Journal of Yaşar University
http://joy.yasar.edu.tr

KABLOSUZ AĞLARDAKİ PAKET TRAFİĞİNE ADLİ BİLİŞİM YAKLAŞIMI

Tuncay ERCAN*
Doğukan NACAK**

Özet

Kablosuz ağların açık ortam özelliği veri trafiğinin kolaylıkla kontrol edilebilmesini sağlar. "Packet analyzer" isimli uygulamalar kullanarak ele geçirilen veri paketlerinin belli esaslar doğrultusunda analiz edilmesiyle hem ağ yöneticileri, hem de ağ trafiği konusunda uzman olan adli bilişim uzmanları bu paketler üzerinde farklı değerlendirmeler yapabilir. Böyle bir inceleme adli soruşturma maksatlı da kullanılabilir. Paket inceleme OSI katmanları içinde özel bir yer tutar ve pasif olarak birçok bilginin elde edilebilmesi imkanını sunar. Böylece hem uygulama bazında (web ve elektronik posta), hem de istihbarat bilgisi (yasak siteler, lisanssız yazılım, suç olabilecek eylemler) taşıyacak şekilde farklı parametrelere göre değerlendirme yapılır. Bu çalışmada "Wireshark" uygulaması ile açık erişimli kablosuz bir ağda yaklaşık bir dakika süresince toplanan bin adet paket üzerinde inceleme yapılmış ve farklı kullanıcılar ve uygulama çeşitlerine göre örnek bir değerlendirme sunulmuştur.

Anahtar Kelimeler: "Packet Analyzer", Adli Bilişim, Veri trafiği, Adli Ağ İncelenmesi, Wireshark.

Abstract

The feature of open environment in wireless networks causes data traffic can easily be controlled. Both network managers and the experts of network forensics can make different evaluations with the analysis of these packages caught from the network traffic, by using tools like "packet analyzer". Such an evaluation may also be used for a judicial inquiry. The analysis of packages reserve a special place among OSI layers and give the opportunity of

* tuncay.ercan@yasar.edu.tr

** dogukan.nacak@yasar.edu.tr

handling passively a lot of useful information. So, an evaluation of both application-based (through web and emails) and intelligence-based (banned web sites, unlicensed software, illegal actions) can be done according to the different parameters. In this study, an analysis of one thousand packages collected in a WLAN environment by the "Wireshark" tool in about one minute period has been done and presented a sample evaluation for different users and application types.

1. Giriş

Bilgisayar sistemlerine yönelik saldırılar bu amaçla kullanılan araçların hızla gelişmesi ve yaygınlaşması sonucunda artmakta ve bu nedenle bilgi güvenliği kavramı tüm sektörlerde önem kazanmaktadır. Birçok kurum günümüzde, bilgi güvenliğinin önemini kavramış ve bu sebeple değişik koruma yöntemlerine başvurmuştur. Güvenlik duvarları, anti-virüs yazılımları, nüfuz tespit sistemleri, açıklık tarayıcıları (port scanner) ve şifreleme araçları gibi teknolojilerin tamamı bilginin güvenliğini sağlamak amacına yöneliktir. Bir ağda neler olup bittiğini anlamanın tek yolu, ağ üzerinde akan trafiği ve bileşenlerini kritik noktalarda sürekli olarak ölçmek ve ölçülen bu değerleri daha eski olanlarla karşılaştırmaktır. Bu ölçümler yanlış giden birşeylerin varlığı kadar kaynak gereksinimlerinin azaldığı ya da odaklandığı noktaların belirlenmesini de sağlar (Kömür ve Ayfer, 2006).

Çok fazla bilişim suçu ile karşılaştığımız günümüzde, yargı ve güvenlik makamları için resmi bilgi/kanıt olacak şekilde, bilişim sistemleri üzerinde inceleme yapılması önem taşımaktadır. Bu yüzden adli bilişim incelemesi yapılacak tüm bilişim cihazları, her bir olay için mutlaka delil niteliği taşıması ve olayla ilgili izleri de üzerinde bulundurabileceği düşüncesi ile oldukça hassas bir biçimde incelenmelidir (Dalyanda, 2006). Ağ üzerinden elde edilebilecek bu bilgilerin uzman kişiler tarafından detaylı olarak değerlendirilmesi ve ortaya çıkarılan sonuçların kullanıcılara gösterilmesi bile, onların kişisel gizliliklerinin böyle bir ortamda ne kadar gözler önünde olduğunu göstermek açısından önemlidir.

