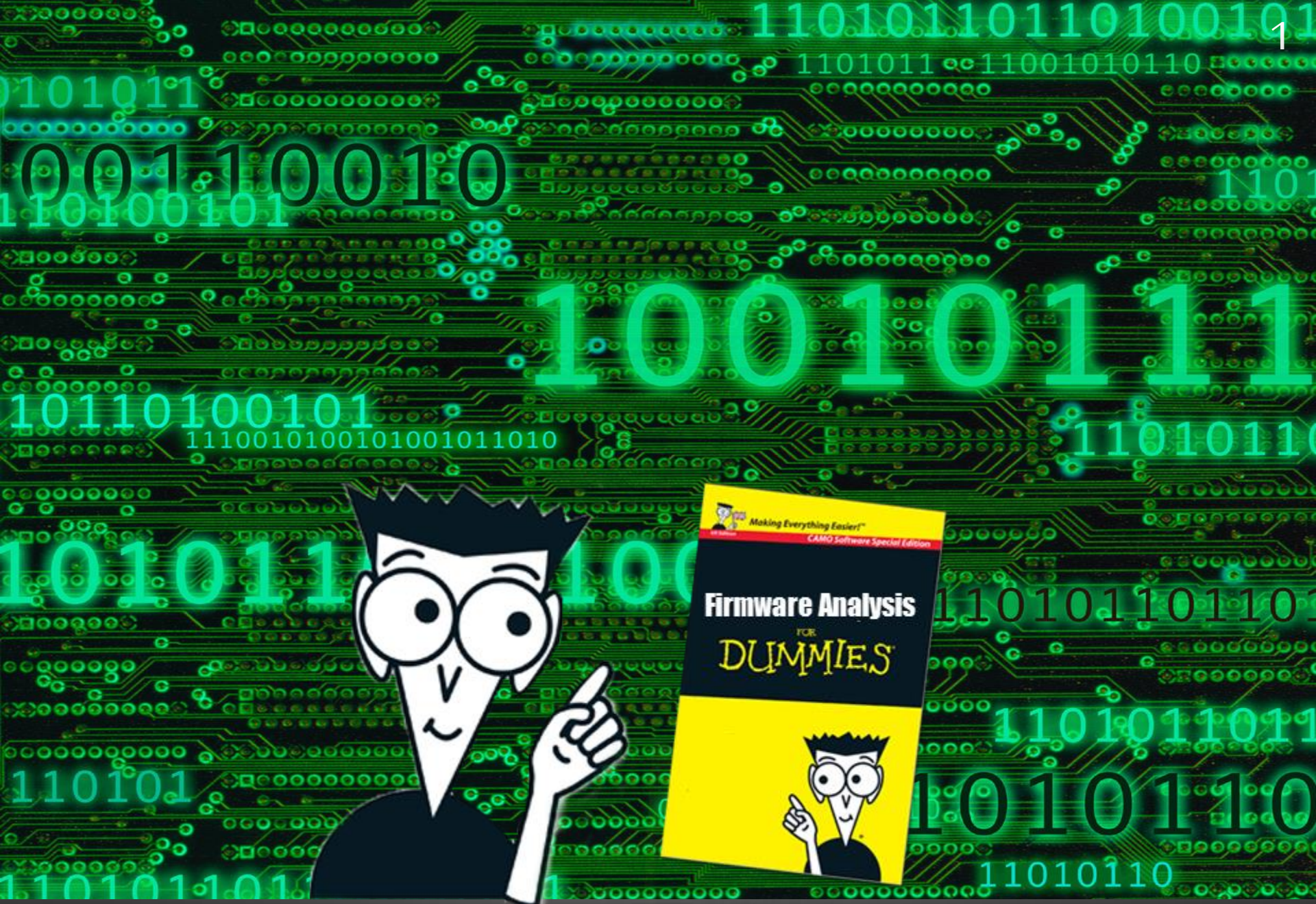

Making Everything Easier!™
CAMO Software Special Edition
Firmware Analysis
FOR
DUMMIES

İÇERİK

Donanım yazılımı (firmware) nedir ?

Neden analiz edilmelidir ?

Analiz yöntemleri ve araçları

Örnek analizler

Sonuç

BEN KİMİM?

Sızma Testi Uzmanı	**Mesai saatlerinde**
Zararlı Yazılım Analisti	**Mesai saatlerinde ve boş zamanlarımda**
Öğretim Görevlisi	**Bahçeşehir Üniversitesi Siber Güvenlik Yüksek Lisans Programı**
Blog Yazarı	**https://www.mertsarica.com**
Güvenlik TV	**http://www.guvenliktv.org**
Sertifika Kolleksiyoncusu	**CISSP , SSCP , OSCP , OPST , CREA, CEREA**

MESLEĞİM

Finans sektörünün ihtiyaçlarına ve günün teknolojilerine uygun hizmetler sunan, ürünler meydana getiren, NBG Grup şirketlerinden Finansbank'ın Bilgi Teknolojileri iştiraki olan IBTech firmasında Kıdemli Sızma Testi Uzmanı olarak çalışmaktayım.

http://www.finansbank.com.tr **http://www.ibtech.com.tr**

DONANIM YAZILIMI NEDİR VİKİ ?

