CYBER DILIGENCE, INC.
575 UNDERHILL BLVD. SUITE 209
SYOSSET, NY 11791
(516)342-9378

10 Mayıs 2010

Av. Celal Ülgen
Üsküdar Caddesi, URAS İş Merkezi
No: 18 Kat:5, Daire:11
Kartal, İstanbul / TÜRKİYE

YALKIN DEMİRKAYA'NIN UZMANLIK GÖRÜŞÜ

I. Uzman vasıfları

1. Ben Cyber Diligence, Inc. kuruluşunun Ekim 2004'ten beri Genel Müdürüyüm. Aynı zamanda sahibi olduğum Cyber Diligence, Inc., yüksek teknoloji alanında bilgisayar adli tıp ve soruşturmalarında uzman bir kuruluştur.

2. New York Polis Teşkilatı'nda (NYPD) Dahili Araştırmalar Bölümü'nde Bilgisayar Suçları Soruşturma Birimi'nin kurucusu ve Şube Müdürü olarak görev yaptım. New York Polis Teşkilatı'nda Ocak 1995'den emekliye ayrıldığım Ocak 2007 tarihine kadar Bilgisayar Suçları Soruşturma Birimi'nde bilgisayar suçları tahkikatı yürüten ve adli tıp tetkikleri yapan kişileri eğittim, mentorluğunu yaptım ve idare ettim.

3. Bilgisayar suç soruşturmaları ve bilgisayar adli tıp tetkikleri alanlarında hizmet veren Digital Services, Co.'nun kurucusuyum. Bu şirketin, kurulduğu 1996 yılından, Cyber Diligence, Inc. halini aldığı 2004 yılına kadar tek ortağıydım.

4. Hem Kamu hemde özel iş kariyerimde, medeni ve ceza hukuku alanlarında yüzlerce bilgisayar suç soruşturması ve bilgisayar adli tıp tetkiki yürüttüm ve yönettim.

5. 2004'te ve 2006'da New York Polis Teşkilatı için Bilgisayar Suçları Soruşturması Eğitim ve Bilgisayar Adli Tıp Eğitim Programları hazırladım ve Teşkilat'taki personeli bizzat eğittim.

6. Bilgisayar eğitimim 1981'de üniversitede başladı ve 1984'te bilgisayar programcısı ve sistem tasarımcısı olarak çalışmaya başlamamla profesyonel düzeye erişti. New York Polis Teşkilatı'nda bilgisayarla ilişkim katıldığım ilk tarihten bu teşkilattan emekliye ayrıldığım 2007 senesine kadar devam etti.

7. Polis Bilimleri dalında bir lisans diplomam ve Ceza Hukuku dalında Bilgisayar Bilimi uzmanlığıyla bir Master diplomam var.

8. Belli başlı tüm adli tıp yazılım imalatçıları tarafından eğitim aldım: "Encase" üzerine Guidance Software tarafından, "FTK" üzerine AccessData Corp. tarafından, "NTI Suite and Foreign Language Threat Detection" üzerine New Technologies, Inc. tarafından, "ProDiscover Incident Response" üzerine Technology Pathways tarafından ve "LiveWire Incident response software suite" üzerine Wetstone Technologies tarafından eğitim gördüm. Aynı zamanda "Certified ProDiscover Incident Response" üzerine eğitim verip müfettiş sertifikası verme yetkisine sahibim.

9. Stevens Üniversitesi'nin lisansüstü programında misafir öğretim üyesi olarak 2005 ve 2006 Güz dönemlerinde Bilgisayar Adli Tıp konusunda dersler verdim.

10. A.B.D. Milli Güvenlik Kurumu tarafından verilmiş Bilgi Güvenliği Denetleyicisi Sertifikam var.

11. Sertifikalı bir Bilgisayar Adli Tıp Denetleyicisi ve Sertifikalı Dijital Adli Tıp Pratisyeniyim.

12. Cyber Diligence, Inc. şirketinin bilgisayar adli tıp uzman tanıklık hizmetleri için saatlik ücreti $450 ve giderlerdir.

13. Çetin Doğan, aile fertleri, ve Çetin Doğan'ı temsil eden hiç bir avukatla bir ilişkim yoktur. Bu vaka ve vakayla ilgili şahıslardan ilk defa Bn. Pınar Doğan'ın beni telefonla araması vesilesiyle 7 Mayıs 2010 Cuma günü haberim oldu.

14. Bu vaka hakkında soruşturma yapmış uzmanlarla hiç bir ilişkim yoktur.

15. Özgeçmişim ektedir.