Bu çalışma ile artık eğitim terminolojisine girmiş olan sayısal adli bilişimin teknolojinin gereği olan bilgisayar ağları ortamına nasıl uygulanabileceği konusunda bir inceleme yapılmıştır. Sistem yöneticileri tarafından bilgisayar ağlarında kullanılan anahtar, yönlendirici, modem, güvenlik duvarı ve girişim tespit cihazları gibi donanımsal ürünlerin

yanında, kazandırılan internet erişim imkanı da günümüzde artık adli bilişim için önemli araştırma alanlarından biri haline gelmiştir. Ağ ortamları gibi farklı kullanıcıların biraraya geldiği ortamlarda (akademik çalışmaların önem kazandığı üniversite ağları) mevcut kaynakların yanlış ve hatalı kullanımları kişileri ciddi adli sorumluluklarla karşı karşıya bırakabilir.

1.1. Ağ Trafiği ve Adli Bilişim

HTTP, HTTPS, POP, SMTP, Telnet, SSH gibi farklı ağ trafiği çeşitleri üzerinden toplanabilecek farklı bilgiler vardır. İnternet trafiği ve elektronik posta mesajları gibi bilgiler ağ trafiğinden sorumlu sistem yöneticileri için önemlidir. Ağ üzerinden toplanan verilerin farklılığı inceleme esnasında analizciler için olumsuz bir hassasiyet yaratabilir. TCP yönlendirmesi, "proxy" sunucular, paket yönlendirmeleri, web ve e-posta isimleri, IP (Internet Protokol) adresi ve e-posta adresi ele geçirme, oturum engelleme, DNS yanıltma gibi uygulamalar bu duruma örnektir (Casey, 2004b; Nikkel, 2005).

Ağ trafik bilgisi ağ yönetimi açısından olduğu kadar, kullanıcıların hangi sitelere girdikleri, hangi resimleri indirdikleri gibi bilgiler gerektiğinde yasal soruşturmalar için de kullanılabilir. Benzer donanım ve yazılım ürünleri bu iki farklı amaç için kullanılabilirken, detaylı bir analiz için farklı değerlendirmeler yapılmalıdır. Bir suçlunun arkasında işlenilen suçla ilgili delil bırakması son derece doğal olduğundan, bilişim sistemleri ile işlenilen suçlarda suç ile ilgili kanıtlar farklı şekil ve formatlarda suç sonrasında adli kanıt olarak tespit edilebilmektedir (Ekizer, 2008). Adli Bilişim uzmanlarının çoğu farklı donanım ve yazılım konularında yetkili iken (Kessler ve Fasula, 2007), bilgisayar ağları trafik incelemesi genel de ağ ve sistem yöneticileri tarafından yapılmaktadır. Ağ trafiği konusundaki uzman adli bilişim uzmanlarının ağ üzerinde kullanılan ürünlerin yönetiminden ziyade genel olarak aktif ve pasif paket incelemesi yapan ürünlerde kendilerini geliştirmesi ve bilgi sahibi olması daha önemlidir.

1.2. Önceki Çalışmalar

Ağ trafiği üzerinde elde edilen paketlere ilişkin verilerin analizi, bilgisayar veya diğer taşınır/taşınmaz her türlü sayısal veri kaynağında yapılan adli analizlerden farklıdır. Bir bilgisayar veya başka depolama kaynağındaki bilgiler (RAM üzerindeki bilgiler hariç),

cihazlar kullanılmadığı zaman hala incelenebilir durumdayken, ağ üzerindeki bilgiler devamlı olarak değişmektedir. Canlı bir ağ analizi, sadece belli bir zamana ilişkin trafiğin yakalanarak (snapshot) daha sonra detaylı olarak incelenmesi ile gerçekleşebilir. Aynı trafiği daha sonra elde etmek ve aynı sonuçları çıkaracak şekilde incelemek imkansızdır. (Casey ve Stanley, 2004; Nikkel, 2005; Shanmugasundaram ve diğerleri, 2006).

