forensic Bridge, https://www.guidancesoftware.com/products/Pages/tableau/products/forensic-bridges/t9.aspx, E.t 30.10.2014

[32] Yazılım son sürümüne http://sourceforge.net/projects/nc110/ adresinden erişilebilir, E.t 30.10.2014

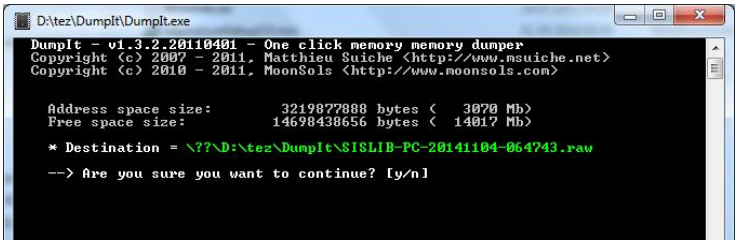
C. Bellek imaj dosyası oluşturma

Sabit disklerde olduğu gibi belleklerde bulunan bilgiler de oldukça önemlidir ve bilgiler üzerinde de adli bilişim incelemeleri gerçekleştirilmektedir. Bellekte bulunan bilgiler uçucu yani bilgisayar kapatıldığında ve üzerine yeni bilgiler eklendiğinde eski bilgiler yok olacağından incelemelerde belleğe öncelik verilmelidir. Sabit disklerde olduğu gibi bellek imajı oluşturmak için çeşitli yazılımlar ve donanımlar bulunmaktadır.

1. Windows ortamında imaj alma

Windows işletim sistemlerinde kullanılan birçok bellek imajı oluşturma yazılımı bulunmaktadır. Dumpit, Mandiant Memoryze, Mantech Memory DD, Win32dd, F-Response, KnTDD, Fastdump, Belkasoft Live RAM Capturer bu yazılımlar içinde öne çıkmaktadır.[33]

Moonsols firması tarafından geliştirilen Dumpit[35] yazılımı ile Windows işletim sistemli bilgisayarların bellek imajı rahatlıkla oluşturulabilir. Yazılım kurulum gerektirmemekte ve kullanımı oldukça kolaydır. Yazılım çalıştırıldığında bellek imajını oluşturmak için onay istemekte ve yazılımın bulunduğu dizine bellek imajını oluşturmaktadır. Aşağıdaki ekran görüntüsünde imaj oluşturma işlemi gösterilmektedir.



Şekil 15 - Windows ortamında imaj alma

[33] Cameron H. MALIN / Eoghan CASEY / James M. AQUILINA; "Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides", sf.71-74, Elseiver Inc, USA, 2012, https://books.google.com.tr/books?id=3GFlrGkMDu4C, E.t. 21.10.2014

[35] Yazılımın son sürümüne (1.3.2) "www.moonsols.com/2011/07/18/moonsols-dumpit-goes-mainstream" adresinden erişilebilir, E.t 01.01.2015

2. Linux ortamında imaj alma

Linux ortamında bellek imajı oluşturmak için sabit disk imajı oluşturmakta kullanılan "dd[36] veya "dc3dd"[37] gibi araçlar kullanılabilir. Bu yazılımlara ilave olarak kullanılabilecek Linux Memory Extractor (LiME)[38], fmem, foriana, memdump gibi araçların yanı sıra Helix3 Pro gibi birçok bilişim aracını bünyesinde barındıran Canlı CD'ler yardımı ile de imaj oluşturulabilir. Dc3dd ile bellek imajı oluşturmak için aşağıdaki örnek komut kullanılabilir.

dc3dd if=/dev/mem of=/home/desktop/bellekimajı.img

Bu komut ile kaynak olarak belirlenen "/dev/mem" sisteme ait belleği ifade etmekte ve bellek imaj dosyasının "/home/desktop" dizininde "bellekimajı.img" ismi ile oluşturulması sağlanmıştır.

3. Mac ortamında imaj alma

Mac sistemler için OSXPMem, Mac Memory Reader, Goldfish gibi yazılımlar ile imaj alma işlemi yapılabilir.[39] Mac Memory Reader ile imaj almak için kullanılacak komut aşağıdadır.[40]

sudo ./MacMemoryReader -v bellekimajı.img

4. Uzak ortama imaj alma

Uzak ortama imaj oluşturmak için Helix3 Pro[41] gibi birçok adli bilişim aracını bünyesinde barındıran canlı CD'ler kullanılabilir.[42] Sabit disk imajı

---

[36] Yazılımın son sürümüne (0.5) "http://www.chrysocome.net/download" adresinden erişilebilir, E.t 21.12.2014

[37] Yazılımın son sürümüne (7.2.6) "http://sourceforge.net/projects/dc3dd" adresinden erişilebilir, E.t 21.12.2014

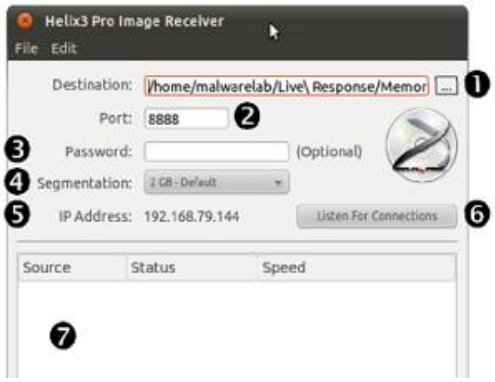
[38] Nicholas GRANT / Joseph SHAW, Unified Communications Forensics: Anatomy of Common UC Attacks, sf.127, Elsevier Inc, Boston, USA, 2014, https://books.google.com.tr/books?id=9lmatCF6L7YC, E.t. 21.10.2014

[39] Cameron H. MALIN / Eoghan CASEY / James M. AQUILIN; Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides, sf.71-74, Elseiver Inc, USA, 2012, https://books.google.com.tr/books?id=3GFlrGkMDu4C, E.t. 21.10.2014

[40] Lorenz KUHLEE / Victor VÖLZOW, Computer-Forensik Hacks, sf.9, O'reilly Verlag, Germany, 2012, https://books.google.com.tr/books?id=bQblShv0v2EC, E.t. 11.10.2014

oluşturulurken kullanılan dd aracında olduğu gibi, uzak ortama bellek imajı oluşturulurken de bir adet hedef bilgisayara ihtiyaç duyulacaktır. Öncelikle hedef bilgisayarın hazırlanması gerekmektedir.

Hedef bilgisayarda "Helix3 Pro Image Receiver" çalıştırılır. Dinlenecek IP ve port numaraları belirlendikten sonra "Destination" alanına imajının oluşturulacağı dizin yazılır ve "Listen For Connections" tuşu ile dinlemeye başlanır. İsteğe bağlı olarak bu işlem parola korumalı olarak da gerçekleştirilebilir.



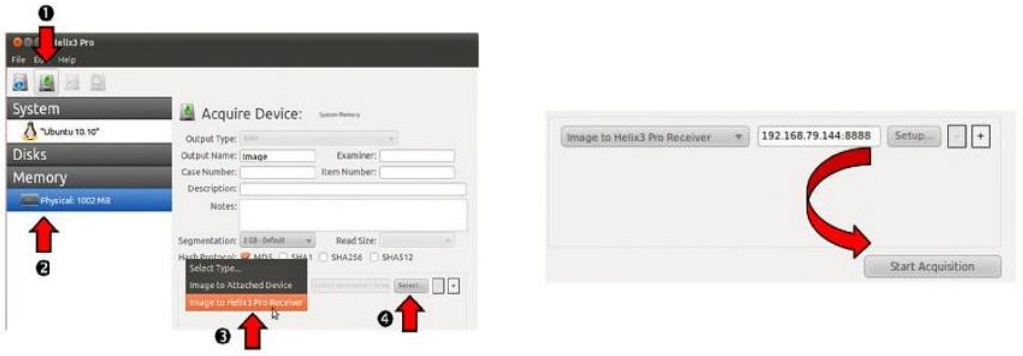
Şekil 16 - Uzak ortama imaj alma - 1

Hedef bilgisayar ayarlandıktan sonra bellek imajı oluşturulacak kaynak bilgisayarda Helix3 Pro çalıştırılır, "Accuire" alanından imajı alınabilecek aygıtlar görülmektedir. Bu alanda sistemin, sabit disklerin veya hafızanın imajı oluşturulabildiği görülmektedir. Bellek imajı oluşturulacağından "Memory" seçilir, uzak ortama imaj oluşturulacağı için "Image to Helix3 Pro Receiver" ardından da "select" seçenekleri ile uzak ortamın belirleneceği pencerenin açılması sağlanır.

---

[41] Yazılımın son sürümüne (2009R1) "https://www.e-fense.com/store/" adresinden erişilebilir, E.t 25.12.2014

[42] Cameron H. MALIN / Eoghan CASEY / James M. AQUILIN, Linux Malware Incident Response : A Practitioner's Guide to Forensic Collection and Examination of Volatile Data : An Excerpt from Malware Forensic Field Guide for Linux Systems, sf. 9-16, Elseiver Inc, USA, 2013, https://books.google.com.tr/books?id=tjnFAwAAQBAJ, E.t. 21.10.2014



Şekil 17 - Uzak ortama imaj alma - 2

Açılan pencereye hedef bilgisayarın IP ve port numarası yazılıp, “Start Acquisition” tuşu ile imaj oluşturmaya başlanır. Bu şekilde uzak ortama başarılı bir imaj oluşturma işlemi gerçekleştirilebilir.

5. Sanal ortamda imaj alma

Windows Virtual PC, Microsoft Hyper-V, VMware, VirtualBox, Xen, Parallels gibi sanallaştırma yazılımlarına bilişim dünyasında sıklıkla rastlanmaktadır. Sanallaştırma yazılımları ile fiziksel bir bilgisayar üzerinde ihtiyaca bağlı olarak birden çok fazla bilgisayar ve/veya birbirinden bağımsız işletim sistemleri çalıştırmak mümkündür. Böylece düşük maliyetle bir fiziksel bilgisayar ile çok daha hızlı işletim sistemleri kurulabilmekte, rahatlıkla yedekleri alınabilmekte, alınan yedeklerden hızlıca geri dönülebilmekte, fiziksel bilgisayarın desteklemediği yazılım ve işletim sistemleri kurulabilmektedir. Çoğunlukla bu özellikleri nedeniyle tercih edilen sanal bilgisayarlar zaman zaman kötü niyetli kişiler tarafından da kullanılmakta ve yaptıkları veya yapmak istedikleri işlemleri gizleyebilmek amacıyla sanal bilgisayar kullanmayı tercih edebilmektedirler. Bu nedenle veya herhangi bir sebeple sanal bilgisayarların hafızalarında analiz yapılması gerekebilir. Sanal bilgisayara ait hafıza alanları, sanallaştırma yazılımlarına göre değişiklik göstermektedir. İncelemeyi yapan kişiden sanallaştırma yazılımlarının hafıza dosyalarının yerlerini bilmesi beklenmektedir. Bilinen bazı sanallaştırma yazılımlara ait hafıza dosyalarına ait bilgiler aşağıdadır.

Sanallaştırma Yazılımı	**Bellek Dosya Uzantısı**	**Bellek Dosyasının Yolu**
VMware	.vmem	Sanal makinanın konfigurasyon dosyası ile aynı lokasyonda
Hyper-V	.bin	Sanal makinanın GUID'si ile oluşturulmuş dizinin altında
VirtualBox	.sav	./VirtualBox/Machines/<Sanal_Makina_Adi>/Snapshots/
Parallels	.mem	/Users/KullanıcıAdı/Paralels/<Sanal_Makina_Adi>/Snapshots/

Tablo 1 - Sanallaştırma yazılımlarına ait bellek dosyaları

Yukarıda bulunan bilgiler sanallaştırma yazılımlarının varsayılan ayarlarıdır. Ancak kullanıcısı tarafından bu dosya yolları değiştirilebilir. Bu durumda inceleme yapacak adli bilişim uzmanı belleğe ait dosyayı fiziksel disk üzerinde araştırması gerekecektir.

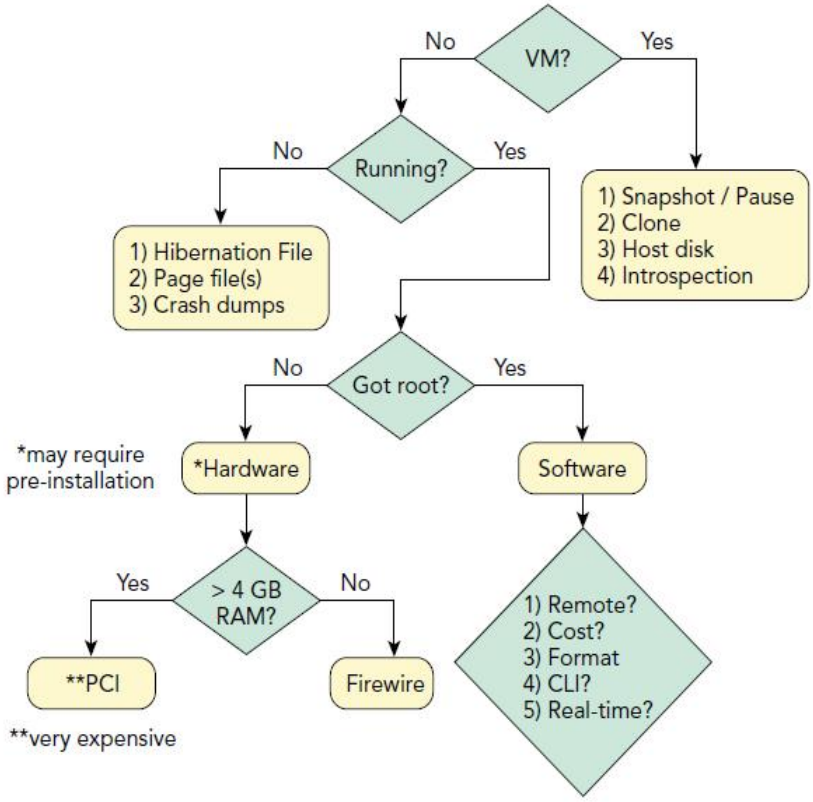
Sanallaştırma yazılımlarının bir başka özelliliği de; sanal bilgisayarlara ait hafıza dosyaları üzerinde herhangi bir uygulamaya ile dönüştürme ve benzeri işleme gerek duyulmaksızın incelenebilmesidir.

Yukarıdaki tabloda yer alan sanallaştırma yazılımlarından; VMware, Hyper-V ve Parallels tarafından kullanılan hafıza dosyası raw formatta, VirtualBox tarafından kullanılan hafıza dosyası ise parçalı hafıza imajı formatındadır. Bununla birlikte sanallaştırma yazılımlarının snapshot olarak adlandırılan ve sanal bilgisayarın belirli bir zamanki haline kolay bir şekilde geri dönülmesini sağlayan özelliği de bulunmaktadır. Sanal bilgisayarlarda snapshot oluşturulmuşsa her bir snapshota ilişkin hafıza dosyası ayrı bir dosyada saklanmakta ve bu dosyaların her biri bellek analiz yazılımına ayrı ayrı girdi olarak verilebilmektedir.[43]

[43] Halil ÖZTÜRKCİ; Adli Bilişim İncelemelerinde Sanal Makinaların Hafıza Dosyalarının Kullanımı, http://halilozturkci.com/adli-bilisim-incelemelerinde-sanal-makinalarin-hafiza-dosyalarinin-kullanimi, E.t. 19.05.2014

Ç. Bellek imajı oluşturma prosedürü

Bellek imajı oluşturma işlemi önceden belirlenmiş bir prosedür ile gerçekleştirilmelidir. Bu konuda yapılan çalışmalar neticesinde oluşturulmuş aşağıdaki prosedür kullanılabilir.[44] Öncelikle işletim sisteminin bulunduğu ortamın belirlenmesi gereklidir.



Şekil 18 - Bellek imajı oluşturma prosedürü

Sistem sanal bir bilgisayar olarak kurulu ise işletim sistemi durdurulmak veya sanal işletim sisteminin snapshot'ı alınmak suretiyle belleğe erişilebilir. Bu durumda sanal sistem altyapısını oluşturan yazılımın bellek için oluşturduğu dosya bilinmelidir. Örneğin Vmware yazılımı memory dosyası olarak .vmem

[44] Michael Hale LIGH / Andrew CASE / Jamie LEVY / Aaron WALTERS, The Art Of Memory Forensics (Dececting Malware and Threads in Windows, Linux and Mac Memory), sf. 71, 471, 537-541, John Wiley & Sons, Inc., Indiana, USA, 2014, http://news.asis.io/sites/default/files/The%20Art%20of%20Memory%20Forensics.pdf

dosya uzantısını kullanmaktadır.[45] Ayrıca Vmware'de; sistemin snaphot'ı alındığında vmname.Snapshotnumber.vmsn seklinde snapshot dosyası oluşmaktadır.[46] Hiper V'de memory dosyası olarak .bin uzantısı kullanılmaktadır. Snapshot dosyası ise .avhd uzantılıdır.

İşletim sistemi; gerçek bir bilgisayarda kurulu ise bilgisayarın çalışıyor veya çalışmıyor olması durumuna göre hareket edilmelidir. Bilgisayar çalışmıyor ve uyku moduna alınmış ise bilgisayar Canlı CD/DVD/USB ile açılmak suretiyle (off-line) disk imajı oluşturulur ve bu imaj içinden hiberfil.sys ve pagefile.sys dosyaları tespit edilmek suretiyle bellek incelemesi yapılmalıdır.

Sistem gerçek bir bilgisayar üzerinde çalışıyor ise çalışan sistemde o an anda oturum açılmış kullanıcının yetkisi önemlidir. Yetkili kullanıcı haklarına sahip olunması durumunda; bellek imajı oluşturabilen yazılımlar ile imaj oluşturulmalıdır. Ancak, yetkili kullanıcı haklarına sahip olunamadığı durumlarda, donanımsal çözümlere başvurulmalıdır.

Donanımsal çözümler oldukça pahalıdır ve sistem üzerinde önceden kurulmuş olması gereklidir. Bazı bilgisayarlar üzerinde bulunan Firewire portu üzerinden donanımsal olarak imaj oluşturulabilir ve bu konu ilerleyen sayfalarda ayrıntılı olarak incelenecektir.

Donamsal çözümler arasında bulunan PCI yuvasına bağlanan kartlar yardımıyla sistemin hafızasında bulunan bilgilere erişmek mümkündür. PCI yuvası üzerinden hafıza imajı oluşturma işleminin gösterildiği video https://www.youtube.com/watch?v=vJszLtaIyIk adresinden izlenebilir. Windowsscope firmasına ait CaptureGUARD kartı ve firma tarafından geliştirilen

---

[45] VMware Workstation 5.5 What Files Make Up a Virtual Machine?, https://www.vmware.com/support/ws55/doc/ws_learning_files_in_a_vm.html, E.t. 06.08.2014

[46] VMware vSphere 5.1 Documentation Center - ESXi and vCenter Server 5.1 Documentation - vSphere Virtual Machine Administration - Managing Virtual Machines - Using Snapshots To Manage Virtual Machines - Snapshot Files https://pubs.vmware.com/vsphere1/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-38F4D574-ADE7-4B80-AEAB-7EC502A379F4.html, E.t. 07.08.2014

uygulama ile mobil cihazlar üzerinden dahi, hedef sisteme ait bellek bilgilerine erişim imkanı sağlanmıştır.[47] Ayrıca yine aynı firmaya ait CaptureGUARD Gateway kart ile; kilitli durumda bulunan Windows işletim sistemli bilgisayarlara parolasız olarak giriş yapılabilmektedir.[48]

II. Hash nedir?

Bilgi güvenliği denilince gizlilik, bütünlük ve erişilebilirlik kavramları ön plana çıkmaktadır. Bilginin gizliliği kavramı ile kastedilen, bilgiye sadece o bilgiye erişmesi gereken kişi ya da kişilerin erişimine izin verilmesidir. Bilginin erişilebilirliği kavramı ile kastedilen ise, bilgiye istenilen ve makul olan bir zamanda erişilmesi ve bilginin kullanılmasıdır.[49] Bütünlük ise bilginin kaynağında olduğu şekliyle, bozulmadan, değiştirilmeden erişilebilir olmasıdır. Bir bilginin kısmen bozulmuş veya kısmen değiştirilmiş olması bütünlüğün bozulması anlamına gelmektedir.[50] Bilginin bütünlüğü özet değeri (Hash) ile sağlanmaktadır.

Özet değeri oluşturulmak amacıyla çeşitli algoritmalar geliştirilmiştir. Özetleme algoritmaları, girdi olarak kullanılan herhangi bir uzunluktaki veriyi işleyerek sabit uzunlukta bir özet değeri üreten tek yönlü algoritmalardır. Özetleme algoritmalarının en önemli özellikleri, birbirinden çok az farklı girdiler için dahi tamamen ayrı çıktılar üreterek çakışmaları önleyebilmeleridir. Özet

---

[47] WindowsSCOPE Live Real-Time Cyber Investigation and Memory Forensics, 2011 BlueRISC Inc., .0http://www.windowsscope.com/index.php?option=com_docman&task=doc_download&gid=41&Itemid=, E.t. 08.06.2014

[48] CaptureGUARD Gateway - Access to Locked Computers, Http://www.windowsscope.com/index.php?page=shop.product_details&flypage=flypage.tpl&product_id=30&manufacturer_id=0&option=com_virtuemart&Itemid=34&cid=10030, E.t. 08.06.2014

[49] Muhammet BAYKARA, Resul DAŞ, İsmail KARADOĞAN; Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi, sf.2, 20-21.05.2013 http://perweb.firat.edu.tr/personel/yayinlar/fua_721/721_80043.pdf, E.t. 23.09.2014

[50] Gökhan MUHARREMOĞLU; Olası Zafiyetlerin Tahmininde Temel Bilgi Güvenliği Prensiplerinin Kullanılması https://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/olasi-zafiyetlerin-tahmininde-temel-bilgi-guvenligi-prensiplerinin-kullanilmasi.html, E.t. 26.12.2013

değerinden girdi verisine ulaşmak imkansızdır. Özet değerleri, veri bütünlüğünün bozulup bozulmadığının kontrolü için kullanılmaktadır.[51]

En çok kullanılan hash algoritmaları ve genel özellikleri şunlardır:

MD2, MD4 ve MD5: Massachusetts Teknoloji Enstitüsünden Ron Rivest tarafından 1991 yılında geliştirilmiş kriptografik özet (tek yönlü şifreleme) algoritmasıdır. Girdi verinin boyutundan bağımsız olarak 128 bitlik (hexadecimal) özet değeri oluşturmaktadır. Günümüzde bu algoritmalardan MD5 algoritması kullanılmaktadır.

Secure Hash Algorithm (SHA): Bu algoritmanın SHA-1, SHA-2, SHA-256, SHA-384 ve SHA-512 olarak birçok çeşidi bulunmaktadır. Bu çeşitlerin aralarındaki fark hash değerinin bit uzunluklarıdır. SHA hash algoritmaları ABD'de kurulmuş olan ve çalışmalarına devam eden NIST ve NSA isimli iki birim tarafından hazırlanmıştır.[52]

Özet değerinin Adli bilişime bakan yönü hakkında bilgi sahibi olabilmek için Polis Akademisi Araştırma Merkezleri Başkanlığı bünyesinde faaliyetlerine devam eden Uluslararası Terörizm ve Sınıraşan Suçlar Araştırma Merkezi (UTSAM) tarafından yapılan "Bilişim Suçları ve Delillendirme Süreci"[53] konulu çalışma incelenebilir. Çalışmada Türkiye'deki bilişim suçlarıyla mücadelede işleyen delillendirme sürecinin ne durumda olduğu, eksiklikleri ve yapılması gerekenler ortaya konmaya çalışılmıştır.

---

[51] Zülfükar SAYGI / Sezen YEŞİL, Telekomünikasyon Kurumu ile ODTÜ-Uygulamalı Matematik Enstitüsü Kriptografi Bölümü tarafından yürütülmüş olan "Açık Anahtar Altyapısı Konusunda Araştırma, Geliştirme ve Uygulamalar" proje makalesi, sf.3 http://www.ueimzas.gazi.edu.tr/pdf/bildiri/24.pdf, E.t. 08.06.2014

[52] Debra Littlejohn SHINDER, Scene of the Cybercrime: Computer Forensics Handbook, sf.380, Syngress Publishing, USA, 2002, https://books.google.com.tr/books?id=BLjomivi1asC, 09.06.2014

[53] Yrd.Doç.Dr. Hüseyin ÇAKIR / Ercan SERT; Uluslararası Terörizm ve Sınıraşan Suçlar Araştırma Merkezi (UTSAM) ve Gazi Üniversitesi, Endüstriyel Sanatlar Eğitim Fakültesi, Bilgisayar Eğitimi Bölümü tarafından hazırlanan "Bilişim Suçları ve Delillendirme Süreci" konulu makale,
http://utsam.org/images/upload/attachment/utsas_2010_secilmis/Bili%C5%9Fim%20Su%C3%A7lar%C4%B1%20ve%20Delillendirme%20S%C3%BCreci.pdf, E.t. 09.06.2014

Araştırma neticesinde bilişim suçu delili olan dijital medyaların (verilerin) olay yerinde teşhis edilmesi sırasında; olay yerine gidecek olan personelin ne araması gerektiği, ne ile karşılaşabileceği hakkında detaylı ön bilgilere sahip olması gerektiği sonucuna ulaşılmıştır.

Ayrıca çevre güvenliğinin iyi bir şekilde alınması, delil olabilecek materyallere sadece adli bilişim alanında uzman personel tarafından müdahale edilmesi, teşhisin acele değil yavaş ve detaylı bir şekilde yapılması gerekmektedir. Bilinçsiz yapılan müdahalelerde delil bütünlüğünün bozulması veya ulaşılabilecek çok önemli bilgilerin elde edilememesi gibi sonuçlar ortaya çıkabilmektedir.

Dijital medyaların barındırdığı verilerin hassas olduğundan olay yerinde bu medyalara müdahale edilirken hassasiyetle dikkat edilmesi, delil bütünlüğünü koruyarak uluslararası adli bilişim standartlarında kopyasının (imajının) alınması gerekmektedir.