II. Giriş

Avukat Celal Ülgen, bu vaka ile ilgili iki bilirkişi raporunu değerlendirmem için başvuruda bulunmuştur. Söz konusu raporlardan ilki 19 Şubat 2010 tarihli TÜBİTAK'ın Bilirkişi Raporu olup, Erdem Alparslan, Tahsin Türköz ve Dr. Hayrettin Bahşi tarafından yazılmıştır. Bu rapor bundan sonra TÜBİTAK Bilirkişi Raporu olarak adlandırılacaktır. İkinci rapor ise 26 Mart 2010 tarihli Kara Kuvvetleri Komutanlığı'nın Bilirkişi Raporu olup, Mu. Alb. Yavuz Fildiş tarafından yazılmıştır. Bu rapor ise bundan sonra Askeri Bilirkişi Raporu olarak adlandırılacaktır.

Öncelikle belirtmeliyim ki, dijital kanıtlar (yani sözkonusu CD'ler) üzerinde doğrudan bir tetkik yapmadan, CD'ler ile ilgili bir uzman görüşü bildirmem mümkün değildir. Celal Ülgen'in talebi doğrultusunda, iki raporu analiz ederek bu raporların bütünlüğü ile raporda sunulan argümanların geçerliliği hakkında kanaatimi oluşturdum. Bu rapor ile bu kanaatlerimi içeren uzmanlık görüşümü bildireceğim.

III. Bilgisayar Adli Tıp Bilimi, Dijital Kanıt ve "Geçmiş Tarih Atma" Uygulamaları Konularında Genel Açıklamalar

Bilgisayar Adli Tıp Bilimi, dijital kanıtların tespiti, saklanması, toplanması, analizi ve raporlanması bilimidir. Uygulayacılarının sadece bilimsel konularda değil, aynı zamanda dedektiflik disiplinlerinde de bilgi ve eğitim sahibi olmaları gerekir. Teknik donanıma, dedektiflik tecrübesi ve ileri derecede teknik uzmanlık eğitiminin de eşlik etmesi gerekir.

Bilgisayar Adli Tıp terminolojisinde sık kullanılan bir terim olan "metadata," bu gibi vakalarda özel bir öneme sahiptir. Metadata, veri hakkında veri anlamına gelir. İki ana tip metadata vardır: Dosya Sistem metadatası ve Uygulama metadatası. Soruşturmayı yürütenlerin ve mahkemenin bu kavramın önemini anlaması bir zorunluluk teşkil etmektedir.

a. Dosya Sistem Metadatası: Bilgisayar işletim sistemi tarafından verilen bir dosyanın hakkındaki bilgiler. En önemlilerinden bir tanesi ise Windows İşletim sisteminin dosyaya tayin ettiği üç zaman damgasıdır; biz bilgisayar adli tıp alanında buna "MAC" (Modified, Accessed, Created) zamanı deriz.

1. Dosya Oluşturuma: Bu dosyanın ***şu anda bulunduğu yerde*** oluşturulduğu tarih ve saat.
2. Son değiştirilme: Bu dosyanın en son değişitirildiği tarih ve saat.
3. En son erişilim: Bu dosyaya en son erişildiği tarih ve saat.

Bu "Zaman Damgaları"nın üçü de bilgisayarların sistem saatinden alınır. Eğer sistem zamanı doğru ise bu damgalar doğrudur. Eğer sistem zamanı (kasıtlı olarak sistem zamanının değiştirilmesi dahil) herhangi bir nedenle yanlışsa, bu zaman damgaları da yanlış olur.

b. Uygulama Metadatası: Dosya sistem metadatasına ek olarak, bazı yazılım uygulamaları kendi metadatasını oluşturur. Örneğin, Microsoft Word yazılımı, dosya sisteminden daha ayrıntılı olan kendi metadatasını sağlar. Bilgisayar sistem zamanının yanlış olduğu durumlarda, doğal olarak bu sistem üzerinde çalışan uygulama yazılımlarının (örn., Microsoft Word) oluşturduğu "Zaman Damgaları" da yanlış olur. Ayrıca, "Yazar" gibi diğer alanlar da kullanıcı tarafından kolayca değiştirilebilir.

