FIRAT ÜNİVERSİTESİ TEKNOLOJİ FAKÜLTESİ
YAZILIM MÜHENDİSLİĞİ BÖLÜMÜ SİBER GÜÇ LABORATUVARI

BÖLÜM 1 – GİRİŞ

Siber Güç Laboratuvarı, Fırat Üniversitesi Teknoloji Fakültesi bünyesinde siber güvenlik, kriptoloji, tehdit istihbaratı, güvenli veri depolama teknolojileri ve yüksek başarımlı hesaplama sistemleri üzerine araştırma ve geliştirme faaliyetleri yürütmek amacıyla kurulmuş ileri seviye bir Ar-Ge merkezidir. Laboratuvar hem ulusal güvenlik öncelikleri hem de akademik mükemmeliyet hedefleri doğrultusunda tasarlanmış altyapısı ile Türkiye'nin dijital güvenlik ekosistemine yüksek katma değer üretmeyi amaçlamaktadır. Günümüzde artan siber tehdit çeşitliliği, kritik altyapılara yönelik istihbarî saldırılar ve veri güvenliği alanındaki karmaşıklık, üniversite–sanayi–kamu üçgeninde güçlü Ar-Ge yapılmasını zorunlu kılmaktadır. Bu bağlamda Siber Güç Laboratuvarı milli siber savunma kapasitesinin geliştirilmesine yönelik projeleri yüksek donanım gücü ve disiplinlerarası bir yaklaşımla yürütmektedir. Laboratuvarın stratejik odağını oluşturan çalışmalar arasında:

- Kriptografik algoritma analizi ve yeni şifreleme sistemleri geliştirme,
- Siber tehdit istihbaratının büyük veri yöntemleriyle modellenmesi,
- Zararlı yazılım davranış analizi ve otomatik sınıflandırma,
- Güvenli veri depolama, yedekleme ve sızıntı önleme teknolojileri,
- Yapay zekâ destekli siber saldırı tespit sistemleri,
- ENF (Electric Network Frequency) tabanlı adli doğrulama ve zaman damgası teknolojileri,
- Ağ güvenliği, zafiyet analizi ve güvenli iletişim protokolleri yer almaktadır.

Laboratuvar altyapısı yalnızca modern siber güvenlik araştırmalarını desteklemekle kalmamakta aynı zamanda öğrenciler, araştırmacılar ve endüstri paydaşları için gerçek dünyaya birebir karşılık gelen test ortamları sunmaktadır. Bu altyapı yüksek performanslı iş istasyonları, gelişmiş veri depolama çözümleri, kriptografik güvenlik bileşenleri, siber operasyon ekipmanları, ileri seviye görüntüleme ve kayıt cihazları ile desteklenmiştir. Siber Güç Laboratuvarı'nda kullanılan tüm donanımlar Fırat Üniversitesi Taşınır Kayıt Yönetmeliği kapsamında kayıtlıdır ve laboratuvarın stratejik hedefleri doğrultusunda seçilmiştir. Cihaz envanteri yüksek hesaplama gücü gerektiren yapay zekâ uygulamalarından kriptografik test süreçlerine, dijital adli analizden veri güvenliği yönetimine kadar tüm kritik operasyonları karşılayacak çeşitliliktedir. Özellikle Dell Precision T7920 iş istasyonu, RTX 6000 GPU, MacBook Pro, NAS sistemleri, şifreli veri saklama birimleri, Kinect kamera, 3D tarayıcı, stüdyo kayıt donanımları ve drone/robot sistemleri gibi unsurlar laboratuvarın araştırma kapasitesini uluslararası standartlara taşımaktadır. Bu dokümanın amacı laboratuvarın mevcut teknik altyapısını bütüncül bir çerçevede açıklamak, cihazların fonksiyonlarını bilimsel araştırma perspektifinden değerlendirmek ve Siber Güç Laboratuvarı'nın ulusal siber güvenlik ekosistemine sunduğu katkıyı belgelerle ortaya koymaktır. İzleyen bölümlerde laboratuvar bileşenleri ayrıntılı teknik verilerle tanımlanmakta ve her cihaz kendi kategorisi ve kullanım amacı üzerinden sistematik olarak ele alınmaktadır.

BÖLÜM 2 — ÇALIŞMA ALANLARI VE ARAŞTIRMA TEMATİKLERİ

Siber Güç Laboratuvarı, siber güvenlik ekosisteminin temel bileşenlerini kapsayan geniş bir araştırma yelpazesinde faaliyet göstermektedir. Laboratuvarın çalışma alanları ulusal güvenlik stratejileri, kriptografik altyapılar, ağ güvenliği, tehdit istihbaratı, veri koruma mekanizmaları ve dijital adli analiz gibi kritik altyapılar üzerinde yoğunlaşmaktadır. Bu bölüm yürütülen araştırma temalarının derinliğini ve laboratuvar altyapısının bilimsel odak noktalarını kapsamlı biçimde ortaya koymaktadır.

2.1. Kriptoloji ve Güvenli İletişim Sistemleri

Kriptoloji araştırmaları laboratuvarın en stratejik araştırma alanlarından biridir. Özellikle:

- Kaos tabanlı şifreleme sistemleri,
- Post-kuantum kriptografi yöntemleri,
- Kriptografik protokol güvenlik testleri,
- Yüksek entropiye sahip anahtar üretim yöntemleri (ENF tabanlı, fiziksel kaos tabanlı, çok kaynaklı entropi modelleri),
- Donanım tabanlı güvenli kimlik doğrulama mekanizmaları,
- Modüler kriptografik kütüphanelerin test edilmesi

gibi çalışmalar doğrudan laboratuvarın HPC mimarisi ve şifreli depolama sistemleri üzerinde yürütülmektedir. Özellikle şifreli USB aygıtları, NAS tabanlı güvenli veri yedekleme birimleri ve Dell Precision / RTX 6000 iş istasyonları, yüksek hacimli kriptografik testleri gerçekleştirmeye uygun altyapı sunmaktadır.

2.2. Siber Tehdit İstihbaratı ve Saldırı Tespit Sistemleri

Laboratuvar gerçek dünya tehdit modellerini simüle ederek:

- Kötücül yazılım analizi,
- Ajan tabanlı otomatik siber tehdit sınıflandırma,
- Davranışsal saldırı tespit sistemleri (Anomaly Detection / AI-assisted IDS),
- Ağ trafiği korelasyon analizi,
- Dark Web tehdit izleme ve veri toplama gibi alanlarda çalışmalar yürütmektedir.

Bu süreçte kullanılan:

- Güç kaynakları ve UPS sistemleri,
- Yüksek hızlı depolama birimleri,

hem ağ adli bilişim analizini hem de gerçek zamanlı tehdit simülasyonlarını desteklemektedir.

2.3. Dijital Adli Analiz (Digital Forensics) ve Cihaz İnceleme

Siber Güç Laboratuvarı cihaz inceleme süreçlerini bütünsel bir yaklaşımla ele almaktadır. Çalışmalar şunları içermektedir:

- Mobil cihaz veri analizi
- USB/SSD veri kurtarma ve dosya yapısı incelemeleri
- ENF tabanlı zaman damgası doğrulama
- Kinect kamera ile hareket/veri sahteciliği araştırmaları
- 3D tarayıcı ile fiziksel kanıt bütünleştirme
- Drone ve robotik sistemlerle olay yeri analizi

Laboratuvar envanterindeki:

- Canon EOS M50 (yüksek çözünürlüklü delil fotoğraflaması),
- 3D MakerPro tarayıcı (sayısal modelleme),
- Kinect kamera (derinlik verisi toplanması),
- DJI FPV Drone (erişilemeyen bölgelerden veri aktarımı),
- Mekânsal haritalama robotu (otonom analiz),

adli süreçlerin dijitalleştirilmesinde etkin biçimde kullanılmaktadır.

2.4. Güvenli Veri Depolama, Veri Entegritesi ve Zaman Damgası Sistemleri

Günümüz siber saldırılarının en kritik hedefi veridir. Bu sebeple laboratuvarda şu alanlarda yoğun Ar-Ge yürütülmektedir:

- Şifreli veri depolama sistemleri,
- Çok katmanlı yedekleme ve veri bütünlüğü izleme,
- ENF tabanlı zaman damgalama (timestamp) teknolojileri,
- Veri sızıntısı tespit (DLP) mekanizmaları,
- Bulut tabanlı ve yerel NAS tabanlı veri replikasyonu,
- Veri imzalama ve bütünlük doğrulama protokolleri.

Bu çalışmalar, envanterde yer alan:

- WD My Cloud PR4100 NAS (8 TB × 2)
- WD Elements veri depolama birimi
- Kingston 960GB SSD'ler
- Şifreli USB bellekler (Kingston, Apricorn)
- ENF Veri Toplama Cihazı

ile gerçekleştirilmektedir.