Kullanılan "packet analyzer" uygulamaları ne olursa olsun ağ trafik bilgisinin bir adli bilişim uzmanı tarafından değerlendirilmesi 1) ağ üzerinde bulunan bütün sunuculardaki her türlü bilgi, 2) sadece belirli bir incelemeye yönelik bilgiler (tek kullanıcının web istekleri, elektronik postaları gibi), 3) girişim tespit cihazlarında olduğu gibi sadece saldırı olarak tanımlanacak alarm bilgileri, 4) tek başına anlam ifade etmeyen ancak diğer bilgilerle beraber analiz edildiğinde önemli olan bilgiler, olmak üzere dört farklı grupta yapılabilir (Jones ve diğerleri, 2006).

Bu konuda daha önce yapılan çalışmaların büyük bölümünde, kullanılan donanımsal ürünlerin yanısıra Unix/Linux temelli komutlar üzerinde durulmuş ve herbirinin detayları açıklanmıştır. Bu makalenin ikinci bölümünde kampüs ağları üzerinde gerçekleştirilebilecek bir ağ analizinin altyapısı açıklanmış, üçüncü bölümde mevcut teknolojilerden biri olan "wireshark" paket analizörü tanıtılarak, toplanan verilere uygulanabilecek en temel incelemeler hakkında kısa bilgi verilmiştir. Son bölümde yapılan incelemelerin ağ yöneticilerine ve bu konuyla ilgili ders alan öğrencilere kazandırdığı hususlar açıklanmıştır.

2. Ağ Trafiğinin İncelenmesi

Bilgisayar ağları üzerinde yapılan inceleme ile çalışan uygulamalar, hizmetler ve kullanıcılar yanında, kullanıcılar hakkındaki bazı ilave bilgilere (işletim sistemi, web browser, kullanıcı cihazlarına ait diğer yazılım ve donanım bilgileri) de erişme imkanı sağlanabilir. Ağ üzerindeki inceleme neticesinde erişilebilecek bilgiler şunlardır:

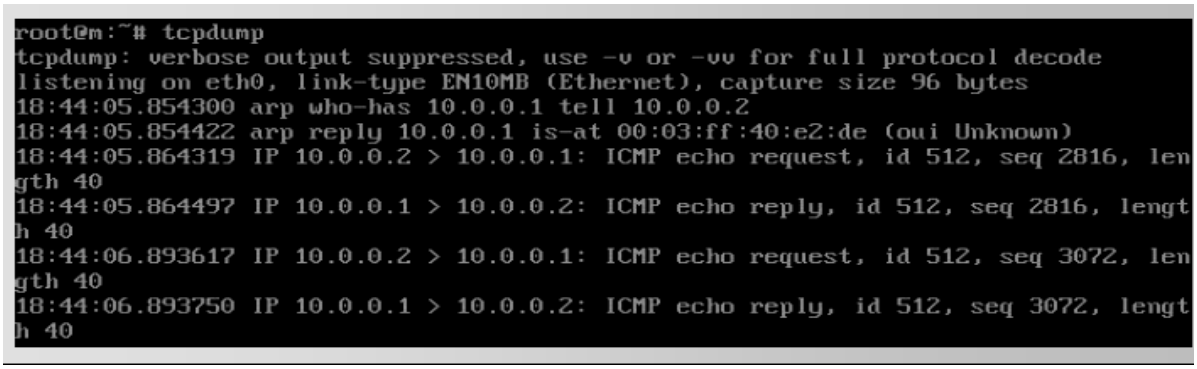
- Ağ topolojisi ve altyapısı,
- Ağdaki muhtelif kaynaklara erişim durumları,
- Bağlı olunan diğer ağlara yetkisiz geçişler

Ayrıca, kullanıcı bilgisayarı ve diğer hafıza içeren elektronik birimler yanında ağ ortamındaki farklı iletişim protokolleriyle ağdaki sunucularda bulunan kayıtlı dosyalara (açık

veya şifreli) erişimler, erişim şifreleri ve kullanıcı adları, e-posta ve anlık iletişim (chat) kayıtları, sistem kayıtları ve sistem üzerindeki yazılımlar, dökümanlar, resimler, ses ve video dosyaları ile diğer her türlü veri taşıdıkları anlam ve bilgilere göre adli kanıt olacak şekilde değerlendirilebilir (Uzunay, 2005). "Network forensics" olarak isimlendirilen, bilgisayar ağları üzerindeki trafiğin adli bilişim yönünden incelenmesi konusunda, aktif ve pasif olmak üzere iki farklı metod kullanılır.