Bu konu ülkemizde Ceza Muhakemesi Kanunu (CMK) 134'ü maddesinde düzenlenmiştir. Kanunda;

> (1) Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve 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) Üçüncü fıkraya göre alınan 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.

yazmaktadır.

Kanunun 3. fıkrasının amacı, bilişim suçlarında çoğunlukla tek delil bulunabilecek olan bilgisayar sistemindeki delillerin kaybolmasını, bozulmasını veya değiştirilmesini engelleyerek adaletin tecelli etmesinin sağlanmasıdır. Bilgisayarlardaki veriler çok hassas verilerdir. Nasıl ki bir cinayet mahallindeki DNA'larda meydana gelebilecek en ufak bir kirlenme sebebiyle tespit edilemez hale geliyorsa elektronik deliller de aynı şekilde ufak bir hareket, enerji kaybı vb. gibi bir sebepten dolayı bozulabilir. Bu gerçeğin farkında olan kanun koyucu bu sebeple 3. fıkra hükmünü getirmiştir.

Bu fıkranın hemen altında yer alan ve bu fıkra ile doğrudan ilgisi bulunan 4. fıkrada ise, "İstemesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır." denilmektedir. Bu hükmün de amacı adaletin tecelli etmesine imkan tanımaktır. Hakim vicdani kanaate ulaşabilmek için sanığın bilgisayarından elde edilen kopyalar ile sanığın veya vekilinin eline bırakılan kopyaların birebir aynı olduğunu, herhangi bir değişikliğin, bozulmanın, müdahalenin söz konusu olmadığını mahkeme dosyasında görmelidir. Bilgisayarlar alınıp götürüldükten sonra artık o bilgisayarlar üzerinde ne gibi işlemler yapıldığını denetlemeye imkan

bulunmamaktadır. Veriler kasten değiştirilebileceği gibi ihmalle de değiştirilebilir.[54]

CMK 134'te sadece yedeklerin alınacağından bahsedilmekte ancak alınan yedeklerin bozulmadan/değiştirilmeden mahkeme huzuruna getirilmesi konusunda bir düzenleme bulunmamaktadır. Delil bütünlüğü açısından CMK 134 yetersiz kalmaktadır. Ancak CMK 134'te yazmamasına rağmen veri bütünlüğü; yedekler alınırken (imaj) hash değerinin de oluşturması ve "şüpheliye veya vekiline" verilmesi ile sağlanabilir.

UTSAM tarafından yapılan "Bilişim Suçları ve Delillendirme Süreci" konulu çalışma sonucunda Türkiye'deki bilişim suçlarıyla mücadelede görev alan bilişim uzmanlarının çözüm önerileri arasında;

> "CMK md. 134, günümüze hitap etmemekte ve çok sınırlı kalmakta, bu da kolluk kuvvetlerinin bu alandaki faaliyetlerini kısıtlamaktadır. Bundan dolayı CMK'nın arama ve el koyma bölümü altında dile getirilen bilgisayarlarda, bilgisayar programlarında ve kütüklerinde, arama, kopyalama ve el koyma maddesinin detaylandırılması, hatta birden fazla madde ile yeniden düzenlenmesi gerekmektedir."[55]

bulunmaktadır.

Hash değeri, hash'i hesaplanan veriye özel ve parmak izi gibi benzersiz bir değerdir. Hash değeri üzerinden tersine mühendislik yapılarak veriye ulaşılamaz. Veri depolama birimi üzerindeki bir karakterin bile değişmesi durumunda hash değişmektedir. Dolayısıyla elektronik delil üzerinde veya o delilden alınan adli kopya üzerinde herhangi bir değişiklik olup olmadığını kontrol etmek için hash

---

[54] Ali Osman ÖZDİLEK, CMK m.134 Uygulamasında Verilerin md5 Algoritması ile "hash" Değerlerinin Alınmasında Çakışma (collision) Sorunu - 1 http://www.turk-internet.com/portal/yazigoster.php?yaziid=34497, E.t. 15.11.2014

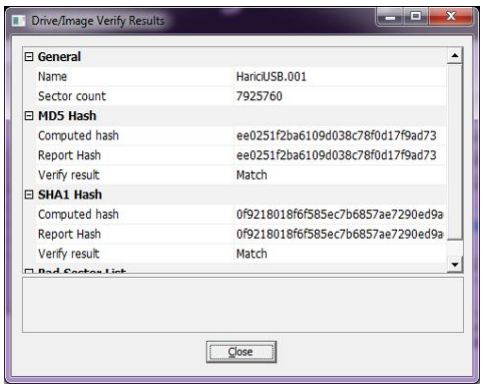
[55] Yrd.Doç.Dr. Hüseyin ÇAKIR / Ercan SERT; Bilişim Suçları ve Delillendirme Süreci, http://utsam.org/images/upload/attachment/utsas_2010_secilmis/Bili%C5%9Fim%20Su%C3%A7lar%C4%B1%20ve%20Delillendirme%20S%C3%BCreci.pdf, sf.160, E.t. 11.09.2014

hesaplatılır. Hash hesaplaması sonucu çıkan hash değeri ile ilk hesaplanan hash değeri birbiri ile aynı ise elektronik delilin veya elektronik delilden alınan adli kopyanın değişikliğe uğramadığı anlamına gelmektedir. Hash değeri elektronik verinin mührü olarak kullanılmaktadır. Uygulamada: açık olan sistemler, RAM'ler ve cep telefonları üzerinde kayıtlı olan verilerin adli kopyaları alındıktan sonra orijinal elektronik delil üzerinde değişiklik olup olmadığının kontrolü amacıyla orijinal delil üzerinden tekrar hash hesaplaması yapılamamaktadır. Çünkü çalışmaya devam eden bu sistemler üzerinde, halen sistem tarafından zararsız ufak değişiklikler olduğundan hash değerleri de değişmektedir.[56]

Hemen hemen tüm imaj alma yazılımları aldıkları imaj dosyalarına ait hash değerini hesaplayabilmektedir. Hesaplanan hash değerleri incelemeye başlanmadan önce mutlak surette not edilmelidir. Genel bilinen bazı imaj alma yazılımları için hash değerlerine ulaşmak için aşağıdaki işlemler yapılır.

FTK Imager; imaj oluşturma işleminin sonlandığını bildiren pencerede bulunan "Image Summary" tuşuna basıldığında imaj alma işlemi hakkında ve hash bilgilerin bulunduğu ve aşağıdaki ekrana benzer bir pencere çıkmaktadır. Aşağıda bulunan ekran çıktısında görüldüğü üzere FTK Imager hem MD5 hemde SHA1 hash değerini aynı anda hesaplayabilmektedir. Ayrıca var ise bozuk sektörleri de gösterebilmektedir.

[56] Murat OZBEK, I. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu (ISDFS'13), "Adli Bilişim Uygulamalarında Orijinal Delil Üzerindeki Hash Sorunları" konulu sunum, 20-21 Mayıs 2013, Elazığ, Türkiye, sf.6, http://www.bilgisayardedektifi.com/wp-content/uploads/2013/06/MuratOZBEK_Adli_Bilisimde_Orijinal_Delil_Uzerindeki_hash_Sorunlari_isdfs_bildiri.pdf, E.t. 09.11.2014

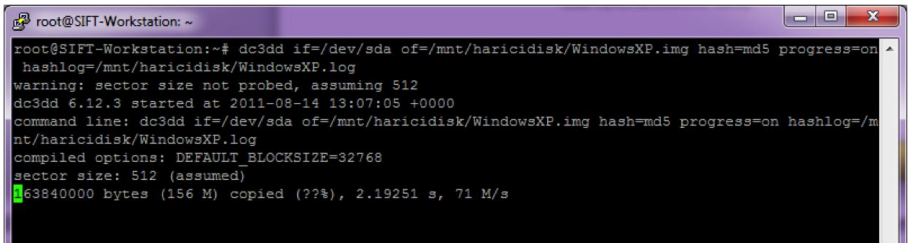


Şekil 19 - Hash değeri hesaplama ekranı – 1

Linux sistemlerde imaj oluşturmak için kullanılan dc3dd yazılımı ayrı zamanda hash değerinin de oluşturabilmektedir. Uygulamanın örnek kullanımını aşağıdadır.

dc3dd if=/dev/sda of=/mnt/haricidisk/WindowsXP.img hash=md5 progress=on hashlog=/mnt/haricidisk/WindowsXP.log

Bu komutta hash=md5 parametresi ile imaj alma işlemi esnasında imaja ait MD5 hash değerinin hesaplanması ve bu hash değerinin hashlog=/mnt/haricidisk/WindowsXP.log parametresi ile WindowsXP.log dosyasına kayıt edilmesi sağlanmıştır. Bu komutun kullanımına ait ekran görüntüsü aşağıdadır.



Şekil 20 - Hash değeri hesaplama ekranı – 2

“Dd” yazılımı ile hash değeri oluşturulmak istenildiğinde kullanılacak parametre –cryptsum md5 olacaktır. Uygulamanın örnek kullanımını aşağıdadır.

dd.exe if=\\.\D: of=E:\imajdosyasi.img --cryptsum md5 -verify --cryptout E:\imajdosyasi.md5

Mac sistemlerde imaj alınırken kullanılan komuta “-H SHA-256” ilave edildiğinde hash değeri oluşturulmaktadır. Örnek kullanımı aşağıdadır.

sudo ./MacMemoryReader -v -H SHA-256 memory.img.

Ayrıca dd, dc3dd ve MacMemoryReader yazılımlarında kullanılan parametrelere “md5”, “sha”, “sha1”, “sha256” girilerek diğer hash formatlarının da hesaplanması sağlanabilir.

III. Bellek incelemesi ile erişilebilecek bilgiler

Bilgisayarlarda çalışan uygulamalar ve bu uygulamalara verilen girdiler çalıştıkları sürece ve belleğin kapasitesine bağlı olarak ilgili işlemlerin sonlandırılması durumunda da dahi bellekte bulunabilir. Örneğin sosyal medya ve e-posta sistemlerine ulaşmak için girilen kullanıcı adı ve parolalar, komut satırından girilen komutlar, ağ bağlantısı bilgileri, ziyaret edilen internet sitelerine ait bilgilere bellek incelemesi erişilebilir. Bu bölümde bellekte bulunan çeşitli uygulamalara ait bilgilere erişmede kullanılabilecek değişik yöntemler ele alınacaktır.

A. Sosyal medya / e-mail şifreleri

ABD’de elektronik delilin kullanıldığı hemen her davada e-posta bulunmaktadır. Yapılan bir araştırmaya göre 2001 yılında e-postaların (özellikle özel hukuk ile ilgili) davalarda delil olarak kullanım oranı %9 iken, bu rakam 2002 yılında %14’e çıkmıştır.[57]

Özellikle tasarlanarak işlenen suçların ceza oranlarının farklı olması nedeniyle, tasarlamaya yönelik hareket ve niyete dair izlerin bulunabileceği elektronik delillerin özellikle e-postaların incelenmesi gereklidir.[58] Mevcut ve

[57] Ali KARAGÜLMEZ, Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri, sf. 252-303, Seçkin Yayıncılık, Ankara, Ocak 2011, http://www.hukukmarket.com/images/contentspdf/137142.pdf, E.t. 24.09.2014

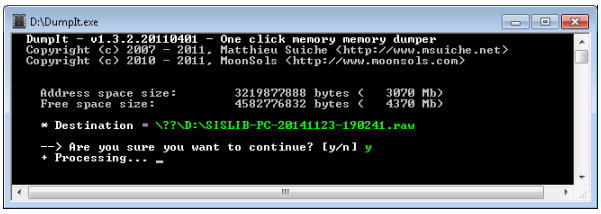
[58] Türkay HENKOĞLU, Adli Bilişim (Dijital Delillerin Elde Edilmesi ve Analizi), sf.121, 2011, Ankara, Pusula Yayıncılık,

silinmiş e-postalara erişilebilmesi ile e-posta başlık bilgilerinin analiz edilmesi bu açıdan önemlidir.[59]

Çeşitli internet gezgini uygulamaları (Internet Explorer, Google Chrome, Mozilla Firefox, vb.) kullanılmak suretiyle girilen sosyal medya ve e-posta sistemlerinde kullanılan parola ve kullanıcı adı bilgisi bellekte tutulmaktadır. Bu uygulamalara girilen bilgiler uygulamanın sonlandırılması sonrasında dahi bellek incelemesi ile elde edilebilir. Bu bölümde internet ortamında hizmet veren 3 farklı sisteme (Facebook, Gmail, Yahoo) ait bilgilere değişik yöntemler kullanılmak suretiyle nasıl erişilebileceği örneklenecektir.

1. Facebook parolasına erişim

Facebook parolasını öğrenebilmek için öncelikle bilgisayarın bellek imajı oluşturulmalıdır. Bellek imajı oluşturmak için "Dumpit"[60] yazılımı kullanılacaktır. Yazılım çalıştırıldıktan sonra çıkan pencere de imaj oluşturma işleminin onaylanmasını müteakiben imaj dosyası oluşturacaktır. Aşağıdaki ekran çıktısında imaj oluşturma işleminin başlatıldığı görülmektedir.



Şekil 21 - İmaj oluşturma ekranı

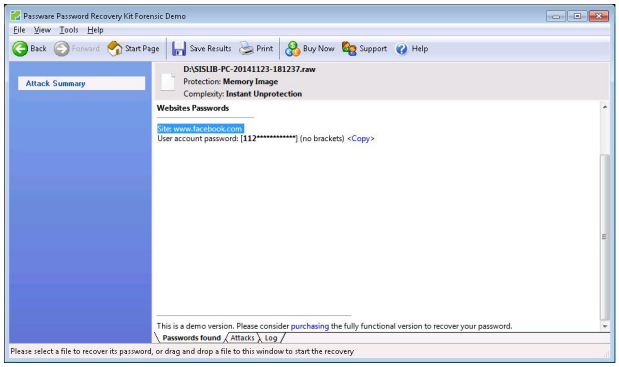
Bellek imajı oluşturma işlemi tamamlandığında "Passware Kit Forensic"[61] yazılımı bellek imajının inceleneceği bilgisayara kurulumu yapılır. Passware Kit

[59] Hüseyin ÇAKIR / Mehmet Serkan KILIÇ, Bilişim Suçlarına İlişkin Delil Elde Etme Yöntemlerine Genel Bir Bakış, sf.14, Polis Bilimleri Dergisi, 15.03.2013, http://www.pa.edu.tr/APP_DOCUMENTS/D478B2AD-3813-4555-9629-6332F8CF8D33/cms_statik/_dergi/2013/3/4%20-%20D34%20Bili%C5%9Fim%20su%C3%A7lar%C4%B1%20veri%20elde%20etme.pdf

[60] Yazılımın son sürümüne (1.3.2) "www.moonsols.com/2011/07/18/moonsols-dumpit-goes-mainstream" adresinden erişilebilir, E.t 01.01.2015

[61] Yazılımın son sürümüne (13.7) "http://www.lostpassword.com/kit-forensic.htm" adresinden erişilebilir, E.t 01.01.2015

Forensic yazılımının çok geniş bir parola elde etme yelpazesi bulunmaktadır.[62] Bu bölümde bellekten internet gezginine girilmiş parolalar elde edileceğinden yazılım çalıştırıldığında açılan pencereden "Memory Analysis" seçilir. Ardından gelen ekranda "Websites" seçeneği ile devam edilir ve oluşturulmuş imaj dosyası yazılıma girdi olarak verilir. Yazılım bellek imaj dosyası içinde parola aramaya başlar. Arama işlemi sonuçlandığında, bellekte bulunan web sitelerine girilen parolalar elde edilecektir. Aşağıdaki ekran görüntüsünde facebook'a girilen parola görülebilmektedir. Yazılımın demo sürümü kullanıldığından parolaya ait ilk 3 karakter yazılım tarafından gösterilmiştir. Tam sürümü elde edildiğinde parolanın tamamı elde edilebilir.



Şekil 22 - Facebook parolasına erişim

Ayrıca yazılıma, parola elde edilecek bilgisayarın hibernation özelliği aktif durumda ise sabit diskinde bulunan "hiberfil.sys" dosyasını da girdi olarak verilebilir.[63] Bu durum adli bilişim için delil toplama kurallarından biri olan "kapalı olan sistemin açılmamasının" gereğinin uygulanabilmesi adına yazılımın güzel bir özelliğidir.

2. Gmail parolasına erişim

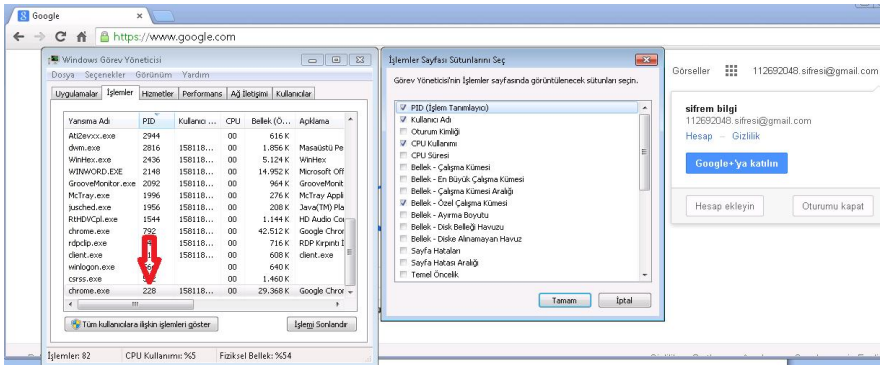
Gmail şifresini öğrenilecek bilgisayarda görev yöneticisi başlatılır ve görev yöneticisinden "Görünüm - Sütün seç" ve PID[64] seçeneği işaretlenir. Bu sayede

[62] Passware Kit Forensic 2015, http://www.lostpassword.com/kit-forensic.htm, E.t. 24.09.2014

[63] Passware Newsletter, http://www.lostpassword.com/news/pnl66.htm, E.t. 25.09.2014

[64] İnternet, ''Vikipedi Özgür Ansiklopedisi'', 2014, http://en.wikipedia.org/wiki/Process_identifier, E.t. 25.09.2014

oturum açılmış olan internet gezginine (Örnek uygulamada Google Chrome kullanılmıştır.) ait uygulamanın işlem süreci belirleyicisi olan PID'nin görüntülenmesi sağlanır.

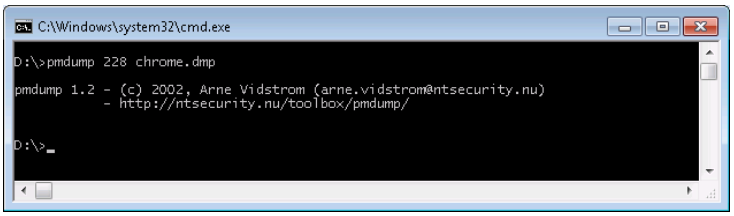


Şekil 23 - Gmail parolasına erişim - 1

Yukarıdaki ekran çıktısında bilgisayarda Google Chrome üzerinde gmail oturumuna giriş yapılmış olduğu ve uygulamaya ait PID numarasının 228 olduğu görülmektedir.

Bu işlemden sonra çalışan proseslerin kopyasını prosese müdahale etmeden oluşturabilen[65] "Pmdump"[66] aracı indirilir. Ardından komut satırına girilir ve 228 numaralı Chrome internet gezgini işlemi için;

pmdump 228 chrome.dmp



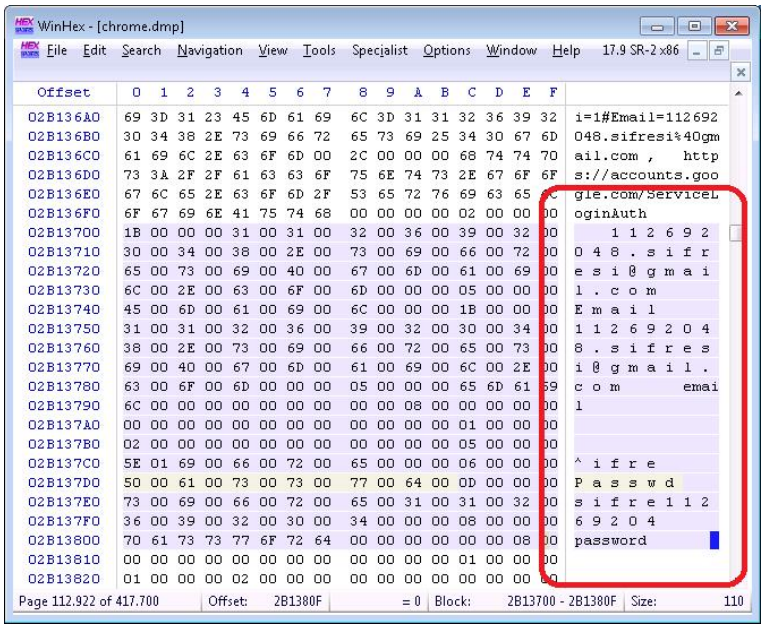
Şekil 24 - Gmail parolasına erişim - 2

komutu verilerek prosesin kopyası oluşturulur. Ardından yapılacak işlem oluşturulan "chrome.dmp" dosyası içinde gmail oturumu için kullanılan parola ve

[65] Cameron H. MALIN / Eoghan CASEY / James M. AQUILIN, A Malware Forensics: Investigating and Analyzing Malicious Code, sf.161-162, Elseiver Inc, USA, 2008, http://books.google.com.tr/books?id=lRjO8opcPzIC, E.t. 21.10.2014

[66] Yazılımın son sürümüne (1.2) "http://ntsecurity.nu/toolbox/pmdump/" adresinden erişilebilir, E.t 26.12.2014

kullanıcı adının tespit edilmesidir. Bu işlem için "Winhex"[68] yazılımı kullanılacaktır. Winhex'te "chrome.dmp" dosyası açılır ve menüsünden "Search – Simultaneous Search" tıklanır. Açılan ekrana gmail oturumuna ait parola aradığımız için "Passwd" yazılır ve tarama işlemi başlatılır. Çıkan sonuçlar analiz edildiğinde kullanıcı adı ve parola bilgisinin bu yöntemle elde edilebildiği aşağıdaki ekran çıktısında görülmektedir.

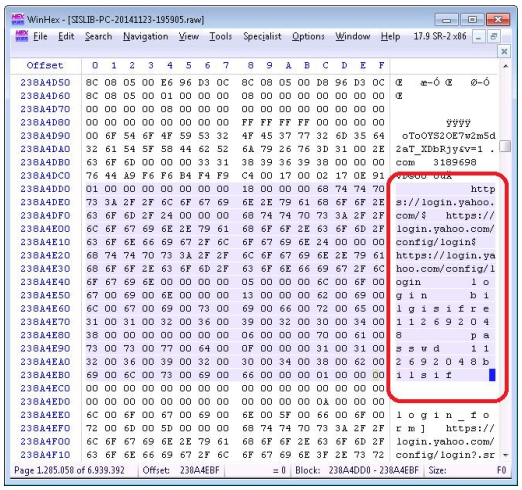


Şekil 25 - Gmail parolasına erişim - 3

3. Yahoo parolasına erişim

Yahoo parolasına; gmail parolasına erişmekte kullanılan yöntem olan parolanın girildiği prosese ait işlemin kopyasının üzerinden elde edilebileceği gibi tüm proseslerin kopyasının (imaj) oluşturulması ile de elde edilebilir. Bu yöntemde de "Dumpit" yazılımı ile sisteme ait belleğin imajının oluşturulması sağlanır. Oluşturulan bellek dosyası Winhex yazılımı ile açılır ve bellek dosyası içinde "passwd" kelimesi aranır. Çıkan sonuçlar incelendiğinde Yahoo kullanıcı adı ve parolasının elde edilebileceği aşağıdaki ekran çıktısında görülmektedir.

[68] Yazılımın son sürümüne (17.9) "http://www.x-ways.net/winhex/" adresinden erişilebilir, E.t 26.12.2014



Şekil 26 - Yahoo parolasına erişim

Yukarıda bahsedilen parola ve kullanıcı adlarına ait bilgiler oturumlar başlatılmış ve/veya sonlandırılmış olsa dahi elde edilebilir. Ancak elde edilememe ihtimali de bulunmaktadır. Bu duruma etki eden unsur ise oturumun başlatılması ve/veya bitirilmesi ile hafıza imajının oluşturulduğu zamanlar arasındaki farktır.

Ayrıca değişik yöntemler kullanılarak elde edilen bu bilgiler için kullanılan yöntemler birbirleri yerlerine de kullanılabilir. Örneğin;

- Facebook parolası için kullanılan Passware Kit Forensics yazılımı ile Gmail parolasına,
- Gmail parolası için kullanılan bellekten işleme ait kopya çıkaran Pmdump ve inceleme yazılımı olan Winhex yazılımları ile Yahoo parolasına,
- Yahoo parolası için kullanılan yöntem olan tüm bellek dökümü içinde parola arama işlemi ile Facebook parolasına,

erişmek mümkün olabilir.

B. Disk bazlı şifreleme sistemlerine ait parolalar

BitLocker, Truecrypt, PGP gibi yazılımlar kullanılarak, bilgisayarda kullanılan sabit diskler ve içinde bulunan dosyalar şifrelenebilmektedir. Ayrıca harici olarak kullanılabilen USB disklerde bulunan dosyalarda şifrelenebilir.

Şifrelenmiş bir sürücüye yeni dosya eklediğinde, bu yazılımlar dosyaları otomatik olarak şifrelemektedir.

Şifreleme işlemleri için uygulanan yöntemler arasında tamamen diskin şifrelenmesi, bir veya birkaç disk bölümünün (partition) şifrelenmesi, istenilen bir boyutta oluşturulacak sanal disk dosyasının (container) şifrelenmesi gibi değişik yöntemler kullanılmaktadır.

Hangi şifreleme yöntemi tercih edilirse edilsin şifreleme işlemi için ilgili yazılıma girilen parola belleğe aktarılmakta ve şifrelenmiş alan kullanıldığı sürece bellekte saklanmaktadır. Bu durumda belleğe erişebilir olmak parolaya erişebilmek anlamına gelmektedir. Bellek içinde bulunan bu parolaları elde edilebilmek için geliştirilmiş birçok yazılım bulunmaktadır.