2.5. Yapay Zekâ Destekli Güvenlik Sistemleri

Siber Güç Laboratuvarı, yapay zekâ tabanlı güvenlik modelleri geliştirmektedir:

- Saldırı tahminleme
- Kullanıcı davranış analizi (UBA/UEBA)

- Makine öğrenimi tabanlı IDS/IPS modelleri
- Kriptoanaliz için GPU hızlandırılmış derin öğrenme
- Görüntü/ses tabanlı tehdit sınıflama

Bu kapsamda:

- RTX 6000 GPU
- Dell & HP yüksek performans istasyonları
- MacBook Pro ve All-in-One 4K iş istasyonları

analiz süreçlerinde aktif şekilde kullanılmaktadır.

2.6. Siber Güvenlik Eğitim ve Simülasyon Platformları

Laboratuvar, uygulamalı eğitim imkânlarını da destekleyecek şekilde tasarlanmıştır. Bu kapsamda:

- Ağ saldırı simülasyonları,
- Kriptografik protokol analizi,
- Adli bilişim iş akışı eğitimleri,
- Gerçek cihazlarla siber olay tatbikatları,
- Veri güvenliği senaryoları,
- API güvenliği ve web zafiyet simülasyonları,
- Sosyal mühendislik ve farkındalık testleri,

gibi uygulamalar yapılmaktadır.

Gerekli görüntü/ses kaydı, laboratuvar içi stüdyo sistemi (Rode, Godox, Canon M50) ile desteklenmektedir.

BÖLÜM 3 — TEKNİK ALTYAPI GENEL MİMARİSİ

Siber Güç Laboratuvarı'nın teknik altyapısı; yüksek başarımlı hesaplama birimleri, güvenli depolama sistemleri, ağ ve haberleşme altyapıları, dijital adli analiz aygıtları ve kayıt–izleme bileşenlerinin entegre edildiği bütüncül bir mimari üzerine kuruludur. Bu mimari hem bilimsel araştırmayı hem de operasyonel siber güvenlik çalışmalarını kesintisiz şekilde desteklemek amacıyla modüler ve ölçeklenebilir bir yapıda tasarlanmıştır.
Aşağıda, laboratuvarın teknik bileşenleri beş çekirdek sistem üzerinden açıklanmaktadır:

3.1. Yüksek Başarımlı Hesaplama (HPC) ve Yapay Zekâ Hesaplama Mimarisi

Bu birim laboratuvarın kriptografik analiz, yapay zekâ eğitimi ve büyük veri işleme görevlerinin merkezinde yer alır. HPC mimarisi üç katmandan oluşmaktadır:

<u>Katman 1: Ana İş İstasyonları (Primary Compute Nodes)</u>

Bu katmanda yer alan cihazlar:

- Dell Precision T7920 Workstation
- RTX 6000 GPU Donanımı
- All-in-One 4K 27" İş İstasyonu
- Apple iMac 24" (4.5K Ekran)
- MacBook Pro (M4 Çip)

Bu sistemler GPU hızlandırmalı iş yüklerini, kaos tabanlı kriptoanalizleri, post-kuantum algoritma testlerini ve derin öğrenme modellerini çalıştırmak için ana hesaplama gücünü sağlamaktadır.

<u>Katman 2: Mobil ve Destek İş İstasyonları</u>

- Dell Precision M3561 Dizüstü
- HP 240 G9
- Monster Tulpar T7 v20.6

Bu sistemler saha çalışmaları, olay yeri analizleri, tehdit istihbaratı veri derlemeleri ve taşınabilir eğitim demo ortamları için kullanılmaktadır.

Katman 3: GPU Odaklı Hızlandırma

RTX 6000 kartı, özellikle:

- Kriptoanaliz (differential/linear cryptanalysis)
- Hash ve şifre çözme hız testleri
- Malware sınıflandırma algoritmaları
- Anomali tespit modelleri

için gerekli GPU çekirdek gücünü sağlar.

3.2. Güvenli Veri Depolama ve Yedekleme Altyapısı

Siber Güç Laboratuvarı'nın veri bütünlüğü ve sızma dayanıklılığı, çok katmanlı bir depolama mimarisi ile güvence altına alınmaktadır.

A) Ana Yedekleme Birimleri

- Western Digital My Cloud Pro PR4100 (8 TB + 8 TB) — NAS sunucu (Tam yedekleme, sistem log depolama, olay kayıtları ve kriptografik veri setleri için)

B) Taşınabilir ve Hızlı Yedekleme Birimleri

- WD Elements USB Depolama Ünitesi
- Kingston 960GB SSD (2 adet)

C) Donanımsal Şifreli Veri Taşıyıcılar

- Kingston 64GB AES-256 Flash Bellek
- Apricorn Aegis Secure Key (FIPS 140-2 Level 3)

Bu cihazlar, hassas siber güvenlik projelerinde kaynak kod, analiz çıktıları, adli materyal ve kritik konfigürasyon dosyalarının güvenli aktarımını sağlar.

D) Özel Sensör Veri Depolama Birimi

- ENF Veri Toplama Cihazı (Elektrik şebeke frekansı tabanlı zaman damgası ve adli doğrulama amaçlı)

Bu yapı, laboratuvarın hem operasyonel bütünlüğünü, hem de akademik veri güvenliğini garanti altına alır.

3.3. Ağ, İletişim ve Güç Yönetimi Sistemi

Siber Güç Laboratuvarı'nın iletişim ve güç altyapısı, sistem sürekliliği ve güvenli bağlantı için aşağıdaki bileşenlerden oluşur:

- SRVS1K Smart 1 kVA UPS
- EcoFlow River Pro (720Wh Mobil Güç Kaynağı)
- EcoFlow 160W Taşınabilir Güneş Paneli

Bu sistemler, yüksek hesaplama istasyonlarının ve NAS birimlerinin kesintisiz çalışmasını garanti eder, veri kaybı riskini ortadan kaldırır ve saha analizlerine mobil enerji desteği sağlar.

3.4. Dijital Adli Analiz, Görüntüleme ve 3D Modelleme Sistemi

Laboratuvar, fiziksel ve dijital kanıtların bütünleştirildiği çok yönlü bir adli analiz mimarisine sahiptir.

A) Yüksek Çözünürlüklü Görüntüleme

- Canon EOS M50 Fotoğraf Makinesi (Delil fotoğraflaması, cihaz içi incelemeler)

B) Derinlik Kamerası ve Hareket Analizi

- Kinect Kamera (Xbox) (Sahtecilik tespiti, hareket verisi analizi, biyometrik araştırmalar)

C) 3D Modelleme Sistemi

- 3D MakerPro Tarayıcı (CR-Scan 01) (Donanım bileşen analizi, obje/cihaz tarama)

D) Hava ve Mekân Analizi

- DJI FPV Drone
- Roborock Mekânsal Haritalama Robotu

Bu cihazlar olay yeri dijitalleştirmesi, tavan/duvar erişimi olmayan alanların taranması ve fiziksel güvenlik değerlendirmeleri için kullanılmaktadır.

3.5. Stüdyo, Kayıt, Sunum ve Eğitim İçerik Üretim Sistemi

Laboratuvar içi eğitim, siber saldırı simülasyonları, çevrim içi dersler ve teknik içerik üretimi için profesyonel bir kayıt sistemi oluşturulmuştur.

A) Ses Sistemleri

- Rode VideoMicro Mikrofon
- Rode Wireless Go II Kablosuz Mikrofon

B) Işık Sistemleri

- Godox M1 RGB Mini Mobil Video Işığı (2 adet)
- Godox ES45 RGB Stüdyo LED Işık Kiti (2 adet)

C) Görsel Destek

- Philips Ekran (2 farklı model)
- Elon Ayaklı TV ve Fuar Standı

Bu altyapı hem bilimsel yayın üretimini hem de öğrencilerin uygulamalı eğitim süreçlerini desteklemektedir.

3.6. Destek ve Genel Kullanım Sistemleri

- 90×120 Mobil Tekerlekli Yazı Tahtası
- Taşıyıcı Standlar

Laboratuvar içi eğitim, proje planlama ve teknik sunumlarda kullanılmaktadır.

BÖLÜM 4 — YÜKSEK BAŞARIMLI HESAPLAMA (HPC) VE YAPAY ZEKÂ İŞ İSTASYONLARI

Siber Güç Laboratuvarı'nın araştırma ve geliştirme faaliyetlerinin temelinde yüksek başarımlı hesaplama altyapısı yer almaktadır. Kriptografik analizden tehdit istihbaratı modellemelerine, büyük veri işleme süreçlerinden yapay zekâ eğitimlerine kadar tüm kritik operasyonlar, laboratuvarda bulunan çok çekirdekli iş istasyonları ve GPU hızlandırıcılı sistemler üzerinde yürütülmektedir. Bu bölümde laboratuvarın HPC kapasitesine doğrudan katkı sunan yedi ana iş istasyonu teknik rolleriyle birlikte açıklanmıştır.