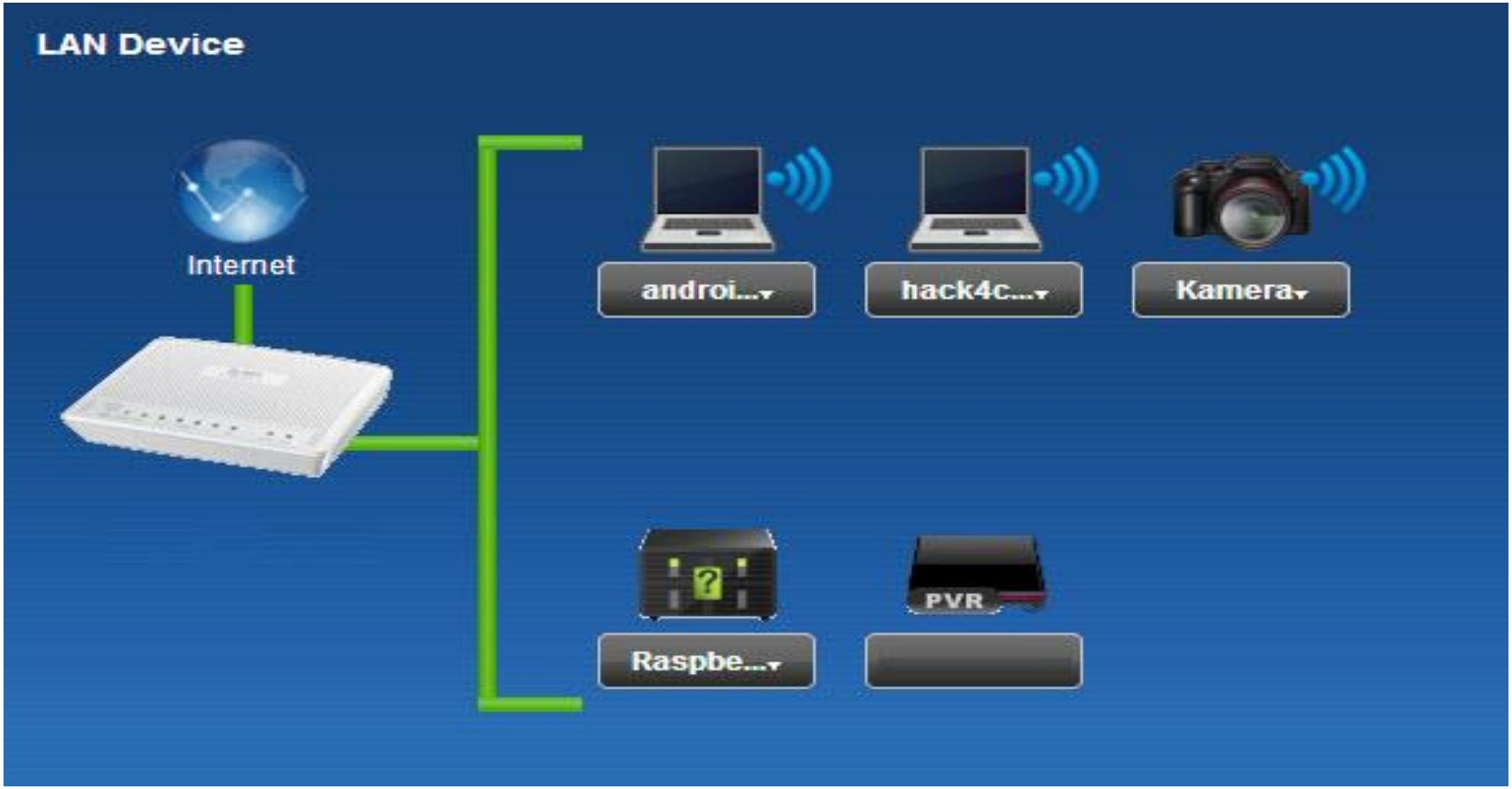
Donanım yazılımı

Vikipedi, özgür ansiklopedi

Donanım yazılımı (veya **bellenim**) (İng: firmware), sayısal veri işleme yeteneği bulunan her tür donanımın kendisinden beklenen işlevleri yerine getirebilmesi için kullandığı yazılımlara verilen addır. Elektronikte ve bilişimde donanım yazılımı, kalıcı bellek, program kodu ve veri deposudur. Donanım yazılımının bulunduğu cihazlara tipik örnekler; (beyaz eşya, elektronik saat, trafik lambaları gibi) gömülü sistemler, bilgisayar çevre birimleri, cep telefonu, dijital fotoğraf makinesi verilebilir. Bu cihazlarda bulunan yazılım, cihazın kontrol programını barındırır. Donanım yazılımı ROM, EPROM, flaş bellek gibi kalıcı bellekte saklanır. Bir cihaz yazılımının değiştirilmesi, cihazın ömrü boyunca ya hiç yapılmaz ya da sadece birkaç kez yapılır. Bazı cihazların yazılımları üretim aşamasından sonra değiştirilemez. Donanım yazılımında güncelleştirme ya yazılım hatası ya da cihaza yeni bir özellik eklemek için yapılır. Bunun için mikroçip ROM'u değiştirilmesi gerekebilir veya flaş belleğin özel bir yöntemle tekrar programlanması gerekir. Bilgisayardaki BIOS yazılımı yalnızca, cihazın temel işlevlerini saklar, işletim sistemi gibi yüksek seviye yazılımlara ön ayak olur.

Donanım yazılımları genellikle kullanılan mikroişlemcinin komut seti ile yazılmış olan yazılımlardır. Bazı mikroişlemci kontrollü elektronik donanımların yazılımları; olası hata ve eksikliklerin giderilmesi veya güncel gereksinimlerin karşılanabilmesi gibi amaçlar ile yenilenebilir.