c. Geçmiş Tarih Atma: Geçmiş Tarih Atma (Antedating), dokümanları yaratıldıklarından daha önceki bir tarihten gecerli kılma uygulamasını tanımlayan bir terimdir. Dijital dokümanları yaratıp, belirli bir bilgisayardan, belirli bir kullanıcı tarafından ve belirli bir zamanda yaratılmış gibi göstermek son derece kolaydır. Bunun

için bütün yapılması gereken, bilgisayar saatini istenen zamana ayarlamak, bilgisayara istenen zamanda geçerli olan işletim sistemini yüklemek, ve yükleme sırasında istenen şirket, kullanıcı adı vs, gibi isimleri tanımlamaktır. Eğer dikkatlice yapılırsa, hiç bir adli tıp incelemesi sözkonusu dokümanın sahte olduğunu, sadece içerdiği metadataya bakarak ispat edemez. Dilenirse, bu uygulamayı göstermek icin mahkemeye, istenen herhangi bir kişi adına, istenen herhangi bir zaman (geçmiş ya da gelecek) ve istenen herhangi bir suç unsuru içeren bir dosya oluşturabilirim. Bunu yapmak için fazla bir teknik donanıma sahip olmak gerekmez, ve bu suç herhangi biri tarafından işlenebilir.

Dolayısıyla, dijital kanıtın nasıl elde edildiği, sözkonusu kanıtın içeriğinden daha fazla önem taşır. Bir dokümanın orijinalliği, diğer ilgili faktörler dikkate alınmaksızın ve sadece metadatanın incelenmesiyle, hiç bir koşulda saptanamaz.

IV. TÜBİTAK Bilirkişi Raporu

19 Subat 2010 tarihli, Erdem Alparslan, Tahsin Türköz ve Dr. Hayrettin Bahşi tarafından hazirlanmis TÜBİTAK'ın Bilirkişi Raporunu okudum.

TÜBİTAK Bilirkişi raporu ve rapora eşlik eden dokümantasyon üzerinde yaptığım analize mütakip, hem genel olarak bu raporun yeterliliği hakkında, hem de raporu hazırlayanların Bilgisayar Adli Tip incelemesi ile Dijital Doküman Doğrulama alanlarındaki yeterlilikleri hakkında ciddi çekincelerim oluştu. Bu raporun içeriği, bende, raporu hazırlayanların bilgisayar adli tıp eğitimi almadıkları ve bilgisayar adli tıp incelemesi tecrübesine sahip olmadıkları kanaatini oluşturdu. Metadatanın adli tıp uygulamalarında geçerli olmayan araçlarla elde edilmiş olması, ve bu şekilde elde edilen metadatanın gerçek olarak kabul edilmesi mazur görülemez. Bu tip bir kanıtın ne kadar kolay bir sekilde imal edilebileceğinden bahsedilmemesi ve bariz çarpıklıklara işaret edilmemesi, bende bu raporu hazırlayanların bilgisayar adli tip uygulamalarında gerekli teknik bilgiye, yeteneğe ve tecrübeye sahip olmadıkları kanaatini oluşturdu.. Potansiyel bir bilgisayar suçu incelemesinde, bilgisayar bilimi hakkında bilgi sahibi olamak, adli tıp incelemesi için tek başına yeterli değildir.

V. Askeri Bilirkişi Raporu

Ordu Komutanlığı Askeri Savcılığı'nın görevlendirdiği Mu.Alb. Yavuz Fildiş tarafından 26 Mart 2010 tarihinde hazırlanan Bilirkişi Raporunu, okudum.

Sözkonusu raporda aktarılan inceleme, bu çeşit vakaları soruşturmada geçerli olan bilgisayar adli tıp uygulamaları ile tutarlı görünmektedir. Rapor, incelemeyi yapanın temel bilgisayar adli tıp kavramları ve uygun soruşturma yöntemleri hakkında bilgili olduğunu göstermektedir. İncelemeyi yapanın profesyonelce bir soruşturma yürüttüğü, ve TÜBİTAK Bilirkişi raporundaki tutarsızlıkları doğru bir şekilde saptadığı görülüyor. Ayrıca yine doğru olarak, bir belge üzerinde çok kolay bir şekilde sahtecilik yapılabileceğine, sahte belge imal edilebileceğine işaret ediyor.

VI. Sonuç

1. İki raporun analizi ve bu soruşturmayla ilgili olguların ışığında vardığım kanı, Mu.Alb. Yavuz Fildiş tarafından hazırlanmış raporun soruşturma teknikleri açısından uygun olduğudur.

2. Erdem Alparslan, Tahsin Türköz ve Dr. Hayrettin Bahşi tarafından hazırlanmış raporda ise kanımca hatalı bir yaklaşım izlenmiştir. Söz konusu rapor, kişilerin hürriyetleri ile itibarlarının mevzubahis olduğu bu denli önemli bir dava için sorumsuz eksiklikler sergilemektedir.

2.a. Bu raporda, Sayın Fildiş'in bilikişi raporunda da dikkati çektiği ve belgelerde sahteciliğe işaret eden bulgular tamamen gözardı edilmiştir.