4.1. Dell Precision T7920 İş İstasyonu

Fiş No: 2022/Z/108 — Sicil: 255.2.1/22/8929

Teknik Özellikler:

- Çift işlemcili mimari (2× Intel Xeon 4216)
- 32 GB RAM
- 256 GB SSD
- Genişletilebilir PCIe mimarisi
- Kurumsal sınıf kasa yapısı

Laboratuvardaki Kullanım Alanları:

- Yüksek hacimli kriptografik işlem testleri
- GPU tabanlı derin öğrenme modelleri için ana düğüm
- Siber saldırı simülasyonlarında büyük veri korelasyonu
- Malware davranış analizi için eğitim ortamı
- Çok katmanlı ağ trafiği analizlerinin gerçek zamanlı işlenmesi

Dell Precision T7920, laboratuvarın "ana hesaplama sunucusu" rolünü taşıyan en kritik cihazdır.

4.2. NVIDIA RTX 6000 Ekran Kartı

Fiş No: 2025/Z/215 — Sicil: 255.2.1/25/28459

Teknik Özellikler:

- 48 GB GDDR6 ECC bellek
- 4608 CUDA çekirdeği
- 72 RT Core / 576 Tensor Core
- HPC ve yapay zekâ hızlandırma mimarisi
- PCIe 4.0 arayüz

Laboratuvardaki Kullanım Alanları:

- Kriptoanaliz süreçlerinde GPU hızlandırma
- Derin öğrenme modellerinin eğitiminde (CNN, LSTM, Transformer)
- Post-kuantum kriptografisi performans testleri
- Saldırı sınıflandırma modelleri
- Büyük ölçekli hash kırma ve şifre denemeleri

RTX 6000, laboratuvarın yapay zekâ ve GPU hızlandırmalı hesaplama kapasitesinin çekirdeğini oluşturmaktadır.

4.3. Apple iMac 24" (4.5K Retina)

Fiş No: 2025/Z/378 — Sicil: 255.2.1/25/46682

Teknik Özellikler:

- 8 çekirdekli CPU
- 256 GB SSD
- 8 GB unified memory
- 24" 4.5K yüksek çözünürlüklü ekran

Laboratuvardaki Kullanım Alanları:

- Unix tabanlı güvenlik testleri
- Swift tabanlı kriptografi prototip geliştirme
- macOS uygulama güvenlik analizleri
- Görsel analiz ve forensik arayüz geliştirme

iMac, laboratuvarda özellikle çapraz platform güvenlik araştırmaları için kullanılmaktadır.

4.4. MacBook Pro (Apple M4 İşlemci)

Fiş No: 2023/Z/62 — Sicil: 255.2.1/23/3139

Teknik Özellikler:

- M4 işlemci (10 CPU + 10 GPU çekirdeği)
- 24 GB unified memory
- 1 TB SSD

Laboratuvardaki Kullanım Alanları:

- Saha çalışmalarında mobil HPC düğümü
- Python/TensorFlow tabanlı tehdit analizi geliştirme
- Taşınabilir veri işleme ve olay yeri inceleme
- Siber saldırı loglarının hızlı analiz edilmesi

MacBook Pro, laboratuvara mobil süper bilgisayar işlevi kazandırmaktadır.

4.5. Dell Precision M3561 Dizüstü Bilgisayar

Fiş No: 2022/Z/31 — Sicil: 255.2.1/22/4069

Teknik Özellikler:

- Intel Core i7-11850H
- 32 GB RAM
- 1 TB SSD
- NVIDIA T600 GPU
- 15.6" FHD ekran

Laboratuvardaki Kullanım Alanları:

- Saha testleri, kablolu/kablosuz ağ analizi
- Hafif makine öğrenimi modellerinin eğitimi
- Kriptografik araçların hızlı prototip geliştirme ortamı
- Tehdit avcılığı (Threat Hunting) süreçleri
- Bu sistem, laboratuvarda portable HPC ihtiyacını karşılayan alan cihazıdır.

4.6. HP 240 G9 Dizüstü Bilgisayar

Fiş No: 2022/Z/111 — Sicil: 255.2.1/22/9433

Teknik Özellikler:

- Intel Core i7-1255U
- 64 GB RAM (üst seviye bellek kapasitesi)
- 2 TB SSD
- 14" FHD ekran

Laboratuvardaki Kullanım Alanları:

- Büyük log dosyalarının mobil analizleri
- Veri toplama cihazlarının yönetimi
- Olay yeri incelemede hızlı veri replikasyonu
- Ulusal/uluslararası siber yarışmalarda kullanım
- Laboratuvarda “yüksek belleğe sahip mobil iş istasyonu” rolünü üstlenir.

4.7. 27” 4K All-in-One İş İstasyonu

Fiş No: 2024/Z/85 — Sicil: 255.2.1/24/1481513

Teknik Özellikler:

- 4 GHz dört çekirdekli CPU

- 27” 4K çözünürlük
- All-in-One kompakt mimari

Laboratuvardaki Kullanım Alanları:
- Ağ güvenliği analiz panellerinin yönetimi
- SIEM sistemlerinin kontrol ekranı
- Saldırı haritaları ve gerçek zamanlı görselleştirmeler
- Eğitim ortamları ve laboratuvar içi gösterimler
- Bu cihaz, laboratuvarın “görsel kontrol istasyonu” olarak işlev görmektedir.

BÖLÜM 5 — GÜVENLİ VERİ DEPOLAMA VE SİBER OLAY ANALİZ SİSTEMLERİ

Siber Güç Laboratuvarı’nın en kritik bileşenlerinden biri veri bütünlüğü, güvenli depolama, dijital delil koruma ve siber olay analiz süreçlerini destekleyen çok katmanlı veri mimarisidir. Günümüz siber güvenlik tehditlerinin odak noktası hâline gelen veri, laboratuvarda hem donanımsal hem yazılımsal düzeyde yüksek güvenlik önlemleriyle korunmaktadır. Bu sistem NAS cihazları, taşınabilir şifreli aygıtlar, yüksek hızlı SSD’ler, ENF tabanlı adli doğrulama cihazları ve yedekleme ünitelerinden oluşmaktadır. Her bir bileşen farklı bir operasyonel katmanda görev alarak laboratuvarın veri güvenliği altyapısını bütüncül hale getirmektedir.

5.1. Ağ Bağlantılı Depolama (NAS) Sistemleri

5.1.1. WD My Cloud Pro Series PR4100 – 8 TB NAS
Fiş No: 2022/Z/108 — Sicil: 253.3.4/22/8928
Teknik Özellikler:
- 4 yuvalı NAS mimarisi
- 8 TB kurulu kapasite
- RAID 0/1/5/10 desteği
- Çok kullanıcılı erişim kontrolü
- HTTPS ve AES-256 şifreleme desteği

Kullanım Alanları:
- Kriptografi araştırmalarında üretilen büyük veri setleri
- AI eğitim loglarının güvenli saklanması
- Yüksek hacimli ağ trafiği kayıtları
- Adli bilişim dosyalarının saklanması

5.1.2. WD My Cloud Pro Series PR4100 – 8 TB (Yeni Nesil)

Fiş No: 2024/Z/87 — Sicil: 253.3.4/24/1481515
Bu model laboratuvarın veri yedekleme altyapısının güncel versiyonudur.
Kullanım Alanları:
- Veri replikasyonları (NAS → NAS)
- Kriptografik anahtar havuzlarının korunması
- Güvenli depolama alanında yüksek erişilebilirlik

5.2. Harici Veri Depolama ve Hızlı Transfer Sistemleri

5.2.1. Western Digital Elements – Harici Depolama Ünitesi
Fiş No: 2022/Z/35 — Sicil: 253.3.4/22/4263

Yüksek güvenlik gerektiren projelerde offline yedekleme amacıyla kullanılır.
Öne Çıkan Kullanımlar:
- Siber olay analizi sırasında disk imajlarının taşınması
- Büyük veri setlerinin çevrim dışı korunması
- Laboratuvar dışı senaryolarda sistem yedekleme

5.2.2. Kingston 960 GB SSD (2 Adet)
Fiş No: 2025/Z/216 — Sicil: 255.2.2/25/28460 – 28461

Teknik Rolü:

- Yüksek hızlı veri aktarımı
- Forensik analizlerde disk imajlama
- Büyük dosya operasyonlarında transfer hızlandırıcı

Kullanım Alanları:

- Mobil olay yeri incelemesi
- SSD analizleri, dosya sistemi çözümlemeleri
- Çoklu sanal makine kurulumlarında çalışma diskleri

5.3. Donanımsal Şifreleme Destekli Flash Bellek Sistemleri

5.3.1. Kingston 64 GB USB 3.0 – AES 256-bit Şifreli Flash Bellek
Fiş No: 2022/Z/31 — Sicil: 255.2.2/22/4068
Kullanım Alanı:

- Kritik yapılandırma dosyalarının taşınması
- Kriptografik anahtar setlerinin aktarımı
- Hassas araştırma verilerinin saha ortamına güvenli taşınması

5.3.2. Apricorn Aegis Secure Key – FIPS 140-2 Level 3 USB Bellek
Fiş No: 2022/Z/31 — Sicil: 255.2.2/22/4070
Kullanım Alanı:

- Olay yeri verilerinin güvenli transferi
- Savunma sanayii prototiplerinin taşınması
- Çok faktörlü korumaya sahip offline veri saklama

5.4. ENF (Electric Network Frequency) Tabanlı Veri Toplama Cihazı

ENF Veri Toplama ve Adli Doğrulama Cihazı
Fiş No: 2025/Z/379 — Sicil: 253.3.4/25/46680

Teknik İşlevi:

- Elektrik şebekesi frekansı (50 Hz) varyasyonlarının kaydı
- Ses ve video dosyalarının zaman damgası doğrulaması
- Manipüle edilmiş kayıtların tespiti
- Adli analizlerde mutlak zaman referansı sağlama

Kullanım Senaryoları:

- Siber saldırı zaman çizelgesi doğrulama
- Delil bütünlüğü denetimi
- Dijital içerik sahteciliği tespiti
- Mahkeme sürecinde delil doğrulama

5.5. Veri Güvenliği Mimarisinin Çok Katmanlı Yapısı

Siber Güç Laboratuvarı'nda veri güvenliği üç ana katmanda çalışır:
Katman 1: Donanımsal Güvenlik

- FIPS onaylı USB'ler
- Yerel şifreli SSD'ler
- NAS üzerinde AES-256 depolama şifreleme

Katman 2: Ağ Tabanlı Güvenlik

- Erişim kontrol listeleri
- IP tabanlı kimlik doğrulama
- Segmentli ağ yapısı (Compute → Storage → Analysis)

Katman 3: Adli ve Operasyonel Güvenlik

- ENF doğrulama
- Hash tabanlı bütünlük izleme
- Çoklu yedekleme (NAS + SSD + Offline Storage)

Bu yapı laboratuvarda üretilen tüm verilerin hem güvenli hem de doğrulanabilir şekilde saklanmasını sağlar.

BÖLÜM 6 — AĞ GÜVENLİĞİ, HABERLEŞME VE GÜÇ YÖNETİMİ SİSTEMLERİ

Siber Güç Laboratuvarı, yürüttüğü siber güvenlik ve kriptoloji çalışmalarının gerekliliği olarak hem yüksek erişilebilirlik hem de kesintisiz güç yapısına sahip bir teknik mimari kullanmaktadır. Ağ haberleşme cihazları, VoIP tabanlı IP telefonlar, UPS sistemleri ve taşınabilir enerji kaynakları, laboratuvarın operasyonlarının sürekliliğini garanti eden kritik bileşenlerdir. Bu bölümde laboratuvardaki tüm iletişim ve enerji yönetimi donanımları, taşınır kayıt belgelerindeki gerçek bilgilerle birlikte kapsamlı biçimde sunulmaktadır.

6.1. Ağ Haberleşme ve VoIP Altyapısı

6.1.1. Ericsson-LG LIP-1010i IP Telefon Cihazları
Fiş No: 2025/Z/430 — Sicil: 255.2.4/25/44767

Teknik Özellikler:

- VoIP (Voice over IP) tabanlı dijital telefon
- Şifreli iletişim için güvenli SIP protokolü desteği
- Lab içi ağ trafiği üzerinde tam kontrol
- Uzaktan yönetilebilir yapı

Laboratuvardaki Kullanım Alanları:

- Ağ trafiği analizi ve VoIP güvenlik testleri
- IDS/IPS sistemlerinin VoIP üzerinde davranış analizi
- Siber saldırı simülasyonlarında iletişim akışı takibi
- Tehdit istihbaratı çalışmaları için laboratuvar içi iletişim kanalı
- IP telefonlar, laboratuvarın ağ güvenliği eğitim modüllerinde sık kullanılan altyapı bileşenleridir.

6.2. Güç Yönetimi, UPS ve Kesintisiz Enerji Sistemleri

Laboratuvarda bulunan yüksek işlem gücüne sahip iş istasyonları, NAS depolama birimleri ve kritik adli cihazların kesintisiz çalışması, güvenli bir güç altyapısı ile sağlanmaktadır.

6.2.1. SRVS1K Smart 1kVA Kesintisiz Güç Kaynağı
Fiş No: 2022/Z/108 — Sicil: 253.2.5/22/8931

Teknik Özellikler:

- 1 kVA çıkış gücü
- Online çalışma tipi
- Gerilim dalgalanmasına karşı tam koruma
- Sunucu ve NAS cihazları için uygun

Kullanım Alanları:

- Ana NAS cihazlarının kesintisiz çalışması
- Kriptoanaliz süreçlerinde işlem kesintisinin engellenmesi
- Veri kaybının önlenmesi
- Laboratuvar çekirdek sistemlerinin otomatik kapanma senaryoları

6.2.2. EcoFlow River Pro – 720 Wh Mobil Güç Kaynağı
Fiş No: 2024/Z/86 — Sicil: 253.2.5/24/1481516

Teknik Özellikler:

- 720 Wh yüksek kapasiteli batarya
- Çoklu çıkış (AC/DC/USB)
- Taşınabilir saha enerjisi çözümü

Kullanım Alanları:

- Saha incelemelerinde mobil iş istasyonlarına güç sağlama
- Drone, 3D tarayıcı, kamera gibi cihazların şarjı
- Elektrik kesintisi altındaki acil veri toplama senaryoları
- Mobil SOC (Security Operations Center) uygulamaları

6.2.3. EcoFlow 160W Taşınabilir Güneş Paneli
Fiş No: 2024/Z/88 — Sicil: 253.3.6/24/1481514

Teknik Özellikler:

- 160W güneş enerjisi üretim kapasitesi
- Katlanabilir portatif yapı
- EcoFlow güç kaynaklarıyla tam uyum

Kullanım Alanları:

- Elektrik erişiminin olmadığı bölgelerde enerji üretimi
- Uzun süreli saha görevlerinde kesintisiz güç
- Adli olay yeri incelemelerinde bağımsız enerji kaynağı
- Siber güvenlik tatbikatlarında mobil operasyon istasyonları

6.3. Güç ve Enerji Sistemlerinin Laboratuvar Mimarisi İçindeki Rolü

Laboratuvarın enerji altyapısı üç temel güvenlik seviyesine ayrılmıştır:

- Seviye 1 — Kritik Sistem Güç Koruması: Dell Precision T7920, NAS cihazları, RTX 6000, iMac vb. cihazların kesintisiz çalışması UPS ile sağlanır.
- Seviye 2 — Saha Operasyon Güç Yönetimi: Mobil iş istasyonları ve adli cihazlar EcoFlow River Pro ile beslenir.
- Seviye 3 — Off-grid Bağımsız Güç: Güneş paneli + EcoFlow kombinasyonu ile laboratuvar dışı bölgelerde bile analiz yapılabilir.

Bu üç katmanlı yapı, laboratuvarı hem siber projelerde hem de adli saha çalışmalarında tamamen bağımsız ve güvenli bir enerji altyapısına kavuşturur.

BÖLÜM 7 — DİJİTAL ADLİ ANALİZ, GÖRÜNTÜLEME VE 3D MODELLEME SİSTEMLERİ

Siber Güç Laboratuvarı dijital adli inceleme süreçlerinde sadece yazılımsal analiz yöntemlerini değil, fiziksel çevrenin ve cihazların sayısallaştırılmasını mümkün kılan gelişmiş bir görüntüleme ve modelleme altyapısına sahiptir. Laboratuvarın siber güvenlik çalışmalarında elde edilen delillerin belgelenmesi, kanıt bütünlüğünün korunması ve karmaşık donanım yapılarına ait detayların analiz edilmesi bu sistemler sayesinde mümkün olmaktadır. Bu bölüm kayıt altına alma, 3D tarama, derinlik analizi ve sahne rekonstrüksiyonu için kullanılan donanımları detaylı biçimde açıklar.