DONANIM YAZILIMLARI



NEDEN DONANIM YAZILIMI ANALİZİ ?

Güvenliğiniz için

Zafiyet araştırması için

Ödül programları (bug bounty) için

Merakınızı gidermek için

NEDEN DONANIM YAZILIMI ANALİZİ ?

OCTOBER 14, 2013

Backdoor found in D-Link router firmware

Advisory (ICSA-14-073-01) More Advisories

Siemens SIMATIC S7-1500 CPU Firmware Vulnerabilities

Original release date: March 14, 2014 | Last revised: March 17, 2014

Print Tweet Send Share

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

redirect attacks as well as privilege escalation. The vulnerabilities could be exploited over the network without authentication.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

ANALİZ YÖNTEMLERİ

Statik Analiz:

Şifreler, gizlenmiş sayfalar, arka kapılar vb. bulunabilir.

Binwalk, firmware-mod-kit, strings, file vb. araçlar ile donanım yazılımı statik olarak analiz edilebilir.

Dinamik Analiz:

Zafiyet analizi / doğrulaması yapılabilir.

JTAG ile donanım cihazı hata ayıklayıcı ile analiz edilebilir.

UART üzerinden işletim sistemine bağlantı kurulabilir.

QEMU ile OS üzerinde yer alan dosyaları analiz edilebilir.

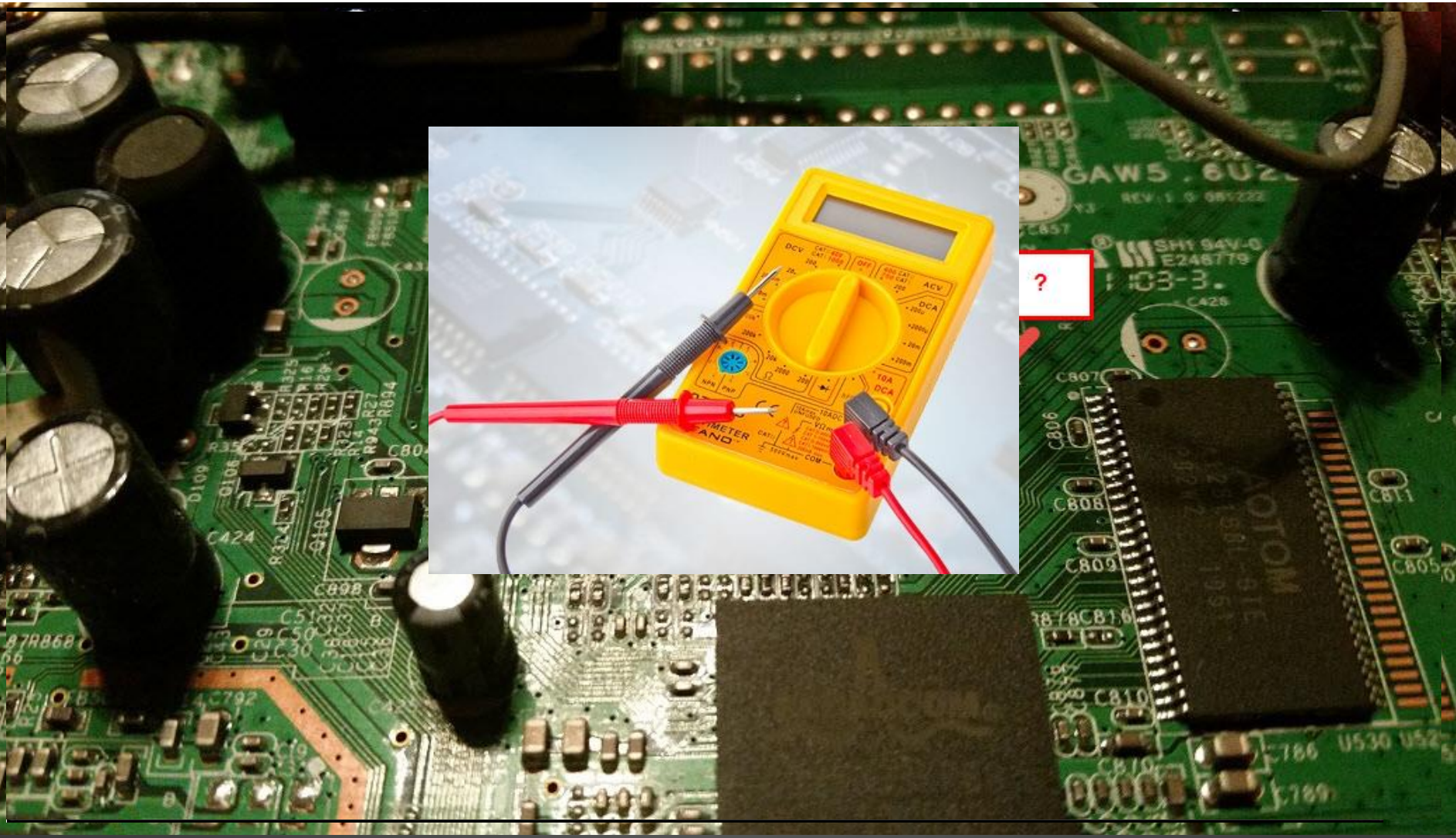
ÖRNEK #1 - DİNAMİK ANALİZ

Evinizde kullandığınız modeminizin ne kadar güvenli olduğunu öğrenmek için güvenlik araştırması yapmaya karar verdiniz.