2.1. Pasif Yöntemler

Ağ analizi birçok sayısal araştırmacı için yeni bir alandır. "Sniffing" gibi ağ trafiğini dinleyerek veya "protocol analyzer" gibi uygulamalarla ağ üzerinde değişik protokollerle (ARP, CDP, RIP, OSPF) gönderilen paketleri toplamak mümkün olabilir. Paket izleyiciler, bilgisayar ağları ile ilgili olaylarda ağ konusundaki uzman adli bilişim uzmanlarının kullandığı araçlardandır (Kent ve diğerleri, 2006). Unix/Linux işletim sistemindeki "tcpdump", en çok bilinen "sniffer" (ağ analiz ve dinleme) programı/komutudur (Şekil 1). Bu programlar, kurulduktan sonra izlemek istedikleri ağa bağlanarak belirtilen IP numarası, port numarası gibi unsurlara bağlı olarak çalışırlar ve kullanıcı bilgisayarından gönderilen ve alınan TCP/IP veya diğer paketlerin görüntülenmesine imkan verirler (MEGEP, 2008).



Şekil 1: tcpdump komutu

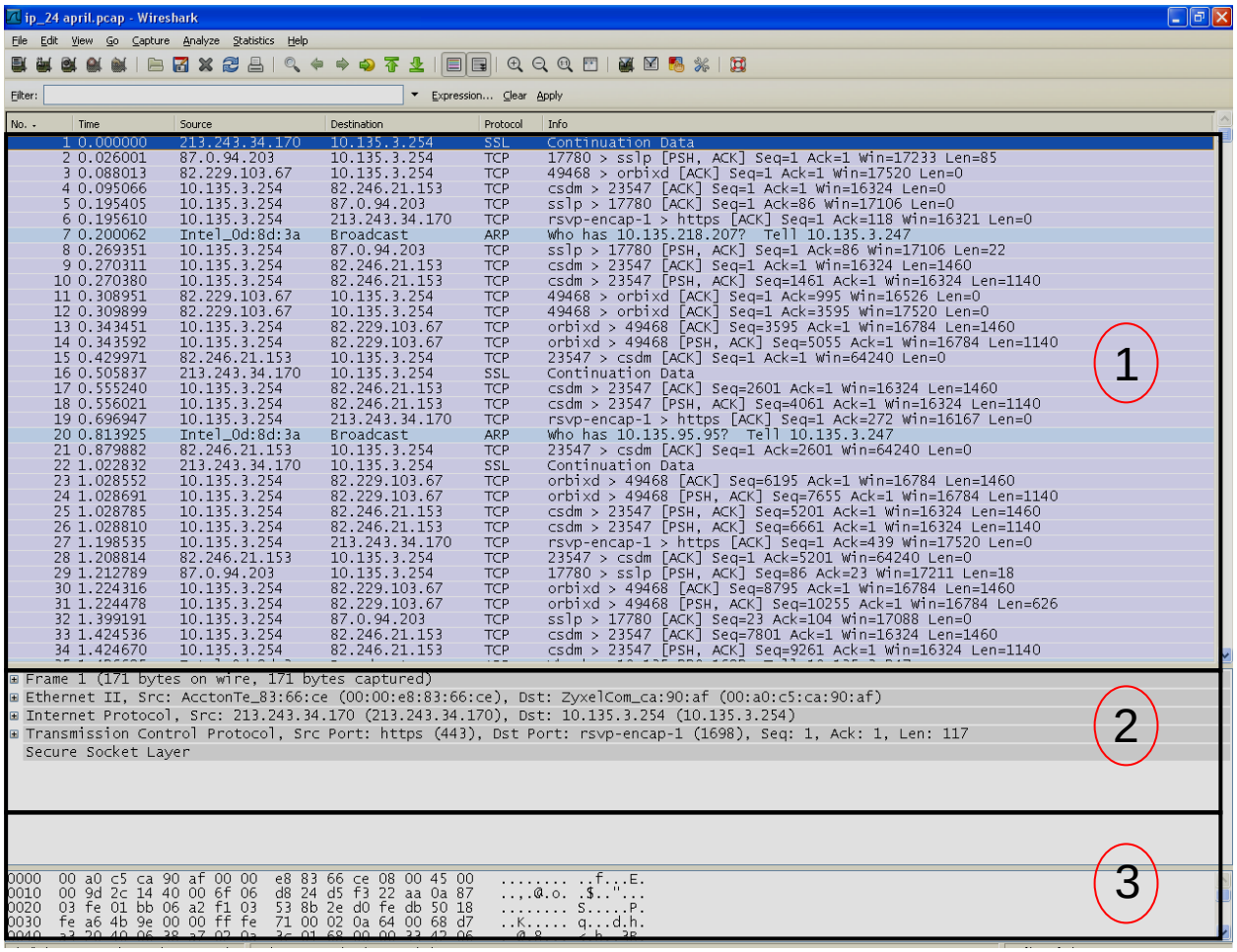
"Ethereal", Unix/Linux ve Windows platformları için ücretsiz, açık kaynak kodlu bir trafik analiz programıdır. Bizim çalışmamızda kullandığımız Wireshark, Ethereal'in yeni versiyonu olup aynı grafik arayüzü ile çalışır ve kablolu/kablosuz ağ kartları üzerinden tüm anlık TCP/IP mesajlarını veya daha önceden yakalanmış bir ağ trafiğini kaydedilen dosya üzerinden inceleme imkanı verir (Şekil 2). Mesajlar ile ilgili olarak farklı seçeneklerde filtreleme özellikleri kullanarak, mesaj yığınları içerisinden istenilen bilgileri elde etme olanağı sağlanmıştır. Kullanıcı interaktif bir şekilde incelenen veri hakkında ayrıntılı bilgi alabilir (Anuk, 2008; MEGEP, 2008).