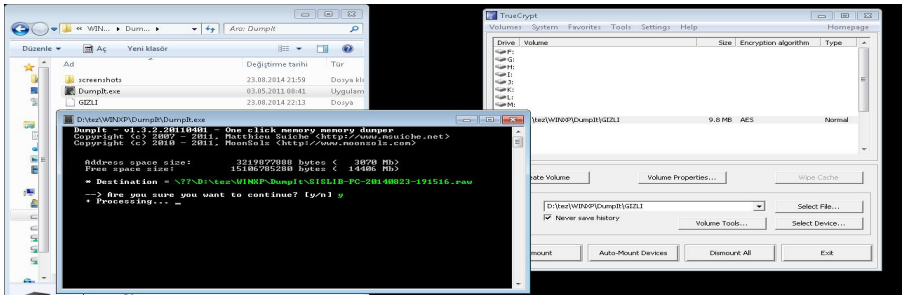
Şifreleme yazılımlarından olan TrueCrypt, açık kaynak kodlu olması, dosya ve disk şifreleme yapabilmesi, desteklediği algoritmalar ve esnek kullanımı gibi sebeplerle bilişim dünyasında sıklıkla kullanılmaktadır.[70] Truecrypt'de diğer şifreleme yazılımlarında olduğu gibi girilen parolayı şifreli olarak bellekte saklamaktadır. Bellekte bulunan şifrelenmiş parola, bellekten dışarıya çıkarılmak suretiyle şifrelenmiş alana erişilebilir. Bu kapsamda; Elcomsoft firması tarafından geliştirilmiş "Forensic Disk Decryptor"[71] yazılımı ile Truecrypt parolasının bellek içinden dışarı çıkarılması örneklenecektir.

Aşağıdaki ekran görüntüsünde Truecrypt parolası girilmek suretiyle oluşturulmuş sabit disk alanının bulunduğu sistemin bellek imajının oluşturulmakta olduğu görülmektedir. Bellek imajını oluşturmak için Dumpit yazılımı kullanılmıştır.

---

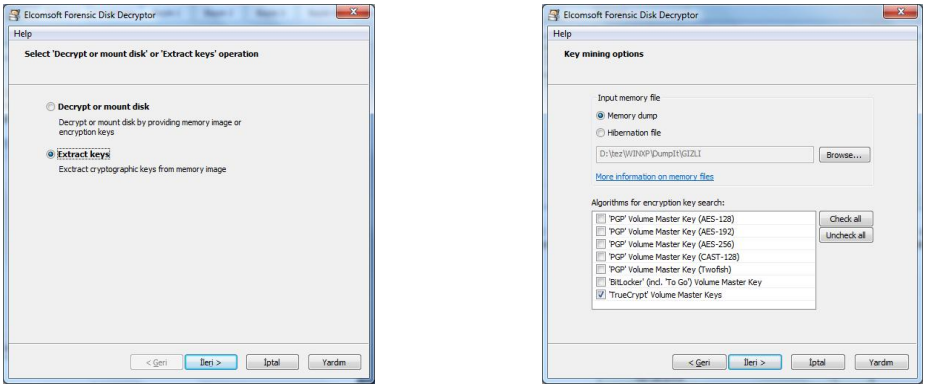
[70] TrueCrypt Kullanılarak Şifrelenmiş Dosyaların Parolalarını Bulma, http://blog.bga.com.tr/2012/03/truecrypt-kullanlarak-sifrelenmis.html, 18.03.2012, E.t. 12.09.2014

[71] Yazılımın son sürümüne (1.01.232) "http://www.elcomsoft.com/efdd.html" adresinden erişilebilir. E.t. 12.09.2014



Şekil 27 - Disk bazlı şifreleme sistemlerine ait parolalar - 1

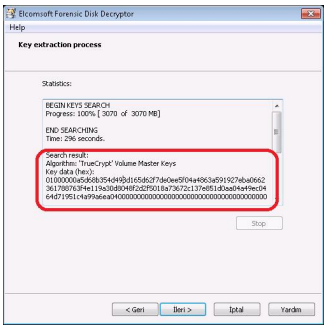
Forensic Disk Decryptor programı çalıştırılır, “Extract keys” ve ardından gelen ekrandan PGP, Truecrypt ve Bitlocker şifreleme yazılımlarından hangisi kullanılmış ise işaretlenir, oluşturulan bellek imaj dosyası programa girdi olarak verilir ve tarama işlemine başlanır.



Şekil 28 - Disk bazlı şifreleme sistemlerine ait parolalar - 2

Tarama işlemi sonrasında “’Truecrypt Volume Master Keys” alanı altında; kullanılan parolanın Heksadesimal (HEX) kodu görülecektir.[73]

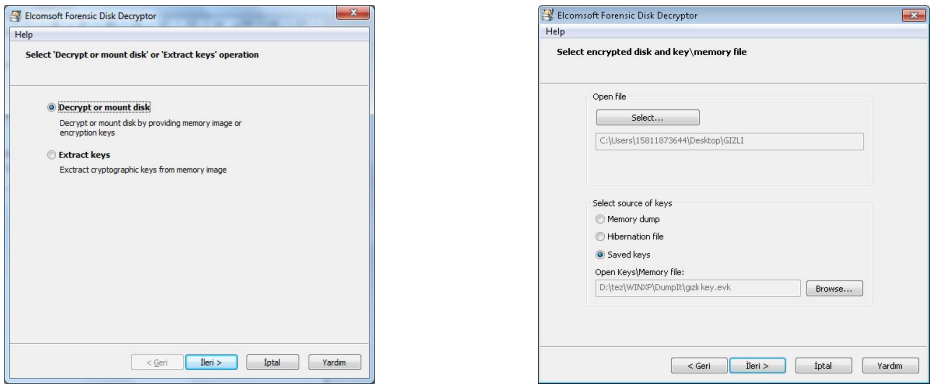
[73] Sattar B. Sadkhan Al MALIKY / Nidaa A. ABBAS, Multidisciplinary Perspectives in Cryptology and Information Security, sf.391,IGI Global,USA, 2014, https://books.google.com.tr/books?id=WgaXBQAAQBAJ, E.t. 12.10.2014



Şekil 29 - Disk bazlı şifreleme sistemlerine ait parolalar - 3

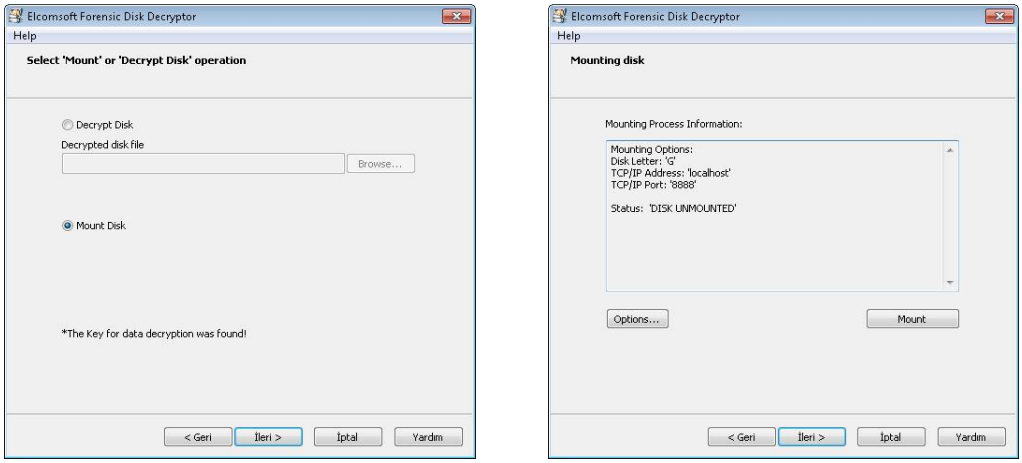
Bellek imajı içinden elde edilen bu Heksadesimal kodu “Master Key” olarak adlandırılmakta ve parola gibi kullanılabilir. Belleğin temizlenmesi (bilgisayar kapatılması veya yeniden başlatılması) ve oluşturulan (mount) şifrelenmiş alanın kapatılması (dismount) gibi durumlarda şifrelenen alanının tekrar oluşturması amacıyla kullanılabilir.

Bu işlem için izlenecek adımlar ise; yine aynı program başlatılır ve bu defa “Decrypt or mount disk” seçilir ardından gelen ekranda Truecrypt ile şifrelenmiş alan ve elde edilen Master Key dosyaları programa girdi olarak verilir.



Şekil 30 - Disk bazlı şifreleme sistemlerine ait parolalar - 4

Bu sayede yazılım şifrelenmiş alana ait parolanın HEX kodunu (Master Key) belleğe aktaracaktır. Bellekte bulunan HEX kodu vasıtasıyla şifrelenmiş alanda bulunan bilgiler isteğe bağlı olarak şifreli alan dışında başka bir dizine çıkarılabilir veya sanal bir disk olarak kullanılabilir. Aşağıdaki ekran görüntülerinde bu işlemler sırası ile gösterilmiştir.

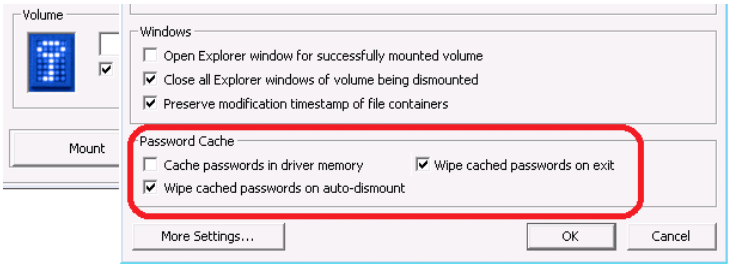


Şekil 31 - Disk bazlı şifreleme sistemlerine ait parolalar - 5

Truecrypt ile şifrelenmiş dosyanın, “Master Key” kullanılmak suretiyle sanal disk (Bu örnekte G: olarak tanımlanmıştır.) olarak oluşturulmuş hali ve şifreli alanda bulunan dosyalara erişilebildiği aşağıdaki ekran çıktısında görülmektedir.

Şekil 32 - Disk bazlı şifreleme sistemlerine ait parolalar - 6

BitLocker, PGP, TrueCrypt gibi şifreleme yazılımlarına girilen parolalar bellekte tutulduklarından, girilen parola bellek üzerinden gerçekleştirilebilecek saldırılara karşı savunmasızdır. TrueCrypt’de bu durum için bir koruma önlemi olarak “Settings - Preferences” ekranında Password Cache gurubunda yer alan “Wipe cached passwords on auto-dismount” ve “Wipe cached passwords on Exit” seçeneklerinin işaretlenmesi durumunda şifrelenmiş alan ile ilişki sonlandırıldığında (dismount) bellekte bulunan parolanın temizlenmesi sağlanacaktır.



Şekil 33 - Disk bazlı şifreleme sistemlerine ait parolalar - 7

Açık kaynak kodlu, ücretsiz ve oldukça da popüler olan şifreleme yazılımı TrueCrypt, Mayıs 2014 tarihinde web sitesinden yaptığı duyuruda, yazılımın geliştirilme çalışmalarının tamamen durdurduğunu belirtmiştir. Yazılımdaki önemli güvenlik açıklarının bir türlü kapatılamaması nedeniyle kullanıcılar açısından önemli risklerin oluştuğunu ve kullanıcıların yazılımı bilgisayarlarından kaldırmaları gerektiğini beyan etmiştir. Kullanıcılarına, Microsoft'un dahili şifreleme hizmeti vermesi nedeniyle TrueCrypt'e artık ihtiyaç kalmadığını ve Microsoft'un şifreleme yazılımı olan Bitlocker'ı kullanmaları tavsiye etmektedir.[74]

Şekil 34 - Disk bazlı şifreleme sistemlerine ait parolalar - 8

C. Windows oturum parolası

Günümüzde sistemlere karşı gerçekleştirilen saldırılar artmaktadır. Bunun paralelinde sızma testlerine (Penetration Test) verilen önem de gün geçtikçe artış göstermektedir. Sızma testlerinin kullanılan yöntemlerden birisi de Windows işletim sistemi kullanıcıların (özellikle etki alanı kullanıcılarının) hesap bilgilerinin elde edilmesidir.[75] Windows işletim sistemlerinde oturum açmak için girilen parolalar, oturum süresi boyunca bellek (RAM) üzerinde saklanmaktadır.

[74] WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues, http://truecrypt.sourceforge.net/, Mayıs 2014

[75] Ertuğrul BAŞARANOĞLU - TÜBİTAK BİLGEM, Bellekten Parolaların Elde Edilmesi - 1, https://www.bilgiguvenligi.gov.tr/microsoft-guvenligi/bellekten-parolalarin-elde-edilmesi-1.html, E.t. 14.09.2014

Son yıllarda bu bilgilerin elde edilmesi için yeni bir yöntem kullanılmaya başlanmıştır.[76] Bu yöntemde etki alanı sızma testlerinde (veya gerçekleştirilen bazı siber saldırılarda) RAM üzerinde kayıtlı bu bilgiler elde edilmeye çalışılmaktadır.

Kullanıcı bilgilerinin elde etme işlemine geçilmeden önce konu ile ilgili bazı önbilgiler verilecektir.

Yerel kullanıcılara ait hesap bilgilerinin (hesap adları ve hesaplara ait parolaların özetleri) elde edilmesi için C:\Windows\System32\config dizini altındaki SAM ve SYSTEM dosyaları kullanılmaktadır. Birçok son kullanıcı bilgisayarının bulunduğu etki alanı (domain) ortamlarında ise etki alanı kullanıcı hesaplarının bilgileri; SAM dosyası yerine etki alanı denetleyicisindeki (DC) NTDS.dit dosyasında depolanmaktadır. Bu dosyaya yetkili kullanıcı hesabı ile erişilmesi durumunda ise etki alanındaki tüm kullanıcıların parola özetleri elde edilebilmektedir. Bir kullanıcıya ait örnek hesap bilgisi aşağıdadır.

tubitak:1131:f26fb3ae03e93ab9c81667e9d738c5d9:47bf8039a8506cd67c524a03ff84ba4e

Bu kayıtta “f26fb3a.....” ile başlayan metin, kullanıcı parolasının LM ve NTLM özeti olmakta ve SAM veya NTDS.dit dosyasından elde edilmiştir. Yukarıdaki özet değeri kullanılarak - bir takım araçlarla veya internet üzerinden - çok kolay bir şekilde parolanın açık hali elde edilebilir. Ancak bu durum her zaman gerçekleşmeyebilmekte veya çok uzun zaman alabilmektedir.

Kurumsal ortamlarda genellikle son kullanıcı bilgisayarları için Windows işletim sistemi tercih edilmekte ve bilgisayarların kurulumunda aynı imaj kullanılmaktadır. Etki alanı sızma testlerinde (domain pentest) kullanılan yöntemlerden birisi, bir şekilde sızılan ve yüksek yetki elde edilen bir bilgisayardaki gömülü yerel yönetici hesabına (Built-in Administrator) ait bilgilerin (hesap adı ve parola) alınmasıdır. Sızılan bilgisayardan alınan bu bilgiler

[76] Fırat Celal ERDİK, Mimikatz ile Windows Sistemlerde Parolaları Açık Olarak Okuma, http://blog.bga.com.tr/2013/01/mimikatz-ile-windows-sistemlerde.html, E.t. 30.11.2014,

erişim sağlanabilen diğer bilgisayarlarda denenmektedir. Böylece aynı imajın kullanıldığı (ve/veya gömülü yöneticilere ait hesap bilgilerinin aynı olduğu) bilgisayarlarda yetkili kullanıcı hesabına sahip olunmaktadır. Kullanıcı hesaplarına ait parola özetlerini kullanılarak diğer bilgisayarlara erişim sağlanabilen bu yönteme Pass-the-Hash (PTH) adı verilir.[77] PTH yöntemi ile kullanıcı adı ve parola özeti kullanılarak giriş yapılabilecek bilgisayarların tespit edilmesine dair örnek bir durum aşağıdaki gibidir:

```
[+] 192.168.201.100:445|WORKGROUP - SUCCESSFUL LOGIN (Windows 5.1) 'administrator' :
'aad3b435b51404eeaad3b435b51404ee:b453cab43d3c46128e1735b897449df9'
[*] Username is case insensitive
[-] 192.168.201.52:445 SMB - [2/3] - |WORKGROUP - FAILED LOGIN (Windows 5.1) Administrator :
aad3b435b51404eeaad3b435b51404ee:b453cab43d3c46128e1735b897449df9 (STATUS_LOGON_FAILURE)
[*] 192.168.201.157:445 SMB - [1/3] - Starting SMB login bruteforce
[*] 192.168.201.177:445 SMB - [1/3] - Starting SMB login bruteforce
[-] 192.168.201.177 - This system allows guest sessions with any credentials, these instances will not be reported.
[-] 192.168.201.177:445 SMB - [1/3] - |WORKGROUP - FAILED LOGIN (Windows 7 Professional 7601 Service Pack 1) Administrator :
(STATUS_LOGON_FAILURE)
[-] 192.168.201.177:445 SMB - [2/3] - |WORKGROUP - FAILED LOGIN (Windows 7 Professional 7601 Service Pack 1) Administrator :
Administrator (STATUS_LOGON_FAILURE)
[*] Auth-User: "Administrator"
[+] 192.168.201.177:445|WORKGROUP - SUCCESSFUL LOGIN (Windows 7 Professional 7601 Service Pack 1) 'Administrator' :
'aad3b435b51404eeaad3b435b51404ee:b453cab43d3c46128e1735b897449df9'
[*] Auth-User: "administrator"
[+] 192.168.201.177:445|WORKGROUP - SUCCESSFUL LOGIN (Windows 7 Professional 7601 Service Pack 1) 'administrator' :
'aad3b435b51404eeaad3b435b51404ee:b453cab43d3c46128e1735b897449df9'
[*] Username is case insensitive
[*] 192.168.201.178:445 SMB - [1/3] - Starting SMB login bruteforce
[*] 192.168.201.200:445 SMB - [1/3] - Starting SMB login bruteforce
[-] 192.168.201.200 - This system allows guest sessions with any credentials, these instances will not be reported.
[-] 192.168.201.200:445 SMB - [1/3] - |WORKGROUP - FAILED LOGIN (Windows 5.1) Administrator :  (STATUS_LOGON_FAILURE)
[-] 192.168.201.178 - This system allows guest sessions with any credentials, these instances will not be reported.
[-] 192.168.201.178:445 SMB - [1/3] - |WORKGROUP - FAILED LOGIN (Windows 5.1) Administrator :  (STATUS_LOGON_FAILURE)
[*] Auth-User: "Administrator"
[+] 192.168.201.200:445|WORKGROUP - SUCCESSFUL LOGIN (Windows 5.1) 'Administrator' : 'Administrator'
[-] 192.168.201.178:445 SMB - [2/3] - |WORKGROUP - FAILED LOGIN (Windows 5.1) Administrator : Administrator (STATUS_LOGON_FAILURE)
[*] Auth-User: "administrator"
[+] 192.168.201.200:445|WORKGROUP - SUCCESSFUL LOGIN (Windows 5.1) 'administrator' : 'Administrator'
```

Şekil 35 - Pass-the-Hash (PTH) yöntemi test ekranı

Parolaların ortak olarak kullanılması, aynı parolanın (gerekli olmamasına rağmen) birçok kritik sistemde ortak olarak kullanması ve aynı imaj ile kurulumu yapılan bilgisayarların yetkili kullanıcı şifrelerinin değiştirilmemesi bir güvenlik zaafiyetidir.

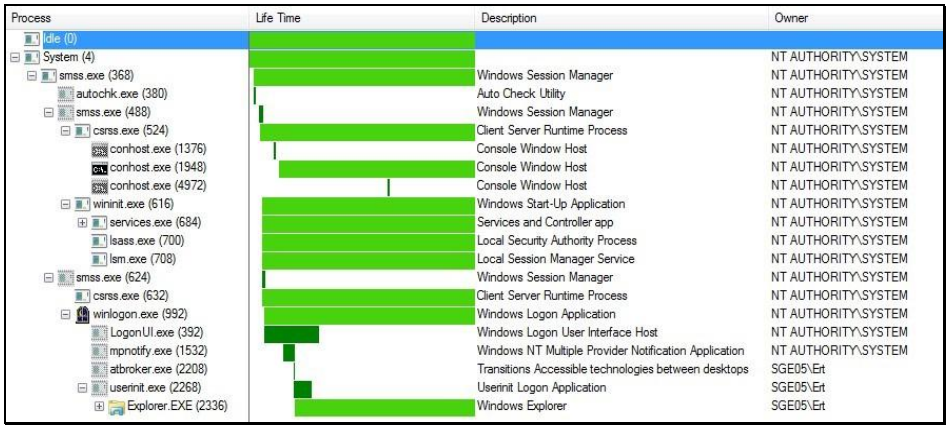
Bazı durumlarda parolanın özeti yeterli olmayabilir. Örneğin, etki alanı parolası ile kimlik doğrulanabilen bir başka sisteme (Outlook web maile, veritabanı sistemlerine, VPN sistemlerine, vs.) bağlanılmaya çalışıldığı durumlarda parola özetinin elde edilmesi yetersizdir. Bu gibi durumlarda parolanın kendisi (açık hali - plaintext) gerekmektedir.

[77] Jesper M. JOHANSSON / Steve RILEY, Protect Your Windows Network: From Perimeter to Data, sf.332. Pearson Education Inc, USA, 2005, https://books.google.com.tr/books?id=yZX2uAoAagwC, E.t. 02.10.2014

Windows İşletim Sisteminde Oturum Açma İşlemi İle İlgili Prosesler[78]

Windows işletim sisteminde çalışan bir proses çekirdek modu (kernel mode) ve kullanıcı modu (user mode) olmak üzere iki farklı modda çalışabilir. Çekirdek modunda işletim sistemi bileşenleri çalışırken, uygulamalar kullanıcı modunda çalışmaktadır. İşletim sistemi bileşenleri yüklendikten sonra, kullanıcı modu ve etkileşimli oturum açma (interactive logon) işlemi başlamaktadır.

Kullanıcıya ait bu modda çalışan ilk proses Smss.exe prosesidir. Ana Smss prosesi her zaman sıfır numaralı etkileşimsiz oturumda bulunur ve başlatılacak olan her bir etkileşimli oturum için bir adet kopya Smss prosesi oluşturur. Oluşturulan kopya Smss prosesi ilgili oturuma ait Csrss ve Winlogon proseslerini oluşturup kendi çalışmasını sonlandırır. Aşağıdaki resimde de gösterildiği üzere PID değeri 368 olan Smss prosesi kendisinin iki kopyasını oluşturmuştur. 488 ve 624 PID değerlerine sahip olan kopya Smss prosesleri başka prosesleri oluşturduktan sonra sonlanmıştır. Prosesler arasındaki bu ilişki aşağıdaki ekran görüntüsünde görülmektedir.



Şekil 36 - Oturum açma işlemi ile ilgili prosesler - 1

Oturum işlemleri ile ilgili en önemli prosesler aşağıdaki gibidir:

[78] Onur Samet ÖZER / Ertuğrul BAŞARANOĞLU- TÜBİTAK BİLGEM; Windows İşletim Sisteminde Oturum Açma İşlemi – Winlogon, http://www.bilgiguvenligi.gov.tr/microsoft-guvenligi/windows-isletim-sisteminde-oturum-acma-islemi-winlogon.html, E.t. 26.11.2014

Smss.exe (Session Manager Subsystem): Windows işletim sisteminin başlangıç prosesidir. Çevresel değişkenlerin oluşturulması, belirli (HKLM\System\CurrentControlSet\Control\Session Manager\SubSystems altında belirtilen) alt sistemlerin başlatılması, bir takım proseslerin (csrss, wininit, winlogon) başlatılması en temel görevlerindendir.

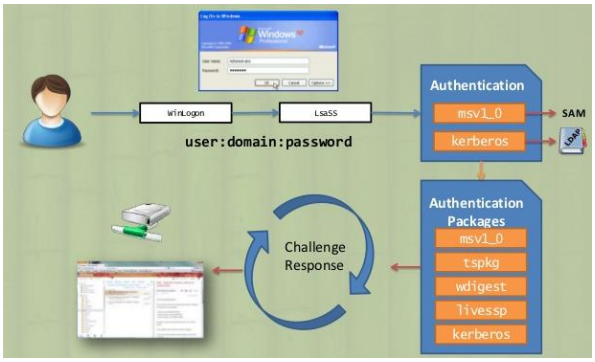
Csrss.exe (Client/Server Runtime Subsystem): Temel olarak, kullanıcı modunda gerçekleşen birçok görevin (task), çekirdek moduna erişmemesini (sistem çağrısının gerçekleştirilmemesini) sağlar. Thread ve Win32 konsolunun (metinsel arayüz, API kullanımı ile kullanıcı dostu arayüze sahip olunabilir) kontrolünden sorumlu olan prosestir.

Winlogon.exe: İşletim sisteminde oturum açılması ve kapatılması, LogonUI prosesinin oluşturulması, beklenmedik bir şekilde sonlanan LogonUI prosesinin yeniden başlatılması, kimlik doğrulama işlemi için LSASS prosesinin çağırılması, kullanıcı şifresinin değiştirmesi, iş istasyonunun (workstation) kilitlenmesi ve kilitli olan iş istasyonunun tekrardan açılması gibi işlemlerden sorumludur. Winlogon bu görevleri yerine getirirken, yetkisi olmayan başka bir prosesin bu işlemleri okuyamaması, değiştirememesi, kısaca araya girememesini sağlar. Winlogon SYSTEM haklarıyla çalışır, bu sebeple sıfır numaralı oturumda çalışmamaktadır. Windows ortamında etkileşimli her bir oturum için bir adet Winlogon oluşturulur.

LogonUI.exe: Kimlik bilgisi sağlayıcılarının (credential provider) yüklenmesinden, oturum değişimi (açma ve kapama işlemleri sırasında) ve etkileşimli oturum açma grafik ara yüzünün gösterilmesinden sorumlu prosestir.

LSASS.EXE (Local Security Authority Subsystem Service): Kullanıcıların oturum açma işlemleri sırasında kimlik bilgilerini doğrulayan, parola değişikliklerinin gerçekleştirilmesinde görevli olan, kullanıcının yerel güvenlik ilkelerine (security policy) uymaya zorlayan, kullanıcı haklarına göre token oluşturan, göreviyle ilişkili bir olay olduğunda bu olayı Olay Günlüklerine (Event Viewer) yazan prosestir.