Telnet ile modeme bağlanıp, OS üzerindeki programlarda arka kapı arayacaksınız fakat telnet şifresini bilmiyorsunuz.

İhtiyaç listesi: Tornavida seti, ana kart üzerinde UART girişi, USB - TTL UART CP2104 çevirici, Putty veya SecureCRT, Dijital Avometre

ÖRNEK #1 - DİNAMİK ANALİZ



ÖRNEK #2 - STATİK ANALİZ

Evinizde kullandığınız modeminiz ile ISS'inizin, TR069 yönetim protokolü üzerinden haberleştiğini öğrendiniz.

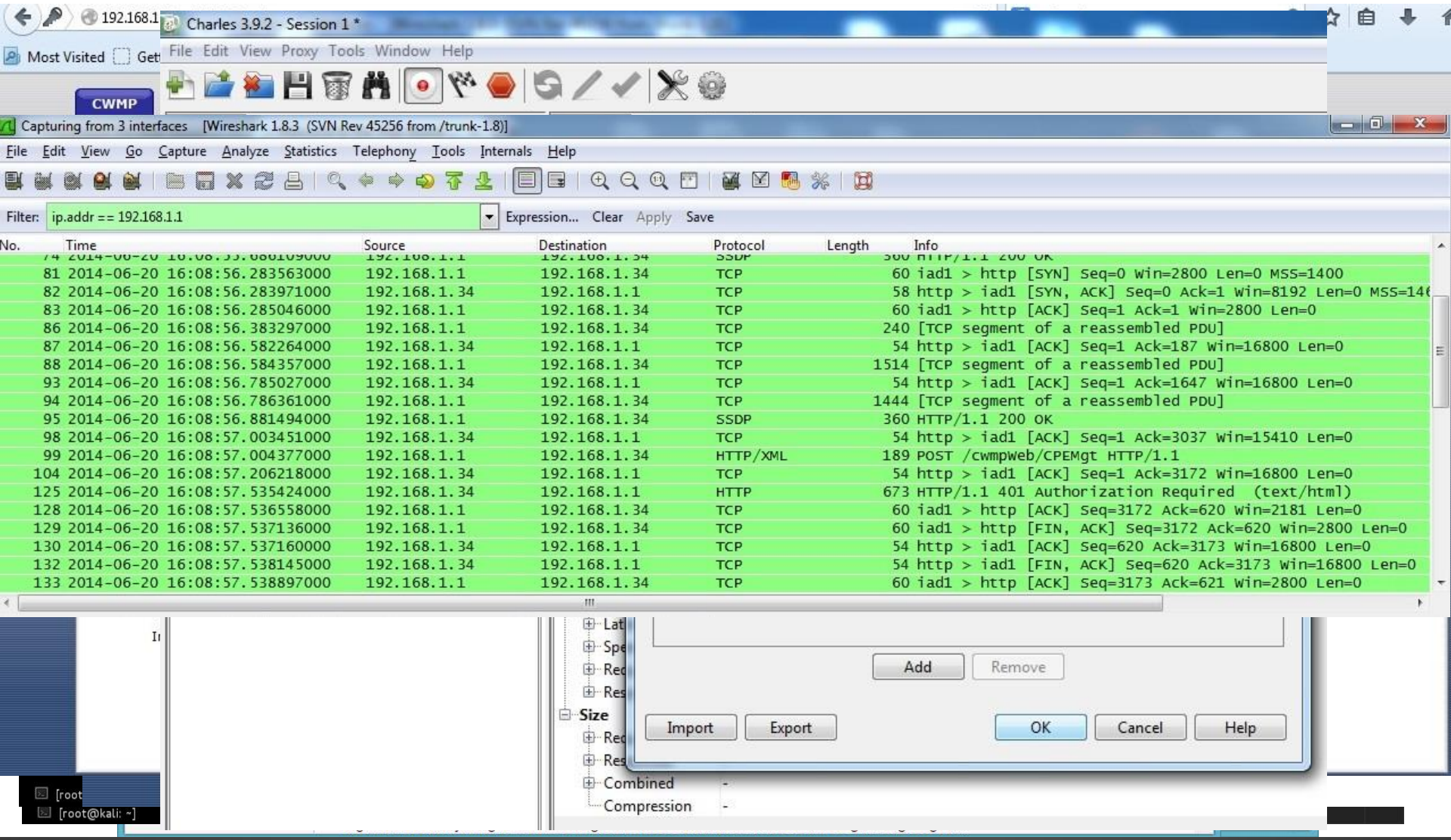
Peki bu protokol üzerinden gelen/giden parametreler neler ?

İletişim, güvenli bir kanal üzerinden mi gerçekleşiyor?

Sorular, sorular aklınızdaki sorular ve yanıtları için;

İhtiyaç listesi: Charles veya Burp Suite Proxy, donanım yazılımı, binwalk, strings

ÖRNEK #2 - STATİK ANALİZ



ÖRNEK #3 - STATİK & DİNAMİK ANALİZ

ISS'inizin hediye modem kampanyasından faydalanarak bir modem aldınız ve bu modem ön tanımlı ISS ayarları ile geldi.