2.2. Aktif Yöntemler

Ağ üzerindeki bütün kullanıcıları teker teker sorgulamak suretiyle adresleri ve çalıştırdıkları uygulamalar hakkında bilgi toplanabilir. Bu amaçla kullanılabilecek birçok komut ve uygulama vardır. Örneğin "***ping, traceroute, nmap ve nessus"*** komutları belirli parametrelerle bu amaç için kullanılabilir. Aktif metodlar ağ üzerinde kullanılan protokollere göre gruplandırılır. Bunlardan birisi olan ***"port scanning"*** en iyi bilinen ağ sızma tekniklerinden (bağlantı noktası taraması) birisidir. Hem TCP hem de UDP protokolleri, kullanıcıların oturumlarını ve çalıştırdıkları servisleri tanımlamak için port numaralarını kullanır. Bir IP adresi ve port numarası ile uzak kullanıcılara ait aynı çeşit bilgiler istemci ve sunucu arasında belirlenebilir (örneğin, 22 numaralı port ile SSH (Secure Shell) uygulaması).

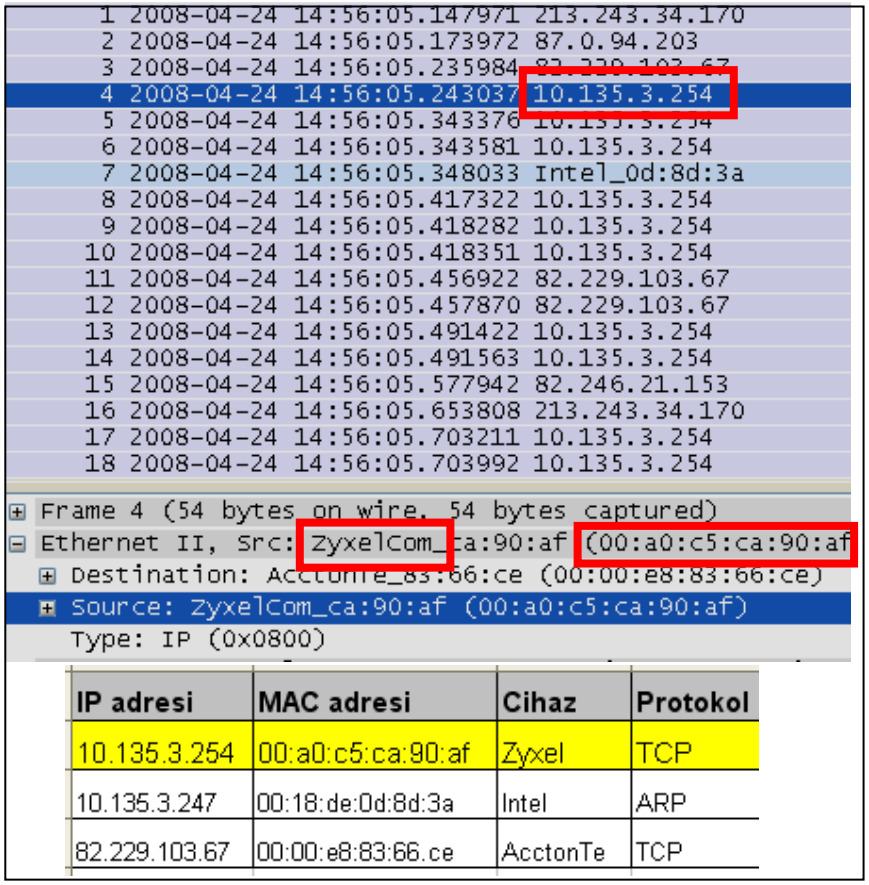
3. Ağ Paketlerinin Toplanması ve Analizi

Wireshark'ın yakalanan paketleri kaydedebilme, kaydedilen paketleri analiz edebilme, bunun yanında diğer sniffer programları ile yakalanan paketleri okuyabilme, filtreleme esnasında istenilen protokolleri istenilen renkte gösterebilme gibi temel ve kullanım kolaylığı sağlayan özellikleri vardır. Arayüz yatay olarak 3 bölüme ayrılmıştır: 1. bölüm, yakalanan paketleri; 2. Bölüm, seçili paketin ayrıntılı teknik özelliklerini ve kullandığı protokolleri; 3. bölüm ise yakalanan paketin içeriğini göstermektedir (MEGEP, 2008; Wireshark, 2008).



Şekil 2. Analiz için kullanılacak Wireshark dosyası