7.1. Yüksek Çözünürlüklü Görüntüleme Sistemleri

7.1.1. Canon EOS M50 + 15–45 mm Lensli Fotoğraf Makinesi

Fiş No: 2022/Z/31 — Sicil: 255.2.5/22/4147

Teknik Özellikler:

- APS-C CMOS sensör
- 4K video kayıt
- Değiştirilebilir lens sistemi
- Düşük ışıkta yüksek performans
- Dual Pixel AF otomatik odaklama

Kullanım Alanları:

- Olay yeri ve cihaz içi donanım fotoğraflaması
- Hassas devre bileşenlerinin ve PCB yüzeylerinin kayıt altına alınması
- Sahtecilik tespitinde mikro detay görüntüleri
- Laboratuvar içi teknik eğitim videolarının üretim
- Çipset, kart okuyucu ve fiziksel bağlantı noktalarının delil niteliğinde belgelenmesi
- Canon EOS M50, laboratuvarda adli fotoğraflama standardını belirleyen ana kameradır.

7.2. Derinlik Kamerası ve Hareket Analizi Sistemleri

7.2.1. Kinect Kamera – Xbox Kinect

Fiş No: 2024/Z/167 — Sicil: 255.2.5/24/1483406

Teknik Özellikler:

- Derinlik sensörü (time-of-flight)
- IR projektör

- RGB kamera
- Kemik/iskelet izleme algoritması

Kullanım Alanları:

- Hareket tabanlı sahtecilik tespiti
- Dijital içeriklerin manipülasyon kontrolü
- Davranış analizinde (UBA/UEBA) sensör destekli veri toplama
- Fiziksel erişim kontrolü araştırmaları
- Derinlik haritalarının adli bilişimde kaybolmuş verilerin yeniden modellenmesi
- Kinect, laboratuvarın sensör tabanlı davranış ve sahne analizleri için temel donanımıdır.

7.3. 3D Tarama ve Sayısal Modelleme Sistemleri

7.3.1. 3D MakerPro – CR Scan 01, 10 FPS 3D Tarayıcı
Fiş No: 2024/Z/169 — Sicil: 255.2.2/24/1483387

Teknik Özellikler:

- 10 FPS tarama hızı
- Tripod ve döner tabla (pıkap) dahil
- Yüksek çözünürlüklü yüzey tarama
- Derinlik füzyonu ve mesh oluşturma desteği

Kullanım Alanları:

- Fiziksel kanıtların üç boyutlu olarak dijitalleştirilmesi
- Donanım bileşenlerinin (anakart, modül, çip) yüzey geometrisinin incelenmesi
- Kasanın veya cihaz içi bileşenlerinin yapısal analizleri
- Siber saldırı sonucu fiziksel hasar değerlendirmesi
- Eğitim amaçlı 3D teknik modellerin oluşturulması
- 3D tarayıcı, laboratuvarın donanım analizini sayısal ortama taşıyan en önemli birimdir.

7.4. Hava ve Mekânsal Taramaya Yönelik Otonom Sistemler

7.4.1. DJI Drone – FPV Combo Drone
Fiş No: 2023/Z/62 — Sicil: 253.3.6/23/3138

Kullanım Amaçları:

- Erişilemeyen alanlardan adli veri toplama
- Kritik altyapı güvenlik değerlendirmesi
- Saha güvenlik denetimlerinde görüntüleme
- Olay yeri havadan kayıt altına alma

7.4.2. Mekânsal Haritalama Robotu – Roborock

Fiş No: 2023/Z/66 — Sicil: 253.3.6/23/3227
Teknik Rolü:

- LIDAR tabanlı SLAM haritalama
- İç mekânlarda 360° tarama
- Otonom navigasyon

Kullanım Alanları:

- Kapalı alanların hızlı mekânsal dijital haritası
- Siber saldırı sonucunda cihaz konumlama analizi
- Olay yeri iç mekân rekonstrüksiyonu
- 3D tarayıcılarla birlikte hibrid mekânsal analiz

7.5. Video, Ses ve Kanıt Toplama Destek Sistemleri

Bu alt başlık, stüdyo ekipmanlarıyla entegrasyonu özetlemektedir. Detaylar Bölüm 8'de verilmiştir.

- Canon M50 ile yüksek çözünürlüklü video üretme
- Rode mikrofonlarla temiz ses kayıt alma
- Godox ışıklarla aydınlatma koşullarının optimize edilmesi

Bu yapı, adli bilişim eğitimleri, teknik demonstrasyonlar ve kanıt doğrulama süreçlerinde yüksek kaliteli kayıt imkânı sunar.

7.6. Adli Görüntüleme Ekosistemi – Sistem bütünlüğü

Dijital adli analiz birimi 4 katmanlı mimariyle çalışır:

- Katman 1 — Fotoğraf ve Video (Canon M50): Delil kayıtlarının temelini oluşturur.
- Katman 2 — Derinlik ve Hareket Analizi (Kinect): Derinlik haritaları ve davranış modellemesi sağlar.
- Katman 3 — 3D Tarama (CR Scan 01): Fiziksel kanıtın üç boyutlu mesh modelini oluşturur.
- Katman 4 — Otonom Mekânsal Tarama (Drone + Roborock): Büyük sahnelerin bütünsel dijital rekonstrüksiyonunu sağlar.

Bu dört katmanlı sistem sayesinde laboratuvar, hem mikro düzeyde (çip, donanım elemanı) hem de makro düzeyde (mekân, olay yeri, erişilemeyen alanlar) dijital analiz gerçekleştirebilmektedir.

BÖLÜM 8 — STÜDYO, SUNUM VE İÇERİK ÜRETİM SİSTEMLERİ

Siber Güç Laboratuvarı yalnızca siber güvenlik araştırmalarının yürütüldüğü bir ortam olmanın ötesinde, teknik eğitim materyallerinin üretildiği, adli bilişim süreçlerinin belgelenebildiği ve bilimsel sunumların kaydedilebildiği profesyonel bir stüdyo altyapısına da sahiptir. Bu altyapı, yüksek kaliteli görüntü–ses kaydı, canlı yayın, eğitim dokümantasyonu ve teknik proje sunumları üretmek için tasarlanmıştır. Laboratuvarın içerik üretim sistemi; mikrofonlar, ışık setleri, ekran birimleri ve görüntüleme cihazlarından oluşan bütünleşik bir ekosistemdir.

8.1. Profesyonel Ses Kayıt Sistemleri

8.1.1. Rode VideoMicro Mikrofon
Fiş No: 2022/Z/31 — Sicil: 255.2.5/22/4146
Teknik Özellikler:

- Süper kardioid yönlü ses yakalama
- Titreşim önleyici montaj
- Kompakt yapı
- Kamera üstü kullanım

Kullanım Alanları:

- Teknik eğitim videolarında net ses kaydı
- Adli bilişim analizlerinin belgelenmesi
- Siber saldırı simülasyonlarında açıklama kaydı
- Laboratuvar içi seminer ve demo çekimleri

8.1.2. Rode Wireless Go II – Kablosuz Mikrofon Sistemi
Fiş No: 2024/Z/142 — Sicil: 255.2.5/24/1482810

Teknik Özellikler:

- Çift vericili kablosuz bağlantı
- Yüksek RF stabilitesi
- 200 metreye kadar kapsama
- Hafıza içi yedekleme

Kullanım Alanları:

- Sunum ve ders kayıtları
- Laboratuvar tanıtım videoları
- Saha analizlerinde kablosuz ses toplama
- Online eğitim ve webinar yayınları
- Wireless Go II, laboratuvarın mobil ve esnek ses kayıt ihtiyaçlarını karşılayan ana çözümdür.

8.2. Profesyonel Stüdyo Işık Sistemleri

Işık sistemleri, görüntü kalitesi için kritik öneme sahiptir. Laboratuvarda hem taşınabilir hem de sabit ışık çözümleri bulunmaktadır.

8.2.1. Godox M1 RGB Mini Mobil Video Işığı (2 Adet)
Fiş No: 2024/Z/143 — Sicil: 255.2.5/24/1482806 ve 1482807

Teknik Özellikler:
- RGB tam renk spektrumu
- Ayarlanabilir sıcaklık (2500–8500K)
- Dahili batarya
- Taşınabilir tasarım

Kullanım Alanları:
- Mobil çekimler
- Donanım incelemelerinde nesne odaklı aydınlatma
- Drone/3D tarayıcı ile çekilen sahnelerin ışık desteği
- Siber olay anlatımlarında görsel kalite artırımı

8.2.2. Godox ES45 RGB Stüdyo LED Işık Kiti (2 Adet)
Fiş No: 2024/Z/144 — Sicil: 255.2.5/24/1482808 ve 1482809
Teknik Özellikler:
- Yüksek parlaklık
- Profesyonel stüdyo için tasarlanmış panel ışık
- RGB destekli renk modları
- Uzaktan kumanda ile kontrol

Kullanım Alanları:
- Stüdyo düzeyinde sunum kayıtları
- Laboratuvar içi eğitim içerikleri
- Online ders videoları
- Resmî tanıtım ve proje anlatım çekimleri

Godox ES45 kitleri, laboratuvarın sabit stüdyo ışık altyapısının temelidir.