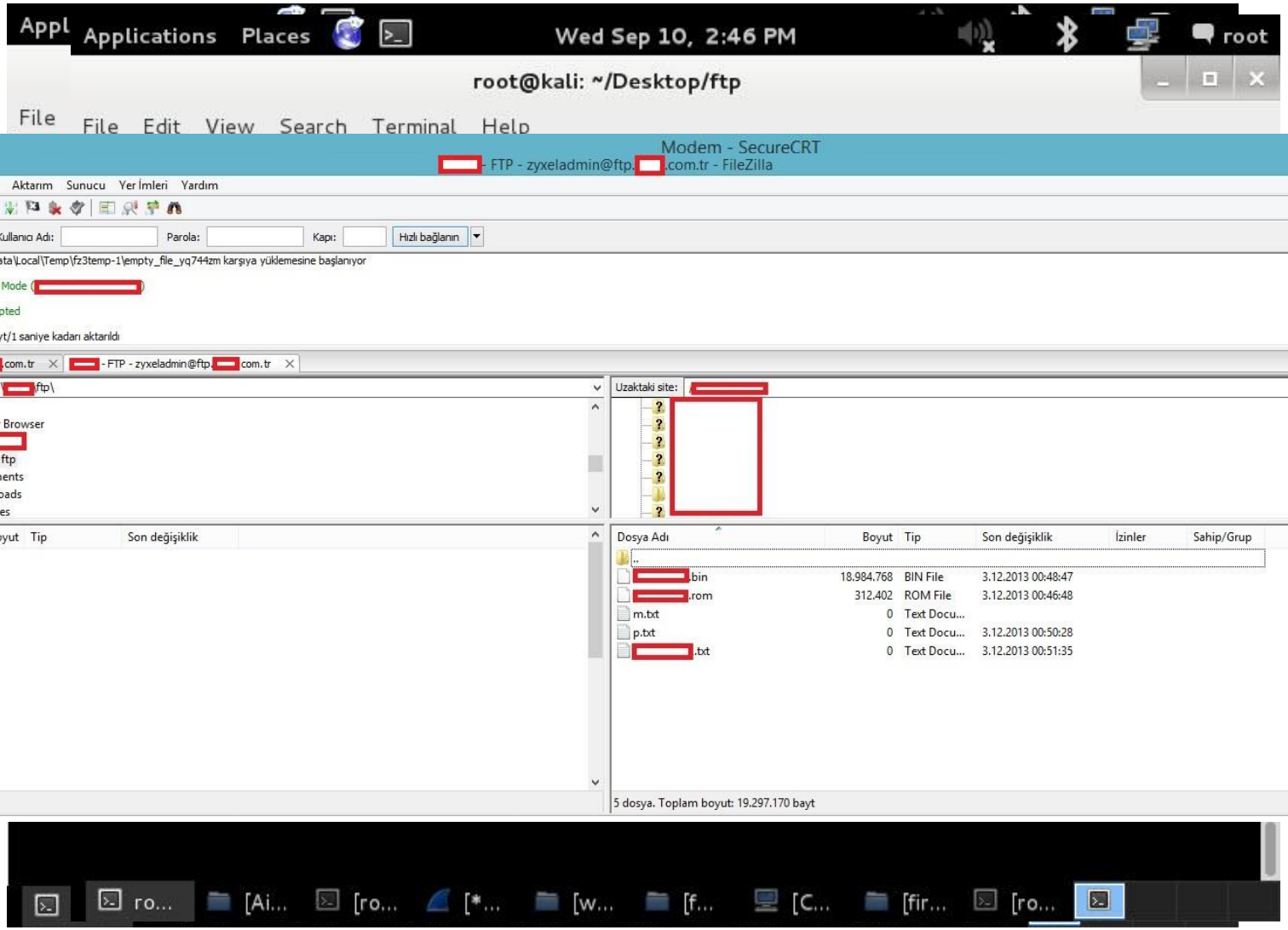
Modemin ayarlarında zafiyete yol açan bir yapılandırma hatası veya eksikliği var mı ?

Modem donanım yazılım güncelemelerini üreticiden mi yoksa ISS'ten mi alıyor ?

Sorular, sorular aklınızdaki sorular ve yanıtları için;

İhtiyaç listesi: donanım yazılımı, binwalk, strings

ÖRNEK #3 - STATİK & DİNAMİK ANALİZ



ÖRNEK #4 - STATİK & DİNAMİK ANALİZ

Modemlerin yönetim sayfalarında kimi zaman zafiyetlerin kimi zaman ise arka kapıların olabileceğini biliyorsunuz.