İncelememizde yaklaşık 20 adet Wi-Fi özellikli Laptop bilgisayarın bulunduğu, 2 farklı erişim noktası olan bir kablosuz laboratuvar ortamında, 35 saniye süreyle wireshark programı çalıştırılmış ve 1119 adet farklı paket toplanarak detaylı analizimize esas olacak şekilde dosyalanmıştır (Şekil 2). İnceleme için gerekli olan en önemli veriler ağ üzerinde bulunan bilgisayarların IP adresleri, MAC adresleri ve mümkünse kullanılan ağ cihazlarının tespitidir. Bu bilgilerle yakalanan bütün paketler için Şekil 3'deki gibi düzenli bir listeleme yapılarak, ayrıntılı filtre uygulamalarıyla istenilen bilgilere ulaşılabilir.



Şekil 3: Analiz Listesi

Ağ trafiğini etkileyen DoS atakları ağ ortamında kullanıcıların beklenilen hizmetleri almasını engelleyen en önemli saldırılardan birisidir. Çalışmamızda topladığımız paketler kendi Wi-Fi kartımız tarafından toplanan verilere ait olduğu için DoS ataklarına rastlamadık. Ancak Şekil 4'deki paket verileri böyle bir saldırıyı örneklemektedir. Burada "Doggie.example.edu" isimli bir sunucu tarafından 192.0.2.7 numaralı adrese her 10 ve 51 saniyede birer ICMP (Ping komutları) paketi gönderilerek ağda yoğun bir trafik yaratıldığı görülmektedir (Kessler ve Fasula, 2007).

```
12:03:36.016502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
12:03:46.016502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
12:04:37.016502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
12:04:47.006502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
12:05:38.016502 doggie.example.edu > 192.0.2.7: icmp: echo reply (DF)
```