Oturum açma işlemini tek bir cümleyle şu şekilde özetleyebiliriz: Oturum açmak için yazılan kullanıcı adı ve parola bilgisi; belleğe (RAM) yüklenen ve kimlik doğrulama işleminde görev alan bazı kütüphane dosyalarında şifreli olarak saklanmakta ve bu bilgiler kimlik doğrulama işlemleri sırasında işlenmektedir. Aşağıdaki resim oturum açma işlemini özetlemektedir.



Şekil 37 - Oturum açma işlemi ile ilgili prosesler - 2

1. Wce aracı ile parolaya erişim

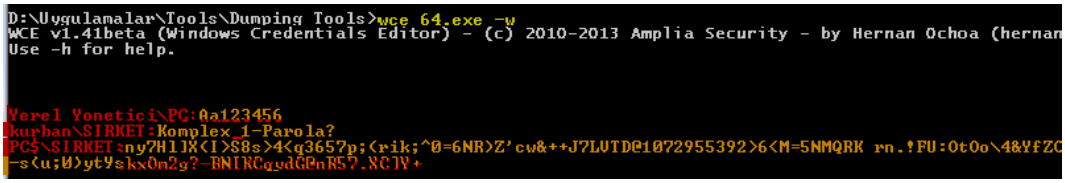
WCE[79] aracı temel olarak RAM'de bulunan kimlik doğrulama paketlerindeki (authentication packages) kimlik bilgilerini (şifreli parola ve parola özetlerini, kullanıcı adı gibi) okumakta, parolayı şifreleyen şifreleme anahtarını ve şifreli parolayı (parola özetini) elde etmektedir.[81]

WCE aracının kullanılması ile ilgili bir senaryo şu şekildedir: SIRKET etki alanındaki bir bilgisayarda, "Kurban" adlı bir etki alanı kullanıcısı ve "Yerel Yonetici" adlı yerel kullanıcı oturumları açık durumdadır. Bu senaryoda, RAM üzerinde bu iki kullanıcının oturum açma işlemi sırasında kullanılan kimlik doğrulama paketlerinden (authentication packages) parola bilgilerinin şifresi

[79] Yazılımın son sürümüne (1.3) "http://www.ampliasecurity.com/" adresinden erişilebilir, E.t 27.12.2014

[81] Georgia WEIDMAN, Penetration Testing: A Hands-On Introduction to Hacking, sf.213-214, No Starch Press Inc, USA, 2014, https://books.google.com.tr/books?id=4b1S0U1fIVAC

çözülerek alınabilir. Bu işlemlere ait ekran görüntüsü ve WCE aracının komut satırından kullanımı aşağıda gösterilmiştir.[82]



Şekil 38 - Wce aracı ile parolaya erişim

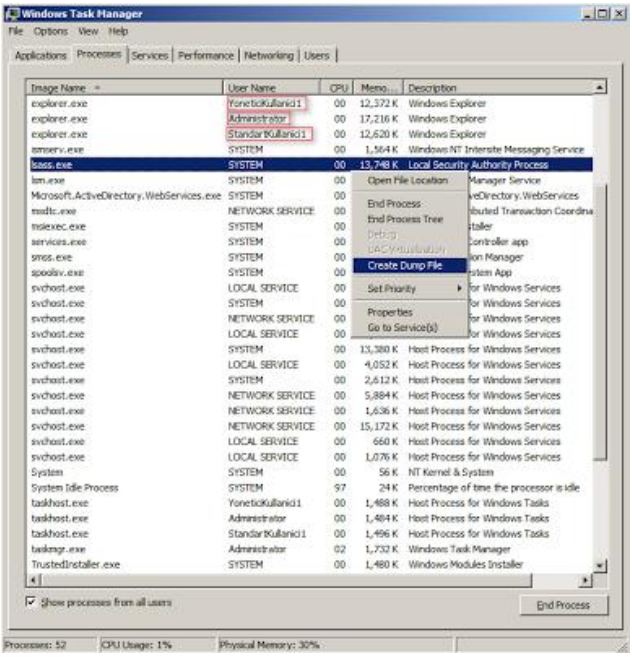
2. Procdump ve Mimikatz araçları ile parolaya erişim

"Mimikatz"[83] içerisinde kimlik bilgileri barındıran LSASS.exe prosesi içinden logon olmuş kullanıcıların parolalarını elde edebilmektedir. Aşağıdaki ekran görüntüsünde; Şirket etki alanında bulunan bir bilgisayarda oturum açan 3 kullanıcının (StandartKullanici1, YoneticiKullanici1, Administrator) parola bilgileri elde edilecektir. Öncelikle bilgisayardan LSASS prosesinin kopyası (dump) dosyası oluşturulur. [84]

[82] Fırat Celal ERDİK; Mimikatz ile Windows Sistemlerde Parolaları Açık Olarak Okuma http://blog.bga.com.tr/2013/01/mimikatz-ile-windows-sistemlerde.html, E.t. 30.08.2014

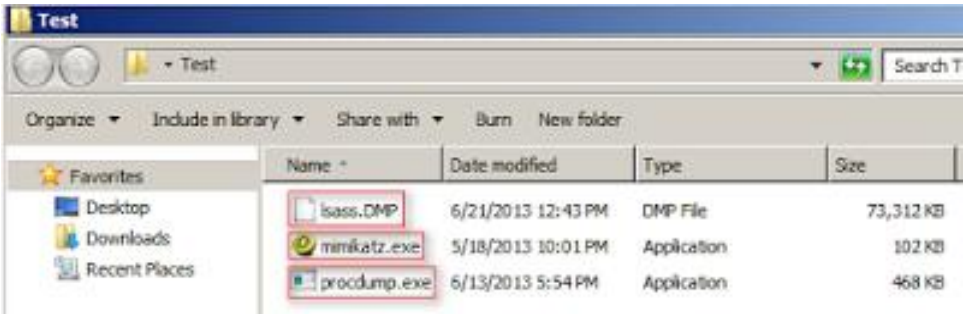
[83] Yazılımın son sürümüne (2.0) https://github.com/gentilkiwi/mimikatz/releases/ adresinden erişilebilir, E.t 01.01.2015

[84] A.g.e. 80



Şekil 39 - Proses kopyası oluşturma ekranı

Dump dosyası, aynı mimariye sahip başka bir bilgisayara taşınır. Taşıma işleminin sebebi antivirüs programları veya engelleyici sistemlerin mimikatz/wce gibi araçlarının çalıştırılmasını engellemesidir. Bu örnekte Windows Server 2008 R2 bilgisayarlar sanal ortamda kullanılmış ve mimikatz'ın çalışmasını engelleyen tüm sistemler devre dışı bırakılmıştır. "Procdump"[85] ve "Mimikatz"[86] uygulamaları ile birlikte dump dosyası sanal bilgisayarda bir klasöre konulur.



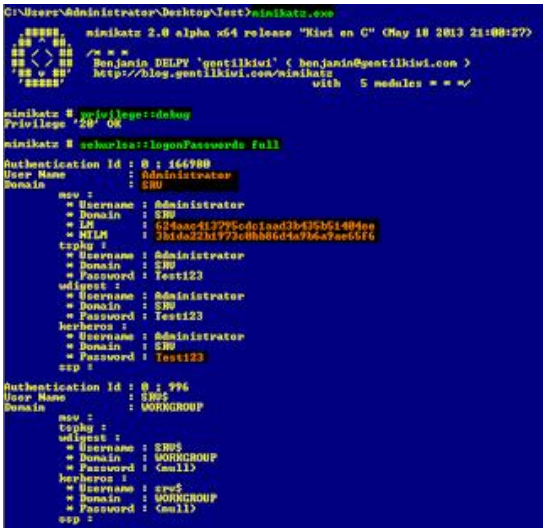
Şekil 40 - Procdump, Mimikatz ve Dump dosyaları

[85] Mark RUSSINOVICH; Microsoft Technet Kitaplığı - ProcDump v7.01, http://technet.microsoft.com/en-us/sysinternals/dd996900.aspx, E.t. 11.09.2014

[86] https://github.com/gentilkiwi/mimikatz, E.t. 11.09.2014

Mimikatz; sanal sunucuda çalıştırılmış ve sadece oturumu açık olan Administrator kullanıcısının parolasının (Test123) elde edilebildiği aşağıdaki ekran çıktısında görülmektedir. Çalıştırılan komutlar aşağıdaki gibidir.

- Mimikatz
- privilege::debug
- sekurlsa::logonPasswords full



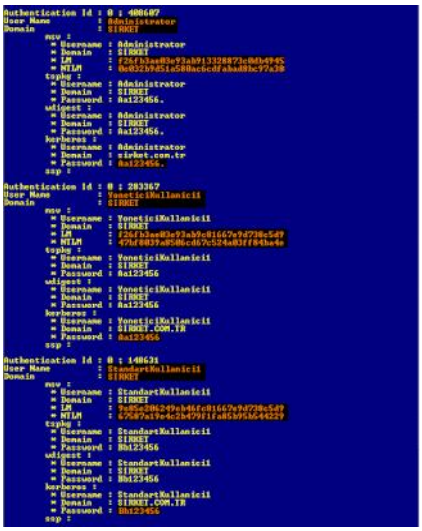
Şekil 41 - Mimikatz çalıştırma ekranı

Dump bilgisi alınan bilgisayarda oturum açmış olan kullanıcıların (StandartKullanici1, YoneticiKullanici1, Administrator) parola bilgilerini elde etmek için sanal bilgisayardaki LSASS prosesine, dump bilgisi alınan LSASS prosesi yazılacaktır. Daha sonra da yukarıdaki örneğe benzer olarak LSASS prosesine DLL enjeksiyonu gerçekleştirilerek proseste kayıtlı olan parola bilgileri alınacaktır.[87] Bu amaçla, komut satırından hazırlanan klasöre gelinerek;

- procdump -accepteula -ma lsass.exe lsass.dmp
- mimikatz.exe
- sekurlsa::minidump lsass.dmp
- sekurlsa::logonPasswords

komutları çalıştırılır ve 3 kullanıcıya ait parolalarnın açık ile birlikte LM ve NTLM özetleri elde edilebilir.

[87] David LLADRO; Plaintext passwords with Procdump and Mimikatz Alpha, http://www.securityartwork.es/2013/11/04/plaintext-passwords-with-procdump-and-mimikatz-alpha/?lang=en , E.t. 04.11.2014



Şekil 42 - LSASS prosesine DLL enjeksiyonu

Bunun yanında parolaların açık olarak elde edilebilmesi için sadece RAM'deki bilgilerin alınması yeterli olamayabilmektedir. Bu durumun sebebi tam olarak bilinmese de Windows işletim sisteminin önbellek (cache) mekanizmasından kaynaklandığı tahmin edilmektedir. Canlı bir bilgisayarda bir prosesin (LSASS gibi) minidump'ı alınırken RAM ve pagefile içerisindeki bilgiler beraber elde ediliyorken, sadece RAM üzerinde ise bu prosese ait tüm bilgiler elde edilemeyebilmektedir. Bu önbellek mekanizmasından dolayı, adli analizlerde (forensics) kullanılan raw halindeki RAM dump içerisinden parola bilgisinin elde edilemediği düşünülmektedir.[88]

Kurumsal bir etki alanı (domain) ortamında, sızılan bir bilgisayardaki RAM üzerinden kullanıcı parolalarının açık olarak elde edilmesini amacıyla yapılan testlerde; Kullanıcı Değiştirme (Switch User), Oturum Bağlantısının Düşmesi (Disconect Your Session Immediately), Uzak Masaüstü Bağlantısını Kesme (Disconnect) ve bazı durumlarda Oturumu Kapatma (Log off) seçeneklerinde de parolaların elde edilmiştir.[89]

[88] Ertuğrul BAŞARANOĞLU - TÜBİTAK BİLGEM, Bellekten Parolaların Elde Edilmesi - 2, https://www.bilgiguvenligi.gov.tr/microsoft-guvenligi/bellekten-parolalarin-elde-edilmesi-2.html, E.t. 14.09.2014

[89] A.g.e. 85

Bu işlemler Exchange Server rolüne sahip bir sunucuda gerçekleştirilirse, mail yollamak için bu sunucudan DC'ye giden tüm kullanıcıların parolaları elde edilebilir. Bu sebeple, DC'ye erişimlerin yanında Exchange sunucuya erişimler de önem arz etmektedir.

Ç. Komut satırından girilen komutlar

Komut satırı, kullanıcı ile işletim sistemi arasında doğrudan iletişim sağlayan ayrı bir yazılım programıdır. Grafik ara yüzü olmayan komut satırı arabirimi ile karakter tabanlı uygulamalar ve hizmet programları çalıştırılmaktadır.

Komut satırı kullanarak, sık yapılan görevleri otomatikleştirmek üzere toplu iş dosyaları (komut dosyaları) oluşturabilmekte ve düzenlenebilmektedir. Örneğin, kullanıcı hesaplarının oluşturulması veya yapılan yedeklemelerin yönetimini otomatikleştirmek için komut dosyaları kullanılabilir.[90]

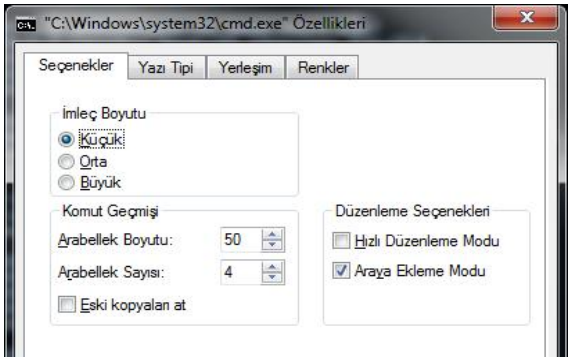
Linux ve Unix sistemlere girilen komutlar "$HOME/.sh_history" dosyasında ve varsayılan olarak geçmişe dönük olarak 128 komutu saklamaktadır.[91] Bu sistemlerde bulunan Terminal penceresi kapatılıp açıldığında dahi geçmişte komutlara bu dosya üzerinden erişmek mümkündür. Windows sistemlerde ise komut geçmişi herhangi bir dosyada saklanmamaktadır. Sadece açık olan komut satırı ekranından geçmiş komutlara erişilmektedir.

Windows işletim sistemlerinde bellek üzerinde yapılacak inceleme ile komut satırından girilen komutları görmek mümkündür. Ancak gerilen komutların sayısı, komut istemi özelliklerinde bulunan "Komut Geçmişi" sekmesi altında belirlenen değer kadardır. Varsayılan olarak Windows işletim sistemleri 50 komut saklamaktadır.

---

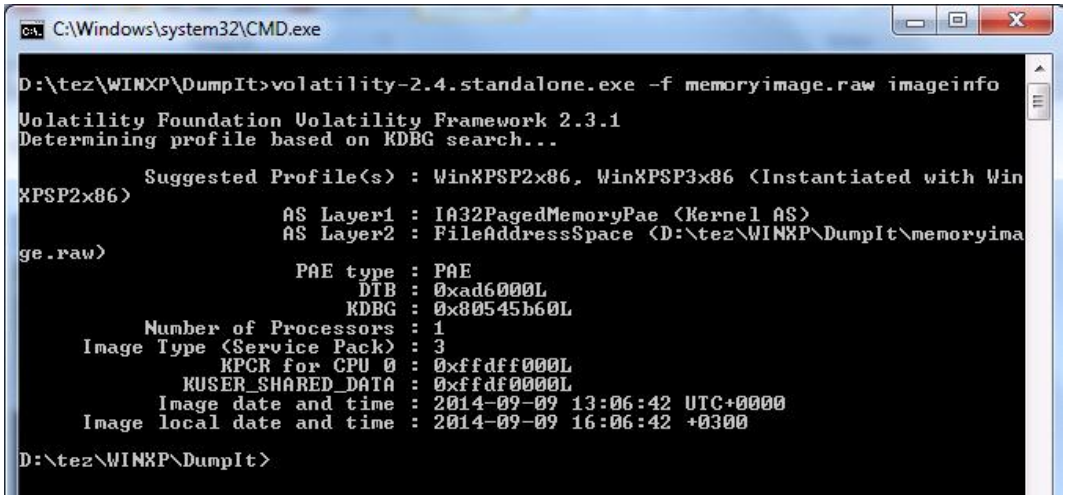
[90] Microsoft Technet Kitaplığı - Komut kabuğuna genel bakış, http://technet.microsoft.com/tr-tr/library/cc737438%28v=ws.10%29.aspx, E.t. 15.07.2014

[91] Anatole OLCZAK, The Korn Shell: Unix and Linux Programming Manual, Volume 1, sf.333, Pearson Education Limited, UK, 2001, http://books.google.com.tr/books?id=dCIJv94vXUMC, E.t. 16.07.2014



Şekil 43 - Komut geçmişi varsayılan ayarları

Windows sistemlerde bellek incelemesi ile eski komutlar görülmek istendiğinde sistemin bellek imajı oluşturulmalıdır. Ardından "volatility"[92] yazılımı yardımıyla öncelikle bellek imajının ait olduğu sistemin özelliklerini bulunmalıdır. Aşağıdaki ekran görüntüsünde sisteme ait bilgilerin öğrenilmesi için girilecek komut gösterilmiştir.



Şekil 44 - Volatility ile sistem özelliklerinin tespiti

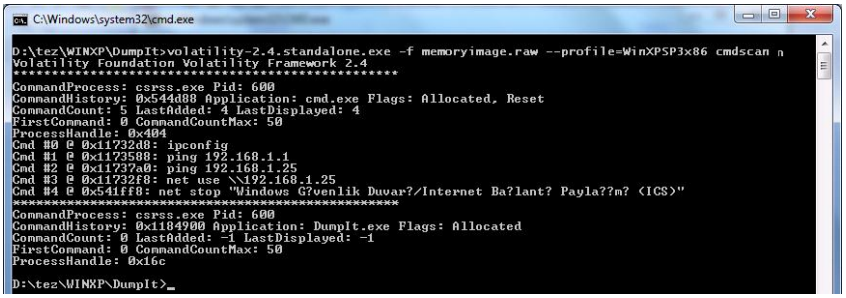
İmaj dosyası incelendiğinde, sistemin Windows XP SP3 olduğu görülmektedir. Ardından volatility aracı "cmdscan"[93] parametresi ile çalıştırıldığında önceden girilen komutlar görülebilir. Komutun örnek kullanımı aşağıdadır.

---

[92] Yazılımın son sürümüne (2.4) https://code.google.com/p/volatility adresinden erişilebilir, E.t. 28.12.2014

[93] https://code.google.com/p/volatility/wiki/CommandReference21#cmdscan, E.t. 17.09.2014

volatility-2.4.standalone.exe -f memoryimage.raw --profile=WinXPSP3x86 cmdscan



Şekil 45 - Volatility ile komut geçmişi

Verilen komut sonrasında çıkan sonuç incelendiğinde;

- “Cmd #0 @ 0x11732d8 : ipconfig” satırından; bellek dökümü alınan sistemi kullanan kişinin öncelikle IP numarasını öğrenmek isteği,
- “Cmd #1 @ 0x1173588: ping 192.168.1.1” satırından; muhtemel ağ geçidi olan cihaza ping attığı,
- “Cmd #2 @ 0x11737a0: ping 192.168.1.25” satırından; yerel ağda bulunan 192.168.1.25 numaralı cihaza ping atma işlemi yaptığı,
- "Cmd #4 @ 0x541ff8: net stop "Windows G?venlik Duvar?/Internet Ba?lant? Payla??m? (ICS)" satırından girilen komut ise bilgisayarın güvenlik duvarı servisini durdurmakta ve bir güvenlik zafiyeti oluşturmaya çalıştığı görülmektedir.

Ekranında açık durumda hiçbir pencere bulunmayan bir bilgisayarın, belleği üzerinde yapılacak incelemede komut satırından girilen komutlara bu şekilde ulaşılabilir.[94] Yapılan inceleme adli veya idari bir konuda ise bu bilgiler olayın hakkında yapılacak rapor için önemli bulgular verebilir.

[94] Richard M. STEVENS / Eoghan CASEY, Digital İnvestigation 7 (2010) Extracting Windows command line details from physical memory, sf.57-63, Digital Forensics Research Conference Paper 2010, http://dfrws.org/2010/proceedings/2010-307.pdf, E.t. 18.11.2014

D. İnternet geçmişi

Sosyal ağlar (Facebook, Twitter, İnstagram, ...), anlık mesajlaşma programları (Skype, Yahoo Messenger, Facebook Chat, ..), e-posta servisleri (Gmail, Yahoo, Outlook), uçtan uca (peer to peer) paylaşım programları (E-mule, İmesh, Shareaza, ..), bulut bilişim teknoloji uygulamaları (Google Mail, Apple MobileMe, Ubuntu One, Picasa, Flickr, Google Docs, Google Drive,), internet gezgini programları (Google Chrome, İnternet Explorer, Mozilla Firefox) gibi internet erişimi vasıtasıyla kullanılan hizmet, program ve uygulamalar hakkında ki bilgilere bellek incelmesi ile elde edilebilir.

Jadsoftware firması tarafından geliştirilmiş olan Internet Evidence Finder yazılımı[95], 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 kullanılabilir.[96] İnternet Evidence Finder yazılımı kullanılarak yapılan analizlerde;

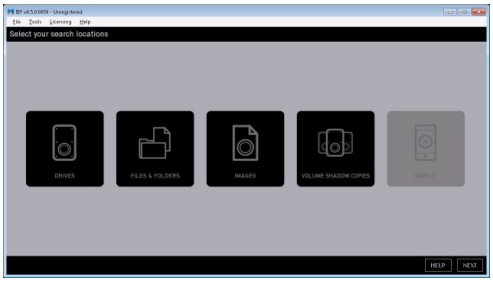
- Bulut Bilişim İzleri
- Anlık Mesajlaşma İzleri
- Medya İzleri
- Mobil Cihaz Yedekleme Dosyaları
- P2P Dosya Paylaşım Ortamları
- Webmail İncelemeleri
- Web Aktiviteleri
- Web Sayfası Kurtarma
- Doküman Verileri
- Windows İşletim Sistemi Verileri

[95] Yazılımın son sürümüne (6.5) "http://www.magnetforensics.com/mfsoftware/internet-evidence-finder" adresinden erişilebilir, E.t 01.01.2015

[96] Ömer ERTÜRK, RAM İmajı Alınması ve Analizi İle Erişilebilecek Bilgiler, http://omererturk.wordpress.com/, 1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu Sunumu, E.t. 12.11.2014

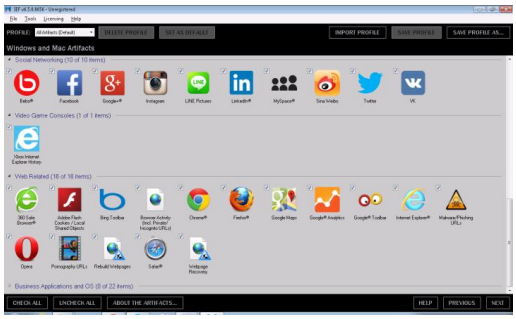
- E-posta Uygulamaları
- Anlık Mesajlaşma Uygulamaları

bilgilerine ulaşılabilir. Yazılımın Demo sürümü ile yapılan taramalarda her bir başlık için 20 adet sonuç görüntülenebilmektedir. Yazılım çalıştırıldığında tarama yapılabilecek seçeneklerin bulunduğu ekran gelmektedir. Bu ekranda sabit disk, dosya, klasör, önceden oluşturulmuş imaj dosyaları, sabit disk bölümlerine ait kopya dosyaları üzerinde tarama yapılabildiği görülmektedir.



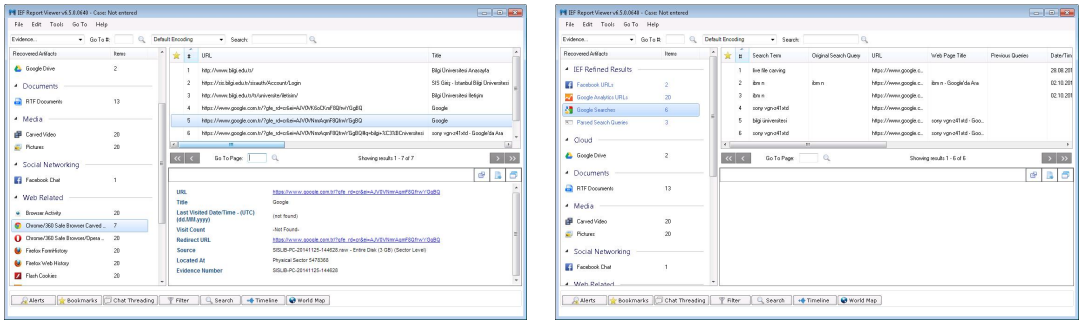
Şekil 46 - İnternet geçmişi - 1

İncelenecek sisteme ait bellek imaj dosyası yazılıma girdi olarak verildiğinde, tarama yapılacak alanların seçileceği aşağıdaki ekran gelmektedir. İlgili alanlar seçilir, sonuçların kaydedileceği dizin belirlenir ve tarama işlemi başlanır.



Şekil 47 - İnternet geçmişi - 2

Ardından gelen ekranda tarama işlemi tamamlandığında seçimi yapılan alanlar ile ilgili sonuçlar görüntülenir. Aşağıdaki ekran çıktıları incelendiğinde inceleme işlemi yapılan bilgisayar ile ziyaret edilen site bilgileri ve google arama motorunda yapılan sonuçlar görülmektedir.

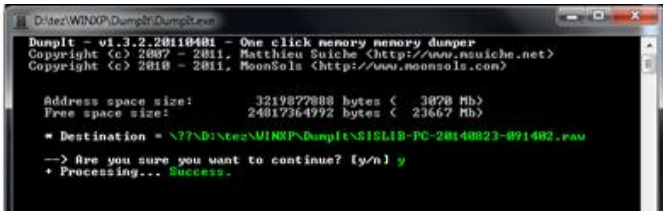


Şekil 48 - İnternet geçmişi - 3

E. Ekran görüntüsü

Bu bölümde bellek imajından bilgisayarda oturum açmış kullanıcılara ait ekran görüntüsünü (screenshot) elde etme aşamaları ayrıntılı olarak incelenecektir.

Öncelikle DumpIt[97] aracı ile sistem ait bellek imaj dosyası oluşturulur.