2.b Kaldı ki, söz konusu CD'lerde sahteciliğe işaret eden bu bulgular yer almasaydı dahi, sadece metadata üzerinden yapılan bir inceleme ile bu CD'lerdeki belgelerin gerçek olduğu sonucuna varmak mümkün olmazdı.

3. Eldeki delillerin kaynağı ve teknik yöntem, soruşturma ve usül açısından tüm çarpıklıklar göz önünde bulundurulduğunda, bu belgelerin sahte olması muhtemeldir ve herhangi bir yargı sürecinde kullanılmaları son derece sakıncalıdır.

Yalkın Demirkaya

Ek 1

YALKIN DEMİRKAYA

Yalkın DemirkayaSoruşturmacı Dedektif ve Dedektif Ekip Amiri olarak 20 yıllık polis tecrübesine sahiptir. Bilgisayar Suçları Soruşturma Şubesi Müdürü olarak edindiği tecrübesinin yanısıra, Sayın Demirkaya New York Polis Teşkilatının (NYPD) Dahili İşler Bölümü'nün Baş Bilgi Güvenliği Müdürü olarak da hizmet vermiştir. Sayın Demirkaya kamu sektörunde dahili soruşturmalar için tahsis edilmiş ilk bilgisayar suçları soruşturma birimini kurma sorumluluğunu üstlenmiştir. Sayın Demirkaya dahili bilgisayar suçlarını soruşturma alanında yöntemleri geliştirmede öncülük etmiş ve bu yöntemleri mükemmelleştirmiştir. "White hat hacker" olarak 29 yıllık biligisayar tecrübesi vardır. New York Polis Teşkilatı'nda Dahili Araştırmalar Bölümü'nün Bilgisayar Suçları Soruşturma Birimi'nin kurucusu ve Şube Müdürü olarak görev yapmıştır.

Dahili bilgisayar suçları soruşturmaları konusunda dünyanın önde gelen uzmanlarından olan Sayın Demirkaya, bilgisayar suçları alanında yöntemlerin ve soruşturma usullerinin geliştirmesine katkıda bulunmuştur. Müşteri kurumlar için hayati tehlike arzeden yüksek düzeyde sanayi casusluklarını soruşturmakta geniş tecrübesi vardır. "Fortune 500" şirketlerinin sanayi casusluk davalarında başarılı soruşturmalar ve delil toplama işlemleri gerçekleştirmiştir. Sayın Demirkaya polis teşkilatları için olduğu gibi hukuk, iş dünyası ve akademik camia için de danışmanlık yapmıs, konuşmalar vermiştir. Bilgisayar Güvenliği, Bilgisayar Suç Soruşturması, Bilgisayar Adli Tıp ve Elektronik Korunma konularında dersler vermiştir.

Sayın Demirkaya'nın Polis Bilimleri dalında bir lisans diploması ve Ceza Hukuku dalında Bilgisayar Bilimi uzmanlığıyla bir Master diploması vardır. A.B.D. Milli Güvenlik Kurumu tarafından verilmiş Bilgi Güvenliği Denetleyicisi sertifikası vardir. Sertifikalı bir Özel Detektif (NYS#11000141778), Sertifikalı bir Bilgisayar Adli Tıp Denetleyicisi ve Sertifikalı bir Dijital Adli Tıp Pratisyenidir.

İş Tecrübesi

2004 – bugüne:
Genel Müdür, Cyber Diligence, Inc.

1995 – 2007:
Şube Müdürü, New York Polis Teşkilatı (NYPD), Dahili İşler Bölümü, Ceza Araştırmaları ve Bilgisayar Suçları Soruşturma Birimi

1996 – 2004:
Kurucu ve Şirket Sahibi, Digital Services, Co.

1994 – 1995:
Devriye Amiri, New York Polis Teşkilatı (NYPD), Devriye Hizmetleri Bölümü

1993 – 1994:
Soruşturma Detektifi, New York Polis Teşkilatı (NYPD), İstihbarat Analiz Birimi, Organize Suçlar Kontrol Bölümü

1988 – 1993:
Uzman Detektif, New York Polis Teşkilatı (NYPD), Teknik Destek Birimi, Bölüm Başkanı Ofisi

1987 – 1988: Polis Memuru, New York Polis Teşkilatı (NYPD), Devriye Hizmetleri Bölümü

1982 – 1987:Bilgisayar Programlayıcısı/Danışmanı

Eğitim

- MA (Master), Ceza Hukuku, Bilgisayar Uzmanlığı, John Jay College of Criminal Justice, CUNY. 1989