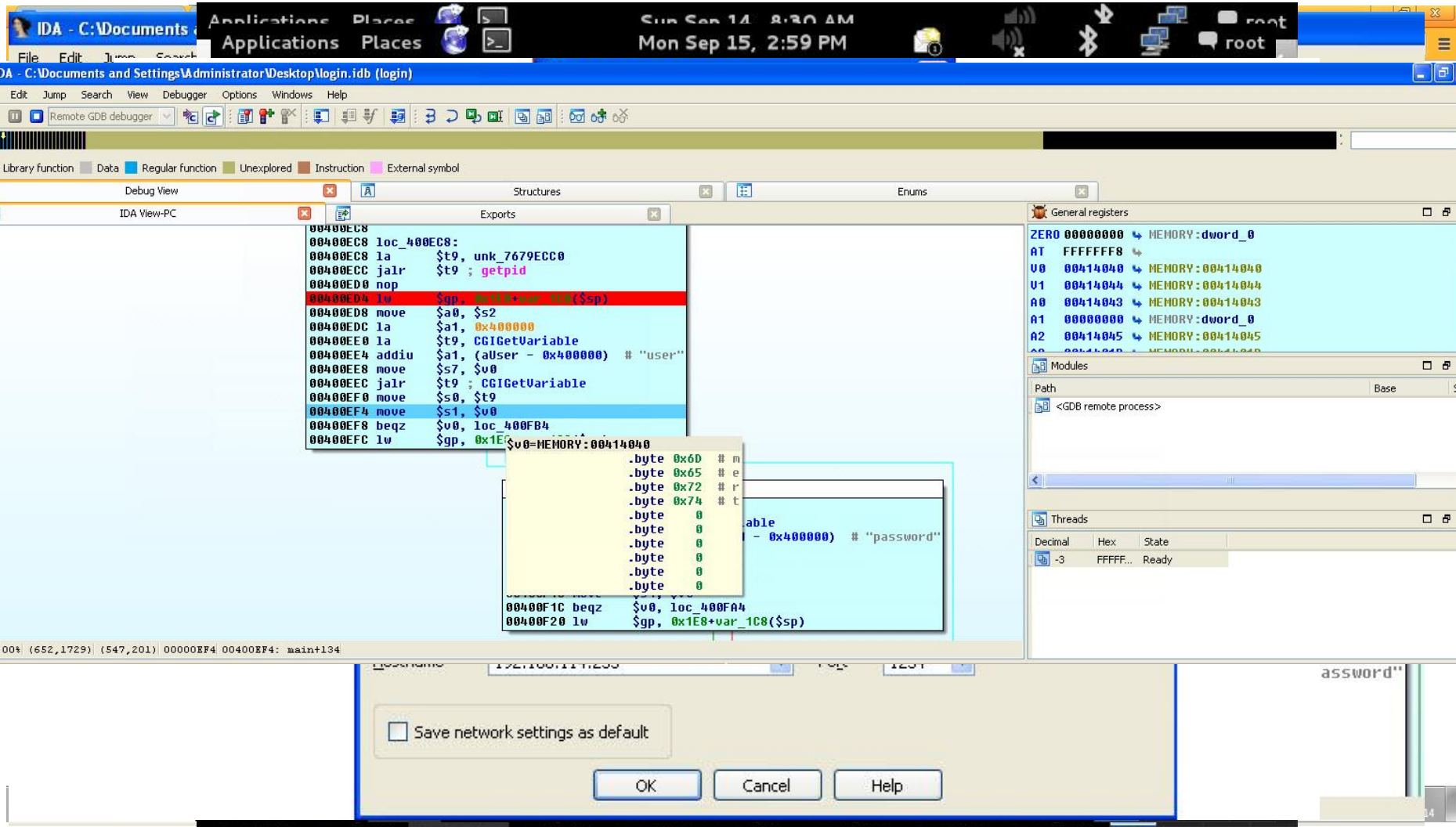
Temmuz ayında TP-Link kullanıcılarının başına gelenleri gördükten sonra modeminizi incelemeye karar verdiniz.

Modeminizde yer alan uygulamalarda ne tür zafiyetler var ? Şüphelendiğiniz de nasıl doğrulayabilirsiniz ?

(Disassemble && Debug)

İhtiyaç listesi: IDA Pro, Qemu, MIPS Assembly bilgisi, file, strings vb.