8.3. Sunum, Eğitim ve Görsel Destek Ekranları
8.3.1. Philips Geniş Format Ekran (Model 1)
Fiş No: 2024/Z/166 — Sicil: 255.10.2/24/1483405

8.3.2. Philips Geniş Format Ekran (Model 2)
Fiş No: 2024/Z/170 — Sicil: 255.10.2/24/1483386

Kullanım Amaçları:
- SIEM, IDS/IPS ve SOC panellerinin canlı gösterimi
- Canlı ağ trafiği görselleştirme
- Siber saldırı simülasyonlarının ekran yansıtması
- Eğitim oturumları ve öğrenci sunumları

Geniş ekranlar sayesinde laboratuvarda eş zamanlı olarak:
- saldırı haritaları,
- şifre kırma süreçleri,
- GPU yük durumları,
- ağ trafiği grafiksel analizleri izlenebilmektedir.

8.4. Sunum ve Sergileme Altyapısı
8.4.1. Elon Ayaklı Televizyon ve Fuar Standı (42")
Fiş No: 2024/Z/146 — Sicil: 255.7.1/24/1482811
Kullanım Senaryoları:
- Proje sergileri
- Üniversite tanıtım etkinliklerinde laboratuvar gösterimi
- Siber güvenlik yarışmalarında harici ekran ihtiyacı
- Mobil sunum alanı oluşturma

8.5. İçerik Üretim Ekosistemi: Entegrasyon Şeması
Laboratuvardaki stüdyo sistemi, dört aşamalı bir medya üretim altyapısına sahiptir:
1) Ses Katmanı (Rode VideoMicro + Wireless Go II)
- Temiz, yönlü ve kablosuz ses kayıt imkânı sağlar.

2) Işık Katmanı (Godox M1 + ES45 Kitleri)
- Profesyonel aydınlatma ile teknik açıklamaların net görünmesini sağlar.

3) Görselleştirme Katmanı (Canon M50 + Philips Ekranlar)
- Hem kayıt hem sunum için yüksek çözünürlüklü görüntü sunar.

4) Eğitim/Sunum Alanı (Elon Standı + Philips Ekranlar)
- Kurs, eğitim, proje sunumu, seminer ve içerik üretimi için hazır ortam sağlar.

Bu altyapı, laboratuvarın eğitim–araştırma–belgeleme üçlüsünü bütünsel bir yapıya kavuşturmaktadır.

BÖLÜM 9 — MOBİLİTE, ENERJİ VE GENEL DESTEK SİSTEMLERİ

Siber Güç Laboratuvarı yalnızca sabit bir araştırma ortamı değil gerektiğinde saha koşullarında da çalışabilen, bağımsız enerji kaynaklarıyla operasyon yürütebilen taşınabilir bir altyapıya sahiptir. Mobilite ve destek ekipmanları, laboratuvarın hem esnekliğini hem de operasyonel etkinliğini artırır. Bu bölümde tüm destek unsurları, taşınır kayıt belgelerindeki gerçek cihaz adları ve kullanım bağlamları ile birlikte sunulmuştur.

9.1. Mobil Enerji ve Dış Ortam Çalışma Sistemleri

9.1.1. EcoFlow River Pro Taşınabilir Güç Kaynağı (720 Wh)
Fiş No: 2024/Z/86 — Sicil: 253.2.5/24/1481516
Teknik Rolü ve Katkısı
- 720 Wh batarya kapasitesi
- Çoklu AC/DC/USB çıkışı
- Hızlı şarj desteği
- Saha incelemelerinde mobil enerji çözümü

Kullanım Alanları
- Mobil iş istasyonlarına güç sağlama
- Drone, kamera, 3D tarayıcı gibi cihazların sahada şarj edilmesi
- Elektrik kesintisinde kritik analiz operasyonlarının devamı
- Açık alan siber tatbikatlarında enerji çözümü

9.1.2. EcoFlow 160W Taşınabilir Güneş Paneli
Fiş No: 2024/Z/88 — Sicil: 253.3.6/24/1481514
Teknik Rolü
- Açık alanlarda bağımsız enerji üretimi
- EcoFlow güç istasyonlarıyla tam uyum
- Portatif ve hafif tasarım

Kullanım Alanları
- Elektriğin olmadığı alanlarda veri toplama
- Afet veya saha tatbikatlarında sınırsız enerji
- Drone ve kamera operasyonlarını uzun süre destekleme
- Mobil SOC kurulumu

9.2. Sunum, Eğitim ve Operasyon Destek Sistemleri

9.2.1. Taraflı Yazı Tahtası
Fiş No: 2024/Z/145 — Sicil: 255.3.5/24/1482812
Kullanım Alanları
- Laboratuvar içi teknik eğitimler
- Kriptografi ve ağ güvenliği dersleri
- Beyaz tahta modellemeleri, saldırı senaryosu çizimleri
- Proje planlama oturumları
- Çift taraflı ve 360° dönebilen yapısı, laboratuvar içi eğitim süreçlerini oldukça esnek hale getirir.

9.2.2. Elon Ayaklı TV ve Fuar Standı (42")
Fiş No: 2024/Z/146 — Sicil: 255.7.1/24/1482811
Kullanım Amaçları
- Mobil sunum alanı oluşturma
- Üniversite etkinliklerinde laboratuvar tanıtımı

- Siber eğitim senaryolarında büyük ekran kullanım
- Kurumsal gösterimlerde bilgi ekranı
- Sabit ekranlara göre mobil kullanım avantajı ile çok yönlüdür.

9.3. Laboratuvar Organizasyonu ve Mekânsal Düzen Ekipmanları
Bu bölümde, laboratuvar içi düzeni ve operasyonel iş akışlarını destekleyen elemanlar yer alır.
Destek Elemanları:
- Stand ve yerleştirme birimleri (Elon standı ana elemandır)
- Mobil yazı tahtası
- Stüdyo ışık ayakları (Godox kitleri ile birlikte)
- Tripod ve kamera aparatı
- Drone ekipman çantaları
- 3D tarayıcı tripodları

Bu sistemler, laboratuvarın hem eğitim hem operasyonel çalışmaları için ergonomik bir yapı sunar.

9.4. Mobilite Sisteminin Siber Güç Laboratuvarındaki Rolü
Siber Güç Laboratuvarı mobilite altyapısı sayesinde:
- Olay yerine anında müdahale kapasitesi sağlar. ENF cihazı, fotoğraf makinesi, 3D tarayıcı ve taşınabilir enerji sistemleri ile olay yeri incelemesi yapılabilir.
- Elektrik kesintilerinden etkilenmez. EcoFlow + UPS kombinasyonu sayesinde kritik analiz süreçleri durmaz.
- Üniversite içi/dışı eğitim ve tanıtımlara hızla adapte olur. Mobil ekran ve stüdyo sistemleri, etkinliklerde profesyonel sunum yapılmasına izin verir.
- Saha koşullarında araştırma yapabilir hale gelir. Özellikle 3D tarayıcı ve drone birleşimi, kampüs dışı veri toplama görevlerinde büyük avantaj sağlar.

BÖLÜM 10 — ORTAK LABORATUVAR ALANLARI VE GENEL DONANIMLAR
Siber Güç Laboratuvarı'nın operasyonel yapısı yalnızca yüksek teknoloji donanımlardan değil aynı zamanda çalışma ortamını destekleyen ortak kullanım alanlarından da oluşmaktadır. Bu alanlar eğitim, proje yönetimi, teknik toplantılar, laboratuvar içi koordinasyon ve çıktı paylaşımı için kritik öneme sahiptir. Ortak donanımlar, laboratuvarın kullanım verimliliğini artırır, bilgi akışını hızlandırır ve ekip çalışmalarının organize bir şekilde yürütülmesine katkı sağlar. Aşağıda laboratuvarın tüm ortak kullanım donanımları, taşınır kayıtlarındaki gerçek bilgilerle eşleştirilmiş şekilde sunulmaktadır.

10.1. Eğitim ve Beyin Fırtınası Alanları
10.1.1. Yazı Tahtası
Fiş No: 2024/Z/145 — Sicil: 255.3.5/24/1482812
Kullanım Rolü
- Siber güvenlik ve kriptografi eğitimleri
- Ağ mimarisi çizimleri
- Saldırı-savar simülasyon adımları
- Ekip içi teknik toplantılar
- Senaryo akış diyagramlarının modellenmesi

Mobil ve dönebilen yapısı, çok yönlü kullanım sağlar. Laboratuvarda teknik planlama ve eğitimlerin ana destek aracıdır.