rŞekil 4: DoS örneklemesi

Ağ ortamında bulunan istemci ve sunucular arasındaki paket alışverişleri (çalışmamızda elde edilen TCP:1078, ARP:38, SSL:41, DNS:3) belirlendikten sonra belirli veriler aktif yöntemlerle detaylı olarak değerlendirilir. "*nmap*", sistem yöneticilerinin açık portları bularak ağdaki kullanıcılar ve sunucular arasında hangi servislerin çalıştığını saptamakta kullandıkları bir komuttur. UDP, TCP, FTP, ICMP, ACK gibi servisler ile birlikte hedef işletim sistemini saptayabilir. "#**nmap -sV -p 22,53,110,143 10.135.3.0-255**" komutu ile kendi 10.135.3.0 ağımızdaki mevcut 254 adres üzerinde sırasıyla SSH, DNS, POP3 ve IMAP servisleri için TCP taraması yapılır. Böylece ilgili paketlerin hangi uygulamalara ait olduğu tespit edilebileceği gibi, SYN/ACK mesajlarının durumları incelenmek suretiyle ilgili paketlerin iletişime başlama paketi mi, kurulmuş bir bağlantı paketi mi, yoksa iletişimi sonlandırma paketi mi olup olmadığı anlaşılabilir (Uzunay, 2005). Daha sonra iletişimdeki bütün paketlerdeki sıra ve onay numaralarının takibi ile bazı konularda ipuçları edinilebilir.

Ağ üzerindeki IM (Instant Messaging) mesajlama paketleri de (Şekil 5) tespit edilip başka araçlarla detaylı inceleme yapılabilir (Wireshark, 2008). Örneğin bir MSN sohbeti esnasında karşı tarafa gönderilen bir dosyanın alındığı anda oluşan FTP/HTTP servisi tespit edilerek karşımızdaki hattın IP adresi tespit edilebilir (Casey, 2004a).

Source	Destination	Size	Protocol	Summary
192.168.1.14	207.46.108.83	105	MSNP	ANS 89 jujurius@msn.com 1115371039.15845 17069658
207.46.108.83	192.168.1.14	98	MSNP	IRO 89 1 1 cecile260992@hotmail.com choupi
207.46.108.83	192.168.1.14	65	MSNP	ANS 89 OK

Şekil 5: Mesaj trafiği örneği

4. Sonuçlar

Bu makale ile kampüs ağlarında sistem/ağ yöneticilerinin karşılaştıkları ağ trafiği ile ilgili problemlerde, profesyonel olarak sorgulama yapabilecekleri belli başlı komut ve araçlar tanıtılmış ve adli bilişim açısından analiz edebilecekleri durumlar özetlenmiştir. Güvenlik ve ağ sorunları hep varolacağına göre, ağ yöneticileri oluşan sorunları çözmek için güvenlik konusundaki güncel bilgileri sürekli olarak takip etmek zorundadırlar. Ayrıca ağ mimarisi ve güvenliği ile ilgili ders alan öğrenciler bu çalışma ile kendileri için birer uygulama örneği olabilecek Ethernet, TCP, UDP ve IP gibi temel ağ konularında adli bilişimin hedeflediği

hususları daha kolay öğrenebileceklerdir. Genel olarak açıklanan "wireshark" programı ile:

- Ağ yöneticileri ağ problemlerini sorgulayabilecekler,
- Güvenlik sorumluları kendi konularında geniş bir uygulama alanı bulabilecekler,
- Öğrenciler ağ protokolleri ve içerikleri konusundaki eğitimlerini pekiştireceklerdir.

Bu şekilde gerçek zamanlı uygulamalar kullanarak karşılaşılan ağ problemleri hakkında tahmin yapmak yerine, bizzat toplanan veri üzerinde çalışılarak daha doğru bir değerlendirme yapılabilir. Paket toplama öncesi ve sonrasında gelişmiş filtreleme metodlarıyla analize derinlik kazandırılır. Bu şekilde elde edilen bilgiler ağ yöneticilerinin veri trafiği akışını optimize etmelerini ve ağ tıkanıklarından kaçınmalarını sağlayacaktır.