ÖRNEK #4 - STATİK & DİNAMİK ANALİZ



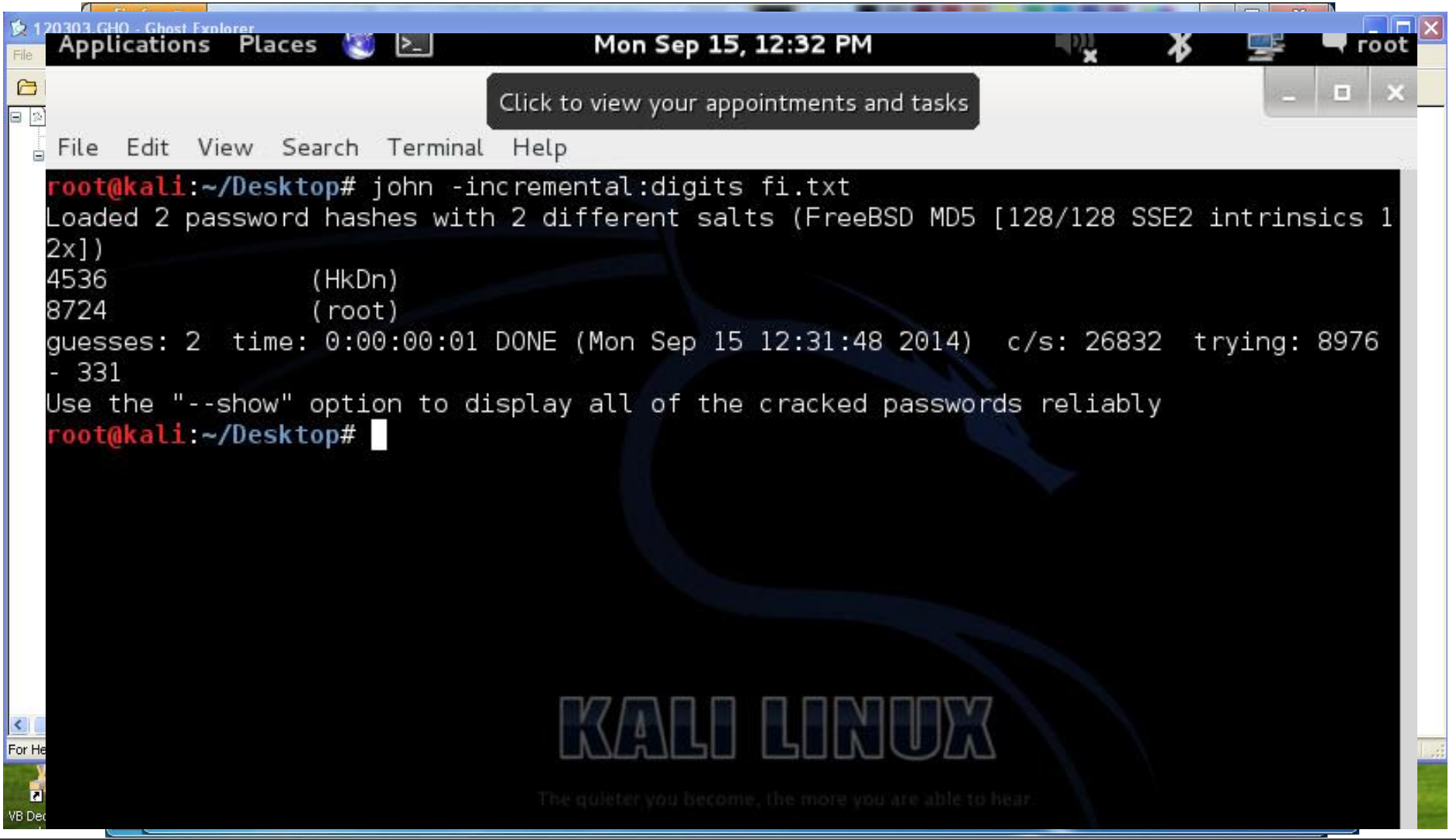
ÖRNEK #5 - DÜNYADAN

Donanım yazılımınızın peşinde rakipleriniz, dolandırıcılar, casuslar olabilir.

Donanım yazılımınızı internette paylaşıma açmadan önce mutlaka sıkılaştırmanız gerekmektedir.

Aksi halde zafiyetlerin keşfedilmesi ve kötüye kullanılması düşündüğünüzden daha da kısa (Retweet) sürebilir.

ÖRNEK #5 - DÜNYADAN



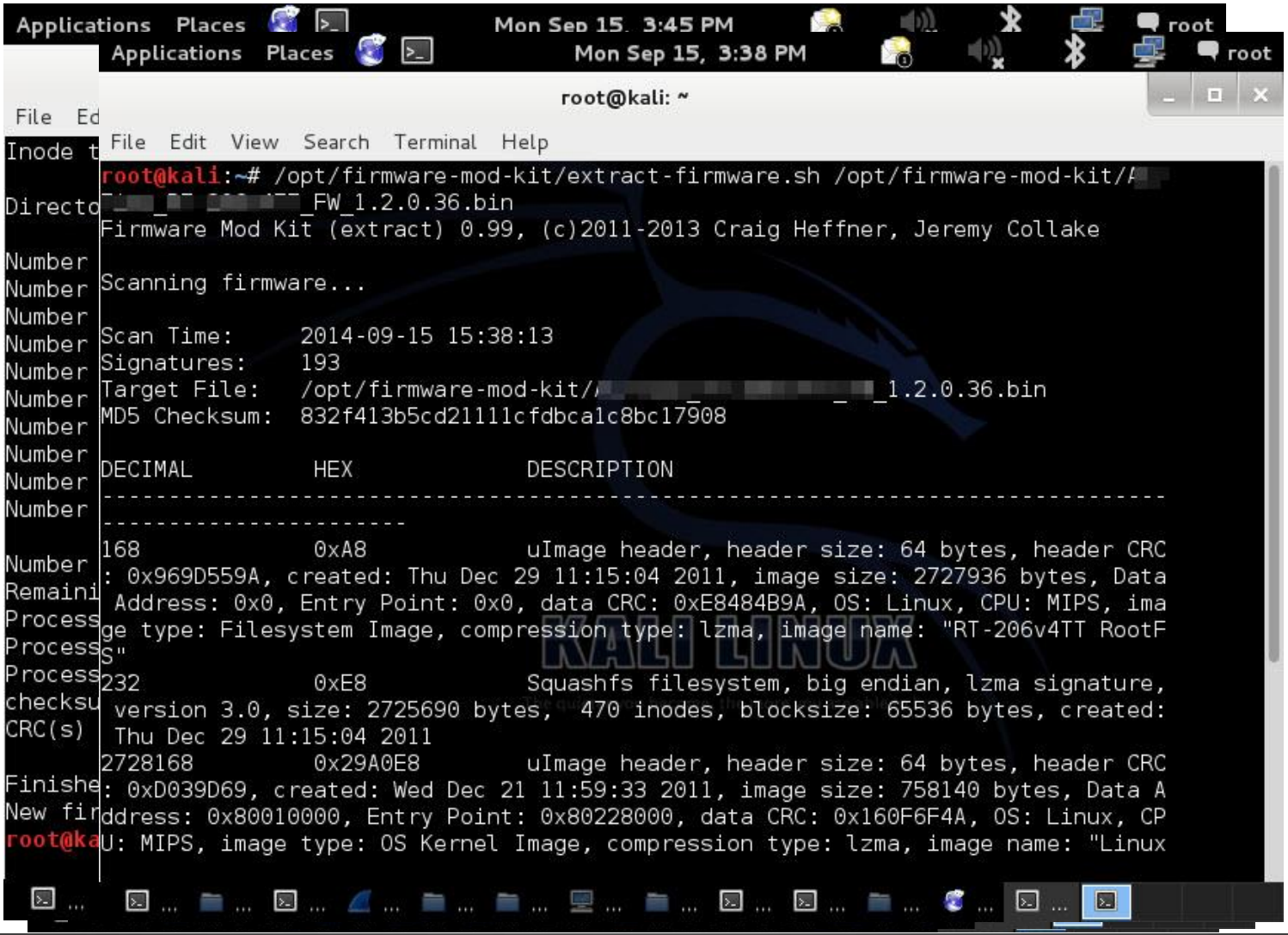
DONANIM YAZILIMI MANİPÜLASYONU

Donanım yazılımını yamamak (patch) için firmware-mod-kit aracından faydalanabilirsiniz.