- BS (Magna Cum Laude), Polis Bilimleri, John Jay College of Criminal Justice, CUNY. 1986

Sertifikalar

- Digital Forensics Certified Practitioner, DFCB, National Center for Forensic Science, Cert # 210-39-135
- Certified Computer Forensic Examiner, New York Police Department
- Certified Information Security Assessor, United States National Security Agency
- Certified ProDiscover Forensic Examiner, Technology Pathways
- Certified Wetstone Investigator
- Licensed Private Investigator NYS # 11000141778
- Master Linguist (Türkçe)

Bilgisayar Adli Tıp Eğitimi

- Hacking Bootcamp, Exploits and Live Incident Investigation. Ekim 2009
- AccessData, Forensic Tool Kit – Windows Vista Forensics. Ağustos 2007
- Technology Pathways, Certified ProDiscover Forensic Examiner. Mayıs 2007
- AccessData, Forensic Tool Kit – Internet Forensics. Subat 2006
- Guidance Software, Encase Intermediate Analysis & Reporting. Haziran 2004
- NYPD, Computer Forensics Course. Ağustos 2006
- AccessData, Forensic Tool Kit – Advanced Windows Forensics. Aralık 2004
- NYPD, Computer Crimes Investigations Course. Nisan 2004
- NTI, Computer Forensics Training Course. Şubat 2002

- NTI, Computer Forensics NTFS Training Course. Şubat 2002

Ders verme tecrübesi

- Eğitmen, Certified ProDiscover Forensic Examiner (CPE) Kursu
- Kurucu ve Baş Eğitmen, Computer Forensics Kursu, NYPD
- Misafir Eğitmen, Computer Forensics and Network Forensics, Stevens University Graduate School, Güz 2005 ve Güz 2006 donemleri.
- Kurucu ve Baş Eğitmen, Computer Crimes Investigation Kursu, NYPD
- Baş Eğitmen, Bilgisayar Adli Tıp Kursu, Turk Emniyet, İstihbarat Bölümü, 2006.
- Eğitmen, Computer Crime & Computer Forensics Kursu, Suffolk County Police Department (2004)
- Eğitmen, Computer Crimes Investigations Course, New Rochelle & White Plains Police Departments (2003)
- Misafir Eğitmen, Computer Forensics, NYU Continuing Studies (2002)
- Misafir Eğitmen, "Computer Crime" Fordam University (2002)
- Eğitmen, "Network Forensics", Techno Forensics 2007 Annual Symposium
- Workshop eğitmeni, "Computer Crimes Investigations", 1997 International CompStat Conference.

Komiteler, vb.

- Üye, Industry Advisory Board, Polytechnic University
- Hakim, CSAW 2007, 2008 & 2009 Computer Forensic Challenge, Polytechnic University.
- Üye, State of Wisconsin, Department of Justice, Governor's Cyber Terrorism Advisory Board (2004)
- Danışman, Chronicle Solutions, Network Forensics
- Danışman, Computer Associates, eTrust Network Forensics

Diğer

- Konuşmacı, ACFE/USIUD, Use of Technology on Internal Fraud Investigations Istanbul, Turkey (2008)
- Konuşmacı, FBI/Infraguard, High Level Internal Threats (2008)
- Özel Konuşmacı, Purdue University, CERIAS – 8th Annual Information Security Symposium (2007)
- Konuşmacı, FBI/Infraguard, Computer Network Forensics (2007)
- Özel Konuşmacı, CA Symposium on Network Forensics – Kiev Ukraine. 2006
- Keynote Konuşmacı, Information Systems Security Association (ISSA), 11th Annual Conference & Exhibition
- Keynote Konuşmacı, Stevens University, MOT Symposium: Guarding Your Business from Cyber Attack.
- Panelist, TechXchange, Columbia University (2003)

- Konuşmacı, Financial Fortress Leadership Group (2002, 2007)
- Misafir, Technogenesis TV, "Cybersecurity – Guarding Your Business in the Post 9-11 Reality" program (2002)
- Özel Konuşmacı, New Jersey Institute of Technology, Cyber Terrorism and Industrial Espionage (2005)
- Konuşmacı, The Association for Women in Computing, "Computer Crime" (2006)
- Konuşmacı, Association of Certified Fraud Examiners, 2004 Fraud Seminar
- Özel Konuşmacı, Employee ROI, Executive Symposium, Homeland Security & Corporate Governance (2003)

Yayınlar

- Katkıda bulunan yazar, "Guarding Your Business: A Management Approach to Security", Kluwer Academic Publisher, 2004
- Katkıda bulunan yazar, "Cyber-Crime Fighter" Newsletter, April 2003