10.2. Sunum ve Bilgilendirme Alanları
10.2.1. Philips Geniş Format Ekranlar
Fiş No: 2024/Z/166 — Sicil: 255.10.2/24/1483405
Fiş No: 2024/Z/170 — Sicil: 255.10.2/24/1483386

Kullanım Rolü
- Büyük ölçekli SIEM panellerinin gösterimi
- Gerçek zamanlı saldırı simülasyonlarının görselleştirilmesi
- GPU kullanım – kripto kırma – trafik analiz ekranları

- Eğitim sunumları, ders içerikleri ve teorik anlatımlar
- Proje gösterimleri ve kurum içi sunum toplantıları
- Laboratuvar içinde farklı noktalarda bulunan bu ekranlar, görsel bilgi merkezleri olarak işlev görür.

10.3. Mobil Sunum ve Etkinlik Sistemleri
10.3.1. Elon Ayaklı Televizyon ve Fuar Standı (42”)
Fiş No: 2024/Z/146 — Sicil: 255.7.1/24/1482811

Kullanım Rolü
- Üniversite etkinliklerinde laboratuvar tanıtım
- Siber güvenlik yarışmalarında mobil sunum istasyonu
- Laboratuvar dışı ders/seminer ortamları
- Proje değerlendirme toplantılarında ekran paylaşımı
- Teknik ekiplerle işbirliği sırasında portatif sunum alanı oluşturma
- Stand, laboratuvarın dış ortama taşınabilir sunum kabiliyeti kazandıran önemli bir donanımdır.

10.4. Çalışma Ortamı ve Mekânsal Organizasyon Elemanları
Laboratuvar içi düzeni sağlayan fiziksel bileşenler:
10.4.1. Tripodlar ve Kamera Aparatları
- Canon M50 için tripod
- Kinect kamera için ayaklık
- 3D tarayıcı tripodları

Kullanım:
- Stabil görüntüleme
- Adli kanıtların açısal doğru kayıt altına alınması
- Eğitim videolarının profesyonel çekimi

10.4.2. Işık Ayakları ve Stüdyo Ekipman Ayakları
- Godox M1 ve ES45 kitlerini taşır
- Çekim açısı ve ışık dağılımını profesyonelleştirir

Kullanım:
- Teknik içerik üretimi
- Karanlık donanım incelemelerinde aydınlatma kontrolü
- Eğitim videoları

10.4.3. Drone ve Robotik Taşıma Çantaları
- DJI FPV
- Roborock haritalama robotu

Kullanım:
- Saha görevlerinde güvenli taşıma
- Hassas sensörlerin fiziksel korunması
- Adli inceleme malzemelerinin taşınması

10.4.4. Kablo, Bağlantı ve Ağ Yönetimi Elemanları
- HDMI, Type-C, LAN kabloları
- RJ45 ağ dağıtım bileşenleri
- Ses/video aktarma adaptörleri

Kullanım:
- SOC izleme istasyonlarının bağlantı altyapısı
- NAS – iş istasyonu – ekran senkronizasyonu
- Stüdyo kayıt sistemleri entegrasyonu

10.5. Ortak Kullanım Alanlarının Laboratuvardaki Stratejik Rolü

Siber Güç Laboratuvarı'nın ortak alan donanımları laboratuvara:

- Etkili Eğitim Yeteneği: Gerçek dünya saldırı modelleri, öğrenciler ve araştırmacılar tarafından whiteboard üzerinden modellenebilir.
- Görsel-İşitsel Dokümantasyon Kabiliyeti: Stüdyo+ekran+ışık sistemi sayesinde laboratuvar hem kendi süreçlerini belgeliyor hem de teknik eğitim içerikleri üretiyor.
- Kurumsal Tanıtım ve İşbirliği Avantajı: Mobil stand ve büyük ekranlar, laboratuvarı fakülte dışı etkinliklerde görünür hale getiriyor.
- Ekip Çalışması ve Proje Yönetimi: Beyin fırtınası, proje planlama, akış şemaları oluşturma ve ekip toplantıları için fiziksel altyapı sağlanıyor.
- Olay Yeri Rekonstrüksiyonu ve Senaryo Modelleme: Adli analiz süreçlerinin görsel olarak modellenmesi için ideal çalışma ortamı oluşuyor.

BÖLÜM 11 — LABORATUVAR SİSTEM ENTEGRASYONU VE TEKNİK MİMARİNİN BÜTÜNCÜL YAPISI

Siber Güç Laboratuvarı birbirinden farklı donanım gruplarının tek bir operasyonel çatı altında bütünleşik olarak çalışmasını sağlayan katmanlı bir teknik mimariye sahiptir. Bu mimari yüksek başarımlı hesaplama altyapısı, güvenli veri depolama sistemleri, ağ-elektrik sürekliliği, adli analiz birimleri ve stüdyo–sunum altyapılarından oluşan çok yönlü bir ekosistemi yönetir. Bu bölüm, laboratuvarın sistem bütünlüğünü 6 temel entegrasyon katmanı üzerinden açıklamaktadır.

11.1. Katman 1 — Hesaplama Çekirdeği (HPC + GPU)

Laboratuvarın tüm karmaşık analiz süreçlerinin başlangıç noktası HPC çekirdeğidir.
Ana Bileşenler

- Dell Precision T7920
- RTX 6000 GPU
- iMac 24"
- MacBook Pro (M4)
- Dell M3561
- HP 240 G9
- 27" 4K All-in-One

Bu katmanın temel işlevleri

- Yapay zekâ modellerinin eğitimi
- Kriptografik analizlerin yürütülmesi
- Ağ trafiği ve malware büyük veri işleme
- Sanal makine kümelerinin yönetimi
- Siber saldırı simülasyonlarının çalıştırılması
- Tüm hesaplama talepleri bu çekirdekte başlatılır ve işlem gücü buradan sağlanır.

11.2. Katman 2 — Veri Güvenliği ve Depolama Katmanı (NAS + Offline Storage)

Hesaplama katmanından çıkan veriler, üç aşamalı bir depolama mimarisine aktarılır.
A) Online Depolama (NAS Sistemleri)

- 2 adet WD My Cloud Pro PR4100

Görevleri:

- Gerçek zamanlı veri yazımı
- Proje klasörlerinin yüksek erişilebilirliği
- Log, model, profil, saldırı kayıtlarının muhafazası

B) Hızlı Erişim SSD Depolama

- Kingston 960 GB SSD (2 adet)
- WD Elements Storage

Görevleri:

- Adli bilişim imaj alma

- Büyük veri setlerinin hızlı taşınması

C) Donanımsal Şifreli Depolama
- Apricorn Aegis Secure Key
- Kingston 64GB AES USB

Görevleri:
- Kritik dosyaların offline koruması
- Adli rapor ve delil transferi
- Savunma projeleri için gizli veri saklama

11.3. Katman 3 — Ağ, VoIP ve Haberleşme Katmanı
Hesaplama ve depolama süreçlerinin güvenli biçimde gerçekleşmesi için laboratuvarın ağ haberleşme sistemi devrededir.
Ana Bileşenler
- Ericsson-LG LIP-1010i IP Telefon
- LAN segmenti ve lokal firewall
- Bağlantı adaptörleri ve ağ yönetim modülleri

Görevler
- Kapalı devre iletişim
- VoIP trafik analizi
- IDS/IPS test ortamları
- Ayrılmış güvenli alt ağlar
- Bu katman hem eğitim hem de araştırma senaryolarında ağ güvenliğinin pratik olarak test edilmesini sağlar.

11.4. Katman 4 — Kesintisiz Güç ve Enerji Yönetimi
Laboratuvarın sürdürülebilirliğini sağlayan enerji katmanı, kesinti ve akım dalgalanmalarına karşı tüm sistemleri korur.
Bileşenler
- SRVS1K 1kVA UPS
- EcoFlow River Pro
- EcoFlow 160W Solar Panel

Görevler
- UPS → kritik cihazların kesintisiz enerjisi
- EcoFlow → saha analizlerinde mobil güç
- Solar Panel → off-grid çalışma
- Bu yapı HPC ünitelerinin, NAS sistemlerinin ve adli cihazların veri kaybı yaşamadan çalışmasını teminat altına alır.