Şekil 49 - Dumpit ile bellek imajı oluşturma ekranı

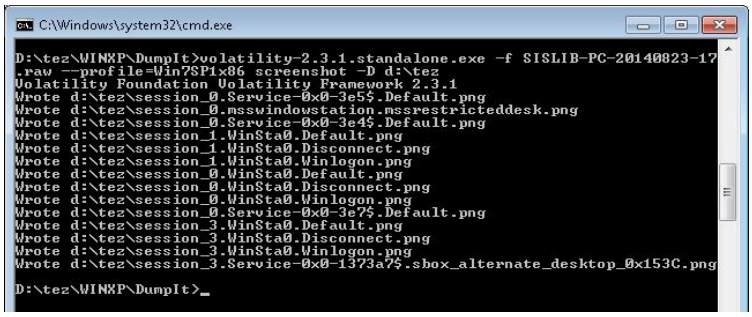
Ardından volatility aracına screenshot parametresi verilerek ekran görüntüsü (wire-frame diagram) elde etme işlemi başlatılır.[98]

volatility-2.3.1.standalone.exe -f SISLIB-PC-20140823-091402.raw
screenshot -D D:\tez\

---

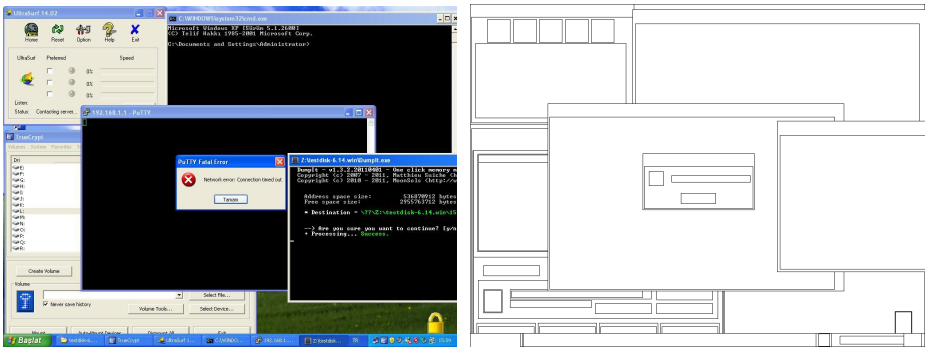
[97] Yazılımın son sürümüne (1.3.2) "www.moonsols.com/2011/07/18/moonsols-dumpit-goes-mainstream" adresinden erişilebilir, E.t. 12.09.2014

[98] Volatility 2.3.1 (Mac OSX and Android ARM), http://www.volatilityfoundation.org/#!23/c173h, E.t. 12.09.2014



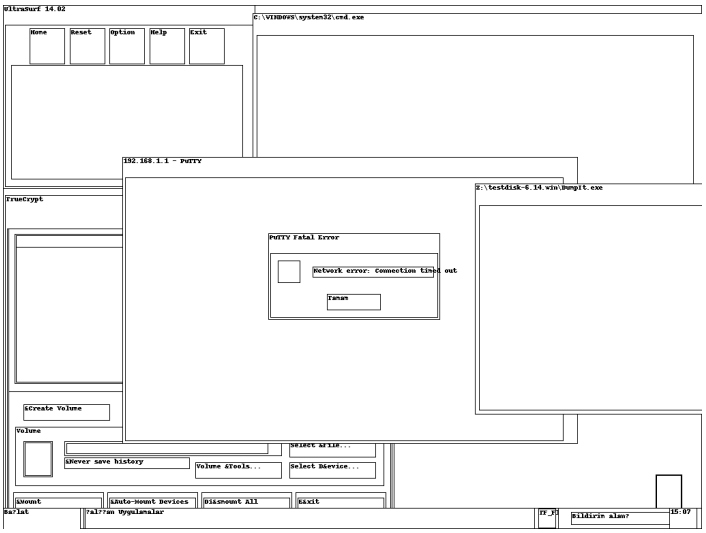
Şekil 50 - Volatility ile ekran görüntüsü elde etme

Volatility aracı bulduğu sonuçları –D parametresi ile belirtilen dizine çıkaracaktır. Bu sayede imaj oluşturma anında ekran da bulunan işlemlere ait yaklaşık pencere görüntüsü elde edilir. Ayrıca Windows Vista, Windows 7 gibi çoklu oturum açma imkânı sağlayan işletim sistemlerinde; oturumu açık olan kullanıcılar veya oturumu kilitlenmiş diğer kullanıcıların ekran görüntülerine de erişmek mümkün olabilmektedir. Ekran görüntülerinin bulunduğu dizinde bulunan session_1 ilk kullanıcıya ait ekran görüntüsünü, session_2 ise diğer bir kullanıcıya ait ekran görüntüleridir.



Şekil 51 - Volatility 2.2 sürümü ile ekran görüntüsü sonuçları

Yukarıdaki ekran görüntüleri Volatility aracının 2.2 sürümü ile oluşturulmuştur. 2.3 versiyonu ile birlikte pencerelere ait başlık bilgilerinin de görüntüleme imkânı sağlanmıştır.



Şekil 52 - Volatility 2.3 sürümü ile ekran görüntüsü sonuçları

Bu görüntü 2.3 versiyonu ile oluşturulmuş ve saat 15:07'de komut satırının açık ve Putty, Truecrypt, Ultrasurf gibi programların çalıştırılmış olduğu görülmektedir.

Bu bilgiler adli analiz açısından sistemin zamanın bilinmesi ve çalışan programların tespit edilebilir olması açısından önemlidir. Geniş bir adli analiz yapılması durumunda; Timeline analizi için önemli bir referans noktası da olabilecektir.

Volatility geliştiricileri tarafından; hala bellekten ekran görüntüsü elde etme alanında yapılması gereken bazı işlerin bulunduğu, etiket düğmeleri, araç çubukları, düzenleme kutuları, görüntülenen metinler gibi diğer özelliklerinde volatility'e de dahil edilebileceği ancak bu ilave özelliklerin renkli olmasının beklenmediği belirtilmektedir.[99] Ancak bu özellikler Ağustos 2014 tarihinde yayımlanan 2.4 sürümüne de dahil edilmemiştir.

[99] MoVP 4.2 Taking Screenshots from Memory Dumps, http://volatility-labs.blogspot.com/2012/10/movp-43-taking-screenshots-from-memory.html, E.t. 11.10.2014

F. Kayıt defteri bilgilerine erişim

Kayıt defteri; işletim sisteminde bulunan donanımlar, yüklü programlar, ayarlar ve bilgisayarınızdaki tüm kullanıcı hesaplarının profilleri ile ilgili önemli bilgileri içeren bir veritabanıdır. İşletim sistemi kayıt defteri bilgilerine sürekli başvurmaktadır.[100]

Kayıt defteri düzenleyicisi (regedit), ileri düzey kullanıcılar için tasarlanmış bir araçtır. Bilgisayarınızda bir değişiklik yaptığınızda (örneğin, yeni program yükleyerek, kullanıcı profili oluşturarak veya yeni donanım ekleyerek) işletim sistemi bu bilgilere başvurur ve ilgili alaları güncelleştirir. Kayıt defteri düzenleyicisi; kayıt defteri klasörlerini, dosyalarını ve her kayıt defteri dosyasının ayarlarını göstermektedir.

Normal sartlarda kayıt defterinde değişiklik yapılmasına gerek yoktur. Kayıt defteri, bilgisayarlar için hayati derecede önem taşıyan karmaşık sistem bilgilerini içerir ve kayıt defterinde yanlış bir değişiklik yapıldığında bilgisayar çalışmaz hale gelebilir. Bununla birlikte, bozuk bir kayıt defteri dosyasında değişiklik yapılması gerekebilir. Ancak değişiklik yapılmadan önce kayıt defterinin yedeğini alınmalıdır.[101]

Kayıt Defteri hiyerarşisi

Kayıt Defteri hiyerarşik bir şekilde dizinlenmiş girdilerden oluşur ve bu girdiler Windows'un klasör yapısı şeklindedir. Kayıt Defteri;

- HKEY_CLASSES_ROOT,
- HKEY_CURRENT_USER,
- HKEY_LOCAL_MACHINE,

[100] Kayıt defteri nedir?, http://windows.microsoft.com/tr-tr/windows-vista/what-is-the-registry, E.t. 12.10.2014

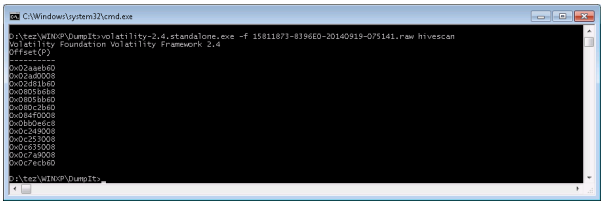
[101] Kayıt Defteri Düzenleyicisi nedir?, http://windows.microsoft.com/tr-tr/windows/what-is-registry-editor#1TC=windows-7, E.t. 12.10.2014

- HKEY_USERS,
- HKEY_CURRENT_CONFIG

isimleri ile beş ana klasörden oluşmaktadır. Bu ana klasörler alt klasörlere, anahtarlara, alt anahtarlara ve değerlere kadar bölünmüştür.

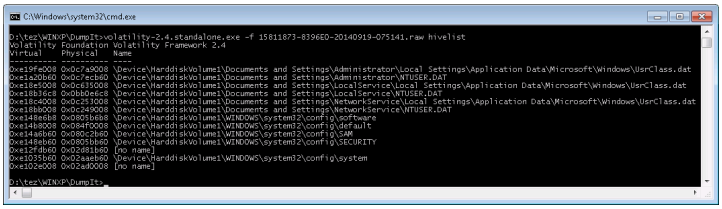
Özetle kayıt defteri; işletim sistemini arka planda yönetmekte ve sistemle ilgili tüm kayıtları tutmaktadır. İşletim sisteminin yüklenmesi ile birlikte kayıt defterinde bulunan bilgiler, sistemin çalışmasını sağlamak üzere belleğe aktarıldığından, yapılacak bellek incelemesi ile bu bilgilere erişilebilir. Aşağıdaki örneklerde, bir bellek imajı üzerinden işletim sistemi hakkındaki değişik bilgilere ulaşılabileceği işlenecektir.

Öncelikle imaj dosyası içinde kayıt defteri bilgisi taraması yapılmalıdır. Tarama işlemi için volatility aracına “hivescan” parametresi ile birlikte çalıştırılır.



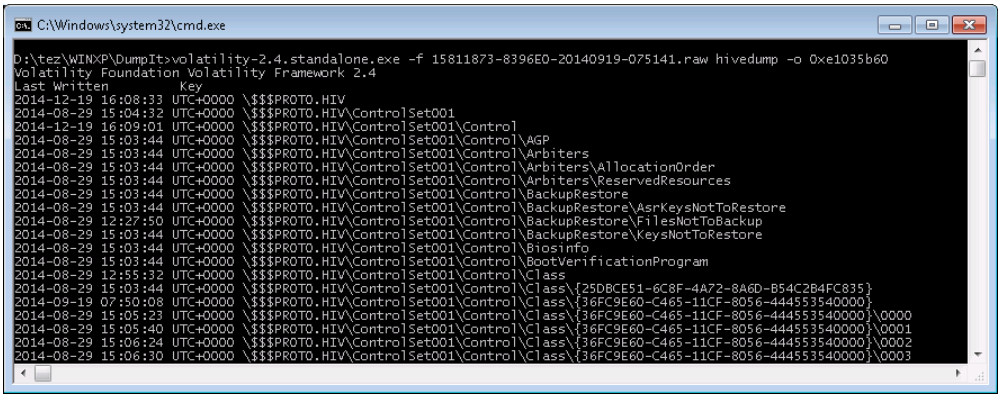
Şekil 53 - Volatility uygulamasının “hivescan” parametresi ile çalıştırılması

Bulunan kayıt defteri bilgilerinin, bellek dökümünün hangi offset değeri içinde saklandığı “hivelist” parametresi ile bulunur.



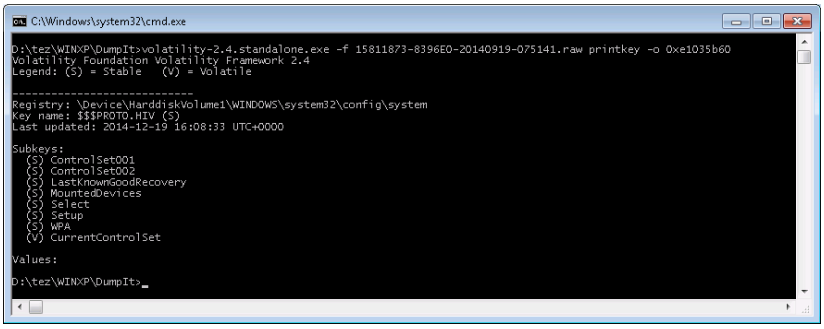
Şekil 54 - Volatility uygulamasının “hivelist” parametresi ile çalıştırılması

Hivelist ile bulunan kayıt defteri bilgileri, “hivedump” parametresi ile bellek imajı üzeriden ekrana çıktısı dökülebilir veya “--output-file=OUTPUT_FILE.txt” parametresi eklenmek suretiyle harici bir dosya içine yazdırılması sağlanabilir.



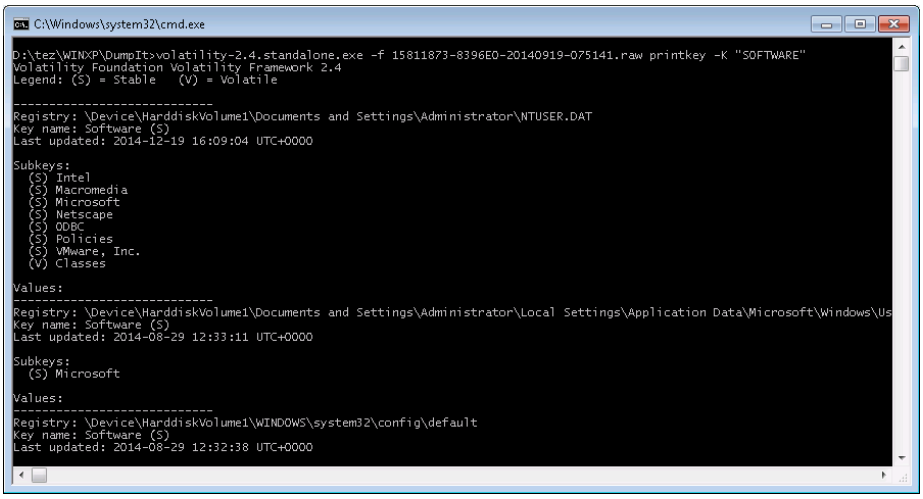
Şekil 55 - Volatility uygulamasının “hivedump” parametresi ile çalıştırılması

“Printkey” parametresi ile ofset değeri verilen kayıt defterine ait bilgiler okunabilmektedir.



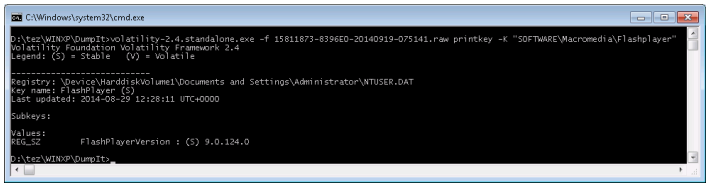
Şekil 56 - Volatility uygulamasının “printkey” parametresi ile çalıştırılması - 1

Bellek imajı alınan bilgisayarda kurulu olan programların listesine –K “SOFTWARE” parametresi ile ulaşılabilmektedir.



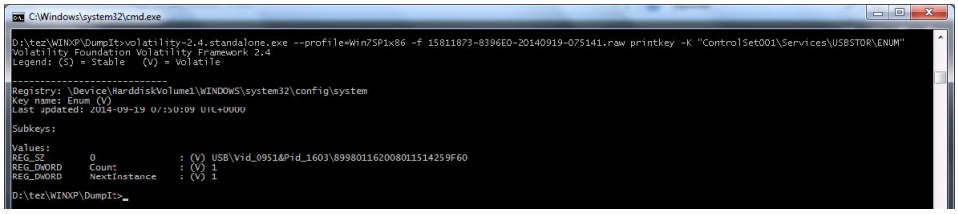
Şekil 57 - Volatility uygulamasının “printkey” parametresi ile çalıştırılması - 2

Ayrıca “printkey” parametresi ile kayıt defteri içinde bulunan alt değerlere ulaşmak mümkündür. Alt kayıt defteri bilgileri için -K “alt kayıt defteri değeri" parametresi kullanılmalıdır. Aşağıdaki ekran çıktısında Flashplayer yazılımına ait bilgiler görüntülenmiştir. Yazılımın 29.08.2014 tarihinde kurulduğu ve versiyon bilgisinin 9.0.124.0 olduğu görülmektedir. 23.09.2014 tarihi itibari ile bu yazılımın 15,0,0,152 versiyonu bulunduğu düşünüldüğünde yazılım versiyonun eski olduğu ve güvenlik açıklığı yaratabileceği değerlendirilebilir.



Şekil 58 - Volatility uygulamasının “printkey” parametresi ile çalıştırılması - 3

Aşağıdaki örnekte -K "ControlSet001\Services\USBSTOR\ENUM" değeri için verilen komut gösterilmektedir.



Şekil 59 - Volatility uygulamasının “printkey” parametresi ile çalıştırılması - 4

Bu kayıt defteri değerinden bilgisayara bir USB disk takıldığı görülmektedir. Ayrıca bu kayıt bilgisinden USB diskin 19.09.2014 tarihinde kullanıldığı ve 8998011620080l514259F60 seri numarasına sahip olduğu anlaşılmaktadır.

Adli veya idari bir incelemede bu bilgilere erişebilir olmak oldukça önemlidir. Bu bilgilerin elde edilmesi ile adli olayın çözümü sağlayabilir.

G. Ağ bağlantısı bilgileri

Her geçen gün teknolojinin ve bu teknolojilere erişilebilirliğin artmasına paralel olarak bilişim sistemlerine yönelik işlenen suçlar da artmaktadır. Siber Suç; bir bilişim sisteminin güvenliğini ve / veya buna bağlı verileri ve / veya kullanıcısını hedef alan ve bilişim sistemi kullanılarak işlenen suçlardır. Siber suçu diğer suçlardan ayıran özelliği bir bilişim sistemi olmadan işlenememesidir. Bu suç türü bilgisayar ve internete özgü suçlar olarak da adlandırılabilir. Siber suç; bir bilişim sistemine izinsiz, hukuka aykırı olarak girilmesi ve sonrasında yapılan eylemlerdir. Bu suçta hedef bir kişi olabileceği gibi kişinin malvarlığı veya bir sistemin kendisi de olabilir. Örneğin, bir sisteme girerek zarar verme, verileri silme, ekleme, şifreleme, ele geçirme, sistemin kullanımını engelleme, özel hayatın gizliliğine müdahale etme, iletişimi engelleme, iletişimi izinsiz izleme ve kayıt etme gibi eylemler siber suç kategorisinde değerlendirilir.[102]

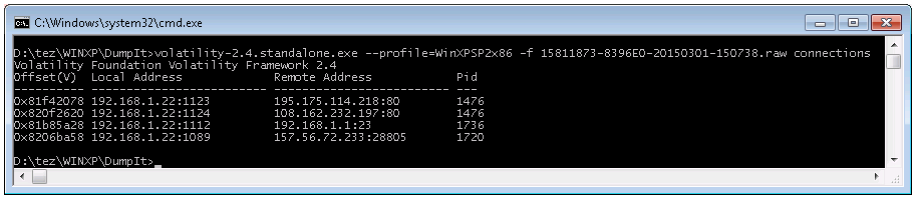
Siber suçların tespit edilmesinde bellekte bulunan bilgilerden faydalanılabilir. Bellek vasıtasıyla sonlandırılmış ve halen açık durumda bulunan ağ bağlantılarına erişmek mümkündür. Günümüzde bilişim suçlarının siber ortamda işlenir olması sebebiyle adli vakaların incelemesinde bu bilgilerden yararlanılabilir.

Bellekten ağ bilgilerine erişebilmek için volatility aracı kullanılabilir. Bellek döküm dosyası içindeki ağ bağlantı bilgileri için volatility aracına girilebilecek parametreler ve kullanımları aşağıda gösterilmiştir.[103]

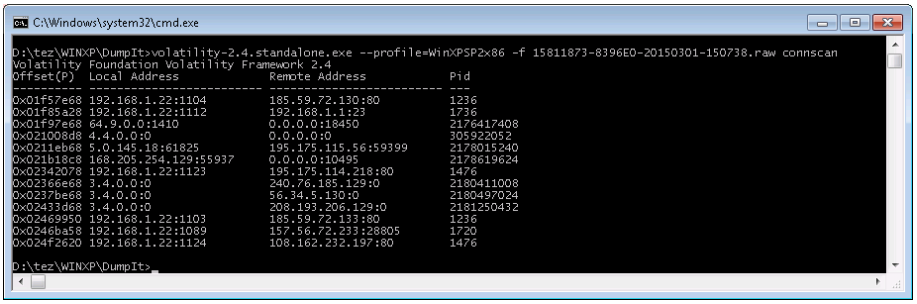
- Aktif ağ bağlantı bilgileri için “connections” parametresi kullanımı;

[102] İstanbul Siber Suçlarla Şube Müdürlüğü Web sayfası; Siber Suçlar Nedir?, http://sibersuclar.iem.gov.tr/siber_suclari.html, E.t. 14.10.2014

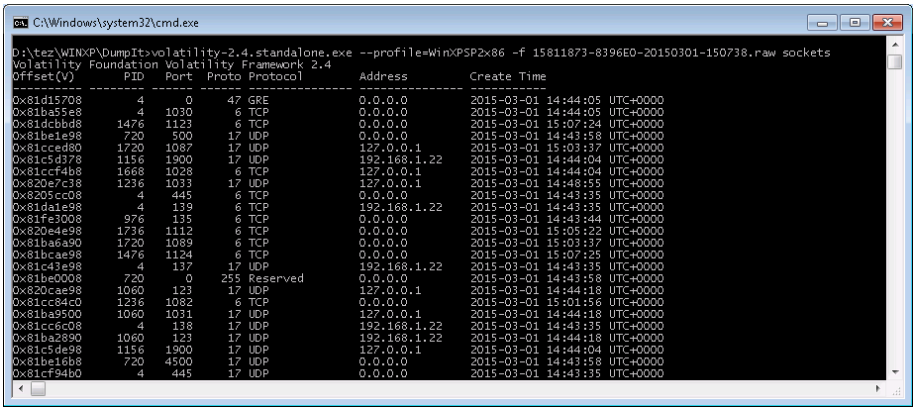
[103] Volatility CommandReference23, https://code.google.com/p/volatility/wiki/CommandReference23, E.t. 14.10.2014



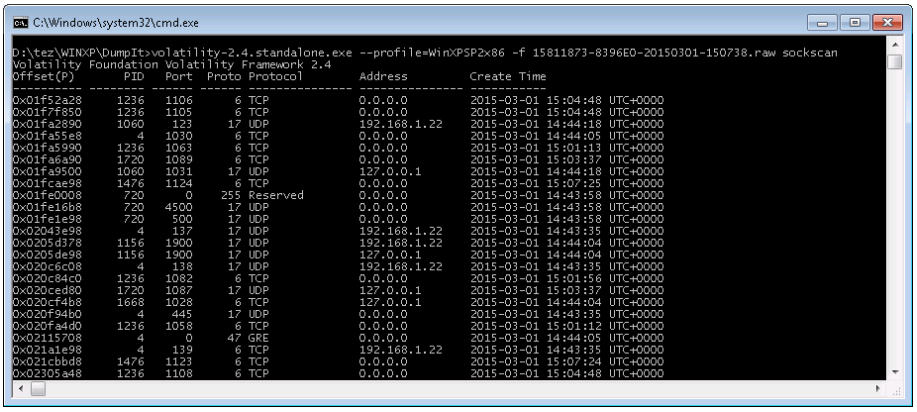
- Sonlandırılmış ağ bağlantı bilgileri için “connscan” parametresi kullanımı;



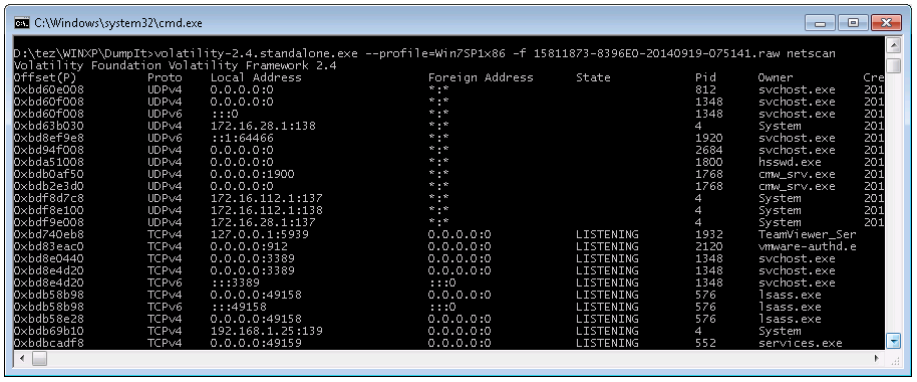
- Aktif bağlantıların kullanıldığı port bilgileri ve kullanılan uygulamaya ait PID bilgileri için “sockets” parametresi kullanımı;



- Sonlandırılmış bağlantıların kullanıldığı port bilgileri ve kullanılan uygulamaya ait PID bilgileri için “sockscan” parametresi kullanımı;



- Bağlantılara ait TCP ve UDP protokollerinin başlangıç ve bitiş durumlarının yanı sıra bağlantının kullanıldığı uygulama ve ağ bağlantılarına ait port bilgileri için “netscan” parametresi kullanımı;



Volatility ile gerçekleştirilen hafıza analizlerinde imajı alınan bilgisayarın üzerinde çalışan uygulamaların hangi port üzerinden hangi IP adresine bağlantı gerçekleştirdiği gibi bilgilere ulaşılabildiği ve bu bilgiler olayın çözülmesinde oldukça önemli bir yere sahip olabildiği görülmektedir.