./extract-firmware ile donanım yazılımını açabilirsiniz.

fmk klasöründe bulunan donanım yazılımına ait olan dosyaları değiştirdikten sonra ./build-firmware.sh ile paketleyebilirsiniz.

DONANIM YAZILIMI MANİPÜLASYONU



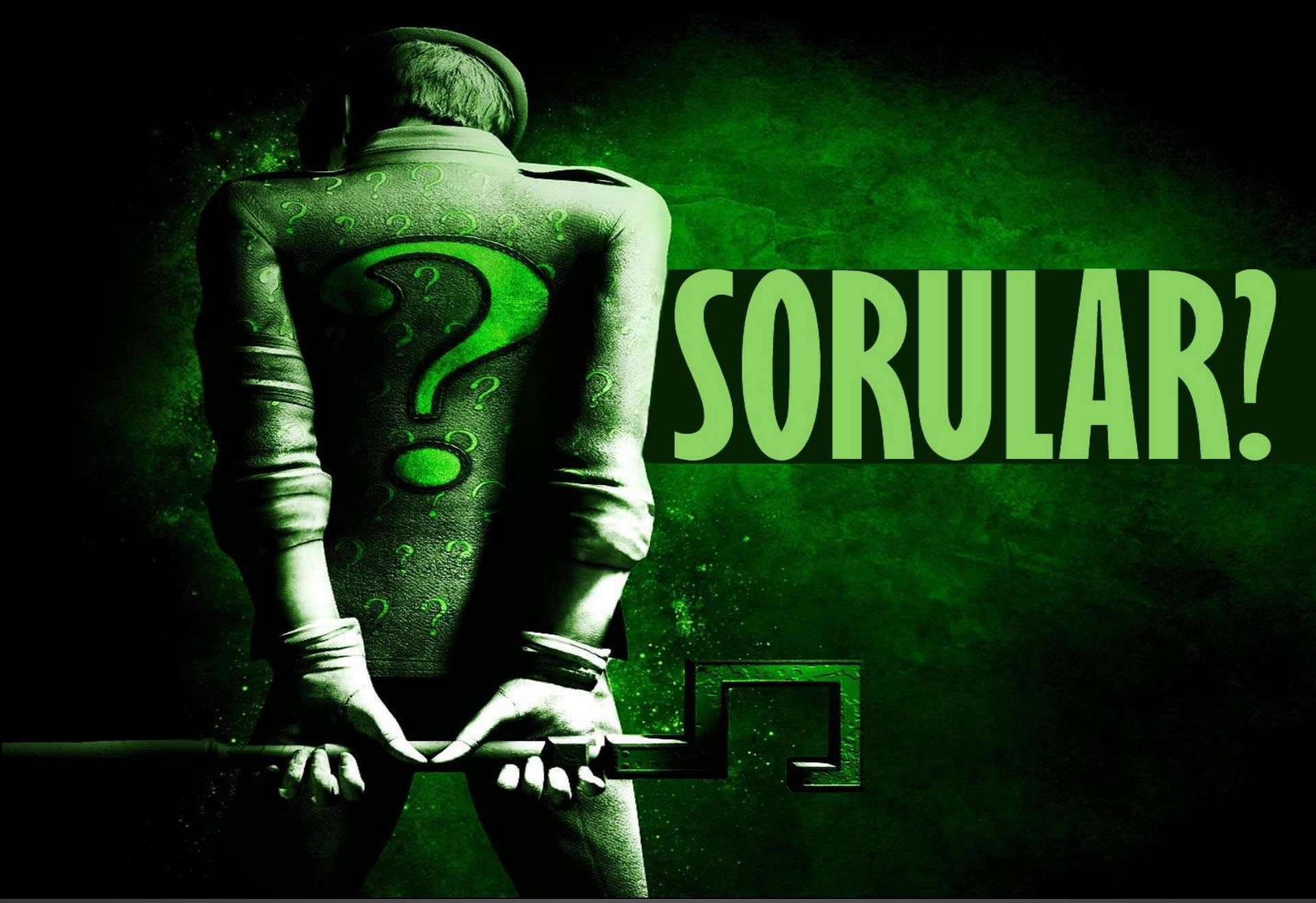
SONUÇ

Donanımlar kapalı kutudan ibaret değildir, donanım yazılımına ulaşmak ve içeriğini görüntülemek oldukça kolay olabilir.

Donanım yazılımlarında tespit edilen bir zafiyetin kötüye kullanımının etkisi çok yüksek olabilir.

Donanımlarda kullanılan işletim sistemleri, modern işletim sistemleri kadar güvenli değildir.

Donanım yazılımları meraklı kişilerce açılabilir, değiştirilebilir ve tekrar paketlenebilir. (imza kontrolü)


SORULAR?

TEŞEKKÜRLER

mert.sarica@gmail.com

https://www.mertsarica.com https://twitter.com/mertsarica