5. Kaynakça

ANUK, E., (2008), *Güvenlik Araçları*, http://www3.itu.edu.tr/~orencik/sectools.pdf.

CASEY, E. (2004a), *Digital Evidence and Computer Crime, Forensic Science, Computers, and the Internet,* 2nd ed., Elsevier Academic Press, Amsterdam.

CASEY, E. (2004b*), Network Traffic as a Source of Evidence: Tool Strengths, Weaknesses, and Future*
Needs, Digital Investigation, 1(1): p.28-43.

CASEY, E., & Stanley, A. (2004), *Tool Review -- Remote Forensics Preservation and Examination*
Tools, Digital Investigation, 1(4): p.284-297.

DALYANDA, M., (2006), *Adli Bilişim ve Bilişim Suçları – 1 (Digital Forensics & Cyber Crimes*),
http://www.dalyanda.com/wp-content/uploads/2006/05/MehmetDalyanda_DigitalForensics & CyberCrimes-1_Nisan2006.pdf.

EKİZER, A.H. (2008). *Adli Bilişim - Computer Forensics,* http://www.bilgisayarpolisi.com/ index.php?sayfa=makaleoku &kategori=11&id=135.

JONES, K.J., Bejtlich, R., & Rose, C.W., (2006), *Real Digital Forensics: Computer Security and Incident*
Response, Addison-Wesley, Upper Saddle River, NJ.

KENT, K., Chevalier, S., Grance, T., & Dang, H. (2006), *Guide to Integrating Forensics Techniques into*
Incident Response, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-86, NIST, Computer Security Division, Information Technology Laboratory, Gaithersburg, MD. http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf, December 4, 2006.

KESSLER, G.C., & Fasula, M., (2007), *The Case for Teachıng Network Protocols to Computer Forensics Examiners,* Center for Digital Investigation.,

KÖMÜR, Y.S., Ayfer, C.A., (2006), *Linux ile Ağ Yönetimi*, XI. "Türkiye'de İnternet" Konferansı, 21-23 Aralık 2006, TOBB Ekonomi ve Teknoloji Üniversitesi, Ankara.

MEGEP, (2008), *Mesleki Eğitim ve Öğretim Sisteminin Güçlendirilmesi Projes*i, Bilişim Teknolojileri, Ağ Güvenliği (Yazılım), Milli Eğitim Bakanlığı, Ankara.

NIKKEL, B.J. (2005), *Generalizing Sources of Live Network Evidence*, Digital Investigation, 2(3): p.193-
200.

SHANMUGASUNDARAM, K., Brönnimann, H., & Memon, N. (2006), *Integrating Digital Forensics in Network Infrastructures*, in *Advances in Digital Forensics*, Proceedings of the

IFIP International Conference on Digital Forensics, eds. M. Pollitt & S. Shenoi, Springer, New York.

UZUNAY, Y., (2005), *Bilgisayar Ağlarına Yönelik Adli Bilişim (Network Forensics),* Adli Bilişim Çalıştayı 2005, İzmir Yüksek Teknoloji Enstitüsü, İzmir

WIRESHARK, (2008), *Wireshark User's Guide,* http://www.wireshark.org/

6. Yabancı Kelimeler ve Kısaltmalar

ARP : Address Resolution Protocol (Adres Çözümleme Protokolü)
MAC : Medium Access Control
CDP : Cisco Discovery Protocol (Cisco ürünleri Keşif Protokolü)
RIP/OSPF : Ağ yönlendirme Protokolü
OSI : Open Systems Interconnection-Açık sistemler Mimarisi
DoS : Denial-of-service
DNS : Alan adı sistemi veya sunucusu
TCP : Transmission Control Protocol
UDP : User Datagram Protocol
IMAP : Internet üzerinde elektronik posta transfer protokolü
HTTP : Hyper Text Transfer Protocol
HTTPS : Şifreleme sağlayan HTTP
POP : Elektronik posta alma protokolü
SMTP : Simple Mail Transfer Protocol
SSH : Emniyetli uzaktan erişim protokolü
SYN/ACK : Synchronize Acknowledge- Sunucunun SYN mesajına verdiği cevap
Telnet : Uzaktan erişim protokolü