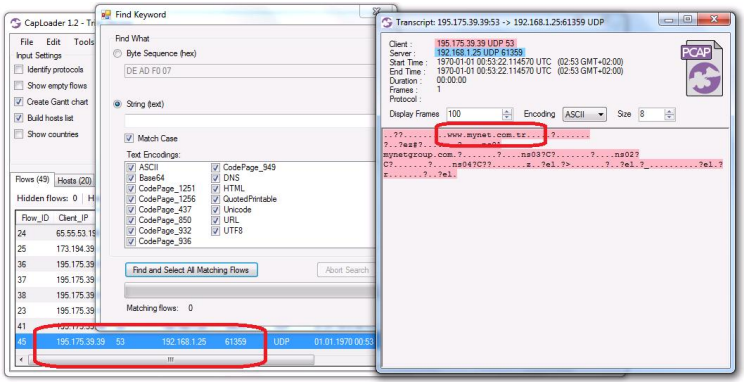
Ancak tespit edilen ağ bağlantı bilgileri içinde ne olduğunu tespit etmekte “volatility” yetersiz kalmaktadır. Bu işlem “CapLoader”[104] yazılımı ile yapılabilir. Yazılımın inceleme yapılacak bilgisayara kurulumu gerçekleştirildikten sonra çalıştırılır. “File” ve “Carve Packets from File” seçeneği ile hafıza imaj dosyası programa girdi olarak verilir ve tarama işlemi başlatılır.

[104] Yazılımın son sürümüne (1.2) “http://www.netresec.com/?page=CapLoader#trial” adresinden erişilebilir, E.t 01.01.2015

Ardından gelen ekranda yer alan listede yer alan herhangi bir paket üzerine sağ tıklayıp açılan menüden “Flow Transcript” seçeneği ile seçim yapılan trafiğe ilişkin ayrıntılı bilgilere erişilebilir. Ayrıca CapLoader ağ paketleri süzme yeteneğine de sahiptir. Böylece istenilen tipteki protokollerin geçtiği paketler elde edilebilir.

Aşağıda bulunan ekran çıktısı incelendiğinde 192.168.1.25 ile 195.175.39.39 ip numaralı adresler arasında UDP 53 portu üzerinden işlem yapıldığı görülmektedir. UDP 53 portu incelendiğinde ise DNS için kullanıldığı görülecektir.[105] DNS (Domain Name System), internet ortamında alan adı ile IP numarası, IP numarası ile alan adı dönüşümlerini gerçekleştiren sistemdir.[106]

Buraya kadar ki bilgilere volatility ile erişilebilirdi ancak UDP 53 portu üzerinden yapılan işleme dair ayrıntılı bilgiyi volatility verememektedir. CapLoader ile UDP 53 portu üzerinden yapılan DNS paketinin detaylarına bakıldığında ise www.mynet.com.tr için sorgulamasının yapıldığı görülmektedir. Bu sayede paket içinde gerçekleştirilen işleme dair ayrıntı bilgilerine dahi erişilmiştir. Caploader, bilişim incelemelerinde ağ bağlantılarına ait ayrıntı bilgilerine ulaşma aşamasında kullanılabilecek bir yazılımdır.



Şekil 60 - CapLoader ile network paketi inceleme

[105] Barney CAPEHART, Information Technology for Energy Managers, sf.220, Fairmost Press, 2004, https://books.google.com.tr/books?isbn=0881734500, E.t. 19.09.2014

[106] William PANEK / James CHELLIS, MCTS Windows Server 2008 Active Directory Configuration Study Guide: Exam 70-640, sf.44-46, Wiley Publishing Inc, Canada, https://books.google.com.tr/books?id=EsQRcBk5QM4C, E.t. 21.07.2014

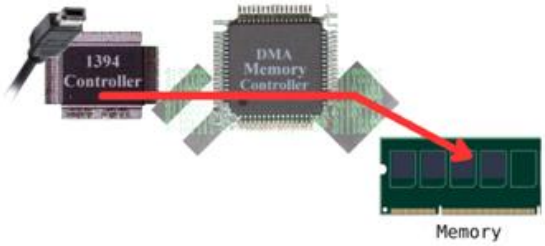
Ğ. Firewire ara yüz açıklığı

Firewire, Apple firması tarafından geliştirilen, bilgisayara çevre ürünleri bağlanmasında kullanılan yüksek hızlı ara yüz bağlantı birimidir. 400 ve 800 Mbps (IEEE 1394b-2002 de 3200 Mbps) hızında veri transferini desteklemektedir. IEEE 1394 portu olarak da geçmektedir.

Firewire USB'ye benzemekle beraber kullanım alanı açısından farklılık gösterir. Bilgisayarlara klavye, fare gibi düşük hızlarda çalışan cihazlar genelde USB veri yolu üzerinden bağlanır. Firewire ise, yüksek veri aktarım hızından dolayı, gerçek zamanlı veri transferi yapabilen video cihazları, kameralar, harici disk gibi cihazlar için kullanılmaktadır.

Firewire portu sadece kameradan görüntü aktarımı için geliştirilmemiş olup aynı zamanda bir ağ protokolüdür. Yani bir Firewire kablosu kullanarak iki bilgisayar birbirine bağlanabilmektedir. Bu şekilde yapılacak bağlantı ile kategori 5 (cat5) kablosu ile yapılan 100 Mbps hızın üzerinde veri transferi gerçekleştirilebilir.

Firewire; doğrudan belleğe erişim (Direct memory access; DMA) yani bilgisayarlarda bulunan işlemciden bağımsız olarak okuma ve/veya yazma işlemi için sistem belleğine direkt erişim sağlamaktadır.



Şekil 61 - Firewire ile doğrudan belleğe erişim (DMA)

DMA, sabit disk kontrol birimleri, ekran kartları, ağ kartları ve ses kartları dahil birçok donanım sistemi tarafından kullanılmaktadır. DMA kanalı olan bilgisayarlar işlem yaparken DMA kanalı olmayan bilgisayarlara nazaran çok daha hızlı veri transferi yapabilmektedir.

DMA'nın genel bir kullanımı, sistem belleğinden bir bellek blokunun, cihazdaki arabelleğe kopyalaması ya da tam tersi olarak cihazdaki arabellekten sistem belleğine bir bellek bloğunun kopyalanmasıdır. Böyle bir işlem işlemciyi geciktirmemektedir. Bu sayede işlemci yorulmamakta ve başka görevleri yapmak üzere programlanabilmektedir.

Yeni Zelanda'da güvenlik danışmanı olarak yaşayan Adam Boileau**,** 2006 yılında Sydney'de düzenlenen bir güvenlik konferansında Windows işletim sistemi yüklü bilgisayarlara saniyeler içinde şifre girmeksizin erişim izni veren, bir ele geçirme yöntemi göstermiştir.[107,108]

Boileau durumu şu sözlerle ifade etmiştir: "Ben 2006 yılında bu programı halka açmamıştım. Çünkü Microsoft, Firewire bellek erişimini bir güvenlik meselesi olup olmadığı konusunda tedbirli davranıyordu. Ve biz de o sıra bir problem yaratmak istemedik."

Bu yöntemi kullanan hacker'lar; öncelikle Linux tabanlı bir bilgisayar ile hedef alınan sisteme Firewire portu üzerinden bağlantı kurmakta ve bilgisayarın hafızasına doğrudan erişim sağlayarak Windows'un parola koruma koduna müdahale etmektedir. Bu yöntem ile ele geçirilen bir bilgisayara ait video görüntüsü "http://vizle.tv/windows-FireWire-hack,5N-C5s_07Ts.html" adresinden izlenebilir.

Güvenlik araştırmaları yapan Sophos[109] şirketinin teknoloji yöneticisi olan Paul Ducklin Firewire portu için "Eğer bir Firewire portunuz varsa, onu

---

[107] Harlan CARVEY, Windows Forensics Analysis DVD Toolkit, Coauthor of Real Digital Forensics, sf.139, Syngress Publishing Inc, USA, 2014, http://160.216.223.99/vyuka/forensics/Windows%20Forensic%20Analysis%20DVD%20Toolkit%20%20Second%20Edition.pdf, E.t. 19.10.2014

[108] Adam BOILEAU, Hit by a Bus: Physical Access Attacks with Firewire, Computer Security Conference Presentation, Ruxcon 2006 http://www.security-assessment.com/files/presentations/ab_firewire_rux2k6-final.pdf, E.t. 19.10.2014

[109] http://www.sophos.com/en-us.aspx

kullanmıyorken etkinliğini sonlandırın. Eğer birisi sizin portunuzu beklenmedik şekilde kullanırsa, Firewire'niz ölmüş demektir." [110] cümlesini kullanmıştır.

Özetle Firewire; DMA özelliği sayesinde belleğe doğrudan erişebilmektedir. Bu durum bir güvenlik açığı olarak değerlendirilmiş ve bu açıklığı kullanan yazılımlar geliştirilmiştir.

Passware firmasına ait "Passware Kit Forensic"[112] yazılımı bunlardan bir tanesidir. Yazılım; Facebook, Google, MS Word, MS Excel, TrueCrypt, FileVault2, PGP gibi yazılımlara ait şifreleri çözme yeteneğine sahiptir. Ayrıca Firewire portu üzerinden bellek imajı da oluşturabilmektedir.

Bu bölümde Firewire portu üzerinden "Passware Kit Forensic" yazılımı vasıtasıyla bellek imajı oluşturulacaktır. Bu işlem için bellek imajı oluşturulacak ve oluşturacak bilgisayarlar arasında bağlantı kurmak için Firewire kablosuna ihtiyaç duyulacaktır.

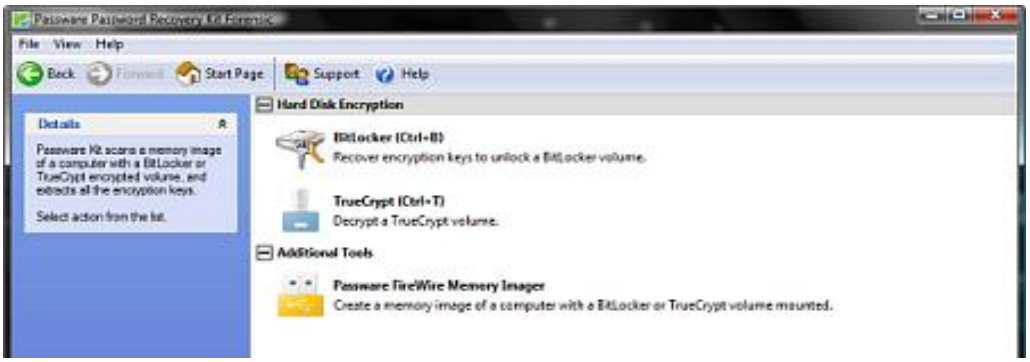
Yazılım çalıştırılır ve Passware Kit Start Page sayfasında "Recover Hard Disk Passwords" (veya Ctrl+D tuş kombinasyonu) ve sonrasında "Passware Firewire Memory Imager" tıklanır.[113]

---

[110] Selim ÖZTÜRK; Windows, Birkaç Saniyede Ele Geçirilebilir, http://www.chip.com.tr/haber/windows-birkac-saniyede-ele-gecirilebilir_5864.html E.t. 20.10.2014

[112] Yazılımın son sürümüne (13.7) "http://www.lostpassword.com/kit-forensic.htm" adresinden erişilebilir, E.t 21.12.2014

[113] Acquiring Memory Image Using Passware FireWire Memory Imager, http://www.lostpassword.com/hdd-decryption.htm#imager, E.t. 20.10.2014



Şekil 62 - Firewire ile bellek imajı oluşturma - 1

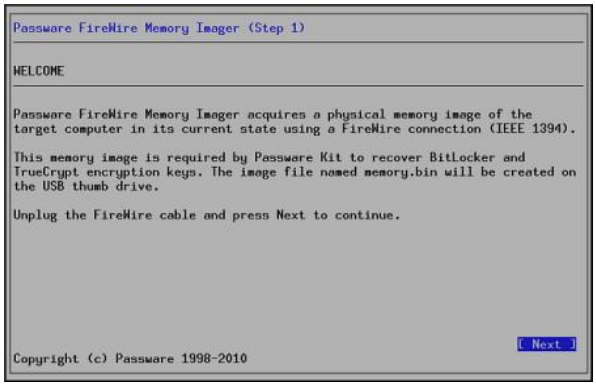
Takip eden sayfada; bellek imajı oluşturacak bilgisayara bir adet boş “USB Disk” takılması istenmektedir.

Şekil 63 - Firewire ile bellek imajı oluşturma - 2

USB Disk takılıp ve “Next” tuşuna basıldığında bellek imajı oluşturmak için ihtiyaç duyulan dosyalar USB Diske kopyalanır.

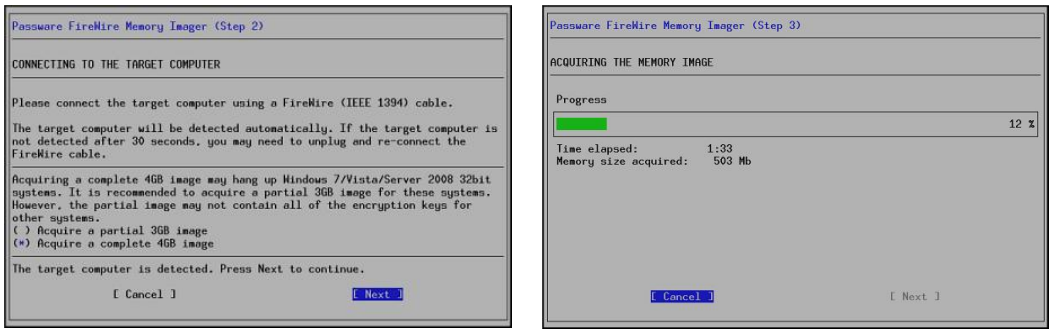
Şekil 64 - Firewire ile bellek imajı oluşturma - 3

Ardından BIOS ayarlarından bilgisayarın USB Disk üzerinden başlatılması için gerekli ayarlar yapılarak, “Passware FireWire Memory Imager” yazılımın çalışması sağlanır.



Şekil 65 - Firewire ile bellek imajı oluşturma - 4

Firewire kablosu ile bellek imajı oluşturulacak ve oluşturacak bilgisayarlara arasında bağlantı kurulur ve “Next” tuşuna basılmak suretiyle imaj oluşturma işlemine başlanır.



Şekil 66 - Firewire ile bellek imajı oluşturma - 5

Bellek imajı oluşturma işlemi tamamlandığında Firewire kablosu ve USB Disk bilgisayardan çıkarılarak bilgisayar yeniden başlatılır. USB Disk içinde bulunan “memory.bin” isimli dosya hedef sisteme ait bellek imaj dosyasıdır. Bu aşamadan sonra “memory.bin” dosyası üzerinden ayrıntılı bellek analiz işlemi yapılabilir.

Firewire portunun bu özelliği yazılımsal olarak imaj oluşturulamayan durumlarda alternatif bir bellek imajı oluşturma yöntemi olarak kullanılabilir.

Firewire portunun bu açıklığının önlemek amacıyla kullanılmayan Firewire portları devre dışı bırakılmalıdır. Ayrıca yüklenmiş FireWire sürücüleri de sistemden kaldırılmalıdır.[114] Bu amaçla aşağıda anlatılan önlemler alınmalıdır.

Windows işletim sistemleri için, BitLocker yapılandırma çeşitlerinden sadece TPM modu kullanılıyor ise Windows SBP-2 sürücüsünün ve tüm Thunderbolt denetleyicilerinin engellenmesini Microsoft firması tarafından önermektedir. TPM+PIN, TPM+USB ve TPM+PIN+USB modlarının tercih edilmesi, bilgisayarların uyku modunu özelliğinin kullanmadığı zamanlarda DMA saldırılarının etkisini azaltacağı belirtilmiştir.[115] Ayrıca yazılımsal olarak FireWire portunu engelleyen Firewire blocker[116] yazılımı kullanılabilir.

Mac OS için FileVault2 ve OS X Lion (10.7.2) ve üzeri işletim sistemleri kullanılıyor ise DMA otomatik olarak kapalı olarak gelmektedir. Ayrıca Mac bilgisayarlara Firewire portu için parola verilemelidir.[117]

Linux'de ise DMA özelliği kernel modülleri seviyesinde kapatılmalı ve 1394 sistemden sürücüleri kaldırılmalıdır.[118]

H. Zaman çizelgesi oluşturma

Zaman çizelgesi incelemeye konu olan olayın gerçekleşme zamanını ve olay anında kullanılan aygıt, program, doküman, araç vb. belirlenmesinde kullanılmaktadır. Zaman çizelgesi oluşturma iki aşamadan oluşmaktadır. Öncelikle dosya sistemleri analiz edilerek metadatalarda bulunan zaman bilgileri

---

[114] Inception, http://www.breaknenter.org/projects/inception/, E.t. 21.11.2014

[115] BitLocker'a yönelik 1394 DMA ve Thunderbolt DMA tehditlerini azaltmak için SBP-2 sürücüsünü ve Thunderbolt denetleyicilerini engelleme, http://support.microsoft.com/kb/2516445, E.t. 21.11.2014

[116] http://www.securityresearch.at/publications/firewireblocker.zip, E.t. 22.11.2014

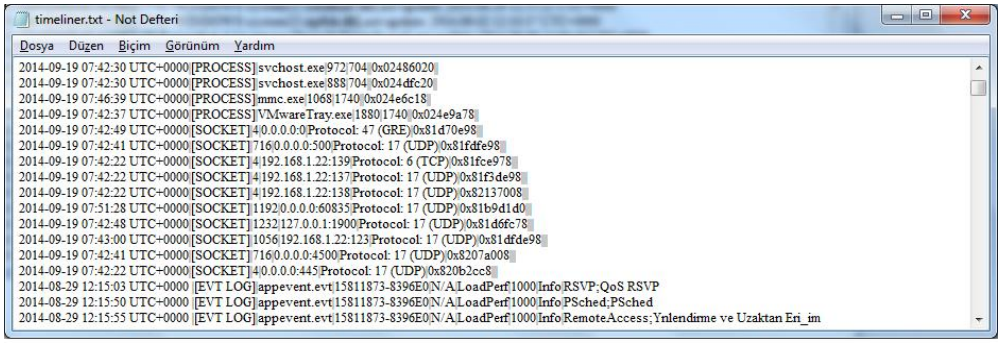
[117] OS X Open Firmware settings: use nvram security-mode to disable firewire DMA without a firmware password, http://ilostmynotes.blogspot.com.tr/2012/01/os-x-open-firmware-settings-use-nvram.html, E.t. 22.11.2014

[118] Physical memory attacks via Firewire/DMA - Part 1: Overview and Mitigation (Update), http://www.hermann-uwe.de/blog/physical-memory-attacks-via-firewire-dma-part-1-overview-and-mitigation, E.t. 22.11.2014

bir dosyaya yazdırılır ve ardından bu dosya bulunan veriler anlaşılabilir bir formata dönüştürülür.

Bu bölümde bellek imaj içinden dosyasından zaman bilgisi oluşturma işlemi gerçekleştirilecektir. Bu işlem için volatility aracı ile birlikte "timeliner" parametresi kullanılacaktır. Komutun örnek kullanımı ve sonuç dosyasına ait ekran görüntüsü aşağıdadır.

volatility-2.4.standalone.exe -f bellekimaji.raw profile=WinXPSP2x86--timeliner --output-file=timeliner.txt --output=text



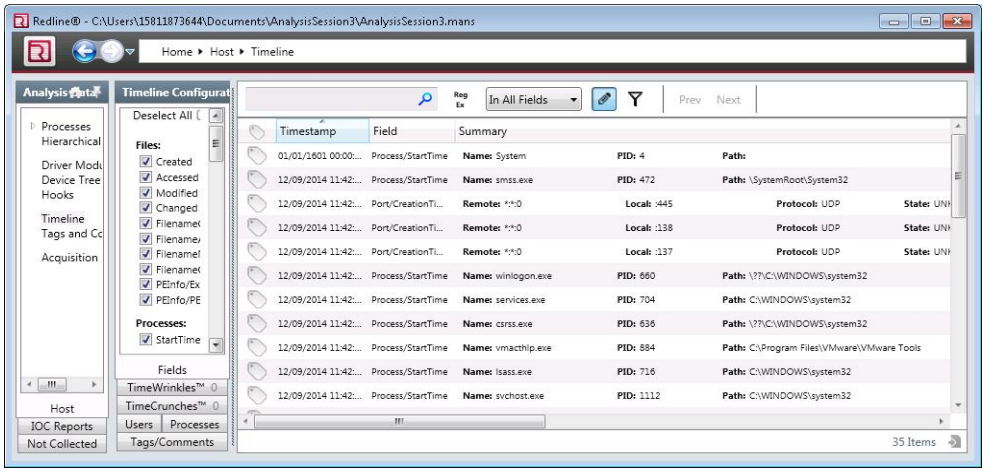
Şekil 67 - Volatility uygulamasının "timeliner" parametresi ile kullanımı

Bellek imaj dosyası içinden; bilgisayarda çalışan işlemler (process), olay geçmişi (event view), kullanıcı tarafından yapılan işlemler, ağ bağlantısı ve benzeri bilgiler gerçekleşme zamanları ile birlikte bir dosya çıkarılmıştır. Bilgisayarda yapılan işlemlerin kronolojik olarak sıralandığı, oluşturulan dosya içinde görülecektir.[119]

Bu bilgilere "Mandiant Redline"[120] yazılımı ile de elde edilebilir. Aynı imaj dosya Redline ile incelendiğinde elde edilen sonuca ait ekran görüntüsü aşağıdadır. Redline yazılımı kullanıcı dostu ara yüzünü ve kullanımının kolay olması sebebiyle zaman çizelgesi oluşturma aşamasında tercih edilebilir.

119 Michael Hale LIGH / Andrew CASE / Jamie LEVY / Aaron WALTERS, The Art Of Memory Forensics (Dececting Malware and Threads in Windows, Linux and Mac Memory), sf. 71, 471, 537-541, John Wiley & Sons, Inc., Indiana, USA, 2014, http://news.asis.io/sites/default/files/The%20Art%20of%20Memory%20Forensics.pdf

120 Yazılımın son sürümüne (1.13) https://www.mandiant.com/resources/download/redline adresinden erişilebilir, E.t 01.01.2015



Şekil 68 - Mandiant Redline ile zaman çizelgesi

Zaman çizelgesi ile gerçekleşmiş bir olay sırasında izlenen yöntem, aygıt, araçlar bu şekilde belirlenebilir ve olay yerinden elde edilen diğer bilgiler ile birleştirilerek olayın çözümünde önemli rol alabilir.

I. Malware tespiti

Kötü amaçlı yazılım veya malware (İngilizce: malicious software (kötü amaçlı yazılım), bilgisayar sistemlerine zarar vermek, bilgi çalmak veya kullanıcıları rahatsız etmek gibi amaçlarla hazırlanmış yazılımlara genel olarak verilen isimdir. Bu yazılımlara virüsler, solucanlar, truva atları, rootkitler vb. örnek olarak verilebilir. Bu yazılımlar bulaştığı bilgisayar sisteminde veya ağ üzerindeki diğer makinelerde zarara yol açmak, çalışmalarını aksatmak, uzaktan erişime açmak, kullanıcı bilgilerini çalmak vb. birçok amaç için kullanılmaktadır.[121]

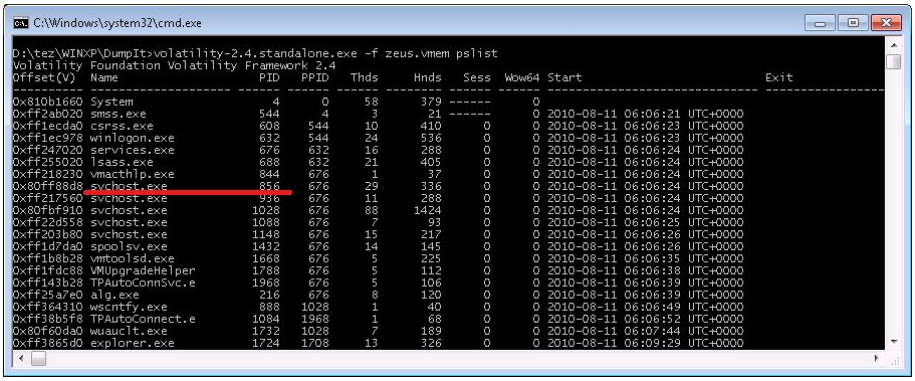
İlk kez 2007'de ortaya çıkan Zeus isimli kötücül yazılım, özellikle ABD'de binlerce internet sitesine bulaşmış ve milyonlarca kullanıcı bilgisayarına yayılmıştır. Kullanıcı bilgisayarını bankacılık işlemleri için kullanmaya başladığında aktif olan Zeus, bankacılık şifrelerini çalıyor ve hesapları boşaltıyordu. Zeus'un bazı sürümleri banka sayfasını taklit edip çok daha fazla

[121] Gürol CANBEK, Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Eylül 2005, E.t. 14.11.2014

bilgiyi ele geçirebiliyor. Ele geçirilen değerli bilgiler daha sonra kara borsada satılıyordu. Ortaya çıktığı günlerde bir türlü engellenemeyen Zeus'un zaman içinde sayısız farklı sürümü türemişti. Tüm dünyadan binlerce saldırganın kullandığı zararlının ne kadar maddi zarara yol açtığı hesaplanabilmiş değildir.

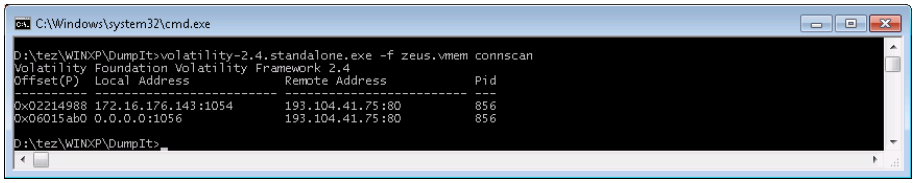
Bu bölümde, Zeus kötücül yazılımının bulaşmış olduğu sistemin bellek imajı[122] üzerinden volatility yardımıyla zararlı yazılımın tespiti yapılacaktır.[123]

Öncelikle sistemde herhangi şüpheli bir işlemin çalışıp çalışmadığını kontrol etmek üzere "pslist" parametresi kullanarak çalışan tüm işlemlerin listesini alınır.