11.5. Katman 5 — Dijital Adli Analiz ve 3D Modelleme Katmanı
Hesaplama ve veri güvenliği katmanlarıyla entegre çalışan adli analiz altyapısı, fiziksel ve dijital delilleri 360° kapsayan bir doğrulama ekosistemi oluşturur.
Bileşenler
- Canon M50 Fotoğraf Makinesi
- Kinect Derinlik Kamerası
- 3D MakerPro CR-Scan 01
- DJI FPV Drone
- Roborock Mekânsal Haritalama Robotu
- ENF Veri Toplama Cihazı

Bu katmanın işlevleri

- Fiziksel delillerin görüntülenmesi
- Cihaz yüzey taraması ve 3D modelleme
- Olay yeri mekânsal haritalama
- Zaman damgası doğrulama (ENF)
- Dijital delillerin fiziksel bağlamla eşleştirilmesi
- Bu katman sayesinde laboratuvar hem mikro hem makro ölçekli inceleme yapabilen bütüncül bir adli kapasiteye sahiptir.

11.6. Katman 6 — Stüdyo, Sunum ve Belgeleme Katmanı

Son katman tüm çalışmaların profesyonel biçimde belgelenmesi ve sunulmasını sağlar.

Bileşenler

- Rode VideoMicro
- Rode Wireless Go II
- Godox M1 ve ES45 ışık setleri
- Philips Geniş Format Ekranlar
- Elon Ayaklı TV Standı
- Mobil Yazı Tahtası (ABC)

Görevler

- Eğitim videoları üretimi
- Proje sunumu ve teknik dokümantasyon
- Siber saldırı senaryolarının kayıt altına alınması
- Ders ve workshop içerikleri
- Bu katman, laboratuvarın bilimsel çıktılarını görünür ve erişilebilir kılar.

11.7. Tüm Katmanların Birbiriyle Çalışma Akışı (Özet Şema)

- Veri üretimi (HPC) → hesaplama, saldırı simülasyonu, model eğitimi
- İlk saklama (NAS) → ham veriler, loglar, modeller
- Güvenlik (Şifreli USB + ENF) → kritik dosya transferi ve zaman damgası doğrulama
- Ağ katmanı → VoIP analizi, trafik yakalama, güvenlik testleri
- Adli analiz → görüntüleme, 3D tarama, mekânsal harita
- Belgeleme ve sunum → stüdyo ekipmanları ile içerik oluşturma

Bu bütünleşik yapı laboratuvara, araştırma → analiz → koruma → doğrulama → sunum döngüsünü kesintisiz biçimde yapabilme kabiliyeti kazandırır.

BÖLÜM 12 — SONUÇ VE SİBER GÜÇ LABORATUVARININ STRATEJİK ÖNEMİ

Siber Güç Laboratuvarı Fırat Üniversitesi Teknoloji Fakültesi bünyesinde oluşturulan teknik, akademik ve operasyonel kapasitesiyle hem ulusal hem uluslararası düzeyde rekabetçi bir araştırma ekosistemi ortaya koymaktadır. Bu raporda detaylandırılan cihaz envanteri ve teknik altyapı, laboratuvarın yalnızca donanım gücünü değil; aynı zamanda stratejik konumlandırmasını, araştırma yetkinliğini ve ileri teknoloji üretme kabiliyetini göstermektedir. Laboratuvar; yüksek başarımlı hesaplama altyapısından gelişmiş adli bilişim sistemlerine, saha operasyonlarını destekleyen mobilite araçlarından profesyonel içerik üretim ekipmanlarına kadar çok katmanlı, entegre bir mimariye sahiptir. Bu mimari sayesinde laboratuvar, modern siber güvenlik araştırmalarının gerektirdiği tüm süreçleri — veri toplama, analiz, doğrulama, modelleme, sızma testi, adli inceleme ve sonuç paylaşımı — aynı çatı altında gerçekleştirebilmektedir.

12.1. Üniversite ve Fakülte Açısından Stratejik Katkılar

Siber Güç Laboratuvarı eğitim kapasitesini güçlendirmektedir. Kriptografi, ağ güvenliği, adli bilişim, yapay zekâ destekli siber savunma ve tehdit istihbaratı gibi derslerde uygulamalı eğitim altyapısı sağlayarak fakültenin teknik eğitim seviyesini uluslararası standartlara taşımaktadır. Ayrıca lisansüstü araştırma altyapısının temelini oluşturmaktadır. Laboratuvar yüksek lisans ve doktora tezlerinin yürütülebileceği yüksek kapasiteli bir çalışma ortamı sunmakta öğrenci yetiştirme, proje üretme ve akademik yayın oluşturma süreçlerini hızlandırmaktadır.

Üniversitenin rekabetçi projelere başvuru kapasitesini artırmaktadır TÜBİTAK, AB Horizon, COST Action, Kalkınma Ajansları vb. programlara yapılan başvurular için somut bir altyapı sunmaktadır.

12.2. Ulusal Siber Güvenlik Ekosistemine Katkılar

Siber Güç Laboratuvarı Türkiye'nin siber güvenlik alanındaki millî kapasitesini güçlendiren bir Ar-Ge merkezidir. Katkı alanları:

- Yeni siber güvenlik araçları geliştirme
- Kriptografik algoritma ve anahtar üretim yöntemleri tasarlama
- Kritik altyapıların zafiyet analizi
- Ulusal siber tatbikatlarda teknik ekip desteği
- Dijital adli doğrulama teknolojilerinin araştırılması (ENF vb.)
- Üniversite–sanayi–kamu işbirliği projelerine teknik zemin oluşturma

Laboratuvar sahip olduğu ekipman ve uzmanlık ile Türkiye'nin dijital bağımsızlık hedefleriyle uyumlu bir yapıdadır.

12.3. Akademik ve Bilimsel Çıktılar Açısından Katkılar

Laboratuvarın sunduğu araştırma altyapısı doğrudan akademik çıktıları artırmaktadır.
Potansiyel Bilimsel Çıktılar:

- SCI/SSCI/ESCI indeksli yayınlar
- Uluslararası konferans bildirileri
- Yeni kriptografik ve güvenlik tasarımları
- Yazılım–donanım hibrit güvenlik prototipleri
- Doktora ve yüksek lisans tezleri
- Ulusal ve uluslararası proje patentleri

Bu çıktılar fakültenin akademik görünürlüğünü artırmaktadır.

12.4. Teknoloji Transferi ve Sanayi İşbirlikleri Açısından Katkılar

Laboratuvar savunma, enerji, telekomünikasyon, finans, otomotiv, akıllı şehirler ve kamu güvenliği gibi sektörlerde ihtiyaç duyulan teknolojilerin geliştirilmesine katkı sağlayabilecek kapasitededir. Somut İşbirliği Alanları:

- Zafiyet analizi ve sızma testi hizmetler
- Güvenli yazılım geliştirme danışmanlığı
- Kriptografi tabanlı güvenlik modülleri
- Adli bilişim raporlama destekleri
- Yapay zekâ tabanlı saldırı tespit sistemleri
- Otonom sistem güvenliği araştırmaları

Bu yönüyle laboratuvar, üniversitenin sanayiye teknoloji transferi kapasitesini önemli ölçüde artırmaktadır.

12.5. Gelecek Vizyonu ve Genişleme Potansiyeli

Laboratuvar, mevcut altyapısı üzerine inşa edilebilecek genişleme alanlarına sahiptir:

- Siber Güvenlik Operasyon Merkezi (Mini SOC): Gerçek zamanlı saldırı–savunma simülasyonları ve SIEM entegrasyonları yapılabilir.
- Post-Kuantum Kriptografi Test Merkezi: Araştırmacı yetiştirme ve algoritma performans analizleri için ideal ortam.
- Biyometrik Güvenlik Test Alanı: Kinect + 3D tarayıcı + drone entegrasyonu ile çok katmanlı biyometrik doğrulama çalışmaları.
- Dijital Adli Bilişim Eğitim Merkezi: ENF cihazı ve 3D modelleme altyapısı ile adli uzman yetiştirme potansiyeli.
- Siber Güç Araştırma Ağı: Ulusal projelerde farklı üniversiteler ve kurumlarla ortak çalışmalara zemin hazırlayan bir yapı.

12.6. Genel Değerlendirme

Bu raporda sunulan sistem bileşenleri, Siber Güç Laboratuvarı'nın modern, entegre, yüksek performanslı, stratejik odaklı, sürdürülebilir ve bilimsel üretime uygun bir yapıya sahip olduğunu göstermektedir. Laboratuvar sahip olduğu teknik altyapı ile yalnızca bir çalışma alanı değil aynı zamanda siber güvenlik ve kriptoloji alanında bölgesel ve ulusal bir mükemmeliyet merkezi olma potansiyeline sahiptir.

Birim Sorumluları	Dahili Numara	E-Mail Adresi
Prof. Dr. Fatih ÖZKAYNAK	4304	ozkaynak@firat.edu.tr
Arş. Gör. Beyzanur DURMUŞ	4318	bdurmus@firat.edu.tr
Arş. Gör. Z. Beyza METİN	4218	zbmetin@firat.edu.tr