Şekil 69 - Volatility uygulamasının "pslist" parametresi ile çalıştırılması

İlgi çekebilecek şüpheli gibi görünen bir işlem görülmemektedir. İncelemeye "connscan" parametresi ile herhangi aktif bir bağlantı olup olmadığı kontrol edilerek devam edilir.



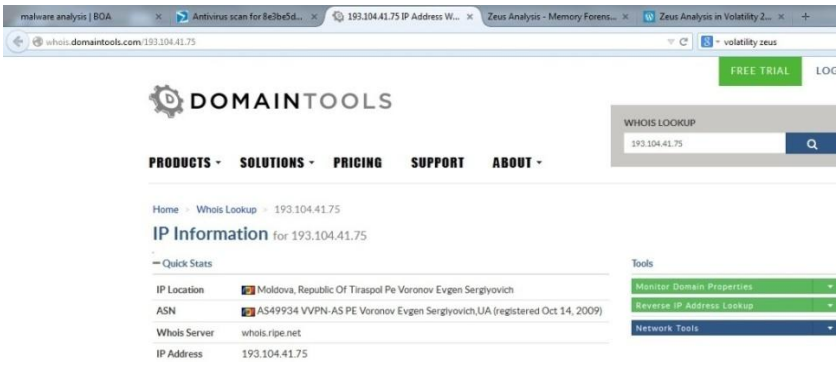
Şekil 70 - Volatility uygulamasının "connscan" parametresi ile çalıştırılması

[122] http://publish.boateknoloji.com/wp-content/uploads/2014/01/zeus.vmem.zip, E.t. 15.11.2014

[123] Volatility: Hafıza Analiz Aracı, http://publish.boateknoloji.com/tag/malware-analysis/, E.t. 15.11.2014

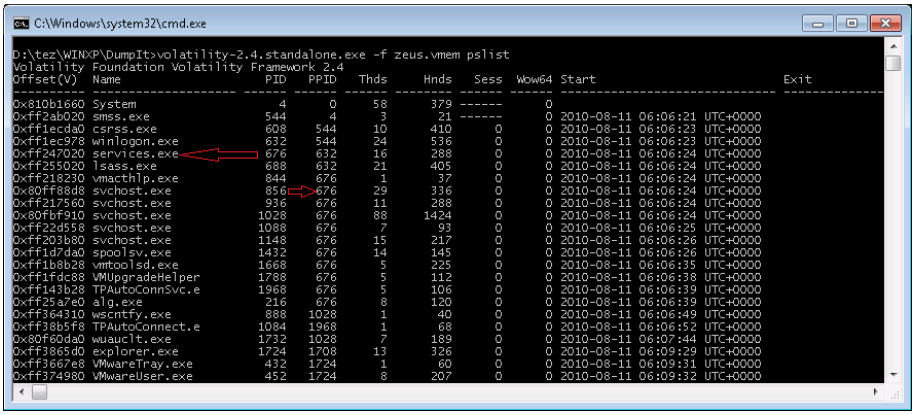
Komut sonucunda çıkan ekran incelendiğinde 856 işlem numarasına (PID) sahip işlemin; 172.16.176.143:1054 ve 0.0.0.0:1056 kaynak adreslerinden; 193.104.41.75:80 hedefine doğru iletişimde olduğu görülmektedir.

193.104.41.75 IP adresi, ip numarası sorgulama siteleri üzerinden incelendiğinde Moldova Cumhuriyeti'ne ait olduğu görülmektedir.[124]



Şekil 71 - Ip numarası sorgulama ekranı

Daha önceki pslist parametresine ait çıktıdan 856 işlem numarasına sahip işlemin "svchost.exe" olduğu bilinmekteydi. "pstree" parametresi kullanarak "svchost.exe"nin işlem ağacındaki yerine bakıldığında,

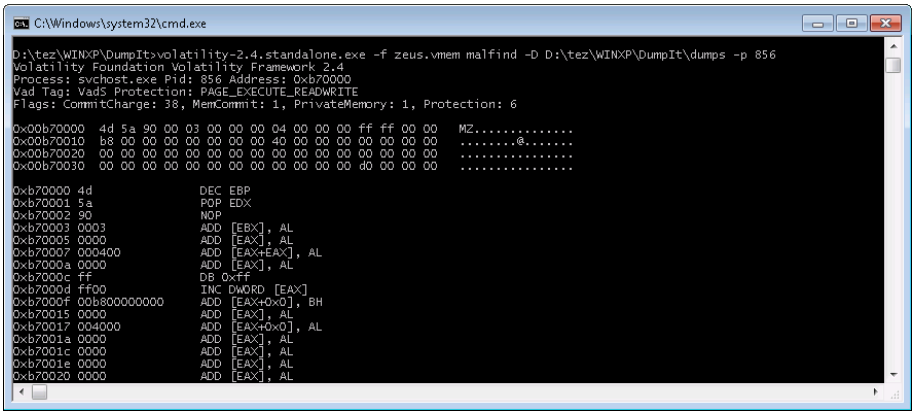


Şekil 72 - Volatility uygulamasının "pstree" parametresi ile çalıştırılması

"services.exe" altında çalıştığı görülmektedir. "svchost.exe" için "malfind" parametresi kullanarak enjekte olup olmadığı kontrol edilir. Malfind

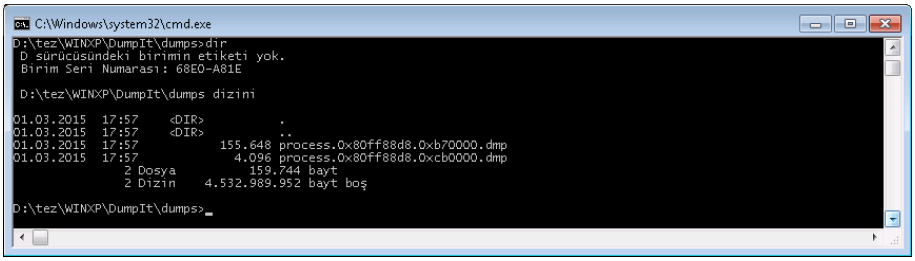
[124] http://www.whois.sc/193.104.41.75

parametresine -D parametresi ile enjekte olan dosyanın nereye çıkarılacağını ve -p parametresi ile de hangi proses üzerinde çalışacağı belirtilir.



Şekil 73 - Volatility uygulamasının “malfind” parametresi ile çalıştırılması

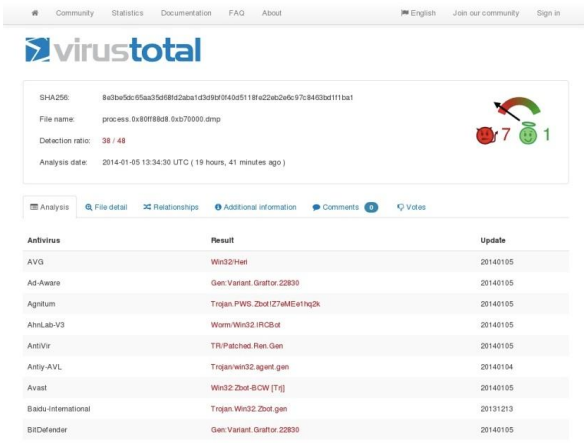
-D parametresi ile verilen dizinde process.0x80ff88d8.0xb70000 ve process.0x80ff88d8.0xcb0000 isimli iki dosyanın oluştuğu görülmektedir.



Şekil 74 - Şüpheli olabilecek dosyaların listelenmesi

Bu dosyaları; şüpheli URL ve dosyaları inceleyen, virüslerin, solucanların ve tüm zararlı yazılımların tespitini sağlayan VirusTotal[125] aracılığıyla taratılması sonucunda process.0x80ff88d8.0xb70000.dmp dosyasının zararlı bir yazılım olduğu görülmüştür. Böylece bellek incelemesi ile sistemde olağan bir şekilde çalışır gibi gözüken ancak zararlı olan yazılımın tespiti yapılmıştır.

[125] https://www.virustotal.com/



Şekil 75 - Şüpheli dosyaları sorgulama ekranı

İ. Cold boot attack

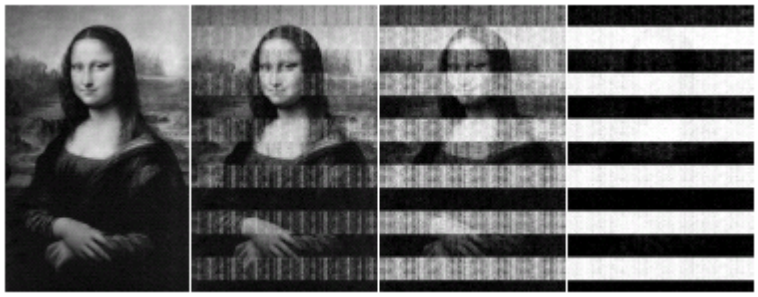
Bilgisayarlardaki DRAM yongaları verileri geçici olarak saklamaktadır. Bilgisayarın elektrik bağlantısı kesildiğinde ise şimdiye kadar bu bilgilerin silinerek yok olduğu düşünülmekteydi. Princeton Üniversitesi'nde bir araştırma grubu tarafından yapılan bir araştırma sonucunda bellekler üzerinde yer alan şifrelenmiş verilerin kolayca okunabilmesine yol açan kritik bir açıklık bulunduğu tespit edilmiştir. Bulunan yöntem ise şaşırtıcı derecede basitti. Uygulanan teknik bilgisayarın bellek yongalarının buz tutacak seviyede dondurulmasına dayanmaktadır.[126] Araştırma sonuçlarıyla hafıza yongalarının aslında verileri birkaç saniye hatta bir dakika içerisinde geri getirebildiği gösterildi.

Kapasitif yöntemle depolanan veriler, kapasitörler deşarj olunca tamamen yok olmuş olur. Belleklerin çok düşük sıcaklıklarda soğutulması ise deşarjı yavaşlatır, bu da belleklerdeki verilerin farklı bir ortama aktarılması için yeterli süreyi sunmaktadır.[127]

---

[126] J. Alex HALDERMAN / Seth D. SCHOEN / Nadia HENİNGER / William CLARKSON / William PAUL; Lest We Remember: Cold Boot Attacks on Encryption Keys, Princeton University, USENIX Security Symposium Paper, 21.02.2008, http://citpsite.s3-website-us-east-1.amazonaws.com/oldsite-htdocs/pub/coldboot.pdf, E.t. 11.10.2014

[127] Onur KARAMANLI, SAM Dosyası ve RAM'deki Bilgilerin Güvenliği, https://www.bilgiguvenligi.gov.tr/donanim-guvenligi/sam-dosyasi-ve-ramdeki-bilgilerin-guvenligi-2.html, E.t. 15.10.2014



Şekil 76 - Bellekten elde edilen resim dosyaları

Araştırma grubu tarafından; bir bilgisayar belleğine resim dosyası yüklenmiştir. Daha sonra bilgisayarın gücü kesilmiştir. 5 saniye sonra görüntünün neredeyse orijinalinin aynısı gibi olduğu, sonra görüntünün yavaş yavaş bozulmaya başladığı görülmektedir. Soldan ikinci resim 30'ncu saniyede, 3'ncü resim 60'ncı saniyede ve 4'ncü resim ise 5 dakika sonra elde edilmiştir.[128]

Grubun yaptığı açıklamada araştırmanın kötü niyetli kullanım amacı taşımasının aksine, olası hırsızlık vakalarının önüne geçmek adına bir önlem olması açısından önem taşıdığı belirtilmektedir.[129]

Bellekleri sıvı nitrojen yardımıyla soğutarak (-50 | -190) bu süreyi daha da artırmak mümkündür. Yongalar buz tutacak seviyede soğutulduktan sonra verilerin ve anahtar bilgilerin sızdırılabildiğini örnekleriyle göstermiştir. Rapora göre donma sonrasında yongalar o anki durumlarını uzun süre muhafaza edebilmektedir. Bu da ilgili yongaların makinede tekrar çalıştırılıp üzerlerindeki bilgilerin kolaylıkla okunabilmesine imkan tanımaktadır.

Şekil 77 - Belleklerin sıvı nitrojen ile soğutulması

[128] Princetion University - Center for information technology policy, https://citp.princeton.edu/research/memory/media/, E.t. 16.10.2014

[129] Henk C.A. van TILBORG / Sushil JAJODIA, Encyclopedia of Cryptography and Security, sf.216, Spinger Science Business Media, London, UK, 2011, https://books.google.com.tr/books?id=UuNKmgv70lMC, E.t. 16.10.2014

Şifrelenmiş verilere genellikle şirketler, devlet kurumları ve olası çalınma riski nedeniyle kullanıcıların dizüstü bilgisayarlarında sıklıkla rastlanmaktadır. Apple kendi ürünlerinde FileVault şifreleme özelliği ile Microsoft ise Vista ve sonrası işletim sistemlerinde BitLocker ile şifreleme imkanı sağlamaktadır. Ancak yapılan araştırmada iki sistemin de şifrelenmiş olsa dahi verilere erişilebileceği çökertilebildiği açıkça gösterilmiştir. Bu nedenle aktif olarak kullanılmayan (özellikle rahatlıkla taşınabilen dizüstü) bilgisayarlar açık bırakılmamalıdır. Ayrıca bilgisayarlar kullanılmadıkları sürece kilitlenmek (Win+L) suretiyle gözetimsiz bırakılmaları da doğru bir yöntem değildir.

J. Pano (Clipboard)'da bulunan bilgilere erişim

Pano, kısa zamanlı veri depolayan ve bu verinin herhangi bir uygulama içerisinde ya da uygulamalar arasında kullanılmasına olanak sağlayan bir depolama sistemidir. Pano herhangi bir veri tipindeki içeriği depolayabilmektedir. Bu durum panonun kullanım alanının genişlemesine ve haliyle depoladığı verinin mahremiyet ya da gizlilik açısından kritik sayılabilecek bilgileri de içermesine yol açmaktadır.[130]

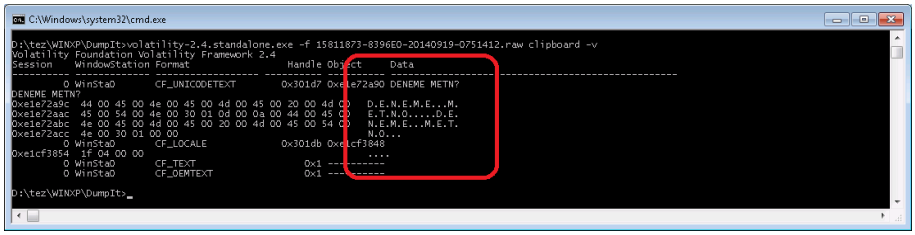
Doğası gereği pano birçok işleme maruz kalmaktadır. Kullanıcı tarafından gerçekleştirilen kesme, kopyalama, yapıştırma operasyonlarının yanı sıra uygulamaların da panoyu çeşitli amaçlarla kullanması, pano içerisinde geçici olarak depolanan panoda e-posta adresleri, kredi kartı numaraları, özel şahıslara ait bilgiler ve hatta kullanıcı şifreleri dahil olmak üzere çok çeşitli bilgi bulunabilmektedir. Panoya uygulamaların ya da kişilerin erişmesinin mümkün olması kritik verilerin güvenliğini önemli bir hale getirmektedir. Bunun yanı sıra panodaki verinin çok sık değiştirilebilmesinin veri kaybına sebebiyet verebileceği unutulmamalıdır.

---

[130] Abdulkadir POŞUL, TÜBİTAK BİLGEM; Pano (Clipboard), https://www.bilgiguvenligi.gov.tr/veri-gizliligi/pano-clipboard.html, E.t. 10.07.2014

Adli bilişim açısından konuya bakıldığında; bellek incelemesi ile panoda bulunan verilere erişilmesi, incelemeyi gerektiren hususun çözümlenmesi açısından önemli olabilir. Tüm bellek incelemelerinde olduğu gibi panoda bulunan verilere ulaşılmak istendiğinde öncelikle sistemin bellek imajı alınmalıdır. Ardından imaj incelenmelidir.

Bellek imajı volatility aracı ile incelenmek istenildiğinde "clipboard" parametresi ile birlikte çalıştırılmalıdır. Komutun kullanımı ve sonuçlarının bulunduğu ekran çıktısı aşağıdadır. Panoda bulunan veriler "Data" bölümü altında görülmektedir.



Şekil 78 - Volatility uygulamasının "clipboard" parametresi ile çalıştırılması

Bilgisayarlarda bulunan her bir dosya tipi disk üzerinde oluşturulduğu anda belirli karakter ile başlamakta ve belirli bir karakter ile sonlandırılmaktadır. Başlangıç bilgisine "Header" bitiş bilgisine de "Footer" denilmektedir. Örneğin, bir sıkıştırılmış resim dosyası (jpg) FFD8 ile başlamakta ve FFD9 ile sonlanmaktadır. Header ve Footer bilgilerine dosya imza bilgisi denilmektedir. Dosya imza bilgileri dosyaların oluşturulduğu platformlar (Windows7, WindowsXP, Fedora, Centos, vb.) farklı olsa dahi aynıdır. Ayrıca dosyaların uzantılarının değiştirilmesi durumunda dahi imza bilgisi değişmemektedir.

Bellekte bulunan belirli dosya tiplerinin (.doc, .xls, .jpg, .pdf, vb.) kurtarılması istendiğinde; Foremost ve Scalpel gibi yazılımlar kullanılabilir.[131,132]

[131] MoVP 3.4: Recovering tagCLIPDATA: What's In Your Clipboard?, http://volatility-labs.blogspot.com.tr/2012/09/movp-34-recovering-tagclipdata-whats-in.html, E.t. 18.11.2014

[132] Michael Hale LIGH / Andrew CASE / Jamie LEVY / Aaron WALTERS, The Art Of Memory Forensics (Dececting Malware and Threads in Windows, Linux and Mac Memory), sf.471, John Wiley & Sons, Inc., Indiana, USA, 2014,

Bu yazılımlar dosya kurtarırken dosyaların imza bilgilerine göre tarama yapmaktadır. Bu yönteme dosya kazıma (file carve) denilmektedir.

§ 5. İmaj oluşturma ve analiz yazılımları

Bellekler dinamik bir yapıya sahiptir. Bellekte bulunan veriler, işlemci tarafından üretilen işlemlere ait bilgiler ile sürekli değişmektedir. Bu değişim işlemine uçuculuk (volatility) denilmektedir. Belleklerde olduğu gibi bilgisayar üzerinde bulunan birçok donanım üzerinde bulunan veriler de uçuculuk özelliğine sahiptir. Uçucu verilerin özelliklerine ve uçuculuk sıralanması dair geniş bilgi için RFC 3227[133]'ye bakılabilir.

İşlemcilerin veri hızı, sabit disklerin veri hızından daha yüksektir. İşlemci sabit diskte bulunan bir veriye ulaşmak istediğinde; sabit diskte bulunan veri belleğe aktarılmakta ve işlemci tarafından işlenebilir hale gelmektedir. İşlemcinin bellekte bulunan veri ile işlemi tamamlandığında veri bu defa sabit diske aktarılmaktadır. Bu sebeple bellekler; işlemci ile sabit disk arasında köprü görevi görmektedir.

Belleğin kapasitesine bağlı olarak bellekte işlenen veri ile işlem tamamlanmış olsa dahi bellekte hala veri bulunabilir. Bu nedenle bellekten önemli verilere ulaşılabilme ihtimali vardır. Bellekte bulunan verilere ulaşılmak istenildiğinde; öncelikte sisteme ait belleğin kopyası (imaj) alınmalıdır. Böylece istenildiği zaman imaj üzerinden imajın alındığı an itibari ile bellek analizi yapılabilir. Sisteme verilecek her bir komut bellekte bulunan verileri değiştireceğinden, imaj alma işlemi sisteme en az müdahale ile yapılmalıdır.

---

http://news.asis.io/sites/default/files/The%20Art%20of%20Memory%20Forensics.pdf., 28.07.2014

[133] D. BREZINSKI, RFC3227:Guidelines for Evidence Collection and Archiving, Şubat 2002, Adavec Inc., https://www.ietf.org/rfc/rfc3227.txt

I. İmaj oluşturma yazılımları

Bellek imajı oluşturmak için kullanılan birçok yazılım bulunmaktadır. FTK Imager, Encasev7, Windd ve Belkasoft Live RAM Capturer, Dumpit adli bilişim alanında kullanılan en önemli yazılımlardandır. Bunların özellikleri ve kullanım alanları kısaca şu şekildedir.

FTK Imager; Accesdata firmasının ürünü olan FTK imager ile sistem üzerinde bulunan RAM'in bire bir (bit to bit) kopyasını oluşturabilir. Ücretsiz olup internet üzerinden rahatlıkla temin edilebilir. Sistem üzerine kurulum yapılmasına ihtiyaç duyulmaksızın çalışmaktadır.

Encase V7; Guidance Software firmasının ürünü olan Encase v7 ile de bellek imajı alınabilmektedir. Encase v7 ücretli bir yazılım olup imaj alma özelliği ücretsiz olarak kullanılabilmektedir. Sistem üzerinde kurulum yapılarak kullanılacağı için bellek üzerinde çok fazla proses kullanarak bellek üzerinde ki verilere kalıcı zarar verebilmektedir.

Belkasoft Live RAM Capturer; Belkasoft Forensics Made Easier firması tarafından geliştirilen ve belleği az seviyede kullanarak bellekte bulunan verilere daha az zarar vererek imaj almaya yarayan özel bir yazılımdır. Sistemlerin mimarleri önemli olup çalışması esnasında kurulum dosyası ile birlikte gelen .sys dosyasına ihtiyaç duyar. Ücretsiz olarak Belkasoft Forensics'in web sayfasından temin edilebilir.

Dumpit; Moonsols firması tarafından geliştirilmiş, 32-bit ve 64-bit Windows işletim sistemlerinde kullanılan ücretsiz bir yazılımdır. Dumpit.exe uygulaması kurulum gerektirmemektedir. Çift tıklamak suretiyle çalışmakta ve varsayılan olarak çalıştırıldığı dizinde hafıza imajı dosyası oluşturmaktadır. Az seviyede proses kullanarak bellek üzerinde ki bilgilere en az oranda müdahale eden bir yazılımdır.

II. İmaj oluşturma yazılımlarının karşılaştırılması

İmaj oluşturma yazılımları da çalıştıkları sürece bellekte yer kaplamaktadır Bellek imajı oluşturmakta kullanılan yazılımlarda aranan en önemli özellik ise bellek üzerinde en az yer kaplaması olmalıdır. Bu sayede bellek üzerinde bulunan verilere en az zarar verilerek imaj oluşturulacaktır.

İmaj oluşturma yazılımların çalıştıkları sistemin belleğinde kaplamış oldukları alan miktarları aşağıda gösterilmiştir. Dumpit yazılımının bellekte kapladığı alanın az olması, kurulum gerektirmemesi ve kullanımının kolay olması nedeniyle tercih edilebilir.

Yazılımın Adı	Kullandığı Bellek Boyutu(Kb)
FTK Imager	15768
Encase v7	130528
Belkasoft Live RAM Capturer	1956
Dumpit	452

Tablo 2 - İmaj oluşturma yazılımları ve bellek kullanım miktarları

III. İmaj dosyası çevrimleri

Bellek imajı oluşturan çeşitli programlar ve bu oluşturulan imaj dosyalarını da inceleyen çeşitli programlar bulunduğundan yukarıda bahsedilmiştir. İmaj oluşturan her bir program kendine dosya uzantıları ile imaj dosyası yaratırken, inceleyecek yazılımlarda kendine özgü uzantılı dosyaları incelemektedir. İmaj dosyalarının incelenmesinde doğru ve kesin sonuçlara ulaşmak adına imaj dosyasını farklı programlar ile incelenmesini gerekebilir veya bir program ile ulaşılamayan verilere başka bir program ile ulaşılabilir. Bu durumlarda imaj dosyalarının inceleme yapılacak programın anlayacağı dosya formatına dönüştürülmesi gerekli olabilir.

Ayrıca sanal ortamda kullanılan bilgisayarlara ait belleklerin incelenmesi durumunda; ilgili sanallaştırma programına ait bellek dosyası formatının

dönüştürülmesi gerekli olabilir ve uyku modu (hibernation) aktif edilmiş kapalı durumdaki bilgisayarların bellek dosyası olan hiberfil.sys dosyasının da dönüştürülme ihtiyacı olabilir.[134]

Bu bağlamda dönüştürme işlemini yapabilen volatility ve MoonSols firmasının geliştirdiği uygulamalar bulunmaktadır. MoonSols firmasına ait uygulamalar basit anlamda kullanımı şu şekildedir.

Uygulama <kaynakdosya_türü> <dönüştürülecekdosya_türü>

Örnek kullanımları ise aşağıdadır.

- hibr2dmp.exe D:\hiberfil.sys E:\converted.raw
- hibr2bin.exe D:\hiberfil.sys E:\raw_hibernation.img
- dmp2bin.exe D:\memory.dmp E:\mem.img
- bin2Dmp.exe D:\rawformat.dmp E:\WinCrashDump.dmp

Ayrıntılı bilgi için http://www.moonsols.com/windows-memory-toolkit/ adresine bakılabilir.

Dönüştürme işleminin “Volatility” ile yapılması durumunda “Imagecopy” parametresi kullanılır. “Imagecopy” parametresi ile değişik formatlar bulunan (crashdump, hibernation, virtualbox core dump, vmware snapshot, live firewire session) imaj dosyalarını raw formata, “raw2dmp” parametresi ile de imaj dosyalarını dmp formatına dönüştürebilir. Örnek kullanımları aşağıdadır.

- volatility-2.4.standalone.exe -f win7_x64.raw raw2dmp –O copy.dmp
- volatility-2.4.standalone.exe -f hiberfil.sys imagecopy –O converted.raw

[134] Harlan CARVEY, Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 8, 4.Edition, sf.11, Elsevier Inc, USA, 2014, https://books.google.com.tr/books?id=oiqSAgAAQBAJ

IV. Bellek analiz araçları

Bellek imajı veya canlı sistemlerde hazır bulunan yazılımlar ile bellek üzerinde incelemeler yapılmaktadır. Bellek içerisinde bulunan veriler hiyerarşik bir yapıya sahip olmayıp içeriğine bakıldığında bellekte dağıtık bir şekilde bulunduğu görülmektedir. İnceleme için kullanılan yazılımlarının her birinin farklı özellikleri olmakla beraber neticede birçok noktada da aynı sonuçlara ulaşılmaktadırlar. Adli bilişim alanında öne çıkan yazılımlar ve genel özellikleri aşağıdadır.

Belkasoft Evidence Center; Belkasoft Forensics Made Easier firması tarafından geliştirilen ücretli bir yazılım olup, sabit diskte bulunan "pagefile.sys", "hiberfile.sys", sistem belleği ve imajları üzerinde inceleme yapmaktadır. Başlıca temel özellikleri;

- Facebook ve Twitter vb. sosyal ağ analizi,
- Skype, Msn gibi anlık yazıma programının analizi,
- İnternet tarayıcısı (browser) analizi,
- E-posta analizi,
- Sabit disk veya bellek üzerinde veri kurtararak çıkan verilerin analizi,
- Canlı bellek analizi,

yapabilmektedir.

Internet Evidence Finder; JADsoftware firması tarafından geliştirilmiştir. Sabit disk üzerinde "pagefile.sys" ve "hiberfile.sys" dosyaları ile birlikte sabit disk, sistem belleği ve imajları üzerinde de analiz yapmaya yarayan ücretli bir yazılımdır. Başlıca temel özellikleri;

- Bulut bilişim analizi,
- Anlık mesajlaşma analizi,
- Medya analizi,

- Mobil cihaz yedekleme dosyaları analizi,
- P2P dosya paylaşım ortamları analizi,
- Webmail incelemeleri analizi,
- Web aktiviteleri analizi,
- Web sayfası kurtarma analizi,
- Doküman verileri analizi,
- Windows işletim sistemi verileri analizi,
- E-posta uygulamaları analizi,
- Anlık mesajlaşma uygulamaları analizi,

yapabilmektedir.

Volatility; Python ile yazılmış, bünyesinde birçok aracı barındıran ücretsiz bir yazılım çatısıdır. Volatility ile imaj dosyası içerisinden öğrenilebilecek bilgilerden bazıları şunlardır;

- İşletim sistemi bilgisi,
- Bellek imajı oluşturma zamanı,
- Sistemde o anda çalışan tüm işlemlerin (process) listesi,
- O anki çalışan işlemlerin işlem ağacı şeklinde listesi,
- Sistemde bulunan aygıtların listesi,
- Sistemden dışarıya herhangi bir bağlantı olup olmadığı,
- Gizli veya kod enjekte edilmiş dll dosyaları,
- Profiller üzerinde bulunan panolardaki verileri,
- Zaman çizelgesi bilgileri,
- Konsol kabuğunu (cmd.exe) kullanarak girdikleri komutları,
- Sistemin pencereler (wire-frame diagram) şeklinde ekran görüntüsü,

Ayrıca volatility; farklı yazılımlar tarafından oluşturulmuş imaj dosyalarını, sanallaştırma yazılımlarına ait bellek dosyalarını, Hiberfil.sys ve Pagefile.sys

dosyalarını değişik bellek imaj dosya formatlarına dönüştürme yeteneğine de sahiptir.

Volatility yazılımının ücretsiz olması, esnek yapısı ile geliştirilmeye müsait olması ve imajlarının formatlarını dönüştürebilmesi gibi özellikleri ile bellek incelemelerinde tercih edilebilir.

§ 6. Sabit disk üzerinde hafıza

I. Pagefile.Sys

Bilgisayarlar fiziksel bellek alanın yetersiz olduğu durumlarda sabit diskin bir bölümünü sanal bellek olarak kullanılabilir. Sabit diskten kullanılan bu alan; Windows işletim sistemlerinde varsayılan olarak pagefile.sys dosyasında tutulmakta ve fiziksel belleğin yaklaşık 2 katı kadar büyüklüktedir. Ancak boyutu ihtiyaca bağlı olarak değiştirilebilir. Sanal bellek, fiziksel bellek azaldığında bellekte bulunan verileri pagefile.sys dosyasına taşmakta ve fiziksel bellek için boş alan oluşturmaktadır. Sanal bellek fiziksel belleğin azaldığı durumlarda bir çözüm gibi gözükmekte ancak sabit disk hızının bellek hızından düşük olması sebebiyle performans açısından bir çözüm değildir. Gerçek çözüm sisteme ilave fiziksel bellek eklenmesidir. Ancak zorunlu hallerde kullanılması gerekiyorsa ve sistemde ikinci bir disk varsa performans açısından sanal bellek dosyası bu alanda oluşturulmalıdır.

Hex Editor yazılımları ile pagefile.sys dosyası içinde kelime taraması yapılarak; belirli bir dosya uzantısı girilerek son çalışılan doküman bilgilerine, “silah” , “terörist”, “hacker” gibi belirli kelimeler taratılarak incelemeye konu olan olay ile ilgili bilgilere, sistem girilmiş kullanıcı adı ve parola bilgilerine ulaşılabildiği görülmüştür.[135] Ayrıca tıpkı fiziksel belleklerde olduğu gibi inceleme yazılımları ile çalıştırılmış programlara ait bilgilere, parolalara,

[135] Nisarg TRİVEDİ; Study on Pagefile.sys in Windows System, Gujarat Forensic Sciences University, sf.5, Mart 2014 http://www.iosrjournals.org/iosr-jce/papers/Vol16-issue2/Version-5/C016251116.pdf, E.t. 18.10.2014

şifreleme anahtarlarına, canlı haberleşme mesajlarına ve benzeri bilgilere de ulaşılabilir.[136]

Adli bilişim açısından içinde veri bulunması sebebiyle önemli ve incelenmesinin gerekli olduğu durumlarda bu dosyaya bellek imaj dosyası gibi önem verilmelidir.

II. SWAP alan

Linux sistemlerde belleğin yetersiz olduğu durumlarda kullanılan sanal bellek alanıdır. Windows sistemlerde kullanılan pagefile.sys'den farkı ise bir dosya olarak değil bir sabit disk alanı (partition) olmasıdır.

III. Hiberfil.sys

Hazırda bekleme (Hibernation) modu özellikle dizüstü bilgisayarlar için tasarlanan bir güç tasarrufu özelliğidir.[137] Hazırda bekletme modu bellekte bunan tüm bilgiyi sabit diskte bir dosyaya kaydetmekte ve bilgisayarı kapmaktadır. Böylece sabit disklerin dönmesi, anakartta bulunan fanların çalışması durdurulmakta vb. ve ekran kartı kapatılmaktadır. Windows tabanlı işletim sistemlerinde bu dosyanın adı "hiberfil.sys"dır.[138] Bu dosya belleğin birebir kopyası olarak değerlendirilmekte ve sıkıştırılmış formatta tutulmaktadır.[139] Hiberfil.sys dosyasının boyutu yaklaşık olarak bellek boyutu kadardır.

Pagefile.sys ve hiberfil.sys dosyasına sahip olmak bellek imajına sahip olmak anlamına gelmektedir. Ancak bu dosyalar üzerinde inceleme yapılmak istenildiğinde sıkıştırılmış olan formatın açılması gerekmektedir. Volatility

---

[136] Eoghan CASEY, Handbook of Digital Forensics and Investigation, sf.261-262, Elsevier Academic Press, 2010, https://books.google.com.tr/books?isbn=0080921477, E.t. 16.10.2014

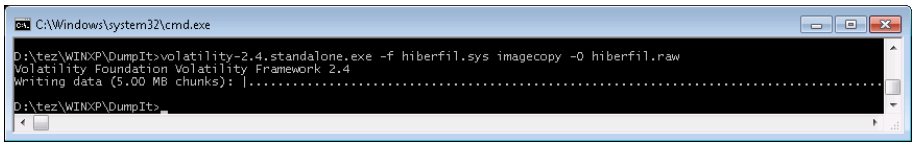
[137] Uyku ve hazırda bekleme: sık sorulan sorular, http://windows.microsoft.com/tr-tr/windows7/sleep-and-hibernation-frequently-asked-questions, E.t. 16.10.2014

[138] İnternet, ''Vikipedi Özgür Ansiklopedisi'', 2014, http://en.wikipedia.org/wiki/Hibernation_%28computing%29, E.t. 17.05.2014

[139] Halil ÖZTÜRKCİ, Adli Bilişim İncelemelerinde Hibernation Dosyası Üzerinden Hafıza Analizi, http://halilozturkci.com/adli-bilisim-incelemelerinde-hibernation-dosyasi-uzerinden-hafiza-analizi/, E.t. 17.05.2014

yazılımı bu imkanı sağlamaktadır. Volatility aracına "hiberfil.sys" dosyası "imagecopy" parametresi ile girdi olarak verildiğinde hiberfil.sys dosyası analiz edilebilecek formata dönüştürülmektedir.[140] Örnek kullanımı aşağıda gösterilmiştir.

volatility-2.4.standalone.exe -f hiberfil.sys imagecopy -O hiberfil.raw

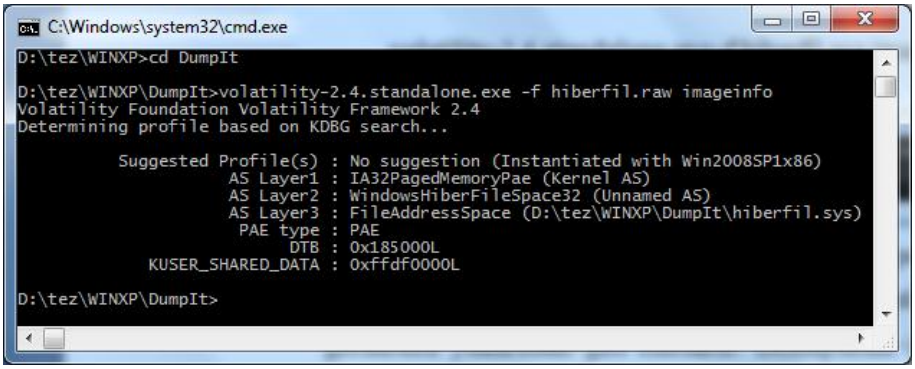


Şekil 79 - Volatility uygulamasının "imagecopy" parametresi ile çalıştırılması

Volatility yazılımı ile gerçekleştirilen dönüştürme işlemine ait ekran görüntüsü yukarıdaki gibi olacaktır. Dönüştürme işleminin başarılı bir şekilde tamamlandığının test yapılmak istendiğinde;

volatility-2.4.standalone.exe -f hiberfil.raw imageinfo

komutu kullanılabilir. Komut sonrasında çıkan sonuç incelendiğinde "hiberfil.sys" dosyasının "Windows 2008 SP1" yüklü bir bilgisayara ait olduğu görülecektir.



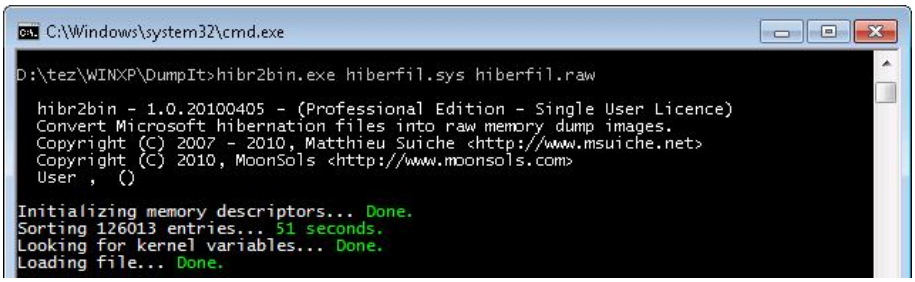
Şekil 80 - Volatility uygulamasının sistem özelliklerinin tespiti

Hiberfil.sys dosyasını inceleme yapılabilecek formata dönüştürebilmek için kullanabilecek yazılımlardan bir tanesi de Moonsols firmasının Moonsols

[140] Babak AKHGAR / Andrew STANIFORTH / Francesca BOSCO, Cyber Crime and Cyber Terrorism Investigator's Handbook, sf.86, Elsevier Inc, USA, 2014, https://books.google.com.tr/books?id=GR2kAwAAQBAJ, E.t. 16.10.2014

Windows Memory Toolkit[141] paketi içinde yer alan "hibr2bin.exe" isimli yazılımıdır.[142] Hibr2bin.exe kullanım şekli aşağıdadır.

hibr2bin.exe <input file> <output file>



Şekil 81 - Hiberfil.sys dosyasının dönüştürülmesi

Hibr2bin.exe vasıtasıyla yapılan dönüştürme işlemi sonrasında derinlemesine bellek analizi yapılabilecek dosya oluşturulmuştur.

Konunun adli bilişim yönünden incelendiğinde; karşılaşılan olay yerinde kapalı bir bilgisayar sistemi varsa kesinlikle açılmamalıdır. Bilgisayar sistemlerinin delil ihtiva etmesi muhtemel durumlarda, sistemin açılması mevcut delillerin kesinlikle ve kesinlikle zarar görmesine sebebiyet verebilecektir. Örneğin bilgisayar sistemlerinin işletim sistemleri açılırken birçok yapılandırma dosyasına erişim sağlamakta ve ileride suç delili olabilecek verilerin zarar görmesine yol açabilmektedir. Dosyaların erişim tarihleri bile bazı durumlarda delil niteliği taşıyabileceği için bu durum oldukça sakıncalıdır. Aynı zamanda işletim sistemlerinin açılırken oluşturabileceği geçici dosyalar ve geçici hafıza disk alanları daha önceden silinmiş olan veri alanlarının üzerine yazılabileceği için silinmiş verilerin delil niteliğinde kurtarılabilme olasılığını ortadan kaldırmış

[141] Yazılımın ücretsiz sürümüne (1.4) "http://www.moonsols.com/windows-memory-toolkit/" adresinden erişilebilir, E.t 01.01.2015

[142] Christiaan BEEK, From Hybernation file to Malware analysis with Volatility, http://www.slideshare.net/cfbeek72/from-hybernation-file-to-malware-analysis-with-volatility, E.t 17.06.2014

olacak ve dolayısı ile delilin bütünlüğünü bozmuş olacaktır. Bu yüzden incelemesi yapılacak bilgisayar sistemleri kapalı durumda iseler kesinlikle açılmamalıdır.[143]

Adli bilişim uzmanları incelediği/inceleyeceği kapalı durumda bulunan sistemlerin hazırda bekleme (Hibernation) modunun etkinleştirilmiş olup olmadığını mutlak suretle kontrol etmelidir. Etkinleştirilmiş ise inceleme yapılırken Hibernation dosyasını incelenerek önemli olabilecek bilgilere ulaşabileceği unutulmamalıdır.

§ 7. Sonuç

Adli bilişim çalışmaları giriş bölümünde de bahsedildiği üzere temelde 4 aşamadan oluşmaktadır. 1'nci aşama olan delil toplama çalışmalarında olay yerinde delil niteliği bulunan ve içinde veri bulunabileceği değerlendirilen tüm kaynaklar toplanmaktadır. Bu kaynaklar genellikle bilgisayar, sabit disk, USB disk, CD/DVD, fotoğraf makinesi, hafıza kartı ve benzeri donanımlar olmaktadır. Bu donanımların genel özelliklerine bakıldığında bünyesinde bulunan veriler sabit olduğu görülmektedir. Ancak veriler sadece sabit ortamlarda bulunmayıp, bazı durumlarda çalışan sistemlerde bulunan uçucu verilerde delil niteliği taşıyabilmektedir. Uçucu veriler bilgisayarlarda verilerin geçici olarak depolandığı belleklerde tutulmaktadır. Uçucu veriler enerjileri veya verinin işlendiği uygulamanın sonlandırılması ile yok olmaktadır. Ancak istisnai durumlarda yok olmadığı da görülebilmektedir. Bu nedenle olay yeri incelemelerinde belleklerde de bilgi bulunabileceği unutulmamalı ve uçucu verilerin analizlerinin yapılabilmesi için bellek imajlarının oluşturulması gerekmektedir.

Delil toplama aşamasında bellekte bulunan verilerin de olayın çözümü adına faydalı olacağı değerlendirildiğinde; öncelikle sisteme ait belleğin kopyası (imaj) oluşturulmaktadır. Böylece adli bilişimin 2'nci aşaması olan delili inceleme

[143] John ASHCROFT; Electronic Crime Scene İnvestigation: A Guide for First Responders, sf.52 Mart 2011, https://www.ncjrs.gov/pdffiles1/nij/187736.pdf, E.t. 21.08.2014

safhasında; imaj üzerinden imajın alındığı an itibari ile bellek analizi yapılmaktadır. İmaj oluşturma yazılımlarının çalıştırılması da dahil olmak üzere sistemde yapılacak herhangi bir işlemin bellekte bulunan verileri değiştirebileceği unutulmamalıdır. Bu nedenle imaj oluşturma yazılımlarının tercihinde bu hususa dikkat edilmeli; kurulum gerektirmeyen, ulaşılması kolay olan, en az komutla çalışabilecek, sisteme en az müdahale edecek ve bellekte en az yer kaplayacak yazılım kullanılmalıdır.

İmaj oluşturan yazılımlar da çalıştıkları sürece bellek bir alan kapladığı inceleme sonucunda yazılacak "adli bilişim inceleme aşamalarının 4'üncü safhası olan" raporda belirtilmelidir. Ayrıca ilgili kanunda yer almamasına rağmen delil ile ilgili ileri de meydana gelebilecek şüpheleri ortadan kaldırmak ve delil bütünlüğünün sağlanabilmesi adına oluşturulan imajın özet değeri de hesaplanarak şüpheli veya vekiline verilmelidir. Ayrıca bu işlemlerin gerçekleştirilme anı bir kamera ile kaydedilerek rapora ek yapılmalıdır.

Türk Hukukunda Adli Bilişime ilişkin hükümlerden olan CMK 134'ncü maddesinin 1'nci bendinde bilişim sistemlerinde arama yapılabilmesi için mahkeme kararı olması gerektiği belirtilmektedir. Mahkeme kararı olmadan arama ve inceleme yapılması mümkün değildir. 2'nci bendinde ise; arama sırasında delillerin şifrelenmiş olması veya içinde gizlenmiş bilgiler olması nedeniyle verilere ulaşılamaması durumunda, şifrelerin çözülebilmesi ve inceleme yapılabilmesi maksadıyla delillerden kopya oluşturmak için delillere el konulabileceği belirtilmiştir. Ayrıca şifrelerin çözülmesi ve gerekli kopyaların alınması durumunda, el konulan cihazların geciktirilmeden iade edilmesi hükmü bulunmaktadır.

Sosyal medya siteleri, e-posta sistemleri, dosya veya disk şifreleme yazılımları ve benzeri uygulamalara ait parolalar bellek incelemesi ile elde edilebilmektedir. Bu kapsamda el konulan cihazlarda bellek incelemesi yapılarak kanunda (CMK 134) ifade edilen "şifrelenmiş veya gizlenmiş bilgilerin açığa çıkarılması" sağlanabilir. Ayrıca yapılacak bellek incelemeleri adli makamlar

tarafından gerçekleştirilen ve kanunda bulunan "el konulan cihazlar gecikme olmaksızın iade edilir." hükmünün uygulanabilirliğine de katkı sağlayacaktır.

Günümüz sosyal yaşamının bir parçası haline gelen bilgisayar ve bilişim teknolojileri ile değişik suçlar işlenmektedir. Kötü niyetli veya şüpheli kişiler tarafından deliller üzerinde adli bilişim yazılımlarının başarılı bir şekilde çalışmasını engellemek ve yapılan işlemleri gizlemek için çeşitli yöntemler geliştirilmektedir. Bu yöntemlere Anti Forensic (AF) yöntemleri denilmektedir.[144] Bu yöntemlerden bir tanesi de çalışan prosesleri sabit diske hiç eriştirmeden direkt olarak bellekte çalıştırma yöntemidir. Ayrıca bazı olay yeri incelemelerinde; bilgisayarın kapanması veya açılması ile çalışan programlar (Örn. wipe ve deep freze) veya uzaktan erişim ile delillerin zarar uğratılmasının engellenebilmesi için bilgisayarların enerjisi direkt olarak sonlandırılması gerekmektedir. Bu bağlamda bahse konu AF yönteminin kullanıldığına ve/veya bilgisayar enerjisinin direkt olarak sonlandırılması gerekli olduğuna karar verildiği durumlarda sistem beleğinde bulunabilecek verilerin kaybedilmemesi için sistem bellek imajı alındıktan sonra kapatılmalıdır.

Bellek incelemesi ile uygulamaların hangi IP ve portlara eriştiği bilgisinin tespit edilebileceği, sonlandırılmış ve/veya halen açık durumda bulunan ağ bağlantılarına ait bilgilere erişilebileceği, şüpheli olduğu değerlendirilen ağ bağlantısına ait network paketlerinde ayrıntılı incelemeler yapılabileceği ve böylelikle internet veya network ortamında işlenen suçların tespit edilmesinde bellekten faydalanabileceği unutulmamalıdır.

Uyku modu aktif edilen bilgisayarların belleğinde tutulan tüm bilgiler sabit diskte bulunan "Hiberfil.sys" dosyasına aktarılmakta ve bilgisayar kapatılmaktadır. Bununla bereber "Kapalı durumda bulunan bilgisayar açılmamalıdır" hususu adli bilişimin delil toplama aşamasındaki genel kurallarından biridir. Bu nedenle kapalı durumda bulunan bilgisayarlara ait

[144] Ryan HARRIS, Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem, sf.44-49, Purdue University, Digital Forensics Research Conference Paper, 2006http://www.dfrws.org/2006/proceedings/6-Harris.pdf, E.t. 11.12.2014

incelemelerde; öncelikle sistem açılmadan (off-line) sabit disk imajı oluşturulmalıdır. Ardından sabit disk imajı içinde bulunan "Hiberfil.sys" dosyası tespit edilerek incelenmesi mutlak suretle usul haline getirilmelidir.

Bir sistemde gerçekleştirilen işlemlere ait kronoloji, zaman çizelgesi (timeline) ile çıkarılabilmektedir. Bellek imajı üzerinden oluşturulacak zaman çizelgesi ile gerçekleşmiş bir olay sırasında kullanılan yöntem, aygıt, araç ve benzeri hususların tespiti yapılabilir.

Kötü niyetli kişiler ele geçirdikleri sistemler üzerinde gerçekleştirdikleri işlemleri iz bırakmadan ve mümkün olan en kısa sürede tamamlayarak sistemden ayrılmaya çalışmaktadır. Bu amaçla yaptıkları işlemleri en seri şekilde gerçekleştirebilmek için bir ya da birkaç işlemi aynı anda ard arda hiç bir müdahale olmadan kendi kendine yapılmasını sağlayan toplu iş dosyaları (batch file) hazırlamaktadırlar. Bu dosyalar komut satırı üzerinde çalışmaktadır. Kötü niyetli işlemlerin gerçekleştirildiği tespit edilen bilgisayarda adli veya idari bir konu nedeniyle yapılacak bellek incelemesinde komut satırından yapılan bu işlemler ortaya konulabilir.

Kamu ve özel sektörde hazırlanan ve uygulanan Bilgi Güvenliği Politikalarında "Son kullanıcılar, güvenlik zafiyetlerine sebep olmamak için, bilgisayar başından ayrılırken mutlaka ekranlarını kilitlemelidir."[145] [146] gibi kurallar yer almaktadır. Ancak kilitlenmiş veya açık durumda bulunan bilgisayarların belleğine değişik yöntemler kullanılmak suretiyle (Firewire attack, Cold Boot Attack, vb.) erişilmesi durumunda bellekte bulunan bilgiler elde edilebilir. Bilgi Güvenliği Politikalarında bulunan bu kural "Son kullanıcılar,

---

[145] Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu v.1, 2014, sf.26, https://bilgiguvenligi.saglik.gov.tr/files/BilgiG%C3%BCvenli%C4%9FiPoltikalar%C4%B1K%C4%B1lavuzu.pdf, E.t. 11.12.2014

[146] Orman Genel Müdürlüğü - Bilgi Güvenliği Yönetim Sistemi Politikası, 01.10.2012, sf.9, http://www.ogm.gov.tr/ekutuphane/Dokumanlar/OGM%20Bilgi%20G%C3%BCvenli%C4%9Fi%20Y%C3%B6netim%20Sistemi%20Politikas%C4%B1.pdf, E.t. 11.12.2014

güvenlik zafiyetlerine sebep olmamak için, bilgisayarlarını kullanılmadıkları sürece ve kısa süreli bilgisayar başından ayrılma durumlarında dahi mutlak surette kapatmalıdır.” şeklinde değiştirilmelidir. Ayrıca sistem yöneticileri tarafından kullanılmayan bilgisayarların tespitini yapan ve bu bilgisayarların kapatılmasını sağlayan merkezi grup politikaları uygulanmalıdır.

Bilgisayar üzerinde bulunan firewire portu vasıtasıyla belleğe direkt olarak erişim sağlanılmaktadır. Özellikle video kameralarda bulunan görüntülerin bilgisayar ortamına aktarılması gibi yüksek kapasiteli verilerin transfer işlemleri bu yöntem ile gerçekleştirilmektedir. Firewire portlarının bu özelliği yüksek hızlarda veri transferi gibi güzel bir kolaylık sağlamakla birlikte aynı zamanda bir güvenlik zaafiyeti de oluşturmaktadır. Bu zaafiyet kullanılarak, çalışır durumda bulunan ve/veya yetkili kullanıcı haklarına sahip olunamaması sebebiyle oluşturulamayan bellek imajları, donanımsal olarak oluşturulabilir. Bu husus bellek imajı oluşturma süreçlerinde alternatif bir yöntem olarak kullanılmalıdır.

Çalışır durumda bulunan bilgisayarların bellekleri incelendiğinde; açık olan oturumlara ait yaklaşık ekran görüntüsüne (wire-frame diagram), kayıt defteri (registry) bilgilerine, çalıştırmış olduğu uygulamalara ait bilgilere, girmiş olduğu internet adreslerine ve bu adresleri ulaşmak için kullanılan kullanıcı adı ve parola bilgilerine, komut satırından girilen komutlara, aktif veya sonlandırılmış ağ bağlantısı bilgilerine, panoda bulunan verilere ve benzeri birçok bilgiye erişilebildiği görülmüştür. Bu kapsamda; belleklerden bu ve benzeri bilgilerin elde edilebilir olduğu düşünüldüğünde, bilişim cihazlarından delil elde etme süreçlerine bellek incelemeleri de mutlak surette dahil edilmelidir.